

校務系ネットワーク更新事業
仕様書

五島市教育委員会

第1 基本事項

1 業務名称

五島市校務系ネットワーク更新事業（以下「本事業」という。）

2 目的

五島市（以下「発注者」という。）は、クラウド型統合型校務支援システム（以下「校務支援システム」という。）を、令和9年度から利用（令和9年4月から試行予定）することを予定している。

本事業では、文部科学省が発出した「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）」（以下「ガイドライン」という。）で示す「アクセス制御による対策を講じたシステム構成」（以下「ゼロトラスト環境」という。）を構築することにより、校務支援システムへのセキュアな接続環境を整備するとともに、後述する現行の校務系ネットワークに係る諸課題を一体的に解消することで、長期間にわたって安心かつ安全に教職員が勤務できる環境整備を目的とする。

3 事業実施場所

別添1「実施場所一覧」のとおり

4 履行期間

契約締結日から令和13年12月31日まで

- ・令和8年12月31日まで ネットワーク構築
- ・令和9年1月1日以降 運用・保守

5 守秘義務及び情報セキュリティ等の確保

- (1) 受注者は、本事業により知り得た内容及び結果を第三者に漏らしてはならない。
- (2) 受注者は、業務で使用する各種資料やデータに含まれる機密情報や個人情報等の紛失、漏えい等が発生しないように、データセキュリティ対策及び個人情報保護対策を講じなければならない。
- (3) 受注者は、業務上取り扱う機密性の高い資料等について、運搬時の紛失等における情報漏えい事故を防止するため、電子メール、データ交換サービスを用いて、データの授受を行う。なお、必要に応じて、発注者へ申請のうえ、受注者が用意したセキュリティ USB メモリ等での対応も可能とする。また、発注者へ提出するデータ等は、事前にウイルスチェック等を実施すること。

(4) 本事業で構築する環境等については、ガイドライン及び「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目指して～（令和5年3月）」を逸脱しないものとするとともに、関係法令、条例及び規則等を順守すること。

(5) 履行期間中にガイドライン等が改訂され、追加で環境整備を行う必要がある場合は、適宜提案を行うこと。

6 著作権

本事業で作成されたドキュメント、データに関する著作権については、発注者に帰属する。ただし、成果物に受注者又は第三者の著作物が含まれる場合、受注者が本事業を行うにあたり、新たに作成した著作物を除き、当該著作物の著作権は従前から著作権者に帰属する。

7 疑義

本仕様書に定めなき事項または疑義が生じた場合は、発注者と受注者にて協議の上で、決定する。

8 損害賠償及び不適合責任

受注者が業務の履行に関し、自己の責に帰すべき事由により発注者に損害を与えたときは、受注者の負担において発注者の指定する期限までに原状に回復するか、またはその損害を全額賠償するものとする。また、完了後の過失等に起因する不良箇所が発見された場合は、受注者の負担で修正及びその他必要な作業を行うものとする。

9 再委託

受注者は、本事業を第三者に委託し、又は請け負わせることはできない。ただし、あらかじめ発注者の承認を受けた場合には、業務の一部を委託することができる。

10 問合せ等管理

受注者は、全履行期間において使用できるプロジェクト管理ツールを調達して、本事業に携わる発注者及び受注者の担当者全員分のアカウントを確保し、発注者からの問合せ等を管理すること。

11 現行の校務系ネットワークに係る諸課題

- (1) 校務支援システムに https でセキュアに接続するためのゼロトラスト環境未構築
- (2) 校務系ネットワークと学習系ネットワークの物理的分割
 - ア 校務系及び学習系間のデータ連携困難
 - イ 校務系ネットワークへの有線 LAN 接続による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の設置
 - ア 校外からのアクセス禁止によるリモートワーク等不可
 - イ 各学校及び教育委員会間でのデータ共有不可

12 想定スケジュール

別添 2 「想定スケジュール」 のとおり

第 2 構築期間（令和 8 年度）における事業詳細

下記に示す各業務について、発注者及び受注者各々の役割を明示したスケジュールをガントチャート様式で作成すること。

1 ゼロトラスト環境基盤の構築

下記に掲げるゼロトラスト環境構築に係る必要な機能について、Microsoft 365 Education A5 303 ライセンスの調達（311 ライセンス）を必須とし、これに含まれる諸機能を主として構築すること。受注者は、本業務を円滑に遂行するため、必要な情報を主体的かつ適時に提供するとともに、発注者との打ち合わせを適宜実施すること。

