契約番号:	135-001
	135-002
	151-073

公　募　説　明　書

下記に記載する内容及び条件において、当該業務等が実施可能であり、かつ、入札または企画競争を実施した場合、参加意思を有する者の有無を調査するため参加者確認公募に付す。

記

１．参加者確認公募に付する事項
（１）公 募 件 名: 「情報セキュリティに係る運用支援業務」
（２）趣旨及び概要: 仕様書による。
（３）数　　量: 一式
（４）作 業 期 間: ２０２２年　４月　１日 から ２０２３年　３月３１日
（５）作 業 場 所: 東京都台東区東上野一丁目２８番９号　キクヤビル
公益財団法人核物質管理センター　東京本部内指定場所

２．必要書類等の提出場所等
（１）契約事項を示す場所及び提出場所等
郵 便 番 号：１１０－００１５
所　在　地：東京都台東区東上野一丁目２８番９号　キクヤビル３階
機　関　名：公益財団法人核物質管理センター
担 当 部 署：総務部　契約課
フ リ ガ ナ：タノ　ミホ
担 当 者 名：太野　美穂
電 話 番 号：０３－５８１６－７７６５
Ｆ　Ａ　Ｘ：０３－３８３４－５２６５
Ｍ ａ ｉ ｌ：mitano@jnmcc. or. jp
（２）参加意志確認書の提出期限
２０２２年　２月１６日（水）　午後４時まで
公益財団法人核物質管理センター　東京本部　総務部　契約課　必着（電子メール可）
なお、参加意思確認書を郵送する場合、書留郵便若しくは配達記録が残るようにすること。
（３）提出書類（電子メール可）
・資格要件確認書に記載されている資料　　１部

３．参加者確認公募に参加する者に必要な資格
（１）次の①～⑤に該当する者は公募に参加することができない。
①成年被後見人
②未成年者、被保佐人及び被補助人（契約締結のための必要な同意を得ている場合は除く。）
③破産者で復権を得ない者
④競争に参加することを妨げ、又は契約の締結もしくは履行を妨げ、公序良俗に違反した者であって、その事実があった後２年を経過しない者（代理人、支配人、その他のとして使用する者についても、同様とする。）
⑤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又は同法第２条第６号に規定する暴力団員もしくはこれらと関係する者
（２）２０２１年度　国・地方公共団体等における競争参加資格（東北、関東・甲信越）の「役務の提供等」の資格を有すると認められた者

４．参加意思確認公募の手続き
参加意思確認書を提出した者に対して審査を行い、審査結果を通知する。
審査の結果、公募要件を満たす者が２者以上いる場合は、指名競争入札、複数者による見積合わせ又は企画競争を行う。
応募者がいない場合は、特定の者と随意契約の手続きを行う。

２０２２年　２月　４日

公益財団法人核物質管理センター
総務部長事務取扱
理事　小林　功

提出方法（いずれか）	電子メール、郵送、持参
押印の省略	可

公益財団法人核物質管理センター
総務部長事務取扱
理事　小林　功　　殿

住　　所
商号又は名称
代 表 者 名

参加意思確認書

2022年2月4日付で公示の下記の業務等について参加意思がありますので、参加意思確認書を提出します。

なお、本確認書に記載されている内容及び添付書類の内容については、事実と相違ないことを誓約します。

記

1．業務等の名称　「情報セキュリティに係る運用支援業務」

2．添付資料

(1) 国・地方公共団体等における競争参加資格（東北、関東・甲信越）を証する書類

(2) 本業務等の遂行に必要な資格及び実績を証する書類

(3) その他必要な書類

※(2)及び(3)は、公募説明書において提出を求めた書類とする。

所　　属
役　職　名
氏　　名
電 話 番 号
ＦＡＸ番号
電子メール

提出方法（いずれか）	電子メール、郵送、持参
押印の省略	可

参考資料 6

資格要件確認書

契約番号：XXX-XXX
契約件名：XXXXXXXXXXXXXXX設備の更新
参加者名：●●●●株式会社

請求元課室：XXX部XXX課
購買区分：A
評価の有無：有（下記のとおり）

社名を手書き又はゴム印で記入してください。
※社印は不要です。

本書は、案件ごとに添付された書式を印刷して手書きで記入してください。
記入後の本書と証明資料は、入札仕様書等の書類と合わせて、入札仕様書等の提出期限までに郵送してください。

複数例示された資料から選択する場合は提出する資料名を手書きで囲んでください。

例示された資料と提出資料が異なる場合は手書きで実際の資料名に訂正してください。
※訂正印は不要です。

			確認項目	証明資料 ※提出する資料名を記入してください。	センター記入欄 判定	判定理由	判定者
			業務の実施に十分な人員及びスキル（業務遂行に必要な有資格等が確保されて	●●資格証（写）			
				品質保証計画書			
	7R情報セキュ		ス を要求項目に沿って提供でム（設計・ている	JIS Q 9001認証証明書 QMS体制図			
			に対するいるこ	情報セキュリティ体制			
	1.3 入札資格		① 国等の入札参加資格を有すること。	国等の入札参加資格を証する書類			
2 技術確認事項	2.1 技術能力の確認		る作業	~~●●資格証（写）~~ □□証明書			
	2.2 技術設備の確認		設備を 設備を	対象設備一覧			
	2.3 物品性能の確認	P.3 4(1)	は、○○の性能要件を満たしていること。	製品のスペックがわかる資料（カタログ等）			
	2.4 物品の実績の確認	P.4 5(1)	① 過去5年間で、当該製品は、（耐震設計基準●クラスで）納入実績を示すこと。	納品実績表			

センター記入欄は何も記入しないでください。

資格要件確認書

契約番号:	135-001, 135-002, 151-	請求元課室：	情報セキュリティ室
契約件名:	情報セキュリティに係る運用支援業務	購買区分：	C
参加者名:		評価の有無：	有（下記のとおり）

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
1 業務の実施・管理体制等	1.1 業務の実施体制		① 業務の実施に十分な人員数及びスキル（業務遂行に必要な有資格等）が確保されていること。				
			② 必要な業務分担（設計開発、製造、調達、試験、検査、保守、設置工事、品質保証等）及び管理体制（品質管理責任者、作業管理者等を含む）がとられていること。				
	1.2 品質管理及び情報セキュリティ体制		① 受注する製品及びサービスを要求項目に沿って提供できる品質管理システム(設計・開発を含む)が確立していること。	JIS Q 9001認証証明書			
			② 情報セキュリティに対する管理体制が確立していること。	ISO/JIS Q 27001認証証明書 情報セキュリティ体制表			
	1.3※ 入札資格		※契約担当部署にて対応				
	1.4 コンプライアンス		①コンプライアンス違反の有無（有の場合はどのように改善したか。）				
			②不適合事象の有無（有の場合はどのように改善したか。）				

資格要件確認書

契約番号:	135-001, 135-002, 151-	請求元課室：	情報セキュリティ室
契約件名:	情報セキュリティに係る運用支援業務	購買区分：	C
参加者名:		評価の有無：	有(下記のとおり)

