第２章　教育情報化システム構築・運用に必要な情報セキュリティ知識

情報セキュリティ、どこが危ない？

◉2.1　学校における情報セキュリティとは

2.1.1　学校における情報セキュリティの範囲と特性

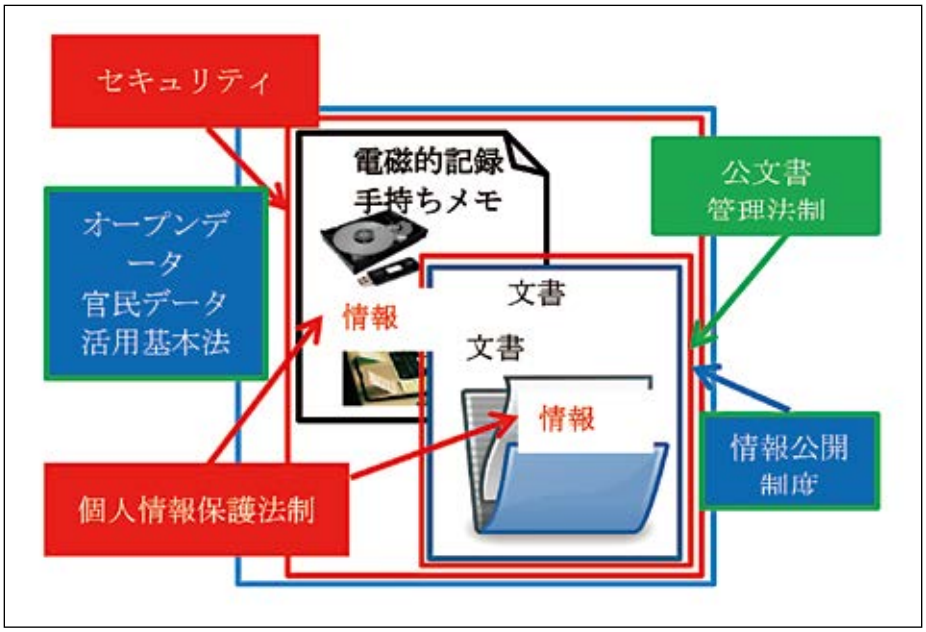
教育委員会や学校などの公的機関においては、さまざまな法制により情報の適正な管理が求められています。公文書管理法においては、地方公共団体は保有する公文書の適正な管理に関して必要な施策を制定・実施するよう努めなければならないとされており、ほとんどの地方公共団体においては、文書管理規則・規程や公文書管理条例等を定めています。また、地方公共団体が管理する文書は情報公開請求の際には原則的に公開すべきもの、という側面もあります。

さらに、地方公共団体ごとに定められている個人情報保護条例では、教育委員会は実施機関と位置づけられ、文書、電磁的な記録、手持ちメモ等に含まれる個人情報の管理、利用に当たって個人情報の保護を図るため必要な措置を講じる義務が課されています。学校における情報セキュリティは下図のとおり、文書管理規則で規定される文書、サーバやＵＳＢメモリーといった電磁的な記録、付箋紙やメモなどに書き込まれた情報などを網羅的に対象としています。

教育委員会や学校が管理する情報は、公文書管理や個人情報保護の法制により適正な管理が求められているため、情報内容により、後述する「機密性」「完全性」「可用性」を維持しなければなりません。公開してはならない情報については、その情報へのアクセスを認められた人だけがアクセスできる状態を確保する「機密性」が重視され、公開しなければならない情報については情報へのアクセスを認められた人が必要時に中断することなく、情報にアクセスできる状態を確保する「可用性」の側面が重視されます。たとえば、児童生徒名簿などの個人情報を格納した記録メディアやノートＰＣの紛失・盗難は「機密性」が損なわれるものであるのに対し、マルウェアの侵入によってファイルが読めなくなってしまった等は「可用性」が損なわれるもので、いずれも情報セキュリティ事故と言うことができます。

公的な機関では、間違い・ミスを「あってはならないもの」と考える傾向があり、情報セキュリティ事故についても具体的な被害が覚知されるまで発生を認識できず、被害が拡大することがあります。「情報セキュリティ事故、またはそのおそれが発生した段階」を想定した備えをすることが重要です。

図表 2-1　情報セキュリティの範囲



情報セキュリティ大学院大学　湯淺教授作成資料

2.1.2　学校における情報セキュリティ事故の状況

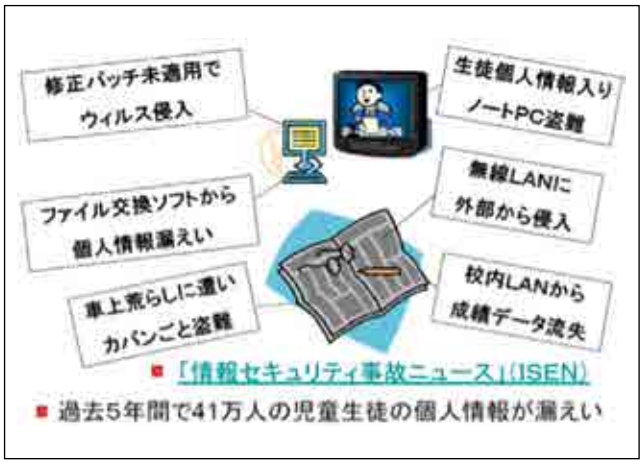
■情報化社会と情報セキュリティ

現実社会において、暴力行為や泥棒といった多様な犯罪があるのと同じように、情報通信技術（ＩＣＴ）が発達した社会にも、情報の盗難やコンピュータシステムの破壊といった犯罪があります。また、いわゆるサーバ空間の中だけではなく、火事や地震、雷といった災害から機器や情報を守ることも、大切な情報セキュリティ対策です。これらの情報セキュリティ対策は、インターネットなど情報通信技術への社会の依存度が高まるにしたがって、ますます重要になってきています。

■学校における情報セキュリティ事故

我が国では学校において、毎年さまざまな情報セキュリティ事故が発生しています。（図表 2-1）（図表 2-2）

図表 2-2　情報セキュリティ事故の例



資料出所：岡山県総合教育センター

図表 2-3　事故発生件数・個人情報漏えい人数

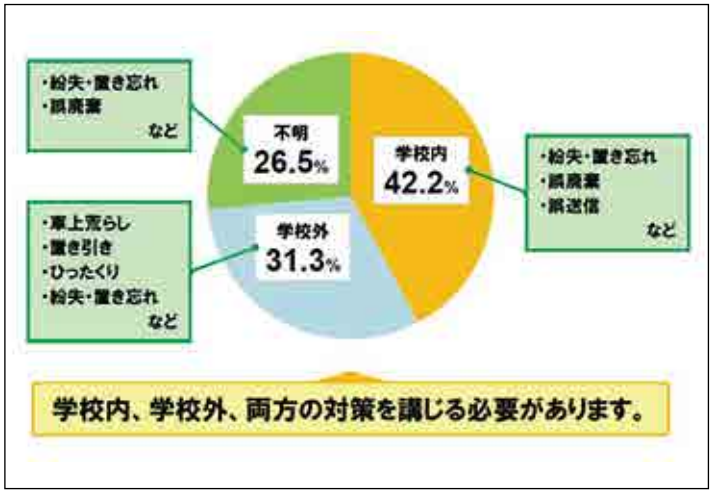
資料出所：ＩＳＥＮ「平成 27 年度学校・教育機関における個人情報漏えい事故の発生状況調査報告書第 2 版」

学校における情報セキュリティの実態等を調査している非営利団体教育ネットワーク情報セキュリティ推進委員会（略称ＩＳＥＮ）によれば、平成 27 年度は全国で 166 件の個人情報漏えい事故が発生しており、のべ 340,701 人の個人情報が漏えいしています。

これらの個人情報漏えい事故の発生場所の比率をみると、「学校内」が最も多く 42.2%、次いで「学校外」が 31.3%、「不明」が 26.5%となっています。（図表 2-4）

それぞれの発生場所での主な原因は、学校内が「紛失・置き忘れ」、「誤廃棄」、「誤送信」など、学校外が「車上荒らし」、「置き引き」、「ひったくり」、「紛失・置き忘れ」など、不明が「紛失・置き忘れ」、「誤廃棄」などとなっており、学校内・学校外の両方での対策を講じる必要があると言えます。

図表 2-4　発生場所別情報セキュリティ事故発生比率



資料出所：ＩＳＥＮ「平成 27 年度学校・教育機関における個人情報漏えい事故の発生状況調査報告書第 2 版」

また、個人情報漏えいを発生経路別にみると、平成 27 年度では学校や教育委員会が管理する「サーバ」からの漏えい（図表 2-5）が最も多く、これは、正規のアクセス権を持たない第三者の不正アクセスにより、有線・無線問わずネットワークを経由するなどして情報システムに侵入、個人情報を盗み出す（盗み見する）ものです。

図表 2-5　漏えい経路・媒体別情報セキュリティ事故発生比率

資料出所：ＩＳＥＮ「平成 27 年度学校・教育機関における個人情報漏えい事故の発生状況調査報告書第 2 版」

■佐賀県の実例

本事案では無職少年が他人の実在するユーザ ID とパスワードを利用して、学校ネットワークにアクセスし侵入。さらに侵入されたネットワーク内から別の重要情報が窃取され、被害の範囲が拡大し、14,355 名の個人情報が窃取されました。

佐賀県学校教育ネットワークセキュリティ対策検討委員会（佐賀県教育委員会が設置した有識者などからなる第三者委員会。以下「検討委員会」）がまとめた提言書によれば、本事案の主な経緯は以下のとおりです。

時　期	経　　緯
平成 27 年 3 月頃	ある高校においてフィッシング画面を工作した学習用 PC で教師から管理者用の ID とパスワードを取得
平成 27 年 4 月頃～	無職少年が不正アクセスを開始したと考えられる
平成 27 年 6 月 14 日	高校で校内 LAN（校務用サーバ）へアクセスできなくなる事象が発生 （無職少年が不正取得し保存した 6 月 14 日付フォルダの中に、校務用サーバより取得したデータが蔵置。なお 6 月 15 日以降の校務用サーバのデータは蔵置されていない。） 上記事案を受け、全校の管理者パスワードの変更とネットワーク設定変更を実施（一部の管理パスワードを変更せず）
平成 27 年 9 月 17 日	高校のヘルプデスク現地員から、管理者の ID とパスワードを入手するため、学習用 PC にフィッシング画面を工作したが未遂
平成 28 年 1 月	無職少年が不正アクセス（立件分）
平成 28 年 2 月 15 日	警視庁から佐賀県教育委員会へ不正アクセス事案の連絡
平成 28 年 2 月 16 日	業者に対しログ保全依頼、管理パスワードの定期変更を開始（一部の管理パスワードを変更せず）
平成 28 年 3 月 11 日	警視庁から SEI-Net システムの脆弱性の情報提供
平成 28 年 3 月 15 日～	SEI-Net の脆弱性への対応を開始（4 月 27 日完了）
平成 28 年 5 月 19 日	警視庁から「パスワード変更以降も不正アクセスを行っていた可能性」について連絡があり、業者に対しサーバパスワードの変更を指示
平成 28 年 5 月 20 日	警視庁から校内 LAN 及び SEI-Net の脆弱性に関する参考情報の提供を受ける
平成 28 年 5 月 25 日	校内 LAN の業者に対し、5 月 20 日に連絡があった情報に対する対応を検討するよう指示
平成 28 年 6 月 27 日	無職少年が不正アクセス禁止法違反の疑いで再逮捕される 不正アクセス事案を公表

検討委員会　提言書（本編）より抜粋、引用

検討委員会では、本事案の情報窃取の原因を「県教育委員会や教職員、委託事業者にセキュリティの基礎知識や実践的な対応が不十分だったことによる。代表的な事例は「管理者パスワードの蔵置」である。また、本事案発覚の一年前にその兆候を覚知したにもかかわらず「トラブル案件の一つ」と過小評価し、縦割り組織の中で情報共有がなされず、責任の所在も不明確だったため、問題が矮小化された。さらに一部のシステムにセキュリティ上の脆弱性が含まれており、その脆弱性を早期に発見する機会を逃していた。」と指摘しています。そして、運用上の課題として以下の 3 点を挙げています。

1．侵入された校内 LAN ネットワーク内に管理者パスワード等、多くの重要情報が保存されていた。また、アカウントの管理やパスワードの設定が不適切であった。主なものは、以下のとおりである。
・教材インストール用のスクリプトファイルを、学習用サーバの生徒がアクセスできる領域に蔵置していた。（学習用サーバの管理者 ID、パスワードを入手可能）
・学習用サーバの管理者 ID、パスワード等が記載されているＩＣＴサポーター引継書を、学習用サーバの教師がアクセスできる領域に蔵置していた。
・Wi-Fi 環境設定等を管理するソフトウェアに係る管理者 ID、パスワードを、学習用サーバの教師及び生徒がアクセスできる領域に蔵置していた。（生徒の MAC アドレスを入手可能）
・学習用サーバの教師がアクセスできる領域に、管理者が曖昧な管理者権限のアカウント（kanriID）が存在していた。
・管理者パスワードに規則性があったため、「学習用サーバの管理者パスワード」から「校務用サーバの管理者パスワード」が推測できた。
2．SEI-Net システムに脆弱性があった。
本システムは県教育委員会の仕様に合わせてパッケージソフトウェアを修正したが、セキュリティが要求仕様に十分に反映されず、修正に脆弱性が含まれていた。
また県教育委員会におけるセキュリティ検証も十分でなく、確認する機会があったものの、結果として脆弱性を見逃すこととなった。また運用後のセキュリティ監査を実施することで早期に発見できる可能性はあった。
脆弱性の内容については、以下のとおりである。
・学習管理機能におけるメッセージ送信機能の宛先検索画面において特殊な操作を行うことにより、本来見ることができない教職員情報を取得することができた。
・開発者ツールを用いて生徒権限を教師権限に変更する操作を行うことにより、生徒情報を取得することができた。
3．ある高校での関連事案（平成 27 年 6 月に教職員が校内 LAN にアクセスできなくなっている事案等）への対応に課題があった。関連事案への対応については、侵入の重大性を理解できなかったこと、セキュリティ侵害に対する知見不足が事案を矮小化させたこと、その結果、県教育委員会・全校での情報共有がなされず、追跡調査も不十分であった。

この事案を受けて、平成 28 年 7 月「2020 年代に向けた教育の情報化に関する懇談会」最終まとめにおいて、「情報セキュリティのための緊急提言」を行いました。システムネットワークの論理的、物理的な分離の必要性と、情報保管の際の暗号化の徹底、認証の強化を盛り込んでいます。また、教職員への情報セキュリティに関する研修の実施、体制の強化もその中に含まれています。佐賀県教育委員会においても事案覚知後、以下の対応を速やかに実施しています。

（1）　無線ＬＡＮへの偽装接続への対応
不使用時（夜間・休日）の無線ＬＡＮの停止措置を講じた。
（2）　管理用セグメント経由の意図しない通信への対応
平成 27 年 6 月の事案覚知後、学習用端末及び校務用端末のネットワークから各サーバへのリモートデスクトップ
接続ができないよう全てのサーバに対してファイアウォールの設定変更を実施した。さらに平成 28 年 2 月の事案
覚知後、学習用サーバから校務用サーバにアクセスできない措置（センタースイッチ及びファイアウォールによる論理的分離）を実施した。
（3）　その他
校内 LAN にログ追跡機能を導入するとともに、校務サーバ内のファイルの暗号化を実施した。
（4）　全ての管理者 ID、パスワードについては、全て変更するとともに、各学校にはその変更内容について意図しない情報拡散を防ぐ目的で通知等を行わないこととした。またヘルプデスク現地員がパスワードを必要な作業を行う場合には、ワンタイムパスワードを教示することとし、利用後は無効化させる措置を講じた。
また、検討委員会は、提言書の中で、短期的、中長期的なセキュリティ対策について以下のように提言しています。

■短期的対応（概要）

可及的速やかに実施し、継続的な対応を行うもの。下記の件を踏まえて、実施計画書を作成すること。
(1) アカウント管理（パスワードポリシーの設定）
(2) セキュリティ／システム監査の実施（内部監査、外部監査）
(3) 関係者による情報共有体制の確立（事例の共有による「気づき」の促進）
(4) セキュリティ文化の確立（グループ、組織としての教育、訓練）

■中長期的対応（概要）

来期以降、中長期的に対応しなければならないと思われるもの。ただし、今期に行う事が可能であれば、実施すること。
(1) セキュリティ組織の検討・実施（CIO、CISO、プロジェクトマネジメントチーム）
(2) 情報公開の検討・実施（小さな事案でも公開すべき）

■情報セキュリティ事故が起こる危険性

これまで示してきたように、学校ではさまざまな情報セキュリティ事故が繰り返し発生しています。その多くは置き忘れや誤送信といった、人間が避けられないミスに起因するものですが、一方で車上荒らし・盗難や第三者による不正アクセスなど、悪意を持った行為による事故も常に発生する危険性があります。

情報システムやネットワークを整備し、運用するシステム担当者の立場として特に重要なのは、このような危険性に対して備えをすることであり、実際に発生してしまった、あるいは発生した可能性が生じた時点から速やかに適切な対応を取って被害を最小限に抑えることです。当然、自組織か他組織かを問わず、実際に起こった情報セキュリティ事故から自組織が改善すべき点を抽出し、速やかに反映していくことが、情報セキュリティ事故の危険性を減らし、事故発生時の被害をも小さくしていくために有効であることは言うまでもありません。

情報セキュリティ事故を防ぐためには、技術的な対応を施すことに加えて、アカウント管理の強化や情報セキュリティ監査による現状の確認など運用面での強化をはかることが重要です。そのためには、システム担当者として情報セキュリティに関する基礎的な知識を身に付け、自らの組織が整備しているＩＣＴ環境において情報セキュリティ事故が起こる危険性を確認することが必要となります。情報セキュリティ事故が起こる可能性を未然に察知し、発生時にも即時対応ができるようにするという点では、学校現場の教職員やシステム担当者自身が情報セキュリティ事故につながりかねない危険性を理解し、そのような事象が発生した時には速やかに情報共有を図る「情報セキュリティ文化」を醸成していくことがポイントとなります。

まず、情報セキュリティに関する基礎知識を確認し、所管の学校の状況を振り返ってみましょう。

2.1.3　学校における情報セキュリティ基礎知識

■情報セキュリティの概念

一般的に「情報セキュリティ」とは、情報の「機密性」「完全性」「可用性」を維持することであり、単に、情報を漏えいしないことではありません。情報セキュリティの概念では、これら３つの守るべき性質をあらわす英単語（機密性 confidentiality ／完全性 integrity ／可用性 availability）の頭文字を取って「情報の CIA」ということもあります。（セキュリティマネジメントシステムの国際標準である ISO/IEC17799 の定義）。（図表 2-6）

図表 2-6　情報の CIA

機密性	ある情報へのアクセスを認められた人だけが、その情報にアクセスできる状態を確保すること
完全性	情報が破壊、改ざん又は消去されていない状態を確保すること
可用性	情報へのアクセスを認められた人が、必要時に中断することなく、情報にアクセスできる状態を確保すること

