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

提言書

平成 28 年 10 月 27 日

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

名　　簿

委員長	内田　勝也　委員	情報セキュリティ大学院大学　名誉教授
委員	堀　　良彰　委員	佐賀大学全学教育機構 自然科学部門／ＩＣＴ活用教育支援室　教授
	山辺　直義　委員	ひらつか西口法律事務所 弁護士（システム監査技術者）
	森本　貴彦　委員	佐賀新聞社編集局メディアコンテンツ部長 兼　論説委員

目　　次

委員会設置の経緯 1
検証及び検討の方法 2
第１　事案の経緯等 3
１　事案の経緯 3
２　窃取されたファイル等 5
２．１　調査対象 5
２．２　調査結果の概要 5
第２　被害を受けたシステムの構成及び発見された脆弱性 7
１　SEI-Net 7
１．１　SEI-Net のシステム構成 7
１．２　発見された脆弱性 9
１．３　脆弱性への対応（実施済） 9
２　校内 LAN 11
２．１　校内 LAN システムの構成 11
２．２　校内 LAN の問題点 11
２．３　校内 LAN の問題点への対応（実施済） 12
第３　運用管理 13
１　SEI-Net 13
１．１　運用管理事項 13
１．２　運用管理体制 14
１．３　運用に係る問題点 14
２　校内 LAN 15
２．１　運用管理事項 15
２．２　運用管理体制 16
２．３　運用に係る問題点 17
２．４　運用に係る問題への事案覚知後の対応（実施済） 21
３　学習用 PC 23
３．１　運用管理事項 23
３．２　運用管理体制 24
３．３　運用に係る問題点 25
第４　不正アクセスの手法 26
１　フィッシングによる管理者 ID、パスワードを取得 26
２　無線 LAN に接続 26
３　学習用サーバ（校内 LAN）へ侵入 26

４　校務用サーバ（校内 LAN）へ侵入 27
５　SEI-Net への不正アクセス 27
６　SEI-Net からのデータ取得 28
【参考】不正取得したデータについて 29
第５　Ｓ高校での関連事案と対応 30
１　平成 27 年 6 月事案 30
１．１　事案概要 30
１．２　事業者の対応 30
１．３　教育情報課の対応 31
２　平成 27 年 9 月事案（ツイッターで投稿がなされている事案） 33
２．１　事案概要 33
２．２　教育情報課の対応 33
３　平成 27 年 9 月事案 35
３．１　事案概要 35
３．２　教育情報課の対応 35
３．３　事業者の対応 35
第６　平成 28 年 2 月 15 日事案覚知後の対応状況 36
第７　提言 39
１　はじめに 39
２　本事案の概要 39
３　運用上の課題など 40
３．１　基礎的・実践的セキュリティ知識の欠如 40
３．２　基礎的・実践的セキュリティ知識について 40
３．３　校内無線 LAN の運用 42
３．４　ログ管理について 43
３．５　業務ソフトウェアの検証について 43
３．６　生徒端末について 44
３．７　セキュリティ監査 44
４　今後のセキュリティ対策について 44
４．１　短期的対応 45
４．２　中長期的対応 47
５　セキュリティ対策実施上の留意点 48
５．１　学校の情報システム設計・運用とセキュリティ対策 48
５．２　学校現場の実態に即したセキュリティ対策 49
６　おわりに 49

委員会設置の経緯

平成 28 年 2 月 15 日、佐賀県教育委員会は警視庁から情報提供を受け、佐賀県の学校教育ネットワークに対する不正アクセスが発生したことを覚知した。

被疑者の押収された自宅パソコンからは、佐賀県の県立学校に係る約 21 万件のファイルが発見され、その中には多くの生徒や保護者の方などの個人情報も含まれるなど、県民の学校教育への信頼を損なう極めて重大な事態となった。

県教育委員会では、今回の事案について、情報技術・情報セキュリティの観点から検証を行うとともに、今後、どのような対策を講じていくべきかについて検討し、提言を得ることを目的として、「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」を設置した。

当委員会においては、今回の事案に関し、事務局が県教育委員会、学校、事業者を対象に行った調査等をもとに、システムそのものの問題のみならず、運用上の問題、初動や事後の対応などについて、情報技術・情報セキュリティの観点から検証し、どこが問題だったのか、何が原因だったのか等を明らかにするとともに、効果的な再発防止策を検討し、その結果を提言書としてとりまとめた。

検証及び検討の方法

当委員会では、事務局である県教育委員会が行った調査結果、委員からの依頼による追加ヒアリングの結果をもとに、発生事象をシステム、運用管理、初動や事後対応の観点から細分化し、それらが「なぜそうなったのか」という、原因となる要素について反復的に分析する手法を採用した。

さらに分析の結果、得られた個々の要素について、各委員が短期的対策、長期的対策の方針を検討し、重複、関連する事項について再構成した上で提言としてとりまとめた。

なお、県教育委員会では、検証の過程で明らかになった短期的対策のうち、応急的に対応すべきものについて、本提言前に実施、あるいは実施のための予算措置を講じており、その内容は本提言書中に記載している。

第1　事案の経緯等

1　事案の経緯

佐賀県の学校教育に係る不正アクセス事案の経緯は、下記のとおりである。

年月日	事案経緯
平成25年4月～	• SEI-Net運用開始
平成26年4月～	• 新校内LAN運用開始
平成27年3月頃	• Ｓ高校で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5月頃～	• 生徒Ａが不正アクセス
平成27年6月14日	• Ｓ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日付けフォルダの中に、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	• Ｓ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16日頃～18日頃、同月20日頃	• 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13日頃	• 生徒Ａが不正アクセス（立件分）
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 日頃	• 生徒Ａが不正アクセス禁止法違反の疑いで任意送致される
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

２　窃取されたファイル等

県立学校の学校教育ネットワークに対する不正アクセス事案で窃取されたファイル等及びその中に含まれていた個人情報は次のとおりであった。

２．１　調査対象

無職少年の押収された自宅パソコンから発見された本県の県立学校に係る約２１万件のファイルのうち、各学校の校内サーバ（校務用サーバ・学習用サーバ）にあった同じファイル名の約１５万３千件及び同少年が窃取後に作成したファイル７件について調査した。

２．２　調査結果の概要

(1) 個人情報が含まれていたファイル数

- 校内 LAN の校務用サーバ　　1,574 件（調査ファイル総数　　6,748 件）
- 校内 LAN の学習用サーバ　　1,943 件（調査ファイル総数　146,423 件）
- 教育情報システム（SEI-Net）　　7 件（調査ファイル総数　　7 件）

合計　　3,524 件

(2) 校内 LAN 及び SEI-Net から窃取された個人情報の内容

		氏名	ID	住所	電話番号	業務用メールアドレス	成績関係	生徒指導関係	進路指導関係	その他
校内 LAN	校務用サーバ	○	○	○	○	○	○	○	○	○
	学習用サーバ	○	○				○		○	○
SEI-Net		○	○			○				

(3) 含まれていた個人情報の人数

- 生徒　　10,741 人
- 保護者　　1,602 人
- 教職員　　1,116 人
- その他[1]　　896 人

合計　　14,355 人

[1] 外部から招いた講師や式典招待者など

(4) 主な個人情報の内容別人数

個人情報の内容	人数	個人情報の内容	人数
氏名	14,355 人	成績関係[2]	808 人
ID	6,368 人	生徒指導関係[3]	67 人
住所	1,922 人	進路指導関係[4]	353 人
電話番号	1,843 人	その他[5]	713 人
業務用メールアドレス	564 人		

保護者名については、生徒の個人情報として集計を行ったため、保護者の住所と電話番号については、生徒のものとしてカウントしている。

[2] 模擬試験偏差値、小テスト結果、学年順位など

[3] 生徒指導調査報告資料、生徒事故報告書など

[4] 進路先の記録、進路希望調査など

[5] 学校行事のスナップ写真、出身中学校名など

第２　被害を受けたシステムの構成及び発見された脆弱性

１　SEI-Net

１．１　SEI-Net のシステム構成

(1)　SEI-Net の機能概要

SEI-Net は、主に学習者と教職員と教材等のやりとりを行う学習管理/教材管理機能、教職員が出席や成績処理を行う校務管理機能、それらをまとめるポータル機能からなっている。

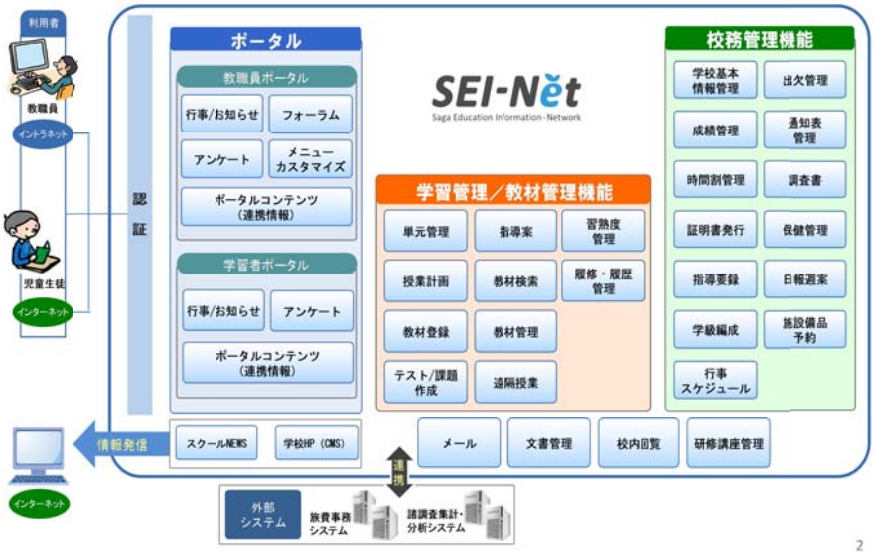

図　SEI-Net の機能概要図

(2)　SEI-Net への接続

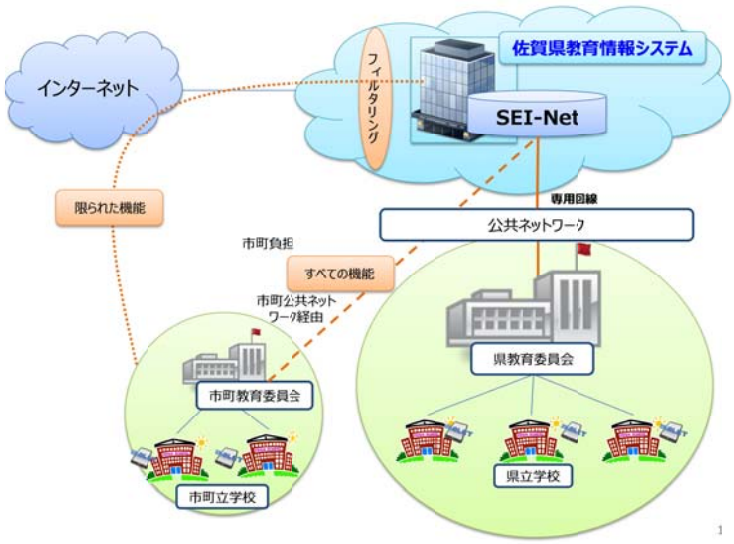

図　SEI-Net への接続について

SEI-Net への接続方法はインターネット経由での接続及び、佐賀県が敷設している公共ネットワーク（閉域網）経由での接続のふたつがある。

ユーザ	接続場所	校務管理機能	学習管理機能
学習者	校内	×	○
	インターネット	×	○
教職員	校内(証明書無)	×	○
	校内(証明書有)	○	○
	インターネット	×	○

インターネット経由では学習管理機能は使用できるが、校務管理機能等は使用できない。教職員が校務管理機能を使用する場合は校内から公共ネットワーク経由で、かつ、個人証明書をインストールしているパソコンからのみアクセスができるようになっている。

