校務系・学習系ネットワークの連携における導入・運用・活用に関するガイドブック

令和4年度

校務系・学習系ネットワークの連携に関する実証研究事業

文部科学省

◆目　次

第１章　はじめに

（1）　本書の位置付け

●背景

クラウド活用を前提としたGIGAスクール構想の推進により、児童生徒への１人１台端末の整備と高速大容量の通信ネットワークの整備が一体的に進められている中、中央教育審議会の「令和の日本型学校教育答申※1」は、ICTを「個別最適な学び」と「協働的な学び」の一体的な充実に必要不可欠なツールであるとともに、教師の長時間勤務を解消し、学校の働き方改革を実現する上でも極めて大きな役割を果たしうるものと位置付けました。

統合型校務支援システムは「教育のICT化に向けた環境整備５か年計画（2018～2022年度）」に基づき地方財政措置がなされ、整備率は年々上昇※2し校務の効率化に大きく寄与してきましたが、多くの自治体では校務支援システムを自前サーバに構築し、閉域網で稼働させており、校務用端末も職員室に固定されていることが多いのが現状です。これらの仕組みは従前の政府全体のセキュリティ対策を踏まえたものでしたが、１人１台端末の整備とクラウド活用を前提としたGIGAスクール時代の教育DXや働き方改革の流れに適合しなくなっています。

また、文部科学省は「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３年５月）」の改訂により、クラウドサービスの利活用を前提としたネットワーク構成として、校務系・学習系のネットワーク連携を目指す方向性を示しましたが、本格的に検討する教育委員会は一部に留まっています。※3

こうした中、校務系・学習系のネットワーク連携を促進するため、本「校務系・学習系ネットワークの連携に関する実証研究事業」において、技術的な対策等の実証を行い、その実現方法を本ガイドブックで整理しています。

●主な対象者

- ✓　ネットワーク・ICT環境の整備を担当されている方（教育委員会、私立学校担当者）
- ✓　各学校のDX担当の教職員

（2）　本書の構成

本書では、校務系・学習系ネットワークの連携について、３つの章に分けて解説します。

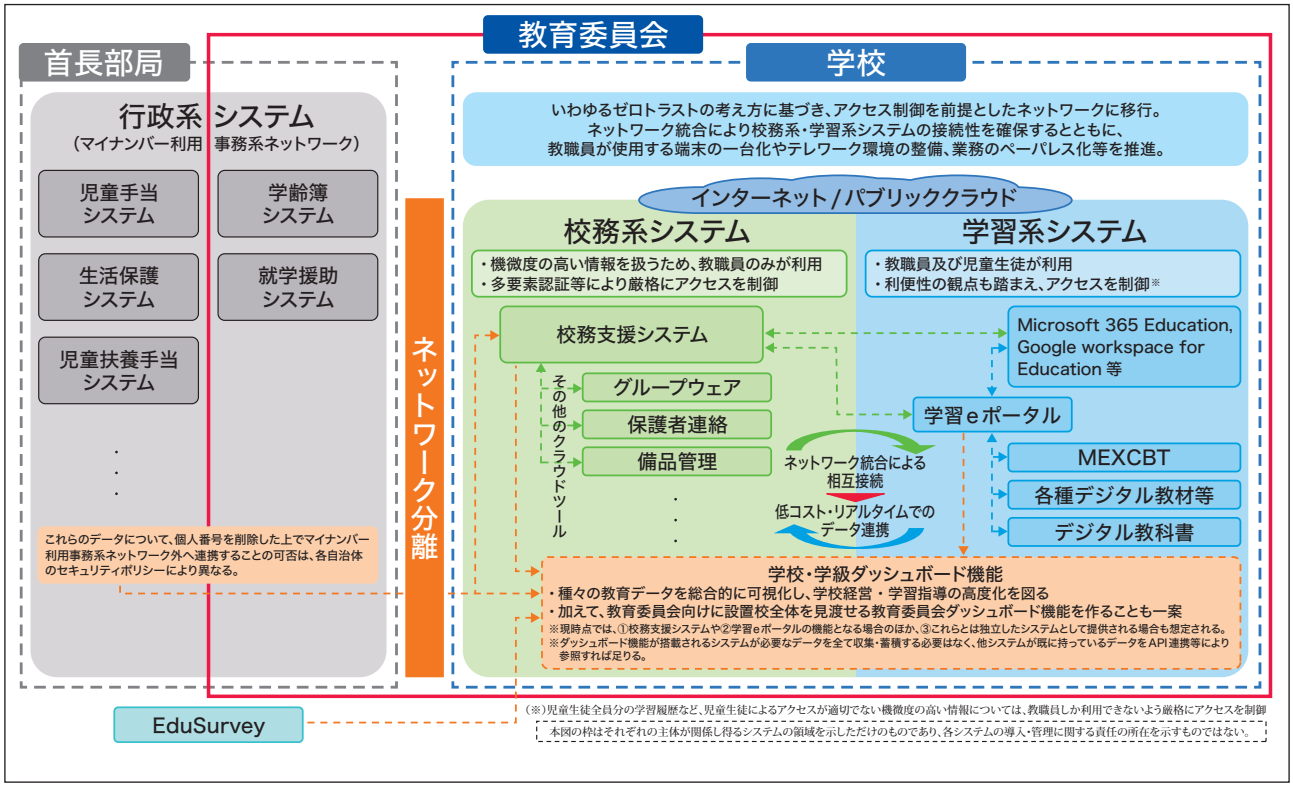
第１章：本書の位置づけや背景を解説します。
第２章：校務系・学習系ネットワークの連携により目指す方向性を、実証事業を通じて得た教育現場の声や専門家の意見を基に整理し解説します。
第３章：自治体の校務系・学習系ネットワーク連携の移行方法を技術的な観点から解説します。
第４章：校務系・学習系ネットワークを連携した後の活用例や効果、並びに先進的な取り組みを行っている自治体の事例を解説します。

（3）　本書で取り扱う範囲

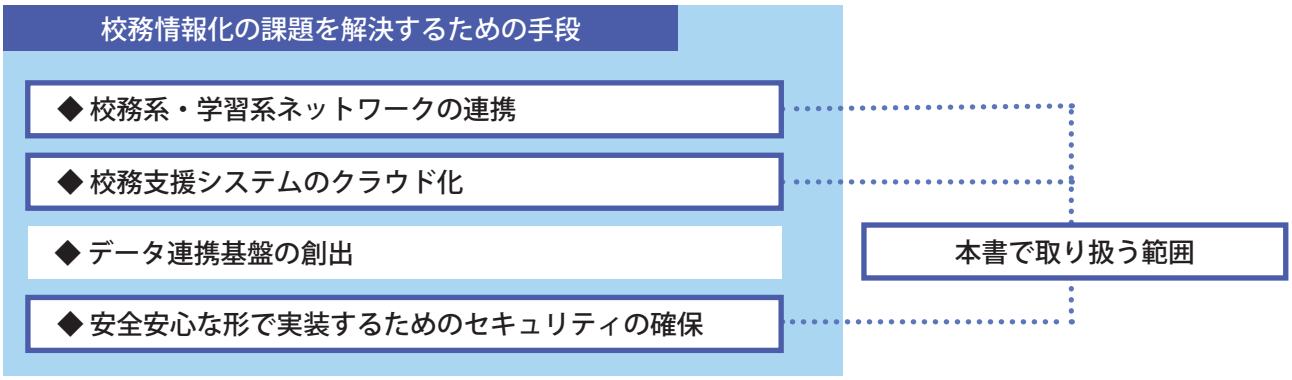
「GIGAスクール構想の下での校務の情報化の在り方に関する専門家会議」において、次世代の校務DXを支えるICT環境のイメージとして以下、図表1-1を図示しています。その上で、現状の校務情報化の課題を解決する手段として、以下図表1-2にて記載の通り、「校務系・学習系ネットワークの連携」「校務支援システムのクラウド化」「データ連携基盤の創出」「安全安心な形で実装するためのセキュリティの確保」の４点を挙げています※3。本書ではそのうち３点、「校務系・学習系ネットワークの連携」「校務支援システムのクラウド化」「安全安心な形で実装するためのセキュリティの確保」について、取り扱います。

※１：「令和の日本型学校教育」の構築を目指して～全ての子供たちの可能性を引き出す，個別最適な学びと，協働的な学びの実現～（答申）」（令和３年１月中央教育審議会）
※２：「令和４年３月１日時点での全国の公立学校における統合型校務支援システムの整備率：81.0%（出典：「学校における教育の情報化の実態等に関する調査」（令和４年１０月文部科学省）
※３：「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月文部科学省）
https://www.mext.go.jp/b_menu/shingi/chousa/shotou/175/mext_01385.html

図表 1-1　次世代の校務 DX を支える ICT 環境イメージ　※ 4



図表 1-2　校務情報化の課題を解決する手段（本書で取り扱う範囲）



コラム：アクセス認証型とネットワーク分離（境界防御）型の違い

教育情報セキュリティポリシーに関するガイドラインでは、校務支援システムの機密性を確保する方法として、アクセス認証型とネットワーク分離（境界防御）型の２つが想定されており、それぞれの差異を認識し、適切な対応を行うことが必要です。

アクセス認証型 (ゼロトラスト)	境界防御型（ネットワーク分離）
端末の認証やセキュリティ対策を充実させ、それぞれのリソースへのアクセス認証や通信の保護を徹 底することで、ネットワークによる制限を必要としな い手法。 接続するネットワークを限定しないため、リモートワーク等の働き方改革の推進に有効。	内部ネットワークと外部ネットワークを明確に切り離すことで、機密性を高める手法。 学校内からの通信のみに限定した場合に有効。

参考：教育情報セキュリティポリシーに関するガイドライン」ハンドブックより
https://www.mext.go.jp/content/20220303-mxt_shuukyo01-100003157_003.pdf

※ 4：「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 月文部科学省）
https://www.mext.go.jp/b_menu/shingi/chousa/shotou/175/mext_01385.html

第２章　校務系・学習系ネットワークの連携により目指す方向性

本章では、校務系・学習系ネットワークの連携により可能となる働き方と、その先にある目指す方向性について説明します。

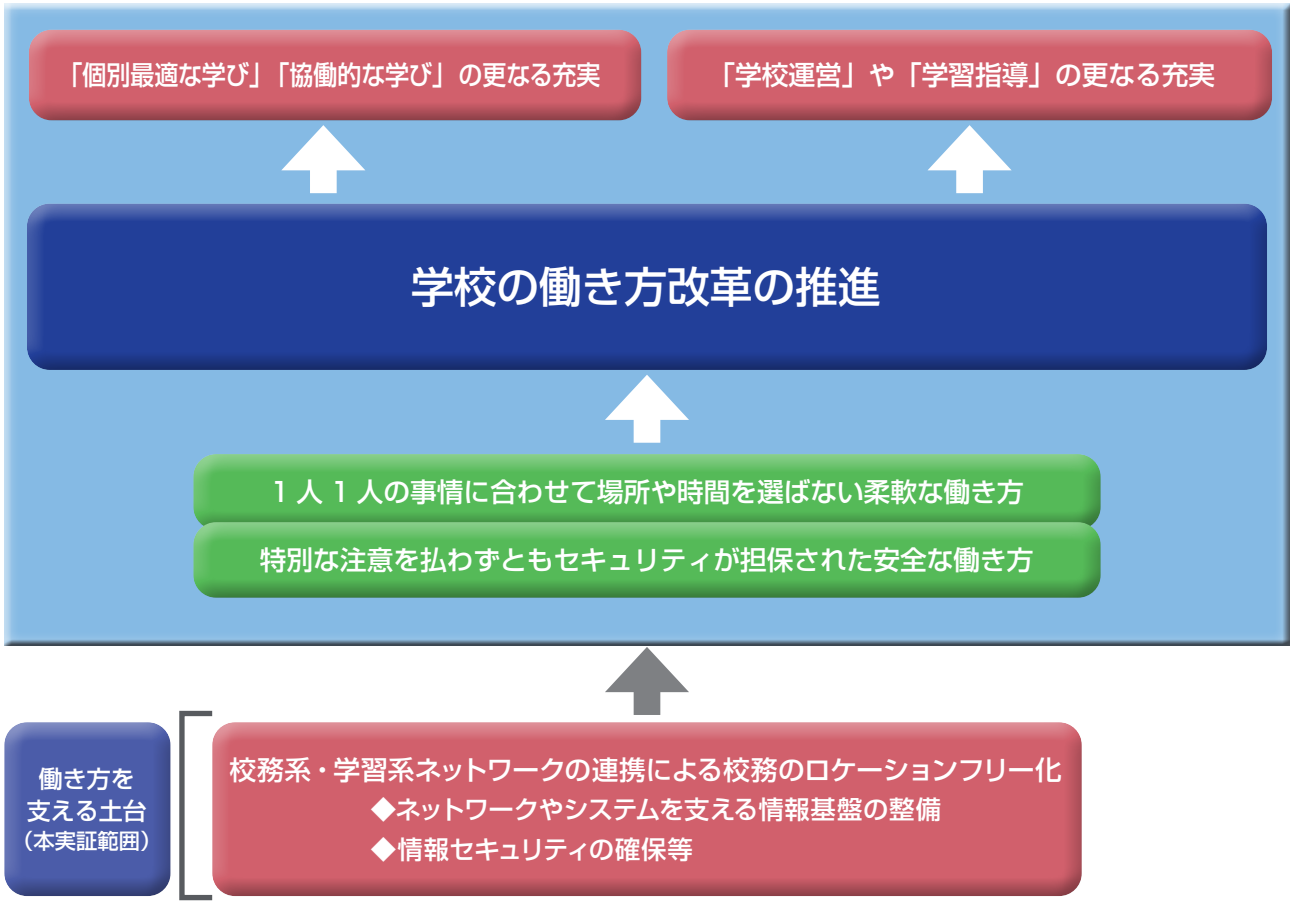
（1）　校務系・学習系ネットワークの連携より目指す方向性

校務系・学習系ネットワークの連携により、教育現場はどのような姿を実現することができるのでしょうか。実証事業を通じて、将来的に校務系・学習系ネットワークの連携により目指す方向性を整理しました。

教職員の働き方を支える土台として、校務系･学習系のネットワーク連携による校務のロケーションフリー化や情報セキュリティの確保等を行うことで、１人１人の事情に合わせて場所や時間を選ばない柔軟な働き方や、特別な注意を払わずともセキュリティが担保された安全な働き方が可能となります。それにより、学校の働き方改革が推進され、「個別最適な学び」「協働的な学び」や「学校運営」「学習指導」の更なる充実につながるものと考えられます。

具体的な環境整備にあたっては、「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～」で示された方向性を踏まえつつ、それぞれの自治体が目指す姿をコンセプトとして策定した上で、実現方法を検討することが必要となります。

図表 2-1　校務系・学習系ネットワークの連携により目指す方向性（イメージ）



（2） 校務系・学習系ネットワークの連携により可能となる働き方

本節では前節で述べた一人一人の事情に合わせて場所や時間を選ばない柔軟な働き方や、特別な注意を払わずともセキュリティが担保された安全な働き方について説明します。

図表 2-2　校務系・学習系ネットワークの連携により可能となる働き方

可能となる働き方

◆場所や時間を選ばない柔軟な働き方

校務系・学習系ネットワークの連携によって、場所や時間を選ばない柔軟な働き方が可能となります。例えば、従来は職員室でしか出来なかった業務を教室で行うことが出来るようになり、業務の効率化につながります。さらに、出張先での会議への参加や学校外からのリモートワーク等も可能となるなど、教職員の働き方の選択肢を増やすことにつながります。

◆セキュリティが担保された安全な働き方

校務系・学習系ネットワークの連携によって、特別な注意を払わずともセキュリティが担保された働き方が実現可能となります。

例えば、従来は情報を持ち出す際は、外部記憶媒体に情報をコピーしたり、紙媒体にメモを取る必要がありました。今後は必要なセキュリティ対策を実施した上でクラウドサービスを利用することで、データのやり取りをクラウド上で行うことができます。

また、従来のネットワーク分離型では、業務別に端末を複数台所有する必要がありましたが、校務系・学習系ネットワークの連携後は業務で使用する端末は一台で済み、端末を複数管理する手間や、校務用端末※５から指導者用端末※６へ必要な資料のデータを移行する手間が不要となります。

※５：校務系情報にアクセス可能な端末
※６：学習系情報にアクセス可能な端末で、教員のみが利用可能な端末。「学校における情報化の実態等に関する調査結果（令和３年度）」（文部科学省）では教育用コンピュータと記載

第３章　校務系・学習系のネットワーク連携に向けた移行方法

◆校務系・学習系ネットワーク連携に向けた移行ステップ

校務系・学習系ネットワークの連携に向けて、以下のステップで移行します。

＜連携に向けた移行ステップ＞

①校務系・学習系ネットワークの連携で実現したいコンセプトの策定（p7）
②システム構成や運用の現状確認（p7）
③校務系・学習系ネットワークの移行先システムの検討（p12）
④校務系・学習系ネットワークの連携により生じる業務の変化に対応するルールの検討（p26）
⑤校務系・学習系ネットワークの連携に必要なシステム移行作業の検討（p27）
⑥移行後の円滑な利用に向けて必要な教育・研修の検討（p29）

（1）　校務系・学習系ネットワークの連携で実現したいコンセプトの策定

◆校務系・学習系ネットワークの連携で実現したいコンセプトの策定

2-（2）「校務系･学習系ネットワークの連携により可能となる働き方」で述べたとおり､校務系･学習系ネットワークの連携によって可能となる働き方は様々です。そのため､校務系･学習系ネットワークの連携によって目指す働き方をコンセプトとして策定することが大切です。

コンセプトは、現状の働き方を確認した上で、必要に応じて自分たちの自治体が目指す方向性にあった先進自治体の働き方や、本実証のフィールドである武蔵村山市の活用例を参考にしながら策定し、校務系・学習系ネットワークの連携に着手しましょう。

（2）　現状のシステム構成や運用の確認

校務系・学習系ネットワークの連携を検討する上で、現状のシステム構成や運用を正しく把握しておくことが大切です。「教育情報システム」「ネットワーク」「端末」「セキュリティ」「運用・ルール」という５つの項目について、現状の確認を行います。

（2）- 1　教育情報システム

◆教育情報システムの現状確認

校務系・学習系ネットワークの連携にあたり、データの重要性やデータ量により移行先や構成するシステムが決定されるため、図表 3-1 の確認項目を参考に教育情報システムの現状の確認を行います。その際、校務系システムに関する情報だけでなく、学習系システムに関する情報についても忘れずに確認しましょう。

図表 3-1　教育情報システムの確認項目例

確認項目	校務系システム※7		学習系システム※8	
	校務支援システム（記載例）	…	学習ドリル（記載例）	…
データの重要性 ※9	• 重要性分類Ⅱ • 重要性分類Ⅲ	…	• 重要性分類Ⅱ • 重要性分類Ⅲ	…
データ量	1TB	…	500GB	…
利用場所	職員室からのみ	…	校内 / 校外	…
利用者数増加見込み	1 年で± 10 人	…	1 年で± 30 人	…
利用時のログイン方法と認証先	• 認証方法：ログイン画面で ID/パスワードを入力 • 認証先：校務支援システムの認証サーバ	…	• 認証方法：ショートカットクリックで利用可能 • 認証先：学習系認証サーバ	…
バックアップの目的	目的：ランサムウェア感染時の業務復旧	…	ー	
教育情報システムの更改時期	R7 年 3 月	…	ー	…

