生駒市教育系ネットワーク構築・維持管理等業務仕様書

目次

1. 業務概要

1.1. 業務件名

生駒市教育系ネットワーク構築・維持管理等業務

1.2. 業務目的

令和３年５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。本市では、校務系及び学習系ネットワークはセンター集約型の構成となっているが、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す。

1.3. 業務方針

本事業の実施にあたり、以下の項目に関する事項に留意すること。

(1) ネットワーク分離を必要とせず認証によるアクセス制御を前提とした、新たな教育情報ネットワークを実現する。

(2) 教職員の柔軟な働き方のため、PC１台及び iPad１台で、校務系ネットワーク及び学習系ネットワークに接続でき、学校内だけでなく、自宅に持ち帰っても安全に利用できる環境を整備する。また、学校での運用を考慮し、端末は１教員あたり２台とする。教員の業務内容を考慮し機器選定・運用提案すること。

1.4. 選定方法

公募型プロポーザル方式

1.5. 契約方法及び支払方法

(1) 契約方法

ア Microsoft 365 A5 ライセンス

令和６年９月１日～令和７年３月３１日の構築に関わる７か月分のライセンス利用料は、受託者が「イ　教育系ネットワークシステム更新構築」に含めること。上記期間中は、本市教職員がインストールアプリ版の Office（Excel、Word、PowerPoint は必須とする。）を利用できるようにすること。また、令和７年４月１日～令和１２年１月３１日のライセンス利用料は「エ　教育系ネットワークシステム運用保守」に含めること。

イ 教育系ネットワークシステム更新構築

初年度の構築にかかる役務部分については、選定により受託候補者（以下「受託候補者」という。）となったものと契約する。

ウ 端末リース

「1.7.調達範囲」に示す教員用ノート PC 及び教員用 iPad はリース対象物件とする。受託候補者が提出した提案書記載のリース会社と本市での２社契約を行う。教員用ノート PC と教員用 iPad のリース会社は別業者でも構わない。

エ　教育系ネットワークシステム運用保守

受託候補者と契約する。

(2)　支払方法等

(1)　契約方法　イ　教育系ネットワークシステム更新構築は、完了払いとする。(1)契約方法　ウ　端末リースのリース料は、毎月払いとする。なお、リース料の支払いは令和７年２月から支払開始とする予定である。エ　教育系ネットワークシステム運用保守の運用保守料は毎月月額払いとする。具体的な契約内容、支払開始日及び支払い方法等は、受託者と協議の上決定する。

1.6. 全体構成

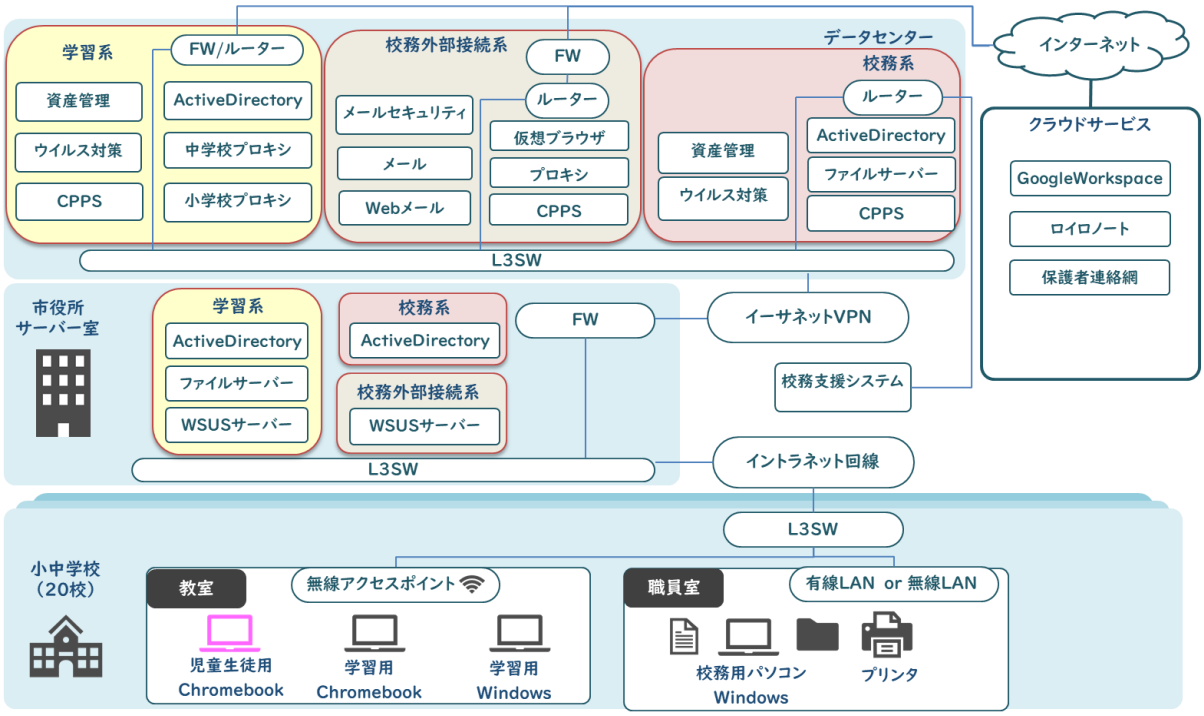
現在の全体構成のイメージを図１．全体構成概念図に示す。現状、「学習系」、「校務外部接続系」、「校務系」の３分離となっているが、本業務ではネットワーク統合を目指している。

本業務は、Microsoft 365 A5 のサービスを活用したクラウド基盤システムによるゼロトラスト型セキュリティネットワーク構成とすること。

校内ネットワークは、ＧＩＧＡスクール構想にて整備済である。新システムの導入にあたり、整備済みの機器等に設計変更の必要が生じる場合は、設計費用を本業務に含めること。各拠点機器への現地設定変更費用は、別途本市にて準備する。

校務支援システムは、奈良県域共同調達により令和７年４月１日から新たに構築される予定であるため、奈良県域共同調達による校務支援システムの仕様等を受託者において確認し、本業務で整備する教職員用端末から利用可能な環境を構築すること。

図 1. 全体構成概念図



1.7. 調達範囲

1.7.1. ハードウェア・ソフトウェアの調達

下表にあるソフトウェアを調達すること。

No.	品名	数量	備考
1	Microsoft 365 A5 Unified Edu Sub Per User（Microsoft 365 A5 Education faculty）	８００式	学生無償ライセンス特典“Student Use Benefit”が利用できること。
2	操作ログ管理サービス	１式	
3	コンテンツ（デジタル教科書）配信システム	１式	
4	ファイアウォール（小中学校）（搭載 EMMC のストレージが 128GB 以上であること。）	２０台	数量には予備機１台を含む。ラックマウントキット（予備機１台分には不要）、５年保守ライセンスも含めること。
5	ファイアウォール（その他）（搭載 EMMC のストレージが 64GB 以上であること。）	４台	ラックマウントキット、５年保守ライセンスも含めること。

