セキュリティを確保した社外・モバイル利用システムを４割以上コスト削減して実現

～出張時だけでなく大規模災害・パンデミックにも対応できるシステムを安価に構築～

株式会社　四国総合研究所

■ 執筆者Ｐｒｏｆｉｌｅ ■

白方　博教

2012 年　株式会社 四国総合研究所　入社
2014 年　現在　電子技術部長

■ 論文要旨 ■

四国総合研究所では、日常業務で使用するグループウェアやファイル共用サーバなどを、出張時に利用するためや研究開発アイデア発想時、大規模災害・パンデミック発生時の対応を自宅など社外で行うための、社外・モバイル利用システムをセキュリティを確保して安価に構築した。

従来はハードディスク暗号化などの対策を行った持出専用パソコンを利用していたが、パソコンにデータを保管する限り、万一の紛失や盗難時に情報漏えいの恐れをなくすことはできない。

近年、LTE や無線 LAN はじめ高速ネットワークが整備され、パソコンに一切のデータを置かないシンクライアントの利用が可能となった。

一般的なシンクライアントは投資が大きいため、利用アプリケーションは限定されるが安価に構築でき使用するパソコンなどにデータを残さない仮想シンクライアントを活用してシステムを構築した。従来に比べ、セキュリティを確保し年間４割以上のコスト削減を実現している。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

四国総合研究所は、四国における技術開発推進の中核的存在を目指し、四国電力株式会社の研究所を母体として、昭和 62 年 10 月に設立され、今年で 27 年目を迎える従業員百数十名の企業である。

設立以来、電力やエネルギーの分野はもとより、バイオ、環境、エレクトロニクス、情報・通信、土木・地質などの分野に至るまで多岐にわたった研究活動を行っている。これらの幅広い分野で培ってきた技術やノウハウを活かし、電気事業の経営効率化に役立つ研究開発に加え、広く地域の皆様方から調査・研究・開発業務を受託するとともに、研究開発から生まれた成果品の販売などを行っている。最近話題となっている水素社会に向けては、水素火炎可視化装置、ガス濃度遠隔計測装置などを開発している。また、四国の民間研究開発機関として、大学・自治体・地元企業との共同研究などを通じて、地域社会の振興発展に役立つ研究開発にも取り組んでいる。

１．２　システム開発の経緯

四国電力グループでは、情報セキュリティリスク増大への対応、利用するパソコン OS である WindowsXP のサポート終了を契機にグループ全体で情報セキュリティ強化を目指したシステム基盤整備を行うこととした。当社でも WindowsXP のサポート終了にあわせて、パソコン取替えを行うとともに、社内システムの整備、あわせて、出張時モバイルなどの対象システムの変更などを行う必要があった。

システムの構築に当たっては、大規模地震の 30 年以内の発生確率が 70%程度と予測されている南海トラフ地震、最近多くなっている異常気象などによる局所的な集中豪雨などをはじめとする大規模災害、新型ウィルスなどの大規模流行などに対する対策も必要となっている。また、電気料金改定に伴う親会社からの受託研究費の大幅削減などに対応するため、できるだけ安価に、既存システムよりコスト削減することが求められている。

今回、これらに対応するために、出張時モバイル利用などの日常業務の効率化に対応するだけでなく、大規模災害・パンデミックなどの緊急事態発生時にも対応できる、セキュリティを確保した、従来システムより４割以上コスト削減した社外・モバイル利用システムを構築した。

２．従来の出張時モバイルシステム

２．１　出張時モバイルシステムの状況

平成 20 年以前に構築した出張時モバイルシステムは、情報セキュリティを確保するために、社内で利用するパソコンとは別に特別に対策を実施した、社外持出専用パソコンを利用することとしていた。社外持出専用パソコンは、社内利用パソコンで実施しているウィルス対策などに加えて、万一のパソコンの紛失・盗難などに備えてハードディスク暗号化をはじめ各種のセキュリティ対策を実施していた。

出張時などの社外で利用するシステムとしては、電子メールの送受信、社内資料の閲

覧・作成などのシステムである。本来は、社外においても、社内と同様にセキュリティを確保して、ネットワークを介して、グループウェアやファイル共用サーバ、社内業務システムを活用することが行いたい。しかし、大きくは２つの問題があった。システム構築・運用コストの問題、低速なネットワーク環境の問題であり、セキュリティリスクはあるが、現実的な解決策として社外持出専用パソコンを利用する形で対応していた。従来システムの概要を**図１**に示す。

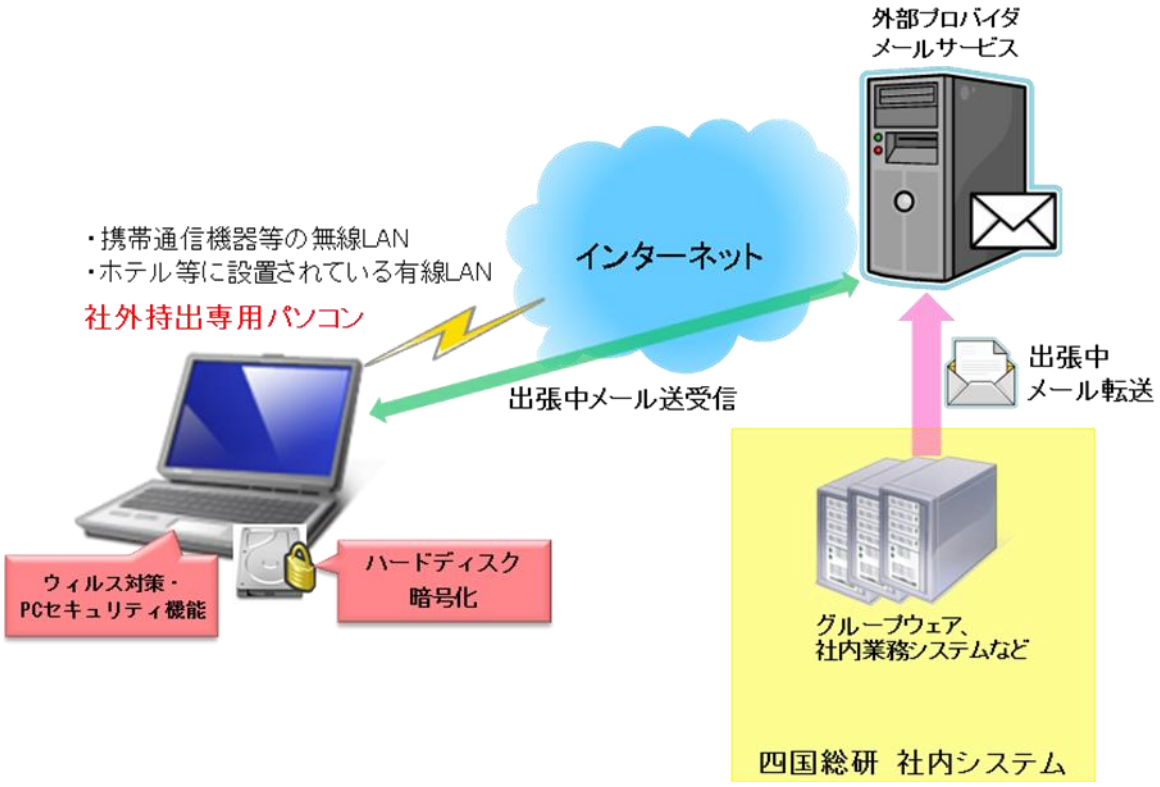

図１　従来の出張時モバイルシステムのシステム概要

社外からセキュリティを確保して社内システムにアクセスするためのシステム構築・運用には多くの費用がかかる。当社では、出張などでの利用者が比較的少ないこと、簡単な対策で社外アクセスを許容すると外部からの侵入リスクが大きくなり、全社のシステムにリスクが発生することなどから、次のように対応した。機会の少ない出張時など社外での利用におけるメール送受信や社内資料の閲覧・作成などのリスクを許容することとして、メール送受信を社外プロバイダに転送することで利用し、社内資料の閲覧・作成などに関しては暗号化したハードディスクの中にデータを保管して利用していた。