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
2 技術確認事項	2.1 技術能力の確認	P. 7 3.2 表3-2 No.1 左	実施責任者は、以下の資格のいずれか一つ以上を有すること。 ①プロジェクトマネージャ(IPA) ②Project Management Professional(PMI) ただし、ITスキル標準V3 2011に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある(その根拠を明確に示し、センターの承認を得ること。)。	資格証明書			
		P. 7 3.2 表3-2 No.1 右	実施責任者は、次期基盤情報システムと同規模(端末200台程度)以上の情報システムの運用プロジェクトにおいて、実施責任者としての経験を有すること。	実績表			
		P. 7 3.2 表3-2 No.2 左	運用チームリーダは、以下の資格のいずれか一つ以上を有すること。 ①システムアーキテクト(IPA) ②ネットワークスペシャリスト(IPA) ③情報処理安全確保支援士(IPA) ④ITサービスマネージャ(IPA) ⑤ITIL Foundationもしくはその上位資格 ただし、ITスキル標準V3 2011に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある(その根拠を明確に示し、センターの承認を得ること。)。	資格証明書			

資格要件確認書

契約番号：	135-001, 135-002, 151-	請求元課室：	情報セキュリティ室
契約件名：	情報セキュリティに係る運用支援業務	購買区分：	C
参加者名：		評価の有無：	有（下記のとおり）

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
		P. 7 3.2 表3-2 No.2 右	運用チームリーダは、次期基盤情報システムと同規模（端末200台程度）以上の情報システムの運用プロジェクトにおいて、チームリーダとしての経験を有すること。	実績表			
		P. 7 3.2 表3-2 No.3 右	運用チームメンバは、次期基盤情報システムと同規模（端末200台程度）以上の情報システムの運用プロジェクトの経験を有すること。	実績表			
	2.2 技術設備の確認	（例） P.2 3(1)	（例） ①●●の製造する設備を持っていること。				
		P.2 3(3)	②●●の試験する設備を持っていること。				
	2.3 物品性能の確認	（例） P.3 4(1)	（例） ①納品される製品は、●●の性能要件を満たしていること。				
		P.3 4(2)	②納品される製品は、●●の環境でも稼働していること。				
		P.3 4(3)	③空調用冷水設備の性能は次の値を保証すること。				
		P.3 4(4)	④●●時間以上の連続運転を保証すること。				
		P.3 4(5)	⑤納品される物品の●クラス相当の耐震設計基準を満たしていること。				
		P.3 4(6)	⑥納品される製品の●●年の設計耐用年数を満たしていること。				
	2.4	（例） P.4 5(1)）	（例） ①過去5年間で、当該製品は、（耐震設計基準●クラスで）納入実績を示すこと。				

資格要件確認書

契約番号：	135-001, 135-002, 151-	請求元課室：	情報セキュリティ室
契約件名：	情報セキュリティに係る運用支援業務	購買区分：	C
参加者名：		評価の有無：	有（下記のとおり）

評価項目		仕様書ページ	確認項目	証明資料	センター記入欄		
					判定	判定理由	判定者
	物品の実績の確認		②過去●年以内に同等製品（同等なサービス）の受注を受けた実績があること。（上記の実績は、当該製品（サービス）に対して重大な不適合を発生させ、発注元に損益を与えた事例がないものとする。）				
	2.5 ●●	（例） P5 6(1)	（例） ①工場立会検査に対応できること。				
		P5 6(2)	②受注者の品質管理システムについて品質監査を実施できること。				

注）各確認事項を証する資料名を「証明資料」欄に記載し、当該資料を入札仕様書又は見積書に添付のうえ契約担当者に提出すること。

情報セキュリティに係る運用支援業務

請負契約仕様書

2022年度

公益財団法人　核物質管理センター

— 目次 —

1. 概要

1.1. 件名

情報セキュリティに係る運用支援業務

1.2. 目的

公益財団法人核物質管理センター(以下、「センター」という。)では、2019 年 7 月よりネットワーク機器、各種基盤サービス、職員用端末等の情報インフラを統合的・一元的に管理運用しており、今後も安定した運用を実施する方針である。

センター全体の業務を支える情報インフラとなる基盤情報システム、既存システム及びテレワーク環境の運用を含む情報セキュリティに係る運用支援により、運用・保守業務の継続性・安全性を強化することを目的とする。

1.3. 用語の定義

本仕様書で使用する用語の定義を「別紙 2 用語の定義」に示す。

1.4. センターの情報システムの概要

センターの情報システムは、基盤情報システム(図 1-1 赤点線枠内)と既存システム(図 1-1 青点線枠内)から構成されている。

基盤情報システムは、センター全体の業務を支える情報インフラとなる「ネットワークサービス(クローズド系 LAN/WAN)」、「基盤サービス(各種基盤サーバ(統合認証、ファイル共有、システム運用管理、バックアップ管理等))」、「端末サービス」及び「仮想デスクトップサービス」を提供するためのシステムである。

サーバ装置等の機器については、物理的セキュリティ、信頼性、事業継続性等の向上の観点から、外部データセンターに配置している。

画面転送方式(VDI 方式)の仮想デスクトップサービスにより、職員用端末や個別業務システムが接続されるネットワークをインターネットから論理的に分離する構成とする。各課室が個別に管理・運用している個別業務システムは、原則としてクローズド系ネットワークに接続している。

既存システムは、センターからインターネットに接続する通信に係るサービス(メールシステム及びネットワークセキュリティ機器等)を提供するシステムである。

テレワーク環境は、センター事業所外の環境(在宅など)からセンターの基盤情報システム及び既存システムにアクセスするサービス(テレワーク端末、通信装置、マネージド EDR サービス)を提供するシステムである。

