学校における情報セキュリティ及び ＩＣＴ環境整備等に関する研修教材

小中高等学校等教職員・教育委員会指導主事向け教材

平成 29 年３月

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

◆はじめに

本教材は学校現場におけるＩＣＴ（Information & Communication Technology：情報通信技術）の環境整備を促進し、アクティブ・ラーニング等におけるＩＣＴ活用の効果を教職員が実感できるようにすること、さらにそのために必要な情報セキュリティの確保のための実践的な研修を支援するためのものです。

ますますグローバル化、情報化が進む社会環境において、子供が未来の創り手となるために、新しい時代に必要となる資質・能力を踏まえ、次期学習指導要領においては小学校外国語教育の教科化や高等学校の「公共」の科目新設など、学ぶ対象が変化していると同時に、「主体的・対話的で深い学び（アクティブ・ラーニング）」の視点から学習過程を改善していく方向となっています。このような学びをデザインし実践するため、授業や学習のさまざまなシーンでＩＣＴは欠くことができない手段（ツール）です。また、教職員が多忙化する中で、デジタル教科書をはじめとするさまざまな教材を効果的に活用し、学習カリキュラムをデザインする余裕を生み出すため校務の情報化による業務改善は有効な手段となります。

スマートフォンが登場して約１０年の今、既に高校生のスマートフォン、携帯電話はほぼすべての子供が所有する時代となりました。現在の子供は多くが幼児期から保護者のスマートフォンなど何らかのＩＣＴ機器、ネットワークと接触しながら育っており、学習、日常生活のさまざまな場面でＩＣＴを使いこなしています。実際、ＩＣＴに関する高度な知識を持ち、ネットワークの世界を縦横無尽に活動する子供の数は着実に増えており、社会や経済のイノベーションも彼らが先導役となることが我が国の活力にもつながると言えるでしょう。

このようにＩＣＴの活用には大きな可能性がある半面、授業・学習におけるＩＣＴ活用の効果がさまざまな取組を通じて確認されているにもかかわらず、学校現場のＩＣＴ環境は地域ごと、学校ごとに整備状況に格差が生じいるのが現状です。さらに、個人情報などの重要な情報に対する脅威も、学校内外のさまざまな場面でさまざまな方法によりもたらされています。そして一度情報漏えいなどが発生すると、当事者のみならず学校管理職や教育委員会も原因究明、説明、再発防止のための対策等に大きな手間が必要となります。教職員や子供の情報モラルを育むこと、情報セキュリティの仕組みをしっかり構築し、実際に活用していく中できちんとＰＤＣＡ（計画・実行・評価・改善）のサイクルを回して、ＩＣＴを安心して使える状態を整備することの重要性が日々高まっています。

教職員の皆さんは、まず自校、自地域のＩＣＴ環境と活用状況を把握してください。それらと教職員や子供、学校を取り巻く地域等の状況とを照らし合わせながら、授業や学習等でのＩＣＴ活用方法の工夫などをレベルアップし、同時並行で情報セキュリティの確保に向けた取組を進めていくことではじめて、ＩＣＴの力を子供たちや教職員自身に還元することが可能となります。

それでは、学校のＩＣＴ環境のチェックリストを活用して、現在の自校の整備状況を確かめてみましょう。

学校ＩＣＴ環境チェックリスト

・選択肢のうち、御自身の学校の状況にもっとも近いと思われるものをチェックしてください。
・チェックが終わったら点数をつけ、合計してください。点数はレベルの番号と同じです。（例：レベル 3=3 点）

学校名　　合計点　　／40

	項目	レベル０	レベル１	レベル２	レベル３	レベル４	得点
ＩＣＴ機器、ネットワーク							
1	教育用コンピュータの整備状況（拡大提示や子供の学習に使用するＰＣ）	ＰＣ教室１クラス分のみ □	（左に加えて）全普通教室に１台 □	グループ１台可動式ＰＣ □	必要な時に１人１台可動式ＰＣ □	常時１人１台可動式ＰＣ □	＿＿
2	電子黒板または大型提示装置の整備状況（電子黒板、大型テレビ、プロジェクター等）	大型提示装置類が校内にない □	フロアに１台未満 □	必要な時に１台（調整不要） □	全普通教室に１台常設 □	（左に加えて）特別教室、体育館１台常設 □	＿＿
3	普通教室のＬＡＮ	教室にはＬＡＮが敷設されていない □	有線の情報ｺﾝｾﾝﾄが一部教室にある □	全教室に情報ｺﾝｾﾝﾄ設置 □	（左に加えて）可動式無線 LAN が利用可能 □	無線 LAN が全教室で利用可能 □	＿＿
4	サーバの個人用フォルダ（授業用教材や学習結果等を個人別に格納できる。例：校内サーバ、Office365, Google Drive, Dropbox など）	教職員用も子供用も個人用フォルダがサーバにない □	ＰＣ教室でつかえる個人用フォルダがある □	校内のみで使える教職員向け個人用フォルダがある □	（左に加えて）校内のみで使える子供の個人用フォルダがある □	家庭等でも使えるクラウド型の個人用フォルダがある □	＿＿
5	教職員（校務）用コンピュータの整備状況	教職員用ＰＣがない □	共用の教職員ＰＣのみ □	常勤教職員に１人１台の教職員用　ＰＣが整備されている □	（左に加えて）非常勤教職員も含め１人１台教職員用ＰＣが整備されている □	（左に加えて）仮想デスクトップ等学校外利用可能な仕組みがある □	＿＿
6	校務支援システムの整備状況	校務支援システム*1 等が導入されていない □	養護、成績等個別業務用の校務支援システム*1 が教職員用ＰＣに入っている □	個別業務用の校務支援システム*1 が学校サーバにあり、複数の教職員が利用している □	統合型校務支援システム*2 が学校サーバにあり、複数の教職員が利用している □	統合型校務支援システム*2 がクラウド型で整備され複数の教職員が利用している □	＿＿
ＩＣＴの活用							
7	教職員の授業・学習におけるＩＣＴ活用	ＩＣＴを活用した授業・学習を行っていない □	一部の教職員が授業（＋準備）等にＩＣＴを活用している □	ほとんどの教職員が授業（＋準備）等に ICT を活用している □	ほとんどの教職員が授業（＋準備）等に ICT を日常的に活用している □	ほとんどの教職員が授業（＋準備）等に ICT のより効果的な活用方法を研究している □	＿＿
8	子供の授業・学習におけるＩＣＴ活用	ＩＣＴを活用した授業・学習を行っていない □	子供が授業等でＩＣＴを活用する場面がある □	子供が ICT を活用する場面を教職員が計画的に設定している □	子供が日常的にＩＣＴを活用している □	子供が日常的・自主的にＩＣＴを活用している □	＿＿
9	教職員のＩＣＴ活用研修	ＩＣＴ活用に関する研修は学校でも教育委員会でも行われていない □	ＩＣＴ活用の研修は教育委員会で一部の教職員を対象に行っている □	（左に加えて）ＩＣＴ活用の研修は校内で一部教職員に行っている □	ＩＣＴ活用の研修は校内で年に複数回、一部教職員対象に行っている □	ＩＣＴ活用の研修を校内で毎年、全教職員を対象に行っている □	＿＿
10	情報モラル	子供の情報モラルを育む授業を行っていない □	一部の子供を対象に情報モラルを育む授業を行っている □	子供の情報モラルを育む授業が計画的に行われている □	子供の情報モラルを育む授業がほとんどの教職員により計画的に行われている □	情報モラルの育成を家庭・地域と連携し学校全体で取り組んでいる □	＿＿

*1　校務文書に関する業務、教職員間の情報共有、家庭や地域への情報発信、服務管理上の事務、施設管理等を行うことを目的とし、教職員が一律に利用する単機能のシステム
*2　教務系（成績処理、出欠管理、時数等）、保健系（健康診断票、保健室管理等）、指導要録等の学籍関係、学校事務系など統合して機能を有しているシステム

◆目　次

第１章　社会の変化に対応した教育におけるＩＣＴ環境の整備・活用

第２章　学校の情報化に必要な情報セキュリティとは

第１章　社会の変化に対応した教育におけるICT環境の整備・活用

◉1.1　教育改革を踏まえた教育の情報化動向

1.1.1　我が国の教育の現状と課題

■急激な社会の変化

近年、情報化、グローバル化の進展に伴って、社会がめまぐるしく変化しています。（図表 1-1）この変化は日本だけに閉じたものではありません。

図表 1-1　社会の急激な変化に関する世界各国の有識者等のコメント

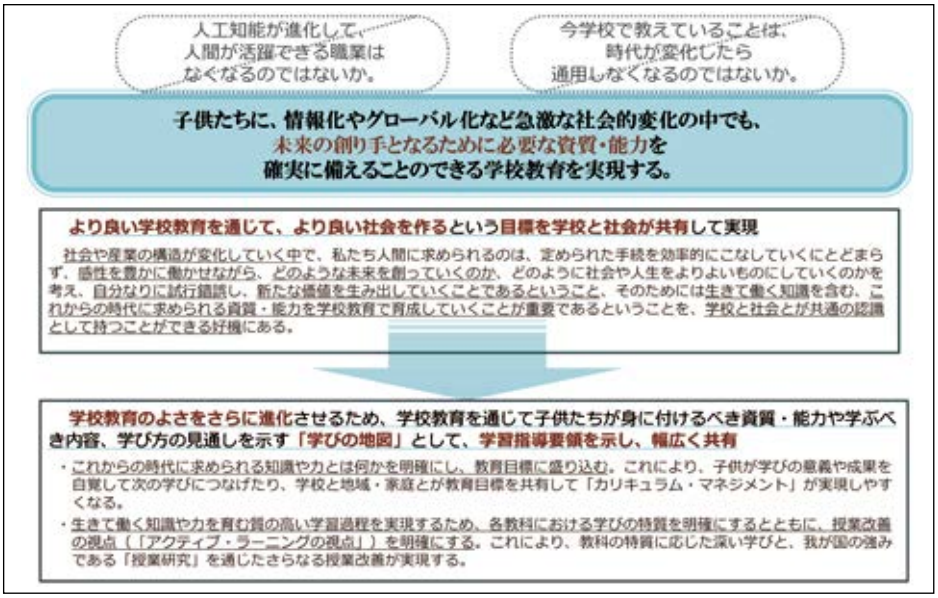
子供たちの 65%は、大学卒業後、今は存在していない職業に就く	キャシー・デビッドソン氏 （ニューヨーク市立大学大学院センター教授）
今後 10 ～20 年程度で、約 47%の仕事が自動化される可能性が高い	マイケル・A・オズボーン氏 （オックスフォード大学准教授）
2030 年までには、週 15 時間程度働けば済むようになる	ジョン・メイナード・ケインズ氏（経済学者）
日本の労働人口の 49%が人工知能やロボット等で代替可能に	株式会社　野村総合研究所（2015 年 12 月 2 日）

これらは、いわゆる第四次産業革命によって発生する変化の一端と言えます。現在の職業の多くは今後なくなっていき、労働の質が高度に発達した情報化社会の中で加速的に変化していくことで、私達の生活、仕事、教育、地域社会などさまざまな場面に影響が及んでいきます。

■学習指導要項の改訂に向けた検討

このような社会の変化により、学習指導要領の改訂に向けた検討においても「今学校で教えていることは、時代が変化したら通用しなくなるのではないか」という議論が行われました。その結果、「子供たちに、情報化やグローバル化など急激な社会的変化の中でも、未来の創り手となるために必要な資質・能力を確実に備えることのできる学校教育を実現する。」ことが学習指導要領改訂の軸となっています。（中央教育審議会「幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）」、平成 28 年 12 月 21 日）（図表 1-2）

図表 1-2　学習指導要領改訂の背景



次期学習指導要領では、「何ができるようになるか」、「何を学ぶか」、「どのように学ぶか」について、以下のような方向性を打ち出しています。（図表 1-3）

●何ができるようになるか　　－育成を目指す資質・能力－

教科等を超えた全ての学習の基盤として育まれ活用される資質・能力

☞情報化の進展の中でますます読解力の重要性が高まっていますが、子供たちが教科書の文章すら読み解け

ていないのではないかという問題提起もされています。全ての学習の基盤となる言語能力を育くんでいくことが重要です。

☞急速に情報化が進展する社会の中で、情報や情報手段を主体的に選択し活用していくために必要な情報活用能力、物事を多面的・多角的に吟味し見定めていく力、統計的な分析に基づき判断する力、問題を見いだし解決に向けて思考するために必要な知識やスキルなどを体系的に育んでいくことが求められます。

さらに情報活用能力については、情報技術が急速に進化していく時代にふさわしい情報モラル、小学校段階からの文字入力やデータ保存などに関する技能を着実に身に付けることが重要だと指摘されています。

●何を学ぶか

☞新しい時代に必要となる資質・能力を踏まえ、小学校高学年の外国語活動の教科化などが答申されています。

●どのように学ぶか　－各教科等の指導計画の作成と実施、学習・指導の改善・充実－

発達の段階や子供の学習課題等に応じて学びを充実させていく必要があります。知識の量を減らすことなく、子供が学習内容を理解できるようにするため、学習過程を質的に改善していきます。

図表 1-3　学習指導要領改訂の方向性

■「アクティブ・ラーニング」の視点からの授業改善や個の学習ニーズに対応した「次世代の学校・地域」の創生

中央教育審議会が検討した学習指導要領の全面改訂で主要な項目の一つが「主体的・対話的で深い学び（アクティブ・ラーニング）」の視点からの授業改善です。

主体的な学び	学ぶことに興味や関心を持ち、自己のキャリア形成の方向性と関連付けながら、見通しを持って粘り強く取り組み、自己の学習活動を振り返って次につなげる「主体的な学び」が実現できているか。
対話的な学び	子供同士の協働、教職員や地域の人との対話、先哲の考え方を手掛かりに考えること等を通じ、自己の考えを広げ深める「対話的な学び」が実現できているか。
深い学び	習得・活用・探求という学びの過程の中で、各教科等の特質に応じた「見方・考え方」を働かせながら、知識を相互に関連付けてより深く理解したり、情報を精査して考えを形成したり、問題を見いだして解決策を考えたり、思いや考えを基に創造したりすることに向かう「深い学び」が実現できているか。

この視点を受けて「2020 年代に向けた教育の情報化に関する懇談会」では、ポイントを以下に指摘しています。

☞子供たちは何が重要かを主体的に考え、他者と協働しながら新たな価値の創造に挑むとともに、新たな問題の発見・解決に取り組んでいくことが求められている。そのためには、「アクティブ・ラーニング」の視点から学び全体を改善し、個の学習ニーズや一人一人の個性に応じた資質・能力を育成するような学びを実現していくことが重要である。

☞学校や学級という集団のメリットを生かし、他者との協働や外界との相互作用を通じて、自らの考えを広げ深める、対話的な学びの過程を実現する指導の改善が必要である。子供たちの発達の段階や、発達の特性、子供の学習形態の多様性、教育的ニーズに応じた指導を工夫して実践できるようにすることが重要である。

また、子供が学習内容を確実に身に付けることができるよう、個別学習やグループ別学習、繰り返し学習、習熟度別学習、補充学習や発展的な学習等も重要である。

☞また、小学校の外国語活動・外国語については、たとえば音声中心にデジタル教材や電子黒板等を活用して、ネイティブスピーカーの発音に触れ、日本語と英語の発音の違いに気付かせるなど、ＩＣＴの効果的な活用に期待が高い。

☞このように、未来社会を見据えて育成すべき資質・能力を育むための「学び」やそれを実現していくための「学びの場」を形成するためにＩＣＴを効果的に活用することが重要である。

☞さらに、このような「学び」を実現させていくためには、学校・教職員だけで行うのではなく「社会に開かれた教育課程」の実現に向けて、地域との連携・協働を一層進めていくということも重要である。

☞ＩＣＴを活用することで、チームとしての学校の経営力を高め、教育の質の向上と教職員が子供と向き合う時間的・精神的余裕を確保することにつながる。

次期学習指導要領のポイント（教育の情報化関連）

○情報活用能力を教科等を超えた全ての学習の基盤として育まれ活用される資質・能力と位置付け、教育課程全体を通じて確実に育成する旨を規定。〔第１章総則　第２の２の（1）〕

○主体的・対話的で深い学び（アクティブ・ラーニング）の視点からの授業改善に向けて、ＩＣＴを活用した学習活動の充実を図る旨を規定。特に小学校においては、情報手段の基本的な操作を習得するための学習活動や、プログラミングを体験しながら論理的思考力を身に付けるための学習活動を計画的に実施する旨を規定。〔第１章総則　第３の１の（3）〕

