# 事業継続対策と情報セキュリティ対策を実現するための進め方とポイント

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
2016 年　現在　電子技術部長

## ■ 論文要旨 ■

28 年４月に熊本地震、８～９月に東北･北海道で大雨、土砂災害が発生したように大規模災害はいつ発生するかわからない、企業の情報漏えい事件も数多くあるが、いつ発生するかわからない。システム部門としては大規模災害などに対する事業継続対策、万一の情報漏えいを防止する情報セキュリティ対策の必要性は十分に認識し、ベンダーから対策機器、システムの提案は多くある。しかし、大規模災害などが発生するか否かも不明で、日常的に費用だけ発生する対策の費用対効果を説明することは非常に難しく、経営環境が不透明な状況では対策実施が困難な場合も多い。

当社では経営環境の厳しい中、事業継続対策と情報セキュリティ対策を行うシステム構築を実現した。本論文では、経営トップが決断できるようシステム構築の進め方をいかに工夫したかを示すとともに、実施したシステム構築内容と効果的にシステム構築を行うためのポイントについて述べる。

## ■ 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 月に設立された。今年で 29 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、水素などのガス濃度遠隔計測装置や人の目には見えない水素火炎可視化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　システム構築の背景と目的

平成 24 年夏当時、

・東日本大震災に伴い、南海トラフ地震の被害想定が大幅に引き上げられ、対策の必要性が増大した

・情報漏えい事件の増加やサイバー攻撃の増大があり、26 年４月の WindowsXP サポート終了をひかえ、四国電力グループ全体で情報セキュリティ強化を行う

・自社導入グループウェアなどのサーバの保守サポートが 26 年度下期に終了する

ことから、２年以内に情報通信システムの見直しが必要であった。

親会社である四国電力の原子力発電所がすべて運転停止となり電気料金値上げが不可避となったことから、売上の８割以上を占める四国電力からの受託研究開発費が年度途中で大幅削減され、全社での大幅なコスト削減が急務になるとともに、業務効率化の必要性が一層増大する状況変化が発生した。

このような厳しい経営環境の中で、多くの費用を必要とするにも関わらず費用対効果の説明が難しい、事業継続対策と情報セキュリティ対策を実施しなければならなかった。対策に関する機器やシステムに関してベンダーなどから多くの提案があるが、ユーザーとしては、いかに経営トップの実施判断を得るか、効果的に実施するためにいかにシステム構築を行うかが大きな課題となる。

# ２．目的とするシステムの要件

## ２．１　大規模災害などの緊急事態発生時の事業継続対策

（１）大規模災害などの緊急事態発生の恐れ

震度６を超える大規模地震の 30 年以内の発生確率が 70%程度の南海トラフ地震が想定されている。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、当社では研究所建物などに支障が生じたり、津波の影響などで地下１階にある電源設備が浸水する恐れがあり、情報通信システムの機器だけでなく、システムが稼動するために必要な電

源設備などが使用できなくなる恐れがある。

地球温暖化の影響か、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発生している。ジカ熱、エボラ出血熱、デング熱、新型鳥インフルエンザなどの流行のようにパンデミックが発生する可能性もある。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、一ヶ所しかない会社事務所に出勤できない事態が発生する恐れがある。現在で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システムが利用できず、業務が実施できなくなる。

（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感染症の大流行などにより、本社が使用できなくなるなどの緊急事態が発生した場合には、次の方針で対応する。

●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次災害の防止などに努める。

●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すべてのサービス提供を大規模災害発生など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に関して短期間で復旧することとし、他の業務に関しては研究設備をはじめとする本社施設を復旧させた後、早急に事業再開できるようにする。

（3）事業継続における情報通信システムへの要求事項

大規模災害発生などの緊急事態時に、

・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。

したがって、当社として緊急事態時に稼動が必要な重要システムは、

・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
・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
・両部門とも緊急事態発生時にも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システム、受注管理、経理・資材・人事労務などの基幹業務システム

である。

## ２．２　情報セキュリティの強化

サイバー攻撃などによる情報通信システムの停止や顧客・個人情報などの重要データの情報漏えいが発生している。純利益の半分以上を失うようなサイバー攻撃を受けた企業も存在するなどビジネスを脅かす大きなリスクであり、情報セキュリティ対策は重要な経営課題である。サイバー攻撃による事業活動の停止や重要情報の情報漏えいの発生は自社の損失だけに止まらず、取引先や顧客にも大きな影響を及ぼす。

このため、四国電力グループではグループ全体の情報セキュリティを確保し、維持･改善していくこととしている。

（１）情報セキュリティ指針

情報通信システムの脆弱性や不適切な取扱による情報の漏えい・破壊・改竄などの情報セキュリティ上の脅威に晒されることのないよう、四国電力グループ各社のセキュリティに対する意識統一をはかり、グループ全体の情報セキュリティを確保し、維持･改善していくための基本事項として「よんでんグループ情報セキュリティ指針」を制定している。

（２）情報セキュリティガイドライン

「よんでんグループ情報セキュリティ指針」に基づき、四国電力グループ各社が具体的に情報セキュリティマネジメントを確立するため実施すべき取組として、「よんでんグループ情報システムセキュリティガイドライン」を定めている。ガイドラインにはセキュリティ技術や社会環境などを踏まえた「最低限の取組」及びそのレベルアップを図るための「更なる取組」を併せて示している。四国電力と一体的に電気事業に関する多くの情報を取扱う企業や管理連結対象会社は四国電力と同程度のセキュリティレベルを確保できるよう「更なる取組」が求められており、その対象である当社は平成 27 年度末までに達成する必要がある。セキュリティ対策として、「よんでんグループ情報システムセキュリティガイドライン」に基づき実施すべき事項は表１のとおりである。

**表１　情報システムセキュリティガイドラインでの実施すべき事項**

| 項　目 | 実　施　事　項 |
|---|---|
| ａ．組織的対策 | 体制・規定類の整備、情報資産の分類、<br>重大なセキュリティ事故発生時の対応 |
| ｂ．人的対策 | 従業員の守秘義務、従業員への情報セキュリティ教育、<br>委託先の監督･指導 |
| ｃ．物理的対策 | 入退管理、火災対策･停電対策･地震対策、パソコンの管理、<br>外部記憶媒体の管理 |
| ｄ．技術的対策 | アクセス制御、不正ソフトウェア対策、情報漏えい対策、<br>アクセスログの取得･分析 |
| ｅ．事業継続対策 | （これについては事業継続計画で対応） |
| ｆ．監査･評価･改善 | 機能の確認、第三者監査･クロスチェック |

# ３．システム構築の進め方

## ３．１　実施の基本的な考え方

経営トップに事業継続対策、情報セキュリティ対策などの必要性を理解してもらうことはもちろんのこと、厳しい経営環境の中で経営トップにプロジェクト実施の判断をしてもらうためには、実現を可能とするための方策を提案する必要がある。このため、事業継続対策と情報セキュリティ強化などの機能向上を実現すると同時に関係する情報通信コストを現状より削減するシステム構築を行うことを目指すこととした。

