セキュリティログ監視サービス
要求仕様書

電力広域的運営推進機関

目次

1.調達要件

(1) 調達物品に係る用語定義

本調達に係る主要なコンポーネントを次のとおり定義する。

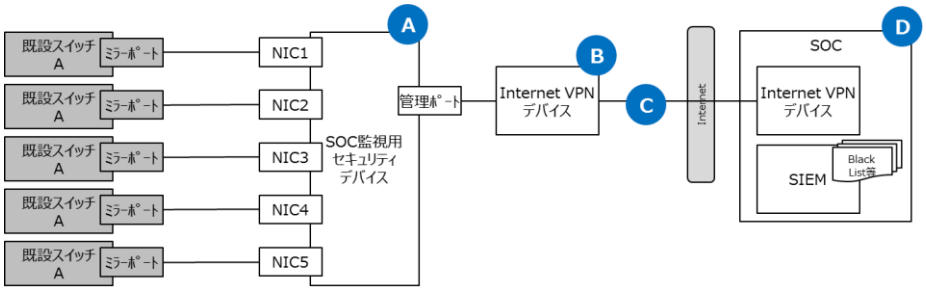

図 1.1 調達物品の定義

#	機器名	用途
A	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、ログの記録及びログを SOC に送信する役割を担う
B	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 を提供する役割を担う
C	インターネット回線	SOC との通信経路を提供する役割を担う
D	SOC	本機関向けにセキュリティログ監視業務を提供する組織又はサービスをいう

(2) 調達対象

(1)の用語定義に基づき、調達対象を次に記載する。なお、本機関における既設の設備に係る設計作業や設定変更作業は、調達の範囲外とする。

表 1.1 調達対象

カテゴリ	調達対象		数量
1) 設備	A	SOC 監視用セキュリティデバイス	2 台（※1）
	B	Internet VPN デバイス	2 台
	C	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
2) 役務	A, B, C, D	要件確認	1 式
	A, B, C, D	設計	1 式
	A, B, C, D	構築	1 式
	A, B, C	設置・工事	1 式
	A, B, C, D	試験	1 式
	D	チューニング	1 式
3) 保守	A	SOC 監視用セキュリティデバイス	2 台*3 年分
	B	Internet VPN デバイス	2 台*3 年分

4) サービス	D	SOC	3 年分

（※1）単一製品でなく、優れる製品の組み合わせでも可

(3) 調達対象となる数量の考え方

本機関では、同一構成となるメインサイトとバックアップサイトを保有している。

本調達に係る設備は、メインサイトとバックアップサイトに配備するため、前述 表 1.1 の「1)設備、3)保守」の数量はバックアップサイトを含む数量となっている。

本機関のバックアップサイトは、ホットスタンバイ構成であり、メインサイトが稼働している場合には、業務通信トラフィックが発生しない仕様である。

このため、SOC 等のサービス費の見積もりにあたっては、監視対象となるアクティブな環境は、いずれか一方の環境（アクティブ-スタンバイ構成）であることに十分留意すること。

(4) サービス継続性の考え方

本機関における事業及びシステムは、前述(3)のとおりメインサイトとバックアップサイトを構築するなどサービス継続性をより重要視している。

今回調達する SOC サービスについても、可能な限り地震、災害などの発生時にも SOC サービスが継続できるよう関連設備や業務実施拠点などの DR 対応を希望している。

上記背景を理解のうえ、SOC サービスの継続性について入札者の対策状況を提案書に記述いただきたい。

(5) SOC 監視用セキュリティデバイスのポート数の考え方

SOC 監視用セキュリティデバイスは、既設スイッチの 5 か所のミラーポートから通信を受信する必要がある。

本機関におけるメインサイトの既存システムは、スイッチを含め冗長化構成としていることから、既設スイッチのミラーポートはアクティブ系スイッチ 5 ポート、スタンバイ系スイッチ 5 ポートの計 10 ポートとなる。バックアップサイトの既存システムは、シングル構成としていることからミラーポートはアクティブ系スイッチ 5 ポートとなる。

入札者においては、上記を理解のうえ、SOC 監視用セキュリティデバイスに 10 ポートの監視機能を設けるか、既設スイッチと SOC 監視用セキュリティデバイス間にスイッチ等のネットワーク機器を配置して通信を束ねるかなど、最適なソリューションを検討のうえ提案いただきたい。

