持ち出し禁止データを外部から安全に利用する一方法

三輪 吉和*・宮田 仁**
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**

セキュリティ対策として社内情報の持出しが厳しく制限されるようになっている．しかし，データファイルを外部に持ち出さないという運用規定だけでは円滑な業務遂行が不可能である．実際には，持ち出し用ストレージ機器に自動暗号化などの手段でデータ保護したうえで外部に持ち出されている．そこで，筆者らは外部へデータを持ち出さず, USB キーを用いた安全な方法で社内のデータを外部から利用するシステムを構築した．本論文では，この実現方法とテスト運用で得られた知見について報告する．

A Proposal of safe method to access 'the confidential information' from outside of the Organization

Yoshikazu Miwa* and Hitoshi Miyata**
* Non-Profit Organization Institute for Learning Development
** Faculty of Education, Shiga University

As part of security countermeasures, taking out the confidential information is severely limited. But, only in the operation regulations of ‘not taking out the confidential data files outside’, a smooth business accomplishment is impossible. Actually, the confidential information is encrypted, preserved in portable storage, and taken out outside. Therefore, we constructed a system that accesses ‘the confidential information’ from outside of the organization using USB key device. You can modify and display ‘the confidential information’ from outside, but cannot copy or printout them at the outside. This report describes an outline of the system and reports some results.

キーワード：VPN，セキュリティ，運用，暗号化，USB キー

1. はじめに

個人情報漏洩が社会問題化している現在，社内情報の取り扱いは企業や官庁でのリスクマネジメント上の最重要課題といっても過言ではないだろう．その対策として，①イントラネットに接続される端末をディスクレスや外部ストレージ機器が接続できないシンクライアント型に切り替えて，端末に情報を記録させないようにする，②アクセス記録を詳細に採取して情報漏洩対策，および万が一漏洩した場合の影響範囲を早期に確定できるような対策がとられるようになってきた．

しかし既存の方法では設備の更新や複雑な操作・設定が必要であったため，多数の一般利用者に適応することが困難であり，十分なセキュリティ対策を徹底することが困難であった．そこで筆者らはUSBキーを用いた簡便で安全なシステムの設計とプロトタイプシステムを構築した．ここでは，その概要と効果を述べる．

2. 外部から持ち出し禁止情報を利用したい事例

本来，関係者外秘の情報を扱うためには，構成員

のみがアクセス可能なイントラネットを整備し，データの持ち出しを不要にする環境整備が必要である．しかし現実にはシステムが未整備の場所での作業が要求されたり，そのようなインフラ整備を行う時間がない場合もある。

本章では，保護されているデータを安全に外部から利用できるシステムを構築する必要があると判断した経緯について述べる．

2.1. 出張の多い営業職やエンジニア

営業職が客先からイントラネット内でのみ閲覧可能な在庫管理システムをリアルタイムに閲覧できれば，在庫に応じた受注の可能性は高まるであろう．顧客に提示するプレゼン資料も移動中に社内スタッフが提示直前まで訂正することも可能となる．

また，Webメールシステムもイントラネット内でのみアクセス可能にしておけば，外部からの攻撃も回避できる．

同様にエンジニアも，社外持出し禁止である技術情報や，グループ会社専用のトラブル対策情報システムに社外からアクセスできれば速やかに現場での対処が可能となる．

2.2. 緊急呼び出しが想定される医療関係者

医療カルテは部外秘にすべき個人情報のうちでも最上位に値するひとつである．しかし，帰宅後や学会などで勤務地を離れた先で，患者に対する緊急措置の指示を仰がれた場合には，当該患者の最新データが必要である．このような場合では，手元に印刷物は不要で，時々刻々と変化する検査結果をリアルタイムに見られることが重要である．

2.3. 持ち帰り仕事が常態化している教員

小中高校の教員が毎日利用しているデータも，医療関係者のカルテと同様に本来は厳密な扱いが必要な個人情報である[1][2]．児童・生徒の住所や電話番号は，家庭の事情によっては極秘扱いにしなければならない．定期テストの点数や出欠記録も指導要録の基礎データであり，将来の進路決定を左右しうるので，本来は校外への持ち出しは厳禁である．そのため，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う規定になっていたり，校務に関する電子データの磁気ディスク保存が禁止されている事例すらある[3]．この方式では校務処理をするためには教員は校内で作業しなければならない．しかし，児童・生徒のクラブ指導，補習，出張などの公務や，教員自身の生活のために残業できず，しかたなく校外にデータを持ち出さざるを得ない場合もある．

