富士河口湖町次世代校務 DX 環境整備業務

仕　　様　　書

富士河口湖町教育委員会

学校教育課

1. 総則

1.1. 件名

次世代校務 DX 環境整備業務

1.2. 概要

本賃貸借による調達仕様書は、富士河口湖町（以下、本町という）が発注する「次世代校務 DX 環境整備業務」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。

1.3. 目的

本町は令和 2 年度に小中学校等の学校ネットワーク強靭化の構築を行った。
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。

1.4. 本業務の基本方針

本町では、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 2 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などで新たな課題も出てきている。また、国の ICT 整備方針や町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、以下のような課題が挙げられる。

・校務処理の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

・端末やアカウントの初期設定や年次更新作業といった、必ずしも学校で行う必要のない機器やシステムに係る運用・管理業務を整備し、現場の業務負担軽減を図る必要がある

・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、以下のとおり方針を掲げて整備を行う。

（ア）ICT 利活用による教育の質の向上

・ICT 技術を利活用し、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

・本町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、本町の実態に応じた ICT の利活用推進を図る

（イ）校務の効率化

・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

・将来構想として、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

（ウ）情報セキュリティの確保

・文部科学省から令和 7 年 3 月に公表された最新の教育情報セキュリティポリシー及び令和 6 年度に策定された以下 4 点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

―教育情報セキュリティポリシー

―情報セキュリティポリシー基本方針

―情報セキュリティポリシー対策基準

―庁内ネットワーク及び情報システムの利用に関する規程

・現行の教育 ICT セキュリティ対策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

1.5. 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以下のとおりとする。

以下に示す(ア)から(ウ)の構築方針を参考に構築すること。

（ア） 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。

（イ） 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、教職員や本町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。

（ウ） 技術動向・政策動向への対応

次期環境の稼働期間は令和 8 年 12 月 1 日から令和 13 年 11 月 30 日までの 5 年間を想定しているが、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、本町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。

例えば、以下の政策動向については準拠が必要であると考えている。

・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

・文部科学省における教育 DX、GIGA スクール等に関する動向

（例）

―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）

―有識者会議（教育データの利活用に関する有識者会議　等）

―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）

・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

（例）

―「教育 DX ロードマップ」等のデジタル化施策（デジタル庁）

―「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）

1.6. 履行対象

学校数：小学校８校、中学校３校

外部施設：３か所

（富士河口湖町教育委員会、富士河口湖町教育センター、河口湖南中学校組合教育委員会）

1.7. 納入対象拠点

機器の搬入設置場所は以下の通りとする。

表 1.7-1. 各拠点所在地

小学校

No	学校名	住所
1	船津小学校	山梨県南都留郡富士河口湖町船津３７３７番地
2	小立小学校	山梨県南都留郡富士河口湖町小立２４４６番地
3	大石小学校	山梨県南都留郡富士河口湖町大石１４２５番地
4	河口小学校	山梨県南都留郡富士河口湖町河口１５６０番地
5	勝山小学校	山梨県南都留郡富士河口湖町勝山１０４７番地
6	西浜小学校	山梨県南都留郡富士河口湖町長浜２４２７番地
7	大嵐小学校	山梨県南都留郡富士河口湖町大嵐５５９番地
8	富士豊茂小学校	山梨県南都留郡富士河口湖町富士ヶ嶺１２０９番地

中学校

No	学校名	住所
1	河口湖北中学校	山梨県南都留郡富士河口湖町河口３２１０番地
2	勝山中学校	山梨県南都留郡富士河口湖町勝山１０４７番地

No	学校名	住所
3	河口湖南中学校	山梨県南都留郡富士河口湖町船津１１６４番地

外部施設

No	施設名	住所
1	富士河口湖町 教育委員会	山梨県南都留郡富士河口湖町船津１７００番地
2	富士河口湖町 教育センター	山梨県南都留郡富士河口湖町船津１７４７番地
3	河口湖南中学校 組合教育委員会	山梨県南都留郡富士河口湖町船津１１６４番地

表 1.7-2.児童生徒数・教職員数

令和 8 年 4 月 24 日時点

小学校

No	学校名	児童・生徒数(人)	教員数(人)	職員数(人)
1	船津小学校	535	45	12
2	小立小学校	337	30	6
3	大石小学校	51	13	2
4	河口小学校	118	13	4
5	勝山小学校	247	21	6
6	西浜小学校	25	9	2
7	大嵐小学校	32	8	1
8	富士豊茂 小学校	15	8	2

中学校

No	学校名	児童・生徒数(人)	教員数(人)	職員数(人)
1	河口湖北 中学校	68	14	1
2	勝山中学校	138	16	1
3	河口湖南 中学校	580	45	6

外部施設

No	施設名	職員数(人)
1	富士河口湖町教育委員会	11
2	富士河口湖町教育センター	7

No	施設名	職員数(人)
3	河口湖南中学校組合教育委員会	3

1.7.1. 納入期限

導入する機器の納入期限は令和 8 年 11 月 30 日とする。

諸般の事情により期日までに遂行できない場合は別途協議とする。

1.7.2. 賃貸借期間

導入する機器の契約（賃貸借）期間は、令和 8 年 12 月 1 日～令和 13 年 11 月 30 日とする。

1.7.3. 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、本町担当者と協議の上、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に含むこととする。

2. 調達範囲

2.1. 調達対象システム

次期環境の調達対象システムは、「表 2.1-1.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」（※表 1.7-1、1.7-2）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。

表 2.1-1.次期環境の調達対象システム

No.	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	証明書管理システム	・教職員 314 ライセンス（非常勤・予備機分を含む）
2		アンチウイルス/EDR（Endpoint Detection and Response）	・教職員 314 ライセンス（非常勤・予備機分を含む

