令和８年度京丹波町立小中学校校務系ネットワーク更新事業

仕様書

1. 概要

1.1. 目的

文部科学省は、GIGAスクール構想の進展に伴うクラウドサービスの本格的な活用や、児童生徒の学び方及び教職員の働き方の変化等を踏まえ、「教育情報セキュリティポリシーに関するガイドライン」を令和7年3月に改訂した。

同ガイドラインにおいては、校務DXの推進に当たり、従来の閉域網及びオンプレミス環境を前提とした境界防御に依存するのではなく、いわゆるゼロトラストの考え方に基づき、強固な認証及びアクセス制御等により情報セキュリティを確保した上で、クラウド活用を前提としたシステム構成へ移行していく方向性が示されている。

京丹波町教育委員会（以下「教育委員会」という。）においても、これら国の方針を踏まえ、新たな校務の在り方として、「学校における働き方改革」、「教育活動の高度化」及び「教育現場のレジリエンス確保」の観点から、校務系システム等のクラウド化を推進するとともに、適切な認証及びアクセス制御、端末管理、ログ管理等の必要なセキュリティ対策を講じ、極力オンプレミス設備に依存しない、新たな教育情報ネットワーク環境の実現を目指している。

本業務は、以上の方針を総合的に踏まえ、計画的な調達及び構築を行うことにより、ICTを活用した校務を一層推進できる環境を整備することを目的として、新たな教育ICT環境の構築、移行及び運用保守に関する業務を委託するものである。

1.2. 基本方針

本業務は、現行システム基盤のサポート終了及び更改時期の到来を踏まえ、文部科学省が令和7年3月に取りまとめた「次世代校務DXガイドブック」及び同月改訂の「教育情報セキュリティポリシーに関するガイドライン」に基づき、次世代校務DXの実現に向けた教育ICT環境の整備を進めるものである。

また、校務DXに不可欠であるクラウドシステムの利活用に当たっては、いわゆるゼロトラストの考え方を踏まえた「強固なアクセス制御」により、適切な認証・アクセス権限管理、端末管理、通信の暗号化、監視・ログ管理等のセキュリティ対策を講じ、ネットワーク環境の整備と併せて学校現場における安全管理措置を確保する。

1.3. 設置場所

設定・設置場所の一覧は下記のとおり

No	学校名	住所	電話
1	竹野小学校	京丹波町高岡高岡23	0771-82-0032
2	丹波ひかり小学校	京丹波町曽根宮ノ浦戸麦54番地	0771-89-2353
3	下山小学校	京丹波町下山上藤ヶ瀬16番地	0771-83-0014
4	瑞穂小学校	京丹波町橋爪桧山118番地	0771-86-0009

5	和知小学校	京丹波町本庄安田7番地	0771-84-9061
6	蒲生野中学校	京丹波町蒲生八ツ谷62番地	0771-82-1108
7	瑞穂中学校	京丹波町大朴段ノ垣内6番地	0771-86-0013
8	和知中学校	京丹波町市場丸ヶ野4番地	0771-84-1104
9	京丹波町和知支所	京丹波町本庄ウエ16番地	0771-84-0028

1.4. 既存ネットワーク概要

既存のネットワーク構成は図１の通り。

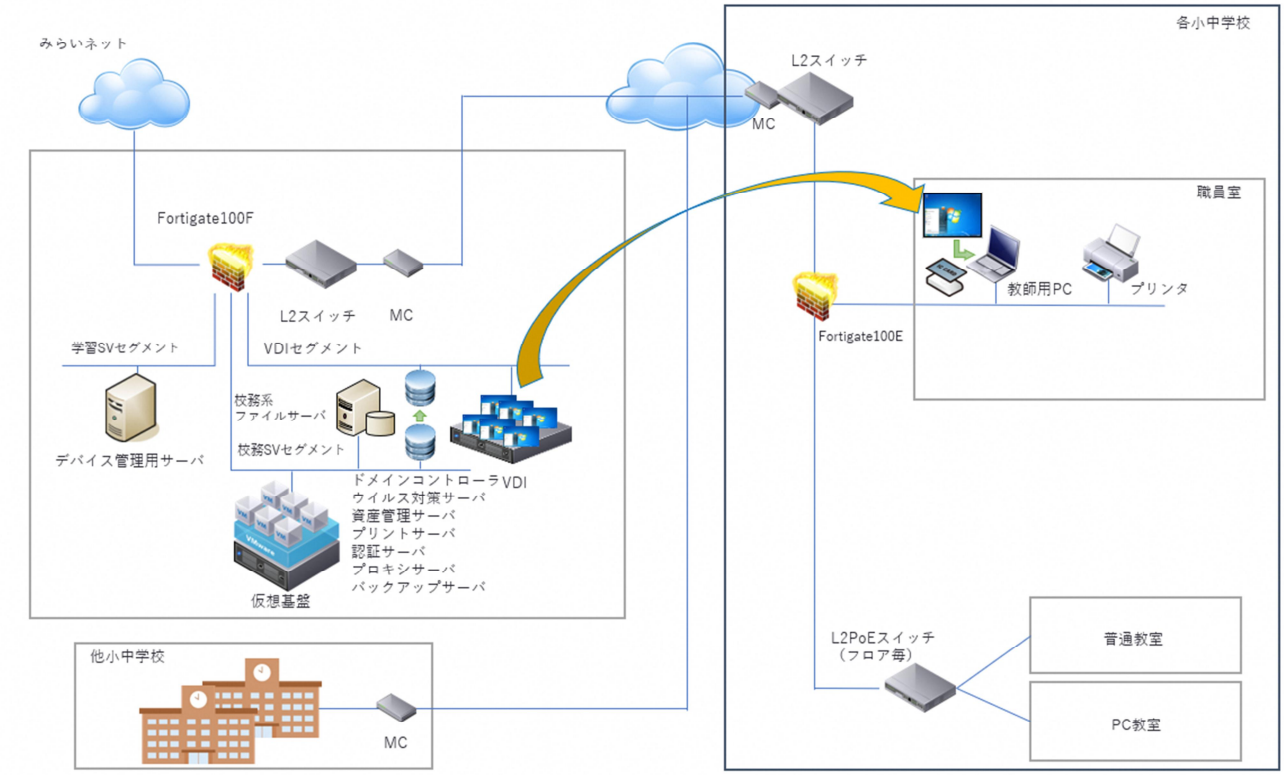


図１　既存ネットワーク図

1.5. 業務期間

（ア）導入構築業務：契約日から令和9年1月31日

（イ）保守運用業務：令和9年2月1日から令和14年1月31日

1.6. 賃貸借期間

令和9年2月1日から令和14年1月31日

2. 機器仕様書

2.1. ハードウェア

番号	項目名	仕様内容	
	校務用パソコン　169 台		
	クライアント PC（ノート型）	筐体	ノート型 PC
		基本 OS	Windows11 Pro(64bit)日本語版
		CPU	Intel　Corei5　13 世代　相当以上
		メモリ	16GB 以上
		SSD	256GB 以上
		本体サイズ	W：313mm、D：225mm、H：20mm 以内(最厚部、突起部含まず)
		質量	1.35kg 以内
		表示機能	解像度 1920×1080 以上
		液晶ディスプレイ	14.0 インチワイド(16:10)WUXGA 液晶ディスプレイ非光沢
		WEB カメラ	720p HD Web カメラ以上
		有線 LAN	1000BASE-T/100BASE-TX/10BASE-対応（Wake-up on LAN 対応）
		無線 LAN	Wi-Fi 6E（IEEE802.11ax）（2.4Gbps） +IEEE802.11ac/a/b/g/n 準拠
		Bluetooth	Bluetooth5.3 以上
		インターフェース	RJ45LAN コネクタ×1 以上内蔵
			USB3.2(Gen1) TypeA ポート×2 以上、
			USB3.2(Gen2) USBTypeC ポート×2 以上
			HDMI ポート×1 以上
			ヘッドホン/ヘッドホンマイクジャック
		内蔵光学ドライブ	なし
		セキュリティチップ	TPM2.0
		電源	AC アダプタ付属すること。
			利用者自身でバッテリー交換可能なこと。
		機器保守	5 年間の翌営業日対応オンサイト保守（内蔵ディスク返却不要オプション）を含めること。
		その他	再セットアップ用媒体を用意すること。(総台数に対して一式)
			セキュリティワイヤー（サンワサプライ・超小型シリンダセキュリティ（型番：SL-80)）を 5 本付けること。
			マウスパッド（サンワサプライ・エコマウスパッド（ブルー）

			（型番：MPD-EC37BL)）を 5 枚付けること。
			RoHS 指令に対応していること。
			PC グリーンラベルに対応していること。

番号	項目名	仕様内容	
2	セキュリティUSBメモリ　18本		
	セキュリティ USB メモリ	対応 OS	Windows 11に対応していること。
		セキュリティ機能	パスワードロック機能を有すること。
			ハードウェア暗号化(AES256bit)機能を有すること。
			ウイルススキャン機能を有すること。 期間は5年間とする。
			ネックストラップを付帯すること
		インターフェース	USB Type-A USB 3.2(Gen 1)/3.1(Gen 1)/3.0/2.0
		容量	4GB
		保証期間	5年

番号	項目名	仕様内容	
3	拠点スイッチ　10 台(うち、予備機 1 台)		
	PoE L2 スイッチ	メーカー	問い合わせ窓口・管理の一元化を可能とするため、SASE、学校用ファイアウォール、アクセスポイントと同一メーカーであること。
		ハードウェア要件	802.3af/at に対応した PoE ポートが 12 ポート以上有すること。
			10GbE SFP+インターフェースを 4 ポート以上有すること。
			RJ-45 のシリアルコンソールポートを持つこと。
			19 インチ幅のラック搭載型として 1RU 以内に収納可能であること
		性能要件	スイッチング容量は双方向で 128Gbps 以上であること。
			レイテンシ(遅延)が 1μs 以下であること。
			1 秒当たりのパケット処理能力が 190Mpps 以上であること。
			学習できる MAC アドレス数は 32,000 以上に対応可能であること。
			PoE での給電容量が 185W 以上有すること
		ソフトウェア要件	ジャンボフレームに対応していること。
			ポートスピードおよび伝送形態のオートネゴシエーションが可能なこと。
			IEEE 802.1D MAC ブリッジ / STP に対応していること。
			IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) に対応していること。

			IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) に対応していること。
			STP ルートガード機能をサポートしていること。
			STP BPDU ガード機能をサポートしていること。
			エッジポート / Port Fast 機能を持つこと。
			IEEE 802.1Q VLAN タギング機能をサポートしていること。
			プライベート VLAN 機能をサポートしていること。
			IEEE 802.3ad LACP によるリンクアグリゲーション機能をサポートしていること。
		管理	https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。
			ファイアウォール(UTM)の GUI から集中管理可能なこと。
			ファイアウォールと連携し、ファイアウォール経由で設定/ログ確認をできる機能を有すること。
			複数の UTM を管理するサーバからでも集中管理可能なこと
		サポート	障害診断に関する問い合わせ対応ができること。
			先出しセンドバック保守、またはこれと同等以上の保守方式であること。また、障害受付後、翌営業日以内で代替機の発送または復旧対応を行うことを目標としたサービスであること。
			平日 9:00-17:00 のサービス受付時間を有すこと。
			サポートサービスの契約期間は、2027 年 2 月 1 日を開始日、2032 年 1 月 31 日を終了日とする 5 年間とする。 また、構築期間中に必要となるサポートサービス費用についても、見積金額に含めること。

番号	項目名	仕様内容	
4	職員室用HUB　9台（既存機器に対する予備機、各校１台）		
	L2スイッチ	インターフェース	10/100/1000Base-Tインターフェースを8ポート以上搭載
		機能	Layer2以上のスイッチング機能を搭載
			ループ検知機能を搭載し、ループ発生時には一時的にポートを遮断することができること
		ファン	ファンレス設計であること
		電源アダプタ	内蔵型であること
		機器保証	1年間以上
		その他	マグネット付きであること

番号	項目名	仕様内容	
5	アクセスポイント　28 台(うち、予備機 1 台)		
	アクセスポイント	メーカー	問い合わせ窓口・管理の一元化を可能とするため、SASE、学校用ファイアウォール、拠点スイッチと同一メーカーであること。
		ハードウェア要件	ラジオ数が 3 つ以上であること。
			内蔵アンテナが 6 つ以上であること。
			100M/1000M/2.5G/5.0G に対応するマルチギガビットポートを 1 つ以上有していること。
			RJ-45 のシリアルコンソールポートを持つこと。
			ラジオ 1 は 2.4Ghz b/g/n/ax(2x2:a2 ストリーム)に対応すること。
			ラジオ 2 は 5Ghz a/n/ac/ax (2x2:2 ストリーム)に対応すること。
			PoE+(IEEE 802.3at)による受電が可能なこと。
		性能要件	2.4GHz 帯での最大データレートが 688Mbps 以上であること。
			5.0GHz 帯での最大データレートが 2.882Gbps 以上であること。
			同時 SSID がラジオあたり 8 以上であること。
			ラジオあたりの最大クライアント数は 512 以上であること。
		ソフトウェア要件	ローカルブリッジ、トンネル、メッシュ各タイプの SSID をサポートすること。
			LED オフモードをサポートすること。
			802.11 UL MU-MIMO をサポートすること。
			パケットスニファモードをサポートすること。
			スペクトラムアナライザ機能をサポートすること。
			OFDMA をサポートすること。
		管理機能	https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること。
			ファイアウォール(UTM)の GUI から集中管理可能なこと。
			ファイアウォールと連携し、ファイアウォール経由で設定/ログ確認をできる機能を有すること。
			AP に接続した端末の IP アドレス、MAC アドレス、接続した AP のホスト名をファイアウォール上で表示する機能を有すること。
			ファイアウォールと連携することで、AP に接続している端末を L2 または L3 レベルで隔離を行うことができる機能を有すること。
			ファイアウォールの GUI から AP のバージョン変更ができること。
			複数の UTM を管理するサーバからでも集中管理可能なこと。
		サポート	障害診断に関する問い合わせ対応ができること。
			先出しセンドバック保守、またはこれと同等以上の保守方式であ

			ること。また、障害受付後、翌営業日以内で代替機の発送または復旧対応を行うことを目標としたサービスであること。
			月～金 9:00-17:00[祝日と年末年始（12/30～1/3）を除く]のサービス受付時間を有すこと。
			サポートサービスの契約期間は、2027 年 2 月 1 日を開始日、2032 年 1 月 31 日を終了日とする 5 年間とする。 また、構築期間中に必要となるサポートサービス費用についても、見積金額に含めること。
	マウントキット	物理仕様	上記のアクセスポイントで利用可能であること。
			壁及び天井のいずれにも取り付け可能なケーブル格納型であること。

番号	項目名	仕様内容	
7	学校用ファイアウォール　8 台		
	ファイアウォール	メーカー	問い合わせ窓口・管理の一元化を可能とするため、SASE、拠点スイッチ、無線アクセスポイントと同一メーカーであること。
		物理ポート	GbE RJ45 ポートを 8 ポート以上有していること。
			管理コンソールに接続可能な管理用ポートを有していること。
		性能	同時セッションは、TCP で最大 1,400,000 以上であること
			新規セッションは、TCP で毎秒最大 100,000 であること
			ファイアウォールスループット（パケット/秒）が、15Mpps 以上であること。
			ファイアウォールのレイテンシは、64byte UDP で最小 2.46μs 以下であること
		VLAN	IEEE802.1Q VLAN トランク機能を有していること
		Link Aggregation	IEEE802.3ad リンクアグリゲーション機能を有していること。
		冗長構成	冗長構成が可能なこと。
		ファイアウォール	ファイアウォールポリシー数は 5,000 以上設定可能なこと。
			ファイアウォール機能として NAT および NAPT のネットワークアドレス変換が可能なこと。
		認証・セキュリティ	RADIUS、LDAP によるユーザー認証をサポートすること。
			DoS 攻撃防御機能を有していること。
			Mac アドレスのラーニング情報を元にしたデバイス情報にて、ファイアウォールのポリシー制御が可能なこと。
			ファイアウォールのポリシー毎にアンチウイルス、Web フィルタ、

			DNS フィルタ、アプリケーションコントロール、IPS、SSL インスペクション機能の有効/無効設定が可能なこと。
			アンチウイルス、Web フィルタ、アプリケーションコントロール、IPS、アンチスパム、DLP は IPv6 に対応していること。
			2,000 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て可視化できること。
			8,000 以上の IPS シグネチャを有していること。
			サーバ証明書のコモンネームを参照して、サーバの FQDN の情報で Web フィルタリングする certificate inspection 機能を有していること。
		管理機能	SNMPv1,SNMPv2c エージェント機能を有すること。
			https 対応の Web インターフェースを有し、それ以外に SSH や Telnet による遠隔保守が可能であること
			日本語の Web GUI を有すること。
			Syslog サーバに log の送信が可能なこと。
			システム設定のバックアップは、暗号化とパスワードを設定してエクスポート可能であること。
			スイッチのコントローラ機能を有し、最大 24 台のスイッチに対して設定と管理を行えること。
			無線 AP のコントローラ機能を有し、最大 96 台の AP に対して設定と管理を行えること。また、トンネルモードの場合、最大 48 の AP に対して設定と管理を行えること。
		物理仕様	19 インチラックに搭載可能なタイプであること。
			ファイアウォール単体の重量は 1.1kg 以下であること。
			単体の寸法は 220mm（幅）x 200mm（奥行）x 50mm（高さ）以下であること。
			動作保証温度は 0-40℃をサポートすること。
		サポート	障害診断に関する問い合わせ対応ができること。
			障害診断後、4 時間対応目標でエンジニアによる訪問修理を受けられること。
			24 時間 365 日のサービス受付時間を有すこと。
			本機器の更新時期は、既存機器の保守期間を考慮し、令和 8 年 9 月中とする。なお、サポートサービスの提供期間は、更新日以前の日を開始日、2032 年 1 月 31 日を終了日とする期間とすること。
		管理	クラウド型のネットワーク機器管理サービスを用いて一元管理を行うこと。なお、サービスの利用期間は、2027 年 2 月 1 日を開始日、2032 年 1 月 31 日を終了日とする 5 年間とする。