今回のプロジェクトでは、WindowsXP サポート終了やサーバの保守サポート終了などに対して期限までに対応するのはもちろんのこと、機能向上に投資する原資を生み出すコスト削減を行うシステム再構築を優先して実施する。具体的には、機能向上に必要な投資以上の原資を既存システムの再構築で生み出し、最初にコスト削減の実績を示した上で経営トップの了解を得ながら進めていく。

実施に当たっては、次の２点を基本とした。一つは、目的とする機能実現と利便性の維持･向上を基本とし、綿密な現状調査、詳細な分析を行い、既存にある設備･システムの把握、活用できる機器･サービスの調査･検討を実施し、有効に活用することである。もう一つは、会社全体を一体の関連するシステムとして捉え、対象となるシステムの最適化ではなく、会社全体という視点で広く取組ことで、全体としての効率化、効果を挙げる全社最適で考え、コスト削減をはかることである。

## ３．２　実施内容と体制

（１）実施内容とスケジュール

24 年８月から 27 年８月まで、システム構築を次の３ステップで実施した。

①全社最適化によるコスト削減　（24 年８月～25 年１月）

日常的に全員が利用する、電話関係、コンピュータ関係、コピー･プリンタ関係の情報通信システムに関して、現状調査分析を行い、全社最適化を目指して、業務に必要な機能と利便性を維持･向上させたシステム再構築を実施し、関係費用を半減して、年間 15 百万円のコスト削減を実現した。

②WindowsXP サポート終了への対応　（25 年４月から 26 年３月）

26 年４月の WindowsXP サポート終了に対応できるよう Windows７パソコンへの取替を事業継続対策や情報セキュリティ対策を考慮して実施し、コスト削減も実現した。

③大規模災害などの対応、情報セキュリティ強化　（25 年 10 月から 27 年８月）

26 年度下期のサーバ保守サポート終了に対応するとともに、目的である「大規模災害などの対応、情報セキュリティ強化」などの機能向上を実現した。

（２）実施組織・体制

提案箇所である電子技術部が主導して全体構想、実施方策の検討、設計･開発を行い、全社の情報通信システムの担当部署である総務部などが機器･サービスの調達・契約、運用などを実施した。情報通信システムの専任要員はいないため、他の業務との兼務の中で実施した。実施組織･体制を図１に示す。

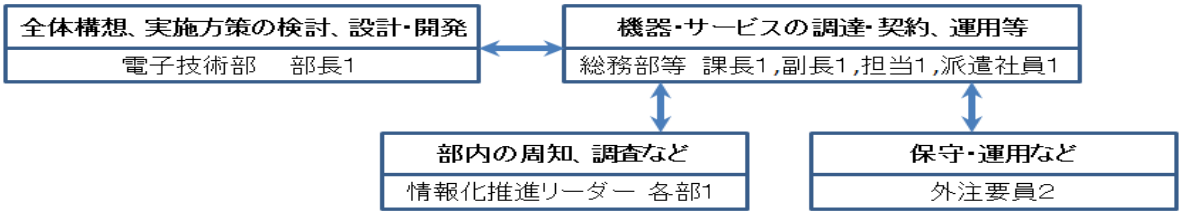


図１　実施組織・体制

# ４．システムの全社最適化によるコスト削減

## ４．１　従来のコスト削減 と現状分析

（１）従来のコスト削減

従来は担当部署が複数の通信事業者や納入業者からの提案を受け、競争見積などにより、

・電話関係の固定電話では、回線の集約化やダイヤルイン番号の活用

・電話関係の PHS・携帯電話では、通信事業者提案による安価なメニューへの変更

・コンピュータ関係では、プリンタでリサイクルトナーの活用

・コピー関係では、交渉による印刷単価の値下げ

などを実施していた。一般的に考えられるコスト削減は実施済みで「担当部署からはこれ以上のコスト削減は無理」とのコメントがあり、大幅なコスト削減は難しいと思われた。

しかし、次のようにコスト削減できる余地があると考え検討した。従来は、利用する機器ごとに担当が分かれ、提供する事業者などからの提案に基づき検討している。事業者は自社の機器、サービスの販売・利用を目指しており、全体最適でない可能性は大きい。対象となる機器やサービスの仕組みは類似しており、重複した機能の削除や効率的な活用を検討することでコスト削減の可能性がある。電子技術部の持つ専門的な知識・技術を活用して全体を一体の関連するシステムとして全社最適を目指して見直し、利用実態に最適なものを選択する。

（２）現状調査と分析

業務を効率的に実施し、かつ、コスト削減を実現するには利用者の利便性の維持・向上が前提となるため、費用と利用状況の実態を把握できるよう利用料金及び利用状況を調査分析した。利用料金は、会計伝票の添付資料により年間 29 百万円であった。利用状況は、会計処理などに必要がなく過去のデータの保管はない。過去の利用状況の把握はできず、直近１ヶ月の機器にあるデータだけが把握できた。利用者ごとの利用状況を把握するためアンケート調査を行い、この結果と利用料金や１ヶ月の機器データの比較から整合性が確認できたため、アンケート結果が利用状況と仮定して分析を実施した。

## ４．２　毎月費用が発生するシステムの全社最適化

（１）電話関係の再構築

従来は、固定電話(NTT 28 回線)は構内交換機を設置し、交換業務効率化のため各部にダイヤルイン番号及び FAX 番号を設定し、１人１台の PHS 電話 158 台を構内コードレス電話と社外 PHS として活用して事務所と社外間の通話を無料とし、山間部や高速移動中の通話のため携帯電話９台を配備していた。費用は年間７百万円である。

利用状況の調査分析に基づき、次のとおり再構築した。固定電話では IP 電話サービスを

利用して、ダイヤルイン番号を全員に付与し固定電話発信で相手先に直通番号を表示することとし、通話料を全国３分８円と低減するとともに、親会社やグループ会社と同じ通信事業者を利用して通話料無料化を実現した。社外は携帯電話１社に統一して安価に調達し、公私分計サービスによる個人携帯電話の活用と社外利用実績に基づく必要台数を算定して、社外利用契約台数を大幅に削減した。事務所と携帯電話間では、携帯電話事業者の固定電話回線を利用することで通話料を無料化し、構内交換機の追加番号ダイヤルイン機能を活用することで、携帯電話と事務所の各人との直通通話を実現した。

再構築が完了した 25 年度からは基本料は３百万円、通話料などは百万円、計年間４百万円と６割のコスト削減を実現するとともに、個人直通着信の転送ができる、覚える電話番号が実質一つになるなどの利便性向上や電話取次業務の減少などの効果があった。携帯電話に関しては新たに通話定額プランなども提供開始されたが、当社では携帯電話 1 台当りの月額は 1150 円であり、３年が経過した現在もコスト削減効果は継続している。

（２）コンピュータ関係の再構築

従来は光回線のインターネット接続(IP アドレス 16 個)を行い、システムとしてはグループウェアやセキュリティ関係システムを自社導入し、運用保守は外部委託していた。インターネット回線費用、サーバなどの運用保守費用は年間 11 百万円である。

事業継続対策や情報セキュリティ強化を考慮すると、データセンターのセキュリティサービスを活用することが将来的に有効と考えられることから、自社導入システムを代替できるセキュリティサービス利用に変更して、サーバ台数削減とそれに伴い IP アドレスを８個に縮小した。