3	オンプレミス サーバー (庁舎へ配備)	Active Directory システム	・教職員 314 人
4		Active Directory 連携用 システム	・教職員 314 人
5		WSUS システム	・教育委員会に配備されたサーバー台数分
6		ファイル共有システム	・教職員 314 人
7		バックアップシステム	・教育委員会に配備されたサーバー台数分
8		データ暗号化システム	・教職員 314 ライセンス（非常勤・予備機分を含む）
9		校務用多要素認証システム	・教職員 314 ライセンス（非常勤・予備機分を含む）

下記サービスは本町より提供する。

No.	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	Microsoft 365 A3	・教職員 314 ライセンス（非常勤・予備機分を含む）

2.2. 共通要件

1. 本町内全 10 校にある校務兼財務会計アクセス用パソコンから庁舎内の財務会計システムにアクセスさせること。
2. 本町と同等規模または同等規模以上相当の教育機関・自治体において校務 DX の構築導入実績があること。
3. 納入する機器は、原則中古品不可とする。
4. 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。
5. 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。
6. 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、追加の電源工事を行うこと。
7. 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。

8. 本調達に含む製品ライセンスは、サービスインから 5 年間にお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、本契約の中で対応すること。

9. 現環境にあるデータ（Active Directory、ファイルサーバー等）は本業務の受託業者が次期環境に移行すること。また移行に係る費用を本調達に含めること。

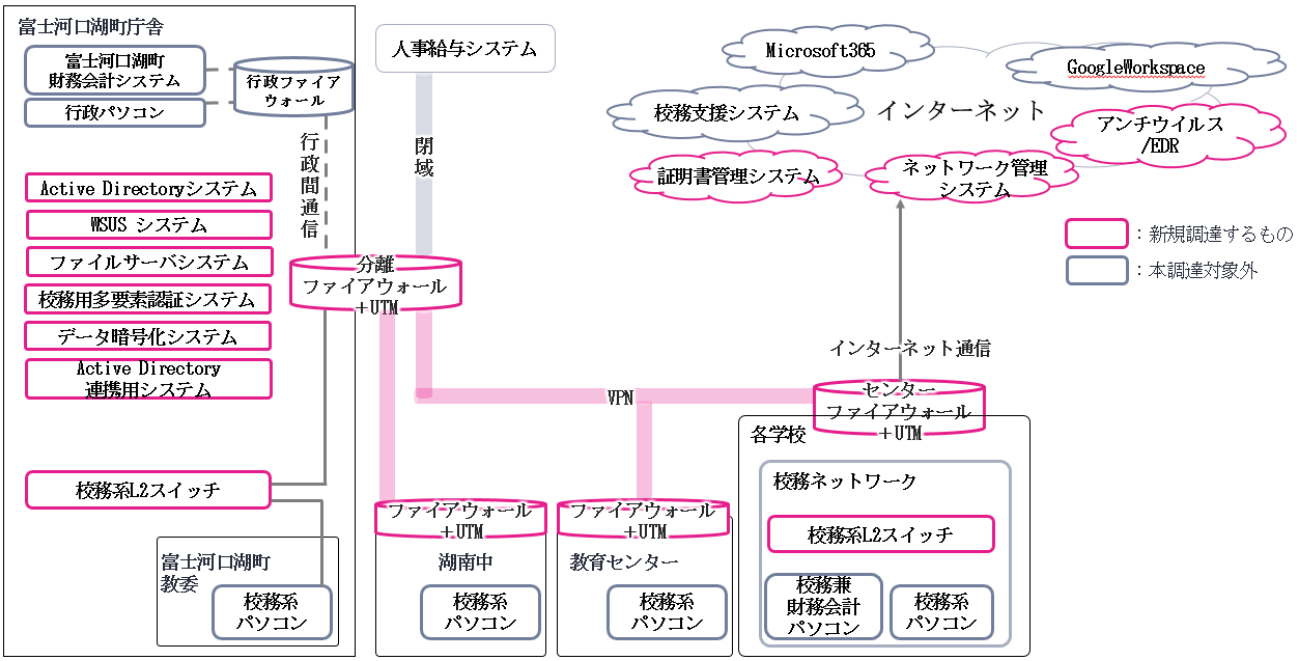
10. 校務系パソコンに対し必要となる設定や作業がある場合は、本調達内で実施すること。また設定や作業にかかる費用は本調達に含めること。なお、校務系パソコンに対し設定や作業を行う場合、校務系パソコン納入業者と連携し、マスターの作成や検証等の作業を必要に応じて実施すること。

3. 整備要件

3. 1. システム構成

教育情報システム（以下、「本システム」という。）は、クラウドシステムを基本的に利用し、庁舎内には現行環境から Active Directory サーバー、ファイルサーバー等と次期環境には多要素認証に係る認証サーバーとデータ暗号化に係るサーバーを設置すること。

図 3.1-1.教育ネットワーク全体イメージ



3.1.1. 機器設置台数内訳

項番	機器名称	船津小学校	小立小学校	大石小学校	河口小学校	勝山小学校	西浜小学校	大嵐小学校	富士豊茂小学校	河口湖北中学校	勝山中学校	河口湖南中学校	教育センター	庁舎	合計
4.1.1	富士河口湖町庁舎用ルータ													1	1
4.1.2	富士河口湖町庁舎用 L3 スイッチ													2	2
4.1.3	富士河口湖町庁舎用 ファイアウォール													2	2
4.1.4	富士河口湖町庁舎用 L2 スイッチ													2	2
4.1.5	富士河口湖町庁舎用 メディアコンバータ													12	12
4.1.6	富士河口湖町庁舎用 仮想化基盤サーバー													2	2
4.1.7	富士河口湖町庁舎用無停電電源装置 (仮想化基盤サーバー用)													2	2
4.1.8	富士河口湖町庁舎用 仮想化ストレージ													1	1
4.1.9	富士河口湖町庁舎用 バックアップサーバー													1	1
4.1.10	富士河口湖町庁舎用無停電電源装置 (バックアップサーバー用)													1	1
4.1.11	学校・教育センター用ルータ	1	1	1	1	1	1	1	1	1	1	1	1		12
4.1.12	学校・教育センター用 ファイアウォール	1	1	1	1	1	1	1	1	1	1	1	1		12
4.1.13	学校・教育センター用 L2 スイッチ	1	1	1	1	1	1	1	1	1	1	1	1		12
4.1.14	学校・教育センター用 メディアコンバータ	1	1	1	1	1	1	1	1	1	1	1	1		12