ネットワーク環境としては、ホテルなどや外部事業所などの建物内であれば、高速インターネットなどが整備されていたので、社内システムにセキュリティを確保してアクセスできる環境があれば、持ち出すパソコンなどにデータを保管しなくてもネットワークを経由して、社内システムを利用することができた。当時、四国など地方では建物外では、ネットワーク環境が十分に整備されていなかったため、ネットワークを介して社内システムにアクセスすることは困難であり、パソコンにデータを保管しておくことが必要であった。

２．２　出張時モバイルシステムの課題

従来の出張時モバイルシステムには、パソコンにデータを保管しているため、社外持出専用パソコンが万一紛失、盗難した場合に情報漏えいのリスクがあり、外部プロバイダにメールを転送するための情報漏えいリスクもある。

この課題を解決して、情報漏えいリスクをほとんどゼロとするには、パソコンにデータを一切保管しない、シンクライアントシステムを利用する方法がある。しかし、当時は全国でも、特に四国内のモバイルネットワークは貧弱であり、モバイルで高速通信回線を利用することが困難であった。また、シンクライアントシステムのシステム構築コストが非常に高価であった。

２．３　他社システムの状況

グループ会社では社外から社内ネットワークに対して仮想専用線接続を行い、グループウェアシステムなどにアクセスして、メールの送受信、スケジュールや掲示板などの確認などを実施していた。システム構成例を図２に示す。

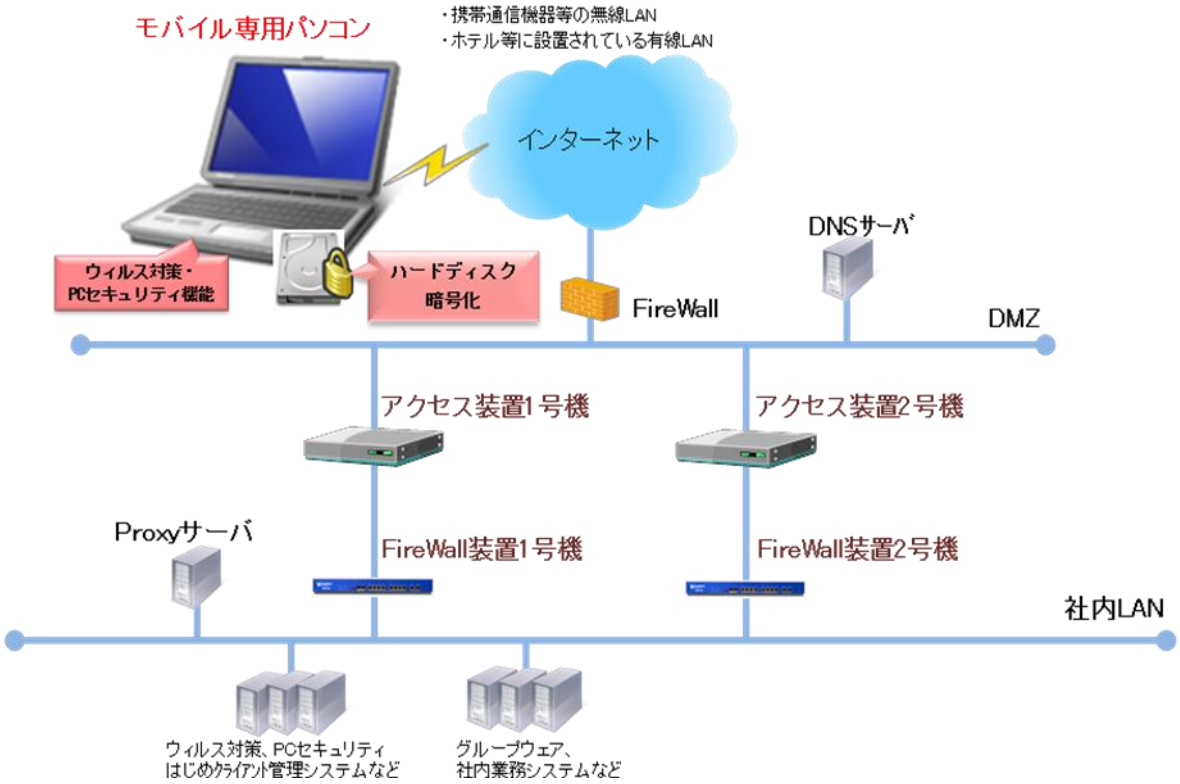

図２　グループ会社などでの出張時モバイルシステムのシステム構成例

グループ会社では、セキュリティを確保するため、システム構成面のハード対策だけでなく、出張期間ごとのパスワードの設定変更、返却の都度、ウィルスパターン更新はじめ必要なソフトのアップデートなど運用面の対策も実施していた。

しかし、利用に際してモバイル専用パソコンにデータを保管することになるので、パソコンが万一紛失、盗難した場合には、ハードディスクを暗号化しているとはいえ、情報漏えいリスクをゼロにすることはできない。

３．新たなニーズや課題への対応

３．１　新たなニーズや課題

新規に社外・モバイル利用システムの構築を考える場合には、社会環境の変化などから、出張時だけでない新たなニーズや課題に対応する必要があると考えられた。

一つは、研究開発など業務の効率化である。研究開発はスピードアップが求められており、いかに速く研究開発成果があげられるかが、成功への大きな要因である。このためには研究員がいかに効率よく研究開発できるかが鍵となる。研究開発のアイデアやヒントなどが思い浮かぶことなどは、時間や場所を問わず、いつ出てくるかわからない。思いついたところで研究資料など参考となる資料が参照できれば、非常に効率的となる。このためのシステム環境としては、出張時モバイル利用と同様に、自宅や外出先などにおいて、いつでもどこでも、グループウェアやファイル共用サーバ、社内業務システムなどが利用できればよいことになる。

もう一つが、大規模災害・パンデミックなどの緊急事態発生時への対応である。大規模災害・パンデミック発生の際には、会社に出社できない状況が発生することが考えられる。この場合に備えて、会社以外の自宅などにおいても、ある程度の必要な業務が実施できるようにしておくことが求められる。

