BCP 対策とコスト削減を両立する情報通信システムの再構築

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
2015 年　現在　電子技術部長

■ 論文要旨 ■

システムの BCP 対策では大規模災害などの万一の事態発生の際にも重要システムが継続稼動できるよう、システムの免震対策・長時間停電対策やデータの遠隔地保管などの対策を行う必要がある。また、重要システムの稼動だけでなく、従業員が事務所に出勤できない場合には社外で業務遂行に必要なシステムの利用ができることが必要となる。これらの必要性は認識されているが、対策には多額のコストがかかる場合が多く、万一の事態はいつ発生するかわからず、システム稼動中に必ず発生するわけではなく、特に中小企業にとって実施することが難しい。

四国総合研究所では、社内主要システムのハードウェア保守期限、使用 OS サポート終了によるシステム更新に当って、必要機能とシステム構成を考慮してデータセンターのサービスを工夫して活用することと、関連するシステム全体の最適化を図ることで、BCP 対策を行いつつコスト削減も両立するシステム再構築を実現した。

■ 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 月に設立された。今年で 28 年目を迎える従業員百数十名の企業で、香川県高松市にある本社研究所で全員が研究開発などの業務を行っている。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

多くの企業と同様に、長期的、経営的な観点からの課題として情報通信システムの大規模災害対応を意識していたが、平成 23 年の東日本大震災の発生に伴い、南海トラフ地震の被害想定が大幅に引き上げられ、対策の必要性が高まっていた。

しかし、大規模災害対策は

・情報通信システムそのものだけでなく建物なども含めた関連設備の対策が必要となり、対策コストが多額となる
・比較的更新周期の早い情報通信システムにおいては対策を行っても稼動期間中に発生しない場合がほとんどである

ことなどから、必要性を認識しつつも実施しにくい課題である。

大規模災害対応のためには、万一の大規模災害が発生した際に利用するシステムの継続稼働体制を整備するとともに、従業員がそのシステムを利用するためのシステム利用環境の整備が必要である。

システムの継続稼働体制の整備に関しては、対象となるシステムが平成 26 年下期にハードウェアの保守サポート期限を迎え、システム更新せざるをえなくなったことから、この機会をとらえ、大規模災害時などの継続稼働対策を検討する。システム利用環境の整備に関しては、平成 26 年４月の WindowsXP のサポート終了にあわせて、パソコン取替を行うとともに、関連する情報通信システムの整備として、社外で利用する出張時システムを再構築する必要があった。出張時システムの更新において、社外で利用する新たなニーズである大規模災害などへの対応も含めて、関連するシステム全体を一体のシステムとして考えて、社外でシステムを利用するための環境整備を行うことを検討する。

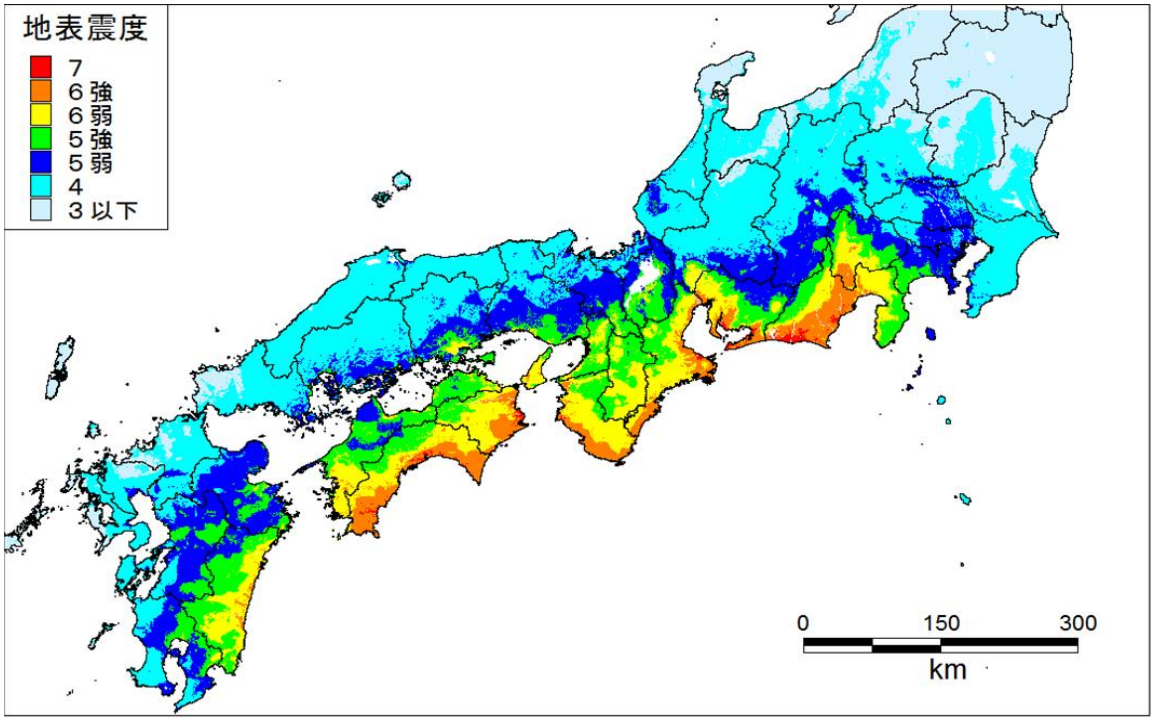
これらのシステム更新を検討していくうえで、コスト削減がはかれるよう、既存にある利用できる資源やサービスを有効活用することで、大規模災害対策を行うための大きな問題である対策コストをできる限りかけることなく、BCP 対策を実現することをめざした。

２．事業継続計画

２．１　大規模災害などの緊急事態発生の恐れ

図１のように震度 6 を超える大規模地震の 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[1]が想定されている。四国ではほぼ全域で震度５と地震発生に伴う津波が想定されており、当社では本社研究所の建物設備などに支障が生じたり、津波などの影響で地下にある電源設備などが浸水する可能性があり、情報通信システムそのものだけでなく、稼働するために必要な関連設備が使用不能になる恐れがある。

近年は地球温暖化の影響か、異常気象による集中豪雨の発生、それに伴う大規模な浸水や土砂災害の発生などが毎年のように発生している。新型鳥インフルエンザ、デング熱、エボラ出血熱などの流行のようにパンデミックが発生する可能性も高まっている。大規模地震だけでなく、異常気象やパンデミックが発生した場合には、会社設備やシステムに問題はなかったとしても、一か所しかない会社事務所に一定期間出勤することができない事態が発生する恐れがある。現在は業務遂行にシステム利用は必要不可欠であり、会社事務所に出勤できなければ業務遂行に必要なシステムが利用できず、業務が実施できなくなる。



（南海トラフの巨大地震モデル検討会（第二次報告）資料[2]　「基本ケースの震度分布」平成 24 年 8 月 29 日発表　より）

図１　南海トラフ地震　基本ケース地表震度分布

２．２　事業継続の基本的な考え方

当社では、南海トラフ地震などの大規模災害や新型インフルエンザなどの感染症の流行などにより、本社施設などが使用できなくなる緊急事態が発生した場合に、以下のような

方針で事業継続を行う。

●安全確保の観点

従業員や来訪者の安全を最優先として、２次災害の防止などの防災対策を進める。

●事業継続の観点

当社は研究機関であり、通常時に実施している全てのサービス提供を大規模災害など発生の緊急事態時に短期間で復旧して継続提供する必要性はない。主要顧客である四国電力が電気供給を短期間で復旧するために、技術的課題解決をサポートする業務を実施することに関して短期間で事業復旧することとし、他の業務に関しては研究設備をはじめとする本社施設などを復旧させた後、早急に事業再開できるようにする。