3.2. 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）

3.3. クラウドサービス要件

Microsoft 365 A3 ライセンスは本町より提供する。

3.3.1. アンチウイルス/EDR (Endpoint Detection and Response) 要件

(ア)環境要件

1. クライアント・エージェント・ソフトウェアはWindows、Windows Server、Mac、Linuxに対応していること。

2. クライアント・エージェント・ソフトウェアのインストールにおいては、システムの再起動を必要としないこと。

3. クライアント・エージェント・ソフトウェアは、設定情報が含まれる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。

4. クラウドサービスとして提供する場合、管理サーバーは日本国内に設置可能なこと。

(イ)検知・分析要件

1. 既知の攻撃のみならず、未知の攻撃にもリアルタイムに対応すること。

2. ランサムウェアにおいては、リアルタイムでの対応を必要とするため、管理者がオペレーション関与することなく、Windows端末にある該当プロセスを停止するなどの処置が自動でおこなえること。

3. ランサムウェアでファイルが暗号化された場合には、自動的にファイルを復元出来ること。

4. アンチウイルスのスキャン機能を回避するよう細工、改変されたマルウェアの亜種をシグネチャ等の配信によらず、0Dayで検知できること。

5. 攻撃者が利用するファイルやドメインや振る舞いと言ったIOCだけでなく、攻撃者の戦術およびテクニックを検知できること。

6. 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、時系列での不正なふるまいの状況を即座に把握できること。

7. 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。

8. 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。

9. 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。

※Windows Management Instrumentation

(ウ)調査・復旧要件

1. 攻撃が検知されたWindows端末に対し、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もおこなえること。

2. 攻撃を検知した場合の上記オペレーションを検知単位（被害単位）で、一括で行うことが可能なこと。

3. 攻撃として検知したファイル以外であっても、管理UI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。

4. 攻撃を検知したプロセスの前後の親プロセスや子プロセスなどプロセスツリーを表示する機能を有すること。

5. 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。

6. 管理画面よりレポートが日本語で PDF 出力できること。

(エ) その他クラウドサービス要件

1. 管理画面が完全に日本語対応していること。

2. 管理画面へのログインに、2 要素認証を設定できること。

3. 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、再起動、アップデート、ログアップロードの停止およびアンインストールが管理画面より遠隔にて実施できること。

4. 部門毎の管理者が部門内のエージェント、アラートのみを管理できるマルチテナント機能を有すること。

5. エージェントを IP アドレスや AD の組織単位などにもとづいて自動的にグループ割り当てが出来ること。また、グループ毎にエージェントのポリシー割り当てが出来ること。

6. 誤検知・過剰検知を低減するために、ハッシュ値やファイル名だけでなく、ふるまい単位での検知除外設定ができること。

7. クラウドサービスとして提供する場合は、クラウド側のサーバーのバージョンアップの実施時期を利用者側と調整できること。

(オ) クラウドサービス基盤非機能要件

1. 管理サーバーのメンテナンス（バージョンアップ作業等）は、ライセンス期間中、回数無制限および無償で提供すること。

2. メーカーは日本に法人格を登記し、社員による製品サポートを実施すること。

3. セキュリティとデータ保護を維持するため、堅牢な管理を行っており、次の規定および規定の認定を受けていること。

- ISO/IEC 27001:2013
- ISO/IEC 27017:2015
- ISO/IEC 27018:2014
- AICPA: SOC2 Type2

4. 監視サービスは、一定の技術要件及び品質管理要件を満たし、品質の維持・向上に努めている情報セキュリティサービスを明らかにする「情報セキュリティサービス基準適合サービスリスト」に登録されていること。

5. クラウドサービスとして提供する場合は、日本政府が求めるセキュリティ要件を満たした「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））」を 2026 年 3 月 31 日時点で取得していること。

3.3.2. 証明書管理機能要件

(ア)認証局機能要件

1. 1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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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。
8. カメラ機能を搭載しないデバイス(パソコンなど)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。
9. カメラ機能を搭載するデバイス(スマートフォンなど)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。
10. 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。
11. 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。
12. 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。
13. 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。
14. 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。
15. 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。
16. 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。
17. 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。
18. 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。
19. 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。
20. 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。
21. 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。
22. 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。

23. 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。

(イ) ID 管理機能要件

1. オンプレミス環境の認証サーバー(Active Directory) および Microsoft Entra ID 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。

2. オンプレミス環境の認証サーバー(Active Directory) および Microsoft Entra ID 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。

3. 認証サーバー(Active Directory) および Microsoft Entra ID 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。

4. 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。

5. 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表示が可能であること。

(ウ) 管理者機能要件

1. 管理 GUI を備えること。

2. 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、同期実行ログを閲覧・検索が可能であること。

3. 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、同期実行ログをファイル出力する機能を有すること。

4. 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。

5. 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。

6. 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

7. 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。

8. 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。

9. 認証サーバーとして複数の Active Directory、Microsoft Entra ID が連携できること。

10. 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) セキュリティ機能要件

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 管理者は、Web ブラウザから以下の内容を含む操作ログを取得できること。

- 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
- 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
- 同期実行の実施日時、成功/失敗、処理内容

7. 重要なクラウドサービスなど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。

(オ)サポート要件

1. 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。
2. Web フォームによる問い合わせ受付ができること。

(カ)クラウドサービス基盤非機能要件

1. 各機能で使用する ID は一元管理可能なこと。
2. クラウド型のサービスであること。
3. 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。
4. 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。
5. データバックアップ運用が備わっていること。
6. ログの保全対応が備わっていること。
7. ログの保存は 90 日まで可能であること。
8. 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。
9. 問題が発生した場合に国内法が適用されること。
10. 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。
11. 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。
12. 本サービスの運用者は、プライバシーマーク、ISMS 認証（ISO27001）など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。
13. ISMS クラウドセキュリティ認証(ISO27017)を取得していること。
14. ISMAP に登録されていること。

