

情報セキュリティ統合プラットフォーム 仕様書

公益財団法人放射線影響研究所
2025 年 8 月

目次

I. 概要

1. 調達背景及び目的・・・・・・・・・・・・・・・・・・・・・1
2. 調達する情報セキュリティ統合プラットフォームの概要・・・・・・・・・・1
3. 調達内容・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・2
4. 作業留意事項等・・・・・・・・・・・・・・・・・・・・・・・・・・2

II. 調達物件が備えるべき技術的要件

1. 技術仕様（検出機能要件）・・・・・・・・・・・・・・・・・・・・・5
2. 技術仕様（連携機能要件）・・・・・・・・・・・・・・・・・・・・・・8
3. 技術仕様（次世代 SIEM 要件）・・・・・・・・・・・・・・・・・・・・・10
4. 技術仕様（MDR サービス要件）・・・・・・・・・・・・・・・・・・・・・・12
5. 作業報告書等の作成・・・・・・・・・・・・・・・・・・・・・・・・・・13
6. 資格・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・13
7. その他・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・13
8. 導入実績・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・14

I. 概要

1. 調達の背景及び目的

放射線影響研究所（以下、放影研という）は、原爆被爆者から提供された貴重な生体試料をはじめ、多くの臨床・疫学・分子生物学情報を保有している。これらの情報の多くは電子化され、様々な形式で保存されたうえで所内各部門において利活用されている。言うまでもなくこれらの情報は極めて機微性の高い情報であり、万が一情報が漏えいした場合には、研究所の信頼失墜にとどまらず、国家的な重大事案に発展しかねない。

一方、研究所は2022年に策定された「放影研戦略計画」において、国内外の共同研究をより一層推進するため、保有する情報資産の可用性を向上すべく、研究資源の一元化およびクラウド環境への移行を表明しているところである。一般に情報資産の可用性の向上と情報セキュリティの担保はトレードオフの関係にあると言われている。可用性を向上させれば、セキュリティのリスクは増大し、逆にセキュリティを強化すれば利便性が損なわれる。このような二律背反を克服し、双方の両立を図るためには、従前から利用している情報セキュリティソリューションでは不十分であり、より高度な対応が求められる。すなわち、クラウドへの研究資源の移行や、所外との情報共有をこれまで以上に安全に推進するためには、所内外を通じた複数のセキュリティレイヤー（エンドポイント、ネットワーク、クラウドなど）における諸活動を統合的に分析し、脅威を検出・調査・対応することができる新たな情報セキュリティ統合プラットフォームが必要とされる。

本仕様書は、当該プラットフォームに求められる要件を明示し、今後の放影研の研究活動を安全かつ円滑に遂行することができる情報環境の整備を目的とするものである。

2. 調達する情報セキュリティ統合プラットフォームの概要

この度調達を予定する情報セキュリティ統合プラットフォームの概要を以下に記す。調達案件が有すべき技術的詳細については、「Ⅱ. 調達物件が備えるべき技術的要件」を参照されたい。

- ・ 研究所内で稼働する約500台のパーソナルコンピュータ、約100台のサーバ、その他研究所管理者が指定するエンドデバイスをエンドポイントとして設定可能であること。
- ・ ネットワーク監視対象として、フロアスイッチおよびコアスイッチ内で疎通するトラヒックを分析対象とすることが可能であること。
- ・ 水際対策として、既設ファイヤーウォール（Palo Alto Networks 社製：PA850）が生成するログファイルを分析対象とすることが可能であること。
- ・ クラウド監視対象として、Microsoft Office365 E3 Exchange Online の監査ログおよびメッセージトレースログをAPI経由で取得し、分析対象とすることが可能であること。
- ・ 前記した4つのセキュリティレイヤーを統合的に監視・分析・検出・調査が可能な統合セキュリティプラットフォームであること。
- ・ プラットフォームの環境はクラウド型であり、SaaS形式でサブスクリプションとして提供

