教育情報セキュリティポリシーガイドラインの概要（令和4年3月）

※　情報セキュリティポリシーとは「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」のこと。

◆　目的・経緯

- 不正アクセス防止等の十分な情報セキュリティ対策を講じることは、学校における安全安心なICT活用のために必要不可欠。**各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考**とするものとして、『教育情報セキュリティポリシーに関するガイドライン』を策定（平成29年10月）。

- セキュリティ対策は定期的に見直しを行うべきものであり、順次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に改訂。
  【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に改訂。

- 今回(令和4年3月)の改訂では、**①アクセス制御による対策の詳細な技術的対策の追記**や、**②「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**するために実施。
  なお、**対策方針や組織体制の在り方などの基本的な方針の変更は無い。**

教育情報セキュリティポリシーガイドライン 目次

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主な改訂内容について（令和4年3月）

① アクセス制御による対策の詳細な技術的対策の追記

アクセス制御による対策を講じたシステム構成を実現するために校務用端末における詳細なセキュリティ対策を追記

項目	概要
校務用端末の詳細なセキュリティ対策の追記	「リスクベース認証」※1、「ふるまい検知」※2、「マルウェア対策」、「暗号化」、「SSOの有効性」などの記述を充実

※1 リスクベース認証：システムへの接続において場所や時間などが通常と異なる場合などにID・パスワードだけではなく追加の認証を行う方式
※2 ふるまい検知　：通信内容を監視し、異常、あるいは不審な挙動を検知する仕組み

② 「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

「ネットワーク分離による対策」及び「アクセス制限による対策」の記述を分岐させることにより表現を適正化

項目	概要
校務用端末の使い分けについて対策毎に記述を適正化	ネットワーク分離による対策を講じたシステム構成の場合 ・ネットワーク毎に複数の端末を使い分ける ※シンクライアント技術等を用いてネットワーク分離に準ずる対策を行い1台の端末で運用する アクセス制御による対策を講じたシステム構成の場合 ・アクセス制御を徹底することにより１台の端末で運用
校務用端末の持ち出しに関する記述を適正化	ネットワーク分離による対策を講じたシステム構成の場合 ・安全管理に関して追加的な措置を定めた上で許可制とする ※MDMによる遠隔でのデータ削除対策や、持ち出しデータを記録しておき返却時には削除するなどの追加的な措置 アクセス制御による対策を講じたシステム構成の場合 ・情報セキュリティ管理者の包括的承認等による持ち出しを検討する

6－1　前提

本ハンドブック発行時点（令和4年3月）時点では、自治体や学校により、校務系システムをはじめとしたオンプレミス型環境が残存していることが想定されます。本章では、校務系システムやオンプレミス型の環境における対策方法を示します。

なお、とりわけ校務系システムの機密性を確保する方法として、旧来は、ネットワーク制御を中心とした境界防御型が一般的でしたが、特に昨今の働き方改革や休校時対応によるリモートワーク等を行う際には、端末への対策を中心としたアクセス制御型への移行又は組み込みがより有効な手段となりえます。それぞれの差異を認識し、特徴に応じた適切な対応を行いましょう（詳細については、6－4を参照）。

図表１２　アクセス認証型と境界防御型の違い

アクセス認証型（ゼロトラスト）	**境界防御型**
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。

図表２８　1人1台端末を活用するために必要なネットワーク構成イメージ（アクセス制御による対策を講じたシステム構成）