電力広域的運営推進機関
セキュリティログ監視等業務の要件定義に係る業務委託
入札仕様書

電力広域的運営推進機関

平成 29 年 5 月 25 日

1　件名

セキュリティログ監視等業務の要件定義に係る業務委託

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。）では、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、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、相関分析等の監視業務を委託するセキュリティログ監視等業務（以下、「Security Operation Center」を略して「SOC」という。）を導入することを検討している。

SOC の導入にあたっては、本機関の情報セキュリティガバナンスの方針に沿った SOC 導入要件を定義するため、知見を有する外部の有識者の支援を得るものとし、本調達を行うに至った。

3　目的

本業務は、本機関に求められる情報セキュリティガバナンスの方針及びこれらの方針と整合性のとれた SOC の要求事項を明確化し、SOC の設計、開発、運用展開に必要な要件定義書の作成を行うものである。

4　業務の概要

4.1　対象範囲

SOC の調達、設計・開発及び運用は、「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」（平成 26 年 12 月 3 日各府省情報化統括責任者(CIO）連絡会議決定。以下「標準ガイドライン」という。）に基づいて進めることを想定し、「図 1 ：SOC 運用開始までのマイルストーン」に記載のとおり、調達手続きの完了を 2017 年 9 月末、設計・開発の完了を 2018 年 2 月末とし、2018 年 3 月からの運用開始を予定している。このうち、本支援業務は、要件定義を対象とする。

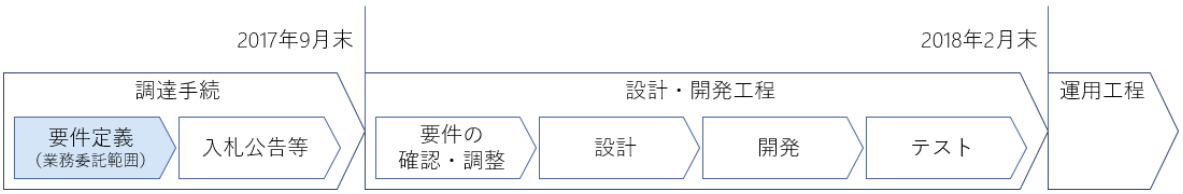

図 1：SOC 運用開始までのマイルストーン

5　委託内容

5.1　要件定義準備

要件定義の準備として、SOC に関連する物品の購入、既存システム及びネットワークの改修その他の役務について、調達単位の整理を行う。調達単位の検討にあたっては、現行

業務及び現行システムの調査と課題整理を実施するとともに、標準ガイドラインを参照し、履行可能性、ライフサイクルコスト、技術的妥当性等を考慮の上で整理すること。調査と課題整理においては、昨今のサイバーセキュリティの脅威動向や組織における情報資産とその重要度を正しく認識した上でリスクシナリオを想定し、監視目標を明確にすること。

5.2　要件定義

関連するステークホルダーにヒアリング等を行い、本機関における SOC のあり方を把握、検討し、これらの導入方針と整合性がとられた業務要件、機能要件及び非機能要件の定義を行う。要件の定義にあたっては、標準ガイドラインを参照するとともに、本機関に求められる要求事項の特徴を踏まえ、記載内容の軽重を検討するものとする。各要件については、以下の点に留意して整理すること。

(1) 業務要件は、SOC 運用時に求められるインシデント対応組織と連携プロセスを考慮し、システム構築（設計・開発・テスト）時、運用時に実施すべき業務委託（役務）要件、及び作成すべきドキュメントの種類や概要を検討すること。また、将来的な脆弱性管理、セキュリティ脅威情報収集等のセキュリティ管理の統合まで考慮することが望ましい。

(2) 機能要件は、業務の質の向上、業務の効率化等に対する有効性等を踏まえ、優先度の高い機能について重点的に要求事項を明確化すること。また、監視ルールを効率的に定義するため、各種ガイドラインで推奨される監視手法をテンプレートとして提供し、想定リスクシナリオ等を踏まえて、本機関に特化した監視ルールの要件を定義すること。

(3) 非機能要件は、本機関独自の仕様を規定・把握できる粒度とし、システム運用の課題解決に資する要件を定義すること。

5.3　進捗管理

本業務の推進にあたって、進捗管理、リスク・課題管理を行い、本機関と連携しながら円滑にプロジェクトを推進する。

(1) プロジェクト開始に先立ち、プロジェクトを推進するために必要な体制・スケジュール・管理手法・各種手続・成果物等を定めたプロジェクト計画書を作成すること。

(2) 本業務の実施内容や実施結果について、適宜ワーキンググループを開催し、報告すること。ワーキンググループの開催にあたっては、本業務開始当初に本機関と開催計画を協議し、決定すること。ワーキンググループ開催前には、報告内容について十分な事前協議を行うこと。

