【仕様書 別紙】マルウェア対策およびEDRの機能要件

目次		詳細要件
1	マルウェア対策	
	機能概要	
		エンドポイント（対象端末）に対してエージェントソフトウェアを導入することで、マルウェア（コンピュータウィルス等の悪意ある動作を行うソフトウェア）に対する「侵入されないための機能」を提供できること。
	機能詳細	
		パターンファイルやシグネチャ等のパターンマッチング方式に加えて、ふるまい検知（脆弱性を突いた不審な動作を検知）やサンドボックス等の機械学習方式により、マルウェアの検知ができること。
		Mac OS、Linuxに対してもパターンマッチング方式のスキャン機能を提供できること。
		対象端末として、各業務端末の他、サーバについても利用できること。
		即時スキャン及びスケジュール設定による定時スキャンができること。
		マルウェアをリアルタイムで検知できること。
		最新のパターンファイルを自動で更新できること。
		マルウェアに感染したファイルを自動隔離できること。
		USBメモリ等の接続時にスキャンが実行できること。
		マルウェアが検知された対象端末に対して、マルウェアの遮断（通信遮断、ファイル削除等）ができること。
		対象端末利用者によるエージェントソフトウェアの無効化やアンインストールを防止できること。
		一定期間、管理サーバと通信していない対象端末の台数を管理サーバ上で確認できること。
		管理サーバにより、対象端末に対して即時スキャン及びスケジュールスキャンの設定ができること。
		管理サーバにより、全ての対象端末の一元管理ができること。（管理サーバの台数は問わない。）
		対象端末を管理サーバ側でグルーピングして、グループごとに異なる設定を適用できること。
		エージェントソフトウェアのアップグレードや設定変更について、管理サーバから実施できること。
		エージェントソフトウェアのインストーラーを管理サーバからダウンロードできること。