図表 1-4　アクティブ・ラーニングの視点に立った学習プロセスにおけるＩＣＴの効果的活用

■高大接続システム改革

高等学校教育改革、大学教育改革と大学入学者選抜改革を一体的に行う高大接続システム改革が進んでいます。学習指導要領の抜本的な見直し、学習・指導方法の改善、多面的な評価の推進という改革の一環として検討されています。改革を一体的に進めることを通じて、「十分な知識と技能を身に付け、それを活用して思考し、判断し、表現する力を磨き、主体性を持って多様な人々と協力して学び、働くことのできる」人材を社会に送り出すことを目的としています。

高大接続システム改革のポイントは以下のとおりです。

☞高等学校教育改革においては、小中学校でのグループ活動や探究的な学習等の延長上に、課題の発見と解決に向けて主体的・協働的に学ぶ学習（アクティブ・ラーニング）の飛躍的充実を図る。

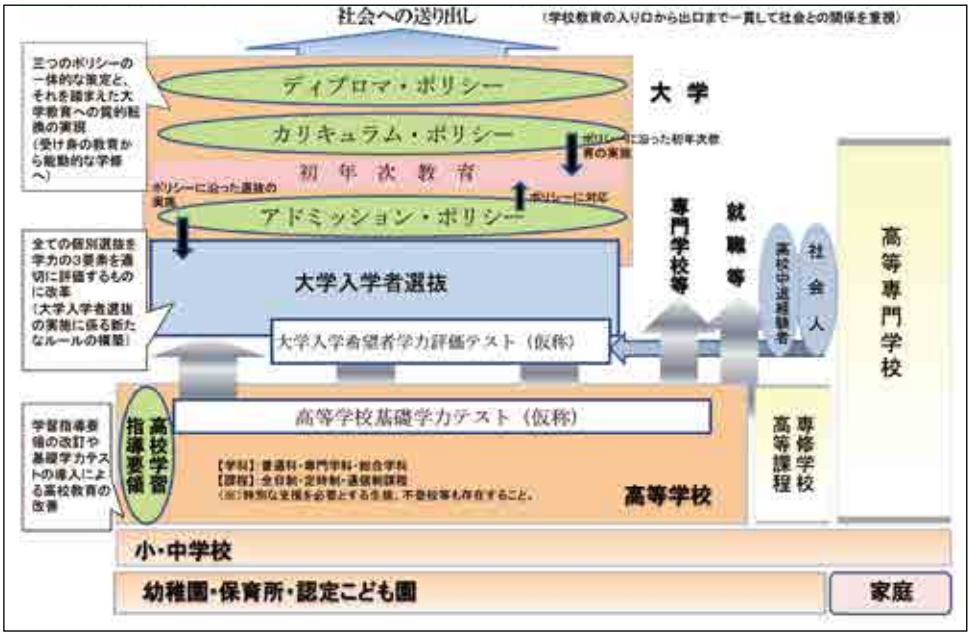
☞大学教育においては、個別の大学は、大学入学以前に培った「学力の３要素」を基に、個々の学生の主体性を更に引き出す多様な学びの場を創り、十分な能動的学習とそれを支える広く深い知識・技能を獲得できるようにする必要がある。そのために、各大学が、「学位授与の方針」（ディプロマ・ポリシー）、「教育課程編成・実施の方針」（カリキュラム・ポリシー）「入学者受入れ方針」（アドミッション・ポリシー）を一体的に策定し、それらに基づいて多様な学生が新たな時代の大学教育を受けられるようにする。

☞大学入学者選抜においては、入学希望者が培ってきた「学力の３要素」を、ディプロマ・ポリシー及びカリキュラム・ポリシーを基に多面的・総合的に評価する方法に転換する。また、個別大学の入学者選抜に資するため、国において、とくに「知識・技能」を基盤として「思考力・判断力・表現力」を中心に評価する「大学入学希望者学力評価テスト（仮称）」を創設し、各大学の利活用を促進する。

☞大学入学者選抜は、特別な支援を必要とする生徒や高等学校中退経験者、社会人等多様な背景や経験を有する者それぞれが大学教育に進むためにも開かれたものであることが必要であり、各大学の個別選抜における評価や「大学入学希望者学力評価テスト（仮称）」において、こうした多様性が十分に尊重されなければならない。

このような改革を進めていくための具体的な制度設計が現在進んでいますが、大学等への進学、公務・民間企業等への就職など多様な進路に進む高校生、既卒業者等が受験する「高等学校基礎学力テスト（仮称）」や大学入学希望者が受験する「大学入学希望者学力評価テスト（仮称）」では、ＣＢＴ（Computer Based Testing：コンピュータを活用した試験）方式での実施が検討されており、情報リテラシーの向上が必要となります。また、いずれのテストでも、次期学習指導要領における教科「情報」に関する中央教育審議会の検討と連動しつつ、情報科を対象科目とすることについても検討がなされています。（図表 1-5）

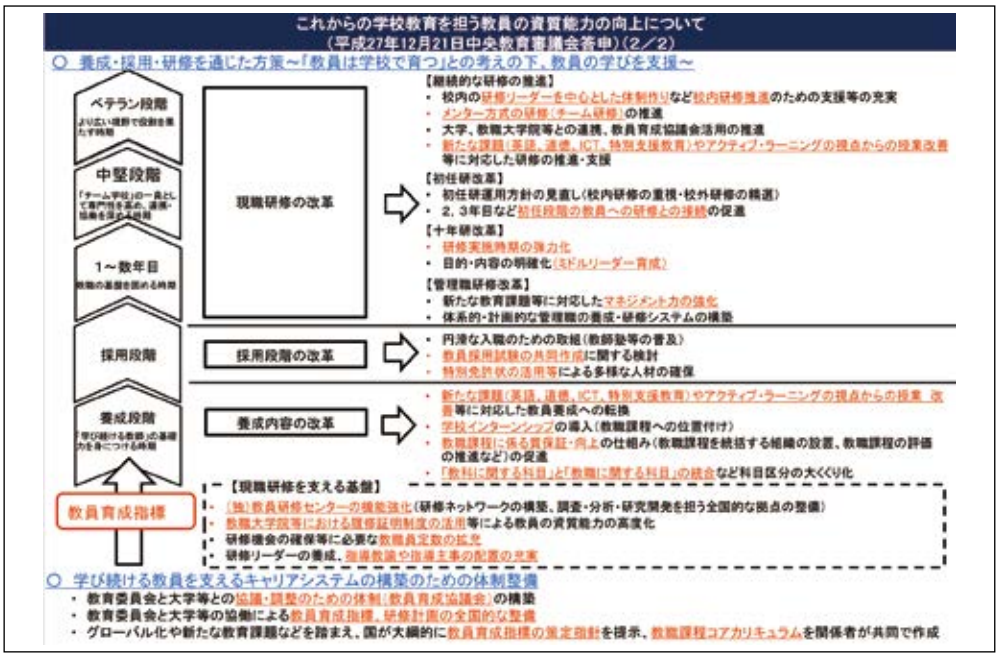
図表 1-5　初等中等教育から大学教育までの一貫した接続イメージ（高大接続改革の全体像）



■教職員の資質・能力の向上

教職員の資質・能力についても教職員の養成・採用・研修を通じた方策として、「教職員は学校で育つ」との考えの下、教職員の学びを支援する方策が提案されています。新たな時代に必要な資質・能力を育むため、新設の教科や特別支援教育、アクティブ・ラーニングの視点からの授業改善等の課題に対応して、採用段階から養成、研修を推進して、教職員の資質・能力を向上していこうというものです。（図表 1-6）

図表 1-6　これからの学校教育を担う教職員の資質能力の向上について（答申）



1.1.2　学校教育の情報化の現状

■教育振興基本計画の流れ

＜教育振興基本計画とは何か？＞

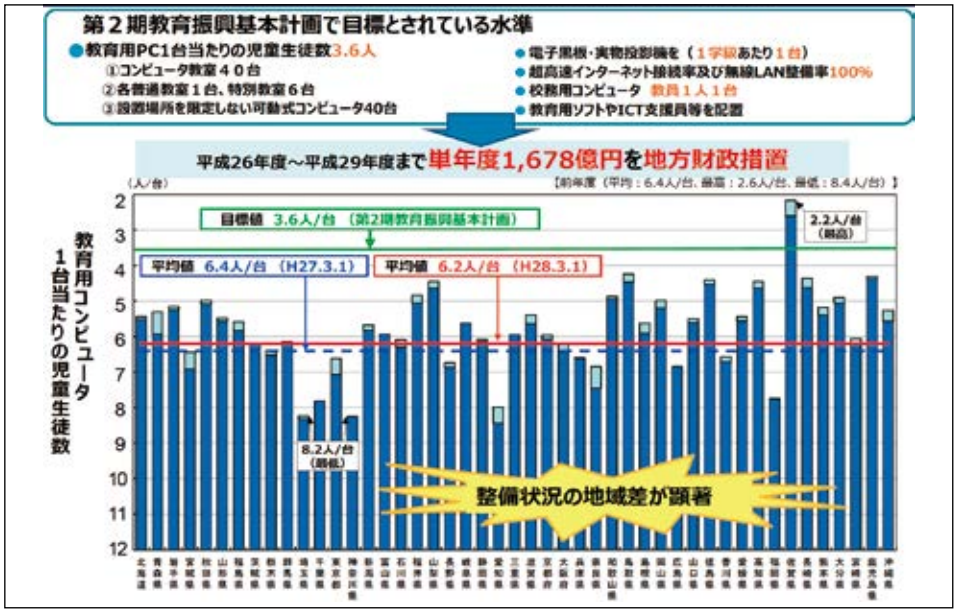
平成 18 年に教育基本法が改正され、科学技術の進歩、情報化、国際化、少子高齢化などの今日的な課題を踏まえ、教育の基本理念が示されました。この理念の実現に向けて、教育基本法の規定に基づき、政府の教育に関する総合的な計画として策定されたのが「教育振興基本計画」です。平成 20 年以降、さまざまな社会情勢の変化や、東日本大震災の発生などを踏まえ、平成 25 年 6 月に第 2 期の教育振興基本計画を策定しました。第 2 期教育振興基本計画は、平成 25 年度から平成 29 年度の 5 年間を計画期間としています。（平成 27 年度文部科学白書第 1 章教育政策の総合的推進より）

平成 29 年度は現在の第 2 期教育振興基本計画の計画期間の最終年度であり、ＩＣＴ環境の整備、活用を着実に進めていくために非常に大切な時期となっています。

■ＩＣＴ整備状況に関する地域、学校間格差

第 2 期教育振興基本計画においては、教育用コンピュータなど 5 項目について目標値を定め、平成 26 年度～平成 29 年度まで単年度 1,678 億円を地方財政措置を講じることで目標達成に向けて地方公共団体の取組を促しています。しかし、図表 1-7 のとおり整備状況は地域差が生じており、どの地方公共団体、地域でも社会の情報化にふさわしいＩＣＴ環境が整備されているわけではありません。

図表 1-7　平成 27 年度　学校における教育の情報化の実態等に関する調査結果



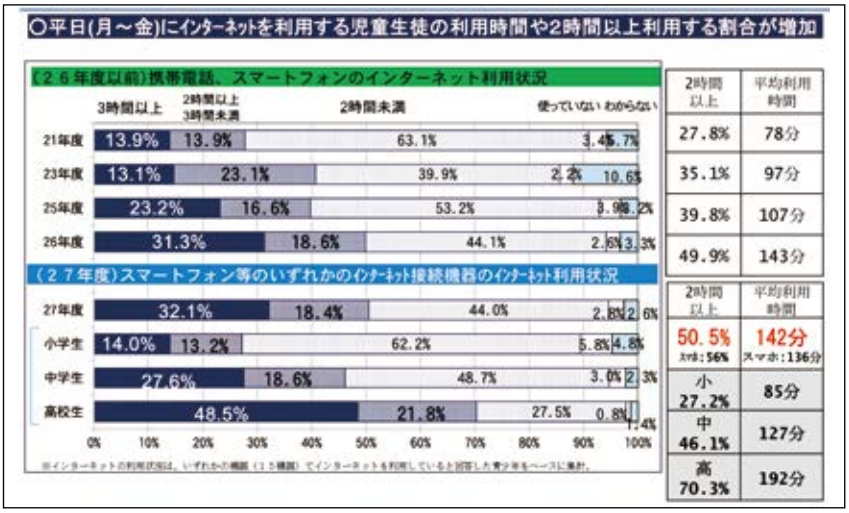
平成 27 年度　学校における教育の情報化の実態等に関する調査結果　より

■現代の子供を取り巻く情報化の状況

内閣府が実施した「青少年のインターネット利用環境実態調査」（調査対象は、満 10 歳から満 17 歳までの青少年）によると、図表 1-8 のとおり全体でスマートフォンの利用率が 75.9% と拡大（携帯電話は 24.1%）していています。平成 22 年度（スマートフォン 2.9%）と比べると、わずか 5 年で携帯端末はスマートフォンに取って代わられたことがわかります。インターネットは、総数で 79.7% が利用（前年度比 3.7% 増）、高校生では、97.7% が利用（前年度比 1.9% 増）していることがわかりました。

同時に、スマートフォン等でインターネットを利用する活用状況では、平日の月曜日から金曜日までの一週間で平

図表 1-8　青少年のインターネット利用状況



資料出所：内閣府「青少年のインターネット利用環境実態調査」

均利用時間が 142 分、一日2時間以上利用する割合は 50.5%、高校生では 70.3% が 2 時間以上利用しています。

■子供の情報活用能力

このようにデジタル社会で育っている子供たちの情報活用能力を把握し、指導の改善、充実に活かすため、文部科学省はコンピュータを用いた情報活用能力調査を平成 25 年 10 月から平成 26 年 1 月にかけて実施しました。その結果、図表 1-9 のとおり小中学生ともに、「整理された情報を読み取ることはできるが複数のウェブページから目的に応じて、特定の情報を見つけ出し、関連付けることに課題がある」、「情報を整理し、解釈することや受け手の状況に応じて情報発信することに課題がある」ことが明らかになっています。同様の課題は、平成 29 年 1 月に公表した高等学校の生徒を対象とした情報活用能力調査の結果（「複数の情報がある多階層のウェブページから、目的に応じて特定の情報を見つけ出し、関連付けることに課題がある。また、複数の統計情報を、条件に合わせて整理し、それらを根拠として意見を表現することに課題がある」）からも読み取ることができます。ＩＣＴ機器の操作に慣れていても、子供が必ずしも情報を適切に活用できているわけではないことがわかるでしょう。

図表 1-9　情報活用能力調査

■教職員のＩＣＴ活用指導力

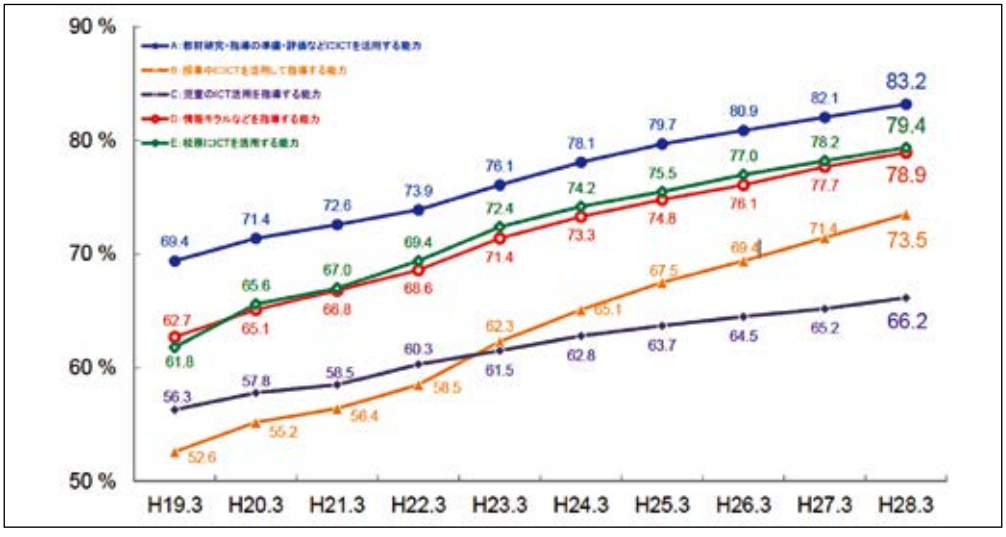
文部科学省は、公立学校を対象に「教職員のＩＣＴ活用指導力の基準（チェックリスト）」に基づく調査を行っています。

