

上野原市次世代校務DX環境機器調達
仕様書

令和8年5月

上野原市教育委員会

1 総則

(1) 件名

上野原市次世代校務 DX 機器調達

(2) 概要

本貸借による調達仕様書は、上野原市教育委員会（以下、「教育委員会」という。）が発注する「上野原市次世代校務 DX 環境機器調達」について受注者の行う業務の範囲、それぞれの責務、その他の業務の実施に必要な条件等を定め、業務の円滑な実施を実現するにあたり、必要最低限の仕様を定めるものとする。受注者は本仕様書の記載事項に沿って遂行しなければならない。

(3) 目的

教育委員会は令和 2 年度に小中学校等の学校ネットワーク強靱化の構築を行った。令和 8 年 4 月 1 日より山梨県統合型校務支援システム更改およびクラウド移行に伴い、令和 7 年 3 月に文部科学省からの教育情報セキュリティポリシーに関するガイドラインが改定されたことを踏まえ、ゼロトラストの考え方にに基づき、現行の教育 ICT 環境からアクセス制御によるセキュリティ対策を十分に講じた次期環境整備を行うことを目的とする。

(4) 本業務の基本方針

教育委員会では、教育 ICT 設備の活用推進、教育現場における不登校対策強化、学習環境の改善、教職員の多忙化解消・働き方改革の推進により学校教育の充実を図り、子どもたちが安全・安心に学べる学校環境整備を目指している。

令和 8 年度より教育 ICT に関わるサーバー関連、ネットワーク関連、ソフトウェア関連、保守・運用関連の業務を委託し、調達から保守・運用までを一元化して障害が発生した場合への早期対応を図り、教育 ICT 環境のセキュリティを強化してきたところである。一方で、現環境の教育現場での利活用が進み、機能面やセキュリティ面等で新たな課題も出てきている。また、国の ICT 整備方針や市場の技術動向が変化する中で、ICT 機器やシステム、ネットワーク等の全体的な見直しの必要が生じているところである。例えば、次のような課題が挙げられる。

- ・ 校務処理操作や情報連携等による業務負荷が高く、子どもたちの教育に時間が割けない。
- ・ 新型コロナウイルスを起因として働き方・学び方の変化が求められているが、ロケーションフリーで業務を実施する環境が整備されておらず、業務の仕組みの見直しが必要である。
- ・ 学校で取り扱うファイルの管理方法やデータの情報漏洩対策の強化が必要である。
- ・ 情報セキュリティ対策が不十分であり、システム面の対策及び教職員の ICT リテラシー向上が必要である。

次期環境においては現環境における課題を解決するため、次のとおり方針を掲げて整備を行う。

① ICT 利活用による教育の質の向上

ア ICT 技術を活用し、児童生徒の興味・関心を引く授業を実施するとともに、学力の向上を図る。

イ 教育委員会の環境や利用実態を踏まえた利活用研修を実施することで、教育委員会の実態に応じた ICT の利活用推進を図る。

② 校務の効率化

ア システム機能強化や業務プロセスの見直しにより、業務のデジタル化を実施して効率化を図る。

イ 将来の拡張性として、テレワークが可能なシステム整備により働き方改革を目指す情報セキュリティを確保する。

- ウ 文部科学省が公表する最新の教育情報セキュリティポリシーの内容に基づき、統一された情報セキュリティ水準を確保するための協議を実施する
- エ 現行の教育 ICT セキュリティ対策について見直しを行い、教職員や児童生徒が安心して指導、学習を実施できる環境を構築する

(5) 次期環境構築仕様

前項の基本方針を踏まえ次期環境構築方針を次のとおりとし、次に示す構築方針を基に構築すること。

① 効果的なハードウェア・ソフトウェアの選定

ハードウェアについては、教育の質向上や多様な働き方への対応を可能にするため、テレワークを含む将来想定される働き方にベストマッチしたハードウェアであることが求められる。またソフトウェアについても、ICT 技術を活用した指導や学習を効果的に行うことができ、児童生徒の学力向上を図ることができるものを選定することが求められる。

② ICT 管理に係る業務負担の軽減

ICT 機器やシステムの管理に係る運用設計や事業者が運用保守内容の設計を行うにあたっては、教職員や教育委員会職員の管理負荷ができるだけ低減されるような提案であることが望ましい。

③ 技術動向・政策動向への対応

次期環境の稼働期間は令和 9 年 1 月 1 日から令和 13 年 12 月 31 日までの 5 年間で想定しているが、さらにその後の運用も視野に含め、持続的な教育効果を高めることができるよう安定的な運用ができる環境が望ましい。一方で、教育 ICT に関する技術動向や政策動向の変化はめまぐるしく、それらの変化に対応できるよう拡張性のある構築であることが求められる。なお、教育委員会としては稼働期間中に次期環境の導入システムの機能強化や新規バージョンのリリースがあった場合には、最新のものを活用したいと考えている。

次の政策動向については準拠が必要である。

ア 内閣官房「デジタル行財政改革会議」における教育 DX の政策動向

イ 文部科学省における教育 DX、GIGA スクール等に関する動向

ウ 中央教育審議会（個別最適な学びと協働的な学びの一体的な充実に向けた学校教育の在り方に関する特別部会、デジタル学習基盤特別委員会、次期 ICT 環境整備方針の在り方ワーキンググループ、教科書・教材・ソフトウェアの在り方ワーキンググループ等）

エ 有識者会議（教育データの利活用に関する有識者会議等）

オ 調査研究事業（次世代の学校・教育現場を見据えた先端技術・教育データの利活用推進（最先端技術及び教育データ利活用に関する実証事業（等））

カ デジタル庁、総務省、経済産業省等の関連省庁における関連施策の動向

キ 教育 DX ロードマップ」等のデジタル化施策（デジタル庁）

ク 「未来の教室」等の学校現場のデジタル環境の推進施策（経済産業省）

(6) 履行対象

- ① 上野原市役所本庁舎（教育委員会執務室、サーバ室等を含む。）
- ② 市立小中学校（小学校 4 校、中学校 3 校）
- ③ その他外部施設（四方津調理場）

(7) 納入対象拠点

納入する機器の対象拠点及び児童生徒数・職員数は次のとおりである。

① 対象拠点

	区分	施設名	住所
1	市役所	上野原市役所	山梨県上野原市上野原 3832
2	小学校	上野原西小学校	山梨県上野原市コモアしおつ 2 丁目 13-1
3	小学校	島田小学校	山梨県上野原市鶴島 2024
4	小学校	上野原小学校	山梨県上野原市上野原 3454
5	小学校	秋山小学校	山梨県上野原市秋山 8674
6	中学校	上野原西中学校	山梨県上野原市四方津 215
7	中学校	上野原中学校	山梨県上野原市上野原 9191
8	中学校	秋山中学校	山梨県上野原市秋山 6770
9	外部施設	四方津調理場	山梨県上野原市四方津 335-1

② 児童生徒数・教職員数

	区分	施設名	児童・生徒数	教職員数
1	市役所	上野原市役所	-	17 人
2	小学校	上野原西小学校	174 人	28 人
3	小学校	島田小学校	58 人	19 人
4	小学校	上野原小学校	349 人	52 人
5	小学校	秋山小学校	36 人	16 人
6	中学校	上野原西中学校	149 人	24 人
7	中学校	上野原中学校	175 人	31 人
8	中学校	秋山中学校	16 人	17 人
9	外部施設	四方津調理場	-	1 人
合計			957 人	205 人

(8) 納入期限

導入する機器の納入期限は令和 8 年 12 月 18 日とする。

(9) 賃貸借期間

導入する機器の契約（賃貸借）期間は、令和 9 年 1 月 1 日から令和 13 年 12 月 31 日とする。

(10) 賃貸借料の支払い

契約金額（月額）を毎月請求（当月分を翌月上旬に請求）により支払うこととし、請求より 30 日以内にこれを支払うこととする。

なお、支払いは令和 9 年 1 月分の支払いからとする。

(11) 留意事項

- ① 受注者は納入するソフトウェアのユーザー登録に関わる諸手続きを代行申請すること。
- ② 仕様の条件は必ず満たすこと。仕様項目においてはスペック同等以上を必須とする。
- ③ 仕様書に満たない構成の場合は、入札参加できないものとする。
- ④ 今回納入する機器で必要となるケーブル部材及び作業費は全て含むこと。
- ⑤ 仕様書に記載されていない事項で疑義が生じた場合は、教育委員会担当者との協議の上、対応するものとする。また明記なくとも当然常識的に行うべきことは本仕様を含むこととする。

2 調達範囲

(1) 調達対象システム

次期環境の調達対象システムは、「表 次期環境の調達対象システム」を参照のこと。ただし、業務ごとにシステムを構築する必要はなく、複数の対象業務に対応したシステム・ソフトウェアの提案や、複数のシステム・ソフトウェアでシステム要件を満たす提案とする。

また、対象となる拠点・教職員数・児童生徒数・学級数等については、「対象拠点・教職員数・児童生徒数一覧」を参照すること。

なお、人口構成の変化や人事異動等により利用者数は多少変動することがあるため留意すること。

	提供形態	システム名	利用対象（ライセンス）
1	クラウドサービス	ゼロトラストネットワーク基盤 (Secure Access Service Edge) ※SASE	教職員 205 ライセンス（非常勤・予備機分を含む）
2		統合認証基盤	教職員 205 ライセンス（非常勤・予備機分を含む）
3		モバイル端末管理（MDM）システム	教職員 205 ライセンス（非常勤・予備機分を含む）
4	オンプレミスサーバ (市庁舎へ配備)	Active Directory システム	教職員 205 人
5		Active Directory 連携用システム	教職員 205 人
6		WSUS システム	教育委員会に配備されたサーバ 一台数分
7		ファイル共有システム	教職員 205 人
8		バックアップシステム	教育委員会に配備されたサーバ 一台数分
9		統合 ID 管理システム	教職員 205 人
10		校務用多要素認証システム	教職員 205 ライセンス（非常勤・予備機分を含む）
11	校務系ネットワーク認証システム	教職員 205 ライセンス（非常勤・予備機分を含む）	

(2) 共通要件

- ① 上野原市内の全 7 校にある校務兼財務会計アクセス用パソコンから市庁舎内の財務会計システムにアクセスさせること。
- ② 納入する機器はすべて新品とすること。
- ③ ソフトウェアはサポートを締結し、契約期間中は問合せ可能な状態とすること。
- ④ 構築及び運用に必要なケーブル、ソフトウェア及びドライバを含めること。また、本仕様書に記載されなくとも、稼動のため必要と判断される製品は本契約内で提供すること。
- ⑤ サーバー及び無停電電源装置（UPS: Uninterruptible Power Supply）の電源電圧は 100V とすること。また、本事業にて設置する機器において既設電源の容量を超過する場合は、追加の電源工事を本契約の中で行うこと。
- ⑥ 本事業にて庁舎に配置する機器が接続される無停電電源装置を、必要数調達すること。また、19 インチラックに搭載する全ての機器は、無停電電源装置に接続すること。
- ⑦ 本調達に含む製品ライセンスは、サービスインから 5 年間に於いて継続して使用可能であること。また、アクティベーション等の作業またはライセンス業者への登録が必要な場合は、本契約