3.4. オンプレミスサーバー要件（富士河口湖町庁舎に配備）

3.4.1. Active Directory システム要件

1. サーバーは Windows Server 2022/2025、クライアント OS は Window11 環境で動作する環境を提供すること。
2. 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。
3. 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。
4. 時刻同期サービスを稼働させること。
5. 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。
6. 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。
7. グループポリシーの設定は現行のものを引き継ぐこと。
8. 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。
9. 顔認証、データ暗号化システム導入に伴い、ユーザー管理を見直すこと。
10. DNS サービスの設定は現行のものを引き継ぐこと。
11. 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。
12. 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、本役場と合意の上、作業を実施すること。

3.4.2. Active Directory 連携用システム要件

1. 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。
2. 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。
3. 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。

3.4.3. WSUS システム要件

1. サーバーは Windows Server 2022/2025 で動作する環境を提供すること。
2. 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。
3. WSUS サーバーの配信の設定は現行のものを引き継ぐこと。
4. 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。
5. Windows Update の管理を実施できること。

3.4.4. ファイル共有システム要件

1. 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。
2. 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。

3. 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。

4. 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。

5. スナップショットにて復元できる機能を有すること。

3.4.5. バックアップシステム要件

3.4.5.1. 機能要件

(ア) バックアップ機能

1. 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。

2. 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。

3. 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。

4. 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。

5. 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。

6. 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。

(イ) リストア・復旧機能

1. 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。

2. 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。

3. 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。

(ウ) ストレージ

1. 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。

2. 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。

3.4.5.2. 運用・管理要件

1. 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。

2. 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。

3. 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。

3.4.5.3. 非機能要件

1. 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。
2. 日本語対応の管理画面をサポートしていること。

3.4.6. データ暗号化システム要件

(ア) 暗号化ポリシー機能要件

1. 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。
2. 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。
3. 端末のローカルディスク内に保存されたファイルを自動または手動にて暗号化できること。暗号化ポリシーの設定により手動での暗号化、暗号化解除が可能であること。
4. 自動暗号化に関して、管理者にて自動暗号化範囲を指定可能であること。また自動暗号化対象外フォルダについても指定可能であること。
5. ファイルサーバー上に保存されているファイルを自動暗号化できること。
6. 暗号化済みファイルについて、端末上から簡単に視認できること。
7. 暗号化済みファイルについて、元のファイルの拡張子より変更がされないこと。
8. 複数の暗号化ポリシーを作成する事ができ、暗号化済みのファイルに関して外部組織からの閲覧ができない事はもちろんの事、内部組織からの閲覧に関してポリシーごとに閲覧者の操作権限(閲覧可/不可、編集可/不可など)を管理・制御できること。
9. Microsoft Purview Information Protection (MIP) との連携機能を有すること。

(イ) 管理要件

1. 暗号化ポリシーは利用者に自動配布・自動適用が可能であること。
2. 暗号化ポリシー全体を管理するサーバー管理者と、利用者を管理するセキュリティグループ管理者を設定し、暗号化ポリシーを階層的に管理できること。
3. セキュリティグループ管理者により部門ごとのより細かな暗号化ポリシーを設定・管理できること。
4. 暗号化ポリシーに関して以下の設定を管理・制御できること。
   - ローカルディスクの自動暗号化設定
   - 右クリックメニューによる手動暗号化設定
   - ログ送信設定
   - 暗号化ポリシーの受信設定(ポリシー受信(取得)するタイミングを指定)
5. 暗号化処理で保護されたファイルの利用状況を端末のイベントログに記録し、暗号化ポリシーで定めたタイミングでサーバー側へ送信できること。
6. 管理者は、端末から送信されたログを確認することにより、ファイルの暗号化を解除した文書を外部に持ち出した可能性のある利用者を特定することができること。

（ウ） 暗号化ファイルの閲覧機能要件

1. 以下の形式のファイル暗号化が実施でき、対象のアプリケーションを利用し暗号化された状態でファイルの閲覧等が実施可能であること。

表 3.4.6-1. 暗号化ファイルの閲覧機能要件

アプリケーション名	プロセス名	文書形式
Windows 標準 メモ帳	notepad.exe	txt、csv、htm、html
Windows 標準 ペイント	mspaint.exe	jpg、jpeg、jpe、jfif、tif、tiff、png、bmp、dib、gif
Adobe Acrobat Reader DC Continuous 版、Classic 2020、 Classic 2017、Classic 2015	acrord32.exe acrobat.exe	pdf、fdf、xfdf
AutoCAD 2011、2012	acad.exe	dwg、dws、dwt、dxf
SolidWorks Premium 2010 SP4.0	sldworks.exe	SLDASM、SLDPRT、SLDDRW
Pro/ENGINEER WILDFIRE 5.0 Creo Parametric Ver1.00	xtop.exe pro_dwgconv.exe pro_medconv.exe pvtopro.exe pro_sthenoconv.exe	prt、asm、drw、frm、sec、rep、mrk (prt.*、asm.*、drw.*、frm.*、sec.*、rep.*、mrk.*)
DocuWorksViewerLight7.2,8.0,9.0,9.1	dwvlt.exe	xdw、xbd、xct
Microsoft 365 Microsoft Office Professional Plus 2016、2019、2021	WINWORD.EXE	docx、docm、doc

3.4.7. 校務用多要素認証システム要件

(ア)構成要件

1. 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。

2. 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。

3. 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。

4. 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）

5. 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。

6. 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などを管理、格納できること。

7. 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。

8. 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。

9. 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などを、登録/変更/削除する専用の管理コンソールを有すること。

10. 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。

11. 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。

12. 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。

13. 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。

14. 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。

15. 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。

16. 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。

17. 顔認証の機能を有し、利用を必須とすること。

18. 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。

19. 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。

20. 代理入力の機能を有すること。

(イ)データ保全要件

1. 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。

2. 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。

3. 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

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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。
8. 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

