生駒市教育系ネットワーク構築・維持管理等業務に係る公募型プロポーザル実施要領

1　業務概要

(1)　目的

令和６年度末で現行の境界分離型セキュリティネットワークの保守運用契約が終了することから、新しくゼロトラスト型セキュリティネットワーク環境を構築し、令和７年度から運用を行うことにより、生駒市小中学校の教育 DX を進める。

ゼロトラスト型セキュリティネットワークの導入により、セキュリティを担保しながら校務系ネットワークと学習系ネットワークを統合し、アクセス場所（校内外）を問わず、安全な校務・学習システムが利用可能となり、教職員の執務環境の向上を図る。教職員の執務環境が向上することにより、児童・生徒と向き合う時間の創出や授業準備の時間の確保を図り、効率的かつ効果的な教育活動を可能とする。

また、ゼロトラスト型セキュリティネットワークの構築と同時に、保守・運用方針、教育委員会のセキュリティポリシー、施設開放時のネットワーク環境等も同時に見直すことにより学校現場が抱える課題の解決も図る。

(2)　業務名

生駒市教育系ネットワーク構築・維持管理等業務

(3)　業務内容

ハードウェア・ソフトウェアの調達業務、ネットワーク構築業務、ネットワーク運用保守業務、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

(4)　業務期間

構築業務　：契約締結日から令和７年３月３１日まで
端末リース：令和７年２月１日から令和１２年１月３１日まで
運用保守　：令和７年４月１日から令和１２年１月３１日まで

2　業務に要する費用（予定価格）

(1)　令和６年度　　：１７１，２９７千円（税込）
(2)　令和７年４月１日～令和１２年１月３１日：３４２，６５４千円（税込）
(3)　合計　　：５１３，９５１千円（税込）

※参考見積書の金額が、業務に要する費用（予定価格）の(3)を超過した場合は失格とする。また、予定価格のうち、(1)及び(2)の予定価格は個別に設定し、いずれかを超過した場合も失格とする。

3　参加資格

(1)　プロポーザルに参加できる者（提案者となろうとする者）は、次に掲げる事項をすべて満たすこととする。

ア　公示日から受託候補者特定の日まで、生駒市の入札参加停止措置を受けていないこと。

イ　地方自治法施行令（昭和２２年５月３日政令第１６号）第１６７条の４第１項の規定に該当

しないこと。

ウ　破産法（平成１６年法律第７５号）の規定により破産の申立てがなされていないこと。

エ　会社更生法（平成１４年法律第１５４号）に基づき更生手続き開始の申立てをしていないこと又は民事再生法（平成１１年法律第２５５号）に基づき再生手続き開始の申立てをしていないこと。ただし、会社更生法の規定による更生計画又は民事再生法の規定による再生計画について、裁判所の認可決定を受けた者を除く。

オ　国税及び地方税を滞納していないこと。

カ　次の(ア)から(オ)までのいずれの場合にも該当しないこと。

（ア）　役員等（法人にあっては役員（非常勤の者を含む。）、支配人及び支店又は営業所（市との契約に関する業務を行う事務所をいう。以下同じ。）の代表者を、法人格を持たない団体にあっては法人の役員と同等の責任を有する者を、個人にあってはその者、支配人及び支店又は営業所を代表する者をいう。以下同じ。）が暴力団員（暴力団員による不当な行為の防止等に関する法律（平成３年法律第７７号。以下「暴対法」という。以下同じ。）第２条第６号に規定する暴力団員をいう。以下同じ。）であると認められるとき。

（イ）　暴力団（暴対法第２条第２号に規定する暴力団をいう。以下同じ。）又は暴力団員が経営に実質的に関与していると認められるとき。

（ウ）　役員等が、その属する法人若しくは法人格を持たない団体、自己若しくは第三者の不正な利益を図る目的で、又は第三者に損害を与える目的で、暴力団又は暴力団員を利用していると認められるとき。

（エ）　役員等が、暴力団又は暴力団員に対して資金等を提供し、又は便宜を供与する等直接的若しくは積極的に暴力団の維持及び運営に協力し、又は関与していると認められるとき。

（オ）　上記（ウ）及び（エ）に掲げる場合のほか、役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有していると認められるとき。

