

第7章

ICT活用の留意事項

ICTを活用した教育を実施する上で、学校等における情報セキュリティ面及び児童生徒の健康面への影響等の両面において留意すべき事項等を整理するため、「ICTを活用した留意事項の整理に関するワーキンググループ」において、参考となる先進事例及び関係情報等について調査を実施した。調査に関する全体の実施概要は以下のとおりである。

1. 学校等における情報セキュリティ面における配慮事項の調査

- ① 教育委員会に対するアンケート調査
- ② 現地訪問ヒアリング調査

2. 児童生徒の健康面への影響等に関する配慮事項の調査

- ① 学校・教員に対するアンケート調査(平成23年度)
- ② ICT活用による児童生徒の健康への影響等に関する調査結果(平成24年度)
- ③ ICT活用による児童生徒の健康への影響等に関する調査結果(平成25年度)

1 情報セキュリティ面における配慮事項

1-1 情報セキュリティ面における配慮事項に関する調査結果(平成23年度)

① 教育委員会に対するアンケート結果概要

今後学校におけるICT環境の整備に伴って、教員のICT活用指導力の向上とともに、教育委員会や学校が整備する各種のシステムやインフラ整備における情報セキュリティの確保方法及び教員の情報セキュリティ意識等が重要となる。将来的に、家庭へのタブレットPCの持ち帰りや学校への持ち込み等の可能性もあることを踏まえ、現状の地方自治体の実態を把握する必要があるとの考えから、以下のとおり、校務支援システムの導入状況及び運用状況、情報セキュリティの確保手段、情報セキュリティポリシーの策定状況などに関して、教育委員会に対するアンケート調査を実施した。

都道府県及び指定都市・市・特別区の全857自治体を対象として、郵送調査にて実施した。

▼ 教育委員会に対するアンケート調査の実施概要

- 調査期間
平成24年2月～3月
- 対象・方法
都道府県及び指定都市・市・特別区の全857自治体を対象として、郵送調査にて実施
- 回収率
都道府県アンケート:87%、指定都市・市・特別区アンケート:67%であった。
- 調査内容
校務支援システムの導入状況・運用状況、システムにおける情報セキュリティやアクセス制御の方法と実態、情報セキュリティ及び個人情報管理に関する規程等の策定状況、当該規定の具体的な事例の収集、児童生徒の1人1台タブレットPCやクラウドの導入状況についてアンケートにより実態調査を実施した。

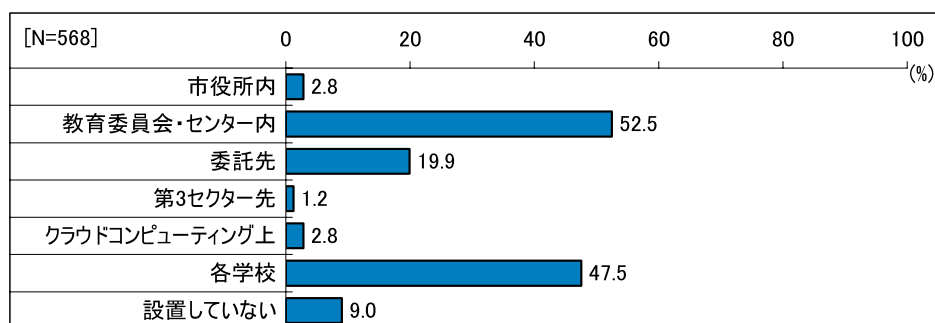
以下、アンケート調査結果に関して、主な内容について掲載する。

i) ネットワーク、サーバ等の整備状況

【管轄するシステムのサーバ等設置場所】

設置場所は、「教育委員会・センター内」(52.5%)、「各学校」(47.5%)が多かった。

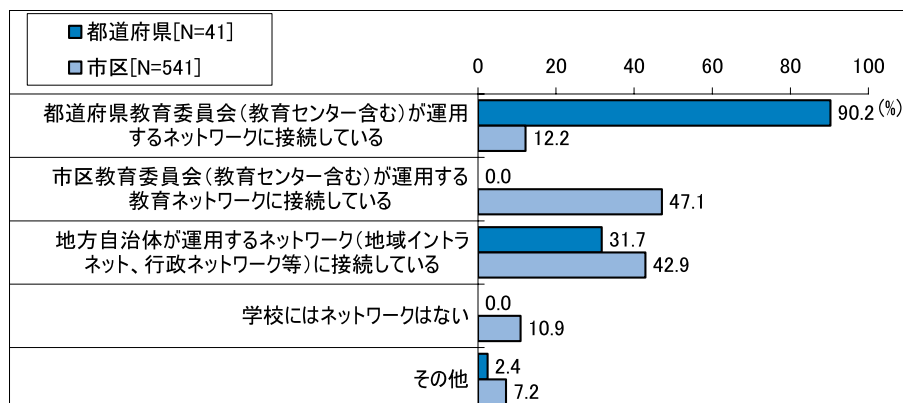
▼ サーバ等の設置場所



【管轄する学校のネットワークへの接続経路】

接続状況は、都道府県では「都道府県教育委員会が運用するネットワークに接続」(90.2%)が最も多く、市区では「市区教育委員会が運用する教育ネットワークに接続」(47.1%)が最も多かった。