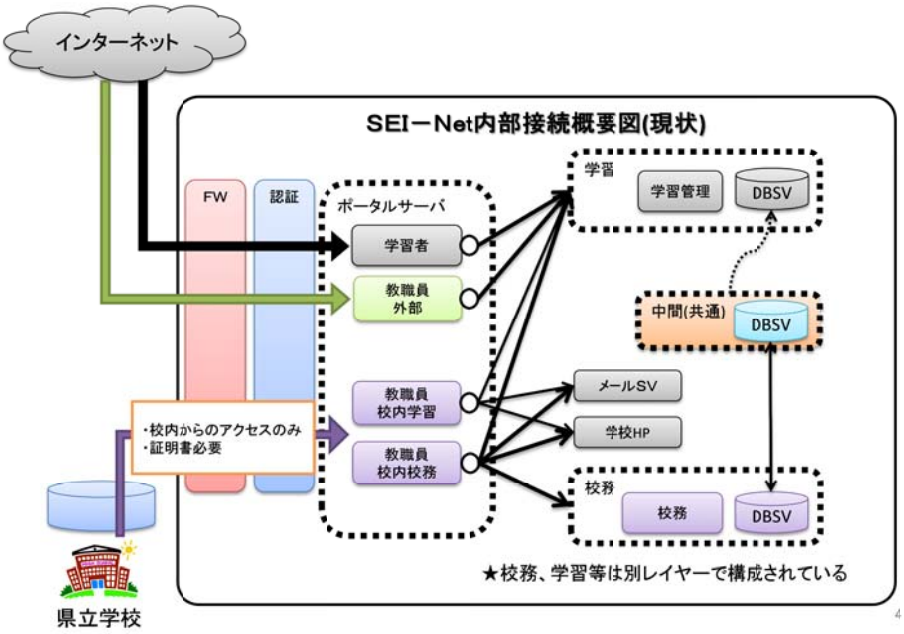

図　SEI-Net 内部接続概要図

(3) SEI-Net の内部構成（セキュリティ上により一部非公表）

SEI-Net の校務管理機能、学習管理機能はネットワーク上論理的に分離されており、保有情報も分離されているため、相互参照できない構成となっている。

なお、共有する必要がある情報は中間（共通）データベースに、校務管理機能のデータベースからコピーされ、それぞれの機能より参照している。

１．２ 発見された脆弱性

SEI-Net の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脆弱性が存在した。これは同画面において、ブラウザがサーバより検索結果の情報を受信する際、その機能では利用しない項目を含んでいたものである。さらに、ブラウザとサーバ間の通信自体は SSL により暗号化されていたが、各項目については平文のまま処理されていた。そのため、これらの情報はブラウザの開発者ツールを用いることにより取得することができていた（脆弱性①）。

その結果、サーバに送信しているパラメータを、ブラウザの開発者ツールを用いて変更すると、本来見ることができない他の学習者の情報を取得することができる状態となっていた（脆弱性②）。

なお、学習管理機能はパッケージソフトウェアを用いて導入しているが、このソフトウェアは学習者同士でメッセージを送信するために学習者も宛先として検索ができる仕様であった。導入時に、県教育委員会の要求仕様「学習者は教職員のみにメッセージが送信できる。教職員は学習者、教職員にメッセージを送信できる。」に合わせるために改修を行ったものの、パラメータの不正な変更があった場合にそれをチェックする機能を実装していなかった。

【問題点】

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、パッケージソフトの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。結果として脆弱性が残る修正をしたことが問題である。

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、自ら望んだ仕様がどのように実装されているのか等を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潜在する脆弱性を早期に発見できる可能性はあった。

１．３ 脆弱性への対応（実施済）

(1) 脆弱性①への対応

使用しない情報については、送信しないように変更した。さらに処理のために必要な情報については、ブラウザ側の処理をサーバ側の処理に変更することで、取得する情報を減らした。また、ログイン ID に関しては、暗号化（AES-128）にて暗号化し、特定できないようにした。

(2) 脆弱性②への対応

権限チェックのロジックを追加し、意図的にパラメータを不正に変更した場合でも、学習者が学習者にメッセージを送信できない処理を追加した。

(3) 脆弱性調査の実施

脆弱性①、②において、類似事象が潜在していないか、システム全体の調査を実施した。併せて、セキュリティ専門者による手動診断を実施し、脆弱性につながる可能性のある機能について予防的に改修を行った。

(4) アラート機能の強化（平成 28 年 9 月補正予算）

SEI-Net の校務管理を取り扱う Web サーバについて通常の利用では取りえない行動をユーザがとった場合に通知（振る舞い検知）される仕組みを導入するとともに、当該ユーザの接続の遮断等を行う機能を組み込むこととした。

(5) ログ記録日数の延長（平成 28 年 9 月補正予算）

不正な操作等のログ記録日数を現在の半年から 1 年間保存ができるように、SEI-Net の記憶装置の変更を行うこととした。

２　校内 LAN

２．１　校内 LAN システムの構成

(1)　校内 LAN システムの機能概要

生徒一人 1 台の学習用タブレット端末、普通教室に 1 台の電子黒板、校務で使用するパソコンを接続するためのネットワークシステムとして、平成 25 年度に全県立学校で整備された。

それまで各校管理下の公有財産として取り扱われていた校内 LAN を構成する各種機器について、県教育委員会で一括して管理すると同時に、全校で標準化された運用・保守の体制並びに一元的に情報管理をする仕組みが必要となったため、新たに管理用セグメントをネットワーク上に設けている。

(2)　校内 LAN システムの物理構成

（セキュリティ上により非公表）

(3) 校内 LAN システムの論理構成

（セキュリティ上により非公表）

２．２　校内 LAN の問題点

(1) 無線 LAN への偽装接続

校内 LAN を構成する無線 LAN は、SSID を通知しない（隠ぺいする）機能（ステルス機能）を利用するなど、セキュリティ対策を講じていた。

無職少年は、端末の MAC アドレスを生徒の学習 PC のものに偽装した上で、何らかの方法で入手していた無線 LAN の接続設定（SSID[6]と事前共有鍵[7]）を使用して校内 LAN に不正に接続している。

【問題点】

本件についてはシステム面よりも運用面で問題があった。

無線 LAN に不正接続する際、偽装した MAC アドレスで侵入を許しているが、MAC アドレスの偽装は簡単であるとの知見があれば、また休日・夜間等に不正接続が行われる可能性を認識していれば、休日等の停止措置を講ずることもできたと考える。

---

[6] 無線 LAN のアクセスポイントの識別名

[7] 端末とアクセスポイントとの間の通信の暗号鍵

(2) 管理用セグメント経由の意図しない通信

学習用サーバと校務用サーバは、機器のメンテナンスのために管理セグメントを介して接続することで一括して監視するよう設計されている。その際、県教育委員会と構築事業者との間で、接続におけるリスクについて議論した事実は確認できなかった。

また、ファイアウォールの設定について議論した事実も確認できなかった。

【問題点】

校務用、学習用の両サーバの監視を簡単にすることの利便性を追求し、セキュリティ対策の視点が欠けてしまった。本来はファイアウォールを設定することが必要であった。

2．3 校内 LAN の問題点への対応（実施済）

(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 の停止措置を実施した。

(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。

第3　運用管理

1　SEI-Net

1．1　運用管理事項

委託仕様書に記載されている主な業務内容は下記のとおりである。

(1) システムの監視

システム内のログ収集や通信状況を定期的に確認し状態を監視する。

異常を検知した場合は、管理者へメール等により自動的に通知を行う。

(2) 問題管理

障害が発生した場合は、速やかに障害の切り分けを行い、原因箇所の特定を行う。

発生した問題に対して復旧を行う。問題解決後に「原因、実施作業内容、再発防止策」を県に報告、原因に対して恒久的な解決措置を検討し解決を行う。

(3) 変更管理

問題の発生や他の要因によって生じる機器・ソフトウェア・各種ドキュメント等の変更に関しては、佐賀県の確認及び承認を受け、開発・変更依頼書等を提出。台帳等に登載し履歴管理を行う。

(4) ヘルプデスク

平日、9時から１７時の間、教職員等からの電話、メールによる問い合わせに対応を行う。ヘルプデスクに問い合わせのあった問題については記録管理を行い、問題が解決した際はその旨を問い合わせ元に通知を行う。

また、問い合わせは適切に記録管理を行い、分析を行う。

(5) システムの保守業務

保守に当たり毎年度(緊急の場合はその都度)保守計画を立て県教育委員会と協議を行う。保守計画によりシステムの設定へ変更や関連システムとの連携のための設定作業を行う。

(6) 県との定期協議

ヘルプデスクに関する内容、機能の改善、月例報告については定期的に県教育委員会と協議を行う。

１．２ 運用管理体制

(1) SEI-Net 運用時の関係業者

項目	企業	備考
システム運用・保守	凸版印刷株式会社	
機器運用・監視	ユニアデックス	FW 監視・設定も含む
ハウジング業者	デジタルコミュニケーションズ佐賀	上位回線等も含む
FireEye 監視	NEC フィールディング	監視

(2) インシデント発生時の連絡体制

インシデントを検知すると、それぞれの関係事業者から教育情報課の担当へ連絡が入るようになっていた。

特にファイアウォールについては、不正通信または異常検知後、メールが担当者へ送信されるようになっていた。

また、FireEye については、不正通信または異常検知後、メールが担当者、学習用 PC へルプデスクにも通知され、現地員も含め対応することとなっていた。

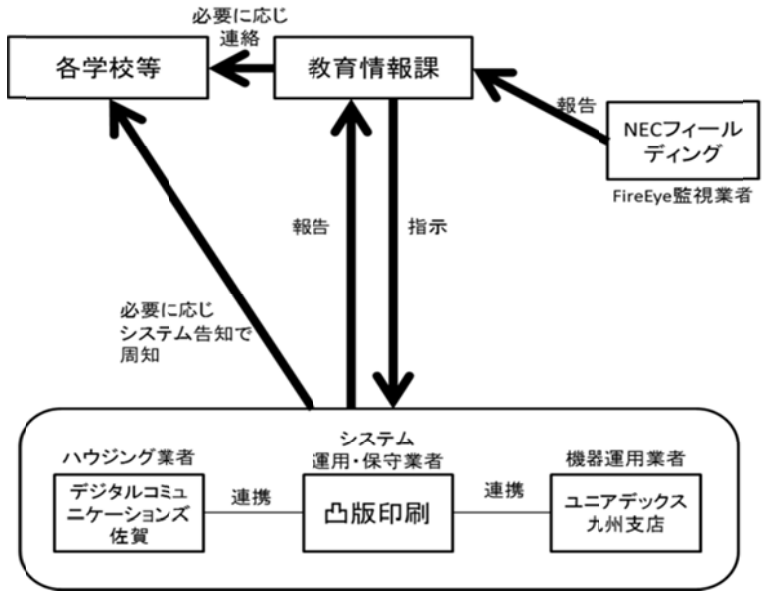

図　SEI-Net におけるインシデント発生時の連絡体制

１．３ 運用に係る問題点

SEI-Net そのものに起因する運用上の問題点は見られなかった。

２　校内 LAN

２．１　運用管理事項

委託仕様書に記載されている主な業務内容は下記のとおりである。

(1) 監視業務

- スイッチ、アクセスポイントの死活監視
- サーバスイッチポート監視（サーバリンク監視）
- 不正接続防止システムの監視（月次で報告）

(2) 障害対応業務

- 校内 LAN 保守対象機器のハードウェア・ソフトウェア障害対応
- 校内 LAN と接続する個別ネットワーク等障害時の原因切り分け、調査支援

(3) 保守業務

- 校内 LAN 保守対象機器の点検業務（年 1 回以上）
- セキュリティパッチの適用、ソフトウェア最適化

(4) 管理業務

- サーバリソース（CPU、メモリ、HDD）の管理
- 他システム機器や端末機器の追加・変更等に伴う、軽微な設定変更作業
  （スイッチのポート設定変更､不正接続防止システムへの許可機器の追加･削除等）
- ネットワークトラフィックの管理（拠点別、送受信別の最大値、平均値）
- 校内 LAN 予備機の管理

(5) ヘルプデスク業務

- Active Directory サーバで管理されているユーザ情報の変更作業支援
- ユーザ情報の変更作業に伴うファイルサーバアクセス権変更作業支援
- 技術サポート（運用管理サポート、セキュリティ対策サポート、工事に関するサポート、技術情報、資料の提供、技術的な事項に関する教育）

(6) 報告業務

- 月次及び年次にて報告会を開催し、主に以下情報について提出、説明を行う。
  - 障害実績報告
  - トラフィック報告
  - サーバリソース状況報告
  - 不正接続検知報告
  - ウイルス検出状況報告
  - 運用実績及びヒアリング結果に基づく、校内 LAN の運用改善の提案
  - その他佐賀県担当者が必要とする資料

