企 画 競 争 説 明 書

令和元年度

原子力規制委員会情報セキュリティ対策に係る

支援業務

原子力規制委員会原子力規制庁

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る
企画書募集要領

１　総則

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画競争の実施については、この要領に定める。

２　業務内容

本業務の内容は、（別添５）「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務の概要及び企画書作成事項」のとおりとする。

３　業務実施期間

契約締結日より令和２年３月３１日までとする。

４　予算額

業務の予算総額は、７，１００万円（消費税及び地方消費税額を含む。）以内とする。

５　参加資格

（１）　予算決算及び会計令（以下「予決令」という。）第７０条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別の理由がある場合に該当する。

（２）　予決令第７１条の規定に該当しない者であること。

（３）　原子力規制庁から指名停止措置が講じられている期間中でないこと。

（４）　令和０１・０２・０３年度（平成３１・３２・３３年度）環境省競争参加資格（全省庁統一資格）の「役務の提供等」の「調査・研究」又は「情報処理」において、企画書等の提出期限までに「Ａ」、「Ｂ」又は「Ｃ」の等級に格付されている者であること。

（５）　企画競争説明会に参加した者であること。

（６）　（別紙）において示す暴力団排除に関する誓約事項に誓約できる者であること。

（７）　環境省 CIO 補佐官、技術アドバイザー及びその支援スタッフ等（常時勤務を要しない官職を示す職員、「一般職の任期付職員の採用及び給与の特例に関する法律」（平成 12 年 11 月 27 日法律第 125 号）に規定する任期付職員及び「国と民間企業との間の人事交流に関する法律」（平成 12 年 12 月 22 日法律第 224 号）に基づき交流採用された職員を除く。）が現に属する又は過去 2 年間に属していた事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第

59 号）第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者などの緊密な利害関係を有する事業者ではないことを誓約できる者であること。

6　企画競争説明会の開催

（1）　日時

令和元年５月２９日（水）１４時３０分

（2）　場所

原子力規制委員会原子力規制庁入札会議室

東京都港区六本木１丁目９番９号（六本木ファーストビル１３階）

7　企画書募集に関する質問の受付及び回答

（1）　受付先・受付方法

メールアドレス：env-info@nsr.go.jp

質問書【様式１】に所定事項を記載の上、電子メールにより提出することとし、質問及び回答は質問者自身の既得情報（特殊な技術、ノウハウ等）、個人情報、原子力規制庁の業務に支障をきたすものを除き公表する。

（2）　受付期限

令和元年６月４日（火）１２時まで

（3）　回答

令和元年６月１１日（火）１７時（企画競争参加者に対してメールにより回答）

8　資格要件に係る提出書類、提出期限等

（1）　提出書類（別添１）

① 本業務を実施する部門において、情報セキュリティ対策、各種脆弱性等に関する調査、情報セキュリティ監査業務等を中心としたコンサルティング業務を専門とする部門として１０名以上の要員がいることを確認できる書類

② 本業務を含む業務について、ＩＳＭＳ（ISO/IEC27001、JISQ27001）認証を取得している、もしくは類似する情報セキュリティ態勢を確認できる書類

③ 過去３年間において、情報システムにおけるペネトレーションテスト、プラットフォーム診断等のセキュリティ診断の実績の合計を毎年３件以上有し、うち年間１件以上はペネトレーションテストの実績を含んでいる事が確認できる書類

④ 本業務に従事する者の技術能力を明確にするため、本業務の中心的役割を担う者１名について、以下のうち１つ以上の資格を所有するとともに、セキュリティコンサルティング業務の経験が５年以上であることを確認できる書類

・　情報セキュリティスペシャリスト（情報処理技術者試験）

・　システム監査技術者（情報処理技術者試験）
・　情報処理安全確保支援士（情報処理技術者試験）
・　情報セキュリティ・プロフェッショナル認証資格（ＣＩＳＳＰ）
・　公認情報セキュリティマネージャ（ＣＩＳM）
・　公認情報セキュリティ監査人（ＣＡＩＳ）
・　公認情報システム監査人（ＣＩＳＡ）

⑤ 本業務を実施する者において、実施責任者、品質管理体制及び情報セキュリティ体制を確認できる書類（実施体制表等）

⑥ 実施責任者において、本作業を遂行するに当たり十分な実務能力及び管理能力を有し、本作業を統括する立場にあることを確認できる書類（業務経歴書類等）

⑦ 本業務の中心的役割を担う者において、政府機関統一基準群に基づいた中央府省庁等における情報セキュリティポリシー及び対策の実施手順の作成に関する支援業務の経験を有すること。並びに体制の中心となる立場で請け負った経験を確認できる書類

⑧ 本業務に従事する全ての者について、所属元の就業規則に秘密保持に関する項目が記載されている、又は雇用者と被雇用者の間で秘密保持に関する契約が締結されていることを確認できる書類

（２） 提出期限等

① 提出期限

令和元年６月１４日（金）１２時

② 提出先

東京都港区六本木１丁目９番９号 六本木ファーストビル
原子力規制委員会原子力規制庁長官官房総務課情報システム室　篠壁

③ 提出部数

（１）①②③④⑤⑥⑦⑧　２部

④ 提出方法

持参又は郵送（提出期限必着）による。
郵送する場合は、書留郵便等の配達の記録が残る方法に限る。

⑤ 提出に当たっての注意事項

ア　持参する場合の受付時間は、平日の１０時から１７時まで（１２時～１３時は除く）とする。

イ　郵送する場合は、封書の表に「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る資格要件書類在中」と明記すること。提出期限までに提出先に現に届かなかった資格要件書類は、無効とする。

ウ　提出された資格要件書類は、その事由の如何にかかわらず、変更又は取消しを行うことはできない。また、返還も行わない。

エ　参加資格を満たさない者が提出した資格要件書類は、無効とする。

オ　虚偽の記載をした資格要件書類は、無効にするとともに、提出者に対して指名停止を行うことがある。

カ　資格要件書類の作成及び提出に係る費用は、提出者の負担とする。

キ　提出された資格要件書類は、原子力規制委員会原子力規制庁において、資格要件書類の審査以外の目的に提出者に無断で使用しない。企画競争の結果、契約相手になった者が提出した資格要件書類の内容は、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）に基づき開示請求があった場合においては、不開示情報（個人情報、法人等の正当な利益を害するおそれがある情報等）を除いて開示される場合がある。

ク　資格要件書類において提出者以外の者の協力を得て事業を実施する旨の提案を行っている場合は、契約の締結に当たりその履行を担保するため、協力の内容、態様等に応じ、提出者と協力者の間の共同事業実施協定書等の提出を求めることがある。

