「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

平成 29 年 11 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」ハンドブック

◆目　次

【このハンドブックについて】

このハンドブックは、文部科学省で策定された「教育情報セキュリティポリシーに関するガイドライン」（平成 29 年 10 月 18 日）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。

第1章 ◉ はじめに

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、大切な情報を、さまざまな脅威から守り、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、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。その際の参考として、総務省では、「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」を策定し公開しています。また、近年は標的型攻撃等、大切な情報を外部から狙うセキュリティ事故が社会的な問題となっています。このような悪意のある外部の者による情報の窃取・改ざん等への対策として、平成 27 年より、全国の地方公共団体において、新たな自治体情報セキュリティ対策の抜本的強化に向けた対策が講じられています。

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を策定した背景[*1]

他の行政事務では、職員以外の者（市民の方など）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が、学校では、教室やパソコン室に児童生徒が自由に使えるパソコンが設置されており、授業はもとより休み時間等においても、児童生徒が、日常的に情報システムにアクセスする機会があります。このことが、学校現場における最大の特徴といえます。

実際に、学校が保有する機微情報に対する不正アクセス事案が発生しており、学校現場ならではの特徴を考慮した情報セキュリティを確立する必要性が高まったことから、「教育情報セキュリティポリシーに関するガイドライン」（以下「本ガイドライン」という）を策定しました。

コラム 1

文部科学省委託調査（平成 29 年 2 月）によりますと、現在、学校を対象とした情報セキュリティポリシーを策定していない教育委員会は全国平均で 36％で、町村教育委員会平均では 59％に上ります。このように学校における情報セキュリティ対策が確立しているとは言い難い状況となっていることも、本ガイドライン策定に至った背景のひとつです。

*1 1.2. 本ガイドライン制定の背景（ハンドブックの記載内容に対応するガイドライン本文の目次を脚注に記しています。）

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

2.1 本ガイドラインの目的

情報セキュリティ対策は、安心して学校において 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、学校においては、児童生徒が日常的に情報システムにアクセスする機会がある等、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、学校向けの情報セキュリティポリシーを策定し、学校現場の特徴を踏まえた情報セキュリティ対策を講じる必要があります。本ガイドラインは、そのための参考として、情報セキュリティ対策の考え方を示したものです。

2.2 本ガイドラインの構成[*2]

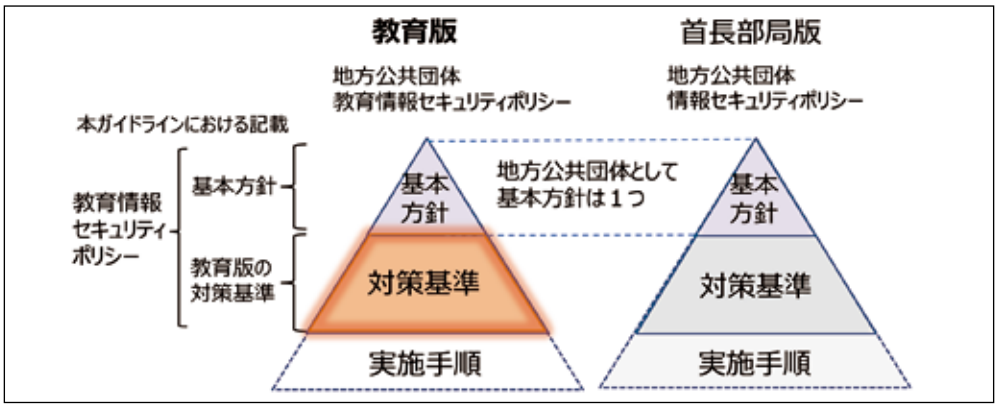
情報セキュリティポリシーは、「基本方針」と「対策基準」の２つから構成されます。

「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、本ガイドラインにおいて具体的な記載をしています（図表１参照）。

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



コラム２

基本方針とは、地方公共団体のトップが、「情報セキュリティに本格的に取り組む」という姿勢を示し、情報セキュリティの目標と、その目標を達成するために地方公共団体がとるべき行動を内外に宣言するものです。「なぜセキュリティが必要か」という「Why」について規定し、何をどこまで守るのか（対象範囲）、誰が責任者かを明確にします。

対策基準とは、基本方針で作成した目的を受けて、「何を実施しなければならないか」という「What」について記述します。組織的に情報セキュリティ対策を行うためのルール集です。実際に守るべき規程を具体的に記述し、適用範囲や対象者を明確にします。

実施手順とは、対策基準で定めた規程を実施する際に、「どのように実施するか」という「How」について記述します。マニュアル的な位置づけの文書であり、詳細な手順を記述します。

（出所：情報処理推進機構（IPA）ホームページ「情報セキュリティポリシ - の作成」）

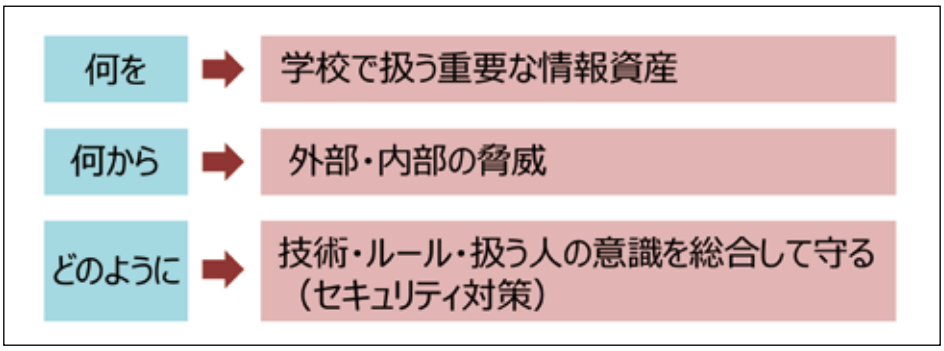
*2　ガイドライン 1.4. 教育情報セキュリティポリシーの構成と学校を対象とした「対策基準」の必要性

第3章 ◉ 情報セキュリティ対策の基本的考え方

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、「何を」、「何から」、「どのように」守るかを明らかにすることです（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？

本ガイドラインで想定する「守る対象」は、「情報資産」です。「資産」とは、業務遂行の過程で生み出される価値あるもののことです。本ガイドラインでは、学校が保有している情報全般を指して「情報資産」と称しています。また、この、学校の名簿や成績などの情報自体に加えて、それらを記載したファイルや電子メールなどのデータ、データが保存されているパソコンやサーバ、CD-ROM、USB メモリなどの記録媒体も情報資産に含まれます。

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。これは、一言で言えば、「脅威」になります。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、大きく分けて以下の５つの観点から整理することができます。

①内部の者による情報資産の窃取・改ざん等

情報資産を扱う内部の人間がルールを守らないことは情報資産の漏えい・紛失等の原因となります。このため、組織的な情報セキュリティポリシーの遵守状態の可視化・ルール改善や、実効性のある人的なセキュリティ対策が必要です。

②自然災害等による情報資産の滅失等

地震、水害、火災等により、サーバ等の情報資産を保管する機器類が被災して、情報資産が滅失する場合もあります。このため、自然災害等の「脅威」に対する対策を講ずる必要があります。

③児童生徒のいたずら等による情報資産の窃取・改ざん等

児童生徒がいたずら等により、学校の情報資産を窃取・改ざんする可能性もあります。これは学校特有の「脅威」と言えます。

コラム３

近年、ある学校で、同校生徒が教職員用サーバに接続して情報を持ち出し、多数の生徒個人情報がインターネット上に流出する事案が発生しました。この生徒は、校内の生徒用パソコンで教職員が管理するサーバにログインして情報を窃取しており、ログインに必要なパスワードを見て記憶し、アクセスしていました。このようなことが起きないように、教職員は自分専用のID/ パスワードを他者に知られないよう十分な安全管理が求められます。

④悪意のある外部の者による情報資産の窃取・改ざん等

児童生徒だけでなく、悪意のある外部の第三者によるインターネット経由での情報資産の窃取や改ざんを防ぐ対策も必要です。

最近は、知り合いを装った電子メールにウイルス付きのファイルを添付し、当該ファイルを開かせ、標的とした組織の情報システムを本人が気が付かないままウイルスに感染させて、情報資産の窃取・改ざん等を行う「標的型攻撃」が大きな社会問題になっています。このような場合は、技術的なセキュリティ対策だけでは防ぎきれず、組織的・人的セキュリティ対策を組み合わせた対策が必要になってきます。

コラム４

情報処理推進機構（IPA）発行の「組織における情報セキュリティ 10 大脅威 2017」（図表３参照）では社会的影響の大きかったセキュリティの脅威として、標的型攻撃による情報流出が 1 位でした。標的型攻撃には充分注意してください。

図表３　情報セキュリティ 10 大脅威 2017

順位	組織
1位	標的型攻撃による情報流出
2位	ランサムウェアによる被害
3位	ウェブサービスからの個人情報の窃取
4位	サービス妨害攻撃によるサービスの停止
5位	内部不正による情報漏えいとそれに伴う業務停止
6位	ウェブサイトの改ざん
7位	ウェブサービスへの不正ログイン
8位	IoT機器の脆弱性の顕在化
9位	攻撃のビジネス化（アンダーグラウンドサービス）
10位	インターネットバンキングやクレジットカード情報の不正利用

（出所：情報処理推進機構（IPA）ホームページ　情報セキュリティ 10 大脅威 2017）

⑤教職員の過失による情報資産の漏えい・紛失等

情報資産への「脅威」は悪意ある者による行為だけが原因になるわけではありません。教職員が情報を外部に持ち出すことで、結果として情報資産を漏えい・紛失してしまうことも「脅威」です。

コラム５

書類の紛失を含めて個人情報の不適切な取扱に係って懲戒処分された教職員は、平成 27 年度で 309 人に上っており他人事ではありません。（出所：平成 27 年度公立学校教職員の人事行政状況調査（文部科学省））