３．２　新たなニーズや課題に対応するためのシステム要件

これらの対応に当たってシステム負荷を考えた場合、研究開発など業務の効率化のためのアイデア発想時の対応など通常時は、出張時モバイルと同じ程度の利用頻度であり、同時アクセス数は高くはない。しかし、大規模災害・パンデミックなど緊急事態発生時には、同時期の利用対象が非常に多数となる。利用対象の多くが同時にアクセスすることとなるので、それに対応できるシステムとする必要がある。概要を図３に示す。

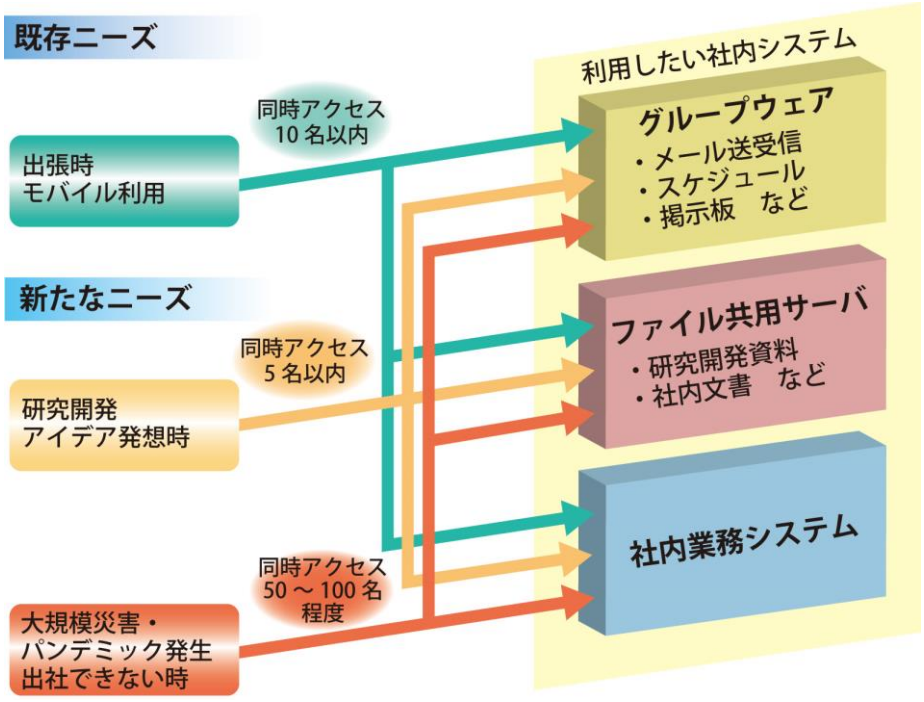

図３　新たなニーズや課題への対応とシステム要件

当然、これらの社外利用においては、出張時モバイル利用と同じく、情報漏えいリスクがないようにしなくてはいけない。

４．システム実現方法の検討

４．１　求められる要件とシステム実現方法

セキュリティ確保の上での問題は次のとおりである。ネットワークを介して利用している場合は仮想専用線を利用するなど暗号化通信が行われており、情報漏えいの問題は基本的に大丈夫である。パソコンにデータが保管されていれば、パソコンが万一紛失したり、盗難にあったりすることで、ハードディスクが暗号化されているとは言え、どうしても情報漏えいの問題が生ずる。つまり、パソコンにデータが一切保管されていなければ、基本的に問題が無くなる。

「情報漏えいリスクをなくす」観点からは、社外で利用するパソコンに一切のデータを保管せず、社内システムとの通信が仮想専用線などの暗号化通信などでセキュリティが確保できていることである。このためには、端末側にデータを保管しないシンクライアントシステムが有効である。

４．２　システム実現方法の課題

このシステムを実現するための課題は、従来のシステム構築を考えたときから変わっておらず、システム構築・運用コストとネットワークの問題である。概要を図４に示す。

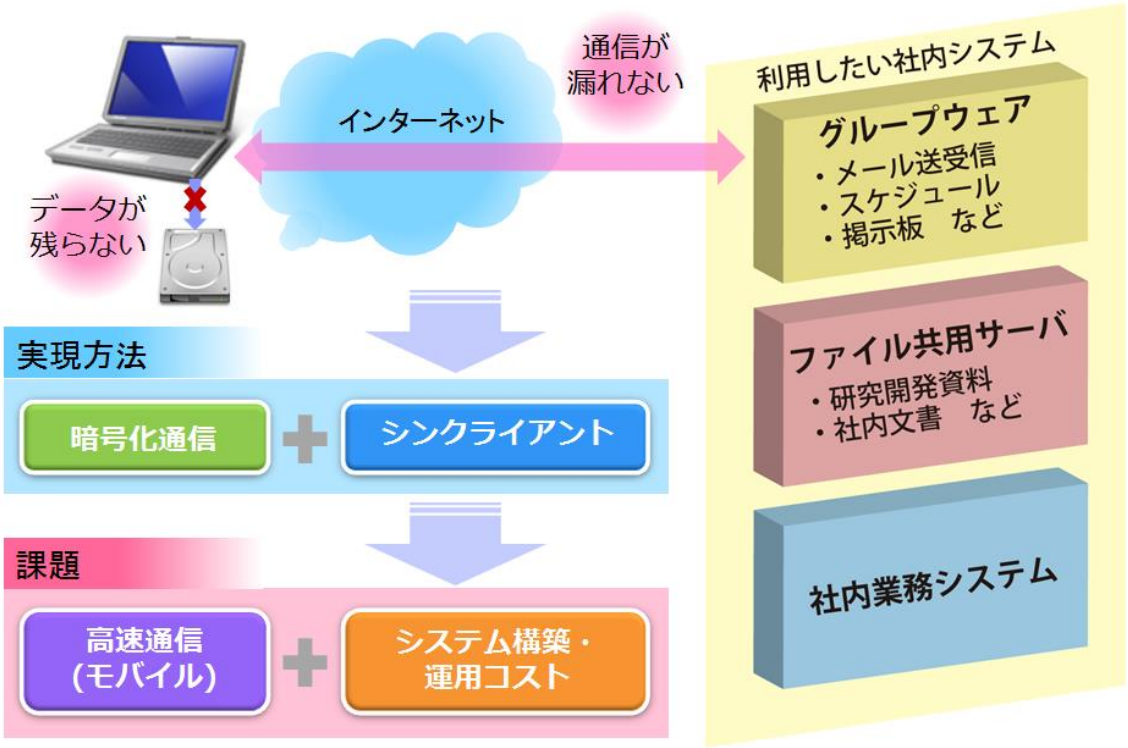

図４　システム実現方法と課題

まず、システム構築・運用コストである。シンクライアントシステムは社外持出専用パソコンを購入するのに比較して、センター側でデータ処理を行いデータ保管を行うために、サーバなどの設備が必要であり、ネットワークを介して実行するため、ローカル処理するよりも高速な処理能力が必要となるなど、大幅にシステム構築・運用コストがかかる。

出張時モバイル、通常時の研究開発アイデア発想時の対応などに関しては、同時アクセス数が多くないので、システム構築コストが大きくなるとしても、シンクライアントシステムでの対応でも可能である。しかし、利用対象者が多くなると、マイクロソフトのライセンス費用などソフトウェアコストをはじめとする運用コストの増大が問題となってくる。