■情報資産とは

学校における情報資産とは、教育を行うに当たって有効な情報です。有形・無形を問わず、組織の財産である情報とその情報を活用するすべてのものが対象となります。

校務系、学習系の学校を取り巻く情報システムは有形無形を問わず、子供の情報をはじめ、さまざまな情報資産を有しています。学校においては学籍関連の情報、生徒指導関連の情報、成績関連の情報、進路関連の情報、保健関連の情報、事務関連の情報などがあります。（図表 2-8）

図表 2-7　情報資産のイメージ

図表 2-8　学校内の情報資産リストの例

資料出所：財団法人コンピュータ教育開発センター「学校情報セキュリティ・ハンドブック改訂版」

その情報を利用する環境は、ソフト面におけるアプリケーション、システムソフトウェア、ハード面におけるパソコン等のコンピュータ装置、スマートフォン等の通信装置、USB メディアやフラッシュメモリーなどのメディアを指します。（図表 2-7）

情報セキュリティを検討する際には、日常業務に携わる教職員の役割として「情報資産の洗い出し」が必要となります。学校で取り扱う情報の中には、子供や保護者の個人情報、学校運営のために必要不可欠な情報が多数存在しています。これらの情報を、誰が・どこに・何を保管しているのか項目のリスト化が必要となります。

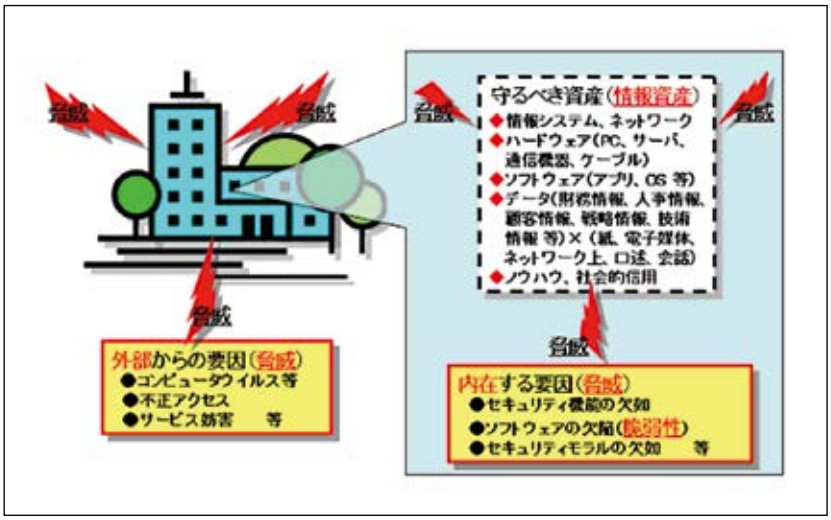
洗い出しが完了した後、顕在化した情報資産のリストを保存形態（紙媒体なのか、電子データなのか）、保存場所（ＰＣのフォルダ内なのか、USB フラッシュメモリーや HDD 等の記録媒体なのか）、公開対象者（教職員全般なのか管理者のみなのか）を絞り込み、再度のリスト化が必要になります。参考として、学校内情報資産リストの例を示します。

■情報資産にもたらされる脅威

情報資産に対して、組織に被害や影響を与える可能性をもたらす要因となる「脅威」が必ず存在しています。情報資産の機密性、完全性、可用性を損なうかもしれない脅威に対して、どのように情報資産を守っていくのか考えてみましょう。情報資産は図表 2-9 のように外部だけでなく内部からもさまざまな脅威にさらされています。

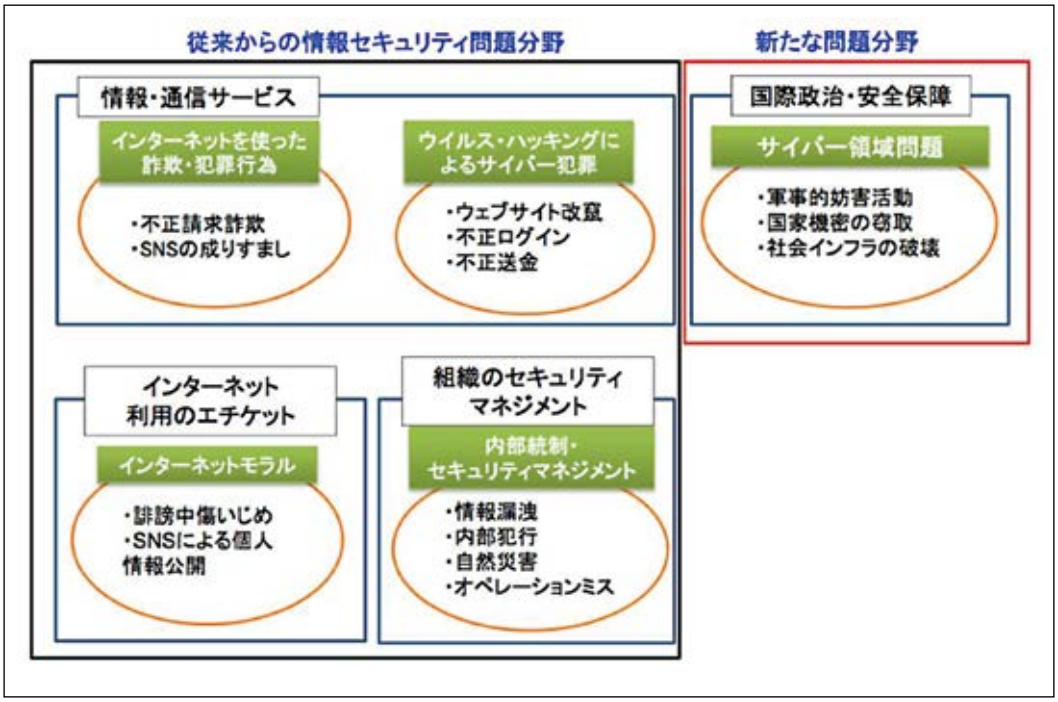
独立行政法人情報処理推進機構セキュリティセンターが 2014 年にまとめた「情報セキュリティ 10 大脅威」によると、情報セキュリティの脅威は、図表 2-10 のように大きく 5 つに類型化されています。特に最近は、国際的なサイバー領域問題が指摘されています。

図表 2-9　リスク評価のイメージ



資料出所：情報処理推進機構 http://www.ipa.go.jp/security/manager/protect/pdca/risk_ass.html

図表 2-10　情報セキュリティの脅威



資料出所：情報処理推進機構（情報処理情報セキュリティの脅威　2014 年版情報セキュリティ 10 大脅威）

代表的な情報セキュリティの脅威を以下に挙げてみましょう。

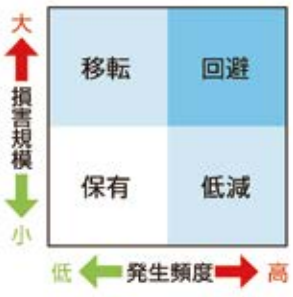
脅　威	内　　容
マルウェア	マルウェアとは、「Malicious Software」（悪意のあるソフトウェア）を略したもので、さまざまな脆弱性や情報を利用して攻撃をするソフトウェア（コード）の総称です。コンピュータウイルスと同じ意味で使われますが、厳密にはさらに広義な用語として使われています。ウイルスのほか、ワーム、スパイウェア、アドウェア、フィッシング、ファーミング、スパム、ボット、キーロガー（キーストロークロガー）、トロイの木馬、論理爆弾、などさまざまな種類のマルウェアが存在しています。（「国民のための情報セキュリティサイト」総務省より）
不正アクセス	不利用する権限を与えられていないコンピュータに対して、不正に接続しようとすること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともあります。（「国民のための情報セキュリティサイト」総務省より）
情報の持ち帰り、パソコンやメディアなどの紛失	パソコンや USB メディア、外付けハードディスクなどの取り扱い方もひとつ誤るとセキュリティの脅威になります。たとえば、仕事を持ち帰る。となったときに USB メディアへ保管することがあります。 小さく持ち運びしやすい反面、紛失しやすくまた盗難にあったとしてもすぐには気がつきにくいものです。こういった不用意な情報の持ち帰りが情報セキュリティの脅威につながります。

情報資産に対する脅威は外部からとは限りません。使用しているソフトウェアを最新のものにすることを怠るだけでも情報漏えいの危険性は高まります。また、情報セキュリティに対するモラル意識が不十分な教職員が存在すれば、持ち出しを禁止されている情報資産を作業のために自宅に持ち帰る途中で紛失したといった情報セキュリティ事故が発生する余地が生まれます。

■リスク評価と対応検討

それぞれの情報資産に対して想定されうる脅威を洗い出し、損害の発生の頻度（確率）と損害の規模を勘案して脅威の大きさをおおよそ「大・中・小」あるいは「１・２・３」といった三段階程度に分類します。この際、リスクの評価、それぞれの情報資産自体の脆弱性も評価の対象となります。このようなリスク評価（アセスメント）を行ったうえで、リスクの処理策を検討し、決定します。

図表 2-11　リスクの処理策



	考え方	例
低減	脅威または脆弱性を小さくするなどの方法により、リスクを小さくする	パスワードを定期的に変更することにより、パスワードが盗まれたときのリスクを小さくする
回避	脅威そのものを取り除くことにより、リスクが発生する可能性をなくしてしまう	ノートパソコンの持ち出しを禁止することにより、外出先で紛失するリスクをなくす
移転	自校の抱えるリスクを他者に移し替える	自校で管理していたサーバーを企業などに委託することにより、自校のリスクを移転する
保有	リスクがあっても、特に対応しない	小さなリスクまですべて対応することは現実的ではないので、対策しない

資料出所：学校情報セキュリティ・ハンドブック

リスクに対しては、「低減」「回避」「移転」「保有」など、さまざまな処理の方法を採りますが、具体的な管理策の検討に当たっては、環境面（業務で使用するパソコンやネットワークなどの機器に関する技術的・物理的な側面）や運用面（情報資産を扱うに当たって教職員や子供が取り扱う管理的・人的な側面）などを意識しながら考える必要があります。（図表 2-11）

リスクの対応策を検討してリストアップできたら、その中から実際に採用する対応策を決定することになります。環境面と運用面の現状やと対応策の効果を考えて、採用する対応策を決定すべきです。

なお、このようなリスク評価の作業は、個々の教職員が行うよりも、客観的な観点から一元的に作業を進める方が望ましいと言えます。

情報セキュリティ対策を考える際には、情報資産に対する脅威に対して、学校での脆弱性の実態を正確に把握する必要があります。各々の教職員が情報資産とそれに対する脅威を意識し、情報資産やリスク対応シートなどのリストづくりの過程を通じて「守るべき資産」が何か、共有していくことが重要となります。（図表 2-12）

図表 2-12　リスク対応策検討シートの例

	リスク名	考えられる対応策	採用する対応策
個人情報保護関連	個人所有パソコンの盗難，紛失による漏洩	個人PCの持ち込み禁止 罰則規定を設ける	個人PCの持ち込み禁止
	USBメモリ等のメディアの盗難，紛失での漏洩	パスワード設定の義務づけ 暗号化の義務づけ 認証式のメディアの導入 持ち出し禁止の規定	パスワード設定の義務づけ 暗号化の義務づけ 認証式メディアを利用
	メールご送信による漏洩	フリーメールの利用制限 研修による扱いの徹底 添付のできないメールツールの採用	フリーメールの利用制限
	情報機器処分時のデータ消し忘れによる漏洩	廃棄時の扱いマニュアル作成 廃棄時のデータチェック	廃棄時の扱い手順を規定
	個人認証におけるなりすましによる漏洩	アカウント，パスワードの管理についての研修 生体認証の導入	アカウント，パスワードの管理義務を明確にする
	ディスプレー盗み見による漏洩	スクリーンセーバの導入 離席時のロックシステム スクリーンフィルタによる視野角制限	離席時のロックシステムを導入
	教職員による意図的な漏洩	研修の実施と義務づけ 罰則規定を設ける	悉皆研修を行い，その中で服務規程に触れる
情報消失関連の脅威	個人所有パソコンの盗難，紛失による喪失	個人PCの持ち込み禁止 罰則規定を設ける	個人PCの持ち込み禁止
	USBメモリ等のメディアの盗難，紛失での喪失	ファイルサーバ上でデータ管理	ファイルサーバ上でデータを一括管理する
	突然の電源断などによる情報喪失	UPSシステムの整備 データを置くファイルサーバの保護	UPSシステムの整備
	メディアの損傷などによる情報喪失	バックアップの実施	バックアップの実施
	誤消去等，人為的なトラブルによる情報消失	バックアップの世代管理 研修による扱いの徹底 ユーザ権限の設定	世代管理して，被害を最小限に止める
	ディスク障害などハードウェアトラブルによる情報消失	バックアップの実施	バックアップの周期を短く
	保存ミスなど，データの取り扱い不全による情報消失	バックアップで保護 研修による扱いの徹底 ユーザの権限を細分化	ユーザの権限を細分化し，重要なファイルを守る。 バックアップの実施
業務停止関連	サーバ，システム等のダウンによる業務停止	サーバ等のシステムチェックを常時実施 ディスクのAlert装置の導入 バックアップ用のシステムを持つ	システムのチェックを定期的に実施
	停電による業務停止	UPSシステムの整備 発電システムを持つ	UPSシステムの整備
	システムの誤用など人為的ミスによる業務停止	基幹システムを扱えるユーザの限定 監視システムで，異常の検知	基幹システムを扱うユーザの限定 監視システムの導入
情報モラル関連	アカウントの不正利用	アカウント，パスワードの管理についての研修 生体認証の導入 罰則規定	アカウント，パスワードの管理についての研修 罰則規定を設ける

資料出所：学校情報セキュリティ・ハンドブック

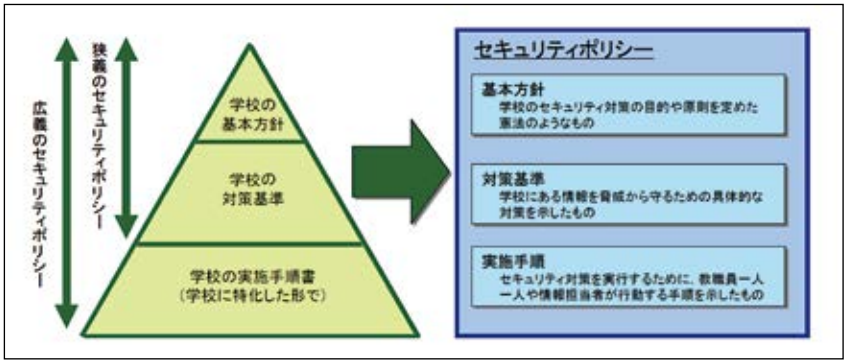
2.1.4　学校における情報セキュリティポリシー

■情報セキュリティポリシーとは

情報セキュリティ確保のため基本文書が、情報セキュリティポリシーです。情報セキュリティポリシーは、以図表 2-13 のように「基本方針」、「対策基準」、「実施手順書」から構成されます。

学校では、子供が教室や職員室に自由に出入りでき、情報資産を隔離したスペースで保管することが難しい状況にあります。また、取り扱う情報資産は学籍や成績の情報など個人情報に関係するものが多いことから、情報セキュリティの確保についても地方公共団体や民間企業とは異なった対応が求められます。公立学校においてこのような学校の特性も考慮し、学校情報セキュリティポリシーを作っていくためには、地方公共団体と学校との役割分担を考えると良いでしょう。

図表 2-13　学校情報セキュリティポリシー文書体系



資料出所：財団法人コンピュータ教育開発センター「学校情報セキュリティ・ハンドブック改訂版」

学校において情報資産を取り扱うＩＣＴ環境は、所管の教育委員会が主体となって整備及び運用することが大半を占めており、学校情報及び児童生徒に関する情報の管理においても教育委員会が一定の責任を担うこととなります。

したがって、学校独自で情報セキュリティポリシーを策定するのではなく、所管の教育委員会が統一的な情報セキュリティポリシーのひな形、「基本方針」と「対策基準」を示し、その内容について学校現場での理解を図りながら「実施手順」のひな形を策定するなど、教育委員会を中心とした学校現場の情報セキュリティ確保が望まれます。

■情報セキュリティポリシー策定・導入～運用のプロセス分担

情報セキュリティポリシーの策定、運用においては図表 2-14 の手順が考えられます。

どの方法を選定するにせよ、教育委員会の責任にて分担を決定し、導入を進めることが望まれます。組織体制に関しては学校はもちろん、教育委員会でも情報セキュリティに関する専門知識を有するスタッフを確保するのが困難なことがあるため、基本方針・対策基準については、下表のうち、首長部局等（情報政策担当部署等）の支援を得ながら教育委員会で策定する方法が望ましいと考えられます。

実施手順については、教育委員会が域内の学校等での校務業務や情報システムの横通し・標準化を図っている度合いにもよりますが、教職員の異動に伴う習熟の手間を考えると、できるだけ同一の実施手順を適用できる方が望ましいと考えられます。

図表 2-14　情報セキュリティポリシー策定までの流れ

資料出所：独立行政法人情報処理推進機構 (IPA)
「中小企業の情報セキュリティ対策ガイドライン第２版」」

地方公共団体の情報セキュリティポリシーに沿って運用している学校もあります。その場合においても、学校が保有する情報資産や学校自体の特性を踏まえた内容での情報セキュリティポリシーを策定し、適切に運用することが望まれます。

■情報セキュリティポリシーの策定作業

「基本方針」は、地方公共団体（教育委員会）が統一的な情報セキュリティポリシーのひな形やガイドラインを示している場合、それに沿って策定します。前述の役割分担イメージにある通り、教育委員会が主導するケースもあれば、学校が策定するケースもありますが、組織の責任者の積極的な参画のもと、専門的知識のあるスタッフがチームを組織する体制が効果的と考えられます。

「基本方針」の形式については、地方公共団体向けガイドラインのように「基本的事項を規定する形式」と、企業などでしばしば用いられる情報セキュリティの最高責任者名での「宣言書形式」の２通りがあります。教育委

員会、学校で多くが採用している前者では、以下のような項目が定められています。

> 目的、対象とする脅威、適用範囲（組織・情報資産）、教職員の遵守義務、必要な情報セキュリティ対策の実施（点検、ポリシー見直しを含む）、対策基準及び実施手順の策定。

「対策基準」には前述のとおり、「情報資産の洗い出し」、「リスク評価と対応検討」の結果、「守るべき情報資産」を守るために必要な対策の基準を物理的、技術的、人的な側面などを総合的に検討し盛り込みます。基本方針と対策基準はセットで策定されるものですので、他の地方公共団体や学校の事例、前述のガイド等を参考とすることができるでしょう。

「実施手順書」は対策基準を実行するために、教職員の作業手順を具体的に示したマニュアルに相当するものです。たとえばシステムにログインするためのパスワードの管理について、字種や桁数、更新頻度などを定め、書き留めたメモは人目につかない自席の引き出し等でカギをかけて保管するといったルールを定めることです。他にも情報セキュリティを確保するためには必要な事項が多数あるので、全ての関係者が情報セキュリティポリシーを遵守できるように、本書末のチェックシートなども参考にしながら、具体的に何をどのように実施するのかを明確にします。その内容に基づいて学校側の「実施手順書」を策定していくことが求められます。