	機器名称	市庁舎	上野原西小学校	島田小学校	上野原小学校	秋山小学校	上野原西中学校	上野原中学校	秋山中学校	四方津調理場	合計
	ール										
4	上野原市庁舎用 L2 スイッチ	2	0	0	0	0	0	0	0	0	2
5	上野原市庁舎用メディアコンバータ	6	2	2	2	2	2	2	2	2	22
6	上野原市庁舎用仮想化基盤サーバー	2	0	0	0	0	0	0	0	0	2
7	上野原市庁舎用無停電電源装置（仮想化基盤サーバー用）	2	0	0	0	0	0	0	0	0	2
8	上野原市庁舎用仮想化ストレージ	1	0	0	0	0	0	0	0	0	1
9	上野原市庁舎用バックアップ兼電源管理サーバー	1	0	0	0	0	0	0	0	0	1
10	上野原市庁舎用無停電電源装置（バックアップ兼電源管理サーバー用）	1	0	0	0	0	0	0	0	0	1
11	上野原市庁舎用無線 LAN コントローラ	2	0	0	0	0	0	0	0	0	2
12	上野原市庁舎用学習系プロキシ	1	0	0	0	0	0	0	0	0	1
13	上野原市庁舎用管理パソコン	1	0	0	0	0	0	0	0	0	1
14	学校用 L3 スイッチ	0	2	2	2	2	2	2	2	1	15
15	学校用メディアコンバータ	0	0	0	6	0	0	0	0	2	8
16	学校用 PoE スイッチ	0	6	4	16	6	6	12	6	0	56
17	学校用 PoE スイッチ（体育館）	1	0	0	1	1	0	0	1	0	4
18	学校用無線アクセスポイント	1	32	14	41	13	28	29	12	0	170
19	上野原市庁舎用サーバーラック	1	0	0	0	0	0	0	0	0	1

(3) 情報セキュリティ対策

文部科学省の教育情報セキュリティポリシーおよび上野原市セキュリティポリシーに関するガイドラインに従い、機密性、完全性、可用性を確保するために十分な対策をとること。（データの盗難・改ざんの防止、動作状況の監視、障害回復等）

(4) クラウドサービス要件

① ゼロトラストネットワーク基盤要件

ア システム要件

- ㊦ メーカーが運用管理するクラウドサービスであること。
- ㊧ サービスが提供される POP で日本国内が選択できること。
- ㊨ サービスで生成されるログが日本国内で保存されること。

- ㊦ ライセンスはユーザーごとのサブスクリプションのライセンス形態であること。
- ㊧ 1ユーザーライセンスで複数台の管理が可能であること。
- ㊨ ライセンスは複数年での購入が可能であること。
- ㊩ 業務利用サービスのアクセス元 IP アドレス制限が可能となるようグローバル IP アドレス固定が可能であること。
- ㊪ ライセンスのアップグレードにより、メーカー管理以外にパブリッククラウドベンダーでの POP 展開も可能であること。
- ㊫ 基本ライセンスにて1ユーザー当たりのデータ通信量が年間 250GB 以上確保されていること。
- ㊬ メーカー管理の POP 利用の場合では、1ユーザー当たりのデータ通信量が年間 250GB を超過した場合もデータ転送の制約が設けられていないこと。

イ セキュリティ機能要件

- ㊭ アプリケーションの識別と制御機能を有していること。
- ㊮ アプリケーション識別型のルーティング機能を有していること。
- ㊯ 学校内外問わず一貫したレベルのセキュリティが提供できること。
- ㊰ POP から複数の拠点に対して IPsec トンネルを確立することでプライベートアプリケーションにアクセスが可能であること。
- ㊱ 主要 SaaS プロバイダーに直接接続し API ベースの CASB が提供できること。
- ㊲ Inline ベースの CASB が提供できること。
- ㊳ SSE エージェントをインストールすることでセキュリティ機能がエンドポイントに提供できること。
 - a IPS 機能
 - b アンチウイルス機能
 - c データ漏洩防止 (DLP)
 - d DNS フィルタリング
 - e サンドボックス
 - f SSL インスペクション
 - g Web フィルタリング
- ㊴ LDAP や RADIUS によるユーザー認証機能を有すること。
- ㊵ ユーザー認証において IdP と SAML 連携ができること。
- ㊶ VPN 機能には、リモートで使用する際常時 VPN が ON になる機能があること。
- ㊷ VPN を経由する通信と VPN を経由しない通信を制御する機能 (スプリットトンネル) を有すること。
- ㊸ スプリットトンネルは IP ベースだけでなく、ドメインにも対応できること。
- ㊹ BYOD やエージェントをダウンロードできない端末に対しては PAC ファイル等の使用にてエージェントレスセキュリティを提供できること。
- ㊺ アプリケーションに対してゼロトラストアクセスにおけるアクセス制御機能を有すること。
- ㊻ アクセス制御にはエージェントから収集したデバイスポスチャ情報を活用してポリシーが作成できること。
- ㊼ エンドポイントのデバイスポスチャ情報が収集できること。
- ㊽ 収集したポスチャ情報が管理画面上で確認ができること。
- ㊾ エンドポイントが管理端末かどうかをデバイス管理情報等で識別できること。
- ㊿ Bluetooth や USB デバイスといったリムーバブルデバイスに対する制御機能を有すること。
- Ⓚ ユーザーが作成したカスタム IPS シグネチャが使用できること。

ウ 端末機能要件

- ㊦ エージェントソフトは Windows、Linux、macOS、Android、iOS に対応していること。
- ㊧ エージェントには VPN 機能とクラウドプロキシ (SWG) への通信を制御するモジュールが統合されていること。
- ㊨ エージェントには EPP とランサムウェア対策が統合されていること。
- ㊩ エージェントはユーザーが容易にサービス停止できないこと。
- ㊪ エンドポイントが学校内外どちらに在るかを自動で検知できること。
- ㊫ 社外だと判断した場合に自動で VPN を接続し、切断が容易でないこと。

エ 管理機能要件

- ㊦ HTTPS 対応の Web インタフェースで遠隔保守が可能であること。
- ㊧ 7 日間分の通信ログを保管できること。外部ストレージサービスと連携することで 7 日以上保管できること。
- ㊨ レポート機能や分析機能を有すること。
- ㊩ レポートのスケジュール機能により任意の日時に指定したメールアドレスに送付する機能を有すること。
- ㊪ オンプレミス機器、および SASE のセキュリティポリシーをシングルコンソールから管理できること。

カ その他機能要件

- ㊦ AI (人工知能)、ML (機械学習) 等のテクノロジーを活用した取り組みが為されていること。
- ㊧ 脅威インテリジェンスを自社で開発・メンテナンスしていること。
- ㊨ 稼働率は実績ベースで 99.99% 以上であること。
- ㊩ サービスの稼働状況やメンテナンス/アップデート日時が確認できるサイトが用意されていること。
- ㊪ 管理コンソールは日本語で表記されていること。
- ㊫ 業界アナリストによる一定の評価を得ていること。
- ㊬ 政府情報システムのためのセキュリティ評価制度 (ISMAP) 取得済みのサービスであること。

② 統合認証基盤要件

ア ID 管理機能要件

- ㊦ オンプレミス環境の認証サーバー (Active Directory) と本サービスを連携し、源泉データとして利用できること。
- ㊧ オンプレミス環境の認証サーバー (Active Directory) と本サービスを連携し、本サービスの認証ユーザーとして利用できること。
- ㊨ オンプレミス環境の認証サーバー (Active Directory) と連携するグループを指定することにより、連携する利用者情報の絞り込みができること。
- ㊩ 認証サーバー (Active Directory) と連携した利用者情報と、直接登録した利用者情報の両方が一元管理できること。
- ㊪ 任意の名称の管理タグを作成し、利用者情報に付与できること。
- ㊫ 利用者一覧画面、招待コード管理画面、招待コード発行画面、利用者操作ログ画面にて、付与した管理タグごとにフィルター表示が可能であること。

イ 認証/シングルサインオン要件

- ㊦ 本サービスにログインすることでクラウドサービスやオンプレミス環境でのシステムにシングルサインオンが可能なこと。
- ㊧ 本サービスへのログイン認証方法は、パスワード、クライアント証明書、統合 Windows 認証、FIDO2 を利用した認証 (Windows Hello/Touch ID/Face ID/セキュリティキー等)、ワ

ンタイムパスワード（メール通知）、IC カード、顔認証から選択でき、これらを組み合わせた二要素認証が可能なこと。

- ㉔ 本サービスへのログイン認証にクライアント証明書の提示を求める場合には、本サービスで発行したクライアント証明書が利用可能なこと。
- ㉕ 本サービスへのログイン認証に統合 Windows 認証や FIDO2 を利用した認証 (Windows Hello / Touch ID / Face ID / セキュリティキー等)、IC カード、顔認証を組み合わせることでパスワードレスでの認証が行えること。
- ㉖ 本サービスへのログイン時に、管理者によって選択された条件に適合した場合に 2 ステップ認証ができること。
- ㉗ 2 ステップ認証時の FIDO2、顔認証、IC カード認証にパスワードレスを設定する機能を有すること。
- ㉘ Active Directory と連携する専用コネクタ機能を提供できること。
- ㉙ Active Directory と連携できない場合に備え、クラウドサービス側でログインが成功したときの認証情報をキャッシュする機能を有すること。
- ㉚ Web ブラウザを使用してシングルサインオンのログインができること。
- ㉛ Web ブラウザによる画面表示では日本語、英語を使用でき、言語設定は Web ブラウザの設定により表示言語の自動切り替えを行えること。また、管理者または利用者が標準言語の指定もできること。
- ㉜ 個々の利用者が利用可能な Web シングルサインオンが表示される利用者ポータル機能を有すること。
- ㉝ SAML/OpenID Connect 連携先のクラウドサービス側のアカウントを複数ユーザーで共有できること。
- ㉞ 重要なクラウドサービス等への SAML/OpenID Connect によるシングルサインオン時に、管理者によって選択された条件に適合した場合に追加認証ができること。
- ㉟ 追加認証として、ワンタイムパスワード（メール通知）、FIDO2、IC カード、顔認証の認証機能が使用できること。
- ㊱ 利用者単位にシングルサインオンが可能なクラウドサービスを設定する機能を有すること（アプリケーションロール）。
- ㊲ SAML/OpenID Connect 連携および代理入力によるシングルサインオンはクラウドサービスやオンプレミス環境を問わず対応できること。
- ㊳ SAML2.0 準拠のクラウドサービスをシングルサインオン対象として追加できること。
- ㊴ IdP として SAML2.0 に対応していること。
- ㊵ IdP Initiated SSO、SP Initiated SSO に対応していること。
- ㊶ ユーザーの任意属性を設定できること。

ウ 管理者機能要件

- ㊷ 管理 GUI を備えること。
- ㊸ 管理ログ、管理者ログインログ、利用者ログインログ、利用者操作ログ、同期実行ログ、SSO アクセスログを閲覧・検索が可能であること。
- ㊹ 管理ログ、管理者ログインログ、利用者ログインログ、利用者操作ログ、同期実行ログ、SSO アクセスログをファイル出力する機能を有すること。
- ㊺ 管理者ログインログ、利用者ログインログ、証明書発行ログ、同期実行ログ、SSO アクセスログについて TLS を使用した Syslog 転送方式で外部システムへ送信する機能を有すること。
- ㊻ ログイン画面のロゴマーク変更や任意メッセージの挿入機能を有すること。
- ㊼ IdP 証明書の有効期限切れ前に、事前に管理者にメールで通知をする機能を有すること。

- ㊦ ユーザー同期処理の結果を管理者にメールで通知する機能を有すること。
- ㊧ Web 管理画面、利用者ログイン画面にアクセスする際、接続元の IP アドレスによって、証明書認証が必要なネットワークと不要なネットワークを識別する機能を有すること。
- ㊨ 認証サーバーとして複数の Active Directory が連携できること。
- ㊩ スケジューラによる自動ユーザー同期と、任意の時間に即時実行が可能であること。

