金沢市立工業高等学校
ゼロトラストセキュリティ環境構築業務

仕様書

1. 概要

1.1. 件名

金沢市立工業高等学校　ゼロトラストセキュリティ環境構築業務

1.2. 背景と目的

令和 7 年 3 月に文部科学省の「教育情報セキュリティポリシーに関するガイドライン」が改訂され、クラウド活用と、ネットワーク分離を必要としないアクセス制御による対策を講じたシステム構成が示された。本校では、利便性向上とコスト削減のため、極力設備を持たず、セキュリティ機器なども含めてクラウド化した、新たな教育情報ネットワークの実現を目指している。

本業務は、以上のことを総合的に考慮したうえで計画的な調達、構築を進め、ICT を活用した校務をより一層推進できる環境を整備することを目的に、新たな ICT ネットワークへ構築移行するものである。

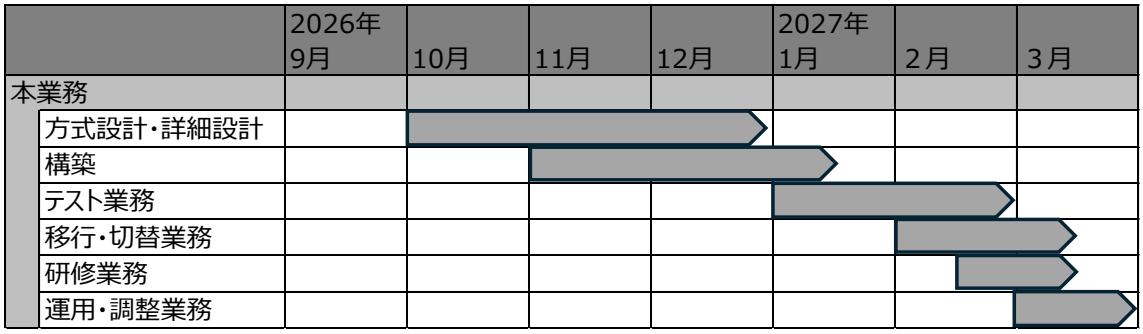
1.3. 業務概要

本業務は、金沢市立工業高等学校（以下、発注者とする）の整備している校務管理システムのクラウドリフト及びセキュリティ基盤構築のプロジェクト管理、設計・構築、テスト、移行・切替、研修の各業務が対象となる。スケジュールの詳細は『1.5. スケジュール』を確認すること。

1.4. 委託期間

契約締結日～令和 9 年 3 月 31 日

1.5. スケジュール



1.6. 調達範囲

実施事項	工程
セキュリティ基盤	・プロジェクト管理 ・設計、構築業務 ※必要に応じてライセンスを調達 ・テスト業務 ・移行、切替業務 ・研修業務
ネットワーク移行	必要に応じて実施
データ移行	・校務、学習ファイルサーバデータ ・メールデータ
システム移行	・Web サーバ、DNS サーバ ・図書館システム ・資産管理システム ・自動採点システム用ファイルサーバ ・グループウェア
端末移行	78 台
機器調達	ファイアウォール（1 台）
機器設計/設定/試験	ファイヤウォール（1 台）

2. 業務委託内容

2.1. 前提条件

本件の受注者は別途契約する保守業務も実施可能であること。なお、構築から一貫性をもってセキュリティ対策を望むため、SOC 業務については受注者自らが可能であること。

2.2. プロジェクト管理業務

本調達の遂行にあたっては下記の業務を実施すること。

- 本システムの導入における具体的な体制、スケジュール、プロジェクト管理方針、プロジェクト管理方法等を含んだ「プロジェクト計画書」を作成すること。
- プロジェクト計画策定時に定義したスケジュールに基づく進捗管理を実施すること。
- プロジェクト計画策定時に定義した方針に基づくリスク管理を実施すること。

2.3. 設計、構築業務

本書で示す、新たな教育 ICT 環境の各種要件に基づき基本設計・詳細設計を行い、設計内容に基づき、環境を構築すること。

2.4. テスト業務

新たに導入する全ての機能等のテストを行うこと。そのうえで、校務系端末、校内ネットワーク機器や回線を含めた新たな校務系 ICT 環境の全体的な総合テストを、各関連事業者と連携のうえ実施すること。

各テストの実施にあたっては、計画策定、テスト実施、テスト結果の報告作成を行うこと。また、テストにあたっては、必要に応じて学校に訪問し、学校からの新たな校務系 ICT 環境への接続及び利用確認のための実地検証を実施すること。