可能なサービスであること。

- ・ 日本語サポート窓口で問い合わせが可能であること。
- ・ 日本語のドキュメントやサポートサイトがあること。

3. 調達内容

(1) 情報セキュリティ統合プラットフォーム一式

(2) 納品物（成果物は電子媒体として提出のこと）

① 管理者用マニュアル

② 運用操作説明書

③ 環境設定書（連携機能設定を含む）

(3) 納期と納入場所

① 納期 2026 年 1 月 31 日

② 納入場所 公益財団法人放射線影響研究所 情報技術部 システム技術課

4. 作業留意事項等

(1) 作業に関する留意事項

- 1) 受託者（以下「乙」という。）は、本調達物の導入にあたり、本仕様書を遵守すること。
- 2) 乙は、導入における作業の全部または一部を第三者に請け負わせることはできない。ただし、研究所の書面による事前の承認を得たときはその限りではない。
- 3) 前項ただし書きにより、乙が第三者に作業の全部または一部を請け負わせる場合、乙は当該第三者に乙が研究所に対して負うべき義務を負わせるとともに、当該第三者のすべての行為およびその結果についての責任を負う。
- 4) 本仕様書に記載のない事項および本仕様書についての疑義はその都度研究所が指定する所内担当者（以下「甲」という。）と協議して定めること。
- 5) 乙は、作業遂行のために甲より提供を受けた技術上または営業その他業務上知り得た情報（以下「機密情報」という）を第三者に漏えいしてはならない。ただし、次の各号のいずれか一つに該当する情報についてはこの限りではない。
 - ・ 機密保持義務を負うことなくすでに保有している情報
 - ・ 機密保持義務を負うことなく第三者から正当に入手した情報
 - ・ 甲から提供を受けた情報によらず、独自に開発した情報
 - ・ 本仕様書に違反することなく、かつ、受領の前後を問わず公知となった情報
- 6) 乙は、乙の従業員に対し前項の義務を順守させるとともに、乙の従業員から機密情報を受領してはならない。
- 7) 乙は、甲との協議内容について、その都度書面を作成し、甲に提出すること。
- 8) 乙は、事前に甲へ報告した事項に変更が生じた場合は、速やかに書面で甲へ内容を

報告したうえで、再度甲の承認・確認を得ること。

- 9) 本仕様書に明記された事項を履行するための費用は本調達にすべて含まれる。

(2) 個人情報の取り扱い

- 1) 本作業における個人情報とは個人に関係する情報であり、当該情報に含まれる氏名、生年月日その他の記述または個人別に付された番号、記号その他の符号、画像等により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む）をいう。
- 2) 乙は、甲より受託した本作業に伴う個人情報を機密として保持し、事前に甲の書面による同意を得ることなく第三者にこれを開示または提供をしてはならない。
- 3) 乙は、本業務を履行するために必要な範囲でのみ個人情報を利用し、他の用途に利用してはならない。
- 4) 乙は、個人情報への不当なアクセスまたは個人情報の紛失、破壊、改ざん、漏えい等の危険に対して、技術面組織面において合理的と判断される安全対策を講じるものとする。
- 5) 乙は、本業務に伴う個人情報の取り扱いについて、必要に応じて上記以外にも甲の指示に従うものとする。
- 6) 甲は、必要に応じて乙に個人情報の取り扱いについて監査を受けるように求めることができるものとし、乙はすみやかにこれに応じるものとする。
- 7) 乙または乙の従業員が本仕様書に違反したことにより機密情報または個人情報に漏えい・紛失され、研究所または第三者に損害が発生した場合には、乙はその損害を賠償しなければならない。

