

平成 26 年度
放射性物質のセキュリティに関する調査
報告書

平成 27 年 4 月
公益財団法人原子力安全技術センター

本報告書は、原子力規制庁の放射線対策委託費事業として、公益財団法人原子力安全技術センターが実施した平成 26 年度「放射性物質のセキュリティに関する調査」の成果をとりまとめたものです。

目次

| | |
|---|----|
| 1. 調査の概要 | 1 |
| 2. 特定放射性同位元素に係る防護措置の調査 | 1 |
| 2.1 事業所における防護措置案の作成 | 1 |
| 2.2 国際基準の防護措置と国内の防護措置との対応の整理 | 2 |
| 2.3 セキュリティ目標とその考え方 | 7 |
| 2.4 脅威評価結果に基づく不法行為シナリオの検討 | 9 |
| 2.5 タイムライン評価と防護措置案の検討 | 10 |
| 2.5.1 タイムライン評価 | 11 |
| 2.5.2 防護措置案の検討 | 11 |
| 3. 標準的なセキュリティ計画案の作成 | 13 |
| 3.1 IAEA セキュリティシリーズに示されているセキュリティ計画の内容 | 13 |
| 3.2 カナダの放射線源に係るセキュリティ文書「Security Measures for Sealed Sources, Appendix A: Sample Site Security Plan」の内容 | 14 |
| 3.3 標準的なセキュリティ計画の作成 | 15 |
| 3.4 今後の検討課題 | 15 |
| 4. 非密封線源のセキュリティに係る調査 | 27 |
| 4.1 核セキュリティ文書の内容確認及び論点整理 | 27 |
| 4.1.1 核セキュリティのための規則と関連行政措置（ドラフト 実施指針） | 0 |
| 4.1.2 核セキュリティ文化の自己評価（ドラフト 技術手引き） | 1 |
| 4.1.3 核セキュリティのためのコンピューターセキュリティ（文書作成計画 実施指針） | 2 |
| 4.1.4 核セキュリティのための能力構築（実施指針） | 5 |
| 4.1.5 核セキュリティ体制の持続性（実施指針） | 6 |
| 4.1.6 使用及び貯蔵中の放射性物質及び関連施設のセキュリティ（文書作成計画 実施指針） | 7 |
| 4.2 放射性物質のセキュリティに関して記述のある文書について和訳作業 | 12 |
| 4.3 NSGC 会合へ専門家若しくは学識経験者等1名の派遣 | 12 |
| 4.3.1 第5回 NSGC | 12 |
| 4.3.2 第6回 NSGC | 13 |
| 4.3.3 非密封線源に関するテクニカルミーティング | 14 |
| 5. 委託調査検討委員会における論点整理 | 17 |
| 5.1 委託調査検討委員会の開催日程 | 17 |
| 5.2 各委託調査検討委員会の議論 | 17 |
| まとめ | 18 |
| 参考資料1：放射性物質のセキュリティに関する調査委員会名簿 | 19 |
| 参考資料2：NUREG-2166「放射性物質防護のための実践ガイド」の概要 | 20 |
| 参考資料3：RD/GD-338 Security Measures for Sealed Sources | 40 |

1.調査の概要

放射性同位元素のセキュリティについては、原子力規制委員会に設置された核セキュリティに関する検討会の第1回会合（平成25年3月）において、当面優先すべき課題の1つとされている。

国際原子力機関（以下、「IAEA」という。）の「放射性物質及び関連施設に関する核セキュリティ勧告」ⁱにおいては、「国は、放射性物質、関連施設及び関連活動に対するその国の脅威を評価するべきである。」、また「規制当局は、放射性物質に対するセキュリティ要件を決定し、定期的にそれらの妥当性を評価するための共通の根拠として、脅威評価の結果を用いるべきである。」と示されている。

これらを受け、平成25年度に特定放射性同位元素を扱う事業所において、どのような脅威（悪意ある脅威）を想定すべきかを調査し、明らかにするため、原子力規制庁委託事業として、密封線源を対象として「特定放射性同位元素に係る脅威評価に関する調査」を原子力安全技術センターにて実施した。

本年度は、放射性同位元素のセキュリティ対策を検討するために、想定される脅威に対抗し、盗取を防ぐための具体的な防護措置について調査・検討を実施するとともに、事業者にてセキュリティ計画を作成する際に参考となる標準的なセキュリティ計画案を取りまとめた。また、セキュリティ対策の有効性を確保するために、最新の知見を入手し、措置の見直し等適切な対応を行うことが必要となるため、特にIAEAで非密封線源のセキュリティに係る実施指針について検討が開始されたことを受け、放射性同位元素に係る核セキュリティシリーズ文書（以下、「RI文書」という。）に係る議論等を含め最新の知見を入手することを目的として、対象RI文書の調査及びIAEAテクニカルミーティング等への出席をとおして、最新の知見を取りまとめた。

なお、本調査では、放射性同位元素の使用及びそのセキュリティについての知見を有する専門家、学識経験者から構成される「放射性物質のセキュリティに関する調査事業委員会」ⁱⁱを設置し、専門的な助言を受け、報告書を取りまとめた。

2.特定放射性同位元素に係る防護措置の調査

2.1 事業所における防護措置案の作成

平成25年度特定放射性同位元素に係る脅威評価に関する調査結果において想定した脅威に対抗し、盗取に係るリスクを受容可能なレベルにまで低減するために、特定放射性同位元素を防護するための防護措置について調査・検討を実施した。

防護対象は、原子力委員会の報告書「我が国の核セキュリティ対策の強化について」に示されているとおり、放射線源登録制度の対象となる特定放射性同位元素（カテゴリー1及び2並びにカテゴリー3のうち、アフターローディング装置及び非破壊検査装置）とした。

事業所における防護措置案の作成に当たり、現在の特定放射性同位元素使用施設におけ

ⁱ IAEA 核セキュリティ・シリーズ No.14 勧告文書 放射性物質及び関連施設に関する核セキュリティ勧告

ⁱⁱ 参考資料：放射性物質のセキュリティに関する調査委員会名簿参照

る IAEA の示す国際基準への対応状況と不法行為に対する脆弱性を把握した上で検討するために、以下の 4 項目について整理、検討した。

- (1) 国際基準の防護措置と国内における防護措置との対応の整理
- (2) セキュリティ目標とその考え方
- (3) 脅威評価結果に基づく不法行為シナリオの検討
- (4) タイムライン評価と防護措置案の検討

2.2 国際基準の防護措置と国内の防護措置との対応の整理

国際基準の防護措置としては、IAEA NSS No.11 放射線源のセキュリティ及び IAEA NSS No.14 放射性物質及び関連施設に関する核セキュリティ勧告を参考として、本調査において防護対象としたカテゴリー1、カテゴリー2 及びカテゴリー3 に要求されている基準を抽出した。

国内の防護措置の状況としては、平成 25 年度に実施した「特定放射性同位元素に係る脅威評価に関する調査」において平成 22 年度に文部科学省が特定放射性同位元素所持事業所を対象に実施した「セキュリティ及び安全の確保」に係るアンケート調査結果及び放射性同位元素等による放射線障害の防止に関する法律（以下、「放射線障害防止法」という。）、医療法、獣医療法等において定められている安全規制のうち、セキュリティに資していると考えられる技術基準を参考として抽出した。

抽出情報を基に、国際基準の防護措置と国内の防護措置との対応を整理した。

表 2.2.1 に国際基準の防護措置と国内における防護措置との対応を示す。

表 2.2.1 国際基準の防護措置と国内における防護措置との対応の整理

| 機能 | 国際基準 (IAEA の示す基準) | | | 国内における防護措置状況 | | 備考 | | |
|--------------------|-------------------------------------|---------------------------------------|-----------|--------------|---|---|--|--|
| | セキュリティ目的 | セキュリティ措置 | セキュリティレベル | | | | 事業者の対応例 (※印は法令の定めがあるもの) | |
| | | | A | B | C | | | |
| 検知 | セキュアな区域/線源位置への無許可立入の即時の検知の提供。 | 電子侵入検知システム及び/又は事業者職員による連続的監視。 | ○ | ○ | | ①障害防止法施行規則第十四条の七：インターロックの設置 (100TB 以上) ※①インターロック ②侵入探知センサー ③監視カメラ ④巡回 | ①照射中においては即時検知に寄与するものの、それ以外は検知不可。 ②センサーのみでは即時検知は不可。また、アンケート結果から大多数の事業所でセンサーは実装されていない。(大学 0%、病院 2%、その他 11%) ③録画のみの場合もあり、即時検知に寄与していない可能性がある。また、大多数の事業所で監視カメラは実装されていない。(大学 20%、病院 33%、その他 29%) ④数時間毎に実施する定期巡回であるため、巡回時間以外は検知不可。 | |
| | 内部脅威者によるものを含めて、線源の不法移転の試みの即時の検知の提供。 | 電子的不正工作検知機器及び/又は事業者職員による連続的監視。 | ○ | | | ①障害防止法施行規則第十四条の七：インターロックの設置 (100TB 以上) ※①インターロック ②侵入探知センサー ③監視カメラ ④巡回 | ①照射中においては即時検知に寄与するものの、それ以外は検知不可。 ②センサーのみでは即時検知は不可。また、アンケート結果から大多数の事業所でセンサーは実装されていない。(大学 0%、病院 2%、その他 11%) ③録画のみの場合もあり、即時検知に寄与していない可能性がある。また、大多数の事業所で監視カメラは実装されていない。(大学 20%、病院 33%、その他 29%) ④数時間毎に実施する定期巡回であるため、巡回時間以外は検知不可。 | |
| | すべての線源の不法移転の試みの検知の提供 | 不正工作の検知機器及び/又は事業者職員による定期的な確認 | | ○ | ○ | 障害防止法第三十九条 (報告の徴収) 第 6 項：許可届出使用者又は表示付認証機器届出使用者 (法第二十八条第七項の規定により許可届出使用者又は表示付認証機器届出使用者とみなされる者を除く。) は、毎年三月三十一日に所持している特定放射性同位元素について、別記様式第五十八により、同日の翌日から起算して三月以内に原子力規制委員会に報告しなければならない。 | ①侵入探知センサー ②監視カメラ ※③線源の定期点検 ④巡回 | ①センサーのみでは即時検知は不可。また、アンケート結果から大多数の事業所でセンサーは実装されていない。(大学 0%、病院 2%、その他 11%) ②録画のみの場合もあり、即時検知に寄与していない可能性がある。また、大多数の事業所で監視カメラは実装されていない。(大学 20%、病院 33%、その他 29%) ③事業所により点検頻度は毎日～年 1 回 (法定) と大きく異なる。 ④数時間毎に実施する定期巡回であるため、巡回時間以外は検知不可。 |
| | 検知の即時の評価の提供。 | 事業者/対応職員による CCTV の遠隔モニタリング又は評価。 | ○ | ○ | ○ | | 監視カメラ | 録画のみの場合もあり、即時検知に寄与していない可能性がある。また、大多数の事業所で監視カメラは実装されていない。(大学 20%、病院 33%、その他 29%) |
| | 対応職員に即時の通信連絡の提供。 | 電話、携帯電話、無線呼出機、無線機のような通信連絡の迅速で信頼できる手段。 | ○ 多重手段 | ○ | | — | 電話 携帯電話 | — |
| 検認による紛失を検知する手段の提供。 | 物理的な確認、CCTV、不正工作指示装置などの日常的確認。 | ○ | | | | ※定期点検 | 半年に 1 度、定期点検を実施する事業所が大多数であり、紛失の検知に時間を要する可能性が高い。 | |
| | 物理的な確認、不正工作の検知機器などを調べること | | ○ 毎週 | ○ 毎月 | | ※定期点検 | " | |

| | | | | | | | |
|----|--|---|---|--|---|---|--|
| | 対応職員が不法移転を妨害するのに十分な検知後の遅延の提供。 | 対応職員が阻止することを可能とするのに十分な遅延を提供する障壁(例えば壁、かご)の少なくとも2つの層のシステム | ○ | | 障害防止法施行規則第十四条の七：管理区域の境界には、さくその他の人がみだりに立ち入らないようにするための施設を設けること。 障害防止法施行規則第十四条の九：貯蔵施設のとびら、ふた等外部に通ずる部分には、かぎその他の閉鎖のための設備又は器具を設けること。 | ※柵設置 遮へい壁 ※鍵 | 大多数の事業所で検知を伴っていないため、遅延に寄与しない。 |
| 遅延 | 不法移転の可能性を最小化するための遅延の提供 | 障壁(例えば壁、かご)の2層のシステム | ○ | | 障害防止法施行規則第十四条の七：管理区域の境界には、さくその他の人がみだりに立ち入らないようにするための施設を設けること。 障害防止法施行規則第十四条の九：貯蔵施設のとびら、ふた等外部に通ずる部分には、かぎその他の閉鎖のための設備又は器具を設けること。 | ※柵設置 遮へい壁 ※鍵 | 大多数の事業所で検知を伴っていないため、遅延に寄与しない。 |
| | 線源の不法移転の可能性を低減するための遅延の提供 | 1つの障壁(例えばかご、線源ハウジング)又は事業者職員による観察 | ○ | | 障害防止法施行規則第十四条の七：管理区域の境界には、さくその他の人がみだりに立ち入らないようにするための施設を設けること。 障害防止法施行規則第十四条の九：貯蔵施設のとびら、ふた等外部に通ずる部分には、かぎその他の閉鎖のための設備又は器具を設けること。 | ※柵設置 遮へい壁 ※鍵 | 大多数の事業所で検知を伴っていないため、遅延に寄与しない。 |
| 対応 | 不法移転を妨害し防止するために評価される警報に対する即時の対応への十分な資源の提供。 | 阻止するために即時に対応する人数、設備及び訓練を有する能力。 | ○ | | | ①監視カメラ ②侵入探知センサー ③セキュリティマニュアルの整備 | ①録画のみの場合もあり、即時検知に寄与していない可能性がある。また、大多数の事業所で監視カメラは実装されていない。(大学 20%、病院 33%、その他 29%) ②センサーのみの場合、即時評価は行えない。また、アンケート結果から大多数の事業所でセンサーは実装されていない。(大学 0%、病院 2%、その他 11%) |
| | 不法移転を妨害するための対応の即時の開始の提供 | 設備及び直ちに対応を開始する手続き | ○ | | | セキュリティマニュアルの整備 | 半数以上の事業所でセキュリティマニュアルを整備。ただし、セキュリティマニュアルの詳細は不明 |
| | 線源の不法移転の場合の適切な活動の実施 | 危機管理計画に従った必要な活動を識別するための手続き | ○ | | 放射線障害防止法施行規則第十五条の十四：密封された放射性同位元素を移動させて使用をする場合には、使用後直ちに、その放射性同位元素については、紛失、漏えい等異常の有無を放射線測定器により点検し、異常が判明したときは、探査その他放射線障害を防止するために必要な措置を講ずること。 放射線障害防止法施行規則第二十一条の十一：放射線管理の状況の報告 | ※放射線障害予防規程等における通報連絡網の整備(火災、盗難、所在不明、漏洩、異常被ばく等) セキュリティマニュアルの整備 | 半数以上の事業所でセキュリティマニュアルを整備。ただし、セキュリティマニュアルの詳細は不明 |

| | | | | | | | |
|----------|---|--|---|---|---|-------------------------------------|--|
| セキュリティ管理 | 認可された者のみに有効にアクセス制限する線源位置への出入管理の提供。 | 本人確認及び検認、例えばカード読み取り機及び暗証番号によって管理される施錠、鍵、鍵管理)。 | ○ | | <p>【通知】放射性同位元素等の管理の徹底について(再通知)(H20.4.9 文部科学省)</p> <p><u>・保管庫入り口における鍵の二重化や責任者のみ鍵の使用を行われるなど厳密な管理等の方策による措置が講じられているか</u></p> <p>・保管庫への立ち入りと放射性同位元素の持ち出しにあたり複数者によるチェック体制がとられているか</p> <p>・放射性同位元素の在庫確認の徹底による異常の早期検知のための措置が講じられているか</p> <p>・異常を発見した場合の迅速な通報連絡体制が構築されているか</p> | <p>※①特定者による鍵管理</p> <p>②電子錠による認証</p> | 本人確認が行われているかは不明。ただし、大多数の事業所では鍵等の管理者及び保管場所が定められているため、線源使用時に何らかの確認が行われているものと考えられる。 |
| | 1つの本人確認措置 | | ○ | ○ | — | ①鍵 ②電子錠 | 〃 |
| | 認可された個人の信頼性の保証。 | 線源位置への付き添いなしの立入り、及び機微情報へのアクセスのためのすべての認可された職員の身元調査。 | ○ | ○ | — | — | — |
| | 放射線源への付き添いなしの立入り及び機微情報へのアクセスを有する認可された個人の信頼性を決定する適切な方法 | | | ○ | — | — | — |

| | | | | | | | | | |
|----------|---|---------------------------------|---|---|---|---|---------------------------------|---|---|
| セキュリティ管理 | 機微情報の識別及び防護。 | 機微情報を識別し、かつ無許可の開示からそれを防護する手続き | ○ | ○ | ○ | 【通知】生活関連等施設の安全確保の留意点(H17.8 文部科学省) 放射性同位元素等の存在位置やアクセス手段等のセキュリティに関連する情報については、やむを得ない場合を除き対外的に非公開としたり、機微情報の漏洩を防止したりするために情報の取扱いルールを定めるなど、情報管理に留意すること。 | セキュリティマニュアルの整備 | 半数以上の事業所でセキュリティマニュアルを整備。ただし、セキュリティマニュアルの詳細は不明 | |
| | 防護計画の提供。 | 規制要件に適合し、増大する脅威レベルへの対応に備える防護計画。 | ○ | ○ | — | — | セキュリティマニュアルの整備 | 〃 | |
| | | セキュリティ準備及び参考人手続きの文書化 | | | ○ | — | — | セキュリティマニュアルの整備 | 〃 |
| | セキュリティ危機管理計画によってカバーされるセキュリティ事件を管理する能力の保証。 | セキュリティに関連するシナリオに対応するための手続き。 | ○ | ○ | ○ | — | — | — | |
| | セキュリティ事件の報告システムの確立。 | セキュリティ事件の適時の報告のための手続き。 | ○ | ○ | ○ | (報告の徴収) 放射線障害防止法施行規則第三十九条 放射線源登録管理制度 | セキュリティマニュアルの整備 ※放射線源登録管理システム | 半数以上の事業所でセキュリティマニュアルを整備。ただし、セキュリティマニュアルの詳細は不明 | |

2.3 セキュリティ目標とその考え方

最終的に防護措置案の検討とタイムライン評価を行うため、防護措置の内容を具体化するための指標となるセキュリティ目標を設定する必要がある。

IAEA NSS No.11「放射線源のセキュリティ」によると、セキュリティ目標は前節表 2.2.1 のとおり、A、B、C の 3 段階が達成目標として設定されており、それぞれ以下の内容となっている。

Security level A: Prevent unauthorized removal of a source.

Security level B: Minimize the likelihood of unauthorized removal of a source.

Security level C: Reduce the likelihood of unauthorized removal of a source.

セキュリティ目標の設定は、防護対象となる線源が盗取等不法行為によってどのような影響が生じるか整理した上で、決定する必要がある。

IAEA NSS No.11 放射線源のセキュリティでは D 値に基づき推奨されるセキュリティレベルが示されている。表 2.3.1 に IAEA が推奨するセキュリティレベルを示す。また、表 2.3.2 に本調査で対象とするカテゴリ 1～カテゴリ 3 の放射能による D 値とその影響を示す。

表 2.3.2 によると、カテゴリ 1 は、数分から 1 時間で致死線量に至り、カテゴリ 2 は、数時間から数日で致死線量に至り、カテゴリ 3 は、数日から数週間で致死線量に至る放射線源である。

いずれのカテゴリの放射線源も最終的に死に至る影響を及ぼすことから、本調査では IAEA が要求するカテゴリごとのセキュリティ目標を適用し、カテゴリ 1 は、不法移転の防止、カテゴリ 2 は、不法移転の可能性の最小化、カテゴリ 3 は、不法移転の可能性の低減をセキュリティ目標とした。

表 2.3.1 IAEA が推奨するセキュリティレベル

TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES

| Category | Source | A/D | Security level |
|----------|--|--------------------------------------|---|
| 1 | RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources | $A/D \geq 1000$ | A |
| 2 | Industrial gamma radiography sources High/medium dose rate brachytherapy sources | $1000 > A/D \geq 10$ | B |
| 3 | Fixed industrial gauges that incorporate high activity sources Well logging gauges | $10 > A/D \geq 1$ | C |
| 4 | Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators | $1 > A/D \geq 0.01$ | Apply measures as described in the Basic Safety Standards [5] |
| 5 | Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources | $0.01 > A/D$ and $A > \text{exempt}$ | |

表 2.3.2 放射能による D 値とその影響についてⁱⁱⁱ

| カテゴリ | 放射能(D値) | 線源の危険性 |
|------|-------------------------|---------------------------|
| 1 | $1000D \leq$ | 数分から1時間で致死線量をあびる (遮蔽なく接近) |
| 2 | $10D \leq \sim < 1000D$ | 数時間から数日で致死線量をあびる (遮蔽なく接近) |
| 3 | $D \leq \sim < 10D$ | 数日から数週で致死線量をあびる (遮蔽なく接近) |
| 4 | $0.01D \leq \sim < D$ | 一時的な症状が出る (接触、または数週間接近) |
| 5 | $< 0.01D$ | 永久的な障害が起こる可能性はない |

ⁱⁱⁱ 放射線源の登録管理制度について、文部科学省放射線規制室、2008年7月30日より引用

前節表 2.2.1 から現状で国際基準に対応していない点は大きく分けて以下の 4 点と考えられる。

- ①IAEA NSS No.11「放射線源のセキュリティ」でカテゴリ1 及びカテゴリ2 の放射性同位元素使用施設に求められている即時検知及び評価を行うための設備が大半の施設で無いこと。そのため、放射線障害防止法に定められている柵、貯蔵施設の施錠管理等の安全のための措置がセキュリティのための遅延に寄与していないこと。
- ②紛失や不法移転を検知するための定期点検頻度等がカテゴリごとに定められておらず、多くの施設で半年に 1 度程度の点検頻度であるため、不法移転を検知するまでに時間を要する可能性が高いこと。
- ③セキュリティ計画について、統一的な基準がなく、独自に定めており、治安当局、規制当局等との連携が円滑になされるか不明であること。
- ④個人の信頼性確認が行われておらず、潜在的な内部脅威を察知する術がないこと。
ただし、個人の信頼性確認制度については、盗取対象が RI であり、核兵器の製造等、著しい破壊につながる可能性がないこと、また、昨年度実施した RI 分野における過去の犯罪事例調査において、個人の信頼性確認を行えば犯罪を未然に防げた類の内部脅威者による犯罪はなく、精神疾患や同僚とのトラブル等の結果、衝動的動機による犯罪であったため、**graded approach** 及び現状で想定される脅威の観点から、本調査では、本人確認にとどめることとした。

よってこれら国際基準に対応するための防護措置案を検討することとした。

諸外国における対応状況は、防護対策として、以下の対策が共通してとられている。

抑止：アクセスコントロールの実施

検知：侵入検知システムの導入

遅延：複数の物理的バリアの設置

計画：セキュリティ計画の策定

対応については、各国で内容に差があり、アメリカ、カナダ、オーストラリアは職員による対応がなされ、ハンガリーは警備員、警察への通報対応がなされるようである。

なお、アメリカについては、米国原子力規制委員会（U.S.NRC）の規則 10CFR Part37 等にこれら防護策の実践ガイドが示されている。

参考資料 2 に詳細を示す。

2.4 脅威評価結果に基づく不法行為シナリオの検討

次に平成 25 年度に実施した脅威評価結果に基づき、代表的な放射性同位元素使用施設として、滅菌施設、非破壊検査装置取扱い施設、病院等のモデル施設における特色（線源を固定して使用、職員、業者、患者等多種多様な人物が出入り可能など）を踏まえ、不法行為シナリオを作成した。

なお、不法行為シナリオは以下を前提条件として検討した。

- ・ 就業時間内外で不法行為シナリオを検討する。
- ・ 本年度は、非密封線源の盗取は想定しない。
- ・ 不法行為シナリオは蓋然性の高い脅威(確実に防ぐ必要がある脅威)に基づき作成し、防護措置を検討した後、蓋然性の低い脅威リスクを低減できるか否かについて確認する。

本シナリオに基づき、タイムライン評価及び防護措置案の検討を行った。

2.5 タイムライン評価と防護措置案の検討

タイムライン評価と防護措置案の検討に当たり、平成 24 年 3 月の原子力委員会報告書「我が国のセキュリティ対策強化について」で示されている、「放射性物質利用による便益と核セキュリティに係るリスクを勘案すること」及び「現行の安全規制による措置がセキュリティ確保に資していること」を考慮し、まず、特段の防護措置を追加しない状態でのタイムライン評価を行い、セキュリティ目標の達成度を確認し、追加的防護措置の内容を検討した。

IAEA NSS No.11 放射線源のセキュリティでは Security Level に応じ、等級別に検知方法が定められており、Security LevelA(カテゴリー1 のセキュリティ目標)及び Security LevelB(カテゴリー 2 のセキュリティ目標)では、即時検知を求めており、Security LevelC(カテゴリー 3 のセキュリティ目標)では特に即時検知は求められていない。本調査においてもこれらセキュリティ目標に従い防護措置の検討を行った。

2.5.1 タイムライン評価

タイムライン評価は、2.4 節で検討した不法行為シナリオに基づき、モデル施設（照射滅菌施設、病院、非破壊検査会社）において、特段の防護措置を追加しない状態での評価を行い、2.5 節で検討した遅延時間の目標値との乖離を把握した後、追加的防護措置案を検討した。

2.5.2 防護措置案の検討

防護措置は、出入り管理が厳密かつ効率的にできる場所を事業所で設定し、管理することが考えられる。ここでは、核セキュリティ措置を必要とする区域を対策区域として設定する。例えば、対策区域は以下のように設定することができる

