仕 様 書

1 目的

宮崎県の次世代セキュリティ運用システムにかかる機器及びライセンスの導入について、必要な仕様を定める。

2 システムの賃貸借期間

令和８年３月１日から令和１３年２月２８日（６０月）

3 数量等

次世代セキュリティ運用システム　一式

4 履行場所

宮崎県庁防災庁舎（宮崎市橘通東 2 丁目 10 番 1 号）

5 概要

本業務では、下記内容の機器及びライセンス及び保守を調達すること。

（１）　県庁 LAN 設備のうち、次に掲げる機器の更新や付随するライセンス並びに保守を調達すること。

＜県庁 LAN 設備機器＞

・IPS（不正侵入防御装置）

・NDR(ネットワーク脅威検知システム)

・EPDR（エンドポイント保護監視対応）

・MAM（モバイルデバイスアプリケーション制御）

・ZTNA（ゼロトラスト・ネットワーク・アクセス）

・インターネットファイアウォール

（２）　既存エンドポイント管理システムの管理デバイスを 1000 デバイス追加できるライセンスを調達すること。

6 機器の仕様

参考製品名等を示しているが、仕様を満たす同等の機器であれば、製造者・製品名は問わない。

（１） IPS（不正侵入防御装置） 1 台

下記仕様を満たす機器を導入し、発注者が指示する構成に向けて、設定及び接続作業を実施し、令和８年３月１日から 5 年間の利用が可能であること。

ハードウェア要件	
1	FPGA を採用した専用設計のハードウェアであること。
2	19 インチラックに固定可能であること。ラック占有は 1RU 以下であること。
3	GbE RJ45 インターフェースを 8 ポート以上搭載していること。

4	SFP+ポートを 2 ポート以上搭載していること。
5	ネットワーク IO モジュールを利用することにより、GbE RJ45 インターフェースを 4 ポート以上拡張可能であること。
6	管理ポートについて、RJ45 MGMT を 1 ポート以上備えること。
7	最大同時接続数が 2,000,000 以上であること。
8	毎秒接続数が 90,000 以上であること。
9	SSL 複合時のスループット(SSL トラフィック 100%の場合)が 0.6Gbps 以上であること。
10	60 か月の保守を調達すること。

機能要件	
1	ネットワーク型 IPS および IDS 両方の動作が可能であること。
2	In-Line 構成で導入する事により、シグネチャに定義された攻撃等をリアルタイムにブロックする機能を有し、監視ポートから TCP リセットパケットを送信し、攻撃通信を遮断可能な機能を有すること。
3	アプリケーション、国情報、有効にする時間帯を含めた ACL を作成する機能を有すること。
4	1500 種類以上のアプリケーションを識別し、且つ制御することが可能であること。
5	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる不審なファイルを脅威情報として活用し、検知・防御することが可能であること。
6	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる不審なファイルを予めローカルで定義したハッシュリストの情報を活用して、検知・防御することが可能であること。
7	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる PDF/Flash/MS Office ファイルに不審な Script が存在した場合に、センサ内部で当該 Script を実行して不審かどうかの判別を行う機能を有すること。
8	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる不審なファイルをセンサ内部の振る舞い検知エンジンにより、シグネチャに依存しない形で検知・防御することが可能であること。
9	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる不審なファイルをクラウド型、或いはオンプレミス型のサンドボックス解析エンジンとの連携により、シグネチャに依存しない形で検知することが可能であること。
10	1 台で、In-Line モード、SPAN モード、TAP モードの併用が可能であること。
11	Fail-Open 機能を使用することにより、アプライアンスの障害発生時に通信を確保するモードへの切り替えることが可能であること。
12	攻撃検知ロジックが公開されており、攻撃検知時にパケットログを使用した誤検知判断が可能であること。
13	センサ内部にボットネット検知用の IP アドレス、URL、ドメイン等のブラックリストを持ち、シグネチャ無しでボットネット通信を検知可能であること。
14	Fast Flux/DGA 技術を利用したボットネット挙動を検知可能であること。
15	SMTP 通信、HTTP 応答通信、FTP 通信に含まれる不審なファイルをファイル解析機能を持つアプライアンスへ送信し、解析結果に応じたアクション（アラート、ブロック等）を取る機能を有すること。
16	閾値ベースでの DDoS 検知技術と、ネットワークトラフィック特性をプロファイリングする機能(自己学習プロファイリング機能)による DDoS 検知技術の両方を有すること。
17	開発元が提供するシグネチャの重要度が変更可能であること。
18	レポートの内容及びレポート作成画面が日本語化されていること。
19	MITRE ATT&CK のフレームワークを取り入れたアラート解析機能を有すること。攻撃者が使用する敵対的な戦

