

分冊 03 SSE・ゼロトラスト仕様書

第 1 章 業務概要

(1) 目的

本業務は、那覇市立小中学校等において利用する校務用 Windows 端末に SSE (Security Service Edge) を導入し、校内、校外、自宅その他の利用場所にかかわらず、安全かつ継続的にクラウドサービス及びインターネットを利用できる環境を整備することを目的とする。

従来のネットワーク境界を中心としたセキュリティ対策に加え、利用者、管理対象端末、端末状態、接続先その他の情報に基づきアクセスを制御するゼロトラストの考え方を取り入れ、ロケーションフリーな校務環境を実現すること。

本調達では、既存の端末管理、エンドポイントセキュリティ及び Web フィルタリング等の対策を踏まえ、SSE により、利用者、管理対象端末、端末状態、接続先等の情報に基づき、校内外を問わずクラウドサービス及びインターネットへのアクセスを一貫して制御・可視化し、ロケーションフリーな校務環境に必要なセキュリティを確保することを目的とする。

なお、本市では現時点で、校外から接続させる必要のあるオンプレミスその他の非公開アプリケーションを想定していない。このため、本調達では、対象 Windows 端末から SSE クラウドまでの安全な通信経路の確立、利用者認証、管理対象端末・端末状態の確認、SaaS 利用制御及びインターネット向け通信制御を主要な実装対象とする。

(2) 適用対象及び規模

- ・ SSE 拠点接続対象：55 施設（市立小中学校 54 校及び那覇市役所本庁舎）。
- ・ 端末単位接続対象施設：大規模給食センター3 施設及び教育相談課。
- ・ 端末単位接続対象施設については、SSE 適用対象となる Windows 端末を有するが、拠点側ネットワーク機器から SSE PoP へ通信を転送する対象拠点には含めず、SSE クライアント等による端末単位の接続を基本とする。
- ・ SSE 適用対象：Windows 端末 3,000 台
- ・ SSE 適用対象外：Chromebook 約 30,000 台
- ・ Chromebook は、本調達における SSE の適用対象外とする。
- ・ 利用場所：学校内、庁内、校外、自宅、公衆無線 LAN、モバイル回線その他発注者が認める場所
- ・ 運用保守期間は 00 共通調達仕様書による。

価格算定に使用するユーザー数、共有端末数その他必要な数量は、発注者が別途提示する。

第 2 章 業務内容及び調達範囲

(1) 実施業務

受託者は、SSE 導入に関し、少なくとも次の業務を実施すること。

- ・ 現行ネットワーク、対象端末、通信、セキュリティ設定及び運用の調査
- ・ SSE の基本設計及び詳細設計
- ・ SSE サービス及び必要なライセンスの提供
- ・ Windows 端末に必要なクライアント、証明書その他設定の設計
- ・ Web アクセス制御、クラウド利用制御、情報漏えい対策及び脅威対策等のポリシー設計
- ・ SSL/TLS 通信検査に必要な設計及び設定
- ・ DNS セキュリティに必要な設計及び設定

- ・利用者認証、端末状態及び既存サービスとの連携
- ・ネットワーク基盤との接続及び通信経路の設計
- ・導入・移行・試験・教育・運用保守及び契約終了支援は、05 導入・移行・試験・運用保守仕様書に従う。SSE 固有の試験項目は本書第 6 章による。

認証・端末状態及び既存サービス連携の主管要件は、04「認証・端末状態・既存サービス連携仕様書」による。校務 SSID の接続認証は 01「ネットワーク部分仕様書」、Windows 端末への展開並びに試験・運用手順は 05「導入・移行・試験・運用保守仕様書」による。

導入、移行、試験、ログ保存、障害対応及び運用保守の共通要件は、「05 導入・移行・試験・運用保守仕様書」に従うこと。

(2) 既存サービスの扱い

次の既存サービスは、本調達開始時点では継続利用することを基本とする。

ただし、i-FILTER@Cloud については、04 に基づき機能統合、構成変更を提案できるものとする。

- ・EVECLOUD
- ・Google Workspace
- ・Sophos Intercept X
- ・SKYSEA Client View
- ・i-FILTER@Cloud

既存サービスとの具体的な連携方式、機能分担、設定変更、責任分界及び障害切り分けは、04「認証・端末状態・既存サービス連携仕様書」による。SSE 自体の機能要件は本書に従うこと。

(3) 基本条件・必須要件・提案事項の区分

- ・基本条件は、対象端末、既存環境、利用場所、既存サービス、ネットワーク構成及び履行条件等、参加者が共通に用いる前提とする。
- ・必須要件は、本業務によって実現しなければならない機能及び成果とする。具体的な製品、方式又は構成は、特段の指定がある場合を除き固定しない。
- ・提案事項は、必須要件を実現する方式、機能分担、効果、制約、運用及び性能について、提案者に回答を求める事項とする。
- ・提案事項であることを理由として、採用に必要な機能、構成、ライセンス又は主要な制約の回答を契約締結後まで留保しないこと。
- ・標準機能、追加ライセンス、オプション、個別開発及び手動運用を区分して示すこと。
- ・必須要件の実現に必要な機能、ライセンス、設定、構築及び契約期間中の運用保守に係る費用は、特段の定めがある場合を除き、SSE 一式の基本提案価格に含めること。基本提案価格に含まれない任意のオプションを提案する場合は、その内容及び追加費用を明示すること。