キ　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。

(2)　共同企業体での参加も可能とする。その場合において、グループの構成団体についても参加資格(1)ア～カをすべて満たさなければならない。また、グループ代表団体は、(1)キを満たさなければならない。なお、グループの構成団体となった場合は、別に単独で本プロポーザルに参加すること及び他の複数のグループの構成団体になることはできないものとする。

４　質問の受付及び回答

(1)　提出期限　令和６年６月２４日（月）１２時００分まで（必着）

(2)　提出方法　別添の質問書（様式１）により、電子メール又はＦＡＸで提出すること。

提出先：電子メール　k-seisaku@city.ikoma.lg.jp

ＦＡＸ　　0743-74-9100

※電子メール又はＦＡＸ以外の方法で提出された質問に対しては回答しない。

(3)　回答日時　令和６年６月２８日（金）１２時００分

(4)　回答方法　生駒市ホームページに掲載

５　企画提案書等の作成及び提出

（1）　提出書類・必要部数

ア　業務実施体制回答書及び企画提案書提出届（様式２）　原本１部

イ　実施体制各種調書及び企画提案書等　原本１部、副本１０部、副本の内容をＰＤＦデータ化して格納したＣＤ－Ｒ１枚（データのファイル名は「(ア)　会社概要（様式３)」のように(ア)～(シ)の名称付してください。）

※本市の令和６年度物品・委託業務業者登録申請書を提出している者については、下記提出書類の内、（ケ)、(コ)、(サ)を省略することができる。

（ア）　会社概要（様式３）

（イ）　業務実績調書（様式４）

「３　参加資格(1)キ」に該当する業務実績をすべて記入すること。また、その業務実績の根拠となる契約書等及びその業務内容がわかる仕様書等の写しを添付すること。なお、グループを組む場合は、すべてのグループ構成団体分を提出すること。業務内容は、主になる業務内容を記入し、記入欄が不足する場合は複写して作成すること。

（ウ）　業務体制等調書（任意様式）

本業務の担当者の業務経歴を記載した名簿と体制図（再委託する場合は再委託先の事業者名も含む。また、グループを組む場合は、すべてのグループ構成団体分を作成し、本事業に係る各グループの役割が分かるようにすること。）を提出すること。

※業務責任者は、必ず第２次審査に参加すること。

（エ）　再委託調書（様式５）※再委託をする場合のみ

本業務の一部を再委託する場合は、再委託の必要性や、その理由（企業の技術的特長等）を企画提案書に記載すること。ただし、業務の主たる部分は、再委託してはならない。

（オ）　グループ協定書（様式６）※グループを組む場合のみ

（ア)、(イ)、(ケ)、(コ)、(サ)は、すべてのグループ構成団体分を提出すること。

（カ）　企画提案書（任意様式）

（キ）　参考見積書（任意様式）

消費税及び地方消費税を抜いた金額と、消費税及び地方消費税１０％を合計した金額が分かるように記載することとし、仕様書「１．５．契約方法及び支払方法」（１）イ～エのそれぞれの業務の内訳がわかるように記載すること。また、令和６年度～令和１１年度の年度ごとの合計金額もわかるようにすること。なお、参考見積書の合計金額が２．業務に要する費用（予定価格）を超えた場合は失格となるので、注意すること。