2.5. 移行、切替業務

「移行・切替計画書」を作成し、発注者の承認のうえ移行及び切替を実施すること。実

施にあたり、移行及び切替に関する事前検証、テストなどにより、確実な移行及び切替を行うために必要な対策を採用するとともに、学校現場の授業や学習環境、教職員の校務にできる限り影響を及ぼさないよう配慮すること。

2.6. 研修業務

新たな校務系 ICT 環境を使用する教職員に対して、校務系 ICT 環境を教職員が存分に活用できるよう、契約期間内で教職員向けに研修を 1 回実施すること。研修用の資料は受注者にて作成し、事前に発注者の承認を得ること。

2.7. 保守運用業務

新教育 ICT ネットワーク環境の安定的な運用を目的として、保守運用業務を行うこと。不具合発生時に早急な原因究明や復旧対応を可能にするために、今回の調達で整備される機器・クラウドサービスについて、発注者からの問い合わせ及び、不具合対応依頼に対して、調査・回答及び復旧対応を受注者自らが実施すること。また、教育委員会に関する SOC 業務の実績を、発注者に提出すること。それらに必要な運用保守マニュアルを作成すること。

新教育ネットワークに関するクラウドサービスについては、SOC 業務を実施するとともに、運用代行業務を行うこと。運用代行には本業務で整備したクラウドサービスに関わる端末やユーザ情報に関連した業務も含まれることとする。

保守運用業務の主な実施事項は 7.運用・保守要件（参考）に記載の通りとし、別途契約とする。

2.8. 納品物

本業務の納品物を以下に示す。次の資料を紙媒体（1 部）および電子データで提出すること。またいずれの納品物も発注者が様式及びファイル形式を指定した場合は、当該様式及びファイル形式で提出すること。

【納品物一覧】

納品物	備考
プロジェクト計画書	
基本設計書	

詳細設計書	パラメータシート
試験成績報告書	
利用者マニュアル	教職員、管理者向け
構成図	システム構成図、IP アドレス管理表
システム運用ドキュメント	システム運用簡易マニュアル
納品物一覧	ライセンス証書など

3. セキュリティ基盤　基本仕様

新教育ネットワークにあたっては、「教職員の業務効率化」と「セキュリティ対策」の両立を目的に、アクセス制御モデルでの校務系システムを構築することとする。本件で構築する機能を以下に示す。

構築期間中に構築事業者が必要なライセンスについては本業務の費用に含めること。

3.1. IDaaS（認証）

「Microsoft Entra ID Plan 2」の機能により以下のことが実装できること。

（1）アカウント管理

新校務系ネットワークにおける教職員のアカウント情報及び、各種システムへの権限設定に必要なセキュリティグループを作成できること。また、教職員アカウントについては管理職ユーザと一般教職員ユーザを区別して管理し、管理職ユーザのみアクセスすることができるようなデータ領域や暗号化の権限設定等が可能とすること。

（2）認証管理

新校務系ネットワークにおける認証については、端末起動時において「BitLocker による PIN」と「Windows Hello for Business」の機能による多要素認証が実装可能であること。認証情報（パスワード等）については、教職員自身で変更することができることとし、変更の際に「個人のスマートフォン」以外でも対応が可能とすること。

（3）SSO（シングルサインオン）機能

新校務系ネットワークにおけるその他システムにおいてＳＡＭＬ認証連携が可能な場合、シングルサインオンが実装可能であること。

※ＳＡＭＬ認証連携に必要な設定情報については、その他システム事業者からの提供とし対象デバイスは Windows とする。

（4）アクセス制御機能

新校務系ネットワークにおける基本サービス（Microsoft365）へのアクセス（接続）について学校管理デバイスのみアクセスを許可し、個人所有端末などの学校管理デバイス以外からの接続ができないよう Intune と連携し制御を実装可能であること。

（５）リスクベース認証

「Identity Protection」の機能を利用し、アカウント ID に関するリスクの検出・管理・脅威からの保護を実施することとし、リスクが高い場合追加の認証が要求される設定が実装可能であること。

3.2. EMM（端末管理）

「Microsoft Intune」の機能により以下のことが実装できること。

（１）Windows 端末のデバイス管理

新校務系ネットワークにおける基本サービス（Microsoft365）で端末管理ができるようデバイス登録が可能であり、デバイスの登録については、学校管理デバイス以外の登録ができないようにするなど、セキュリティ対策が実装可能であること。