① 特定放射性同位元素が設置されている建物（図 2.5.6）

メリット：既存の一般出入管理システムが利用可能。

デメリット：窓、非常口等の出入口が複数存在する。

放射線業務従事者以外の者の立入りがある。

② 管理区域（例：特定放射性同位元素が設置されている管理区域）（図 2.5.7）

メリット：既存の管理区域に係る入退出管理システムが利用可能。

対策区域への立入りを放射線業務従事者に絞ることが可能。

デメリット：管理区域を広く設置している場合には考慮が必要。

③ 特定放射性同位元素が設置されている管理区域の一部（図 2.5.8）

メリット：対策区域への立入りを放射線業務従事者のうち必要な者に限ることが可能。

デメリット：管理区域とは別に対策区域への入退出管理が必要。



図 2.5.6 特定放射性同位元素が設置されている建物を対策区域とした例

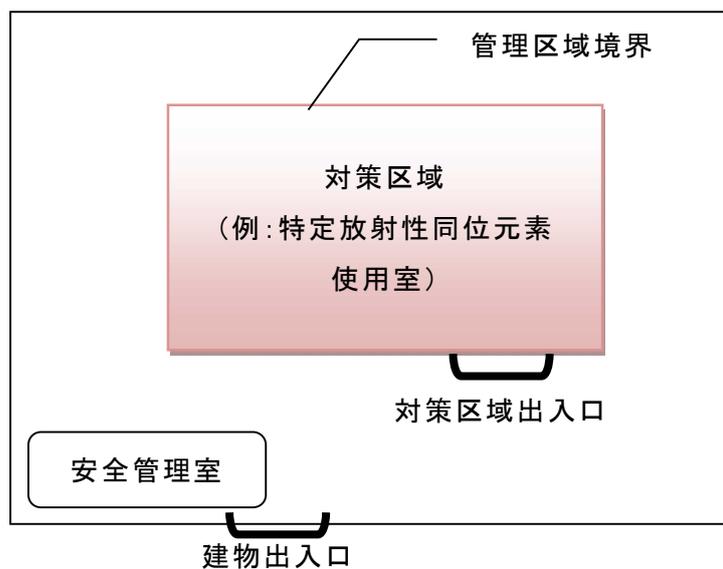


図 2.5.7 管理区域を対策区域とした例

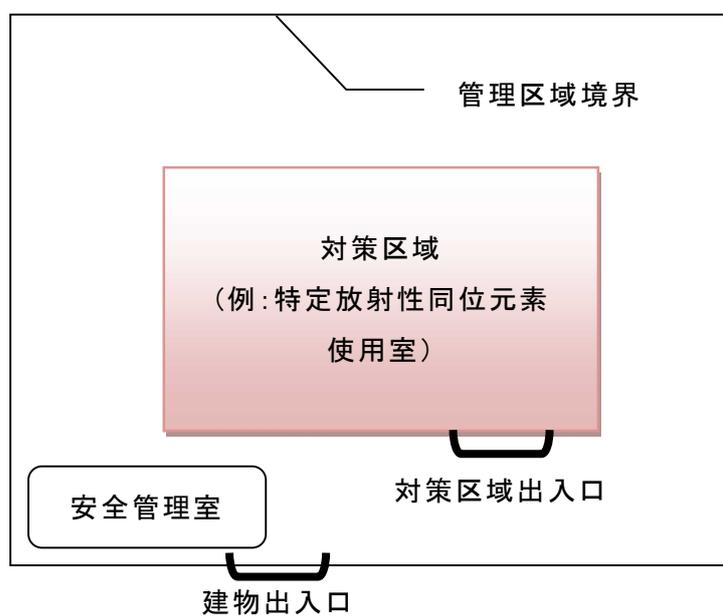


図 2.5.8 特定放射性同位元素が設置されている管理区域の一部を対策区域とした例

国際基準との対応調査及びタイムライン評価の結果を基に防護措置案を検討した。

3.標準的なセキュリティ計画案の作成

事業所における円滑なセキュリティ計画の作成に資するために、標準的なセキュリティ計画の作成を行った。

標準的なセキュリティ計画は、2章で検討した特定放射性同位元素に係る防護措置の検討結果を踏まえるとともに、IAEA NSS No.14「放射性物質及び関連施設に関する核セキュリティ勧告」4.20項、4.21項及びNSS No.11「放射線源のセキュリティ」付属文書Ⅱ防護計画の内容と放射線障害防止法で届出が定められている放射線障害予防規程及びカナダの放射線源に係るセキュリティ文書「Security Measures for Sealed Sources, Appendix A: Sample Site Security Plan」を比較し、必要と考えられる事項を抽出した。

3.1IAEA セキュリティシリーズに示されているセキュリティ計画の内容

IAEA NSS No.14「放射性物質及び関連施設に関する核セキュリティ勧告」4.20項、4.21項及びNSS No.11「放射線源のセキュリティ」付属文書Ⅱ防護計画の内容の事例に示されているセキュリティ計画に含むべき項目は以下のとおり。

(1) 放射性物質及び関連施設に関する核セキュリティ勧告 4.20 項、4.21 項

- ①放射性物質及びその使用及び貯蔵の環境についての記述
- ②取り組むべき特定のセキュリティ上の懸念の記述
- ③実施されるセキュリティシステム及びその目的の記述
- ④セキュリティ装置を操作し、維持する事業者職員への手引きを提供するためのセキュリティ手続き及び保守作業の前後で実施されるセキュリティ手続き
- ⑤セキュリティ責任を有する個人の役割及び責任、アクセス許可プロセス、個人の信頼性の決定プロセス、情報の防護プロセス、在庫量及び記録簿、事案の報告及び（レビューの間隔の最大時間を含む）セキュリティ計画のレビュー及び改定について規定することを含む管理上の側面
- ⑥手続き上及び管理上のセキュリティ措置が、国によって評価される脅威の増加するレベルに適合するかをどのように評価するか。
- ⑦国の慣行と整合した放射性物質の搜索及び回収における関連する所管当局との協力を含む対応活動

(2) 放射線源のセキュリティ付属文書Ⅱ防護計画の内容の事例

- ①線源、その区分及びその使用の記述
- ②線源が使用又は貯蔵される環境、建物及び/又は施設の記述、並びに必要な応じて、施設レイアウト及びセキュリティシステムのダイアグラム
- ③公衆がアクセス可能な区域に関する建物又は施設の位置
- ④特定の場所のセキュリティ手続き
- ⑤次のものを含む、特定の建物又は施設の防護計画の目的
- ⑥取り組む必要のある特定の懸念：不法移転、破壊又は悪意に満ちた使用
- ⑦必要となるかもしれない補助設備を含めて、好ましくない影響を防止するための管理の種類

⑧セキュアとされる設備又は建屋

次のものを含む、使用されるセキュリティ措置

- ・セキュアとする措置、監視の提供、出入管理の提供、検知、遅延、対応及び通信連絡
- ・想定脅威に対する措置の品質を評価するための設計上の特徴

⑨次のものを含む、使用される管理上の措置

- ・管理者、職員及びその他の者のセキュリティ役割及び責任
- ・線源の計数計量を含む、日常的及び非日常的な作業
- ・機器の維持管理及び試験
- ・職員の個人の信頼性の決定
- ・情報セキュリティの適用
- ・アクセス認可の方法
- ・事象報告を含む、緊急時計画のセキュリティ関連事項
- ・訓練
- ・鍵管理手続き

⑩脅威レベルの増大に取り組む手続き

⑪定期的な計画の有効性評価及び更新のプロセス

⑫使用する必要があるかもしれないすべての補完的措置

⑬現行規則又は基準の引用

3.2 カナダの放射線源に係るセキュリティ文書「Security Measures for Sealed Sources, Appendix A: Sample Site Security Plan」の内容

Security Measures for Sealed Sources (RD/GD-336) は、IAEA の核セキュリティに関連する文書を施行するためのカナダ国内の規則の運用を支援し、セキュリティ方策の適用における一貫性を提供するものである。RD/GD-336 は、許可所有者が許可を受けた施設において保管している密封線源の紛失、妨害破壊行為、不法な使用、不法な所持又は不法な移転を防止するために履行すべき最低限の物理的セキュリティ方策を規定するものである。この中には、セキュリティ計画に関連する内容が含まれている。Appendix A: Sample Site Security Plan にしめされているセキュリティ計画の例に含まれている項目とその内容は以下のとおり。

- ① 施設セキュリティ計画
- ② 周辺及び物理的バリアー
- ③ 保管のセキュリティ
- ④ アクセス規制
- ⑤ 輸送セキュリティ計画
- ⑥ 輸送機器のセキュリティ計画
- ⑦ 信頼性確認又はバックグラウンドチェック
- ⑧ 情報セキュリティ
- ⑨ 維持及びテスト

⑩ セキュリティ認知計画

参考としたカナダの放射線源に係る Security Measures for Sealed Sources については、参考資料 3 に示す。

3.3 標準的なセキュリティ計画の作成

表 3.3.1 IAEA が求めるセキュリティ計画の内容と日本（放射線障害予防規程）及びカナダにおけるセキュリティ計画の現状比較に示す。

標準的なセキュリティ計画案は、まず、① 区分Ⅰ施設（例：照射滅菌施設）のセキュリティ計画を作成した。セキュリティ計画の条項には線源の区分によらず共通の内容が多い。そのため、標準的なセキュリティ計画の対象施設として、具体的な防護措置に相違のある以下の施設を選択した。

- ① 区分Ⅰ施設（例：照射滅菌施設）
- ② 区分Ⅱ施設（例：血液照射装置）
- ③ 区分Ⅲ施設（例：アフターローディング装置）
- ④ 区分Ⅳ施設（例：非破壊検査装置）

3.4 今後の検討課題

標準的なセキュリティ計画を作成する上で、以下の課題が抽出された。

(1) セキュリティ対策や管理における放射線取扱主任者の役割の明確化

放射線取扱主任者の職務は、放射線障害の防止のための監督をすることである。医療機関では、医師が放射線取扱主任者に選任されている例も多い。表 3.4.1 に示すとおり、原子炉等規制法では、核燃料取扱主任者とは別に核物質防護管理者の選任について規定されている。

(2) 核セキュリティ計画の遵守対象者範囲

一般的に事業所の規模が大きくなると放射線業務従事者数も増える傾向にある。また、医療機関では、放射線業務従事者に看護師が含まれている。さらに、放射線業務従事者ではないが、核セキュリティに関する機微情報に触れる可能性のある職員（総務、経理関係）も存在する。核セキュリティ計画の遵守対象者の範囲を検討する必要がある。

(3) 今後セキュリティ計画に取り込む内容として検討を要する事項

平成 26 年 3 月 25 日、「放射性同位元素等車両運搬規則関係取扱要領及び核燃料物質等車両運搬規則関係取扱要領について（依命通達）」が一部改正された。概要は、核燃料輸送物の運搬に係る防護の措置について、IAEA セキュリティ勧告文書（INFCIRC/225/Rev. 5）の内容を踏まえ、次の事項を考慮した防護対象特定核燃料物質の防護のために必要な体制を継続して適切に維持するための計画を作成することである。

- ①セキュリティ文化の醸成（経営責任者の関与を含む）に関すること。
- ②品質保証に関すること。
- ③持続可能性プログラムに関すること。

これらの項目が、今後放射性同位元素の輸送に適用されることになるかは不明だが、放射

性同位元素のセキュリティについて、施設と輸送の整合の観点からも動向を注視する必要がある。

表 3.3.1 IAEA が求めるセキュリティ計画の内容と日本（放射線障害予防規程）及びカナダにおけるセキュリティ計画の現状比較

| IAEA(NSS_No.11 Security of Radioactive Source,NSS_No.14 Nuclear Security Recommendations on Radioactive Material and Associated Facilities) | 日本(放射線障害予防規程) | カナダ(RD/GD-338 Security Measures for Sealed Sources, Appendix A: Sample Site Security Plan) | セキュリティ計画に記載する事項 |
|---|---|---|---|
| <p>○線源の区分、その区分及びその使用の記述 (NSS_No.11)</p> <p>○線源が使用又は貯蔵される環境、建物及び/又は施設の記述、並びに必要なに応じて、施設レイアウト及びセキュリティ・システムダイアグラム (NSS_No.11)</p> <p>○公衆がアクセス可能な区域に関する建物又は施設の位置 (NSS_No.11)</p> <p>○放射性物質及びその使用及び貯蔵の環境について (NSS_No.14)</p> | <p>第 30 条 放射性同位元素は<u>所定の容器に入れ、所定の貯蔵室又は貯蔵箱に貯蔵すること。</u></p> <p>2 <u>貯蔵又は貯蔵箱はその貯蔵能力を超えて放射性同位元素を貯蔵しないこと。</u></p> <p>3 <u>貯蔵箱及び耐火性の構造の容器は放射性同位元素を保管中にこれをみだりに持ち運ぶことができないようにするための措置を講ずること。</u></p> <p>4 <u>非密封放射性同位元素を貯蔵室又は貯蔵箱に保管する場合は、容器の転倒、破損等を考慮し、吸収剤、受皿を使用する等、貯蔵室内又は貯蔵箱内に汚染が拡大しないような措置を講ずること。</u></p> <p>5 <u>密封放射性同位元素であって、機器に装備されているものは、装備した状態で保管し、シャッター機構のあるものは、保管中容器のシャッターを閉止すること。</u></p> | <p>Security organization</p> <p>セキュリティ組織</p> <p>* <u>密封線源およびその使用の記述を含んでいます。</u></p> <p>* <u>建物の記述での公衆がアクセス可能な区域及びセキュリティーゾーン(制限区域)を識別します。</u></p> <p>* ルーチンおよび非ルーチン・オペレーション中にセキュリティ・プロトコルについて記述します。</p> <p>* 上級管理人員、およびスタッフ、およびセキュリティ(サイト・セキュリティ計画の維持として担当者を指定することを含む)に責任を負う人々の役割および責任を識別します。</p> <p>* 契約者あるいは雇用されたスタッフにセキュリティ準備の詳細を供給します。</p> <p>* 特にこれらが施設のセキュリティに対する責任に関係があるか含んでいるところで、設備のために管理準備の詳細を提供します。</p> <p>Site plan</p> <p>配置図</p> <p>* <u>図面、写真あるいはサイトの他の正確な実例を提供します。</u></p> <p>* 適切なフェンス・ライン、境界および設備をすべて含んでいます。</p> <p>* すべてのセキュリティ・システムの位置を示します。</p> <p>* すべてのアクセスおよび退出ポイントの位置を示します。</p> | <p>○具体的な使用及び貯蔵環境を示す、図面等が必要。許可申請書類の図面、貯蔵核種、貯蔵料等の流用が可能。</p> <p>○セキュリティ・システムダイアグラム</p> <p>○公衆がアクセス可能な区域及び制限区域の識別</p> |
| <p>○次のものを含む、特定の建物又は施設の防護計画の目的</p> <ul style="list-style-type: none"> ・取り組む必要のある特定の懸念：不法移転、破壊または悪意に満ちた使用 ・必要となるかもしれない補助設備を含めて、好ましくない影響を防止するための管理の種類 ・セキュアとされる設備又は建屋 (NSS_No.11) <p>○取り組むべき特定のセキュリティ上の懸念 (NSS_No.14)</p> | <p>第 44 条報告</p> <ul style="list-style-type: none"> ・放射性同位元素の<u>盗取又は所在不明</u>が生じたとき ・記帳及び保存 | <p>Appendix A: Sample Site Security Plan</p> <ul style="list-style-type: none"> ・紛失、窃盗、破壊、悪意に満ちた行為 ・アクセスコントロール ・内部のセキュリティ ・保管時のセキュリティ ・輸送時のセキュリティ ・情報のセキュリティ ・信頼性と信頼度を決定する素性調査 ・危機管理とセキュリティのレスポンス計画 | |

| | | | |
|---|---|---|---|
| <p>○特定の場所の手続き (NSS_No.11)</p> <p>○セキュアとする措置、監視の提供、出入管理の提供、検知、遅延、対応及び通信連絡</p> <p>○セキュリティ措置を操作し維持する事業者職員へ手引きを提供するためのセキュリティ手続き及び保守作業の前後で実施されるセキュリティ手続き (NSS_No.14)</p> | <p>第 19 条 3 安全管理担当者は次の業務を行う。</p> <p>(1) <u>管理区域に立ち入る者の入退域、放射線被ばく及び汚染の管理</u></p> | <p>Access control</p> <p>* <u>放射線源か、物質(つまり放射性物質への監督されていないアクセス権限を持った認定ユーザおよび人のリスト)にアクセスすることを認められる、サイト上の従業員の数を提供します。</u></p> <p>* <u>アクセス・コントロール・システム(例えばカード読み取り機または押しボタン式ロック)、キーあるいはコード管理についての詳細および他の一般的なアクセス・コントロール手続きを含んでいます。</u></p> <p>* <u>設備(例えば、政策を護衛する)にアクセスするビジターと契約者のプロセスについて記述します。</u></p> <p>* <u>武器と爆発物のための詳細、車両をふるいわけおよび探索を含んでいます。</u></p> <p>Interior security</p> <p>* <u>放射エネルギーが捜し出されるエリアに特有の評価装置(例えばカメラ)、アクセス・コントロール、探知装置、遅れ手段、レスポンスおよびコミュニケーションをテストするために情報を提供します。</u></p> | <p>○アクセス許可リスト (業務従事者登録で代用可)</p> <p>○セキュリティ装置 (カード読み取り機または押しボタン式ロック)、キーあるいはコード管理等) への登録手続き</p> <p>○セキュリティ装置等のセキュリティダイアグラム</p> <p>○職員等常時立入者に対するセキュリティ手続き</p> <p>○メンテナンス業者等一時立入者に対するセキュリティ手続き (入退管理等)</p> <p>○不要物の持ち込み禁止</p> <p>○管理区域入域時における個人識別票の掲示</p> <p>○持ち込み手続き</p> <p>○セキュリティ装置・設備</p> |
| <p>○機器の維持管理及び試験 (NSS_No.11)</p> | <p>記載なし</p> | <p>3.2.7.1 Requirements for inspection, maintenance and testing of security-related equipment</p> <p>セキュリティに関する機器の検査、維持及びテストの要件</p> <p><u>許可使用者は、物理的セキュリティ機器のテスト、定期的テストの予定、製造者の仕様に従った維持管理のための文書化された手順を作成し維持しなければならない。最低限、侵入検知機器などのセキュリティ機器のテストは6月毎に実施しなければならない。許可所有者は警報試験が実施されている事を証明しなければならない。予防的維持管理手順には、時期を得て欠陥のある機器を交換する方策を含むべきである。</u></p> <p>3.2.7.2 Guidance for inspection, maintenance and testing of security-related equipment</p> <p>セキュリティに関する機器の検査、維持管理及びテストの指針</p> <p><u>すべての検知機器は、製造者の仕様書及び許可所有者の手順書に従って、設置され、動作し、維持管理されなければならない。許可所有者は、信頼性を確実にし文書化された記録を維持するために、定期的に検知機器の性能試験をしなければならない。</u></p> | <p>○セキュリティに係る機器の点検・保守頻度</p> <p>○性能確認方法</p> <p>○セキュリティ機器故障に係る措置</p> |
| <p>○管理者、職員及びその他の者のセキュリティ役割及び責任 (NSS_No.11)</p> | <p>記載なし</p> | <p>Security organization</p> <p>セキュリティ組織</p> | <p>セキュリティ組織及び責任を明確にする。また、セキュリティ</p> |

| | | | |
|---|--|---|---|
| <p>○セキュリティ責任を有する個人の役割及び責任 (NSS_No.14)</p> | | <p>* 密封線源およびその使用の記述を含んでいます。</p> <p>* 建物の記述での公衆がアクセス可能な区域及びセキュリティーゾーン(制限区域)を識別します。</p> <p>* ルーチンおよび非ルーチン・オペレーション中にセキュリティー・プロトコルについて記述します。</p> <p>* <u>上級管理人員、およびスタッフ、およびセキュリティー(サイト・セキュリティー計画の維持として担当者を指定することを含む)に責任を負う人々の役割および責任を識別します。</u></p> <p>* 契約者あるいは雇用されたスタッフにセキュリティー準備の詳細を供給します。</p> <p>* <u>特にこれらが施設のセキュリティーに対する責任に関係があるか含んでいるところで、設備のために管理準備の詳細を提供します。</u></p> | <p>組織における各人の業務内容について明確にする。</p> <p>放射線障害予防規程等で責任が明確にされているアクセス許可については、同規定の内容で責任を割り当てる。</p> <p>セキュリティー責任の割り当て(例)</p> <p>アクセス許可・・・事業所長 アクセス許可申請・所属部長 取扱主任者</p> <p>本人確認・・・事業所長 本人確認申請・・・所属部長 放射性同位元素の管理・取扱主任者</p> <p>セキュリティー装置・設備等の運用・管理・・・セキュリティー管理者等</p> |
| <p>○職員個人の信頼性の決定 ((NSS_No.11)</p> <p>○個人の信頼性の決定プロセス (NSS_No.14)</p> <p>○アクセス許可プロセス (NSS_No.14)</p> | <p>第 15 条 事業所において放射性同位元素又は放射線発生装置の取扱い等業務に従事する者は、<u>業務従事者または取扱等業務従事者として登録しなければならない。</u></p> <p>2 <u>所属部長の申請に基づき、主任者及び施設長の同意のもとに事業所長が指定し、承認したうえで業務従事者または取扱等業務従事者として登録する。</u></p> | <p>3.3.4.1 Requirements for personal trustworthiness and reliability</p> <p><u>許可所有者は、許可所有者の場所にある密封線源又は指定された機微情報にアクセスすることが必要な者、エスコートなしにアクセスできる保守会社の人を含めてすべての人の信頼性確認を実施しなければならない。業務として放射線源や機微情報にアクセスする人で、許可所有者により承認されていない者は、承認された者にエスコートされるべきである。</u></p> <p><u>個人の的確検査の性質と深さは放射性物質の区分を基礎とすべきである。</u></p> <p><u>区分 1, 2, 3 線源について、許可所有者は、最低限以下の情報を確認すべきである。</u></p> <p>a <u>パスポートや他の組織の文書 (運転免許証、健康保険証、出生証明書) と併せて個人特定をする。</u></p> <p>b <u>個人の犯罪者の氏名検査の結果を示す、地方の警察サービスセンター又は Canadian Police Information Center から寄せられた記録</u></p> <p>c <u>そこで 10 年以上雇用されていない者について、学歴を含めた職歴、及び専門資格</u></p> <p>d <u>直近 5 年間の履歴が確認できないときは、可能な場合は、直近 5 年間の 1 年以上の居住している地区の CRNC からの信頼性確認に関する情報を収集する。</u></p> | <p>○立入の必要性確認</p> <p>○公的証明書等による本人確認</p> <p>○一時立入者への付添い</p> <p>○出入管理</p> <p>○本人確認を行う範囲を明確にする。</p> <p>○区分 1、2、3 線源に付添い無しにアクセスする個人</p> <p>○区分 1、2、3 の施設への一時立入者 (メンテナンス業者等)</p> |

| | | | |
|---|-------------|--|--|
| | | <p>許可所有者は、現在の雇用者について少なくとも 2 年間は信頼性確認に関する文書を保持しなくてはならず、3.3.5 節に従って情報を防護しなくてはならない。</p> <p>3.3.4.2 Guidance for personal trustworthiness and reliability</p> <p>個人の的確性行為は、個人セキュリティ基準に基づかなければならない。</p> <p>許可所有者が行う信頼性確認計画は、高いリスクを有する密封線源へエスコートなしにアクセスする個人が信頼でき、個人の健康と安全及びセキュリティの不合理的なリスクを有していない事を確実にすべきである。許可所有者は、申請により提出されたすべての文書の写しを維持しなくてはならず、組織益に照合している事を確実にしなくてはならない。信頼性確認計画は定期的に見直されなければならない。信頼性確認計画は以下に適用される。</p> <ul style="list-style-type: none"> ・ <u>区分 1, 2, 3 線源にエスコートなしにアクセスする個人</u> ・ 区分 1 線源を輸送する車両機器ドライバー及び添乗者 ・ <u>指定されたもの及び機微情報に業務としてアクセスする、又は区分 1 線源の取扱をする個人</u> | |
| <p>○情報セキュリティの適用 (NSS_No.11)</p> <p>○情報の防護プロセス (NSS_No.14)</p> | <p>記載なし</p> | <p>3.3.5.2 Guidance for protection of prescribed and/or sensitive information</p> <p><u>以下の情報は指定されるべきであり、防護される情報と考えられる</u></p> <ul style="list-style-type: none"> ・ <u>施設セキュリティ計画、セキュリティに関する文書、セキュリティ対応計画、危機管理計画及び適用される場合は輸送セキュリティ計画</u> ・ <u>線源の在庫、特定の場所、設備の略図及び性能試験などのセキュリティシステム</u> ・ <u>脅威及びリスク評価 及び又は脆弱性評価</u> <p>指定された及び又は機微情報は以下を満たすべきである</p> <ul style="list-style-type: none"> ・ <u>不法な公開を防止し、不在時に安全である</u> ・ <u>定められている業務を実施するために必要な情報のみその人に公開する</u> ・ <u>移転や盗難を防止するように保管する</u> <p><u>高い機密情報はハードメディア (ディスク、CD-ROM 又は USB) に保管すべきであるか、紙の形でのみ保管する。また、知っておくべき人だけがアクセスできる安全な場所に保管する。この情報は公開されている、又は適切に防護されていないネットワーク上に保管してはならない。</u></p> <p><u>指定された又は機微情報について、許可所有者は以下を実施しなければならない。</u></p> <ul style="list-style-type: none"> ・ <u>移動でき、安全にすることができるように、携帯できる機器を使用する (コンピュータ、外付けハードディスク、USB キー)</u> ・ <u>パスワード又は暗号で防護された保管機器を使用する。及びサイバーセキュリティ手順により承認された使用者のみアクセスする。</u> ・ <u>指定された情報を含む情報又は文書の機密性、利用可能性及び性能を防護する</u> <p><u>指定された及び又は機微情報の移動又は送信については、</u></p> <ul style="list-style-type: none"> ・ <u>文書の各ページの右上の端にセキュリティ区分分けを含むべきである</u> ・ <u>文書又は関連する書類は郵便事業者により、又はファクシミリにより CNSC に提</u> | <p>情報の防護に係るプロセス検討</p> <ul style="list-style-type: none"> ○線源の保管場所、設備の略図、セキュリティ装置等のシステムダイアグラム等の防護 ○機微情報へのアクセス規制プロセス ○機密情報の保管、廃棄方法 ○モバイルメディアの取扱い方法 ○電子的送信に対する暗号化等 |

| | | | |
|--|---|---|--|
| | | <p>出する。</p> <p>・これら情報の電子的送信（e-mail など）は、適切な技術を用いて暗号化されない限り受け入れられない。</p> <p>もはや使われていない機微情報を含む指定された情報や文書は、破壊すると割り当てられたセキュリティ格付けに従って、細かく切り刻むか破壊されるべきである。</p> | |
| <p>○線源の計数を含む、日常的及び非日常的な作業（NSS_No.11）</p> <p>○在庫量及び記録簿（NSS_No.14）</p> | <p>第 19 条 3 安全管理担当者は次の業務を行う。</p> <p>(4) <u>放射性同位元素等の受入れ、払出し、使用、保管、運搬及び廃棄に関する管理</u></p> <p>(9) <u>記帳・記録の管理及びその保存</u></p> | <p>3.3.6 Inventory control</p> <p>在庫管理の要求事項</p> <p>許可所有者は、線源が安全であり変えられていない又は不正なアクセスが無い又は不法移転が無い事を確認するために、検知目的で定期的在庫確認を実施しなければならない。この在庫確認は核物質及び放射線機器規則第 36 条第 1 項(a)に従わなければならない。</p> <p>操業者は彼らの責務の基で密封線源のリストを作成し維持しなければならない。在庫確認は検知方策の一部として使用することができる。定期の在庫確認は、線源が存在し改ざんされた事が無い事を確実にするための方策から成る。これらの方策は、線源が存在しているという物理的チェック、又は CCTV を用いた遠隔監視、又は封印の確認、又は他の改ざん検知装置が含まれる。在庫管理の手順は実施され、強固な確認手順であるべきである。</p> | <p>放射線障害予防規程に定められる記録を利用</p> |
| <p>○鍵管理手続き（NSS_No.11）</p> | <p>記載なし</p> | <p>3.2.4.1 Requirements for locking hardware and key control</p> <p>施錠機器と施錠管理の要件</p> <p>保管区域へのアクセス管理するアクセスカード、ドアの鍵は許可所有者により承認された者に制限されるべきである。</p> <p>許可所有者は、施錠機器（電子的又は手動か）などのアクセス管理承認の記録を維持すべきである。これらの記録には、施錠機器又は組み合わせ数字が発行された個人の名前、及び発行日が含まれるべきである</p> <p>許可所有者は、効力が無くなったり、紛失、盗難又は不法に移動されたり、又は情報漏洩した、施錠機器、鍵、アクセスカード又は組み合わせ数字の交換、補修の方策を含む書面にした手順を作成し、維持しなければならない。</p> <p>3.2.4.2 Guidance for locking hardware and key control</p> <p>施錠機器及び施錠管理の指針</p> <p>鍵が使用されるときは、許可所有者は以下に示す施錠管理方針を実施しなければならない；</p> <ul style="list-style-type: none"> ・<u>鍵を有する個人の数を制限し</u> ・<u>マスターキーの数を制限し</u> ・<u>従業員の鍵複製を禁止し</u> ・<u>不正な鍵複製を防止するために専用の鍵又は特許を得ている鍵を用いる</u> ・<u>もはやアクセスすることがなくなった従業員に鍵の返還を求める規定を含める</u> ・<u>ブランクな鍵（合い鍵を作る前のブランクキー）は安全に保管されるべき</u> | <p>○鍵へのアクセス権</p> <p>○鍵の取り換え、構造の変更等</p> <p>鍵の複製を禁ずる措置</p> |