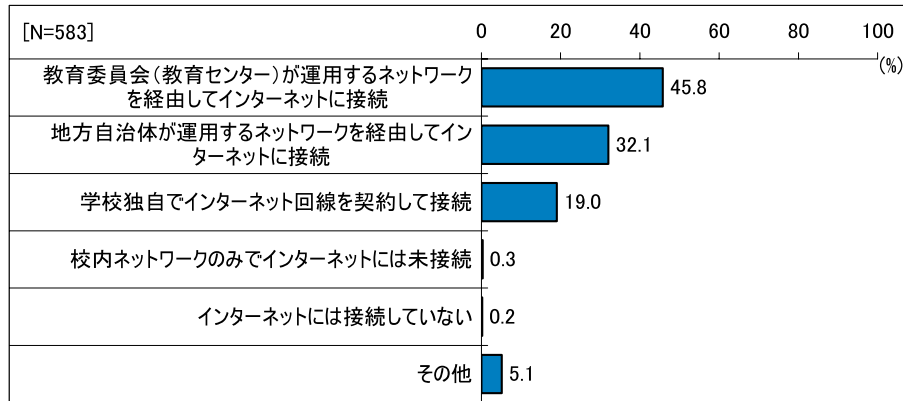
▼ ネットワークへの接続経路



【管轄する学校のインターネットへの接続経路】

接続経路は、「教育委員会が運用するネットワークを経由して接続」が最も多く、45.8%であった。

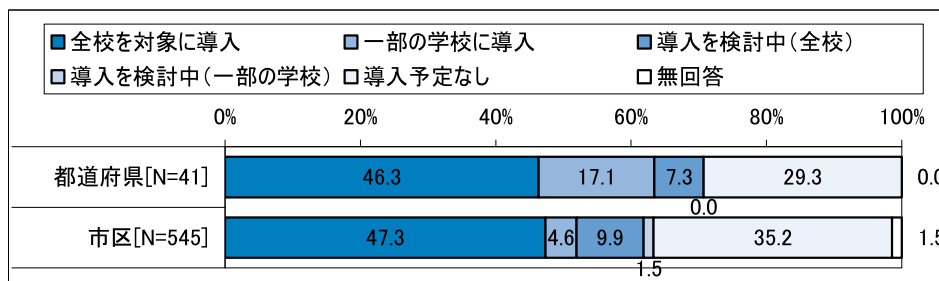
▼ インターネットへの接続経路



【指導案や教材等を教員間で情報共有するための共有サーバの導入状況】

導入状況は、都道府県、市区共に「全校を対象に導入」が最も多く、都道府県46.3%、市区47.3%であった。

▼ 教員間の共有サーバの導入状況

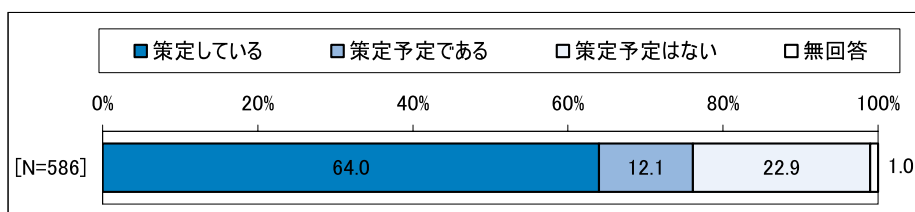


ii) 個人情報管理規程及び情報セキュリティポリシー等の策定状況

【教育委員会における個人情報管理規程の策定状況】

教育委員会における個人情報管理規程の策定状況は、64.0%であった。

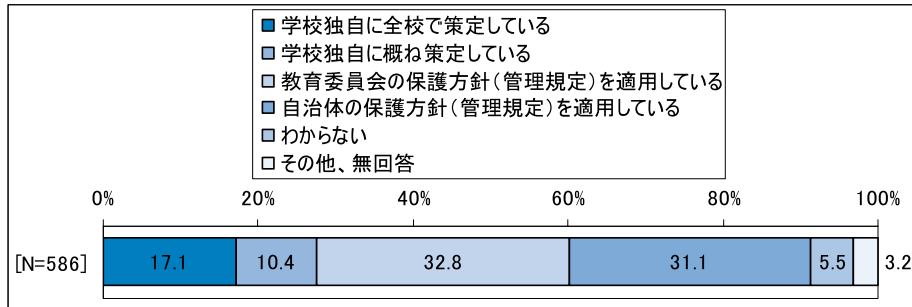
▼ 個人情報管理規程の策定状況(教育委員会)



【管轄する学校における個人情報管理規程の策定状況】

「学校独自に全校で策定している」(17.1%)と回答した教育委員会が管轄する学校では、例えば、教育委員会が作成した規定のサンプルを利用するなど、教育委員会の個人情報管理規程を準用している。