それ以上に、大規模災害・パンデミックなど緊急事態発生時の対応では、同時アクセス数が急激に増大することになり、それに対応できるだけのシンクライアントシステムのサーバを準備しておくことは膨大なコストとなる。これは当社のような中小企業にとっては不可能に近く、実質的に無理であり、何らか別の対策をとることが必要である。

次にネットワークの問題である。自宅や外部事業所、出張時のホテルなどなどの建物内であれば、光インターネットなどが以前から普及して高速ネットワーク環境が既に整備されており問題はない。しかし、建物外で利用できるのは携帯電話回線などによるモバイルネットワークしかない。平成 20 年代初めでは、全国でも大都市圏は別にすると、四国などの地方都市においてはモバイルネットワークが貧弱であり、モバイルで高速通信回線を利用することは困難であった。

４．３　ネットワーク環境の変化

平成 20 年代半ばとなり、WiFi、LTE などにより高速のモバイルネットワーク環境が急速に整備されてきた。新幹線や航空機の中においても高速の無線 LAN が利用できるようになり、LTE によって室外などにおいても、数十 Mbps という高速ネットワークが利用できるようになってきた。このように、四国などの地方都市においても、社外から社内システムにアクセスして利用することができる高速なモバイルネットワーク環境が整備されてきた。

社外において、高速なネットワークが利用できるようになれば、シンクライアントシステムを活用して、パソコンにデータなどを保管することなく、高速ネットワークを介して仮想通信線などの暗号化通信方式を用いて社内システムにアクセスすることで、セキュリティを確保した利用が可能となる。これにより、ネットワークの問題は解決できる。

４．４　シンクライアントシステムの方式

残る問題は、システム構築・運用コストである。このため、シンクライアントシステムの構築・運用を安価に実現する方法はないのか、更に検討を進めた。

シンクライアントシステムは、様々な実装方式があり、また、新たな実装方式が次々と考案されている。代表的なシンクライアントの実装方式として、一般的には大きく３つの方式、ネットワークブート方式、サーバベース方式、ブレード PC 方式・仮想 PC 方式がある。

なお、サーバベース方式、ブレード PC 方式・仮想 PC 方式は処理方法から「画面転送方式」ともいう。各方式のシステム概要を**図５**に示す。

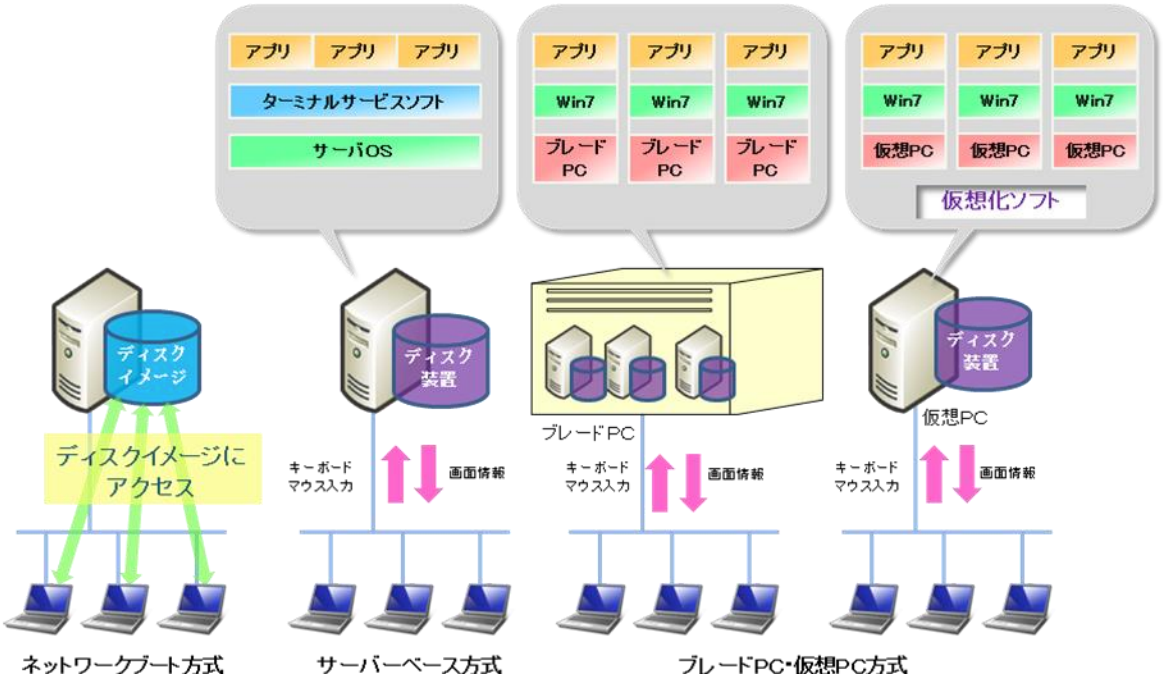

図５　シンクライアントシステムの方式によるシステム構成比較

（1）ネットワークブート方式

サーバ側のディスク装置に OS イメージをおき、端末起動時にはネットワーク経由で OS をブートする方式である。アプリケーションの処理は端末側で行う。一般的に、Linux や MacOS などの Unix 系の OS が使われることが多いが Windows をベースとしたネットワークブート方式のシステムもある。

画面転送方式と異なり、アプリケーションの処理を端末側で行うため、アプリケーションの互換性の問題が発生しにくいことが利点である。しかし、端末起動時にアプリケーションを含めた OS イメージ全体がネットワークを流れるため、ネットワークへの負荷が大きいことが問題となることが多い。端末上のアプリケーションで作成したデータはサーバ側にあるファイルサーバに保存される。

構内 LAN など高速のネットワークがあることが前提の方式であり、今回、検討している社外・モバイル利用システムでは適用することはできない。

（2）サーバベース方式

アプリケーションの実行などすべての処理をサーバ側で行い、端末側は操作端末としての役割だけを担う方式である。サーバから端末には画面情報が転送され、端末からサーバへはキーボードやマウスの入力情報が転送される。1 台のサーバに複数のユーザーが同時ログオンして使用するために、マルチユーザー対応していない Windows アプリケーションの互換性やライセンス面での問題が課題である。近年はマルチユーザー対応したアプリケーションなどが提供され技術的課題は解消されつつあるが、ライセンス面での問題は難しい。

（3）ブレード PC 方式・仮想 PC 方式

ブレード PC 方式は、サーバベース方式でのサーバと端末の通信方式はそのままに、すべての処理をサーバ側にあるブレード PC で行う方式である。ブレード PC 上では

Windows などのクライアント OS を動作させることで、サーバベース方式で課題となっていた Windows アプリケーションの互換性の課題を解決することができる。一方で専用のブレード PC を利用するため、今まで「パソコン」だけのコストが、ハードウェアとしては「比較的高価なブレードサーバ」+「端末」となり、ウィルス対策などはクライアント OS ごとに必要となるなど、システム全体の価格が高くなる。

