

渡嘉敷村立学校ネットワーク統合後
端末整備事業業務委託

仕様書

令和7年9月
渡嘉敷村教育委員会

1. 件名

渡嘉敷村立学校ネットワーク統合後端末整備事業業務委託

2. 背景・目的

本事業では、文科省より発出された「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7年3月)」の示す、「強固なアクセス制御によるセキュリティ対策」環境を構築し、「GIGA スクール構想の下での校務DXについて～教職員の働きやすさと教育活動の一層の高度化をめざして～」で示されている、ロケーションフリーでの教職員の働き方改革を推進し、安全なセキュリティを担保したうえで働きやすい環境を整備することで、教職員の負担軽減と、児童・生徒と向き合う機会を増やすことを目的とする。

3. 履行場所

- (1) 渡嘉敷村立 渡嘉敷小学校
- (2) 渡嘉敷村立 阿波連小学校
- (3) 渡嘉敷村立 渡嘉敷中学校

4. 履行期間

契約締結の日から令和7年11月30日まで

5. 提出書類

完成図書

- (1) 要件定義書および設計書
- (2) システム運用マニュアル
- (4) 障害対応マニュアル
- (5) 教職員操作手順マニュアル
- (6) 調達した各ライセンス証書
- (7) 機器保証書
- (8) その他、発注者が提出を求めるもの

6. 現行の諸課題

- (1) クラウドシステムにセキュアに接続するための「ゼロトラスト環境」が未構築
- (2) 校務系ネットワークと学習系ネットワークの分離
 - ① 教職員1人につき2台の調達及び管理等に係るコスト発生
 - ② 校務執務場所の固定化
- (3) オンプレミス型ファイルサーバー(NAS等)
 - ① 校外からのアクセス禁止によるリモートワーク不可
 - ② サーバー管理やメンテナンスに関するオンサイト対応の負荷
 - ③ 経年劣化などによる機器の性能低下

(4) 校務用端末の課題

- ① 機器の性能不足などによる活用効果の低下
- ② 強力なセキュリティ対策を施した自社製 BIOS 端末の未整備
- ③ 要素認証対応デバイス未搭載によるゼロトラスト環境非対応
- ④ 高度なアンチウイルスおよびエンドポイント対策(EDR 等)未実装
- ⑤ ディレクトリサービス未導入による制御環境等の未整備

7. 事業詳細

次に記載されている業務を実施すること。

(1) ゼロトラスト環境基盤の構築

次に示すゼロトラスト環境の構築に必要な機能について、Microsoft 365 Education A5 を採用し、それに含まれる諸機能を主として構築すること。

① ID 統制 (IDaaS)

- a) ID 管理及び各システムへの認証基盤としての機能を備えていること
- b) 人事異動などが発生した際に、アカウントの随時追加、削除、編集等が可能であること。
- c) 既存の Google Workspace for Education のアカウント情報を引継ぎ、発注者が業務で使用する連携可能な各システム及びサービスとシングルサインオン連携またはユーザー情報連携が可能であること。
- d) 管理者(発注者が指定する本村教育委員会に所属する職員および一部の教職員を指す。以下同様。)が許可した端末およびその利用者のみがサービスを利用できるよう制御できること。また、ユーザーが通常と異なるネットワークやブラウザなどからアクセスしようとした場合に、追加の認証を要求するなど、動的な認証を実施できること。
- e) 知識認証(ID 及びパスワード等)、生体認証(指紋、静脈、顔、声紋等)、物理認証(IC カード、USB トークン、トークン型ワンタイムパスワード等)のうち、異なる認証方式2要素以上を組み合わせた多要素認証機能を構築すること。また、将来的な運用を考慮し、沖縄県次世代型校務支援システム県域共同調達で選定された製品との多要素認証も可能であること。

② 端末管理・保護 (MDM)

- a) Windows Update やアプリケーションの配信などの一斉配信や管理が可能であること。その際、配信の時間帯を発注者が任意に指定でき、ネットワークなどの負荷分散を図る機能を備えていること。
- b) IDaaS と連携し、管理者が許可していない端末からのログインを制御できること。
- c) 端末紛失時に遠隔操作で端末のデータ消去が可能であること。なお、ネットワークに接続していない場合は、次回接続時に即座にメール等で管理者へ当該端末情報を通報できること。
- d) Bluetooth や外部記憶媒体などへの接続を端末ごとに制御できること。
- e) ネットワーク接続している機器のログを収集し、可視化及び分析が可能であること。

