

次世代校務DX環境と教育情報セキュリティ

初等中等教育局 参事官（デジタル学習基盤担当）付
校務データ連携企画係 係長 伊藤 遼吾

ICTは「個別最適な学び」と「協働的な学び」の充実に不可欠なツールであり、こどもたちは文房具のように使いこなしている。一方、教職員の業務では・・・

依然として、多くの校務がアナログ・紙ベースで行われている。

多くの自治体ではシステムを自前サーバに構築し、閉域網で稼働させている。

校務用端末も職員室に固定されていることが多く、ネットワーク環境として時代の流れに合っていない。

“ICTは長時間勤務を解消して、**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”

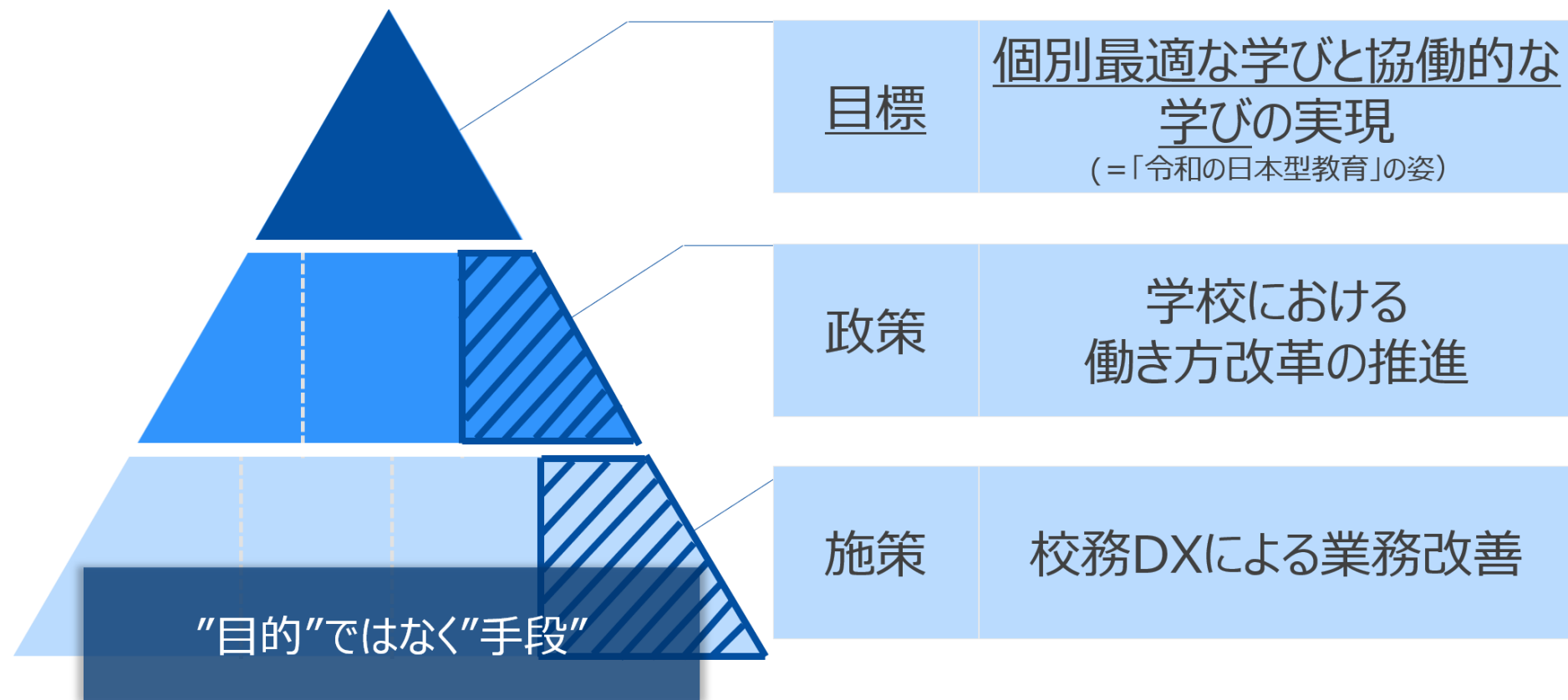
『令和の日本型学校教育（答申）』において、ICTの活用に関する基本的な考え方として記載。
GIGAスクール時代の教育DXや働き方改革の流れに適合するためには、校務DXが必須。

Before

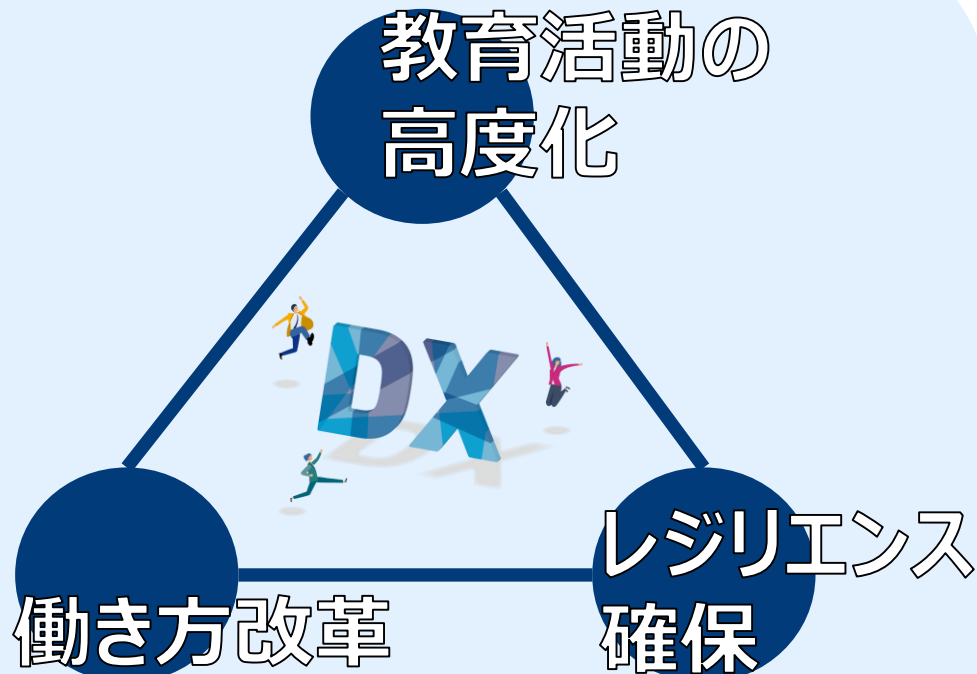
- ✓ 校務処理の多くが職員室に限定
- ✓ 紙ベースの業務が主流
- ✓ 教育委員会ごとにシステムが異なるため
人事異動の際の負担が大きい
- ✓ 学習系データと校務系データとの連携が困難
- ✓ 災害対策が不十分な自前サーバで稼働

After

- ✓ **ロケーションフリー化**により、
働き方の選択肢が増加
- ✓ クラウドベースの業務が主流となり、
ペーパーレス化
- ✓ システムの共同利用により、
人事異動の負担が大幅軽減
- ✓ **ネットワーク統合**によりデータ連携が容易になり、**ダッシュボード機能**が実装
- ✓ クラウド利用により、災害によるデータ喪失等のリスク低減