| | | | |
|---|--|---|---|
| | | <p>施錠管理のために、許可所有者は</p> <ul style="list-style-type: none"> ・定期的に鍵又は鍵所持者の在庫量を見直しし ・記録に鍵又は鍵所持者の変更及び追加を記録し ・発行された鍵及び紛失又は盗難にあったと記録されている鍵の報告義務を維持する <p>組み合わせ式の鍵又は数字組み合わせの鍵は推奨されない。</p> <p>従来型の鍵が使用されている場合は、それらは良質のものであるべきである。施錠管理手順は不正アクセスやセキュリティ侵害を防止するために設計されるべきである。施錠の切断を防止するために鍵は覆われているべきである。</p> | |
| <p>○事象報告を含む、緊急時計画のセキュリティ関連事項 (NSS_No.11)</p> <p>○事案の報告、及び(レビューの間隔の最大時間を含む)セキュリティ計画のレビュー及び改定について規定することを管理上の側面 ((NSS_No.14)</p> | <p>第 43 条 放射性同位元素等に関し、地震、火災、運搬に係る事故等の災害が起こったことにより、放射線障害が発生した場合又はそのおそれがある場合その発見者は、別に定める放射線防護措置要領に従い直ちに災害の拡大防止、通報及び避難警告等応急の措置を講じなければならない。</p> <p>2 事業所長は前項の事態が生じた場合は、直ちに関係機関に通報するとともに遅滞なく原子力規制委員会に、運搬に係る事故の場合には原子力規制委員会又は国土交通大臣に届け出なければならない。</p> <p>第 44 条 次の各号に掲げる事態の発生を発見した者は、別に定める放射線防護措置要領に従い通報しなければならない。</p> <p>(1) 放射性同位元素の盗取又は所在不明が生じたとき。</p> | <p>3.2.6.1 Requirements for alarm response protocol</p> <p>許可所有者は放射性物質又は放射線機器への盗難、転用又は妨害破壊行為の意図又は実施に対して直ちに対応すべきである。</p> <p>許可所有者は、警報の起こった時及び解除の記録についての文書化された警報対応手順を作成し維持しなければならない。この手順には許可所有者の対応部隊及び施設外の対応部隊の責務と役割が含まれるべきであり、危機管理計画又は同等な文書に文書化されるべきである。</p> <p>許可所有者は、管轄の地方警察に届け出て、密封線源が施設にあるということを情報提供すべきであり、これには施設の見学も含まれる。許可所有者は施設外の緊急時対応部隊への文書化された準備を作成し維持すべきであり、施設のデザインが変更され又は線源の潜在的脆弱性に影響しそうな施設の設計や作業が変更された時又は年次で見直しをすべきである。文書化された準備は一時的作業場所には適用されない。</p> | <p>○放射線防護措置要領に定められる事案の報告プロセスを利用</p> <p>○セキュリティ計画のレビュー及び改定に係る期間等を定める規定</p> |
| <p>○想定脅威に対する措置の品質を評価するための設計上の特徴 ((NSS_No.11)</p> <p>○脅威レベルの増大に取り組む手続き (NSS_No.11)</p> <p>○定期的な計画の有効性評価及び更新のプロセス (NSS_No.11)</p> <p>○使用する必要があるかもしれない補完的措置 (NSS_No.11)</p> <p>○手続き上及び管理上のセキュリティ措置が国によって評価される脅威の増加するレベルに適合するかをどのようにして評価するか (NSS_No.14)</p> | <p>記載なし</p> | <p>3.1.2 Guidance for general security measures</p> <p>許可所有者は、密封線源が保管中又は輸送中に紛失、不法使用、不法所持、又は不法移転から防護するために設計された現存の物理的防護システムにおける脆弱性を決定するために、脅威及びリスク評価を開発し維持しなければならない。年に1回最新のものとする、脅威及びリスク評価は、特定の脅威に対処し、リスクを管理し、脆弱性を減少するための緩和セキュリティ方策を決定するために使用される。</p> | <p>○事業者に対して DBT を提供しないため、想定脅威に対する脆弱性、リスク等の評価は行えないものの、セキュリティ計画の実施を通じた気づき等を踏まえ、セキュリティ計画の定期的改善を行う。</p> |
| <p>○国の慣行と整合した放射性物質の捜索及び回収における関連する所管当局との協力を含む対応活動 (NSS_No.14)</p> | <p>第 43 条 放射性同位元素等に関し、地震、火災、運搬に係る事故等の災害が起こったことにより、放射線障害が発生した場合又はそのおそれがある場合その発見者は、別に定める放射線防護措置要領に従い直ちに災害の拡大防止、通報及び避難警告等応急の措置を講じなければならない。</p> | <p>3.2.6.2 Guidance for alarm response protocol</p> <ul style="list-style-type: none"> ・密封線源の盗難、紛失、妨害破壊が起こった時の対応手順 ・許可所有者の職員の役割及び対応 ・地方の法執行機関及び当てはまる官署への連絡準備 ・事象の報告、届け出 | <p>放射線障害防護措置要領における活動を利用</p> |

| | | | |
|--|---|---|--|
| | <p>2 事業所長は前項の事態が生じた場合は、<u>直ちに関係機関に通報するとともに遅滞なく原子力規制委員会に、運搬に係る事故の場合にあつては原子力規制委員会又は国土交通大臣に届け出なければならない。</u></p> <p>第 44 条 <u>次の各号に掲げる事態の発生を発見した者は、別に定める放射線防護措置要領に従い通報しなければならない。</u></p> <p><u>(1) 放射性同位元素の盗取又は所在不明が生じたとき。</u></p> | <p>・規制が回復された線源の即時の報告</p> <p><u>地方の法執行機関、又は他の施設との相互協力協定の準備を推奨するために、許可所有者は覚え書きのような書面の支援協定を考慮すべきである。この準備された書面は、施設内の守衛と施設内にいる法執行機関の職員との間の関係を詳述すべきである。</u></p> | |
| <p>○訓練 (NSS_No.11)</p> <p>○事業者は、セキュリティ責任を有するすべての職員が、彼らの責任を遂行する前及びその後定期的に、適切に訓練され資格があることを確実にすることを要求されるべきである。(NSS_No.14)</p> | <p>第 38 条 安全管理責任者は管理区域に立ち入る者及び取扱等業務従事者に対し、本規定の周知等を図るほか、放射線障害を防止するために必要な教育及び訓練を実施しなければならない。</p> <p>2 前項の規定による教育及び訓練は次の各号の定めるところによる。</p> <p>(1) 実施時期は次のとおりとする。</p> <p>ア 業務従事者として登録する前または取扱等業務従事者として登録する前</p> <p>イ 初めて管理区域に立ち入る前及び取扱等業務に従事する前</p> <p>ウ 管理区域に立ち入った後及び取扱等業務の開始後にあつては 1 年を超えない期間ごと</p> <p>(2) 前号ア並びにイについては、次に掲げる項目及び時間数を又ウについては次に掲げる項目について実施すること。ただし、()内は取扱等業務従事者の場合とする。</p> <p>ア 放射線の人体に与える影響 30 分以上 (30 分以上)</p> <p>イ 放射性同位元素等の安全取扱 4 時間以上 (1 時間 30 分以上)</p> <p>ウ 放射線障害の防止に関する法令 1 時間以上 (30 分以上)</p> <p>エ 放射線障害予防規程 1 時間以上 (30 分以上)</p> <p>オ その他放射線障害に関して必要な事項</p> <p>3 前項の規定にかかわらず前項第 2 号に掲げる実施項目に関して十分な知識及び技能を有していると認められる者に対しては、教育及び訓練の一部を省略することができる。</p> <p>4 安全管理責任者は管理区域に一時的に立ち入る者を一時立入者として承認する場合は、当該立入者に対して放射線障害を防止するために必要な教育を実施しなければならない。</p> | <p>3.3.3.1 Requirements for a security awareness program</p> <p><u>許可所有者の場所で密封線源や指定された情報にアクセスすることを承認されたすべての者 (修繕会社、契約者、建築物維持管理職員) は、施設の行為、セキュリティ方針、手順を教育させるべきである。教育及び訓練の記録はすべての作業員に対して維持されるべきである。セキュリティ教育計画は文書化されており許可所有者により毎年更新されるべきである。新規採用者に対する訓練及び再教育を実施する。</u></p> <p>3.3.3.2 Guidance for a security awareness program</p> <p><u>セキュリティ教育訓練は密封線源と指定された情報を防護するため、及び疑わしい事象やセキュリティ事象を報告することに関するセキュリティ行為、手順の指示を含むべきである。</u></p> <p><u>最低限、セキュリティ教育計画は以下を確実にすべきである。</u></p> <ul style="list-style-type: none"> ・職員はセキュリティに関する彼らの役割と責務の理解 ・疑わしい活動を認識し報告するための職員の訓練、例えば <ul style="list-style-type: none"> ・偽の身分証明書 ・疑わしい振る舞いを示す人 ・承認を得ないで警報を発する人 ・組織内で制服や資材が紛失又は盗難される ・作業場で安全では無い振る舞い ・指定された又は機微情報の防護 ・疑わしい活動を特定する活動又は個人又は契約者の行動の変更に関する方策の訓練 <p><u>セキュリティ教育計画について、許可所有者は、彼らの業務を遂行するために求められる長期の品質維持及び安全とセキュリティの役割を認識するという目標への訓練を基礎とした全体的な訓練方針、新規及び再教育計画を作成し維持しなければならない。</u></p> | <p>○教育訓練</p> <p>今後要件等</p> |
| <p>○現行規則又は基準の引用 (NSS_No.11)</p> | <p>記載なし。</p> | | <p>○現行規則又は基準の引用については、放射線障害予防規程等の引用を図る。</p> |

表 3.4.1 原子炉等規制法と放射線障害防止法における「主任者」の規定（抜粋）

| 原子炉等規制法 | | 放射線障害防止法 |
|--|---|--|
| (核燃料取扱主任者) | (核物質防護管理者) | (放射線取扱主任者) |
| <p>第二十二條の二 加工事業者は、核燃料物質の取扱いに関して保安の監督を行わせるため、原子力規制委員会規則で定めるところにより、次条第一項の核燃料取扱主任者免状を有する者であつて、原子力規制委員会規則で定める実務の経験を有するものの中から、核燃料取扱主任者を選任しなければならない。</p> <p>2 加工事業者は、前項の規定により核燃料取扱主任者を選任したときは、選任した日から三十日以内に、その旨を原子力規制委員会に届け出なければならない。これを解任したときも、同様とする。</p> | <p>第二十二條の七 加工事業者は、第二十一條の二第二項に規定する場合には、特定核燃料物質の防護に関する業務を統一的に管理させるため、原子力規制委員会規則で定めるところにより、特定核燃料物質の取扱い等の知識等について原子力規制委員会規則で定める要件を備える者の中から、核物質防護管理者を選任しなければならない。</p> | <p>第三十四條 許可届出使用者、届出販売業者、届出賃貸業者及び許可廃棄業者は、放射線障害の防止について監督を行わせるため、次の各号に掲げる区分に従い、当該各号に定める者のうちから、放射線取扱主任者を選任しなければならない。この場合において、放射性同位元素又は放射線発生装置を診療のために用いるときは医師又は歯科医師を、放射性同位元素又は放射線発生装置を医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和三十五年法律第百四十五号）第二條に規定する医薬品、医薬部外品、化粧品、医療機器又は再生医療等製品の製造所において使用をするときは薬剤師を、それぞれ放射線取扱主任者として選任することができる。</p> <p>一 特定許可使用者、密封されていない放射性同位元素の使用をする許可使用者又は許可廃棄業者 次条第一項の第一種放射線取扱主任者免状（次号及び第三号において「第一種放射線取扱主任者免状」という。）を有する者</p> <p>二 前号に規定する許可使用者以外の許可使用者 第一種放射線取扱主任者免状又は次条第</p> |

| | | |
|---|---|--|
| | | <p>一項の第二種放射線取扱主任者免状（次号において「第二種放射線取扱主任者免状」という。）を有する者</p> <p>三 届出使用者、届出販売業者又は届出賃貸業者 第一種放射線取扱主任者免状、第二種放射線取扱主任者免状又は次条第一項の第三種放射線取扱主任者免状を有する者</p> <p>2 許可届出使用者、届出販売業者、届出賃貸業者及び許可廃棄業者は、放射線取扱主任者を選任したときは、原子力規制委員会規則で定めるところにより、選任した日から三十日以内に、その旨を原子力規制委員会に届け出なければならない。これを解任したときも、同様とする。</p> |
| <p>(核燃料取扱主任者の義務等)</p> <p>第二十二條の四 核燃料取扱主任者は、加工の事業における核燃料物質の取扱いに関し、誠実にその職務を遂行しなければならない。</p> <p>2 加工の事業において核燃料物質の取扱いに従事する者は、核燃料取扱主任者がその取扱いに関して保安のためにする指示に従わなければならない。</p> | <p>(核物質防護管理者の義務等)</p> <p>第十二條の四 核物質防護管理者は、誠実にその職務を遂行しなければならない。</p> <p>2 製錬施設に立ち入る者は、核物質防護管理者がこの法律若しくはこの法律に基づく命令又は核物質防護規定の実施を確保するためにする指示に従わなければならない。</p> | <p>(放射線取扱主任者の義務等)</p> <p>第三十六條 放射線取扱主任者は、誠実にその職務を遂行しなければならない。</p> <p>2 使用施設、廃棄物詰替施設、貯蔵施設、廃棄物貯蔵施設又は廃棄施設に立ち入る者は、放射線取扱主任者がこの法律若しくはこの法律に基づく命令又は放射線障害予防規程の実施を確保するためにする指示に従わなければならない。</p> |

| | | |
|--|--|--|
| | | <p>3 前項に定めるもののほか、許可届出使用者、届出販売業者、届出賃貸業者及び許可廃棄業者は、放射線障害の防止に関し、放射線取扱主任者の意見を尊重しなければならない。</p> |
|--|--|--|

4. 非密封線源のセキュリティに係る調査

現在、IAEAにおいて策定中である核セキュリティ関連文書については、核セキュリティ文書の審議委員会となるNSGCにおいて、承認手続きが行われる。こととなっており、NSGCの開催に際しては、日本を含むNSGCのメンバー国が作成プロセス中の文書に対しては事前にコメントを提出することとしてが求められることになっている。

セキュリティ対策の有効性を確保するためには、常に最新の知見を入手し、措置の見直し等、適切な対応を行うことが必要になる。特に、RI文書の見直しの一環として、非密封線源のセキュリティに係る実施指針についての検討が開始されたところであり、今後、新たな知見として改訂版の実施指針が刊行される予定である。

こうした状況を踏まえ、放射性物質のセキュリティに関する国内外の動向等に関する情報を収集、整理し、核セキュリティ文書に記載された内容について、意見を述べることにより、国際的に責任を果たしていくことが重要との原子力規制庁の認識のもと、センターでは、RI文書への対応方針の作成に資することを目的としてIAEA核セキュリティシリーズ文書の調査を実施した。

センターでは、本調査においてIAEAが策定した核セキュリティ関連文書のうち、RI文書について、その策定状況を把握し、我が国としてのコメント提出等の対応方針の作成に資するため事前に論点となり得る事項を抽出した上で、センター内に委託調査運営委員会を設置し、専門家からの意見を聴取した上で、論点整理を行い、原子力規制庁に提出した。論点整理に当たっては、対象のセキュリティ文書と我が国の法令、放射性同位元素の利用の実情等との整合性を主な着眼点とした。さらに、IAEAからNSGCのメンバー国に提示される新たな核セキュリティ関連文書のうち、放射性物質のセキュリティに関して記述のある文書について和訳作業を行った。

第5回NSGC（平成26年6月16～20日）、第6回NSGC（平成26年11月10～14日）及び非密封線源に関するテクニカルミーティング（平成27年3月30日～4月2日）については、平成24,25年度放射性物質のセキュリティに関する調査事業を担当したセンターの職員1名を会合へ派遣し、議論の動向、参加国の動向等の情報を収集、整理を行った。

4.1 核セキュリティ文書の内容確認及び論点整理

NSGCは、IAEAに設置された委員会であり、主に核セキュリティシリーズ文書の見直し提案、発刊前等の文書レビュー・コメント、安全とセキュリティのインターフェースに関する課題の調整等を活動内容としている。本調査では、第5,6回NSGCに向けた、核セキュリティ文書草案についての論点を整理することを目的の一つとしている。

NSGCでは、多数の核セキュリティに関する文書が策定段階にある。図4-1に放射線障害防止法の対象事業所に関連する核セキュリティに関する文書及び文書草案の体系図を示す。文書は、核セキュリティ基本文書を頂点とする階層構造となっている。

<核セキュリティ基本文書>

NSS 20

国の核セキュリティ体制の目的
及び不可欠な要素

<勸告>

NSS 13

核物質及び原子力施設の物理的防護に関するセキュリティ勸告

NSS 14

放射性物質及び関連施設に関するセキュリティ勸告

NSS 15

規制上の管理を外れた核物質及びその他の放射性物質に関するセキュリティ勸告

<実施指針・技術手引き>

【NSS 14 の下位文書】

NST 048(改訂 NSS 11)

使用、貯蔵及び関連施設に関する放射性物質のセキュリティ

NST 024

放射性物質及び関連施設のセキュリティ管理及びセキュリティ計画

NST 044(改訂 NSS 9)

放射性物質の輸送中のセキュリティ

【NSS 13, 14 に共通の下位文書】

NSS 10 設計基礎脅威の策定、使用及び維持

NST 026 核セキュリティ文化の自己評価

NST 027 施設及び活動のための核セキュリティ文化の強化

【NSS 13, 14, 15 に共通の下位文書】

NST 002 規則と関連行政措置

NST 006 国際協力と援助

NST 009 核セキュリティのための能力開発

NST 020 核セキュリティ体制の持続

NST 022 核セキュリティにおける情報のセキュリティ

NST 041 内部脅威者の脅威に対する予防及び防護措置 (改訂 NSS 8)

NST 045 核セキュリティのためのコンピュータセキュリティ

NSS 19 原子力計画のための核セキュリティの構造基盤の確立

NSS 7 核セキュリティ文化

NSS 12 核セキュリティの教育プログラム

NSS 17 原子力施設のコンピューターセキュリティ

図 4-1 放射線障害防止法の対象事業所に関連する核セキュリティに関する文書及び文書草案の体系図

表 4-1 及び表 4-2 に第 5 回及び第 6 回 NSGC における本調査での検討対象文書とその本調査における対応状況を示す。

放射線障害防止法に直接または間接的に関連する文書について、核セキュリティに関連する文書草案 5 件並びに文書作成計画草案 1 件の内容確認を行い、我が国の現状を踏まえた論点整理を行った。検討結果は原子力規制庁へ報告した。

表 4-1 第 5 回 NSGC の検討対象文書の分類と本調査における対応状況

◎：直接関連する文書， ○：関連のある文書

| | 進捗 | 文書番号 | 文書名称 | セキュリティ関連文書 | | セイフティ関連文書 | | Submission to MS for comments | Target publication date | 本調査における対応状況 |
|---|----|--------------|---|------------------|----------------|-----------|---|-------------------------------|-------------------------|--------------------|
| | | | | RI ^{iv} | 核 ^v | RI | 核 | | | |
| 1 | 7 | NST002 | Regulations And Associated Administrative Measures For Nuclear Security | ○ | ○ | — | — | — | — | 論点を整理し、原子力規制庁へ報告した |
| 2 | 7 | NST026 | Self-Assessment Of Nuclear Security Culture In Facilities And Activities That Use Nuclear And/Or Radioactive Material | ○ | ○ | — | — | — | — | — |
| 3 | 3 | NST045 (DPP) | Computer Security for Nuclear Security | ○ | ○ | — | — | Oct 2015 | Jan 2017 | — |

進捗状況の意味：STEP 1～14---- DS 文書準備の開始から完成までの進捗状況を 14 段階で表示する。

STEP 1-----文書作成計画（DPP（Document Preparation Profiles））の準備

STEP 2-----DPP の内部レビュー

STEP 3-----安全基準委員会（SSC(s)（Safety Standards Committee(s)））による DPP のレビュー

(STEP 4)※-----安全基準委員会（CSS（Commission for Safety Standards））による DPP のレビュー

STEP 5-----ドラフト基準（DS（Draft Standard））の準備

STEP 6-----DS の第 1 回内部レビュー

STEP 7----- SSC(s)による DS の第 1 回レビュー

STEP 8-----加盟国コメント要求

STEP 9-----加盟国コメントへの対処

STEP 10-----DS の第 2 回内部レビュー

STEP 11-----SSC(s)による DS の第 2 回レビュー

(STEP 12)※-----CSS による DS のレビュー

STEP 13-----IAEA 基準としての確立

STEP 14-----発刊

※：NSGC は、CSS へ承認は求めず、当該ステップは踏まれない。

^{iv} 放射性同位元素等による放射線障害の防止に関する法律に関連する文書

^v 核原料物質、核燃料物質及び原子炉の規制に関する法律に関連する文書

4.1.1 核セキュリティのための規則と関連行政措置（ドラフト 実施指針）

NST002: Regulations and Associated Administrative Measures for Nuclear Security

(1) 概要

本実施指針（NST002）は、核セキュリティ体制を統制するための立法と規制の枠組みを整備し、実施するために講じるべき措置に関して、国に指針を提供することを目的としている。

国に対して適切な規則、協定および関係する行政措置の整備を支援することによって、国内、また必要に応じ国家間で協力し調整のとれた方法で、割り当てられた任務と責任が実施され、法律に従って権限が行使されることを目指している。核セキュリティ体制を確立し、継続的に維持するための十分な財源的、人的および技術的資源を割り当てることの重要性を強調し、効果的な核セキュリティ体制を確立して持続するために適切な規則、協定および関連行政措置が整備できるように、国が核セキュリティに関与する人々の責任を特定することを支援する。

この実施指針は、国に対して、国の立法の枠組みや制度と両立する規則、協定および関連行政措置を選択して整備するための手段を提供しているが、規則案の作成についての具体的な勧告及びモデルとなる規則、協定または関連行政措置は与えられていない。

(2) 我が国の規制等との関連

我が国の放射線障害防止法と関連規則・告示には、核セキュリティ対策について、具体的な技術基準が示されていないため、本実施指針の策定が我が国の法制度と直接的な矛盾を生じる可能性は低いと考えられる。

本実施指針では、効果的な核セキュリティ体制を確立して持続するために適切な規則、協定および関連行政措置を整備するために、以下について指針が示されている。

- 核セキュリティのための一般的規制活動
- 脅威の評価
- 情報のセキュリティ
- 規制管理を外れた核物質とその他の放射性物質の検知
- 核セキュリティ事象の対策と対応
- 犯罪化を含む核セキュリティに関係する犯罪と刑罰

今後、我が国の RI 規制に追加すべき情報セキュリティ対策について検討するための参考となると考えられる。

(3) 論点の整理

本実施指針に対する論点の整理を行った。放射線障害防止法と関連規則・告示では、核セキュリティ対策について、具体的な技術基準が示されていないものの、安全に係る技術基準は体系的に構築されている。本実施指針の要求事項は、今後核セキュリティ対策について、具体的な技術基準を法制化するためには妥当なものであると考えられる。よって、以下の論

定整理の結果及び数点の編集上の修正案を原子力規制庁へ報告した。

- ・既存の安全に係る規則にセキュリティ条項を追加することが可能であることを明確にする。

(4) 第5回 NSGC での検討概要

NSGC 事務局から、本実施指針が説明された。事前に、ロシア、フランス、ウクライナ及び日本からコメントが提出されており、NSGC 事務局はそれらのコメントに対する対応を概説した。特に、ロシアからは実施指針ではなく、技術手引きに再区分すべきとの事前コメントがあり、事務局は、付録に記載されたモデル規則は、技術手引きとしての作成予定のものではないとの説明があった。原子力途上国からも重要な文書であり、実施指針として出版を望むコメントがあげられたが、ロシアから法令を作成する上でのハンドブックのような文書であり、実施指針のレベルではないとのコメントが出された。そのため、NSGC による決議（原子力安全・セキュリティ局事務次長（DDG-NS（Deputy Director General for Nuclear Safety and Security））へ提出すること）を一旦延期した。

再度の議論では、文書のレベル（ヒエラルキー）について、NSGC メンバーにより決定することとし、ロシアから、NSS 外の文書として作成すれば迅速な出版が可能とのコメントがあったが、西側諸国からは、多くの国が必要としており、実施指針として出版を望むとのコメントが出された。ロシアは一切妥協せず、議論は堂々巡りを繰り返した。結果、6th NSGC で再度議論し決定することとなった。

4.1.2 核セキュリティ文化の自己評価（ドラフト 技術手引き）

NST026 : SELF-ASSESSMENT OF NUCLEAR SECURITY CULTURE IN FACILITIES AND ACTIVITIES THAT USE NUCLEAR AND/OR RADIOACTIVE MATERIAL

(1) 概要

本技術手引き(NST026)は、核セキュリティ文化の自己評価を行ない、組織のセキュリティ管理体制に対する人的要因の影響を分析するための手引きを提供することを目的としている。

この評価は、組織の文化がどのように脅威環境に影響を与えるかを分析することによって行うものであり、その組織におけるセキュリティ文化の主要な特徴についての評価を伴うものである。セキュリティ文化の自己評価は、核セキュリティについての理解に焦点を当てて実施することにより、経営者から従業員まですべてのレベルに渡って認識、見識の向上を支援するものである。

本技術手引きは、自己評価について準備段階から調査分析と是正措置計画まで段階的なガイダンスを提供するために、以下の要素を含んでいる。

- ・ 一般的な組織文化と核セキュリティ文化の理解
- ・ IAEA の核セキュリティ文化へのアプローチ

- ・ セキュリティ文化の自己評価の概念と実施
 - 目的と利益， 特別の考慮， セキュリティ文化指標
- ・ セキュリティ文化の自己評価プロセス
- ・ 自己評価の方法
 - 調査， インタビュー， 文書レビュー， 観察
- ・ 分析の実施
- ・ 調査結果の伝達と活動の進展

(2) 我が国の規制等との関連

我が国では、放射線障害防止法と関連規則・告示による安全規制が実施され、教育訓練（法第 22 条）に放射線業務従事者に対する教育訓練に関して規定されている。ただし、核セキュリティ文化に関する事項は取り入れられていない状況にある。

核原料物質、核燃料物質及び原子炉の規制に関する法律関連規則には、核物質防護規定に記載すべき事項として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。）について規定されている。今後、我が国の RI 規制に追加すべき核セキュリティ文化について検討するための参考となる。

(3) 論点の整理

本技術手引きに対する論点の整理を行った。放射線障害防止法と関連規則・告示では核セキュリティ文化に関する規定が取り入れられていないものの、核セキュリティ文化については NSS No.14 でも言及されており、また本技術手引きの内容は、核セキュリティ文化の自己評価のためには妥当なものである。

(4) 第 5 回 NSGC での検討概要

本技術手引きは、120 日コメントのため加盟国への提出が承認された。米国から事前に提出されていた詳細なコメントは、120 日コメントの後、加盟国からのコメントとともに取り組むこととされた。

4.1.3 核セキュリティのためのコンピューターセキュリティ（文書作成計画 実施指針）

DPP NST045: Computer Security for Nuclear Security

(1) 概要

本実施指針(DPP NST045)は、2011 年に出版された核セキュリティシリーズNo.17「原子力施設におけるコンピューターセキュリティ（以下、「NSS No.17」という。）の改訂である。

コンピュータ、計算システム及びデジタル部品は核物質及び他の放射性物質と関連施設及び関連活動において機微情報管理、原子力安全、核セキュリティ及び計量管理で広範な役割を果たしている。Stuxnet マルウェアは、サイバー攻撃が巧妙になってきていることとまた核施設がサイバー攻撃により影響を受け得ること、コンピュータの使用が増大するに連れ、攻撃の対象も増えることを示している。

本文書の目的は、国の政策立案者が専門家、関係当局、事業者、施設管理者、セキュリティ担当者、技術者、協力会社の幅広い層を対象とし、核セキュリティのすべての分野のためのコンピュータセキュリティプログラムの作成を指導するための指針を提供することにある。