9　企画書等の提出書類、提出期限等

（1）　提出書類

① 企画書

「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務の企画書作成事項」に基づき作成すること。

② 経費内訳書

「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務」を実施するために必要な経費のすべての額（消費税及び地方消費税額を含む。）を記載した内訳書

③ 提出者の概要（会社概要等）が分かる資料

（2）提出期限等

①　提出期限

８（２）① に同じ

②　提出先

８（２）② に同じ

③　提出部数

ア　（１）①　　６部

イ　（１）②　　６部

ウ　（１）③　　２部

④　提出方法

８（２）④ に同じ

⑤　提出に当たっての注意事項

ア　持参する場合の受付時間は、平日の１０時から１７時まで（１２時～１３時は除く）とする。

イ　郵送する場合は、封書の表に「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等在中」と明記すること。提出期限までに提出先に現に届かなかった企画書等は、無効とする。

ウ　提出された企画書等は、その事由の如何にかかわらず、変更又は取消しを行うことはできない。また、返還も行わない。

エ　１者当たり１件の企画を限度とし、１件を超えて申し込みを行った場合はすべてを無効とする。

オ　参加資格を満たさない者が提出した企画書等は、無効とする。

カ　虚偽の記載をした企画書等は、無効にするとともに、提出者に対して指名停止を行うことがある。

キ　企画書等の作成及び提出に係る費用は、提出者の負担とする。

ク　提出された企画書等は、原子力規制委員会原子力規制庁において、企画書等の審査以外の目的に提出者に無断で使用しない。企画競争の結果、契約相手になった者が提出した企画書等の内容は、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）に基づき開示請求があった場合においては、不開示情報（個人情報、法人等の正当な利益を害するおそれがある情報等）を除いて開示される場合がある。

ケ　企画書等において提出者以外の者の協力を得て事業を実施する旨の提案を行っている場合は、契約の締結に当たりその履行を担保するため、協力の内容、態様等に応じ、提出者と協力者の間の共同事業実施協定書等の提出を求めることがある。

10　企画提案会の開催

（１）　必要に応じて企画提案会を開催する。開催する場合には、開催場所、説明時間、出席者数の制限等について、有効な企画書等を提出した者に対して、令和元年６月１９日（水）１８時までに連絡する。

（２）　上記により連絡を受けた者は、指定された場所及び時間において、提出した企画書等の説明を行うものとする。

11　暴力団排除に関する誓約

当該業務に係る（資格要件に係る提出書類及び）企画書等については、（別紙）において示す暴力団排除に関する誓約事項に誓約の上、提出すること。また、提出書類（別添２）の誓約事項に誓約する旨を明記すること。

12　審査の実施

（１）審査は、「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等審査の手順」（別添３）及び「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等審査基準及び採点表」（別添４）に基づき、提出された企画書等について行い、業務の目的に最も合致し優秀な企画書等を提出した１者を選定し、契約候補者とする。ただし、優秀な企画書等の提出がなかった場合には、この限りではない。

（２）審査結果は、企画書等の提出者に遅滞なく通知する。

13　契約の締結

企画競争の結果、契約候補者として選定されたとしても、会計法令に基づく契約手続の完了までは、原子力規制委員会原子力規制庁との契約関係を生ずるものではない。

支出負担行為担当官である原子力規制委員会原子力規制庁長官官房参事官は、契約候補者から見積書を徴取し、予定価格の制限の範囲内であることを確認し、契約を締結する。

なお、契約書には、提案書が添付され、又は提案書の内容が記載されるものであり、契約の相手方となった者は提案書の履行を確約しなければならない。

◎添付資料

（別紙）　暴力団排除に関する誓約事項
（別添１）　資格要件書類の提出について
（別添２）　企画書等の提出について
（別添３）　企画書等審査の手順
（別添４）　企画書等審査基準及び採点表
（別添５）　業務の概要及び企画書作成事項
【様式１】　質問書

（別紙）

暴力団排除に関する誓約事項

当社（個人である場合は私、団体である場合は当団体）は、下記事項について、入札書（見積書）の提出をもって誓約いたします。

この誓約が虚偽であり、又はこの誓約に反したことにより、当方が不利益を被ることとなっても、異議は一切申し立てません。

また、官側の求めに応じ、当方の役員名簿（有価証券報告書に記載のもの（生年月日を含む。）。ただし、有価証券報告書を作成していない場合は、役職名、氏名及び生年月日の一覧表）及び登記簿謄本の写しを提出すること並びにこれらの提出書類から確認できる範囲での個人情報を警察に提供することについて同意します。

記

１．次のいずれにも該当しません。また、将来においても該当することはありません。

（１）契約の相手方として不適当な者

ア　法人等（個人、法人又は団体をいう。）の役員等（個人である場合はその者、法人である場合は役員又は支店若しくは営業所（常時契約を締結する事務所をいう。）の代表者、団体である場合は代表者、理事等、その他経営に実質的に関与している者をいう。）が、暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第 77 号）第２条第２号に規定する暴力団をいう。以下同じ）又は暴力団員（同法第２条第６号に規定する暴力団員をいう。以下同じ。）であるとき

イ　役員等が、自己、自社若しくは第三者の不正の利益を図る目的又は第三者に損害を加える目的をもって、暴力団又は暴力団員を利用するなどしているとき

ウ　役員等が、暴力団又は暴力団員に対して、資金等を供給し、又は便宜を供与するなど直接的あるいは積極的に暴力団の維持、運営に協力し、若しくは関与しているとき

エ　役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有しているとき

（２）契約の相手方として不適当な行為をする者

ア　暴力的な要求行為を行う者

イ　法的な責任を超えた不当な要求行為を行う者

ウ　取引に関して脅迫的な言動をし、又は暴力を用いる行為を行う者

エ　偽計又は威力を用いて会計課長等の業務を妨害する行為を行う者

オ　その他前各号に準ずる行為を行う者

２．暴力団関係業者を再委託又は当該業務に関して締結する全ての契約の相手方としません。

３．再受任者等（再受任者、共同事業実施協力者及び自己、再受任者又は共同事業実施協力者が当該契約に関して締結する全ての契約の相手方をいう。）が暴力団関係業者であることが判明したときは、当該契約を解除するため必要な措置を講じます。

４．暴力団員等による不当介入を受けた場合、又は再受任者等が暴力団員等による不当介入を受けたことを知った場合は、警察への通報及び捜査上必要な協力を行うとともに、発注元の契約担当官等へ報告を行います。