2. 設備に関する要件

(1) 機能要件

本書で調達する設備に関する機能要件は次のとおりとする。

表 2.1 設備に係る機能要件

項目	内容
SOC 監視用セキュリティデバイスに関する要件	
TAP モード機能	・ スイッチ(ミラーポート)に接続のうえ、当該スイッチから SOC 監視用セキュリティデバイスに届く通信パケットに対して、「FW」「IDS」「URL フィルタ」「AntiVirus」「Sandbox」のセキュリティ検査を実施すること
FW 機能	・ 送信元/宛先 IP アドレス、プロトコル（ポート番号）に基づく通信ポリシーを設定できること ・ ポリシーにマッチした通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、データサイズ、セッション時間」を含むこと ※本機能はポリシーに基づくログ収集機能であり、通信制御を求めているものではない。
IDS 機能	・ シグネチャ（攻撃パターンのプロファイル）とのパターンマッチングによる攻撃の検知ができること ・ シグネチャにマッチした通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、シグネチャ名」を含むこと ・ パターンマッチングにより攻撃と判断した場合には、当該通信の PCAP データを取得すること
URL フィルタ機能	・ URL カテゴリ（Web サイトの種別リスト）とのパターンマッチングによる通信先となる Web サイトの分類ができること ・ 「クライアントから Proxy サーバ間の通信」、「Proxy サーバから Internet 間の通信」に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、URL、プロトコル、カテゴリ名」を含むこと ※本機能はパターンマッチングによるログ収集であり、特定の URL へのアクセス制御を求めているものではない。
AntiVirus 機能	・ パターンファイル（ウィルス、マルウェアのプロファイル）とのパターンマッチングによる不審ファイルの検査ができること ・ パターンファイルにマッチしたデータに対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、ウィルス名」を含むこと

Sandbox 機能	・ 受信データを、検査用領域で実行（既知のマルウェアリストとの照合を含む）し、マルウェアであるかの検査ができること ・ マルウェアと判断した通信に対して、ログを記録すること。ログには、少なくとも「時間、送信元/宛先 IP アドレス、プロトコル、マルウェア名」を含むこと
ログ管理機能	・ 各種セキュリティ機能で取得したログを Syslog プロトコルで、SOC にリアルタイムで転送すること ・ デバイスが記録したログは可能な限りデバイス内の記憶領域に保存し、本機関の要求に応じてログを提出できること
Internet VPN デバイスに関する要件	
FW 機能	・ 送信元/宛先 IP アドレス、プロトコル（ポート番号）に基づく通信ポリシーを設定できること
VPN 機能	・ 本機関と SOC との Site to Site の Internet VPN が構築できること。なお、VPN の機能及び動作仕様は、対向機器となる SOC デバイスと互換性のあるものとする
NAT 機能	・ SOC 監視用セキュリティデバイスからインターネットへの通信をグローバル IP アドレスに NAT すること ・ SOC 監視用セキュリティデバイスから SOC 設備への通信を SOC が指定するプライベート IP アドレスに NAT すること
インターネット回線に関する要件	
通信機能	・ SOC 監視用セキュリティデバイスから SOC、及び SOC 監視用セキュリティデバイスからインターネットに接続できること
グローバルアドレス	・ 固定のグローバル IP アドレスを少なくとも１つは利用できること
各デバイス共通の要件	
管理機能	・ 管理者によるオペレーションは、HTTPS や SSH など暗号化されたプロトコルが利用できること ・ 管理者のログインに対して、ID、パスワードによる認証、及び送信元 IP アドレスによる制御を行うこと
証跡管理	・ 管理者の設定変更履歴をログとして記録させること。ログには、少なくとも「時間、アカウント名/操作元 IP アドレス、操作内容」を含むこと ・ デバイスが記録したログは可能な限りデバイス内の記憶領域に保存し、本機関の要求に応じてログを提出できること
時刻同期	・ タイムゾーンは Asia/Tokyo（UTC+09:00）とし、本機関が指定する NTP サーバと同期できること
バックアップ機能	・ 機器の機能停止を伴わずにバックアップが取得できること