２．３　事業継続における情報通信システムへの要求事項

基本的な考え方より、大規模災害など発生の緊急事態時に実施すべき、

・四国電力の技術的課題解決をサポートする支援業務の実施

・研究設備など本社施設などを復旧させた後の早急な事業再開

を実現するために必要なことは、研究部門が持つ研究開発資料・データと間接部門が持つ当社資料･データを万一の際にも利用できるようにしておくことである。具体的には、「本社施設使用不能時点での四国電力への支援業務の実施」と「研究設備をはじめとする本社施設などを使用可能にできた後の業務復旧」で必要となる資料･データを遠隔地にも保管しておき、緊急事態発生時にも利用可能にしておくことが必要となる。

このために必要なシステムは、研究開発部門では、研究開発成果としての知的財産、研究データなどを保管している研究開発資料、データファイルなどを利用するための情報通信システムである。間接部門の重要な業務処理は四電グループで共同利用する「四電グループ総合業務システム」を使用することで全て実施しており、間接部門では、間接部門が持つ当社独自の資料、データなどを利用するための情報通信システムである。

したがって、当社として必要な重要システムは、緊急事態発生時に業務を実施していくために必要となる社内外とのコミュニケーション、情報収集・発信などを行うための情報通信システムと、研究開発部門や間接部門が持つ独自の資料･データを利用するための情報通信システムである。

３．重要システム継続稼動体制整備

重要システムの継続稼働体制の整備については、事業継続の基本的な考え方に基づき、万一の大規模災害発生などの緊急事態時に必要なシステムについてだけ対策を実施することとし、コスト削減をはかり、コスト増分を抑制する。

３．１　重要システムの状況

四国電力グループでは連結決算対象のグループ企業を含めた「四電グループ総合業務システム」を構築している。基幹業務である工事･受注管理、経理、資材、人事労務、資金管理、従業員申請サポートなどに関してはグループ会社で共同利用する。「四電グループ総合業務システム」は、四国電力の基幹業務を実施するシステムであるため、データセンタ

ーに設置、広域イーサネット網（閉域網）を利用してアクセス、大規模災害などの発生に対するBCP対策が実施されている。

当社では計画･実施･統制に関する基幹業務は「四電グループ総合業務システム」を活用するため、自社が所有する重要システムは、コミュニケーション、情報共有などを行う「グループウェアサーバ」とインターネット関係の「ホームページ公開などのための Web サーバ、メールサーバ、DNS サーバ」などである。研究開発用として重要なシステムは研究開発設備として各研究部が個別に管理しているが、事業継続の基本的な考え方で述べたようにBCP対策の必要性がなく、ここでは対象外である。

研究部門における研究開発資料やデータ、間接部門における当社独自資料やデータに関しては、全社として統一したシステム環境にはなく、各部で研究グループ単位など独自にファイル共用サーバを利用したり、各自が個人別パソコンの内蔵ディスクなどに保管していた。

３．２　重要システム再構築の必要性

基幹業務を行う「四電グループ総合業務システム」は BCP 対策実施済で必要性はないが、自社所有のグループウェアやインターネット関係のシステムはLinuxやWindowsのOSを使用したサーバ４台の上に構築し自社サーバ室に設置していた。このサーバ４台が平成26年下期にハードウェア保守期限を迎えるため、システム更新を平成26年上期末までに完了する必要がある。

現状のシステム構成では、

①システム機能に関係なく、６年程度でハードウェア保守期限でのシステム更新があり、その都度多くのコストが発生する

②システム監視が勤務時間内で、夜間･休日のトラブル発生などでは対応が遅れる

③ビル電源点検で年１回停電があり、バックアップ電源の準備・切替などが必要となる

④大規模災害などが発生した場合に継続稼動できるための免震設備の設置、長時間停電対策などシステム関係設備がない

などの課題がある。自社でのサーバ構築･設置では建物設備や電源設備の大幅変更が必要となるなど、これらの課題解決が困難であるため、データセンターの活用などを考え今回のシステム更新にあわせて解決することをめざした。

各部独自のファイル共用サーバや個人別パソコンへのデータ保管では、大規模災害発生時に重要データを保全するための遠隔地保管を実施することは難しい。重要データの遠隔地保管を実施するためには、まず重要データに関しては全社統一したシステム環境で管理、保管しておかなくては、実施することができないため、重要データを保管する全社のファイル共用サーバを構築しておく必要がある。

３．３　重要システム再構築の実施

（１）グループウェアやインターネット関係システム

グループウェアやインターネット関係の社内重要システムを再構築するに当たり、BCP対策を行うためにデータセンターの活用も考え比較検討した結果、現行と同条件での BCP 対策をしていない自社サーバ構築･設置よりもデータセンターのクラウドサーバサービスを利用する方が安価に構築できる見通しが得られた。データセンターのクラウドサービスで

はセキュリティに関する懸念があったが、インターネット網用と社内ＬＡＮ接続する閉域網用のサービスを活用することでネットワーク分離ができる。当社として必要なセキュリティ確保ができると判断し、データセンターのクラウドサーバサービスを利用して、図２に示すとおり再構築する。データセンターを活用することで、24 時間 365 日の連続稼動・監視と大規模災害など発生時にも継続稼動できるシステム環境が整備できる。

