コンタクトセンターの情報管理強化事例
セキュリティ強化と業務効率化について

富士通コミュニケーションサービス株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

篠原　誠志

2000年　富士通コミュニケーションサービス（株）入社
　　電話オペレーター業務担当
2002年　社内イントラ管理業務担当
2007年　現在 部門内システム・セキュリティ管理担当

山本　龍洙

2000年　富士通コミュニケーションサービス（株）入社
　　電話オペレーター業務担当
2002年　社内イントラ管理業務担当
2007年　現在 部門内システム・セキュリティ管理担当

■ 論文要旨 ■

当社事業所の中で最も規模の大きい、北九州サポートセンターにおける各種情報セキュリティ強化に対する施策をご紹介する。

昨今、インフォメーションワーカーとして事業展開するコンタクトセンターに対し、情報セキュリティの強化に対する要件はますます高くなっており、クライアントから提示される要件も厳しくなっている。

当社はそれら各種要件に対応すべく、事業所移転を契機にビルの設計段階からセキュリティ基準を見直し、堅牢なセキュリティ設備への投資や、システム運用における工夫を施し、対策・強化を行った。

その中で講じた対策は、場当たりなものではなく、今後、中長期的に見ても有効且つローコスト化を見据えていたため、大変有用なものとなった。

本論文では、人的要素や物理的要素、システム的な要素など、様々な視点・観点から取り組んだ情報セキュリティの強化事例についてご説明する。

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

富士通コミュニケーションサービス株式会社(以下、当社)は、富士通グループにおいて、コンタクトセンターサービスを中核とするアウトソーシングビジネスを展開し、天王洲、川崎、北九州、新潟、松山に拠点を持つ、従業員数約 2400 名(2007 年 3 月末時点)の会社である。

1994 年の創業以来、情報技術（Information Technology）領域をはじめ、非技術系の業務プロセスサポートに至るまで、幅広い領域で事業展開を図っており、現在 400 社以上のお客様へ、そのサービスを提供している。

当社は、個人情報保護ポリシーとして、JIS Q 15001 に準拠した個人情報保護に関するコンプライアンス・プログラムを制定し、2006 年 5 月 25 日付けで日本情報処理開発協会（JIPDEC）から「プライバシーマーク」を取得しており、また新潟サポートセンターの全業務を認証対象範囲として、国際的な情報セキュリティマネジメント規格「BS7799-2:2002」並びに、これに準拠する国内規格「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」の認証（ISMS 認証基準 Ver.2.0）を取得している。

１．２　北九州サポートセンターの特徴

「北九州サポートセンター」は、当社の中で最大規模(約 700 席)かつ、唯一の 24 時間稼働で運営する事業所である。

この事業所となるビルは、一棟借りをしており、さらに、コールセンター専用設計となっている。設計段階から当社のスタッフが携わり、セキュリティ確保しながらも、業務において効率的な動線を確保できるよう工夫をこらしているのが特徴である。

２．背景

２００５年４月の個人情報保護法施行後、多くの企業において情報セキュリティの強化が重要視された。

当社においても特に、多くの個人情報を取り扱っている部門、部署が存在する「北九州サポートセンター」では、業務を遂行する上で、より一層のセキュリティ強化と、適切な情報管理体制を要求された。

「北九州サポートセンター」は、２０００年９月に雑居ビルの２フロアを使用して、オープンした。

その後、業務を拡大し、２００４年には４フロアを使用する規模となる。

しかし、同業務を複数フロアで実施することは、人や物の移動が頻繁に発生することを意味しており、そのリスクも課題であった。

２００６年１０月に、さらなる事業拡大を目的とし、「北九州サポートセンター」は事業所移転をすることとなる。

その物理的な変化を契機に、ビル設備やシステム、体制の見直しを図り、様々なセキュリティ強化施策を実施したので、以下に紹介する。

２．１　事業所移転前の情報管理体制

ビルに関するリスクについては、「背景」でも記述したとおりである。複数に分かれている業務エリアでは、セキュリティレベルを統一することが困難であった。

また、ビルの共用部分など、他社も使用するエリアが多く存在し、事業所内のセキュリティ設定をさらに困難にしていた。このような、物理的な問題に加えて、内部の体制にも課題があった。