1. 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)。
2. 人事異動時などに変更情報を 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。
3. 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。
4. 生体情報の有効化・無効化が設定できること。
5. 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。
6. 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。
7. 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。
8. 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。
9. 管理コンソールの操作をログとして記録できること。
10. 認証/設定管理サーバーの OU 毎にセキュリティ設定情報などを設定、変更し、運用が可能なこと。

11. 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。

12. ユーザーに変更権限が与えられた情報（パスワードなど）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

1. ユーザーは生体証成功後、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。

2. 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。

3. 写真など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、笑顔など顔の動きをチェックする機能を有すること）

4. ログオン画面の画像を任意の画像に変更できること。

5. ログオン時に必要な認証情報を、下記パターン以上の方式から選択可能であること。

① 生体情報+校務用多要素認証システム アカウント

② 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

③ 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

④ Windows アカウント/パスワード

ただし④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。

6. 5-④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おこな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。

7. 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おこなえるように設定できること。

8. 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。

9. 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など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。

10. 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。

11. 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できること。

12. 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

フまたはシャットダウンする機能を有すること。

13. スクリーンセーバー起動時に校務系パソコンがロックする機能を有すること。

14. スクリーンセーバー起動までの時間設定が 0 分から 999 分までの間で設定可能であること。

15. 離席時に校務系パソコンをロックする機能を有すること。またテレビ会議利用時などに一時停止する機能を有すること。

16. 照合(本人確認)機能により、ログオン後も定期的に顔を照合し、ログオン時の認証情報と異なる場合はロックする機能を有すること。

17. 検出(人の存在を確認)機能により、ログオン後も定期的に顔を検出し、離席している場合はロックする機能を有すること。

18. 照合機能と検出機能は併用できること。

19. 照合間隔、検出間隔は任意に設定できること。

20. PC 操作中は照合・検出を行わない機能を有すること。

21. 照合・検出に失敗した場合、画面表示を行なったうえで再度照合・検出を行う機能を有すること。これにより、利用者が予期しないタイミングで PC をロックすることを避けられること。

22. タスクトレイアイコンから、指定した時間離席ロックを一時解除する機能を有すること。

23. カメラアプリ起動時に自動で離席ロックを一時停止する機能を有すること。

24. ユーザー毎にロック解除を許可する他のユーザーを指定できること。

25. ロック解除時も二要素で解除できること。

26. クライアントがネットワークから切り離された場合、任意に設定された期間内であれば、クライアントにログオンできること。

27. クライアントがネットワークから切り離された場合、クライアントへのログオンを許可しないような設定も可能であること。

28. クライアントがネットワークから切り離された場合、ログオンできる期間が切れる前にユーザーに対しメッセージを表示できること。その残りの日数を任意に指定できること。

29. PC メンテナンス時等、一時的にクライアントモジュールを停止させるパスワードを使用できること。

30. クライアントモジュールを停止させるパスワードは、有効期限、利用可能回数、使用目的の制限が設定可能であること

31. クライアントモジュールを停止させるパスワードは、数字・英文字・記号を含む複雑性を確保していること。

32. 生体情報を利用できない際のユーザーに対する緊急救済装置として、生体情報の代用になるパスワードを利用できること。

33. 生体情報の代用となるパスワードは、有効期限、利用可能回数の制限が設定可能であること。

34. 生体情報の代用となるパスワードは、数字・英文字・記号を含む複雑性を確保してい

ること。

35. クライアントの認証時やロック解除時のログをローカルやログサーバーに出力する機能を有すること。

36. 認証スコア（類似度）がログに出力されること。

3.5. ネットワークセキュリティ要件

3.5.1. ソフトウェア要件

1. https 対応の Web インタフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。

2. GUI は一般的な Web ブラウザを利用したものであること。

3. IPv6 による WebUI/CLI の管理通信に対応していること。

4. 次世代ファイアウォール装置（2 式）は Active-Standby の冗長化構成で導入できること。

5. Active-Standby の冗長化を構成する次世代ファイアウォール装置は、外部、内部それぞれに 1 つの IP アドレスで構成できること。

6. Active/Passive、Active/Active 両方の冗長構成に対応していること。

7. 仮想 UTM（VDOM）ごとにプライマリハードウェアを選択することで、Active/Active 構成が取れること。

8. 次世代ファイアウォール装置は、ワンアームスニファー（ミラーポート接続）、バーチャルワイヤーペア、トランスペアレントモード（ブリッジ）、NAT/ルートモード（L3 ルータ）を特別なファームウェアなどに変更することなく、一筐体内で設定が可能なこと。

9. NAT 機能を有すること。

10. 仮想 UTM（VDOM）を利用することにより、次世代ファイアウォール装置内で NAT 型と透過型の混在可能なこと。

11. IEEE802.1Q VLAN トランク機能を有すること。

12. IEEE802.3ad リンクアグリゲーション機能を有すること（StaticLACP）。

13. ジャンボフレーム（9216 byte）をサポートすること。

14. インタフェースを指定して、パケットキャプチャを採取できること。

15. RIPv2、OSPFv3、BGP のダイナミックルーティングに対応していること。

16. IPv4 および IPv6 の OSPF Graceful Restart に対応していること。

17. インターネットサービスの IP アドレスデータベースを有し、Amazon、Salesforce、Microsoft Azure、Microsoft Office 365、Box、Google Cloud を宛先に選択し、ルーティングできること。また、インターネットサービスの IP アドレスデータベースを管理者が更新することなく動的に更新される運用が可能なこと。

