別紙1　校務情報ネットワーク基盤システム　システム機能要求一覧表

Ⅰ．ネットワークセキュリティシステム機能要件対応

項　　目　（※は必須要件）					提案内容が当該要件を満たしている場合は〇、満たしていない場合は×（×の場合でも条件付きで満たす場合は条件を記載）
（1）	基本要件	ア）	※	SWGの機能をSaaS型で提供すること。	
		イ）	※	日本国内において複数サイトでサービスを展開していること。	
		ウ）	※	国内外の利用実績が多数あること。	
		エ）	※	外部SaaSなどでIPによるアクセス制限に対応できるために、送信元IPアドレスを固定できること。	
		オ）	※	Microsofft365との快適な通信を可能にすることにより、ユーザビリティが向上されること。	
		カ）	※	日本国内の教育機関や自治体で校務システムの運用基盤としての導入・利用実績があること。	
		キ）	※	サービスのヘルスステータスを公開するWebサイトを提供していること。	
		ク）	※	米国国立標準技術研究所（NIST）のNIST 800-63C及び800-53に準拠したサービス事業者であること。	
		ケ）	※	各サービスのソフトウェアバージョンアップやホットフィックスの適用は、サービス事業者により速やかに実施されること。	
		コ）	※	オートスケールに対応し、高負荷時に自動拡張すること、拡張時にもサービスの停止なく安定した性能を提供できること。	
		サ）	※	各種セキュリティ機能の定義やパターンのアップデートは通信の停止を伴わず自動で実施され	
		シ）	※	教育情報セキュリティポリシーに関するガイドライン（文科省）の改訂に対応すること。	
		ス）	※	クラウドサービスについては、以下の2つの認証制度を取得していること。 [認証制度] ・ISO27001（国際標準規格） ・SOC2TypeⅡ	
		セ）		クラウドサービスについては、ス）以外に、以下の認証制度を取得していること。 [認証制度] ・ISO27017（クラウドコンピューティングの情報セキュリティに関する国際規格） ・ISO27018（クラウド上に保管されている個人情報の取り扱いに関する国際規格）	
（2）	SLA（サービス品質保証）	ア）	※	可用性に対するSLA(99.99%)を提示していること。	
		イ）	※	性能(Latencyなど)に対するSLAを提示していること。	
		ウ）	※	SLAによるLatencyはパケット単位だけではなく、トランザクション単位でも設定されていること。	
（3）	ポータル	ア）	※	アクセスポリシーなどの設定を行うポータルをSaaS型で提供していること。	
		イ）	※	ユーザのWebのアクセス状況、ポリシー違反状況、検知した脅威などを一元的に可視化する機能を有すること。	
		ウ）		ユーザのアクセスポリシー、セキュリティ設定を実施可能なダッシュボードを提供すること。	
		エ）		随時設定を変更することが可能で、設定され次第すぐに反映されること。	
		オ）	※	役割に応じた管理者権限の設定ができること。	
（4）	レポート	ア）	※	事前設定済みのレポート機能が用意されていること。	
		イ）		レポートのカスタマイズ作成ができること。	
		ウ）	※	レポート配信機能を有していること。	
		エ）		SaaSサービスのリスク評価レポートを提供できること。	
（5）	認証	ア）	※	IdP(Azure AD, Oktaなど)と連携し、SAMLでユーザ認証できること。	
		イ）	※	複数のIdPと連携する機能を有すること。	
		ウ）	※	指定された端末以外での認証を拒否できること	
		エ）	※	SWGとリモートアクセスで認証頻度をそれぞれで設定できること。 (例) SWGは初回認証のみ。 リモートアクセスは1日1回認証を行う。	
（6）	接続方式	ア）	※	エンドポイントエージェントはWindows/macOS/iOS/Androidに対応していること。	
		イ）	※	GREもしくはIPSecに対応し、拠点内のサーバからの通信も保護できること。	
		ウ）		エージェントをインストールしていないクライアントの通信も保護できること。	
（7）	機能(セキュリティ)	ア）	※	時間単位でインターネットの利用制限が可能なこと。	
		イ）	※	カテゴリベースのURLフィルタリングの機能を有すること。	
		ウ）	※	アクセスコントロールの条件にユーザ、セキュリティグループ、ロケーション、組織等の情報を指定できること。	
		エ）	※	マルウェアプロテクションが実装されておりファイルやWebのコンテンツについてもマルウェア等の検知、ブロックが可能なこと。	
		オ）		既知の悪意のあるサイトだけではなく、疑わしいサイトに対する通信もブロックできる高度なセキュリティ機能を有すること。	
		カ）		さまざまなリスク要因に基づいてセキュリティ ポリシーを自動的に適応すること。	
		キ）	※	ブラウザ制御（Chrome,Microsoft browserなど)の機能を有すること。	
		ク）		L7ファイアウォール機能を有していること。(アプリ挙動、ユーザ識別でポリシー制御できること。	
		ケ）		iPhoneやAndroidのモバイル端末からの通信も保護できること。	
		コ）	※	SSLの復号化が上限なく可能なこと。	
		サ）		SSLトライフィックの復号化スキャン時、SSLターミネートに伴うroot証明書はエージェントに内包して展開できること。	
		シ）		サンドボックス分析において疑わしいファイルは、ML機能でインラインで止めることが可能なこ	
		ス）	※	CASB機能によりSaaSサービスの利用状況を可視化できること。	
		セ）	※	CASB機能によりCloudアプリケーションの利用制限できること。	
		ソ）		攻撃を検知した場合、アラートを生成し、管理者に対してメール、syslogにより通知が可能である	
		タ）		クラウド上の機械学習エンジンを使って、未知のコマンド＆コントロール（C2）の脅威を検出して、防御できること。	
		チ）	※	APIを利用したCASB機能により、SaaSアプリケーション(MS365,Sharepoint,Boxなど）の利用監視ができること。	
		ツ）		アクセスコントロールの条件にユーザ、セキュリティグループ、ロケーション、組織等の情報を指定できること。	
		テ）	※	SaaSサービスの利用状況を可視化できること。	
		ト）		SaaSサービス利用のダッシュボードのカスタマイズができること。	
（8）	機能(リモートアクセス)	ア）	※	SDP(Software Defined Perimeter)アーキテクチャによるゼロトラストネットワークアクセス機能をSaaS型で提供すること。	
		イ）		SDPによるZTNAがオンプレミス環境でもハイブリッドで利用できること。	
		ウ）	※	アクセスポリシーなどの設定を行うポータルをSaaS型で提供していること。	
		エ）		アプリケーションのヘルスステータスを確認可能なこと。	
		オ）	※	ユーザのアクセス状況を可視化する機能を有すること。	
		カ）	※	Windows/macOS/iOS/Androidに対応していること。	
		キ）		プライベートアプリケーションにアクセス可能な特定のデバイスを限定する機能を有すること。	
		ク）		校内ネットワーク、校外ネットワークを自動的に認識し、接続場所に応じてアクセスポリシーを設定できること。	
		ケ）	※	ユーザーにより、クライアントエージェントの停止を防ぐ機能を有すること。	
		コ）		ユーザーにより、クライアントエージェントのログアウト/機能停止をパスワードにより防ぐ機能を有すること。	
		サ）		特定の許可されたユーザーのみ、グローバルIPに対するインバウンドの通信を許可することなく、外部からインターネット経由で指定のプライベートアプリケーションにアクセスできる機能を提供すること。（攻撃表面を設けない方式でインターネット経由でプライベートアプリケーションへの	