(3) 調達物の導入作業の要件

- 1) 作業の期間は「本調達案件の契約日を開始日とし、2026年1月31日までとする。
- 2) 作業時間は、原則として「月曜日～金曜日（祝祭日と年末年始12/29～1/3を除く）9時～17時」とするが、研究所の判断のもと、休祭日に支援業務を依頼することがある。
- 3) 1)項に掲げる期間中、所内情報技術部門からの問合せに対して、受付窓口（電話とメール）無制限受付とし、以下の事項に相当する質問や相談があった際に対応すること。
 - ① 操作方法
 - ② 設計および設定に起因する障害対応
 - ③ 軽微な設定変更（サービス全体にかかる大幅な設定変更については、甲と協議の上、別途有償で実施する）

- 4) 導入作業の履行において不具合が発生した場合は、原因の切り分けを行い、本作業に起因するものは対処すること。
また、必要に応じて現地にて対処すること。
- 5) 導入サービスの不具合が判明した場合には、24 時間以内に対応が可能であること。
- 6) 導入作業に係る打合せを必要に応じて適宜行い、またその議事録を作成して研究所の承認を得ること。

II. 調達物件が備えるべき技術的要件

1. 検出機能要件

1.1. エンドポイントセキュリティ要件

- 1) Microsoft Windows 10/11, Windows Server (2016 以降), Linux (主要ディストリビューション), macOS (最新 3 世代以上) に対応していること.
- 2) 仮想環境 (VMware, Nutanix, Hyper-V, Azure, AWS) のゲスト OS 上で動作可能であること.
- 3) シグネチャベースではなく、振る舞いベースによるマルウェア／ファイルレス攻撃の検出が可能であること.
- 4) 検出対象のデバイスのメモリ内の異常挙動、権限昇格、レジストリ改変、スクリプト実行 (PowerShell, WMI 等) などをリアルタイムで検知できること.
- 5) 端末の現在のレジストリの状態が検索で表示できること。また、任意のレジストリがリモートから削除できること.
- 6) MITRE ATT&CK フレームワークに基づく分類表示が可能であること.
- 7) 管理者が任意の対象端末を遠隔で隔離 (ネットワーク遮断) できる機能を有すること.
- 8) インシデントに関連している複数台の端末ネットワーク隔離を一度の操作で同時に実施できること.
- 9) ネットワーク隔離後も管理コンソール経由では当該端末へアクセス可能なこと。また、インシデント対処がリモートから実施できること.
- 10) 端末で現在稼働している全プロセスの一覧、及び端末上にあるファイルの一覧が表示できること (修復前に現状把握がリアルタイムにできること) .
- 11) 任意のファイルがリモートから取得・削除できること。また、ファイル採取時は自動的に暗号化されたアーカイブ形式で、無害な状態で採取できること.
- 12) 自動的に隔離されたファイルの詳細確認、及びダウンロードやリリース (ホワイトリスト登録) が管理コンソールから可能なこと.
- 13) プロセスの強制終了、ファイル削除、レジストリ削除、ログ収集などのリモート操作が可能であること.
- 14) 検出アラート発生時の自動対応ルール (ポリシー) 設定が可能であること.
- 15) 事前に用意した PowerShell で動作するスクリプトを検知等の指定した条件下において自動で実施可能なこと.
- 16) 検知アラートは重大度によってリスク判定されること.
- 17) アラートの一覧はトリアージしやすいように、重要度が自動で表示されること.
- 18) 個別の情報の関連づけを手動で行う必要がなく、自動で端末にまたがるラテラルムーブメントの全体像を可視化できること.
- 19) コマンド実行履歴が確認可能であること.

