経済産業省委託調査

平成１５年度

初等中等教育現場における
情報セキュリティに係る現状調査報告書

平成 16 年 3 月

グローバルセキュリティエキスパート株式会社

この報告書は、平成 15 年度受託事業として、グローバルセキュリティエキスパート株式会社が経済産業省から委託を受けて、財団法人コンピュータ教育開発センターの協力を得て実施した「平成１５年度初等中等教育現場における情報セキュリティに係る現状調査」の成果を取りまとめたものです。

はじめに

本調査は、小中高等学校の情報セキュリティの現状について調査を行ったものである。

個人情報の漏えいなどの事件・事故が連日のように報道されている昨今、情報のセキュリティ対策の強化が求められている。学校現場でも、インターネットの教育への活用や、日常の業務の中での電子データの取り扱いなどの比重が日増しに大きくなってきている。今回の調査では、学校における情報セキュリティの実態や教育センターが運営する学校ネットワークの管理状況等について調査を実施した。

今後、本報告書が、学校における情報セキュリティ対策を検討及び推進する上での一助になれば幸いである。

謝　辞

経済産業省委託調査研究である「平成１５年度初等中等教育現場における情報セキュリティに係る現状調査」の実施にあたっては、財団法人コンピュータ教育開発センター様にアンケートの配付、回収、インタビュー先の選定等で大変お世話になりましたことを厚く御礼申し上げます。また、ご多忙中にもかかわらず、アンケートの回答、インタビューへの応対など積極的に協力して頂いた教育関係者の皆様にも厚く御礼申し上げます。

平成 16 年 3 月

グローバルセキュリティエキスパート株式会社

学校における
情報セキュリティの現状について
(要約、課題と提言)

目　次

1. 学校における情報セキュリティの現状調査について

1.1. 背景

平成 15 年 10 月に経済産業省が策定した「情報セキュリティ総合戦略」では、国民のセキュリティリテラシーの向上施策として「義務教育段階からのセキュリティリテラシー教育の実践」を求めている。セキュリティ意識（セキュリティ文化）を身につけられる環境を整備するにあたって、教育現場がどの程度相応しい環境を有しているのか、相応しくないならば、どのような整備が行われるべきかが検討される必要がある。しかしながら教育現場のセキュリティ環境についての実態調査は、かつて実施されたことがなく、十分な検討材料がないのが現状である。

> 第３章　戦略実現のための具体的施策
> ３．２．２企業・個人における事前予防策
> (３）セキュリティリテラシーの向上
> ②義務教育段階からのセキュリティリテラシー教育の実践
> 義務教育の段階からセキュリティリテラシーに関する内容を学習カリキュラムに組み込み、子供がネット社会の一員となるための基礎的素養としてセキュリティ意識（セキュリティ文化）を身につけられる環境を整備するよう、検討を進める。その際、IT リテラシーの内容の一部として盛り込む他に、「知らない人についていかない」「道路に急に飛び出さない」といった一般的な安全教育や安全保障教育の一部として盛り込むことが必要である。
> 【情報セキュリティ総合戦略より】

1.2. 今回の調査の目的と狙い

こうした背景から、「情報セキュリティ総合戦略」が求める義務教育段階でセキュリティ意識（セキュリティ文化）を身につけられる環境整備を推し進めて行くにあたって、今後、継続的に整備状況を評価するためにも小中高等学校におけるインターネットやコンピュータの利用環境と都道府県及び政令指定都市教育センターが行っている学校関係のネットワーク管理業務を対象とした「学校における情報セキュリティの実態に関する定点観測」が行えるフレームワークを構築する必要がある。フレームワークの構築に際しては、定点観測としての定期的な調査が実施可能か、可能とすればどのような調査が適切かを模索するための予備的な調査が不可欠であり、今回の調査は、教育現場におけるセキュリティ上の喫緊の課題を明らかにするとともに、将来の定点観測を可能とするための実態調査のあり方を目的として行った。

1.3. 調査方法と調査対象

調査方法と期間	➢アンケート方式:平成 16 年 2 月 1 日～平成 16 年 2 月 20 日 ➢インタビュー方式:平成 16 年 2 月 17 日～平成 16 年 3 月 12 日
アンケート配付先と回収率	➢全国の小中高等学校無作為抽出 206 校配付、回収 99 部(回収率 48%) ➢都道府県ならびに政令指定都市の教育センター59 ヵ所配付、回収 41 部(回収率 69%)
インタビュー	インタビュー時間は、1 ヵ所あたり 1.5 時間設定した。 ① 都道府県及び政令指定都市の教育センター8 ヵ所 ② 学校の教職員(高等学校 1 名、小学校 4 名) ③ 都道府県及び政令指定都市以外の教育センター2 ヵ所

1.4. 分析に利用した情報セキュリティ基準

実態調査項目の網羅性を保証するため情報セキュリティ対策の国際標準と目される「ISMS 認証基準(Ver.2.0)」(以下、ISMS と表記)を参考にアンケートならびにインタビュー項目の作成を行った。

2. 学校における情報セキュリティに関する課題と提言

2.1. 学校の実状を踏まえた情報セキュリティポリシー策定ガイドラインの提示

課題	現状の学校の情報セキュリティポリシーは、県あるいは市の教育委員会から配布されたものがあるものの実状に合っていないために運用されていなかったり、運用されている場合でもネットワークやパソコンを対象とした限定的なものが多い。本来の情報セキュリティポリシーとは、ネットワークなどに対象を限定したものでもなく、幹部教職員を中心に学校が組織として取組むものであり、組織のセキュリティ・レベルを継続的に向上させていくものにしなければならない。
提言	学校の情報セキュリティポリシーは、学校が児童・生徒の成長に係わる機微な個人情報を保有することや、児童・生徒に対して情報セキュリティ教育や情報モラル教育を行う場でもあることから、官庁や民間の情報セキュリティポリシーとは異なった要件が求められる。加えて多くの学校では、授業時間外に教職員が情報システムの保守管理業務などを兼務している実態がある。これら学校の実状を踏まえた、情報セキュリティポリシーのあるべき姿を示すガイドラインが提示されることが望まれる。実現のために、次のような施策が求められる。 ① 現状の情報セキュリティポリシーがどのように利用されているのか、あるいは規律としての拘束力を持つものかを調査する。 ② 情報セキュリティポリシーに責任者と担当者の権限と責任がどのように明記されているのか、その内容の実行可能性と十分性について調査する。 ③ ①と②の調査を踏まえて、情報セキュリティリティポリシーの類型化を試みるとともにそれぞれの類型の長所、短所について分析を行う。
付録参照ページ	3.2.1 策定しても実践されない学校の情報セキュリティポリシー 3.2.2 不明確な学校の情報セキュリティに関する責任と権限