		シ)		ユーザ単位でアクセス可能なプライベートアプリケーションを制御できること。	
		ス)		ユーザがアクセスしたアプリケーションを可視化可能なこと。また悪質なアプリケーションには接続できないようにすること。	
		セ)	※	オンプレミスに加えてAWS/Azureなどクラウド上にあるアプリケーションへのアクセスにも対応していること。	
		ソ)		80番/443番以外のポートでの通信にも対応していること。	
		タ)		ユーザに対して、アクセス可能なプライベートアプリケーションの一覧を表示するユーザポータルの機能を有すること。	
		チ)		アプリケーションとSDP SaaS間の接続のパフォーマンスをニーズに応じてスケールできること。	
		ツ)		マルウェアプロテクションが実装されておりファイルやWebのコンテンツについてもマルウェア等の検知、ブロックが可能なこと。	
		テ)		既知の悪意のあるサイトだけではなく、疑わしいサイトに対する通信もブロックできる高度なセキュリティ機能を有すること。	
(9)	ログ	ア)	※	リモートアクセス用のログを保持できること。	
		イ)		リモートアクセス用のログをsyslogとしてサーバに転送可能なこと。	
		ウ)	※	インターネットアクセス用のログを保持できること。	
		エ)		インターネットアクセス用のセキュリティログをsyslogとしてサーバに転送可能なこと。	
		オ)	※	SIEMなどにリアルタイムにログ送付が可能なこと。	
		カ)	※	SIEMなどにログが送れなかった際、一定期間ログを保持し再送可能なこと。	
(10)	その他	ア)	※	区立学校64校外3カ所の拠点接続がすべて可能であること。今後の増設可能性も含め67か所以上の拠点との接続が可能であり、校務支援システム「C4th」の個人連絡メール機能において、教職員同士の連絡に影響がないこと。	
		イ)	※	データセンター内に設置されているイントラシステムの閲覧、およびファイルサーバの共有フォルダの利用に影響がないこと。インターネット上にあるSharepointの利用に影響がないこと。	
		ウ)		万が一のクラウドサービス全停止の際においてレジリエンス(回復)する機能を有していること。	
		エ)		特定のサイトおよびユーザーに対してブラウザ分離(仮想ブラウザ)でアクセス制御できること。	
		オ)		ブラウザ分離の機能として、コピーペーストの制限、ファイルのダウンロード/アップロードの制限ができること。	
		カ)		端末単位でアプリのユーザー体感を可視化でき、障害発生時に原因調査できること。	
		キ)	※	端末単位でSaaSアプリのユーザー体感を可視化できること、障害発生時に原因調査できること。	
		ク)		ホップバイホップでネットワーク経路を確認できること。	
		ケ)		DNSフィルタリング(DNSベースのデータ窃取制御)ができること。	
		コ)		拠点からの通信はアプリに応じた帯域制御が可能なこと。	
		サ)	※	DLP機能による情報漏えい対策が可能なこと。	
		シ)		DLP機能にはマイナンバーに対応した辞書が含まれていること。	
		ス)	※	プライベートアプリケーションにアクセスする際には特別なツールの必要なくネットワークアクセスが可能なこと。	