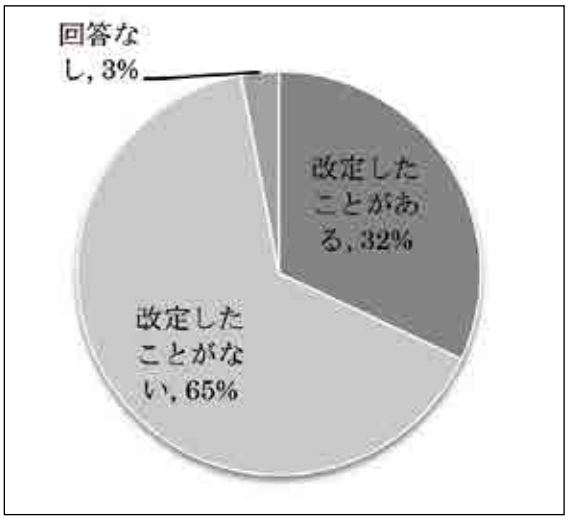
■情報セキュリティポリシーの運用

情報セキュリティポリシーを運用するのは学校であり、個々の教職員です。

ただし、策定して終わり、ではなく、情報セキュリティポリシーの実効性を挙げるためには、絶えず運用状況を確認し、改善や見直しの必要を検討する必要があります。そのため、運用計画には、情報セキュリティポリシー策定後も組織の変更や法令の改正、情報通信技術の進展に伴う新たな脅威の出現、運用を通じた新たな課題の発生等に応じて、都度改善、見直していくことを盛り込んでいくべきです。

「教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック（総務省　H28.5）」によると、情報セキュリティポリシーを制定した後に見直しをした地方公共団体の割合は約32％にすぎません。（図表2-15）情報資産への新たな脅威等へ適切に対応できているか、確認していただくと良いでしょう。

図表2-15　情報セキュリティポリシーを改定したことがあるか



教育分野におけるクラウド導入に対応する
情報セキュリティに関する手続きガイドブック（総務省　H28.5）

このガイドブックに記載された情報セキュリティ見直しの内容を見ると、どのような脅威や情報利用に対応しているか確認できます。教育関連ではタブレットＰＣ等の機器の活用に伴い、無線ＬＡＮの使用範囲を拡大したり、可搬型機器の利用規定を追加したりしていることがわかります。（図表2-16）

システム構築時に情報セキュリティを十分に考慮したとしても、日々の運用の中で、あるいはシステム更改の際に、想定していなかった脆弱性が露わになってしまうことがあります。そのような事象を防ぐために、情報セキュリティポリシーや手順書を作成し、管理者・利用者といった関係者の基本動作を徹底することが期待されます。

「教育分野におけるクラウド導入に対応する情報セキュリティに

図表2-16　情報セキュリティポリシーの改定

分類	改定の内容
個人情報	・個人情報を含むファイルの保存方法について、パスワードの設定の規則を追加した。 ・情報資産を外部提供する際に、自治体の個人情報保護条例等の規定に抵触しないことを確認する義務を追加した。 ・学校ホームページに写真等をアップロードする場合の個人情報保護や同意の取得についての項目を改定した。
無線ＬＡＮ	・教育用パソコン（タブレット端末を含む）の使用に限り、無線ＬＡＮの使用を認めた。 ・タブレット端末導入にあわせて、無線ＬＡＮを授業用ネットワークのみで認め、無線ＬＡＮアクセスポイントの情報セキュリティ機能要件を明記した。 ・学校内で無線ＬＡＮを利用する場合に必要な情報セキュリティについて定めた。
ＩＣＴ機器	・タブレット端末の利用規定を追加した。 ・タブレット端末の利用上の注意事項と、情報モラル教育について追記した。 ・教職員の情報機器の取り扱いに関する事項を追記した。 ・ＩＣＴ機器の管理（施錠できる保管庫等への格納）に関して記載した。
クラウドサービス	・クラウドサービスのような外部サービスの利用、委託先の管理、ネットワーク（公衆通信網）の利用、支給品以外の個人所有のスマートフォンなどの端末等やソーシャルメディアサービスの業務利用、情報セキュリティインシデント対策体制の強化について追記した。 ・クラウドサービスを利用する場合の基準について追記した。 ・クラウドサービスへの無断登録（保存）の禁止事項を追記した。

教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック（総務省　H28.5）

関する手続きガイドブック（総務省 H28.5）」には具体的な事例も記載されています。札幌市では、クラウドサービスを活用するにあたり、情報セキュリティポリシーに関する進め方について細かく検証しました。クラウドサービスの導入毎に、機能や取り扱う情報、運用体制等を定める「ガイドライン」と、学校長や教頭、利用者の責任範囲や情報セキュリティ対策を定める「利用手順」を作成しています。（図表 2-17）

図表 2-17　札幌市におけるセキュリティガイドライン・手順書の例

<ｱﾌﾟﾘｹｰｼｮﾝ A を利用した情報共有に関するｶﾞｲﾄﾞﾗｲﾝ>	<アプリケーション A 利用手順>
1．本ガイドラインの目的	1．目的および適用範囲
2．情報共有の定義	2．実施体制と責務
3．アプリケーション A の利用にあたっての基本原則	3．情報資産の特定
4．利用する機能について	4．人的セキュリティ対策
5．取り扱う情報について	5．情報セキュリティ対策の遵守義務
6．運用体制について	6．技術面及び運用面における情報セキュリティ対策
7．効果の検証等について	

■情報セキュリティポリシーの教育、改善

作成した情報セキュリティポリシーは、教職員に配布し、同意を求めます。専門用語が多い場合は、情報セキュリティポリシーの各条項がなぜ必要かを説明するとともに、対策基準及び実施手順書を使って、具体的な操作を含む研修会を実施すると良いでしょう。

さらに成績情報や就学援助、住所録などの個人情報の管理の重要性とマルウェア対策などは、具体的な担当と実施時期を定め、定期的に点検を行い、問題点の把握と改善に努める必要があります。点検や運用の中で発生した問題を把握するとともに、教職員の意見も収集します。この情報をもとに、情報セキュリティポリシーの見直しや改善を行い、組織の変更や法令の改正などによっても変更が必要になる場合には、再度配布し同意を求めて運用します。

図表 2-18　「学校情報セキュリティお役立ち Web」

資料出所：ＩＳＥＮ（http://school-security.jp/）

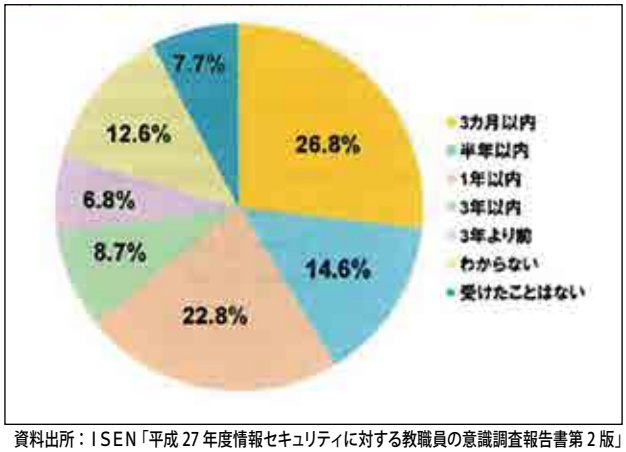
情報セキュリティポリシーの作成及び運用に当たっては、トラブルに対する問題意識を校内で共有しあうことが大切になります。これまでに発生した個人情報漏えい等の情報セキュリティ事故の内容を知り、情報資産を取り扱う教職員自身が事故を他人事ではない身近なこととして捉える意識を涵養することが重要です。

運用していく中で、事故が発生することも考えられますが、責任を問われることを恐れて報告も対処もしないといったことが起こらないよう、情報セキュリティに関して素早い報告や相談がしやすい雰囲気を作っておくべきです。

情報セキュリティの重要性を理解し、さまざまな情報セキュリティ対策を実施している場合でも、情報漏えいやマルウェア感染や不正アクセスといった事故が発生してしまうケースはあります。技術的な対策だけで万全とは言えず、情報を取り扱っている教職員や子供の情報セキュリティの意識が低ければ事故は発生する可能性があります。

教職員や子供の意識を高めるためには、さまざまな教育コンテンツを活用し、どのような脅威があるのか知る必要があります。ＩＳＥＮ「学校情報セキュリティお役立ち Web」（図表 2-18）をはじめ、最新の教育コンテンツが提供される Web サイトなどを活用して、知識の共有を図ることが望まれます。

図表 2-19　教職員が情報セキュリティ研修を最後に受けた時期



資料出所：ISEN「平成 27 年度情報セキュリティに対する教職員の意識調査報告書第 2 版」

また、情報セキュリティ研修を受けたことのない教職員や、長期にわたって研修を受けていない教職員もいるという実態を踏まえて（図表 2-19）、学校内で実施できる情報セキュリティポリシーや運用ルール、情報セキュリティの脅威の事例などを題材としたミニ研修などを準備することも、意識向上には有効でしょう。

一方的な情報提供ではなく、自分たちの身近な問題として認識してもらうことで人的セキュリティ意識が向上します。

事例を活用したグループディスカッションでリスク回

避のための方法や実施時の課題などを話し合うことで、情報セキュリティをより身近な問題として考えることができるようになり、当事者意識を高めることができます。

また、企業などでは、

●毎月１回、「情報セキュリティの日」を設定し、過去の事故事例を紹介し問題点についてグループ討議を行う

●毎年１回、「情報セキュリティ啓発期間」を設定し、トップメッセージ・啓発動画視聴・改善施策展開・事故事案の再周知を図る

など、継続的に取組を続けている例もあります。教育現場にも参考になる点もあるでしょう。

■三鷹市の情報セキュリティへの取組

三鷹市では、セキュリティの確保と職員のＩＣＴリテラシーの向上を大きな課題として、人材育成・技術的対応・組織的対応といった、さまざまな観点からのアプローチを行っています。市民部を中心とした 11 課は情報セキュリティマネジメントの認証を取得（平成 20 年には、教育委員会総務課・学務課・指導課も取得）し、認証取得課以外でも、認証取得課である企画部情報推進課が業務システムのサーバ機器やネットワークを管理運用することで高いセキュリティ水準を維持しています。体制面でも副市長をトップとした情報セキュリティ運営委員会を組織し、庁舎管理部門・文書管理部門・情報システム部門及び庁内各部署の責任者・管理者による全庁網羅的な体制で、情報セキュリティ対策に取り組んでいます。

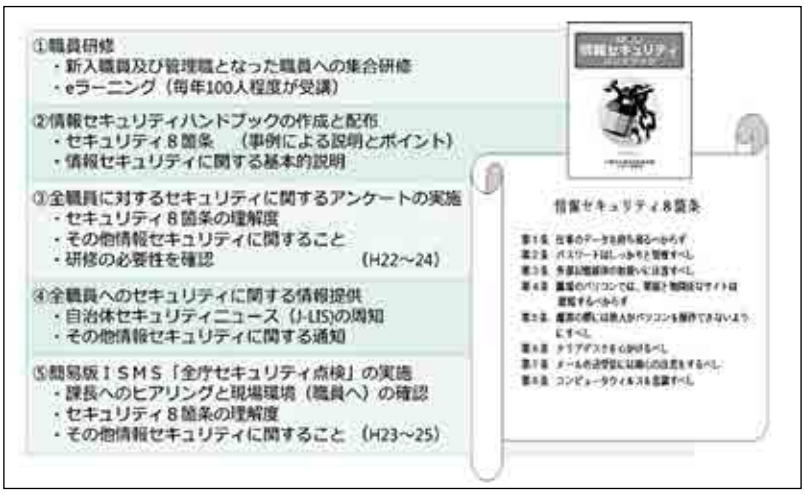
また、集合研修やｅラーニングを活用した職員研修のみならず、情報セキュリティハンドブックの配布を始めとした職員への情報提供などを行っています。

さらに、職員を対象としたアンケート調査や点検の実施により、対策の履行状況をチェックし、見直しに反映しています。

図表 2-20　三鷹市での情報セキュリティへの取組の経緯

年度	トピック	動向
H14年度	・情報セキュリティポリシー策定　・リスクアセスメント手法の基礎確立	準備
H15年度	・ISMS構築の取り組み開始　・市民課、市政窓口、情報推進課で認証取得	事業開始
H16年度	・市民課から市民部全課に適用範囲拡大　・市民税課、資産税課、納税課、保険課が認証取得	拡大
H18年度	・ISO27001への移行対応　・政策法務課と契約管理課が認証取得	拡大
H20年度	・教育委員会総務課、学務課、指導課が認証取得　全庁11課で認証取得 ・情報セキュリティハンドブックの配布	拡大・更新
H21年度	・リスクアセスメント手法、内部監査手法の見直し ・全庁管理職を対象としたセキュリティ研修の実施	運用 見直し
H22年度	・全職員を対象とした情報セキュリティに関するアンケートの実施（以降毎年実施）　・「自治体セキュリティニュース」による啓発開始・情報セキュリティハンドブックの更新（第2版）	運用 底上げ
H23年度	・ISMS認証取得課以外への啓発 ・全庁セキュリティ点検（1年目）	運用 底上げ
H24年度	・更新審査 ・全庁セキュリティ点検（2年目）	運用 底上げ
H25年度	・ISMS認証取得課以外への啓発 ・研修の充実（外部職場、嘱託職員への啓発） ・全庁セキュリティ点検（最終年）	運用 底上げ
H26年度	・ISMS規格改訂に伴う移行審査	運用 見直し
H27年度	・情報セキュリティハンドブックの改訂（第3版）　・情報セキュリティポリシーの見直し検討	運用 見直し

図表 2-21　三鷹市での情報セキュリティの研修・職員への周知



■三鷹市立学校情報セキュリティ基本方針の策定（平成 28 年 6 月）

三鷹市教育委員会ではこれまで、三鷹市立小・中学校教育用コンピュータ及びインターネット取扱基準（平成 15 年）、校務のために教職員が作成したデータの管理に関する運用指針（平成 17 年）、三鷹市立学校における個人情報及び情報資産の適正な管理について（通知）（平成 20 年）など、環境や制度の変化に応じて学校への情報セキュリティに関する指導や情報提供を行ってきました。

しかし、上記の通知には課題があったことから、それらに対応、解決するため、平成 28 年 6 月に市長部局の「情報セキュリティマネジメント（ISMS 認証取得）」を参考に、以下のとおり「三鷹市立学校情報セキュリティ基本方針」を策定しました。

①「三鷹市立学校情報セキュリティ基本方針」

②「三鷹市立学校情報セキュリティ対策基準」

　○「学校情報取扱基準」　　○「利用要領」

③「三鷹市立学校情報セキュリティ対策実施手順」（参考モデル）

○学校情報資産取扱一覧表
○私物機器・媒体使用記録票
○学校情報セキュリティ研修等実施記録表
○学校情報セキュリティ文書・記録一覧表
○学校情報セキュリティ事故発生報告書
○学校情報外部持ち出し記録票
○学校情報セキュリティ対策実施体制図
○学校情報セキュリティ対策実施状況報告書

表 2-22　三鷹市立学校情報セキュリティ基本方針策定前の課題と解決に向けた取組

課　　題	解決に向けた取り組み
①個々の規定が独立しており、体系化されていないため分かりにくい	①⑤既存の規定類を、現在のＩＣＴ技術動向、社会情勢及び教育ネットワークシステムの運用を踏まえ、三鷹市のＩＳＭＳの運用を参考に「三鷹市立学校情報セキュリティ基本方針」として再構成 →規定類の体系化による情報の整理
②学校における情報セキュリティに関する事項について、学校と教育委員会事務局の役割分担が不明確	②学校における情報セキュリティに関する事項について、学校と教育委員会事務局の役割分担を明確化 →教育委員会全体で取り組む体制の整備
③各学校が策定した「個人情報等安全管理基準」の運用状況を定期的にチェックする仕組みがない	③各学校の情報セキュリティに関する運用状況を定期的にチェックする仕組みの導入 →策定したルールの有名無実化の予防
④私物機器（タブレットＰＣ及びスマートフォン等）の利用も校長の許可があれば全て可 ⑤教職員の遵守事項が現在のＩＣＴ技術動向、社会情勢及び教育ネットワークシステムの運用と乖離	④⑤現在のＩＣＴ技術動向、社会情勢及び教育ネットワークシステムの運用を踏まえた教職員の遵守事項の見直しと校長裁量範囲の明確化 →グレーゾーン減少による情報セキュリティリスクの低減

これに伴い、各学校には「三鷹市立学校情報セキュリティ対策実施手順」（参考モデル）を基として「（各校における）情報セキュリティ対策実施手順」を作成・提出するよう求めました。

■三鷹市立学校情報セキュリティ基本方針のポイント

①基本方針の構成

教育委員会が策定した「三鷹市立学校情報セキュリティ基本方針」において、学校の情報セキュリティに関する教育委員会としての方針、運用方法及び教育委員会事務局と学校の役割分担を定めています。

また、この基本方針に基づき教育委員会が策定した「三鷹市立学校情報セキュリティ対策基準」において、情報セキュリティに関する共通の義務事項や禁止事項を定めています。

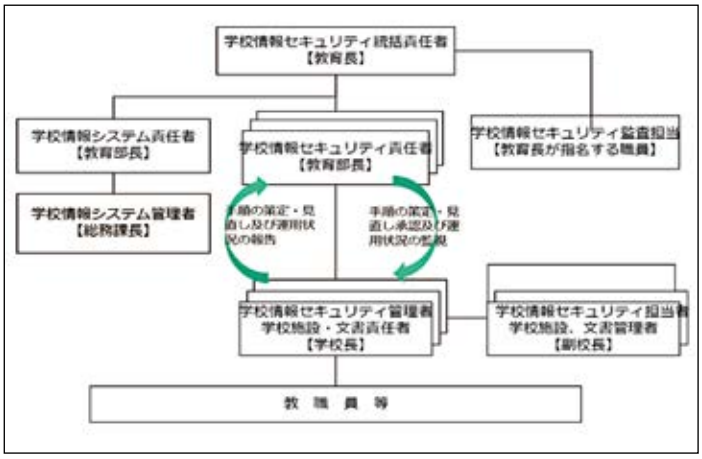
各学校では、この「基本方針」「対策基準」を踏まえて、教育委員会がまとめた「三鷹市立学校情報セキュリティ対策実施手順」（参考モデル）に則って、各学校における情報セキュリティ対策実施手順を策定し、具体的な運用ルールや役割分担を定めています。

②学校と教育委員会事務局の役割分担

三鷹市立学校情報セキュリティ基本方針で、図表 2-23 の役割分担を定めています。

教育委員会事務局の学校情報セキュリティ責任者は、各学校に対して情報セキュリティ対策実施手順の策定を指示します。各学校は、策定した実施手順を学校情報セキュリティ責任者に報告し、承認を得ます。さらに、各学校は毎年度手順の見直しを行い、教育委員会の学校情報セキュリティ責任者に報告する義務があります。この仕組みを運用することにより、運用状況を教育委員会事務局・学校間で共有します。

表 2-23　セキュリティ基本方針（役割分担）



③チェック機能

三鷹市立学校情報セキュリティ基本方針の策定

前は、平成 20 年度に指導課より、各学校に「個人情報等安全管理基準」の策定と校内研修の実施を通知していましたが、基準の運用と研修実施は各学校に委任していました。