2.2. 教職員のシステム保守作業などの負担軽減

課題	学校運営予算の制約から、校内ネットワークやコンピュータの管理業務は付随業務として、わずかな担当教職員が放課後や授業の休み時間に行っている。したがって、担当教職員の不在時にコンピュータの障害が発生した場合には、授業が不可能になるといった状況が予測される。また、システムの保守作業が加重なため、パソコンの新規導入などの作業を拒む傾向があるとの意見も聞かれた。教育の情報化を推し進めるためにも、教職員のシステム保守作業などの負担を軽減させる必要がある。
提言	担当教職員の作業負荷が授業に支障を与えない仕組みや担当教職員の負担を軽減するために、システムの保守管理業務支援や情報セキュリティの専門家の派遣、あるいは巡回サービスを実施するなどの効果的な管理体制を検討し、整備されることが望まれる。実現のために、次のような施策が求められる。 ① 情報システム担当教職員がシステム保守など、作業に費やしている時間とその作業内容について実態を把握する。
付録参照ページ	3.2.3 学校のネットワーク及びシステム管理業務を行うわずかな要員 3.2.4 学校の情報セキュリティ対策費の状況

2.3. 児童・生徒の個人情報の分類及び取扱い基準の提示

課題	現在多くの学校で、教職員の私物のパソコンや電子媒体が持ち込まれて業務が行われている実態がある。さらに児童・生徒の個人情報が私物のパソコンや電子媒体に記録され、教職員の自宅で作業が行われている。私物のパソコンや電子媒体を紛失したり、盗難されることで、児童・生徒の個人情報が漏えいの危険にさらされている状況がある。教職員の私物のパソコンや電子媒体の持ち込みを必要としない環境整備を推し進める必要がある。
提言	教職員が接する児童・生徒の個人情報は、学習能力、生活態度、家族関係、身体能力、健康状態といった極めて機微な情報である。これらの情報は、「**児童・生徒の将来に係わる極めて秘密性が要求される情報**」である。 児童・生徒の個人情報の取り扱い基準を、学校の情報セキュリティポリシー策定のためのガイドラインとともに提示し、個人情報の漏えいを予防する措置を講ずることが望まれる。実現のために、次のような施策が求められる。 ① 私物のパソコンの持ち込み数量と利用目的を調査する。 ② 私物のパソコンを利用しないで済む環境を構築するための必要数量を調査する。
付録参照ページ	3.2.5 学校への私物のパソコンや電子媒体の持ち込みの問題 3.2.6 教育センターへの私物のパソコンや電子媒体の持ち込みの問題

2.4. 学校長をはじめとする教職員の情報セキュリティへの理解と意識の向上

課題	学校では、教員の私物のパソコンや電子媒体の持込みに起因するコンピュータウイルス感染や私物のパソコンの盗難事件などが発生している。情報セキュリティ教育を実施しても「関心」を示さない教員もいるとの意見があった。情報セキュリティの重要性が教職員に十分理解されていない状況が見受けられる。また、教育センターに対するアンケートでも学校教職員に対する情報セキュリティ教育を求める声が上がっている。教職員の情報セキュリティに対する理解と意識の向上を図っていく必要がある。
提言	セキュリティ事件・事故を予防するため、学校長をはじめとする全教職員を対象とした情報セキュリティ意識を定着させるための教育の実施が望まれる。実現のために、次のような施策が求められる。 ①　学校長や教頭の情報セキュリティに対する意識調査をする。 ②　教職員に必要な情報セキュリティの基本的知識などの理解状況の調査をする。 ③　①と②を踏まえて、これらの調査をレベル評価する。 ④　ネットワークとシステム管理を担当する教職員に、これらの業務を行う場合の不安事項や必要事項を調査する。
付録参照ページ	3.2.3 学校のネットワーク及びシステム管理業務を行うわずかな要員 3.2.7 セキュリティ事件・事故から学ぶ情報セキュリティ教育と情報モラル教育

2.5. 児童・生徒への情報セキュリティと情報モラルについての教育の実施

課題	一般に公開されているホームページの掲示板への「いたずら書き」の発覚によって、掲示板管理者からのクレームも発生している。一般に「掲示板荒らし」といわれるもので、発覚した件数は、氷山の一角であると考えられる。掲示板への「いたずら書き」によって相手を傷つけることもある。したがって、自身の身を守る情報セキュリティ教育とともにネット社会を構成する一員としてのルールを守る情報モラル教育を確実に行う必要がある。
提言	義務教育の段階からセキュリティリテラシーに関する内容を学習カリキュラムに組み込み、ネット社会の一員となるための基礎的素養としてセキュリティ意識（セキュリティ文化）を身につけられる環境を整備する必要がある。児童・生徒がネット社会のルール違反の罪の重さや被害者の痛みがわかる教育が望まれる。実現のために、次のような施策が求められる。 ① 児童・生徒への情報セキュリティと情報モラルの意識と理解度を調査する ② 児童・生徒への情報セキュリティと情報モラルに関する教材を提供する。
付録参照ページ	3.2.7 セキュリティ事件・事故から学ぶ情報セキュリティ教育と情報モラル教育