（別添１）

令和元年　　月　　日

原子力規制委員会原子力規制庁長官官房参事官　殿

所　在　地
商号又は名称
代 表 者 氏 名　　印

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務
に係る資格要件書類の提出について

標記の件について、次のとおり提出します。

① 本業務を実施する部門において、情報セキュリティ対策、各種脆弱性等に関する調査、情報セキュリティ監査業務等を中心としたコンサルティング業務を専門とする部門として１０名以上の要員がいることを確認できる書類

② 本業務を含む業務について、ＩＳＭＳ（ISO/IEC27001、JISQ27001）認証を取得している、もしくは類似する情報セキュリティ態勢を確認できる書類

③ 過去３年間において、情報システムにおけるペネトレーションテスト、プラットフォーム診断等のセキュリティ診断の実績の合計を毎年３件以上有し、うち年間１件以上はペネトレーションテストの実績を含んでいる事が確認できる書類

④ 本業務の中心的役割を担う者１名について、以下のうち１つ以上の資格を所有するとともに、セキュリティコンサルティング業務の経験が５年以上であることを確認できる書類
- 情報セキュリティスペシャリスト（情報処理技術者試験）
- システム監査技術者（情報処理技術者試験）
- 情報処理安全確保支援士（情報処理技術者試験）
- 情報セキュリティ・プロフェッショナル認証資格（ＣＩＳＳＰ）
- 公認情報セキュリティマネージャ（ＣＩＳM）
- 公認情報セキュリティ監査人（ＣＡＩＳ）
- 公認情報システム監査人（ＣＩＳＡ）

⑤ 本業務を実施する者において、実施責任者、品質管理体制及び情報セキュリティ体制を確認できる書類（実施体制表等）

⑥ 実施責任者において、本作業を遂行するに当たり十分な実務能力及び管理能力を有し、本作業を統括する立場にあることを確認できる書類（業務経歴書類等）

⑦ 本業務の中心的役割を担う者において、政府機関統一基準群に基づいた中央府省庁等における情報セキュリティポリシー及び対策の実施手順の作成に関する支援業務の経験を有すること。並びに体制の中心となる立場で請け負った経験を確認できる書類

⑧ 本業務に従事する全ての者について、所属元の就業規則に秘密保持に関する項目が記載されている、又は雇用者と被雇用者の間で秘密保持に関する契約が締結されていることを確認できる書類

(担当者)
所属部署：
氏　　名：
ＴＥＬ：
ＦＡＸ：
E-mail：

（別添２）

令和元年　　月　　日

原子力規制委員会原子力規制庁長官官房参事官　殿

所在地

商号又は名称

代表者氏名　　印

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務
に関する企画書等の提出について

標記の件について、次のとおり提出します。

なお、書類の提出にあたり、企画競争説明書「５　参加資格」（７）及び暴力団排除に関する誓約事項に誓約します。

（1） 企画書

（2） 経費内訳書

（3） 会社概要等

(担当者)
所属部署：
氏名：
TEL：
FAX：
E-mail：

（別添３）

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等審査の手順

1. 企画審査委員会による審査

原子力規制庁長官官房総務課情報システム室に設置する「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書審査委員会」（委員は下記のとおり。以下「企画書審査委員会」という。）において、提出された企画書等の内容について審査を行う。

表 1 企画書審査委員会の構成

委員長	原子力規制委員会原子力規制庁長官官房　ｻｲﾊﾞｰｾｷｭﾘﾃｨ・情報化参事官
委員	原子力規制委員会原子力規制庁長官官房総務課　課長補佐
	原子力規制委員会原子力規制庁長官官房総務課　情報システム専門職
	原子力規制委員会原子力規制庁長官官房総務課　情報システム専門職
	原子力規制委員会原子力規制庁長官官房総務課　防災システム専門職

注 委員長又は委員が出席困難な場合は、同じ課(室)の者を代理として出席させることができる。

2. 企画書等の審査方法

(1) 「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等審査基準及び採点表」（別添４）に基づき、委員ごとに採点する。

【採点基準】

	10 点満点	30 点満点	50 点満点
優	10 点	30 点	50 点
良	6 点	18 点	30 点
可	2 点	6 点	10 点
不可	0 点	0 点	0 点

(2) (1)の採点結果の合計点を算出し、その点数が最も高い者を契約候補者とする。

(3) 合計点が同点の場合、次の基準で契約候補者を選定する。

① 「優」の数が多い者を契約候補者とする。

② 「優」の数が同数の場合は、「良」の数が多い者を契約候補者とする。

③ 「良」の数も同数の場合は、「可」の数が多い者を契約候補者とする。

④ 「可」の数も同数の場合は、委員の多数決により契約候補者を選定する。

ただし、組織のワーク・ライフ・バランス等の推進に関する認定等取得状況については、審査基準欄に記載の基準による。

3. 契約委員会による契約候補者の確定

企画書審査委員会は、選定した契約候補者及び審査経過を原子力規制委員会原子力規制庁長官官房参事官へ報告し、同参事官を委員長とする契約委員会において契約候補者を確定する。

（別添４）

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務に係る企画書等審査基準及び採点表

委員名

提案者名

事項		作成方法	配点	採点
１．業務の基本方針		・業務の目的を的確に理解し、妥当な基本方針であるか。 ・基本方針に専門性、創造性、新規性、確実性等があるか。	５０点	点
２．業務の実施計画		・明示された作業の実施期限が遵守されており、実施可能な実施計画であるか。 ・実施計画が効率的で確実性があるか。 ・業務分担や業務量の検討が適切であるか。また、その実効性があるか。 ・実施計画の策定に当たって、「デジタル・ガバメント推進標準ガイドライン」等各種指針で対応すべき内容が明示されていること。	１０点	点
３．業務の実施方法	（１）原子力規制委員会情報セキュリティポリシー及び関連規程類（以下「ポリシー等」という。）の改定支援	・原子力規制庁の現状及びや政府の動向を十分に考慮した内容であるか。 ・提案された内容が、求められた趣旨に適合したものであり、具体的なものであるか。 ・提案された内容に、専門性、創造性、新規性、確実性等があるか。特に、工程管理を行なう際の役割や実施する内容が具体的に提案されているか。 ・追加事項として提案された内容が、本業務の目的に適合しているものであり、その内容に専門性、創造性、新規性、確実性等があるか。	５０点	点
	（２）ポリシー等に係る情報セキュリティ教育の実施支援		５０点	点
	（３）自己点検に係る支援		５０点	点
	（４）情報システム運用継続計画の運用支援		５０点	点
	（５）情報セキュリティマネジメントに係る改善支援		５０点	点