なお、本事業で構築された各環境及びデータ等は、名義変更等による管理権限の引き渡しにより、受注者以外への引き継ぎを可能とする。

(1) ID 統制（IDaaS 等）

- ア ID 管理及び各システムへの認証基盤等としての機能を備えること。
- イ 人事異動等の発生時に、発注者によるアカウントの随時追加、削除、編集等が可能であること。
- ウ 管理者（発注者が決定する本市教育委員会所属職員及び一部の教職員を指す。以下同じ。）が許可を与えた端末及びその利用者のみがサービスを利用できるようコントロールできること。
- エ 端末のサインインログ、ファイル操作ログ、およびデバイスの挙動ログを網羅的に収集し、最大 1 年間の保存を可能とすること。また、保存されたログに対し、管理画面において、条件指定（ユーザー、日時、操作種別、ファイル名、IP アドレス等）による検索・抽出を容易に行える構成とすること。

(2) 端末統制・保護 (MDM 等)

- ア Windows Update 等の一斉管理が可能であること。
- イ 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等を制御できること。
- ウ 端末紛失時に、遠隔操作にて当該端末のデータ消去等ができること。
- エ 端末のサインインログ、ファイル操作ログ、およびデバイスの挙動ログを網羅的に収集し、最大 1 年間の保存を可能とすること。また、保存されたログに対し、管理画面において、条件指定 (ユーザー、日時、操作種別、ファイル名、IP アドレス等) による検索・抽出を容易に行える構成とすること。
- オ 管理者によるリモート操作が可能なこと。

(3) EPP (Endpoint Protect Platform) 及び EDR (Endpoint Detection and Response)

- ア パターンマッチングの他、機械学習やふるまい解析等の技術により、既知又は未知にかかわらず、マルウェア等の検知や遮断が可能であること。
- イ IDaaS と連携するとともに、脅威が検出された時は、即座にメール等で管理者へ当該端末やユーザー情報等を通報できること。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。
- ウ 随時最新のセキュリティ状態に更新できること。
- エ 脅威の侵入経路等について、トラッキングが可能であること。

(4) ネットワークセキュリティ (SWG、CASB、等)

- ア IDaaS と連携するとともに、悪質な Web コンテンツやアプリケーション等へのアクセス制限 (フィルタリング) が可能であること。また、フィルタリング設定のテンプレートが用意されているとともに、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。
- イ 通信経路を暗号化するとともに、Web 経由でのマルウェア等の検知・遮断が可能であること。また、脅威を検知した時は、即座にメール等で管理者へ当該端末やユーザー情報等を通報できること。
- ウ 端末からクラウドサービスへの接続において、事前に定義した不正アクセスパターンとのマッチング等の技術により、クラウド等への不正なアクセスを検知・遮断できること。
- エ 個人契約テナントやシャドーIT 等、セキュリティ上懸念があるサービス等へのアクセスを制御できること。

(5) クラウドストレージ及びデータ漏えい防止 (DLP/IRM 等)

ア 全体で 100TB 以上の容量を備えるとともに、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、当該ユーザーがアクセス可能なフォルダについては、Windows 標準のエクスプローラからショートカット等により直接接続できるよう、個人で設定するためのマニュアルを作成すると共に、MDM 等でのクラウドストレージへのショートカットの一斉配付が設定できること。

フォルダ構成及びアクセス権限等については、発注者との協議により決定する。

イ バージョン履歴機能及び削除ファイルの復元機能を有すること。復元可能な期間は、削除操作から 90 日以上を保障すること。

ウ 重要度が含まれるファイル等については、自動暗号化等の技術によりアクセス権限がないユーザー（第三者含む）が扱えないように制御できること。アクセス権限については、ユーザーの職位等に合わせて柔軟に設定可能であること。また、ファイルの操作ログ、もしくは、全てのファイルの操作ログを取得し、外部記憶媒体への持ち出しが制限可能であるとともに、クラウド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。