3.4　情報資産を脅威から「どのように」守るのか？

最後に、①～⑤に代表される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。

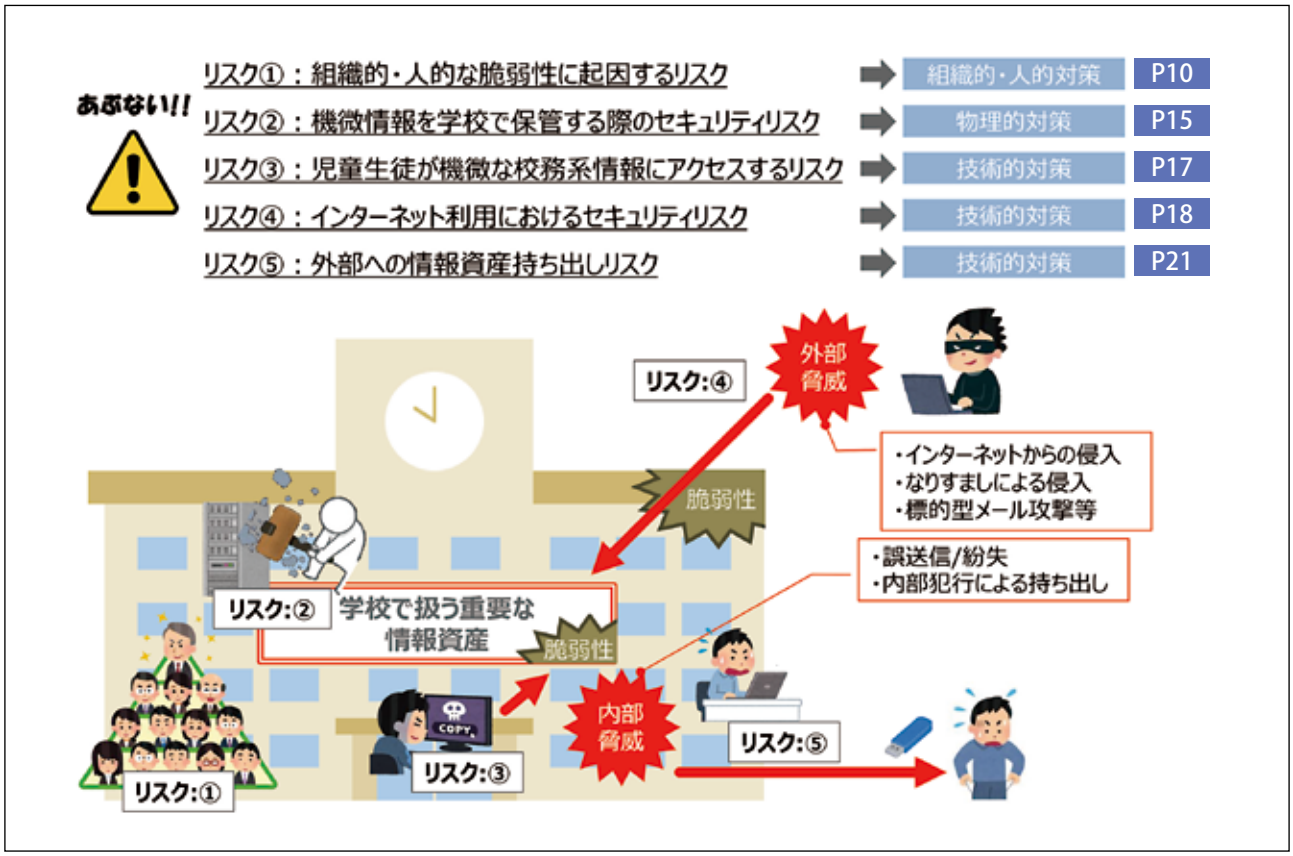
情報セキュリティ面で弱い部分（脆弱性）があると、そこから脅威が侵入しやすくなります（図表４参照）。

そこで、情報資産を脅威から守るためには、脅威の大きさに応じて情報セキュリティ面の弱い部分を補強し、リスクを基準以下に保つ必要があります。

この具体的な対策手段として、本ガイドライン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」などが挙げられ、各観点から総合的に対策を講ずる必要があります。もし対策の一部に弱い部分があると、そこから「脅威」の侵入を許してセキュリティ事故につながる危険性が高まります。ただし、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、校務情報の安全性の両面を共存させながら対策を講ずる必要があります。

これらの具体的な対策については第４章に記します。

図表４　学校における情報セキュリティリスクと対策



第4章 ◉ 学校を対象とした情報セキュリティ対策

4.1 情報資産の分類と管理方法 *3

(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。したがって、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（図表5参照）。

図表５　重要性分類ごとの情報資産の持ち出し制限と例示（抜粋）

情報資産の分類					情報資産の例示		
重要性分類	機密性	完全性	可用性	定義	持ち出しの禁止	持ち出しの制限	持ち出しの制限無し
Ⅰ	3	2 B	2 B	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。	・指導要録原本 ・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	2 B	2 B	2 B	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。	○学籍関係 ・出席簿 ○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 ・健康診断に関する表簿 ・健康診断票 ○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 ・情報端末ログインID/PW	○成績関係 ・通知表 ○指導関係 ・児童・生徒等の写真 ○進路関係 ・調査書 ○健康関係 ・児童・生徒等健康調査票 ○その他 ・給食関係書類・寄宿関係資料 ○名簿等 ・児童生徒名簿 ○児童生徒の学習系情報（学習後に回収したもの） ・児童生徒の学習記録（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）	
Ⅲ	2 A	2 A	2 A	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。		○児童生徒の学習系情報（学習中） ・児童生徒の学習記録 ・学習活動の記録（動画・写真等） ○学校運営関係 ・卒業アルバム	
Ⅳ	1	1	1	影響をほとんど及ぼさない。			○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 ・授業用教材 ・教材研究資料 ・生徒用配布プリント

(2) 情報資産の管理の考え方

学校で扱う情報資産は，大きく校務系情報と学習系情報に分けられます。

成績処理や児童生徒の指導記録等の校務系情報は、機微な情報を含み、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づけられます。このため、インターネット等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。

*3　ガイドライン 2.3. 情報資産の分類と管理方法

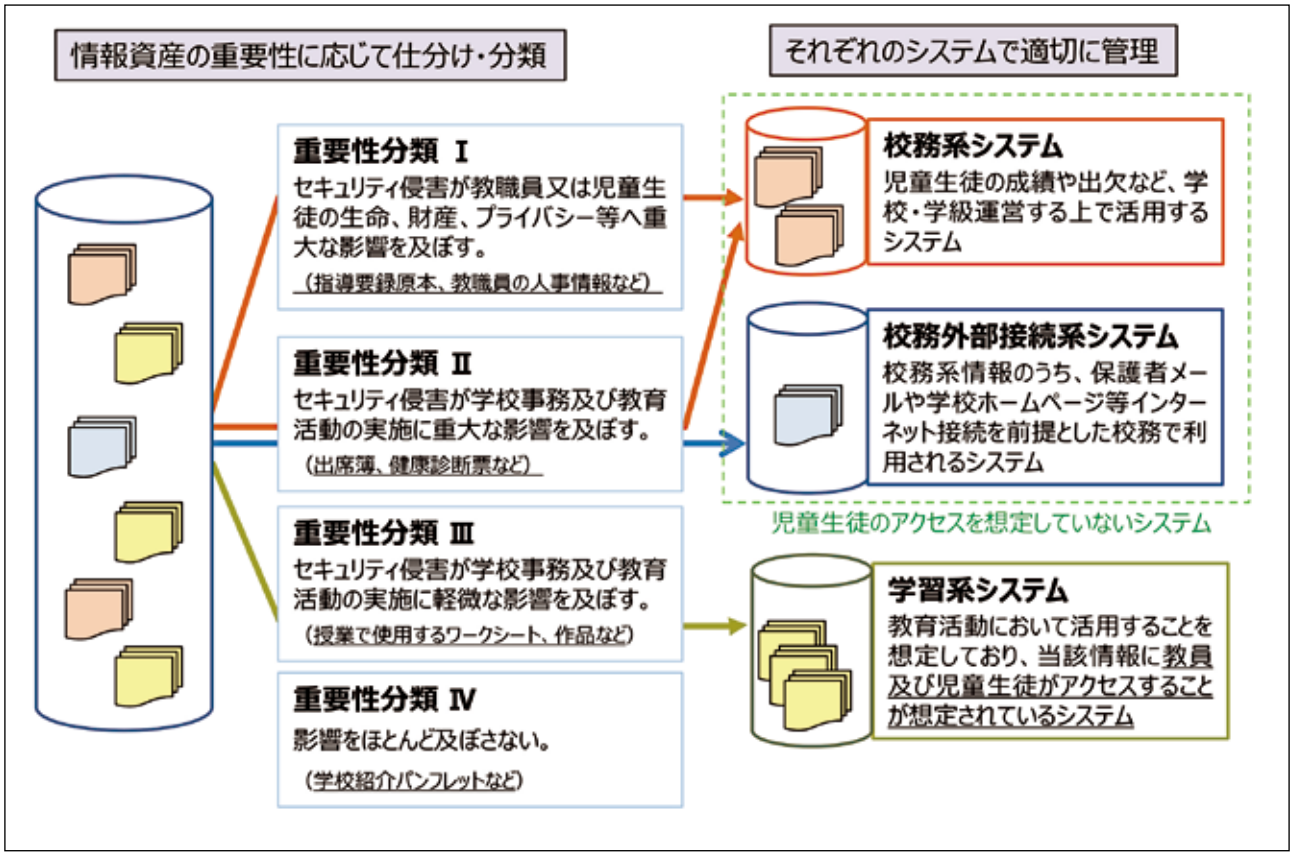
一方で、児童生徒が授業等で活用するワークシート等の学習系情報は、学習活動を通して生成されるものであり、教員はもとより、児童生徒もアクセスすることが前提となっています。このため、「校務系情報」とは区別して対策を講ずる必要がある一方で、学習系情報であっても、学外に公表することを前提にしていない情報を含む場合もあるため、学校の外に漏えいしないように対策を講ずることが必要となります。

情報資産は、図表５で書かれている「重要性分類」によってその守り方が異なるため、重要性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。

本ガイドラインでは、重要性分類Ⅰ とⅡの情報資産については、機微な情報を含むため、インターネット接続を前提とするシステムで管理しないことを原則としています。

一方で、機微な校務系情報であっても、保護者との緊急時メール連絡等、インターネット接続が必要な場合があります。このような情報については、「校務外部接続系情報」と定義し、その他の機微な校務系情報と重要性分類が同じであっても、インターネット接続を前提とした上で、必要な対策を講ずることとしています（図表６参照）。