仮想 PC 方式は、高性能サーバ上で VMWare、Xen などのハイパバイザーを使用して仮想マシンを多数実行することにより機能集約を実現する方式である。ブレード PC 方式ではハードウェアであるブレード PC で行うところを、ハイパーバイザーによる仮想マシンというソフトウェアで行うものである。ユーザーは個々の仮想マシンに接続してシングルユーザーのクライアント OS を使用する。サーバやネットワークなどの機能や性能の向上により、大手企業をはじめ多くの企業で利用が進んでいる。

４．５　シンクライアントシステムの詳細調査

このシンクライアントシステムのシステム構築・運用コストが大きな課題である。一般的には、センター中心のサーバ型のシンクライアントシステム、具体的には、サーバベース方式、ブレード PC 方式・仮想 PC 方式でシステムを構築した場合、１ユーザー当たりのコスト、すなわち、パソコン導入であれば１台あたりのコストの方がはるかに安価であると言われている。当社のような中小企業では、出張時モバイルや研究開発アイデア発想時の対応などの通常時のシンクライアントシステム構築・運用のコスト負担も困難であり、ましてや、いつ発生するかわからない大規模災害・パンデミックなどの緊急事態発生時に対応するためのコスト負担に対して、経営トップの理解を得ることは非常に難しい。

しかし、セキュリティを確保したシステムを構築するためには、シンクライアントシステムは有効である。そこで、シンクライアントシステムについて、課題を解決する何らかの方法・対策がないか、詳細に調査・検討を実施した。

当社で社外で利用するためのシステムを考えた場合、社内で使用しているすべてのシステムを利用する必要はない。利用するのは、グループウェアやファイル共用サーバ、社内業務システムなどである。求められる要件は、情報漏えいリスクを無くし、出張時のモバイル、自宅などの社外から安全にグループウェアやファイル共用サーバ、社内業務システムなどの社内システムが利用できることである。つまり、グループウェアや社内業務システムは基本的に Web システムであり、アプリケーションとしては Web ブラウザとファイル共用サーバアクセス、資料などの閲覧・作成などを行うオフィスソフトが利用できればよいことになる。

この利用方法を前提に、シンクライアントシステムを調査すると、前述の３方式のほかに、機能限定、利用できるアプリケーションに制限はあるものの「仮想シンクライアント」という方式があることがわかった。詳細に調査すると、仮想シンクライアント方式では、利用できるアプリケーションが限定されるものの、処理するための OS やプログラム、処理能力などは端末側の資源を利用し、パソコンのハードディスクなどには一切データを保存することがないというものである。利用できるアプリケーションとして、Web ブラウザとファイルサーバアクセスやオフィスソフトは、ほとんどの仮想シンクライアント方式のシステムで利用できる。

社外・モバイル利用のシステムに適用できる前述したサーバベース方式、ブレード PC・

仮想 PC 方式などの方式は、センター側のサーバの資源を利用しているのに対して、この仮想シンクライアント方式は端末側の既存パソコンのハード・ソフトを利用するために、コスト面で大きなメリットがある。新たに必要となるハード・ソフトが少ないということである。デメリットは、利用できるアプリケーションに制限があるということであるが、利用できるアプリケーションとして、当社で必要とする Web ブラウザ、ファイルサーバアクセス、オフィスソフトなどはある。

当社で考えれば、出張時モバイルや研究開発アイデア発想時の対応、大規模災害・パンデミックなどの緊急事態発生時の対応において、必要なものは、グループウェアやファイル共用サーバ、社内業務システムなどの社内システムが利用できることである。当社としては、仮想シンクライアントのデメリットである利用できるアプリケーションに制限があるということは特別に問題にならないことになる。

したがって、「仮想シンクライアント方式」を活用することで、システム構築・運用コストの問題が解決できる。

５．新たな社外・モバイル利用システムの構築

５．１　仮想シンクライアント方式

上述の詳細調査・検討の結果、当社での社外・モバイル利用システムにおけるシンクライアントシステム適用の課題を解決できる方式として、仮想シンクライアント方式があることがわかった。この仮想シンクライアント方式のシステム構成の概要を図６に示す。

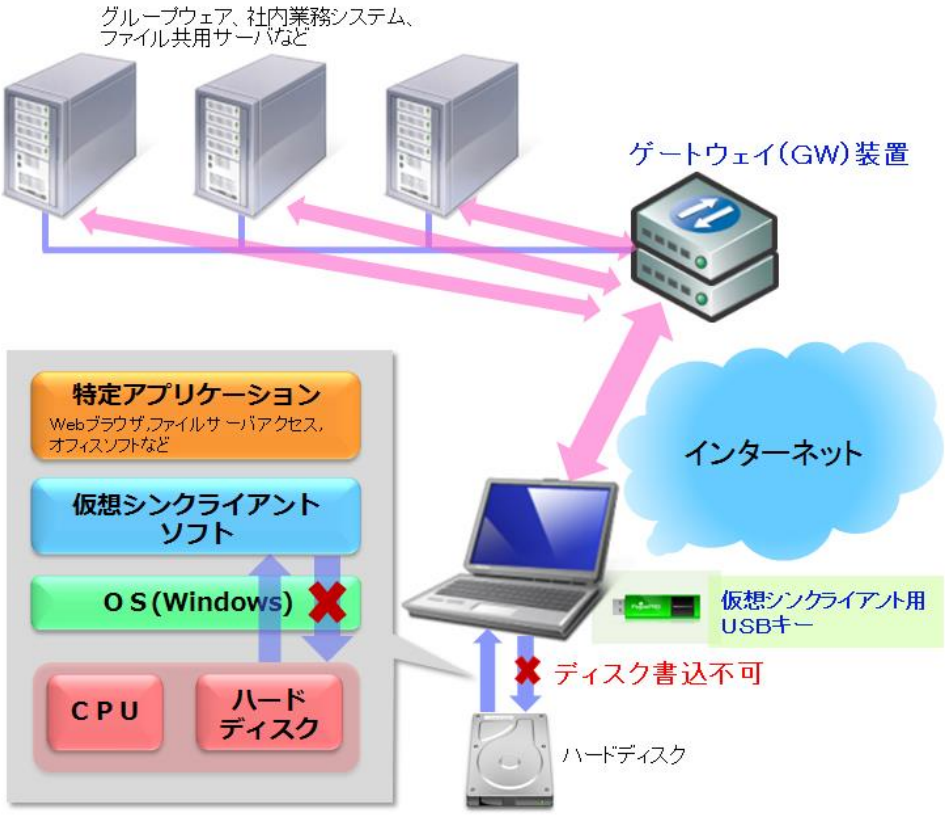

図６　仮想シンクライアント方式のシステム構成

仮想シンクライアント方式の構成や機能を説明する。仮想シンクライアント方式は確立されたものではなく、実装の詳細は提供するベンダーにより異なる点があるが、概ね次のとおりである。仮想シンクライアント方式のシステムは、**図６**に示すように端末側のパソコンを仮想的にシンクライアントとして動作させるソフトウェアとそれと連動するセンター側のゲートウェイ装置で構成する。端末側のパソコンで動作する仮想シンクライアントソフトはパソコンに専用ソフトウェアを導入するもの、USBキーなどを差込み起動するものなどがある。連動するセンター側のゲートウェイ装置は安価な専用サーバやSSL-VPN装置などで構成する。

