

「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月版) ハンドブック

令和3年5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」(令和3年5月版)ハンドブック

目次

第1章 はじめに ～児童生徒1人1台端末の時代における教育情報セキュリティ～	3
1-1 地方公共団体における情報セキュリティについて	3
1-2 教育情報セキュリティポリシーに関するガイドライン（令和3年5月版）改訂の背景	4
第2章 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目的と適用範囲	5
2-1 本ガイドラインの目的	5
2-2 本ガイドラインの位置付け	6
第3章 情報セキュリティ対策の基本的考え方	7
3-1 情報セキュリティ対策の基本	7
3-2 「何を」守るのか？	7
3-3 情報資産を「何から」守るのか？	8
3-4 情報資産を脅威から「どのように」守るのか？	9
第4章 学校を対象とした情報セキュリティ対策	11
4-1 情報資産の分類と管理方法	11
(1) 情報資産の分類の必要性	
(2) 情報資産の管理の考え方	
4-2 セキュリティ対策の対象範囲	14
4-3 組織的・人的対策（クラウド、オンプレミス、ハイブリッド共通）	15
(1) 組織体制の確立	
(2) 組織的な情報セキュリティの確保	
第5章 GIGAスクール構想における児童生徒1人1台端末・クラウド利活用時の情報セキュリティ対策	18
5-1 前提	18
5-2 組織的・人的対策	19
(1) 教職員が児童生徒と共有すべき行動規程	
(2) クラウドサービスの利用	
(3) 運用・連絡体制の整備	
5-3 物理的対策	22
(1) 通信回線及び通信回線装置の管理	
5-4 技術的対策	23
(1) 児童生徒ID・PW	
(2) 端末のセキュリティ（管理設定）	
(3) 学校外での利用（持ち帰り）を前提とした際の技術的ポイント	
(4) その他、関連して必要になる対応	
(5) システム運用管理	
第6章 校務系システムやオンプレミス環境等を対象とした情報セキュリティ対策	27
6-1 前提	27
6-2 組織的・人的対策	28
(1) 教職員が注意すべき行動規程	
(2) 外部サービスの利用	
6-3 物理的対策	31
(1) 校務系サーバの教育委員会による一元管理	
(2) 通信回線及び通信回線装置の管理	
6-4 技術的対策	33
(1) 重要性が高い校務系情報にアクセスされるリスクへの対応	
(2) 教職員の個人認証強化	
(3) アカウント情報の使い回し防止	
(4) 潜在的なセキュリティリスクへの対応	
(5) 外部への情報資産持ち出しリスクへの対応	
(6) その他、関連して必要になる対応	
(7) 情報資産の重要性によるシステム運用管理	
第7章 個人情報の取扱について	42
7-1 事業者・自治体に確認すべき事項	42
(1) 事業者の確認すべきプライバシーの事項	
(2) 地方自治体における個人情報の利用について	
終章 おわりに	44
(参考) 用語集	45

【このハンドブックについて】

このハンドブックは、文部科学省で改訂された「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月版）の内容について、主に教育委員会の担当者向けに中核となる考え方を解説したものです。

1-1 地方公共団体における情報セキュリティについて

情報セキュリティとは、大切な情報（情報資産）を、様々な脅威から守り、安全な状態を保つことです。情報セキュリティ対策とは、私たちがインターネットやコンピュータを安心して使い続けられるように、大切な情報が外部に漏れたり、コンピュータウイルス（以下「ウイルス」という）に感染してデータが壊されたり、普段使っているサービスが急に使えなくなったりすることを防ぐために、必要な対策を指します。

地方公共団体では、住民の大切な情報を取り扱いますので、これらの情報を安全に管理するため、教育情報セキュリティポリシーを策定し、必要なセキュリティ対策を講じます。その際に、令和2年12月に策定された「デジタル・ガバメント実行計画」（令和2年12月25日閣議決定）の示す方向性*に従い、各地方公共団体においてもクラウドの活用を念頭に置いてセキュリティを確保していく必要があります。

*「政府情報システムについて、共通的な基盤・機能を提供する複数のクラウドサービス（IaaS、PaaS、SaaS）の利用環境（「（仮称）Gov-Cloud」）を整備し、早期に運用を開始する。（略）また、独立行政法人、地方公共団体、準公共分野（医療、教育、防災等）等の情報システムについても、「（仮称）Gov-Cloud」の活用に向けて、具体的な対応方策や課題等について検討を進める。」

コラム

クラウドサービスの特徴は？

クラウドサービスの特徴に、「随時最新機能へのアップデートが行われる」という点があります。

旧来のインストール型のソフトウェアでは、5年に1回インストールし、操作マニュアルを作成して、それを見ながら運用する、という形式でしたが、クラウドソリューションでは「その都度作業側で操作をしなくても、常に最新のセキュリティとテクノロジーを活用したバージョンに自動でアップデートされる」ことが強みです。サービスの見た目が時々変わるのも、こうしたアップデートの一部です。

突然のアップデートに驚いて、ICT機器やクラウドソリューションの活用を止めるのではなく、新たな時代の流れとして適応していきましょう。

地方公共団体の行政事務では、職員以外の方（住民の方など）が、情報端末を活用して日常的に情報システムにアクセスする機会は極めて限られています。また、従来の学校でも、職員以外の児童生徒の情報端末利用は、教室やパソコン教室に設置された端末など限定された環境に留まっていました。

しかしながら、社会全体のデジタル化、デジタルトランスフォーメーション（DX）が加速していく大きな潮流の中で、学校教育の基盤としても ICT は必要不可欠なものになりつつあります。このような社会的背景を踏まえた「GIGA スクール構想」に基づき、児童生徒の1人1台端末、1人1アカウント、教育用クラウドアプリ環境が整備されました。令和3年度からは、これらの利活用が本格的に始動し、授業はもとより休み時間や家庭学習等においても、児童生徒が日常的にクラウドサービスにアクセスすることが当たり前となります。従って、児童生徒の自由な学習に支障が出ないよう、コミュニケーションツール（メールやチャットなど）やクラウド連携機能などを不用意に制限しすぎることなく、正しいセキュリティを実現することこそが、学校現場の1人1台環境において必須となります。

上記を踏まえ、学校現場ならではの特徴を考慮しつつ、GIGA スクール構想に適した情報セキュリティを確立する必要が高まったことから、各教育委員会・学校に最適な環境を選択いただくための参考として、「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「本ガイドライン」という。）を改訂しました。

コラム

「GIGAスクール構想」を意義あるものにするためには

今回のGIGAスクール構想では、全ての児童生徒に1人1台端末が整備されました。

1人1台端末や教育用アプリは、特定の場面にもみ使う特別な機器ではなく、学校内外を問わずに主体的・対話的で深い学びの実現を後押しする強力な「文房具」となります。

しかし、端末及び各種教育用アプリは、あくまでツールにすぎません。教育委員会や現場の先生方に求められる、子供たちの学びをサポートする役割はこれまでとそんなに変わるものではありません。

今後、子供たちがGIGA環境を活かして学びを深めることができるかどうかは、ひとえにGIGAスクール構想への教育委員会、学校、先生方の理解にかかっています。

2-1 本ガイドラインの目的

情報セキュリティ対策は、学校において安心してICTを活用できるようにするために不可欠な条件です。しかしながら、1-2 で述べたように、教育現場においては、学校内外で児童生徒が日常的に1人1台端末、1人1アカウント、教育用クラウドアプリを利活用する等、他の行政事務とは異なる特徴があります。そこで、地方公共団体においては、児童生徒の自由な学習に支障が出ないよう十分に留意しつつ、教育現場の特徴を踏まえた学校向けの教育情報セキュリティポリシーを策定し、情報セキュリティ対策を講じる必要があります。

本ガイドライン（令和3年5月版）は、GIGAスクール構想の実現に基づいた教育情報ネットワーク及び1人1台端末の環境整備における情報セキュリティ対策の基本的な方針及び対策基準の参考とするものです。

コラム

「厳しく制限」はもう古い？

「使わせない、制限を厳しくすることが最大のセキュリティ対策だ！」という主張をかつてよく見かけたものです。しかし、十分に学校で情報活用能力を身につけず、機密情報の入ったUSBを持ち出してしまうたり、不確実な情報を信じて拡散してしまうたり、インターネット上で誹謗中傷を行ってしまうという事例が後を絶ちません。

学校の外で無数の情報にさらされたときであっても、正しく情報の価値や真偽を見極め、自分の力で判断できる児童生徒を育てるためにも、「まずは学校内で、先生と一緒に、インターネットやクラウドにつながる端末を毎日利用する」のは絶好の機会です。

まず禁止、制限ではなく、児童生徒のうちから、適切なセキュリティの確保された環境下で活用の実践を積み重ねることこそが、これからの時代で生きていくためには不可欠なのではないでしょうか。

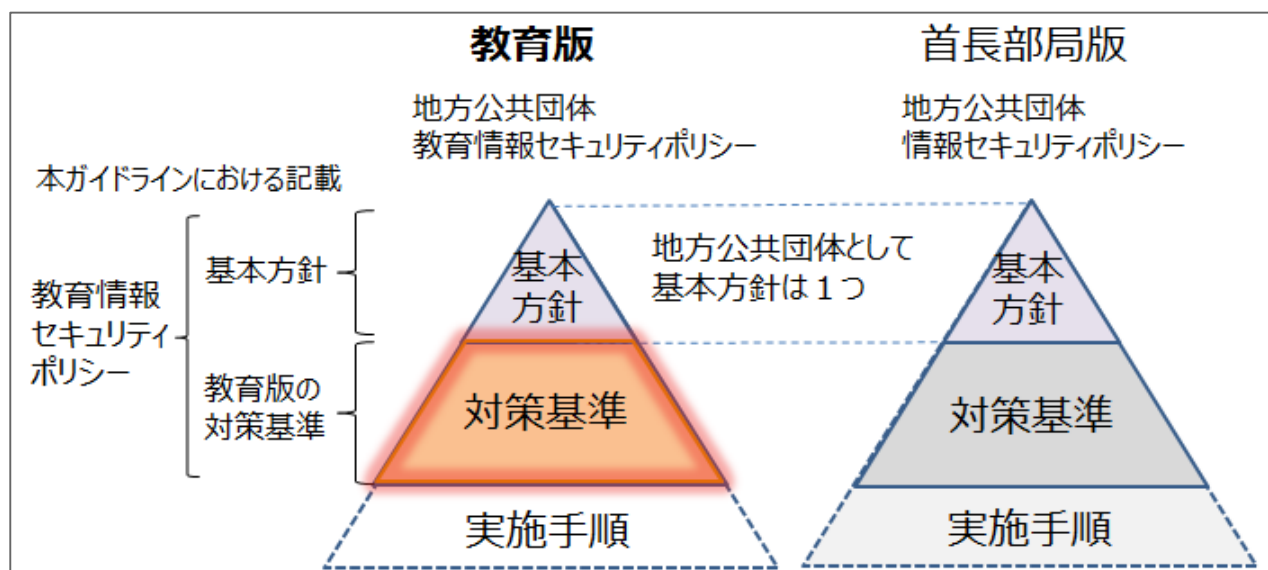
2-2 本ガイドラインの位置付け

情報セキュリティポリシーは、「基本方針」と「対策基準」の2つから構成されます。「基本方針」は、情報セキュリティに関する組織の基本方針・宣言であり、教育委員会も地方公共団体の部局のひとつであることから、教育情報セキュリティポリシーについても、「基本方針」は地方公共団体が策定する共通の基本方針として、「地方公共団体の情報セキュリティポリシーに関するガイドライン」に従います。「対策基準」は、学校の特徴を踏まえる必要があるため、本ガイドライン（令和3年5月版）において具体的な記載をしています（図表1参照）。

これらの基本方針と対策基準は、時代の変化に則して順次見直しを行うべきものです。適切なタイミングで見直しがなされないと、セキュリティ上重大なリスクが生じる恐れがあるばかりか、学校現場での情報端末の利活用を継続できなくなる恐れがあります。特に今回の改訂は、GIGAスクール構想への対応を前提として記載しているため、必ず内容を把握し、基本方針と対策基準を見直しましょう。

なお、「実施手順」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的なものですが、教育委員会が「ひな形」を学校に提示した上で、各学校において、実態を踏まえて整備していくことが必要となります。

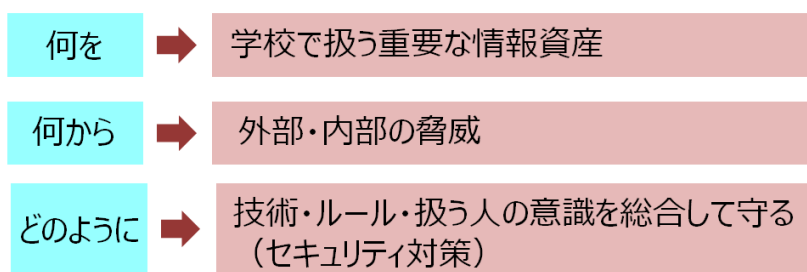
図表1 教育情報セキュリティポリシーに関するガイドラインの構成



3-1 情報セキュリティ対策の基本

情報セキュリティ対策とは、時代に則した ICT 環境を安全かつ十分に利活用することを目的に行われるべきです。セキュリティ対策自体が目的化しないよう留意しつつ、「何を」、「何から」、「どのように」守るかを明らかにする必要があります。（図表 2 参照）。

図表 2 情報セキュリティ対策の基本



3-2 「何を」守るのか？

本ガイドライン（令和3年5月版）で想定する「守る対象」は、「情報資産」です。「情報資産」とは、学校が保有している情報全般を指します。学校が保有するデータはもちろん、児童生徒が利用する端末も管理対象になります。特に、児童生徒端末は学校内のみならず学校外での利用も想定されることから、端末管理（MDM）を採用し適切に管理されることは重要です。（P24 5- 4 (3)を参照）

コラム

端末管理（MDM）の重要性

GIGAスクール構想の標準仕様では、MDM（モバイル端末管理：Mobile Device Management）の採用が前提となっています。MDMの導入により、学校内外における児童生徒端末の安心安全な利活用のための管理・設定が行えるほか、一括での端末管理が可能となり、先生方のデバイス維持管理時間を最小限に抑えることができます。

また、予め一元的なセキュリティ設定が行えることから、現場の教職員が都度設定を行う必要なく、授業内外で想定される数々のトラブルを未然に防ぐことができます。これにより、例えば授業時間内の設定変更対応等による授業の停止など、児童生徒に影響を及ぼすことも防げます。

3-3 情報資産を「何から」守るのか？

次に情報資産を「何から」守るのか、という点です。具体的には、「機密情報の漏えい」、「不正アクセス」、「データの改ざん」、「情報の滅失」などが脅威として挙げられます。情報資産が「脅威」にさらされる原因には様々なものがありますが、悪意のある人間が故意に行うものだけではなく、過失や自然災害による脅威まで含まれます。

また、IT製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、サプライチェーンの過程において意図せざる変更が加えられないよう、直接の供給者に要求することが必要となります。

どのような媒体を活用する場合においても、脅威は常に存在します。脅威を情報機器を活用しない理由にするのではなく、脅威の特徴や予防法を正しく理解し、事前の対策を行うことが必要です。