6	ファイアウォール クラウド管理ツール	１式	
7	教員用ノート PC	８００式	PC 本体はリースにすること。提案書に契約締結を行うリース会社を明記すること。 各対象施設への搬入設置費用も含めること。
8	無線マウス（光学式）	８００式	動作に必要な電池を付属すること。
9	教員用 iPad	８００式	iPad 本体は AFS（Apple Financial Services）を利用すること。なお、AFS が難しい場合はリースでも可とするが、AFS と同等の保証条件とすること。提案書に契約締結を行うリース会社を明記すること。 各対象施設への搬入設置費用も含めること。
10	Jamf Pro iOS 教育機関用クラウド	８００式	
11	Jamf Pro iOS 技術支援サービス（６インシデント/１年）	５年	
12	Apple TV 4K 64GB ストレージ搭載 Wi-Fi モデル	３７８台	設置・設定作業は不要。
13	Aruba AP-515 (JP) Unified AP	３５台	AP mount bracket も含めること。 HPE ファウンデーションケア Exchange5 年 AP-515 用も含めること。 設定作業費用も含めること。 設置作業は不要。
14	PoE スイッチングハブ （参考型番：BS-GS2016P/HP）	１０台	５年保守も含めること。 設定作業費用も含めること。

No.2～10・12 の調達項目の要件は別紙「ハードウェア・ソフトウェア仕様」記載内容を満たすこと。調達物品については、品名、型番、メーカー、数量、保証の有無、保証内容、見積金額等がわかる内訳明細書を作成すること。また、物品管理及び学校からの問い合わせに対応できるよう、管理番号等を記載したラベルを貼り付けること。

その他にも、ゼロトラストセキュリティを実現するために必要なサービスがあれば全て見積に含めること。また、保守やライセンス等は構築期間についても見込むこと。

1.7.2. 構築業務委託

仕様書に基づき、受託者及び本市双方による協議を行い、構築に必要な業務を行うこと。

(1) プロジェクト管理
(2) 要件定義
(3) 各拠点－クラウド間接続環境整備
(4) ネットワーク設計　設計変更
(5) システム調達
(6) システム構築
(7) ハードウェア調達
(8) ハードウェア導入作業
(9) マニュアル作成

1.7.3. 運用保守業務委託

仕様書に基づき、受託者及び本市双方による協議を行い、運用保守に必要な業務を行うこと。

(1) ヘルプデスク対応
(2) ソフトウェア保守
(3) ハードウェア保守
(4) 研修会の実施
(5) 定例会の実施
(6) その他

1.7.4. その他

(1) 本業務を実現するにあたり、受託者が提案する構成を実現するために必要なハードウェア・ソフトウェア・ライセンス等が別途必要な場合はあわせて調達すること。
(2) 業務管理者（PM）又は主任技術者（PL）が、マイクロソフトからサポート支援を受けられること。なお、マイクロソフトの法人向けマイクロソフトユニファイドサポート契約による支援を得られることが好ましい。
(3) 本市と同等規模以上の自治体において、Microsoft 365 A5(A5 Security)及び Azure 上に構築された IaaS 基盤に関する運用保守業務の実績を保有すること。

1.8. スケジュール

(1) 現行システム契約期間　令和７年３月３１日まで
(2) 新システムの構築期間　契約締結日から令和７年３月３１日まで
(3) 教員用 PC・教員用 iPad 納期日　令和７年１月３１日まで（利用開始は令和７年２月１日から）
(4) 新システムの本稼働日　令和７年４月１日

(5) 新システムの運用保守期間　令和７年４月１日から令和１２年１月３１日まで（５８か月）
(6) 教員用 PC リース契約期間　令和７年２月１日から令和１２年１月３１日まで（６０か月）
(7) 教員用 iPad リース契約期間　令和７年２月１日から令和１２年１月３１日まで（６０か月）

1.9. 対象施設一覧

(1) 小・中学校

	学校名	住所
1	生駒小学校	生駒市山崎町４－４４
2	生駒南小学校	生駒市萩原町３３５
3	生駒北小中学校	生駒市高山町６７９４
4	生駒台小学校	生駒市新生駒台１－３３
5	生駒東小学校	生駒市東生駒４－３９８－１１０
6	真弓小学校	生駒市真弓１－１１－１５
7	俵口小学校	生駒市俵口町６１４ー1
8	鹿ノ台小学校	生駒市鹿ノ台西1ー5ー2
9	桜ヶ丘小学校	生駒市桜ヶ丘７－１５
10	あすか野小学校	生駒市あすか野南２ー5ー1
11	壱分小学校	生駒市壱分町３５６ー1
12	生駒南第二小学校	生駒市小平尾町９２７
13	生駒中学校	生駒市西松ヶ丘9ー１９
14	生駒南中学校	生駒市萩原町９０
15	緑ヶ丘中学校	生駒市緑ヶ丘２２３２
16	鹿ノ台中学校	生駒市鹿ノ台南２ー１６
17	上中学校	生駒市上町３０００
18	光明中学校	生駒市小明町５５
19	大瀬中学校	生駒市小瀬町９１１－1

(2) その他

	施設名	住所
1	生駒市役所教育委員会事務局	生駒市東新町８－３８
2	教育支援施設	生駒市北新町１２－３２
3	学校給食センター	生駒市小明町１７８７－２８
4	生駒北学校給食センター	生駒市高山町１２５９５－1

1.10.　児童生徒数及び教職員数

（1）児童生徒数（令和５年度時点）

小学校　６，５５０人　　中学校　３，０５１人

（2）教職員数（令和５年度時点）

７６２人（小学校・中学校・教育支援施設・教育委員会事務局を含む。）

2.　ソフトウェア要件

1.9.対象施設一覧において利用するシステム基盤を構築し、その基盤上で稼働する学校の業務に必要となるシステムを提供すること。

2.1. クラウド基盤システム

2.1.1. 概要

クラウド基盤システムはMicrosoft 365 A5による導入を行うものとする。以下のサービスについて導入方針を提示すること。

（1）　認証基盤
（2）　メール
（3）　ファイル管理
（4）　コミュニケーションツール
（5）　フィルタリング
（6）　ウイルス対策
（7）　ファイル暗号化
（8）　情報漏えい対策
（9）　デバイス管理
（10）　多要素認証
（11）　振る舞い検知、EDR

3.　構築業務要件

3.1. 基本要件

（1）　生駒市情報セキュリティポリシーを基にした、教育情報セキュリティポリシーの策定支援も本業務に含めること。
（2）　各校が保有する既存ファイルの移行対象とする容量や手法について提案すること。受託者と協議を行った後、実際の手法は最終決定する。
（3）　５年間運用できるシステム及びハードウェア（リース対象物件を除く）を選定すること。
（4）　本市向けのオンプレミス型サーバによる構築ではなく、「2.1 基盤システム」の全ての機能をクラウドサービスによる提供とすること。