2.6. 教育センターに対する情報セキュリティ監査の実施

課題	教育センターでは、委託先によってシステム管理業務、ネットワーク管理業務が営まれている。大半が「性善説」に立った民間業者への委託という形で行われている。一方、近年相次いでいる個人情報の漏えい事件は、委託先要員など内部関係者によっておこされている状況があり、委託先の管理、監督が厳しく行われる必要がある。一旦事件・事故が発生した場合、委託元である教育センターの監督責任が問われるが、現状、委託元として、委託先を監督し、内部統制上のけん制を行う仕組みが機能しているとは言い難い。委託先に対する監督責任を果たすために必要な要件を明らかにし、委託を行う際のガイドラインが示される必要がある。
提言	教育センターの学校関係のネットワークの運用管理は、定期的にネットワーク侵入検査を含めた情報セキュリティ監査を行い、不正行為が行われていないかを点検、評価できる体制の確立が望まれる。実現のために、次のような施策が求められる。 ① 運用委託先から学校のネットワークに対する侵入検査を行い、ネットワークセキュリティ上の脆弱性について調査する。 ② 運用委託先のアクセスログの解析を行い、運用委託先から提出されている作業報告書などの妥当性について調査する。 ③ 運用委託先の情報セキュリティポリシーの内容と遵守状況を調査する。 ④ システム上あらゆる実行権限が付与されているシステム管理者権限が付与されたユーザーID の取扱いが適切に行われているか、使用されているパスワードが脆弱なものでないか調査する。
付録参照ページ	3.2.8ID の管理とパスワードの取り扱い 3.2.9 委託業務の信頼関係に関する懸念 3.2.10 委託先要員へのシステム管理者権限の ID とパスワード 3.2.11 ネットワーク侵入検査と情報セキュリティ監査への要望

3. 情報セキュリティ現状調査の要約

前節の「学校における情報セキュリティに関する提言と課題」に関する調査要約を掲載する。

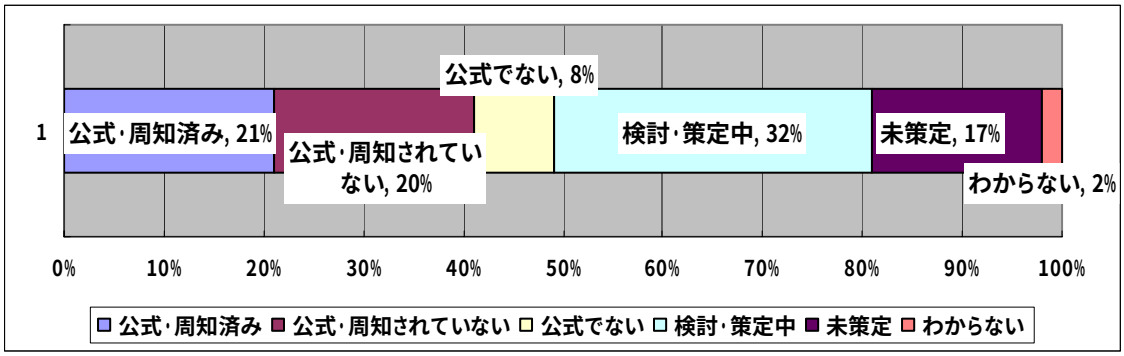
3.1. 調査概要

学校の調査概要	学校のネットワーク及びシステム管理業務を担当する教職員に、ISMS をもとに作成した 50 項目の質問と情報セキュリティ教育の質問、政策への意見などのアンケートを実施した。アンケート回収数は、小中高等学校合わせて 99 校であった。また、アンケートを補完する意味で、これらの業務を担当する教職員にインタビューを実施した。
教育センターの調査概要	学校関係のネットワーク及びシステム管理業務を担当する方に、学校と同じくISMS をもとに作成した 50 項目の質問と政策への意見などのアンケートを実施した。アンケート回収数は、41 センターであった。また、アンケートを補完する意味で、アンケートが回収できた 41 センターの約 2 割に相当する 8 センターに対してインタビューを行った。教育センターには、「運用委託先の管理者」としての立場の側面と「学校ネットワークの運用管理者」の立場の側面とがあり、それぞれの立場に対するインタビューを実施した。
アンケートに寄せられた政策への意見	アンケートの最後に、政策への意見を頂いている。頂いた意見は、「学校における現状報告について(アンケートの部)」、「教育センターにおける現状報告について(アンケートの部)」に掲載している。学校からの政策に対する意見としては、「予算の厳しさ」、「学校への専任スタッフの配置などによる担当者の負担軽減」、「教員へのパソコンの支給」などが共通してあげられている。
留意事項	インタビュー先では、手順書などの閲覧、運用記録の精査やサーバ室への調査などは行っていない。また、インタビュー時間を 1.5 時間と設定し、訪問先の業務を極力妨げないように配慮し実施した。インタビュー記録については、訪問先の教育センターや学校の情報セキュリティ上の脆弱性も掲載しているために、個別の名称は全て匿名としている。アンケートの意見欄も同様の扱いとした。