次世代校務DX環境の整備はこれらの礎



“次世代”＝クラウド上での実施を前提 

学校における働き方改革

- ・ 汎用型クラウドツールの積極的活用による情報共有の迅速化・活性化、事務負担軽減
- ・ ロケーションフリー化による場所や時間を選ばない働き方の実現

教育活動の高度化

- ・ データ連携によるダッシュボード実装により、個別最適な学びやきめ細かな指導、教育政策の改善を実現

教育現場のレジリエンス確保

- ・ クラウド活用により、非常時のデータ損失等を防止



今の環境でできる校務DX

環境整備を伴う校務DX

教育現場のセキュリティ対策

校務DXチェックリスト

本日はここが中心

次世代校務 DX ガイドブック

-都道府県域内全体で取組を進めるために-

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

令和7年3月

主に都道府県域内全体で次世代校務DX環境を整備・運用する際に必要となる取組やポイントを整理

目次

はじめに

1. 次世代校務 DX の姿
2. 次世代校務 DX を実現するために必要な取組

2 - 1. 今の環境でできる校務 DX の実施

- (1) 従来業務の見直し
- (2) 汎用クラウドツールの活用
- (3) 生成 AI の利活用

2 - 2. 環境整備を伴う校務 DX の実施

- (1) ビジョン・ロードマップの設定
- (2) 体制整備
- (3) 次世代校務 DX 環境の整備
 - ① 関連システムの共同調達・共同利用に向けた事前検討
 - ② 次世代校務 DX 環境の仕様検討
- (4) ルール整備
- (5) 研修等の実施

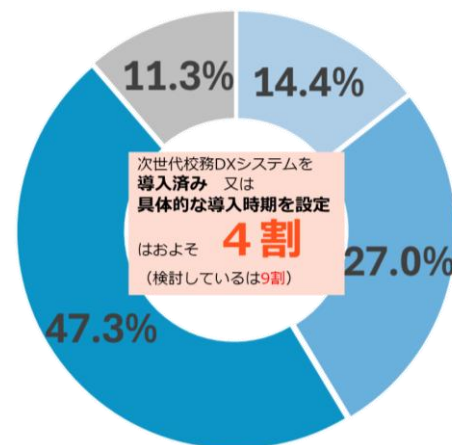
3. 参考資料

校務支援システムに搭載することが想定される帳票の参考様式 等

次世代校務DX環境の整備

都道府県教育委員会の主導の下で、関連システムを**共同調達・共同利用**しながら、次世代校務DX環境を整備・運用

都道府県教育委員会と域内市町村教委は各々が独自に取り組もうとしていることを活かしつつも、全体最適を目指し、**丁寧な対話**と適切な**役割分担**が必要



■ 導入済み ■ 具体的な導入時期を設定している ■ 導入時期は未定だが検討している ■ 検討していない

【出典】文部科学省「GIGAスクール構想の下での校務DXチェックリスト」（令和8年3月）

次世代校務DX環境の整備の要素

- ア. 強固なアクセス制御による対策の実施 ← セキュリティ対策（いわゆる“ゼロトラ”）
- イ. ネットワーク統合 ← ロケーションフリー・データ連携
- ウ. クラウド型校務支援システムの整備
- エ. データの可視化・利活用を行うための機能の整備 ← ダッシュボード実装

国・地方における
data drivenな教育政策推進

校務処理の更なる効率化
（重複入力の徹底排除等）

支援を要する子供の
早期発見・支援

端末整備コストの減
（2台→1台）

学習指導・学校経営の
高度化

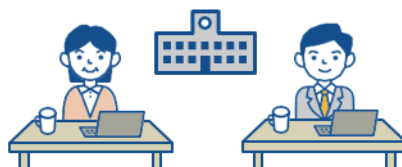
人事異動時の負担軽減

大規模災害等、緊急事態への
レジリエンス向上

ロケーションフリー化
（USB等の持ち出しリスクも減）

保護者や地域人材との
コミュニケーション活性化

システム調達コスト減・
共同調達も更に促進

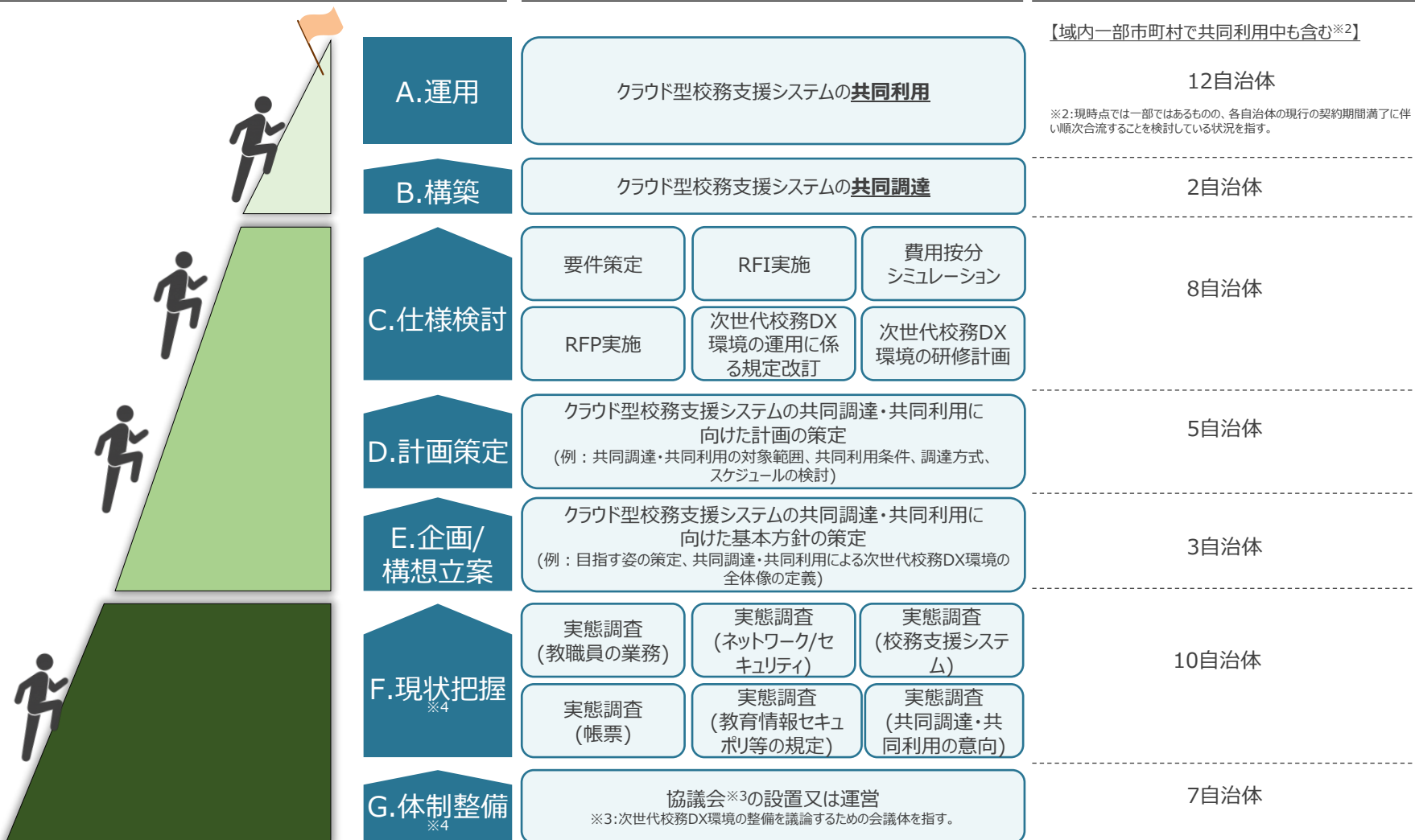


次世代校務DX環境の整備ステータス(2026年4月時点※1)

