

原子力規制庁長官官房放射線防護グループ核セキュリティ部門 殿

令和6年度原子力利用安全対策等業務委託費
(米国NRC・英国ONRの検査ガイド調査) 事業

報告書

令和7年3月

日本エヌ・ユー・エス株式会社

本報告書は、原子力規制庁から委託された令和6年度原子力利用安全対策等業務委託費（米国NRC・英国ONRの検査ガイド調査）事業に係る調査について実施した業務の成果をとりまとめたものです。

目 次

1 本調査の概要	1-1
1.1 背景・目的	1-1
1.2 実施内容	1-1
1.2.1 検査ガイドの比較調査	1-1
1.2.2 検査ガイドの改善内容の検討	1-4
1.2.3 調査報告書の作成	1-4
1.3 実施期間	1-5
2 検査ガイドの比較調査	2.1-1
2.1 はじめに	2.1-1
2.2 検査ガイド比較調査の対象と実施方法	2.1-1
2.3 日米検査ガイド比較調査の結果	2.3.1-1
2.3.1 日米検査ガイドの全体体系および図書構成の概要について	2.3.1-1
2.3.2 日米検査ガイド別の比較調査	2.3.2-1
2.3.2.1 PP1301「防護区域等への人の立入り」と IP81000.01「Access Authorization-Effective date」における調査の結果	2.3.2-1
2.3.2.2 PP1801「教育および訓練」と IP81000.07「Security Training」 における調査の結果	2.3.2-12
2.3.2.3 PP1801「教育および訓練」と IP81200.07「Security Training for Decommissioning Nuclear Power Reactors」における調査 の結果	2.3.2-24
2.3.2.4 IP81200.09「Security Plan Changes for Decommissioning Power Reactors」における調査の結果	2.3.2-38

2.3.2.5 IP81300「Physical Security Requirements for Independent Spent Fuel Storage Installations」における調査の結果	2.3.2-45
2.4 日英検査ガイド比較調査の結果	2.4.1-1
2.4.1 英国 ONR 検査ガイドの全体体系および図書構成の概要について	2.4.1-1
2.4.2 日英検査ガイド別の比較調査	2.4.2-1
2.4.2.1 CNS-TAST-GD-1.1 (Issue 1) 「Security Governance and Leadership」における調査の結果	2.4.2-1
2.4.2.2 PP1801「教育および訓練」と CNS-TAST-GD-1.4 (Issue 1) 「Organizational Learning for Security」における調査の結果	2.4.2-13
2.4.2.3 PP1802「定期的な評価および必要な改善」と CNS-TAST-GD-2.1 (Issue 2) 「Maintenance of a Robust Security Culture」における調査の結果	2.4.2-23
2.4.2.4 PP1704「法令遵守および核セキュリティ文化醸成の体制」と CNS-TAST-GD-5.1 (Issue 2) 「Reliability and Resilience of the Security System」における調査の結果	2.4.2-38
2.4.2.5 CNS-TAST-GD-6.1 (Issue 2) 「Categorization for Theft Leadership」における調査の結果	2.4.2-48
2.4.2.6 CNS-TAST-GD-6.2 (Issue 2) 「Categorization for Sabotage」における調査の結果	2.4.2-61
2.4.2.7 PP1201「核物質防護秘密の管理」と CNS-TAST-GD-7.2 (Issue 2.1) 「Information Security」における調査の結果	2.4.2-72
2.4.2.8 PP1202「管理情報の管理」と CNS-TAST-GD-7.4 (Issue 2) 「Physical Protection of Information」における調査の結果	2.4.2-91
2.4.2.9 PP1801「教育および訓練」と CNS-TAST-GD-7.5 (Issue 4) 「Preparation for and Response to Cyber Security Events」における調査の結果	2.4.2-109
2.4.2.10 PP1705「非常の場合の対応」と CNS-TAST-GD-10.2 (Issue 2.2) 「Testing and exercising the security response」における調査の結果	2.4.2-137
2.4.2.11 CNS-INSP-GD-001 (Issue 1) 「Nuclear Security Inspections」における調査の結果	2.4.2-147

2.5 検査ガイドの比較調査まとめ	2.5-1
3 検査ガイドの改善内容の検討	3.1-1
3.1 はじめに	3.1-1
3.2 検査ガイドの改善内容の検討結果	3.2-1
3.2.1 セキュリティ関連検査ガイド図書体系の検討と整備	3.2-1
3.2.2 セキュリティ検査での確認事項の明確化	3.2-4
3.2.3 施設の状態に応じたセキュリティ検査ガイドの拡充および 実務的な検査要領の充足	3.2-4
3.2.4 セキュリティ検査根拠図書の整備	3.2-5
3.2.5 セキュリティ指摘事項に関する評価基準の確立	3.2-6
3.2.6 リスクの考え方の確立 と運用指針の整備	3.2-7
3.2.7 セキュリティ検査に役立つ背景知識・助言の提供	3.2-9
3.2.8 セキュリティ検査に関わるグッドプラクティスの整備と活用	3.2-10
3.3 検査ガイドの改善内容の検討まとめ	3.3-1
4 まとめ	4-1

1 本事業の概要

1.1 背景・目的

原子力規制庁（NRA）は、2018 年より米国原子力規制委員会（Nuclear Regulatory Commission, NRC）の原子炉監督プロセス（Reactor Oversight Process, ROP）を参考に検査制度の見直しを進め、ROP に倣った検査制度として、2020 年より原子力規制検査を運用している。そのため、原子力規制検査を行う上で原子力規制庁が参照する検査ガイドについても、ROP に関連する検査ガイドの内容を参考に 2020 年に策定しており、2020 年の原子力規制検査の制度運用開始以降も適宜検査ガイドを改善するための改正を加えている。このような中、NRC においても改善のために検査ガイドを見直しているが、NRC の検査ガイドは多岐にわたっており、膨大な量があるため、原子力規制庁として米国 NRC に加えて、英国原子力規制局（Office for Nuclear Regulation, ONR）など諸外国規制当局の検査ガイドの全容や改訂の動向の把握に務めている。また、実用発電用原子炉の原子力規制検査は、前述のとおり、実用発電用原子炉の先進国である米国 NRC の検査制度を参考にしているところ、核燃料施設の原子力規制検査は、核燃料施設の先進国である英国 ONR の検査制度も参考にしようとしている。ONR の検査ガイドも適宜改善されていることから、その動向の把握等にも注力している。原子力規制庁として、NRC、ONR の検査ガイドの継続改善等 NRC 側、ONR 側の動向を適時適切に把握し、原子力規制庁が参照する検査ガイドの継続改善に検討、反映させることが求められる。

本調査は、原子力規制検査にて原子力規制庁職員が参照する検査ガイドと NRC、ONR の検査ガイドを比較する調査を行い、原子力規制検査の運用改善に資する情報を得ることを目的としている。

1.2 実施内容

本事業の実施内容は、以下に示す「検査ガイドの比較調査」、「検査ガイドの改善内容の検討」から構成される。各項目についての調査から得られた結果を整理し、報告書にまとめる。

1.2.1 検査ガイドの比較調査

検査ガイドの比較調査では、仕様書に示されている原子力規制庁が参照する検査ガイドと NRC、ONR の検査ガイドの内容の比較を行い、その相違を調査する。具体的には、表 1.2.1-1 に示す原子力規制庁と NRC、ONR の検査ガイドの内容の比較を行い、相違を調査し、調査した結果を整理してまとめる。また、調査の過程で、表 1.2.1-1 に示す以外の

NRC の検査ガイドのうち、関連のある検査マニュアル (IMC)、検査手順書 (IP)、NRC 文書のほか、ONR の検査ガイド関連文書、原子力規制庁から公開された原子力規制庁の検査ガイドに関する情報ソースなどを参考情報として活用した。それぞれの情報ソースの詳細内容は、表 1.2.1-2 に示す。

原子力規制庁が参照する検査ガイドは、主に NRC の ROP に関連する検査ガイドの内容を参考に 2018 年～2019 年の新検査制度の検討時に策定され、以降適宜見直し、改訂されてきた。この経緯を踏まえて、本年度の調査では、原子力規制庁の検査ガイドと仕様書に示された NRC、ONR にて発行された関連の検査ガイドと対応したものを中心に調査を行った。このほかに、現段階で原子力規制庁が用いる検査ガイドとして対応したものがないが、近い将来日本でも整備したほうが良いと思われるものの参考として、原子力セキュリティ検査 (ONR の CNS-INSP-GD-001 Nuclear Security Inspections) を追加して調査した (2.4.2-11 参照)。これらすべての調査結果を整理し、本年度の調査報告書にまとめた。

表 1.2.1-1 原子力規制庁の検査ガイドと NRC、ONR の検査ガイド

No	原子力規制庁の 検査ガイド	NRC の検査ガイドのうち関連性があると思 われるガイド	比較ま とめ表
1	PP1301 防護区域等へ の人の立入り	IP81000.01 Access Authorization – Effective date 01/01/2025（建設フェーズ） IP71130.01 Access Authorization – Effective date 01/01/2025（運転フェーズ）	2.3.1-1 —
2	PP1801 教育および訓 練	IP81000.07 Security Training（建設フェーズ） IP71130.07 Security Training（運転フェーズ）	2.3.1-2 —
3	PP1801 教育および訓 練	IP81200.07 Security Training for Decommissioning Nuclear Power Reactors（廃 止措置フェーズ）	2.3.1-3
4	—	IP81200.09 Security Plan Changes for Decommissioning Power Reactors	2.3.1-4
5	—	IP81311 Physical Security Requirements for Independent Spent Fuel Storage Installations	2.3.1-5
	原子力規制庁の 検査ガイド	ONR の検査ガイドのうち関連性があると思 われるガイド	
6	—	CNS-TAST-GD-1.1 (Issue 1) Security Governance and Leadership	2.4.2-1
7	PP1801 教育および訓 練	CNS-TAST-GD-1.4 (Issue 1) Organizational Learning for Security	2.4.2-2
8	PP1802 定期的な評価 および必要な改善	CNS-TAST-GD-2.1 (Issue 2) Maintenance of a Robust Security Culture	2.4.2-3
9	PP1704 法令遵守およ び核セキュリティ文 化醸成の体制	CNS-TAST-GD-5.1 (Issue 2) Reliability and Resilience of the Security System	2.4.2-4
10	—	CNS-TAST-GD-6.1 (Issue 2) Categorization for Theft	2.4.2-5
11	—	CNS-TAST-GD-6.2 (Issue 2) Categorization for Sabotage	2.4.2-6
12	PP1201 核物質防護秘 密の管理	CNS-TAST-GD-7.2 (Issue 2.1) Information Security	2.4.2-7
13	PP1202 管理情報の管 理	CNS-TAST-GD-7.4 (Issue 2) Physical Protection of Information	2.4.2-8
14	PP1801 教育および訓 練	CNSS-TAST-GD-7.5 (Issue 4) Preparation for and Response to Cyber Security Events	2.4.2-9
15	PP1705 非常の場合の 対応	CNS-TAST-GD-10.2 (Issue 2.2) Testing and exercising the security response	2.4.2-10
16	—	CNS-INSP-GD-001 Nuclear Security Inspections	2.4.2-11 仕様外 *参考

表 1.2.1-2 本調査で活用した主な情報ソース

No.	項 目	情報ソース
1	原子力規制庁の検査ガイド	https://www2.nra.go.jp/activity/regulation/kiseikensa/guide_index.html
2	NRC の検査ガイド 関連	https://www.nrc.gov/reading-rm/doc-collections/insp-manual/manualchapter/index.html https://www.nrc.gov/reading-rm/doc-collections/insp-manual/inspectionprocedure/index.html
3	ONR の検査ガイド 関連	https://www.onr.org.uk/publications/regulatory-guidance/ https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-safety-tags/technical-assessment-guides-tags-nuclear-safety-full-list/ https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/security-assessment-principles-syaps/security-assessment-principles-syaps/ https://www.onr.org.uk/publications/regulatory-guidance/regulatory-inspection/technical-inspection-guides-tigs/nuclear-safety-tigs/technical-inspection-guides-tigs-nuclear-safety-full-list/ https://www.onr.org.uk/publications/regulatory-guidance/regulatory-inspection/compliance-inspection-operational-experience-guidance/operational-experience-guidance-full-list/

1.2.2 検査ガイドの改善内容の検討

上記で調査した米国 NRC、英国 ONR、原子力規制庁の各々の検査ガイドの相違等をもとに、原子力規制庁が用いる検査ガイドに対する改善内容を検討しまとめた。具体的には、日米、日英検査ガイドの主な相違点を踏まえて、今後原子力規制検査の運用改善に資するような改善点を検討、整理し、検討の結果をまとめた。

1.2.3 調査報告書の作成

本調査において、上記各項目における調査、検討した結果等を整理して、調査報告書にまとめた。

1.3 実施期間

本事業の実施期間は、以下に示す。

実施期間：令和 6 年 12 月 18 日～令和 7 年 3 月 28 日まで

2 検査ガイドの比較調査

2.1 はじめに

本年度実施した検査ガイドの比較調査では、原子力規制庁が用いる検査ガイド（セキュリティ関連）および米国 NRC、英国 ONR の検査ガイド（セキュリティ関連）との調査を実施した。具体的には、以下に示す検査ガイドの調査対象、調査方法で行った。また、調査の中で、原子力規制庁、NRC、および ONR から公開されたセキュリティ関連のガイド最新版を使用した。日米検査ガイドの比較調査、日英検査ガイドの比較調査について、調査した結果をそれぞれ整理し、まとめた。

2.2 検査ガイド比較調査の対象と実施方法

(1) 日米検査ガイド比較調査の対象と実施方法

日米検査ガイド比較調査の対象について、仕様書に示している原子力規制庁が用いる検査ガイド（セキュリティ関連）と、米国 NRC 検査ガイド（セキュリティ関連）との関連性のあるものとして選定されたものを対象に調査した。調査対象の検査ガイド、原子力規制庁が用いる検査ガイドと NRC の検査ガイドのうち関連性があると思われるガイドとの対応を表 2.2-1 に示している。

表 2.2-1 原子力規制庁の検査ガイドと NRC 検査ガイドの対応
(セキュリティ関連)

No	原子力規制庁の検査ガイド	NRC の検査ガイドのうち関連性があると思われるガイド	比較 まとめ表
1	PP1301 防護区域等への人の立入り	IP81000.01 Access Authorization – Effective date 01/01/2025（建設フェーズ）	2.3.2-1
2	PP1801 教育および訓練	IP81000.07 Security Training（建設フェーズ）	2.3.2-2
3	PP1801 教育および訓練	IP81200.07 Security Training for Decommissioning Nuclear Power Reactors（廃止措置フェーズ）	2.3.2-3
4	—	IP81200.09 Security Plan Changes for Decommissioning Power Reactors	2.3.2-4
5	—	IP81311 Physical Security Requirements for Independent Spent Fuel Storage Installations	2.3.2-5

日米検査ガイド比較調査の実施方法について、原子力規制庁の検査ガイドと NRC の検査ガイドのうち関連性があると思われるガイドを抽出し、整理した。対応する原子力規制庁の検査ガイドおよび NRC 検査ガイドの図書構成を踏まえて、各項目にあるガイドの関連記載内容を抽出し、比較した。

比較の結果から、日米検査ガイド両者間の相違点などを整理し、まとめた。調査の中で、原子力規制庁の検査ガイドにない内容の記載が NRC 検査ガイドにある場合、NRC 検査ガイドの項目を追加して記載した。同じように、NRC 検査ガイドになく、原子力規制庁の検査ガイドにあり、今後も日本の規制検査に有用で、有効に機能するようなガイドの内容がある場合、これを追加記載する。

さらに、対象の検査ガイド以外に、日米検査ガイドの関連情報から、今後原子力規制庁の検査ガイドの継続運用の見直しに資するような内容がある場合、これも参考として追加記載することにした。

比較調査結果について、各ガイド別に、図 2.2-1 に示す日米検査ガイド比較結果まとめのイメージのように、原子力規制庁の検査ガイドの主な内容、NRC 検査ガイドの関連内容、両者間の主な相違点等をまとめた。

NRA検査ガイドの内容 (抜粋)		米NRC検査ガイドの内容 (抜粋)		両者の相違点等
NRA 検査ガイド ⁴²⁾ 【ガイド】 PP1301 防衛区域等への人の立入り ⁴³⁾ 改正 2、2023/05/31 (記載の補正) ⁴⁴⁾ (2頁) ⁴⁵⁾		米NRC 検査ガイド ⁴⁶⁾ 【ガイド】 IP81000.01 「Access Authorization-Effective date」 ⁴⁷⁾ (Issue Date: 04/01/19, Effective Date: 04/01/2019) (16頁) ⁴⁸⁾		両者の主な相違点 ⁴⁹⁾
項目 ⁵⁰⁾	主な内容 ⁵¹⁾	項目 ⁵²⁾	主な内容 ⁵³⁾	
図書全体構成 ⁵⁴⁾	本文 ⁵⁵⁾ 改訂履歴 ⁵⁶⁾	図書全体構成 ⁵⁷⁾	本文 ⁵⁸⁾ 改訂履歴 ⁵⁹⁾	
— ⁶⁰⁾	— ⁶¹⁾	PROGRAM APPLICABILITY ⁶²⁾	IMC 2200 Appendix A, IMC 2562 ⁶³⁾	NRC ⁶⁴⁾ ・対象検査プログラム ⁶⁵⁾ ✓ IMC 2200 App.A (建設時セキュリティ検査プログラム) ⁶⁶⁾ ✓ IMC 2562 (度ふ停止後の LWR 再稼働検査プログラム) ⁶⁷⁾
1. 監視機能 ⁶⁸⁾	大分県及び分県：「防衛防衛」 ⁶⁹⁾ 邦国防衛：「立入承認」 ⁷⁰⁾ 検査分野：「防衛区域等への人の立入り（常時立入者への説明書等の発行）」 ⁷¹⁾	— ⁷²⁾	— ⁷³⁾	NRA ⁷⁴⁾ ・監視機能の区分 ⁷⁵⁾
2. 検査の目的 ⁷⁶⁾	2.1 目的 ⁷⁷⁾ 当第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防衛防衛）のうち、原子力施設の運転などの防衛防衛に係る規則事項で規定される防衛区域等への人の立入り（常時立入者への説明書等の発行）状況を監視する。当該事項は、当第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（防衛防衛防衛）の遵守状況の監視と合わせて行う。 ⁷⁸⁾ これらの監視については、防衛区域等への人の立入り（常時立入者への説明書等の発行）の検査分野における防衛、訓練、教育及び監理等の力量にも留意する。 ⁷⁹⁾ 2.2 防衛防衛の目的 ⁸⁰⁾ 防衛区域等への常時立入者の必要性を監視し、常時立入者を必要最低限の者に限定することにより、内部脅威のリスクを低減する。 ⁸¹⁾	01. INSPECTION OBJECTIVES ⁸²⁾	01.01 To verify that the licensee has developed and is implementing, or is prepared to implement, its Access Authorization (AA) program in accordance with the U.S. Nuclear Regulatory Commission (NRC)-approved security plans. ⁸³⁾ 01.02 To verify that the licensee has developed and is implementing, or is prepared to implement, measures to ensure that its AA program provides assurance that individuals granted unescorted access are trustworthy, reliable, and do not constitute an unreasonable risk to public health and safety or the common defense and security. ⁸⁴⁾ 01.03 To verify that the licensee has developed and is implementing, or is prepared to implement, measures to ensure that the behavioral observation provisions of the licensee's AA program provides assurance of continued reliability and trustworthiness of personnel with unescorted access. ⁸⁵⁾ 01.04 To verify and assess that the licensee has developed and is implementing, or is prepared to implement, provisions of the insider mitigation ⁸⁶⁾	NRA ⁸⁷⁾ ・検査の目的 ⁸⁸⁾ ✓ 防衛的な位置づけと目的（防衛区域等への立ち入りの監視） ⁸⁹⁾ NRC ⁹⁰⁾ ・検査の目的 ⁹¹⁾ ✓ NRC が承認したセキュリティ計画に従ってアクセス許可（AA）プログラムを構築し、実施中か実施準備できていることを確認 ⁹²⁾ ✓ エスコートなしアクセスを許可された個人に対する適切な対策を講じ、実施中か実施準備ができていることを確認 ⁹³⁾ ✓ エスコートなしアクセスを許可された個人の継続的な信頼性と信頼性を保証する適切な対策を講じ、実施中か実施準備できていることを確認 ⁹⁴⁾ ✓ 活動的なインサイダー、活動的で潜在的なインサイダーを識別する効果的なインサイダー識別プログラムを構築し、実施中か実施準備できていることを確認・評価 ⁹⁵⁾

図 2.2-1 日米検査ガイド比較結果まとめのイメージ

日米検査ガイドの各ガイド別の比較調査結果は、表 2.3.2-1～表 2.3.2-5 にまとめている。

(2) 日英検査ガイド比較調査の対象と実施方法

日英検査ガイド比較調査の対象について、仕様書に示されている原子力規制庁が用いる検査ガイド（セキュリティ関連）と、英国 ONR 検査ガイド（セキュリティ関連）との関連性のあるものとして選定されたものを対象に調査した。調査対象の検査ガイド、原子力規制庁が用いる検査ガイドと ONR の検査ガイドのうち関連性があると思われるガイドとの対応を表 2.2-2 に示している。なお、原子力規制庁が用いる検査ガイドおよび ONR の検査ガイドは、現在公開されているものを使用した。

さらに、仕様書対象外ではあるが、今後原子力規制庁の検査ガイドにおける運用改善の検討に資する資料として、ONR のセキュリティ検査に共通の検査用ガイダンスを示す「セキュリティ検査、CNS-INSP-GD-1.0 - Nuclear security inspections」を追加して調査した。

表 2.2-2 原子力規制庁の検査ガイドと ONR 検査ガイドの対応
(セキュリティ関連)

No	原子力規制庁の検査ガイド	ONR の検査ガイドのうち関連性があると思われるガイド	比較まとめ表
1	—	CNS-TAST-GD-1.1 (Issue 1) Security Governance and Leadership	2.4.2-1
2	PP1801 教育および訓練	CNS-TAST-GD-1.4 (Issue 1) Organizational Learning for Security	2.4.2-2
3	PP1802 定期的な評価および必要な改善	CNS-TAST-GD-2.1 (Issue 2) Maintenance of a Robust Security Culture	2.4.2-3
4	PP1704 法令遵守および核セキュリティ文化醸成の体制	CNS-TAST-GD-5.1 (Issue 2) Reliability and Resilience of the Security System	2.4.2-4
5	—	CNS-TAST-GD-6.1 (Issue 2) Categorization for Theft	2.4.2-5
6	—	CNS-TAST-GD-6.2 (Issue 2) Categorization for Sabotage	2.4.2-6
7	PP1201 核物質防護秘密の管理	CNS-TAST-GD-7.2 (Issue 2.1) Information Security	2.4.2-7
8	PP1202 管理情報の管理	CNS-TAST-GD-7.4 (Issue 2) Physical Protection of Information	2.4.2-8
9	PP1801 教育および訓練	CNSS-TAST-GD-7.5 (Issue 4) Preparation for and Response to Cyber Security Events	2.4.2-9
10	PP1705 非常の場合の対応	CNS-TAST-GD-10.2 (Issue 2.2) Testing and exercising the security response	2.4.2-10
11	—	CNS-INSP-GD-001 Nuclear Security Inspections	2.4.2-11 仕様外 *参考

日英検査ガイド比較調査の実施方法について、原子力規制庁の検査ガイドと ONR の検査ガイドのうち関連性があると思われるガイドを抽出し、整理した。対応する原子力規制庁の検査ガイドおよび ONR 検査ガイドの図書構成を踏まえて、各項目にあるガイドの関連記載内容を抽出し、比較した。比較の結果として、日英検査ガイド両者間の相違点などを整理し、まとめた。調査の中で、原子力規制庁の検査ガイドにない内容の記載が ONR 検査ガイドにある場合、ONR 検査ガイドの項目を追加して記載した。同じように、ONR 検査ガイドにない、原子力規制庁の検査ガイドにあり、今後も日本の規制検査に有用で、有効に機能するようなガイドの内容がある場合、これを追加記載する。

さらに、対象の検査ガイド以外に、日英検査ガイドの関連情報から、今後原子力規制庁の検査ガイドの継続運用の見直しに資するような内容がある場合、これも参考として追加記載することにした。

比較調査した結果を整理した。整理の中で、原子力規制庁検査ガイドの主な内容、ONR 検査ガイドの関連内容、両者間の主な相違点等をガイド別に、図 2.2-2 に示す日英検査ガイド比較結果まとめのイメージのようにそれぞれまとめた。

NRA検査ガイドの内容 (抜粋)		英ONR検査ガイドの内容 (抜粋)		両者の相違点等
原子力規制庁検査ガイド 【ガイド】 PP1801 教育及び訓練 (2023.05/31 初版) (2 頁)		英国 ONR 検査ガイド 【ガイド】 CNS-TAST-GD-1.4 (Revision 1) Organizational Learning for Security (March 2020) (13 頁)		両者間の主な相違点
項目	主な内容	項目	主な内容	
図書全体構成	本文 改訂情報	図書全体構成	表紙 目次 本文 参考文献 用語・略語 付録 改訂情報	
1. 監督権限	大分類及び小分類: 「核物質防護」 評価領域: 「特定核燃料物質の管理」、「核物質 防護情報の管理」、「立入承認」、「出入管 理」、「物理的防護」、「情報セキュリティ防護」。 検査分野: 「教育及び訓練」	ガイド ID カテゴリー	CNS	原子力規制庁 ・ 監督権限の区分 ONR ・ ガイドの大分類 (CNS=検査セキュリティ)
本文		1. Introduction	1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that <u>dutyholders</u> must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the <u>dutyholders</u> , which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 1.2 The term 'security plan' is used to cover all <u>dutyholder</u> submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 <u>dutyholders</u> may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	原子力規制庁 ・ とくになし ONR ・ 序論 (CNS ガイド共通。概要は CNS-TAST-GD-1.1 の比較表に同じ)

図 2.2-2 日英国査ガイド比較結果まとめのイメージ

日英検査ガイドの各ガイド別の比較調査結果は、表 2.4.2-1～表 2.4.2-11 にまとめている。

2.3 日米検査ガイド比較調査の結果

2.3.1 日米検査ガイドの全体体系および図書構成の概要について

本年度実施した日米検査ガイドの比較調査では、仕様書に示されている原子力規制庁が用いる検査ガイド（セキュリティ関連）および米国 NRC の検査ガイド（セキュリティ関連）を踏まえて、原子力規制庁および NRC から発行されたセキュリティ規制検査と関連のある検査ガイド、およびセキュリティ規制検査の関連情報などを含めて調査を実施した。

NRC 検査ガイドの全体体系は、基本的には安全関連とセキュリティ関連に分けて構成されている。セキュリティ関連検査ガイド図書は、上位図書の NRC 検査マニュアル（Inspection Manual Chapters, IMC）と、下位図書の検査手順書（Inspection Procedures, IP）で構成されている。上位図書の IMC は、IP が適用される検査分野の共通事項を記載したマニュアルである。NRC のセキュリティ関連検査ガイド IMC、IP のうち、主なものとして、それぞれ表 2.3.1-1、表 2.3.1-2 にまとめた。以下に、主要なセキュリティ関連検査ガイド全体体系のイメージを示す。

上位図書（IMC の例）：

- ・発電用運転炉セキュリティ検査プログラム（IMC 2201：Security Inspection Program for Operating Commercial Nuclear Power Reactors）
- ・セキュリティ検査プログラム（建設）（IMC 2200：Security Inspection Program for Construction）

下位図書（IP の例）：

- ・セキュリティの検査手順書（IP 81000：Security）
- ・アクセス許可の検査手順書（IP 81000.01：Access Authorization）
- ・訓練セキュリティの検査手順書（IP 81000.07：Security Training）
- ・廃炉訓練セキュリティの検査手順書（IP 81200.07：Security Training for Decommissioning Nuclear Power Reactors）
- ・廃炉計画変更セキュリティの検査手順書（IP 81200.09：Security Plan Changes for Decommissioning Power Reactors）
- ・単独の使用済燃料貯蔵施設（ISFSI）の物理的防護要件に関する検査手順書（IP 81311：Physical Security Requirements for Independent Spent Fuel Storage Installations）など

NRC の検査ガイドの図書構成では、IMC には、ガイド別に多少の違いはあるものの、概して表紙、目次、本文、参考文献、付録、改訂情報などで構成されている。IMC の内容と

しては、主に目的、目標、適用範囲、定義（用語など）、権限と義務、検査要件などの内容を記載している。IP の内容は、IMC と同様、ガイド別に多少の違いはあるものの、概して表紙、目次、本文、参考文献、付録、改訂情報などで構成されている。NRC のセキュリティ関連検査ガイドは、機微なセキュリティ情報等のため、非公開のものがある。公開版のガイドは、その記載内容が全体的に比較的シンプルなものとなっている。NRC のセキュリティ関連検査ガイド図書構成の詳細は、表 2.3.2-1～表 2.3.2-5 を参照する。

表 2.3.1-1 NRC セキュリティ関連検査ガイド（上位図書 IMC 例）

区分	番号	タイトル	調査対象 (仕様書より)	関連の IP
IMC	2200	Security Inspection Program for Construction	—	81000.01
IMC	2200A	Security Construction Inspection Program	—	81000.01
IMC	2201	Security Inspection Program for Operating Commercial Nuclear Power Reactors	—	
IMC	2201C	Generic, Special, and Infrequent Inspections	—	81311
IMC	2202	Security Inspection Program for Decommissioning Nuclear Power Reactors	—	
IMC	2202A	Security Core Inspection Program	—	81200.07 81200.09
IMC	2202B	Supplemental Inspection Program	—	81311
IMC	2562	Light-Water Reactor Inspection Program for Restart of Reactor Facilities following Permanent Cessation of Power Operations	—	81000.01
IMC	2690	Inspection Program for Storage of Spent Reactor Fuel and Reactor-related Greater-THAN-Class C Waste at Independent Spent Fuel Storage Installations and for 10 CFR Part 71 Transportation Packagings	—	

表 2.3.1-2 NRC セキュリティ関連検査ガイド (IP 例)

区分	番号	タイトル	調査対象 (仕様書 より)	関連の IMC
IP	81000	Security	—	
IP	81000	Security – Effective date 01/01/2025	—	
IP	81000.01	Access Authorization – Effective date 01/01/2025	○	2200A 2562
IP	81000.02	Access Control		
IP	81000.07	Security Training	○	2200A
IP	81200	Security	—	
IP	81200.01	Access Authorization for Decommissioning Nuclear Power Reactors	—	
IP	81200.06	Protection of Safeguards Information for Decommissioning Nuclear Power Reactors	—	
IP	81200.07	Security Training for Decommissioning Nuclear Power Reactors	○	2202A
IP	81200.09	Security Plan Changes for Decommissioning Power Reactors	○	2202A
IP	81311	Physical Security Requirements for Independent Spent Fuel Storage Installations	○	2201C 2202B 2690
IP	81700.01	Category I Fuel Cycle Facility Strategic Special Nuclear Material Security Controls	— 非公開	
IP	81700.02	Category I Fuel Cycle Facility Access Control Measures	— 非公開	
IP	81700.04	Category I Fuel Cycle Facility Security Equipment Performance, Testing and Maintenance	— 非公開	
IP	81700.06	Licensee Conducted Force-on-Force Exercises at Category I Fuel Cycle Facilities	—	
IP	81700.07	Category I Fuel Cycle Facility Security Training	— 非公開	
IP	81700.08	Category I Fuel Cycle Facility Fitness-for-Duty Programs	— 非公開	
IP	81700.09	Security Measures for Licensed Facilities	— 非公開	
IP	81700.11	Annual Observation of Licensee Conducted Force-on-Force Exercises at Category I Fuel Cycle Facilities	—	
IP	81815	Authorization for Access to National Security Information (NSI) & Restricted Data (RD)	— 非公開	

2.3.2 日米検査ガイド別の比較調査

2.3.2.1 PP1301「防護区域等への人の立入り」と IP81000.01「Access Authorization Effective date」における調査の結果

原子力規制庁および NRC の検査ガイドの主な内容および相違点を整理し、表 2.3.2-1 にまとめた。主な比較結果を以下に示す。より詳細は、表の備考欄参照。

2.3.2.1.1 対象とする検査プログラム

NRC の検査ガイドでは、上位図書（IMC）情報から、次の検査プログラムで使うことが分かる。

- ・ 建設時セキュリティ検査
- ・ 恒久停止後の軽水炉再起動検査

2.3.2.1.2 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

NRC の検査ガイドでは、監督領域を定義していない。（建設フェーズの検査ガイドであって、運転フェーズの原子炉監督プロセス（ROP）の検査ガイドではないため）

2.3.2.1.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（防護区域等への立ち入りの確認）を簡潔に記載している。

NRC の検査ガイドでは、検査官が確認すべき事項を具体的に列挙している（5 項目）。例えば、最初の項目は、「NRC が承認したセキュリティ計画にしたがって、アクセス許可（AA）プログラムを策定し、実施中か実施準備できていることを確認する」である。

2.3.2.1.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

NRC の検査ガイドでは、検査リソースの目安（検査時間、サンプル数）が示されている。検査要件そのものは、次項の検査手順に対応する部分でガイダンスを含めて詳細に示している。

2.3.2.1.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 立ち入りの必要性、資格の確認

- ・ 証明書等の発行の適切性を文書、ワークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

NRC の検査ガイドでは、次のように分けて具体的な検査手順および個別のガイダンスを詳細に示している（添付表の備考欄参照）。

- ・ 一般的ガイダンス（共通事項）
- ・ 実施手順書
- ・ エスコートなしアクセスの承認、再調査および承認の維持
- ・ 行動観察プログラムおよびインサイダー脅威の緩和
- ・ 情報共有
- ・ 人事情報管理
- ・ レビュー

2.3.2.1.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

2.3.2.1.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

NRC の検査ガイドでは、より詳細な改訂履歴を示しており、旧版検査ガイドの発行日、ADAMS 登録番号、改訂内容の説明などを記載している。さらに、本文中では改訂部分のテキストを赤字で、改訂範囲を欄外の縦バーで示し、改訂部分が明示している。

表 2.3.2-1 原子力規制庁検査ガイド PP1301 と米国 NRC 検査ガイド IP81000.01 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1301 防護区域等への人の立入り 改正 2、2023/05/31（記載の適正化）（2 頁）			米国 NRC 検査ガイド 【ガイド】IP81000.01 「Access Authorization-Effective date」 (Issue Date: 04/01/19, Effective Date: 04/01/2019)（16 頁）		両者間の主な相違点
項目		主な内容	項目	主な内容	
図書全体構成		本文 改訂情報	図書全体構成	本文 改訂情報	
	—	—	PROGRAM APPLICABILITY	IMC 2200 Appendix A, IMC 2562	NRC ・対象検査プログラム ✓ IMC 2200 App. A（建設時セキュリティ検査プログラム） ✓ IMC 2562（恒久停止後の LWR 再起動検査プログラム）
	1. 監督領域	大分類および小分類：「核物質防護」 評価領域：「立入承認」 検査分野：「防護区域等への人の立入り（常時立入者への証明書等の発行）」	—	—	NRA ・監督領域の区分
	2. 検査の目的	2.1 目的 法第 6 1 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される防護区域等への人の立入り（常時立入者への証明書等の発行）状況を確認する。当該事項は、法第 6 1 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、防護区域等への人の立入り（常時立入者への証明書等の発行）の検査分野における体制、訓練・教育および警備員等の力量にも留意する。 2.2 防護措置の狙い 防護区域等への常時立入者の必要性を確認し、常時立入者を必要最低限の者に限定することにより、内部脅威者のリスクを低減する。	01. INSPECTION OBJECTIVES	01.01 To verify that the licensee has developed and is implementing, or is prepared to implement, its Access Authorization (AA) program in accordance with the U.S. Nuclear Regulatory Commission (NRC)-approved security plans. 01.02 To verify that the licensee has developed and is implementing, or is prepared to implement, measures to ensure that its AA program provides assurance that individuals granted unescorted access are trustworthy, reliable, and do not constitute an unreasonable risk to public health and safety or the common defense and security. 01.03 To verify that the licensee has developed and is implementing, or is prepared to implement, measures to ensure that the behavioral observation provisions of the licensee’s AA program provides assurance of continued reliability and trustworthiness of personnel with unescorted access. 01.04 To verify and assess that the licensee has developed and is implementing, or is prepared to implement, provisions of the insider mitigation program that are effective in mitigating the active insider and active violent insider. 01.05 To verify that the licensee’s physical protection	NRA ・検査の目的 ✓ 法的な位置づけと目的（防護区域等への立ち入りの確認） NRC ・検査の目的 ✓ NRC が承認したセキュリティ計画にしたがってアクセス許可 (AA) プログラムを策定し、実施中か実施準備できていることを確認 ✓ エスコートなしアクセスを許可された個人に対する適切な対策を開発し、実施中か実施準備ができていることを確認 ✓ エスコートなしアクセスを許可された個人の継続的な信頼性と信用性を保証する適切な対策を開発し、実施中か実施準備できていることを確認・評価 ✓ このサンプルに関連する物理的防護プログラムが 10 CFR) 73.55(b) の一般的なパフォーマンス目標を満たすよう設計され実施中か実施準備で

				program associated with this sample is designed and implemented, or is prepared to implement, to meet the general performance objective of Title 10 of the <i>Code of Federal Regulations</i> (10 CFR) 73.55(b).	きているかを確認
3. 検査要件	3.1 検査対象 防護区域等への常時立入者として証明書等を発行された者の全てが検査対象となり得るが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、当該施設の防護区域等への人の立入り（常時立入者への証明書等の発行）の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 １年間に１回程度 （２）検査時間 ３人／１．２５（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	03. RESOURCE ESTIMATE		The resource estimate for this inspection procedure is approximately 32 hours of direct on-site inspection. The sample size for this procedure is 36.	NRA ・検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 NRC ・検査リソースの目安 ✓ 検査時間、サンプル数
検査手順	防護区域、周辺防護区域または立入制限区域に常時立ち入ろうとする者については、各区域への立入りの必要性を確認の上、証明書等を発行していることを確認する。また、証明書等の発行に関する活動が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等によって確認する。 4.1 検査前準備 証明書等の発行に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する常時立入者への証明書等の発行に係る措置が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 （１）本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等においては是正処置が適切に講じられていることを確認する。 （２）本検査に関連する不適合の履歴からサン	02. INSPECTION REQUIREMENTS		<u>General Guidance.</u> This inspection procedure (IP) was developed to ensure the operational program established for implementation at a plant licensed in accordance with 10 CFR Part 50 and 10 CFR Part 52 meet all NRC requirements and objectives for operational program readiness. Note that this inspection is conducted as licensees activate the operational program. Therefore, verification through observation of activities may not be possible. In such cases, the inspector(s) should review the appropriate licensee procedures and conduct inspections of all associated areas to ensure program compliance upon implementation. ...	NRA ・検査手順（概略） ✓ 方法 NRC ・一般的ガイダンス ✓ この検査は、IMC 2200 App. A または IMC 2562 に対応する運転プログラムが開始された場合に実施されることに注意。 ➤ 建設中の場合、この IP は、建設中原子炉監視プロセス (cROP) の監視対象となる全ての原子炉に適用される。 ➤ 運転認可終了後の再起動の場合、この IP は、廃止または長期停止中の原子炉から ROP 対象の運転中原子へ移行中の場合に適用。 ➤ 活動の観察による確認が不可能な場合もある。その場合、適切な手順書を確認し、関連する全エリアの検査を実施し、プログラムが遵守されていることを確認する。

		ブルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。			✓ 物理的防護プログラムが 10 CFR 73.55(b) の一般的なパフォーマンス目標にしたがって設計され、実施されているか準備できていることを確認する。 ✓ 検査準備として、検査官は、事業者の関連文書に精通する必要がある（セキュリティ計画、サイト固有／企業大の手順書、セキュリティポスト命令、セキュリティプログラムのレビュー・監査など）。 ➤ 特に、検査に関連する最近のセキュリティ計画変更に注意を払う。 ✓ 検査官は、過去のセキュリティ検査報告書のレビューも検討する。 ➤ 検査官は、検査手順書の全サンプルの検査が完了し、NRC 規制要件を満たしていることを保証できるレベルまで評価したことを確認すべき。 ➤ ガイダンスは、(1) 検査官がセキュリティプログラムの遵守と有効性を判断する方法とテクニックの提示、または (2) 検査要件に関する規制要件の明確化のために提供。 ✓ 検査官は、AA プログラムを評価する際、個人にエスコートなしアクセスを許可する最初の決定で十分な根拠情報を取得していたかどうか判断する必要がある。 ✓ 事業者は、いかなる場合も、最善の努力を前提に例外アクセスを認めてはならない。
—	—	—	—	02.01 Implementing Procedures. a. Verify that the licensee has established measures to implement procedures to ensure that personnel denied unescorted access after January 1, 1997, are included in a common industry database. (10 CFR 73.56(o)(6)(i), 10 CFR 73.56(o)(6)(ii)) <u>Specific Guidance.</u> When inspecting this requirement, the inspector(s) should review the licensee’s procedures to verify that the licensee has established a method to share AA information with other licensees. Specifically, the inspector(s) should verify that the licensee has procedures that outline the implementation of an information sharing mechanism to share information with other licensees pertaining to individuals who	NRC • 02.01 実施手順書 a. 立ち入り拒否された職員が業界共通 DB に含まれることを確実にする手順書の実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> - 事業者が他の事業者と情報共有する方策を確立していることを関連手順書のレビューで確認する（アクセス拒否された個人に関連する情報を共有するメカニズムの実施）。 b. 身元調査を実施する個人が身元調査を受ける者の要件と一致する基準を満たすことを確実にする手順書の実施方策を確立していること確認する ➤ <u>具体的なガイダンス</u> 手順書は、最低限、以下の事項を扱うべきで

				have been denied unescorted access as a result of not meeting or maintaining the trustworthiness and reliability criteria for unescorted access in accordance with 10 CFR 73.56. ...	ある：(1) 個人の真の身元確認、(2) 州または地方の裁判所を通じた犯履の確認、(3) 地方の信用履歴評価の実施、(4) 過去３年間の職歴評価の実施、および(5) 性格および評判の評価の実施。 c. エスコートなし立ち入りを許可された者が法執行機関または裁判所による法的措置を報告する責任があり、その責任が文書で通知されることを認識していることを確実にする手順書の実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 適切な法的措置報告プログラムを確立していることを手順書のレビューにより確認する方法。 d. 必要な身元調査の対象者について、同意撤回を含むインフォームド・コンセントの取得および説明に対処する手順およびプロセスの実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書／アクセス承認（AA）記録を確認し、エスコートなしアクセスを申請する個人の身元調査を実施するためのインフォームド・コンセントを取得する方策を確立していることを確認する方法。 e. 手順書に、人事情報管理システムに登録されている個人情報の保護方法が記載されていることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書が、エスコートなしアクセス申請の処理に使用する個人情報の保護に対処していることを確認する方法。
	—	—	—	02.02 Granting Unescorted Access, Reinvestigations, and Maintaining Authorization. a. Verify that the licensee has established measures to implement adequate provisions to obtain sufficient information to determine the true identity of applicants for unescorted access. (10 CFR 73.56(d)(3)) <u>Specific Guidance.</u> The inspector(s) should review licensee’s procedures, records, and practices to verify that the licensee demonstrates measures to validate an individual’s true identity. Those measures should	NRC ・ 02.02 エスコートなしアクセスの承認、再調査および承認の維持 a. エスコートなしアクセス申請者の真の身元を確認する十分な情報を入手する適切な規定の実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書、記録、および実務をレビューし、個人の真の身元を確認する手段を実証していることを確認する方法。 b. 職歴および学歴の確認並びに適切な照会を必要な時間制約内で実施する方策を確立していることを確認する。

				include the following minimum requirements: (1) a process to validate that the social security number that the individual has provided is his or hers and, in the case of foreign nationals, validate the claimed non-immigration status that the individual has provided is correct; and (2) a method to determine whether the results of the fingerprinting confirm the individual’s claimed identity, if such results are available. ...	➤ <u>具体的なガイダンス</u> 手順書、記録、および実務をレビューし、職歴・学歴を確認する方法等を実証していることを確認する方法。
—	—	—		02.03 Behavioral Observation Program and Insider Threat Mitigation. a. Verify that the licensee has established measures to reassess and re-approve personnel access lists for vital areas (VAs) at the prescribed frequency to confirm that personnel on the VAs access list have a continued need to access VAs. (10 CFR 73.56(j)) Specific Guidance. The inspector(s) should review the licensee’s procedures, records, and practices to confirm that the licensee reassesses and reapproves personnel access lists for VAs at the prescribed frequency to confirm that personnel on the VA access list have a continued need to access VAs. Specifically, the licensee’s access list for VAs must include: (1) only individuals who have a continued need for access to those specific VAs in order to perform their duties and responsibilities; (2) must be approved by a cognizant licensee or applicant manager or supervisor who is responsible for directing the work activities of the individual who is granted unescorted access to each VA; and (3) the list is updated and re-approved no less than every 31 days. ...	NRC ・02.03 行動観察プログラムおよびインサイダー脅威の緩和 a. 枢要区域（VA）の職員アクセスリストを所定頻度で再評価、再承認し、アクセスリスト中の職員が継続的なアクセスの必要性を有しているか確認していることを、手順書、記録、実務のレビューから確認する。 b.要員アクセスリスト中の個人で、不特定の将来にエスコートなしアクセスが必要となる可能性だけでなく、VA への継続的なアクセスが必要な人を選別する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> なし。 c. 特定施設の安全かつ確実な運転に重要な一つ以上の職務を行う個人について、5 年を超えない間隔で心理的再評価を実施する規定の実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> ・ 手順書、記録、実務の確認方法。 ・ 対象となる個人のカテゴリ、職務 d. 年次監督レビューを実施・レビューする規定の実施方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> なし。 e. 行動観察プログラムにより、施設の安全とセキュリティに悪影響のある振る舞いや行動を認識する能力を確保する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 行動観察プログラムの手順書、記録、レッスン計画のレビュー方法。 f. オフサイトの従業員でエスコートなしアクセス

					を維持する者に対して行動観察プログラムの実施を確認する方法が手順書に含まれていることを確認する。 ➤ <u>具体的なガイダンス</u> なし。
—	—	—		02.04 Information Sharing. a. Verify that the licensee has established measures to ensure that shared information, which may have an adverse effect on an individual’s trustworthiness and reliability, is updated or provided to other licensees or industry entities in a timely fashion so informed AA decisions can be made. (10 CFR 73.56(o)(6)(i)) <u>Specific Guidance.</u> When inspecting this requirement, the inspector(s) should review the licensee’s procedures, records, and practices to confirm that the licensee implements measures to ensure that shared information which may have an adverse effect on an individual’s trustworthiness and reliability is updated or provided to other licensees or industry entities in a timely fashion. Specifically, the inspector(s) should review the licensee’s AA program to confirm that the licensee has methods in place to ensure if/when shared information is developed about an individual; the licensee that acquired the information shall correct or augment the data and ensure it is shared with other licensees. If the information has implications for adversely affecting an individual’s trustworthiness and reliability, the licensee who discovered or obtained the information, informs the reviewing official of any licensee AA program under which the individual is maintaining his or her unescorted AA or unescorted access status of the updated information on the day of the discovery. ...	NR 02.04 情報共有 a. 個人の信用・信頼性に悪影響を及ぼす可能性のある共有情報がタイムリーに更新され、または他の事業者／業界団体に提供され、情報を活用した AA の意思決定が行われる方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書、記録、実務のレビュー方法と要点。 b. 職務適性（FFD）プログラムの違反が、違反した事業者の活動を信用を得たまたは信用しようとした事業者に対して確実に特定される方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> FFD 情報の共有に関するプロセスのレビュー方法。 c. AA プログラム維持を義務付けられた他の事業者・事業体と、エスコートなしアクセス個人に関する情報共有を実施する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> ・手順書、記録、実務のレビュー方法。 ・具体的な確認事項。 d. アクセスを拒否された職員の PA へのアクセスを拒否する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> なし。 e. 事業者、請負業者、ベンダーの FFD フォローアッププログラム対象のエスコートなし職員が、後続の事業者・事業体に確実に識別され、フォローアップの継続を可能にする方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> ・手順書、記録、および実務のレビュー方法。 ・具体的な確認事項。 f. 個人のアクセス拒否情報を AA プログラム維持が要求される他の事業者・事業体と共有する方

					法を実施する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> なし。 g. 情報共有のバックアップ・マニュアルの手順書およびプロセスを実施する方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書、記録、実務のレビュー方法。
	—	—	—	02.05 Personnel Information Management. a. Verify that the licensee has established measures to implement a personnel information management system to protect sensitive personal information. (10 CFR 73.56(m), 10 CFR 73.56(m)(1), and 10 CFR 73.56(m)(3)). <u>Specific Guidance.</u> When inspecting this requirement, the inspector(s) should review the licensee’s procedures, records, and practices to confirm that the licensee implements and maintains a personnel information management system to protect sensitive personal information. Additionally, and where applicable, this includes the licensee obtaining a release (consent) form from non-citizens prior to querying the Department of Homeland Security Systematic Alien Verification for Entitlement (DHS-SAVE) database. This is applicable to unescorted and escorted access if the licensee is or has used the DHS-SAVE database. ... 02.06 Reviews. <u>Events and Logs.</u> Review licensee event reports, safeguards log entries, and corrective action program entries for the previous 12 months (or since the last inspection) that concern the AA program, and follow up, if appropriate. (10 CFR 73.55(b)(10) and 10 CFR 73.71) <u>Security Program Reviews.</u> Verify that the licensee has established measures to conduct security program reviews upon implementation of its security plan in accordance with 10 CFR 73.55(m) and that the licensee’s AA program is included in a review as required by the regulation. (10 CFR 73.55(m) and	NRC • 02.05 人事情報管理 a. 機微な個人情報を保護するための人事情報管理システムの運用方策を確立していることを確認する。 ➤ <u>具体的なガイダンス</u> 手順書、記録、実務のレビュー方法。 b. 検査官は、国土防衛省の DHS-SAVE データベースが米国市民権・移民局（USCIS）により管理されていることにも留意する。 c. 情報管理システムが電子形式で保存または送信される情報を保護していることを確認する。 ➤ <u>具体的なガイダンス</u> なし。 d. 情報管理システムが情報への不正アクセスを禁止し、権限なしデータ変更を禁止していることを確認する。 ➤ <u>具体的ガイダンス</u> なし。
	—	—	—		NRC • 02.06 レビュー ✓ 事象および記録 AA プログラムに関する事象について、過去 12 ヶ月または前回検査以降の物理的セキュリティ事象ログをレビューし、適切であればフォローアップする。 ✓ セキュリティプログラムのレビュー セキュリティプログラムのレビューを実施していること、および AA プログラムが規則で要求されるレビューに含まれていることを確認する。 ✓ 問題の把握と解決。 適切な閾値で AA プログラムに関する問題を特

			Security Plans) <u>Problem Identification and Resolution.</u> Verify that the licensee identifies problems with the AA program and its integration with the FFD program at an appropriate threshold and enters the problems in the corrective action program. Verify that the licensee has appropriately resolved the regulatory requirement issue for a selected sample of problems with AA. If applicable, see IP 71152, “Problem Identification and Resolution,” for additional guidance. (10 CFR 73.55(b)(10)) <u>Specific Guidance.</u> The inspector(s) should review safeguards log entries, licensee condition reports, licensee corrective action program entries, etc., for the previous 12 months to determine whether the licensee has experienced issues with the implementation of its AA program. The inspector(s) should follow-up on issues identified to ensure the licensee has taken appropriate corrective actions to prevent a re-occurrence of the issues identified. For the inspection of this requirement the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its AA program. The inspector(s) should ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). The inspector(s) should also request that the licensee provide a copy of the report that was developed and provided to licensee management for review. The inspector(s) should review the report to identify any findings that were identified via the review or audit to ensure the findings were entered in the licensee’s corrective action program.	定し問題の把握と解決（PI&R）プログラムに入力していること、問題を適切に解決していることを確認する。 ➤ <u>具体的なガイダンス</u> ・検査前に、セキュリティ事象報告書（SER）がNRCに提出されているかどうか確認する。 ・少なくとも前回検査以降に文書化された AA プログラムに関する物理的セキュリティ事象のログをレビューし、矛盾・欠陥が特定された場合、必要に応じてフォローアップする。 ・セキュリティプログラムのレビュー／監査の記録をレビューし、AA プログラムの継続的な有効性を確認する。 ・AA プログラムに関する PI&R プログラムの入力をレビューし、適切な閾値で欠陥を特定し、傾向を分析し、セキュリティ上の重要度に応じて欠陥を是正していることを確認する。
法令、基準等	（１）実用炉規則第 91 条 （２）研開炉規則第 86 条 （３）加工規則第 7 条の 9 （４）貯蔵規則第 36 条 （５）再処理規則第 16 条の 3 （６）審査基準	—	—	—

改訂情報	変更日、施行日、簡潔な変更理由（「記載の適正化」）	Revision History	Attachment 1: Revision History for IP 81000.01, “Access Authorization”	日本の検査ガイドは、日付と簡潔な改訂履歴を示している（「記載の適正化」など）。 NRC 検査ガイドは、より詳細な改訂履歴を示しており、旧版検査ガイドの発行日と ADAMS 登録 ID、改訂内容の説明などを記載している。さらに、本文中では改訂部分のテキストを赤字で、改訂範囲を欄外の縦バーで示し、改訂部分が明示している。
------	---------------------------	------------------	--	--

2.3.2.2 PP1801「教育および訓練」と IP81000.07「Security Training」における調査の結果

原子力規制庁および NRC の検査ガイドの主な内容および相違点を整理し、表 2.3.2-2 にまとめた。主な比較結果を以下に示す。より詳細は、表の備考欄参照。

2.3.2.2.1 対象とする検査プログラム

NRC の検査ガイドでは、上位図書（IMC）情報から、次の検査プログラムで使うことが分かる。

- ・建設時セキュリティ検査

2.3.2.2.2 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

NRC の検査ガイドでは、監督領域を定義していない。（建設フェーズの検査ガイドであって、運転フェーズの原子炉監督プロセス（ROP）の検査ガイドではないため）

2.3.2.2.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（教育および訓練状況の確認）を簡潔に記載している。

NRC の検査ガイドでは、検査官が確認すべき事項を具体的に列挙している（4 項目）。例えば、最初の項目は、「規制要件、NRC が承認したセキュリティ計画等にしながら、核セキュリティ訓練プログラムを開発し、実施中か実施準備できていることを確認する」である。

2.3.2.2.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

NRC の検査ガイドでは、検査リソースの目安（検査時間、サンプル数）が示されている。検査要件そのものは、次項の検査手順に対応する部分でガイダンスを含めて詳細に示している。

2.3.2.2.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・教育および訓練が行われていることの確認
- ・証明書等の発行の適切性を文書、ワークダウン、インタビューを活用して確認
- ・検査前準備、検査、CAP 検査の趣旨

NRC の検査ガイドでは、次のように分けて具体的な検査手順および個別のガイダンスを詳細に示している。より詳細は、添付の表 2.3.2-2 の備考欄参照

- ・ 一般的ガイダンス（共通事項）
- ・ 訓練&資格認定（T&Q）実施手順書
- ・ 初期訓練
- ・ OJT 訓練
- ・ 銃器習熟訓練
- ・ 日中・夜間火器資格認定
- ・ 戦術資格認定
- ・ 必要な知識とパフォーマンス
- ・ 再資格認定
- ・ 訓練の文書化
- ・ 医療面の資格認定
- ・ 身体適性検査
- ・ 銃器優先権
- ・ レビュー
- ・ 問題の把握と解決

2.3.2.2.6 法令・基準等

2.3.2.1.6 に同じ。

2.3.2.2.7 改訂情報

2.3.2.1.7 に同じ。

表 2.3.2-2 原子力規制庁検査ガイド PP1801 と米国 NRC 検査ガイド IP81000.01 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1801 教育および訓練 2023/05/31（制定）（2 頁）			米国 NRC 検査ガイド 【ガイド】IP81000.07 Security Training (Issue Date: 09/24/19, Effective Date: 09/24/2019（21 頁）		両者間の主な相違点
項目		主な内容	項目	主な内容	
図書全体構成		本文 改訂情報	図書全体構成	本文 改訂情報	－
	－	－	PROGRAM APPLICABILITY	IMC 2200, Appendix A	NRC ・ 検査プログラム（上位図書） ✓ IMC 2200 App. A（建設時セキュリティ検査プログラム）
	監督領域	大分類および小分類：「核物質防護」 評価領域：「特定核燃料物質の管理」、「核物質 防護情報の管理」、「立入承認」、「出入管理」、 「物理的防護」、「情報システム防護」、「核物質 防護体制」 検査分野：「教育および訓練」	－	－	NRA ・ 監督領域の区分 NRC （建設時は ROP の対象でないので、コーナーストーンは示されていない）
	1. 検査の目的	2.1 目的 法第 6 1 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される教育および訓練状況を確認する。当該事項は、法第 6 1 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、教育および訓練の検査分野における体制および警備員等の力量にも留意する。 2.2 防護措置の狙い 従業者に対し計画的な教育および訓練を実施することにより、必要な知識・能力（技術）等を継続的に維持していく。	01. INSPECTION OBJECTIVES	01.01 To verify and assess the licensee has developed and is implementing or is prepared to implement its nuclear security training program in accordance with the U.S. Nuclear Regulatory Commission (NRC) requirements, NRC-approved security plans, and any other applicable requirement. 01.02 To assess security-personnel knowledge, skills, and abilities to conform with the licensee training and qualification (T&Q) plan, regulatory requirements, and any other applicable NRC requirement. 01.03 To verify required security equipment assigned to security personnel meets the objective’s outlined in the licensee’s T&Q plan, NRC regulatory requirements, and any other applicable requirement. 01.04 To verify that the licensee’s physical protection program associated with this sample is designed and implemented, or is prepared to implement, to meet the general performance objectives of Title 10 of the Code of Federal Regulations (10 CFR) 73.55(b).	NRA ・ 検査の目的 ✓ 法的な位置づけと目的（教育および訓練状況の確認） NRC ・ 検査の目的 ✓ 規制要件、NRC が承認したセキュリティ計画等にしたがって核セキュリティ訓練プログラムを開発し、実施中か実施準備できていることを確認 ✓ セキュリティ担当者の知識、スキル、および能力を評価 ✓ セキュリティ担当者に割り当てられた必要なセキュリティ機器が目的を満たしていることを確認 ✓ このサンプルに関連する物理的防護プログラムが 10 CFR) 73.55(b) の一般的なパフォーマンス目標を満たすよう設計され実施中か実施準備できているかを確認
	2. 検査要件	3.1 検査対象 核燃料物質防護に係る全ての業務に関連する従業者に対する教育計画、内容、実績、被教育者の理解度、現場確認等の全てが検査対象となり得るが、本検査では、限られた数の検査対象	03. RESOURCE ESTIMATE	The resource estimate for this section is approximately 27 hours of direct inspection. The sample size for this procedure is 38.	NRA ・ 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 NRC

		（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、核燃料物質防護に関する教育および訓練の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 １年間に１回程度 （２）検査時間 ３人／５．２５（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。			・検査リソースの目安 ✓ 検査時間、サンプル数
	3. 検査手順	従業者に対し、その職務の内容に応じて核燃料物質防護のために必要な教育および訓練が行われていることを確認する。また、教育および訓練が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等により確認する。 4.1 検査前準備 教育および訓練に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する教育および訓練が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 （１）本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 （２）本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	02. INSPECTION REQUIREMENTS	<u>General Guidance.</u> This inspection procedure (IP) was developed to ensure the operational program established for implementation at a plant licensed in accordance with 10 CFR Part 50 or 10 CFR Part 52 meets all NRC requirements and objectives for operational program readiness. Note that this inspection is conducted as licensees activate the operational program. Therefore, verification through observation of activities may not be possible. In such cases, the inspector(s) should review the appropriate licensee procedures and conduct inspections of all associated areas to ensure program compliance upon implementation. Through verification of the inspection requirements within this IP, inspector(s) shall ensure that the licensee’s physical protection program associated with this sample is designed and implemented, or is prepared to implement, to meet the general performance objectives of 10 CFR 73.55(b). ...	NRA 3. 検査手順（概略） ✓ 教育および訓練が行われていることの確認 ✓ 文書、ウォークダウン、インタビューの活用 ✓ 検査前準備、検査、CAP 検査の趣旨 NRC 2. 検査要件 ・一般的ガイダンス ✓ この検査は、運転プログラムが開始された場合に実施されることに注意。 ➤ 活動の観察による確認が不可能な場合もある。その場合、適切な手順書を確認し、関連する全エリアの検査を実施し、プログラムが遵守されていることを確認する。 ✓ 物理的防護プログラムが 10 CFR 73.55(b) の一般的なパフォーマンス目標にしたがって設計され、実施されているか準備できていることを確認する。 （以下、次の個別の検査要件とガイダンス） 2.1 <u>T&Q Plan and Implementing Procedures</u> 2.2 <u>Initial Training</u> 2.3 <u>On-the-Job (OJT) Training</u> 2.4 <u>Firearms Familiarization Training</u> 2.5 <u>Daylight and Night Fire Qualification</u> 2.6 <u>Tactical Qualification</u> 2.7 2.7 <u>Requisite Knowledge and Performance</u> 2.8 <u>Re-qualification</u> 2.9 <u>Training Documentation</u>

					<u>2.10 Medical Qualifications</u> <u>2.11 Physical Fitness Test</u> <u>2.12 Firearms Preemption Authority</u> <u>2.13 Reviews</u> <u>Problem Identification and Resolution</u>
				<u>02.01 T&Q Plan and Implementing Procedures</u> a. Verify that the licensee has established, maintains, implements, and follows an NRC-approved T&Q plan that describes how the criteria set forth in 10 CFR Part 73, Appendix B, Section VI will be implemented. (10 CFR 73.55(c)(4), 10 CFR Part 73, App. B, Sec. VI, A.3.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review the licensee's NRC-approved security plans to verify that the licensee has established, maintains, and implements, and follows a T&Q plan that describes how the criteria set forth in 10 CFR Part 73, Appendix B, will be implemented. Specifically, the T&Q plan must describe how the minimum T&Q requirements will be met and include the process by which all individuals will be selected, trained, equipped, tested, and qualified. ...	NRC 2.1 訓練&資格認定(T&Q)計画および実施手順書 （以下について、確認事項、具体的なガイダンスが示されている。） a. T&Q 計画の作成、維持、実施の確認 b. 銃器射撃場活動への参加 c. 無資格活動の禁止方策 d. 銃器の T&Q の確実な実施 e. 銃器の T&Q の実習観察
				<u>02.02 Initial Training.</u> a. Verify that, before being permitted to perform any security-related duty or responsibility, personnel have been trained, equipped, and qualified to perform each assigned security-related job task or duty. (10 CFR Part 73, App. B, Sec. VI, C.1.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and a sample of training records for individuals assigned security tasks to determine that prior to performing assigned security-related job tasks or duties, security personnel have been trained, equipped and qualified. If the licensee qualifies facility personnel (e.g., warehouse personnel) to perform security-related job tasks or duties, review a sample of records to determine whether there has been adequate training, qualification and certification prior to performance.	NRC 1.2 初期訓練 （以下について、確認事項、具体的なガイダンスが示されている。） a. 活動前の T&Q b. 機器・デバイス使用の T&Q c. 筆記と実技試験 d. 武装警備要員の年次筆記試験 e. 武装警備要員の得点率（80%以上） f. 武力の使用訓練 g. セキュリティの確実な実施の訓練 h. 銃器訓練 （中略） l. 年次戦術資格認定コース