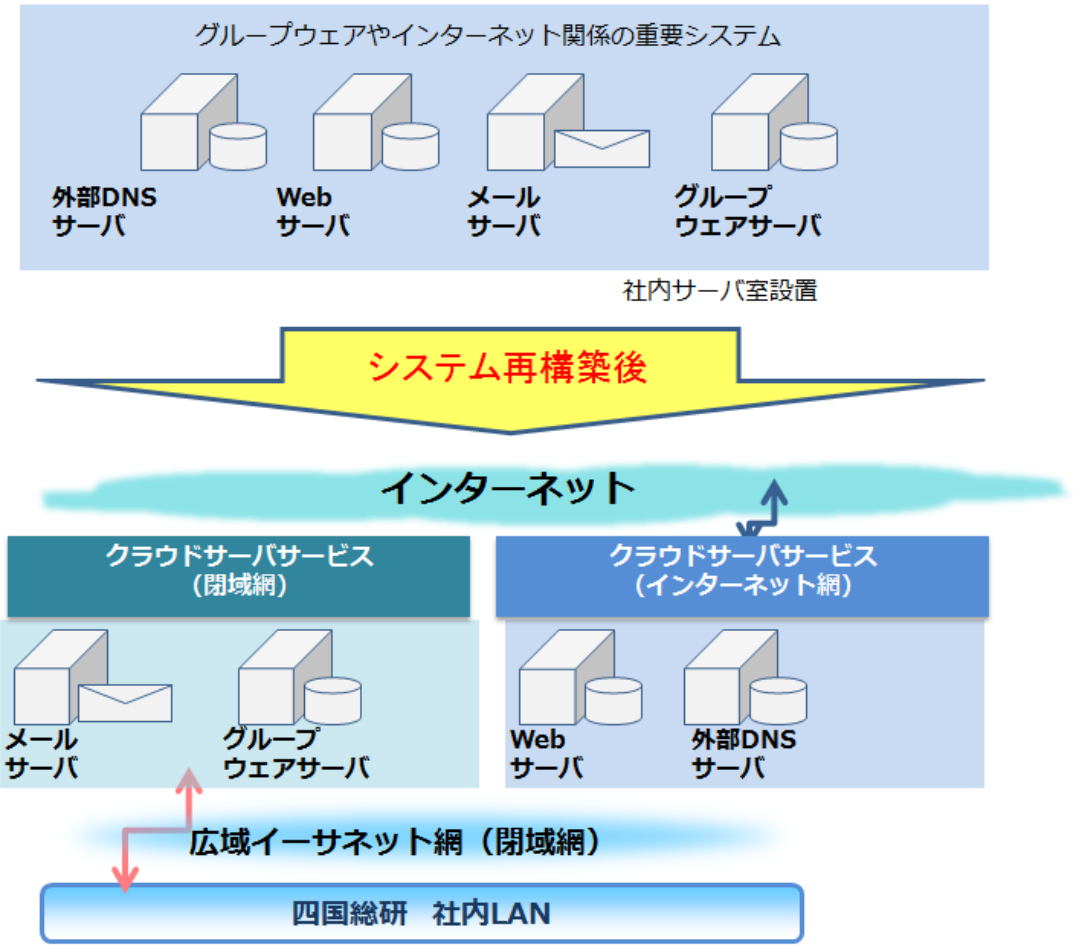


図２　グループウェアやインターネット関係システムのデータセンター活用による再構築

（２）全社ファイル共用サーバ

重要な資料やデータを保管するためのファイル共用に関しては、全社ファイル共用サーバの構築を行うこととする。これは WindowsXP パソコンを Windows７パソコンに取替することから、パソコンのハードディスクに保管されているデータを移行する必要があり、移行作業を効率的に実施するとともに、重要な資料やデータについて情報共有を推進することも兼ねて、全社統一したシステム環境に移行するためである。

全社ファイル共用サーバは全社･部･課・グループ毎の組織別フォルダと個人別フォルダを用意して、

・組織別フォルダは必要なデータが保存できる容量を確保
・個人別フォルダは現在１人当り 50GB を確保
・いずれのフォルダとも、今後、必要に応じて容量追加

することとし、重要な業務情報や研究開発データの情報共有を可能として、各自のパソコ

ンに重要データなどを保管しなくてもよいシステム環境を整備する。

全社ファイル共用サーバは図３に示すシステム構成とし、RAID ディスクサーバのメイン機とバックアップ機によるフェイルオーバー構成として高い信頼性を確保し、これまで各部で独自にファイル共用サーバを設置したり、各自がパソコンに保管していた場合に必要であった重要データのバックアップ作業などから、各部や研究員を解放する。万一の大規模災害などが発生した際にも重要データの継続利用が可能となるよう、データセンターに遠隔地データ保管サーバを設置して毎日夜間転送を行い、万一、大規模災害などが発生しても重要データが継続利用できる。

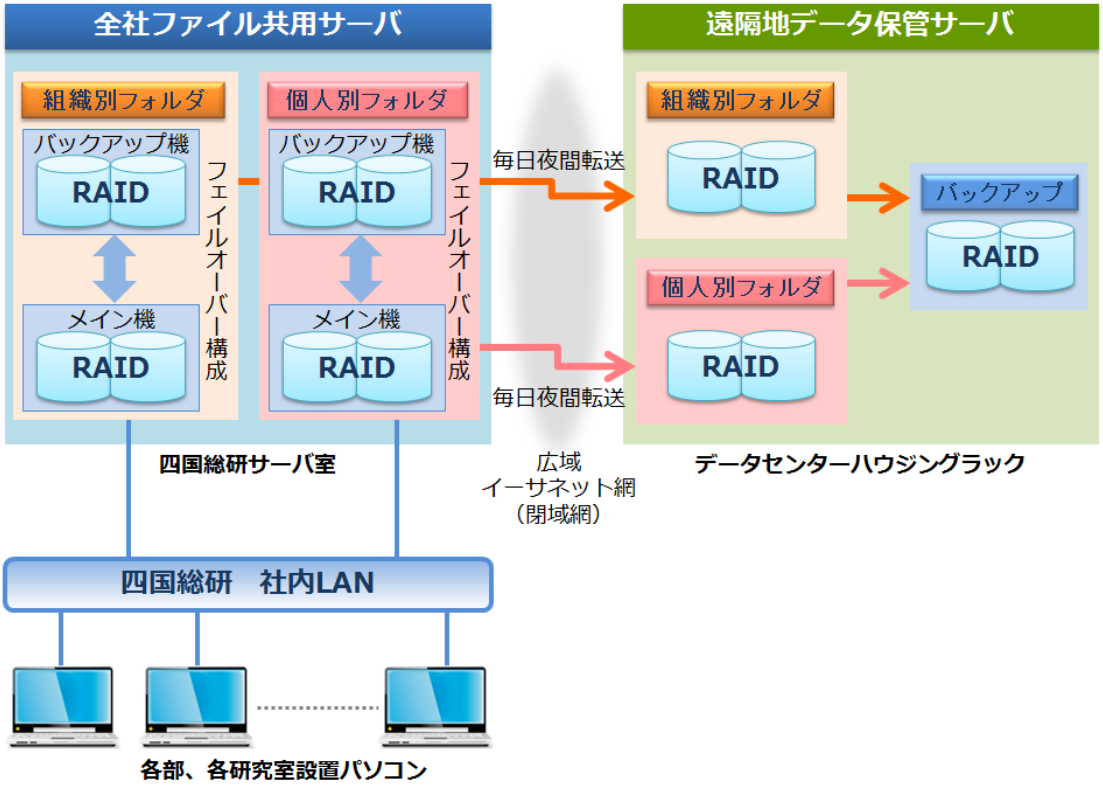


図３　全社ファイル共用サーバのシステム構成

（３）構築スケジュール

グループウェアやインターネット関係システムについては平成 26 年上期に再構築を完了するため、平成 26 年４月より本格検討を開始してデータセンターでの再構築を５月に決定して、６月から８月でデータセンターでの再構築を完了し、９月から運用を開始した。

全社ファイル共用サーバについては次のように進めた。平成 26 年４月までに Windows７パソコンへの移行を完了するため３月にパソコンや OS の取替を実施する。この取替作業までに全社ファイル共用サーバの構築が完了するよう、１月より本格検討を開始し、２月までに構築を完了して、３月より運用を開始した。データの遠隔地保管に関しては、全社ファイル共用サーバの運用が１年以上経過した平成 27 年５月に遠隔地保管サーバをデータセンターに設置した。

４．システム利用環境整備

システム利用環境整備については BCP 対策としてだけ考えたのでは、対策コストがそのまま増分となる可能性が高い。このため、コスト削減と利便性の向上がはかれるよう、従来ある出張時システムを、新たなニーズである BCP 対策、在宅勤務などの新たなワークスタイルへの対応、研究開発のスピードアップなど更なる業務の効率化への対応をサポートするシステムとして、関連するシステム全体を一体で考えて、社外利用システムとして再構築する。