三鷹市立学校情報セキュリティ基本方針の策定後は、情報セキュリティ対策に関するチェック機能を強化し、学校長に対して次の各項目の実施を義務付けました。

(1) 毎年 4 月中に教職員等向け研修実施（新規任用の教職員等に対しては着任時に実施）
(2) 年 1 回の手順見直しの検討
(3) (1) 及び (2) の実施状況の記録と、教育部長への報告（年度毎）

④教職員の遵守事項の見直しと校長裁量の明確化

(1) 教職員遵守事項の見直し

実際に守られ、的確に運用されるポリシー、ルールとするため三鷹市立学校情報セキュリティ基本方針の策定に伴い、教職員の遵守事項として、項目を新たに追加し、常に確認しやすいように A4 用紙 1 枚に一覧化しました。（図表 2-24）

表 2-24　三鷹市教職員の遵守事項

【三鷹市立学校情報セキュリティ遵守事項】
1　学校が保有する情報は、「原則外部への持ち出し禁止（メール送信も禁止）」
2　上記の情報のうち、三鷹市立学校情報セキュリティ対策基準別表に定める分類S-1に該当する情報資産は、「絶対に持ち出し禁止」※1、「指定場所以外への保存禁止」、「メール送信の禁止」
3　三鷹市及び三鷹市教育委員会が配置している「機器（※2）の持ち出し禁止」
4　業務上の目的で、電子ファイル・記録媒体（※3）等の情報資産を校外へ持ち出す場合は、「事前に書類の提出及び校長の許可が必要」※3、「電子ファイルにはパスワードを設定」、「パスワードと記録媒体（※4）を一緒に携帯しない」、「校長の許可の下、記録媒体（※4）を外部に持ち出す場合は、記録媒体（※4）を入れるかばんなどを身体から離さない」
5　私物の機器（※5）・記録媒体（※4）は、「校務・授業等での使用（校内の機器（※2）への接続を含む。）禁止」
6　三鷹市立学校情報セキュリティ対策基準別表に定める分類S-1に該当する情報資産は、「S-1とS-1以外を分けて保管・管理」、「児童・生徒も使用するフォルダでの作業は禁止」
7　業務に関係のないインターネット上のウェブサイトへのアクセス禁止
8　ｗｅｂメールサービス（Gmail、Yahoo!メール及びhotmail等）の利用禁止
9　インターネット上のストレージサービス（Dropbox、Googleドライブ及びOneDrive等）の利用禁止
10　業務上必要のない送信先への電子メールの送信禁止
11　学校・学園ホームページ及び三鷹ＳｃｈｏｏｌＳＮＳ上への、児童・生徒の本人が特定可能な画像及び動画掲載の原則禁止（※6）

※1法令に定めのある場合を除く。※2テレビ、プロジェクター、実物投影機、パソコン（タブレット端末を含む。）、プリンタ、各教室の情報コンセント、スイッチングハブ、その他校内の全ての機器が対象　※3　校外への持ち出しに当たっては、1使用目的　2内容　3作業場所・方法　4使用期間　5作業後の扱い等について事前に確認した上での許可とする。※4ＩＣボイスレコーダー、デジタル（ビデオ）カメラ、パソコン（タブレット端末を含む。）、メモリーカード、ＵＳＢメモリ、フロッピーディスク、ＣＤ／ＤＶＤ－Ｒ等、データ記録可能なものは全て対象　※5ＩＣボイスレコーダー、デジタル（ビデオ）カメラ、パソコン（タブレット端末を含む。）、スマートフォン、ガラケー、外付けＨＤＤ、ＮＡＳ、プリンタ、無線ルーター、スイッチングハブ、その他学校資産でないものは全て対象　※6保護者が事前に同意した場合を除く。

(2) 私物機器の利用に関する校長の裁量を限定

三鷹市では、三鷹市立学校情報セキュリティ基本方針の策定前は、「校長の許可」があれば

☞校務・授業等における私物機器の利用
☞校内機器への私物機器の接続

について許容してきましたが、三鷹市立学校情報セキュリティ基本方針の策定により、以下の場合のみを例外として、原則（すなわち、校長の許可を得ても）私物機器の利用を禁止することとしました。

☞他地方公共団体から転入してきた教職員が、それまで使用していた教材等のファイルをファイルサーバに保存する場合（任用の初日から一週間以内）
☞校内における外部講師による講演会等で、外部講師が持ち込んだプレゼンテーション資料を使用する場合
☞学校運営協議会委員等が作成した資料を校内のパソコンで修正したり、印刷する場合

ただし、これらの例外についても、ウイルスチェック等の対策を十分に行った上での許可とし、許可の履歴・理由を記録する運用としました。

(3) 学校情報取扱基準一覧の分類の見直し

守るべき情報資産を明確にする学校情報取扱基準一覧の分類についても、三鷹市立学校情報セキュリティ基本方針の策定前は、東京都立学校の分類を基に持ち出しを制限する情報資産を特定し、それら以外は原則持ち出しを可とする考え方でしたが、これを逆に、持ち出しを許可する情報資産を特定し、それら以外の情報資産については、原則として持ち出し不可、との考え方に改めました。（図表 2-25）

表 2-25　基本方針策定前後の比較

基本方針策定前		策定後	
S－1	原則持出禁止（プライバシー性が高い情報並びに指導要録や成績一覧表などは持出禁止）	S－1	法令に定めのある場合を除いて持出禁止
S－2	持出す都度、校長等の承認を得る	S－2	校長、副校長の承認を得た場合を除いて持出禁止
S－3	包括的承認（上記以外は全て可）	S－3	持出可（配布、公開されてもよい校務情報のうち個人情報を含むもの） 学園・学校・学年・学級だより学校行事のしおり、卒業アルバムなど（個人情報についてはS－2の扱い）
		S－4	持出可（配布、公開されてもよい校務情報うち個人情報を含まないもの） 授業用教材、教材研究資料など

また、上記の分類にあてはまる記載がないものについては、管理職に協議・相談をすることとしました。

■三鷹市のＩＳＭＳ規定と教育委員会の規定の違い

三鷹市では、市長部局の情報セキュリティマネジメントは ISMS の規定を遵守した仕組みを策定していますが、学校現場において事務負担の軽減を図りながら、適切に規定を運用・遵守できる仕組みとしました。

図表 2-26　ISMS の規定と三鷹市立学校情報セキュリティ基本方針の違い

	ISMS	三鷹市立学校情報セキュリティ基本方針	違いの理由
情報セキュリティ委員会	設置する	設置しない	学校の負担となるため ただし、問題が生じた際は早急に教育委員会事務局に報告する規定と報告様式を定めた
情報の管理及びリスク評価	実施する	実施しない （リスク評価のみ）	情報管理は規定あり リスク評価は「学校情報取扱基準」によるリスク評価の標準化で対応
業務委託契約	規定あり	規定しない	学校が業務委託契約をすることはないため
内部・外部監査	実施する	実施しない	学校の負担となるため ただし、毎年度運用状況と規定の見直しについて報告を求める
事業継続管理	規定あり	規定しない	ISMS 認証を取得しないため
保険	規定あり	規定しない	ISMS 認証を取得しないため

三鷹市の事例のように「学校の負担にも配慮しつつ情報セキュリティの実質的な維持・向上を図るために、このような基準を策定し、首長部局と連携しつつ教育委員会･学校全体で管理･運用していく」ことが望ましいと考えられます。

2.1.5　学校における情報セキュリティを確保するための体制づくり

情報セキュリティポリシー策定後は、適切な運用ができているか定期的に確認が必要です。どのような体制・役割分担で策定されたものであっても、情報セキュリティポリシーを学校管理者のみが理解していればいいというものではなく、学校に関わる職員全てが理解していなければなりません。そのためには、具体的な事例を盛り込んだ研修会を実施し、理解を深め、学校で取り扱う情報資産の管理状況について定期的に確認をしていくと良いでしょう。

また、万が一事故が発生した際の報告体制についても予め取り決め確認しておくことが重要です。事故が発生してしまった時に責任を問われることを恐れて報告を怠り、二次被害、三次被害が発生することは絶対に避けなければなりません。

情報セキュリティポリシー上で策定したルール通りに運用しても事故が発生してしまった場合、また運用ルールに反して事故が発生した場合のそれぞれに罰則を規定します。

情報セキュリティポリシーで定めたルールに抵触して情報セキュリティ事故が発生した場合を想定し、事故を隠ぺいした場合にはより重度の罰則を適用することと合わせて、速やかに報告し対処を講じた結果大事に至らなかった場合には罰則の適用に柔軟性を持たせることも考慮するなどすることも運用面では検討の価値があります。情報セキュリティポリシーを策定するのは、2.1.3 で解説したように「情報の機密性、完全性、可用性を維持する」ためです。「情報セキュリティ事故につながるかもしれない事象が発生した」等の報告や相談がしやすい体制を作り、そういった運用が行われていることを広く関係者の間で情報共有しておくことも、情報セキュリティポリシーには規定されない項目とはいえ情報セキュリティの確保の観点では非常に有効です。

また、運用面においては常に言われることですが、「計画 (Plan)」→「導入・運用 (Do)」→「点検・評価 (Check)」→「見直し・改善 (Act)」の PDCA サイクルを回していくことが重要です。

◉2.2　情報セキュリティ確保のための具体的対策

2.2.1　個人情報の保護

■個人情報とは

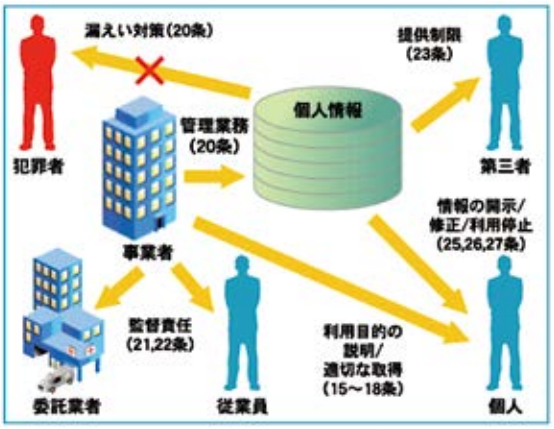
学校が管理する情報資産の中でも、個人情報の取り扱いは注意が必要です。個人情報は、国や地方公共団体、事業者などが扱う各種の情報のうち、生存する個人の情報で、特定の個人を識別できる情報を指します。個人情報保護法では、

> 第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

と規定されています。

地方公共団体については、個人情報保護法に準じた個人情報保護条例が制定され、個人情報の対象、個人情報取得のルール、個人情報保管・管理のルール、個人情報の第三者への提供のルール、などが規定されています。地方公共団体が設置者となる公立学校においても、当然に個人情報の保護に努めなくてはなりません。（図表 2-26）

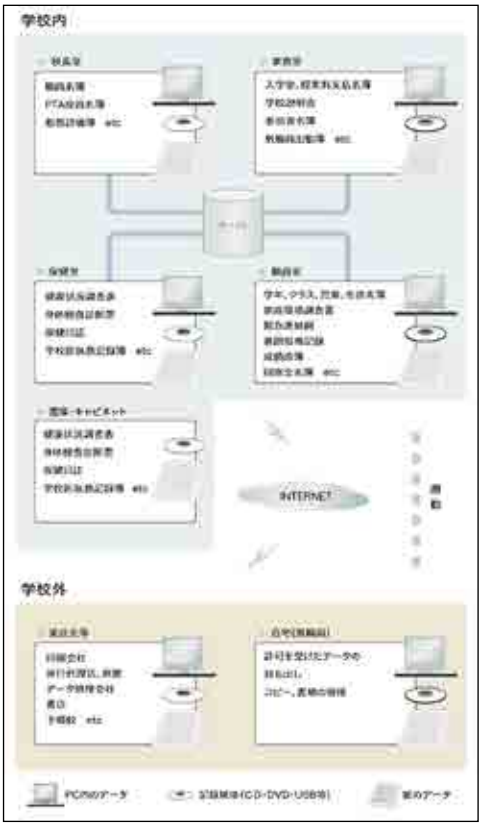
図表 2-26　個人情報保護に関する事業者の義務（個人情報保護法の場合）



資料出所：https://thinkit.co.jp/free/compare/7/1/

学校においては、個人情報保護法が「基本情報」と定める「氏名」「住所」「性別」「生年月日」といった情報はもちろん、「電話番号」や「メールアドレス」といったプライバシー情報や、「成績」「家庭環境」「病歴」などといった、他人に知られたくない機微情報（センシティブ情報）もあります。学習だけでなく、健康診断等の保険業務、同窓会やＰＴＡとの関連などから情報収集されているため、学校には実にさまざまな個人情報や機微情報があふれていることが分かります。（図表 2-27）

図表 2-27　学校における個人情報の例



資料出所：https://thinkit.co.jp/free/compare/7/1/

さらに、平成 28 年から利用が開始された「個人番号（マイナンバー）制度」により、個人情報の扱いが変わってきます。個人情報にマイナンバーが含まれると、単なる個人情報ではなく、「特定個人情報」と位置付けられます。特定個人情報も個人情報の一種といえますが、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）が適用されます。さらに特定個人情報は、マイナンバーによって名寄せが行われるリスクがあることから、個人情報保護法よりも厳しい保護措置が法律で課されています。個人情報は本人が同意すれば第三者に提供することが可能ですが、特定個人情報には利用制限や提供制限があり、本人が同意したとしても原則として、利用範囲を超えて利用することはできません。

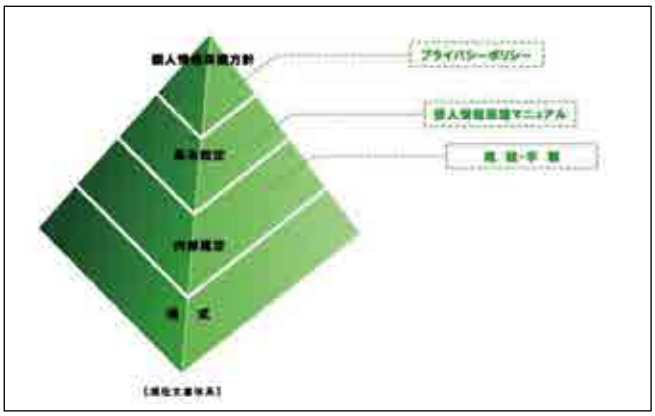
学校においても、給与に関する業務を実施する事務職員はもとより、教職員でも就学援助等の手続きに関わるなど、マイナンバーを取り扱うことがあります。その際、極めて厳重な運用が求められることを認識しておく必要があります。

■個人情報の保護

仮に、これらの個人情報報が漏えいしてしまうと、児童生徒や教職員の個人情報が DM やセールス電話などの商品販売に利用されるのみならず、架空請求や詐欺行為といった犯罪に利用される可能性もあります。特に、デジタル化されたデータは容易に大量のコピーができ、一度流出すれば、情報の回収は不可能といえます。また、情報同士を照合することによって個人の行動履歴や居所なども割り出せるほど多様な情報が流通するようになりました。

個人情報に関しては内容の重要性を考えると、確実で慎重な取り扱いが必要です。にもかかわらず、2.1で示したように、平成27年度だけでも、学校での個人情報漏えい事故が166件発生し、約34万人分の個人情報が漏えいしてしまっているのです。個人情報を保護するためには、個人情報保護方針を定め、その方針のもとで、個人情報保護のためのルールやマニュアルを定め、運用する必要があります。（図表2-28）

図表2-28　個人情報保護規定のイメージ



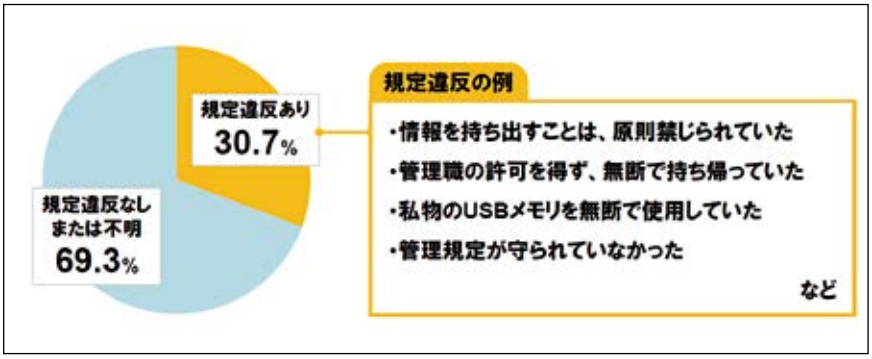
資料出所：http://www.secom-sanin.co.jp/sec_manual/

個人情報を含む情報の台帳を整備し、それぞれの情報の収集・保管・利用・破棄などに関する規程を定め運用するとともに、情報を取り扱うＩＣＴ機器の利用ルールなども定め、厳格に運用する必要があります。

ところが、ルールを遵守しないがゆえのセキュリティ事故が多数発生しているのも事実です。

学校における監査や教職員等に対する教育を徹底することによって、個人情報保護のためのルールを厳格に運用することが重要であることは言うまでもありません。しかし、情報セキュリティは、常に利便性とトレードオフの関係にあります。情報セキュリティを追求するあまり、日常業務に支障をきたすようになると、ルール違反の行為が陰に陽に行われるようになり、却ってセキュリティレベルを下げる結果に陥りがちであることに留意しましょう。（図表2-29）

図表2-29　規定違反を伴う事故の発生比率



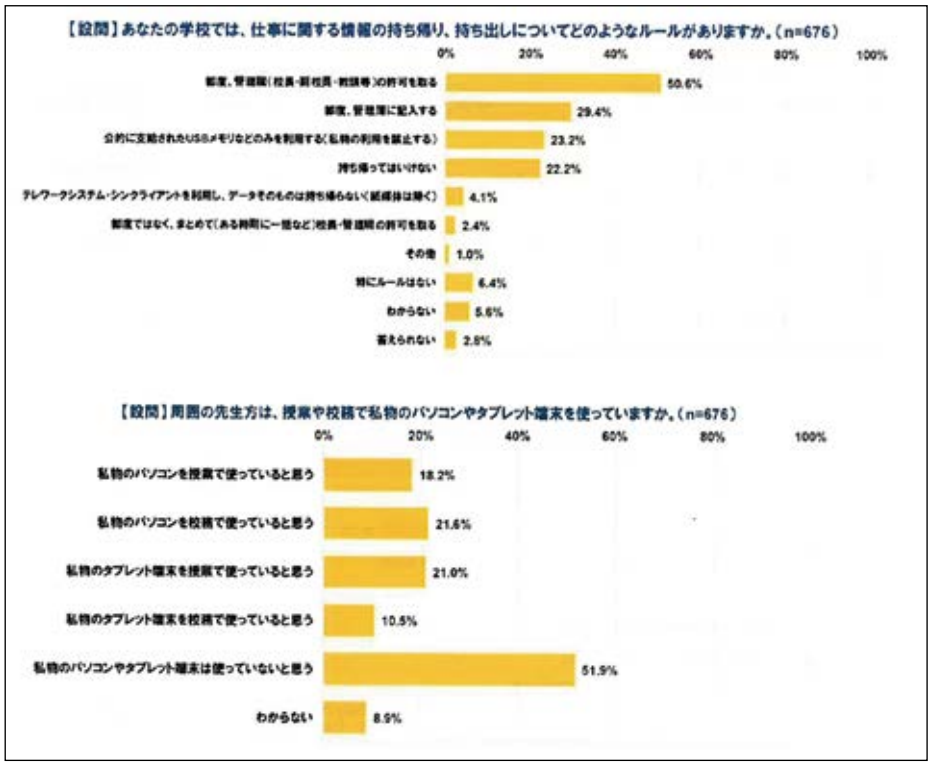
資料出所：ISEN「平成27年度学校・教育機関における個人情報漏えい事故の発生状況調査報告書第2版」