	術、テクニック、および関連するサブテクニックを示すマトリックスの形式でアラート参照が可能なこと。
20	開発元が提供するシグネチャ以外にカスタムシグネチャ作成機能も有すること。
21	カスタムシグネチャでは正規表現も指定可能な文字列のパターンマッチングと数値の比較による検査が可能であること。
22	カスタムシグネチャは標準で用意されているテンプレートで作成する機能を有すること。
23	カスタムシグネチャのテンプレートは、URL の検出、電子メールの添付ファイル名検出、DNS クエリ応答の検出、特定 IP アドレスからの TCP 接続施行の検出等が用意されていること。
24	マネージャーサーバの管理は専用クライアントをインストールすることなく Web ブラウザから可能であること。
25	機能要件を満たすソフトウェアライセンスを 60 か月調達すること。

参考機種：Trellix NS-3600

（２） NDR（ネットワーク脅威検知システム）

本県では、ネットワーク全体の可視化および脅威の検出を目的として、NDR（Network Detection and Response）ソリューションを導入する。

発注者が指定する本庁および各総合庁舎に設置されたネットワーク機器に対して、sFlow の設定を行い、ラテラルムーブメント（水平移動）などの脅威を検知可能な仕組みを構築すること。

また、VLAN ID 単位でネットワークの可視化および制御が可能であり、最大 12,000 台のデバイスを監視対象とすることができる、エージェントレスな仕組みとすること。

下記の仕様を満たす製品を導入し、令和 8 年 3 月 1 日から 5 年間の利用が可能であること。

機能要件	
1	任意のネットワーク範囲を柔軟に指定可能であること。
2	デバイスの種類およびサーバの種別を任意に設定・変更可能であること。
3	CSV ファイルを用いたデバイス情報の一括インポートが可能であること。
4	事前定義された静的ポリシーが存在すること。
5	静的ポリシーの編集および新規追加が可能であること。
6	ポリシーの有効／無効（アクティブ／非アクティブ）切り替えが可能であること。
7	ポリシーの重要度（優先度）を変更可能であること。
8	ポリシー違反が検出された場合、自動的に通信をブロックできること。
9	内部から外部の通信で telnet、ftp、ssh、RDP 通信の制御が可能であること。
10	外部から内部の通信で telnet、ftp、ssh、RDP 通信の制御が可能であること。
11	内部から外部への異常な接続数の増加を検出できること。
12	外部から内部への異常な接続数の増加を検出できること。
13	内部から外部への異常な長時間通信が検出できること。
14	外部から内部への異常な長時間通信が検出できること。
15	High ポート（動的ポート）の使用を検出できること。
16	脅威国への通信および脅威国からの通信を検出できること。
17	脅威国の定義は管理者が任意に編集可能であり、最新の脅威インテリジェンスに基づく更新が可能であること。