- 20) 複雑な攻撃（実行された PowerShell のコマンド履歴や、追加/削除されたレジストリの内容、インジェクション履歴などの詳細）がプロセスツリーでわかりやすく表示されること。
- 21) RAT ツールによる攻撃者の操作内容の把握が可能なこと。
- 22) 各エンドポイントから発生するセキュリティ関連イベントログをクラウド基盤にリアルタイムで転送可能であること。
- 23) タイムライン形式でのインシデント可視化、過去の挙動検索機能を提供していること。
- 24) イベントログの保存期間は最低 7 日以上であること。
- 25) 検知有無によらず、エージェントから取得した生ログがリアルタイムに管理コンソールから確認可能であること。
- 26) エージェントから取得した生ログを外部連携できる機能を有すること。
- 27) グローバルな脅威インテリジェンス情報（IOC: Indicator of Compromise）と連携し、疑わしい通信や実行ファイルの検知精度を向上できること。
- 28) 国内脅威情報（JPCERT/CC 等）との連携も可能であることが望ましい。
- 29) エンドポイントにインストールされるエージェントは軽量であり、CPU 使用率が 5% 未満、メモリ使用量は 200MByte 以下であること。
- 30) エージェントはクライアント・サーバ双方にインストールが可能であること。
- 31) エージェントはシングルエージェントで動作すること。
- 32) センサはカーネルモードで作動していること（カーネルレベルの情報をリアルタイムに取得可能なこと）。
- 33) エージェントは本番環境に影響なく展開するためにインストール/アンインストールともに再起動が不要なこと。
- 34) エージェントのアップグレードによる再起動が不要であること。
- 35) エージェントのアップグレードが自動で行えること。
- 36) エージェントの自動アップグレード時には一斉ダウンロードを制御できること。
- 37) エージェントを停止させる行為に対して、防御ができること。
- 38) 将来的に脆弱性管理の機能や DLP の機能、USB デバイス制御などの機能を追加インストール不要でライセンス追加と機能の有効化だけで利用することが可能であること。
- 39) ネットワークの使用量が低い(1 日 5-10MB 程度) こと。
- 40) センサがアンインストールされないように管理者がパスワードでパスワードロックが行えること。
- 41) センサの改ざんなどを検知・防御できること。
- 42) Word 形式・EXE 形式のファイルベース攻撃を検知・自動防御できること。
- 43) Windows 標準の WMI・Rundll32 を悪用したファイルレス攻撃（任意のスクリプトを

実行される振る舞い)を検知・自動防御できること.

- 44) 攻撃者が権限昇格や検知回避のために行うプロセスインジェクションの振る舞いを検知・自動防御できること.
- 45) 標的型攻撃の自動判断が可能であること.
- 46) 攻撃者が証拠隠滅のためにファイルやタスクスケジューラを操作する等の振る舞いが検知・自動防御できること.
- 47) API 等を利用して端末から収集されたイベントを外部へ転送が可能であること.
- 48) プロキシ環境においても正常に通信可能であり, オフライン時にもイベントのローカル保持と再送信機能を有すること.
- 49) 管理者は Web ベースのコンソールから一元的でリアルタイムに全端末の状態を可視化・制御できること.
- 50) アラート通知において, メールおよびMicrosoft Teams との連携が可能であること.
- 51) ロールベースアクセス制御により, 閲覧・捜査権限を設定可能であること.
- 52) 拠点ごとにテナント分けや、テナントの親子関係など、柔軟な構成がとれること.
- 53) 拠点毎にアラート通知先を個別に設定できること.
- 54) アカウントに対してテナント（拠点）単位での権限設定が行えること.
- 55) ライセンスは年間サブスクリプション方式であり, エンドデバイスごとのライセンス数に応じて管理できること.

1.2. ネットワークセキュリティ要件

- 1) 所内に設置されたフロアスイッチ (CISCO 社製 : C2960) およびコアスイッチ (CISCO 社製 : C9500) を対象機器とすること.
- 2) 前項に掲げる機器から出力された syslog を分析対象とすることが可能であること.
- 3) syslog の形式は標準 syslog (RFC5424/RFC3164) およびベンダ拡張形式 (Cisco Syslog 形式等) に対応していること.
- 4) スイッチから送信される syslog は, 所内中継サーバを経由してクラウド上の統合プラットフォームに転送されること.
- 5) 前項に掲げるログ転送は安全性を考慮し, TLS などによる暗号化通信であること.
- 6) 収集されたログに基づき, 以下のイベントの可視化と傾向分析が可能であること.
 - ・ インタフェースの up/down やブロック/アンブロック等の状況変化
 - ・ 新規端末の出現 (MAC アドレスの追加)
 - ・ スパニングツリーに関連するイベント (ルートブリッジの変更, BPDU ループの発生など)
 - ・ ループ構成が原因と思われる MAC フラッピング, ポート遮断, トポロジー変化等の検出
 - ・ リンクフラッピングやケーブル障害に起因するポートの断続的な状態変化
 - ・ 通信ポートの利用状況や通信量の変動傾向