2.2.2　情報セキュリティを確保する学校文化づくり

情報セキュリティ対策においては、ネットワークやシステムによって対策を講じる「技術的」なセキュリティ、部屋やキャビネットなどを利用して対策を講じる「物理的」なセキュリティ、などといった環境面からのアプローチがあります。しかし、いかにセキュアな環境を構築しようとも、当事者による運用がずさんでは脅威を防ぐことは難しいと言えます。「情報セキュリティポリシー」の策定・運用、情報セキュリティマネジメントシステムの導入・運用、監査、教育など、人的なセキュリティ面での検討、対策が伴ってこそ、他のセキュリティ対策が有効となるのです。

人的セキュリティ対策が効果をあげるか否かは、最終的には関係者（教職員や子供）の意識に依拠することになります。たとえば、情報を扱うＩＣＴ機器や取り扱いについて一定のルールを定めている学校は多いものの、実際には私物のＩＣＴ機器を校務や授業で利用している教員もかなりの比率にのぼることが図表2-30のアンケート結果から推察されます。

図表 2-30　情報の取り扱いルール、私物ＩＣＴ機器の利用状況



資料出所：ＩＳＥＮ「平成 27 年度情報セキュリティに対する教職員の意識調査報告書第 2 版」

このようなルールの不徹底が、学校において発生している事故の約８割を占める、「紛失・置き忘れ」や「盗難」につながっていると言っても過言ではないでしょう。(図表 2-31)

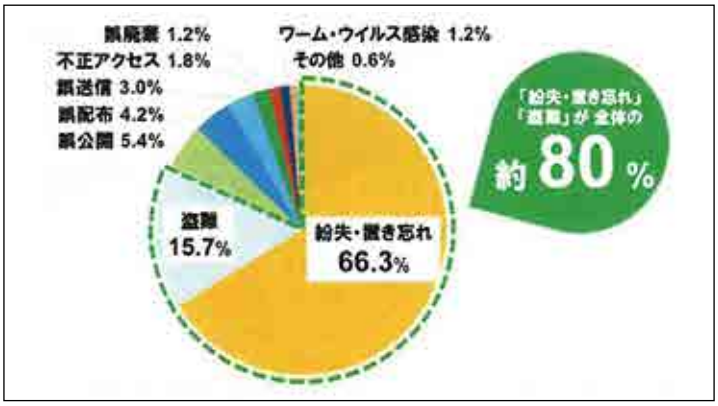
情報セキュリティ対策においては、ポリシー、規程や手順書などのルールを策定することと同じくらい、それらのルールに則り、教職員や子供への教育や情報・意識の共有を進めていくことが重要と言えます。

このような情報セキュリティ意識は学校管理職が間断なく教職員や子供にその重要性を問いかけ、情報セキュリティ確保に必要な手順やルールの遵守については、手間であってもゆるがせにしないと示していくことを通じて、学校文化として定着していきます。

2.1.2 に示した佐賀県の情報セキュリティ事故に関しても、佐賀県学校教育ネットワークセキュリティ対策検討委員会から、「数年で人事異動を伴う組織の場合、組織体制を構築しても、その後の実効性が失われがちである。そのためにも「セキュリティ文化」とも言うべき体制の構築が必要。
県教育委員会、県議会や既設の検討委員会等で、普段からセキュリティについて論議を続け、深めることが必要。
それが本提言の実効性の担保にもつながる。

また、本事案を機に学校現場や生徒、県民からも広く意見を聴く場を設け、セキュリティのみならず教育の質的向上や利用者の利便性向上、校務の効率化という本来のミッションについても情報を共有・交換し、県教育委員会自らが考え、改革していく姿勢を示すことで、保護者や生徒、県民の不安を払拭し、信頼回復につながるものと考える。」
との提言がなされています。学校や教育委員会がその特性を踏まえた情報セキュリティを考えていくに当たって、大変重要な指摘と言えます。

図表 2-31　情報の取り扱いルール、私物ＩＣＴ機器の利用状況



資料出所：ISEN「平成 27 年度学校・教育機関における個人情報漏えい事故の発生状況調査報告書第 2 版」

2.2.3　教育情報セキュリティのための緊急提言

大規模なセキュリティ事故が発生したことを受けて、文部科学省は平成 28 年 8 月、「教育情報セキュリティのための緊急提言」を全国の教育委員会等へ周知しました。

緊急提言の内容及び、仮に緊急提言に即した対応を行わないことによって想定される脅威は以下のとおりです。

図表 2-32　教育情報セキュリティのための緊急提言

緊急提言内容	対策しないことによる脅威
1．情報セキュリティを確保するため、校務系システムと学習系システムは論理的または物理的に分離し、児童生徒側から校務用データが見えないようにすることを徹底すること。	・児童生徒が校務用データにアクセスできることにより、児童生徒から情報が流出
2．児童生徒が利用することが前提をされている学習系システムには、個人情報を含む情報の格納は原則禁止とし、個人情報をやむを得ず格納する場合には、暗号化等の保護措置を講じること。	・児童生徒が学習系システムより個人情報を入手し、情報を流出（意図しないものも含む）
3．各学校において情報セキュリティの専門家を配置することが困難な現状を踏まえれば、重要な個人情報を扱う校務系システムは、教育委員会が管理もしくは委託するセキュリティ要件を満たしたデータセンター（クラウド利用を含む）で一元的に管理すること。	・学校設置サーバへ蔵置した重要データ（個人情報、 システム管理者情報等）の情報漏えい ・専門職のいない学校の教職員がサーバを管理するセキュリティリスク
4．校務系ならびに学習系システムにおいても、教職員や児童生徒の負担増にならないように配慮しつつ、二要素認証の導入など認証の強化を図ること。	・教職員等のパスワード流出を起因とした権限のない者の機微情報不正アクセス
5．セキュリティチェックの徹底の観点から、システム構築時及び定期的な監査を実施すること。	・システム的な脆弱性からの情報漏えい
6．セキュリティポリシーについて、実効的な内容及び運用となっているか検証を行うこと。その際、アクセスログの６か月以上保存、デフォルトパスワードの変更等について確認すること。	・セキュリティーポリシーの実効的な運用がされないことまたは陳腐化よるセキュリティリスク高 ・インシデント発生時に不正操作、 不正アクセスの証跡を追跡できない ・パスワードの漏えいによる不正アクセス
7．教職員の情報セキュリティ意識の向上を図るため、全学校・全教職員に対する実践的な研修を実施すること。	・セキュリティ意識の希薄を原因とした情報漏えい（USB メモリによる情報持ち出し、標的型メールからの情報漏えい 等）
8．情報セキュリティの強化の観点から、教育委員会 事務局への情報システムを専門とする課・係の設 や首長部局の情報システム担当との連携強化等 教育委員会事務局の体制を強化すること。	・セキュリティの担当者が決まっていないことによる情報セキィリティポリシーの実効性の低下

緊急提言の内容を踏まえた対応策の詳細に関しては、以下の項を参照してください。

1．校務系システムと学習系（授業支援系）システムは論理的または物理的に分離し児童生徒から校務用データが見えないようにすることを徹底すること。

校務系ネットワークと学習系ネットワークを分離して構築・運用するためには、「物理的分離」と「論理的分離」の２つの方法があります。「物理的分離」とは、校務系ネットワークと学習系ネットワークをまったく別のネットワークとして構築・運用する考え方です。学校の中に、校務系ネットワークである校内ＬＡＮと、学習系ネットワークである校内ＬＡＮという２つの校内ＬＡＮを構築し、両方のネットワークに接続する機器等を設置せずに運用します。物理的に分離することで、学習系システムの利用者である子供は、校務系システム内の情報にアクセスすることができません。また、ネットワーク分離の手法として、「物理的分離」ではなく「論理的分離」という方法が採られることがあります。校務系システムと学習系システムを同一の物理ネットワーク内に構築するものの、ルータ等のネットワーク機器によって、別々のネットワークとして運用し、相互間の通信を制御することができます。道路上に車線変更禁止のレーンがあり、一つのレーンにいる車は別のレーンと違う目的地に行く状況をイメージしてください。また、1 台の機器をあたかも複数台の

機器であるかのように運用する仮想化と呼ばれる技術を用いる論理的分離の方法もあります。詳細は 1.3.2「学校におけるネットワークの構成」を参照。

2．学習系（授業支援系）システムには、個人情報を含む情報の格納は原則禁止とし、個人情報をやむを得ず格納する場合には、暗号化等の保護措置を講じること。

地方公共団体については、個人情報保護法に準じた個人情報保護条例が制定され、個人情報の対象、個人情報取得のルール、個人情報保管・管理のルール、個人情報の第三者への提供のルール、などが規定されています。地方公共団体が設置者となる公立学校においても、当然に個人情報の保護に努めなくてはなりません。詳細は 2.2.1「個人情報の保護」、2.1.2「学校における情報セキュリティ事故の状況」を参照）なお、個人情報をやむを得ず格納する場合には、暗号化等の保護措置が必要です。ファイルの守秘：標的型攻撃により、クライアント PC がマルウェアなどに感染し、個人情報などの機密情報が含まれる電子ファイルが外部に流出したとしても、ファイルを暗号化していれば、攻撃者は中身の閲覧ができないため、情報漏えいを防止できます。詳細は 2.4.4「守秘のための対策」を参照。

3．校務系システムは教育委員会が管理もしくは委託するセキュリティ要件を満たしたデータセンター（クラウド利用を含む）で一元的に管理すること。

安全性や保守運用面を考慮すると、サーバ類は学校内よりもクラウドやセンターに設置する方が望ましいといえます。特に学校数が多い場合、教育委員会はクラウドもしくはセンターにサーバ類を設置することによって、一元的・効率的な管理・運用が可能となり、学校ごとに安全対策を講じたり、メンテナンス対応を実施したりする等の管理負担を低減することができます。詳細は 1.3.1「学校におけるネットワーク　■ネットワークの分類」を参照。

4．二要素認証の導入など認証の強化を図ること。

認証の要素は、大きく「記憶」「所持」「生体情報」の 3 つに分けられます。「記憶」とは、本人のみが記憶しているデータに基づいて利用者を認証する方式で、暗証番号やパスワードがあります。「所持」とは、本人のみが所持している物によって利用者を認証する方式で、職員証や IC カードがあります。「生体情報」とは、本人の生体に基づくデータにより利用者を認証する方式で、指紋・静脈や顔認証などがあります。これらの認証要素のうち、種類の異なる 2 つの要素を組み合わせて認証する方式が、二要素認証です。一つの要素のみで認証する方式に比べセキュリティ強度が高まるため、なりすまし等の第三者による不正アクセスを防ぐことができます。詳細は 2.4.2「なりすまし対策のための利用者の認証」を参照。

5．システム構築時及び定期的な監査を実施すること。

システムの構築時の監査は、技術面と物理面の脆弱性を指摘するために必ず行い、不備があれば是正を講じます。情報セキュリティ対策では、ネットワークやシステムによって対策を講じる「技術的」なセキュリティ、部屋やキャビネットなどを利用して対策を講じる「物理的」なセキュリティ、など環境面からのアプローチがあります、これらは定期的な監査において、技術的対策、物理的対策も含めて、総合的に行う必要があります。しかし、いかにセキュアな環境を構築しようとも、当事者による運用がずさんでは脅威を防ぐことは難しいと言えます。「情報セキュリティポリシー」の策定・運用、情報セキュリティマネジメントシステムの導入・運用、監査、教育など、人的なセキュリティ面での検討、対策が伴ってこそ、他のセキュリティ対策が有効となるのです。詳細は 2.1.4 「学校における情報セキュリティポリシー　■情報セキュリティポリシーの教育、改善」2.2.2「情報セキュリティを確保する学校文化づくり」を参照。

6．セキュリティポリシーについて、実効的な内容及び運用となっているか検証を行うこと。

情報セキュリティ確保のため基本文書が、情報セキュリティポリシーです。情報セキュリティポリシーは、「基本方針」、「対策基準」、「実施手順書」から構成されます。学校において情報資産を取り扱うＩＣＴ環境は、所管の教育委員会が主体となって整備及び運用することが大半を占めており、学校情報及び児童生徒に関する情報の管理においても教育委員会が一定の責任を担うこととなります。したがって、学校独自で情報セキュリティポリシーを策定するのではなく、所管の教育委員会が統一的な情報セキュリティポリシーのひな形、「基本方針」と「対策基準」を示し、その内容について学校現場での理解を図りながら「実施手順」のひな形を策定するなど、教育委員会を中心とした学校現場の情報セキュリティ確保が望まれます。なお、基本方針と対策基準はセットで策定されるものですので、他の地方公共団体や学校の事例等を参考とすることができるでしょう。「実施手順書」は対策基準を実行するために、教職員の作業手順を具体的に示したマニュアルに相当するものです。たとえば、システムにログインするためのパスワードの管理や、字種や桁数、更新頻度などを定め、具体的に何をどのように実施するのかを明確にします。その内容に基づいて学校側の「実施手順書」

を策定していくことが求められます。情報セキュリティポリシーの策定は、教育委員会が主導するケースもあれば、学校が策定するケースもありますが、やはり専門的知識のあるスタッフがチームを組織して策定する体制が望まれます。詳細は 2.1.4「学校における情報セキュリティポリシー　■情報セキュリティポリシーの運用」を参照のうえ 2.5.3「情報セキュリティチェックシート（ネットワーク管理者編）」を用いて点検してください。

7．全学校・全教職員に対する実践的な研修を実施すること。

教育委員会では情報セキュリティに関する研修プログラムを策定し、所管する全学校に対して実践的な研修会を行います。研修会では、情報セキュリティポリシーの各条項がなぜ必要かを説明するとともに、対策基準および実施手順書を使って、具体的な操作を含む研修会を実施すると良いでしょう。なお、各学校の学校長は、研修会に参加するよう働き掛けるとともに、研修会に参加した教職員は学校での校内研修等の機会を活用して「全教職員」を対象に伝達研修を行います。詳細は 2.1.4 「学校における情報セキュリティポリシー　■情報セキュリティポリシーの教育、改善」、2.1.5「学校における情報セキュリティを確保するための体制づくり」を参照のうえ 2.5.3「情報セキュリティチェックシート（教育委員会システム担当者編）」を用いて点検してください。

8．教育委員会事務局への情報システムを専門とする課・係の設置や首長部局の情報システム担当との連携強化等、教育委員会の体制を強化すること。

教育委員会事務局の中に情報システムを担う部門（課・係）を設置し、その部門の担当者は教育委員会内の各部署のセキュリティに対して組織横断的に取り組めるようにしましょう。また、専門的な知識や最新動向の情報収集・補完、地方公共団体のＩＣＴコスト最適化等も考慮し、首長部局の情報システム担当とも連携強化を図ることを重視しましょう。詳細は 1.2.3「ＩＣＴ環境の整備　■推進組織の確立、■導入促進への体制、関係者の理解、2.1.5　学校における情報セキュリティを確保するための体制づくり」を参照。

A 市では緊急提言の 8 つの項目への対応を行いました。

平成 27 年 11 月に総務省から発出された「新たな地方公共団体情報セキュリティ対策の抜本的強化に向けて」を踏まえ、既にインターネット接続系統は強靭化対策を講じておりましたが、これに加え、以下の 8 つの対策を図っています。（図表 2-33）

図表 2-33　A 市における緊急提言を踏まえた対応

提言内容	導入された対策
校務系システムと学習系システムの論理的又は物理的に分離する	・ルータやスイッチによる論理分割。 ・アクセス制御設定の再確認、再設定。
学習系システムへの個人情報の格納禁止 ※やむを得ない場合は暗号化	・運用ルールの徹底 ・ファイルサーバ暗号化システムの導入
校務系システムは教育委員会が管理か、セキュリティ要件を満たしたデータセンターでの一元管理	・校務サーバの教育センターへの集約
二要素認証の導入などの認証の強化	・USBトークンを使った二要素認証の導入
システム構築時および定期的な監査の実施	
セキュリティポリシーが実行的な内容、運用か検証する	・セキュリティポリシーの見直し ⇒アクセスログの保管、外部デバイス、パスワード運用等
全学校、全教職員に対する実践的な研修の実施	・情報セキュリティ研修の実施
専門の課や係を設置、首長部局との連携を行う等、教育委員会事務局の体制強化	・調達時、設計時における情報政策課の関与・承認

具体的には、校務系システムと学習系システムを論理的に分離したほか、校務系サーバを教育センターへ集約し、改めてアクセス制御の再確認、再設定を行いました。また、個人情報の格納ルールを徹底し、ファイルサーバの暗号化システムも新たに導入しています。ユーザ認証についても、パソコンの USB ポートに接続して使う小型の認証装置（USB トークン）の導入を行い、従前からの ID・パスワード運用に加えることでセキュリティを更に強化しています。

これらは極めて大きなセキュリティ改革であり、情報セキュリティポリシーの改定や設計時における情報政策課の関与・承認を必要とする等、全市一丸となった対策を図るとともに、セキュリティ研修の徹底を通じ現場に状況を周知しています。

このように、情報セキュリティ確保のためには利用者・管理者といった関係者に対する教育の徹底や、監査に

ついても充実が求められます。しかしながら、これらに膨大な時間や人手を取られてしまうようでは、ＩＣＴの導入目的に照らして、本末転倒とも言え、可能な限りシステムでの対応を試みる事例も現れています。

Ｂ区では、IT 資産管理システムを導入し、「ハード・ソフト情報収集」、「資産台帳作成」、「セキュリティパッチ適用」、「非管理ＰＣ検知」、「記憶媒体・デバイス制御」、「電源管理」、「ソフトウェア起動制御」、「ＰＣ操作ログの取得」等の機能を実現しています（図表 2-34）。これらの機能は、「教育情報セキュリティのための緊急提言」の中の、「システム構築時及び定期的な監査の実施」や、「情報セキュリティポリシーが実行的な内容、運用か検証する」ことに関連します。

Ｂ区では膨大な数の端末が導入されており、「定期的な監査」を行うだけでも大きなコストと手間がかかります。また、情報漏えいの多くはセキュリティパッチが適用されていない端末の脆弱性を利用した攻撃から始まります。定期的に端末状況を確認し、確実にパッチを適用することがシステム全体の安全性を高めるために極めて重要となります。

図表 2-34　Ｂ区での IT 資産管理システム概念図

多くの教育現場で課題であるＵＳＢメモリー等のリムーバブルメディアの管理についても、情報セキュリティポリシーに照らし合わせて一元管理することが可能となりました。同システムの「記憶媒体・デバイス制御」機能を用い、情報セキュリティポリシーの最適な運用をシステム上で担保しています。

◉2.3　情報セキュリティ事故が発生してしまったら

2.3.1　情報セキュリティ事故の発生後の対応

■情報セキュリティ事故と事故対応

情報セキュリティ事故は「重要な情報を守れなかった結果の事象」と言え、次のような事象が考えられます。
①重要な情報を決められた以外の人が利用した (⇒重要な情報が漏えいした／機密性)
②重要な情報の完全さ正確さを保護できなかった (⇒重要な情報が改ざんされた／完全性)
③重要な情報が必要な時使えなかった (⇒重要な情報 (システム) が利用できなくなった／可用性)