監視機能	・ SNMP 等のスタンダードプロトコルを用いた稼働監視・パフォーマンス監視に対応していること ・ ハードウェア等の障害が発生した場合に、SNMP Trap やエラーメールなどの通知機能を有すること
電圧	・ 100V 対応機器であること

(2) **非機能要件**

① 規模及び性能

本書で調達する設備に関する規模及び性能について記載する。本機関の通信量を考慮し、十分な性能が発揮できる機種及び回線を選定すること。

表 2.2 設備に係る非機能要件-規模

項目	内容
SOC 監視用セキュリティデバイスに関する要件	
監視対象となるシステムの規模	・ SOC 監視用セキュリティデバイスの検査対象となる本機関のメインサイトは、以下の規模とする 利用者数：300 名 端末数：500 台
監視対象	・ デバイスが検査する（TAP する）ネットワークポイントは 5 か所とする（既存スイッチのアクティブ系 5 ポート、スタンバイ系 5 ポート）
通信量	・ １日あたりの通信量は以下の通りとする ポイント 1）メインサイト(503.95GB) 帯域 1Gbps ：平均 48Mbps ポイント 2）バックアップサイト(272.40GB) 帯域 1Gbps：平均 20Mbps
同時セッション	・ デバイスが検査するポイントのそれぞれのセッション数は不明であるため、通信量をもとに受託者にて推測のうえ提案すること
Internet VPN デバイスに関する要件	
通信量	・ SOC 監視用セキュリティデバイスが SOC に送信するログ量を主たる通信量として考えること。なお、当該デバイスが出力するログ量（EPS）は、現時点で不明なため、受託者の実績をもとに推測のうえ提案すること
VPN トンネル数	・ VPN トンネル数は、SOC 間と接続で必要となるスペックとすること
インターネット回線に関する要件	
通信量	・ SOC 監視用セキュリティデバイスが SOC に送信するログ量を含む本機関と SOC 間の通信量を推測のうえ提案すること

	・ SOC 監視用セキュリティデバイスがシグネチャダウンロードなどインターネットにアクセスする通信量を踏まえ提案すること

② 信頼性・拡張性

本書で調達する設備に求める信頼性及び拡張性について記載する。

表 2.3 設備に係る非機能要件-信頼性

項目	内容
各デバイス共通の要件	
稼働時間	・ 24 時間 365 日の運用を前提とし、定期的な再起動やバージョンアップ以外の保守時の停止を要さないこと
耐障害性	・ シングル構成とするが、耐障害性の高い機器を選定すること
信頼性	・ 調達対象の設備に障害が発生しても、本機関の業務に影響を与えない製品を選定すること
バックアップ	・ 設定ファイルは、設定変更後の状態をリカバリポイントとすること。ただし、デバイス内に記録するログ等のデータは、リカバリ対象から除く
拡張性	・ 監視対象となる通信量が 2 倍となった場合でも、設備増強を必要としない製品を選定すること

③ 情報セキュリティ

本書で調達する設備に求めるセキュリティについて記載する。本書の要件に鑑み、追加で考慮すべきセキュリティ施策がある場合は、本機関に提案すること。

表 2.4 設備に係る非機能要件-情報セキュリティ

項目	内容
ファームウェア	・ 最新の OS 及びファームウェアを利用し、既知の脆弱性のない状態で納品すること
管理者アクセス	・ 本機関が指定する担当者に対して、管理者用画面を提供すること ・ 複数回の認証エラーは、アカウントロックアウト機能を有することが望ましい
管理者 ID	・ 管理者 ID は、本機関及び受託者で異なる ID を発行し、必要最低限の権限のみ与えること ・ 本機関の管理者 ID は共有ではなく、個人単位で発行すること
第三者認証	・ SOC 監視用セキュリティデバイスについて、「IT 製品の調達におけるセキュリティ要件リスト」に記載されている「国際標準 に基づくセキュリティ要件」に準拠した第三者認証を取得していること