図表６　情報資産の重要性分類に応じた管理の考え方



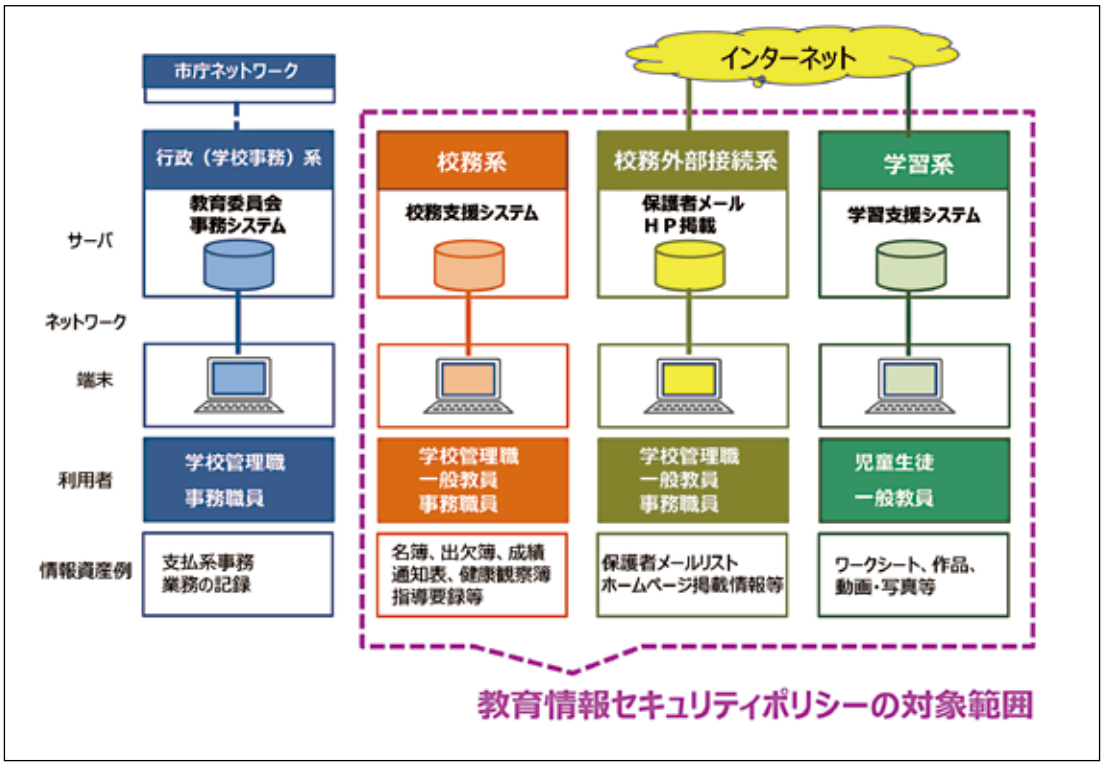
4.2　セキュリティ対策の対象範囲

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」、「校務外部接続系システム」、「学習系システム」、「行政系システム」の４つの情報システムが存在します[*4]。

本ガイドラインでは、このうち、「校務系システム」、「校務外部接続系システム」、「学習系システム」を対象とします（図表７参照）。

*4　各システムの用語の定義は、ガイドライン 2.1. 対象範囲及び用語説明の章に記載してあります。

図表７　セキュリティ対策の対象範囲



4.3　組織的･人的対策

（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。

①学校と教育委員会の役割分担[*5]

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。

特に、学校は、児童生徒の教育を司る教員を中心に構成されることを踏まえると、情報システム及びセキュリティに関することは、教育委員会が責任を持って管理することが、極めて重要になります。

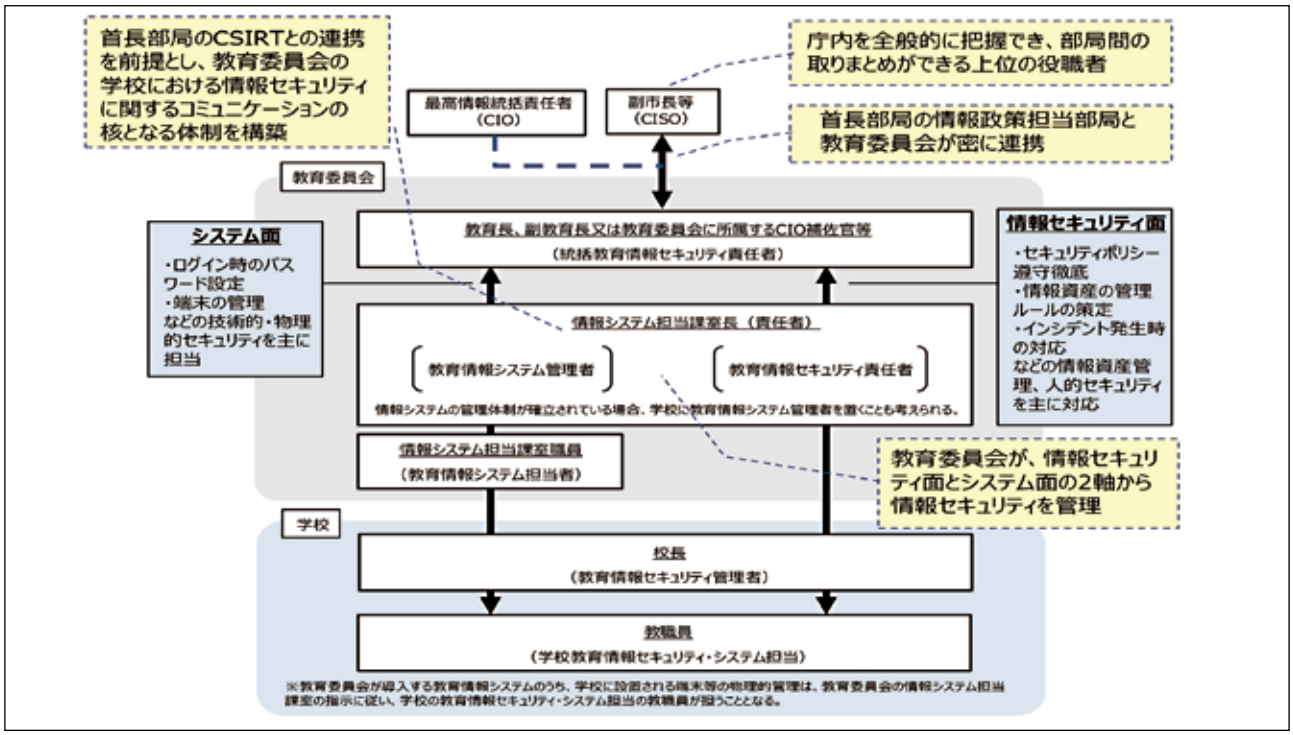
②組織体制の考え方[*6]

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、本ガイドラインにおいては、教育情報セキュリティの最高責任者（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、情報セキュリティ対策を組織的に実行することや、新たなセキュリティ事故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です。（図表 8 参照）。

*5　*6　ガイドライン 1.3. 地方公共団体における教育情報セキュリティの考え方①及び 2.2. 組織体制

図表８　情報セキュリティ推進の組織体制例



コラム６

情報セキュリティ事故が発生した際には、内容把握･分析し、被害拡大防止、復旧、再発防止、対外対応等が必要になるため、首長部局の「情報セキュリティにおける統一的な窓口：CSIRT（Computer Security Incident Response Team）とも呼ぶ」に報告する必要があります。一方、学校で発生する情報セキュリティ事故については、その重要度や影響範囲等を勘案するには教育委員会の関与が不可欠であるため､教育委員会においても首長部局のCSIRTと連携する体制を確立し､日頃は情報セキュリティに関する学校の相談窓口や情報共有をすることが望まれます。

（２）　組織的な情報セキュリティの確保

「４．３（1）組織体制の確立」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が確立できたら、次は、CISO 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、以下のような対策を講ずることが必要です。

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

情報セキュリティ事故の原因の多くは、情報資産を扱う教職員の過失によるものであることから、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、セキュリティ事故は、適切な初期対応が被害を最小限に留めるうえで重要です。このため、セキュリティ事故について疑いがある場合を含めて報告ルールを整備することも重要です（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

情報セキュリティを維持するために必要な行動	ガイドライン規定要約	ガイドラインの出所
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	2.5.人的セキュリティ2.5.2.(1)
研修計画の策定及び実施	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【推奨事項】	2.5.人的セキュリティ2.5.2.(2)
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	2.5.人的セキュリティ2.5.2.(4)
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	2.5.人的セキュリティ2.5.3.(1)

②評価・見直し[*7]

（ア）監査

監査により、情報セキュリティポリシーの遵守実態を把握し、セキュリティ対策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

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、自己点検を定期的に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、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を、定期的に見直すことが求められます。

（3） 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場合、重大な情報セキュリティ事故につながるため、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セキュリティ事故が発生しやすい注意すべき行動

情報資産の外部への持ち出し等は、セキュリティ事故につながりかねない注意すべき行動であり、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につながるリスクがあります。また、最近では標的型攻撃の事故が多発しており、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 10 にまとめました。

図表 10　セキュリティ事故につながりかねない注意すべき行動

注意すべき行動	ガイドライン規定要約	ガイドラインの出所
電子メールの利用	差出人が不明又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	2.6.技術的セキュリティ2.6.4.(3)⑤
	業務上必要のない送信先への送信禁止	2.6.技術的セキュリティ2.6.1.(16)②
	無許可での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	2.6.技術的セキュリティ2.6.1.(16)⑤
	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	2.6.技術的セキュリティ2.6.4.(3)⑤
	機密性２A以上の情報を外部送信する者は、必要に応じ暗号化又はパスワード設定	2.3.情報資産の分類と管理方法 (2)⑦
電子メールによる情報資産の外部持ち出し	無断では持ち出し不可能となるシステム上の措置	2.6.技術的セキュリティ2.6.1.(15)
USBメモリで外部へ情報を持ち出す行為	教育情報セキュリティ管理者の許可が必要	2.5.人的セキュリティ2.5.1.(1)③
外部で情報処理作業を行う行為	教育情報セキュリティ管理者の許可が必要	2.5.人的セキュリティ2.5.1.(1)③
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場合には、必ず不正プログラム対策ソフトウェアによるチェックが必須	2.6.技術的セキュリティ2.6.1.(3)②
支給端末への外部からのソフトウェア取り込み	無許可でソフトウェアの導入禁止	2.6.技術的セキュリティ2.6.1.(18)
	外部からソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックが必須	2.6.技術的セキュリティ2.6.4.(3)②
約款による外部サービス（メール、ファイルストレージ、グループウェア）の利用	機微な校務情報（機密性２B以上）の扱い禁止	2.8.外部サービスの利用2.8.1.(1)
ソーシャルメディアサービスの利用	機密性２A以上の情報の発信禁止	2.8.外部サービスの利用2.8.3.②
学校のモバイル端末、情報資産等の持ち出し	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	2.5.人的セキュリティ2.5.1.(1)③

*7　ガイドライン 2.9. 評価・見直し 2.9.1

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

教育情報システムは、サーバやネットワーク、利用端末に対して個々にセキュリティ対策を講ずることで総合的に外部からの脅威の侵入を防御することが重要ですが、たとえば、

（ア）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。

（イ）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。

（ウ）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性のある行為です。以上のような、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 11 にまとめました。