※7：校務系ネットワーク、校務系サーバ及び校務用端末から構成される校務系情報を取り扱うシステム及び、校務系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
※8：学習系ネットワーク、学習系サーバ、学習者用端末及び指導者用端末から構成される学習系情報を取り扱うシステム及び、学習系情報を扱う上で、適切なアクセス権が設定された領域で利用されるシステム
※9：同システム内に異なる重要性分類に属するデータを含む場合は、それぞれのデータの重要性を確認する

◆データの重要性分類について

教育情報システムの移行先は、利用している教育情報システムに含まれるデータの「重要性分類」に基づいて検討します。以下の図表 3-2 を参考とし、具体的な分類は個々の自治体において個別に実施する必要があります。

また、同システム内に異なる重要性分類に属するデータを含む場合は、それぞれのデータの重要性を把握しましょう。

図表 3-2　データの重要性分類例

● 文部科学省発行「GIGA スクール構想の下での校務 DX について」より

重要性分類 （流出･改ざん･棄損等による影響で分類）	校務系情報 （教職員のみアクセス）	学習系情報 （教職員及び児童生徒からのアクセス）	公開系情報 （不特定多数からのアクセス）
Ⅰ 教職員及び児童生徒の生命･財産･プライバシー等に重大な影響を及ぼす	○教職員の人事情報 ○入学者選抜問題 ○教育情報システム仕様書		
Ⅱ 学校運営に重大な影響を及ぼす	○学籍関係（卒業証書） ○成績関係（評定一覧） ○指導関係（事故報告） ○進路関係（卒業生進路先一覧） ○健康関係（健康診断票） ○児童生徒個人情報 ○教職員個人情報 ○機密性の高い情報（ID/PW管理台帳等）	○児童生徒の認証情報（ID/PW管理台帳等）	
Ⅲ 学校運営に軽微な影響を及ぼす	○児童生徒の氏名（出席簿 / 座席表等） ○学校運営関係（卒業アルバム）	○学校運営関係（授業用教材） ○児童生徒学習系情報（学習記録 / レポート等）	個々の学習履歴については重要性Ⅲとしつつ、児童生徒全員分の学習記録などは重要性Ⅱとして取り扱うことが考えられる。
Ⅳ ほとんど影響がない			○学校運営 / 活用関係（学校紹介パンフレット･学校行事写真等(データ含む)）

イメージ図引用元：文部科学省（2023 年 3 月発行）
GIGA スクール構想の下での校務 DX について
https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf

（2）- 2　ネットワーク

◆ネットワークの現状確認

校務系・学習系ネットワークの連携に向けて、図表 3-3 の確認項目を参考に、現状のネットワーク構成を確認します。その際、校務系のネットワークだけでなく、学習系のネットワークについても確認しましょう。

既存のネットワークを導入した時期等の違いにより、学校ごとに構成が異なる場合がありますので、注意してください。また、GIGA スクール構想による環境整備において、学習系のネットワークを学校からインターネットに直接接続する構成としている場合がありますので、端末から各システムへの通信方法を確認しましょう。

図表 3-3　現状のネットワーク確認項目例

確認項目	確認内容
ネットワーク分離型	• 二層分離※ 10（校務系ネットワークの外部接続有 / 無） • 三層分離※ 11
ネットワーク機器	• ファイアウォール • ルーター • スイッチ • アクセスポイント
ネットワーク機器のスペック	• 処理性能 • 帯域 • セッション数
システムへの通信方法	• 集約して接続（集約する場所についても確認すること） • 学校から直接接続
ネットワーク機器の更改時期	• 校務系ネットワーク機器の更改時期 • 学習系ネットワーク機器の更改時期
ネットワーク機器の冗長化	• ネットワーク機器の冗長化の有無 • ネットワーク機器の冗長化の方法

（2）- 3　端末

◆端末の現状確認

校務系・学習系ネットワークの連携に向けて、図表 3-4 の確認項目を参考に現状の端末の OS やスペック等を確認します。その際、校務用端末だけでなく全ての端末についても確認しましょう。

また学校が独自に端末を購入し利用している場合がありますので、端末の情報を確認する際は各学校にも確認を行いましょう。

図表 3-4　現状の端末確認項目例

確認項目	確認内容
端末の種類	• 利用端末のメーカー • OS の種類 / バージョン • ライセンス形態
機能・スペック	• CPU/ メモリ • HDD • 画面サイズ • 重量 • カメラや指紋デバイスの有無 • ポートの種類と数 • 有線 LAN コネクタ / 無線 LAN コネクタの有無 • 周辺機器 (モニタ／キーボード等)
LAN 接続方法	• 有線 LAN/ 無線 LAN
端末の導入時期	• 端末の導入時期
端末の管理方法	• MDM の利用有無

※ 10：「校務系ネットワーク / 校務外部接続系ネットワーク」と「学習系ネットワーク」ないしは、「校務系ネットワーク」と「校務外部接続系ネットワーク / 学習系ネットワーク」のいずれかの二層に分離している構成
※ 11：インターネットとは分離された閉域網に重要性の高い情報を扱うシステムが配置されている「校務系ネットワーク」、教職員が校務用端末からインターネット接続可能な「校務外部接続系ネットワーク」、児童生徒の学習でインターネット接続をする「学習系ネットワーク」の三層に分離している構成

（2）- 4　セキュリティ

校務系・学習系ネットワークの連携により目指す働き方を実現するため、ネットワーク基盤を従来のネットワーク分離型から、必要なセキュリティ対策が施されたアクセス認証型※12へと移行します。移行に向けて、教職員の業務とセキュリティ対策の確認を行います。

◆教職員の業務の確認

セキュリティ対策を考える上では、想定されるセキュリティ上の脅威を整理することも必要となります。そして、セキュリティ上の脅威は業務内容によって変わるため、図表 3-5 の確認観点や確認項目例を参考に、データを利用する教職員の業務を確認しましょう。

◆セキュリティ対策の確認

業務の確認と併せて、現在のシステムにおけるセキュリティ対策の確認を行います。その際、校務系システムと学習系システムの両方のセキュリティ対策を確認しましょう。

また、自治体として保有している、学校でも利用可能なセキュリティライセンス等についても漏れがないように確認しましょう。

図表 3-5　データを利用する教職員の業務の確認例 ※13

確認観点	教職員の業務例	業務のやり方（例）
・いつ／どこで／誰が／どのような手段でデータを入手、作成したか ・どこで／誰が／どのくらいの期間／どのような手段でデータを活用、管理しているか ・いつ／どこで／誰が／どのような手段でデータを廃棄したか	生徒の出欠管理	・毎朝担任の先生が生徒の出欠を確認し、その情報を校務支援システムに登録する。
	試験問題の作成 / 試験の実施	・校務用端末に導入されている文書作成ツールを利用して試験問題を作成し、試験を実施する。採点結果を校務支援システムに登録する。
	通知表の作成	・校務支援システムを利用し、通知表を作成する。通知表の内容に影響する出欠情報や成績情報は校務支援システム内で連携される。
	生徒指導の内容管理	・校務用端末に導入されている表計算ツールで生徒指導情報を管理する。
	職員会議用の資料作成	・毎月１回程度、今後の行事やイベントについて各担当職員が校務用端末で作成した資料を持ち寄り、データまたは紙で共有する。重要な書類については会議後、ファイリングして保管する。
	各種配布物の作成	・学級だよりや保護者会の出席票などの配布書類は校務用端末で作成し、印刷して配布する。作成したデータは個人のデスクトップで管理する。
	授業で利用する資料の作成	・校務用端末に導入されている文書作成ツールを利用して、放課後や朝の時間に授業用の資料を作成する。 ・作成した資料は校務用ストレージ、校務用端末のデスクトップに保管する。
	指導者用端末を投影する授業の実施	・校務用端末で作成した資料を指導者用端末に移行し、指導者用端末を投影して授業を進める。 ・授業に関連する画像や情報をインターネットで検索し、生徒に共有する。
	相互コミュニケーションを取り入れた授業の実施	・教師の授業に対する感想や意見について、指導者用端末のチャットツールにてコミュニケーションを行う。

※12：端末の認証やセキュリティ対策を充実させ、情報・データへのアクセス認証や通信の保護を徹底することで、ネットワークによる分離を必要としないモデルのこと
※13：武蔵村山市の教職員にヒアリングした内容より作成

（2）- 5　運用・ルール

◆運用の確認

校務系・学習系ネットワークの連携後、どのようなシステム運用とするかを検討するため、現状のシステム運用における業務や体制を確認します。

◆ルールの確認

校務系・学習系ネットワークを連携することにより、学校外から校務系システムへのアクセスが可能となるなど、これまでと働き方が変わります。こうした働き方の変化により既存のルールに抵触する可能性が生じるため、自治体や教育委員会が定める情報セキュリティポリシーや就業規則、その他各自治体で定められたルールを再確認することが大切です。また、教職員がそれらのルールをどの程度理解しているかについても確認が必要です。

図表 3-6 を参考に、現状のシステム運用やルールに関する項目を確認しましょう。

図表 3-6　現状の運用・ルール確認項目例

確認項目	確認内容
運用業務	• ユーザ管理業務（転出入時の ID 作成／変更／削除） • 端末管理業務（新規購入端末の設定作業／端末の故障対応業務） • 運用対処しているセキュリティ対策
運用体制	• 教職員 / 教育委員会 / 情報システム部門 / 外部委託ベンダー
ルール	• 情報セキュリティポリシー 例）端末の持ち運びに関するルール ※ 14 「職員等は、本市のモバイル端末を外部に持ち出す場合には、管理責任者の許可を得なければならない」 • 就業規則 例）リモートワークに関するルール ※ 15 「通常の勤務場所以外での勤務時間については、勤務時間が算出し難い場合には、正規の勤務時間勤務したものとみなす」 • その他学校や自治体で定められたルールなど

（3）　校務系・学習系ネットワークの移行先システムの検討

校務系･学習系ネットワークの連携に向け､「教育情報システム」「ネットワーク」「端末」「セキュリティ」「運用」の 5 つの項目について、（2）現状のシステム構成や運用の確認で確認した情報を基に、移行先のシステムの検討方法を示します。

（3）- 1　教育情報システム

教育情報システムの現状の確認情報を基に、それぞれのデータをどの環境に移行するかを検討します。図表 3-7 では例として 4 種類の移行先環境の特徴を記載していますが、この 4 種類に限らず、広く移行先の環境を検討することが大切です。

また校務系システムは将来的なデータ連携・利活用を踏まえて、学習系システムと柔軟に連携することも考慮し、検討しましょう。

※ 14：参考：大阪府吹田市「吹田市情報セキュリティポリシー（令和 4 年 10 月 12 日改正）」
https://www.city.suita.osaka.jp/_res/projects/default_project/_page_/001/007/890/security_policy.pdf（2023 年 3 月 7 日時点）
※ 15：参考：東京都「学校職員の勤務時間、休日、休暇等に関する条例及び同条例施行規則の解釈及び運用について（令和 4 年 11 月 1 日施行）」
https://www.kyoiku.metro.tokyo.lg.jp/static/reiki_int/reiki_honbun/g170RG00002643.html （2023 年 3 月 7 日時点）

図表 3-7　移行先環境ごとの特徴サマリ

<table>
<tr><th colspan="2">環境の特徴</th><th>パブリッククラウド
(SaaS ※ 16)</th><th>パブリッククラウド
(IaaS ※ 17)</th><th>プライベート
クラウド
(ホスティング型※ 18)</th><th>オンプレミス /
プライベートクラウド
(ハウジング型) ※ 19</th></tr>
<tr><td>①データの重要性</td><td>≒ セキュリティ</td><td>提供サービスによる</td><td>提供サービスを利用
※ 20</td><td colspan="2">環境整備が必要</td></tr>
<tr><td rowspan="2">②データ量</td><td>≒ イニシャルコスト</td><td colspan="3">低</td><td>高 ※ 21</td></tr>
<tr><td>≒ ランニングコスト</td><td colspan="3">高※ 22</td><td rowspan="2">低 / 中 ※ 25</td></tr>
<tr><td></td><td></td><td>定額 ※ 23</td><td>変動 ※ 24</td><td>定額 ※ 23</td></tr>
<tr><td>③利用場所</td><td>≒ ネットワーク</td><td colspan="2">オープン ※ 26
（インターネット接続）</td><td colspan="2">閉域 ※ 27（インターネット非接続）</td></tr>
<tr><td>④利用者数
増加見込み</td><td>≒ 拡張性</td><td>プラン変更 ※ 28</td><td>自動拡張</td><td>プラン変更 ※ 28</td><td>機器増強が
必要</td></tr>
<tr><td>⑤バックアップ</td><td>≒ データの保全性</td><td>提供サービスに
含まれる ※ 29</td><td>提供サービスを利用</td><td colspan="2">環境整備が必要</td></tr>
</table>

※ 16：Software as a Service の略称。クラウド事業者がアプリケーションプログラムを持つ機能を提供するサービスのこと
※ 17：Infrastructure as a Service の略称。クラウド事業者がサーバやストレージ、ネットワークなどのハードウェアが提供する機能を仮想環境として提供するサービスのこと
※ 18：クラウド事業者からクラウド環境を借り受けて外部からのアクセスを遮断し、自組織専用として使用するようにしたもの
※ 19：サーバやネットワーク機器、ソフトウェアなどをデータセンターに設置して、使用者自身で運用する利用体系のこと
※ 20：セキュリティ機能が不足している場合はオプションサービスや別途環境の整備が必要
※ 21：オンプレミス / ハウジングの場合は、利用者数、データ量に応じたシステム利用料が発生
※ 22：パブリッククラウド / プライベートクラウド（ホスティング型）の場合は、利用者数やデータ量に応じたシステム利用料が発生する
※ 23：クラウド事業者や提供サービスによって異なる
※ 24：料金体系は基本的に従量課金だがクラウド事業者や提供サービスによって異なる
※ 25：プライベートクラウド（ハウジング型）の場合、データセンター利用料が発生
※ 26：プラン変更により閉域接続とすることも可能
※ 27：インターネット経由で接続するためには環境整備が必要
※ 28：クラウド事業者や提供サービスによって異なる
※ 29：バックアップデータの保証の責任範囲はクラウド事業者によって異なる

（3）- 2　ネットワーク

校務系・学習系ネットワークの連携に向けて、学校外のネットワークと学校内のネットワークのそれぞれについて検討します。

◆学校外のネットワークの検討

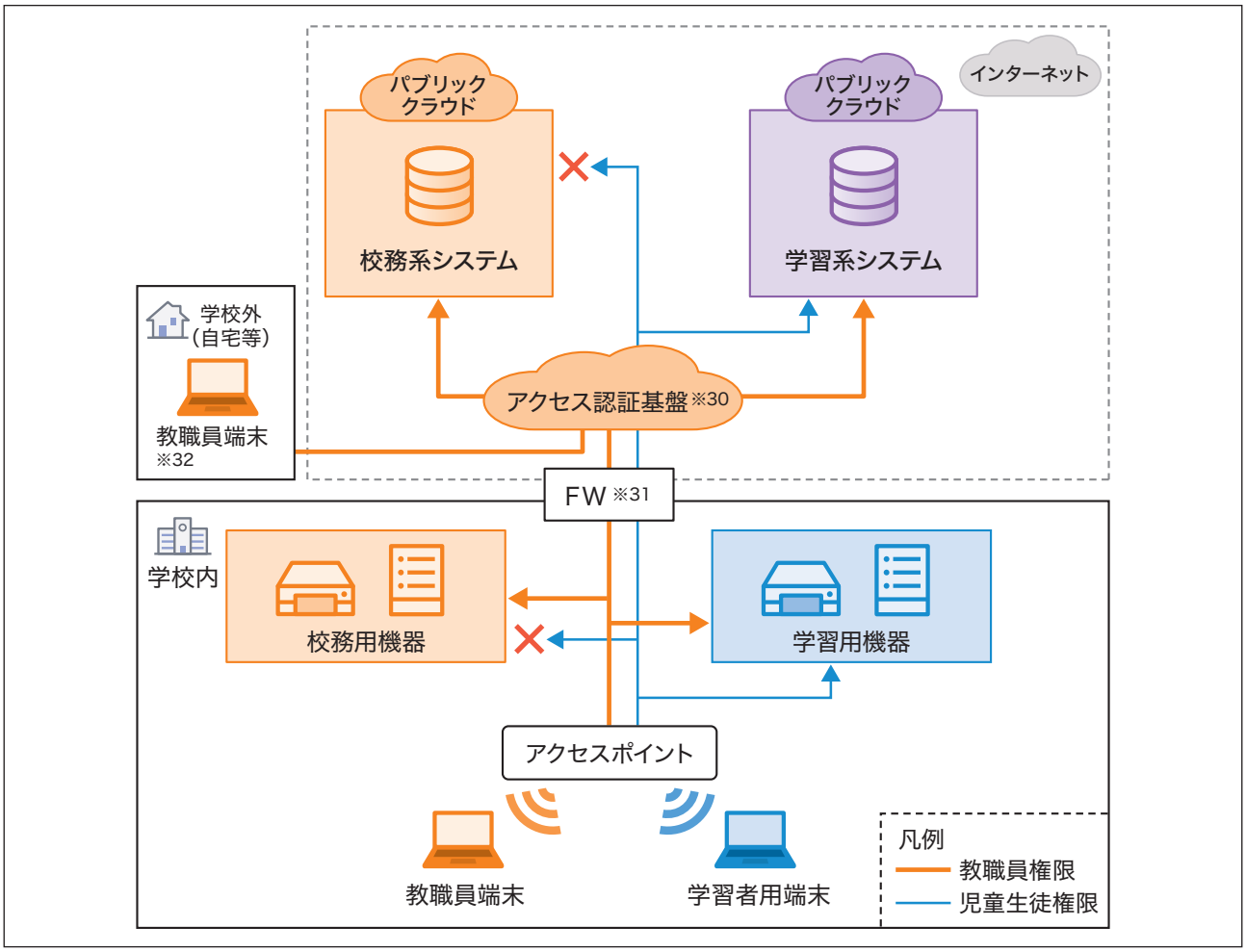
学校外のネットワークについては、場所を問わず教職員の端末からパブリッククラウド上の校務系・学習系システムの双方にアクセスできるネットワーク構成を検討します。なお、パブリッククラウド上のシステムにアクセスする際は、必ずアクセス認証基盤※ 18 に接続し、適切な認証が行われるようなネットワーク構成とすることが大切です。

◆学校内のネットワークの検討

学校内のネットワークについては、GIGA スクール構想にて整備した LAN 環境を利用することなどにより、校内のどこからでも校務系システムにアクセスできる構成を検討します。

ただし、学習者用端末から校務用機器および校務用端末にアクセスできない構成にする必要があります。一例として、校務系と学習系のネットワークを論理的に分けることで、生徒による校務用機器への不正アクセスや学習者用端末がランサムウェア等のマルウェアに感染した場合の校務系システムへの感染拡大を防ぐ方法が挙げられます。

図表 3-8　校務系・学習系システムの双方にアクセス可能なネットワーク構成イメージ



※ 30：情報・データへのアクセス認証の適正さについて、常に確認できるセキュリティ機能を備えた認証基盤
※ 31：ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと
※ 32：校務系・学習系ネットワークの連携を目指すにあたり、指導者用端末と校務用端末を 1 台に統合した端末の呼称