調査では、このチェックリストに基づき、教職員が項目別に 4 段階（「わりにできる」「ややできる」「あまりできない」「ほとんどできない」）の自己評価を行い、「わりにできる」若しくは「ややできる」と回答した教職員の割合により、ＩＣＴ活用指導力を把握しています。

調査開始以来、いずれの分野のＩＣＴ活用能力も年々、向上していますが、常に「教材研究・指導の準備・評価などにＩＣＴを活用する能力」と分類される授業前後での活用能力が最も高く（H28 年には 83.2%）、授業中の活用能力（同 73.5%）を大きく上回っており、授業中の活用そのものには課題を残していることが分かります。（図表 1-10）

また、「児童生徒のＩＣＴ活用を指導する能力」が伸び悩んでおり（同 66.2%）、今後の課題と言えそうです。

図表 1-10　教職員のＩＣＴ活用指導力の推移



「平成 27 年度学校における教育の情報化の実態等に関する調査」（平成 28 年 3 月 1 日）より

◉1.2　教育の情報化の目指すもの

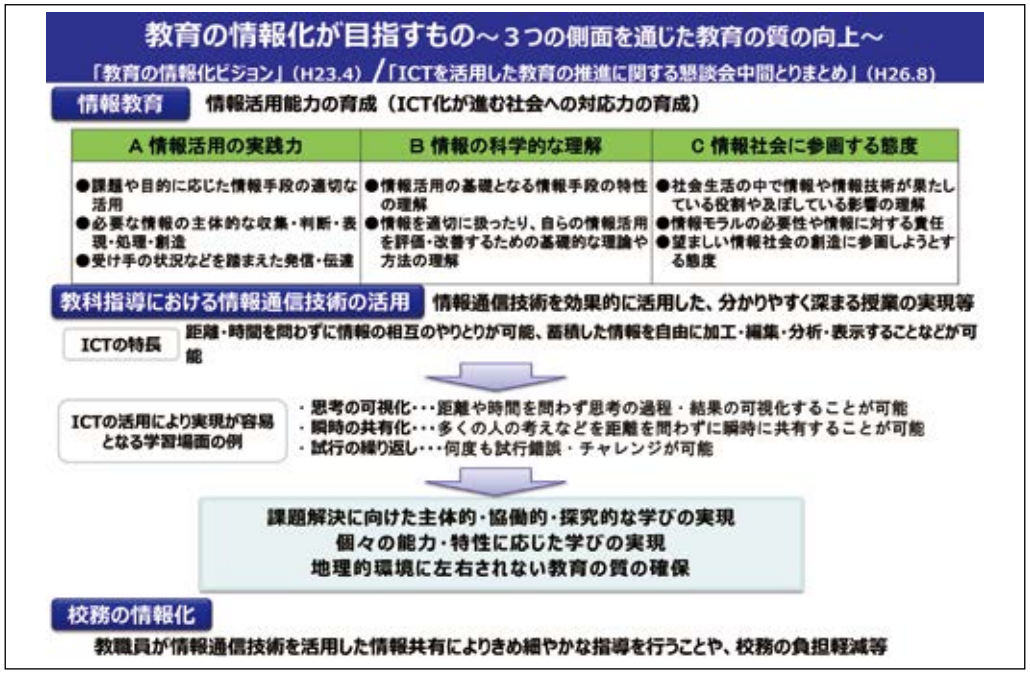
1.2.1　教育の情報化の重要性

「教育の情報化」とは、指導場面に着目した従来の整理とともに、昨今の教職員の事務負担の軽減等の観点も含め、

- 情報教育～子供たちの情報活用能力の育成～
- 教科指導でのＩＣＴ活用～各教科等の目標を達成する際に効果的に情報機器を活用すること～
- 校務の情報化～教職員の事務負担の軽減と子供と向き合う時間の確保～

の３つの側面があり、これらをそれぞれ充実していくことを通して教育の質の向上を目指すものです。(図表 1-11)

図表 1-11　教育の情報化が目指すもの



情報教育の側面では、社会がグローバル化、情報化の大きな動きの中でさまざまに変化していく中、子供たちが生涯を通して主体的に対応できるよう情報活用の実践力を育んでいきます。そのために、基礎となる情報手段の特性や情報を適切に扱うための基礎的な理論、方法などを学ぶとともに、情報や情報技術の役割、影響、情報モラル等を身に付け、望ましい情報社会の創造に対して積極的に参画する態度を養います。

教科指導における情報通信技術の活用については、授業や学習の指導案づくりから実践、評価におけるＩＣＴ活用の側面に着目しています。教職員が子供たちにとってわかりやすい授業、学習を実現していくことで、子供たちの「確かな学力」が身についていきます。特に、今後の学びの在り方として重視されているアクティブ・ラーニングの視点に立った学習を行っていったり、児童生徒数が非常に少ない山間部等の学校での「子供の関係固定化」、「自己の環境で得られにくい学習機会・教材が多い」といったさまざまな課題に対する支援を考えたりする際、ＩＣＴの活用は有効な手段と言えます。

しかし、指導案づくりや教材検討に十分な時間を割くことができない「教職員の多忙化」という問題が現実に存在しています。この点でも、校務支援システムの導入、活用などＩＣＴを活用した校務の効率化を図ることで、教職員の多忙感を解消し、子供と向き合う時間を確保していくこと、すなわち教育の質の向上が可能となります。

一方で、どれだけ効果が高いものであってもリスクの側面があることには注意が必要です。コミュニティサイトでの「ネットいじめ」、リベンジポルノなどのインターネット犯罪をはじめ、ＩＣＴが負の側面で使われていることは社会問題となっています。子供の生活時間もスマートフォンの利用等で大きく影響を受けており、依存症等の指摘がされる場合もあります。このような負の側面とそれに対する対処方法について、情報モラル／情報リテラシー教育を通じて子供自身及び保護者が正しく理解し適切に行動することがますます重要になっています。

教育におけるＩＣＴ活用を通じて教育の質を向上していくためには「教職員のＩＣＴ活用指導力の向上（研修等）、学校のＩＣＴ環境整備が必要であるとともに、教育の情報化を推進するための教育委員会や学校におけるサポート体制の整備が極めて重要である」「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」と言う点にも着目する必要があるでしょう。

1.2.2　情報教育の充実

■情報教育の目標

平成９年 10 月の「情報化の進展に対応した初等中等教育における情報教育の進展等に関する調査研究協力者会議」第１次報告において、情報教育の目標を次の３つの観点に整理しています。これら３つの観点は独立したものではなく、これらを相互に関連付けて、バランスよく身に付けさせることが重要です。

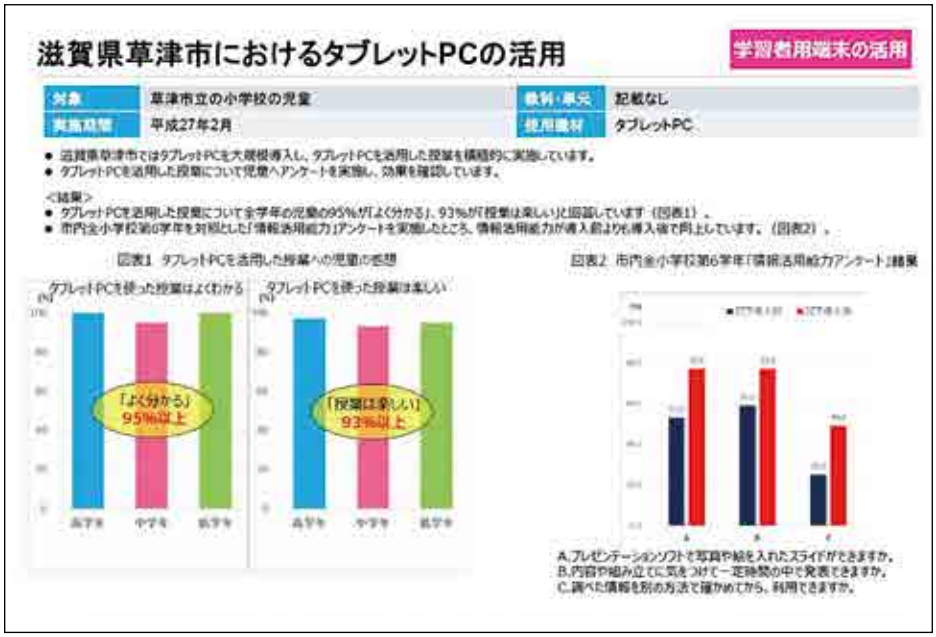
情報活用の実践力	課題や目的に応じて情報手段を適切に活用することを含めて、必要な情報を主体的に収集・判断・表現・処理・創造し、受け手の状況などを踏まえて発信・伝達できる能力
情報の科学的な理解	情報活用の基礎となる情報手段の特性の理解と、情報を適切に扱ったり、自らの情報活用を評価・改善するための基礎的な理論や方法の理解
情報社会に参画する態度	社会生活の中で情報や情報技術が果たしている役割や及ぼしている影響を理解し、情報モラルの必要性や情報に対する責任について考え、望ましい情報社会の創造に参画しようとする態度

これら３つの観点を重視することで、子供たちが社会の変化に主体的に対応するための基礎的な力である「生きる力」、情報社会に対応する「豊かな心」を身に付けることができるようになります。さらに、今後、情報活用能力を資質・能力の三つ目の柱によって捉えていくことで、教育課程全体を通じて体系的に育んでいくことが期待されます。

■情報活用能力への効果例

草津市では、タブレットＰＣを活用した授業について、児童へのアンケート調査を実施し、95% の児童が「よく分かる」、93% の児童が「授業は楽しい」と評価していることを明らかにしています。また、「プレゼンテーションソフトで写真や絵を入れたスライド」を作成する能力、「内容や組み立てに気を付けて一定時間の中で発表」する能力、「調べた情報を別の方法で確かめてから利用」する能力、といった情報活用能力（自己評価）についても、タブレットＰＣ導入の前後で大きく伸長していることが検証されています。（図表 1-12）

図表 1-12　タブレットＰＣの効果検証の例（草津市の例）



「ＩＣＴを活用した学習支援」の手引き（平成 28 年９月）より

1.2.3　授業・学習における効果的なＩＣＴ活用

■授業におけるＩＣＴ活用の本質的課題

単に授業でＩＣＴを活用すれば教育効果が期待できるわけではなく、ＩＣＴ活用の場面やタイミング、活用する上での創意工夫など教職員の授業設計が教育効果に大きく関わります。ＩＣＴを活用して学習指導の効果を高めるためには、ＩＣＴ活用と教職員の授業技術との関連を意識することが重要であり、「教職員がしっかり検討、設計した授業にＩＣＴの活用が有効に組み込まれることで、子供の学力向上につながる」と言えます。

子供の興味関心を高めるためにコンピュータや実物投影機等の映像をプロジェクターや大型ディスプレイ等で大きく映すのであれば、指導の狙いや子供の実態に応じた題材や素材を教職員が十分吟味して選んでいくことが重要です。また、その映像をタイミングよく教職員が提示し、教材を指し示しながら発問、指示や説明をしたりすることで子供の理解度向上が期待できます。つまりＩＣＴを活用する際、指導の狙いの整理、日頃からの子供の実態把握、授業における教材提示タイミング、発問、指示や説明といった基本的な学習指導の手法や設計とＩＣＴとを融合していく必要があるのです。ＩＣＴによる情報の提示は板書の代わりになるものではなく、提示した情報について説明等をした上で、従来とおり重要な点は板書をし、子供にノートをとらせる指導も必要となるため、ＩＣＴによる情報の提示と黒板が連携しやすいように機器等の配置を考えてみると良いでしょう。

一方、子供はＩＣＴ活用の際、提示された情報を見て、教職員の説明や指示等を聞き、それに対応する学習活動を行います。教職員の説明等を子供がしっかり理解するためにどのような情報をどのように提示したら良いか、設計することが重要です。ＩＣＴの特徴の一つである対話性（双方向性）の活用についても、教職員と子供間、子供同士とのやりとりを確実に行えるようにすることが重要です。高機能なＩＣＴ機器やアプリケーションを利用すること、操作が難しい仕組みを用いることが目的ではないことは自明です。学習効果を高めるためにどのようなコミュニケーションを教職員・子供が行うか、その中でＩＣＴを使うと何が良くなるのか見通しを立ててＩＣＴ活用を進めましょう。

■授業におけるＩＣＴ活用の課題

ＩＣＴ環境整備・活用について、多くの学校現場では以下のような課題を抱えていると推測されます。

- ☞各教科等の「学び」にどのようにＩＣＴを活用すれば「学び」が深まるのか、どのように授業でのＩＣＴ活用を進めていくべきか、学習指導要領との関係も不明確。
- ☞ＩＣＴを活用した授業で有効に活用できる教材、学びが深まる教材（コンテンツ・アプリケーション）が不足し、教職員・学校間での教材等の共有・活用も一部での取組にとどまる。
- ☞タブレットＰＣや電子黒板・提示機器等の機器や無線 LAN 等のネットワーク、システムなどの構築にコストがかかること、専門知識が必要となることで整備が進まず、教職員や子供が使いやすい状況になっていない。
- ☞授業に活用するためにどのような機器やシステムを整備すべきか、第２期教育振興基本計画に示された以上の詳細な基準がなく、地方公共団体や学校によって整備状況が異なる。特に教育用コンピュータは、平均で6.2人に一台の整備にとどまっており、地方公共団体や学校によってＩＣＴの活用に大きく差が生じる。
- ☞他方、一部の私立学校や高等学校においては、家庭の理解を得ながら、学校が指定するコンピュータを家庭で購入し、学校の授業等で活用する取組が行われているところが増えている。
- ☞障害のある子供に対するＩＣＴを活用した教育については認識が定着しつつあり、特に特別支援学校においては、他の学校種よりも教育用コンピュータの整備が進んでいる。
- ☞子供一人一人の障害の状態や発達段階等から生じる個別的教育的ニーズに応じＩＣＴ活用を図ることが必要。

■授業等での効果的なＩＣＴ活用の在り方

中央教育審議会「幼稚園、小学校、中学校、高等学校及び特別支援学校の学習指導要領等の改善及び必要な方策等について（答申）」（平成 28 年 12 月 21 日）においては、全ての学習の基盤となる言語能力や情報活用能力の育成及びアクティブ・ラーニングの視点から学習活動を改善していくことの重要性がうたわれています。

アクティブ・ラーニングは特定の単元のみでおこなわれるものではなく、各教科等の特質に応じ、課題の探究、解決、表現等全ての教科等における学習活動に関わるものです。これを継続的に実践していくためには、日常的にＩＣＴを活用できる環境整備が不可欠であるとされています。各教科等の学びを深める上で効果的なＩＣＴ活用の実践例や、個に応じた学習における活用の実践例を蓄積し、日常的・継続的・一般的なＩＣＴ活用を推進するための学習環境等について検証、検討が引き続き行われていきます。このような検証の際、学校種や発達段階に応じたＩＣＴ活用の在り方について留意する必要、プログラミング教育の重要性も指摘されています。

■ＩＣＴ活用事例（小学校、中学校）

教育におけるＩＣＴ活用の取組は全国で行われています。文部科学省の「ＩＣＴを活用した教育の推進に資す

る実証事業」、「学びのイノベーション事業」等の事例やインターネットで入手できる事例情報も参考にしてください。ここでは、特色のあるＩＣＴ活用を進めた事例を小学校、中学校それぞれ一例ずつ紹介します。

■小学校の例～仙台市立吉成小学校

仙台市立吉成小学校の総合的な学習の時間の取組“復興応援プロジェクト「元気のでるマガジンを作ろう」”。（図表 1-13）

図表 1-13　仙台市立吉成小学校の実践

資料出所：2016 年秋一般財団法人 コンピュータ教育推進センター主催「ＩＣＴ夢コンテスト」

▶活動目標

- ❖震災復興の現場を訪問し、見たり感じたりした内容をもとに、自分たちができることを考える。
- ❖テーマに基づき取材活動を行い、自分の思いや考えを表現する。
- ❖復興応援雑誌「元気のでるマガジン」を作る。

▶実践後の成果

- ❖ iPad、ＰＣの操作活動では、レイアウト、文章、写真、イラストなどの様々な場面で、児童一人一人の特性を生かした活動が展開される。
- ❖機器操作が不慣れな児童も積極的に取り組み力を発揮した。
- ❖ＩＣＴ機器を使用して目的に適う映像を児童に見せると、問題が可視化されるので児童の言語活動が豊かになり、教師の期待以上の効果を得ることができた。