(6) その他

ア 今後利用が想定される校務支援システムについて、SAML 連携システム等を用いて、IDaaS と連携すること。

2 端末のキッティング・搬入作業

受注者は、新規導入端末および既存端末のキッティングを一括して担うものとする。また、作業にあたってはマスターデータの管理に必要なソフトウェア一式を本業務内で調達し、運用開始後の保守についても本仕様書の定めに従い対応すること。

(1) キッティング対象端末は、発注者が新規に別途調達した新規端末（以下、「新規端末」とする。）と既に市内小学校で業務に使用している既存端末（以下、「既存端末」とする。）合計 303 台（内訳は新規端末約 100 台、既存端末約 203 台）である。また、現在、複数の教職員で利用している共有端末（以下、「共有端末」とする。）も引き続き共有端末として利用する想定である。キッティング内容については、契約締結後に発注者との協議で適宜決定する。

(2) 令和 8 年 1 1 月までに新規端末のマスターデータを作成し、テスト運用及び検証を経

た上で他の新規端末へ展開すること。また、マスターデータのバックアップ及びリカバリーができるソフトウェアを別途調達し、そのライセンスは永続かつ発注者に帰属すること。なお、既存端末については、新規端末のマスターデータを参考に手順書を作成し、発注者が指定する時期に現地又は発注者が指定する場所で設定作業を行うこと。

(3) 共有端末について、1 台の端末に複数名の顔情報、PIN 情報を登録することを想定し、登録した教職員が登録した端末を利用することを想定しているため、条件に応じた設定を行うこと。

(4) 運用開始後、端末に問題が発生した際の保守窓口および責任分担は以下の通りとする。

ア 端末本体（物理故障、初期不良等）に起因する場合は、受注者が切り分けを行った上で、端末購入業者へ繋ぎ、連携して対応すること。

イ キット内容およびゼロトラスト環境に起因する不具合については、受注者が迅速かつ誠実に対応し、解消すること。

ウ 設定不具合等が判明した場合は、完全に解消できるよう、遅滞なく対応を行うこと。

3 Microsoft Teams の構築

ゼロトラスト基盤を用いた新たなネットワークにおける教職員の情報共有ツールとして利用する Microsoft Teams について、次に示す条件にて構築すること。

(1) 外部とのデータのやり取りの可否および取扱方針については、セキュリティおよび運用上の観点から、発注者と受注者との協議により決定すること。

(2) モバイルアプリの利用および制御内容については、発注者の運用方針を踏まえ、発注者と受注者との協議により決定すること。

4 Microsoft SharePoint の構築

データの共有領域として利用する Microsoft SharePoint について、次に示す条件にて構築すること。作成した SharePoint サイトは、Teams に接続したデータの共有領域としての利用と、既存環境データの共有領域として利用を想定しており、既存環境データについては、必要なアクセス権の設定を実施することとする。

(1) 外部とのデータのやり取りができないこと。

(2) 構築する SharePoint サイトは、次を想定している。

ア 各学校が利用するサイト

イ 全教職員が利用するサイト

ウ 全校長が利用するサイト

エ 全教頭が利用するサイト

オ 全事務職員が利用するサイト

(3) 作成したサイトには「記憶域の制限」を設定すること。

(4) 年度更新を見越したグループ設計を行うこと。

5 Exchange online の構築（メール）

教職員と業務上必要と教育委員会により認められた場合に利用できる校務用のメールとして以下のことを実現すること。

(1) 校務系メール

ア 校務系メールとは、教職員と業務上必要と教育委員会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。

イ 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。

ウ 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ものとする。

エ アドレス帳については全小中学校の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

ア 「Exchange Online Protection + Defender for Office365」の機能を活用したセキュリティ対策について提案を行うこと。