端末側のパソコンで仮想シンクライアントソフトが動作すると、端末側のパソコンに、一時的な作業レイヤーができ、この作業レイヤーでパソコン内に導入済みの特定アプリケーション、具体的にはWebブラウザやオフィスソフトなどが動作する。この作業レイヤーでは、パソコンのハードディスクや入出力機器などへのアクセスは仮想シンクライアントソフトの管理下にあり、ハードディスクへの書込みは禁止であり、プリンタ印刷などは禁止・許可を制御できる。端末側の仮想シンクライアントソフトやWebブラウザなどとセンター側のゲートウェイ装置が連動することにより、センター側にある社内業務システムやファイル共用サーバへのアクセスが実施される。仮想シンクライアントを終了させると、一時的な作業レイヤーが消滅し、ハードディスクへの書込みは禁止されているので、端末側のパソコンには情報が残らないことになる。

利用するアプリケーションであるWebブラウザやオフィスソフトなどは、端末側のパソコンのCPU、メモリ、導入ソフトなどの資源を利用するため、センター側では処理は少なく処理能力の高い高価なサーバなどは必要がない。一方、端末側のパソコンで動作するアプリケーションは、仮想シンクライアントソフトの管理下で一時的な作業レイヤーで動作するため、特定のアプリケーションに限定されることになる。

５．２　仮想シンクライアント方式によるシステム構築

新たな投資を少なくできること、既存の機器が利用できることから、安価にシステム構築・運用できる仮想シンクライアント方式を活用した、社外・モバイル利用システムを構築した。

仮想シンクライアント方式に該当するシステムは、複数のベンダーから各種のシステムが提供されている。端末側で利用する既存のパソコンに仮想シンクライアントを実現する方法に関しては、既存のパソコンに専用ソフトウェアを導入するもの、既存のパソコンにUSB キーなどを差し込み起動するものなどがある。

当社での利用を考えると、出張時での利用や研究開発アイデア発想時や大規模災害・パンデミックなど緊急事態発生時の自宅利用などいろいろな場面で利用することから、持ち運びに便利なことが求められる条件となる。このことから、仮想シンクライアントを実現するものとして、小さなUSB キーなどを持ち運び、既存のパソコンなどに差し込むことで利用できるものが適していると考えられる。

当社の利用で有望と思われるシステムに関して試行を行い、機能確認を実施した。これらのシステムはシステム構成などに若干の差異はあるものの、

・仮想シンクライアントをUSB キーを利用して起動する
・利用するパソコンのハードディスクなどには一切データを保管しない

・Web ブラウザ、ファイルサーバアクセス、オフィスソフトなどのアプリケーションは利用できる

というものである。試行した結果、複数のシステムは当社利用において活用できると判断した。

当社に導入するシステムを決定するため、これら複数のシステムに対して競争見積を行い、システム構築、その後の運用・保守も含めた５年間の合計費用でコスト比較して、最も安価なシステムを採用した。採用したシステムを用いたシステム構成を図７に示す。

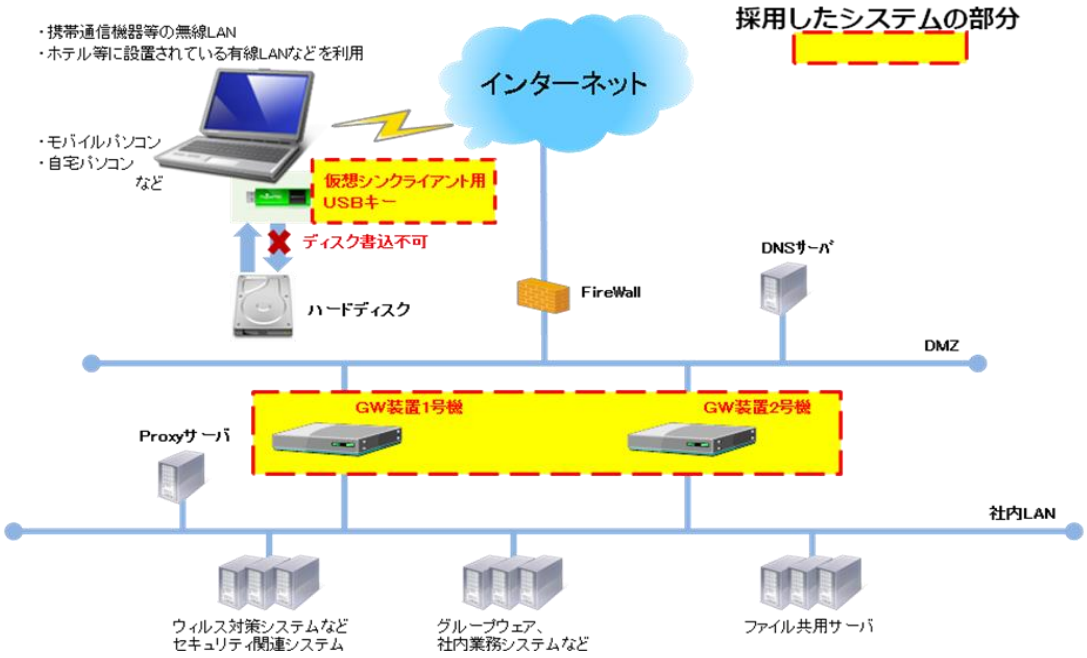

図７　構築した仮想シンクライアント方式のシステム構成

５．３　セキュリティ対策の概要

社外・モバイル利用システムにおいては、しっかりしたセキュリティ対策を行い、情報漏えいリスクがないようにしておく必要がある。仮想シンクライアント方式を利用したシステムでは、社内システムとの通信には暗号化通信を行うことで、通信回線上での漏えいを防止し、使用するパソコンのハードディスクなどに一切のデータを保管しないことで、パソコンの万一の紛失、盗難時にパソコンからの情報漏えいを防止している。

仮想シンクライアント方式を利用したシステムを正規に利用する場合は、原理的に情報漏えい防止の対策はできているが、専用 USB キーの紛失、盗難などにより不正使用される場合などを防止する対策が必要である。このために追加しているセキュリティ対策の一部を説明する。

まず、専用 USB キーが不正使用されることを防ぐため、

・専用 USB キーは業務上必要な者だけが利用できるよう、上長許可による貸与申請に基づき使用期間期限付きの社外利用登録を行い、利用者に貸与する
・専用 USB キーの利用者認証として、８文字以上など最低文字数制限や３種類以上など最低文字種制限のついた Pin コード入力を必要とする

などを実施している。

専用 USB キーが不正使用されたり、専用 USB キーに暗号化して格納している外部ネットワーク接続情報が万一漏洩することなどによる外部ネットワークからの不正アクセスを防止するために、ワンタイムパスワードを使用している。社外・モバイル利用では、インターネットからのアクセスを許可する必要があり、どのネットワークから接続されるかなど、利用するネットワークの IP アドレスに制限をかけることはできない。このため、専用 USB キーの利用者ごとにメールアドレスが物理的な機器と紐付けされている携帯電話用のメールアドレスの登録を行い、接続時点ではワンタイムパスワードを送付することで利用者の確認を行うなど、セキュリティ強化をはかっている。