Ⅱ. 統合ログ管理とシングルサインオン機能要件対応

項　　目 (※は必須要件)					要件を満たしている場合は○、満たしていない場合は×(×の場合でも条件付きで満たす場合は条件を記載)
(1)	統合ログ管理	ア)	※	統合ID監理におけるIDはガイドラインに従いIDを登録可能であること。	
		イ)	※	同一組織内における転入/転出時等にID変更を不要とするようにし、IDはパーマネント/パーシスタント(永続的な識別)として扱う。属性変更時には校務支援システム「C4th」属性情報を取得し、統合ID管理上で属性を付与すること。	
		ウ)	※	教職員及び児童・生徒のIDは属性によりグループ分けし、アクセスできる資源・アカウント・リソースを分割すること。	
		エ)	※	ガイドラインに定義される情報セキュリティ対策の監査・報告に必要な情報へのアクセスなどの権限が明確に与えられ、迅速に確認・提出できること。	
		オ)	※	外部DCに配置されている校務支援システム「C4th」よりマスターデータを取得できること。	
		カ)	※	校務支援システム「C4th」から取り込むことのできない情報(常用漢字の氏名等)に対し、教職員等のユーザーが直接入力するインタフェースがあること。また、インタフェースを利用する際には運用保守要員の補助を必要とせず、教職員のみで作業が完結できること。	
		キ)	※	統合ID管理からユーザー情報を受け取るシステムは以下とする。 ActiveDirectory(AD)(校務系) 校務支援システム「C4th」 Active!mail 校務集中ファイルサーバ Proself Microsoft365(Azure) OneDrive sharepoint Google Workspace for education まなびポケット ロイロノートスクール ミライシード	
		ク)		統合ID管理からユーザー情報を受け取るシステムの追加が容易に実現できること。	
		ケ)		校務支援システム「C4th」で更新した情報が、統合ID管理システムに取り込まれること。取込の頻度は日次以上で人の手を介さず自動で行うこと。	
		コ)		統合ID管理における各システムとのデータ連携は、ネットワーク上で行い、自動で連携すること。また、連携は日次以上の頻度で行うこと。	
(2)	シングルサインオン	ア)	※	統合ID管理システムと連携し、SSO対象のユーザー情報も一元的に管理すること。	
		イ)	※	一度の認証により一定時間は各種サービスにアクセスが行えること。	
		ウ)		複数のアクセス元からSAML、Kerberos等にて複数システムにログインさせること。	
		エ)	※	ユーザ毎に利用可能なアプリケーションを指定が可能で、証明書を持つ端末に限り、学校ネットワーク外や自己保有端末(BYOD)からもアクセスできるよう識別すること。	
		オ)	※	ログインすることで対象システムやクラウドサービスへシングルサインオンが可能なこと。	
		カ)		Active Directory と連携する専用コネクター機能を提供できること。	
		キ)	※	Microsoft Azure Active Directory と連携するコネ クター機能をクラウド サービス 側で提供できること。	
		ク)		Active Directory と連携できない場合に備え、クラウド サービス側で ログ イン が成功したときの 認証情報をキャッシュする機能を有すること。	
		ケ)	※	Webブラウザを使用してシングルサインオンのログインができること。	
		コ)	※	Webブラウザによる画面表示では日本語、英語を使用でき、言語設定はWebブラウザの設定により表示言語の自動切り替えを行うこと。	
		サ)	※	利用者単位にシングルサインオンが可能なクラウドサービスを設定する機能を有すること。	
		シ)	※	アプリケーションやWebシステムに対して代理入力方式 によるシングルサインオンが可能なこと。	
		ス)		代理入力方式によるシングルサインオンでは、フォームベース認証、基本認証、アプリケーションの認証に対応すること。	
		セ)		SAML 連携および代理入力によるシングルサインオンは SaaS やオンプレミス環境を問わず対応できること。	
		ソ)	※	代理入力によるシングルサインオンは、Windows、iOS、Android環境で利用できること環境で利用できること。	