（ク）　業務スケジュール（任意様式）

（ケ）　誓約書（暴力団排除関係）（様式７）及び役員等一覧表（受任者を含む）（様式８）

（コ）　納税証明書（①法人市民税、②納税証明書その３の３（「法人税」及び「消費税及地方消費税」）

※申請提出時前３ヶ月以内のものに限る（写し可)。

（サ）　登記簿謄本又は登記事項全部証明書（その他の団体等で法人登記がない場合は、定款そ

の他の規約）

※申請提出時前３ヶ月以内のものに限る（写し可）。

（シ） ハードウェア・ソフトウェア要件一覧表（様式９－１～様式９－６）

提案するハードウェア・ソフトウェアについて、対応できるものには区分欄に「○」を記載して提出すること。なお、必須欄に○がない場合は失格とする。

(2) 企画提案書の作成方法及び注意事項

企画提案書は仕様書及び「７　審査方法及び配点」に基づき、提案の概要を簡潔に記入すること。

ア　原本は事業者名を入れて記載をすること。ただし、副本については提案者名や社章などの提案者がわかる内容は黒塗りをし、提出者がわからないようにすること。

イ　提出書類のサイズはＡ４とし、長辺２箇所をホッチキスで綴じる。ただし、図表等については、必要に応じＡ３折り込みは可（Ａ４の大きさに折り込むこと）とする。

ウ　カラーでの作成を認める。

エ　ページ数は表紙、表紙及び目次を除いて３０ページ以内（片面刷り、Ａ３の場合は、２ページとカウントする）で簡潔に記載すること。

オ　文字フォントサイズは１２ポイント以上とする。ただし、図表内の文字には適用しないが、読みやすいフォントサイズを選択すること。

カ　複数の企画提案書を提出することはできない。

キ　提出期限以降に企画提案書に明記していない資料の追加や提出済み資料の差し替えは不可とする。

ク　目的を達成するために必要な追加提案も可とする。この場合において、追加提案に係る費用も参考見積書に含めること。

ケ　専門知識がない者でも理解ができるようにわかりやすい内容とすること。

コ　企画提案書は、仕様書に基づき、次の章立てで作成すること。

章名	各章にて記載する内容
第１章 提案の考え方について	仕様書の１．２業務目的や、１．３業務方針で記載をしている内容に関し、３．構築業務要件を満たしつつ、１．６全体構成における図 1. 全体構成概念図にあるように、生駒市の全体構成に合わせた形で、課題解決と目標を達成するための考え方やその手法について説明すること。
第２章 クラウド基盤システム（Microsoft365 A5）の導入方針について	(1) 仕様書の２．１クラウド基盤システムで記載をしている Microsoft365 A5 導入を行うにあたっての以下のサービスについての導入方針を説明すること。 ア　認証基盤 イ　メール

	ウ　ファイル管理 エ　コミュニケーションツール オ　フィルタリング カ　ウイルス対策 キ　ファイル暗号化 ク　情報漏えい対策 ケ　デバイス管理 コ　多要素認証 サ　振る舞い検知、EDR (2)　他自治体の導入実績を紹介し、今回の提案との差異や特徴を簡潔に説明すること。
第３章 提案するセキュリティについて	今回提案するシステムにおいて本市が目指す新たな教育情報ネットワークを実現するために必要なセキュリティの構築についてシステム導入や体制の在り方などについて説明すること。
第４章 実施体制及び業務スケジュールについて	(1)　教育ＩＣＴ基盤クラウドサービス導入にあたって、実施体制の組み方やスケジュール作成にあたっての考え方や考慮する点を説明すること。 (2)　作業内容、作業量、担当の役割が明確なスケジュールを作成し、構築業務における人員の割り当てと担当者の経験年数や経歴、本業務への専従度合いが適切なものとなっているかを説明すること。 (3)　教育委員会及び各小中学校における導入後の負担感を軽減するための方策について説明すること。 (4)　令和７年４月から新しいネットワークとなることから、学校現場が混乱なく新しいネットワークを利用できるための方策について説明すること。
第５章 運用・保守・研修会について	(1)　運用・保守のサービス内容（平時・障害時）について説明すること。 (2)　ヘルプデスク等のサービス内容について説明すること。 (3)　新しいネットワーク環境下で新サービスを活用できるように、研修会の具体的提案内容と実施方式について説明すること。
第６章 セキュリティポリシーガイドライン策定支援業務	教育情報セキュリティポリシーガイドライン策定にあたり、具体的な業務内容や支援体制について説明すること。
第７章 その他	(1)　本事業の目的を達するために有用な追加提案を積極的に記載すること。

	(2)　その他、各章で記載できなかったものがあれば、本章にて説明すること。

(3)　提出期限等

ア　提出期限　令和６年７月８日（月）１７時００分まで（必着）

イ　提出場所　生駒市役所　教育部　教育指導課　教育政策室

ウ　提出方法　持参又は郵送によること。なお、郵送で提出する場合は、受け取り日時及び配達されたことが証明できる方法としてください。また、郵便事故については提案者にて責任を負うこと。