(2) 我が国の規制等との関連

我が国の放射線障害防止法と関連規則・告示には、核セキュリティ対策のうち、コンピュータセキュリティについては具体的な技術基準が示されていないため、本実施指針の策定が我が国の法制度と直接的な矛盾を生じる可能性は低いと考えられる。

本実施指針では、効果的なコンピュータセキュリティプログラムの作成を支援するため、以下について指針が示されている。

- ・ 国の政策実施
- ・ 組織の課題
- ・ 脅威、脆弱性とリスクマネジメント
- ・ コンピュータセキュリティの実装と維持
- ・ 特定の分野における考慮

核原料物質、核燃料物質及び原子炉の規制に関する法律関連規則には、必要な防護措置及び核物質防護規定に記載すべき事項として情報システムセキュリティについて規定されている。今後、我が国の RI 規制に追加すべきコンピュータセキュリティ対策について検討するための参考となると考えられる。

(3) 論点の整理

本実施指針に対する論点の整理を行った。放射線障害防止法と関連規則・告示では情報セキュリティ対策が取り入れられていないものの、コンピュータセキュリティを検討すること自体に問題はないと考える。現状段階は文書作成計画の段階でありため、具体的な要求事項は明らかでないが、示されている目次案は、コンピュータセキュリティの実装のためには妥当なものである。

(4) 第 5 回 NSGC での検討概要

本実施指針（DPP）は、すべての核セキュリティ分野をカバーする優先文書として承認された。また、本実施指針（DPP）のような分野横断的な指針を作成することに関する困難さについて、NSGC 加盟国の技術的な関心事項を議長報告に記載し、草案作成時に考慮することされた。

表 4-2 第 6 回 NSGC の検討対象文書の分類と本調査における対応状況

◎：直接関連する文書,

○：関連のある文書

| | 進捗 | 文書番号 | 文書名称 | セキュリティ関連文書 | | セイフティ関連文書 | | Submission to MS for comments | Target publication date | 本調査における対応状況 |
|---|----|--------|--|------------------|------------------|-----------|---|-------------------------------|-------------------------|--------------------|
| | | | | RI ^{vi} | 核 ^{vii} | RI | 核 | | | |
| 1 | 7 | NST009 | Building Capacity for Nuclear Security | ○ | ○ | — | — | — | — | 論点を整理し、原子力規制庁へ報告した |
| 2 | 7 | NST020 | Sustaining a Nuclear Security Regime | ○ | ○ | — | — | — | — | 論点を整理し、原子力規制庁へ報告した |

進捗状況の意味：STEP 1～14---- DS 文書準備の開始から完成までの進捗状況を 14 段階で表示する。

STEP 1-----文書作成計画（DPP（Document Preparation Profiles））の準備

STEP 2-----DPP の内部レビュー

STEP 3-----安全基準委員会（SSC(s)（Safety Standards Committee(s)））による DPP のレビュー

(STEP 4)※-----安全基準委員会（CSS（Commission for Safety Standards））による DPP のレビュー

STEP 5-----ドラフト基準（DS（Draft Standard））の準備

STEP 6-----DS の第 1 回内部レビュー

STEP 7----- SSC(s)による DS の第 1 回レビュー

STEP 8-----加盟国コメント要求

STEP 9-----加盟国コメントへの対処

STEP 10----DS の第 2 回内部レビュー

STEP 11----SSC(s)による DS の第 2 回レビュー

(STEP 12)※----CSS による DS のレビュー

STEP 13----IAEA 基準としての確立

STEP 14----発刊

※：NSGC は、CSS へ承認は求めず、当該ステップは踏まれない。

^{vi} 放射性同位元素等による放射線障害の防止に関する法律に関連する文書

^{vii} 核原料物質、核燃料物質及び原子炉の規制に関する法律に関連する文書

4.1.4 核セキュリティのための能力構築（実施指針）

NST009 : Building Capacity for Nuclear Security

(1) 概要

この実施指針は、組織と個人に有効な核セキュリティ体制を実行するための能力構築をするために、参考文書となることを意図している。核セキュリティに係る組織と個人の役割と責任を定義し、ニーズを評価し、プログラムを開発するための方法論が提供される。

主として国の管轄当局、機関および他の組織(学術機関および治安機関)向けであり、核物質と核施設のセキュリティ、放射性物質および関連施設および活動のための能力構築に取り組むことが記載されている。

(2) 我が国の規制等との関連

本文書は、政府、国の組織及びその属する個人に対し、核セキュリティのための能力構築の方法を与えている。本実施指針には、具体的な核セキュリティ対策の要求事項が示されているわけではないため、本実施指針の策定が我が国の法制度と直接的な矛盾を生じる可能性は低いと考えられる。

本実施指針では、効果的な核セキュリティのための能力開発を実施するために、以下について指針が示されている。例えば政府に対しては以下の要求事項が示されている。

- 国の組織と個人の能力を構築することについて、中心的な役割を持つことを認識すること。
- 法的枠組みの中で、必要とされる能力を構築する計画の策定と実施のための基礎を提供すること。
- 核セキュリティの責任を割り当てられた異なる組織の役割を確立すること。
- 核セキュリティ組織が、短期的、中期的、長期的に十分な人的資源を保持することを確実にすること。
- 核セキュリティ体制のために必要な人材の育成を支援するために、国の教育訓練基盤の妥当性を評価すること。
- 能力を構築するための知識管理の概念と知識交換のプログラムを支援すること。
- セキュリティ計画を実施するために必要な能力構築を促進するために、事業者との効果的関わりがあることを確実にすること。
- 核セキュリティ体制に責任のある組織を監視し、組織が政府に重要な問題点をフィードバックできることを確実にすること。
- 国際組織及びネットワークとの協力を可能にする仕組みを確立すること。

上記の政府への要求事項を踏まえ、組織及びその属する個人に対する要求事項が示されている。今後、我が国の核セキュリティ体制のための能力構築を実施する際には、参考となると考えられる。

(3) 論点の整理

本勧告文書に対する論点の整理を行った。本文書は、放射線障害防止法の対象となる事業者に指針を与えることを意図していない。我が国では、核原料物質、核燃料物質及び原子炉の規制に関する法律関連規則により、原子力施設に係る核物質防護体制が確立され、規制当

局、関係当局及び関連組織の責任と役割分担が明確になっている。また、その属する個人の能力開発も実施されている。

本実施指針の要求事項は、今後核セキュリティ体制のための能力構築を実施していくために妥当なものであると考えられる。よって、数点の編集上の修正案を原子力規制庁へ報告した。

(4) 第 5 回 NSGC での検討概要

NSGC 事務局から、本実施指針の概要が説明された。フランス、日本、ロシア、アルゼンチン及びウクライナから事前に多数のコメントが提出されており、それらを踏まえ、必要な修正が要求された。修正点が多数に及ぶため、120 日コメントのために加盟国へ提案することは承認されなかった。

4.1.5 核セキュリティ体制の持続性（実施指針）

NST020 : Sustaining a Nuclear Security Regime

(1) 概要

核セキュリティ体制が効果を維持するためには、国レベルと事業所レベルの両方で長い期間にわたって核セキュリティ体制を持続させなければならない。国レベルでは、核セキュリティへの統合的アプローチを支援する包括的な政策と戦略に取り組むため、以下の核セキュリティ体制の要素が含まれる。

- ・核セキュリティに関する法規制の枠組み
- ・核セキュリティの役割と責任の割り当て
- ・脅威を国レベルで定義する責任

国レベルの関係行政機関はまた、以下に述べるように運用レベルの核セキュリティ対策を支援し、事業所レベルにおける法規制の枠組みの実施に欠落や矛盾がある場合、関係行政機関はフィードバックを得る仕組みをもっていなくてはならない。

事業所レベルには、施設で実施されるか、あるいは核物質やその他の放射性物質の所有、生産、使用、処理、貯蔵、処分などの活動、核物質やその他の放射性物質の輸送活動、および規制を逸脱した核物質やその他の放射性物質の検知・対応活動に関連して実施される核セキュリティシステム・対策が含まれる。

本実施指針（NST020）は、核セキュリティ体制の持続を目的とし、国、関係行政機関、ライセンス保持者、核セキュリティ体制を持続させる原則と行動に関する核セキュリティ上の責任を有するその他の団体に指針を与える。

(2) 我が国の規制等との関連

本文書は、国レベル、事業所レベルの核セキュリティ体制の持続について、持続可能性の原則と取るべき実施行動を含めて、国レベル及び事業所レベルで核セキュリティ体制を持続させることについての指針を与えている。わが国では、放射線安全については、放射線障害防止法と関連規則告示により、体系的に規制の枠組みが構築、持続されている。今後、わが国の核セキュリティ体制の持続のための検討をする際には、参考となると考えられる。

(3) 論点の整理

本実施指針に対する論点の整理を行った。放射線障害防止法と関連規則・告示では、具体的核セキュリティ対策が取り入れられていないものの、国レベル、事業者レベルでの核セキュリティ体制の持続性について検討すること自体に問題はないと考える。本実施指針に示されている、具体的な要求事項は、核セキュリティ体制の持続のためには妥当なものである。

本文書に対する論点の整理を行った。我が国では、核原料物質、核燃料物質及び原子炉の規制に関する法律関連規則により、原子力施設に係る核物質防護体制が確立され、持続されている。今後放射線障害防止法とその関連規則告示に核セキュリティに関する要求事項を取り入れる際にも参考になる。

本実施指針の要求事項は、今後核セキュリティ体制のための持続を検討するために妥当なものであると考えられる。よって、数点の編集上の修正案を原子力規制庁へ報告した。

(4) 第5回 NSGC での検討概要

NSGC 事務局から、本実施指針の概要が説明されたのち、120 日コメントのために加盟国へ提案することを承認した。

4.1.6 使用及び貯蔵中の放射性物質及び関連施設のセキュリティ（文書作成計画 実施指針）

NST048 : Security of Radioactive Material in Use and Storage and of Associated Facilities

(1) 概要

本実施指針（NST048）は、2009 年に出版された NSS No.11 放射線源のセキュリティに関する実施指針の改訂を意図している。NSS No.11 は NSS No.20（核セキュリティ基本文書：国の核セキュリティ体制の目的及び不可欠な要素）や NSS No.14 より先に出版され、その結果、NSS No.11 の中で使用される事項および用語のうちのいくつかは、NSS No.14 および No.20 と整合していない部分が生じている。

この改訂の最初の理由は、NSS No.14 および No.20 において提供されるガイダンスを正確に反映することである。

NSS No.13 核物質及び原子力施設の物理的防護に関する核セキュリティ勧告（INFCIRC/225/Rev.5）に基づいた実施指針は NST023 として開発中である。本実施指針（NSS No.11）の改訂は、NSS No.13 に基づいた実施指針（NST023）と構成上の整合性を確保しつつ、放射性物質、関連施設および活動への適用のために包括的手引きを提供することを第二の理由としている。

本実施指針を改訂する第三の理由は、NSS No.11 においてカバーされない事項に関して追加の事項を含むより包括的な実施指針を確立することである。具体的には、

- ・密封線源だけでなく密封されていない放射性物質（NSS No.14 の適用範囲に含まれている）を含めるために NSS No.11 の適用範囲を広げること
- ・脅威評価に関してより詳細な説明を記載すること
- ・セキュリティ管理要素に関してより詳細な説明を記載すること

が挙げられている。なお、放射性物質、関連施設及び関連活動のセキュリティ管理とセキュ

リティ計画に関する個別の実施指針(NST024)は現在開発中である。

(2) 我が国の規制等との関連

我が国では、放射線障害防止法と関連規則・告示による安全規制が実施され、その安全対策が核セキュリティに寄与する 경우가多々あるが、核セキュリティ対策の具体的な技術基準が明確に示されていないため、現時点では本実施指針の策定が我が国の法制度と直接的な矛盾を生じる可能性は低いと考えられる。

(3) 論点の整理

本実施指針に対する論点の整理を行った。表 4-3 に NST048 に対する論点整理のための検討表を示す。

表 4-3 NST048 に対する論点整理

| 論点整理の対象となる NST048 の内容 | 論点整理結果 |
|--|---|
| <p>1.序論</p> <ul style="list-style-type: none"> - 付属文書Ⅰ -セキュリティ対策の概要 - 付属文書Ⅱ -事業者のセキュリティ計画に関する注釈付きアウトライン - 付属文書Ⅲ -脆弱性評価の例 | <p>現行の NSS No.11 にある付属文書Ⅳ「選定された施設及び活動に適用されるセキュリティ措置の実例」は、具体的な核セキュリティ対策を検討する上で参考となる。削除されたことが疑問である。</p> |
| <p>3.放射性物質、関連施設、及び関連活動に関する国家核セキュリティ体制の要素</p> <p>防護が必要な機微情報の種類は以下を含む。</p> <ul style="list-style-type: none"> - 放射性物質・関連施設・関連活動に対して整備されたセキュリティ・システム及びその他セキュリティ対策の詳細（警護部隊及び対応部隊に関する情報を含む） - 放射性物質の品質・形状・位置に関する情報（放射性物質の計量情報を含む） - セキュリティにとって直接的または間接的に重要な情報を処理・操作・保存・伝送する、通信システムを含むコンピューター・システムの詳細 - 対応計画 - 雇用者・ベンダー・受託業者の個人情報 - 脅威の評価及び情報 - 機微技術の詳細 - 上記項目に関する脆弱性または弱点の詳細 - 上記項目のいずれかに関する履歴情報 | <p>核セキュリティシリーズ文書で機微技術に関するセキュリティ対策の取り扱いを確認する必要がある。</p> |
| <p>国際協力及び支援</p> <p>各国は、国家核セキュリティ体制に由来する情報・知識の適切な共有を含め、核セキュリティ情報の機微性及び国内法の枠組みに基づいてそれを防護・共有する必要性を考慮して、他国との協力は是非及び協力範囲を検討しなければならない。</p> | <p>NSS No.14、3.14 項では、「推奨する」と記載されており、勧告文書との整合性の観点からも義務にすべきではないと考える。</p> |
| <p>脅威の識別及び評価</p> <p>脅威の増加</p> <p>セキュリティ・システムは、国家脅威評価に基づく脅威に反撃する上で、または必要に応じて DBT もしくは ATS で確定されるように、有効でなければならない。しかし、規制機関</p> | <p>セキュリティ計画に含めた時点でテストの対象になるため、改めて記述する必要はないと考える。 あわせて、付録Ⅱ セキュリティ</p> |

| | |
|---|---|
| <p>は脅威が突然増加している期間中の一時的なセキュリティ・システムの強化を保証する事前措置も確立すべきである。そのような事前措置は、脅威の増加に対抗する追加セキュリティ管理対策を事業者が導入するという要件を含んでいなければならない。該当の対策は事業者のセキュリティ計画に包括され、定期的にテストされなければならない。</p> | <p>計画の概要(注釈付き) 4.セキュリティシステム に脅威の増加に対抗する追加のセキュリティ対策の導入について追記することが望ましい。</p> |
| <p>5.放射性物質のセキュリティに関する規制プログラムの確立 5.2 ステップ 2:放射性物質に適用可能なセキュリティレベルを決定 - 「セキュリティに基づく区分け」 5.2.1.1 放射性崩壊 放射性崩壊のため、A/D 比は徐々に低下する。規制当局は、これを規制業務に取り入れる必要がある。 例えば、Co-60 線源は装置に最初に使用された 2015 年 1 月 1 日時点で、放射能レベルは 56 TBq であった。A/D 比を計算すると、$56 \text{ TBq} / 0.03 \text{ TBq} = 1867$ となる。そのため、最初、この線源に区分 1 が割り当てられる。 Co-60 の半減期は 5.2714 年である。半減期を 3 回迎えると(約 15 年)、Co-60 線源は崩壊し、放射能レベルは 7 TBq であるため、A/D 比は $7 \text{ TBq} / 0.03 \text{ TBq} = 233.33$ となり、これは区分 2 に相当する。</p> | <p>現在の密封線源の管理は、原則的に減衰を考慮しない運用となっている。 減衰の考慮を義務化すると、規制の運用を大きく変える必要が生じるかもしれない。規制業務への放射性壊変の考慮は、国ごとに運用を任せると考える。</p> |
| <p>5.2.3.セキュリティレベルの割り当てに関する追加の考慮事項 5.2.3.8 放射性廃棄物 放射性廃棄物は、管理するために次の 3 つの一般区分に分けられることが多い[参考文書 GSG-1]。使用済み核燃料、及び使用済み核燃料の再処理によって生じた廃棄物が定義に含まれる高レベル廃棄物 (HLW)、中レベル廃棄物 (ILW)、及び低レベル廃棄物 (LLW)。表 5 の放射性核種が放射性廃棄物として指定される場合、その放射能レベルは一般的に LLW 又は ILW に区分けされ[参考文書 GSG-1 中の図 iii-1]、セキュリティレベル A が割り当てられる。</p> | <p>低レベル廃棄物にセキュリティレベル A を割り当てることは過剰であり、放射性廃棄物は、5.2.1 及び 5.2.2 項に従って、区分され、セキュリティレベルが割り当てられるべきと考える。</p> |
| <p>6.規則内容に関する推奨事項 6.1 規範的手法 規制当局は、セキュリティ対策を規定する規則を確立することができる。このセキュリティ対策とは表 3 のセキュリティの目的に適合するために、事業者が実施しなければならないものである。表 8、表 9、表 10 は、セキュリティレベル A、B、及び C、それぞれに対する検知対策、遅延対策、及び対応対策を特定した。これらの表は、使用中又は貯蔵中の放射性物質に適用される。表 9 には、野外で使用する可搬型装置に対する特定のセキュリティ対策も含まれている。表 11 では、3 つの全セキュリティレベルに関するセキュリティ管理対策を特定している。上記の対策については、対応する各表の後に詳述する。本文の意図は主に読者に対して各表を明確に説明することであるが、諸規則又はガイダンスに抜粋することもできる。</p> | <p>表 11 に示されている核セキュリティ措置以外に選択できないような記載であり、各国が実情を考慮して、具体的核セキュリティ措置を選択できるようにすべきと考える。</p> |
| <p>セキュリティレベル C に対する対策の概要 セキュリティレベル C の目標は、セキュリティシステムが放射性物質の不法移転を防止する信頼度を確保することである。セキュリティレベル C の放射性物質が収容された可搬型装置を野外で使用する場合、セキュリティレベル B の装置に関するセキュリティ措置で防護することができる。</p> | <p>セキュリティレベル C の対応は、放射性物質の不法移転が発生した場合に適切な措置を実施することである。即時の対応を要求するものではなく、セキュリティレベル B の核セキュリティ措置中、特に対抗部隊への事前通報を義務化すること</p> |

| | |
|---|--|
| <p>セキュリティ管理対策の概要</p> <p>セキュリティ管理</p> <p>セキュリティの目的： 許可を受けた個人の信用性（trustworthiness）及び信頼性（reliability）を確保。</p> <p>セキュリティ対策： 放射性物質への付き添いなしのアクセス及び/又は機微情報へのアクセスの許可を受けた全要員の身元調査。</p> <p>個人の信頼性（trustworthiness）を評価する場合、当該個人に対して放射性物質、或いは放射性物質を使用又は貯蔵する場所への付き添いなしのアクセスを許可する前、或いは関連の機微情報へのアクセスを許可する前に十分な身元調査を行うものとする。身元調査の性質及び深さは、放射性物質のセキュリティレベルに比例し、国の規則又は規制当局の決定によるものとする。身元調査で最低必要なのは、各個人の識別情報の確認、及びその信用性（trustworthiness）及び信頼性（reliability）を決定するための参考書類の検証である。<u>身元調査では、犯罪行為歴も開示する必要がある。このプロセスは定期的に見直すものとし、これをサポートするために監督者又は管理者が継続監視を行うものとする。これは、確実に全レベルの要員が責任及び信頼性を持って行動し、これに関連する懸念を関係当局に知らせるためである。定期的（例、5年毎）に再確認を実施するものとする。</u></p> <p>多くの国において、事業者は身元調査を実際に実施する許可を受けていない、又はその能力がない。その代わりに、事業者の要求を受けて身元調査を実施する法執行機関、法務省、又はその他の所管当局に依存している。この場合、<u>規制当局は国の行政組織内で身元調査を実施する責任を負う実施主体を特定し、事業者とこの実施主体間の必要な連絡を促すものとする。</u>身元調査結果は、セキュリティ及びプライバシー上の理由から機微情報と見なされるため、しかるべく防護するものとする。</p> | <p>は過剰な要求であると考える。</p> <p>犯罪行為例を身元調査の必須項目とすること及び規制当局の犯罪行為歴の取得に関する役割が記載されている。</p> <p>日本では、犯罪行為歴については非常に機微な個人情報となっており、事業者は言うまでもなく規制機関においても入手することは不可能と考えられる。</p> |
|---|--|

放射線障害防止法と関連規則・告示では放射性物質の核セキュリティ対策が取り入れられていないが、勧告文書と実施指針との整合性を確保することや密封されていない放射性同位元素の核セキュリティ対策は重要と考えられ、NSS No.11 を改訂するという方針自体は妥当である。

本実施指針案は「使用、貯蔵及び関連施設における放射性物質のセキュリティ」の表題が提案されている。特に大きな変更は、密封されていない放射性物質を実施指針の対象に追加した点である（勧告では密封されていない放射性物質も対象とされている）。この点については、

- ・セキュリティ対象となる放射性物質を区分するための数量に密封線源と同様なD値が使用されており、このD値を超えるような数量の密封されていない放射性物質を使用している事業所が少数であること。
- ・半減期の短い（10日以下が例示されている）放射性物質については、その点を考慮できることが記載されていること。

の観点から、我が国に与える影響は限定的であると考えられる。

また、個人の信頼性確認における身元確認の要素において、特に犯罪歴の扱いについては、放射性同位元素の規制制度に取り入れることが非常に難しいと思われる。

表 4-3 の検討結果から、以下の論点を原子力規制庁へ報告した。

- ・ 現行の NSS No.11 にある付属文書 IV 「選定された施設及び活動に適用されるセキュリティ措置の実例」の削除理由が不明。
- ・ 核セキュリティシリーズ文書で機微技術に関するセキュリティ対策の取り扱いを確認する必要がある。
- ・ 勧告文書との整合性の確保について（特に、「should」と「may, could」の使い分けなど）。
- ・ 「付録 II セキュリティ計画の概要（注釈付き） 4.セキュリティシステム」に脅威の増加に対抗する追加のセキュリティ対策の導入について追記することが望ましい。また、セキュリティ計画に含めた時点でテストの対象になると考える。
- ・ 現在の密封線源の管理は、原則的に減衰を考慮しない運用となっている。減衰の考慮を義務化すると、規制の運用を大きく変える必要が生じるかもしれない。規制業務への放射性壊変の考慮は、国ごとに運用を任せるべきと考える。
- ・ 低レベル廃棄物にセキュリティレベル A を割り当てることは過剰であり、放射性廃棄物は、放射能と D 値に従って、区分され、セキュリティレベルが割り当てられるべきと考える。
- ・ 各国が実情を考慮して、具体的核セキュリティ措置を選択できるようにするべきと考える。
- ・ セキュリティレベル C の対応は、放射性物質の不法移転が発生した場合に適切な措置を実施することである。即時の対応を要求するものではなく、対抗部隊への事前通報は過剰な要求であると考えられる。
- ・ 犯罪行為例を身元調査の必須項目とすること及び規制当局の犯罪行為歴の取得に関する役割が記載されている。日本では、犯罪行為歴については非常に機微な個人情報となっており、事業者は言うまでもなく規制機関においても入手することは不可能と考えられる。

(4) 技術会合（TM）での検討概要

全体的に、参加国は当該実施指針案の重要性を理解し、実施指針の改訂自体に否定的な意見は見受けられなかった（ロシアからも、特段の反対意見はなかった）。

各国から出されたコメントは、当該実施指針の対象範囲が拡大したことに伴い変更された部分について、記載の明確化、表現の適正化、表現の斉一化を求めるものが多かった。

また、非密封放射性同位元素、核分裂性以外の核物質（劣化ウランなど）の区分の方法、安全とセキュリティのインターフェースに関心を示す国があり、記載の充実を求めている。

本実施指針案は本年 11 月に予定されている NSGC において審議される予定となっている。加盟国への 120 日コメント手続きは、当初の文書作成計画から遅れて、本年第 4 四半期の予

定となった。しかしながら、出版予定時期については、当初の計画どおり 2016 年第 4 四半期の計画となっていることが事務局から説明された。

4.2 放射性物質のセキュリティに関して記述のある文書について和訳作業

IAEA から NSGC のメンバー国に提示された新たな核セキュリティ関連文書（下記①～④）及び今後我が国における核セキュリティにかかる検討を行う際に参考になるような文献（下記⑤）について、和訳作業を行った。以下に、和訳作業を行った関連文書のリストを示す。

①「核セキュリティのための規則と関連行政措置」

「NST002 : Regulations and Associated Administrative Measures for Nuclear Security」

②「核セキュリティ体制の持続性」

「NST020 : Sustaining a Nuclear Security Regime」

③「使用及び貯蔵中の放射性物質及び関連施設のセキュリティ」

「NST048 : Security of Radioactive Material in Use and Storage and of Associated Facilities」

④「規制管理を外れた核物質及びその他の放射性物質のための予防措置」

「NST011 : PREVENTIVE MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL」

⑤「NUREG-2166 リスクの大きい放射性物質の防護のための物理的セキュリティのグッドプラクティス」

「NUREG-2166 Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material」

4.3 NSGC 会合へ専門家若しくは学識経験者等 1 名の派遣

4.3.1 第 5 回 NSGC

I. 開催日程 平成 26 年 6 月 16 日（月）～20 日（金）

II. 開催場所 IAEA A 会議室（ウィーン）

III. 主な論点（放射性同位元素に関連する事項）

1. 6th NSGC を 2014 年 11 月 10-14 日に開催することが確認された。7th NSGC は、2015 年 6 月 22-26 日の週に開催する。
2. NST026（核セキュリティ文化の自己評価に関する技術手引き）は、120 日コメントのため加盟国への提出が承認された。懸案の米国のコメントは、120 日コメントの後、加盟国からのコメントとともに取り組む。
3. NST045 の文書作成計画（核セキュリティのためのコンピュータセキュリティに関する実施指針）は、核セキュリティのすべてをカバーする範囲で、優先文書として承認された。すべての領域についてこの様なガイダンスの準備の困難さに関して、NSGC メンバーの技術的な関心事項は、議長報告書に記載するとともに草案作成時に考慮すること。
4. NST002（規則と行政措置に関する実施指針）は、NSGC による決議を延期した。主な議論は、以下のとおり。

- ・事務局から、付録に記載されたモデル規則は、技術手引きとしての作成予定のものではないとの説明があった。
 - ・原子力途上国からは重要な文書であり、実施指針として出版を望むコメントがあげられたが、ロシアから法令を作成する上でのハンドブックのような文書であり、実施指針のレベルではないとのコメントがあった。
5. NST023（核物質と原子力施設の物理的防護に関する実施指針）は、フランスから表 2 中の施設の特定の種類を挙げることを削除する要求とともに加盟国へ提出することを承認した。
 6. NST002（規則と行政措置に関する実施指針）の議論の続きについて
 文書のレベル（ヒエラルキー）について、NSGC メンバーにより決定することとした。
 ロシアから、NSS 外の文書として作成すれば迅速な出版が可能とのコメントがあったが、西側諸国からは、多くの国が必要としており、実施指針として出版を望むとのコメントが出された。ロシアは一切妥協せず、議論は堂々巡りを繰り返したが、6th NSGC で再度議論し決定することとなった。