次世代校務DX環境の整備に向けた工程

各工程における実施内容例

対象都道府県



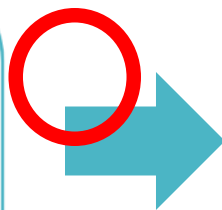
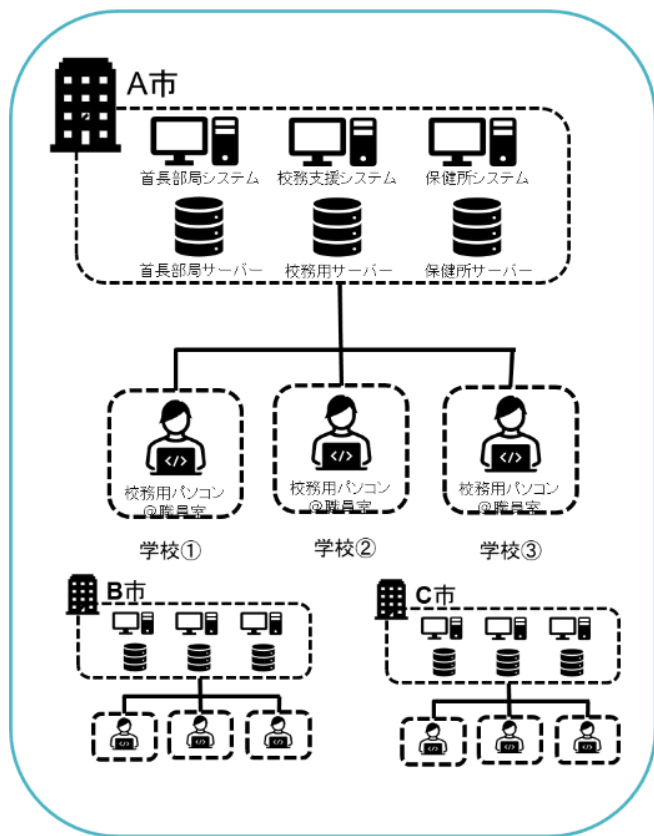
※1:校務DX等加速化事業(事業II)において実施した都道府県教育委員会向けの調査を基に作成。

※4:必ずしも「体制整備」から「現状把握」に進む取り組みだけでなく、「現状把握」と並行、もしくは「現状把握」を先行して、次世代校務DX環境の整備を議論するための「体制整備」に取り組んでいる場合も含む。