(4) 導入の優先順位及び段階導入

- ・本市では、既存 UTM を令和 9 年 3 月（2027 年 3 月）をもって撤廃する予定であることから、本業務においては、UTM が担っているインターネット接続時のセキュリティ機能を SSE へ適切に移行し、UTM 撤廃後も必要なセキュリティを継続して確保することを最優先とする。
- ・このため、SSE の基本接続、インターネット向け通信の可視化及び制御、FWaaS 又は同等機能、脅威対策、DNS セキュリティその他 UTM 撤廃に必要となる機能について、優先して設計、構築、検証及び移行を行うこと。

- ・CASB、DLP、SSL/TLS 通信検査、詳細なアクセス制御その他のセキュリティポリシーについては、前記の基本構築及び移行状況を確認しながら並行して設計及び検証を進め、令和8年度を通じて段階的に導入及びチューニングを行うこと。
- ・ロケーションフリー環境については、校内における SSE 接続及び各種セキュリティポリシーの安定稼働を確認した後、SSE クライアントを利用した校外接続の検証及びチューニングを行い、発注者による段階的な展開を支援すること。

第3章 SSE 導入に係る基本条件及び必須要件

(1) 基本条件

- ・対象端末及び施設区分は第1章(2)による。
- ・SSE 適用対象 Windows 端末からインターネット向けに発生する通信について、Web 通信に限定せず、原則として全ポートの TCP/UDP 通信を可視化及び制御の対象とすること。TCP/UDP 以外の IP プロトコル層の通信は可視化の対象とし、制御の可否及び方法は、採用構成及び実利用状況を踏まえ、設計フェーズで確定すること。
- ・前項は全通信の内容を常時復号して検査することを求めるものではない。暗号化通信の復号・内容検査は、本仕様書に定める SSL/TLS 通信検査その他の要件に従い、必要性、技術的制約及び業務影響を踏まえて適用すること。
- ・校内及び校外を問わず、必要なセキュリティポリシーを適用できること。
- ・既存ネットワークとの整合及び共通連携条件は 00「共通調達仕様書」第3章、LAN 側の具体的な変更条件は 01「ネットワーク部分仕様書」、Chromebook への非影響及び移行・試験条件は 05「導入・移行・試験・運用保守仕様書」による。
- ・SSE クラウド、接続拠点 (PoP)、通信経路及び障害時の構成を明確にすること。
- ・対象 Windows 端末又は拠点側ネットワーク機器から SSE クラウドまでの通信転送方式について、校内・校外及びその他対象施設ごとの適用方式を区別して設計・説明すること。

(2) 必須要件

ア SSE への接続方式及び通信経路

- ・対象 Windows 端末は、校内、校外、自宅、公衆無線 LAN、モバイル回線その他の利用場所にかかわらず、SSE サービスへ安全に接続できること。
- ・第1章(2)の SSE 拠点接続対象 55 施設では、原則として、拠点側ネットワーク機器から SSE PoP へ通信を転送する方式を優先すること。ただし、必要なセキュリティ要件等を満たし、性能、端末負荷、可用性及び運用管理等を踏まえて合理的と認められる場合は、端末エージェント方式その他の方式を選択できるものとする。IPsec VPN その他の採用方式、通信経路、冗長性及び必要なネットワーク設定を明示すること。
- ・対象拠点から SSE への拠点接続については、SSE サービス又は PoP の障害、メンテナンス等により単一の接続経路が利用できない場合においても通信を継続できるよう、原則として異なる終端先への 2 本以上の IPsec VPN トンネルその他これと同等以上の冗長構成とすること。採用する冗長方式、切替方式、切替条件及び切替時の通信影響を明示すること。
- ・拠点接続に用いる SSE サービスについては、将来のインターネット回線及びネットワーク機器の高速化を考慮し、サービス側の仕様又はライセンス上、拠点当たり最大 10Gbps まで通信帯域を拡張可能な構成であること。1 トンネル当たりの帯域上限を有する場合は、複数トンネルその他の方式により拠点当たりの帯域を拡張できること。なお、本要件は、現行の拠点側ネットワーク機器において 10Gbps の実効スループットを確保することを求めるものではない。