				...	
				<u>02.03 On-the-Job (OJT) Training.</u> a. Verify that the licensee’s T&Q program includes OJT training performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry out assigned duties and responsibilities before the individual is assigned the duty or responsibility. (10 CFR Part 73, App. B, Sec. VI, C.2.(a)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the licensee’s security plans, implementing procedures, and associated training documentation (to include a sample of individual training records) to verify that the licensee’s T&Q program includes OJT performance standards and criteria for each individual assigned security duties and responsibilities. OJT performance standards and criteria must ensure that each individual demonstrates the requisite knowledge, skills, and abilities for effective performance of assigned duties and responsibilities. The licensee must implement OJT to ensure that individuals have a basic level of hands-on experience in nuclear security functions before they are considered qualified and assigned duties and responsibilities. Licensees may consider the use of a formalized OJT checklist to identify those duties and responsibilities associated with each duty position and job task. Typically, qualified security training instructors and field training officers and/or subject matter experts designated by the security training staff conduct the OJT. A qualified security supervisor must attest to all OJT and the records must be retained consistent with 10 CFR 73.70, “Records.” ...	NRC 2.3 OJT 訓練 （以下について、確認事項、具体的なガイダンスが示されている。） a. T&Q に OJT を含む b. T&Q に 40 h 以上の緊急時対応 OJT 含む
				<u>02.04 Firearms Familiarization Training</u> a. Verify that the licensee has established measures to conduct annual firearms familiarization training	NRC 2.4 銃器習熟訓練 （以下について、確認事項、具体的なガイダンスが

				for armed security personnel in accordance with the NRC-approved T&Q plan. (10 CFR Part 73, App. B, Sec. VI, E.1.(c)) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include courses of fire and training records) to verify that the licensee has established measures to conduct annual firearms familiarization training for armed security personnel. Firearms familiarization, at a minimum, must include the following: 1. Firearms handling drills; 2. Clearing, loading, unloading, and reloading procedures for each firearm; 3. Training for engaging potential targets when obstacles such as smoke, fencing, ...	示されている。) a. 年次銃器習熟訓練の実施方策
				<u>02.05 Daylight and Night Fire Qualification.</u> a. Verify that the licensee’s daylight and night fire weapons qualifications results are documented and retained as a record. (10 CFR Part 73, App. B, Sec. VI, F.1.(b)) <u>Specific Guidance</u> No inspection guidance. b. Verify that the licensee conducts daylight and night fire qualification courses for each type of firearm employed at the site and that each qualification course is in accordance with standards established by law enforcement or an equivalent nationally recognized course. (10 CFR Part 73, App. B, Sec. VI, F.4.) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include daylight and night fire qualification courses) to verify that the licensee’s daylight and night fire qualification courses are in	NRC 2.5 日中・夜間火器資格認定 (以下について、確認事項、具体的なガイダンスが示されている。) a. 年次銃器習熟訓練の実施方策 b. 日中・夜間火器資格認定の文書化 c. 上級武器訓練コースの実施

				accordance with standards established by law enforcement or an equivalent nationally recognized course. Armed personnel must qualify by achieving the standards and scores established by a Federal- or State-approved law enforcement qualification course or an equivalent nationally recognized course. Examples of the latter include courses recognized by the NRA, the U.S. Department of Defense (DoD), and the International Association of Law Enforcement Firearms Instructors (IALEFI). Once the qualification courses have been designed, licensees may submit them to the recognized entity for certification before the courses are implemented. The licensee may use current qualification courses developed and certified by the above-listed entities; however, such courses may not be modified. When using the qualification courses that have been developed and certified by a recognized entity, the weapons operating system must be similar to that for which the course was designed (e.g., a revolver course must not be used to qualify armed security officers on the use of a semiautomatic handgun). ...	
				<u>02.06 Tactical Qualification</u> a. Verify that the licensee has established measures to conduct tactical weapons qualification for armed security personnel in accordance with the NRC-approved T&Q plan. (10 CFR Part 73, App. B, Sec. VI, F.2) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include courses of fire and training records) to verify that the licensee has established measures to conduct an annual tactical weapons qualification for armed security personnel. ...	NRC 2.6 戦術資格認定 (以下について、確認事項、具体的なガイダンスが示されている。) a. 戦術武器資格認定の実施方策 b. 戦術武器資格認定のパフォーマンス基準
				<u>02.07 Requisite Knowledge and Performance.</u> a. Verify that security personnel possess adequate knowledge to carry out their assigned duties and	NRC 2.7 必要な知識とパフォーマンス (以下について、確認事項、具体的なガイダンスが

				responsibilities, including response procedures, use of deadly force, and armed response tactics. (10 CFR Part 73, App. B, Sec. VI, A.4.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should interview a sample of security personnel and/or facility personnel (if applicable) to determine if they possess adequate knowledge to carry out their assigned duties and responsibilities, including response ...	示されている。) a. セキュリティ担当者の保有知識
				<u>02.08 Re-qualification</u> a. Verify that armed and unarmed individuals are re-qualified annually in accordance with 10 CFR Part 73 Appendix B, VI. and the NRC-approved T&Q plan. (10 CFR Part 73, App. B, Sec. VI, D.2 and 10 CFR Part 73, App. B, Sec. VI, A.7) <u>Specific Guidance</u> No inspection guidance. b. Verify that armed members of the security organization re-qualify with each assigned weapon at least annually in accordance with NRC requirements and the NRC-approved T&Q plan. (10 CFR Part 73, App. B, Sec. VI, F.5 and 10 CFR Part 73, App. B, Sec. VI, A.7) <u>Specific Guidance</u> No inspection guidance.	NRC 2.8 再資格認定 (以下について、確認事項、具体的なガイダンスが示されている。) a. 武装・非武装個人の年次再資格認定 b. 武装メンバーの割り当てられた武器の年 1 回以上の訓練
				<u>02.09 Training Documentation.</u> a. Verify that the licensee maintains training documentation in accordance with regulations and requirements. (10 CFR 73.55(b)(4)(i) and 10 CFR Part 73, App. B, Sec. VI, H.) <u>Specific Guidance</u> In the review of training documentation, the inspectors should select a sample of training records which include newly hired security personnel. The inspector should ensure that training records reflect	NRC 2.9 訓練の文書化 (以下について、確認事項、具体的なガイダンスが示されている。) a. 訓練の文書化

				successful completion and certification of on duty tasks specified in the licensee’s NRC-approved T&Q plan. The inspector should also determine from records that response personnel meet the physical and psychological criteria for armed status.	
				<u>02.10 Medical Qualifications.</u> a. Verify that armed and unarmed individuals assigned security duties and responsibilities are subject to a medical physical examination that is designed to measure the individual’s physical ability to perform assigned duties and responsibilities. (10 CFR Part 73, App. B, Sec. VI, B.2.(a)(2)) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review a sample of the licensee’s T&Q records to verify that all individuals who are performing security functions for the security organization are subject to a physical examination. The purpose of this physical examination is to verify that an individual is physically capable to perform assigned duties and responsibilities as identified in NRC-approved security plans and ...	NRC 2.10 医療面の資格認定 （以下について、確認事項、具体的なガイダンスが示されている。） a. 健康診断 b. 医師免許保有者による診断書 c. 身体資格認定記録
				<u>02.11 Physical Fitness Test</u> a. Verify that the armed members of the security organization demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test. (10 CFR Part 73, App. B, Sec. VI, B.4.(b)) <u>Specific Guidance</u> To inspect this requirement, the inspectors(s) should review a sample of the licensee’s training records to verify that armed members of the security organization demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test as described in the site’s NRC-approved security plans and implementing procedures. ...	NRC 2.11 身体適性検査 （以下について、確認事項、具体的なガイダンスが示されている。） a. 身体的適性 b. 通常時と緊急時の職務に対応 c. インストラクターの資格

				<u>02.12 Firearms Preemption Authority</u> a. Verify the licensee has completed satisfactory firearms background checks, as required by NRC Order EA-13-092, for members of the security organization who are required to possess, use, or have access to covered firearms and devices as a part of their assigned duties and responsibilities. (NRC Order EA-13-092) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review a sample of firearms background check records for members of the licensee or contracted security organization who are required to possess, use, or have access to firearms and devices. The inspector(s) should verify and consider (as applicable) the following items listed below, which are defined in the NRC Order EA-13-092, to ensure the licensee has completed satisfactory firearms background checks: (1) a satisfactory firearms background check means a “proceed” response has been received by the ...	NRC 2.12 銃器優先権 （以下について、確認事項、具体的なガイダンスが示されている。） a. 銃器に関する背景調査 b. 資格喪失者の除外方策 c. FBI 提供情報の保管（5年）
				<u>02.13 Reviews.</u> <u>Events and Logs.</u> Review and evaluate licensee event reports, safeguards log entries, and corrective action documents for the previous 12 months, or since the last inspection, which are associated with the training program and follow up, if appropriate. (10 CFR 73.55(b)(10) and 10 CFR 73.71) <u>Security Program Reviews.</u> Verify that the licensee is conducting security program reviews in accordance with 10 CFR 73.55(m) and that the licensee’s training program was included in a review, as required by the regulation. (10 CFR 73.55(m) and 10 CFR Part 73, App. B, Sec. VI, I)	NRC 2.13 レビュー （以下について、確認事項、具体的なガイダンスが示されている。） a. 事象とログ b. セキュリティプログラム c. 問題の把握と解決
				<u>Problem Identification and Resolution.</u> Verify that the licensee is identifying issues related to the security training program at an appropriate	問題の把握と解決 ✓ 是正処置プログラムへの登録および解決（詳細は IP71152 参照）

				threshold and entering them in the corrective action program. Verify that the licensee has appropriately resolved the issues regarding regulatory requirements for a select sample of problems associated with the security training program. Refer to IP 71152, “Problem Identification and Resolution,” for additional guidance. (10 CFR 73.55(b)(10)) <u>Specific Guidance.</u> Before commencement of the inspection, the inspector(s) should review all licensee event reports relating to security training to determine if the licensee is capturing security training issues and properly reporting them. For the inspection of this requirement, the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its security training program. The inspector(s) should ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). The inspector(s) should also request that the licensee ...	
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	—	—	—
参考文献	—	—	Reference	—	—
別紙・附属書	—	—	Appendix	—	—
改訂情報	変更日、施行日、簡潔な変更理由（「制定」）	—	Revision History	Attachment 1: Revision History for IP 81000.07, “Security Training”	日本の検査ガイドは、日付と簡潔な改訂履歴を示している。 NRC 検査ガイドは、改訂履歴として、日付、改訂の概要、旧版検査ガイドの ADAMS 登録 ID などを示しており、必要に応じて旧版の検索も容易にできる。また、検査ガイド本文中で改訂された部分を赤字で示す、改訂範囲を縦バー示すなど、具体的な改訂部分を明示している。

2.3.2.3 PP1801「教育および訓練」と IP81200.07「Security Training for Decommissioning Nuclear Power Reactors」における調査の結果

NRA および NRC の検査ガイドの主な内容および相違点を整理し、表 2.3.2-3 にまとめた。主な比較結果を以下に示す。より詳細は、表の備考欄参照。

2.3.2.3.1 対象とする検査プログラム

NRC の検査ガイドでは、上位図書（IMC）情報から、次の検査プログラムで使うことが分かる。

- ・建設時セキュリティ検査

2.3.2.3.2 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

NRC の検査ガイドでは、監督領域を定義していない。（建設フェーズの検査ガイドであって、運転フェーズの原子炉監督プロセス（ROP）の検査ガイドではないため）

2.3.2.3.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（教育および訓練状況の確認）を簡潔に記載している。

NRC の検査ガイドでは、検査官が確認すべき事項を具体的に列挙している（4 項目）。例えば、最初の項目は、「規制要件、NRC が承認したセキュリティ計画等にしたがって、核セキュリティ訓練プログラムを開発し、実施中か実施準備できていることを確認する」である。

2.3.2.3.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

NRC の検査ガイドでは、検査の完了（検査実施上の留意事項。例えば、運転中と同等の品質、厳格さ、有効性を持つものとして評価すべきなど）、検査リソースの目安（検査時間、サンプル数）が示されている。検査要件そのものは、次項の検査手順に対応する部分でガイダンスを含めて詳細に示している。

2.3.2.3.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・検査の対象範囲
- ・証明書等の発行の適切性を文書、ウォークダウン、インタビューを活用して確認
- ・検査前準備、検査、CAP 検査の趣旨

NRC の検査ガイドでは、次のように分けて具体的な検査手順および個別のガイダンスを詳細に示している。より詳細は、添付の表 2.3.2-3 の備考欄参照

- ・ 一般的ガイダンス（共通事項）
- ・ 訓練&資格認定(T&Q)計画および実施手順書
- ・ 初期訓練
- ・ 日中・夜間火器資格認定
- ・ 戦術資格認定
- ・ 銃器習熟訓練
- ・ T&Q 計画および実施手順書
- ・ OJT 訓練
- ・ 必要な知識とパフォーマンス
- ・ 再資格認定
- ・ 訓練の文書化
- ・ 医療面の資格認定
- ・ 身体適性検査
- ・ レビュー
- ・ 問題の把握と解決
- ・ 銃器優先権

2.3.2.3.6 法令・基準等

2.3.2.1.6 に同じ。

2.3.2.3.7 改訂情報

2.3.2.1.7 に同じ。

表 2.3.2-3 原子力規制庁検査ガイド PP1801 と米国 NRC 検査ガイド IP81200.07 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1801 教育および訓練 2023/05/31（制定）（2 頁）		米国 NRC 検査ガイド 【ガイド】IP81200.07 Security Training for Decommissioning Nuclear Power Reactors (Issue Date: 04/01/21)（20 頁）		両者間の主な相違点
項目	主な内容	項目	主な内容	
図書全体構成	本文 改訂情報	図書全体構成	本文 改訂情報	—
	—	PROGRAM APPLICABILITY	IMC 2202, Appendix A	NRC ・検査プログラム（上位図書） ✓ IMC 2200 App. A（建設時セキュリティ検査プログラム）
	監督領域	—	—	NRA ・監督領域の区分 NRC （廃止措置段階は ROP の対象でないので、コーナーストーンは示されていない）
	検査の目的	INSPECTION OBJECTIVES	01.01 To verify and assess the licensee’s implementation of its nuclear security training program in accordance with the U.S. Nuclear Regulatory Commission (NRC) requirements, NRC-approved security plans, and any other applicable requirement. 01.02 To assess security personnel knowledge, skills and abilities to conform with regulatory requirements, the licensee’s Training and Qualification Plan (T&QP), and any other applicable NRC requirement. 01.03 To verify required security equipment assigned to security personnel meets the objective’s outlined in the licensee’s T&QP, and any other applicable requirement. 01.04 To verify that the licensee’s physical protection program, associated with this sample, provides assurance that the licensee’s program is designed and implemented in a manner that protects against the design basis threat (DBT) of radiological sabotage.	NRA ・検査の目的 ✓ 法的な位置づけと目的（教育および訓練状況の確認） NRC ・検査の目的 ✓ 規制要件、NRC が承認したセキュリティ計画等にしたがって核セキュリティ訓練プログラムを開発し、実施中か実施準備できていることを確認 ✓ セキュリティ担当者の知識、スキル、および能力を評価 ✓ セキュリティ担当者に割り当てられた必要なセキュリティ機器が目的を満たしていることを確認 ✓ このサンプルに関連する物理的防護プログラムが 10 CFR) 73.55(b) の一般的なパフォーマンス目標を満たすよう設計され実施中か実施準備できているかを確認

	検査要件	3.1 検査対象 核燃料物質防護に係る全ての業務に関連する従業者に対する教育計画、内容、実績、被教育者の理解度、現場確認等の全てが検査対象となり得るが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、核燃料物質防護に関する教育および訓練の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 １年間に１回程度 （２）検査時間 ３人／５．２５（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	3. Procedure Completion 4. RESOURCE ESTIMATE	・ PROCEDURE COMPLETION The decommissioning security inspection program for power reactor facilities that have permanently shut down emphasizes a balanced look at a cross section of licensee activities important to the conduct of safety and security at decommissioning sites. Licensee decommissioning security programs and procedures should be assessed to ensure that they afford a comparable level of quality, rigor, and effectiveness as those in existence during reactor power operations. The decommissioning security inspection program also provides Regional Administrators flexibility in the application of inspection resources to deal with issues and problems at specific plants. Therefore, all inspection requirements need not be completed for every particular inspection. However, the inspector(s) should perform a minimum of 50 percent of the applicable inspection requirements within this ・ Resource Estimate The resource estimate for this inspection procedure is approximately 26 hours of direct on-site inspection effort every 2 years. These hours of inspection effort are allocated every 2 years. Inspection hour estimates are based on current experience and will be reviewed and revised periodically. It is expected that actual inspection hours will vary from site to site and from the estimate depending on the level of security at decommissioning sites. The sample size for this procedure is 1.	NRA ・ 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 NRC ・ 検査の完了 ✓ 発電炉廃止措置セキュリティ検査プログラムは、廃止措置サイトで安全とセキュリティが重なる部分をバランスよく見ることに重点を置いている。 ✓ 事業者の廃止措置セキュリティプログラムと手順書は、運転中と同等の品質、厳格さ、有効性を持つものとして評価すべき。 ✓ NRC の廃止措置セキュリティ検査プログラムは、個別のプラントの問題に対処する検査リソースの柔軟性も提供する。すべての検査要件を個々の検査ごとに完了する必要はない。ただし、検査官は、この検査手順書の目的が満たされるように、この検査手順書内の該当する検査要件の少なくとも 50 パーセントを実行する必要がある。 ・ 検査リソースの目安 ✓ 検査時間、サンプル数
	検査手順	従業者に対し、その職務の内容に応じて核燃料物質防護のために必要な教育および訓練が行われていることを確認する。また、教育および訓練が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等により確認する。 4.1 検査前準備 教育および訓練に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する教育および訓練が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 （１）本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プロ	INSPECTION REQUIREMENTS	<u>General Guidance.</u> Through verification of the inspection requirements within this inspection procedure, the inspector(s) shall ensure that the licensee’s physical protection program associated with this sample provides assurance that the licensee’s program is designed and implemented in a manner that protects against the DBT of radiological sabotage. In preparing to complete this procedure, the inspector(s) should familiarize themselves with relevant documentation which may include, but is not limited to, the licensee's Physical Security Plan, site-specific and/or corporate implementing procedures, security post orders; all NRC-approved licensing	NRA 3. 検査手順（概略） ✓ 検査の対象範囲 ✓ 文書、ウォークダウン、インタビューの活用 ✓ 検査前準備、検査、CAP 検査の趣旨 NRC 2. 検査要件 ・ 一般的ガイダンス ✓ この検査は、物理的防護プログラムが適切に設計、実施されていることを確認する。 ✓ 検査の準備として、セキュリティ計画、その他の関連プログラムおよび文書に精通しておくことが必要。

		グラム（CAP）等において是正処置が適切に講じられていることを確認する。 （2）本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。		actions (i.e., exemptions, license amendments, alternative measures) and security program reviews and audits. This documentation review should not only be used to gain an understanding of a licensee's implementation in a particular program area, but to also identify the licensee's progress during the transition from operating status to decommissioning. This information should be used as a factor in determining the scope of the inspection activity to be conducted in each program area. The inspector(s) should consider conducting a review of past security inspection reports for the facility. Specifically, the inspector should apply additional attention to recent security plan changes that could be relevant to the inspection activity. The inspector(s) are responsible for ensuring that inspection requirements for security training inspections are completed and evaluated to a level which provides assurance that licensees are meeting NRC regulatory requirements within the security program area being inspected. This guidance is being provided as a tool which: (1) recommends to the inspector(s) certain methods and techniques for determining licensee security program compliance and effectiveness related to an inspection requirement or; (2) clarifies certain aspects of a regulatory requirement associated with a particular inspection requirement. Where minimum sampling numbers are indicated (i.e., at least three) intrusion detection system (IDS) zones shall be tested, or at least 20 percent of the total personnel on a shift will be selected for weapons firing, etc.), the inspector(s) should adhere as closely as possible to the numbers identified in the guidance. The inspector(s) may expand the minimum number to aid in determining the extent of the condition, should compliance concerns arise. Completion of recommended actions contained in this guidance should not be viewed as mandatory. Should questions arise regarding procedural requirements or guidance, the inspector(s) should consult with Regional management or the Office of Nuclear Security and Incident Response (NSIR), the program office, for clarification. ...	✓ この文書レビューは、特定のプログラム領域の理解だけでなく、運転段階から廃止措置段階への移行の進捗状況の把握にも活用すべき。 ✓ その情報は、各プログラム領域の検査対象範囲決定の参考になる。 ✓ 検査官は、過去のセキュリティ検査報告書のレビューの実施を検討することも必要。とくに最近のセキュリティ計画変更には注意すべき。 ... （以下、個別の検査要件とガイダンスが示されている。） 2.1 <u>Training and Qualification Plan and Implementing Procedures</u> 2.2 <u>Initial Training</u> 2.3 <u>Daylight and Night Fire Qualification</u> 2.4 <u>Tactical Qualification</u> 2.5 <u>Firearms Familiarization Training</u> 2.6 <u>Training and Qualification Plan and Implementing Procedures</u> 2.7 <u>On-the-Job (OJT) Training</u> 2.8 <u>Requisite Knowledge and Performance</u> 2.9 <u>Re-qualification</u> 2.10 <u>Training Documentation</u> 2.11 <u>Medical Qualifications</u> 2.12 <u>Physical Fitness Test</u> 2.13 <u>Reviews Problem Identification and Resolution</u> 2.14 <u>Firearms Preemption Authority</u>
--	--	---	--	--	--

				<u>02.01 Training and Qualification Plan and Implementing Procedures</u> a. Verify that the licensee does not allow any individual to perform any security function, assume any security duty or responsibility, or return to security duty until that individual satisfies the training and qualification requirements of 10 CFR Part 73, Appendix B VI, and the NRC-approved T&QP. This includes facilities personnel who perform security tasks. (10 CFR Part 73, Appendix B VI, A.6.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review the licensee's security plans, procedures, and training records to verify that the licensee does not allow any individual to perform any security function, assume any security duty or responsibility or return to security duty; until that individual satisfies the training and qualification requirements of 10 CFR, Appendix B VI, and the NRC-approved T&QP. Specifically, the inspector(s) should review samples of training records for the following personnel: members of the security organization; members of the security organization who have returned to duty after an extended leave (e.g., illness or military deployment); and facility personnel who have been trained and qualified to perform security tasks. While reviewing these records, the inspector(s) should evaluate T&QP and implementing procedure compliance regarding the fulfillment of applicable training and qualification requirements as outlined in 10 CFR Part 73, Appendix B VI. Dependent upon the individual's security duties, the training and qualification requirements to be inspected may include: 1. employment suitability and qualification (e.g., education, age, criminal history, and physical and medical requirements); ...	NRC 2.1 訓練&資格認定(T&Q)計画および実施手順書 (以下について、確認事項、具体的なガイダンスが示されている。) ・ T&Q 無しでセキュリティ活動していないこと
--	--	--	--	---	---

				<u>02.02 Initial Training.</u> a. Verify that, before being permitted to perform any security-related duty or responsibility, personnel have been trained, equipped, and qualified to perform each assigned security-related job task or duty. (10 CFR Part 73, App. B, Sec. VI, C.1.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and a sample of training records for individuals assigned security tasks to determine that prior to performing assigned security-related job tasks or duties, security personnel have been trained, equipped and qualified. If the licensee qualifies facility personnel (e.g., warehouse personnel) to perform security-related job tasks or duties, review a sample of records to determine whether there has been adequate training, qualification and certification prior to performance. ...	NRC 2.2 初期訓練 （以下について、確認事項、具体的なガイダンスが示されている。） a. 活動前の T&Q b. 機器・デバイス使用の T&Q c. 筆記と実技試験 d. 武装警備要員の年次筆記試験 e. 武装警備要員の得点率（80%以上） f. 武力の使用訓練 g. セキュリティの確実な実施の訓練 h. 銃器訓練
				<u>02.03 Daylight and Night Fire Qualification</u> a. Verify that the licensee’s daylight and night fire weapons qualifications results are documented and retained as a record. (10 CFR Part 73, Appendix B VI, F.1.(b)) <u>Specific Guidance</u> No inspection guidance. b. Verify that armed members of the security organization meet the daylight and night fire qualification requirements outlined in 10 CFR Part 73, Appendix B VI, for each firearm that is applicable to the member’s assigned duties and responsibilities prior to being assigned the duty. (10 CFR Part 73, Appendix B VI, F.3.(a) & (b)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include courses of fire and a sample of training records) to verify that armed	NRC 2.3 日中・夜間火器資格認定 （以下について、確認事項、具体的なガイダンスが示されている。） a. 日中・夜間火器資格認定の文書化 c. 武装メンバーが銃器資格要件を有する ...

				members of the security organization meet the licensee’s daylight and night fire weapons qualification courses, as outlined in 10 CFR Part 73, Appendix B VI., and the licensee’s NRC-approved T&QP. All armed personnel assigned duties and responsibilities involving the use of weapons must be qualified on each weapon type configured with the primary firearms sighting system that the individual will be assigned. The inspector(s) should verify that the qualifying score for annual daylight qualification courses must be an accumulated total of 70 percent with the handgun and shotgun, and 80 percent with the semiautomatic rifle. ...	
				<u>02.04 Tactical Qualification</u> a. Verify, through observation, that the licensee conducts an annual tactical qualification course that simulates site-specific conditions under which assigned personnel are required to carry out their assigned duties. (10 CFR Part 73, Appendix B VI., F.2) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include the tactical course of fire and training records) to verify that the licensee has developed, conducts, and maintains an annual tactical qualification course that simulates site-specific conditions under which assigned personnel are required to carry out their duties in accordance with the licensee’s protective strategy. The licensee’s tactical qualification course should include the following elements: 1. combined use of handguns (if carried) and shoulder-fired weapons employed during a contingency event; ...	NRC 2.4 戦術資格認定 （以下について、確認事項、具体的なガイダンスが示されている。） a. 年次戦術資格認定コースの実施 b. 年次戦術資格認定の成績
				<u>02.05 Firearms Familiarization Training.</u> a. Verify that the licensee conducts annual firearms familiarization training for armed security personnel in accordance with the NRC-approved T&QP.	NRC 2.5 銃器習熟訓練 （以下について、確認事項、具体的なガイダンスが示されている。）

				(10 CFR Part 73, Appendix B VI, E.1.(c)) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review security plans, implementing procedures, and associated training documentation (to include courses of fire and training records) to verify that the licensee conducts annual firearms familiarization training for armed security personnel. Firearms familiarization, at a minimum, must include the following: a. firearms handling drills; ...	a. 年次銃器習熟訓練の実施
				<u>02.06 Training and Qualification Plan and Implementing Procedures</u> a. Verify that the licensee has established, maintains, implements, and follows an NRC-approved T&QP that describes how the criteria set forth in 10 CFR Part 73, Appendix B VI, will be implemented. (10 CFR 73.55(c)(4), 10 CFR Part 73, Appendix B VI. A.3.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review the licensee’s NRC-approved security plans to verify that the licensee has established, maintains and implements, and follows a T&QP that describes how the criteria set forth in 10 CFR, Appendix B will be implemented. Specifically, the T&QP must describe how minimum training and qualification requirements will be met and include the process by which all individuals will be selected, trained, equipped, tested, and qualified. ...	NRC 2.6 訓練&資格認定(T&Q)計画および実施手順書 (以下について、確認事項、具体的なガイダンスが示されている。) a. T&Q 計画の作成、維持、実施の確認 b. 銃器射撃場活動への参加 c. セキュリティ欠陥の把握と解決の確認
				<u>02.07 On-the Job Training.</u> a. Verify that the licensee’s training and qualification program includes on-the-job training (OJT) performance standards and criteria to ensure that each individual demonstrates the requisite knowledge, skills, and abilities needed to effectively carry out assigned duties and responsibilities before	NRC 2.7 OJT 訓練 (以下について、確認事項、具体的なガイダンスが示されている。) a. 実際の活動の前に OJT を含む資格認定されている b. 緊急時対応に参加する前に 40h 以上の緊急時対

				the individual is assigned the duty or responsibility. (10 CFR Part 73, Appendix B VI., C.2.(a)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the licensee’s security plans, implementing procedures, and associated training documentation (to include a sample of individual training records) to verify that the licensee’s training and qualification program includes OJT performance standards and criteria for each individual assigned security duties and responsibility. OJT performance standards and criteria must ensure that each individual demonstrates the requisite knowledge, skills, and abilities for effective performance of assigned duties and responsibilities. The licensee must implement OJT to ensure that individuals have a basic level of hands-on experience in nuclear security functions before they are considered qualified and ...	応 OJT を含む資格認定されている
				<u>02.08 Requisite Knowledge and Performance</u> a. Verify that security personnel possess adequate knowledge to carry out their assigned duties and responsibilities, including response procedures, use of deadly force, and armed response tactics. (10 CFR Part 73, Appendix B VI, A.4.) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should interview a sample of security personnel and/or facility personnel (if applicable) to determine if they possess adequate knowledge to carry out their assigned duties and responsibilities, including response procedures, use of deadly force, and armed response tactics. Observe a sample of security personnel and/or facility personnel (if applicable) performing their routine duties and/or participating in training activities, if scheduled during the inspection. If the licensee is not conducting certain routine duties or training at the	NRC 2.8 必要な知識とパフォーマンス （以下について、確認事項、具体的なガイダンスが示されている。） a. セキュリティ担当者の保有知識 b. 銃器の取扱いの熟練度

				time of the inspection ...	
				<u>02.09 Re-qualification</u> a. Verify that armed and unarmed individuals are re-qualified annually in accordance with 10 CFR Part 73 Appendix B VI, and the NRC-approved T&QP. (10 CFR Part 73, Appendix B VI, D.2., 10 CFR Part 73, Appendix B VI, A.7.) <u>Specific Guidance</u> No inspection guidance. ...	NRC 2.9 再資格認定 （以下について、確認事項、具体的なガイダンスが示されている。） a. 武装・非武装個人の年次再資格認定 b. 武装メンバーの割り当てられた武器の年 1 回以上の訓練
				<u>02.10 Training Documentation</u> a. Verify that the licensee maintains training documentation in accordance with regulations and requirements. (10 CFR 73.55(b)(4)(i), 10 CFR Part 73, Appendix B VI, H.) <u>Specific Guidance</u> In the review of training documentation, the inspector(s) should select a sample of training records which include newly hired security personnel. The inspector(s) should ensure that training records reflect successful completion of and certification on duty tasks specified in the licensee’s NRC-approved T&QP. The inspector(s) should also determine from records that response personnel meet the physical and psychological criteria for armed status.	NRC 2.10 訓練の文書化 （以下について、確認事項、具体的なガイダンスが示されている。） a. 訓練の文書化
				<u>02.11 Medical Qualifications</u> a. Verify that armed and unarmed individuals assigned security duties and responsibilities are subject to a physical examination that is designed to measure the individual’s physical ability to perform assigned duties and responsibilities. (10 CFR 73 Appendix B VI, B.2.(a)(2)) <u>Specific Guidance</u> To inspect this requirement, the inspector(s) should review a sample of the licensee’s training and qualification records to verify that all individuals	NRC 2.11 医療面の資格認定 （以下について、確認事項、具体的なガイダンスが示されている。） a. 健康診断 b. 医師免許保有者による診断

				who are performing security functions for the security organization are subject to a physical examination. The purpose of this physical examination is to verify that an individual is physically capable to perform assigned duties and responsibilities as identified in NRC-approved security plans and implementing procedures. Physical ...	
				<u>02.12 Physical Fitness Test</u> a. Verify that armed members of the security organization demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test. (10 CFR Part 73, Appendix B VI, B.4.(b)) <u>Specific Guidance</u> To inspect this requirement, the inspectors(s) should review a sample of the licensee's training records to verify that armed members of the security organization demonstrate physical fitness for assigned duties and responsibilities by performing a practical physical fitness test as described in the site's NRC-approved security plans and implementing procedures. ...	NRC 2.12 身体適性検査 (以下について、確認事項、具体的なガイダンスが示されている。) a. 身体的適性 b. 通常時と緊急時の職務に対応 c. インストラクターの資格
				<u>02.13 Reviews</u> <u>Events and Logs.</u> Review and evaluate licensee event reports, safeguards log entries, and corrective action documents for the previous 12 months, or since the last inspection, which are associated with the training program and follow up, if appropriate. <u>Security Program Reviews.</u> Verify that the licensee is conducting security program reviews in accordance with 10 CFR 73.55(m) and that the licensee's training program was included in a review, as required by the regulation. (10 CFR 73.55(m) and 10 CFR Part 73, App. B, Sec. VI, (I), Security Plans)	NRC 2.13 レビュー (以下について、確認事項、具体的なガイダンスが示されている。) a. 事象とログ b. セキュリティプログラム c. 問題の把握と解決

				<u>Identification and Resolution of Problems.</u> Verify that the licensee is identifying issues related to the security training program at an appropriate threshold and entering them in the corrective action program. Verify that the licensee has appropriately resolved the issues regarding regulatory requirements for a select sample of problems associated with the security training program. <u>Specific Guidance.</u> Before commencement of the inspection, the inspector(s) should review all licensee event reports relating to security training to determine if the licensee is capturing security training issues and properly reporting them. For the inspection of this requirement, the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its security training program. The inspector(s) should ensure that the reviews have been conducted in accordance with the requirements of 10 CFR 73.55(m). The inspector(s) should also request that the licensee ...	問題の把握と解決 ✓ 是正処置プログラムへの登録および解決
				<u>02.14 Firearms Pre-emption Authority</u> a. Verify the licensee has completed satisfactory firearms background checks, as required by NRC Order EA-13-092, for members of the security organization who are required to possess, use, or have access to covered firearms and devices as a part of their assigned duties and responsibilities. (NRC Order EA-13-092) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review a sample of firearms background check records for members of the licensee or contracted security organization who are required to possess, use, or have access to firearms and devices. The inspector(s) should verify and consider (as applicable) the following items listed below, which are defined in the NRC Order EA-13-092, to ensure the licensee has completed satisfactory firearms background checks: (1) a satisfactory	NRC 2.14 銃器優先権 (以下について、確認事項、具体的なガイダンスが示されている。) a. 銃器に関する背景調査 b. 資格喪失者の除外方策 c. FBI 提供情報の保管 (5 年)

				firearms background check means a “proceed” response has been received by the licensee, from the Federal Bureau of Investigation (FBI), through the NRC; (2) ensure the ...	
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	—	—	—
参考文献		—	Reference	—	—
別紙・附属書		—	Appendix	—	—
改訂情報		変更日、施行日、簡潔な変更理由（「制定」）	Revision History	Attachment 1: Revision History for IP 81200.07	—

2.3.2.4 IP81200.09「Security Plan Changes for Decommissioning Power Reactors」における調査の結果

原子力規制庁の対応する検査ガイドがないため、NRC の検査ガイドの主な内容を整理し、表 2.3.2-4 にまとめた。主な調査結果を以下に示す。より詳細は、表の備考欄参照。

2.3.2.4.1 対象とする検査プログラム

NRC の検査ガイドでは、上位図書（IMC）情報から、次の検査プログラムで使うことが分かる。

- ・建設時セキュリティ検査

2.3.2.4.2 監督領域

NRC の検査ガイドでは、監督領域を定義していない。（運転フェーズの原子炉監督プロセス（ROP）の検査ガイドではないため）

2.3.2.4.3 検査の目的

NRC の検査ガイドでは、検査官が確認すべき事項を具体的に列挙している（2 項目）。例えば、最初の項目は、「セキュリティ計画の変更によりセーフガードの有効性が低下していないことを確認する」である。

2.3.2.4.4 検査要件

NRC の検査ガイドでは、検査手順の完了（完了時の文例など）、検査リソースの目安（検査時間、サンプル数）が示されている。検査要件そのものは、次項の検査手順に対応する部分でガイダンスを含めて詳細に示している。

2.3.2.4.5 検査手順

NRC の検査ガイドでは、次のように分けて具体的な検査手順および個別のガイダンスを詳細に示している。より詳細は、添付の表 2.3.2-4 の備考欄参照

- ・一般的ガイダンス（共通事項）
- ・セキュリティ計画変更のレビュー

2.3.2.2.6 法令・基準等

2.3.2.1.6 に同じ。

2.3.2.2.7 改訂情報

2.3.2.1.7 に同じ。

表 2.3.2 -4 原子力規制庁検査ガイド（該当なし）と米国 NRC 検査ガイド IP81200.09 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		米国 NRC 検査ガイド		両者間の主な相違点
【ガイド】－ （－）		【ガイド】 IP81200.09 Security Plan Changes for Decommissioning Power Reactors （Issue Date: 02/18/21, Effective Date: 02/18/2021）（5 頁）		
項目		主な内容		
図書全体構成		図書全体構成		本文 改訂情報
	－	－	PROGRAM APPLICABILITY	IMC 2202, App A
	－	－	－	－
	検査の目的	－	01. INSPECTION OBJECTIVES	01.01 To verify that changes to the licensee’s security plans have not decreased the safeguards effectiveness as required by Title 10 of the Code of Federal Regulations (10 CFR) 50.54(p)(2). 01.02 To verify and assess licensee implementation of the change process in accordance with 10 CFR 50.54(p)(2).
	検査要件	－	03. Procedure Completion 04. RESOURCE ESTIMATE	03 PROCEDURE COMPLETION The security plan change reviews should be documented in an inspection report in accordance with Inspection Manual Chapter 0611. Performance of this inspection procedure does not constitute approval of the security plan changes. An example of documentation wording for security plan changes with no apparent decrease in safeguards effectiveness is as follows: “Since the last NRC inspection of this program area, Security Plan Revision(s) XX to XX were implemented based on your determination, in accordance with 10 CFR 50.54(p)(2), that the changes resulted in no decrease in safeguards effectiveness of the security plan, and that the revised security plan continues to meet the requirements of 10 CFR 73.55(b). The inspectors conducted a review of the security plan changes to evaluate for potential decrease in safeguards effectiveness of the security plan. However, this review does not constitute formal NRC approval of the

				changes. Therefore, these changes remain subject to future NRC inspection in their entirety.” This procedure is considered complete when the inspection requirements listed in the procedure have been satisfied. For sites that have not made any security plan changes since the last baseline inspection, the minimum sample size is the security plan review per 81200.09-02.01. <u>04 RESOURCE ESTIMATE</u> The resource estimate for completion of this procedure consists of a range between 12- 16 hours of direct inspection effort per sample. The resource allocation includes one or multiple security plan changes that have been submitted to the NRC since the last inspection. The frequency at which this inspection activity is to be conducted is annually (once per year) or as needed dependent on changes that could result in a decrease in safeguards effectiveness. The sample size for this procedure is one.	
	検査手順	—	02. INSPECTION REQUIREMENTS	<u>General Guidance.</u> Each application for an operating license subject to the provisions of 10 CFR 73.55, must include a Physical Security Plan, Training and Qualification Plan, a Safeguards Contingency Plan, and a Cyber Security Plan. These four plans describe the licensee's physical protection system/program that will be used (or implemented) to prevent radiological sabotage in accordance with the Commission requirements. These plans are collectively referred to as the "Security Plan.” A review of the licensee’s current approved exemptions and license amendments should be completed before implementing this inspection procedure. Licensees may request an exemption to address certain requirements to implement specific components of their programs (e.g., use of a certified fuel handler, communications with the control room, de-vitalization of the control room). The licensee can change an element of the plan if an evaluation is performed to demonstrate that the plan change continues to ensure the licensee’s capability for detection, assessment, interdiction, and neutralization	NRC 2. 検査要件 • 一般的なガイダンス ✓ セキュリティ計画は、次の総称 ➤ 物理的セキュリティ計画 ➤ 訓練・資格認定計画 ➤ セーフガード緊急事態計画 ➤ サイバーセキュリティ計画 ✓ 計画変更によっても設計基準脅威（DBT）の検出、評価、阻止、緩和能力が維持されることが実証されれば、計画要素を変更できる。 ✓ 計画変更がセーフガードの有効性を低下させるかどうかに関する事業者による評価は、NRC承認なしに変更を実施できるか、事前にNRCの承認が必要かを判断ために使用される。 ✓ 認可変更など、NRC承認を必要とする提出物は、この検査の対象外。 ✓ NRCによる評価は、規制要件の遵守、DBTに対する防護能力への影響、サイト固有の脆弱性の発生有無の観点から行われる。 ✓ この手順書は、オフィス内、サイトのいずれかまたは両方に適用できる。

				is maintained to adequately protect against the design basis threat (DBT) of radiological sabotage. This plan change can be submitted as a 10 CFR 50.54(p)(2) if, in addition to the above, the change meets all regulations and considers site specific conditions (site characteristics, location, size, etc.). If a plan change can meet these criteria, it is not considered a decrease in safeguards effectiveness. If the change cannot meet these criteria, the proposed plan change must be submitted as a license amendment request under 10 CFR 50.90 and receive U.S. Nuclear Regulatory Commission (NRC) approval prior to implementation, pursuant to 10CFR 50.54(p)(1). The licensee's evaluation as to whether the plan change constitutes a decrease in safeguards effectiveness is used by the licensee to determine whether it has the authority to implement the change without prior NRC approval under 10 CFR 50.54(p)(2), or must submit for prior NRC approval under 10 CFR 50.90. Licensee submittals that require NRC approval, such as license amendment requests, are not subject to this inspection procedure and will be reviewed by the Office of Nuclear Security and Incident Response (NSIR) and approved by the Office of Nuclear Reactor Regulation (NRR) or the Office of Nuclear Material Safety and Safeguards (NMSS). The NRC's inspection of 10 CFR 50.54(p)(2) should verify that changes to security programs did not result in: (1) a noncompliance or violation of established regulatory requirements; (2) an adverse impact to the licensee's ability to detect, assess, interdict, and neutralize to protect against the DBT of radiological sabotage; and (3) a site-specific vulnerability. As an example, suppose a licensee has more than the minimum number of ten armed responders (AR)s, required by 10 CFR 73.55(k)(5)(ii). The licensee could use the 10 CFR 50.54(p)(2) process to reduce the number of ARs to ten, the regulatory minimum. If the site-specific evaluation determines that the requirements of 10 CFR 73.55 continue to be met, and there is no adverse impact to the licensee's capability to detect, assess, interdict, and neutralize as a result of the change, the licensee can make the change in	
--	--	--	--	--	--

			accordance with 10 CFR 50.54(p)(2). However, if the licensee plans to reduce the number of ARs below the minimum requirement of ten ARs, the licensee must submit a license amendment request in accordance with 10 CFR 50.90 for review and approval by the NRC, prior to making this change. To prepare for inspection activity, inspectors should review the previous security plan revision in effect at the time of the last baseline inspection to gain a better understanding of the nature of the changes. If the regional inspector anticipates the inspection of all security plan changes would likely exceed the 16-hour resource allocation, the inspector should contact NRC Headquarters (HQ) NSIR for support. This procedure can be conducted in-office, on-site, or a combination of both.	
			<u>02.01 Review Security Plan Changes</u> For this portion of the inspection, the inspector(s) should review the licensee’s security plan. The inspector(s) should also review all 10 CFR 50.54(p)(2) security plan changes that have been submitted to the NRC since the last inspection. a. Verify that the licensee submits reports associated with security plan change(s) under 10 CFR 50.54(p)(2) to the NRC within 2 months after the change has been made. (10 CFR 50.54(p)(2)) <u>Specific Guidance</u> Inspector(s) should review the report, submitted by the licensee to the NRC, which documents the changes associated with the licensee’s implementation of its physical protection program. The inspector(s) should verify that the submittal was provided to the NRC within the required two-month period. b. Assess each licensee-submitted security plan change to verify that the change(s) does not decrease the safeguards effectiveness of the plan. (10 CFR 50.54(p)(2)) <u>Specific Guidance</u>	NRC 2.1 セキュリティ計画変更のレビュー a. 変更後 2 カ月以内に NRC に報告書を提出したか？ <u>具体的なガイダンス</u> ➤ 事業者が提出した報告書を確認 b. 変更を評価し、セキュリティ対策の有効性が低下していないことを確認 <u>具体的なガイダンス</u> ➤ 具体的な裏付け文書の要求と確認（訓練・演習報告、自己評価、爆破解析、地図、是正処置文書、手順書、教育計画など） ➤ セーフガード能力低下の影響可能性がある変更について詳細レビュー c. 変更の実施前に緊急時対応計画のセーフガード能力が全て利用可能で発揮できることを確認していることを確認 <u>具体的なガイダンス</u> ➤ 計画変更の実施に関する文書をレビューし、影響を受ける可能性がある領域がカバーされていることを確認。 ➤ 計画変更の実施関係者へのインタビュー ➤ 関連図書のリクエスト d. 計画変更に関わる手順書の新規作成または改訂の妥当性 <u>具体的なガイダンス</u> ➤ 最近の計画変更に関わる手順書のレビュー

				Inspector(s) should request supporting documentation that demonstrates the change does not represent a decrease in safeguards effectiveness of the security plans and how the change continues to provide reasonable assurance through the effective implementation of the security plans and site-protective strategy. Types of documentation may include drill and exercise reports, self-assessments, blast analyses, maps, corrective action documentation, procedures, and lesson plans. The inspector shall perform an in-depth review of selected security plan change items that could potentially result in a decrease in safeguards effectiveness. c. Verify that prior to implementing the plan change(s), the licensee ensured all safeguards capabilities specified in the safeguards contingency plan are available and functional. (10 CFR 50.54(p)(2)(i)) <u>Specific Guidance</u> For inspection of this requirement, inspector(s) should review documentation that describes the licensee’s implementation of the plan change. This documentation should cover areas of implementation such as impacts associated with contingency response, physical protective measures, communication capabilities, and other areas that may have been impacted by the change. The inspector(s) should conduct interviews with security personnel responsible for implementing the plan change. The inspector(s) may also request that the licensee provide a protective strategy overview/briefing that addresses the impacts of the plan change(s) on the site protective strategy and all supporting physical protection measures and security equipment that the licensee employs in support of its protective strategy. The documentation review should provide insights pertaining to the plan changes’ impacts to the licensee's protective strategy and should support the completion of the inspection requirements within this section.	e. 計画変更の影響を受ける職員がセーフガード事象に対応できる訓練を受けていることを確認 <u>具体的なガイダンス</u> ➤ 職員のサンプルにインタビュー ➤ 計画変更の実施に携わる職員向け訓練マテリアル（レスンプラン、概要説明、コンピュータベース訓練など）のレビュー
--	--	--	--	---	---

				d. Verify that the licensee has developed new or revised procedures associated with the plan change(s), according to Appendix C to Part 73, as appropriate. (10 CFR 50.54(p)(2)(ii)) <u>Specific Guidance</u> Inspector(s) should review licensee procedures associated with recent plan changes. Specifically, inspectors should ensure the procedures reflect the plan change and align with licensee implementation practices. Inspectors should consider conducting observations of activities associated with the plan change to verify that the licensee implementation aligns with the plan change(s). e. Verify that licensee personnel impacted by the plan change(s) have been trained to respond to safeguards incidents as outlined in the plan and specified in procedures. (10 CFR 50.54(p)(2)(iii)) <u>Specific Guidance</u> Inspector(s) should conduct interviews with a sample of licensee personnel to determine the methodology the licensee used to ensure it has appropriately trained the personnel responsible for implementation of the plan change(s). Additionally, the inspector(s) should review training material (i.e., lesson plans, briefing materials, computer-based training) developed to provide training to licensee personnel responsible for implementing the plan change(s).	
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	—	—	—
参考文献	—	—	Reference	—	—
別紙・附属書	—	—	Appendix	—	—
改訂情報	変更日、施行日、簡潔な変更理由（「制定」）	—	Revision History	Attachment 1: Revision History for Inspection Procedure 81200.09, “Security Plan Changes for Decommissioning Power Reactors”	—

2.3.2.5 IP81300「Physical Security Requirements for Independent Spent Fuel Storage Installations」における調査の結果

原子力規制庁およびNRCの検査ガイドの主な内容および相違点を整理し、表 2.3.2.5 にまとめた。主な比較結果を以下に示す。より詳細は、表の備考欄参照。

2.3.2.5.1 対象とする検査プログラム

NRC の検査ガイドでは、上位図書（IMC）情報から、次の検査プログラムで使うことが分かる。

- ・一般の、特別な、頻繁でない検査
- ・セキュリティ追加検査プログラム
- ・使用済燃料貯蔵および GTCC 廃棄物の検査プログラム

2.3.2.5.2 監督領域

NRC の検査ガイドでは、監督領域を定義していない。（運転フェーズの原子炉監督プロセス（ROP）の検査ガイドではないため）

2.3.2.5.3 検査の目的

NRC の検査ガイドでは、検査官が確認すべき事項を具体的に列挙している（2 項目）。例えば、最初の項目は、「独立使用済燃料貯蔵施設（ISFSI）の物理的防護プログラムが規制を遵守して実施されていることを確認する」である。

2.3.2.5.4 検査要件

NRC の検査ガイドでは、検査の完了（検査項目の全てが完了）、検査リソースの目安（検査時間、サンプル数）が示されている。検査要件そのものは、次項の検査手順に対応する部分でガイダンスを含めて詳細に示している。

2.3.2.5.5 検査手順

NRC の検査ガイドでは、次のように分けて具体的な検査手順および個別のガイダンスを詳細に示している。より詳細は、添付の表 2.3.2-5 の備考欄参照

- ・一般的ガイダンス（共通事項）
- ・共同立地/AFR ISFSI の一般認可要件とガイダンス
 - ✓ 一般認可要件とガイダンス
 - ✓ リサーチ活動（人、物、車両）
 - ✓ アクセス制御ポイントとアクセス制御
 - ✓ 情報へのアクセスの制御

- ✓ セキュリティ設備
- ✓ 地元法執行機関（LLEA）
- ✓ 武器の保守
- ✓ レビュー
- ✓ 特定の認可要件およびガイダンス

2.3.2.5.6 法令・基準等

2.3.2.1.6 に同じ。

2.3.2.5.7 改訂情報

2.3.2.1.7 に同じ。

表 2.3.2-5 原子力規制庁検査ガイド（該当なし）と米国 NRC 検査ガイド IP81311 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		米国 NRC 検査ガイド		両者間の主な相違点
【ガイド】－ （－）		【ガイド】 IP81311 Physical Security Requirements for Independent Spent Fuel Storage Installations (Issue Date: 06/28/22, Effective Date: 08/01/2022) (29 頁)		
項目	主な内容	項目	主な内容	
図書全体構成	—	図書全体構成	本文 改訂情報	—
	—	PROGRAM APPLICABILITY	IMCs 2201C, 2202B, 2690	NRC ・検査プログラム（上位図書） ✓ IMC 2201 App. C（一般の、特別な、頻繁でない検査） ✓ IMC 2202 App. B（セキュリティ追加検査プログラム） ✓ IMC 2690（使用済燃料貯蔵および GTCC 廃棄物の検査プログラム）
	監督領域	—	—	—
	検査の目的	1. INSPECTION OBJECTIVES	01.01 Verify the licensee’s physical protection program for an independent spent fuel storage installation (ISFSI) is implemented in accordance with the U.S. Nuclear Regulatory Commission (NRC)-approved security plans, regulatory requirements, and any other applicable requirements and orders. 01.02 Determine if the ISFSI physical protection program provides assurance, consistent with regulations in Title 10 of the <i>Code of Federal Regulations</i> (10 CFR 73), that activities involving spent nuclear fuel and high-level radioactive waste do not constitute an unreasonable risk to public health and safety.	NRC 1. 検査の目的 ✓ 独立使用済燃料貯蔵施設（ISFSI）の物理的防護プログラムが規制を遵守して実施されていることの確認 ✓ ISFSI の物理的セキュリティプログラムにより、使用済燃料や高レベル廃棄物を扱う活動が公衆に不合理なリスクをもたらさないことが保証されているかどうかを判断
	検査要件	RESOURCE ESTIMATE	<u>03 PROCEDURE COMPLETION</u> This procedure is considered complete when all of the applicable inspection requirements listed within this procedure have been completed. There are 51 inspection requirements for a general license and 26 inspection requirements for a specific license. <u>04 RESOURCE ESTIMATE</u>	NRC 3. 検査の完了 ✓ 検査手順書の検査項目がすべて完了 4. リソース見積り ✓ 検査時間（サイトの ISFSI とオフィス） ✓ 検査頻度（3 年毎）

				The resource estimate for the completion of this procedure consists of 16 hours for the inspection of a co-located ISFSI, at a reactor, and 24 hours for the inspection of a non-co-located ISFSI, away from reactor. The frequency at which this inspection activity is to be conducted is triennially (once every 3 years).	
	検査手順	—	2. INSPECTION REQUIREMENTS AND GUIDANCE	This inspection procedure (IP) is applicable to ISFSIs licensed under 10 CFR Part 50, Part 52, and Part 72. This IP is divided into two sections to address the two different types of licenses (general and specific) for the receipt, transfer, packaging, and possession of spent nuclear fuel (SNF) and power reactor-related greater-than-class C (GTCC) waste. (10 CFR 72.2(a)(1)) Spent fuel is stored at an ISFSI located either at an operating power reactor site (i.e., inside the reactor’s protected area (PA), in the owner-controlled area (OCA), or in a separate PA), at a decommissioning power reactor site, or at an away-from-reactor (AFR) site using a dry cask storage system (DCSS). In lieu of a DCSS, a wet storage ISFSI may use a spent fuel pool (SFP) as part of a wet storage system to store the spent fuel. This IP will be implemented at an AFR site that is 1) a specifically licensed ISFSI whose associated support programs are not inspected under a 10 CFR Part 50 license, or 2) any generally licensed ISFSI where decommissioning and final survey activities related to reactor operations are completed and the only remaining operation conducted under the 10 CFR Part 50 license is the operation of the general licensed ISFSI. Section 02.01 through 02.08 applies to a 10 CFR Part 50 or Part 52 licensee issued a general license for an ISFSI under 10 CFR 72.210 of Subpart K. This general license authorizes the use of a DCSS that has been approved in accordance with 10 CFR Part 72 and uses casks listed in 10 CFR 72.214. Section 02.09 applies to any licensee issued a specific license for an ISFSI under 10 CFR 72.40. Under a specific license, any approved DCSS design can be used at any location. While a specific 10 CFR Part 72 license is independent from a co-located 10 CFR Part 50 reactor license, some structures, systems, and programs that are part of the licensing basis for the	NRC 2. 検査要件とガイダンス ✓ この IP は、使用済燃料（SNF）およびクラス C を超える（GTCC）廃棄物の受領、移送、梱包、保有に関する 2 種類の認可（一般、個別）に対応するため、2 セクションに分かれる ✓ 使用済燃料は、廃炉サイト（防護区域（PA）内、所有者管理区域（OCA）内、または別の PA 内）のまたは原子炉から離れた（AFR）サイトに乾式キャスクシステム（DCSS）を用いて貯蔵されている。 ✓ DCSS の代わりに、湿式貯蔵 ISFSI では、湿式貯蔵設備の一部として使用済燃料プールが使用される。 ✓ 本 IP は、AFR サイトの ISFSI で実施される。次のいずれかの ISFSI になる。 ➢ 個別認可された ISFSI。関連プログラムは、10 CFR 50 の認可に基づく検査の対象外。 ➢ 一般認可された ISFSI。廃止措置および原子炉運転の最終調査活動が完了し、10 CFR 50 の認可に基づく残りの運転が一般認可された ISFSI の運転のみ。 ✓ セクション 2.1～2.8 は、ISFSI の一般認可が発行された事業者、2.9 は ISFSI の個別認可が発行された事業者に適用。 ✓ 一般認可 ISFSI と個別認可 ISFSI に関する補足説明。 ✓ 本 IP の準備として、検査官は適用される認可の種類を把握し、セキュリティ計画、安全評価報告等の関連文書に精通しておくこと。

				reactor license may be shared and subject to different security requirements and or security orders. In accordance with 10 CFR 73.55(r), “Alternative measures,” for general licenses, the Commission may authorize a licensee to provide a measure for protection against radiological sabotage other than one required by 10 CFR 73.55. Exemptions under 10 CFR 73.5 and 10 CFR 72.7 can be granted by the Commission for both general and specific ISFSI licenses from the requirements in 10 CFR Part 73 and 10 CFR Part 72, respectively. Inspector(s) should review the licensee’s physical security plans that describe any alternative measures authorized and/or any exemptions granted by the Commission. Likewise, in accordance with 10 CFR 73.51(d) for specific licenses, the Commission may, on a specific basis and upon request or on its own initiative, authorize other alternative measures for the protection of spent fuel and high-level radioactive waste subject to the requirements of 10 CFR 73.51 if after evaluation of the specific alternative measures, it finds reasonable assurance of compliance with the performance capabilities of the general performance objectives (10 CFR 73.51(b)). The requirements of 10 CFR 73.21 and 73.22 apply to both general and specific licensees. This IP establishes a method for inspecting an ISFSI. The primary application is for the inspection of a licensed ISFSI containing cask-stored spent fuel; however, most requirements are also applicable to existing wet storage facilities. Prior to the first loading of SNF, a general license must notify the NRC at least 90 days in advance in accordance with 10 CFR 72.212(b)(1). To promote efficiency, selected portions of this procedure may be conducted as early as practical during construction and installation of security features or components to identify problems early before completion of the work which may make their resolution difficult. In preparing to complete this procedure, the inspector(s) needs to identify what type of license the licensee has been issued e.g., general license or specific license. Additionally, the inspector(s) should familiarize themselves with relevant documentation which may include, but is not limited to the licensee’s	
--	--	--	--	--	--

				security plans, safety evaluation report (SER), and site-specific and/or corporate procedures. Specifically, the inspector(s) should apply additional attention to the NRC approved SER and any recent security plan changes that could be relevant to the inspection activity. Additionally, the inspector(s) should note that not all inspection requirements are applicable for each ISFSI licensee. The inspector(s) will need to review the licensee's approved exemptions, alternative measures, physical security plan, and SER to identify any requirements that may not apply. The inspector(s) should note that some requirements may already be inspected under other security inspection programs, (e.g., reactor security baseline inspection program, security decommissioning inspection program) if the inspector(s) identifies elements that are included under another program they do not need to be reinspected under this IP. This IP applies to ISFSIs located inside an operating reactor PA for its initial inspection. For subsequent inspections, ISFSIs located inside an operating power reactor PA are subject to the security requirements of 10 CFR 73.55 and subject to the baseline security inspection within the reactor oversight program.	
				<u>General License Requirements and Guidance for Co-Located / AFR ISFSI</u> <u>02.01 General License Requirements and Guidance.</u> Under 10 CFR 72.210, a general license is issued for the storage of SNF in an ISFSI at power reactor sites to persons authorized to possess or operate nuclear power reactors under 10 CFR Part 50 or Part 52. Through completion of the inspection activities for this IP, inspector(s) shall verify or determine that the licensee's physical protection program associated with this sample is designed and implemented to protect the SNF against the design basis threat (DBT) of radiological sabotage (10 CFR 72.212(b)(9)) and meet the requirements of site-specific security orders (e.g., interim compensatory measures (ICMs), additional security measures (ASMs)). Inspector(s) should note that ICMs and ASMs are two different documents that encompass the same security requirements. Licensees	NRC 共同立地/AFR ISFSI の一般認可要件とガイダンス 02.01 一般認可要件とガイダンス ✓ 原子炉所有／運転を認可された者に対して、発電炉サイトにおける ISFSI での使用済燃料（SNF）保管のために一般認可が発行される。 ✓ 検査官は、物理的防護プログラムが設計基準脅威（DBT）から SNF を防護するために設計、実施され、サイト固有のセキュリティ命令、追加のセキュリティ措置を満たしていることを確認する。 a. 規制要件にしたがって、使用済燃料を DBT から保護していることを確認する。 具体的なガイダンス 対象となる関連文書、確認内容、検討事項。 b. ISFSI 防護対策の有効性を確認する。 具体的なガイダンス 対象となる関連文書、確認内容。 c. 使用済燃料の貯蔵が PA 内にあることを確認す

				who had an existing ISFSI prior to September 2007 were issued the ICMs and licensees who built an ISFSI after September 2007 were issued the ASMs. a. Verify the licensee protects the spent fuel against the DBT of radiological sabotage in accordance with the provisions and requirements as are set forth in the licensee’s physical security plan pursuant to 10 CFR 73.55 and the conditions and exemptions under the provisions of 10 CFR 72.212(b)(9) and any site-specific security orders. <u>Specific Guidance</u> For this portion of the inspection, the inspector(s) should review the licensee’s site security orders, security plan, training and qualification plan, safeguards contingency plan, protective strategy, and relevant implementing procedures and ensure the protection of the ISFSI has been incorporated into the relevant documents. The inspector(s) should consider conducting a review of past security inspection reports for the ISFSI. ...	る。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容。
—	—	—	—	<u>02.02 Search Activities (Personnel, Materials, and Vehicles)</u> a. Verify the licensee has established measures to observe all vehicle search functions (OCA and PA) in a manner that enables the initiation of a response. (10 CFR 73.55(g)(1)(ii)(C)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the licensee’s security plans and implementing procedures for the conduct of vehicle search at the OCA and PA vehicle access control points. The OCA vehicle access control points are required to have video surveillance equipment that is monitored by a member of the security organization (other than the armed over-watch officer who is positioned to provide the immediate response) to observe search activities and initiate a response when necessary. The PA vehicle access control point may have either video surveillance equipment used by security force	NRC 02.02 リサーチ活動（人、物、車両） a. 対応開始を可能にする方法で、全車両リサーチ機能（OCA および PA）を観察する方策を確立していることを確認する <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、検討事項。 b. PA へのアクセスを許可する前に、人、物、車両が適切にリサーチされていることを確認する <u>具体的なガイダンス</u> なし。 c. PA への入域前に、身体検査または銃器・爆発物検出器による人員の検査がなされていることを確認する <u>具体的なガイダンス</u> 現場観察、確認内容、考慮事項。 d. サーチプロセスから物を除外するセキュリティ方策には、明確な特定等の適切な実施が含まれていることを確認する <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、検討事項。

				members to monitor the search process and initiate response or may be the subject of direct surveillance by a member of the security organization to monitor the search process and initiate a response if necessary. ...	e. サーチプロセスから大きな物を除外するセキュリティ方策には、武装エスコート等の適切な実施が含まれていることを確認する <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、検討事項。 f. 銃火器、爆発物等の持ち込みの試み／疑いに対するアクセス拒否行動が実施されていることを確認する <u>具体的なガイダンス</u> 必要な予備知識、必要な場合の質問、確認内容、考慮事項。 g. PA 内の全車両が、(1)プラントの機能または緊急時対応に使用される、(2)エスコートなしで PA にアクセスが認められた人等が運転する、(3)未使用時はキーが外されているか使用できなくなっていることを確認する <u>具体的なガイダンス</u> なし。 h. 有害物質を運ぶ車両に武装したエスコートをアサインする方策を確立していることを確認する <u>具体的なガイダンス</u> なし。
—	—	—	—	<u>02.03 Access Control Points and Access Controls.</u> a. Verify the licensee has established and implements measures to control keys, locks, combinations, passwords, and related access control devices used to control access to the PA and security systems. (10 CFR 73.55(g)(6)(i)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the licensee’s security plans and implementing procedures to identify security systems for which the licensee controls access. The security systems that should have access control measures associated with them could be areas such as alarm stations, access badging terminals, or secondary power supplies for alarm annunciation equipment and communications systems which are required by regulation or through the licensee’s security plans and implementing procedures. Access controls implemented by the licensee may include equipment or systems that are maintained in a locked	NRC 02.03 アクセス制御ポイントとアクセス制御 a. PA およびセキュリティシステムへのアクセスを制御するための鍵、ロック、組み合わせ、パスワード、および関連するアクセス制御装置をコントロールする方策を確立し実施していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、検討事項。 b. 人、物、車両が PA に入る各アクセスポイントでアクセスが適切に制御されていることを確認する。 <u>具体的なガイダンス</u> 事前の学習の必要性、対象となる関連文書、確認内容、観察、考慮事項 c. アクセス制御装置が、エスコートなしアクセス権があり業務遂行のためにアクセスが必要な人物にのみ提供されることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、入手方法、確認内容 d. アクセス制御装置が貸与された人物の記録を保

				area with the specific keys/key cards for entry to the area being controlled. Additionally, the control of passwords that provide access to the functions of a security computer system or an access badging terminal should be controlled. ...	持し、少なくとも年 1 回、PA およびアクセス制御装置を説明するプロセスを実施していることを確認する。 <u>具体的なガイドンス</u> なし e. 不正利用やアクセス権喪失者による利用がなされたアクセス制御装置を検索、変更、回転、無効化する方策を確立していることを確認する。 <u>具体的なガイドンス</u> 対象となる関連文書、確認内容 f. PA へのエスコートなしが認められた人物に対する番号・写真付 ID バッジシステムが実行されていることを確認する。 <u>具体的なガイドンス</u> なし g. PA へのエスコート付アクセスを認められた人物が公認の写真付 ID カードの提示により確認されるアイデンティティを有し、エスコートが必要なことを示すバッジを着用し、入域の日付、時間、目的等を記入し、その記録が3年間保持されることを確認する。 <u>具体的なガイドンス</u> 対象となる関連文書、可能な場合の観察、確認内容 h. PA への人物アクセス制御ポイントで、アクセス制御設備もアクセス制御方策も、入域または再入域の前に人物の特定、承認、サーチなしで入域または再入域を許容しないことを確認する。 <u>具体的なガイドンス</u> 活動の観察、プロセスの確認、確認内容 i. PA に入域する全ビジターにエスコートが付くことを確認する。 <u>具体的なガイドンス</u> なし j. PA 内でビジターにエスコートが付く割合がセキュリティ計画通りか確認する。 <u>具体的なガイドンス</u> なし k. アクセス制御ポータルを物理的障壁の外側にまたは同時に確立していることを確認する。 <u>具体的なガイドンス</u> なし l. ザクセス制御ポータルには、意図する機能に応じて、ロック装置、侵入検知設備、サーバイラ
--	--	--	--	---	---