- 7) 過去のログと比較してトラヒックなどに異常な変化がある場合にはアラート生成が可能であること。
 - ・ 業務時間帯以外での新規端末の接続
 - ・ 特定のウェルノウンポート以外での高頻度通信
 - ・ 突発的な DHCP 要求の急増
- 8) 取得されたログに基づき、以下のような識別情報の突合・相関分析が可能であること。
 - ・ MAC アドレス ― IP アドレス ― スイッチのポートの対応付け
 - ・ DHCP ログや ARP ログとの突合による端末装置の特定支援
 - ・ ユーザ情報と EDR 端末装置との関連付けは、別途統合プラットフォーム側で実施可能であること。
- 9) ログ分析結果は Web ベースのコンソール上で可視化可能であること。
- 10) ログは 30 日間以上保管され、CSV/JSON 形式でダウンロードが可能であること。

2. 連携機能要件

2.1. 境界装置連携

- 1) 本調達時における境界装置としては、Palo Alto Networks 社製 PA850 を対象とするが、将来的な装置更新にも対応可能な標準仕様のな仕組みを採用していること。
- 2) 連携可能なログ形式は、Syslog (RFC5424/3164) ベースの標準形式、または CEF (Common Event Format) 等の SIEM 連携形式に対応していること。
- 3) PA850 が出力する以下の主要ログカテゴリに対応していること。
 - ・ Threat ログ
 - ・ Traffic ログ
 - ・ URL フィルタリングログ
 - ・ System ログ
- 4) 境界装置から出力されたログは、クラウド上の統合セキュリティプラットフォームに対して中継サーバを介して安全に転送可能であること。
- 5) 前項におけるログ転送時には暗号化 (TLS, Syslog over TLS 等) されたうえで転送が行われること。
- 6) 収集したログ情報を元に、以下のような境界型の脅威イベントの自動分類・可視化・アラート通知が可能であること。
 - ・ マルウェア通信 (C2) , ランサムウェアによる外部接続
 - ・ ボットネット通信, 異常なポートスキャン
 - ・ Web アクセスにおける不審な URL, カテゴリ違反サイトへのアクセス
 - ・ 不許可ポートや宛先 IP アドレスへのアクセス試行
 - ・ トラヒック傾向の異常 (通信量の急増や外部送信の多発)