3.2. 分析結果総括

3.2.1. 策定しても実践されない学校の情報セキュリティポリシー

【学校の情報セキュリティポリシー】

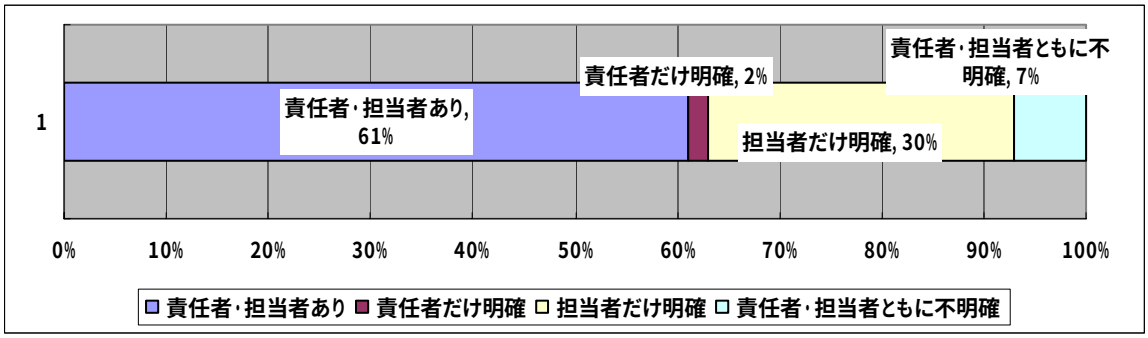


「公式で周知されていない」、「公式でない」を合わせると 28%になる。策定しても実践がともなわない。

【インタビュー結果】今回のアンケートでは、情報セキュリティポリシーの詳細についての質問を行っていない。インタビューの結果からは、情報セキュリティポリシーに対する理解が、まちまちであることがわかった。「システム運用要綱」、「学校ネットワーク利用規程」と呼ぶものが、情報セキュリティポリシーであるとする回答もあり、情報セキュリティポリシーに該当するとされているものが必ずしも情報セキュリティ・レベルを組織的に向上させていくためのＰＤＣＡサイクルを規定したものとはなっていない。情報セキュリティポリシーとされているものが、パソコンやネットワークを対象とした限定的なものである可能性が高いことが伺える。「学校への情報セキュリティポリシー策定支援はどのようにしていますか」との質問に対しては、多くが、「管轄している学校へ情報セキュリティポリシーを教育委員会長名で通達している」と回答している。したがって、教育委員会単位で見た場合、同じ情報セキュリティポリシーが共用されていると考えられる。

3.2.2. 不明確な学校の情報セキュリティに関する責任と権限

【責任者・担当者の権限と責任】



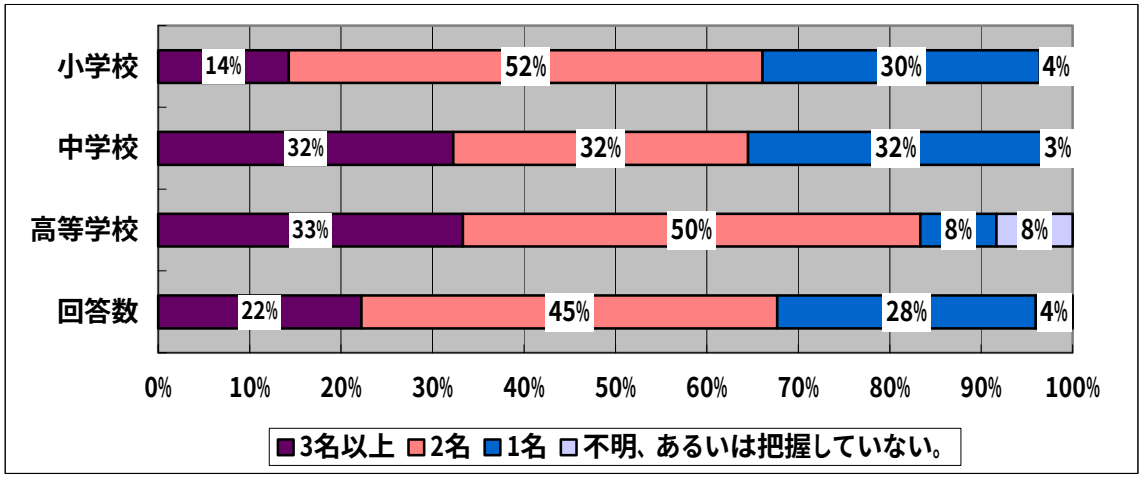
責任者が不明確 30%、責任者と担当者が不明確 7%を合わせると 37 パーセントで責任者が不明確になっている。

【インタビュー結果】情報セキュリティポリシーまたはその付随文書などに、責任者や担当者の権限と責任が明記されている必要があるが、学校の情報セキュリティに対する権限と責任は、不明確な状態であることが伺える。

【責任者不在の懸念】学校のネットワーク及びシステム管理業務を担当する教職員からは、責任者が不在、また、責任者の存在が不明確とする回答を得ている。責任者が不明確な状態は、情報セキュリティに係わる事件・事故といった緊急時に混乱が予想されることもさることながら、平時においても学校長等のしかるべき地位にあるものが責任を負わなければ、組織として情報セキュリティが向上する土壌が醸成されないと考えられる。したがって担当の教職員では、技術的な取り組みは行えても、組織的な取り組みについては、困難であることが予想される。

3.2.3. 学校のネットワーク及びシステム管理業務を行うわずかな要員

【学校のシステム担当者数】

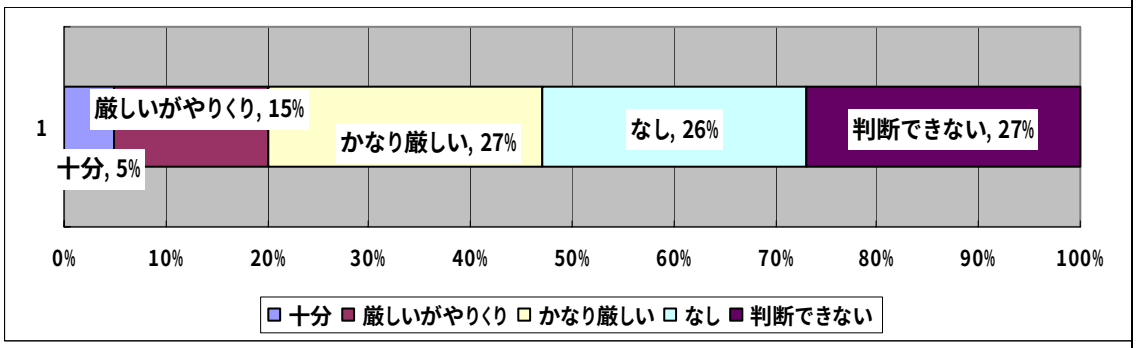


学校のシステム管理担当は 1 名が 28%、2 名が 45%で、合わせて 73%が 2 名以下で実施している。

【インタビュー結果】教職員がネットワーク及びシステム管理業務について、担任と兼務している者が 2 名体制で行っている高等学校や小学校でも補助者を入れて 2 名体制の学校もあるが、他は全て 1 名で行っていた。児童・生徒への授業や部活動以外に、これらの業務を行っていることがわかる。自宅で学校のホームページのコンテンツ作成作業を行っているケースや、教育用パソコンを持ち帰りオペレーティングシステムの修正パッチの適用を自宅で実施しているケースもあった。担当者からは、情報セキュリティに関し、十分な知識があるわけではないために、技術的な対策も十分に行えないとの要望があった。

