電力広域的運営推進機関
EDR 製品及び MDR サービスの調達
に関する
入札仕様書

電力広域的運営推進機関

２０２５年１月

仕様書

1. 件名

電力広域的運営推進機関　EDR 製品及び MDR サービスの調達

2. 目的

本件は、総務省ガイドラインにおいて求められている未知の不正プログラム対策（以下「EDR」という。）、及びそれを活用した情報セキュリティ専門人材によるインシデントの早期検知・対処サービス（以下「MDR」という。）として導入するものであり、初期設定、導入支援等を行う。

3. 契約内容及び契約期間

製品：Cybereason-EDR、Cybereason-Endpoint Prevention、Cybereason-MDR Complete、
Product Support

内容：ライセンス（400 ライセンス）及び 構築運用支援

※内訳：サーバライセンス（１０ライセンス）、クライアントライセンス（３９０ライセンス）

契約期間：2025 年４月１日から 2026 年3月３１日までの１年間

4. 導入業務等

（１） 作業要件

- センサーインストール作業は、当機関が行うものとし、受注者は資産管理ツールを用いた配布を実施できるようにサポートすること。なお、事前配信前にクラウド環境は構築していることとする。
- 共存するウイルス対策の検索対象から、導入する EDR 関連のディレクトリを除外するため、検索除外対象とすべきディレクトリ情報を必ず提供すること。
- センサーをインストールした端末が正常に管理サイトに登録されているか、管理画面で確認できること。
- 当機関管理者向けに、利用方法及びインシデント発生時対応方法等のレクチャーを実施すること。
- インシデント発生時の、対応フローを提示すること。

（２） 端末の機能要件

OS： Windows10 Pro 64bit
Windows10 Enterprise 64bit
Windows11 Pro 64bit
Windows11 Enterprise 64bit

メモリ：8GB～16GB

CPU：Intel

5. システム要件

各機能は以下に記載する要件を有するサービス、ソフトウェアを導入するものとし、必要となる物品の調達及び構築作業を実施すること。

（1） エンドポイントセキュリティ機能

- セキュリティとデータ保護を維持するため、次の既定及び規格の認定をうけていること。
  ISO/IEC 27001:2013
  ISO/IEC 27017:2015
  ISO/IEC 27018:2014
  AICPA：SOC2 Type2
- 監視サービスは、一定の技術要件及び品質管理要件を満たし、品質の維持・向上に努めている情報セキュリティサービスを明らかにする「情報セキュリティサービス基準適合サービスリスト」に登録されていること。
- クラウドサービスとして提供する場合は、日本政府が求めるセキュリティ要件を満たした「政府情報システムのためのセキュリティ評価制度（Information system Security Management and AssessmentProgram: 通称、ISMAP（イスマップ））」を取得していること。
- クライアント・エージェント・ソフトウェアは Windows、Windows Server、Mac、Linux に対応していること。
- クライアント・エージェント・ソフトウェアのインストールにおいては、システムの再起動を必要としないこと。
- クライアント・エージェント・ソフトウェアは、設定情報が含まれる単一のファイルを実行することでサイレント・インストールが可能であること。
- クラウドサービスとして提供する場合は、ログを保存する管理サーバは専用サーバがクラウド上に構築されること。
- クラウドサービスとして提供する場合は、管理サーバは日本国内に設置可能なこと。
- 既知の攻撃のみならず、未知の攻撃にもリアルタイムに対応すること。
- ランサムウェアにおいては、リアルタイムでの対応を必要とするため、管理者がオペレーション関与することなく、Windows 端末にある該当プロセスを停止するなどの処置が自動でおこなえること。
- 攻撃者が利用するファイルやドメインや振る舞いと言った IOC だけでなく、攻撃者の戦術及びテクニックを検知できること。
- 攻撃を検知した場合には、その根本原因、感染した端末の全台の特定、影響範囲の関係、時系列での不正なふるまいの状況を即座に把握できること。
- 正規プロセス（Powershell や WMI など）を不正利用した攻撃も検知できること。
- 感染端末にある検知したマルウェアを管理コンソールより、安全な形でリモートから取得できること。
- エージェントが収集した情報を任意のキーワードで検索できること。また、検索条件に合致する端末、プロセス及びファイルなどが特定できること。検索した結果を CSV にて出力できること。また日本語データの出力にも対応していること。
- 攻撃を検知した場合には、メールにて通知が可能であること。
- 攻撃が検知された Windows 端末に対し、必要に応じて該当プロセスの停止、該当マルウェアの検疫、レジストリの修復を管理コンソールより遠隔操作でおこなえること。また必要に応じて、ネットワークからの隔離もおこなえること。
- 攻撃を検知した場合の上記のオペレーションを検知単位（被害単位）で一括に行うことが

可能なこと。

- 攻撃として検知したファイル以外であっても、管理 UI から遠隔で端末上にある任意の PE 形式ファイルを取得することができること。
- 攻撃を検知したプロセスの前後の親プロセスや子プロセスなどプロセスツリーを表示する機能を有すること。
- リモートシェル機能などで遠隔に存在する端末へのコマンドライン操作などが可能なこと。
- 管理画面よりレポートが日本語で PDF 出力できること。
- 管理 UI が日本語で表示されること。
- 管理 UI へのログインに、2 要素認証を設定できること。
- クライアント・エージェント・ソフトウェアの動作ログ取得、再起動、アップデート、Log アップロードの停止が、管理画面より遠隔にて実施できること。
- 誤検知・過剰検知を低減するために、ハッシュ値やファイル名だけでなく、ふるまい単位での検知除外設定ができること。
- クラウドサービスとして提供する場合は、クラウド側のサーバのバージョンアップの実施時期を利用者側と調整できること。
- 管理サーバのメンテナンス（バージョンアップ作業等）は、ライセンス期間中、回数無制限及び無償で提供すること。
- メーカーは日本に法人格を登記し、社員による製品サポートを実施すること。
- 監視サービスを提供できる体制があること。
- 監視サービスは、メーカーの国内拠点から提供可能であること。
- 初動通知はインシデント検知後に 30 分未満であること。
- 製品の検知ロジックに応じた脅威監視だけではなく、定期的なスレッドハンティングを提供すること。
- 月次で日本語によるレポートが可能なこと。
- 危険度の高い攻撃が検知された場合には、電話にて連絡が可能なこと。
- 攻撃を検知した場合には、高度解析をおこない、その結果を日本語でレポートとして提供すること。

6. 導入支援要件
   - 5. システム要件の項目を導入するための、構築導入支援を実施すること。
   - 本調達で実施した範囲に係る内容の管理者向け教育を行うこと。

7. 運用支援要件
   - 当機関管理者からのサービス利用方法に関する問い合わせは、24 時間３６５日で電話、メール、Web 等の問い合わせ窓口にて受付、対応すること。
     ※問い合わせの対応可能時間帯については、双方協議の上決定すること。

8. 納品物
   - ライセンスの保有を証明するエビデンス資料
   - 製品問い合わせ先を示す資料
   - 各種マニュアル
     ※納品物の詳細内容については、双方で協議し決定すること。

9. その他

本仕様書に記載のない事項及び疑義については、当機関と協議の上決定することとする。