４．１　従来システムの状況と再構築の必要性

従来、当社では社外で利用するシステムとして図４で示すシステム構成の社外持出専用パソコンを利用した出張時システムを活用していた。このシステムは社外持出専用パソコンを WindowsXP パソコンで構成しているため、平成 26 年４月の WindowsXP のサポート終了までにシステム再構築が必要となっていた。

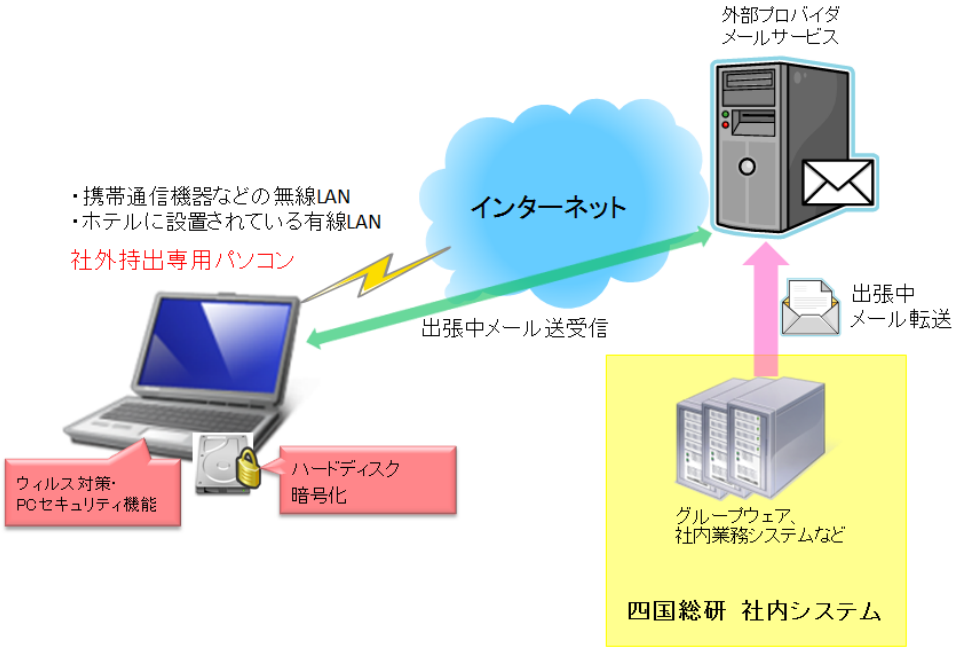


図４　従来の出張時システムのシステム構成

４．２　要求事項と利用できる既存資源

（１）求められる要件

求められる最も重要な要件は、自宅や外出先など社外で利用することから、情報漏えいリスクをなくし、安全に、業務システム、グループウェアやファイル共用サーバなどの社内システムが利用できることである。

これらの情報漏えいリスク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を行えば、通信回線上からの情報漏えいを防止できる。利用するパソコンにデータを保管している場合は、パソコンが万一紛失したり盗難にあうことで、ハードディスクを暗号化していても、どうしても情報漏えいの問題が生ずる。つまり、利用するパソコンなどの端末機器にデータが保管されていなけれ

ば問題がなくなる。

したがって、「情報漏えいリスクをなくす」点からは、社外で利用するパソコンなどの端末機器にデータを保管せず、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、端末機器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。

もう一つの大きな要件は、コストである。業務遂行の効率化に寄与する出張時、研究開発アイデア発想時、在宅勤務など通常時での活用は、期待される効果に見合う費用を投入することが可能である。しかし、大規模災害やパンデミックなど緊急事態発生時での活用は、万一の場合に発生する大きな損害を防止する効果を算定することはできるが、構築したシステムの稼動期間中に必ず緊急事態が発生するわけではなく、特に中小企業にとって投資することは難しい。

今回のシステム構築においては、万一の際にシステムが有効に活用できるよう緊急事態発生時に利用するシステムも、日常業務を遂行する中で活用する出張時、研究開発アイデア発想時、在宅勤務などで利用するシステムと一体で考えていくこととしている。できれば、日常業務の遂行を効率化する効果によって、システム全体の費用を賄うようにしたい。そのためには、既存にある資源をいかに有効に利用して、かかる費用を削減できるかが鍵と考える。

（2）利用できる既存資源

利用場所に既存にある資源として何が利用できるかを検討した。四国電力グループでは情報漏えい防止のために毎年「個人所有パソコンにおける業務情報等に関する調査」を実施している。この結果によると８割を超える従業員の自宅には Windows パソコンがあり、光ファイバーなどの高速インターネット環境があることがわかっている。また、出張時などを考えると、出張に持出専用パソコンを持参したり、ホテルには宿泊者が利用できるパソコンの設置や貸出パソコンがある。通信としては、ホテルで高速のインターネット回線が利用できるのは当たり前であり、屋外においても WiFi、LTE など高速な通信環境が利用できる。

端末機器としては、緊急事態発生時に出社が困難となった場合や研究開発アイデア発想時、在宅勤務の場合など、自宅にあるパソコンが活用できる。出張時には、持出専用パソコンやホテル設置のパソコンや貸出パソコンが利用できる。

通信回線としては、自宅では光ファイバーなどの高速インターネット環境、ホテルでも高速のインターネット回線、屋外でも、WiFi、LTE など高速な通信回線が利用できる。

移動時などを考えると、ビジネスマンは携帯電話を持っており、携帯電話の半数以上がスマートフォンである。出張・外出時での短時間での簡単な利用や、緊急事態発生時でもグループウェアなどによるコミュニケーションや資料参照などであれば、スマートフォンが利用できる。

したがって、これらの資源を有効に利用したシステム構築を考えることによって、システム構築にかかる費用を抑制することができる。

４．３　社外利用システムの構築

（1）システム構成と課題

構築するシステムに機能面で求められていることは、「情報漏えいリスクをなくす」、「どこでも必要なときに利用できる」「パソコンやスマートフォンで利用できる」であることから、有力なシステム実現方法は「デスクトップ仮想化」である。一般的にデスクトップ仮想化は万能ではなく、適していない用途もある。デスクトップ仮想化に不向きな、多様な周辺機器を使う場合や動画データを頻繁に利用する場合は、研究開発そのものを実施する場合であり、当社において研究所内で実施したのでよく、社外で実施する必要はない。したがって、社外利用システムの実現手段としてデスクトップ仮想化は非常に有力である。

デスクトップ仮想化のシステム構成と適用における課題の概要を図５に示す。デスクトップ仮想化に関して、前述のとおり、端末機器、高速通信については既存にある資源が利用できることから、残る課題はシステム構築･運用コストである。

