セキュリティログ監視サービス
仕様書

電力広域的運営推進機関

目次

1.調達案件の概要に関する事項 1
(1) 調達件名 1
(2) 調達の背景 1
(3) 目的及び期待する効果 1
(4) 用語の定義 1
(5) 業務・情報システムの概要 2
(6) 契約期間・作業スケジュール 2
2. 作業の実施内容に関する事項 2
(1) 作業の内容 2
(2) 成果物の範囲、納品期日等 3
3. 満たすべき要件に関する事項 6
4. 作業の実施体制・方法に関する事項 6
(1) 作業実施体制 6
(2) 作業場所 6
(3) 作業の管理に関する要領 6
5. 作業の実施に関する事項 6
(1) 機密保持、資料の取扱い 6
(2) 遵守する法令等 7
6. 成果物の取扱いに関する事項 7
(1) 検収 7
7. 再委託に関する事項 7
(1) 再委託の制限及び再委託を認める場合の条件 7
(2) 承認手続 7
8. その他特記事項 8
(1) 前提条件及び制約条件 8
9. 附属文書 8

1.調達案件の概要に関する事項

(1) 調達件名

セキュリティログ監視サービス

(2) 調達の背景

電力広域的運営推進機関（以下「本機関」という。）においては、政府機関全体としてのサイバーセキュリティ強化の取り組み方針等を踏まえ、昨年度までに本機関が所有するシステムについて外部監査やペネトレーションテスト等を実施する等のサイバーセキュリティ対策を実施してきている。

また、さらなるセキュリティ対策として、ファイアウォール等の通信機器や情報システムのセキュリティログからの異常検出及びアラート通知を行う技術的対策の導入及びセキュリティログの 24 時間監視、相関分析等の監視を行う Security Operation Center（以下「SOC 業務」という。）を 2018 年 2 月より導入している。現在利用中のセキュリティ監視デバイス機器について、2025 年度中に製造ベンダーによる保守サポートの期限が到来することから、老朽化した機器の交換を行う必要がある。

(3) 目的及び期待する効果

本調達は、本機関内のセキュリティログを 24 時間監視し、相関分析等を継続して行い、以下の効果を実現する。

・対応時間の短縮・・・収集した過去のセキュリティログを調査することで、被害状況の特定までに必要となる人的な作業量を削減し、対応完了までの時間を短縮する。

・被害の低減・・・内部に侵入したマルウェアが外部の C&C サーバと通信を繰り返している段階で、異常を検知して対応することで、重大な情報漏えいの拡大を阻止する。

(4) 用語の定義

本仕様書で使用する用語の定義を以下に示す。

表 1-1 用語の定義

用語	定義
OA システム	本機関のインターネット接続を唯一保有し、役職員にメール、ファイル共有等の OA 環境を提供するシステム メインサイトとバックアップサイトの 2 拠点に設置している
既設スイッチ	OA システム内に既に設置されているスイッチ
C&C サーバ	悪意のあるソフトウェアに感染したコンピュータ群に指令を送るサーバ
SOC	本機関向けにセキュリティログの 24 時間監視、相関分析等の監視を行う組織又はサービス
SOC 監視用セキュリティデバイス	既設スイッチのミラーポートより受信したパケットをもとに、セキュリティ検査を行い、ログを記録し、SOC に送信する機器
Internet VPN デバイス	SOC と暗号化された通信経路を構築するために、サイト間 VPN を提供する機器
メインサイト	OA システムが通常に稼働する東京江東区のデータセンター

バックアップサイト	OA システムが災害等の大規模障害時にメインサイトから引き継いで稼働する大阪北区にあるデータセンター
運用細則	SOC 業務の運用にあたり、情報を適正に管理し、恒常的に情報セキュリティ対策を維持することを目的に、今後、本機関が定めるシステム運用の基本的ルール

(5) 業務・情報システムの概要

本調達における業務・情報システムは OA システムを対象に以下のとおり想定している。

① 既存システムである OA システム内に SOC 監視用セキュリティデバイスが検査するネットワークポイントを設定する。

② SOC 監視用セキュリティデバイスを設置し、OA システムの通信パケットに対して当該デバイスにてセキュリティ検査を実施する。

③ SOC 監視用セキュリティデバイスは各セキュリティ検査で取得したログを SOC にリアルタイムで転送する。

④ SOC は SOC 監視用セキュリティデバイスからのログを取得・保管し、リアルタイムで分析する。

⑤ SOC にてインシデントを検知した場合は本機関に通知し対応を協議する。

詳細については、別紙「セキュリティログ監視サービス要求仕様書」を確認のこと。

(6) 契約期間・作業スケジュール

① 環境構築については、契約締結日から 2025 年 1 月末まで

② 保守については、機器導入時から 2028 年 1 月末まで

③ サービスについては、2025 年 2 月から 2028 年 1 月末まで（3 年間運用）

※ ②保守 及び ③サービスについては、１年単位の契約期間とする。

※ ②保守 及び ③サービスについては、4 年目以降 5 年目まで延長契約が任意で可能なこと。

2. 作業の実施内容に関する事項

(1) 作業の内容

作業の実施内容は以下を想定している。

なお、詳細は別紙 「セキュリティログ監視サービス要求仕様書」を参照のこと。

Ａ．環境構築

① プロジェクト計画／管理

本作業の実施にあたり、目的、実施体制、役割、作業内容と作業方法、作業スケジュール、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