２．２ 運用管理体制

(1) 校内 LAN 運用時の関係業者

項目	企業	備考
機器設置、機器交換	九電工	
機器設定	学映システム	
ICT サポーター	ベネッセ	

(2) インシデント発生時の連絡体制

運用保守業務の大部分を学映システムに再委託しており、後述する学習用 PC の運用保守と併せて業務を行っている。そのため、校内 LAN のみのインシデント対応組織は存在していない。

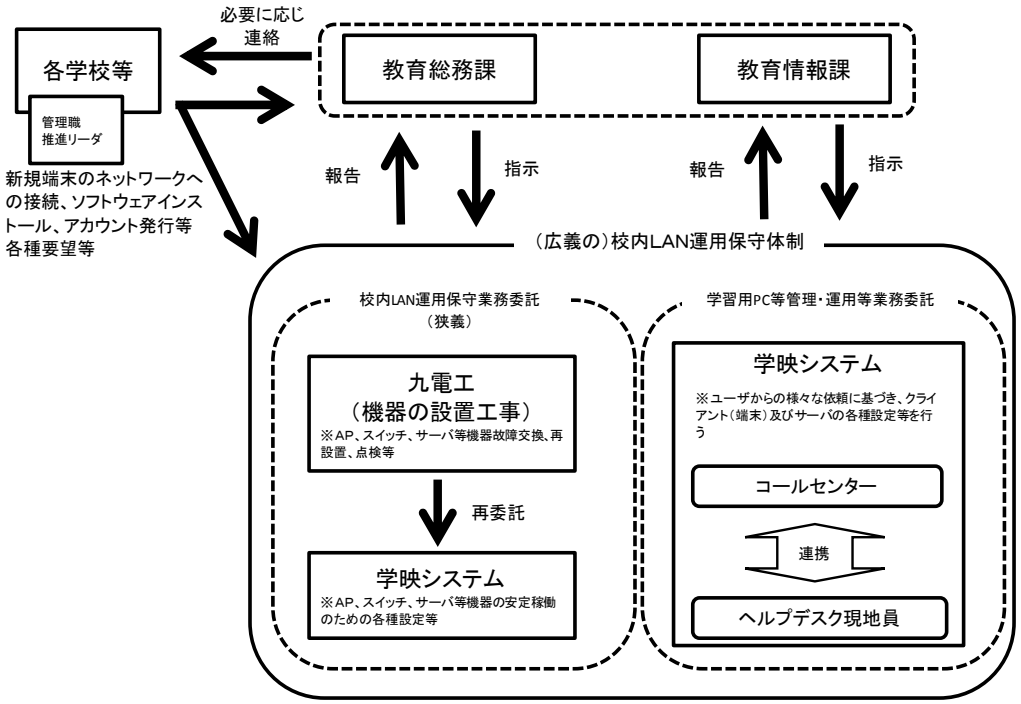

図　校内 LAN におけるインシデント発生時の連絡体制

(3) アカウント管理の状況

委託仕様書によると、校内 LAN 運用保守業務委託事業者がドメイン管理者アカウントのパスワードを保管・管理することとなっている。一方、委託事業者では、使用・保管している意識はあっても、所有は学校及び県教育委員会という認識であった。

２．３ 運用に係る問題点

校内 LAN において、下記のような不適切な運用がなされていた。

(1) 教材インストール用のスクリプトファイルを学習サーバの生徒がアクセスできる領域に置いていた

当該スクリプトファイルは、生徒の学習用 PC に教材をインストールする際に、管理者権限による作業を自動化するために、生徒に使用させていたものである。

このファイルは主に年度初期の教材インストール時に必要であるが、学習用 PC が故障した際に初期化し再度、教材のインストールを行う必要があったため、学習用サーバの生徒がアクセスできる領域に常時配置されていた。

教材のインストール手法については、平成 26 年度導入時３つのパターンで検討されていた。

パターン１は、今回の問題であるスクリプトファイルを使用するもの

パターン２は、学習用 PC を集めて、作業員がインストールするもの

パターン３は、SCCM サーバを使用しインストールするもの

平成 26 年 3 月に導入方法を決定するため、県教育委員会及び学映システムで一部の学校で実証試験を行ったが、SCCM サーバを使用しインストールする方法では、個別端末ごとに所要時間に差があり、長いものでは数時間を要するものがあった。また、パターン２の方法では、学習用 PC が生徒の所有物であるため学校側でインストールすることができないとの判断であった。そのため、県教育委員会及び業者合意のもと、パターン１の方法を採用するよう決定していた。

なお業者からは、当該スクリプトファイルを使用することを決定する際に、業者及び県教育委員会の間で危険性等の協議を口頭で行ったとのことであった。

【問題点】

県教育委員会及び業者によるパターン１の方法を決定する際にセキュリティについての検討が不十分であったことに加え、管理者権限を含んだスクリプトやプログラムは、実行時のみオンラインにして利用し、利用後はオンライン上から削除する徹底がなされていなかったことが問題だった。

(2) 校内 LAN 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 サポーター引継書が学習用サーバに蔵置されていた

S 高校で ICT サポーター引継書が蔵置されていた。ICT サポーター業務を受託しているベネッセに確認したところ、「平成 27 年 3 月 30 日に、ご担当先生から依頼を受け、ICT サ

ポーターが紙媒体を元に、平成 26 年度 ICT サポーター引継書を電子媒体で作成いたしました。作成した電子媒体を ICT サポーターが「ICT サポーターより」フォルダにアップし、依頼をいただいたご担当先生に、作業の完了およびアップ場所をご報告いたしました。」との回答であった。この回答について、学校に確認したところ、記憶にないとのことであった。

さらに、平成 28 年 1 月に学映システムのヘルプデスク現地員は、平成 26 年度 ICT サポーター引継書が学習用サーバに蔵置されていることを確認し、自らの業務に必要な情報と考え、加筆修正をした平成 27 年度 ICT サポーター引継書を作成したとのことであった。

【問題点】

本件については、ICT サポーター引継書の統一的運用の想定がなされていなかったこと、重要情報（管理者 ID、パスワード）をオンライン状態で保存していたこと、また、学校、業者ともに、重要情報に関するリスクへの知見が不足していたこと等が問題だった。

⑶ 学習用サーバの教師及び生徒がアクセスできる領域に、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、パスワードを利用し、各パソコンに設定された MAC アドレスを確認することが可能であった。

当該ソフトウェアに係る管理者 ID、パスワードについては、S 高校の校内 LAN 学習用サーバの教師、生徒がアクセスできる領域に保存されていた。本パスワードを利用すれば、他校の PC の MAC アドレスも閲覧可能である。また当該システムに係る管理者 ID、パスワードについては、教職員、生徒が利用することはない。

学映システムに確認したところ、「当該ファイルは、学映システムが平成 26 年 12 月に、PC 端末の設定変更及びソフトウェアのインストール作業で使用したファイルであると思われる」とのことであった。

また、「インストール方法はサーバに保存せず USB メモリから直接実行する方法で実施し、作業前後には USB メモリの本数確認をしており紛失等はなかった」とのことである。なお学映システムに対し、なぜサーバに保存されているのか確認したところ、「作業手順は USB メモリから直接実行する方法でした。当該作業を数日間に渡り行っていたが、その期間内に何等かの理由でサーバに置かれたと推測される」との回答であった。

【問題点】

本件については、人為的ミスあるいは、USB メモリファイルから直接実行する方式でしなかったことのいずれかと考える。

いずれにしても蔵置してはいけないファイルを蔵置していたことによるものであり、業者のセキュリティ面を踏まえた作業手順が確立されていなかった。

(4) 学習用サーバ内に、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

SKYMENU（学習用 PC と電子黒板をつなぐソフトウェア）の教職員のパスワードを教職員が忘れた際に、ヘルプデスク現地員がユーザ情報管理ツールを使って調べるために管理者権限が必要となる。この問合せに速やかに対応するため、学習用 PC のコールセンター担当者が管理者権限のアカウント（kanriID）を作成している。

当該アカウントについては、平成 27 年 4 月 14 日、学映システムが、「数校の教師より「教職員のパスワードを確認する方法はないか、サーバ側で教職員のパスワードを変更することができないか」との要望を受け、学映システムより「教頭教職員用の学習用 PC に SKYMENU ユーザ情報保守機能をインストールし、教頭先生の ID でログインしたときのみ全教職員のパスワードが確認できる・変更できるように設定する等の対応方法があるが、学校が教職員のパスワード管理を行うことはセキュリティ的に可能か。」との問い合わせを教育情報課へ行っている。

教育情報課からは、「お問い合わせいただいたパスワードの確認・変更の方法について、「サーバ側に新しくアカウントを追加して、そのアカウントを使ってパスワードの確認・変更を行う」ように指示し、また「既にドメインの管理者権限を学校で管理しており、校務用 PC に関してもパスワードの管理は学校で行っているため、指導者用 PC の権限も学校に任せることは問題ないと思います。」」との回答をしている。

平成 27 年 6 月、S 学校の教職員が校内 LAN へアクセスできなくなっている事案が発生し、教育情報課は、管理者権限パスワードで不正接続した可能性が高かったため、管理者権限パスワードの変更を学映システムに依頼した。その際には、kanriID 及び SKYMENU の管理者 ID のパスワードについては変更をしていない。

平成 28 年 2 月には、教育総務課（平成 28 年 3 月まで教育支援課、以下同じ。）は九電工に対して、「校内 LAN のログ保全と校内 LAN に接続されている全ての機器の管理パスワードの即時変更及びその後の定期変更依頼を保守業者に行うよう指示」した。（その後、九電工は学映システム（校内 LAN 保守運用業務）に指示）。

また、教育情報課は学映システム（学習用 PC 等管理・運用業務）に対し、「校内で使用する全てのパソコンのパスワード変更」を指示した。

これは、「校内 LAN 保守運用業務」は「九電工・学映システム」に教育総務課より委託し、「学習用 PC 等管理・運用等業務」は「学映システム」に教育情報課が委託していることによる。なお教育情報課担当者は、kanriID については、校内 LAN 保守運用業務で担当していると認識していた。

平成 28 年 5 月に警察より kanriID のパスワードの変更がなされていない旨の連絡があり、教育情報課及び教育総務課は、学映システムに変更を指示した。

その際、教育情報課及び教育総務課担当者は、kanriID、パスワードの存在を「校内 LAN 保守業務担当者」が知り得ていない様子であったため、誰が管理をしていたのか確認した結果、「本アカウントは、「校内 LAN 保守運用業務」ではなく、「学習用 PC 等管理・運用

等業務」内で管理をしていた。そのため、当時教育総務課からの連絡を受けた「校内 LAN 保守運用業務」担当者は、本アカウントについては知り得ていなかった」との回答であった。

【問題点】

本件については、学校、業者ともに、重要情報に関するリスクへの知見が不足していたこと、管理者権限を持ったパスワードを安易に作成していたことに課題があった。

また管理者アカウントの全容を把握していないことにも課題があった。

(5) SKYMENU（学習 PC と電子黒板をつなぐソフトウェア）の管理者アカウント（設定を行う学映システムが管理）が学習用ドメイン管理者アカウントと同じパスワードであった

SKYMENU（パッケージソフト）は、学習 PC と電子黒板をつなぐソフトフェアである。パッケージソフトの管理アカウントで、上記(kanriID)を兼ねるものであり、当該管理アカウントについては、学映システムのみが把握し、学校へは通知等は行っていない。

学映システムに確認した結果、事案発生当時は、当該管理者アカウントについては、学習用ドメイン管理者アカウントと同じパスワードを使用していた。

また平成 27 年 6 月、平成 28 年 2 月には、kanriID と同様の理由で変更がなされていなかった。

【問題点】

本件については、パスワードが漏れることを想定してなく、パスワードポリシーの確立がされていなかった。

(6) 教職員への操作等の研修会用に作成したテスト用アカウントが、研修会終了後も無効化されていなかった

テスト用アカウントは、学校での研修会や、中学生のためのタブレット体験会などで学習用 PC を使用する際に利用するアカウントである。

テスト用アカウントは教職員用テストアカウント、生徒用テストアカウントの２種類あるが、教職員用テストアカウントは各教職員が使用している ID、アカウントのことである。