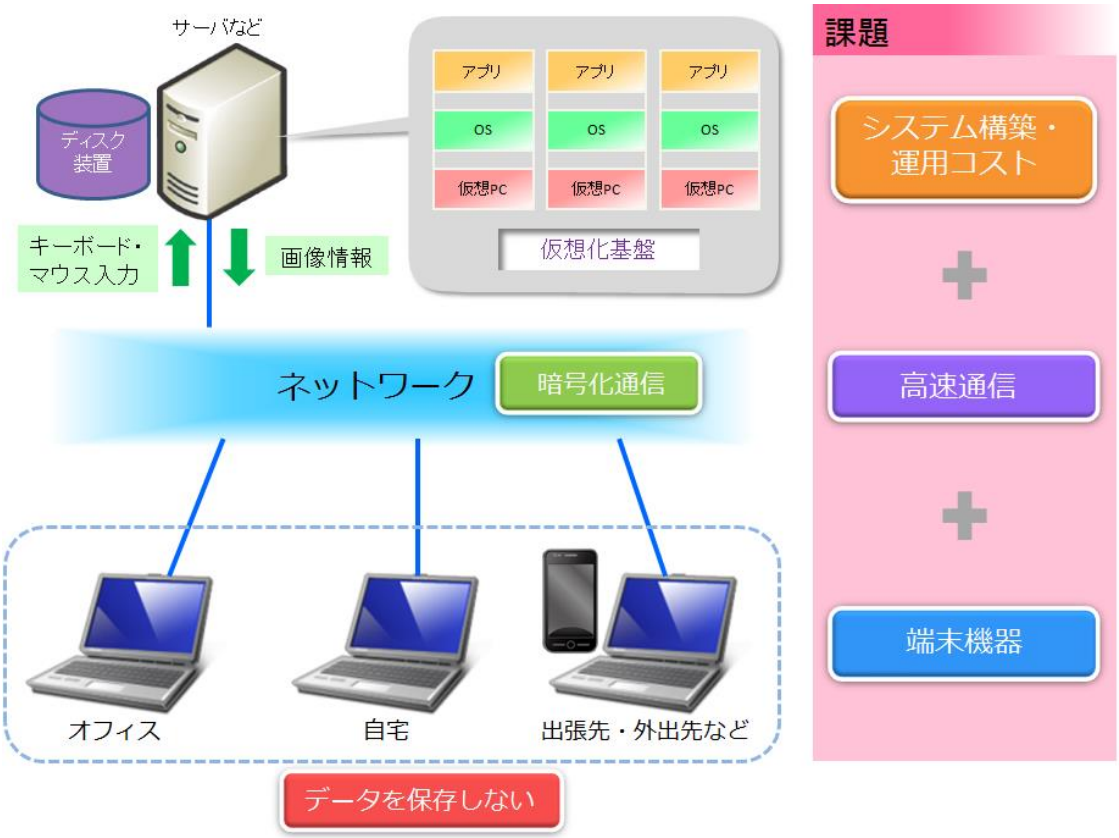


図５　デスクトップ仮想化のシステム構成（仮想 PC の例）と課題

デスクトップ仮想化は、パソコンを直接使用するのに対して、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る。ネットワークを介してサーバで実行するため高速な処理能力が必要となるなど、センター側に多くのシステム構築・運用コストがかかる。

特に、緊急事態発生時の対応では、多くの利用者が一度に集中するので、同時アクセス数の急激な増大に対応できるサーバを準備しておく必要があり、膨大なコストとなる。これは当社のような中小企業で導入することは無理であり、何らか別のシステム実現方法を考える必要がある。

（２）システム実現方法の詳細検討

デスクトップ仮想化はシステム構築・運用コストが大きすぎて採用が困難であるため、原点に立ち返り検討する。目指すところは、必要な機能を必要とする場所で情報漏えいリスクをなくし安全に利用できることと、利用場所に既存にある資源を活用することでコストを抑制することである。デスクトップ仮想化ではセンター側で処理を行い、利用場所にあるパソコンなどの端末機器の能力を十分に活用していない面がある。これは情報漏えいリスクをなくすため端末機器側にデータを保管しないことと、利用するデバイスに依存しないシステムを構築するためなどである。

利用する場面を考えると、時間のとれる時と短時間しかない時、パソコンなどの大画面とスマートフォンなどの小画面など、利用場所の状況や利用できる機器の特性によって、利用方法などが異なってくる。既存の資源を有効活用するため、デスクトップ仮想化のように全部を一括で考えるのではなく、利用する機器を中心に考えて、パソコンを利用する場合とスマートフォンを利用する場合の２つの場合を考えることとする。

いずれの場合も、利用する端末機器は十分な処理能力を有しているので、この能力を最大限活用してデータ処理を行い、端末機器にデータを保管しない方法はないのか、詳細に調査・検討する。

（３）パソコンを利用したシステム構築

社外で利用するアプリケーションは 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である。当社での利用を前提に調査した結果、パソコンの処理能力を活用してデータ処理を行い、パソコンにはデータを保管しないシステムがあることがわかった。シンクライアントシステムの一方式で、機能限定、利用アプリケーションに制限はある「仮想シンクライアント」という方式である。詳細に調査すると、仮想シンクライアント方式では、利用アプリケーションが限定されるものの、処理する 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にはデータが残らない。利用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などが利用できる。

仮想シンクライアント方式は端末側のパソコンのハード・ソフトを利用するために、新たに必要となるハード・ソフトが少なくコスト面でメリットがある。デメリットは利用アプリケーションの制限であるが、当社で必要とする Web ブラウザ、ファイルサーバアクセス、オフィスソフトは利用できる。当社で考えれば、仮想シンクライアントのデメリットである利用アプリケーションの制限は問題にならない。「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。

仮想シンクライアント方式によるシステム構築を進める。仮想シンクライアント方式は一般的に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、構成や機能は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構成は、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はパソコンに専用ソフトウェアを導入するもの、専用 USB などを差込み起動するものがある。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 装置である。

