情報システムの脆弱性対策及び認証基盤運用等に関する請負業務

仕様書

目次

添付資料

(1) 別紙１　情報システムの脆弱性対策に関する業務の内容
(2) 別紙２　認証基盤運用に関する業務の内容
(3) 別紙３　事業継続対策に関する業務の内容
(4) 別紙４　産業財産権特約条項
(5) 別紙５　情報セキュリティ強化に係る特約条項
(6) 様式１情報システムの脆弱性対策及び認証基盤運用等に関する請負業務　要員経歴書

１．目的

本仕様書は、国立研究開発法人日本原子力研究開発機構（以下「機構」という）の情報システムの安定運用に不可欠な情報セキュリティ上の脆弱性対策、認証基盤運用、及び事業継続対策に係る業務を請負者に請負わせるための仕様を定めたものである。

本件は、情報システムの脆弱性対策、認証基盤運用、及び事業継続対策に係る業務を効率的かつ円滑に実施するものであり、請負者は情報セキュリティ上の脅威や脆弱性の現状、アクセス管理の一元化・効率化を図る認証基盤、及び非常時の事業継続対策について十分理解し、本業務を実施するものとする。

２．契約範囲

(1) 情報システムの脆弱性対策に関する業務
(2) 認証基盤運用に関する業務
(3) 事業継続対策に関する業務
(4) 上記に付随する作業で機構との協議により定められた作業

３．対象設備等

本業務の対象となる主な装置、設備は以下のとおりである。なお、対象設備は交換等により変更することがある。

3.1 情報システムの脆弱性対策に関連する機器等

(1) 情報セキュリティ対策機器のログ分析システム	1式
(2) 情報システム脆弱性スキャンシステム	1式
(3) 更新プログラム一括管理・配布システム	1式
(4) 海外事務所 UTM（総合脅威管理）システム	1式

3.2 認証基盤関連の機器

(1) Microsoft 365 システム（うち、Entra ID、Intune）	1式

3.3 事業継続対策関連の機器等

(1) データバックアップシステム	1式

４．実施場所

本仕様書に定める業務を実施する場所は、以下のとおりとする。

(1)原子力科学研究所　情報交流棟
〒319-1195 茨城県那珂郡東海村白方 2-4

(2)その他、統括責任者と事前に協議して定めた場所

(3)業務は、上記（1）～（2）に定める場所で行う。ただし、原子力機構が求める場合には、別の場所で業務を行うことがある。別の場所で業務を行うことにより発生した出張経費は、契約書別紙に基づき支払う。

５．実施期日等

機構の施設管理、情報管理等を鑑み、本仕様書に定める業務は以下の期間及び時間で実施することとする。

(1) 実施期間

令和 8 年 4 月 1 日から令和 9 年 3 月 31 日まで。

ただし、土曜日、日曜日、祝日、年末年始（12 月 29 日～翌年 1 月 3 日まで)、機構創立記念日（10 月の第 1 金曜日とする。ただし、10 月 1 日が金曜日の場合は、10 月 8 日とする。）、その他機構が特に指定する日を除く。

(2) 標準実施時間

原則として次の時間帯に実施する。

平日　9:00～17:30

定常外において 6. に定める定常外業務を行うことにより発生した経費は、契約書別紙に基づき支払う。

６．業務内容

本業務を実施するにあたっては、本仕様書に定める事項の他、各機器のマニュアル、取扱説明書等を十分理解のうえ実施するものとし、請負者は予め業務の分担、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、機構の確認を受けるものとする。本業務の詳細な内容は別紙 1～3 に示す。

業務内容	作業頻度
(1)情報システムの脆弱性対策に関する業務（業務内容の詳細は別紙 1）	
1) 情報リスクマネジメントに関する業務 ①脅威の特定 ②脅威分析 ③リスク低減策の検討 ④リスク低減措置の実施	72 hr
2) 情報セキュリティ対策機器のログ分析に関する業務 ①相関分析ルールの開発 ②独自ブラックリストの開発 ③リアルタイム分析 ④ログ分析システムの管理、運用	72 hr
3) 情報システムの脆弱性検査に関する業務 ①検査計画書の作成、被検査部署との調整 ②脆弱性検査 ③課題分析、対策提言 ④脆弱性スキャンシステムの管理、運用	1200 hr
4) 更新プログラムの一括管理・配布に関する業務 ①更新プログラム一括管理・配布システムの管理、運用	1200 hr