（3）- 3　端末

◆環境移行後、教職員が利用する端末の検討

1 台の端末から、場所にとらわれず、校務系システム・学習系システムの双方にアクセス可能とする観点から、利用する端末を選定します。

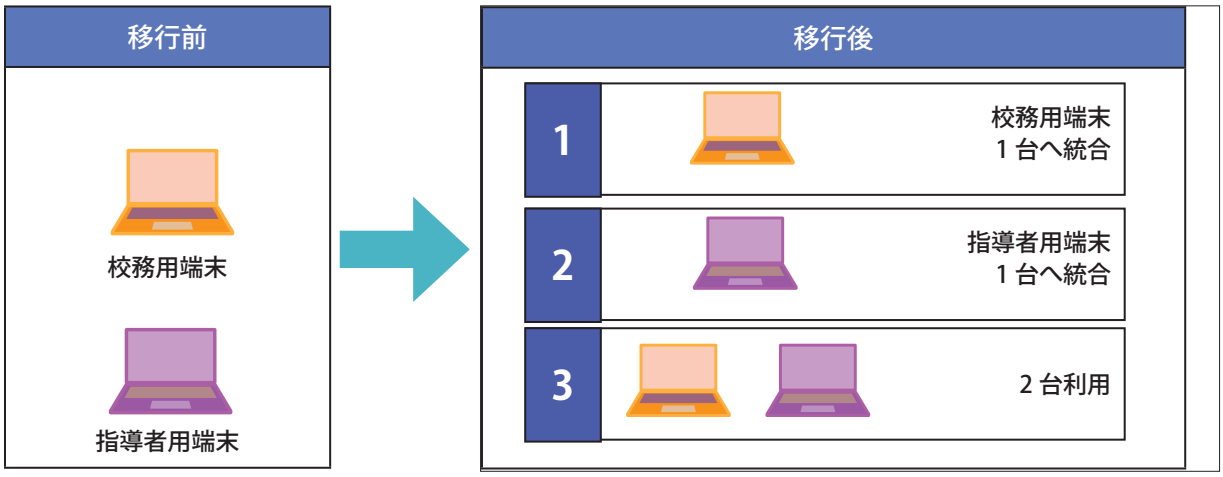
利用する端末は新規で調達することも考えられますが、既存端末をそのまま利用することも考えられます。端末の移行先の検討パターンとしては図表 3-9 の 3 パターンがあります。選定の際は、図表 3-10 を参考に、教職員の利便性やコストなどを総合的に勘案して決定しましょう。

また、教職員の利便性を考慮すると端末は 1 台とすることが望ましいですが、過渡期では校務用端末と指導者用端末の 2 台の端末を併用し、端末の更改時期に合わせて段階的に 1 台化することもあり得ます。

図表 3-9　端末の選定観点例

選定観点	項　　目
教職員の利便性	• 授業への影響はどの程度か （教材作成の容易さ / 学習者用端末との親和性など） • 持ち運びを想定したサイズや重量であるか
端末の導入時期	• 端末導入の時期はいつか
端末のスペック	• 利用するシステムに対応した OS / スペックであるか • 導入するセキュリティ製品の推奨スペックを満たしているか

図表 3-10　端末移行先の検討パターン※ 33



（3）- 4　セキュリティ

校務系・学習系ネットワークの連携に向けて、「何を」「何から」「どのように」守るかという観点でセキュリティ対策を検討します。※ 34

「何を」に該当するのが（2）-1 で確認した「教育情報システムに含まれるデータ」であるため、本節では「何から」に該当する「業務で発生し得るセキュリティ脅威」と、「どのように」に該当する「セキュリティ対策を実現する技術（以下、要素技術という）」の検討における考え方を説明します。考え方のステップは以下のとおりです。

◆考え方のステップ
ステップ①：「何から」ネットワーク分離型とアクセス認証型の違いによるセキュリティ脅威の変化の理解
ステップ②：「どのように」アクセス認証型におけるセキュリティ対策と対応する要素技術の把握
ステップ③：「どのように」要素技術の導入パターンとその特徴の理解

※ 33：ここでは既存端末の例として「校務用端末」と GIGA スクール構想で整備した「指導者用端末」を示す
※ 34：文部科学省（2023 年 3 月発行）GIGA スクール構想の下での校務 DX について
https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf　p15

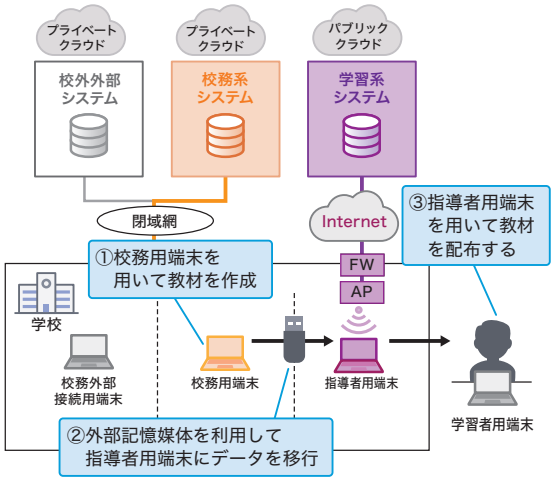
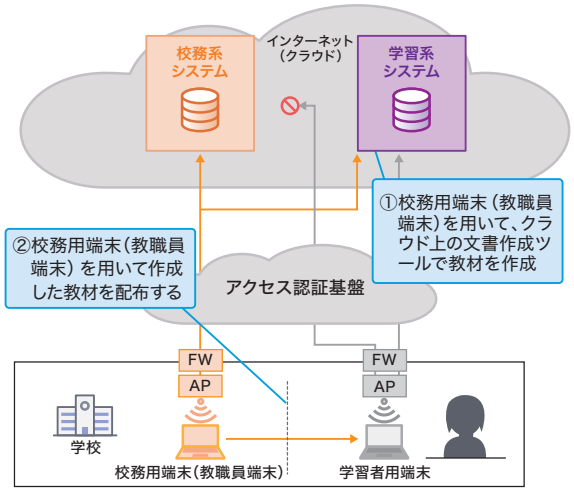
ステップ①「何から」 ネットワーク分離型とアクセス認証型の違いによるセキュリティ脅威とセキュリティ対策の変化

ネットワーク分離型の場合は校務系システムにアクセスできる場所が限定されていましたが、アクセス認証型の場合はインターネットに接続できる環境であれば場所を選ばず、校務系システムへのアクセスが可能となります。

アクセス認証型とネットワーク分離型で発生し得るセキュリティ脅威と取り得るセキュリティ対策が異なることを理解した上で、アクセス認証型で取るべきセキュリティ対策を考えることが必要です。図表 3-11 にその違いの一例を記載しています。

図表 3-11　ネットワーク分離型とアクセス認証型の違いによるセキュリティ脅威とセキュリティ対策の変化

【教職員の業務例：校務用端末を利用して作成した教材を児童生徒の学習者用端末に配布し、授業を実施】

	ネットワーク分離型の場合	アクセス認証型の場合
業務のやり方		
セキュリティ脅威例	◆ 悪意のある関係者（教職員、児童生徒等）の過失 ● 利用が禁止されている外部記憶媒体へのデータ移行 ● 重要性の高い情報を含むデータを私用端末に移行 ● ID/PWの漏洩による校務用端末への不正アクセス ● … ◆ 関係者（教職員、児童生徒等）の過失 ● 外部記憶媒体の紛失 ● 校務用端末の紛失 ● 利用が禁止されている外部記憶媒体の利用 ● …	◆ 悪意のある他者 ● 不正なWebサイトのアクセスによる校務用端末のマルウェア感染 ● … ◆ 脆弱性のある機器・ソフトウェア者 ● 校務支援システムや校務ファイルサーバに対する、不正アクセスやOSの脆弱性を利用した攻撃 ● … ◆ 悪意のある関係者（教職員、児童生徒等）の過失 ● ID/PWの漏洩による校務支援システムへの不正アクセス ● … ◆ 関係者（教職員、児童生徒等）の過失 ● 校務用端末（教職員端末）の紛失 ● 児童生徒に重要性の高い情報を含むデータを誤配布 ● …
セキュリティ対策例	●外部記憶媒体の利用を制限する ●外部記憶媒体のデータを暗号化する ●…	● 不正なWebサイトへのアクセスを制限する ● 各種サーバやシステムの保護を行う ● ログインID/パスワードに加え、二要素以上の認証手段を導入する ● 予め許可された端末やユーザからのみアクセスを許可する ● 端末に保存されるデータを暗号化する ● 端末にマルウェア対策ソフトを導入する ● …

ステップ②「どのように」 アクセス認証型におけるセキュリティ対策と対応する要素技術

アクセス認証型において、教職員の業務の中で発生し得るセキュリティ脅威、その脅威に対するセキュリティ対策、そしてセキュリティ対策に対応する要素技術を理解しましょう。図表 3-12 のセキュリティ脅威例、セキュリティ対策例、対応する要素技術の記載例※35 を参考に、各自治体の業務に即したセキュリティ対策及び要素技術を検討しましょう。

図表 3-12　アクセス認証型におけるセキュリティ脅威例、セキュリティ対策例、要素技術例

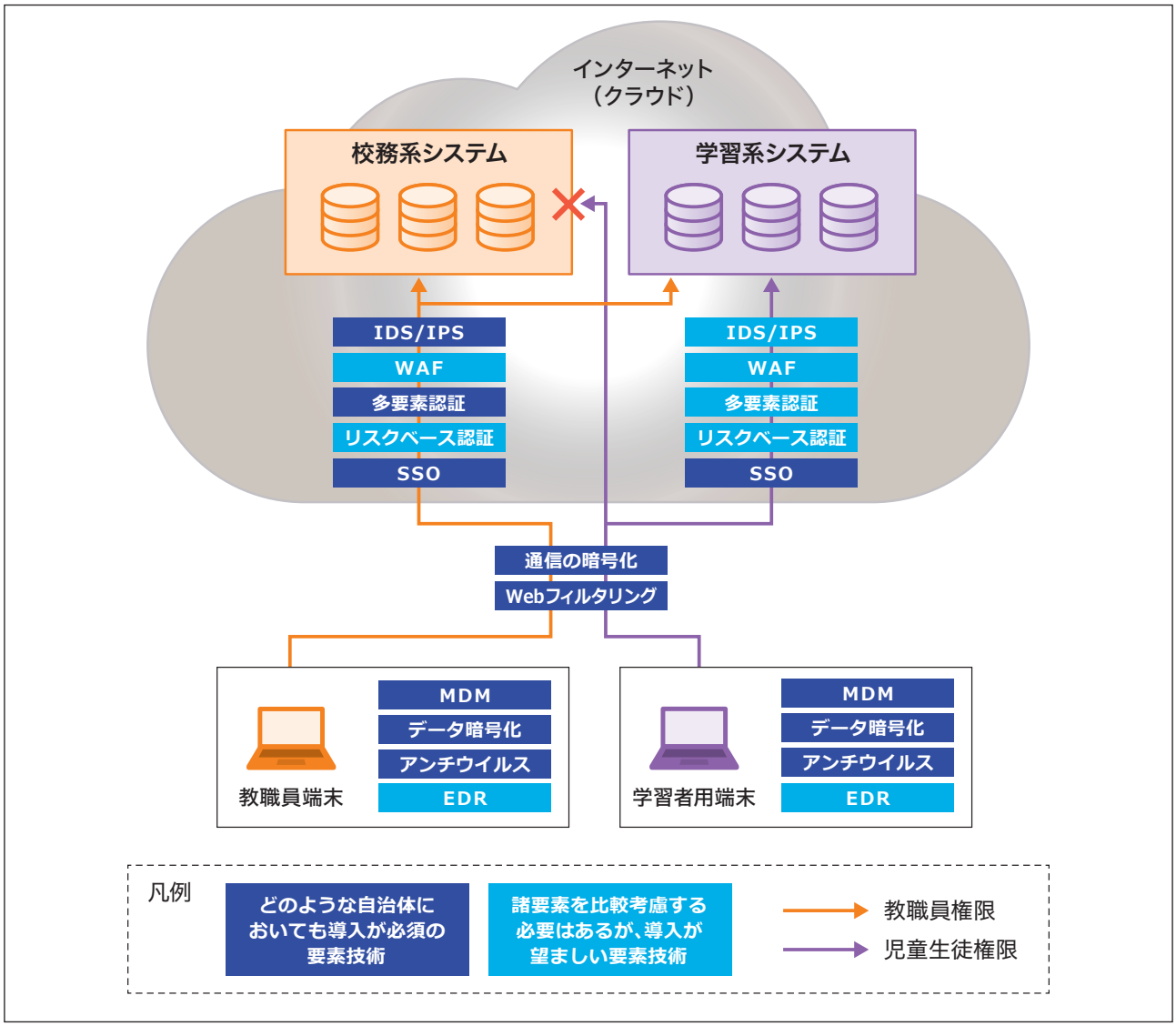
「何から」守るか	「どのように」守るか	
発生し得るセキュリティ脅威例	セキュリティ対策例	対応する要素技術例※36
組織管理外の端末を利用した校務支援システムへの不正アクセス	• 組織内の全ての端末を一元的に管理し、組織管理下の端末のみ校務支援システムにアクセスできるよう制限する	• MDM
不正なソフトウェアのダウンロードによるマルウェア感染	• 不要なアプリケーションのダウンロードを制限する	• MDM
端末 OS やソフトウェアの脆弱性を突いた攻撃	• 端末 OS や各種ソフトウェアのバージョンを最新版にする	• MDM
校務用端末の紛失	• リモートワイプ機能を利用する • デバイス上のデータを暗号化する	• MDM • データ暗号化
重要性の高い情報をやり取りする通信への不正アクセス	• 通信を暗号化し、第三者から閲覧されないようにする	• 通信の暗号化
不適切な Web サイトへのアクセス履歴の消去	• Web サイトのアクセスに関するログを収集する	• Web フィルタリング
不正な Web サイトへのアクセスによる校務用端末のマルウェア感染	• 不正な Web サイトへのアクセスを制限する • 端末にマルウェア対策ソフトウェアを導入する • 不審な挙動が見られた際に自動でネットワークから隔離する	• Web フィルタリング • アンチウイルス※37 • EDR/SOC
第三者による重要性の高い情報の窃取	• 端末の IP アドレスや位置情報を基にデータへのアクセス制御を行う	• リスクベース認証
ID/PW の漏洩による校務支援システムへの不正アクセス	• 二要素以上の認証手段を導入する	• 多要素認証
複数のサービスで共通かつ安易に推測できるパスワードを設定する	• 複数のクラウドサービスを一回の認証でアクセス可能とする	• SSO
校務支援システムや校務ファイルサーバに対する、不正アクセスや OS の脆弱性を利用した攻撃	• クラウド上に保存するデータを暗号化する • 各種サーバやシステムの保護を行う	• データ暗号化 • IDS/IPS
校務支援システムに対する、Web アプリケーションの脆弱性を利用した攻撃	• Web アプリケーションの保護を行う	• WAF

※35：本ページのセキュリティ脅威は、Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）の 6 つの脅威から脅威分析を行う「STRIDE 分析」を利用して抽出しています。またセキュリティ対策は「教育情報セキュリティポリシーに関するガイドライン」や、2022 年に組織で発生したセキュリティ脅威や対策について記載されている「IPA 情報セキュリティ 10 大脅威 2022」、組織で「最低限行うべきこと」に着目し、技術的な対策 153 項目を整理したガイドラインである「CIS Controls Version 8」等を参考に検討した内容を記載
※36：要素技術：各要素技術の詳細説明は図表 3-15 に記載
※37：マルウェア駆除機能が含まれるアンチウイルス製品の場合

◆要素技術について

要素技術は「アクセス認証型のセキュリティを確保するために、どのような自治体においても導入が必須の要素技術」と、「諸要素を比較考慮する必要があるが、導入が望ましい導入要素技術」に分別されます。※ 38 教職員の業務から考えられるセキュリティ脅威に対して、どのようなセキュリティ対策及び要素技術が必要か、検討を行いましょう。要素技術の構成例として、文部科学省発行の「GIGA スクール構想の下での校務 DX について」より抜粋した内容を図表 3-13 に記載しています※ 39。

図表 3-13　アクセス認証型における要素技術の構成例



◆要素技術について

重要性の高い情報を保存する校務支援システムや校務ファイルサーバ、一部の学習系システムについては情報漏洩の際の被害が大きいため、IDS / IPS など必要十分な要素技術を導入し、セキュリティ強度を上げることが大切です。ただし、SaaS サービスを利用する場合は、教育委員会で IDS / IPS 等の要素技術を導入することが難しいため、利用する SaaS サービスの事業者に対して、それらのセキュリティ対策が実施されているか確認しましょう。

※ 38：文部科学省（2023 年 3 月発行）GIGA スクール構想の下での校務 DX について
https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf　p15
※ 39：これらの要素技術は「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 4 年 3 月改訂・文部科学省）において取り上げられているセキュリティ技術のうち、いわゆるゼロトラストセキュリティに関するもの中心に整理したものであ り、今後の技術動向等により変化し得るものであることに留意すること

ステップ③「どのように」 要素技術の導入パターンとその特徴

アクセス認証型の要素技術の導入パターンとして、「専用製品」「端末 OS メーカー提供の製品」「運用で代替」の3パターンがあります。これらの導入パターンについては図表 3-14 を参考に、ユーザビリティや発生するコスト、運用の負荷などを総合的に勘案して導入を検討しましょう。

なお、ネットワークのセキュリティ対策として SWG ※ 40 を導入すると、Web フィルタリング機能に加えて、SSL 復号機能やデータ損失防止機能などのセキュリティ対策が可能となります。

また、EDR や WAF を導入し、その効果を最大限発揮するには事前のチューニングとログ分析が必要となります。その場合、管理者がそのためのスキルを習得するか、SOC ※ 41 等の外部の事業者に委託することが必要です。

◆専用製品

各要素技術に特化した製品を導入するパターンであり、必要な機能や求めるコストに適合した製品を自由に選択できることが特徴です。それぞれの要素技術を同一メーカーの製品とすることで、まとめて管理することも可能です。（図表 3-15）

◆端末 OS メーカー提供の製品

端末 OS メーカーが提供しているライセンスで要素技術を導入するパターンで、ライセンスの種類に応じて複数の要素技術を導入できることが特徴です。また、端末とグループウェアを同じ管理コンソールから管理することができます。（図表 3-16）なお、GIGA スクールで導入した端末 OS メーカー提供の要素技術を利用し、不足している要素技術については専用製品を採用することも可能です。

◆運用で代替

他の導入パターンと組み合わせた上で、人でセキュリティ対策を実施するパターンです。製品にかかるコストは抑えることが可能ですが、マルウェア感染などのセキュリティインシデントに対応できる運用体制を構築する必要があります。（図表 3-17）

図表 3-14　要素技術の導入パターンとその特徴

		専用製品		端末 OS メーカ提供の製品 ※ 43		運用で代替 ※ 44
提供される要素技術		• 多要素認証※ 42 • SSO ※ 42 • Web フィルタリング • MDM • アンチウイルス	• データ暗号化 • IDS/IPS • リスクベース認証※ 42 • EDR • WAF	• 多要素認証 • SSO • Web フィルタリング • MDM • アンチウイルス • データ暗号化	• リスクベース認証 •EDR	• EDR (SOC)
特徴	技術的フィジビリティ（前提）	• 導入時や端末 OS アップデートの際に、事前の動作検証を行い、確実に動作する製品の導入が必要		• 端末 OS メーカーが提供している製品の導入が必要		• セキュリティインシデントに対応可能な運用体制の構築が必要
	ユーザビリティ	• それぞれの要素技術を同メーカーの製品に統一することで、要素技術間の連携が容易		• 端末 OS やグループウェアと連携したスムーズな認証が可能		• 問い合わせ対応やインシデント時の対応が遅くなる可能性有り
	コスト	• ユーザビリティやセキュリティ、運用とコストのバランスを考慮した上で適切な製品を選択可能		• ライセンスの種類によっては、複数の要素技術を同時に導入可能		• セキュリティ製品の導入にかかるコストを抑えることが可能
	運用	• それぞれの要素技術を同メーカーの製品に統一することで、まとめて管理可能		• グループウェアと端末を同じ管理画面から管理可		• 要素技術で実現する機能を運用で代替するため、運用の負荷は高い