	（6）サイバーセキュリティ技術的対策調査		５０点	点
	（7）ペネトレーションテスト		３０点	点
	（8）サイバーセキュリティ演習		３０点	点
	（9）定例ミーティングの実施および照会対応		３０点	点
４．実施体制、役割分担等	4.1　実施体制、役割分担等	・効果的、効率的な人員配置、内・外部の協力体制等が構築されているか。 ・実施責任者及びその他の主要な従事者が本業務に従事する十分な時間があると認められるか。	３０点	点
	4.2　従事者の実績、能力、資格等	・企画競争説明書に記載の資格要件について、業務責任者が有する経験・実績は「業務の件数」「業務の規模及び内容」「業務における役割」「保有資格」などの観点より充実しているか。 ・企画競争説明書に記載の資格要件について、業務責任者以外のその他の主要な従事者の経験・実績は「業務の件数」「業務の規模及び内容」「業務における役割」「保有資格」などの観点より充実しているか。 ・関連する保有資格が記載されており、そのことを確認できる書類が示されているか。	１０点	点
５．組織の実績		・企画競争説明書に記載の資格要件について、提案者の組織の実績は「業務の件数」「業務の規模及び内容」「業務における役割」「保有資格」などの観点より充実しているか。	３０点	点
６．見積価格、積算内訳		・経費内訳書について、提案内容等に応じた価格、積算内訳は妥当か。	１０点	点

７．組織のワーク･ライフ･バランス等の推進に関する認定等取得状況	女性の職業生活における活躍の推進に関する法律（以下「女性活躍推進法」という。）、次世代育成支援対策推進法（以下「次世代法」という。）、青少年の雇用の促進等に関する法律（以下「若者雇用推進法」という。）に基づく認定等（えるぼし認定等、くるみん認定、プラチナくるみん認定、ユースエール認定）の有無、有の場合は認定通知書等の添付。ただし、企画書提出時点において認証期間中であること。 ※ 複数の認定等に該当する場合は、最も得点が高い区分により加点を行うものとする。 --- ○ 女性活躍推進法に基づく認定等（えるぼし認定等） ・1段階目（※1） 8点 ・2段階目（※1） 16点 ・3段階目 20点 ・行動計画（※2） 4点 ※1 女性活躍推進法に基づく一般事業主行動計画等に関する省令第8条第1項第1号イの項目のうち、労働時間等の働き方に係る基準は必ず満たすことが必要。 ※2 女性活躍推進法に基づく一般事業主行動計画の策定義務がない事業主（常時雇用する労働者の数が300人以下のもの）が努力義務により届出し、企画書提出時点において計画期間が満了していないものに限る。 ○ 次世代法に基づく認定（くるみん認定･プラチナくるみん認定） ・くるみん認定 8点 ・プラチナくるみん認定 16点 ○ 若者雇用推進法に基づく認定（ユースエール認定） 16点	２０点	点
８．プレゼンテーション	・プレゼンテーションの説明の内容が明確であり、また提案書の内容と齟齬がなく、要求事項に対して的確な提案の説明となっているか。 ・提案内容や業務実施方法に対する質疑応答内	３０点	点

	容が的確かつ明確であり、本業務を確実に遂行する能力があると特に期待できるか。		
合計		５８０点	点

注１　企画書等において、提出者の外部協力者へ再委託又は共同実施の提案を行う場合、業務における総合的な企画及び判断並びに業務遂行管理部分を外部に再委託してはならず、そのような企画書等は不合格として、選定対象としないことがある。

注２　積算内訳書において、再委任に係る外注費が見積価格１／２以上である場合は、不適切として、選定対象としないことがある。

【採点基準】

	10 点満点	30 点満点	50 点満点
優	10 点	30 点	50 点
良	6 点	18 点	30 点
可	2 点	6 点	10 点
不可	0 点	0 点	0 点

ただし、事項 ７．組織のワーク・ライフ・バランス等の推進に関する認定等取得状況については、審査基準欄に記載の基準による。

（別添５）

令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務の概要及び企画書作成事項

１．件名

令和元年度原子力規制委員会情報セキュリティ対策に係る業務支援

２．概要

近年の急激な行政事務の電子化に伴い、各種情報システムや、電子情報を中心とした情報資産に対するセキュリティ維持、向上に対する必要性はますます高まってきている。

また、平成30年度の情報セキュリティ戦略本部において、政府機関等の情報セキュリティ対策のための統一基準群（以下「政府機関統一基準群」という。）が改定されるとともに、サイバーセキュリティ戦略（平成30年度から３年間の基本方針）においても、サイバー攻撃の様態は、深刻化・巧妙化が図られる等、予断を許さない状況であり、新たなランサムウェア等による様々な侵入手口も高度化の一途にあるとされることから、政府機関等の更なる情報セキュリティ強化が求められている。そのような状況の下、原子力規制委員会内の情報セキュリティ対策を早急に実施し、かつ確実なレベルにすることが必要である。本件は、そのために必要となる情報セキュリティ対策に係る支援業務を行うものである。

３．用語の定義

本仕様書で使用する用語の定義は以下の通りである。

用語	定義
主管課	情報システムの維持（サービス提供を含む。）管理・運用、他課室等の情報システム管理責任者との連絡調整等を行う庁内の組織 ※原子力規制委員会原子力規制庁長官官房総務課情報システム室
行政ＬＡＮシステム	原子力規制委員会ネットワークシステムの略称 所管行政の業務効率化及び情報化を推進するために、端末、サーバ、プリンタ及びその他の情報機器を接続し、職員等が作成した情報資産を共有するための情報システム
統合原子力防災ネットワークシステ	原子力緊急事態発生時に国・地方公共団体・原子力事業者・専門家等関係者が一体となって住民の安全防護等の対

ム	応を行う拠点となる「原子力災害対策本部」、「原子力規制庁緊急時対応センター」及び「緊急事態応急対策等拠点施設」等をネットワークで接続し、情報共有するための情報システム
情報セキュリティマネジメント	企業・組織における情報セキュリティの確保に組織的・体系的に取り組むこと（総務省）。
対象システム	原子力規制委員会原子力規制庁が主管する情報システム