再構築が完了した 25 年度からはインターネット回線費用やシステム保守料、運用委託費用の減少と、セキュリティサービス利用料金の増加による差引で年間３百万円のコスト削減を実現した。最終の情報セキュリティの強化に関しては、今回導入したデータセンターのセキュリティサービスの追加サービスをうまく活用することで安価に実現するなど、３年が経過した現在もコスト削減効果は継続している。

（３）コピー･FAX･プリンタ関係の再構築

従来は、コピー機はコピー･プリンタ･スキャナ･FAX 機能を持つ複合機を導入して必要最小限の台数とし、高価なカラー機は共用としてフロアに１台程度４台設置し、モノクロ機は高速機を共用としてフロアに１台ずつ３台設置し、各部に通常機を１台設置してコピー･プリンタ･スキャナ･FAX として活用した。報告書印刷が多いためモノクロレーザープリンタを各部１台程度、15 台設置していた。費用は年間 11 百万円である。

カラー複合機の印刷の７割はプリンタ利用であるため、各部に印刷単価の安いカラーレーザープリンタを導入してカラー印刷機能を変更するとともに、コピーや FAX 受信をできる限り電子データ化して印刷を必要最小限とした。

再構築が完了した 25 年度からは複合機とレーザープリンタの印刷単価差やレスペーパー化などにより、カラーで７百万円、モノクロで百万円、計年間８百万円と７割のコスト削減を実現するとともに、機器台数増加によるカラー印刷の利便性向上や可用性向上などの効果があった。３年が経過した現在では、研究報告書などのカラー印刷枚数はますます増大しており、コスト削減効果は更に大きく増加している。

## ４．３　効果実現の考察

（１）要因の考察

この全社最適化によるコスト削減で効果を発揮できた要因は、

①日常的に利用している電話、コンピュータ、コピーなどについて、使用量や料金だけでなく、どのように利用しているか使用状況を詳細に調査・分析して改善したこと

②固定電話、携帯電話、コンピュータ、コピーなどを個別に考えたため効果が出なかったものを、全体を一体の関連するシステムとして全社最適を目指して検討したこと

の２つであると考えている。その理由は次のとおりである。

今回実施した「050IP 電話の活用」や「携帯電話への統一」は過去に担当部署が通信事業者から提案を受けたものである。提案内容は１社で提供できる機器やサービスに限られるため、050IP 電話は固定電話だけ、携帯電話は PHS の取替だけの提案となり、その提案だけではメリットがなく、採用できなかったということである。今回は使用状況を詳細に分析し、携帯電話を含めた電話関係全体で一体のシステムとして検討することによって、大きなメリットを出すことができたからである。

（２）実施手法の有効性の検証

25 年度下期に当社事例を聞いた、四国内 20 数ヶ所の事業所がある、従業員 240 名全員が携帯電話を利用する会社から携帯電話のコスト削減のコンサル依頼があった。実施した結果、従来は携帯電話会社提案による料金プランにより月額 120 万円で利用していたが、当社コンサルにより従業員の携帯電話の利用方法を変更せず月額 70～80 万円に削減でき、当社手法の有効性が実証されるとともにコンサルビジネスの展開につながった。コンサルビジネスを展開できたことにより数百万円の利益を獲得することができ、システム構築のプロジェクトが進めやすくなった。

（３）コスト削減のチェックポイント

コンサルビジネスなどを通してアンケート調査やヒアリングを行ったことから、いろいろな会社の状況を把握することができた。当社やコンサル受注した会社だけでなく、ほとんどの会社で同様のコスト削減の可能性があることが判明した。これらの結果からコスト削減のチェックポイントをまとめる。

どの会社でも社員皆が利用している、電話関係、コンピュータ関係、コピー関係などでコスト削減できるかどうかの大きなチェックポイントは次の３つであると考える。

①担当部署は分かれていないか

つまり、個々の部署ごとの個別最適になっている可能性がある。

②実績把握は使用量や料金だけではないか

つまり、使用状況が把握できていないため、最適な料金プランでない可能性がある。

③提案と競争見積だけで決めていないか

つまり、提供者が都合よく、利用者にとって適したものになっていない可能性がある。

これらのポイントに該当することがあれば、コスト削減できる可能性があると考える。

# ５．WindowsXP サポート終了への対応

## ５．１　WindowsXP パソコン継続使用への対策

（１）WindowsXP サポート終了への対応と課題

WindowsXP サポート終了時に Windows７パソコンへ取替する予定であったが、研究開発用ソフトや周辺機器が WindowsXP だけでしか稼動しないものがあることが判明し、蓄積した計測・解析結果の継続性などから WindowsXP パソコン 40 台の継続使用が必要となった。WindowsXP パソコン継続使用のためネットワーク接続や外部接続媒体などのリスク発生経路をすべて遮断することとしたが、研究開発のために必要な情報収集やデータ連携の課題が発生した。

（２）WindowsXP パソコンのセキュリティ確保対策

WindowsXP パソコンのリスク発生経路を遮断し、かつ、必要な情報収集やデータ連携を実現するために、WindowsXP パソコンを既存の社内 LAN と分離した閉鎖 LAN に接続した。原則他の機器などとの接続を禁止し、操作ログの収集、状態監視などを行う管理システムと、外部と接続するためのシンクライアントのゲートウェイ装置（SSL-VPN 装置）との接続だけを許可することで、リスク発生経路を遮断し、研究開発に必要なデータ連携だけをセキュリティを確保して実現した。システム構成を図２に示す。