(5)　調達する全てのソフトウェアは、原則、導入時の最新バージョンを導入すること。
(6)　各拠点からのローカルブレイクアウト構成を前提とすること。
(7)　各拠点―クラウド間へ新しく 1Gbps 以上の回線を敷設し、複数回線による構成とすること。少なくとも 1 回線は、セッション制限・許容量の制限が無く、かつ災害時は自動的に通信料無制限となること。また、いずれか一方の回線事業者は、生駒市内に事業所をもっていることが好ましい。
(8)　システムの運用に関して、本市で必要となる運用設計支援を行うこと。
(9)　教職員用端末はマルウェア対策、情報漏えいなどのセキュリティ対策をすること。ログの取得を前提とし、インシデント発生時など本市の要望に応じてレポートを提出すること。その他、通常認証と異なる状況での認証が行われた場合や認証ブロックされた際の理由など認証許可に関するユーザー認証ログや、万が一、情報漏洩が発生した場合に当該データの操作経路ログを取得でき、本市の要望に応じて CSV に吐き出してレポートを提出すること。
(10)　将来的にテレワーク（学外からのデータアクセス）が実現できる構成を提案すること。

3.2. プロジェクト体制

(1)　プロジェクト体制表の作成にあたっては、作業責任者、役割、連絡先を明確にすること。
(2)　プロジェクトマネージャー又は作業責任者について、以下の各条件を満たすこと。
ア　本市と同程度規模以上の地方公共団体でのシステム設計・構築・運用等の業務経験を３年以上有していること。
イ　近畿圏内でのサポート経験を有すること。

3.3. プロジェクト管理

(1)　本システムの導入過程の経過、進捗状況を、定例会議（月 1 回）を通じて報告すること。また進捗報告書及び打合せ会議に際しては、議事内容を事前に提示するとともに、毎回、受注者が議事録を作成し、会議終了後、速やかに提出すること。
(2)　本サービスの提供を進めていくうえで必要となる関係部署、関係機関との調整用資料等の作成についても支援すること。なお、課題や資料を随時共有すること。
(3)　設計、構築期間においては、必要に応じて検討会を実施し、スムーズな業務進行を図ること。また、仕様や要件の確認及び確定に関しては、必ず書面により行うこと。
(4)　課題管理表については、毎回の会議の中で確認を行うこと。

3.4. 要件定義

(1)　本業務に伴い、以下の作業を含む調査及びシステム設計を受注者の責任と負担において実施すること。

(2)　本業務に係るシステムが、円滑かつ迅速に導入され、かつ運用されるよう設計を行うこと。
(3)　構築期間中、学校現場への負担が極力無いように設計を行うこと。
(4)　ネットワーク設計（物理構成設計、論理構成設計）、システム設計（基本設計、詳細設計、セキュリティ設計、移行設計、運用設計等）、ネットワーク配線設計を実施すること。
(5)　各種設計する際に配線や電波利用の調査が必要な場合は、その作業にかかる費用も本契約に含めること。
(6)　調査した内容を踏まえて設計した結果、示している機器台数に増減が生じる場合は、発注者の承認を得て調整すること。
(7)　各設計にて作成した資料は、発注者へ納品すること。

3.5. 教育情報セキュリティポリシーガイドライン策定支援等業務

3.5.1　業務目的

本件業務は、次に掲げる事項を実現するために行うものとする。
(1)　生駒市教育委員会が保有する情報資産の安全管理対策の強化に向けた諸活動を推進すること。
(2)　国（個人情報保護委員会含む。）の方針等を基に、「教育情報セキュリティポリシーに関するガイドライン(令和６年１月　文部科学省)」に準拠して、生駒市教育委員会が実施すべき具体的な施策について指導・助言して、「生駒市教育委員会情報セキュリティポリシー対策方針」、「生駒市教育委員会情報セキュリティポリシー対策基準」の策定を行うこと。
(3)　各職場での自己点検の実施等による情報資産の安全管理対策について指導を行うこと。

3.5.2　業務内容

(1)　生駒市教育委員会情報セキュリティポリシー策定支援等業務実施計画の策定業務

ア　「生駒市教育委員会情報セキュリティポリシー対策方針」及び「生駒市教育委員会情報セキュリティポリシー対策基準」の案の策定

「教育情報セキュリティポリシーに関するガイドライン(令和６年１月　文部科学省)」に準拠して、「生駒市教育委員会情報セキュリティポリシー対策方針」、「生駒市教育委員会情報セキュリティポリシー対策基準」の策定を行う。さらに、以下のガイドライン等に定められた事項及び要請等についても準拠する。

（ア）　教育情報セキュリティポリシーに関するガイドライン(令和６年１月　文部科学省)
（イ）　教育情報セキュリティポリシーに関するガイドラインハンドブック(令和４年３月　文部科学省)
（ウ）　地方公共団体における情報セキュリティポリシーに関するガイドライン(令和

５年３月　総務省）

イ　職員向け情報セキュリティ研修支援

教育情報セキュリティポリシーに関するガイドライン(令和６年１月　文部科学省）及び地方公共団体における情報セキュリティポリシーに関するガイドライン(令和５年３月　総務省)に基づいた職員研修を支援する。研修回数は計４回とし、生駒市教育委員会事務局・各校管理職を対象とする。

ウ　自己点検支援

職員の情報セキュリティに対する意識と運用状況を把握するために自己点検を実施する。

(2)　資料の提供等

本業務の実施にあたり、必要な資料及びデータの提供は本市が妥当と判断する範囲内で受託者に提供する。なお、受託者は、本市から提供された資料は適切に保管し、特に個人情報及び情報システムのセキュリティ対策、情報資産の安全管理に関連する資料の保管は厳格に行うものとする。また、契約終了後は本業務にあたり収集した一切の資料を速やかに本市に返還し、又は廃棄するものとする。

3.6. システム導入テスト

(1)　システムテスト

各サービス、サーバの正常系・異常系のテストを実施すること。バックアップ及びリストアテストについては、本市と必要性を協議の上で実施すること。セキュリティ要件に記載のアクセス制御・データ分類・情報漏洩対策については設計とおりに動作することをシステムテストにて確認すること。

(2)　テスト実施計画

テストは、本番運用を行う環境を用いて実施すること。テストを行う際には利用者への影響を十分考慮した上で計画・実施すること。

(3)　テスト環境

運用環境とは別にテスト環境を用意する場合は事業者負担で構築すること。

3.7. 成果物

本事業の完了にあたり、以下の成果物を作成し、納品すること。

(1)　仕様に基づくハードウェア

(2)　仕様に基づくソフトウェア

(3)　仕様に基づくシステムのマニュアル及び本市が求める資料（紙及び電子媒体１部ずつ）

ア　実施計画書

イ　体制図（体制図・緊急連絡先）

ウ　課題管理表

エ　要件定義書

オ　ネットワーク構成図
カ　配線図（市が提供する現況図を基に作成すること）
キ　設計書
（ア）　基盤システムの基本設計書
（イ）　基盤システムの運用設計書
（ウ）　操作研修計画書
（エ）　デジタル教科書－学習 e ポータル連携運用設計書
ク　操作マニュアル
ケ　議事録及び付随資料
コ　その他本市が必要と定めたドキュメント
サ　情報セキュリティ対策支援業務実施計画
シ　「生駒市教育委員会情報セキュリティポリシー対策方針」及び「生駒市教育委員会情報セキュリティポリシー対策基準」の改正案

4. 運用・保守要件

4.1. 運用統括者

運用の全体統括者を設置すること。全体統括者は、システム運用状況について、本市に定期的な報告を行うとともに、システムの維持・向上を図るために、継続的な運用改善の提案を本市に対して行い、本市の承認を得た改善策を推進させること。