		タ)	※	代理入力によるシングルサインオン連携対象は、管理者による登録、管理ができ、連携対象を登録するためのサポート機能が提供されていること。	
		チ)		利用者がシングルサインオン 設定を行う 際に、代理入力用の ランダムパスワードを生成する機能を有すること。	
		ツ)		クライアント端末が一時的に本サービスに接続できない場合でも代理入力によるシングルサインオンが行えること。	
		テ)	※	Windows ログインとクラウドサービスのシングルサインオンが実現できること。	
		ト)		個々の利用者が利用可能な W eb シングルサインオンが表示される利用者ポータル機能を有すること。	
(3)	管理者機能	ア)	※	管理 GUI を備えること。	
		イ)	※	導入時のセットアップを簡単にする設定ウィザード機能を有すること。	
		ウ)	※	管理ログ、管理者ログインログ、利用者ログインログ、利用者操作ログ、同期実行ログ、SSOアクセスログを閲覧・検索が可能であること。	
		エ)	※	管理ログ、管理者ログインログ、利用者ログインログ、利用者操作ログ、同期実行ログ、SSOアクセスログをファイル出力する機能を有すること。	
		オ)	※	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。	
		カ)		ユーザーのクラウドサービス利用状況を管理者が参照できること。	
		キ)	※	IdP証明書の有効期限切れ前に、事前に管理者へメールで通知をする機能を有すること。	
		ク)		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。	
		ケ)	※	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。	
		コ)	※	シングルサインオンとして利用するクラウドサービスの有効化・無効化できる機能を有すること。	
		サ)	※	認証サーバーとして複数のActive Directory 、 Microsoft Azure Active Directory が連携できること。	
		シ)		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。	
(4)	セキュリティ機能	ア)	※	Web管理画面、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。	
		イ)	※	クライアント証明書によるWeb管理画面、ログイン画面のアクセス制御ができること。	
		ウ)		Web管理画面、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。	
		エ)	※	Web管理画面、ログイン画面のアクセスをIP アドレス により制御ができること。	
		オ)	※	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。	
		カ)		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	
		キ)	※	運用する者は、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。	
		ク)	※	ISMS クラウドセキュリティ認証 (ISO27017) を取得していること。	
		ケ)		ISMAP を取得している、または取得予定であること。	
		コ)	※	登録する利用者アカウントのパスワードポリシーを定義できること。 1. パスワードの最小文字数、最大文字数を設定できること。 2. パスワードへの使用を禁止する文字を設定できること。 3. 以前に使用したパスワードの履歴を記録し以前使ったことがあるパスワードを繰り返し使用できないよう設定できること。 4. パスワードに大文字、小文字、数字、記号を含むよう複雑さの条件を設定できること。 5. 利用者のログイン名が含まれるパスワードの使用を禁止できること。 6. パスワード有効期間を設定できること。 7. パスワード変更後、再度パスワードを変更できるようになるまでの期間を設定できること。	
		サ)	※	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。 1. 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 2. 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 3. 同期 実行 の実施日時、成功 失敗、処理内容 4. SAML 連携時の シングルサインオンに関するログ	
		シ)		登録する利用者アカウントの パスワード有効期限が切れた際に、利用者にメールで通知できる	
		ス)		登録する利用者アカウントのパスワードリセット機能を提供すること。	
		セ)		登録する利用者のアカウントについて、連続でログイン失敗した際、アカウントを自動ロックする機能をもつこと。	
(5)	校務情報へのアクセス制御	ア)	※	アクセスコントロールの条件にユーザ、セキュリティグループ、ロケーション、組織等の情報を指定できること。	
		イ)		ブラウザ分離の機能として、コピーペーストの制限、ファイルのダウンロード/アップロードの制限ができること。	
(6)	庶務事務情報へのアクセス制御	ア)	※	アクセスコントロールの条件にユーザ、セキュリティグループ、ロケーション、組織等の情報を指定できること。	
		イ)		ブラウザ分離の機能として、コピーペーストの制限、ファイルのダウンロード/アップロードの制限ができること。	

