セキュリティ対策システム調達及び運用保守業務仕様書

１　件名

セキュリティ対策システム調達及び運用保守業務

２　目的

本業務は、徳島県の庁内ネットワークに接続される端末等に対し、次世代アンチウイルス（NGAV）及び Endpoint Detection and Response（EDR）機能を備えたクラウド型セキュリティ対策システムを導入するとともに、24時間365日体制の専門家による運用監視サービス（MDR）を利用することで、ランサムウェア等の高度なサイバー攻撃の早期検知、対処、及び被害拡大の防止を図ることを目的とする。

３　納入期限及び利用期間

1. **納入期限：** 令和８年４月１日
2. **利用期間：** 令和８年４月１日から令和１３年３月３１日まで

４　納入場所

徳島市万代町１丁目１番地　徳島県庁５階 徳島県企画総務部情報政策課

５　調達物品の内容及び数量

1. **品名**：セキュリティ対策システム（NGAV、EDR、MDR機能を含む）
2. **数量**：5,500 ライセンス（デバイスライセンス）
   ※５年間の利用に必要となるライセンス及び運用監視サービス、サポート、バージョンアップすべてを含むものとする。

６　機能要件

本調達におけるシステム及びサービスの要件は以下の通りである。

（１）基本要件

1. クラウドサービス（SaaS）型のシステムであること。
2. システムは、以下のセキュリティ評価または認証のうち、２つ以上を取得していること。
   - SOC2 Type II
   - FedRAMP
   - ISO/IEC 27017
   - ISMAP
3. 今後のセキュリティ強化において、本調達範囲に含まれない拡張機能を追加する場合、端末にインストールされているソフトウェアに追加、変更を加える事なく、管理サーバもしくはクラウド側のライセンスを追加するだけで拡張できること。

4. 導入対象OSとして、Windows (11、 Server 2016/2019/2022/2025) 及び Linux に対応していること。一部対応できないOSがある場合は、代替手段を提示できること。
5. 攻撃に悪用されているような脆弱性が報告されていないこと。

（２）エージェント要件

1. システムレベルでの深い監視と、高度な攻撃手法の検知を可能にする目的と、昨今の攻撃のトレンドである、管理者権限などを窃取された場合の機能の停止を考慮し、エージェント（ソフトウェア）は、NGAV、EDR共にユーザモードではなく、カーネルモードで動作すること。
2. スケジュールの調整や再起動待ちで、最新の機能が有効化されないことを防ぐため、エージェント（ソフトウェア）をインストール後、再起動が必要ないこと。
3. エージェントの自動更新機能を有すること。
4. エージェント（ソフトウェア）はEDRSilencerなどの攻撃によって機能を無効化、強制終了される攻撃に耐性を持つこと。
5. 端末がオフライン状態でもマルウェア、ファイルレス攻撃の検知、ブロックができること。

（３）検知・防御要件

1. シグネチャ配信による通信負荷及び、シグネチャバージョンの運用管理負荷をなくすため、シグネチャに依存しない、新しい検知技術を実装していること。
2. IOC（脅威の痕跡）だけではなくIOA（攻撃の痕跡）による検知、ブロックができること。
3. Powershellを使うファイルレス攻撃の検知、ブロックができること。
4. ファイルレスの攻撃にも対応するため、プロセスの不正な振る舞いに対しても自動的にブロックする機能を有すること。
5. 最近の攻撃手法である、正規ドライバを偽装した攻撃や、未知の脆弱性を悪用した攻撃の分析ができるように、カーネルのメモリダンプ(フルメモリダンプ)が取得できること。
6. インシデント対応時の証跡保全と詳細分析のため、マルウェアの隔離ができること。誤検知時は隔離前の状態に復元できること。
7. リスクの軽減とブロック率の向上のために、ファイルの実行時だけでなく、実行される前のファイルの書き込み時にもログが収集される機能を有すること。
8. アラート発生時のトリアージを容易にするために 「Critical」や「Low」などの重要度（３段階以上）が自動的に表示されること。

（４）管理・分析要件

1. 各機能の管理は同一のクラウド管理コンソールで実施できること。
2. 庁内に管理サーバの設置・設定が必要無いこと。
3. 端末のグルーピングができ、グループごとに任意のポリシー（ブロック設定、自動更新）が適用できること。
4. ブロックの設定が柔軟に行えるようにするため、サーバや業務端末、利用する組織ごとにグルーピングが自動的に行え、それぞれのグループごとに異なるブロック設定が適用できること。
5. 個別に端末の範囲を指定してグループ化でき、新規クライアント・インストール・管理運用時には、管理グループの指定が可能なこと。機能を有していない場合、メーカー運用にて対応を行うこと。
6. クライアントの設定の確認/変更はクラウド管理画面上からしか実行できないこと。