②システム監視、障害対応	
5) 海外事務所の脆弱性対応に関する業務 ①海外事務所 UTM システムの管理、運用 ②通信制御要件の設計、実装 ③海外事務所担当部署との調整業務	120 hr
6) その他 ①リスク分析に関する相談対応 ②関係個所との連絡打合せ ③情報セキュリティに関する動向調査、分析 ④IT アーキテクチャ設計に関する最新技術や産業動向の関する調査、分析	72 hr
(2) 認証基盤運用に関する業務（業務内容の詳細は別紙 2）	
1) 認証基盤の運用に関する業務 ①エンタープライズアプリケーション、シングルサインオンの実装支援、運用 ②条件付きアクセス、多要素認証、管理者アカウント管理の実装支援、運用 ③モバイルデバイス管理の実装支援、運用	480 hr
2) その他 ①不審ログインの監視、障害対応、利用者対応	48 hr
(3) 事業継続対策に関する業務（業務内容の詳細は別紙 3）	
1)データバックアップシステムの稼働維持に関する業務 ①バックアップシステムの検討と要件定義 ②管理用サーバ、バックアップアプライアンスの管理、運用 ③Firewall の管理、運用 ④システム接続用ネットワーク（SW、UPS 含む）の管理、運用	240 hr
2) その他 ①関係個所との連絡打合せ ②運用計画・稼働状況に関する資料及び、運用管理マニュアルの作成・修正 ③情報セキュリティ対策に係る作業 ④障害・保守・停電対応	48 hr
(4) 上記に付随する作業で機構との協議により定められた作業	
1) 機構監督員及び総括責任者の協議･調整により決定した業務	協議により定められた時期

※定常外業務

1)トラブル発生時の対応（各システム等において、トラブル等緊急を要する対応が

必要となった場合）

2)地震等の災害発生時の対応（地震発生時の現場点検、その他災害時の対応）

7．受注者と機構の主な役割分担

7.1 定常作業

業務内容	受注者	原子力機構
(1) 情報システムの脆弱性対策に関する業務		
1)情報リスクマネジメントに関する業務 ①脅威の特定 ②脅威分析 ③リスク低減策の検討 ④リスク低減措置の実施	・脅威の特定、分析 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認
2)情報セキュリティ対策システムのログ分析に関する業務 ①相関分析ルールの開発 ②独自ブラックリストの開発 ③リアルタイム分析 ④ログ分析システムの管理、運用	・システムの管理、運用 ・障害及び保守情報の把握 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認
3)脆弱性検査に関する業務 ①検査計画書の作成、被検査部署との調整 ②脆弱性検査 ③課題分析、対策提言 ④脆弱性スキャンシステムの管理、運用	・システムの管理、運用 ・障害及び保守情報の把握 ・検査レポートの作成 ・利用者対応 ・業務報告書の作成	・業務報告書の確認
4)更新プログラムの一括管理・配布に関する業務 ①更新プログラム一括管理・配布システムの管理、運用 ②システム監視、障害対応	・システムの管理、運用 ・障害及び保守情報の把握 ・運用資料の作成 ・利用者対応 ・業務報告書の作成	・業務報告書の確認
5)海外事務所の脆弱性対応に関する業務 ①海外事務所 UTM システムの管理、運用 ②通信制御要件の設計、実装	・機器の管理、運用 ・障害及び保守情報の把握 ・運用資料の作成 ・利用者対応 ・業務報告書の作成	・業務報告書の確認
6)その他 ①リスク分析に関する相談対応 ②関係個所との連絡打合せ ③情報セキュリティに関する動向調査、分析	・利用者対応 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認