- ・校内利用時に端末ごとの SSE クライアント等による通信転送方式を採用する場合は、接続確立又は再接続に起因する待ち時間、通信断、端末負荷その他の利用者影響を可能な限り低減すること。
- ・校外、自宅、公衆無線 LAN、モバイル回線その他の場所で利用する場合は、SSE クライアント又は同等機能により端末から SSE PoP まで安全な通信経路を自動的に確立し、校内利用時と同等の必要なセキュリティポリシーを継続して適用できること。
- ・採用する接続方式に応じ、利用場所の変更時に利用者が接続方式を意識して手動変更することなく、必要な SSE 接続が継続又は適切に切り替わること。
- ・第 1 章 (2) の端末単位接続対象施設は、SSE クライアント等による端末単位の接続を基本とすること。
- ・SSE への接続方式について、端末クライアント、プロキシ、PAC、DNS 転送、拠点トンネルその他の方式を採用する場合は、それぞれの適用対象、利用場所、通信経路及び制御範囲を明示すること。
- ・OS 起動、利用者ログイン、ネットワーク切替、スリープ復帰その他の通常利用において、必要な SSE 接続が自動的に確立又は復旧できること。
- ・一般利用者が、発注者の承認なく SSE クライアント、プロキシ設定その他の SSE 接続機能を停止、無効化、変更又は回避できないこと。
- ・ローカル LAN 通信、プリンタ、内部 DNS その他の通信については、採用する接続方式及びセキュリティ設計に応じ、SSE 経由から除外又は経路分離する方式のほか、SSE クラウド側で一元的に制御する方式を含め、適切な通信経路を設計できること。SSE 経由とする場合又は経路分離を行わない場合は、その通信経路、制御範囲、性能、障害時の影響及び必要な対策を示すこと。
- ・SSE 接続に必要なネットワーク条件 (FQDN、IP アドレス、ポート、DNS、プロキシ、NAT、証明書、MTU 等) を提示すること。
- ・SSE 接続に伴い既存ネットワーク設定に変更が必要となる場合は、変更内容、理由及び影響範囲を示し、必要に応じて切戻し可能な構成とすること。01「ネットワーク部分仕様書」及び 05「導入・移行・試験・運用保守仕様書」と整合させること。
- ・SSE への接続方式は、特定メーカー固有の方式に限定せず、本市のロケーションフリー環境、対象端末数、既存ネットワーク、運用負荷、性能及び可用性を踏まえた方式とすること。

イ FWaaS (Firewall as a Service) 及びインターネット向け通信の可視化・制御

- ・FWaaS (Firewall as a Service) 又は同等機能により、SSE 適用対象 Windows 端末からインターネット向けに発生する通信について、HTTP/HTTPS 通信に限定せず、原則として全ポートの TCP/UDP 通信を可視化及び制御の対象とすること。TCP/UDP 以外の IP プロトコル層の通信は可視化の対象とし、制御の要否及び方法は、採用構成及び実利用状況を踏まえ、設計フェーズで確定すること。
- ・通信について、送信元、通信先、宛先ポート、プロトコル、利用者、端末、アプリケーションその他取得可能な情報を確認でき、ポリシーに基づき通信の許可又は遮断を設定できること。
- ・通信ログについては、採用する接続方式に応じて取得可能な利用者、端末、送信元 IP、日時、通信先、宛先ポート、プロトコル及び判定結果等を確認できること。
- ・Web プロキシで処理されない通信についても、FWaaS 又は同等機能により制御可能な範囲を明示すること。
- ・製品仕様上、可視化又は制御の対象外となるポート、プロトコル、通信方式又はアプリケーションがある場合は、提案時に対象外範囲、理由、リスク及び代替対策を明示すること。
- ・ローカル LAN、プリンタ、内部 DNS、認証、OS 又は端末管理上必要な通信その他 SSE による制御から除外する通信については、対象、宛先、ポート、プロトコル及び用途を明示し、必要最小限の範囲で設定すること。

ウ セキュア Web ゲートウェイ (SWG)

- Web アクセスについて、URL、ドメイン、カテゴリ、危険度その他必要な条件に基づく制御ができること。
- 利用者認証を伴う接続方式では、認証により識別した利用者情報その他、提案 SSE で利用可能な情報をアクセス制御ポリシーの条件として利用できること。
- 許可、拒否、警告その他必要な制御を設定できること。
- 発注者が必要とするサイト又はサービスについて、例外設定を行えること。
- 例外設定について、理由、対象、期間及び変更履歴を管理できること。
- URL カテゴリ及び脅威情報が、サービス提供者又はセキュリティベンダーにより継続的かつ自動的に更新されること。
- 誤分類又は業務上必要なサイトが遮断された場合の確認及び解除手順を有すること。
- i-FILTER@Cloud との具体的な機能分担、通信順序及び移行の考え方は 04 による。

エ クラウドサービス利用の可視化及び制御 (CASB)

- 対象 Windows 端末から利用されるクラウドサービスを可視化できること。
- クラウドサービスについて、サービス名、利用者、利用状況、通信量、リスク等を確認できること。
- 発注者が許可していない又は未評価のクラウドサービスを識別できること。
- 発注者が指定するクラウドサービスについて、利用の許可、警告又は制限を行えること。
- 対応可能なクラウドサービスについて、アップロード、ダウンロード、投稿その他のアクション単位で利用を制御できること。
- 対応可能なサービスについて、組織が管理するテナントと個人又は外部テナントを識別した制御が可能であること。
- GWS の CAA との具体的な制御分担は 04 による。
- クラウドサービス上に既に保存されているデータを API 連携により一括検査する機能は、本調達の必須要件とはしない。対応可能な場合は、対象サービス、検査可能な範囲及び追加ライセンスの要否を提案すること。

オ 情報漏えい対策 (DLP)

- Web サービス及びクラウドサービスへの情報送信又はファイルアップロード等について、発注者が指定する情報を検知できること。
- 検知時に、監査、警告、遮断その他の制御を選択できること。
- キーワード、パターン、個人情報その他一般的な情報識別方法を利用できること。
- 日本語を含む業務文書について利用可能な検査方式及び対応ファイル形式を示すこと。
- 誤検知による業務影響を考慮し、段階的なポリシー適用及び例外設定ができること。
- 生成 AI サービスに対する入力及び出力の可視化又は制御に対応可能な場合は、対象サービス、制御範囲、方式及び追加ライセンスの要否を提案すること。