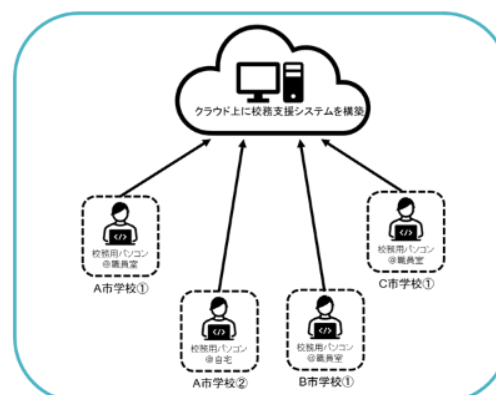
次世代校務DX環境の整備 -クラウド型校務支援システムの整備-

外部システムからのデータ連携における接続ポイントを共通で利用できる、マルチテナント構成のクラウド型校務支援システムを整備することをいう

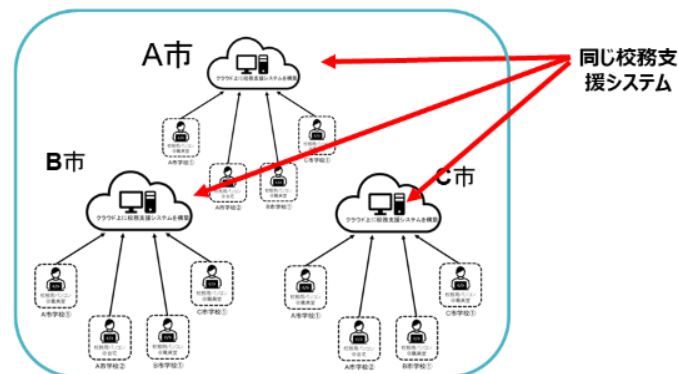
これまでの校務支援システム



マルチテナント構成の校務支援システム

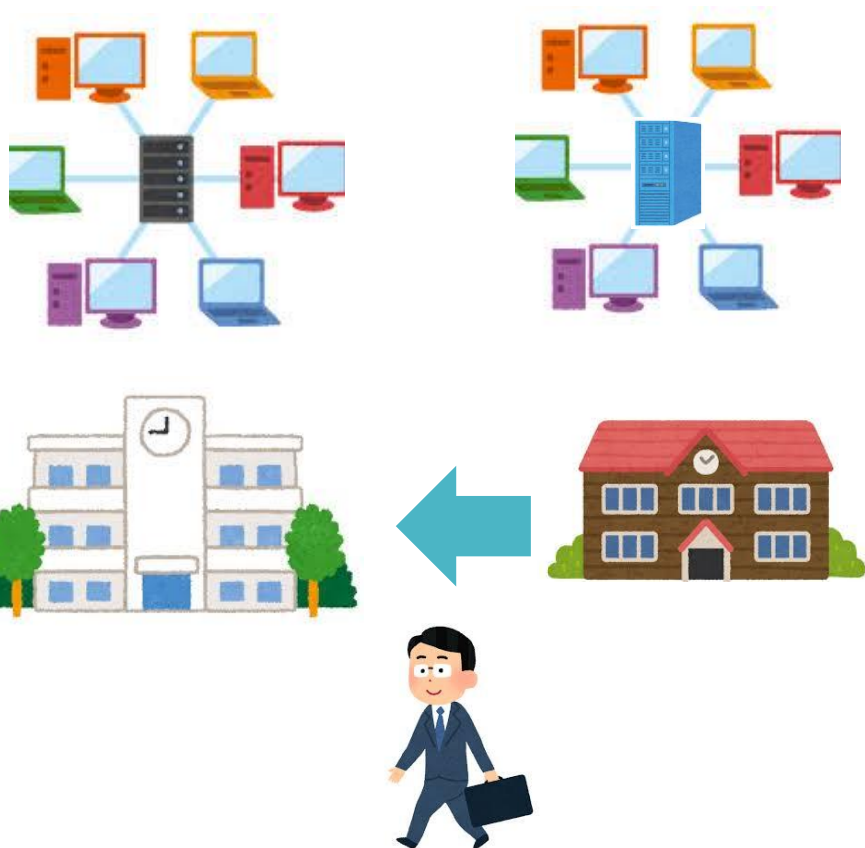


シングルテナント構成の校務支援システム

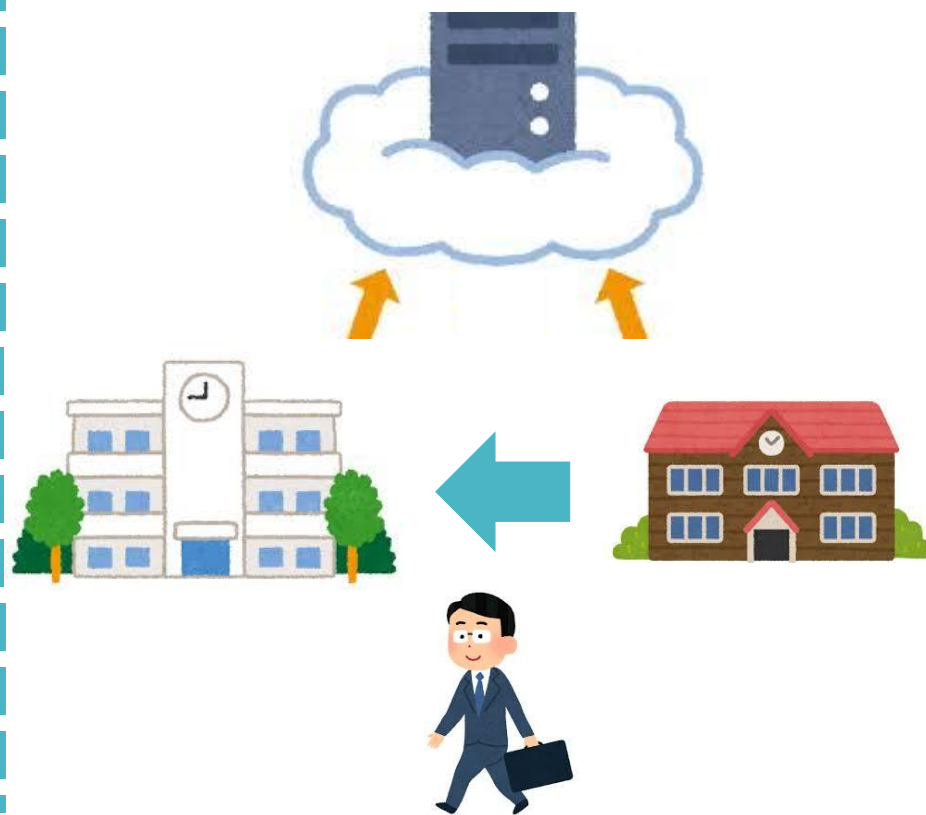


負担が少ないのはどちらですか？

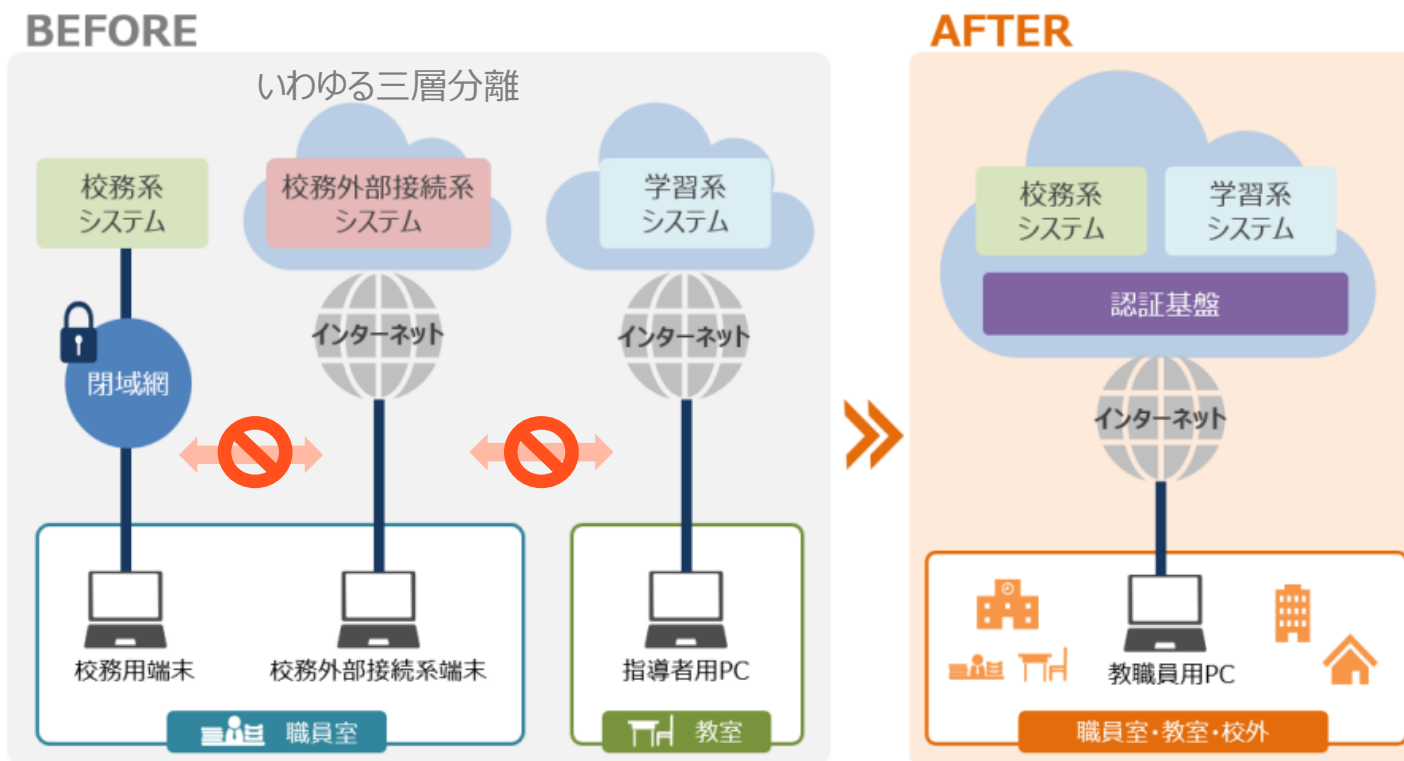
異動したら覚えなおし



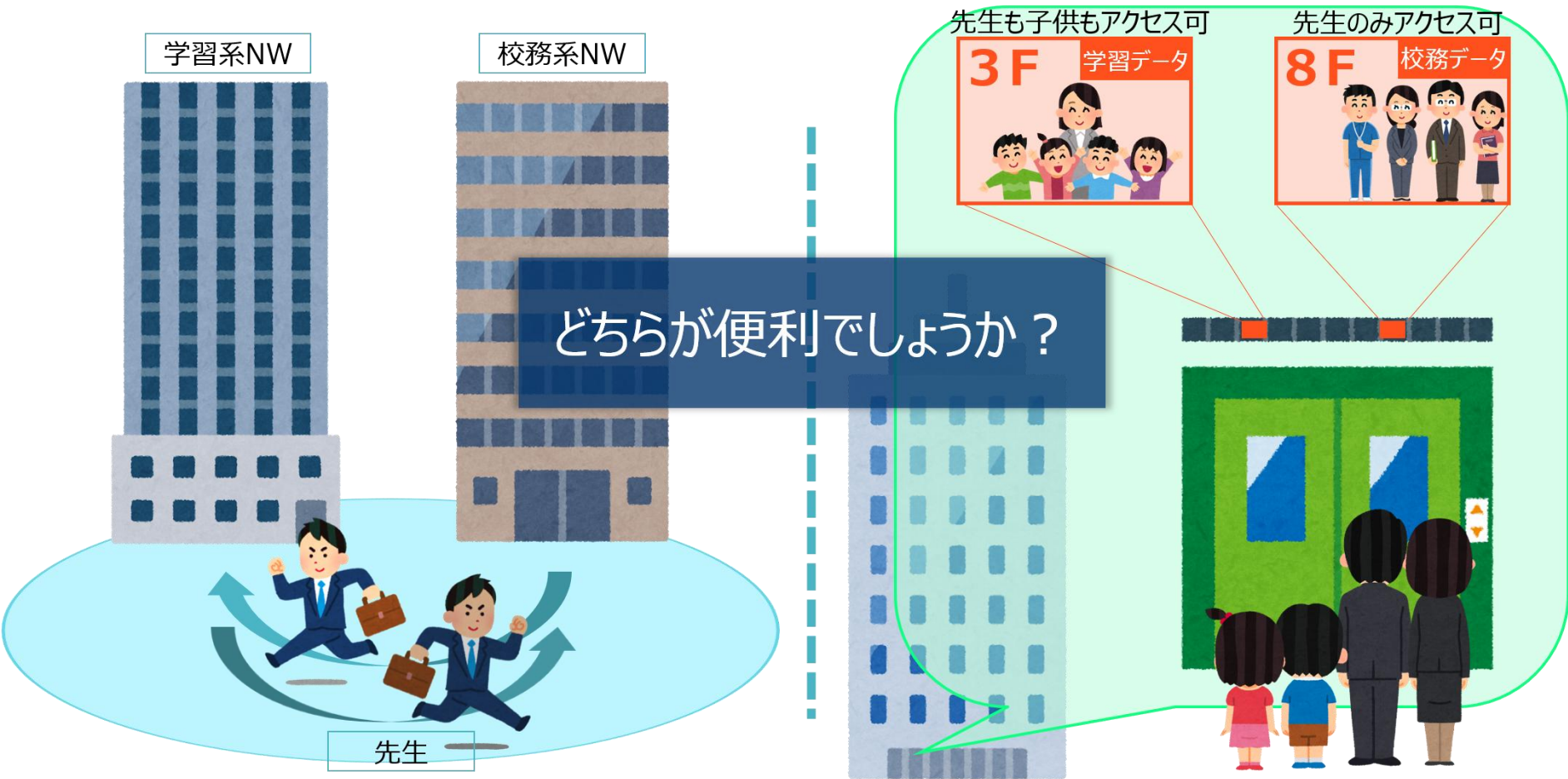
異動してもシステムが同じ



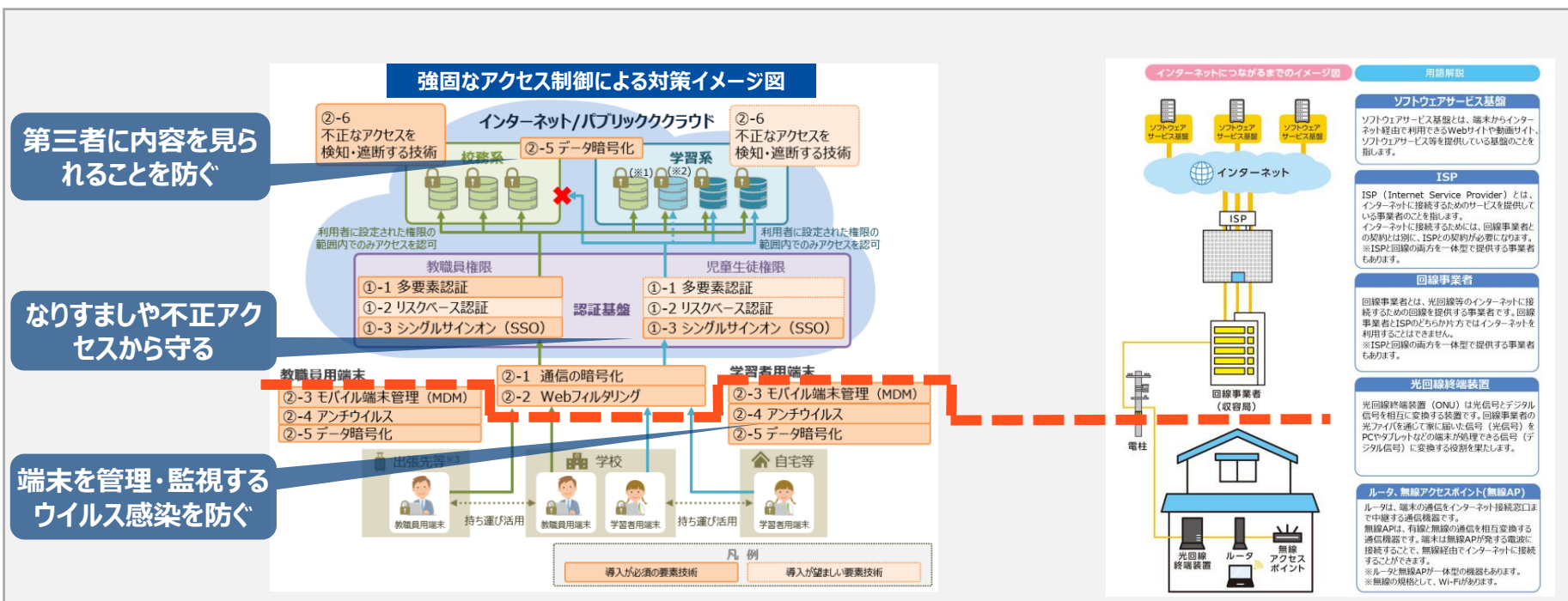
既存のネットワークを統合することで、学校内外どこからでも
教職員用の端末から校務系・学習系システムいずれにもアクセス可能に



次世代校務DX環境の整備 -ネットワーク統合-



児童生徒の成績情報等の重要性の高い情報をクラウド上で扱うため、**情報ごとに真に必要な者に限定してアクセスできるように対策することが重要**



大切なものを保管しておきたいのはどちらですか？

ファイル（紙）ベース

クラウドベース



データ統合・可視化により、児童生徒へのきめ細かな指導や、効果的な学校経営が可能に



【ポイント】

- ・従来の教職員の観察や見取りによる情報とのバランスをとること
- ・どのようなデータ可視化ツールが適切か定め、必要なデータを選択することが必要

現状・課題

- 現行の**GIGA環境を活用した教育現場ではクラウド活用が進んでいる**
- GIGAスクール構想の進展に伴い**クラウドサービス事業者との契約が増加**
- **重要性の高い情報を取り扱う校務も、次世代校務DXの進展に伴いクラウド環境に移行予定**
- セキュリティ対策を講じるに当たっては、情報資産を取り扱う当事者のルール順守などを通じた対策である**人的セキュリティの確保が重要**