7. インシデント調査において、以下の詳細情報の確認・可視化が可能であること。
    - コマンドラインの内容
    - イベントログの内容
    - 別プロセスへのインジェクション状況
    - プロセスが実行したディスク上の書き込み／読み込み
    - プロセスが実行したネットワークオペレーション(DNS、IPアドレス)
    - プロセスが実行したレジストリ上の更新
    - インシデントに紐付く各プロセスの動作の可視化（正規プロセス含め）
    - ファイルハッシュ、ファイル名、ホスト名、ドメイン、IPアドレス等による調査
8. 昨今のランサムウェアによる被害報道を鑑み、最新の脅威情報をリアルタイムで取得した上で、独自の脅威インテリジェンス(攻撃者、攻撃の分析情報等)に基づき未知の攻撃に対する防御力を向上させること。
9. 攻撃者の特定と攻撃手法の理解による効果的な対策立案のため、検知された脅威を自動的に照合し、攻撃者の情報がリアルタイムに表示されること。
10. 独自の脅威インテリジェンス構築のための追跡グループ数が少ないと、重要な攻撃者を見逃す可能性が高まることから、十分な数の攻撃者グループを追跡していること。
11. 管理画面より端末をネットワークから隔離・解除ができること。
12. 端末の紛失または盗難時に、リモートでPC内のデータの削除ができること。
13. ネットワーク全体のセキュリティレベルを維持し、侵害拡大を防止するため、セキュリティ対策ソフトウェアが導入されていない端末の把握ができること。
14. セキュリティ対策ソフトウェアが導入されていない端末からの侵害を導入されている端末で検知した場合、未管理端末を特定し通知が可能であること。
15. 管理画面より端末に対してリモートにより脅威の調査、除去などが行えること。
16. ハッシュ値によるブラック／ホワイトリスト登録が可能なこと。
17. イベントログファイルが取得できること。

（５）運用監視サービス（MDR）要件

1. 日本語によるメール・電話での問い合わせに24時間365日対応すること。
2. セキュリティ対策システムの、監視、調査、およびスレットハンティングのサービスを提供すること。
3. サービスの提供は、24時間365日であること。提供時間内において、インシデント発生の影響を最小化するために必須である、検知、トリアージ、詳細調査、対応（修復含む）のサービスを提供すること。また対応（修復含む）はチケット制などの回数制限がなく、かつ、追加費用も発生しないこと。
4. 標準化された修復プロセスにより、迅速かつ確実に端末を復旧ができるように、あらかじめ設定された対処フローに応じて、端末の修復作業を行い、速やかに復旧させること。また、その修復結果については、完了時にメールにて報告されること。
5. 特定インシデントについて、そのインシデントへの対応終了後にレポートを提供すること。レポートには、影響を受けたホスト、侵害の痕跡情報 （IOC）、推奨される軽減オプションを適宜示した脅威詳細情報を記載すること。
6. 発生したインシデントについて、EDRのアルゴリズムだけでは誤検知や見逃しが発生するため、専門家による分析で精度の向上を想定し、EDRの判定だけではなく、運用管理サービスによる分析調査による判定を行い脅威の隔離、端末の隔離措置が行えること。
7. 昨今の高度な攻撃は単一のアラートではなく、複数のイベントの相関関係から判断する必要があるため、分析調査にはアラートの調査、テレメトリーデータの調査、エンドポイントに対する直接的な調査が含まれること。

8. 最新の脅威に対応するため、常に最新バージョンを維持することを目的に、セキュリティ対策ソフトウェアのバージョンアップ、ポリシーチューニングが運用管理サービスにて行えること。
9. セキュリティ対策システムから送信されたログ、データ、不審イベントを監視し脅威インテリジェンス、攻撃手法等と関連付けてインシデントと想定される事象を特定する機能を有すること。
10. インシデントと想定される事象を特定した場合は、速やかに通知すること。
11. 侵害の痕跡情報 (IOC) に基づき潜在的脅威有無を確認できる機能を有すること。
12. 監視対象について常時監視を行い、本調達で対象となる製品の領域の相関分析できる機能を有すること。
13. 昨今の攻撃ではEDRが導入されていたにもかかわらず、それを上回る高度な標的型攻撃が発生した事例があるため、そのような脅威を早期発見する目的で、機械的に検知できない脅威を24時間365日でメーカーアナリストによる監視、探索により検知精度を強化する体制をとること。なお、サービスの安定性と専門知識の蓄積による高品質なサービス提供の保証のために、TAM等のアカウントマネージメントによるアカウントごとの個別サービスは不可とする。また、そこで発見された新しい脅威について管理画面上にアラートを通知すること。
14. アラートがCritical以外でも攻撃に利用されることが多いため、早期対応ができるよう、発生したアラート全てをトリアージし優先順位をつけ、その全てについて調査対応すること。
15. 単純にシステムが検知したイベントをそのまま通知するだけではなく、あらかじめ設定された対処フローに応じて、端末の修復作業を行い、速やかに復旧させること。また、その修復結果については、完了時にメールにて報告されること。
16. 重要システムの隔離といった大きな業務影響を伴う判断など、分析調査時において確認を要する場合、運用管理サービスから管理者に対して確認が行われ、その結果に応じて対処されること。
17. 監視対象環境でサイバーセキュリティ脅威となる可能性があり、追加措置または分析の必要があると判断した場合、対象事象に対して更なる追加調査を実施し、該当するイベントがサイバーセキュリティ脅威であるか否かを判断すること。
18. サイバーセキュリティ脅威だと判断された場合、関連するイベントおよび一連の攻撃全般を含めてインシデントと定義し、必要に応じてスレットレスポンスの対応をすること。
19. インシデントが確認された場合、必要に応じて下記内容を実施すること。
    a. 調査の為の情報収集
    b. 侵害の痕跡情報(IOC）に基づく潜在的脅威の確認
    c. 是正措置案の提案
    d. 発生したインシデントに対するレビューとセキュリティ強化・是正措置に関するアドバイス
20. インシデントが発生した際は、残存脅威を適切に駆除・根絶する機能を有すること。

7　運用・保守要件

1. **導入支援**　　：正常に稼働するまでの導入支援を行うこと。
2. **トレーニング**：運用担当者に対し、管理画面の操作等に関するトレーニングを１回実施すること。
3. **障害対応**　　：提供するクラウドサービスに起因する不具合に対し、迅速に対応すること。
4. **誤検知対応**　：誤検知（過検知）が発生した場合、県担当者と連携し、例外設定等のチューニングを行うこと。