（２）Windows 端末の Windows Update の管理（パッチ配信管理）

新校務系ネットワークにおける管理対象の Windows 端末について自動で Windows Update の管理（パッチ配信管理）が行えるよう設定が実装可能であること。

なお、配信については、「先行配信グループ」と「本番配信グループ」の二つのグループを作成し 0～30 日間の範囲で差をつける設定が実装可能であること。

（３）アプリケーション（ソフト）の配信

新校務系ネットワークで利用するアプリケーション（ソフト）を管理センターから対象端末を選択し配信可能であること。対象はサイレントインストール対応のアプリケーションとする。また、配布するアプリケーションは発注者と協議し決定すること。

（４）セキュリティポリシーの適用

校務端末でのセキュリティとして、以下の設定が実装可能であること。

・Windows ファイアウォール
・Bitlocker
・Bluetooth の機能制御
・サインイン時の表示設定

（５）外部記憶媒体制御

校務端末での外部記憶媒体（USB デバイス等）を接続した利用を禁止する設定が実装可

能であること。発注者が許可したUSBデバイス等については、許可したユーザで利用できる設定が実装可能であること。

（6）Windows端末の遠隔操作

管理対象のWindows端末は遠隔から管理者が操作できるように設定を実施すること。遠隔操作は特定のユーザ・グループのみ利用できる設定が実装可能であること。

3.3. EPP/EDR（脅威検知）

「Microsoft Defender for Endpoint P2」の機能により以下のことが実装可能であること。

（1）脅威検知

- 既知のマルウェア情報が登録されたシグネチャベースでの検知を行うこと。校務系端末に配布するシグネチャはインターネット上のサイトより取得し、配信は1日1回行うなど管理が可能であること
- リアルタイム（ファイル操作や実行時）スキャンや一括スキャンが実施可能であること。
- 脅威の検出は、機械学習などの先進的な技術を用いて、ファイルや端末の悪意ある挙動（振る舞い）に基づき検出が可能であること。

（2）脅威対応

- 脅威検知後の対応（通知、実行のブロック、通信遮断、ファイル除去、調査・分析、復旧等）について定義が可能であること。
- 脅威を検出した際に、被害拡大を防止するため、当該端末の通信を論理的に遮断し、隔離できることとし、隔離された端末の問題が解消した後、元の通信状態に戻すことができること。
- 脅威の検出結果や端末の状態を可視化するダッシュボード機能を有すること。

3.4. CASB（クラウド監視）

「Microsoft Defender for Cloud Apps」の機能により以下のことが実装可能であること。

（1）シャドーITの可視化

・　クラウドサービスの利用状況を把握し承認していないシャドーIT の検出が可能であること。

（2）脅威検知

・　不審なファイルアップロードの対策
1 日あたりに規定値を越える大容量ファイルをクラウドアプリケーションへアップロードした場合にアラート発報が行える設定が実装可能であること。

・　不審なファイルダウンロードの対策
単一のユーザが SharePoint/OneDrive から規定値を超える異常なダウンロードを行った場合に、アラート発報が行える設定が実装可能であること。

3.5. IRM（情報漏洩）

「Microsoft Purview Information Protection」を利用して以下のことが実装可能であること。下記の内容が「Microsoft Purview Information Protection」で実現が困難な場合は、3rdParty アプリを組み合わせて実装が可能であること。3rdParty アプリを選定する場合は、SaaS サービスを選定することとし、契約期間中のサービス利用が可能となるようにすること。

例示品：Actsecure FileShell

数量：78 アカウント

（1）情報ラベルの作成（秘密度ラベル）

・　文部科学省策定の「教育情報セキュリティポリシーに関するガイドライン」に基づき、発注者と協議の上、秘密度ラベルが実装可能であること。下記に秘密度ラベルの例を示す。

No	秘密度ラベル	ガイドライン対応
1	重要性分類Ⅰ	Ⅰ　セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。
2	重要性分類Ⅱ	Ⅱ　セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。
3	重要性分類Ⅲ	Ⅲ　セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。
4	重要性分類Ⅳ	Ⅳ　影響をほとんど及ぼさない。

・　発注者と協議の上、秘密度ラベルごとにアクセス権の設定が実装可能であること。

No	秘密度ラベル	暗号化	ファイル操作	ラベルの変更
1	重要性分類Ⅰ	あり	特別なユーザ	特別なユーザ
2	重要性分類Ⅱ	あり	特別なユーザ	特別なユーザ
3	重要性分類Ⅲ	あり	すべてのユーザ	すべてのユーザ
4	重要性分類Ⅳ	なし	すべてのユーザ	すべてのユーザ