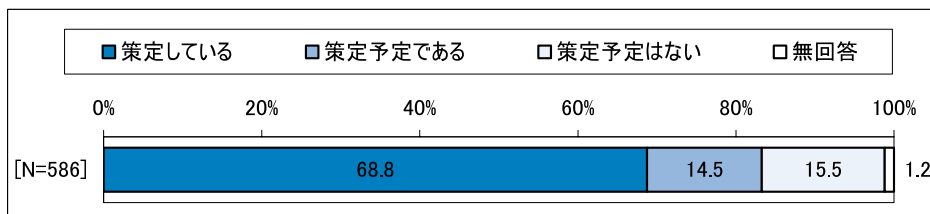
▼ 個人情報管理規程の策定状況(学校)



【教育委員会における情報セキュリティポリシーや情報セキュリティ管理規程の策定状況】

教育委員会における情報セキュリティポリシーや情報セキュリティ管理規程の策定状況は、68.8%である。

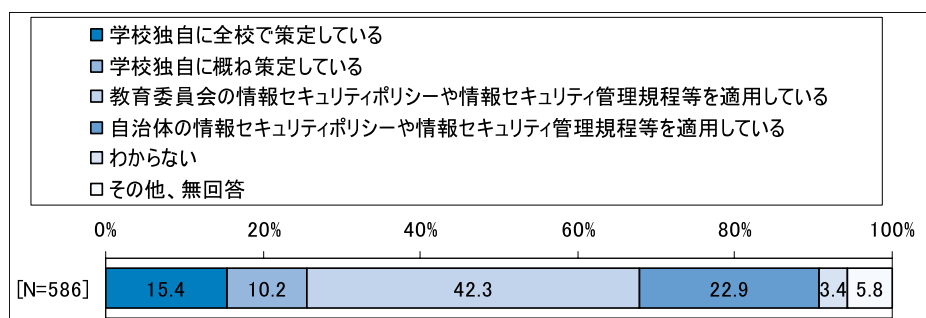
▼ 情報セキュリティポリシーや情報セキュリティ管理規程の策定状況(教育委員会)



【管轄する学校における情報セキュリティポリシーや情報セキュリティ管理規程の策定状況】

「学校独自に全校で策定している」(15.4%)と回答した教育委員会が管轄する学校では、例えば、教育委員会が作成したポリシーや規定のサンプルを利用するなど、教育委員会の情報セキュリティポリシーや情報セキュリティ管理規程を準用している。

▼ 情報セキュリティポリシーや情報セキュリティ管理規程の策定状況(学校)



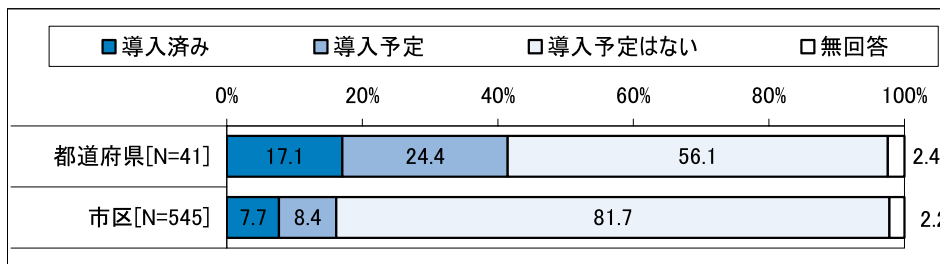
教員が活用しやすいネットワークを構築するためには、情報セキュリティ上の問題がなく、できるだけ多くの教員がネットワークにアクセスできるようにするとともに、そのために最低限必要な規制の範囲を整理することが重要である。その結果、校務系と学習系のネットワークの分離が情報セキュリティ面の留意事項のポイントの一つであり、学校においてシステムで扱う情報セキュリティやプライバシーのレベルが一律ではなく多様性があること、校務情報と学習情報は本質が異なることなど、情報セキュリティに関する認識と行動を徹底していくために、教育委員会や学校現場における情報セキュリティポリシーの策定をさらに促していく必要がある。

iii) クラウドの導入状況

【クラウドの導入状況】

都道府県、市区共に「導入予定はない」が最も多く、都道府県56.1%、市区81.7%であった。

▼ クラウドの導入状況



【導入自治体の数】

以下のとおり、7都道府県、42市区で導入している。

▼ クラウド導入自治体の数

	都道府県	市区
クラウド導入済み	7	42

内訳は、以下のとおりである。

・「既に導入済み(一部学校の場合を含む)」と回答した自治体

〈都道府県〉

富山県、静岡県、京都府、和歌山県、岡山県、高知県、福岡県

〈市区町村〉

北海道(室蘭市)、青森県(八戸市)、岩手県(久慈市)、茨城県(取手市)、栃木県(栃木市)、群馬県(高崎市、太田市)、千葉県(銚子市、柏市、八千代市)、埼玉県(戸田市)、東京都(新宿区、町田市、多摩市、西東京市)、神奈川県(横浜市、平塚市)、新潟県(糸魚川市、見附市、上越市、南魚沼市)、岐阜県(大垣市、可児市、海津市)、愛知県(春日井市、犬山市、江南市、弥富市)、大阪府(堺市、泉南市)、兵庫県(神戸市、淡路市)、広島県(広島市)、高知県(土佐市)、福岡県(宗像市、うきは市)、熊本県(玉名市、宇城市)、大分県(豊後大野市)、宮崎県(小林市)、沖縄県(浦添市、宮古島市)

