

持ち帰り業務を支援する“マジックコネクト”

— 持ち帰るのはUSBキーだけ、全ての業務が自宅ができる —

NTTアイティ株式会社 取締役 一之瀬 進

ichinose.susumu@ntt-it.co.jp

<http://www.magicconnect.net/>

キーワード：情報漏洩、個人情報保護、インターネット、VPN、テレワーク、パソコン、PC

1. はじめに

教育業務ではパソコンが必須となっている。しかし、試験問題、生徒の成績、個人情報などの重要情報が教師の個人パソコンに入っていることが多い。このパソコンは、学校と自宅の間を往復しており、常に情報漏洩の危険にさらされている。ここでは、新技術により情報漏洩の危険性を低減させ、教師の持ち帰り業務を支援する新しいツールについて提案する。

2. 教育における情報保護の課題

2.1 情報漏洩の危険性

主に教育機関の経費不足により、教師は自費でパソコンを購入し、このパソコンで試験問題を作成して、生徒の成績を入力している場合が多い。個人用パソコンであるため、ファイル交換ソフトが入っていたり、ウイルス対策が不十分だったりして、情報漏洩の危険性が高い。また、学校と自宅の往復時に紛失、事故、犯罪に遭遇して情報が流出する可能性が高い。

2.2 課題

全教師に管理されたパソコンが支給されることが理想であるが、すぐには不可能である。そのため、個人のパソコンを利用した場合でも、情報漏洩の危険がなく安全に業務が遂行できるツールの提供が大きな課題である。

3. 安全なテレワークの提案

3.1 テレワークツールの必要条件

自宅などの学校外で、個人所有のパソコンを使用して、業務を安全に遂行できることが重要な必要条件である。このような必要条件を満たすシステムとして、サーバベースコンピューティング（SBC）システムとVPNを組み合わせたシステムが従来より存在するが、大規模で高価であるため、小規模から開始でき、かつ安価であることが必要条件である。また、導入に際して、ネットワーク機器の設定変更が容易なこと、使用方法が簡単なことなどが必要条件である。

3.2 マジックコネクトの提案

マジックコネクトは、学内のSBCサーバや自席パソコンの画面を手元のパソコンに転送する方式であり、手元のパソコンにはファイルが保存されないため、情報流出の可能性は極めて低い。また、個人所有のパソコンを利用した場合に、ウイルスチェック機能が正確に動作していない場合は使用できないようにしてあるため、安全に学校外で業務を遂行することができる。

使用方法は極めて簡単である。教師は、特別なUSBキーを任意のパソコンに指すだけですぐに業務を始めることが可能となる。このUSBキーには個人対応に固有のIDが入っており、このUSBキーを持っていないと自分のアカウントにログオン出来ない構成となっている。ID、パスワードだけでログオンできる他の方式に比較して、安全性は極めて高い。

システム購入に高額な費用が必要な従来のVPNに対して、マジックコネクトはASPサービス（システムを購入せず、使用料のみでサービスの提供を受ける方式）で提供しているため、安価に1アカウントからのスモールスタートが可能である。（ASPサービス以外にシステムでの提供も可能。）

インターネットのWebサーバが閲覧できる環境であれば、ネットワーク機器の設定変更は不要であるため、導入に際してほとんど手間がかからないことが大きな特徴である。

図1にマジックコネクトの使用例を示す。従来は個人のパソコンを持って移動していたため、パソコンの紛失、事故、盗難などによる情報漏洩の危険があった。マジックコネクトは、USBキーだけを持って移動するため、移動時に情報が漏洩する危険性がない。ファイルが学校外に流出しないため、安心して業務を遂行することが可能となり、業務の生産性が向上する。

4. まとめ

情報漏洩を防止する手段として、モラル、プロセス、技術の3点が重要である。しかし、モラル、プロセスは、個人の資質に依存し、徹底させることは極めて難しい。しかし、高速広帯域ネットワークの発展、セキュリティ技術の進歩により、情報の流出を技術的に防止することが可能となってきた。ここで紹介したマジックコネクトなどの新技術を教育業務に展開することにより、より豊かな教育環境が実現できると考える。