【少ない要員数と授業や業務への影響】1 名で校内のネットワーク及びシステム管理業務をしている場合、病気などの長期休暇時に教育系のコンピュータの障害に、速やかな対処が行えないなどの事態も想定され、授業への影響も懸念される。また、担当者が 1 名の場合は、誤謬や不正の発見が困難になる場合もある。ネットワーク及びシステム管理業務の担任を持っている教職員が行っているために、日常の作業の負担が大きく、コンピュータの新規導入やシステムの更新を拒むなどのケースが発生しているとの回答もあった。

3.2.4. 学校の情報セキュリティ対策費の状況

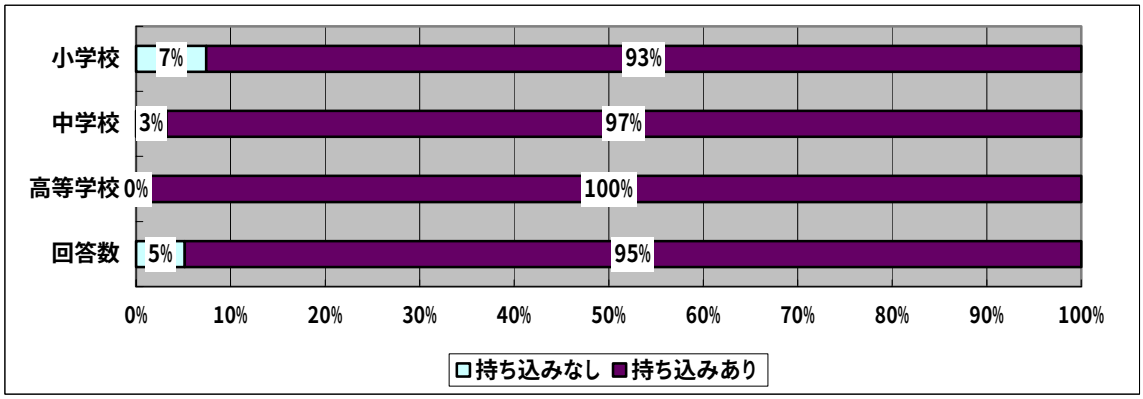


「かなり厳しい」27%、「なし」26%を合わせると 53%に上り、「十分」は 5%しかない。

【インタビュー結果】学校へのインタビューでも、ネットワーク作業などを行う場合、費用的に厳しく十分な措置が講じられないとの回答や、業者への依頼についても、費用が捻出できないために教員が手間と時間を掛けて行っているとの回答があった。

3.2.5. 学校への私物のパソコンや電子媒体の持ち込みの問題

【私物パソコンの学校への持ち込みの有無】



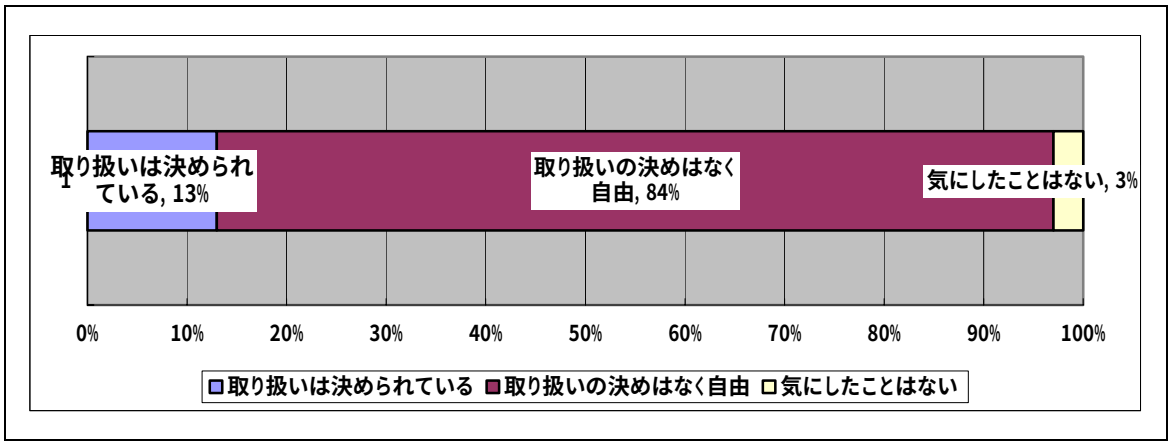
私物パソコンの持ち込みが常態化の傾向にある。

【インタビュー結果】教育センターでの紹介のあった事例も含み 10 ヵ所全てで、学校での持ち込みが行われていることが確認された。

学校のアンケート:私物パソコンの持ち込み実数欄への回答の合計

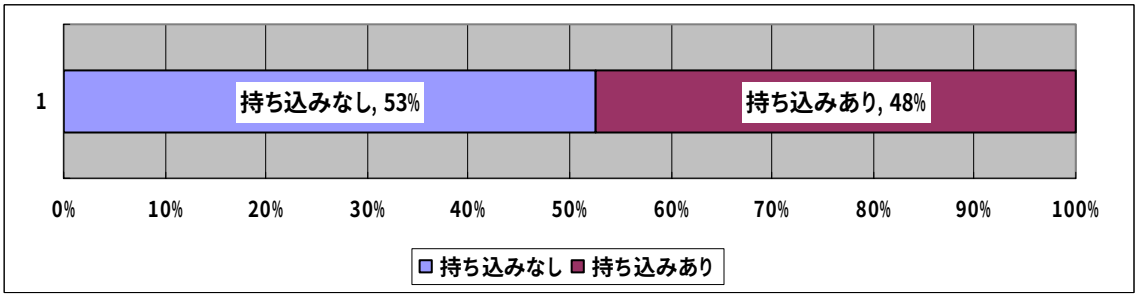
学校別	持ち込み校の全教職員数	持ち込み教職員数(内数)	持ち込み教職員比率
小学校	1,195	685	57%
中学校	751	504	67%
高等学校	747	259	35%
計	2,693	1,448	54%