エ 認証局機能要件

- ㊰ ユーザーID あたり 10 枚までの証明書発行が可能であること。
- ㊱ プライベート CA 機能を有し、X.509 version3 形式のクライアント証明書およびサーバー証明書を発行できること。
- ㊲ OCSP (Online Certificate Status Protocol) および CRL (Certificate Revocation List) にて、証明書の失効状態を公開していること。
- ㊳ 秘密鍵の生成を端末内で行い、秘密鍵を外部に出すことなく安全に証明書を発行する機能を有すること。
- ㊴ 信頼する認証局を登録することにより、外部の認証局で発行されたクライアント証明書で認証する機能を有すること。
- ㊵ 管理者が招待コードを発行する招待コード方式による証明書発行が可能なこと。
- ㊶ 秘密鍵の生成、証明書の申請、証明書の取得までの一連の操作が安全かつ簡単に行える機能が提供できること。
- ㊷ カメラ機能を搭載しないデバイス (パソコン等) 向けに提供する証明書の取得用 URL にアクセスするだけで自動的に証明書が取得できる機能を有すること。
- ㊸ カメラ機能を搭載するデバイス (スマートフォン等) 向けに提供する証明書の取得用 QR コードにアクセスするだけで自動的に証明書が取得できる機能を有すること。
- ㊹ 利用者による操作のみでクライアント証明書の更新が可能なこと。
- ㊺ Windows ドメイン名や OS の種類により、証明書発行先の端末を限定する機能を有すること。
- ㊻ OS の種類により証明書の格納先を指定する機能を有し、利用者に負担を与えることなく適切な格納先へ証明書が配布できること。
- ㊼ 証明書発行時に端末名を取得し、管理者が管理できる機能を有すること。
- ㊽ 不要なクライアント証明書は、管理者が任意のタイミングで失効できること。
- ㊾ Windows OS について、Wi-Fi 接続に必要な情報を管理者が設定し、証明書配布時にあわせて配布できること。
- ㊿ Windows のコンピュータストアに複数のクライアント証明書がインストールされていても、無線認証で正しいクライアント証明書が利用できる様に、Wi-Fi 設定配布時に、認証で利用するクライアント証明書の発行者を指定できること。
- ㊰ 管理者がクライアント証明書の有効期限を任意に設定できること。
- ㊱ 招待コード方式で発行した証明書の期限切れを利用者にメールで通知する機能を有し、通知を開始するタイミングと頻度を設定できること。
- ㊲ 証明書署名要求ファイルをインポートしてサーバー証明書を発行可能なこと。
- ㊳ 秘密鍵を含んだ PKCS#12 形式または PEM 形式でサーバー証明書を発行可能なこと。
- ㊴ PKCS#12 ファイルのクライアント証明書を発行できること、また一括発行にも対応すること。
- ㊵ PKCS#12 ファイルのクライアント証明書を発行する際に、証明書の発行先情報を設定できること。
- ㊶ SCEP 固定チャレンジに対応した MDM 機能と連携しクライアント証明書の配布ができる機能を有すること。

オ オ セキュリティ機能要件

- ㊦ Web 管理画面、利用者ログイン画面を使用する際の通信は SSL/TLS により暗号化ができること。
- ㊧ クライアント証明書による Web 管理画面、利用者ログイン画面のアクセス制御ができること。
- ㊨ Web 管理画面、利用者ログイン画面のアクセスを接続元 IP アドレスにより制御ができること。
- ㊩ Web 管理画面、利用者ログイン画面で操作が行われなかった場合の、タイムアウトするまでの時間を任意に指定できること。
- ㊪ Active Directory とシングルサインオンサービス間の通信は SSL/TLS により暗号化ができること。
- ㊫ 管理者は、Web ブラウザから次の内容を含む操作ログを取得できること。
 - a ユーザーのログイン日時、ログイン名、成功/失敗、接続元 IP アドレス、クライアント証明書認証時の証明書情報
 - b 管理者のログイン日時、ログイン名、成功/失敗、接続元 IP アドレス、操作に関するログ
 - c 同期実行の実施日時、成功/失敗、処理内容
 - d SAML 連携時のシングルサインオンに関するログ
- ㊬ 重要なクラウドサービス等へのアクセス時に通常 Web ブラウザからのアクセスは禁止して、外部から保護された専用の Web ブラウザからのみアクセスを許可する制御が可能なこと。

カ サポート要件

- ㊭ 証明書管理機能については、24 時間 365 日のシステム監視を実施すること。
- ㊮ Web フォームによる問い合わせ受付ができること。

キ クラウドサービス基盤非機能要件

- ㊯ 各機能で使用する ID は一元管理可能なこと。
 - ㊰ クラウド型のサービスであること。
 - ㊱ サービスの操作マニュアル、その他の関連文書は日本語で提供すること。
 - ㊲ サービスの操作は Web 管理画面で提供され、日本語の表記が行えること。
 - ㊳ データバックアップ運用が備わっていること。
 - ㊴ ログの保全対応が備わっていること。
 - ㊵ ログの保存は 90 日まで可能であること。
 - ㊶ サービスを提供しているデータセンターが日本国内にあること。
 - ㊷ 問題が発生した場合に国内法が適用されること。
 - ㊸ 本番利用を検討するうえで、30 日の無償トライアルが利用できること。
 - ㊹ 本サービスのサーバーの Web アプリケーション、OS、ミドルウェアの定期的な脆弱性の検査、対策を実施すること。
 - ㊺ 本サービスの運用者は、プライバシーマーク、ISMS 認証 (ISO27001) 等の情報セキュリティの運用に関する第三者機関の認証を取得していること。
 - ㊻ ISMS クラウドセキュリティ認証 (ISO27017) を取得していること。
 - ㊼ ISMAP に登録されていること。
- ③ モバイル端末管理 (MDM) システム要件
モバイル端末管理 (MDM) システムには、AssetView Cloud を導入すること。
- (5) オンプレミスサーバー要件 (上野原市庁舎に配備)
- ① Active Directory システム要件
 - ア サーバーは Windows Server 2022/2025、クライアント OS は Windows11 環境で動作する環境

を提供すること。

イ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。
ウ ディレクトリサービスを提供すると共に、DNS サービスについても提供できるようにすること。

エ 時刻同期サービスを稼働させること。

オ 2台正副構成（仮想サーバー2台）で冗長化し、片側に障害が発生してももう一方でサービスを継続して提供できるようにすること。

カ ドメインは新規作成ではなく、現行ドメインの移行を行うこと。

キ ネットワーク構成変更に伴い、本市と協議の上グループポリシーを見直すこと。

ク 顔認証システム導入に伴い、ユーザー管理を見直すこと。

ケ DNS サービスの設定は現行のものを引き継ぐこと。

コ 移行前に必ずスキーマ拡張を行い、FSMOを新Active Directoryサーバーへ移行すること。
ドメイン及びフォレストの機能レベルを上げる必要がある場合は実施すること。

サ 本市と協議の上、固定プロファイルまたは移動プロファイルを利用すること。

シ フォルダのリダイレクトの設定をすること。

ス その他、移行作業に影響を及ぼす機能の設定変更及び切り替えがある場合は、本市と合意の上、作業を実施すること。

② Active Directory 連携用システム要件

ア サーバーはWindows Server 2022/2025、クライアントOSはWindows11環境で動作する環境を提供すること。

イ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。

ウ 認証システムと連携する専用コネクタ機能を構築すること。

③ WSUS システム要件

ア サーバーはWindows Server 2022/2025で動作する環境を提供すること。

イ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。

ウ WSUSサーバーの配信の設定は現行のものを引き継ぐこと。

エ ネットワーク構成変更に伴い、グループポリシーを見直すこと。

オ Windows Updateの管理を実施できること。

カ 自動設定配信をしないこと。

④ ファイル共有システム要件

ア サーバーはWindows Server 2022/2025、クライアントOSはWindows11環境で動作する環境を提供すること。

イ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。

ウ 現行ファイルサーバーの共有フォルダ・アクセス権を含めた全データを新規ファイルサーバーに移行すること。

エ 生徒・児童用ネットワークから接続できないよう制限すること。

オ スナップショットにて復元できる機能を有すること。

⑤ バックアップシステム要件

ア 機能要件

㊶ 物理サーバー（Windows）、仮想環境（Hyper-V）のバックアップに対応していること。

㊷ イメージベースのバックアップ（ディスク全体の保護）が可能であること。

㊸ バックアップ管理サーバーにてバックアップエージェントの増分バックアップと重複排除（リソース効率化）が可能であること。

㊹ バックアップ管理サーバーにてバックアップエージェントのバックアップスケジュールの柔軟な設定（時間、頻度、ポリシー）が可能であること。

- ㊸ バックアップエージェントの稼働状態（停止、稼働）に関係なくバックアップタスクを実行できること。
- ㊹ バックアップ管理サーバーからバックアップエージェントに対してリモート操作によるバックアップタスクの実行が可能であること。ファイル単位、フォルダ単位、ボリューム単位でのリストアが可能であること。
- ㊺ バックアップエージェントが稼働状態でもファイル単位でのリストアが可能であること。
- ㊻ ベアメタルリカバリ（BMR）によるシステム全体の復旧が可能であること。
- ㊼ バックアップエージェントのバックアップイメージをローカルディスク、NAS、SANへバックアップ可能であること。
- ㊽ データ保持ポリシー（世代管理、保持期間）の設定が可能であること。

イ 運用・管理要件

- ㊾ Webベースの管理コンソールによるバックアップエージェントの集中管理が可能であること。
- ㊿ Webベースの管理コンソールを用いてバックアップエージェントのバックアップの進捗状況の照会、実施結果、バックアップ実行時のログの照会が可能であること。
- ㋀ ジョブのステータス、履歴、エラーのレポート機能を備えていること。

ウ 非機能要件

- ㋁ バックアップ管理サーバーからバックアップエージェントに対してバックアップモジュールのリモートインストールを行えること。
- ㋂ 日本語対応の管理画面をサポートしていること。

⑥ 統合 ID 管理システム要件

ア ID 管理要件

- ㋃ サーバーは Windows Server 2022/2025、クライアント OS は Windows11 環境で動作する環境を提供すること。
- ㋄ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。
- ㋅ 人事異動時に必要となる組織、ユーザー情報を事前に登録でき、指定した日時に反映できる機能を有すること
- ㋆ Excel 形式 (xlsx) による組織・ユーザー情報のデータインポート、エクスポート機能を有すること。
- ㋇ 作成したルールに沿って、組織、ユーザー情報の属性情報を変更できること。
- ㋈ データの加工（文字列の結合、分割、ローマ字変換、ひらがな変換等）が行える機能を有すること。
- ㋉ ID 連携の作業を自動化できる機能を有すること。また、実行結果をメールで通知する機能を有すること。
- ㋊ ルールの定義は GUI の管理コンソール上から設定でき、職員でメンテナンスできる UI であること。
- ㋋ 操作ログを記録する機能を有し、ログを出力する機能を有すること。操作ログは DB に保存し、期間、ログイン ID、氏名等で検索できること。また、設定前、設定後の各属性の内容が検索結果から確認できること。

イ ID 連携要件

- ㋌ Active Directory の OU・グループ・ユーザー情報の追加・変更・削除を容易に管理者で行えるソフトウェアの提供を行うこと。
- ㋍ 人事異動時に必要となる OU・グループ、ユーザー情報を事前に登録でき、指定した日時に各システムに反映できること。

- ㉞ Active Directory へ反映時にアクセス権の猶予期間を設定できる機能を有していること。猶予期間中は、ファイルサーバー上の異動前の部署と移動後の部署のフォルダにアクセス可能な状態に設定すること。
- ㉟ 作成したルールに沿って、グループ、ユーザー情報の属性情報を変更できること。
- ㊀ CSV ファイル/Excel ファイルによるグループ・ユーザー情報の追加・変更・削除ができること。
- ㊁ Active Directory の OU・グループの階層構造をツリー表示できること。
- ㊂ Active Directory の OU・グループをマウスのドラックアンドドロップ操作で変更できること。
- ㊃ ユーザーの作成、削除、更新した内容がログに保存されること。更新した場合は変更前、変更後の設定値が表示される画面を提供すること。
- ㊄ AD 内のユーザ・セキュリティグループ・OU のプロパティ情報を CSV、または xlsx 形式で出力できることが望ましい。

㊅

ウ その他非機能要件

- ㊆ 公共団体で 5 年以上の導入実績があるパッケージ製品を選定すること。
- ㊇ 6,000 件以上のユーザーカウントを処理した実績を有する製品を選定すること。
- ㊈ 大規模人事異動でも夜間で処理が完了できる性能を有すること（数時間での処理）。
- ㊉ 導入するパッケージの製造元については ISO9001、ISMS27001 の認証を取得されている企業であること。
- ㊊ 年度更新等においては大量の人事異動処理が想定され不測の事態においても適切な運用を実施するため、導入するパッケージメーカーのサポートについては、電話やメールでのサポートが可能であること。