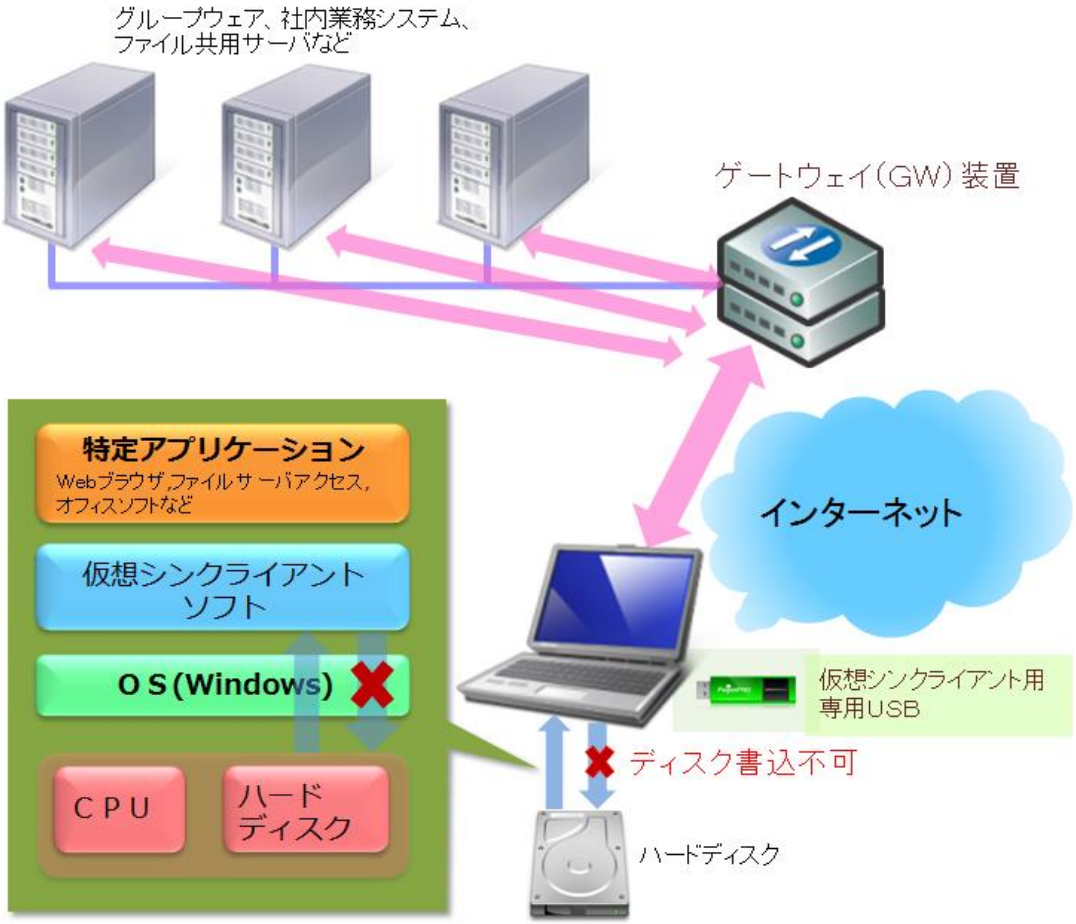


図６　仮想シンクライアント方式のシステム構成

当社では自宅、出張時などいろいろな場所で利用することから、持ち運びに便利な専用 USB 起動のシステムを導入することとして試行を行い、機能確認を実施した。システム構成に若干の差異はあるものの試行した結果、複数ベンダーのシステムが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、機能とシステム構築・運用・保守など５年間合計費用で総合評価した。最終候補に残った２方式の比較を表１に示す。

表１　仮想シンクライアント方式システムの比較

		A社システム	「FogosPRO」
構成	端末側	専用 USB 起動	専用 USB 起動
	センター側	専用サーバ	SSL－VPN装置
利用可能 アプリケーション		Web ブラウザ、ファイルサーバアクセス、オフィスソフト、PDF リーダーなど	Web ブラウザ、ファイルサーバアクセス、オフィスソフト、PDF リーダーなど
印刷などの制御		○	○
拡張性		△（専用サーバ）	○（汎用の SSL-VPN 装置）
5年間合計費用		△	○
総合評価		△	○

費用が安価で、拡張性に優れるシステムインテリジェント㈱開発の「FogosPRO」を採用し、パソコン側に仮想シンクライアントとして動作する「FogosPRO」の専用 USB を、センター側では汎用的な SSL-VPN 装置を導入した。セキュリティ機能強化をはかるため、当社において SSL-VPN 装置とファイアウォール装置などが連動する多重的なセキュリティ機能を追加して、システムを構築した。構築したシステムの構成を図７に示す。

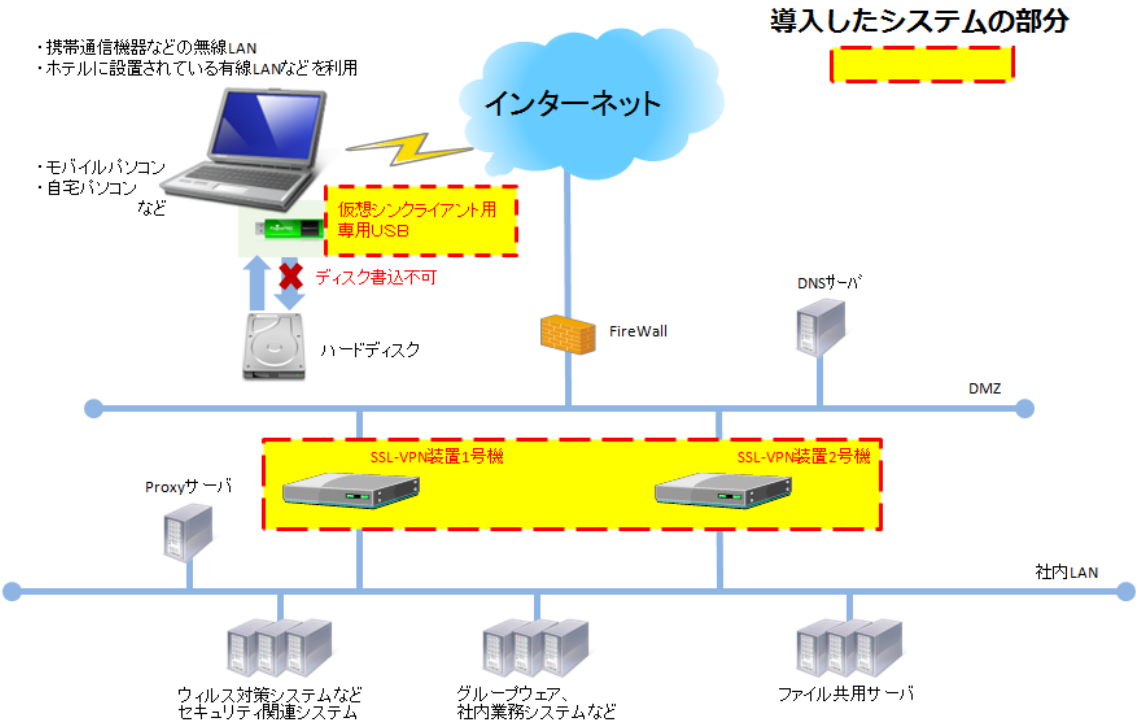


図７　仮想シンクライアント方式を活用したシステム構成

（４）スマートフォンを利用したシステム構築

スマートフォンを利用する場合は、画面の大きさ、入力手段から考えて、表示や参照が中心となる。多くは交通機関での移動中など短時間の利用であり、グループウェアを利用して、メールの送受信、スケジュールの確認などを行うことである。利用アプリケーションは暗号化通信を行う Web ブラウザ主体である。セキュリティ設定を集中管理することができ、スマートフォンなどにデータを一切保管しないセキュアなブラウザがあることがわかった。このブラウザを活用することで、スマートフォンを情報漏えいリスクなしで安全に利用することが可能となる。

パソコン利用のシステムとして、センター側に SSL-VPN 装置を導入したので、これを活用してスマートフォンとの間に暗号化通信を実施する。スマートフォン側には、セキュリティ設定を集中管理することができ、スマートフォンにデータを一切保管しないセキュアなブラウザを利用する。

セキュアなブラウザの製品は複数ベンダーから提供されており、必要な機能は多くの製品で満足している。当社導入を考えた場合、導入台数が数十程度までであることから、セキュリティ設定管理サーバを自社設置する必要がないものがよい。これらの条件を満足する製品に対して調査・検討・試行を実施した結果、

・必要なセキュリティ設定を集中管理できる
・データをデバイスに保管しない
・センター側で端末側のセキュアブラウザ利用の検証が可能

などセキュリティ確保に必要な機能が確認でき、導入・保守費用が安価なものを採用した。導入したブラウザは㈱JMA システムズの「KAITO」である。

スマートフォン側にセキュアなブラウザとして「KAITO」を導入し、集中管理するセキュリティ設定を行う。センター側では、セキュリティ機能強化をはかるため、当社においてセキュリティブラウザ、SSL-VPN 装置とファイアウォール装置などが連動する多重的なセキュリティ機能を追加して、システムを構築した。