② 要件確認

本機関における要件について、受託者との認識のずれや齟齬がないことを確認すること

③ 設計

確認した要件に基づき、基本設計、運用設計、試験設計、移行設計を行うこと。

④　構築

設計に基づき、システムをセットアップすること。

⑤　設置・工事

ラックの設置、電源工事、SOC 監視用セキュリティデバイス、インターネット回線の設置・工事を行うこと。

⑥　試験

試験設計に基づき、システムの試験を実施すること。また、SOC と連携し、ログファイルの授受や SOC 業務のシナリオ試験を実施すること。

⑦　チューニング

試験設計に基づき、システムの試験を実施すること。また、SOC と連携し、ログファイルの授受や SOC 業務のシナリオ試験を実施すること。

B．**保守**

①　プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

②　保守

運用細則及び環境構築作業にて作成した運用設計書に基づき、作業計画書を策定のうえ、導入した機器に関する稼働監視やシグネチャ更新等を実施すること。

C．**サービス**

①　プロジェクト計画／管理

本作業の実施にあたり、リスク管理、情報セキュリティ管理、課題管理、品質管理、人的資源管理、コミュニケーション管理、構成・変更管理等を明確にしたプロジェクト計画書を作成すること

②　サービス

運用細則及び環境構築作業にて作成した運用設計書に基づき、インシデントの監視、検知、通知等の業務を実施すること。

(2) 成果物の範囲、納品期日等

A．環境構築

本調達における想定している調達機器（設備）は以下のとおりであり、受託者は作業の詳細スケジュールと併せて、納品予定日をプロジェクト計画書等に記載すること。

また、追加の調達機器（設備）などがあれば提案書に記載すること。

なお、設置場所については、メインサイト及びバックアップサイトの本機関が指定する場所とする。

表 3-1 調達機器（設備）

調達機器（設備）	数量
SOC 監視用セキュリティデバイス	2 式
Internet VPN デバイス	2 台
インターネット回線	2 本（3 年分）
UTP ケーブル、スイッチ	適量
ラックマウントキット	2 式

B．保守

本調達における想定している保守は以下のとおりである。

また、追加の保守などがあれば提案書に記載すること。

表 3-2 保守内容

保守内容	数量
SOC 監視用セキュリティデバイス	2 式*3 年分
Internet VPN デバイス	2 台*3 年分

C．サービス

本調達におけるサービスは以下のとおりである。

表 3-3 サービス内容

サービス	数量
SOC	3 年分

D．本調達に係る付帯業務

① 成果物・提出物

付帯業務において想定している成果物は以下のとおりであり、受託者は作業の詳細スケジュールと併せて、納品予定日をプロジェクト計画書等に記載すること。

また、追加の成果物があれば提案書に記載すること。

表 3-1 作業の内容と成果物

作業の内容	作業の内容	成果物
A．環境構築	プロジェクト計画／管理	プロジェクト計画書
		進捗管理表
		課題管理表
		リスク管理表

		会議議事録
	設計	基本設計書
		運用設計書
		試験設計書
		移行設計書
	試験	試験結果報告書
B．保守	プロジェクト計画／管理	プロジェクト計画書
	保守	作業計画書
		月次報告書
C．サービス	プロジェクト計画／管理	プロジェクト計画書
	サービス	運用マニュアル
		インシデント報告書
		月次報告書

② 納品方法

項番	分類	要件
1	言語	・成果物は、全て日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
2	準拠すべき規格	・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）」に準拠すること。 ・情報処理に関する用語の表記については、原則、日本工業規格（ＪＩＳ）の規定に準拠すること。
3	納品形態	・成果物は電磁的記録媒体（ＣＤ-Ｒ等）により作成し、本機関から特別に示す場合を除き、原則電磁的記録媒体は 1 部を納品すること。なお、保守及びサービスの成果物については、メールでの納品も可能とする。 ・紙媒体による納品について、用紙のサイズは、原則として日本産業規格Ａ列４番とするが、必要に応じて日本産業規格Ａ列３番を使用すること。また、バージョンアップ時等に差し替えが可能なようにバインダ方式とすること。 ・電磁的記録媒体による納品について、Microsoft Word、Excel 又は同 PowerPoint で読み込み可能な形式、及びＰＤＦ 形式で作成し、納品すること。なお。これらは原則として文字列検索機能を活用して文字列が検索可能な状態のものを納品すること。ただし、本機関が他の形式による提出を求める場合は、協議の上、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルが