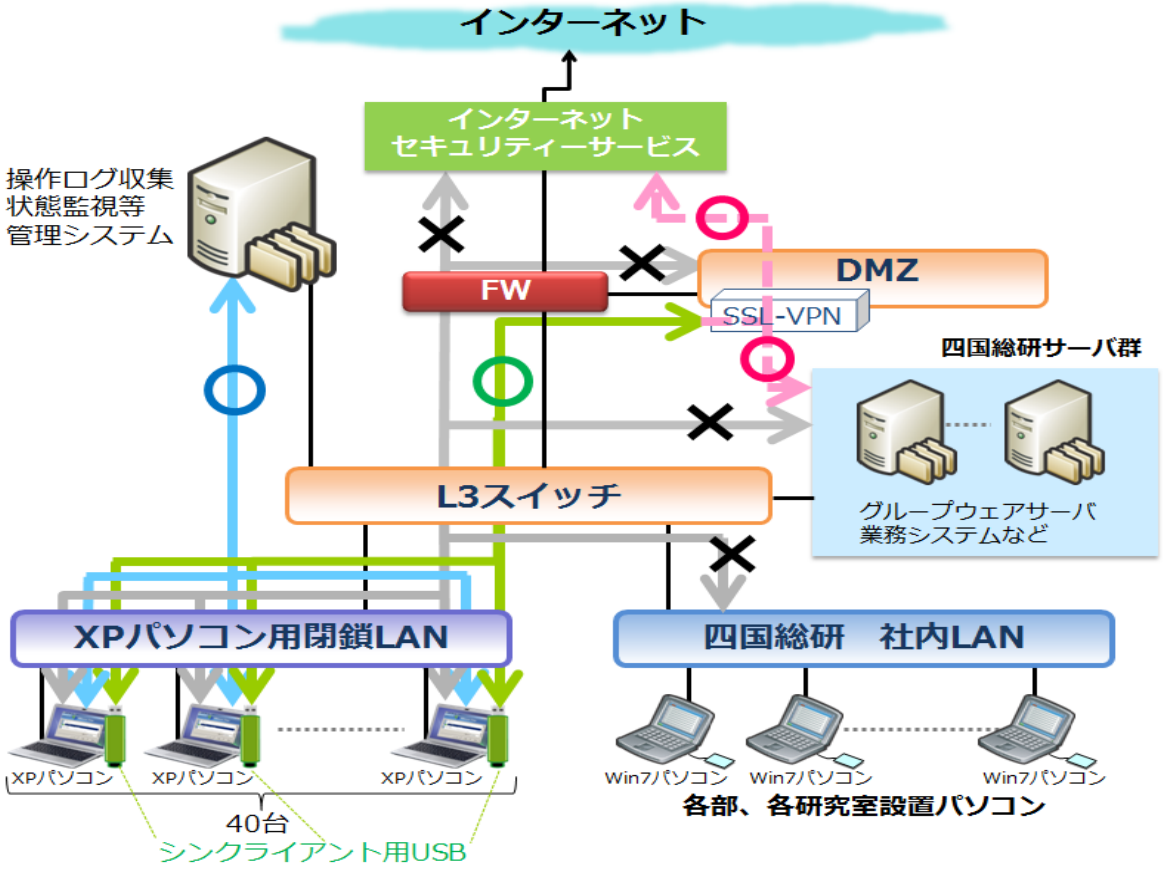


図２　WindowsXP パソコン用閉鎖 LAN のシステム構成図

（３）対策の効果

本対策により、WindowsXP パソコンをセキュリティを確保して継続使用することが可能となり、蓄積した計測・解析結果を活用できるとともに、ソフトや周辺機器の変更やシステム改修の費用削減とパソコンを２年程度延命でき、６百万円以上削減することができた。WindowsXP パソコンの継続使用が必要な期間は実施中の研究開発テーマ完了までであり、通常テーマは３～５年のため、３年経過した現時点では WindowsXP パソコンはほとんどなくなっている。

また、ここで使用したシンクライアントシステムは事業継続対策などを実現するために必要となる社外利用システムでの活用も考慮して導入したものである。

システム環境の移行に関しては、特殊な開発用ソフトや周辺機器などを蓄積した計測･解析結果の継続性から利用せざるをえない事態は今後も発生すると考えられる。今回の対策手法は当社で今後も活用できるとともに、当社以外でも、諸事情により旧型パソコンなどを継続使用せざるをえない場合にはシステム環境移行時対策として活用できると考えられる。

## ５．２　全社ファイル共用サーバシステムの構築

（１）パソコン取替に伴うデータ移行の効率化と全社情報共有の促進

26 年４月の WindowsXP サポート終了に対応できるよう、25 年度中に継続使用せざるをえない WindowsXP パソコン 40 台を除く WindowsXP パソコン 165 台を Windows７パソコンに取替する。パソコン取替に当たっては既存 WindowsXP パソコンのハードディスク保管データを新たな Windows７パソコンへ移行する必要がある。

ここで、データ移行を効率的に実施することと、事業継続対策や情報セキュリティ強化などを考えると、単に旧パソコンから外付けハードディスクなどを経由して新パソコンにデータ移行を行うのではなく、重要データの遠隔地保管や情報セキュリティ強化の実施、業務効率化のための情報共有の促進を実現するため、全社ファイル共用サーバシステムを構築して、データ移行の作業量を削減するとともに、重要データの情報共有化を促進することとした。

（２）全社ファイル共用サーバの構築

全社ファイル共用サーバは全社･部･課・グループごと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し、個人別フォルダは１人 50GB を確保する。全社ファイル共用サーバは 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、高い信頼性を確保する。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た。なお、データ移行作業用に関しては臨時で容量追加も実施した。

パソコンなどに重要データを保管しなくてもよいシステム環境を整備し、これまで各部で独自に設置したファイル共用サーバやパソコンに保管していた場合には困難であった重要データを全社統一したシステム環境で管理、保管することを実現するとともに、各部や研究員が実施する必要のあった重要データのバックアップ作業から解放した。全社ファイル共用サーバのシステム構成を図３に示す。

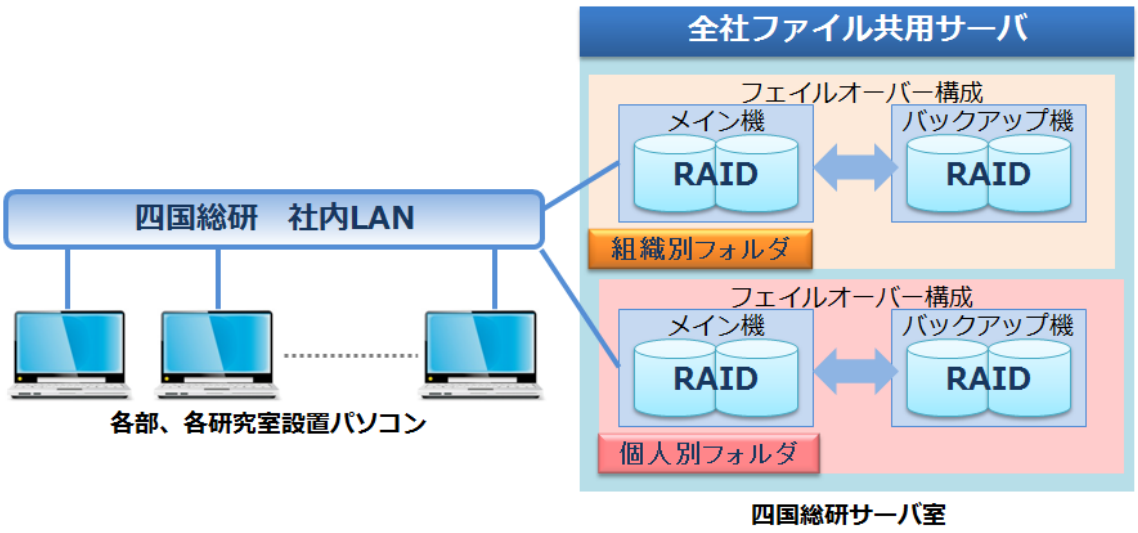


図３　全社ファイル共用サーバシステムの構成図

（３）コスト面での評価

全社ファイル共用サーバを構築して実施したデータ移行及び情報共有化作業は、単純にWindowsXP パソコンのハードディスクに保管されているデータを取替する Windows７パソコンのハードディスクに移行する場合と比較すると、データ移行を行う場合の外部ディスク購入費用と全社ファイル共用サーバ構築費用の差と、全社ファイル共用サーバ利用による百数十名の１人当り２時間程度のデータ移行作業の時間短縮効果がほぼ同等であり、費用的には同じでコストの増分はない。