					ンス設備が付いていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 m. バッジプロセスを保護するための方策を、必要に応じて、実施および維持していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、検討事項
—	—	—	—	<u>02.04 Controlling Access to Information</u> Verify the licensee, certificate holder, or applicant has established, implemented, and maintains an information protection system that includes the applicable measures for SGI as specified in 10 CFR 73.22 and subsequently published NRC Orders. (10 CFR 73.21(a)(1)(i) and 10 CFR 73.21(b)(2)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should verify that the licensee has developed a program to address the control, protection, and designation of safeguards information, and that the implementing measures are documented in procedures. ...	NRC 02.04 情報へのアクセスの制御 ・SGI に適用可能な方策を含む情報保護システムを確立、実施、維持していることを確認する。 <u>具体的なガイダンス</u> 対象となるプログラム、関連文書、確認内容、検討事項。
—	—	—	—	<u>02.05 Security Equipment</u> a. Verify the licensee has developed testing and maintenance procedures for all security equipment identified as a component of the licensee’s physical protection program and protective strategy in accordance with the security plans and implementing procedures. (10 CFR 73.55(c)(7) and 10 CFR 73.55(n)) <u>Specific Guidance</u> The inspector(s) should review the licensee’s security plans and implementing procedures for equipment maintenance and testing. This review should be conducted to determine that testing is performance-based, challenges the capabilities of the equipment, and is in accordance with the security plans and associated implementing procedures. The inspector(s) should also verify that the licensee’s	NRC 02.05 セキュリティ設備 a. セキュリティ計画および実施手順書に従い、物理的防護プログラムおよび防護戦略の構成要素として特定された全てのセキュリティ機器の試験および保守の手順書を策定していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 b. 境界侵入検知システム（IDS）および評価装置が、操作性および信頼性の確保のために保守手順書にしたがって保守されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連プログラム、確認内容 c. 試験活動の観察を通じて、PA 周辺のバリアへの侵入が完了する前に、IDS が侵入やその試みを検出すること、規制を遵守して試験されているこ

				testing and maintenance procedures are in accordance with the manufacturers’ design specifications for system application and conform to manufacturers’ recommendations for testing and maintenance. ...	とを確認する。 <u>具体的なガイダンス</u> 試験の観察、確認内容、試験の補足説明 d. 試験活動の観察を通じて、警報装置が改ざん防止機能および自己点検機能を有していること、試験が規則および試験手順書にしたがって実施されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 e. PA 周辺で検出された活動の評価機能と対応の開始を確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 f. 試験活動の観察を通じて、PA 周辺のビデオ評価資産が視覚的表示を提供し、警報の前後に検出された活動のリアルタイムおよび録画再生ビデオ画像を提供し、装置が規則およびライセンスの試験手順にしたがって試験されていることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容、考慮事項 g. 試験活動の観察または試験・保守記録のレビューを通じて、侵入検知システムが、警報システムまたはその構成部品が故障した時やシステムがバックアップ電源で作動している時に自動表示を提供すること、この機能の試験が適切に実施されることを確認する。 <u>具体的なガイダンス</u> 観察、対象となる関連文書、確認内容 h. 建物の壁または屋根が、隔離区域を設定していない PA 周辺バリアの一部を構成する場合、適切な検知・評価方法および物理的バリアを導入していること、この区域がセキュリティ計画に記載されていることを（該当する場合）確認する。 <u>具体的なガイダンス</u> 観察、対象となる関連文書、確認内容 i. 物理的防護プログラムおよび防護戦略を支援するために採用している内部検出・評価装置が、操作性および信頼性を確保するために、保守手順書にしたがって保守されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連プログラムおよび文書、確認内
--	--	--	--	--	---

					容 j. 物理的防護プログラムおよび防護戦略を支援するために採用している警報局コンソール機器が、保守手順にしたがって保守され、操作性および信頼性が確保されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 k. 警報ステーション内で、警報の検知と評価、適切な対応の開始と調整、オフサイト支援の要請、指揮統制などを行うオペレーター能力を妨げる活動が行われていないことを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 l. 中央警報ステーション（CAS）が次のように構成されていることを確認する：(1) PA 内に設置されている，(2) PA 周辺から内部が見えない，(3) 弾丸に耐える構造である，(4) VA として指定されている（適宜）。 <u>具体的なガイダンス</u> CAS の補足説明 m. 試験活動の観察を通じて、CAS が各当直警備隊員との継続的な通信機能を維持し、機能の試験が適切に実施されていることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 n. OCA および PA バリアを含むすべての物理的バリアの完全性を維持するプロセスを有していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 o. アクティブ車両バリア・システム(AVBS)の作動が、試験手順書に従った試験を通じて定期的にチェックされていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 p. 試験活動の観察を通じて、隔離ゾーンが設計され、PA バリアの両側で活動の観察と評価ができる十分な広さがあることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 q. 試験および評価手順が、製造業者の設計特性、性能仕様、試験勧告と一致していることを確認し、機器が受入基準を満たすように試験および評価されていることを確認する。
--	--	--	--	--	--

					<u>具体的なガイダンス</u> 対象となる関連文書、確認内容 r. 評価および対応活動を支援するために、隔離ゾーンおよび PA の外部エリア内の照明が、規制要件にしたがって維持および／または低照度技術によって増強されていること、機器が適切に試験されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、考慮事項 s. セキュリティ部隊により決定された警報の原因および最終処分を含む、すべての警報の記録が維持されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 t. 劣化または動作不能な設備、系統、機器を補償するために実施している補償措置が、すべての規制要件を満たしていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、考慮事項
				<u>02.06 Local Law Enforcement Agency (LLEA)</u> Verify the licensee has a documented agreement with applicable LLEA to include estimated response times and capabilities. (10 CFR 73.55(k)(9)) <u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the documented liaison that the licensee has established with LLEA (local, state, federal). The liaison should be in the form of a written document (i.e., letter, agreement, memorandum of understanding, etc.) that demonstrates that the licensee has requested the assistance of these agencies to support its security force with contingency events. The inspector(s) should verify the licensee’s established law enforcement liaison to the extent documented in security plans and implementing procedures.	NRC 02.06 地元法執行機関（LLEA） ・ 該当する LLEA との間で、想定される対応時間および能力を含む文書化された協定を結んでいることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容
—	—	—	—	<u>02.07 Weapons Maintenance</u> a. Verify (if applicable) that the licensee has established and implements measures for the control and accountability of all assigned firearms and ammunition.	NRC 02.07 武器の保守 a. 割り当てられたすべての銃器・弾薬の管理および説明責任のための手段を確立し、実施していることを確認する（該当する場合）。

			<u>Specific Guidance</u> For the inspection of this requirement, the inspector(s) should review the licensee’s physical security plan, firearms and ammunition control and accountability procedures. The inspector(s) should verify, through a review of records and through observation, that firearms control and accountability measures are being implemented in accordance with physical security plan, licensee procedures and that these measures restrict unauthorized access to firearms and ammunition. Accountability measures should be conducted at a periodicity that would provide a timely indication that a firearm is missing or has an unknown disposition. ...	<u>具体的なガイダンス</u> 対象となる関連文書、確認内容、考慮事項 b. 銃器の保守に関する活動を文書化していることを確認する（該当する場合）。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、考慮事項
—	—	—	<u>02.08 Reviews</u> a. <u>Events and Logs</u>. Review and evaluate licensee event reports and safeguards log entries for the previous 12 months, or since the last inspection. (10 CFR 73.55(b)(10) and 10 CFR 73.71) b. <u>Security Program Reviews</u>. Verify that the licensee is conducting security program reviews in accordance with 10 CFR 73.55(m). c. <u>Identification and Resolution of Problems</u>. Verify that the licensee is identifying issues related to the security program at an appropriate threshold and entering them in the corrective action program. Verify that the licensee has appropriately resolved the issues regarding regulatory requirements for a selected sample of problems associated with the security program. (10 CFR 73.55(b)(10)) <u>Specific Guidance</u> Before the inspection, the inspector(s) should review and evaluate licensee event reports and safeguards log entries, since at least the last inspection, that are associated with the access control program. If discrepancies or deficiencies are identified during this review, the inspector(s) should follow up as necessary.	NRC 02.08 レビュー a. 事象およびログ：過去 12 カ月または前回検査以降の事象報告およびセーフガード・ログの入力をレビューおよび評価する。 b. セキュリティ・プログラム・レビュー：規制要件にしたがってセキュリティ・プログラムのレビューを行っていることを確認する。 c. 問題の把握と解決：セキュリティ・プログラムに関する問題を適切な閾値で特定し、是正措置プログラムに記入し適切に解決していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容、考慮事項

				For the inspection of this requirement, the inspector(s) should review the documented results of the security program reviews or audits performed by the licensee to ensure the continued effectiveness of its security program. ...	
				<u>02.09 Specific License Requirements and Guidance</u> Requirements of 10 CFR 72 Subpart H and 10 CFR 73.51 are applicable for the physical protection of spent nuclear fuel (SNF) and power reactor-related GTCC waste stored under a specific ISFSI license issued pursuant to 10 CFR 72.40. Through verification of the inspection requirements within this IP, inspector(s) shall verify or determine that the licensee’s physical protection program is designed and implemented to meet the general performance objective of 10 CFR 73.51(b); specific requirements under 10 CFR 72.180, 72.182, 72.184, and 72.186 of Subpart H; and site-specific security orders (e.g., interim compensatory measures and additional security measures). Inspector(s) should note that ICMs and ASMs are two different documents that encompass the same requirements. Licensees who had an existing ISFSI prior to September 2007 were issued the ICMs and licensees who built an ISFSI after September 2007 were issued the ASMs. a. Verify that SNF and power reactor-related GTCC waste is stored only within a PA. (10 CFR 73.51(b)(2)(i)) and (10 CFR 73.51(d)(1)) <u>Specific Guidance</u> To inspect this requirement the inspector(s) should observe a sample of a few physical barriers (surrounding the PA to which access is controlled) that the licensee has established and installed to verify the integrity of the barriers (ability to perform their intended function) and that the barriers are designed and constructed of materials in accordance with 10 CFR 73.2, Definitions, “Physical Barriers.” For the PA perimeter barrier, the inspector(s) should take sample measurements of the barrier in any locations that appear to be less than the prescribed	NRC 02.09 特定の認可要件およびガイダンス a. SNF と発電炉関係 GTCC 廃棄物が PA 内のみに貯蔵されていることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 b. PA への入域を認められたものだけが PA にアクセスできることを確認する。 <u>具体的なガイダンス</u> 対象となる記録、確認内容 c. アクセス承認および指紋確認に関するサイト固有のセキュリティ命令を遵守していることを確認する。 <u>具体的なガイダンス</u> なし d. 隔離ゾーンへの侵入を検出および評価可能であることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 e. 必要な場合いつでも指定の対応部隊にタイムリーにコミュニケーションできることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 f. 物理的防護システムが、規定の線量を超える放射線被ばくを引き起こすのに十分な施設の制御喪失に対して防護できるように設計されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 g. 物理的防護計画のコピーを 3 年間または認可終了まで保持していることを確認する。 <u>具体的なガイダンス</u> なし h. 規制の性能目標を満たす物理的防護システム、機器および手順書の規定に準拠していることを確認する。

				height and verify that any opening in the barrier is secured and monitored in accordance with the regulation. If building walls comprise a portion of the PA barrier, the inspector(s) should verify that the building (barrier) height and material is in accordance with 10 CFR 73.2, Definitions, “Physical Barriers.” ...	<u>具体的なガイダンス</u> 対象となる関連文書、観察、確認内容 i. PA 内への無許可の侵入や PA 内での活動を適切に評価するのに十分な照明を提供していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 j. PA 周辺を常時監視し、隔離ゾーン（IZ）への侵入を検知できるアクティブな侵入警報システムで保護されていること、常時スタッフの配置された一次警報ステーションおよび常時スタッフの配置されたもう一つの場所で監視されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、観察、確認内容 k. 一次警報ステーションが PA 内にあり、耐弾性の壁、ドア、天井、床を備え、ステーションの内部が PA の外から見えないことを確認する。 <u>具体的なガイダンス</u> なし l. 全ての警報の評価を適時に実施することを確認する。冗長ロケーションは、警報発生を要約表示するだけでよい。 <u>具体的なガイダンス</u> なし m. PA が毎日のランダム巡回によって監視されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、観察、確認内容 n. セキュリティ組織が、検知システムの監視、評価、アクセス制御、通信を実施して適切な対応を確実にするために、シフトごとに十分な人員を確保する手順書を持っていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 o. 無許可の侵入や活動にタイムリーに対応できるよう、指定された対応部隊または LLEA との文書化された連絡関係を持っていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 p. 個人識別システムと、許可された個人のみにアクセスを制限する制御ロックシステムを備えて
--	--	--	--	---	---

					いることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 q. 現場のセキュリティ部隊メンバーと指定された対応部隊または LLEA 間の冗長通信機能を備えていることを確認する。 <u>具体的なガイダンス</u> 観察、確認内容 r. PA に入域する全ての人、車両、および手持ちの荷物が適切な許可を受けているかどうか確認され、入域前に爆発物がないか目視検査されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 s. PA への不正侵入または PA 内での活動に対処するために、対応手順書が確立され、維持されていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容 t. 全ての検出システムとサポート・サブシステムに、ライン監視機能付きの改ざん表示システムが含まれていることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、観察、確認内容 u. 不正な開示から情報を保護していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、質問、確認内容 v. 物理的保護プログラムが、その管理者と実施に直接責任を負う担当者の両方から独立した個人によって 24 か月ごとにレビューされていることを確認する。物理的保護プログラムのレビューには、物理的保護システムの有効性の評価と、指定された対応部隊または LLEA と確立された連絡の検証を含める必要がある。 <u>具体的なガイダンス</u> なし w. 記録作成後 3 年間または認可終了まで、対象文書を記録として保持していることを確認する。 <u>具体的なガイダンス</u> なし x. セキュリティ要件および/またはセキュリティ命令にしたがって、PA に入る車両の制御方策およびプロセスを実施していることを確認する。
--	--	--	--	--	---

					<u>具体的なガイダンス</u> 対象となる関連文書、確認内容 y. セキュリティ要件および/またはセキュリティ命令にしたがって、インサイダー緩和プログラムを実施していることを確認する。 <u>具体的なガイダンス</u> なし z. 物理的セキュリティ要件および/またはセキュリティ命令に該当する場合、LLEA とのオフサイト対応調整を策定していることを確認する。 <u>具体的なガイダンス</u> 対象となる関連文書、確認内容
	法令、基準等	—	—	—	個別ガイダンス内に記載
参考文献	—	Reference	• Interim Compensatory Measures (ICMs) for Dry Spent Fuel Storage, October 16, 2002. SLES Reference No. NS106674 • Additional Security Measures (ASMs) for the Physical Protection of Dry Independent Spent Fuel Storage Installations, September 28, 2007. SLES Reference No. NS106675 ...	—	
別紙・附属書	—	Appendix	—	—	
改訂情報	—	Revision History	Attachment 1: Revision History for IP 81311	—	

2.4 日英検査ガイド比較調査の結果

2.4.1 英国 ONR 検査ガイドの全体体系および図書構成の概要について

本年度実施した日英検査ガイドの比較調査では、仕様書に示されている原子力規制庁が用いる検査ガイド（セキュリティ関連）および英国 ONR の検査ガイド（セキュリティ関連）を踏まえて、原子力規制庁および ONR から発行されたセキュリティ規制検査と関連のある検査ガイド、およびセキュリティ規制検査の関連情報などを含めて調査を実施した。

英国 ONR 検査ガイドの全体体系は、基本的には安全関連とセキュリティ・安全保障関連に分けて構成されている。セキュリティ・安全保障関連検査ガイド図書には、主に上位図書（セキュリティ評価原則）と下位図書（詳細の各検査ガイド）で構成されている。具体的には、上位図書は、セキュリティ評価原則（SyAPs）である。下位図書には、核セキュリティ検査（CNS-INSP-GD-1.0）、核運搬セキュリティ（CNSS-SEC-GD-001）、安全保障検査（SG-INSP-GD-001）などのガイドがある。ONR のセキュリティ・安全保障関連検査ガイドの詳細は表 2.4.1-1 を参照する。以下に、主要なセキュリティ・安全保障関連検査ガイド全体体系のイメージを示す。

上位図書：

- ・セキュリティ評価原則（Security Assessment Principles, SyAPs）

下位図書：

- ・核セキュリティ検査（CNS-INSP-GD-1.0 - Nuclear security inspections）
- ・核運搬セキュリティ（CNSS-SEC-GD-001 - Nuclear Transport Security Guidance for Class B Approved Carriers）
- ・原子力産業セキュリティ規制（CNSS-SEC-GD-002 - Nuclear Industries Security Regulations 2003 (NISR): Guidance for Inspectors）
- ・安全保障検査（SG-INSP-GD-001 – Safeguards）など

英国 ONR の検査ガイドの図書構成には、ガイド別に多少の違いはあるものの、概して表紙、目次、本文、参考文献、用語・略語、付録、法令・基準、改訂情報などで構成されている。ガイドの内容としては、主に監督領域、序論、検査目的、検査要件、検査手順などの内容を記載しているほか、全ての検査ガイドに共通の留意事項（セキュリティ評価原則 SyAPs）、原子力産業セキュリティ規制（NISR）、セキュリティ計画（SP）、機微な原子力情報（SNI）などに関する事項）を記載している。また、各検査ガイドの中で、検査官向けに検査における注意点（考え方）またはアドバイスのような内容を多く盛り込んで

いる。この点においては、NRC の検査ガイドにない特徴の一つといえる。各ガイド本文の記載は、全体的に比較的シンプルで分かりやすい。ONR の検査ガイド（セキュリティ関連）図書構成の詳細は、表 2.4.2-1～表 2.4.2-11 を参照する。

表 2.4.1-1 ONR の検査ガイド（セキュリティ関連）

文書 ID	タイトル	調査対象
CNS-TAST-GD-1.1 (Issue 1)	Security Governance and Leadership	○
CNS-TAST-GD-1.2 (Issue 2.1)	Organizational Security Capability	
CNS-TAST-GD-1.3 (Issue 1)	Security Decision Making	
CNS-TAST-GD-1.4 (Issue 1)	Organizational Learning for Security	○
CNS-TAST-GD-1.5 (Issue 2)	Security Assurance Processes	
CNS-TAST-GD-2.1 (Issue 2)	Maintenance of a Robust Security Culture	○
CNS-TAST-GD-3.1 (Issue 3.1)	Identification and Analysis of Security Tasks and Roles	
CNS-TAST-GD-3.2 (Issue 3)	Sufficiency and Competence of Personnel Delivering Security	
CNS-TAST-GD-3.3 (Issue 3)	Workspaces, Equipment and User Interfaces	
CNS-TAST-GD-3.4 (Issue 3)	Procedures and Administrative Controls	
CNS-TAST-GD-4.1 (Issue 2)	Procurement and Intelligent Customer Capability	
CNS-TAST-GD-4.2 (Issue 2)	Supplier Capability	
CNS-TAST-GD-4.3 (Issue 2)	Oversight of Suppliers	
CNS-TAST-GD-4.4 (Issue 2)	Commissioning of security systems and infrastructure	
CNS-TAST-GD-5.1 (Issue 2)	Reliability and Resilience of the Security System	○
CNS-TAST-GD-5.2 (Issue 2)	Examination, Inspection, Maintenance and Testing of Physical Protection Systems	
CNS-TAST-GD-5.3 (Issue 2)	Sustainability of Nuclear Security Arrangements	
CNS-TAST-GD-6.1 (Issue 2)	Categorization for Theft	○
CNS-TAST-GD-6.2 (Issue 2)	Categorization for Sabotage	○
CNS-TAST-GD-6.4 (Issue 1.1)	Vulnerability Assessments	
CNS-TAST-GD-6.5 (Issue 1.1)	Adjacent or Enclave Nuclear Premises	
CNS-TAST-GD-6.6 (Issue 2)	Nuclear Construction Sites	

CNS-TAST-GD-6.7 (Issue 2)	Class A Carriers ? Transport Security Statements and Plans	
CNS-TAST-GD-7.1 (Issue 2)	Effective Cyber and Information Risk Management	
CNS-TAST-GD-7.2 (Issue 2.1)	Information Security	○
CNS-TAST-GD-7.4 (Issue 2)	Physical Protection of Information	○
CNSS-TAST-GD-7.5 (Issue 4)	Preparation for and Response to Cyber Security Events	○
CNS-TAST-GD-8.1 (Issue 2)	Cooperation of Departments with responsibility for delivering vetting and ongoing personnel security arrangements	
CNS-TAST-GD-8.2 (Issue 2)	Pre-employment Screening and National Security Vetting	
CNS-TAST-GD-8.3 (Issue 1.1)	Ongoing personnel security aftercare	
CNS-TAST-GD-9.1 (Issue 2)	Civil Nuclear Constabulary (CNC) Response Force	
CNS-TAST-GD-9.2 (Issue 2)	Local Police Operations Support to the Duty holder	
CNS-TAST-GD-9.3 (Issue 2)	Security Guard Services	
CNS-TAST-GD-10.1 (Issue 3)	Counter terrorism (CT) measures and emergency preparedness and response (EP&R) planning arrangements	
CNS-TAST-GD-10.2 (Issue 2.2)	Testing and exercising the security response	○
CNS-TAST-GD-10.3 (Issue 3)	Clarity of Command, Control and Communications Arrangements During and Post a Nuclear Security Event	
CNSS-TAST-GD-11.1 (Issue 1.2)	Guidance on the Security Assessment of Generic New Nuclear Reactor Designs	
CNS-TAST-GD-11.4.1 (Issue 1.1)	Secure by Design	
CNS-TAST-GD-11.4.2 (Issue 1)	The Threat	
CNS-TAST-GD-11.4.5 (Issue 1)	Functional Categorization and Classification of Security Structures, Systems and Components	
CNS-TAST-GD-11.4.6 (Issue 1.1)	Managing Changes to Security Standards, Procedures and Arrangements	
CNS-INSP-GD-001	Nuclear Security Inspections	追加 *仕様外

2.4.2 日英検査ガイド別の比較調査

2.4.2.1 CNS-TAST-GD-1.1 (Issue 1) 「Security Governance and Leadership」における調査の結果

原子力規制庁検査ガイドに対応するものがないため、ONR の検査ガイドの主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-1 にまとめた。

2.4.2.1.1 監督領域

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.1.2 序論

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（セキュリティ評価原則 SyAPs（基本セキュリティ原則 FSyPs 含む）、原子力産業セキュリティ規制（NISR）、セキュリティ計画（SP）、機微な原子力情報（SNI）などに関する事項）。

2.4.2.1.3 検査の目的

ONR の検査ガイドでは、検査ガイドの目的（検査官がガバナンスとリーダーシップの方策に関する評価を行う際の一般的な助言と情報を提供）について説明している。

2.4.2.1.4 検査要件及び検査手順

ONR の検査ガイドでは、次のように分けて説明している。

- ・ 検査官への助言（検査の背景、注目点、該当する SyAPs）
- ・ 規制上の期待事項（事業者に求められること、該当する FSyPs）
- ・ 以下、各検査項目について検査に必要な知識、それを踏まえた検査官の考慮事項（検査の視点）を詳細に説明。
 - ✓ 核セキュリティのガバナンスおよび監督
 - ✓ 核セキュリティのリーダーシップ

2.4.2.1.5 法令・基準等

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.1.6 改訂情報

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載

している。

表 2. 4. 2. 1 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-1.1 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		英国 ONR 検査ガイド		両者間の主な相違点
【ガイド】－ (－)		【ガイド】 CNS-TAST-GD-1.1 (Revision 1) Security Governance and Leadership (March 2020) (11 頁)		
項目	主な内容	項目	主な内容	(注) 原子力規制庁の対応する検査ガイドがないため、以下は、ONR 検査ガイドの記載概要を示す
図書全体構成	－	図書全体構成	表紙 目次 本文 参考文献 用語・略語 改訂情報	－
本文	監督領域	－	ガイド ID カテゴリー	CNS ONR ガイドの大分類 (CNS=核セキュリティ)
	－	－	1. Introduction	1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 1.2 The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide. ONR 1. 序論 1.1 ・ ONR はセキュリティ評価原則(SyAPs)を策定。事業者 (dutyholders) が適合を実証しなければならない基本的セキュリティ原則 (FSyPs) が含まれる。 ・ 事業者は原子力産業セキュリティ規制 (NISR) に従う。 1.2 ・ セキュリティ計画 (SP)は、サイトセキュリティ計画、一時的セキュリティ計画、輸送セキュリティ計画など全てを含む。 ・ 機微な原子力情報 (SNI) の防護に係るサイバーセキュリティ&情報保証 (CS&IA) 文書化の根拠も SyAPs を適用可能。 ・ 検査官が SyAPs への適合性判断をする場合、TAG 等のガイダンスを利用可能。

検査の目的	—	2. Purpose and Scope	2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder’s governance and leadership arrangements. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	ONR 2. 目的および範囲 ・本 TAG は、検査官がガバナンスとリーダーシップの方策に関する評価（規制判断）を行う際の一般的な助言と情報を提供
—	—	3. RELATIONSHIP TO RELEVANT LEGISLATION	3.1 The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ...	ONR 3. 規制との関係 ・本ガイドにおける事業者（dutyholder）の定義 ・NISR 要件の概要
—	—	4. RELATIONSHIP TO IAEA DOCUMENTATION AND GUIDANCE	4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides. ...	ONR 4. IAEA 文書との関係 ・規制の枠組みは、IAEA 核物質防護条約（CPPNM）、IAEA 核セキュリティ原則と整合 ・CPPNM 基本原則 F はセキュリティ文化に言及、ガバナンスとリーダーシップが重要と指摘。 ・より詳細なガイダンス：NSS 13
—	—	5. RELATIONSHIP TO NATIONAL POLICY DOCUMENTS	5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve SyDP 1.1 – Security Governance and Leadership, in support of FSyP 1 – Leadership and Management for Security. The TAG is consistent with other TAGs and associated guidance and policy documentation. ...	ONR 5. 国の政策文書との関係 ・セキュリティ政策枠組み（SPF）に、国の組織および第三者に対して国情報の取扱いに関する政府の期待事項を提示 ・SPF の成果および要件の詳細は SyAPs に記載 ・SNI のカテゴリーはクラス分類方針に基づく
検査要件および検査手順	—	6. Advice to Inspectors	6.1 Organizational and cultural shortcomings are identified consistently as the underlying causes of major accidents and events around the world. This applies to the nuclear industry and to other sectors regardless of the technology involved or the regulatory regime. The Organizational and cultural issues are often complex but a number of common factors have been identified from the event investigations	ONR 6. 検査官への助言 6.1 ・組織的、文化的不備は、世界で主要な事故・事象を引き起こしている 6.2

				and research studies. These include: ineffective leadership, inadequate management oversight and scrutiny of security; poor decision making and lack of effective challenge; and failure to apply lessons from experience. 6.2 Most nuclear regulators, including ONR, have recognised the need to consider Organizational and cultural factors as part of their regulatory activities. There is also recognition of the need for increased focus on Board/Director/Senior Management levels within Organizations due to their strong influence on culture and security. 6.3 As detailed above, the SyAPs incorporate an FSyP on Leadership and Management for Security (L&MfSy). L&MfSy embraces Organizational factors, drawing upon lessons from major accidents and events along with studies into the characteristics of high reliability Organizations. L&MfSy principles cover the broad areas of governance and leadership, capable Organization, decision making, learning and assurance processes. In the SyAPs document, for each of these principles there are further details on more specific factors relating to broad topic area. This guidance document is focused on governance and leadership. Regulatory Expectations 6.4 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies clear security governance arrangements, a commitment to maintaining security at all times and programmes that support strong security governance and leadership. FSyP 1 - Leadership and Management for Security / Organizational Learning / SyDP 1.4 Lessons should be learned from internal and external sources to continually improve leadership, Organizational capability, the management system, security decision making and security performance.	・規制活動の中で組織的・文化的要因を考慮することが必要（規制者の一般的な認識） ・とくに文化やセキュリティに強い影響を持つ役員会／責任者／上級管理者を重視する 6.3 ・SyAPs に「セキュリティのためのリーダーシップとマネジメント」に関する FSyP あり 規制上の期待事項 6.4 ・SP に明確なセキュリティ・ガバナンス方策や誓約事項を示していること FSyP 1：セキュリティのためのリーダーシップとマネジメント／組織的学習／SyDP 1.4 ・組織内外の教訓を学び、リーダーシップ、組織能力等を継続的に改善する
		—	7. Nuclear Security Governance and Oversight	7.1 The UK Corporate Governance Code published by the Financial Reporting Council in 2014 (Reference 9) defined corporate governance as: Corporate governance is the system by which companies are directed and controlled. Boards of directors are responsible for the governance of their companies. The shareholders' role in governance is to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place. The responsibilities of the board include setting the company's strategic aims, providing the leadership to put	ONR 7. 核セキュリティのガバナンスおよび監督 7.1 企業ガバナンスの定義（英国規格） ・企業が指示・コントロールされるシステム 7.2 英国規格の定義の改訂 ・依然としてクラシックな定義 7.3 ガバナンスの標準とグッドプラクティス ・英国規格（2018）および Wates 原則（2019）参

				them into effect, supervising the management of the business and reporting to shareholders on their stewardship. The board's actions are subject to laws, regulations and the shareholders in general meeting. 7.2 Whilst the UK Corporate Governance Code has more recently been significantly revised the above definition is still regarded as the classic definition of Corporate Governance. 7.3 The UK Corporate Governance Code published in July 2018 (Ref 10) together with the Wates Corporate Governance Principles for Large Private Companies published in December 2019 (Ref. 11) provide guidance to UK companies on the standards of governance expected in the UK and are widely regarded as relevant good practice in Corporate Governance. 7.4 Dutyholder boards should have clear roles and responsibilities, both collectively and individually. They should also be questioning and challenging and effective at holding the senior management to account. 7.5 It is essential that dutyholder boards treat security as an appropriate priority when providing strategic direction and leadership. In order to do this effectively, board members must have access to good quality, current security information regarding threats and risks in addition to any operational performance information generated by the Organization, including metrics. Furthermore, boards must have appropriate membership and competence (either through direct experience or readily accessed subject matter experts) to interpret the security information and use it to validate the efficacy of security programmes. Oversight 7.6 Effective oversight should be facilitated through structured, integrated and diverse means such as self-assessments at facility/department level, internal independent oversight or regulation, robust governance structure, external assessments or peer reviews. The level and rigour applied to this oversight should be implemented using a graded approach. 7.7 Sometimes, oversight of nuclear security is delegated (either explicitly or implicitly) to a dutyholder's security department. However, line management also have responsibilities and department managers should continually monitor and question security performance. Therefore it is beneficial for management to have oversight	照 7.4 役員会 ・役割と責任の明記 7.5 役員会でのセキュリティの扱い ・戦略的指示やリーダーシップを示す時、適切な優先事項である 監督 7.6 有効な監督 ・体系的、総合的、多様な手段を活用（例. 自己評価、内部規制、ガバナンス構造、外部評価） 7.7 セキュリティ部門とラインマネジメント ・監督権限がセキュリティ部門にされる場合でもラインマネジメントが責任を持つ 7.8 パフォーマンス指標活用上の注意 ・補足情報（例：問題の傾向、関連情報（スタッフの意見、調査／監査結果））も示す 7.9 自己評価活用上の注意 ・ラインマネジメントと独立した内部チャレンジ能力により補強すべき ・より詳細は、IOWG 作成の監督グッドプラクティスガイド参照 検査官の考慮事項 ✓ 役員会の役割と責任は明確か？ ✓ 戦略的な指示やリーダーシップの発揮時、セキュリティを優先事項としているか？ ✓ 役員会が、脅威やリスクについてカレントの良質なセキュリティ情報を受ける仕組みができているか？ ✓ 役員会には、セキュリティ情報に対する適切な資格条件と有効に評価・行動する能力があるか？ ✓ 監督は、段階的アプローチに基づき、体系的・総合的・多様な手段で実施されているか？ ✓ 情報収集は、多様なソース（例. パフォーマンス指標、スタッフ意見、事象調査、独立評価、自己評価）を利用しているか？ ✓ 独立の監督または内部規制機能があり、効率的
--	--	--	--	--	--

				of security as an integral part of their responsibilities. 7.8 Oversight is dependent on information and performance indicators may be adopted to assist in data collection. However, performance indicators are known to have limitations and, therefore, reports on performance should also include qualitative discussion of trends and issues, supplemented by other sources of information such as feedback from staff, event investigations and assessments/audits. 7.9 Self assessments can be valuable but should be supplemented by a robust internal challenge capability that is independent of the operational line management. Such independent oversight or internal regulation function should be adequately equipped with the skills and resources required to perform its role effectively. Furthermore, it should be valued and supported by senior management, even when it is conveying ‘bad news’. Further information is available in the Independent Oversight Good Practice Guide produced by the cross-industry Internal Oversight Working Group (IOWG) and Published on behalf of the Safety Directors Forum (SDF) (Reference 8). Inspectors should consider: ✓ Does the board have clearly defined roles and responsibilities? ✓ Is security treated as a priority when providing strategic direction and leadership? ✓ Are there mechanisms in place to ensure the board receive current, quality security information on threats and risks? ✓ Has the board got appropriate membership and competence to assess and act effectively on security information? ✓ Is oversight facilitated through structured, integrated and diverse means in line with the graded approach? ✓ Is data collected from a range of sources such as performance indicators, staff feedback, event investigations, independent and self-assessment? ✓ Is there an independent oversight or internal regulation function with the capability, capacity and authority to perform its role effectively?	な職務遂行のための能力、権限があるか？
			Nuclear Security Leadership	8.1 All dutyholders should develop a Nuclear Security Policy (NSyP). The NSyP should be clear, concise and focused on nuclear security. It is an essential document that influences	ONR 8. 核セキュリティのリーダーシップ 8.1 核セキュリティ方針 (NSyP)

				the behaviours, actions and decisions of the board, leaders and managers. Accordingly, its existence and purpose should be communicated and understood across the dutyholder’s managers, staff and contractors. In that regard, TAGs 4.2 and 4.3 provide additional information on management of the nuclear supply chain. They recommend that potential suppliers be subjected to a screening process designed to ensure that they have a positive security culture, which will enable adherence to the NSyP. 8.2 Security plans should reference the dutyholder’s management of the NSyP and commitment to maintain security at all times, ensuring that expectations are met in all situations (adhering to the values and expectations set out in the NSyP is particularly important in high pressure situations – although it is in these instances when there is greater risk of non-adherence). This will help in developing a culture throughout the Organization that is resistant to nuclear security being compromised for cost, programme or other reasons without due cause, consideration and governance. 8.3 Dutyholders should ensure that roles, accountabilities, standards and expectations of behaviour for nuclear security are clear, linked to the NSyP and apply to all from the board down. Communication is essential and the standards and expectations should form an integral part of induction and training programmes (including leadership selection/development and key contractors). 8.4 It is important that everyone adheres to the standards and expectations and therefore compliance should be monitored and reinforced. The lessons from major events world-wide show that inappropriate attitudes and behaviours at the highest levels of Organizations can undermine safety or security. Often, senior managers are involved in ‘look down’ monitoring but a top-level review is missing. Accordingly, dutyholders should demonstrate how assurance is sought that board members and senior/facility managers (in addition to front-line staff) are acting in accordance with the company’s standards and expectations. 8.5 Actions demonstrate commitment to nuclear security. The actions and decisions taken by senior management should demonstrate clearly their overriding commitment to maintaining nuclear security. Management should ensure	・明確&簡潔に ・サプライチェーンについては TAGs 4.2 および 4.3 参照 8.2 SP で NSyP に言及 ・SP で NSyP および誓約事項の管理に言及（高プレッシャー状況では NSyP の価値観と期待事項が特に重要） 8.3 核セキュリティに関する役割 ・核セキュリティに関する役割、責任、振る舞いの標準・期待事項が明確で、NSyP にリンクし、役員会以下全員に適用 8.4 標準と期待事項の遵守 ・すべての人の遵守が重要 ・最上位の人の影響大きい（世界の教訓） 8.5 行動と意思決定による実証 ・上級管理者は、行動と意思決定により原子力セキュリティ優先の誓約を明確に実証する ・報奨制度の活用と注意事項 8.6 コミュニケーション ・コミュニケーションとエンゲージメントは強力なリーダーシップ・ツール 8.7 スタッフのスキル・知識・経験 ・上級職の意思決定への情報源として、スタッフのスキル・知識・経験を尊重し活用する 8.8 マネジメントシステム ・優れたリーダーは、有効なマネジメントシステムを用いて前向きなセキュリティ文化と業務プロセスを構築する 8.9 マネジメントシステムを支える 4 原則 ・4 つの原則がある： ・原則 1 オーナーシップとリーダーシップ 上級管理者は、セキュリティを適切に優先しながら事業目的を達成するためにマネジメントシステムを所有・評価・使用している ・原則 2 統合的、重点的で最適化されている 上級管理者は、変化する事業の要求および課題
--	--	--	--	--	--

				that Organizational security arrangements are robust, seek effective solutions to nuclear security issues and set out key objectives and targets for improving nuclear security, with a strong and consistent emphasis on reducing risks. To support these aims, the management team should regularly visit work areas to observe conditions first hand, model and reinforce standards and expectations, and to interact with staff. They should also implement reward systems that promote the identification and management of risk, encourage positive security behaviours and discourage complacency. However, dutyholders should be careful when designing any reward system to avoid it introducing negative drivers and encouraging perverse behaviours. 8.6 Communication and engagement with staff can be a powerful leadership tool. Dutyholders should encourage frequent, face-to-face engagement between Board members, senior management and staff, recording the outcome and seeking improvement where it has been negative. Other interactions such as company news letters should routinely emphasise nuclear security and not be restricted solely to business issues. 8.7 The skills, knowledge and experience of staff should be respected and utilised to inform decision making at senior levels. Dutyholders should therefore also encourage a culture of engagement with staff such that they are genuinely consulted and involved about issues relating to security, rather than simply being informed about decisions that have been taken. 8.8 Good leaders use effective, efficient and dynamic management systems to engender strong, positive security cultures and work processes which drive continually improving security, safety and business performance and ensure on-going compliance with the law. Dutyholders should therefore implement an integrated management system that ensures security is considered in all their activities and is not confined to the quality management system. It also promotes a more consistent approach to treatment of other areas such as environment, safety, transport and safeguards, and other business activities, and reduces the likelihood of incompatible arrangements. 8.9 There are four principles that underpin effective, efficient and dynamic management systems: Principle 1 – Ownership and leadership	を理解し、それに応じたマネジメントシステムを構築する ・原則 3 有効なプロセス マネジメントシステムは、事業目的の達成を実現および支援するプロセスの階層で構成されている ・原則 4 目に見えてアクセス可能で使用する マネジメントシステムは、全ての職員が、その目的を理解し、適用部分を知り、手順書の意義や報告の重要性を理解し、関連情報に容易にアクセスできるように構成されている 検査官の考慮事項 ✓ 簡潔明瞭な NSyP が、遵守の誓約とともに、整備されているか？ ✓ 核セキュリティに関する役割、説明責任、振る舞いの基準・期待事項は明確で、NSyP と整合し、取締役会以下全員が適用対象か？ ✓ NSyP、基準・期待事項は、有効に伝達されているか？ ✓ 事業者は、役員会を含め、NSyP、基準・期待事項の遵守を強化し監視しているか？ ✓ 管理者は、核セキュリティを維持するコミットメントを明らかに実行しているか？ ✓ 事業者は、役員会、上級管理者チーム、スタッフ間の定期的な対面の交流を奨励しているか？（例：状況を直接観察し、基準・期待事項の模範を示し強化するための現場訪問） ✓ 不注意に逆向き要因を導入せずに核セキュリティを推進する業績管理システムが運用されているか？ ✓ スタッフは、上級職の意思決定にそのスキルや知識が活用されるように、ルーチンの相談され関与を求められているか？ ✓ 現在関連するグッドプラクティスを遵守する統合的なマネジメントシステムが使用されているか
--	--	--	--	--	--

				The senior management demonstrably own, value and use their management system to achieve their business aims whilst giving due priority to security: ✓ Through a shared leadership belief that an effective security culture must be underpinned by an effective and efficient management system. ✓ By advocating adherence to the management system. ✓ By ensuring that their management system continues to meet current national or international quality management system standards (e.g. as laid out in IAEA General Safety Requirements No GSR Part 2 (Leadership and Management for Safety)). ✓ Developing and deploying effective governance, internal challenge and independent assessment arrangements. Principle 2 – Integrated, focused and optimised, Senior management understand their changing business requirements and challenges, and proactively develop their management system accordingly. ✓ The scope of the management system covers all the dutyholder’s activities, from board to shop floor. It should also cover interfaces with external Organizations where this is important to security (e.g. supply chain or regulators) ✓ The extent and detail of management system controls is applied in a proportional manner depending upon risk and complexity of activities. ✓ The management system integrates all elements of management including security, health, environment, safety, quality, societal and economic elements such that security is never compromised. ✓ The senior management pursue vigorously all opportunities to improve the effectiveness and efficiency of the management system by: - o Setting and achieving objectives for continual improvement. - o Responding and learning from positive and negative events and situations both internally and externally. - o Establishing effective performance monitoring and feedback mechanisms. - o Encouraging everyone to contribute improvement suggestions. - o Critically reviewing performance. - o Championing improvements	
--	--	--	--	---	--

				Principle 3 – Effective processes The management system comprises a hierarchy of processes which deliver and support the achievement of business objectives. ✓ The needs of processes that directly achieve the business aims (e.g.: operations, decommissioning, manufacturing, project management, etc.) determine the scope and extent of support processes (e.g. security plans and design, supply chain management, technical and engineering support, assurance, etc.). ✓ Process ownership is assigned to suitable senior personnel who have the necessary support, resources and authority to consult, develop, deploy, monitor and improve the processes across all relevant functions. ✓ Personnel use and value the process arrangements, providing feedback for Improvement. Principle 4 – Visible, accessible and used The management system is structured such that all personnel: ✓ Understand the purpose of the management system. ✓ Know what it looks like, know what their role is and know what parts of the management system apply to them. ✓ Understand why it is important to comply with instructions and procedures, to report mistakes and make improvement suggestions. ✓ Can easily access the information relevant to their job. ✓ The level of detail is pitched at their level of task competency. Inspectors should consider: ✓ Is there a clear and concise NSyP in place together with commitment to adhere to it? ✓ Are roles, accountabilities, standards and expectations of behaviour for nuclear security clear, linked to the NSyP and apply to all from the board down? ✓ Are the NSyP, standards and expectations effectively communicated? ✓ Does the dutyholder reinforce and monitor compliance with the NSyP, standards and expectations from the board down? ✓ Does dutyholder management demonstrate clearly their commitment to maintaining nuclear security? ✓ Does the dutyholder encourage regular face-to-face engagement between the board, the senior management team and staff? (such as visits to work	
--	--	--	--	--	--

				areas to observe conditions first hand, model and reinforce standards and expectations) ✓ Is there a performance management system in place that promotes nuclear security without inadvertently introducing perverse drivers? ✓ Are staff routinely consulted and engaged on security issues such that their skills and knowledge are used to inform decision making at senior levels? ✓ Is there an integrated management system in place that adheres to current relevant good practice?	
参考文献	—	References	• Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 • IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011. www- pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. • •	—	
用語集	—	Glossary and Abbreviations	CPPNM : Convention on the Physical Protection of Nuclear Material CS&IA : Cyber Security and Information Assurance • •	—	
改訂情報	—	(表紙に記載)	Revision No., Date Issued, Review Date など	改訂 1 回、 次回見直し予定 (2025 年 3 月)	

2.4.2.2 PP1801「教育および訓練」と CNS-TAST-GD-1.4 (Issue 1)「Organizational Learning for Security」における調査の結果

原子力規制庁が用いる検査ガイド PP1801「教育および訓練」と、ONR の検査ガイド CNS-TAST-GD-1.4 (Issue 1)「Organizational Learning for Security」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-2 にまとめた。

2.4.2.2.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.2.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.2.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（教育および訓練状況の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官がガバナンスとリーダーシップの方策に関する評価を行う際の一般的な助言と情報を提供）について説明している。

2.4.2.2.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（核セキュリティの枠組み、規制上の期待事項、該当する FSyP など）を記載している。

2.4.2.2.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ワークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

- ・ 次の各検査項目について背景知識を提供（ポイントを含む解説）

- ✓ 運転に関する学習
- ✓ 運転経験（OpEx）
- ✓ 事象および悪影響のある状態の報告および追跡
- ✓ 重要度スクリーニング
- ✓ 調査および分析
- ✓ 是正処置の管理
- ✓ 情報の利用および伝達
- ・ 検査官の考慮事項（上記知識を踏まえた検査の視点）

2.4.2.2.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.2.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-2 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-1.4 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1801 教育および訓練 (2023/05/31 制定) (2 頁)			英国 ONR 検査ガイド 【ガイド】CNS-TAST-GD-1.4 (Revision 1) Organizational Learning for Security (March 2020) (13 頁)		両者間の主な相違点
項目		主な内容	項目	主な内容	
図書全体構成		本文 改訂情報	図書全体構成	表紙 目次 本文 参考文献 用語・略語 付録 改訂情報	—
本文	1. 監督領域	大分類および小分類：「核物質防護」 評価領域：「特定核燃料物質の管理」、「核物質 防護情報の管理」、「立入承認」、「出入管 理」、「物理的防護」、「情報システム防護」、 「核物質防護体制」 検査分野：「教育および訓練」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類 (CNS=核セキュリティ)
	—	—	1. Introduction	1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 1.2 The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論 (CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ)

	2. 検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される教育および訓練状況を確認する。当該事項は、法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、教育および訓練の検査分野における体制および警備員等の力量にも留意する。 2.2 防護措置の狙い 従業者に対し計画的な教育および訓練を実施することにより、必要な知識・能力（技術）等を継続的に維持していく。	2. Purpose and Scope	2.1 This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's Organizational learning arrangements. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（教育および訓練状況の確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官が組織的な学習の方策を評価する際の一般的な助言と情報を提供
	3. 検査要件	3.1 検査対象 核燃料物質防護に係る全ての業務に関連する従業者に対する教育計画、内容、実績、被教育者の理解度、現場確認等の全てが検査対象となり得るが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、核燃料物質防護に関する教育および訓練の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （1）検査の頻度 1 年間に 1 回程度 （2）検査時間 3 人／5. 2 5 （h） 3.3 実施体制 （1）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （2）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	6. Advice to Inspectors	6.1 An Organizational learning programme is an important process which enables a dutyholder to maintain and improve efficiency and enhance nuclear security. Furthermore, it is recognised by ONR as a key element of a nuclear industry that has a culture of continuous improvement and sustained excellence in operations. 6.2 Organizational Learning is more than just learning from individual events or learning for learning's sake – it is the engine which drives improvement and is relevant in all business areas and sectors, including nuclear safety. There are two important aspects: an ability to identify learning opportunities and (crucially), the commitment to take action. Both of these aspects are significantly influenced by the working environment and culture in any Organization or team. The culture is set by the leadership within the Organization: setting expectations, leading by example (by applying learning to their own behaviours and activities), driving learning activities, realising learning opportunities through managed change, and recognising and rewarding improvements. Regulatory Expectations 6.3 The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies a clear structure, framework and processes which supports Organizational learning. FSyP 1 - Leadership and Management for Security / Organizational Learning / SyDP 1.4 Lessons should be learned from internal and external sources to continually improve leadership, Organizational	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 ONR - 検査官への助言 ✓ 組織的学習プログラムの重要性 ✓ 組織的学習の意義 ✓ 規制上の期待事項 ➢ 事業者のセキュリティ計画が、組織学習をサポートする明確な構成と枠組みを示していること ✓ 基本セキュリティ原則（FSyP）1 - L&MfS : 組織的学習（セキュリティ実現原則（SyDP）1.4）

				capability, the management system, security decision making and security performance.	
	4. 検査手順	従業者に対し、その職務の内容に応じて核燃料物質防護のために必要な教育および訓練が行われていることを確認する。また、教育および訓練が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等により確認する。 4.1 検査前準備 教育および訓練に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する教育および訓練が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	7. Framework for Operational Learning	7.1 The diagram below shows a framework and essential components that support operational learning. ✓ Component One – Leadership and Cultural Aspects for Learning in Place Effective learning involves reviewing and changing processes and behaviours at all levels, starting with the Board and senior management. It is a fundamental requirement that an Organization must learn from its experience by senior management commitment. In the first instance this commitment takes the form of a policy statement which explains clearly the dutyholder’s commitment to the prevention of security events by applying lessons learned from previous operating experience, whether internal or external. This commitment should be underpinned by adequate resourcing of the function, management prioritisation of lessons identified and ongoing monitoring of action plans to ensure the issues which have been identified are addressed. ✓ Component Two – Diverse Sources of Learning Identified and Used .. ✓ Component Three – Learning Opportunities Realised Through Managed Change ..	NRA ・ 検査手順（概略） ✓ 確認事項 ✓ 文書、ウォークダウン、インタビューの活用 ✓ 検査前準備、検査、CAP 検査の趣旨 ONR ・ 検査手順の個別説明（以下 7～13 参照） ・ 7. 運転に関する学習 ✓ 組織的学習を支える仕組み（図） ➢ 要素 1. 学習のためのリーダーシップと文化の存在 ➢ 要素 2. 学習の多様な情報源の特定と利用 ➢ 要素 3. 管理された変更による学習機会の実現
			8. Operational Experience	8.1 OpEx is an important part of Organizational learning. The objective of OpEx is to proactively collect, document, organise, analyse and apply previous learning, whether it relates to equipment, personnel or procedures. Such learning extends from a number of sources, the	ONR ・ 8. 運転経験（OpEx） ✓ 組織的学習の中でも重要な部分 ✓ セキュリティ事象や悪影響を与える状態の情報をタイムリーに特定・収集するシステ

				dutyholder’s Organization, other operators, industry groups, governments and scientific and educational institutions. 8.2 Dutyholders should have a system that identifies and collects pertinent information on security events and adverse conditions in a timely manner. These include any deviation from the site’s security arrangements in the security plan or events that could have led to a security vulnerability developing. Adverse conditions include any deviation (e.g. a noticeable or marked departure from the expected norm), abnormality, equipment/human failure or non-conformity to procedure, and information, that relates to breakdowns or conditions that resulted in no serious consequences, but reduced the layers of defence. All personnel at the dutyholder’s site (staff, contractors, agency workers) should be expected to report all security events and adverse conditions. 8.3 To ensure the capture of all events and incidents which could affect security, the dutyholder should establish clear reporting criteria with low tolerability thresholds. The issues should be analysed in sufficient depth to facilitate the identification of root causes and action plans which can be implemented to address the issue. An effective learning Organization will share its experiences, both internally and externally. It is recognised that the sharing of learning from security events will need to be controlled especially where security vulnerabilities are identified. Nevertheless, there are a number of CPNI industry forums where this is possible.	ムの整備 ✓ 明確・適切な閾値の報告基準を確立し、セキュリティに影響する全ての事象・異常を把握
			9. Event and Adverse Condition Reporting and Tracking	9.1 The dutyholder should establish a process for all employees at the dutyholder site to identify security deficiencies, as well as improvement suggestions. A confidential means should be established for security staff to identify and track events and adverse conditions which might potentially identify an exploitable vulnerability in the security systems or processes. Managers should reinforce the requirement to report all events and adverse conditions that occur within the Organization constantly. All events and adverse conditions that affect security should be reported and tracked, including low-level events and “near misses”. 9.2 In addition to having processes and procedures to learn from security events in place, dutyholders have a legal obligation to report security events as required by the NISR	ONR ・ 9. 事象および悪影響のある状態の報告および追跡 ✓ サイトの全員がセキュリティの劣化や改善案を特定できるプロセスの確立 ✓ NISR の報告要件に該当するセキュリティ事象の報告実施

				2003 Regulations 10, 18 and 22. ONR therefore expects security events which meet reporting criteria specified in NISR and the ONR Guide on this matter [ONR-OPEX-GD-001 Revision 5] (Reference 9), to be reported as specified. This includes the findings from dutyholders investigations and Learning from Experience reports.	
			10. Screening for Significance	10.1 The dutyholder should screen event information to ensure all security significant matters are considered and that all applicable lessons learned are taken into account. The screening process should be used to select events for detailed investigation and analysis. A categorization system should be developed which grades events and conditions and prioritises them according to security significance and the identification of adverse trends.	ONR ・ 10. 重要度スクリーニング ✓ セキュリティ上重要な事項や教訓を全て考慮したスクリーニングの実施（詳細な調査・分析の対象を抽出）
			11. Investigation and Analysis	11.1 Dutyholders should have a policy and procedures specifying the type of investigation appropriate for an event of a particular category. The policy should typically outline the means of initiating an investigation, its duration, the composition of the investigating team, terms of reference for the investigation team and how it is to report. Investigations are to be performed promptly so that information and physical evidence is not lost or corrupted. Event participants should be interviewed while memories are fresh. A typical outline of the investigation process is at Appendix 1. 11.2 Highly significant events should be evaluated by a formally qualified multi-disciplinary evaluator team, using structured root cause investigation methods. The objective is to identify the root causes so that when they are corrected, the event or condition should not be repeated. Lower significance events or adverse conditions can be assessed with less formality and rigour. For example, individual expert evaluators can be used rather than a multi-disciplinary team. Notwithstanding an acknowledgement that repeat events are still possible, the objective should be to identify likely or apparent causes that, when corrected, would prevent recurrence. 11.3 The analysis of any event should be performed by an appropriate method. It is common practice that Organizations which conduct evaluations regularly use standard methods to achieve a consistent approach for the assessment of events. These standard methods usually involve different techniques and each of these may have its particular advantages for cause analysis, depending on the	ONR ・ 11. 調査および分析 ✓ 事象の分類に応じて調査の種類を特定する方針と手順書の整備 ✓ 特に重要な事象は、正式に認定された多分野の評価チームで根本原因を評価 ✓ 事象の評価には適切な手法を使用（標準的な手法が複数あり、夫々に長所がある）

				issue under investigation.	
			12. Corrective Action Management	12.1 Actions taken in response to events constitute the main basis of the process of feedback of operational experience to enhance security at dutyholders' sites. Such actions are aimed at correcting a situation, preventing a recurrence or improving the security arrangements. Corrective actions may also be identified to improve security management systems and culture, particularly where there is evidence of complacency. 12.2 Corrective actions should, as appropriate: ✓ Be specific and practical; ✓ Address fundamental causes and not symptoms; ✓ Include immediate actions which decrease the risk of a subsequent event or adverse condition; ✓ Include long term actions that should be taken to achieve a permanent solution; and, ✓ Focus on strengthening existing security arrangements, in preference to developing new ones. 12.3 Recurring events warrant special attention, such as increasing its significance level. The assessment of root causes should identify why previously-completed corrective actions failed to prevent a recurrence of the event. The reason for the original corrective action's ineffectiveness should be addressed as part of the follow up. 12.4 The dutyholder should ensure the dates assigned to complete each corrective action are commensurate with the importance of the action, Organizational priorities, and consideration of avoiding recurrence. Actions should be tracked and the responsible persons held accountable for completing them, according to agreed timescales.	ONR ・ 12. 是正処置の管理 ✓ 是正処置が運転経験反映プロセスの重要な基盤を構成 ✓ 是正処置の要点 ✓ 再発事象に対する対応 ✓ 是正処置の完了予定日に関する考慮
			13. Use and Dissemination of Information	13.1 Information on operational experience should be readily accessible to all security staff and - where appropriate - all employees. This can be done in a number of ways, such as team briefings. Effective use of the feedback from operational experience should be encouraged and reinforced by the management chain. Lessons identified should also be included in the dutyholder's refresher training material. 13.2 Where the event has resulted in a reportable event under NISR 2003 (as amended), a follow up report should be sent to ONR.	ONR ・ 13. 情報の利用および伝達 ✓ 運転経験情報は、セキュリティ・スタッフ全員と（適切な場合は）全従業員がアクセス可能 ✓ NISR の報告要件に該当する報告を ONR に提出 ・ 検査官の考慮事項 ✓ 事業者は、3つの必須要素を含めた組織的学習の仕組みを構築しているか？ ✓ セキュリティの劣化を体系的に特定および

				Inspectors should consider: ✓ Whether the dutyholder has a framework for Organizational learning that incorporates the three essential components. ✓ Whether the dutyholder has a policy for systematically identifying and correcting deficiencies in security. ✓ Whether the dutyholder’s security and safety OPEX policies are effectively aligned. ✓ Whether the dutyholder encourages staff to report security deficiencies and security improvement opportunities. ✓ Whether the dutyholder’s policies focus on corrective action rather than blame of personnel who report security deficiencies. ✓ Whether the dutyholder encourages a learning Organization through actively seeking lessons learned from other Organizations and, where appropriate, apply them to their Organization. ✓ Whether the dutyholder regularly debriefs staff on recent security issues that have occurred at the facility and draw on lessons identified to refresh staff understanding. ✓ Whether the dutyholder has sufficient training for staff and management to recognise and report problems and enough experienced staff trained in root cause analysis to assess all security deficiencies that are reported fully. ✓ Whether the dutyholder has adequate resources allocated to managing and reporting security deficiencies and whether they are compliant with legislation and the ONR mandated reporting process. ✓ Whether the dutyholder’s process informs their Board on the findings of identified security deficiencies including analysis of the event and emerging trends. ✓ Whether there are indicators regarding backlogs in event investigations and corrective action closure, looking particularly for adverse trends.	是正する方針が策定されているか？ ✓ 事業者のセキュリティと安全の OpEx 方針は有効に整合しているか？ ✓ 事業者は、スタッフにセキュリティの劣化や改善案の報告を奨励しているか？ ✓ 事業者の方針は、セキュリティの不備を報告した職員への非難でなく、是正措置に重点を置いているか？ ✓ 事業者は、他組織から積極的に教訓を学び、適切な場合は自組織に適用することを、学習する組織に奨励しているか？ ✓ 事業者は、その施設で最近生じたセキュリティ問題をスタッフに定期的に報告するとともに、スタッフの理解を新たにする教訓を見出そうとしているか？ ✓ 事業者は、スタッフと管理者に問題を把握および報告するための十分な訓練を施しており、根本原因分析の訓練を受けた経験豊富なスタッフを十分に有しているか？ ✓ 事業者は、セキュリティ劣化を管理・報告する十分な資源を割り当てているか、また、それは法令および ONR 要求の報告プロセスに適合しているか？ ✓ 事業者のプロセスは、事象の分析や新たな傾向を含め、特定されたセキュリティ劣化の知見を役員会に情報提供しているか？ ✓ 特に悪影響のある傾向について、事象調査や是正措置の終結の実施遅れに関する指標があるか？
法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3	3. Relationship to Relevant Legislation	3.1 The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR.	NRA ・適用法令 ONR ・規制との関係（CNS ガイド共通の記載、概要は	

		(6) 審査基準		It is also used to refer to those holding SNI. ・ ・	CNS-TAST-GD-1.1 の比較表参照) ✓ 「事業者」の定義 ✓ NISR 要件の概要
			4. Relationship to IAEA Documentation and Guidance	4.1 The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides. ・ ・	ONR ・ IAEA 文書との関係 (CNS ガイドほぼ共通の記載、検査対象のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照)
			5. Relationship to National Policy Documents	5.1 The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve SyDP 1.4 – Organizational Learning, in support of FSyP 1 – Leadership and Management for Security. The TAG is consistent with other TAGs and associated guidance and policy documentation. ・ ・	ONR ・ 国の政策文書との関係 (CNS ガイドほぼ共通の記載、FSyP/SyDP の原則番号のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照)
参考文献	—	—	References	・ Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 ・ IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. ・ ・	—
用語集	—	—	Glossary and Abbreviations	CPPNM : Convention on the Physical Protection of Nuclear Material CS&IA : Cyber Security and Information Assurance ・ ・	—
別紙・附属書	—	—	Appendix	Appendix 1 : Investigation of Events Appendix 2 : Analysis of Events	—
改訂情報	変更日、施行日、変更概要 (「制定」など)	(表紙に記載)	Revision No., Date Issued, Review Date など	改訂 1 回、 次回見直し予定 (2025 年 3 月)	

2.4.2.3 PP1802「定期的な評価および必要な改善」と CNS-TAST-GD-2.1 (Issue 2)

「Maintenance of a Robust Security Culture」における調査の結果

原子力規制庁が用いる検査ガイド PP1802「定期的な評価および必要な改善」と、ONR の検査ガイド CNS-TAST-GD-2.1 (Issue 2)「Maintenance of a Robust Security Culture」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-3 にまとめた。

2.4.2.3.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.3.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.3.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（定期的な評価と改善状況の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官が強固なセキュリティ文化の育成と維持に関する方策を評価する際の一般的な助言と情報を提供）について説明している。

2.4.2.3.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（例えば、核セキュリティの枠組み、規制上の期待事項、適用する基本セキュリティ原則（FSyP 2））を記載している。

2.4.2.3.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ウォークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて解説および検査官の考慮事項を示している。

- ・核セキュリティ文化の要素
 - 3つの主要な要素の解説
 - ONRにも規制活動の中で例示や改善への関与を通じて主導する責任がある
- ・原子力安全文化と核セキュリティ文化の関係および相違の解説
- ・企業／組織の役割
 - セキュリティ文化の解説
 - 検査官の考慮事項
- ・リーダーおよびマネージンの役割
 - セキュリティ文化への影響の解説
 - 検査官の考慮事項
- ・その他の職員の役割の解説
- ・その他の行動特性の解説
- ・保証とガバナンスの解説

2.4.2.3.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONRの検査ガイドでは、NISR要件の概要、IAEA文書との関係、国の政策文書との関係などを記載している。

2.4.2.3.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONRの検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-3 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-2.1 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1802 定期的な評価および必要な改善 (2023/05/31 制定) (2 頁)			英国 ONR 検査ガイド 【ガイド】CNS-TAST-GD-2.1 (Issue 2) Maintenance of a Robust Security Culture (March 2023) (182 頁)		両者間の主な相違点
項目		主な内容	項目	主な内容	
図書全体構成		本文 改訂情報	図書全体構成	表紙 目次 本文 参考文献 用語・略語 付録 改訂情報	—
本文	1. 監督領域	大分類および小分類：「核物質防護」 評価領域：「特定核燃料物質の管理」、「核物質 防護情報の管理」、「立入承認」、「出入管 理」、「物理的防護」、「情報システム防護」、 「核物質防護体制」 検査分野：「定期的な評価および必要な改善」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 1.2 The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNSS-TAST-GD-1.1 の比較表参照）

	2. 検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される定期的な評価、必要な改善状況を確認する。当該事項は、法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、定期的な評価、必要な改善の検査分野における体制、訓練・教育および設備の保全のほか、警備員等の力量にも留意する。 2.2 防護措置の狙い 核物質防護のために必要な措置についての定期的な評価と必要な改善により、防護措置を常に最適な状態に保ち、核物質防護に影響を及ぼす問題が特定された場合に適切に対応する。	2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's arrangements to develop and maintain a strong security culture. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the detail or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（定期的な評価と改善状況の確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官が強固なセキュリティ文化の育成と維持に関する方策を評価する際の一般的な助言と情報を提供
	検査要件	3.1 検査対象 核物質防護に関する定期的な評価および必要な改善の全てが検査対象となり得るが、本検査では、定期的な評価および必要な改善に関する事項の中か？ら、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、核物質防護に関する定期的な評価および必要な改善の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 １年間に１回程度 （２）検査時間 ３人／５．２５（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	6. Advice to Inspectors	14. A dutyholder's nuclear security regime takes into account a range of elements and activities. These include the requirements of regulation, consideration of the threat to Nuclear Material (NM) and Other Radioactive Material (ORM), associated locations/facilities, administrative systems, technical hardware systems, response capabilities and mitigation activities. No single government or industry Organization can address all these elements in isolation and an effective nuclear security culture is dependent on proper planning, training, awareness, operation and maintenance, as well as on the people who plan, operate and maintain nuclear security systems. 15. Even a well-designed security system can be degraded if procedures in place to operate and maintain it are inadequate, or if a dutyholder fails to follow sound procedures. Therefore, a dutyholder's nuclear security regime is dependent on the staff involved and their management, and it is the human factor, including management and leadership, that should be addressed in any effort to enhance existing nuclear security culture. Regulatory Expectation 16. The regulatory expectation placed upon the dutyholder is that they will ensure that the security plan identifies appropriate measures and a clear commitment to support a strong security culture throughout the Organization,	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 ONR - 検査官への助言 ✓ 核セキュリティの枠組み ✓ セキュリティシステムの設計が良くても、手順書の不備や遵守が不十分では劣化する ✓ 規制上の期待事項 ✓ 基本セキュリティ原則（FSyP）2－組織文化：強固なセキュリティ文化の維持（セキュリティ実現原則（SyDP）2.1）

				recognising the importance it has in maintaining an effective nuclear security regime. FSyP 2 - Organizational Culture / Maintenance of a Robust Security Culture / SyDP 2.1 Dutyholders should ensure that the Board gives due priority to the development and maintenance of a security culture necessary to ensure the entire Organization recognises that a credible threat exists, nuclear security is important and the role of the individual in maintaining it is key.	
	検査手順	核物質防護のために必要な措置について、定期的に評価し必要な改善を行っていることを関連文書の調査、ワークダウン、インタビュー等によって確認する。また、定期的な評価および必要な改善に関する活動の有効性の評価が定期的に行われていることを確認する。 4.1 検査前準備 定期的な評価および必要な改善に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する定期的な評価および必要な改善が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴か？らサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	7. Components of Nuclear Security Culture	17. Nuclear security culture in the UK has three major components. The first concerns the policy that the government requires to be in place given national and international contexts and how this policy is adopted by the dutyholder. The second is the Organization introduced by a dutyholder to apply government policy in this area and the subsequent management of that Organization. The third component concerns the attitude of individuals at all levels in an Organization towards implementing this policy and making it an integral part of their work and responsibilities. 18. ONR also has a responsibility to lead by example and engage with a dutyholder regarding any improvement that may be needed in a site's nuclear security culture when necessary, using appropriate regulatory interventions.	NRA ・検査手順（概略） ✓ 確認事項 ✓ 文書、ワークダウン、インタビューの活用 ✓ 検査前準備、検査、CAP 検査の趣旨 ONR ・検査手順の個別説明（以下 7～13 参照） ・7. 核セキュリティ文化の要素 ✓ 3つの主要な要素 ➢ 方針 ➢ 組織 ➢ 全員の振る舞い ✓ ONR にも規制活動の中で例示や改善への関与を通じて主導する責任がある
			8. Relationship and Differences Between Nuclear Safety Culture and Nuclear Security Culture	19. Nuclear Safety and Security culture are defined as: • Nuclear Safety Culture. ‘That assembly of characteristics and attitudes in Organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance’. • Nuclear Security Culture. ‘The assembly of characteristics, attitudes and behaviour of individuals, Organizations and institutions which serve as a means to support and enhance nuclear security’. 20. Nuclear safety primarily considers the risk of inadvertent human error and to a lesser extent deliberate acts that could cause harm, which are referenced in ONR's Safety Assessment Principles for Nuclear Facilities (Reference 10). In contrast, nuclear security places more emphasis on the mitigation of malicious actions relating to the theft and sabotage of NM and ORM and to a lesser extent on performance failings or inadvertent human error. 21. For a safety culture, great emphasis is placed on sharing	ONR ・8. 原子力安全文化と核セキュリティ文化の関係および相違 ✓ それぞれの文化の簡単な定義 ✓ 原子力安全はヒューマンエラーや意図的行動により生じるリスクに着目、核セキュリティは盗取やサボタージュ関連の悪意ある行動の緩和に焦点。 ✓ 安全文化では情報のオープンな共有を強調、セキュリティ文化では脅威への迅速な対応と「知る必要」に基づくコミュニケーション制限が重要 ✓ 安全文化とセキュリティ文化で要求される行動が異なる場合（例：情報の機密保持、悪意行動の阻止）と矛盾の迅速な特定 ✓ 良いセキュリティ文化には誓約、リーダーシップ、他の人の関与が必要（詳細は 9～11 参照）

				information openly, because of an overriding concern for transparency and dialogue wherever possible. A strong security culture places responsibility on a dutyholder to respond immediately to confirmed or perceived threats/incidents and to restrict associated communication to authorised persons on a strict ‘need-to-know’ basis. That does not necessarily preclude the sharing of suitably expurgated case histories where there is value in doing so. Although there is a difference in approach in some areas, both safety and security cultures need to coexist and should wherever possible reinforce the goals of each, because they share a common objective of limiting the risk resulting from non-malicious and malicious acts associated with NM, ORM (including transport) and associated facilities. This objective is founded largely on similar principles. For example, adopting a questioning attitude, rigorous and prudent adherence to procedures and effective communication. 22. It should be noted that a security culture will require some different attitudes and behaviour, compared with a safety culture, such as, when appropriate, the confidentiality of information and the approach taken to deter, detect, delay and respond to malicious capabilities. On occasions when there are differences between safety and security needs, any conflict should be identified by a dutyholder as soon as possible without undermining either discipline. 23. A good security culture requires commitment at an Organizational level, leadership from managers, and the engagement of other personnel as detailed in Sections 9, 10 and 11 of this document. Strong security culture indicators could be demonstrated by: all workers understanding that a credible threat exists, understanding their personal responsibilities for security, and through the adoption of security practices as normal behaviour.	
			9. The Role of a Company / Organization	24. Introduction. An important aspect of a good security culture is the role of a company/ Organization in developing and maintaining systems to ensure that effectiveness of an appropriate nuclear security regime on a site is a high priority for staff. The following paragraphs cover various topics that should be considered when assessing on the adequacy of a security culture.	ONR ・ 9. 企業／組織の役割 ✓ 良いセキュリティ文化にとって仕組みを構築・維持する企業／組織の役割が重要 ✓ 核セキュリティ方針 ✓ マネジメントの構造と仕組み ✓ リソース ✓ 見直しと改善