情報資産に内在する脆弱性が、情報資産を取り巻くさまざまな脅威に突かれ、顕在化したものが情報セキュリティ事故と位置づけられます。(図表 2-35)

図表 2-35　情報資産・脅威・脆弱性とセキュリティ事故の関係

資料出所：情報セキュリティ大学院大学「情報セキュリティ事故対応ガイドブック」

事故内容によって、取るべき事故対応は異なってきます。また、事故の要因により対応内容も変わってくる場合がありますが、一般的に事故のフェーズは図表 2-36 のようになります。

図表 2-36　情報セキュリティ事故対応の実施フェーズ

資料出所：情報セキュリティ大学院大学「情報セキュリティ事故対応ガイドブック」

①検知：人やさまざまな仕組みにより、事故の発生を検知する。
②初期対応：問題の切り分けや被害拡大の防止、犯罪行為時の証拠保全など、まず始めに実施すべき対応を行う。
（例）事実確認・調査、ログなどの記録の保全（調査や分析、連絡などに必要)、
ネットワーク接続やシステムの遮断・停止、
影響範囲の特定、関連者への連絡、謝罪、情報提供、
情報セキュリティ事故の事実の公表（公表の是非を含めて検討。公表する範囲に注意)、アクセス元などへの通知連絡
③回復：事故を復旧し、元の状況に戻すための対応を行う。
④事後対応：事故の原因・経緯等から、今後同じようなことが起きないような対策について検討、実施する。
（例）要因の特定（脆弱性・運用体制)、システムの復旧、再発防止策の検討・実施、
作業結果の報告、作業の評価、
情報セキュリティポリシー・運用手順の見直し

2.3.2　情報セキュリティ事故の発生に備える

■事故対応者

2.3.1 の事故対応を行うための前提条件として、フェーズゼロとも言うべき事前準備が必要となります。

具体的には、「情報セキュリティポリシーや実施手順書の準備」「作業記録（対応時刻・対応者・対応内容をまとめたもの）の作成」「責任者・担当者への連絡体制、情報セキュリティ事故対応担当者への連絡体制を整備」などです。

体制整備としては、下記のように、事故対応に実務的に対応する人、これを組織として大局的に判断・指揮する人が必要になります。

① 管理者：情報セキュリティ事故に対する大局的な判断や指揮を行い、情報セキュリティ事故対応全体を統括する。学校においては、校長などの管理職を想定。
② 窓口・実務担当：情報セキュリティ事故報告の受け付け、情報セキュリティ事故原因や重要性の切り分け、回復作業・事故対応実務を担う。学校においては、ＩＣＴ担当の教職員を想定。
③ 組織員：業務に従事している組織員であり、情報セキュリティ事故の検知の役割を担う。学校においては、教職員を想定。
④ その他：サービス提供相手（学校においては子供や保護者など）、保守委託業者、システムベンダ、警察など、状況によって異なる。

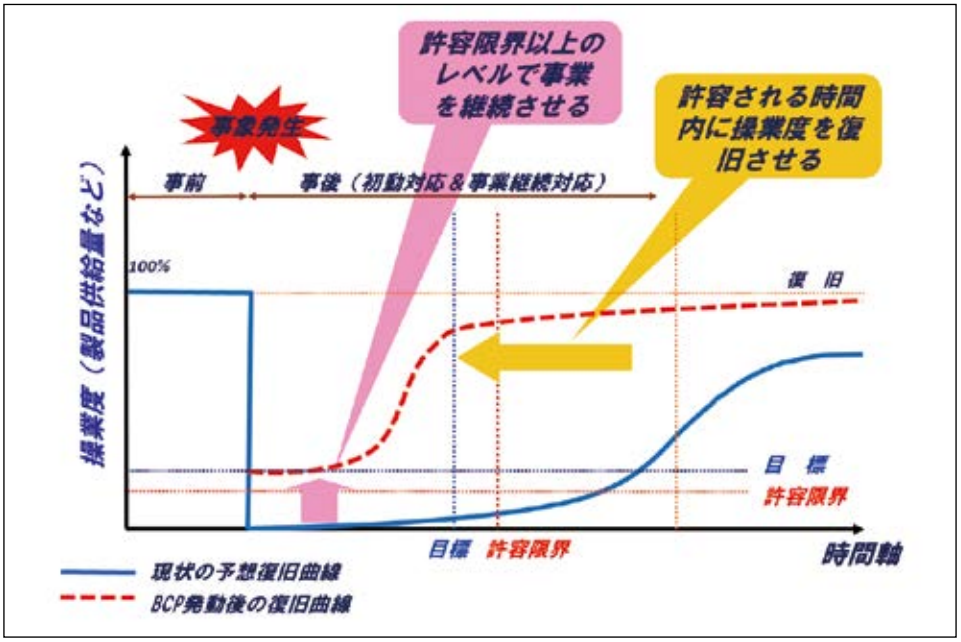
また、情報セキュリティ事故への対応には専門的な知識が必要なことも多く、教育委員会でも適任者が常時いるわけではありません。教育委員会内部での連絡・情報共有に加えて、情報政策部局との連絡体制も明確にしておくべきです。

■ BCP（Business Continuity Plan：事業継続計画）

事故対応は、情報セキュリティ事故そのものを復旧することに主眼が置かれていますが、大きな情報セキュリティ事故では、業務そのものが停止してしまうことすら想定されます。

BCP（Business Continuity Plan：事業継続計画）では、情報セキュリティ事故のみならず、地震・火災・システム障害などの原因によって業務が継続できなくなったときに、最低限の事業継続や、短時間での復旧をどのように図るかを計画するものです。計画を立てておかない場合、あらゆる業務が停止してしまったり、業務再開までに時間を要したりすることがありますので、必ず災害や情報セキュリティ事故の備えとして検討、策定しておくべきです。（図表 2-37）

図表 2-37　BCP のイメージ



資料出所：内閣府　事業継続のガイドライン第三版　ーあらゆる危機的事象を乗り越えるための戦略と対応ー

◉2.4　情報ネットワークを守る認証技術と情報セキュリティシステム技術

2.4.1　ネットワーク攻撃と対策の概要

教育委員会及び学校が接続する地域の教育ネットワークにおいて、まず検討すべきことは「校務系と学習系のネットワークを（物理的もしくは論理的に）分離することです。（1.3.2 参照）　しかしそれだけでは情報セキュリティの脅威を防ぎきることはできません。

■巧妙化する攻撃

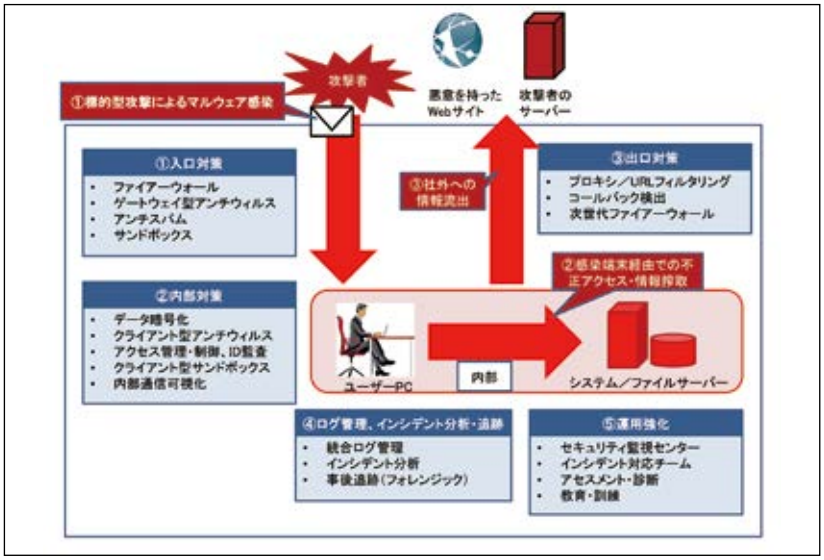
ネットワークやインターネットを通じて、組織の IT インフラを脅かすサイバー攻撃は、年々増加傾向にあり、特に最近では、特定の業種や企業を狙って、執拗に攻撃を行う「標的型攻撃」による被害が拡大しています。

標的型攻撃は、攻撃対象の組織に対し、あたかも自組織に関係する組織・団体からのメールのように偽装した上で、正規の文書ファイルに偽装したファイルを受信者に開かせることにより、利用者に気付かれることなく利用者のＰＣ上にマルウェアを展開して攻撃を開始します。1 台のＰＣが侵害されると、その組織の同じサブネットワークにある他のＰＣが次々と侵害され、更に管理者アカウント情報が盗まれると、機密情報やさまざまな重要データが盗まれる可能性があります。

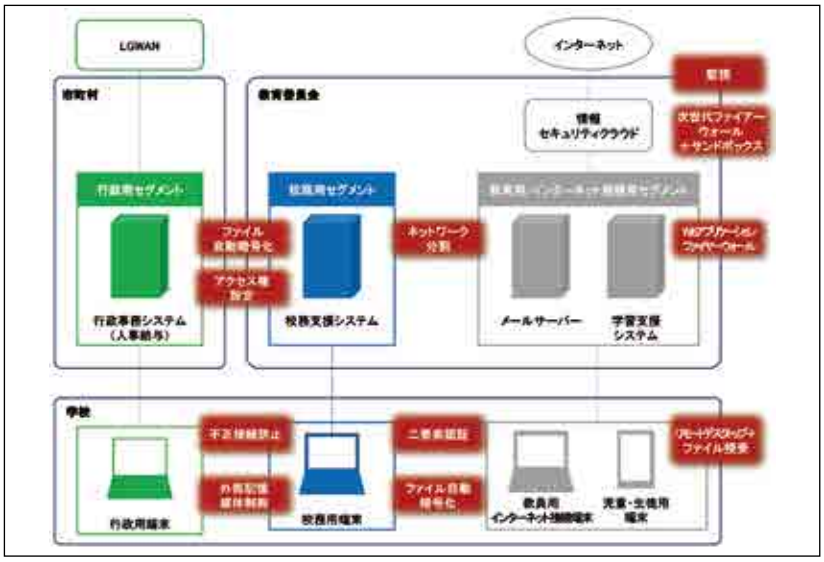
■多層防御による対策

標的型攻撃は日を追うごとに巧妙化し、従来の対策では防ぐことが難しくなっているだけでなく、標的型攻撃を目的とした防御策であっても、単一の対策では防ぎきれないケースが増えています。このため、最近では、インターネット接続のファイアウォールや、内部ネットワーク、サーバ、ＰＣなど、各ポイントで個々の対策を行い、全体として標的型攻撃から IT インフラを守る「多層防御」の考え方が推奨されています。また、対策ソリューション・製品の導入だけでなく、攻撃を早期に検知し、被害を最小限に抑えるための運用業務や、緊急時の対応手順・体制の整備、平常時からの利用者教育など、システムと運用、体制、教育・訓練の各メニューが相互に連携し、解決に導ける仕組み作りが必要です。
（図表 2-38、図表 2-39）

図表 2-38　標的型攻撃における多層防御モデル例



図表 2-39　校務系システムにおける多層防御モデル例



2.4.2　なりすまし対策のための利用者の認証

■認証の種類

認証の要素は、大きく「記憶」「所持」「生体情報」の３つに分けられます。

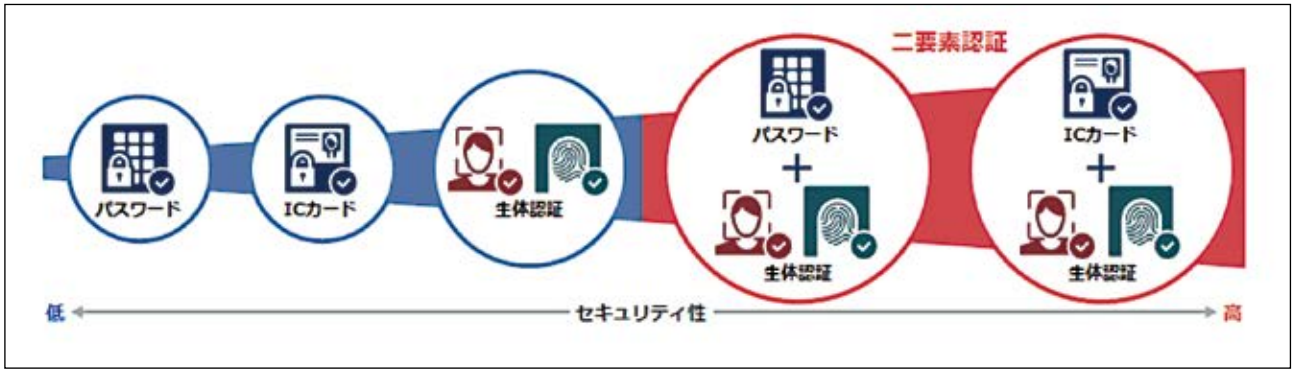
「記憶」とは、本人のみが記憶しているデータに基づいて利用者を認証する方式で、暗証番号やパスワードがあります。忘失・類推・使い回し等のリスクがあり、運用上も、定期的に変更が必要で手間がかかる、複雑なものをいくつも覚えられないなどの課題があります。

「所持」とは、本人のみが所持している物によって利用者を認証する方式で、職員証やICカードがあります。紛失・盗難・偽造等のリスクがあり、必要数を携行しなければならず面倒であったり、カード発行や機器にコストがかかったりします。

「生体情報」とは、本人の生体に基づくデータにより利用者を認証する方式で、指紋・静脈や顔認証などがあります。その人にしかない固有の特徴を用いるため、紛失・盗難・偽造といったリスクが少なく、なりすましが極めて困難であり、より確度の高い本人認証が可能です。

これらの認証要素のうち、種類の異なる２つの要素を組み合わせて認証する方式が、二要素認証です。一つの要素のみで認証する方式に比べセキュリティ強度が高まるため、なりすまし等の第三者による不正アクセスを防ぐことができます。（図表 2-40）

図表 2-40　認証方式とセキュリティ性



2.4.3　電子メールの送信者認証によるなりすまし対策

■電子メールのなりすまし対策

インターネットで使われる電子メールは、送信元メールアドレスを自由に設定できます。そのため、偽の送信元メールアドレスが設定されている、いわゆる「なりすましメール」が多くあります。「なりすましメール」は、標的型攻撃メールや迷惑メールの中で多く使われるため、いかにして「なりすましメール」を減らしていくかが、課題となっています。

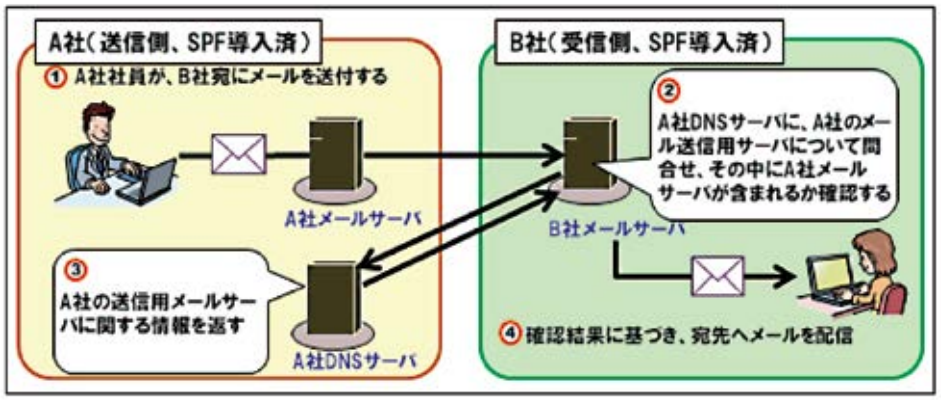
「なりすましメール」をなくすためには、メールの送信側と受信側の連携が必要です。まず送信側は、正しく送信するメールがどのようなものか、情報を提供することが必要です。これができて初めて、受信側は、受信したメールが「なりすましメール」なのかどうかを判別することができ、排除することが可能になります。
このように送信側と受信側が連携するための方式の 1 つが、SPF（Sender Policy Framework）です。

この SPF を送信側・受信側の両方に導入している場合は、受信側で SPF による確認が取れるため、受信側は、安心してメールを受信できます。「なりすましメール」があった場合でも、受信側の SPF で「なりすましメール」だと判断できるため、排除することが可能となります。

送信側の SPF が未導入の場合、受信側は「なりすましメール」かどうかの区別ができないため、全体として機能せず、攻撃者からの「なりすましメール」をブロックできません。

このため、電子メールを導入する組織は、受信側への気配りとして送信側での SPF を導入することを推奨します。しかしながら、SPF には運用上の注意点もあり、特にメールの転送時に問題を生じやすいことが知られております。SPF を導入する際は、このような注意点も考慮する必要があります。（図表 2-41）

図表 2-41　送信側・受信側とも SPF 対応済の場合



資料出所：独立行政法人情報処理推進機構 (IPA)「なりすましメール撲滅に向けた SPF 導入の手引き」

2.4.4　守秘のための対策

■ハードディスクの守秘

「紛失・置き忘れ」「盗難」が原因の情報漏えい事故で、漏えい媒体が電子データであれば、ハードディスク暗号化が大きな効果を発揮します。最新のOSを搭載したパソコンやタブレットスマートフォン、内蔵するハードディスクを自動的に暗号化して利用する機能が搭載されていたりします。これらの機能を利用することで、ディスク（メモリー）の抜き取りによる情報漏えいは防ぐことができます。

■ Web アクセスの守秘

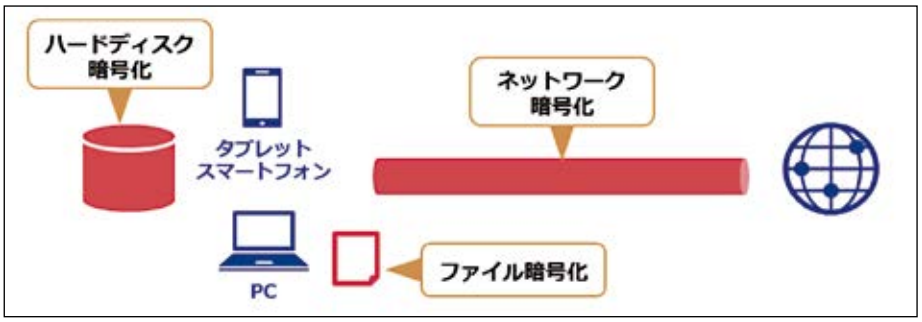
個人情報などの重要なデータを暗号化してサーバ～ PC 間での通信を安全に行なうため SSL（Secure Sockets Layer）と TLS（Transport Layer Security）は、いずれもインターネット上でデータを暗号化して送受信する仕組みを利用します。

SSL/TLS によって、サイトの運営者を装ったサイトが個人情報などの情報を取得し悪用されるリスク（なりすまし）、メールアドレスや住所などの情報を収集し悪用されるリスク（盗聴）、登録内容などが第三者により変更されるリスク（改ざん）の３つのリスクを防ぐことができます。