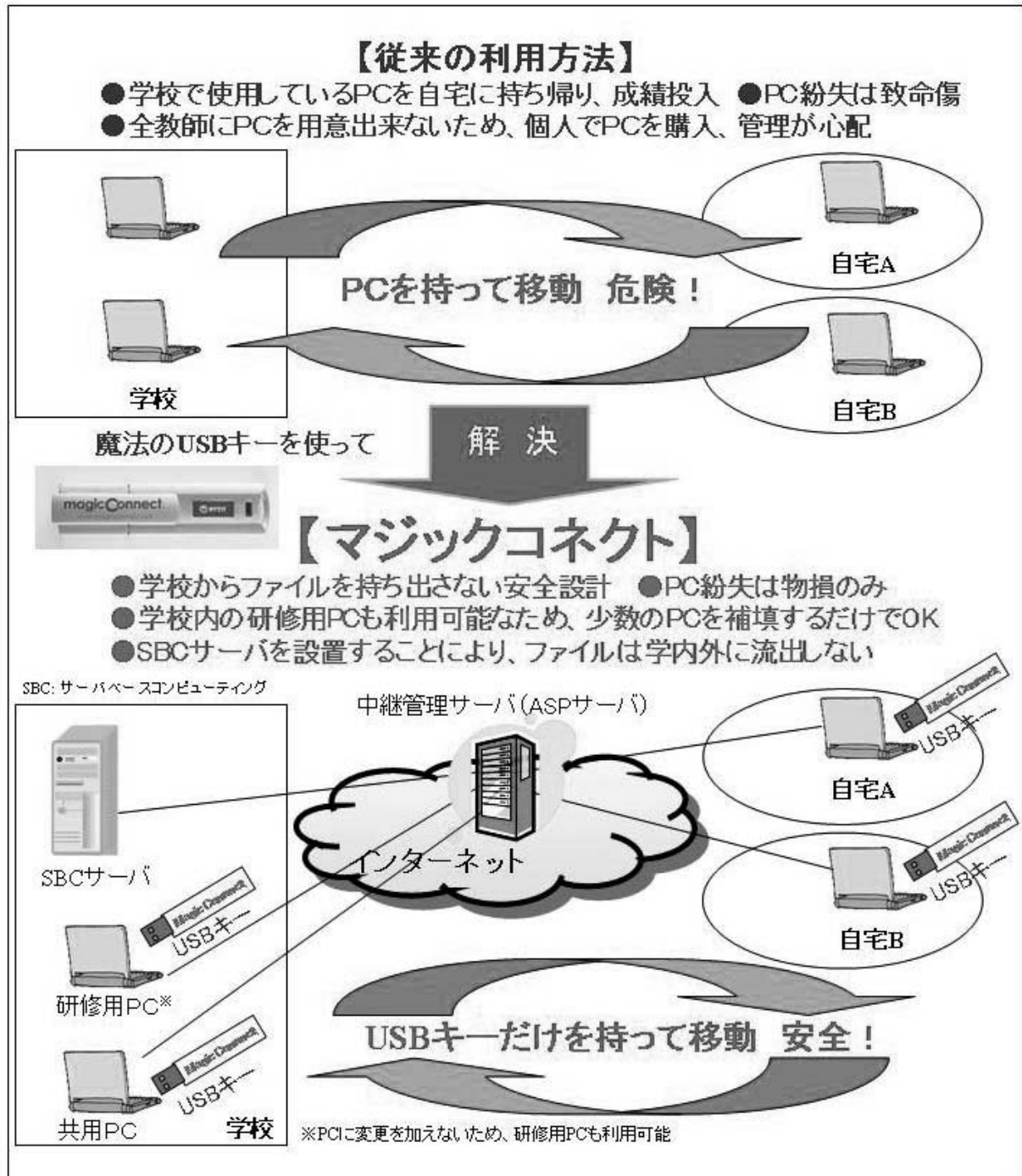


図1 持ち帰り業務を支援するマジックコネクトの利用例