教育データ利活用における校務DXの将来的なイメージ（改訂）（案）

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（第９回） R4.12.14
資　料　3

第８回会議における議論を踏まえ、同回資料４に追記・修正。

教育委員会

首長部局

学校

いわゆるゼロトラストの考え方に基づき、アクセス制御を前提としたネットワークに移行。
ネットワーク統合により校務系・学習系システムの接続性を確保。

インターネット（クラウド）

行政系システム
（マイナンバー利用事務系ネットワーク）

- 児童手当システム
- 学齢簿システム
- 生活保護システム
- 就学援助システム
- 児童扶養手当システム
- ・・・

これらのデータをマイナンバー利用事務系ネットワーク外で連携することの可否は、各自治体のセキュリティポリシーにより異なる。

ネットワーク分離

校務系システム

・機微度の高い情報を扱うため、教職員のみが利用
・多要素認証等により厳格にアクセスを制御

- 校務支援システム
- 汎用のクラウドツール
  - グループウェア
  - 保護者連絡
  - 備品管理
  - ・・・

学習系システム

・教職員及び児童生徒が利用
・利便性の観点も踏まえ、アクセスを制御※

- Office365 Education, Google Workspace for Education等
- 学習ｅポータル
- MEXCBT
- 各種デジタル教材等
- デジタル教科書

ネットワーク統合による相互接続

低コスト・リアルタイムでのデータ連携

学校・学級ダッシュボード機能

・種々の教育データを総合的に可視化し、学校経営・学習指導の高度化を図る
・加えて、教育委員会向けに設置校全体を見渡せる教育委員会ダッシュボード機能を作ることも一案
※現時点では、①校務支援システムや②学習ｅポータルの機能となる場合のほか、③これらとは独立したシステムとして提供される場合も想定される。
※ダッシュボード機能が搭載されるシステムが必要なデータを全て収集・蓄積する必要はなく、他システムが既に持っているデータをAPI連携等により参照すれば足りる。

EduSurvey

（※）児童生徒全員分の学習履歴など、児童生徒によるアクセスが適切でない機微度の高い情報については、教職員しか利用できないよう厳格にアクセスを制御

校務DXの位置付け・校務支援システムが果たすべき役割（たたき台）

第８回会議における議論を踏まえ、同回資料４に追記・修正。

従前の校務情報化

- 紙ベースの業務の効率化（法定帳票の作成等）
- 一つの校務支援システムに様々な機能を統合

校務DXが目指すべき方向性

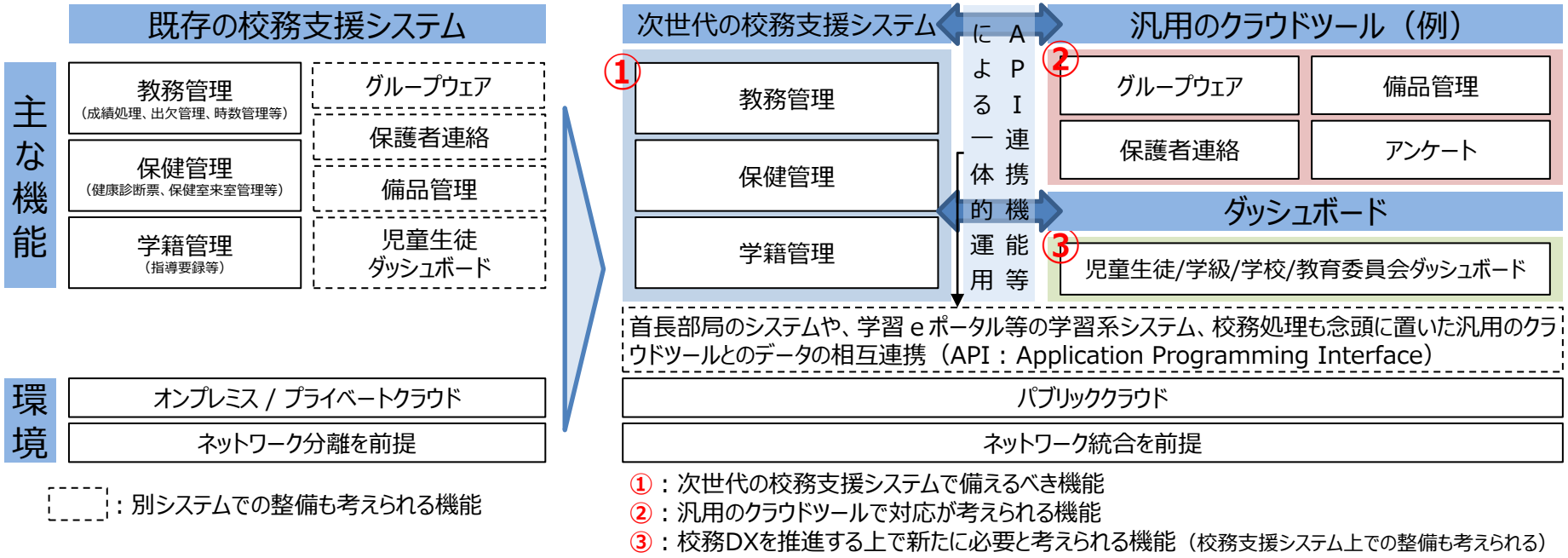
- 紙ベースの業務の抜本的な見直し※や業務用端末の一台化、業務のロケーションフリー化等による更なる業務効率化
- 様々なソフトウェアとの最適な役割分担・一体的運用
- データ活用による学習指導・学校経営・教育施策の高度化