■隠岐の島町立西郷中学校の取組

西郷中学校では以下の３点を狙いとして、ＩＣＴを活用した授業改善の取組を行っています。

①英語学習の楽しさや喜びを感じさせ、主体的に取り組もうとする意欲を高める。
②効果的な導入や繰り返し学習などを取り入れた「わかる授業」により、学習事項の定着を図る。
③他者との関わり合いを通して「つながり感」を得させ、温かい人間関係やコミュニケーション能力を育成する。

図表 1-14　隠岐の島町立西郷中学校の取組

資料出所：2016 年秋一般財団法人 コンピュータ教育推進センター主催「ＩＣＴ夢コンテスト」

予算の制約も厳しいため、オーディオプレーヤーなどの身近なＩＣＴ機器をアイディアと創意工夫で活用しています。（図表 1-14）

英語ではプレゼンテーションソフトによる単語練習、文型練習で発話量が増え、視覚による刺激を加えることで定着率が向上しています。他の教科でも短時間の学習活動を組み合わせて学習を構成する工夫をしたことで、生徒の集中力は大幅に向上し、時間が経つのを早く感じる生徒も多くなっています。

他者との関わりについては、グループ単位でデジタルカメラ等を活用する学習を意図的に実施したり、毎時間席替えをする等の工夫をしたりしたことで、生徒の人間関係への不安感を軽減し、相手のことを考えて関わり合おうとする思いやり、コミュニケーション能力を育むことに有効に働いています。

一方、ＩＣＴ教材の多くを自作しているため、準備に時間がかかり敬遠する教職員が存在すること、教職員のＩＣＴ活用指導力に個人差が大きく、授業のアイディアを共有しても実践につながらないこと等が課題となっています。また、今後はＩＣＴ教材を自校内、他校の教職員とも共有し、誰もが活用できるようにするための環境整備が必要と考えています。

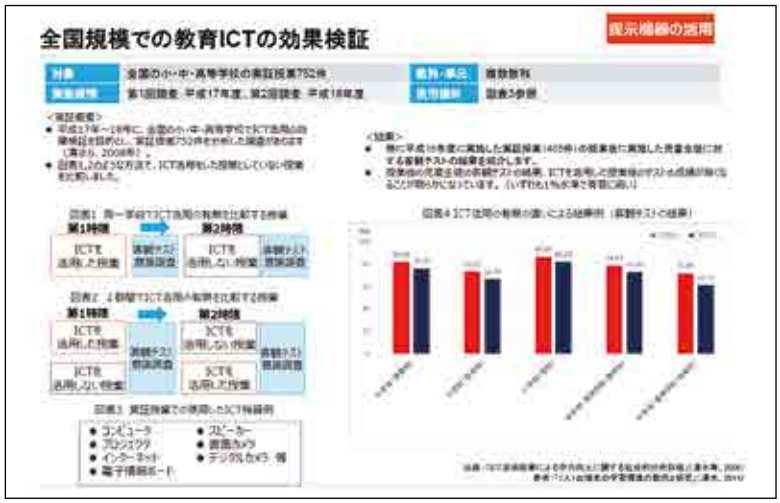
■ＩＣＴ活用の効果検証

教育ＩＣＴの普及初期に、全国の小中高校で多数（752 件）の実証授業を実施し、ＩＣＴ活用効果を検証した調査研究事例があります。（図表 1-15）「コンピュータ」「プロジェクター」「インターネット」「電子情報ボード」「スピーカー」「書画カメラ」「デジタルカメラ」等のＩＣＴ機器を授業で用い、

- ❖同一学級で『ＩＣＴ活用授業』を実施した後で『ＩＣＴ非活用授業』を実施し、各授業後の「客観テスト」「意識調査」の結果を比較
- ❖『ＩＣＴ活用授業』を実施した後で『ＩＣＴ非活用授業』を実施する群と、『ＩＣＴ非活用授業』を実施した後で『ＩＣＴ活用授業』を実施する群を設け、各授業後の「客観テスト」「意識調査」の結果を比較

の方法により、検証をした結果、授業後の子供の客観テストの結果、ＩＣＴを活用した授業後のテストの成績が統計的に有意に高くなることが明らかになっています。

図表 1-15　全国規模での教育ＩＣＴの効果検証の例



「ＩＣＴを活用した学習支援」の手引き（平成 28 年９月）より

■タブレットＰＣ効果検証

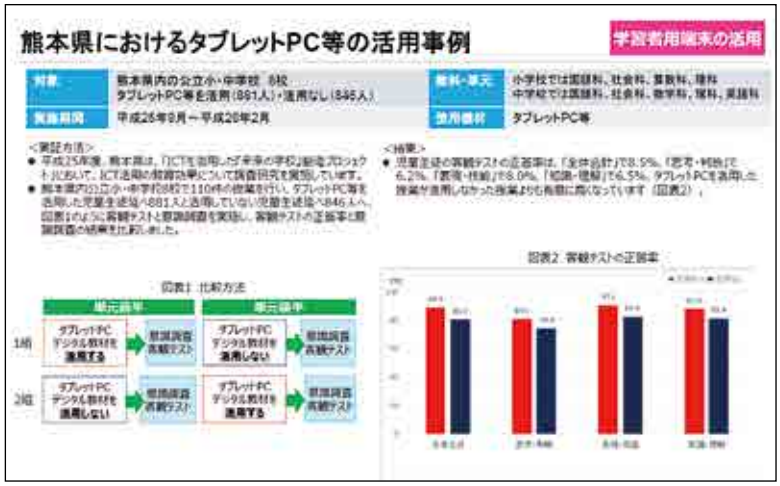
最近では、平成 26 年度に文部科学省が「ＩＣＴを活用した教育の推進に資する実証事業」として、教育効果の検証方法を示す取組を行いました。（図表 1-16）この検証方法は、タブレットＰＣを授業で活用する際の効果を検証する調査研究事例の手法を用いて実施しました。熊本県では県内小中学校で

①単元前半において『ＩＣＴ活用授業』を実施した学級と『ＩＣＴ非活用授業』を実施した学級を設定
②単元後半で『ＩＣＴ非活用授業』と『ＩＣＴ活用授業』を逆転させて実施
③各授業後の「客観テスト」、「意識調査」の結果を比較

という方法により 110 件の授業を行いました。授業後の児童の客観テストの成績を比較検討したところ、タブレットＰＣを活用した授業の方が、タブレットＰＣを活用しなかった授業に比べて正答率が有意に高いことが分かりました。（図表 1-17）

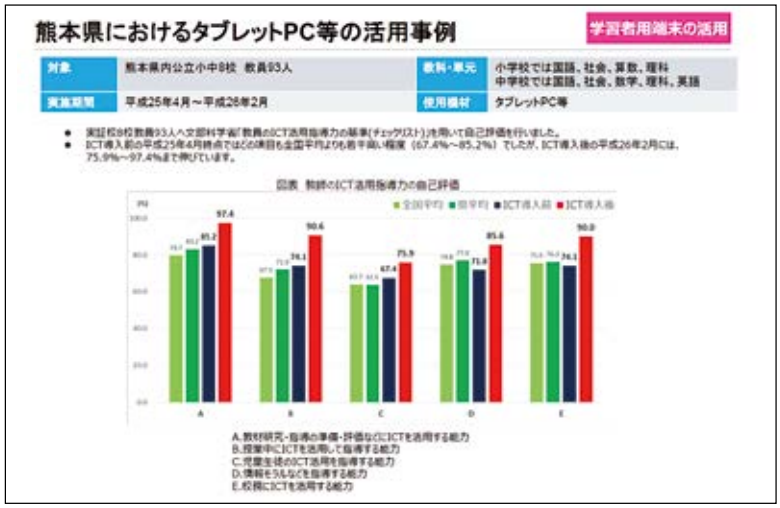
また、タブレットＰＣを活用した授業を実施することにより、教職員のＩＣＴ活用指導力（自己評価）が上昇することも分かりました。ＩＣＴを実際に活用することは、教職員のＩＣＴ活用指導力も伸ばすと言えるようです。

図表 1-16　タブレットＰＣの効果検証の例（熊本県の例）



「ＩＣＴを活用した学習支援」の手引き（平成 28 年９月）より

図表1-17　タブレットＰＣを活用した授業を実施した教職員のＩＣＴ活用指導力の変化



「ＩＣＴを活用した学習支援」の手引き（平成 28 年９月）より

1.2.4　校務支援システムの活用による業務の効率化

■統合型校務支援システムによる業務改善

○「統合型校務支援システム」とは
　教務系（成績処理、出欠管理、時数等）、保健系（健康診断票、保健室管理等）、指導要録等の学籍関係、学校事務系など統合して機能を有しているシステム。

○「校務支援システム」とは
　校務文書に関する業務、教職員間の情報共有、家庭や地域への情報発信、服務管理上の事務、施設管理等を行うことを目的とし、教職員が一律に利用する単機能のシステム。

図表１-18　業務改善プロセス（例）

　統合型校務支援システムの効果的な導入によって、教職員１人当たりの事務業務を年間 100 時間以上削減できたという教育委員会がいくつも存在します。同じ情報を複数の書類に転記する手間を削減できること等による時間の創出はもちろんのこと、ＩＣＴの活用による情報共有の徹底、職員会議等の会議回数の削減など学校内の業務のやり方を少しずつ変えていくことによって、子供と触れ合う時間や教材研究に時間を割く余裕が生まれます。このような業務改善を進めるためには、アイディアを出し合って実践した後の効果を的確に測定していくことが重要となります。また、教育委員会も活用推進に積極的に介在し、効果のある使い方を他校にも共有していくことで、地方公共団体全体での業務改善が推進されます。

■大阪市の事例

　大阪市では、教職員の校務負担、特に教頭への校務の集中が課題となっていたことから、「ＩＣＴの活用により教職員が児童生徒と向き合う時間を増やす」ことを目的として、平成 23 年度より校務支援ＩＣＴ活用事業を進めてきました。

　具体的には、統合型校務支援システムを導入することによって、

- ❖学校教育の質の向上、学校経営の効率化・高度化を図る
- ❖学校から保護者・地域への情報発信を促進する
- ❖教職員のＩＣＴリテラシーの向上と情報セキュリティの強化

を進め、教職員１人あたり年間 100 時間の児童生徒と向き合う時間の増加（KPI（Key Performance Indicator）重要業績評価指標）を目指しています。

　大阪市では、校務が多忙かつ負担となっているために、本来業務である教育に時間が割けない状況を段階的に解消する計画を立て、既に校務課題の多くは解消し、現在はシステム活用による教育の質の向上に転換中としています。

図表１-19　大阪市の統合型校務支援システムのイメージ

図表１-20　大阪市の校務支援ＩＣＴ活用事業の成果

　グループウェア・校務支援サービスと勤務情報システムの導入の結果、平成 26 年度には、教頭で年間約 230 時間、担任で年間約 224 時間、に相当する時間の校務効率化を実現することができ、１日あたりに換算すると、１時間程度、教員が子供と向き合う時間を増やすことができる成果をあげています。

1.2.5　教育の情報化の整備ステップ

学校におけるＩＣＴ環境の整備に当たっては、地方財政措置が講じられています。第２期教育振興基本計画の目標水準を達成するため、教育のＩＴ化に向けた環境整備４か年計画（平成 26 年度から 29 年度）に沿って、単年度で約 1,678 億円を計上しています。（図表 1-21）文部科学省では、教育委員会に対し、学校のＩＣＴ環境整備の狙いや効果、地方財政措置の内容について周知するなど学校におけるＩＣＴ環境の整備の取組を促進しています。

図表１-21　教育のＩＴ化に向けた環境整備４か年計画

教育の情報化の推進に向けた取組について、文部科学省の「2020 年代に向けた教育の情報化に関する懇談会」において今後の方向性が議論されました。その最終まとめで示されたアクションプランをもとに、昨年７月、「教育の情報化加速プラン（平成 28 年７月 29 日文部科学大臣決定）」を策定しました。

■教育の情報化の加速化に向けた主な施策、検討事項

平成 28 年７月 29 日、「2020 年代に向けた教育の情報化に関する懇談会」の最終まとめで示されたアクションプランを基に、次期学習指導要領を見据えた情報活用能力の育成や教科指導におけるＩＣＴ活用の充実，学校におけるＩＣＴ環境整備を加速させる等の観点から、「教育の情報化加速化プラン」（文部科学大臣決定）（以下、「加速化プラン」）を策定しました。（図表 1-22）

図表１-22　教育の情報化加速化プラン

未来社会を見据えて育成すべき資質・能力を育むための新たな「学び」や，それを実現するための「学びの場」を形成するためには、ＩＣＴを効果的に活用する必要があります。「加速化プラン」においては、2020 年代に向けた教育の情報化に対応するため、おおむね５年を対象とした今後の対応方策について示しています。

主な施策としては，児童生徒一人一台の教育用コンピュータ環境の実現を目指し、効果的なＩＣＴ活用の在り方の明確化とそれに基づく機器等の計画策定等を行うとしています。また、校務面のＩＣＴ活用として統合型校務支援システム普及推進や、システム・ネットワーク調達改革・標準化、セキュリティポリシーガイドラインの策定をはじめとするデータ管理・情報セキュリティに対する考え方の確立等について検討することとしています。そして、授業・学習面・校務面での活用に向けて、教材開発等官民連携コンソーシアム構築や、スマートスクール（仮称）構想実証などの取組が示されています。

さらに、ＩＣＴによる地方公共団体と地域，学校の連携として，教育委員会・学校の体制整備（首長部局連携等）及び産学官連携支援体制の構築についても盛りこまれています。

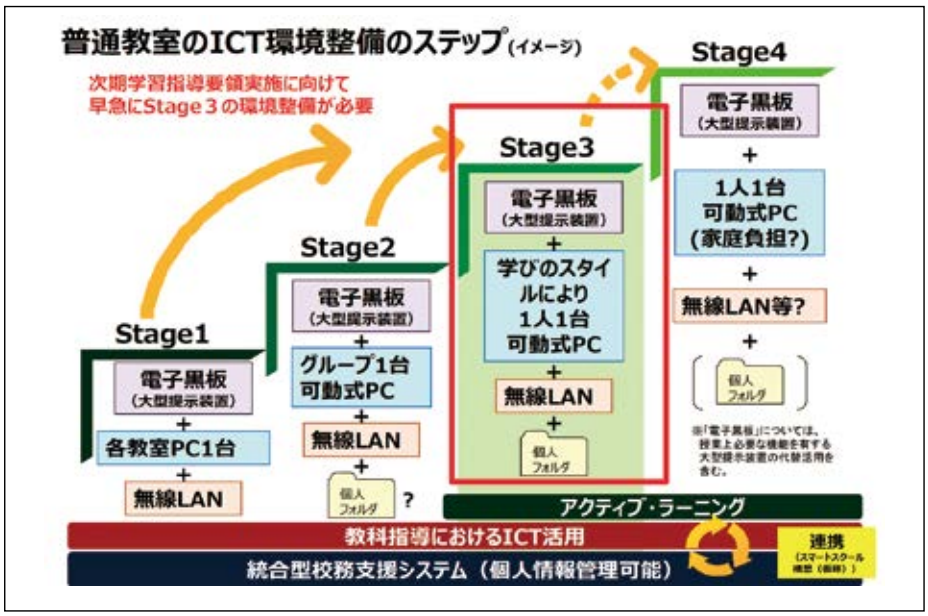
■教育の質的改善とＩＣＴ環境の段階的整備

「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（3 教職員・学校が使いやすく教育の質的改善

につながるＩＣＴ環境の段階的整備）では、教育の質的改善とＩＣＴ環境の段階的整備について、以下の内容をポイントとしてあげています。

- ☞教育現場でのＩＣＴの活用は、授業・学習と校務の両面で教職員をサポートするものであり、情報セキュリティの確保を大前提とした上で、学校・教職員が使いやすいものにするという視点からの取組が必要
- ☞ＩＣＴの活用により、教職員の指導力の向上につながり、子供たちと向き合う時間も増え、教育活動の質の向上につながる。その際、教職員や子供を守るという視点も重要（安心・安全に情報の利活用を行うことができる情報セキュリティの確立や、情報モラルを含めた情報活用能力を身に付けていくことが必要）
- ☞国においては、地方公共団体や学校のＩＣＴ環境の実態を踏まえつつ、地方公共団体や学校が、段階的に目標を設定し、教育のＩＣＴの活用に取り組めるような支援策を行っていくことが必要

