教員用パソコンの情報漏えい対策

― シンクライアントシステムによる業務継続性の実現 ―

株式会社アルファシステムズ　経営企画本部技術推進部
課長　千葉　大作
http://www.alpha.co.jp/

キーワード：教員用シンクライアント,情報漏えい対策,新型インフルエンザ対策,校務の効率化

１．はじめに

校務の情報化により､公立･私立を問わず教員用パソコンの配備が進み、同時に取り扱う情報量が増加しています。

自宅のパソコン保有率も高まったこともあり、パソコンの操作に不慣れな教員が遅れを取り戻すためにＵＳＢメモリ等で情報を持ち出し、自宅で校務を継続、その結果、誤操作や自宅パソコンのウィルス対策の不整備が原因の情報漏えい事故が増加しています。

また教員用パソコンの配備もまた完全ではなく、職員室へ個人所有のパソコンの持ち込み、ＵＳＢメモリで機密情報を持ち出し自宅で校務を継続しているのが現状です。そのためパソコンの紛失・盗難による情報漏えいが増加しました。(図 1　漏えい原因（インシデント件数))。

文教分野においては、ルールとしての拘束以外にデータの暗号化、指紋認証機能、生体認証などのデータ保護のためのセキュリティＵＳＢメモリを教員に配布し、情報漏えい対策を実施していますが、本当にそれで情報漏えい対策が万全と言えるのでしょうか。

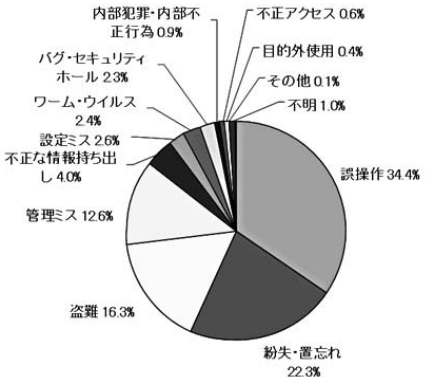

図 1　漏えい原因（インシデント件数）

出典：NPO 日本ネットワークセキュリティ協会
2008 年上半期情報セキュリティインシデントに
関する調査報告書

２．校務用パソコンの暗号化セキュリティと脆弱性

２．１ 機密情報の暗号化による情報漏えい対策

ＵＳＢメモリ内のデータ、ノートパソコンのハードディスクを暗号化したものが広く普及していますが、成績など個人情報の入ったまま紛失した場合､情報流出の有無に拘わらず保護者に対し､説明会や謝罪を行う必要があります。

２．２ デバイスキーを利用したシステム制御による情報漏えい対策

パソコンの起動にＵＳＢキーやＩＣカードを利用することで、正しい利用者（所有者）であることを判別するシステムでも、個人情報の入ったパソコンを紛失した場合は、0 と同様に説明会、謝罪の説明責任があります。

３．校務用パソコンのシンクライアント化と課題

機密情報を直接持ち歩くことなくデータを編集可能にするシステムがあります。かつては SSL-VPN により通信路を暗号化してサーバ上にあるデータを取り出し、編集できるものが主流でした。しかし Winny などファイル交換ソフトの普及により、悪意あるウィルスが意図せず感染し、通信路を暗号化しても情報漏えいするケースもでてきました。そこで新たに登場したのがデータを表示させた画面を転送する方式です。

３．１ アプリケーションをインストールして利用する画面転送

既存のパソコンに専用アプリケーションをインストールして、デスクトップ上に堅牢な仮想環境を構築して個人情報を操作・編集することが可能なシステムで、導入のしやすさから広く普及しています。機密情報は学校内のネットワーク上のサーバに保存されているため直接持ち歩くよりも安全ですが､利用パソコンがウィルスに感染していると、仮想環境上の操作画面をまるごとキャプチャーされ情報漏えいしてしまう恐れがあります。

３．２ 専用ハードウェアを利用する画面転送

既存のハードディスクを一切利用せず、専用のハードウェアから仮想環境を呼び出すことで上記問題を解決することができます。また既存ディスプレイも活用してコストを抑えることが可能になります。

３．３ 専用ＵＳＢメモリを利用する画面転送

０と同様に既存のハードディスクを利用せず、端末にＵＳＢメモリを差し込むだけでＵＳＢメモリからＯＳを立ち上げ、仮想環境を呼び出します。専用ハードウェアよりも形態性が高く、職員室内だけでなく、早めに校務を切り上げて育児・介護と平行して自宅から校務を安全に継続するテレワーク的な運用も可能になります。

３．４ ハードディスクレス端末を利用する画面転送

専用のハードディスクレス端末を利用することで非常に強固なセキュリティ強度を保つことができます。しかし、既存パソコンや自宅のパソコンなどの利用はできず、校務用パソコンシステムとして一括購入には向いていません。

４．新型インフルエンザ対策とセキュリティ

データ持ち出しに関するセキュリティ対策は、事業継続という観点でも注目を集めています。厚生労働省は世界的な大流行（パンデミック）を引き起こすと言われている新型インフルエンザ対策に対し、ガイドラインを設けてテレワークを推奨し、企業・地自体に呼びかけています。予期せぬ学級閉鎖や学校閉鎖により、自宅作業を余儀なくされた場合でも、個人情報を持ち出すことなく安全な校務環境を自宅に構築できるシステムとしてシンクライアントシステムが注目を集めています。

表１　セキュリティ方式別説明責任とテレワーク可否

方式	詳細	PCやＵＳＢの紛失時謝罪が必要か?	新型インフルエンザ対策として自宅利用できるか	コスト
暗号化によるデータ保護	暗号化ＵＳＢ／ＨＤＤの暗号化	必須	**情報流出の危険あり** データを自宅に持ち帰ることは危険。	既存資源流用可能
システム起動制御	ＵＳＢキー／ＩＣカードでパソコンを起動	可能性あり パソコン自体を紛失した場合は必要	**情報流出の危険あり** 起動していれば校務利用パソコンを持ち歩くのと同等の危険性。	
画面転送型	Windowsアプリケーションから画面転送	不要	**情報流出の危険あり** 秒間で画面キャプチャーなどを実施するウィルスには対処方なし。	
	専用ハードウェアから画面転送	不要	**安全** 校内と自宅にそれぞれ専用ハードを用意する必要がある	
	ＵＳＢメモリから独自ＯＳを立ち上げ画面転送	不要	**安全** ＵＳＢメモリは書き換え不可、校務データも一切ない。既存ＨＤＤを利用しないのでウィルス被害の心配がない	
	ハードディスクレス端末から画面転送	不要	**安全**	全て新規購入

５．alpha Teleworker 教員用シンクライアントお問い合わせ

当社は、セキュリティ・校務継続性の観点から『ＵＳＢメモリから独自ＯＳを立ち上げるシンクライアント』を各自治体様、学校様にご案内させていただいております。

ご不明な点は、メール、またはお電話でお問い合わせ下さい。

株式会社アルファシステムズ テレワーカー係　Tel：044-738-4125　Mail：teleworker@alpha.co.jp