② 自治体報告及び先進地域ヒアリング調査結果

情報ネットワークの整備状況によって、減価償却期間やシステム運用における各種制約等から、無線LANの活用やフィルタリング、リモートアクセス環境など情報セキュリティ確保の在り方に関して、地方自治体間で相当の相違があることが明らかとなった。そこで、ICT環境の整備と情報セキュリティ対策の状況等について大分県及び和歌山市から報告いただくとともに、横浜市、大分県、宮古島市、柏市、杉並区について現地訪問ヒアリング調査を実施して、先進事例となる地域の実情について把握した。

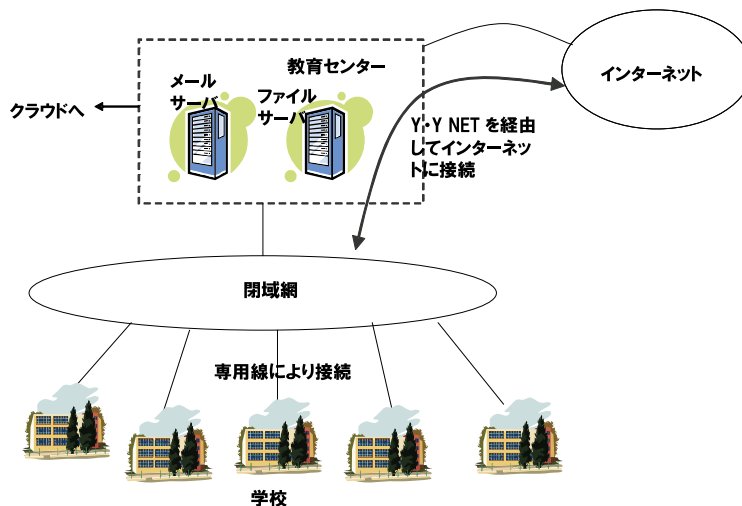
以下、自治体報告及びヒアリング調査結果について、自治体ごとに、ICT環境の特徴、ICT環境の運用における特徴、効果という点から、主要な内容について掲載する。

i) 横浜市の事例(大規模プライベートクラウド、自宅へのデータ持ち帰り)

【ICT環境の特徴】

- ・市内のすべての市立学校514校(小・中学校、高等学校、特別支援学校)を結ぶ閉域網であるY・Y NET横浜市教育情報ネットワーク)を整備
- ・市内のすべての市立小学校344校(教職員数 約10,000人)にて、プライベートクラウドで在籍、出欠、成績、保健情報を管理
- ・校外からアクセスされる恐れがあるため、無線LANの利用は禁止

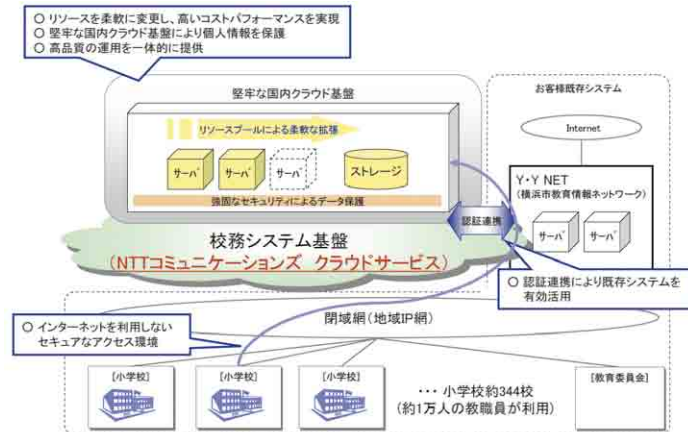
▼ 横浜市閉域ネットワーク(Y・Y NET)の構成図



【ICT環境の運用における特徴】

- ・Y・Y NETとクラウドサービスの間は専用回線によって接続され、認証をクラウドの外に配置して連携を実施
- ・校務支援システムの操作ログ等を取得し、適正な権限での利用や不正操作等を防止

▼ クラウド構成図



【効果】

- ・クラウドを導入したことで、機器更新によるシステムの入替え負荷が軽減
- ・学校現場におけるサーバのメンテナンスの負担を軽減
- ・インターネットに接続しないプライベートクラウドにて校務支援システムを提供することで、教育現場で不安とされる情報セキュリティを確保

ii) 大分県の事例(校務系・学習系ネットワークの設計・構築、パブリッククラウド)