図表 1-23　第２期教育振興基本計画におけるＩＣＴ環境整備目標の考え方の再整理と第３期教育振興計画に向けた検討事項について（イメージ）



これらの取り組み姿勢を前提とし、ＩＣＴ環境整備のステップを以下の図表のとおり４つのステージに分け、ステップアップするイメージを提示されています。（図表 1-23）

アクティブ・ラーニング推進の趣旨を踏まえるとステージ３以降が、より積極的なＩＣＴ環境整備の新しい段階と見ることができます。

■第３期教育振興基本計画に向けた具体的なＩＣＴ環境整備目標（検討事項）

教育の質的改善とＩＣＴ環境の段階的整備として、第３期教育振興基本計画に向けた具体的なＩＣＴ環境整備目標に向けた検討事項が以下のとおり提示しています。

- ☞教職員が必要なときに、児童生徒一人一台分の教育用コンピュータ環境で授業が行えるようにするための教育用コンピュータの整備の在り方
- ☞大型提示装置やネットワーク環境（学習系システム含む）の在り方、今後の校務の情報化も見据えた校務用コンピュータの在り方等について（次期学習指導要領に向けた中央教育審議会における議論や学校現場の現状等も踏まえながらさらに検討を深めていく）

●【参考】教育の情報化動向や教材等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　中央教育審議会　教育課程部会　次期学習指導要領等の検討状況
http://www.mext.go.jp/b_menu/shingi/chukyo/chukyo3/004/index.html

文部科学省ホームページ　教育の情報化の推進
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/

内閣府ホームページ　青少年のインターネット利用環境実態調査
http://www8.cao.go.jp/youth/youth-harm/chousa/

国立教育政策研究所ホームページ　教育情報共有ポータルサイト（ＣＯＮＴＥＴ）
https://www.contet.nier.go.jp/

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/

一般財団法人 日本視聴覚教育協会ホームページ
http://www.javea.or.jp/

公益財団法人　パナソニック教育財団ホームページ
http://www.pef.or.jp/

第２章　学校の情報化に必要な情報セキュリティとは

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

皆さんの学校にはどのような情報がありますか？　また情報が外部に流出するなどの事故が起こったらどのような影響があるでしょうか？　情報セキュリティを考えていくに先立って、ご自身が持っているイメージを書き出してみましょう。

2.1.1　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 2-1　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 2-2　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」

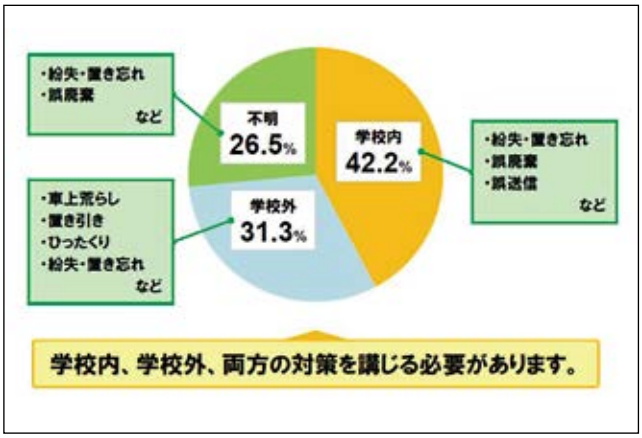
学校における情報セキュリティの実態等を調査している非営利団体教育ネットワーク情報セキュリティ推進委員会（略称ＩＳＥＮ）によれば、平成 27 年度は全国で 166 件の個人情報漏えい事故が発生しており、のべ 340,701 人の個人情報が漏えいしています。

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 2-3）

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。

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 2-4）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 2-3　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」

図表 2-4　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」

■学校における個人情報

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。

学校において、取り扱うことが多い個人情報には、たとえば「児童生徒名簿・職員名簿・ＰＴＡ役員名簿」等の名簿類、「健康状況調査表、身体検査診断票、保健日誌」等の保健関係書類、「家庭状況調査書、成績原簿、進路指導記録」等の児童生徒及び保護者に関する情報などがあります。

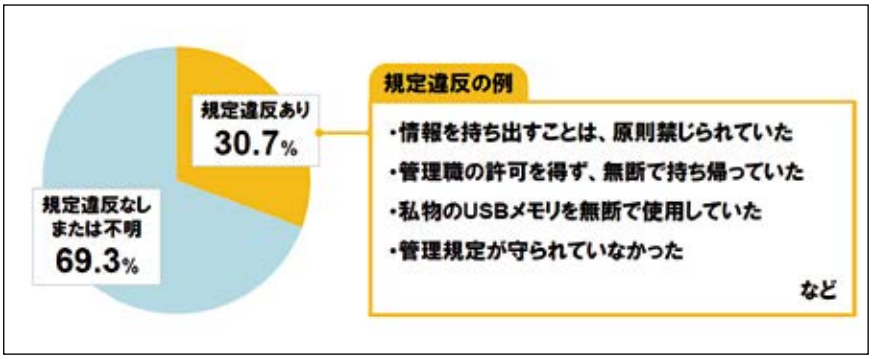
地方公共団体については、個人情報保護法に準じた個人情報保護条例が制定され、個人情報の対象、個人情報取得のルール、個人情報保管・管理のルール、個人情報の第三者への提供のルール、などが規定されています。地方公共団体が設置者となる公立学校においても、当然に個人情報の保護に努めなくてはなりません。また、平成 28 年から、国民一人一人が持つユニークな 12 桁の番号によって表される「個人番号（マイナンバー）制度」の利用が開始されました。個人情報にマイナンバーが含まれると、単なる個人情報ではなく、「特定個人情報」という情報と位置付けられ、マイナンバーによって名寄せが行われるリスクがあることから、個人情報保護法よりも厳しい保護措置が義務付けられています。

たとえば個人情報保護法では、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、地方公共団体の就学援助の手続きに関わるなど、マイナンバーを取り扱う場合には極めて厳重な運用が求められます。

■個人情報の保護

個人情報を保護するためには、組織ごとに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。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情報セキュリティ事故が多数発生しているのも事実です。（図表 2-5）

図表 2-5　規定違反を伴う事故の発生比率



資料出所：ＩＳＥＮ

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当然です。

しかしながら、情報セキュリティは、常にユーザビリティ（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、教職員等の日常業務に支障を来すようになると、ルール違反の行為が陰に陽に行われるようになり、却って情報セキュリティレベルを下げる結果に陥りがちです。ルールをいったん制定した後も実際の運用状況を確認し、課題を抽出してルールを見直すことで、最適なルールを作りあげ情報セキュリティを確保していく必要があります。

■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、文部科学省は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）

＜教育情報セキュリティのための緊急提言＞

平成 28 年 8 月 5 日、「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。緊急提言の内容と対策をしないことによる脅威は以下のとおりです。（図表 2-6）

図表 2-6　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

2.1.2　学校の情報資産

前項では学校における情報セキュリティ事故の概況を確認しましたが、情報セキュリティは単に情報の漏えいを防ぐことだけではなく、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「情報の機密性」、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「完全性」、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「可用性」を維持することです。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。（図表 2-7）

図表 2-7　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

つまり、「守るべき情報」が存在し、それが正当な使用者によって適正に使うことができる状態を維持するためにさまざまな仕組みを用意し、その仕組みが正しく動くようにすることが情報セキュリティを確保する上では必要となります。この「守るべき情報」を情報資産と表現します。情報資産とは、教育活動を行うために必要とされる情報を意味し、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。（図表 2-8）

図表 2-8　情報資産のイメージ

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などのメディアを指します。

学校における情報資産は、下図のとおり「校務系情報」と「学習系情報」に分類できます。校務系情報には個人情報等、機密情報が多く、特に保護する必要があります。（図表 2-9）

図表 2-9　学校における情報資産の分類

校務 / 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、児童生徒の情報をはじめ、さまざまな情報資産を有しています。たとえば、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。

情報セキュリティを確保するため、それぞれの教職員は「情報資産の洗い出し」あるいは「洗い出した結果の確認」

が必要です。学校で取り扱う情報の中には、児童生徒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リストとして管理します。

情報資産のリストについては、さらに保存形態（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、整理し現行化を図ります。（図表 2-10）は、学校内情報資産リストの例です。

図表 2-10　学校内の情報資産リストの例

種別	情報資産	管理者	作成者	保存形態	保存場所	公開対象者	主な記載内容	重要度
学籍関連	学校沿革史	校長		紙			学校の沿革	大
	卒業生台帳	教頭		紙			卒業生の氏名、住所、生年月日等	大
	同窓会名簿	教頭		電子媒体	サーバー	校内	卒業生の氏名、住所、生年月日等	大
	学校要覧	教頭		電子媒体	サーバー	一般	学校の沿革、職員等の現況	小
	教育計画	教務主任		電子媒体	サーバー	一般	学校の指導計画一覧	小
	指導要録（学籍）	学籍		紙			児童生徒の氏名、住所、保護者等	大
	出席簿	出席統計		紙			出欠席の状況	大
	生徒(児童)名簿	教頭		電子媒体	サーバー	校内	生徒の氏名、住所、生年月日等	大
	転出入関係書類	転出・転入		紙		職員	生徒，保護者の氏名，住所，在籍校	中
	記載事項変更書類	学籍担当		紙		職員	生徒の氏名、住所、保護者等の変更事項	大
成績関連	定期考査問題	教務主任		電子媒体	USB	職員	試験問題	大
	成績一覧	教務主任		電子媒体	サーバー	職員	評価結果	大
	通知票	教務主任		紙			評価結果	大
	通知票の下書き	担任		電子媒体	ＵＳＢ		評価結果	大
	学習履歴控え	担任		紙			学習の到達等の状況	大
	学力テスト結果	教務主任		紙			個別の学力テストの結果	大
	知能検査結果	教務主任		紙			知能検査の結果	大
	特別活動記録	教務主任		紙			特別活動の参加状況	小
	ポートフォリオ	担任		紙			学習の状況，履歴	小
	評価基準	教務主任		電子媒体	CD	校内・保護者	各学年，教科毎の評価基準	中
生徒指導関連	家庭環境調査	教頭		紙		職員	氏名，住所，連絡先，保護者等	大
	緊急連絡網	教頭		電子媒体	サーバー	校内・該当学級	氏名，連絡先	大
	事故報告	教頭		紙			氏名，事故状況	小
	教育相談記録	教育相談		紙			氏名，相談内容	
	指導記録	生徒指導		紙			氏名，指導状況	
	在校生顔写真	教頭		紙		職員	氏名，	
	所属別名簿	教頭		電子媒体	USB	校内		
	健康診断票	養護教諭		紙				
	[illegible]	養護教諭		紙				
	[illegible]	養護教諭		紙				

〈セキュリティポリシー対象範囲〉

情報資産	管理者	作成者	保存形態	保存場所	公開対象者	主な記載内容	重要度
生徒(児童)名簿	教頭		電子媒体	サーバー	校内	生徒の氏名、住所、生年月日等	大
同窓会名簿	教頭		電子媒体	サーバー	校内	卒業生の氏名、住所、生年月日等	大
定期考査問題	教務主任		電子媒体	USB	職員	試験問題	大
成績一覧	教務主任		電子媒体	サーバー	職員	評価結果	大
緊急連絡網	教頭		電子媒体	サーバー	校内・該当学級	氏名，連絡先	大
保健統計	養護教諭		電子媒体	サーバー	校内・保護者	健康状況の統計データ	大
入試成績	担任		電子媒体	サーバー	校内	氏名，成績	大
調査書	担任		電子媒体	サーバー	校内	氏名，成績，履修状況	大
通知票の下書き	担任		電子媒体	ＵＳＢ		評価結果	大
所属別名簿	教頭		電子媒体	USB	校内	氏名，所属	中
評価基準	教務主任		電子媒体	CD	校内・保護者	各学年，教科毎の評価基準	中
学校要覧	教頭		電子媒体	サーバー	一般	学校の沿革、職員等の現況	小
教育計画	教務主任		電子媒体	サーバー	一般	学校の指導計画一覧	小
進路結果	進路指導		電子媒体	CD	一般	氏名，進路先	小

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」

これらの情報資産に対し想定しうる脅威を洗い出し、脅威の大きさをおおよそ、大･中･小の三段階程度に分類し、リスクの評価を行うことが必要です。情報資産も多少欠落しても回復が可能なものもあり、一部でも欠落等が許されないもの（原本等）もあるため、それらも考慮し情報資産のリスク評価をします。

情報資産への脅威に対して、学校がどのくらい弱いのか正確に認識しなければ情報セキュリティを維持・確保することはできません。情報資産の状況やリスクは、情報セキュリティの運用に際しても教職員一人一人が常に理解しておかなければならない事項と言えます。

2.1.3　情報セキュリティの脅威

前項では「脅威」という言葉が繰り返し使われました。情報は常に脅威にさらされているため、洗い出した情報資産をどのようにして守って行くのか、検討は必須です。まず、脅威とはどのようなものか、イメージをつかみましょう。

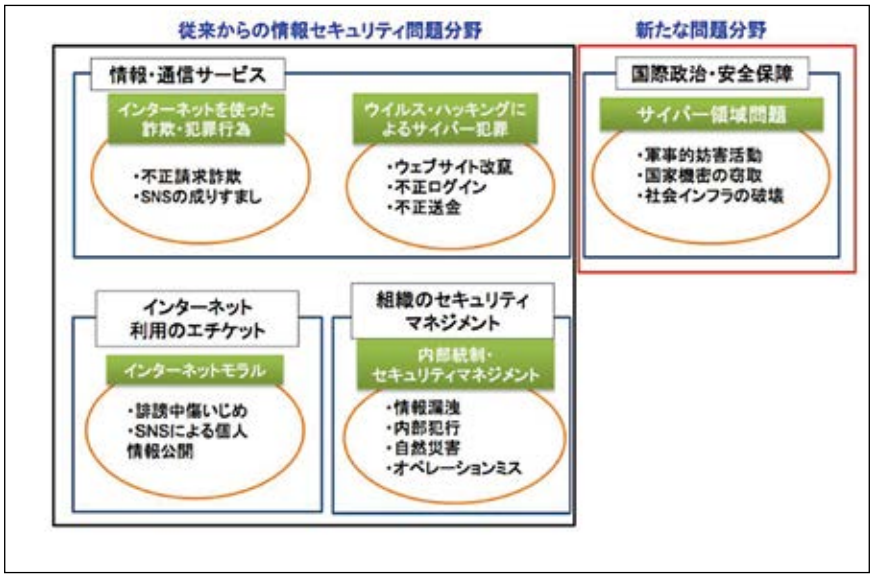
■脅威の種類

「脅威」とは、組織に損害や影響を与える可能性であるリスクを引き起こす要因です。

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 2-11）

図表 2-11　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）

■脅威の例

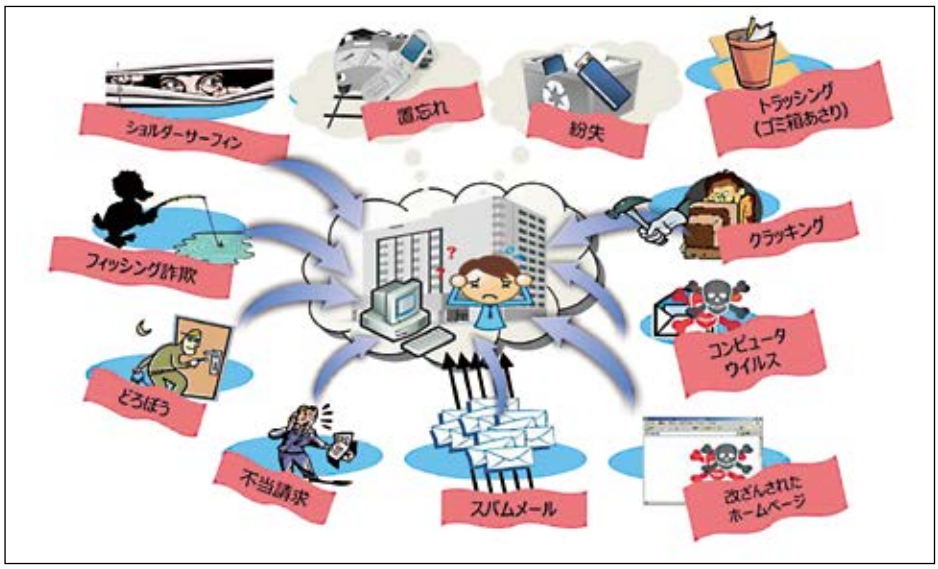
脅威とは、自然災害や機器障害、悪意のある行為などのように、情報資産に損害をもたらす要因です。