図表3 情報セキュリティの脅威

脅威の原因		想定される脅威（具体例）
人為による脅威	悪意のある他者	情報資産の窃取・改ざんを目的とした標的型攻撃
	悪意のある関係者（教職員、児童生徒）	不正アクセスによる成績等情報の改ざん
	関係者（教職員、児童生徒）の過失	端末、物理的な電磁的記録媒体（USB等）の紛失
自然災害等		データの消失

3-4 情報資産を脅威から「どのように」守るのか？

最後に、3-3に代表される多様な脅威から、情報資産を「どのように」守るのかという手段についてです。情報セキュリティ面で弱い部分（脆弱性）があると、そこから脅威が侵入しやすくなります。そこで、時間や場所を問わずに情報資産を脅威から守るためには、本ガイドライン（令和3年5月版）の対策基準に記載されている「人的セキュリティ」、「物理的セキュリティ」、「技術的セキュリティ」等の対策を総合的に行う必要があります。

図表4 学校における情報セキュリティリスクへの対策

人的セキュリティ	物理的セキュリティ	技術的セキュリティ
過失によるセキュリティ上のリスクを最小限に抑えるための対策（マニュアル作成、研修実施等） 	情報資産の機密性を確保するための対策を実施（パスワード設定や端末の管理等） 	悪意の有無を問わず情報資産の流出を防ぐための技術的な対策を実施（アクセス制限等） 

なお、悪意のある脅威の手口は年々巧妙化しているため、情報資産は、常に最新のセキュリティ対策により保護されていることが必須です。ただし、セキュリティ対策の本質を理解せずに「とりあえず制限や禁止」をしたり、保管場所にのみ拘泥したりすると、肝心の対策がおろそかになる恐れもあります。本ガイドラインや本ハンドブックの最新版（いずれも令和3年5月版）を参照し、適切な対策を行いましょう。

さらに、セキュリティ対策を実施するにあたっては、児童生徒の学習活動での使いやすさと、安全性の両面を共存させる必要があります。セキュリティを懸念するあまり、「使わせないことが最大のセキュリティ」という発想にならないよう、十分な留意が必要です。

具体的な対策については第4章に記します。

技術の発展に伴い、セキュリティに関する考え方も日々アップデートされていきますが、セキュリティ対策のよくある誤解に、パスワードに関するものがあります。

まず一つが、メールにファイルを添付して送信する際に1通目でパスワード付きの添付ファイルを送り、2通目に解除用のパスワードのメールを送る方法です。近年、この方法はパスワード付き添付ファイルを送付することによりウイルス対策ソフトによるスキャンがなされないなど、セキュリティリスクの増大につながることが指摘されています。また、今後は教育現場においても多様なデバイスを活用することを想定すると、スマートフォンやタブレットで暗号化ファイルを表示できなかったり、この方法を行うことでセキュリティ対策をしたつもりになってしまうといった運用上の不便さ・リスクも孕んでいます。

また、近年見直しがなされた慣習のもう一つが「パスワードの定期的な変更が必要」というものです。こちらは総務省の「国民のための情報セキュリティサイト」にも、以下のような記載があります。

「これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に、米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです。また、日本においても、内閣サイバーセキュリティセンター（NISC）から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています。」

<https://www.nisc.go.jp/security-site/handbook/index.html>

各自治体や学校においては、一度定めたセキュリティポリシーを慣習としてただ引き継ぐのではなく、最新のセキュリティ対策を反映したものになっているか、本ガイドライン（令和3年5月版）に基づき、適切に見直しましょう。

4-1 情報資産の分類と管理方法

(1) 情報資産の分類の必要性

学校で扱う情報資産は、公開の可否、万一の場合の影響が異なることから情報資産の重要度に応じて、守り方を変える必要があります。従って、学校が保有する情報資産の重要度による仕分けが重要です。情報資産は、情報を漏えいさせない（機密性を確保）、情報を改ざんさせない（完全性を確保）、情報がいつでも扱える状態を保つ（可用性を確保）の3つの観点から影響度を評価し、分類します。本ガイドライン（令和3年5月版）では、分類時の参考として3つの観点を総合した4段階の重要性分類について例示しています（次頁参照）。

コラム

クラウドは「組織内部」

GIGA スクール構想において、学習系のシステムはクラウド利用を前提としています。

第三者機関による認証（ISO/IEC27017,27018）等に基づき、適切にセキュリティ基準を満たしていると判断の上で教育委員会・学校が構築・管理・採用している環境は、クラウドの利用を含め「組織内部」と整理できるため、クラウドへのアップロードは「組織外部への情報資産持ち出し」や「情報の外部送信」にあたりません（本ガイドライン（令和3年5月版）図表6「情報資産の取扱例」注釈を参照）。

すなわち、子供たちが作成した学習の記録をクラウドにアップロードしたり、クラウド上で教師と児童生徒及び児童生徒間のコミュニケーションを行うことが規定上も可能になっています。積極的に環境を活用していきましょう。

図表5 情報資産の例示

情報資産の分類					情報資産の例示		
重要性 分類	定義	機密性	完全性	可用性	校務系	学習系	公開系
I	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	3	2B	2B	・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	セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。	2B	2B	2B	○学籍関係 ・卒業証書授与台帳 ○成績関係 ・評定一覧表 ○指導関係 ・事故報告書・記録簿 ○進路関係 ・卒業生進路先一覧等 ○健康関係 ・健康診断票 ・健康診断に関する表簿 ○児童・生徒に関する個人情報 ○学校教職員に関する個人情報 ○教職員に割り当てた機密性の高い情報 ・情報システムログインID/PW管理台帳 ・情報端末ログインID/PW管理台帳	○児童生徒の学習系情報 ・学習システムログインID/PW管理台帳 ・学習用端末ID/PW管理台帳	
III	セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。	2A	2A	2A	○児童生徒の氏名 ・出席簿 ・名列表 ・座席表 ・児童生徒委員会名簿 ○学校運営関係 ・卒業アルバム ・学校行事等の児童・生徒の写真	○学校運営関係 ・授業用教材 ・教材研究資料 ・生徒用配布プリント ○児童生徒の学習系情報 ・児童生徒の学習記録 (確認テスト、ワークシート、レポート、作品等) ・学習活動の記録(動画・写真等)	
IV	影響をほとんど及ぼさない。	1	1	1			○学校運営関係 ・学校・学園要覧 ・学校紹介パンフレット ・学校行事のしおり ○学校活動の記録 ※保護者の承諾がある場合、以下は公開可能 ・学校行事等の児童・生徒の写真 ・学習活動の記録(動画・写真・作品等)

(出典) 教育情報セキュリティポリシーに関するガイドライン「図表5 情報資産の例示」

(2) 情報資産の管理の考え方

学校で扱う情報資産は、大きく校務系情報、学習系情報、公開系情報に分けられます。以下では、セキュリティ対策上留意すべき校務系情報、学習系情報について記します。

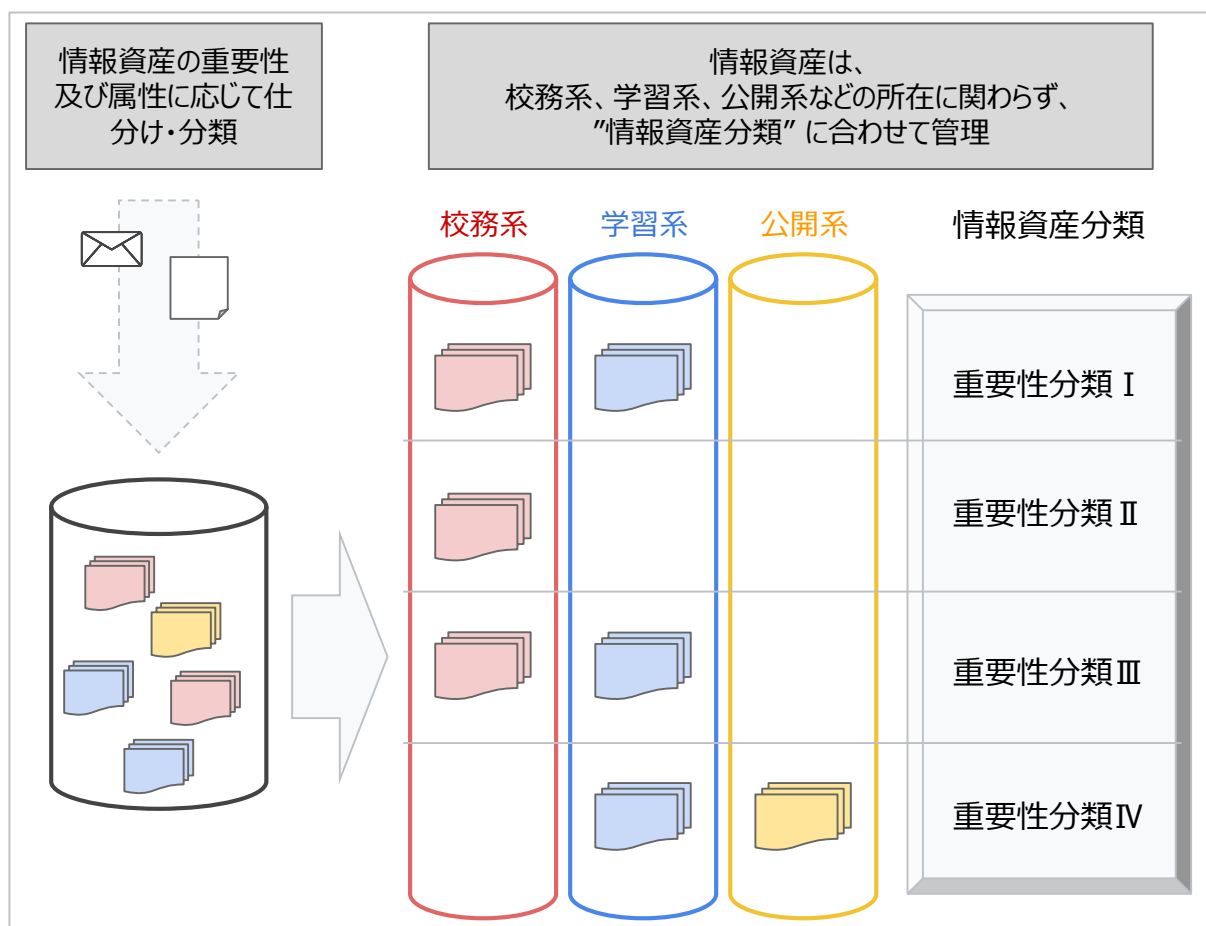
成績処理や児童生徒の指導記録等の校務系情報は、機密性の高い情報を含み、セキュリティ侵害が学校事務や教育活動の実施に重大な影響を及ぼすため、教職員以外にはアクセスできない重要な情報に位置付けられます。**このため、外部からの脅威の侵入はもとより、児童生徒からもアクセスできないように対策を講ずることが必要です。**

一方で、児童生徒が授業等で活用するワークシート等の学習系情報は、学習活動を通して生成されるものであり、教員はもとより、児童生徒もアクセスすることが前提となっています。このため、「校務系情報」とは区別して対策を講ずる必要がある一方で、学習系情報であっても、学外に公表することを前提にしていない情報を含む場合があり、学校の外に漏えいしないように対策を講ずることが必要となります。

なお、情報資産は、前頁に一部引用した教育情報セキュリティガイドライン（令和3年5月版）の図表5「情報資産の例示」で示されている「重要性分類」によってその守り方が異なるため、各分類毎にシステムを分けて管理することが求められます。

また、GIGA スクール構想によって児童生徒の1人1台端末利活用が日常的なものになることで、例えば健康状態の報告や欠席連絡等、学校外との連携においてもICTの利用が活発化することが想定されます。適切にアクセス権を設定したり、適切なツールやアプリケーションを選択することによって、重要性の高い情報資産への部外者のアクセスを許すことなく情報の送受信が可能です。ICTがもたらす利便性を享受しつつ、安全な情報の受け渡しが行われるよう適切な管理を行いましょう。

図表6 情報資産分類の考え方



4-2 セキュリティ対策の対象範囲

前ページの図表6のとおり、「重要性分類」に従い情報資産を分類し、それぞれの情報資産の重要度と、活用実態を踏まえ情報システムを整理すると、学校には、「校務系システム」、「学習系システム」、「行政系システム」の3つの情報システムが存在します。本ガイドラインでは、このうち、「校務系システム」、「学習系システム」を対象とします。

図表 7 情報資産の取扱例

情報資産の分類								
重要性分類	定義	組織外部への持ち出し制限*	情報の組織外部への送信**	情報資産の運搬***	組織外部での情報処理****	使用する電磁記録媒体	情報資産の保管	情報資産の廃棄
I	セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。	本ガイドラインに準拠していることを確認した上で業務遂行上必要な場合には、情報セキュリティ管理者の判断で持ち出しを可	限定されたアクセスの措置がとられていること*****	鍵付きケースへの格納	禁止	施錠可能な場所への保管	<ul style="list-style-type: none"> ・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ ・6か月以上のログ保管 ・サーバの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止 	電子記録媒体の初期化、復元できないようにして廃棄
II	セキュリティ侵害が、学校事務及び教育活動の実施に重大な影響を及ぼす。	同上	同上	同上	安全管理措置の規定が必要	同上	同上	同上
III	セキュリティ侵害が、学校事務及び教育活動の実施に軽微な影響を及ぼす。	情報セキュリティ管理者の包括的承認で可	同上	同上	同上	同上	<ul style="list-style-type: none"> ・耐火、耐熱、耐水、耐湿を講じた施錠可能な場所に保管（電子データの場合もこれらの対策に準じたサーバに保管） ・情報資産を格納するサーバのバックアップ（推奨事項） ・一定期間以上のログ保管 ・サーバーハードディスクの冗長化（推奨事項） ・オンラインで情報資産を利用する場合は通信経路の暗号化を実施 ・保管場所への必要以上の電磁記録媒体の持ち込み禁止 	同上
IV	影響をほとんど及ぼさない。							

- * : 組織外部への持ち出しとは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスを含む環境)の外に情報資産を持ち出すことを示す。
- ** : 情報の組織外部への送信とは、情報システムを構成するネットワーク、端末、サーバの閉じた領域の外側に、情報資産をオンラインで持ち出すことを示す。
- *** : 情報資産の運搬とは、USBメモリやハードディスク等の電磁的記録媒体を介して情報資産を運搬する場合を示す。
- **** : 組織外部での情報処理とは、教育委員会・学校が構築・管理している環境(本ガイドラインが適用されているクラウドサービスを含む環境)の外において情報資産を管理・電算処理することを示す。
- ***** : 限定されたアクセスの措置とは、適切かつ限定的な利用を前提とし、外部に送信される際に適切なアクセス制限を講じることを指す。

(出典) 教育情報セキュリティポリシーに関するガイドライン「図表6 情報資産の取扱例」

（１）組織体制の確立

情報セキュリティ対策の基本は、組織体制を確立することから始まります。統括教育情報セキュリティ責任者は、GIGAスクール構想を背景とした1人1台端末及びクラウドの利用を前提に、学校内外において利便性とセキュリティを両立した安心・安全な利活用を促進するため、児童生徒及びその保護者、並びに外部委託等の第三者情報提供先を念頭に置いた運用体制を確立することが極めて重要になります。