図表 11　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

情報セキュリティレベル維持するために「してはいけない」行動		ガイドライン規定要約	ガイドラインの出所
業務以外の目的でのウェブ閲覧		禁止	2.5.人的セキュリティ2.5.1.(1)①
		禁止	2.6.技術的セキュリティ2.6.1.(21)
無許可での私物機器等の持ち込み		無許可で私物機器等を持ちこんでの業務利用禁止	2.5.人的セキュリティ2.5.1.(1)④、⑥
		無許可でのネットワーク接続禁止	2.6.技術的セキュリティ2.6.1.(20)
パソコンや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変更禁止	2.6.技術的セキュリティ2.6.4.(3)①
		パソコンやモバイル端末におけるセキュリティ設定変更の禁止	2.5.人的セキュリティ2.5.1.(1)⑥
		不正プログラム対策ソフトウェアによるフルチェックを定期的に実施	2.6.技術的セキュリティ2.6.4.(3)④
無許可での機器の改造及び増設・交換		禁止	2.6.技術的セキュリティ2.6.1.(19)
コンピュータウイルスへの感染が疑われる場合の状況の放置		LANケーブルの即時取り外し（パソコン端末等）	2.6.技術的セキュリティ2.6.4.(3)⑦
		直ちに利用を中止し、通信を行わない設定に変更（モバイル端末）	2.6.技術的セキュリティ2.6.4.(3)⑦
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	他者に知られないように管理	2.5.人的セキュリティ2.5.4
	教職員用パソコンに重要な情報が表示されたまま放置	離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等	2.5.人的セキュリティ2.5.1.(1)⑦
	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	引出しが開け放され、鍵も付けっぱなし	離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等	2.5.人的セキュリティ2.5.1.(1)⑦
	業務書類をゴミ箱にそのまま廃棄		
	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児童生徒への指導事項

児童生徒もパソコンやタブレットを利用して、情報システムにアクセスするため、教員からの指導を通して、情報セキュリティ対策の実施が求められます（図表 12 参照）。

図表 12　児童生徒への指導事項 [*8]

児童生徒への指導事項
①モバイル端末やＵＳＢメモリ等を、学校外に持ち出す場合は、担任の許可を得ること。
②学校では、承認されていない個人のパソコン、モバイル端末等を学校の情報システムに接続してはいけないこと。
③学校では、承認されていない個人のＵＳＢメモリ等をパソコン、モバイル端末等に接続してはいけないこと。
④モバイル端末等のソフトウェアに関するセキュリティ機能の設定を、許可なく変更してはならないこと。
⑤モバイル端末が動かない、勝手に操作されている、いつもと異なる画面が出るといった症状がでた場合、すぐに担任に報告すること。
⑥自分のＩＤは、他人に利用させてはいけないこと。 ※共用でＩＤを利用している場合は、共用ＩＤの利用者以外に利用させてはいけないこと。
⑦パスワードは他人に知られないようにすること。

（4） 外部サービスの利用 *9

学校教育分野では、タブレットを利用したドリルサービス等、外部サービスの利用が普及・浸透しつつあります。これらの外部サービスを利用する際に、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。図表 13 に外部サービスの利用のポイントを記します。

図表 13　外部サービス利用における情報セキュリティ確保のポイント

外部サービスの利用	情報セキュリティ確保のポイント	ガイドラインの出所
外部委託	（ア）情報システムの構築・運用・保守等を外部委託する際は、外部委託事業者からの情報漏えい等の事案を防止するために、情報セキュリティを確保できる外部委託事業者を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要あり。	2.8 外部サービスの利用 2.8.1. (1)(3)
	（イ）外部委託事業者に起因する情報漏えい等の事案を防ぐため、各地方公共団体が自ら実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要あり。	2.8 外部サービスの利用 2.8.1. (2)
約款による外部サービスの利用	（ア）フリーメール等の約款による外部サービスについては、機密性確保や情報の改ざん防止策等について約款上で規定されていない場合が多く、約款内容から充分な情報セキュリティ要件を確認できないことが多いため、約款による外部サービスを利用する範囲と条件を整備する必要あり。	2.8 外部サービスの利用 2.8.2.(1)(2)
	（イ）当該サービスの利用において、機微な校務系情報（機密性2B以上）が取扱われないようにする必要あり。	2.8 外部サービスの利用 2.8.2. (1)
ソーシャルメディアサービスの利用	（ア）住民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービスを利用することがあるが、なりすましやサービス停止のおそれがあるため、情報発信時の対策を講じる必要あり。	2.8 外部サービスの利用 2.8.3. ①
	（イ）機密性のある校務系情報や学習系情報（機密性2A以上）をソーシャルメディアサービスで発信することは禁止。	2.8 外部サービスの利用 2.8.3. ②

コラム 7

インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要があります。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、日本の法令では認められていない場合であっても、データセンターが設置されている国の法令により、海外の当局による情報の差し押さえや解析が行われる可能性があるため、個人情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要があることに留意ください。

*8　ガイドライン 2.5. 人的セキュリティ対策 2.5.1.(1)　　*9　ガイドライン 2.8. 外部サービスの利用

4.4　物理的対策

（1）　校務系サーバの教育委員会による一元管理 *10

学校内は、入室制限の徹底が困難な場合があり、学校設置サーバの盗難・損傷等による物理環境面からの情報資産の窃取・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等は教育委員会等のセンターサーバ又はセキュリティ要件を満たしたデータセンター等に集約した上で、教育委員会による一元的な管理を行う必要があります。また、地震・水害・火災等により重要な情報資産を滅失することも考えられるため、自然災害等に対する対策を講ずることが重要です。

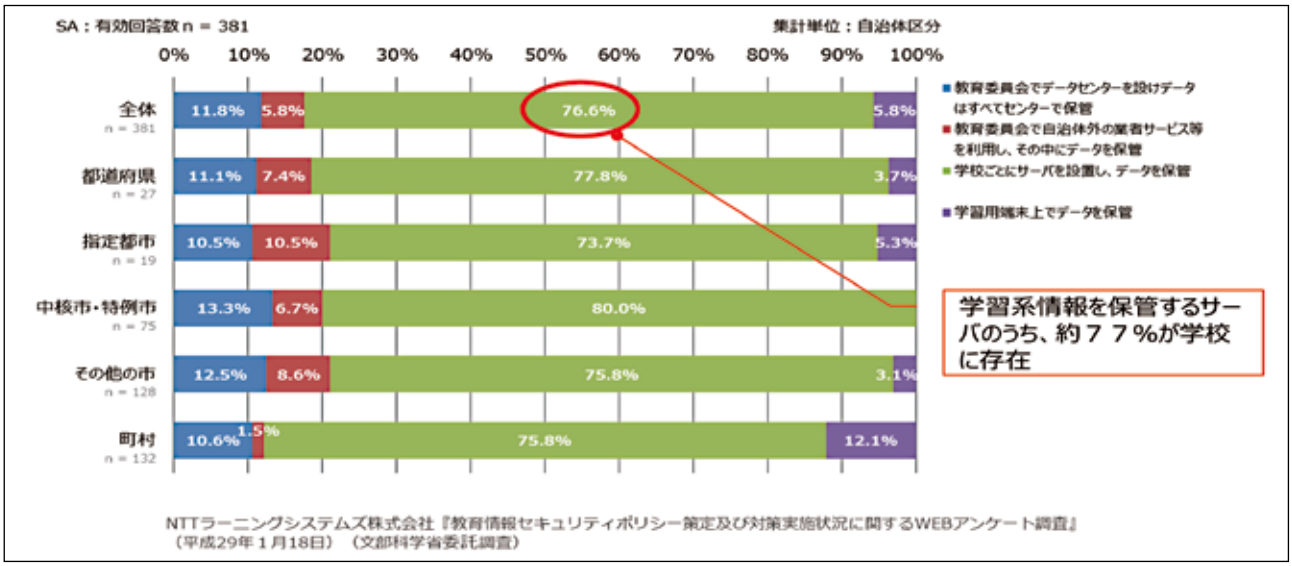
なお、学習系サーバについても教育委員会による一元管理が望まれる一方で、学校からデータセンター等のサーバ設置先までの通信回線が狭帯域であるなど通信インフラ上の課題がある場合や、学習系では大容量のデータを取り扱う場合があるなどネットワーク負荷の課題があるため、安定的な稼働を担保する前提で将来的に一元管理することとしています。

コラム 8

学習系情報を保管するサーバのうち約 77％が学校に存在しているという実態が調査結果から分かりました（図表 14 参照）。これは、動画･写真等の学習系情報はファイルサイズがとても大きく、学校のネットワーク事情（100Mbps 以上のインターネット接続をしている学校の割合は 38.4%）を踏まえ安定的な運用を図る観点から、サーバを学校に設置することを選択している地方公共団体が多いためです。

なお、サーバを学校に設置する場合は、サーバラックに固定したうえで施錠管理を実施し、不特定多数の者が出入りできない場所に設置する必要があります（図表 15 参照）。

図表 14　学習系情報のデータ保管形態



NTTラーニングシステムズ株式会社『教育情報セキュリティポリシー策定及び対策実施状況に関するWEBアンケート調査』（平成29年１月18日）（文部科学省委託調査）

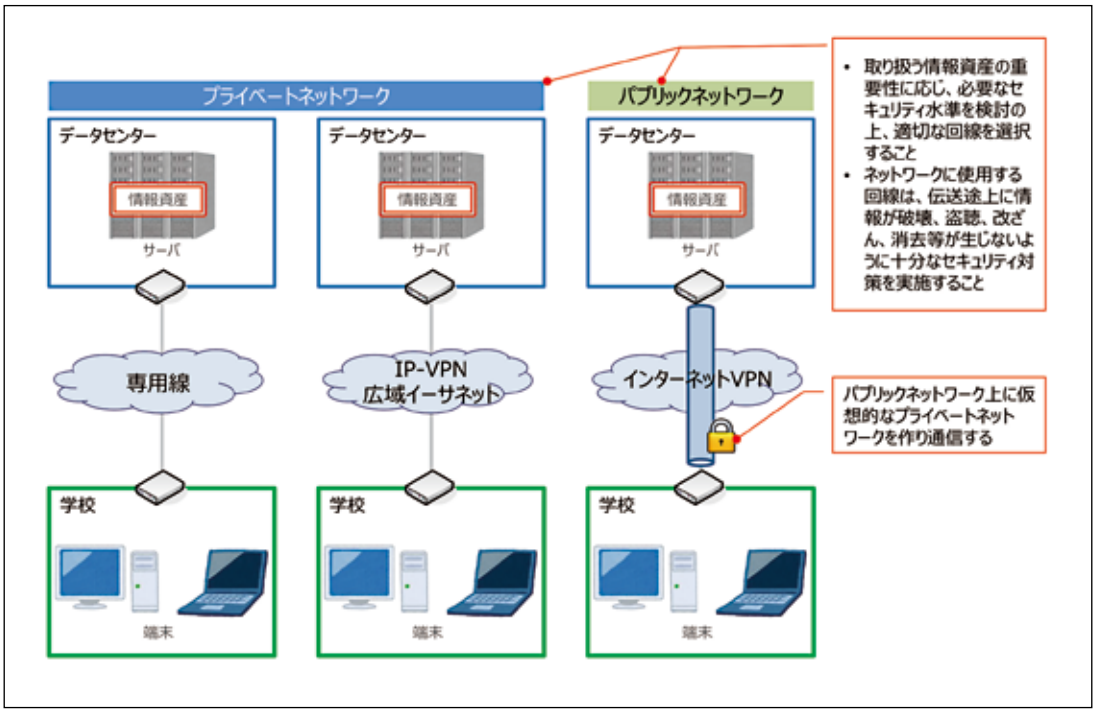
図表 15　学校内でサーバを設置する場合の設置事例

*10　ガイドライン 2.4 物理的セキュリティ 2.4.2

（2） 通信回線及び通信回線装置の管理 *11

データセンターと学校間の通信回線として利用する回線は、当該システムで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ものを選択することが必要です（図表 16 参照）。