4.3.2 第 6 回 NSGC

I. 開催日程 平成 26 年 11 月 10 日（月）～14 日（金）

II. 主な論点（放射性同位元素に関連する事項）

1. 第 7 回 NSGC を 2015 年 6 月 22～26 日、第 8 回を 2015 年 11 月 2～6 日に開催することが確認された。第 9 回 NSGC は、2016 年 6 月 20～24 日に開催することを暫定的に合意した。
2. NST020（実施指針：持続可能な核セキュリティ体制）は、120 日コメントのために加盟国へ提案することを承認した。
3. NST009（実施指針：核セキュリティの能力開発）の草案について、NSGC のコメントを踏まえ、必要な修正を要求し、120 日コメントのために加盟国へ提案することは承認されなかった。加盟国からの修正コメントが多く、本会合では承認されなかったため、今後修正版草案が提示される。
4. NST036(技術手引き:原子力施設における I&C システムのコンピュータセキュリティ) は、120 日コメントのために加盟国へ提案することを承認した。CSS により、DS431 へ挿入された安全とセキュリティのインターフェースに関する記載とドイツにより提案された記載は、3.48 項の代わりの記載として加盟国へ提案する草案に含めるべきである。草案は、NUSSC と WASSC の会合に情報提供するべきである。
 本文書は、放射性同位元素取扱施設について適用範囲外であるが、コンピュータセキュリティ、サイバーセキュリティについては、勧告レベルでの要求事項の有無について検討が進められている。新たな関連文書草案が提案された場合には詳細な検討が必要と思われる。
5. NST041（実施指針：内部脅威対策のための準備と防護措置）は、フィンランドから提案された、段階的手法に従って規制管理外の物質に係る内部脅威対策も含まれるべきと

の声明を適用範囲へ包含し、120日コメントのために加盟国へ提案することを承認した。

6. DPP NST051（原子力施設の存続期間のセキュリティ）は、実施指針への文書区分の変更と文書の作成準備計画に技術会合を入れることとして承認した。
7. NSGC、現時点においてNSS No.13, 14, 15を修正する必要ないことを承認した。それでも、コンピュータセキュリティに係る勧告レベルの指針を同定する作業は継続するべきである。NSGCメンバーは、2015年2月末までにNUSECの現在の文書についてコメントする。そして事務局は次回会合の議論のために進捗の状況を次回NSGC会合の前に提出する。
8. NSGCは、OIOSが提出した委員会構造のレビューの結論と勧告の内容について注目した。NSGCは、JTF（ジョイントタスクフォース）の長期間のビジョンの妥当性について整理された立場を持っていない。

NSGCは、OIOSレビューにおけるいくつかの改善点を認めたが、OIOSレビューによる全ての勧告は、NSGCに改善を与える最善の方法であるということは認めなかった。特にNSGCは、

- ・複数の核セキュリティ委員会を組織するべきではない
- ・NSGCは、複数のテーマの委員会に分けるべきではなく、可能であれば、NSGCの下にアドホックなワーキンググループを設置する

ということもNSGCの決定事項として勧告することを試みたが、意見はまとまらなかった。NSGCは、メンバーはOIOSレビューについてもコメントがあれば、2014年12月中旬までにアップロードすることとした。

4.3.3 非密封線源に関するテクニカルミーティング

I. 開催日程 平成27年3月30日（月）～4月2日（木）

II. 主な論点

1. テクニカルミーティング（以下「TM」という。）で議論すべき、専門家会合で提起された論点が以下のとおり挙げられた。
 - ①セキュリティに基づく放射性物質の区分
 - ②全ての放射性物質を含めるための現行NSS No. 11の適用範囲の拡大
 - ③廃棄物及び使用済み線源
 - ④携帯形及び可搬形の線源
 - ⑤セキュリティ管理及びセキュリティ計画
2. 放射性物質のセキュリティに関係するIAEAの活動に関するプレゼンテーション
以下のIAEAの活動について発表が行われた。
 - ・輸送中の放射性物質のセキュリティを扱う改訂版NSS No.9の策定の進捗状況
 - ・全体的な及び放射性物質のセキュリティに関連した情報とコンピュータセキュリティに関連する文書の作成状況
3. 実施指針草案に関するコメントと推奨事項

出席者は、ドラフト文書に関し、質問、意見及び提案を提供した。具体的な論点は文書ファイルにコメント追記又は変更履歴を残した形での修正を行うことによって記録さ

れた。一般的なコメントを以下に示す。

- ①「関連した活動」を文書名に含めるべきであり、文書全体に渡って、必要な場所に追記するべきである。
- ②文書名は、処分が含まれ輸送が除かれる文書の範囲を反映したものに修正されるべきである。
- ③核物質を含む全ての放射性物質に対する指針草案の適用性について提起され、記載を明確化するために NSS No. 14 の 1.16-1.18 の内容を追記することについて検討することが提案された。
- ④書全体をとおして用語の一貫性をチェックすべきである。「認可/認可された者」と「許可/被許可者」、「セキュリティ対策」と「セキュリティシステム」と「物理的セキュリティ」、「放射線源」と「密封された放射線源」、「行政手続き」と「管理手続き」、「不法移転」と「盗難」、「被許可者としての事業者」と「放射線作業員としての事業者」を含む例が挙げられた。また、用語「事業者」は NSS No.14 と NSS No.20 で定義が異なり、放射線源を使用する者を一概に事業者とはしていないことについても言及された。
- ⑤略語のリストを追加する必要がある。
- ⑥3つのセキュリティレベルの目標は、不法移転のみを念頭に置いたセキュリティ措置を記載した実施指針であることを考慮しつつ、すべての犯罪行為の防止を含むように広げられるべきである。
- ⑦セキュリティに関する放射線防護要員の役割を明確にすべきである。
- ⑧安全（放射線防護）とセキュリティの間の調整や協議を含む、安全とセキュリティのインターフェースをどのように考慮するかについて、記載の明確化が必要である。概念図が有用であることが指摘された。
- ⑨D 値の適用や放射性廃棄物、放射線源以外の放射性物質及び核物質のカテゴリー分けについては、さらなる議論が必要であるとともに、実施指針での例示を拡充すべきである。
- ⑩目次と章番号の割り振りは完了されるべきである。
- ⑪総論として付属文書は有用であると確認されたが、技術的な設備要件に関連する言葉（“十分な”、“良好な品質”のような）のいくつかは、付属文書 I をわかりやすくするために明確化されるべきである。

また、以下に記載されている特定のトピックスについても出席者により提起され議論された。

- ・可能性のある放射性物質の悪用方法として、故意の空気中への拡散と吸入に対応する手引きが、文書に追加されるべきである。
- ・メンテナンスや事業所外での対応などを含むセキュリティに関係がある契約先に対する要求事項の必要性
- ・代替技術の尊重に関して、指針の記載をどのレベルまで詳細にするべきか。
- ・少数の従業員しかいない施設の安全とセキュリティのインターフェースの問題。

- ・セキュリティ計画の一部若しくは別文書としての対応計画の明確化。「危機管理計画」がNSS No.13で使用され、「対応計画」がNSS No.14で使用されており、用語の明確化も求められた。

4. 更なるIAEA手引きの必要性に関する自由討論

以下のトピックスは、放射性物質のセキュリティに関連した更なる手引きが有用となるかもしれない分野として出席者によって認識された。

- ①セキュリティ要員のためのオンライントレーニング
- ②放射線源に関する脆弱性評価
- ③セキュリティシステムの有効性評価
- ④緊急時におけるセキュリティ対策
- ⑤現場でセキュリティ規制当局職員により使われる様式とチェックリスト
- ⑥輸送時に安全とセキュリティに関する統合されたアプローチを取り入れること
- ⑦国のセキュリティ体制の中でのNSS No.13と14の統合
- ⑧セキュリティに関係がある契約先に対する要求事項
- ⑨情報を分類するための基準、機微情報の識別
- ⑩関連文書や異なるレベルの文書（例、勧告、実施指針、技術手引き）を特定できるようにする、安全とセキュリティの分野における、IAEA文書の管理手順書及びIAEA文書を体系化する仕組み
- ⑪NSS No.11を実際に使用した実演的な説明

5. 全体的な結論

出生者は、TMにおけるコメントや改善提案の慎重な検討を通じて、実施指針草案が、IAEAメンバー国における放射性物質のセキュリティのための規制制度の構築及び一層の改良の際の手助けとなる適切なものであると認識した。

6. 今後の手順

議長報告は2015年4月2日に参加者に配布され、報告へのコメントは2015年4月14日まで事務局が受け付け、その後、報告は最終版としてNUSECに掲示されることとなる。

事務局は、TM前及びTM中に受けたコメント及び決定事項を含めた対応状況の一覧を作成する予定である。新たな実施指針草案は、参加者からの提案、コメント、修正を反映して作成される予定である。対応状況の一覧と新たな実施指針案は可能な限り早急に参加者に配布される予定である。

5. 委託調査検討委員会における論点整理

放射性同位元素の使用及びそのセキュリティについての知見を有する専門家、学識経験者から構成される委託調査検討委員会（参考資料 1 委託調査検討委員会名簿参照）を立ち上げ、事務局が予め作成した調査検討案について議論及び論点整理を行った。本委員会は、第 5 回、第 6 回 NSGC 会合の日程も踏まえ開催日を調整した。

5.1 委託調査検討委員会の開催日程

以下に、委託調査検討委員会の開催概要を示す。

(1) 第 1 回委託調査運営委員会

日 時：平成 26 年 5 月 22 日（木）14：00～16：45

場 所：（公財）原子力安全技術センター 3 階 小会議室

論 点：平成 26 年度調査事業計画について、事務局より説明し、調査内容のうち、特定放射性同位元素の防護措置に係る調査及び非密封線源セキュリティに係る調査について議論された。特に、タイムライン評価、不法行為シナリオについて具体的な検討が行われた。

(2) 第 2 回委託調査運営委員会

日 時：平成 26 年 9 月 17 日（水）14：30～18：10

場 所：（公財）原子力安全技術センター 4 階 大会議室

論 点：放射線施設の具体的なセキュリティ対策について議論された。信頼性確認の必要性について、本人確認とセキュリティの必要なエリアへ入室する必要性の確認は、最低限実施するべきだが、セキュリティの重要性とどこまで実施するかのバランスを考慮することも必要であるとされた。

(3) 第 3 回委託調査運営委員会

日 時：平成 27 年 2 月 4 日（木）15：55～17：00

場 所：（公財）原子力安全技術センター 4 階 大会議室

論 点：セキュリティ計画の記載内容、運用方法等について議論された。核セキュリティ対策機器の維持管理の方法については、検査期間、予防保全の必要性の有無、安全に係る機器等に対するものとの整合について意見が出された。運用方法については、認可又は届出の必要性の有無について検討された。

(4) 第 4 回委託調査運営委員会

日 時：平成 27 年 4 月 21 日（火）14：00～16：00

場 所：（公財）原子力安全技術センター 3 階 中会議室

論 点：平成 27 年 3 月 31 日から 4 月 2 日に実施された非密封線源に関するテクニカルミーティングの内容に関する報告及び我が国に規制を取り入れる際の課題について議論された。また、本年度調査に係る報告書の全体構成について確認し、特に防護措置案の内容については、文言の詳細な確認が行われた。

5.2 各委託調査検討委員会の議論

各委託調査検討委員会では、予め委託調査検討委員会事務局が作成した検討資料について議

論を行い、出されたコメントや意見を踏まえた修正を加えながら、最終報告書を作成した。

まとめ

本調査は、放射性同位元素のセキュリティ対策を検討するために、想定される脅威に対抗し、盗取を防ぐための具体的な防護措置案を作成するとともに、事業者にてセキュリティ計画を作成する際に参考となる標準的なセキュリティ計画案を取りまとめた。

防護措置案の作成については、防護対象を放射線源登録制度の対象となる特定放射性同位元素（カテゴリー1及び2並びにカテゴリー3のうち、アフターローディング装置及び非破壊検査装置）とし、以下の4項目について整理、検討した。

- (1) 国際基準の防護措置と国内における防護措置との対応の整理
- (2) セキュリティ目標とその考え方
- (3) 脅威評価結果に基づく不法行為シナリオの検討
- (4) タイムライン評価と防護措置案の検討

標準的なセキュリティ計画案の作成については、防護措置案の検討結果を踏まえるとともに、上位文書である勧告文書 IAEA NSS No.14 及び実施指針 NSS No.11 にある防護計画の内容及びカナダの例を参考に、必要と考えられる記載内容を抽出した。

また、IAEA における RI 文書に係る議論等を含め最新の知見を入手することを目的として、対象 RI 文書の調査及び IAEA テクニカルミーティング等への出席をとおして、最新の知見を取りまとめた。

IAEA NSGC で策定されている核セキュリティ文書のうち、5 件のドラフト文書及び 1 件の文書作成計画（DPP）に対して、我が国の法令、我が国における放射性同位元素の利用の実情等との整合性を比較した上で、原子力規制庁が対応方針を作成する際の材料となるよう論点整理を行った。また、我が国にとって参考になると思われる核セキュリティに関連する資料について和訳作業を実施した。

特に、IAEA の NST048 使用及び貯蔵中の放射性物質及び関連施設のセキュリティ（実施指針）の改訂については、NSS No.14 と整合性のとれたものにするためのものである。特に大きな変更は、密封されていない放射性物質を実施指針の対象に追加した点であるが、以下の観点から我が国に与える影響は限定的であると考えられる。

- ・セキュリティ対象となる放射性物質を区分するための数量に密封線源と同様な D 値が使用されており、この D 値を超えるような数量の密封されていない放射性物質を使用している事業所が少数であること。
- ・半減期の短い（10 日以下が例示されている）放射性物質については、その点を考慮できることが記載されていること。

また、個人の信頼性確認における身元調査の項目として犯罪歴が挙げられているが、日本では、放射性同位元素の規制制度に取り入れることが非常に難しいと考えられるため、今後 IAEA NSGC の議論とともに国際的な検討を注視することが必要と考えられる。

参考資料 1: 放射性物質のセキュリティに関する調査委員会名簿

平成 26 年度放射性物質のセキュリティに関する調査事業
委員名簿

平成 27 年 3 月 31 日現在
(敬称略 50 音順)

| グループ員 | 所属 |
|---------------------|--|
| いいた とおる 飯田 透 | 独立行政法人日本原子力研究開発機構 安全・核セキュリティ統括部 核セキュリティ・保障措置課 課長 |
| いがうえ としゆき 伊賀上 利幸 | 日本原子力防護システム株式会社 安全防護事業部 部長 |
| きむら としお 木村 俊夫 | 公益社団法人日本アイソトープ協会事業推進本部技術部 部長 |
| しみず きくお 清水 喜久雄 | 大阪大学ラジオアイソトープ総合センター准教授 |
| どい えいし 土肥 英司 | 日本核燃料開発株式会社社長補佐 |
| もりかわ やすまさ 森川 康昌 | 富士フイルム RI ファーマ株式会社 千葉工場 工場長代理 日本放射性医薬品協会 流通委員会 委員長 |
| わたなべ ひろし 渡邊 浩 | 独立行政法人労働者健康福祉機構 横浜労災病院 中央放射線部 主任診療放射線技師 日本放射線公衆安全学会 副会長 日本核医学学会 理事 日本核医学技術学会 理事長 |

参考資料 2: NUREG-2166「放射性物質防護のための実践ガイド」の概要

1. はじめに

本実践ガイド^{viii}は、米国原子力規制委員会（U.S.NRC）の規則 10 CFR Part 37「区分 1 及び区分 2 量の放射性物質の防護」における要件を満たすと考えられる方法を与えるとともに、NUREG-2155「10 CFR Part 37 実施ガイド^{ix}」を補足するものである。

本実践ガイドは全 157 頁で、本文（75 頁）と付録（66 頁）から成り、本文では防護の重要事項について解説がなされ、付録では主として放射性物質の具体的な使用法について、防護の具体的な実践例が示されている。

^{viii} NUREG-2166, Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material, U.S.NRC, May 2014

^{ix} NUREG-2155, Implementation Guidance for 10 CFR Part 37, “Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material”, U.S.NRC, Feb. 2013（平成25年度調査済み、10 CFR Part 37のQ&A方式逐条解説） 概要は次のとおり。

- 防護対象：区分 1 または区分 2
- アクセス規制：エスコート無しアクセスを必要とする業務任務を持つ者のみ。審査担当者がエスコート無しアクセスを可能とする信用性および信頼性を決定。素姓調査としては犯罪履歴、本人確認、雇用履歴、学歴、性格および評判。
- 物理的防護要件：
 - ✓ セキュリティプログラム：セキュリティ計画（方策および戦略を記述、セキュリティ資源、設備および技術を同定）、実施手順、訓練。
 - ✓ 地域警察との協調：武装対応を含めて実行可能な程度に協調。
 - ✓ セキュリティゾーン：連続複数の物理的バリア、直接規制、物理的バリアと直接規制の組合せ。
 - ✓ モニタリング、検知および評価：モニタリングと検知、要員通信連絡とデータ伝送、対応。
 - ✓ 保守および試験：侵入警報器、付随通信連絡システム、およびシステムのその物理的機器。
 - ✓ 移動式装置に対する要件：直接管理および常時監視下でない場合、実際的なバリアを形成する二つの独立した物理的な規制を設ける。
 - ✓ セキュリティプログラム見直し：定期的（少なくとも毎年）。
 - ✓ 事案の報告：盗取、妨害破壊行為または横流しを地域警察、NRC へ通報。

2. 本文の概要

本文は、6章で構成され、第1章「本ガイドの目的」に続いて、

- 第2章「効果的な防護プログラム」で、防護プログラムの目的設定（施設の概要、ターゲットの特定および脅威の特定）と防護プログラムの主要要素（アクセス承認、アクセス規制、検知、遅延、評価、対応）について、
- 第3章「管理的セキュリティ対策」で、アクセス承認手続き（素姓調査、信頼性決定、アクセス管理）、セキュリティ計画、セキュリティ手順、情報防護、セキュリティ訓練、保守試験プログラム、不測事態計画、および対応計画と調整について、
- 第4章「全施設に適用するセキュリティ実践」で、セキュリティゾーンの決定（連続障壁、壁・床および天井、ドア・窓その他の開口部、錠および施錠システム、アクセス規制）、セキュリティゾーンの監視（侵入検知器/装置、警報と表示、および非常用電源）、警報評価と対応（ビデオ評価、対応と連絡）について、

具体的な例を挙げて、解説している。

本文の第5章「放射性物質を含む移動式装置と放射性物質の輸送に対するセキュリティ実践」では、車両警報と不動化システム、車両と梱包物の追跡システム、錠と施錠システム、および連絡と対応について説明している。第6章には参照文献がリストされている。

3. 付録の概要

本ガイドには、A～Iの9つの文書が本文を補足するために付けられている。

付録A「セキュリティ計画の策定」（全15頁）では、10 CFR Part 37が求めるセキュリティ計画の記述内容について、項目ごとに具体的に説明している。付録I「グローバル脅威低減構想プログラム（GTRI）」では、放射性物質がテロ行為に使われることを防止するためのセキュリティ強化策として進められている各種の活動について説明している。

付録のBからHには、放射性物質の具体的な使用法毎のセキュリティ実践について説明している。

- 付録B「展開式および水中型照射装置」
- 付録C「自己遮蔽型照射装置」
- 付録D「固定式ゲージ」
- 付録E「医療装置」
- 付録F「製造・頒布施設」
- 付録G「検層用線源」
- 付録H「工業用放射線検査線源」

これら装置等の防護についての説明の概要は別添のとおり。

放射性物質の具体的な使用法毎のセキュリティ実践

B. 展開式および水中型照射装置

★ 防護上の特徴

主として滅菌に用いられるこの種の装置では、線源がコンクリ・鉛製のコンテナもしくは水中に貯蔵され、照射時に所定位置に引き出される（水中型の場合、線源は常時、水中にある）。線源近傍の線量率は短時間（数秒から数分）で行動不能になるほど高いから、使用中のこれら装置の線源は自己防護的（self-protecting）であると考えられる。従って、これら装置の防護の目標は、線源が貯蔵されている場合に、個別の線源棒の不正持ち出しを防止することである。

B. 1 アクセス規制

これらの装置は昼夜連続使用が普通であるから、承認された者（即ち、信頼性が決定されている者）のみがセキュリティゾーン（制御室、貯蔵庫）にアクセス可能とするアクセス規制対策が講じられなければならない。

- 正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 内部脅威対策としての、主セキュリティシステムとは分離独立した警報・アクセス規制システム。
- セキュリティゾーンへの付添い無しアクセスは、業務上必要で、かつ信頼性が決定されている者に限定。
- 最低 2 種類の個人認証（例えば、キーカードと個人識別番号または生体認証）を用いたアクセス規制システムの使用。
- セキュリティゾーン内での線源の使用と貯蔵以外の行為（例えば、照射済み製品の保管）の禁止（可能な場合）。
- 付添い無しアクセスが必要でなくなった者が出た場合における、アクセス・警報コードの即時停止または変更。
- セキュリティ錠の使用と、緊急避難出口等の外側開閉金具の取り外し（防火対策上許容される場合）。
- 装置運転や貯蔵庫開放用鍵の不使用时、厳重保管。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器（例えば、フォークリフト、クレーン）の厳重管理。

B. 2 不正アクセス検知

- セキュリティゾーンを取り囲む検知器の取付け（制御室への全ての出入り口、製

品の出し入れ口)

- 高性能検知器の使用（銀行等で使用されるのと同等のもの）
- 警報表示盤や無停電源などを設置するセキュリティ機器室や通信連絡室の嚴重警備と、必要とする者へのアクセス許可。
- 少なくとも 2 種類のモーションセンサー（赤外線とマイクロ波）と、誤報防止のための発報（AND）ロジックの使用。
- 照射室内での耐放射線センサー、機器の使用。貯蔵庫への立ち入りを検知するためのセキュリティゾーン内でのカメラの使用（照射室外）。
- 故障による不作動対策としての最少 2 個のセンサーの取付け。
- 警報システムへのバックアップ電池または無停電電源の使用（最低 2 時間。長期停電のための対策も）。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- 制御室および貯蔵庫周辺から緊急信号を発信するための押しボタンの設置。
- 貯蔵庫からの線源の持ち出しを検知するための放射線検出器の設置（貯蔵庫出入り口）。内部者対策として、同検出器は常時作動とし、監視所へ独立に信号/警報を送るべき。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 内部者対策としての、検知器と監視所間での監視信号線、連続監視検知器不正工作スイッチの使用。
- 警報関係システムの定期試験と保守。

B. 3 警報評価

- 対応の必要性を確認するための、不正アクセスの即時評価。
- 各検知器のゾーンをカバーするビデオカメラ（CCTV、IP カメラ、ビデオ画像）の評価機能の提供。
- 目視評価は暫定措置に限定（ビデオ評価システム不作動時）。武装あるいは暴力的侵入への対応訓練を含む、警報評価について訓練された者による目視評価。
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- ビデオシステムの品質はビデオ画像から得たい情報に依存するが、カメラは装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つべき。高品質ビデオシステムは入手可能であり、証拠として使える。
- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。

- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）を区別する方法は対応活動を調整するのに有用。

B. 4 対応

- 地域警察（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- 施設は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有すべきで、連絡装置は制御パネルと貯蔵庫内に配置。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

C. 自己遮蔽型照射装置

★ 防護上の特徴

この装置は、固体（鉛）構造の容器に完全に収納され、かつ、常に遮へいされている密封線源を用いているので、本質的に安全で、遮へいのない部屋の中で保管することが出来る。通常、病院、血液銀行、大学、研究所等に置かれ、研究試料、小動物、血液などの照射に使われている。

C. 1 アクセス規制

- セキュリティゾーン（装置が置かれている部屋）へのアクセスを限定するため、正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 障壁の壁は丈夫な構造で、不正侵入を遅延。障壁の窓（ドアの窓も）は装置が直接見えず、かつ、強化ガラス（遅延効果のある網目入りセキュリティガラス）製。
- 内部脅威対策としての、主セキュリティシステムとは分離独立した警報・アクセス規制システム。
- セキュリティゾーンへの付添い無しアクセスは、業務上必要で、かつ信頼性が決

定されている者に限定。

- 鍵およびキーカードの紛失に備えて、最低 2 種類(キーカードと個人識別番号(PIN)または生体認証)の認証方式を持つアクセス規制システム。
- セキュリティゾーン内での装置の使用と貯蔵以外の行為(例えば、装置使用以外の研究)の禁止(可能な場合)。
- セキュリティ錠の使用と、緊急避難出口等の外側開閉金具の取り外し(防火対策上許容される場合)。
- 装置運転鍵の不使用时、厳重保管。
- 緊急通報機能付きのアクセス規制・警報システム。緊急ドア開放と通報。
- 付添者に指名されている者への指導と定期的試験(信頼できるかどうか)。訓練。
- 付添い無しアクセスが必要でなくなった者が出た場合における、アクセス・警報コードの停止または変更。
- 付添い無しアクセスが認められている者と、そうでない者の明確な見分け法(色別または特別バッジの使用)。
- 装置の場所に特別な注意を引かないように、照射装置室のドアに「注意!放射性物質」を掲示しない(装置から 30 センチ離れて 5 ミリレム以下の密封線源は、注意掲示不要(10 CFR 20.1903))。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器(例えば、フォークリフト、クレーン)の厳重管理。

C. 2 不正アクセス検知

- セキュリティゾーンへの全てのアクセスポイントにおける、全ての不正立入の遅滞ない検知能力。多様方式の採用(ドアのマグネチックスイッチと照射装置室内のモーション検知器)。
- (装置または検知システムの不動作時での)暫定的または臨時的な人による直接規制および連続監視。
- 少なくとも 2 種類のモーションセンサー(赤外線とマイクロ波)と、誤報防止のための発報(AND)ロジックの使用。
- 高性能検知器の使用(銀行等で使用されるのと同等のもの)。
- 警報システムへのバックアップ電池または無停電電源の使用(最低 2 時間。長期停電のための対策も)。
- 故障による不作動対策としての最少 2 個のセンサーの取付け。
- 照射装置室ドアの長時間開放(不完全閉)警報。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。

- 照射装置室からの線源の持ち出しを検知するための放射線検出器と不正工作警報の設置。内部者対策として、同検出器は常時作動とし、監視所へ独立に信号/警報を送るべき。
- セキュリティゾーン警報は表示と吹鳴。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 内部者対策としての、検知器と監視所間での監視信号線、連続監視検知器不正工作スイッチの使用。
- 警報表示盤や無停電源などを設置するセキュリティ機器室や通信連絡室の嚴重警備と、必要とする者へのアクセス許可。
- 警報関係システムの定期試験と保守。

C. 3 警報評価

- 対応の必要性を確認するための、不正アクセスの即時評価。
- 各検知器のゾーンをカバーするビデオカメラ（CCTV、IP カメラ、ビデオ画像）の評価機能の提供。
- 目視評価は暫定措置に限定（ビデオ評価システム不作動時）。武装あるいは暴力的侵入への対応訓練を含む、警報評価について訓練された者による目視評価。
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- ビデオシステムの品質はビデオ画像から得たい情報に依存するが、カメラは装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つべき。高品質ビデオシステムは入手可能であり、証拠として使える。
- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）を区別する方法は対応活動を調整するのに有用。

C. 4 対応

- 地域法執行機関（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- 施設は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有すべき。

- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

D. 固定式ゲージ

★ 防護上の特徴

固定ゲージは紙、鉄板、フィルムなどの厚み、密度、容器やタンク内のレベル、配管中の液体流量などを測定するために、通常、配管や容器などにボルト止めされる。複数のゲージを使う場合、単一のゲージでは防護必要量にならなくても、集合量では防護必要量になることがある。個別に防護されているゲージや他の放射性物質は集合して防護する必要はない。セキュリティゾーンとしては、施錠できる部屋、ケージ、固定された金属覆いなどが考えられ、ゲージをケーブルや鎖で固定することも有効である。これらの障壁は一般的な工具では破壊されないことが重要であり、特殊工具は厳重に管理されるべきである。

D. 1 アクセス規制

- 正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 固定ゲージへ付添い無しでのアクセスは、信頼性が決定されており、かつ、アクセスが業務上必要な者に限定。
- 2 様式 of アクセス規制システム。例えば、電子キーカードと鍵。
- 線源を固定するための錠または鎖はセキュリティ用に特別設計のもの。鍵は厳重に管理。
- 取付け用の不正工作防止ボルトの特殊工具は厳重に管理。
- 内部者対策として、ツーパーソナルルールを適用するアクセス規制システムの採用。一人が電子キーカードを、他の者が鍵を使用。
- キーカードや鍵は管理が困難であるので、電子キーカードと、個人識別番号または生体認証を組み合わせることが有効（ツーフアクタ識別）。
- ある種の電子アクセス規制システムは、不正立入りを防止するのに有効。指定された時間（個別設定）だけにアクセスを限定。
- 要員の変更（雇用の終了）時の錠、キーカード、警報コード、パスワード等の速やかな変更または停止。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器（例えば、フォークリフ