6　審査方法

プロポーザルの審査は以下のとおりとする。

(1)　第１次審査（書類審査）

審査委員会が、提出された業務実施体制回答書、ハードウェア・ソフトウェア要件一覧表及び企画提案書を審査基準に基づいて審査し、高い評価を得た提案者（３者）を選定する。ただし、プロポーザルの提案者が３者以下である場合は、第１次審査を省略し、第２次審査において提出書類審査及びプレゼンテーション等による審査を実施できるものとする。

実施日：令和６年７月１７日（水）

(2)　第２次審査（ヒアリング等による最終審査）

審査委員会が、第１次審査により選考された者に対し企画提案についてのプレゼンテーション等を実施し、審査基準に基づいて評価するとともに、書類審査を考慮し最も優れている提案を特定する。ただし、総得点が上位であっても、個別の評価項目において著しく低い評価であると認める場合は、特定者としないことができるものとする。また、審査委員会が一定の評価に達した者がないと判断する場合は、適格者なしとすることができるものとする。

なお、提案者がプレゼンテーションを行うにあたっては、企画提案書の範囲内で作成した資料を使用すること。

実施日：令和６年７月２９日(月)

(3)　審査結果の通知

ア　第１次審査

審査結果を電子メールで通知する。なお、選考された者のみ、審査結果及びヒアリング等を実施する旨を電子メールで通知する。

イ　第２次審査

審査結果を電子メールで通知する。

7　審査基準及び配点

プロポーザルは(1)及び(2)の評価内容に基づき審査する。

(1)　書類による審査　（７５点）

評価項目	評価内容	配点
業務実績	本市と同等規模以上の自治体での、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数	１０点
	本市と同等規模以上の自治体での運用実績が豊富で円滑な導入及び手厚い運用支援が期待できるか。	５点
	本市と同等規模以上の自治体での運用実績を豊富にもっており、ノウハウの蓄積があるか。	５点
ハードウェア・ソフトウェア要件	ハードウェア・ソフトウェア要件について、必須要件以外の対応ができるか。	４０点
参考見積書	予定価格に対する参考見積書の割合	１５点

(2)　企画提案内容による審査　（１２５点）

評価項目	配点
提案内容の実現性と有用性	２０点
クラウド基盤システム（Microsoft365 A5）の導入	２０点
セキュリティ	２０点
実施体制とスケジュール	１５点
運用・保守・研修会	２０点
セキュリティポリシーガイドライン策定支援業務	１５点
その他	１５点

8　日程

(1)　公示　令和６年６月１７日（月）

(2)　質問受付締切　令和６年６月２４日(月)１２時００分(電子メール又はＦＡＸ)

(3) 質問回答　　令和６年６月２８日（金）１２時００分
(4) 提案書受付期間　　令和６年６月１７日（月）～
　　令和６年７月８日（月）１７時００分　（持参又は郵送）
(5) 第１次審査（書類）　令和６年７月１７日（水）
(6) 第２次審査（プレゼン）　令和６年７月２９日（月）
(7) 結果通知　　令和６年８月上旬
(8) 契約締結　　令和６年８月上旬
(9) 業務開始　　令和６年８月上旬

9 失格事項

本プロポーザルの提案者若しくは提出された提案書が、次のいずれかに該当する場合は、その提案を失格とする。

(1) 提案書の提出方法、提出先、提出期限に適合しないもの
(2) 提案書の作成形式及び記載上の留意事項に示された要件に適合しないもの
(3) 提案書等提出期限後に参考見積書内の金額に訂正を行ったもの
(4) 第２次審査（プレゼンテーション及びヒアリング）に出席しなかったもの
(5) 虚偽の申請を行い、提案資格を得たもの
(6) 参考見積書の金額が、２.業務に要する費用（予定価格）を越えたもの

10 契約

受託候補者特定後、随意契約に係る協議を行い、協議が整い次第、速やかに随意契約の手続きを行うものとする。なお、その際には、特定された者はあらためて見積書を提出するものとする。