- ③ 高度なアンチウイルスおよびエンドポイント対策 (EDR 等)
 - a) パターンマッチングに加え、機械学習やふるまい検知などの技術を用いることで、既知・未知を問わずマルウェアの検知と遮断が可能であること。
 - b) IDaaS と連携し、脅威が検出された際に、即座にメール等で管理者へ当該端末やユーザー情報を通報できること。また、遠隔操作で当該脅威の除去や端末をネットワークから隔離することが可能であること。
 - c) 常に最新のセキュリティ状態を更新できること。

- ④ ネットワークセキュリティ (SWG、CASB、IDS/IPS 等)
 - a) IDaaS と連携し、悪質な Web サイトやアプリケーションへのアクセスを制限 (フィルタリング) できること。また、フィルタリング設定において、グループごとのルール設定やホワイトリスト運用が可能であること。
 - b) 事前に定義した不正アクセスパターンとのマッチング技術などを用いて、クラウドへの不正なアクセスを検知・遮断できること。
 - c) 個人契約テナントやシャドーIT など、セキュリティ上懸念のあるサービスへのアクセスを制御できること。
 - d) SWG (Secure Web Gateway) として、Microsoft 365 A5 に含まれる Defender for Endpoint を活用し、有害情報の含まれる Web サイトや、マルウェア、フィッシングなどのセキュリティ脅威の高いサイトをブロックして、教職員が安心してインターネットを利用できる環境を提供すること。また、Web フィルタリングソフトとして、カテゴリごとにサイトをブロックでき、管理者側でブロックリストの追加や変更を簡単に行えること。

- ⑤ クラウドストレージ及びデータ漏えい防止 (DLP/IRM 等)
 - a) IDaaS と連携してユーザー及びグループごとにフォルダへのアクセス権限を制御できること。また、各ユーザーがアクセス可能なフォルダに対し、Windows 標準のエクスプローラーからショートカットを用いて直接接続できるように、個別設定のためのマニュアルを作成し、MDM などを利用してクラウドストレージへのショートカットを一斉配信できる設定があること。フォルダ構成及びアクセス権限については発注者と協議の上決定する。
 - b) 自動暗号化技術により、アクセス権限がないユーザー (第三者を含む) がファイルを扱えないように制御できること。アクセス権限はユーザーの職位などに応じて柔軟に設定可能であること。また、事前に定義された重要度に応じたファイルの操作ログ、もしくはすべてのファイルストレージからのファイルのダウンロードを検知できること。
 - c) 原則として、ストレージサービスとしては、個人データの保存領域に OneDrive を使用し、学校・校区・全校での連携領域には SharePoint Online を利用すること。SharePoint Online では、学校や職種、校区ごとにフォルダを作成し、教職員間でデータを共有・共同編集することが可能であり、教職員の所属校や職種に応じてフォルダへのアクセス権を細かく制御すること。また、自宅や出張先からも、学校と同様にファイルにアクセスして業務が可能であること。

⑥ テスト

- a) 発注者と協議に基づいて作成した要件に規定された、アクセス制御などセキュリティに関する諸設定が設計どおりに動作することを確認すること。
- b) 上記以外で受注者が必要と判断したテストについては、適宜提案すること。

(2) 機器の調達

ゼロトラスト環境に対応可能な以下の仕様を満たす以下の機器を調達すること。

① 教職員指導者用端末（調達台数：35 式）

項目	仕様(同等以上の性能を有すること)
形状	ノート型パソコン
機器メーカー	NEC、富士通、Dynabook のいずれかのメーカーとする。納入は一つのメーカー及び機種に統一し納品すること。参考機種/ Dynabook / G83/LY
OS	Windows 11 Pro 64 ビット(24H2)
CPU	インテル® Core™ i5-1334U プロセッサ
ディスプレイ	13.3 型以上 15.6 型以下 FHD 高輝度・高色純度・広視野角 (ノングレア)
Web カメラ	有効画素数 92 万画素 (デュアルマイク付)+顔認証センサー
メモリ	16GB
ストレージ	512GB SSD(PCIe、NVMe 対応)
有線 LAN	1000Base-T/100Base-TX/10Base-T
無線 LAN	Wi-Fi 6E(IEEE802.11ax)(2.4Gbps)+IEEE802.11ac/a/b/g/n
Bluetooth	Bluetooth® (Ver5.3)
マウス	有線光学式マウス
キーボード	86 キー (JIS 配列準拠)、キーピッチ:19mm、キーストローク:1.5mm
インターフェース	HDMI×1、USB3.2 (Gen1)×2、LAN コネクタ×1、SD カードスロット×1 Thunderbolt™ 4 (USB4™ Type-C) コネクタ (電源コネクタ)×2 マイク入力/ヘッドホン出力端子、セキュリティロックスロット
セキュリティ基準	・NIST SP 800-147/155/193 準拠 ・自社製 BIOS による BIOS 改ざんを保護する機能を備えていること ・TPM(TCG Ver2.0 準拠)
堅牢性	MIL 規格 (MIL-STD-810H) に準拠していること
質量	880g 以下
外形寸法	306.0(幅)×210.0(奥行)×17.9(高さ) mm 以下
駆動時間	7.5 時間 (動画再生時) / 21.0 時間 (アイドル時)
適用ライセンス	Microsoft 365 Education A5
保証期間	5 年引取修理
環境調和	EPEAT 認証で Gold を取得していること

