「教育情報セキュリティポリシーに関するガイドライン」の改訂について

令和７年３月

文部科学省 MINISTRY OF EDUCATION, CULTURE, SPORTS, SCIENCE AND TECHNOLOGY-JAPAN

「教育情報セキュリティポリシーに関するガイドライン」の改訂について

- 教育現場には、**児童生徒や保護者の存在等、地方公共団体の他の行政事務とは異なる特徴がある**ことから、**これらを考慮した情報セキュリティ対策を講じる必要**がある。
- 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

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

改訂概要

◆ 情報資産の分類・仕分け・管理方法の見直し

項目	概要
情報資産の分類の見直し （第２編 ３.１.等）	• 教育委員会等や学校で情報資産をより客観的で適切に分類できるよう、ガイドラインP36図表７「重要性分類に基づく情報資産の例示」の分類についてアクセスする主体に基づく内容に見直し。
情報資産の仕分けの見直し （第２編 ３.１.等）	• 教育委員会等や学校でより教育現場の実態に即した情報資産の分類を行えるよう、各重要性分類の考え方の解説を拡充。 • ガイドラインP36図表７「重要性分類に基づく情報資産の例示」の各分類にそれぞれの情報の性質を記載。 • ガイドラインP36図表７「重要性分類に基づく情報資産の例示」で示す情報資産の例示の仕分けを見直し。 （例：要配慮個人情報を含む情報を重要性分類Ⅰに仕分ける 等）
情報資産の管理方法の見直し （第２編 ３.２. 等）	• 児童生徒やその保護者が重要性分類Ⅱ以上の情報資産にアクセスする際の安全管理措置を加筆。 （例：「パブリッククラウド上で重要な情報（重要性分類Ⅱ以上）を取り扱う際には、多要素認証を含む強固なアクセス制御による対策を講じなければならない。ただし、児童生徒またはその保護者が重要性分類Ⅱ以上の情報資産にアクセスする場合は、児童生徒本人またはその保護者が、当該児童生徒に関するもののみにアクセスすることを想定していることから、多要素認証を設定することが望ましいものの、パスワードの秘匿管理の徹底、複数回誤ったパスワードを入力した際のロック機能の有効化、パスワードの複雑性の確保等により本人確認を厳格に行う前提で、ID及びパスワードでの認証を許容する。」 等

◆ 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

項目	概要
次世代校務DX環境への移行期に関する加筆 （第２編 ６.３. 等）	• 次世代校務DX環境への移行期間（オンプレミス環境とクラウド環境が共存する期間）は、それぞれの環境に応じた適切なセキュリティ対策を講じなければならないという考え方を加筆。
「強固なアクセス制御」の定義・解説に関する記載の見直し （第３編（１）（３） 等）	• 強固なアクセス制御に基づくセキュリティ対策を講じる際には多要素認証による本人認証が望ましいものの、教育現場の実態や特徴を踏まえ、端末の電子証明書等を用いた端末認証と知識認証・生体認証のいずれかを組み合わせて認証を行うことも考えられる旨を記載。 • 強固なアクセス制御に基づくセキュリティ対策に関わる要素技術について、最新の知見や教育現場の実態に基づき項目を一部見直し。

◆ その他

項目	概要
ガイドラインのスコープの補足 （第１編第１章（３））	• ガイドラインの主な対象である地方公共団体が設置する学校以外の学校における情報セキュリティ対策の実施においても、ガイドラインを参照いただきたい旨を明記。
シャドーITについての加筆 （第２編 ９.４.）	• シャドーITの懸念と対策について加筆。

※その他修辞上の修正など軽微な修正を実施