18. マルチキャストルーティング機能を有し、PIM モードでスパース、デンスを設定できること。

19. SD-WAN 機能により、複数インタフェースのバンド幅、通信量、セッションに基づく WAN 最適化を行えること。

20. WAN リンクの冗長が可能で、自動的に経路障害の検出が可能なこと。

21. Web プロキシサーバー(フォワードプロキシ)機能を有し、プロキシの自動設定ファイル（PAC）、Web プロキシ自動検出プロトコル（WPAD）で Web ブラウザを設定する方法を展開できること。

22. Office365 通信のローカルブレイクアウトを自動化させる機能を有すること。

23. ネットワーク内の機器や OS を自動的に識別し、かつリスト表示可能なこと。

24. IPsecVPN によるサイト間 VPN に対応していること。

25. IPsec サイト間 VPN における IKE 証明書認証に対応していること。

26. WebUI で、CPU 使用率、メモリ使用率、セッション数の推移をリアルタイムでモニタリングが可能であること。

3.5.2. セキュリティ機能要件

1. DoS 攻撃防御機能を有すること。

2. Mac アドレスのラーニング情報を元にしたデバイス情報にて、ファイアウォールのポリシー制御が可能なこと。

3. ファイアウォールのポリシー毎にアンチウイルス、Web フィルタ、DNS フィルタ、アプリケーションコントロール、IPS、SSL インスペクション機能の有効/無効設定が可能なこと。

4. アンチウイルス、Web フィルタ、アプリケーションコントロール、IPS、アンチスパム、DLP は IPv6 に対応していること。

5. ユーザー識別、アプリケーションコントロール、IPS、アンチウイルス、Web フィルタリング、DNS フィルタ、DLP 機能を提供可能なこと。

6. 6401 種類以上のアプリケーションをポート番号に関わらず識別して可視化できること。（2026/3/31 時点）

7. ファイアウォールで適用するサービス(UDP/TCP/SCTP)とアプリケーション制御のアプリケーションライブラリは分かれていること。

8. クレジットカード番号、またはカスタマイズした文字列パターンでのデータフィルタが可能であること。

9. 19597 以上の IPS シグネチャを有すること。（2026/3/31 時点）

10. カスタムでアプリケーションおよび IPS 防御のシグネチャを作成できること。

11. 70000 以上のボットネット C&C ドメインの FQDN 情報を有し、ファイアウォールのポリシーで有効/無効に設定できること。（2026/3/31 時点）

12. サーバー証明書のコモンネームを参照して、サーバーの FQDN の情報で Web フィルタリングする certificate inspection 機能を有すること。

13. 次世代ファイアウォール装置内で SSH 通信を復号し、ポートフォワード通信を検知可能であること。

14. 次世代ファイアウォール装置内で SSL 通信を復号し、アプリケーションコントロール、IPS、アンチウイルス、Web フィルタリングの Full SSL inspection（Deep inspection）が可能であること。

15. 次世代ファイアウォール装置内にサーバー証明書と鍵をインポートし、その証明書と鍵をもとに該当するサーバー宛ての SSL 通信を復号し、アプリケーションの識別およびコンテンツ検査のポリシーが適用可能であること。

16. Active Directory 等と連携し、IP アドレスとユーザー情報を紐付けて可視化と制御が可能であること。

17. インターネット経由でファームウェアならびにシグネチャファイルを次世代ファイアウォール装置に直接ダウンロードおよびインストール可能であること。また Proxy 経由でもこれが可能であること。

18. Web フィルタリング機能は、92 以上のカテゴリーに分類されて、クラウドクエリを行って最新の URL 情報に基づくフィルタリング機能を提供できること。

19. アンチウイルス機能に未知のファイルを仮想 OS 環境で実行する Cloud Sandbox 検査機能が含まれていること。

20. アンチウイルスは、ヒューリスティック検査に対応していること。

21. 不正なデバイスに対して管理者が隔離を実施できること。スイッチのコントローラ機能を有効化している場合は、Mac アドレスレベルの隔離をスイッチで行えること。

22. 日本を含むグローバルで合計 200 名を超える脅威リサーチャーによる最新の脅威対策を実施していること。

3.5.3. 管理機能要件

1. WebUI は、日本語、英語、フランス語、スペイン語、ポルトガル語、中国語、韓国語に対応していること。
2. WebUI 上でコマンドラインインタフェースを利用可能なこと。
3. 過去の設定を自動保存し、GUI 上で設定を比較する機能を持つこと。
4. 複数の異なるバージョンの OS を保存できること。
5. ポリシー毎に UTM ログにするかすべてのログにするかを選択できること。
6. 4 台以上の外部 Syslog サーバーにログ出力可能であること。
7. 次世代ファイアウォール装置上でログ閲覧が可能であり、ログ管理装置と連携した場合は、次世代ファイアウォール装置の WebUI でログ管理装置にて収集されているログを閲覧できること。
8. 次世代ファイアウォール装置の通信ログは、許可も拒否もログに残せること。
9. 特定時間内で発生した脅威や通信を視覚的に表示して、マウスクリックのみで情報をフィルタして抽出できる機能を有すること。
10. 仮想 UTM（VDOM）単位で管理者を分割することが可能なこと。
11. 複数台の次世代ファイアウォール装置のファームウェア、シグネチャ、設定を一元管理できるアプライアンスと連携可能なこと。また、当該アプライアンスとの連携により、各次世代ファイアウォール装置がインターネットに接続しなくてもシグネチャを提供できること。
12. 複数台の次世代ファイアウォールのログを集中管理し、レポート生成可能なアプライアンスと連携可能なこと。

13. システム設定のバックアップは、暗号化とパスワードを設定してエクスポート可能であること。
14. 仮想 UTM（VDOM）ごとに設定のバックアップ・リストアが可能なこと。
15. Cloud によるログの分析と管理が可能で、利用帯域、セッション数、Web の利用状況、脅威に関するレポートをメールで所得できること。

3.5.4. エンドポイント連携要件

1. Windows と Mac OS の IPSec-VPN のクライアントソフトウェアを無償で提供できること。
2. エンドポイント管理システムのソリューションと連携して、Windows、Mac、Linux の OS バージョン、特定アプリケーションの利用、レジストリ Key などをトリガーにして、動的にファイアウォールのユーザーグループに適用され、ファイアウォールポリシー制御が可能なこと。

