

分冊 04 認証・端末状態・既存サービス連携仕様書

第 1 章 目的及び本書の位置付け

(1) 目的

本仕様書は、03「SSE・ゼロトラスト仕様書」に基づき導入する SSE について、本市が既に利用している認証基盤、Google Workspace for Education Plus、端末管理・セキュリティ製品及び Web フィルタリング等と適切に組み合わせ、利用者認証、管理対象端末の確認、端末状態を用いたアクセス制御及び既存サービスとの役割分担を実現することを目的とする。

また、SSE 単体の設定のみを検討するのではなく、関連する既存サービスを含め、認証、SSO、ユーザー・グループ管理、端末状態、アクセス制御、ログ及び障害切り分けを全体として整理し、継続的に運用可能な構成とすること。

(2) 本書の位置付け

- ・ 本仕様書は、03「SSE・ゼロトラスト仕様書」に定める SSE 機能要件を前提として、SSE と既存サービス間の認証、ユーザー・グループ情報、端末状態、証明書、アクセス制御及び役割分担に関する要件を定める。
- ・ SSE の SWG、FWaaS、CASB、DLP、脅威対策、SSL/TLS 通信検査、DNS セキュリティその他の機能要件は、03「SSE・ゼロトラスト仕様書」に従うこと。
- ・ 校務 SSID への接続認証に関する要件は、01「ネットワーク部分仕様書」に従うこと。
- ・ 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。

(3) 用語

- ・ Google Workspace for Education Plus（以下「GWS」という。）
- ・ GWS の Context-Aware Access（以下「CAA」という。）
- ・ EVECLOUD：本市が利用する既存の IdP 及び認証基盤
- ・ SSE：03に基づき導入する Security Service Edge サービス。特定メーカー又は製品に限定しない。

第 2 章 基本方針及び既存環境

(1) 基本方針

- ・ EVECLOUD を SSE 利用時の IdP として継続利用すること。
- ・ 利用者認証及び MFA は、EVECLOUD その他既存認証基盤の機能を活用することを基本とし、SSE 専用の追加認証製品の導入を必須としないこと。追加認証が必要となる場合は、既存機能で実現可能な範囲を優先すること。
- ・ SSE 側では、IdP による認証結果に加え、本市管理端末であること、OS の状態、端末セキュリティ機能の稼働状況その他取得可能な端末状態情報をアクセス制御条件として利用できること。
- ・ SSE で利用するユーザー・グループ情報については、GWS の OU、グループ、属性情報等を活用できる場合はこれを利用し、運用上適さない場合は、他の適切な方式を採用すること。認証基盤とユーザー情報の連携元を区別して設計すること。
- ・ 新たな IDaaS の導入は本調達の前提としない。SCIM 等の自動プロビジョニングに対応しない教育系 SaaS が多いこと、現行の CSV 運用が残ること及び費用対効果を踏まえ、既存運用を活用すること。
- ・ 本市では、Excel 又はスプレッドシートで人事・アカウント情報を管理し、GAS、数式等により各サービス用 CSV を生成している現行運用がある。SSE 連携のために当該運用を不必要に複雑化しないこと。

- ・ SSE のユーザー・グループ構成は、GWS の OU、グループ、属性情報等を活用する場合を含め、SSE のアクセス制御及び運用に適した構成とすること。
- ・ メーカーが正式にサポートしない設定又は将来のバージョンアップ等で継続性が保証されない方式を、本番運用の前提としないこと。
- ・ 本仕様書の必須要件を満たすために必要な機能、ライセンス、設定、連携及び運用保守は、原則として SSE 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に限り、その内容及び追加費用を明示すること。

(2) 主な既存サービス

- ・ EVECLOUD : 利用者認証、SSO、MFA その他既存認証機能
- ・ GWS : ユーザー・組織管理、CAA 及び SSO 等によるアクセス制御
- ・ Sophos Intercept X : EDR 及び端末セキュリティ
- ・ SKYSEA Client View : Windows 端末・IT 資産管理、ソフトウェア及び設定配布
- ・ i-FILTER@Cloud : 既存の Web フィルタリング
- ・ 03 で導入する SSE : 校内外共通の通信セキュリティ、クラウド利用制御及びコンテキストに基づくアクセス制御