図表 16　通信回線のセキュリティの考え方



コラム 9

適切なセキュリティ機能を備えた回線を選択する際の考え方として、IP-VPN では利用するネットワーク自体が通信事業者のプライベートネットワークであるため、通信データを暗号化しなくても安全性や信頼性を確保することができます。一方で、インターネット VPN ではインターネット上に仮想的なプライベートネットワークを作り、通信データを暗号化した上で通信します。インターネットを経由した通信では、通信データの盗聴や改ざんなどによるセキュリティ上のリスクを伴うために通信データを暗号化する技術を利用しますが、重要な情報資産がインターネットを物理的に通過するということも忘れてはいけません。

*11　ガイドライン 2.4 物理的セキュリティ 2.4.3

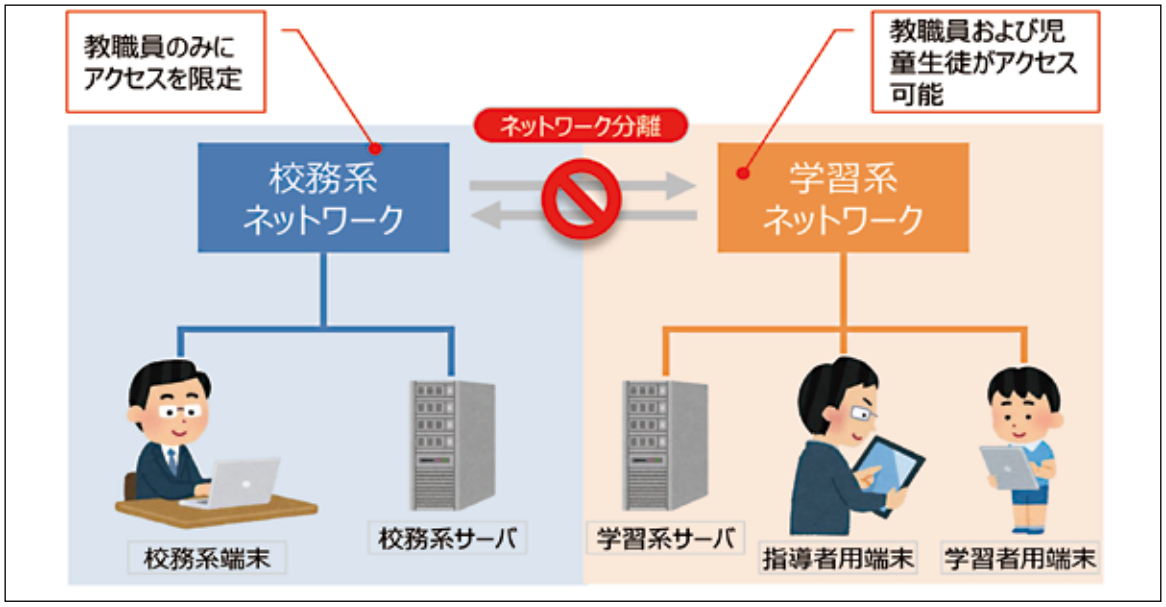
4.5　技術的対策

（1）　児童生徒が機微な校務系情報にアクセスするリスクへの対応

①学習系システムから校務系システムへのアクセスの防止 *12

児童生徒による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、教職員および児童生徒が利用する学習系システムから、教職員のみが利用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で論理的又は物理的な分離を徹底することが必要です（図表 17 参照）。

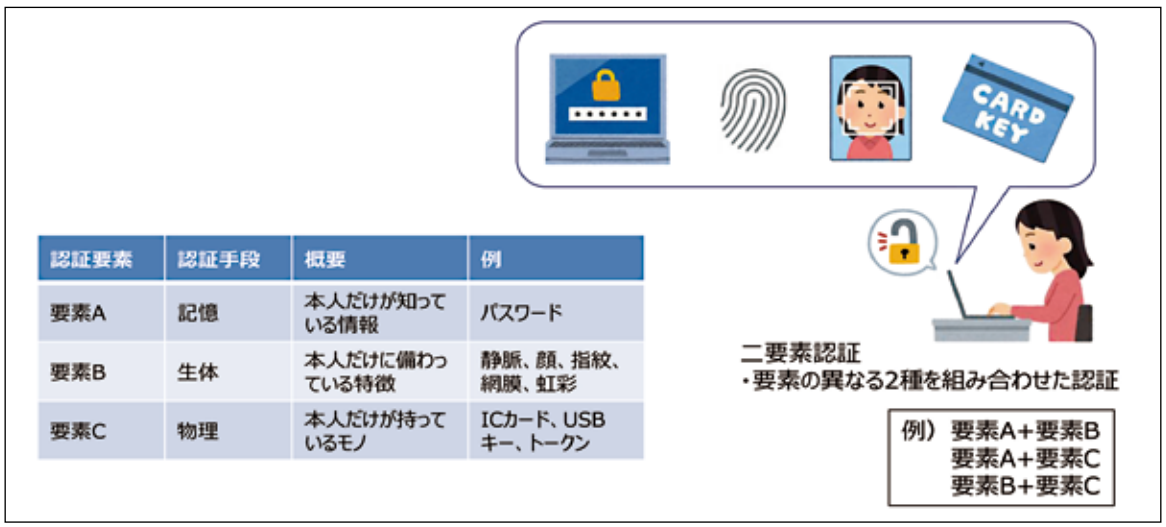
図表 17　学習系システムと校務系システムの通信経路の分離



②教職員の個人認証強化

教職員は機微な校務系情報を日常的に扱いますが、職員室に児童生徒が出入りできる状況等を踏まえると、これらの情報への不正アクセスを防止することが重要になります。そのため、機微な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を推奨事項*13としています。個人認証の方式としては、記憶に頼る ID/ パスワードの利用が一般的ですが、万が一 ID/ パスワードが流出した場合には外部からの遠隔操作等の危険性があります。そのため、ID/ パスワードに加えて生体認証や物理認証を併用する「二要素認証」を用いることで、個人認証を強化することも推奨されます（図表 18 参照）。

図表 18　教職員の個人認証強化の考え方



認証要素	認証手段	概要	例
要素A	記憶	本人だけが知っている情報	パスワード
要素B	生体	本人だけに備わっている特徴	静脈、顔、指紋、網膜、虹彩
要素C	物理	本人だけが持っているモノ	ICカード、USBキー、トークン

*12　ガイドライン 2.6 技術的セキュリティ 2.6.1(11)

*13　各地方公共団体において、その事項の必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項については、「推奨事項」として示しています。

コラム 10

「二要素認証」とよく似た言葉で、「二段階認証」というものがあります。この２つの言葉がたびたび同義語として扱われることが見受けられますが、意味には微妙な違いがあります。

二要素認証とは、認証の三要素で説明した３つの要素のうち、２つ以上を組み合わせて認証する仕組みです。一方で、二段階認証とは、認証を２回に分けてセキュリティを強化する仕組みです。例えば、暗証番号の入力による認証後に、生年月日を入力し認証するのは二段階認証となります。暗証番号と生年月日はどちらも「本人だけが知っている情報」ですので、二要素認証にはなりません。

このように二要素認証と二段階認証は意味合いが異なりますが、単一の認証よりもセキュリティを強化している点では共通しています。一方で、昨今のソーシャルメディアの普及等により生年月日等の情報を公開していると「本人だけが知っている情報」ではなくなるため注意が必要です。

③学習系システムへの機微情報保管の禁止

出欠情報や健康情報等の機微情報の一部が学習系システムに保管され、情報システムの設定不備等により児童生徒がアクセスできる状態になっている場合があります。このような場合、児童生徒がいたずら等により、学校の情報資産を窃取・改ざんする可能性があるため、学習系システムへの機微情報の保管については原則禁止とし、児童生徒による機微情報へのアクセスを防止する必要があります。

コラム 11

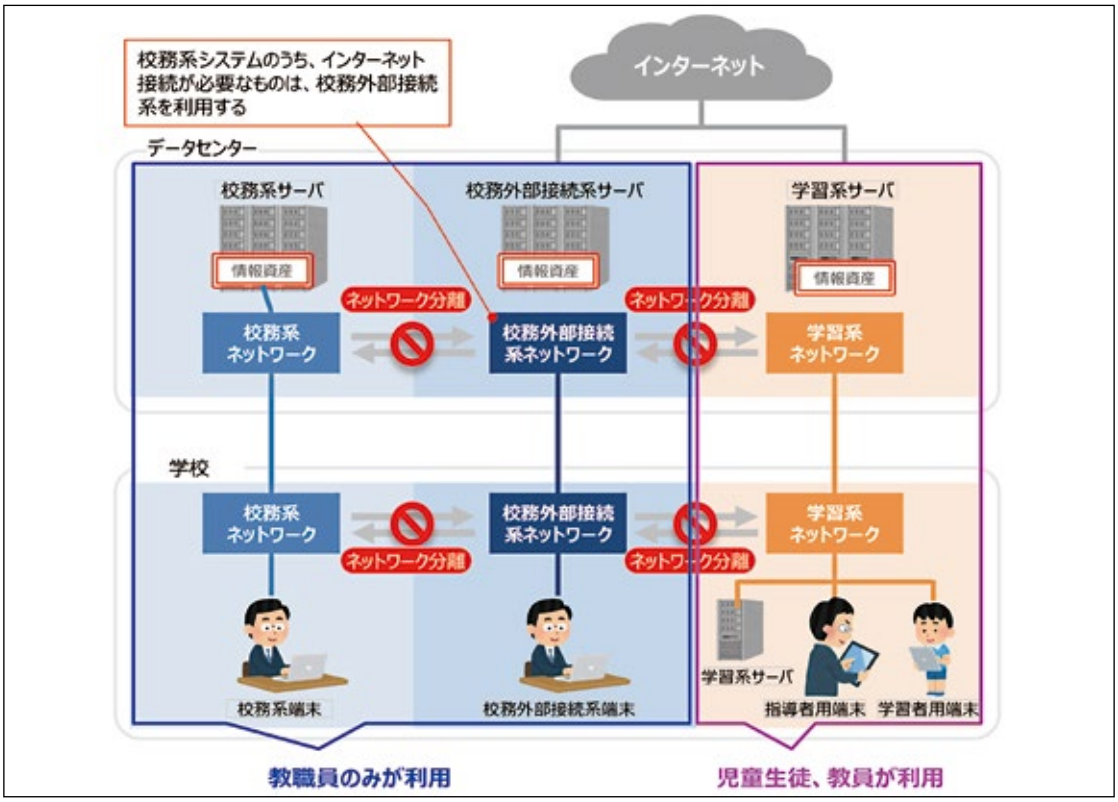
現在普及しているサービスの中には、教室において児童生徒の出欠や所見等の機微情報をタブレット端末で入力している場合がありますが、これらの情報を、学習系システムを使って入力を補完しているなど、学習系システムに機敏情報を保管しないことを徹底することは難しい場合があります。学習系システムには機微情報を保管しないことが望ましいのですが、機微情報を保管する場合には当該情報を暗号化し、情報漏えい後の対策を講ずることが重要になります。