3. 役務に関する要件

(1) 業務要件

① 業務実施手順

本書で調達する役務について、要件を記載する。

表 3.1 役務に係る業務要件-業務手順

フェーズ	作業内容
要件確認	・ 本機関における要件（本書の要件）について、受託者との認識のずれや齟齬がないことを作業着手前に確認すること ・ 受託者が SOC 業務開始までの作業を進めるにあたり、前提となる要件を本機関にヒアリングし、当該内容を要件確認書として取りまとめること ・ 要件確認の内容を本機関と合意のうえ、設計作業に着手すること
設計	基本設計 ・ 要件確認に基づき、SOC 業務に必要なシステム及びシステムで利用する全ての機能について設計し、基本設計書として取りまとめること ・ 要件確認に基づき、SOC 監視用セキュリティデバイスの機能設計を行うこと。なお、設計には次のカスタムシグネチャの作成を含める - HTTP：POST, PUT、User-Agent、Connect メソッド、特定拡張子 - Mail：特定拡張子 - DNS：txt レコード ・ SOC 監視を実施することを十分に考慮のうえ、ネットワーク環境や機器のログ・アカウントなどの設計を行うこと 運用設計 ・ SOC 業務及びシステム運用における業務フロー、手順（判断基準を含む)、バックアップサイトへの切替手順、体制、連絡先を設計し、受託者のサービス仕様を運用設計書に取りまとめること。また、SOC 業務に係る通知メールやレポート等の内容についても、設計フェーズで本機関と合意すること ・ 運用設計書には、本機関と SOC との役割や責任及び情報連携方法などを含めること ・ システムの障害時に影響を受ける業務や業務復旧までの時間及び対応フローについて運用設計書に取りまとめること ・ システムの設定変更に関する依頼フォームを提示し、本機関と合意すること 試験設計 ・ 単体試験、結合試験、障害試験、情報セキュリティの観点に基づく試験などの試験項目を計画し、その合否判定基準を設計すること。

	・ 運用設計にもとづき、SOC 業務及びシステム障害を想定したシナリオテストを行うこと 移行設計 ・ 本機関の既存システムに影響をあたえないように、設置作業及び工事計画を立て移行設計書として取りまとめること。また、既存システムとの接続に際し、リスクや留意事項があれば、本機関に提示すること ・ 本機関の既存システムに設定変更を必要とする場合は、その内容や順序についても可能な限り支援すること
構築	・ 設計に基づき、システムの設定値を設計し、セットアップすること ・ 各デバイスは、既知の脆弱性がないソフトウェアで構築すること ・ システムのバックアップファイルを取得すること
設置・工事	・ 本機関の指定したサーバラックに機器を設置すること。（ラックマウントキットは用意すること） ・ インターネット回線の工事を行うこと。 ・ デバイスをラックに搭載し、各デバイス間をネットワークケーブルで結線すること。なお、本機関の既設デバイスとの接続にあたっては、本機関の既存システムの停止は不可（停止が必要である場合は 2 重化を切り替えながら実施）であることを前提に、平日深夜又は休日の作業を想定すること ・ 接続に必要となるネットワークケーブル等は、本業務の受託者にて用意すること ・ データセンタでの工事にあたり必要な申請は本機関にて実施するが、申請内容の作成は受託者が実施すること
試験	・ 試験設計に基づき、システムの試験を実施すること ・ デバイス単体で、各機能が適切に動作していることを確認すること ・ 本調達に係るシステム及び各機能を結合し、設計通りに動作していることを確認すること ・ 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 ・ バックアップ及びリストアの試験を実施し、設計通りに障害からの復旧ができることを確認すること ・ 運用開始にあたり、本機関は情報セキュリティに関する検査を実施する。
SIEM ルールのチューニング	・ 本機関が要求する SIEM ルールにおいて、誤検知、過剰検知が発生する場合は、必要に応じてルール条件の見直しやホワイトリストなどで誤検知排除に向けたチューニングを実施すること

② 業務実施期間

本書で調達する役務について、本機関が想定している実施期間を記載する。

表 3.2 役務に係る業務要件-業務実施期間

フェーズ	作業内容
要件確認	・ 契約締結日～2024 年 10 月中旬
設計	・ 2024 年 10 月中旬～2024 年 11 月中旬
構築	・ 2024 年 11 月中旬～2024 年 12 月中旬
設置・工事	・ 2024 年 12 月中旬
試験	・ 2024 年 12 月中旬
チューニング	・ 2024 年 12 月中旬～2025 年 1 月末