また生徒用テストアカウントは、研修者等が利用しやすくするため、ログイン ID とパスワードの両方が同じアカウントとし、また規則性があるアカウントであり、常時設置していた。

当該アカウントについての作成、同パスワードとすることは、教育情報課より業者へメールで依頼している。

【問題点】

本件については、学校、業者ともに、重要情報に関するリスクへの知見が不足しており、管理者権限を持ったパスワードを簡単に作成していた。

テスト用アカウントについて、セキュリティリスクの検証が十分でなかったこと、また、ログイン ID とパスワードが同じアカウントが存在することについては、セキュリティ常識が欠如していると言える。

⑺ パスワードを定期的に変更していない

生徒用パスワードを変更することについて、平成 27 年当時は、保守業者、県教育委員会で規定されたものはない。

ただし、教育情報課、学映システムでは、平成 27 年の教材インストールが行われる４月、５月以降には変更が必要であると問題意識はあった。

【問題点】

本件については、パスワードポリシーがないことが問題だった。

⑻「学習用サーバへのパスワード」から「校務用サーバのパスワード」が推測できた

校内 LAN の管理者 ID、パスワードについては、九電工・岡田電気建設共同企業体が作成した校内 LAN 設計書をもとに設定されている。

当該設計書には、「新校内 LAN 導入機器について、機器パラメータを学校ごとに設計する必要があります。これは、運用が開始され障害が発生した際、監視システム上においてどの学校・どの場所を特定する必要があります。」との記載があった。

【問題点】

本件については、パスワードが漏れることを想定してなく、パスワードポリシーの確立がされていなかった。

規則性を持ったパスワードを設定する危険性について、セキュリティ知識、認識が不足しており、また、利便性を追求した結果、セキュリティ対策がおろそかになったことが問題だった。

２．４ 運用に係る問題への事案覚知後の対応（実施済）

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。

また教育総務課内に対策チームを編成して今回の事案に対応していくこととし、情報通信技術に関する専門家である県情報監を教育総務課に併任し、対策チームや県教育委員会にお

ける情報セキュリティ強化対策について指導・支援を受けることとした。

3　学習用 PC

3.1　運用管理事項

委託仕様書に規定する主な業務内容は下記のとおりである。

(1) 維持管理業務

- 校内 LAN に接続される全ての機器の維持管理業務
- ソフトウェアのインストール・アンインストール支援
- プリンタ、複合機等周辺機器のドライバインストール及びネットワーク設定
- Active Directory サーバを利用したアカウントおよびパスワード設定
  ※ サーバ管理者（Administrator）以外の全てのユーザーアカウント
- 佐賀県からの依頼に対するネットワークサーバのログ調査
- ハードウェア・ソフトウェア・システム等の障害原因の切り分け
- 修理が完了したパソコンの初期設定（校内 LAN 接続設定)、再インストールなどの復旧作業
- 共有フォルダ内のデータ等を誤って削除した場合の復旧（可能な範囲）
- 学習用 PC 紛失の遠隔操作による内蔵ディスクのデータ削除またはロック
- 利用者からの依頼に基づく、ユーザーアカウントの作成・管理

(2) セキュリティ管理

- 管理対象機器に係わるセキュリティ情報の入手及び対策
- OS およびソフトウェア等の脆弱性、ウイルス・マルウェア等のセキュリティ
- リスクに関する情報提供
- 対象となるパソコン等に対するセキュリティパッチ等の配信
- 「校内 LAN 運用保守」業者と連携した不正接続防止システムへの機器の登録

(3) 利用者への情報提供・教育

- 計画的な情報提供や教育
  （教職員・生徒対象の機器操作説明・研修等や授業時間中の機器操作説明含）
- FAQ やマニュアル等の整備

(4) サーバ設定等

- 校内 LAN に設置されている各種サーバ等の効率的な設定
  - SCCM サーバ
  - アンチウイルスソフト配信サーバ
  - 不正接続監視サーバ
  - Windows（Active Directory）サーバ
  - ファイルサーバの共有の容量管理、アクセス権の設定等
  - その他、今回の業務に必要なサーバ機器等

３．２ 運用管理体制

(1) 学習用 PC 運用時の関係業者

項目	企業	備考
端末設定、サーバ設定 コールセンター、ヘルプデスク現地員	学映システム	

(2) インシデント発生時の連絡体制

教職員や生徒が､新たに導入された電子黒板や学習用タブレット端末を操作するにあたり､それらの各種設定作業や機器トラブル対応等に追われることなく学習活動等に集中できるよう、平成 26 年度にコールセンターを設置、平成 27 年度には全県立学校にヘルプデスク現地員を配置し、各種相談等に対応できる体制を整備していた。

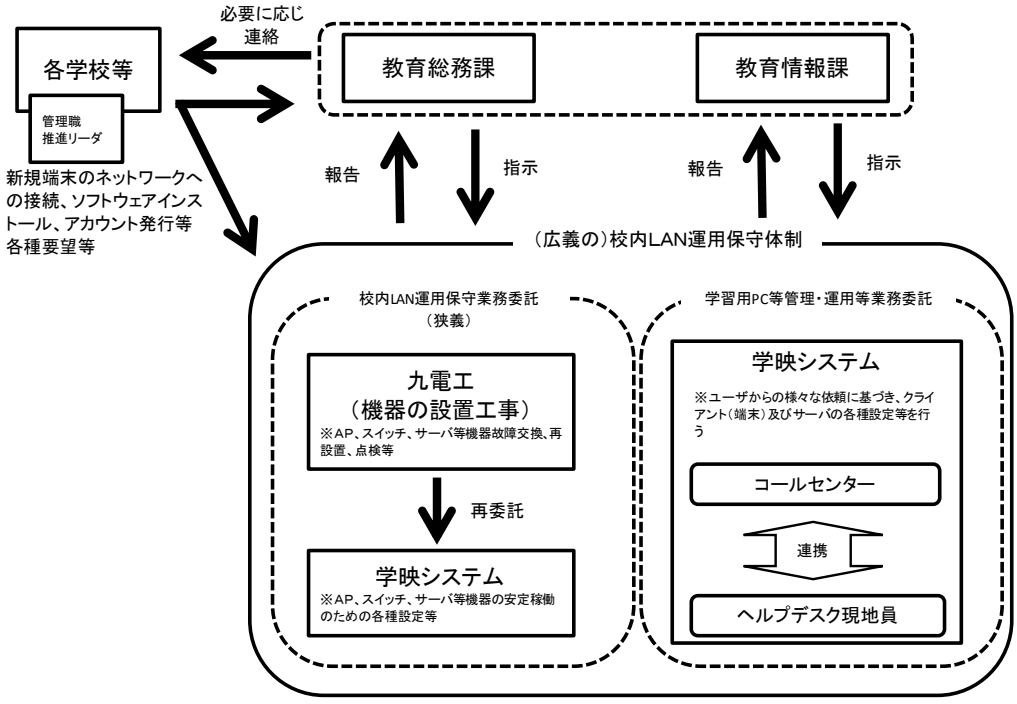

図　校内 LAN におけるインシデント発生時の連絡体制（再掲）

(3) アカウント管理の状況

委託仕様書によると、アカウント及びパスワード設定並びに校内 LAN に設置されている各種サーバ等の設定については､ヘルプデスク現地員ならびにコールセンターが使用することとなっていた。

なお委託事業者では、使用・保管している意識はあっても、所有は学校及び県教育委員会

という認識であった。

3．3　運用に係る問題点

学習用 PC のみに起因する運用上の問題点は見られなかった。運用上の問題は校内 LAN における問題点としてまとめている。

第4　不正アクセスの手法

不正アクセスの手法については、直接、犯行手口等を確認できないところであるが、警視庁からの情報、平成 28 年 7 月に実施した生徒からの聞き取り調査、各事業者からの脆弱性等の報告、無職少年の押収された自宅パソコンから発見された本県の県立学校に係るデータを確認した結果から、下記のとおり推定される。

なお生徒Ａも校内 LAN 学習用サーバ及び SEI-Net に不正アクセスを行っているが、その方法については、無職少年から教えてもらったと話している。

１　フィッシングによる管理者 ID、パスワードを取得

平成 27 年 3 月頃、無職少年及び生徒は学習用 PC（管理者権限）の ID とパスワードを入手するため、フィッシング画面を工作した生徒の学習用 PC で教師から管理者用の ID とパスワードを取得している。

２　無線 LAN に接続

無職少年は端末の MAC アドレスを同校生徒の学習 PC のものに偽装した上で、何らかの方法で入手していた無線 LAN の接続設定及び偽装した MAC アドレスを使用して校内 LAN に不正に接続している。

何らかの方法は、下記の①、②が推定される。

① 生徒の学習 PC を確認し、当該学校の無線 LAN の接続設定、事前共有鍵及び MAC アドレスを入手

② 無職少年の押収された自宅パソコンから発見された本県の県立学校に係るデータのＳ高校から窃取されたファイルに、校内 LAN 学習用サーバに収納されていた県立学校全校の無線 LAN の接続設定と事前共有鍵を含むファイルがあることが確認できた。

また、同様にＳ高校から窃取されたファイルより、校内 LAN 学習用サーバに収納されていた Wi-Fi 環境設定等を管理するソフトウェアの管理者 ID、パスワードを含むファイルがあることを確認できた。当該パスワード等を利用することにより、MAC アドレスを入手することが可能である。

３　学習用サーバ（校内 LAN）へ侵入

上記１で取得した学習用 PC（管理者権限）の ID、パスワード、２で取得した無線 LAN の接続設定、事前共有鍵及び MAC アドレスを用いて、校内 LAN のうち学習用サーバへ侵入することが可能であった。

なお、学習用サーバの生徒がアクセスできる領域に置いていた教材インストール用のスクリプトファイルを解析する方法についても学習用 PC（管理者権限）の ID、パスワードを入手することは可能であった。

平成 27 年 6 月 14 日（S 高校の教職員が校内 LAN へアクセスできなくなっている事案）の事案への対応により、S 高校については、平成 27 年 6 月 16 日に学習用及び校務用の管理者権限パスワードの変更を行ったが、一部のパスワードについては変更を行っていないため、平成 27 年 6 月以降も侵入することは可能であった。

無職少年の押収された自宅パソコンから発見された本県の県立学校に係るファイルには、平成 27 年 4 月 19 日付けフォルダ及び平成 28 年 1 月 5 日付けフォルダの中に ICT サポーター活動引継事項が保存されていた。本ファイルにより学習用サーバへ侵入することは可能であった。

4　校務用サーバ（校内 LAN）へ侵入

校内 LAN 学習用サーバを経由し校務用サーバへ侵入している。不正取得した引継資料に記載されていた学習用サーバの ID、パスワードは規則性があるため、校務用サーバの管理者権限 ID、パスワードを含めて他校の同 ID、パスワードを類推することが可能であった。校務用サーバより窃取されたデータを保存したフォルダの記載日は、平成 27 年 5 月 11 日から 6 月 14 日の間であり、平成 27 年 6 月 14 日は、S 高校の教職員が校内 LAN へアクセスできなくなった日と同日である。

S 高校の教職員が校内 LAN へアクセスできなくなった事案の経緯は、平成 27 年 6 月 15 日午前 8 時頃 S 高校からヘルプデスクコールセンター（学映システム）へ校務用サーバにアクセスできないとの連絡があった。原因は、校務用サーバ共有フォルダのセキュリティ設定（アクセス権）が変更されていることであった。その後、午前 9 時頃に正常な設定へ変更し復旧した。

学映システムによるログ解析の結果、6 月 14 日に生徒が所有する学習用パソコンの MAC アドレスを偽装した不審な Macintosh のパソコンがリモートデスクトップにて管理者 ID 及びパスワードを用いて学習用サーバへ接続後、校務用サーバへ接続した可能性が高いことが判明した。

6 月 14 日午前 10 時 30 分前後に校務用サーバへのアクセスができなくなっており、この時間にアクセス権設定を変更したと推測された。また、当該時間の校務用サーバのネットワークトラフィックを確認したところ、トラフィックが数十 bps であった。アクセス権の変更には時間がかかるため、午前 9 時頃にログオン後、アクセス権の設定変更を行っただけで、データのコピーは行われていないと学映システムは推測した。