- 7) 収集された境界装置のログは、以下の異なるセキュリティレイヤー情報との相関分析が可能であること。
 - ・エンドポイントログ：外部との接続前後の端末挙動を統合表示
 - ・クラウド（m365）ログ：メールを起点としたアクセスの追跡
 - ・Active Directory ログ：通信を発生させたユーザの識別（IP Address⇔端末装置⇔ユーザアカウント）
 - 8) 境界装置からのイベント情報は Web ベースの管理コンソールにて可視化・検索・分析が可能であること。
 - 9) 前項における分析結果が CSV または JSON 形式で出力が可能であること。
 - 10) PA850 だけでなく、将来的に別ベンダの境界装置（Fortinet, Check Point, CISCO ASA 等）の境界装置や UTM 製品のログも取り込みが可能なマルチベンダー対応設計になっていること。
 - 11) ログ種別のカスタムマッピング機能（フィールド正規化）が具備されていること。
- 2.2. クラウド連携
- 1) クラウド連携機能として、以下のクラウドサービスに対応可能であること。
 - ・Microsoft 365 Exchange Online（E3 プラン相当）
 - ・必要に応じて SharePoint Online, OneDrive for Business, Teams にも拡張が可能であること。
 - 2) 監査ログの取得時には、以下のいずれかの API が利用可能であること。
 - ・Microsoft Graph API
 - ・Office 365 Management Activity API
 - 3) 以下のログを分析対象とすることが可能であること。
 - ・メール送受信履歴
 - ・メール転送設定の変更
 - ・添付ファイルの操作（ダウンロード、転送等）
 - ・不審なログイン（多拠点同時アクセス、ログイン失敗回数等）
 - 4) クラウド連携ログから以下のような不振イベントが検出可能であること。
 - ・フィッシングメールの送受信
 - ・不正な自動転送設定の作成・変更（ルールベースの情報漏洩）
 - ・同一ユーザによる短時間での地理的に矛盾するアクセス
 - ・多要素認証バイパスの試み
 - ・マルウェア付きのメールの受信と開封
 - 5) クラウドからのイベント情報は以下と相関分析され、統合的に脅威判定が可能であること。
 - ・エンドポイントログ（受信メール内 URL のクリック後の動作）
 - ・境界装置のログ（メールに記述された URL からの外向きアクセスログ）

- ・Active Directory 情報（対象ユーザの権限，過去の操作履歴との突合）
- 6) 管理者は Web ベースのコンソール上から以下のような可視化・検索などが可能であること。
 - ・メール通信量，危険な添付ファイル数，転送設定変更の履歴
 - ・ユーザ別・部署別のメール通信傾向
 - ・時系列での不審なイベントのトレンド分析
- 7) イベントログは 7 日以上保管され，CSV または JSON 形式でエクスポート可能であること。
- 8) API 等を利用して検知イベントを外部へ転送が可能であること。
- 9) API 連携に利用するアカウントは最小限の権限スコープに制限が可能であること。
- 10) データ転送は TLS による暗号化通信で行われること。

3. 次世代 SIEM 要件

3.1. 製品要件

- 1) エンドポイントやクラウド、ネットワーク機器から取得したログを 1 つのコンソールから統合的な分析が実施できること。
- 2) データの取り込みと健全性を簡単に監視できること。
- 3) 24 時間以上データを受信しなかった際にアラートメール通知を送ることができること。
- 4) ログから検知を発生させるためのルールのテンプレートが用意されていること。
- 5) ダッシュボード機能を使い簡単に取り込んだログを分析・可視化できること。
- 6) カスタムダッシュボードの作成や、インポートが容易にできること。
- 7) インシデント調査機能によって、検知情報や検出されたプロセス、ユーザ、デバイスなどの情報を 1 つの画面上にグラフビューで可視化することで、それぞれの要素の関連性を整理し調査やコラボレーション用に利用できること。
- 8) SOAR の機能と統合され、定型業務を簡単に自動化ができる機能を用意しており、作成した自動化ワークフローのインポートやエクスポートができること。
- 9) 検知を MITRE ATT&CK フレームワークにおける戦術・手法に照らし合わせて分類・可視化できること。
- 10) ログを転送する際に中継サーバが必要な場合には、中継サーバの設定方法のマニュアルが用意されバージョン管理も容易にする機能が実装されていること。
- 11) 取り込んだログに対して分析に活用・参照できる脅威情報データベースを用意しており、ログを取り込めばその他のセットアップが不要ですぐにクエリを通して活用可能であること。