## ６．大規模災害などの対応、情報セキュリティ強化などの実現

### ６．１　事業継続対策

（１）事業継続対策のためのシステム要件

大規模災害対応の事業継続対策のためには、「重要システムの継続稼動」と地震や土砂災害、パンデミックなどで会社に出勤できなくともシステムを利用して業務ができる「システム利用環境の整備」が必要となる。重要システムの継続稼動を実現するには、継続稼動できるシステム環境での「重要システムの再構築」と「重要データの遠隔地保管」が必要となる。システム利用環境の整備を実現するには、継続稼動対策を含む「社外利用システムの整備」が必要となる。

事業継続対策のシステム構築をいかに行うかの基本的な考え方は次のとおりである。大規模災害発生時でもシステムが継続稼動できるには、免震装置などの建物設備、長時間停電に対応できる自家発電設備などが必要となる。当社事務所にはこのような設備はなく、30 年以上を経過するビルに新たな設備を設置することは困難であることから、必要な設備のあるデータセンター活用が現実的である。実施コストを見積ると、自社の設備設置よりもデータセンター利用の方がはるかに安価であったことから、データセンターを活用して事業継続対策を実現する。

（２）重要システムの再構築

当社として緊急事態時に稼動が必要な重要システムのうち、受注管理、経理・資材・人事労務などの基幹業務システムに関しては、四国電力グループで連結決算対象会社を含めて構築している「四電グループ総合業務システム」を利用しており、この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り事業継続対策済みである。このため、当社が管理する重要システムは、情報共有などを行う「グループウェア」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、メール、DNS」などである。研究開発用システムは事業継続の考え方で述べたように緊急事態時に稼動する必要性がなく対象外である。

データセンターを利用してシステムを構築することとしたが、セキュリティに関する懸念があった。インターネット網用と社内 LAN を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ことなどから、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構築する。

従来システムと今回のデータセンターを活用したシステムを構築・運用・保守を含めた５年間の費用で比較すると８百万円のコスト削減を実現するとともに、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た。

（３）重要データの遠隔地保管

WindowsXP サポート終了に対応するため構築した全社ファイル共用サーバの構築により、重要データは全社統一したシステム環境で管理できたことから、大規模災害発生の際にも重要データが継続利用できるよう、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システム環境を整備する。重要データを遠隔地保管するシステム構成を図４に示す。

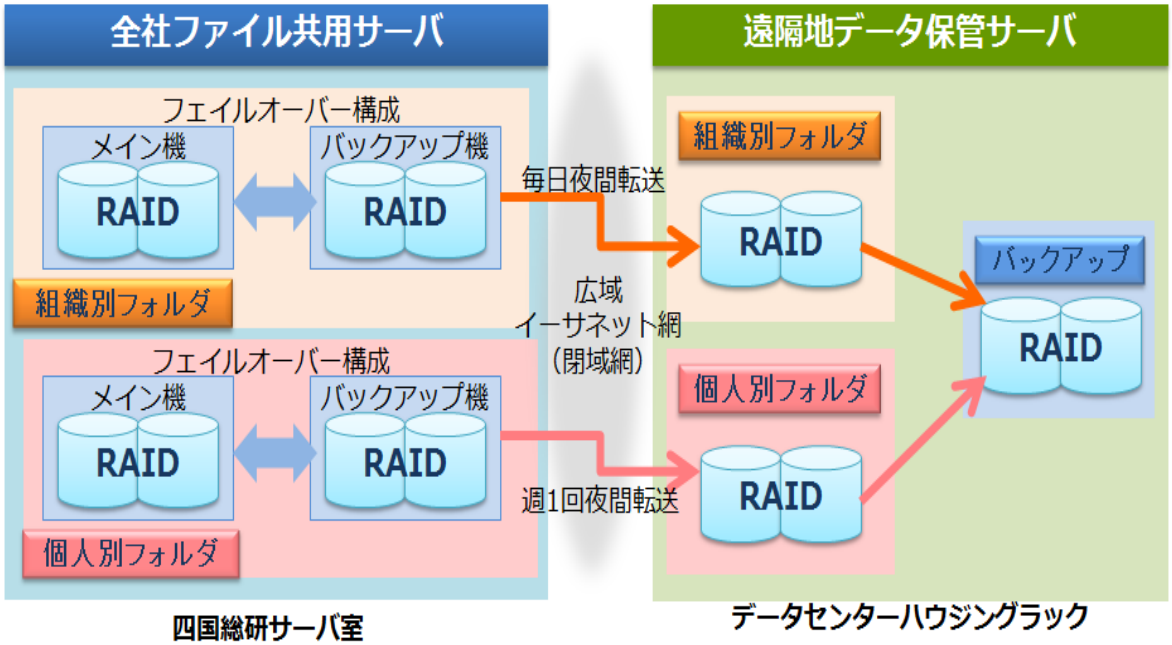


図４　重要データの遠隔地保管のシステム構成図

（４）社外利用システムの構築

社外利用システムは、社外から情報漏えいリスクをなくし安全に必要なシステムが利用できることが求められる。WindowsXP パソコンで構築した既存の出張時システムの再構築が必要であること、いざという緊急事態時に活用できるためにはシステムを日常的に利用していることが必要であることから、在宅勤務やアイデア発想時の通常時利用システムも含めて、一体で考えて構築する。システム負荷を考えると、通常時には同時アクセスは多くないが、緊急時は対象者のほぼ全員利用となり、非常に多数となるため、緊急事態発生時の同時アクセスに対応できるシステム構成が必要である。

社外利用の情報漏えいリスクをなくすには、社外利用の端末機器にデータを保管せず、暗号化通信で通信データが漏えいしないようにするシンクライアントシステムが有効である。シンクライアントシステムを構成する場合、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。

・端末機器は、緊急事態発生時に出社が困難となった場合などは自宅にあるパソコンが活用でき、出張時などには持出パソコンやホテル設置のパソコンが利用できる。
・通信回線は、自宅では高速インターネット回線、ホテルでも高速インターネット環境、屋外でも WiFi、LTE など高速通信回線が利用できる。

これらの資源を有効に利用できるシステム構築を考えることでシステム構築にかかる費用を抑制することができる。

残る課題はシステム構築･運用コストであるが、緊急時の同時アクセスの急激な増大に対応できるサーバ準備は膨大なコストである。緊急時利用はシステム稼動中に発生しない可能性があり、中小企業では投資は困難であることから何らかの対策が必要である。

シンクライアントシステムを詳細調査し、その一方式である「仮想シンクライアントシステム」は端末側のハード･ソフトを利用するがハードディスクなどにデータは残らない。利用できるアプリに制限はあるが当社が必要なものは利用でき、安価である。この仮想シンクライアントでコストの課題を解決できる。

実装の詳細はベンダーにより異なるが、システム構成は概ね同じである。当社で導入したシステムでは、端末側でシンクライアントとして動作するソフト(USB キー起動)と、連動するセンター側のゲートウェイ装置(SSL-VPN 装置)で構成する。