Ⅲ. 端末セキュリティ機能要件対応

項　　目 （※は必須要件）					要件を満たしている場合は〇、満たしていない場合は×（×の場合でも条件付きで満たす場合は条件を記載）
(1)	機密情報へのアクセス制御と情報漏えい防	ア)	※	機密情報へのアクセス制御と情報漏えい防止正当にアクセス権限を有する者のみが機密情報へアクセスできるように、アクセス制御を実施し、不正接続を排除すること。機密情報の漏えいやデータの改ざんを防止する対策を行うこと。	
(2)	マルウェア 等への対策	ア)		ゼロトラストネットワーク化に伴い、マルウェアの侵入を防ぐことは無論、侵入をいかに早く検知し、被害拡散を防止するとともに迅速に復旧するかが重要となる。また、テレワーク環境の実装に伴い、学校外での端末利用時に一層の注意を払う必要が生じる。以上の点から、エンドポイントセキュリティについて、EPP（エンドポイント保護）とEDR（エンドポイントにおける検出と対応）の二層に分けて提案すること。ただし、提案ソリューションがEPPとEDRの両方の機能を十分に有している場合は、当該単一ソリューションのみを提案しても差し支えない。	
		イ)	※	多層防御の考え方に基づき、本仕様書で規定するEPP及びEDRに加え、他メーカーの製品も含め、SASE等の各セキュリティ機能、フィルタリングソフト等などによる重層的な構えを築くこと。	
		ウ)	※	セキュリティパッチを適用するのに帯域負荷がかかると想定される場合は、段階的に適用する仕組を構築すること。	
(3)	EPP	ア)	※	リアルタイム検知（ファイル入出力・WEBアクセス等のあらゆるアクション）、時間を設定した予約検索及び手動検索の全てに対応していること。	
		イ)		予約検索実施時には利用者に事前通知を示せること。	
		ウ)	※	USBメモリなどの外部ストレージデバイスや、ネットワークリソースに対するアクセス制御ができる機能を有していること。	
		エ)	※	USBストレージデバイス等外部記憶媒体を端末に挿入した際に、自動的にUSBストレージ内のファイルに対して不正プログラムの検索をする機能を有すること。なお、パスワード機能付きUSBストレージデバイス等については、パスワードを認証した直後に不正プログラムの検索を行うなど、マルウェアが動作する前にチェックが行われること。	
		オ)		シグネチャ検知に加え、未知や亜種のマルウェアも検知及び隔離できるよう、「動的ヒューリスティック検知（ビヘイビア法）」及び「静的ヒューリスティック検知」を備えたソリューションを実装すること。	
		カ)		EPPにおいてC＆Cサーバへの接続を検出し、ブロックする機能を有すること。なお、C＆Cサーバ情報は定期的に取り込むこと。	