3.2. サービス要件（MDR サービス）

- 1) 対応する機器に関する検知アラートをあげるためのコンテンツを、MDR サービスを

提供するベンダが開発・維持すること。具体的には、2. 連携機能要件に対する検知ルールを MDR ベンダとして保有し、かつ適用されていること。

- 2) 単一のベンダがエンドポイントと SIEM の両方の検知に対して 24 時間 365 日体制で監視、調査、対応（遠隔隔離のみではない）できるサービス提供できること。
- 3) MDR サービスにて SIEM から発出される検知アラートのポジティブ性を判定すること。特に EDR エージェントが入っている機器に関連する検知アラートのポジティブ性については原則 MDR ベンダ側で判定することが望ましい。
- 4) EDR エージェントと緊密に統合され、SIEM 側で発生した検知に対してアナリストが対処するために遠隔から EDR エージェントの入ったエンドポイントへの任意のアクション（調査および対応）が実施できること。
- 5) EDR エージェントからの検知に対する MDR の調査・分析において、関連する SIEM に取り込まれたログを利用することでより深い洞察や対応すべき具体的な施策を導き出すことができること（例えば、Exchange Online のログと EDR の検知アラートを調査することでどのドメインから発せられたメールが起因して検知が上がったため、そのドメインをブロックすべき、など）。

3.3. ログ収集と対応形式

- 1) SIEM は以下のソースからのログをリアルタイムまたはバッチジョブ、または事前に用意されているパーサーなどを利用して収集可能であること。
 - ・ エンドポイント
 - ・ ネットワーク機器（L2/L3 スイッチ）
 - ・ 境界装置
 - ・ クラウドサービス
- 2) 上記以外の任意のログをパーサーやコネクタを用意して柔軟に取り込む仕組みがあること
- 3) 受信可能なログ形式として、Syslog (RFC5424/3164) , CEF, LEEF, JSON, Windows Event Log, API 経由ログ（Graph API ログ等）

3.4. ログ保管と検索機能

- 1) 収集したログは暗号化された状態でクラウド上に保存され、最低 30 日間の保持が可能であること。
- 2) 大規模データでも数秒以内の全文検索が可能であり、正規表現や構造化フィルタによる高速検索に対応していること。

3.5. 相関ルールと脅威検知ロジック

- 1) SIEM 上で以下のような相関ルールの定義が可能であること。
 - ・ IP アドレス、ユーザ ID, MAC アドレス、メールアドレス等の共通キーによるクロスレイヤ照合
 - ・ イベント間の時間的關係性（数分以内の EDR 検知と境界装置アラートの発生）

- 2) 初期構成として MITRE ATT&CK に準拠した検知テンプレートが多数用意されていること.
 - 3) ユーザ, ホストデバイスおよびネットワークトラフィックの振る舞いに基づく異常検知に対応していること.
- 3.6. 対応自動化機能
- 1) 検知した脅威イベントに対して自動的な対応フローを設定・実行可能であること.
 - 2) 組込み型の SOAR 機能, または外部 SOAR との API ベース統合が可能であること.
- 3.7. アクセス制御と監査
- 1) ロールベースアクセス制御により, ユーザ毎に検索・ダッシュボード・対応権限を制御可能であること.
 - 2) SIEM 上での管理者操作はすべて監査ログに記録され, 追跡が可能であること.
- 3.8. 拡張性およびクラウド環境対応
- 1) すべての SIEM 機能は SaaS 形式またはクラウドホスト型で提供され, オンプレミスサーバ構築を必要としないこと.
 - 2) クラウドにデータを圧縮保管することでコストを抑えつつインフラ更新の手間を削減できること
 - 3) 利用規模の拡張 (対象ログ数, 端末数, 保持期間等) に対してスケーラブルに対応可能なライセンス体系であること.
 - 4) 将来的に以下のような外部システム連携が可能であること.
 - ・ Azure Active Directory
 - ・ Windows Defender, 他ベンダ CASB や DLP

4. MDR サービス要件

4.1. 基本要件

- 1) MDR サービスの提供時間は 24 時間 365 日で、アナリストによる有人監視が行われていること.
- 2) MDR サービスの提供 (問い合わせ窓口) は日本語であること.
- 3) MDR に従事するアナリストは対象製品の認定資格を有し、十分なインシデントレスポンス経験を有していること.
- 4) 発生したアラートに対して検知、調査、根絶・修復作業を行うこと.
- 5) 製品が検知しないイベントログに対して、24 時間 365 日でアナリストによるプロアクティブな脅威ハンティングが提供されること.
- 6) 分析するアラートの脅威レベルは製品が定義する重大度「緊急/高/中/低/脅威ハンティング」の全てが対象であること.
- 7) 発生したアラートの調査は発生前後の EDR ログ調査やサンドボックス、独自の脅威インテリジェンス等を活用すること.