※ 40：Secure Web Gateway の略称。Web / インターネットトラフィックを分析し、悪意ある宛先へのアクセスをフィルタリングする機能
※ 41：Security Operation Center の略称。端末やシステム、ネットワークを監視し、セキュリティ上の脅威が発生した場合には脅威への対応（分析、調査、隔離、報告など）を実施
※ 42：多くは多要素認証の製品の一機能として提供
※ 43：2023 年 1 月末の情報を基に作成
※ 44：アクセス認証型を実現する上でどのような自治体においても導入が必須の要素技術については代替が難しい

図表 3-15　専用製品の特徴

要素技術	「専用製品」の特徴	
多要素認証（SSO, リスクベース認証）	概要	• 情報・データへのアクセスに対する認証にあたり、記憶（ID・PW 等）、所持（端末の電子証明書、IC カード等）、生体（指紋、顔等）の３要素のうち、２以上の要素を求めることで、なりすましや不正アクセスを防止する技術
	特徴	• 採用する認証要素によって利用者のユーザビリティは変化する • 認証要素が利用端末に内蔵されている場合は、別途認証機器を持ち運ぶ必要がないため、ユーザビリティが高い • SSO は導入することで、ユーザビリティが向上するだけでなく、認証の煩雑化から生じるセキュリティ脅威が軽減する • リスクベース認証は導入により、セキュリティが高められる一方で、ユーザビリティを損なう可能性があるので、適切なリスク判定基準の設定が必要となる
Web フィルタリング	概要	マルウェアへの感染につながりうるセキュリティリスクの高い Web ページへの接続を防止する技術
	特徴	• ホワイトリスト方式、ブラックリスト方式、カテゴリフィルタリング方式※45 の３種類の方式がある • ホワイトリスト方式は有害な Web サイトを確実に遮断できるが、登録された Web サイト以外の閲覧が不可のためユーザビリティは低くなる。一方でブラックリスト方式はユーザビリティは高いが、有害な Web サイトを管理者が登録するという日々の運用の手間が発生する。 • カテゴリフィルタリング方式は予め設定したカテゴリの精度によっては、誤ブロックが発生し、ユーザビリティやセキュリティが損なわれる可能性があるため、注意して運用する必要がある
IDS/IPS	概要	事前に定義した不正アクセスパターンとマッチングすることによりサーバ・クラウドへの不正なアクセスを検知（IDS）または遮断（IPS）する技術
	特徴	•IaaS ではオプションサービスとして提供されることが多い •SaaS サービスを利用する場合は、SaaS サービスに付帯されていることが多いため、その場合は別途製品を用意する必要がない
MDM	概要	端末等のアップデートや各種セキュリティ設定を一元的に管理することで、端末毎のセキュリティに関する設定の違いによるセキュリティホールの発生を防止するとともに、紛失・盗難に遭った際に、データの遠隔消去等を行う技術
アンチウイルス	概要	既知のパターンファイル（マルウェア情報）からマルウェアを検知し駆除する技術やパターンファイルは存在しないが不審な挙動をするプログラムを検知し、駆除する技術
	特徴	• OS としてマルウェア感染リスクが低い仕組みとなっている製品もある
データ暗号化	概要	データを端末（ユーザー端末）やサーバ（クラウド）に保存する際に暗号化し、アクセス権限が無い者による情報の閲覧・編集を制限する技術
	特徴	• ハードディスクの暗号化はユーザビリティが高いが、端末が起動している場合に外部記憶媒体等を利用することで未暗号化データを持ち出されるリスクを伴う • ファイル暗号化はファイル流出時の情報漏洩対策が可能だが、ファイルを暗号化する際にユーザ側で作業が発生することがあり、ユーザビリティを損なう可能性がある
EDR	概要	パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行う等の不審な挙動をするプログラムを検出し、そのログを管理者等が分析して適切に対処することで、感染の拡大を防止する技術
	特徴	• アンチウイルス製品との相性によっては動作が不安定となり、ユーザビリティを損なう可能性があるため、アンチウイルスソフトと EDR は同ベンダの製品が望ましい • 高度な機能を持つ製品を導入する場合は、端末のメモリや CPU に高い負荷がかかるため、ユーザビリティに影響する可能性がある • 効果を最大限に発揮するためには、専門的な知識を持つ人材による事前のチューニングとログ分析が必要であり、管理者がそのためのスキルを取得するか、外部の事業者にこれを委託することが必要
WAF	概要	インターネットと繋がっているサーバ（Web サーバ）への外部からの攻撃を検知し、防御する技術
	特徴	• IaaS ではオプションサービスとして提供されることが多い • SaaS を利用する場合は、サービスに付帯されていることが多いため、サービス提供事業者に確認が必要

コラム：ライセンスについて

要素技術を製品で導入する場合は、機能を利用するためにライセンスの購入が必要な場合があります。ユーザーライセンスや端末ライセンスなど、ライセンスには複数の購入形態がありますが、いずれのライセンスも必ず教職員全員分の購入が必要という訳ではありません。システムの利用頻度が低い教職員のライセンスは購入しないなど、実際に利用するユーザや端末の数を適切に見定め、必要性とコストを総合的に勘案して購入を検討しましょう。

図表 3-16　端末 OS メーカ提供の製品の特徴

「端末 OS メーカ提供の製品」の特徴	
提供される 要素技術 ※ 46	•MDM/ 多要素認証※ 47/SSO ※ 47/ リスクベース認証※ 47 /Web フィルタリング※ 48/EDR ※ 49/ アンチウイルス※ 50/ データ暗号化 ※ 50 ※ 51
技術的 フィジビリティ	• 端末 OS における動作が予め保証されている
ユーザビリティ	• 端末 OS やグループウェアと連携したスムーズな認証が可能
コスト	• 当該ライセンスを購入することで、アクセス認証型において必要なセキュリティ対策を複数実現可能 • ライセンスの種類によって費用や搭載されるセキュリティ機能が異なるため、すでに導入済みのライセンスや端末 OS 等を考慮して、適切なライセンスを選択することが重要
運用	• セキュリティ機能間の連携機能が豊富なため、包括的なセキュリティ対策が可能 • 同メーカが提供するグループウェアと端末を同じ管理コンソールから管理可能 • 同メーカが提供する IaaS を利用することで、IaaS と端末、グループウェアを同じ操作感で管理可能

図表 3-17　運用で代替の特徴

「運用で代替」の特徴	
要素技術を 運用で実現する場合 の実現イメージ	• 要素技術：EDR（SOC） • 実現イメージ：アンチウイルスソフトのマルウェア監視機能を利用し、マルウェア検知時に教育委員会の担当者にメールを自動送付、手動で隔離を行う。ただし、パターンマッチング形式のため、未知のマルウェアには対応できない
技術的 フィジビリティ	• アクセス認証型を実現する上で最低限必要とされる要素技術については代替が難しい • マルウェア感染などのセキュリティインシデントに対応し得る運用体制を確立する必要がある
ユーザビリティ	• 問い合わせ対応やインシデント時の初動対応が遅くなる可能性がある
コスト	• セキュリティ対策の導入にかかるコストを抑えることが可能
運用	• 要素技術で実現する機能を運用で代替するため、運用の負荷は高くなる可能性が高い

※ 45：Web サイトに特定の情報が含まれる場合に、その閲覧を防ぐフィルタリング方式

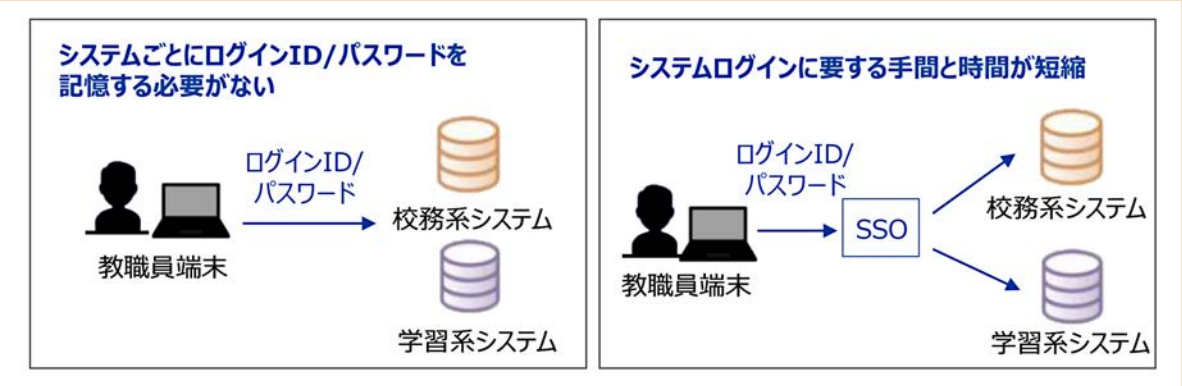
※ 46：2023 年 1 月末時点の情報より作成
※ 47：端末 OS メーカ提供のクラウド上の認証機能に登録されたアプリケーションが対象。認証機能上でユーザアカウントの作成が必要
※ 48：URL 単位のホワイトリスト方式 / ブラックリスト方式によるフィルタリング機能を指す。カテゴリフィルタリング方式は一部のクラウドツールにのみ含まれる機能
※ 49：一部のクラウドツールにのみ含まれる機能
※ 50：クラウドツールに対応する OS と組み合わせることで実現可能。ただし、一部の OS は OS 自体がマルウェア感染リスクの低い仕組みとなっている
※ 51：端末 OS メーカ提供の製品に含まれるクラウドストレージ機能を利用する際は、データを格納する際に自動的に暗号化が行われる

コラム：認証設計について

◆ユーザビリティを考慮した認証設計

校務系・学習系ネットワークの連携により、ロケーションフリーで校務系システムが利用可能となるため、各システムのログイン ID ／パスワードを適切に設定・維持する必要があります。図 3-18 の事例のように、認証設計を行うことでユーザビリティの向上に加え、ログイン ID ／パスワードの漏洩によるセキュリティ脅威の軽減といった効果があります。

図表 3-18　ユーザビリティを考慮した認証設計例 ※ 52

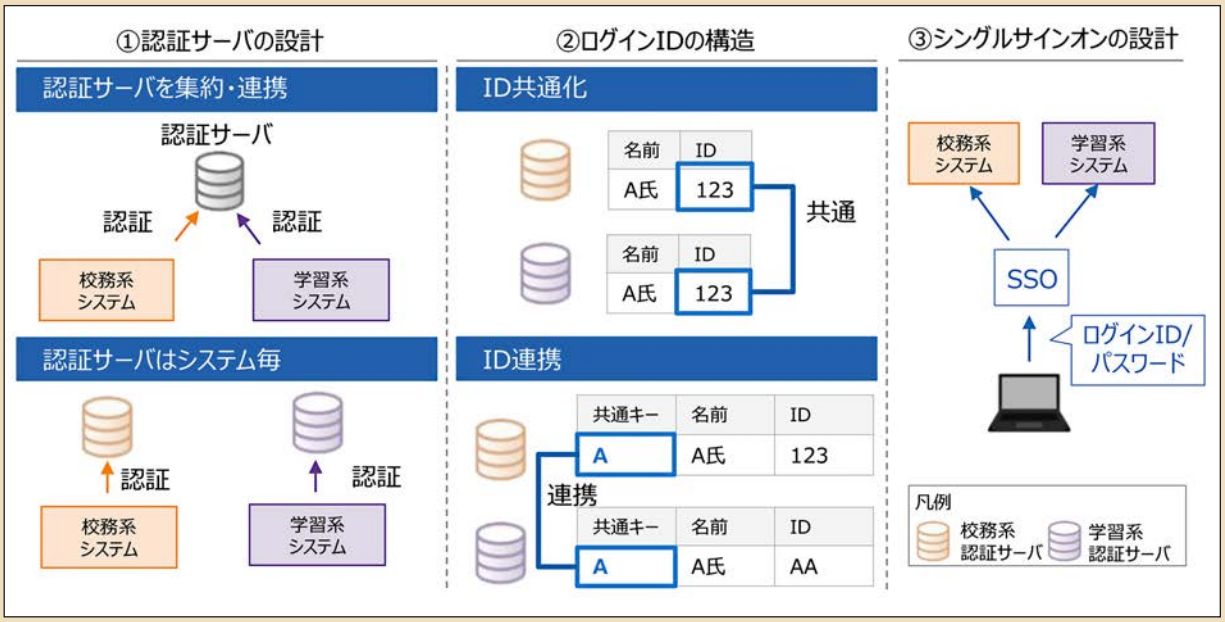


◆認証設計の手法

認証設計は、図表 3-19 に記載の「①認証サーバの設計」「②ログイン ID の構造」「③シングルサインオン（SSO）の設計」といった手法があります。

また、端末のログイン情報を連携し、システムログイン時の認証として利用すると、ユーザビリティの向上に効果的です。ただし、その場合は重要性の高い情報を扱うシステムへのログイン時に多要素認証の導入が必要となります。

図表 3-19　認証設計の手法例

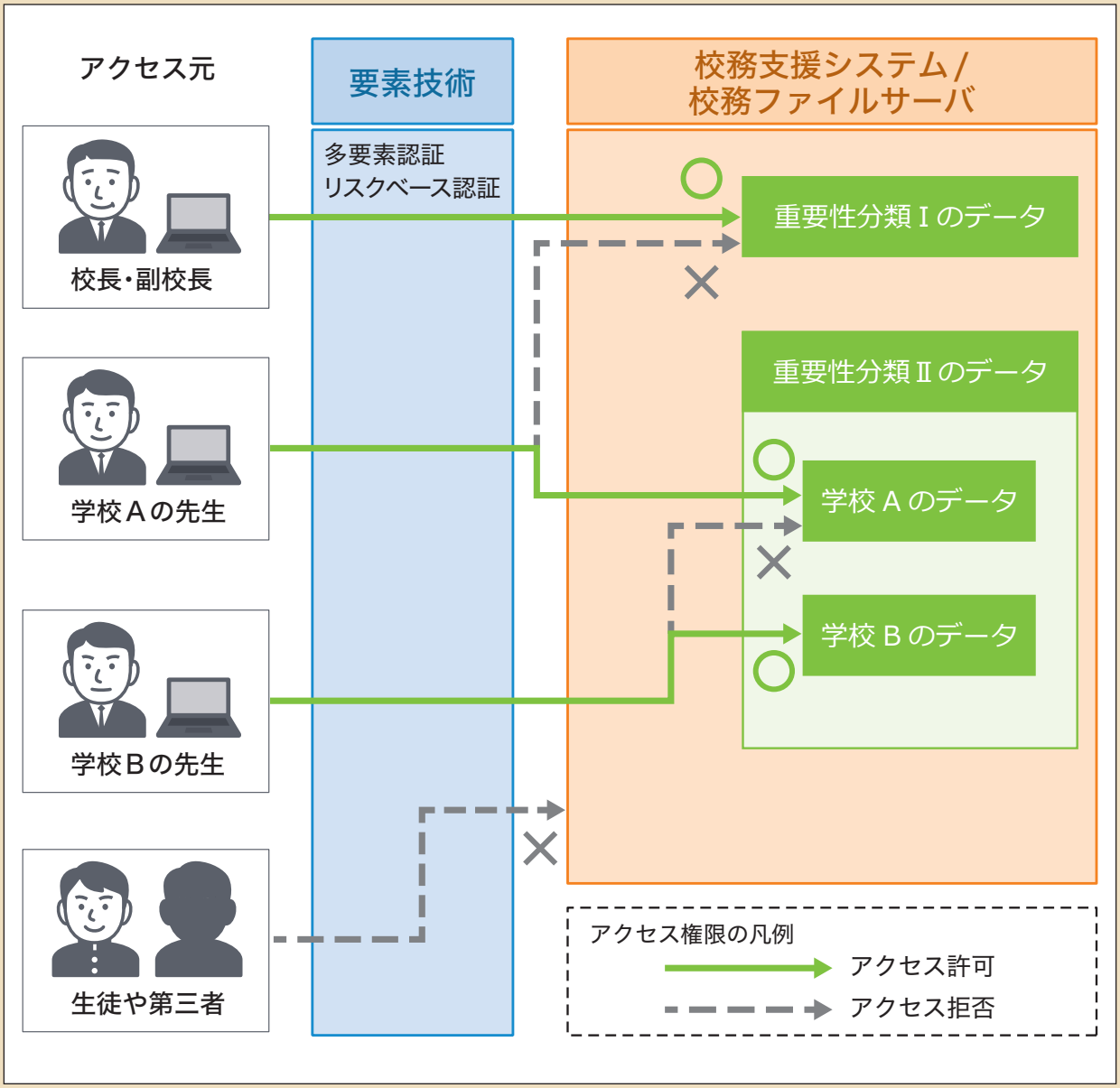


※ 52：サーバに保存されるデータの重要性によっては多要素認証の導入が必要。多要素認証の検討については p24 に記載

コラム：アクセス権限の管理と要素技術の組み合わせ

アクセス認証型におけるセキュリティ対策は要素技術による技術的な対策に加え、保存されている情報資産の重要性※ 53 に応じたアクセス権限の管理を行います（図表 3-20）。重要性が最も高いデータについては、担当職員とその管理者のみに限定するなど、真に必要な職員からのアクセスのみに設定しましょう。また、重要性が同じデータについても必要性のある情報のアクセスに絞るなど、適切な教職員からのアクセスのみに限定しましょう。

図表 3-20　アクセス権限の管理と要素技術の組み合わせ例



※ 53：文部科学省（2023 年 3 月発行）GIGA スクール構想の下での校務 DX について
https://www.mext.go.jp/content/20230308-mxt_jogai01-000027984_001.pdf　p16
なお、アクセス権限は、個々の自治体におけるデータの重要性分類や想定される脅威を整理した上で、個別に設定する

コラム：多要素認証における認証手段とその特徴について

◆認証手段について

アクセス認証型の要素技術の一つである多要素認証は、利用者の本人以外の不正アクセスを防ぐための重要な要素技術です。

認証の手段として、記憶・所持・存在の３種類があります（図表 3-21）。記憶はパスワードや暗証番号等の利用者本人が知っている「情報」で本人か否かを判断する手段で、所持は IC カードや QR コードなど利用者が持っている「モノ」で判断する手段で、存在は生体認証等の本人に備わっている「特徴」で判断する手段です。

図表 3-21　多要素認証における認証手段 ※ 54

	検証手段		
	記憶	所持	存在
概要	利用者だけが知っている『情報』で本人か否かを判断する方法	利用者だけが知っている『モノ』で本人か否かを判断する方法	利用者の身に備わっている『特徴』で本人か否かを判断する方法
具体例	・パスワード ・暗証番号 ・PINコード 等 パスワード **** PINコード ・・・・・	・ICカード ・QRコード ・ワンタイムパスワード 等 123 456	・生体認証 （指紋、顔、指静脈、手のひら静脈）等