教育現場に求められるセキュリティ対策は高度化しているが・・・

一方で、

- 独自の教育情報セキュリティポリシーを策定している教育委員会は**半数程度**
- 児童生徒がコンピュータを活用した学習活動の実施などにおいて、日常的に情報システムにアクセスする機会があるなど、**地方公共団体の他の行政事務とは異なる特徴を有することから、地方自治体の情報セキュリティポリシーの準用では不十分**
- 教育現場の環境は変化しており、**新たな環境に対応したセキュリティ対策の見直し**が重要

自治体のセキュリティポリシーとは別に、教育情報セキュリティポリシーを教育委員会独自に策定していますか。



出典：文部科学省「GIGAスクール構想の下での校務DXチェックリスト」（令和8年3月）

➤ 学校が何をやっていいのか、悪いのかわからない

児童生徒が閲覧できる場所に成績情報等の校務情報が混じる

→児童生徒や保護者の閲覧

重要性の高い情報の持ち出し・私用端末への転送

→意図しない情報漏洩

➤ 教育委員会が学校現場におけるセキュリティリスクを把握できない

セキュリティインシデントが発生した際に

- 原因の特定が困難
- 報告ルートが設定されていない
- 責任の所在があいまい
- 罰則等の明確な規定が存在しない



- 再発防止策を検討できない
- 教育委員会の状況把握が遅れ大きな事故に
- 不正行為や過失であるかを認定する根拠がない
- 事故の範囲や影響を把握できない

せっかく進んだGIGAの後退につながりかねない

情報セキュリティ対策の基本（基本的な考え方）

- 情報セキュリティ対策は**時代に即した環境を十分に利活用し、質の高い教育、円滑な学校運営を実現**するために行われるもの。**セキュリティ対策が目的化し、これらを阻害することはあってはならない**。インシデントを恐れるあまり何もかも規制する、ということとならないよう、「何を」「何から」「どのように」守るかを意識した**セキュリティ対策**を講じる必要がある

- ✓ 何を守るのか？→情報資産

（※）情報資産とは：

学校が保有している情報そのもの（文書やデータファイル）や、その情報を生成・保管・流通する媒体（紙、ネットワーク、サーバ、端末等）

- ✓ 何から守るのか？→セキュリティを侵害して損害を引き起こす要因（＝脅威）

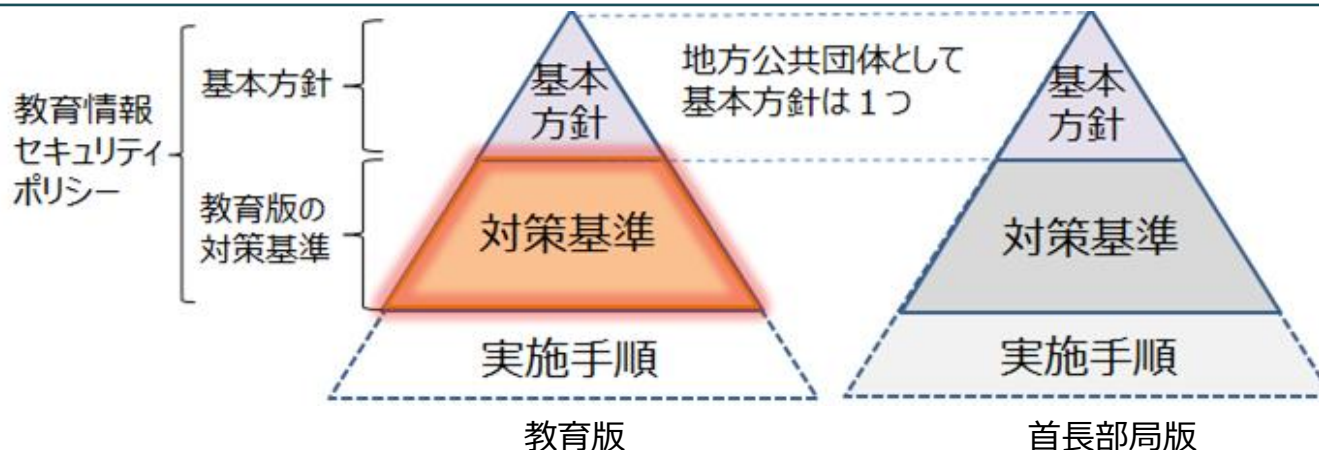
- ✓ どのように守るのか？→人的セキュリティ・技術的セキュリティ・物理的セキュリティ対策を組み合わせる

物理的セキュリティ対策	サーバ、通信回線等の機器の設置や設定、保守管理に関する措置や機器等の管理区域の適切な管理等の物理的な方法を通じて情報資産を守る対策
人的セキュリティ対策	情報資産を取り扱う当事者の ルール遵守 などを通じて情報資産を守る対策
技術的セキュリティ対策	ハードウェア・ソフトウェアやネットワークなどに対するアクセス制御、不正プログラム対策、不正アクセス対策等の技術的な安全管理措置を通じて情報資産を守る対策

- **情報セキュリティ対策に100%は無い。インシデントは起こる、人は失敗をする**という前提で対策を講じる必要がある

情報セキュリティ対策の基本（教育情報セキュリティポリシー）

- 教育情報セキュリティポリシーは「基本方針」と「対策基準」から成る。
- 教育委員会は、教育現場独自の「対策基準」の策定・見直しを実施する。
- 教育現場が教育情報セキュリティポリシーを適切に履行できるよう、各学校は「対策基準」を実施するための具体的な手順等をまとめたマニュアルである「実施手順」を定める
- 対策基準の策定に際する参考資料として文科省が「教育情報セキュリティポリシーに関するガイドライン」を公表



「情報セキュリティ」の体系

基本方針：各地方公共団体の情報セキュリティ対策における基本的な考え方を定めるもの。教育情報セキュリティポリシーにおいては地方公共団体が策定したものを準用。

対策基準：基本方針に基づき全ての情報システムに共通の情報セキュリティ対策の基準を定めるもの。ガイドラインに基づき各教育委員会が策定・見直しを行う。

実施手順：対策基準に基づき具体的なシステムや手順、手続に展開して個別の実施事項を定めるもの。教育委員会等は各自治体の実態を踏まえた実施手順のひな形を策定し、各学校はひな形に基づき策定・見直しを行う。

- 文部科学省は平成29年10月に、教育委員会等が**教育情報セキュリティポリシー**（※1）の策定や見直しを行う際の参考として、「**教育情報セキュリティポリシーに関するガイドライン**」（以下「ガイドライン」という。）を策定。
- 児童生徒の学びや学校の働き方の変化に合わせて、教育現場で必要とされる情報セキュリティ対策は変化しており、これまで随時ガイドラインの改訂を実施。

【令和元年12月改訂】

GIGAスクール構想の始動時に対応するため改訂

【令和3年5月改訂】

新たに必要なセキュリティ対策やクラウドサービスの活用を前提としたネットワーク構成等の課題に対応するため改訂

【令和4年3月改訂】

アクセス制御による対策の詳細な技術的対策の追記と、「ネットワーク分離による対策」、「アクセス制御による対策」を明確に記述するため改訂

【令和6年1月改訂】

次世代の校務DX環境（※2）の整備を見据えた情報セキュリティの考え方の提示、関連法令・指針の改訂・改正に伴う対応、各自治体における教育情報セキュリティポリシーの策定推進に向けた読みやすさ向上のため改訂