（２） インターネット利用におけるセキュリティリスクへの対応

①校務系システムのインターネットリスクからの分離

校務系システムおよび学習系システムの分離[*14]を徹底した上で、さらに校務系システムにおいては、標的型攻撃やランサムウェア等のインターネットから侵入する脅威への対策として、機微な校務系情報を扱う校務系システムと、ウェブ閲覧やインターネットメールなどインターネット接続を前提とする校務外部接続系システムとを分けて管理する必要があります。そのため、両システム間の通信経路の論理的又は物理的な分離の徹底が必要です（図表 19 参照）。

図表 19　セキュリティレベルの異なるシステム間の論理的分離の例



*14　ガイドライン 2.6 技術的セキュリティ 2.6.1（11）

コラム 12

校務外部接続系システムでは保護者メールのような機微な校務系情報（重要性分類Ⅱに相当）を扱い、学習系システムでは学習系情報（重要性分類Ⅲ）を扱います。両システムともにインターネット接続を前提としますが、重要性の異なる情報資産を扱う点と利用者が異なることから、システム間の分離が必要になります（図表６参照）。

【事例】 教職員の利便性を考慮したセキュリティ対策事例 ～福島市教育委員会～

校務処理用とインターネット接続用のデスクトップを分け、児童生徒の情報等をインターネットのセキュリティリスクから分離。複数のセキュリティ対策を組み合わせた多層防御で、外部からの攻撃に対処。

【導入に至った経緯】

福島市の公立学校では、公的費用によるパソコン端末整備が十分でなかったことに加え、多様化する教育課題への対応や保護者・外部機関への対応が増加し、教員が児童生徒ひとりひとりに掛けられる時間が少ないことが課題となっていました。

そこで、教職員の校務負荷を軽減し、教員が児童生徒と向き合う時間を確保できる教育現場の実現とセキュリティ対策を目的として、情報の紛失・漏えいや外部からの不正アクセスなどのリスクを解消できる仮想デスクトップを導入することにしました（図表 20 参照）。また、システム面の整備だけでなく、学校現場に即したセキュリティポリシーを新たに策定することで、統一的な情報セキュリティを維持管理するための組織体制を確立し、情報資産を重要度に応じて分類したうえで適切なセキュリティ対策を実施しました。

【検討事項】

- 個人情報の漏えい事故を０にするため、セキュリティ性が担保された端末システム整備の必要性
- 児童生徒の個人情報データが含まれる校務処理用のネットワークと、インターネット接続用のネットワークの切り離し
- 外部記憶装置（USB メモリ等）の利用制限
- 新規セキュリティポリシーの策定

【導入システム概要】

新たに導入したシステムでは、以下を組み合わせた多層防御の仕組みによってセキュリティを強化しています。

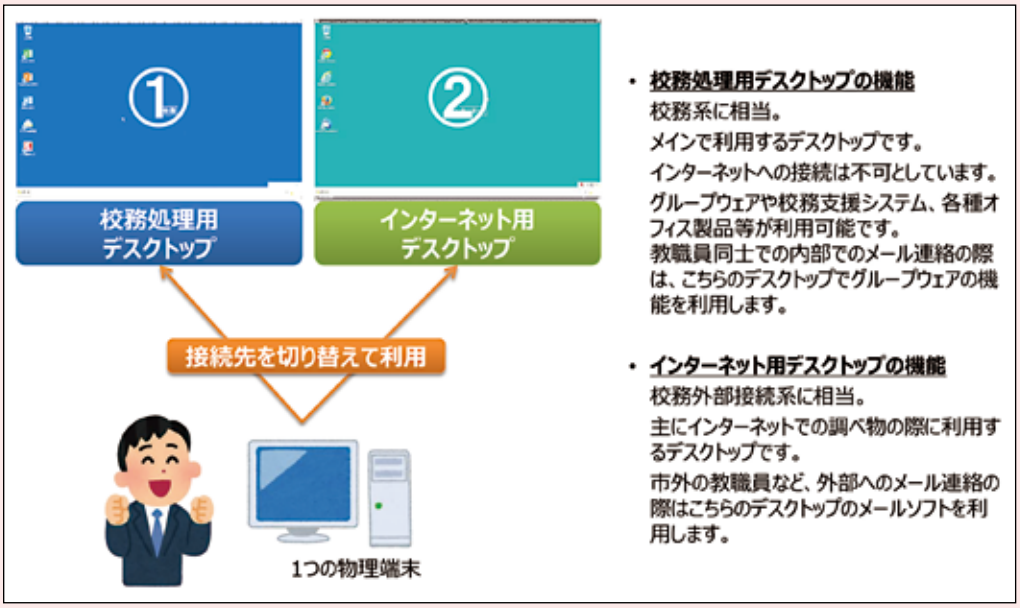
- 校務処理用とインターネット接続用のデスクトップを分離
- 外部からの不正アクセスを、ファイアウォールで遮断
- 標的型攻撃には、メール添付データのウイルスチェックを実施するとともに、出口対策として Web フィルタリングで悪性 Web サイトへの通信を検知して遮断
- 個々の仮想デスクトップ上でもウイルス対策ソフトでウイルスの侵入・実行・コピーを防ぐ

さらに、教職員の利便性にも考慮したセキュリティポリシーをシステムで実現しています。

- データの機密性を守りつつ市内他校の教職員とデータ共有を可能にするため、全教職員が利用可能でアクセス権が管理された全校共有 / 各学校用 / 個人用のファイルサーバを用意
- 行事写真などの外部メディアデータを安全に利用するため、一般教職員にはデータ読み込みは許可するが、校長・教頭の許可なしでは外部メディアにデータを書き込みできない仕組みを構築
- インターネットから教材等のデータを安全にダウンロードして利用するため、インターネット接続用と校務処理用のデスクトップでデータの受け渡しが可能な専用領域を用意し、校務処理用デスクトップからは読み込みのみを許可することで、インターネットを経由した情報流出を防止

また、1 週間分のユーザーデータのバックアップを作成しており、利用者が誤操作でデータを消去した場合などに、利用者自身の操作で特定の時点のデータに復旧・アクセスすることを可能にしています。

図表 20　福島市教育委員会におけるネットワーク分離イメージ

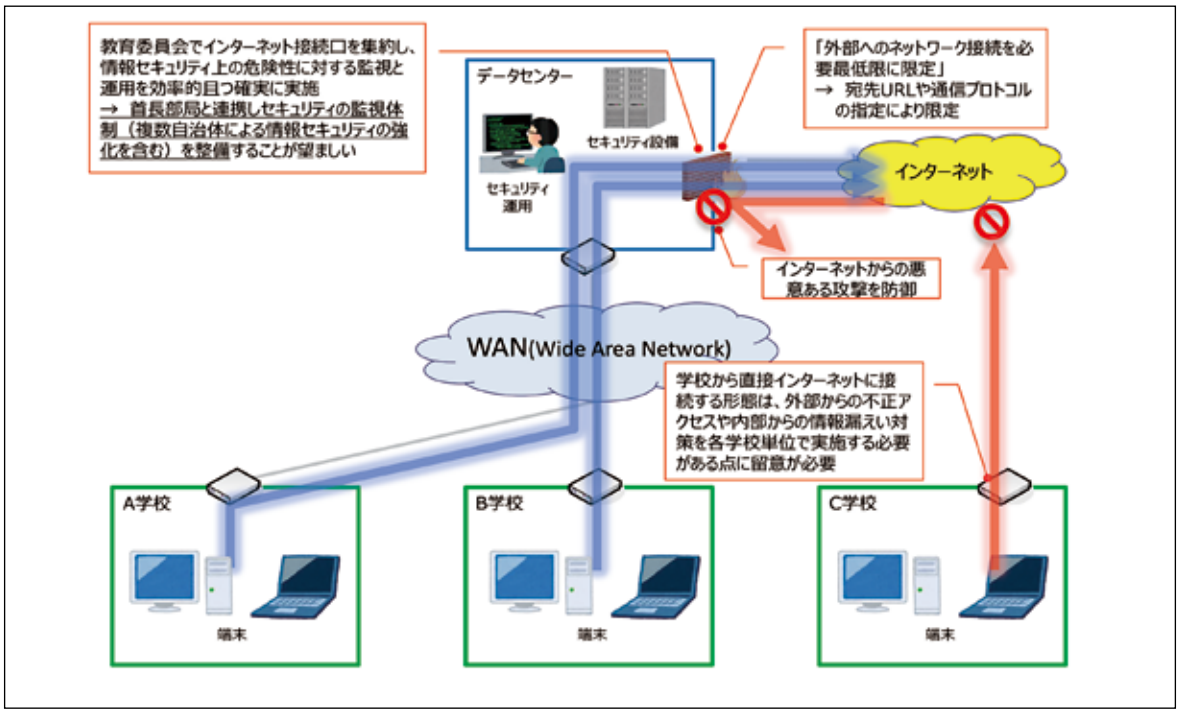


②学校のインターネット接続環境のセンター集約によるセキュリティ対策強化

外部のネットワークへの不必要な接続は、情報セキュリティ上の危険性が高まることから、その接続は必要最低限のものに限定する必要があります。とりわけ、学校から直接インターネットに接続する形態は、外部からの不正アクセスや内部からの情報漏えい対策を学校単位で実施する必要があり、セキュリティ機器の整備や運用体制の構築など、各学校において必要となるセキュリティレベルを確保することが困難となります。