（2）秘密度ラベルについて

・　秘密度ラベルを付与した状態で、SharePoint Online や OneDrive へアップロード可能であり、SharePoint Online や OneDrive 上からローカルアプリによって開くことが可能であること。
・　秘密度ラベルは原則 Microsoft Purview Information Protection を利用するものとし、3rdParty アプリを利用する場合は、Microsoft Purview Information Protection と連携できること。また、EntraID とも連携し、EntraID 上のユーザやグループごとに権限付与が可能であること。

（3）秘密度ラベルの付与設定について

■手動ラベル付けポリシー

すべての教職員が新規に下記の表 1 の拡張子のファイルを作成する際に、既定のラベルとして秘密度ラベルを付与可能であること。

・　手動にてラベルを付与することが可能であること。
・　手動にてラベルの変更や取外しが可能であること。

■自動ラベル付けポリシー

・　保護対象であるファイルを自動的に分類/保護する動作は、新規作成や更新、ファイル・フォルダーの移動やコピー動作により、自動適用対象フォルダの配下にファイルを保存した場合に自動でラベルを付与可能であること。
・　保護対象となるファイルを検知してから、5 秒程度でファイルの分類/保護が可能であること。
・　クライアント端末のローカルディスク上を巡回し、ファイルの分類/保護を実行可能であること。

（4）ファイル分類/保護に対応する拡張子

・　下記の表の拡張子のファイルに秘密度ラベルが適用可能であること。

・　下記の表の拡張子ファイルを暗号化した際に拡張子が変わらないこと。

ファイル形式	ファイル拡張子
Microsoft Office ファイル（word）	doc,docx,docm
Microsoft Office ファイル（excel）	xls,xlsx,xlsm
Microsoft Office ファイル（powerpoint）	ppt,pptx,pptm
テキストファイル	txt
CSV ファイル	csv
画像系ファイル	jpg,jpeg,jfif,tif,png,bmp,dib,gif
PDF ファイル	pdf

上記以外のファイルについては、発注者と協議すること。

（5）クライアント端末について

秘密度ラベルの適用に向けて、校務端末にクライアントアプリインストールが必要になる場合は、手順書を作成し、「校務管理システム環境構築業務」の受注者と連携の上インストールと利用設定を実施することとし、必要な費用は本業務に含めること。

（6）ログについて

・　ファイルに関する以下の動作についてログを取得可能であること。
  - ファイル保護
  - 保護解除
  - 保護されたファイルの閲覧
  - 設定変更

・　ポリシー受信履歴が確認可能であること。

・　ログ発生から 1 年間は保存されること。

3.6. DLP（データ損失）

「Data Loss Prevention」の機能により以下のことを実装できること。

（1）エンドポイント DLP ポリシー

・　データ損失防止

重要性分類Ⅰ、重要性分類Ⅱ、重要性分類Ⅲが適用されたファイル、ラベルが付与さ

れていないファイルについて以下の条件における動作をブロック可能であること。

- 「MicrosoftEdge、Chrome」以外のブラウザからのファイルアップロード
- 「MicrosoftEdge、Chrome」からのホワイトリスト形式で許可されていないサイトへのファイルアップロード
- 外部記憶媒体へのコピー
- ネットワーク共有へのコピー
- ドキュメントの印刷
- クリップボードへのコピー

（2）ExchangeDLP ポリシー

メール作成時、秘密度ラベル（暗号化）の付いたファイルを送付する際に、送信禁止の制御及び送信時における送信確認が可能なこと。

3.7. SWG

以下のことが実装可能であること。実装にあたり必要なライセンスを調達し、契約期間中のサービス利用が可能となるようにすること。

例示品：Microsoft Entra Internet Access

数量：78

（1）プロキシ機能

インターネットへの通信をプロキシ経由とすることにより、教職員毎での Web 接続の通信履歴が確認できること。

（2）送信元 IP 復元機能

Entra ID での条件付きアクセスで Microsoft 365 サービスへの通信において、送信元 IP アドレスで通信が可能であること。

（3）バイパス機能

インターネットへの通信において、送信元の IP アドレスで接続制限を実施しているサイトに対してプロキシ経由ではなく（バイパス）直接接続の設定が可能とすること。

（4）管理機能

設定やログ等の画面は Microsoft 365 と連携し、同じ管理画面から遷移することが可能であること。

3.8. 校務系メール（メール）

校務系メールとは、発注者により認められた場合に利用できる校務用のメール機能とする。「Exchange Online Plan 2」の機能により以下のことを実装可能であること。