4.2. ヘルプデスク

(1) 平日（日曜日、土曜日、国民の祝日に関する法律（昭和２３年法律第１７８号）に規定する休日及び １２月２９日から翌日の１月３日までのほか、夏季休業期間等のメーカー指定の休日は除く。）８：３０から１７：００までは、電話にて受付対応すること。
(2) (1)の電話受付対応時間外についても、メールでの問合せであれば、２４時間３６５日受け付けること。ただし、時間外に受け付けた問い合わせの対応については、翌営業日以降とする。
(3) 本契約におけるサポート期間については、令和７年４月１日から令和１２年１月３１日までとする。
(4) ヘルプデスクの対応業務は以下のとおりとする。
ア　本調達に含まれるハードウェアの設定内容、利用方法に関する問い合わせ
イ　本調達に含まれるソフトウェアの設定内容、利用方法に関する問い合わせ
ウ　GIGA スクール構想にて整備した校内ネットワーク（無線アクセスポイント・フロアスイッチ等）の障害問い合わせ（GIGA 端末は除く。）なお、機器ハードウェア障害の場合は、導入業者へエスカレーションまで行うこと。
(5) 上記以外の問い合わせで本契約外に関するものは可能な限り問い合わせ先を案内すること。

(6)　現地での対応が必要な場合は、早急に現地に作業員を派遣し、対応すること。
(7)　問い合わせ対応業務の対応経過について、一案件毎に必要な項目を記録し、全件蓄積・保管し、定例会で報告すること。

4.3. ソフトウェア保守

本業務で調達し、端末へインストールしているソフトウェア及びクラウドサービスについて、障害が発生した場合、早急に対応すること。また、必要に応じてオンサイト保守要員を派遣し、対応にあたること。

(1)　システム運用に関する問合せ（ヘルプデスク受領質問を含む。）のエスカレーション受付及びその対応を実施すること。
(2)　クラウド運用である利点を活かしたリモート保守を原則とし、軽微な障害・問合せ等について迅速な対応を実施すること。
(3)　クラウドで提供する各システムについて、運用サービスを提供する拠点からリモート操作ができる環境を用意すること。リモート操作に必要となる回線・機器については本契約に含み、事業者による負担とすること。本市のクラウド環境へ接続の際はグローバルＩＰアドレスや保守用アカウントによる制御や、本市と同等のセキュリティ対策を講じること。
(4)　本業務で導入するクラウドシステムについては、(3)のリモート環境からリモート操作ができるようにすること。なお、学校に設置のプリンタのリモート操作は必須とせず、現地対応などで対応をすること。
(5)　クラウド環境のリモートサポート内容として、以下を実施すること。ただし、セキュリティレベルの維持のため、一部の作業については本市と協議の上で実施とすること。
　ア　受領質問に対する回答
　イ　操作結果に対するデータ調査
　ウ　利用者が変更できない内部パラメータの設定
　エ　不具合改修資源の適用
　オ　毎月の報告
　カ　ポリシー調整・アプリ配信
　キ　フィルタリングの設定変更
　ク　セキュリティツールの設定変更
　ケ　ファイル共有の設定変更、及び横断的なチームやポリシーの設定
(6)　システムメンテナンス
　ア　利用者に影響のあるシステムへのメンテナンスは、可能な限り業務影響がない時間帯で実施すること。
　イ　利用者に影響のあるメンテナンスを行う際には、事前に本市と調整の上、エンドユーザへの周知を行った上で実施すること。
(7)　GIGA スクール構想によって整備したＬ３スイッチのソフトウェア障害については、config 流し込みまでの対応を行うこと。

4.4. ハードウェア保守

(1) ハードウェアに関する問合せ（ヘルプデスク受領質問を含む。）のエスカレーション受付及びその対応を実施すること。

(2) 機器等が正常に動作するように、受注者の負担において、機器の調整、修理、交換又は、部品の交換等所要の保守を行うこと。なお、「正常な作動」とは、導入時の各種設定、インストール作業が完了し、動作確認を完了した状態をいう。

(3) GIGA スクール構想にて整備した校内ネットワーク（無線アクセスポイント・フロアスイッチ等）においても、本業務での運用保守対象とする。一時切り分けを行い、機器ハードウェア障害の場合は、導入業者へエスカレーションまで行うこと。なお、教育支援施設、学校給食センター及び生駒北学校給食センターに関しては、本業務におけるファイアウォールについては本業務での運用保守対象とするが、無線アクセスポイント及びフロアスイッチはこの限りではない。

4.5. 基盤システム保守

(1) サービス提供期間中、運用サービスを間断なく提供できる体制を用意すること。

(2) 以下の対応を行うこと。

ア 基盤システムに関する問い合わせ対応

イ 導入システムの障害対応

ウ 端末修理後の基盤システムにアクセスするための手順書の提供

4.6. 研修会

(1) 今回、ファイルサーバの環境を刷新するため、システムの操作研修のほか、研修を実施すること。

(2) 研修対象者に即したマニュアルの作成も業務範囲とする。

(3) 研修を実施する上で必要となる会場や端末の準備については本市が行う。スケジュール詳細は本市との打ち合わせで決定する。

(4) 想定している研修対象者、研修内容、研修方法、開催時期/回数は以下のとおりとするが、詳細な内容や開催日程については、本市と別途協議の上で決定すること。

受講者分類	研修対象者	研修内容	開催時期/回数
システム管理者	生駒市教育委員会システム担当	年次更新業務についての説明 管理ポータルの使用方法	導入後 1 回程度
管理職･情報担当・一般職員	学校管理職・各学校の情報担当・学校の教職員	システムの利用方法 問合せ方法の説明	導入後 1 回程度
情報担当･一般職員	各学校の情報担当・学校の教職員	システムの利用方法 問合せ方法の説明	運用保守期間 毎年 1 回程度