				25. Nuclear Security Policy. A risk driven security programme which takes due consideration of proportionality is a key element of an adequate security culture. It follows that a dutyholder's security plan should contain the nuclear security policy statement that declares a sound commitment to quality and high performance in all nuclear security activities and makes it clear that security has a high priority, potentially overriding operational demands where necessary. If there is any conflict regarding the relative priorities of safety, security or operations, senior management should be authorised to resolve the conflict taking into account the overall impact of the risk. This policy underpins the management systems that are an integral part of a company/Organization's security culture and it should be communicated to, and understood by, everyone affected. Nuclear security policy statements may vary in both form and content depending on a site's function, complexity and operational needs. An operating company/Organization has full responsibility for nuclear security in all the activities under its control and its nuclear security policy statement, endorsed by the company/Organization's Board (or equivalent), and should be clear and available to all staff. 26. Management Structure and Systems. An appropriate, independent governance regime, led by the Board, should exist to ensure that an adequate nuclear security culture is in place and maintained by the use of appropriate management systems/ structures. A primary requirement should be setting out the security expectations and standards that need to be met, which should be communicated to all staff. In this context, the dutyholder should define the roles, responsibilities and accountability for each level within the company/Organization and ensure all staff are accountable for complying with all aspects of the site's nuclear security regime, as detailed in the security plan. In addition, management should appoint an individual who is responsible for nuclear security, with sufficient authority, autonomy and resources to implement and oversee all nuclear security activities. There should also be sufficient resilience to ensure continuity. Where appropriate, management should also establish procedures to facilitate the timely resolution of any	✓ 検査官の考慮事項 ➤ 事業者は、核セキュリティ活動の品質とハイパフォーマンスへの誓約を含むセキュリティ方針を有しているか？ ➤ 組織の全レベルの職員に方針が伝えられ理解されることを保証するメカニズムが整備されているか？ ➤ 強固な核セキュリティ文化が確立され、マネジメントシステムによってサポートされることを保証するための、役員会主導の適切で独立したガバナンスの仕組みがあるか？ ➤ セキュリティの期待事項と基準が明確に定められており、それが全スタッフに伝達され理解されることを保証するメカニズムが整備されているか？ ➤ 全核セキュリティ活動を実施・監督するのに十分な権限、自律性、リソースを持つ、核セキュリティの責任者が任命されているか？ ➤ 安全、セキュリティ、環境、および運転間の矛盾をタイムリーに特定・解決するための手順書は整備されているか？ ➤ セキュリティの責任を履行するために十分な資金、技術、および人的リソースが割り当てられているか？ ➤ セキュリティ職員は、その役割を果たすのに必要なスキル、経験、資格を持っているか？ ➤ 組織の全レベルでセキュリティのパフォーマンスが監視されているか？ ➤ 教訓を考慮したセキュリティ・プラクティスについて定期レビューが行われているか？
--	--	--	--	---	---

				conflict between nuclear and radiological safety, security and operations. Management systems should also be in place for each security function to define expectations, determine trustworthiness, implement and maintain processes, measure progress, assess compliance, improve performance through learning from experience, and manage change. 27. Resources. The company/Organization should allocate sufficient financial, technical and human resources to implement assigned security responsibilities. It should also ensure that all security personnel have the necessary qualifications and that these qualifications are maintained by an appropriate training and development programme. Personnel should also have the necessary equipment, adequate work areas, up to date information and other support to effectively discharge their security responsibilities. 28. Review and Improvement. As part of an adequate security culture, a dutyholder's security plan should cover the requirement for security performance to be monitored at all levels in the company/Organization from Board level to delivery. This should include ensuring that learning and performance processes for security are in place, and that these are subject to continued improvement, where appropriate. Regular reviews of nuclear security practices should also be conducted taking into account lessons learned from both internal and external reviews, security exercises or incidents, and any relevant changes in the threat. In particular, a dutyholder should ensure that any weakness that relates to nuclear security is comprehensively analysed and expeditiously corrected. As appropriate, experience should be shared with other Organizations in the civil nuclear sector, and with ONR. The aim should be to establish an expeditious means of communicating security related information, including learning from experience, and maintain close cooperation with others for the exchange of intelligence and data that could impact on the security of NM/ORM (including transport), associated facilities and SNI. Inspectors should consider: ✓ Does the dutyholder have a security policy that incorporates a commitment to quality and high performance in all nuclear security activities?	
--	--	--	--	---	--

				✓ Are there mechanisms in place to ensure that the policy is communicated to, and understood by personnel at all levels of the Organization? ✓ Is there an appropriate, independent governance regime, led by the Board, to ensure that a robust nuclear security culture is in place and supported by management systems and structures? ✓ Are security expectations and standards clearly set out and mechanisms in place to ensure they are communicated and understood by all staff? ✓ Is there an individual appointed responsible for nuclear security, who has sufficient authority, autonomy and resources to implement and oversee all nuclear security activities? ✓ Are there procedures in place to facilitate timely identification and resolution of conflict between safety, security, environment and operations? ✓ Is there sufficient allocation of financial, technical and human resources to implement security responsibilities? ✓ Do security personnel have the necessary skills, experience and qualifications to perform their role? ✓ Is security performance monitored across all levels of the Organization? ✓ Are there regular reviews of security practices that take into account any lessons learned?	
			10. The Role of Leaders and Managers	29. Introduction. The human factor is generally a contributor to all nuclear security related activities and incidents. Therefore, leadership and management are vital components in dealing with malicious capabilities, unintentional personnel errors, inadequate Organizational procedures/processes and management failures. The following paragraphs cover various topics concerning the role of leaders and managers that should be considered when assessing the adequacy of a security culture. 30. Influencing Security Culture. A dutyholder's leaders, including Board members (or equivalent) and managers, can influence security culture throughout a company/Organization by their leadership, example and management practices. With sustained effort, and by employing the incentives and disincentives at their disposal, they should establish appropriate patterns of behaviour and even alter the physical environment where	ONR ・ 10. リーダーおよびマネージンの役割 ✓ ヒューマンファクターは一般に核セキュリティ関連の活動および事象に関わる ✓ セキュリティ文化への影響 ✓ 意思決定 ✓ 訓練および育成 ✓ モチベーション ✓ 事象報告 ✓ パフォーマンスの改善 ✓ 検査官の考慮事項 ➤ 役員会メンバーを含むリーダーは、行動（模範を示す）とマネジメント慣行を通じて核セキュリティへの誓約を実証しているか？ ➤ 組織は、適切な行動パターンを確立するために適切なインセンティブおよびディスインセンティブを採用し

				necessary, to facilitate a satisfactory security culture. Normally, leaders and senior managers are responsible for defining and revising policies and security objectives, while operational managers are responsible for initiating practices to comply with these objectives. Through their behaviour, leaders and managers should demonstrate their commitment to nuclear security and, in so doing, play an important role in promoting security culture. Leaders and managers should also foster an effective nuclear security culture by ensuring people understand that a credible threat exists and that effective and proportionate nuclear security is of vital importance in countering it. 31. Decision Making. Another task for leaders and managers is to carefully consider the views of others and to establish a formal decision-making mechanism that is well understood and involves all staff (see Appendix 1, paragraph 2 b (iii)). The quality of a decision is improved when the individuals involved are able to contribute their knowledge and ideas and take ‘ownership’ for addressing a problem or implementing the solution. All personnel should be made aware of, and be committed to, nuclear security requirements and best practices. Security technology should be appropriately used and maintained, and security regulations and procedures properly implemented. Leaders and managers should ensure that the skills and authorisations required to perform tasks relating to nuclear security are in place. Leaders and managers should also maintain effective communications with other companies/Organizations to consider, as appropriate, the requirements for protecting NM/ORM (including transport), associated facilities and SNI. 32. Training and Development. Training and professional development are essential in supporting the expected cultural behaviour. At all levels of an Organization, managers should ensure training is conducted to develop skills and provide tools to promote and implement a strong security culture. Managers should ensure that temporary and permanent staff; including contractors and service providers, understand the importance of protecting NM/ORM (including transport), associated facilities and SNI. 33. Motivation. All leaders, managers and other staff should	ているか？ ➤ リーダーおよびマネージャは、全スタッフが、信用できる脅威が存在し、それに対抗するには効果的で比例的なセキュリティが不可欠であることを理解できるようにしているか？ ➤ リーダーおよびマネージャは、全スタッフが十分に理解し関与する正式な意思決定メカニズムの中で、他の人の意見を慎重に検討しているか？ ➤ リーダーおよびマネージャは、組織の全レベルで訓練が実施され、強力なセキュリティ文化を推進し実施するためのスキルの開発とツールの提供を保証しているか？ ➤ リーダーおよびマネージャは、核セキュリティに影響をする可能性のある事象や問題を報告することを職員に奨励しているか？ ➤ 組織は、核セキュリティ文化の継続的な改善を追求し、自己満足を防ぐように設計されたプログラムを採用しているか？
--	--	--	--	--	--

				understand the specific threats to security that they face and their part (appropriate to their role/responsibilities) in managing and mitigating the risks. Leaders and managers have a key role in ensuring staff are appropriately motivated and their role in enhancing nuclear security is recognised and valued. Performance management tools can encourage vigilance, questioning attitudes and personal accountability. Maintaining and improving nuclear security culture needs persistent effort, frequent monitoring and leaders and managers have a responsibility to ensure that appropriate behaviour is reinforced through constructive feedback. They should also serve as positive role models through their attention and adherence to nuclear security practices. 34. Reporting of Events and Matters. As part of a good security culture, leaders and managers should encourage personnel to report any event or matter that could affect nuclear security. Whilst this is a legal requirement in accordance with NISR 2003, Regulations 10, 18 and 22, it also enables dutyholders to monitor trends and address any systemic problems. There should be a well-publicised process in place for reporting which should be reviewed from time to time as considered appropriate by the dutyholder. Part of the review should focus on the need to maintain a reporting system that is effective, whilst being simple to use. 35. Improving Performance. Leaders and managers should seek continual improvement in nuclear security culture and work to prevent complacency from compromising overall security objectives. They should consider all sources of relevant experience, research, technical developments, operational data, and events of security significance, which should be carefully evaluated and used to enhance nuclear security culture as appropriate. For example, leaders and managers should: • Ensure that experience and events that affect security, including those from other locations, are analysed and appropriate improvements or corrective actions are implemented; • Conduct self-assessments and arrange for independent audits of the management systems for which they are responsible in order to identify and correct weaknesses; • Establish a programme of exercises to test the	
--	--	--	--	--	--

				performance of security systems and associated human factors such as assessment and response; • Analyse patterns and trends arising from known deficiencies and implement corrections; • Observe operational performance to confirm objectives are being met; • Periodically review training programmes, staff nomination and authorisation procedures, working methods, management systems and staff access processes to sensitive locations, such as Vital Areas (VAs) and to SNI; and, • Maintain an awareness of the need for appropriate security procedures, processes and equipment, so staff have the appropriate tools with which to implement security effectively. Inspectors should consider: • Do leaders, including Board members, demonstrate their commitment to nuclear security through their behaviours (leading by example) and management practices? • Does the Organization employ appropriate incentives and disincentives to establish appropriate patterns of behaviour? • Do leaders and managers ensure that all staff understand that a credible threat exists and that effective and proportionate security is essential in countering it? • Do leaders and managers carefully consider the views of others within a formal decision-making mechanism that is well-understood and involves all staff? • Do leaders and managers ensure that training is conducted across all levels of the Organization to develop skills and provide tools to promote and implement a strong security culture? • Do leaders and managers encourage personnel to report any event or matter that could affect nuclear security? • Does the Organization seek continual improvement in nuclear security culture and employ programmes designed to prevent complacency?	
			11. The Role of Other Personnels	36. Introduction. A key aspect in achieving and maintaining an adequate security culture is engaging with personnel throughout an Organization. An individual understanding of, and commitment to, security management, roles and responsibilities and a	ONR • 11. その他の職員の役割 ✓ セキュリティ文化の達成・維持にとって は、組織全体の職員の関与が重要 ✓ 説明責任

				commitment to continuous security improvement are all important in achieving an effective nuclear security culture, which should be included, where appropriate, in approved security plans. The following paragraphs cover various topics concerning the role of non-security personnel that should be considered during an assessment on the adequacy of security culture. 37. Accountability. For a satisfactory security culture, all personnel should be accountable for their behaviour and should be properly motivated to assist in ensuring effective nuclear security. Personnel should also be expected to conduct themselves in a manner that recognizes the circumstances and potential consequences of their behaviour. Therefore, they should adopt a rigorous and prudent approach to their security responsibilities, with continuous regard for the security of protecting NM/ORM (including transport), associated facilities and SNI. 38. Compliance with Regulations and Procedures. Another indication that an adequate nuclear security culture exists is the level of compliance with regulations and associated instructions/procedures, and where constant vigilance and a proactive questioning attitude is evident. All personnel should recognize the importance of protecting SNI as part of an effective nuclear security culture, as well as not sharing site access badges and they should also understand the need to avoid divulging any information that has the potential to undermine security. Whilst staff feedback on procedures and processes should be encouraged, it should not undermine culture or constitute an unauthorized workaround that may compromise compliance. 39. Teamwork and Cooperation. An adequate nuclear security culture also depends upon teamwork and cooperation among all staff involved in security, which will extend beyond the security team itself. Personnel should therefore understand how their particular roles and relationships contribute to maintaining security. Inspectors should consider: • Are all personnel accountable for their behaviour and motivated to assist in ensuring effective nuclear security? • Is there evidence of a culture of compliance with regulations, associated instructions and procedures?	✓ 規制および手順書の遵守 ✓ チームワークと協力 ✓ 検査官の考慮事項 ➤ 全職員が自分の行為に説明責任を持ち、効果的な核セキュリティの確保に協力する意欲を持っているか？ ➤ 規制、関連する指示書・手順書を遵守する文化の証拠があるか？ ➤ 職員は自分の特定の役割がセキュリティの維持にどのように貢献するか理解しているか？
--	--	--	--	---	--

				Do personnel understand how their particular role contributes to maintaining security?	
			12. Other behavioural Characteristics	40. A satisfactory nuclear security culture has certain behavioural characteristics common amongst leaders, managers and other personnel, which lead to more effective nuclear security. For most of these characteristics there are performance indicators that provide a means of evaluating and assessing whether a nuclear security culture is adequate and these are detailed in Appendix 1 to this guidance.	ONR 12. その他の行動特性 - 十分なセキュリティ文化に共通するリーダー、マネージャ、その他職員の行動特性 - 多くの特性についてパフォーマンス指標がある。(核セキュリティ文化の妥当性を判断するための基準は、付録 1 参照)
			13. Assurance And Governance	41. As part of developing and maintaining a nuclear security culture, the methods used by a company/organization should be subject to an internal assurance and governance process by Suitably Qualified and Experienced (SQEP) security and operational staff. This is to ensure that the security culture in place is considered appropriate, effective and proportionate. The extent of this process may vary, taking into account site specific considerations. However, it is important that the Board member (or equivalent) with Board responsibility for security is aware of all aspects of the nuclear security culture and has endorsed the approach used for its development and maintenance.	ONR 12. 保証とガバナンス - 核セキュリティ文化の育成・維持の一環として、企業／組織が使用する手法は、SQEP セキュリティ・運転スタッフによる内部の保証・ガバナンスプロセスの対象とすべき (注) SQEP = Suitably Qualified and Experienced (適切な資格と経験を有する)
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant Legislation	4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ・ ・	NRA - 適用法令 ONR - 規制との関係 (CNS ガイド共通の記載) 「事業者」の定義 - NISR 要件の概要
			4. Relationship to IAEA Documentation and Guidance	6. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides. ・ ・	ONR IAEA 文書との関係 (CNS ガイドほぼ共通の記載、検査対象のみ相違、概要は CNSS-TAST-GD-1.1 の比較表参照)
			5. Relationship to National Policy Documents	10. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Security Delivery	ONR 国の政策文書との関係 (CNS ガイドほぼ共通の記載、FSyP/SyDP の原則番号のみ相違、概要は CNSS-TAST-GD-1.1 の比較表参照)

				Principle (SyDP) 2.1 – Maintenance of a Robust Security Culture, in support of FSyP 2 – Organizational Culture. The TAG is consistent with other TAGs and associated guidance and policy documentation. ・ ・	
参考文献	—	References	・ Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 ・ IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. ・ ・	—	
用語集	—	Glossary and Abbreviations	CPPNM : Convention on the Physical Protection of Nuclear Material CS&IA : Cyber Security and Information Assurance ・ ・	—	
別紙・附属書	—	Appendix	Appendix 1 : Characteristics of an Effective Nuclear Security Culture	ONR ・ 有効な核セキュリティ文化の特性 (核セキュリティ文化の妥当性の判断基準)	
改訂情報	変更日、施行日、変更概要（「制定」）	（表紙に記載）	Revision / Issue No., Date など		

2.4.2.4 PP1704「法令遵守および核セキュリティ文化醸成の体制」と CNS-TAST-GD-5.1 (Issue 2)「Reliability and Resilience of the Security System」における調査の結果

原子力規制庁が用いる検査ガイド PP1704「法令遵守および核セキュリティ文化醸成の体制」と、ONR の検査ガイド CNS-TAST-GD-5.1 (Issue 2)「Reliability and Resilience of the Security System」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-4 にまとめた。

2.4.2.4.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.4.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.4.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（法令遵守および核セキュリティ文化醸成の体制の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官が、セキュリティシステムについて、適切なレベルの信頼性とレジリエンス有することを評価する際の一般的な助言と情報を提供する）について説明している。

2.4.2.4.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（セキュリティシステムの重要な点、規制上の期待事項、該当する FSyP など）を記載している。

2.4.2.4.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ウォークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

- ・ システム・レジリエンスの要素の解説
- ・ 適切に資格認定された経験豊富な職員の解説
- ・ 必須サービスとセキュリティシステムの解説
- ・ 検査官の考慮事項

2.4.2.4.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.4.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-4 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-5.1 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1704 法令遵守および核セキュリティ文化醸成の体制 (2023/05/31 記載の適正化) (2 頁)		英国 ONR 検査ガイド 【ガイド】CNS-TAST-GD-5.1 (Issue 2) Reliability and Resilience of the Security System (March 2023) (13 頁)		両者間の主な相違点
項目	主な内容	項目	主な内容	
図書全体構成	本文 改訂情報	図書全体構成	表紙 目次 本文 参考文献 用語・略語 改訂情報	—
本文	監督領域	大分類および小分類：「核物質防護」 評価領域：「核物質防護体制」 検査分野：「法令遵守および核セキュリティ文化醸成の体制」	ガイド ID カテゴリー CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction 1. The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 2. The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）

	検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）のうち、法令遵守および核セキュリティ文化醸成の体制を確認する。 これらの確認については、法令遵守および核セキュリティ文化醸成の体制の検査分野における体制、訓練・教育にも留意する。 2.2 防護措置の狙い 法令遵守および核セキュリティ文化醸成を推進することにより、事業者一体となった適切な核物質防護体制を維持する。	2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder’s arrangements to ensure their security systems have appropriate levels of reliability and resilience. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（法令遵守および核セキュリティ文化醸成の体制の確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官がセキュリティシステムについて適切なレベルの信頼性とレジリエンス有することを評価する際の一般的な助言と情報を提供
	検査要件	3.1 検査対象 法令遵守および核物質防護規定遵守のための体制（経営責任者の関与を含む。）、核セキュリティ文化を醸成するための体制（経営責任者の関与を含む。）に係る全ての事項が検査対象となるが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定 に際しては、体制の構築状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （1）検査の頻度 1 年間に 1 回程度 （2）検査時間 3 人／1. 0 0 （h） 3.3 実施体制 （1）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （2）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	6. Advice to Inspectors	12. It is particularly important to ensure, so far as possible, that the security system is capable of performing its function with an adequate level of reliability. This objective may be achieved by the adoption of a number of different provisions, together with the use of techniques to demonstrate the adequacy of the specified measures. The reliability of plant and systems to provide the security effect should be demonstrated by the dutyholder to be consistent with the risks associated with the loss of this capability. This should be informed by the Category of the security function and the Classification of the Security Structure, System or Component (SySSC) concerned. 13. The security system design should incorporate an appropriate level of redundancy to reduce the effects of random failure, and diversity and segregation to reduce the effects of common cause failure and malicious actions. This should take account of the site or facility the system is protecting and its vulnerability to threats described in the Design Basis Threat (DBT) (Reference 8). 14. In assessing the fitness for purpose of the security system, and particularly the ability to deliver a particular effect, a number of issues relating to redundancy and diverse provisions should be considered. Security plans should clearly identify the security function of all SySSCs so that this assessment can be carried out. Regulatory Expectation 15. There is a regulatory expectation that dutyholders demonstrate in the security plan how they ensure that the design and operation of the security system delivers	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 ONR - 検査官への助言 ✓ セキュリティシステムが適切なレベルの信頼性を以て機能を発揮できることが重要 ✓ セキュリティシステムに適切なレベルの冗長性と多様性・分離（共通原因故障や悪意ある行為の影響低減）が組み込まれていること ✓ セキュリティシステムの目的への適合性や、特定の効果の発揮能力の評価では、冗長性と多様性に関わる多数の問題を考慮 ✓ 規制上の期待事項 ➤ セキュリティ計画の中で、セキュリティシステムの適切なレベルの冗長性、多様性、分離について説明している ➤ 適切なリソースを確保 ✓ 基本セキュリティ原則（FSyP）5 - 信頼性、レジリエンス、持続性／信頼性とレジリエンス（SyDP）5.1

				appropriate levels of redundancy, diversity and segregation. Dutyholders should provide sufficient resources (including personnel) to inform the design, to maintain/repair and to operate SySSCs, thus building resilience to enable an appropriate and effective incident response, and a recovery programme that reflects the risk of any loss of service. Essential services critical to the correct functioning of the security system should be given the same priority as the system itself and as such are required to have appropriate levels of reliability and resilience. FSYP 5 - Reliability, Resilience and Sustainability / Reliability and Resilience / SyDP 5.1 Security structures, systems and components should be appropriately qualified, with design incorporating reliability and resilience through ‘failsecure’, redundancy, diversity and segregation. There should also be sufficient resources available and contingency arrangements developed to ensure continuity of security provision.	
	検査手順	法令遵守および核セキュリティ文化醸成の体制が適切にとられていることを関連文書の調査、ウォークダウン、インタビュー等によって確認する。 4.1 検査前準備 法令遵守および核セキュリティ文化醸成の体制に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する法令遵守および核セキュリティ文化醸成の体制に係る措置が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等においては是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	7. Elements of System Resilience	Redundancy 16. Redundancy is frequently defined as the provision of more than the minimum number of equipment items, components or elements required to perform a specific security function. Such redundancy allows a specified security function to be delivered when one or more items (but not all) are unavailable, due to a variety of unspecified potential failure mechanisms or maintenance (e.g. identified faults or hazards). 17. Experience dictates there are deterministic and probabilistic arguments to justify the provision of redundancy in SySSCs. A design which is considered acceptable will display adequate levels of system redundancy to ensure it is fit for purpose and should perform the required security function. These characteristics will include final provisions to satisfy the deterministic and probabilistic requirements of any potential design for SySSCs. Dependent Failure 18. A possible threat to SySSC resilience is that posed by dependent failure. These have the potential to prevent the performance of a required security function through simultaneous loss of redundancy provisions. Particular illustrations of this type of failure are common-cause failures (CCF). The inspector should be satisfied that the	NRA ・検査手順（概略） ✓文書、ウォークダウン、インタビューの活用 ✓検査前準備、検査、CAP 検査の趣旨 ONR ・7. システム・レジリエンスの要素 ✓冗長性 ➢ 経験上、SySSC の冗長性については、決定的と確率論的な論拠がある ✓従属故障 ➢ SySSC のレジリエンスに対する脅威は、潜在的な従属故障 ➢ 共通の弱点または従属性により、複数の故障が発生する可能性 ➢ 主な従属性の種類（機能／空間／固有／ヒューマンエラー関連の従属性） ➢ 従属故障防止に関する検査官の確認事項（事業者による把握と対策の実施）と対策例（空間依存性を排除する隔離方策など） ✓多様性 ➢ 共通原因故障によるリスクが考えられる場合、多様性を活用 ✓隔離 ➢ 多様性の他、火災や悪意などのハザードに

				risk from dependent failures has been reduced to a level which is acceptable within the limits set by design requirements. It is important to note that reliability does not necessarily increase indefinitely in proportion to levels of redundancy, and this is primarily due to common origin or common cause effects. This type of failure is often referred to either as CCF or a common mode failure (CMF). A CCF is a dependent failure event where approximately simultaneous multiple failures result from a single shared cause (e.g. fire). A CMF is a common cause event where multiple equipment items fail in the same mode. 19. Multiple failures can occur due to common weaknesses or dependencies shared by components. Such failures can cause failure of all redundant components in a single security system or failure of components in more than one system. Dependent failures can considerably reduce the reliability of the security systems relative to that expected of random failures occurring in isolation. 20. The main types of dependencies which could cause potential loss of a security function are described below. • Functional dependencies, which arise from shared or common functional features; such as a common electrical power source, common wiring or a shared communication node. • Spatial dependencies, which arise from physical features shared by components located in a common location; such as common radiation or chemical conditions, a common environment and support structures, and vulnerability to leaks of dangerous fluids (high temperature, corrosive or toxic) or anything else potentially attributable to SySSCs' common location. • Inherent dependencies, which arise from shared characteristics; such as a common principle of operation or technical feature such as electrical overload. • Human error related dependencies, which arise from human errors affecting some shared or common human process; such as human error in design or manufacture, or staff error during operation and maintenance. 21. To provide protection against dependent failures, the inspector should seek confirmation that the dutyholder	よる共通原因故障の脅威を低下させるには 隔離（距離または物理障壁）がある ✓システムの独立性 ➤ 可能な限り、他システムの誤操作や故障の悪影響（とくに隠れた依存性による）を受けない方策が必要
--	--	--	--	---	--

				has identified and, where necessary and practicable, implemented measures in design, construction and operation to eliminate them or reduce their potential effect. Examples of such measures are: • the provision of segregation to eliminate spatial dependencies; • the avoidance of functional dependencies by segregation of SySSCs and their support services; • the provision of alternative and independent equipment to eliminate undue reliance on any single system. The purpose of this approach is to help provide protection against any 'hidden failure dependencies' that may not be identified; and • approaches and procedures should be implemented to minimize the possibility of failure dependencies arising during design, manufacture, construction and operation, including dependencies due to operator and other human error. Diversity 22. Where a component of the security system is at potential risk from common cause failures, one means of reducing the susceptibility is to employ diverse provisions in separate redundant trains or systems. For example, the detect function over a given area could be delivered by both fixed-line and pan-tilt-zoom closed circuit television powered by segregated electricity supplies and supported by a dual perimeter intruder detection system utilizing complementary technologies (for example infrared and microphonic technologies), again powered by segregated power supplies. A dutyholder should consider appropriate measures to include diversity within the components of the system which is designed to deliver an individual effect and/or across SySSCs in their entirety. Engineering diversity is defined as the provision of dissimilar means of achieving the same objective, e.g. the use of features which differ in the physical means of achieving a specific objective or use of different equipment made by different manufacturers. 23. Diversity provides one means of protection against some causes of failure, by removing common features which may lead to failure dependencies. Diversity particularly provides protection against inherent dependencies and human error related dependencies.	
--	--	--	--	--	--

				24. The physical co-location or functional support of diverse systems could lead to dependencies that defeat the objective of providing diversity. This should be addressed through the layout and functional design of the SySSC where appropriate. Segregation 25. In a resilient SySSC, despite diverse provisions, the threat of common cause failures from hazards such as fire or hostile intent may be reduced by system segregation. This is the separation of components by distance or physical barriers, a particular example being provision of principal fire barriers to delineate individual fire zones; they may also serve as barriers to other hazards such as blast. Appropriate levels of segregation should be present in a dutyholder's provisions in order to maximize the likelihood that a security function will be performed, despite the occurrence of faults and hazards, possibly in combination. 26. Equipment segregation is the separation of redundant and/or diverse components by distance or by barriers in order to prevent all (or sufficient to enable system failure) of the components being damaged, particularly in the event of common hazards or malicious action. A system's design should ensure that internal hazards, such as fire and certain external threats do not damage separate chains of security equipment to the extent that its functional reliability is unacceptably reduced. The most straightforward manner in which segregation can be achieved is through distance and avoiding collocating components. System Independence 27. SySSC may be subject to spurious operation in addition to operational failures. These can arise because a given system component does not possess a sufficient level of independence from other separate systems. Measures need to be employed by the dutyholder to ensure that, wherever possible, SySSCs are not adversely affected by the spurious operation or failure of other systems, especially through any potential for hidden dependency (for example, by having a single system responsible for fire and security response). This is best achieved by designing in both functional and physical isolation.	
--	--	--	--	---	--

			8. Suitably Qualified and Experienced Personnel	28. The dutyholder’s security organization should possess adequate Suitably Qualified and Experienced (SQEP) personnel to support SySSCs. This includes having sufficient personnel with the necessary competences and knowledge to manage, operate, maintain and repair security systems at all times.	ONR 8. 適切に資格認定された経験豊富な職員 ・セキュリティ組織は、適切に資格認定された経験 ある（Suitably Qualified and Experienced : SQEP）職員を十分に確保すべき
			9. Essential Services and the Security System	29. Where essential services (such as computer-based security systems) are necessary to support the functioning of a Physical Protection System (PPS), then these services should be sufficiently resilient and secure to ensure that their loss or interruption does not adversely affect the ability of the PPS to achieve the required outcome as defined in SyAPs Annexes C and D. Inspectors should consider: ✓ Has reliability, resilience and sustainability been considered throughout the design stage for any new facility or SySSC and incorporated within relevant operational requirements or equivalent? ✓ Are requirements for SySSCs regularly reassessed in conjunction with all stakeholders? ✓ Are there sufficient SQEP and other resources to manage, operate, maintain and repair the SySSC? ✓ Does the design and operation of the SySSC display appropriate levels of redundancy, diversity and segregation? ✓ Do essential services (such as power) necessary for the correct functioning of the SySSC have the appropriate levels of security, reliability and resilience? ✓ Have potential dependencies and/or vulnerabilities of the SySSC been identified and mitigated? ✓ Do SySSCs ‘fail secure’ and, if they do not, are security requirements appropriately balanced against safety requirements and are adequate compensatory security measures available? ✓ Does the dutyholder demonstrate the ability to learn from their experience in maintaining a SySSC? ✓ Is there a process of continuous improvement in place in relation to SySSCs’ reliability, resilience and sustainability? ✓ Are appropriate quality performance and assurance mechanisms applied to SySSC? ✓ Is the response to the failure or loss of part of or all of a SySSC regularly exercised or rehearsed?	ONR ・ 9. 必須サービスとセキュリティシステム ✓ 核物質防護システム（PPS）の支援に必須サービス（コンピュータベースのセキュリティシステム等）が必要な場合、それが十分にレジリアントであり、喪失または干渉が PPS の能力に影響しないようにすること ・ 検査官の考慮事項 ✓ 新規施設または SySSC の設計で信頼性、レジリエンス、持続可能性が考慮され、運転要件等に組み込まれているか？ ✓ SySSC の要件は、全ての利害関係者とともに定期的に再評価されているか？ ✓ SySSC を管理、運転、維持、修理する十分な SQEP 等のリソースがあるか？ ✓ SySSC の設計と運転は、適切なレベルの冗長性、多様性、分離を示しているか？ ✓ SySSC が正しく機能するために必要な必須サービス（電力等）は、適切なレベルのセキュリティ、信頼性、レジリエンスを有するか？ ✓ SySSC の潜在的な依存性および／または脆弱性が特定され、緩和されているか？ ✓ SySSC は「フェイル・セキュア」か？そうでない場合、セキュリティ要件は安全要件と適切にバランスして、適切な補償セキュリティ手段が利用可能か？ ✓ 事業者は SySSC の維持経験から学ぶ能力を実証しているか？ ✓ SySSC の信頼性、レジリエンスおよび持続可能性を継続的に改善するプロセスがあるか？ ✓ 適切な品質パフォーマンス&保証メカニズムが SySSC に適用されているか？ ✓ SySSC の一部または全部が故障または喪失した場合の対応は、定期的に訓練またはリハーサルされているか？

法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant Legislation	4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ・ ・	NRA ・ 適用法令 ONR ・ 規制との関係（CNS ガイド共通の記載） ✓ 「事業者」の定義 ✓ NISR 要件の概要
		4. Relationship to IAEA Documentation and Guidance	6. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference 3). Further guidance is available within IAEA Technical Guidance and Implementing Guides. ・ ・	ONR ・ IAEA 文書との関係（CNS ガイドほぼ共通の記載、検査対象のみ相違、概要は CNSS-TAST-GD-1.1 の比較表参照）
		5. Relationship to National Policy Documents	9. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Security delivery Principle SyDP 5.1 – Reliability and Resilience, in support of FSyP 5 – Reliability, Resilience and Sustainability. The TAG is consistent with other TAGs and associated guidance and policy documentation. ・ ・	ONR ・ 国の政策文書との関係（CNS ガイドほぼ共通の記載、FSyP／SyDP の原則番号のみ相違、概要は CNSS-TAST-GD-1.1 の比較表参照）
参考文献	—	References	・ Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 ・ IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011. www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. ・ ・	—
用語集	—	Glossary and Abbreviations	CCF：Common Cause Failure CMF：Common Mode Failure ・ ・	—
改訂情報	変更日、施行日、変更概要（「制定」）	（表紙に記載）	Revision / Issue No., Date など	—

2.4.2.5 CNS-TAST-GD-6.1 (Issue 2) 「Categorization for Theft Leadership」における調査の結果

原子力規制庁検査ガイドに対応するものがないため、ONR の検査ガイドの主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-5 にまとめた。

2.4.2.5.1 監督領域

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.5.2 序論

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（セキュリティ評価原則 SyAPs（基本セキュリティ原則 FSyPs 含む）、原子力産業セキュリティ規制（NISR）、セキュリティ計画（SP）、機微な原子力情報（SNI）などに関する事項）。

2.4.2.5.3 検査の目的

ONR の検査ガイドでは、検査ガイドの目的（検査官が核物質および他の放射性物質（NM/ORM）の在庫分類による盗取ターゲット特定プロセスを評価する際の助言と情報を提供）、適用範囲の注意事項（悪用のための無許可の持ち出し行為を念頭にした物質の分類に限定）について説明している。

2.4.2.5.3 検査要件

ONR の検査ガイドでは、検査官への助言（サイトおよび施設の分類、規制上の期待事項、該当する FSyP など）を記載している。

2.4.2.5.4 検査手順

ONR の検査ガイドでは、次のように分けて説明している。

- ・以下、各項目について検査に必要な知識、注意点、検査官の考慮事項（検査の視点）を説明。
 - ✓ 分類の概要
 - 解説
 - 検査官への注意点
 - ✓ 物質の形態に基づく段階的防護要件の設定における考慮事項の解説
 - ✓ 核物質の合算に基づく追加的考慮事項の解説
 - ✓ 核物質の物理的防護と分類に関する注意（注意事項）
 - ✓ 放射線源の分類の解説

- ✓ その他の放射性物質の分類の解説
- ✓ 在庫の変化の解説
- ✓ 検査官の考慮事項

2.4.2.5.5 法令・基準等

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.5.6 改訂情報

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2. 4. 2-5 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-6.1 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		英国 ONR 検査ガイド		両者間の主な相違点
【ガイド】－ (－)		【ガイド】 CNS-TAST-GD-6.1 (Issue 2) Categorization for Theft (March 2023) (15 頁)		
項目	主な内容	項目	主な内容	(注) 原子力規制庁の対応する検査ガイドがないため、以下は、ONR 検査ガイドの記載概要を示す
図書全体構成	－	図書全体構成	表紙 目次 本文 参考文献 用語・略語 改訂情報	－
本文	監督領域	－	ガイド ID カテゴリー	CNS ONR ・ガイドの大分類 (CNS=核セキュリティ)
	－	－	1. Introduction	1. The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 2). 2. The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide. ONR ・序論 (CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ)

	検査の目的		2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder’s processes to identify theft targets through the categorization of its inventory of Nuclear Material and Other Radioactive Material (NM/ORM). It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate. 4. Inspectors should note that the scope of this TAG is limited to the categorization of materials where the intent is an act of unauthorized removal for subsequent malicious use. Dutyholders are also required to categorise their inventories from the perspective of direct acts of sabotage (i.e. attacking the radioactive material or associated facilities). This is known as vital area identification and TAG 6.2 is provided to assist inspectors assessing dutyholder vital area identification studies.	ONR ・本ガイド（TAG）の目的 ✓ 検査官が核物質および他の放射性物質（NM/ORM）の在庫分類による盗取ターゲット特定プロセスを評価する際の助言と情報を提供 ✓ 本 TAG の適用範囲は、悪用のための無許可の持ち出し行為を念頭にした物質の分類に限定されていることに注意
	検査要件	—	6. Advice to Inspectors	13. Dutyholders should categorise their site and facilities for theft in accordance with the quantities of all NM and ORM. For some dutyholders this may be a relatively simple task but for others, with a large and varied inventory that may also change over time, requires suitable access to specific knowledge and expertise. Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the nuclear material and potential consequences associated with its unauthorized removal. Table 1 in Annex A to the SyAPs reflects the schedule to NISR that defines categories of nuclear material based on isotope (and enrichment for uranium) and weight but provides more granularity to facilitate application of the graded approach. Table 2 provides an alternative scheme for categorization that takes dilution, dispersion, type and form into account. Table 3 and Table 4 are to be used for the categorization of radioactive sources and Other Radioactive Material (ORM).	ONR ・6. 検査官への助言 ✓ 事業者は、NM および ORM の量に応じて、盗取を念頭にサイトおよび施設を分類すべき ✓ 放射性物質は、段階的アプローチを踏まえた正しいセキュリティ成果を特定するために適切な分類に当てはめることが重要 ➤ 表 1, 2：核拡散の観点から分類（核爆発装置作成以外の悪意ある行為には不適当） ➤ 表 3, 4：被ばくによる健康リスクの観点から分類（核不拡散の考慮には不適当） ✓ 事業者が示す分類が高度に技術的で複雑な場合、検査官は ONR のサボタージュ・ターゲット解析・レビュー（STAR）チームに助言を求めるべき ✓ 規制上の期待事項 ➤ 事業者は、盗取に関するサイトおよび施設の分類を NM および ORM の量および形態に応じてどのように行っているか、セキュリティ計画の中で実証する ✓ FSyP 6：核物質防護システム／盗取に関する

				14. It is essential that radioactive materials are allocated to the appropriate categories in order to identify the correct security outcome to be achieved in applying the graded approach. Both Table 1 and Table 2 grade materials based on their utility from a proliferation perspective and are not appropriate when considering malicious acts other than constructing a Nuclear Explosive Device (NED), for example the improvisation of a Radiological Dispersal Device (RDD) or Radiological Exposure Device (RED). The security groups within Table 3 and Table 4 are provided for the purpose of grading the risk to human health posed by exposure to radioactive materials (and hence utility in the construction of an RDD or RED) and similarly, these tables are not appropriate for consideration of proliferation. Therefore, where categorization for theft is being applied to radioactive material that is also nuclear material (for example a radioactive source comprising of plutonium), it will require a nuclear material category under Table 1 or Table 2 and a security group against Table 3 or Table 4. However, in application this is only necessary where the nuclear material falls below Category III because at this quantity and above, the security outcome dutyholders need to achieve will be driven by the proliferation categorization . Allocation of categories is explained in more detail later. 15. Wherever cases regarding categorization for theft presented by a dutyholder are challengingly technical and complex, inspectors should seek advice from the ONR Sabotage, Target Analysis, Review (STAR) team. When arriving at any judgement on the dutyholder's case, they might also seek appropriate peer review. Regulatory Expectation The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how site or facility categorization for theft has been implemented according to the quantities and forms of all NM and ORM held or used. They should also demonstrate how they identify and manage planned or potentially unplanned changes to the inventory and/or operations at a site/facility that might affect its categorization , in order to ensure an appropriate PPS and the associated outcomes are maintained at all times.	分類 (SyDP6.1)
--	--	--	--	--	--------------

				FSyP 6 - Physical Protection Systems / Categorization for Theft/ / SyDP 6.1 Dutyholders should undertake a characterisation of their site and facilities in order to determine the categorization for theft.	
	検査手順	—	7. Categorization Overview	16. Table 1 (with notes) of Annex A to SyAPs details the categorization of NM. It reflects the schedule to NISR and the table in the extant versions of INFCIRC/225, the Nuclear Suppliers Group Guidelines, the CPPNM and the contents of the Guidelines for the Management of Plutonium. However, Table 1 is not identical with the schedule or these international tables/documents and should not be referenced outside the UK. 17. Intermediate and low level waste containing NM may be categorized in accordance with Table 2 where specific criteria are met. This table provides an alternative scheme for categorization that makes allowances for considerations of dilution, dispersion, type and form. For example, waste maybe in the form of a sludge and NM not be easily recoverable because it might be highly dispersed and not readily separated. Dutyholders may also be able to make a case for materials to be categorized in accordance with Table 2 under special arrangements where the characteristics do not meet every aspect, but are broadly comparable to, the specific criteria. 18. Radioactive sources and ORM should be assigned a security group in accordance with Table 3 and Table 4 respectively. This categorization system is taken from the IAEA Safety Guide RS-G-1.9 Categorization of Radioactive Sources and is based on the concept of ‘dangerous sources’, which is quantified in terms of ‘D values’. The D value is the radionuclide specific activity of a source which, if not under control, could cause severe deterministic effects for a range of scenarios that include both external exposure from an unshielded source and internal exposure following dispersal of the source material. 19. Inspectors should note that Table 1 and Table 2 both categorise materials solely based on the attractiveness of the material from a proliferation perspective (i.e. the ease with which it could be used to fashion an improvised nuclear device). Hence, the categorization s are derived from the quantities, isotopes and	ONR • 7. 分類の概要 ✓ SyAPs の付属書 A の表 1 に詳細な NM 分類 ✓ NM を含む中・低レベル廃棄物は、特定の基準を満たせば、表 2 により分類可能。 ✓ 放射線源および ORM には、それぞれ表 3 および 4 にしたがってセキュリティグループを割り当てるべき ✓ 検査官は、次の点に注意。 ➤ 表 1 と 2 は、核拡散の観点から見た物質の魅力のみに基づいて分類していることに注意。すなわち、核分裂性物質の量、同位体、濃縮度を考慮。 ➤ 表 3 および 4 は、主に放射性物質の健康影響の観点から分類。RDD または RED を作るための盗難の観点から見た物質の魅力を考慮。 ➤ 多くの場合（放射線源がプルトニウムで構成されている場合など）、物質を表 1 と 2 のいずれか、および表 3 と 4 のいずれかに分類するのが適切。

			enrichments of fissile materials. Table 3 and Table 4 are based primarily on the potential for radioactive material to cause deterministic health effects and considerations therefore relate to the attractiveness of material in terms of theft in order to fashion a RDD or RED. In many cases (e.g. where a radioactive source is comprised of plutonium), it will be appropriate for material to be categorized against one of either Table 1 or Table 2 and one of either Table 3 or Table 4. Where this is the case, the categorization resulting in the highest security outcome should be used as the basis for physical protection system design	
		8. Considerations in Setting Graded Protection Requirements Based on Material Form	20. A three-factor methodology is initially used to categorise un-irradiated NM in order to determine the appropriate physical protection against theft. With this methodology, for any NM, the element, the isotopic composition, and the quantity, are the three factors considered to initially determine the level of physical protection required to protect against theft. This methodology is simple, but there are situations when it may result in overly conservative protection requirements for the material being protected and the form of the material also needs to be considered. In light of this, Table 2 of Annex A to SyAPs describes an alternative categorization scheme that considers other attributes of the material which might provide additional impediments to an adversary aspiring to develop a NED, such as dilution or extensive material separation issues. Dutyholders may make a case for their inventory to be categorized according to this scheme where the associated criteria are fulfilled, noting that a degree of flexibility may be catered for under special arrangements as detailed above. 21. The IAEA recommendations recognise the need for consideration of other factors: • For NM in general, “the categorization is the basis for a graded approach for protection against unauthorized removal of nuclear material that could be used in a nuclear explosive device, which itself depends upon: the type of NM (e.g. Pu and U), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution radiation level, and quantity.” • For waste, “Nuclear material which is in a form that is no longer usable for any nuclear activity, minimises	ONR • 8. 物質の形態に基づく段階的防護要件の設定における考慮事項 ✓ 盗取に対する適切な物理的防護を決定するために、未照射 NM の分類に 3 要素を考慮する方法が最初に使用される。 ➤ 必要な物理的防護レベルの最初の決定で 3 要素（元素、同位体組成、量）を考慮 ➤ この方法は単純だが、過度に保守的な保護要件となる場合があり、物質の形態も考慮する必要がある。 ➤ この点を考慮し、SyAPs の付属文書 A の表 2 は、希釈化または大規模な物質分離の問題など、NED 開発を望む敵対者に追加的な障害となる可能性のある物質の他の属性を考慮した代替分類スキームを記載。 ✓ IAEA の勧告は、他の要因を考慮する必要性を認めている。 ✓ 希釈-希釈状態の核物質は、敵対者が相当量の NM を得るのに、より大量の取得を強制する。また変換に大規模な処理が必要になるなど、敵対者にとって NM の回収がより困難になる。 ✓ 分散-広く分散している物質は、敵対者が相当量の NM を得るのに、より大量の物質の取得を強制する。NM を他の魅力的でない物質から識別し分離することがより困難になる。 ✓ 形態 - NM の加工および保管は、化学的・物理的形態が盗取の魅力に重要な影響を及ぼす可能性がある（例：セメント系グラウトやガラス固化体のような流動性のないマトリックスに結合した材料は、敵対者にとって困難な

				environmental dispersal and is practically irrecoverable, may be protected against unauthorized removal in accordance with prudent management practice.” • For irradiated fuel, the IAEA guidance allows reduction of category based on radiation level. 22. Dilution - Material that is in a dilute form will force an adversary to acquire much larger volumes and masses of material to obtain a significant quantity of NM. The adversary may also be faced with greater difficulty in recovering the NM such as a need to perform extensive processing to convert the NM to a form usable in a NED. Possible additional factors could be the concentration of NM and the homogeneity of the concentration within the material. 23. Dispersion - Material which is widely dispersed within a store, either in individual containers, or as part of a homogenous mass, will force an adversary to acquire larger volumes and masses of material to obtain a significant quantity of NM. The adversary then has greater difficulty in identifying and separating the NM from the other less attractive materials. These considerations form the basis of the criteria against which a dutyholder may make a case for their inventory to be categorized against Table 2 of Annex A to SyAPs 24. Form - The processing and storage of NM may be beneficial as a control measure because the chemical and physical form of the material may have a significant impact on the attractiveness for theft. For example, materials that are bound into immobile matrices, such as cementitious grout or a vitrified product, will also create difficulties for adversaries. Table 2 incorporates these considerations by limiting the highest possible categorization where the chemical and physical form is appropriate. 25. Irradiation - The CPPNM and NISR Schedule defines the term ‘irradiated’, in relation to any kind of material, means that the material has a total radiation output giving a dose rate exceeding 1 Gray per hour at one metre from the unshielded surface of the material. The categorization of material meeting these criteria may be reduced based on the reduced attractiveness because of the high dose rate and hence danger to life. However, this rate may be insufficiently high to deter (neither will it incapacitate) modern threats where adversaries are	ものとなる)。 ✓ 照射 - CPPNM と NISR は、「照射された」とは材料表面から 1m で 1 時間あたり 1Gy を超える線量率を与える材料と定義。この基準を満たす材料は生命に危険を及ぼすため、魅力が低下し分類を下げられる。しかし、敵対者が健康に無頓着な現代の脅威を抑止するには（無力化するには）不十分かもしれない。 ✓ 事業者は、NM 在庫の特性を完全に文書化し、SyAPs の附属書 A の表 1 または表 2 に照らして盗取に関する分類を説明すべき。
--	--	--	--	---	---

				unconcerned about preservation of their health. Therefore, inspectors should be cautious about dutyholder claims for reduced NM categorization based on the irradiated criteria where the dose rate is close to the threshold. This is especially the case where the half-life of the material is relatively short in comparison to the life of the facility in which it is to be stored or processed. Further advice should be sought from specialists in SINS, health physics and/or radiation protection specialists as required. 26. The dutyholder should develop a fully documented characterisation of their NM inventory and make a case to categorise for theft against either Table 1 or Table 2 of Annex A to SyAPs. This will ensure that the basic three-factor methodology and other factors considered above are appropriately incorporated within the categorization case.	
				27. Regulation 3(5) of NISR states that in determining the categorization of material used or stored on nuclear premises, the quantities of all material of the kind in question (i.e. materials as specified in column 1 of the Schedule to NISR) that is being used or stored on the nuclear premises are to be aggregated. Therefore, careful consideration will need to be given to adding together, or aggregating, the total amount of NM contained within a nuclear facility, group of buildings or group of rooms when categorizing nuclear material. The principle of aggregation is an important element in deciding (and potentially increasing) the appropriate categorization on a site and facility basis. 28. In some facilities, NM of the same type may be located in several different buildings, for different purposes or at different stages of processing. For example, there may be Category II quantities of specific material in one building and a Category II quantity of similar material in another building within the same Protected Area. Considered individually, each quantity of material is Category II. However, if all the material could be taken during a single adversary attack, the material should be designated as Category I. Consideration should also cover the possibility that quantities of NM may be removed by a single adversary from several locations or buildings (e.g. by an insider), which may include small quantities over an extended	ONR 9. 核物質の合算に基づく追加的考慮事項 ✓ NISR は、施設内で使用または貯蔵される物質の分類を決定する際、当該物質（NISR の別表の第 1 欄に規定）の全量を合算するとしている。 ✓ 施設によっては、同じ種類の NM が異なる目的のために、或いは処理の異なる段階で、複数の異なる建物に配置されている場合がある。また、NM が一人の敵対者（例：内部者）によって複数の場所または建物から持ち出される可能性も考慮すべき。 ✓ 異なる種類（例：濃縮度の異なる Pu、Np、U）の NM が同じ施設内に存在する可能性がある。施設内の NM の総量は、特定の場所における NM の分類を決定する際に考慮されるべき。 ✓ ONR の SINS チーム が、事業者が採用した手法の妥当性について助言を提供できる。

				period of time. 29. NM of different types (e.g. Pu, Np and U with different levels of enrichment) may be co-located in the same nuclear facility. The total amount of NM in the facility should be considered in determining the categorization of the NM in any specific location. There are several mathematical approaches for calculating the category for aggregated quantities of different NM, and the dutyholder should decide which approach is appropriate. The ONR SINS team can provide advice on the adequacy of the methodology adopted by the dutyholder.	
			10. Notes on Physical Protection and Categorization of Nuclear Material	30. Inspectors should note that prior to the publication of SyAPs and the associated adoption of outcome focused security regulation, it was acceptable for dutyholders to make a case for reducing the categorization of NM to take into account aspects of attack scenarios and physical protection. For example, cases were made for a Category III NM inventory to be protected as Category IV because of its location within robust vaults combined with the sheer volume and mass that would need to be removed. This was entirely appropriate under the previous prescriptive approach to regulation in order to avoid the application of disproportionate security measures driven by model standards, which were based on a worst-case scenario of material attractiveness. Conversely, such an approach is not appropriate in an outcome focused regulatory regime where, in the absence of model standards, the previous motivation is no longer relevant and can lead to inadequate protective security.	ONR ・ 10. 核物質の物理的防護と分類に関する注意 ✓ 検査官は、SyAPs が公表され、結果を重視するセキュリティ規制が採用される前は、事業者が攻撃シナリオと物理的防護の側面を考慮して NM の分類を下げるのが容認されていたことに注意（例：分類 III の NM 在庫は、堅牢な保管庫内にあり、取出しの体積と質量が膨大であることから、分類 IV とされるケースがあった）。 ✓ しかし、このアプローチは、結果を重視する規制においては適切ではなく、モデル基準がない以上、不十分な防護措置につながりかねない。
			11. Categorization of Radioactive Sources	31. Radioactive sources are placed in security groups according to guidance issued by the IAEA. For the purposes of determining security protection these groups and categories of source are set out in Table 3 of Annex A of the SyAPs. Many of the sources referred to are typically used in medical or industrial applications, and the examples given here are intended to serve as a guide to source types and categorization. The IAEA methodology for categorizing radioactive sources, based on the A/D activity ratio, is set out in IAEA Safety Guide Ref RS-G-1.9 (Reference 8). Whilst the methodology is based on the A/D ratio, factors such as the physical and chemical forms, the type of shielding	ONR ・ 11. 放射線源の分類 ✓ 放射線源は、IAEA が発行したガイダンスにしたがってセキュリティグループに分類される（線源の多くは一般に医療用または工業用で使用）。 ✓ 分類システムには 5 つの分類がある。この中で、分類 1 の線源は、安全かつ確実に管理されなければ人の健康に非常に高いリスクをもたらす可能性があり最も有害なもの。 ✓ 多くの線源が一緒に定期使用または保管されている或いは近接している場合、A/D 値を合計して線源を集計すべき。い。

				or containment employed, the circumstances of use and accident case histories are also taken into consideration within the categorization for sources of specified types and practices in Table 3. Where a dutyholder possesses a source that does not fit within the specified types or practices, then it would be reasonable for categorization to be based solely on the A/D ratio. 32. The categorization system has five categories. Within this, sources in Category 1 are considered to be the most harmful because they can pose a very high risk to human health if not managed safely and securely. An exposure of only a few minutes to an unshielded Category 1 source may be fatal. At the lower end of the categorization system, sources in Category 5 are the least dangerous; however, even these sources should be kept under appropriate control. 33. Where a number of radioactive sources are regularly used or stored together, or are in close proximity, their aggregation should be applied by summing the A/D values. Thus, the total radioactivity of the sources should be assessed using the IAEA methodology (Reference 8) to identify the security grouping and level of security protection needed. Inspectors should take particular note of sources in IAEA Category 3, where aggregation of just two may cross a threshold resulting in a higher SyAPs security outcome to be achieved, which may not be possible with a physical protection system designed to achieve the lower outcome. 34. Dutyholders should also be able to demonstrate how they identify and manage potential planned or unplanned changes to operations at a site/facility that might affect its categorization to ensure an appropriate PPS and outcomes are maintained at all times.	✓ 事業者は、適切な PPS と成果が常に維持されることを確実にするため、サイト／施設の分類に影響を及ぼす可能性のある潜在的な計画的または計画外の運転変更をどのように特定し、管理するか実証できること。
			12. Categorization of Other Radioactive Material	35. In addition to radioactive sources, dutyholders may have inventories of ORM, which should also be categorized because it may similarly be of use to adversary wishing to construct an RDD or RED. Given this similarity, Table 4 of the SyAPs annexes provides a categorization scheme for ORM that reflects the radioactive source methodology. Dutyholders should determine the A/D value of any inventory of ORM to determine the appropriate security group. However, certain inventories of ORM may have extremely low	ONR • 12. その他の放射性物質の分類 ✓ 線源の他に、RDD または RED を作成しようとする敵対者にとって同様に使用される可能性があるため、ORM も分類すべき。

				concentrations of activity and in these cases, it may be appropriate for dutyholders to make alternative cases for categorization .	
			13. Inventory Changes	36. In many cases, site inventories may be subject to change, particularly during commissioning and decommissioning. Therefore, dutyholders should also be able to demonstrate how they identify and manage both planned or unplanned changes to operations at a site/facility that might affect its categorization to ensure an appropriate PPS and security outcomes are maintained at all times. Inspectors should consider: - Has the dutyholder categorized all nuclear material in accordance with Table 1 and/or 2 of the SyAPs Annexes? - Where Table 2 of the SyAPs Annexes is used, has the dutyholder made a sufficient case against the criteria? - Have all sources been categorized in accordance with Table 3 of the SyAPs Annexes? - Has all ORM been categorized in accordance with Table 4 of the SyAPs Annexes? - Where material has been categorized against both Table 1 or Table 2 and Table 3 or Table 4 of the SyAPs Annexes, has the correct overall category and security outcome been identified? - Has the dutyholder given appropriate consideration to aggregation within their categorization methodology? - Are there processes in place to identify and manage planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorization ?	ONR 13. 在庫の変化 ✓ サイトの在庫は、特に試運転中や廃止措置時に変化する可能性がある。したがって、適切な PPS とセキュリティの成果が常に維持されるよう、サイト／施設の分類に影響を及ぼす可能性のある計画的または計画外の運転変更をどのように把握し管理するか示せること。 - 検査官の考慮事項： ✓ 事業者は、全ての核物質を SyAPs 付属書の表 1 および／または表 2 にしたがって分類しているか？ ✓ SyAPs の附属書の表 2 が使用されている場合、事業者はその基準に照らして十分な説明を行ったか？ ✓ 全ての線源が SyAPs 付属書の表 3 にしたがって分類されているか？ ✓ 全ての ORM は、SyAPs 付属書の表 4 にしたがって分類されているか？ ✓ 物質が SyAPs 付属書の表 1 または表 2 と表 3 または表 4 の両方に照らして分類されている場合、正しい全体的分類とセキュリティの結果が特定されているか？ ✓ 事業者は、その分類方法の中で、合算について適切に考慮しているか。 ✓ 分類に影響を及ぼす可能性のあるサイト／施設の在庫および／または運転の計画的または計画外の変更を特定し管理するプロセスがあるか？
	法令、基準等	—	3. Relationship to Relevant Legislation	5. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. • •	ONR - 英国の関連法との関係 ✓ NSIR における用語の定義と NM&ORM に関する主な要件
			4. Relationship to IAEA Documentation and Guidance	7. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) (Reference 4) and the IAEA Nuclear Security Fundamentals (Reference	ONR - 国際的な基準およびガイダンスとの関係 ✓ 国の核セキュリティ体制の必須要素は、核物質防護条約（CPPNM）および IAEA 核セキ

				3). Further guidance is available within IAEA Technical Guidance and Implementing Guides. ・ ・	リティ基本文書に規定、ガイダンスは、IAEA 技術ガイダンスおよび実施ガイド参照。 ✓ より詳細なガイダンスは NSS 13 等参照。
			5. Relationship to National Policy Documents	10. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission demonstrating they have effective processes in place to achieve Security Delivery Principle (SyDP) 6.1 – Categorization for Theft, in support of FSyP 6 – Physical Protection Systems. The TAG is consistent with other TAGs and associated guidance and policy documentation ・ ・ ・	ONR ・ 英国の政策文書との関係 ✓ セキュリティ評価原則（SyAPs）が、検査官が行う評価の判断基準となる ✓ 政府機関および第三者が国の情報等を取扱う場合の期待事項を示している。 ✓ 政府が効果的、効率的かつ安全に機能できるように、政府組織および国情報等を扱う第三者がどのように保護セキュリティを適用するかについて、政府のセキュリティ政策の枠組み（SPF）に期待事項が示されている。
参考文献	—	—	References	・ “Security Assessment Principles for the Civil Nuclear Industry. ONR.,” [Online]. Available: http://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf . ・ Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 ・ ・	—
用語集	—	—	Glossary and Abbreviations	CPPNM : Convention on the Physical Protection of Nuclear Material CS&IA : Cyber Security and Information Assurance ・ ・	—
別紙・附属書	—	—	Appendix	—	—
改訂情報	—	—	（表紙に記載）	Revision / Issue No., Date など	—

2.4.2.6 CNS-TAST-GD-6.2 (Issue 2) 「Categorization for Sabotage」における調査の結果

原子力規制庁検査ガイドに対応するものがないため、ONR の検査ガイドの主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-6 にまとめた。

2.4.2.6.1 監督領域

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.6.2 序論

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項（セキュリティ評価原則 SyAPs（基本セキュリティ原則 FSyPs 含む）、原子力産業セキュリティ規制（NISR）、セキュリティ計画（SP）、機微な原子力情報（SNI）などに関する事項）を記載している。

2.4.2.6.3 検査の目的

ONR の検査ガイドでは、検査ガイドの目的（検査官がサイトおよび施設のサボタージュ・ターゲット特定プロセスを評価する際の助言と情報を提供）について説明している。

2.4.2.6.3 検査要件

ONR の検査ガイドでは、検査官への助言（サイトおよび施設の分類方法の評価の検査、事業者との連携、該当する FSyP、STAR チームの判断など）を記載している。

2.4.2.6.4 検査手順

ONR の検査ガイドでは、次のように分けて説明している。

- ・規制上の期待事項（事業者に求められること、該当する FSyPs）
- ・以下、各検査項目について検査に必要な知識、それを踏まえた検査官の考慮事項（検査の視点）を詳細に説明。
 - ✓ 重要区域特定（VAI）提出図書
 - 解説
 - 検査官の考慮事項
 - ✓ VAI 図書の提出の解説

2.4.2.6.5 法令・基準等

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.6.6 改訂情報

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-6 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-6.2 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		英国 ONR 検査ガイド		両者間の主な相違点
【ガイド】－ （－）		【ガイド】 CNS-TAST-GD-6.2 (Issue 2) Categorization for Sabotage (June 2023) (26 頁)		
項目	主な内容	項目	主な内容	（注）原子力規制庁の対応する検査ガイドがないため、以下は、ONR 検査ガイドの記載概要を示す
図書全体構成	－	図書全体構成	表紙 目次 本文 参考文献 用語・略語 付録 改訂情報	－
本文	監督領域	－	ガイド ID カテゴリー	CNS ONR ・ガイドの大分類（CNS=核セキュリティ）
	－	－	1.Introduction	1.The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 1). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 2). 2.The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide. ONR ・序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）