【ICT環境の特徴】

- ・大分県と市町村を高速・大容量の光ファイバ網で結ぶ既存の情報通信ネットワーク(豊の国ハイパーネットワーク)の中に「大分教育ネットワーク(OEN)」を構築
- ・市町村の要望も反映した形で大分県教育委員会がすべてのネットワークの設計を実施し、市町村も運用費用を負担
- ・学校の全教室で無線LAN 環境を構築済み
- ・4,000人が利用可能なテレワーク環境を提供

▼ 大分教育ネットワーク構成図

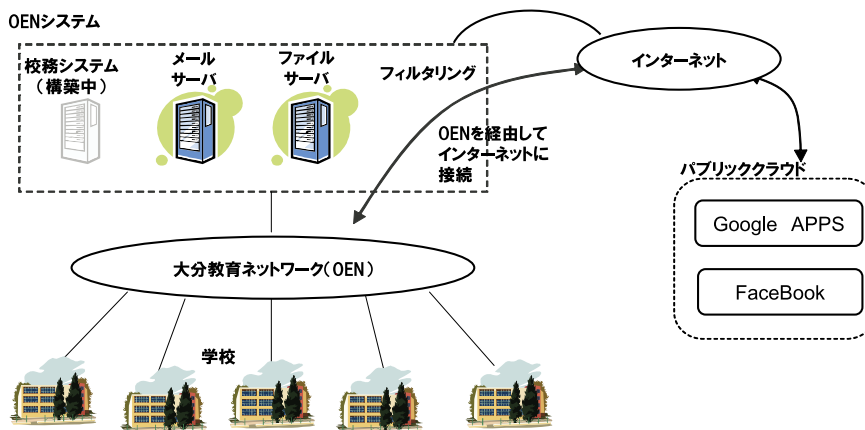


(出展:大分県商工労働部情報政策課資料)

【ICT環境の運用における特徴】

- ・情報の重要度をA(指導要録、定期考査素点表等)、B(通知表、住所録等)、C(学校パンフレット、PTA資料等)、D(授業用教材、課題プリント等)の4段階に分類し、媒体ごとに扱える情報はどれかを情報セキュリティ実施手順にて明確化
- ・重要度C、D の情報についてはパブリッククラウド上(Google Apps)で管理(メール、チャット、スケジュール管理、教材の保管等)、生徒の成績等の重要度A、Bの情報はプライベートクラウドで開発中で、現在、一部の学校で試行導入中
- ・市町村教育委員会の要望を反映し、県教育委員会にて情報セキュリティポリシーを作成

▼ クラウド構成図



【効果】

- ・市町村が大分教育ネットワーク(OEN)の運用費用を負担することにより、市町村が積極的にOENの改善に参加する環境を実現
- ・パブリッククラウドを利用することにより、構築及び運用費用の削減を実現
- ・テレワーク環境の提供により、USB媒体の紛失事故を防止

iii) 宮古島市の事例(コミュニティクラウド)

【ICT環境の特徴】

- ・通信路を暗号化した上で、インターネット経由により宮古島市教育委員会及び市内のすべての小中学校35校がクラウドに接続
- ・コミュニティクラウドで出欠・グループウェア、備品管理、指導要録管理の機能を提供(学籍管理は住基系のシステムと連動のため別システム)

▼ ネットワーク全体図

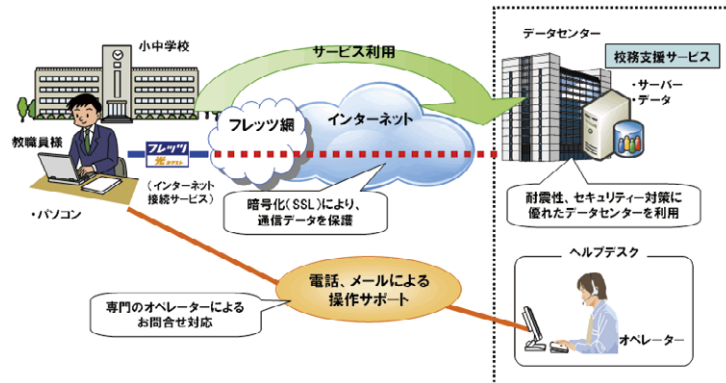


(出典:NTT西日本資料)

【ICT環境の運用における特徴】

- ・コミュニティクラウド上の情報はPCのローカル環境にダウンロードできないように制御
- ・コミュニティクラウド上のシステムでは、一定時間、操作しなかった場合は自動でログアウトを実施

▼ クラウド構成図



(出典:NTT西日本資料)

【効果】

- ・コミュニティクラウドを利用することにより、教育委員会でサーバを所有する場合と比較して費用の削減を実現
- ・通信路の暗号化により、情報漏洩を防止

iv) 柏市の事例(プライベートクラウド、パブリッククラウド)

【ICT環境の特徴】

- ・児童生徒の出欠情報、成績情報を扱うプライベートクラウドの環境を、市内のすべての中学校向けに提供予定(平成25年度より)
- ・緊急時に携帯メールで保護者に連絡ができるメール配信システム(スクールメール)をパブリッククラウドで導入
- ・スクールメールはクラスごとや学年ごと、部活動ごとの連絡配信システムとしても活用