ト、クレーン) の厳重管理。

D. 2 不正アクセス検知

- 固定ゲージがある部屋や建物が承認された者による管理または常時監視下でない場合、ゲージへの全てのアクセスポイントは、不正立入を遅滞なく検知すること。人員用ドアの検知器は、同じエリアへの車両機材搬入口に検知がなく、かつ同エリアにモーション検知器がない場合、有効ではない。
- 多重多様な複数の不正アクセス検知器の使用が望ましい。ドア用マグネチックスイッチとエリア内モーションセンサー（赤外、マイクロウェーブ）。信頼性向上と不正工作防止。
- 警報システムのキーパッドと通報連絡パネルは防護区域内に設置。
- 警報システムへのバックアップ電池または無停電電源の使用（最低 2 時間。長期停電のための対策も）。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- セキュリティゾーン警報は表示と吹鳴。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 固定ゲージ区域での緊急警報（警報コントロールパネルまたはアクセスコントロールパネルへの緊急コード）。
- 警報関係システムの定期試験と保守。

D. 3 警報評価

- 対応の必要性を確認するための、不正アクセスの即時評価。
- 承認された者が警報の評価を行う場合、悪意行為時に何を行うか訓練されていること（区域からの退去、緊急ボタンを押す、助けを呼ぶ）。
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- ビデオシステムの品質はビデオ画像から得たい情報に依存するが、カメラは装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つべき。高品質ビデオシステムは入手可能であり、証拠として使える。
- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーション

センサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。

- 緊急警報とその他の警報（強行立入警報）を区別する方法は対応活動を調整するのに有用。
- 固定ゲージはプロセスのレベルや流量のモニタリングに使われるので、プロセスコンピュータがゲージ信号の不具合を検知した場合、直ちに、それが機器の故障であり、ゲージまたはゲージの線源を持ち去ろうとする不正なアクセスによるものでないことを確認すべき。

D. 4 対応

- 所内のセキュリティ要員（居る場合）と LLEAs は、安全かつ効果的に対応出来るように施設の詳細情報、装置の線源の概要、その危険性を十分に知っているべき。
- 施設は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有し、施設内の各所に連絡装置を配置すべき。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

E. 医療装置

★ 防護上の特徴

放射性物質を含む医療装置はがん組織を殺したり、がんの大きさを小さくしたり、苦痛を和らげたりするのに使われる。遠隔治療装置は、患者の外にある強力な線源からの、がん組織に集中する高強度放射線ビームを使う医療装置の例で、ガンマナイフは脳深部に多数のコバルト線源からの放射線を集中させる。

E. 1 アクセス規制

- 正規のアクセスポイント以外の箇所からのセキュリティゾーン（制御室と処置室）への不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 障壁の壁は丈夫な構造で、不正侵入を遅延。障壁の窓（ドアの窓も）は、強化ガラス（遅延効果のある網目入りセキュリティガラス）製。
- セキュリティゾーンへの付添い無しアクセスは、業務上必要で、かつ信頼性が決定されている者に限定。
- 内部脅威対策としての、主セキュリティシステムとは分離独立した警報・アクセ

ス規制システム。

- 鍵およびキーカードの紛失に備えて、最低 2 種類(キーカードと個人識別番号(PIN)または生体認証)の認証方式を持つアクセス規制システム。
- セキュリティ錠の使用と、緊急避難出口等の外側開閉金具の取り外し(防火対策上許容される場合)。
- 付添い無しアクセスが必要でなくなった者が出た場合における、アクセス・警報コードの停止または変更。
- 付添い無しアクセスが認められている者と、そうでない者の明確な見分け法(色別または特別バッジの使用)。

E. 2 不正アクセス検知

- セキュリティゾーンへの全てのアクセスポイントにおける、全ての不正立入の遅滞ない検知能力。多様方式の採用(ドアのマグネチックスイッチと処置室および制御室内のモーション検知器)。
- 少なくとも 2 種類のモーションセンサー(赤外線とマイクロ波)と、誤報防止のための発報(AND)ロジックの使用。
- 警報システムへのバックアップ電池または無停電電源の使用(最低 2 時間。長期停電のための対策も)。
- 高性能検知器の使用(銀行等で使用されるのと同等のもの)
- 故障による不作動対策としての最少 2 個のセンサーの取付け。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- 医療装置からの線源の持ち出しを検知するための放射線検出器と不正工作警報の設置。内部者対策として、同検出器は常時作動とし、監視所へ独立に信号/警報を送るべき。
- セキュリティゾーン警報は表示と吹鳴。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 内部者対策としての、検知器と監視所間での監視信号線、連続監視検知器不正工作スイッチの使用。
- 警報表示盤や無停電源などを設置するセキュリティ機器室や通信連絡室の厳重警備と、必要とする者へのアクセス許可。
- 承認された者が処置室およびその周辺から緊急コード/警報を発するための緊急ボタン。緊急コードは、緊急時にアクセスドアを開放し、監視所に緊急伝言を送信。
- 医療装置の重要部分の遅延を増やしたり、強化することで、放射性物質を持ち出すために必要な時間が増え、地方法執行機関が対応出来る時間が増える。

- 最近のガンマナイフは Elekta と GTRI の協力で遅延効果を増やした製品が売られており、既存のものの遅延を増やすためのキットも検討されている。
- 警報関係システムの定期試験と保守。

E. 3 警報評価

- 対応の必要性を確認するための、不正アクセスの即時評価。
- 各検知器のゾーンをカバーするビデオカメラ（CCTV、IP カメラ、ビデオ画像）の評価機能の提供。
- 目視評価は暫定措置に限定（ビデオ評価システム不動作時）。武装あるいは暴力的侵入への対応訓練を含む、警報評価について訓練された者による目視評価。
- 処置室や共通作業区域からの出入り口を評価するが、処置室内へのカメラの設置には患者の秘密問題を避ける必要がある（管理上の問題）。
- ビデオシステムの品質はビデオ画像から得たい情報に依存するが、カメラは装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つべき。高品質ビデオシステムは入手可能であり、証拠として使える。
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- カメラは破壊防止容器に格納。カメラアングルの調節。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）を区別する方法は対応活動を調整するのに有用。

E. 4 対応

- 地域法執行機関（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- 施設は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有すべき。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時

には LLEA と調整すべき。

F. 製造・頒布施設

★ 防護上の特徴

これらの施設は放射性物質を製造・頒布するか、他が製造した物質を各種の装置等で使われる密封線源の形で頒布する。密封は、非密封状態で国内から受け取った物質を、ホットセルとマニピュレータを使って行われ、密封線源は特定の目的に使う者に頒布される。主な線源は Ir-192、Co-60、Cs-137、Am-241 である。

F. 1 アクセス規制

施設が無人の時でも不正アクセスを検知するアクセス規制対策が求められ、日々同時に設定される多くの臨時のセキュリティゾーンにも対応する必要がある。

- 密封線源が製造・保管される常設のセキュリティゾーンへのアクセスを限定するための、正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 常設のセキュリティゾーンから放射性物質を移動する時は、臨時のセキュリティゾーンを設定する必要がある、設定中は、物質への不正アクセスを避けるため信頼出来る者を配置する。
- セキュリティゾーンへのアクセスは、業務上必要で、かつ信頼性が決定されている者に限定。
- 製造・頒布施設では臨時のセキュリティゾーンが定常的に設定されるので、当該ゾーンへのアクセスが承認されていない者を直ちに見分けられる必要がある。例えば色違いのバッジの着用。
- 内部脅威対策としての、主セキュリティシステムとは分離独立した警報・アクセス規制システム。
- 常設のセキュリティゾーンでは、最低 2 種類の個人認証（例えば、キーカードと個人識別番号または生体認証）を用いたアクセス規制システムの使用。
- セキュリティ錠の使用と、緊急避難出口等の外側開閉金具の取り外し（防火対策上許容される場合）。
- 緊急通報機能付きのアクセス規制・警報システム。緊急ドア開放と通報。
- 付添い無しアクセスが必要でなくなった者が出た場合における、アクセス・警報コードの停止または変更。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器（例えば、フォークリフト、クレーン）の厳重管理。

F. 2 不正アクセス検知（常設のセキュリティゾーン）

- 常設のセキュリティゾーンへの全てのアクセスポイントでの不正立入りを遅滞なく検知する能力。多様方式の採用（ドアのマグネチックスイッチと製造・頒布室室内のモーション検知器）。
- 少なくとも 2 種類のモーションセンサー（赤外線とマイクロ波）と、誤報防止のための発報（AND）ロジックの使用。
- 高性能検知器の使用（銀行等で使用されるのと同等のもの）
- 警報表示盤や無停電源などを設置するセキュリティ機器室や通信連絡室の嚴重警備と、必要とする（信頼出来ると考えられる）者へのアクセス許可。
- 故障による不作動対策としての最少 2 個のセンサーの取付け。
- 警報システムへのバックアップ電池または無停電電源の使用（最低 2 時間。長期停電のための対策も）。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- セキュリティゾーンからの密封（非密封）線源の持ち出しを検知するための放射線検出器の設置。内部者対策として、同検出器は常時作動とし、監視所へ独立に信号/警報を送るべき。
- セキュリティゾーン警報は表示と吹鳴。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 警報表示盤や無停電源などを設置するセキュリティ機器室や通信連絡室の嚴重警備と、必要とする者へのアクセス許可。
- 内部者対策としての、検知器と監視所間での監視信号線、連続監視検知器不正工作スイッチの使用。
- 警報関係システムの定期試験と保守。

F. 3 警報評価

- 対応の必要性を確認するための、不正アクセスの即時評価。
- 各検知器のゾーンをカバーするビデオカメラ（CCTV、IP カメラ、ビデオ画像）の評価機能の提供。
- 目視評価は暫定措置に限定（ビデオ評価システム不作動時）。武装あるいは暴力的侵入への対応訓練を含む、警報評価について訓練された者による目視評価。
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- ビデオシステムの品質はビデオ画像から得たい情報に依存するが、カメラは装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つべき。高品質ビデオシステムは入手可能であり、証拠として使える。

- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）を区別する方法は対応活動を調整するのに有用。

F. 4 対応

- 地域法執行機関（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- 施設は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有し、施設内の各所に連絡装置を配置すべき。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

G. 検層用線源

★ 防護上の特徴

検層ではフィールドステーションまたはベースキャンプで保管する線源を現場へ運んで使うので、線源セキュリティ上の課題があり、単一の線源では防護が不要でも、複数が集積すると防護が必要な場合がある。

G. 1 フィールドステーションまたはベースキャンプでの線源保管

G. 1. 1 アクセス規制

- 正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 線源保管区域への付添い無しアクセスは規制され、アクセスが承認（信頼性が決定）され、かつ業務上アクセスの必要な者に限定。
- 線源を防護するための錠、鎖その他の金具類はセキュリティ用に特別に設計された物。

- ツーパーソナルールの採用。保管庫に対する電子式カードアクセスと通常鍵の使用。
- キーカードや鍵は管理が困難であるので、電子キーカードと、個人識別番号または生体認証を組み合わせることが有効（ツーフアクタ識別）。
- ある種の電子アクセス規制システムは、不正立入りを防止するのに有効。指定された時間（個別設定）だけにアクセスを限定。
- 要員の変更（配転、解任、解雇）時の錠、キーカード、警報コード、パスワード等の速やかな変更または停止。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器（例えば、フォークリフト、クレーン）の厳重管理。線源取扱い具や空輸送容器は線源とは離して管理。

G. 1. 2 不正アクセス検知

- 線源保管区域が承認された者による常時監視下でない場合、保管区域への全ての立入箇所への不正アクセスを遅延なく検知できること。多数の立入箇所がある場合、個々のドアへの検知器の他、区域内全体をカバーするモーション検知器。
- 多重多様な複数の不正アクセス検知器の使用が望ましい。ドア用マグネチックスイッチとエリア内モーションセンサー（赤外、マイクロウェーブ）。信頼性向上と不正工作防止。
- 警報システムのキーパッドと通報連絡パネルは、いつでも使い得るようにし、防護区域内に設置。
- 警報システムへのバックアップ電池または無停電電源の使用（最低 2 時間。長期停電のための対策も）。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- 警報を通知するためのサイレンと点滅装置の設置。施設運用上適切であれば、遠隔監視所。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 線源保管区域での緊急警報の使用。
- 警報関係システムの定期試験と保守。
- 保守と性能試験プログラムの策定。

G. 1. 3 警報評価

- 承認された者が警報評価する場合、悪意行為時に何を為すべきか訓練されるべき（退去、援助要請、緊急通報）
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしく

は、低照明下作動カメラ（赤外カメラ）の使用。

- 装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つカメラの使用。高品質ビデオシステムは入手可能であり、証拠として使える。
- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）の区別を可能とするプログラム。対応活動を調整する場合。

G. 1. 4 対応

- オンサイトのセキュリティ要員と地域法執行機関（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- フィールドステーションまたはベースキャンプは対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有すべき。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

G. 2 検層用線源の使用と輸送

G. 2. 1 アクセス規制

- 承認された者（信頼性が決定されている検層担当者）が検層線源へのアクセス規制に責任を持つ。セキュリティ手順と訓練。
- 業務上必要な者だけが線源と輸送車両にアクセスを限定。
- 直接の監視下でない場合、車両の不動化。ホイールロックや電子的不動化。種類によって遅延効果が違う。
- 車両上の線源を防護するための二つの独立した物理的方法。施錠された格納庫内の車両に固定された、施錠された輸送遮へい容器内に保管。

- 内部者対策としてツーパーソンルール。保管格納庫へのアクセスと、輸送容器へのアクセス。
- 錠や固定用の鎖は頑丈でセキュリティ用のもの。

G. 2. 2 不正アクセス検知

- 輸送中に承認された者の常時監視下でない場合、監視と不正アクセスを検知。車両警報システムでも良いが、現場で吹鳴するとともに、承認された者の呼出器や携帯電話と監視所に送信すべき。
- 車両（積荷）追跡装置。予定経路を外れると通報するタイプもある。

G. 2. 3 対応

- 必要に応じて、対応者を呼ぶための最低 2 種類の通信手段（無線と携帯電話）。
- 対応要請のための業務特有手順への習熟。対応または LLEA への支援要請のための現場セキュリティ要員も。

H. 工業用放射線検査線源

★ 防護上の特徴

主な放射性核種は Co-60 と Ir-192。Cf-252、Yb-169、Se-75 も。セキュリティ上は保管と移動が課題。単一の線源では防護が不要でも、複数が集積すると防護が必要な場合がある。

H. 1 許可された場所での線源保管

H. 1. 1 アクセス規制

- 正規のアクセスポイント以外の箇所からの不正アクセスを可能とする如何なる開口部も有しない連続障壁。
- 線源保管区域への付添い無しアクセスは規制され、アクセスが承認（信頼性が決定）され、かつ業務上アクセスの必要な者に限定。
- 線源を防護するための錠、鎖そのたの金具類はセキュリティ用に特別に設計された物。
- ツーパーソンルールの採用。保管区域に対する電子式カードアクセスと、装置を防護している鎖や保管庫の鍵の使用。
- ある種の電子アクセス規制システムは、不正立入りを防止するのに有効。指定された時間（個別設定）だけにアクセスを限定。
- 要員の変更（配転、解任、解雇）時の錠、キーカード、警報コード、パスワード等の速やかな変更または停止。
- 線源の持ち出しまたは取扱いに使われる可能性がある機器の厳重管理。線源取扱い具や空輸送容器は線源とは離して管理。

H. 1. 2 不正アクセス検知

- 線源保管区域が承認された者による常時監視下でない場合、保管区域への全ての立入箇所への不正アクセスを遅延なく検知できること。多数の立入箇所がある場合、個々のドアへの検知器の他、区域内全体をカバーするモーション検知器。
- 多重重多様な複数の不正アクセス検知器の使用が望ましい。ドア用マグネチックスイッチとエリア内モーションセンサー（赤外、マイクロウェーブ）。信頼性向上と不正工作防止。
- 警報システムのキーパッドと通報連絡パネルは、いつでも使い得るようにし、防護区域内に設置。
- 警報システムへのバックアップ電池または無停電電源の使用（最低 2 時間。長期停電のための対策も）。
- 所外監視所または防護された所内監視所による警報とビデオシステムの監視。所外監視所は公的機関により認可され、警報を受信し、状況を速やかに評価し、かつ対応部隊を派遣できること。
- 警報システムは、電源喪失または信号線断線時に警報を発報。
- 線源保管区域での緊急警報の使用。
- 警報関係システムの定期試験と保守。
- 保守と性能試験プログラムの策定。

H. 1. 3 警報評価

- 承認された者が警報評価する場合、悪意行為時に何を為すべきか訓練されるべき（退去、援助要請、緊急通報）
- CCTV、IP カメラ、ビデオ画像での確認の容易性を達成するための、照明もしくは、低照明下作動カメラ（赤外カメラ）の使用。
- 装置または線源への不正行為を示す明瞭な画像を監視所へ提供できるに十分な分解能を持つカメラの使用。
- カメラは破壊防止容器に格納。
- 警報とビデオ伝送線は不正工作検知付きで、切断・接触防止のため電線管で防護。
- ビデオ画像は防護された場所で記録。デジタルビデオレコーダー（DVR）で十分だが、大規模事業所ではネットワークビデオレコーダーが良い。旧式のビデオテープレコーダーは経時劣化があるので避けるべき。ある種の DVR は、モーションセンサーが動きを検知した場合だけ記録し、画像を数カ月間蓄積出来る。
- 緊急警報とその他の警報（強行立入警報）の区別を可能とするプログラム。対応活動を調整する場合。

H. 1. 4 対応

- オンサイトのセキュリティ要員と地域法執行機関（LLEAs）は適切に対応するため、施設、線源または装置、線源の潜在的危険性について十分な情報を有しているべき。
- 保管区域は対応部隊（LLEA）へ連絡する複数の手段（無線、地上電話、携帯電話）を有すべき。
- 対応部隊との連絡に通常の無線システムを使うのは、敵が盗聴すると想定して、本当に必要な場合で、かつ、地上電話や有線電話のようなより安全な手段が使えない場合だけに限定すべき。偽伝言を防ぐには、敵でなく対応部隊員による通信であることを確認する認証コードを使うべき。
- LLEA と定期的な警報対応試験を実施すべき。
- 少なくとも毎年、または、放射性物質の脆弱性を損なう施設設計と運用の変更時には LLEA と調整すべき。

H. 2 工業用放射線検査線源の使用と輸送

H. 2. 1 アクセス規制

- 承認された者（信頼性が決定されている放射線検査者）が検層線源へのアクセス規制に責任を持つ。セキュリティ手順と訓練。
- 業務上必要な者だけが線源と輸送車両にアクセスを限定。
- 直接の監視下でない場合、車両の不動化。ホイールロックや電子的不動化。種類によって遅延効果が違う。
- 車両上の線源を防護するための二つの独立した物理的方法。施錠された格納庫内の車両に固定された、施錠された輸送遮へい容器内に保管。
- 錠や固定用の鎖は頑丈でセキュリティ用のもの。

H. 2. 2 不正アクセス検知

- 輸送中に承認された者の常時監視下でない場合、監視と不正アクセスを検知。車両警報システムでも良いが、現場で吹鳴するとともに、承認された者の呼出器や携帯電話と監視所に送信すべき。
- 車両（積荷）追跡装置。予定経路を外れると通報するタイプもある。

H. 2. 3 対応

- 必要に応じて、対応者を呼ぶための最低 2 種類の通信手段（無線と携帯電話）。
- 対応要請のための業務特有手順への習熟。対応または LLEA への支援要請のための現場セキュリティ要員も。

参考資料 3: RD/GD-338 Security Measures for Sealed Sources

RD/GD-338

Security Measures for Sealed Sources

密封線源のセキュリティ方策

序文

密封線源のセキュリティ方策という規定文書 RD/GD-336 は、許可所有者が許可を受けた施設において保管している密封線源の紛失、妨害破壊行為、不法な使用、不法な所持又は不法な移転を防止するために履行すべき最低限の物理的セキュリティ方策を規定するものである。この中には、輸送中又は輸送途上での保管中である間の密封線源の紛失、妨害破壊行為、不法な使用、不法な所持又は不法な移転を防止するための方策が含まれている。

本文書は、また、輸送機器、輸送容器そしてセキュリティ計画などの最低限の物理的セキュリティ方策にどのように合致させるかの指針と情報を提供する。本文書はカナダ国内における道路運送に適用する。(危険品の海上輸送、航空輸送及び鉄道輸送にあっては他の安全輸送のための法令文書や技術文書がある)

2003年の9月に、IAEAは放射線源の安全とセキュリティに関する行動規範を承認した。カナダは、多くの他国とともに、本行動規範を遵守するよう取り組んできており、その完全履行に向けて努力してきた。RD/GD-338、密封線源のセキュリティ方策は、IAEAが定めた国際的指針施行のための法規制の枠組みを支持し、セキュリティ方策の適用における一貫性を提供するものである。

多くの運送事業者は CNSC による許可を得ていなく、輸送中又は輸送途上での密封線源の保管に当たって CNSC からの許可所有者に適用されるセキュリティ要求事項に従うものではない。本文書は、輸送請負事業者とともに許可所有者を支援することを意図するものであり、それにより密封線源輸送に当たって輸送中又は保管中に考慮すべき特定の物理的セキュリティ方策を確実にする。

RD/GD-338、密封線源のセキュリティ方策は、国連の専門の機関のセキュリティ目標と計画を反映している。—IMO、ICAO 及び鉄道国際貨物の様な政府間組織—は海上輸送、航空輸送、鉄道輸送における危険品輸送の改善されたセキュリティを提供している。これら組織は、国際危険品海上輸送規範、危険品航空輸送の安全輸送のための技術文書など様々

な規定を定めている。

本文書は密封線源（カプセルされている又は固体）に適用し、非密封線源には適用しない。本文書は区分1，2，3線源に適用し、区分4，5線源の優良事例を提供する。本文書において、区分1～5線源という用語はIAEA行動規範又は放射線源の区分分け（IAEA/TECDOC-1344）において定義されているものを用いる。

本文書に記載されていないからと言って、該当する要件からすべての許可所有者が解放されると解釈してはならない。適用される法令と許可の条件を特定し従うことは許可所有者の責務である。

Table of Contents

| | |
|---|----------|
| 1. Introduction..... | 1 |
| 1.1 Purpose | 1 |
| 1.2 Scope..... | 1 |
| 1.3 Relevant regulations | 1 |
| 1.4 National and international standards..... | 2 |
| 2. Background | 3 |
| 2.1 Application..... | 3 |
| 2.2 Categorization of sources..... | 3 |
| 2.2.1 Nuclear substances and thresholds for the activity levels..... | 4 |
| 2.2.2 Methodology for assigning a category..... | 6 |
| 3. Security Measures..... | 6 |
| 3.1 General security measures | 6 |
| 3.1.1 Requirements for general security measures | 6 |
| 3.1.2 Guidance for general security measures | 6 |
| 3.2 Technical security measures | 9 |
| 3.2.1 Requirements for technical security measures..... | 9 |
| 3.2.2 Access control..... | 9 |
| 3.2.3 Detection of unauthorized access..... | 10 |
| 3.2.4 Locking hardware and key control | 11 |
| 3.2.5 Physical barriers..... | 12 |
| 3.2.6 Alarm response protocol..... | 15 |
| 3.2.7 Inspection, maintenance and testing of security-related equipment | 16 |

| | | |
|-----------|--|-----------|
| 3.2.8 | Security officers..... | 16 |
| 3.3 | Administrative security measures | 17 |
| 3.3.1 | General requirements for administrative security measures | 17 |
| 3.3.2 | Site security plan..... | 17 |
| 3.3.3 | Security awareness program | 17 |
| 3.3.4 | Personal trustworthiness and reliability | 18 |
| 3.3.5 | Protection of prescribed and/or sensitive information | 19 |
| 3.3.6 | Inventory control..... | 20 |
| 4. | Security Measures for Sealed Sources during Transport | 21 |
| 4.1 | Vehicle security | 21 |
| 4.1.1 | Requirements for vehicle security | 21 |
| 4.1.2 | Guidance for vehicle security | 21 |
| 4.2 | Security measures for sealed sources during transport | 21 |
| 4.2.1 | Requirements for security measures for sealed sources during transport | 21 |
| 4.2.2 | Guidance for security measures for sealed sources during transport | 23 |
| 4.3 | Transport security plan | 23 |
| 4.3.1 | Requirements for the transport security plan | 23 |
| 4.3.2 | Guidance for the transport security plan..... | 24 |
| | Appendix A : Sample Site Security Plan..... | 27 |
| | Glossary | 31 |
| | References..... | 33 |
| | Additional Information | 35 |

Security Measures for Sealed Sources

密封線源のセキュリティ方策

1.序

1.1 目的

本規定文書は、許可所有者が許可された活動を行う施設において保管している密封線源が紛失、妨害破壊活動にあうこと、不法な使用、不法な所持、又は不法な移転を防止するために実施すべき最低限のセキュリティ方策を定めたものである。これはまた、輸送中又は輸送中に保管している間の紛失、妨害破壊活動にあうこと、不法な使用、不法な所持、又は不法な移転を防止するための方策も含まれている。

1.2 適用範囲

本文書は、技術的及び管理的物理セキュリティの両方の方策など、密封線源を保管するために求められる最低限のセキュリティ方策を述べている。密封線源が輸送中又は輸送途上で保管されている時に輸送事業者が合致する様に許可所有者が行うべき最低限のセキュリティ方策も定めている。輸送機器、輸送容器そしてセキュリティ計画に関する方策も含んでいる。

本文書はセキュリティ要求事項にどのように合致させるかの指針と情報を提供する。

本文書はカナダ国内のみの道路運送に適用する。(海上輸送、航空輸送そして鉄道輸送の危険品安全輸送を規制する多くの規定や技術文書がある。)

本文書は密封線源（カプセルに入っている又は固体）に適用し、非密封線源には適用しない。本文書は区分1，2，3の線源に適用し、区分4，5線源には優良事例を提供する。本文書において、区分1～5線源という用語は IAEA 行動規範又は放射線源の区分分けに定義されているものを用いる。

1.3 関係法令

原子力安全と規制法（NSCA）の以下の規定及び NSCA の基に作成される規則は本規定文書に関連する。

一般原子力安全と規制規則の第3条第1項(g)、(h)は、許可申請書には以下の情報が含まれるべきである。(g)許可された活動の施設、放射性物質、規定の機器又は規定の情報に対するアクセスを規制する方策、(h)放射性物質、規定の機器又は規定の情報の紛失、不正な使用、所持又は移転を防止する方策

一般原子力安全と規制規則の第 12 条第 1 項(c)、(g)、(h)、(j)では、「すべての許可所有者は以下の事を確実にしなければならない。

- (c) 環境及び人の健康と安全を防護するため、及び原子力施設及び放射性物質のセキュリティを維持するためのすべての合理的注意を払う。
- (g)放射性物質、規定の効き又は規定の情報の不法な使用又は不法移転、又は施設の不法な使用を防止するための許可使用者の対策を実施する。
- (h)許可された活動の場所のどこでも、妨害破壊発動又はその意図を許可所有者に対して警告する方策を実施する。
- (j)許可された活動を行う事業所での物理的セキュリティ計画及びその計画に基づく義務に関する作業を指し示す。

・一般原子力安全と規制規則第 21 条、22、23 条は、規定の情報及び人が規定情報を所持し、移動し、輸入、輸出し、使用又は公開することに関する詳細情報を提供する事を定めている。