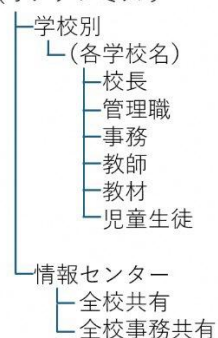
(3) 学校代表メール

ア 学校代表メールを作成し、該当する受信者の設定を実施すること。

6 既存環境の移行

(1) 既存環境の総容量（約 24.6TB：小学校 11.8TB、中学校 12.6TB、情報センター0.2TB）を対象に、センター内オンプレミスサーバ上の整理済みデータおよび各校 NAS 内のデータを、上記 1（5）で構築したクラウドストレージに移行する作業について、効率的な実施時期及び手法等を提案すること。なお、クラウドストレージ内のフォルダ構成は、発注者が指示する各校統一した構成とすること。

(オンプレミスサーバ ルート)



※写真動画は各学校のNASに格納

図 1:既存環境のフォルダ構成

- (2) 現在稼働している各学校設置のプリンタ及び複合機の IP アドレス変更や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等を提案すること。また、複合機について、スキャンデータを教職員用端末に送信することが出来るよう設定すること。
- (3) 現行の学習系ネットワーク及び校務系ネットワークの統合作業は、別途既存保守業者により実施するため、本事業には含めない。
- (4) 上記 1 の構築を含めて、令和 8 年 12 月末までにテスト運用、令和 9 年 1 月 1 日から本運用が開始できるスケジュール作成及び人員等の確保を行うこと。

7 説明会の開催及び操作手順マニュアル等作成

- (1) 新規端末の配付後、令和 9 年 4 月までに教職員を対象とした説明会を実施すること。内容や手法、回数等については、発注者と協議して決定する。また、説明会等で教職員から受けた質疑等については、発注者と協議の上回答を作成すること。
- (2) 管理者対象の研修会についても、令和 8 年度中に説明会を実施すること。内容や手法、回数等については、発注者と協議して決定する。また、質疑や課題等のやり取りについては、プロジェクト管理ツール内での対応を原則とする。
- (3) 各説明会の内容について、操作手順マニュアル等を含めたドキュメントを作成し、後日でも随時確認ができるようにすること。操作手順マニュアル等に記載する内容に変更があった場合は、随時差し替えを行うこと。

8 情報セキュリティポリシー策定支援

- (1) 文部科学省 教育情報セキュリティポリシーに関するガイドラインの内容を反映し、五島市教育情報セキュリティポリシーの策定支援をすること。
- (2) 発注者の一般行政事務を対象とした情報セキュリティポリシーの内容についても調査・検討の上、本業務で作成するポリシーとの間で齟齬がないよう整合性を確保すること。
- (3) 以下に示す内容で、構成し進めるものとする。
 - ア 現状把握・分析
 - (ア) 情報資産調査
 - (イ) 組織・体制確認

(ウ) 現地調査・学校アンケート

イ セキュリティポリシー案作成

(ア) 基本方針案作成

(イ) 対策基準案作成

(ウ) 管理策検討

(エ) 行政側セキュリティポリシーとの整合性確認

ウ 実施手順書案作成

(ア) 具体的手法の整理

(イ) 各校独自システムや手順などの整理

エ 運用支援

(ア) 研修

(イ) 定着作業・自己点検

(ウ) チェックリスト作成

(エ) アンケート実施、集計

(オ) アンケート分析

(カ) 報告書提出

(4) 本業務の円滑な推進と専門性を担保するため、受託者は以下の要件を満たす体制を構築しなければならない。なお、再委託先の実績を含めることも可能とする。

ア チームメンバーの実績要件

(ア) 他の教育委員会において、教育情報セキュリティポリシー案、実施手順案、研修資料案の作成実績を複数有すること。また、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月版）に基づく作成実績を複数有すること。

(イ) 過去3年以内に教育情報セキュリティポリシー策定および監査支援等の同種実績を有すること。

9 既存端末用外付け認証機器の調達

上記で構築したゼロトラスト環境に既存端末を対応させるため、下記仕様を満たす、利用者認証を実現するための外付け認証機器を、同一機種かつ未使用品にて203台調達する。

(1) Windows Hello for Businessに対応し、IDaaSと連携してログイン時に多要素認証が可能であること。なお、具体的な認証方式、機器の種別および運用方法等の詳細については、受注者からの提案を踏まえ、発注者との協議により決定するものとする。