上記とは別に、「３．５．教育情報セキュリティポリシーガイドライン策定支援等業務」に示すとおり、セキュリティポリシーガイドラインに関する研修も実施すること。

4.7. 定例会

(1) 毎月１回定例会を実施し、本システムの稼働状況、利用状況、システム保守対応状況等を報告すること。

(2) 定例会でシステム運用の課題、問題の報告を行い、必要に応じてルールの見直しや設定変更を行い、活用促進に努めること。

(3) 定例会では次の提出物を用意すること。

ア 課題管理表

イ 議事録、付随資料

4.8. 受託者の業務範囲外

次の業務は、システム利用者側の業務範囲とする。

(1) 児童生徒に関するデータの登録・編集・削除作業

(2) 児童生徒の進級進学等に関する作業

(3) 初期登録後の学校情報の変更・更新作業

(4) 児童生徒・教職員データを誤って削除した際の復旧作業

(5) 学校数の増加に伴う追加設定作業

(6) 本業務での範囲外のシステム等に関する現地訪問・個別調査対応教職員の校務作業全般に関するデータの登録・抽出等の作業

（別紙）ハードウェア・ソフトウェア仕様

操作ログ管理サービス

以下機能を有すること。

機能	機能概要	区分 必須
ログ取得	ログ取得対象端末の電源オン/オフ及びサスペンドの記録が可能であること。	○
	OSログオン/ログオフ操作の記録が可能であること。	○
	OSログオン中に実際に操作した時間の記録が可能であること。	○
	アプリケーションの起動と終了の記録が可能であること。	○
	アプリケーション稼働中に次のキーを押下した回数及びマウスのクリック数や移動距離をアプリケーション別に記録可能であること。 ※Delete、Back Space、英数字キー、Alt、Ctrl、Space、右クリック、左クリック	
	アプリケーション稼働中に実際にそのアプリケーションを操作した時間の記録が可能であること。	
	サービスやスタートアップなど、バックグラウンドで起動したアプリケーションの記録が可能であること。	○
	ファイル操作の記録が可能であること。アプリケーションの種別やバージョンに依存せずに記録可能であること。	○
	ファイル操作において、OSのカーネルレベルでのログ取得が可能なこと。	
	印刷の記録が可能であること。※プリンター名、ファイル名、ファイルパス、ページ数、印刷アプリケーション名の記録が可能であること。	○
	SMTP(S)/POP3(S)を用いたEメールの送受信の記録が可能であること。 ※本文、添付ファイルの復元が可能であること。 ※メーラーに依存せずにEメールの記録が可能であること。 ※Eメールの通信経路（ネットワーク構成）に変更を加えないこと。	
	Gmail/Office 365の送信メールの記録が可能であること。	○
	インターネット操作の記録が可能であること。ブラウザの種別やバージョンに依存せず、http及びhttpsの記録が可能であること。（アドオン不要）	○
	FTPの記録が可能であること。	
	任意のタイミング（指定したアプリケーションが起動したタイミング、指定したキーワードがタイトルに含まれたウィンドウが起動したタイミング、PrintScreenキーが押下されたタイミング等）でスクリーンショットの記録が可能であること。	
	リモート接続元端末のホスト名及びIPアドレスの記録が可能であること。	○
	ファイル操作において、ファイル操作の「移動」が記録可能であること。また、ファイル/フォルダのアクセス監査（成功、失敗）が記録可能であること。	○
	クライアントPCの操作中に次のキーを押下した回数およびマウスのクリック数や移動距離をユーザー別にアクションログとして記録可能であること。 ※Delete、Back Space、英数字キー、Alt、Ctrl、Space、右クリック、左クリック	

機能	機能概要	区分 必須
ログ取得	Webログにおいて「HTTPステータスコード」の記録が可能であること。	
	ユーザーログにおいて、リモートデスクトップ接続による接続・切断の履歴を記録可能であること。	
	一定時間間隔（６０秒～８時間）、Print Screenキーを押下時、特定のWebサイト閲覧時やファイルのアップロード時に画面イメージを記録できること。	○
	WebログにおいてChromeのシークレットモードの操作ログを取得できること。	
ログ管理	収集したログ情報は、ログ管理サーバーで集中管理が可能であること。	○
	緊急時等に特定の端末を指定して優先的にログを回収できること。（最低でも５分間隔でログを回収できること。）	○
	Active DirectoryとLDAP連携が可能であること。	
	管理コンソールへのアクセス履歴、及び操作概要の履歴の記録が可能であること。	○
	ログ収集エージェントがログをログ管理サーバーに送信する際は、AES 256bit相当の強度で暗号化すること。	
	部門情報の設定において任意の部門を10階層以上設定できること。	
	各管理者の権限に応じて、ログの閲覧範囲（部門単位）を設定できること。	○
	各管理者の権限に応じて、ログの閲覧範囲（ログ種別）を設定できること。	
	ログ収集エージェントがログ取得対象端末の「アプリケーションの追加と削除」にリストアップされないこと。	
	ログ収集エージェントが容易に停止できないこと、停止された場合は自動的に再開できること。	
その他	ログ取得対象端末で、システム日付や時刻を変更できないよう制御が可能であること。	○
	SBC（Server Based Computing）環境（Citrix XenApp、VMware Horizon View、Microsoftリモートデスクトップサービス、Microsoft ターミナルサービス、Ericom PowerTerm WebConnect、Ericom Connect、Remote Application Server）に対応でき、且つ、物理環境との混在でも同一のログ管理サーバーで管理・ログの閲覧ができること。	
	VDI（Virtual Desktop Infrastructure）環境（Citrix XenDesktop、VMware Horizon View、Microsoft VDI、Ericom PowerTerm WebConnect、Ericom Connect、Remote Application Server）に対応でき、且つ、物理環境との混在でも同一のログ管理サーバーで管理・ログの閲覧ができること。	
	Citrix Xen Desktopにおいては、プロビジョニング（PVS、MCS）に対応できること。	
	Citrix XenAppのアプリケーションサーバーをPVS方式で管理し、プロビジョニングが行われる環境に対応できること。	
	VMware Horizon Viewにおいてはリンククローン・インスタントクローンに対応できること。	

コンテンツ配信システム

以下機能を有すること。

機能概要	区分 必須
デジタル教科書及び教育用コンテンツをクラウド上で利用できるシステムであること。	○
学校ごとに1年単位でもコンテンツを選択・購入、利用できること。	○
各学校のパソコンに特殊なプログラムをインストールする必要がなく運用できること（但し、コンテンツ動作上必要なプラグインは除く）。	○
コンテンツが快適に利用できない状況が発生した場合などに備えて、将来的に機能をオプションにより拡張できるシステムであること。また、その機能は、利用しているコンテンツのライセンス契約期間と紐づき、ライセンス規約違反になることなくコンテンツを利用できる機能を有していること。	
システムから配信できるコンテンツは、10社以上のコンテンツメーカーによる1,000タイトル以上であり、10社以上の教科書会社のデジタル教科書が含まれていること。	
コンテンツ発行元によるコンテンツの修正、バージョンアップがなされた場合、それを反映して最新の状態で提供すること。	○
コンテンツの選択・購入にあたっては、同システム上で、前述の1,000タイトル以上のコンテンツを教員が自由に試用でき、購入前に十分な確認ができること。また、試用・確認はシステムメンテナンス日を除く毎日、授業終了後の15時以降とする。	
教育委員会管理者用アカウントを発行し、市内の学校のコンテンツの利用状況を確認できるようにすること。	○
学校毎に権限の異なる２つ以上のユーザーアカウント（①先生、②生徒）を設定できること。	○
プログラミング、タイピング、キャリア教育、特別支援プリント教材を含む10タイトル以上の無償コンテンツを有していること。	
AzureAD（Microsoft 365）、Google Workspace for Educationとのシングルサインに対応していること。	○
学習eポータル「L-Gate」からの名簿連携機能を有しており、名簿（アカウント）登録作業を行うことなく利用できるシステムであること。なお、名簿連携は夜間に自動同期によって行われ、更新された名簿情報は翌日に反映されるものとする。	
教員が教科・クラス・学年・用途など任意の単位でコンテンツを分類することによって、児童生徒の円滑なコンテンツの活用を支援できる機能をもつこと。	○