・放射性物質及び放射線機器規則の第 36 条第 1 項(a),(d)は、すべての許可所有者は以下の記録を保持しなければならないと規定している。

(a) 許可証に記載されている許可所有者が所持しているすべての放射性物質に関する以下の情報の記録

放射性物質の核種、数量、物理的・化学的性状及び場所

密封線源の場合、線源の型式及び製造番号

放射線機器に装備されている場合は、機器の型式及び製造番号

使用している放射性物質の数量

放射性物質の使用方法

(d)各作業者が受けた訓練の記録

放射性物質の梱包と輸送規則第 17 条は、すべての放射性物質の荷主は IAEA 規則第 549 項に示す輸送物に関する情報を輸送に関する文書に記載しなければならない、それは明確に印字されていなければならない。

危険品輸送規則（カナダ国内輸送）は密封線源に適用される。

1.4 国内及び国際基準

本規制文書は密封線源の物理的セキュリティ方策のための最新の国内及び国際的指針と基準と一貫したものとなっている。密封線源の物理的セキュリティに関する出版物には以下のものがある。

- ・ IAEA 行動規範
- ・ IAEA 放射線源の区分分け

- ・ IAEA 放射性物質の安全輸送規則
- ・ IAEA 放射線源のセキュリティ（暫定版）
- ・ IAEA 核物質及び施設の物理的防護に関するハンドブック
- ・ IAEA 輸送中の放射性物質のセキュリティ
- ・ IAEA 放射性物質及び関連施設の核セキュリティ勧告

2.背景

密封線源及び放射性物質を装備する規定された機器は、原子力安全及び規制法（NSCA）及び NSCA により定められた規則により規制されている。

線源の輸送に関連する追加の規則には以下のものがある。

CNSC 放射性物質の梱包及び輸送規則

運輸省 危険品輸送規則

本文書は密封線源のセキュリティのために等級別手法を用いている。密封線源を区分 1～5 間での 5 等級に分けている。本文書は、環境及び人の健康と安全に重篤なリスクを有する密封線源（すなわち区分 1， 2， 3 線源）に適用する。区分 4， 5 線源は危険の度合いがもっとも少ないので、本書はこれら区分に対して慣行による慎重な管理を提供する。

2.1 適用

本規定文書は表 A に定める放射性物質の密封線源に適用する。これらの物質と閾値は行動規範を基礎としている。本規定文書の主目的は、防護されていない状態になった時に人の健康と安全及び環境に対して危険な放射線源を特定することにある。

IAEA TECDOC-1344 に述べられているように、一つの保管場所にいくつかの線源が集積したり、線源が近づいた場所で使用される行為がなされる時は、合計放射能が区分分けの目的では一つの線源の様に取り扱われる。

セキュリティ要求事項は、カナダ政府又は許可所有者により定められたリスクのレベル又は閾値、区分に整合したものであるべきである。移動使用及び携帯できる放射線源は、特定のセキュリティ要求事項を満たすことを確実にするために異なる取扱となること、それにより意図した使用がなされる事を許可するという点に注意がいる。

2.2 線源の区分分け

CNSC は IAEA/TECDOC-1344 において定義されている IAEA 線源区分に関する区分けを基にしている。この文書は、すべての放射線源は同じに扱うことができないと認識し、区分 1（かなり危険）～区分 5（危険ではない）の間での 5 つの線源区分を確立した。

IAEA 区分分けの方法論は世界中で受け入れられており、もっとも一般的に使用されている密封線源と放射線機器に付随しているリスクの区分の一定の手段を提供している。

密封線源と放射線機器は一つの場所で使用され（例えば、製造機器として使用される固定ゲージ）、又は異なる業務で使用（例えば、非破壊検査、土壌の携帯型水分密度計）され、移動使用されている。

区分 1 線源は CNSC により許可されたもっとも危険な密封線源である。人の健康と安全及び環境に対してもっとも多くのリスクを有しているため、区分 1 線源は常によく遮蔽され、よく管理された場所にある。がん治療用の Co-60 遠隔治療用線源と滅菌用 Co-60 線源などが例である。これら線源は遮蔽され安全な状態にある。

もっとも一般的な区分 2 線源の例は、工業用非破壊検査装置である。これら機器は携帯可能であり、パイプライン作業や圧力容器などで使用されている。

より多く使用されているものは、区分 3, 4 線源の固定又は携行型の放射線ゲージである。区分 3 線源はしばしば、パイプ、容器、10 年も過酷な環境で信頼性高く稼働している組み立てラインに固定されて使用される固定ゲージである。区分 4 線源は、道路建設に使用される土壌の水分密度計がある。

区分 5 線源はリスクが低い。残留農薬を計測する ECD、蛍光 X 線分析装置、低線量永久挿入用近接治療装置の例がある。区分 5 の線源のいくつかは CNSC の発行する許可を必要としないで使用できる。

表 A は、放射能で表した区分 1, 2, 3 の閾値を示す。

2.2.1 放射性物質と放射能で表した閾値

表 A に示されている放射性物質と閾値は IAEA 行動規範を基礎としている。これら閾値は、放射性物質の防護のための国内及び国際的要求事項の間の一貫性を提供している。

人の健康と安全及び環境に重篤な脅威を有するであろう 16 の核種を示している。照射済みの燃料及び MOX 燃料は、かなりの量の放射性物質を含んでいるがこのリストには入っていない。これらの物質は核セキュリティ規則により取り扱われている。

TBq 単位は、放射性物質が区分 1, 2, 3 であるか否かを決定するために正式に使用される測定単位である。多くの許可使用者が Bq の代わりに Ci を使用しているため、実用的な

意味で等価な Ci 数も示している。

IAEA RS-G-1.9 は行動規範を発展させた方法論を提供している。

これら規制要求事項は密封線源に対してのみ適用される。しかし、保管の適正さを考慮するときに非密封線源を考慮に入れて同等なセキュリティ要求事項を求める事が勧告されている。

Table A: 16 核種についての D 値表

(略)

2.2.2 区分分けの方法論

線源が非常に接近している場合は、区分を割り当てるために、一つの施設にあるすべての線源の合計放射能が区分毎に示されている数値と同じか大きいかがである。たとえば、

- ・ Co-60 の 555TBq までの遠隔治療用密封線源は区分 1 線源である (555 > 30)
- ・ Ir-192 2.5TBq の密封線源を装備した認定された非破壊検査用機器は区分 2 線源である
- ・ Ir-192 の 0.44TBq 未満の密封線源を装備した医療用高線量率近接治療装置は区分 3 線源である

セキュリティ規制の目的のために、一つの保管場所（又は使用場所）に線源が集合している場合は状況に応じた特別の線源区分を決定することを怠ることができない。線源の実際の放射能を合計し、表 A の区分を決定する事により行う事ができる。たとえば、Cs-137 0.19TBq を装備した工業用レベル計は区分 3 線源である。しかし、この線源が 6 台一つの許可された場所にある場合は、区分 2 線源として取り扱う事ができる。

3. セキュリティ対策

3.1 一般セキュリティ対策

3.1.1 一般セキュリティ対策のための要求事項

保管している間は、放射線源が不法な移転（盗難又は紛失）又は妨害破壊活動から防護するための技術的及び管理的セキュリティ対策を開発し履行しなければならない。

IAEA TECDOC-1355 に述べられている様に、これら対策は、工業安全確保、放射線防護対策及び放射線源の不法移転から防護するための必要なレベルを実施するために適切な設計など、安全とセキュリティ概念を統合したものとしなくてはならない。

3.1.2 一般セキュリティ対策のための指針

許可所有者は、密封線源が保管中又は輸送中に紛失、不法使用、不法所持、又は不法移転から防護するために設計された現存の物理的防護システムにおける脆弱性を決定するために、脅威及びリスク評価を開発し維持しなければならない。年に1回最新のものとする、脅威及びリスク評価は、特定の脅威に対処し、リスクを管理し、脆弱性を減少するための緩和セキュリティ方策を決定するために使用される。

表 B はセキュリティ計画を区分 1～5 に如何に適用するかの情報を提供している。

表 B: セキュリティレベルとセキュリティ目的

| セキュリティプログラム | 区分 1- 高いリスク | 区分 2-高いリスク | 区分 3- 中程度のリスク | 区分 4, 5- 低いリスク |
|-------------------|--|---|---|---|
| 施設セキュリティ計画 | <ul style="list-style-type: none"> 毎年最新のものとする又は施設に重要な変更があった時 規定の又は機微なものを分類し、適切に保管する 知っておくべき事に関する連絡 脅威が増加したときの方策を示す | | <ul style="list-style-type: none"> 定期的に最新なものにする又は施設の重要な変更があった時 規定の又は機微なものを分類し、適切に保管する 知っておくべき事に関する連絡 | <ul style="list-style-type: none"> 最良事例 |
| 周辺及び物理的バリア(第1防護線) | <ul style="list-style-type: none"> 線源を許可されていない者と分離し、即時の検知と敵対者が線源を移転する前に介入するための対応部隊に対して十分な遅延を与えるために、少なくとも二つの物理的バリアにより防護されるべきである | | | <ul style="list-style-type: none"> 線源は許可を得ないアクセスと移転に対して防護されるべきである。 |
| 保管のセキュリティ(第2防護線) | <ul style="list-style-type: none"> 良質の南京錠又は同等のセキュリティシステムにより安全になっている 少なくとも二つの侵入検知システムを備える 安全な容器は携帯型の工具で攻撃された時に耐える事ができるべきである | | <ul style="list-style-type: none"> 良質の南京錠又は同等のセキュリティシステムにより安全になっている 少なくとも一つの侵入検知システムを備えている | <ul style="list-style-type: none"> 安全な容器又は場所に保管すべき |
| 侵入検知システム | <ul style="list-style-type: none"> セキュリティ事象が発生したときに、検知し評価し、対応部隊と連絡するために、Operator 24/7 によりモニターされたULC承認のコントロール室に接続すべき、又は同等の機構。 | | | |
| アクセス規制 | <ul style="list-style-type: none"> 承認された者のみにアクセスが制限され 二人ルール(最適) 訪問者、学生、契約者は常にエスコートされるべき | <ul style="list-style-type: none"> 承認された者のみにアクセスが制限され 訪問者、学生、契約者は常にエスコートされるべき | <ul style="list-style-type: none"> 承認された者のみにアクセスが制限され 訪問者、学生、契約者は承認された使用者にエスコートされるべき | <ul style="list-style-type: none"> 線源は承認されていないアクセスと移転に対して防護されるべき |

| | | | |
|----------------|---|---|---|
| 輸送セキュリティ計画 | <ul style="list-style-type: none"> ・特別の輸送セキュリティ計画を開発しCNSCに検討と承認を受けるために提出すべき。 ・一般的な輸送セキュリティ計画を開発し維持すべき。 | <ul style="list-style-type: none"> ・最良実施 | <ul style="list-style-type: none"> ・線源は承認されていないアクセスと移転に対して防護されるべき |
| 対応計画 | <ul style="list-style-type: none"> ・特定の対応計画及び危機管理計画 ・地方の法執行機関との交流 ・効果的な対応までの時間 ・紛失や放射線源が関与する悪意ある行為が起こった時の手順を開発する | <ul style="list-style-type: none"> ・一般対応計画と危機管理計画 ・紛失や放射線源が関与する悪意ある行為が起こった時の手順を開発する | <ul style="list-style-type: none"> ・線源は承認されていないアクセスと移転に対して防護されるべき |
| 輸送車両のセキュリティ | <ul style="list-style-type: none"> ・車両機器は盗難防止装置又は動作停止装置、及び侵入検知システムを装備すべき、又は同等の方策 ・車両機器は放射線源の不法移転を防止するために少なくとも2つの技術的障壁を設けるべき ・アクセスは承認された者にのみ制限すべき ・GPS 又は追跡システム(最善) ・運転手は緊急時に連絡手段を有するべき ・二人ルール(最善) ・運転者及び操作者は信頼性確認を受けなければならない | <ul style="list-style-type: none"> ・車両機器は盗難防止装置又は動作停止装置、及び侵入検知システムを装備すべき、又は同等の方策 ・車両機器は放射線源の不法移転を防止するために少なくとも2つの技術的障壁を設けるべき | <ul style="list-style-type: none"> ・線源は承認されていないアクセスと移転に対して防護されるべき |
| 個人の信頼性確認又は身元調査 | <ul style="list-style-type: none"> ・犯罪者名簿照会 ・信用調査、教育及び職務歴調査 ・放射線源にエスコートなしにアクセスする運転手及び契約者(運送事業者)はこの照会をするべき | <ul style="list-style-type: none"> ・信用調査、教育及び職務歴調査 ・犯罪者名簿照会 | <ul style="list-style-type: none"> ・信用調査、教育及び職務歴調査 ・犯罪者名簿照会(最良事例) |
| 情報セキュリティ | <ul style="list-style-type: none"> ・すべての規定の情報は防護されるべきであり、知っておくべき事は共有されるべきである。 | | |
| 維持及びテスト | <ul style="list-style-type: none"> ・維持及びテストは少なくとも半年毎に実施しなければならない。その記録は保持されるべきである。 | | |
| セキュリティ認知計画 | <ul style="list-style-type: none"> ・すべての作業者は定期的にセキュリティ認知訓練を受けなければならない。 | | |

3.2 技術的セキュリティ方策

3.2.1 技術的セキュリティ方策の要求事項

放射線源、機器又は施設の技術的セキュリティ方策には以下の物理的方策は含まれるべきである。:

- ・承認されていない者がこれら線源にアクセスすることを防止
- ・承認されていない移転の行動又は意図から防護し；
- ・妨害破壊活動の行動又は意図から防護する。

技術的セキュリティ方策は、深層防護の原則及び検知、遅延及び対応の物理的防護システムの機能に従って設計された、ハード及びセキュリティシステムを含むべきである。

本節は以下の方策のためのセキュリティ要求事項を含む

- ・アクセス規制
- ・承認されていないアクセスの検知
- ・施錠のハード及び施錠管理
- ・物理的バリア（安全な容器、囲い物）
- ・警報対応手順
- ・物理的セキュリティに関する機器の検査、維持及びテスト
- ・警備員

上述の特定された分野ごとに、許可所有者は密封線源により示されるリスクのレベルに釣り合った適切なセキュリティ方策を定めなければならない。さらなる詳細は3.2.2から3.2.8に示す。

一般原子力安全及び規制規則の第3条第1項(g)及び(h)の裏付けとして、許可所有者はアクセス規制、物理的バリア、不正アクセスの検知、物理セキュリティに関する維持とテストについて許可申請書に詳細に記載したものを含めるべきである。

3.2.2 アクセス規制

3.2.2.1 アクセス規制のための要求事項

許可所有者は、アクセス規制方策（例えば、アクセスカードリーダー、PIシステム、手動又は電子施錠）を実施、又は常に密封線源を保管している区域には承認された者のみがアクセスすることを確実にするために警備員を用いる。

訪問者、施設メンテナンス要員など密封線源が保管されている区域にアクセスすることが求められる者は、許可所有者による信頼性確認が行われていない場合は、常にエスコートされるべきである。

3.2.2.2 アクセスコントロールの指針

密封線源へのアクセスコントロールを行うために、許可所有者は以下の事を行わなければならない。

- ・線源への承認されていないアクセスを防止
- ・日報、追跡可能なアクセス規制システムを用いて、安全な保管区域にアクセスするすべての人の記録を監視し維持する。
- ・手動で起動する施錠機器、南京錠、カードリーダー及び生体認証機器及び入域管理の使用により有効なアクセス管理方策の実施。
- ・他人へ渡したり、前の人に続いて入ったり受け入れがたい行為を防止する事を組み込んだアクセス規制方策を確実にする。
- ・アクセス規制システムを使用するときは PIN コードを割り当てる。
- ・もはやアクセスすることが必要となくなったら、直ちに個人のアクセス権限を削除する。
- ・システムデータベースの不正な妨害（コンピュータへの不法侵入やソフトの破壊など）を防止するために、管理システムやソフトへのアクセス権限を制限する。
- ・警報監視会社又は対応部署へ通知するために、線源保管場所の近くに脅迫状態通報伝達の方法を確立し、
- ・線源保管場所内の問題や侵入を近くの人に警告するために、保管区域の近くで動作する区域警報を備える。

セキュリティ計画には、セキュリティ事象への検知、遅延、対応のセキュリティ方策が含まれるべきである。

3.2.3 不正アクセスの検知

3.2.3.1 不正アクセスの検知のための要件

許可所有者は、不正アクセス又はその意図を時期を得て検知する方策を実施しなければならない。例えば；

- ・目視監視
- ・ビデオ評価警報
- ・検知機器
- ・保管記録、封印又は製造監視システムなどの改ざん指示機器（例えば、線源が存在している事を確実にするために、日々又は2回／週の検査）

移動使用する線源の場合、適切な連絡手段を有する作業員による継続的な目視監視は、1又は二重のバリアの代替えになるであろう。

侵入検知システムを使用するときは、以下の条件を満たすこと、

- ・密封線源保管区域への不正な侵入を直ちに検知する
- ・警報システムの誤動作又は機能を起こさせるといふいかなる改ざんも直ちに検知する
- ・侵入が検知された時、許可所有者のいる場所又は承認された監視ステーションに、管理された連絡方法を用いて、音声及び視覚の両方で継続的警報が発せられる。監視ステーションはカナダ基準委員会又は CNSC が受け入れられると考える他の承認機関により承認された物でな

なければならない。

- ・セキュリティシステムの継続的動作を確実にするために、継続的電源供給は定期的に試験されなければならない。

3.2.3.2 不正アクセス検知のための指針

不正アクセスを検知するために、警報システムは以下を満たさなければならない。

- ・侵入又は改ざん事象を検知したら直ちに動作する。
- ・承認された者が認知するまで警報状態が維持されている
- ・各保管施設にさらに区域を有する。
- ・迷惑又は誤動作が受け入れ可能な程度に低い
- ・UL 又は ULC により承認されている。

- ・許可所有者は、承認されていない人による改ざんに対して警報監視機器及び予備電源が防護されていること
- ・キー操作部は安全な環境下に設置され、改ざんから防護されていること。
- ・保管区域内に専用の警報区域を設け（他の警報区域を分離して）、承認された者にアクセスを限定する。
- ・警報が発せいられた記録に対する追跡監査を維持する

例えば、警報システムを設置している倉庫を有する非破壊検査会社を考えると、二つの区域設定は、一つ目の区域は倉庫であり二つ目は保管区域である。日中は、倉庫の警報システムは動作を止めているが、保管区域のセキュリティシステムは依然として動作しており、主システムとは独立して動作している。

3.2.4 施錠機器と施錠管理

3.2.4.1 施錠機器と施錠管理の要件

保管区域へのアクセス管理するアクセスカード、ドアの鍵は許可所有者により承認された者に制限されるべきである。

許可所有者は、施錠機器（電子的又は手動か）などのアクセス管理承認の記録を維持すべきである。これらの記録には、施錠機器又は組み合わせ数字が発行された個人の名前、及び発行日が含まれるべきである・

許可所有者は、効力が無くなったり、紛失、盗難又は不法に移動されたり、又は情報漏洩した、施錠機器、鍵、アクセスカード又は組み合わせ数字の交換、補修の方策を含む書面にした手順を作成し、維持しなければならない。

3.2.4.2 施錠機器及び施錠管理の指針

許可所有者は、効力が無くなったり、紛失、盗難又は不法に移動されたり、又は情報漏洩した、施錠機器、鍵、アクセスカード又は組み合わせ数字の交換、補修の方策を含む書面にした手順を作成し、維持しなければならない。

鍵が使用されるときは、許可所有者は以下に示す施錠管理方針を実施しなければならない；

- ・ 鍵を有する個人の数制限し
- ・ マスターキーの数制限し
- ・ 従業員の鍵複製を禁止し
- ・ 不正な鍵複製を防止するために専用の鍵又は特許を得ている鍵を用いる
- ・ もはやアクセスすることがなくなった従業員に鍵の返還を求める規定を含める
- ・ ブランクな鍵（合い鍵を作る前のブランクキー）は安全に保管されるべき

施錠管理のために、許可所有者は

- ・ 定期的に鍵又は鍵所持者の在庫量を見直しし
- ・ 記録に鍵又は鍵所持者の変更及び追加を記録し
- ・ 発行された鍵及び紛失又は盗難にあったと記録されている鍵の報告義務を維持する

組み合わせ式の鍵又は数字組み合わせの鍵は推奨されない。

従来型の鍵が使用されている場合は、それらは良質のものであるべきである。施錠管理手順は不正アクセスやセキュリティ侵害を防止するために設計されるべきである。施錠の切断を防止するために鍵は覆われているべきである。

3.2.5 物理的バリア

3.2.5.1 物理的バリアの要件

表 A に示す区分 3 の閾値未満の放射能である密封線源については、許可所有者は 3.2.3.1.1 節に示す安全な容器内に線源を保管しなければならない。

表 A の区分 1， 2， 3 の閾値を超える放射能である密封線源については、許可所有者は、密封線源への不法なアクセスを防止するため、又は対応部隊が必要な介入をすることができる十分な遅延を提供するために、少なくとも二つの異なる物理的バリアをもうけなければならない。

物理的バリアは安全な容器と他の安全な囲い物の結合であるべきである。

例えば；

- ・ 施錠され安全に密封線源を保管する許可所有者は、施錠され閉鎖された室の中の安全な場所に置き、その場所に容器を安全な状況にする。（床、壁又は輸送機器）
- ・ もう一つの方法として、施錠された金属製のかご又は他の適切な囲いで安全にする。
- ・ 許可所有者のアクセス規制された周辺は、第二番目も安全になった囲い又は内部の安全な容

器がある第一番目の安全な囲いにより提供される。

移動使用線源の場合、上述のセキュリティ方策を実施することは常に可能なものではない。そのような場合、他の形を提供することにより代替の方策を実施する。(適切な連絡手段を有する目視監視など)

3.2.5.1.1 安全な容器の要求事項

安全な容器には、ファイルキャビネット、金属製の箱、編み目のかごなどがある。

安全であると考えられる容器では、以下を満たすこと

- ・そこに安全に取り付けられている
- ・手で持って操作できる工具を用いた物理的攻撃に耐えられること
- ・手で持って操作できる工具を用いた不正の又は強制的な攻撃に耐えられる、鍵などが備えられている
- ・編み目のかごが用いられているときは、かごの編み目は10番ゲージより大きく拡張する金属メッシュであるべきである。

3.2.5.1.2 安全な囲いの要件

囲いには安全にすることができる室、建物又はかごが含まれる。安全と考えられる囲いでは、すべての外装は(壁、ドア及び窓など)手で持って操作できる道具を用いて物理的攻撃に耐えられ、出入り口はアクセスコントロール機器が備えられ、又は警備員により規制されているべきである。

線源の近くの内部区域にアクセスすることができる窓は、鉄格子(格子の間隔は15cm以下で無ければならない)、金属グリル、金属メッシュが広げられたもの、UL/ULCの承認を得たフィルムやガラスにより改善されているものが備えられるべきである。

放射性物質及び放射線機器が使用、所持又は保管される区域へアクセスできるドアは、誰もいない時も安全になっているべきである。ドアは中まで詰まった木製又は金属で覆われたものであるべきであり、等価な物質で強化されたフレームに取り付けられるべきである。

ドアは補修され良い状態に維持され、蝶番が外部に取り付けられている時は蝶番のピンが取れないようになっている。ドアのガラス及び大きな通気口は、セキュリティガラス又は鉄格子、金属グリル又は等価なものであるべきである。グリルは不正改造防止装置が備えられ安全であるべきである。

3.2.5.2 物理的バリアの指針

金網のフェンス、施錠されたドア、グリル付きの窓、石造の壁、地下の貯蔵所などの従来のバリアは放射性密封線源の貯蔵に一般的に使用されている。バリアは敵対者の目的との関係で考

慮されるべきである。

許可所有者は放射線源を防護するために多重の物理的バリアを実施すべきである。多重バリアは潜在的に個々のバリアを打破するために様々な道具を持って来る事を敵対者に強制するものであり、それにより敵対者に遅延をもたらし対応部隊に介入する時間を提供する。深層防護の概念の実施は、様々な道具や技能を求める事により敵対者の進行を面倒にする経路となるように異なる多重バリアをもうける事である。

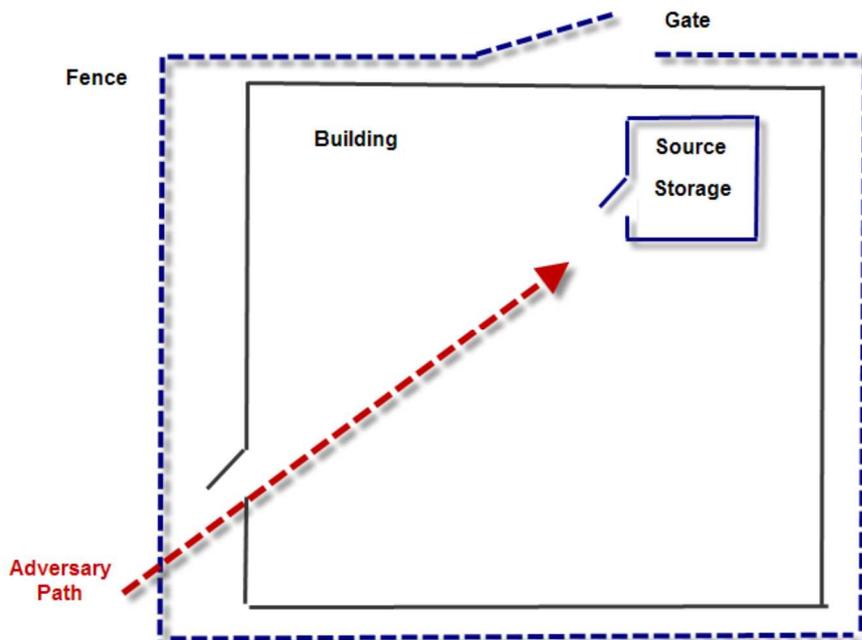


図 1: 貯蔵場所への敵対者の進路

例えば、多重防護には以下が含まれるべきである。

- ・携帯型機器（携帯型計測機器、照射装置など）は地下貯蔵所又は床にボルト固定されており一般的な攻撃道具に耐えうる能力があり安全に保管される
- ・移動できる機器（近接照射治療機器など）は保管区域内で床に縛り付けられている。鎖は一般的な攻撃道具に耐えられる材料でできており、同じレベルの強固さを有する南京錠で安全になっている
- ・中まで満たされている木製又は金属製のドアは、ドア蝶番のピンが抜けないようになっており、掛け金が保護されており、自動ドア閉鎖装置がある。
- ・住居侵入攻撃に耐えられる様にラミネートフィルムがついた、15cm 以下の隙間で金属メッシュ又は金属格子、及び移動できない様にされているねじがある窓

3.2.5.2.1 安全な容器の指針

保管場所及び容器は以下を満たすべきである

- ・施錠機器又は不正な移転を防止するための他の方策により安全であり

- ・不在時でも安全であり
- ・不正なアクセスや入室を検知するための警報システムが備えられている
- ・一般的な攻撃道具（大きなハンマー、バール、ドリル、ブローーチ）に耐える十分な強固さがある。

3.2.5.2.2 安全な囲いの指針

開口部、窓又は排気ダクト、で安全な囲いにアクセスできるものは、バー、金属製グリル、金属のメッシュが備えられている、及び又は UL/ULC の承認を得たセキュリティフィルム又はガラスで改善されているべきである。窓に取り付けられたハードは内部から取り付けるべきであり、外部から取り付けられている時は改ざん防止アンカーで取り付けられるべきである。

密封線源又は放射線機器が使用、措置、保管されている区域へのアクセスできるドアは、不在時に安全であるべきである。ドアに用いられる材料は中が詰まった木製又は金属で覆われているべきであり、同等の材料で補強されたフレームに付けられるべきである。ドアは補修され良い状態であるべきである。もし蝶番が安全では無い側に付けられている時は、ピンを抜くことができない蝶番を用いるべきである。ドアのガラスや排気口は安全ガラスや金属格子、金属グリル又は同等なものが備えられているべきである。グリルは改造防止アンカーで安全になっているべきである。

継続的な目視監視が作業者により行われる時は、作業者は連絡手段を有しており、不正アクセスや移転の事象が起こった時に対応部隊に速やかに連絡する対応手順を知っているべきである。