	検査の目的	—	2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR inspectors in the exercise of their regulatory judgement during intervention activities relating to assessment of a dutyholder’s processes for target identification for sabotage of their site and facilities. It aims to provide general advice and guidance to ONR inspectors on how dutyholders’ Vital Area Identification (VAI) submissions should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail or methodologies for dutyholders to follow to demonstrate they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail within their submission and for ONR to assess whether the arrangements are adequate. 4. Appendix A to this guide contains details on the type of information that will need to be considered by a dutyholder and covered in a VAI submission. As the content of this Appendix is primarily concerned with technical issues associated with nuclear safety, responsibility for the content and the ownership of this Appendix rests with ONR Safety Assessors employed in the Sabotage Target Analysis and Review (STAR) team.	ONR ・本ガイド（TAG）の目的 ✓ 検査官がサイトおよび施設のサボタージュ・ターゲット特定プロセスを評価する際の助言と情報を提供（重要区域特定（Vital Area Identification：VAI）図書の評価方法） ✓ 付録 A に事業者が考慮し VAI 提出図書でカバーすべき情報の種類の詳細を示す。
	検査要件	—	5. Advice to Inspectors	14. ONR inspectors make judgements on how sites and facilities are categorized for sabotage. Due to the technical nature and complexity of the process, advice can be sought from the ONR STAR team, and engagement with the dutyholder is essential to fully understand the process. This guidance informs regulatory assessment of the dutyholder’s target identification for sabotage and will inform the design and management of the Physical Protection Solution (PPS) whilst recognizing that target identification, including categorization for sabotage in accordance with the table in Annex B to the SyAPs, is only the start point for designing PPS measures. PPS is defined as an integrated set of physical protection measures intended to prevent the completion of a malicious act. 15. The judgment of the ONR STAR team can be sought when deciding the adequacy of a dutyholder’s submission relating to potential Vital Areas (VAs). The ONR STAR team will make an assessment of the technical adequacy of each VAI submission, taking the respective parts of the DBT and the graded approach to sabotage into account. The ONR STAR team will	ONR ・6. 検査官への助言 ✓ ONR 検査官は、サボタージュに関するサイトおよび施設の分類方法を評価する。 ➤ このプロセスは技術的で複雑なため、ONR の STAR チームの助言が有益。 ➤ プロセスを完全に理解するには、事業者との連携が不可欠。 ➤ SyAPs の附属書 B の表に従ったサボタージュに関する分類を含むターゲットの特定は、核物質防護解決策（PPS）を設計するための出発点に過ぎない。 ✓ 事業者の提出図書が潜在的な重要エリア (VA) に関して適切かどうか判断する際、STAR チームの判断を求めることが可能。

			provide specialist advice to security inspectors and dutyholders relating to each VAI submission as required. However, the relevant key features described below should be found in all VAI submissions developed by dutyholders.	
検査手順	—	6. Regulatory Expectation	16. The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how site and/or facility categorization for sabotage has been implemented through the conduct of a VAI study. They should also demonstrate how they identify and manage potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its categorization, in order to ensure an appropriate PPS and the associated outcomes are maintained at all times. FSyP 6 - Physical Protection Systems / Categorization for Sabotage / SyDP 6.2 Dutyholders should undertake a characterization of their site and facilities in order to determine the categorization for sabotage. 17. Once accepted, the VAI submissions will provide information which is to be used as a basis for the VA protection detailed in security plans. The security plan should refer to the current VAI submission and list the VA protection supporting assumptions/commitments.	ONR ・ 6. 規制上の期待事項 ✓ 事業者が、セキュリティ計画の中で、サボタージュに関するサイトおよび／または施設の分類が VAI 検討を通じてどのように実施されるか実証する。 ✓ FSpP 6：核物質防護システム／サボタージュに関する分類（SyDP6.2） ✓ 受理されれば、VAI 提出図書は、セキュリティ計画で詳述される VA 防護の根拠として利用される情報となる。
		7. Vital Area Identification Submissions	7.1. Vital Area (VA) Criteria 18. A VA is defined as ‘an area containing nuclear material and/or other radioactive material (including radioactive sources) or equipment, systems, structures or devices the sabotage or failure of which, alone or in combination, through malevolent acts as defined in the extant DBT document, could directly or indirectly result in Unacceptable Radiological Consequences (URCs), thereby endangering public health and safety by exposure to radiation’. 19. To ensure that VAs are provided with a proportionate level of protection, each is to be categorized as a Vital Area or a High Consequence Vital Area in accordance with the table in Annex B of the SyAPs. Each VA must be considered on a case-by-case basis, to take account of the relevant threats contained in the DBT document. 20. Any consideration of nuclear material and other radioactive material including sources is additional to those requirements for theft defined in [8] and associated	ONR ・ 重要区域特定（VAI）提出図書 ✓ 重要区域（VA）の基準 ✓ VAI 提出図書の一般的特徴 ✓ VAI 提出図書の作成 ✓ VAI 提出図書のレビューと改訂 ✓ VAI－ピアレビュー、保証、ガバナンス ✓ 検査官の考慮事項 ➤ 施設のサボタージュの分類は、SyAP の付録 B の閾値と一致するか？ ➤ 不確かさ、仮定、感度解析は、特に潜在的な VA が線量閾値に近い場合、適切か？ ➤ VAI 提出図書には、8 つの一般的な「良い特徴」がそれぞれ適切に取り入れられているか？ ➤ 事業者は、サボタージュの分類と VAI プロセスに関する効果的なトレーニングを提供しているか？

				IAEA Safety Guide (11). 7.2. General Features of a VAI Submission 21. General features of a good VAI submission should include the points summarised below. Subsequent sections of this guide translate these into more specific points. In general submissions should be: • Complete - Submissions should assume the loss of off-site power (LOOP) as this cannot be protected by a dutyholder. They should also take into account all plant states and consider both the active and passive systems required to maintain plant safety. They should detail how the malicious capabilities in the DBT could bring about an URC and take into account the graded approach identifying, for example, where a VA is High Consequence. • Clear - A submission should identify the PPS outcomes given in the SyAPs document that need to be met, relevant malicious capabilities in the DBT that need to be addressed, and the radiological consequences that could result. The submission should be clear, logical and understandable. The basis for all assumptions, conclusions and recommendations in the submission, and unresolved issues, should be explained and justified. Clarity should extend to the correct referencing of supporting information. The results of the VAI need to be deterministic; there is, or is not, a vital area. • Accurate - A submission should accurately reflect the plant, equipment and components. For a plant in design, the submission should accurately reflect the proposed build, with due consideration given to the state of the design development at that time. • Objective - The arguments developed in a submission should be supported with factual evidence, and the necessary understanding of the behaviour of associated systems or processes should be established. In the absence of directly relevant information, the use of inferred or extrapolated detail should be carefully substantiated. There is also a need to provide visibility of the sensitivity to assumptions that validate the robustness of associated claims. The adequacy of respective operational procedures, managerial controls and resources should all be demonstrated to an appropriate level.	➤ VAI は SQEP 職員により実施されているか? ➤ VAI 提出図書の作成支援に請負業者が使われる場合、その作業は独立した技術レビューの対象となっているか? ➤ VAI 提出図書の作成において、安全、運転、セキュリティのスタッフ間で効果的な連絡・協力が行われているか? ➤ VAI 提出図書は、適切な内部レビューとガバナンス方策の対象となっているか? ➤ サイト／施設のサボタージュの分類に影響を及ぼす可能性があるサイト／施設の在庫や運転に関する計画的または計画外の変更可能性を特定し、VAI レビューを開始させるプロセスが実施されているか? ✓ VAI 図書の提出 ➤ 完了後、事業者は VAI を ONR の CNSS（Civil Nuclear Security & Safeguard：民間核セキュリティ・安全保障部）に提出し、CNSS はその技術的内容の評価をアレンジする。 ➤ 評価の範囲および程度は、ONR の既存のサンプリングおよび選択基準に従う。
--	--	--	--	--	---

				• Appropriate - Any analytical methods, such as Deterministic Safety Analysis (DSA) used by the dutyholder to substantiate safety arrangements in a VAI submission should be shown to be fit for purpose with adequate verification by the ONR STAR Team in conjunction with other safety inspectors. Any assumptions that have been made should be identified and shown to be appropriate. • Integrated - A submission should be holistic, with clear links between any engineering/technical substantiation or analysis. It should also define where VA protection depends on external facilities and services, and clearly substantiate any associated assumptions that are made. • Current - A submission should be current, concise and relevant. The content of a VAI submission may change if the plant/area concerned undergoes a major modification, or a series of minor modifications, which could also have a significant cumulative effect on radiological consequences. The VAI process should also be repeated when design changes are being considered prior to their implementation, and whenever the DBT has been updated. Where possible this process should be applied in the design phase of a new facility to help ‘engineer out’ potential VAs. • Forward looking - A submission should demonstrate that VAs, and the processes involved to identify them, will be regularly reviewed throughout the lifetime of the site/plant/area to ensure the analysis remains valid and appropriate. 7.3. Preparation of a VAI Submission 22. A graded approach to the assessment of VAI studies will consider the outcome and its proximity to each of the dose thresholds. Inspectors should subject those which are close to the boundaries to greater review and assessment to confirm that the assumptions and uncertainties have been considered appropriately by the dutyholder. Particular attention will be given to the sensitivity studies and validation and verification of calculations. 23. Dutyholders should carry out VAI, aimed at identifying those targets that are vulnerable to sabotage that could potentially cause URCs. This work should be carried out by suitably qualified and experienced specialist safety and operational staff with advice from the security	
--	--	--	--	---	--

				department concerned. Where a dutyholder does not develop all aspects of the submission and uses contractors for this purpose, the dutyholder must demonstrate that a technical review has been undertaken independently of the contractor producing the submission. During the process, these specialists should also consider how a potential VA can be ‘engineered out’ from a safety perspective or through application of ‘security by design’ principles. This could involve the provision of additional safety systems or further diversification and is an important aspect of VAI that should be considered before a decision is made to apply physical protection. 24. Preparation of a VAI submission should be based on a number of factors. These include the graded approach against sabotage and potential radiological consequences resulting from a successful attack. It should also be based on a thorough review of plant structures, systems and components (SSCs) taking account of their location, physical separation, vulnerability to the threats detailed in the DBT and the potential for the loss of protection they provide to result in an URC. In all cases the calculation of radiological consequences should be based on conservative, but realistic assumptions, and on up-to-date data and information, including best estimate data where appropriate. This should be undertaken without consideration of the active protection and mitigation measures at the site. 25. An example process map for VAI is provided at Appendix B. The key elements of this process map should be employed by all sites in their VAI studies. Any ONR inspection of the process by which VAI studies are undertaken would look for all the key features of this sample process map. 7.4. VAI Submission 26. Some examples of points that need to be considered in a VAI submission are detailed in Appendix A to this TAG. 7.5. Review and Production of a Revised VAI Submission 27. It is important that a VAI is up to date and reviews are undertaken when any changes take place that could reduce, increase or change the status of VAs on site. Significant changes may also occur during operations, such as modification, incidents, revised lifetime plans,	
--	--	--	--	--	--

				operational experience etc, or as a result of any changes to the DBT or SyAPs. Such changes should be recorded and taken forward as necessary in an updated VAI, which accurately reflects the current situation. 28. The responsibility for reviewing and producing a revised VAI submission, together with document control arrangements, should be clearly defined and detailed in the security plan, as part of a dutyholder's assurance arrangements. This will include an appropriate timescale in which any submission will be reviewed. Suitably qualified and experienced staff should discharge these responsibilities. 29. Documentation which no longer forms part of a current VAI submission, or which has been superseded, should be archived and securely stored. This information still forms part of the formal audit trail and should remain available for reference by the dutyholder and ONR. 7.6. VAI – Peer Review, Assurance and Governance 30. As part of the pre-submission process, a VAI should undergo an internal peer review by the dutyholder and be subject to an assurance and governance process. This process should ensure that: • Appropriate methods and relevant safety and security standards and specifications have been used, and that the calculations used are correct. • The site/plant and operational details as documented are consistent with the actual site/plant and its operations. • Where necessary, there has been independent verification or advice provided by suitably qualified and experienced staff. • Where there has been any third-party involvement, there is evidence of their competence to undertake the work, and evidence that challenges raised have been addressed and the VAI amended accordingly. • Any evidence available from the dutyholder's internal audit function should confirm the VAI submission has been produced in compliance with relevant company procedures. • The VAI is complete, all key security and safety assumptions are considered to be valid, and the Board member (or equivalent) with responsibility for security has been briefed on all aspects of the submission and endorsed the approach used for its production. Inspectors should consider:	
--	--	--	--	---	--

			- Is the sabotage categorization of facilities consistent with the thresholds detailed in Appendix B of SyAPs? - Are uncertainties, assumptions and sensitivity analysis appropriate, particularly where a potential VA is close to a dose threshold? - Does the VAI submission appropriately incorporate each of the eight general ‘good features’? - Does the dutyholder provide for effective training on sabotage categorization and the VAI process? - Has the VAI been conducted by SQEP personnel? - Where a contractor has been used to assist preparation of the VAI submission, has their work been subject to independent, technical review? - Has there been effective liaison and cooperation between safety, operational and security staff in production of the VAI submission? - Has the VAI submission been subject to appropriate internal review and governance arrangements? - Are there processes in place that identify potential planned or unplanned changes to inventory and/or operations at a site/facility that might affect its sabotage categorization and trigger a review of the VAI? 7.7. Submission of a VAI Document 31. Once completed, dutyholders are expected to submit a VAI to OONRNSS who will arrange an assessment of the technical content of the VAI to an agreed programme. The scope and extent of the assessment will be subject to any extant sampling and selection criteria within ONR.	
法令、基準等	—	3. Relationship to Relevant UK Legislation and Policy	5. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ...	ONR - 英国の関連法および政策との関係 ✓ NSIR における用語の定義と NM&ORM に関する要件 ✓ エネルギー安全保障・ネットゼロ省（DESNZ）が設計基準脅威（Design Basis Threat, DBT）を作成、ただし、このうちサイバーセキュリティは別の TAG でカバー
		4. Relationship to International Standards and Guidance	10. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [3] and the IAEA Nuclear Security Fundamentals [4]. Further guidance is available within IAEA Technical Guidance and Implementing Guides. ...	ONR - 国際的な基準およびガイダンスとの関係 ✓ 国の核セキュリティ体制の必須要素は、核物質防護条約（CPPNM）および IAEA 核セキュリティ基本文書に規定、ガイダンスは、IAEA 技術ガイダンスおよび実施ガイド参照。

					✓ 核セキュリティ体制は、核セキュリティシステムおよび核セキュリティ措置への資源配分を含め、段階的アプローチおよび深層防護に基づく核セキュリティ関連活動の実施において、リスク情報を活用したアプローチを用いる。 ✓ より詳細なガイダンスは NSS 13 等参照。
参考文献	—	References	• “Government Functional Standard GovS007: Security. Cabinet Office.,” [Online]. Available: Government functional standard GovS 007: Security (publishing.service.gov.uk). • “NISR 2003 Classification Policy for the Civil Nuclear Industry (Nov 17),” [Online]. Available: http://www.onr.org.uk/documents/classification-policy.pdf 	—	
用語集	—	Glossary and Abbreviations	CNSS : Civil Nuclear Security and Safeguards CPPNM : Convention on the Physical Protection of Nuclear Material ...	—	
別紙・附属書	—	Appendix	Appendix A : Examples of the Types of Information for Inclusion in a VAI Submission Appendix B : Example VA Process Flow Chart	—	
改訂情報	—	(表紙に記載)	Revision / Issue No., Date など	—	

2.4.2.7 PP1201「核物質防護秘密の管理」と CNS-TAST-GD-7.2 (Issue 2.1) Information Security」における調査の結果

原子力規制庁が用いる検査ガイドPP1201「核物質防護秘密の管理」と、ONRの検査ガイド CNS-TAST-GD-7.2 (Issue 2.1) Information Security」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-7 にまとめた。

2.4.2.7.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.7.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.7.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（核物質防護秘密の管理状況の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官が情報の防護策を評価する際の一般的な助言と情報を提供）について説明している。

2.4.2.7.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（情報セキュリティの重要性、機微な原子力情報(SNI)、関連グッドプラクティス（RGP）の活用、リスク評価のガイダンスなど）を記載している。

2.4.2.7.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ワークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

- ・規制上の期待事項

次の各項目について、検査のポイントを含む解説および検査官の考慮事項を示している。

- ・情報保証戦略、方針、基準
 - 情報保証戦略の解説
 - CS&IA 方針および基準の解説
 - 検査官の考慮事項
- ・データの分類と感度
 - 解説
 - 検査官の考慮事項
- ・機密契約の把握
 - 解説
 - 検査官の考慮事項
- ・第三者サプライヤの CS&IA 評価
 - 解説
 - 検査官の考慮事項
- ・第三者サプライヤの保証
 - 解説
 - 検査官の考慮事項
- ・契約の終了
 - 解説
 - 検査官の考慮事項

2.4.2.7.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.7.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-7 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-7.2 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1201 核物質防護秘密の管理 (2023/05/31 記載の適正化) (3 頁)		英国 ONR 検査ガイド 【ガイド】CNS-TAST-7.2 (Issue 2.1) Information Security (August 2023) (25 頁)		両者間の主な相違点	
項目		主な内容			
図書全体構成		図書全体構成		—	
本文	監督領域	大分類および小分類：「核物質防護」 評価領域：「核物質防護情報の管理」 検査分野：「核物質防護秘密の管理」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	1.1 The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) (Reference 7). This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 (Reference 1). 1.2 The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）
	検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の	2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgement during assessment activities relating to a dutyholders	NRA ・ 検査の目的 ✓ 法的な位置づけと目的（核物質防護秘密の管

	—	種別ごとの防護措置に係る規則条項で規定される核物質防護秘密の管理状況を確認する。当該事項は、法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、核物質防護秘密の管理の検査分野における体制、教育にも留意する。 2.2 防護措置の狙い 核物質防護秘密を厳重に管理することにより、情報漏えいを防止し、不法行為のリスクを低減する。		arrangements to protect information. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholders arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholders responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	理状況の確認) ONR ・本ガイド（TAG）の目的 ✓ 検査官が情報の防護策を評価する際の一般的な助言と情報を提供
	検査要件	3.1 検査対象 核物質防護秘密の管理については、情報管理要領に定められた核物質防護秘密文書の管理等の全てを検査対象とする。なお、核物質防護秘密の文書については、過去 12 か月間または前回検査以降の核物質防護秘密文書の登録、接受、廃棄の記録、情報保護区域の保全記録、秘密情報用 P C 内の記録、核物質防護秘密文書の保管状況、秘密保持事業者の登録、解除等を検査対象とする。 3.2 検査の頻度等 （１）検査の頻度 １年間に１回程度 （２）検査時間 ３人／１．００（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	5. Advice to Inspectors	12. The security of information is essential to maintain civil nuclear operations and ensure public confidence. Therefore, to operate effectively, the civil nuclear industry should maintain the confidentiality, integrity and availability of its SNI . 13. SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise data in various formats (such as digital, hard copy and knowledge) as well as information technology (IT) and operational technology (OT) (equipment or software). It is a dutyholders responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI, computer-based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilized on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should always be considered. 14. Whilst not taking precedent over the legal definitions highlighted in the NISR Classification Policy [6], a simple working definition of SNI can be described as information relating to activities carried out on or in relation to civil nuclear premises; and of value to an adversary planning a malicious act . It includes information which requires a classification in accordance with the NISR Classification Policy. The NISR Classification Policy uses the principles and classifications detailed in the HMG GSC System [5]. The NISR Classification Policy provides descriptions of	NRA ・検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 ・検査手順（概略） ✓ 確認事項 ✓ 文書、ウォークダウン、インタビューを活用して確認 ✓ 検査前準備、検査、CAP 検査の趣旨 ONR ・5. 検査官への助言 ✓ 情報セキュリティの重要性 ✓ 機微な原子力情報（SNI） ✓ SNI のシンプルな定義 ✓ 情報および関連資産は、事業者職員およびサプライチェーン企業により保有される可能性があり、効果的なサイバーセキュリティ&情報保証（CS&IA）方策でそれを保護し、また、あらゆる形態に対応すべき。 ✓ この TAG は、情報保証の国家技術機関（NTA）である国家サイバーセキュリティセンター（NCSC）提供の関連グッドプラクティス（RGP）を大いに活用した他、国際機関、米国を含む様々な RGP 情報を活用。 ✓ リスク評価のアプローチと方法論等に関するガイダンスは、TAGs 7.1（有効なサイバーおよび情報のリスク管理）、7.3（原子力技術および運転の防護）、7.4（情報の物理的防護）参照。
	検査手順	特定核燃料物質の防護のために必要な措置に関する詳細な事項は、当該事項を知る必要があると認められる者以外の者に知られること			ONR ・5.1 規制上の期待事項 ✓ 事業者が、セキュリティ計画に、効果的な

		がないよう管理していることを確認する。また、特定核燃料物質の防護に関する秘密については、秘密の範囲および業務上知り得る者を指定し、管理の方法を定めることにより、その漏えいの防止を図っていることを確認する。さらに、核物質防護秘密の管理が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等によって確認する。 4.1 検査前準備 核物質防護秘密の管理に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する核物質防護秘密の管理が審査基準に適合することを確認する。 4.3 問題点の特定と解決に関する確認 （１）本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 （２）本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。		consequences relating to the nuclear industry that should form part of the basis of judgement when applying a security classification to a specific document. Specific examples for different types of documents and data that may contain SNI are provided in the Classification Guidance at Annex A to the NISR Classification Policy. 15. Information and associated assets may be held by personnel of dutyholders, and their supply chain companies (and/or if SNI is shared with customer/peer organizations), and effective CS&IA arrangements should always address the protection of these assets and in all forms. Information security includes management of classified contracts involving SNI and encompasses all relevant aspects including: • Information Assurance (IA) strategy, policy and standards • Data classifications and sensitivities • Identification of classified contracts • CS&IA assessments of third party suppliers • Assurance of third party suppliers • End of contract 16. This TAG draws heavily on Relevant Good Practice (RGP) provided by National Cyber Security Centre (NCSC) as the National Technical Authority (NTA) for information assurance. Other sources of RGP which support the protection of information includes, but is not limited to, international standards such as International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001 [13] and International Society of Automation (ISA) ISA/IEC 62443 [14], the Information Security Forum (ISF) Standard of Good Practice for Information Security, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework [15]. Advice and guidance on a risk assessment approach and methodology, the protection of IT and OT, and the physical protection of information can be found in TAGs 7.1: Effective Cyber and Information Risk Management [16], 7.3: Protection of Nuclear Technology and Operations [17], and 7.4: Physical Protection of Information [18], respectively. 5.1. Regulatory Expectations 17. The regulatory expectation is that the dutyholder will	CS&IA の維持に役立つ情報保護のアプローチを明確に示していること。 ✓ FSyP 7 - サイバーセキュリティと情報セキュリティ／情報セキュリティ／SyDP 7.2 （事業者は、機微な原子力情報等の機密性、完全性および利用可能性を維持すべき） ONR • 5.2. 情報保証戦略、方針、基準 • 5.2.1. 情報保証戦略 ✓ 事業者は、CS&IA を実施するための首尾一貫した戦略を有すること。戦略の対象範囲は、TAG 7.1 で定義されているリスク管理プロセスの一環として実施されるリスク評価の範囲と同じとすべき。 ✓ 対象範囲には、組織が責任を負う情報および関連資産を保有するパートナー、顧客、サービス提供者およびサプライヤを含める。第三者への要求事項は、強制力を持たせるため、違反した場合の結果とともに契約に明記すべき。 ✓ この戦略は、役員会に正式承認され、サイバー&情報リスク管理を担当するメンバーによって監督されるべき。 ✓ 戦略の実現を促進するために CS&IA のための特別プログラムを検討すべき。 • 5.2.2. CS&IA 方針および基準 ✓ CS&IA 戦略および関連プログラムは、組織に合う包括的な方針体系に裏打ちされるべき。 ➤ 方針は、達成可能で、実施可能で、監査可能であるべき。 ➤ 方針に含むべき項目 ✓ 技術的な CS&IA 方針については、TAG-7.3 参照。 • 5.2.3. 検査官の考慮事項： ✓ 事業者は、組織に適した CS&IA 戦略を策定しているか？ ✓ 情報保証戦略は、組織の戦略目標とどのように整合するか明記しているか？両者が統合されている証拠を提示できるか？事業目的と IT およびセキュリティ目標の整合性を考慮せよ。 ✓ 情報および関連資産に対するリスクを特定し
--	--	--	--	--	--

				ensure that the security plan clearly details their approach to the protection of information in support of maintaining effective CS&IA arrangements. FSyP 7 - Cyber Security and Information Assurance / Information Security / SyDP 7.2 Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets 5.2. Information Assurance Strategy, Policy and Standards 5.2.1. Information Assurance Strategy 18. Dutyholders should ensure that the organization has a coherent strategy to implement CS&IA in all relevant areas of the business. The scope of the strategy should be the same as that of the risk assessment carried out as part of the defined risk management process in TAG 7.1 [16]. 19. The scope should include partners, customers, service providers and suppliers holding information and associated assets for which the organization is responsible. The requirements for third parties should be embodied in contracts along with consequences for non-compliance so that they are enforceable. 20. The strategy should be formally endorsed by the Board and overseen by a member responsible for cyber and information risk management. It should be delivered under a governance structure that defines those roles that ensure it is implemented effectively. 21. A specific programme for CS&IA (or a similar mechanism) should be considered to facilitate delivery of the strategy. The programme should have clear aims and those delivering it should be accountable under governance and reporting arrangements. The scope of the CS&IA programme should be the same as that of the CS&IA strategy with clear line of sight between the two, and with adequate resourcing and support from a communications plan to explain its purpose across the organization (to include third parties). 5.2.2. CS&IA Policy and Standards 22. The CS&IA strategy and its associated programme should be underpinned by a comprehensive policy structure that is tailored to the organization. The policy should be achievable, enforceable and auditable. The topics within the policy should include, but not be limited to, the following:	管理する戦略が適切か？ ✓ 戦略は、それを実現する適時かつ適切なリリース計画により裏付けられているか？ ✓ 事業者は、組織に適用される CS&IA 方針を定めているか？ ➤ 事業者の情報戦略を推進するために使用される文書化された方針があるか？ ➤ その方針は、どのようにして達成可能、強制可能、監査可能か？ ➤ その方針は、組織のどの分野を対象としているか？ ➤ すべての関連事項が適切に取り上げられているか？ ➤ 方針の中で、関連グッドプラクティスを実証する基準への言及があるか？（例：HMG、原子力当局、国際機関）
					ONR ・ 5.3. データの分類と感度 ✓ 事業者は、責任を負う情報と関連資産を明確に理解しておくべき。 ✓ 情報および関連資産には、価値および所有者を割り当てるべき。サイバー&情報リスク管理は、資産の価値を理解し、適切な保護に責任を負うことに依存するため後者は特に重要。 ✓ SyAPs の附属書 F および G は、SNI（処理、保管、伝送に使用される IT 含む）および機器またはソフトウェア（核物質や他の放射性物質を含む活動に関連して使用されるもの）を分類する枠組みを示しており、事業者の分類およびプロセスはこれに適合すべき。 ✓ 事業者は、組織がどのような SNI および関連資産に責任を持ち、どのような形態で、どのような価値を持ち、どこにあるかを正確に記録する情報資産台帳（IAR）を作成し、維持し、適切に保護すべき。 ✓ 事業者は、メタデータを使用して情報および関連資産にマークを付け追跡するために電子データラベリングまたはタグ付けツールの使用を検討すべき。 ✓ IAR の対象範囲には、第三者サプライヤが管理する SNI および関連資産を含めるべき。場合によっては、第三者サプライヤが独自の IAR を維持することを契約上義務付けること

				- Organizational structure - Information asset identification and management - Risk assessment, treatment and management - Records retention - Physical and environmental management - Personnel security & management - System security design - Computer and network security - Operational procedures - Social engineering - Acceptable system use - Security training - Third party management - Incident management - Business Continuity and Disaster Recovery (including pandemic response) - Remote/home working practices - Identification and handling of SNI 23. Technical CS&IA policy measures are described in more detail in TAG-7.3 [17]. Further guidance on CS&IA policy aspects is available from a number of sources including: - HMG (e.g. Centre for the Protection of National Infrastructure (CPNI), NCSC, Cabinet Office) - Nuclear authorities (e.g. ONR, IAEA, IEC, other regulators including the US Nuclear Regulatory Commission and Canadian Nuclear Safety Commission) - International Bodies (e.g. IEC, NIST, ISACA, SANS, ISF) 5.2.3. Inspectors should consider: - Does the dutyholder have a CS&IA strategy in place that is appropriate to the organization? - Does the information assurance strategy state how it will align to the organization’s strategic objectives? Can they provide evidence the two are integrated? Consider how business objectives are aligned to IT and security objectives. - Is the strategy adequate to identify and manage risks to information and associated assets? - Is the strategy underpinned by a timely and appropriately resourced programme to deliver it? - Does the dutyholder have a CS&IA policy in place that is scoped to the organization?	でも達成可能。 ✓ 事業者は、上記「公式-機密 SNI」の保有に関する特定の登録簿を作成し、維持すべき。 ✓ 事業者は、承認された破棄手順およびセキュリティ上承認された破棄機器（TAG 7.4 参照）を使用することで、機密保持レベルを最小化するため文書の廃棄に真摯なアプローチを採用することが奨励される。破棄の記録は登録簿に反映されるべき。 ・ 5.3.1. 検査官の考慮事項： ✓ 事業者は、関連する全ての分類方針にしたがって SNI、機器およびソフトウェアを分類する仕組みおよびプロセスを有しているか？ ✓ 情報および関連資産を適切に識別し、価値、分類、デジタル的または物理的場所を示す登録簿があるか？ ✓ 組織は、サプライチェーンのパートナーによって共有・作成される SNI を管理するための記録を保管しているか？ ✓ 事業者は、上記の 公式—機密:SNI を専用の登録簿に記録しているか？また、適切な文書管理および処理（集積、廃棄、破棄など）を実証しているか？ ONR ・ 5.4. 機密契約の把握 ✓ 事業者は、自身のサイトで SNI を使用して運用されるシステムにサービスを提供する第三者サプライヤと契約を結ぶ場合がある。 ➤ 事業者のリスク管理プロセスに、このようなサービス提供（例：システム管理の外注）関連のリスクを含めるべき。さらに、SNI の特定を「セキュア・バイ・デザイン」プロセスに組み込むべき。 ✓ 事業者は、第三者のサイトまたは IT システムに SNI が含まれるサービスを第三者サプライヤと契約する場合もある。その場合でも、事業者は SNI に常に責任を負うことに変わりはない。 ✓ 事業者は、SNI が移転されるまたは契約の一部として発生することを特定する仕組みを持つべき。 ➤ サプライチェーン全体について各契約の様々なリスクレベルを把握し、SNI 保護を確実にすべき。
--	--	--	--	--	---

			○ Is there a documented policy which is used to drive the dutyholders information strategy? ○ How is the policy made to be achievable, enforceable and auditable? ○ What areas of the organization does the policy cover? ○ Are all relevant topics adequately addressed? ○ Within the policy, is there reference to standards to demonstrate relevant good practice? (e.g. HMG, Nuclear Authorities, International Bodies)? 5.3. Data Classification and Sensitivities 24. It is imperative that dutyholders should have a clear understanding of information and associated assets for which they have responsibility. This is reinforced in the qualifying text in SyAPs under SyDP 7.2, which states that dutyholders should establish mechanisms and processes within their organization to ensure assets are properly classified in accordance with all relevant classification policy. 25. Information and associated assets should be ascribed a value and an owner. This latter element is crucial because effective cyber and information risk management relies upon understanding of the value of assets and responsibility for ensuring that they are protected adequately. 26. Annexes F and G to the SyAPs provide a framework for categorizing SNI (including IT used for processing, storage or transmission) and equipment or software (used in connection with activities involving nuclear material and other radioactive material), with which a dutyholders classification mechanisms and processes should fit within. 27. Dutyholders should create, maintain and appropriately protect an Information Asset Register (IAR) or similar mechanism that is an accurate record of what SNI and associated assets the organization is responsible for, what format they are in, what value they have and where they are located. 28. Dutyholders should consider the use of electronic data labelling or tagging tools to mark and track information and associated assets using metadata. 29. The scope of the IAR should include SNI and associated	➤ このアプローチは、産業界の負担軽減を目的とする ONR の「リスク集中」原則に盛り込まれている。 ➤ 事業者は、自身または第三者が使用するどの施設が ONR の日常的な監視の範囲内に入るべきか決定する独自の指針を確立し、文書化する。 ➤ そのような施設は、リスト N ポータルでの処理を通じて ONR に通知されるべき。 ➤ 事業者はまた、「リスク集中」の閾値を下回ると判断される SNI 取扱い施設のリストを保持し、ONR の適切なサンプリングとプロセスの保証を実施可能とすべき。 ➤ 付録 1 にリスク集中の原則を示す。 ✓ 事業者は、調達チームが各契約に適用できる限定された基準を持つ手順書の実施を検討すべき。 ➤ ONR の「内在的リスクプロファイル質問票」は、このリスクを確定するための方法の一例である。 ➤ リスト N ポータルを利用する事業者はこの方法を利用するが、他の事業者のアプローチで補完される場合もある。 ✓ 事業者の調達チームおよびプロジェクトチームは、各契約の関連情報および関連資産を正しく識別できるように体系的な訓練を必要とする場合がある。 ✓ 内閣府契約プロセスの要件に従い、事業者は、サービスまたは物品の契約に入札する企業に、特定の契約が SNI 資産に関わるものであることを警告する手段を持つべき。 ✓ 事業者は、SNI 資産に関わる全ての第三者契約の中央登録簿を維持すべき。 ✓ 登録簿は、定期的に独立したレビューを受けべき。契約がリストに追加または削除された場合、リスク見直しのトリガーとして機能すべき。 ・ 5.4.1. 検査官の考慮事項： ✓ 事業者は、プロジェクトや計画に対して「セキュア・バイ・デザイン」プロセスの一環として SNI の早期特定を奨励しているか？ ✓ 事業者は、第三者と締結している SNI および関連資産に関わる契約を明確に特定することができているか？また、どのように管理・維持されているか？
--	--	--	---	---

				assets managed by third party suppliers. In some circumstances this can be accomplished by a contractual obligation for them to maintain their own IAR. It should be subject to maintenance and review on a regular basis to confirm that its contents are accurate. 30. Dutyholders should create and maintain a specific register for holdings of above OFFICIAL-SENSITIVE SNI (including legacy documents classified CONFIDENTIAL where appropriate). Appropriate document control and accounting should accurately reflect: • What SNI information and associated assets the organization is responsible for, what format they are in, and what classification they are. • Where they are located (final and temporary disposal). Details of who the responsible and supervisor officers are for the register upkeep and maintenance and indicate when they assumed the role. • A structured approach to mustering documents/assets and when these checks have occurred (a 100% documents/assets muster should be conducted on hand over/take over whenever the incumbents of the responsible officer or supervisor roles are changed). • If copies of SNI have been formally issued by the dutyholder – both internally and externally – with evidence of a signed receipt. • All live entries and provide an audit of legacy document control and accounting. 31. Dutyholders are encouraged to adopt a diligent approach to document weeding (purge) to minimize levels of classified holdings through approved destruction procedures and using security approved destruction equipment (refer to TAG 7.4 [18]). A record of the date, responsible person(s) and witness signatures, and the method used for the destruction of above OFFICIAL-SENSITIVE SNI should be reflected in the register. SNI accounted for in the register should be cross-referenced back to the register. 5.3.1. Inspectors should consider: • Does the dutyholder have mechanisms and processes in place to categorize SNI, equipment and software in accordance with all relevant classification policy? • Is there a register which adequately identifies	✓ そのような契約に内在するサイバーリスクや情報リスクを評価する仕組みがあるか? ✓ 第三者との契約において、保有および／または生成情報および関連資産、並びにその機密性を特定する仕組みがあるか? ➤ その仕組みはサプライチェーン全体で利用され効果的に管理されているか? ➤ 主要なセキュリティ文書が、契約期間を通じて改訂されたコピーを含め、第三者に提供されているか? ➤ 第三者との間で、SNI に関連する保証に関する期待事項を明確にし、強化するための契約締結会議が開催されているか? ➤ 事業者は、SNI の資産に関わる全ての第三者との契約を一元的に登録しているか? ONR • 5.5. 第三者サプライヤの CS&IA 評価 ✓ 評価は、リモート（質問票）、検査および監査、または複数アプローチの組み合わせで行える。 ➤ 事業者は、どのアプローチが十分な保証を提供するか検討すべき。 ➤ ONR は第三者サプライヤへの直接介入を行う場合があるが、サンプルベースで行われることに注意。 ➤ したがって、事業者は、独自の保証およびデューデリジェンス活動の代わりに ONR の介入に頼るべきではない。 ➤ 事業者が独自にサイト調査する場合、様々な CS&IA 方法論（例を列挙）の特徴を考慮すべき。 ➤ セキュリティ管理チェックリストだけでなく、結果重視のアプローチを検討すべき。 ➤ アプローチについては、SyAPs の FSyP 7 および関連の付属書 F ～ J 参照。 ✓ ONR は、SyAP に示す原則に反する証拠を収集するために設計された「期待事項の証明」質問セットを開発した。次の原則の証拠を確認する。 • FSyP 1 – セキュリティのためのリーダーシップとマネジメント • FSyP 2 – セキュリティ組織文化 • FSyP 3 – 能力管理 • FSyP 7 – サイバーセキュリティと情報保証 • FSyP 8 – 従業員の信頼性。 ✓ これらは、固有のリスクプロファイルレベル
--	--	--	--	---	--

				information and associated assets, which denotes value, classification and digital or physical location? • Does the organization keep records to control SNI shared and produced by supply chain partners? • Does the dutyholder account for above OFFICIAL-SENSITIVE:SNI in a dedicated register? If so, does this demonstrate appropriate document control and accounting (such as mustering, disposal and destruction)? 5.4. Identification of Classified Contracts 32. Dutyholders may have contracts with third party suppliers to provide services to systems operating with SNI on the dutyholders’ own sites. The dutyholders risk management process should include any relevant risks from such service provision (e.g., outsourcing of IT system management). Additionally, dutyholders should embed the identification of SNI into a ‘Secure by Design’ process as contracting is often directly integrated into project and programme activity. 33. Dutyholders may also have contracts with third party suppliers for services involving SNI on the third-party sites or IT systems. In such circumstances dutyholders should be aware that they are responsible for the SNI with which they have been entrusted at all times and that this remains the case when they have outsourced a particular service either partially or completely to a third party. 34. Dutyholders should have a mechanism that will identify if SNI is going to be transferred (by any means) or generated as part of the delivery of a specific contract to any third party. The intention is that dutyholders should be able to identify the different levels of risk for specific contracts throughout their supply chain and assure themselves that SNI will be protected. This approach is captured in an ONR principal termed “concentration of risk” that aims to reduce the scope of routine regulatory attention to those areas that present the greatest risk to SNI, consequently reducing the regulatory burden on Industry. 35. This principal is generally used in relation to a specific facility by applying several factors to scope areas subject to routine regulatory attention. Dutyholders should use these factors to establish and document their own	に整合する。リスト N ポータルを利用する事業者はこの方法を利用するが、他の事業者のアプローチで補完される場合がある。 ✓ 事業者は、第三者評価を実施する体系的アプローチを持つべき。 ✓ 第三者の CS&IA 対策の妥当性評価の際、事業者は、組織がベストプラクティスを満たすセキュリティ対策を講じられ、深層防護アプローチで互いに補完し合っていることを確認すべき。 ✓ サイトの物理的セキュリティ調査の実施に関する助言は、CPNI および他の組織から入手可能。物理的セキュリティ要件の詳細は、TAG 7.4 参照。 ・ 5.5.1. 検査官の考慮事項: ✓ 事業者が第三者の CS&IA 契約を評価するために確立された方法があるか? ✓ 評価ではどのような第三者のセキュリティ対策が強調されているか? ✓ 事業者が第三者企業の CS&IA 成熟度を評価するために用いる方策は適切か? ✓ 方策はサプライチェーンを適切に管理しているか? ✓ 方策は SyAP に一致しているか? ✓ 評価の中で既知の評判の良い方法論への言及があるか? ✓ 問題が発生した場合に問題を確実に解決するためのプロセスがあるか? ✓ 特定された問題を速やかに報告し対処するプロセスがあるか? これにより、あらゆる問題の迅速な管理が促進されるか? 呼び出し（call out）事象の報告が含まれているか? ✓ 方策では、対象組織の状況を考慮した一貫性のある監査可能な結果を生み出す構造化されたアプローチが使用されているか? ✓ 事業者は、SNI の共有または作成を含む国内外第三者組織との関係の開始と完了を ONR に通知するメカニズムを導入しているか?
					ONR ・ 5.6. 第三者サプライヤの保証 ✓ 検査官は、事業者が契約期間全体を通じて第三者のサイバーおよび情報リスク管理の有効

				guidance for determining which facilities, used by the dutyholder or one of their third parties, should fall inside the scope of ONR’s routine regulatory attention. ONR should be informed of such facilities, likely through being processed through the List N Portal . Dutyholders should also maintain a list of facilities, where SNI is handled, which are deemed to fall below the ‘concentration of risk’ threshold, enabling ONR to undertake appropriate sampling and assurance of their process. Appendix 1 expands on the concentration of risk principal. 36. Dutyholders should consider implementing a procedure with a limited set of criteria which can be applied by procurement teams to each contract. This list of questions can operate as part of a risk assessment for each contract providing a value for the level of risk regarding the impact of the compromise of the information and associated assets. The Inherent Risk Profile Questionnaire [19], developed by ONR, is an example method for establishing this risk. Dutyholders utilizing the List N Portal will make use of this methodology, but it may be supplemented by other dutyholder approaches. 37. Dutyholder procurement and project teams may require some structured training to confirm that they can correctly identify relevant information and associated assets for each contract. Dutyholders should develop standards, procedures, and arrangements to ensure third parties are made aware of and provided with key information security documentation such as company SNI identification and handling guidance, and incident reporting and handling procedures as part of the contract security aspects letter. They should be made aware of any revisions to this key documentation throughout the contract period. Dutyholders should also consider holding a contract inaugural meeting with third parties to underline and reinforce SNI related assurance expectations and other security related topics such as the reporting and escalation of security incidents/issues, site security policies and practices, and remote working practices etc. 38. In accordance with the requirements from the Cabinet Office Contractual Process [20], dutyholders should have a means of alerting companies bidding for contracts	性を監視するメカニズムを備えていることを確認すべき。 ➤ 事業者は、毎年、少なくとも評価のレビューを行うことが良好事例。 ➤ 事業者は、合意された頻度でまたは報告対象事象を踏まえて、第三者の CS&IA レビュー（専用のセキュリティ・アスペクト・ト レター (SAL) を通じた契約条件の一部）を開始するプロセスを持つべき。 ✓ CS&IA リスク管理体制に影響する変更があった場合に事業者に通知されるような条件をプロセスに組み込むべき。 ✓ 第三者組織のリスク管理で欠陥が特定された場合、懸念事項にタイムリーに対処するメカニズムが必要。 ✓ 事業者は、第三者組織での SNI のリスク管理を独自のリスク管理構造に統合するあらゆる努力を払うべき。 ✓ 共通のガバナンス構造は、懸念事項を可視化し、問題に対する可能な解決策を共有するのに便利な方法。そのような構造の 1 つがセキュリティ・ワーキング・グループ。第三者 サプライヤや規制当局などの外部専門家を含めることもできる。 ・ 5.6.1. 検査官の考慮事項 ✓ 事業者は、第三者企業の CS&IA 方策を継続的に評価およびレビューするメカニズムを備えているか? ✓ 第三者サプライヤは、下請け契約に関連する活動を管理・保証する方策を含め、セキュリティ体制に影響する可能性のある変更を契約組織に通知する義務があるか? ✓ このような問題が特定された場合の報告プロセスとガバナンス構造はどのようなものか? ✓ 評価結果は適切な報告によりフィードバックされ、リスクレジスターなどの事業者の中央リスク管理機能に反映されているか? ✓ 適切なガバナンス構造があるか? ✓ 上記の期待事項は、SAL を通じて契約上の方策の中で定義されているか? ONR ・ 5.7. 契約の終了 ✓ 事業者と第三者請負業者間で、契約期間終了
--	--	--	--	---	---

				for services or goods that a particular contract will involve SNI assets. 39. Dutyholders should maintain a central register of all third-party contracts involving SNI assets. This register will record which companies are operating with SNI and for what period of time. It may also record details such as the classification of SNI held, details of IT systems processing SNI and potential access to the dutyholders own IT systems or shared cloud environments. 40. The register should be independently reviewed periodically to confirm that it is current. It should function as a trigger for reviews of risk when contracts are added or removed from the list. The register should also capture details of subcontracts that may involve SNI. 5.4.1. Inspectors should consider: • Does the dutyholder encourage the early identification of SNI as part of a ‘Secure by Design’ process for projects and programmes? • Are dutyholders able to clearly identify contracts they have with third parties that involve SNI and associated assets, and how are these managed and maintained? • Do they have a mechanism for assessing the inherent cyber and information risk for such contracts? • Is there a mechanism for identifying in third-party contracts the information and associated assets that will be held and/or generated, and their sensitivity? - o Is this mechanism used down the supply chain and managed effectively? - o Is the third party provided with key security documentation, including revised copies throughout the contract period? - o Is a contract inaugural meeting held with the third party to underline and reinforce SNI related assurance expectations? - o Does the dutyholder maintain a central register of all third party contracts involving SNI assets? 5.5. CS&IA Assessments of Third-Party Suppliers 41. Assessing third party suppliers can be undertaken remotely (using questionnaires), directly by inspection and audit or by a combination of approaches. Dutyholders should consider which approach provides them with adequate assurance, although sample	時に情報および関連資産がどうなるか明確に理解されるべき。 ✓ 契約終了時のデータ管理アプローチは、合理的な期間内に同様の作業で再契約する可能性があるかどうかによって異なる。そのような場合、事業者はリスクベースのアプローチを取れる。 ✓ 情報および関連資産が正式な契約期間を超えて第三者に保持される場合、事業者はそれが適切に保護されていることを保証すべき。 ✓ 後続の契約要件がない場合、事業者はすべての情報と関連資産を安全に返却または破棄するプロセスを持つべき。 ➤ 機密情報を破棄する適切な方法に関するガイダンスは、TAG 7.4 参照。 ✓ 事業者は、TAG 7.4 に示される現行の NTA の RGP にしたがって、情報と関連資産が適切に返却または破棄された時期を特定する資産管理プロセスを持つべき。 ✓ 第三者サプライヤが SNI を保持する正当な必要性がある場合、ONR による規制介入の対象となることに注意。 ・ 5.7.1. 検査官の考慮事項 ✓ 事業者は、情報および関連資産を含む第三者企業との契約終了を管理するプロセスを持っているか? - o 契約条件を通じて強制できるか? - o 事業者は、契約終了後も第三者が SNI を取り扱う状況に対処するメカニズムを備えているか? ✓ 第三者の情報および関連資産を返却または安全に破棄するための確立されたプロセスはあるか? どのようなものか? ✓ 契約終了プロセスの一環として SNI を安全に処分する適切な方策が、現在の NTA の RGP に沿って、関連の標準、手順書、方策に盛り込まれているか? ✓ 資産の移転と破棄の証拠を求めるプロセスがあり、これは事業者の資産およびリスク管理登録簿に反映されているか? ✓ 情報および関連資産が正式な契約期間後も第三者に残る場合、適切かつ十分な保護が保証されるか?
--	--	--	--	--	--

				checking should be established where a remote method is relied upon. It should be noted that whilst ONR may conduct direct interventions of third-party suppliers, such activities are undertaken to meet regulatory objectives and are done so on a sampling basis. Dutyholders should not therefore rely upon ONR interventions in lieu of their own assurance and due diligence activities. 42. Dutyholders undertaking their own site survey should consider features from CS&IA methodologies such as: NCSC 10 Steps to Cyber Security [21], the IASME Consortium Cyber Essentials Standard [22], the Center for Internet Security 18 CIS Critical Security Controls [23], NIST Cybersecurity Framework [15], or Annex A of ISO/IEC 27001 [13] amongst others. Consideration should be given to an outcome focused approach rather than just a checklist of security controls. Such an approach is described in SyAPs FSyP 7 and the associated Annexes F to J and will better prepare third party suppliers for any subsequent ONR intervention activity. 43. ONR has developed the ‘Evidencing Expectations’ question sets [24] which are designed to capture evidence against the principles found in SyAPs: • FSyP 1 – Leadership and Management for Security • FSyP 2 – Security Organizational Culture • FSyP 3 – Competence Management • FSyP 7 – Cyber Security and Information Assurance • FSyP 8 – Workforce Trustworthiness. 44. These are aligned to the inherent risk profile levels [19]. Dutyholders utilising the List N Portal will make use of this methodology, but it may be supplemented by other dutyholder approaches. 45. Dutyholders should have a structured approach to the conduct of third-party assessments. The approach must be recordable and repeatable so that results are consistent and should consider the following stages: • A clearly defined scope for the assessment. • A process for a review of available evidence to include CS&IA Strategy, CS&IA Policy, Cyber Risk Management approach, Physical Security Plan, Business Continuity and Disaster Recovery plans, Information Asset Register, Risk Register, third party classified contract register, personnel security	
--	--	--	--	--	--

				management, reports from IT Health Checks and technical scans and reports from the incident management process. • A process for a physical review (internal and external) of security features. Physical and environmental security controls for the protection of SNI should be applied according to layering principles and based on a risk assessment to determine applicable threats and risks in line with guidance set out by the CPNI, as the NTA for Protective Security. • A mechanism to identify and interview key roles in the organization to determine if management functions are in place and effective. • A sampling function could be used to review security controls to confirm that they are effective. • A reporting function that summarizes assessment results in a consistent and traceable manner that can be highlighted to managers and escalated appropriately. • A process to follow up on identified areas of concern to ensure that they are addressed. 46. When assessing the adequacy of third-party CS&IA measures, dutyholders should assure themselves that the organization has security measures that meet current good practice and that these measures complement each other in a defense in depth approach. They should also confirm that these measures are implemented by effective procedures and that they are governed by an appropriate management structure. They should consider: • Has the third party defined ownership of security at a senior level within the business? • Is cyber and information risk management in place and effective? • Is the third party physical and personnel security adequate? • Is third party security for information and associated assets adequate? • Are both aspects supported by appropriate procedures? • Does the third party have its own mechanism for gaining independent assurance of its CS&IA arrangements?	
--	--	--	--	---	--

				47. Advice on the conduct of a site physical security survey is available from CPNI and other organizations. Details of physical security requirements are in TAG 7.4 [18]. 5.5.1. Inspectors should consider: • Is there an established method for dutyholders to assess third party CS&IA arrangements? • What third party security measures does the assessment highlight? • Are the arrangements used by dutyholders to assess CS&IA maturity for third party companies adequate? • Do the arrangements manage down the supply chain appropriately? • Are the arrangements consistent with SyAPs? • Is there any reference to known, reputable methodologies within the assessment? • Is there a process for ensuring that any issues identified are reported promptly and addressed? Does this encourage a prompt management of any issues? Does it include call out incident reporting? • Do the arrangements use a structured approach that produces consistent, auditable results that take account of the context of the organization in scope? • Does the dutyholder have a mechanism in place for notifying ONR of the initiation and completion of relationships with third party organizations, domestically and internationally, involving the sharing or creation of SNI? 5.6. Assurance of Third-Party Suppliers 48. Inspectors should assure themselves that dutyholders have a mechanism in place to monitor the effectiveness of third party cyber and information risk management throughout the period of their contracts. It is considered good practice that there is at least a review of the assessment on an annual basis and dutyholders should have a process to initiate reviews of third-party CS&IA (this should be part of the contract conditions through a dedicated Security Aspects Letter (SAL) or similar) on an agreed frequency or in response to a notifiable event. The periodicity of review could reflect the level of risk for the contract or the CS&IA maturity of the relevant third-party company as defined by the assessment process. 49. Conditions should be built into the process to ensure that	
--	--	--	--	--	--

				dutyholders are notified in the event of changes that affect the CS&IA risk management posture of the third-party such as: • A security incident that has or could compromise information and associated assets • Changes to the business, technology or threats • Changes of location, company ownership and of security managers 50. In the event that deficiencies are identified in third party contractor risk management, a mechanism is required to address concerns in a timely manner. The requirement for the contractor to do this should be built into the contract and this could include financial penalties for either a failure to address issues completely or for a failure to address them in an agreed timeframe. The dutyholder should also be able to demonstrate notifying the third party of their legal obligations under NISR, as a result of handling SNI and their subjection to ONR regulation as a result. 51. Dutyholders should make every effort to integrate the management of risks to SNI in third party organizations with their own risk management structure. This should include the sharing of threat information, good practice, incident lessons learned or technology changes. 52. A common governance structure could be a useful way of providing visibility of concerns and of sharing possible solutions to problems. One such structure is the Security Working Group which can run both internally within an organization, but which could usefully include third party suppliers as well as external expertise from regulators and others. 5.6.1. Inspectors should consider: • Does the dutyholder have a mechanism to assess and review CS&IA arrangements for third party companies on a continuing basis? • Are third party suppliers obliged to inform the contracting organization of any changes which might impact their security posture – including arrangements to control and assure activities involving sub-contracts? • What is the reporting process and governance structure if such issues are identified? • Are the results of the assessments fed back by adequate reporting and are they reflected in	
--	--	--	--	---	--

				dutyholder central risk management functions such as the risk register? • Is there an adequate governance structure? • Are the above expectations defined in contractual arrangements i.e. through a Security Aspects Letter (SAL) or similar? 5.7. End of Contract 53. There should be a clear understanding between dutyholders and third-party contractors of what will happen to information and associated assets at the end of the contract period, or the end of the period during which the contractor is required to hold the information and associated assets (whichever is longer). The dutyholder should ensure that the requirements around this are made clear at the outset of the engagement and are embedded in the contract. This is because in many instances the requirements will need to be included in the technical solution and will have cost implications for delivering the contract to both parties. 54. The approach to data management at the end of a contract will vary dependent upon if there is a likelihood of a re-engagement on similar work within a reasonable time frame. In such an event dutyholders could take a risk-based approach. 55. If information and associated assets are retained by the third party for any time beyond the formal contract, dutyholders should assure themselves that it remains appropriately protected. However, dutyholders may also consider having all information and associated assets returned to them regardless and store it themselves until a fresh contract is in place. 56. Assuming that there is no follow-on contract requirement, dutyholders should have a process for all information and associated assets to be either returned or destroyed securely. Dutyholders should have a registry of exactly what type and sensitivity of information and associated assets are held, in what format, and by which third party contractors. The register should be used to issue instructions on which assets are to be returned and which destroyed securely, and how. Further guidance on the appropriate methods of destroying classified information can be found in TAG 7.4 [18]. 57. Dutyholders should ensure that they have an asset	
--	--	--	--	--	--

				management process that identifies when information and associated assets have been returned or destroyed appropriately in line with current NTA RGP as provided in TAG 7.4 [18]. This process should be supported by evidence such as destruction certificates and data transfer documentation. For legal, contractual and financial reasons, information relevant to the contract may need to be retained for a number of years. It is unlikely but still possible that SNI may be contained in that material. Dutyholders should consider a risk managed approach on how it is to be protected and should assure themselves that third parties are aware of the need to protect it adequately for as long as it is held. In these cases, dutyholders should continue their management of the contractor CS&IA risk as before, but potentially with redefined assurance timescales and review milestones. 58. It should be noted in instances where third party suppliers have a legitimate need to retain SNI, they remain subject to regulatory interventions by ONR. 5.7.1. Inspectors should consider: • Does the dutyholder have a process to manage the closure of contracts with third party companies involving information and associated assets? - o Is it enforceable through conditions within the contract(s)? - o Does the dutyholder have a mechanism for handling situations where the third party is required to handle SNI beyond the closure of the contract? • Is there an established process for returning or securely destroying information and associated assets from third parties, if so, what is it? • Are there adequate arrangements captured in relevant standards, procedures and arrangements, in line with current NTA RGP, for the secure disposal of SNI as part of the end of contract process. • Is there a process that requires evidence of asset transfer and destruction and is this reflected in the dutyholder asset and risk management registers? • If information and associated assets stay with the third party post formal contract period, what is the assurance for appropriate and adequate protection?	
--	--	--	--	---	--

	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant Legislation	4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ...	ONR ・英国の関連法との関係 ✓ NSIR における用語の定義と NM&ORM に関する要件 ✓ セキュリティに関する政府機能基準 ➤ サイバー、物理、人員、技術、事象の管理に関するセキュリティ・リスク管理、計画、対応活動に対する期待事項を示す。 ✓ 政府セキュリティ分類（GSC） ➤ NISR 分類方針とともに、SNI を含む情報の種類、適用すべきセキュリティ分類レベル、その管理と運用全体にわたり実施すべき保護対策を示す。
			4. Relationship to Security Assessment Principles and IAEA Security Standards and Guides	8.The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholders security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholders submission demonstrating they have effective processes in place to achieve SyDP 7.2 – Information Security, in support of FSyP 7 – Cyber Security & Information Assurance. This TAG is consistent with other TAGs and associated guidance and policy documentation. ...	ONR ・セキュリティ評価原則（SyAP）と IAEA セキュリティ標準およびガイダンスとの関係 ✓ SyAP は、事業者のセキュリティ方策の有効性について一貫した規制判断を行うための枠組みを ONR 検査官に提供。 ➤ 本 TAG は、検査官が「FSyP 7 – サイバーセキュリティと情報保証」をサポートする「SyDP 7.2 – 情報セキュリティ」を実証する事業者の提出書類を評価する際のガイダンスを提供。 ✓ 国の核セキュリティ体制の必須要素は、核物質防護条約（CPPNM）および IAEA 核セキュリティ基本文書に規定、ガイダンスは、IAEA 技術ガイダンスおよび実施ガイド参照 ✓ より詳細なガイダンスは NSS 13 等参照。
参考文献	—	—	References	・ ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” 2017. ・ HM Government, “The Nuclear Industries Security Regulations 2003 (NISR),” 2003.. ...	—
用語集	—	—	Glossary and Abbreviations	CA : Contracting Authority CPNI : Centre for the Protection of National Infrastructure ...	—
別紙・附属書	—	—	Appendix	Appendix 1 : Concentration of Risk	—
改訂情報	変更日、施行日、変更概要（「記載の適正化」）	（表紙および本文前に記載）		・ Revision / Issue No., Date など ・ Table 1 - Revision commentary	—

2.4.2.8 PP1202「管理情報の管理」と CNS-TAST-GD-7.4 (Issue 2)「Physical Protection of Information」における調査の結果

原子力規制庁が用いる検査ガイド PP1202「管理情報の管理」と、ONR の検査ガイド CNS-TAST-GD-7.4 (Issue 2)「Physical Protection of Information」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-8 にまとめた。

2.4.2.8.1 監督領域

原子力規制庁では、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.8.2 序論

原子力規制庁では、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.8.3 検査の目的

原子力規制庁では、法的な位置づけと目的（管理情報の管理状況の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官が情報および情報資産の防護策を評価する際の一般的な助言と情報を提供）について説明している。

2.4.2.8.4 検査要件

原子力規制庁では、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（機微な原子力情報(SNI)、管理、情報および関連資産の効果的な物理的な管理、関連グッドプラクティスの活用など）を記載している。

2.4.2.8.5 検査手順

原子力規制庁では、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ワークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

- ・ 規制上の期待事項（事業者に求められること、該当する FSyPs）
- の各項目について、検査のポイントを含む解説および検査官の考慮事項を示している。

- ・ 物理的セキュリティのリスク評価
 - ✓ 解説
 - ✓ 検査官の考慮事項
- ・ 物理的セキュリティの管理方策の解説
 - ✓ 設備の置き場所の解説
 - ✓ ケーブルのセキュリティの解説
 - ✓ 電磁波盗聴（TEMPEST）と電磁波セキュリティ(EMS)の解説
 - ✓ リムーバブル・メディアの管理の解説
 - ✓ リモート／在宅勤務およびモバイル・デバイスの解説
 - ✓ 資産の確実な処分の解説
 - ✓ セキュリティ管理システムー保護およびレジリエンスの解説
 - ✓ 環境の管理の解説
- ・ 検査官の考慮事項

2.4.2.8.6 法令・基準等

原子力規制庁では、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.8.7 改訂情報

原子力規制庁では、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4.2-8 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-7.4 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1202 管理情報の管理 (2023/05/31 記載の適正化) (2 頁)		英国 ONR 検査ガイド 【ガイド】CNS-TAST- GD-7.4 (Issue 2) Physical Protection of Information (April 2022) (29 頁)		両者間の主な相違点	
項目		主な内容			
図書全体構成		図書全体構成		—	
事業者	監督領域	大分類および小分類：「核物質防護」 評価領域：「核物質防護情報の管理」 検査分野：「管理情報の管理」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	1. ONR has established its assessment principles, which apply to the assessment by ONR specialist inspectors of safety, security and safeguards submissions for nuclear facilities or transports that may be operated by potential licensees, existing licensees, or other dutyholders. These assessment principles are supported by a suite of guides to further assist ONR’s inspectors in their technical assessment work in support of making regulatory judgements and decisions against all legal provisions applicable for assessment activities. This technical assessment guide (TAG) is one of these guides. 2. The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. Dutyholders under Regulation 22 of the Nuclear Industries Security Regulations 2003 (‘NISR 2003’) [1] may also use the ONRs Security Assessment Principles (SyAPs) [2] as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This TAG is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）

	検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される管理情報の管理状況を確認する。当該事項は、法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、管理情報の管理の検査分野における体制、訓練・教育および設備の保全にも留意する。 2.2 防護措置の狙い 管理情報を適切に管理することにより、情報漏えいを防止し、不法行為のリスクを低減する。	2. Purpose and Scope	This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities relating to a dutyholder's arrangements for the protection of information and information assets. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder's arrangements. It does not prescribe the methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder's responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（管理情報の管理状況の確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官が情報および情報資産の防護策を評価する際の一般的な助言と情報を提供
	検査要件	3.1 検査対象 情報管理要領に定められた管理情報文書の管理状況等の全てが検査対象となり得るが、本検査では、作成された管理情報文書の確認については、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、管理情報の管理状況を考慮し、検査対象を選定する。なお、検査対象は、過去 12 か月間または前回検査以降の文書等とする。 2.2 防護措置の狙い 管理情報を適切に管理することにより、情報漏えいを防止し、不法行為のリスクを低減する。 3.2 検査の頻度等 （1）検査の頻度 3 年間に 1 回程度 （2）検査時間 3 人／0. 5 0（h） 3.3 実施体制 （1）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （2）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	5. Advice to Inspectors	13. SNI is information relating to activities carried out on or in relation to civil nuclear premises which needs to be protected in the interests of national security. Information and associated assets comprise data in various formats (such as digital and hard copy) as well as information technology and operational technology (equipment or software). It is a dutyholder's responsibility to determine which information and associated assets are considered relevant. However, hard copy SNI and computer-based systems that store, process, transmit, control, secure or access SNI should always be included; and technology stored or utilised on the premises in connection with activities involving nuclear or other radioactive material relating to either nuclear safety or nuclear security, should always be considered. Appendix 1 of CNS-TAST-GD-7.2 [10] provides a description of SNI and a flow chart to assist in its identification. 14. Controls are the primary components to consider when developing an information security strategy and can be physical, technical or procedural. The choice of controls must be based on a number of considerations including ensuring their effectiveness in mitigating assessed risks and what the optimal form the control will be. 15. Effective physical protection of information and associated assets encompasses all relevant aspects of: - Physical security risk assessment - Physical security control measures - Assurance of physical control measures	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 ONR 5. 検査官への助言 ✓ 機微な原子力情報（SNI）とは。CNS-TAST-GD-7.2 の付録 1 に SNI の説明と識別に役立つフォローチャートあり。 ✓ 管理（controls）は、情報セキュリティ戦略を策定する際に考慮すべき主要な要素であり、物理的、技術的、または手続き的なもので、多くの考慮事項に基づくべき。 ✓ 情報および関連資産の効果的な物理的保護は、物理的セキュリティ・リスク評価、物理的セキュリティ管理、物理的管理の保証のすべてを含むべき。 ✓ 本 TAG は、国家技術機関（NTA）の CPNI（英国インフラ防護センター）と NCSC（英国サイバーセキュリティセンター）が提供する関連グッドプラクティス（RGP）を多く利用。その他、海外のグッドプラクティスもある。