学映システムに対し、当該内容について再度調査を依頼したが、ネットワークトラフィックの保存期間が 400 日間であるため、確認はできないとの回答であった。

5　SEI-Net への不正アクセス

無職少年は、7 校の生徒の ID、パスワードを利用し、SEI-Net に係るデータを不正取得している。

凸版印刷にログの抽出および提出を要請し、生徒の ID、パスワードを使用し、該当 7 校で不正な動きを行っているログを確認した。当該ログを持つ生徒へ聞き取り調査を行った結果、Ｕ高校及びＴ高校、各１名の生徒は、情報収集会議[8]のメンバーに ID、パスワードを教えたこと、Ｓ高校の生徒は情報収集会議のメンバーであったこと、またＶ高校、W高校、Ｘ高校及びＹ高校の各々の生徒は、誰かに自分の学習用 PC の ID、パスワードを教えた覚えがなく、本事案への関与に全く心当たりがないことを確認した。

なお、無職少年の押収された自宅パソコンから発見された本県の県立学校に係るファイルには、校内 LAN 学習用サーバ内にある SKYMENU（学習 PC と電子黒板をつなぐソフトウェア）に関するファイル名があることを確認した。当該ソフトウェアを管理者権限で使用することにより、SEI-Net のユーザ ID、パスワードを入手することが可能である。押収されたファイルの中に SKYMENU のファイル名があるのは、Ｓ高校、Ｖ高校、W高校、Ｘ高校及びＹ高校であった。

６　SEI-Net からのデータ取得

無職少年は、SEI-Net が提供しているメッセージ機能を使用し、教職員に向けてメッセージを作成する画面を出した。

その際に送信先を選択する画面でブラウザの開発者機能を用い、教職員名を検索すると、表示される内容以上の教職員の情報（その学校の全教職員の ID、氏名、メールアドレス）が、ブラウザ側に送信されることを発見し、それを窃取した。

また、メッセージ機能では、生徒は、教職員にはメッセージを送れるが、生徒から生徒へのメッセージを送ることができないようになっている。

同少年は、開発者機能を用いて、ブラウザからサーバへ送信される、あるパラメータを変更することにより、教職員に権限昇格し生徒の氏名・ID が見えることを発見し、その情報を窃取した。

さらに同少年は、情報を効率よく窃取するため、上記の一連の操作を自動的に行うアプリケーションを作成した。

[8] 無職少年を中心とした情報共有、情報交換などを目的としたグループ

【参考】不正取得したデータについて

(1) 学習用サーバ(校内 LAN)で不正取得の手口として利用可能であったファイル

無職少年の押収された自宅パソコンから発見された本県の県立学校に係る約２１万件のファイルの中に、不正取得の手口として利用可能な下記のファイルが含まれていた。下記年月日については、無職少年が保存しているフォルダ名に記載されていた年月日を記載している。

	引継書[9]	無線 LAN 情報[10]	MAC アドレス
S 高校・中学校	H26 年度 2015/04/19 H27 年度 2016/01/05	2015/06/09 (全校分)	年月日の記載なし (全校分)
V 高校		2016/01/16 (全校分)	
W 高校		2015/12/09 (全校分)	

(2) 無職少年が保存しているフォルダ名に記載されていた年月日

無職少年が取得したデータを保存しているフォルダ名に記載された年月日は、次のとおりであった。

	学習用サーバ		校務用サーバ	
	最古	最新	最古	最新
X 高校	2015/05/17	2015/05/17	2015/5/24	2015/5/24
S 高校・中学校	2015/04/05	2016/01/20	2015/5/11	2015/6/14
Y 高校	2015/04/25	2015/04/25		
V 高校	2016/01/16	2016/01/16		
W 高校	2015/12/09	2016/01/06		
Z 高校			2015/6/14	2015/6/14

[9] 校内 LAN 学習用サーバ内で教職員用権限及びヘルプデスク現地員がアクセス可能な場所に保管されていた、ICT サポーター活動引継事項

[10] 校内 LAN 学習用サーバ内で教職員用権限及びヘルプデスク現地員がアクセス可能な場所に保管されていた、無線 LAN の接続設定と事前共有鍵

第５　S高校での関連事案と対応

Ｓ高校では、本事案と関連していると考えられる事案が発生していたため、事案概要、及びその対応を県教育委員会関係職員、事業者等に対し調査を行い、文書等で回答を得た結果は次のとおりであった。

１　平成 27 年 6 月事案

１．１　事案概要

平成 27 年 6 月 15 日午前 8 時頃Ｓ高校から学映システムヘルプデスクコールセンターへ校務用サーバにアクセスできないとの連絡があった。原因は、校務用サーバ共有フォルダのセキュリティ設定（アクセス権）が変更されていることであった。午前 9 時頃に正常な設定へ変更し復旧した。

学映システムによるログ解析の結果、6 月 14 日に生徒が所有する学習用パソコンの MAC アドレスを偽装した不審な Macintosh のパソコンがリモートデスクトップにて管理者 ID 及びパスワードを用いて学習用サーバへ接続後、校務用サーバへ接続した可能性が高いことが判明した。

6 月 14 日午前 10 時 30 分前後に校務用サーバへのアクセスができなくなっており、この時間にアクセス権設定を変更したと推測された。アクセス権変更やデータのコピーについて断定できるログはなかったが、当該時間の校務用サーバのネットワークトラフィックを確認したところ、トラフィックが数十 bps であった。アクセス権の変更には時間がかかるため、午前 9 時頃にログオン後、アクセス権の設定変更を行っただけで、データのコピーは行われていないと学映システムは推測した。

１．２　事業者の対応

平成 27 年 6 月 15 日、学校からの連絡を受け、校務用サーバ共有フォルダのセキュリティ設定（アクセス権）が変更されていることを確認し、設定を正常な状態に変更した。
同日、同社の社員から教育情報課の副課長に電話にて報告を行った。

翌日、ログ解析を実施していたが、原因が不明であったため、学映システムの社員が校長及び教頭と学校で打ち合わせをした際に提案、指示を受けて、学習用及び校務用の管理者権限パスワード変更を現地で行った。

翌々日、ログ解析の結果、偽装された MAC アドレスの端末からリモートデスクトップにて学習用サーバへ接続後、校務用サーバへ接続した可能性が高いことが判明したため、学校へ報告。学習用端末及び校務用端末のネットワークより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ファイアウォールの設定変更を現地で行った。

同年７月、教育情報課からの電話指示により校務用管理者権限パスワード変更を学映システムサービスデスクよりリモートにて行った。（全県立学校の学習用・校務用パスワード変

更を行った際に実施。学習用管理者権限パスワードについては、他の学校と規則性を合わせるために変更なし。）。また、同月には、「学習用ネットワーク」から「学習用サーバネットワーク」へのリモートデスクトップの切断を全県立学校に対して措置した。

１．３ 教育情報課の対応

(1) 事案への対応

学映システムヘルプデスクから事象の報告を数日後（日程は忘却）に受けた際、本来、学習用と校務用のネットワークは分離されているのにもかかわらず、学習用ネットワークから学習用サーバへ接続後、なぜ校務用サーバへ接続ができたのかを確認したところ、学習用ネットワークと校務用ネットワークの他にサーバ系ネットワークがあり、サーバ系ネットワークにおいては、学習用サーバから校務用サーバへの接続が可能になっていることが判明したため、報告日（日程は忘却）以降、速やかに以下の対応をヘルプデスクに口頭（電話および報告の場等）で実施依頼している。（これらの対応は、他の全ての県立学校へ行った。）

- 各サーバの管理者権限のパスワード変更をヘルプデスクに依頼
- 学習用サーバから校務用サーバへのネットワーク接続の禁止（設定変更）を依頼

(2) 教育ネットワーク管理者（教育庁企画・経営グループ長）への報告

当時の担当副教育長（教育情報課長事務取扱）は、当時「ネットにつながらない」「ネットワークが不安定」「SEI-Net が使いにくい」等、ネットワークシステムに関するトラブルが複数の学校から繰り返し報告されており、S 高校は特にその頻度が多かったので、この案件についても、そうした案件の中の１つと捉え、事件性を含め、取り立てて教育ネットワーク管理者への報告を行うべきレベルの案件とは考えず、報告されていない。

当時の教育情報課副課長は、教育情報課に組織改編があった平成 26 年かその翌年に、担当副教育長（教育情報課長事務取扱）から、従来、教育情報化担当が担っていたセキュリティ関連業務はシステム担当が行うようにとの指示があっていたことと、県教育委員会の教育ネットワーク管理者は教育情報課長（副教育長）であると聞いた記憶があり、そのため教育情報課長（副教育長）に伝えるものだと考えていたとしている。

(3) 教育支援課（当時、校内 LAN の運用・保守を所管）への報告

当時の担当副教育長（教育情報課長事務取扱）は、組織の業務分担で、ICT 利活用教育に関係する校内ネットワーク及び SEI-Net に関する管理は教育情報課で担当し、無線 LAN の構築と管理等については教育支援課で対応することで確認ができていたこと、また、教育支援課との協議が必要な場合は、それまでもその都度、副課長までのところで必要な協議がなされていたので、この件についても、受けた報告内容からは教育情報課で対応すべきレベルの案件と判断している。

(4) 過去に遡ったログの保全、解析

当時の担当副教育長（教育情報課長事務取扱）は、S高校では、その当時、「ネットがつながらない」「ネットワークが不安定」等の相談が繰り返しあっていたので、教育情報課の担当者及び学映システムからの報告から、「この件も事件性はない」と判断している。

このため、学映システムには、「S高校はモデル校でもあるので、特に注意して対応するよう、通信環境の確認を含め管理の徹底」を依頼し、不正アクセス等、事件性がある事案まで想定した指示ではなく、それまでの対応の強化を指示するにとどめている。

【問題点】

本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とに課題があった。

２　平成 27 年 9 月事案（ツイッターで投稿がなされている事案）

２．１　事案概要

平成 27 年 9 月 2 日に Optim 東京本社で開催された協議会の会場で Optim 社員から教育情報課主査及び学映システム社員に対して、Twitter に「学習用 PC の i - Filter 停止に成功した」等の書き込み（平成 27 年 6 月 11 日投稿）があるとの情報提供があった。

Optim からの情報提供で教育情報課が確認したところ、投稿には「佐賀県立 S 高等学校の皆様、SPECTab で実行したいアプリケーションの名前を grapes3D.exe に変更してみて下さい。そのアプリケーションが実行できます。・・・」と呼びかけている内容があった。また、「県立高等学校のネットワーク環境用学校番号一覧です」、「県庁教育政策課の〇〇〇〇が作成された ICT 利活用教育月別実績報告書をご覧ください」、「SPECTab でのより快適な Web ブラウジングを可能にするため、i-FILTER ブラウザ＆クラウドを停止するソフトを開発しました。さらに端末所有者の権利を保護するため Optimal Biz を停止するソフトも開発しました。」、「ICT 利活用に伴う授業評価集計表こと ICT 利活用教育実践記録簿をご覧ください。」、「SPECTab にインストールされている教材のアップデートスクリプトには、管理者アカウントのログオン情報を生成するコードを敢えて生で書いて、アカウント情報の秘匿の大切さを教育します。」などの書き込みがあり、一般には公開していない情報等を公開していた。

平成 27 年 10 月に Twitter の記事は削除された。当時は、誰が掲載したのかわからなかったが、平成 28 年 7 月の聞き取り調査において、生徒の一人が無職少年に削除するよう要請したと言っている。

２．２　教育情報課の対応

(1) 事案への対応

当時の担当副教育長（教育情報課長事務取扱）は、教育情報課でシステム担当者から他の課員を含めて報告を受けている。ただし、課内のシステム担当ラインからの報告を聞く限り、Optim 社からの情報提供も保守管理を委託している学映システムからの報告も、取り立てて新たな対応が必要という内容ではなかった。6 月の事案を揶揄することでの書き込みとのことだったので、安全を期して、再度お願いする形で、学映システムには、ネットワークに不備やトラブル等がないかの再度の確認と修復及び管理の徹底を、また、S 高校には、先生方及び生徒への指導の徹底を依頼している。