(3)	EPP	キ)	※	EPPに無償のソフト(Microsoft Defenderなど)を用いても差し支えないが、貴社の他の提案を含めて一元管理ができるよう留意すること。 具体的には、以下を満たすこと。 ・Microsoft Defender等におけるリアルタイム保護の状態やシグネチャのバージョン、スキャン実行日時など、各端末におけるMicrosoft Defender等の稼働状態を管理コンソールで確認できる機能 ・Microsoft Defender等における脅威検出、シグネチャ更新、スキャン実行などの主要なイベント／ログを管理コンソールで確認できる機能 ・Microsoft Defender等のシグネチャのアップデート命令配布およびスキャン命令配布が管理コンソールから実行できる機能	
		ク)	※	マルウェアの検知に必要な情報(エンジン更新やシグネチャ情報)を定期的に自動でクライアントにアップデートする仕組を整えること。	
		ケ)		クライアントに対するウイルス定義ファイルなどの配信時に、ネットワークの負荷を軽減するよう、差分パターンファイルのみの配信が可能なこと。	
(4)	EDR	ア)	※	EDRの目的は、感染後の迅速な隔離、状況把握、対応一元化、ログ収集、他端末／ネットワークへの被害拡散防止等である為、SOC等のサービスを経由することなく ZDPエンジン、スタティック分析エンジン、サンドボックスエンジン、HIPSエンジン、機械学習エンジン等の最低5つのエンジンを用い、マルウェアの検知、検知ファイルの隔離、およびマルウェアを検知したクライアントコンピューターをネットワークから自動的に遮断を行う機能を有すること。	
		イ)		脆弱性攻撃の防御、マルウェア特有の振る舞いの検知や、仮想環境でのプログラム実行による検知(サンドボックス)などの機能を組み合わせて有しており、未知のマルウェアやゼロデイ攻撃などに対しても、パターンファイルのみに依存しない多層的なマルウェア検知が可能であること。	
		ウ)	※	改竄されたレジストリや設定ファイルを復旧する機能を有すること。	
		エ)	※	収集したログの分析が可能であること。	
		オ)		検知ログをSyslogにて転送できること。その際、情報の分析や操作を容易にするための標準形式であるCEFフォーマットを選択できること。	
		カ)	※	検知ファイルと本ソフトウェアで収集した操作ログを紐づけて、マルウェアの侵入経路を調査し、他端末へのマルウェアの存在確認およびネットワーク遮断が行えること。また、調査結果および確認結果はレポートとして出力できること。	
		キ)	※	ネットワークから遮断した端末及び隔離した検知ファイルは、マルウェア駆除など安全が確認できた後、管理機能から復旧できること。	
		ク)		EDRの判断により遮断設定を行った脅威については、他の端末も含め、ネットワーク全体として以後自動的にブロックできること。	
		ケ)		EDRが収集したログは、ファイル名、ドメイン、IPアドレスなどから複数の条件を選んで本区職員が検索できること。	
		コ)		ソフトウェアの開発・保守サポートはすべて日本国内で行われていること	
(5)	テレワーク	ア)	※	端末、教職員が管理するスマートフォン等の携帯デバイス、ログイン用トークン(USBなど)の3つを入手した第三者が本ネットワークやシステムへのログインを試みたとしても、ログインを拒否できる仕組を整えること。(例:生体認証を必須とすることで拒否)	
		イ)	※	端末紛失等に備え、全体管理者はリモートロック(ログイン不可設定)が行えること。	
		ウ)	※	端末紛失等に備え、全体管理者はリモートワイプ(消去と初期化)が行えること。	
		エ)	※	クライアントコンピューターを紛失した際などに、インターネットを経由して遠隔から、クライアントコンピューターの画面をロックし操作の制御を行うことや、あらかじめ登録したクライアントコンピューター上の指定フォルダの削除を行う機能を有すること。また、GPSやWi-Fi、IPアドレス、携帯電話基地局からの取得情報を用いて、クライアントコンピューターの位置情報をインターネット	
		オ)	※	テレワーク実施時における個人情報の保護・漏洩防止に留意すること。	
		カ)	※	テレワーク実施時は外部記録媒体の接続を原則として禁止すること。「テレワーク実施時」という条件付けが困難である場合は、常時実施する仕様としてもよい。	