「教育情報セキュリティポリシーに関するガイドライン」 目次

はじめに

第1編 総則

第1章 本ガイドラインの目的等

第2章 地方公共団体における

教育情報セキュリティの考え方

第3章 教育現場におけるクラウドの活用について

第2編 教育情報セキュリティ対策基準

1. 対象範囲及び用語説明

2. 組織体制

3. 情報資産の分類と管理方法

4. 物理的セキュリティ対策

5. 人的セキュリティ対策

6. 技術的セキュリティ

7. 運用

8. 外部委託

9. SaaS型パブリッククラウドサービスの利用

10. 評価・見直し

第3編 付録

令和7年3月の改訂は、GIGAスクール構想の進展により教育現場のクラウド活用が進んでいること等を踏まえ、**情報資産の分類・仕分け・管理方法の見直し及び次世代校務DX環境への移行を進める上で必要となるセキュリティ対策に関する記載の見直し**を主な目的として実施。

※1 教育分野に関して、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書

※2 次世代校務DX（クラウド上での校務実施を前提とし、ロケーションフリーやデータ利活用・データ連携を通じて、学校の働き方改革・教育活動の高度化・教育現場におけるレジリエンス確保の実現に資する新しい校務の在り方）を実現するために整備が必要となる環境

総務省令によるサイバーセキュリティ対策の義務化

概要

- 地方自治法の一部を改正する法律（令和6年法律第65号。以下「改正法」という。）は、令和6年6月26日に公布され、教育委員会を含めた普通地方公共団体は、情報システムの適正な利用を図るために必要な措置を講じなければならないものとされたが※1、改正規則は、改正法により改正された地方自治法を実施するため、**サイバーセキュリティの確保等の情報システムの適正な利用を図るために必要な措置について、規定を整備するもの。**
- 改正規則は**令和9年7月1日に施行予定**であり、施行日までに必要な準備を行う必要がある。

総務省令の内容

第1 サイバーセキュリティに係る必要な措置に関する事項

地方自治法第244条の5第2項の規定による必要な措置は、次のとおり。

- ① **組織体制の整備**（新規則第16条の3第1項第1号関係）
- ② **適切な情報資産の分類及び管理の実施**（新規則第16条の3第1項第2号関係）
- ③ **物理的なサイバーセキュリティに関する対策の適切な実施**（新規則第16条の3第1項第3号関係）
- ④ **人的なサイバーセキュリティに関する対策の適切な実施**（新規則第16条の3第1項第4号関係）
- ⑤ **技術的なサイバーセキュリティに関する対策の適切な実施**（新規則第16条の3第1項第5号関係）
- ⑥ **サイバーセキュリティに関する対策の適切な運用の実施**（新規則第16条の3第1項第6号関係）
- ⑦ **適切な業務委託の実施及び外部サービス（クラウドサービス）の適切な利用**（新規則第16条の3第1項第7号）
- ⑧ **サイバーセキュリティに関する対策の適切な評価及び見直しの実施**（新規則第16条の3第1項第8号）

ただし、国又は他の地方公共団体の重要な情報又は重要な情報システムに影響を及ぼす可能性があるネットワークに電気通信回線で直接又は間接に接続されていない地方公共団体であって、かつ、個人情報を多量に保有していない団体及び公安委員会についてはこの限りではない。

第2 施行期日

改正規則の施行期日は、令和9年7月1日。

第3 経過措置

改正規則の施行の際現に存する情報システム等及び現に実施されている業務委託については、新規則第16条の3第1項第5号（技術的なサイバーセキュリティに関する対策）及び第7号（業務委託及び外部サービス（クラウドサービス）の利用）の規定にかかわらず、なお従前の例による。

第4 留意事項

第1に掲げた必要な措置の具体的な内容に関しては、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参照

**総務省令を踏まえ教育現場の状況を考慮しながら、
「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8年度末までに改訂予定**

※1 地方自治法（昭和22年法律第67号）第244条の5第2項、地方独立行政法人法（平成15年法律第118号）第24条の2において準用する場合を含む。

重要性分類に基づく情報資産の取扱い（基本的な考え方）

- 教育現場の情報資産を適切に守るためには、情報資産をセキュリティ侵害による影響度（被害の大きさ）に応じて4段階に分類・仕分けし、その**重要性に応じた対策を講じる必要がある**
- また、それらの情報に**誰がアクセスすることが想定されるか（アクセス主体）を整理した上で対策を検討**する必要がある
- **重要性が高い情報であればあるほどセキュリティ対策はより強固にすべき**であり、アクセス権限を与える関係者を制限する必要がある

重要性分類	各情報資産にアクセスする主体		
	教職員等・教育委員会	教職員等・教育委員会・児童生徒・保護者	不特定多数
I：情報が侵害された場合に甚大な被害が想定され、学校もしくは特定個人が著しい不利益を被る情報であり、要配慮個人情報を含むもの等	業務に係る特定の教職員等・教育委員会のみがアクセスすることが想定される情報 指導要録原本	業務に係る特定の教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含む情報 健康診断票	
II：情報が侵害された場合に大きな被害が想定され、学校もしくは特定個人が大きな不利益を被る情報であり、重要性分類Iには該当しないものの機密性の高いもの（健康、指導、成績、進路に関わる情報等）等	業務に係る教職員等・教育委員会のみがアクセスすることが想定される情報 調査書、進路希望調査	業務に係る教職員等・教育委員会に加えて、児童生徒またはその保護者がアクセスする場合、児童生徒本人の情報のみにアクセスすることが想定される、要配慮個人情報等を含まない情報 通知表、定期考査・テスト等の採点結果	
III：情報が侵害された場合に学校もしくは特定個人が不利益を被る情報であり、II以上には該当しないものの侵害の影響を無視できないもの（学校運営・学習活動・学習指導など）	教職員等全員・教育委員会がアクセスすることが想定される情報 出席簿	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される情報 授業用教材、児童生徒の学習記録（確認テスト、ワークシート、日常的な簡易な健康観察等）	
IV：上記以外の、セキュリティ侵害が発生しても学校事務及び教育活動の実施にほとんど影響を及ぼさない情報	教職員等全員・教育委員会がアクセスすることが想定される、III以上を除く情報	教職員等全員・教育委員会に加えて、児童生徒及び保護者がアクセスすることが想定される、III以上を除く情報	不特定多数に公開することが想定される情報 学校紹介パンフレット、学校・学園ホームページ掲載情報