５．４　システム利用イメージ

社外・モバイル利用システムの利用イメージは次のとおりである。

①利用するパソコンに仮想シンクライアント専用 USB キーを差し込み、仮想シンクライアントを起動する。

②利用者認証のための Pin コードを入力する。

③しばらくすると、画面右下に利用するためのメニューが表示される。（**図８**参照）

④画面右下のメニューから接続先を選択し、クリックする。（**図８上部**参照）

⑤ブラウザが立ち上がり、「社外アクセス仮想オフィスへようこそ」の画面が表示され、自動的にログインが実行される。（**図９**参照）

⑥仮パスワードを送信したことを示す「社外アクセス仮想オフィスへようこそ」のワンタイムパスワード入力画面が表示される。（**図 10** 参照）

⑦ワンタイムパスワードを入力すると「社外アクセス仮想オフィスへようこそ」のメニュー画面が表示され、「サイボウズ（グループウェア）」、「Web 検索」、「ファイル共有」があるので、利用するものをクリックする。（**図 11** 参照）

⑧終了する場合は、「社外アクセス仮想オフィスへようこそ」のメニュー画面の右上にある「ログアウト」をクリックすると、接続が切断され、ブラウザが消える。

⑨画面右下のメニューの「終了・取り出し」をクリックすると、ログオフされるので、ログオフされたら専用 USB キーを取り出す。

アクセス先を選択する時 ⇒

図８　利用メニュー画面

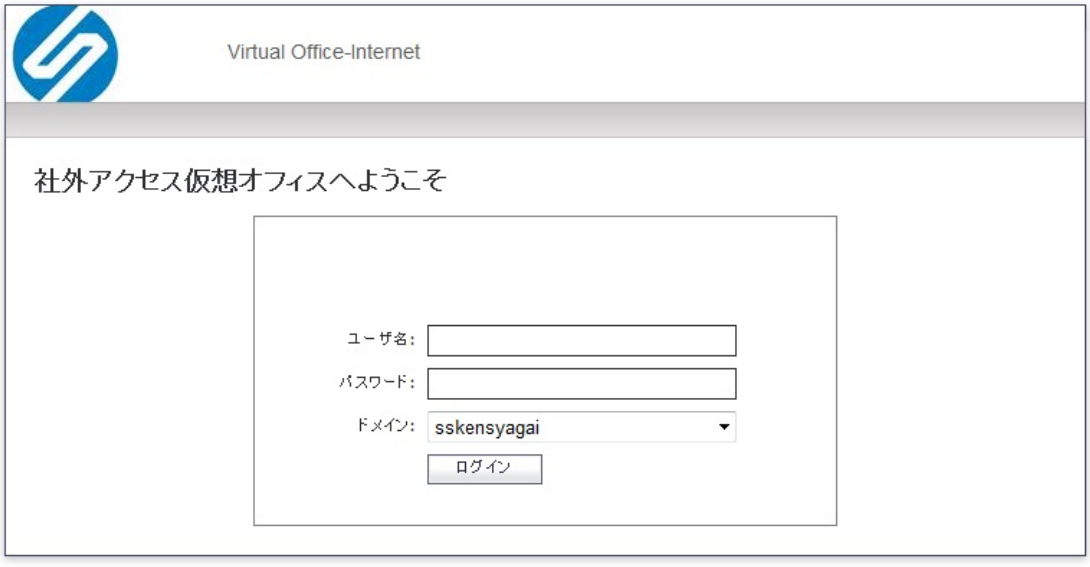

図９　「社外アクセス仮想オフィスへようこそ」の画面

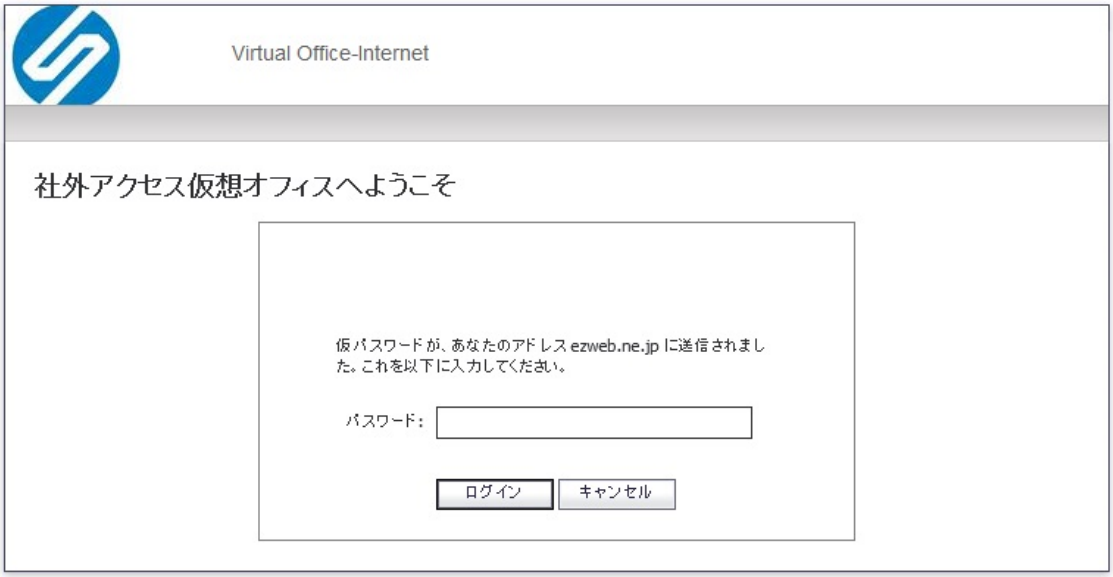

図 10　ワンタイムパスワード入力画面

図 11　「社外アクセス仮想オフィスへようこそ」のメニュー画面

５．５　システム構築の実施

社外・モバイル利用システムを WindowsXP のサポートが終了する平成 26 年 4 月までに運用開始することとし、システム構築を次のスケジュールで実施した。

・25 年 9 月　社外・モバイル利用システム構築の検討開始、候補システムの選定
・25 年 10 月～12 月　複数の候補システムの試行を行い機能確認
・26 年 1 月　複数システムに対し競争見積を実施し５年間の合計費用でシステムを決定
・26 年 1 月～3 月　システム構築を実施し、予定通り 26 年 3 月で完了

当社ではシステム調査、試行、システム仕様検討・構築の一部を実施し、要した人役は２人月以内である。

システムの詳細設計・構築及び５年間の運用・保守を含めたシステム導入による合計費用を５年と専用USBキーの個数で割って算定すると、専用USBキー１個当たり年間12千円未満である。

26年4月から運用を開始して、ほぼ順調に稼動しており、６ヶ月が経過している。

５．６　システム構築の効果

（１）定量的効果

定量的効果については、前提条件が明確な出張時モバイル利用について金額面での効果を算定することとし、従来どおりの社外持出専用パソコンを整備することと比較する。

仮想シンクライアントシステムの導入コストは、専用USBキー１個当たり年間費用12千円未満である。従来どおりの社外持出専用パソコンを導入すると１台当たりハード・ソフト購入費用とウィルスチェックなどの年間費用などで５年間で少なくとも10万円は要しており、年間費用は20千円以上となる。比較すると、仮想シンクライアントシステムの導入により、年間４割以上のコスト削減ができたことになる。従来の社外持出専用パソコンは50台程度あることから、年間４百千円の削減となる。