(3) 全体最適及び関係事業者との調整

- ・ 受託者は、SSE 単体の要件のみでなく、EVECLOUD、GWS、CAA、Sophos Intercept X、SKYSEA Client View、i-FILTER@Cloud その他関連サービスを含め、認証、SSO、ユーザー・グループ管理、端末状態、アクセス制御及びログの全体構成を整理すること。
- ・ 既存サービスとの設定変更、連携条件、責任分界及び障害切り分け方法を整理すること。関係事業者との調整、作業管理及び試験の共通要件は、05「導入・移行・試験・運用保守仕様書」による。
- ・ 既存サービスの仕様上の制約により直接連携が困難な場合は、運用、CSV、標準機能その他の代替方法を示し、追加製品の導入のみを解決策としないこと。

第 3 章 認証及びユーザー・グループ情報連携

(1) EVECLOUD による認証

- ・ 対象利用者が EVECLOUD による認証を経て SSE を利用できること。
- ・ SAML 2.0、OpenID Connect その他の標準的な方式により EVECLOUD と提案 SSE を連携できること。採用方式のサポート条件、制約及び必要な設定を明示すること。特定の製品名同士の公式連携実績のみを必須条件とはしない。
- ・ 採用するユーザー識別子、認証フロー、セッションの扱い及び認証障害時の影響を明示すること。EVECLOUD から所属、グループ、役職、ロール等の属性が SSE へ連携されることを前提とせず、利用者認証結果及びユーザー識別情報を基本として設計すること。
- ・ SSE 利用時の MFA は、原則として EVECLOUD 側の既存運用及び認証ポリシーを活用すること。SSE 側で追加の認証機能を利用する場合は、その必要性、対象、効果及び標準機能・任意オプションの別を明示すること。
- ・ 接続元、利用場所その他の条件に応じた追加認証又はアクセス制限を行う場合は、EVECLOUD その他既存認証基盤で利用可能な機能を基本とし、動的なリスクベース認証機能の導入を必須要件とはしないこと。

(2) 利用者識別及び共有端末

- ・ SSE 上で、採用する接続方式に応じて利用者又は端末を適切に識別し、アクセス制御及びログ確認に利用できること。

- ・共有端末又は複数利用者が利用する端末では、利用者の切替に応じて認証状態及びアクセス制御が適切に切り替わること。採用する利用者識別方法、認証状態の切替方法及びログ上の識別方法は、提案時に示すこと。その他、共有端末に係る試験、展開及び運用の共通要件は、05「導入・移行・試験・運用保守仕様書」による。
- ・前利用者の認証情報が次利用者のアクセス制御に不適切に利用されないよう設計すること。
- ・製品仕様又は接続方式上、利用者単位で識別できない通信がある場合は、その条件、ログ上の識別単位、運用上の影響及び代替となる確認方法を提案時に示すこと。

(3) GWS を用いたユーザー・グループ情報の連携

- ・SSE で利用するユーザー・グループ情報については、GWS の OU、グループ、属性情報等を活用できる場合はこれを利用し、運用上適さない場合は、他の適切な方式を採用すること。
- ・GWS の OU、グループ、属性情報等を SSE で利用する場合は、SSE のアクセス制御に有効であり、かつ運用負荷の軽減につながる範囲で活用すること。
- ・SSE におけるユーザー同期、グループ利用、属性利用その他に製品上の制約がある場合は、提案時に制約、影響及び代替方法を明示すること。

(4) 連携方式及び代替運用

- ・SSE へのユーザー情報の登録又は同期については、提案 SSE 及び GWS 等の既存環境で利用可能な方式を確認し、運用負荷、反映時間及び継続性を踏まえて適切な方式を採用すること。
- ・自動プロビジョニングが利用できない又は適さない場合は、CSV、管理画面操作その他の代替方法を採用できること。現行の Excel、スプレッドシート、GAS 等によるアカウント管理及び CSV 生成の仕組みを活用できる場合は、その活用も検討すること。

(5) 変更・停止等の反映

- ・異動、退職、利用停止その他の変更が発生した場合に、SSE 上のユーザー情報又はアクセス権限を適切に反映する方法を提案すること。
- ・SSE 自体にアカウントライフサイクル管理機能を持たせることを必須とはしない。既存のアカウント管理運用と整合した反映方法を示すこと。

第 4 章 管理対象端末及び端末状態を用いたアクセス制御

(1) 基本方針

SSE におけるアクセス制御では、IdP による利用者認証結果に加え、本市が管理する Windows 端末であること及び取得可能な端末状態情報を判断材料として利用すること。具体的な判定方法及び情報源は、次項以降に定める。

(2) 管理対象端末の判定

- ・本市が管理する Windows 端末であるか否かを判定し、SSE のアクセス制御条件として利用できること。
- ・判定方式として、SSE クライアントの登録状態、端末証明書、端末 ID、Windows 情報その他提案 SSE が正式にサポートする方法を利用できること。
- ・端末交換、廃棄、紛失その他により管理対象外となった端末について、判定情報を失効又は無効化できること。