カ 脅威対策

- マルウェア、フィッシング、サポート詐欺、悪性サイト及び不審なダウンロード等を検知又は遮断できること。
- URL・ドメインの評判情報、ファイル検査その他の仕組みにより、既知及び未知の脅威への対策を提供すること。
- インターネット向け通信について、既知の攻撃パターン、不正アクセスその他のネットワーク脅威を検知し、必要に応じて遮断できること。
- 脅威情報及び検査機能を継続的に更新すること。

- ・危険なファイル又は通信を検知した場合は、採用する接続方式に応じて取得可能な利用者、端末、送信元 IP、通信先及び判定結果等を確認できること。利用者又は端末を直接識別できない通信については、その条件及び追跡方法を示すこと。
- ・Sophos Intercept X との具体的な機能分担、連携及び障害切り分けは 04 による。

キ SSL/TLS 通信への対応

- ・暗号化された Web 通信について、必要に応じて復号し、SWG、CASB、DLP 及び脅威対策を適用できること。
- ・SSL/TLS 通信を検査する場合に必要な証明書及び端末設定を管理できること。
- ・業務上又は技術上復号に適さない通信を、対象外として設定できること。
- ・SSL/TLS 通信検査を適用できない又は制御に制約が生じる通信について、その条件及び対応方法を示すこと。
- ・SSL/TLS 検査対象外通信についても、残存するセキュリティ対策を明示すること。
- ・既存サービスとの SSL/TLS 検査・復号の具体的な役割分担は 04 による。

ク DNS セキュリティ

- ・マルウェア、フィッシング、C2 その他の悪性ドメインへのアクセスを検知又は制御できること。
- ・校内、校外及び SSE 障害時の DNS 通信経路を明示すること。
- ・内部 DNS 及び既存の名前解決に影響を与えないこと。
- ・DoH、DoT その他暗号化 DNS の扱い及び制御可能範囲を示すこと。
- ・SSE 向けの DNS 設定が SSE 適用対象外ネットワークへ影響しない構成とすること。

ケ 利用者・端末等のコンテキストに基づく制御

- ・SSE は、IdP による利用者認証結果に加え、提案 SSE が取得可能な管理対象端末、端末状態その他のコンテキスト情報を、アクセス制御条件として利用できること。
- ・本市が管理する Windows 端末であること及び端末のセキュリティ状態を、アクセス判断の条件として利用できること。
- ・端末状態の情報源、取得方法、判定方法及び既存サービスとの具体的な連携要件は 04 による。
- ・端末状態を取得できない場合又は非準拠と判定した場合の動作を設定できること。

コ ZTNA

※本仕様書における ZTNA は、特定製品における機能名称に限定せず、IdP による利用者認証、管理対象端末、端末状態、接続先等の情報に基づき、SaaS を含むアプリケーションへのアクセスを制御する仕組みを含むものとして扱う。

- ・提案する SSE サービスは、ZTNA 又は同等の機能を利用可能であること。
- ・ZTNA 又は同等機能を利用する場合は、IdP による利用者認証結果に加え、提案 SSE が取得可能な管理対象端末、端末状態その他のコンテキスト情報を SSE のアクセス制御条件として利用できること。
- ・将来、非公開アプリケーションへの安全なアクセス制御が必要となった場合に、既存の SSE 環境を大規模に再構築することなく、ZTNA 又は同等機能へ拡張できること。なお、現時点で非公開アプリケーションへの実接続は想定しておらず、非公開アプリケーション接続用コネクタ等の設置、設定及び実接続は、本調達の対象外とする。

サ SSE 障害時及び業務継続

- ・SSE クラウド、接続 PoP、クライアント、DNS、認証、証明書又はネットワークの障害時における通信動作を明示すること。
- ・SSE によるセキュリティ制御が実施できない場合は、セキュリティを優先した通信制御を基本とすること。

- ・ただし、業務継続上重大な影響が生じる場合に備え、発注者の承認により、対象、期間及び通信範囲を限定した緊急バイパスその他の代替手段を利用できること。
- ・緊急措置については、実施者、承認者、開始・終了日時、対象、理由及び実施中の通信又は操作を記録し、復旧後に通常のセキュリティ制御へ戻ったことを確認すること。

シ 管理、可視化及びログ

- ・SSE のポリシー、利用状況、端末接続状況、脅威及び障害を一元的に確認できること。
- ・管理者の権限を、全体管理、ポリシー変更、ログ閲覧、ヘルプデスク、監査等に分離できること。
- ・管理者操作を記録できること。
- ・ログ取得、保存、検索、出力、外部連携、監視、通知及びインシデント対応の共通要件は、05「導入・移行・試験・運用保守仕様書」による。

ス 性能及びサービス提供

- ・対象 Windows 端末及び利用者数を収容できる十分なサービス能力を有すること。
- ・SSL/TLS 検査、DLP、CASB、脅威対策その他採用する機能を有効にした状態で、業務利用に支障のない性能を確保すること。
- ・SSE クライアントによる CPU、メモリ、起動時間及び通信への影響を過度に増加させないこと。
- ・本市からの利用に適した PoP を利用できること。
- ・サービス提供地域、データ処理地域及びログ保管地域を示すこと。
- ・サービス稼働率その他の SLA は、「05 導入・移行・試験・運用保守仕様書」に従うこと。