3. 既存システムの課題

3.1. 外部ストレージの利用

外出先にネットワーク環境が存在するとは限らない．そこでいちばん良く利用されるのが，USB接続による外部ストレージ機器の利用である．USBフラッシュメモリーや，USBポータブルハードディスクにファイルの自動暗号機能が附属したものが市販されており，データを暗号化することで情報漏洩の危険性を下げることで持ち出しを許可する場合がある[4]．しかし，その場合でも接続先のパソコンがコンピュータウィルスに感染していた場合，たとえデータが暗号化されていてもファイルそのものが流出することは防げない．

特に暗号化チップを内蔵したUSBフラッシュメモリーを利用していた場合，一旦接続が許可されると，そのなかに保存されている各ファイルをさらに個別に暗号化しておかない限り平文ファイルとして扱われる．このため，利用者は暗号化されていると勘違いした情報漏洩が発生しうる．加えてパスワードをケースに貼り付けたり，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．

なお，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）できるものも販売されている[5]．しかし，これを利用するには専用のデバイスドライバのインストールが必要である上，ウィルス対策ソフトウェアとの相性問題も考慮に入れる必要がある．

3.2. VPN を用いた外部からの利用

前節で述べたとおり外部ストレージを用いた外部での利用には問題点が残る。そこでVPNを利用して外からデータをアクセスさせる組織も少なくない([6]のコラム5)．

ただし，VPNで社外から利用する端末はシンクライアント型とは限らない．このため外部ストレージを用いた外部での利用と同様に，部外秘のデータが

社外に漏洩する危険性がある．

これに対して，VNCなどの仮想端末ソフトウェアを利用してイントラネット内のデータを外部から直接操作する方式を採用している場合もある[7][8]が，仮想端末サーバの性能やネットワークの性能に大きく影響を受ける．

さらにVPN接続には専用の通信ソフトウェアのインストールと設定が必要である．特にクライアントソフトの設定は難しく，インターネットプロバイダへの接続すらパソコン販売店などに依存する一般利用者がVPNの設定を自身で行うことは不可能に近いといわざるを得ない．このため，コストがかかるが情報部門が事前に設定した端末を貸与することもある．この面倒さとコスト高を避けるために，SSL-VPN[9]やPPTPが利用されている．しかし，PPTPの設定もインターネット初心者に簡単であるとは言えない．

4．提案システムの概要

3章で述べたとおり，既存の方法では外部から持出し禁止データを安全に取り扱うには問題が多い。そこで筆者らは，USB キーを用いて簡便に VPN 接続ができ，さらに情報の持ち出しができないように工夫したデータアクセス方法を組み合わせたシステムを構築し[10]，評価を行っている．ここではシステムの概要について述べ，従来の問題をどのように解決することができるかについてまとめている．

4.1.提案システムで必要な機能について

2章で述べた例から，外部で持出し禁止データを利用する場合であっても，必ずしも外部へデータを持ち出す必要がないことが多いことがわかった．持出し禁止のデータを①外部から閲覧する，②訂正する，逆に，③イントラネットサーバへ外部からデータを送信するというよ要求はあっても，「社外端末にデータを保存する必要がない」という点が重要である．

まず，提案システムに必要なのは①いつ，②誰が，③どこから，④何に対して，⑤どのような操作をしたかの記録を常に採取できることである．

また，イントラネット内には所属部署やプロジェクト毎にアクセス可能なファイルサーバや，グループウェアサーバが複数台用意されている．これら複数サーバとの接続関係の組み合わせに加えて，同じファイルサーバであってもユーザIDによってアクセス権限や利用できる共有フォルダが異なるという条件がある．

このため，提案システムでは，ファイルサーバとはSMBプロトコルやWebDAVで通信することを前提としている．sambaであれば共有フォルダのアクセス権限を各sambaサーバ毎のユーザID別に細かく制御できるからである．

4.2. 提案システムの概要

前節で示した機能を実現するために，インターネット側からイントラネット内のサーバにアクセスする方式として，SSL-VPNアプリケーションゲートウェイ方式を採用することにした．