■総合的な対策

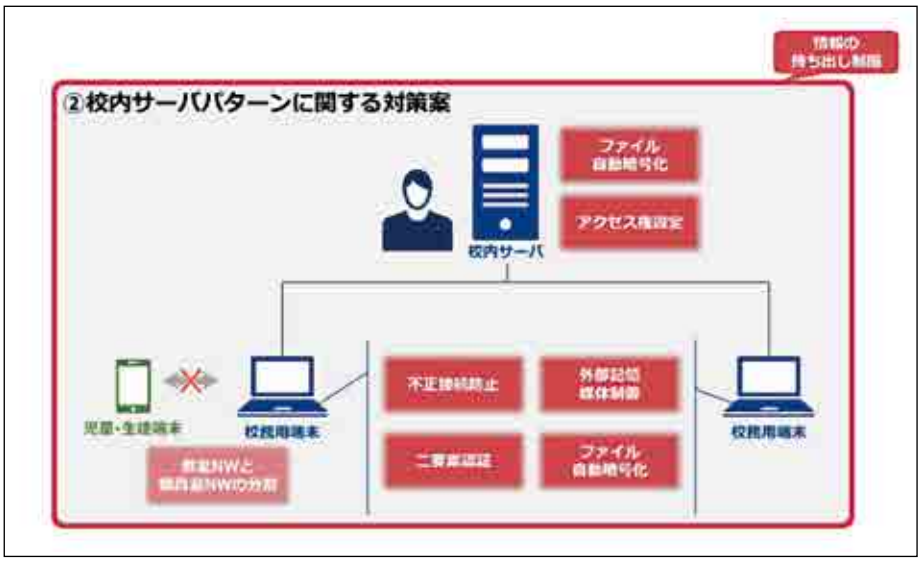
標的型攻撃により、クライアント PC がマルウェアなどに感染し、個人情報などの機密情報が含まれる電子ファイルが外部に流出したとしても、ファイルを暗号化していれば、攻撃者は中身の閲覧ができないため、情報漏えいを防止できます。（図表 2-42）

図表 2-42　さまざまな守秘の方法



たとえば教員の校務用端末にデータが保存されていて、暗号化もされていないと、そのデータの管理は教員に依存することになり、大変危険です。まずは、校務用端末自体へのアクセス制御、ファイルの暗号化を行い、校内で管理しているファイルサーバに対しても同じようにアクセス制御、暗号化の対策を行い、合わせて個人情報の日常的な管理ができる仕組みづくりを進めることが肝要です。（図表 2-43）

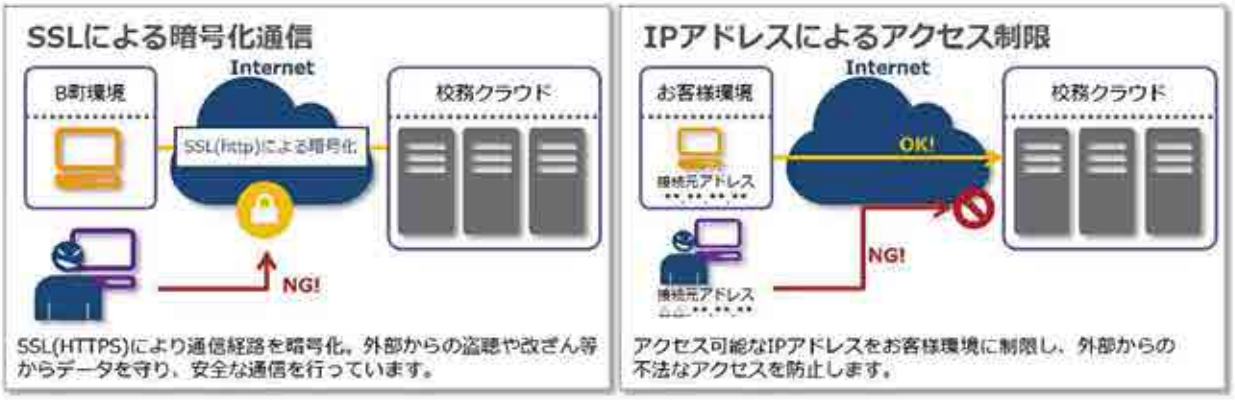
図表 2-43　校内サーバパターンに関する対策案



実際の利用事例を紹介します。C町では統合型校務系システムを導入し、該当データをクラウドに格納しています。

セキュアな接続で安全・安心にクラウドを利用できるよう、「強固なセキュリティ対策」、「システムの二重化、「24 時間 365 日の監視体制、「震度 6 の耐震強度」、「UPS・自家発電設備設置」など、堅牢な国内のデータセンターでシステム運用を行っており、「月間のサーバ稼働率 99.95％以上」のサービス品質を業者に担保させています。クラウドへの通信経路は SSL により暗号化し、IP アドレスによるアクセス制限を設けています。（図表 2-44）

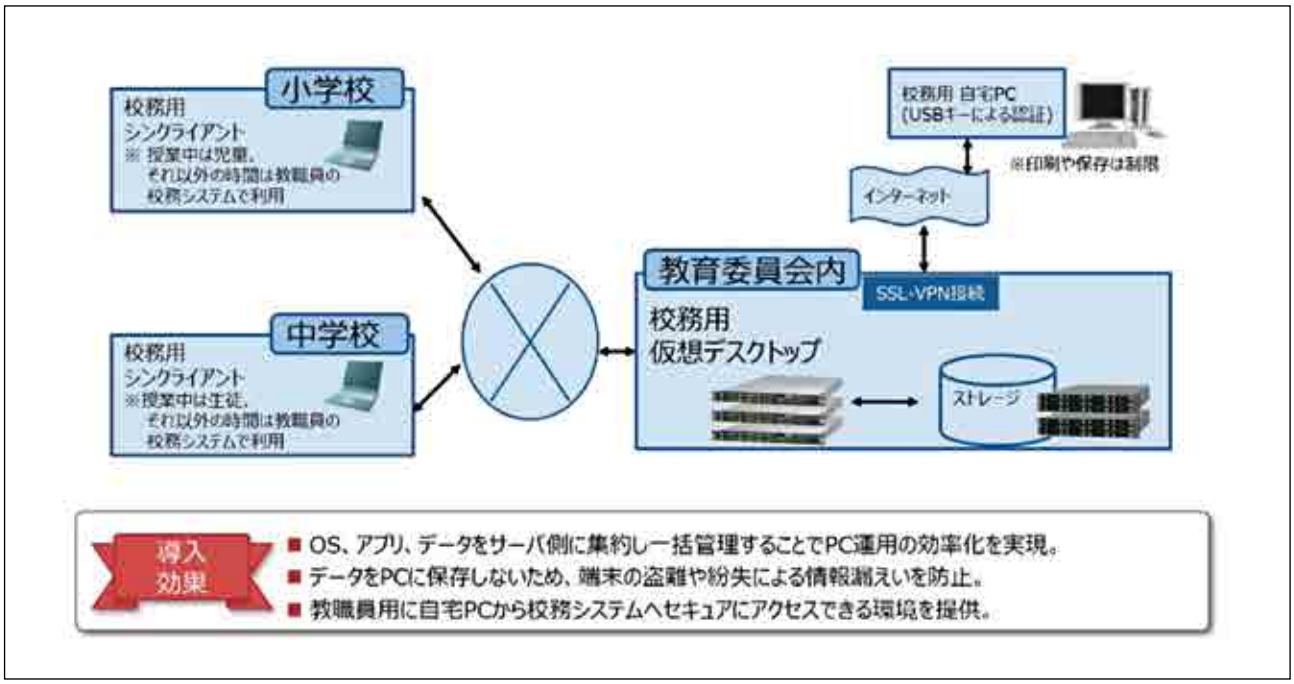
図表 2-44　C 町における校務クラウドのセキュリティ対策



また、D 市ではノートパソコンを授業中は普通教室で子供が活用し、それ以外は教職員が校務で利用するため仮想デスクトップ方式を採用しました。利用者はネットワークを通じて、サーバ上に仮想化（あたかも実在するように）されたデスクトップにリモートで接続し、それぞれのデスクトップ環境を利用しています。（図表 2-45）

この方式を採用することにより、校務データが教職員のノートパソコンに保存されることがなくなり、情報漏えいのリスクを軽減できました。また、基本ソフト（ＯＳ）のセキュリティパッチの対応、ウィルスパターンファイルについても、サーバ側で一括して適用できます。市内に点在する多くの台数のパソコン個別に適用する場合は、パソコンの利用者が不在、あるいはパソコンを利用したいため更新作業の時間が確保できずに後回しにするなどが発生し、セキュリティパッチ等が適切なタイミングで適用されない、もしくは適用漏れが発生するなどのリスクがありますが、それを回避することができます。

図表 2-45　D 市における仮想デスクトップを活用した校務系システム環境構築例



さらに D 市では、SSL-VPN と、USB キーによる認証を組み合わせ、自宅から校務系システムを利用できるようにしました。教員が自宅で作業せざるを得ない場合に、自宅のパソコンから安全に校務系システムに接続ができ、自宅パソコンにはデータ保存や印刷ができないように制限することで、利便性向上に加えて情報漏えいリスクも軽減しています。（図表 2-45）

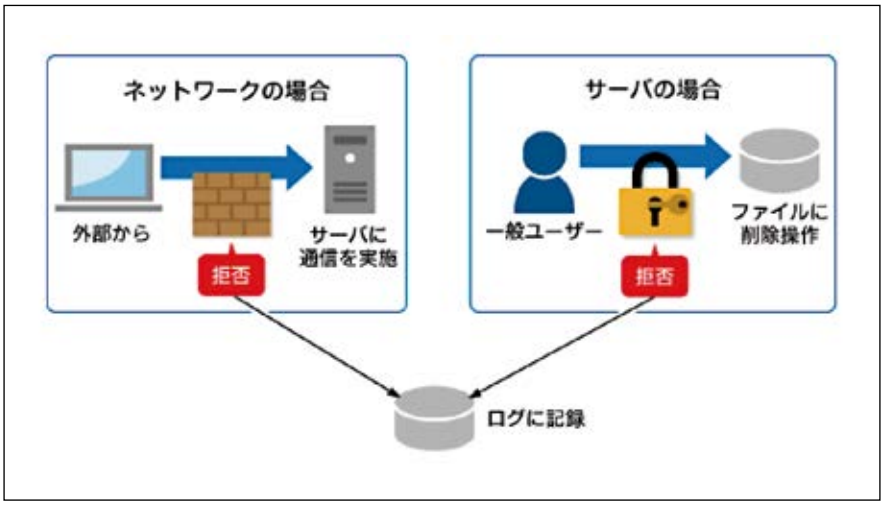
2.4.5　アクセス制御

■アクセス制御の役割

アクセス制御の役割は「ポリシーに沿った必要なアクセスを許可する」「ポリシーに沿わない不要なアクセスを拒否する」の２つがあります。また、重要なアクセスについては許可・拒否の内容を証拠（証跡）としてログに記録することで、管理者が異常を検知、対応できるようにします。（図表 2-46）

アクセス制御が許可／拒否の判断材料にするのは「誰が」「どこに対して」「何をしようとしたのか」という情報です。ここでは、アクセス制御として、「サーバやクライアントでのアクセス制御」と「ネットワークアクセス制御 (次項)」について考えます。

図表 2-46　アクセス制御のイメージ



資料出所：Security & Trust (2016)「ネットワークアクセス制御の基本――「正しいセキュリティ設計の考え方」入門」

■サーバやクライアントでのアクセス制御

サーバやクライアントではいくつかの観点でアクセス制御が行われますが、本稿ではその中でも代表的な「ユーザのアクセス制御機能」と「ネットワークアクセスの制御機能」の２つを取り上げます。

・ユーザのアクセス制御

「ユーザのアクセス制御機能」は、OS が提供する機能で、ユーザがファイルなどに対して読み取りや変更といった操作をする際に、「アクセスするユーザ」や「アクセス対象を所有しているユーザ」「アクセス対象に設定されたルール」などの情報を基に、アクセスの許可／拒否を決定するものです。なお、ここでいう“ユーザ”には、利用者（人）だけでなく、Microsoft Windows の「System」ユーザのような、OS やサービスが使用するユーザも含まれます。

・ネットワークアクセス制御

個々のサーバやクライアントから出入りする通信を制御の対象としたアクセス制御です。「Web サーバでは 80/TCP、443/TCP 以外の通信を拒否する」といったように、サーバやクライアントの役割などに合わせた細かな制御ができます。

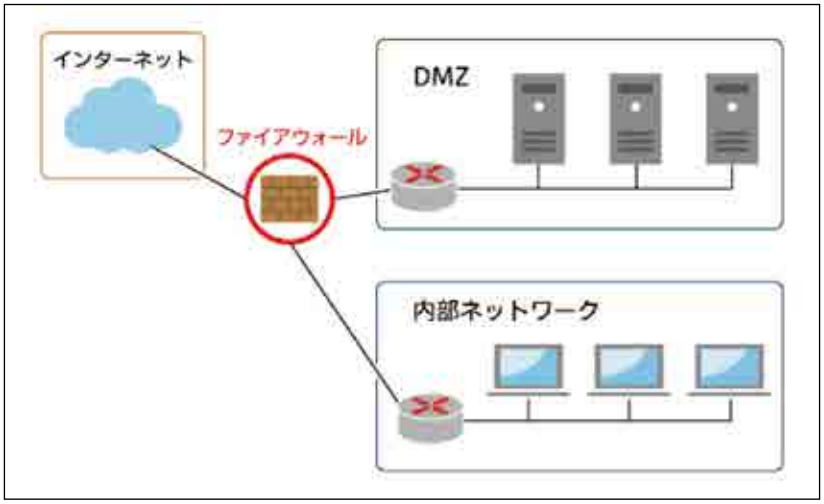
2.4.6　アクセス制御とネットワーク･アプライアンス

■ネットワークにおけるアクセス制御

ネットワークにアクセス制御を実装した機能を、本解説では「ファイアウォール」「アプリケーションファイアウォール」と呼びます。

「ファイアウォール」「アプリケーションファイアウォール」は、ネットワークを「インターネット接続領域」「DMZ（非武装）領域」「内部ネットワーク領域」などの情報セキュリティポリシーの違う領域に区切り、その間の通信をアクセス制御により制限するものです。（図表 2-47）

図表 2-47　ファイヤウォールの設置例



資料出所：Security & Trust (2016)「ネットワークアクセス制御の基本――「正しいセキュリティ設計の考え方」入門」

両者の違いは、アクセス制御を実施する“対象レイヤー”の違いです。ファイアウォール機能が、通信機能のOSI 参照モデルのうち、主に「ネットワーク層（L3 ／レイヤー 3）」から「トランスポート層（L4）」までを制御対象として IP アドレスやポート番号を用いたアクセス制御を行うのに対して、アプリケーションファイアウォール機能は、「アプリケーション層（L7）」までを制御の対象とします。

アプリケーションファイアウォールを使うと、たとえば、アクセス先の Web サイトのサービスの内容を基にアクセス可否を判断するなど、より細かな単位でのアクセス制御を実施できます。

従来のファイアウォール機能では、アプリケーションや Web アプリケーションの通信の“内容”に基づいたアクセス制御は行えませんでした。それに対して、通信パケットの中身までを見ることでファイアウォール機能の欠点を解消したのが、アプリケーションファイアウォール機能というわけです。ゆえに、この機能は「次世代ファイアウォール（NGFW）」あるいは「L7 ファイアウォール（L7FW）」などと呼ばれることもあります。

■ネットワーク・アプライアンス

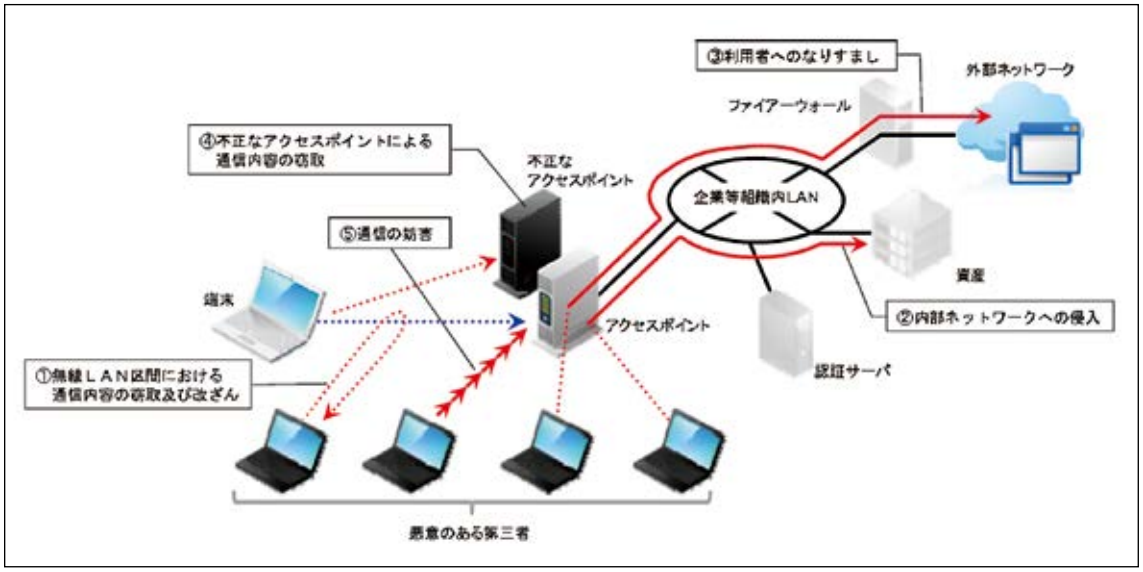
複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理、つまり統合脅威管理 (Unified Threat Management) を行う UTM という機器があります。ファイアウォールのみならず、IDS/IPS やアンチマルウェア、アンチスパム、Web フィルタリングなどの機能を集約し、管理･運用負荷の低減とネットワーク脅威管理の一元化を実現しています。

2.4.7　無線LANのセキュリティ

■無線 LAN 利用時のセキュリティ上の脅威

無線 LAN は、電波を利用するために、有線 LAN と比較して傍受等が容易であることに起因する脅威にもさらされています。企業等の組織による無線ＬＡＮの運用における情報セキュリティ上の主な脅威を以下に示します。（図表 2-48）

図表 2-48　セキュリティ上の主な脅威



資料出所：総務省 (2013)「企業等が安心して無線 LAN を導入・運用するために」

これらの脅威への対策として、以下の設定を行います。

■無線 LAN 利用時のセキュリティ設定

・暗号化設定

暗号化設定を利用することで、通信内容が暗号化されるので、物理的に通信が傍受されても通信内容は守られ、また、暗号化をするために必要な認証機能が、無線 LAN の利用者の認証機能になります。
なお、無線 LAN の暗号化には、WEP など強度が弱いものもあります。利用するクライアントとの組み合わせの中で、最強の暗号化設定を利用しましょう。

・パスフレーズ設定

力ずくでパスフレーズを破ろうとする攻撃に晒されることを考えるなら、できるだけ桁数の多いパスフレーズを利用すべきです。通常は利用するクライアントに一度パスフレーズを設定 (自動接続設定) したら、パスフレーズを変更しない限り二度と入力することはないので、覚えやすいなどの考慮は不要です。