		キ)	※	テレワーク実施時、校務システムなどの機密情報を取り扱う場合は、コピー＆ペーストを禁止するなどの漏洩防止措置を施すこと。「テレワーク実施時」という条件付けが困難である場合は、常時実施する仕様としてもよい。	
		ク)		テレワーク時における、業務に無関係な私的利用を抑止する方法があること。(業務利用との線引きが難しいので、操作ログや閲覧画面情報を確保する等の方法になると思われる。)	
(6)	端末制御	ア)	※	ウイルス感染時等の特定の条件下において、障害発生前後の挙動がわかるよう画面操作を録画できる機能を有すること。	
		イ)		SKYSEA Client Viewの管理コンソール上からマルウェア感染時のマルウェアの挙動監視及び追跡が行えること。	
		ウ)		端末がマルウェアに感染した際に、当該端末のWebへの通信を遮断しつつSKYSEA Client Viewの管理コンソールからリモート操作による復旧作業は継続できる仕組みを有すること。	
		エ)	※	BitLockerによるドライブ暗号化が実施されていないクライアントコンピューターに対して、暗号化実施を促すメッセージを自動的に表示できること。また、クライアントコンピューターに表示されたメッセージ画面から、管理者が事前に設定した内容に沿ってBitLockerによるドライブ暗号化をユーザーが実行できること。	
		オ)	※	BitLockerおよび他サードパーティ製品により、ハードディスクを暗号化した際に生成される回復キーを収集し、管理できること。収集したBitLockerの回復キー情報はCSV形式でエクスポートできること。また、これらの暗号化状態をハードウェア一覧で確認でき、暗号化状態が変更された時はドライブログとして記録できること。	
		カ)	※	クライアントコンピューターがあらかじめ指定した設定条件に適合しているかを、PCログオン時に自動で判断し、結果をクライアントコンピューターに表示できること。不適合があれば、クライアントコンピューターに通知し、ユーザーに対処法を案内する仕組みを有すること。 クライアントコンピューターを管理する管理画面で、セキュリティ診断結果を、端末機別・診断項目別に確認できること。	
		キ)	※	診断項目は部署ごとに設定できること。設定条件には、ウイルス対策ソフトウェアのインストール状態/有効化状態/定義ファイル更新状態、Windows更新プログラムの適用状態、Windows Updateの更新プログラムのチェック実行状態、WSUSサーバーの設定状態、Windows Defenderのスキャン状態/保護状態、OSバージョンの更新状態、指定したアプリケーション/不許可アプリケーションのインストール状態、アプリケーションの更新状態、Windowsへのログオンパスワード設定状態、スクリーンセーバー設定状態、BIOSパスワード設定状態、Guestアカウントの設定状態など、クライアントコンピューターのセキュリティに関する項目を指定できること。	
(7)	データ暗号化	ア)	※	紛失時にHDDの盗難を想定し、BitLockerおよび他サードパーティ製品によるドライブ暗号化を図ること。運用観点から暗号化の回復キーの一元管理ができること。また、セキュリティの観点からドライブの暗号化状態が変更された時はドライブログとして記録出来ること。	
		イ)	※	マルウェア感染時に校務データの情報漏洩が発生したとしてもファイル単位で暗号化されており、外部ユーザーが読み取れない仕組みを有すること。	
		ウ)		任意のフォルダを自動暗号化フォルダとして設定し、自動暗号化フォルダにファイルやフォルダをコピー・保存することで自動的に暗号化できること。また、指定したWebサイトにファイルをアップロードする際、自動暗号化フォルダに格納されている暗号化されたファイルのみをアップロードするよう設定ができること。	
		エ)		暗号化形式は、復号ツールを使用して復号する形式、もしくは復号ツールが不要なパスワード付きzipファイルを作成する形式から選択できること。	
		オ)		暗号化ファイルは、本ソフトウェアをインストールした組織内のPCでのみ復号が可能に設定でき	
		カ)		暗号化の際、パスワード入力の失敗回数の上限および復号可能な期間を設定できること。	
(8)	教職員の多要素認証	ア)	※	ID/パスワードに加え、生体認証(静脈認証、虹彩認証、顔認証等)を設定し、認証装置の配布方法や紛失対策などの運用が容易であること。	
		イ)	※	個人の生体認証は、クラウド上に残さないこと。	
(9)	児童・生徒認	ア)	※	ID/パスワードによる認証とすること。	