４．契約期間

契約締結日～令和２年３月３１日

５．主管課

原子力規制委員会原子力規制庁長官官房総務課

〒１０６－８４５０　東京都港区六本木一丁目９番９号　六本木ファーストビル

連絡先：ＴＥＬ０３－５１１４－２１３０

６．本調達の内容

（１）原子力規制委員会情報セキュリティポリシー及び関係規程類（以下「ポリシー等」という。）の改定支援

（ア）原子力規制委員会情報セキュリティポリシーの改定支援

主管課の依頼及び平成30年度に実施した原子力規制委員会における情報セキュリティ施策の結果並びに政府機関統一基準群において対応が求められる情報セキュリティに関する重大な変化等への最新動向に基づき、現在制定されている原子力規制委員会情報セキュリティポリシーへの影響を評価し、改定案を作成すること。その際、新旧対照表を作成し、改定箇所を示すこと。また、改定案を元に主管課が行う改定作業を支援すること。

（イ）原子力規制委員会情報セキュリティ関係規程の改定支援

前記（ア）の作業後、主管課の依頼又は政府機関統一基準群及び原子力規制委員会情報セキュリティポリシーの改定内容を踏まえ、原子力規制委員会情報セキュリティ関係規程について改定案を作成すること。その際、新旧対照表を作成し、改定箇所を示すこと。また、改定案を元に主管課が行う改定作業を支援すること。

（ウ）運用管理規程類の改定支援

前記（イ）の原子力規制委員会情報セキュリティ関連規程の改定に伴い、原子力規制委員会の所管する情報システムの運用管理規程類について改定案を作成するこ

と。その際、新旧対照表を作成し、改定箇所を示すこと。また、改定案を元に主管課が行う改定作業を支援すること。

（エ）ポリシー等の内容に係る照会対応支援

ポリシー等の内容に関する照会があったときは、主管課が作成する回答案について、解釈等について助言すること。

（オ）情報セキュリティハンドブックの改定支援

ポリシー等に規定されたもののうち、一般職員（行政事務従事者）が遵守すべき重要なルールを簡潔に取りまとめた情報セキュリティハンドブックの改定案を作成すること。改定案には、必要に応じて図表等を用いることで、職員にとって分かりやすいものとすること。

（２）ポリシー等に係る情報セキュリティ教育の実施支援

（ア）情報セキュリティ教育用資料及び理解度確認テストの改定支援

ポリシー等の理解度の向上を目的として、最近の脅威動向等を踏まえた情報セキュリティ教育用資料及び理解度確認テストの改定案を作成すること。

（イ）情報セキュリティ教育及び理解度確認テストの実施支援

主管課が行う下記対応について、必要に応じて助言を行うこと。

・全職員（１，６００人）向けのe-Learning等の実施環境の準備
・情報セキュリティ教育及び理解度確認テストの実施
・実施期間中の受講促進の支援

（ウ）理解度確認テストの結果集計、評価分析及び次年度に向けての改善提案

理解度確認テストの実施結果データを集計及び分析し、次年度に向けた改善提案を含む実施報告書案を作成すること。

（エ）ポリシー等の内容に関する照会対応支援

ポリシー等の内容に関する照会があったときは、主管課が作成する回答案についてポリシー等の解釈等について助言すること。また、主管課がポリシー等の変更を行う必要があると判断したときは、修正案を作成すること。

（３）自己点検に係る支援

（ア）自己点検実施手順書の作成支援

情報セキュリティ対策の自己点検に関する年度計画の策定、準備、実施、評価及び改善を含む自己点検実施手順書案を作成すること。なお、作成にあたっては、こ

れまでの自己点検に係る運用方法や主管課の方針を確認し、内閣サイバーセキュリティセンターが公表している「自己点検の考え方と実務への準備 解説書」を参考にすること。

（イ）自己点検調査票の改定支援

昨年度の自己点検の結果、主管課の方針及び内閣サイバーセキュリティセンターからの指摘事項等を踏まえて、前記（ア）を基に今年度の自己点検調査票の改定案を作成すること。

（ウ）自己点検の実施支援

主管課が行う下記対応について、必要に応じて助言を行うこと。

・行政事務従事者の自己点検に係るe-Learning等の実施環境の準備
・自己点検の実施

（エ）自己点検結果の集計及び報告支援

自己点検を実施して得られた回答結果を抽出し、個々の自己点検調査票における矛盾した回答の組み合わせなどの論理的な整合性を点検すること。不整合点は主管課と協議の上、回答を補正すること。

結果は、主体別、課室等別、情報システム別等を考慮し、主管課の指示するフォームを用いて集計する。集計結果は、セキュリティの専門的な見地から分析、評価を行い、報告書案を作成し、提出すること。

なお、報告書案は、集計結果のとりまとめだけではなく、結果内容について問題点の指摘や一般的に優れている点などの考察を含め、そこで指摘した事項については、その対処方法や改善策などについて提案すること。

（４）情報システム運用継続計画（以下「ＩＴ－ＢＣＰ」という。）（案）の改定支援

（ア）ＩＴ－ＢＣＰ（案）の改定に係る対象範囲の整理支援

原子力規制員会業務継続計画（首都直下型地震対策）に記載されている情報システムについて、主管課からの指示のもと、主管課が整備及び向上すべきＩＴ－ＢＣＰの範囲を整理すること。

（イ）ＩＴ－ＢＣＰ（案）の改定支援

前記（ア）で得た情報を基に、ＩＴ－ＢＣＰ（案）の改定案を作成すること。

（ウ）ＩＴ－ＢＣＰに関する教育資料の作成支援

ＩＴ－ＢＣＰに基づき教育資料案を作成すること。教育資料案には、災害時における体制及び対応フロー等に関する内容を含めること。

（エ）ＩＴ－ＢＣＰに係る訓練計画の作成支援

ＩＴ－ＢＣＰの訓練実施において、主管課と訓練実施範囲を協議した後に、想定する災害、災害による被害、訓練までの実施事項、訓練当日の手順等をまとめた訓練実施計画案を作成すること。

（オ）ＩＴ－ＢＣＰに係る訓練の実施支援

前記（エ）で作成した訓練実施計画書に基づき、ＩＴ－ＢＣＰの訓練実施を支援すること。

（カ）ＩＴ－ＢＣＰに係る訓練の実施結果の集計、分析及び実施報告書の作成支援

訓練の実施結果について集計及び分析を行い、ＩＴ－ＢＣＰ及び情報システムの構成、情報システムの復旧に係る手順書における改善事項を含むＩＴ－ＢＣＰに係る訓練の実施報告書案を作成し、主管課に提出すること。