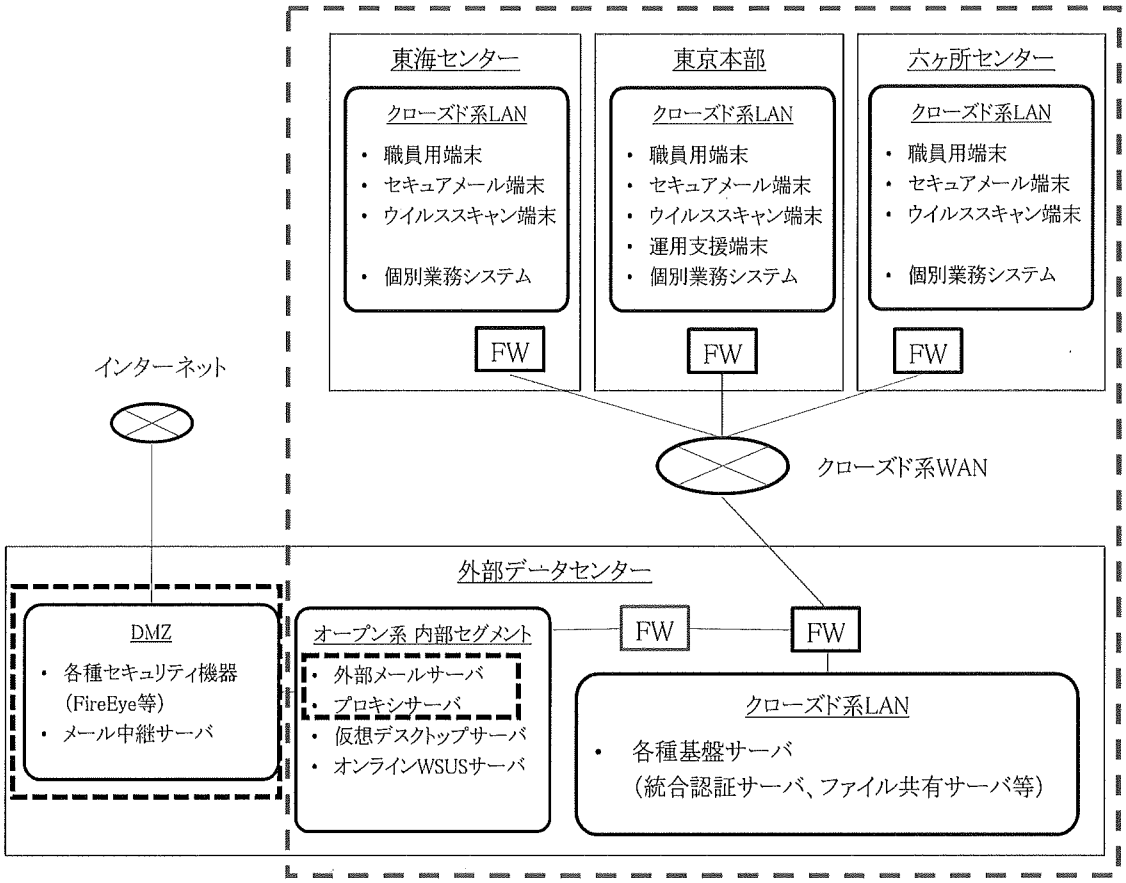

図 1-1 センターの情報システムの全体構成図
(赤点線枠:基盤情報システム(外部メールサーバとプロキシを除く)、
青点線枠:既存システム)

1.5. 実施場所

東京都台東区東上野一丁目 28 番地 9 号 キクヤビル
センター　総務部 情報セキュリティ室
その他 センターが指示する場所(在宅勤務時の自宅を含む)

1.6. 実施期日

(1)実施期間

2022年4月1日から2023年3月31日まで。
なお、土曜日、日曜日、祝日及びセンターが指定する日を除く毎日。
ただし、センターの業務の都合により、休日労働を行わせることができる。

(2)就業時間及び休憩時間

・就業時間　9時から17時30分まで(センターが指定する時間内で変更可能)
・休憩時間 12時から13時まで
ただし、センターの都合により、就業時間外労働を行わせることができる。

2. 業務内容

2.1. 基盤情報システムの運用作業

(1) 受注者は、「別紙 1 運用作業一覧 1.基盤情報システムの運用作業」に示す作業を実施すること。なお、作業の詳細は、閲覧資料として開示する「運用計画」、「運用実施要領」、「運用手順書」に従うこと。

(2) 受注者は、「別紙 1 運用作業一覧 3.その他支援作業」に示す作業を実施すること。

2.2. 既存システムに関する業務運用支援作業

(1) 受注者は、「別紙 1 運用作業一覧 2.業務運用支援作業」に示す作業を実施すること。

(2) 受注者は、「別紙 1 運用作業一覧 3.その他支援作業」に示す作業を実施すること。

2.3. 運用実績の報告

(1) 運用実績の報告は、「別紙 1 運用作業一覧 4.運用実績の報告」の記載に従い実施すること。なお、基盤情報システムの運用作業に関する報告の詳細は、閲覧資料として開示する「運用計画」、「運用実施要領」、「運用手順書」に従うこと。

(2) 受注者は、会議の議事録を、原則として、会議実施後 3 営業日以内に作成し、センターに提示すること。

2.4. 提出物等の範囲、提出期日等

2.4.1. 提出物一覧

本業務の提出物を以下に示す。なお、「提出期日」については本業務の契約締結時期や作業計画等を踏まえ、必要に応じてセンターと協議の上で見直しを行うこと。

表 2-1 提出物一覧

No.	提出物名	内容及び提出数量	提出期日
1	情報セキュリティ管理計画書	紙媒体 1 部 電磁的記録媒体 1 部	契約後速やかに
2	業務運用支援作業実施要領	紙媒体 1 部 電磁的記録媒体 1 部	契約後速やかに
3	日次チェックシート	紙媒体 1 部 電磁的記録媒体 1 部	契約後速やかに
4	議事録	紙媒体 1 部 電磁的記録媒体 1 部	随時
5	運用報告書(週次)	紙媒体 1 部 電磁的記録媒体 1 部	毎週
6	運用報告書(月次)	紙媒体 1 部 電磁的記録媒体 1 部	毎月
7	情報セキュリティ管理報告書	紙媒体 1 部 電磁的記録媒体 1 部	2023 年 3 月 31 日

2.4.2. 提出方法

(1) 提出物は全て日本語で作成すること。
(2) 用字・用語・記述符号の表記については、「公用文作成の要領(昭和 27 年4月4日内閣閣甲第 16 号内閣官房長官依命通知)」を参考にすること。
(3) 情報処理に関する用語の表記については、日本工業規格(JIS)の規定を参考にすること。
(4) 提出物は紙媒体及び電磁的記録媒体により作成し、センターから特別に示す場合を除き、原則紙媒体1部、電磁的記録媒体1部を提出すること。
(5) 紙媒体による提出について、用紙のサイズは、原則として日本工業規格 A 列 4 番とするが、必要に応じて日本工業規格 A 列 3 番を使用すること。
(6) 電磁的記録媒体による提出は、CD-R 又は DVD-R の媒体に格納して提出すること。
(7) 提出後センターにおいて改変が可能となるよう、図表等の元データも併せて提出すること。
(8) 提出物の作成に当たって、特別なツールを使用する場合は、センターの承認を

得ること。

(9) 提出物が外部に不正に使用されたり、提出過程において改ざんされたりすることのないよう、安全な提出方法を提案し、提出物の情報セキュリティの確保に留意すること。

(10) 電磁的記録媒体により提出する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、提出物に不正プログラムが混入することのないよう、適切に対処すること。また、それを証明する書類を提出すること。

2.4.3. 提出場所

原則として、提出は次の場所において引渡しを行うこと。ただし、センターが提出場所を別途指示する場合はこの限りではない。

センター 総務部 情報セキュリティ室

3.　作業の実施体制・方法に関する事項

3.1.　作業実施体制

受注者に求める作業実施体制は次の図及び表のとおりである。なお、受注者内のチーム編成については想定であり、受注者決定後に協議の上、見直しを行う。

また、受注者は本業務開始時に、本業務に関与するすべての要員の一覧を作成し、センターに提示すること。また、要員を変更する場合、センターの承認を得た上で、速やかに一覧を更新し、提示すること。