システム構築･運用コストであるが、社外利用システムの構築は既存の出張時システムの再構築であることから両者を比較すると、５年間費用は社外利用システム８百数十万円、出張時システム９百万円であり、百万円弱の削減を実現している。社外利用システムは全員が利用可能で１利用者当たり月額千円のコストである。

大規模災害など発生の際にもシステム利用環境の継続稼動を確保するため、社外利用システムに使用する SSL-VPN 装置などの機器を全社ファイル共用サーバシステムの遠隔地データ保管サーバと同じデータセンターのハウジングラックに 27 年５月に設置し、大規模災害時などでも従業員のシステム利用環境の継続稼動を確保している。

仮想シンクライアントシステムの利用イメージを図５に示す。

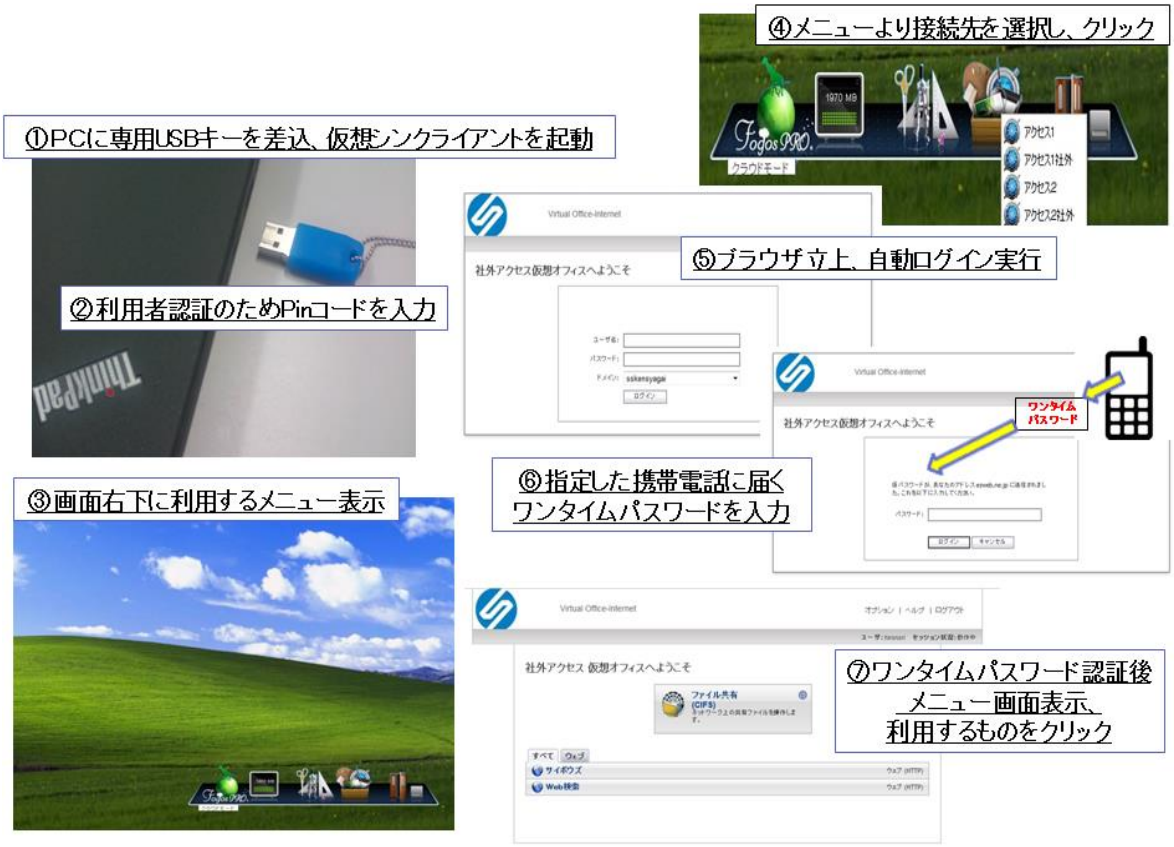


図５　システム利用イメージ　画面展開図

社外利用システムに関して、アイデア発想時や出張時などでは資料などの参照だけでよい場合も多いので、センター側に導入した SSL-VPN 装置を活用して、ユーザーが簡単に利用できるスマートフォンを使用するシステムも構築している。セキュリティ設定を集中管理でき、データを一切保管しないセキュアブラウザをスマートフォンに導入し、センター側ではパソコン使用の場合と同様に、セキュリティ機能強化をはかるため、セキュアブラウザ、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いる。利用方法はブラウザを起動して ID とパスワードを入力するが、それ以降はパソコン使用の場合と同じである。このスマートフォン利用のシステムも機器代・通信料を含み１利用者当り月額千円のコストである。

## ６．２　情報セキュリティ強化

当社は「よんでんグループ情報システムセキュリティガイドライン」に基づき 27 年度末までに四国電力と同程度のセキュリティレベルを確保できる「更なる取組」を達成することが求められており、このため、表２に示すシステム面での技術的対策を実施している。

今回、IC カード、外部記憶媒体の利用制限、社外電子メール添付ファイルの自動暗号化などを追加したが、データセンターのセキュリティサービスの有効活用、パソコン台数の削減、一括購入などにより、対策費用全体は従来と同程度に納めることができた。

表２　技術的対策としての主な実施事項

| 項　目 | 実　施　内　容 |
|---|---|
| ①アクセス制御 | ・利用者認証ではICカードによるログイン、社外ではワンタイムパスワードによる認証、電子証明書による認証を実施<br>・アクセス管理では、利用者のアクセス権限付与をルール化し、付与対象者やレベルを必要最小限とし、定期的に確認を実施<br>・インターネット利用では、接続ルールを整備し、ファイアウォールによるアクセス制限の実施、コンテンツフィルタによる不要なWebサイト等の閲覧禁止、適切に機能していることの定期確認を実施。<br>・インターネット侵入検知･防護システム等によるリアルタイムの監視･遮断<br>・社内ネットワークでは、接続ルールを整備し、セグメント間の端末接続制限、許可端末以外LAN接続できない接続制限を実施 |
| ②不正ソフトウェア対策 | ・原則全てのパソコン、サーバーにウィルス対策ソフトの導入とネットワークでWeb・メールのウィルス対策を実施。<br>ウィルス対策ソフトの起動･パターンファイルの更新確認を実施。<br>・セキュリティパッチ管理では適用の必要性を見極め、<br>原則、最新セキュリティパッチを適用し、状況の定期的確認を実施。 |
| ③情報漏洩対策 | ・暗号化等では、適用可能なハードディスクは暗号化し、外部記憶媒体は利用制限と書出し暗号化を行い、社外電子メール添付ファイルの自動暗号化<br>社外持出機器への原則データ保存禁止を実施。 |
| | ・証跡管理では、万一漏洩した場合の対応ルールを定め、<br>社外電子メールの一定期間保存の実施 |
| ④アクセスログの取得･分析 | ・サーバーのアクセスログやパソコンの操作ログの取得を実施し、一定期間保管するとともに、定期的および必要に応じてアクセスログの分析を実施。 |

日本ネットワークセキュリティ協会「2015 年情報セキュリティインシデントに関する調査報告書」によると企業からの情報漏えい原因のうち圧倒的に多いのはパソコンなどの紛失・置忘れ、誤操作、管理ミスなどのヒューマンエラーということである。