① 教育委員会の役割

教育委員会は、情報システムを導入し、教育情報セキュリティ全般を管理する立場として、管下の学校を含めて、情報セキュリティの組織体制を整備します。

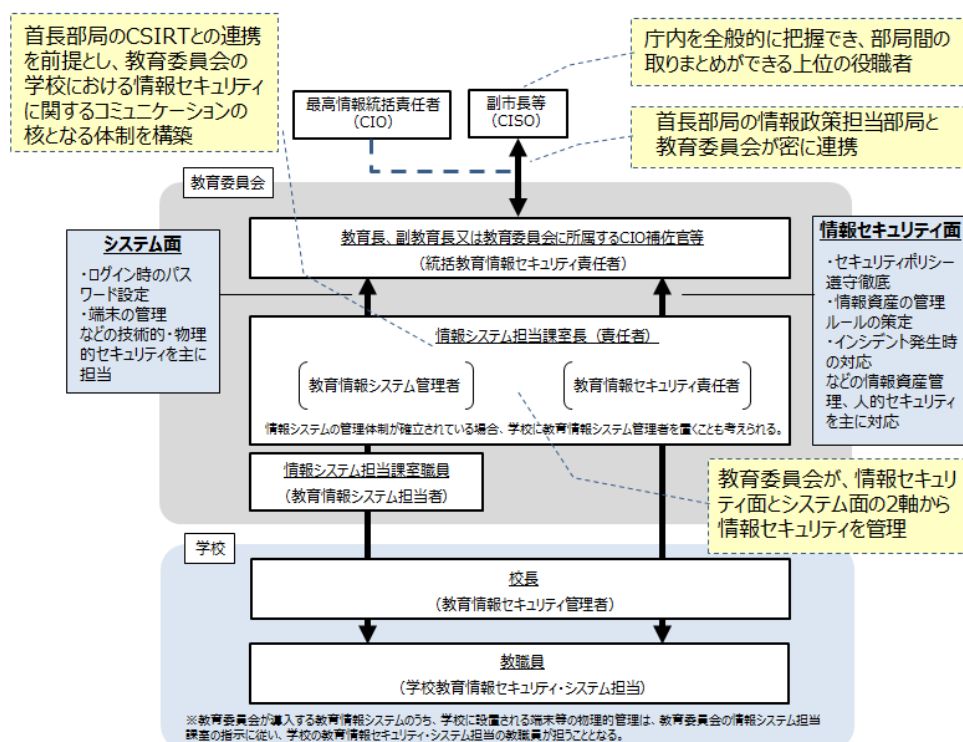
教育委員会は、基本方針や対策基準の策定及び定期的な見直しを学校と協力しつつ進めましょう。

② 組織体制の考え方

教育情報セキュリティに関する組織体制は、地方公共団体の考え方に沿って様々な形態があり得ますが、本ガイドライン（令和3年5月版）においては、教育情報セキュリティの最高責任者（Chief Information Security Officer, 以下「CISO」）は、地方公共団体におけるCISOと共通（副市長等）とすることを基本としています。

教育委員会と学校だけでは、専門的な知見を有している職員の不在等により十分な情報セキュリティ体制を構築することが難しい場合が多いこと、新たな情報セキュリティインシデントの共有及び対策等は、部局ごとではなく、地方公共団体が一体となって対策を講ずることが望ましいこと等を踏まえると、CISOは地方公共団体で統一し、教育委員会と首長部局が連携しながら情報セキュリティの確保に取り組むことが重要と考えられます。（図表8参照）。

図表8 情報セキュリティ推進の組織体制例



（２）組織的な情報セキュリティの確保

（１）に記載したように、情報セキュリティ対策のための組織体制を確立した上で、CISOの配下で情報セキュリティポリシーが適切に運用されるよう、マニュアルを作成することが必要です。

① 組織として情報セキュリティレベルを維持するための行動

情報セキュリティインシデントには、情報資産を扱う教職員の過失に起因するケースも多いことから、組織的に情報セキュリティ意識を醸成することが求められます。

現場の教職員に対し、情報セキュリティ意識を持ってもらえるよう、CISOは研修計画（eラーニング、集合研修、説明会等）を策定し、毎年度、最低１回は研修を実施することが推奨されています。また、教育情報セキュリティ責任者は教育情報セキュリティ管理者と連携し、児童生徒及びその保護者と第三者情報提供先に対しても協力を要請すると一層効果的です。情報セキュリティインシデントの発生時に被害を最小限に留めるためには、適切な初期対応が肝要です。そのため、情報セキュリティインシデントについては、その疑いがある場合を含めて報告ルールを整備しましょう。（図表 9 参照）

図表 9 情報セキュリティレベルを維持するために必要な行動の例

情報セキュリティを維持するために必要な行動	具体的な実施事項 (本ガイドライン（令和3年5月版）記載内容の要約)
情報セキュリティに関する研修・訓練	CISOは、定期的に情報セキュリティに関する研修・訓練を実施しなければならない
	CISOは、緊急時対応を想定した訓練を定期的に実施しなければならない
研修計画の策定及び実施	CISOは、職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。また、研修計画において、教職員等は、毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない
研修・訓練への参加	全ての教職員等は、定められた研修・訓練に参加しなければならない
情報セキュリティインシデントの報告	教職員等は、情報セキュリティインシデントまたはその疑いのある事象を認知した場合、速やかに情報セキュリティ管理者に報告しなければならない
外部委託事業者に対する説明	教育情報システム管理者は、外部委託事業者からの再委託先も含めて、守るべき内容の遵守及びその機密事項を説明しなければならない
データ漏洩防止機能の活用	教育情報セキュリティ管理者及び教育情報システム管理者は、電子メール等による情報の組織外部への送信時に安全性を高めるため、添付される情報資産を監視する等、出口対策の実施及び設定の維持・管理を行わなければならない
レポート機能の活用	統括教育情報セキュリティ責任者及び教育情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、実施しなければならない

本ガイドライン（令和3年5月版）に基づくマニュアルは、「作って終わり」では意味がありません。
災害に備えた避難訓練と同様に、情報セキュリティインシデント発生時に迅速かつ的確に報告が行われるよう、事前の訓練を行いましょう。その際に、保護者や情報の第三者提供先も含めて訓練を行うことが重要です。

② 評価・見直し

（ア）監査

監査により、教育情報セキュリティポリシーの遵守実態を把握し、徹底の状態や業務の実態に合わない状況を可視化及び改善を繰り返すことで、実効性のあるセキュリティ対策が維持されます。

（イ）自己点検

教育情報セキュリティポリシーの遵守状況等を学校が自ら点検し、不備な部分を洗い出すだけでなく、レポーティング機能を活用した定期的なシステムの健全性を把握することは、組織全体のセキュリティ対策の改善や教職員等の情報セキュリティに関する意識向上に有効であるため、自己点検を定期的実施することが必要です。（自己点検は、チェックシートに基づく方法が有効です。）

（ウ）教育情報セキュリティポリシー及び関係規程等の見直し

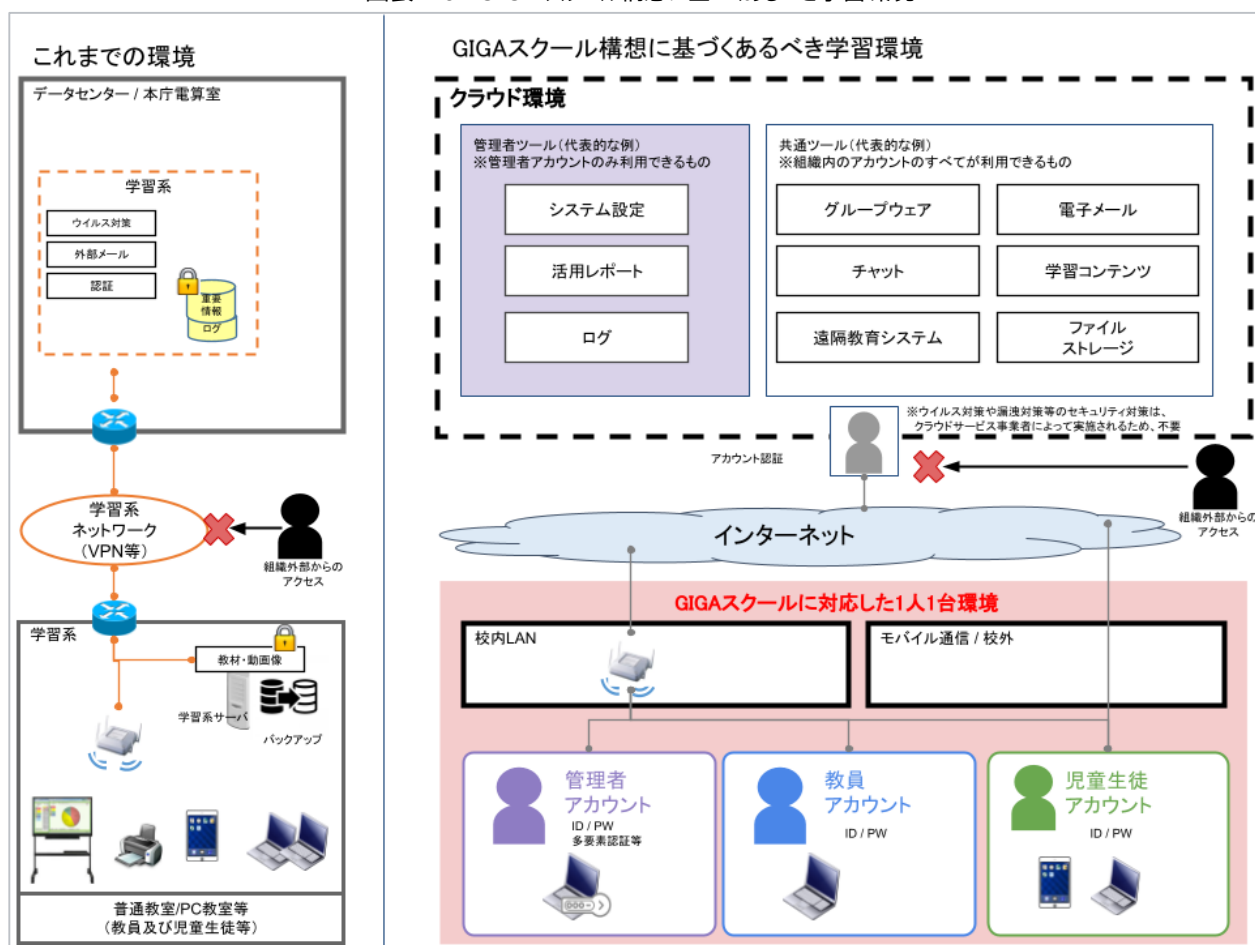
情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化します。また監査や自己点検の結果等から、教育情報セキュリティポリシー及び関係規程等を見直す必要性が明らかになる場合もあります。したがって、情報セキュリティ脅威及び技術等の変化や、監査・自己点検の結果等を踏まえ、教育情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められます。

5-1 前提

本ガイドライン（令和3年5月版）では、1人1台端末、1人1アカウント、クラウド利用を前提とした学習環境において、安全に、かつ充実した学びの実現のために必要な検討事項を示しています。教室内はもちろん、持ち帰りや校外学習、遠隔学習まで含めた学校内外での学びを充実させるためには、GIGA スクール構想において整備された環境を十分に活用することがポイントです。

本ハンドブックの発行（令和3年5月）時点では、旧来のオンプレミス型環境を利用している自治体や学校も、徐々にクラウド環境への移行が進んでいくことが想定されます。一度に全て移行しようと身構えるのではなく、少しずつ進めていくことが大切です。

図表 1 0 GIGA スクール構想に基づくあるべき学習環境



「クラウドサービスではインターネット上にデータを保管する」と聞くと、漠然と不安を感じていませんか？しかし、「データを預けている」という事例は、実は身近にたくさんあります。

たとえば銀行。みなさんが銀行に預けたお金の情報はデータとして保管されています。しかし、そのデータが、どのデータセンターでどのように管理されているのかまで把握することは困難でしょう。だからといって、「銀行預金よりタンス預金のほうが安全だ」と考えている方は少ないのではないのでしょうか。銀行では大切なお客様の預金データが流出、改ざんされることのないよう、様々なセキュリティ対策がなされていることが想像されます。

クラウドサービスも同様です。特に、第三者機関により認証を得ているクラウドサービスであるかどうかにより、セキュリティ観点での安全性を確認することができます。

漠然とした不安で拒絶するのではなく、適切な環境下において、特性を理解して使うことが重要です。

5-2 組織的・人的対策

（１）教職員が児童生徒と共有すべき行動規程

新学習指導要領では、情報活用能力が「学習の基盤となる資質・能力」に位置付けられています。GIGAスクール構想により整備された1人1台端末環境を安全かつ効果的に活用し、情報活用能力を育成する際のはじめの一歩として、教職員間、及び教職員と児童生徒の間で安心・安全な利活用の前提となる事項（図表1-1）を共有しておくことは非常に重要です。そのこと自体が人的なセキュリティ対策にも直結します。

現在の児童生徒は、産まれたときから情報端末がそばにある、いわば「デジタルネイティブ世代」です。先生方よりも、「デジタル」「端末の使い方」に詳しいこともたくさんあるでしょう。

そのようなとき、「先生が使えないからこの機能を使わせない」では、児童生徒がせっかくGIGAスクール構想で整備された機会を享受することができません。十分にセキュリティが確保された環境で、先生と生徒で協力しながらその学級らしい使い方を見つけてみましょう。時には、「児童生徒から先生が教わる」なんてこともあるかもしれません。

情報セキュリティを確保するためには、児童生徒、教職員、どちらも正しく情報端末やクラウド環境を使うことが必須になります。児童生徒と教職員のスキルの差を警戒し、「使わせない」という方針を採るのではなく、一緒に適切に使っていくことがセキュリティ保全にもつながります。

図表 1 1 教職員が児童生徒と共有すべき事項

項目	内容
各教委員会及び自治体採用のクラウドサービスの理解・利活用	新学習指導要領に基づく学びの実現のために、適切なクラウドサービスを利用し、GIGA スクール構想に基づく環境を最大限活用することが想定されます。過度な規制で学びの機会を失うことのないよう、判断を行うこと
電子メールの利用	<p>メールを送信する際には、誤った宛先や必要のない宛先に送付しないよう、送付前によく確認すること</p> <p>差出人が不明または不自然に添付されたファイルを受信した場合は、開封する前に教職員に報告すること</p> <p>学校で定められた適切なアカウントを使用すること。また、差出人が認識できるアカウント名を設定すること （認識できない暗号化されたアカウント名からのメールは犯罪等で使用されるものと区別がしづらいため。詳細は 5－4（１）参照のこと）</p>
ID及びパスワードの管理	<p>自分のIDは、自分のみが利用する（他の人には利用させない）こと</p> <p>パスワードは他の人には知られないようにすること。忘れた場合及び漏えいした場合はすぐに教職員に報告し、再設定を行うこと</p>
写真、動画の撮影	学校内外で動画や写真の撮影を行う場合は適切な許可を得てから行うこと
故障、紛失、盗難時の対応	<p>端末が動かない、勝手に操作されている、いつもと異なる画面が出ているといった症状が出た場合、すぐに教職員に報告すること</p> <p>端末を紛失した場合には、すぐに教職員に報告すること</p>

