持ち出し禁止データの校外からの安全利用法の提案

A Proposal of Method to access 'the data used only inside' from outside the school safely

三輪 吉和*・宮田 仁**

Yoshikazu Miwa* and Hitoshi Miyata**

特定非営利活動法人　学習開発研究所（滋賀大学大学院教育学研究科）*・滋賀大学教育学部**

* Non-Profit Organization Institute for Learning Development

** Faculty of Education, Shiga University

＜あらまし＞　個人情報の管理が厳しく制限されているが，学校現場では個人情報を含んだデータファイルを外部に持ち出さないという杓子定規な運用規定だけでは円滑な業務遂行が不可能な現実がある．このため，強制的にデータファイルを暗号化するなどの対策がなされている．この方法ではストレージの紛失には有効だが，校外での利用環境を管理者が制御できないため，USB ストレージには一切の記録を禁止するセキュリティポリシーのところもある．

そこで，筆者たちは校外へデータを持ち出すのではなく，安全な方法で校内のデータを利用するシステムを構築し，運用可能性を探ることにした．本論文は，この方法を実現するに至った理由，その実現方法とテスト運用で得られた知見を報告するものである．

＜キーワード＞　学校事務処理，システム設計，システム開発，ネットワーク，インターネット

1.はじめに

教育用ネットワークでは①インターネットと教育センター等で接続，②教育センターと各学校や社会教育施設と地域ネットワーク経由でイントラネットを構成，③各学校では校内LANで各校毎に教員用や児童生徒用のファイルサーバを利用，というシステムが多い．

さらに校内LANでは、生徒用LANと教職員LANに分割し、教職員専用のファイルサーバで校務情報の共有化が図られている．

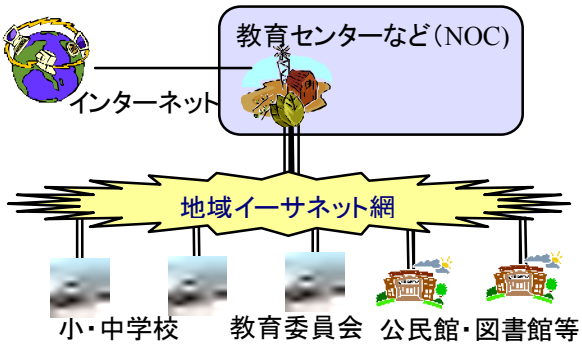

図　1　教育用ネットワーク概略

本報告では，教職員用のデータ共有システムを安全に校外からでも利用できるシステムを考案するに至った経緯と，システム概略について述べる．

2.イントラネットのセキュリティと利便性

2.1. 勤務時間中に終了しない校務処理

学校内の教職員サーバでは，教職員のみがアクセス可能なファイル共有機能をサーバに構築し，セキュリティを確保した状態で成績処理などの個人情報を取り扱っている．この方式では校務処理をするには校内にいなければならない．しかし，教員の事情や出張などで校外にデータを持ち出さざるを得ない場合もある．

2.2. 地域イントラ内でのデータ共有

教育委員会事務局に対して，個人情報を含んだデータを提出する場合がある．このような目的のため，データを自動的に暗号化するUSBストレージに記録して運搬したり，地域イントラネットの共用ファイルサーバにアクセス権限を制限した特別な領域を用意して，そこに保存させる仕組みを採用しているところもある．この「イントラネット内は安全」「暗号化すれば安全」という考えを活用したいと考えた．

2.3. 安全な USB ストレージの利用方法

USBストレージに暗号化チップを内蔵し，自動的に保存したデータを暗号化するだけでなく，OSの動作を制限（印刷，LAN通信の制限や，ファイルの移動，コピー&ペーストの制限）ができるも

のも販売されている．

これらは，データが暗号化されているので安全ではあるが，作業中は平文になっているうえ，ファイルのコピー制限とLAN通信制限をきちんと制御しなければ，情報漏洩の原因となる．さらにパスワードが貼り付けられたり，簡単に想像できるようなものであっては，意味をなさない．