(3) 提案事項

- ・提案者は、本章に定める必須要件を満たすことを前提として、SSE の構成、接続方式、セキュリティ機能、既存環境との連携・機能分担、性能、可用性、運用管理、導入・移行その他本業務の実現方法について、提案者の知見、技術及びノウハウを活用した具体的な提案を行うこと。
- ・提案に当たっては、採用する方式及びその選定理由、効果、制約、前提条件、運用方法、達成目標並びに必要なライセンス及び費用を明示し、本文の要件を単に再掲するだけの内容としないこと。
- ・提案事項の取扱いは、00「共通調達仕様書」第 2 章 (1) による。本業務で実施する事項、任意のオプション並びに将来構想・参考情報を明確に区分して示すこと。
- ・各要件への適合可否は、別添「機能証明書」に記載すること。
- ・提案書の様式は指定しないが、仕様書及び機能証明書の各項目との対応関係が確認できるよう記載すること。
- ・基本提案価格に含まれない任意のオプションを提示する場合は、その内容、効果及び追加費用を明示すること。

第 4 章 現行調査及び詳細設計要件

(1) 現行調査

受託者は、少なくとも次の事項を確認・調査すること。

- ・対象 Windows 端末の台数（個人割当端末・共有端末の別）、OS、利用形態及び既存ソフトウェア
- ・校内及び校外における通信経路
- ・現行インターネット接続、DNS、プロキシ、PAC、NAT 及びファイアウォール
- ・認証、ユーザー情報、端末状態及び既存サービス連携に係る現行調査は、04 に従うこと。
- ・主要な Web サービス、業務システム、更新サービス及び外部通信
- ・対象 Windows 端末から発生する Web 以外の外部通信、使用ポート、プロトコル及び主要アプリケーション

- ・現行 URL フィルタリング、脅威対策及び情報持出し制御
- ・現行ログ及び問い合わせ対応
- ・SSE 導入により競合又は影響が生じる可能性のあるクライアント、証明書、VPN、プロキシその他設定
- ・現行資料と実態の差異、既知障害、既知制約及び運用課題

(2) 基本設計及び詳細設計

基本設計には、少なくとも次を含めること。

- ・SSE 全体構成
- ・校内及び校外の通信フロー

第 1 章 (2) の SSE 拠点接続対象 55 施設の拠点転送方式、並びに校外・端末単位接続対象施設の SSE クライアント等による接続方式。

- ・FWaaS 又は同等機能によるインターネット向け TCP/UDP 通信の原則全ポートに対する可視化・制御方針、TCP/UDP 以外の IP プロトコル層の通信の可視化方針及び制御の考え方、除外通信及び対象外通信への代替対策
- ・PoP 及び障害時通信
- ・SWG、CASB、DLP、脅威対策、SSL/TLS 検査及び DNS セキュリティの基本方針
- ・利用者・端末等を用いたアクセス制御方針
- ・ZTNA 又は同等機能の提供範囲及び SSE のアクセス制御への適用方針
- ・認証、端末状態及び既存サービスとの具体的な連携設計・機能分担は 04 による。
- ・LAN、WAN 及び認証基盤との接続
- ・ログ及び管理
- ・移行、切戻し及び緊急バイパス

詳細設計には、採用した方式に応じ、ポリシー、グループ、URL カテゴリ、例外、DLP 条件、SSL/TLS 除外、DNS 設定、クライアント設定、証明書、ポート・プロトコル・アプリケーション単位の通信許可・遮断、除外通信、管理権限、障害時動作その他本番運用に必要な設定を含めること。

第 5 章 ネットワーク基盤及び他分冊との接続要件

(1) LAN との接続

- ・SSE 導入に伴う通信経路、DNS、プロキシ、トンネル、NAT、MTU その他 LAN 側に影響する事項を整理すること。
- ・既存 VLAN 及び IP アドレスを原則として維持すること。
- ・SSE の導入だけを理由として、不要な LAN 構成変更を行わないこと。
- ・必要な変更がある場合は、01 の変更管理及び設計要件に従うこと。

(2) 認証及び既存サービス連携

- ・認証、ユーザー情報連携、管理対象端末・端末状態の取得、GWS・CAA、Sophos Intercept X、SKYSEA Client View、i-FILTER@Cloud 等との具体的な連携要件、設定変更、責任分界及び障害切り分けは 04 によること。本書では、SSE として必要な機能要件を定める。