ファイアウォール

以下機能を有すること。

機能	機能概要	区分 必須
ハードウェアアプライアンス要件	ハードウェアとソフトウェアが一体となったアプライアンス機器であること。	○
	各単一の管理ポート（イーサネット、シリアルコンソール）で全てのモジュールを一元管理できること。	○
	機器内部にログや設定を保存するためのストレージとして、128GB以上搭載されていること。 ※教育支援施設、給食センター、北給食センター、生駒市役所の4拠点に関しては、64GB以上で可とする。	○
	静音化のためファンレスで動作可能なこと。	
	電源が冗長化されていること。 ※教育支援施設、給食センター、北給食センター、生駒市役所の4拠点に関しては、本機能は有する必要はない。	○
	本装置は、L3（ルータ）モードに対応していること。	○
	本装置はL1モード(MACアドレスを保持しない)をサポートすること。	
	IEEE802.1Q VLANトランク機能を有すること。 仮想システム等を利用することなく、L1モード、L2モード、L3モードにおいて最大4094個のVLANをサポートすること。	
	IEEE802.1ax リンクアグリゲーション機能を有すること。（Static及びLACP）	
	ジャンボフレーム (9,216Bytes) をサポートすること。	
	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。	
	IPv4及びIPv6のOSPF Graceful Restartに対応していること。	
	Pingによるスタティックルートの死活監視を行い、監視先がダウンした際には当該ルートを動的に削除する機能を有すること。	○
	Static RouteやPBRのNexthopとして、IPアドレス以外にFQDNを指定可能であること。	
	BGP PeerとしてFQDNで指定可能であること。	
	マルチキャストルーティング(PIM-SM)に対応していること。	
	NAT機能を有すること。	
	宛先NATの変換先として、IPアドレス以外にFQDNを指定可能であること。	
	ポリシー設定の送信元及び宛先にFQDNが利用できること。なお、FQDNのIPアドレス情報は、DNSレスポンスのTTLに基づいて自動的に更新すること。	
	DNSプロキシー機能を有すること。また、特定のドメイン毎に指定したDNSサーバーを利用する制御が可能であること。	

機能	機能概要	区分 必須
ハードウェアアプライアンス要件	ポリシーベースのQoSに対応しており、アドレス、ポート番号、利用ユーザ、アプリケーションといった情報を基に帯域制御が可能であること。	
	アドレス、ポート番号、利用ユーザ、アプリケーションの情報を基にセッション単位で指定したインターフェースにIPパケットを転送する機能を有すること。	
	IPv6 RA(Router Advertisement)にDNS情報を付与する機能を有すること。	
	IPv6 NDP（Neighbor Discovery Protocol)をモニタリングすることで、IPv6アドレスとMACアドレスのマッピング情報を確認することができること。	
	GREトンネルの終端が可能であること。	
冗長構成/クラスタリング機能	Active/Passive、Active/Active両方の冗長構成に対応していること。（なお、いずれの冗長構成でもアプリケーション識別やIPS機能、アンチウィルス機能も制限なく利用可能なこと。）	
	冗長構成のOSアップグレード作業時、セッションを維持しつつアップグレード作業が可能であること。	
アプリケーション識別及びポリシー設定機能	3500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可視化できること。	
	追加設定なく、初期状態（デフォルト）で全てのトラフィックを対象にしたアプリケーションの識別のシグネチャが適用されていること。	
	ファイアウォールのポリシーは送信元/送信先とアプリケーション名を元に処理可能であること。	
	1つのセキュリティポリシーでIPv4及びIPv6通信に対するアクセス制御やアプリケーション識別による制御が可能であること。	
	同一のTCP/UDPポートを使用するアプリケーションに対し、異なるセキュリティポリシーを設定可能であること。	
	宛先/送信元の国別アドレスでポリシー制御が可能であること。	
	ポリシー設定を簡素化するために、IPアドレスの任意のビットに対してワイルドカードマスクを使用した柔軟なアドレス指定が可能であること。	
	特定のイベントを検知した場合、そのイベントの送信元又は宛先のIPアドレスに関する通信に対して、一定時間異なるセキュリティポリシーを自動的に適応することが可能であること。	
	ポリシー設定をCSV/PDF形式又はCSV/JSON形式で出力できること。	○
	ポリシー設定画面において、トラフィックに対する各ルールのヒット状況(ヒット数、最後のヒット日時、最初のヒット日時)を確認できること。	
	ポリシー設定画面において、ポリシーが作成された日付と最後に更新された日付を確認できること。	
	任意の通信に対して、設定したポリシーが適切に機能するかどうかをGUI上で確認するためのテスト機能を有すること。	
	設定ポリシー変更の際、すべてのセッションを再マッチングできること。	

機能	機能概要	区分 必須
アプリケーション識別及びポリシー設定機能	アプリケーションに依存せずTCP/UDPポート番号単位でセッションタイムアウト時間を設定可能であること。	
	セッション数が閾値を超えた場合に、自動的にセッションタイマーを短くすることでセッション数の増加を抑制する機能を有すること。	
	ポリシーの使用状況や通信内容を分析し、既存のポリシーに対するポリシー最適化機能を有すること。	
	X-Forwarded-For(XFF)に付与されたIPアドレスに基づいたセキュリティポリシーの制御が可能であること。	
	HTTP/2を利用するアプリケーションの可視化及び制御が可能であること。	
コンテンツ検査/脅威防御/URLフィルタリング機能	ファイアウォールのポリシー毎にウィルス・スパイウェア、URLフィルタリング等のコンテンツ検査機能を有効/無効に設定が可能であること。	○
	外部からIPアドレス/Domain/URL情報を自動的に取り込み、ポリシー制御に反映する機能を有すること。また、取り込んだリストによるアクセス制御が行われた場合、ログに記録されること。	
	GoogleやDropbox等のSaaSアプリケーションに対して、HTTPリクエストヘッダに企業用のドメインを挿入することにより、個人アカウントの使用を制限できること。	
	他のセキュリティデバイスにおいてもユーザ情報の可視化や制御が行えるよう、ユーザ情報をHTTPヘッダに挿入する機能を有すること。	
	PDF、Excel、Word、PPT、ZIPなど100種類以上のファイルタイプによる通信の可視化やフィルタリングが可能なこと。	
	ブロックすべきファイルは事前に定義されたプロファイルが用意されていること。	
	暗号化されたPDF、Microsoft Office、ZIP、RARファイルと暗号化されていない前述ファイルの通信を区別してファイル名の可視化やフィルタリングが可能なこと。	
	クレジットカード番号又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。	
	VxLANトンネル内の通信データの検査が可能であること。	
	SaaS アプリケーションプロバイダが公開しているサービス提供エンドポイントの最新の IP アドレス・URL 情報をファイアウォールに配布する無償のホスティングサービスがインターネット上で提供されており、セキュリティポリシー、Policy Based Forwarding、SSL 復号等の設定に利用できること。	
ユーザ識別及び認証機能	Active Directory等と連携し、IPv4及びIPv6環境に関わらずIPアドレスとユーザ情報を紐付け、可視化と制御が可能であること。	
	Captive Portalによるユーザの認証が可能であり、かつ、多要素認証に対応すること。	
	Syslogによる外部認証システムと連携可能であり、Syslogメッセージより取得したユーザ情報を基にトラフィックの可視化と制御が可能であること。	
	Webプロキシ装置が付与したX-Forwarded-Forの情報を元にユーザ識別機能が使用できること。	
	SAML 2.0に対応した認証機能を有し、SPとして動作すること。	