学校でも、パソコンの紛失・盗難による児童・生徒の重要な情報の漏えい、ウイルス感染、ファイル共有ソフトによる情報流出など多くのトラブルが発生しています。代表的な脅威には以下のものがあります。

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。

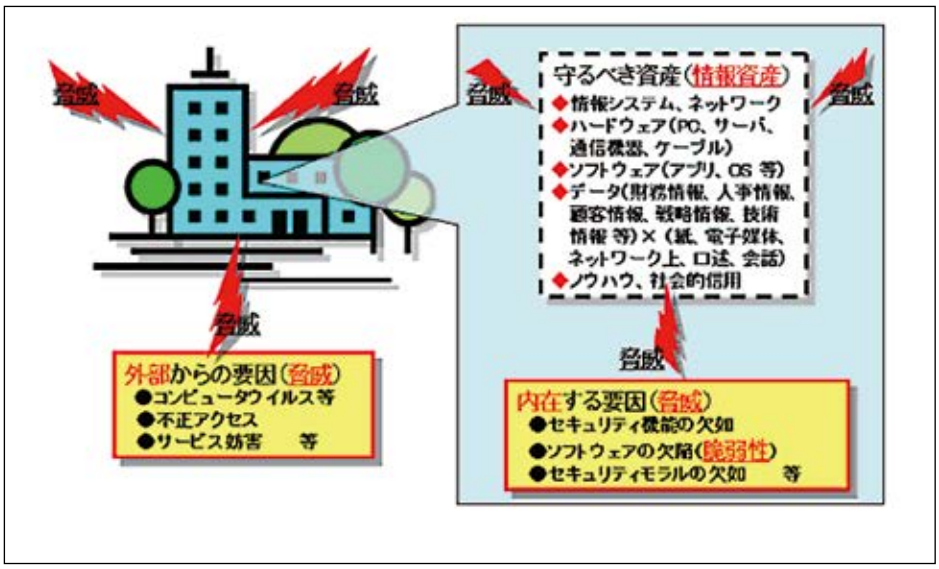
脅威はこれらに限りません。図表 2-12 のように、実にさまざまな脅威が情報資産を取り巻いているのです。

図表 2-12　情報資産を取り巻く多種多様な脅威



「守るべき資産（情報資産）」に対して、外部並びに内部にはさまざまな脅威が存在しています。（図表 2-13）

図表 2-13　情報資産に対する内外の脅威



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

◉ 2.2　教職員に求められる情報セキュリティ

2.2.1　情報セキュリティの基本動作

「正当なユーザにはサービスを提供し、正当でないユーザは拒否する」ことが情報セキュリティ対策の基本原則です。

この基本原則を守るために、環境面からのアプローチ（物理的対策･技術的対策）、運用面からのアプローチ（管理的対策・人的対策）が行われる訳ですが、多額の費用を投じて構築し運用されるシステムのセキュリティが意外に小さな抜け穴から崩壊することもあります。

多くのシステム・情報資産へのアクセスには認証が必要とされるケースが多いことは既に述べましたが、同僚や児童生徒に対して認証のカギとなるモノ（例：職員証）を一時的に貸与したり、パスワードを教えたり、といった経験はないでしょうか。これらの行為は、本来、情報資産にアクセスしてはいけない人がアクセスできる状態を作り出してしまっている可能性があります。

これまでも、システムのパスワードを付箋紙に書いてパソコンに貼り付けている、などといった事案もありましたが、本当にそのような光景は見られないでしょうか。逆に、パスワードを手帳や書類に記入して保管していたのに、無くしてしまって、必要なタイミングで必要な情報資産にアクセスできない、といった事象も情報セキュリティ上の事故と言うこともできます。このような行為は、気軽に行ってしまう割には、情報資産に大きな損害を与える可能性があります。逆に、極めて簡単な基本動作を徹底するだけで、リスクを低減することができるとも言えるでしょう。

また、オンラインでファイルを送信したり物品を購入したりするといったやり取りの際、機密性の高い情報を平文のまま送信してしまうケースもありますが、たとえば、Web サイトに表示される URL を確認する（URL が http:// ～ではなく https:// ～と表記される）だけで、Web サーバと Web ブラウザの間の通信が暗号化されていることを確認できます。このように、極めて簡単な URL 確認という基本動作を徹底するだけでリスクを低減することができます。（図表 2-14）

次ページから、教職員が守るべき基本動作十か条をまとめています。

図表 2-14　情報資産・脅威・脆弱性と情報セキュリティ事故の関係

2.2.2　情報セキュリティ十か条

教職員が情報セキュリティを確保するために守ってほしい十のポイントを確認してください。

■データや書類の管理

一　データ持ち出しルールを確認する。記録メディアは暗号化対応タイプのみを使用

ＵＳＢメモリーなどの記録メディアは大量のデータを手軽に格納して運ぶことができるため、学校現場に限らずさまざまな場所で使用されています。しかし、データを持ち出すことで情報漏えいの危険性は間違いなく高まります。仕事上やむを得ずデータを持ち出さなければならない場合、「持ち出し記録簿に記入して管理職の承認を得る、常に携行する」など、学校で定められた手続きを確認し、それに則って対処することが教職員自らの身を守ります。

また、万が一持ち出した記録メディアが電車での置き引きや車上荒らし等により盗難にあったり、紛失してしまったりした場合、パソコン等に差し込むだけで中のデータが確認できる状態は、財布を開いて歩いているようなものです。財布の中のお札を見えなくするように、記録メディアに暗号化機能がついているものを使用し、第三者が簡単に操作できないようにすると良いでしょう。暗号化の機能が付いた記録メディアが学校で準備されていない場合は、パスワード等で暗号化・復号化ができるソフトウェアを使用する（後述する「三．パスワードは桁数、字種と推測困難性を兼ね備えたものを」を参照）など、ひと手間かけるだけで情報セキュリティ事故の可能性をおさえることができます。

二　クリーンデスクを徹底。共用書類や物品は定位置に戻す。廃棄ルールを作る

廃棄した書類やメモなどに個人情報等の機密情報が含まれていることがあります。また、短時間であっても席を離れるときには、児童生徒や学外者に機密情報を含んだ書類をのぞき見されたり、盗まれたりする恐れが無いとは言えません。

離席、帰宅する時はＰＣをログオフし、共用の物品や書類は元の位置に戻す、個人の書類は引き出しにしまうことを徹底する必要があります。コピー機やプリンターに作業結果などをプリントアウトした場合には放置せず、迅速に回収することを習慣化してください。また、学校全体で廃棄ルールを作ると良いでしょう。機密情報等を含む書類はシュレッダーにかけたり書類廃棄サービスを利用したりします。ＰＣや記録メディアの処分時は、データを完全に消去するソフトウェアや業者のサービスを活用して、情報漏えいを未然に防ぐようにしましょう。

■ＰＣのログオン、パスワード、ファイル等の管理

三　パスワードは桁数、字種と推測困難性を兼ね備えたものを

パスワードの設定は、システム毎、組織ごとにさまざまな考え方があり、一概にルールを決めることは容易ではありません。ここでは共通的な事項と、安全なパスワード運用の例を挙げます。

- ８ケタ以上、英大文字小文字、数字、記号などから３種類以上の字種を用いたパスワードにする。
- 生年月日や姓名のアルファベット表記などをそのままパスワードにしない。
- ＩＤとパスワードを容易に人目に触れるところにさらさない。記憶が難しい場合は、パスワードを記した紙を鍵のかかる引き出しに格納する等、パスワード記録にもセキュリティ措置を施す。
- ＩＤやパスワードを記録した電子ファイルを扱う時は、必要最小限の人しかアクセスできないよう、ファイル自体にパスワードを設定し、他の人がアクセスできないフォルダに格納する。
- 指紋などの生体情報や教職員のみに渡されたＵＳＢキーなど、ＩＤ／パスワード以外に利用者固有の情報を用いてシステムへのアクセスを行う二要素認証の仕組みが利用可能な場合は、積極的に使う。

四 機密情報を格納するフォルダにはアクセス権を設定。機密情報を含むファイルは暗号化またはパスワードを設定

機密情報をまもるためには、そもそもその情報にアクセスできる利用者を限定することが有効です。コンピュータのファイルフォルダにはアクセスできる人を限定したり、利用者によって閲覧のみを可能とするといった権限を設定したりすることができます。また、ファイルにもソフトウェアでパスワードをかけたり暗号化をしたりすることが可能です。手順や必要なソフトウェアについては、参考情報リストで確認してください。

■電子メール、Web アクセス、ソフトウェア、機器等の管理

五 電子メールの宛先、送信元確認、添付ファイル確認は念入りに

電子メールは、いったん送信すると宛先を修正したり取り消したりすることが不可能です。多くの電子メールソフトでは、過去に送信した履歴やアドレス帳のデータを元に、宛先のメールアドレスを補完入力する機能を備えていますが、便利な機能ゆえに指定間違いが起こりやすいという短所もあります。手入力もタイプミスによる送信ミスが起こりやすいため、一長一短ですが、いずれの方法を採る場合でも送信前に正しいアドレスであることを必ず確認しましょう。

メーリングリストで広い範囲に情報共有を図っているケースもありますが、電子メールソフトの「返信」「全員に返信」の確認をしないで送ると、送信者のみに送ったつもりでもメーリングリスト参加者すべてに情報が行きわたってしまうことがあります。

また、近年急増しているマルウェアには、電子メールの添付ファイルによって感染するものもあります。パソコン内のファイルを利用者が知らない間に外部のサーバへ送ってしまったり、勝手に暗号化して使えなくしてしまったりするものもありますので、普段やり取りしない相手から送信されたメールに添付ファイルがある場合は、送信元が信頼できるかしっかりと確認すべきです。

六 マルウェアやファイル共有ソフトは要注意

一昔前のインターネット上での悪意は、マルウェア（コンピュータウイルス）による利用者への妨害行為が主流でしたが、近年は金銭の詐取を目的として利用者が気付かないものが増えています。マルウェアは悪意を持ったWeb サイトへのアクセスで感染することも多いので、Web ブラウザによるサイトの評価機能などを参考に、怪しいサイトにはアクセスを避けることが重要です。最近は、政府機関、仕事の関係者、友人・知人を装って、マルウェア付きの電子メールをて送りつける標的型と呼ばれる攻撃も多くなっています。標的型攻撃ではメール受信者の不信感を低減させるさまざまな「だましのテクニック」（受信者の興味をひくような件名や本文、関係者を装った差出人、ファイル名やアイコンで文書ファイルに見せかける等）を駆使し、添付ファイルを開かせようとします。

添付ファイル等を開いた瞬間に、自分の意志ではなくダウンロードが発生したら即座にキャンセルしてください。ＰＣのＯＳ（基本ソフト）が警告を発した場合は、内容をよく確認し、わからない場合は周囲の助言を仰いでください。

また、マルウェアではありませんが、ファイル共有ソフトは自分が意図していないファイルでも他に共有してしまうことがあります。自宅のパソコンも含めてインストールしないようにしてください。

七 OS（基本ソフト）やソフトウェア、アプリは定期的に更新し最新状態を保つ

悪意のある行為は複合化の傾向があり、情報セキュリティ対策もウイルス対策ソフト単独では十分とは言えませんが、少なくともウイルス対策ソフトのアップデートは定期的に行い、最新の状態で利用することは情報セキュリティの確保のためには不可欠です。パソコン・タブレットのＯＳは、定期的にアップデートの案内を受けとることが可能なよう設定し、その内容に従って、ソフトウェアそのもの、セキュリティパッチ等は常に最新の状態にします。

八　私物機器は学校の機器やネットワークへの接続、学校の機密情報の記録をしない

授業等でＩＣＴを活用するため、私物の無線ＬＡＮアクセスポイントやタブレットＰＣ、周辺機器などを学校に持ち込み、ネットワークに接続したことはありませんか？また、私物のスマートフォンに学校の機密情報をダウンロードしたり撮影して持ち帰ったりしたことはありませんか？　これらは情報セキュリティの抜け穴になり、万一紛失、盗難が起こった時には事故として扱われてしまいます。また、機器のセキュリティ状態も学校のものと同レベルの最新のものとは限りません。私物機器は学校で定められた手順以外では学校内で使用しないことが推奨されます。

■著作権や肖像権への配慮

九　デジタルカメラは機微情報の記録機と捉える

デジタルカメラやカメラ機能が付いたスマートフォン等は、日常的に画像やビデオ映像を撮影することを可能にしています。しかし、便利な一方で、設定を良く確認せずに使うと撮影した場所の位置情報がファイルに記録されたり、クラウドサービスにアップロードされて知らぬうちに共有されたりしてしまうこともあります。

また、肖像権の取り扱いや、複数の情報の組み合わせによる個人情報の特定等、トラブルにつながりかねない事象も考えられますので、仕組みを理解して設定を調整し、ファイルの取り扱いは注意を持って行います。

十　SNS、ストレージサービスは関係者との合意なしにはアップしない

ＳＮＳは近況を共有したり、さまざまなイベント情報を伝えて参加者・賛同者を募ったりするために有効なメディアです。利用に当たっては、情報の公開範囲を理解して設定し、センシティブな話題は投稿しない、画像等をアップロードする際は写っている人の同意を獲得する、等の対応を行います。また、アドレス帳の情報を収集するために架空のアカウントによる友達申請が来る場合もあります。基本情報を確認しても心当たりのない申請は保留にする等、着実に管理することが求められます。また、子供たちのやり取りが、ちょっとした行き違いや勘違い、軽はずみな表現などで誹謗中傷、ネットいじめに至ることもあります。子供たちへの情報モラル指導により、多様性を受容する心を育んでください。

◉2.3　情報セキュリティを守る仕組み

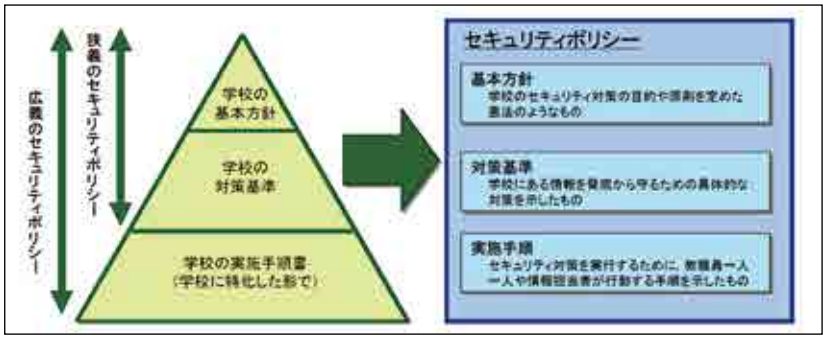
2.3.1　情報セキュリティポリシー

■学校における情報化の現状と情報セキュリティに関する基本的考え方

学校の現場は、児童生徒が教室や職員室に自由に出入りできます。また、取り扱う情報資産が、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。

情報セキュリティ確保のためには、情報セキュリティポリシーの策定が基本となります。

図表 2-15　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」

■情報セキュリティポリシーの策定

「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。ふさわしいものが示されていない場合は、既存の地方公共団体や教育委員会、他校で定めた基本方針や政府、外郭団体のガイド（例：（一社）日本教育情報化振興会の「学校情報セキュリティ・ハンドブック」等）を参考に作成します。基本方針には、最低限以下の項目、内容が盛り込まれます。

- 目的
- 学校の責務（管理責任の明確化、既定の整備、リスク分析・評価、条例・規則等の順守）
- 管理職及び各情報管理者の責務
- 情報セキュリティ管理体制の整備（管理責任の明確化、義務及び責任）
- 教職員の責務など
- 対策の規定整備（組織的な取組の明文化、対策実行化のしくみ）
- 評価及び見直しなど

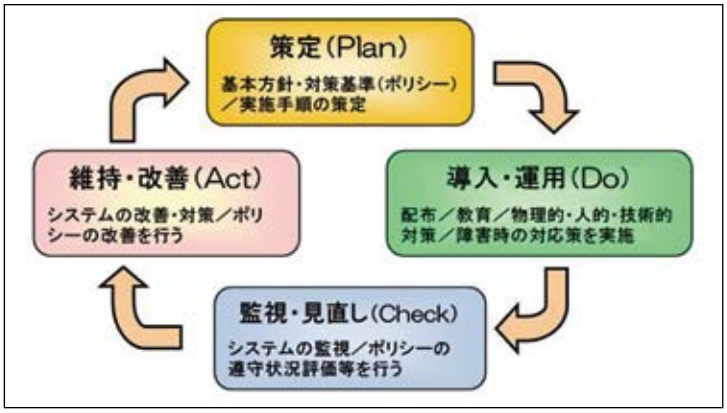
「対策基準」には前述のとおり、「情報資産の洗い出し」、「リスク評価と対応検討」の結果、「守るべき資産」を守るために必要な対策の基準を盛り込みます。基本方針とセットで策定すべきものですので、他の地方公共団体や学校の事例、前述のガイド等を参考とすることができるでしょう。