【学校の MO などの電子媒体の取り扱い】



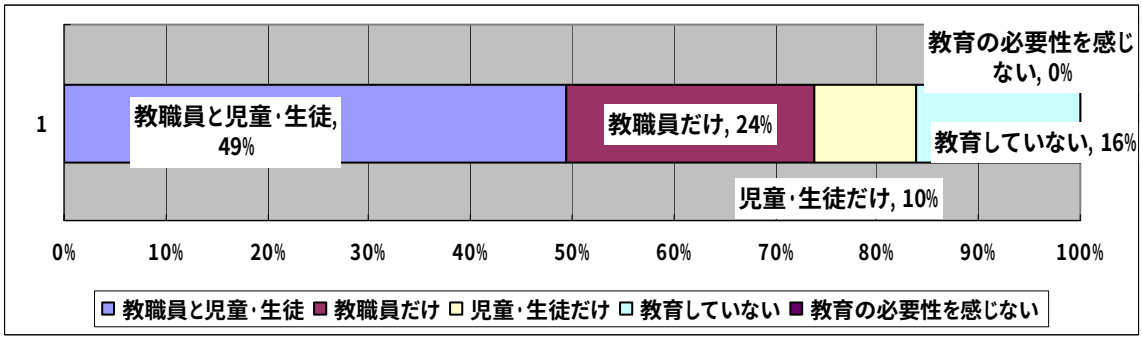
3.2.6. 教育センターへの私物のパソコンや電子媒体の持ち込みの問題

【私物パソコンの教育センターへの持ち込みの有無】



3.2.7. セキュリティ事件・事故から学ぶ情報セキュリティ教育と情報モラル教育

【情報セキュリティ教育の状況】



情報セキュリティ教育が「必要ない」との意見は 0%で、アンケート回答者全員が「必要性」を認めている。教育センターへのアンケート項目でも、学校のセキュリティへ最も望む事項として、教職員への情報セキュリティ教育の充実、または実施を要望している割合は、66%に上る。

【インタビュー結果】学校へのインタビューでも、教職員へ情報セキュリティ教育をしても、

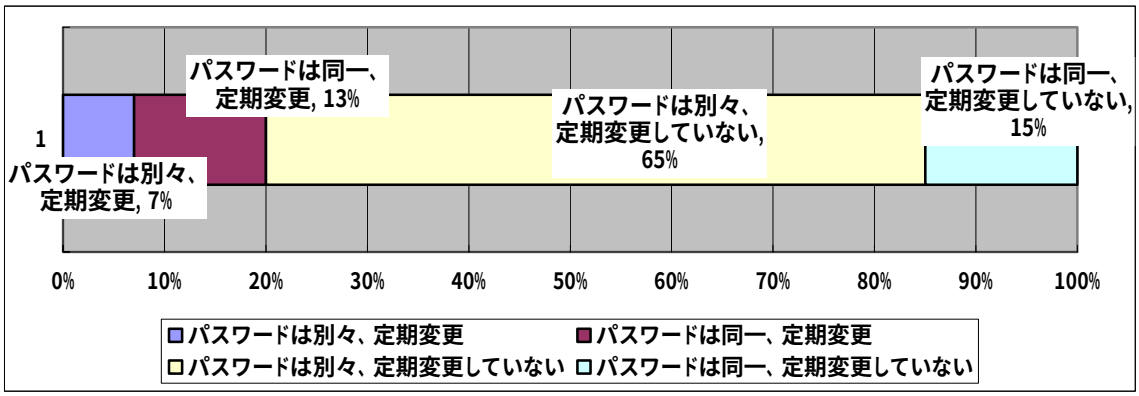
「関心」を示さない教職員には、教育をしても理解してもらえないとの回答を得ている。教育センターのインタビューでは、「技術的な対策は限界がある。」、「教職員のヒューマンセキュリティへの取り組みが必要」との意見があった。

情報セキュリティ教育・情報モラル教育への課題－事故からの学習

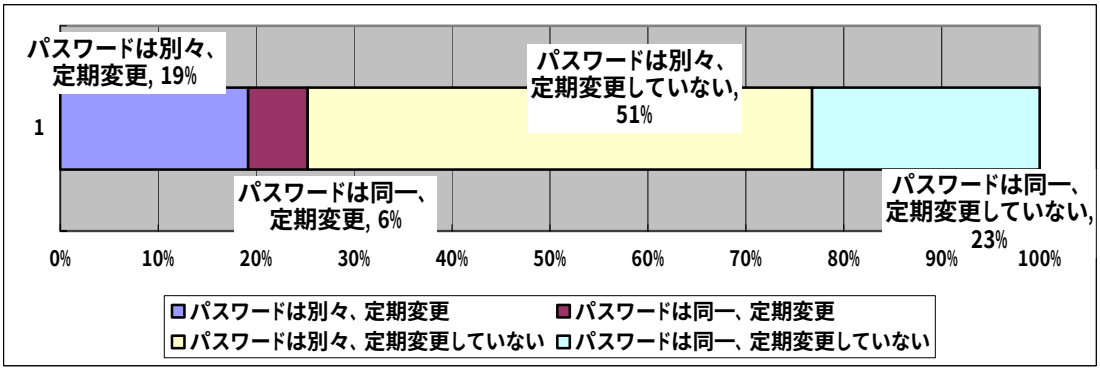
【コンピュータウイルス感染】コンピュータウイルスは、現状でも十分な対策が行われているが、校内での感染例が多い。原因は、私物のパソコンにコンピュータウイルス検知ソフトウエアが導入できていないことやパターンファイルの更新も個人任せになっていることが挙げられる。 持ち込みパソコンの校内ネットワークへの接続については、ウィルスチェックを前提に許可している例があるが、私物のパソコンが持ち込まれた際、所有者以外がウィルスチェックをしているのか、いないのかを確認することは、私物のパソコンであるが故にプライバシーへの配慮から困難であるとの指摘があった。
【私物のパソコンの盗難】教職員が校内に持ち込んで使用していた私物のパソコンが、通勤途上で「車上荒らし」に遭い、盗まれたケースがあった。
【掲示板荒らし】生徒による外部の掲示板へのいたずら書きが発覚し、掲示板管理者からクレームとして教育センターに連絡があった。この種の事例は、幾つかの教育センターで確認されている。掲示板の管理者から報告が来るものは、氷山の一角であると考えられる。児童・生徒への情報モラル教育の重要性が改めて認識される必要がある。
【ポートスキャン】学校から教育センターへのポートスキャン行為は、56%あるとのアンケート結果を得ている。教育センターへのインタビューでも工業高校などで、ポートスキャンツールを利用した授業が行われている場合があるとの回答があった。ポートスキャンツールは、システムへの不正侵入の準備行為として利用されるツールでもある。ポートスキャンそのものは、違法行為ではないが、不正アクセスを助長するおそれもありツールの利用方法などを定めておく必要がある。