(3) 端末状態の利用

- ・OS の状態、SSE クライアントの状態、端末セキュリティ機能の稼働状況その他取得可能な端末状態を、アクセス制御条件として利用できること。

- ・取得可能な端末状態項目、取得方法、更新間隔、判定タイミング及び標準機能・任意オプションの別を提案時に示すこと。必須要件の実現に必要な機能は基本提案価格に含めること。
- ・管理対象端末又は端末状態の判定に、Sophos Intercept X、SKYSEA Client View、SSE クライアント、Windows その他の情報を利用する場合は、その情報源、判定方法及び制約を示すこと。
- ・パッチ適用状況、ディスク暗号化、ホストファイアウォール等については、取得可能な範囲を示すものとし、全項目の取得を一律に必須とはしない。

(4) 非準拠・取得不能時

- ・端末が非準拠と判定された場合又は端末状態を取得できない場合に、拒否、制限、警告その他の動作を設定できること。
- ・採用する制御は、セキュリティと業務継続を踏まえて発注者と協議の上決定すること。

第 5 章 既存サービスとの連携及び役割分担

(1) GWS 及び CAA

- ・GWS 及び CAA は、継続利用を想定する。
- ・Google サービス固有のアクセス制御については、CAA の既存機能を有効活用し、SSE と併用する場合は、それぞれの役割及び判定条件を整理し、不要な二重制御が生じないようにすること。
- ・SSE で利用するユーザー・グループ情報の連携については、第 3 章 (3) 「GWS を用いたユーザー・グループ情報の連携」によること。

(2) Sophos Intercept X

- ・Sophos Intercept X を EDR 及び端末セキュリティとして継続利用すること。
- ・SSE と Sophos Intercept X のマルウェア検知、通信遮断、端末隔離、通知、調査及び復旧の役割分担を整理すること。

(3) SKYSEA Client View

- ・SKYSEA Client View を Windows 端末・IT 資産管理及び配布基盤として継続利用すること。
- ・SKYSEA Client View は IaaS 環境上のサーバーを利用し、リモートアクセス機能を継続利用することを前提とする。現行環境では 2 つの VLAN ごとにリモートアクセス用の管理端末を 2 台配置し、計 4 台で運用している。
- ・SSE 導入に伴う通信経路、ルーティング、プロキシ、SSL/TLS 検査、DNS、ポートその他の変更により、SKYSEA Client View のリモートアクセス、資産管理、ログ収集その他の既存機能に影響を与えないこと。必要に応じて SSE 経由とする通信及び SSE 経由から除外する通信を整理すること。

(4) i-FILTER@Cloud

- ・i-FILTER@Cloud は、現行の Web フィルタリングサービスとして利用している。SSE 導入に当たっては、SSE との機能重複、通信経路、Web アクセス制御、プロキシ、PAC、SSL/TLS 通信検査、危険サイト対策、ログ、運用管理、性能、二重プロキシ・二重復号・ポリシー競合等による影響及び既存運用への影響を総合的に整理した上で、i-FILTER@Cloud との併用、機能分担、構成変更、機能統合又は SSE への機能移行を含め、本市にとって最適な構成を提案すること。提案に当たっては、採用する構成の考え方、既存運用への影響、移行方法及び役割分担を明示すること。

(5) その他のサービス・アプリケーション

- ・デジタル教科書、本市が調達する教育支援ツール（WinBird 等）、発注者が指定するその他のサービス・アプリケーション及び今後導入するサービス・アプリケーションについても、SSE 導入に伴う影響確認及び必要なチューニングの対象とすること。

第 6 章 連携設計、証明書及び責任分界

(1) 連携設計

- ・受託者は、認証、ユーザー・グループ情報、端末状態及び既存サービスとの連携について、採用する連携方式、情報の流れ及び役割分担を整理し、設計書、連携一覧、通信フロー図その他必要な成果物に反映すること。成果物の共通条件は 00「共通調達仕様書」及び 05「導入・移行・試験・運用保守仕様書」による。

(2) 証明書及び秘密情報

- ・認証・連携に用いる証明書、API キー、クライアントシークレットその他の認証情報を使用する場合は、その用途、発行主体及び管理主体を整理すること。
- ・認証・連携に用いる証明書の更新、切替又は失効により、認証又は通信に長時間の影響が生じない設計とすること。
- ・証明書、API キー、秘密鍵その他の認証情報の保管、更新、失効、漏えい時対応その他の管理は、00「共通調達仕様書」による。端末への証明書配布及び更新に係る共通の導入・運用手順は、05「導入・移行・試験・運用保守仕様書」による。