			また、構築期間中に必要となるサービス費用についても、見積金額に含めること。

2.2. ソフトウェア

番号	項目名	仕様内容
1	多要素認証・シングルサインオン	
	端末台数	169台
	ユーザー数	183名
	期間	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。
	認証方式	顔認証+パスワード方式であること。
	提供方式	利用する認証システムはクラウドで提供されるサービスであること。
	動作環境	Windows11に対応していること。
	シングルサインオン、アプリケーション認証関連	PCのウェブブラウザで利用するSAML2.0に対応したウェブサービスや業務システムに連携し、生体情報（「指紋」「顔」「FIDO（WebAuthn/パスキー）」）、所持情報（「ワンタイムパスワード」、「QRコード」、「ICカード」、「一時パスワード」、「メール」）、知識情報（「パスワード」「PIN」）を利用、または、これらを組み合わせた多要素認証を利用したログイン（シングルサインオン）が可能な認証システムであること
		SAML2.0による連携ができない業務システムに対し、システム側を改修することなく、多要素認証を使ったログイン（またはシングルサインオン）が可能な代理入力方式が利用できる認証システムであること
	Windows関連仕様	Windows OS（Windows 11）のログオンに、生体情報（「指紋」「顔」）、所持情報（「ワンタイムパスワード」、「QRコード」、「ICカード」）、知識情報（「パスワード」「PIN」「一時パスワード」）を利用、または、これらを組み合わせた多要素認証が利用可能な認証システムであること。
		Windowsログオンは、Active Directoryで管理するドメイン端末のほか、ワークグループ端末、Windowsアカウントを使用する端末でも利用可能なこと。
		Windowsアカウントの利用にあたって、ユーザーやグループを、Microsoft Entra IDと同期する機能を有すること。
		Windowsログオンおよび代理入力方式での認証において、ネットワーク途絶等により共通認証基盤提供サービスを利用できない場合には、クライアント端末単独でログオン認証を代替できるオフライン認証機能を有すること。
		緊急時を想定し、標準のWindows認証画面への切り替えが可能であること。また、切替に際してパスワードで保護する機能を有すること。
		Windowsログオン時の認証、SAML2.0での認証、および代理入力方式での認証を、共

		通のユーザーインタフェースで対応できること。
		Windowsで利用するクライアントソフトウェアは、インストーラーを利用したインストールに加えて、グループポリシーやIT資産管理ツールによる配布によるサイレントインストールにも対応すること。また、アンインストール防止機能を備えていること。
	アカウントロック	一定回数以上（設定により変更可能）認証に失敗した場合、アカウントをロックする機能を有すること。また、その場合ロックされたアカウントをユーザーによってアカウントリカバリする機能も有すること。
	ネットワーク設定	IPアドレスを登録し、安全なネットワーク環境として認証セットのネットワーク設定で利用することで、登録のないIPアドレスのもとでは、安全が確認できていないネットワークとして認識し、利用できる認証セットを変更できる機能を有すること。
	代理認証	業務を代行するユーザーへの権限委譲や、共有端末で同じアカウントでログオンしたい場合などに利用する、自分のアカウントを別のユーザーに権限を委譲する機能を備えていること。
	画面ロック機能	ユーザーの離席等により、顔を検知しなくなった際、Windowsをロックまたはログアウトする機能を有すること
	顔認証	認証サーバに登録された顔情報によって、PCに搭載されたカメラ（もしくは外付けのウェブカメラ）に顔をかざすことで認証が可能なこと
		設定により顔認証のみのリトライが可能であること
		顔の向きや、環境の変化や、メガネや帽子などに影響されにくく、マスク着用時の認証が可能であること。
		顔写真や動画によるなりすましを防止するため、パッシブ方式（追加動作不要で、リアルタイムに顔を撮影したものか否かを判定する方式）による偽造対策が顔認証エンジンにより取られていること。
		複数のカメラが接続または搭載されている場合、カメラの選択が可能であること。
	データ保管・暗号化	本サービスにおいて使用されるサーバの設置場所および、本サービスが取り扱うすべてのデータの保存先は、日本国内であること。
		本サービスで利用されるデータベースに保存されるデータについては、AES256相当以上の強度を有する暗号化方式により暗号化されていること。
	稼働率	99.9%以上であること。
	その他	保守性を鑑み、本システムで採用する顔認証ソフトウェアの開発業者と、顔認証ソフトウェア内部で使われている顔認証技術の開発業者は同一であること。
		ISO/IEC 27001（ISMS）および、ISO/IEC 27017（ISMSクラウドセキュリティ）の認証を取得していること。

番号	項目名	仕様内容
2	SASE製品	
	端末台数	169台
	ユーザー数	183名
	期間	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。
	メーカー	問い合わせ窓口・管理の一元化を可能とするため、学校用ファイアウォール、拠点スイッチ、無線アクセスポイントと同一メーカーであること。
	システム仕様	本システムは、和知支所に既設のファイアウォール（FortiGate-100F　2台）をSASE接続時の拠点側エッジ装置として継続利用するものとする。
		サービスが提供されるPOPで日本国内が選択できること。
		サービスで生成されるログが日本国内で保存させること。
		業務利用サービスのアクセス元IPアドレス制限が可能となるようグローバルIPアドレス固定が可能であること。
	機能仕様：セキュリティ	アプリケーションの識別と制御機能を有していること。
		アプリケーション識別型のルーティング機能を有していること。
		社内/社外問わず一貫したレベルのセキュリティが提供できること。
		POPから複数の社内拠点に対してIpsecトンネルを確立することでプライベートアプリケーションにアクセスが可能であること。
		主要SaaSプロバイダーに直接接続しAPIベースのCASBが提供できること。
		InlineベースのCASBが提供できること。
		SSEエージェントをインストールすることで、IPS機能、アンチウイルス機能、アンチスパム機能、データ漏洩防止(DLP)、DNSフィルタリング、サンドボックス、SSLインスペクション、Webフィルタリングがエンドポイントに提供できること。
		LDAPやRADIUSによるユーザー認証機能を有すること。
		ユーザー認証においてIdPとSAML連携ができること。
		VPN機能には、リモートで使用する際常時VPNがONになる機能があること。
		VPNを経由する通信とVPNを経由しない通信を制御する機能（スプリットトンネル）を有すること。
		スプリットトンネルはIPベースだけでなく、ドメインにも対応できること。
		BYODやエージェントをダウンロードできない端末に対してはPACファイル等の使用にてエージェントレスセキュリティを提供できること。
		社内アプリケーションに対してゼロトラストアクセスにおけるアクセス制御機能を有すること。
		アクセス制御にはエージェントから収集したデバイスポスチャ情報を活用してポリシーが作成できること。

		エンドポイントのデバイスポスチャ情報が収集できること。
		収集したポスチャ情報が管理画面上で確認ができること。
		エンドポイントが管理端末かどうかをデバイス管理情報等で識別できること。
		BluetoothやUSBデバイスといったリムーバブルデバイスに対する制御機能を有すること。
		外部の脅威情報フィードを取り込み、フィルタリングポリシーに動的に適用できる機能を有すること。
	機能仕様：端末	Windows 11に対応していること。
		エージェントにはVPN機能とクラウドプロキシ(SWG)への通信を制御するモジュールが統合されていること。
		エージェントにはEPPと簡易ランサムウェア対策が統合されていること。
		端末の脆弱性をスキャンし、OSやアプリのパッチ適用状況を管理できる機能を有すること。
		エージェント接続においてIPsec VPNプロトコルで接続できること。
		エージェントはユーザーが容易にサービス停止できないこと。
		エンドポイントが社内もしくは社外どちらにいるかを自動で検知できること。
		社外だと判断した場合に自動でVPNを接続し、切断が容易でないこと。
	管理機能	HTTPS対応のWebインターフェースで遠隔保守が可能であること。
		Webインターフェースは日本語GUIでの表示に対応していること。
		外部ストレージサービスと連携することで、6ヶ月以上保管できること。
		レポート機能や分析機能を有すること。
		レポートのスケジュール機能により任意の日時に指定したメールアドレスに送付する機能を有すること。
		ユーザーからSaaSまでの通信経路や遅延、デバイスリソースを監視するDEM機能を有すること。
		管理者権限を細分化し、特定の機能やログのみ閲覧可能なロールを作成できること。
	サポート	SASE運用にあたり、技術問い合わせおよび障害時一次対応を行うヘルプデスクサポートを付帯すること。サポート期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるサポート期間についても、本案件の見積金額に含めること。なお、年間10インシデント以上の問い合わせ対応が可能であること。
	稼働率	実績ベースで99.99%以上であること。
	その他	ISMAP取得済みであること。

番号	項目名	仕様内容
3	バックアップソフト	

	端末台数	169台
	ユーザー数	183名
	期間	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。
	ライセンス	ライセンス追加は1ユーザーから追加可能であること。
		所有しているライセンス数を超えない範囲でバックアップ対象のユーザーを柔軟に管理者にて変更可能であること。
		ライセンスにはデータ容量による従量課金や価格変動要素がないこと。
		ライセンスは最小購入数量以上であれば、組織全体でなくとも導入可能であること
	サポートアプリケーション	下記Microsoft365アプリケーションに対応して、バックアップが取得できること。 ・SharePoint ・Exchange ・OneDrive ・Teams
	バックアップ要件	バックアップを実施する対象アプリケーションをユーザー毎に柔軟に設定可能であること。
		バックアップ環境としては、HWやソフトウェアインストール必要としない完全なSaas型であること。
		バックアップデータの保存先として、日本国内を選択できること。
		バックアップデータは保存量が無制限であること。
		必要とする期間、Microsoft365データを保持することが可能であること。 また、保存期間による追加費用が発生しないこと。
		バックアップ周期は日次、即時で実行可能であること。
		Microsoft365の元の場所や別の場所へのリストアを行えること。
		メールやファイル等のデータをエクスポートできること。
		複数のユーザーやサイトを横断的に検索し、必要なメールやファイルを抽出する機能を備えること。
		送信元、受信先、件名、本文など少なくとも50種類以上の検索フィルタを備え、柔軟に組み合わせることが可能であること。
		契約終了時はバックアップデータを返却可能であること。 また、返却されたバックアップデータからM365やその他の場所に無償で復元可能であること。
		サイバー攻撃等による大規模データ損失に備え、1時間あたり1TB以上のスループットの高速大規模リストア機能を備えること。あるいは必要に応じてライセンスアップグレードにより当該機能を充足できること。
		RBACの機能によりバックアップデータに対するアクセス権限をコントロール可能な

		こと。
	セキュリティ	データの転送中並びに保存の際、256ビットの暗号化を行い保護できること。
		ユーザーインタフェースへのログインに際し多要素認証によるアカウントログイン保護ができること。
		データ保存に際しバックアップデータのイミュータブルロックにより、管理者によってもデータの変更・改ざん・削除が行えないこと。
	管理機能	Web UIを備えること。
	サポート	サポートは管理者のポータルサイトから直接日本語で実施可能であること。
	稼働率	99.9%以上であること。
	その他	脆弱性やバグについてサービス側で利用者が意識せずに修正対応が行われていること。
		ISO/IEC 27001（ISMS）および、ISO/IEC 27017（ISMSクラウドセキュリティ）の認証を取得していること。

2.3. ソフトウェア（製品指定）

番号	ライセンス名	数量	期間
1	Microsoft365 A3(Education Faculty Pricing)	183ライセンス	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。

番号	ライセンス名	数量	期間
2	IT資産管理ツール		
	SKYSEA Client View S1H Cloud Edition ｸﾗｲｱﾝﾄﾗｲｾﾝｽ(100-249)	169ライセンス	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。
	SKYSEA Client View S1 Cloud Edition ﾘﾓｰﾄ操作 ｸﾗｲｱﾝﾄﾗｲｾﾝｽ (100-249)	169ライセンス	
	SKYSEA Client View S1/S3 Cloud Edition 紛失端末制御 ｸﾗｲｱﾝﾄﾗｲｾﾝｽ(1-499)	169ライセンス	
	ログ保管容量追加オプション（1TB)	5年	

番号	ライセンス名	数量	期間
3	EDR製品		
	SKYSEA Client View S1/S3 Cloud Edition EDRプラスパックCloud 年間利用料(5年間)（※構築費用、教育費用を含むこと）	169ライセンス	ライセンス期間は、2027年2月1日を開始日、2032年1月31日を終了日とする5年間とし、構築期間中に必要となるライセンス費用についても、本案件の見積金額に含めること。

※パターンマッチング型のエンドポイント保護（EPP：Endpoint Protection Platform）製品については、別途調達を行うこと。

3. 構築作業

3.1. 作業内容

(ア)機器の搬入及び設置

(イ)校務系パソコンの構築、導入

・エンドポイントセキュリティ対策

・Microsoft365 office

・多要素認証ソフトウェア

・IT資産管理ツール

(ウ)校務系プリンタの構築、導入

(エ)セキュリティUSBメモリの初期設定、導入

(オ)校務系ネットワークの構築、導入

・クラウド管理システム

・学校用PoE L2SWスイッチ

・学校用スイッチングハブ

・学校用無線AP

・学校用ファイアウォール

・和知支所用ファイアウォール（現行流用）設定変更

(カ)Microsoft 365の導入

(キ)Microsoft EntraID（ID管理サービス）への運用移行

(ク)Microsoft Intune（デバイス管理）への運用移行

(ケ)Microsoft SharePoint（ファイルサーバ）への運用移行

(コ)多要素認証システム（クラウドサービス）の構築、導入

(サ)SASE製品（クラウドサービス）の構築、導入

(シ)EDR製品（クラウドサービス）の構築、導入

(ス)Microsoft 365バックアップサービスの構築、導入

(セ)IT資産管理ツール（クラウドサービス）の構築、導入

(ソ)新規インターネット回線の敷設、導入

(タ)不要となる既存機器等の撤去、廃棄

(チ)ネットワークの配線・接続・取り付け

(ツ)既存ネットワーク機器の設定変更

(テ)利用者向け研修

(ト)完成図書作成

3.2. 作業に係る特記事項

各校での作業日程については教育委員会と協議の上、決定すること。

3.3. 設置・接続

(ア) 新規に導入する機器は全て開梱し、教育委員会の指示に従い設置、配線、接続を行うこと。また、機器開梱後に発生した梱包材（空箱等）は受注者において速やかに撤去するとともに、既存機器については教育委員会の指示に基づき指定された場所へ移動させ、移動後は機器単位、学校単位その他の区分により整理・集約を行うこと。

(イ) ネットワーク構築に必要なLANケーブル（カテゴリ6タイプ以上）は受注者が用意し、各機器を接続すること。LANケーブルの色は教育委員会と協議し決定すること。また、LANケーブルについては、接続先機器を識別できるよう、両端に機器名等を明示したタグを貼付すること。

(ウ) 別紙②に記載する各ソフトウェアをインストールし、動作確認を行うこと。各ソフトウェアの初期設定については、教育委員会と協議の上設定すること。

(エ) その他、接続・設定に必要な機器等は受注者が用意すること。

3.4. 検証

(ア) 機器、ソフトウェア、ネットワーク等が全て支障なく動作するように調整すること。

(イ) 設置、完了設定後は教育委員会に完了届を提出し、立ち会い検査を受けること。検査で指摘を受けた不備な点は教育委員会の指示どおり期日までに速やかに改善すること。

3.5. 研修

(ア) 設置・設定完了後、教育委員会と日程調整を行い、導入時研修を行うこと。

(イ) 研修は各学校において最低1回は実施すること。

(ウ) 研修内容は、新しい校務用端末の基本的な使用方法、多要素認証（顔認証）によるログオン方法、Microsoft 365（Outlook、Teams、SharePoint等）の基本操作、クラウドファイル共有サービスの使用方法、セキュリティに関する注意事項等とする。

3.6. 提出物

(ア) 導入機器明細表を提出すること。

(イ) 新規に導入した機器の設定書及び操作マニュアルを提出すること。

(ウ) 新規に導入した機器の設置後の写真を作成し、提出すること。

(エ) 工事を行った場合は、設置前、設置後の写真を提出すること。

(オ) LAN工事を行った場合は、配線図を提出すること。

(カ) システム構成図、ネットワーク構成図、ポート収容図を提出すること。

(キ) 研修で使用した研修マニュアルを提出すること。

(ク) 2. 機器仕様書の 2.2. ソフトウェアに関し、各仕様項目において要件として定める認証について、当該認証を取得していることを確認できる資料を提出すること。

(ケ) 上記資料は各2部ずつ紙で提出すること。また、データも別途CD-R等にて2部提出すること。

4. 設定業務について

4.1. 基本事項

教育委員会が指定する構築要件を「4.2 機器の搬入及び設置 詳細」以降に説明する。この要件に沿って、最適な学校ICTシステム環境基盤、学校ネットワーク基盤を構築すること。また、本仕様書で記載している学習系ネットワークとは、既存のパソコン教室や一般教室で使用しているネットワークのことを指し、校務で使われているネットワークは校務系ネットワークと記載する。なお、「本仕様書」に記載されている物品以外で必要となる物品は受注者で準備し整えること。

4.2. 機器の搬入及び設置 詳細

(ア) 機器搬入に係る詳細（経路等）については、教育委員会と協議の上、進めること。施設等を傷つけることの無いよう万全を期すこと。

(イ) 導入した機器には、教育委員会が指定する名称、番号等を記載したテープラベルを貼り付けること。

(ウ) 機器の導入に伴い不要となった配線及び梱包物等は撤去すること。

4.3. 校務系パソコンの構築、導入 詳細

(ア) 本件で調達するクライアントパソコン（ノート型）のマスター端末の構築およびマスターイメージの作成を行い、同一型番の168台にマスターイメージのクローニング作業を行うこと。

(イ) OSはWindows 11 Proで構築を行うこと。

(ウ) BitLocker 機能を使用し、PC 内の論理ボリューム（ドライブ）を暗号化すること。

(エ) 本事業で導入する各システムおよびクラウドサービスで必要なソフトウェアのインストールを行うこと。

(オ) 本町が指定するソフトウェアのインストールを行うこと。（別紙②参照）なお、教育委員会から別途インストール依頼があった場合は対応すること。

(カ) マスターイメージの検証期間を設け、イメージ展開前に教育委員会の了承を得ること。その際、追加のソフトウェアインストール等を指示された場合は対応すること。マスターイメージは小学校向け・中学校向けの2種類を作成すること。

(キ) クローニング作業後に個別設定を行うこと。（個別設定とはクローニング作業を実施したことで重複する設定項目の調整や個別インストールが必要なソフトウェアのインストールを表す。）

(ク) Microsoft Entra IDへのデバイス登録（Entra Join）を行い、組織のセキュリティポリシーおよび条件付きアクセスポリシーが適用される状態にすること。

(ケ) Microsoft Intuneへのデバイス登録を行い、コンプライアンスポリシー、デバイス構成プロファイル等による端末管理が行える状態にすること。

(コ) エンドポイント検知・対応（EDR）製品のエージェントをインストールし、脅威の検知および対応が行える状態にすること。また、パターンマッチング型のエンドポイントプロテクション（EPP）製品も同時にインストールし、ウイルス対策を行える状態にすること。

(サ)SASE製品のエージェントをインストールし、インターネット接続時のセキュリティポリシーが適用される状態にすること。
(シ)多要素認証ソフトウェアのクライアントをインストールし、顔認証およびパスワードによるOSログオンが行えるように設定すること。
(ス)IT資産管理ツールのクライアントをインストールし、操作ログ取得、資産管理、デバイス制御が行える状態にすること。
(セ)Microsoft 365のOfficeアプリケーション（Word、Excel、PowerPoint、Outlook、Teams等）をインストールすること。
(ソ)小中学校の養護教諭が使用する端末（計8台）には保健管理システムをセットアップし、既存端末からデータ移行を行うこと。
(タ)栄養計算ソフトの設定が必要な端末（3台）については教育委員会と協議の上対応すること。
(チ)京都府共同調達された校務支援システムが動作するよう校務用端末に設定を行うこと。
(ツ)校務用端末のIPアドレスはDHCPにより自動取得を行うこと。
(テ)端末の設置ヵ所によって有線LANもしくは無線LANに接続して動作確認を行うこと。
(ト)校務用端末にはセキュリティワイヤーを取り付け、盗難防止対策を行うこと。
(ナ)既設プリンタについても校務系パソコンから印刷が行えるように設定すること。
(ニ)校務用端末は導入時のディスクイメージを教育委員会に提供すること。
(ヌ)導入時からの不具合については受注者負担により復旧すること。