そのため、情報セキュリティ上の危険性に対する監視と運用を効率的かつ確実に実施するためにも、教育委員会でインターネット接続口を集約することで、機器・運用の共同利用によるコスト低減（割り勘効果への期待）や、情報セキュリティ専門人材による情報セキュリティ事故の早期発見と対処といったセキュリティレベルの確保・向上を図る必要があります（図表 21 参照）。

図表 21　インターネット接続口の一元集約管理の考え方



③校務外部接続系サーバ及び学習系サーバ（機微な個人情報を保管する場合に限る）の暗号化の実施

機微な校務系情報はインターネットのセキュリティリスクから分離する必要がありますが、これらのうち、保護者メール等の情報はインターネット接続を前提とするシステム上に保管される場合があります。また、学習系サーバに健康情報や学習所見等の情報資産がやむなく一時的に保管される場合もインターネット接続を前提とするシステム上に保管されます。このような場合は、機微情報として保管するファイルを暗号化するなど、ファイルが流出しても関係者以外が情報を閲覧することができないようにする対策が必要になります。[*15]

なお、校務系システムについては、インターネットのセキュリティリスクから分離できていることを前提に、当該システムでのファイル暗号化までは求めていません。また、学習系情報など重要性分類Ⅲの情報についてもファイル暗号化することまでは求めていません。

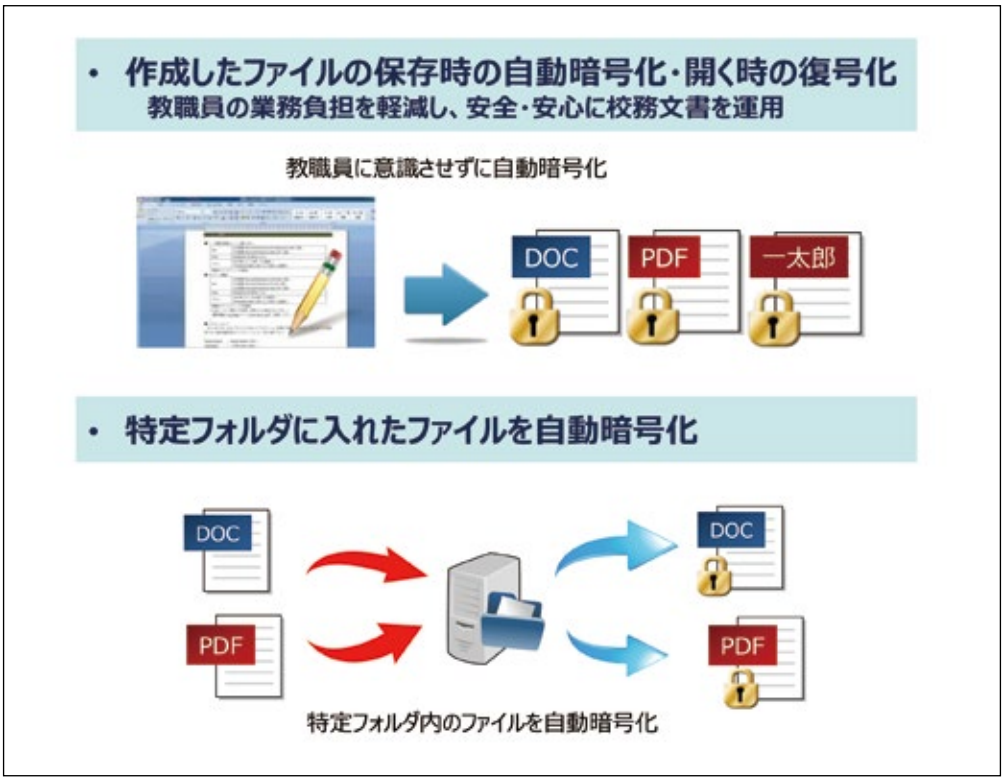
コラム 13

ファイル暗号化等による安全管理措置を講ずる際は、教職員の業務負担軽減等に考慮して、教職員が意識せずに作成したファイルが自動的に暗号化されるような対策を採ることも選択肢の一つとして考えらます（図表 22 参照）。これは、運用ルールのみでファイルの暗号化を徹底することは困難（手間が増えるからやらない、うっかり暗号化するのを忘れてしまった等）になることが考えられるため、システムによる制御をかけることで、業務負担軽減の側面だけでなく、ファイル暗号化を徹底する際にも有効になります。

なお、ファイルの暗号化さえ行えば、インターネット接続を前提とするシステム上に機微情報を保管しても良いという考え方ではありません。取り扱う情報資産をしっかりと分類した上で、適切なセキュリティレベルのシステムに正しく保管することが重要です。

*15　ガイドライン 2.6 技術的セキュリティ 2.6.1（1）

図表 22　ファイル自動暗号化の例



（3）　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機微情報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、教職員の校務用端末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。これは、インターネットに接続していない校務系システムにおいては、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。

コラム 14

成績処理等を自宅で行うことを目的として、教員が、電磁的記録媒体等を介して個人情報を自宅に持ち帰る場合があります。一方で、個人情報が記載された電子データを紛失することにより懲戒処分等を受けた教員は平成 27 年度で 62 名（文部科学省「平成 27 年度公立学校教職員の人事行政状況調査」）も存在することを踏まえ、教員が個人情報を外部に持ち出す際の安全管理措置の徹底が必要です。

②電磁的記録媒体の暗号化の徹底 *16

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 23 参照）。

図表 23　電磁的記録媒体の暗号化

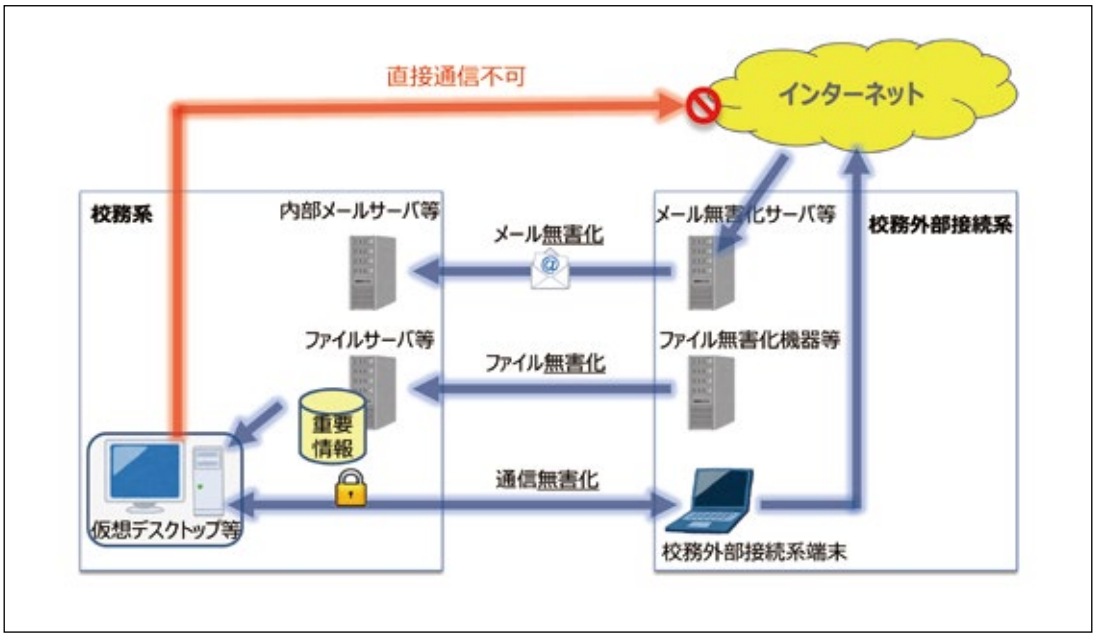
（4）　その他関連して必要になる対応

①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の実施 *17

校務系・校務外部接続系・学習系システムの分離徹底後、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場合には、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。なお、校務外部接続系システムと学習系システム間の通信については特段規定していません。

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、現状ではすべ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 24 参照）。

図表 24　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



*16　ガイドライン 2.4 物理的セキュリティ 2.4.4 ⑤　*17　ガイドライン 2.6 技術的セキュリティ 2.6.1（11）

②専用端末の考え方

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校務外部接続系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う点に留意が必要です。

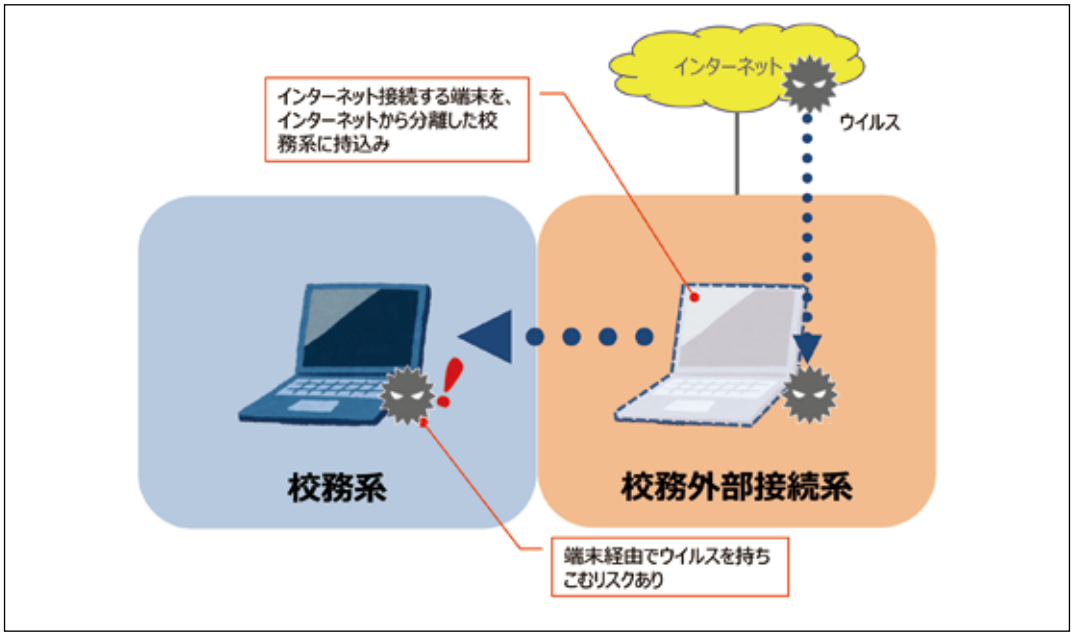
なお、上記の考え方に従った場合、校務用端末については、以下のいずれかの対応が必要となりますが、各地方公共団体においては、学校現場における校務事務の実態と対策に係る費用等を勘案したうえで、対応策について判断する必要があります（図表 25 参照）。