④IT アーキテクチャ設計に関する最新技術や産業動向の関する調査、分析		
(2) 認証基盤運用に関する業務		
1) 認証基盤の運用に関する業務 ①エンタープライズアプリケーション、シングルサインオンの実装支援、運用 ②条件付きアクセス、多要素認証、管理者アカウント管理の実装支援、運用 ③モバイルデバイス管理の実装支援、運用	・システムの管理、運用 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認
2) その他 ①不審ログインの監視、障害対応、利用者対応	・利用者対応 ・障害及び保守情報の把握 ・業務報告書の作成	・業務報告書の確認
(3) 事業継続対策に関する業務		
1) データバックアップシステムの稼働維持に関する業務 ①バックアップシステムの検討と要件定義 ②管理用サーバ、バックアップアプライアンスの管理、運用 ③Firewall の管理、運用 ④システム接続用ネットワーク（SW、UPS 含む）の管理、運用	・システムの管理、運用 ・障害及び保守情報の把握 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認
2) その他 ①関係個所との連絡打合せ ②運用計画・稼働状況に関する資料及び、運用管理マニュアルの作成・修正 ③情報セキュリティ対策に係る作業 ④障害・保守・停電対応	・利用者対応 ・運用資料の作成 ・業務報告書の作成	・業務報告書の確認

7.2 定常外作業

業務内容	受注者	原子力機構
a.トラブル発生時の対応（において、トラブル等緊急を要する対応が必要となった場合）	・トラブル発生時の対応 ・作業計画書、作業報告書の作成、提出	・指示書の作成 ・作業計画書、作業報告書の確認
b.地震等の災害発生時の対応（地震発	・地震等の災害発生時の	・指示書の作

生時の現場点検、その他災害時の対応）	対応 ・点検記録の作成、提出	成 ・点検記録の確認

８．実施体制及び業務に従事する標準要員数

受注者は機構が原子力の研究・開発を行う機関であるため、高い技術力及び信頼性を社会的に求められていることを認識し、機構の関係法令及び規程等を遵守し安全性に配慮し業務を遂行しうる能力を有する者を従事させること。

(1) 実施体制

受注者は、業務を確実に実施できる体制をとるとともに、以下に示す体制をとること。

① 総括責任者及び代表者を専任すること。

② 総括責任者及び代表者は、次の任務に当たらせること。

1) 受注者の従事者の労務管理（要員の人員調整を含む）及び作業上の指揮命令

2) 本契約業務履行に関する機構との連絡及び調整

3) 受注者の従事者の規律秩序の保持並びにその他本契約業務の処理に関する事項

③ 総括責任者は、常時連絡をとれる状態とすること。

④ ４項「実施場所」に必要な要員を常駐させること。

⑤ トラブル発生時に迅速な原因究明、復旧の対応がとれる総合的な体制を有していること。

(2) 業務に従事する標準要員数

情報システムの脆弱性対策及び認証基盤運用等に関する請負業務　2 名程度（年間の業務量）※

※４．に定める実施場所に常駐して業務を実施する業務量を標準要員数（目安）として記載。要員の配置等については、日々常に業務の完全な履行をなし得るように適切な役割の要員を配置し、実施すること。

※ 想定する要員クラスは、「８．業務に必要な資格等」に記載する。

９．業務に必要な資格等

各業務の従事者は、以下の要件①～⑧のいずれか５項目以上を有し、かつ、各業務の従事者を組み合わせて要件①～⑧の全項目を有すること。経験年数は、令和 8 年 3 月 31 日現在とする。

情報システムの脆弱性対策及び認証基盤運用等に関する請負業務

技術者 S（2 名）

① 情報リスクマネジメントの業務経験：　10 年以上

② SIM/SIEM の業務経験：　8 年以上

③ 侵入検査の業務経験：　8 年以上

④ Firewall の運用経験：　8 年以上

⑤ RDBMS の運用経験：　8 年以上

⑥ Linux 及び Windows サーバの運用経験：　8 年以上

⑦ 仮想化サーバの運用経験： 8年以上
⑧ Active Directory 及び WSUS の運用経験 8年以上

１０．技術等の要求要件

(1) 事業者の信頼性に関する事項

資本関係・役員の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修等）・実績及び国籍についての情報を提示すること。