4.4. 校務系ネットワークの構築、導入 詳細

(ア)事前にネットワークセキュリティ強靭化（ゼロトラスト化）の構成内容の説明を行い、教育委員会の了承を得てから作業に着手すること。
(イ)校務系ネットワークで必要となる通信要件を調査し、それをもとに校務系ネットワーク機器の設計を行うこと。その際、必要に応じて既設機器の設定内容の確認や関連業者へのヒアリングを行い、過不足がないように留意すること。各学校のネットワークトラフィックは和知支所を経由してインターネットに接続する構成とすること。
(ウ)各学校にPoE対応L2スイッチを設置し、校務用端末およびネットワーク機器への電力供給および通信を行えるようにすること。
(エ)L2スイッチはファイアウォール経由で管理し、遠隔からの設定変更、監視、ファームウェア更新が行えるように設定すること。
(オ)校務系ネットワークと学習系ネットワークをVLANにより論理的に分離すること。VLAN設計については教育委員会と協議の上決定すること。
(カ)既設ネットワーク機器に接続されている機器を考慮し必要な通信要件を整理すること。その際、必要に応じて既設機器の設定内容の確認や関連業者へのヒアリングを行い、過不足がないように留意すること。
(キ)スイッチングハブを各学校および和知支所に設置し、端末の接続ポートを確保すること。
(ク)各学校に無線アクセスポイントを設置し、校務用端末からの無線LAN接続を可能にすること。無線アクセスポイントはPoE対応L2スイッチから給電すること。設置場所は別紙③に記載。

(ケ)無線アクセスポイントはIEEE802.11ax以上の規格で構築し、WPA3-Enterprise以上の認証方式に対応すること。SSIDへの接続は許可された端末のみ可能な構成とすること。

(コ)無線アクセスポイントの電波設計を行い、各学校の職員室、校長室、保健室、事務室、通級指導教室等の必要な範囲をカバーすること。

(サ)導入後にSSIDの追加が可能であること。

(シ)無線LANアクセスポイントに設定する SSIDについては、SSIDステルス化（SSID非公開設定）を行い、ブロードキャストを行わない設定とすること。

(ス)無線アクセスポイントの物理障害発生時に内蔵仮想コントローラの障害（全体への影響）が発生しない構成とすること。

(セ)各学校にファイアウォールを設置し、校務系ネットワークと学習系ネットワークを分離し、セキュリティを確保すること。

(ソ)各学校ファイアウォールについては、既存機器の保守期間を考慮し、令和8年9月中に更新をすること。

(タ)ファイアウォールはDHCPサーバ機能を有し、校務用端末へのIPアドレスの自動割当てを行うこと。ネットワークセグメントは学校毎で割当を行い重複しないように設計すること。

(チ)拠点内端末のトラフィックをSASEサービス経由でインターネットに接続できるようにすること。ただし、拠点内通信については、SASEサービスを経由せず直接通信ができるようにすること。

(ツ)和知支所のファイアウォールは現行機器を流用するため、本件で調達するネットワーク機器との連携に必要な設定変更を行う場合は、既存業者に設定変更を依頼すること。

(テ)各学校のファイアウォールおよび無線アクセスポイントはクラウド管理サービス経由で、L2スイッチはファイアウォール経由で管理できる構成とし、設定・監視・ログ管理を一元的に行えるようにすること。なお、和知支所のファイアウォールは現行流用のためクラウド管理システムの対象外とする。

(ト)各学校のファイアウォールのログはクラウド管理サービスに集約し、一元的に監視・分析が行えるようにすること。ログは最低1年間保存すること。

(ナ)各学校の通信はファイアウォールおよびSASEサービスのポリシーによって制御すること。ポリシーの内容については教育委員会と協議の上決定すること。

(ニ)インターネット回線の障害が発生した際、校務系ネットワークにリモート接続し、保守業務を継続できる環境を構築すること。リモート回線は閉域VPNなどを用いて、インターネットから論理的に分離されていること。また、リモート接続元においては、以下のセキュリティ対策を講じること。

- 接続端末は、不正な物理アクセスを防止するため、第三者の立ち入りが制限された場所に設置すること。
- 接続端末の利用時においては、画面の覗き見防止等の措置を講じ、第三者による情報漏えい防止が図られていること。
- 接続ログ及び操作ログを取得し、一定期間保管するとともに、不正アクセスの監視が可能であること。

・接続端末は、定期的に最新のセキュリティパッチを適用し、ウイルス対策ソフト等のセキュリティ対策ソフトウェアにより、常時保護されている状態を維持すること。
・アクセスにあたっては、ID・パスワードによる認証に加え、多要素認証を実施すること。
・リモート接続に利用する端末は、業務専用とし、許可された端末以外からの接続を禁止すること。
・端末の利用については、適切な運用管理を実施し、不正利用及び情報漏えいの防止措置を講ずること。また、接続端末は、社外への持ち出しを禁止するものとする。
・通信内容は暗号化されていること。

4.5. Microsoft 365の導入 詳細

(ア) 教育委員会用のMicrosoft 365テナントを構成し、組織情報（組織名、所在地等）、タイムゾーン、言語等の基本設定を行うこと。

(イ) 独自ドメインを新規取得しMicrosoft 365テナントに追加し、ドメイン所有権の検証を行うこと。ドメインの追加にあたっては、当該ドメインの権威DNSサーバに対して必要なDNSレコード（TXTレコード等）の設定を行うこと。

(ウ) Microsoft Entra IDの自動デバイス登録に必要なDNSレコード（enterpriseregistration、enterpriseenrollment等のCNAMEレコード）を権威DNSサーバに設定すること。

(エ) テナントのセキュリティ既定値群を確認し、教育委員会の運用方針に合わせた設定を行うこと。

(オ) 全体管理者、ユーザー管理者等の管理者アカウントを作成し、役割に応じた権限を付与すること。管理者の構成については教育委員会と協議の上決定すること。

(カ) Microsoft 365管理センターのサービス正常性通知およびセキュリティアラートの通知先を設定すること。

(キ) 教育委員会の職員に対してMicrosoft 365 A3ライセンスの割当てを行うこと。割当て対象については教育委員会と協議の上決定すること。

(ク) M365テナントに接続できる環境を制御し、管理機器、ネットワーク外からの接続を禁止すること。

4.6. Microsoft EntraID（ID管理サービス）への運用移行 詳細

(ア) Microsoft Entra IDのテナントを構成し、教育委員会の組織構造に合わせた設定を行うこと。

(イ) 学校職員用のユーザーアカウントを作成すること（180ユーザー程度）。

(ウ) 校長、教頭、事務職員、養護教諭等の役職・役割に応じたセキュリティグループを作成すること。グループ構成については教育委員会と協議の上決定すること。

(エ) 各学校の管理単位（OU相当）を作成し、ユーザーをそれぞれに所属させること。

(オ) Microsoft Entra IDの条件付きアクセスポリシーを設定し、端末のコンプライアンス状態、場所、サインインリスクレベル等に基づいたアクセス制御を行うこと。ポリシー内容については教育委員会と協議の上決定すること。

(カ) Microsoft Entra IDの認証ログ、サインインログ、監査ログを適切に管理すること。

(キ) 既存のActive Directoryのアカウント情報、グループ情報をMicrosoft Entra IDに移行すること。移行手順および移行スケジュールについては教育委員会と協議の上決定すること。移行するユーザーについては教育委員会に確認して承認を得ること。

4.7. Microsoft Intune（デバイス管理）への運用移行 詳細

(ア) Microsoft Intuneの環境を構成し、校務用端末の管理基盤を構築すること。

(イ) デバイスコンプライアンスポリシーを設定し、OSバージョン、セキュリティ更新プログラムの適用状況、BitLocker暗号化状態等の端末状態を評価できるようにすること。コンプライアンス不適合端末に対してはMicrosoft Entra IDの条件付きアクセスと連携し、Microsoft 365等のクラウドサービスへのアクセスを制限できるようにすること。

(ウ) デバイス構成プロファイルを作成し、校務用端末のセキュリティ設定（BitLockerによるディスク暗号化、Windows Defenderファイアウォール設定、パスワードポリシー等）を一元的に配布すること。

(エ) Microsoft Intuneのアプリケーション配信機能を用いて、必要なソフトウェアの配布およびバージョン管理を行えるようにすること。

(オ) Windows Update管理機能を用いて、更新プログラムの配布を段階的に行えるようにすること。検証グループに先行して適用し、問題がなければ全体に適用する運用が可能となるよう更新リングを構成すること。

(カ) 紛失・盗難時にMicrosoft Intuneからのリモートワイプ（遠隔初期化）およびリモートロックが行える状態にすること。

(キ) 既存のActive Directoryグループポリシー（GPO）の設定内容をMicrosoft Intuneのデバイス構成プロファイルに移行すること。移行内容については教育委員会と協議の上決定すること。

4.8. Microsoft SharePoint（ファイルサーバ）への運用移行 詳細

(ア) Microsoft SharePoint Onlineのサイト構成を行い、各学校の共有領域および学校全体の共有領域を作成すること。

(イ) 各学校のSharePointサイトには、Microsoft Entra IDのセキュリティグループと連携し、適切なアクセス権を割り当てること。

(ウ) 各学校の共有領域を作成し、容量制限を行うこと。容量の設定値については、SharePointの契約容量の範囲内で、現在のファイルサーバの使用量および職員数を加味して教育委員会と協議の上決定すること。

(エ) 各学校からアクセスできる学校全体の共有領域を作成し、容量制限を行うこと。容量の設定値についてはSharePointの契約容量の範囲内で教育委員会と協議の上決定すること。

(オ) SharePointのバージョン管理機能を有効にし、最低14世代のバージョンを保持すること。ユーザーが過去のバージョンを復元できるようにすること。

(カ) Microsoft 365のデータ保持ポリシーを設定し、一定期間経過後のファイル自動削除等の運用ルールを教育委員会と協議の上設定すること。

(キ) 和知支所に設置している現行のファイルサーバからSharePoint Onlineへデータ移行を行うこ

と。移行対象データおよびフォルダ構成については教育委員会と協議の上決定すること。なお、移行対象データの整理は事前に教育委員会にて行うものとする。

(ク)校務用端末からSharePoint Onlineへのアクセスはエクスプローラからシームレスにアクセスできるようにすること。

(ケ)その他共有領域の構成については教育委員会と協議の上決定すること。

(コ)Microsoft 365への通信は京丹波町が管理及び許可した端末からしかアクセスできないように通信制御を行えるようにすること。

4.9. Microsoft Teams環境の構築 詳細

(ア)Microsoft Teamsの組織全体の設定を行い、教育委員会の運用方針に沿ったTeams環境を構築すること。

(イ)各学校のチームを作成し、学校ごとの情報共有基盤を構築すること。チーム構成（学校単位、教科単位、管理職単位等）については教育委員会と協議の上決定すること。

(ウ)各チームにチャネルを作成し、用途に応じた情報の整理が行えるようにすること。チャネル構成については教育委員会と協議の上決定すること。

(エ)Teamsの会議ポリシーを設定し、会議の録画、画面共有、外部ユーザーの参加等に関する制御を行えるようにすること。ポリシー内容については教育委員会と協議の上決定すること。

(オ)外部組織とのTeams連携（外部アクセスおよびゲストアクセス）について、教育委員会の方針に基づき許可または制限の設定を行うこと。

(カ)Teams管理センターにおいて、利用可能なアプリの許可設定を行うこと。許可するアプリの範囲については教育委員会と協議の上決定すること。

4.10. 多要素認証システム（クラウドサービス）の構築、導入 詳細

(ア)多要素認証システムのクラウドサービス環境を構成し、顔認証およびパスワードによるOSログオン認証が行えるようにすること。顔情報はクラウド上で一元管理し、端末に依存せず任意の校務用端末から顔認証によるログオンが行えること。

(イ)学校職員（180名程度）の顔情報の登録を行うこと。登録作業は各学校にて行い、日程については教育委員会と協議の上決定すること。

(ウ)Microsoft Entra IDと連携したシングルサインオン（SSO）機能を有し、OSログオン後のMicrosoft 365等のクラウドサービスへのアクセスをSSO認証により簡略化できること。一般的なID／パスワードでの認証を行うWebシステムであればSSO対象とすること。ただし、技術的に困難な場合は教育委員会に説明の上、承認を得ること。

(エ)SSOの対象サービスの設定を行うこと。対象サービスについては教育委員会と協議の上決定すること。

(オ)認証ポリシーを設定し、認証の失敗回数によるアカウントロック、認証時間帯の制限等が行えるようにすること。

(カ)認証ログを適切に管理し、最低1年間は保存すること。ログはCSV等でエクスポートが行えること。

(キ)ユーザー情報はMicrosoft Entra IDと連携し、ユーザーの追加・変更・削除を一元的に管理できること。

(ク)管理者が認証状況の監視・確認を行える管理コンソールを提供すること。

4.11. SASE製品（クラウドサービス）の構築、導入 詳細

(ア)SASE（Secure Access Service Edge）サービスのクラウド環境を構成し、校務用端末からのインターネット通信に対してセキュリティを適用すること。通信は原則として暗号化されたトンネルを経由すること。ただし、OS由来の通信など技術的にSASEサービスを経由できない通信が存在する場合は、その一覧を教育委員会に報告し、承認を得ること。

(イ)Webフィルタリング機能を設定し、教育現場に不適切なサイトへのアクセスを制限すること。フィルタリングカテゴリおよびホワイトリスト・ブラックリストの設定については教育委員会と協議の上決定すること。

(ウ)SSL／TLS通信の検査機能を設定し、暗号化通信内の脅威を検知できるようにすること。検査除外対象については教育委員会と協議の上決定すること。

(エ)侵入検知・防御機能を設定し、不正なアクセスの検知および遮断が行えるようにすること。

(オ)クラウドアプリケーション制御機能を設定し、許可されていないクラウドサービスの利用を制限できるようにすること。

(カ)プライベートアクセス機能を設定し、校務用端末から庁内ネットワーク（和知支所）へのセキュアなリモートアクセスを行えるようにすること。学校拠点のファイアウォールとの連携設定を行い、拠点内からのアクセスも同様にSASEサービスを経由するようにすること。

(キ)校務用端末が学校外（自宅・外出先等）から利用される場合にも、同一のセキュリティポリシーが適用されるようにすること。

(ク)通信ログを適切に管理し、最低1年間は保存すること。

(ケ)管理コンソールにてポリシーの管理、通信状況の監視、レポート出力が行えるようにすること。

4.12. EDR製品（クラウドサービス）の構築、導入 詳細

(ア)EDR（Endpoint Detection and Response）製品のクラウド管理環境を構成すること。EDR製品は振る舞い検知による高度な脅威対策を主機能とし、EPP（Endpoint Protection Platform）機能については別途用意し、従来のアンチウイルス・マルウェア対策とEDR機能を組み合わせた多層防御を実現すること。

(イ)校務用端末にEDRエージェントを配布し、全端末（169台）のエンドポイントセキュリティを一元管理できるようにすること。

(ウ)端末上で実行されるプロセスのアクティビティを常時記録し、不正な挙動の兆候を検知する機能を有効にすること。

(エ)脅威検知時のアラート通知および自動対応ルールを設定すること。通知先および対応ルールについては教育委員会と協議の上決定すること。

(オ)脅威が検知された端末のネットワーク隔離が行えるようにすること。

(カ)端末がオフライン環境にある場合でも、不審な通信や挙動を検知した際に自動的にブロックする機能を有効にすること。
(キ)管理コンソールにて脅威の検知状況、端末の保護状態を一元的に確認できること。
(ク)検知ログおよびイベントログを適切に管理し、最低1年間は保存すること。

4.13. Microsoft 365バックアップサービスの構築、導入 詳細

(ア)Microsoft 365のデータ（SharePoint Online、Exchange Online、OneDrive for Business、Teams）のバックアップ可能なサービスを構成すること。バックアップデータは、バックアップ元テナントから独立（論理分離）した保管先（別テナント等）に保存し、元テナントの障害または管理者アカウント侵害時にもバックアップデータが保護される構成とすること。
(イ)バックアップの対象範囲、スケジュール、保持期間については、サービスのサブスクリプションに含まれる保存容量の範囲内で教育委員会と協議の上決定すること。
(ウ)バックアップデータからユーザー単位、フォルダ単位、ファイル単位での復元が行えるようにすること。
(エ)バックアップの実行状況および成否を管理コンソールから確認できるようにすること。
(オ)バックアップ・リストアの手順書を作成し、教育委員会に提出すること。

4.14. IT資産管理ツール（クラウドサービス）の構築、導入 詳細

(ア)IT資産管理ツールのクラウドサービス環境を構成し、校務用端末の一元管理を行えるようにすること。
(イ)本件で調達する校務用端末（169台）にクライアントソフトウェアをインストールすること。
(ウ)端末の操作ログ（ファイル操作、アプリケーション利用、Web閲覧履歴、印刷履歴等）を取得し、各学校の端末のログを管理コンソールから一元的に確認できるようにすること。
(エ)ハードウェア情報、ソフトウェア情報等の資産情報を自動収集し、台帳管理が行えるようにすること。
(オ)USBデバイス、外部記録媒体等のデバイス制御機能を設定し、許可されていないデバイスの使用を制限できるようにすること。制御ポリシーについては教育委員会と協議の上決定すること。
(カ)管理対象端末に対してリモート操作によるユーザサポートを行える機能を有すること。
(キ)紛失端末に対してリモートロックおよびリモートワイプが行える機能を有すること。端末の位置情報を取得し、紛失時の発見を支援する機能を有すること。
(ク)操作ログはCSV等でエクスポートを行い、最低1年間は保存すること。
(ケ)アラート機能を設定し、セキュリティポリシー違反等の事象を検知した際に管理者に通知が行われるようにすること。

4.15. 新規インターネット回線の敷設、導入 詳細

(ア)和知支所に新規のインターネット回線（1Gbps以上のベストエフォート回線）を敷設し、校務系ネットワークのインターネット出入口とすること。なお、回線敷設に係る初期費用

および回線利用料（60か月分）を含めた金額をすべて見積金額に含めること。
(イ)固定IPアドレスオプションを付与すること。
(ウ)回線工事に係る調整を回線事業者と行い、教育委員会の承認を得た上で施工すること。
(エ)回線終端装置からファイアウォールへの接続を行い、インターネット接続が行えるようにすること。
(オ)回線の開通テストを行い、教育委員会に報告すること。