(3) 責任分界及び技術調整

- ・既存サービスとの連携に伴い他事業者による設定変更等が必要となる場合は、SSE 導入に必要な技術条件及び影響範囲を整理すること。責任分界、事業者間調整及び障害対応の共通要件は、00「共通調達仕様書」及び 05「導入・移行・試験・運用保守仕様書」による。

第 7 章 障害時及び運用設計

(1) 認証・連携障害時

- ・EVECLOUD、GWS その他の認証・ユーザー情報連携が利用できない場合について、既存セッション、新規認証、再認証、既存ユーザー情報の扱い及び復旧時の動作を整理すること。GWS のグループ情報等を利用する構成の場合は、その影響も考慮すること。
- ・端末状態情報又は既存サービスとの連携情報を取得できない場合の動作を整理し、03「SSE・ゼロトラスト仕様書」に定める障害時及び業務継続の方針と整合させること。
- ・障害切り分け、連絡、復旧及び試験に関する共通要件は、05「導入・移行・試験・運用保守仕様書」による。

(2) 運用変更

- ・GWS の OU、グループ、属性情報等を SSE で利用する場合は、GWS 側の変更が SSE のアクセス制御及び運用へ与える影響を考慮した設計とすること。
- ・ユーザー・グループ情報の連携方式が運用上適さないことが判明した場合は、発注者と協議の上、連携方式又は管理方法を見直すこと。
- ・設定変更、影響確認、承認、試験及び切戻し等の変更管理に関する共通要件は、05「導入・移行・試験・運用保守仕様書」による。

第 8 章 現行調査及び試験要件

(1) 現行調査

- ・ 受託者は、05「導入・移行・試験・運用保守仕様書」に基づく現行調査において、認証、ユーザー・グループ情報、管理対象端末・端末状態及び既存サービスとの連携に必要な現行構成、設定及び制約を確認し、本仕様書に定める設計へ反映すること。
- ・ 特に、EVECLOUD の認証方式、GWS のユーザー・OU・グループ・CAA 等の構成、GWS から SSE へ利用可能なユーザー・グループ情報、管理対象端末・端末状態の判定に利用可能な情報及び既存サービスとの連携条件を確認すること。

(2) 試験

- ・ 認証、ユーザー・グループ情報連携、管理対象端末・端末状態判定及び既存サービスとの連携について、採用した設計どおりに動作することを確認すること。
- ・ 試験の共通条件、実施方法、証跡及び検収要件は、05「導入・移行・試験・運用保守仕様書」による。

第 9 章 成果物

- ・ 受託者は、00「共通調達仕様書」及び 05「導入・移行・試験・運用保守仕様書」に定める成果物の共通条件に従い、本仕様書に係る設計内容を成果物へ反映すること。
- ・ 少なくとも、次の内容を基本設計書、詳細設計書、構成図、連携一覧その他適切な成果物に整理すること。
- ・ EVECLOUD と SSE の認証方式及び認証フロー
- ・ GWS から SSE へのユーザー・グループ情報の連携方式及び管理方法
- ・ SSE におけるユーザー・グループ情報の利用方法及びポリシー適用方針
- ・ 管理対象端末及び端末状態の判定方式
- ・ GWS・CAA、Sophos Intercept X、SKYSEA Client View、i-FILTER@Cloud 等の既存サービスと SSE の役割分担
- ・ 認証、ユーザー・グループ情報、端末状態及び既存サービスとの連携構成

第 10 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、本仕様書に定める要件を満たすことを前提として、認証、ユーザー・グループ情報連携、管理対象端末・端末状態判定及び既存サービス連携について、採用する実現方式、効果、主な制約、運用方法及び必要なライセンス等を具体的に示すこと。

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。

提案書の様式は指定しない。要件への適合可否については、別添「機能証明書」により回答すること。また、提案書には仕様書の各要件との対応関係が確認できるよう記載すること。

提案内容の採用範囲、役割分担、主要な条件及び費用については契約締結前に整合し、契約締結後は、契約した提案内容及び本仕様書の要件に基づき、具体的な設定、管理方法及び運用条件を詳細設計において確定すること。