(2) クラウドサービスの利用

GIGA スクール構想による1人1台端末環境は、クラウドサービスの利用を前提としています。利用するクラウドサービスは、第三者機関の認証を取得しているなど、適切なセキュリティ対策が施されていることが確認できる事業者のものを選定しましょう。新しくクラウドアプリケーションを利用する場合にも同様の留意が必要です。

※インストール型のアプリケーションを利用する場合は、本ガイドライン及び本ハンドブック（いずれも令和3年5月版）の第6章を参照しつつ対策を行いましょう。

(3) 運用・連絡体制の整備

GIGA スクール構想に基づく1人1台端末環境では、学校内外問わずに日常的に端末を利用することになります。情報セキュリティインシデントの発生場所や発生時刻も学校内や授業時間内に限定されないことが想定されるため、教育情報セキュリティ管理者が中心となり、端末の学校内外における端末の利用ルールを定める必要があります。特に学校外での利用に際しては、児童生徒の保護者への定期的な説明も行いましょう。

また、情報セキュリティインシデント発生時の報告に関しても可能な限り定期的な訓練を行い、万が一があった場合に迅速に対応できるようにしましょう。

コラム

ICT活用時の心構え

GIGA スクール構想においてICT環境が整備が急激に進んだことで、「ICT機器やシステムをなんとしても使わなくては」ということで頭がいっぱいになっていませんか？もちろん、ICT環境を上手く活用することは、これまで先生方が行ってきた授業実践を発展させたり、今までできなかったことを実現するのに非常に効果的です。

しかし、「次世代を支える子供たちを育てる学校という場において、どうやって子供の力を伸ばしていくのか？」という観点や、それに基づく授業・教育実践の在り方はこれまでと変わるものではありません。大切なのは、「ICTを使っている」ことではなく、「ICTを使ってどうするか／どうなったか」です。今一度、心に留めましょう。

(1) 通信回線及び通信回線装置の管理

学校内のネットワークを通じてインターネットに接続する場合、通信帯域が必要以上に圧迫されることで、通信の遅延や切断が発生し、学習の妨げになる恐れがあります。故に、以下のような対策が必要です。

① インターネット接続帯域の確保

児童生徒が同時にインターネットに接続し、クラウドサービスを活用した円滑な授業を行うことができるよう、設計の段階で十分に評価を行いましょう。その際に、理論値のみに頼るのではなく、実際の運用に則した評価項目を設定することが極めて重要です。例えば、平日の授業時間帯における帯域の状況や、授業開始時の短時間で同時接続が発生した場合などを想定し、評価項目を設定しましょう。

また、回線契約時に帯域に関するサービス水準合意（SLA）が含まれていない場合、学校周囲の環境変化や回線利用の混雑状況により通信品質に影響が出る場合があるので、運用開始後であっても定期的に評価・見直しを行いましょう。

② 校内の無線LANへの接続

インターネット接続帯域と同様に、学校内の無線LANの可用性を確保することは、児童生徒の学習を止めないための必須条件です。学校内の無線通信の干渉による影響で、インターネット回線には問題がなくても、想定通りの品質が発揮されないといったことがないよう、十分な注意が必要です。また、各アクセスポイントの同時接続数や、複数のアクセスポイントでカバーされた校内のエリアを移動した際にネットワークが切断されないことも予め評価しましょう。

なお、無線LANの接続の際には、セキュリティの観点からクライアント証明書を用いることが推奨されます。

更に、日本国内の無線LANの周波数は2.4GHz帯及び5GHz帯がありますが、それぞれ電波の特性があるため、各校の構造も踏まえた上での設計が重要です。

コラム

SSID非表示設定はセキュリティ対策ではない？！

SSIDの非表示設定（ステルスSSID）は一見してネットワークが見つからないため、安心感があります。しかし、実際には非表示ネットワークは簡単に見破ることができてしまい、セキュリティ対策とは見なされないので十分な注意が必要です。

SSIDの非表示設定がされているネットワークを優先的に攻撃するツールもありますので、SSIDを隠蔽するのではなく、WPA2以降による暗号化を利用しましょう。

暗号化を含めた無線LANのセキュリティ対策全般については「Wi-Fi提供者向け セキュリティ対策の手引き」も参照しましょう。

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

自治体によっては、費用等の理由によりグローバルIPアドレスを最小限の利用で留めているケースがあります。セキュリティ上の問題点はないように思えますが、サービス配信業者によっては、ロボットによる不正アクセスを制限するため、一定期間に同一IPからのアクセスが集中した場合や、普段の傾向と大幅に異なるアクティビティが検出された場合に、アクセスが遮断される場合があります（一般に、「私はロボットではありません」というチェック画面が表示されるのも不正アクセス防止の一環です）。

具体的にどの程度でアクセスが遮断されるのか、という数値はセキュリティ上公開されていませんが、教員や児童生徒のアクセスが遮断され、授業に支障がでることのないよう、必要なグローバルIPアドレスの個数について、ネットワーク設計段階でテストをしておくことが重要です。

5-4 技術的対策

（1）児童生徒ID・PW

① アカウント作成、管理ポリシー

児童生徒が使用するアカウント（ID）は、同一組織内で重複せず、シンプルかつ識別可能であることが必要です。また、クラウド利用の場合には各IDに紐付いて児童生徒の学びの履歴が蓄積されるため、入学時、進級時、転出入時、卒業時などの運用を含めて対応方針を定め、適切に管理しましょう。

先生と生徒の間はもちろん、生徒間のコミュニケーション時の利便性を高める上で、「アカウント名で個人が識別できること」は見落としがちなポイントです。

クラウドを活用した協働学習を行う際に足かせにならないためにも、ある程度の利便性の確保は不可欠です。また、ランダムな英数字の羅列をアカウント名にしてしまったために、結局それらが誰のアカウントか判別できず、アカウント名と個人を紐付ける資料を別途作成するようでは、セキュリティの観点からも本末転倒です。

最新の本ガイドライン、ハンドブック（いずれも令和3年5月版）を参照し、適切なセキュリティ上の対応を行った上で、アカウント名は複雑化しないことを強く推奨します。

また、児童生徒個人のアカウントには、個人の学びの履歴が紐付いています。先生方も、ご自身で作成された教材等はアカウントに紐付いて保管されています。そのため、同一の組織、環境（学校、市区町村、都道府県）で同じクラウドサービスを利用しているのであれば、基本的にアカウントは個人に紐付く（異動の際に都度リセットされない）運用にしておくといでしょう。また、別自治体への転校・異動などアカウントの変更を余儀なくされる場合は、児童生徒には学習データが、教師には作成した教材データ等が移行できるように準備しましょう。

② パスワードと多要素認証

一般に、パスワードは複雑性が高いほどセキュリティ強度が上がります。学校での運用については、児童生徒の発達段階に応じ、適宜見直しを行いましょう。また、多要素認証や二段階認証を活用することにより、なりすましの防止だけでなく、パスワードの強度とセキュリティのバランスを取ることが可能です。

特に成績評価につながるCBT（Computer Based Testing：試験における工程を全てコンピュータ上で行う事）など、本人確認を厳格に行う必要がある場合においては児童生徒のID/パスワードに加えて多要素認証を設定することが有効です。

また、教育情報セキュリティガイドライン（令和3年5月版）でも触れている通り、シングルサインオン（SSO）を組み合わせることにより、パスワード管理の労力を技術的に減らすことも可能ですので、必要に応じて利用を検討しましょう。

（２）端末のセキュリティ（管理設定）

① MDM（Mobile Device Management）の利用

児童生徒の1人1台端末は、MDM（Mobile Device Management）等を活用し一元的に管理を行うことが必要です。また、学校内外など利用する場所にかかわらず、ポリシーの展開は必要なタイミングで随時行い、ログイン・アプリケーションの利用履歴ログ等は、必要な際に閲覧できる環境を整えましょう。

② 不適切なアプリの使用やウェブページの閲覧の防止

児童生徒が悪意のあるウェブサイト等へのアクセスを行わないような人的対策も非常に重要ですが、それだけでなく、技術の面でも安心・安全な利活用をサポートできるように環境を整えましょう。

その際に、児童生徒による不適切なウェブページの閲覧を防止するような対策を行うことが必要です。

各自治体の要件に応じて、以下のような対策を単独または組み合わせて行うことが効果的です。

ア. フィルタリングソフトの導入

イ. 検索エンジンのセーフサーチの有効化

ウ. セーフブラウジングの有効化

児童生徒が無許可でこれらのセキュリティ対策を変更できないよう、システム側での管理を行いましょう。

参考：OS事業者による端末の安心・安全な活用方法についての解説

https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_01172.html

コラム

「使わせない」環境で教えられますか？

新学習指導要領では、情報活用能力が言語能力と同様に「学習の基盤となる資質・能力」に位置付けられています。情報活用能力の育成に、GIGA スクール構想で整備されたICT環境を使わない手はありません。

児童生徒に1人1台端末を使わせる際に、メールやチャット等の機能を一律に制限してしまう自治体がありますが、実社会ではもはや、メールやチャットでコミュニケーションを取ることは当たり前です。児童生徒も、学校の外では自分や保護者の端末でそれらを使っているという場合も多いでしょう。制限ばかりでは、実社会で活かせる情報活用能力は身につけません。

最新の本ガイドライン（令和3年5月版）を正しく理解し、安全に、適切な形でサービスを利用できるようにしましょう。

（３）学校外での利用（持ち帰り）を前提とした際の技術的ポイント

① 児童生徒端末保護の基本方針

クラウド環境を前提とした持ち帰りの際に必要なセキュリティ対策は、学校内での利活用の時と同様に確保される必要があります。本ハンドブック等を参照し、MDM（Mobile Device Management）で児童生徒端末のセキュリティ対策（遠隔ロック/初期化、各種セキュリティプログラムのアップデート確認、各種ログの管理等）が適切に実施されていることを確認しましょう。

② 持ち帰り時に特に留意すべきこと

ア. 遠隔管理（端末の盗難や紛失時の情報漏洩対策）

持ち帰りの際に重要なのが盗難や置き忘れ等の紛失対策です。従来は、一般に「盗難・紛失時にいかにデータを漏洩させないか」という観点の対策が主流でしたが、児童生徒が使う端末については、予め「そもそも盗難されづらい（盗難されても意味をなさない）」ような対策（遠隔からのロック・初期化）を施すべきでしょう。

これらを実現する前提として、MDM（Mobile Device Management）による一元管理を行うことが不可欠です。

コラム 「そもそも盗難されづらい（盗難されても意味をなさない）」対策とは？

MDM（Mobile Device Management）により、盗難された端末が第三者によりネットワークに接続された瞬間、端末がロックされたり、端末のデータが消去されるような環境を構築しましょう。

また、端末の盗難はOSを上書きし転売する目的で行われることが多いため、簡単に初期化ができないような仕組みや、万が一初期化された場合でも強制的に管理下に戻せるような仕組みの構築が必要です。

イ. 各種セキュリティプログラムのアップデート

セキュリティ対策においては、OS等のシステムを常に最新の状態にしておくことが非常に重要です（６－４（４）に詳細記載）。持ち帰り実施の際も、学校内での利用と同様に、最新の状態を確保する必要があります。

学校外で使うからといって、セキュリティプログラムのアップデートが滞ったり、アップデートにより問題が発生し使用に支障が起こることのないようにしましょう。

ウ. 各種ログの適切な管理

持ち帰りを含めた学校外での利用時であっても、1人1台端末のログは取得、保管されるべきです。これらのログは、端末にローカルで保存されるのではなく、クラウド等で集中管理されていることが重要です。

また、繰り返しになりますが、これらは安心・安全な利活用を実現する上で非常に重要な対策です。持ち帰り時のみならず、学校内での活用時にも同様に設定しましょう。

GIGAスクール構想で整備された1人1台端末は、文部科学省通知※にも記載がある通り、授業内だけではなく、授業外や学校外（家庭への持ち帰り）も含めた利用が想定されています。

これまで教室やパソコン室に配備されていた端末とは使用の目的が根本的に異なるため、過去の端末管理の経験に基づく管理や、旧版の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、クラウド利用を前提としない個人情報保護条例などにより、学校内外における子供たちの端末利活用の機会が奪われることのないよう、十分に留意しましょう。

※ G I G A スクール構想の下で整備された 1 人 1 台端末の積極的な利活用等について 令和 3 年 3 月 12 日（通知）

https://www.mext.go.jp/content/20210312-mxt_jogai01-000011649_002.pdf

（４）その他、関連して必要になる対応

年次更新時の作業

卒業後の児童生徒や、異動した教職員らによる意図せぬ利用が発生しないように、毎年年次更新の作業を実施する必要があります。児童生徒の卒業や教職員の異動に伴って発生する各種管理作業の流れを予め把握し、対応時期も含めて検討の上、適切な時期に行うことが重要です。代表的な作業の例としては以下があります。

- ア. 児童生徒が作成したデータの外部メディア等への書き出し
- イ. 児童生徒の使用していた端末の故障有無を確認
- ウ. 児童生徒の使用していた端末の初期化と最新セキュリティの適用
- エ. 児童生徒のアカウントの削除と新入生のアカウント登録
- オ. 個人端末の持ち込み端末（BYOD）の管理対象外への設定変更及び設定情報の削除

不定期に発生する対応事項の代表例に、故障時の修理対応があります。通常、端末の故障時には、メーカーに修理を依頼します。その際には端末本体のストレージ全体が暗号化されているべきですが、メーカーに提出するシステムログやスクリーンショットの中にも重要性の高い情報が含まれることがあります。

このようなケースに留意しつつ、修理依頼時等でも本ガイドラインやハンドブック（いずれも令和3年5月版）に従った運用を行いましょう。

（５）システム運用管理

① ログの取得に関する考え方

各種ログを適切に取得・保管しておくことは、情報セキュリティインシデントやトラブル等が発生した場合に、問題を解明するための重要な判断材料となります。そのため、ログは一定の期間、端末本体ではなく管理ツールで一元的に保存し、万が一に備えることが重要です。

② 不正ログイン等の防止

MDM（Mobile Device Management）等を用いて適切なポリシーを端末に適用することにより、組織外のアカウントによる不正ログインや不正利用を防止することが可能です。また、本ハンドブック 5-2-(1)でも記載の通り、他人の目に付く場所に重要な情報を放置しないことや、パスワード漏洩が疑われる場合には直ちにパスワードをリセットするなどの運用の徹底が重要です。

6-1 前提

本ハンドブック発行時点（令和3年5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 1 2 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
<p>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。</p> <p>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。</p>	<p>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。</p> <p>学校内からの通信のみに限定した場合に有効。</p>

コラム

効率化のチャンスを活用しよう！

令和2年、内閣府より「地方地方公共団体における押印見直しマニュアル」が公表されるなど、行政手続きの効率化が進められています。教育業界においても、令和2年に「学校が保護者等に求める押印の見直し及び学校・保護者等間における連絡手段のデジタル化の推進について 令和2年10月20日（通知）」が outされています。

https://www.mext.go.jp/content/20210112-mxt_gyokaku-000012094_6.pdf

GIGA スクール構想は子供たちのためだけではなく、教職員の校務・教務の最適化、効率化を実現することも一つの大きな目的です。過去の慣習にとらわれず、新たな取り組みができるチャンスやヒントを最大限活用してみたいかがでしょうか。