		ある場合は、協議に応じるものとする。
4	セキュリティ対策	・成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。 ・電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行う等して、成果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。
5	留意事項	・納品後、本機関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納品すること。 ・成果物の作成にあたって、特別なツールを使用する場合は、本機関の承認を得ること。

③ 納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、本機関が納品場所を別途指示する場合はこの限りではない。

〒135-0061

東京都江東区豊洲 6-2-15

電力広域的運営推進機関　総務部 情報システム室

3. 満たすべき要件に関する事項

本調達の実施に当たっては、別紙「セキュリティログ監視サービス要求仕様書」の各要件を満たすこと。

4. 作業の実施体制・方法に関する事項

(1) 作業実施体制

本プロジェクト実施に当たり、体制図及びその従事する人数について記載すること

(2) 作業場所

別紙「セキュリティログ監視サービス要求仕様書」に従うものとする。

(3) 作業の管理に関する要領

別紙「セキュリティログ監視サービス要求仕様書」に従うものとする。

5. 作業の実施に関する事項

(1) 機密保持、資料の取扱い

本機関から受託者に提供する秘密情報及び秘密情報を記録した資料等は、本契約期間中の如何を問わず、第三者に開示、漏えい又は他の目的に使用しないこと。ただし第三者に開示の必要性がある場合は、開示方針や漏えいの防止策を明示し本機関の承認を得ること。

(2) 遵守する法令等

① 本仕様書に示す業務の実施に当たっては、次の文書に記載された事項を遵守すること。

ア　政府情報システムの整備及び管理に関する標準ガイドライン

イ　政府機関の情報セキュリティ対策のための統一基準

ウ　本機関の情報管理セキュリティ関連規程

② 受託者は、現行情報システムの設計書等を参照する必要がある場合は、作業方法等について本機関の指示に従い、秘密保持契約を締結する等した上で、作業すること。

③ 受託者は、受託業務の実施において、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、個人情報の保護に関する法律等の関連する法令等を遵守すること。

6. 成果物の取扱いに関する事項

(1) 検収

① 本仕様書に則って成果物を提出すること。

② 検査の結果、成果物の全部又は一部に不合格品を生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映された全ての成果物を納入すること。

③ 本仕様書以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

7. 再委託に関する事項

(1) 再委託の制限及び再委託を認める場合の条件

① 受託者は本仕様書に示す業務の全部又は総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託することは不可とする。また、本業務の契約金額に占める再委託契約金額は、原則2分の1未満とする。

② 受託者は、知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本仕様書が定める受託者の債務を、再委託先事業者も負うような必要な処置を実施すること。

③ 再委託者、再委託者が業務を委託する第三者（以下「再々委託者」という。）及び再々委託者が業務を第三者へ委託する場合の責任は受託者が負うこと。

④ 以下に示すものについても本仕様書「6 作業の実施に当たっての遵守事項」に示した事項を遵守させること。

ア　再委託者

イ　再々委託者

ウ　再々委託者が業務を委託する第三者

(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、契約予定金額について本機関に提出し、承認を受けること。

② 再委託の相手方からさらに第三者に委託が行われる場合には、当該第三者の商号又は名称及び住所並びに委託を行う業務の範囲について本機関に提出すること。

8. その他特記事項

(1) 前提条件及び制約条件

・本仕様書は、受託者に業務遂行を求める最低限の基準を示したものである。したがって、本仕様書に記載していない事項であっても、本調達に必要と認められる事項は、本機関と追加負担を含め協議の上、これを行うこと。

・本件受託後に本仕様書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、本機関に申し入れを行うこと。

・受託者は、業務の遂行に当たり、本機関の作業負荷等を十分考慮すること。

・受託者のプロジェクトマネージャーは、業務の円滑な運営を図るため、本機関との連絡を密にして業務を遂行すること。

・本機関から貸し出された資料又は支給を受けた物品等については、善良なる管理者の注意をもって保管及び管理するものとし、紛失又は破損の場合直ちに本機関に報告し、本機関の指示に従って措置を講ずること。

・受託者は、常に作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法、労働安全衛生法等を遵守して安全の徹底を図り、作業を行うこと。

・受託者が行う提案や報告及び相談等は全て書面を持って実施し、内容については、本機関の承認を得ること。

・本仕様書に記載したスケジュールは現時点での想定である。スケジュール変更があった場合の対応については、本機関と協議の上、決定すること。

9. 附属文書

別紙「セキュリティログ監視サービス要求仕様書」

以上