11 その他留意事項

(1) 提出期限以降における書類の差し替え及び再提出は認めない。
(2) 提出書類に虚偽の記載をした場合は、提出書類を無効とするとともに、入札参加停止措置を行うことがある。
(3) 提出書類は返却しないとともに、提出者の特定以外には提出者に無断で使用しない。
(4) 書類の作成、提出及びその説明に係る費用は、提出者の負担とする。
(5) 「業務実施体制回答書」に記載した配置予定の業務責任者は、原則として変更できないものとする。なお、やむを得ない理由により変更する場合には、生駒市と協議のうえ決定するものとする。
(6) 生駒市情報公開条例に基づく開示請求があった場合は、原則として開示の対象となる。ただし、提案者が事業を営む上で、正当な利益を害すると認められる情報は不開示となる場合がある。なお、本プロポーザルの受託候補者特定前において、決定に影響が出るおそれがある情報については決定後の開示とする。

12 担当部署（提出・問合せ先）

生駒市役所　教育部　教育指導課　教育政策室　（担当　三室・佐竹）
住　　所　〒６３０－０２８８　生駒市東新町８番３８号
電話番号　０７４３－７４－１１１１（内線２７３０）
電子メールアドレス　k-seisaku@city.ikoma.lg.jp

（様式１）

令和６年　　月　　日

質　　問　　書

生駒市教育系ネットワーク構築･維持管理等業務について、次の項目を質問いたします。

質 問 項 目	質　問　内　容
商号又は名称	
部署名及び担当者名	
連絡先	TEL　： Mail　：

注）記入欄が不足する場合は複写して作成してください。

（様式２）

業務実施体制回答書及び企画提案書提出届

令和６年　　月　　日

生駒市長　小紫　雅史　殿

所在地
商号又は名称
代表者職氏名

業務名　　生駒市教育系ネットワーク構築・維持管理等業務

本業務について別添のとおり、業務実施体制各種調書及び企画提案書を提出します。

（様式３）

会社概要	
会社名	
本社所在地	
委任先所在地	
設立年月	
資本金	
事業所数	
株式上場の有無	有り（　　部上場）・なし
従業員数	名
その他	
注）提出日時点で記入してください。	

（様式４）

業務実績調書			
業務名	発注者	業務内容	運用保守期間
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）
			年　月　日～ 年　月　日 （運用保守年数　年　ヶ月）

注 1）業務内容は、主になる業務内容を記入してください。
注 2）記入欄が不足する場合は複写して作成してください。
注 3）「３　参加資格(1)キ」※に該当する業務実績をすべて記入してください。
※「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。」
注 4）運用保守年数も記入してください。

（様式５）

再　委　託　調　書		
分担業務の内容	再委託先又は協力先	理由（企業の技術的特徴等）
注）他の企業等に当該業務の一部について再委託を実施する場合にのみ記入すること。 ただし、業務の主たる部分を再委託してはならない。		

（様式６）

グループ協定書

令和６年　　月　　日

生駒市長　小紫　雅史　様

（グループ代表団体）所在地

法人等名

代表者氏名

生駒市教育系ネットワーク構築・維持管理等業務の参加に当たって、グループを結成し、生駒市との間における下記事項に関する権限を代表に委任して提出します。

記

グループの名称	
グループの事務所所在地	
グループの代表者 【受任者】	代表団体　グループにおける主な役割（　　） 所在地 名称 代表者名
グループの構成団体 （その１） 【委任者】	構成団体　グループにおける主な役割（　　） 所在地 名称 代表者名
グループの構成団体 （その２） 【委任者】	構成団体　グループにおける主な役割（　　） 所在地 名称 代表者名
グループの成立、解散の時期及び委任期間	令和　　年　　月　　日から令和　　年　　月　　日まで。（ただし、当グループが委託業者とならなかった場合はこの限りでない。また、代表団体及び構成団体の変更は、事前に生駒市の了承がなければ、これを行わない。）
委任事項	１　生駒市教育系ネットワーク構築・維持管理等業務の申請に関する件 ２　契約締結に関する件 ３　契約保証金の納付及び還付に関する件 ４　入札書の提出に関する件 ５　委託料の請求受領に関する件 ６　その他（　　）
その他	１　本協定書に基づく権利義務は他人に譲渡することができない。 ２　この契約に定めのない事項については、代表団体及び構成団体全員により協議する。