（５）情報セキュリティマネジメントに係る改善支援

（ア）情報セキュリティマネジメントに係る改善支援の実施計画書の作成

主管課と調整して、調査対象範囲、スケジュール、評価方法（評価基準を含む。）、実施結果に対する分析・評価方法等を記載した実施計画書を作成すること。なお、細部は下記のとおりである。

- 課室等及び情報システムの運用及び状況について、情報セキュリティマネジメントの観点から調査すること。
- 対象は、行政ＬＡＮシステム又は統合原子力防災ネットワークシステムとする。
- 資料の閲覧、対象システムの担当者へのヒアリング、現場の視察等を含めること。

（イ）情報セキュリティマネジメントに係る改善支援の実施

実施計画書に基づき、対象課室等及びシステムに対する状況調査を実施すること。調査において重大な問題が発見された場合には速やかに課室等又は対象システムの担当者に報告し、要すれば暫定的な処置案を提示すること。

（ウ）情報セキュリティマネジメントに係る改善支援の分析及び実施報告書の作成

状況調査の結果について分析を行い、実施報告書を作成すること。実施報告書には、状況調査の内容、調査の範囲、発見事項（問題の細部）、改善推奨事項（推奨する処置及び着意事項を優先順に箇条書きに列挙したもの。）を含めること。

（エ）情報セキュリティマネジメントに係る改善支援の照会対応

実施報告書について、対象課室等又はシステムの担当者からの問合せを受けた場合には対応すること。

（６）サイバーセキュリティ技術的対策調査

（ア）サイバーセキュリティ技術的対策調査の実施計画書の作成

主管課と調整して、調査対象範囲、スケジュール、評価方法（使用するベンチマーク等の内容も含む）、実施結果に対する分析・評価方法等を記載した,実施計画書を作成すること。なお、細部は下記のとおりである。

- 対象は、統合原子力防災ネットワークシステムとする。
- 資料の閲覧、対象システムの担当者へのヒアリング、現場の視察等を含めること。
- インターネット経由の攻撃、内部セグメントまで侵入され遠隔操作による攻撃、内部不正者による攻撃等、想定される全てのサイバー攻撃に対する技術的対策の評価を実施すること。

（イ）調査の実施

実施計画書に基づき対象システムに対するサイバーセキュリティ技術的対策調査を実施すること。重大な問題を発見した場合には速やかに主管課に連絡をするとともに、暫定対策案を提示すること。

（ウ）実施報告書の作成

実施の結果について分析を行い、実施報告書を作成すること。実施報告書には、調査の内容、調査の範囲、発見事項（発見した問題の内容及び深刻度）、想定される改善推奨事項（暫定対策及び本格対策がある場合にはそれぞれ記載）を記載すること。

（エ）実施結果に係る照会対応

実施結果について、対象システムの担当者からの問合せを受けた場合にはこれに対応すること。

（オ）能動的な侵入検知技術に係る検討

高度標的型攻撃の対策強化策として、攻撃者に偽の情報を与えて攻撃を遅らせると共に、侵入を検知することを目的とした囮を、行政ＬＡＮシステムまたは主管課が指示する環境に設置して効果を確認すること。情報システムの特性を調査したうえで、攻撃遅滞及び検知等の観点から、期待する効果、囮の構成、設定する偽の情報、設置場所、スケジュール等を含む実証計画書を作成し、主管課で準備する機器

上に囮を設置すること。なお、囮は設置する情報システムへの影響を極限するとともに、囮自体が脆弱性とならないこと。設置後、期待する効果を検証し、報告書を作成すること。

（７）ペネトレーションテスト

（ア）実施概要

対象ＩＰアドレス数は、３０ＩＰとする。

実施方法は、インターネット経由の直接攻撃及び標的型攻撃等によりサーバセグメントまで侵入される攻撃を想定し、遠隔操作の可能性も検討すること。ツールによる診断に加えて、診断の網羅性や正確性を担保するための手動による検査を実施すること。また、インターネット側からの診断により内部ネットワークへ侵入することができた場合には、内部ネットワークの問題点についての検証も行うこと。また、稼働中のサービスに対して影響を伴うことが想定される攻撃手法については実施しないこと。実施日時、実施の細部方法は主管課と調整のうえ決定すること。

（イ）実施計画書の作成

主管課と調整して、ペネトレーションテスト実施のための計画書を作成すること。実施計画書にはスケジュール、ペネトレーションテスト方法（攻撃方法、使用するツール等の内容を含む）、ペネトレーションテストの完了条件、実施結果に対する分析・評価方法、連絡先等を記載し、提出すること。

（ウ）ペネトレーションテストの実施

実施計画書に基づき、対象システムに対するペネトレーションテストを実施すること。テスト実施期間中の各日の作業開始時及び作業終了時には、主管課及び対象システムの担当者に連絡をすること。また、ペネトレーションテストにおいて重大な問題が検出された場合や、検出された問題を利用し内部ネットワークへ侵入することができた場合には、速やかにペネトレーションテストを中断し、主管課及び対象システムの担当者に連絡をすること。

（エ）実施報告書の作成

実施の結果について分析を行い、ペネトレーションテストの内容、ペネトレーションテストの範囲、実施結果（検出した問題の内容、深刻度及び再現方法）、想定される対策案（暫定対策と本格対策がある場合にはそれぞれ記載すること）及びペネトレーションテスト結果全体の評価を記載した実施報告書をシステム毎に作成すること。実施報告書には、ペネトレーションテスト完了後、概ね３週間以内に提出すること。その後、内容を協議の上、対象システムを所管する課室毎（最大２課室）に報告会を開催すること。

（オ）実施結果に係る照会対応

実施報告書について、対象システムの担当者からの問合せを受けた場合にはこれに対応すること。

（８）サイバーセキュリティ演習

（ア）実施概要

行政ＬＡＮシステムを対象に、情報漏洩やサービス停止等、具体的な脅威シナリオを１つ作成し、関連するシステムやネットワークの実機に対して疑似的な攻撃を加えることにより、既存のセキュリティ対策の有効性を検証する。攻撃手法については、予め防御側に攻撃方法を開示して実施するホワイトボックス型と、開示することなく実施するブラックボックス型が考えられるが、情報システムの特性を考慮し、主管課と調整のうえ決定すること。

（イ）実施計画書の作成

行政ＬＡＮシステムをネットワーク構成図やヒアリングなどで確認し、業務やシステムへの影響を考慮したうえで、脅威シナリオと攻撃手順を作成して提案すること。また、演習を実施するために必要な前提条件、環境の準備や作業項目を洗い出し、役割分担やスケジュールなどを含むサイバーセキュリティ演習実施計画書を作成すること。