「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。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、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。

地方公共団体の情報セキュリティポリシーに沿った運用をしている学校においても、学校が保有する情報資産の特性を踏まえた上で、学校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は、「計画 (Plan)」→「導入・運用 (Do)」→「点検・評価 (Check)」→「見直し・改善 (Act)」のＰＤＣＡサイクルの出発点になります。実際に策定し、運用した上で課題が発生した場合は、対策を練るとともに対策基準実施手順書を見直す等、ＰＤＣＡサイクルを回していくことが重要です。（図表 2-16）

図表 2-16　情報セキュリティマネジメントの実施サイクル



資料出所：総務省　http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-1.html

2.3.2　学校における体制づくり

■人的セキュリティの現状と重要性

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。

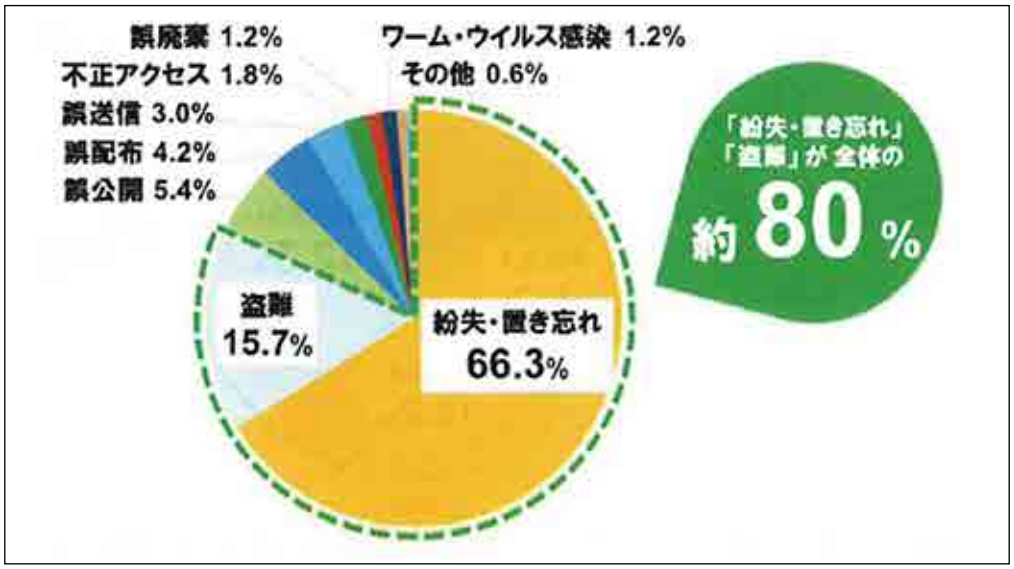
人的セキュリティ対策が効果をあげるか否かは、最終的には関係者（教職員や児童生徒）の意識に依拠することになります。たとえば、情報を扱うＩＣＴ機器や取り扱いについて一定のルールを定めている学校は多いものの、実際には私物のＩＣＴ機器を校務や授業で利用している教職員もかなりの比率にのぼることが以下のアンケート結果から推察されます。（図表 2-17）

図表 2-17　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」

このような状況が、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 2-18　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」

運用以外の面でも、万が一事故が発生した場合の報告体制についても予め策定しておく必要があります。

2.3.3　学校のネットワーク

■校務支援系・授業支援系（学習系）のネットワーク

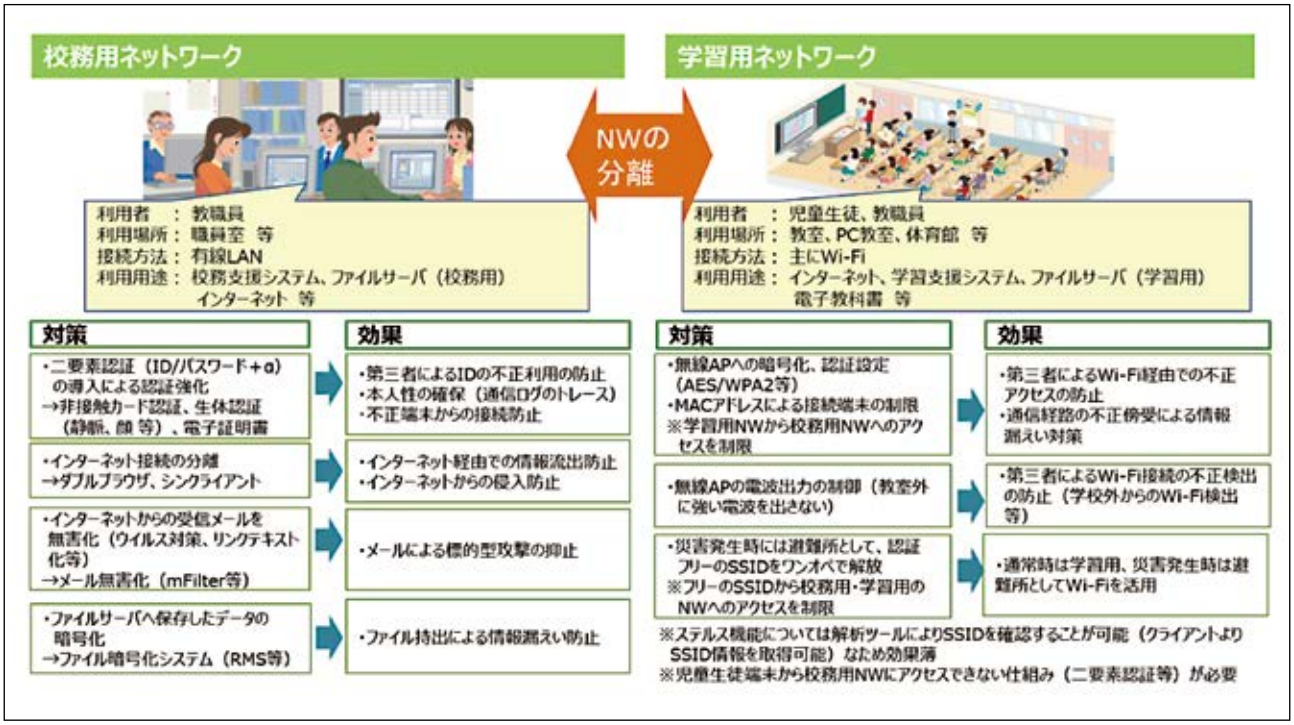
学校において教職員が使うネットワークは、主に校務支援系･授業支援系（学習系）の２つとなります。この他、経費の精算や稟議処理のための地方公共団体事務ネットワークが設置されている学校もありますが、利用者は管理職と事務職員に限られます。

校務支援系ネットワークについては、児童生徒の重要なデータ（住所、電話番号等の個人情報や健康診断データや成績情報等の機微データ等）を扱うことから高い情報セキュリティ対策が必要なため職員室での有線ＬＡＮ接続が用意されていることが一般的であり、インターネット等の外部ネットワークとは接続しないことが推奨されます。また、情報持ち出しをコントロールするために機器のＵＳＢポートに記録メディアを接続できないようにしてあったり、認証の仕組みに利用者固有の情報（指紋等の生体情報や個別に配付されたＵＳＢキー等）を使うよう、情報セキュリティが強化されている場合も数多くあります。

一方、授業支援系（学習系）ネットワークについては、児童生徒もアクセスし、インターネット上のコンテンツも教材としてアクセスすることから、情報漏えいが発生した際にもそのリスクを低くする必要があります。機密を要する情報は日頃から使わない、記録しないことはもちろん、普通教室等での無線ＬＡＮ（Wi-Fi）接続を進めるなかでも校外からのネットワーク侵入や学生によるなりすましへの対策が必要と考えられ、予め許可を受けた機器以外は接続できない設定にする等の対策がとられます。

このようなネットワークの特性を踏まえて、少なくとも校務支援系と授業支援系（学習系）ネットワークはネットワーク分離をし、できる限り二要素認証等強い情報セキュリティ手段を使用することで、情報セキュリティ対策をしていくことが推奨されます。（図表 2-19）

図表 2-19　校務用ネットワークと学習用ネットワークの分離



2.3.4　定期的な確認

■情報セキュリティ実施状況の確認

情報セキュリティポリシーを策定し運用を開始した後は、適切な運用が出来ているか、事故は発生していないかの定期的な運用の確認が必要となります。情報セキュリティポリシーについても実効性を挙げられるように、運用計画には、情報セキュリティポリシーの見直しと改善を盛り込みます。あらかじめ情報セキュリティポリシーの中で、運用時にチェックすべき項目をピックアップしておき、チェックの結果実施できていなかった項目については、自校で対策が必要かどうかを再検討します。

学校で取り扱う個人情報（生徒の氏名、住所、成績など）を含んだ情報資産、成績や就学援助、住所録などの個人情報の管理や、ウイルス対策などの重要事項については、具体的な担当と実施時期を定め、一年に一度以上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。

また、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っていくことで、現場の状況に沿った実効性のあるルールができていきます。

■情報セキュリティ教育／研修

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、教職員や児童生徒への教育を行っていくことが重要と言えます。情報セキュリティポリシーは、教職員に配布し、年に一度程度は内容の確認をします。専門用語も多いため、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の解説、具体的な事例を盛り込んだ研修会を実施する必要があります。また、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、再度配布し説明をおこないます。これらの説明の際には、内容を確実に理解し、遵守することを確認する書面等をもちいて教職員の参画意識を醸成することもあります。

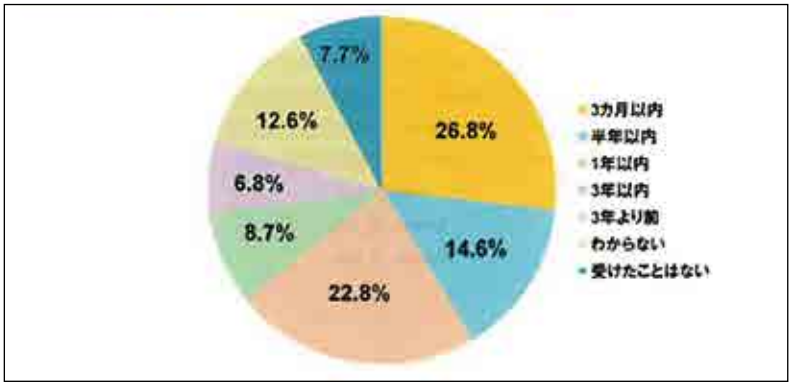
また、情報セキュリティの脅威を知ることが対策の基本となります。教職員や児童生徒への情報セキュリティ教育／研修においては、ＩＳＥＮ「学校情報セキュリティお役立ち Web」（図表 2-20）など、最新の教育コンテンツが提供される Web サイトなどを活用して、知識の共有を図ると良いでしょう。

図表 2-20 「学校情報セキュリティお役立ち Web」

資料出所：ＩＳＥＮ（http://school-security.jp/）

図表 2-21 のとおり、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多数存在しています。一方的な情報提供ではなく、セキュリティの脅威の事例を活用したグループディスカッションを行い、事例のようなリスクを回避するためにはどのような方法があるのか、その方法を運用する

図表 2-21　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」

とどのような問題が発生するか、などのポイントを話し合うことで、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。

情報セキュリティ研修の中で伝えるべき重要なことがもう一つあります。実際に情報セキュリティ事故が発生した、あるいは発生したかもしれないといった状況への対処です。事故が発生したときの責任や影響を伝えることも重要ですが、責任を問われることを恐れて、報告も対処もしないことは最も避けなければなりません。デジタル情報の拡散スピードは驚くほど速いため、危険性が生じた段階での初動対応がカギとなります。情報セキュリティ事故が発生した恐れがある時には、素早い報告や相談を行うことが最良の選択であることを自覚し、教職員間でお互いに情報共有しやすい雰囲気を作っておくべきです。

■企業における取組例

企業では従業員の情報セキュリティ意識を高めるため、継続的に以下のような取組を行っている例があります。

- ☞毎月 1 回、「情報セキュリティの日」を設定し、過去の情報セキュリティ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、「お客様情報等保護強化期間」を設定し、集合研修・Web 研修・クロス点検・監査・委託先調査等を実施する
- ☞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・情報セキュリティ事故事案の再周知を図る

◉2.4　いざという時に

2.4.1　情報漏えいの危険さ

■個人情報漏えいの場合

学校に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。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、多様な情報が流通しているため、情報同士を照合することによって、個人の居場所を割り出したり、行動履歴を追ったりといったことが可能になってきている側面もあります。

情報の重要性を鑑みると、確実な情報の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。（図表 2-4）

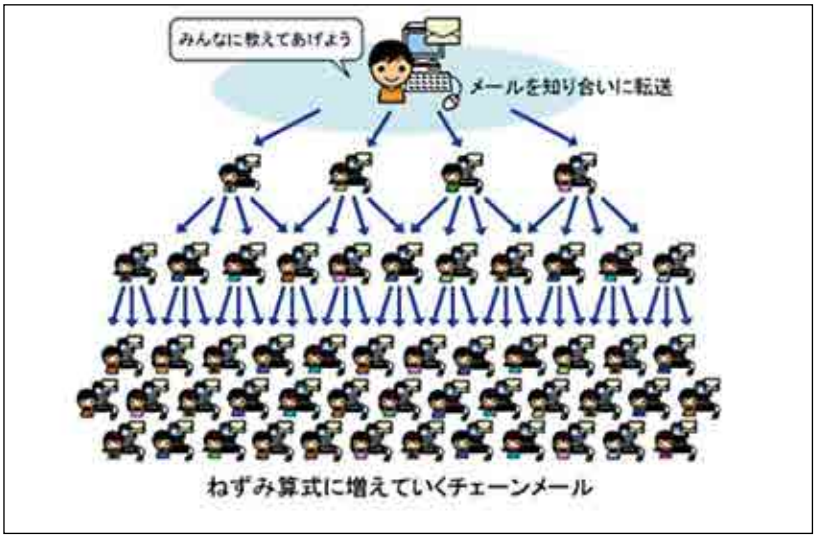
■デジタル情報の特性

さらに、悪意を持っていないはずの私たち自身が、知らないうちに他者にとっての脅威となってしまうケースもあります。たとえば、私たちが日常的に使用しているパソコンやサーバが、マルウェア（コンピュータウイルス）や不正アクセスによって、何者かに乗っ取られてしまうと、そのパソコンやサーバが「踏み台」にされて、第三者に対して SPAM メールが大量に送られるといったことが容易に起こりえます。被害者になると同時に加害者になってしまうわけです。

デジタルの世界では手法さえ知っていれば、名前やメールアドレスなどの詐称が容易にできます。また、デジタル情報は複製（コピー）が簡単で、送信や共有に必要なコスト、手間が小さいという特徴があります。

たとえば、自分が受け取った電子メールの内容を評価して、その情報を友人知人などにも知ってほしいと思い、転送することによって、メールがネズミ算式に増殖してしまう「チェーンメール（チェーンレター）」という現象もあります。（図表 2-22）過去には、「臓器移植のための寄附活動」といった一見、有益そうな偽の情報が、電子メールによって日本中に拡散された実例もあります。受け手にとって興味関心のない情報を電子メールで送りつけられるだけでも愉快なことではありませんが、その内容が不正確であったり虚偽であったり、あるいは、コンピュータウイルスが添付されていたり、悪意のある Web サイトに誘導するものであったり、など、善意に基づく行動が、第三者にとって、脅威となることもあるのです。

図表 2-22　チェーンメールのイメージ



2.4.2　情報セキュリティ事故が起こったら

■情報セキュリティ事故とその対応

情報セキュリティ事故とは、次のような事象が発生することです。

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)

情報セキュリティ事故の内容によって、取るべき対応（事故対応）は異なってきます。また、これらの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、一般的に事故対応は図表 2-23 のように進んでいきます。

図表 2-23　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。

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。

■教職員の役割

情報セキュリティ事故は発生すると影響が甚大になることがしばしばあります。そのため、教育委員会や学校においては、情報セキュリティ事故の発生に備えた事前準備がなされなければなりません。