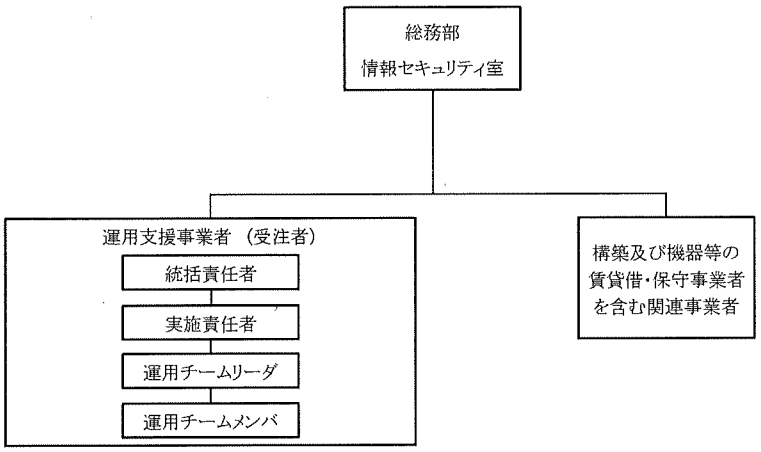

図 3-1 作業実施体制図(想定)

表 3-1 作業実施体制(想定)

No.	要員	役割
1	統括責任者	本業務全体を統括し、必要な意思決定を行う。
2	実施責任者	本業務全体の管理を行い、業務の遂行に必要な意思決定を行う。
3	運用チームリーダ	センターに常駐し、センターで管理する情報システムに関する運用作業の管理を行う。 また、各関連する組織・部門とのコミュニケーション窓口を担う。
4	運用チームメンバ	センターに常駐し、センターで管理する情報システムに関する運用作業を行う。

3.2. 業務に必要な資格等

本業務の作業要員に求める資格及び経験等の要件は次の表のとおりである。

表 3-2 作業要員に求める資格・経験等の要件

No	要員	資格	経験等
1	実施責任者	以下の資格のいずれか一つ以上を有すること。 ① プロジェクトマネージャ(IPA) ② Project Management Professional(PMI) ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある(その根拠を明確に示し、センターの承認を得ること。)。	基盤情報システムと同規模(端末 200 台程度)以上の情報システムの運用プロジェクトにおいて、実施責任者としての経験を有すること。
2	運用チームリーダ	以下の資格のいずれか一つ以上を有すること。 ① システムアーキテクト(IPA) ② ネットワークスペシャリスト(IPA) ③ 情報処理安全確保支援士(IPA) ④ IT サービスマネージャ(IPA) ⑤ ITIL Foundation もしくはその上位資格 ただし、IT スキル標準 V3 2011 に基づき、当該資格保有者等と同等の能力を有することを示した場合は、これを認める場合がある(その根拠を明確に示し、センターの承認を得ること。)。	基盤情報システムと同規模(端末 200 台程度)以上の情報システムの運用プロジェクトにおいて、チームリーダとしての経験を有すること。
3	運用チームメンバ	ー	基盤情報システムと同規模(端末 200 台程度)以上の情報システムの運用プロジェクトの経験を有すること。

IPA:独立行政法人情報処理推進機構

PMI:Project Management Institute

受注者に求める資格等の要件は以下のとおりである。

(1) 品質管理体制について、ISO9001 又は CMMI のレベル 3 以上の認定を受けていること(当該認定を受けていることが確認できる認証の写し等を提出すること。)。なお、事業部単位で認定を受けている場合は、当該事業部が本業務の実施体制に参画することができること。

(2) 情報セキュリティの徹底を図る観点から ISO/IEC27001 の認定を受けていること(当該認定を受けていることが確認できる認証の写し等を提出すること。)。なお、事業部単位で認定を受けている場合は、当該事業部が本業務の実施体制に参

画することができること。

(3) プライバシーマークの使用許諾又は個人情報保護マネジメントシステム(JIS Q 15001)の認定を受けていること。

3.3. 作業の管理に関する要領

(1) 基盤情報システムの運用支援作業について、受注者は、センターが提示する「運用実施要領」に基づき、運用支援業務に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

(2) その他の作業について、センターが承認した「業務運用支援作業実施要領」に基づき、業務運用支援作業に係るコミュニケーション管理、体制管理、作業管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

4. 作業の実施にあたっての遵守事項

4.1. 機密保持、資料の取扱い

受注者は、機密保持や資料の取扱い等について、以下の措置を講ずること。

(1) 業務上知り得た情報は、本業務以外の目的で利用しないこと。

(2) 業務上知り得た情報について第三者への開示や漏えいをしないこと。

(3) 業務上知り得た情報は、センターの許可なく作業場所以外の場所に持出さないこと。

(4) 受注者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合、直ちにセンターに報告すること。また、受注者の責によりセンターに損害が生じた場合に賠償等の責任を負うこと。

(5) 業務の履行中に受け取った情報は管理を行い、業務終了後は返却又は抹消等を行い、復元不可能な状態にすること。

(6) 適切な措置が講じられていることを確認するため、遵守状況の報告を行うこと。また、必要に応じて行うセンターによる実地調査を受け入れること。

4.2. その他の情報セキュリティ対策要件

その他のセキュリティ対策要件を以下に示す。

(1) 受注者は、センターの情報セキュリティポリシー及び情報管理規程(以下、「情報セキュリティ関係規程」という。)を十分に理解し、遵守すること。
(2) 受注者は、本業務の開始時に、本業務に係る情報セキュリティ対策の実施内容及び管理体制について記載した「情報セキュリティ管理計画書」をセンターに提出し、承認を得ること。なお、管理体制において、実施責任者と品質管理責任者の兼務は認めない。
(3) 受注者は、本業務の開始時に受注者の資本関係・役員等の情報、請負事業の実施場所、請負事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報について、センターに書面にて提出し、承認を得ること。
(4) 受注者は、可搬機器について、盗難、不正な持ち出し等の物理的な脅威から保護するため、セキュリティワイヤ等を用いて固定すること。
(5) 受注者は、本業務において情報セキュリティインシデントが発生した場合の対処方法を整備すること。
(6) 受注者は、センターの求めに応じ、情報セキュリティ対策その他の契約の履行状況についてセンターに定期的に報告を行うこと。また、センターの指示に応じて、情報セキュリティ対策に関する監査を受け入れること。
(7) 受注者は、情報セキュリティ対策の履行が不十分な場合、センターと改善について協議を行い、合意した改善策を実施すること。
(8) 受注者は、本業務の一部を再委託する場合、再委託先に上記の措置及び「4.1 機密保持、資料の取扱い」の措置の実施を担保させることで、受注者の責任で情報セキュリティの確保を行うこと。また、再委託先の情報セキュリティ対策状況について、センターに書面にて提出し、承認を得ること。
(9) 受注者は、本業務の終了時に、本業務で実施した情報セキュリティ対策を報告すること。