- 8) NGAV/EDR の防御ポリシーの設定管理、最適化、および過検知判断時のホワイトリスト登録を MDR 側で実施すること。
- 9) インシデント発生時の端末およびサーバのネットワーク隔離は自動で実施されず業務への影響を鑑みながら MDR チームの人間が判断すること。
- 10) 感染端末の修復に関しては、自動ではなく人間の判断を介してマルウェアの除去・レジストリ修復・スケジュールタスク削除等を実施可能であること。
- 11) 修復作業の実施後に実施した修復作業および分析結果を通知すること。

5. 作業報告書等の作成

5.1. 作業報告書

- 1) 本支援業務の遂行にあたり、実施した業務内容について履行日毎に作業報告書を作成し、その都度甲に提出すること。
- 2) 作業報告書の様式は任意で良い。乙内関係者間において稟議済みであること。
- 3) 提出にあたっては媒体を問わないが、機密事項が記載されている場合には、第三者への漏えいがないように配慮すること。

5.2. 情報セキュリティ統合プラットフォーム環境設定書

- 1) 完成図書として本業務において構築されたすべての環境設定内容について記載された文書を納入期限までに提出すること。
- 2) 当該文書は電子データとし、CD-ROM に格納して 2 部提出すること。

6. 資格

6.1. 受注者の資格

研究所が保有する個人情報を取り扱う業務の性格上、乙は一般財団法人日本情報経済社会推進協会が付与したプライバシーマークの使用許諾又は公益財団法人日本適合性認定協会が認定もしくは相互認証した認証機関（これらの認証機関が認定した認証機関を含む。）から ISO27001 に適合していることの認証を取得している者とする。

7. その他

7.1. 秘密保持

- 1) 乙は支援業務の遂行において取り扱う情報の機微性に鑑み、その取扱いを慎重に行うとともに、業務上知り得た内容を外部に漏えい又は開示してはならない。
- 2) 前項における秘密の保持は、業務委託の履行期間が終了しても継続しなければならない。
- 3) 業務委託の履行期間完了後に、乙または乙の従業員により機密情報または個人情報 が漏えいした場合には、乙はその損害を賠償しなければならない。
- 4) 正当な理由があつてやむを得ず第三者に開示する場合、書面によって事前に甲の承

諾を得ること。また、情報の厳格な管理を実施すること。

- 5) 甲が支援業務遂行のために乙に提供した資料は、原則としてすべて複製禁止とする。ただし、業務遂行上やむを得ない理由で複製する場合であって、事前に書面にて甲の許可を得た場合はこの限りではない。
- 6) 前項において、複製物は使用終了後に研究所に返納しなければならない。
- 7) 乙の故意または重大な過失によって損害が生じた場合には、乙の責により原状復帰されなければならない。

7.2. 検収

- 1) 乙はI.3項(4)に記載された期日までに、I.3項(3)に記載された成果物を甲に納品すること。
- 2) 甲の立ち合いのもとに本仕様書に記載される技術的要件の可否について動作確認を行う。
- 3) 甲は前2項に記載された事項が履行されたことを条件として検収する。

7.3. 疑義

- 1) この仕様書についての疑義、もしくは定めのない事項又は作業中に発生した問題点などについては、その都度甲と乙で協議のうえ、その解決にあたるものとする。

8. 導入実績

- 8.1. 乙は本仕様書に記載された類似業務の受注実績に関する資料を予め甲に提出したうえで、甲の確認を得ること。