情報が漏れることで生命が脅かされたり、差別につながるような情報。

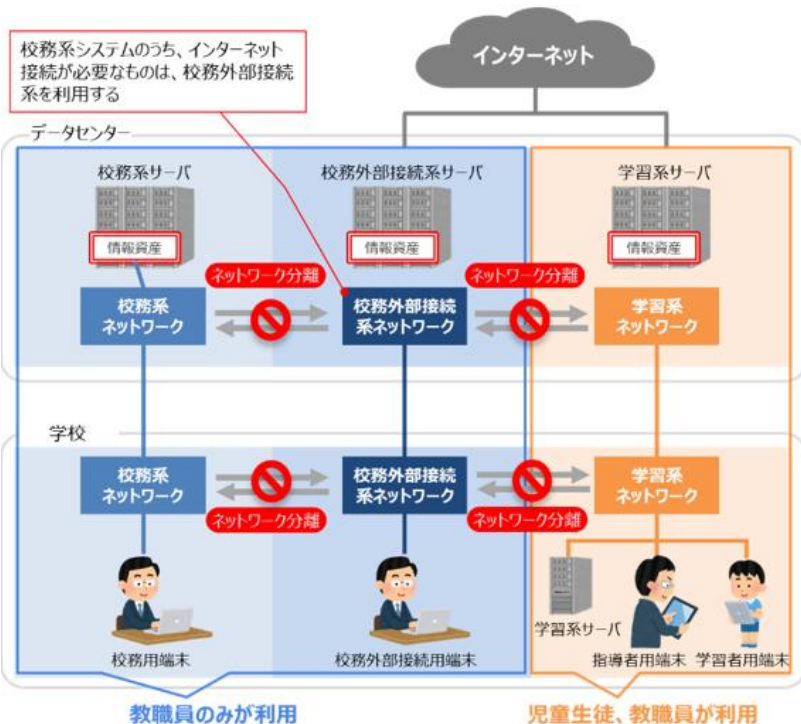
いわゆる校務系情報。児童生徒がアクセスするとしても自分の情報のみ。

いわゆる学習系情報。学習活動で生み出される情報全般。

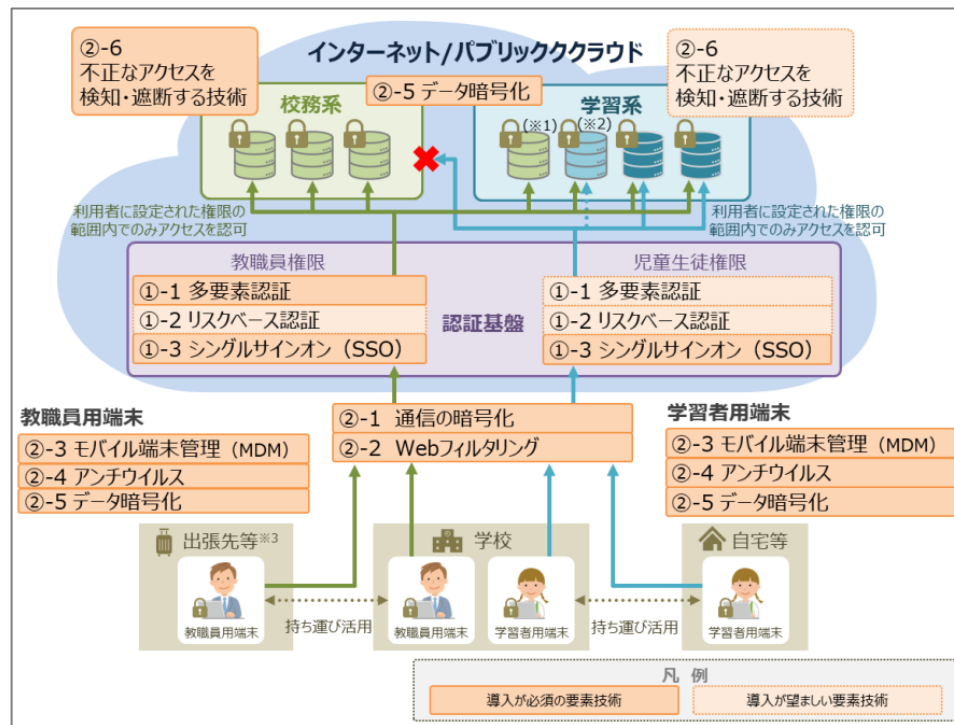
公表情報。

- クラウド上で重要性の高い情報を扱うことを前提とする次世代校務DXを実現させるためには、重要な情報にアクセスできるネットワークをその他のネットワークと分けることで情報を守る従来のネットワーク分離型のセキュリティ対策から、必要な人が必要な情報にのみアクセスできるように権限を設定することで情報を守る**強固なアクセス制御によるセキュリティ対策への移行**が必要

ネットワーク分離型（境界防御型）のセキュリティ対策



強固なアクセス制御によるセキュリティ対策



(出典)「教育情報セキュリティポリシーハンドブック」(R7.3) P24

- 強固なアクセス制御によるセキュリティ対策の要素として記載されている技術は、次世代校務 DX 環境に移行する際に**特に留意すべき要素技術を整理**したもの。
- これらの技術を網羅したからといって**確実なセキュリティが確保される**というものではないため、実際の検討に当たっては、各教育委員会・学校の**既存のネットワーク環境やセキュリティ対策、端末の OS、コスト面等を考慮した上で、導入した要素技術が十分な効果を発揮するよう、必要な対策を講じる必要**がある

教育委員会担当者の情報セキュリティに関する理解の深化を図り、自治体自らが教育情報セキュリティポリシーの策定・見直しを適切に実施できるように、教育現場における情報セキュリティの基本的な考え方及びガイドラインの基本的な考え方とポイントを解説した「教育情報セキュリティポリシーハンドブック」を策定



目次

第1章 はじめに

第2章 教育現場における情報セキュリティのポイント

- 2-1 教育現場における情報セキュリティの基本的な考え方
- 2-2 何を守るか
- 2-3 何から守るか
- 2-4 どのように守るか

第3章 教育情報セキュリティポリシー策定の際のポイント

- 3-1 教育情報セキュリティポリシーとは
- 3-2 「教育情報セキュリティポリシーに関するガイドライン」のポイント
 - (1) 対象範囲及び用語説明
 - (2) 組織体制
 - (3) 情報資産の分類と管理方法
 - (4) 物理的セキュリティ
 - (5) 人的セキュリティ
 - (6) 技術的セキュリティ
 - (7) 運用
 - (8) 外部委託
 - (9) SaaS 型パブリッククラウドサービスの利用
 - (10) 評価・見直し

校内研修のさらなる充実を図り、教員の資質能力の向上を目指す独立行政法人教職員支援機構（NITS）と協力し、**教育現場におけるセキュリティ対策にする基本的な考え方やポイントを解説した動画教材「校内研修シリーズ」**を作成・公表。

教育現場におけるセキュリティ対策Ⅰ：校内研修シリーズ No.181



- ①教育現場におけるセキュリティ対策、②物理的セキュリティ③、人的セキュリティ④技術的セキュリティの4部構成



YouTubeリンク

校内研修シリーズ

教育現場におけるセキュリティ対策Ⅱ （物理的セキュリティ）



YouTubeリンク

校内研修シリーズ

教育現場におけるセキュリティ対策Ⅲ （人的セキュリティ）



YouTubeリンク

校内研修シリーズ

教育現場におけるセキュリティ対策Ⅳ （技術的セキュリティ）



YouTubeリンク

適切なセキュリティ対策を前提とした次世代校務DX環境の整備は、
教師の働き方が改善するのみならず
「教師の時間を、児童・生徒と向き合う時間に還す」行為そのものです。

都道府県域での共同調達・共同利用をともに推進していきましょう。
何卒よろしくお願いいたします。

ご清聴ありがとうございました