4.16. 不要となる既存機器等の移設 詳細
(ア)パソコンおよびプリンタ、サーバ、その他教育委員会が指定する機器について、既存機器については教育委員会の指示に基づき指定された場所へ移動させ、移動後は機器単位、学校単位その他の区分により整理・集約を行うこと。

4.17. ネットワークの配線・接続・取り付け 詳細
(ア)新規に導入するネットワーク機器（ファイアウォール、PoEスイッチ等）の設置、およびインターネット回線終端装置からファイアウォールまで、ファイアウォールからPoEスイッチ、PoEスイッチから無線アクセスポイント間の配線・接続を行うこと。なお、校内のLAN配線については既設を流用する。
(イ)新規に敷設する配線はモール等で補強すること。
(ウ)配線工事は原則として業務終了後に行うこと。ただし、休校日等業務に支障がない場合はこの限りではない。
(エ)既存のLANケーブルで不要なものは撤去すること。

4.18. 既存ネットワークの配線・接続・取り付け 詳細
(ア)各学校に設置されている既設のファイアウォール、L2スイッチ等について、並行稼働や機器更新に伴い設定変更が必要な場合は、学校教育課の許可を得た上で設定変更を行うこと。なお、既存設定内容については契約締結後に開示する。
(イ)学習系ネットワークへの影響が生じないよう、十分な検証を行った上で設定変更を行うこと。
(ウ)和知支所のファイアウォール（現行流用機器）については、本件のネットワーク構成変更に伴い必要となる設定変更を行うこと。現行設定との整合性を確認した上で実施すること。
(エ)既存機器の設定変更にあたっては、教育委員会から既存保守業者への確認が必要となるため、余裕をもって設定変更内容を教育委員会に提示すること。

4.19. 利用者向け研修 詳細
(ア)設置・設定完了後、教育委員会と日程調整を行い、導入時研修を行うこと。
(イ)研修は各学校において最低1回は実施すること。
(ウ)研修内容は、新しい校務用端末の基本的な使用方法、多要素認証（顔認証）によるログオン方法、Microsoft 365（Outlook、Teams、SharePoint等）の基本操作、クラウドファイ

ル共有サービスの使用方法、セキュリティに関する注意事項等とする。研修内容の詳細については教育委員会と協議の上決定すること。

(エ)研修資料を作成し、教育委員会に提出すること。

4.20. 完成図書作成 詳細

(ア)導入機器明細表を提出すること。

(イ)新規に導入した機器の設定書及び操作マニュアルを提出すること。

(ウ)新規に導入した機器の設置後の写真を作成し、提出すること。

(エ)工事を行った場合は、設置前、設置後の写真を提出すること。

(オ)LAN工事を行った場合は、配線図を提出すること。

(カ)システム構成図、ネットワーク構成図、ポート収容図を提出すること。なお、事業実施前と実施後の構成の違いが分かるよう作成すること。

(キ)クラウドサービスの設定書（Microsoft Entra ID、Microsoft Intune、SharePoint Online、多要素認証システム、SASEサービス、EDRサービス、バックアップサービス、IT資産管理ツール）を提出すること。

(ク)クラウドサービスおよびネットワーク機器等のアカウント情報・パスワード一覧表を提出すること。

(ケ)2. 機器仕様書の2.2.ソフトウェアに関し、各仕様項目において要件として定める認証について、当該認証を取得していることを確認できる資料を提出すること。

(コ)研修で使用した研修マニュアルを提出すること。

(サ)上記資料はデータを電子媒体にて2部提出すること。

4.21. 既存機器の設定変更について

本案件において、更新対象外となる既存機器に関する設定変更が必要になると想定している。

なお、当該作業は、既存の保守業者により実施することを前提とするため、入札者は、上記設定変更に係る費用として、4,656,000円（税抜）を見積金額に含めること。

4.22. その他

(ア)その他、構築段階で発覚した作業は受注者が対応すること。

(イ)校務系ネットワーク接続前の機器については、受注者が用意した場所での構築等を認めるものとする。

(ウ)納品前の故障については、受注者側で対応を行うこと。

(エ)一次納品先を受注者が用意した場所にすることも可能だが、運送費等は受注者側で負担するものとする。

5. 保守業務について

5.1. 対応内容

(ア) 本稼働後5年間の保守業務を行うこと。

(イ) 対応時間は平日8時30分～17時00分とする。

(ウ) 機器およびクラウドサービスに関する技術的な問い合わせを、E-mailおよび電話にて対応すること。問い合わせについては学校の意見を聞き取りした上で教育委員会から受注者へ行う。

(エ) クラウドサービス（Microsoft 365、SASE、EDR、多要素認証、IT資産管理ツール、バックアップサービス等）の障害発生時には、サービス提供元との連携を含め、速やかに原因調査および復旧対応を行うこと。

(オ) 校務用端末のOS及び本案件で導入したソフトウェアの不具合対応を行うこと。

(カ) クラウドサービスの設定変更のうち、設計に関わらない軽微な修正・変更対応を行うこと。

(キ) 機器のトラブル発生時に、電話またはリモートで障害の切り分けを行うこと。クラウド管理コンソールを活用した遠隔診断を含むこと。

(ク) 緊急を要する機器のトラブル発生時には、技術者の訪問により障害の切り分けを行うこと。

(ケ) 技術者の訪問により、機器の修理手配やリカバリによる復旧作業を行うこと。

(コ) 障害発生時においては、対象となる拠点へ2時間以内に到着できること。

(サ) 導入したソフトウェアおよびクラウドサービスにおいて、セキュリティ上重大な脆弱性が発見された場合は、教育委員会と対応協議すること。

(シ) 機器障害が発生し保証対象の場合は、メーカーへの問い合わせを行い、交換対応を実施すること。

(ス) 機器仕様を満たしている機器保守を含むものとする。

(セ) インターネット回線を介さない、リモート保守環境に必要な機器類においても本稼働後5年間の保証をすること。

(ソ) 製品の機能や概要に関する質問に回答すること。但し、ソフトウェア製品の操作方法については、対象範囲外とする。

(タ) Microsoft 365の管理者向け運用支援（ユーザーの追加・変更・削除、セキュリティグループの管理、ライセンスの割当て変更等）について、教育委員会からの依頼に基づき対応すること。

(チ) 年に1回以上、クラウドサービスの利用状況、セキュリティインシデントの発生状況等をまとめた運用報告書を教育委員会に提出すること。

(ツ) 月次点検を実施し、対象システムが正常に稼働していることやバックアップが正常に取得できていること等を確認すること。点検結果については月次報告書として教育委員会へ提出すること。月次報告書には、点検結果に加え、当該月に受付・対応した問い合わせ及び障害対応の概要（内容、対応状況等）を取りまとめて記載すること。

(テ) 学校の教職員が誤操作等によりファイルサーバ上のファイル又はフォルダを削除した場合、教育委員会からの依頼に基づき、当該クラウドサービスの提供する復元機能又はバックアップサービスを用いて、可能な範囲で速やかに復元対応を行うこと。なお、復元可否は保持期間、権限、削除状況（ごみ箱からの削除を含む）等の条件により左右されるため、受注者は復元可否及び復元

方法・所要時間の見込みを教育委員会に報告のうえ対応すること。

（ト）四半期に1回以上、教育委員会との定例会を実施すること。定例会では、当該期間の問い合わせ及び障害対応状況、クラウドサービスの利用状況、セキュリティ上の懸念事項並びに改善提案等を報告し、今後の対応方針について協議すること。なお、定例会の議事録を作成し、教育委員会へ提出すること。

6. 賃貸借契約内容について

6.1. 契約方法

長期継続契約による賃貸借契約

6.2. 契約期間

令和９年（２０２７年）２月１日から令和１４年（２０３２年）１月３１日まで

6.3. 支払方法

支払は月単位とし、当月分の賃借料を受理した日から３０日以内に支払うものとする。契約期間に１月未満の端数がある場合は、賃借料月額に基づき日割り計算とする。

消費税及び地方税については、法定の税率を乗じた金額（円未満は切り捨て）とする。

6.4. 賃貸借期間満了後の措置

賃貸借物件を無償にて譲渡すること。

6.5. 契約の変更・解除

本件は、地方自治法第２３４条の３の規定による長期継続契約のため、契約締結の日の属する年度の翌年度以降において、当該契約に係る賃借人の歳出予算について減額又は削除があった場合、賃借人は、契約を変更し、又は解除することができる。上記の規定により契約を変更し、又は解除された場合において、賃貸人に損害が生じたときは、賃借人は、賃貸人に対して損害賠償の責めを負うものとする。この場合における賠償額は、賃借人と賃貸人が協議したうえで決定するものとする。

6.6. その他

賃貸借期間を通じて賃貸借物件を火災、盗難等を対象とする動産総合保険に加入する。

7. 納入期限及び納入方法等について

7.1. 納入期限

令和９年（２０２７年）１月３１日

7.2. 納入方法

各納入場所に機器を設置し、機器、ソフトウェア及びネットワーク等が支障なく安定的に動作することを確認すること。

7.3. 納入検査

京丹波町内において納入検査を行うものとする。賃貸人は納入予定の物品をあらかじめ発注者へ連絡し、納品後、賃貸人の立会いのうえ検査を行うこと。

8. 入札金額について

６０箇月分の賃貸借料率で算定し、１箇月分の賃貸借金額（消費税抜き）を入札価格として記載する。

9. 業務体制

9.1. 資格要件等

（ア）本業務構築にあたり以下の要件を満たす者が行うこと。

・ISMS情報セキュリティマネジメントシステム認証を取得していること。

・本件に係る人員に情報処理安全確保支援士、ネットワークスペシャリストの資格を保有したものが含まれること。当該人員は、自社と直接的かつ恒常的な雇用関係にあるものとする。この場合、恒常的な雇用関係とは、入札時点において３箇月以上の雇用関係があることをいう。

・個人情報保護の観点から本件の保守業者に関しては会社としてPマークを取得していること。

なお、自社で要件を満たすことができない場合は、要件を満たす構築業者を１社のみ指定できるものとし、原則、構築業者による再委託は認めない。ただし、業務遂行上必要であり、発注者が承諾した場合に限り再委託を行うことができる。

（イ）本業務構築にあたり従事者の能力が不足していると判断した場合は、従事者の交代を求めることができるものとする。

（ウ）従事者を変更する場合は、十分な引継ぎを行い業務に支障をきたさないようにすること。

（エ）本業務にあたり、定期的に発注者と打合せ（議事録の提出）を行い構築すること。

（オ）契約締結後、５日以内に「業務計画書」「業務履行体制図」「業務従事者名簿」等を提出すること。

（カ）必要に応じて、本町行政情報ネットワークシステム保守業者、本町イントラネット保守業者、本町デジタル広報課と調整及び連携し、システム停止及び障害発生することなく構築すること。

（キ）現地作業の際、従事者は身分証を必ず携帯し、受注者名の記載された腕章を身につけること。

10. その他

10.1. 各種要件

（ア）本業務で調達する機器は、全て新品とすること。

（イ）機器運搬に係る一切の費用等については、賃貸人が負担すること。また、機器運搬の際は慎重かつ丁寧に扱うこと。万が一、運搬中に故障した場合は、即日修理を行うか、予備機を賃貸人において準備すること。

（ウ）機器運搬中に事故・盗難等が発生しないよう十分注意を払うこと。事故・盗難等発生した場合は、賃貸人の責任で処理すること。

（エ）機器納品作業等において、庁舎設備に損傷を与えないように十分注意すること。また、必要な場合は養生を行うこと。もし、建築物及び構築物等に損傷を与えた場合は、賃貸人の責任において現形復旧すること。

（オ）災害・事故等により機器納入等の工程変更が発生した場合は、直ちに監督職員と協議の上、調整を行うこと。

（カ）本業務の履行にあたり「教育情報セキュリティポリシーに関するガイドライン」に準拠するほか、京丹波町並びに京丹波町教育委員会の規定を遵守すること。また、機器納品作業及び構築作業等においては、京丹波町教育委員会の指示に従い作業を行うこと。

（キ）本業務において、仕様書に明記されていない事項でも、その履行上当然必要な事項については、賃貸人が責任を持って対応すること。

（ク）その他、問題が発生した場合は賃借人と賃貸人が協議の上、解決にあたること。

10.2. 情報保護関係

（ア）受注者は、何人に対しても、受注期間中又は受注期間終了後を問わず、業務上知り得た内容を一切漏らしてはならない。また、受注者は、本業務の実施において知り得た知識・情報及び貸与資料等を第三者へ漏洩してはならない。

（イ）本業務において関連する資料は、管理を厳重にし、発注者の指示又は承認があるときを除き他の業務に利用してはならない。

別紙①　ハードウェア割当て一覧

機器名	竹野小学校	丹波ひかり小学校	下山小学校	瑞穂小学校	和知小学校	蒲生野中学校	瑞穂中学校	和知中学校	和知支所（教委）	予備機	合計
校務用パソコン	14	25	13	21	16	32	23	22	1	1	168
管理用パソコン	0	0	0	0	0	0	0	0	1	0	1
セキュリティワイヤー	1	1	0	0	1	0	0	1	0	1	5
拠点スイッチ(PoE L2 スイッチ)	1	1	1	1	1	1	1	1	1	1	10
職員室用 HUB	1	1	1	1	1	1	1	1	1	0	9
無線 LAN アクセスポイント	3	3	3	3	3	4	4	4	0	1	28
学校用ファイアウォール	1	1	1	1	1	1	1	1	0	0	8
セキュリティ USB メモリ	2	2	2	2	2	2	2	2	2	0	18

別紙②　アプリケーション割当て一覧

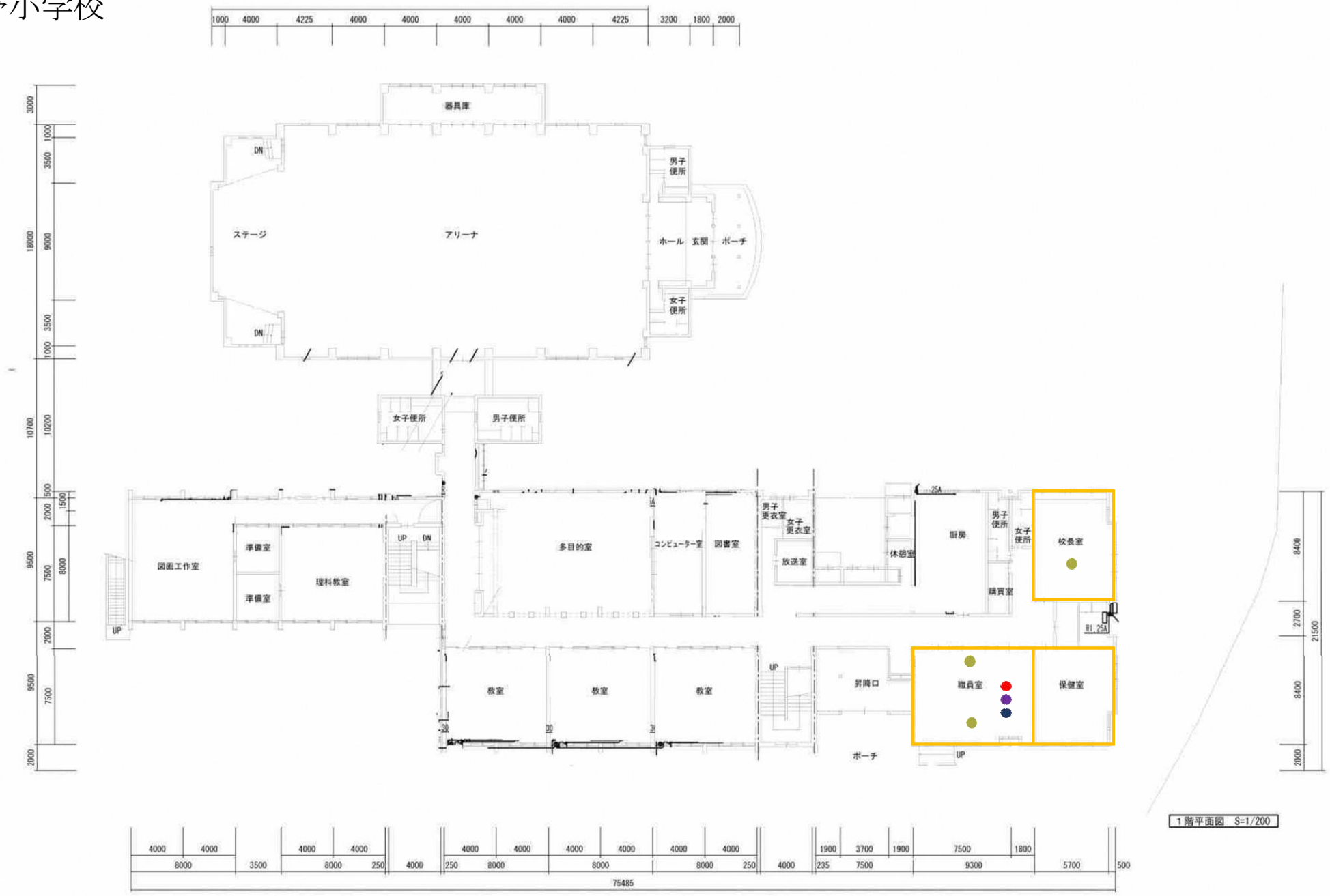
アプリケーション名	竹野小学校	丹波ひかり小学校	下山小学校	瑞穂小学校	和知小学校	蒲生野中学校	瑞穂中学校	和知中学校	和知支所（教委）	合計
Microsoft 365 A3 (Education Faculty Pricing)	17	28	14	23	18	31	23	21	8	183
多要素認証・シングルサインオン	17	28	14	23	18	31	23	21	8	183
SASE 製品	17	28	14	23	18	31	23	21	8	183
EDR 製品	14	25	13	21	16	32	23	22	3	169
EPP 製品	14	25	13	21	16	32	23	22	3	169
IT 資産管理ツール	14	25	13	21	16	32	23	22	3	169
バックアップソフト	17	28	14	23	18	31	23	21	8	183
えがお４	1	1	1	1	1	1	1	1	0	8
カロリーメイク	0	1	0	1	1	0	0	0	0	3