(1) 教職員が注意すべき行動規程

教職員の情報セキュリティに関する意識が低いと、重大な情報セキュリティインシデントにつながりかねません。教職員一人一人が重要な情報資産を扱っているという意識を持つ必要があります。教職員が注意すべき事項について、3つの観点から記します。

① 情報セキュリティインシデントが発生しやすい注意すべき行動

情報資産の外部への送信等は、情報セキュリティインシデントにつながりかねない注意すべき行動です。例えば、USBメモリ等の電磁的記録媒体の紛失・盗難、電子メールの誤送信等のリスクがあります。最近では標的型攻撃の事故が多発しており、データ漏洩防止機能等でシステム的に保護するだけでなく、教職員一人一人が十分に注意することが必要です。

教職員が注意すべき行動を図表1-3にまとめました。

図表1-3 情報セキュリティインシデントにつながりかねない注意すべき行動と対応方針の例

注意すべき行動	対応方針 (本ガイドライン(令和3年5月版) 記載内容の要約)
情報資産などの持ち出し	重要性分類Ⅱ以上の情報資産については、無許可での持ち出し禁止
電子メールの利用	差出人が不明または不自然に添付されたファイルを受信した場合は、速やかに削除
	業務上必要のない宛先への送信禁止
	無許可でウェブで利用できるフリーメールサービス等の使用禁止等利用制限
	添付ファイルが付いた電子メールの送受信は不正プログラム対策ソフトウェアでチェックの実施 (暗号化ファイルはウイルススキャンができないため、原則として添付を行わないこと。コラム3-4も参照)
	組織外とのメールで暗号化が必要な場合は、高度な暗号化(S/MIME等)で実施 ※この場合はファイル添付を行わないこと
	重要性分類Ⅱ以上の情報を外部送信する際には、必要に応じクラウド上の共有ドライブで適切なアクセス権限を設定しリンクを送信
USBメモリ等メディアで組織外部へ情報を持ち出し	記録が残るクラウド上のストレージに適切なアクセス制限を設定した上で共有やむを得ず各種メディアにデータを保存する場合は暗号化等の紛失対策を実施
印刷等で組織外部へ情報を持ち出し	印刷物は物理的な暗号化が困難であり、FAXによる送信も受信トレイに放置など、不特定多数の目に触れる可能性が高いため、特に留意して適切な管理を実施
支給端末への外部データ取り込み	外部からデータを取り入れる際の不正プログラム対策ソフトウェアによるチェックを必須化
支給端末への外部からのソフトウェア取り込み	無許可でのソフトウェア導入禁止
	外部からソフトウェアを取り入れる際の不正プログラム対策ソフトウェアによるチェックを必須化
ソーシャルメディアサービスの利用	業務上知り得たすべての非公開情報について無許可での公開を禁止。

② 情報セキュリティレベルを維持するために「してはいけない」行動

学校内の情報システムは、サーバやネットワーク、利用端末にそれぞれセキュリティ対策を講じ、外部からの脅威の侵入を総合的に防御しています。

- ・外部からアプリケーションを取り入れる際に安全の確認をしない。
- ・利用端末のウイルス対策ソフトウェア設定を無断で変更する。
- ・私物端末を学校に持ち込み学校のネットワークに接続する。

これらの行動は、システムのセキュリティレベルを低下させる危険のある行為です。上記のような、情報セキュリティレベルを維持するために「してはいけない」行動を図表 1 4 にまとめました。

図表 1 4 情報セキュリティレベルを維持するために「してはいけない」行動と対応方針の例

情報セキュリティレベルを維持するために「してはいけない」行動		対応方針 (本ガイドライン（令和3年5月版）記載内容の要約)
業務以外の目的でのウェブ閲覧		禁止
無許可で私物機器等の持ち込み		無許可で私物機器等を持ち込んでの業務利用禁止 無許可でのネットワーク接続禁止
端末及びモバイル端末におけるセキュリティ設定の変更		不正プログラム対策ソフトウェアの設定の変更禁止 端末本体の無許可でのセキュリティ設定の変更禁止 不正プログラム対策ソフトウェアによるチェックを定期的実施
無許可での機器の改造及び増設・交換		禁止
コンピュータウイルスへの感染や不正アクセス等、インシデントの発生が疑われる場合の状況放置		インシデントの発生が疑われる端末の電源をスタンバイ状態（サポートされていない場合はシャットダウン）にした上、LANケーブルを取り外し直ちに報告を実施 インシデントの発生が疑われるモバイル端末は、機内モード等電波を発しないモードに設定し、電源をオフにした上、直ちに報告を実施 インシデントの発生が疑われる端末は隔離し、管理者の指示があるまで不特定多数の人が触れないように管理
秘匿すべき情報が容易に目に入る状況の放置	ID,パスワードが目につく場所に表示	パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことの禁止 パスワードを忘れた場合は再発行の処理を実施
	教職員用パソコンに重要な情報が表示されたまま放置	離席時には端末の画面をロックを実施 書類等も容易に閲覧されない場所への保管を実施 端末は、使用中もプライバシーフィルター等で覗き見の防止を行うことを推奨
	重要書類がプリンタやFAXに放置	
	重要書類が机上に放置	
秘匿すべき情報が容易に盗める状況の放置	引き出しが開けっ放し、鍵の付けっ放し	離席時は端末の画面をロックを実施 USBメモリなど電磁的記録媒体や書類等は容易に持ち出されない場所への保管等を実施 廃棄文書はシュレッダーでの裁断等、指定の方法で適切な処理を実施 施錠管理が必要な場合は、施錠確認の確実な実施
	業務書類をゴミ箱にそのまま破棄	
	USBメモリがパソコンにつないだまま放置	
	サーバラックや端末収納ラックが開けっ放し	

③ 保護者への説明事項

校外での端末やクラウドの使用が行われることから、教育情報セキュリティ管理者は運用ルール等を明確にし、必要に応じて保護者へ説明及び協力の依頼をすることが推奨されます。

コラム

セキュリティ認識を最新にしよう

言うまでもないことですが、世の中には不確かな情報が溢れています。特にシステムやセキュリティ周りの情報は、不確定なものや、最新のセキュリティ基準を満たしていないものも散見されます。

最新の本ガイドライン、ハンドブック（いずれも令和3年5月版）等を参照することを心がけ、古い認識や思い込みのままシステム選定を行うことや、根拠（エビデンス）のない情報をSNSや動画サイトで広く公開することは慎みましょう。

（２）外部サービスの利用

外部サービスを利用する場合は、扱う情報資産の重要性に応じた情報セキュリティ対策が講じられていることを利用者側が確認することが重要です。

また、外部委託等で重要性分類Ⅱ以上の情報資産を取り扱う場合、外部委託事業者からの情報漏えい等の情報セキュリティインシデントを防止するために、事業者選定の際には適切な基準に照らして行いましょう。

更に、契約で遵守事項を定めるとともに、定期的実施状況を監査することが必要です。

コラム

クラウドサービスの安全性を確認する規格

使用するクラウドサービスの安全性を確認するには、第三者機関の認証規格を取得しているかが一つの判断基準になります。

例えば、国際標準化機構によって定められたISO規格のISO/IEC27017、ISO/IEC27018等を確認するとよいでしょう。

(1) 校務系サーバの教育委員会による一元管理

学習系サーバのクラウド化が進む中、校務系は従来通りオンプレミスにサーバがある等、本ハンドブック発行（令和3年5月）時点では多くの自治体や学校がハイブリッドな環境にあることが想定されます。学校は入室制限の徹底が難しいことから、学校設置サーバの盗難、損傷等が原因となった情報資産の窃取、喪失等を防止するため、重要な情報資産を格納する校務系サーバは教育委員会管理の校務系クラウドへの移行を計画するなど、教育委員会での一元的な管理を進めていきましょう。また、オンプレミス環境においては、盗難や不正アクセス対策だけではなく、自然災害や火災等により重要な情報資産を滅失すること考えられるため、これらの対策も必須です。

図表 1 5 学校内でサーバを設置する場合の設置事例

- 職員室内の施錠可能なラック内に設置



- 職員室の机上に設置



コラム

データ管理を見直そう

過去の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情報に基づき、「各学校のサーバやストレージは目の届く場所に設置しているので安心」という学校が非常に多いです。

しかし昨今、「想定外」の災害によってデータが失われてしまうという事例が散見されます。また、現在では「信頼性の高いデータセンターなどにデータを保存することが重要」というのが通説になってきています。

改めて、最新の本ガイドライン（令和3年5月版）を参照し、データ管理の在り方を見直しましょう。

(2) 通信回線及び通信回線装置の管理

クラウドサービスの日常的な利活用が標準となる中で、ネットワーク接続に関しては十分に評価を行った上で運用開始に望むことが必須です。また、クラウドサービスとオンプレミスのハイブリッドのように校務系と学習系のネットワーク環境を分ける必要がある場合、セキュリティの観点からも適切なセキュリティ技術を用いての運用を行う必要があります。

① ネットワークとの接続

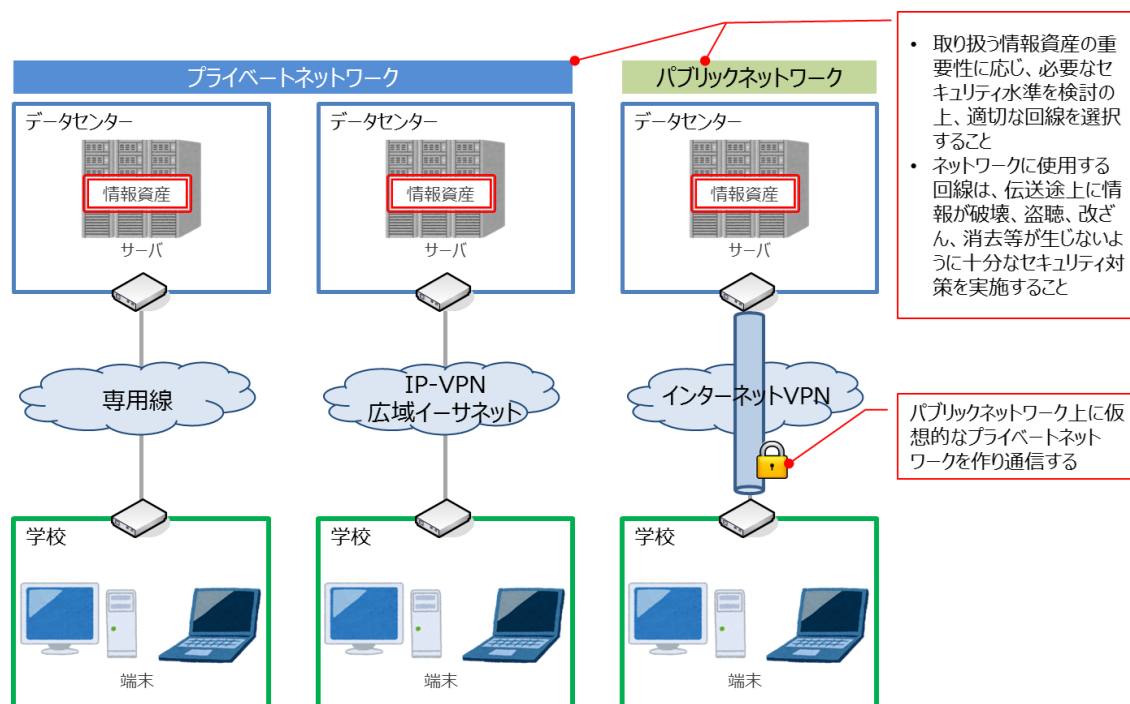
ネットワークとの接続は、円滑な校務及び教務のために重要です。理論値のみに頼らず、例えば平日の時間帯による帯域の状況や授業開始時の短時間で発生する同時接続など、実際の運用に即した評価を項目に加えましょう。また、オンプレミス型のサーバを利用している場合は、受け手側の通信環境も重要になります。適切な処理能力を含んだ環境の選定が重要です。

② 境界防御型におけるデータセンターとのWAN接続

境界防御型の場合、校務系システムで取り扱う情報資産の重要性に応じて、専用線やIP-VPNなど適切なセキュリティ機能を備えたものを選択することが必要となります。このネットワークでは、重要性の高い情報が主に使用されるため、第三者が通信機器やケーブルに容易にアクセスできないようサーバと同様に施錠管理等の管理が必要です。

また、外部ネットワーク（自宅等）からアクセスする場合にも、取り扱う情報資産の重要性に応じて適切なセキュリティ機能を備えた接続が必要になります。

図表 1 6 通信回線のセキュリティの考え方



③ 校内の無線LAN接続

インターネット接続と同様に学校内の無線LANの可用性を確保することは、児童生徒の学習を止めないためにも必須事項です。無線LANの接続にはセキュリティの観点からクライアント証明書を用いることが推奨されます。また、無線LANのアクセスポイントは同時接続数だけでなく、複数のアクセスポイントでカバーされた校内のエリアを移動しても切断されないかを評価する必要があります。

また、日本国内の無線LANの周波数は 2.4GHz帯及び5GHz帯がありますが、それぞれ電波の特性があるため、各校の構造も踏まえた上での設計が重要です。

コラム

MAC アドレス認証は「認証」ではない？！

MACアドレス認証は、「認証」という名前が付いていますが、実はセキュリティの確保された認証ではなく、端末固有のネットワーク ID によるフィルタリングにすぎません。

MAC アドレススプーフィング（偽装）によりアクセスされた情報セキュリティインシデントも報告されており、非常にセキュリティリスクが高いため、使用は避けましょう。

同様に、固定IPを設定したフィルタリングは、セキュリティ対策としての効果は低いのに対して、個々の端末に対して手動で設定を行う必要が生じてしまうため、学校側の作業負担を増大させかねません。端末には、DHCP を利用した動的 IP アドレスを割り振るようにしましょう。

6-4 技術的対策

近年、ネットワークが混在する環境下においては、「全てのネットワークやユーザー、接続される端末を信頼しない」という考え方に基づくセキュリティ対策を行うことが一般的です。教育現場においても、「学校内外を問わず、全ての通信を信用しない」という前提に立った監視及び管理を行うことが必要です。その際に、認証など適切な条件を満たす場合のみアクセスを許可する方式を前提として環境構築を行いましょう。