当時の教育情報課副課長は、連絡を受けてすぐに（日時までは覚えていない。）当該ツイッターか何かのページを確認している。確認したところ、佐賀県のタブレット環境のことが記載してあるものの、個人情報やパスワード等といった記載は見当たらず、いたずらかどうかの判断もできず、かといって、このまま放置しておくのは望ましくないと思えたので、副教育長（教育情報課長事務取扱）に相談のうえ、心当たりの生徒がいれば削除するように指導してもらうよう学校に連絡している。

また、当時の教育情報課副課長は、Twitter の記事にあった情報は、通常、一般には公開されない情報で、学校内でどのように流通しているかわからないが、一般的に考えると、生徒には提供されない情報だと思う。通常は入手できない情報が公開されている原因については、当時、教育情報課として議論して推測まではできていなかったと思うと答えている。

(2) 教育ネットワーク管理者（教育庁企画・経営グループ長）への報告

当時の担当副教育長（教育情報課長事務取扱）は、誰かが 6 月の案件をネット上で揶揄して取り上げたもので、新たに何らかの事案が発生したということではなかったため、取り立てて報告を行うべきこととは考えず、教育ネットワーク管理者への報告はなされていない。

【問題点】

本事案への対応については、事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とは問題だった。

３　平成 27 年 9 月事案

３．１　事案概要

平成 27 年 9 月 17 日生徒からヘルプデスク現地員に対して、9 月 15 日に行った授業支援ソフトのアップデート後に学習用パソコンが動作しなくなったとの相談があった旨、学映システム担当者へ電話があった。

リモートにて確認した画面には「システムファイルに問題が発生しました。管理者権限を持つユーザーアカウントで修復を実行してください。」と表示され、ID 及びパスワードの入力を促す画面が表示された。確認の結果、管理者 ID 及びパスワード入力を促すプログラムがスタートアップに登録されていた。

学映システムは、画面の内容から管理者の ID 及びパスワードを入力させ、その情報を抜き取るようなプログラムと推測した。

生徒は、平成 28 年 7 月の生徒聞き取り調査の際、無職少年にパソコンを貸したと言っている。

３．２　教育情報課の対応

当時の教育情報課担当によると、学映システムヘルプデスクから電話で連絡を受け、その際に管理者パスワードを把握しているメンバー（各校に配置されているヘルプデスク現地員を含む。）に、安易に管理者パスワードを入力しないようにヘルプデスクに依頼をしたと思うとのこと。

連絡を受けた後に口頭で係長、副課長等へ報告をし、報告時に上記対応を行う旨、了承（口頭）を得たと思うが、詳細は記憶していないとのこと。（なお、当該事案については、当時の副教育長（教育情報課長事務取扱）、副課長等から事案を知っていたとの回答はあっていない。）

３．３　事業者の対応

9 月 18 日に学映システム社員が学校を訪問し、学校と対応について協議した結果、プログラムへの ID 及びパスワード入力は危険と判断し、リカバリによる対応を行うこととなり、対応を行った。

なお、（他の県立学校の）現地員に伝える事案では無いと判断し、事案としては伝えていない。現地員の定例会内のセキュリティについてウイルス、フィッシング等についての研修会を行っている。

【問題点】

本件については、追跡調査が不十分であったことに問題があった。

第6　平成 28 年 2 月 15 日事案覚知後の対応状況

平成 28 年 2 月 15 日に県教育委員会に対し警視庁から不正アクセスに関する連絡があった時点以降の県教育委員会等の対応は下記のとおりである。

平成 28 年 2 月 15 日に警視庁サイバー犯罪対策課から教育情報課へ不正アクセスに関する下記の連絡があった。

- 事案の全容や詳細は不明、業者の可能性を含め被疑者は特定できないこと
- SEI-Net、校内 LAN とも攻撃があった

連絡を受けた教育情報課は教育長まで報告のうえ、対応や情報共有範囲を協議するとともに、知事部局の情報担当部署にも報告し、緊密に連絡をとりながら対応にあたった。

県教育委員会は、限られた情報しか得られていない中で、二次被害などこれ以上の被害の拡大を防ぎながらできる限り早く収束させるため、犯人逮捕に向けて警視庁に捜査協力しながら、可能な手立てを講じていくこととした。

事案の公表については、捜査中に公表することは、警察の捜査に大きな影響を与えることは確実であり、犯人逮捕や原因究明につながらなくなるリスクが大きいことから、そのようなリスクが解消されるまでの間、公表を控えざるを得ないと判断している。

2 月 16 日に教育情報課及び教育総務課は、委託業者に対して、SEI-Net、校内 LAN（校内サーバ、校務用パソコン、学習用パソコン等、全ての機器）の管理者パスワード変更及びその後の定期変更を行うよう依頼し、合わせてログ保全を依頼した。

2 月 19 日に教育情報課は、SEI-Net について県教育委員会内各課、現地機関、県立学校及び市町教育委員会等にパスワード変更の依頼、また、校内 LAN について県立学校に校内で使用する全てのパソコンのパスワード変更を依頼した。

3 月 11 日に警視庁から県教育委員会へ訪問があり、教育情報課からは SEI-Net、校内 LAN の仕組み、確保したログについて提供・説明を行うとともに、警視庁からは窃取された情報例についての情報提供を受けた。また、警視庁から被疑者が作成していた SEI-Net への攻撃ツールについて説明を受けた。

3 月 15 日に教育情報課から凸版印刷へ SEI-Net 「学習者 LMS メッセージ機能」の脆弱性の究明とその緊急対処準備を指示し、その後、4 月 1 日に教育情報課が凸版印刷から SEI-Net「学習者 LMS メッセージ機能の脆弱性」について調査報告を受けた。

4 月 13 日に教育情報課から警視庁へ SEI-Net の脆弱性改修開始について問い合わせを行

い、改修の準備を進めることについて了承を得て、4 月 15 日に凸版印刷へ SEI-Net「学習者 LMS メッセージ機能」の改修を指示し、実施した。（4 月 27 日改修完了）

4 月 20 日に教育情報課は、警視庁から以下の今後必要な対応策について助言を受ける。

- アカウントの管理の徹底
- 無線 LAN の夜間・休日の停波
- ログ保全日数の延長
- 第三者のチェックが必要

5 月 13 日頃

- 生徒 A が不正アクセス

5 月 17 日に教育情報課から警視庁へ確認し、事案発生の業者への告知について問合せをし、了解を得た。

5 月 19 日に警視庁から教育情報課へ「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がある」との連絡があり、教育総務課から学映システムに対して S 高校のサーバパスワードの早急な変更を指示した。

5 月 20 日に教育総務課から九電工へ不正アクセス事案の概要を正式に説明し、今後対策に協力してほしいことを伝達した。
また同日、佐賀県警から県教育委員会へ訪問があり、以下の脆弱性に関する参考情報（11 項目）の提供を受けた。

① SEI-Net で、生徒でログインしたにもかかわらず先生の権限のデータが取得できる
② スクリプトファイルの記載内容から学習用ドメインの Administrator のパスワードが推測できる
③ Administrator でログインしたままで生徒にタブレットを返却
④ 先生権限と推測される先生用フォルダに学習用ドメインの Administrator のパスワードが記載されたファイルが蔵置されている
⑤ テスト用アカウントが無効化されていない
⑥ ログイン ID とパスワードが同じアカウントが存在する
⑦ パスワードを定期的に変更していない
⑧ あるパスワードがわかると他のパスワードが推測できる
⑨ 学習用サーバから認証ハブを経由せずに校務用サーバにアクセス可能
⑩ Administrator を使用している
⑪ ログから不正な行動を検知できていない

5 月 25 日に、教育総務課から九電工に警察から提供された項目の対応を検討するよう指示する。

同日夜、警視庁から、「kanri」という ID があり、不正アクセスに使用された形跡がある旨の連絡があり、教育総務課から委託業者へ確認したところ、アカウントの内容は把握していないとの回答であったが、取り急ぎ当該アカウントの無効化を指示し、完了した。

5 月 26 日、6 月 3 日、6 月 8 日、6 月 17 日の 4 回に分けて、警視庁から、校内 LAN の被害校 7 校分の窃取された情報のファイル名一覧が送付される。

6 月 7 日に、県教育委員会から学映システムに不正アクセス事案の概要を正式に説明し、警察提供の 11 項目の現状確認を踏まえて、①委託の範囲で用いられているすべてのアカウント調査、②使われていないアカウントの消去、③パスワードをすべて規則性のないものに変更、④パスワードは本当に必要な者にのみ教え、教えた者を管理する、⑤上記の①～④のオペレーションを定期的に実施すること、を指示した。

6 月 13 日に、教育総務課と教育情報課は、校内 LAN の管理者アカウントのパスワード変更を学校に通知し、今後は学校には管理者アカウントのパスワードを知らせないことや、校務用サーバ内フォルダに格納している管理者アカウントの情報が記載されたファイル等を削除する措置を講じた。

6 月 20 日、21 日に、校内 LAN の被害校 7 校へ、窃取された情報のファイル名を送付し、窃取された情報内容の確認調査を依頼する。

6 月 27 日に不正アクセス事案公表

7 月 1 日から生徒調査を行う。（～15 日）

第7　提言

1　はじめに

今回の事案は教育現場から 1 万 4,355 人という大量の個人情報が窃取され、生徒や保護者をはじめ県民に不安と不信感を抱かせたが、その〝被害者〟の多さ以上に、将来を担う人材を育成する教育において、少年ら〝加害者〟を生み出してしまったことが最大の罪である。二度と繰り返さないためにも、原因を究明し、真摯な反省の上に立って、同一の問題を二度と起こさない組織を構築することが大切である。県教育委員会におかれては、当委員会の検証結果と提言を最大限尊重し、速やかに対応するよう要請する。

2　本事案の概要

本事案は、無職少年が生徒の ID、パスワードを使って学校ネットワークへ侵入することから始まった。

これは、高度な情報通信技術を使用した攻撃とは異なり、ソーシャルエンジニアリング攻撃[11]のように人間の心理的な弱さや行動におけるミスに要因があると考えることができる。無職少年は生徒が利用していた正規のユーザ 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、侵入した。

現実の世界に例えると、シェアハウスの玄関の鍵は、住人だけに渡されているが、住人の誰かが外部の知人に玄関の鍵を貸したために発生したと考えることができる。玄関は常時鍵がかかっていたが、外部の知人は借りた鍵を使って玄関を開け、シェアハウスに入ってきた。

どんなに堅固で高度な鍵を使っていても、住人が外部の知人に玄関の鍵を貸してしまえば、外部の知人は、住民と同じようにシェアハウスの中に入ることができる。

本事案は、この例えをネットワーク内で行われたものと考えることができ、技術的な対応やセキュリティ規則等だけで防ぐことが困難であった。

しかしながら、以上の状況だけであれば、大きな問題になる可能性は低かったが、侵入されたネットワーク内に多くの重要情報が保存されており、それらは、簡単に見つけることができた。

県教育委員会、学校、一部の業者の基礎的・実践的セキュリティ知識が十分でなく、管理・運用に基礎的・実践的セキュリティ知識を活かすことができていれば、大量の情報窃取が発生した可能性は低かったと推察する。

---

[11] 人間の心理的な弱さを利用するもので、他人になりすます等して、必要な情報を盗み見する、或いは盗取する。複数方法を組み合わせることや複数人から情報収集することもある。

3　運用上の課題など

3．1　基礎的･実践的セキュリティ知識の欠如

本事案は、ネットワークシステムの脆弱性を見つけ出して侵入したのではなく、正規のユーザ ID とパスワードを入手して侵入した。情報窃取に繋がったのは、ICT 教育プロジェクトを推進･統括する県教育委員会や教職員、一部業者にセキュリティの基礎知識や実践的な対応が十分でなかったことにある。

直接的な原因は、重要な情報、即ち、管理者権限のアカウント（Administrator のユーザ ID、パスワード）が、ネットワーク内に保存されていた。操作マニュアルやスクリプトファイル、ツール類などに含まれており、これらを利用できたことが、被害を大きくした。

更に、本事案は事件発覚 1 年前の 2015 年 6 月にも発生し、県教委は当時、それを覚知したにもかかわらず「ネットワークシステムに関するトラブル案件の一つ」と過小評価し、なおかつ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。加えて定期的なセキュリティ監査や業者間の情報交換などもそれまで一切行われておらず、セキュリティをないがしろにしてきたことが、本事案の被害を大きくした主因である。