（1）校務系メール

- 校務系メールとは、教職員と業務上必要と発注者により認められた場合に利用できる校務用のメール機能とする。
- カスタムドメイン利用、セキュリティ機能（ＳＰＦ、ＤＫＩＭ、ＤＭＡＲＣ 等)関連のレコードの変更登録に関して外部 DNS 管理事業者へ必要な情報を提供すること。
- 本メールの利用は校務系端末から Microsoft Outlook アプリによる利用とし、校務系端末へのログイン情報と連携し、自動認証機能によりアカウント・パスワードを入力せずとも自身のメールボックスを利用できる設定が実装可能であること。
- アドレス帳については教職員の情報を検索・利用できることとする。

（2）メールセキュリティ

- 送信スパム対策ポリシー
  メール送信がブロックされた場合アラートが通知させる機能を実装すること。
- 受信スパム、マルウェア、フィッシング対策ポリシー
  マルウェアを検知した場合アラートを通知させる機能を実装すること。
  スパムメールを検知した場合、メッセージを検疫する設定を実装すること。
- 添付ファイル対策
  添付ファイルをサンドボックスによるスキャンを実施する設定が実装可能であること。なおサンドボックスによるスキャンについては、SharePoint Online、OneDrive for Business、Teams にも同様の設定を実装可能であること。
- URL リンク対策
  メール本文や添付ファイル内に含まれる悪意のある URL へのリンクを検知し、アクセスを動的にブロックする設定が実装可能であること。
- 電子メール内の URL 書き換え機能を実装可能であること。

3.9. ファイルストレージ

ファイルストレージとは、教職員の個人作成データの保存領域、校内で共有するデータの保存領域の機能とする。「SharePoint Online Plan 2、OneDrive for Business」の機能に

より以下のことが実装可能であること。

（1）個人用保存領域
- OneDrive を利用することとし、校務系端末からであればどのネットワークからでもアクセス可能とすること。
- 個人用の保存領域の容量を指定可能なこと。

（2）学校保存領域
- SharePoint Online を利用することとし、既存のファイル構成に併せてファイルストレージサイトを構築すること。
- ファイルストレージサイトは、現行のエクスプローラーと類似されたデザイン構成とし、ドキュメントフォルダのみ利用できる構成とすること。
- 学校毎で作成されたサイト毎にアクセス権限設定を実施すること。
- サイト内でのドキュメントフォルダに対して、校内の指定されたアカウントのみアクセス可能となるよう設定をすること。
- 本サイトへのアクセス権限については、『4.1.iDaaS（認証）』と連携し、教職員の人事異動に伴い自動的にアクセス権の付与・削除が行えるように実施すること。

3.10. Teams（コミュニケーション）

「Microsoft Teams」の機能により以下のことを実現すること。

（1）チーム・チャネル
- 学校で利用するチームの利用環境（権限・機能）について設計・設定を実施すること。

（2）チャット機能
- チャット機能が利用できる範囲など設計・設定を実施すること。
- チーム所有者がメッセージの削除を可能とすること。

（3）Web 会議
- Web 会議では外部機関に対して「匿名ユーザ」での参加を可能とし、匿名ユーザは参加を許可するまでロビーで待機させる設定とすること。
- コンテンツ共有(画面共有)、クラウドレコーディングについては、組織内のユーザの

み実施すること。

（4）チームの作成
・　発注者と協議しチームを作成すること。

4. 移行要件

4.1. ネットワーク移行

クラウド環境への移行が実施されたことによって、現環境の UTM や L3SW などのネットワーク機器に設定変更等が生じた場合は既存保守事業者と連携の上、設定変更を行うこととし、それらの設定変更作業にかかる費用は本事業に含めること。

4.2. データ移行

4.2.1. 校務、学習ファイルサーバデータ移行

・　現在、既存の校務ファイルサーバ・校務 NAS・学習ファイルサーバ・学習 NAS 上のデータを SharePoint Online 上への移行を実施すること。
・　現在保有するデータのうち、移行を必要とするものの確認、SharePoint Online の設計に基づくデータの移行先について、発注者と協議の上これを決定すること。
・　移行にあたり、サイトのアクセス権を設計し設定すること。

4.2.2. メールデータ移行

新メールシステムを利用するための手順書を作成すること。

4.3. システム移行

4.3.1. Web サーバ、DNS サーバ、メールサーバ

現在オンプレサーバにて運用している Web サーバ、DNS サーバをクラウドサーバへの移行を実施すること。また、契約期間中のサービス利用が可能となるようにすること。