18	任意の通信サイズを定義し、ファイル共有サイト等への大容量通信を検出できること。
19	NDR が検出した IP アドレス、ネットワーク、ドメイン等のゾーン情報を任意に変更可能であること。
20	NDR が管理するブロックリストと、ネットワーク上の全通信に含まれる IP アドレスを照合することが可能なこと。
21	ブロックリストに一致する IP アドレスとの通信が発生した場合、自動的にアラートを生成すること。
22	ブロックリストの監視対象は、内部デバイスゾーンから外部ドメインゾーンへのすべての通信とすること。
23	ブロックリストの情報は定期的に更新されること。
24	ポリシー設定において、特定の内部サブネットや組織単位を監視対象から除外可能であること。
25	ユーザー独自の高リスク IP アドレスを宛先ゾーンに追加し、例外ポリシーまたは独自ポリシーとして設定可能であること。
26	ランサムウェア攻撃に対する防御体制の整備状況を評価するレポートが作成可能であること。
27	ネットワーク上で発生した脅威、脆弱性、ポリシー違反、資産の可視性に関する情報を収集・分析したレポートが作成可能であること。
28	レポートは指定された期間（週次、月次）に基づき自動生成が可能で、指定した複数の受信者へメール配信が可能であること。
29	レポートは、PDF 形式で発行及びダウンロードが可能なこと。
30	クラウド管理コンソールの設定により、レポートヘッダ部分のロゴを任意の画像へ変更可能であること。
31	NetFlow（v5 および v9）、sFlow、IPFIX の収集をサポートしていること。
32	ネットワーク機器の NetFlow（v5 および v9）、sFlow、IPFIX を収集するコレクションエージェントは、下記 OS をサポートしていること。 Microsoft Windows10、11、Windows Server2022 Ubuntu 22.04 Server LTS, Ubuntu 24.04 Server LTS
33	契約ライセンス数を超過するアクティブデバイスを検出しても動作を停止しないこと。
34	ライセンスの使用状況は、クラウド上の管理コンソールから常に確認することができること。
35	IP デバイスの合計数が確認でき、内部デバイス、外部デバイスの数が把握できること。
36	ネットワーク上のデバイスを自動的に検出・分類できること。使用目的（重要資産、業務用端末など）に応じて適切なデバイスグループを構成できること。
37	境界を越える南北トラフィックおよびネットワーク内部を横断する東西トラフィックを継続的に監視・分析できる機能を備えていること。
38	組織の通常の運用に基づいて正常なネットワークトラフィックを識別し、異常と判断される疑わしい通信を可視化できること。
39	機械学習や高度な分析技術を活用した非シグネチャベースの検知手法と、既知のパターンに基づくシグネチャベースの検知手法の両方を提供できること。
40	機械学習、深層学習、機械推論などの AI(人工知能)技術を活用して脅威検知・分析を行うこと。
41	NDR は SaaS で提供が可能なこと。また、情報資産の保存先を日本リージョンのみに留めることができること。
42	システムへのアクセスは、Edge、Chrome、Firefox などの一般的なブラウザでアクセス可能で MFA 機能を有すること。
43	送信元 IP アドレスや宛先 IP アドレス、ポート番号、TCP フラグ、ホスト情報に基づいてパケット検索が可能であること。

44	イントラネット外の外部デバイスについても、IP アドレスや組織情報、国、場所などの情報が確認できること。
45	AI(人工知能)技術を活用し下記の内容を含むアクティビティを検知し、管理者にメールで通知が可能なこと。 ・ブロービングまたは偵察活動 ・ピアツーピアによる漏洩 ・ラテラルムーブメント ・トンネリング技術を悪用したデータ外部送信及びポリシー回避 ・情報資産に対する不審な活動 ・データ漏洩 ・ポートスキャン ・IP スキャン ・学習できてないプライベート IP に対する通信 ・OS フィンガープリンティング ・サービスフィンガープリンティング ・エクスプロイト ・攻撃に使用されるリレーホスト ・TOR ネットワークを利用した匿名化通信 ・ボットネットによる収益化行動（クリック詐欺、ビットコインマイニング、DoS 攻撃、スパム送信など） ・ランサムウェアによるファイル共有の暗号化行為 ・ブルートフォース攻撃
46	AI を利用し、リスクと脅威が計算された上で、脅威スコア付けが可能であること。
47	クラウド管理コンソールのユーザー管理は下記内容のロール設定が可能であること。 ・全てのサービスの設定や管理、ユーザーの追加、編集、削除などが可能なフルアクセス権限。 ・サービスの設定に関する権限のみ付与され、その他は読み取り権限。 ・読み取り権限のみ。
48	クラウド管理コンソールは標準機能として多階層管理（マルチティア・マルチテナンシー）が実装されていること。
49	NDR およびクラウド管理プラットフォームに関するヘルプガイドが Web で公開されていること。
50	NDR 及び EDR は、同一クラウド管理コンソール上から一元的に管理できること。
51	最低 7 日間のメーカーによるオンサイトの導入支援サポートが含まれていること。
52	サポート体制においては、海外ベンダー本社とのエスカレーションが必要な場合でも、日本時間に即した対応が可能であり、国内業務時間内での迅速な問題解決が期待できること。