第3 全履行期間（契約締結日の翌日から令和14年3月31日まで）における運用保守

1 運用体制

(1) 本事業に携わる全ての人員について、所属、氏名、役割、メールアドレス、緊急連絡先等を記載した体制表を契約締結後速やかに提出すること。また、人員の変更が

発生する度に修正版を作成し、差し替えること。

- (2) 発注者（教育委員会担当部門）からの問合せや課題管理等は、プロジェクト管理ツール内での対応を原則とする。ただし、障害発生等緊急の対応が必要な場合は、電話又はメール等、他の連絡手段を用いることがある。
- (3) 発注者からの問合せ対応は、メールおよび電話等で受け付けること。また、受注者は連絡を受けた翌営業日までに、一次回答を行うこと。ただし、障害発生等緊急の対応が必要な場合は、迅速な対応を行うこと。
- (4) 対応作業の迅速化を図るため、クラウド環境及びクライアント端末等に係るリモート保守対応が可能となる環境を構築すること。当該環境に必要な機器やライセンス等の費用は受注者の負担とするとともに、契約締結時にリモート保守対応に係る覚書を締結すること。

2 運用内容

本事業で構築及び調達等を行った全てのシステム及び機器等に係る業務全般を、運用保守業務の範囲とする。また、運用保守業務の実施は、原則として業務時間中とする。ただし、教職員の業務に影響を及ぼす作業が発生する場合は、発注者と協議の上、業務時間外や休日等も含めて計画を立案し、実施すること。

(1) セキュリティメンテナンス

システム及び機器等への更新プログラム適用やアップデート等に係る情報を随時提供するとともに、発注者の求めに応じて技術的助言及び支援等を行うこと。特に脆弱性に係る情報は発注者及び受注者双方が迅速に共有し、可能な限り早期に適用できるようにすること。また、計画的なシステム等停止が発生する場合は、1週間前までに発注者に事前通知すること。

(2) 運用代行業務

ゼロトラスト環境の円滑な運用を維持するため、発注者の依頼に基づき以下の運用代行業務を実施すること。

ア ID 運用代行

人事異動等に伴うアカウント・グループ情報の登録・削除・変更
Bitlocker の回復キー管理
一時アクセスパスワードの提供

イ パスワード・多要素認証登録、リセット対応

パスワード変更等ができない場合や MFA のリセットが必要となった場合に登録リセットを対応

- ウ SSO 連携管理（証明書）
3rd Party アプリケーションとの SSO 連携設定
SSO 連携追加時の作業アカウント払出
- エ 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・配信再開対応を実施
- オ Windows 端末アプリケーション配信
お客様からの依頼に基づくアプリケーション配信
（サイレントインストール対応アプリケーションのみ）
- カ 外部記憶媒体制御
外部記憶媒体の利用申請に基づき、利用媒体の登録と利用ユーザの設定を実施
- キ リモートワイプ代行
紛失したデバイスのリモートワイプを実施
- ク Intune 構成プロファイル設定
設定構築した構成プロファイルの設定変更
- ケ Web アクセス管理
申請内容に基づき、通信先のホワイトリスト・ブラックリストへの登録を実施
Microsoft 365 のテナント制御
SWG を介さない（バイパス）アクセス制御
- コ メールセキュリティ管理
問合せ依頼に基づき、検疫ボックスに格納されたメールの確認・再配送の実施
- サ Intune デバイス登録
新規端末導入・端末故障修理の際に、端末を Microsoft365 へ接続可能とする設定を実施
- シ 端末キッティング用アカウント払い出し
新規端末導入・端末故障修理の際に、キッティング用アカウントの払い出し
- ス SharePoint サイト/フォルダの追加・削除
SharePoint サイト/フォルダの追加・削除の実施
- セ SharePoint サイト/フォルダのアクセス権追加・削除
SharePoint フォルダへのアクセス権変更の実施
- ソ SharePoint/One Drive ストレージ容量
SharePoint/OneDrive ストレージ容量についてストレージプールから再割り当てを実施
- タ Teams チームの追加・削除
Teams チームの追加・削除を実施
- チ Teams チームのアクセス権追加・削除

- Teams チームへのアクセス権変更を実施
- ツ Exchange メールボックス容量の再割り当て
- Exchange メールボックスについてストレージプールから再割り当てを実施