▼ スクールメール画面イメージ

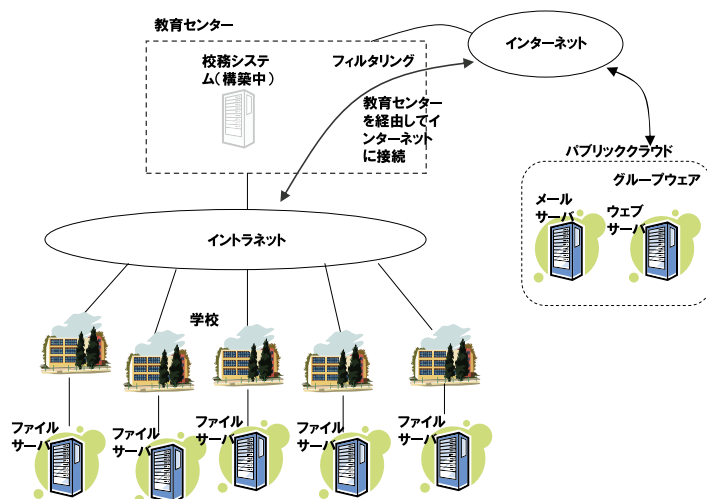


(出典:アルプスシステムインテグレーション資料)

【ICT環境の運用における特徴】

- ・プライベートクラウドの導入以降も、校内サーバは残し、成績や出欠簿はセンターで管理、教材は各学校で管理する分散環境によりシステムが停止するリスクを軽減
- ・教職員に配付しているPCを起動する際は、USB認証(PINコード)による認証を導入

▼ 市イントラネット構成図



【効果】

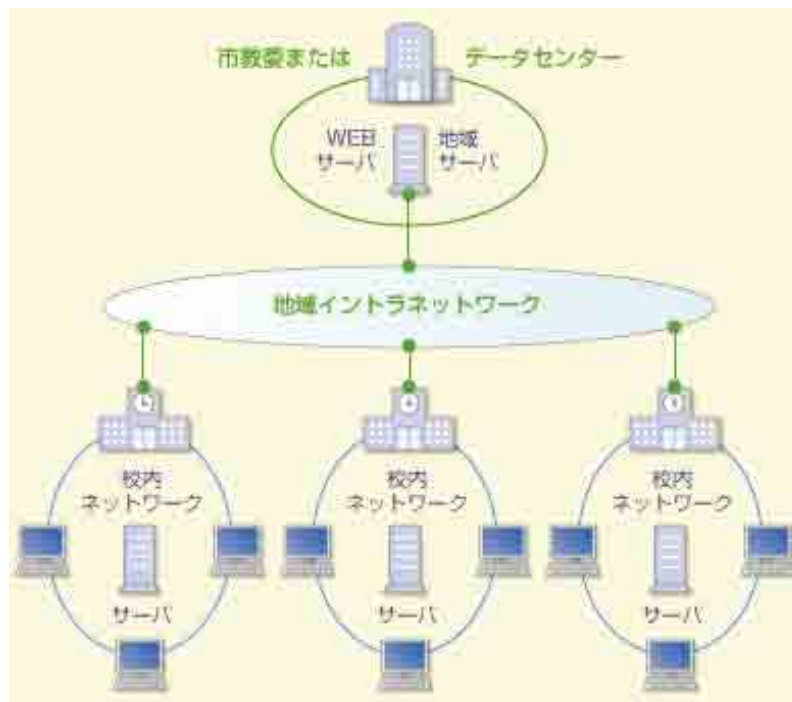
- ・USB認証の導入により、教職員のパスワード管理を簡素化
- ・スクールメールの導入により、児童生徒に関する様々な情報発信(学級通信、部活動情報、修学旅行時の状況報告等)を学校に期待している保護者のニーズに対応

v) 杉並区の事例(データセンター型システム、リモートアクセス)

【ICT環境の特徴】

- ・区の教育委員会がデータセンターに校務支援システムを導入して、児童生徒の出欠・成績管理、指導要録情報、保健情報を扱う機能をすべての学校を対象に提供
- ・各学校からのデータセンターへの接続及び、自宅からのリモートアクセス環境は閉域網にて接続
- ・区の方針からクラウドの利用は禁止

▼ ネットワーク全体図



(出典: スクールオフィスホームページ)

【ICT環境の運用における特徴】

- ・児童生徒の出欠・成績管理、指導要録情報、保健情報はデータセンターのサーバ、教材や児童生徒の作成したファイルは校内のサーバに格納
- ・リモートアクセスは自宅の私有PCからインターネット経由でワンタイムパスワード(パスワードとして毎回異なる意味のない文字列を使って認証を行う仕組み)による認証を行った上で接続

【効果】

- ・校務支援システムをデータセンターに導入することにより、学校ごとに校務支援システムを導入する場合と比べて構築費用を削減
- ・リモートアクセス環境の提供で、USB媒体の紛失事故を防止