（ウ）サイバーセキュリティ演習の実施

演習の実施においては、ログの取得を含め、何をいつ実施したのか把握しつつ、疑似的な攻撃を行うこと。使用するツールは、商用、オープンソースあるいは自社開発したツール等の信頼できるツールを使用し、実際のマルウェアは使用しないこと。

（エ）演習結果の振り返り

演習の過程で発見された技術的側面及びインシデント対応に係る側面を含め、多角的な視点から問題点を整理し、改善案をワークショップ形式で検討（ディスカッション）すること。

また、攻撃に対して対象システムの担当者がログやアラートをもとに、適切に対処できるかを検証し、課題を明らかにすること。

（オ）実施報告書の作成

対象システムのサイバー攻撃に対する耐性を評価し、改善点が発見された場合はその改善策をまとめた実施報告書を作成すること。

（９）定例会の実施及び照会対応

本調達の進捗状況の把握及び課題事項の解決を目的とする定例会を実施すること。定例会の頻度は、原則週１回とするが、契約締結後に状況を考慮の上、出席者、開催日時及び開催場所等の詳細について、主管課と調整すること。また、主管課が本調達に関連した問合せ（（１）（ウ）に掲げるものを除く。）をメール又は書面により行ったときは、これに対応すること。

７．提出物（紙媒体２部、電子媒体１部）

作業項目	提出物
６．（１）	・原子力規制委員会情報セキュリティポリシー改定（案） ・新旧対照表 原子力規制委員会情報セキュリティポリシー ・原子力規制委員会情報セキュリティ関係規程類改定（案） ・新旧対照表 原子力規制委員会情報セキュリティ関係規程類 ・情報セキュリティハンドブックの改定（案）
６．（２）	・情報セキュリティ教育用資料（案） ・理解度確認テストの改定（案） ・情報セキュリティ教育及び理解度確認テストの実施報告書
６．（３）	・自己点検実施手順書（案） ・自己点検票（案） ・自己点検実施報告書
６．（４）	・情報システム運用継続計画（ＩＴ－ＢＣＰ）（案） ・情報システム運用継続計画（ＩＴ－ＢＣＰ）に関する教育資料（案） ・情報システム運用継続計画（ＩＴ－ＢＣＰ）に係る訓練計画（案） ・情報システム運用継続計画（ＩＴ－ＢＣＰ）訓練の実施報告書
６．（５）	・情報セキュリティマネジメントに係る改善支援の実施計画書 ・情報セキュリティマネジメントに係る改善支援の実施報告書
６．（６）	・サイバーセキュリティ技術的対策調査の実施計画書 ・サイバーセキュリティ技術的対策調査の実施報告書
６．（７）	・ペネトレーションテストの実施計画書 ・ペネトレーションテストの実施報告書
６．（８）	・サイバーセキュリティ演習実施計画書 ・サイバーセキュリティ演習実施報告書
６．（９）	・定例会資料、議事録 ・課題解決のための個別検討資料

- その他、本業務に関連して作成した資料等一式
- 提出場所：原子力規制委員会原子力規制庁長官官房総務課情報システム室
- 提出期限：令和２年３月３１日

８．受注者の要件

（１）本業務を実施する部門において、情報セキュリティ対策、各種脆弱性等に関する調査、情報セキュリティ監査業務等を中心としたコンサルティング業務を専門とする部門として１０名以上の要員がいること。また、本業務を含む業務についてＩＳＭＳ（ISO/IEC27001、JISQ27001）認証を取得していること、もしくは類似する情報セキュリティ態勢が構築されていること。

（２）過去３年間において、情報システムにおけるペネトレーションテスト、プラットフォーム診断等のセキュリティ診断の実績の合計を毎年３件以上有し、うち年間１件以上はペネトレーションテストの実績を含むこと。

（３）本業務に従事する者の技術能力を明確にするため、当該業務の中心的役割を担う者１名については、以下のうち１つ以上の資格を所有するとともに、セキュリティコンサルティング業務の経験が５年以上であること。

・　情報セキュリティスペシャリスト（情報処理技術者試験）
・　システム監査技術者（情報処理技術者試験）
・　情報処理安全確保支援士（情報処理技術者試験）
・　情報セキュリティ・プロフェッショナル認証資格（ＣＩＳＳＰ）
・　公認情報セキュリティマネージャ（ＣＩＳM）
・　公認情報セキュリティ監査人（ＣＡＩＳ）
・　公認情報システム監査人（ＣＩＳＡ）

（４）作業体制

・　本業務を実施する者は、実施責任者、品質管理体制及び情報セキュリティ体制を明示した実施体制表を提出すること。なお、実施責任者と品質管理責任者の兼務を行ってはならない。
・　実施責任者は、本作業を遂行するに当たり十分な実務能力及び管理能力を有し、本作業を統括する立場にある者とすること。なお、受注者の責任者が業務終了まで継続して遂行すること。万一交代する場合は同等以上の人物が担当するものとして事前に主管課の承認を得ること。
・　あらかじめ外注先が決まっている場合は、外注先名及びその発注事業内容を含めて記載すること。ただし、金５０万円未満の外注業務、印刷費、会場借料、翻訳費及びその他これに類するものを除く。

（５）業務に従事するすべての者が政府機関統一基準群について理解していること。また、本業務の中心的役割を担う者は、政府機関統一基準群に基づいた中央府省庁等における情報セキュリティポリシー及び対策の実施手順の作成に関する支援業務の経験

を有すること。並びに体制の中心となる立場で請け負った経験を有するとともに、原子力規制委員会における情報セキュリティポリシー及び対策の実施手順等の作成に関する支援業務に当たっても、中心的な役割を担い、原則、情報セキュリティに関する定例会において説明等を行うほか、原子力規制委員会における情報セキュリティポリシー及び対策の実施手順等の解釈等に関する問合せ等の対応窓口となること。

（６）本業務に従事する全ての者について、所属元の就業規則に秘密保持に関する項目が記載されている、又は雇用者と被雇用者の間で秘密保持に関する契約が締結されていること。

（７）令和０１・０２・０３年度（平成３１・３２・３３年度）環境省競争参加資格（全省庁統一資格）の「役務の提供等」の「調査・研究」又は「情報処理」において、企画書等の提出期限までに「Ａ」、「Ｂ」又は「Ｃ」の等級に格付されている者であること。