第 6 章 導入・移行及び試験要件

導入・移行・試験の共通要件は 05 に従うものとし、SSE について少なくとも次を確認すること。

段階導入方針は第 2 章、具体的な移行計画及び判定手順は 05「導入・移行・試験・運用保守仕様書」第 6 章による。

- ・校内及び校外からの SSE 接続
- ・OS 起動、利用者ログイン、ネットワーク切替及びスリープ復帰時の SSE 接続確立・復旧
- ・SSE クライアントを利用する端末について、単に通信接続が可能であることのみでなく、OS 起動後、利用者ログイン後、ネットワーク切替時、スリープ復帰時その他通常利用時に、接続確立又は復旧に過度な待ち時間が生じないこと。
- ・Web 閲覧、Google Workspace その他主要な SaaS の利用において、SSE クライアントに起因する著しい通信遅延、画面停止、タイムアウトその他の利用者影響が生じないこと。
- ・実利用環境での接続時間、通信遅延及び利用者影響を測定し、05 のパイロット判定及び本番展開前のチューニングへ反映すること。
- ・SWG 及び URL 制御
- ・FWaaS 又は同等機能による、Web 以外の通信を含む代表的な TCP/UDP ポート・プロトコルの可視化、許可及び遮断
- ・クラウド利用の可視化及び制御
- ・DLP 代表ポリシー
- ・マルウェア及び危険サイト対策
- ・SSL/TLS 検査及び除外
- ・DNS セキュリティ
- ・利用者及び端末状態を用いたアクセス制御
- ・ZTNA 又は同等機能の利用可否及び利用者・端末・端末状態等を用いたアクセス制御への適用確認。非公開アプリケーションへの実接続試験は対象外とする。
- ・SSE クライアントの配布、更新及び撤去
- ・SSE、PoP、認証、DNS その他障害時の動作
- ・緊急バイパス及び通常状態への復旧
- ・ログ及び管理者操作
- ・性能及び端末負荷
- ・認証、端末状態及び既存サービス連携に係る試験は 04 及び 05 に従うこと。

第 7 章 運用保守要件

運用保守は 05「導入・移行・試験・運用保守仕様書」による。SSE 固有の対応範囲は次のとおりとする。

- ・SSE サービス及びクライアントの障害切り分け
- ・ポリシー変更、例外管理及び継続的なチューニング
- ・セキュリティポリシーは、導入時及び契約期間中を通じ、業務・利用サービス・脅威・誤検知・通信影響に応じて発注者と協議し、必要な変更及びチューニングを随時実施すること。変更管理は 05「導入・移行・試験・運用保守仕様書」による。
- ・クライアント及び必要なソフトウェアの更新
- ・証明書の更新及び失効対応
- ・URL 誤分類その他のメーカー問い合わせ
- ・脅威、DLP その他セキュリティ事象への対応支援
- ・SSE 及び既存製品間の障害切り分け
- ・PoP その他サービス障害時のメーカー連携
- ・定期的な設定及び機能分担の見直し

第 8 章 成果物

共通の提出形式・版管理は 00「共通調達仕様書」による。次の SSE 固有情報を各主管成果物へ収録し、移行・試験・運用の共通成果物は 05「導入・移行・試験・運用保守仕様書」に集約すること。

- ・ 現行環境調査報告書
- ・ SSE 基本設計書及び詳細設計書
- ・ SSE 全体構成図
- ・ 校内・校外通信フロー図
- ・ SSE 接続及び PoP 構成図
- ・ SWG、FWaaS 又は同等機能、CASB、DLP、脅威対策、SSL/TLS 及び DNS ポリシー一覧
- ・ インターネット向け通信制御ポリシー一覧（ポート、プロトコル、アプリケーション、除外及び対象外通信を含む。）
- ・ 認証、端末状態及び既存サービス連携に係る成果物は 04 による。
- ・ SSE クライアント配布・更新・撤去手順
- ・ 証明書及び SSL/TLS 検査除外一覧
- ・ ZTNA 又は同等機能の提供範囲及びアクセス制御への適用方針
- ・ 障害時動作及び緊急バイパス手順
- ・ 管理権限一覧
- ・ ログ取得項目一覧、180 日保存方式、アーカイブ・復元手順、Syslog・API 等の外部連携方式及び重大イベントの通知設定一覧
- ・ ライセンス及び数量一覧
- ・ 管理者向けマニュアル

第 9 章 提案時の提示事項及び契約後の確定事項

次表は、発注者の事前提示、提案及び契約前の合意、契約後の詳細確定の各段階で整理する事項を示す。提案者は第 3 章（3）及び別添「機能証明書」に基づいて回答し、採用範囲、必要なライセンス、主要な性能・可用性条件、機能分担及び費用条件を契約前に整合する。

契約後は、契約した構成及び達成条件の範囲内で個別設定値、ポリシー、対象端末群、詳細な通信条件、作業手順及び試験手順等を詳細化し、提案時の機能、性能又は費用条件を引き下げないこと。

提案時に求める事項は、提案比較及び契約範囲の確定に必要な実現方式、対応範囲、主要条件、制約、ライセンス及び費用を基本とし、個別設定値、対象一覧、詳細な通信条件、作業手順、試験方法、測定条件及び詳細な合否基準は、契約締結後の現行調査及び詳細設計において確定する。

項目	発注者の事前提示	提案及び契約前の合意	契約後の詳細確定
(1) 対象端末、利用者及びライセンス	SSE 適用対象となる Windows 端末 3,000 台及び Chromebook が SSE 適用対象外であることを共通条件とする。提案比較に必要な利用者数、Windows 端末の利用形態（個人割当・共有）、OS その他必要な数量は、発注者が別途提示する。	提案者は、ユーザー単位、端末単位、同時接続単位その他のライセンス体系、基本提案価格に含む数量、数量増減条件及び検証・パイロット用ライセンスの扱いを示す。必須要件の実現に必要な追加ライセンスは基本提案価格に含めること。任意のオプションがある場	受託者は、契約した数量・ライセンス体系に基づき、対象端末群、利用者グループ、管理者、検証環境及びライセンス割当てを確定する。