たとえば、「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整備」などです。教職員は日常的にＩＣＴ環境等で情報資産を取り扱っているので、期待される最大の役割は情報セキュリティ事故の発生を検知することです。事故が発生した時には初期動作として「事故発生をしかるべき責任者、担当者へ速やかに報告すること」が非常に重要です。責任者としては校長などの管理職、担当者としてはＩＣＴ担当（情報担当）担当の教職員等が学校毎にその役割を担います。ＵＳＢメモリーを紛失した場合などでは確実に情報セキュリティ事故が発生しているかがすぐにはっきりすることは稀ですが、「事故が発生した可能性があること」を責任者や担当者と共有し、その支援を受けることで事故の影響を最低限にとどめることが可能となります。

また、情報セキュリティ事故が発生した場合、関係者への連絡、謝罪等が必要になることがあります。校長等の指示や助言を仰ぎつつ、落ち着いて行動することが重要です。

校長などの管理職は、「情報セキュリティ事故が発生した（かもしれない）」という報告を受けた場合、内容や重大性を検討して教育委員会へ情報共有（報告）します。教育委員会は学校に比べて情報の専門家等の支援も受けやすいので、判断に迷ったら速やかに情報共有をし、連携して対応を進めることが重要です。

◉ 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）にウイ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、ウイ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

- □ 児童生徒の写真、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。

●【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/

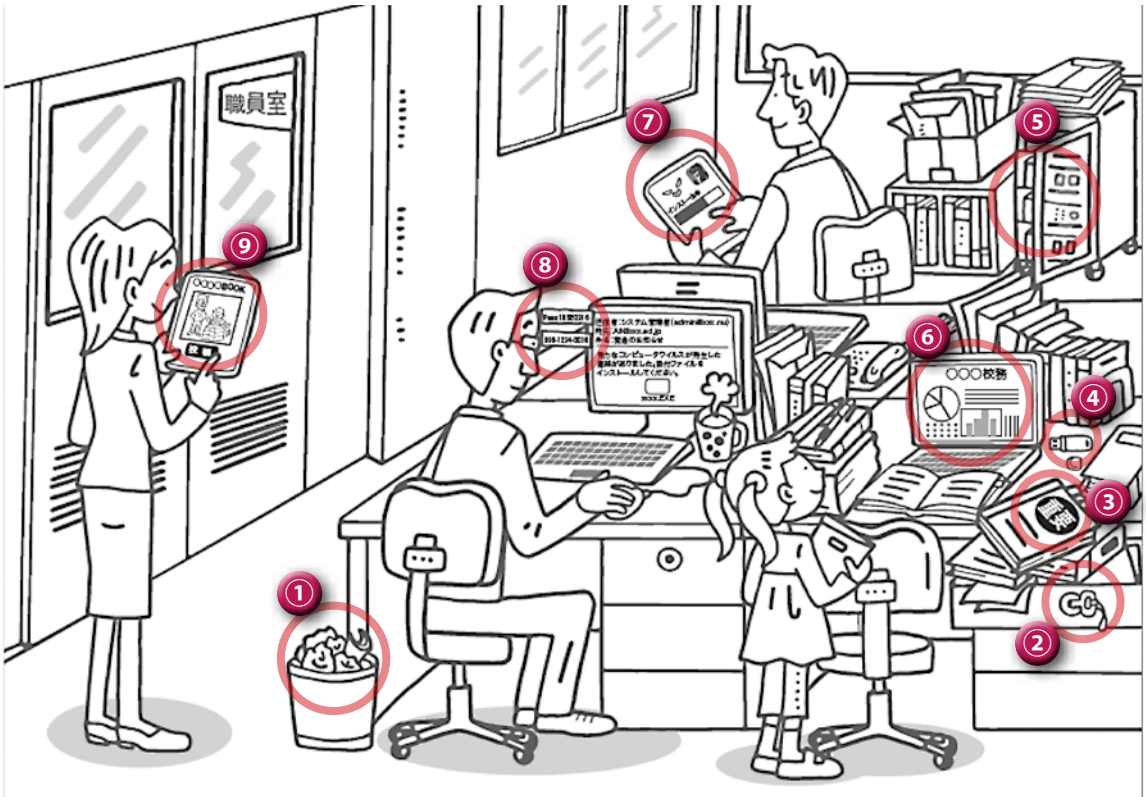
独立行政法人　情報処理推進機構（IPA）ホームページ
http://www.ipa.go.jp/

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

◉ 用語集

ＩＣＴ関連用語	用語解説
AES	データ暗号化方式のひとつ。Advanced Encryption Standard の略。現在実用化されている方式の中では、極めて強度が高い（暗号が解読されにくい）。
CIO	最高情報責任者のこと。Chief Information Officer の略
CIO 補佐官	CIO を補佐し、情報システム技術及び情報セキュリティに関する専門的な知識・経験を有する専門家のこと。
CISO	組織の情報セキュリティを統括する責任者のこと。Chief Information Security Officer の略。ＩＣＴのセキュリティ対策だけでなく、機密書類や個人情報の管理等も統括し、地方公共団体では副知事／副市長が務めることが多い。
HDD	コンピュータ等の記憶装置。Hard Disk Drive の略。磁気記憶方式によってデータを読み書きする装置のこと。ハードディスクと呼ばれる。
ID/ パスワード	ID は本教材ではコンピュータシステムの利用において、利用者を識別するために用いられる符号のこと。Identification の略。パスワードは正当な利用者であることを示すために入力する文字、数字及び記号の列をいう。
LAN	一施設内程度の規模で用いられるコンピュータネットワークのこと。Local Area Network の略。企業のオフィスや研究所、工場、公共機関等に限らず、近年では一般家庭にも普及している。
無線 LAN（Wi-Fi）	無線 LAN とは無線（電波）を用いて数 m ～数十 m 程度の範囲内で高速なデータ通信を行う LAN のこと。 Wi-Fi（ワイファイ）は Wi-Fi Alliance という業界団体が定めた無線 LAN の規格であり、同団体の規格に対応した機器には Wi-Fi Certified という認定ロゴが貼付されている。近年では意味が転じて、無線 LAN によるインターネット接続サービスを指す言葉として使われることも増えている。
無線 LAN アクセスポイント	無線 LAN（Wi-Fi）で機器がネットワークに接続するための電波中継機のこと。
MAC アドレス	ネットワーク機器等に付与された固有の識別番号のこと。Media Access Control Address の略。物理アドレスと呼ばれることもある。LAN で接続されているネットワーク機器等には製造段階で原則一意となるように付与される。一般には　0 ～ 9、A ～ F の 16 進数 6 つで、A0：B2：D3:4F:56:B7 のように表記されている。
SPAM（スパム）メール	広告等の目的で、受信者の意向を無視して無差別かつ大量に一括して送信される電子メールのこと。SPAM は電子メール以外の無差別かつ大量のメッセージの送信を意味することがある。迷惑メール、ジャンクメールとも呼ばれる。
SSID	無線 LAN（Wi-Fi）におけるアクセスポイントの識別名のこと。Service Set Identifier の略。無線 LAN 接続の混信を避けるために付けられる名前で、最大 32 文字までの英数字をアクセスポイント毎に任意に設定できる。
USB キー／ USB メモリ（フラッシュメモリ、フラッシュドライブ）	USB はコンピュータ等に周辺機器を接続するための規格のひとつ。Universal Serial Bus の略。USB キーは、パソコンの USB 端子に接続し、ログオン／ログオフを制御する機能を持ったものをいう。USB メモリ（フラッシュメモリ、フラッシュドライブ）は、半導体メモリを内蔵した USB で接続する外部記憶装置であり、データの移動や持ち運びに用いられている。
Web（ウェブ）サーバ／ Web サイト／ Web ブラウザ	Web とはインターネット上で情報の閲覧を行う仕組み。「クモの巣」の意味と言われる。Web サーバは、情報の掲載、検索や取引等の機能を持った Web ページを利用者に提供する仕組みを搭載したコンピュータのこと。Web サイトは、組織等の単位で複数の Web ページをまとめたものであり、ホームページと呼ばれることもある。Web ブラウザは、Web を閲覧・利用するために用いるパソコンやタブレット機器用の表示ソフトウェア。Web ページの印刷、ページ内に埋め込まれた（ハイパー）リンクと呼ばれる情報により、他の Web ページに移動したり新しい Web ページを開いたりする機能を持つ。
WPA2	無線 LAN の暗号化の技術のひとつ。AES に対応し、セキュリティが強固な最新の暗号化規格。
アイコン	コンピュータ等で、目的となるファイルやプログラムを見つけやすくするため、内容を図や絵で表現したもの。
アカウント ID (ユーザ ID，管理者 ID)	ID は利用者を識別するために用いられる符号。アカウント ID は、利用者がコンピュータやサーバの特定の領域を使用するために割り当てられた識別符号である。これを利用者毎に割り当てたものをユーザ ID, ユーザ ID の追加、削除、権限変更などシステム等の管理者のみに認められた権限を実行するための ID を管理者 ID と呼ぶことがある。
アクセス権	コンピュータネットワークにおいて、特定のファイルやシステム等を利用する権限のこと。
アップデート	コンピュータ等の基本システム（OS）やソフトウェアのセキュリティ、機能向上、不具合対応のために提供されたプログラムを実行すること。ソフトウェア更新ともいう。
アップロード（アップ）	ネットワークを通じて、SNS や画像共有等のサービス、別のコンピュータへデータを送ること。
アプリケーション（アプリ）	パソコンで利用するソフトウェア（プログラム等）の総称。応用ソフトウェアとも言われ、アプリケーション、アプリ、App、app（アップ）などと略されることもある。
インストール	パソコンにソフトウェアを追加し、使用可能にすること。
情報モラル（インターネットモラル・ネチケット）	インターネットを利用する上でのルールやマナーのこと。厳密に定められている規則ではなく、他人への配慮など、社会で最低限必要とされていることに基づいたものが多い。
インフラ	インフラストラクチャー (infrastructure) の略。ＩＣＴ分野では、ネットワークやシステム基盤のことを指す。
ウイルス（コンピュータウイルス）／ウイルス対策	パソコンに被害をもたらす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。ウイルス対策は、ソフトウェアや Web サイトアクセスの制限等によりコンピュータウイルスに感染しないための防御を行うことをいう。
オペレーションミス	システムの運用における、人為的な操作ミスを意味する。
ガイドライン	一般的には指標、指針の意味。テーマに沿って従うべきルールや依拠する基準がまとめられたドキュメント。
クライアント	コンピュータネットワーク上でサービスを受ける側、及び受ける機器等。サービスを提供する側のサーバに対していう。

ＩＣＴ関連用語	用語解説
クラウドサービス	クラウドは、インターネットなどのネットワークで提供されるサービス。このサービスを利用者はネットワーク経由で手元のパソコンやスマートフォンで使うことが可能。たとえば、これまでカメラで撮影した画像ファイルはカメラ内の記憶装置に格納されたが、技術の進展・普及によりネットワーク上の記憶装置に記録し、他の機器での利用や共有が容易になっている。
クラッキング／ハッキング	コンピュータネットワークに繋がれたシステムへ不正に侵入したり、機密情報を入手したりすること。コンピュータシステム、通信システム等の動作解析によるプログラムの破壊や改竄等を伴うこともある。
クリーンデスク（クリアデスクポリシー）	情報セキュリティ保護のための指針の一種で、机上に情報媒体を放置しないことによって機密を守るためのセキュリティポリシーのこと。
クロス点検	いろいろな角度、視点から確認、点検をすること。
コンテンツ	ネットや書籍等において、文字、図形、音声、映像等で表現された「中身」「内容」のこと。プログラムを指すことが多い「ソフトウェア」と区別するため、著作物というニュアンスで「コンテンツ」という言葉が広く使われている。
サイバー犯罪	パソコンやネットワークを利用して行われる犯罪。不正アクセスやオンライン詐欺、著作権侵害、児童ポルノの頒布・所持など、法律に抵触する行為のこと。
サイバー領域問題	ネットワークを対象に行われるテロ行為、サーバ攻撃により発生する機密情報の窃取や社会インフラ破壊等のこと。
ショルダーサーフィン	他人のキーボードやディスプレーを盗み見て、パスワードや暗証番号などの個人情報を入手すること。
シンクライアント	クライアント端末では起動等、必要最小限の処理を行い、ほとんどの処理をサーバ側で集中的に行うシステムのこと。
スクリプトファイル	簡単な文字等での指定（コマンド）を入力するだけで実行可能なファイルのこと。
ステルス機能	発見されることを避けること、及びそのための技術のこと。ステルスは「隠密」の意味。
ストレージサービス	インターネット上で利用 ID 毎に上限の容量が設定され、データやファイルを預けられるサービス。
スパムメール	SPAM メールの項を参照してください。
セキュア	情報分野では「安全である」「危険がない」ことを示す。
セキュリティの脅威	情報システムにおいて情報の完全性、機密性、可用性に悪い影響を与え、損失を発生させる直接の原因のこと。
セキュリティパッチ	ソフトウェアが正常に動作しなくなる等の弱点（セキュリティホール）が発覚した時に作成･配布される修正プログラム。
センシティブ情報	個人のプライバシー情報や国家の機密情報など、慎重に扱わなければならない機微な情報のこと。
ダウンロード	ネットワーク上に存在する情報（データ）を手元のコンピュータに転送すること。
ダブルブラウザ	仮想ブラウザ方式を用いて、インターネット接続を分離する方法。端末から仮想ブラウザサーバを経由してインターネットへ接続し、仮想ブラウザのデスクトップ情報を表示するため、パソコンは直接インターネットに接続する必要がない。
トレードオフ	一方を追求すれば他方を犠牲にせざるを得ない、同時に両方が成り立たないという状態や関係のこと。
パスワードポリシー	コンピュータやインターネット、システムを利用する際のパスワードについて、字種、字数、入力条件等をまとめたもの。
ファイアウォール	インターネット上で信頼できない相手からの攻撃や不正アクセスから、組織内部のネットワークを保護する仕組み。
ファイル暗号化システム（RMS 等）	あらかじめ指定したフォルダにファイルが格納された場合、すべて自動的に暗号化するシステムのこと。
フィッシング	電子メール等の受信者に偽のホームページにアクセスするよう誘導し、そのページでクレジットカード番号や ID・パスワード等の情報を入力させるなどして、アクセスした人や機器の情報を不正に入手する行為。
プロジェクトマネジメント（チーム）	プロジェクトの実施に際して、期限や予算といった制約の中でプロジェクトを予定とおりに完了するための、計画立案や実行管理の手法のこと。それらの組織。
マイナンバー（マイナンバー制度）	国民の一人一人に固有の個人番号（マイナンバー）を付与し、社会保障、税、災害対策の分野で効率的に情報を管理する制度。法律の範囲内で、複数の機関が保有する個人の情報が、同一人の情報であることが確認可能となる。
マルウェア	マルウェアとは、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行ったりするソフトウェアの総称。“malicious software”（悪意のあるソフトウェア）を縮めた略語。
ユーザビリティ	パソコンにおけるソフトウェア等の操作における「使いやすさ」のこと。
リスク評価	リスク評価は、リスク を定量化し、比べたり現状把握をしたりする方法。
リモートデスクトップ	手元のパソコンからネットワークで接続された他のパソコンやデスクトップ環境を操作する技術の総称。
ログ	パソコンの利用状況を記録したデータ、またはデータを記したファイルのこと。
ログオフ／ログオフ	ネットワークから切断しサービスの利用を終えることをログオフ（ログアウト）、開始することをログオン（ログイン）という。
ワーム	マルウエアの一種で、ネットワークなどを通じてコンピュータに侵入し、自己増殖をするプログラムのこと。
ワンタイムパスワード	短時間のみ 1 回限り有効な毎回違うパスワードを使う方式のこと。
学校 CIO ／教育 CIO	学校 CIO は学校における情報関係の責任者のこと。教育 CIO は地方公共団体における情報責任者のこと。
記録メディア	データを記録するメディアの種類や、媒体そのもののこと。
校務サーバ	児童生徒の出欠・成績・時数・給食・保健などの管理ができる校務システム用サーバのこと。
校務支援システム／統合型校務支援システム	校務文書に関する業務、教職員間の情報共有、家庭や地域への情報発信、服務管理上の事務、施設管理等を行うことを目的としたシステム。統合型校務支援システムでは、これらが統合されて一つのシステムとして提供されている。
学習系システム	教材の準備・学習の記録を効率化し、教室での授業を支援するシステムのこと。
非接触カード認証	カードの内部にアンテナを持ち、外部の端末が発信する弱い電波を利用してデータを送受信するカードのこと。

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）