◆認証手段の特徴

図表 3-22 は各認証手段を比較し、ユーザビリティ・セキュリティ・コスト・運用の観点で評価した表です。認証手段は教職員が日々の業務で利用するため、特に、ユーザビリティの観点が大切です。

多要素認証において、二要素目はすでに導入済みの手段があればそれを利用することも可能です。個々の自治体で認証手段の評価観点に対する重要度は異なるので、各認証手段の特徴と個々の自治体で重視する観点を総合的に勘案し、導入する認証手段を検討しましょう。

図表 3-22　認証手段の特徴

凡例
★★★ 他方式と比較し相対的に評価が高い
★★☆ 相対的に評価が標準
★☆☆ 相対的に評価が低い

認証手段＼評価観点		前提条件	評価の観点			
		技術的フィジビリティ	ユーザビリティ	セキュリティ	コスト	運用
記憶 ・ID＆パスワード		－ （既に利用されている）	ログイン画面にID＆パスワードの入力が必要 ★☆☆	盗み見などで流出した場合、容易に悪用される ★☆☆	－ （既に利用されている）	IDやパスワードの発行と削除が必要 ★★☆
所持	ハードウェア ・ハードウェアトークン ・ICカード	端末OSと互換性のある製品の選定が必要	トークンパスワードの入力やICカードの読み取りなどの操作が必要 ★☆☆	ハードウェアの盗難により悪用される可能性がある ★☆☆	デバイスの調達・保守費用が必要 ★★☆	デバイスへのデータ登録と削除、物理的な配布が必要 ★★☆
	ソフトウェア ・ソフトウェアトークン ・SMS ・メール		ソフトウェアで受け取った認証情報の入力が必要 ★☆☆	認証情報を受信するデバイスがロックされていれば盗難しても容易には悪用されない ★★☆	モバイルデバイスとSWの調達・保守費用が必要 ★☆☆	モバイルデバイスのセットアップやソフトウェアインストール・アンインストールが必要 ★★☆
	クライアント証明書		証明書を一度インストールすれば、認証操作は不要 ★★★	端末がロックされていない場合、盗難時に悪用される可能性がある ★☆☆	ライセンス調達・更新費用が必要 ★★☆	証明書のインストール・アンインストールが必要 ★★☆
存在 ・指紋　・顔 ・虹彩　・静脈		カメラなどが端末標準装備でない場合、端末OSと互換性のあるデバイス選定が必要	カメラやリーダに生体情報を映す/かざす行為が必要 ★★☆	悪意のある内部ユーザによる悪用の可能性はあるが、第三者への流出はない ★★★	外部デバイスが必要な場合は、調達・保守費用が必要 ★★☆	生体情報の登録と削除が必要 ★★☆

※ 54：参考：IPA「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル（解説編）（2013 年 4 月 23 日）」

（3）- 5　システム運用

校務系・学習系ネットワークの連携により、場所を問わず校務系・学習系システムにアクセス可能となる一方で、教職員の業務及び発生し得るセキュリティ脅威が変化します。 図表 3-23 はアクセス認証型への移行に伴い変化が生じる運用業務例及び必要な作業・知識を整理した表です。教職員の業務やセキュリティ脅威の変化に合わせたシステムの運用方法を検討しましょう。

図表 3-23　アクセス認証型のシステム運用業務例

運用業務	運用項目	必要な作業	必要な知識
教職員の利便性	ID 管理	・定期的な ID/ アクセス権の棚卸	・ユーザー権限の考え方 ・ID 管理システムの考え方
		・転入出時の ID 作成 / 変更 / 削除	
	ライセンス管理	・利用ライセンス数の定期的な棚卸	・ライセンス管理の知識
端末運用	端末管理	・定期的な端末（物品）の棚卸	・端末設定に関する知識 ・MDM の考え方
		・転入出時の端末設定初期化 / 変更 / 削除	
	ライセンス管理	・利用ライセンス数の定期的な棚卸	・ライセンス管理の知識
ネットワーク セキュリティ運用	ポリシー管理	・Web フィルタ例外設定	・Web フィルタリングの考え方
セキュリティ インシデント対応	インシデント発生時の対応	・端末紛失対応	・MDM の考え方 ・感染端末の対応方法 ・セキュリティログの分析方法
		・ウイルス感染時の対応	
		・セキュリティシステムからの警告調査（SOC）	

コラム：インシデント発生時の対応について

端末紛失やマルウェア感染といったインシデントは、発生時に「誰が」「どのような対応を行うか」を事前に検討しておくことが大切です。事前検討が十分でない場合、インシデント発生後の対応が遅れ、二次被害が発生する恐れがあります。図表 3-24 に記載のポイントを踏まえて、インシデント発生時の対応フローを検討しましょう。

また、インシデントはその発生要因によって２種類に分別されます。図表 3-25 を参考に、それぞれの種別ごとにインシデント発生時の対応方法を検討しましょう。

図表 3-24　インシデント発生時の対応フローを検討する際のポイント

❶ 役割分担　インシデント発生から対応完了までに「誰が」「何を」行うのか整理しておくことで、円滑にインシデントへ対応することが可能

❷ 連絡体制　インシデント発生後は最初に連絡する相手が分からず、迷ってしまうことが多いため、予めインシデント発生後の連絡先を決めておく

図表 3-25　インシデントの種別と対応例

種別	インシデント例	インシデント発生時の対応例
内的要因（過失）	・端末紛失 ・メールやチャットの誤送信	・管理者に連絡・判断を仰ぎ、対応を行う
外的要因	・第三者による不正アクセス ・Web サイトのアクセスによるマルウェア感染	・システム側でネットワーク隔離を行うなど、速やかに対応を行う

（4） ルールの検討

校務系・学習系ネットワークの連携によって、教職員には働き方や端末、データの取り扱い等で業務の変化が生じます。重大なセキュリティインシデントを未然に防止するためにも、個別のルールの見直しを行うことが大切です。見直したルールに合わせシステムで制御することで、教職員の負担を軽減できます。本節では、ルールの見直しの際に参考となるよう、想定されるルール例を示します。

図表 3-26　想定されるルール例

教職員の業務の変化	変化によりルールの見直しが必要な項目	ルール例
働き方	勤務時間	・リモートワーク時の勤怠連絡に関するルール
		・適切に労働時間を管理するためのルール
	勤務場所	・自宅で業務を行う際のルール
		・学校外で作業を行う際のルール（利用禁止場所等）
端末の取り扱い	端末の保管・持ち運び	・職員室外で端末を利用する際のルール
		・端末保管場所に関するルール
		・学校外に端末を持ち出す際のルール
		・学校外でネットワークに接続する際のルール
データの取り扱い	重要性の高い情報の取り扱い	・ダウンロード可否についてのルール
	インターネットからのデータのダウンロード	・危険なデータをダウンロードしてしまった際の対処策
		・危険なデータのダウンロードを未然に防ぐルール
	インターネットへのデータのアップロード	・重要性の高い情報の誤ったアップロードを防止するルール
		・情報の適切なアップロード先を定めたルール

コラム：ルールの反映・周知・運用

ルールはセキュリティポリシーや運用マニュアル等への反映を検討し、効果的に周知することで、小中学校へ浸透、普及、定着し、校務系・学習系ネットワークの連携の円滑な運用につながります。ルールを周知した後、実際に運用をする中で収集した改善点や要望事項を基に適宜ルールの見直しを実施します。

◆埼玉県鴻巣市

先進自治体として後述する鴻巣市では、令和３年４月より校務系・学習系のネットワークを連携し、複数のシステムをパブリッククラウド上で構築しました。移行後の環境の変化に対応するため、同時期に「鴻巣市学校情報セキュリティポリシー」を改訂しています。

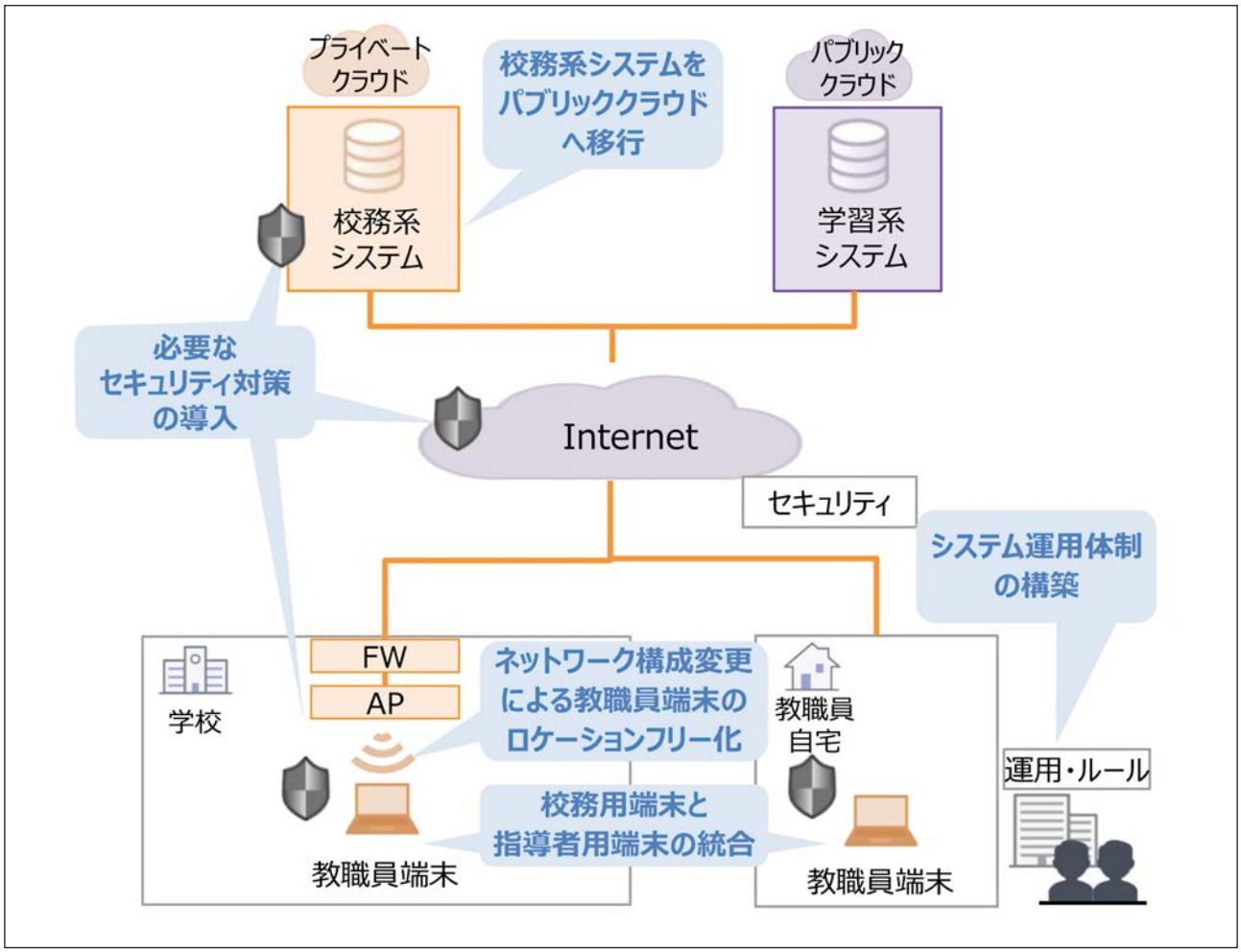
図表 3-27　鴻巣市学校情報セキュリティポリシー項目

学校セキュリティポリシー	学校セキュリティ基本方針	・学校セキュリティ対策に関する統一的かつ基本的な方針
	学校セキュリティ対策方針	・学校セキュリティ基本方針を実行に移すための全ての情報システムに共通の学校セキュリティ対策の基準
学校セキュリティ実施手順		・学校セキュリティポリシーに基づき、学校セキュリティ対策を実施するための具体的な手順（各学校作成）職員室外に端末を放置する際のルール

（5） 校務系・学習系ネットワークの連携に必要なシステム移行作業の検討

校務系・学習系ネットワークの連携に向けた移行作業では、図表 3-28 に記載のように、「校務系システムをパブリッククラウドへ移行」「ネットワーク構成変更による教職員端末のロケーションフリー化」「校務用端末と指導者用端末の統合」「必要なセキュリティ対策の導入」「システム運用体制の構築」を実施します。

図表 3-28　校務系・学習系ネットワーク連携後のシステム構成例



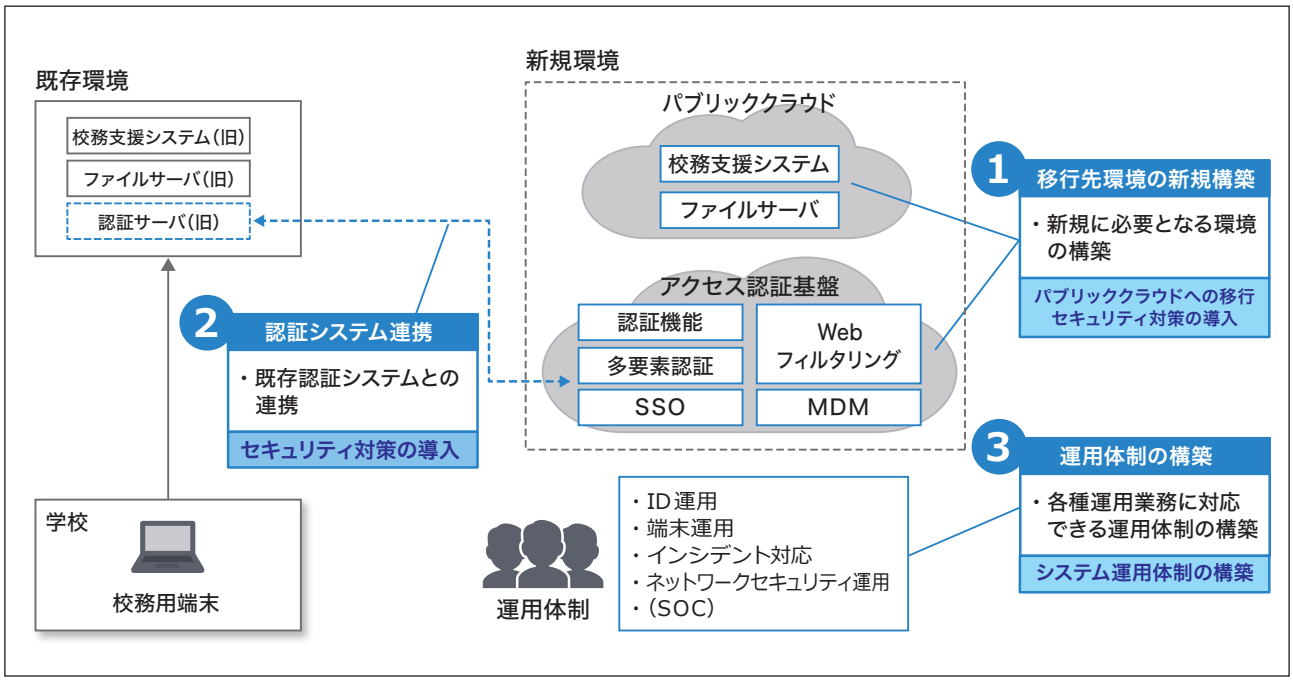
（5）- 1　切替前の作業

切替前の作業の一例として移行先環境の新規構築、既存の認証システムの連携、運用体制の構築について記載します（図表 3-29、図表 3-30）。

図表 3-29　切替前の作業例

実施項目	実施項目
1 移行先環境の新規構築	・アクセス認証型導入にあたり新規に必要となる移行先環境の構築（アクセス認証基盤、パブリッククラウド上へ移行対象となる教育情報システム）
2 既存の認証システム等と連携	・アクセス認証基盤と既存の認証システム等の連携
3 運用体制の構築	・SOC の立ち上げ等、運用体制を構築

図表 3-30　切替前の作業例



(5) - 2　切替作業

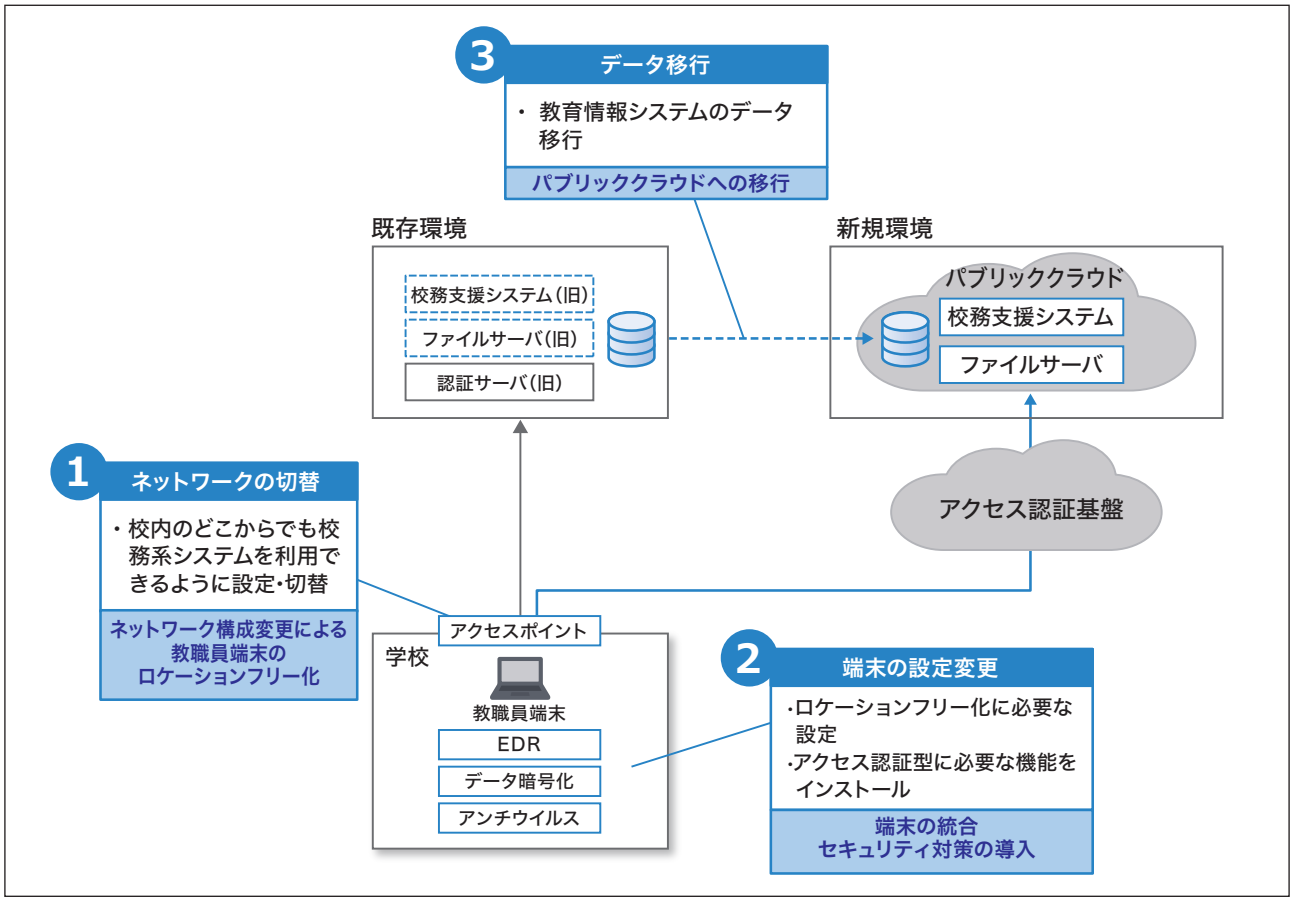
切替作業の一例として、下記の図表 3-31、図表 3-32 でネットワーク設定・切替、端末の設定変更、教育情報システムのデータ移行について記載します。ネットワークや端末、教育情報システムは設定変更の際に利用不可となる可能性があるため、教職員への業務影響を考慮したスケジュールを立てることが大切です。