（５）社外利用システムの BCP 対策

大規模災害など発生の際にも継続稼動できるよう、図８に示すように社外利用システムが使用するセンター側の DMZ 及び SSL-VPN などの機器を、遠隔地データ保管サーバと同じデータセンターハウジングラックに設置する。これにより、万一の大規模災害時などでも社外利用システムの継続稼動を確保してシステム利用環境の BCP 対策が完成した。

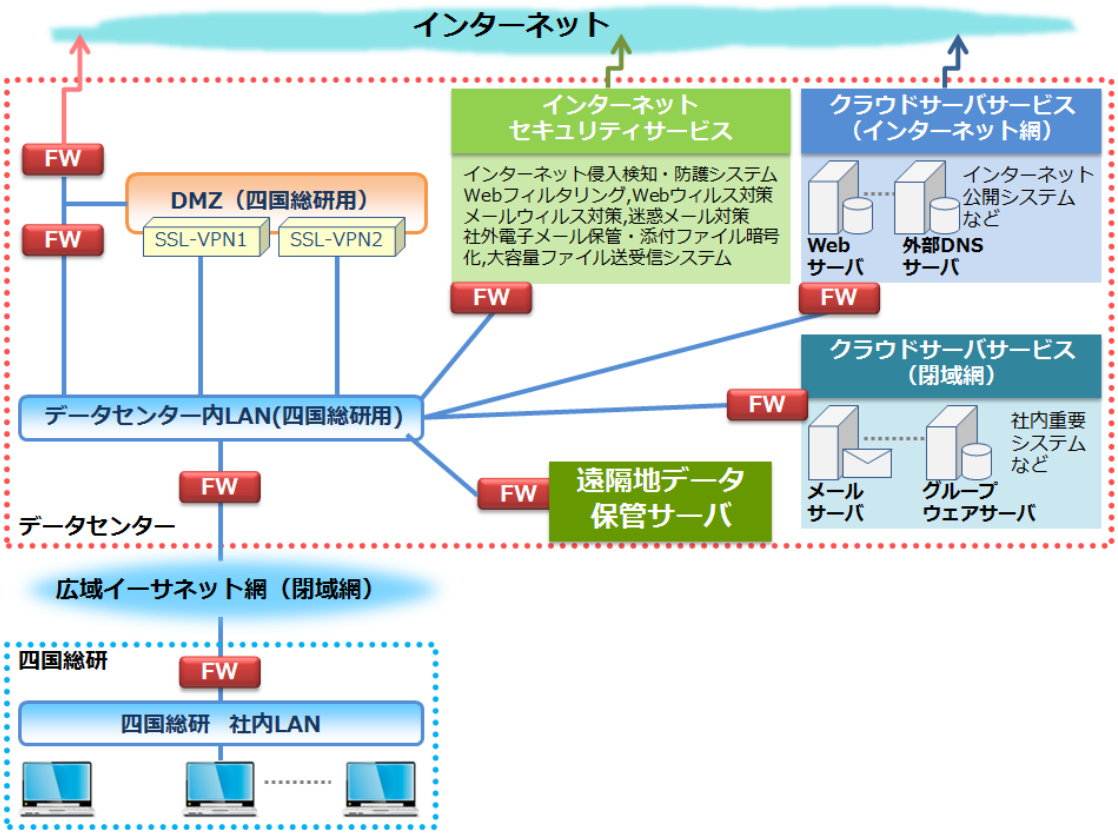


図８　BCP 対策した社外利用システムのシステム構成

（６）構築スケジュール

出張時の利用に関しては、新しい社外利用システムで代替できるよう 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必要がある。出張時の利用を平成 26 年４月までに開始できるよう、システム構築、運用開始を次のとおり実施した。

・25 年９月　システム構築の本格的な検討開始。
・25 年 10 月～12 月　パソコン利用の複数の候補システムの試行を行い機能確認。
・26 年１月　導入する仮想シンクライアントシステムを決定。
・26 年１月～３月　パソコンで仮想シンクライアント方式を活用したシステム構築を実施し、予定通り 26 年３月で完了。
・26 年４月　パソコン利用システムで出張時利用を開始するとともに、研究開発アイデア発想時などの利用を順次開始。パソコン利用システムの運用状況を見ながら、スマートフォン利用システムの検討開始。
・26 年 10 月　在宅勤務制度開始に伴い、在宅勤務利用本格開始。
・27 年１月～３月　スマートフォン利用で導入するセキュアブラウザを決定。
システム構築を実施して 27 年３月で完了し、運用開始。
・27 年５月　社外利用システムのセンター側機器をデータセンターへ移設。

５．システム構築の効果検証

５．１　定量的効果

（１）重要システムの再構築

グループウェアとインターネット関係のシステムの再構築では、今回のデータセンター活用による再構築の５年間費用は約６百万円であり、従来と同じ方式・構成の自社サーバ設置・構築によるシステムの５年間費用で比較すると、５百万円以上のコスト削減が実現できている。

全社ファイル共用サーバの構築では、Linux のアプライアンスサーバを利用したファイル共用サーバの導入費用は機器購入百万円と設計・構築人役 20 時間・人で合計 110 万円である。WindowsXP パソコンを Windows７パソコンに取替する際に、一時的に外付 RAID ハードディスクを用いてデータ移行を行う場合とを比較すると、十数台の外付 RAID ハードディスク購入費用と百数十名の１人当り２時間程度のデータ移行作業の時間短縮効果などを考えると、費用的にほぼ同じでありコストの増分はない。

（２）社外利用システムの構築

今回のシステム構築は既存の出張時システムの再構築であることから、既存システムとの比較でコスト削減を説明する。

既存の出張時システムは、社外持出専用パソコン 50 台とハードディスク暗号化などをはじめとするセキュリティ管理システムで構成している。社外持出専用パソコンのハードウェアの購入、パソコンに導入するオフィスソフトやウィルス対策ソフトなどソフトウェアの購入、セキュリティ管理システムの購入および保守費用を合計すると５年間費用で９百万円である。

再構築した社外利用システムの費用は次のとおりである。

・ベンダー導入分は、社員数に相当する 120 個の専用 USB と仮想シンクライアント管理システム、仮想シンクライアントシステムの設計・構築、SSL-VPN 装置 2 台、スマートフォン、セキュアブラウザの購入と、これらの保守契約である

・当社実施分は、システムの調査・試行・全体設計、SSL-VPN 装置などを用いたセキュリティシステムの設計・構築、セキュアブラウザを用いたシステムの設計・構築である

これらのベンダー導入分の機器・ソフトなどの購入とシステム構築費用、保守費用、当社で実施した人役に基づく人件費を合計すると、５年間費用で８百数十万円である。

社外持出パソコンについては次に説明するとおり社内パソコンが利用できる。重要システムの再構築で説明したように、ファイル共用サーバに全社・部の組織別のフォルダと個人別フォルダがあり、各自のパソコンにデータを保管する必要はない。新システムを利用してファイル共用サーバにアクセスできるため、社外持出パソコンにデータを保管しておく必要はない。つまり、業務情報を保管していない社内パソコンが利用できるため、新たに社外持出専用パソコンを用意する必要がないことになる。