本システムの概要を図1に示す．

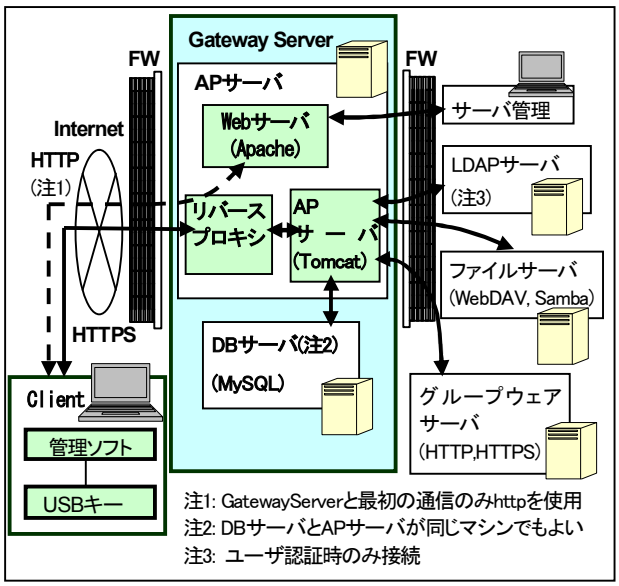

図 1　システム概要

インターネット側からは，USBキーとパスフレーズを利用してゲートウェイ・サーバに対してSSL-VPNで暗号化して接続を行う．

また，ゲートウェイ・サーバからイントラネット内のサーバに対してもSSL-VPN方式の暗号化通信も可能である．

イントラネットのデータにアクセスするクライアント端末は，現在のところWindows2000(SP4以上) / XP(SP2以上) / VISTAに限られている．しかし，その認証方法はいたって簡便である． Internet

Explorer(IE)でゲートウェイ・サーバにアクセスできるように設定するだけで済む. 具体的には, HTTPS接続で一般のWebサイト(Gmailなど)が利用可能になればよい.

ゲートウェイ・サーバのアドレスをユーザに通知する必要もない. 利用者が使用するUSBキーには, ①クライアント認証キー（ファイルとしてはアクセス不能), ②ゲートウェイ・サーバのURL, ③USBキーの所有者用「ユーザID」, ④クライアント起動用プログラム（USBキーからのみ起動可能で、取り出しても動作しない）が記録されている. このため利用者がUSBキーをUSBポートに差し込めば自動的にゲートウェイ・サーバにHTTPS接続し, パスフレーズを入力するだけでゲートウェイ・サーバとSSL-VPNが確立する.

USBキーに記録されているクライアント認証キーと, ユーザ用パスフレーズによる「二因子認証」方式であるため, たとえゲートウェイ・サーバのURL, ユーザIDとパスフレーズが漏洩したとしても, USBキーがなければゲートウェイは応答しない.

このシステムはイントラネット内での利用も可能である. この目的のシステムは多数販売されているが[11], それらはVLAN切り替えを自動で行うため802.1x方式のようにマルチサプリカント対応などのセキュリティ機能が内蔵されたハブやアクセスポイントが必要になる. しかし本システムはSSL-VPN方式であるため, 既存のネットワーク設備をそのまま利用できるメリットがある.

このUSBキーには, USBフラッシュメモリーの機能はない. この方式の利点は, USBキーにはユーザデータを記録できず, 万一紛失した場合は, 管理者がすぐにそのUSBキーの利用停止をゲートウェイ・サーバに指示するだけで不正アクセスを防止できる点にある. また, ゲートウェイ・サーバには, 各USBキーからの接続記録が保存されるため, 不正アクセスされた場合の記録も採取できる.

本システムはUSBキーをUSBポートに刺すだけで起動する[12]. CD-ROMによる自動起動とおなじ原理でUSBキーの「クライアント起動用プログラム」が自動起動し, クライアントPCのハードディスクに図２に示す作業用の「揮発領域」を作成し, 印刷機能や画面キャプチャ機能を停止させる. 揮発領域内に格納される各ファイルは自動的に暗号化される.

Microsoft Office システムの Word や Excel , PowerPointの作業領域も「揮発領域」内の「作業用エリア」を使用するよう起動情報が変更される. そのため, USBキー接続前にWordなどOfficeソフトを起動していると終了を求められる.