(2) 業務の実施体制に関する事項

① 業務責任体制（統括責任者名、総括責任者代理名、業務担当者名、業務担当者の実績・保有資格、統括責任者と業務担当者の役割分担、機構との連絡体制）を提示すること。

② 専門知識を有する業務担当者を実施体制に組み入れていること。

③ 過去に類似の作業を行った実績があること。または、類似内容の作業に求められる知見・技術力を有していること。

イ 情報リスクマネジメントの業務

（類似作業の目安：6,500 以上【現用の 1/2 以上】のクライアント端末を有する環境の情報リスクマネジメントの業務）

１１．支給品及び貸与品等

(1) 支給品

イ．電気、ガス、水
ロ．事務用品
ハ．各種用紙

(2) 貸与品等

イ．作業室
ロ．机、椅子
ハ．ＰＣ、プリンタ、その他情報機器
ニ．工具類
ホ．マニュアル及び参考図書

１２．提出書類

	書類名	指定様式	提出期日	部数	備考
1	総括責任者届	機構様式	契約後および変更の都度速やかに	1部	総括責任者代理も含む
2	実施要領書	指定なし	〃	1部	
3	従事者名簿	指定なし	〃	1部	
4	業務日報	指定なし	業務終了時	1部	
5	業務月報	指定なし	翌月7日まで	1部	

6	終了届	機構様式	〃	1部	
7	その他機構が必要とする書類				詳細は別途協議

※実施要領書の作成に際しては機構と協議を行うこと。

（提出場所）

原子力科学研究所　情報交流棟

システム計算科学センター　サイバーセキュリティ統括室

１３．検収条件

終了届、業務月報の確認並びに仕様書の定めるところに従って業務が実施されたと機構が認めたときをもって業務完了とする。

１４．産業財産権等

産業財産権等の取り扱いについては、別紙4「産業財産権特約条項」に定められたとおりとする。

１５．情報セキュリティ強化

情報セキュリティ強化の対策については、別紙5「情報セキュリティ強化に係る特約条項」に定められたとおりとする。

１６．本業務開始時及び終了時の業務引継ぎ

⑴受注者は、本業務の開始日までに業務が適正かつ円滑に実施できるよう機構の協力のもと現行業務実施者から必要な業務引継ぎを受けなければならない。なお、機構は当該業務引継ぎが円滑に実施されるよう、現行業務実施者及び受注者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。この場合、業務引継ぎで現行業務実施者及び受注者に発生した諸経費は、現行実施者及び請負者各々の負担とする。

⑵本業務期間満了の際、次期業務の開始日までに受注者は機構の協力のもと次期業務実施者に対し、必要な業務引継ぎを行わなければならない。なお、機構は、当該業務引継ぎが円滑に実施されるよう、受注者及び次期業務実施者に対し必要な措置を講ずるとともに、引継ぎ完了したことを確認する。この場合、業務引継ぎで受注者及び次期業務実施者に発生した諸経費は、受注者及び次期業務実施者各々の負担とする。基本事項説明の詳細は、機構、受注者及び次期業務実施者間で協議のうえ、一定の期間（３週間目途）を定めて原契約の期間終了日までに実施する。

なお、本業務の受注者が次期業務実施者となる場合には、この限りではない。

１７．検査員及び監督員

検査員：管財担当課長

監督員：システム計算科学センター　サイバーセキュリティ統括室室長

１８．グリーン購入法の推進

(1) 本契約においては、グリーン購入法（国等による環境物品等の調達の推進等に関する法律）に適用する環境物品（事務用品、OA 機器等）が発生する場合は、これを採用するものとする。

(2) 本仕様に定める提出図書（納入印刷物）については、グリーン購入法の基本方針に定める「紙類」の基準を満たしたものであること。

１９．特記事項

・受注者は業務を実施することにより取得した当該業務及び作業に関する各データ、技術情報、成果その他のすべての資料及び情報を当機構の施設外に持ち出して発表もしくは公開し、または特定の第三者に対価をうけ、もしくは無償で提供することはできない。ただし、あらかじめ書面により機構の承認を受けた場合はこの限りではない。