3. SSL-VPN でイントラネットに接続する

3.1. 共用ストレージを活用する方法

2.2で示したように学校内外からファイルサーバを暗号化通信してアクセスできるようにすればデータの持ち出しをしなくても校務処理が可能である．このようなシステムとして，USBストレージに記録されたプログラムの自動起動に関する特許を持つ会社（株式会社サスライト）が，イントラネットとインターネットの両方から安全にファイルをアクセスするUSBドングル方式のシステムを販売していることを知った．

しかしこの方式では，専用のファイルサーバが必要であり，校内にある各教職員のホームディレクトリを，校外からアクセスさせるのはかなり困難だった．

この方式の利点は，USBドングルにはデータが記録されておらず，ドングルを紛失しても，管理者がすぐに利用停止することでデータの流出を防げる点にある．しかし，同一データを複数サーバに保存するため一貫性を保持するのが難しく，さらに「外部からそのファイルにアクセスできる」＝「データを外部に持ち出せる」ことを意味しており，安全面においての不安が残った．言い換えると，このシステムは「データの外部持出し」と同一と判断したのである．

3.2. ゲートウェイ方式＋情報持ち出し禁止機能

3.1.で述べた方式の欠点は，①データを複数サーバで管理する，②外部からアクセスしたときにデータをコピーできる，の2点に集約される．これを防げれば，安全に外部からデータの編集ができると考えて，その開発を上記企業に持ちかけた．

その結果，①SSL-VPNでゲートウェイサーバに接続，②ゲートウェイサーバが接続要求元のIDをUSBドングル内の暗号キーとユーザが入力したパスワードを元にアクセスできるデータを特定，③ゲートウェイサーバはSSL-VPNで社内Webサーバやファイルサーバにアクセス，④アクセスした情報がファイルであれば，現在ユーザが利用しているPCへの保存（ペーストバッファや画面キャプチャを含む）や印刷を禁止，というシステムの実現に至った．

一般ユーザはWindowsのInternet ExplorerでWebアクセスできるPCさえあれば，暗号化された経路で，校内のホームディレクトリを自宅等の校外から直接編集可能となる．複数のファイルサーバに対しても一元管理可能である．このシステムを利用中のPC内では一時保管データも暗号化されており，ドングルが引き抜かれた段階で一時保管データも消去される．このため，データを外部に持ち出さずに，校内データの編集が自宅等の校外から可能となる．

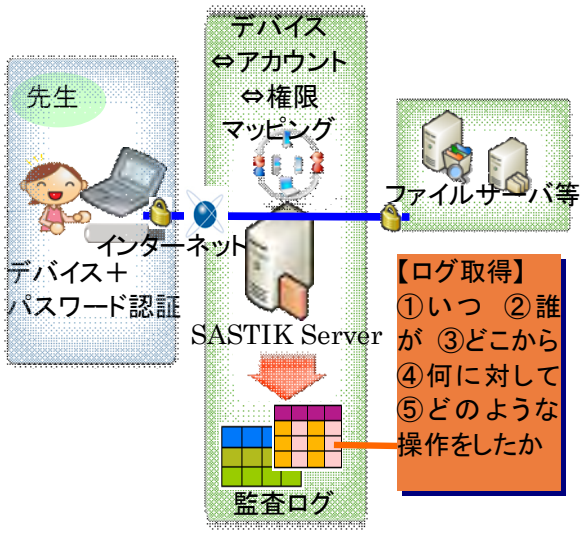

図 2 提案システムの概要

逆に校外PCから校内ファイルサーバへのデータ保管は可能である．この場合コンピュータウィルスの混入が危惧されるが，ファイルサーバ側でウィルスチェックをすることでその対策は可能である．

4. まとめ

すでにこのシステムは稼動しており，①本当にデータの漏洩を防止できるか，②利用者環境に依存する点の洗い出し，③教員が利用する場面を想定した利用方法のチェックを行っている。これに引き続き，数名の教員に協力してもらって，テスト運用を行い，利用方法のマニュアルを作成後，本格運用を計画している．