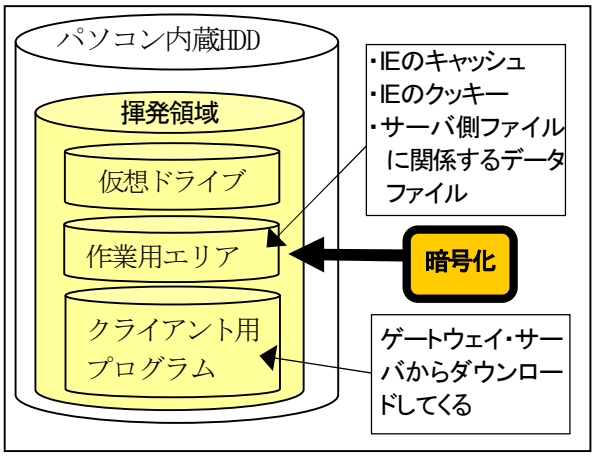

図 2　クライアント・パソコン内部の作業領域

続いて起動用プログラムは, USBキーに暗号化して記録されているURLを利用してゲートウェイ・サーバに接続し、パスフレーズの入力を待つ. パスフレーズとクライアント認証キーによる認証が成功すると, ゲートウェイ・サーバからイントラネット内のサーバにアクセスするための「プラグイン」を揮発領域にダウンロードする. 現在動作確認に使用しているプラグインは, ①イントラネット内のファイルをアクセスする「ストレージ・ブラウザ」, ②イントラネット内のグループウェアにアクセスする「ブラウザ・プラグイン」の2つである. これらのプラグインも「作業用エリア」を使用する. このため, イントラネット内のグループウェアにアクセスした際のキャッシュデータや, クッキーはもちろん, イントラネット内のデータファイルを閲覧してもそのデータは暗号化されている.

しかもイントラネット内のOfficeデータはもとより, テキストファイルなどのデータをコピーバッファに記録できないように制御している. いわゆる「コピペ」によるデータの持ち出しも不可能となる. もちろん, Word, Excel, テキストエディタの「名前をつけて保存」機能を利用してローカルドライブに保存することも禁止される. 印刷も画面キャプチャ

もできないため，表示されたディスプレイをカメラで撮影しない限り情報を持ち出すことはできない.

また, このUSBキーは前述のとおりUSBストレージではないため，「ハードウェアの安全な取り外し」手順を必要としない．イントラネット内のファイルサーバのデータを閲覧しているだけであれば，いきなりUSBキーを引き抜くことも可能である．編集中であれば，ファイル保存後に引き抜くだけでよい．自動的にUSBキー用のデバイスドライバが，USBキーがなくなったことを認識し，SSL-VPNを切断した上で，揮発領域の作業データを削除する.

削除されないように電源を切断したとしても，次回電源を入れた段階で作業領域は削除される. また, 作業領域のデータを含んだハードディスクをコピーしても，その作業領域は暗号化されているため，情報漏洩の危険性はかなり低い．なお，誤ってUSBキーを抜いた場合，すぐに差し込み直しても作業の継続はできない．USBキーが無くなった事を直ちに認識し，揮発領域を削除するためである.

現在のところ，情報漏洩に対応するOfficeシステムはMicrosoft Office 2000/XP/2003/2007であり，Just Officeについても一太郎2006/2007/2008等の一部に対応している．対応アプリケーションは，順次拡大していく予定である.

4.3. ユニーク ID によるアクセス管理

ゲートウェイ･サーバでは, 各ユーザを「管理職」,「営業部員」,「開発部員」等の職種や,「東京本社」「北海道支社」などの地域別など「ビジネスドメイン」と呼ぶ任意のグループに所属させ，そのグループに応じたアクセス権限を設定することができる.

各ユーザは, ゲートウェイ･サーバによって, USBキーに記録されたクライアント認証キーに含まれる「ユニークID」を元に，ユーザ認証と同時に所属する「ビジネスドメイン」を決定され，その「ビジネスドメイン」に設定された「利用可能なプラグイン」と「利用可能なイントラネットサーバ」が決定される.

したがって，ただ1つのグループウェアサーバにしかアクセスできない「ビジネスドメイン」に所属させた「ユニークID」のUSBキーを持ったユーザは，その1台のサーバしか利用できない.

ゲートウェイ・サーバのユーザ認証には，イントラネット内に設置したLDAPサーバに任せることでユーザ認証用パスフレーズが漏洩した場合の迅速な利用停止や再発行も可能である.

イントラネット内のWebグループウェアにアクセスする「ブラウザ・プラグイン」のエンジンはIEなので多くのグループウェアに対応できる.