③ 業務実施場所

本調達に係る作業は、本機関が承認した作業場所でのみ実施を許可する。

表 3.3 役務に係る業務要件-業務実施場所

項目	内容
作業場所	・ 本役務の一部は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関の許可を得ること ・ 本役務に関する打合せ、レビュー、報告会議等については、本機関が提供する会議室で実施すること ・ 本役務における設置工事、試験については、本機関が指定するシステム設置場所で実施すること

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 3.4 役務に係る業務要件-業務管理

項目	内容
進捗管理	・ 進捗管理については、プロジェクト計画書に基づき各タスクの状況把握及びスケジュール管理を行うこと
リスク管理	・ 各作業工程における目標の達成に対するリスクの抽出、リスクの影響を最小限にする対応策の実施等のリスク管理を行うこと
文書管理	・ 各作業工程において作成する設計書等の文書について、改ざん、漏えい、盗用及び目的外の利用を未然に防止するよう文書管理を行うこと
課題管理	・ プロジェクト遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと

品質管理	・ 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと
人的資源管理	・ 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・ 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
コミュニケーション管理	・ 各作業工程における各種作業に関する打ち合わせ、成果物等のレビュ、進捗確認、課題共有等を行うためのプロジェクト会議を開催すること
構成・変更管理	・ 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

4. 保守に関する要件

(1) 業務要件

① 業務実施内容

本書で調達する保守及び運用業務について、要件を記載する。

表 4.1 保守に係る業務要件-実施内容

項目	内容
稼働監視	・ 本システムのデバイス及び提供機能を監視し、障害発生を検知した場合は、速やかに本機関にメールと電話で報告を行うこと。 ・ 稼働状況が確認できるための監視ポータル（監視結果レポート画面）を用意すること。 ・ トラフィック量やリソース情報を監視し、品質の低下が危惧される場合は通知すること
障害対応	・ システム障害を検知した場合は、速やかに切り分けを実施の上、事象及びその原因特定、及び復旧作業を行うこと。なお、障害対応においては、本機関と密に情報連携を行うこととする（情報連携の方法等は運用設計で定義すること） ・ 必要に応じて、ハードウェアを交換し、最新のバックアップファイルからリストアを行うこと
設定変更	・ 本システムのデバイス及び提供機能に係る設定変更を実施すること。なお、設定変更は本機関の依頼から起算し、5 営業日以内に実施すること。ただし、緊急性の高い設定変更については、1 営業日以内に実施すること ・ 保守業務における設定変更作業では、本機関のメインサイトに影響を与えないように作業を実施すること。

シグネチャ更新	・ 本システムのデバイスに係るシグネチャやパターンファイルを更新し、最新の脅威が検知できる環境を維持させること
バックアップ	・ 設定変更及びバージョンアップ時には、設定ファイルのバックアップを取得すること ・ バックアップ保存期間は、3 世代又は 1 年のうち、保存期間の長いものを適用すること
バージョンアップ	・ ソフトウェア/ファームウェアのアップデートは、保守サービスの範囲内とすること。ただし、ソフトウェア/ファームウェアのアップデートは、重大な脆弱性が発見された場合、又は SOC 業務の提供に影響を与える場合に限る。 ・ 保守業務におけるバージョンアップ作業では、本機関のメインサイトに影響を与えないように作業を実施すること
保守受付	・ 本機関からの各種依頼に対して、電話、メールによる受付窓口を準備し、依頼事項に対する支援を実施すること ・ 本システムの動作仕様や技術的な質問に対して、電話及びメールにて回答を行うこと ・ 専任の担当者を設置し、本機関の環境を踏まえた回答やサポートを行うことが望ましい。なお、専任担当者は、本機関の専属である必要はなく、本機関の環境を理解した応対ができればよい
保守情報通知	・ ソフトウェア/ファームウェアのリリースや、当社にて使用中のソフトウェア/ファームウェアに脆弱性が発見された際、電話又はメールにて通知を行うこと。緊急性の高いものは即時情報を提供すること ・ メーカーサポート終了（EOL）が発表された場合、速やかに本機関へ通知すること ・ インターネット回線に保守作業による断時間が発生する場合、その内容を速やかに本機関に通知すること
月次報告	・ 稼働状況及び本機関からの各種依頼への対応状況を月次で報告すること。また、各デバイスの脆弱性やソフトウェア不具合情報を提供し、バージョンアップの要否について報告すること
その他	・ 本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること ・ 対応言語は日本語とすること