機能	機能概要	区分 必須
ユーザ識別及び認証機能	脅威ログが確認された場合に、対象となるユーザを自動で隔離又は通信を制限する機能を有すること。	
	ファイアウォールとオンプレミスのLDAP認証から、クラウドベースのIDプロバイダー(IdP)への移行の際、ファイアウォールとIdPの間に認証を中継するクラウドサービスを設けることで、設定の複雑さを軽減できること。	
サンドボックス（WildFire）機能	追加機器等なく、未知のファイルを仮想OS環境で実行し、解析する機能を有すること。	○
	仮想OS環境をクラウドで提供する場合は、日本国内に解析システムが存在すること。	
	仮想OS環境をクラウドで提供する場合は、少なくとも全世界で40,000社以上での利用実績があること。	
	未知の脅威が確認された場合に、感染の疑いのある端末を自動で隔離する機能を有すること。	
SSL復号機能	筐体内でSSLに準拠した通信を復号し、アプリケーションの識別及びコンテンツ検査のポリシーが適用可能であること。また、TLS 1.3の復号にも対応していること。	
	筐体内で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。	
	筐体内にサーバ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宛てのSSL通信を復号し、アプリケーションの識別及びコンテンツ検査のポリシーが適用可能であること。	○
	インバウンドインスペクション方式のSSL復号機能を有すること。復号用のサーバ証明書は、有効期限切れ直近の証明書と、新規発行の証明書の両方を同時に設定することで、サービスを中断することなく新しい証明書への切り替えが可能なこと。	
	SSL復号通信のセッション数や暗号方式、SSL復号失敗理由の情報を管理GUIにて確認可能であること。	
	クライアント証明書要求など、特定の理由でSSL復号ができないと判断されたURLは、自動的に一定時間SSL復号除外する機能を有すること。	
Global Protect（SSL-VPN）機能	SSL VPNやIPSecによるリモートアクセスVPNに対応していること。	○
	クライアント端末(Windows, Mac OS X)の接続先ネットワークを自動識別し、外部ネットワークに接続された場合に自動的に最寄りのファイアウォールに対してVPN接続を行う機能を有すること。	
	VPN接続端末からのトラフィックが5分間ない場合、自動的にVPNセッションをログアウト処理する機能を有すること。	
マネージメント機能	設定操作は、装置単体で候補コンフィグを作成し、コミット操作にて設定を有効にするアーキテクチャであること。また、候補コンフィグを実行中の状態を戻すことが可能であること。	
	設定操作に関しては、管理者毎に、その管理者が設定変更した分だけをコミット及びロールバックできること。	
	WebUI上で候補コンフィグと実行中コンフィグの差分が確認できること。	
	設定情報を名前付きのスナップショットとして保存可能であり、またスナップショットから設定を復元できること。	

機能	機能概要	区分 必須
マネージメント機能	設定ファイルについてはXML形式でインポート/エクスポート可能であること。	
	設定及びレポートデータをXMLベースのAPIを使用して外部システムと連携可能であること。	
	ファイアウォールをWebUIで管理する際は操作端末側に別途ソフトウェアをインストールする必要がないこと。	
	セキュリティ機能毎（ファイアウォール、アンチウイルス、IPSなど）で管理WebUIが統一されていること。	
	WebUIは日本語を含む5種類以上の言語に対応しており、設定変更を伴わずに言語切替ができること。	
	IPv6によるWebUI/CLIの管理通信に対応していること。	
	1つの管理インターフェースを用いてSyslogの送出、シグネチャの自動アップデート及びサンドボックスとの連携が可能であること。	
	複数のログを串刺しで検索する機能を持っていること。	
	SNMPプロトコルによる管理処理部のメモリ利用率、スワップ利用率、仮想システム毎のセッション利用率、及びデータ転送処理部のパケットバッファ利用率のモニタリングが可能なこと。	
	外部syslogサーバにログ出力可能であること。また、各Syslogサーバー毎に送出するログフォーマットの設定が可能であること。	
	Syslogデータ転送方式としてUDPに加えてTCP又はTLSに対応していること。	
	HTTPでのログ転送が可能なこと。	
	送信元/宛先IPアドレス、送信元/宛先国名、アクション、通信量、Malwareカテゴリ等のログ属性でログをフィルターし、特定のログのみをメール通知、Syslog、SNMPで通知することが可能であること。	
	SyslogやSNMP等でlogを外部に送信する際に、ログのタイムスタンプについてミリ秒単位で出力できること。	
	インターネット経由でファームウェア並びにシグネチャファイルを製品に直接ダウンロード及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。	
	その管理者が実行したすべてのアクションを詳細に分析して対処できるよう、WebインターフェイスとCLIで管理者のアクティビティを追跡できること。	
	受信/送信/ファイアウォール/破棄の4つのステージ毎のパケットキャプチャ機能を有し、pcap形式でダウンロード可能であること。また、キャプチャ機能は、タイマーやCPUバッファのしきい値ベースで自動的に停止する機能を有すること。	
	OpenConfig (https://www.openconfig.net/) に対応したAPIをサポートすること。	
	ファイアウォールのデバイス状態やセキュリティ状態に対する修復すべき推奨事項の情報を提供する AIOps の機能が利用可能であること。	

機能	機能概要	区分 必須
マネージメント機能	複数のバージョンをまたがるバージョンアップ作業時に、必要なソフトウェアやコンテンツを1回でまとめてダウンロードできること。	
レポート機能	追加機器等不要で、レポートデータをPDF形式でエクスポートし、スケジュール機能により定期的に電子メールに添付し送付することが可能であること。	
	追加機器等なく、通信量の統計情報を元に、宛先/送信元の国別で通信量を世界地図上に視覚的に表示する機能を有すること。	
	WebUI上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URLカテゴリ、脅威をランキング形式で表示できること。	
	50以上の事前に定義されたレポートテンプレート及びカスタムレポート機能を有し、それらをPDF形式にして設定されたスケジュールで自動メール送信可能なこと。	
	特定時間内で発生した脅威や通信（アプリケーション）を視覚的に表示し、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。	
	非標準ポートを使用する偽装通信やアノマリー通信を可視化するレポート機能を有すること。	
	過去と現在の通信内容を比較し、その差分を表示するレポート機能を有すること。	
	SaaSアプリケーションに特化したレポート機能を有し、それをPDF形式で出力可能なこと。	