5.4　情報管理

本委託業務に関連して開示する機関の秘密情報を適正な情報管理を維持するため、本機関情報セキュリティ関連規程を遵守し、情報セキュリティを確保するものとする。特に下記の点に留意すること。

(1) 本委託業務の開始時に、業務に係る情報セキュリティ対策の遵守方法及び管理体制について、本機関担当者に書面で提出すること。

(2) 本機関から秘密情報を提供された場合には、当該情報の機密性の格付けに応じて適切に取り扱われるための措置を講ずること。

(3) 本機関の情報セキュリティ関連規程の履行が不十分と見なされるとき又は受託者において委託業務に係る情報セキュリティ事故が発生したときは、必要に応じて本機関の行う情報セキュリティ監査を受け入れること。

(4) 本機関から提供された秘密情報が業務終了等により不要になった場合には、確実に返却し又は廃棄すること。

(5) 外注することとなる場合は、外注先にも以上と同様の制限を課して契約すること。

6 成果物

以下について納入期限までに紙ベース（両面印刷）による提出と合わせて、電子データを提出することとする。電子媒体は、特に定めのない場合は Microsoft Office2013 で読み込み可能な Word、Excel、Power Point で作成すること。

成果物	数量	納入期限	備考
プロジェクト計画書	1 部	契約締結後、7 日以内	作業項目、実施期間、業務履行体制表等を記載
成果物	一式	平成 29 年 7 月 31 日	要件定義書

7 実施スケジュール

本業務委託の実施スケジュールの想定は、図２：実施スケジュールのとおり。

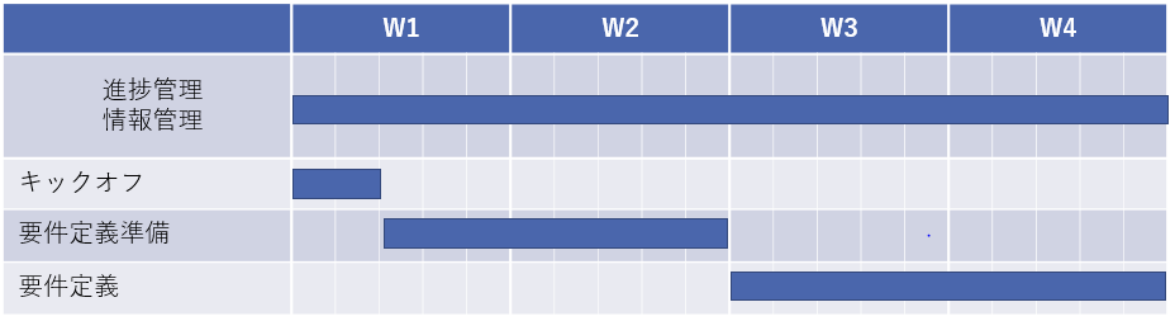

図２: 実施スケジュール

8 実施体制

本業務の目的を理解したうえで、受託者にて最適な体制を構築するものとする。なお、業務を実行するにあたり選任する者は、以下に定める事項に該当すること。

（ア） プロジェクトマネージャーは、独立行政法人情報処理推進機構の IT スキル標準に定める PM レベル 5 クラス以上の専門性を有する者である、サイバーセキュリティ関連業務で 15 年以上の経験を有する者である、又は、以下のいずれかの資格を保持している者であること。

- プロジェクトマネージャープロフェッショナル（PMP）
- 情報処理技術者試験　プロジェクトマネージャー試験（PM）合格者

（イ） プロジェクトメンバーは、サイバーセキュリティ関連のコンサルティング業務で 10 年以上の経験を有する者である、又は以下のいずれかの資格を保持している者であること。

- 情報処理技術者試験　情報セキュリティスペシャリスト試験（SC）合格者
- 情報処理技術者試験　システム監査技術者試験　（AU）　合格者
- 公認システム監査人（CSA）
- 公認情報システム監査人　（CISA）
- 公認リスク・情報システム管理者（CRISC）
- 公認情報セキュリティマネージャー（CISM）

なお、本機関は、次の場合は受託者に対して選任された者の交代を要求することができるものとする。

（ア） 選任された者の業務実施が当仕様書又は契約条件に適合しないとき

（イ） 選任された者のスキル不足等により、業務の遂行に著しく支障が生じると本機関が認めるとき

9　完了期限

平成 29 年 7 月 31 日

10　納入場所

電力広域的運営推進機関 事務所（総務部）

11　その他

(1) 本業務について、作業場所や作業端末等は受託者にて確保するものとする。

(2) この仕様書に定めのない事項について必要のある時は、委託者と受託者が都度協議し、決定するものとする。

以　上