これらへの対応を社外利用システムを例に説明する。ハードディスクなどにデータを保管せずパソコンが紛失しても漏えいする情報がないようにし、社内との通信は暗号化通信を行い通信回線上の漏えいをなくして基本的に情報漏えいリスクを防止している。誤操作や管理ミスなどによる専用 USB の不正使用やネットワークの不正アクセスなどを防止するためワンタイムパスワードなどセキュリティ対策を多重的に追加するほか、フェイルセーフとなるようシステム構築を行っている。

しかし、セキュリティシステムを構築したり、ルールで禁止を行っても利便性が維持されていないと、隠れたルール違反が発生するなど意図的な情報漏えいリスクが高まるので、利便性の維持向上を図っている。具体的に、WindowsXP サポート終了への対応、社外利用システムの事例で説明する。WindowsXP サポート終了対応では、計測・解析結果の継続性などから継続使用が必要な WindowsXP パソコンを安全に利用できる仕組みを構成して利便性を維持し、危険な WindowsXP パソコンを隠れて使い続けることを防止している。社外利用システムでは、これまで重い出張時専用パソコンを持参する必要があったものを軽い専用 USB やスマートフォンでの利用を可能とするシステムを整備して、必要時に社外から必要な情報に簡単にアクセス可能とする利便性を向上させることで、ルール違反による意図的な情報の社外持出を防いでいる。

# ７．システム構築の評価とポイント

## ７．１　システム全体概要と評価

３年間の情報通信システム構築で、目的とする大規模災害への対応、情報セキュリティ強化などの機能向上を実現したシステム構成を図６に示す。

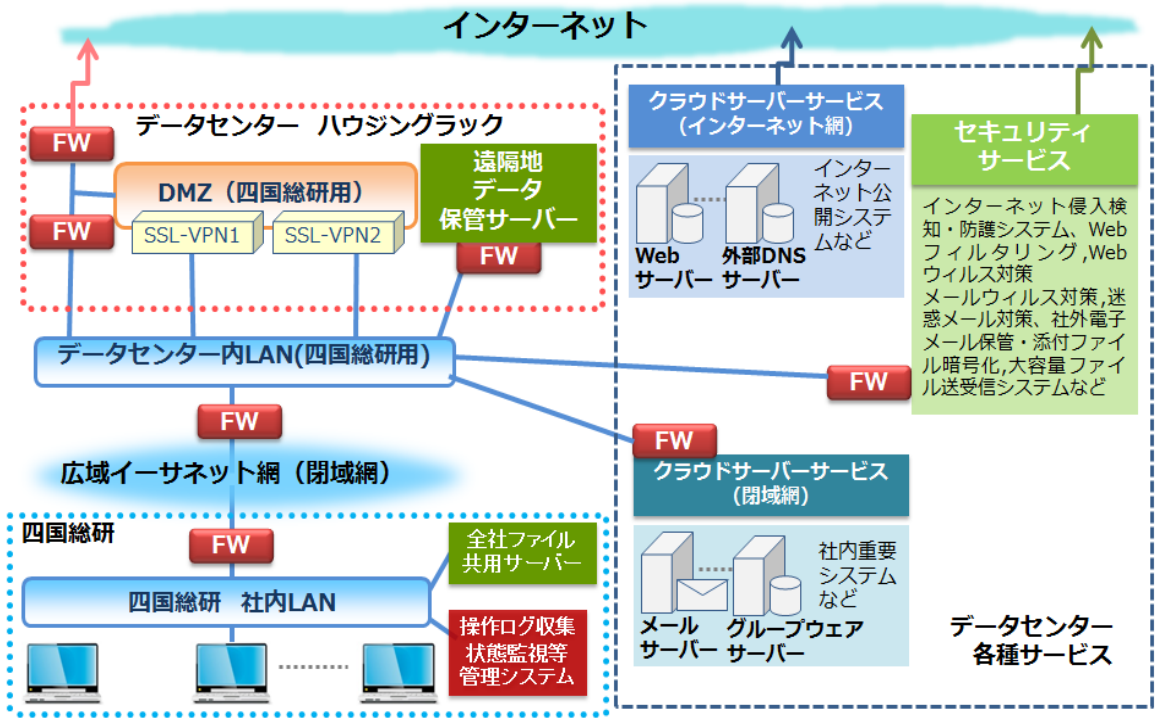


図６　構築したシステム全体構成図

定量的効果として、実現したコスト削減をまとめると、関係する情報通信システムで年間 15 百万円の削減と５年間費用 15 百万円を削減（年間では３百万円に相当）したことから、合計すると年間 18 百万円のコスト削減の実現である。

定性的効果は次のとおりである。

事業継続対策に関しては、27 年７月の台風 11 号が四国上陸し香川県を直撃した際に、対応訓練を実施して機能どおり稼動することを確認した。自宅パソコンの使用など通常時からの利用確認の重要性が再確認されたことから、定期的に通常時での利用、重要データの確実な保管などを実施するよう周知･啓蒙を行い、確実に機能するようにしている。

情報セキュリティ強化に関しては、情報漏えいリスクは従来より大幅に低減しており、万一の情報漏えい防止効果は非常に大きい。

ワークスタイル変革対応に関しては、社外利用システムを活用することで、26 年 10 月の在宅勤務制度開始にあわせた適用はじめ問題なく対応できており、高度な知識･技術を有する研究員を有効活用できるなど研究開発推進に大きな効果がある。

業務の効率化、利便性の向上に関しては、社外利用システムを活用することで研究開発アイデア発想時に必要な資料･データが参照できることによる時間短縮効果をはじめ、日常業務の中で有効に機能している。

ユーザーからは日常業務の遂行に関して、

・出張先、外出先や自宅から、資料の参照、メール･スケジュールの確認ができる

・バックアップ作業の削減、人事異動や組織変更の際の資料確認や移管業務の軽減

・パソコンや資料・データの紛失などを心配せず仕事に専念できる安心感がある

という評価を受けており、効果としては定量的効果より定性的効果が大きいと考えている。また、システムの全社最適化によるコスト削減はコンサルビジネスの展開にも繋がった。

## ７．２　システム構築のポイント

今回のプロジェクトにおけるシステム構築のポイントは大きく２つである。一つは、利用状況を詳細に調査分析するとともに、システムの対象とする業務を広く捉え、会社全体のシステムと見ることで全体最適をはかったことであり、もう一つは、データセンターをうまく活用することで目的とする機能向上を安価に実現していることである。

一つ目の全体最適をはかるポイントは、「システムの全社最適化によるコスト削減」や「社外利用システムの構築」などで説明しているので、ここでは２つ目のデータセンター活用のポイントを説明する。一ヶ所のデータセンターを利用する場合のポイントは、目的に応じて、データセンターをいかに選択するかがポイントと考えている。

今回の目的は、事業継続対策と情報セキュリティ対策である。情報セキュリティ対策については、セキュリティベンダーの機器やシステムを共同利用することなどによるネットワークを通したサービス提供であり、サービス内容についてデータセンターによる相違はほとんどないと考えられるが、事業継続対策に関しては、いろいろな相違がある。