イントラネット内のファイルサーバに対しても，「ストレージ・ブラウザ」を経由してアクセスが許可される．ストレージ・ブラウザに表示される「共有フォルダ」はビジネスドメインで指定されたものに限定される．また，ストレージ・ブラウザは，ストレージ･ブラウザ内でのみデータの移動, コピー, 削除, 更新, 名前の変更が可能である．ストレージ・ブラウザから外部へのファイル移動・コピーは禁止しているが，外部のファイルシステムからストレージ・ブラウザへのコピーは可能である.

ここで問題になるのは，オリジナルのファイルを保存したままで，新たに一部を修正したファイルを作成する場合である．このため，ストレージ・ブラウザが起動すると，揮発領域に「仮想ドライブ」が作成される。この仮想ドライブにオリジナルファイルをコピーした後，そのファイルの名前を変更し，元のフォルダにコピーするのである．これで，ファイルを外部に持ち出すことなく，オリジナルを保存したまま，新たなファイルを作成できる.

5 セキュリティ対策に関するまとめ

5.1. データ管理の一元性について

企業の情報系システムや大学のキャンパスネット, 教育委員会が運営管理する情報教育ネットワークなどでは，多数のファイルサーバやグループウェアサーバが稼動している．そして，インターネットとは数箇所で接続させ，Firewallでイントラネットを守っているというのが基本姿勢であろう.

こうした場合，外部からアクセスできる特定のファイルサーバを用意しておき，そこをバケツ代わりにして外部とデータをやりとりする方法が取られることがある．ちょうど一昔前のFTPサーバの発想である.

しかし，この方法では①データを複数サーバで管理するため最新データに更新し続ける手間がかかる，②外部からアクセスしたときにデータを外部に持ち

出されてしまう，という大きな欠点が残る．これを防ぎ，安全に外部からデータの編集ができれば，ほとんどの課題は解決できると考えて，本システムを構築した.

5.2. データ流出の危険性について

本システムでは，画面をデジカメで撮影しない限り，デジタルデータそのものの流出はほぼ防げると考えている．ただし，キー・ロガーのようなウィルスに感染していた場合，更新時に入力したデータの漏洩は発生する.

仮に利用しているパソコンがファイル共有ソフトのウィルスに感染したとしても，イントラネット内から取り出そうとしたデータはアップロード用エリアに移動できないし，万が一作業用のデータが流出してもそのデータは暗号化されているため，比較的安全性が高いと考えている.

さらにイントラネット内で利用できるWebメーラを本システム経由で外部から利用した場合も、添付ファイルを外部メディアに保存できない．しかしメールにファイルを添付して外部へ送信できれば持ち出し可能であり，これには別の対策が必要である.

5.3. 接続操作の簡便性について

いくらセキュリティが高くても，その設定が複雑であれば利用されない．より簡便な方法で自分の仕事を効率よく処理しようとするのが「優秀な人材」である．本システムは，WindowsのIEでWebアクセスできるパソコンさえあれば,暗号化された経路で,イントラネットのホームディレクトリを自宅等のパソコンから直接編集可能となる.

イントラネットにアクセスするプログラムもゲートウェイ･サーバからダウンロードする「プラグイン」形式のため,クライアントPCへのインストール作業が不要である．したがって，パソコンを持ち運ばなくてもHTTPS通信可能なパソコンを借りてUSBキーを挿すだけでイントラネットにアクセスできる.

出先からインターネットのWebサーバにアクセスできるように設定することくらいは，電話で説明することも可能である．SSL-VPNの本来の簡便性が生かせることになるといえる.

さらにUSBキーにはクライアント起動用プログラムしかなく，プラグインなどのシステム本体はゲートウェイ・サーバに集約されている．したがってシステムのバージョンアップはゲートウェイ・サーバだけの作業で済むという運用・管理面でのメリットもある.

6．実験システムによる評価

表１～２に示す２台の実験用クライアント機と，表３の諸元によるゲートウェイ･サーバ機を用いて実験用システムを構築し，動作環境の検証を行った。

表1　クライアント機A（FMV-BIBLO LOOX T70M/T）

ハードウェア	CPU：Pentium M753(1.20GHz) HDD：内蔵80GB メモリー：1.5GByte
ソフトウェア	OS：日本語版Windows XP(SP3) IE：ver6(SP3) Microsoft Office 2003
ネットワーク	家庭用ルータでベストエフォート100Mbps光インターネット接続. 宅内100Mbps有線LANと802.11g無線LANで接続. 他にイー・モバイルにてモバイル接続実験を行った.