・認証サーバの利用

セキュリティ対策の多重化（多層化）として、複数の無線 LAN 機器を一括管理できるような無線 LAN スイッチと認証サーバを利用するのもよいでしょう。

・無線 LAN の電波漏れの防止

無線 LAN の親機に限らず、教室等に見合った機器を利用しましょう。あまりに強力な電波を飛ばす機器であれば、業務スペースを超えた場所でも接続情報が知られていれば接続できたり、暗号化されていても通信データが傍受されたりすることがあります。こういった問題を防ぐ物理的な対策は、業務スペースに見合った無線 LAN 機器を選定するだけでなく、電波の漏れない環境を作ることができます。たとえば、電波遮蔽シートを窓に貼るのも有効です。

2.4.8　IoTにかかわるセキュリティ

■ IoT のセキュリティ

インターネットに接続される機器の数は年々増加しており、「モノのインターネット（IoT）」が形成されると言われています。

これらの「モノ」が所有する情報がネットワークを介して収集・分析・フィードバックされ、さまざまな形で活用されることが見込まれています。そのような IoT 機器は、インターネットを含むさまざまなネットワークと接続すること、プライバシーに関わる機微な情報を外部とやり取りすること、クラウドを活用すること等を前提とし、適切なセキュリティ対策が行われていることが必須となります。

複合機などの大型の機器やウェブカメラのような小型の機器も、ネットワーク上では 1 台 1 台がサーバとして機能しています。そのため、業務用のサーバやＰＣと同様に、IoT 機器も導入前に機能や動作を理解した上で、ネットワークに接続する必要があります。

IoT 機器の多くは、購入してすぐ利用できるように設定されて出荷されているため、初期設定でログイン認証が設定されていない場合や利用しない不要な機能が有効となっている場合があることを認識する必要があります。初期設定のままインターネットに接続することは、適切な利用者だけでなく、他のインターネット利用者からもアクセス可能な状態となるため、不正アクセスや機密情報の漏えいといった、セキュリティ事故を引き起こす可能性があります。

IoT 機器においても初期設定のままとせず、適切な設定を行うことが重要です。

2.4.9　セキュリティ監視技術とシステム

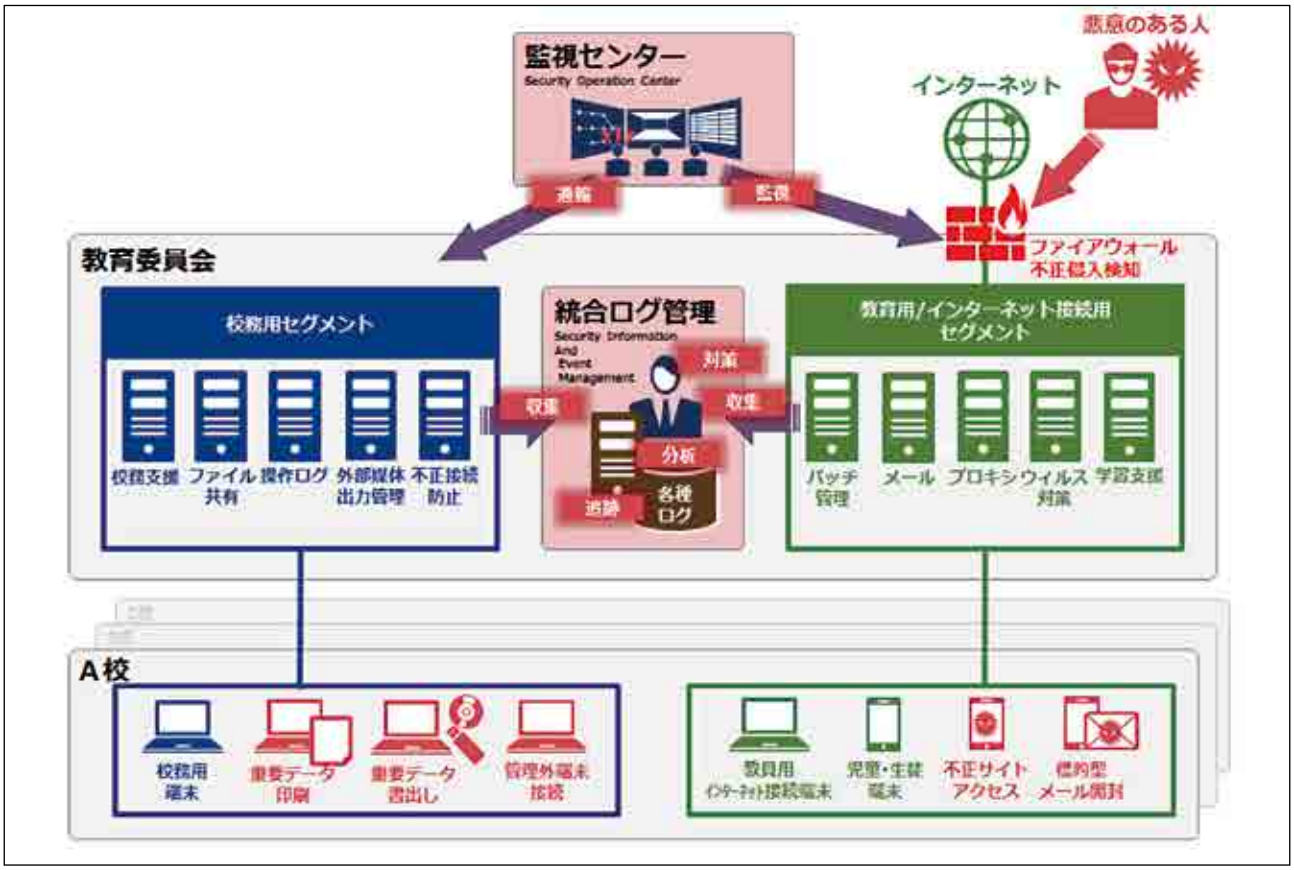
■平時の監視と有事の追跡

学校で扱う情報資産には個人情報を含む重要データが大量にあります。情報セキュリティ対策を講じただけでは効果がありません。外部からの脅威に対しては、いつ攻撃されるかわかりません。即座に対策を講じなければならない脅威にさらされることも考えられます。常時の監視により、脅威に対して最小限の被害に抑えることが可能です。

ただ、常時監視するためには監視体制の構築とセキュリティに精通した要員の確保が必要ですが、監視を請け負うサービスもあります。下図の監視センターがそれにあたります。また、データ流出等の情報セキュリティ事故が発生した場合に、誰（どこ）から、いつ、どのように重要データが流出したのかの証跡を調査する必要があります。さらに、同様の情報セキュリティ事故が発生しないように対策を講じる必要があります。

そのためには、証跡の調査に必要なシステムの導入はもちろんのこと、大量のログデータから情報セキュリティ事故の発生要因を短期間で調査可能な仕組みが必要です。下記の図の統合ログ管理は、複数のシステムのログを収集し、分析しやすいようにした仕組みとなっています。（図表 2-49）

図表 2-49　セキュリティ監視の全体像



◉ 2.5　学校に戻ったら（情報セキュリティ実施状況の確認）

2.5.1　情報セキュリティチェックシート（管理職編）

データや書類

- □ データを持ち出す時のルール、手続きを定めている。または使用システムがデータ持ち出しができない仕組みとなっていることを確認している。
- □ データをやむを得ず持ち出す際のために自動的に暗号化される記録メディア（ＵＳＢメモリー等）を用意し、使用・返却状況を毎学期以上の頻度で確認している。
- □ 機密情報を含む書類やメモ、記録メディア等の廃棄ルールを定め、実施状況を毎年確認している。
- □ 書類や記録メディア等があるべきところに配置されているか、学期ごとに（以上の頻度で）確認し、記録を残している。

機器やソフトウェア

- □ 管理職のコンピュータのＩＤやパスワードを他の教職員等に知らせていない。
- □ 全てのＰＣ（タブレットＰＣを含む）にウィルス対策ソフトを導入している。
- □ 学校サーバはない。または、システム管理者以外が触れないように管理している。
- □ 私物のＰＣや無線アクセスポイントなどを学校のネットワークや機器に接続した時の危険性を理解している。

教　育

- □ 日常的にクリーンデスク、パスワードの管理などについて、教職員向けのポスター掲示や声掛けを通じて働きかけている。
- □ 情報セキュリティや情報モラルに関する校内研修を最低年１回以上行っている。
- □ 保護者、地域、地元の企業等、外部と連携した情報セキュリティ維持・向上のための仕組みづくりを行っている。
- □ 情報セキュリティ事故を教職員が起こした場合の懲戒処分等の重さを理解している。

情報セキュリティ事故発生への備え

- □ 情報セキュリティ事故（あるいは事故のおそれ）が発生した時に備えて、連絡体制を定めている。
- □ 情報セキュリティ事故につながる可能性がある事象が発生した時、即座に情報共有する雰囲気づくり、声掛けを日常からしている。
- □ 情報セキュリティ事故（あるいは事故のおそれ）が発生した時に、教育委員会の担当者に即座に連絡できるよう、連絡先を常に携行している。

2.5.2　情報セキュリティチェックシート（教職員編）

データや書類の管理

- □ データを持ち出す時には学校で定められたルールに従っている。
- □ データを持ち出すためＵＳＢメモリーを使う時は暗号化対応のものだけを使い、常に携行している。
- □ 機密情報を含む書類（メモなども含む）や記録メディアは学校で廃棄ルールを設け、それに従って適切な方法で廃棄、削除している。
- □ 学校で書類を印刷したりコピーしたりした時は、出力した紙をすぐに回収している。
- □ 帰宅する時、業務の書類や記録メディア等は引き出しなど所定の場所にしまっている。

PCのログオン、パスワード、ファイル等の管理

- □ コンピュータのパスワードは桁数を８桁以上にし、３種類以上の字種を入れたものにしている。
- □ コンピュータのＩＤやパスワードは、他人に知られないよう管理している。
- □ 機密情報を含む電子ファイルは、必要な人以外はアクセスできないところに保管している。
- □ 機密情報を含むファイルは暗号化、パスワードにより保護している。
- □ 自席から離れる時は、ＰＣをログオフするか、画面をロックしている。

電子メール、Web アクセス、ソフトウェア、機器等の管理

- □ 電子メールは違う人に送っていないか、宛先を確認してから送っている。
- □ 電子メールに添付ファイルが付いていたら、送信者やファイルの拡張子を確認している。
- □ 機密情報を電子メールで送っていない。やむを得ず送る際は暗号化している。
- □ 業務上必要のない Web サイト（ホームページ）には学校のＰＣからアクセスをしていない。
- □ 今までアクセスしたことがない Web サイト（ホームページ）にアクセスするときはサイト評価を確認している。
- □ 学校のコンピュータに無断でソフトウェアをインストールしていない。
- □ ＯＳ（基本ソフト）やソフトウェアのアップデートは確実かつ速やかに適用している。
- □ 私物のＰＣや無線アクセスポイントなどの機器は学校のネットワークや機器には接続していない。
- □ 私物のＰＣ等を学校に持ち込む際は、ウィルス対策ソフトを入れ、ソフトウェアのアップデートを行っている。

著作権や肖像権への配慮

- □ 子供の写真、作品等は、事前に本人と保護者の同意を得てからコンテストへの応募や学校ホームページへの掲載等を行う。
- □ 写真等をＳＮＳにアップする時は、写っている人が同意できるか確認している。

2.5.3　情報セキュリティチェックシート(教育委員会システム担当者編)

情報セキュリティポリシー

- □ 傘下の学校の情報資産を抽出・重要度分類した一覧を作成し、更新の有無を定期的に確認している。
- □ 傘下の学校の情報資産に対する脅威とその対応を一覧化し、定期的に見直しをかけている。
- □ 情報セキュリティポリシーの策定に関する基本的な考え方を傘下の学校に示している。
- □ (上記に該当する場合) 情報セキュリティポリシー見直しの必要がないか、定期的に確認している。
- □ 情報セキュリティポリシーで規定した体制図を氏名や連絡先も含めて作成し、関係者で共有すると同時に毎年更新している。
- □ 自組織及び傘下の学校の情報セキュリティポリシーの遵守状況について、毎年一回以上確認や検査を行っている。

データや書類を扱う仕組み

- □ 情報セキュリティポリシー、実施手順の内容に応じて、教員ＰＣのＵＳＢポート使用可否やデータ持出の仕組みを実現している。(ポリシー等で禁止している場合はシステム上も持出不可としている)
- □ 教職員の異動時等が発生した時は、教職員用フォルダのアクセス権限設定を適時に更新している。

機器やソフトウェア、ネットワーク

- □ 傘下の学校の情報システム／ネットワーク構成を最新の状態にアップデートした書類が手元にある。
- □ 校務系と授業支援（学習）系のネットワークは分離している。
- □ パスワードの設定ルールに抵触するパスワードは設定できないようシステム側でガードしている。
- □ 私物の機器や記憶メディア等の取り扱いに関するルールを定め、抵触する機器接続を試みる者がいても、ルールで禁じている時は「機器を接続させない」等の設定をシステム側で行っている。
- □ システムやネットワークのログを６か月分以上保存し、定期的にチェックしている、または業者等からチェック結果の報告を受け確認している。

教　　育

- □ クリーンデスク、パスワードの管理などの情報セキュリティの基本事項、取組事例等について、学校向けの研修を年間で計画的に行っている。
- □ 新たな情報セキュリティの脅威や情報セキュリティ事故等に関する情報を収集し、脅威の度合いや対応方法を分析・検討し、必要に応じて学校へ周知・連絡を行っている。

情報セキュリティ事故発生への備え

- □ 情報セキュリティ事故（あるいは事故のおそれ）が発生した時に備えて、連絡・報告の体制を定め、人事異動等が発生した時には更新している。
- □ 情報セキュリティ事故（あるいは事故のおそれ）の情報が入った時、上司以外に情報セキュリティの専門的な知識を持った助言者に相談できる体制をとっている。
- □ 万一、学校等が情報セキュリティ事故等で事業継続が困難になった際に備えて、事業継続計画（BCP）を定めている。

●【参考】教育情報セキュリティに関する情報が入手できる Web サイト

文部科学省ホームページ　教育の情報化推進
http://www.mext.go.jp/a_menu/shotou/zyouhou/index.htm

総務省ホームページ　教育情報化の推進
http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/

経済産業省ホームページ　情報セキュリティ政策
http://www.meti.go.jp/policy/netsecurity/

一般社団法人　日本教育情報化振興会ホームページ
http://www.japet.or.jp/

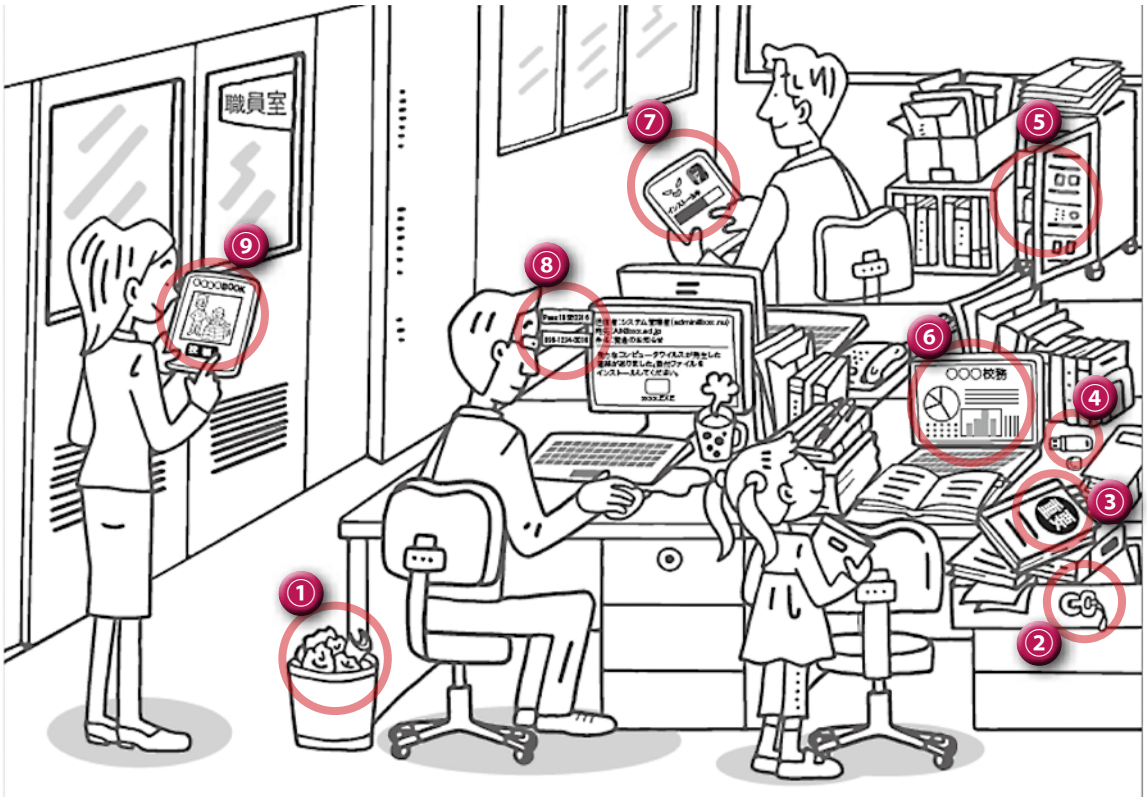
独立行政法人　情報処理推進機構（IPA）ホームページ
http://www.ipa.go.jp/

教育ネットワーク情報セキュリティ推進委員会（ISEN）ホームページ
http://school-security.jp/

情報セキュリティ、どこが危ない？

解答例

① ＵＳＢメモリーを挿入したまま放置している
② 業務で必要ない Web ページを閲覧している
③ 他人のＩＤでログインしようとしている
④ 教職員のタブレットを子供が勝手に操作している
⑤ 授業に関係ない Web ページ閲覧
⑥ 子供を見取らずスマートフォンを操作している
⑦ 引出を開け放している
⑧ 重要資料を開け放している



① 業務の書類をゴミ箱に廃棄している
② 引出が開け放され、鍵も付け放しにされている
③ 重要書類を乱雑に放置している
④ ＵＳＢメモリーが机上に放置されている
⑤ サーバラックが開け放し
⑥ 教職員 PC がロックされず、子供が内容を見ている
⑦ 無断で (不正の可能性のある) アプリをダウンロードしている
⑧ ID、パスワードを付箋紙で PC に貼っている
⑨ ＳＮＳに子供の写真を投稿

監修：「学校における情報セキュリティを確保したＩＣＴ環境強化事業」事業推進委員会

益川　弘如　（静岡大学教育学部　准教授・事業推進委員長）
秋元　大輔　（船橋市教育委員会学校教育部 参事 船橋市教育センター　所長）
石田　淳一　（株式会社アールジェイ　代表取締役）
猪俣　敦夫　（東京電機大学未来科学部情報メディア学科　教授）
太田　耕司　（千代田区立神田一橋中学校　校長）
西田　光昭　（柏市立柏第二小学校　校長）
宮野　　誠　（神奈川県教育局 総務室ＩＣＴ推進グループ　副主幹）
毛利　敏久　（静岡市教育委員会事務局 教育局学校教育課 企画管理係　指導主事）
湯淺　墾道　（情報セキュリティ大学院大学学長補佐・情報セキュリティ研究科　教授）

◇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　　佐賀県教育委員会、三鷹市教育委員会、豊島区、株式会社内田洋行、株式会社ＪＭＣ
　　日本電気株式会社、富士通株式会社（五十音順）