※法定帳票の原本電子化や、各種業務フローの電子化等

その中で、次世代の校務支援システムが果たすべき役割

- ネットワーク統合を前提としたクラウド化による、データ連携・データ分析機能の実装
  - ・児童生徒の出席状況や保健室の利用状況など、日々の生活情報を収集する基盤としての機能
  - ・首長部局が運用する各種システムとデータ連携を行う上での窓口としての機能（福祉の受給状況等機微度の高い情報とデータ連携を行うには、成績情報等の機微度の高い情報を扱う校務支援システムに窓口機能を持たせることが考えられる。）

※汎用のクラウドツールで対応できない、真に必要な機能に限定



アクセス制御を前提としたネットワークにおけるセキュリティの確保について（たたき台）・1

- インターネット上のクラウドサービスで情報を安全に取り扱う上では、一切の情報アクセスを信頼せず（＝ゼロトラスト）、権限を持つ利用者からの適正なアクセスかを常に確認すること（＝アクセス制御）で、不正アクセスを防止する必要がある。
- そのためには、利用者毎に情報へのアクセス権限を適切に設定するとともに、①アクセスの真正性、②通信の安全性、③端末の安全性の観点から、利用者のアクセスの適正さを常に検証する必要がある。
- ①～③に関するセキュリティ技術（いわゆるゼロトラストセキュリティに関する要素技術）として、以下のようなものが挙げられる。

①アクセスの真正性に関する要素技術		
①-1	**多要素認証**	情報・データへのアクセスに対する認証に当たり、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
①-2	**リスクベース認証**	情報・データへのアクセスに対する認証に当たり、端末のIPアドレスや位置情報、使用されているWebブラウザ、アクセス時間が通常と異なる等の際にリスクを判定し、追加の認証を求める技術 ※日本からのアクセス直後に同一IDで海外からアクセスされる等の場合には事前登録した「秘密の質問」等による追加認証を求める
①-3	**シングルサインオン（SSO）**	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ことで、利便性の向上と認証の煩雑化によるリスクの低減を図る技術　※パスワード管理の煩雑化は、複数のサービスで共通かつ推測容易なパスワードを設定する温床となる
②通信の安全性に関する要素技術		
②	**Webフィルタリング**	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 ※対象Webページへの接続可否を直接設定するホワイトリスト/ブラックリスト方式や暴力・薬物等の不適切なカテゴリに分類されたWebページへの接続を包括的に防止するカテゴリフィルタリング方式がある
③端末の安全性に関する要素技術		
③-1	**モバイル端末管理（MDM）** (Mobile Device Management)	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・盗難に遭った際は、データの遠隔消去等を行う技術
③-2	**アンチウイルス**	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 ※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
③-3	**ふるまい検知（EDR）** (Endpoint Detection and Response)	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
③-4	**データ暗号化**	データを端末に保存する際に自動的に暗号化し、アクセス権限が無い者の情報の閲覧・編集を制限する技術

※これらは、「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を整理したものであり、今後の技術動向等により変化しうるものであることに留意。

アクセス制御を前提としたネットワークにおけるセキュリティの確保について（たたき台）・2

- 学校現場で取り扱う情報のうち、特に機微度の高い情報※1や、児童生徒の情報がまとまっているデータ※2については、高いセキュリティを確保し、取扱の安全性を高める必要がある※3。

（※1）教職員の人事情報や、児童生徒の成績情報、生活指導に関する履歴、健康診断の結果等が考えられる。
（※2）学級/学年/学校に属する児童生徒全員の名簿や、学級/学年/学校に属する児童生徒全員の学習アプリの利用履歴等が考えられる。
（※3）その前提として、管理者は利用者の職位や職務に応じ、利用者毎にアクセスし得るデータの範囲を適切に設定する必要がある。

- 具体的には、校務系システムに蓄積される情報や、学習系システムにおいて教員がアクセスし得る複数の児童生徒の学習履歴などへのアクセスについては、前ページで示したセキュリティ技術を複数組み合わせることが適当。

- 教職員が使用するネットワークや端末は、こうした情報・データを扱うことから、最低でも※4**【①-1 多要素認証、①-3 SSO、②Webフィルタリング、③-1 MDM、③-2 アンチウイルス、③-4 データ暗号化】**によりセキュリティを確保することが適切か。

（※4）ここではあくまで最低限必要と考えられる要素技術を挙げている。①-2 リスクベース認証は認証の強度を高めうるものである一方、セキュリティと利便性を両立させるリスクの判定基準などを今後検討していく必要があることから、現時点で必須の要素技術とは位置付けられない。③-3 EDRは未知のマルウェア対策として有効であるが、その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膨大なログ分析が必要であり、そのためには管理者のスキル取得又は外部の事業者に委託することが考えられるが、運用体制や費用の面から効果に見合わぬ負担が生じる可能性がある。以上から、これらについては、取り扱うデータの量（≒児童生徒の人数）を踏まえたセキュリティリスクと導入・運用費用を比較考量した上で、導入の要否を検討する必要がある。