⑦ 校務用多要素認証システム要件

ア 構成要件

- ㊋ サーバーは Windows Server 2022/2025、クライアント OS は Windows11 環境で動作する環境を提供すること。
- ㊌ 定期的にバックアップを取得し、障害発生時はバックアップデータからリカバリできること。
- ㊍ 認証/設定管理サーバーは、生体情報に基づき認証を行うこと。
- ㊎ 既存の Active Directory に変更を加えないこと。（ソフトウェア等をインストールしたり、認証情報を保存したりしないこと。）
- ㊏ 異なるドメイン環境においても、ドメイン間で認証情報を共有することなく、認証/設定管理サーバーで一元管理ができること。
- ㊐ 認証/設定管理サーバーは、ユーザーの属性や Windows 認証のための情報、アプリケーション権限、暗号鍵、アプリケーション認証用パスワード、クライアント設定情報等を管理、格納できること。
- ㊑ 認証/設定管理サーバーは、クライアント端末にインストールするクライアントモジュールの設定情報を管理し、ネットワーク経由で自動的にクライアントモジュールの更新インストール作業を行う機能を有すること。
- ㊒ 認証/設定管理サーバーは、冗長化及び負荷分散構成が可能であること。
- ㊓ 認証/設定管理サーバーに対して、ユーザー情報、生体認証情報、クライアントモジュール設定情報等を、登録/変更/削除する専用の管理コンソールを有すること。
- ㊔ 管理コンソールは、複数インストールが可能であること。また管理コンソールにログインするユーザーの権限に応じた操作制限が可能であること。
- ㊕ 管理コンソールは、リモートデスクトップ接続での利用が可能であること。

- ㉔ 管理コンソールの操作ログや、クライアント端末から送信されたログを受信し、CSV、syslog、SQL サーバーに出力できること。
- ㉕ 出力されたログを閲覧・検索できる機能を標準で有すること。
- ㉖ クライアント端末は、生体情報を使った二要素によるログイン認証がおこなえること。
- ㉗ ネットワークに繋がっていない環境においても暗号化された期限付きキャッシュ設定により、セキュリティの適用された利用環境を提供する機能を有すること。
- ㉘ 認証サーバーに接続不可の環境でキャッシュによるログイン認証をする際に、指定した回数認証に失敗した場合、キャッシュをロックアウトする機能を有すること。
- ㉙ 顔認証の機能を有し、利用を必須とすること。
- ㉚ 外付けのカメラ (USB2.0 以上の DirectShow 9.0 に対応し、640x480 以上の解像度)、またはコンピュータ内蔵カメラが使用できること。
- ㉛ カメラを複数台利用していても、顔認証時に利用するカメラの切り替えができる機能を有すること。
- ㉜ 代理入力の機能を有すること。

イ データ保全要件

- ㉝ 認証／設定管理サーバーに格納されるパスワード情報、生体認証情報は暗号化されていること。
- ㉞ 認証／設定管理サーバーとクライアント端末間において、通信を暗号化するか否か選択できること。
- ㉟ 認証／設定管理サーバーに格納される生体情報は、生体画像から特徴点を抽出してデータ化・暗号化した状態で格納され、データからの生体画像の復元は不可能であること。

ウ 導入支援要件

- ㊱ ユーザー情報を CSV ファイルで、認証／設定管理サーバーにインポートするツールを有すること。
- ㊲ 画像データから顔認証情報を一括登録できる機能を有すること。
- ㊳ 画像データから登録された認証情報を利用する場合、初回認証時に使用した現在の顔を認証情報として、サーバーに自動更新されること。
- ㊴ ユーザーが利用している Windows パスワードを管理者が知らなくとも、ユーザーによる初回ログオン時に、Windows パスワードの入力を求め、Windows パスワードをユーザー情報として認証／設定管理サーバーに登録できること。
- ㊵ クライアント端末に認証ソフト導入後、初回ログオン時に生体情報の登録が行えること。
- ㊶ ユーザーが利用する端末から生体情報の登録が可能なこと。かつ、生体情報の登録はユーザーの操作で完結すること。
- ㊷ サイレント・インストールパラメーターが用意されていること。
- ㊸ インストールモジュール内にレジストリファイルを配置してインストールを行うと、そのレジストリを適応できる機能を有すること。

エ 運用管理要件

- ㊹ 管理コンソールを操作する管理者を、管理者用の生体情報、またはパスワードで認証する機能を有すること。(ランタイムが対応している OS のみ)。
- ㊺ 人事異動時等に変更情報を CSV ファイルでインポートすることで、各ユーザー権限の一括変更処理が行えること。
- ㊻ 顔認証成功時に定期的に認証／設定管理サーバーに格納されている顔認証情報を自動更新する機能を有すること。
- ㊼ 生体情報の有効化・無効化が設定できること。
- ㊽ 管理者により認証用パスワードのロック回数、変更ポリシー (複雑性、文字数、変更履歴)

管理や変更履歴管理が行えること。また期限が切れる前に変更を催促する機能を有し、ユーザーによるパスワードの変更が可能であること。

- ㉔ 何らかの事情により、Windows ドメインのパスワードと生体情報に関連付けされている Windows パスワードに相違が生じた場合、再登録する画面を表示することができること。
- ㉕ 自動的に Windows パスワードを生成・変更する機能を有すること。
- ㉖ 管理コンソールを操作できる管理者権限をロールとして分類して、管理権限を委譲、分散できる機能を有すること。
- ㉗ 管理コンソールの操作をログとして記録できること。
- ㉘ 認証/設定管理サーバーの OU 毎にセキュリティ設定情報等を設定、変更し、運用が可能なこと。
- ㉙ クライアントモジュールがアップデートされていることを検知し、自動的に更新する機能を有すること。また、この自動更新はスケジュール（更新期日）設定が可能なこと。
- ㉚ ユーザーに変更権限が与えられた情報（パスワード等）をユーザーが変更した場合、クライアント端末から認証/設定管理サーバーにアップロードを行い、常に認証/設定管理サーバーに最新の情報を格納する機能を有すること。

オ クライアント機能要件

- ㉛ ユーザーは生体認証成功後、認証/設定管理サーバーからダウンロードされた設定情報により Windows 認証を自動で行うことができること。
- ㉜ 顔認証成功/失敗時の画像を保存する機能を有すること。また、保存する画像は暗号化されていること。
- ㉝ 写真等によるなりすまし対策の機能を有すること。（首振り、うなずき、瞬き、笑顔等顔の動きをチェックする機能を有すること）
- ㉞ ログオン画面の画像を任意の画像に変更できること。
- ㉟ ログオン時に必要な認証情報を、次のパターン以上の方式から選択可能であること。
 - a 生体情報+校務用多要素認証システム アカウント
 - b 生体情報+校務用多要素認証システム アカウント/パスワード
 - c 生体情報+校務用多要素認証システム アカウント+Windows アカウント/パスワード
 - d Windows アカウント/パスワード
- ㊱ ただし㉟の場合、二要素認証システムとしてはユーザーを特定できないため、ユーザー毎の操作制御やシングルサインオンは利用できなくてよいが、端末毎に設定された操作制御機能が有効となること。
- ㊲ ㉟でのログオンを許可した場合でも、Windows アカウント/パスワード手入力によるログオンが行える期限を設けることができ、その期限を過ぎた後は生体認証を用いた二要素認証を強制できること。
- ㊳ 生体認証情報の登録・認証前は、Windows アカウント/パスワード手入力によるログオンが行えるように設定できること。
- ㊴ ユーザーに対して複数の Windows アカウントを割り当てることが可能であり、認証成功時に Windows アカウントを選択することができること。
- ㊵ 管理コンソールの操作により、校務系パソコンメンテナンス時等に一時的に利用させる管理者権限の付与、解除等の適宜変更が可能であること。
- ㊶ オフライン時に校務系パソコンログオン認証が失敗した際に、認証画面を再度表示させるのを遅らせる機能を有すること。
- ㊷ ログオン認証・ロック解除認証時に、メッセージを表示し、原因を特定できる機能を有すること。また本メッセージは簡略することにより、特定できないよう切り替えることができること。
- ㊸ クライアントがロックされた時間から、設定された時間が経過すると自動的にログオフまた

ワーク、システムの状態が正常または異常であることを確認できること。

- ㊤ Web 管理ページ上で、ファームウェアに内蔵されたマニュアルを参照できること。
- ㊦ 購入済のライセンスは、お客様の操作にてクラウドサービスより発行およびダウンロードができること。

イ ソフトウェア要件

- ㊶ RADIUS (Remote Authentication Dial In User Service) 機能を有し、ネットワーク機器等と連携し、認証システムを実現できること。
- ㊷ 認証方式として、PAP CHAP MS-CHAP MS-CHAPv2 EAP-MD5 EAP-TLS EAP-TTLS (PAP/CHAP/MSCHAP/MSCHAPv2/EAP-TLS/EAP-MSCHAPv2) EAP-PEAP (MS-CHAPv2/GTC/TLS) に対応すること。
- ㊸ Windows11 24H2 で WPA3-Enterprise192 ビットモードを使用した EAP-TLS 認証が可能であること。
- ㊹ 認証に用いるアカウントは 200 以上登録できること。
- ㊺ 認証アカウント毎に最終認証成功日時を記録できること。記録した日時の情報は検索条件として利用でき、その結果は CSV ファイルとしてエクスポートできること。
- ㊻ パスワードの有効期限、およびパスワードの変更禁止期間を設定できること。
- ㊼ 利用者パスワードの期限切れと期限切れリマインダーを、管理者および利用者宛にメール通知できること。
- ㊽ 期限切れ通知の場合、アプライアンス上で期限切れが確認された際にメール通知すること。
- ㊾ 期限切れリマインダーの場合、何日前（当日、1 週間前、10 日前、30 日前）に通知するかを指定できること。また、1 度だけの通知か毎日通知かを選択できること。
- ㊿ 利用者ページにログインした際に、パスワード有効期限切れまでの日数がしきい値以下であれば、警告メッセージが表示される機能を有すること。
- ㊽㉿ 認証に用いるアカウント、連携する認証ネットワーク機器はグループで管理できること。また両グループの組合せにより認証の結果を制御できること。
- ㊽㊰ 認証連続失敗によりアカウントロックができること。アカウントロックに至る失敗回数、連続失敗カウントのリセットやロックの解除までの秒数は管理者により指定できること。
- ㊽㊱ 同一アカウントによる多重ログオンの有無や、曜日と時間帯の組合せ、任意のチェックアイテムにより認証の成否を制御できること。
- ㊽㊲ アカウントは機器内のデータベースに登録するほか、外部の認証・データベースサーバーの情報を利用できること。外部データベースとして、LDAP (Lightweight Directory Access Protocol) データベース、及び RADIUS 認証サーバーを想定する。
- ㊽㊳ ゲストユーザーアカウント登録機能を持つこと。
- ㊽㊴ 利用者にゲストユーザーアカウントの登録申請をさせる機能を持つこと。
- ㊽㊵ 事前承認用コードを用いて利用者によるゲストユーザー申請を事前に許可する機能を持つこと。事前承認用コードの有効期限を日数および時刻で設定でき、有効期限切れの事前承認用コードを自動的に削除する機能を持つこと。
- ㊽㊶ ユーザーによるゲストユーザーアカウントの代理登録が可能であり、代理登録が可能なユーザーは、ゲスト管理権限を持つユーザーまたは正規ユーザーから選択できること。
- ㊽㊷ ゲストユーザーアカウントの有効期限を日数および時刻で設定でき、有効期限切れのゲストユーザーアカウントを自動的に削除する機能を持つこと。
- ㊽㊸ ゲストユーザーアカウント登録完了通知を利用者のメールアドレスに送信可能なこと。
- ㊽㊹ ゲストユーザー申請時に入力させる利用者情報を管理者が設定できること。
- ㊽㊺ 認証連続失敗によりゲストユーザーアカウントのロックができること。アカウントロックに至る失敗回数、ロックの解除までの秒数は管理者により指定できること。