（1）Web サーバ移行

- 現行サーバ内の HP コンテンツを移行すること。
- SSL 証明書の発行、インストールを実施し、有効化すること。設定作業に関わる費用は本契約に含めること。
- Web サーバのホスト名およびドメイン名は変更の無いこと。

（2）DNS サーバ移行

- DNS サーバのゾーン情報を新たな構成に変更すること。受注者は、パラメータを提出すること。
- ドメインは既存のドメイン名を利用すること。

（3）メールサーバ移行

- 既存のメールサーバから 4.8.校務系メールで構築するメールサーバにメールの送受信ルートを移行すること。
- ドメインは既存のドメイン名を利用すること。
- 現行の運用を引き継げるようにメールユーザ及びメーリングリストも移行または新規作成すること。

（4）クラウドサーバ　基本要件

- クラウドサーバ提供事業者はプライバシーマークを取得していること。
- クラウドサーバ提供事業者は ISMS クラウドセキュリティ認証を取得していること。
- 独自ドメインを割り当てられること
- ストレージ容量は 900GB 以上を有すること。
- SSL 証明書に対応すること。
- CMS として Wordpress が利用できること。

（5）セキュリティ要件

- サイトへの攻撃を検知し、ブロックするウェブアプリケーションファイアウォールを利用できること。
- 国外の IP アドレスからのアクセスを制限することができること。

4.3.2. 図書館システム

現在オンプレサーバにて運用している図書館システム（探検隊）を「校務管理システム

用機器等賃貸借業務」にて調達するサーバに移行すること。また、図書館システムを利用する端末のキッティングも受注者が実施すること。それらの作業にかかる費用は本事業に含めること。

4.3.3. 資産管理システム

現在オンプレサーバにて運用している資産管理システム（SKYSEA client View）を「校務管理システム用機器等賃貸借業務」にて調達するサーバに移行すること。また、資産管理システムを利用する端末のキッティングも受注者が実施すること。それらの作業にかかる費用は本事業に含めること。

4.3.4. 自動採点用ファイルサーバ

現在クラウドサービスを利用して運用している自動採点システム（百問繚乱）のデータ保存領域を「校務管理システム用機器等賃貸借業務」にて調達するサーバ（自動採点システム用ファイルサーバ）に移行すること。それらの作業にかかる費用は本事業に含めること。

4.3.5. グループウェア

現在オンプレサーバにて運用しているグループウェア（スクールエンジン）をクラウド環境に移行することとし、2027 年 3 月 1 日から利用できるようにすること。移行に必要な環境構築やデータ移行作業及び 2027 年 3 月 1 日から 1 年間利用できるライセンス費用を本事業に含めることとする。

4.4. 端末移行

（1）新旧端末の入替について

「校務管理システム用機器等賃貸借業務」にて調達する端末設定のうち、セキュリティ基盤に関連する設定は受注者が全てを請け負うこと。

（2）旧端末のデータ移行

新端末への旧端末データの移行は各自教職員が実施することとし、必要に応じて移行手順書を作成することとする。

5.機器調達

5-1.ファイアウォール

- 例示品：Fortinet 社製/Fortigate 120G
- 数量：1 台

項目	仕様
ハードウェア	・ 1GbE RJ-45インターフェースが16ポート以上有すること。 ・ 1GbE RJ-45 Management/HA用インターフェースをそれぞれ1ポート以上有すること。 ・ 10/GE SFP＋ fortiLink Slotを8ポート以上有すること ・ SFPポートを8ポート有すること。 ・ RJ-45インターフェースのコンソールポートを1ポート以上有すること。
パフォーマンス	・ IPS スループットはエンタープライズ混合テストかつログを有効にした状態で 5.3Gbps 以上であること。 ・ NGFW スループットはエンタープライズ混合テストかつログを有効にした状態で 3.1Gbps 以上であること。 ・ 同時セッションは TCP で最大 3M 以上であること。 ・ 新規セッションは TCP で毎秒最大 140,000 であること。 ・ ゲートウェイ間の IPsec VPN トンネルは最大 2000 以上接続できること。 ・ クライアント-ゲートウェイ間の IPsec VPN トンネルは最大 16000 以上であること。 ・ SSL インスペクションのスループットは HTTPS を利用し、IPS を実施した際の平均値が 3Gbps 以上であること。
セキュリティ	・ 下記の機能を含むライセンスを令和 14 年 3 月末まで含めること。 ・ ファイアウォールポリシーは最大 10,000 以上設定できること。 ・ セキュリティ機能としてファイアウォール機能、次世代ファイアウォール機能(アプリケーション制御) 、VPN 機能に加