なお、移行前のシステムと移行後のシステムを並行稼働する場合、データの移行後にネットワークや端末の切替作業を実施する可能性もあります。その場合は、アクセス認証型への移行が完了した端末のみ、パブリッククラウドへのアクセスが可能となるよう設定を行う必要があります。

図表 3-31　切替作業

実施項目	内容	留意点
1 ネットワーク設定・切替	・校内のどこからでも校務系システムにアクセスできるよう校内のネットワークを設定・切替	・ネットワークが切れる可能性があるため、業務影響を考慮したスケジュールをたてる
2 端末の設定変更	・端末にMDMやEDR等をインストール ・必要に応じて多要素認証デバイスを取付	・新規端末を導入するか、既存端末を流用するかによりセットアップ方法が異なる ・一時的に端末利用ができなくなる可能性があるため、業務影響を考慮したスケジュールを立てる ・端末にインストールするアプリケーションに応じて、OSアップデートの必要性が生じる場合がある
3 教育情報システムのデータ移行	・パブリッククラウド上に移行対象となる教育情報システムのデータを移行	・システム利用ができなくなる期間が発生するため、業務影響を考慮したスケジュールを立てる

図表 3-32　切替作業のイメージ図



（6）　導入後の円滑な利用に向けて必要な教育・研修の検討

校務系・学習系ネットワークの連携により、1台の端末で業務が可能となり、校務系ネットワーク・学習系ネットワーク間のデータの連携方法が変わるなど、これまでの業務や利用ルール等に変化が生じます。研修・教育を実施することで、移行後に教職員の業務が滞ってしまう等の影響を軽減する効果が見込めます。

また、図表 3-33 に記載のとおり、教育・研修の中で校務系・学習系ネットワークの連携の概要・コンセプトを説明することで、具体的な活用イメージを持つことができ、移行後の積極的な利活用が期待されます。

図表 3-33　教育・研修の実施内容例と効果

教育・研修の実施内容例	効　果
・校務系・学習系ネットワークの連携の概要・コンセプトの説明	校務系・学習系ネットワークの連携の活用イメージを共有し、積極的な利活用を推進
・業務の変更点や新たな利用ルールの説明 ・操作手順、運用中の問い合わせ先の共有	端末利用方法の変化や、学校内の移行作業等により教職員の業務が滞ってしまう影響を軽減

コラム：武蔵村山市の教育・研修の概要

武蔵村山市では、教育・研修として以下のようにシステム概要説明会と操作説明会を実施しました。

	システム概要説明会	操作説明会
概　要	・校長に対し、アクセス認証型の概要・コンセプト、各学校における業務の変更点、端末切替・操作説明会のスケジュール等を事業者より説明	・教職員へアクセス認証型の概要・コンセプト、業務の変更点、各種設定や操作手順、運用中の問い合わせ先等を事業者より説明 ・各種設定や操作手順は、本実証委託事業者がハンズオン形式にて事業者より説明
効　果	・アクセス認証型への理解が深まり、校長を起点とした、学校全体の利活用を推進することができた	・運用開始後に混乱が起きることなく、教職員が業務を滞りなく継続することができた

参加者の感想

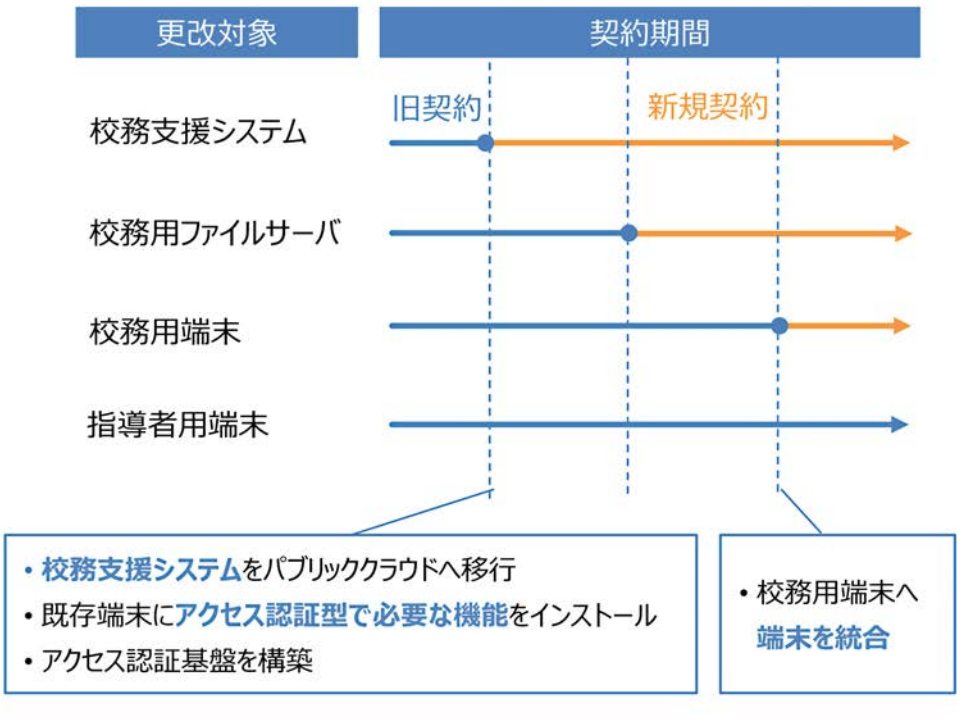
「情報記憶媒体（USB メモリ）の利用制限がセキュリティ事故を防ぐためのものだと理解できた」
「校務支援システムへの多要素認証によるログイン方法が理解できた」
「教室で無線 LAN につなげるので、校務用端末を用いて授業アンケートを実施したい」「職員室以外で校務ができるようになったので、自宅で利用したい」など

◆校務系・学習系ネットワーク連携に向けた段階的な導入計画

校務系・学習系ネットワークの連携に向け、端末や教育情報システムを全て同時期に整備することが難しい場合は、段階的な導入計画を策定しましょう。

また、校務系・学習系ネットワークの連携に向けては、更改対象の端末やシステムを確認し、更改のタイミングで性能等を見直すと効果的です。（図表 3-34, 図表 3-35）。それぞれの更改時期を踏まえた移行計画を策定することで、効率的に移行することが可能です。

図表 3-34　更改対象の契約期間例



図表 3-35　更改対象に関して見直すポイント

更改対象	見直しポイント
校務支援システム	• 校務支援システム上の機能の役割分担
校務用ファイルサーバ	• サーバ内に保存された各データの重要性
校務用端末	• 性能 (セキュリティ対策製品や業務アプリケーションの推奨動作環境) • 利便性 (操作性／持ち運びやすさ) • 端末統合の実施有無
指導者用端末	

第４章　校務系・学習系ネットワークの連携の活用例・効果

本章では、校務系・学習系ネットワーク連携の実現例、実現後の活用例、効果について、自治体の実例を基に説明します。

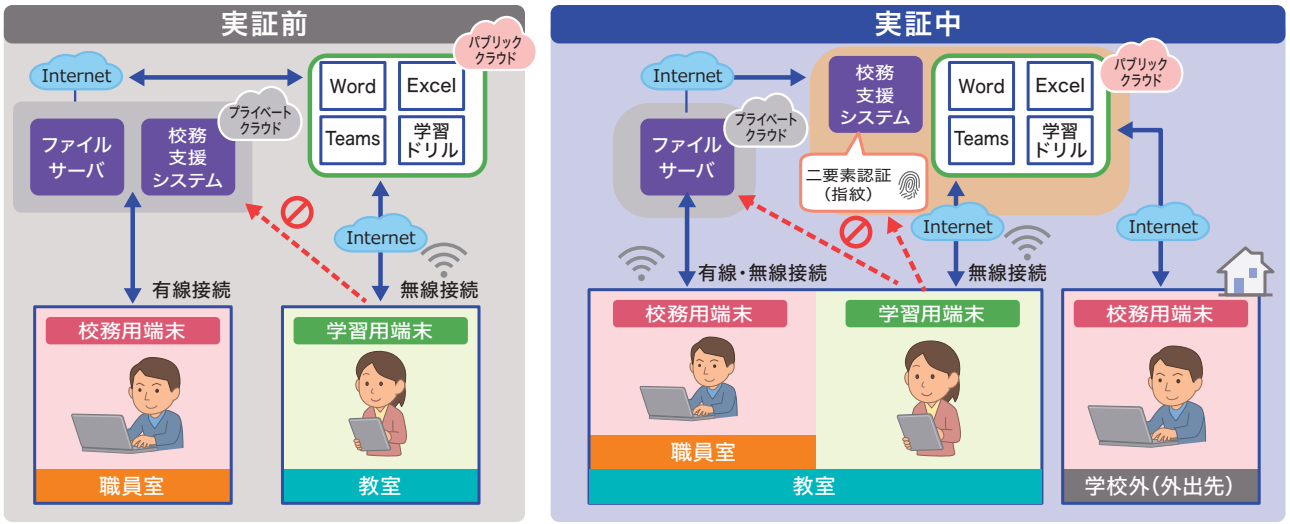
（1）　武蔵村山市での活用例・効果

本事業では、東京都武蔵村山市内の小中学校において、校務系・学習系ネットワークの連携に関する実証研究を行いました。ネットワーク連携の実証構成、切替にあたっての周知や教育委員会の気付き、教職員へのヒアリングやアンケートを通じた効果検証の結果を解説します。

◆実証構成

本事業では、現状の二層分離型のネットワーク構成から、アクセス認証型に移行し校務系・学習系ネットワークの連携を実現しました。下記にイメージ図と、移行後の変更内容を記載します。実証事業として、校務における働き方の変化を検証するため、校務支援システムのみをパブリッククラウドへの移行対象としました。

図表 4-1　武蔵村山市での校務系・学習系ネットワークの連携イメージ



	実証前	実証中
ネットワーク構成	二層分離型	アクセス認証型
校務支援システム構成場所	プライベートクラウド	パブリッククラウド
校務支援システムへのアクセス方法	校務用端末／有線／職員室からのみ	校務用端末／ロケーションフリー

◆利活用事例の作成・周知

校務系・学習系ネットワーク連携の実現後の利活用促進のため、端末の利活用事例を作成し、小中学校に向けて周知いたしました。端末の利活用事例は一部教員から活用例をヒアリングした上で作成し、校務支援システムの掲示板機能を用いて、全教員に対して周知を行いました。

図表 4-2　各学校に周知された利活用事例（一部抜粋）

見込まれる効果	利活用事例紹介
ペーパーレス化による業務時間短縮	学内会議をロケーションフリーかつペーパーレスで実施
	Microsoft Forms(アンケートツール) で進路調査を実施し、校務用端末で集計を行う
場所を問わない働き方による利便性向上	冬休み期間の出勤日に、校務用端末を持ち帰り、在宅で業務（授業資料作成や校務）を実施
	校務用端末で Teams を利用して、学外会議をオンラインで実施
端末統合による利便性向上	校務用端末で授業資料を作成し、教室に持ち運び大型モニターに提示しながら授業
	校務用端末で、学習系動画サイト（YouTube や NHK for School）にアクセスし、授業を実施

◆注意点の作成・周知

校務系・学習系のネットワーク連携の実現後、セキュリティインシデントの発生を防ぐため利活用の注意点を作成し、周知しました。注意点は総務省「テレワークセキュリティガイドライン」を基に、本実証特有の状況を考慮して作成し、図表 4-3 のとおり、ガバナンス・リスク管理、資産・構成管理、脆弱性管理等の項目で構成されています。上記の利活用事例と同様に、校務支援システムの提示板機能等を通じ周知を行いました。

図表 4-3　各学校に周知された注意点（一部抜粋）

区　分	注意点
ガバナンス（組織管理）・リスク管理	情報セキュリティ関連規定を確認し、規定に沿った業務を行う
	クラウドサービスの利用に際して、定められた利用ルールの範囲で利用する
資産・構成管理	校務用端末が教育機関等として守るべき情報資産に該当することを認識して適切に管理し、盗難・紛失防止に努める
脆弱性管理	校務用端末における OS をはじめとしたソフトウェアについて、定められた場所（公式アプリケーションストア、ベンダーの公式 HP 等）からのみインストールする
データ保護	テレワークで取り扱う情報は、定められた取扱方法（利用者・保管場所・利用可能なシステム構築の要件等）に従って取り扱う
マルウェア対策	少しでも不審を感じたメール（添付ファイルや URL リンクを含む）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心掛ける

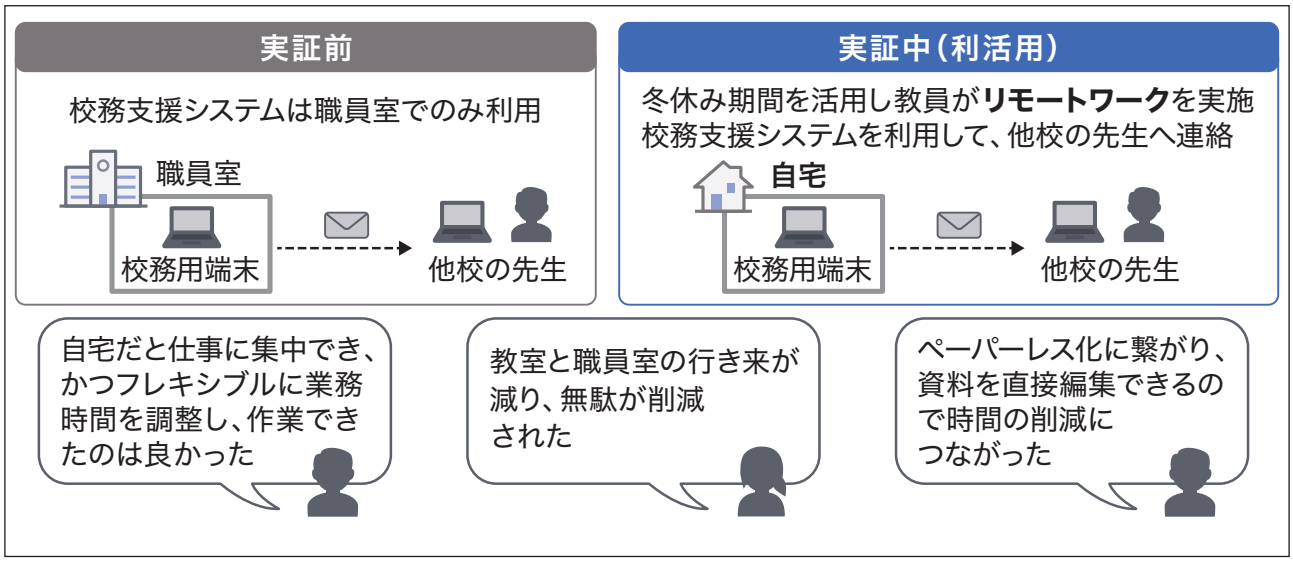
◆利活用事例

校務系・学習系ネットワークの連携により、武蔵村山市で実際に利活用が進んだ事例について、教職員の声と合わせて示します。

✓校務系システムの職員室外利用と校務用端末 / 校務支援システムの学校外利用

実証前は校務用端末の利用は職員室に限定し、校務支援システムも職員室からのみアクセスできました。実証中は校務系システムは職員室以外の学校内でも利用でき、校務用端末と校務支援システムは学校外でも利用できるようになりました。

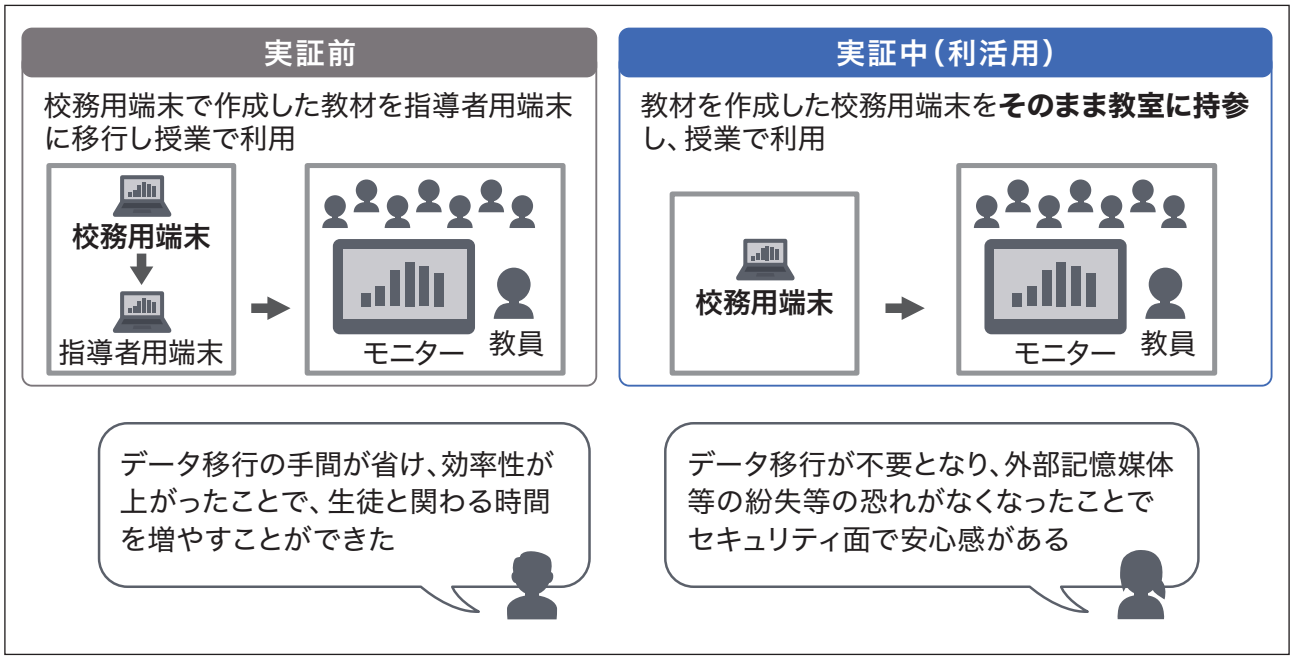
図表 4-4　校務系システムの職員室外利用と校務用端末 / 校務支援システムの学校外利用



✓校務用端末から指導者用端末にデータ移行をせずに授業を実施

校務系ネットワークと学習系ネットワークの端末間の資料やデータの受け渡しについて、実証前は外部記憶媒体の利用が必要でしたが、実証中はデータ移行をせずに一部の業務が実施できるようになりました。

図表 4-5　外部記憶媒体の利用が不要



◆教育委員会からの声

校務系・学習系ネットワークの連携を利用した教育委員会の声を、導入時と導入後に分けて紹介します。

✓導入時における気付き

新環境導入時の、導入作業、研修･教育、ルール･制度作りの観点別に教育委員会の気付きをご紹介します。

図表 4-6　導入作業における気付き

教育委員会のコメント
• 校務系・学習系ネットワークの連携は、教育委員会の考える運用方針と密接に関連するため**仕様検討は慎重に行う必要**がある • 独自端末の存在が現場調査で発覚する等、教育委員会で情報が収集できていない場合、**丁寧な現状把握が必要**となる