- ㉔ ゲストユーザーはゲストユーザー用グループに所属することができ、ゲストユーザー用 RADIUS アトリビュートを返すことができること。
- ㉕ ネットワーク機器と連携し、MAC アドレス認証を行う機能を有すること。管理可能な MAC アドレス情報は利用者ライセンス数の 10 倍であること。
- ㉖ ネットワーク機器と連携し、MAC アドレス認証 (PAP/CHAP) を行う機能を有すること。
- ㉗ MAC アドレス情報は複数の認証サーバー間で共有できること。情報の複製は手動のほか、任意間隔を指定した自動複製ができること。
- ㉘ MAC アドレス認証の失敗を確認した場合、認証に失敗した端末が接続されているネットワーク機器のネットワークインタフェースに対して SNMP にてシャットダウンを指示できること。
- ㉙ ローカルデータベースのユーザーに対して、MAC アドレス管理者としてのロールを付与できること。
- ㉚ 利用者による MAC アドレスの申請ができること。承認は、事前承認用コードによる事前承認と自動承認ができること。
- ㉛ 事前承認用コードの有効期限を日数および時刻で設定でき、有効期限切れの事前承認用コードを自動的に削除する機能を持つこと。
- ㉜ ローカルデータベースのユーザーによる MAC アドレスの代理登録ができること。
- ㉝ 代理登録が可能なユーザーは、MAC アドレス管理者権限を持つユーザー、または正規ユーザーから選択できること。
- ㉞ MAC アドレス申請時に入力させる利用者情報を管理者が設定できること。
- ㉟ MAC アドレス登録完了通知を利用者のメールアドレスに送信できること。
- ㊀ RADIUS 認証時に MAC アドレスの自動収集ができること。
- ㊁ MAC アドレス申請ページや代理登録ページを提供する LAN インタフェースを設定できること。
- ㊂ システム管理者が、申請・収集した MAC アドレス、事前承認用コードの一覧を確認できること。
- ㊃ MAC アドレス毎に最終認証成功日時を記録できること。その結果は CSV ファイルとしてエクスポートできること。
- ㊄ ダッシュボードの画面から、本登録待ちの MAC アドレス件数を確認できること。
- ㊅ 複数台の構成にて利用者情報を他の RADIUS サーバーに複製する機能を持ち、複製先として動作すること。また、複製元の特定の利用者グループに所属する利用者情報のみ複製する機能を有すること。
- ㊆ 複製された利用者情報を参照して認証を行えること。
- ㊇ アカウントを登録する外部のデータベースとして、クライアント証明書認証を使用した外部 LDAPS サービスを利用できること。
- ㊈ アカウントを登録する外部のデータベースへ LDAPS 接続する際に SNI (Server Name Indication) に対応しており、一つのサーバーで複数のドメイン名を使用している環境でも利用可能であること。
- ㊉ EAP 認証時の TLS プロトコルとして TLS 1.3 をサポートすること。
- ㊊ RADIUS 認証成功/失敗時に出力するログに、NAS-Identifier 属性、NAS-IP-Address 属性、送信元 IP アドレスを出力可能であること。また、EAP-TLS 認証成功時には、クライアント証明書のサブジェクトとシリアル番号が出力されること。
- ㊋ EAP-TLS 認証成功ログに、クライアント証明書のサブジェクトとシリアル番号を出力可能であること。
- ㊌ 全ての LAN ポートで RADIUS サービスを有効に出来ること。

ウ 管理運用機能要件

- ㊍ 登録アカウントの管理は個別のほか、CSV ファイルからの一括登録・変更・削除ができるこ

と。

- ① 証明書の管理は個別のほか、CSV ファイルインポートによる証明書一括失効/一時停止、証明書の一括解除ができること。
- ② 利用者ページでユーザー自らパスワードの変更ができること。
- ③ Web 管理画面からの平易な操作により設定の保存（バックアップ）と復元（リストア）が可能であること。設定の保存は手動のほか、外部サーバーへの自動保存が指定できること。
- ④ NTP（Network Time Protocol）クライアント、SNMP（Simple Network Management Protocol）エージェント機能を有すること。
- ⑤ システムや RADIUS、CA サービスのログを記録できること。ログの記録先は内部のみ、もしくは内部に加え外部とする設定のいずれかより指定可能で、外部 Syslog サーバーへのログ出力は UDP、TCP どちらにも対応すること。
- ⑥ Web 管理画面からネットワーク通信状況の確認が可能であること。使用するネットワークコマンドとして、ping、traceroute、nslookup、dig、packet capture を想定する。
- ⑦ 管理用コンピュータと直接コンソール接続することで、システム情報表示、設定の初期化、システムの停止、及びアクセス制御の無効化ができること。
- ⑧ Web 管理画面は Google Chrome もしくは Microsoft Edge の Web ブラウザを使って操作できること。
- ⑨ ダッシュボードの画面からライセンスの利用状況および認証失敗状況を確認できること。
- ⑩ 初期構築をサポートするために、初期設定ウィザードを用いて、システム及びサービスの初期設定ができること。
- ⑪ モニタリング機能を有し、RADIUS システムの項目ごとにチャート等視覚的な情報を用いて状況を確認できること。
- ⑫ 本サーバー自身の設置先や用途等を把握するために、機器毎にニックネームを設定し、Web 管理画面より確認できること。
- ⑬ 設定をサポートするために、設定画面上に配置されたボタンを選択することでヘルプを表示する機能を有すること。
- ⑭ 設定をサポートするために、初期設定ウィザードによる設定後に行う主な設定や管理のタイトルメニューが表示できること。また、カテゴリ および フィルタリング の項目をチェックすることにより両方に該当するタイトルメニューのみを絞り込み表示できること。
- ⑮ クラウドサービスと連携することにより、クラウドの管理コンソールからバックアップ・リストアやファームウェアアップデート、停止・再起動、ログ閲覧等を行えること。
- ⑯ 無停電電源装置と連携し、USB 接続または SSH 接続によるシャットダウンに対応すること。仮想版の場合は SSH 接続によるシャットダウンのみ対応すること。
- ⑰ 旧モデルから新モデルへの設定情報の引継ぎが可能であること。
- ⑱ 認証局（CA）および発行済の証明書情報を引継ぎ、旧モデルで発行済の証明書はそのまま利用可能となること。
- ⑲ 設定引継ぎのためのマニュアルおよび設定のチェックシートを用意していること。
- ⑳ 設定の引継ぎはバックアップデータのリストアにより自動で行われること。ただし、一部の設定は手動による設定変更が発生することを許容すること。
- ㉑ アクセスログのリクエストヘッダに X-Forwarded-For が記録されること。

エ システムセキュリティ要件

- ㉒ 2 台以上の機器による冗長構成に対応すること。
- ㉓ ネットワーク認証サーバーへの通信に対し、機器インタフェース、プロトコル、送信先・送信元ネットワーク情報（IP アドレス、サブネットマスク、ポート番号）の組合せにより、許可・拒否等の制御ができること。

- ㊸ 利用者向けのサービスページにて、第三者から製品の特定につながるコピーライト表記を非表示にするためにフッタを非表示にできること。
 - ㊹ BlastRADIUS 対策のため、初期設定状態で RADIUS 応答パケットで常に Message-Authenticator 属性を応答できること。
 - ㊺ 冗長構成時のノード間相互監視によるメール通知ができること。
- ⑨ ネットワーク監視システム要件
- ア クラウド上で管理対象機器の統合管理が可能なサービスであること。また、1 グループあたり 2,000 台まで管理できること。
 - イ 管理サービスのすべての機能が GUI で提供され、日本語表示に対応していること。
 - ウ 管理者のアクセス権限が設定できること。(閲覧のみで設定変更不可等)
 - エ 管理対象機器のイベントログをクラウド上に保存し、検索できること。また、過去 30 日分のイベントログを保存できること。
 - オ アラーム発生時に管理者に E メールによる通知ができること。
 - カ トラフィックの情報は、90 日間全ポートで確認できること。またアプリごとに通信量の確認ができること。
 - キ アプリケーションごとに帯域制御ができること。
 - ク CPU 使用率、メモリ使用率、温度の情報を過去 90 日間さかのぼって確認できること。
 - ケ アラームを過去 365 日分さかのぼって確認出来ること。
 - コ トラフィック情報を CSV 形式でダウンロードできること。
 - サ コンフィグを毎週自動で保存する機能を有すること。
 - シ イベントログを管理する機能を有すること。
 - セ コンフィグを一括切替え出来る機能を有すること。
 - ソ コマンドによる一括設定が出来る機能を有すること。

4 調達対象ハードウェア・ソフトウェア

(1) ハードウェア/ソフトウェア

次の要求仕様を満たすこと。

① 上野原市庁舎用ルーター

項目	詳細	仕様
用途	使用用途	10G インターネット接続用ルーター
本体メーカー	型番	NEC IX2310 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること。
	動作条件	温度 0~50℃ 湿度 90%以下 (結露しないこと)
性能	基本性能	基本性能 10.0Gbps 以上であること。
	VPN 性能	(a) IPsec 性能 3.5Gbps 以上であること。 (b) IPsec 最大対地数 256 以上であること。
構成	インタフェース	(a) 100/1000/2.5G/5G/10GBASE-T を 2 ポート以上有すること。 (b) 10/100/1000BASE-T を 4 ポート以上有すること。
機能	セッション	65,535 以上のセッションに対応可能であること。
	VLAN	ポートベース VLAN、タグ VLAN (IEEE802.1Q)
	ルーティング	IPv4: BGP4、ポリシールーティング、スタティックルーティング

項目	詳細	仕様
		IPv6: ポリシールーティング、スタティックルーティング
	ファイアウォール	MAC フレームフィルタリング、IP パケットフィルタリング
	QoS	送信優先制御 (PQ、CBQ)、帯域制御 (Traffic Shaping)
	トンネル	IPv4 over IPv6、IPv4 over IPv4、GRE、L2TP (LNS) over IPsec (IPv4)、MAP-E、 IPv6 標準プロビジョニング方式 (DS-Lite, IPIP)
	冗長構成	IPv4: VRRPv2, ネットワークモニタ、リンクアグリゲーション IPv6: ネットワークモニタ、リンクアグリゲーション
	運用管理	syslog、SSH、telnet、SCP、HTTP/HTTPS
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 55W 以下であること

② 上野原市庁舎用 L3 スイッチ

項目	詳細	仕様
用途	使用用途	各サーバー・ネットワーク機器を収容するスイッチ
本体メーカー	型番	NEC QX-S5628GT-4X2Q 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0~45℃ 湿度 10~90% (結露しないこと)
性能	基本性能	(a) スイッチング容量 296Gbps 以上であること (b) 最大転送性能 180.0Mpps 以上であること (c) 登録 MAC アドレス数が 48,000 以上であること (d) 最大 VLAN 数が 4,094 以上であること
構成	インタフェース	(a) 10/100/1000BASE-T×24 ポート以上 (b) 1000/10GBASE-X (SFP/SFP+スロット) ×4 ポート以上
機能	VLAN	ポート VLAN、Tag VLAN (IEEE802.1Q)
	スパンニングツリー	STP (IEEE802.1D)、RSTP (IEEE802.1w)、MSTP (IEEE802.1s)
	ルーティング	スタティックルーティング、RIP (v1/v2/ng)、OSPF (v2/v3)
	セキュリティ	パケットフィルタリング、IEEE802.1X、MAC アドレス認証
	QoS	Line Rate、Committed Access Rate、Generic Traffic Shaping、QoS クラス数 8 以上
	信頼性	リンクアグリゲーション (LACP 対応)、 ストーム抑制、スタック機能
電源	運用管理	SNMP、syslog、SSH、telnet、ポートミラーリング、NTP (クライアント、サーバー)、RMON、sFlow
	電源電圧	AC100V で動作すること
	消費電力	最大で 100W 以下であること