5. 提出物等の取扱いに関する事項

5.1. 知的財産権の帰属

本業務における知的財産権の帰属に係る要件を以下に示す。

(1) 提出物に関する著作権、著作隣接権、商標権、商品化権、意匠権及び所有権(以下、「著作権等」という。)は、センターが保有するものとする。
(2) 提出物に含まれる受注者又は第三者が権利を有する著作物等(以下、「既存著作物」という。)の著作権等は、個々の著作権者等に帰属するものとする。
(3) 提出物に既存著作物等が含まれる場合には、受注者が当該既存著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。

(4) 本業務の遂行に当たって、第三者が権利を有する著作権、知的財産権等を有するものを使用する場合は、受注者の責任において、その権利の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うこと。

6. 再委託に関する事項

6.1. 再委託の制限及び再委託を認める場合の条件

(1) 本業務の受注者は、業務の大部分を一括して再委託してはならない。
(2) 受注者における統括責任者及び実施責任者を再委託先事業者の社員や契約社員とすることはできない。
(3) 受注者は再委託先の行為について一切の責任を負うものとする。
(4) 再委託を行う場合、再委託先が「3.2 業務に必要な資格等」に示す要件を満たすこと。
(5) 再委託先における情報セキュリティの確保については受注者の責任とする。

6.2. 承認手続

(1) 本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した再委託承認申請書をセンターに提出し、あらかじめ承認を受けること。
(2) 前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面をセンターに提出し、承認を受けること。
(3) 再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合(以下「再々委託」という。)には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

6.3. 再委託先の契約違反等

再委託先において、本仕様書の「6.1.再委託の制限及び再委託を認める場合の条件」から「6.2.承認手続」に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、センターは、当該再委託先への再委託の中止を請求することができる。再々委託先についても同様とする。

7. その他特記事項

本件受注後に仕様書(「別紙 1 運用作業一覧」を含む。)の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもってセンターに申し入れを行うこと。双方の協議において、その変更内容が軽微(契約金額、納期に影響を及ぼさない)かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

8. 附属資料

(1) 別紙1 運用作業一覧

(2) 別紙2 用語の定義

(3) 閲覧要領

閲覧対象とする資料は以下のとおり。

① 基盤情報システムに係る以下の資料

(ア) 要件定義書

(イ) 基本設計書

(ウ) 運用計画

(エ) 運用実施要領

(オ) 運用手順書

(カ) 保守計画

(キ) 保守実施要領

(ク) 保守手順書

② 情報セキュリティポリシー

③ 情報管理規程

④ 情報管理要領

別紙 1

運用作業一覧

2022 年度

公益財団法人　核物質管理センター

— 目次 —

1. 基盤情報システムの運用作業

運用支援事業者は、基盤情報システムの構築事業者が作成する「運用計画」、「運用実施要領」及び「運用手順書」に基づき、以下に示す基盤情報システムの運用作業を実施すること。

1.1. 作業条件

運用作業の条件を以下に示す。

1.1.1. 対応時間、実施頻度

各作業の対応時間及び実施頻度を以下に示す。

表 1-1 各運用作業の対応時間及び実施頻度

No.	作業分類	作業項目	対応時間	実施頻度	補足
1	運転管理・監視等業務	死活監視	平日 9:00～17:30(※1)	常時	基盤情報システムの自動監視・管理機能を利用して実施
2		リソース監視			
3		セキュリティ監視			
4		バックアップ管理			
5		ログ管理			
6		問題・インシデント対応		随時	監視等により異常を検知した場合に実施
7		ソフトウェア脆弱性管理		日次	
8		計画停止	休日又は平日 9:00～17:30 以外の時間帯	随時	インシデント対応、セキュリティパッチの適用作業等に対応
9		構成管理	平日 9:00～17:30	随時	システム構成の変更時に実施

※1:対応時間外の作業が必要な場合はセンターと協議し、作業時間等について合意を得た上で作業を行うこと。

1.1.2. 作業場所・作業環境

(1) センターの東京本部に常駐の上、作業を実施すること。ただし、センターからの指示があった場合は、東海センター、六ヶ所センターでの現地作業またはテレワーク(在宅などセンターが認めた場所)による作業を実施すること。

(2) 運用作業の実施に当たっては、センターが用意する基盤情報システムの「運用支援端末」(6台程度)を利用すること。

1.2. 運転管理・監視等要件

基盤情報システムの運転管理・監視等に係る作業要件を以下に示す。

1.2.1. 死活監視

基盤情報システムを構成する機器類の稼動状況を監視し、障害の発生を早期検知するため、以下の監視を実施すること。

なお、監視の実施に当たっては、基盤情報システムの「システム運用管理サービス」による統合監視環境のクライアントソフトウェアを利用すること。

(1) 監視対象

死活監視の対象は、基盤情報システムを構成するハードウェア(サーバ装置、サーバ周辺機器、ネットワーク機器等)とすること。

(2) 監視内容

以下の監視を行い、「システム運用管理サービス」のアラート等により異常を検知した際はセンターの担当者へ報告すること。

① 定期的なポーリング等により、基盤情報システムのハードウェアの異常・障害を検知すること。
② ハードウェアの異常時等に発行されるSNMPトラップを検知すること。
③ ハードウェア及びソフトウェア製品から出力されるログを監視し、エラー等を検知すること。
④ サーバ装置に搭載するソフトウェア製品のプロセス(サービス)を監視し、プロセスダウンを検知すること。

1.2.2. リソース監視

基盤情報システムを構成する機器類の稼動状況を監視し、リソースの不足・逼迫等を検知するため、以下の作業を実施すること。

なお、監視の実施に当たっては、基盤情報システムの「システム運用管理サービス」による統合監視環境のクライアントソフトウェアを利用すること。

(1) 監視対象

リソース監視の対象は、基盤情報システムを構成するハードウェアとすること。

(2) 監視内容

以下の監視を行い、「システム運用管理サービス」のアラート等により異常やリソース不足を検知した際はセンターの担当者へ報告すること。

① CPU 使用率、メモリ使用率、ハードディスク空き容量、ネットワーク帯域等のリソースを監視し、しきい値を超えた場合に検知すること。

1.2.3. セキュリティ監視

基盤情報システムの情報セキュリティに関する事象の発生を監視し、情報セキュリティ上の脅威を早期検知するため、以下の作業を実施すること。

なお、監視の実施に当たっては、基盤情報システムの「システム運用管理サービス」による統合監視環境のクライアントソフトウェア、「端末管理サービス」による統合端末管理環境のクライアントソフトウェア、センターのウイルス対策管理サーバの機能等を利用すること。

(1) 監視対象

セキュリティ監視の対象は、基盤情報システムを構成するサーバ装置及びネットワーク機器とすること。

(2) 監視内容

以下の監視を行い、「システム運用管理サービス」等のアラート等により異常を検知した際はセンターの担当者へ報告すること。

① ファイアウォールにおけるブロックの発生状況を監視し、異常を検知すること。
② 統合認証サービス等における認証の失敗状況を監視し、異常を検知すること。
③ サーバ装置及びクライアント端末の不正プログラム検知状況を監視し、異常を検知すること