参考機種：WatchGuard ThreatSync+ NDR

（3） EPDR（エンドポイント保護監視対応）

下記仕様を満たす EPDR を導入し、発注者が指示す端末に対して、設定及び展開作業を実施すること。

6820 デバイス分のライセンスを調達し令和 8 年 3 月 1 日から 5 年間利用が可能なこと。

機能要件	
1	すべての実行ファイルを検査し、信頼できるプロセスだけ実行させることができること。
2	フォレンジック分析機能や修復ツールを有し、既知及び未知の脅威を発見し、事前対応的に不明な脅威を排除

	すること。
3	エージェントがインストールできる OS は、Windows、macOS、Linux、Android であること。
4	Windows では、以下の OS にエージェントがインストールできること。 ・Workstations：Windows XP SP3、Windows Vista、Windows 7、Windows 8、Windows 10、Windows 11 ・Servers：Windows 2003 SP2、Windows 2008, Windows Server Core 2008、Windows Small Business Server 2011、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019、Windows Server 2022
5	macOS では、以下の OS にエージェントがインストールできること。 ・macOS 10.10 Yosemite 以降
6	Linux では、以下の OS にエージェントがインストールできること。 ・64 ビット OS：Ubuntu 14.04 LTS 以降、Fedora 23 以降、Debian 8 以降、Red Hat 6.0 以降、CentOS 6.0 以降、Linux Mint 18 以降、SuSE Linux Enterprise 11.2 以降、Oracle Linux 6 以降 ・32 ビット OS：Red Hat 6.0 から 6.10、CentOS 6.0 から 6.10.
7	Android では、以下の OS にエージェントがインストールできること。 ・Lollipop 5.0/5.1、Marshmallow 6.0、Nougat 7.0 - 7.1、Oreo 8.0、Pie 9.0、Android 10 以降
8	ホストマシンに 3rd パーティのセキュリティー製品があるときは、インストーラーが 3rd パーティ製品をアンインストールし、そのあとエージェントのインストールが可能なこと。
9	EPP、EDR 及びオプション機能のすべてが単一のエージェントで実装されること。
10	インストーラーは MSI 形式で提供され、サイレントインストールや GPO を使用したインストール方法が実行できること。
11	クラウドベースの管理コンソールでシステム全体の一元管理ができること。
12	エージェントは永続的及び非永続的 VDI 環境にも展開ができること。
13	サーバやワークステーション、または OS バージョンやプラットフォームによりエージェントライセンスの区別はないこと。
14	管理コンソールは日本語にローカライズされていること。
15	EDR として下記の機能を有すること。 (可視化) プロセスの実行データで証跡を追うことができること。 (検知) 実行プロセスを常時監視し、ゼロデイ攻撃、標的型攻撃など、従来のアンチウイルスソリューションを回避するように設計された高度な脅威を検出できること。 (対応) フォレンジック情報および修復ツールによる分析を行い対処できること。 (予防) マルウェア、エクスプロイト、ゼロデイとして分類されていない未知のアプリケーションからの被害を防ぐことができること。
16	悪意のあるアプリケーションとして分類されたアプリケーションは、アプリケーションによってダウンロードされたファイルやインストールされたソフトウェア、作成されたドライバーをはじめ、LAN や公衆ネットワークとの通信の確立、ロードされた DLL、サービスの作成、レジストリキーの生成または削除、ファイルやフォルダーへのアクセスなどのデータを収集すること。
17	すべてのプロセスを、信頼できるプログラム及び悪意のあるプログラム、または潜在的に望ましくないプログラム（PUP）に自動的に分類すること。
18	管理コンソールは、どのブラウザからも、またタブレットやスマートフォンなどのデバイスからもアクセスでき、MFA 機能