図表 4-7　研修・教育における気付き

教育委員会のコメント
• 外部記憶媒体の取り扱いの変更等、業務への影響について、**教職員に対しても理解を得られるよう丁寧に説明することが大切** • 校務系・学習系ネットワークの連携のコンセプトを教職員に対してわかりやすい言葉で説明し、活用方法の議論を十分に行うことが大切

図表 4-8　ルール・制度作りにおける気付き

教育委員会のコメント
• アクセス認証型の環境を有効に活用できるよう、**現場の声を拾いながらより最適な運用ルールの作成を行っていくことが大切** • 自治体単位でセキュリティポリシーや運用ルールを設定すると、市町村を超えた人事異動が発生する度に、教職員は異動先のポリシー及びルールの確認が必要となる。そのような観点から、**セキュリティポリシーや運用ルールは統一して作成されることが望ましい**（例 東京都内で統一のポリシーやルール）

✓導入後の運用における気付き

導入後に運用を行う中での教育委員会の気付きを紹介します。

図表 4-9　導入後の運用時における気付き

教育委員会のコメント
• 導入後の積極的な利活用推進のために、環境構築の段階から教育員会だけでなく、**業務に理解があり実際に利用をする教職員に参画してもらうことが大切** • ユーザー数や端末数を定期的に確認することで、システムのライセンスについて適切に管理することができる

◆校務系・学習系ネットワークの連携を利用した教員の声

校務系・学習系ネットワークの連携を利用した教員からの声を紹介します。

校務系・学習系ネットワークの連携全体を通して

校務系・学習系ネットワークの連携に伴うクラウドの活用は、**教職員の業務を効率化**すると思いました。教育現場のITを利用した業務効率化は、過剰なセキュリティ対策等により、なかなか前進していかないのが現状です。
今回の、校務系・学習系ネットワークの連携も課題は浮かび上がってきているものの、是非、その**課題を乗り超えて推進していただきたい施策**だと感じました。

（小学校の管理職）

どの場所でも端末が使えることで、今後リモートワークに限らず**新たな働き方が期待**できます。また、交流学習を通じてオンラインで他校の先生に授業をしていただく等の**新たな授業の実践も期待**できます。

（小学校の管理職）

従来は業務での紙媒体への依存度が高く、印刷や保管場所を決める等の業務が負担となっていました。
しかし、今回の校務系・学習系ネットワークの連携で**負担が軽減**しそうな兆しが見えました。

（中学校クラス担任）

指紋認証の精度等、課題はありますが、従来の校務用端末が鍵付きのケーブルで繋がれていた環境から、無線を用いて業務が出来るようになるのは、楽になります。
学校外で業務が出来るようになることは、とても便利です。

（中学校クラス副担任）

育児や介護と両立しながら、業務ができる環境を作ることは、働き方改革につながると思います。
時間の使い方は人それぞれ、どこでもパソコンを使えるようになることは助かります。

（小学校クラス担任）

◆武蔵村山市の教職員のアンケート結果

校務系・学習系ネットワークの連携の効果を定量的に評価するため、武蔵村山市の教職員へアンケートを実施しました。【期間：2023 年 1 月 27 日～2 月 9 日、回答数：193 件（回答対象者 451 名）】

本節では、実証における教職員の業務上の変更点として影響の大きかった、校務用端末の利用方法と、リモートワークの実施についてのアンケート結果を示します。

●校務用端末の利用方法の変化について

【結果】

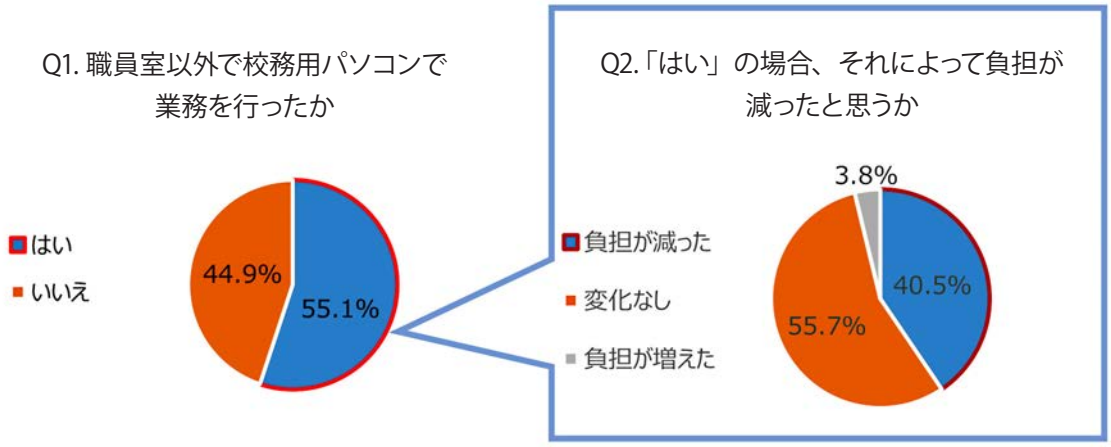
◆約 55% の教職員が、職員室以外の場所でも校務用端末を利用。そのうち約 41% が負担の軽減を実感している。

◆新たに教室で行うようになった業務としては、「教材作成、授業準備」「校務支援システムの利用」が上位となった。

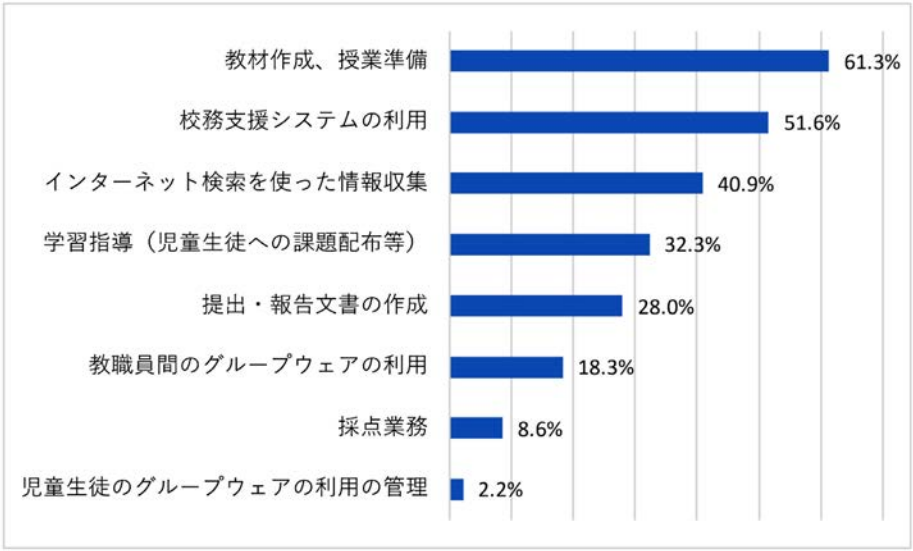
【考察】

◆教室等の職員室以外の場所で、校務用端末を利用し教材の作成や授業の準備を実施できたことで、教職員の負担軽減の効果が見られた。

Q1. 職員室以外で校務用パソコンで業務を行ったか
Q2.「はい」と答えた場合、それによって負担は減ったと思うか



Q3. 校務用端末を用いて実際に教室で行うようになった業務は何か



●リモートワークについて

【結果】

◆約 6.8%の教職員が通常の勤務日において自宅等からリモートワークを実施し、そのうち約 54%が負担の軽減を実感している。

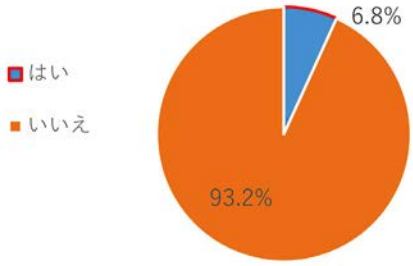
◆自由記述では、新型コロナウイルス感染症の濃厚接触者となった際にリモートワークを実施したことや、改善点として大型で重量のある端末では持ち帰りに苦労したこと、持ち帰りの行いやすい端末選定の要望等が見られた。

【考察】

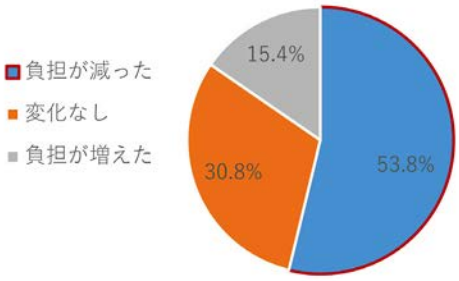
◆学校へ出勤せずに業務を行うことができることが、一定の業務上の負担軽減に寄与する。

Q1. 通常の勤務日において、リモートワークは実施したか
Q2.「はい」と答えた場合、それによって負担は減ったと思うか

Q1. 通常の勤務日において、
リモートワークは実施したか



Q2.「はい」と答えた場合、
それによって負担は減ったと思うか



●その他自由記述

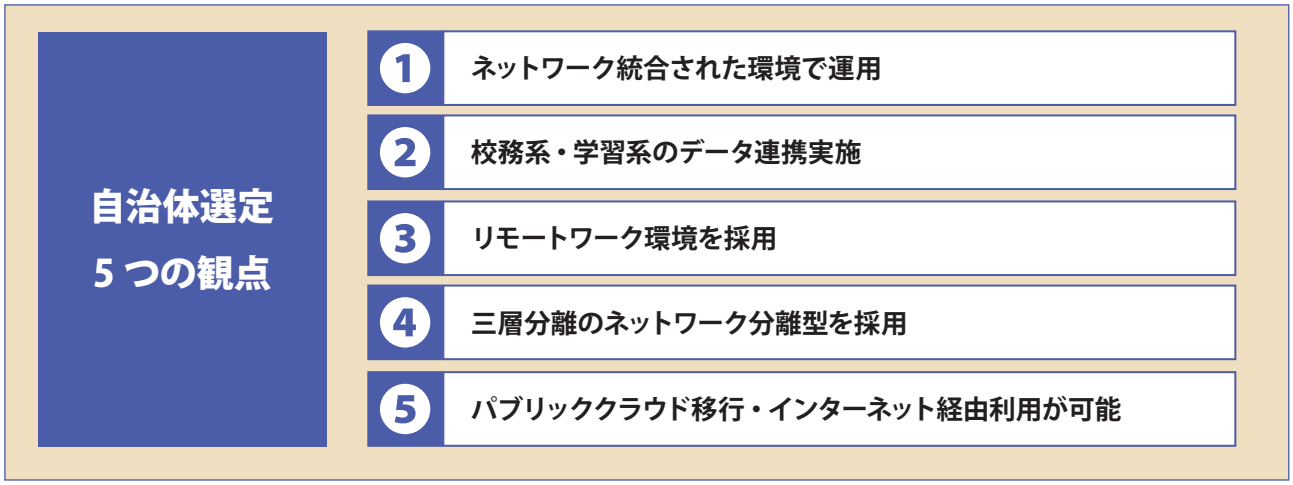
リモートワークを実施したシーン
• 冬休み期間中 • 新型コロナウイルス感染症の濃厚接触者となった期間

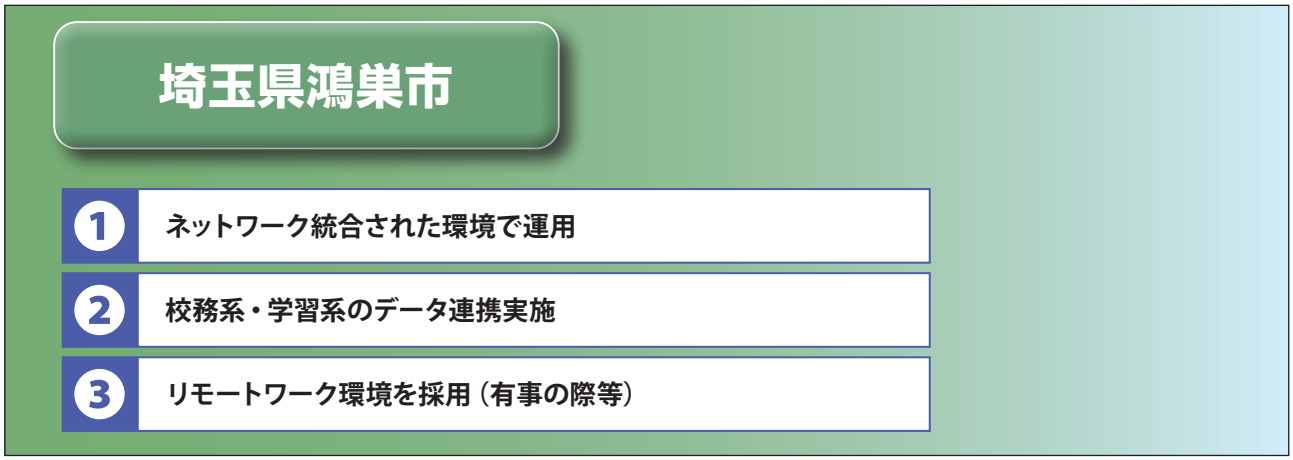
リモートワークを実施したシーン
• 授業の無い冬休み期間中に、従来は学校に出勤して行っていた、次年度の教育課程の作成等の業務を自宅から行えた • 出張後に直帰して自宅から業務を行えた • 新型コロナウイルス感染症の濃厚接触者となった際、自宅待機期間も業務を止めずに済んだ

（2） 先進自治体の取り組み・効果

本節では、図 4-10 の 5 つの観点を基に選定した先進的な取り組みにより教職員の働き方改革を目指している 8 つの自治体を紹介します。取り組みと合わせて、教職員からの声も紹介しますので、是非参考にしてください。（今後の取り組みは一部自治体のみ記載）

図表 4-10　先行自治体の選定観点





埼玉県鴻巣市は令和３年４月より校務系・学習系のネットワークを統合し、複数のシステムをパブリッククラウド上で構築して運用しています。例えば、勤怠管理等のシステムを構築し、各種電子申請が可能です。また、学習データのみならず、校務支援システムの名簿情報を学習 e ポータルに連携し集約しています。

図表 4-11　埼玉県鴻巣市の取り組み

カテゴリ	内　容
具体的な取り組み	・運用ルールをマニュアル化して配布 ・休暇申請の電子化に伴い、服務規程を一部変更 ・新入生の保護者を対象に、ICT 利用の同意書を配布し、データ利用の同意を取得 ・作業ファイルのローカルストレージへの保存、USB メモリへのデータの書き出し、私用パソコンの利用は不可 ・インシデント発生時には、教職員から教育委員会へ連絡し遠隔ロック ・学習データは分かりやすい形で学校に返して活用
教職員の声	「すべての業務を 1 台の端末でどこからでも行えるようになったことで、心理的な余裕が生まれた」 「データはクラウドに保存されているため、セキュリティの心配なく自宅に端末を持ち帰れるようになった」 「出欠情報等が入力と同時に共有されるため、学校全体の状況が瞬時に把握できるようになった」 「個々の学習データから学習状況の把握ができ、より細かい個別の指導ができるようになった」 「職員会議や事務職員同士の打ち合わせでもオンライン会議を利用するようになり、便利になった」

大阪府大阪市

2 校務系・学習系のデータ連携実施

3 リモートワーク環境を採用

大阪府大阪市は平成 29 年より文部科学省と総務省による、スマートスクール・プラットフォーム実証事業に参画し、令和 2 年 9 月より校務系データと学習系データの連携を実現しました。次世代学校支援システムとして、児童生徒ボード、学級ボード、個別の教育支援計画・指導計画ボードを用意しました。また、校務系端末と学習系端末を統一し、教室からも利用可能な環境を用意しました。

図 4-12　大阪府大阪市の取り組み

カテゴリ	内　　容
具体的な取り組み	・ ネットワーク構成はネットワーク分離の環境下でデータ連携を実施 ・ 教職員の端末利用にあたっては、顔認証と ID・PW 認証。教室での利用ではタイムアウト機能を運用
教職員の声	「個別の教育支援計画・個別の指導計画のデータ化により、会議の迅速化と教職員全体の情報共有が進んだ」 「教室から校務データ（出欠）を入力できるので、管理職・養護教諭との児童生徒に関わる情報共有が早くなった」 「職員朝礼の簡略化や廃止、児童生徒理解連絡会の効率化等、情報共有を効率的に行えるようになった」

大阪府箕面市

2 校務系・学習系のデータ連携実施

大阪府箕面市は令和 3 年 9 月より児童生徒への学力・体力・生活の状況調査の結果を成績予測システムと連携することで、児童生徒への指導に活用しています。

図表 4-13　大阪府箕面市の取り組み

カテゴリ	内　　容
具体的な取り組み	・ 児童生徒への学力・体力・生活の状況調査の結果を成績予測システムと連携 ・ 保護者へ成績画面を見せる際は、誤投影防止のため、プリントアウトして活用
教職員の声	「児童生徒別に、学び直しが必要な学習単元を、校種をまたぎ可視化や提示ができるようになった」 「上級生が過去にたどった成績推移と照合することで、児童生徒一人ひとりの今後の成績推移予想が行えるようになった」 「保護者との面談時にも、データに基づいた会話が可能となったことで、学習に関して保護者の納得感を得やすくなった」

茨城県大子町

3 リモートワーク環境を採用（有事の際等）

5 パブリッククラウド移行・インターネット経由利用が可能

茨城県大子町は令和４年度よりクラウド型校務支援システムを導入し、指導者用端末から校務支援システムが利用可能です。また、指導者用端末の持ち帰りを許可し、自宅から校務支援システムへのアクセスも可能となりました。加えて、保護者からの欠席連絡は自動的に校務支援システムに登録することで、働き方改革を推進しています。

図表 4-14　茨城県大子町の取り組み

カテゴリ	内　　容
具体的な取り組み	・ 校務支援システムの導入にあたっては、項目別に複数回に分けてオンライン研修を実施 ・ クラウド側のシステム設定により、機能を制限し、セキュリティを担保(ex: ローカルストレージへのファイルのダウンロードができない 等)
教職員の声	「自宅での持ち帰り業務に際し、USB メモリを用いる必要がなくなったため、セキュリティ面で安心感がある」 「放課後になるまで教室にいたので、従来は放課後にまとめて行っていた校務を教室で行えて助かる」 「手元のパソコンで書類を見やすくなり、職員会議の書類のペーパーレス化が進んだ」 「システムの既読機能により、各種日誌の押印対応が不要になった」 「欠席確認をパソコンでどこからでも行えるようになった」
今後の取り組み	・ 管理職など一部教職員を対象に、私用端末から校務支援システムへアクセスできる環境も準備中 ・ SSO や多要素認証の導入は今後検討予定

愛媛県西条市

3 リモートワーク環境を採用（有事の際等）

愛媛県西条市は令和４年 11 月よりネットワーク分離を維持したまま、校務系システムへアクセスできるリモートデスクトップシステムと多要素認証システム（私用スマートフォンを利用）を導入しました。

図表 4-15　愛媛県西条市の取り組み

カテゴリ	内　　容
具体的な取り組み	・ テレワークによる在宅勤務は、長期休業中又は臨時休業中に限定して許可 ・ 学期中の自宅勤務は、持ち帰り仕事の対応のみ適用可能 ・ 指導者用パソコンや指導者用タブレット端末を自宅に持ち帰ってもセキュリティが担保される設計になっており、今後、運用も可能 ・ 平成 31 年にテレワークを想定したセキュリティポリシーに規定 ・ 教職員用アプリの利用は指導者用端末に限定
教職員の声	「終業後、介護や子育てのための用事を済ませた後、再度学校へ出勤せずとも自宅で校務ができる」 「成績処理業務やグループウェアの利用を自宅から行えるようになった」 「新型コロナウイルス感染症の濃厚接触者になっても、自宅待機した状態で業務を行うことができる」