※グループを結成して応募する場合は、この様式を提出してください。また、グループ構成員が３者を上回る場合は、この様式に準じて様式を作成してください。

（様式７）

誓　約　書（暴力団排除関係）

令和６年　　月　　日

生駒市長　小紫　雅史　殿

所在地
商号又は名称
代表者役
職名・氏名

当社（私）は、生駒市教育系ネットワーク構築・維持管理等業務に係る契約の締結にあたり、下記の記載内容を誓約します。

なお、この誓約に違背した場合は、生駒市から契約解除措置等のいかなる措置を受け、かつ、その事実を公表されても異存ありません。

また、下記事項の該当の有無を確認するため、求めがあるときは、役員等一覧表（様式８、受任者を含む。）を提出するとともに、生駒市が奈良県生駒警察署長に照会することを承諾いたします。

記

1　当社（私）は、次に掲げる事項に該当いたしません。

（１）暴力団（暴力団員による不当な行為の防止等に関する法律（平成３年法律第 77 号）第２条第２号に規定する暴力団をいう。以下同じ。）及び暴力団員（暴力団員による不当な行為の防止等に関する法律第２条第６号に規定する暴力団員をいう。以下同じ。）

（２）暴力団又は暴力団員と社会的に非難されるべき関係を有する者

（３）役員等が暴力団員であると認められる者

（４）暴力団又は暴力団員が経営に実質的な関与をしていると認められる者

（５）役員等がその属する法人若しくは法人格を持たない団体、自己若しくは第三者の不正な利益を図る目的で、又は第三者に損害を与える目的で、暴力団又は暴力団員を利用していると認められる者

（６）役員等が、暴力団又は暴力団員に対して資金等を提供し、又は便宜を供与する等直接的若しくは積極的に暴力団の維持及び運営に協力し、又は関与していると認められる者

（７）役員等が、暴力団又は暴力団員と社会的に非難されるべき関係を有していると認められる者

2　当社（私）は、上記１に掲げる事項に該当する者と下請契約又は資材、原材料の購入契約等の契約を行いません。

3　当社（私）は、契約の履行に当たって、暴力団又は暴力団員から不当介入を受けた場合は、遅滞なくその旨を市長に報告するとともに、警察に届けます。

注）「役員等」とは、法人にあっては役員（非常勤の者を含む。）、支配人及び支店又は営業所（市との契約に関する業務を行う事務所をいう。以下同じ。）の代表者を、法人格を持たない団体にあっては法人の役員と同等の責任を有する者を、個人にあってはその者、支配人及び支店又は営業所の代表者をいう。

（様式８）

役 員 等 一 覧 表（受任者を含む）

令和６年　　月　　日現在

所在地
商号又は名称
代表者役職名・氏名

役職名	氏名（ﾌﾘｶﾞﾅ）	生年月日	住所

※　この名簿には、法人の場合は登記簿謄本の「役員に関する事項」に記載されている役員（事業協同組合の場合は理事）を記入してください。監査役については除きます。また、契約の締結に関して営業所等に権限が委任されている場合には、その委任を受けている営業所等の代表者も記入してください。
　個人の場合については、個人事業主を記入してください。

※　法人については、法人登記事項証明書又は法人登記簿謄本を添付（写し可）してください。

※　この役員一覧表で取得した個人情報については、個人情報の保護に関する法律（平成十五年法律第五十七号）の規定に基づき適正に管理するとともに、生駒市の契約関係事務及び暴力団排除措置以外の目的には使用しません。

※　同内容の記載があれば別の書式でもかまいません。なお、欄不足の場合は適宜追加をお願いします。

（様式９-１）ハードウェア・ソフトウェア要件一覧表

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	加点対象
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	加点対象
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。		

（様式９-2）ハードウェア・ソフトウェア要件一覧表

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	加点対象
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。		

（様式９-３）ハードウェア・ソフトウェア要件一覧表

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	加点対象
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	加点対象
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	加点対象
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	加点対象
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	加点対象
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	加点対象
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。		

（様式９-４）ハードウェア・ソフトウェア要件一覧表

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	加点対象
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	加点対象
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。		

（様式９-５）ハードウェア・ソフトウェア要件一覧表

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	加点対象
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。		

（様式９-６）ハードウェア・ソフトウェア要件一覧表

教員用iPad

以下機能を有すること。

機能	機能概要	区分	
		必須	加点対象
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。		