(3) 問合せ対応

発注者からの問合せに対し、随時回答又は対応すること。

なお、文教分野での Microsoft365 A5 の運用実績がある問い合わせ窓口を用意すること。

(4) アカウント管理及び年次更新業務

教職員の異動に伴う必要な作業について実施又は発注者の求めに応じて技術的助言及び支援等を行うこと。

(5) 運用支援

教職員及び教育委員会の業務効率化に資する、本事業で構築したシステム等の機能や活用方法等について、随時情報提供すること。

(6) 定例会の実施

ア 構築期間については、発注者が指定する場所において、毎月 1 回は必ず実施し、環境構築等の進捗状況や課題等を報告及び協議する。

この時、報告及び協議に必要な資料は受注者が作成し、提出すること。

イ 運用保守を主とする期間（令和 9 年度から令和 14 年度まで）についても、引き続き実施し、運用状況や課題等について報告及び協議する。

この時、クラウドストレージ容量の推移、障害、セキュリティインシデント、問合せ対応状況等を取りまとめた報告書を作成し、提出すること。

なお、協議方法については、オンラインでの実施を妨げるものではない。実施頻度については、別途協議とする。

ウ 上記にかかわらず、発注者が必要と認めるときは、発注者が指定する方法及び場所で随時実施する。

(7) その他

受注者は、発注者の業務効率化に資するものについては、積極的に提案又は情報提供すること。

第3 成果物等の納品

1 提出書類

受注者は契約締結後、令和8年度中の発注者が指定する期日までに、下記の書類を提出すること。数量は、各々紙媒体（製本済）1部、電子データ1部とし、(1)～(10)の電子データはPDF形式に加え、編集可能なデータ形式（.docx,.xlsx,.pptx等）も合わせて提出すること。なお、マニュアルについては、発注者との協議の上、内容等に変更があった場合は随時差し替えたものを提出すること。ただし、(11)については、電子データのみを納品とする。

- (1) プロジェクト実施計画書
- (2) スケジュール表（ガントチャート様式）
- (3) 運用保守体制表及び緊急連絡先
- (4) 要件定義書及び設計書
- (5) システム運用マニュアル
- (6) 端末キッティングマニュアル
- (7) 障害対応マニュアル
- (8) 教職員対象操作手順マニュアル
- (9) 説明動画及びテキスト
- (10) テスト仕様書兼運用成績表
- (11) 端末マスターデータ（専用の外部記憶媒体に格納し、2個納品すること。）
- (12) その他発注者が提出を求めるもの

2 その他

- (1) 本事業は、交付金を活用する予定であるため、実績報告書等に必要となる資料についても提出を依頼することがある。
- (2) 契約期間満了後においても、発注者から書類やデータ等の提出を求められた場合は、随時対応すること。
- (3) 成果物等の納品場所は、五島市教育委員会とする。

(別添1)

実施場所一覧

- 1 五島市立福江小学校 (五島市錦町 1-1)
- 2 五島市立緑丘小学校 (五島市木場町 765)
- 3 五島市立奥浦小学校 (五島市奥浦町 1316-1)
- 4 五島市立本山小学校 (五島市堤町 1341)
- 5 五島市立富江小学校 (五島市富江町富江 111)
- 6 五島市立盈進小学校 (五島市富江町黒瀬 1240)
- 7 五島市立三井楽小学校 (五島市三井楽町濱ノ畔 1148)
- 8 五島市立岐宿小学校 (五島市岐宿町楠原 544-1)
- 9 五島市立福江中学校 (五島市松山町 75-4)
- 10 五島市立翁頭中学校 (五島市堤町 1765)
- 11 五島市立富江中学校 (五島市富江町狩立 464)
- 12 五島市立三井楽中学校 (五島市三井楽町濱ノ畔 1502-1)
- 13 五島市立岐宿中学校 (五島市岐宿町楠原 544-1)
- 14 五島市立久賀小中学校 (五島市久賀町 245-8)
- 15 五島市立玉之浦小中学校 (五島市玉之浦町小川 1130-1)
- 16 五島市立奈留小中学校 (五島市奈留町浦 1225-1)
- 17 五島市教育委員会学校教育課 (五島市福江町 1-1)