項目	発注者の事前提示	提案及び契約前の合意	契約後の詳細確定
		合は、その内容及び追加費用を区分して示すこと。	
(2) SSE 接続方式及び通信経路	施設別接続区分、対象 Windows 端末の利用形態その他、提案に必要な現行環境情報については、発注者が提示可能な範囲を前提とする。詳細未確定の事項は、契約締結後の現行調査及び詳細設計において確認する。現行構成維持の条件は 00「共通調達仕様書」による。	提案者は、拠点接続及び端末単位接続について、採用する接続方式、その選定理由、通信経路、冗長化、帯域、端末負荷、利用者影響、障害時動作、運用方法及び主な制約を示すこと。必須要件の実現に必要な機器・ライセンスは基本提案価格に含め、任意のオプションとなる場合のみ追加費用を示すこと。	受託者は、採用した接続方式に基づき、端末群別の適用方法、具体的な FQDN、IP、ポート、DNS、プロキシ、NAT、証明書、MTU、トンネル構成、内部通信の経路、SSE 適用・除外、切替条件及び設定投入順序を詳細設計で確定し、01 及び 05 と整合させること。
(3) インターネット向け通信の可視化及び制御	発注者は、SSE 適用対象 Windows 端末について、HTTP/HTTPS 通信に限定せず、インターネット向けに発生する原則として全ポートの TCP/UDP 通信を可視化及び制御対象とする方針を示す。Chromebook 約 30,000 台は SSE 適用対象外とする。	提案者は、HTTP/HTTPS 以外を含む通信の転送・識別・制御方式、FWaaS 又は同等機能の有無、対応範囲、主な制約、対象外となる通信、性能影響及び追加ライセンスの可否を示すこと。原則として全ポートの TCP/UDP 通信を制御できない場合は、その範囲、理由、リスク及び代替対策を明示すること。TCP/UDP 以外の IP プロトコル層の通信については、可視化可能な範囲を示すこと。	受託者は、実際の業務通信を確認した上で、許可・遮断するポート、プロトコル及びアプリケーション、TCP/UDP 以外の IP プロトコル層の通信の制御可否及び方法、除外通信、ログ確認方法、例外変更手順及び障害時動作を詳細設計で確定すること。
(4) PoP、性能及び可用性	対象拠点、対象端末数及び校内・校外での利用条件は、本仕様書に定めるとおりとする。	提案者は、本市利用時に想定する PoP、PoP 選択方式、冗長構成、障害時の代替 PoP、サービス稼働率、想定性能及びその根拠を示すこと。SSL/TLS 検査、CASB、DLP 及び脅威対策を有効にした場合の性能上の主な制約又は影響がある場合は、併せて示すこと。	受託者は、採用したサービスに基づき、本市から利用する PoP、経路、監視方法、障害時切替、性能試験条件及び通知方法を確定する。契約した性能・可用性条件を設計だけで引き下げない。
(5) SWG 及び i-FILTER@Cloud との機能分担	i-FILTER@Cloud との具体的な機能分担、通信経路、移行方法、責任分界及び提案時の提示事項は 04 による。		
(6) CASB 及びクラウド利用制御	本市は、Google Workspace を中心にクラウドサービスを利用する。個人アカウント及び外部組織が発行するアカウントについては、発注者が指定するサービス又はアカウントの利用を許可しつ	提案者は、可視化可能なクラウドサービス、リスク評価、未許可クラウド検知、テナント制御及び操作単位制御の対応範囲、方式、主な制約並びに追加ライセン	受託者は、利用実態及び発注者方針に基づき、許可・監査・警告・遮断する対象サービス、テナント及び操作を詳細設計で確定する。

項目	発注者の事前提示	提案及び契約前の合意	契約後の詳細確定
	つ、ファイルアップロードその他の操作を制限できることを想定する。クラウドサービス上に既に保存されているデータを API 連携により一括検査する機能は、本調達 の必須要件とはしない。	スの可否を示すこと。外部アカウント又はテナントの利用を許可しつつ特定操作を制限する場合の対応可否を示すこと。	
(7) DLP	本市は、個人情報その他の情報持出し対策として、業務影響を考慮しながら DLP を段階的に適用する方針とする。	提案者は、キーワード、パターン、辞書等の検知方式、日本語及び対応ファイル形式、対象チャネル、制御可能な動作、誤検知時の運用、主な制約並びに追加機能・ライセンスの可否を示すこと。必須要件を満たすために必要な機能は基本提案価格に含めること。	受託者は、代表ルール、しきい値、対象チャネル、例外及び段階導入順序を発注者と確定し、パイロットでチューニングする。
(8) 脅威対策及び Sophos Intercept X との分担	Sophos Intercept X との具体的な機能分担、端末状態連携、責任分界及び提案時の提示事項は 04 による。		
(9) SKYSEA Client View 及び IaaS 環境との共存	SKYSEA Client View との具体的な共存・連携、IaaS リモートアクセスへの影響、配布・照合、責任分界及び提案時の提示事項は 04 による。		
(10) SSL/TLS 通信検査及び証明書	本市は、暗号化通信について必要なセキュリティ検査を実施することを基本とする。	提案者は、SSL/TLS 検査方式、対応範囲、主な制約、性能影響、二重復号の回避及び既存製品との役割分担の考え方を示すこと。証明書配布等に追加機能又はライセンスが必要な場合は、その可否を示すこと。	受託者は、発注者が提示する主要 SaaS、業務システム及び既存通信について SSL/TLS 通信検査による影響を確認し、発注者と協議の上、検査対象・除外対象、証明書発行・配布・更新方法、具体的な除外 FQDN・アプリケーション及び例外申請手順を確定し、主要業務サービスで互換性試験を実施する。
(11) DNS セキュリティ	SSE 適用対象ネットワークと SSE 適用対象外ネットワークを分離して運用することを前提とする。	提案者は、DNS セキュリティの適用方式、校内・校外の DNS 通信経路、悪性ドメイン制御、DoH・DoT への対応、内部 DNS との共存方法及び主な制約を示すこと。	受託者は、対象 Windows 端末の DNS 経路、内部名前解決、除外、DoH・DoT 設定、障害時動作及び具体的なネットワーク設定を確定する。