まず、事業継続対策においては、データセンターが万一の災害時にも稼動していることが大前提となる。日本はどこでも地震は発生することから、大規模地震にも対応できるかを確認することが第一である。これはデータセンターの公開されている設備などの仕様を調べることで、想定される大規模な南海トラフ地震などが発生しても機能継続できるよう、免震装置などの建物設備、複数ルートの通信回線設備、複数変電所からの受電設備、長時間給電できる自家発電設備などを設置しているかなどを確認でき、多くのデータセンターは満足していると考えられる。

当社検討結果では、事業継続対策のためのデータセンターを選択するポイントは、ネットワーク、設置場所と現地作業場所、ハウジングサービスの３つがあると考えている。

（1）ネットワーク

ネットワークに関しては、通常時はデータセンターと自社事務所との間のネットワークであり、ネットワーク障害はほとんど発生せず、発生してもすぐに復旧できるので問題はない。大規模災害発生時には、利用場所が自社だけでなく、従業員の自宅などからの利用もあることから、データセンターと利用場所間のネットワークが利用する通信回線の経路などの検討が必要である。東日本大震災を考えると、海底ケーブルの切断が大量発生しているほか、被災地域と他の健全地域との間では急激に大量通信要求が発生して、通信容量不足となっている。データセンターが利用するプロバイダーと事務所や従業員自宅が利用するプロバイダーが異なると、データセンターと事務所や従業員自宅とが通信する場合、相互接続点のある東京や大阪などで接続して、折り返して通信することになる。つまり、利用する地域と東京、大阪間の往復通信を行うことになり、通信容量不足が大きく影響す

る。したがって、大規模災害発生時にデータセンターと事務所や従業員自宅との通信が円滑に行えるネットワークとなるように考慮して、データセンターを選択する必要がある。

当社の場合で考えると、想定する第一の大規模災害は南海トラフ地震であり、利用場所は高松である。データセンターが四国外にあると、データセンターと通信する際には四国と本州を結ぶ瀬戸大橋、鳴門大橋、海底に敷設された光ケーブルを経由するしかないため、四国と他の健全地域との間では通信容量不足が大きく影響することとなる。データセンターが四国内にあっても、データセンターが利用するプロバイダーと当社事務所や従業員自宅が利用するプロバイダーが異なると、四国と東京、大阪間の往復通信を行うことになり、通信容量不足が大きく影響する。従業員自宅が多く利用しているのは、地域で料金が安価な光ネットワークやCATVネットワークを提供するプロバイダーであり、当社事務所も同じプロバイダーを利用していることから、利用するデータセンターは高松にある同じプロバイダーを利用できるところを選択して、南海トラフ地震などの大規模災害時でも必要な通信が確保できるようにしている。

（2）設置場所と現地作業場所

設置場所に関しては、データセンターはネットワークを介して利用することから、通常時は設置場所はどこにあってもよく、データセンターで作業する必要は基本的にない。しかし、大規模災害が発生した際に、利用場所が同時被災する場合はすべてのネットワークが不通となる可能性がある。その際には、データセンターに行き最低限の業務実施を行うなど、何らかの手段でデータセンターにあるシステムが活用できる必要がある。したがって、利用するデータセンターは大規模災害発生の際に必要な要員が移動できる場所にあるか、データセンターにおいて業務が実施できる作業場所が提供されているかなどを考慮する必要がある。

当社の場合、利用場所が本社一ヶ所と従業員自宅などであり、高松及び周辺地域という一つの地域となることから、大規模災害発生の際には、すべてのネットワークが不通となることが考えられる。したがって、利用するデータセンターは大規模災害発生の際に必要な要員が移動できる場所にあるデータセンターであり、データセンターの現地でシステム利用などの業務が実施できる作業場所が提供されているところを選択する必要がある。当社ではデータセンターにおいて業務実施が可能な高松にあるデータセンターを活用している。

高松のデータセンターということで同じ都市で大丈夫かという疑問を持たれる可能性がある。これに関しては、同じ都市でも断層など地形的なことを考慮すれば同時被災することはほとんどないこと、データセンターそのものは大規模地震に対応できるかどうかを確認していることから問題はないと考えている。

（3）ハウジングサービス

事業継続対策には遠隔地データ保管が必要で、重要データをデータセンターに保管をしておくことで、万一の際にも重要データが失われないようにしている。これを活用するには、ネットワークにより利用するか、設置場所に行き利用することができるので、活用するという機能面ではネットワークや設置場所を考慮していることでよい。しかし、保管する重要データのデータ量は増大しており、今後も増加していくことが容易に想定できるこ

とから、コストの面で考慮する必要がある。

データセンターではデータ保管サービスの提供があり機能面で問題はないが、料金面で考えると問題がある。データ保管サービスは更新・参照周期も短く活用頻度の多いデータを利用する場合はよいが、更新・参照は少ない大量データを保管したい場合には非常に高価となる。大量データを安価に保管する目的で考えると、データ保管サービスを利用するよりも、ハウジングサービスを利用して NAS などの機器を必要とする機能レベルに応じて自社設置した方が安価に実現できる。したがって、大量の遠隔地データ保管を考えるとハウジングサービスも利用できるかどうかが考慮点である。

当社が利用しているデータセンターではハウジングサービスがあり、更新の少ない大量データについては当社設置の NAS を使用して安価にデータ保管を実現している。

## ８．おわりに

28 年４月の熊本地震や８～９月の東北･北海道の大雨･土砂災害の発生、大手企業での情報漏えい事件が発生して、事業継続対策や情報セキュリティ対策の実施の必要性が増す一方で、英国の EU 離脱や IS などによるテロの多発、急速な円高の進展などで不透明な経営環境にある各企業の現在の状況は、当社の 24 年当時の状況に近いのではないかと思われる。当社の取組が、厳しい状況の中、事業継続対策や情報セキュリティ対策などを実施しようとする企業の参考にしていただけるのではないかと考えている。

今回の取組を通して強調しておきたいことは、システムの機能向上がコスト削減と両立して実施できることである。東日本大震災や平成 28 年熊本地震にみられるように大規模災害はいつ発生するかわからない、普段からの備えが重要である。事業継続対策と情報セキュリティ強化は自社のためだけでなく、できていないと万一の際にはお客さまや取引先をはじめとする社会全体に影響を与えることになる。大企業はもちろんのこと、中小企業においても工夫することで多くのコストをかけずとも事業継続対策や情報セキュリティ強化は実施可能である。当社事例などを参考にしていただき、システム更新などの機会を捉えて、各企業とも実施していただきたい。

当社の今後の取組としては、システム高度化や利便性の向上を推進して競争力強化につなげていくとともに、各企業の事業継続対策や情報セキュリティ強化が推進されるよう要望があれば事例紹介を行い、コンサルティングにも応じていきたいと考えている。

以　上

## 参考文献

[1] NPO 日本ネットワークセキュリティ協会「2015 年 情報セキュリティインシデントに関する調査報告書」　４ページ　図３原因別の漏えい件数
参考 URL:http://www.jnsa.org/result/incident/data/2015incident_survey_sokuhou.pdf