② 業務提供時間

受託者は保守契約の期間において、次の時間帯で保守業務を提供すること。

表 4.2 保守に係る業務要件-提供時間

項目	内容
稼働監視	・ 24 時間 365 日
障害対応	・ 24 時間 365 日
設定変更	・ 平日 9:00-18:00
シグネチャ更新	・ 24 時間 365 日
バックアップ	・ 平日 9:00-18:00
バージョンアップ	・ 平日 夜間、又は、休日（都度、本機関と調整すること）
保守受付	・ 受付：24 時間 365 日 ・ 回答：平日 9:00-18:00
保守情報通知	・ 平日 9:00-18:00
月次報告	・ 平日 9:00-18:00（毎月 10 営業日以内に報告すること）

③ 作業場所

本調達に係る保守作業は、原則として受託者の事業所とするが、予め本機関にその業務場所について開示すること。

表 4.3 保守に係る業務要件-業務場所

項目	内容
作業場所	・ 保守業務は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関に案内すること ・ 保守業務に関する打合せ、報告会議等については、本機関及び受託者が協議の上決定すること

④ 業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 4.4 保守に係る業務要件-業務管理

項目	内容
情報セキュリティ管理	・ 各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと、並びに発生した場合に被害を最小限に抑えること
課題管理	・ 業務遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと
品質管理	・ 品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと

人的資源管理	・ 本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・ 主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
構成・変更管理	・ 構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

5.サービスに関する要件

(1) 機能要件

① 機能

SOC 側の運用設備に求める要件を次に記載する。

表 5.1 サービスに係る機能要件

項目	内容
ログの取得及び保管機能	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで収集すること ・ 収集・保管するログ情報は、漏えいや改ざん等の被害を防止し、1年間保管すること。なお、少なくとも 3 ヶ月分についてはオンラインでの保存が望ましい
ログの監視機能	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで分析すること ・ 本機関が指定する以下の分析要件を SIEM に実装すること。具体的なルール要件は、契約後に本機関が受託者に提示する
単純条件型①	・ SOC 監視用セキュリティデバイス（Sandbox、IDS 機能など）が異常と判断したセキュリティログが出力された場合に、アラートとすること ※IDS は、カスタムシグネチャを含めること
単純条件型②	・ 特定の条件に合致するセキュリティログが出力された場合に、アラートとすること ・ 例）プライベートアドレスからグローバルアドレス宛ての通信 ・ 例）URL フィルタで脅威サイトとカテゴリ分類された通信
相関分析型①	・ セキュリティログに記録された IP や URL を、SOC が保有する脅威 DB（ブラックリスト）と照合し、DB の内容に一致した場合、アラートとすること
相関分析型②	・ セキュリティログに記録された IP や国情報を、本機関が指定するブラックリストと照合し、DB の内容に一致した場合、アラートとすること

	閾値型	・ ログの特定カラムを計算し、一定の閾値に達する場合、アラートとすること ・ 例）1 日分の送信データ Byte 数を積算し、閾値を超えた場合 ・ 例）指定した時間帯以外で、指定するログが出力された場合
VPN 接続機能		・ 本機関に設置する Internet VPN デバイスとの Site to Site の Internet VPN が構築できること
運用管理端末		・ 本機関のシステムを操作するオペレーション端末は、脆弱性のないセキュアな端末で実施すること。なお、パッチ管理、アンチウィルス、ID 管理、ログ管理のセキュリティ対策は必須とする