3.2.8. ID の管理とパスワードの取り扱い

【教職員のパスワードの取り扱い】



【児童・生徒のパスワードの取り扱い】

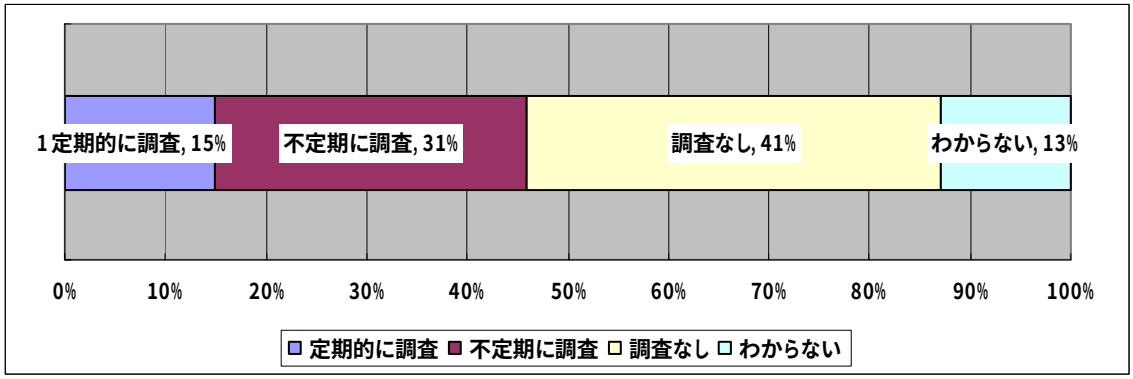


教職員のパスワードを別々に設定し定期変更しているのは、19%だけであり、児童・生徒についても、7%しかない。

【インタビュー結果】学校ホームページのコンテンツ更新に使用する ID とパスワードについて、教育委員会から「表」として一覧が配付されているために、パスワードが公開された形で運用されている状況があった。教員の異動があっても、前任者のパスワードがそのまま利用されているケースもあり、ID とパスワードのずさんな管理は、不正アクセスやホームページの改ざんにつながるおそれがある。

3.2.9. 委託業務の信頼関係に関する懸念

【委託先要員のアクセスログ等の調査】

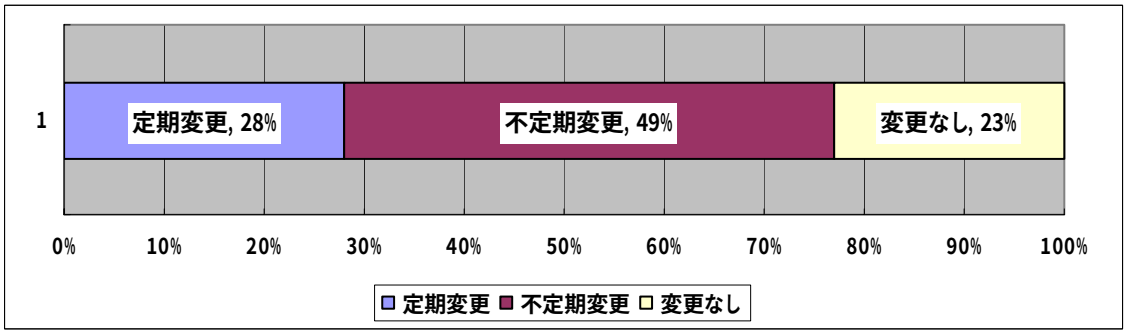


委託先の調査をしていない割合は 41%に上り、定期的な調査も 15%しかない。

【インタビュー結果】教育センターの学校へのネットワーク及びシステム管理業務は、完全な外部委託やセンター内に派遣要員が常駐する形で行われているケースがあり、全ての教育センターで何らかの委託が行われていた。委託業者からの定例報告や定例会などで確認を行っているとの回答は得られたが、「委託先要員のアクセスログの点検を行っていますか」との質問については、「実施していない」との回答が大半であった。

3.2.10. 委託先要員へのシステム管理者権限の ID とパスワードの提供

【システム管理者権限 ID のパスワード変更】



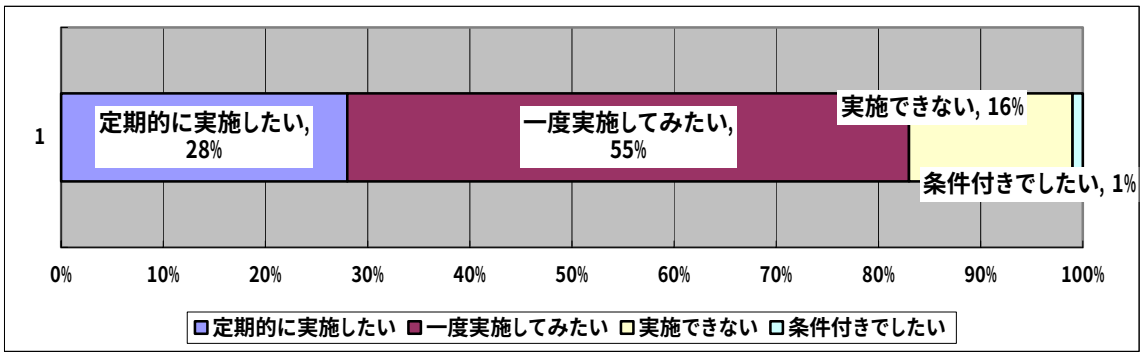
教育センターのシステム管理者権限 ID の「変更なし」は、23%になる。「定期変更」している割合も 28%しかない。