表 2　クライアント機B（Let's Note CF-R3）

ハードウェア	CPU：Pentium M733(1.10GHz) HDD：内蔵40GB メモリー：768MByte
ソフトウェア	OS：日本語版Windows XP(SP2) IE：ver7 Microsoft Office 2003
ネットワーク	家庭用ルータでベストエフォート100Mbps光インターネット接続. 宅内100Mbps有線LANと802.11g無線LANで接続.

表 3　ゲートウェイ･サーバ機（PRIMERGY RX100 S4）

ハードウェア	CPU：Xeon3070(2.66GHz) HDD：73.4GB×2(内蔵RAID1) メモリー：2GByte
ソフトウェア	OS : RedHat Enterprise Linux ES Version 4 Webサーバ：Apache 2.2.2 DBサーバ：MySQL 5.0.21 アプリケーションサーバ：Tomcat 5.5
ネットワーク	GBEthernでセンター内の他サーバと接続.

	Netscreen204でMIPによるグローバルアドレス接続をし，HTTPとHTTPSのみを許可. インターネットとはベストエフォート100Mbpsで接続.

イントラネット内サーバとして，実稼動している表４～６に示す2台のファイルサーバと，グループウェアとしてWebメーラ用サーバを利用した．ファイルサーバ2台のうち1台はセンターに設置してあり，もう1台は地域イーサネット網を介した各拠点にあるファイルサーバを使用した．各拠点には一般ユーザ用と管理職員用の２つのLANセグメントがあり，各拠点のファイルサーバ(samba)は，管理職員用セグメントからのみファイル共有が可能と設定しているが，ゲートウェイ・サーバからのSMB通信を例外として許可した．イントラネットの構成を図3に示す．

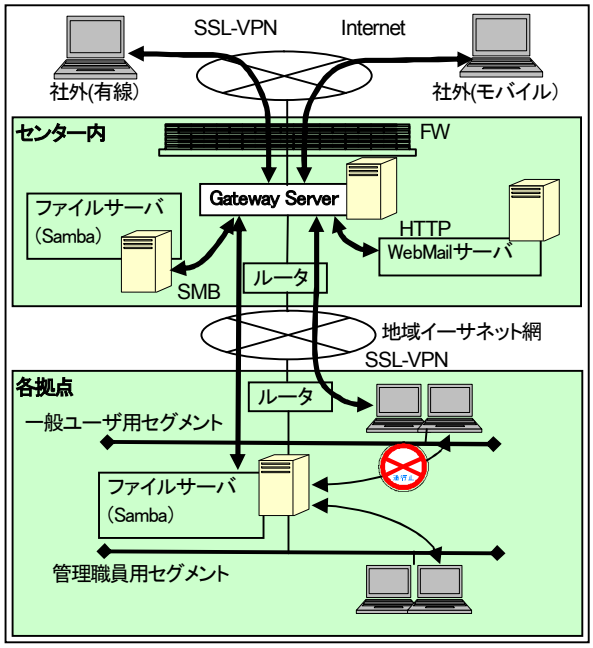

図 3　イントラネットの構成図

表 4　センター内ファイルサーバ（FMV-D5250）

ハードウェア	CPU：Celeron 420(1.60GHz) HDD：内蔵320GB，外付500GB メモリー：1GByte
ソフトウェア	OS：SiSBiC/NetBSD Version 1.4.5 Samba version 3.0.28a
ネットワーク	GBEthernで他のサーバと接続.

表 5　センター外ファイルサーバ（FMV-D5250）

ハードウェア	CPU：Celeron 420(1.60GHz) HDD：内蔵320GB，外付500GB メモリー：1GByte
ソフトウェア	OS：SiSBiC/NetBSD Version 1.4.5 Samba version 3.0.28a
ネットワーク	各拠点は地域イーサネット網と100Mbps, センターは同1Gbpsで接続.

表 6　Webメールサーバ（PRIMERGY RX300 S3）

ハードウェア	CPU：Xeon5110(1.60GHz) HDD：内蔵300GB×2(内蔵RAID1) メモリー：2GByte
ソフトウェア	OS：RedHat Enterprise Linux ES Version 4 WEBサーバ：Apache2
ネットワーク	GBEthernでセンター内他サーバと接続し，イントラネットクライアントからのみアクセス可能.