・受注者は異常事態等が発生した場合、機構の指示に従い行動するものとする。なお、安全衛生上緊急に対処する必要がある事項については指示を行う場合がある。また、契約に基づく作業等を起因として異常事態等が発生した場合、受注者がその原因分析や対策検討を行い、主体的に改善するとともに、結果について機構の確認を受けること。

・受注者は、従事者に関して労基法、労安法その他法令上の責任並びに従事者の規律秩序及び風紀の維持に関する責任を全て負うとともに、これらコンプライアンスに関する必要な社内教育を定期的に行うものとする。

・受注者は業務の実施に当たって、次に掲げる関係法令及び所内規定を遵守するものとし、機構が安全確保の為の指示を行ったときは、その指示に従うものとする。

イ　電気事業法（昭和 39 年 7 月 11 日法律第 170 号）

ロ　機構が定める電気工作物保安規程

ハ　労働安全衛生法（昭和 47 年 6 月 8 日法律第 57 号）

ニ　機構が定める安全衛生管理規則

ホ　消防法（昭和 23 年 7 月 24 日法律第 186 号）

ヘ　その他、機構が定める規則等

・技術的能力など受注者の技術水準を維持するために社内教育や以下の教育を行うものとする。

教育名	実施者	機構による内容確認	備考
その他機構が指定する教育	機構	教育の受講に係る記録にて確認を受ける。	出入りに係るもの等の一部は業務開始前までに実施

・受注者は、善管注意義務を有する貸与品及び支給品のみならず、実施場所にある他の物品についても、必要なく触れたり、正当な理由なく持ち出さないこと。
・受注者は機構が原子力の研究・開発を行う機関であるため、高い技術力及び高い信頼性を社会的にもとめられていることを認識し、機構の関係法令及び規定等を遵守し安全性に配慮し業務を遂行しうる能力を有する者を従事させること。
・受注者は機構が伝染性の疾病（新型インフルエンザ等）に対する対策を目的として行動計画等の対処方針を定めた場合は、これに協力するものとする。
・受注者は、本仕様書の各項目に従わないことにより生じた、機構の損害及びその他の損害についてすべての責任を負うものとする。
・その他仕様書に定めのない事項については、機構と協議のうえ決定する。

以上

別紙 1

情報システムの脆弱性対策に関する業務の内容

1) 情報リスクマネジメントに関する業務
   ① 脅威の特定
   ② 脅威分析
   ③ リスク低減策の検討
   ④ リスク低減措置の実施

2) 情報セキュリティ対策システムのログ分析に関する業務
   ① 相関分析ルールの開発
   ② 独自ブラックリストの開発

3) 脆弱性検査に関する業務
   ① 検査計画書の作成、被検査部署との調整
   ② 脆弱性検査
   ③ 課題分析、対策提言
   ④ 脆弱性スキャンシステムの管理、運用

4) 更新プログラムの一括管理・配布に関する業務
   ① 更新プログラム一括管理・配布システムの管理、運用
   ② システム監視、障害対応

5) 海外事務所の脆弱性対応に関する業務
   ① 海外事務所 UTM システムの管理、運用
   ② 通信制御要件の設計、実装

6) その他
   ① リスク分析に関する相談対応
   ② 関係個所との連絡打合せ
   ③ 情報セキュリティに関する動向調査、分析
   ④ IT アーキテクチャ設計に関する最新技術や産業動向の関する調査、分析