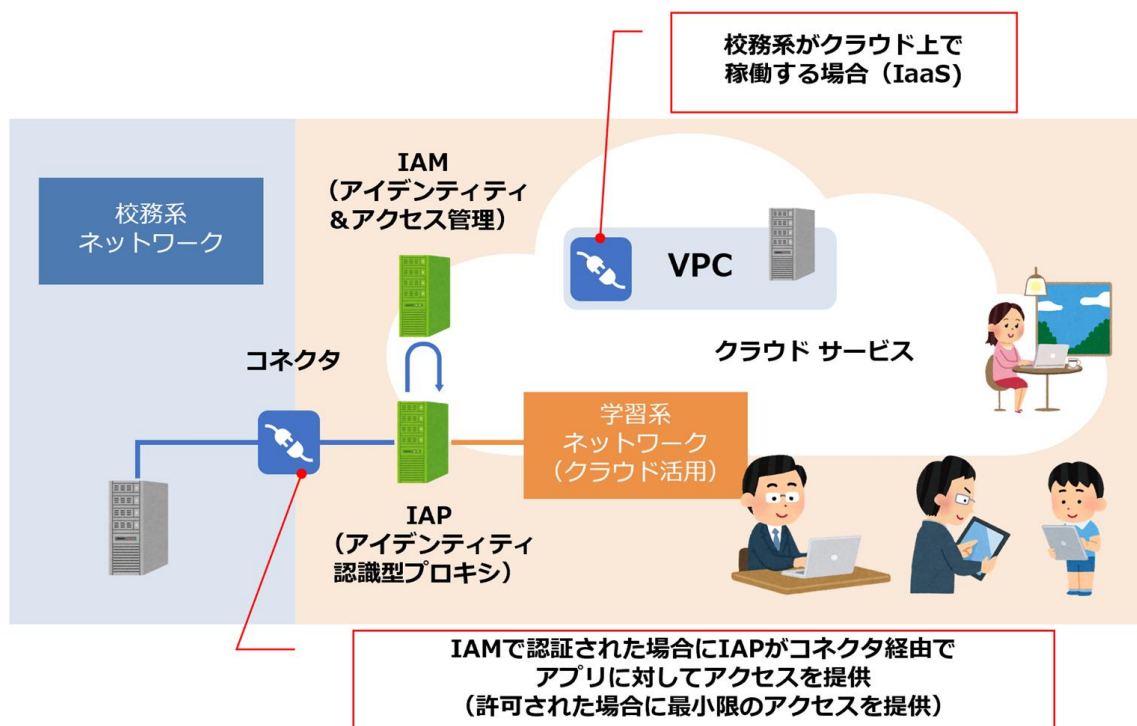
（１）重要性が高い校務系情報に不正アクセスされるリスクへの対応

① アイデンティティ認識型プロキシ（IAP）を用いたアクセス認証型対策

ネットワークが混在する環境下においては、ネットワークやユーザー、端末を原則として信頼せず、IAPなどの技術を用いて全てのアクセスをチェックし、接続の可否を判断するのが一般的になりつつあります。これにより、アプリケーション単位で、教職員及び児童生徒が適切な条件を満たした場合にのみ情報へアクセスできるよう、事前の設定に基づくアクセス制御が可能になります。外出先からでもアクセスできる点は旧来のVPNと同じですが、アプリケーションはネットワークそのものを接続させるわけではなく、コネクタを経由してアクセスするため、極めて限定的なアクセスに留めることができます。

校務系サーバのクラウドへの移行の際にも同一のアクセス制御を用いることが可能ですので、ネットワークの移行計画を進める場合には検討を行いましょう。

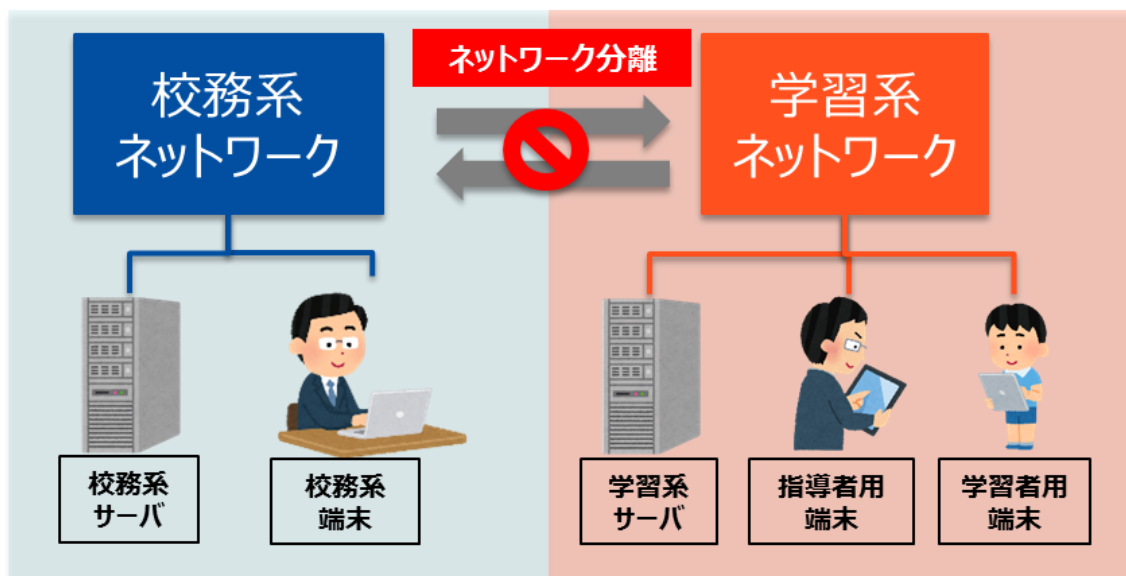
図表 1 7 IAPを用いたアクセス制御



② ネットワーク分離を用いた境界防御型対策

児童生徒を含めた校務系システムへの不正アクセスを防止するため、ネットワークに適切なアクセス制御を施す必要があります。そのため、教職員及び児童生徒が利用する学習系システムから、教職員のみに利用を限定する校務系システムへ不正にアクセスされないように、両システム間の通信経路において論理的又は物理的な分離の徹底が必要です (図表 1 8 参照)。また、校外からオンプレミスの校務系ネットワークへのアクセスを許可する場合にはVPNなどの技術を用いることとなり、セキュリティ対策が複雑になるため注意が必要です。

図表 1 8 境界型防御による通信経路の分離

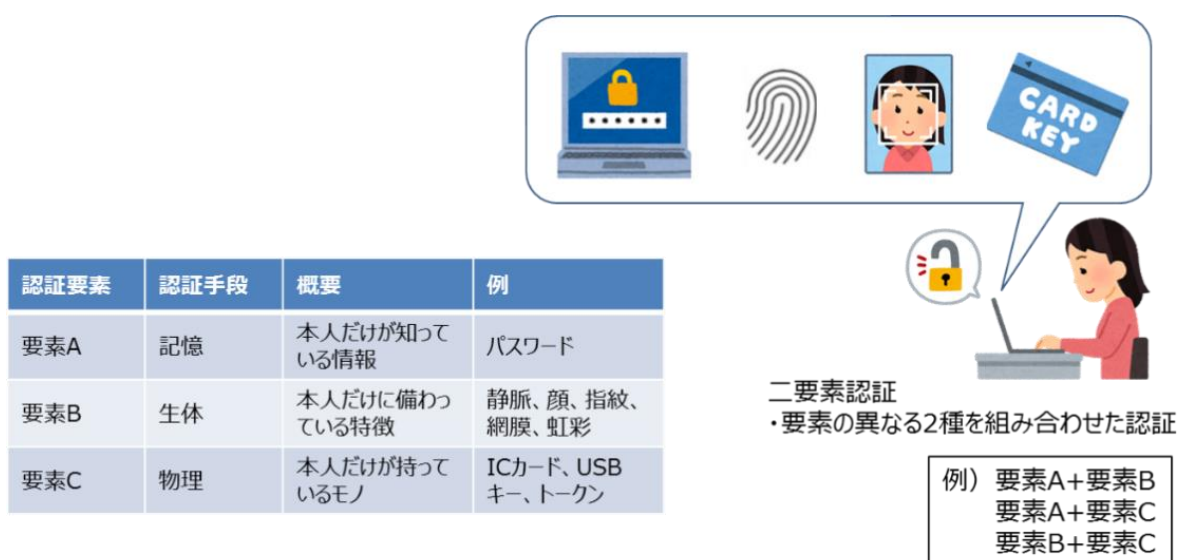


（２）教職員の個人認証強化

教職員は、日常的に重要性分類Ⅱ以上の重要性が高い校務系情報を扱います。学校では厳格な入室制限をするのが難しい（例えば、教職員が校務系情報を扱う職員室等に児童生徒も出入りできる）状況を踏まえると、これらの情報への不正アクセスを防止することが重要なポイントとなります。

アクセス認証型対策及び境界防御型対策のどちらの場合であっても、重要性が高い校務系情報を許可された教職員のみが利用できるよう、取り扱う情報の重要性に応じて、確実な本人確認を行うことが必須です。個人認証の方式としては、従来はID/パスワードの利用が一般的でしたが、それだけに依存してしまうと、万が一ID/パスワードが流出した場合に「なりすまし」で操作される危険性があります。故に、記憶要素、生体要素、物理要素の２つ以上の要素で認証する「多要素認証（MFA：Multi-Factor Authentication）」を用いることで、個人認証を強化することが重要になります（図表 1 9 参照）。また、場所認識型アクセス制御（LAAC：Location Aware Access Control）が利用できる場合には併用することで、セキュリティを強化することが可能です。

図表 1 9 教職員の個人認証強化の考え方

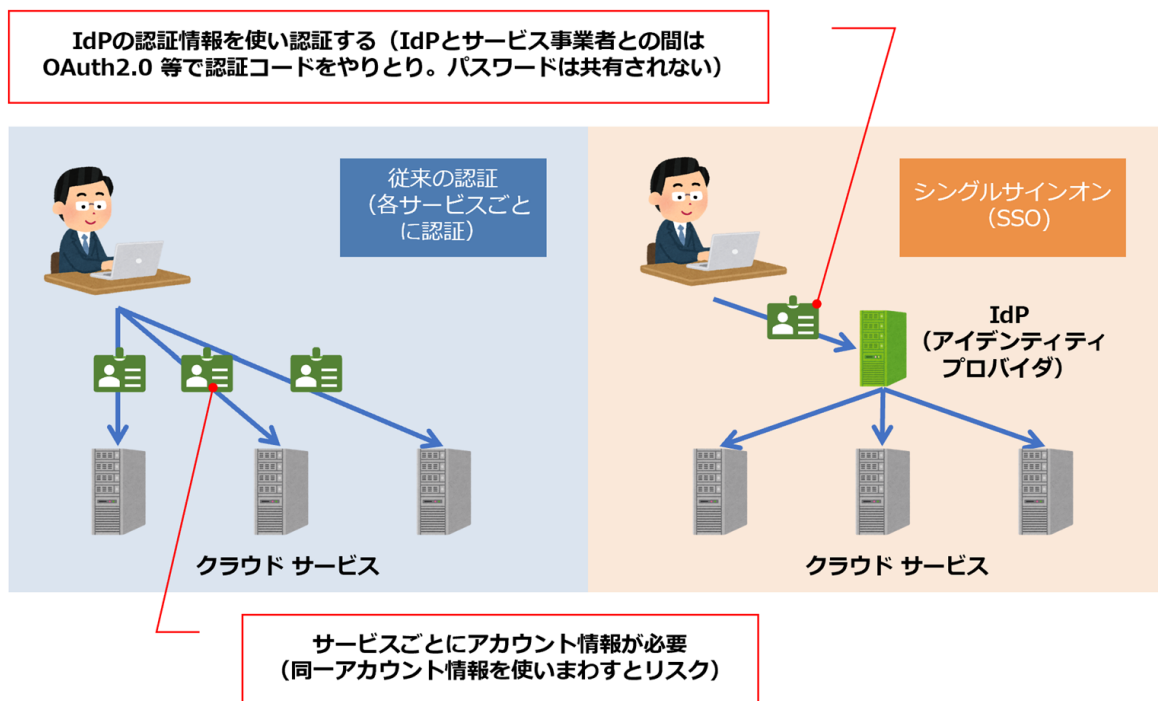


（３）アカウント情報の使い回し防止

異なる会社から提供される複数のサービスを利用する際に、同一のIDとパスワードの組み合わせは、セキュリティ侵害のリスクを増やす大きな要因となります。近年、ニュースで大手企業のアカウント情報流出が取り上げられることも珍しくなくなっています。あるアカウントの情報流出が発生した際に、同一のアカウントの設定を他のサービスでも利用していたために、流出したアカウント情報を用いて他のサービスに侵入されたという情報セキュリティインシデントが多く報告されています。一方、このようなリスクを恐れてパスワードをサービスごとに変えて運用している場合、暗記しやすいパスワードを設定することによって、それぞれのパスワードの強度が低くなる傾向もみられます。

これらを防止するために、シングルサインオン（SSO）を利用することで、アカウントの使い回しによるセキュリティリスクを減らすことが可能です。

図表 2 0 シングルサインオン



コラム

安全なパスワードの作り方

総務省が定める安全なパスワードの作成条件としては、以下のようなものがあります。

総務省「国民のための情報セキュリティサイト」

https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html

- (1) 名前などの個人情報からは推測できないこと
- (2) 英単語などをそのまま使用していないこと
- (3) アルファベットと数字が混在していること
- (4) 適切な長さの文字列であること
- (5) 類推しやすい並び方やその安易な組合せにしないこと

また、第3章（4）のコラムでも触れたように、内閣サイバーセキュリティセンター（NISC）から、**パスワードは定期的に変更する必要はなく**（定期的な変更は逆にセキュリティリスクが高まるため）、流出が疑われる際には速やかに変更する旨が示されています。

（４）潜在的なセキュリティリスクへの対応

セキュリティ対策において、OS等のシステムを常に最新の状態にしておくことは最も重要です。各OSメーカーが頻繁に更新を行う理由の一つが、「最新のセキュリティを提供し続けることにより、悪意のある者が攻撃に準備する時間と労力を掛けさせ、より攻撃されにくい環境を作り出す」という点にあります。故に、アップデートせずに放置しておく、その分だけセキュリティ上のリスクが高まります。

ただし、OSのアップデートの際にはアプリや周辺システムへの影響が発生することもあります。管理者の責任において予め検証等を行う組織体制を整え、OSが最新の状態を確保できるようにしましょう。

一方で、潜在的なセキュリティリスクを下げるために、コミュニケーション用アプリケーション等、児童生徒の学習に役立つ機能を制限をかけるという考え方は、将来の人材を育成するICT教育の趣旨から外れることになります。「次世代を支える子供たちを育てる学校という場において、どうやって子供の力を伸ばしていくのか？」という観点でツールを活用し、学習効果の最大化に繋げることも非常に重要です。

（５）外部への情報資産持ち出しリスクへの対応

① 管理されたUSBメモリ等の電磁的記録媒体以外の使用禁止

私物の電磁的記録媒体の利用による無許可での重要性が高い情報の持ち出し等を禁止するため、教育委員会が管理する電磁的記録媒体以外は業務に利用してはいけませんが、運用ルールのみで制御することは非常に困難であるため、教職員の校務用パソコンにおける電磁的記録媒体へのコピー制限等システムによる制御を併用することで、電磁的記録媒体の持ち込みやデータの持ち出しを綿密に管理し、情報漏えいを防止することが重要です。

また、ウイルス感染を防止するという点でも、教育委員会が管理する電磁的記録媒体以外を教職員に利用させないようにすることが重要です。特に、旧来のインターネットに接続していない校務系システムを利用している場合においては、インターネット経由での不正プログラムの侵入や感染の可能性はありませんが、教職員が持ち込んだ電磁的記録媒体や古くから保管していた電磁的記録媒体から感染することもあり得ますので、電磁的記録媒体の使用は組織内で管理しているものに限る必要があります。

② 電磁的記録媒体の暗号化の徹底

電磁的記録媒体の紛失あるいは盗難は、単に「情報の紛失」のみではなく、それが第三者の手に渡り、情報の漏えいにつながる危険性があるため、電磁的記録媒体については、データ暗号化機能を備える媒体を使用する必要があります。