2	EDR	
	機能概要	
		エンドポイントにおいてマルウェア等の脅威が侵入した後に「被害を拡大させないための機能」を提供できること。
	機能詳細	
		各エンドポイントからログの収集ができること。また、収集したログを一定期間保存できること。
		収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい等による検知の他、感染の痕跡（IOC Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知できること。
		マルウェア等の検知後、C&Cサーバ（Command and Control Server）との通信遮断や特定プロセスの停止等を管理サーバ側から実施できること。本機能については、マルウェア対策による対応も可とする。
		被害があった対象端末に対して、被害の拡大を防ぎつつ、迅速な対応を行うため、セキュリティインシデント対応で利用する通信（例えば、調査を行うためのリモート接続等）以外の通信を全て遮断できること（論理抜線）。本機能については、マルウェア対策による対応も可とする。
		収集した情報（ファイルハッシュ(MD5/SHA1/SHA256)、ファイル名、プロセス名、WindowsイベントID、アクセス先URL等）を基に、マルウェア等の脅威がどの端末から感染し広がったのか、他の端末に広がっていないか、どのような被害（どのファイルがアップロードされたのか、どの管理者権限が奪取されたのかなど）があったのか、などについて、調査、分析ができるとともに、わかりやすく可視化できること。
		管理サーバ上で、特定のエンドポイントにおけるマルウェアの動作等について時系列等、わかりやすく表示できること。
		対象端末のデスクトップに管理サーバからリモートアクセスができること。ただし、EDRと別製品による対応も可とする。
		情報漏洩対策として、ファイル変更にかかる情報だけでなく、ファイル書き込みにかかる情報も取得できること。
		セキュリティインシデント発生時における動作中のプロセスについて、時系列で前後関係がわかるようにツリー表示等ができること。
		対象端末利用者によるエージェントソフトウェアの無効化やアンインストールを防止できること。
		一定期間、管理サーバと通信していない対象端末の台数を管理サーバ上で確認できること。
		エージェントソフトウェアのCPU利用優先度を管理サーバ側で設定できること。ただし、エージェントソフトウェアを導入することによるCPU負荷等への影響が軽微な場合は、不要とする。
		管理サーバにより、全ての対象端末の一元管理ができること。（管理サーバの台数は問わない。）
		対象端末を管理サーバ側でグルーピングして、グループごとに異なる設定を適用できること。
		エージェントソフトウェアのアップグレードや設定変更について、管理サーバから実施できること。
		エージェントソフトウェアのインストーラーを各端末からアクセス可能なサーバ（管理サーバ、イントラサーバ等）からダウンロードできること。
3	SOC(NOC)	
	機能概要	
		マルウェア対策によるアラートを監視するとともに、EDRにより収集したログの常時監視、又は、全エンドポイントに対するログ分析等を通じて、セキュリティインシデントが発生した際に、具体的な影響の把握、当該対象端末の隔離による脅威の拡散抑止、全対象端末を対象とした被害範囲の特定、脅威除去支援および回復支援等のセキュリティ監視等業務を提供できること。
	機能詳細	
		セキュリティ監視等業務のサービスを24時間365日提供できること。
		セキュリティ監視等業務におけるマルウェアの検知として、マルウェア対策やEDRによる判定結果だけでなく、収集したログ等にかかるログ分析（SIEM）の結果や、SOC（NOC）が有する脅威インテリジェンス等による総合的な判定基準から、危険度（アラートレベル）の判定ができること。
		危険度は4段階（0～3）以上で定義し、危険度に応じた対応ができること。
		危険度に応じて、接続団体毎に対応フローを策定でき、運用できること。なお、対応フローには、隔離措置時における運用管理者の承認確認や、危険度、重大度、時間帯などの条件等による、初期通知や初期対応の内容を盛り込めること。
		セキュリティインシデントが発生した際、初期対応に必要な情報について、初期通知ができること。
		初期通知は、危険度の判定後60分以内の通知を目標とし、通知内容に「セキュリティインシデント概要」、「対応状況」、「対策の必要性と推奨される対策内容」を可能な限り含めること。
		初期通知は、SOC（NOC)からメールでの通知だけでなく、指定された番号に対して、電話による連絡ができること。また、平日業務時間内、平日業務時間外、土日祝祭日で通知先の切り替えができること。

	セキュリティインシデントの発生後、初期通知に加えて追加の通知が必要と判断した場合、速やかに、詳細の分析結果（セキュリティインシデントの発生に至るまでのプロセスや影響範囲など）を通知できること。
	セキュリティインシデントが発生した場合、対応フローに従い、初期対応ができること。
	初期対応として、判定された危険度に応じて、脅威（検体）や被疑端末の隔離等の措置が60分以内に可能なこと。
	疑わしい端末を一斉隔離できること。
	対応フローについて、追加や変更が無償でできること。
	解析等により特定されたマルウェア等について、セキュリティ対策やEDRで駆除できなかった場合、脅威を除去するための支援ができること。このとき、マルウェア本体の除去だけでなく、侵害の痕跡を含めた除去作業について支援し、再検知されない状態にできること。また、再発防止策等（検出された検体のファイルハッシュ値などを用いたブラックリストの登録、攻撃に用いられたC&Cサーバーの URL情報や適用すべきパッチ、ソフトウェア情報の提供等）の対応ができること。
	本県からの要望に応じて、EDR以外の関連するセキュリティ装置（ADサーバーやUTMファイアウォール、プロキシなど）にかかるログの突合調査も対応可能なこと。
	検知したセキュリティインシデントに対する支援について、費用の追加なしに回数無制限で対応できること。
	組織内に侵入潜伏している未検知のマルウェア等に対して、本県からの要望に応じて、月に1回以上、全端末の一斉調査（脅威ハンティング）が実施できること。
	業界団体から早期警戒情報など緊急情報を入手した際、回数無制限で脅威ハンティングが実施できること。
	月次レポートを提出すること。
	報告会を実施できること。