				16. This TAG draws heavily on Relevant Good Practice (RGP) provided by CPNI and NCSC as the National Technical Authorities (NTAs). Other sources of RGP which support the physical protection of information includes, but is not limited to, international standards such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 [11] and IEC 62443 [12], the Information Security Forum (ISF) Standard of Good Practice for Information Security, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Advice and guidance on a risk assessment approach and methodology can be found in CNS-TAST-GD-7.1 [13].	
検査手順		管理情報について、特定核燃料物質の防護に関する秘密に準じた情報管理を行っていることを確認する。また、管理情報の管理が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等によって確認する。 4.1 検査前準備 管理情報の管理に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する管理情報の管理が審査基準に適合することを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	Regulatory Expectation	17. The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements for the physical protection of information and associated assets in support of maintaining effective CS&IA arrangements. FSyP 7 - Cyber Security and Information Assurance / Physical Protection of Information / SyDP 7.4 Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.	ONR ・ 5.1 規制上の期待事項 ✓ 効果的なCS&IA（サイバーセキュリティ&情報保証）方策の維持に役立つ情報および関連資産の物理的保護方策をセキュリティ計画に明確に記載すること。 ✓ FSyP 7-サイバーセキュリティと情報保証／情報の物理的保護／SyDP 7.4 （事業者は、情報および関連資産が様々な脅威から確実に保護されるよう、適切な物理的保護手段を採用すべき。）
			7. Physical Security Risk Assessment	18. Physical and environmental security controls for the protection of SNI should be applied according to layering principles and based on a risk assessment to determine applicable threats and risks in line with guidance set out by CPNI. 19. Inspectors should gain assurance that a comprehensive physical security risk assessment has been undertaken. The scope of the assessment should be clearly defined and should derive some of its input from the work to identify and classify information and associated assets (see CNS-TAST-GD-7.3 [14] for further guidance). The purpose of the risk assessment is to ensure that all relevant risks are identified so that they can be managed effectively in the context of the business. If the risk assessment is conducted early in the process to deliver new capabilities or upgrades to existing facilities, then physical security can be built in at the outset which is far more effective. 20. Where information and associated assets are located on	ONR ・ 7. 物理的セキュリティのリスク評価 ✓ SNI 保護のためのセキュリティ管理は、CPNI のガイダンスを参照し、階層化の原則およびリスク評価に基づくべき。 ✓ 検査官は、包括的な物理的セキュリティのリスク評価が実施済みであることを確認すべき。 ✓ 核物質（NM）および他の放射性物質（ONM）並びに原子力施設に対する悪意ある行為のリスクを評価するために、物理的セキュリティ評価が完了し、包括的な物理的保護システムが設計されているはず。このリスク評価は、盗取および妨害破壊行為の両方を十分に考慮すべきであり、これらの脅威を緩和するための管理は既に実施されているべき。 ✓ CPNI ガイダンスおよびRGPに記載されているように、リスク評価は内部者の脅威も反映

				nuclear premises, it is highly likely that a comprehensive site physical security assessment will already have been completed to assess the risk of malicious acts to Nuclear Material (NM), Other Radioactive Material (ORM) and nuclear facilities. This should have resulted in a comprehensive physical protection system designed to protect those assets for which the dutyholder is responsible. This risk assessment should fully consider acts of both theft and sabotage and therefore controls to mitigate these threats should already be in place for the NM/ORM and the site (refer to SyAPs FSyP 6, the associated SyDPs and TAGs for further guidance). Accordingly, for nuclear premises, the risk assessment for information and associated assets should sit within the context of the overall site physical security assessment. 21. The risk assessment should also reflect the insider threat and consider the unique problem this poses due to the advantages they have over an adversary that does not have authorised access, as described in CNS-TAST-GD-11.4.2 [15], CPNI guidance [16] and other RGP in this area, when mitigating the associated risks. 22. The initial stage of the risk assessment should be to develop a specification of the Organization’s needs. CPNI promote their Operational Requirements (OR) process as a tool to enable an Organization to produce a clear, considered and high-level statement of their security needs based on the risks they face and leads to the application of effective and proportionate protective security measures. CPNI recommends completing both a risk assessment and their OR used in line with the CPNI Protective Security Risk Management [17] and CPNI Guidance to Producing Operational Requirements [18], respectively, as an essential part of any security project. 23. Information and associated assets in scope may include data centres, data storage systems, IT/OT system management areas, communications systems and their components, Security Management Systems (SMS), workstations, IT peripherals used to hold information, hard copy storage areas, removable media (and their associated physical transfer mechanisms), mobile devices of all types, peripherals (such as printers) and relevant supporting infrastructure, both within the	し、アクセス権を持たない敵対者よりも優位性があるため、これがもたらす固有の問題を考慮すべき。 ✓ リスク評価の初期段階は、組織ニーズの明確化である。CPNI は、組織が直面するリスクに基づき、明確で高レベルのセキュリティニーズ声明を作成し、効果的で適切な防護セキュリティ対策に役立つことを可能にするツールとして、運用要件（OR）プロセスを推進している。 ✓ 対照範囲に含まれる情報および関連資産の例示（データセンター、データ保管システム、IT／OT システムの管理領域、通信システム、セキュリティ管理システム（SMS）、ワークステーション、・・・） ✓ 事業者は、その状況に応じて適切と思われる方法論やツールを採用すべき。CPNI は、密かな攻撃（情報の窃取、サービスの拒否、悪意あるソフトウェアのインストールなど、攻撃が行われたことを検知されず、またその兆候を残さずに、悪意ある理由で機密情報にアクセスすることを望む者により実行される）によるリスクを具体的に検討するために、密かな脅威緩和プロセス（STaMP）の使用を勧めている。 ✓ リスク評価で考慮すべき事項（脅威-秘密攻撃、強制攻撃を含む、職員、全スタッフおよび訪問者、情報の作成・受領から情報・保管装置の廃棄に至る情報のライフサイクル、新しい勤務形態-リモート／在宅勤務、リムーバブル・メディアおよびその他のデータ転送形態、自然災害および環境災害） ✓ リスクとして、事業継続および災害復旧計画の一環として実施される事業影響評価を考慮すべき。 ・検査官の考慮事項 ✓ 物理的セキュリティ対策は、リスク評価に基づく階層的アプローチの一環か？ ✓ リスク評価は、関連するすべての脅威を適切に考慮しており、それらは信用できる脅威情報／諜報機関によるものか？ ✓ リスク評価の方法を正しく適用しているか？ ✓ リスク評価は定期的にレビューされ、実施さ
--	--	--	--	---	--

				context of office/site and remote/home working environments. The CPNI Asset Identification Guide [19] has been developed to assist anyone responsible for identifying an Organization’s critical assets as part of the Protective Security Risk Assessment process. 24. The threat vectors relevant to any given asset should be informed through the conduct of a protective security risk assessment. There are a number of methodologies and tools for conducting a physical risk assessment and dutyholders should employ a mechanism that they feel is appropriate to their context. To specifically consider the risks from surreptitious attack – carried out by a party who wishes to gain access to classified material for nefarious reasons to steal information, deny service, install malicious software, etc without being detected or leave any indication that an attack has taken place – CPNI advise the use of the Surreptitious Threat Mitigation Process (STaMP) [20]. 25. Whichever mechanism is used the risk assessment should consider the following: ▪ The threat – including surreptitious and forced attack. ▪ Personnel, all staff and visitors. ▪ Information lifecycle from creation and receipt through to disposal of information and storage devices. ▪ New working arrangements – remote/home and mobile working. ▪ Removable media and other forms of data transfer. ▪ Natural and environmental hazards. 26. These risks should take account of business impact assessments conducted as part of business continuity and disaster recovery planning. Inspectors should consider ▪ Are the physical security measures part of a layered approach based upon a risk assessment? ▪ Does the risk assessment adequately consider all relevant threats, and are these derived from credible threat information/intelligence? ▪ Has the dutyholder applied their chosen risk assessment methodology correctly? ▪ Has the risk assessment been reviewed periodically to confirm the controls in place are commensurate with the threat? ▪ Are risks defined and mapped to the areas under consideration?	れている管理が脅威に見合っていることを確認しているか？ ✓ リスクが定義され、検討対象領域にマッピングされているか？ ✓ リスクに対処するための一連の防護セキュリティ勧告を選定および作成したか？ ✓ 適切な仕様（OR など）が作成され、情報および関連資産の物理的防護対策の設計に使用されているか？ ✓ 防護セキュリティ勧告の評価（成功の可能性の観点から）が行われたか？ ✓ 実施された対策によってリスクは緩和されたか？残存リスクは許容できるか？ ✓ 変化する脅威を特定し、必要に応じて物理的セキュリティを強化するために、どのようなプロセスが整備されているか？
--	--	--	--	---	---

				▪ Has the dutyholder identified and developed a suite of protective security recommendations to address the risks? ▪ Has an appropriate specification (such as an Operational Requirement) been produced and used to design the physical protection measures for information and associated assets? ▪ Has an assessment of protective security recommendations (in terms of likelihood of success) been made? ▪ Have the risks been mitigated by the measures implemented? Is the residual risk acceptable? ▪ What processes are in place to identify changing threats and to scale up physical security if/when necessary?	
			8. Physical Security Control Measures	27. The risk assessment should inform a plan to mitigate the risks. A physical security plan or similar should be used to summarise what measures are required, how they should be implemented and how assurance should be provided and maintained. 28. The types of controls that could be in place to mitigate physical security risks should include, but not be limited to, those listed in Appendix 1, below. The inspector should be able to see a clear link between risks and why particular controls are specified. Dutyholders should consider controls that will deter, delay, detect, assess and respond to physical risks, including those posed by insiders. 29. Physical security measures should be deployed in a defence in depth approach that provides layers of protection. The risk assessment should enable controls to be implemented in a proportionate manner focussed on the most sensitive assets. 30. For these physical security elements to be effective, they must be supported by a Suitably Qualified and Experienced Person (SQEP) and enforced by appropriate standards, procedures and arrangements. Training or guidance must also be provided to enable staff to implement, use and manage physical security controls correctly and where appropriate recognise, react to and report signs of a possible attack.	8. 物理的セキュリティの管理方策 ✓ リスク評価は、リスクを緩和するための計画に反映させるべきであり、物理的セキュリティ計画が使用されるべき。 ✓ 物理的セキュリティ・リスクを緩和するために実施される管理の種類には、付録1に示すものが含まれるべき。 ✓ 物理的セキュリティ対策は、深層防御アプローチで展開されるべき。 ✓ 物理的セキュリティ要素が効果的であるためには、適切な資格と経験を有する者（SQEP）による支援が必要であり、適切な基準、手順書、方策により実施されるべき。
				8.1. Equipment Siting 31. Technology should be sited in a manner to mitigate the risk of overlooking and overhearing from personnel without a need to know. In many modern buildings an	ONR 8.1 設備の置き場所 ✓ 技術は、知る必要のない職員から見られたり、立ち聞きされるリスクを緩和する場所に

				open plan environment is favoured but this must be balanced by maintaining the need to know where SNI is potentially at risk. 32. Suitable measures and processes (physical and otherwise) should be considered for meeting rooms and other communal areas (including staff restaurants) where overhearing or eavesdropping may be a risk to managing access to SNI or as a minimum, to preserving need to know. Siting of conferencing equipment may also give rise to risk of overseeing/overhearing or eavesdropping, particularly where it is capable of being remotely operated.	置かれるべき。近代的な建物では開放環境が好まれるが、SNI が潜在的にリスクに曝される場所がどこか知っておく必要性とのバランスが必要。 ✓ 立ち聞きや盗聴がリスクとなる可能性がある会議室などの共用エリア（職員用レストラン含む）に対する適切な対策やプロセスを検討すべき。遠隔操作可能な場合、会議装置の設置も監視／盗聴／盗聴のリスクを生じさせる可能性がある。
				8.2. Cable Security 33. Dutyholders should assess the risks to cables running through working areas and measures should be considered to prevent unauthorized access or physical damage (accidental or deliberate). The decision to use a particular network cable type (e.g., fibre, copper or coaxial) for technology has a security dimension in addition to capacity and functionality requirements. Consideration should be given to network patching security, and the physical control of network ports in office areas and in data cabinets, and the implementation of controls around physical switch ports. 34. Cable security should be maintained so that cable runs for secure systems are either segregated (using locked but inspectable trunking) or differentiated (e.g., different colour cables or labels) as appropriate. This is a matter not only of good housekeeping from a support perspective but is also a system segregation measure that contributes to resilience. 35. Dutyholders should take account of the possibility of crosstalk between systems of different security sensitivity with long parallel cable runs, especially when they are in close proximity in shared trunking. IT/OT cables for systems carrying SNI should not routinely be in the same trunking as power cables. 36. Sites should determine the potential impact of the consequences of malicious or non-malicious damage to the exposed cables on the security infrastructure (see paragraphs 55-56).	ONR 8.2 ケーブルのセキュリティ ✓ 作業場所を通るケーブルのリスクを評価し、無許可のアクセスや物理的な損傷（偶発的または故意）を防止するための対策を検討すべき。 ✓ セキュリティシステム用のケーブルは、隔離されるか（施錠され検査可能なケーシングを使用）、必要に応じて識別される（異なる色のケーブルやラベルなど）ように維持されるべき。 ✓ 特に共有ケーシング内で近接している場合、長い並行ケーブル配線でのセキュリティ感度の異なるシステム間のクロストークの可能性を考慮すべき。 ✓ 露出ケーブルに悪意があるまたは悪意のない損傷が発生した場合に、セキュリティ・インフラに与える潜在的な影響を判断すべき。
				8.3. TEMPEST and Electromagnetic Security (EMS) 37. Most locations hosting information and associated assets should, by their very nature, have extensive controlled	ONR ・ 8.3 電磁波盗聴（TEMPEST）と電磁波セキュリティ(EMS)

				space around them which should prevent some types of TEMPEST/EMS attack. This is not the case for all locations however and dutyholders should consider TEMPEST/EMS compromise methods in their risk assessments and implement measures as appropriate to manage the level of unintentional signals emanating from IT which may expose SNI. 38. Dutyholders should implement measures to prevent crosstalk between systems operating with SNI and those of different security sensitivity. Furthermore, dutyholders should implement measures to prevent interference or crosstalk where the cables of systems with SNI are unavoidably close to system power lines. Such measures could include filtering of mains power or use of shielded cabling. 39. Dutyholders concerned about the exploitation of Electromagnetic (EM) signals around data security classified above OFFICIAL-SENSITIVE can request support from NCSC, as the NTA for TEMPEST and EMS, for consultancy, vulnerability assessments and operational assurance services [21]. ONR can also engage with the UK National Authority for Counter Eavesdropping (UK NACE) where deemed appropriate.	✓ リスク評価において TEMPEST／EMS 関係の情報漏えいを検討し、SNI を暴露する可能性のある IT から発せられる非意図的な信号レベルの管理方策を適宜実施すべき。 ✓ SNI を使用して運用されるシステムとセキュリティ感度の異なるシステムとの間のクロストークを防止する対策を実施すべき。 ✓ 「公式-機密」以上の分類のデータセキュリティ周辺での電磁（EM）信号の悪用を懸念する事業者は、NCSC に支援を要請可能。ONR は、適切な場合、英国盗聴対策国家機関（UK NACE）との連携も可能。
				8.4. Control of Removable Media 40. Where media (of all types) is used to transfer SNI, physical security risks including loss and/or theft of such media should be mitigated. Dutyholders should limit the use of all removable media devices except when specifically authorised. An inventory of removable media should be maintained to determine the location of assets and identify which individuals have access to them. Personal/unapproved removable media devices should never be used on official systems. 41. Protection of removable media (USB devices, flash drives, CD/DVD, backup tapes) in transit can be achieved effectively using hardware and software controls (e.g., using suitable encryption products). Physical protection measures could include packaging, transit cases, escorting and courier companies. Dutyholders should ensure that the reasons for data transfer are clear and that SNI is protected adequately. NCSC provide Device Security Guidance on how to use peripherals securely [22].	ONR ・ 8.4 リムーバブル・メディアの管理 ✓ SNI の転送にメディアを使用する場合、メディアの紛失および／または盗難を含む物理的セキュリティ・リスクを緩和すべき。 ✓ 移動中のリムーバブル・メディア（USB、CD/DVD など）の保護は、ハードウェアおよびソフトウェアの管理（適切な暗号化製品の使用など）により効果的に達成可能。

				8.5. Remote/Home Working and Mobile Devices 42. Where remote/home working is required operationally, dutyholders should have a clear understanding of the risks involved and should have measures in place to mitigate them adequately, supported by a remote/home working policy. Since mobile devices are often used in less secure environments, the physical security aspects of device storage should be considered both in transit (e.g., in a vehicle or train) and at rest (e.g., in a user’s house, accommodation such as a hotel, or public places). 43. A number of layered security measures should be implemented (such as device secure configuration and encryption) to protect mobile devices and remote connections. Physical measures could include secure containers and tethering mechanisms. Dutyholders should be able to demonstrate that the risks are understood and have been mitigated to an adequate extent. Vigilance at all times and equipment siting, as described above, when using a mobile device, are important considerations to ensure that a conversation during conference/phone calls and meetings cannot be overheard and screen data cannot be seen – through physical positioning or the use of privacy screens – by others in these environments. 44. CPNI encourages the undertaking of a Personnel Risk Assessment for remote working to identify and address concerns [23], whilst further guidance can be found on the NCSC website [24].	ONR ・ 8.5 リモート／在宅勤務およびモバイル・デバイス ✓ リモート／在宅勤務が業務上必要な場合、関連リスクを明確に理解し、リスクを適切に緩和する対策を講じるべき。 ✓ モバイル・デバイスおよびリモート接続を保護するために、多くの階層的なセキュリティ対策が実施されるべき（デバイスの安全な設定や暗号化など）。 ✓ CPNI は、リモートワークのための個人リスク評価を実施することを勧めている。
				8.6. Secure Disposal of Assets 45. Information and associated assets should be sanitised adequately for re-use or destroyed securely using appropriate equipment when no longer required. This applies to both hard copy and digital information however stored. Advice on appropriate sanitisation techniques and destruction mechanisms is available from the NCSC [25], CPNI [26] and other RGP. Sanitisation or destruction mechanisms must be supported by an appropriate tracking and recording mechanism to provide traceability of information and associated assets at all stages. Where information and associated assets have been physically destroyed a destruction certificate	ONR ・ 資産の確実な処分 ✓ 情報および関連資産は、再利用のために適切に秘密情報が削除されるべきであり、必要がなくなった場合は、適切な装置を用いて安全に破棄されるべき。 ✓ 事業者は、NCSC、CPNI および他の RGP から助言を入手可能。 ✓ NCSC は、製品の認証サービスおよびガイドンスの提供を行っている。 ✓ 破壊または秘密情報の削除が施設内で行われない場合、CNS-TAST-GD-7.2 に沿って、機密契約プロセスを考慮すべき。

				should be provided. 46. Commercial tools are available for secure sanitisation and NCSC provide guidance on these together with a certification service for approved products. Similarly, commercial companies can gain certification to required standards to demonstrate that they are qualified to conduct various types of secure destruction. The use of mobile paper destruction service providers does not comply with CPNI’s secure destruction standard regarding the particle sizes media should meet for above OFFICIAL. In some circumstances it may be more appropriate for an Organization to use mobile paper destruction techniques on their establishment compared to fixed site destruction techniques, which results in material being transited prior to being destroyed. NCSC guidance states that consideration to the geographic distance, in terms of the stops suppliers’ vans have to make enroute, introduces risks which must be managed (for example using the ‘two-person rule’). 47. Inspectors should confirm that consideration has been given to SNI stored on rented equipment such as printers or multi-function devices. Rental contracts for such devices often require the return of out-of-date equipment intact so that it can be replaced with newer versions. Where destruction or sanitisation doesn’t take place on premise the classified contracts process should be considered in line with CNS-TAST-GD-7.2 [10]. 48. In some instances, SNI may be retained for an extended period of time due to the lifecycle of the asset it relates to. A lack of dedicated document storage space at a facility may cause a dutyholder, or even their supply chain partner, to procure the services of an off-site archiving company. Under such circumstances, an assessment should be undertaken to ensure that the archiving company has suitable security arrangements in place to protect SNI in transit and in storage at their facility. The assessment of the archiving company should consider the classified contracts process in line with CNS-TAST-GD-7.2 [10].	✓ SNI は、施設に専用の保管スペースがないため、オフサイトのアーカイブ会社のサービスを利用する場合がある。そのような場合、アーカイブ会社が、輸送中および保管中の SNI を保護する適切なセキュリティ方策を有していることを確認する評価が実施されるべき。
				8.7. Security Management Systems – Protection and Resilience 49. The increasingly sophisticated nature of IT systems and networks associated with SMS provides increased functionality in managing a site’s physical security	ONR ・ 8.7 セキュリティ管理システムー保護およびレジリエンス ✓ 悪意ある脅威アクター、特に内部関係者が、混合攻撃シナリオの一部としてサービスを妨

				regime, but also introduces opportunity for a malicious threat actor, particularly an insider, to disrupt its service, potentially as part of a blended attack scenario. The physical protection of core components of the system represents one of several control areas CPNI consider in their Cyber Assurance of Physical Security Systems (CAPSS) standard that need to be implemented to protect against identified threats [26]. 50. These include: disabling non-operational physical interfaces to prevent the exploitation of insecure internal or external interfaces; installing tamper alarms to prevent access to structures inside the tamper-protection boundary of the device; the protection of security related physical structures to prevent physical compromise of the device and unauthorized physical access to security critical data stored on the device; and physical security of management interfaces to prevent their physical compromise. It also highlights that users should confirm the behaviour of the device on power loss to ensure that in the event of power failure the system cannot be exploited if the device fails or restarts in a way that undermines the device’s security. 51. Power supply, and more significantly its back-up provision, is an important resilience feature and can be defined as an essential service critical to the operational process of the SMS to enable it to maintain the security infrastructure of the site. Other essential services may include communications, IT systems and infrastructure (including associated server rooms and cable infrastructure), and potentially air-conditioning systems. 52. The identification of single points of failure (SPOFs) in the SMS network topology or essential services supporting the SMS is vital as their loss would cause the functionality of the SMS to cease or be unacceptably impaired. It relies on the concept of diversity which can be described as the point at which a service splits onto two bearers, each taking a different direction, and each being capable of taking the entire service, which is only achieved when the service functionality is allied with separation of service. 53. If the SPOF is vulnerable to sabotage the service provided by the SMS could be disrupted. Dutyholders should determine the potential impact of the consequences of malicious and non-malicious damage to SPOFs and	害する機会も生まれている。システムのコアコンポーネントの物理的保護は、CPNI が物理的セキュリティシステムのサイバー保証 (CAPSS) 標準で考慮しているいくつかの管理領域の 1 つである。 ✓ これには、安全でない内部または外部インターフェイスの悪用を防ぐための稼働しない物理的インターフェイスを無効にすることなどが含まれる。 ✓ 電源、特にそのバックアップ提供は、重要なレジリエンス能力であり、SMS の運用プロセスに不可欠なサービスである。他の重要なサービスには、通信、IT システムなどがある。 ✓ SMS ネットワーク・トポロジまたは SMS をサポートする重要なサービスにおける単一障害点 (SPOF) の特定は、それらが失われると SMS 機能が停止するか、許容できないほど損なわれるため、非常に重要。 ✓ SPOF に対する悪意のあるまたは悪意のない損傷の潜在的な影響を判断し、機能喪失を回避する緊急時対応策の策定、設計による脆弱性の排除などでレジリエンスを向上させる方策を検討すべき。
--	--	--	--	---	--

				consider arrangements to improve resilience by developing contingencies to operate around the loss of their functionality, design out the vulnerability, or harden the vulnerability with physical security controls.	
				8.8. Environmental Controls 54. SNI will be stored in a variety of locations and systems within dutyholder Organizations and the environmental controls for all these locations should be considered to ensure that information and associated assets are not damaged or destroyed by changes in conditions. Technology may be susceptible to extremes of temperature and humidity, whilst information in hard copy is vulnerable to damage from excess humidity and flooding. 55. Environmental controls are often managed through Building Management System software and while that can be a pragmatic and cost-effective solution, inspectors should gain assurance that dutyholders have taken into account relevant factors such as any SPOF or vulnerabilities of sensors and remote management systems to assessed risks. 56. Electrical equipment storing or processing SNI may be vulnerable to changes in electricity supply such as power fluctuations and total supply failure. Dutyholders should make provision for such eventualities and ensure critical services are supported by a standby power supply or uninterruptible power supply solution in the event that the mains supply is disrupted. Other essential services should be considered and addressed as per paragraphs 55-56. Inspectors should consider ▪ Has a physical security plan been developed to describe the controls in place and is it appropriate? ▪ Is there a clear documented link between identified risks and the security controls in place? ▪ Has the purpose of physical security control measures been clearly defined and is the technical implementation adequate? ▪ Has the risk of overlooking and overhearing been considered in the siting of equipment used for processing SNI and meeting rooms where SNI is discussed? ▪ Is cable layout and security part of a planned and structured process? ▪ Has consideration been given to network patching security,	ONR • 8.8 環境の管理 ✓ SNI は組織内の様々な場所やシステムに保存されるため、情報や関連資産が状況の変化によって損傷または破壊されないように、すべての場所の環境の管理を考慮すべき。 ✓ 環境管理は多くの場合、ビル管理システム ソフトを通じて管理され、実用的で費用対効果の高いソリューションではあるが、検査官は SPOF や評価されたリスクに対するセンサー やリモート管理システムの脆弱性などの関連要因を考慮していることを確認すべき。 ✓ SNI を保存または処理する電気機器は、電力供給の変化の影響を受けやすい場合がある。これに備え、主電源が中断された場合に重要なサービスがスタンバイ電源または無停電電源ソリューションによってサポートされるようにすべき。 • 検査官の考慮事項 ✓ 実施されている管理策を説明する物理的セキュリティ計画が策定されており、適切か? ✓ 特定されたリスクと実施されているセキュリティ管理策の間に、明確な文書化されたリンクがあるか? ✓ 物理的セキュリティ管理策の目的が明確に定義されており、技術的に適切に実施されているか? ✓ SNI の処理に使用される設備の設置場所や SNI について話し合う会議室の設置場所に関して、覗き見や立ち聞きのリスクが考慮されているか? ✓ ケーブルのレイアウトとセキュリティは、計画され構造化されたプロセスの一部か? ✓ ネットワーク・パッチのセキュリティ、オフィス・エリアとデータ・キャビネット内のネットワーク・ポートの物理的管理、および物理スイッチ・ポート周辺の管理策の実施が考慮されているか? ✓ サイトの TEMPEST/EMS の考慮事項が評価

				the physical control of network ports in office areas and in data cabinets, and the implementation of controls around physical switch ports? ▪ Have TEMPEST/EMS considerations for the site been assessed and mitigated adequately where appropriate? ▪ What measures does the dutyholder have in place to limit the use of removable media devices? ▪ Is removable media being thoroughly scanned for malware before it is brought in to use or received from any other source? ▪ Does the dutyholder have a clear understanding of the risks around remote working? What physical and procedural security measures are in place to mitigate them adequately? ▪ Is there consideration to have a re-use and disposals policy in place, with key roles understood by everyone in your business? ▪ Are there records documenting the lifecycle of storage media and assets in terms of when they are in use and stored as well as the duration? ▪ How much physical storage space is available to store end-of-life equipment, and what are the security arrangements around storage and disposal? ▪ Have SPOFs been identified within the SMS infrastructure? What measures are in place to mitigate risks? ▪ Have any risks to the operation of environmental management systems been identified and mitigated adequately? ▪ Are ‘detect’ capabilities monitored appropriately? ▪ Has the dutyholder ensured that guard forces have clearly defined responsibilities and are SQEP for their roles? CNS-TAST-GD-9.3 [27] covers this topic in more detail. ▪ Is the dutyholder able to provide assurance that the alarm response force is trained and resourced adequately to respond to physical security events that affect SNI?	され、必要な場合、適切に緩和されているか? ✓ リムーバブル・メディアデバイスの使用を制限するためにどのような対策を講じているか? ✓ リムーバブル・メディアは、使用のために持ち込まれる前、または他のソースから受け取る前に、マルウェアがないか徹底的にスキャンされているか? ✓ 事業者は、リモートワークに関するリスクを明確に理解しているか? リスクを適切に緩和するために、どのような物理的および手続的セキュリティ対策が実施されているか? ✓ 再利用および廃棄ポリシーの導入を検討しているか? 主要な役割を社内の全員が理解しているか? ✓ ストレージ・メディアと資産のライフサイクルについて、使用および保管時期と期間の観点から文書化された記録があるか? ✓ 耐用年数の終了した設備を保管するために利用できる物理的な保管スペースはどれくらいあるか? また、保管および廃棄に関するセキュリティ対策はどのようなものか? ✓ SMS インフラ内で SPOFs が特定されているか? リスクを軽減するためにどのような対策が実施されているか? ✓ 環境管理システムの運用に対するリスクが特定され、適切に緩和されているか? ✓ 「検出」能力は適切に監視されているか? ✓ 事業者は、警備隊が明確に定義された責任を持ち、その役割に対して SQEP であることを確実にしているか? CNS-TAST-GD-9.3 でこのトピックについて詳しく説明している。 ✓ 事業者は、警報対応部隊が SNI に影響を及ぼす物理的セキュリティ事象に対応できるよう適切に訓練され、リソースが確保されていることを保証できるか?
			9. Assurance of Physical Security Measures	57. As with all security controls, assurance, and independent assurance, is required to ensure they are effective both on implementation and throughout the lifetime of the information and associated asset. Accordingly, dutyholders should have a mechanism in place to provide appropriate assurance. 58. Dutyholders should recognise that threats, technology	ONR • 9 物理的セキュリティ方策の保証 ✓ その実施と情報および関連資産の存続期間全体の両面で、有効であることを確保するための保証および独立した保証が必要。事業者は適切な保証を提供するメカニズムを整備すべき。

				and business functions all change over time and have mechanisms in place to monitor these changes and react accordingly. CNS-TAST-GD-7.1 [13] describes the requirement for a risk management process managed by a security governance structure and physical security should be part of that approach. 59. Physical security measures and their associated management should be able to respond quickly to a change in threat or to an event and scale up so that existing controls can be expanded and/or augmented by additional measures. Such measures could include for example additional personnel, increased monitoring, introducing exit searches or increased CCTV coverage. Further information on assurance and how it fits within a corporate governance structure can be found in CNS-TAST-GD-1.1 [28] and CNS-TAST-GD-1.5 [29]. 60. Physical security considerations should be an intrinsic part of the change management function so that the distinctive issues around it can be taken into account when site and system changes are being discussed. 61. Dutyholders should have arrangements in place to ensure their security systems are subject to an appropriate regime of Examination, Inspection, Maintenance and Testing (EIMT) to ensure that they remain effective. Further guidance on these issues can be found in CNS-TAST-GD-5.2 [30].	✓ 事業者は、脅威、技術、事業内容は時間経過とともに変化することを認識し、変化を監視して対応するメカニズムを整備すべき。 ✓ 物理的セキュリティ対策と関連する管理は、脅威または事象の変化に迅速に対応し、既存の管理を拡張・追加対策により強化できるように拡張可能なものとすべき。 ✓ 物理的セキュリティの考慮事項は、変更管理機能の本質的な部分であるべきであり、サイトおよびシステムの変更が議論されるとき、それに関する特有の問題が考慮されるべき。 ✓ 事業者は、セキュリティシステムが適切な点検、検査、保守、試験 (EIMT) の対象となり、その有効性が維持されるようにする方策を有するべき。
			9.1 Contractor Management	62. Dutyholders are responsible for managing risks to their information and associated assets held within their supply chain. Dutyholders should adopt a risk-based methodology to ensure that the level of assurance required for the physical protection of SNI is proportionate to the risk of loss, theft, unauthorized disclosure of, or unauthorized access to any SNI held either electronically or in physical (hard copy) form at a third-party premises. They should therefore approve the physical security (and other security) measures implemented by their contractors. This approval should take account of the requirements in GovS 007 [3], as qualified by the relevant FSyPs and RGP. Inspectors should consider ▪ Is there adequate assurance that physical security measures are effective? Can they be scaled up as necessary? ▪ Is there a process for monitoring and for identifying and	ONR ・ 9.1 請負業者管理 ✓ 事業者は、サプライチェーン内に保持されている情報および関連資産に対するリスクを管理する責任がある。SNI の物理的保護に必要な保証レベルが、第三者の施設で保持される SNI の紛失、盗難、不正開示、または不正アクセスのリスクに比例していることを保証するために、リスクベースの手法を採用すべき。 ・ 検査官の考慮事項 ✓ 物理的セキュリティ対策が有効という十分な保証があるか？必要に応じて拡大可能か？ ✓ 監視および欠陥の特定・対処を行うロセスはあるか？ ✓ 脅威、技術、または事業内容の変更が、変更管理プロセスの一環としてセキュリティ対策

				addressing deficiencies? ▪ Is there confidence that changes to threats, technology or the business are reflected in a review of security measures as part of the change management process? ▪ Are all physical security measures adequately supported by procedural and personnel measures? ▪ Does the dutyholder ensure that SNI held within its supply chain is appropriately physically protected? ▪ Are supply chain facilities holding SNI suitably recorded and approved on List N? ▪ Does the duty holder have a suitable in contract monitoring process in place to ensure that security controls are maintained and remain commensurate to the risks they address, for the life of the contract or period that SNI will be held for? ▪ Does the dutyholder have arrangements in place to ensure their security systems are subject to an appropriate regime of EIMT? ▪ Is the dutyholder able to describe how they assure their physical security measures? List any supporting processes and procedures.	のレビューに反映されているという確信があるか？ ✓ 全ての物理的セキュリティ対策は、手順書および人的対策により十分に裏付けられているか？ ✓ 事業者は、サプライチェーン内で保持されている SNI が適切に物理的に保護されていることを確認しているか？ ✓ SNI を保有しているサプライチェーン施設は、リスト N に適切に記録され、承認されているか？ ✓ 事業者は、契約期間中または SNI 保持期間中、セキュリティ管理が維持され、リスクに見合った状態を維持することを保証する適切な契約内監視プロセスを実施しているか？ ✓ 事業者は、セキュリティシステムが適切な EIMT の対象であることを保証する方策を実施しているか？ ✓ 事業者は、物理的セキュリティ対策をどのように保証しているかを説明できるか？ サポートプロセスと手順書をどれでも列挙すべし。
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant UK Legislation and Policy	4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ...	ONR ・英国の関連法および政策との関係 ✓ NSIR における用語の定義と NM&ORM に関する要件 ✓ SyAPs は、事業者のセキュリティ方策の有効性について一貫した規制判断を行うための枠組みを ONR 検査官に提供。 ✓ 本 TAG は、検査官が「FSyP 7 – サイバーセキュリティと情報保証」をサポートする「SyDP 7.2 – 情報セキュリティ」を実証する事業者の提出書類を評価する際のガイダンスを提供。 ✓ セキュリティに関する政府機能基準 ➤ サイバー、物理、人員、技術、事象の管理に関するセキュリティ・リスク管理、計画、対応活動に対する期待事項を示す。 ✓ 政府セキュリティ分類（GSC） ➤ NISR 分類方針とともに、SNI を含む情報の種類、適用すべきセキュリティ分類レベル、その管理と運用全体にわたり実施すべき保護対策を示す。

			4. Relationship to International Standards and Guidance	9. The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [5] and the IAEA Nuclear Security Fundamentals [6]. Further guidance is available within IAEA Technical Guidance and Implementing Guides. ...	ONR ・ IAEA セキュリティ標準およびガイダンスとの関係 ✓ 国の核セキュリティ体制の必須要素は、核物質防護条約（CPPNM）および IAEA 核セキュリティ基本文書に規定、ガイダンスは、IAEA 技術ガイダンスおよび実施ガイド参照 ➤ より詳細なガイダンスは NSS 13 等参照。
参考文献	—		References	・ H.M. Government, “The Nuclear Industries Security Regulations 2003 (NISR) (2003/403),” 2003. ・ ONR, “Security Assessment Principles for the Civil Nuclear Industry,” 2017. ・ ・	—
用語集	—		Glossary and Abbreviations	AACS : Automatic Access Control System CAPSS : Cyber Assurance of Physical Security Systems ・ ・	—
別紙・附属書	—		Appendix	Appendix 1 : Types of Physical Security Control Measures	—
改訂情報	変更日、施行日、変更概要（「記載の適正化」）		（表紙に記載）	Revision / Issue No., Date など	—

2.4.2.9 PP1801「教育および訓練」と CNSS-TAST-GD-7.5 (Issue 4)「Preparation for and Response to Cyber Security Events」における調査の結果

原子力規制庁が用いる検査ガイド PP1801「教育および訓練」と、ONR の検査ガイド CNSS-TAST-GD-7.5 (Issue 4)「Preparation for and Response to Cyber Security Events」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-9 にまとめた。

2.4.2.9.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.9.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.9.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（教育および訓練状況の確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官がサイバーセキュリティへの準備および対応に関する方策を評価する際の一般的な助言と情報を提供）について説明している。

2.4.2.9.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（規制上の期待事項、コンピュータ・セキュリティ事象の定義、関連グッドプラクティスの利用、OODA ループなど）を記載している。

2.4.2.9.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ウォークダウン、インタビューを活用して確認

- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

次の各項目について、検査のポイントを含む解説および検査官の考慮事項を示している。

- ・ 準備の解説
- ・ 事象対応方針および計画
 - 解説
 - 検査官の考慮事項
- ・ 事象報告
 - 解説
 - 検査官の考慮事項
- ・ 訓練および演習
 - 解説
 - 検査官の考慮事項
- ・ デジタル法医学的検査
 - 解説
 - 検査官の考慮事項
- ・ コミュニケーション
 - 解説
 - 検査官の考慮事項
- ・ 環境の整備
 - 解説
 - 検査官の考慮事項
- ・ 対応および復旧能力
 - 解説
 - 検査官の考慮事項
- ・ 特定
 - 解説
 - 検査官の考慮事項
- ・ ログの保護
 - 解説
 - 検査官の考慮事項
- ・ 警報の生成
 - 解説
 - 検査官の考慮事項
- ・ セキュリティ事象の把握
 - 解説

- 検査官の考慮事項
- ・ 事象の通知の解説
- ・ 監視ツールとスキルの解説
- ・ 積極的なセキュリティ事象および異常の検出の解説
- ・ 積極的な攻撃の発見の解説
- ・ 封じ込め、根絶、復旧の解説
- ・ 事象の特性評価と封じ込め戦略
 - 解説
 - 検査官の考慮事項
- ・ 証拠の収集と取扱い
 - 解説
 - 検査官の考慮事項
- ・ 短期的な封じ込め
 - 解説
 - 検査官の考慮事項
- ・ システムの法医学的検査
 - 解説
 - 検査官の考慮事項
- ・ 復旧
 - 解説
 - 検査官の考慮事項
- ・ 教訓
 - 解説
 - 検査官の考慮事項

2.4.2.9.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.9.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

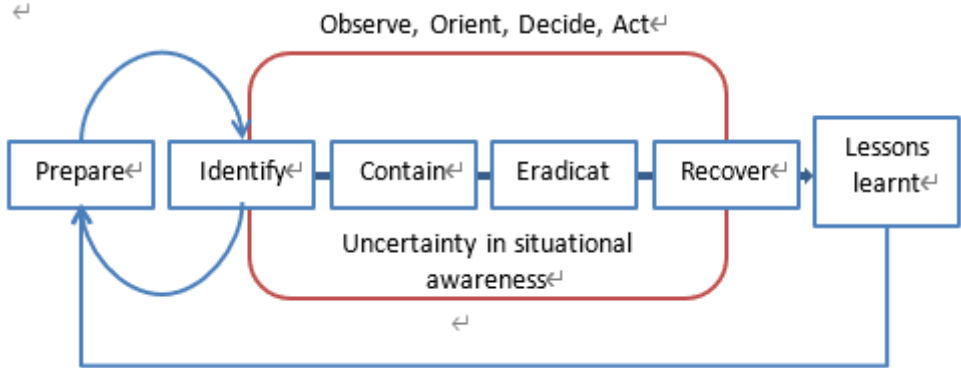
ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

ブランクページ

表 2.4.2-9 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-7.5 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1801 教育および訓練 (2023/05/31 制定) (2 頁)		英国 ONR 検査ガイド 【ガイド】CNS-TAST- GD-7.5 (Issue 4) Preparation for and Response to Cyber Security Events (January 2024) (30 頁)		両者間の主な相違点	
項目		主な内容			
図書全体構成		本文 改訂情報	図書全体構成	表紙 目次 本文 参考文献 用語・略語 付録 改訂情報	—
事 象 対 応	1. 監督領域	大分類および小分類：「核物質防護」 評価領域：「特定核燃料物質の管理」、 「核物質防護情報の管理」、「立入承認」、 「出入管理」、「物理的防護」、「情報システム防護」、「核物質防護体制」 検査分野：「教育および訓練」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	1.The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) [1]. This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully taken into account in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 [2]. 2.The term ‘security plan’ is used to cover all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）

	2. 検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 4 号イで規定される事項（防護措置）のうち、原子力施設の種別ごとの防護措置に係る規則条項で規定される教育および訓練状況を確認する。当該事項は、法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）の遵守状況の確認と合わせて行う。 これらの確認については、教育および訓練の検査分野における体制および警備員等の力量にも留意する。 2.2 防護措置の狙い 従業者に対し計画的な教育および訓練を実施することにより、必要な知識・能力（技術）等を継続的に維持していく。	2. Purpose and Scope	3. This TAG contains guidance to advise and inform ONR Inspectors in exercising their regulatory judgement during assessment activities relating to a dutyholder’s arrangements to prepare for and respond to cyber security incidents. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（教育および訓練状況の確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官がサイバーセキュリティへの準備および対応に関する方策を評価する際の一般的な助言と情報を提供
	3. 検査要件	3.1 検査対象 核燃料物質防護に係る全ての業務に関連する従業者に対する教育計画、内容、実績、被教育者の理解度、現場確認等の全てが検査対象となり得るが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、核燃料物質防護に関する教育および訓練の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 1 年間に 1 回程度 （２）検査時間 3 人／5. 2 5 （h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	6. Advice to Inspectors	14. The regulatory expectation is that the dutyholder will ensure that the security plan clearly details their arrangements to prepare for and respond to cyber security incidents in support of maintaining effective CS&IA arrangements. FSyP 7 - Cyber Security and Information Assurance Preparation for and Response to Cyber Security Incidents SyDP 7.5 Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges. 15. IAEA Nuclear Safety and Security Glossary, 2022 (Interim Edition) [12] Glossary definition: “Computer security incident” defines “An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of a computer-based system (including information), or that constitutes a violation or imminent risk of violation of security policies.” 16. SyAPs reflects a range of Relevant Good Practice (RGP) (such as the NIST cyber security framework [13]) in its approach to define the security posture for sensitive nuclear information and equipment and software used in connection with activities involving nuclear material/other radioactive material. This ensures that defence in depth is provided through the implementation of plans, policies and procedures that define: i) how assets should be protected dependent on their categorization and classification. ii) how the Organization should detect and respond to a cyber security incident, and iii) how the Organization will recover to ensure effective operations are re-established as efficiently as possible. Fundamentally, this Security Delivery Principle establishes an expectation that the dutyholder will make, implement, and test	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 - 検査手順 ✓ 確認事項 ✓ 文書、ウォークダウン、インタビューを活用して確認 ✓ 検査前準備、検査、CAP 検査の趣旨 ONR 5. 検査官への助言 ✓ 規制上の期待事項 ➢ 事業者が、セキュリティ計画にサイバーセキュリティ事象への備えと対応の方策を明確に記載し、効果的な CS&IA 方策の維持を保証していること。 ✓ 「コンピュータ・セキュリティ事象」の定義。 ✓ SyAPs は、一連の関連グッドプラクティス (RGP) (NIST サイバーセキュリティフレームワークなど) を活用。 ✓ SANS Institute、米 DOE、NIST などの RGP は、事象対応 (IR) の 6 つの主要な段階を定義している（図

			arrangements that enable the Organization to effectively and efficiently respond to cyber security incidents. 17. Current RGP described by various Organizations, including the SANS Institute, the US Department of Energy, and NIST defines 6 key stages of incident response (IR). Figure 1 summarises the stages, each of which will be considered in greater detail in subsequent sections. However, there are some general principles and considerations that should be recognised during incident response.  Figure 1. Stages of Incident Response 18. Whilst this TAG bases its regulatory expectations on the framework set out in Figure 1, it is to be expected that some dutyholders may take a different approach. This is entirely reasonable, and inspectors should ensure that judgements are made against the dutyholder's ability to achieve the expected security outcome and response in line with ONR's outcome focused non-prescriptive approach to regulation. 19. The Observe, Orient, Decide, Act (OODA) loop represents the period of intensity during incident response, and is intended to prevent spontaneous poorly considered reactions. It promotes a construct that requires the Cyber Incident Response Team (CIRT) to pause, analyse, incorporate information received from the environment and then integrate new knowledge into the next course of action. 20. There is significant uncertainty associated with situational awareness particularly in the early stages of a cyber incident. This is compounded by the needs of a wide range of stakeholders to understand what is happening. A successful CIRT and its leader are responsible for managing the uncertainty by keeping informed and controlling the flow of information to stakeholders but also allowing subject matter experts to focus on their tasks. 21. It is critical that unity of command is maintained across the entire IR process, from Preparation to Lessons Learnt, that ensures there is a solid, reliable and well-known decision-making process in place. Roles and responsibilities should be defined through the command structure. 22. There are several sources of guidance and advice available, including: • NSS No. 23-G 'Security of Nuclear Information' [7], • Technical Guidance NSS No. 17-T (Rev1) 'Computer Security at Nuclear Facilities' [9]	1)。 ✓ 本 TAG は、図 1 のフレームワークに基づいて規制上の期待を示しているが、事業者が異なるアプローチを提案することも妥当。 ✓ 観察、方向付け、決定、行動 (OODA) ループの説明。 ✓ サイバー事象の初期段階。 ✓ 準備から教訓抽出まで、IR プロセス全体にわたって指揮統制を維持し、堅固で信頼性が高く、よく知られた意思決定プロセスを確立することが重要。 ✓ ガイダンスおよび助言の情報源の列挙。 ✓ IR（事象対応）活動は、潜在的な影響に比例すべきである。多くの事業者は、IR 機能の大部分を第三者にアウトソースする。そのような場合、規制活動は、第三者プロバイダーが規制上の期待事項を満たす適切なサービスを提供できることを確認するために事業者が行ったデューデリジェンスを中心にすべき。 ✓ 事業者は様々な理由で IR を実施するが、検査官は原子力安全とセキュリティ確保に関連するセキュリティ成果の達成に重点を置くべきである。 ✓ 英国の原子力施設は複雑で、IR の実施に課題をもたらす多くのレガシー・システムが存在する老朽化した施設が含まれる。検査官は、レガシー・システムに伴う課題にもかかわらず、異なる手段であっても、期待されるセキュリティ成果と対応が達成できるという保証を求める必要がある。
--	--	--	---	---

				• NSS 33-T Computer Security of Instrumentation and Control Systems at Nuclear Facilities [9] • Good Practice Guide for Incident Management – ENISA [14] • Guide to Incident Management – CERT [15] • Incident Handler’s Handbook – SANS [16] • Computer Security Incident Handling Guide – NIST [17] • Incident Management guidance - NCSC [18] • Computer Security Incident Response Planning at Nuclear Facilities - IAEA [10] • ISO/IEC 27035 – Infosec Incident Management [19] 23. As with all regulatory activity, when assessing dutyholder arrangements for cyber IR, activity should be proportionate to the potential impact. Many dutyholders will outsource large parts of their IR capability to a third party. In such cases, regulatory activity should focus around the due diligence the dutyholder has undertaken to ensure the third party provider can provide a suitable service that meets regulatory expectations. In addition, consider the control the dutyholder has over that contract, the separation of responsibilities as well as interfacing activities such as providing access to digital systems and assets. 24. Inspectors should also be cognisant of ONR’s regulatory vires in this area. Dutyholders will conduct IR for a variety of reasons, but an inspector’s focus should be on achieving security outcomes associated with ensuring nuclear safety and security. It is also important to keep in mind that many IR activities are associated with business continuity and disaster recovery, which will only be within regulatory scope where they are required to maintain safety or security, or to facilitate hazard and risk reduction. 25. The UK’s nuclear estate is complex and includes aged facilities where there are many legacy systems that present challenges to conducting IR. However, this does not serve as an excuse nor abdicate the dutyholder of responsibility for conducting effective IR. Inspectors should seek assurances, that the expected security outcome and response can be achieved despite the challenges presented by legacy systems, albeit by potentially different means. Such assurance arrangements should be clearly detailed within dutyholder’s security plans.	
	4. 検査手順	従業者に対し、その職務の内容に応じて核燃料物質防護のために必要な教育および訓練が行われていることを確認する。また、教育および訓練が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等により確認する。 4.1 検査前準備 教育および訓練に係る関連文書を確認する。 4.2 検査の実施	7. Preparation	26. Preparation is about readying the CIRT to handle an incident at short notice and under any reasonable conditions. An incident can range from a phishing attempt to more extreme incidents such as a violation of Organizational policy by disgruntled employees (insiders) or networks being infiltrated by state sponsored adversaries. Regardless of the cause, preparation is arguably the most important phase, as it will determine how well the CIRT will be able to respond in the event of a crisis. 27. There are several key considerations in this phase that will help to mitigate any potential issues that could hinder the CIRT’s ability to handle an incident. Incident response policies and plans 28. Dutyholders should develop a sound and clear incident response policy and	ONR • 7. 準備 ✓ 準備段階の定義と考慮事項 • 事象対応方針および計画 ✓ 事業者活動の説明 ✓ 検査官の考慮事項 ➢ 事象対応計画は、セキュリティ・リスクを明確に理解した上で策定されているか? ➢ 事象対応計画は包括的で、既知

		対策官は、事業者が実施する教育および訓練が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム（CAP）等において是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。		supporting documentation. Shaping a workable policy involves creating a set of written principles, rules and processes that act as a guide, setting out the correct actions, responsibilities and practices individuals across the Organization need to adhere to in order to maintain the risk appetite and cyber security posture the company has decided on. 29. Along with creating and maintaining a policy, developing a response plan is one of the very first steps Organizations should take in the initial phase of the incident response methodology. An effective response plan should typically prioritise incidents by level of impact on nuclear safety and security as well as the wider business impact, and clearly define the most appropriate actions to deal with them. The 2022 Civil Nuclear Cyber Security Strategy [20] sets out that dutyholders should ensure that incident response plans are in place for both IT and OT. This can be one plan detailing both IT and OT or two sperate plans with appropriate interfaces and cross referencing. There will be different risks associated with information and operational technologies which the dutyholder must take account of, and likewise different personnel involved in IR, therefore requiring a different response. 30. The response plan should determine the CIRT team membership and rotation and should clearly articulate the command and control structure. While IR team membership will vary depending on the dutyholder expertise the following roles are typical in an incident response: analyst, senior analyst, IR lead and IR manager. Other roles may form part of the team dependent on the incident. In particular, this may include interface with nuclear safety and communications. The size of the team that is stood up should be proportionate to the significance of the event or incident. The response plan should also detail roles and responsibilities of senior leadership. 31. ONR TAG CNS-TAST-GD-11.4.2 [21] sets out regulatory expectations for the use of threat information against which the security regime should be designed, evaluated, and tested. Incident response plans should therefore be informed by threat assessment information from Organizations such as the National Cyber Security Centre (NCSC). 32. If an incident response retainer exists, knowing when to use internal teams or when to ‘break glass’ and engage an external CIRT provider is essential. This can and should be defined ahead of time and be documented in the incident response policy. 33. A system of independent testing should be designed and documented within the approved security plan. Independent testing may be performed using methods such as penetration testing, purple team testing, cyber-attack simulation, or a combination thereof. When designing the Organizations testing arrangements, the frequency and level of assurance required should be commensurate to the categorization and classification of the associated assets and system functions, to provide confidence that CPS outcomes can be achieved. Any shortfalls identified in such testing should be logged, risk assessed and if necessary, mitigated in line with risk appetite. In all instances the frequency and level of assurance should be clearly detailed in the dutyholder’s security plan.	の攻撃と前例のない攻撃の両方の影響を網羅しているか? ➤ 事象対応計画は、サプライチェーンと顧客からのリスクを考慮しており、裏付文書が揃っているか? ➤ 事象対応計画には、計画実行に必要な承認、権限、リソースなど、上級管理職の支援があるか? ➤ IR チームの各役割は十分にカバーしているか? ➤ 計画には、ニッチな機能（OT スペシャリストなど）について IR チームに通知する必要がある関係者が含まれているか? ➤ 事象対応計画は文書化され、より広範な組織の事業およびサプライチェーン対応計画と統合されているか? ➤ 事象対応計画は、重要な機能の運用に関与する事業領域に伝達され、理解されているか? ➤ 事象対応計画とポリシーのオフラインコピーはあるか(ランサムウェア事象の場合など)? ➤ 対応計画は定期的にはまたは脅威に大きな変化があったときに見直されているか? ➤ 外部サポートを利用するための手配が事象対応ポリシーに文書化されているか? ➤ 事象発生時に封じ込めまたは隔離に関する決定を迅速に行えるように、資産は定期的に分類および/またはクラス分けされているか? ➤ 侵入テスト、パープルチームテスト、攻撃シミュレーションなど、脅威アクターをシミュレートする環境の定期的なテストが行われているか? ➤ セキュリティ計画にテストの頻度が適切に定義されているか? ➤ 最高カテゴリーのシステムの保
--	--	---	--	---	--

			34. The dutyholder should have policies in place whereby a cyber attack may involve decision making from senior leadership and legal teams. An example would be a ransomware policy so there is no delay in decision making during a live incident. A ransomware policy will allow the dutyholder to have risk assessed all options should a payment be demanded by the threat actor. Inspectors should consider • Is the incident response plan based on a clear understanding of the security risks to the networks and information (IT/OT) systems supporting their essential function? • Is the incident response plan comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen? • Does the incident response plan consider the risk from supply chain and customers and have supporting documentation to deal with such an incident? • Does the incident response plan have senior management sponsorship, including the necessary approvals, authorities, and resources to execute the plan? • Is there sufficient cover for each IR team role? • Does the plan cover the relevant personnel required to inform the IR team for niche functions, e.g. OT specialists? • Is the incident response plan documented and integrated with wider Organizational business and supply chain response plans? • Is the incident response plan communicated and understood by the business areas involved with the operation of their essential functions? • Are there offline copies of the incident response plan and policies (e.g. in the event of a ransomware incident)? • Is the response plan reviewed on a periodic basis or when there is a significant change to the threat landscape? • Are arrangements for engaging external support documented in the incident response policy? • Are assets periodically categorized and/or classified so decisions on containment or isolation can be quickly made during an incident? • Is there regular testing of the environment which simulates a threat actor such as pen testing, purple team testing or attack simulation? • Is frequency of testing adequately defined in the approved security plan? • Is assurance activity of the highest category systems completed at least annually or is appropriate justification provided for alternative frequencies in the security plan? • Has the dutyholder considered the guidance or advice from HMG or NCSC with respect to paying ransomware?	証活動は少なくとも年に1回完了しているか、またはセキュリティ計画で代替頻度の適切な正当性が示されているか? ➤ 事業者は、ランサムウェアの支払いに関して HMG または NCSC からのガイダンスまたは助言を考慮したか?
--	--	--	--	--

				Incident reporting 35. A formal cyber incident reporting system for staff and external security researchers aids with the identification of incidents. Inspectors should consider: • Does the dutyholder have a process that details when and how to inform relevant regulatory authorities and how to engage the National Technical Authority? • Do the dutyholder’s staff know the process to report a suspected cyber security incident?	ONR • 事象報告 ✓ スタッフと外部セキュリティ研究者向けの正式なサイバー事象報告システムは、事象の特定に役立つ。 ✓ 検査官の考慮事項 ➤ 事業者は、規制当局にいつ、どのように通知し、国家技術機関とどのように連携するか、詳細に規定したプロセスを有しているか? ➤ 事業者スタッフは、疑わしいサイバーセキュリティ事象を報告するプロセスを知っているか?
				Training and exercising 36. Regular practice is essential to staying calm and collected during an incident. Cyber security exercising tests roles and responsibilities of those involved in incident response. It also tests the arrangements in place with third party providers, parent body and other stakeholders. Ongoing cyber security training and information sessions should be a central pillar supporting any cyber security regime. 37. Training and exercising should not be limited to technical skills; media and Public Relations (PR), privacy and legal all require specific training for an Organization and its people to be ready for an incident. Dutyholder Organizations should also consider incident response retainers to augment their teams where certain skills are hard to find. Where third parties, parent body Organizations or other stakeholders are used as part of response efforts their roles and responsibilities should be clearly understood, exercised and documented as part of overall IR arrangements. 38. Organizations should also periodically involve senior managers and executives in their incident response training and exercises. Although they do not have to participate as frequently as the Incident Response team, it is prudent to have them participate on occasion to ensure they are familiar with their roles and the decisions they would be expected to make during an incident. 39. Dutyholders should carry out exercises to test response plans, using past incidents that affected their (and other) Organization, and scenarios that draw on threat intelligence and their risk assessment. Inspectors should consider: • Can the dutyholder evidence that CIRT staff have received recent and relevant response training? • How often is training provided and how often is a training needs analysis conducted? • Are the dutyholder’s exercise scenarios based on experience and/or composed using relevant threat intelligence?	ONR • 訓練および演習 ✓ 事象発生時に冷静さを保つには、定期的な演習が不可欠ト。 ✓ 訓練と演習は、技術的スキルに限定されるべきではない。メディアと広報 (PR)、プライバシー、法務に関して、組織とその従業員が事象に備える特別な訓練が必要。 ✓ 上級管理職や幹部を定期的に事象対応の訓練や演習に参加させるべき。 ✓ 自組織 (および他組織) に影響を与えた過去の事象および脅威情報とリスク評価を活用したシナリオを使用し、対応計画をテストする演習を行う ✓ 検査官の考慮事項 ➤ 事業者は、CIRT スタッフが最近関連する対応訓練を受けたことを証明できるか? ➤ 訓練はどのくらいの頻度で提供され、訓練のニーズ分析はどのくらいの頻度で実施されているか? ➤ 事業者の演習シナリオは、経験に基づいており、および／また

				• Are exercise scenarios documented, regularly reviewed, and validated? • Does the dutyholder ensure that exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learnt? • Do the dutyholder’s exercises test all parts of their response cycle relating to their essential functions (e.g. Restoration of normal function levels)? • Are third party, parent body Organizations and other stakeholders roles and responsibilities clearly understood, exercised and documented? • Does the dutyholder have a schedule for cyber exercising and have they invited the inspector to observe?	は、関連する脅威情報を使用して作成されているか? ➤ 演習シナリオは文書化され、定期的にレビューされ、検証されているか? ➤ 事業者は、演習が定期的に行われ、その結果が文書化され、教訓に沿って事象対応計画と保護セキュリティを改善するために使用されていることを確実に化しているか? ➤ 事業者の演習では、必須機能 (通常の機能レベルの復旧など) に関連する対応サイクルのすべての部分をテストしているか? ➤ 第三者、親組織、および他の利害関係者の役割と責任は明確に理解され、実行され、文書化されているか? ➤ 事業者はサイバー演習のスケジュールを持っており、検査官を観察に招待しているか?
				Digital Forensic investigation Tooling 40. Ensuring the response team or third party has the appropriate hardware, software and licensing is essential. These elements will likely involve a mixture of open source and licensed software, such as forensic tools, memory analysis, log parsers, scripts to interact with cloud services and something to generate a timeline. All tooling should have the appropriate hours of training invested. Law enforcement may perform this role for criminal cases. 41. Examples of hardware can include USB hard drives, up-to-date anti-malware applications, write blocker devices, evidence bags, and an appropriate secure storage location to maintain the chain of custody. More specialised equipment can be employed for specific cases. This might include Field Programmable Gate Arrays (FPGA)-based devices that may be used together with Direct Memory Access (DMA) attack toolkits. Inspectors should consider: • Has the dutyholder identified digital forensic tools needed for use in a computer security incident response and ensured their availability? • Are digital forensic tools and supplies audited on a periodic basis to ensure kits are up to date and complete? • Are digital forensic tools and supplies refreshed after use? • Do incident response tools and supplies include an incident journal, evidence	ONR • デジタル法医学的検査 ✓ 対応チームまたは第三者が適切なハードウェア、ソフトウェア、ライセンスを持っていることを確認することが重要。 ✓ ハードウェアの例 ✓ 検査官の考慮事項 ➤ 事業者は、コンピュータ・セキュリティ事象対応で使用するために必要なデジタル法医学的検査ツールを特定し、その利用可能性を確保したか? ➤ デジタル法医学的検査ツールと供給品は、キットが最新かつ完全であることを確認するために定期的に監査されているか? ➤ デジタル法医学的検査ツールと供給品は、使用後に更新されているか?

				forms, evidence bags etc? • Has the dutyholder performed the appropriate assurance activities (e.g. audit) for the digital forensic tools held by the third party? • Has the dutyholder considered when law enforcement would be contacted and is this recorded in relevant procedures?	➤ 事象対応ツールと供給品には、事象ジャーナル、証拠フォーム、証拠バッグなどが含まれているか? ➤ 事業者は、第三者が保有するデジタル法医学的検査ツールに対して適切な保証活動 (監査など) を実行したか? ➤ 事業者は、法執行機関に連絡する時期を検討し、それが関連手順に記録されているか?
				Communication 42. There are a number of different types of communication that are important in the event of a cyber incident. All should be included in a communications plan. Internal communication processes are essential to handling the incident itself. IR teams need a secure communication capability that cannot be monitored by an attacker or insider. External communication plan for communicating the incident to external agencies, supply chain, customers etc. For example, everyone on the IR team should have a work mobile phone and a secondary external email account. The IR team should know the correct people within the business to help triage an incident. 43. External activities such as public relations require clear and timely communications. Dealing with media enquiries requires experience and should be limited to those with proper training. Any staff with public relations responsibilities should have appropriate crisis training. Inspectors should consider: • Has an out-of-band communications capability been established? • Have internal and external communications plans been established? • Does the dutyholder have a mechanism for sharing a journal of the incident status?	ONR • コミュニケーション ✓ サイバー事象が発生時に重要なコミュニケーションには、様々な種類がある。コミュニケーション計画には、これらすべてを含める。 ✓ 広報などの外部活動には、明確でタイムリーなコミュニケーションが必要。 ✓ 検査官の考慮事項 ➤ 帯域外通信機能が確立されているか? ➤ 内部および外部のコミュニケーション計画が確立されているか? ➤ 事業者は、事象状況のジャーナルを共有するメカニズムを持っているか?
				Environment preparation 44. An incident journal to track the who, what, where, when and why of an incident can aid with internal communication of incident status and later review as part of lessons learnt. 45. There are several technical measures that can be established ahead of time that will support and facilitate efficient and timely incident resolution. Examples include, but not limited to, ensuring Network Time Protocol (NTP) is enabled for all networked devices, appropriate network segregation is in place to aid the containment phase and network redundancy for the recovery phase. 46. A protected logging aggregation point that has multiple terabytes of storage should be established. All systems should be instrumented to detect an incident and report both locally and to the central server. 47. An accurate asset inventory is essential for IR teams to receive timely information	ONR • 環境の整備 ✓ 事象ジャーナルの作成 ✓ 事前に確立できる技術的対策 ✓ 数テラバイトのストレージを備えた保護されたログ集約ポイントの確立 ✓ 正確な資産インベントリ ✓ 検査官の考慮事項 ➤ 事業者は、組織がビジネス目的を達成できるようにし、組織の目標とリスク戦略に対する相対的な重要性にしたがって管理さ

				about the assets on the network, such as operating system patch level, purpose, app usage, configuration, backup status, criticality/importance, access rules and other key data. Ownership for all generic, shared service and system accounts should be established ahead of time. Inspectors should consider: • Can the dutyholder identify the data, personnel, software applications, devices, systems, and facilities that enable the Organization to achieve business purposes and are managed consistent with their relative importance to Organizational objectives and risk strategy? • Has a central logging capability been established, are networked systems instrumented to detect an incident and are they configured to report locally and to the central server and is the logging capability resilient? • Is NTP enabled on all networked devices, synchronised across the estate and, in the corporate environment, are all windows clients synchronised with Active Directory? • Have potential key decisions been identified and worked through in advance, for example, have system changes that may need to be made during an incident been pre-negotiated? • Is there an accurate asset inventory and has ownership of all generic, shared, service and system accounts been established?	れているデータ、人員、ソフトウェア アプリケーション、デバイス、システム、および施設を特定できるか? ➤ 中央ログ機能が確立されているか? ネットワーク システムは事象を検出するように装備されているか? ローカルおよび中央サーバーにレポートするように構成されているか? ログ機能は復旧力があるか? ➤ すべてのネットワーク・デバイスで NTP が有効になっているか? 資産全体で同期されているか? 企業環境では、すべての Windows クライアントが Active Directory と同期されているか? ➤ 潜在的な重要な決定が事前に特定され、検討されているか? たとえば、事象中に行う必要がある可能性のあるシステム変更は事前に交渉されているか? ➤ 正確な資産インベントリがあり、すべての汎用アカウント、共有アカウント、サービス アカウント、およびシステム アカウントの所有権が確立されているか?
				Response and recovery capability 48. Dutyholders should have the capability and resources to enact their incident response plan, including effective limitation of impact on the operation of their essential function. During an incident, they should have access to timely information on which to base their response decisions. Inspectors should consider: • Does the dutyholder understand the resources that will likely be needed to carry out any required response activities, and ensure that arrangements are in place to make these resources available? • Do they understand the types of information that will likely be needed to inform response decisions and ensure that arrangements are in place to make this information available? • Do their response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and do they have the authority to carry them out? • Does the dutyholder have a defined methodology for the prioritisation of	ONR • 対応および復旧能力 ✓ 事業者は、重要な機能の運用への影響を効果的に制限するなど、事象対応計画を実行する能力とリソースを備えている必要がある。 ✓ 検査官の考慮事項 ➤ 事業者は、必要な対応活動を実行するのに必要なリソースを理解し、リソースを利用できる手配が整っていることを確認しているか? ➤ 事業者は、対応決定を通知するために必要な情報の種類を理解し、情報を利用できる手配が整っていることを確認しているか?