1.2.4. バックアップ管理

基盤情報システムのバックアップを取得・管理し、障害・災害時に基盤情報システムを復旧可能とするため、以下の作業を実施すること。

なお、バックアップ管理の実施に当たっては、基盤情報システムの「バックアップ管理サービス」の機能を利用すること。

(1) 管理対象

バックアップ管理の対象は、基盤情報システムを構成するハードウェアとすること。

(2) 作業内容

作業内容の要件を以下に示す。

① 「バックアップ管理サービス」のスケジュール設定等を利用し、バックアップ対象データに対し、定期的にバックアップデータを取得すること。
② バックアップデータについて、必要な世代管理を行うこと。
③ ハードウェアの故障やデータ破壊が発生した場合、必要に応じて、バックアップデータからの復旧作業を行うこと。なお、復旧作業は「1.2.6 問題・インシデント対応」に基づいて対応すること。

1.2.5. ログ管理

基盤情報システムのログ監視や証跡管理等を行うため、ログ管理に係る以下の作業を行うこと。

なお、ログ管理の実施に当たっては、基盤情報システムの「ログ管理サービス」の機能を利用すること。

(1) 管理対象

ログ取得の対象は、基盤情報システムを構成するサーバ装置及びネットワーク機器とすること。管理対象ログファイルを以下に示す。

表 1-2 管理対象ログファイル

No.	対象ログファイル	概要及び用途	保管期間
1	ソフトウェアログ	・ OS やソフトウェア等の動作に伴い出力されるログファイル。障害発生時の原因特定や追跡調査の際に利用する。	最低 1 年間
2	証跡管理用ログ	・ 情報セキュリティインシデント発生時に原因の特定、追跡調査、及び点検等に用いる。	最低 1 年間
3	性能情報	・ サーバ装置の稼動統計情報が記録されたログファイル。リソース使用状況の確認に利用する。	最低 1 年間

(2) 作業内容

作業内容の要件を以下に示す。

① 基盤情報システムの「ログ管理サービス」により、管理対象ログの収集及び蓄積を行うとともに、正常にログを収集・蓄積できていることを定期的に確認すること。
② センターからの求めに応じて、蓄積されたログに対して「ログ管理サービス」の機能を用いて集計・解析等を行い、結果をセンターに報告すること。
③ 蓄積したログは必要に応じて、基盤情報システムのバックアップ装置（ディスクアレイ装置、テープライブラリ装置等）へのアーカイブを行うこと。

1.2.6.　問題・インシデント対応

基盤情報システムの異常や問題等を検知した際は、以下の要件に基づき必要な対応を行うこと。

(1) 以下の例に示す異常、障害、問題等（以下「インシデント」という。）を検知した場合は、センターに報告すること。
- 死活監視により、基盤情報システムの異常、障害等を検知した場合
- リソース監視により、基盤情報システムのリソース不足を検知した場合
- セキュリティ監視により、情報セキュリティ上の不審動作やウイルス感染等を検知した場合
- バックアップ管理により、バックアップの異常、失敗等を検知した場合
- ソフトウェア脆弱性管理により、基盤情報システムに関係のある脆弱性情報やバージョンアップ情報を入手した場合
- データ破損等により、バックアップデータからのリカバリが必要となった場合
- その他、基盤情報システムに関連する問題が発生した場合

(2) 発生したインシデントに対し、センターと協議の上で当該事象の調査、発生原因の調査、対応方法の検討及び復旧対応を行うこと。この際、必要に応じて基盤情報システムの保守事業者への連絡・確認を行うこと。

(3) インシデントへの対応完了後には、当該インシデントの発生経緯、原因、復旧作業、再発防止策等について取りまとめた報告書を作成し、センターの確認を受けること。

(4) インシデントに対する再発防止策のうち、運用支援事業者で対応可能な事項（基盤情報システムの設定変更、運用手順の変更等）については、センターと協議の上で実施すること。

1.2.7.　ソフトウェア脆弱性管理

基盤情報システムのソフトウェア製品の脆弱性情報を収集し、必要に応じてセキュリティパッチを適用することで基盤情報システムの情報セキュリティを確保するため、以下の作業を実施すること。

(1) 管理対象

ソフトウェア脆弱性管理、バージョンアップ対応の対象は、基盤情報システムを構成するサーバ装置、端末及びネットワーク機器で利用するソフトウェアとすること。

(2) 作業内容

作業内容の要件を以下に示す。

① サーバ装置、端末及びネットワーク機器で利用するソフトウェアにおける脆弱性対策の状況(脆弱性の公開情報及び製造元によるセキュリティパッチの公開状況等)を定期的に確認すること。
② 脆弱性対策状況の確認によって脆弱性情報を入手した場合、センター及び保守事業者への報告を行うこと。
③ 保守事業者から受領する手順及び必要な電子ファイルを基にバージョンアップ対応をすること。
④ 上記の対応の結果、基盤情報システムが正常に動作していることを確認すること。
⑤ 対応日時、対応内容等について報告書を作成し、センターに報告すること。

1.2.8. 計画停止

障害対応やセキュリティパッチの適用のために計画停止を行う必要がある場合は、センターと協議の上で以下の要件に基づき計画停止を行うこと。

(1) 問題・インシデント対応やセキュリティパッチの適用等を目的として、計画停止の必要がある場合、作業計画を策定し、センターの承認を得ること。
(2) 作業計画には、計画停止中に行う作業の切り戻しのための判断基準、期限、手順等を記載すること。
(3) 作業計画に基づき、機器類又はソフトウェアの停止による計画停止を行い、必要な作業を実施すること。
(4) 作業実績等を取りまとめた報告書を作成し、センターへ提出すること。

1.2.9. 構成管理

基盤情報システムを構成するハードウェア、ソフトウェア、ネットワークについて、以下の要件に基づく構成情報の管理を行うこと。

(1) 管理対象

構成管理の対象は、基盤情報システムを構成するサーバ装置及びネットワーク機器とすること。

構成管理における管理対象は以下に示す例に基づき、センターの承認を得た上で定めること。

表 1-3 管理対象

No.	資産	管理項目(例)	整備するドキュメント(例)
1	ハードウェア	メーカ名、品番、シリアル番号、数量、設置場所、OS、バージョン、実装メモリ、ハードディスク容量、MAC アドレス、IP アドレス 等	・ ハードウェア一覧 ・ ハードウェア構成図
2	ソフトウェア	名称、バージョン、数量、契約ライセンス数、サポート期限、使用済ライセンス数、媒体保管場所 等	・ ソフトウェア一覧 ・ ハードウェアとソフトウェアの関連図
3	ネットワーク	ネットワーク種類、帯域、設定情報等	・ ネットワーク接続構成図 ・ ネットワーク機器構成図
4	その他(ケーブル、消耗品等)	名称、対応する機器 等	・ 消耗品一覧