③ 上野原市庁舎用ファイアウォール

項目	詳細	仕様
用途	使用用途	各学校との接続に利用
本体メーカー	型番	FortiGate-201F または FortiGate-201G 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0～40℃ 湿度 20～90% (結露しないこと)
システム性能	一般	(a) ファイアウォールスループット 27/27/11 (1518/512/64 バイト UDP パケット) 以上であること (b) ファイアウォールスループット (パケット / 秒) 16.5 Mpps 以上であること (c) ファイアウォール同時セッション (TCP) 3 M 以上であること (d) ファイアウォール新規セッション / 秒 (TCP) 280,000 以上であること (e) ファイアウォールポリシー10,000 以上設定できること (f) アプリケーション制御スループット (HTTP 64 K) 13 Gbps 以上であること
構成	インタフェースとモジュール	(a) 1000BASE-T×8 ポート以上 (b) USB インタフェース×1 以上 (c) シリアル管理コンソールインタフェース×1 以上 (d) 内蔵ストレージ 1×480GB SSD 以上
機能	ポリシー定義	送信元 I/F、送信元アドレス、宛先 I/F、宛先アドレス、アクション (accept、Deny)、スケジュール、サービス、ログの対象、NAT 有効、無効といった項目を指定し、ポリシー設定ができること
	GUI	Web GUI を利用して、設定、状態確認、ログ確認、バックアップ、リストアといった操作が行えること
	オブジェクト	アドレス、アドレスグループ、サービス、サービスグループの設定ができ、ポリシーの定義に利用できること
	運用管理	SNMP、syslog、SSH、HTTPS
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 180W 以下であること

④ 上野原市庁舎用 L2 スイッチ

項目	詳細	仕様
用途	使用用途	仮想化基盤・各サーバー・ネットワーク機器を収容するスイッチ。各機器との接続を冗長化するために 2 台で構成
本体メーカー	型番	NEC QX-S5124GT-4X 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0～45℃ 湿度 10～90% (結露しないこと)
性能	基本性能	(a) スイッチング容量 128Gbps 以上であること (b) 最大転送性能 95.2Mpps 以上であること (c) 登録 MAC アドレス数が 16,000 以上であること

項目	詳細	仕様
		(d) 最大 VLAN 数が 4,094 以上であること
構成	インタフェース	(a) 10/100/1000BASE-T×24 ポート以上 (b) SFP+10G スロット×4 ポート以上 上記ポート構成のスイッチを 2 台
機能	VLAN	ポート VLAN
	スパンニングツリー	STP (IEEE802.1D) , RSTP (IEEE802.1w) , MSTP (IEEE802.1s)
	セキュリティ	IEEE802.1X、MAC アドレス認証
	QoS	Line Rate、Committed Access Rate、Generic Traffic Shaping、QoS クラス数 8 以上
	運用管理	NTP クライアント、SNMP、syslog、SSH、telnet、RMON、ポートミラーリング
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 28W 以下であること

⑤ 上野原市庁舎用メディアコンバータ

項目	詳細	仕様
用途	使用用途	ファイアウォールの 1000BASE-T インタフェースを光インタフェースに変換し特定の学校内の接続に使用する
本体仕様	外形	サブラックオプションを使用し、庁舎に設置する 12 台のメディアコンバータを 19 インチラックに搭載可能であること
	動作条件	温度-10～55℃ 湿度 95%RH 以下（結露しないこと）
FX ポート	準拠規格	IEEE802.3Z 1000BASE-SX
	伝送速度	1000Mbps
	インタフェース	SC コネクタ (JIS C 5973 F04 型)
	発光中心波長	1260～1360nm
	受光波長	1480～1580nm
	伝送距離 (目安)	2m～25km の製品×8 対 15～50km の製品×3 対
TX ポート	準拠規格	IEEE802.3Z 1000BASE-X
	伝送速度	1000Mbps
	適合コネクタ	RJ-45 コネクタ
	最大伝送距離	100m
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 10W 以下であること

⑥ 上野原市庁舎用仮想化基盤サーバー

項目	詳細	仕様
用途	使用用途	仮想化基盤として機能し、仮想サーバーを稼働させる
本体メーカー	型番	Lenovo ThinkSystem SR630 v4 相当以上の性能を有する製品であること
本体仕様	外形	2U 以内であり 19 インチラックに搭載できること

項目	詳細	仕様
		※後述のラックに搭載すること
	監視	ハードウェア故障時に電子メール通報方式で障害内容を通知できる機能を有すること。
構成	CPU	Intel Xeon 6520P (2.4GHz/24コア) 相当以上の性能を有するCPUを2基以上搭載していること
	メインメモリ	(a) 256GB以上搭載していること (b) すべて同一型番のメモリであること
	SSD	(a) RAID5相当以上の構成であること (b) RAID構成後の実効容量が600GB以上であること (c) RAID0/1/5/6/10/50/60に対応したキャッシュ4GB以上のRAIDコントローラを搭載すること (d) RAIDをフラッシュバックアップユニットで保護すること (e) RAIDでSSDを冗長化すること (f) ホットスワップに対応すること
	光ディスクドライブ	内蔵型ディスクドライブを搭載有無は不問とするが、搭載しない場合は、外付けUSB DVD-RWドライブを本調達内で1機用意すること
	インタフェース	(a) 1GBase-T×4ポート以上 (b) 管理用LANポート×1ポート以上 (c) Fiber Channel (32Gbps) ×外部接続2ポート以上 ※後述の仮想基盤サーバー用ストレージへ接続すること ※管理用LANポート以外のインタフェースはOS標準機能を用いて冗長構成(チーミング設定)を行うこと
	ディスプレイ出力	コンソールユニット(N8143-144 18.5型LCDコンソールユニット(8Server))または相当以上の製品を準備し接続すること。なお、上野原市庁舎用バックアップ兼電源管理サーバーと切り替えての利用も可能とする。
電源	電源電圧	AC100Vで動作すること
	消費電力	最大で1300W以下であること
環境条件	温度条件	動作時は10~35℃で動作可能であること -40~60℃で保管可能であること
	湿度条件	稼働時: 8~80%、保管時: 8~90% 動作時/保管時ともに結露しないこと
ソフトウェア	仮想化基盤用OS	Microsoft Windows Server 2022 或いは Microsoft Windows Server 2025
	クラスタソフトウェア	Windows Server Failover Clustering (WSFC)、相当以上の性能を有する製品であること
	仮想サーバー一覧	(a) Active Directoryサーバー (b) Active Directory 連携用サーバー (c) WSUSサーバー (d) ファイルサーバー (e) 認証基盤サーバー

項目	詳細	仕様
		(f) 統合 ID 管理サーバー (g) 校務用多要素認証サーバー (h) 校務系ネットワーク認証サーバー

⑦ 上野原市庁舎用無停電電源装置（仮想化基盤サーバー用）

項目	詳細	仕様
無停電電源装置	用途	バックアップサーバーに電源を供給する
	メーカー	NEC N8142-101 無停電電源装置（1500VA）または相当以上の性能を有する製品であること
	外形	2U 以内であり 19 インチラックに搭載できること
	出力電力容量	使用最大容量 1500VA 以上であること
	入力電圧	100V で動作すること
	電源供給方式	常時商用（ラインインタラクティブ）
	出力プラグ	並行 2 極アース付き（NEMA 5-15R）6 口
	ハードウェア接続	SNMP カード経由で、ハードウェア機器と接続すること
	障害発生時の動作	無停電電源装置より給電されたハードウェア機器は、電源管理ソフトウェアにより、自動起動、自動停止のスケジューリング設定を行い、システムの構成に応じて適切な起動順序、停止順序設定を行うこと
	環境条件	室内温度 10℃～35℃、湿度 45%～70%で動作可能なこと
LAN ケーブル等	必要となる LAN ケーブルや電源ケーブルを手配すること	

⑧ 上野原市庁舎用仮想化ストレージ

項目	詳細	仕様
用途	使用用途	仮想化基盤として機能し、仮想サーバーを稼働するためのディスクリソースとして使用
本体仕様	外形	4U 以内であり 19 インチラックに搭載できること
	型番	IBM Storage FlashSystem 5045 または、相当以上の性能を有する製品であること
構成	コントローラ	コントローラが冗長されていること
	メインメモリ	(a) 装置あたり 32GB 以上搭載していること (b) 停電時、キャッシュデータを無制限に保持できること
	HDD	(a) 実効容量が 20TB 以上であること (b) ホットスペア用 HDD を 1 台以上搭載すること (c) RAID6 で HDD を冗長化すること (d) ホットスワップに対応すること (e) 容量拡張の際、追加ライセンスが必要ないこと
	インターフェース	装置あたり Fiber Channel（16Gbps）×4 ポート以上 ※前述の仮想化基盤サーバーへ接続すること
電源	電源電圧	AC100V で動作すること

項目	詳細	仕様
	消費電力	最大で 800W 以下であること
環境条件	温度条件	動作時は 10～35℃で動作可能であること -40～60℃で保管可能であること
	湿度条件	稼働時：20%～80%、保管時：5～100% 動作時/保管時ともに結露しないこと

⑨ 上野原市庁舎用バックアップ兼電源管理サーバー

項目	詳細	仕様
用途	使用用途	仮想化基盤上の仮想サーバーのバックアップを取得する その他ソフトウェアの管理機能を有する
本体メーカー	型番	Lenovo ThinkSystem SR650 V4 または、相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載できること
	監視	ハードウェア故障時に電子メール通報方式で障害内容を通知できる機能を有すること。
構成	CPU	Intel Xeon 6505P (2.2GHz/12 コア) 相当以上の性能を有する CPU を 1 基以上搭載していること
	メインメモリ	(a) 128GB 以上搭載していること (b) すべて同一型番のメモリであること
	HDD	(a) RAID6 相当以上の構成であること (b) RAID 構成後の実効容量が 32TB 以上であること (c) RAID 0/1/5/6/10/50/60 に対応したキャッシュ 8GB 以上の RAID コントローラを搭載すること (d) RAID をフラッシュバックアップユニットで保護すること (e) RAID で HDD を冗長化すること (f) ホットスワップに対応すること (g) OS ブート領域については 480GB SSD で RAID1 構成とすること
	光ディスクドライブ	内蔵型ディスクドライブを搭載有無は不問とするが、搭載しない場合は、外付け USB DVD-RW ドライブを本調達内で 1 機用意すること
	インタフェース	(a) 1GBase-T ×4 ポート以上 (b) 管理用 LAN ポート×1 ポート以上 ※管理用 LAN ポート以外のインタフェースは OS 標準機能を用いて冗長構成（チーミング設定）を行うこと
	ディスプレイ出力	コンソールユニット（N8143-144 18.5 型 LCD コンソールユニット（8Server））または相当以上の製品を準備し接続すること。なお、上野原市庁舎用仮想化基盤サーバーと切り替えての利用も可能とする。
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 1300W 以下であること

項目	詳細	仕様
環境条件	温度条件	動作時は 10～25℃で動作可能であること -40～70℃で保管可能であること
	湿度条件	稼働時：-20～80%、保管時：8～90% 動作時/保管時ともに結露しないこと
ソフトウェア	バックアップサーバー用 OS	Microsoft Windows Server 2022 或いは Microsoft Windows Server 2025
	無停電電源装置管理	停電検知時、無停電電源装置に接続されている仮想化基盤サーバー2基とバックアップサーバーが自動でシャットダウンされること
	バックアップ	(a) 前述の仮想化基盤サーバー上で動作する仮想マシンを自動で定期的にバックアップすること (b) 必要に応じて仮想マシン全体・個別ファイルのリストアが可能なこと (c) 今後の仮想マシン追加でライセンス追加が不要なこと

⑩ 上野原市庁舎用無停電電源装置（バックアップ兼電源管理サーバー用）

項目	用途	仕様
無停電電源装置	用途	バックアップサーバーに電源を供給する
	メーカー	NEC N8142-101 無停電電源装置（1500VA）または相当以上の性能を有する製品であること
	外形	2U 以内であり 19 インチラックに搭載できること
	出力電力容量	使用最大容量 1500VA 以上であること
	入力電圧	100V で動作すること
	電源供給方式	常時商用（ラインインタラクティブ）
	出力プラグ	並行 2 極アース付き（NEMA 5-15R）6 口
	ハードウェア接続	SNMP カード経由で、ハードウェア機器と接続すること
	障害発生時の動作	無停電電源装置より給電されたハードウェア機器は、電源管理ソフトウェアにより、自動起動、自動停止のスケジューリング設定を行い、システムの構成に応じて適切な起動順序、停止順序設定を行うこと
環境条件	室内温度 10℃～35℃、湿度 45%～70%で動作可能なこと	
LAN ケーブル等		必要となる LAN ケーブルや電源ケーブルを手配すること