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、主な制約、ライセンス及び費用を基本とし、個別設定値、対象一覧、詳細な判定条件、設定値、運用手順及び試験条件は、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) EVECLOUD 認証及び利用者識別	EVECLOUD を SSE 利用時の IdP として継続利用する。利用者認証及び MFA は、EVECLOUD その他既存認証基盤の機能を活用することを基本とし、SSE 専用の追加認証製品の導入を必須としない。	EVECLOUD と SSE の認証方式、利用者識別の考え方、MFA の役割分担、対応範囲及び主な制約を示すこと。追加機能又はライセンスが必要な場合は、その必要性及び標準機能・追加ライセンス・任意オプションの別を示すこと。必須要件の実現に必要なものは基本提案価格に含めること。	採用した認証方式に基づき、具体的な認証設定、ユーザー識別子、認証フロー、セッション、MFA、管理方法及び認証障害時の運用条件を詳細設計で確定する。
(2) ユーザー・グループ情報連携	SSE で利用するユーザー・グループ情報については、GWS の OU、グループ、属性情報等を活用できる場合はこれを利用し、運用上適さない場合は他の適切な方式を採用する。現行の Excel、スプレッドシート、GAS 等によるアカウント管理及び CSV 生成の運用を不必要に複雑化しない。	GWS 等から SSE へのユーザー・グループ情報の登録又は同期方式、利用方法、主な制約及び代替方式を示すこと。自動プロビジョニングが利用できない又は適さない場合は、CSV、管理画面操作その他の代替方法及び運用負荷の考え方を示すこと。	連携対象となるユーザー・グループ情報、登録・同期方式、具体的な設定、異動・退職・利用停止その他の変更の反映方法及び管理方法を詳細設計で確定する。
(3) 共有端末、管理対象端末及び端末状態	SSE のアクセス制御では、IdP による利用者認証結果に加え、本市が管理する Windows 端末であること及び取得可能な端末状態情報を判断材料として利用する。共有端末又は複数利用者が利用する端末についても適切に識別できる構成とする。	共有端末における利用者識別の考え方、管理対象端末の判定方式、利用可能な端末状態情報、情報源、主な制約及び標準機能・任意オプションの別を示すこと。	利用者識別及び切替方法、管理対象端末の具体的な判定条件、利用する端末状態項目、取得方法、更新・判定タイミング、非準拠・取得不能時の動作並びに端末交換・廃棄・紛失時の失効又は無効化方法を確定する。

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
(4) 既存サービスとの連携及び役割分担	GWS・CAA、Sophos Intercept X、SKYSEA Client View 及び i-FILTER@Cloud を既存サービスとして利用している。各サービスの役割及び既存機能を踏まえ、SSE との全体構成を整理する。	GWS・CAA、Sophos Intercept X、SKYSEA Client View、i-FILTER@Cloud 等との役割分担、主な制約及び必要な設定変更を示す。i-FILTER@Cloud については、SSE との機能重複、通信経路、Web アクセス制御、プロキシ、PAC、SSL/TLS 通信検査、危険サイト対策、ログ、運用管理、性能、二重プロキシ・二重復号・ポリシー競合等による影響及び既存運用への影響を総合的に整理し、併用、機能分担、構成変更、機能統合又は SSE への機能移行を含め、本市にとって最適な構成を示す。	採用した構成に基づき、既存サービスとの具体的な役割分担、設定変更、責任分界、既存運用への影響及び必要な移行方法を詳細設計で確定する。
(5) 連携設計、証明書及び責任分界	既存サービスとの設定変更、連携条件、責任分界及び障害切り分け方法を整理する。既存サービスの仕様上、直接連携が困難な場合は、運用、CSV、標準機能その他の代替方法を検討する。	採用する連携方式、情報の流れ、主要な設定変更の有無、必要なライセンス、関係事業者との役割分担・調整の考え方及び主な制約を示すこと。既存サービスの設定変更が必要となる場合は、その対象及び影響範囲の考え方を示すこと。	具体的な連携設定、設定変更対象、証明書・認証情報の用途及び管理主体、更新・切替・失効方法、事業者間の作業分担並びに連絡・調整方法を詳細設計で確定する。
(6) 障害時及び代替運用	EVECLOUD、GWS その他の認証・ユーザー情報連携、端末状態情報又は既存サービスとの連携情報を取得できない場合の動作は、03「SSE・ゼロトラスト仕様書」に定める障害時及び業務継続の方針と整合させる。	認証、ユーザー情報連携、端末状態取得又は既存サービス連携が利用できない場合の主な影響及び代替方法を示す。復旧後の動作及び運用上必要となる対応も示す。	既存セッション、新規認証、再認証、既存ユーザー情報の扱い、復旧時の動作、連絡・復旧手順及び必要な変更管理・試験・切戻しの条件を詳細設計で確定する。