1-2 調査結果を踏まえた議論のポイント(学校ICT環境及び情報セキュリティ)

アンケート調査及び現地訪問調査結果等を踏まえて、学校等における情報セキュリティ面において留意すべき事項等として、以下の事例を整理した。

① 各先進事例の特徴整理

まず、各先進事例におけるネットワーク環境と情報セキュリティ対策の特徴について、以下のよう
に分類整理を行った。

i) 学校のネットワーク環境について

ア 学校外のネットワーク環境

- ・各学校は、教育委員会が構築した閉域網の学習系ネットワークを経由してインターネットに接続することで情報セキュリティを確保(横浜市、大分県、柏市、杉並区)
- ・学習系ネットワークの設計・構築を、県教育委員会が市町村の要望も盛り込んで実施し、市町村も運用費用を負担(大分県)
- ・児童生徒の個人情報扱うシステムについては、教育委員会が専用で利用するクラウドサービス(プライベートクラウド)に学習系ネットワーク経由(横浜市、柏市)又は、校務系ネットワーク経由(大分県)で接続して利用、あるいは複数の組織向けに共同で運用されるクラウドサービス(コミュニティクラウド)に通信路を暗号化した上でインターネット経由で利用(宮古島市)
- ・保護者等への公開が前提となっている情報(メール連絡、スケジュール管理等)については、一般に開放され、インターネット上でサービス提供されているクラウドサービス(パブリッククラウド)を利用(大分県、柏市)
- ・教員が自宅のPCから学校内にいる場合と同様の作業が行えるように、リモートアクセスの環境を整備(大分県、杉並区)

イ 学校内のネットワーク環境

- ・ネットワークの共有・相互接続によるリスクへの対応として、児童生徒が授業でデジタル教材やインターネット上の情報等を扱う際に利用する学習系ネットワークと、教員が学籍・成績情報等を扱う際に利用する校務系ネットワークとを分離(横浜市、大分県、宮古島市、柏市、杉並区)
- ・教材や児童生徒が作成したファイル等は学校内のサーバに保管し、学習系ネットワークへの負荷を軽減(杉並区)

ii) 学校における情報セキュリティ対策

ア 技術面の対策

- ・校務支援システムの操作ログ等を取得し、適正な権限統制や不正操作等を防止(横浜市)

- ・クラウド上の情報を、教員がPC等のハードディスクにダウンロードできないように制御(宮古島市)
- ・教職員に配付しているPCを起動する際は、USB認証(PINコード)による認証を導入(柏市)
- ・教員が自宅から校務支援システムに接続するリモートアクセス環境には、ワンタイムパスワードによる認証の仕組みを導入(杉並区)

イ 運用面の対策

- ・情報の重要度を4段階に分類し、段階ごとにデータの扱い方を県の学校情報セキュリティ実施手順にて明確化(大分県)
- ・市町村教育委員会の要望を反映し、県教育委員会にて情報セキュリティポリシーを作成(大分県)
- ・市区教育委員会の情報セキュリティポリシーを各学校が実情に応じ修正して準用(横浜市、宮古島市、柏市、杉並区)
- ・教員が自宅で作業を行えるよう、規定に基づき、パスワードロックが掛かるUSBによる情報の持ち出しを許可(横浜市、柏市)

② 学校における情報セキュリティポリシーの必要性

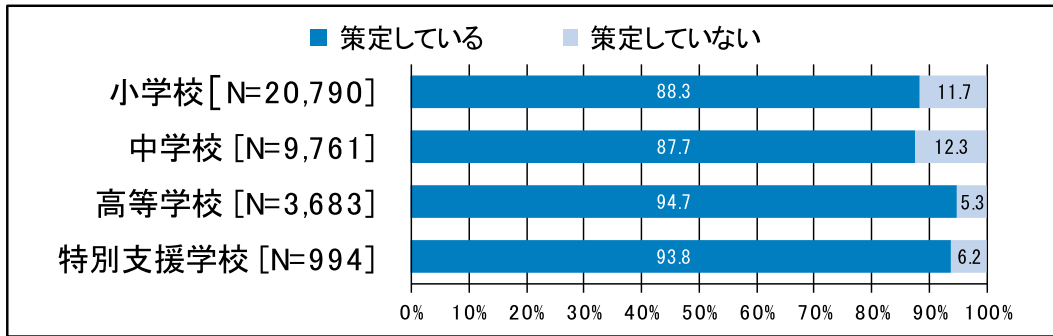
学校における教育の情報化が進みつつある中で、教員1人1台の校務用コンピュータの整備が進むとともに、校務支援システムの導入により、教員の業務負担を軽減し、児童生徒と向き合う時間の確保に取り組む地方公共団体の事例が見られる一方、学校現場における情報漏洩など、情報セキュリティ対策が徹底されていないことを要因とする事故が増えてきている。したがって、学校におけるICTの活用を推進する上で、情報セキュリティの確保は極めて重要であり、こうしたことへの対応として、学校が保有する情報資産の取扱を定め、一人一人の教員がその取扱いを確実に厳守するため、学校における情報セキュリティポリシー[※]の整備が必要という認識が共有された。