仮想シンクライアントシステム利用では、次に説明するとおり、社外持出パソコンとして新たな投資が必要でなく、仮想シンクライアントシステムの導入コストだけでよい。

仮想シンクライアントは専用 USB キーで起動でき、Windows パソコンがあれば専用 USB キーだけを持ち運べば、利用できることになる。最近は、ホテルなどで Windows パソコンの貸出サービスを行っているところも多い。社員の８割以上が自宅に Windows パソコンを所有している。仮想シンクライアントは USB 起動で利用できるが、利用するパソコンのハードディスクなどの記憶装置にはデータは一切残さないので、ホテルの貸出パソコンや自宅のパソコンを利用したとしてもデータが残ることは無く、情報漏えいのリスクはない。

社内資料などを作成したり、既存資料を修正した場合などデータを保存する必要がある場合はファイル共用サーバに保存することができる。当社では、全社のファイル共用サーバに全社・部などの組織別のフォルダをはじめ個人別フォルダが用意されている。出張時など社外に持ち出すパソコンにデータを保管しておく必要はないため、社外持出パソコンは特別なものは必要なく、業務情報を保管していないパソコンであればよい。Windows７，Windows８などの社内で使用する一般的なセキュリティ対策を行った既存パソコンが利用でき、社外持出パソコンとして新たな投資は必要ない。

（２）定性的効果

情報漏えいリスクの低減、大規模災害・パンデミックなどの緊急事態発生時の対応などに対する効果を定量的に算定することは可能であり、前提条件の設定によっては、非常に大きな効果を出すことができるが、コンセンサスを得ることが難しいため、定性的効果として説明する。

最も大きな定性的効果は、導入目的どおり、情報漏えいリスクをゼロに近くしていることであり、従来の社外持出専用パソコン利用時に比べて、大幅に低減できている。

大規模災害・パンデミックなどの緊急事態発生時に業務上必要な者に対しては、通常時に専用 USB キーを渡しておけば、自宅にあるパソコンで緊急事態発生時にある程度の必要な業務対応ができることになる。

これらは万一の事態への対応であるため、発生しなければ実際は効果がないことになるが、通常時における定性的効果として、次のものがある。

研究開発をはじめとする業務の効率化である。研究員が自宅などの社外で研究開発アイデアを発想した際に、すぐに研究資料などを確認することができれば、効率的であり、良いアイデアが思いついた際に研究開発を有効に推進することができる。これまでであれば、会社に行き資料を確認したり、後から思い出すのに時間がかかることになるが、すぐに確認できることによって、月に１回、時間を 20 分程度短縮することができれば仮想シンクライアントシステムの導入コストを回収することができる。

ユーザーからの評価としては、上記以外に、次のような効果があげられている。

・これまで出張時などで必要な場合には、必ず重い社外持出専用パソコンを持って行く必要があったが、新システムではほとんど荷物にならない専用 USB キーだけを持っていけばよい場合もあるので、非常に楽になった
・業務情報の入った社外持出専用パソコンを持っていると万一の紛失や盗難などに気をつける必要があり精神的な負担になっていたが、それがなくなり気分的に楽になった
・休日や帰宅時に、自宅で何か思いついたときに資料の確認やスケジュールの確認、メールの送受信ができるので、すぐに解決できる

などである。

６．展開と今後の課題

６．１　他社での活用の可能性

今回、当社で構築した社外・モバイル利用システムは、セキュリティを確保して安価に構築・運用できるシステムであると考えており、他社でも、中小企業、大企業を問わず、活用できるものと考えている。

他の企業で考えても、近年のシステムは Web システム化されてきており、ほとんどの場合対応可能なのではないかと考えられる。当然、クライアント・サーバシステムなど特殊なシステムがあり、対応できないものがあることが考えられる。その場合は、その特殊なシステムに対応する部分だけ、ブレード PC 方式・仮想 PC 方式などのシンクライアントシステムで構成し、他の大部分のシステムに対しては仮想シンクライアント方式のシステムで構成して組み合わせることで対応すれば、センター側のシステムを小規模にすることができる。大半のシステムは、仮想シンクライアントシステムで対応できるため、大幅にコスト削減することが可能である。

まず、中小企業での活用を考える。最小システム構成について検討したところ、専用 USB キー５個で同時アクセス数を５とするならば、50 万円未満で構築でき、パソコン購入より安価な費用で、セキュリティを強化し情報漏えいリスクを大幅に低減することが実現できる。

次に、大企業での活用を考える。出張時モバイルシステムなどは多くの企業で既にシステム構築済みではないかと思われる。しかし、万一の大規模災害やパンデミックなどの緊急事態発生時の対策を考えるとどうなるか？情報漏えいリスクを低減して対応できるシステムの構築はまだのところも多いのではないかと思う。多くの利用者に対して用意する必

要がある専用 USB キーは比較的安価である。多くの利用者の同時アクセス数の増大を緊急事態発生時だけに行うために、センター側に利用するゲートウェイ(GW)装置に、緊急事態発生時のみ一定期間同時アクセス数を増加することができるパンデミックオプションを活用すれば、通常時のコストはかからず、緊急事態が発生した時だけコストが発生するということで、大幅に安価に対応することが実現できる。

６．２　今後の課題

今回のシステム構築は、通常時や緊急事態発生時にある程度の業務ができるようにすることを想定しているため、パソコンを利用することを前提として構築している。つまり、出張時、研究開発アイデア発想時や大規模災害・ハンデミックなど緊急事態発生時にメール送受信などグループウェアの活用、ファイル共用サーバへのアクセスによる研究開発資料の活用や社内業務システムの利用を想定している。

しかし、出張時やちょっとした外出時のことを考えた場合には、メールの送受信、スケジュールの確認だけなら、スマホの方が手軽で簡単ということが考えられる。スマホ利用に関しては、現状でもシステム的にはスマホでアクセスできるようにすることは可能であるが、情報漏えいリスクを無くすということに関しては、スマホにデータが確実に残らないようにすることが保証できていないため、実施していない。

コストを別にすれば、富士通が提供するサービス「FUJITSU Thin Client Solution モバらくだ for スマートデバイス」など、すぐに対応できるサービスが提供されており、対応策はいろいろある。しかし、現行の仮想シンクライアント方式のシステムによるパソコン利用に比べて、月額２千円以上とより多くのコストがかかることになる。必要性とコストの関係を見極め、より安価な費用対効果に優れる対応策の検討を考えていきたい。

７．おわりに

今回の当社の事例は、出張時や大規模災害・パンデミックなどの緊急事態発生時などに社外から社内システムをセキュリティを確保して利用できるようにするシステムを、できるだけコストを押さえて実現することを目指したものである。

中小企業、大企業を問わず、コストの関係で十分なセキュリティ対策ができず、社外から社内システムを利用している企業や、大規模災害などに対応するためのシステムをいかに安価にセキュリティを確保して構築するかなど、対策に困っている企業などもあるのではないかと考える。

今回の当社事例が、これらの企業にとって参考になれば幸いである。

以　上