資　料「小中学校平面図」

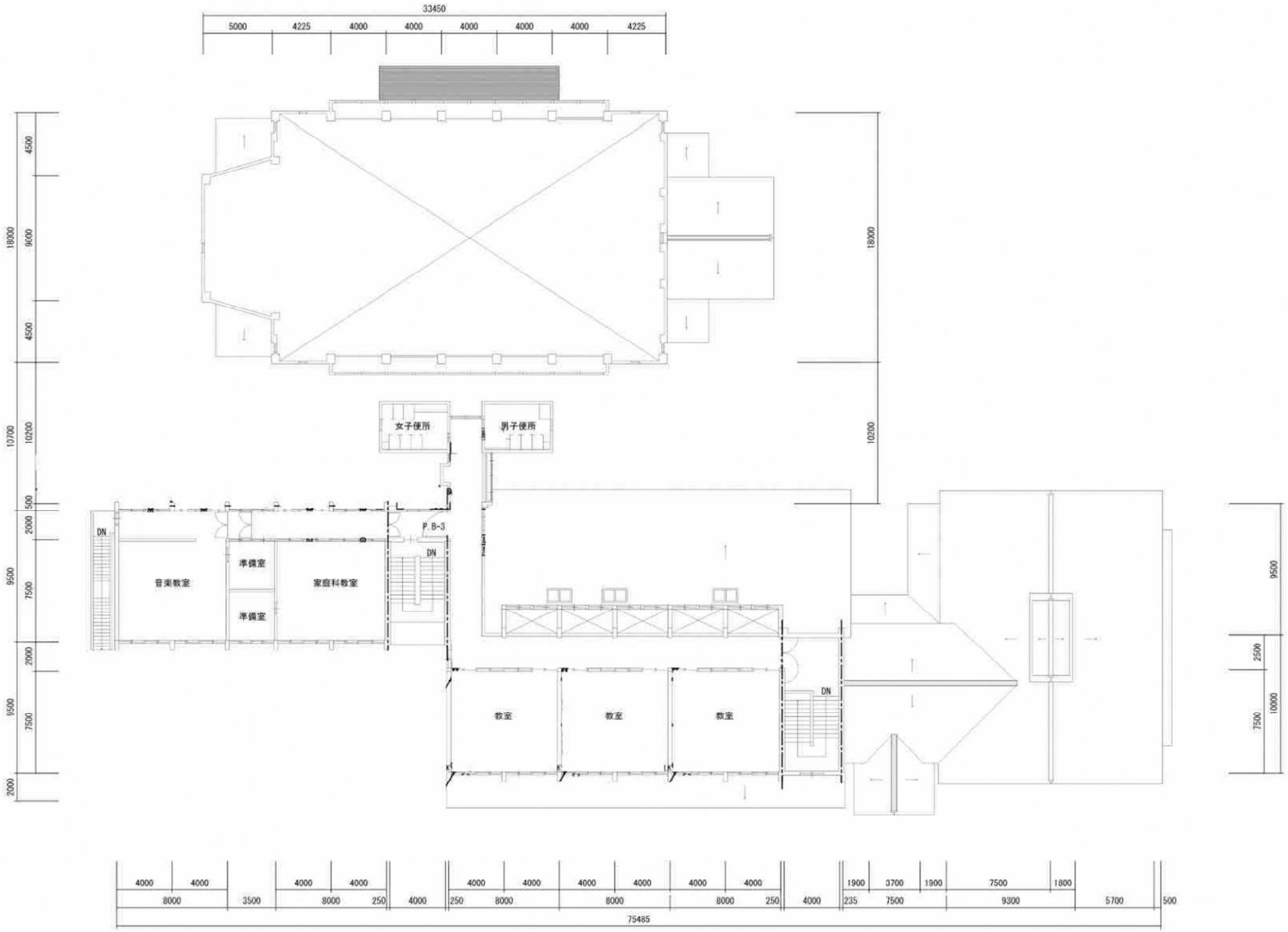
●印：「校務系ルーター」設置場所
●印：「ファイアウォール」設置場所
●印：「拠点スイッチ(PoE L2 スイッチ)」設置場所
●印：「無線アクセスポイント」設置場所

別紙③

竹野小学校



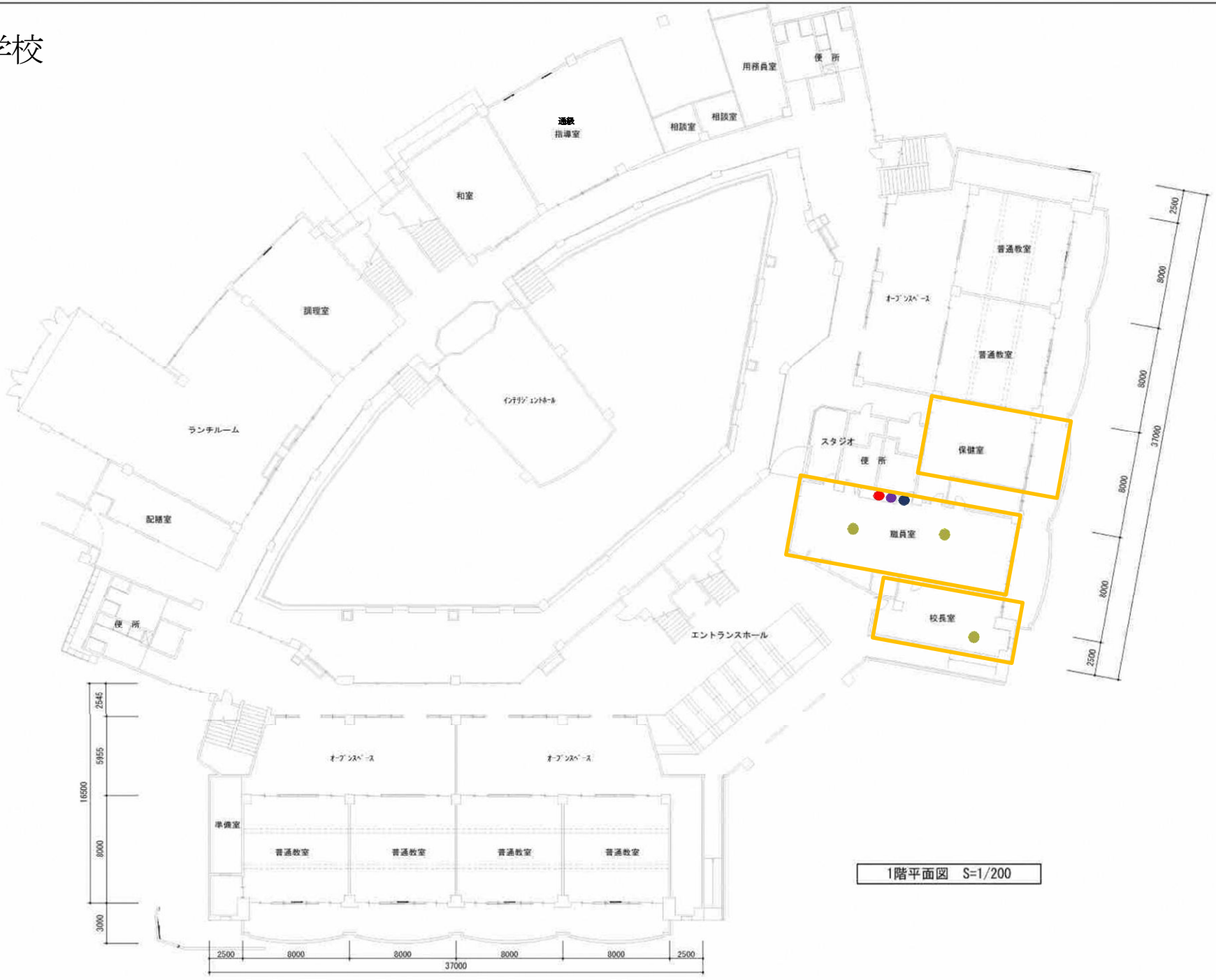
学校名	竹野小学校		1階平面図
			1/200



2階平面図　S=1/200

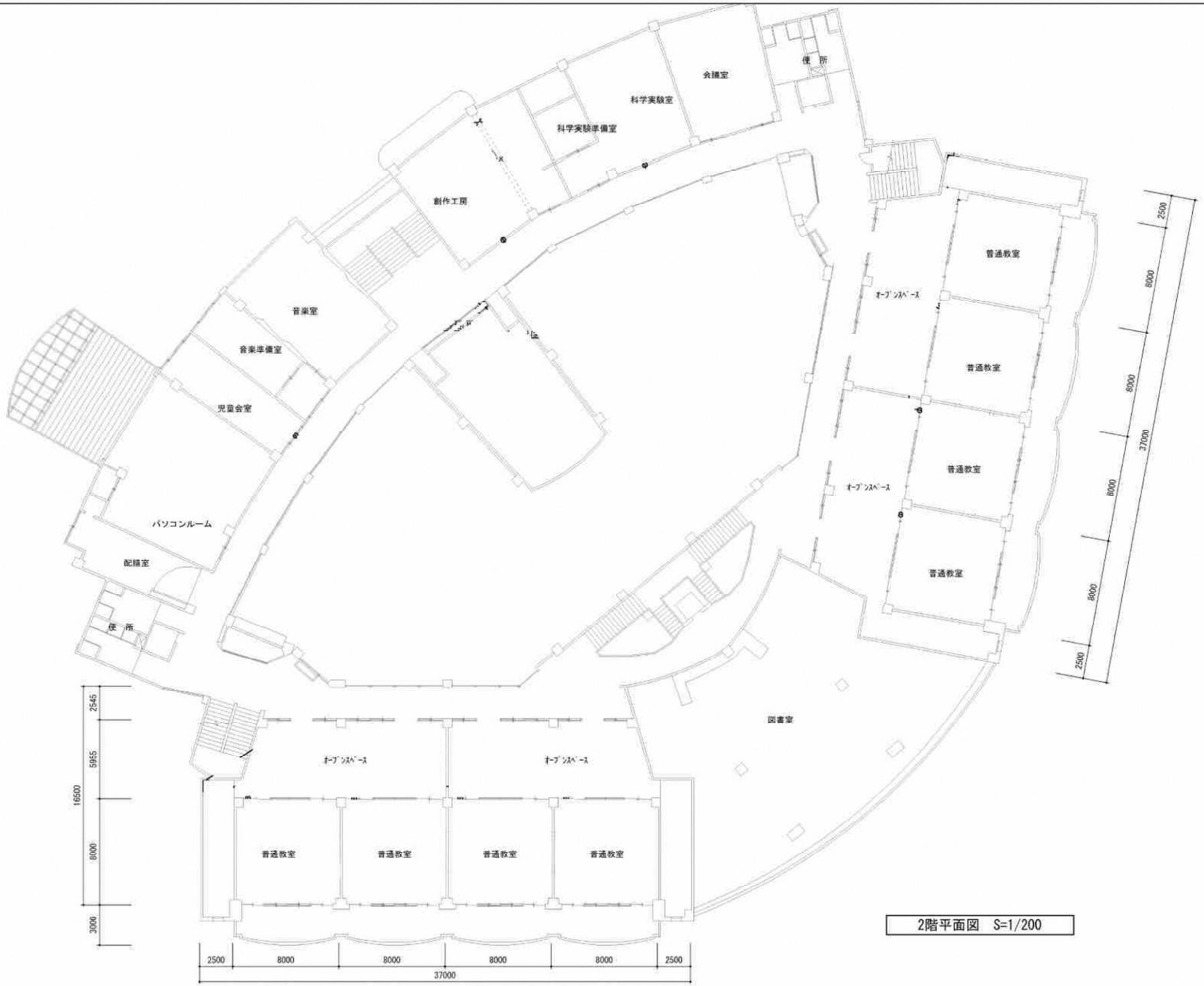
京丹波町		学校名	竹野小学校	図名	2階平面図
	日	工事名		縮尺	1/200