【インタビュー結果】システム管理者権限が付与されたユーザーID の管理は、システムに対して全ての実行権限が付与されているために非常に重要である。システム管理者権限が付与されたユーザーID を委託先要員が利用する場合、アクセスログなどの保管や点検が重要になる。また、システム管理者権限が付与されたユーザーID に対するパスワードは定期的な変更を行い、パスワードの漏えいを予防する措置を講じる必要がある。

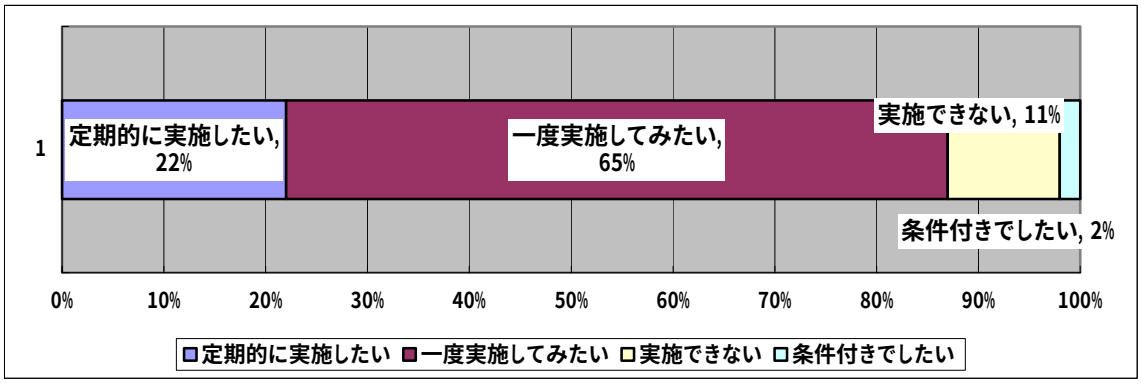
3.2.11. ネットワーク侵入検査と情報セキュリティ監査への要望

学校も教育センターも、「定期的に実施したい」と、「一度実施してみたい」との思いを合わせると 8 割以上になる。教育センターでは、9 割になる。

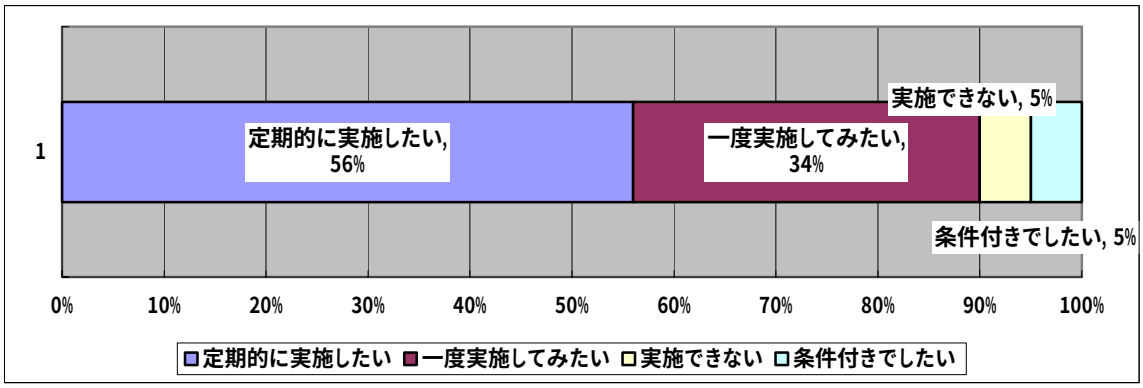
【学校のアンケート結果:ネットワーク侵入検査】



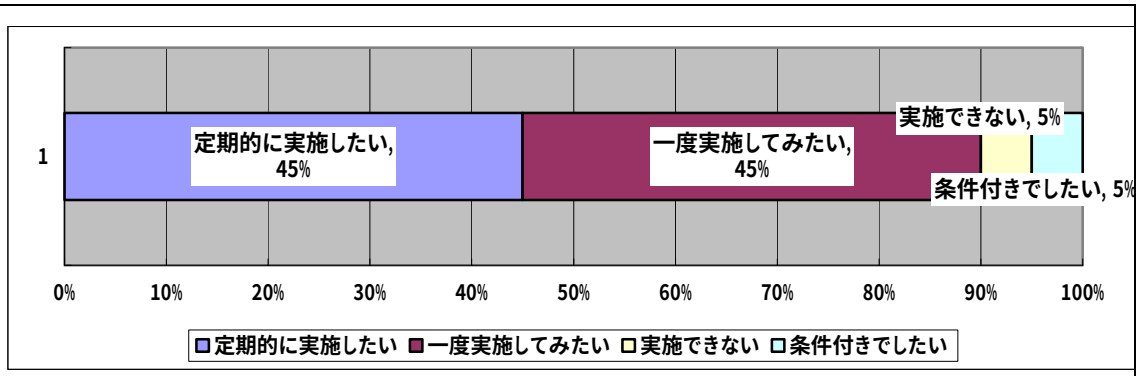
【学校のアンケート結果:情報セキュリティ監査】



【教育センターのアンケート結果:ネットワーク侵入検査】



【教育センターのアンケート結果:情報セキュリティ監査】



【インタビュー結果】インタビュー先の教育センターでは、完全に外部委託しているセンターもあったが、委託先要員の不正行為を予防する観点からの点検は行われていない。外部委託している教育センターを対象にネットワーク侵入検査、情報セキュリティ監査を行う必要がある。

以上