3.5.5. スイッチ・AP 連携要件

1. LGWAN-ASP サービスとして、ライセンス情報の登録とシグネチャ配信のソリューションを提供しており、無償にてサービスを利用できること。
2. ファブリックコネクタで、Cisco ACI、Google Cloud Platform、Microsoft Azure、Nuage Virtualized Services Platform、OpenStack（Horizon）、Oracle Cloud Infrastructure（OCI）、VMware NSX、AWS との SDN 連携が可能なこと。
3. 追加ライセンス無しで、ファイアウォールの管理画面よりスイッチと AP を一元管理（接続状態の可視化）し、網トポロジーの論理構成図と物理構成図を自動出力できること。

3.6. ネットワーク監視システム要件

1. 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 2000 台まで管理できること。
2. 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。
3. 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など)
4. 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。
5. 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。
6. 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。
7. アプリケーションごとに帯域制御ができること。
8. 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。
9. アラームを過去 365 日分さかのぼって確認出来ること。
10. トラフィック情報を CSV 形式でダウンロードできること。

11. コンフィグを毎週自動で保存する機能を有すること。
12. イベントログを管理する機能を有すること。
13. コンフィグを一括切替え出来る機能を有すること。
14. 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

4.1. ハードウェア/ソフトウェア

以下の 4.1.1 から 4.1.15 までの要求仕様を満たすこと。

4.1.1. 富士河口湖町庁舎用ルータ

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
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 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

項　目	詳　細	仕　　様
	消費電力	最大で 55W 以下であること

4.1.2. 富士河口湖町庁舎用 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
	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 100W 以下であること

4.1.3. 富士河口湖町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、教育センターとの接続に利用
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)

項　目	詳　細	仕　　様
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 (g) スイッチのコントローラ機能を有し､最大 64 台のスイッチに対して設定と管理を行えること (h) 無線 AP のコントローラ機能を有し、最大 256 台の AP に対して設定と管理を行えること。また、トンネルモードの場合､最大 128 の AP に対して設定と管理を行えること (i) 二要素認証用トークン(ハードウェア/ソフトウェア)をサポートし、最大 5000 まで管理可能なこと
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) 内臓ストレージ 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

4.1.4. 富士河口湖町庁舎用 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 (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

4.1.5. 富士河口湖町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、教育委員会と各学校及び教育センターとの接続に使用する
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-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	1260～1360nm
	受光波長	1480～1580nm

項　目	詳　細	仕　　様
	伝送距離(目安)	2m～25km の製品×11 15～50km の製品×1
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

4.1.6. 富士河口湖町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 ※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) 10GBASE-T ×2 ポート以上 (c) 管理用 LAN ポート×1 ポート以上 (d) Fiber Channel(32Gbps)×外部接続 2 ポート以上

項　目	詳　細	仕　　様
		※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、4.1.9.富士河口湖町庁舎用バックアップ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) ファイル暗号化サーバー (f) 認証基盤サーバー (g) 校務用多要素認証サーバー

4.1.7.　富士河口湖町庁舎用無停電電源装置(仮想化基盤サーバー用)

項　目		仕　　様
無停電電源装置	用途	仮想化基盤サーバー及び仮想化基盤サーバー用ストレージに電源を供給する
	メーカー	NEC N8142-102 無停電電源装置(3000VA)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 3000VA 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)

項　目		仕　　様
	出力プラグ	並行 2 極アース付き（NEMA 5-15R）6 口 並行 2 極アース付き（NEMA 5-20R）2 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、仮想化基盤サーバー上の仮想マシンについても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

4.1.8.　富士河口湖町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 30TB 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
	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

4.1.9. 富士河口湖町庁舎用バックアップサーバー

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 40TB 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
	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、4.1.6.富士河口湖町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
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

項　目	詳　細	仕　　様
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

4.1.10. 富士河口湖町庁舎用無停電電源装置(バックアップサーバー用)

項　目		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

4.1.11. 学校・教育センター用ルータ

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
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

項　目	詳　細	仕　　様
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（非結露）
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 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

4.1.12. 学校・教育センター用ファイアウォール

項　目	詳　細	仕　　様
用　途	使用用途	教育委員会との接続に利用
本体メーカー	型番	Fortigate-70G 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　10/10/6(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) 9M pps

項　目	詳　細	仕　　様
		以上であること (c) ファイアウォール同時セッション　(TCP) 700,000 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) 35,000 以上であること (e) ファイアウォールポリシー5,000 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) 1.8 Gbps 以上であること (g) スイッチのコントローラ機能を有し､最大 24 台のスイッチに対して設定と管理を行えること (h) 無線 AP のコントローラ機能を有し、最大 96 台の AP に対して設定と管理を行えること。また、トンネルモードの場合、最大 48 の AP に対して設定と管理を行えること (i) 二要素認証用トークン(ハードウェア/ソフトウェア)をサポートし、最大 500 まで管理可能なこと
構　成	インタフェースとモジュール	(a) 1000BASE-T×5 ポート以上(運用インタフェース) (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
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 20W 以下であること

4.1.13. 学校・教育センター用 L2 スイッチ

項　目	詳　細	仕　　様
用　途	使用用途	校務端末機器を収容するスイッチ。
本体メーカー	型番	NEC QX-S1124GT-4G 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) スイッチング容量 56Gbps 以上であること (b) 最大転送性能 41.6Mpps 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
構　成	インタフェース	(a) 10/100/1000BASE-T×24 ポート以上 (b) 1000(SFP スロット)×4 ポート以上
機　能	VLAN	ポート 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	Lins Rate
	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

4.1.14. 学校・教育センター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及び教育センター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	1480～1580nm
	受光波長	1260～1360nm
	伝送距離(目安)	2m～25km の製品×11 15～50km の製品×1
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

4.1.15. 富士河口湖町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。 ※本町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