				recovery of services? Have systems been prioritised based on their importance? • Does the dutyholder have the capability to deal with a protracted incident which may extend beyond a few days into weeks? • Are fail-over mechanisms available that can be readily activated to allow continued operation of their essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable? • Do arrangements exist to augment the dutyholder’s incident response capabilities with external support if necessary (e.g. specialist cyber incident responders) and have such arrangements been tested? 49. In the event of a cyber incident, backups will be required to restore systems to a known good state. To support recovery, dutyholders should have adequate backups of systems with agreed Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). A common principle is the 3-2-1 backup strategy that states there should be 3 copies of data (production data and 2 backup copies) on two different media with one copy off-site for disaster recovery. Inspectors should consider: • Does the dutyholder have a policy for testing IT and OT backup systems? • Does the dutyholder backup and test the recovery of key IT and OT systems? • Does the recovery process include data integrity checks at completion of the recovery activity? • What is the backup strategy, plan and testing regime for cloud systems?	➤ 対応チームのメンバーは、被害を制限するために必要な対応措置決定に必要なスキルと知識を備え、実行する権限を持っているか? ➤ 事業者は、サービス復旧の優先順位付けに関する明確な方法論を持っているか? システムは、その重要性に基づいて優先順位付けされているか? ➤ 事業者は、数日から数週間に及ぶ可能性のある長期の事象に対処する能力を持っているか? ➤ 主要ネットワークと情報システムが故障または利用不能になった場合、重要な機能（ただし、レベルは低下する可能性がある）を継続的に運用できるように、すぐ起動できるフェイルオーバーメカニズムが利用可能か? ➤ 必要に応じて、事業者の事象対応能力を外部サポート（サイバー事象対応の専門スタッフなど）で強化する方策があり、テスト済みか? ✓ サイバー 事象が発生した場合、システムを既知の良好な状態に復旧するにはバックアップが必要。復旧をサポートするため、事業者は合意された復旧時間目標（RTO）と復旧ポイント目標（RPO）を備えたシステムの適切なバックアップを用意すべき。一般的な原則は、3-2-1 バックアップ戦略。 ✓ 検査官の考慮事項 ➤ 事業者は IT および OT バックアップシステムをテストするためのポリシーを持っているか? ➤ 事業者は主要な IT および OT システムのバックアップとリカバリのテストを行っているか? ➤ リカバリプロセスには、リカバリ活動の完了時にデータの整合性チェックが含まれているか?
--	--	--	--	---	---

					➤クラウドシステムのバックアップ戦略、計画、テスト体制は何か?
			8. Identification	50. Dutyholders should ensure that capabilities exist to detect/identify cyber security incidents affecting, or with the potential to affect, categorized functions defined within SyAPs. This would include those systems affecting the protection of SNL.	ONR ・8. 特定 ✓ 事業者は、SyAP で定義・分類された機能に影響を与えるサイバーセキュリティ事象を検出／特定する機能があることを確認すべき。
				Security Monitoring 51. The Organization or third party provider should monitor the security status of networks and systems supporting the operation of categorized functions, in order to detect potential security problems and to track the ongoing effectiveness of protective security measures. The data sources that dutyholders include in their monitoring should allow for timely identification of security events in order to achieve the associated cps outcome identified for a particular system. Inspectors should consider: - Is the dutyholder’s monitoring based on an understanding of their network’s baseline characteristics, common cyber-attack methods and what they need awareness of in order to detect potential security incidents that could affect the operation of their essential function (e.g. presence of malware, malicious emails, and user policy violations.)? - If monitoring is provided by a third party then does the dutyholder have the people, processes and technology in place to adequately respond to the incident? - Does the monitoring data provide enough detail to reliably detect security incidents that could affect the operation of their essential function? - Can the dutyholder detect the presence or absence of indicators of compromise on systems delivering or supporting essential functions? - Does extensive monitoring of user activity in relation to the operation of essential functions enable the dutyholder to detect policy violations and an agreed list of suspicious or undesirable behaviour? - Does the dutyholder have multi-layer monitoring coverage that includes host-based monitoring and network gateways? - Are new systems considered as potential monitoring data sources to maintain a comprehensive monitoring capability? - Does the dutyholder provide appropriate security monitoring measures if the systems for essential functions cannot provide host-based security monitoring functions or security data? - Does the dutyholder have arrangements in place for out of hours monitoring and incident escalation?	ONR ・セキュリティ監視 ✓ 組織またはサードパーティ・プロバイダの役割（セキュリティ状態の監視、潜在的なセキュリティ問題の検出、保護セキュリティ対策の継続的な有効性の追求）。 ✓ 検査官の考慮事項 ➤事業者の監視は、ネットワークのベースライン特性、一般的なサイバー攻撃方法、および重要な機能の運用に影響を与える可能性のある潜在的なセキュリティ事象を検出するために認識すべき事項(マルウェアの存在、悪意のある電子メール、ユーザーポリシー違反など)を理解した上で行われているか？ ➤第三者が監視を提供する場合、事業者は事象に適切に対応するための人材、プロセス、技術を備えているか？ ➤監視データは、必須機能の運用に影響を与える可能性のあるセキュリティ事象を確実に検出するのに十分な詳細を提供するか？ ➤事業者は、必須機能を提供またはサポートするシステムにおける侵害の兆候の有無を検出できるか？ ➤必須機能の運用に関連するユーザー活動の広範な監視により、事業者はポリシー違反や合意さ

					れた一連の疑わしい振る舞いまたは望ましくない振る舞いを検出できるか？ ➤ 事業者は、ホストベースの監視とネットワークゲートウェイを含む、多層の監視カバレッジを有しているか？ ➤ 包括的な監視機能を維持するために、新しいシステムは潜在的な監視データ源と見なされているか？ ➤ 必須機能のシステムがホストベースのセキュリティ監視機能またはセキュリティデータを提供できない場合、事業者は適切なセキュリティ監視手段を提供しているか？ ➤ 事業者は、時間外監視と事象エスカレーションに関する方策を実施しているか？
				Securing logs 52. Dutyholders should hold logging data securely and grant read only access to accounts with business need. No staff should ever need to modify or delete logging data within an agreed retention period, after which it should be deleted. 53. Inspectors should consider: • Is the integrity of logging data protected, or is any modification detected and attributed? • Does the logging architecture have mechanisms, processes and procedures to ensure that it can protect itself from threats comparable to those it is trying to identify? This should include protecting the function itself, and the data within it. • Is log data analysis and normalisation only performed on copies of the data keeping the master copy unaltered? • Are logging datasets synchronised, using an accurate common time source, so separate datasets can be correlated in different ways? • Is access to logging data limited to those with business need and no others? • Can all actions involving all logging data (e.g. copying, deleting or modification, or even viewing) be traced back to a unique user? • Are legitimate reasons for accessing logging data given in use policies? • Are logs retained long enough for incident response analysts to inspect during an incident? • Are logs easily accessible for the analyst during an incident?	ONR • ログの保護 ✓ 事業者のログデータ保護義務 ✓ 検査官の考慮事項 ➤ ログデータの整合性は確保されているかまたは変更が検出され原因が特定されるか？ ➤ ログアーキテクチャには、識別しようとしている脅威に匹敵する脅威から自身を保護できるメカニズム、プロセス、および手順書があるか？ これには、機能自体とその中のデータの保護が含まれる。 ➤ ログデータの分析と正規化は、マスターコピーを変更せずにデータのコピーに対してのみ実行されているか？ ➤ ログデータセットは、正確な共通時間ソースを使用して同期されているため、個別のデータセットを様々な方法で関連させることができるか？ ➤ ログデータへのアクセスは、事

					業上必要なユーザーのみに制限されているか？ ➤すべてのログデータに関連するすべてのアクション(コピー、削除、変更、または表示など)を一意のユーザーにまで遡ることができるか？ ➤ログデータにアクセスする正当な理由は、使用方針に記載されているか？ ➤ログは、事象対応アナリストが事象発生時に検査するのに十分な期間保持されているか？ ➤ログは、事象発生時にアナリストが容易にアクセス可能か？
				Generating alerts 54. Dutyholders should ensure that evidence of potential security incidents contained in their monitoring data is reliably identified and triggers alerts. Inspectors should consider: • Is logging data enriched with other network knowledge and data when investigating certain suspicious activity or alerts? • Are a wide range of signatures and indicators of compromise used for investigations of suspicious activity and alerts? • Can alerts be easily resolved to network assets using knowledge of networks and systems? • Are security alerts relating to all essential functions prioritised and this information is used to support incident management? • Are logs reviewed almost continuously, in real time? • Are alerts tested to ensure that they are generated reliably and that it is possible to distinguish genuine security incidents from false alarms? • Are rules reviewed on a regular basis to ensure they are effectively able to identify malicious tactics, techniques and procedures (TTP's) aligned with the MITRE ATT&CK framework or other applicable frameworks and the evolving threat landscape? • Is relevant threat intelligence utilised to aid efficient alerting? • Is the dutyholder aware of critical devices that cannot generate logs or pass logs to the SIEM and have compensatory measures for them? • If logs from a network or single host stop being received, does the dutyholder have sufficient monitoring in place?	ONR • 警報の生成 ✓ 事業者は、監視データに含まれる潜在的なセキュリティ事象の証拠が確実に識別され、警報がトリガーされるようにすべき。 ✓ 検査官の考慮事項 ➤特定の疑わしい活動や警報を調査する際に、ログデータは他のネットワーク知識やデータで強化されているか？ ➤疑わしい活動や警報の調査には、様々なシグネチャーや侵害の兆候が使用されているか？ ➤ネットワークとシステムの知識を使用して、ネットワーク資産への警報を簡単に解決できるか？ ➤すべての重要な機能に関連するセキュリティ警報が優先され、この情報が事象管理のサポートに使用されているか？ ➤ログはほぼ継続的にリアルタイムで確認されているか？ ➤警報が確実に生成され、本物のセキュリティ事象と誤報を区別できることを保証するために、警報がテストされているか？ ➤MITRE ATT&CK フレームワーク

					またはその他の適用可能なフレームワーク、および進化する脅威の状況に沿った悪意のある戦術、手法、および手順 (TTP) を効果的に識別できるように、ルールが定期的に見直されているか？ ➤ 関連する脅威インテリジェンスが、効率的な警報を支援するために活用されているか？ ➤ 事業者は、ログを生成できないまたはログを SIEM に渡すことができない重要なデバイスを認識しており、それらに対する補償措置を講じているか？ ➤ ネットワークまたは単一のホストからのログの受信が停止した場合、事業者は十分な監視を実施しているか？
				Identifying security incidents Dutyholders should contextualise alerts with knowledge of the threat and their systems, to identify those security incidents that require some form of response. Dutyholders should have a process of categorization based on the type and severity (impact on confidentiality, integrity and availability) to allow quick and efficient triaging of incidents. This will help to determine the urgency and escalation thresholds to support dutyholder response. A useful resource for establishing such a framework is the NCSC incident Management Guidance severity matrix and categorization table [22]. Inspectors should consider: • Does the dutyholder gauge the severity of impact of the incident in order to deliver a proportionate response? • Has the dutyholder selected threat intelligence feeds using risk-based and threat-informed decisions based on their business needs and sector (e.g. Vendor reporting and patching, anti-virus providers, sector and sector-based information sharing)? • Have they applied all new signatures and indicators of compromise within a reasonable (risk-based) time of receiving them? • Does the dutyholder receive signature updates for all their protective technologies (e.g. anti-virus, IDS)? • Does the dutyholder track the effectiveness of its intelligence feeds and actively share feedback on the usefulness of indicators of compromise and any other indicators with the threat community (e.g. civil nuclear sector, threat intelligence providers, government agencies)? • Is there a process for initial determination i.e. who declares an incident based on observable events?	ONR • セキュリティ事象の把握 ✓ 事業者は、脅威とシステムに関する知識に基づいて警報を文脈化し、何らかの対応が必要なセキュリティ事象を特定すべき。 ✓ 検査官の考慮事項 ➤ 事業者は、適切な対応を行うために、事象影響の重大度を評価しているか？ ➤ 事業者は、事業ニーズとセクター (ベンダー報告とパッチ適用、ウイルス対策プロバイダー、セクターとセクターベースの情報共有など) に基づいて、リスクベースおよび脅威情報に基づく決定を使用して脅威インテリジェンス フィードを選択したか？ ➤ 新しいシグネチャーと侵害の兆候をすべて、受信後 (リスクに基づく) 妥当な時間内に適用したか？ ➤ 事業者は、すべての保護技術 (アンチウイルス、IDS など) のシグネチャー更新を受信している

				• Is there a process for assigning an initial handler and assigning responders? • Have survey identification points been pre-determined? • Is there an understanding of the limitations of the incident response capability? (knowing when to call in others) • Have checklists been pre-prepared, for example, to check asset state against a known good baseline? • Does the IR team have up to date network architecture diagrams? • Is there a process for performing system and network activity consistency/baselining checks? • Have potential key decisions been identified and worked through in advance?	か？ ➤ 事業者は、インテリジェンス フィードの効果を追跡し、侵害の兆候やその他の兆候の有用性に関するフィードバックを脅威コミュニティ (民間原子力セクター、脅威インテリジェンス プロバイダー、政府機関など) と積極的に共有しているか？ ➤ 初期判定のプロセス (すなわち、観察可能なイベントに基づいて事象を宣言する人) はあるか？ ➤ 最初のハンドラーを割り当て、対応者を割り当てるプロセスはあるか？ ➤ 調査識別ポイントは事前に決定されているか？ ➤ 事象対応機能の制限について理解しているか？ (いつ他の人を呼び出すか把握しているか) ➤ 資産の状態を既知の良好なベースラインと比較するためのチェックリストが事前に準備されているか？ ➤ IR チームは最新のネットワークアーキテクチャ図を持っているか？ ➤ システムおよびネットワーク活動の一貫性/ベースラインチェックを実行するプロセスはあるか？ ➤ 潜在的な重要な決定事項が事前に特定され、検討されているか？
				Incident Notification 55. When an incident is identified, the incident response team must make notifications both within the dutyholder Organization, and external to it. Incident response policies should include provisions for incident reporting - at a minimum, what must be reported, to whom and at what times (e.g. initial notification, regular status updates). In some cases, there are time critical legislative reporting requirements. The exact reporting requirements will vary among dutyholder Organizations, but parties that are typically notified include: • Individuals in the Organization’s security vertical and relevant executives • Other internal incident response team members	ONR • 事象の通知 ✓ 事象が特定された場合、事象対応チームは事業者組織内と外部の両方に通知すべき。 ✓ 検査官の考慮事項 ➤ 事業者は、規制当局や第三者に通知するための事象報告の要件とプロセスに精通しているか？

				• External incident response support resource • System owner • Communications team • National Cyber Security Centre • ONR and/or other regulators (e.g. ICO) as appropriate • National Cyber Crime Unit/ Police • Anyone with whom a contractual arrangement or parent body Organization ownership arrangement exists e.g. a Contracting Authority, Group Headquarters or Government Department e.g. Department for Energy Security and Net Zero (DESNZ). Inspectors should consider: 56. Is the dutyholder familiar with the incident reporting requirements and processes to inform regulators and third parties?	
				Monitoring tools and skills 57. A dutyholder’s monitoring staff must have skills, tools, and roles that reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff must have knowledge of the essential functions and data they need to protect. 58. Inspectors should consider: • Does the dutyholder have monitoring staff, who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and performance? • Do monitoring staff have defined roles and skills that cover all parts of the monitoring and investigation process? • Are there playbooks to ensure consistency and to enable monitoring staff to make the determination regarding the initial validity of the alert in front of them as quickly as possible? • Do monitoring staff follow processes and procedures that address all governance reporting requirements, internal and external? • Are monitoring staff empowered to look beyond the fixed process to investigate and understand non-standard threats, by developing their own investigative techniques and making new use of data? • Do their monitoring tools make use of all logging data collected to pinpoint activity within an incident? • Can their monitoring staff and tools drive and shape new log data collection and make wide use of it? • Are monitoring staff aware of the operation of essential functions and related assets and can identify and prioritise alerts or investigations that relate to them?	ONR • 監視ツールとスキル ✓ 事業者の監視スタッフは、ガバナンスと報告の要件、予想される脅威、および使用すべきネットワークまたはシステムデータの複雑さを反映したスキル、ツール、および役割を備えているべき。 ✓ 検査官の考慮事項 ➤ 事業者には、セキュリティとパフォーマンスの両方をカバーする監視警報の分析、調査、および報告を担当する監視スタッフがいるか？ ➤ 監視スタッフは、監視および調査プロセスのすべての部分をカバーする定義された役割とスキルを備えているか？ ➤ 一貫性を確保し、監視スタッフが目の前の警報の初期の有効性に関する判断をできるだけ早く行えるようにするためのプレイブックはあるか？ ➤ 監視スタッフは、内部および外部のすべてのガバナンス報告要件に対応するプロセスと手順にしたがっているか？ ➤ 監視スタッフは、独自の調査手法を開発し、データを新しく使用することで、固定プロセスを超えて非標準の脅威を調査して

					理解する権限を与えられているか？ ➤ 監視ツールは、収集されたすべてのログ データを使用して、事象内の活動を正確に特定しているか？ ➤ 監視スタッフとツールは、新しいログ データの収集を推進および形成し、それを幅広く使用できるか？ ➤ 監視スタッフは、重要な機能と関連資産の動作を認識しており、それらに関連する警報または調査を識別して優先順位を付けることができるか？
				Proactive security event and abnormality discovery 59. The dutyholder should detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature based security prevent/detect solutions (or when standard solutions are not deployable). 60. The dutyholder should define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify. 61. Inspectors should consider: • Does the dutyholder fully understand normal system behaviour to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity (i.e. do they fully understand which systems should and should not communicate and when)? • Are system abnormality descriptions from past attacks and threat intelligence, on dutyholder and other networks, used to signify malicious activity? • Do the system abnormalities they search for consider the nature of attacks likely to impact on the networks and information systems supporting the operation of essential functions? • Are the system abnormality descriptions they use updated to reflect changes in their networks and information systems and current threat intelligence?	ONR ・積極的なセキュリティ事象および異常の検出 ✓ 事業者は、ネットワークと情報システム内で、重要な機能の動作に影響を与える、または影響を与える可能性のある悪意のある活動を検出すべき。 ✓ 事業者は、システム動作の異常の例を定義し、それ以外では識別が難しい悪意のある活動を検出する実用的な方法を提供すべき。 ✓ 検査官の考慮事項 ➤ 事業者は、システム異常の検索が悪意ある活動を検出する潜在的に効果的な方法であるほど、通常のシステム動作を完全に理解しているか (どのシステムがいつ通信すべきか、通信すべきでないかを完全に理解しているか)？ ➤ 事業者および他のネットワークにおける過去の攻撃や脅威インテリジェンスからのシステム異常の説明は、悪意のある活動を示すために使用されているか？ ➤ 彼らが検索するシステム異常は、重要な機能の運用をサポートするネットワークおよび情報

					システムに影響を与える可能性のある攻撃の性質を考慮しているか？ ➤彼らが使用するシステム異常の説明は、ネットワークおよび情報システムの変更と現在の脅威インテリジェンスを反映するように更新されているか？
				Proactive attack discovery 62. Dutyholders should use an informed understanding of more sophisticated attack methods and of normal system behaviour to monitor proactively for malicious activity. Inspectors should consider: - Does the dutyholder routinely search for system abnormalities indicative of malicious activity on the networks and information systems supporting the operation of their essential function, generating alerts based on the results of such searches? - Does the dutyholder have justified confidence in the effectiveness of their searches for system abnormalities indicative of malicious activity? - Does the dutyholder routinely test the capability of the monitoring service to detect cyber incidents based on new and existing threats?	ONR - 積極的な攻撃の発見 ✓ 事業者は、より洗練された攻撃方法と通常のシステム動作に関する十分な知識を活用して、悪意のある活動を積極的に監視すべき。 ✓ 検査官の考慮事項 ➤ 事業者は、重要な機能の運用をサポートするネットワークおよび情報システム上で悪意のある活動を示すシステム異常を定期的に検索し、そのような検索の結果に基づいて警報を生成しているか？ ➤ 事業者は、悪意のある活動を示すシステム異常の検索の有効性に正当な自信を持っているか？ ➤ 事業者は、新しい脅威と既存の脅威に基づいてサイバー事象を検出する監視サービスの機能を定期的にテストしているか？
			9. Containment, Eradication and Recovery	63. In line with RGP this TAG combines the Containment, Eradication and Recovery phase as there is a degree of overlap and iteration between each. 64. The containment phase sees responders work to limit any system damage caused by an incident and take measures to prevent further damage occurring.	ONR 9. 封じ込め、根絶、復旧 ✓ RGP に従い、この TAG は封じ込め、根絶、復旧の各フェーズを組み合わせる。各フェーズの間にはある程度の重複と反復がある。 ✓ 封じ込めフェーズでは、対応者が事象によるシステム被害を最小限に抑え、さらなる被害の発生を防ぐ対策を講じる。
				Incident characterization and containment strategy 65. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g. isolate an endpoint, shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and	ONR - 事象の特性評価と封じ込め戦略 ✓ 封じ込めの重要な部分は意思決定 (エンドポイントの隔離、システムのシャットダウン、ネットワーク

				procedures for containing the incident. 66. Containment strategies vary based on the type of incident. For example, the strategy for containing an email-borne malware infection is quite different from that of a network-based DDoS attack. Inspectors should consider: - Has the dutyholder identified the major incident types that could impact its operations? - Has the dutyholder created separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision-making? - Has the dutyholder defined risk appetite for incident handling? - Do the containment strategies enable the Organization to remain within that risk tolerance? - Does the dutyholder have means to monitor for potential re-infection during the containment, eradication and recovery phase?	から切断、特定の機能を無効化など)。 ✓ 封じ込め戦略は事象の種類によって異なる。 ✓ 検査官の考慮事項 ➤ 事業者は、業務に影響を与える可能性のある主要な事象の種類を特定したか？ ➤ 事業者は、意思決定を容易にするために基準を明確に文書化した上で、主要な事象の種類ごとに個別の封じ込め戦略を作成したか？ ➤ 事業者は、事象処理のリスク許容度を定義したか？ ➤ 封じ込め戦略により、組織はそのリスク許容度内にとどまることができますか？ ➤ 事業者は、封じ込め、根絶、復旧の段階で再感染の可能性を監視する手段を持っているか？
				Evidence gathering and handling 67. Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings. In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved. 68. Computer based digital evidence is fragile in nature and may be altered or destroyed through improper handling or examination. Forensic processes should ensure the use of a write blocker to ensure that data is not inadvertently changed. 69. Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court. In particular, a master copy and a working copy of the imaged data should be made in line with best forensic practice. Any forensic services provider should be accredited to ISO17025, the legal standard for admissible evidence, as a minimum. 70. Whenever evidence is transferred from person to person, chain of custody forms should detail the transfer and include each party's signature. A detailed log should be kept for all evidence, including the following: - Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer). - Name, title, and phone number of each individual who collected or handled the evidence during the investigation.	ONR - 証拠の収集と取扱い ✓ 事象中に証拠を収集する主な理由は事象の解決であるが、法的手続きにも必要になる場合がある。 ✓ コンピュータベースのデジタル証拠は本質的に壊れやすく、不適切な取り扱いや検査によって変更または破壊される可能性がある。 ✓ 証拠は、法務スタッフや適切な法執行機関との以前の話し合いから策定された、すべての適用法および規制を満たす手順にしたがって収集すべき。 ✓ 証拠が人から人へと転送されるときは常に、保管記録フォームに転送の詳細を記載し、各当事者の署名を含めるべき。 ✓ 検査官の考慮事項 ➤ 事業者スタッフは、ACPO デジタル証拠に関するグッドプラクティスガイドの 4 原則に沿って証拠を保存するための適切な資格と

				- Time and date (including time zone) of each occurrence of evidence handling. - Locations where the evidence was stored. Inspectors should consider: - Are dutyholder staff suitably qualified and experienced for preserving evidence in line with the four principles in the ACPO Good Practice Guide for Digital Evidence [22].	経験を有しているか？
				Short-term containment 71. The focus of this step is to limit the damage as soon as possible. Short-term containment can be as straightforward as isolating a network segment of infected workstations to taking down production servers that were hacked and having all traffic routed to failover servers. Short-term containment is not intended to be a long-term solution to the problem; it is only intended to limit the incident before it gets worse. Inspectors should consider: - Does the dutyholder have pre-agreed procedures for containment (e.g. disconnecting networks)? - Does the dutyholder have a process to record temporary changes?	ONR - 短期的な封じ込め ✓ このステップの焦点は、できるだけ早く被害を抑えること。 ✓ 検査官の考慮事項 ➤ 事業者は封じ込めのために事前に合意された手順書を持っているか (ネットワークの切断など)? ➤ 事業者は一時的な変更を記録するプロセスを有しているか？
				System forensics 72. Before wiping and reimaging any system it is necessary to take a forensic image of the affected system(s) with tools that are well known in the computer forensics community such as Forensic Tool Kit (FTK), EnCase, et al. The reason behind this is that the forensic software will capture the affected system(s) as they were during the incident and thereby preserving evidence in the event that the incident resulted from a criminal act or to be used for observing how the system(s) were compromised during the lessons learnt phase. Inspectors should consider: 73. Do dutyholders have forensic capability or arrangements to call on a third party?	ONR - システムの法医学的検査 ✓ システムをワイプして再イメージ化する前に、法医学的検査ツールキット (FTK)、EnCase などのコンピューターの法医学的検査コミュニティでよく知られているツールを使用して、影響を受けたシステムの法医学的検査 イメージを取得すべき。 ✓ 検査官の考慮事項 ➤ 事業者は法医学的検査能力または第三者を呼ぶ方策を有しているか？
				Recovery 74. In this step affected systems should be rebuilt to remove any malware such as a logic bomb which can activate at a time of choosing by the threat actor. other activities may include removing accounts and/or backdoors left by attackers on affected systems, installing security patches on both affected and neighbouring systems, and doing other work to limit any further escalation of the incident while allowing normal business operations to continue. 75. Eradication is usually necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. Often threat actors will attempt to maintain persistence on systems beyond the scope of the initial incident. During eradication, it is therefore important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is	ONR - 復旧 ✓ このステップでは、影響を受けたシステムを再構築して、脅威アクターが選択したタイミングでアクティブ化できるロジックボムなどのマルウェアを削除すべき。 ✓ マルウェアの削除や侵害されたユーザーアカウントの無効化など、事象の要素を排除するには、通常、根絶が必要。 ✓ 復旧の目的は、影響を受けたシステムを制御された方法で実稼働環

			either not necessary or is performed during recovery. 76. The purpose of recovery is to bring affected systems back into the production environment in a controlled way to ensure that further outbreaks do not occur. It is essential that dutyholders test, monitor, and validate the systems that are being put back into production to verify that they are not being re-infected or compromised by some other means. 77. Eradication and recovery may involve restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). 78. RGP would be to use disk images that were created prior to a system being deployed into production to restore the system, and then installing patches and disabling unused services to harden the system against further attacks. Dutyholders should also scan affected systems and/or files with anti-malware software to ensure any latent malware is removed. Inspectors should consider: · Does the dutyholder have in place arrangements to ensure the continuity of critical operations during a prolonged containment stage? · Does the dutyholder have a contemporary asset inventory that identifies the system and asset categorization ? · Does the dutyholder have pre-prepared plans for rebuilding critical systems to a known good state and returning them to service in appropriate timescales? · Does the dutyholder have long-term containment plans that identify network segregation options, system and asset isolation strategies etc? · Does the dutyholder have procedures in place for restoring key systems to a known good state? 79. Where third party system vendors are involved does the dutyholder have SLAs in place to recover systems?	境に戻して、さらなる感染が発生しないようにすること。 ✓ 根絶と復旧に含まれること。 ✓ RGP は、システムを本番環境に展開する前に作成されたディスク イメージを使用してシステムを復元し、その後パッチをインストールして未使用のサービスを無効にして、システムをさらなる攻撃から保護すること。 ✓ 検査官の考慮事項 ➤ 事業者は、長期にわたる封じ込め段階中に重要な操作の継続性を確保するための手配を整えているか？ ➤ 事業者は、システムと資産の分類を識別する最新の資産インベントリを持っているか？ ➤ 事業者は、重要なシステムを既知の良好な状態に再構築し、適切な時間枠でサービスに戻すための計画を事前に準備しているか？ ➤ 事業者は、ネットワーク分離オプション、システムと資産の分離戦略などを特定する長期的な封じ込め計画を持っているか？ ➤ 事業者は、主要なシステムを既知の良好な状態に復元するための手順を整えているか？ ➤ サードパーティのシステムベンダーが関与している場合、事業者はシステムを復旧するためのSLAを整備しているか？
	10. Lessons Learnt	79. Dutyholders should ensure that when an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents. 80. Dutyholders should use lessons learnt from incidents to improve their security measures. This can be during an incident to inform the containment and eradication phase or post incident to improve security controls. Inspectors should consider: · Does the dutyholder ensure that root cause analysis is conducted routinely as a key part of their lessons learnt activities following an incident?	ONR ・ 10. 教訓 ✓ 事業者は、事象が発生した場合、根本原因を理解し、将来の事象に対して適切な回復処置を講じる手順が取られることを確実化すべき。 ✓ 事業者は、事象から学んだ教訓を用いてセキュリティ対策を改善すべき。	

			・ Is the root cause analysis comprehensive, covering Organizational process issue, as well as vulnerabilities in their networks, systems or software? ・ Is all relevant incident data made available to the analysis team to perform root cause analysis? ・ Does the dutyholder have a documented incident review process/policy which ensures that lessons learnt from each incident are identified, captured, and acted upon? ・ Does the dutyholder’s lessons learnt process/policy cover issues with reporting, roles, governance, skills and Organizational processes as well as technical aspects of networks and information systems? ・ Do they use lessons learnt to improve security measures, including updating and retesting response plans when necessary? ・ Are security improvements identified as a result of lessons learnt prioritised, with the highest priority improvements completed quickly? ・ The lessons learnt may reveal vulnerabilities in the system. Is lessons learnt on a “need to know” basis and part of policy?	✓ 検査官の考慮事項 ➤ 事業者は、事象後の教訓活動の重要な部分として、根本原因分析が定期的に実施されるようにしているか？ ➤ 根本原因分析は包括的で、組織プロセスの問題だけでなく、ネットワーク、システム、またはソフトウェアの脆弱性もカバーしているか？ ➤ 分析チームが根本原因分析を実行するために、関連するすべての事象データを利用できるか？ ➤ 事業者は、各事象から学んだ教訓が特定され、記録され、対処されることを保証する、文書化された事象レビュープロセス/ポリシーを有しているか？ ➤ 事業者の教訓プロセス/ポリシーは、報告、役割、ガバナンス、スキル、組織プロセス、およびネットワークと情報システムの技術的側面に関する問題をカバーしているか？ ➤ 必要に応じて対応計画を更新および再テストするなど、教訓を使用してセキュリティ対策を改善しているか？ ➤ 教訓の結果として特定されたセキュリティの改善は優先順位が付けられ、最も優先度の高い改善は迅速に完了しているか？ ➤ 教訓により、システムの脆弱性が明らかになる場合がある。教訓は「必要に応じて」公開され、ポリシーの一部となっているか？
法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant Legislation	4. The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR. It is also used to refer to those holding SNI. ・ ・	NRA ・ 適用法令 ONR ・ 規制との関係（CNS ガイドほぼ共通の記載、概要は CNS-TAST-GD-1.1 の比較表参照）

				✓ 「事業者」の定義 ✓ NISR 要件の概要
		4. Relationship to IAEA Documentation and Guidance	7.The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) and its amendment [5]. Further guidance is available within IAEA Technical Guidance and Implementing Guides. ・ ・	ONR ・ IAEA 文書との関係（CNS ガイドほぼ共通の記載、検査対象のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照）
		5. Relationship to National Policy Documents	12. The SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission or measures in place demonstrating they have effective processes in place to achieve Security Delivery Principle (SyDP) 7.5 – Preparation for and Response to Cyber Security Incidents in support of FSyP 7 – CS&IA. The TAG is consistent with other CNSS TAGs and associated guidance and policy documentation. ・ ・	ONR ・ 国の政策文書との関係（CNSガイドほぼ共通の記載、FSyP／SyDP の原則番号のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照）
参考文献	—	References	・ ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” 2017. ・ HM Government, “The Nuclear Industries Security Regulations 2003 (NISR),” 2003. ・ ・	—
用語集	—	Glossary and Abbreviations	BC&DR : Business Continuity and Disaster Recovery CERT : Computer Emergency Response Team ・ ・	—
別紙・附属書	—	Appendix	—	—
改訂情報	変更日、施行日、変更概要（「制定」）	（表紙および本文前に記載）	Revision / Issue No., Date など Revision commentary	—

2.4.2.10 PP1705「非常の場合の対応」と CNS-TAST-GD-10.2 (Issue 2.2)「Testing and exercising the security response」における調査の結果

原子力規制庁が用いる検査ガイド PP1705「非常の場合の対応」と、ONR の検査ガイド CNS-TAST-GD-10.2 (Issue 2.2)「Testing and exercising the security response」の主な内容を調査、整理した。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-10 にまとめた。

2.4.2.10.1 監督領域

原子力規制庁の検査ガイドでは、監督領域を定義し、どの分野を検査するか示している。

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.10.2 序論

原子力規制庁の検査ガイドでは、特に記載していない。

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（表 2.4.2-1 と同じ）。

2.4.2.10.3 検査の目的

原子力規制庁の検査ガイドでは、法的な位置づけと目的（非常の場合の対応について確認）を簡潔に記載している。

ONR の検査ガイドでは、検査ガイドの目的（検査官がセキュリティ緊急事態対応のテストおよび演習に関する方策を評価する際の一般的な助言と情報を提供）について説明している。

2.4.2.10.4 検査要件

原子力規制庁の検査ガイドでは、検査対象、検査頻度等、検査体制を簡潔に記載している。

ONR の検査ガイドでは、検査官への助言（核セキュリティ事象への効果的な対応策、演習、規制上の期待事項、該当する FSyP など）を記載している。

2.4.2.10.5 検査手順

原子力規制庁の検査ガイドでは、次の内容を簡潔に記載している。

- ・ 確認事項
- ・ 文書、ウォークダウン、インタビューを活用して確認
- ・ 検査前準備、検査、CAP 検査の趣旨

ONR の検査ガイドでは、次のように分けて説明している。

次の各項目について、検査のポイントを含む解説および検査官の考慮事項を示している。

- ・セキュリティ対応の訓練と演習の方策に関するガイダンスの解説
- ・適切に資格認定された経験豊富な職員の解説
- ・REDE の実施の解説
 - ✓ REDE 計画プロセスの解説
 - ✓ 目標、成功基準、シナリオの解説
 - ✓ 悪意あるアクターの解説
 - ✓ サイトのセキュリティを維持するの解説
- ・検査官の考慮事項

2.4.2.10.6 法令・基準等

原子力規制庁の検査ガイドでは、規則および審査基準を列挙している。

ONR の検査ガイドでは、NISR 要件の概要、IAEA 文書との関係、国の政策文書との関係などを記載している。

2.4.2.10.7 改訂情報

原子力規制庁の検査ガイドでは、変更日、施行日、簡潔な変更理由（「記載の適正化」）を記載している。

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2. 4. 2-10 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-10.2 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド 【ガイド】PP1705 非常の場合の対応 （2023/05/31 記載の適正化）（2 頁）		英国 ONR 検査ガイド 【ガイド】CNS-TAST- GD-10.2 (Issue 2.2) Testing and exercising the security response （September 2024）（16 頁）		両者間の主な相違点	
項目		主な内容			
図書全体構成		図書全体構成		—	
本文	監督領域	大分類および小分類：「核物質防護」 評価領域：「核物質防護体制」 検査分野：「非常の場合の対応」	ガイド ID カテゴリー	CNS	NRA ・ 監督領域の区分 ONR ・ ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	1. The Office for Nuclear Regulation (ONR) has established a set of Security Assessment Principles (SyAPs) [1]. This document contains Fundamental Security Principles (FSyPs) that dutyholders must demonstrate have been fully considered in developing their security arrangements to meet relevant legal obligations. The security regime for meeting these principles is described in security plans prepared by the dutyholders, which are approved by ONR under the Nuclear Industries Security Regulations (NISR) 2003 [2]. 2. The term ‘security plan’ covers all dutyholder submissions such as nuclear site security plans, temporary security plans and transport security statements. NISR Regulation 22 dutyholders may also use the SyAPs as the basis for Cyber Security and Information Assurance (CS&IA) documentation that helps them demonstrate ongoing legal compliance for the protection of Sensitive Nuclear Information (SNI). The SyAPs are supported by a suite of guides to assist ONR inspectors in their assessment and inspection work, and in making regulatory judgements and decisions. This Technical Assessment Guidance (TAG) is such a guide.	NRA ・ とくになし ONR ・ 序論（CNS ガイド共通、概要は CNS-TAST-GD-1.1 の比較表に同じ）

	検査の目的	2.1 目的 法第 61 条の 2 の 2 第 1 項第 3 号ロで規定される事項（核物質防護規定）のうち、非常の場合の対応について確認する。 これらの確認については、非常の場合の対応の検査分野における体制、訓練・教育および設備の保全のほか、警備員等の力量にも留意する。 2.2 防護措置の狙い 非常の場合の対応を万全とすることにより、必要な核物質防護に係る措置を維持する。	2. Purpose and Scope	3.This TAG contains guidance to advise and inform ONR inspectors in exercising their regulatory judgment during assessment activities, relating to a dutyholder’s arrangements, to test and exercise the security contingency response. It aims to provide general advice and guidance to ONR inspectors on how this aspect of security should be assessed. It does not set out how ONR regulates the dutyholder’s arrangements. It does not prescribe the detail, targets or methodologies for dutyholders to follow in demonstrating they have addressed the SyAPs. It is the dutyholder’s responsibility to determine and describe this detail and for ONR to assess whether the arrangements are adequate.	NRA - 検査の目的 ✓ 法的な位置づけと目的（非常の場合の対応について確認） ONR - 本ガイド（TAG）の目的 ✓ 検査官がセキュリティ緊急事態対応のテストおよび演習に関する方策を評価する際の一般的な助言と情報を提供
	検査要件	3.1 検査対象 非常の場合の対応についての全てが検査対象となり得るが、本検査では、限られた数の検査対象（サンプル）を選定し、それら対象について検査を実施することとする。サンプル選定に際しては、非常の場合の対応措置の状況を考慮し、検査対象を選定する。 3.2 検査の頻度等 （１）検査の頻度 ３年間に１回程度 （２）検査時間 ３人／０．７５（h） 3.3 実施体制 （１）当該検査に係る資格・知識を有する対策官をリーダーとして実施する。 （２）必要に応じて他部門の協力・支援（技術的な助言や専門検査官の現場派遣など）を要請できる。	6. Advice to Inspectors	12. Effective response arrangements to a NSE are an integral part of the overall strategy for ensuring nuclear or other radioactive material and any associated vital areas are properly secured. Maintenance of an exercise programme, stringent self-evaluation via post security contingency exercise reports and decisively acting on lessons identified, are key indicators of a dutyholder’s understanding of the importance of an effective security response. 13. Exercising allows for personnel with emergency and security response responsibilities to be trained in the Security Contingency Plan (SCP). It also provides an opportunity to rehearse the arrangements described in the SCP and test their effectiveness. Therefore, security response drills should be undertaken regularly if staff and contractors are to be familiar with procedures, the actions to be taken and their responsibilities in the event of a real or suspected NSE. 14. Dutyholders are also expected to deliver a Regulator Evaluated Demonstration Exercise (REDE). However, these are a demonstration of capability and should not be used for training or exercising. 15. This TAG informs regulatory assessment of the dutyholder’s Emergency Preparedness and Response arrangements from a security perspective, arrangements for testing and exercising of the SCP. Regulatory expectations 16. The regulatory expectation placed on the dutyholder is that they should demonstrate within their security plan how they maintain an effective programme to test and exercise the SCP. Table 1: Fundamental security principle (FSyP) 10 FSyP 10 - Emergency Preparedness and Response / Testing and Exercising the Security Response / SyDP 10.2 Dutyholders should implement a regime of exercising to train	NRA - 検査要件（概略） ✓ 検査対象、検査頻度等、検査体制 - 検査手順 ✓ 確認事項 ✓ 文書、ウォークダウン、インタビューを活用して確認 ✓ 検査前準備、検査、CAP 検査の趣旨 ONR 6. 検査官への助言 ✓ 核セキュリティ事象（NSE）に対する効果的な対応策 ✓ 演習により、緊急対応およびセキュリティ対応の責任を負う職員がセキュリティ緊急対応計画 (SCP) の訓練を受けられる。 ✓ 事業者は、規制当局評価実証演習 (REDE) も実施することが求められる。 ✓ この TAG は、セキュリティの観点から見た事業者の緊急事態準備および対応の方策、SCP のテストおよび演習の方策に関する規制評価を通知する。 ✓ 規制上の期待事項 ➤ 事業者がセキュリティ計画で、SCP をテストおよび演習する効果的なプログラムをどのように維持しているか示すこと ✓ 表 1: 基本セキュリティ原則 (FSyP) 10 ➤ FSyP 10 - 緊急事態準備および対応／セキュリティ対応のテストおよび演習／SyDP 10.2 （事業者は、職員を訓練し、核セキュリティ緊急時対応計画の有効性をテストす

				personnel and test the efficacy of the nuclear security contingency plans.	る演習体系を実施すべき。)
	検査手順	非常の場合の対応に関する活動が適切に行われていることを関連文書の調査、ウォークダウン、インタビュー等によって確認する。 4.1 検査前準備 非常の場合の対応に係る関連文書を確認する。 4.2 検査の実施 対策官は、事業者が実施する非常の場合の対応に係る措置が審査基準に適合していることを確認する。 4.3 問題点の特定と解決に関する確認 (1) 本検査に関連する核物質防護に影響を及ぼす問題が特定された場合は、是正措置プログラム (CAP) 等において是正処置が適切に講じられていることを確認する。 (2) 本検査に関連する不適合の履歴からサンプルを抽出し、当該不適合が適切な期間内に適切な是正処置が講じられ、問題点の特定と解決が行われていることを確認する。	7. Guidance on arrangements for training and exercising the security response	17. The dutyholder should deliver a training programme that: - Ensures members of the Site Emergency Organization (SEO) are trained and remain competent to be suitably qualified and experienced persons (SQEP), for their role and responsibilities as required under the SCP. - Demonstrates SEO integration and interoperability in order to deliver the required PPS Response and Required Effect in an effective and timely manner. - Conducts an appropriate combination of ‘live’ and ‘table-top’ Security Contingency Exercises (SCXs) at regular intervals throughout the year, that is comparable to safety exercise activities. - Includes, wherever possible, off-site first responders. - Implements an assurance regime for SCXs and associated training, in order that: - Activities are recorded at individual and collective level - Performance is assessed and reviewed objectively and documented, with good practice and learning points incorporated into the SCP and used to inform future training needs and plans.	ONR 7. セキュリティ対応の訓練と演習の方策に関するガイダンス ✓ 事業者は次のような訓練プログラムを実施すべき。 ➤ サイト緊急対応組織 (SEO) のメンバーがセキュリティ緊急事態計画 (SCP) で要求される役割と責任を果たす適切な資格と経験を持つ人材 (SQEP) として訓練を受け能力を維持できる。 ➤ 必要な物理的防護システム (PPS) 対応と必要な効果を効果的かつタイムリーに提供するために、SEO の統合と相互運用性を実証する。 ➤ 安全演習活動に匹敵する「ライブ」と「テーブルトップ」のセキュリティ緊急対応演習 (SCX) を年間通じて定期的に適切に組み合わせて実施する。 ➤ 可能な限り、オフサイトの第一対応者を含める。 ➤ SCX と関連する訓練の保証体制を実装し、次のことを行う。 ○ 活動は個人レベルと集団レベルで記録される ○ パフォーマンスは客観的に評価およびレビューされ、文書化される。グッドプラクティスと学習ポイントは SCP に組み込まれ、将来の訓練ニーズと計画への情報提供に使用される。
				18. ONR promotes an enabling approach to outcome focussed regulation, which acknowledges the benefits of reducing the regulatory burden to the dutyholder wherever possible. Accordingly, we acknowledge that an informed, risk-based approach to dutyholder’s demonstrations of their arrangements should be proportionate and (potentially) achievable. 19. As part of the non-prescriptive SyAPs approach, there is no automatic expectation that sites should demonstrate annually, although delivering a ‘regular’ demonstration (as specified in NISR) is an expectation. Regulatory judgements about the frequency of REDEs are likely	ONR ・REDE の実施 ✓ ONR は、可能な限り事業者の規制負担を軽減することの利点を認めるパフォーマンス重視規制の有効なアプローチを推進している。 ✓ サイトは毎年でなく「定期的な」実証を行うことが期待されている。 ✓ REDE の頻度に関する規制上の判断。 ✓ 期待事項は、核物質／その他放射性物質 (NM/ORM) の保有と 枢要区域 (VA) (ある場合)、サイトのリスクと脅威のプロファ

				to be delivered on a site-by-site basis and based on the 'graded approach' and the relevant ONR site inspection team's analysis. The form of demonstration, depending on regulatory judgement, can be either a full practical REDE or a combination of a tabletop/command-post exercise. 20. Expectations are to be based on the NM/ORM holdings and VAs (if any), risk and threat profile of the site. Other key factors to consider will include outstanding regulatory issues as a result of the dutyholder previous demonstration and adequacy of extant arrangements of the dutyholder's training, testing and exercising regime for the SEO.	イルに基づく。
				8.1. REDE Planning Process 21. The dutyholder should deliver a planning process that: • Secures agreement from the appropriate ONR inspector for an ONR observed 'live play' or 'table-top' REDE, in a timely manner to allow for annual planning processes. • Ensures that the CNC (where deployed) give prior agreement to the date for a REDE. • Conducts an initial planning meeting (excluding exercise participants), no less than six months before the date of the exercise. The meeting should be attended by the ONR security inspector and/or ONR emergency preparedness and response security inspector. The draft exercise objectives and success criteria should be forwarded to the ONR security inspector prior to the meeting. Where appropriate a representative from the CNC (where applicable) and any other relevant stakeholders (internal and external) should also attend these meetings. Subsequent meetings to develop the scenario should be held as required with the ONR inspector attending where needed. • Ensures all elements of the SEO are exercised. In addition, an agreed and meaningful proportion of the work force is to take part in the demonstration. • Produces an exercise instruction that is forwarded to reach ONR no later than four weeks prior to the date of the exercise. • Undertakes a REDE review meeting (to be attended by all relevant stakeholders) no later than six months after the REDE has taken place.	ONR • 8.1 REDE 計画プロセス ✓ 事業者が実施すべきプロセスの説明
				8.2. Objectives, success criteria and scenarios 22. The dutyholder should: • Maintain a record/matrix to ensure all aspects of the SCP	ONR • 8.2 目標、成功基準、シナリオ ✓ 事業者の実施すべき事項の説明

				are exercised against relevant threats within a reasonable period. • Ensure the objectives, success criteria and scenario for the SCX are agreed with ONR in advance prior to the initial planning meeting. • The objectives and success criteria should be decided first and then applied to a scenario that allows the SCP to be demonstrated in a proportionate manner. They should: - o Be challenging and fully expose security contingency planning and response to a NSE. - o Reflect multiple aspects of the SCP, elements of the emergency plan and/or handbook. - o Challenge the Command, Control and Communication (C3) of the SEO at OPERATIONAL and TACTICAL levels, and the integration of external stakeholders. - o Require exercise participation at all levels, from OPERATIONAL first responders to TACTICAL actions of personnel in command roles. - o Consider previous REDEs both in terms of the malicious scenario chosen and any learning points arising. Unless a requirement of ONR, the dutyholder should ensure that differing DBT actors are used than that on previous demonstrations. - o Be agreed by all stakeholders. - o Driven by the security outcome required of the Physical Protection System (PPS) and associated response as defined in Annex C and D of SyAPs. • The following objectives could be utilised: - o To establish and maintain a comprehensive understanding of the situation, to cater for the worst credible developments, formulate measures and plans to achieve recovery and prevent deterioration of the situation. - o Mobilise, deploy and direct appropriate resources in the most effective and timely manner. - o Demonstrate site's ability to mitigate the security, safety and environmental threats posed. - o Ensure adequate arrangements are in place for the arrival of off-site first responders, including an effective process for their reception, staging and onward integration. - o Demonstrate adequate consideration and arrangements for preservation of a crime scene and concurrent post-incident recovery.	
--	--	--	--	--	--

				- o Demonstrate arrangements to notify all external agencies and for responding to public and media enquiries. - o To demonstrate a comprehensive record of events and decision-making is taken for evidence preservation and for use in informing subsequent investigations. 23. The dutyholder could consider a flexible approach towards achieving objectives and success criteria, through incorporating a series of scenarios in order to demonstrate a range of capabilities in responding to an NSE. Use of a phased approach may offer the following opportunities: • Phase 1 - Immediate Response. Phase 1 could allow the dutyholder, in conjunction with the CNC and/or other on or off-site responders, to demonstrate operational capability against a credible threat. Where applicable it will involve the CNC (where deployed), the Civilian Guard Force (CGF), local police force first responders and all C3 elements of the Site Emergency Organization (SEO). • Phase 2 – Event Management. Phase 2 could allow the dutyholder to demonstrate effective management of the event, integrated with all relevant supporting agencies and responders. The same scenario as Phase 1 or a completely different one can be used. • Phase 3 – Consequence Management. Phase 3 could allow the dutyholder to demonstrate an understanding of the post-incident recovery and their facilitation of crime scene management in a response to a NSE. Phase 3 would typically be exercised via a table-top exercise. As with phase 2, it may utilize the same scenario as earlier phases or have a completely different one, depending on the exercise objectives and success criteria.	
				8.3. Malicious actor(s) 24. The dutyholder should: • Include malicious capabilities drawn from the extant United Kingdom Design Basis Threat (UKDBT). Specifically, they should identify a malicious actor(s) with target objectives that accords with the category of the site, which can be used to realistically test arrangements across all phases of the site's response to an NSE. The arrangements should demonstrate that the Physical Protection System (PPS) Response and Required Effect can consistently and effectively be delivered to achieve the required security outcome.	ONR • 8.3 悪意あるアクター ✓ 事業者が実施すべきことの説明

				• Ensure REDEs are conducted using ‘live-play’ malicious actors, based on relevant threats and capabilities given in the UKDBT, and that the scenario(s) properly reflects the consequence of compromise (theft and sabotage) of the NM/ORM/VAs and facilities on the site. On sites required to meet PPS Outcome 4, a malicious presence on site may not be required and, subject to approval from ONR, the malicious actor could be simulated.	
				8.4. Maintain the security of the site 25. The dutyholder should ensure the security of the site is maintained whilst the REDE and associated training is being conducted. Measures that could be considered include: • Compensating for the abstraction of personnel who are attending training by deploying additional SQEP staff to undertake the roles of those engaged in training. • Develop temporary security plans, where appropriate, for approval by ONR before any activity takes place. For example, this could be for buildings left insecure post-evacuation. Inspectors should consider: • Does the security plan define an effective REDE delivery process and training programme for the Site Emergency Organization (SEO)? • Are all relevant stakeholders involved in the exercise and training programme planning process? • Is there a structured and informed planning process to facilitate a REDE? • Is there an audit in place that records individual and collective training in delivering roles, responsibilities and required effects of the SCP? • Is there an audit of performance assessment of the SEO undertaking SCXs? • Are a range of SCX scenarios, objectives and success criteria developed that are specific to the site characteristics? • Does the security plan ensure that the dutyholder’s REDE and SCXs demonstrate their arrangements across the immediate response, event management and consequence management phases of a response to a NSE? • Does the security plan require realistic SCX scenarios that reflect relevant UKDBT capabilities and the required PPS Response and Required Effect for the site? • Does the security plan require that a formal review of SCXs is undertaken and that good practice and learning points are disseminated to relevant stakeholders? • Does the security plan ensure that the PPS of the site and key	ONR • 8.4 サイトのセキュリティを維持する ✓ 事業者は、REDE および関連する訓練が実施されている間、サイトのセキュリティが維持されるようにすべき。 • 検査官の考慮事項 ✓ セキュリティ計画には、サイト緊急対応組織 (SEO) 向けの効果的な REDE 配信プロセスと訓練 プログラムが定義されているか？ ✓ すべての関連する利害関係者が、演習および訓練 プログラムの計画プロセスに関与しているか？ ✓ REDE を促進するための構造化された情報に基づいた計画プロセスがあるか？ ✓ SCP の役割、責任、および必要な効果を実行するための個人および集団の訓練を記録する監査が実施されているか？ ✓ SCX を実施する SEO のパフォーマンス評価の監査はあるか？ ✓ サイトの特性に固有のさまざまな SCX シナリオ、目標、成功基準が策定されているか？ ✓ セキュリティ計画では、事業者の REDE と SCX が、NSE への対応の即時対応、イベント管理、結果管理の各フェーズにわたってその取り決めを実証することを確実にしているか？ ✓ セキュリティ計画では、関連する UKDBT 機能と、サイトに必要な PPS 対応と必要な効果を反映した現実的な SCX シナリオを要求しているか？ ✓ セキュリティ計画では、SCX の正式なレビューを実施し、優れた実践と学習ポイントを関連する利害関係者に広めることを要求しているか？

				facilities is maintained throughout a SCX /REDE? 26. Further information on ONR-observed exercises can be found in ONR’s Technical Inspection Guide [8].	✓ セキュリティ計画では、サイトと主要施設の PPS が SCX /REDE 全体にわたって維持されることを確実にしているか？ ✓ ONR が観察する演習の詳細については、ONR の技術検査ガイド参照。
	法令、基準等	(1) 実用炉規則第 91 条 (2) 研開炉規則第 86 条 (3) 加工規則第 7 条の 9 (4) 貯蔵規則第 36 条 (5) 再処理規則第 16 条の 3 (6) 審査基準	3. Relationship to Relevant Legislation	4.The term ‘dutyholder’ mentioned throughout this guide is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation, a ‘developer’ carrying out work on a nuclear construction site and approved carriers, as defined in NISR [2]. It is also used to refer to those holding SNI. ...	NRA ・適用法令 ONR ・規制との関係（CNS ガイドほぼ共通の記載、概要は CNS-TAST-GD-1.1 の比較表参照） ✓ 「事業者」の定義 ✓ NISR 要件の概要
			4. Relationship to IAEA Documentation and Guidance	6.The essential elements of a national nuclear security regime are set out in the Convention on the Physical Protection of Nuclear Material (CPPNM) [3] and the IAEA Nuclear Security Fundamentals [4]. Further guidance is available within IAEA Technical Guidance and Implementing Guides. ...	ONR ・IAEA 文書との関係（CNS ガイドほぼ共通の記載、検査対象のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照）
			5. Relationship to National Policy Documents	9.SyAPs provide ONR inspectors with a framework for making consistent regulatory judgements on the effectiveness of a dutyholder’s security arrangements. This TAG provides guidance to ONR inspectors when assessing a dutyholder’s submission to see if they have demonstrated effective processes in place to achieve SyDP 10.2 – Testing and Exercising the Security Response, in support of FSyP 10 – Emergency Preparedness and Response. The TAG is consistent with other TAGs and associated guidance and policy documentation. ...	ONR ・国の政策文書との関係（CNS ガイドほぼ共通の記載、FSyP/SyDP の原則番号のみ相違、概要は CNS-TAST-GD-1.1 の比較表参照）
参考文献		—	References	・ ONR, “Security Assessment Principles (SyAPs) for the Civil Nuclear Industry,” 2017. [Online]. Available: https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/security-assessment-principles-syaps/. ・ HM Government, “The Nuclear Industries Security Regulations 2003 (NISR),” 2003. [Online]. Available: https://www.legislation.gov.uk/ukxi/2003/403/contents/made....	—
用語集		—	Glossary and Abbreviations	C3 : Command, Control and Communications CNC : Civil Nuclear Constabulary ...	—
別紙・附属書		—	Appendix	—	—
改訂情報		変更日、施行日、変更概要（「記載の適正化」）	（表紙および本文前に記載）	Revision / Issue No., Date など Revision commentary	—

2.4.2.11 CNS-INSP-GD-001 (Issue 1) 「Nuclear Security Inspections」における調査の結果

原子力規制庁検査ガイドに対応するものがないため、ONR の検査ガイドの主な内容を調査、整理した。この検査ガイドは、セキュリティ検査で共通したものなどをまとめたガイドである。調査した結果の主な内容を以下に示す。詳細は、表 2.4.2-11 にまとめた。

2.4.2.11.1 監督領域

ONR の検査ガイドでは、とくに定義していない。検査ガイドの大分類（CNS=核セキュリティ）が ID 記号から分かる程度である。

2.4.2.11.2 序論

ONR の検査ガイドでは、全ての検査ガイドに共通する留意事項を記載している（原子力産業セキュリティ規制（NISR）、アウトカムベースのセキュリティ評価原則 SyAPs（基本セキュリティ原則 FSyPs 含む）、SyAPs を支えるセキュリティ実現原則（SyDPs）などに関する事項）。

2.4.2.11.3 目的

ONR の検査ガイドでは、この上位文書の目的を次のように記載している。

- ・ SP に記載された標準・手順書・方策（SPA）の妥当性を、技術評価ガイド（TAGs）を用いて評価する。
- ・ この TIG（CNS-INSP-GD-001）により 一貫した効率的な検査を支援する。

2.4.2.11.3 適用範囲

- ・ ONR の検査ガイドでは、この核セキュリティ検査の適用範囲を次のとおりとしている。
 - ①サイバーセキュリティ
サイバーセキュリティ、情報保証、サプライチェーン
 - ②防護セキュリティ
物理的セキュリティ、輸送セキュリティ、人的セキュリティ
- ・ 検査の視点（SPA の実施を重視）、課題の抽出、事業者の改善に向けたインプット提供など、検査官への一般的な助言を記載している。

2.4.2.11.4 定義

ONR の検査ガイドでは、用語の定義、略語一覧表を記載している。

2.4.2.11.5 ガイダンス

ONR の検査ガイドでは、次のことについて解説している。

- ・ セキュリティ検査の目的
- ・ 2003 年原子力産業セキュリティ規制（NISR 2003）適合のガイダンス

- ・ SPA とその実施の検査ガイダンス
 - ✓ 検査対象 SPA の選定およびスコーピング
 - ✓ 検査実施ガイダンス
 - ✓ 戦略的イネーブラー検査ガイダンス
 - ✓ 主席原子力検査官の検査テーマの支援

2.4.2.11.6 改訂情報

ONR の検査ガイドでは、表紙に改訂番号、発行日、次回見直し予定日などを簡潔に記載している。

表 2.4. 2-11 原子力規制庁検査ガイドと英国 ONR 検査ガイド CNS-TAST-GD-2.1 の比較調査結果：主な相違点のまとめ

原子力規制庁検査ガイド		英国 ONR 検査ガイド		両者間の主な相違点
【ガイド】 — (—)		【ガイド】 CNS-INSP-GD-001 (Issue 1) Nuclear Security Inspections (August 2023) (18 頁)		
項目	主な内容	項目	主な内容	
図書全体構成	—	図書全体構成	表紙 目次 本文 参考文献 付録 改訂情報	—
本文	監督領域	—	ガイド ID カテゴリー	CNS ONR ガイドの大分類（CNS=核セキュリティ）
	—	—	1. Introduction	ONR 1. 序論 ✓ 原子力産業セキュリティ規制（NSIR）は、原子力施設と施設に貯蔵されている核物質（NM）・その他放射性物質（ORM）のセキュリティ確保を要求している。 ✓ ONR はアウトカムベースのセキュリティ評価原則（SyAPs）を設けており、これに基づいて事業者のセキュリティ計画（SP）を評価する。 ✓ SyAPs およびそれを支えるセキュリティ実現原則（SyDPs）はアウトカムベースで事業者の SP に何を含むべきかは規範的に規定していない。 ➤ 事業者は、セキュリティ方策の策定、実施、有効性の保証に責任を有する。 ➤ 事業者は承認済のセキュリティ計画を ONR に提出する。 ➤ ONR は SP との（したがって NSIR との）適合性を定期的に検査する。
	—	—	1.1 Purpose	ONR 1.1 目的 ・ SPに記載された標準・手順・方策（SPA）の妥当性を、技術評価ガイド（TAGs）を用いて評価する。 ・ この TIG により一貫した効率的な検査を支援す

				dutyholder’s SP. Once an SP has been approved by ONR, this Technical Inspection Guide (TIG) assists inspectors in judging compliance against the approved SP. 5. The purpose of this TIG is to facilitate a consistent and effective approach to inspecting compliance with SPA described in an approved SP. It is applicable across the Nuclear Security purpose and therefore covers both Protective Security and Cyber Security and Information Assurance, as well as their sub-specialisms.	る。
		—	1.2 Scope and Applicability	6. This TIG is applicable to all ONR security specialisms and sub-specialisms: - Cyber Security and Information Assurance - Cyber Security - Information Assurance - Supply Chain - Protective Security - Physical Security - Transport Security - Personnel Security 7. The term “standards, procedures and arrangements” (SPA) is used extensively throughout NISR 2003 in reference to nuclear premises, approved carriers, and holders of SNI. Full explanations and application can be found in NISR 2003 (Ref [1]). 8. The judgements made by the inspector will relate primarily to implementation of SPA described in the SP, to ensure that the written claims, arguments and evidence (CAE) are fully demonstrated on the ground. This guide will assist in making consistent regulatory judgements and decisions. 9. Inspectors are reminded that an inspection may reasonably require review of the described SPA themselves (as distinct from their implementation). As ONR takes a sampling approach to regulation, it is possible that elements of an approved SP have not previously been assessed. It is also possible that a security situation may evolve over time. Therefore, when reviewing or inspecting evidence as part of a compliance inspection, inspectors may also form judgements on the adequacy of the SPA described in the approved SP. 10. Straightforward judgements might be addressable as part of the inspection, (for instance through updating supporting documentation referenced in the SP e.g. local working instructions) or through raising a regulatory issue.	ONR 1.2 適用範囲 ①サイバーセキュリティ サイバーセキュリティ、情報保証、サプライチェーン ②防護セキュリティ 物理的セキュリティ、輸送セキュリティ、人的セキュリティ ・ 検査の視点（SPAの実施を重視）、課題の抽出、事業者の改善に向けたインプット提供

				Alternatively, inspector observations can provide regulatory intelligence which assists in targeting future ONR assessment activity. SyAPs (Regulatory Assessment of Security Plans (RASyP) 7 – Security Plan Maintenance) advises that an SP should be actively maintained and reviewed regularly, and dutyholders should welcome regulatory input in the interests of continuous improvement. 11. This TIG should not be regarded as either comprehensive or mandatory, but provides a framework for inspectors on which to base their judgements and discretion during such inspections.	
		—	1.3 Definitions	12. Within this document, the term security plan (SP) refers primarily to site security plans required under NISR 2003 (Ref [1]) Regulation 4, and Transport Security Statements (TSS) required under Regulation 16. It may also apply to written cyber security and information assurance arrangements adopted by Regulation 22 dutyholders. 13. The term standards, procedures and arrangements (SPA) refers to the totality of a SP, including SPA explicitly detailed within, relied upon, or referenced by, the plan. For example (not exhaustive) it can be interpreted to cover: • any Security System, Structure or Component (SySSC) such as an intrusion detection system, IT network firewall, or security camera etc. • any Task Important to Nuclear Security (TINS) such as the conduct of vetting checks, IT network monitoring, or conduct of searching etc. • any standard such as a social media policy, homeworking policy etc. 14. The term ‘dutyholder’ is used to define ‘responsible persons’ on civil nuclear licensed sites and other nuclear premises subject to security regulation; a ‘developer’ carrying out work on a nuclear construction site; approved carriers, as defined in NISR 2003; and those handling, storing and processing (or proposing to do so) SNI . Table 1 – Table of Acronyms (内容省略)	ONR 1.3 定義 ✓ 用語の定義 ➢ セキュリティ計画 ➢ 標準、手順書および方策 (SPA) ➢ デューティホルダー ✓ 略語一覧表 (表 1)