	え、オプションとして不正侵入検知機能(IPS) 、アンチウイルス機能、Web フィルタリング機能、アンチスパム機能、DNS フィルタ機能の利用が可能であること。 ・ ファイアウォールのポリシー単位でプロファイルを適用することで、ユーザーやグループ、アプリケーション、アンチウイルス、アンチスパム、IPS、Web フィルタリング、DNS フィルタリングの設定できること。 ・ 各種シグネチャ・エンジンは自社開発であること。 ・ IPS 機能はユーザーが個別でシグネチャを設定（カスタムシグネチャ）できる機能を有すること。 ・ 80 カテゴリー以上のデータベースを持ち、カテゴリーごとに設定可能な Web フィルタリング機能を有すること。 ・ 仮想システムを利用することにより L3 型ファイアウォールと L2 型ファイアウォールが 1 台で混在可能なこと。 ・ 2,000 以上のアプリケーションを識別し遮断が可能なこと。 ・ 10,000 以上の IPS のシグネチャを有すること。
管理機能	・ https 対応の Web インターフェースを有し、それ以外に SSH による遠隔保守が可能であること。 ・ WebUI は日本語対応していること。 ・ WebUI 上でコマンドラインインターフェースを利用可能なこと。 ・ 複数の異なるバージョンの OS を保存できること。 ・ 複数台のファイアウォールのファームウェア、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。
保守サポート	・ メーカーの先出センドバック保守が令和 14 年 3 月末まで含めること。

6.機器設計/設定/設置

・ 5. 機器調達で調達するファイアウォールは発注者拠点で運用している既存ファイアウォールと同様の動作となるように設定すること。
※なお既存ファイアウォールは 5. 機器調達に記載の例示品とは機種が異なる。

・　セキュリティ機能に関しては、発注者と協議のうえ、設計及び設定を実施すること。
・　発注者の指定する場所に機器を設置すること。

7. 運用・保守要件（参考）

保守運用業務は「ゼロトラストセキュリティ保守運用業務」で別途契約とする。

7.1. SOC（セキュリティオペレーションサービス）

下記のセキュリティオペレーションサービスを提供すること

No.	機能	概要
1	EDR 監視分析	EDR の常時監視、ネットワーク遮断、アラート分析を実施します
2	SWG ログ調査	インシデント発生時のログ調査、追跡を実施します
3	IRM/DLP ログ調査	インシデント発生時のログ調査、追跡を実施します
4	Microsoft 365 監査ログ提供	インシデント疑いがある場合に指定期間・条件における監視ログを提供します

7.2. EDR 監視分析

EDR を常時監視し、危険度の高いアラート発生時には、端末の通信を遮断し、ネットワークから隔離します。隔離後、端末の分析および脅威ファイルが発見された場合は遠隔から当該ファイルを除去すること。

下記の内容を実施すること。

対応項目	対応時間
監視・アラート通知	24 時間 365 日対応
ネットワーク遮断	24 時間 365 日対応
アラート分析	平日 9-17 時対応
脅威ファイル除去	平日 9-17 時対応 ※自動除去は 24 時間 365 日対応
ネットワーク遮断解除	平日 9-17 時対応
アラートチューニング	平日 9-17 時対応

（1）監視・アラート通知

管理ポータルから監視を実施し、アラート検知時に発注者へ通知すること。

（2）ネットワーク遮断

危険度の高いアラートを検知した場合、該当端末を論理的にネットワークから隔離すること。

（3）アラート分析

- 危険度の高いアラートについて分析を実施すること。
- アラート内容の確認及びアラート名・被害端末情報をメール通知すること。
- 検知したアラートの原因調査を実施すること。
- 検知したアラートに含まれるファイルまたはウェブサイトが悪性かどうかを確認すること。
- マルウェアの場合、該当端末が外部と通信しているのか確認すること。
- 必要に応じて発注者へのヒアリングを実施すること。

（4）ネットワーク遮断解除

発注者からの依頼に基づき、遮断した該当端末のネットワーク遮断を解除すること。

（5）アラートチューニング

無害なアラート（過検知）に対する抑止ルールを設定（アラート非通知の設定）すること。ログの保存期間は発注者と受注者で協議の上決定する。

7.3. SWG ログ調査

EDR で危険度の高いアラートを検知した場合、SWG（Entra Internet Access）のログを追跡調査すること。

（1）追跡調査対応

- Entra Internet Access のログより以下を確認すること。
  - フィッシングサイトや C2 サーバ等外部不審サイトとの通信有無および成功可否
  - 当該サイトへのアクセス履歴（EDR アラート発生端末以外含む）
  - ログの保存期間は発注者と受注者で協議の上決定する。