	を有すること。
19	悪意ある振る舞いやプログラムの判定には、データレイク、集合知、解析アルゴリズムによる分類スコアを高い精度で算出して決定すること。
20	インシデントや悪意あるオブジェクト、異常値発生などに関わらず、下記のテレメトリデータを収集していること。 (プロセス) 生成されたプロセス、プロセスの実行、プロセスのインジェクション、子プロセスのインジェクション等 (ファイル) イベントやプロセスによるファイルの生成、ファイルの編集、ファイルの削除、ファイルへのアクセス等 (通信) 通信情報、IP、ソケット、プロトコル、方向、通信起点等 (レジストリ) レジストリキーの作成、編集、削除等 (監査) 管理者権限の使用、アクセスイベント、プロセスのインストール、サービス活動等
21	脅威ハンティングと調査サービスが機能として製品に組み込まれていること。
22	脅威ハンティングで検出された攻撃の指標（IOA：Indicatior of Attack）は、管理コンソールで MITRE の ATT&CK マトリックスにマッピングされ表示されること。
23	脅威検出において、取得されたイベントデータから仮説策定を行い、新しい検出アルゴリズムを生成すること。
24	パッチに含まれる CVE ID などにより、その重要度が示され、即時適用するかスケジューリングにより適用するかを選択できること。
25	適用後端末の再起動をするかどうかを設定でき、ロールバック機能を有していること。
26	HTTP、HTTPS、POP3 などの検査を行い電子メールと Web アプリケーションを保護できること。
27	ファイアウォールと IDS（不正侵入検知システム）機能でネットワークトラフィックの保護ができること。
28	USB や CD/DVD や SD カード、Bluetooth など、端末に接続できるデバイスの使用ブロック機能や、読み出し専用機能を有すること。
29	アンチスパム、アンチウィルス、アンチマルウェアの保護により、Microsoft Exchange に対してハッキングツール、疑わしいアプリケーション、潜在的に望ましくないプログラム（PUP）の検出ができること。
30	カテゴリや、アクセスを許可または拒否する URL/ドメインのリスト（ホワイトリスト/ブラックリスト）を設定することで、Web へのアクセスを制御・制限する機能を有するとともに、制御ポリシー適用の時間帯指定も可能なこと。
31	まだ分類されていないプロセスに対するアクションとして以下の設定モードを実装していること。 (Audit) 脅威検出時、ブロックはしないが記録と報告は行うこと。 (Hardening) インターネットなど外部から来たプロセスはブロックすること。 (Lock) 分類されていないプロセスはすべてブロックすること。
32	管理コンソールは、攻撃や侵害を受けているかどうかや、感染の範囲、ネットワークへの影響など、必要な情報を表示することができること。
33	インシデントについて、マルウェアが行ったイベントやマルウェアがネットワークに侵入した経路を含むフォレンジック分析することができること。
34	管理コンソールから任意にホストを隔離する機能を有すること。
35	隔離機能でネットワークから切り離されたホストは、管理コンソールから隔離解除することができること。
36	隔離されたホストに対して、例外的にソケット使用できるアプリケーションやプロセスを設定することができること。
37	管理コンソールから任意にホストマシンを再起動することができること。
38	管理コンソールから任意にエージェントの再インストールができること。
39	管理コンソールから任意にエージェントの削除（アンインストール）ができること。
40	自動スキャンとオンデマンドスキャンによるマルウェア駆除が行えること。