クライアント機A, Bを各拠点の一般ユーザ用セグメントからゲートウェイ・サーバに接続実験を行ったところ，持出し禁止データを安全に操作できる機能に問題は生じないことが確認された．このとき，実験用のUSBキーは，①センター内のファイルサーバ，②センター外のファイルサーバ，③Webメールサーバの3台に接続可能なビジネスドメインに所属させた．

さらに，この２台のクライアント機を外部から利用する実験も行った．センターと同じプロバイダではあるが別契約の2地点や，別のプロバイダ経由での接続実験（出張先の大学や，イー・モバイル経由）はもとより，USBキーを別のPCに取り付けて稼動することも確認した．

表 7　接続形態の違いによるアクセス時間の変化

単位：秒 (3回の平均)	ｹﾞｰﾄｳｪｲｻｰﾊﾞの接続まで	ﾛｸﾞｲﾝ認証	1.0MBのWordﾌｧｲﾙを表示するまで
K-Opti.com	１３	１３	１２
ｲｰ･ﾓﾊﾞｲﾙ	２２	３０	１９

ただし表7に示すとおり，D02HW(下り最大7.2Mbps)を用いてイー・モバイル網経由で接続した

場合は，認証するまでに時間がかかるだけでなく，プラグインのダウンロードにも時間がかかることが判明した．しかし，接続後のファイル閲覧や編集などファイルアクセス機能は有線ネットワークと同等の利用が可能であり，実用に耐えうる結果が得られた．

7．まとめ

特定の利用者のみにアクセスを許可するシステムでは，外部へのデータ持ち出しを禁止するという運用規定を設けているところが多い．しかしながら，現実には，何らかの方法で持ち出されている実態があり，それが原因となった個人情報の漏洩が社会問題となっている．

本論文では，既存の解決方法であるVPN接続方式にUSBキーを用いることでアクセス手順を簡便化し，さらに，データのアクセス方式に制限を加えることでデータの漏洩を防止できる新方式の提案を行い，プロトタイプシステムでの検証でその有効性を明らかにした．

提案したシステムは実験的にではあるが実稼動しており，現在①データの漏洩防止手順に見落としはないか，②利用者環境に依存する点の洗い出し，③一般利用者が個人所有機で利用する場面を想定した運用方法のチェックなどを行っている．

今後の本格運用に向けたテスト運用を継続しているところである．

謝　辞

本研究のプロトタイプ作成について，株式会社サスライト 内田 康弘氏には特別の配慮をいただいている．

本研究のフィールド実験への協力と併せて記して深謝したい．

参考文献

[1] 前橋市教育委員会学校教育課編，教職員の個人情報取扱の手引き，学陽書房，ISBN4-313-65142-X，2006

[2] 山崎文明，学校セキュリティの課題　－初等中等教育現場の情報セキュリティに関する課題と提言－，http://www.cec.or.jp/e2e/symp/kyotopdf/A06.pdf

[3] 社団法人日本教育工学振興会，平成１８年度文部科学省委託事業「校務情報化の現状と今後の在り方に関する研究」報告書，http://www.japet.or.jp/komuict/dl_report.html

[4] 株式会社バッファロー，USBメモリー セキュリティモデル，http://buffalo.jp/products/catalog/flash/usbflash.html#business

[5] イーディーコントライブ株式会社，SD-Shelter，http://www.safety-disclosure.jp/shelter/

[6] 総務省，平成17年版情報通信白書，http://www.microsoft.com/japan/forefront/edgesecurity/iag/default.mspx

[7] 株式会社三技協，PlatformV System，http://www.sangikyo.com/jp/products/info/platformv/index.html

[8] 株式会社ユーエスシー，シンクライアントOS「FKEY」，http://fkey.jp/

[9] Whale Communications，Intelligent Application Gateway (IAG) 2007の技術概要　テクノロジおよび機能の概要　ホワイト ペーパー，http://www.microsoft.com/japan/forefront/edgesecurity/iag/default.mspx，2007

[10] 株式会社サスライト，SASTIK III Thin-Client Layer アカデミック版, http://www.keyman.or.jp/3w/prd/57/10012457/

[11] 株式会社JMCエデュケーションズ，Hardlockey，http://edu.jmc.ne.jp/service/hardlockey/

[12] 特許公開番号：特開2004-151785，発明の名称：着脱式デバイス及びプログラムの起動方法，出願：2002年10月