（８）作業場所

本業務の作業は受注者の作業場所で実施すること。

（９）本調達の下請

① 本件の受注者は、この契約の全部または一部を第三者に委任し、又は請け負わせないこと。但し、契約の主要な部分を除く補助的な業務について、受注者があらかじめ下請の相手方の住所、氏名、下請を行う業務範囲、下請の必要性及び契約金額について記載した書面を提出し、主管課の承認を得た場合はこの限りではない。

② 受注者は、本調達に関して下請先の行った業務についてすべての責任を負うこと。また、受注者は下請先に対して、機密保持を含め本調達仕様書の情報セキュリティ対策を定める義務を負う旨及び受注者が下請先に対して十分な監査を行うことができる権利を定めるものとし、本調達の受注者及び下請先の事業者間の契約においてその旨定めること。

③ 受注者は、下請先の事業者に対して、定期的又は必要に応じて、作業の進捗状況及び下請先における情報セキュリティ対策の実施状況を確認し、報告させるなど、下請先の事業者に対する監督を適切に行うこと。

（１０）遵守すべき法令等

当該調達案件の業務遂行に当たっては、以下に準拠して作業をおこなうこと。

・ デジタル・ガバメント推進標準ガイドライン
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_

20190225.pdf

- 政府機関等の情報セキュリティ対策のための統一基準群（平成30年度版）
  https://www.nisc.go.jp/active/general/kijun30.html

- 中央省庁における情報システム運用継続計画ガイドライン
  http://www.nisc.go.jp/active/general/itbcp-guideline.html

- 原子力規制委員会情報セキュリティポリシー
  https://www.nsr.go.jp/data/000129977.pdf

９．秘密の保持

受注者は本契約に関して、原子力規制委員会が開示した情報（公知の情報等を除く。以下同じ。）を本契約の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講じなければならない。また受注者は、本契約に基づく役務提供実施により知り得た情報の秘密保持に関し、誓約書を主管課に提出すること。また、企画書の検討を目的とし、入札前に本件に係る資料を閲覧する場合にも、「資料閲覧に係る機密保持契約書」を提出すること。

１０．知的財産権等

（１）本契約履行過程で生じた納入成果物に関し、著作権法第２７条及び第２８条に 定める権利に含む全ての著作権及びノウハウ（営業秘密）は原子力規制委員会に帰属し、原子力規制委員会が独占的に使用するものとする。但し、受注者は本契約履行過程で生じた著作権又はノウハウ（営業秘密）を自ら使用又は第三者をして使用させる場合は、原子力規制委員会と別途協議するものとする。

（２）納入成果物に第三者が権利を有する著作物（以下「既存著作物」という。）が含まれている場合は、原子力規制委員会が特に使用を指示した場合を除き、当該著作物の使用に必要な費用の負担及び使用承諾契約に係る一切の手続を行うこと。この場合、受注者は当該契約等の内容について事前に主管課の承認を得ることとし、原子力規制委員会は既存著作物について当該許諾条件の範囲内で使用するものとする。

（３）本仕様書に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら原子力規制委員会の責めに帰す場合を除き、受注者の責任、負担において一切を処理すること。この場合、原子力規制委員会が紛争等の事実を知った時は、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講ずるものとする。

１１．情報管理

（１）本業務の実施のために原子力規制委員会から提供する情報の管理について、別添１「情報管理計画書において定めるべき項目」に従い、事前に情報管理計画書を作成・提出すること。また、情報管理計画書の内容に変更が生じたときは、速やかに再提出すること。

（２）受注者は、契約書又は提出書類等に含まれている情報セキュリティ対策及び情報管理計画書の履行状況を定期的に主管課に報告すること。また、受注者が下請を実施する場合には、下請先の情報セキュリティ対策の履行状況もあわせて報告すること。

（３）受注者は、主管課の求めに応じて主管課から受注者の作業場所に対する立入検査を受け入れること。

（４）本業務の遂行における情報セキュリティ対策の履行が不十分である可能性を主管課が認める場合には、受注者の責任者は、主管課の求めに応じこれと協議を行い、合意した対応を取ること。

１２．その他

（１）本仕様書の内容及び解釈等について疑義が生じた場合、その他特に必要がある場合は、事前に原子力規制委員会と協議し、決定・解決すること。この場合、当該協議に関する議事録を作成し、確認を受けること。

（２）詳細については、主管課の指示によること。

別添１

情報管理計画書において定めるべき項目

	分類	記載すべき内容	
①	社内規程類	情報セキュリティ対策に係る規程	
		個人情報保護に係る規程	
		下請に係る規程	
②	秘密情報等の取扱い方法	情報取扱責任者、情報取扱管理者、情報取扱者の役割と体制	
		秘密情報の取扱方法	取得・入力時の対策内容
			利用・加工・複製の対策内容
			保存・保管の対策内容
			移送・送信・運搬の対策内容
			消去・廃棄、その他の対策内容
③	情報管理及び返却に関する計画	情報管理簿のフォーマット（情報資産名称、保管形態、利用場所、貸与日、貸与者、返却日及び返却者等を管理する文書）	
④	秘密情報の教育・研修・周知に関する計画	教育内容、対象者、実施目的、実施方法、実施時期等	
⑤	情報セキュリティ確保に関する計画	物理セキュリティ	具体的な作業場所
			入退室制御に係る設備（ICカードリーダ等）
			入室許可者
			持込禁止物
			入室許可者以外の管理
			その他対策内容詳細
		情報機器のセキュリティ	セキュリティ機能（ID管理、ウイルス対策、アクセスブロック等）
			利用者IDや情報機器の管理方法（管理簿等）
			モニタリング手法（稼働監視等）
			その他対策内容詳細
⑥	情報セキュリティ事故発生時の対応手順	事故発生時の体制（責任者・対応者）及び連絡先	
		想定される事象	
		報告手順	
⑦	その他	セキュリティ認証の取得状況	

【 様 式 １ 】

令和元年　　月　　日

原子力規制委員会原子力規制庁 担当者 殿

質 問 書

「令和元年度原子力規制委員会情報セキュリティ対策に係る支援業務」に関する質問書を提出します。

法人名	
所属部署名	
担当者名	
電話番号	
E-mail	

質問書枚数
枚中 枚目

＜質問箇所について＞

資料名	例）　○○書
ページ	例）　P○
項目名	例）　○○概要
質問内容	

備考

1. 質問は、本様式１枚につき１問とし、簡潔にまとめて記載すること。
2. 質問及び回答は、本件入札参加事業者の全てに公表する。（電話等による個別回答はしない。）但し、質問者自身の既得情報（特殊な技術、ノウハウ等）、個人情報、原子力規制委員会原子力規制庁の業務に支障をきたすものに関する内容については、公表しない。