丹波ひかり小学校



1階平面図　S=1/200

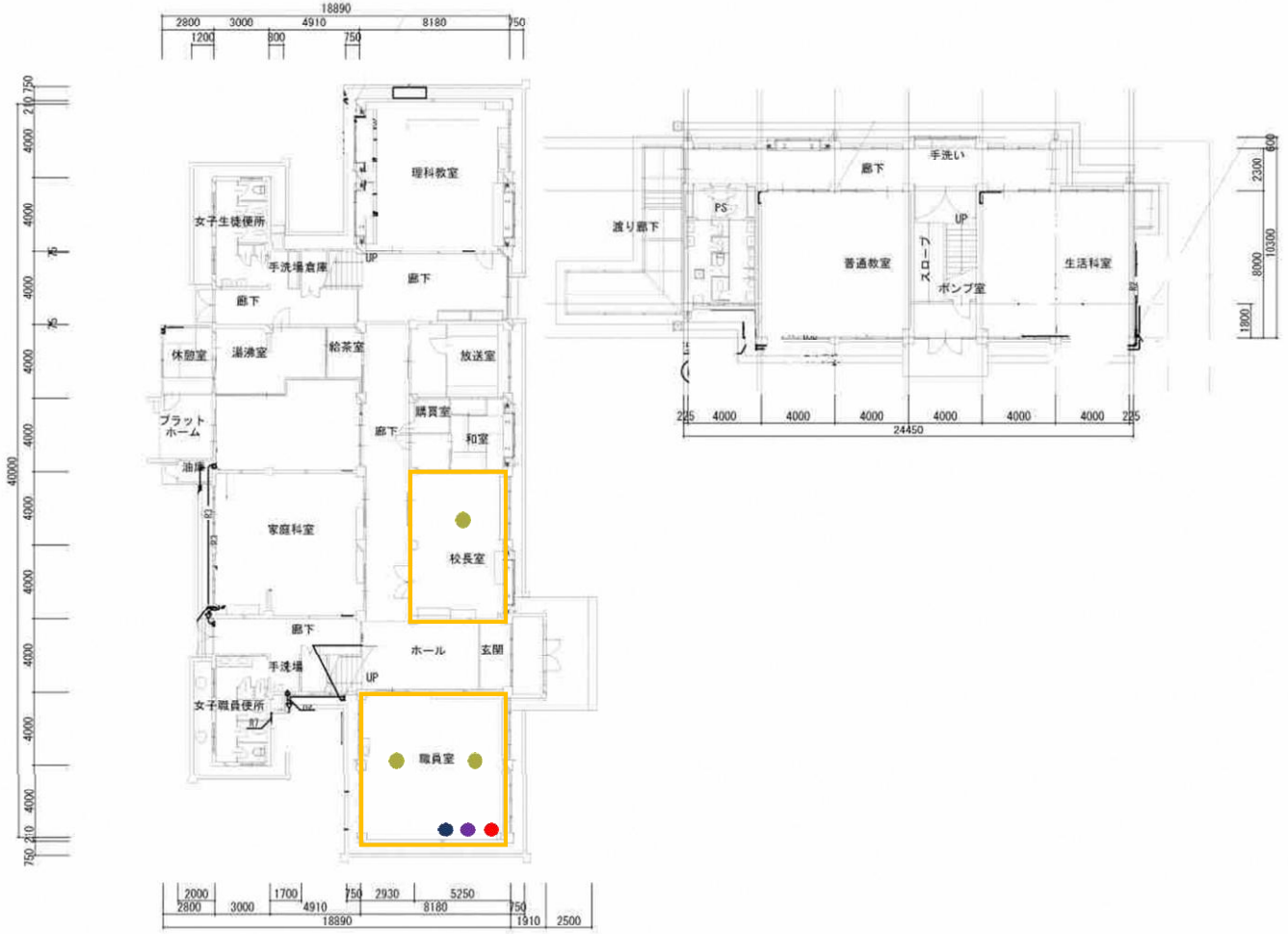
学校名	丹波ひかり小学校		1階平面図
			1/200



2階平面図　S=1/200

京丹波町					
	学校名	丹波ひかり小学校	図名	2階平面図	
	工事名		縮尺	1/200	

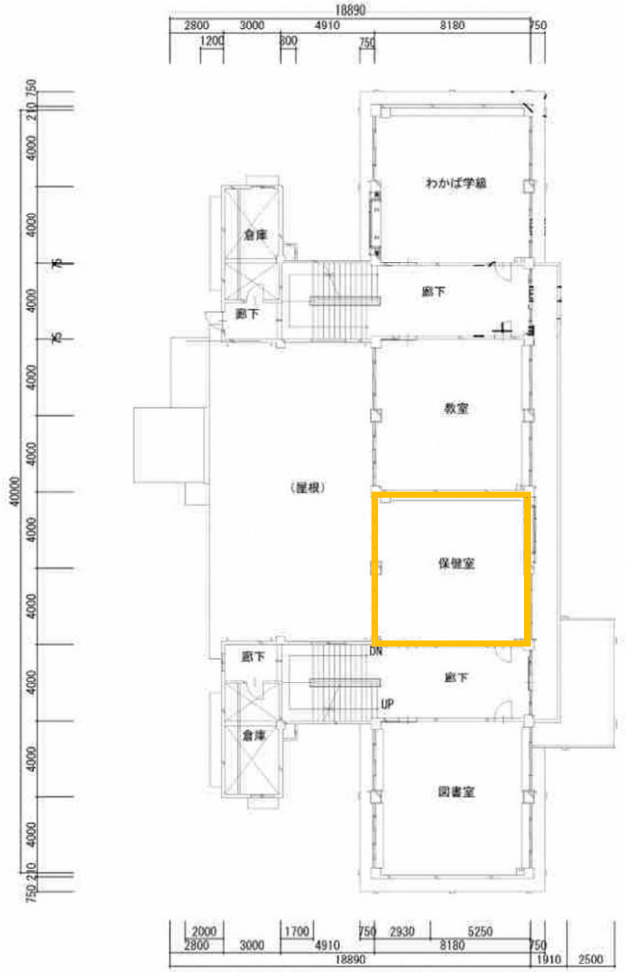
下山小学校

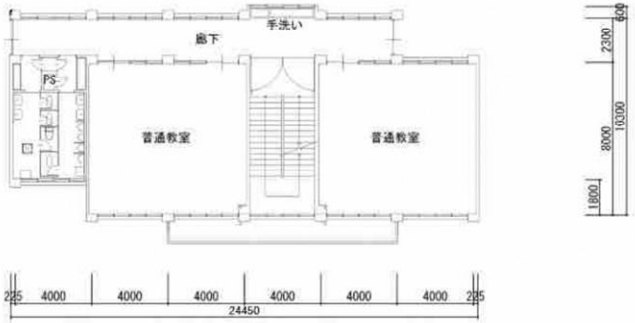


断面図

1階平面図　S=1/200

検図		学校名	下山小学校	図名	1階平面図
		工事名		縮尺	1/200





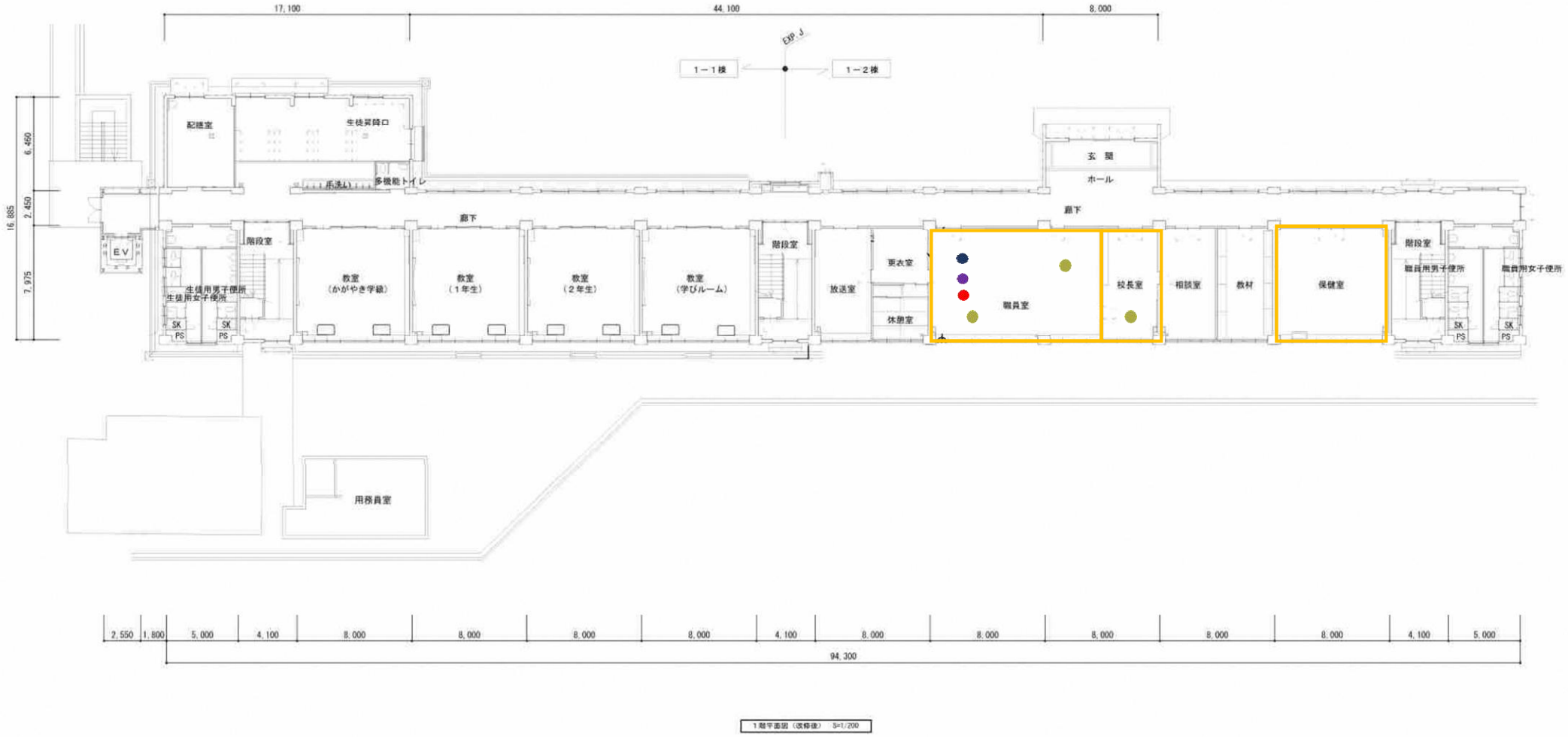
2階平面図　S=1/200

京丹波町				学校名	下山小学校	図名	2階平面図
				工事名		縮尺	1/200

3階平面図 S=1/200

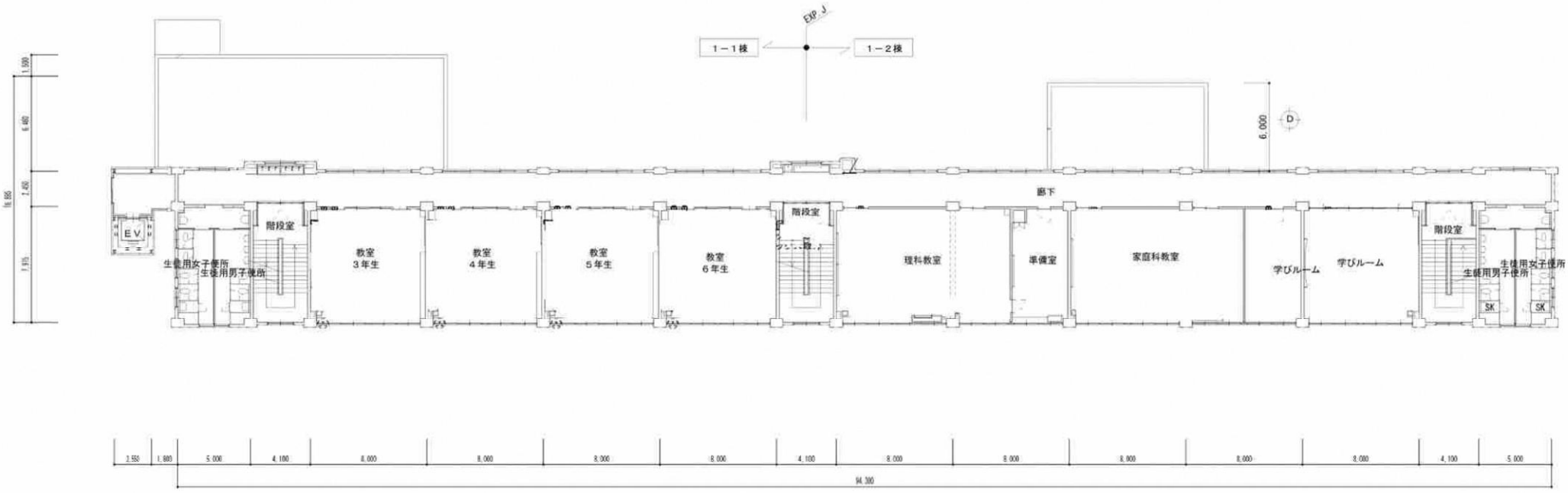
京丹波町	学校名	下山小学校	図名	3階平面図
	工事名		縮尺	1/200

瑞穂小学校



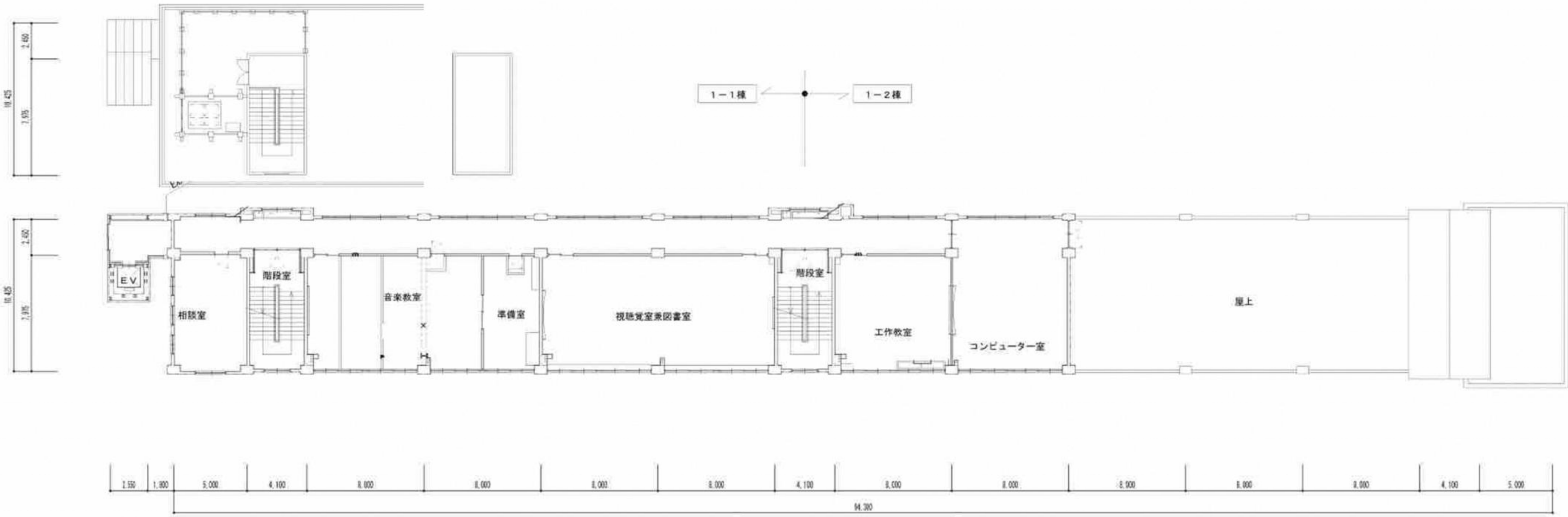
1階平面図（改修後） S=1/200

学校名	瑞穂小学校		1階平面図
			1/200



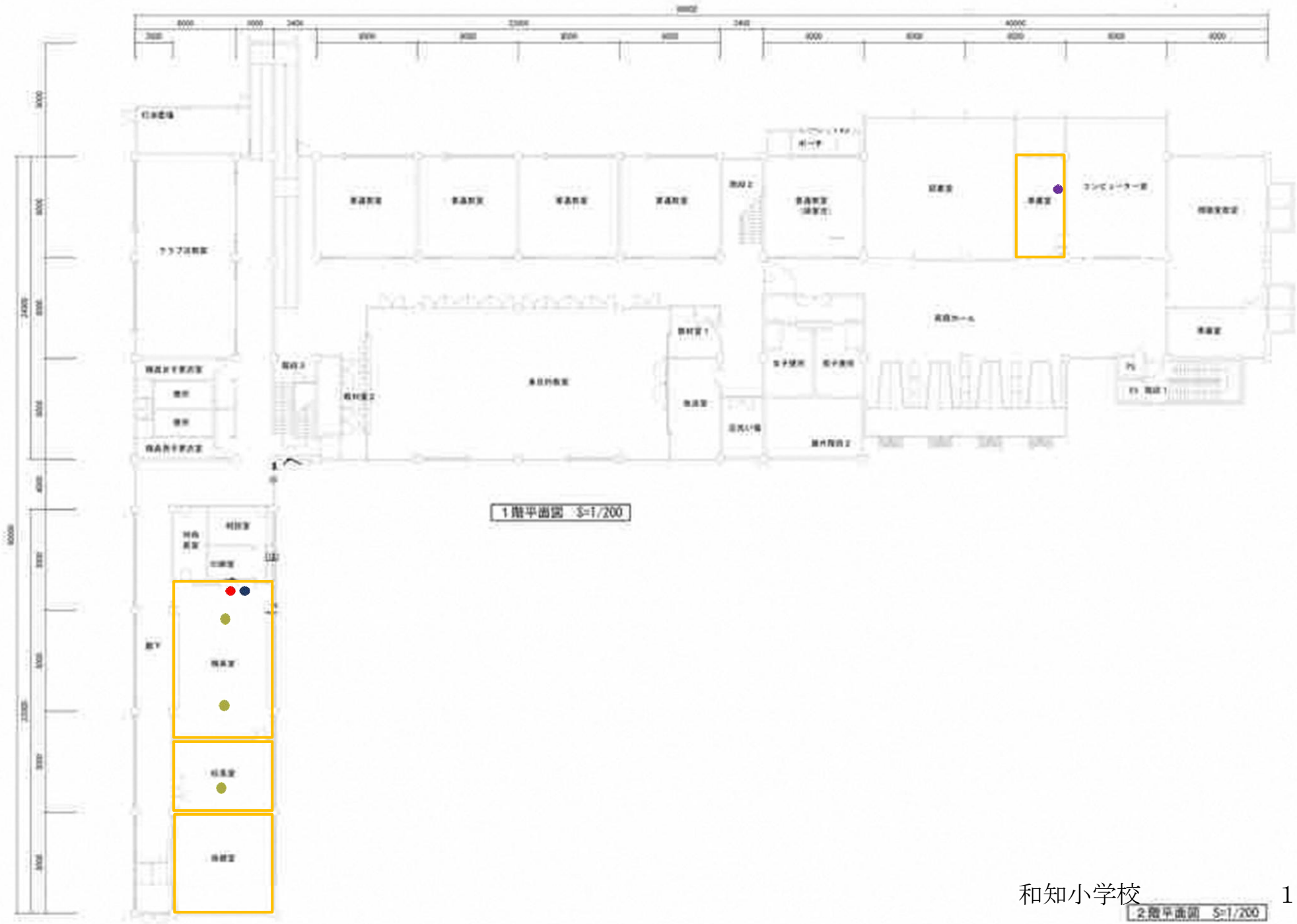
2階平面図　1/200

京丹波町			
学校名	瑞穂小学校	図名	2階平面図
工事名		縮尺	1/200



3階平面図　1/200