(2) 対応内容

構成管理における対応内容の要件を以下に示す。

① 基盤情報システムを構成するハードウェア、ソフトウェア、ネットワーク等の各資産を台帳等により記録し、適切に管理すること。

② 基盤情報システムの構成を変更した際には、変更内容等の情報をセンターに報告し、それらの情報を更新すること。

2. 業務運用支援作業

情報セキュリティ室の業務を支援するための、業務運用支援の要件を以下に示す。

運用支援事業者は、本項に定める事項の他、機器の設定情報、マニュアル、機器取扱説明書等を充分理解のうえ実施するものとし、あらかじめ業務の分担、人員配置、スケジュール、実施方法等について実施要領を定めセンターの確認を受けること。

2.1. 定常業務

2.1.1. 日次チェック

センターが所管する既存システム(基盤情報システムに含まれないサーバ装置等)について、日次チェックシート等を用いて以下の事項を日次で確認すること。なお、作業に用いる日次チェックシートは運用支援事業者にて作成の上で、センターの合意を得ること。

(1) ログの確認

① サーバ装置、ネットワーク機器等のログ(syslog)の出力内容、レベル(情報/警告/重大/エラー等)別の出力件数等を確認・記録し、異常を検知した場合はセンターの担当者に報告すること。

② ログの確認は、センターが指定する機器(最大 10 台程度)を対象とすること。

(2) ディスク空き容量の確認

① サーバ装置等のディスクの空き容量を確認・記録し、容量の逼迫等を検知した場合はセンターの担当者に報告すること。

② ディスク空き容量の確認は、センターが指定するサーバ装置(最大 10 台程度)を対象とすること。

(3) ウイルス対策ソフトウェアの更新確認

① センターが使用するウイルス対策ソフトウェア(3 種類程度)のパターンファイル(ウイルス定義ファイル)の更新状況を確認・記録すること。

② パターンファイルの更新があった場合には、ウイルス対策ソフトウェアが導入されているセンターの各種端末・サーバ装置への適用を実施するとともに、適用状況を確認・記録すること。

③ パターンファイルの適用対象は、以下とすること。

- ウイルス対策管理サーバ(オープン環境、1 台)
- ウイルス対策管理サーバ(クローズド環境、1 台)
- 東京本部に設置されているウイルススキャン端末(スタンドアロン環境、数台程度)

④ 東海センター及び六ヶ所センターに設置されているウイルススキャン端末(スタンドアロン環境)に対しては、現地の職員がパターンファイルの適用を実施するため、パターンファイルの提供、作業手順の連絡等の支援を実施すること。

(4) 情報セキュリティ関連情報の確認

(1) センターが別途契約しているセキュリティ監視サービス(SOC によるセキュリティ常時監視サービス、IPS 監視サービス等)からの日次報告をセンターより受領し、確認・記録すること。

(2) テレワーク環境監視サービス(マネージド EDR サービスによる監視)からの報告をセンターより受領し、確認・記録する。

(3) JPCERT/CC 等により公開された脆弱性情報を確認し、センターの既存システムで利用しているハードウェア・ソフトウェア等への影響がある情報について、センターの担当者へ報告すること。

(4) SHODAN(https://www.shodan.io/)等のインターネット接続機器検索サービスを利用し、意図せずインターネット上に公開されているセンターの機器・装置等がないかを確認・記録すること。

2.1.2. その他の定常業務

(1) セキュリティパッチの適用

① センターの既存システムで利用しているハードウェア・ソフトウェア等のセキュリティパッチ(セキュリティアップデートを含む。)の情報が公開された際に、当該パッチファイルを入手し、関係する既存システムへのパッチ適用を実施すること。

② セキュリティパッチの適用に当たっては、事前に既存システムへの影響度を調査した上で、適用可否を判断すること。その際、必要に応じて当該既存システムの保守事業者に、パッチ適用可否、作業手順等を確認すること。

(2) セキュリティ監視サービスからの月次報告への対応

センターが別途契約しているセキュリティ監視サービス(SOC によるセキュリティ常時監視サービス、IPS 監視サービス等)からの月次報告を確認し、当該報告への対応を支援すること。

(3) 既存システムの設定変更

センターからの求めに応じて、センターが管理する既存システムの設定変更作業を実施すること。なお、設定変更を行う主な対象及び実施頻度を表 2-1 主な設定変更対象及び実施頻度に示す。

表 2-1 主な設定変更対象及び実施頻度

No.	対象	設定変更例	実施頻度
1	統合認証サービス	アカウントの登録・変更・削除、権限の変更、グループポリシーの変更	随時 (月 1 回程度を想定)
2	外部 DNS サービス	レコードの設定変更	随時 (年 1 回程度を想定)
3	内部 DNS サービス	レコードの設定変更	随時 (年 1 回程度を想定)
4	ファイル共有サービス	アクセス権限の変更、記憶領域の追加割当	随時 (月 1 回程度を想定)
5	外部メールサービス	メールアカウントの設定の変更	随時 (月 1 回程度を想定)
6	内部メールサービス	メールアカウントの設定の変更	随時 (月 1 回程度を想定)
7	端末管理サービス	管理対象の追加・変更・削除、デバイス管理の設定の変更	随時 (月 1 回程度を想定)
8	ログ管理サービス	保存対象の変更、保存期間の変更	随時 (年 1 回程度を想定)
9	サーバ装置の設定変更	各種サーバの設定変更等	随時 (年 1 回程度を想定)
10	ネットワーク機器及びセキュリティ機器	不正通信元 IP アドレスからの通信遮断 等	随時 (月 1 回程度を想定)
11	各種ソフトウェア製品	ウイルス対策ソフトウェアの検索エンジンのアップデート、Web 接続先のフィルタ設定	随時 (年 1 回程度を想定)

(4) PC 端末交換時の初期設定作業

① PC 端末(職員用端末、セキュアメール端末、ウイルススキャン端末等)の故障等により交換が必要となった場合に、予備機に対して必要な初期設定(アカウント設定、ネットワーク設定、ライセンス設定等)を行い、端末の交換対応を行うこと。ただし、予備端末の OS 及び標準ソフトウェアのインストール等のキッティング作業については保守事業者により実施する。

② PC 端末の交換時の初期設定作業を効率的に行うために、必要に応じて端末のシステムバックアップ等の取得・管理を行うこと。

2.2. 定常外業務

2.2.1. 情報セキュリティインシデント対応支援

(1) インシデント検知時の対応支援

① ウイルス対策ソフトウェアによる検知、セキュリティ監視サービスからのイベント検知、マネージド EDR サービスからのイベント検知等が発生した場合、ウイルス対策ソフトウェアの提供ベンダやセキュリティ監視サービス会社への連絡・確認を行うとともに、当該検知内容への対応を支援すること。