例えば、通常のUSBメモリは、PCに接続すればすぐに情報を見ることができますが、暗号化機能付きのUSBメモリであれば、データを暗号化して保存したり、データ保存領域へのアクセスにパスワードロックをかけたりすることができるようになるため、USBメモリの紛失や盗難が直ちに情報の漏えいにつながることはなくなります（図表 2 1 参照）。

図表 2 1 電磁的記録媒体の暗号化



学校外へ情報の持ち出しを行う場合、電磁的記録媒体に頼らざるを得ませんでした。しかし、電磁的記録媒体は、各種媒体自体の紛失や盗難が起こりやすく、またそのような際に情報のログを追うことも不可能です。

暗号化等により、紛失や盗難が起こった際に直ちに情報の漏えいにつながるリスクを減らすことはできますが、それらも完全ではないため、過信は禁物です。

「学校が管理しているUSBメモリ＝安心、安全、自由」といった誤った解釈をしないように留意が必要です。アクセス認証型であれば、適切なアクセス権を設定して情報の外部送信を行うことが可能になります。その際、物理的な各種媒体の紛失・盗難は起こりえませんが、全てのログが記録されています。

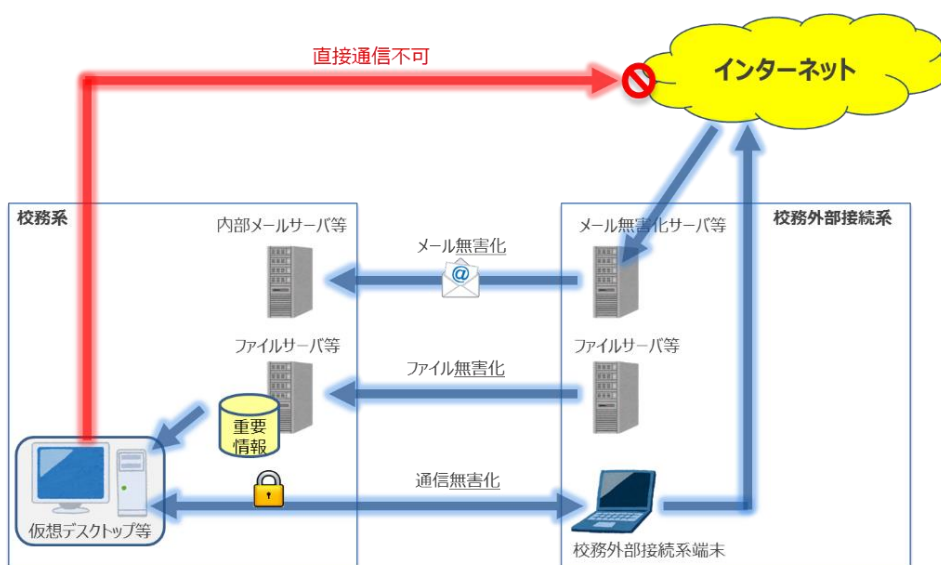
（６）その他、関連して必要になる対応

① 境界防御型対策時の異なるシステム間での無害化処理の実施

校務系・学習系システム及び旧版の教育情報セキュリティポリシーに関するガイドライン（令和元年12月版）で示す校務外部接続系をネットワークで分離している場合、校務系システムと、校務外部接続系システム及び学習系システム間で通信する際に、ウイルス感染のない無害化通信など、適切な措置を講ずる必要があります。

無害化通信とは、インターネットメールに添付されたウイルス付きのファイルを削除しメール本文のみを校務系システムで閲覧可能とすること（メール無害化）や、仮想デスクトップ等サンドボックス化の技術によりインターネット接続を前提としたシステムからのウイルス感染がないようにすること（通信の無害化）の総称となります。なお、ファイルの取り込みにおいては、ファイル無害化機器（ソフトウェア、サービス等も含む）の活用が考えられますが、現状では全てのファイル種に対応していない等、万能ではない点に留意が必要です（図表 2 2 参照）。

図表 2 2 セキュリティレベルの異なるシステム間での無害化処理例



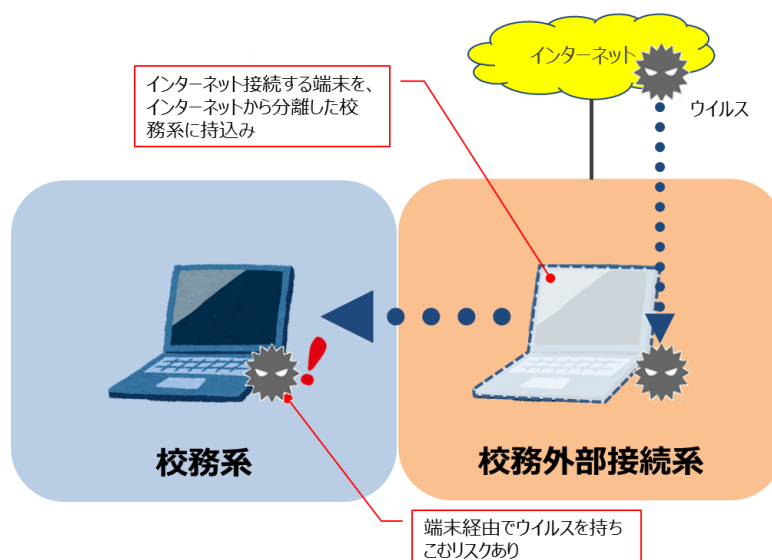
② 校務専用端末の考え方

境界防御型対策では、必要とされるセキュリティレベルの異なるシステム間での端末の共用は避ける必要があります。例えば、インターネット接続を前提とするシステムで利用している端末をインターネットから分離した校務系システムでも利用しようとした場合、端末内にインターネットを介して感染したウイルスが混入している可能性があるためです。この端末を校務系システムに持ちこんでしまった場合、校務系システムにウイルスが拡散するリスクがあり、校務系からインターネットのセキュリティリスクを分離した意味が無くなってしまふ点に留意が必要です。

なお、上記の考え方に従った場合、校務用端末については、以下のいずれかの対応が必要となりますが、各地方公共団体においては、学校現場における校務事務の実態と対策に係る費用等を勘案した上で、対応策について判断する必要があります（図表 2 3 参照）。

- ア アクセス認証型であるアイデンティティ認識型プロキシ（IAP）を用い、コネクタを経由して校務系にアクセスを行うことにより 1 台の端末とする
- イ 「校務系システム」用と「校務外部接続系システム」用の 2 台の端末を使い分ける
- ウ 「校務系システム」用と「校務外部接続系システム」用を論理的に分離（仮想化技術等）することにより 1 台の端末とする
- エ 職員室等に共用のインターネット接続用の端末を配備し、校務用端末についてはインターネット接続を不可とする

図表 2 3 専用端末の考え方



③ 年次更新時の作業

異動した教職員らによる意図せぬ利用が発生しないように、毎年年次更新の作業を実施する必要があります。各組織で運用ルールを定めて適切に実施される必要があります。教職員の年次更新として想定される代表的な例は以下になります。

- ア アカウントの停止・削除
- イ 管理権限の変更・付与
- ウ 法令及び条例の更改に伴うポリシー変更
- エ リソースへのアクセス権限の変更・付与

（７）情報資産の重要性によるシステム運用管理

① ログの取得に関する考え方

各種ログを適切に取得・保管しておくことは、セキュリティ事故が発生した場合に、不正侵入や不正操作等の検知及び問題を解明するための重要な判断材料となります。そのため、一定期間保存し、万が一の際に備えることが重要です。特に、校務系情報は、6か月以上の保管が望ましいです（図表 2-4 参照）。

また、ログは端末本体に保管されるのではなく、MDM等の利用によりサーバで一元管理する必要があります。

図表 2-4 情報セキュリティにおけるログの種別

目的	内容	取得されるログの特長
不正監視	不正な行為によってセキュリティ上の問題が発生していることを知らせる。	不正の早期発見や対応をするために、リアルタイムで収集や分析をする必要がある。
証拠保全	不正な行為があった場合に、事後でその行為の内容や影響を確認する。	不正な行為を厳密に再現し検証できるため、ログの完全性が重要となる。業務利用者や運用者のすべての監査証跡を保存する場合は、大量となることが多い。リアルタイム性はほとんど必要ない。
セキュリティ監査	日々の運用活動の中でセキュリティ対策が正しく機能しているどうかを確認する。	稼働状況や監視状況などまとめられたデータが該当する。

② 情報システムの監視

情報システムにおいて、外部からの攻撃又は侵入、教職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されること等を防ぐためには、情報システムの監視等により稼働状況を常時監視することが必要です。本ガイドライン（令和3年5月版）では、格納する情報資産の重要性に応じ、校務系システムの常時監視を義務付け、学習系システムは常時監視を推奨事項としています。

なお、情報システムの監視において、特に小規模の自治体においては、教育委員会単独でセキュリティの監視体制を整備することは人的・費用的にも困難となることが考えられるため、首長部局と連携しセキュリティの監視体制（複数自治体による情報セキュリティの強化を含む。）を整備することが望ましいです。

また、ログの自動分析ツールを利用することにより、通常と異なる挙動を検出した場合に自動でアラートが発出される仕組みを作ることができます。このような機能は積極的に活用しましょう。特に、ネットワーク以外にも迷惑メールの送受信や巨大なファイルの保存など不審なアクティビティを検出する機能が提供されている場合があります。最新のセキュリティ対策に有効なログ分析ツールに関しても知識を深め、必要な機能を活用しましょう。

図表 2 5 情報システム監視の種別

項目	セキュリティ監視	システム監視 (性能監視、死活監視、リソース監視など)
主に守るべき価値	機密性 (Confidentiality)	可用性 (Availability)
脅威	外部からの攻撃 (標的型、マルウェア、フィッシングなど)、内部漏洩など	自然災害、システムトラブル、操作ミス、設計ミスなど
主なログ	アンチウイルス、ファイアウォール、IDSアラート、アクセス履歴 (監査証跡) など	プロセス稼働、リソース利用状況、Ping、ジョブ結果など
備考	典型的なセキュリティ監視というとこれを指す。	通常 of システム運用で検討される。セキュリティ監視とは位置づけられない場合が多い。

③ バックアップの取得

校務系システムは、成績処理等、教員が毎日の業務において活用するものであり、情報資産を消失した場合、学校事務の遂行に支障を及ぼすことが危惧されます。校務系サーバ及び校務外部接続系サーバについては、必要に応じて定期的にバックアップを実施しましょう。また、学習系サーバにおいても、児童生徒が作成した情報資産が消失し、学習が継続できなくなることを防ぐために、原則バックアップを行うことが望ましいです。

なお、バックアップを行う場合は、災害等による同時被災を回避するため、クラウド上に暗号化して保管したり、バックアップデータの別施設等への保管を考慮することが重要です。

7-1 事業者・自治体に確認すべき事項

(1) 事業者を確認すべきプライバシーの事項

外部委託やクラウドサービスの利用に当たっては、事業者における個人情報の適切な管理が行われていることが必要です。利用を検討しているクラウドサービスにおいて、クラウドサービス事業者における個人情報の収集・利用範囲や管理期間、データの統制と所有の在り方等を確認しましょう。特に、ISO/IEC 27018等の第三者認証の取得状況を確認することや、「児童生徒のプライバシー誓約」「学習者のプライバシーに関する宣言書」等を参考に確認を行いましょう。なお、必ずしも全てを取得している必要はありません。全ての取得を要件とすることで、サービスの過剰な排除となることがないように留意しましょう。

図表 2-6 確認項目の例

確認項目例
(1) 個人情報の定義
(2) 個人情報の取得
(3) 個人情報の利用
(4) 利用目的
(5) 個人情報の第三者への提供
(6) 不適切なポリシー等の変更禁止
(7) 個人情報の保持期間
(8) 個人情報の取扱いについての情報開示
(9) 利用者による個人情報の開示等の請求
(10) 個人情報の適正管理
(11) 委託
(12) 合併/事業譲渡
(13) 匿名加工情報の取り扱い

【参考】

- ・児童生徒のプライバシー誓約 (<https://studentprivacypledge.org/privacy-pledge/>)
- ・学習者のプライバシーに関する宣言書 (<https://giga.ictconnect21.jp/declare/>)

（２）地方自治体における個人情報の利用について

今般の法改正により、地方公共団体の個人情報保護制度について、全国的な共通ルールを規定し、公的部門を含めて全体の所管を個人情報保護委員会に一元化することとなりました（施行は令和５年春頃が見込まれる。）。

改正法においては、いわゆる「オンライン結合制限」に相当する規定は設けず、今後その解釈が示される安全管理措置や利用・提供の制限に係る規定等により、個人情報の安全性を確保することとされています。

しかしながら、現状の地方公共団体における個人情報の取り扱いに関しては、地方公共団体ごとに定められた個人情報保護条例に準拠する必要があるとあり、クラウドサービスを活用して個人情報を取り扱う場合には、個人情報保護審議会へ諮問答申を得ることが必要な自治体も多くあります。