⑪ 上野原市庁舎用無線 LAN コントローラ

項目	詳細	仕様
用途	使用用途	無線 LAN アクセスポイントを集中管理する無線 LAN コントローラ。各機器との接続を冗長化するために 2 台で構成
本体メーカー	型番	NEC QX-W2310AC 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0～45℃ 湿度 10～90%（結露しないこと）

項目	詳細	仕様
性能	基本性能	(a) 最大スループットが 10Gbps 以上であること (b) 登録 MAC アドレス数が 7,500 以上であること (c) 最大 VLAN 数が 4,094 以上であること (d) 管理 AP 数が 384 以上であること (e) 管理クライアント数が 7680 以上であること
構成	インタフェース	(a) 10/100/1000BASE-T×8 ポート以上 (b) SFP スロット×8 ポート以上 上記ポート構成のコントローラを 2 台
機能	VLAN	VLAN
	スパニングツリー	STP (IEEE802.1D), RSTP (IEEE802.1w), MSTP (IEEE802.1s)
	セキュリティ	IEEE802.1X、MAC アドレス認証
	QoS	WMM
	運用管理	NTP クライアント、SNMP、syslog、SSH、telnet、RMON、ポートミラーリング
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 62W 以下であること

⑫ 上野原市庁舎用学習系プロキシ

項目	詳細	仕様
用途	使用用途	学習系端末へプロキシ機能を提供する
本体メーカー	型番	NEC InterSec/CS400n アプライアンスパック (S) または、相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載できること
	監視	故障の兆候を検出し、電子メール通報方式、ダイヤルアップ通報方式または HTTPS 通報方式で通知できる機能を有すること。
構成	メインメモリ	16GB 以上搭載していること
	HDD	(a) RAID1 相当以上の構成であること (b) RAID 構成後の実効容量が 300GB 以上であること (c) RAID で HDD を冗長化すること (d) ホットスワップに対応すること
	光ディスクドライブ	内蔵型ディスクドライブであり CD/DVD を読み込み可能であること
	インタフェース	(a) 1000BASE-T ×8 ポート以上 (b) 管理用 LAN ポート×1 ポート以上 ※管理用 LAN ポート以外のインタフェースは OS 標準機能を用いて冗長構成（チーミング設定）を行うこと
	ディスプレイ出力	コンソールユニット (N8143-142 18.5 型 LCD コンソールユニット (1Server)) または相当以上の製品を準備し接続すること
電源	電源電圧	AC100V で動作すること

項目	詳細	仕様
	消費電力	最大で 413W 以下であること
環境条件	温度条件	動作時は 10～35℃で動作可能であること -30～60℃で保管可能であること
	湿度条件	稼働時：8～90%、保管時：5～95% 動作時/保管時ともに結露しないこと
ソフトウェア	無停電電源装置管理	N8142-101 無停電電源装置（1500VA）（ラックマウント用）または相当以上の製品を準備し接続すること 停電検知時、自動でシャットダウンされること

⑬ 上野原市庁舎用管理パソコン

項目	詳細	仕様
用途	使用用途	各サーバーの管理に利用する
本体メーカー	型番	NEC M1P50/E-S・11Pro・Ci5 または、相当以上の性能を有する製品であること
本体仕様	外形	本体外寸が 89 (W) × 298 (D) × 340 (H) mm 以内であること、また本体質量が 4.3kg 以下であること
構成	CPU	Core (TM) i5-14500 相当以上の性能を有する CPU を搭載していること
	メインメモリ	(a) 32GB 以上搭載していること (b) すべて同一型番のメモリであること
	SSD	(a) 容量が 256GB 以上であること (b) 暗号化機能を有していること
	光ディスクドライブ	内蔵型ディスクドライブであり CD/DVD を読み書き可能であること
	インタフェース	(a) 1000BASE-T ×1 ポート以上 (b) Type-C : USB 3.2 Gen2 (本体前面×1 ポート以上) (c) Type-A : USB 3.2 Gen2 (本体前面×2 ポート以上) (d) USB 3.2 Gen1 (本体前面×2 ポート以上、本体背面×2 ポート以上) (e) HDMI ポート×1 ポート以上 (f) DisplayPort×2 ポート以上
	ディスプレイ出力	LCDE244F-CA 24 型 3 辺狭額縁フル HD 液晶または相当以上の製品を準備し接続すること
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 293W 以下であること
環境条件	温度条件	動作時は 10～35℃で動作可能であること
	湿度条件	稼働時：20～80%（結露しないこと）
ソフトウェア	OS	Windows11 Pro または、相当以上の性能を有する製品であること

⑭ 学校用 L3 スイッチ

項目	詳細	仕様
用途	使用用途	各サーバー・ネットワーク機器を収容するスイッチ
本体メーカー	型番	NEC QX-S4308XT-2X-PW 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0~45℃ 湿度 10~90% (結露しないこと)
性能	基本性能	(a) スイッチング容量 200Gbps 以上であること (b) 最大転送性能 148.8Mpps 以上であること (c) 登録 MAC アドレス数が 32,000 以上であること (d) 最大 VLAN 数が 4,094 以上であること
構成	インタフェース	(a) 100/1000/2.5G/5G/10GBASE-T×8 ポート以上 (b) SFP+スロット×2 ポート以上
機能	VLAN	ポート VLAN、Tag VLAN (IEEE802.1Q)
	スパンニングツリー	STP (IEEE802.1D)、RSTP (IEEE802.1w)、MSTP (IEEE802.1s)
	ルーティング	スタティックルーティング、RIP (v1/v2/ng)
	セキュリティ	パケットフィルタリング、IEEE802.1X、MAC アドレス認証
	QoS	Line Rate、Committed Access Rate、Generic Traffic Shaping、QoS クラス数 8 以上
	信頼性	リンクアグリゲーション (LACP 対応)、 ストーム抑制、スタック機能
	運用管理	SNMP、syslog、SSH、telnet、ポートミラーリング、NTP (クライアント、サーバー)、RMON、sFlow
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 467W 以下であること

⑮ 学校用メディアコンバータ

項目	詳細	仕様
用途	使用用途	ファイアウォールの 1000BASE-T インタフェースを光インタフェースに変換し、教育委員会と各学校との接続に使用する
本体仕様	外形寸法	W52mm×H198mm×D74mm (固定用ホルダー部及び突起部除く)
	動作条件	温度-10~55℃ 湿度 95%RH 以下 (結露しないこと)
FX ポート	準拠規格	IEEE802.3Z 1000BASE-X
	伝送速度	1000Mbps
	インタフェース	SC コネクタ (JIS C 5973 F04 型)
	発光中心波長	820~860nm
	受光波長	770~860nm
	伝送距離 (目安)	2m~550m の製品×8
TX ポート	準拠規格	IEEE802.3ab 1000BASE-T
	伝送速度	1000Mbps
	適合コネクタ	RJ-45 コネクタ

項目	詳細	仕様
	最大伝送距離	100m
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 10W 以下であること

⑩ 学校用 PoE スイッチ (各フロア)

項目	詳細	仕様
用途	使用用途	無線アクセスポイントを接続する PoE スイッチ
本体メーカー	型番	NEC QX-S5124GT-4X-PW 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0～45℃ 湿度 10～90% (結露しないこと)
性能	基本性能	(a) スイッチング容量 128Gbps 以上であること (b) 最大転送性能 95.2Mpps 以上であること (c) 登録 MAC アドレス数が 16,000 以上であること (d) 最大 VLAN 数が 4,094 以上であること (e) 給電可能インタフェース数が 24 ポート以上であること (f) IEEE802.3af/at に対応していること (g) 最大供給電力が 370.0W 以上であること
構成	インタフェース	(a) 10/100/1000BASE-T×24 ポート以上 (b) SFP+10G スロット×4 ポート以上 上記ポート構成のスイッチを 2 台
機能	VLAN	ポート VLAN
	スパンニングツリー	STP (IEEE802.1D), RSTP (IEEE802.1w), MSTP (IEEE802.1s)
	セキュリティ	IEEE802.1X、MAC アドレス認証
	QoS	Line Rate、Committed Access Rate、Generic Traffic Shaping、QoS クラス数 8 以上
	運用管理	NTP クライアント、SNMP、syslog、SSH、telnet、RMON、ポートミラーリング
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 471W 以下であること

⑪ 学校用 PoE スイッチ (体育館)

項目	詳細	仕様
用途	使用用途	無線アクセスポイントを接続する PoE スイッチ
本体メーカー	型番	NEC QX-S1108GT-2G-PW 相当以上の性能を有する製品であること
本体仕様	外形	19 インチラックに搭載可能であること
	動作条件	温度 0～45℃ 湿度 10～90% (結露しないこと)
性能	基本性能	(h) スイッチング容量 20Gbps 以上であること (i) 最大転送性能 14.8Mpps 以上であること (j) 登録 MAC アドレス数が 16,000 以上であること

項目	詳細	仕様
		(k) 最大 VLAN 数が 4,094 以上であること (l) 給電可能インタフェース数が 8 ポート以上であること (m) IEEE802.3af/at に対応していること (n) 最大供給電力が 125.0W 以上であること
構成	インタフェース	(c) 10/100/1000BASE-T×8 ポート以上 (d) SFP+10G スロット×2 ポート以上 上記ポート構成のスイッチを 2 台
機能	VLAN	ポート VLAN
	スパンニングツリー	STP (IEEE802.1D), RSTP (IEEE802.1w), MSTP (IEEE802.1s)
	セキュリティ	IEEE802.1X、MAC アドレス認証
	QoS	Line Rate、Committed Access Rate、Generic Traffic Shaping、QoS クラス数 8 以上
	運用管理	NTP クライアント、SNMP、syslog、SSH、telnet、RMON、ポートミラーリング
電源	電源電圧	AC100V で動作すること
	消費電力	最大で 162W 以下であること

⑱ 学校用無線アクセスポイント

項目	詳細	仕様
用途	使用用途	各学校に設置される無線アクセスポイント
本体メーカー	型番	NEC QX-W1210 相当以上の性能を有する製品であること
本体仕様	動作条件	温度-10～50℃ 湿度 10～90% (結露しないこと)
性能	基本性能	(a) IEEE 802.11a/b/g/n/ac (wave2) /ax/be に対応していること (b) アンテナ内蔵型であること (c) 最大 SSID 数が 32 以上であること (d) 最大 VLAN 数が 256 以上であること (e) PoE 給電で動作すること (f) 最大接続クライアント数が 512 以上であること
構成	インタフェース	(a) 10/100/1000BASE-T×1 ポート以上 (b) マルチギガビットイーサネット×1 ポート以上
機能	VLAN	VLAN
	スパンニングツリー	STP (IEEE802.1D), RSTP (IEEE802.1w), MSTP (IEEE802.1s)
	セキュリティ	IEEE802.1X、MAC アドレス認証
	QoS	WMM
	運用管理	NTP クライアント、SNMP、syslog、SSH、telnet、RMON
電源	電源電圧	AC100V で動作すること (AC アダプタ)
	消費電力	最大で 19W 以下であること

⑲ 上野原市庁舎用サーバーラック

項目	仕様
19 インチラック	前述のハードウェア機器を搭載できること ※本市の所有する既設ラック利用でも可とする
コンソールユニット	(a) 前述の仮想化基盤サーバー、バックアップサーバーをディスプレイ、キーボード、マウスとして使用できること (b) 接続した機器の画面表示・操作を手動で切り替えできること (c) 1U 以内で前述の 19 インチラックに搭載できること