(2) 業務要件

① 業務内容

本書で調達する SOC 業務について、要件を記載する。

表 5.2 サービスに係る業務要件-業務内容

項目	内容
ログの取得保管	・ SOC 監視用セキュリティデバイスから送信されるログをリアルタイムで収集すること ・ 収集・保管するログ情報は、漏えいや改ざん等の被害を防止し、1 年間保管すること。なお、少なくとも 3 ヶ月分についてはオンラインでの保存が望ましい
インシデントの検知（ログの監視）	・ 収集したログを相関分析することにより、脅威や不正の発生を検知すること ・ 入札者が保有するナレッジや独自のブラックリストとの突合などで検知能力を高めること
インシデントの分析	・ 検知したアラートについて誤検知、過剰検知等を調査し実害の有無を判断すること ・ 事前の運用設計に基づき、発生したインシデントのトリアージを行うこと（トリアージの基準は運用設計で定めること） ・ 調査は、ログ保管期間である 1 年間に遡って調査すること
インシデントの通知	・ インシデント発生を認めた場合、発生事象、その影響及びトリアージ結果と共に、隔離等の対処方法を通知・案内すること ・ インシデントの通知は、そのアラートが発生してから 4 時間以内を目標とすること。なお、詳細なレポートを待たずして初報が可能な場合は、可能な限り早期に行うこと
QA 対応業務	・ 本機関からの各種依頼に対して、電話、メールによる受付窓口を準備し、依頼事項に対する支援を実施すること

	・ 本サービスの仕様や技術的な質問に対して、電話及びメールにて回答を行うこと ・ 専任の担当者を設置し、本機関の環境を踏まえた回答やサポートを行うことが望ましい。なお、専任担当者は、本機関の専属である必要はなく、本機関の環境を理解した応対ができればよい
インシデントの対応支援	・ 本機関からのインシデントの対応策等の問い合わせに対して、推奨手順等の回答を行うこと
定期報告	・ 月次レポートの発行 ・ 月次レポートの内容ついて、本機関からの問い合わせがあった場合は、会議を開催の上その内容について説明すること ・ 月次レポート以外に、世の中の脅威や脆弱性の情報を定期的に報告すること
改善提案	・ あらたなサイバー攻撃や脆弱性に対する監視方法や対処方法について、プロアクティブな提案を行うこと
その他	・ 本機関では情報システムのセキュリティ検査及びシステム監査を毎年実施していることから、受託者は本機関からの求めに応じ、問合せへの対応や必要な資料を提供すること ・ 本機関とのサービス契約終了時（途中解約等も含む）には、インシデント履歴やログデータ、レポート等の全ての情報を削除すること ・ 言語は日本語とすること

② 業務提供時間

受託者は SOC 契約の期間において、次の時間帯で保守業務を提供すること。

表 5.3 サービスに係る業務要件-提供時間

項目	内容
ログの取得保管	・ 24 時間 365 日
インシデントの検知（ログの監視）	・ 24 時間 365 日
インシデントの分析	・ 24 時間 365 日
インシデントの通知	・ 24 時間 365 日
QA 対応業務	・ 受付：24 時間 365 日 ・ 回答：平日 9:00-18:00
ログの提供	・ 平日 9:00-18:00
インシデントの対応支援	・ 24 時間 365 日
定期報告	・ 平日 9:00-18:00（毎月 10 営業日以内に報告すること）

改善提案	・　平日 9:00-18:00

③　作業場所

本調達に係る保守作業は、原則として受託者の事業所とするが、予め本機関にその業務場所について開示すること。

表 5.4 サービスに係る業務要件-作業場所

項目	内容
作業場所	・　保守業務は、受託者の事業所内での実施を許可するが、事前に作業内容と作業場所について本機関に案内こと ・　保守業務に関する打合せ、報告会議等については、本機関及び受託者が協議の上決定すること

④　業務管理

受託者は、次に示す管理業務を、本業務の全工程に渡り実施すること。

表 5.5 サービスに係る業務要件-作業場所

項目	内容
情報セキュリティ管理	・　各作業工程において、セキュリティに関する事故及び障害等の発生を未然に防ぐこと、並びに発生した場合に被害を最小限に抑えること
課題管理	・　業務遂行上様々な局面で発生する各課題について、課題の認識、対応案の検討、解決までの追跡等の課題管理を行うこと
品質管理	・　品質評価計画の立案、検証及び品質改善策の検討、実施を管理する体制の構築等の品質管理を行うこと
人的資源管理	・　本調達に参画する要員の選定、変更及び体制維持に関する管理を行うこと ・　主たる要員に変更が生じた場合には、本機関へ報告すること。また、代替要員については、サービスレベルの低下を防ぐために、知識及び経験が妥当な者を選定すること
構成・変更管理	・　構成管理対象（設計書等）を特定し、管理レベル（参照・更新権限、保存方法・期間等）を定めること

以上