平成２８年１２月２７日

佐賀県学校教育ネットワークセキュリティ対策実施計画

佐賀県教育委員会

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において、提言書がとりまとめられた。

この提言を踏まえ、今後の情報セキュリティ対策について、以下のとおり実施計画を策定する。

なお、対策のうち、中長期対応（セキュリティ組織の検討・実施等）については、引き続き検討を行い、実施計画に反映させるなど、実施計画については必要に応じて随時、見直しを行う。

また、実施計画への取組状況については、毎年度、ICT 利活用教育の推進に関する事業改善委員会へ報告、意見を伺うとともに、ホームページ等で公表することとする。

１　運用時間帯の見直し

＜提言内容＞

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。

※ 提言書（45 頁）－第 7 提言－4.1 短期的対応－（1）運用時間帯の考察

＜実施計画＞

○　校内無線 LAN について、夜間や閉校日など、不使用時の停止措置を実施する。（実施済）

○　休日等に学校行事等があり、校内無線 LAN を使用する場合は、学校から教育総務課に申し出ることとし､教育総務課は委託事業者に対し当該時間帯に接続が可能となるよう設定変更を依頼するものとする。（実施済）

2　業務ソフトウェア導入時のセキュリティチェックの強化

＜提言内容＞

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。

※ 提言書（45 頁）－第 7 提言－4.1 短期的対応－（2）業務ソフトウェアの検証

＜実施計画＞

○　業務ソフトウェアである SEI-Net システム運用契約について、開発企業が製作したオペレーティングシステム等の基本ソフトを含めた脆弱性の有無の確認や、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こと等、セキュリティ項目及び検収時のチェック項目を含めた仕様に契約変更する。

○　検収時の確認等については、情報技術の専門家（情報監等）が行うこととし、その状況については、監査（詳細は後述）でも確認する。

3　アカウント管理（ID、パスワードの管理）の強化

＜提言内容＞

①　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。

②　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を行う。

③　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。

④　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。

⑤　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。

※ 提言書（45 頁）－第 7 提言－4.1 短期的対応－（3）アカウント管理

＜実施計画＞

○　①については、既に運用していた教職員パスワードポリシーに加え、生徒パスワードポリシーを策定し、利用者に遵守させるとともにシステム側でパスワード条件（文字長、期間等）を設定し、ルールに適合するパスワードが設定されるようにする。（実施済）

○ ②及び③については、県立学校全校の監査を毎年度、実施する。（平成２９年～）

○ ④については、端末をコールセンターで預かり、対象端末のみしか利用できないワンタイムパスワードを発行し、修復を行う。また毎月、業者からの報告を受け確認を行う。（実施済）

○ ⑤については、初期設定パスワードは教職員及びヘルプデスク現地員には事前に配布せず、パスワードを忘れた際には、ヘルプデスク現地員よりコールセンターに当該機種のみしか利用できないワンタイムパスワード発行を依頼し、ヘルプデスク現地員立ち合いのもと、その場で、生徒等本人により新たなパスワードを変更させる。（実施済）

4　重要アカウントを含む文書類のオフライン管理の徹底

＜提言内容＞

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。

※ 提言書（46 頁）－第 7 提言－4.1 短期的対応－（4）重要アカウントを含む文書類

＜実施計画＞

○　重要アカウント（各学校では使用しない管理者用アカウント）を含む文書を各学校に配付しないこととする。なお、オンラインで利用することが必要な場合は、教育総務課の許可を必要とする。（実施済）

5　セキュリティ／システム監査の実施

＜提言内容＞

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。

※ 提言書（46 頁）－第 7 提言－4.1 短期的対応－
（5）セキュリティ／システム監査の実施

＜実施計画＞

○　各教職員の端末の使用状況に係る監査及び校内 LAN 監査については、平成２８年度内に実施手順を策定する。

○　各教職員の端末の使用状況に係る監査については、毎年度、外部監査法人の指導・助言のもと、全県立学校への内部監査を実施する。

○　SEI-Net システム監査については、外部監査を実施する。

○　校内 LAN 監査については、毎年度、外部監査法人の指導・助言のもと、全県立学校への内部監査を実施する。

○　監査結果については、ホームページで公表する。

６　関係者（教育委、学校、業者等）による情報共有体制の確立

＜提言内容＞

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。

※ 提言書（46 頁）－第 7 提言－4.1 短期的対応－
（6）関係者（教育委、学校、業者等）による情報共有体制の確立

＜実施計画＞

○　毎月の業者毎の定例会議とは別に、全ての業者を集めた会議を四半期ごとに開催し、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及び対策について周知･確認するとともに、その情報等については、蓄積し、関係者が利用できるようにする。（実施済）

○　インシデント発生時に、TV 会議が可能な環境を整備する。（業者については実施済、全県立学校については平成２９年１月末までに整備予定）

○　SEI-Net システムを利用し、外部で発生した事も含めてセキュリティインシデント等の情報共有を行う。（平成２９年３月～）
○　関係業者すべてが参加する机上訓練を毎年度、実施する。（平成２８年度は３月までに開催予定）

7　セキュリティ文化の確立

＜提言内容＞
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。

※ 提言書（46 頁）－第 7 提言－4.1 短期的対応－（7）セキュリティ文化の確立

＜実施計画＞
○　県立学校の ICT に関する運用ルールや情報セキュリティ等について、「佐賀県立学校 ICT 運用ルール集（仮称）」としてまとめ、学校に周知する。（平成２８年度内に周知）
○　教職員に基礎的・実践的セキュリティの知識を身につけさせるため、各種研修会にて情報セキュリティのカリキュラムを加える。また、県教育委員会事務局職員に対して、毎年度、研修を実施する。（平成２９年度～）
※　各種研修会・・・ICT 推進リーダー、管理職、初任者、３年経験者、１０年経験者
○　教職員向けに専門研修（情報セキュリティ部門）及び e ラーニング研修を開設する。（平成２９年度～）
○　インシデント発生時の対応フローや運用ルール等を盛り込んだ、県立学校教職員向け

のセキュリティハンドブックを作成し、毎年度更新する。（平成２９年度～）

○　SEI-Net システムを利用し、ヒヤリ・ハット、インシデント情報を共有し、教職員の注意喚起を図る。（平成２９年３月～）

○　生徒向けには、各県立学校において、情報モラル教育に関する年間指導計画を作成するなど、情報モラル教育を組織的、体系的に推進し、情報セキュリティを含めた情報モラル教育をより一層充実させる。（平成２９年度～）

８　県教育委員会による情報の把握・統制

＜提言内容＞

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。

※ 提言書（47 頁）－第 7 提言－4.1 短期的対応－（8）その他

＜実施計画＞

○　端末の更新に伴う設定変更等、システム運用に関することについては、教育総務課経由で実施する。（実施済）

○　また、全ての県立学校に対して、指導主事を割り当て、定期的な訪問（担当校訪問）を行い、情報収集等を行う。（実施済）

９　デジタルコンテンツのインストール方法の改善

＜提言内容＞

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。

※ 提言書（47 頁）－第 7 提言－4.1 短期的対応－（8）その他

＜実施計画＞

○　平成２８年度中に新たな教材インストール手順、動作検証手順を確立し、平成２９年４月から実施する。

10　生徒端末規約の策定

＜提言内容＞

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 ）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。

※ 提言書（44 頁）－第 7 提言－3.6　生徒端末について

＜実施計画＞

○　学習用パソコン運用について利用規約を作成し､生徒／保護者はネットワーク接続申請を行うこととする。（平成２９年度～）