したがって、社外利用システムの費用は、既存の出張時システムより安価であり、日常業務遂行での効果だけでシステム全体の費用を賄うことが実現できている。社外利用システムの利用者１人当り費用は専用 USB やスマートフォンの費用を含んで月額千円である。スマートフォン利用を追加する場合、スマートフォン購入・通信契約費用を含んでも月額千円で１台追加できる。

５．２　定性的効果

（１）重要システムの再構築

自社でのサーバ構築、設置の場合、サーバなどのハードウェア保守期限により５～６年程度の周期で、サーバ取替・システム構築が必要になること、システム監視は運用保守サポートと同様の勤務時間内が基本となること、年一回のビル受電設備点検に伴う作業停電対応などが必要となることがある。これに対して、データセンターのクラウドサーバサービスを利用すると、自社サーバと同様にソフトウェア側の理由によるシステム更新は必要となるが、ハードウェア保守期限によるサーバ取替・システム構築は不要となること、システム監視は 24 時間 365 日可能なこと、電源設備や空調関係の問題もなくなることなどのメリットがある。このほか、使用するシステム資源を、自社サーバの場合では同時使用量やデータ量の増大を考慮して余裕を持った構成とする必要があるのに対して、クラウドサーバサービスでは同時使用量やデータ量の増大があった際に必要時点で能力増強が可能となる。

（２）社外利用システムの構築

次のとおり、システム構築の当初目的の効果が得られている。

BCP 対策では、緊急事態発生時に業務上必要な者に専用 USB を渡しておけば自宅のパソコンを使って業務に必要なシステムを利用でき、緊急事態発生時にも必要な業務対応ができる。

情報漏えい対策の点では、

・センター側と端末機器間は暗号化通信を行い、通信部分での漏えいを防ぐ

・端末機器にはデータを持たず、漏えいするものをなくす

・利用者は２要素認証を行い、不正使用を防ぐ

・登録した複数機器の利用チェック、ワンタイムパスワードなどの多重的対策を追加

するなど、以前の出張時システムに比べて情報漏えいリスクを大幅に低減できており、ゼ

ロに近くしている。万一の情報漏えいを防止できるとすれば効果は非常に大きい。

研究開発をはじめとする業務の効率化では、帰宅後や休日に研究員が自宅などで研究開発アイデアを発想した際に研究資料を確認でき、管理者が自宅でメールの確認・送受信、スケジュールの確認ができることにより、時間短縮の効果があがっている。これまで会社に行き資料を確認したり、後日出勤して思い出すのに時間がかかっていたことが、すぐに確認できることで短縮した時間は1回で30分以上になる。専用USBを持つ社員は、平均的に月に1回以上経験しており、明らかに導入コスト以上の効果がある。

在宅勤務は現在対象者が1名であるが、他の要員にはない高度な知識･技術を有する研究員を継続して活用できることに繋がっており、研究開発推進の上で非常に効果がある。

利用者からは次のような評価を受けている。

・これまで出張時には重い社外持出専用パソコンを持参する必要があったが、新しい社外利用システムでは軽い専用USBだけで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紛失や盗難に気をつける必要があり精神的な負担が大きかったが、それがなくなり気分的に楽になった
・休日や帰宅時に、自宅や外出先でも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

５．３　展開と今後の課題

（1）展開

今回の社外利用システムの事例は、出張時などの通常時だけでなく、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したものである。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る。

近年のシステムは Web システム化されてきており、ほとんどの場合に対応可能なシステムになっているのではないかと考える。クライアント・サーバシステムなどのシステムがあり、仮想シンクライアント方式では対応できないものがある。その場合は、対応できないシステムに対する利用に関してだけ、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合せることで、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方式のシステムで対応できるため、センター側システムのコストを大幅に削減できる。

最小システム構成では専用USB５個・同時アクセス数５とすれば50万円未満で構築でき、小規模な企業においても活用できると考える。

（2）今後の課題

情報通信システム環境としての BCP 対策は整備できたが、万一の際に活用できなければ意味がない。重要システムの継続稼働に関してはシステム側の体制整備により万一の際にも継続稼働できることになるが、従業員のシステム利用に関してはシステム側の整備だけでは万一の際に機能しない可能性がある。万一の際に機能するために、従業員に対して定期的に対応訓練を実施する方法もあるが、当社の場合、社外利用システムは通常時に利用するシステムと一体となっており、日頃から利用することで緊急時も対応できるようにす

ることで考えている。しかし、出張時など会社パソコンを利用するのに対して、緊急時に自宅で利用する場合は自宅にあるパソコンとなり、機器やシステム環境が異なる。このため、BCP 対策のシステム環境の整備が完了した段階で平成 27 年７月の台風 11 号が四国に上陸し香川県を直撃した際に、対応訓練を実施して機能確認を行った。システムの機能面では想定どおり稼動することが確認できたが、自宅パソコンを利用するため、会社パソコンとは動作や操作が一部異なるなど通常時からの利用確認が重要であることが再確認された。平成 27 年８月に再度、社外利用システム、全社ファイル共用サーバシステムの説明会などを開催して、通常時での利用、重要データの確実な保管などを実施するよう周知･啓蒙をはかった。万一の大規模災害などへの対応は、防災意識などと同様に一般的にはまだまだ意識が低い面もあることから、今後も周知･啓蒙が重要であると考えている。

６．おわりに

今回のシステム構築は、BCP 対策に必要な緊急時に利用する重要システムの継続稼動、そのシステムを利用するために必要なシステム利用環境を、従来のシステムの再構築にあわせ、BCP 対策などを考え、既存資源やサービスを有効活用するとともに、新たな視点や工夫を行うことで、BCP 対策の機能を実現するとともに、コスト削減も同時に実現した事例である。

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に関しては、中小企業だけでなく、大企業でもまだのところもあるのではないかと思う。多くの利用者に対して用意する専用 USB は安価である。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、センター側に利用する SSL-VPN 装置に緊急事態発生時のみ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、緊急事態が発生した時だけコストが発生するという対応ができ、大幅に通常時のコストを削減できる。

特に、中小企業では BCP 対策を行うとなると、情報通信システムの問題だけでなく関連する建物設備や電源設備などの問題があることから、多くのコストがかかることとなり、着手が難しい場合が多い。当社の事例のように、データセンターをうまく活用することでクリアできることも多いのではないかと考える。その他にも BCP 対策だけを考えるのではなく関連するシステムを会社全体で考えてうまく工夫することで、BCP 対策だけに余分なコストをかけず、逆にコスト削減をしながら実現できる可能性がある。

BCP 対策は自社のためになるだけでなく、万一の際に業務が停止することになると取引先などのパートナー企業にも大きな影響が及ぼすことになるので、企業の社会的責任として重要なことと考えられる。システム更新などの機会を捉えて、ぜひ実施していただけたらと考える。当社の取組が BCP 対策を検討される企業にとって参考になれば幸いである。

以　上

参考文献

[1]文部科学省地震調査研究推進本部「南海トラフで発生する地震」
参考 URL：http://www.jishin.go.jp/main/yosokuchizu/kaiko/k_nankai.htm
[2] 内閣府南海トラフの巨大地震モデル検討会（第二次報告）資料
参考 URL：http://www.bousai.go.jp/jishin/nankai/taisaku/pdf/20120905_09.pdf