② ファイアウォール、不正アクセス検知機器、等により不審な通信を検知した場合、当該通信元の調査及び通信の遮断設定等の対応を実施すること。

③ その他、情報セキュリティインシデント発生時に、ログ情報の調査等の証跡確認支援、関係するシステムの保守事業者への連絡・確認支援を実施すること。

(2) 原因調査及び再発防止策の検討支援

センターが情報セキュリティインシデントの原因調査及び再発防止策の検討を実施するに当たり、情報システムの調査、公開情報の調査、情報提供等の技術的支援を実施すること。

3. その他支援作業

(1) ヘルプデスク支援業務

① 情報セキュリティ室の職員がセンターの職員から質問を受け付けた際に、回答・助言等の支援を行うこと。

② ヘルプデスク支援における情報セキュリティ室からの問合せ内容、回答・助言内容、対応内容等を記録し、管理すること。

(2) 外部発注業者との打合せ支援

センターが他の外部発注業者との打合せを行う際、センターからの求めに応じて、同席、助言、情報提供等の技術的支援を行うこと。

(3) 情報セキュリティ対策の検討・導入支援

センターが情報セキュリティ対策の導入等について検討する際、センターからの求めに応じて、助言、情報提供等の技術的支援を行うこと。

(4) ログ情報等の現地収集

東海センター又は六ヶ所センターのスタンドアロン環境等のログ情報や設定情報等を収集する必要が生じた際は、現地での情報収集作業を実施すること。

(5) その他

その他、上記に付随する作業でセンターとの協議により定められた作業を実施すること。

4. 運用実績の報告

「1. 基盤情報システムの運用作業」及び「2. 業務運用支援作業」において実施した作業について、報告資料を作成し、週次及び月次の頻度で報告を行うこと。なお、報告内容の詳細は、受託後にセンターと協議の上で定めること。

各作業の報告内容の例及び報告頻度を以下に示す。

表 4-1 基盤情報システムの運用に係る報告内容

No.	作業項目	報告内容(例)	報告頻度	
			週次	月次
1	死活監視	・ システムの稼働率 ・ 異常検知数 ・ 異常検知を報告するまでの時間 ・ システム停止回数 ・ システム停止時間	-	○
2	リソース監視	・ ハードディスク空き容量 ・ メモリ使用率 ・ CPU 稼働率 ・ 通信速度の推移	-	○
3	セキュリティ監視	・ ファイアウォールのブロック件数 ・ 統合認証サービスへのログイン失敗件数 ・ 不正プログラムの検知回数 ・ セキュリティ事故件数	○	○
4	問題・インシデント対応	・ 対応実績及び直近の対応予定	○	○
5	ソフトウェアの脆弱管理	・ 脆弱性対策の状況	-	○
6	構成管理	・ 基盤情報システムの構成の変更内容	-	○

表 4-2 業務運用支援作業に係る報告内容

No.	作業項目	報告内容(例)	報告頻度	
			週次	月次
1	日次チェック	・ 日次チェックにおける異常検知件数、対応実績等	○	○
2	その他定常業務	・ セキュリティパッチの適用実績 ・ セキュリティ監視サービスからの月次報告への対応実績 ・ 情報システムの設定変更実績 ・ ヘルプデスクの問合せ件数、対応実績等	○	○
3	情報セキュリティインシデント対応支援	・ 情報セキュリティインシデントへの対応実績等	○	○
4	その他支援作業	・ 情報セキュリティ対策の検討・導入支援に係る報告等	-	○

別紙2 用語の定義

No.	分類	用語	定義
1	新情報システムにより提供するサービス	LANサービス	各拠点内のPC端末、システム等がクローズド系ネットワークに接続するためのLAN回線を提供するサービスのこと。
2		WAN高速化サービス	ファイル転送の性能向上及び帯域制御のためのWAN高速化機能を提供するサービスのこと。
3		統合認証サービス	ActiveDirectoryによる統合認証を提供するサービスのこと。
4		Windowsアップデート管理サービス	WSUS(Windows Server Update Services)によるWindows Updateサービスを提供するサービスのこと。
5		内部DNSサービス	職員向けのクローズド系ネットワーク内部のアドレスを管理するDNSサービスのこと。
6		仮想デスクトップサービス	職員や運用支援事業者がインターネット環境(Web閲覧、メール送受信等)を利用するための仮想デスクトップ(VDI)を提供するサービスのこと。
7		ファイル共有サービス	職員向けのファイル共有サーバ機能を提供するサービスのこと。
8		内部メールサービス	職員向けのクローズド系ネットワーク用電子メールサーバ機能を提供するサービスのこと。
9		端末管理サービス	新情報システムの各端末を一元管理するための機能(情報資産管理、構成管理、デバイス管理等)を提供するサービスのこと。
10		システム運用管理サービス	新情報システムのハードウェア、ソフトウェア及びネットワークの統合運用管理・監視機能を提供するサービスのこと。
11		バックアップ管理サービス	新情報システムの各サービスのバックアップを一元管理するための機能を提供するサービスのこと。
12		ログ管理サービス	新情報システムの各機器が出力するログの管理機能を提供するサービスのこと。
13		職員用端末	センター職員が業務を行うため、全職員に配布される端末のこと。
14		セキュアメール端末	S/MIMEによるセキュアメールの送受信を行うための端末のこと。
15		ウイルススキャン用端末	USBメモリや光学メディア等からデータの読込みを行う際のウイルススキャンを行うための端末のこと。
16		運用支援端末	運用支援事業者が本システムを運用・管理するための端末のこと。
17	その他サービス	外部DNSサービス	新情報システムのアドレスを管理し、センター外部にサービスを提供するDNSサービスのこと。
18		外部メールサービス	センター外部とのメール送受信を行うために使用するメールサービスのこと。
19	拠点	東京本部	東京都台東区にある、センターの本部のこと。
20		東海センター	茨城県那珂郡東海村にある、東海保障措置センターのこと。
21		六ケ所センター	青森県上北郡六ケ所村にある、六ケ所保障措置センターのこと。
22		外部データセンター	基盤サービスを提供するためのサーバ装置等を配置するデータセンターのこと。
23	ネットワーク	オープン系ネットワーク	センターのネットワークのうち、インターネットへの接続を持つネットワークのこと。
24		クローズド系ネットワーク	センターのネットワークのうち、インターネットへの接続を持たないネットワークのこと。オープン系ネットワークとは仮想分離ファイアウォールを介して接続される。
25	事業者	構築事業者	新情報システムの設計・構築・テスト・移行等を実施した事業者のこと。 「次期基情報システムの構築及び機器等の賃貸借・保守業務」の受託者である。
26		保守事業者	新情報システムの機器等の賃貸借・保守を実施する事業者のこと。 「次期基情報システムの構築及び機器等の賃貸借・保守業務」の受託者である。
27		構築及び機器等の賃貸借・保守事業者	上記の保守事業者及び構築事業者のこと。 「次期基盤情報システムの構築及び機器等の賃貸借・保守業務」の受託者である。
28		運用支援事業者	本調達案件の受託者。 新情報システムを含む情報システムの運用支援業務を行う。