② 村職員指導者用端末(調達台数 : 2 式)

※調達要件(仕様)については、①で示した製品に準ずるものとする。

(3) 端末の保管およびキッティング作業

- ① キッティング対象端末は、上記(2)で調達した端末とする。
- ② キッティング内容については、契約締結後、発注者と協議して決定する。
- ③ マスターデータを作成し、テスト運用および検証を経て他の新規端末へ展開すること。
- ④ 端末の設定は Intune を使用した Autopilot で行い、端末故障時の再インストールや年次更新作業におけるリフレッシュ作業を簡易に行えるように構築を行うこと。また、ソフトウェアや端末の制限事項等の詳細な設定も事前に行い、端末を初期化するだけで発注者の環境がクラウドから自動的に復元されるように設定すること。
- ⑤ 村職員指導者用端末は、指定のソフトウェアをインストールし、各学校の指示に基づいて設置を行うこと。
- ⑥ 設定の不具合等が判明した場合、迅速かつ誠実に対応し、早急に解消すること。

(4) 既存環境の移行

- ① 各学校に設置されているファイルサーバー(全3拠点)上のデータを、構築したクラウドストレージに移行する作業については、効率的な実施時期及び手法を提案し、移行作業を実施すること。
なお、クラウドストレージ内のフォルダ構成は学校環境に適した最適な構成とすること。
- ② 現在稼働中の各学校に設置されているプリンター及び複合機等の IP アドレス変更、新規端末へのドライバインストール等について、効率的な実施時期及び手法を提案すること。
- ③ 端末の入れ替え期間中に、現行端末と新規端末が混在することを考慮し、業務への影響を最小限に抑えるための対応策を随時提案及び実施すること。

(5) 操作手順マニュアル等の作成

- ① 操作手順マニュアル等を作成し、後日でも随時確認ができるようにすること。
- ② 操作手順は、多要素認証によるログイン方法から Microsoft365でのデータの作成・分類方法及びクラウドストレージ(Onedrive または SharePoint)に保存するまでの流れを中心とした内容とすること。

(6) 運用保守体制

- ① 本事業に携わる人員の緊急連絡先等を記載した体制表を提出すること。
- ② 発注者からの問い合わせ、課題等に迅速に対応すること。
- ③ 発注者からの問い合わせ方法は電話やメールにて対応すること。

(7) 運用保守内容

① 設定変更及び更新業務

本業務で整備したシステムおよび機器について、暫定対策やセキュリティ対策の見直しが必要になった場合に設定変更を実施すること。教職員の異動に伴う必要な作業は年次移行時ではなく随時実施すること。また、発注者の求めに応じて技術的助言および支援を行うこと。

② 運用支援

本事業で構築したシステムについて、教職員および教育委員会のセキュリティ対策の強化や業務効率化に資する機能や活用方法を随時情報提供すること。

③ 機器等の不具合、故障発生時は、症状切り分けを行い、故障の場合は速やかに機器を回収しメーカーにて修理を行い、正常な状態に復旧させること。また、復旧後はすぐに使用できるように再設定を行ったうえで返却すること。

④ 復旧に時間を要する場合は、代替え機を手配し対応すること。

⑤ 運用保守期間は導入後 5 年間とする。

⑥ 令和 10 年までに整備予定の次世代型校務支援システムへの多要素認証設定も含めるものとする。

<別紙> 納品先一覧

No.	項目	渡嘉敷小学校	阿波連小学校	渡嘉敷中学校	数量計
1	教職員指導者用端末	12	12	11	35
2	村職員指導者用端末	1	1	-	2