別紙 2

認証基盤運用に関する業務の内容

1) 認証基盤の運用に関する業務

①エンタープライズアプリケーション、シングルサインオンの実装支援、運用

②条件付きアクセス、多要素認証、管理者アカウント管理の実装支援、運用

③モバイルデバイス管理の実装支援、運用

2) その他

①不審ログインの監視、障害対応、利用者対応

別紙 3

事業継続対策に関する業務の内容

1) データバックアップシステムの稼働維持に関する業務

① バックアップシステムの検討と要件定義

② 管理用サーバ、バックアップアプライアンスの管理、運用

③ Firewall の管理、運用

④ システム接続用ネットワーク（SW、UPS 含む）の管理、運用

2) その他

① 関係個所との連絡打合せ

② 運用計画・稼働状況に関する資料及び、運用管理マニュアルの作成・修正

③ 情報セキュリティ対策に係る作業

④ 障害・保守・停電対応

別紙４

産業財産権特約条項

（乙が単独で行った発明等の産業財産権の帰属）

第１条　乙は、本契約に関して、乙が単独でなした発明又は考案（以下「発明等」という。）に対する特許権、実用新案権又は意匠権（以下「特許権等」という。）を取得する場合は、単独で出願できるものとする。ただし、出願するときはあらかじめ出願に際して提出すべき書類の写しを添えて甲に通知するものとする。

（乙が単独で行った発明等の特許権等の譲渡等）

第２条　乙は、乙が前条の特許権等を甲以外の第三者に譲渡又は実施許諾する場合には、本特約条項の各条項の規定の適用に支障を与えないよう当該第三者と約定しなければならない。

（乙が単独で行った発明等の特許権等の実施許諾）

第３条　甲は、第 1 条の発明等に対する特許権等を無償で自ら試験又は研究のために実施することができる。甲が甲のために乙以外の第三者に製作させ、又は業務を代行する第三者に再実施権を許諾する場合は、乙の承諾を得た上で許諾するものとし、その実施条件等は甲、乙協議の上決定する。

（甲及び乙が共同で行った発明等の特許権等の帰属及び管理）

第４条　甲及び乙は、本契約に関して共同でなした発明等に対する特許権等を取得する場合は、共同出願契約を締結し、共同で出願するものとし、出願のための費用は、甲、乙の持分に比例して負担するものとする。

（甲及び乙が共同で行った発明等の特許権等の実施）

第５条　甲は、共同で行った発明等を試験又は研究以外の目的に実施しないものとする。ただし、甲は甲のために乙以外の第三者に製作させ、又は業務を代行する第三者に実施許諾する場合は、無償にて当該第三者に実施許諾することができるものとする。

２　乙が前項の発明等について自ら商業的実施をするときは、甲が自ら商業的実施をしないことにかんがみ、乙の商業的実施の計画を勘案し、事前に実施料等について甲、乙協議の上、別途実施契約を締結するものとする。

（秘密の保持）

第６条　甲及び乙は、第１条及び第４条の発明等の内容を出願により内容が公開される日まで他に漏洩してはならない。ただし、あらかじめ書面により出願を行った者の了解を得た場合はこの限りではない。

（委任・下請負）

第７条　乙は、本契約の全部又は一部を第三者に委任し、又は請け負わせた場合においては、その第三者に対して、本特約条項の各条項の規定を準用するものとし、乙はこのために必要な措置を講じなければならない。

２　乙は、前項の当該第三者が本特約条項に定める事項に違反した場合には、甲に対し全ての責任を負うものとする。

（協議）

第８条　第１条及び第４条の場合において、単独若しくは共同の区別又は共同の範囲等について疑義が生じたときは、甲、乙協議して定めるものとする。

（有効期間）

第９条　本特約条項の有効期限は、本契約締結の日から当該特許権等の消滅する日までとする。

別紙５

情報セキュリティ強化に係る特約条項

受注者（以下「乙」という。）は、本契約の履行に当たり、情報セキュリティの強化のため、契約条項記載の情報セキュリティに係る遵守事項に加え、以下に特約する内容を遵守するものとする。

（情報セキュリティインシデント発生時の対処方法及び報告手順）

第１条 乙は、情報セキュリティインシデントが発生した際の対処方法（受注業務を一時中断することを含む。）及び発注者（以下「甲」という。）に報告する手順について整備しておかなければならない。

