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　提言書要旨

本事案では大量の個人情報が窃取され、生徒や保護者をはじめ県民の不安と不信感を抱かせた。原因を究明し、真摯な反省の上に立って、同一の問題を再び起こすことのないよう、県教育委員会には、下記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。

１　本事案の概要

無職少年が他人のユーザ 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。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のように人間の心理的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。

２　運用上の課題

情報窃取の原因は、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。

３　今後のセキュリティ対策

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」に終わる。そのため「包括的なセキュリティ対策」を考える必要がある。

３．１　短期的対応

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。

⑴ アカウント管理 （パスワードポリシーの設定）

⑵ セキュリティ／システム監査の実施 （内部監査、外部監査）

⑶ 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）

⑷ 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）

３．２ 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。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）

４ まとめ

数年で人事異動を伴う組織の場合、組織体制を構築しても、その後の実効性が失われがちである。そのためにも「セキュリティ文化」とも言うべき体制の構築が必要。

県教育委員会、県議会や既設の検討委員会等で、普段からセキュリティについて論議を続け、深めることが必要。それが本提言の実効性の担保にもつながる。

また、本事案を機に学校現場や生徒、県民からも広く意見を聴く場を設け、セキュリティのみならず教育の質的向上や利用者の利便性向上、校務の効率化という本来のミッションについても情報を共有・交換し、県教育委員会自らが考え、改革していく姿勢を示すことで、保護者や生徒、県民の不安を払拭し、信頼回復につながるものと考える。

資料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

資料２

運用上の課題

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　S 高校での関連事案（平成 27 年 6 月に教員が校内 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。