3．2　基礎的･実践的セキュリティ知識について

本提言で述べている「基礎的･実践的セキュリティ知識」とは、セキュリティを考えると、攻撃側も被害側も人間である[12]ことを考え、人間の特性、特に、セキュリティ分野での特性を知見として持つことが、非常に大切なものであると考えている。

それらの具体的な内容について、本事案での課題を中心に説明する。

(1) 内部犯行

過去の国内でのセキュリティ事案でも、組織内部の人間が犯罪を行っている[13]。教育機関の場合には、教職員や卒業生だけでなく、本事案のように生徒が事件をおこすこともある。内部犯行では、正規の権限を持っている者が、ネットワークにアクセスして、犯行に及ぶこともあるため、技術的な対応だけで、犯行を防ぐことが難しい。

(2) 集団心理

一人一人が悪いことをしなくても、集団になると思考停止状態に陥り、自分の考えや行動などを深く省みることなく無意識のうちに規則等を無視し、いじめ等や違法行為に加担する

---

[12] カナダの出会い系サイト「アシュレイ・マディソン」では、ロボット（AI 技術を利用したもの）が、人間に対応していたと言われており、最近は、人間だけではないケースも散見される。

[13] 最近の内部犯行例としては、2009 年、国内証券会社の部長代理が、約 149 万人の個人情報を CD-ROM にコピーし、名簿業者に約 5 万人の情報を転売した。2014 年、通信教育会社の業務委託社員が、顧客情報、約 2,300 万件を違法コピーし、名簿業者に転売した等がある。

等、想像以上のことを行うことがある。

無職少年と一部の生徒との関係が十分に解明されていないが、電話会議ができるソフトウェアを使った「情報収集会議」で、情報共有を行っており、情報収集会議の方向が本事案に進展していった可能性も考えられる。

(3) 環境犯罪学

犯罪を防ぐには、犯罪がし難い環境を作ることが大切である。逆に言えば、犯罪者の欲求を満たすものが眼前にあれば、犯罪を起こす可能性がある。本事案では、生徒のユーザ ID、パスワードを利用して、侵入したネットワークには、管理者権限を持つユーザ ID、パスワードなどが保存されていた。

(4) 机上訓練の実施

セキュリティ事案が自組織で頻繁に発生することがないため、「自組織では発生しない」と考えがちで、事前の対応が十分でないことがある[14]。セキュリティ関連の犯罪でも、過去の事案の繰り返しや複数の犯罪手段を利用して、新たな方法に変更したケースがあり、それらの情報共有をすることにより、事件・事故を防ぐ、あるいは、大規模事案を生じさせないことが求められる。

机上訓練[15]では、国内外で発生した事件・事故等の情報収集を行い、関係者全てで情報交換を行うことにより、自組織での事件・事故の対応を考えることにより、同様の事件・事故への対応力を高めることができる。これは、航空業界で行われているチーム訓練[16]をセキュリティ分野に適応したものと考えている。

(5) パスワードポリシー

ユーザ ID とパスワードは、組にして語られることがあるが、パスワードはいかなる理由があっても、ユーザ ID の利用権限のない利用者に開示してはならない。また、簡単に類推

---

[14] 2016 年、旅行業者に標的型メール攻撃により、約 800 万件の個人情報が漏えいしたが、定期的に、標的型メールの訓練は行われていたが、単に、「添付メールのクリック率」を低くすることが中心になっていたと思われる。送信元の国内航空会社に返信をしたが、「未達メール」になったと言われており、未達メールを受信した時点で、対応していれば情報漏えいにならなかったと考えられる。

[15] 「机上訓練（Desktop simulation）」は、本報告書での造語で、適当な言葉がないため、上記のようなものとした。

[16] 「CRM: Crew Resource Management」と言われており、その中で、「ハンガーフライト（Hangar flight）」と言われるものがあり、これは、天気が悪くなるとパイロットは、天気の回復を待つばかりだったが、格納庫（Hangar）に集まり、経験談や自慢話を行うことで、情報交換／情報収集を行っていた。 これにより、他人の経験をあたかも自分の経験のように吸収し、成長に繋がった。

できる文字列を使ってはならない。パスワードチェックリストを利用して、推測しやすい短いパスワードやごく限られた文字種からなるパスワードを設定させないようにする。また、パスワード変更時期等を設定する。

しかしながら、本事案では、一部のパスワードが、規則性を持って作成されていたため、１つのパスワードが分かると、他のパスワードも全てわかってしまった。更に、ユーザ ID とパスワードが同一のものもあった。

(6) 重要情報の取り扱い

システムを利用する上で、最も重要なものは、個人情報や知的財産等の情報であるが、業務上それらを処理するためには、ユーザ ID やパスワード、あるいは、それらを含むソフトウェアツール、操作説明書が必要となる。これらの情報をネットワーク内に保存することは非常に危険であるが、そのように認識していない利用者は多い。本事案でも県教育委員会、教職員だけでなく、業者の中にも、運用の利便性を優先するあまり、セキュリティを軽視した対応がみられ、不正アクセスの一因になった。

(7) 問題の矮小化

多くの事件・事故を考察すると、知らないことや詳しくない事に対して、問題を矮小化してしまうことがある。未知の課題や詳細を知らない課題については、関連部門や外部等との情報共有を行うことにより、矮小化を防ぐことが大切になる。

(8) セキュリティ対策と運用の利便性

セキュリティ対策をすればするほど、利用者や管理者の利便性も通常下がる。厳しいセキュリティポリシーを作成し、それを遵守させることで、逆に、ポリシー違反をする者がでてくる可能性がある。ポリシーに反する事柄については、事前申請の提出・承認システムを考えることが有効である。

本事案では、運用段階で、当初求めていたセキュリティレベルを忘れ、利便性を優先した例がある。

３．３ 校内無線 LAN の運用

校内無線 LAN の運用では、無権限者の利用を防ぐための対応を考える必要がある。本事案では、権限者（生徒）のユーザ ID、パスワードを利用し、MAC アドレスを偽造し、無線 LAN 経由でネットワークに侵入されたが、無線 LAN の管理・運用から、無権限者のアクセスを防ぐ方法を考える必要がある。

本事案では、利用者認証として、ユーザ ID、パスワードと MAC アドレスを利用していたが、ユーザ ID、パスワードを生徒から取得できたため、簡単に無線 LAN を利用してアクセスできてしまった。

なお、MAC アドレス[17]は、ネットワーク接続機器を識別するために予め一台ごとに決められているが、ネットワーク上を流れる MAC アドレスを収集するツールもあり、他のネットワーク機器の MAC アドレスを偽装できるため、無線 LAN 等で、MAC アドレスを利用機器の識別に使うことはあまり意味がない。

校内無線 LAN の運用で、24 時間／日の管理・運用を再考する必要もある。運用上の利便性や煩雑さを考え、特定の時間帯の利用者（アカウント）ログの監視を強化する等で対応することも考えられる。

3．4 ログ管理について

ログは生ものと同じで、単に保存するだけでは意味がない。また、全てのログを取得し、それらを監視することが有効なのかも考える必要がある。大量のログを収集し、監視すれば、「偽陽性（false positive）」と「偽陰性（false negative）」の課題[18]もあり、簡単に判断できない事もある。偽陰性では誤っているものを正しいものと判断されるため、本来検出されなければならないものが、検出されない（正常なものと判断される）ため、問題発見が遅れる可能性がある。

どの様なログを取得する、ログ取得を時間帯で変更する、ログ監視を即時監視／遅延監視等を検討し、費用対効果を考え、検討する。

なお、平成 27 年 6 月の事案時に見逃しがあり、ログの保存期間も検討する必要がある。

3．5 業務ソフトウェアの検証について

最近のソフトウェアの脆弱性を考えると、Windows 等のオペレーティングシステムでは、「セキュリティ開発ライフサイクル（Security Development Lifecycle : SDL）[19]」の適用が行われており、当初と比較すると格段にセキュリティが向上してきた。

一方、アプリケーションの場合、特に、開発企業と販売業者が異なる場合、セキュリティ仕様を販売業者が十分に理解していないことがある。このため、セキュリティを要求仕様に入れることも必要であり、不要な仕組み等がアプリケーションに組み込まれていないか確認する必要がある。

本事案では、セキュリティ検証が十分でなかった。

---

[17] MAC アドレス（Media Access Control address）とは、ネットワークに接続される機器を、一意に識別するために割り当てられる物理アドレスで、48 ビットからなる。前半の 24 ビットは、機器メーカーの識別で、後半 24 ビットは 1 台ごとの機器に割り当てられている。

[18] 偽陽性とは、正しいものが、誤りであると判断される。偽陰性とは、誤りであるにもかかわらず、正しいと判断される

[19] マイクロソフト、信頼できるコンピューティングのセキュリティ開発ライフサイクル、2005 年 5 月、https://msdn.microsoft.com/ja-jp/library/ms995349.aspx

3．6　生徒端末について

端末の利用形態はBYOD（私物機器利用）であり、学校支給のプログラム導入は、学校側で行うことを検討すべきである。

マルウェアの感染やシステムトラブルの場合には、生徒の端末を学校側で操作する必要があることを考えれば、事前に「利用端末規約」を作成し、生徒／保護者の承認を得ることで、対応できる。

なお、本事案では、生徒が教員に操作を行わせ、管理者ユーザID、パスワードの盗取（フィッシング[20]）が行われており、生徒等による重要情報の盗取があるうることを示している。

BYOD機器の内部構造例

3．7　セキュリティ監査

第三者的な立場から、構築されたシステムが適切に管理・運用されているかを検証する方法として、監査がある。

どの様なシステムも、時間の経過や環境の変化によりリスクは変化する。技術の陳腐化や関係者による処理方法の変更でリスクが顕在化することもある。このため、定期的、あるいは、システム変更等が行われた場合、リスク評価や監査を行う必要がある。

しかしながら、国内では、「監査」について多くの誤解もある。「被監査部門の内容を知らないのに、監査を行い、指摘できるはずがない」というのが、典型的なものの１つである。

ただ、実際、「監査」は英語では「Audit」であり、聴く（audio）と同じ語源であるが、日本語の「監査」の意味合い（上から目線的な意味）とは異なる。 日本的な言葉でいえば、「岡目八目[21]」だと考えている。

セキュリティ監査で内部監査は技術的なセキュリティ監査が困難である可能性があるが、管理・運用面の監査は可能である。内部監査人が対象組織に精通していれば、管理・運用面では、外部監査人より望ましい。

本事案では、内部のセキュリティ監査が行われていれば、原因の多くは指摘できた。また外部監査では、内部監査では難しい技術的監査を中心に委託することも考えられる。

4　今後のセキュリティ対策について

本事案のみを考慮したセキュリティ対策では、「モグラ叩き」に終わってしまう。

---

[20] ここでは、「フィッシング」と言っているが、「ID窃盗（ID Theft）」ということもある

[21] 「岡目八目」とは、囲碁に関係した言葉で、脇、あるいは第三者的立場から見ている者は、対局者より、八目先の手が見えるというもので、第三者的立場の者は、冷静に観察でき、的確な判断、指摘ができるということ

ウェブの脆弱性等により、ネットワーク内に侵入される、あるいは、標的型メール攻撃等により、「マルウェア感染」や「ランサムウェア[22]」等の攻撃も考慮する必要がある。これらの攻撃により、情報漏えいや情報削除等が発生する可能性もある。

このための対応として、「包括的なセキュリティ対策」を考える必要がある。そこで、ここでは、主に本事案に対応した短期的な対応と国内外で発生している事案へのセキュリティ対策を考慮した中長期的対応に分けた。

4．1 短期的対応

既に実行されている対策もあるが、可及的速やかに実施し、継続的な対応を行うもので、原則として今期中に実施することが望ましい。

本事案に関連して、顕在化したリスク対応では、既に実行されているもの、及びこれから実施すべきものをリストアップし、実施計画書を作成する。

但し、実施計画スケジュールの公開は、未実施の項目を攻撃される可能性もあるため、公開には十分注意を払う必要がある。

(1) 運用時間帯の考察

セキュリティを確保するために、その機能を稼働する時間を制限できれば、セキュリティ事件・事故が発生する可能性は低くなる。

校内無線 LAN の運用時間帯を 24 時間／日でなく、利用しない時間帯を設ける、あるいは、特定の時間帯の利用者（アカウント）ログの監視を強化する等で対応することも考えられる。