（情報セキュリティ強化のための遵守事項）

第２条 乙は、次の各号に掲げる事項を遵守するほか、甲の情報セキュリティ強化のために、甲が必要な指示を行ったときは、その指示に従わなければならない。

(1) この契約の業務を実施する場所を、情報セキュリティを確保できる場所に限定し、それ以外の場所で作業をさせないこと。

(2) 業務担当者に遵守すべき情報セキュリティ対策について教育・訓練等を受講させるとともに、業務担当者には甲の情報セキュリティ確保に不断に取り組み、甲の情報及び情報システムの保護に危険を及ぼす行為をしないよう誓約させること。また、業務担当者の異動・退職等の際には異動・退職後も守秘義務を負うことを誓約させ、これを遵守させること。

(3) 暗号化を要する場合は、「電子政府推奨暗号リスト」に記載された暗号化方式を実装し、暗号鍵を適切に管理すること。

(4) 甲の承諾のない限り、この契約に関して知り得た情報を受注した業務の遂行以外の目的で利用しないこと。

(5) 甲が提供する情報を取り扱う情報システムへの不正アクセスを検知・抑止するために、ログを取得・監視し全ての業務担当者についてシステム操作履歴を取得すること。

(6) 甲が提供する情報を格納する装置、機器、記録媒体及び紙媒体について、業務担当者のみがアクセスできるよう施錠管理や入退室管理を行い、セキュアな記録媒体の使用や使用を想定しないUSBポートの無効化、機器等の廃棄時・再利用時のデータ抹消など想定外の情報利用を防止すること。

(7) 情報システムの変更に係る検知機能やログ解析機能を実装し、外部ネットワークへの接続を伴う非ローカルの運用管理セッションの確立時には、多要素主体認証を要求するとともに定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時の脆弱性対策を行うこと。

(8) システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施するとともに、システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと。

(9) 委任をし、又は下請負をさせた場合は、当該委任又は下請負を受けた者に対して、業務担当者が遵守すべき情報セキュリティ対策についての教育・訓練等を行うこと。

(10)契約条項に基づき甲が乙に対して行う情報セキュリティ対策の実施状況についての監査の結果、情報セキュリティ対策の履行が不十分である場合には、甲と協議の上改善を行い、甲の承諾を得ること。

(11) 契約の履行期間を通じて前各号に示す情報セキュリティ対策が適切に実施されたことの報告を含む検収を受けること。また、本契約の履行に関し、甲から提供を受けた情報を含め、本契約において取り扱った情報の返却、廃棄又は抹消を行うこと。

以上

様式１

情報システムの脆弱性対策及び認証基盤運用等に関する請負業務　要員経歴書

氏名：〇〇　〇〇	要員種別：運用技術者 S

	作　業　件　名	作業期間	作業月数	業務に必要な資格等			
				情報リスクマネジメントの業務経験	侵入検査に関する業務経験	利用者 6,500 名以上のﾘｽｸﾏﾈｼﾞﾒﾝﾄ経験	
1	例）　△△社　●●●の業務	H17.4.1～H20.3.31	36	36			
2	例）●●研究所　〇〇〇〇〇の業務	H20.4.1～H23.3.31	36	36	36	36	
3	例）▲▲機構　△△△△の運用業務	H23.4.1～H26.12.31	33	33	33	33	
4							
5							
6							
7							
8							
	合　計　（経験月数）		105	105	69	69	

記入上の注意事項

1）経験年数は令和 8 年 3 月 31 日現在とする
2）これまでの各作業において、実際に「要求資格要件」に該当する作業を実施（経験）した月数のみを経験年数（月数）とする
3）実際に「要求資格要件」に該当する作業を実施していない期間は経験年数に加算しない
4）これまでの各作業において、該当する（実際に作業をした）「要求資格要件」の欄にその作業の「作業月数」を記入し、その合計を経験年数とする
5）作業月数は、平行して複数の作業を実施している場合は、それらの比率をかけること （各人の１年間の作業月数の合計は１２ヶ月）
　但し、作業管理は除く
6）　要員交代等にて経歴書に変更が生じた際は、随時、差し替えを提出すること。