項目	発注者の事前提示	提案及び契約前の合意	契約後の詳細確定
(12) 利用者・端末状態等を用いたアクセス制御	利用者認証、ユーザー情報連携、管理対象端末・端末状態の具体的な連携及び提案時の提示事項は 04 による。ZTNA 又は同等機能そのものの要件は本書第 3 章 (2) コによる。		
(13) 障害時動作及び緊急バイパス	SSE によるセキュリティ制御が利用できない場合は、セキュリティを優先することを基本とする。ただし、重大かつ長時間の障害時には、発注者承認による限定的な業務継続手段を確保できること。	提案者は、SSE クラウド、PoP、クライアント、DNS、認証、証明書及び回線等の障害時について、基本的な動作、復旧方式、業務影響並びに緊急バイパスの実現方式及びセキュリティ上の影響を示すこと。	受託者は、障害種別ごとの判定条件、承認者、対象、開始・終了、最大継続時間、通信範囲、ログ及び復旧確認を障害時動作表・手順書として確定する。
(14) 管理、ログ及び SLA	ログ保存、検索、監視、通知及びインシデント対応の共通要件は 05「導入・移行・試験・運用保守仕様書」による。SSE 固有の管理及び可視化要件は、本書第 3 章による。	提案者は、SSE 固有の管理、可視化、権限管理、管理者操作記録並びにログの保存、検索、出力、外部連携、監視及び通知について、実現方式、対応範囲、主な制約及び必要なライセンスを示すこと。必須要件に必要な機能・ライセンスは基本提案価格に含め、任意の追加分析等をオプションとして提案する場合のみ追加費用を示すこと。	受託者は、ログ項目、保存先、SSE 製品上でのオンライン保存期間、アーカイブ期間、復元手順、通知先、閲覧権限、レポート、しきい値、連絡先及び日常運用手順を確定する。
(15) ポリシー変更及び継続的なチューニング	SSE の各種セキュリティポリシーは、導入時だけでなく契約期間中を通じて、業務内容、利用サービス、脅威、誤検知及び通信影響等に応じて見直し・変更を行うものとする。	提案者は、契約期間中のポリシー変更、例外設定及びチューニングについて、対応範囲、実施体制、発注者との役割分担及び追加費用が生じる条件を示すこと。本仕様書で求める対応は基本提案価格に含めること。	受託者は、変更申請、影響確認、承認、設定変更、動作確認及び切戻し等の手順並びに発注者と受託者の役割分担を確定する。設定変更は、原則として発注者と変更内容及び影響範囲を確認した上で実施する。
(16) ライセンス及び価格条件	構築・検証期間、契約期間中の利用・保守及び価格算定数量は 00「共通調達仕様書」による。	提案者は、ライセンス指標、数量増減条件、自動更新、価格改定条件及びサポート終了時の取扱いを示す。必須要件を満たすために必要な機能、ライセンス、構築及び契約期間中の運用保守は、SSE 一式の基本提案価格に含めること。基本提案価格に含まれない任意のオプションを提案する場合は、その内容及び追加費用を区分して示すこと。機能別の価格内訳は、	受託者は、契約した価格・数量条件に基づき、ライセンス割当、管理アカウント、更新日、更新手続及び容量監視方法を確定する。

項目	発注者の事前提示	提案及び契約前の合意	契約後の詳細確定
		任意のオプションを除き求めない。	
(17) 移行、試験及び受入条件	3,000 台の Windows 端末への段階展開、作業日時、パイロット実施その他の共通条件は、本書第 6 章及び 05 による。UTM 撤廃への対応を最優先とし、CASB、DLP 等の詳細ポリシー及びロケーションフリー環境については、検証及びチューニングを行いながら段階的に適用するものとする。	提案者は、パイロット導入、端末展開、切戻し、性能確認、障害試験及び既存サービスとの結合試験について、基本的な実施方針及び考え方を示すこと。SSE クライアントについては、接続確立・復旧及び主要 SaaS 利用時の利用者影響を確認する考え方を示すこと。	受託者は、契約した主要条件に基づき、対象端末、日程、展開単位、詳細な試験手順、測定条件、合否基準、期待結果、証跡、切戻し判定、再試験方法及びチューニング方法を確定し、試験開始前に発注者の承認を得ること。パイロット導入で確認した接続時間、通信遅延及び利用者影響を踏まえ、本番展開の可否を発注者と確認すること。