（様式第３号）必須機能要件確認票

貴社名

No	区分	要求仕様	可否	補足事項
1	共通事項	収集データ、ログは異なる団体の情報が共有されないよう分割されていること。		
2		管理サーバ及び管理画面へのアクセスは、制限をかけられること。		
3		脅威インテリジェンスを有しており、かつ、複数のリソースを活用して構築されていること。		
4		管理画面、インシデントの報告に関しては日本語で行われること。		
5		クライアントエージェントのアップグレードにおいて、管理画面から実施可能なこと。		
6		クライアントエージェントは設定情報を含めることができ、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。		
7		クライアントエージェントは、収集データとしてファイルコンテンツ（ファイルの中身）は収集しないこと。		
8		クライアントエージェントは、Windows 8、8.1, 10(22H2まで)、11 (22H2まで)、Windows Server 2008 R2 SP1、2012、2012 R2、2016、2019、2022、Red Hat Enterprise Linux 7.x/8.xに対応すること。		
9		既存ウィルス対策ソフト（Trend Micro ）と展開作業時等共存できるように、対象端末について管理機能によりNGAV機能を停止させることができること。		
10	3-2（1） NGAV防御	既知の攻撃のみならず、未知の攻撃にもオフラインでリアルタイムに対応すること。		
11		サンドボックスを検知回避する技術を持った攻撃にも対応すること。		
12		検知、防御したマルウェアは管理画面上で既知・未知の判断が可能であること。		
13		ファイルレス攻撃に対応していること。		
14	3-2（2） EDR検知・分析	あらゆるファイル型の攻撃を検知できるだけでなく、ファイルレスマルウェア（メモリに対して直接書き込まれる悪意ある振る舞い）にも対応すること。		
15		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、時系列での不正な振る舞いの状況を即座に把握できること。		
16		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。		
17		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。		
18		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。		
19		端末のログ収集は、端末がネットワークに接続していない間も収集可能であること。		
20		一度検知した危険なバイナリについては、端末がネットワークに接続していない状態であってもその実行を防止する機能を有すること。		
21		ファイルの操作履歴が取得可能なこと（例：ファイルの作成履歴など）		
22	3-2（2） EDR調査・復旧	攻撃が検知されたWindows端末全てに対し、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を台数無制限でおこなえること。		
23		攻撃として検知したファイル以外であっても、管理画面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。		
24		クライアント・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、プロセスおよびファイルなどが特定できること。		
25		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。		
26		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		
27	3-2（3） EDR運用	クライアント・エージェント・ソフトウェアの動作ログが、管理画面より遠隔にて取得できること。		
28		管理画面にアクセスする複数のユーザが作ることができ、それぞれの閲覧範囲、システム設定の権限、メール通知の有無を個別に設定できること。		
29		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、アップデート等が、管理画面より遠隔にて実施できること。		
30		誤検知・過剰検知を低減するために、検知除外設定ができること。		
31		NGAV機能として、従来のパターンファイル方式のAV機能を用いる場合、更新間隔や端末のスキャンに関しては、実施タイミングを管理画面により設定できること。		
32		インシデント発生時の状況把握を効率化する目的として、組織内で進行する攻撃の状況（攻撃フェーズ、感染規模、経過時間、統計情報）を直感的に確認できる管理画面を有すること。		
33		インシデント解析結果の概要抽出画面により、影響する端末及びユーザー、根本原因、通信の状況、用いられた悪質なプロセス、複数端末にまたがる攻撃のタイムライン表示等が行えるとともに、当該画面より各種対処（端末隔離、プロセス停止、レジストリ削除、ファイル隔離、リモートシェル）へ遷移できること。		
34		インシデント発生時に、対応漏れや二重対応を防ぎ、効率的に対応状況を管理する機能として、対応結果の管理、レポート出力、ラベル管理、攻撃タイプ、根本原因、感染端末、台数等が一覧で確認・管理できる機能を有すること。		

No	区分	要求仕様	可否	補足事項
35	3-2（3） SOCサービス	監視サービスを提供できる体制があること。		
36		監視サービスは日本語対応可能であること。		
37		監視サービス拠点には、上級セキュリティアナリストが常駐していること。		
38		監視サービスはEDR/NGAV製造及びサービス提供元により直接提供可能であること。		
39		必要に応じて、日本語でのインシデント発生時の報告、管理画面での標記、レポートの提供を行うこと。		
40		攻撃の兆候を振る舞い分析や攻撃手法などから洗い出し、自動脅威ハンティング機能により脅威の検知が行えること。また、検知した場合は、メールによる通知及びそれらの脅威に対する推奨対策を実行（脅威の隔離・除去・修復）すること。		
41		サービス提供元において、全世界より収集された最新の攻撃手法に基づき、本市の監視対象から収集される情報に対して、リアルタイムに高精度の監視を実現できること。		
42		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。		
43		攻撃を検知した場合には、高度解析をおこない、脅威の隔離・除去・修復を行った結果を日本語で通知すること。除去・修正を行わない場合は、検知結果を日本語でのレポートとして提供すること。		
44		監視サービスにおいては、事前の取り決めによって、危険な活動が認められた場合に、当該プロセスを停止等の初動対応が可能なこと。		
45		検知サービスは年末年始も含め３６５日提供できること。		
46		事前の取り決めによって検知した脅威や攻撃の隔離・除去・修正を行うこと。除去・修正を行わない場合は、検知された脅威や攻撃、抑止制御策、および関連する不審な挙動に関してEmail・電話による問い合わせ対応が可能なこと。		