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、以下の要件に則り構築すること。

1. 要件定義・基本設計を行い、本町の承認を得ること。
2. 機器設置前に必要なテストが完了していること。
3. 業務影響を最小限となるよう移行計画を作成し、本町の承認を得ること。
4. 構築上現行機器に設定変更が必要となる場合は、本町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。説明会の内容は本町と協議の上、決定する。
6. 既存データについては本町と協議し、必要なデータを本システムに移行すること。尚、移行など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町と協議し、合意した代替手段により実施すること。

5.1.　ネットワーク

1. 本町が別途調達する通信回線を利用し、各小・中学校、教育センター、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. 山梨県校務支援システムへの接続は、SAML 認証によるシングルサインオンが出来るよう設定すること。
3. 各小・中学校、教育センター、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。
4. インターネット回線を経由した内部通信は、ルータ間でデータの暗号化を行うこと。
5. 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。

6. 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。

7. 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。

8. 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。

9. 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。

10. 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。

11. 本賃貸借で導入するサーバーにアンチウイルス／EDR をインストールすること。

12. 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。

13. 本町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。

5.2. 富士河口湖町庁舎

5.2.1. 基本要件

1. 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。

2. ラックに搭載されているサーバー機器までの LAN ケーブルを新規で敷設すること。

5.2.2. 構築要件

1. 富士河口湖町庁舎用 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、接続ルータ等と同様のラックへ収容すること。

2. 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。

3. 仮想化基盤サーバー上で、以下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
- データ暗号化システム
- 校務用多要素認証システム

4. 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。

5. 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。

6. 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。

7. 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。

8. 顔認証システム、ファイル暗号化システムは、各小・中学校、教育センター、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。

9. 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。

10. 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、教育センター、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。

11. 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町と協議の上、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。

12. 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、本町と協議の上決定すること。

13. 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ー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ーの動作試験を実施すること。

5.3. 各小・中学校、教育センター、教育委員会

5.3.1. 基本要件

1. 各小・中学校、教育センターに校務系 L2 スイッチ及び校務系センターファイアウォールを設置すること。

2. 各小・中学校、教育センターは校務系 L2 スイッチからサーバー、プリンターなどの機器までの LAN ケーブルは既設を流用すること。

5.3.2. 構築要件

1. 各小・中学校、教育センター、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。

2. 現在使用している各小・中学校、教育センター、教育委員会の職員が使用する端末に以下のシステムを導入すること。

- 顔認証システム

・　ファイル暗号化システム
・　アンチウイルス／EDR

5.4. セキュリティクラウド要件

1.　各小・中学校、教育センター、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。

5.5. モバイル端末管理（MDM）システム要件

1.　モバイル端末管理（MDM）システムは、本町が提供する Microsoft 365 A3 を利用して設定すること。また設定費用は本調達に含めること。

2.　設定する際は、校務系パソコン納入業者と連携すること。校務系パソコン納入業者の連絡先は 2.2 共通要件に記載。

5.6.　成果品

項番	成果物	想定する内容
1	プロジェクト計画書	当該業務に関する計画を記述し、本町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。
2	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、本町の承認を受けること。
3	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。
4	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。
5	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。
6	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。
7	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。
8	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。
9	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。
10	保守体制表	保守体制・問合せ一覧表を記載したもの。
11	利用者向けマニュアル	各小・中学校、教育センター、教育委員会の教職員向けのマニュアル。
12	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。

項番	成果物	想定する内容
		※各サーバーx2 枚ずつ納入すること
13	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

6.1. 受付問い合わせ対応

1. ハードウェア及びソフトウェアに一貫したサポートを提供するための一次窓口を設けること。また、一次窓口は本町内に準備すること。

2. 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 8:30－17:30 とする。

3. 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。

6.2. 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換修理等にかかる費用は全て本調達に含めること。

3. 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。

4. 障害修理完了後は、学校および教育委員会に書面にて報告をすること。

5. サーバー、ネットワーク機器の保守サービス部局は山梨県内より対応できること。また、ISO9001 規格の認証を取得していること。

6.3. 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、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

内容については別途協議とし本契約の事業者と随意契約とする。

7.1. システム運用支援

1. 稼働後、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 8:30－17:30 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。

7.2. 問い合わせ対応

1. ハードウェアからソフトウェアまで一貫した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。ただしMicrosoft 365 A3についての問い合わせは本町がMicrosoftへ直接行うため除外する。）

2. 受託者は問合せについての窓口を平日8:30－17:30で常設し、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。

7.3. 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8:30－17:30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。

7.4. 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8:30－17:30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。

7.5. ネットワーク監視

1. 受託者はネットワーク監視を平日8:30－17:30で行うこと。

2. 異常を検知した場合は、速やかに復旧対応を行うこと。

7.6. SOCによる常時監視

1. 監視サービスを提供できる体制があること。
2. 監視サービスは、メーカーの国内拠点から提供可能であること。
3. エンドポイントセキュリティと監視サービスは同一メーカーで提供すること。
4. 初動通知はインシデント検知後30分未満であること。
5. 製品の検知ロジックに応じた脅威監視だけではなく、定期的なスレッドハンティングを提供可能であること。
6. 月次で日本語によるレポートが提供可能であること。
7. 危険度の高い攻撃が検知された場合には、電話での連絡が可能であること。
8. 攻撃を検知した場合には高度解析をおこない、その結果を日本語でレポートとして提供可能であること。
9. 監視サービスが、日本政府が求めるセキュリティ要件を満たした「政府情報システム

のためのセキュリティ評価制度（Information system Security Management and Assessment Program：通称、ISMAP（イスマップ））」を 2026 年 3 月 31 日時点で取得していること。

7.7. ログ採取・調査

1. 受託者はハードウェア障害発生時などに、各種ログの採取・調査を行うこと。

7.8. 定例業務

7.8.1. バージョンアップ対応

1. 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。
2. 更新プログラムの配信が必要な場合は、適宜教育委員会の担当者と協議し、対応を行うこと。

7.8.2. バックアップ成否確認

1. 受託者は定期的にバックアップの成否確認を行うこと。
2. 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。

7.9. 非定例業務

7.9.1. 復旧作業

1. 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、本町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。

以上