7.4. IRM/DLP ログ調査

EDR で危険度の高いアラートを検知かつ外部へのファイル送信が行われている場合に IRM/DLP のログを追跡調査すること。

（1）追跡調査対応
EDR で検知したインシデントに関して、該当の通信状況や動作状況を確認すること。ログの保存期間は発注者と受注者で協議の上決定する。

（2）ファイル一覧提示
機密情報の漏えい疑いがある場合は、発注者からの依頼に基づき、指定された期間においてラベル変更されたファイルの一覧を提示すること。ログの保存期間は発注者と受注者で協議の上決定する。

7.5. Microsoft 365 監査ログ提供

指定された期間の Microsoft 365 監査ログを提示すること。
（1）監査ログ提示
インシデントの疑いがある場合に発注者からの依頼に基づき、指定された期間・条件の監査ログを提示すること。ログの保存期間は発注者と受注者で協議の上決定する。

7.6. 月次レポート

月次レポートを作成し専用ポータルサイトにて確認できること。
（1）セキュリティオペレーションサービス
・　セキュリティオペレーション対応状況
（2）ネットワークオペレーションサービス
・　ヘルプデスク（ゼロトラスト）の対応状況
・　運用代行サービスの対応状況
・　端末に関する情報
・　セキュリティ対策状況
・　グループウェアの利用状況

7.7. SSO 連携管理

（1）証明書更新
・　3rdParty アプリケーションとの SSO 連携に使用する証明書の更新を実施すること。
（2）SSO 連携追加の作業アカウント払い出し

・　作業時に受注者にアカウントを払い出す。作業のアカウントは削除すること。

7.8. Windows パッチ配信

品質更新プログラム（QU）/機能更新プログラム（FU）の配信停止・再開

・　動作検証にて不具合が見つかった場合、発注者からの申請に基づいてパッチ配信を停止すること
・　発注者からの申請により、配信処理の再開を実施すること

7.9. アプリインストール作業

・　発注者からの依頼に基づき、校内で管理している端末に対しアプリケーションのインストールを実施すること。
・　「共有 PC 向け環境保護ソフト」導入端末においては、保護状態を一時解除し、アプリインストールの配信およびアップデートを実施後に保護状態に戻すこと。

7.10. Web アクセス管理

（1）Web フィルタリング ホワイト/ブラックリストの登録

・　発注者からの依頼に基づき、対象サイトをホワイトリスト・ブラックリストに登録すること。セキュリティレベルを合わせるために Entra Internet Access、GIGA 端末で利用している Web フィルタリング、UTM で同等の設定を登録すること。（発注者から禁止/許可する Web サイトの情報を提供する。）
・　Entra Internet Access 機能により Web アクセス制御を実施すること。

（2）バイパス設定

・　Entra Internet Access を介さず Web アクセスする場合、発注者の依頼に基づき当該 Web サイトをバイパスする設定を実施すること。

（3）テナント制御

・　Entra Internet Access で Microsoft 365 の自テナント以外にアクセスしたい場合、発注者の依頼に基づき当該テナントへのアクセスを許可する設定を実施すること。

7.11. メールセキュリティ管理

（1）フィッシング/迷惑メール管理

- 発注者の依頼に基づき、検知ボックスに格納されたメールの配送を実施すること
  - 過検知の場合、発注者の依頼に基づき、ホワイトリスト登録を実施すること。

7.12. GIGA 端末の年次更新処理

- 年次更新時に不要となるユーザプロファイルを削除すること。
- 校内で管理している端末の windows アップデートをオンサイトに 2 月～3 月に実施すること。その際に故障して取り換えた GIGA 端末があれば再セットアップを実施すること。

7.13. システムログ・トラフィック調査

- 発注者からの依頼に基づき、校内で管理している端末のシステムログを確認し、提示すること。
- 発注者から依頼に基づき、指定期間のトラフィック追跡を実施し、提示すること。

8. その他

- 現環境の学校内のデータセンターネットワーク接続用機器、データセンター内の学校ネットワーク接続用機器、データセンター内のネットワーク機器やサーバの撤去すること。また、撤去物品は受注者の指定する場所に移動すること。