侵入検知システムの動作、動作解除にキーパッドが使用されている場合は、機器と電氣的結合ボックスは、改造のリスクを低減するために安全な区域に設置されるべきである。

初期電源喪失時に警報監視システムへの継続的電源を維持するために、許可所有者は検知能力を維持するために、代替え又は予備電源バックアップ又は同等のものを考慮すべきである。

3.2.6 警報への対応手順

3.2.6.1 警報への対応手順の要件

許可所有者は放射性物質又は放射線機器への盗難、転用又は妨害破壊行為の意図又は実施に対して直ちに対応すべきである。

許可所有者は、警報の起こった時及び解除の記録についての文書化された警報対応手順を作成し維持しなければならない。この手順には許可所有者の対応部隊及び施設外の対応部隊の責務と役割が含まれるべきであり、危機管理計画又は同等な文書に文書化されるべきである。

許可所有者は、管轄の地方警察に届け出て、密封線源が施設にあるということを情報提供すべ

きであり、これには施設の見学も含まれる。許可所有者は施設外の緊急時対応部隊への文書化された準備を作成し維持すべきであり、施設のデザインが変更され又は線源の潜在的脆弱性に影響しそうな施設の設計や作業が変更された時又は年次で見直しをすべきである。文書化された準備は一時的作業場所には適用されない。

3.2.6.2 警報への対応手順についての指針

許可所有者は、以下を含む文書化された警報への対応手順を作成し維持しなければならない。

- ・ 密封線源の盗難、紛失、妨害破壊が起こった時の対応手順
- ・ 許可所有者の職員の役割及び対応
- ・ 地方の法執行機関及び当てはまる官署への連絡準備
- ・ 事象の報告、届け出
- ・ 規制が回復された線源の即時の報告

地方の法執行機関、又は他の施設との相互協力協定の準備を推奨するために、許可所有者は覚え書きのような書面の支援協定を考慮すべきである。この準備された書面は、施設内の守衛と施設内にいる法執行機関の職員との間の関係を詳述すべきである。

3.2.7 セキュリティに関する機器の検査、維持、テスト

3.2.7.1 セキュリティに関する機器の検査、維持及びテストの要件

許可使用者は、物理的セキュリティ機器のテスト、定期的テストの予定、製造者の仕様に従った維持管理のための文書化された手順を作成し維持しなければならない。最低限、侵入検知機器などのセキュリティ機器のテストは6月毎に実施しなければならない。許可所有者は警報試験が実施されている事を証明しなければならない。予防的維持管理手順には、時期を得て欠陥のある機器を交換する方策を含むべきである。

3.2.7.2 セキュリティに関する機器の検査、維持管理及びテストの指針

すべての検知機器は、製造者の仕様書及び許可所有者の手順書に従って、設置され、動作し、維持管理されなければならない。許可所有者は、信頼性を確実にし文書化された記録を維持するために、定期的に検知機器の性能試験をしなければならない。

許可所有者は、検知機器の不良を追跡する予防的維持計画により信頼性を確保しなければならない。機器が補修や交換となる様な動作をしないときは、代替え措置が行われるべきである。

3.2.8 警備員

3.2.8.1 警備員の要求事項

許可所有者が警備保障サービスを使うときは、許可所有者は、以下の事項について文書化された手順書と指示書を作成し維持しなければならない。

- ・ 許可された区域へのアクセス規制のための方策

- ・ 徒歩又は車両機器によるパトロールでの監視
- ・ 警報の評価と対応
- ・ 武装していない侵入者の留置と逮捕
- ・ 武装している侵入者などの疑わしい活動を所轄の警察へ報告する。
- ・ セキュリティ機器の動作方法
- ・ 割り当てられた義務に関するセキュリティ訓練

3.2.8.2 警備員についての指針

警備員は適切に訓練され能力が備わっている。警備員に特定された正式な訓練計画が確立しているべきである。訓練計画には以下が含まれるべきである。

- ・ 地方の法令の要件（適用される場合）
- ・ 法令と官署
- ・ 施設の知識
- ・ 役割、責務及び機能
- ・ 緊急時放射線防護手順、対応手順
- ・ 応急措置訓練

警備員は信頼性確認プログラムに従って選抜されるべきであり、地方の官署による認定証又は有効な免許を有するべきである。許可所有者は施設内対応部隊の準備を確認するために、定期的に練習を実施すべきである。

警備員に対して、許可所有者は、長期の品質維持及び業務遂行のために求められる能力及び安全とセキュリティの重要な役割を認識するという目標への訓練という事を基礎とする、全体的な訓練方針と最初と継続の訓練計画を確立し維持すべきである。

3.3 管理的セキュリティ方策

3.3.1 管理的セキュリティ方策のための一般的要求事項

管理的セキュリティ方策は技術方策を支援する、そして不法移転及び妨害破壊行為から許可された放射性物質を安全にする事を支えるために許可所有者が実施すべき、計画、方針、手順、指示及び行為を含むべきである。

これらの方策には、これに限るものではないが、以下を含むべきである。

- ・ 事業所内セキュリティ計画
- ・ セキュリティ認知計画
- ・ 個人の信頼性確認
- ・ 規定された又は機微情報の防護
- ・ 在庫管理
- ・ アクセス規制手順

3.3.2 事業所内セキュリティ計画

3.3.2.1 事業所内セキュリティ計画の要求事項

区分1，2，3線源に対して、技術的及び管理的方策は、事業所内セキュリティ計画の中に許可所有者により文書化されるべきである。事業所内セキュリティ計画は、許可された施設の変更に対処するために、少なくとも1年に1回許可所有者によって確認され最新のものとすべきである。

3.3.2.2 セキュリティ計画のための指針

事業者内セキュリティ計画の指針

事業所内セキュリティ計画及びひな形に関する情報として、付録A「事業所内セキュリティ計画の例」を参照してください。

3.3.3 セキュリティ教育計画

3.3.3.1 セキュリティ意識向上プログラムのための要求事項

許可所有者の場所で密封線源や指定された情報にアクセスすることを承認されたすべての者（修繕会社、契約者、建築物維持管理職員）は、施設の行為。セキュリティ方針、手順を教育させるべきである。教育及び訓練の記録はすべての作業員に対して維持されるべきである。セキュリティ教育計画は文書化されており許可所有者により毎年更新されるべきである。新規採用者に対する訓練及び再教育を実施する。

3.3.3.2 セキュリティ教育計画の指針

セキュリティ教育訓練は密封線源と指定された情報を防護するため、及び疑わしい事象やセキュリティ事象を報告することに関するセキュリティ行為、手順の指示を含むべきである。

最低限、セキュリティ教育計画は以下を確実にすべきである。

- ・職員はセキュリティに関する彼らの役割と責務の理解
- ・疑わしい活動を認識し報告するための職員の訓練、例えば
 - ・偽の身分証明書
 - ・疑わしい振る舞いを示す人
 - ・承認を得ないで警報を発する人
 - ・組織内で制服や資材が紛失又は盗難される
 - ・作業場で安全では無い振る舞い
- ・指定された又は機微情報の防護
- ・疑わしい活動を特定する活動又は個人又は契約者の行動の変更に関する方策の訓練

3.3.4 個人の信頼性確認

3.3.4.1 個人の信頼性確認のための要件

許可所有者は、許可所有者の場所にある密封線源又は指定された機微情報にアクセスすること

が必要な者、エスコートなしにアクセスできる保守会社の人を含めてすべての人の信頼性確認を実施しなければならない。業務として放射線源や機微情報にアクセスする人で、許可所有者により承認されていない者は、承認された者にエスコートされるべきである。

個人的確検査の性質と深さは放射性物質の区分を基礎とすべきである。

区分 1, 2, 3 線源について、許可所有者は、最低限以下の情報を確認すべきである。

a パスポートや他の組織の文書（運転免許証、健康保険証、出生証明書）と併せて個人特定をする。

b 個人の犯罪者の氏名検査の結果を示す、地方の警察サービスセンター又は **Canadian Police Information Center** から発せられた記録

c そこで 10 年以上雇用されていない者について、学歴を含めた職歴、及び専門資格

d 直近 5 年間の履歴が確認できないときは、可能な場合は、直近 5 年間の 1 年以上の居住している地区の CRNC からの信頼性確認に関する情報を収集する。

許可所有者は、現在の雇用者について少なくとも 2 年間は信頼性確認に関する文書を保持しなくてはならず、3.3.5 節に従って情報を防護しなくてはならない。

3.3.4.2 個人の信頼性確認についての指針

個人的確検査行為は、個人セキュリティ基準に基づかなければならない。

許可所有者が行う信頼性確認計画は、高いリスクを有する密封線源へエスコートなしにアクセスする個人が信頼でき、個人の健康と安全及びセキュリティの不合理的なリスクを有していない事を確実にすべきである。許可所有者は、申請により提出されたすべての文書の写しを維持しなければならない、組織的に照合している事を確実にしなければならない。信頼性確認計画は定期的に見直されなければならない。

信頼性確認計画は以下に適用される。

- ・ 区分 1, 2, 3 線源にエスコートなしにアクセスする個人
- ・ 区分 1 線源を輸送する車両機器ドライバー及び添乗者
- ・ 指定されたもの及び機微情報に業務としてアクセスする、又は区分 1 線源の取扱をする個人

3.3.5 指定された及び/又は機微情報の防護

3.3.5.1 指定された及び/又は機微情報の防護のための要求事項

許可所有者は、一般核セキュリティ及び規制規則の第 21 条から第 23 条に占められている指定された情報にアクセスすることを規制するため、及び規定の情報の紛失、不法な使用、不法な所持、不法な移転を防止するために、防護方策を提供しなければならない。この情報は知っておくべき事を基に管理されるべきである。

3.3.5.2 指定された及び又は機微情報の防護のための指針

指定された情報とは、一般原子力安全と規制規則第 21 条に定めるものをいう。

以下の情報は指定されるべきであり、防護される情報と考えられる

- ・施設セキュリティ計画、セキュリティに関する文書、セキュリティ対応計画、危機管理計画及び適用される場合は輸送セキュリティ計画
- ・線源の在庫、特定の場所、設備の略図及び性能試験などのセキュリティシステム
- ・脅威及びリスク評価 及び又は脆弱性評価

指定された及び又は機微情報は以下を満たすべきである

- ・不法な公開を防止し、不在時に安全である
- ・定められている業務を実施するために必要な情報のみその人に公開する
- ・移転や盗難を防止するように保管する

高い機密情報はハードメディア（ディスク、CD-ROM 又は USB）に保管すべきであるか、紙の形でのみ保管する。また、知っておくべき人だけがアクセスできる安全な場所に保管する。この情報は公開されている、又は適切に防護されていないネットワーク上に保管してはならない。

指定された又は機微情報について、許可所有者は以下を実施しなければならない。

- ・移動でき、安全にすることができるように、携帯できる機器を使用する（コンピュータ、外付けハードディスク、USB キー）
- ・パスワード又は暗号で防護された保管機器を使用する。及びサイバーセキュリティ手順により承認された使用者のみアクセスする。
- ・指定された情報を含む情報又は文書の機密性、利用可能性及び性能を防護する

指定された及び又は機微情報の移動又は送信については、

- ・文書の各ページの右上の端にセキュリティ区分分けを含むべきである
- ・文書又は関連する書類は郵便事業者により、又はファクシミリにより CNSC に提出する。
- ・これら情報の電子的送信（e-mail など）は、適切な技術を用いて暗号化されない限り受け入れられない。

もはや使われていない機微情報を含む指定された情報や文書は、破壊すると割り当てられたセキュリティ格付けに従って、細かく切り刻むか破壊されるべきである。

3.3.6 在庫管理

3.3.6.1 在庫管理のための要求事項

在庫管理の要求事項

許可所有者は、線源が安全であり変えられていない又は不正なアクセスが内又は不法移転が無

い事を確認するために、検知目的で定期的在庫確認を実施しなければならない。この在庫確認は核物質及び放射線機器規則第 36 条第 1 項(a)に従わなければならない。

3.3.6.2 在庫管理指針

操業者は彼らの責務の基で密封線源のリストを作成し維持しなければならない。在庫確認は検知方策の一部として使用することができる。定期の在庫確認は、線源が存在し改ざんされた事が無い事を確実にするための方策から成る。これらの方策は、線源が存在しているという物理的チェック、又は CCTV を用いた遠隔監視、又は封印の確認、又は他の改ざん検知装置が含まれる。在庫管理の手順は実施され、強固な確認手順であるべきである。

4. 輸送中の密封線源のためのセキュリティ方策

4.1 輸送車両のセキュリティ

4.1.1 輸送車両のセキュリティ要求事項

区分 1 線源の輸送では、輸送車両は以下を備えなければならない

- ・もし盗まれた場合、輸送車両を取り戻す事ができる輸送車両追跡装置
- ・継続的に監視する脅迫状態通報機器又は同等な機器；許可所有者は管轄の警察などの適切な対応部隊に通報するために、警告監視本部に指示しなければならない。

区分 1,2,3 線源のために、許可所有者の輸送車両は盗難防止装置を装備しなければならない。

盗難防止装置は以下で構成されるべきである

- ・輸送車両無効化装置（適切な鍵又は同等なものを使用しないで輸送車両が発進することを防止するための発進無効化装置）
- ・輸送車両がだれもいないとき、不法なアクセス又は輸送車両への攻撃を直ちに検知し、音又は可視的な刑法を発する機器。輸送車両の運転者は警報を聞いたり見たりすることができない場所にいる場合は、運転者は遠隔で警報機器を監視できること。

盗難防止装置は、輸送物を搭載している輸送車両が誰もいない時はいつでも運転者により手動で又は自動的に動作状態と成らなければならない。

輸送中に保管されている間は、輸送物は輸送車両の中の安全なコンテナ中又は物理的セキュリティ方策により防護されている場所に保管され、輸送物が誰もいない状態の時は継続的に監視されなければならない。

For Category 4 and 5 sources, the licensee shall implement prudent management practices by using effective access control and ensuring the security of radioactive material and devices at all times.

区分 4,5 線源のために、許可所有者は有効なアクセス規制及び放射性物質及び放射線機器の常

にセキュリティを確実にする事により慣行による慎重な管理を実施しなければならない。

4.1.2 車両セキュリティのための指針

区分 1,2,3 線源を輸送している間、許可所有者の輸送車両が誰もいない状態になった時、許可所有者は密封線源を実際に盗難する又は転用する又はその意図を直ちに検知、評価及び対応するための方策を有しなければならない。警報システムは期待に沿う方法です。有効な遅延をもたらす期待に沿う輸送車両無効化機器の例は、トレーラー連結器ロック、車輪止め装置、又はエンジンが動作しなくなる方法がある。

許可所有者は、同様な攻撃に耐えうる安全機構（鎖、鍵及び封印）など輸送車両を防護する第2の方法を確実にすべきである。

4.2 輸送中の密封線源のためのセキュリティ方策

4.2.1 輸送中の密封線源のためのセキュリティ方策のための要求事項

許可所有者は輸送中の密封線源の安全とセキュリティへの責務があるので、許可所有者は、承認された輸送事業者が輸送中又は輸送中に保管している間の密封線源のための物理的セキュリティ方策を提供する能力があることを確実にしなければならない。

放射性物質の梱包及び輸送規則で求められている様に、許可所有者は密封線源に関する適切な発送文書を輸送事業者を提供しなければならない。発送文書には密封線源のためのセキュリティ方策を述べた対応する記述を含めなければならない。1以上の区分の放射性核種が適用される場合は、適用される方策はもっとも厳しい区分を基にすべきである。

区分 1,2,3 線源を含む輸送物は輸送中及び輸送中の一時的保管中に不正アクセス、盗難又は不法移転から防護されるべきである。荷受人は追跡番号及び到着予定日時を含めて、いつ、どこから、誰が輸送物を移動するかを通知されるべきである。荷主である許可所有者は

1. 密封線源を含んでいる輸送容器は、安全なコンテナに格納されるべきである。

500kg 以上のパッケージは、それらの重量が故の、扱う障害により安全であると考えられる。安全なコンテナは他のパッケージング現存する規則により求められるラベルを付ける事により取って代わることはできません。

安全なコンテナは:

- a. 鋼、あるいは携帯型のツールによる物理的な攻撃に強い他の材料で作られるべきである。
- b. 携帯型のツールを使用して、攻撃に強いキー、コンビネーション南京錠あるいは同様のロック装置を装備しているべき。
- c. もし開放型輸送車両(例えば、後ろが開く 0.5 トンのトラック、フラットベッド・トラック)で輸送される時は、コンテナの無許可の移転を防ぐために、それは輸送車両に安全に据え付けられるべきである。

- d. 区分 3 (表 A を参照)未満の放射能レベルを装備した密封線源を含んでいる場合、輸送機器の安全にロックされたトランクあるいは他の積荷エリアに格納されるかもしれない
2. 輸送される間の途中下車中に、パッケージは、輸送車両(リスト・アイテム 1 に述べられていたように)、あるいは物理的セキュリティ手段(セクション 3 に述べられていたように)によって保護される位置の中の安全なコンテナに格納されるものとします。
3. 輸送車両運転者は、いかなる時も、信頼できる移動通信能力(例えば携帯電話)、連絡窓口のリスト、および緊急事態の場合のそれらの連絡番号を持つべきである。

上述と同等の物理的セキュリティレベルを提供する代替の方法は、検討のために CNSC に提出され、又は許可申請書や変更許可申請書に定める事ができる。

区分 1 あるいは 2 の線源又は装置の輸送のために、許可所有者は次のことを確認しなければならない。輸送事業者が:

- * パッケージ・トラッキング・システムを使用します
- * ドライバーの信頼性および信頼度を確実にする方法を実施している
- * 通過の間に一定のコントロールおよび(または)監視を維持します。
- * 即時のコミュニケーションが適切な対応部隊あるいは援助を呼び出す能力を持っています。

カテゴリー 3 線源の輸送のために、許可所有者は次のことを確認すべきである。輸送事業者は:

- * ドライバーの信頼性および信頼度を確実にする方法を実施
- * 通過の間に一定のコントロールおよび(または)監視を維持します。
- * 即時のコミュニケーションが適切なレスポンスあるいは援助を呼び出す能力を持っています。

区分 4 と 5 線源の輸送のために、許可所有者は、有効なアクセスコントロールを使用し放射性物質と装置のセキュリティをいつでも確実にすることにより、慣行に基づく慎重な管理を実施すべき。

4.2.2 輸送中の密封線源のためのセキュリティ方策指針

許可所有者は以下のことをすべきです:

- * 求められた時の再教育トレーニングを含む、密封線源の取り扱いか輸送に従事していたすべての個人にセキュリティ意識トレーニングを提供する。
- * カテゴリー 1 と 2 線源を輸送する前に成功裡に密封線源を輸送する輸送事業者によって雇用された人がみな信頼性と信頼度のためのセキュリティ検査を終えたことを確認します

セキュリティ意識トレーニングは、次のものに関する輸送セキュリティ計画(セクション 4.3 を参照)および具体的情報のためにリストされたアイテムを含んでいるべきです:

- * 運搬車両の識別された脅威
- * 輸送の間にセキュリティ事象があった時に取られるセキュリティ上の問題およびアクション

許可所有者の輸送車両のセキュリティ装置は以下のことを満たすべきです:

- * それらの指定の機能に悪影響を及ぼす干渉または悪化のあらゆる表れのために許可所有者によって定期的に検査されます。
- * 6 か月ごとに許可所有者によって少なくともテストされます。
- * カテゴリー1 あるいは 2 線源を輸送するために使用される手段上のセキュリティ・メカニズムの完全を保証するために資格のあるオペレーターによって検査される

使用、あるいは通過中の線源については、そのような手段は安全になったか固定コンテナ、あるいは安全になった記憶エリア(例えば乗り物につながれたかボルトで締められたコンテナ)の内部の線源容器の配置を含んでいるかもしれません。

使用中のモバイルの線源については、常時の視覚的な監視は 1 つあるいは 2 つの物的障壁の代わりかもしれません。

通過(例えば倉庫中の)で間に、密封線源が一時的に格納される場合、カテゴリー1 と 2 つ線源の保管用に上に議論されたセキュリティ対策と一致している等価なセキュリティ対策が適用されるべきです。

容器が開放型の輸送車両で輸送される場合、容器は安全性とセキュリティのために遮蔽されに保護されるべきです。

4.3 輸送セキュリティ計画

4.3.1 輸送セキュリティ計画のための要求事項

セクション 4.2.1 の必要条件に加えて、次の必要条件がカテゴリー1 と 2 線源に適用されます。:

- * カテゴリー1 線源の輸送のために、許可所有者は増強されたセキュリティ対策を実施し、特定の輸送セキュリティを出荷の予定日時の 60 日前までに委員会法廷によって認可された委員会法廷あるいは指定のオフィサーによる承認のために CNSC に計画を提出する。
- * カテゴリー2 線源の輸送のために、許可所有者は増強されたセキュリティ対策を実施し、また総括的な輸送セキュリティを策定し実施し定期的に検討されるものとする。

輸送セキュリティ計画は脅威レベル、セキュリティの出来事へのレスポンス・プロトコルおよび敏感な情報の保護の変更に取り組むのに柔軟であるべきです。

カテゴリー1 線源については、輸送セキュリティ計画は次の情報を含んでいるものとします:

1. 名前、量、放射性物質の化学的/物理的特性
2. 許可所有者、荷送り人、輸送事業者の役割および責任
3. 輸送のモード
4. 提案されたセキュリティ対策
5. 出荷の位置をモニターするための方策。
6. 情報セキュリティに対する準備

7. 許可所有者、輸送事業者および荷受け人中に行われたコミュニケーション準備
8. 輸送路に沿った任意の警察機関と行われたコミュニケーション準備
9. 計画されたルート
10. 緊急の場合には使用される代替経路

4.3.2 輸送セキュリティ計画のための指針

(略)

付録 A:施設セキュリティ計画のサンプル

この付録は、事業所内セキュリティ計画[4]を策定する場合に考慮されるために題目のリストを提供します。

脅威とリスク評価はどんな潜在的な脅威および危険も識別し、事業所内で可能な脆弱性を明らかにします。事業所セキュリティ計画は、それらの脅威を緩和し、かつ危険と脆弱性を減らす/除去するために展開されています。事業所セキュリティ計画は、許可された設備で格納されるか、処理されるか、使用されるか、輸送される核物質を保護する物理的防護手段を含んでいます。

序文

- * 事業内容、建物勘定、従業員の数および位置を識別し概説します。
- * 核物質か放射線装置が使用されるか格納される場合、環境、建物および(または)設備の記述を含んでいます。

セキュリティ組織

- * 密封線源およびその使用の記述を含んでいます。
- * 建物の記述での公衆がアクセス可能な区域及びセキュリティーゾーン(制限区域)を識別します。
- * ルーチンおよび非ルーチン・オペレーション中にセキュリティー・プロトコルについて記述します。
- * 上級管理人員、およびスタッフ、およびセキュリティー(サイト・セキュリティ計画の維持として担当者を指定することを含む)に責任を負う人々の役割および責任を識別します。
- * 契約者あるいは雇用されたスタッフにセキュリティ準備の詳細を供給します。
- * 特にこれらが施設のセキュリティに対する責任に関係があるか含んでいるところで、設備のために管理準備の詳細を提供します。

セキュリティ・ポリシー

- * 企業セキュリティ・ポリシー(適用可能な場合)について記述します。
- * 裁判管轄上の警察と合意書(MOU)のコピーを含んでいます。

配置図

- * 図面、写真あるいはサイトの他の正確な実例を提供します。
- * 適切なフェンス・ライン、境界および設備をすべて含んでいます。
- * すべてのセキュリティシステムの位置を示します。
- * すべてのアクセスおよび退出ポイントの位置を示します。

周囲

- * 適切のように、含めて、周囲について記述する、フェンス、ゲート/障壁、ウィンドウ、セキュリティ照明、周囲侵入探知システム(PIDS)、有線テレビ・カメラ(CCTV)あるいは他の配置(受理または門衛詰所のような)の詳細
- * 歩行者、およびアクセスコントロール手段を含む車両の両方のためのサイトをアクセスと退出が指すことを説明します。

アクセスコントロール

- * 放射線源か、物質(つまり放射性物質への監督されていないアクセス権限を持った認定ユーザおよび人のリスト)にアクセスすることを認められる、サイト上の従業員の数を提供します。
- * アクセス・コントロール・システム(例えばカード読み取り機または押しボタン式ロック)、キーあるいはコード管理についての詳細および他の一般的なアクセスコントロール手続きを含んでいます。
- * 設備(例えば、政策を護衛する)にアクセスするビジターと契約者のプロセスについて記述します。
- * 武器と爆発物のための詳細、車両をふるいわけおよび探索を含んでいます。

内部者のセキュリティ

- * 放射線源が捜し出されるエリアに特有の評価装置(例えばカメラ)、アクセスコントロール、探知装置、遅延措置、レスポンスおよびコミュニケーションをテストするために情報を提供します。

保管

- * 核物質が使用されるか、格納されるか、輸送される建物、部屋あるいは位置(名前、数あるいは他の確認者による)のリストを提供します。
- * 各建物、部屋あるいは位置については、次のものについての詳細を含めてください:
- * 線源を含んでいる設備の保管のためのセキュリティ準備
- * 無許可の侵入あるいは(格納先への)設備を検知する手段
- * 許可された設備にアクセスする過程あるいは手続き
- * 核物質のタイプおよび分類

輸送

- * 放射性の密封線源の輸送に使用された車両のリストを提供します。
- * 次のものを含む密封線源の輸送のために適所にセキュリティ対策について記述してください：
 - * 線源が輸送されている間のセキュリティ準備
 - * 設備の無許可の移転を検知する手段
 - * 線源が輸送されている間のセキュリティ・プロセス

情報のセキュリティ

- * 位置、放射線源の性質、保管および移動に関する機微情報の保護のための準備について記述します。
- * セキュリティ(事業所内セキュリティ計画を含む)と関係する通信はすべて「PRESCRIBED INFORMATION」あるいは「SECURITY PROTECTED」とマークされます。また、そういうものとして、それは、一般的な原子力安全性および規制規則の(セクション、21~23)に準ずるように保護されるに違いありません。また、ラベルが付けられるに違いありません。
- * 規定された情報がインターネットに接続された会社サーバー上に格納される場合は、考察がITシステムからの潜在的な脅威および脆弱性に与えられることを確認してください。

信頼性と信頼度を決定する素性調査

- * 核物質にアクセスするスタッフの同一性および信頼度の確認のために準備について記述します。
- * 契約者あるいは建物保全要員を含む設備のためにセキュリティ保護を提供する人の同一性および信頼度の確認のために準備について記述します。

セキュリティシステムのメンテナンス、修理および試験

- * すべてのセキュリティシステムのメンテナンスおよび試験のための準備について記述します。
- * セキュリティシステムの補償の手段、性能試験および信頼度立証についての情報を含んでいます。
- * CNSC 期待(例えば半年ごとの試験)に従って計画を更新するために頻度を含むセキュリティ整備計画書の有効性を評価する過程について記述します。

危機管理とセキュリティのレスポンス計画

- * セキュリティ手続き、および放射性物質に関する紛失、窃盗、破壊、悪意に満ちた行為あるいは他のセキュリティの出来事に応答するセキュリティ対策をアドレスする指示についての詳細を提供します。
- * 緊急対策および出来事報告についての情報を含んでいます。
- * アラーム・レスポンス・プロトコルあるいは他のセキュリティの出来事のために離れた応答者(例えば警察)への協定について記述します。
- * 必要かもしれないあらゆる補償の手段についての詳細を備えた増加した脅威レベルをアドレ

スする手続きを含んでいます。

セキュリティ意識プログラム

- * セキュリティ意識プログラムについて記述します
- * セキュリティ対策上の従業員に与えられたどんな指示も含んでいます。
- * 放射性物質あるいは資料(契約者、建物保全要員および臨時従業員に対する制限を含む)のアクセス、使用、記憶装置あるいは輸送に関するどんな制限も含んでいます。

参照、手続きおよびセキュリティ指示

- * 現行規則(セキュリティと関係する任意の手続き)または標準への言及を含んでいます。

この印刷物は国等による環境物品等の調達に関する法律（グリーン購入法）に基づく基本方針の判断の基準を満たす紙を使用しています。