ファイアウォールクラウド管理ツール

以下機能を有すること。

機能	機能概要	区分 必須
ハードウェア要件	VMware ESX(i)上で動作するバーチャルアプライアンス形態であること。	
	バーチャルアプライアンスはAWSやAzure上でも動作可能であること。	○
	ログや設定を保存するために、最大24TBのストレージが使用可能なこと。(バーチャルアプライアンス)	
マネージメント要件	http及びhttps対応のWebインタフェースを有すること。	○
	管理クライアント端末に対して専用クライアントソフトウェアがインストール必要とされないこと。	○
	管理対象ファイアウォール装置と同様のWebUI 操作性を有すること。	
	設定については、候補コンフィグと実行コンフィグを分けたCommitベースのアーキテクチャとなっていること。	
	通信ログ閲覧とデバイスの一元管理（設定変更やで脅威シグネチャの更新）が一つのシステム上で可能なこと。	
	設定ファイルについては、インポート/エクスポートが可能であること。	○
	設定及びレポートデータを外部システムと連携可能であること。（ＸMLベースのAPIなどを使用しての連携を想定）	○
	管理用ロールとログ収集用ロールを設定することにより、複数台構成によるスケールアウトモデルに対応すること。	
	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製品に直接ダウンロード及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。	
レポート機能	WebUI 上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URLカテゴリ、脅威をランキング形式で表示できること。	
	通信量の統計情報をもとに、宛先/送信元の国別通信量を世界地図上にグラフ表示する機能を有すること。	
	通信量の統計情報をもとに、宛先/送信元の国別脅威発生量を世界地図上にグラフ表示する機能を有すること。	
	デバイス単位のレポートのみならず、任意のグループや全てのデバイスにおいて集約したレポートを作成可能なこと。	○
	管理デバイス毎に負荷状況(CPU使用率、メモリ使用状況、スループット、セッション数、CPS等)をグラフで表示可能なこと。	

機能	機能概要	区分 必須
ソフトウェア要件	最大5000台までのデバイスをグループ化して階層的に管理できること。	
	複数のファイアウォール装置をグループ化し、ファイアウォールグループごとに異なるポリシーを適用することが可能であること。	○
	1筐体で複数の仮想システムが稼働しているファイアウォール装置について、仮想システムごとに異なるファイアウォールグループに所属させ管理することが可能であること。	
	管理対象デバイスから転送されたログを、SyslogやSNMP Trap、E-mail 等を用いて外部システムへ転送する機能を有すること。	
	ログの相関分析が可能なこと。	
	複数ファイアウォール装置のポリシーが一元管理が可能であること。	
	宛先/送信元の国別アドレスでポリシー制御が可能であること。	
	Snort, Suricata シグネチャをカスタムシグネチャに変換する機能を有すること。	
	システムの冗長化(HA)機能を有すること。	○
	管理対象ファイアウォールの複数の仮想システムへの構成プッシュが、単一のコミット操作に統合できること。	
	管理ツールから、単一又は複数のファイアウォールのコンフィグレーションのプッシュをスケジュール化できること。また、1回限り又は定期的なプッシュのスケジュールが可能であること。	
	管理ツールからファイアウォールへのコンフィグ送信(プッシュ)は、自分が管理ツール上でコミットした構成変更分だけに制限できること。	
	管理対象のログコレクターのヘルスステータスを一元的に表示できること。	

教員用ノートPC

以下機能を有すること。

機能	機能概要	区分 必須
OS	Windows11Pro	○
CPU	Core i5以上	○
ストレージ	128GB以上	○
メモリ	8GB以上	○
画面	15.6型	○
通信機能	LAN：1000Base-T／100Base-TX／10Base-T（自動認識、Wake-up on LAN対応）	○
	無線：Wi-Fi 6 （IEEE802.11ax）（2.4Gbps）対応＋IEEE802.11ac/a/b/g/n準拠 （WPA™/WPA2™/WPA3™対応、WEP対応、AES対応、TKIP対応）	○
	Bluetooth：Bluetooth®ワイヤレステクノロジーVer5.1準拠	○
セキュリティチップ	TPM（TCG Ver2.0準拠）	○
キーボード	106キー（JIS配列準拠）（テンキー付き）　※同等の要件を満たすものであれば可とする。	○
オーディオ	ステレオスピーカー / マイク	○
内蔵カメラ	有効画素数 約92万画素 WindowsHello対応	○
	デュアルマイク付き	
インターフェース	HDMI®出力端子×1、RGB（15ピン ミニD-sub 3段）×1、LAN（RJ45）×1、USB3.2（Gen1）Type-Aコネクタ×3、USB4™ Type-Cコネクタ×1（PD対応、外部ディスプレイ出力対応）、マイク入力/ヘッドホン出力端子×1 ※同等の要件を満たすものであれば可とする。	○
外部寸法（幅x奥行x高さ）	379.0×257.9×16.9～23.9mm以下	○
質量	2.5kg以下	○
バッテリー駆動時間	10時間以上	○
保証	5年	○
その他	端末設定作業及び各拠点配送設置費用も含めること。 リース満了後、ノートPC本体は受注者にて引取り、データ消去を行うこと。また、データ消去証明書を市担当者に提出すること。	○

教員用iPad

以下機能を有すること。

機能	機能概要	区分 必須
OS	iPad OS 17以上	○
容量	64GB以上	○
重量	500g以下	○
ディスプレイ	10.2インチ、IPSテクノロジー搭載10.2インチ（対角）LEDバックライトMulti-Touchディスプレイ、2,160 x 1,620ピクセル解像度、264ppi、True Toneディスプレイ、500ニト輝度、耐指紋性撥油コーティング	○
チップ	A13 Bionicチップ　Neural Engine	○
カメラ	8MP広角カメラ、ƒ/2.4絞り値、最大5倍のデジタルズーム、5枚構成のレンズ、パノラマ（最大43MP）、写真のHDR、写真へのジオタグ添付、自動手ぶれ補正、バーストモード	○
ビデオ	1080p HDビデオ撮影（25fpsまたは30fps）、720p HDビデオ撮影（30fps）、3倍ビデオズーム、720pスローモーションビデオ（120fps）に対応、手ぶれ補正機能を使ったタイムラプスビデオ、ビデオの手ぶれ補正、映画レベルのビデオ手ぶれ補正（1080pと720p）、連続オートフォーカスビデオ、再生ズーム、ビデオ撮影フォーマット：HEVC、H.264	○
フロントカメラ	12MP超広角カメラ、122°視野角、ƒ/2.4絞り値、写真のHDR、1080p HDビデオ撮影（25fps、30fpsまたは60fps）、手ぶれ補正機能を使ったタイムラプスビデオ、ビデオの拡張ダイナミックレンジ（最大30fps）、映画レベルのビデオ手ぶれ補正（1080pと720p）、レンズ補正、Retina Flash、自動手ぶれ補正 バーストモード	○
スピーカー	ステレオスピーカー	○
マイク	通話、ビデオ撮影、オーディオ録音のためのデュアルマイク	○
センサー	Touch ID、3軸ジャイロ、加速度センサー、気圧計、環境光センサー	○
ビデオミラーリング	Apple TV（第2世代以降）へのAirPlayミラーリング、写真、ビデオ出力	○
電源とバッテリー	32.4Whリチャージャブルリチウムポリマーバッテリー内蔵、Wi-Fiでのインターネット利用、ビデオ再生、オーディオ再生：最大10時間、電源アダプタ、又はUSB-C経由でコンピュータを使って充電	○
保証	5年（物損はAFSの動産保険を利用してもよい）	○
その他	端末設定作業及び各拠点配送設置費用も含めること。 リース満了後、受注者にて引取り、データ消去を行うこと。また、データ消去証明書を市担当者に提出すること。 第9世代の販売が終了している場合は、第10世代以降のiPadを納めること。	○