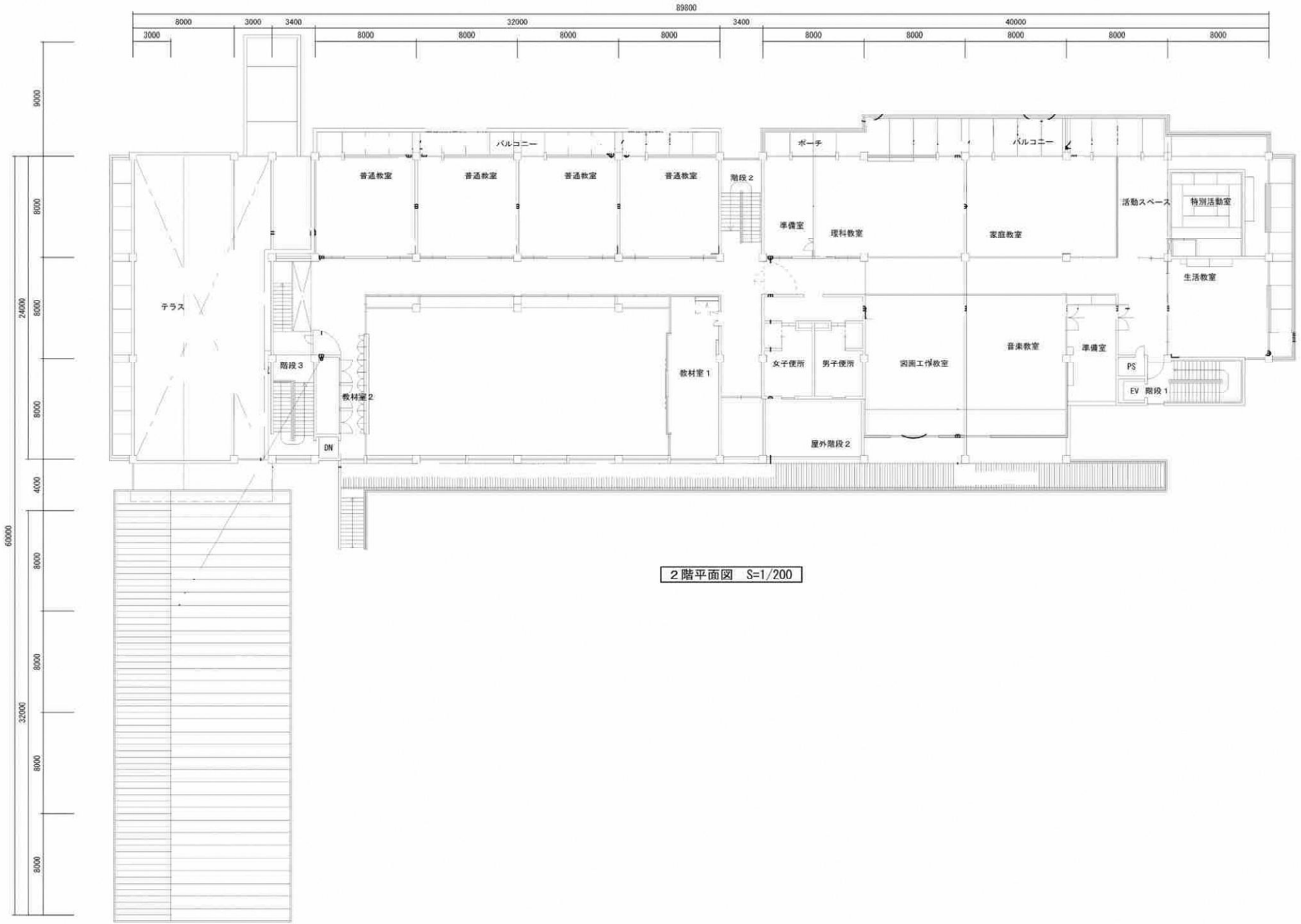
京丹波町	学校名 瑞穂小学校	図名	3階平面図
	工事名	縮尺	1/200



1階平面図　S=1/200

2階平面図　S=1/200

和知小学校

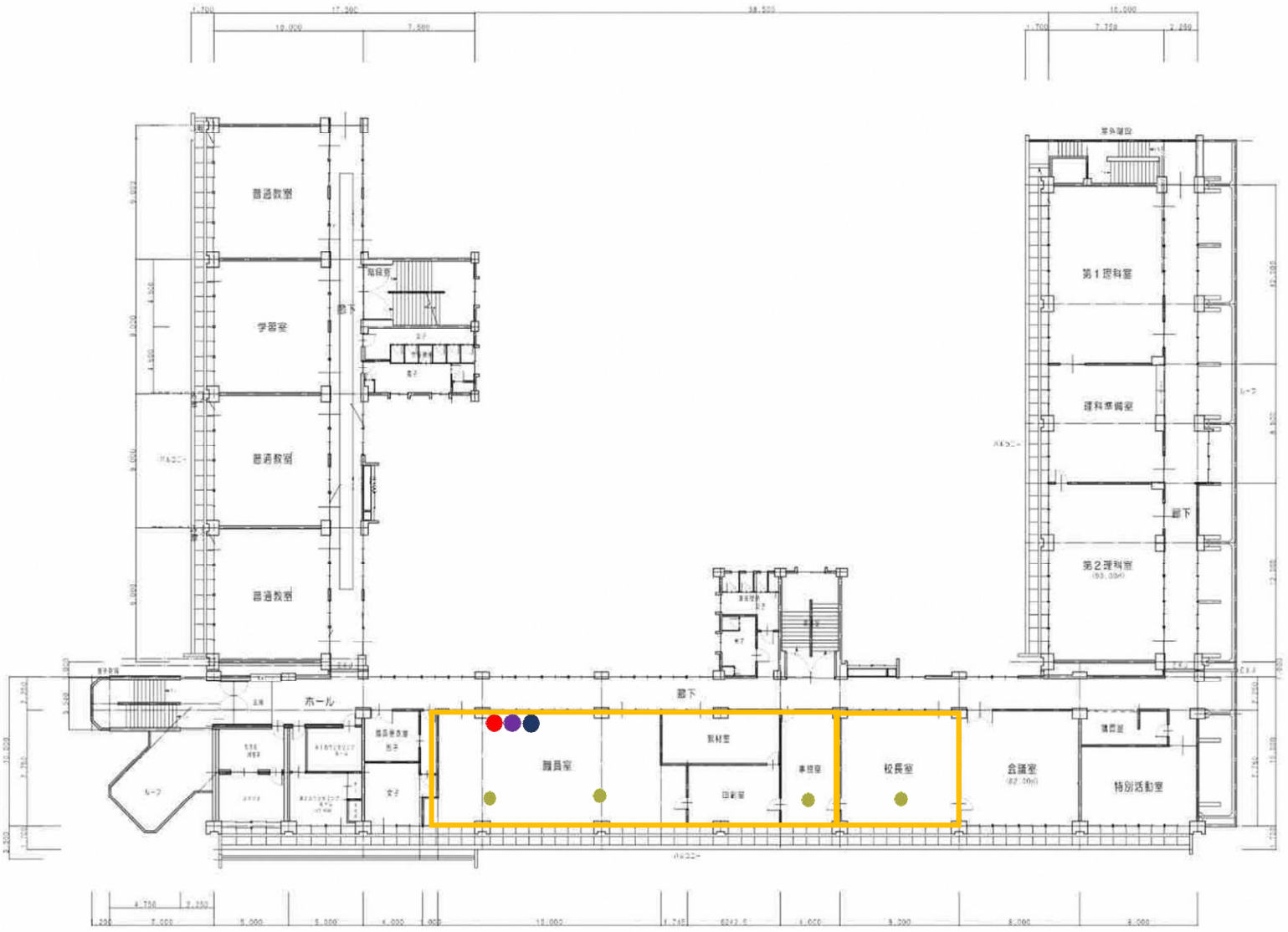


２階平面図　S=1/200

京丹波町					
	学校名	和知小学校	図名	２階平面図	
	工事名		縮尺	-	

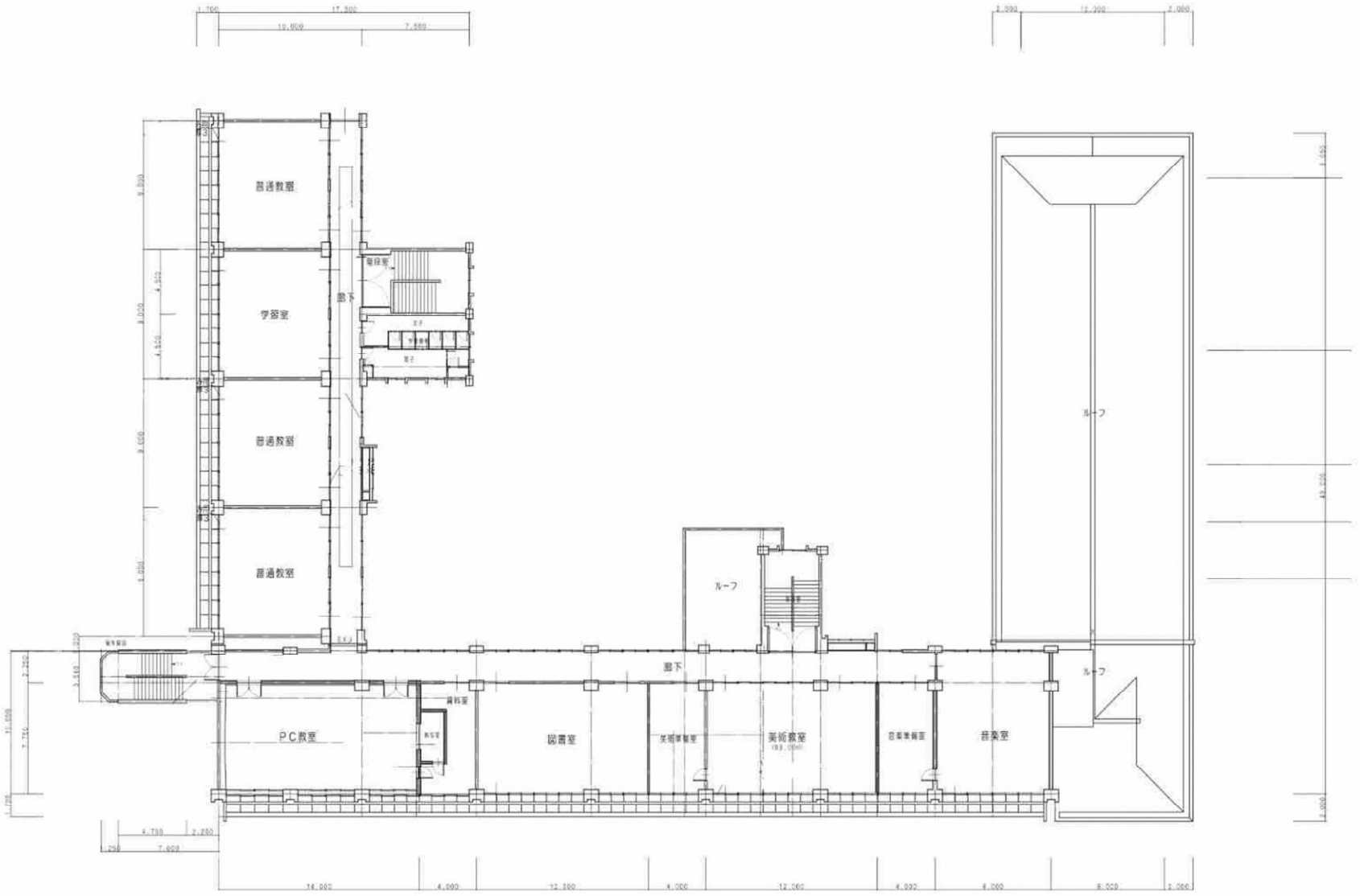

学習室
普通教室
普通教室
普通教室
階段室
廊下
テラス
技術室
準備室
倉庫
廊下
通路
ホール
廊下
生徒昇降口
保健室
障害児学級1
障害児学級2
被服教室
家庭科準備室
調理教室

蒲生野中学校　　1F



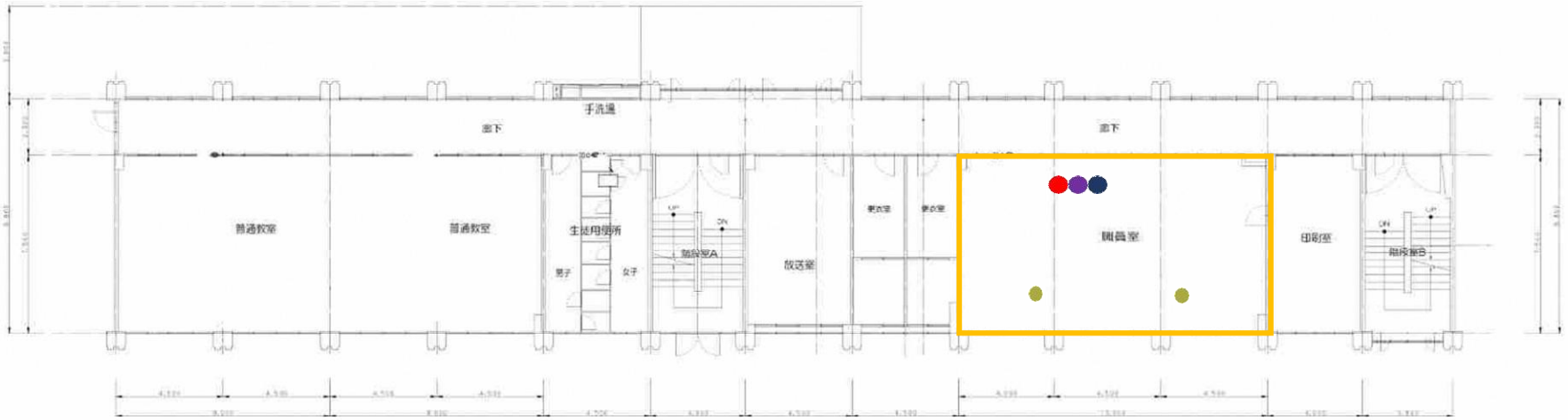
蒲生野中学校

蒲生野中学校

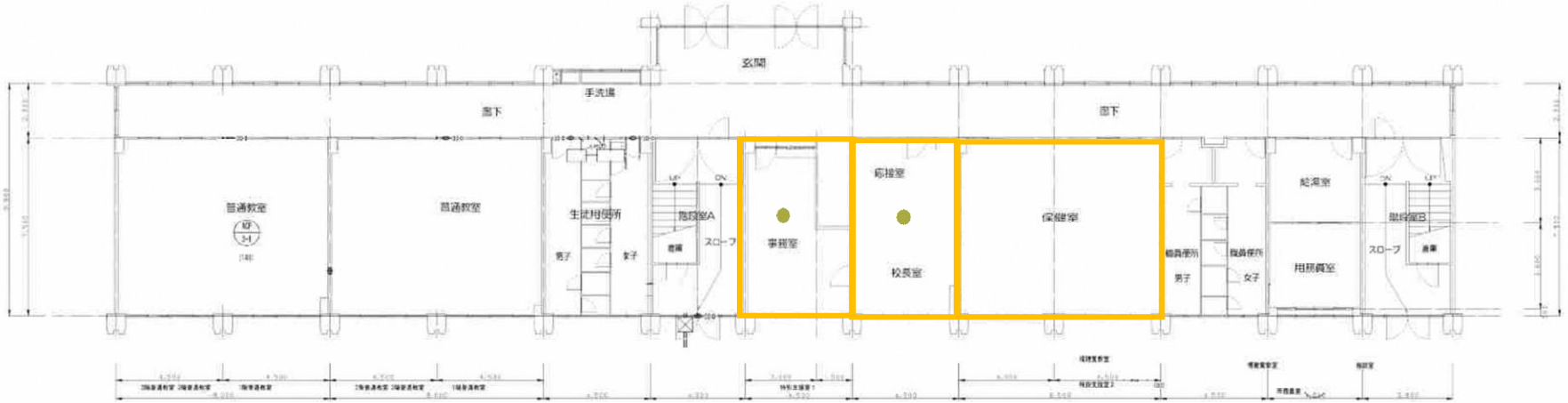


滝生野中学校				3階平面図
DR.	CK.	SV.	DATE	

瑞穂中学校

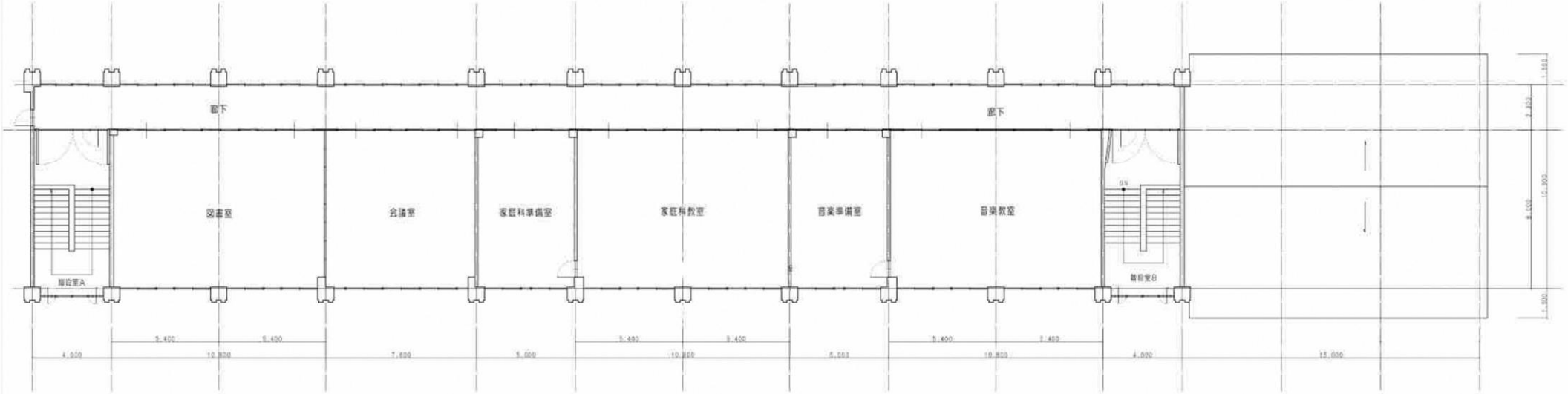


2階平面図

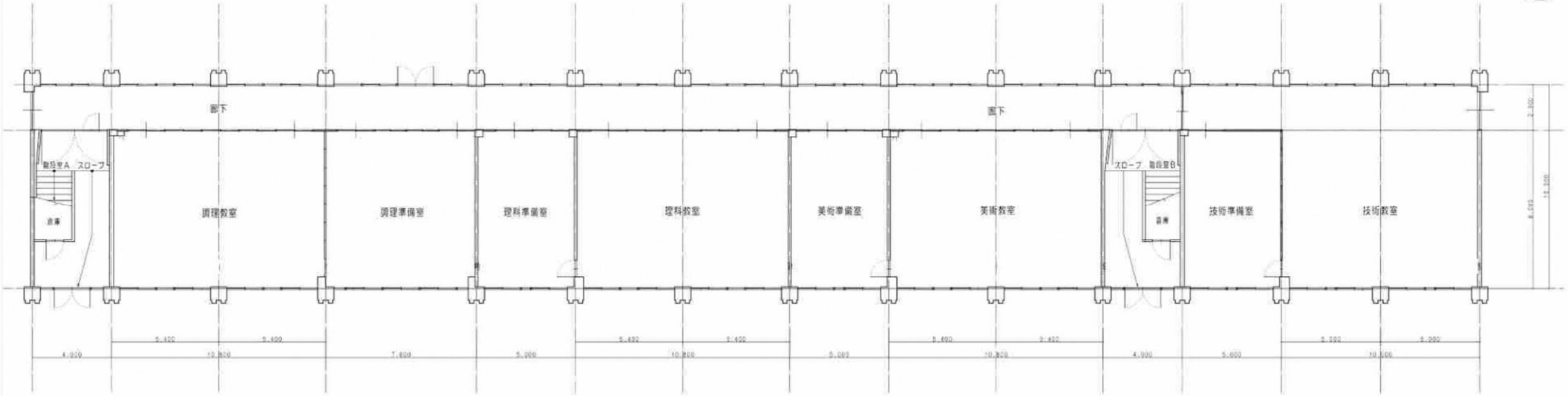


1階平面図

瑞穂中学校

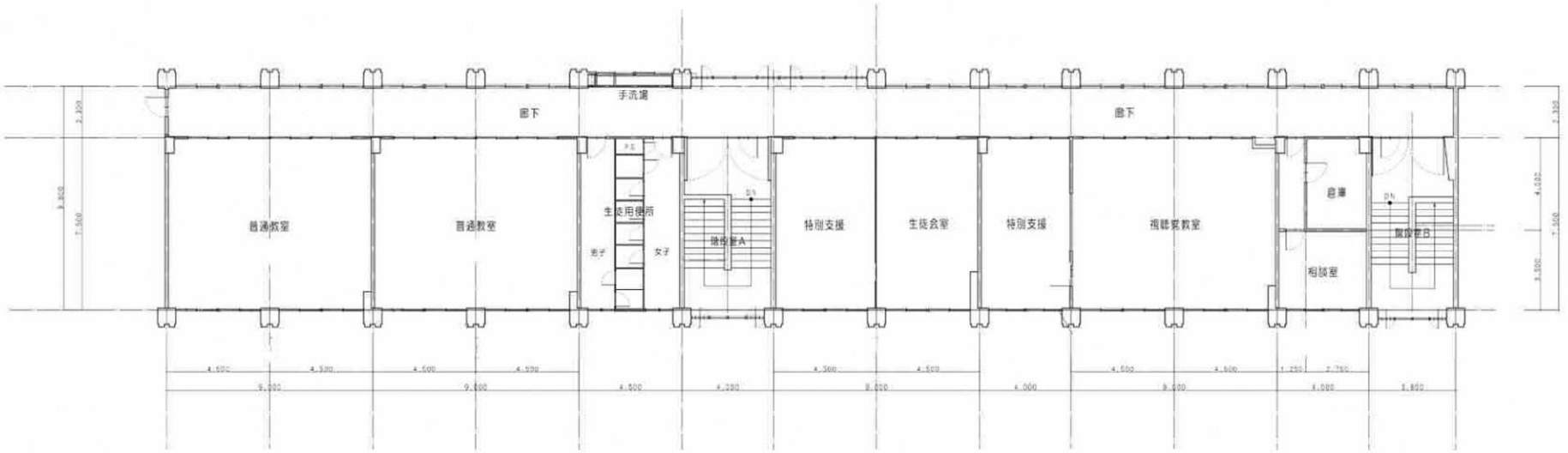


2階平面図



1階平面図

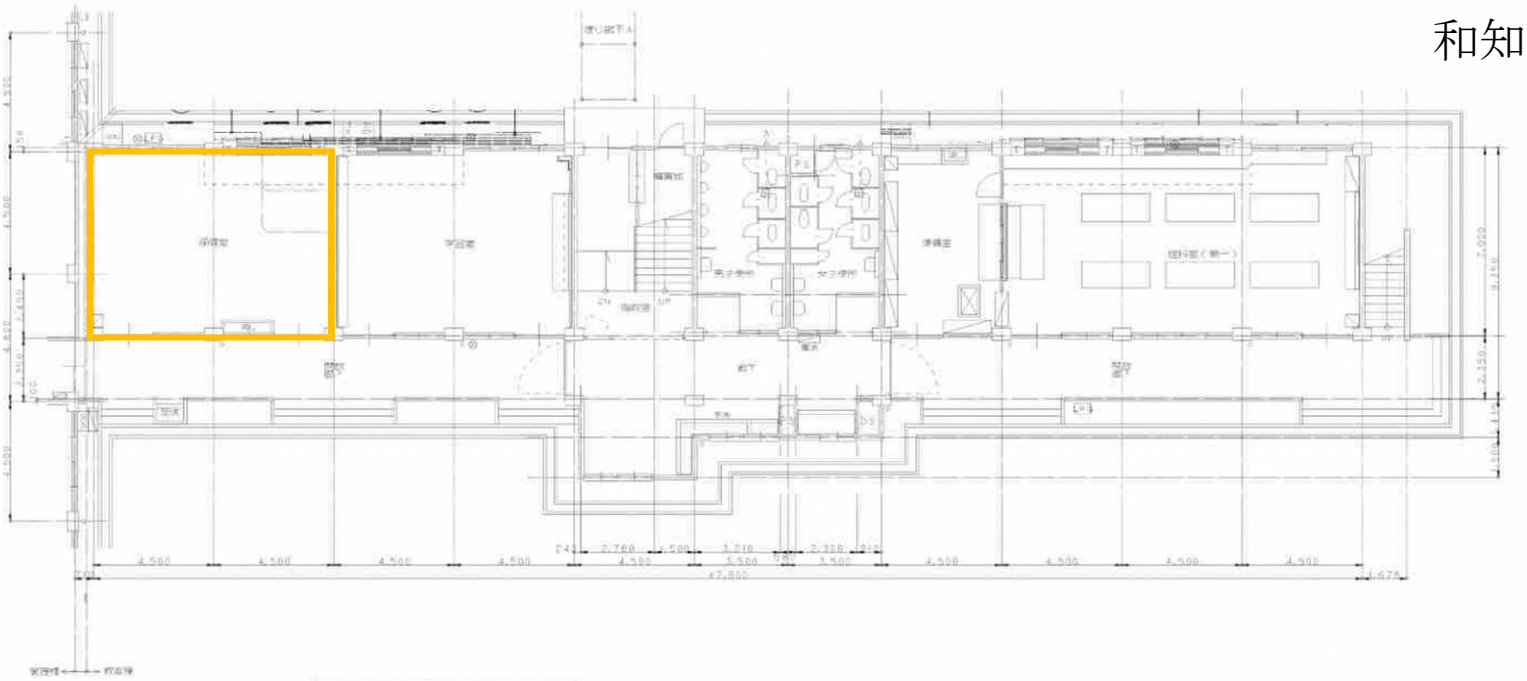
	瑞穂中学校	
	瑞穂中学校特別教室	2階平面図
DR.	CK.	NO. DATE