(2) 業務ソフトウェアの検証（含 利用アカウントの脆弱性）

業務ソフトウェアでは、開発企業と販売業者が異なることがあり、販売業者が十分に理解していないことがある。そのため、要求仕様にセキュリティ項目を含めることや検収時のチェック項目（含セキュリティ監査）を検討する。

(3) アカウント管理

本事案の最初の脆弱性は、生徒が無職少年にユーザ ID、パスワードを教えたことであり、アカウント管理の重要性を示している。パスワードについては、文字長、文字種、推測し難い、過去のものを利用しない、ユーザ ID と異なるもの等のパスワードポリシーを定め、適用する。

更に、ユーザ ID やパスワードを不用意にオンライン保存せず、保存していないかの監査

[22] ランサムウェア（Ransomware）とは、パソコン内のファイルを暗号化等をして使用不能にし、元に戻すために、「身代金（Ransom）」を要求するマルウェアで、1980 年代末に「AIDS ウイルス」と呼ばれるものが国内でもあった。

を行う。

なお、ユーザ ID については、パッケージソフト等には、特別なユーザ ID（テスト ID、ゲスト ID 等）が存在することがあり、パスワードが固定されていることもあるため、必ず確認する。

更に、生徒端末エラーの対応時の修復用ユーザ ID、パスワードについても、当該端末だけに対応できる機能の採用等の検討を行う。

利用者、教職員、生徒等がパスワードを忘れた場合の対応では、初期設定パスワードを配布する方法やシステムで自動的生成する等を行い、パスワードを平文で保存してはならない。

(4) 重要アカウントを含む文書類

可能な限り、オフラインで利用する。オンラインでないと利用できない場合には、終了後、直ちにオフラインに戻す仕組みを構築する。

(5) セキュリティ／システム監査の実施

監査は、内部監査と外部監査があるが、外部については、実施内容、年間監査回数、委託先等を決める必要がある。

一方、内部監査では、外部監査を実施する前提であれば、主に、管理・運用について監査を行い、技術的な部分については、外部監査に任せることで良い。

(6) 関係者（教育委、学校、業者等）による情報共有体制の確立

教育システムは、各学校で同じようなことを行うが、地理的に分散していることが特徴である。

セキュリティ事案では、業者を始め、各学校等の担当との情報共有を迅速に行う環境を利用することが望ましい。県庁で TV 会議の利用があるため、その設備を利用し、教職員や業者等の月次や四半期、年次等の会議に TV 会議システムを利用し、普段から設備の利用等に習熟することで、大規模トラブルやセキュリティインシデントなどに迅速に対応できるようにする。

セキュリティ事案は、頻繁に発生するものではないため、外部で発生したセキュリティインシデント等の情報共有サイトやデータベース等の構築を行い、関係者の利用や TV 会議等で利用できる仕組み、「机上訓練」を構築する。

(7) セキュリティ文化の確立

本事案での情報漏えいの原因の一つは、「基礎的・実践的セキュリティ」の知見が希薄であったことにある。

更に、今回は直接的な影響はなかったが、ルールやポリシーがない場合の対応やセキュリティ倫理、コンプライアンス等の教育・訓練も大切な事柄である。

利用者個々の課題の教育・訓練だけでなく、グループ、組織としての対応についての教育・訓練も大切になる。

この訓練では、セキュリティ関連の知識・経験だけでなく、問題発見や問題解決、ヒューマンエラーとチーム／組織対応、事件・事故の発生を完全にゼロにできなくても、関係者等のリスクを小さくし、「ヒヤリ・ハット」の段階で解決することの重要性等を体験的な教育・訓練を通して行う体制を構築する。

なお、生徒に対する情報セキュリティ教育の検討を行い、現行のモラル教育の見直しを行う。

(8) その他

情報共有を行うためにも、各校からの運用等に係る要望は、県教育委員会経由で行う。また、新規作成したデジタル教材の動作検証手順を確立する。例えば、動作検証は新規にデジタル教材を作成した教員と運用担当業者で行い、教員が単独で行うことがない仕組みを構築する。

4．2 中長期的対応

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を示す。但し、今期、行う事が可能なものは、実施する。

(1) セキュリティ組織の検討・実施

行政・教育・システムに精通した最高情報統括監（CIO）やセキュリティ統括のセキュリティ統括監（CISO）等を新設し、組織体制を構築する。なお、担当職位や各職位の権限・能力、内・外部採用等の検討を行い、適材適所を実現する。

また、情報通信システム教育やセキュリティ教育・訓練を横断的に統括し、情報通信システムや情報セキュリティを最適化する「プロジェクト・マネジメント・チーム（PMT）」を設置する。

危機管理に対し、県庁関連部門との連携をより図り、業務継続計画（BCP）を策定することが望ましい。

(2) 技術的セキュリティ対策の検討

本事案では、外部者（無職少年）が、内部者（生徒）の持つ情報を取得し、不正アクセスを実行したもので、技術的セキュリティ対策は、殆ど関係ないが、今後、外部からネットワークや業務プログラムの脆弱性等の攻撃や電子メールでの標的型攻撃(マルウェア感染やランサムウェア等）対策に関連する製品・サービスや導入計画等の調査・研究を行う。

生徒端末での不正を防止するための、複数要素認証システムの調査・研究を行う。

(3) ヘルプデスクの電話録音

ヘルプデスクに集まる情報は貴重な情報であるが、緊急時では、記録することが困難な場合が多い。しかしながら、それらの収集により、より高い品質のサービスが可能になり、セキュリティ対策に寄与することも多い。ヘルプデスクへの電話情報を月次レベルで集約できれば、ヘルプデスク担当者への教育にも有効である。 なお、録音は適当な保存期間を定めること。

(4) ログ管理

現在のログ管理の検証を行い、今後のログ管理について調査・検討を行う。

(5) 情報公開の検討・実施

本事案だけでなく、ヒヤリ・ハット、小さな事案を含め、可能な限り、公開を目指す。

「秘すれば花」という世阿弥の言葉もあるが、セキュリティでは、小さな事案等を公開することが結果的には、大きなセキュリティ事案をなくし、ヒヤリ・ハットや小さな事案を減らすことになる。

事案情報の非公開は、それが発覚した場合、10 倍、20 倍の問題に拡大することは、本事案でも明らかであり、県教委のウェブサイトを活用し、県民や保護者等を始め、県立学校全体に広く、早く伝える公開方法や、公開内容等の調査・検討を行い、実施すべきである。

5　セキュリティ対策実施上の留意点

5．1　学校の情報システム設計・運用とセキュリティ対策

学校における情報システムは、教職員や生徒の活動を支援する道具であることを忘れてはならない。必要なセキュリティ対策は確実に実施すべきであるが、セキュリティ対策が教員や生徒に大きな負担を強いてはならない。情報通信システム導入の良さを不便さが上回るようでは本末転倒である。

そのためには、可能な限り、教職員や生徒に対し、大きな負担にならないように、十分な検討を行い、セキュリティ対策を行わなければならない。短期的には難しくても、中長期的には利用者負担が軽減する対策があることを十分調査・検討し、実施することが重要である。

セキュリティ対策により、教職員や生徒に過度なセキュリティ対策を強いることは、業務効率を落とす、あるいは隠れてポリシー違反をする等の弊害を引き起こすことがある。実際、本事案でも、セキュリティを無視した対応がいくつか見られる。

システム更新時だけでなく、定期的にシステム／セキュリティの見直し[23]を行い、教職員や生徒から、使い勝手等の情報収集を行う必要がある。なお、教職員や生徒から情報収集す

[23] 「見直し」は、変更をするのではなく、適切な処理ができているかの調査・検討を行うことで、変更不要であれば、見直しを実施したとの記録を残すだけでよい。

る場合、利用者が指摘しやすい環境を作ることが大切である[24]。

収集した情報を基に、システム設計や運用手順の変更に役立たせると共に、情報提供者にも、変更の情報を提供する。

５．２ 学校現場の実態に即したセキュリティ対策

セキュリティ対策でも、往々にして利用者の実情を十分調査せずに、全面実施が行われることがある。その結果、利用者に大きな負担がかかることがある。

セキュリティポリシーの下位層である「対策基準」や「実施手順」を利用者全員に画一的に適用する例が多々見られる。学校現場でも、全ての教職員が同一のルールで対応できるとは限らない。そうであれば、例外を認める仕組みを確立すべきであり、それによって、管理・運用面が明確になる。

例えば、通常の勤務時間から判断し、コンピュータ利用時間を厳格すれば、定められた時間外には、サーバに接続できなかったり、ネットワークプリンタが使えなくなったりすることもある。事前申請で、利用時間を変更できるとか、利用時間外には、不正アクセスがないか等の監視を強化する等の方策も考えられる。

また、ファイルの暗号化についても、暗号化[25]の意義を十分理解して行い、通常の業務処理であれば、一般の利用者は暗号化の有無を感じない仕組みを構築すべきである。

６　おわりに

セキュリティ対策は、情報通信システムの一部として発展してきたこともあり、技術的対策が中心である。必要な機器やソフトウェアを導入すれば、一定期間、問題が発生することはなく、処理が正しく実行されない場合や全面的な問題が発生する場合でも、高々、システムが停止する程度であると考えられてきた。

しかしながら、ネットワークを利用した業務システムの利用者は人間であり、また、それらのシステムを管理・運用しているのも人間である。更に、インターネット等に業務システムが接続されていれば、正規の利用者だけでなく、システム侵入をはかり、内部の情報を盗取しようとする攻撃者・犯罪者もいる。

そうであれば、システムをインターネットに接続せず、重要な情報の安全を確保するには、「コンピュータの電源を切り、金庫の中に置く」事だと言われてきた。しかしながら、攻撃者が巧妙であれば、「金庫にあるコンピュータを取り出し、電源を入れ、ネットワークに接

---

[24] 参考： D.A.ノーマン、誰のためのデザイン？、新曜社　ページ 54～56、「自分を責めてしまうという誤り」

[25] セキュリティ対策としての暗号化は必ずしも安全を担保するものではない。例えば、①暗号化ファイルも削除可能、②業務プログラムを実行できれば、暗号化は意味がない、③ネットワーク上の暗号化（SSL/TLS）は各端末側では暗号化されていない、④ワンタイムパスワードも 100%安全ではない。

続させるように誘導する」可能性も否定できない[26]。

日本の多くの組織では、数年で人事異動が行われる。このため、組織体制を構築しても、実効性がないものになったりすることが、特にセキュリティ関連では数多く見受けられる。そのためにも、単に組織を構築するのではなく、「セキュリティ文化」とも言うべき体制の構築が必要だと考えている。

定期的な検証・考察、改善などを行うと共に、本事例からの大きな課題は、

- 人間の弱さを攻撃手段[27]とするものが、今後も増大する
- 運用の利便性を優先した、あるいは、実践的セキュリティ知識・経験の乏しさにより、セキュリティ対策が有効に機能しない仕組みになっていた。

等であり、これらを防ぐためにも、ヒューマンエラー等を報告するルールの確立／都合の悪い情報でも公開する体制／情報共有の仕組みの構築／これらのための教育･訓練等により、システム、あるいはセキュリティの強靭化[28]を図り、セキュリティ文化を醸成することが必要不可欠である。そのためには、県教委内部はもちろん、県議会や既設の「ＩＣＴ利活用教育の推進に関する事業改善検討委員会」等で、普段からセキュリティについて論議を続け、深めることが必要であり、そうすることによって本提言の実効性の担保にもつながる。加えて、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が、ひいては保護者や生徒、県民の不安を払拭し、信頼回復に繋がることを指摘し、本提案の結びとする。

---

[26] コンピュータ関連犯罪ではないが、「振り込め詐欺」は、これに近いことが行われている。

[27] ソーシャルエンジニアリング攻撃では、ユーザ ID／パスワードの盗取や遠隔操作ツールを埋め込み、それを利用して、サーバ等にある情報を盗取する。

[28] 強靭化（Resilience）とは、強くてしなやかなものを言う。