そのため、クラウドサービスにて個人情報を取り扱う際に個人情報保護審議会に諮る上で整理すべき主な項目例を整理しました。

個人情報保護条例は自治体ごと規定されており、個人情報保護審議会への諮問の要否及び、求められる項目はそれぞれ異なるため、確認が必要となります。

図表２７ 整理すべき項目の例

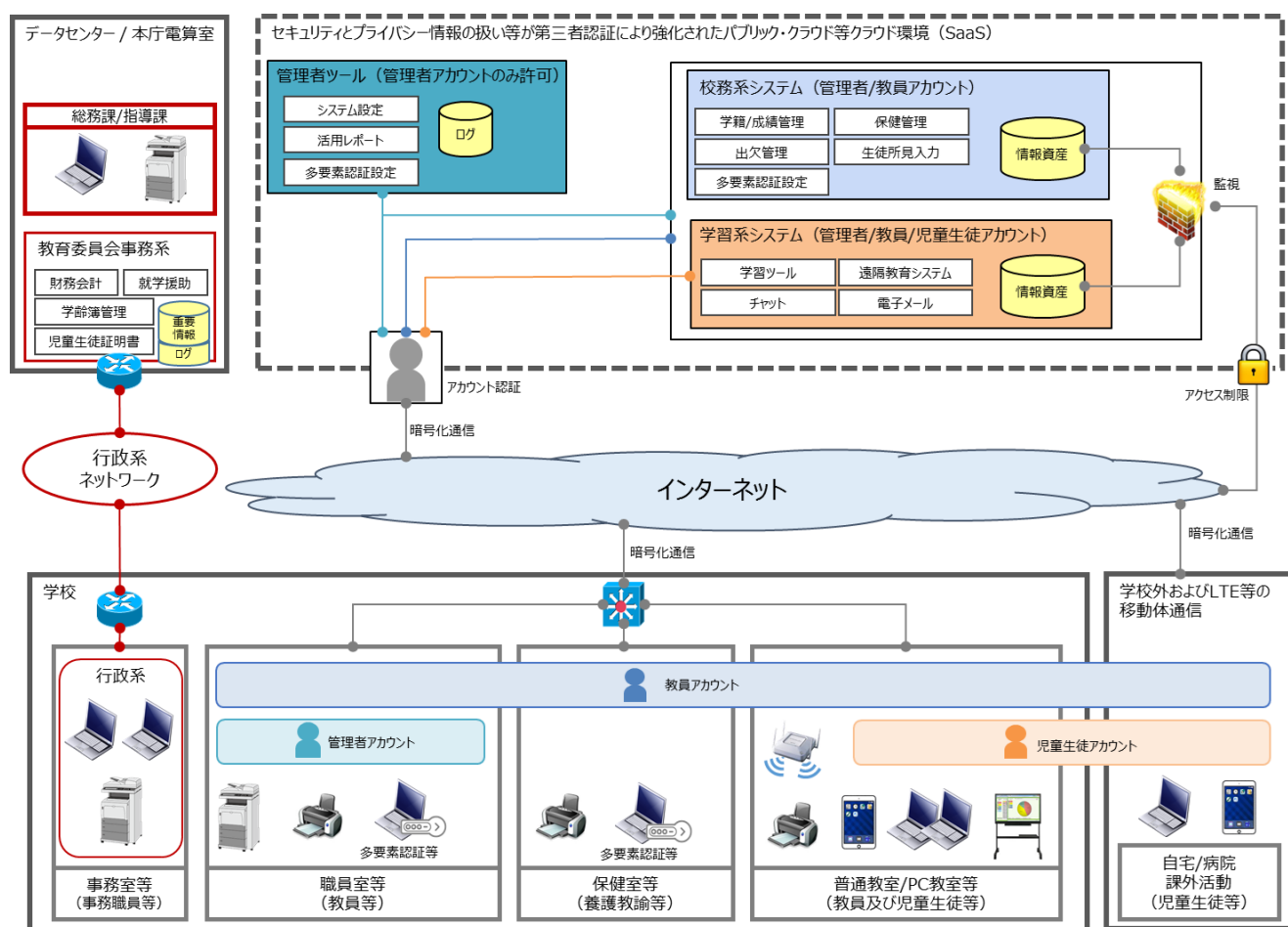
項目例	内容
(1) クラウド活用の目的	当該システムの目的を明確にしておくことが重要。また、個人情報を取り扱う理由も明確化すること。
(2) システムの対象範囲	システムの対象範囲を明確にすること。新規のシステムでは全てが対象になること考えられるが、既存システムの一部にクラウドサービスを利用し、そこで個人情報を取り扱う場合などは、対象部分がわかるように整理することが求められる。
(3) 本人(保護者)同意の要否	本人（保護者）同意の必要性を確認すること。なお、同意を得ることにより個人情報保護審議会への諮問を不要としている自治体もあるため、自治体ごとに確認を行うこと。
(4) セキュリティリスクに対する技術的対策	想定されるリスクを洗い出し、それらのリスクに対してどのような技術的対策を講じているかを整理すること。
(5) インシデント発生時の責任分界点の明確化（クラウド事業者側の体制含む）	組織体制を明確化し、インシデント発生時の取り決めに整理すること。特に、クラウドサービス提供事業者における責任分界点に留意する必要がある。
(6) クラウド事業者の二次利用に対する対策	個人情報提供先のクラウド事業者における二次利用に対する対策を整理する。契約内容で縛ることやクラウド事業者における「個人情報保護方針」及び「プライバシーポリシー」などを確認すること。
(7) クラウド事業者の第三者認証取得の有無	クラウド事業者において、セキュリティやプライバシーに関する第三者認証を取得しているかどうかを確認する。ガイドラインに明記している認証制度の例や「児童生徒のプライバシー誓約」及び「学習者のプライバシーに関する宣言書」などを参考にすること。

テクノロジーの発展に伴い、社会は目まぐるしい速さで変化しています。

次世代を生きる子供たちが、このような変化の激しい社会を生き抜く力をつけるために、教育の在り方や学習の環境も時代に則して変化することは避けられないでしょう。その際に、新たに教育現場に導入されたテクノロジーや、日々更新されるセキュリティの考え方について、「よくわからないから」という理由で見て見ぬ振りをしたり、拒絶したりしては、セキュリティ上のリスクが高まるだけではなく、教育だけが社会から取り残されることにもつながりかねません。次世代を生きる子供たちのためにも、セキュリティを確保した上で適切に活用していくことが求められます。

本ガイドライン及びハンドブック（いずれも令和3年5月版）では、GIGA スクール構想を背景に、児童生徒1人1台端末及びクラウドの利用を前提としました。校務系システムにおいても、クラウド化の流れが想定されます。

図表 2 8 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



本ガイドラインやハンドブックも、時代の流れに則して随時アップデートが行われます。それらを手がかりに、最新のセキュリティの概念や機能を踏まえて、自治体や学校におけるセキュリティ対策を見直すことが大切です。教育委員会の総力を結集して、実態に則した教育情報セキュリティポリシーの策定・見直しをお願いします。

用語	解説
BYAD	Bring Your Assigned Device の略語で、組織に指定された端末を個人が購入し、持ち込みで業務等に使用すること。個人の資産のためライセンス管理等に留意が必要。
BYOD	Bring Your Own Device の略語で、個人の所有する端末を持ち込み業務等に使用すること。個人の資産のためライセンス管理等に留意が必要。
CYOD	Choose Your Own Device の略語で、組織が端末を何種類か用意し、個人は用途に応じて最適な端末を選ぶ方式。
DHCP	Dynamic Host Configuration Protocol の略語で、ネットワークに参加する端末に IP アドレスを動的に（アドレスプールから割り当てて）配布する仕組み。端末の増減にも柔軟に対応可能。
IaaS	Infrastructure as a Service の略語。サーバやストレージ、ネットワークなどのハードウェアやインフラまでをインターネット経由で使えるサービスとして提供。オンプレミスの環境を IaaS に移行し、IAP 等と組み合わせることにより、場所を選ばずにサービス利用が可能。加えて、災害対策の目的でも使用。
IAM または IdM	Identity and Access Management の略語。認証の際に本人、利用目的、接続先、権限等を一元管理で評価。IdM (Identity Management) と同義。
ICT	情報処理 (IT) にコミュニケーション (Communication) が加わった (Information and Communication Technology) もので情報通信技術全般のこと。
IdP	Identity Provider の略語で、SSO 認証時に各種クラウドサービスが行う認証を代行しクラウドサービス側に提供。
IDSアラート	Intrusion Detection System アラートの略称。別称「不正侵入検知システム」。不正な通信を検出し管理者へ警告（アラート）を出すことが可能。
IP-VPN	通信事業者が提供する閉域 IP ネットワーク網を利用した通信技術。
IPアドレス	Internet Protocol アドレスの略語。IP を使って通信する際に端末やサーバを識別する番号。IPv4 や IPv6 というバージョンがあるが一般的には IPv4 を指す。
ISO/IEC 27017	国際標準化機構 (ISO) が「ISO / IEC 27001」のオプションとして標準化した規格で、一般財団法人日本情報経済社会推進協会 (JIPDEC) が ISMS クラウドセキュリティ認証として採用した規格。
ISO/IEC 27018	ISO/IEC 27017 と同様に ISO によって標準化された規格であり、クラウドサービス上の個人情報保護に関する規格。
MACアドレス	ネットワークに接続可能な機器に振られる管理番号。個体識別できるように重複なく提供されるが、設定変更等で書き換えが容易。
MDM	Mobile Device Management の略語で、「モバイル端末管理」ともよばれる端末の管理を行う仕組み。一般に、ポリシーの設定、利用状況の管理、盗難紛失時の対応といった機能を包含。モバイル端末に限らず固定端末の管理も可能であり、端末の持ち出しの有無に関わらず管理の際には使用すべきもの。

用語	解説
OASIS	Organization for the Advancement of Structured Information Standards の略語。eビジネスの非営利国際コンソーシアムであり、各種技術の標準化を推進。
OS	Operating System の略語。端末（コンピュータ）が動作（操作・運用・運転）するための基礎となるシステム。
PaaS	Platform as a Service の略語。IaaS と異なりプラットフォーム（OS）をインターネット経由で使えるサービスとして提供。各サービスプロバイダによって異なるプラットフォームを提供。
Ping	インターネットや LAN 等、IP ネットワーク（IP アドレスを使用したネットワーク）で端末から端末などへの通信が繋がっているかを確認するコマンドの一つ。「ピン」または「ピング」と発音。ping で応答がある場合はネットワークの経路があるとみなすことが可能。一方、セキュリティの観点で端末をpingに回答させない設定も可能であり、ネットワーク経路があってもpingで回答がないケースも存在。
OAuth 2.0	RFC で定義された権限の認可（authorization）を行うための規格。特定のデータに対し、特定の操作を許可するための仕組みでアカウント等の認証（Authentication）を行うものとは異なる。
RFC	Request for Comments の略語。インターネットに関する標準化団体（IETF：the Internet Engineering Task Force）により、技術仕様ドキュメントは RFC 番号で管理（例えば TCP/IP の TCP は RFC793 にて定義）。
SaaS	Software as a Service の略語。IaaS と異なりアプリケーションをインターネット経由で使えるサービスとして提供。インターネット上のメールサービスやストレージサービスなどは SaaS に分類。
SAML	Security Assertion Markup Language の略称。OASIS によって定義された標準で、異なるサービスでユーザーの認証を行う際に使用。SSO を実現する際に使用されるプロトコルの代表。
VPC	Virtual Private Cloud の略語。インターネット上に構築する仮想プライベートネットワークで、多くは IaaS として提供。
WAN接続	LAN と LAN を結ぶネットワーク（最上位にあたるのがインターネット）。
アイデンティティ認識型プロキシ（IAP）	Identity-Aware Proxy の略語。別称「ID 認証型プロキシ」。オンプレミスや IaaS など、保護されたネットワーク上にコネクタと呼ばれるサーバを設置し、IAP が認証とアプリケーションの通信を橋渡しする。VPN とは異なり、ネットワークそのものを繋がないため、セキュリティを高めたままインターネット経由での利用が可能。
アカウント	コンピュータやネットワークに接続（ログイン）するために必要になる権利情報のこと。 ※一般的には単に「ID」や「メールアドレス」を指す場合もある。
アクセスポイント	有線ネットワークと端末等を無線で接続するための機器。
アクセス制御	ユーザー等に対して、どのような権限をもって情報にアクセスできるか（禁止、閲覧、編集等）を設定することで行う制御。
アプリケーション	OS 上で動作するソフトウェア。ソフトウェアまたはソフトをアプリケーションと同義で使用されているケースもあるが、本来は OS やファームウェアなどを含み、ハードウェアと対比して使用。
オンプレミス	サーバーやソフトウェア等のシステムをユーザーが管理する施設に設置し、管理運用する方式。
クラウド	ユーザー側の環境に影響されず、インターネット上で利用可能なサービスの総称。

用語	解説
グローバルIPアドレス	インターネットに接続する端末に一意に割り振られた識別番号（電話番号をイメージすると良い）。別称「パブリック IP アドレス」。
固定IPアドレス	DHCP サーバがない場合など、手動で端末に設定する固定の IP アドレス。別称「スタティック IP アドレス」。管理運用及びセキュリティ上のリスクから非推奨。
コネクタ	IAP に接続するためのコネクタ。別称「IAP コネクタ」。
サーバ	ユーザーのリクエスト（命令）に対してサービス（機能）を提供するソフトウェアまたは、それらが搭載されたコンピュータ。
情報セキュリティインシデント	情報流出等の情報セキュリティに関わる事件や事故。
シングルサインオン（SSO）	英語表記では Single Sign-On（SSO）。一度のユーザ認証で複数の異なるサービスの認証と利用を可能にする仕組み。同一のアカウント情報を複数のサービスに使い回すリスクがなくなるほか、管理するアカウントも 1 つのみで良くなり管理性と利便性が向上。SSO の実現には SAML、OAuth2.0、OpenID Connect等のプロトコルを使用。
スイート製品	単体でも利用可能なアプリケーションやサービスをセットにした製品。電子メール、文章作成、プレゼンテーション、表計算、チャット機能などのビジネスアプリケーション及びサービスをセットにしたものが代表的。
ストレージ	端末やサーバ等でデータを保管するための記憶装置またはその領域。
セーフサーチ	検索エンジン等で提供される過激なコンテンツへのアクセスを制限する仕組み。
セーフブラウジング	検索エンジン等で提供される悪意のあるWebサイトへのアクセスを制限または警告する仕組み。
セキュリティ対策パッチ	システムやプログラムで判明した脆弱性を補填するためのプログラム更新。
ゼロトラスト	クラウドサービスの登場によりいつでもどこでもサービスの利用ができるようになったことを背景に、接続後のネットワークは安全だと信頼するのではなく、「全てのアクセスにはセキュリティリスクが潜んでいる」という前提の上で、IAM を用いてアクセス時に本人の認証や安全性の確認を毎回行い、管理・監視する方式。旧来の方式（VPN 等）では不十分なセキュリティを置き換える技術。
多段認証	リソースに限定されず、2 回以上の認証を行うこと。多要素認証と混同されやすいが、例えば第一パスワード、第二パスワードのように、同一リソースの要素を 2 回認証した場合も多段認証に包含。
多要素認証	記憶と物理や生体といった、リソースの異なる要素を 2 つ以上利用した認証を行うこと。
データセンター	サーバやストレージ、ネットワーク接続機器を管理する施設。データセンターの住所はセキュリティ上の理由から非公開になっている場合も多い（国や地域のみを公表など）。
デジタルトランスフォーメーション（DX）	社会の急速な変化やニーズに対応し、データとデジタル技術を活用して、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、組織文化・風土を変革することで人々の生活の質を向上させる活動。
電磁的記録媒体	情報資産を扱うサーバ装置、端末、デジタルカメラ、デジタルビデオカメラ、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体。
動的IPアドレス	DHCP サーバより端末に動的に配布された IP アドレス。別称「ダイナミックIPアドレス」。

用語	解説
ネットワーク制御	閉域網等を利用して、物理的または論理的に通信が可能な領域を制限する方法。
ハイブリッドクラウド	オンプレミス環境とクラウド環境が混在した状態。
場所認識型アクセス制御（LAAC : Location Aware Access Control）	地理情報に基づいたアクセス制御を行う仕組み。例えば、海外からのアクセスは不可とするといった運用ルールを作ること、不正なアクセスリスクを低減させることが可能。
バックアップ	不測の事態に備えて、情報資産等を事前に二重で保管しておくこと。
ファイアウォール	ネットワークの接続点において、通信を監視、制御、防御するシステム。
フィルタリングソフト	特定の動作（ウェブサイト閲覧やダウンロード等）をルールに基づいて制限するソフト。
無害化通信	受け渡しされるデータに対して、悪意のあるプログラムを取り除いて行われる通信。
無線LAN	無線で構成されるローカルネットワーク。
ローカルIPアドレス	無線や有線 LAN 等、IP を使用して通信する際に使用される IP アドレスで、同一ネットワーク上で一意に割り振られた識別番号（内線番号をイメージすると良い）。別称「プライベート IP アドレス」。
ログ	各種機器の利用状況やネットワークにおける通信履歴等の記録。
ワイプ	端末等の記憶装置に保存されているデータを消去すること。

「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

- ◇ 発行日 令和3年5月
 - ◇ 発 行 文部科学省
-