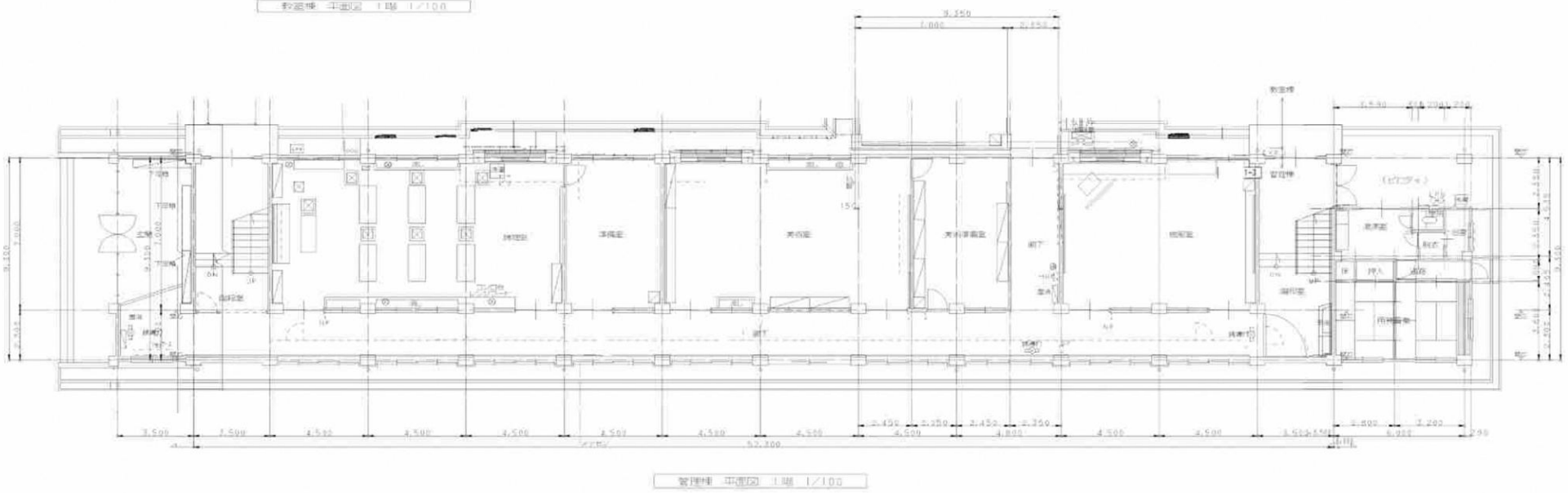

廊下
手洗場
廊下
普通教室
普通教室
生徒用便所
男子
女子
特別支援
生徒会室
特別支援
視聴覚教室
倉庫
相談室
EV
EV

3階平面図

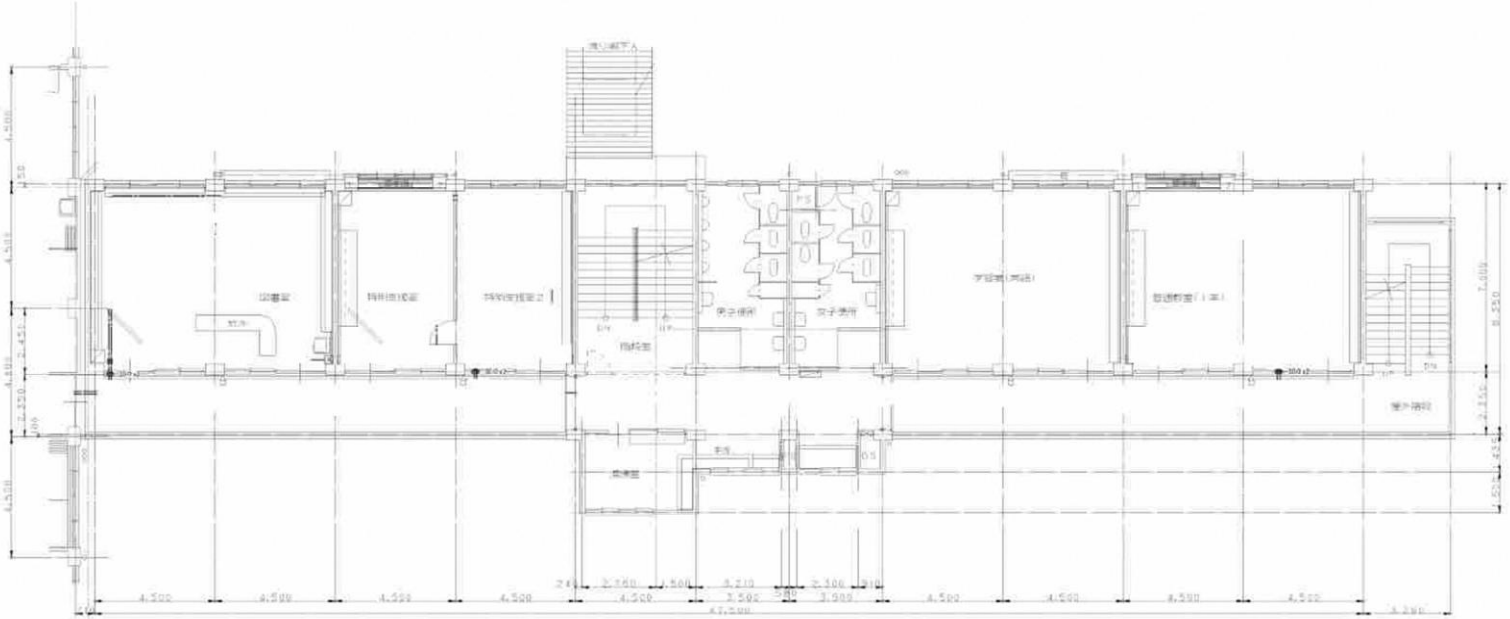
瑞穂中学校

和知中学校

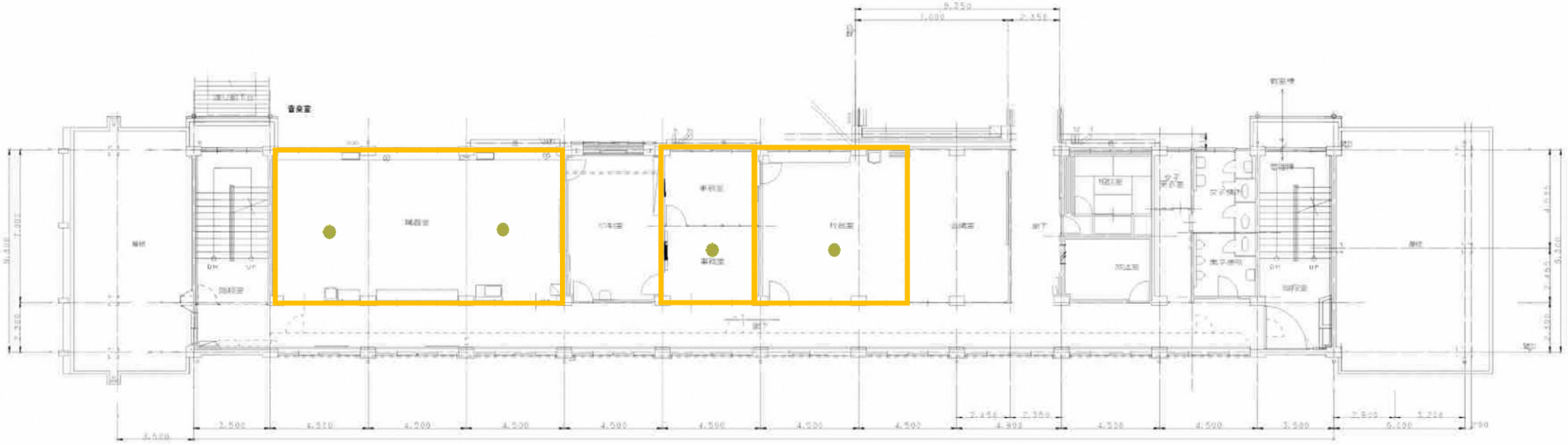




和知中学校

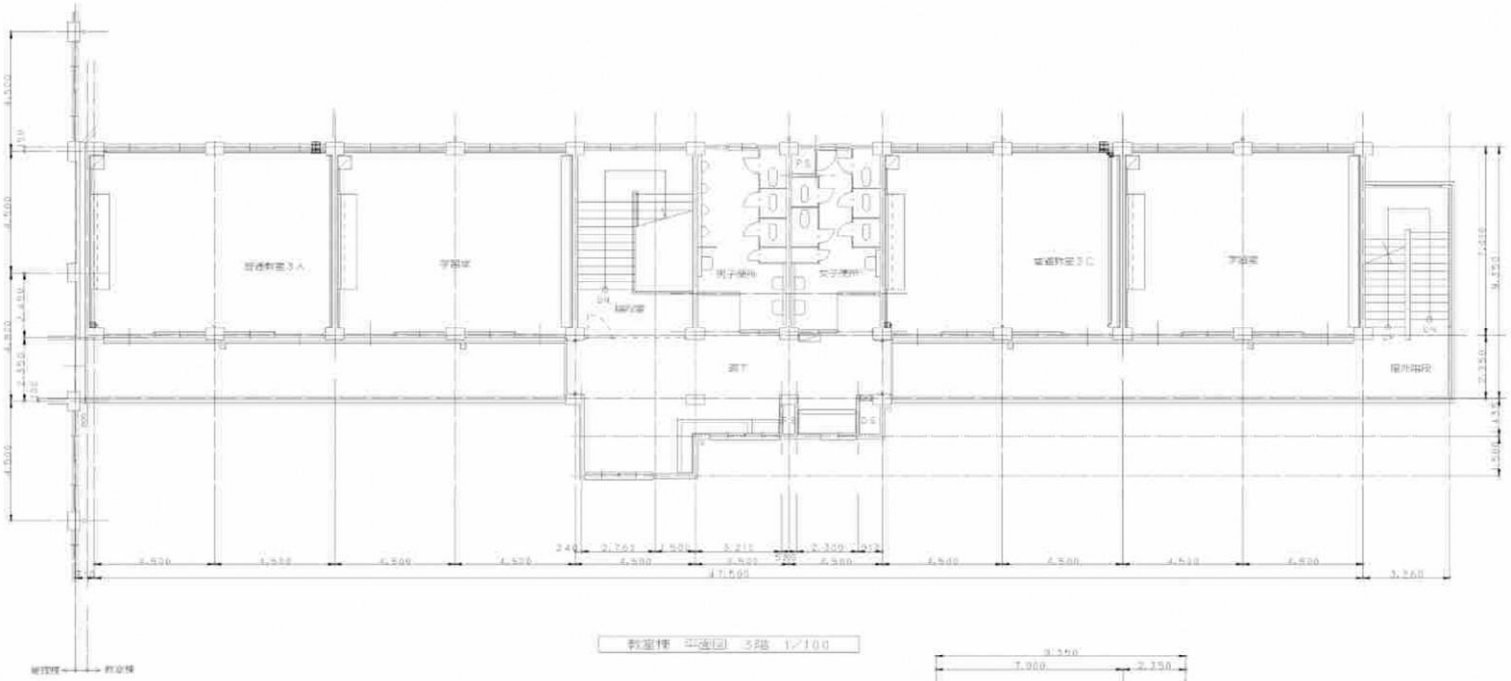


教室棟 平面図 2階 1/100

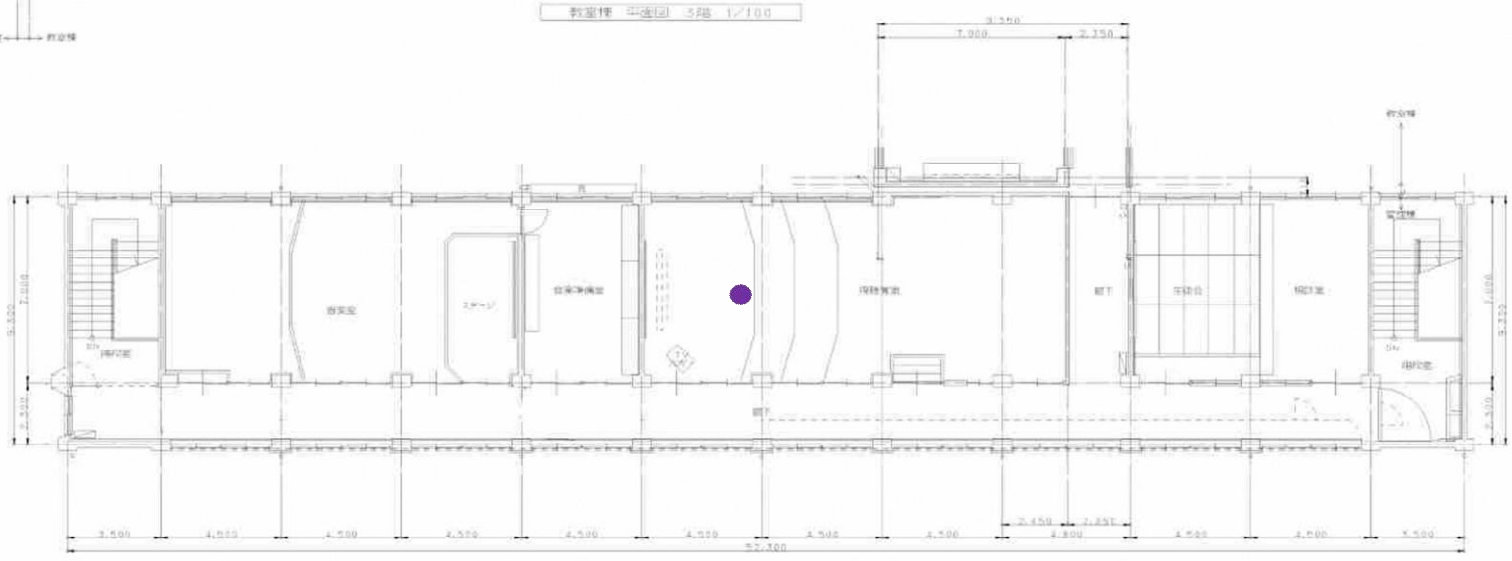


管理棟 平面図 2階 1/100

和知中学校



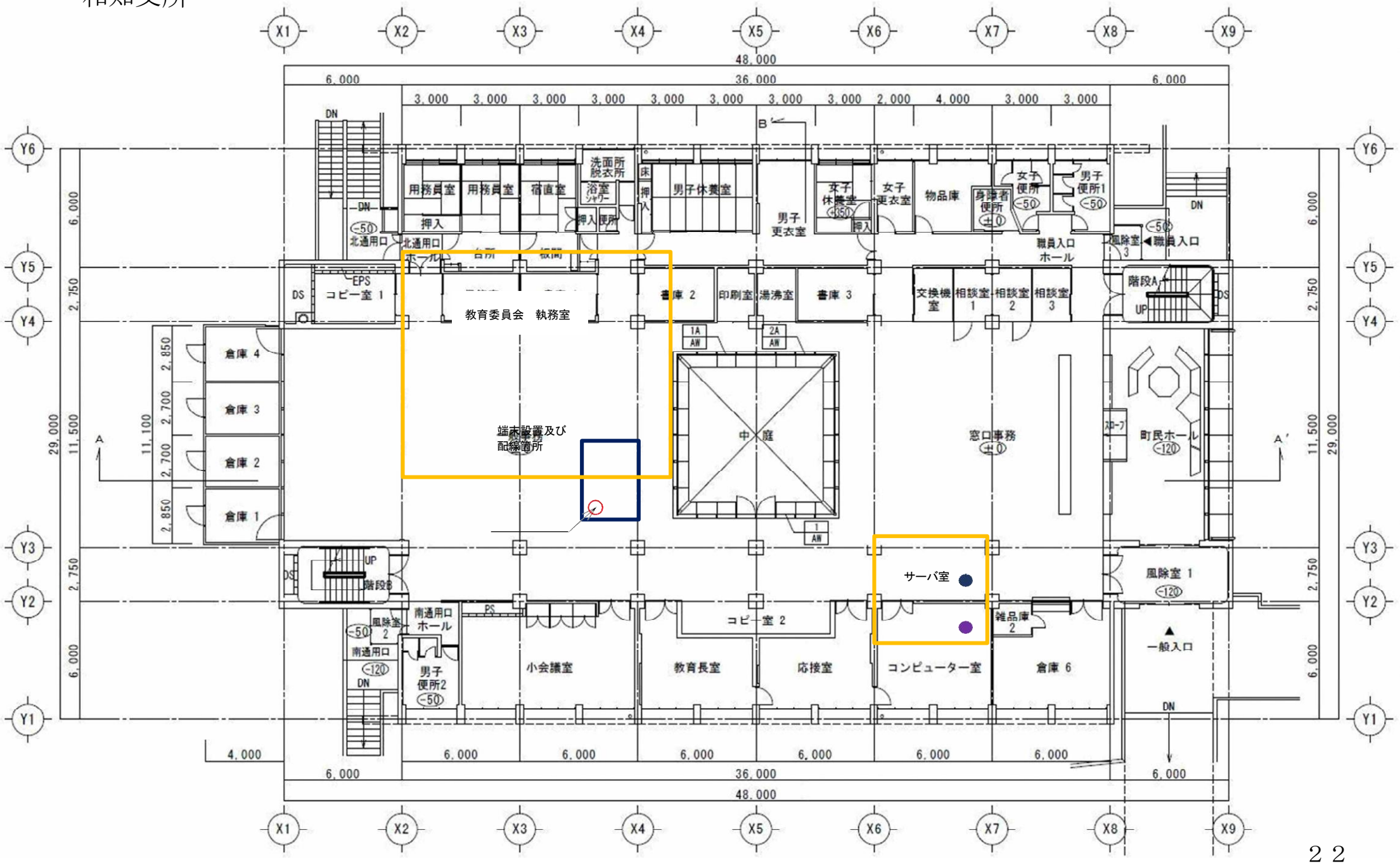
教室棟　平面図　3階　1/100



管理棟　平面図　3階　1/100

		和知中学校		
		1:100 SCALE		SCALE
		3階平面図		
DR.	DA.	NO.	DATE	

和知支所


教育委員会　執務室
端末設置及び
配線箇所
サーバ室
中　庭
窓口事務
町民ホール
コピー室 2
小会議室
教育長室
応接室
コンピューター室
倉庫 6
倉庫 4
倉庫 3
倉庫 2
倉庫 1
コピー室 1
書庫 2
印刷室
湯沸室
書庫 3
交換機室
相談室 1
相談室 2
相談室 3
男子休養室
女子休養室
女子更衣室
男子更衣室
物品庫
用務員室
用務員室
宿直室
洗面所
脱衣所
浴室
シャワー
男子便所2
風除室 1
風除室 2
風除室 3
雑品庫 2
一般入口
職員入口
ホール
北通用口
南通用口
階段A
階段B
EPS
PS
DS
DN
UP
押入
便所
48,000
36,000
6,000
29,000
11,500
11,100
2,850
2,700
2,750