5 構築要件

(1) 基本要件

本システムの「アクセス制御による対策を講じたシステム構成」とするゼロトラスト型を実現するため、次の要件に則り構築すること。

- ① 要件定義・基本設計を行い、本市の承認を得ること。
- ② 機器設置前に必要なテストが完了していること。
- ③ 業務影響が最小限となるよう移行計画を作成し、本市の承認を得ること。
- ④ 構築上現行機器に設定変更が必要となる場合は、本市の承認を得たうえで受注業者が負担し行うこと。
- ⑤ 本番稼働前に本システム操作説明会を実施すること。なお、説明会の内容は本市と協議の上、決定すること。
- ⑥ 既存データについては本市と協議し、必要なデータを本システムに移行すること。尚、移行等で発生する機材等は受注業者が負担すること。
- ⑦ 構成要素の特性上実施できない項目については本市と協議し、合意した代替手段により実施すること。

(2) ネットワーク

- ① 本市が別途調達する通信回線を利用し、各小中学校、教育委員会、山梨県校務支援システム、パブリッククラウドサービス (SaaS)、行政セキュリティクラウドの人事給与システムと通信できるよう構成すること。
- ② 各小・中学校、教育委員会、山梨県校務支援システム、パブリッククラウドサービス (SaaS) の校務ネットワークからのインターネット通信は SWG を経由し、セキュリティを確保すること。
- ③ インターネット回線を経由した内部通信は、ルーター間でデータの暗号化を行うこと。
- ④ 各学校から校務系ネットワークへ接続する場合は、校務系ネットワーク専用の L2 スイッチを用いることにより、生徒・児童が利用する学習系ネットワークと分離し、生徒・児童が校務ネットワークにアクセスできないように構築すること。
- ⑤ ゼロトラストネットワーク基盤と各拠点の境界に、インターネットファイアウォールを配置しファイアウォール機能でセキュリティ対策を講じること。
- ⑥ 庁舎に各サーバー及びネットワーク機器を設置してシステムを構築すること。
- ⑦ 既設の LAN ケーブルは流用可能とするが、追加で必要となる LAN ケーブルは本賃貸借に含むこと。
- ⑧ LAN ケーブルは、接続元・接続先が分かるタグ等を取り付けること。
- ⑨ 本賃貸借で導入する機器の故障等に対し、迅速に対応するための監視ツールを導入すること。
- ⑩ 本賃貸借で利用するクラウドサービスの管理者アカウントは、第三者に利用されないためのセキュリティ対策を施すこと。
- ⑫ 上野原市教育委員会職員が利用する行政系パソコンからファイルサーバーシステムへのアクセスの想定も考慮すること。

(3) 上野原市庁舎

① 基本要件

- ア 導入機器は、耐震設置された施錠可能なラックに搭載し、関係者以外操作できない環境とすること。
- イ 導入機器は、本市が指定する箇所に収めること。
- ウ ラックに搭載されているサーバー機器及び、ネットワーク機器からプリンター等の機器までの LAN ケーブルを新規で敷設すること。

② 構築要件

- ア 上野原市庁舎用 L2 スイッチはスタック構成の冗長化を行い、仮想化基盤サーバー、接続ルーター等と同様のラックへ収容すること。
- イ 仮想化基盤サーバーは 2 台で共有ディスクを用いたクラスタ構成とすること。
- ウ 仮想化基盤サーバー上で、次のシステムを稼働させること。
 - ㊦ Active Directory Domain Service
 - ㊧ Active Directory 連携用システム
 - ㊨ Windows Server Update Service (WSUS)
 - ㊩ ファイル共有システム
 - ㊪ バックアップシステム
 - ㊫ 統合 ID 管理システム
 - ㊬ 校務用多要素認証システム
 - ㊭ 校務系ネットワーク認証システム
- エ 仮想化基盤サーバー上で稼働する仮想サーバーのうち、Active Directory システム、Active Directory 連携用システムは異なる仮想化基盤サーバー上で 2 台以上の冗長構成とし、各サービスを継続すること。その他のシステムについても、仮想化基盤サーバーで障害が発生した場合、残った仮想化基盤サーバー上で動作するよう構築すること。
- オ 本賃貸借で導入するサーバー機器等の障害等を検知するシステムを構築すること。
- カ Active Directory 及び DNS では、本調達のネットワーク要件を鑑みて適切なユーザー構成を検討すること。また Active Directory は校務系システムサーバー群に対して名前解決機能を提供すること。
- キ WSUS は、アップデートファイルのダウンロードによるインターネット通信量を削減するため、アップデートファイル管理対象を校務系システムサーバー群に限定し、WSUS サーバーからダウンロードが行われる構成とすること。
- ク 顔認証システムは、各小・中学校、教育委員会の職員が使用する端末の管理サーバーとして構築すること。
- ケ ファイル共有システムの現行データは、本賃貸借で導入する新規ファイル共有サーバーに移行すること。
- コ 統合 ID 管理システムは Active Directory とファイル共有サーバーに対し、人事異動に伴う各種データ連携が適切に行われるよう構築すること。
- サ Active Directory 連携用システムは、クラウドサービスに対し各小・中学校、教育委員会の職員が使用する端末のサインインユーザーに紐づいた SAML 認証が実現できるよう認証システムと連携した構築を行うこと。
- シ ファイル共有では、Active Directory と連携し、共有フォルダ毎に適切なアクセス権限を設定すること。なお、共有フォルダ構成 及び アクセス権限の設定内容は本市と協議の上、決定すること。また、現行ファイルサーバーのデータを移行すること。
- ス 校務系システムサーバーのバックアップを取得し、校務系システムバックアップサーバーに

保存すること。なお、バックアップスケジュール及びバックアップファイルの世代管理等のポリシーについては、本庁と協議の上決定すること。

セ 本賃貸借で導入する校務系システムサーバー及びネットワーク機器のハードディスク障害に備え、ハードディスクリカバリ作業に必要なリカバリメディア及びリカバリ手順書を教育委員会及び各学校へ提供すること。尚、リカバリメディア作成またはリカバリ用ライセンスが必要な場合、かかる費用は本調達に含めること。惨事復旧を想定したディスクリカバリの動作試験を実施すること。

(4) 各小中学校、教育委員会

① 基本要件

各小中学校に L2 スイッチ及び L3 スイッチを設置すること。

② 構築要件

ア 各小・中学校、教育委員会の職員が使用する校務系パソコンについては、SaaS 製品を用いたアップデートファイル管理に運用変更を行うものとし、Microsoft Update サーバーから直接、各校務系パソコンへダウンロードが行われる構成とすること。

イ 現在使用している各小・中学校、教育委員会の職員が使用する端末に次のシステムを導入すること。

㊦ 顔認証システム

(5) セキュリティクラウド要件

各小中学校、教育委員会の職員が使用する行政セキュリティクラウドにあるメール機能を利用できること。

(6) 成果品

	成果物	想定する内容
1	着手届	本業務の開始にあたり、受注者の代表者名、業務責任者、着手日等を記載し、本市へ届け出ること。
2	工程表	契約期間内における作業の進捗管理を行うための全体スケジュール。マイルストーンや各工程の期間を明記し、本市の承認を受けること。
3	プロジェクト計画書	当該業務に関する計画を記述し、本市の承認を受けること。目的、実施概要、体制、スケジュール及び WBS、会議体及びプロジェクト標準事項を記載する。
4	要件定義書	本書に定める要求要件を定義する内容を記載し、本市の承認を受けること。
5	基本設計書	要件定義書をインプット資料としたシステムの全体像を定義したシステム概要書。
6	ネットワーク構成図	本調達範囲のネットワーク詳細図を記載したもの。
7	ラック構成図	本調達範囲のハードウェア機器のラック搭載構成を記載したもの。
8	詳細設計書	本調達範囲のネットワーク機器、サーバー及びストレージ機器、無停電電源装置の詳細設定（パラメータ）を記載したもの。
9	試験仕様書兼結果報告書	本調達範囲の各種テストの実施計画、結果を記載した者。

	成果物	想定する内容
10	スイッチポート接続表	本調達範囲のネットワーク機器のポートアサイン表を記載したもの。
11	納入機器一覧表	本調達範囲にて納入したハードウェア、ソフトウェア等を一覧表に記載したもの。
12	保守体制表	保守体制・問合せ一覧表を記載したもの。
13	利用者向けマニュアル	各小・中学校、教育委員会の教職員向けのマニュアル。
14	システム復旧メディア	仮想化基盤サーバー及びバックアップサーバーの惨事復旧用イメージを DVD メディアに書き込んだもの。 ※各サーバーx2 枚ずつ納入すること
15	システム操作手順書	仮想化基盤サーバー、バックアップサーバー、ネットワーク機器、ソフトウェア等の運用時、障害時のシステム操作手順を記載したもの。

6 保守要件

(1) 受付及び問い合わせ対応

- ① 本業務の問い合わせにおいては本業務の範囲内において問い合わせ対応を行うこと。対応時間は平日 9:00-17:30 とする。
- ② ハードウェアの障害受付に関しては、24 時間 365 日対応できる緊急受付窓口も準備すること。
- ③ 導入したハードウェア、ソフトウェア（SaaS 含む）、およびそれらの連携に関する技術的な支援を含むこと。

(2) ハードウェア保守

- ① 本契約で導入するサーバー及びネットワーク機器については、契約（賃貸借）期間中継続して保守サービスを提供すること。
- ② システム障害発生時の交換修理等にかかる費用は全て本調達に含めること。
- ③ 契約（賃貸借）期間中の無停電電源装置のバッテリー交換費用を本調達に含めること。
- ④ 仮想化基盤サーバーについては、障害等を自動で通報する仕組みを有し、縮退等が発生した場合も、遅滞することなく検知でき、保守対応が可能であること。
- ⑤ 障害修理完了後は、学校および教育委員会に報告をすること。
- ⑥ ISO9001 規格の認証を取得していること。

(3) ソフトウェア保守

- ① 導入ソフトウェアは、サービスイン後 5 年間製品サポートを提供すること。
- ② ソフトウェアのリビジョンアップ・バージョンアップの適用作業については、対応について別途協議すること。

7 運用要件

(1) システム運用支援

- ① 稼働後 5 年にわたり、システムの運用及び業務の遂行を円滑に行うために、十分な支援体制を有し、助言等の技術的支援を実施すること。その対応は平日 9:00 から 17:30 とし、実際の対応については、職員と相談のうえ決定することとする。
- ② 導入業者にて運用体制や構成変更が発生した場合は、都度修正し最新版を提出すること。
- ③ ソフトウェアのリビジョンアップ・バージョンアップの適用作業については、対応について別

途協議すること。

- ④ 運用中に発生した障害対応について、保守担当者と速やかに情報を共有し連携することで、迅速な復旧対応ができる体制とすること。

(2) 問い合わせ対応

- ① ハードウェアからソフトウェアまでサポートを提供できるようにすること。(他社製の製品を選定する場合においても、受託者が問い合わせを受け付けること。)
- ② 受託者は問合せについての窓口を平日 9:00 から 17:30 で電話やメールで受け付けること。
- ③ 受付した問合せ内容については調査・切り分けを行い、問合せ者へ回答を行うこと。一次回答ができない場合はベンダー等に確認を行い、問合せ者へ回答すること。

(3) システム障害対応

- ① 受託者はシステム障害に関する連絡を電話やメールで受け付けること。その対応は平日 9:00 から 17:30 で行うこと。
- ② 連絡を受け付けた際は、速やかに復旧対応を行うこと。

(4) セキュリティインシデント対応

- ① 受託者はセキュリティインシデントが発生した場合、その内容を報告し、復旧支援を行うこと。その対応は平日 9:00 から 17:30 で行うこと。
- ② 対応後は、教育委員会の担当者に報告すること。

(5) ログ採取・調査

受託者はハードウェア障害発生時等に、各種ログの採取・調査を行うこと。

(6) 定例業務

- ① バージョンアップ対応
 - ア サーバーの更新プログラムについての情報を定期的に確認すること。
 - イ 更新プログラムの配信が必要な場合は、別途教育委員会の担当者と協議し、対応を行うこと。
- ② バックアップ成否確認
 - ア 受託者は定期的にバックアップの成否確認を行うこと。
 - イ バックアップの不具合が発生した場合は現地で対応を行うこと。

(7) 非定例業務

障害等が原因でデータに何らかの問題が発生した場合、事前に採取したバックアップデータを用いて復旧すること。また、本市の依頼によりバックアップデータよりファイルの復旧作業を行うこと。