41	スキャニングの例外設定ができること。
42	エージェントのバージョンアップのスケジュール定義ができること。
43	エージェントのアンインストールパスワードを設定することができること。
44	システムトレイにアイコンを表示するかどうかを設定することができること。
45	ユーザーやマルウェアによるエージェントの改ざん不可機能を有すること。
46	ローカルクライアントのインターフェースは、日本語にローカライズされていること。
47	エアギャップ環境のホストに対して、特定のエージェントにプロキシの役割を持たせることができること。
48	特定のエージェントに検出の役割を持たせ、エージェントがまだ導入されていないネットワーク上のコンピュータを検出し、これに対してエージェントのインストールを行うことができること。
49	マルウェアなどが検出されたときやエラー発生時などのイベントが発生した際にメールにてアラート通知することができること。

参考機種：WatchGuard EPDR

（４） MAM（モバイルデバイスアプリケーション制御）

下記仕様を満たす機器を導入し、発注者が指示する構成に向けて、設定及び接続作業を実施し、令和８年３月１日までに利用を開始し 5 年間利用が可能なこと。

機能要件	
1	業務データはすべて専用アプリ内で完結し、端末ローカルには保存されないこと。
2	専用アプリを閉じるだけで業務データが消去されるセキュアな仕組みであること。
3	紛失時でもリモートワイプ不要で情報漏洩リスクを回避できること。
4	専用アプリは外部と隔離された「サンドボックス」環境で動作すること。
5	マルウェア感染時でも専用アプリ内への侵入を防げること。
6	ID/パスワード認証＋端末認証（UUID など）による二要素認証が可能なこと。
7	生体認証（指紋・顔）や Pincode にも対応し、利便性と安全性を両立できること。
8	OAuth や SAML2.0 など多様な外部認証サービスと連携可能なこと。
9	UUID による端末識別で証明書不要の端末認証が実現できること。
10	VPN 不要で、SSL/TLS による暗号化通信が可能なこと。
11	通信経路上の盗聴・改ざんを防止できること。
12	中継アプライアンスを設置しアウトバウンド通信のみで、社内システムにも安全に接続可能なこと。
13	端末にデータが残らない仕組みとし、デバイス紛失時のリモートワイプも必要ないこと。
14	通信はクラウドセンター経由で行われ、特定の IP アドレスからアクセスが可能なこと。
15	コピー＆ペースト、画面キャプチャ、ダウンロードなどの操作を制限可能なこと。
16	端末紛失時には管理画面から即時アクセス停止が可能なこと。
17	専用アプリ上で安全に Teams が利用できること。
18	専用アプリは iOS・iPadOS・Android・Windows にインストールが可能なこと。
19	1500 ユーザが利用可能なライセンスを調達すること。
20	平日対応の保守が 5 年間含まれていること。