千葉県船橋市

3 リモートワーク環境を採用

4 三層分離のネットワーク分離型を採用

千葉県船橋市は平成 28 年度に、多要素認証に対応した認証専用デバイスによるリモートアクセス環境を実現しました。認証専用デバイスを持ち帰ることにより、自宅から私用端末で校務を行うことができます。

図表 4-16　千葉県船橋市の取り組み

カテゴリ	内　　容
具体的な取り組み	・私用端末からの印刷を不可にする等、システム設定によりできることを制限し運用 ・認証専用デバイスを持ち出す際は、管理簿に記載 ・校務用端末の持ち帰りは不可 ・紛失等の際には、教育委員会へ連絡
教職員の声	「持ち帰り業務を行う際、USB メモリへのデータ移行等を行う必要がなくなったため、利便性が増した」 「持ち帰り業務を認証のかかったリモート環境から行えるようになったことで、セキュリティ上の安心感が向上した」 「自宅からの業務が容易となったため、早く帰宅することが可能になった」

兵庫県佐用町

1 ネットワーク統合された環境で運用

2 校務系・学習系のデータ連携実施

5 パブリッククラウド移行・インターネット経由利用が可能

兵庫県佐用町は 2022 年 11 月構築段階ですが、校務系・学習系のネットワークを統合し、複数のシステムをパブリッククラウド上で構築していく予定です。また、健康保健データ、校務系データ、学習系データをシステム間連携し、校務支援システムで全てのデータが参照可能になります。

図表 4-17　兵庫県佐用町の取り組み

カテゴリ	内　　容
教職員の声（期待されている効果）	「一台の端末で、職員室以外の場所でも業務を行えるようになるため、職員会議の電子化や、教室からの成績入力等が実現すると期待」 「出欠情報については、保護者アプリから入力＆連携される仕組みを選定しており、負荷軽減を期待」
今後の取り組み	・セキュリティポリシーは文部科学省のガイドラインに準拠して教育委員会で策定予定 ・データ連携にあたってのルールは、OECD のガイドライン等を参考に準拠する予定

東京都渋谷区

2 校務系・学習系のデータ連携実施

3 リモートワーク環境を採用

4 三層分離のネットワーク分離型を採用

東京都渋谷区は、2017 年 9 月から 1 人 1 台端末等の教育 ICT 環境を整備しており、2020 年 9 月に全面的にシステムを再構築しています。再構築にあたり、校務系・学習系システムの各機能や、区内学校・教職員間の情報共有の利便性向上等に取り組みました。また、オンプレ環境にある各種データ（校務情報、端末利用ログ等）をクラウド上に構築したデータ利活用基盤で蓄積・連携させ、BI ツールで可視化（教育ダッシュボード）しています。ダッシュボードでは学校・クラス・個人単位でデータを確認できます。データ利活用においては、「子供一人一人の幸せ（Well-being）の実現」を目指し、教員の子ども理解に基づく指導・支援の充実と子共たちの学校満足度の向上を図っています。

図表 4-17　東京都渋谷区の取り組み

カテゴリ	内　容
具体的な取り組み	・保護者に対しては、取り組みへの理解を得るため、教育ダッシュボードの利活用の目的等を説明する QA 形式の通知を作成し、学校経由で周知 ・区例規集における勤怠管理関係規程等を整備して、出勤記録、休暇・職免等の申請・承認等を紙管理でなく、システム管理できるようにした
教職員の声	「勤怠・旅費管理のシステム化により、、出張申請等がデジタル化して楽になった」 「教育ダッシュボードでクラスや個々の子どもの課題を他の教員と共有し、チームとして迅速に対応できるようになった」 教育ダッシュボードに関しては、「根拠に基づいた働きかけが可能」、「生み出された時間でじっくり話を聞ける」「先手を打った指導・助言・声掛けが可能」といった指導・支援の充実の観点から意見や、「これまで教員同士の長時間の情報交換が時間短縮につながる」といった校務の効率化の観点からの意見もあった
今後の取り組み	・先進的な機能（教員は 1 台の端末で校務系も学習系も利用可能等）は維持・発展させつつつつ、システムのフルクラウド化とゼロトラストの考え方によるセキュリティ確保と運用等の最適化を行い、コスト削減を図る

（3） コスト

◆本章の目的と留意点

本節では、予算折衝時の参考となるように、アクセス認証型のコスト検討の材料となる情報を、多くの自治体が導入している二層分離型、三層分離型と比較しながら記載します。

なお、取り扱うシステム構成図や数値は本書で独自に設定した条件下におけるもので、各自治体固有の条件や実現したい内容によって、変動が予想されます。よって、金額規模や構成要素に関してはあくまでも参考となります。

◆ネットワーク構成とその構成要素

二層分離型、三層分離型、アクセス認証型における構成図（図表 4-19）に基づき、各構成の構成要素を図表 4-20、4-21 に記載しております。コスト要素を整理する際には各自治体の条件や実現したい内容を加味して、下記図表を参考に検討ください。

コストの算出対象は赤枠範囲を対象としております。本比較においては、以下を範囲としております。

・校務支援システムのサーバ基盤（アプリケーションの費用は含まず）
・三層分離構成の境界ファイアウォール（集約拠点や学校設置のネットワーク機器は含まず）

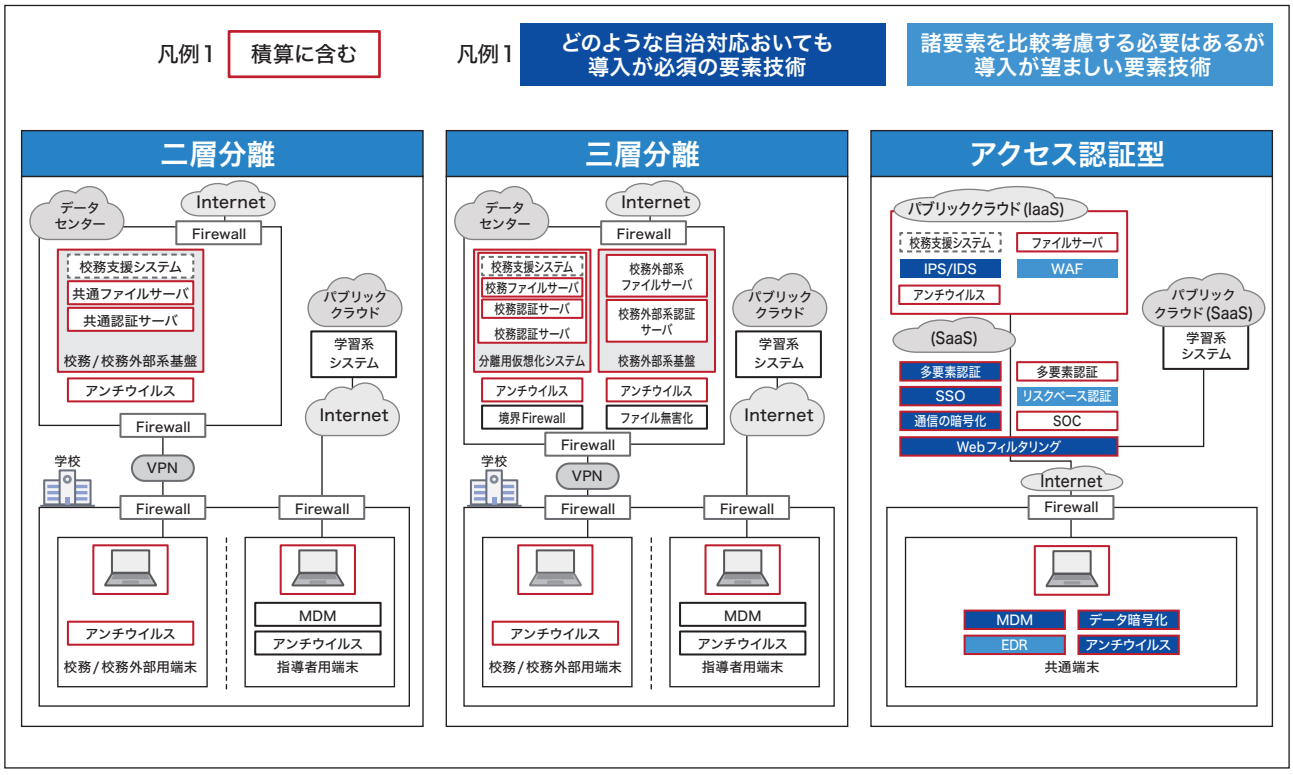
また、構成については以下を採用しております。

・三層分離型
校務系システムと校務外部系システムの分離のために仮想化システムを利用し実現する構成
・アクセス認証型

校務系システムを IaaS 基盤上に設置し、Web フィルタリングや統合 ID 基盤などは SaaS サービスを利用し、利用端末は 1 台に統合する構成

なお二層・三層分離型については現状の構成となっており、今後はより一層のセキュリティ対策が必要と想定されます。

図表 4-19　システム構成図例（二層分離型 / 三層分離型 / アクセス認証型）



図表 4-20　構成要素例（二層分離型 / 三層分離型）

	二層分離-要素	三層分離-要素		イニシャルコスト	ランニングコスト	
		校務系	校務外部系		運用	物品/ライセンス
集約拠点	データセンター	データセンター		集約拠点設計費用 集約拠点構築費用 ハードウェア購入 ソフトウェア購入	アカウント管理 故障時対応	利用料
	-	境界ファイヤーウォール				メーカー保守
	-	ファイル無害化				利用ライセンス
	サーバ基盤	サーバ基盤	サーバ基盤			メーカー保守 OSライセンス
	認証サーバ	認証サーバ	認証サーバ			※ADサーバ想定
	ファイルサーバ	ファイルサーバ	ファイルサーバ			利用ライセンス
	サーバ用ウィルス対策	サーバ用 アンチウイルス	サーバ用 アンチウイルス			利用ライセンス
	-	分離用- 仮想化システム	-			OS/CALライセンス 利用ライセンス
学校	端末	端末	端末	端末購入/初期設定	ヘルプデスク 端末再設定	メーカー保守
	端末用アンチウィルス	端末用アンチウイルス				利用ライセンス
	-	-				

図表 4-21　構成要素例（アクセス認証型）

	アクセス認証-要素	イニシャルコスト	ランニングコスト	
			運用	物品/ライセンス
集約拠点	IaaSサービス ※サーバ基盤/ファイルサーバ	IaaS/SaaS設計費用 IaaS/SaaS構築費用	アカウント管理 セキュリティシステム 故障時対応	利用料
	サーバ用アンチウィルス			利用ライセンス
	統合ID基盤			利用ライセンス
	MDM			利用ライセンス
	多要素認証			利用ライセンス
	Webフィルタリング			利用ライセンス
	SSO			利用ライセンス
学校	端末	端末購入/初期設定 ネットワーク現場調査/設計 ネットワーク設定変更	ヘルプデスク 端末再設定	メーカー保守
	端末用アンチウィルス・EDR			利用ライセンス
	データ暗号化			利用ライセンス

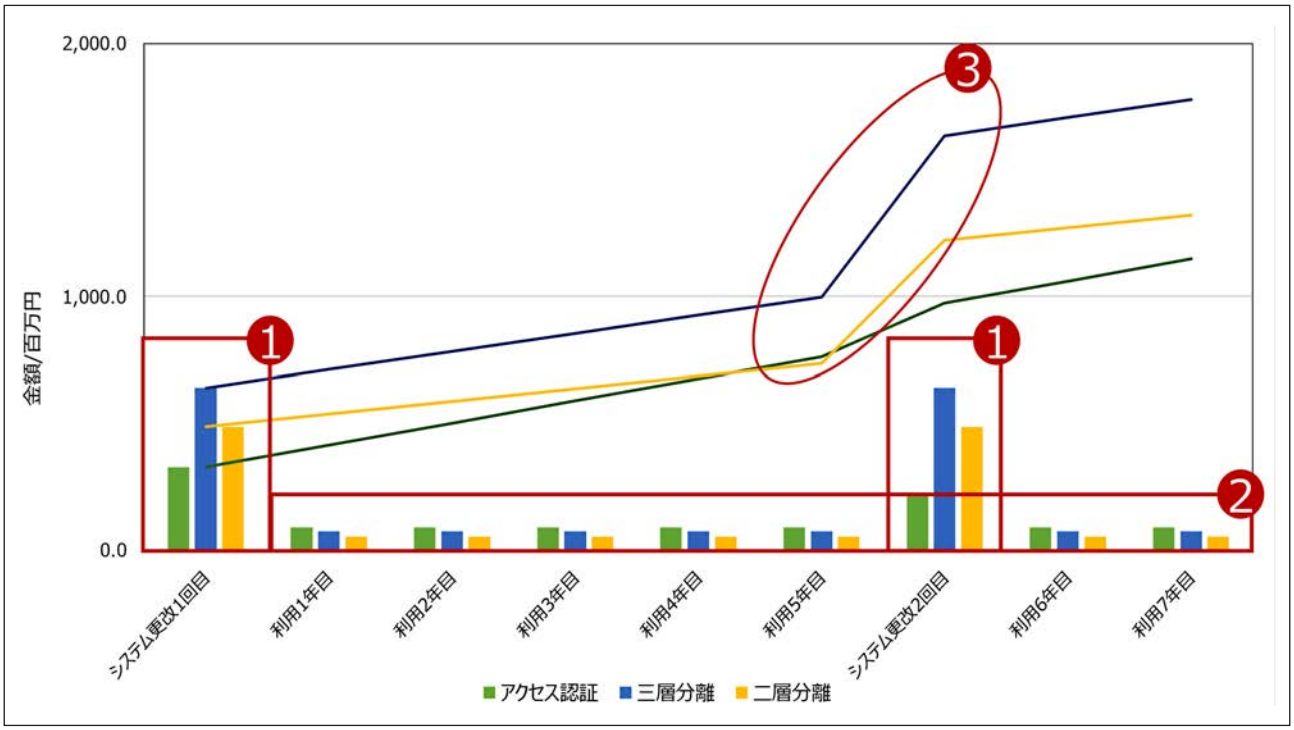
◆コスト推移イメージ

アクセス認証型、二層分離型、三層分離型への移行で発生する一般的なコスト推移のイメージを図表 4-22 に記載し、特徴的な部分を説明します。二層分離型でネットワークを構築し 5 年後も二層分離型で更改するパターン（黄色）、三層分離型でネットワークを構築し 5 年後も三層分離型で更改するパターン（青色）、アクセス認証型でネットワークを構築し､5 年後もアクセス認証型で更改するパターン（緑色）以上の 3 パターンのコスト推移を図表に記載しております。

◆コストを算出する上で設定した前提条件・留意点

・本章で示すコストとは、校務系システムの構築費用及び移行、運用費用を指します
・移行前のシステムは撤去とし、新環境へはデータのみの移行を想定しています
・自治体の規模は学校数は 30 校で各校教員数は 25 名の想定です
・校務系システムのアプリケーションは移行前後を含めて全て同じメーカーの利用を想定しています
・各自治体で実際に算出するコストは各自治体固有の条件や実現したい内容によって、変動が予想されます

図表 4-22　コスト推移イメージ



❶ イニシャル費用

アクセス認証型は二層分離型、三層分離型と比較するとシステム更改の時に発生するイニシャル費用を抑えることができます。

二層分離型、三層分離型においてはネットワークを構築する上で、ハードウェアなどの物品購入費用が発生しますが、アクセス認証型は IaaS や SaaS を利用することで物品購入は不要です。

なお、端末購入費用や利用するライセンス、製品によってはアクセス認証型でも物品購入費用が発生します。

❷ ランニング費用

アクセス認証型は導入後 IaaS や SaaS を利用するため、ライセンス費用が年次で発生します。そのため、二層分離型、三層分離型と比較すると、年次で発生するランニング費用は上がります。

❸ システム更改費用

アクセス認証型で IaaS や SaaS を利用している場合は、ハードウェアを調達することなく、サービスとして利用することができるため継続した利用が可能です。そのため、5 ～ 6 年周期で行ってきたシステム更改が不要となります。

なお、端末購入費用や利用する校務支援システムのアプリケーションの入れ替えなどで費用が発生する場合があります。

一方、二層分離型、三層分離型は、前回のシステム更改時と同等の費用が発生します。

事業推進委員

※敬称略　所属・役職は令和５年３月時点のものです。

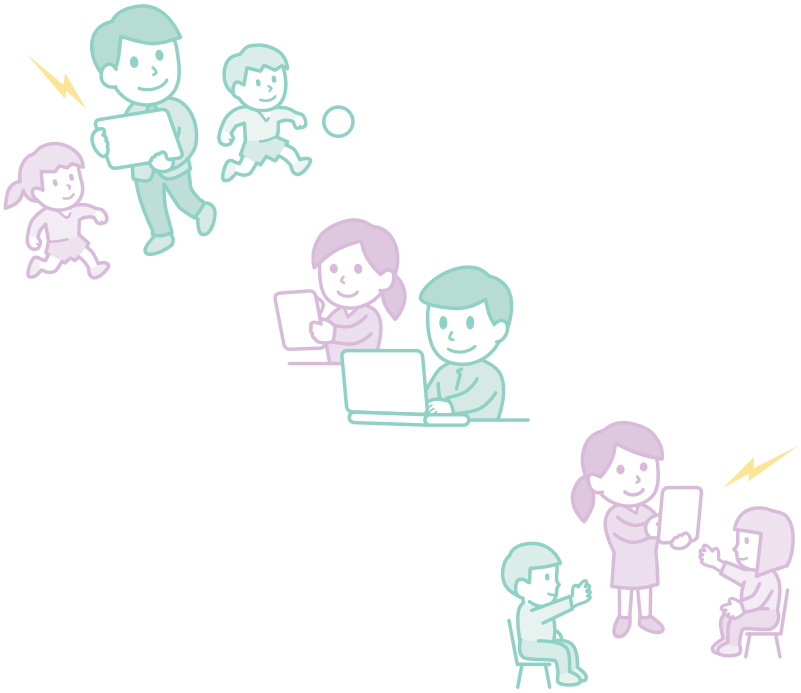
氏　　名	所　　属
高橋　純（委員長）	東京学芸大学 教育学部 教授
髙橋　邦夫	合同会社 KU コンサルティング 代表
西田　光昭	柏市教育委員会 教育研究専門アドバイザー
林山　耕寿	シスコシステムズ合同会社 ビジネスディベロップメントマネージャー
藤村　裕一	鳴門教育大学大学院 学校教育研究科 教授

フィールド

氏　　名	所　　属
平崎　智章	東京都武蔵村山市 教育部 教育総務課 課長
池谷　正太郎	東京都武蔵村山市 教育部 教育総務課 教育政策係 係長
阿部　詩織	東京都武蔵村山市 教育部 教育総務課 教育政策係

校務系・学習系ネットワークの連携における
導入・運用・活用に関するガイドブック
令和４年度
校務系・学習系ネットワークの連携に関する実証研究事業
（令和５年３月発行）

東日本電信電話株式会社
〒 163-8019　東京都新宿区西新宿 3-19-2



文部科学省　初等中等教育局学校デジタル化プロジェクトチーム
〒100-8959 東京都千代田区霞が関 3-2-2　　TEL：03-5253-4111

NTT 東日本
東日本電信電話株式会社
〒163-8019 東京都新宿区西新宿 3-19-2
URL:http://www.ntt-east.co.jp