※ 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」の三層構造となっている。「基本方針」では、情報セキュリティ対策の目的や原則を定め、「対策基準」では、「基本方針」に基づく情報資産の重要度の定義等を明示している。行政機関等が保有する情報資産の分類と取扱制限等について、「実施手順」で明確にしている。

しかし、小・中学校では12%程度、高等学校及び特別支援学校では6%程度の学校が、情報セキュリティポリシーを策定しておらず、早急な対応が必要である。また、情報セキュリティポリシーを策定している学校であっても、首長部局の情報セキュリティポリシーを適用している学校があり、これらの学校でも、学校が保有する情報資産を踏まえた情報セキュリティポリシーの策定が必要であるとの認識が共有された。

このため、学校における情報セキュリティポリシーの策定を促進し、すべての学校で情報セキュリティポリシーの適切な運用と情報セキュリティの確保につなげることを目的として、学校における情報セキュリティポリシーのポイントについて、実例を挙げながら整理した資料を作成することの必要性について指摘がなされた。

▼ 学校情報セキュリティポリシーの策定状況



1-3 「学校における情報セキュリティについて」の作成

学校現場での情報セキュリティポリシーの整備に向けて、教育委員会が中心となってどのように情報セキュリティポリシーの策定を進めればよいかについて、先進的な取組を実施する地方公共団体の事例等を踏まえ、留意事項や記載内容等を分かりやすく記載した冊子資料「学校における情報セキュリティについて」を作成した。

主な目次構成は以下のとおりであるが、ポイントとなる留意事項を厳選し、ガイドラインとして整理することが大きな目的であり、学校現場で取扱う情報の特殊性から、教育委員会の情報セキュリティポリシーを学校現場がそのまま準用できない場合があると考えられるため、そうした点についての留意事項についてもあわせて記載することとした。

こうした冊子資料が広く学校教育関係者に配布され読まれることを通じて、学校における情報セキュリティポリシーの策定を促進し、すべての学校で情報セキュリティポリシーの適切な運用と情報セキュリティの確保につながることが期待されることである。

▼ 「学校における情報セキュリティについて」の目次

- (目次構成)
1. 本資料の位置づけ
 2. 学校情報セキュリティポリシーの整備について
 - 2.1. 学校情報セキュリティポリシーの全体像
 - (1) 地方公共団体における情報セキュリティポリシーの整備の流れ
 - (2) 学校情報セキュリティポリシーの必要性
 - (3) 学校情報セキュリティポリシーの概要
 - ① 基本方針と対策基準の記載事項
 - ② 実施手順の記載事項
 - (4) 学校情報セキュリティポリシーの整備に向けて
 - 2.2. 実施手順の内容
 - (1) 「実施手順」における記載事項の概要
 - (2) 「5 情報区分」における記載事項
 - (3) 「6 日常の留意事項」における記載事項
 - 2.3. 学校情報セキュリティポリシーの運用と啓発

① 学校における情報セキュリティポリシー作成上のポイント

教育委員会に対するアンケート調査結果及び各先進事例の検討に基づいて議論を行い、学校における情報セキュリティポリシー作成上のポイントとして、以下の項目を具体的に記載している。

1. 情報資産の分類

(1) 情報の重要性に応じて、3～4程度の区分に分類する(対策基準)

→ 個人情報の有無、情報漏洩による被害の程度を基準とし、重要度A～Dの4つの区分に分類(大分県教育委員会)

→ 情報漏洩による被害の程度を基準とし、重要度高～低の3つの区分に分類(杉並区教育委員会)

(2) 各情報資産を(1)の区分のいずれかに分類する(実施手順)

→ 指導要録や出席簿は重要度Aに分類(大分県教育委員会)

2. 情報資産の取扱制限の整理(実施手順)

→ 重要度Aの情報資産は持ち出し禁止とし、電子データは、教育委員会が設置するアクセス制御の決定ができる装置に保存(大分県教育委員会)

3. 教職員が遵守すべき具体的な取扱いの整理(実施手順)

→ 重要度A、Bに該当する情報資産の電子データを、校務用パソコンのローカルハードディスクに保存したまま退校することを禁止(大分県教育委員会)

→ 保存する必要のない情報(一時ファイル)は確実に消去(大分県教育委員会)

なお、学校が保有する情報資産は、例えば、指導要録や出席簿など各学校に共通するものが多いと考えられるため、その分類や取扱制限等も各学校で共通のものとするのが適切であると考えられる。このため、学校における情報セキュリティポリシーは、学校の設置者である教育委員会と学校とが連携してその内容を整理することが望ましい。

また、教職員の人事異動を考慮すれば、都道府県と市町村の教育委員会とが連携協力して、情報資産の分類や取扱制限等の共通化を図ることが望ましいと考えられる。