	検査の目的	—	2. Purpose of Security Inspection	15. The primary purpose of the inspection is to ensure compliance with the law. NISR 2003 (Ref [1]), Regulation 7 states that the responsible person in relation to each nuclear premises must comply with the SPA described in the approved SP for the premises. Similarly, Regulation 17 states that an approved carrier must comply with the SPA described in an approved TSS. This is the basis for the majority of ONR security inspections: ensuring the dutyholder is complying with the approved plan. 16. Whilst this principle holds true for the majority of ONR security activity, some specialist areas may deviate slightly and merit additional explanation: • Transport Security – Class B carriers. NISR 2003 applies to all approved carriers, but ONR takes a proportionate approach in relation to the size and structure of carrier Organizations and the category of NM they are approved to transport. Class B approved carriers based at UK civil licensed nuclear sites may incorporate transport security arrangements into their approved SP. For other Class B approved carriers, it will be sufficient that SPA described in the TSS comply with ‘Guidance for Class B Approved Carriers’ (Ref. [3]). • Personnel Security / Workforce Trustworthiness. ONR ensures dutyholders’ workforce trustworthiness arrangements comply with His Majesty’s Government (HMG) Government Functional Standard GovS007: Security (Ref. [4]) and other underpinning documents (including the OFFICIAL-SENSITIVE Personnel Security Policy, HMG Personnel Security Controls, and UK Government guidance on the pre-employment screening of civil servants, members of the armed forces, temporary staff and government contractors). Additional areas of mandated workforce trustworthiness compliance exist within ONR SyAPs, specifically annexes (OFFICIAL-SENSITIVE) relating to the mandated clearance levels to be applied, dutyholders’ signing authorities against the Baseline Personnel Security Standard, and visit arrangements. Such arrangements shall be contained within a nuclear site’s SP or an approved carrier’s transport security statement. • Supply Chain - Regulation 22 Dutyholders. As Regulation 22 dutyholders are not required to produce	ONR 2. セキュリティ検査の目的 ✓ 法令遵守の確保（NSIR で事業者は承認済み SP に記載されている SPA を遵守しなければならないと規定）。 ✓ この原則は一部の分野では若干相違がある： ➤ 輸送セキュリティ（クラス B 輸送業者） ➤ 人事セキュリティ／作業員の信用性 ➤ サプライチェーン（SP が要求されていないケース：App. A 参照） ➤ 規制当局評価演習（REDE）（DBT に対する緊急時対応能力の実証）
--	-------	---	-----------------------------------	--	--

			an SP for approval, ONR has a different arrangement for gathering assurance regarding their securing of SNI and application of relevant good practice. This arrangement is detailed in Appendix A. • Regulator Evaluated Demonstration Exercises (REDE). REDEs are a means by which a dutyholder must demonstrate that they can: implement effective and integrated emergency preparedness and response arrangements, for all credible events based upon the Design Basis Threat (DBT); achieve the required security outcomes, with the appropriate level of confidence; and effectively manage the consequences of such DBT events. The scope of a REDE, its associated objectives and supporting scenario should be agreed by the inspection team. A REDE should be evaluated against specific areas and functions and associated performance statements. It is for the inspection team to decide which areas and performance statements are relevant, taking account of the required security outcomes, the characteristics of the site, the challenges presented by the scenario and agreed objectives. The inspection team should not be beholden to, or constrained by, the exercise performance criteria established by the dutyholder. If a REDE is judged to be inadequate, then the inspection team must decide whether a full or partial re-demonstration is required. Further guidance on evaluating REDEs and associated relevant good practice is contained in the associated guidance document ‘Regulator Evaluated Demonstration Exercises – Aide Memoire for Inspectors’ (Ref [5]).	
検査要件	—	3. Guidance on NSIR 2003 compliance	17. NISR 2003 (Ref [1]), Regulation 4 sets out the need for an approved SP to be in place at all times which describes the SPA to ensure the security of the elements specified within this regulation and which are applicable to the dutyholder. It further describes a number of key aspects that require additional and specific consideration: pre-employment checks and national security vetting; movement of NM; equipment and software used in connection with activities involving nuclear material / ORM; policing and guarding, and contingency plans. Finally, it covers the consideration of threats posed to existing sites by plant and machinery being used during	ONR 3. NISR 2003 適合のガイダンス ✓ NISR（原子力産業セキュリティ規制）の要件の補足説明 ➤ 規則 4 では、承認された SP を常に実施する必要性について規定 ➤ 原子力施設：規則 7 では、施設の責任者は承認済 SP に記載されている SPA を遵守すべきことを規定 ➤ 原子力施設：規則 9 では、指定された職員は適切な性格と誠実さを備えていると評価されている者とするを規定

				construction of an adjacent site. 18. Nuclear premises: Regulation 7 states that the responsible person in relation to each nuclear premises must comply with the SPA described in the approved SP for the premises. Regulation 9 states that specified personnel must have been assessed to be of suitable character and integrity. 19. Transport security and approved carriers: Regulation 17 states that an approved carrier must comply with the SPA described in an approved TSS. (See also paragraph 15 regarding Class B carriers.) 20. Regulation of SNI, uranium enrichment equipment and software: Regulation 22 sets out the need for those specified to maintain such security SPA as are necessary for the purpose of minimising the risk of loss, theft or unauthorized disclosure of, or unauthorized access to, any sensitive nuclear information, uranium enrichment equipment or uranium enrichment software within their possession or control. Details of how ONR determines whether or not the risk has been minimised are contained in Appendix A. 21. Full wording can be found in NISR 2003, and comprehensive guidance on interpretation of the law is provided in ONR publication ‘Nuclear Industries Security Regulations 2003 - Guidance for Inspectors’ (Ref. [6]).	➤ 輸送セキュリティと承認済み運送業者：規則 17 では、承認済み運送業者は承認済み TSS に記載されている SPA を遵守すべきと規定 ➤ SNI、ウラン濃縮装置およびソフトウェアの規制：規則 22 では、指定された者が、所有または管理下にある機密情報、ウラン濃縮装置、またはウラン濃縮ソフトの紛失、盗難、不正開示、不正アクセスのリスクを最小限に抑えるために必要なセキュリティ SPA を維持すべきことを規定
	検査手順	—	4. Guidance on inspection of SPA and their implementation	22 This TIG should be read in conjunction with existing ONR guidance on inspection activity, which is both detailed and comprehensive: • ONR-INSP-GD-059 (Guidance for Inspection Strategy Planning and Recording – Ref. [7]) covers the production of annual inspection plans, regulatory attention levels, resource allocation, the integrated intervention strategy, inspection types, and associated governance arrangements. • ONR-INSP-GD-064 (General Inspection Guide – Ref. [8]) covers the stages of the inspection process – Planning, Preparation, Delivery and Record. This guidance applies to all security compliance inspections, whether planned or reactive. It provides detailed advice on a variety of important topics such as use of the WIRed system, inspection ratings, Regulatory Issues and the Enforcement Management	ONR 4 SPA とその実施の検査ガイダンス ✓ この TIG は、詳細かつ包括的な検査活動に関する既存の ONR ガイダンスと併せて読む必要がある。 • ONR-INSP-GD-059 (検査戦略の計画と記録に関するガイダンス) は、年間検査計画の作成、規制の注目レベル、リソースの割り当て、統合介入戦略、検査の種類、および関連するガバナンスの方策について説明。 • ONR-INSP-GD-064 (一般検査ガイド) は、検査プロセスの段階 (計画、準備、実施、記録) について説明

				Model (EMM).	
			4.1 Guidance on selecting and scoping SPA to inspect	23. Compliance inspections are an essential element of ONR's overall intervention strategy on nuclear premises. These are intended to establish that the arrangements within the SP have been effectively implemented, such that they are fit for purpose and will fulfil their security functional requirements, in support of achieving the required security outcome. 24. Whilst it is recognised that all nuclear premises are required by law to have an approved SP, there will be considerable variation between, for example, SPA for an operational reactor site versus a site holding only Cat IV material and undergoing decommissioning. ONR is a sampling Organization and it would not be appropriate to inspect every aspect of SPA compliance with all aspects of every SP. 25. The purpose and principles of enforcement, as set out in the ONR Enforcement Policy Statement (ref. [9]), should be at the forefront of an inspector's mind when undertaking all stages of compliance inspection. In particular, security inspectors should ensure that inspections are targeted according to relevant factors such as regulatory attention level, regulatory strategy, level of risk, and regulatory intelligence. 26. Through interrogation of CAE in the approved SP, inspectors will be able to identify appropriate SPA, their intended function, and the contribution they make towards meeting required security outcomes. Inspectors can then shape the inspection scope, to obtain assurance that SPA have been implemented in accordance with the approved SP and are achieving the necessary effect. 27. SyAPs broadly divides FSyPs into two categories: Strategic Enablers (FSyPs 1-5) and Secure Operations (FSyPs 6-10). Many compliance inspections will include the sampling of selected elements from FSyPs 6-10 (depending on security specialism), which focus upon the operational implementation and maintenance of nuclear security: • FSyP 6: Physical Protection Systems (Categorization for Theft; Categorization for Sabotage; Physical Protection System Design; Vulnerability Assessments; Adjacent or Enclave Nuclear Premises; Nuclear	ONR 4.1 検査対象 SPA の選定およびスコーピング ✓ SPA もフェーズに応じて様々 ✓ サンプルングの観点 ✓ 検査項目の候補 ✓ 評価原則

				Construction Sites; Protection of Nuclear Material During Offsite Transportation). ...	
			4.2 Guidance on inspection delivery	33. Inspectors will inspect SPA as set out in the approved SP, review the implementation of those SPA, and judge whether the dutyholder is complying with the SPA described in the approved SP (NISR 2003, Regulation 7 (Ref [1])). 34. ONR requires inspectors to conduct compliance inspections in accordance with ONR guidance, policy and with an enabling approach (Ref. [10]) which satisfies the provisions of the Regulators Code (Ref. [11]). The inspector should apply the detailed guidance in the ‘General Inspection Guide’ ONR- INSP-GD-064 (Ref [8]). These documents explain a range of regulatory tools and approaches available to inspectors, from influence and persuasion through to formal enforcement. Evaluation of compliance is covered in detail under section 5 (Delivery) of ONR-INSP-GD-064. 35. One additional tool for security inspections is available under NISR 2003 (Ref [1]). Regulation 4.(2) states that an SP must describe the SPA “adopted or to be adopted...” (or for a TSS, Regulation 16.(2)). Measures to be adopted are recorded as a regulatory commitment in the dutyholder’s “Security Improvement Schedule” (or equivalent title), a key supporting document which forms part of the approved SP. It lists regulatory commitments with deadlines for delivery, against which dutyholders can be held to account under NISR 2003. 36. The inspector should adopt a proportionate and graded approach, utilising the history from previous interventions to inform their expectations. Inspectors should ensure that any issues identified in previous interventions have been followed up.	ONR 4.2 検査実施ガイダンス ✓ 適合性の確認 ✓ 規制ツールの利用 ✓ 比例的、グレード別アプローチ
			4.3 Guidance on inspecting strategic enablers	37. This TIG covers security SPA including protective and physical security; emergency preparedness and response; workforce trustworthiness; and cyber security and information assurance. Whilst these form the core of security inspection activity, inspectors must also consider SyAPs strategic enablers, which overlap heavily with the other ONR purposes. SyAPs aligns closely with the Safety Assessment Principles (SAPs) and inspectors should consider a cross-purpose approach. Brief examples include:	ONR 4.3 戦略的イネーブラー検査ガイダンス ✓ SAPs とオーバーラップする領域あり（下記に例示）、両者の目的を念頭に置く（クロス・パーパス・アプローチ） ➤ FSyP 1: Leadership and Management for Security ➤ FSyP 2: Organizational Culture ➤ FSyP 3: Human Performance Management ➤ FSyP 4: Nuclear Supply Chain Management

				• FSyP 1: Leadership and Management for Security · Responsibility, accountability and decision making · Learning from experience (e.g. security events, internal inspections) · Assurance processes to support internal assessment of performance • FSyP 2: Organizational Culture · NS-INSP-GD-070 (Ref. [12]) identifies cultural “warning flags” e.g.: · Overconfidence, lack of healthy unease and drift in standards · Deviation from established arrangements · Impaired sharing and isolationism • FSyP 3: Human Performance Management · Required numbers and competencies of personnel · Ergonomic design of workspaces, equipment and user interfaces · Procedures and administrative controls to minimise human error • FSyP 4: Nuclear Supply Chain Management · Procurement by an intelligent customer · Screening and oversight of suppliers · Commissioning arrangements • FSyP 5: Reliability and Resilience² · Detailed design specification covering reliability and resilience · Contingency to cover periods of maintenance or unserviceability · Records of examination, inspection, maintenance and testing	➤ FSyP 5: Reliability and Resilience
			4.4 Chief Nuclear Inspector Themed Inspections	38. Inspectors may be required to support Chief Nuclear Inspector (CNI) themed inspections. Introduced in 2017, these are designed to examine regulatory matters that are strategic or broader in nature than ONR’s more routine regulatory inspection activities. Previous themes have included climate change, and management of ageing facilities. Further details can be found in ONR-INSP-GD-059, Appendix 1D.	ONR 4.4 主席原子力検査官の検査テーマの支援 ✓ 検査官は、主席原子力検査官 (CNI) のテーマ別検査の支援を求められる場合がある。 ➤ 2017 年に導入されたこの検査は、ONR の日常的な規制検査活動より戦略的またはより広範な規制事項を調査する。 ➤ 以前のテーマには、気候変動や老朽化施設の管理などがあった。詳細は、ONR-INSP-GD-059（検査戦略計画作成および記録に関するガイダンス）、付録 1D（CNI）参照。

参考文献	—	References	• Nuclear Industries Security Regulations 2003. Statutory Instrument 2003 No. 403 • IAEA Nuclear Security Series No. 13. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). January 2011. www- pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf. • .	—
別紙・附属書	—	Appendix	Appendix 1 : Supply Chain / Regulation 22	—
改訂情報	変更日、施行日、変更概要（「制定」）	（表紙に記載）	Revision / Issue No., Date など Table 1 - Revision commentary	—

2.5 検査ガイドの比較調査まとめ

2.3 に示した日米比較結果および 2.4 に示した日英比較結果を踏まえ、それぞれについて主要な相違点等を抽出し、まとめた。

2.5.1 米国 NRC 検査ガイドとの比較調査のまとめ

日米の検査ガイド間において、ガイドの構成、内容などそれぞれの特徴や相違点がみられる。両者間の相違のうち、主なものとして抽出し、整理したものを以下に示す。

- ・ 図書体系
- ・ 検査での確認事項
- ・ 検査手順に関する実務的なガイダンス
- ・ 検査の技術的な根拠

上記の図書体系、検査での確認事項、検査手順に関する実務的なガイダンス、および検査の技術的な根拠について、それぞれの比較結果を以下にまとめる。

2.5.1.1 図書体系

原子力規制庁の検査ガイドは、検査項目別に作成されているが、例えば、セキュリティの検査に共通する内容をまとめたような上位図書は見当たらない。また、参考文献として参照可能な関連図書、または関連資料との関連付けなどの記載は少ない。

一方、NRC の検査ガイドでは、「関係する検査プログラム」欄に、どの分野の検査に係するかを示す情報がある（例えば、IMC 2200 App. A 「建設時セキュリティ検査プログラム」）。IMC は、IP の上位図書になるもので、当該検査領域の検査プログラムとしてまとめられている。また、ほとんどの検査ガイドには、そのガイドの参考文献を多く記載している（例えば、比較まとめ表 2.3.2-5 の IP81311 Physical Security Requirements for Independent Spent Fuel Storage Installations の参考文献欄を参照する）。

検査ガイドとそれに関わる上位図書や関連図書の図書体系を構築し、その中に検査ガイドを位置づけることにより、当該検査ガイドの背景や関連内容、知識を探す際にも便利で、検査に関する視野も広がる。こういった関連知識、知見があれば、検査ガイドに関する共通の理解が深まり、検査ガイドの運用能力の向上が期待できる。

(図書体系に関する比較の例)

NRA

—

NRC

- ・ 検査プログラム（この IP が使用される検査分野を示す、IP の上位図書）

例：

- ✓ IMC 2200 App. A（建設時セキュリティ検査プログラム）

- ・ 参考文献

例：

- ✓ Interim Compensatory Measures (ICMs) for Dry Spent Fuel Storage, October 16, 2002. SLES Reference No. NS106674
- ✓ Additional Security Measures (ASMs) for the Physical Protection of Dry Independent Spent Fuel Storage Installations, September 28, 2007. SLES Reference No. NS106675

2.5.1.2 検査での確認事項

原子力規制庁の検査ガイドでは、「検査の目的」において、検査の法的な位置づけと検査の大きな目的（例えば、「教育および訓練状況の確認」）を簡潔に記載している。また、「検査要件」において、検査対象、検査頻度、検査時間、検査体制を簡潔に記載している。

一方、NRC 検査ガイドは、「検査の目的」において、法的な位置づけは記載していないが、検査で、何を確認するかを具体的に列挙し、標準化している。

NRC が検査の法的な位置づけを記載していないのは、「事業者は、NRC が行う検査を受け入れること」という検査全体を包括した要求を法令に規定しているので、検査ごとに準拠法令を示す必要がないということが背景にある。

検査で、何を確認するかは、検査官にとって非常に重要なことであり、また、標準化することが求められるものである。検査の大きな目的も必要な情報であるが、それだけでは検査対象の選定や検査内容が検査官によってバラつくことが避けられない。実用的な検査ガイドには、何をどう確認するかを標準化された明確な指針を示すことが求められる。

(検査での確認事項に関する比較の例)

NRA

- ・ 1. 検査の目的（次に関する簡潔な記載）
 - ✓ 法的な位置づけと大きな目的
（例：防護区域等への立ち入りの確認）
- ・ 2. 検査要件（次の簡潔な記載）
 - ✓ 検査対象
（例：核燃料物質防護に係る全ての業務に関連する従業者に対する教育計画、内容、実績、被教育者の理解度、現場確認等の全てが検査対象となり得る...）

NRC

- ・ 1. 検査の目的
 - ✓ 検査対象と確認事項を具体的に列挙している
- 例：
1. NRC が承認したセキュリティ計画にしたがって、アクセス許可 (AA) プログラムを開発し、実施中か実施準備できていることを確認する。
 2. エスコートなしのアクセスを許可された個人に対する適切な対策を開発し、実施中か実施準備ができていることを確認する。
 3. エスコートなしのアクセスを許可された個人の継続的な信頼性と信用性を保証する適切な対策を開発し、実施中か実施準備できていることを確認する。
 4. 活動的なインサイダー、活動的で暴力的なインサイダーを緩和する効果的なインサイダー緩和プログラムを開発し、実施中か実施準備できていることを確認・評価する。
 5. このサンプルに関連する物理的防護プログラムが 10 CFR) 73.55(b) の一般的なパフォーマンス目標を満たすよう設計され、実施中か実施準備できているかを確認する。

2.5.1.3 検査手順に関する実務的なガイダンス

原子力規制庁の検査ガイドでは、「3. 検査手順」において、何を確認するか、どのような方法で確認するか、検査前の準備・検査の実施・CAP 検査の趣旨について簡潔に記載されている。詳細は公開されていない。

NRC では、「2. 検査要件」において、その検査共通のガイダンス（ない場合もある）、個別の検査事項とその手順およびガイダンスが詳細に示されている。このうち、共通のガイダンスでは、例えば、その検査ガイドが適用される施設の状態、それに対する検査ガイド適用上の考え方や注意事項などが示されている。また、それに続いて、個別の検査事項ごとに、検査手順および具体的なガイダンスを記載している。

その他、NRC では、同じような検査ガイドでも施設の運転フェーズに分けて作成するなど実用面のことを考慮して検査ガイドを分けている。例えば、セキュリティの訓練に関する検査ガイドは、建設、運転、廃止措置の各フェーズに対応したものが個別に作成されている。

効果的で、効率的な検査を行うためには、施設の状態などに即して、実際に適用できる、そして検査手順やガイダンスの記載が充実している実務的なガイダンスが必要となる。

(検査手順に関する実務的なガイダンスに関する比較の例)

NRA

例：

- ・ 3. 検査手順（次に関する簡潔な記載）
 - ✓ 立ち入りの必要性、資格の確認
 - ✓ 証明書等の発行の適切性を文書、ウォークダウン、インタビューを活用して確認する。
 - ✓ 検査前準備、検査、CAP 検査の趣旨

NRC

例：

- ・ 2. 検査要件
 - ✓ 一般的ガイダンス
 - この検査は、IMC 2200 App. A または IMC 2562 に対応する運転プログラムが開始された場合に実施されることに注意する。
 - 建設中の場合、この IP は、建設中原子炉監視プロセス (cROP) の監視対象となる全ての原子炉に適用される。
 - 運転認可終了後の再起動の場合、この IP は、廃止または長期停止中の原子炉から、ROP 対象の運転中原子炉へ移行中の場合に適用する。
 - 活動の観察による検証が不可能な場合もある。その場合、適切な手順書を確認し、関連する全エリアの検査を実施し、プログラムが遵守されていることを確認する。
 - 物理的防護プログラムが、10 CFR 73.55(b) の一般的なパフォーマンス目標にしたがって設計され、実施されているか準備できていることを確認する。

...

- ・ 2.1 実施手順書
 - a. 立ち入り拒否された職員が、業界共通 DB に含まれることを確実にする手順書の実施方策を確立していることを確認する。

具体的なガイダンス

事業者が、他の事業者と情報共有する方策を確立していることを関連手順書のレビューで確認する（アクセス拒否された個人に関連する情報を共有するメカニズムの実施）。

- ・ b. 身元調査を実施する個人が、身元調査を受ける者の要件と一致する基準を満たすことを確実にする手順書の実施方策を確立していること確認する。

具体的なガイダンス

手順書は、最低限、以下の事項を扱うべきである： (1) 個人の真の身元確認、(2) 州または地方の裁判所を通じた犯履の確認、(3) 地方の信用履歴評価の実施、(4) 過去 3 年間の職歴評価の実施、および (5) 性格および評判の評価の実施。

...

(以下、2.6「レビュー」まで、このように細分化された実施手順と具体的なガイダンスを組み合わせた記載が続く。より詳細は、比較まとめ表参照。)

2.5.1.4 検査の技術的な根拠

NRC では、様々な技術的根拠を文書化しており、検査プログラムに関しても同様である。そのような文書から、背景、経緯が分かり、技術的な根拠が分かる。

セキュリティの検査に関する技術的根拠は、例えば、セキュリティ基本検査ガイド関連で、技術的根拠図書として、次に示す IMC 0308 Attachment 3 Appendix E がある。

- ・ IMC 0308 Attachment 3 Appendix E, “Technical Basis for the Baseline Security Significance Determination Process”

これには、セキュリティ検査の指摘事項について、セキュリティ上の重要度を評価するための SDP の考え方や技術的な根拠が示されており、この SDP をよく理解して運用するための知識・ノウハウがまとめてられている。セキュリティ分野の指摘事項は、パフォーマンスが劣化する前に、迅速に対応することが求められるものがあり、特殊である。

また、今回の調査より、IP 81000.01, “Access Authorization”の上位図書である IMC 2562, “Light-Water Reactor Inspection Program for Restart of Reactor Facilities Following Permanent Cessation of Power Operations”の参考文献に、次のセキュリティ検査指摘事項の需要度決定プロセス（SDP）の技術的根拠を示す文献が含まれている。

(検査の技術的な根拠に関する比較の例)

NRA									
—									
NRC									
・ IP 81000.01 の上位図書 IMC 2562 の参考文献（抜粋）									
<table><tr><th colspan="2">Operational Strategic Performance Area: Reactor Safety</th></tr><tr><th>IMC/IP No.</th><th>Title</th></tr><tr><td>0305</td><td>Operating Reactor Assessment Program</td></tr><tr><td>0308</td><td>Reactor Oversight Process Basis Document</td></tr></table>		Operational Strategic Performance Area: Reactor Safety		IMC/IP No.	Title	0305	Operating Reactor Assessment Program	0308	Reactor Oversight Process Basis Document
Operational Strategic Performance Area: Reactor Safety									
IMC/IP No.	Title								
0305	Operating Reactor Assessment Program								
0308	Reactor Oversight Process Basis Document								
(注) IMC 0308 は、ROP 関係の技術的根拠文書で、多数の Attachment および Appendix で構成されている。そのうち、Att.3 App. E がセキュリティ SDP の技術的根拠である。									

2.5.2 英国 ONR 検査ガイドとの比較調査のまとめ

日英の検査ガイド間において、ガイドの構成、内容などそれぞれの特徴や相違点がみられる。両者間の相違のうち、主なものとして抽出し、整理したものを以下に示す。

- ・セキュリティ指摘事項の評価基準
- ・リスクの考え方
- ・検査に役立つ背景知識・助言の提供
- ・検査に関わるグッドプラクティスの整備と活用

上記のセキュリティ指摘事項の評価基準、リスクの考え方、検査に役立つ背景知識・助言の提供、検査に関わるグッドプラクティスの整備と活用について、それぞれの比較結果を以下にまとめる。

2.5.2.1 セキュリティ指摘事項の評価基準

原子力規制庁が公開している「原子力規制文書」には、原子力安全の指摘事項に係る重要度評価ガイドはあるが、セキュリティの指摘事項に係る重要度評価ガイドはない。

(注：米 NRC には、セキュリティの指摘事項に関する重要度評価ガイド IMC 0609 Att. E がある。) ONR は、セキュリティ分野の評価基準として、セキュリティ評価原則 (SyAPs) を策定し、その中に事業者が適合を実証しなければならない基本的セキュリティ原則 (FSyPs) を含めている。また、規制要件として、原子力産業セキュリティ規制 (NSIR) が定められており、事業者はセキュリティ評価原則への適合とともに、この法令の遵守が求められている。このようなセキュリティ分野の評価基準を定めることで、共通認識に基づいて評価を行うことができる。

(セキュリティ指摘事項の評価基準に関する比較の例)

NRA
—
ONR
1. 序論
1.1
✓ ONR はセキュリティ評価原則(SyAPs)を策定。事業者 (dutyholders) が適合を実証しなければならない基本的セキュリティ原則 (FSyPs) が含まれる。
✓ 事業者は原子力産業セキュリティ規制 (NISIR) に従う。
1.2
✓ セキュリティ計画 (SP)は、サイトセキュリティ計画、一時的セキュリティ計画、輸送セキュリティ計画など全てを含む。
✓ 機微な原子力情報 (SNI) の防護に係るサイバーセキュリティ & 情報保証 (CS&IA) 文書化の根拠も SyAPs を適用可能。
✓ 検査官が SyAPs への適合性判断をする場合、TAG 等のガイダンスを利用可能。

2.5.2.2 リスクの考え方

原子力規制庁の検査ガイドでは、例えば「防護措置の狙い」において「・・・不法行為のリスクを低減する」のようにリスクという用語を使用し、事業者のリスク低減活動を監督している。ただし、リスクをどのように評価するか、管理するかについて、具体的な記載（参考情報など含む）が示されていない。また、規制者として、事業者活動に関するリスクがどの程度か、どのように対応するかについても、具体的な記載は見当たらない。

ONR の検査ガイドでも、随所にリスクという用語を使用しており、事業者によるリスクの評価や管理などを監督している。事業者によるセキュリティ分野のリスク評価やリスク管理については、例えば、CNS-TAST-GD-7.1「効果的なサイバーおよび情報のリスク管理」などの検査ガイドの中に、参考文献例を挙げている。また、検査ガイドではないが、規制者としての対応の考え方については、別途、標準を定めている（行政措置方針）。詳細は、「3.2.5 リスクの考え方の確立と運用指針の整備」を参照する。

（リスクの考え方に関する比較の例）

NRA

1.検査の目的（簡潔に記載）

例：

2.2 防護措置の狙い

- ✓ 核物質防護秘密を厳重に管理することにより、情報漏えいを防止し、不法行為のリスクを低減する。

ONR

・随所に「リスク」について言及

例：

検査官への助言

- ✓ リスク評価のアプローチと方法論等に関するガイダンスは、TAGs 7.1（有効なサイバーおよび情報のリスク管理）、7.3（原子力技術および運転の防護）、7.4（情報の物理的防護）参照。

5.2.1 情報保証戦略

- ✓ 事業者は、CS&IA を実施するための首尾一貫した戦略を有すること。戦略の対象範囲は、TAG 7.1 で定義されているリスク管理プロセスの一環として実施されるリスク評価の範囲と同じとすべき。
- ✓ この戦略は、役員会に正式承認され、サイバー&情報リスク管理を担当するメンバーによって監督されるべき。

検査官の考慮事項

- ✓ 情報および関連資産に対するリスクを特定し管理する戦略が適切か？

2.5.2.3 検査に役立つ背景知識・助言の提供

原子力規制庁の検査ガイドでは、検査に役立つ背景知識などに関する記載は、見当たらない。

一方、ONR の検査ガイドでは、検査ガイドの目的を検査官に「一般的な助言と情報」を提供するものとしており、検査に必要な背景知識や助言を盛り込んでいる。その上で、それらを踏まえた検査の視点を「検査官の考慮事項」として疑問文形式で列挙している。

(検査に役立つ背景知識・助言の提供に関する比較の例)

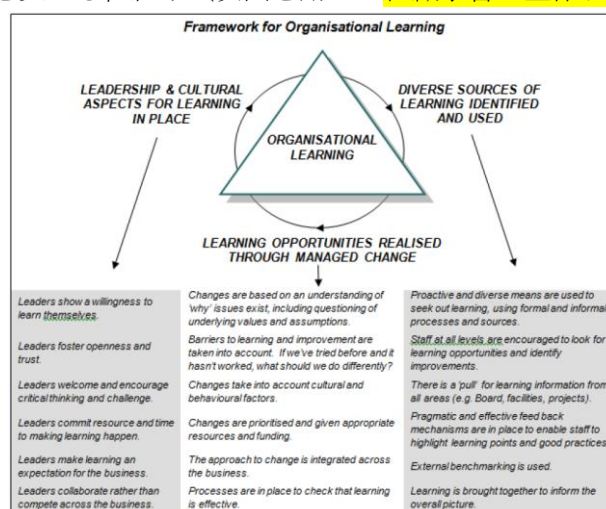
NRA

—

ONR

例：

- ・ 検査ガイドの目的
 - ✓ 検査官が、情報の防護策を評価する際の一般的な助言と情報を提供する。
- ・ 運転に関する学習（以下、CNS-TAST-GD-1.4 の例）
 - ✓ 組織的学習を支える仕組み（次図を用いて組織学習の全体および要素を解説）



- 要素 1. 学習のためのリーダーシップと文化の存在
 - 要素 2. 学習の多様な情報源の特定と利用
 - 要素 3. 管理された変更による学習機会の実現
- ・ 検査官への助言
 - ✓ 組織的学習プログラムの重要性
 - ✓ 組織的学習の意義
 - ✓ 規制の期待事項
 - ✓ 事業者のセキュリティ計画が、組織学習をサポートする明確な構成と枠組みを確実に特定していること
 - ✓ 基本セキュリティ原則（FSyP）1 - L&MfS：組織的学習（セキュリティ実現原則（SyDP）1.4）

・ 検査官の考慮事項：

- ✓ 事業者は、3つの必須要素を含めた組織的学習の仕組みを構築しているか？
- ✓ セキュリティの劣化を体系的に特定および是正する方針が策定されているか？
- ✓ 事業者のセキュリティと安全の OpEx 方針は有効に整合しているか？
- ✓ 事業者は、スタッフにセキュリティの劣化や改善案の報告を奨励しているか？
- ✓ 事業者の方針は、セキュリティの不備を報告した職員への非難でなく、是正措置に重点を置いているか？
- ✓ 事業者は、他組織から積極的に教訓を学び、適切な場合は自組織に適用することを、学習する組織に奨励しているか？
- ✓ 事業者は、その施設で最近生じたセキュリティ問題をスタッフに定期的に報告するとともに、スタッフの理解を新たにする教訓を見出そうとしているか？
- ✓ 事業者は、スタッフと管理者に問題を把握および報告するための十分な訓練を施しており、根本原因分析の訓練を受けた経験豊富なスタッフを十分に有しているか？
- ✓ 事業者は、セキュリティ劣化を管理・報告する十分な資源を割り当てているか、また、それは法令および ONR 要求の報告プロセスに適合しているか？
- ✓ 事業者のプロセスは、事象の分析や新たな傾向を含め、特定されたセキュリティ劣化の知見を役員会に情報提供しているか？
- ✓ 特に悪影響のある傾向について、事象調査や是正措置の終結の実施遅れに関する指標があるか？

2.5.2.4 検査に関わるグッドプラクティスの整備

原子力規制庁のセキュリティ関連検査ガイドでは、セキュリティ検査に関するグッドプラクティスに関する記載（活用含む）は見当たらない。

一方、ONR の検査ガイドでは、「関連グッドプラクティス（RGP）」という用語を規制活動の随所で使用している。セキュリティ検査のグッドプラクティスは、ONR と事業者が協力して開発したものだけでなく、国の機関、海外規制当局（NRC など）、国際機関が開発したものまで様々な RGP が利用可能となっている。

（検査に関わるグッドプラクティスの整備と活用に関する比較の例）

NRA

—

ONR

例：

・検査官への助言（CNS-TAST- GD-10.2）

- ✓ 情報セキュリティの重要性
- ✓ 機微な原子力情報（SNI）
- ✓ SNI のシンプルな定義
- ✓ 情報および関連資産の防護

✓ 関連グッドプラクティス（RGP）の活用

- この検査ガイドは、情報保証の国家技術機関（NTA）である国家サイバーセキュリティセンター（NCSC）提供の RGP を大いに活用した他、国際機関、米国を含む様々な RGP 情報を活用した。

✓ リスク評価のアプローチと方法論等に関するガイダンス文書

具体的な RGP の例を挙げれば、次のようなものがある。

・ CNS-TAST-GD 1.1（Security Governance & LS）で引用されている RGP の例：

- ✓ Independent Oversight Good Practice Guide. Produced by the cross-industry Internal Oversight Working Group (IOWG) and Published on behalf of the Safety Directors Forum (SDF). – December 2018:

https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/IOWG/SDF_sub-group_Good_Practice_Guide_Issue_2.pdf

- ✓ UK Corporate Governance Code. Financial Reporting Council- July 2018.

<https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code>

- ✓ The Wates Corporate Governance Principles for Large Private Companies - Financial Reporting Council- December 2018.

<https://www.frc.org.uk/directors/corporate-governance-and-stewardship/governance-of-large-private-companies>

なお、RGP は、ONR の検査ガイドにある特有の規制アプローチと相まって、「良い方向に導く」ためのツールとして活用されている。詳細は、「3. 2. 6 リスクの考え方の確立 と運用指針の整備」を参照する。

3 検査ガイドの改善内容の検討

3.1 はじめに

検査ガイドの改善内容の検討は、本年度実施した原子力規制庁が用いる検査ガイド（セキュリティ関連）および米国 NRC の検査ガイド（セキュリティ関連）の比較調査結果から得られた日米検査ガイド間の相違点等、原子力規制庁の検査ガイド（セキュリティ関連）および英国 ONR の検査ガイド（セキュリティ関連）の比較調査結果から得られた日英検査ガイド間の相違点等のほか、検査の現状、課題等を踏まえて、より効率的で、効果的な検査の実施を支える実用的な検査ガイドの在り方を念頭に、今後の原子力規制庁の検査制度の運用改善の見直しに資する改善点を検討した。

3.2 検査ガイドの改善内容の検討結果

原子力規制庁が参照する検査ガイドおよび米国 NRC、英国 ONR の検査ガイドの比較調査結果より、日米、日英の検査ガイド間における主な相違を整理し、抽出した結果から、原子力規制庁が用いる検査ガイドに対する改善内容の検討を行った。具体的には、日米、日英検査ガイドの比較調査結果から得られた両者間の主な相違点のほか、原子力規制検査の現状や事業者との議論など原子力規制庁が用いる検査ガイドの今後の改善活動に寄与するような情報を踏まえて、今後原子力規制検査の運用改善に資するような改善点を抽出し、改善内容の検討を行った。以下に、整理した主な検査ガイドの改善内容の検討結果を示す。

日米検査ガイドの比較調査結果から、次の改善策を提案する。

- ・セキュリティ関連検査ガイド図書体系の検討と整備
- ・セキュリティ検査での確認事項の明確化
- ・施設の状態に応じたセキュリティ検査ガイドの拡充および実務的な検査要領の充足
- ・セキュリティ検査根拠図書の整備

日英検査ガイドの比較調査結果から、次の改善策を提案する。

- ・セキュリティ指摘事項に関する評価基準の確立
- ・リスクの考え方の確立と運用指針の整備
- ・セキュリティ検査に役立つ背景知識・助言の提供
- ・セキュリティ検査に関わるグッドプラクティスの整備と活用

上記各改善策の検討内容の詳細を 3.2.1～3.2.8 にまとめた。

3.2.1 セキュリティ関連検査ガイド図書体系の検討と整備

原子力規制庁が用いる検査ガイドは、規制要求事項に従ったガイド構成となっている。対象施設の種類や運用状態などに応じて、どのような検査を行うべきかの検査内容が分かれてくる。そうした大きな検査の分類に合わせて、その検査に共通する事項をまとめた上位図書を整備すれば、検査現場で使用する各検査ガイド（下位図書）の使い勝手がさらに向上すると考えられる。

NRC の検査ガイドでは、上位図書として、その検査ガイドが使用される「検査プログラム」(IMC) を参照している。例えば、運転フェーズのセキュリティ検査プログラム (IMC 2201)、廃止措置段階のセキュリティ検査プログラム (IMC 2202)、中間貯蔵施設関連のセキュリティ検査プログラム (IMC 2690) などの検査プログラムを参照している。これらの

IMC には、それぞれの検査に共通する事項がまとめられている。

NRC の検査ガイド IMC（セキュリティ関連）については、以下に示すような IMC がある。

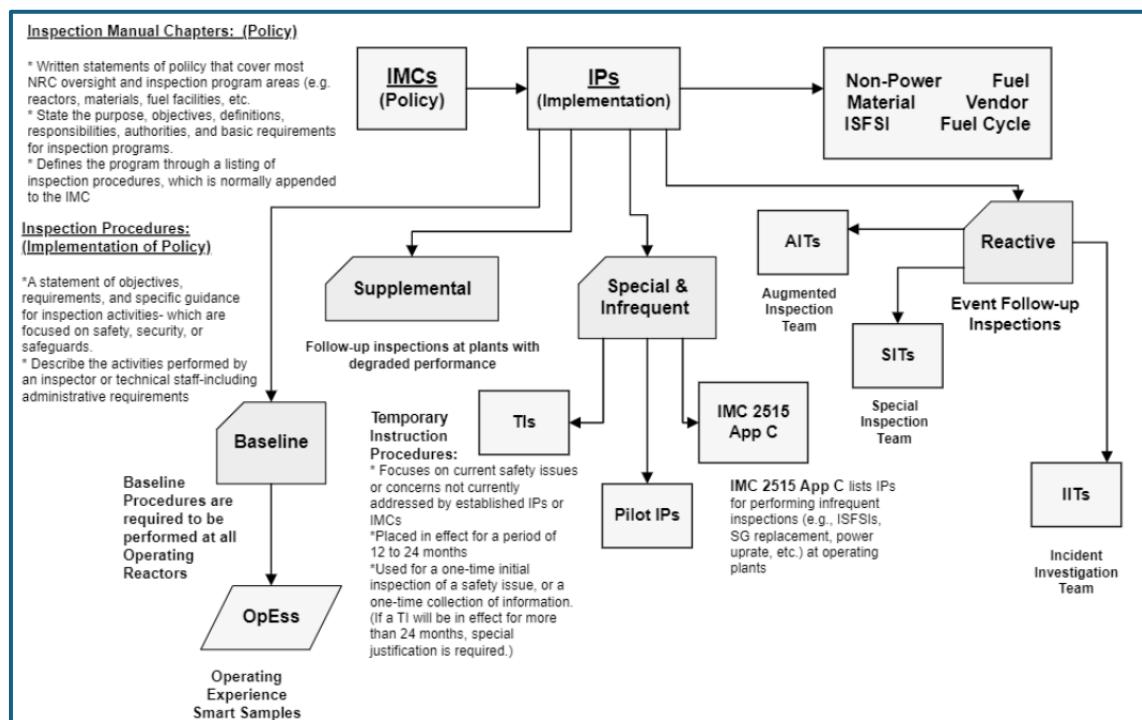
- IMC2201, Security Inspection Program for Operating Commercial Nuclear Power Reactors
- IMC2201C, Generic, Special, and Infrequent Inspections
- IMC2202, Security Inspection Program for Decommissioning Nuclear Power Reactors
- IMC2202A, Security Core Inspection Program
- IMC2202B, Supplemental Inspection Program
- IMC2690, Inspection Program for Storage of Spent Reactor Fuel and Reactor-related Greater-Than-Class C Waste at Independent Spent Fuel Storage Installations and for 10 CFR Part 71 Transportation Packaging など

このような上位図書を念頭に置いて、検査ガイドの図書体系を検討し、上位図書を含めて関連の検査ガイドを整備することを提案する。上位図書としては、上記の IMC が参考になる。

また、ONR にも、セキュリティの検査ガイドに共通する事項をまとめた次のような上位図書があり、これも一つの参考になる。

- ONR, CNS-INSP-GD-001, Nuclear Security Inspections

なお、NRC 検査ガイドの図書体系の全体的なイメージは、図 3.2.1 に示している。上位図書 IMC が方針（検査プログラム）を、下位図書 IP が実施手順を示すという位置づけである。また、各検査ガイドにおいては、基本検査、追加検査、特別検査などに大別されており、検査目的に合わせて整備した検査ガイドの図書体系を構築している。



出典：IMC 0040, “Preparation, Revision, Issuance, and Ongoing Oversight of NRC Inspection Manual Documents,” Effective Date: 01/17/2023

図 3.2.1 NRC 検査ガイドの図書体系

3.2.2 セキュリティ検査での確認事項の明確化

原子力規制庁の検査ガイドは、検査の対象範囲が抽象的に示されており、何を確認するのか、どの程度まで確認するかが具体的に示されていない。具体的な検査の対象や検査の程度が検査官の判断に任されると、検査官の負担が大きくなるとともに、検査がバラつき、検査の品質に影響する。

それゆえ、検査の対象や確認の深さ等を適宜例示することも含めて、検査で何を確認すべきかの内容を標準化して、具体的に明確に示すことを提案する。

NRC の検査ガイドでは、最初の「検査の目的」で、何をどのように確認するのかを、適宜その内容を具体的に示している。これが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しに一つの参考になると考えられる。

また、ONR の検査ガイドでは、「検査官の考慮事項」というものを記載している。この「検査官の考慮事項」では、検査官が確認する内容の標準を具体的に列挙している。これも今後、原子力規制庁が用いる検査ガイドの運用改善の見直しなどで参考になる。

3.2.3 施設の状態に応じたセキュリティ検査ガイドの拡充および実務的な検査要領の充足

原子力規制庁の検査ガイドは、施設の状態に応じた検査方法ではなく、状態を問わず、一律の検査方法を適用するものとなっているようなものが多い。しかし、例えば、検査対象施設やその施設の状態が検査ごとに異なり、事業者側でも、その組織、施設管理、運営方法も通常時、非常時（緊急時）の活動内容も一様ではないため、運転フェーズと廃止措置フェーズで、全く同じ検査方法を適用することはやや硬直的で、場合により検査ガイドの使い勝手が悪くなることが考えられる。

また、検査手順やガイダンスの記載内容が漠然としていると、検査官が検査現場で利用できる実用的なガイドにならないため、今後、原子力規制庁が用いる検査ガイドの運用改善の見直しに、できるかぎり具体性のある実用的な検査要領を盛り込むことが重要である。

それゆえ、例えば、発電炉、燃料施設など施設別のほか、運転炉、停止炉、廃棄炉など施設の状態別の検査ガイドを整備し、拡充するとともに、それぞれにふさわしい実務的で、ガイドの内容も実務向けにふさわしい検査要領を盛り込むことを提案する。

NRC の検査ガイドでは、3.2.2 で述べたように「検査の目的」で、検査での確認事項の標準を具体的に列挙しているが、さらに「検査要件」において、全般的なガイダンス、個別の検査項目のそれぞれについて、検査手順と具体的なガイダンスを記載している。これらの検査ガイドが、今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

3.2.4 セキュリティ検査根拠図書の整備

原子力規制庁の検査ガイド（セキュリティ関連）は、セキュリティの検査で指摘事項を摘出する場合にスクリーニングを行う、セキュリティ上の重要度を判断するなどのために、指針となる図書が少ない（未整備）。セキュリティの問題は、パフォーマンスが悪くなる前に、事業者の対応を要求すべきものも含まれるため、安全に関する指摘事項とは異なる視点で、重要度を判断し、規制対応を行うことが要求される。しかし、こうした図書が不足すると、検査の判断に資する情報が乏しいことから、評価がばらつく、時間を要するなどの不都合が生じやすいと言われている。

そのため、セキュリティの検査における指摘事項の重要度を判断するための図書、およびその技術的根拠を示す図書など、検査の判断に資する根拠図書等を整備することを提案する。

NRC の検査ガイドでは、セキュリティ検査に関する判断に関して、共通の理解を促進し、効率的な運用を図るために、次の図書を整備している。

- IMC 0308 Attachment 3 Appendix E, Technical Basis for the Baseline Security Significance Determination Process
- IMC 0609, Appendix E, Security Significance Determination Process for Power Reactors
- IMC 0612, Issue Screening
- IMC 0612, Appendix B, Issue Screening Directions
- IMC 0612, Appendix E, Examples of Minor Issues

上記のうち、安全およびセキュリティに関わる懸念事項がマイナーを超えるかどうかを判断するためのスクリーニングが IMC 0612 および IMC 0612 B（フローチャート）、問題がマイナーかどうかの判断事例が IMC 0612 E である。そして、「緑」以上の検査指摘事項の重要度決定プロセス（発電炉）が IMC 0609 E、その技術的根拠が IMC 0308 Att.3, App. E と対応している。検査官にとって、技術的根拠から、重要度決定の考え方、注意事項などが理解されやすい。これらの IMC が今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

3.2.5 セキュリティ指摘事項に関する評価基準の確立

原子力規制庁では、セキュリティ分野の事業者活動を評価するための共通指針が見当たらない（未整備）。検査ガイドとは別に、セキュリティ分野に関する共通の評価基準があれば、セキュリティ分野全体で重視される様々な側面がどのようなものかを知ることができる。また、各検査ガイドに、その検査では、どの評価基準を適用するかを示すことで、共通に認識された評価基準を念頭に、その評価に必要な側面にフォーカスした検査を行うことができる。逆に、こうした評価基準がない、またはあっても実用性に乏しい記載であれば、検査官の視点に関しても、指摘事項の摘出や評価に関しても、ばらつきが生じることになる。

そのため、検査官の視点が共通に認識された基準を念頭に、検査が行えるように、セキュリティ分野の事業者活動に関する標準的な評価基準を整備することを提案する。

ONR では、セキュリティ分野の事業者活動の評価基準として、セキュリティ評価原則（SyAPs）を策定し、その中に事業者が適合を実証しなければならない基本的セキュリティ原則（FSyPs）を含めている。このことが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

ONR のセキュリティ評価原則は、公開されており、次に示すところから入手できる（原則および解説で構成されており、全体で約 100 頁の記載内容がある。）

ONR のセキュリティ評価原則：

<https://www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/security-assessment-principles-syaps/security-assessment-principles-syaps/>

3.2.6 リスクの考え方の確立と運用指針の整備

原子力規制庁の検査ガイドには、例えば「・・・不法行為のリスクを低減する」という記載の中で、リスクという用語を用いて、事業者のリスク低減活動を監督している。ただし、リスクをどのように評価するか、管理するかについては、具体的な内容や情報が示されていない。また、規制者として、事業者活動に関するリスクがどの程度か、どのように対応するかについても、具体的に示されていない。

そのため、セキュリティの検査において、リスクを共通認識のもとに把握し、評価し、規制対応するために活用できるリスクの考え方を確立し、分かりやすい運用指針を整備することを提案する。

ONR の検査ガイドにおいて、同じく多くの箇所でリスクという用語を使用しており、事業者によるリスクの評価や管理などを監督している。違いは、ONR の検査ガイドの中で、事業者によるセキュリティ分野のリスク評価やリスク管理については、例えば、検査ガイド中 CNS-TAST-GD-7.1「効果的なサイバーおよび情報のリスク管理」で、参考文献の例を挙げて、検査官が参照すべき情報を具体的に提供している。また、規制者としての対応の考え方も別途、「行政措置方針」にその標準を定めている。このことが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。以下に、その概要内容を以下に示す。

まず、結論から示すと、検査官は、事業者活動に関するリスクのレベルを、次図に示される 4 段階（緑：通常、黄：中程度、橙：大きい、赤：極めて大きい）で判断する。縦軸は、実際のまたは可能性がある問題の影響（軽微、重要、深刻）、横軸は、事業者の管理方策の有効性（ほぼ問題なし、有効性が低下、存在しない／不十分）である。例えば、問題の影響が深刻な可能性があっても、管理方策に問題がなければ「緑」、影響が軽微でも管理方策がない／不十分であれば「橙」と判断する。

Consequence	Serious	Nominal	Substantial	Extreme
	Significant	Nominal	Moderate	Substantial
	Minor	Nominal	Nominal	Moderate
		Broadly ↓ satisfied	Weakened	Absent/↓ inadequate
		Control measures		

（リスクのレベル、出典：ONR-ENF-GD-006, Enforcement）

この他の主な関連部分を抜粋して以下に示す。

- ・行政措置は、健康、安全、セキュリティ、およびセーフガードに関するリスクと規制遵守のギャップ、および／または違反の深刻度に比例すべきである。
- ・このガイダンスは、ONR が原子力産業および非原子力産業の関連分野をどのように規制しているかを反映しており、ONR のすべての目的に適用される。
- ・機械的な意思決定ツールとして意図されているわけではない。むしろ、判断を支援し、**検査官が ONR の期待に沿って行政措置決定を下せるように支援することである。**
- ・規制当局の関与（検査、調査、異常報告、事象、苦情／懸念／内部告発のフォローアップなど）において、**検査官は、ハザード、リスク管理措置、セキュリティ上の脅威に関する情報を収集するまたは提供される。そこから、活動に関連する健康、安全、セキュリティ、セーフガードのリスクについて判断を下す。**検査官は、具体的なハザード／脅威を特定し、重大なリスクに直ちに対処できるよう、**共通する根本的／根源的な原因を検討する。**
- ・リスクを決定する際、検査官はまず、事業者の活動から生じる実際のリスクのレベルを評価すべきである。これは、訓練、経験、ガイダンス、その他の関連情報源から得たハザードと管理方策の判断に基づくべきである。

また、NRC の検査ガイドでは、3.2.4 に示したとおり、セキュリティの懸念事項がマイナーを超えるかどうかのスクリーニング、マイナーかどうかの判断事例、「緑」以上の指摘事項の重要度評価方法、その技術的根拠などを体系的に文書化している。その中で、リスクの考え方を扱っているが、安全性に関するリスクのように PRA 解析で評価するものではなく、決定論的に評価する方法が採用されている（IMC 0609 E、IMC 0308 Att.3, App. E）。このことが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

3.2.7 セキュリティ検査に役立つ背景知識・助言の提供

原子力規制庁の検査ガイドには、検査に役立つ背景知識や検査官への助言は、多く見当たらない。もちろん、検査官の資格認定教育の中で、一通りの知識を得ていると考えられるため、さらに、検査ガイドでどの程度までこうした情報を盛り込むべきかについては、現場の検査官の知識・経験レベルやニーズに依存するところがある。検査の現場で、事業者の活動を実際に検査しようとした場合、その検査で見るべき側面にフォーカスした事業者活動の解説などの背景知識が提供されている場合、検査の具体的な視点や手法を検討する上で大きく役に立つ。また、検査官への助言なども同様、検査活動の効率向上の助けになる。さらに、検査官の知識伝承は、常に重要なテーマの一つであるが、知識の伝承活動を支援することにも役に立つと考えられる。

そのため、検査官にとって、実用的な知識を充実させ、効果的で、効率的な検査の実施を支援するために、検査ガイドの中に検査に役立つ背景知識・助言を標準として盛り込むことを提案する。

ONR では、検査ガイドを検査官に「一般的な助言と情報」を与えるものと位置づけ、検査で考慮すべき事項を導出する前提として、前段で様々な背景知識や助言を盛り込んだ解説を行い、その後に、検査官が考慮すべき事項を示す構成としている。例えば、前出の「2.5.2.3 節の検査に役立つ背景知識・助言の提供」で示した記載例である。この中で、組織的学習を支える仕組みについて、図解を含めて詳細に解説し、重要なポイントなどの検査官への助言を示し、その後に検査官の考慮事項（検査の視点）として標準的なチェックポイントを列挙している。ONR の他の検査ガイドでも共通して、同様な構成になっている。このことが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

なお、NRC の検査ガイドでは、検査の手順と、それに関する具体的なガイダンスを詳細に示しているものの、ONR の検査ガイドのように解説までは行っていない。

3.2.8 セキュリティ検査に関わるグッドプラクティスの整備と活用

原子力規制庁の検査ガイド関連図書では、検査で活用できるグッドプラクティスが見当たらない。ONR の検査ガイドでは、検査で活用できるグッドプラクティスに関して記載されている。これが、ONR ならではのものかもしれない。そもそも、検査ガイドの作成や検査活動において、グッドプラクティスをそのまま利用するという発想はなかなか難があるかもしれない。2.5.2.4 節で示したように、ONR の検査ガイドには、「関連グッドプラクティス (RGP)」という用語を規制活動の随所で使用しており、様々な RGP を活用している。ONR が活用しているこれらのグッドプラクティスには、もともと事業者と協力して開発したもの、国の機関、国際機関、海外の機関 (NRC など) が開発したものなど、様々なものがある。事業者も RGP を活用しており、検査官との認識合わせにも役立っている。

例えば、現状に対する有効な改善策を検討する場合に、RGP が参考になり、ヒントを与えてくれる。すなわち、何をどう改善すべきかについて、共通に認識されたモデルを参照し、合意しやすい回答を見出すことができる。例えば、次のようなグッドプラクティスが引用されている。

CNS-TAST-GD 1.1 (Security Governance & LS) で引用している RGP :

- ✓ Independent Oversight Good Practice Guide. Produced by the cross-industry Internal Oversight Working Group (IOWG) and Published on behalf of the Safety Directors Forum (SDF). – December 2018:
https://www.nuclearinst.com/write/MediaUploads/SDF%20documents/IOWG/SDF_sub-group_Good_Practice_Guide_Issue_2.pdf
- ✓ UK Corporate Governance Code. Financial Reporting Council- July 2018.
<https://www.frc.org.uk/directors/corporate-governance-and-stewardship/uk-corporate-governance-code>
- ✓ The Wates Corporate Governance Principles for Large Private Companies - Financial Reporting Council- December 2018.
<https://www.frc.org.uk/directors/corporate-governance-and-stewardship/governance-of-large-private-companies>

CNS-TAST-GD 7.2 (Information Security)で引用している RGP :

- ✓ This TAG draws heavily on Relevant Good Practice (RGP) provided by National Cyber Security Centre (NCSC) as the National Technical Authority (NTA) for information assurance, NCSC, “Guidance: 10 Steps to Cyber Security,” [Online]. Available:
<https://www.ncsc.gov.uk/collection/10-steps>.
- ✓ ISO, “ISO/IEC 27001:2013 - Information technology — Security techniques — Information

security management systems — Requirements,” 2013.

- ✓ International Society of Automation/International Electrotechnical Commission (ISA/IEC), “ISA/IEC 62443 Series of Standards,” [Online]. Available: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.
- ✓ Information Security Forum (ISF) Standard of Good Practice for Information Security,
- ✓ NIST, “Cybersecurity Framework,” [Online]. Available: <https://www.nist.gov/cyberframework>.

CNS-TAST-GD 2.1 (Maintenance of Robust Security Culture)で引用している RGP :

- ✓ WINS International Best Practice Guide – Nuclear Security Culture,” [Online]. Available: <https://wins.org/document/1-4-nuclear-security-culture/>

このため、規制側と事業者が利用できるグッドプラクティスを含め、検査ガイドの作成や検査の実施に活用できるグッドプラクティスを整備し、活用することを提案する。ONRの活用しているグッドプラクティスが今後、原子力規制庁が用いる検査ガイドの運用改善の見直しで参考になる。

なお、検査ガイドの内容やグッドプラクティスの活用などは、ONR 独特の規制アプローチの中で行われている。NRC とは異なり、事業者を良い方向に導く意思を持ったアプローチである。英国の規制情報を活用する場合の参考情報として、ONR の規制アプローチについて、以下に補足として示す。

ONR は、「実現化規制 (enabling regulation)」という理念を持って、規制監督を実施している。これは、規制要件の遵守を見るだけでなく、規制に適合するように、または改善できるように、事業者に「影響を与える (influence)」アプローチを言い表している。

実現化規制を実施するために、ONR と産業界の双方で RGP などを活用して、安全で、確実な成果の効果的な実現を支援する、または阻害する可能性のある行動特性を認識している。次表は、ONR として、実現化規制の効果的と、効果的でない振る舞い、および仕事のやり方を例示したものである。ONR にとっては、事業者との協力や事業者への助言の提供が「効果的な振る舞いおよび仕事のやり方」(表 3.2.8-1)に通じている。

表 3.2.8-1 ONR の検査ガイドに示している「実現化規制の効果的と
非効果的な振る舞いおよび仕事のやり方」の概要内容

効果的な振る舞いおよび仕事のやり方	非効果的な振る舞いと仕事のやり方
戦略的、長期的、リスクベースの優先順位を設定し、それらが十分な根拠を持ち、より広い文脈の中で適切に理解されていることを確実にする。	全体の優先順位や長期的な成果をあまり考えず、短期的で反応的なアプローチを採用する。
利害関係者とオープンに関わり、優先事項について合意し、ガイダンスや助言を提供し、「ノーサプライズ」文化を確立する。	利害関係者と閉鎖的なアプローチを採用し、情報をほとんど、あるいはまったく共有しない。
安全やセキュリティの利益を最大化する解決策を確保するために規制を行う。	規制に対して過度に慎重なアプローチをとり、社会や労働者へのリスクよりもむしろ ONR への風評リスクを重視する。
提案されたアプローチの不備を早期に積極的に特定し、助言を提供する。	問題が発生するのを受け身で待つ。
事業者と協力して、規制上の問題と関連するアクションプランの工程表の時間枠に合意し、タイムリーな遵守を達成するために積極的に規制を行う。	事業者の視点、合理的な制約、安全やセキュリティの優先順位を理解しようとせず、問題と遵守の時間枠を押し付ける。
結果を重視する。	求められる結果を十分に考慮することなく、タスク/プロジェクトを重視する。
意思決定の一環として広い文脈でリスク要因を検討し、戦略的要因や ALARP、他の法的要件も確実に考慮されるようにする。	不備間の相互作用を考慮せず、またはより広い文脈でリスクをとらえることなく、ケースバイケースでリスクを評価する。
法的要求事項を満たし、実情に適したグッドプラクティスとなる、目的に適した解決策の策定を促す。	複雑な設計に対して非現実的または不釣り合いな設計基準を求めるまたは金メッキの解決策を推し進める。
長期的なリスクおよびハザードを低減するために短期的なリスクプロファイルの増加が必要な場合があることを認識し、容認する。	リスク低減に対して硬直的または短期的なアプローチをとり、全体像を考慮することなくリスクを低減しようとする。
十分なコントロールは行うが、不必要な注意散漫を避けるような方法で規制監督を行う。	結果に意味のある影響を与えない細部に過度の注意を払う。

出典：ONR, “A guide to enabling regulation,” August 2020

検査報告書にも、実現化規制の側面が反映されており、事業者の良好事例や改善のために与えた助言も適宜記載される。実際に、再処理施設 Sellafield（廃止措置移行中）に関する 2023 年 3 月の検査報告書（概要版）には、その例が見られる。以下に、良好事例および助言に関する例を 1 例ずつ示す。

- ・良好事例：オープンで誠実、そして有益な議論と、関係者の熱意と知識
- ・助言：セラフィールド社の指名委員会が認めたサイバー セキュリティ能力のギャップ

を、どのように最善に解決できるか。

この時点のサイトの安全性およびセキュリティの規制注目度が「著しく高い／高い」というリスクの高い状態にあった背景の中で、このような良好事例や助言が記載されたことを付記する。

①検査報告書および②当時のサイトの状態に関する詳細については、次に示すところから入手できる。

① <https://www.onr.org.uk/publications/regulatory-reports/site-specific-reports/inspection-records/2023/04/sellafield-site-inspection-id-ir-52091/>)

② <https://www.onr.org.uk/our-work/what-we-regulate/sellafield-decommissioning-fuel-and-waste/sites/sellafield/>

3.3 検査ガイドの改善内容の検討のまとめ

検査ガイドの改善内容の検討では、本年度実施した原子力規制庁が用いる検査ガイド（セキュリティ関連）および米国 NRC の検査ガイド（セキュリティ関連）の比較調査結果から得られた日米検査ガイド間の相違点等、原子力規制庁の検査ガイド（セキュリティ関連）および英国 ONR の検査ガイド（セキュリティ関連）の比較調査結果から得られた日英検査ガイド間の相違点等のほか、検査の現状、課題等を踏まえて、より効率的で、効果的な検査の実施を支える実用的な検査ガイドの在り方を念頭に、今後の原子力規制庁の検査制度の運用改善の見直しに資する改善点を検討した。原子力規制庁が用いる検査ガイドに対する改善内容として、検討した結果を整理した。以下に、今年度実施した検査ガイドの改善内容の主な検討結果を示す。

日米、日英検査ガイドの比較調査結果から、検査ガイドの改善内容として検討した結果を以下に示す。

- ・セキュリティ関連検査ガイド図書体系の検討と整備
- ・セキュリティ検査での確認事項の明確化
- ・施設の状態に応じたセキュリティ検査ガイドの拡充および実務的な検査要領の充足
- ・セキュリティ検査根拠図書の整備
- ・セキュリティ指摘事項に関する評価基準の確立
- ・リスクの考え方の確立 と運用指針の整備
- ・セキュリティ検査に役立つ背景知識・助言の提供
- ・セキュリティ検査に関わるグッドプラクティスの整備と活用

4 まとめ

本調査では、原子力規制庁が用いる検査ガイドおよびNRCの検査ガイド、ONRの検査ガイド（ともにセキュリティ関連）の比較調査を実施し、日米、日英検査ガイド間における主な相違を整理した。比較調査の結果を踏まえて、原子力規制検査の運用改善に資する情報を得ることを目的に、改善内容の検討を行った。これら比較調査、および改善内容の検討結果を整理し、調査報告書にまとめた。

具体的には、実施内容としては、検査ガイドの比較調査に関する実施内容および整理した結果等を2章「検査ガイドの比較調査」に、うち、日米の検査ガイドの比較調査に関する実施内容および整理した結果等を「2.3 日米検査ガイド比較調査の結果」に、日英の検査ガイドの比較調査に関する実施内容および整理した結果等を「2.4 日英検査ガイド比較調査の結果」にそれぞれまとめた。また、参考として、日米検査ガイドの全体体系および図書構成の概要について、まとめた資料を2.3.1節に、英国ONR検査ガイドの全体体系および図書構成の概要について、まとめた資料を2.4.1節にそれぞれ示した。検査ガイドの改善内容の検討に関する実施内容および整理した結果を3章「検査ガイドの改善内容の検討」にそれぞれまとめた。

検査ガイドの比較調査では、原子力規制庁の検査ガイド、NRCの検査ガイド、ONRの検査ガイドの公開版（最新版）を使用し、調査した。調査結果から、両者間の相違点等を抽出し、整理した。また、日米、日英の比較調査結果から、両者間における主な相違点等を整理したガイド別の比較調査結果まとめを作成し、参考資料として報告書にまとめた。このほかに、仕様対象外ではあるが、今後、原子力規制庁が検査ガイドの運用改善の見直しなどで参考になるONRの検査ガイド「CNS-INSP-GD-001（Issue 1）「Nuclear Security Inspections」」について調査した。調査の結果を整理して参考資料としてまとめた（詳細は2.4.2.11節参照）。

検査ガイドの改善内容の検討では、原子力規制庁が用いる検査ガイド、NRCの検査ガイド、およびONRの検査ガイドの比較調査から得られた結果を踏まえて、日米、日英の検査ガイド間における主な相違点等を整理し、今後の原子力規制検査の運用改善に資するような主な改善点を抽出し、今後、原子力規制庁が検査ガイドの運用改善の見直し等で参考になることを目的に、原子力規制庁が用いる検査ガイド向けの改善内容の検討を行い、改善内容の検討結果をまとめた。詳細は、3.2.1～3.2.8を参照する。

- ・セキュリティ関連検査ガイド図書体系の検討と整備
- ・セキュリティ検査での確認事項の明確化
- ・施設の状態に応じたセキュリティ検査ガイドの拡充および実務的な検査要領の充足
- ・セキュリティ検査根拠図書の整備
- ・セキュリティ指摘事項に関する評価基準の確立
- ・リスクの考え方の確立と運用指針の整備

- ・セキュリティ検査に役立つ背景知識・助言の提供
- ・セキュリティ検査に関わるグッドプラクティスの整備と活用

今後、原子力規制庁が用いる検査ガイドの改善活動の中で、重点的に改善するものについて、例えば、優先的に「セキュリティ関連検査ガイド図書体系の検討と整備」、「セキュリティ検査根拠図書の整備」、「施設の状態に応じたセキュリティ検査ガイドの拡充および実務的な検査要領の充足」などを見直しつつ、「セキュリティ検査に関わるグッドプラクティスの整備と活用」を見据えた改善活動を進めていくというのも一案である。その際には、NRC、ONR の検査ガイドや関連の情報のほか、NRC や ONR の検査ガイド見直しに関する動向も役に立つと考えられる。また、NRC、ONR が独自に実施してきた検査ガイド見直し活動中で行われてきた検討およびその内容、事業者との議論、協力によって実施した見直しの内容など、今後、原子力規制庁が用いる検査ガイドの継続改善活動に寄与するような情報について、必要に応じて継続調査を実施し、NRC、ONR の手法や取り組み等を参考にするのも有益である。