Ⅳ. データセンターセキュリティ機能要件対応

項　　目（※は必須要件）					要件を満たしている場合は〇、満たしていない場合は×（×の場合でも条件付きで満たす場合は条件を記載）
(1)	有人管理時間	ア)	※	24時間365日常駐していること。	
(2)	室内監視カメラ	ア)	※	監視カメラを有すること。	
(3)	耐震／免震化	ア)	※	耐震対策又は免震対策を行っていること。	
(4)	火災警報設備	ア)	※	火災警報設備を有すること。	
(5)	ハザードマップ浸水区域内／外	ア)	※	ハザードマップ浸水区域外であること又は区域内の場合、床上げなど水害対策を講じていること。	
(6)	落雷対策	ア)	※	落雷対策を施してあること。	
(7)	非常電源装置	ア)	※	N構成以上であること。	
(8)	非常時連続運転可能時間	ア)	※	停電時に24時間以上電源を供給できること。	
(9)	入退室管理方法	ア)	※	生体認証、共連れ防止ゲートを有すること。	
(10)	入退室ログ管理状況	ア)	※	入退室者のログを管理できること。	
(11)	サーバ操作ログ管理状況	ア)	※	サーバの操作ログを管理できること又は運用作業はダブルチェックを行い、作業歴を保管すること。	
(12)	その他特筆したいこと	ア)		通信設備がマルチキャリアを有すること等	

Ⅴ.システムサポート機能要件対応

項　　目（※は必須要件）					要件を満たしている場合は〇、満たしていない場合は×（×の場合でも条件付きで満たす場合は条件を記載）
(1)	運用監視	ア)	※	24時間365日システム監視していること。	
		イ)	※	障害の切り分けを行い対応できること。	
(2)	コールセンター運営	ア)	※	サポートデスクは平日9時から18時までの電話受付を可能とし、WEBフォーム又は専用メーリングリストでの受付は24時間365日可能とすること。	
		イ)	※	教職員やICT支援員からの問い合わせを一元的に受け付けるサポートデスクを置くこと。	
		ウ)	※	機器及びクラウドサービス等の故障・破損について対応すること。	
		オ)		機器及び学習用クラウドサービス、導入アプリなどの操作問い合わせについて対応すること。なお、MS365、Google関連については、メーカー直接またはヘルプデスク用のアカウントを作成し対応できること。	

Ⅵ.インターネット接続回線機能要件対応

項　　目（※は必須要件）					要件を満たしている場合は〇、満たしていない場合は×（×の場合でも条件付きで満たす場合は条件を記載）
(1)	インターネット接続回線	ア)	※	各拠点への固定IP設定すること。	
		イ)	※	各拠点の装置は、特定の機種に限定されず汎用的な製品を利用できること。	
		ウ)	※	将来的にトラフィックが増加した際に対応できるよう、帯域の増強に柔軟に対応できること。	
		エ)	※	StaticまたはBGPを使用したルーティングが可能であること。	
		オ)	※	下り最大10Gbps、上り最大10Gbpsであること。	
		カ)	※	24時間365日のオンサイト保守ができること。	
		キ)	※	ONU（回線終端装置）からインターネット接続に関わる直前までの一元サポートができること。	

Ⅶ. システム連携要件（現在のシステム運用事業者との調整事項）

項　　目（※は必須要件）					協議・調整結果
(1)	NTT東日本	ア)	※	Azure、TEAMS、sharepoint等のMicrosoft365A3ライセンス使用機能	
		イ)	※	校務支援システム（エデュコム「C4th」）	
		ウ)	※	ファイリングサーバシステム	
(2)	富士電機ITソリューション	ア)	※	校内LAN及びCiscoDNAセンター	
		イ)	※	電子黒板（教員用タブレット）システム	
(3)	ライオン事務器	ア)		区立学校図書館システム（㈱OEC　探調TOOL DX2　等）	

（注）参考見積書作成時に、各社とのシステム設定を引き継ぐための作業経費の算出が必要なため、原則、本件提案に先立って各システム運用事業者と協議・調整を行うこと。