（ア）「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。

（イ）「校務系システム」と「校務外部接続系システム」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。

（ウ）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 25　専用端末の考え方



（5）　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（校務外部接続系情報を含む）は、6 か月以上の保管が望ましいです（図表 26 参照）。

図表 26　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。

コラム 15

ログの保存期間を考慮する時、どれくらいの期間保存するべきかという問題に関して、一律に解が定められるものではありません。ガイドラインにおいては、校務系情報（校務外部接続系情報を含む）のログについては、6 か月以上の保管が望ましいとしていますが、「どのような目的でログを取得するのか」、「取得対象とすべきログは何か」、「取得期間をどれほどにするのか」等、地方公共団体において取得目的や優先順位をつけながら適切に判断する必要があります。一般的に、ログの保存期間はリスクとコストのバランスによって決定し（図表 27 参照）、実際のログの中身や監視の詳細は、組織内部の者に見せないことが多いようです。

図表 27　ログ保存期間の考え方

項目	考慮点	備考
セキュリティリスクの観点	ログの監視やインシデント発生時の調査の観点で、保存期間に対する要請がないか？	１年前のセキュリティ事案までは、追えるようにしたい、など。
コストの観点	大量のログを「安全に」保存するためのコスト負担にどこまで耐えられるのか？	セキュリティ事案が何もなければ、ほとんどのログは一度も検証されることなく、捨てられることとなる。

②情報システムの監視 *18

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動状況を常時監視することが必要です。ガイドラインでは、格納する情報資産の重要性に応じ、校務系システムは常時監視を必須とし、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。

コラム 16

ガイドラインの「2.7.1 情報システムの監視」では、主に外部攻撃や内部漏えいなどのセキュリティ事件や事故に対する監視を対象としていますが、教育情報システムが安定的に稼働するために、通常はシステムに対する監視も併せて行われます。（図表28参照）。

図表 28　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。	通常の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 *19

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、校務系サーバ及び校務外部接続系サーバの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予想されるため、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する必要があります。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の消失を防ぐために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、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。

*18　ガイドライン 2.7 運用 2.7.1　　*19　ガイドライン 2.6 技術的セキュリティ 2.6.1（2）

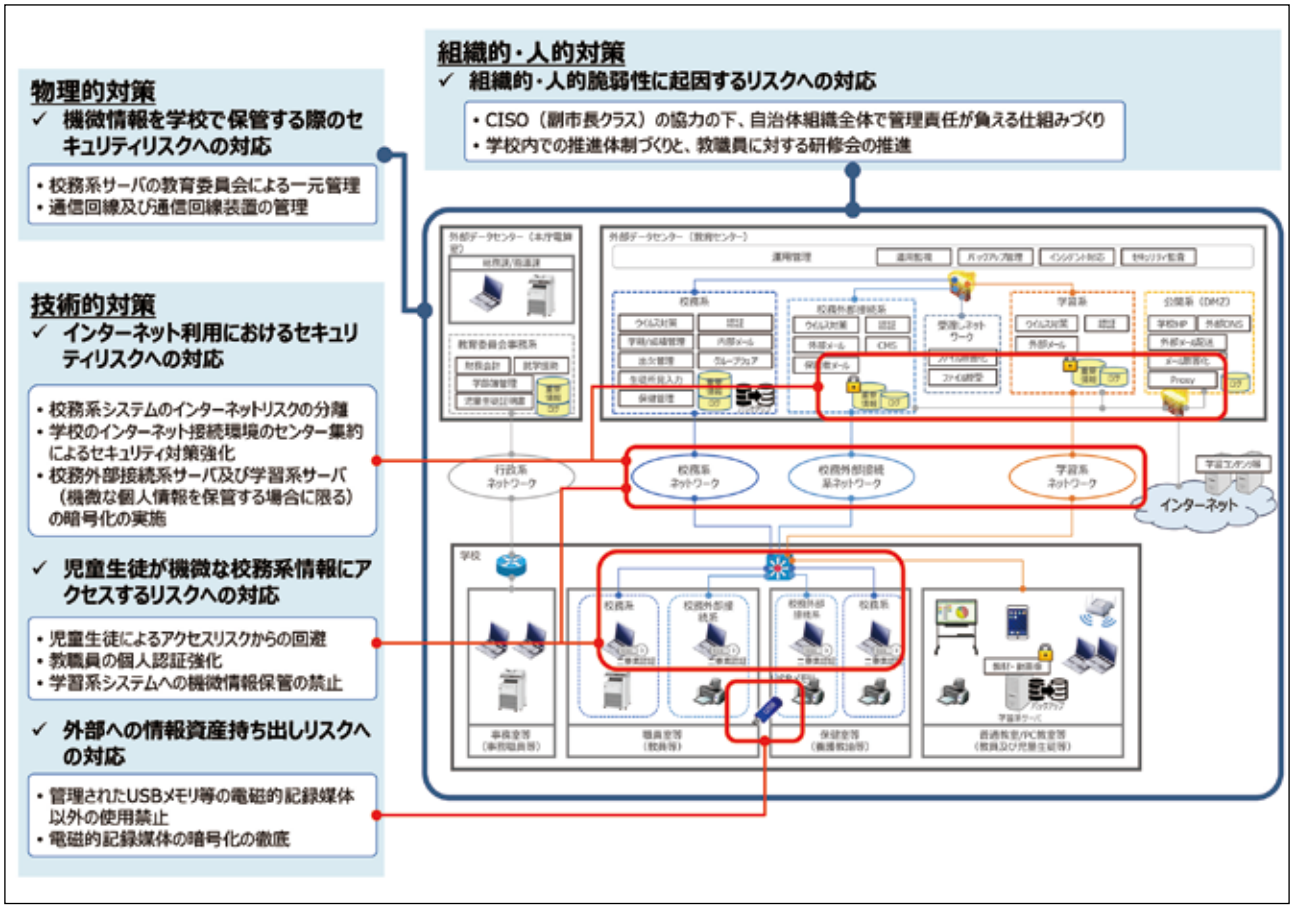
第5章 ◉ おわりに

本ガイドラインでは、情報資産の重要性に応じてセキュリティ対策を講じ、重要性の異なる情報資産は、同一システムでは扱わず、機微な校務系情報と学習系情報はシステム分離を基本としています。一方で今後は、校務系システムと学習系システムの連携により、学校が保有する情報を学習指導や生徒指導等の質の向上、学級・学校運営の改善に活用することなどが期待されています。

このため、校務系システムと学習系システムのセキュアな連携のあり方及びインターネットを介したASPサービスの利用における留意点については、文部科学省において、平成29～31年度で実施予定の「次世代学校支援モデル構築事業」において実証し、ガイドラインに反映していく予定です。

【参考】

図表29　主な教育情報セキュリティ対策（概要）



【用語集】

用語	解説
コンピュータウイルス（ウイルス）	パソコン等コンピュータ端末に被害をもたらす不正プログラムの一種でプログラムファイルからプログラムファイルへと感染するものを指す。
新たな自治体情報セキュリティ対策の抜本的強化に向けた対策	日本年金機構における個人情報流出事案を受けて、平成27年に総務省において、地方自治体の情報セキュリティに係る抜本的な対策として打ち出した三層からなる対策。
標的型攻撃	明確な意思と目的を持った人間（攻撃者）が特定の組織に対して特定の目的（情報の窃取や削除）のために行うサイバー攻撃の一種。知り合いを装って電子メールを送付し、添付ファイルを開かせることでウイルス感染させる「標的型メール攻撃」が代表的なもの。
機微情報	慎重に扱われるべき情報のこと。 定義として、OECDの個人情報保護ガイドラインでは、広く、『(情報漏えいによって)社会的差別を受けうる情報』と規定される
CISO	Chief Information Security Officerの略で、組織の情報セキュリティを統括する最高責任者
CSIRT	Computer Security Incident Response Teamの略で、情報セキュリテ事故が発生した際に、内容把握・分析し、被害拡大防止、復旧、再発防止等を担う体制のこと。
パブリックネットワーク	不特定多数の利用者と共有するネットワーク。公衆網とも呼ぶ。
プライベートネットワーク	組織内などの限られた利用者のみと通信を行うネットワーク。閉域網とも呼ぶ。
IP-VPN	地理的に離れた構内ネットワーク(LAN)同士を接続して一体的に運用するVPN(Virtual Private Network：仮想専用ネットワーク)の方式の一つで、通信事業者の運用するIP(Internet Protocol)ベースの閉域ネットワークを経由して拠点間を接続するもの。
インターネットVPN	インターネット上に暗号化された専用の通信経路を形成し、仮想的な組織内ネットワークを構築すること。
ランサムウェア	攻撃者が端末自体をロックしたり、端末内に保存しているデータを暗号化する等して使用不能にし、端末やデータの回復のために身代金を要求する悪意のあるソフトウェアのこと。
WAN	Wide Area Networkの略で、LANと比較して広い範囲（拠点を越えて自治体全域、場合によっては県内外、国際の範囲）におよぶネットワークのこと。
仮想化技術	物理的な構成にとらわれずに、論理的に統合・分割できる技術のこと。代表的な仮想化技術としてサーバ仮想化があるが、これは1台の物理的なサーバの中に、複数台の仮想的なサーバを動作させる技術となる。なお、サーバ仮想化以外の仮想化技術としては、デスクトップ仮想化・ストレージ仮想化・ネットワーク仮想化など様々な種類がある。
マルウェア	malicious software（悪意のあるソフトウェア）の略で、コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を及ぼす不正な動作を起こすソフトウェアの総称。
フィッシング	ユーザーからIDやパスワードなどの個人情報を盗み取る犯罪。一斉送信されたメールを使って、あらかじめ用意した本物そっくりの偽サイトへ誘導する。
IDS	Intrusion Detection Systemの略で、Intrusion（＝侵入）をDetection（＝検知、検出）するシステムとして、侵入検知システムと呼ばれる。
Ping	IPネットワーク上で通信状況を確認するために、目的のPCやサーバーから返事が返ってくる時間などを測定するプログラム。

「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　平成 29 年 11 月
◇発　行　文部科学省
◇制　作　エヌ・ティ・ティラーニングシステムズ株式会社
◇協　力　ネットワンシステムズ株式会社　市場開発部　エキスパート　林山　耕寿
◇監　修　東京都豊島区　区民部　税務課長　高橋　邦夫
　　千葉県柏市教育委員会　教育専門アドバイザー　西田　光昭