参考機種：moconavi

（５） ZTNA（ゼロトラスト･ネットワーク･アクセス）

下記仕様を満たすサービスを導入し、発注者が指示する構成に向けて、設定及び接続作業を実施し、令和 9 年 9 月 30 日まで利用が可能なこと。

機能要件	
1	端末の代理で Web サイトへアクセスし、コンテンツの取得、実行、表示を安全な環境で行った後、無害化された表示情報のみを端末に送付すること。
2	端末の代理で Web サイトへアクセスし、コンテンツの取得、実行、表示をおこなう環境ではコンテナ技術を利用し、端末上のブラウザを閉じるたびに、利用されたコンテナとコンテナ内のコンテンツが破棄されること。
3	イントラネット内で利用しているシステムに対して下記要件を満たしアクセスが可能なこと。 ・シングルサインオン環境で利用してるシステムに対して、安全にアクセスが可能なこと。 (シングルサインオンでは Cookie 認証及びリーバースプロキシ認証を利用している) ・接続元のユーザーエージェントの情報をそのまま透過させることが可能なこと。
4	ユーザー、グループ、IP、地理情報に基づいた最小権限アクセス制御が可能なこと。
5	クロスサイトスクリプティング、セッションハイジャック、HTML スマグリングなどの Web 脅威から保護できること。
6	ユーザーのブラウジングセッションをリアルタイムで可視化し、必要に応じて記録・分析できること。
7	インターネット上および閉域ネットワークのブラウザベースの Web アプリケーションが利用できること。
8	Microsoft Windows のブラウザ Edge および Chrome から利用ができること。
9	モバイル端末の Safari(iOS および iPadOS), Google Chrome(Android)から利用できること。
10	アプリケーション利用環境に専用ソフトウェアをインストールすることなくブラウザのみで完結できること。
11	利用者毎に利用可能なアプリケーションを制御できること。
12	利用者のアプリケーションのアクセスのログを記録できること。
13	接続元 IP アドレスによりアプリケーションへのアクセスの可否を制御できること。
14	Web アプリケーションの表示されたページにウォーターマークを挿入できること。
15	Web アプリケーションへの書き込みを禁止できること。
16	Web アプリケーションからのファイルのダウンロードを禁止できること。
17	Web アプリケーションへのファイルのアップロードを禁止できること。
18	Web アプリケーションのファイル（Word,PowerPoint,PDF,Excel)をダウンロードすることなく内容を閲覧できること。
19	Web アプリケーションのファイル（Word,PowerPoint,PDF,Excel)を閲覧する際、表示にウォーターマークを表示できること。
20	Web アプリケーションのテキスト情報のコピー操作を禁止できること。
21	Web アプリケーションのフォームへのテキストのペースト操作を禁止できること。
22	サービスの利用にあたり外部の認証サービスと SAML 連携ができること。
23	平日対応の保守が、利用期間中含まれていること。
24	要件を満たすサービスは、ISMAP に登録されているサービスであること。

25	1500 ユーザー以上が利用可能なライセンスを調達すること。

参考機種：Menlo Secure Application Access

（6） インターネットファイアウォール

現在インターネットファイアウォールはシングル構成で稼働している。下記仕様を満たす機器を導入し、発注者が指示する設定及び接続作業を実施し HA 構成に変更すること。

ハードウェア要件	
1	アプライアンス製品を導入すること。
2	19 インチラックに搭載固定が可能であり、単一筐体当たり高さが 1U 以下であること。
3	冗長電源ユニットを搭載すること。
4	NXP LX2160A を搭載していること。
5	メモリサイズが 16GB 以上であること。
6	GbE RJ45 インターフェースを 8 ポート以上搭載していること。
7	10GbE SFP+インターフェースを 2 ポート以上搭載していること。
8	先出しセンドバック保守(5 年間)を調達すること。

機能要件	
1	IPv4 ファイアウォールスループット（1518 バイト UDP パケット）が 29.7 Gbps 以上であること。
2	ファイアウォールポリシー定義が 10,000 以上定義可能であること。
3	ファイアウォール同時セッション(TCP)が 15,000,000 以上であること。
4	ファイアウォール新規セッション(TCP)が秒間、146,000 以上であること。
5	ポリシーベースルーティング機能を有すること。
6	トラフィックシェーピング機能を有しており各ポリシー（ルール)単位で最低／最大値の帯域を設定できること。
7	Optional（DMZ）を含めた 3 つのセキュリティゾーン（Trusted, External, Optional）を構成できるこ。と
8	多数の定義済みレポートを生成できるサーバアプリケーションまたはクラウド環境を提供していること。
9	アプライアンスを通過するトラフィックを「ツリーマップ」ビューで表示（可視化）できること。
10	デバイスのコンフィグ作成や変更など WebUI、CLI、そして専用の管理ツールを使ってコンフィグ管理が出来ること。

参考機種：WatchGuard Firebox M690

（7） エンドポイント管理システムライセンス

・発注者が指定するライセンスを調達しサーバに適用すること。

・サイバーハイジーン用プログラムを発注者が指示する PC にインストールすること。

・ライセンス数：1000 本（2026 年 3 月 1 日から 2029 年 1 月 31 日まで）

※同等品不可

品番：Tanium TAN-CORE-S、TAN-CSM-S