当初、我々は社内要件やクライアント要件にあるセキュリティチェック作業、監査用エビデンスの作成といった必要最低限の作業を、最小限の人員で実施していた。

また、各情報セキュリティ強化に対する施策は、各担当者において独自で管理されており、部門を横断した施策や管理が十分ではなかった。

以上の状況で発生した問題点とその原因をまとめると以下のようになる。

２．２　情報管理体制の問題点と原因

- 情報セキュリティに関する教育や、教育カリキュラムが十分に整備されていないため、従業員の情報セキュリティ強化に対する理解が薄く、抽象的かつ曖昧なものとして捉えられていた。
- 情報管理を推進する人員が不足していたため、センター全体の効果的な情報管理が実施されていなかった。
- 情報セキュリティ強化を推進する組織が脆弱なため、情報セキュリティ強化のために、センター全体で取り組む必要がある、大規模なインフラ設備導入や、IT 環境構築に至らなかった。
- 情報セキュリティに対する施策を包括的に管理、監督していないため、情報セキュリティ強化施策に対して発生した費用の計上や、実施済み施策の効果を次回に応用することができなかった。

３．課題

前項で挙げた問題点と原因を分析し、より具体化したものを以下に課題として設定した。

今回、事業所移転を契機とした、情報セキュリティ強化施策は、この４つの課題をクリアすることを主目標として、取り組んだ。

３．１　情報管理体制の課題

（１）情報セキュリティ強化施策の一括管理

セキュリティ強化施策の実施状況を把握し、その費用と効果を測定する必要がある。

（２）情報管理教育の整備

従業員は業務を行う上で、最低限必要な情報セキュリティに対する理解と知識を備える必要がある。

（３）セキュリティの意識向上要求

セキュリティ強化のために、運用や施策が効果的に実行されるよう、個人の意識向上と、

実施体制の強化が必要である。

３．２　物理的なセキュリティ強化に対する課題

（１）入退室管理

ビル内、全てのエリアにおいて、個人ごとに入退室が可能なエリアを決め、それを監督するシステムの構築が必要である。

（２）私物の持ち込み制限

業務エリアへの私物の持込禁止と、業務エリアからの資料・資材の持ち出しを禁止を徹底する。

（３）業務エリアの監視を強化

業務エリア内全てを 24 時間監視できる設備が必要がある。また機材による監視のみではなく、目視でお互いを認識しやすい環境を作る必要がある。

（４）機材の使用制限

PC、FAX、コピー機、プリンタなど、情報発信が可能な機材の使用者を制限し、管理監督が可能なシステムの構築が必要である。

（５）資産の管理

業務用 PC、周辺機器などの設置場所把握、盗難・紛失防止や、持ち出し制限・管理が必要である。

３．３　システム面のセキュリティ強化に対する課題

（１）アクセス制限と管理

サーバ内に保存されている各種情報の把握と、情報にアクセス可能な個人の設定・管理が必要である。

（２）社内ネットワーク内のサーバ、クライアント端末のセキュリティ強化

クライアント端末へのデータ保存を制限、その他情報漏洩につながるリスクの低減が必要である。

（３）セキュリティソフト、ネットワークの管理

ウィルス駆除ソフトや、Windows アップデートなど、セキュリティ関連の定義ファイルが常に最新の状態を保つように管理し、またネットワークの状態も常に監視可能なシステムの構築が必要である。

３．４　ローコスト化に対する課題

（１）導入・導入検討時のローコスト化

情報セキュリティ強化に対する設備投資を、セキュリティ要件を満たすだけではなく、現場業務の効率化も視野に入れて、検討、実施する必要がある。

（２）情報セキュリティ強化施策の成果物の利用

情報セキュリティ強化施策によって作成されたエビデンス資料や、整理された情報を利用し、現場業務の効率化を推進する必要がある。

４．セキュリティ強化への取り組み

前項で挙げた４つの課題に対しての取り組みを以下に説明する。

４．１　情報管理体制強化への取り組み

当社プロジェクト内の情報セキュリティ強化を推進する体制は、情報管理責任者（管理職）と、情報管理推進員とで構成される。

今回、事業所移転時に大規模かつ迅速な取り組みが実施できるように、移転前の早い段階において、以下のような情報管理体制の強化をおこなった。

- 情報管理責任者として、プロジェクト内の管理職全員（3 名）が就き、情報管理推進員を 4 名から 29 名へ増員した。
- 情報管理推進員は、現場管理者のみではなく、インフラ担当者、システム担当者、ファシリティ担当者、プロモーション担当者など、多くの要員を含む構成になっており、多面的な取り組みに対応できる体制へと強化した。
- プロジェクト内の情報管理責任者と情報管理推進員の半数以上は、それぞれ、プライバシーマーク管理責任者、プライバシーマーク推進員を兼任し、当社が取得している「プライバシーマーク」の理解と知識をもって、情報セキュリティ強化へ取り組む体制を整えた。
- 情報管理推進員は、クライアントが開催する情報セキュリティ強化のためのワーキンググループへ参加し、様々なセキュリティ要求をいち早く、より正確に反映できる体制を整えた。

図１．過去の情報管理体制

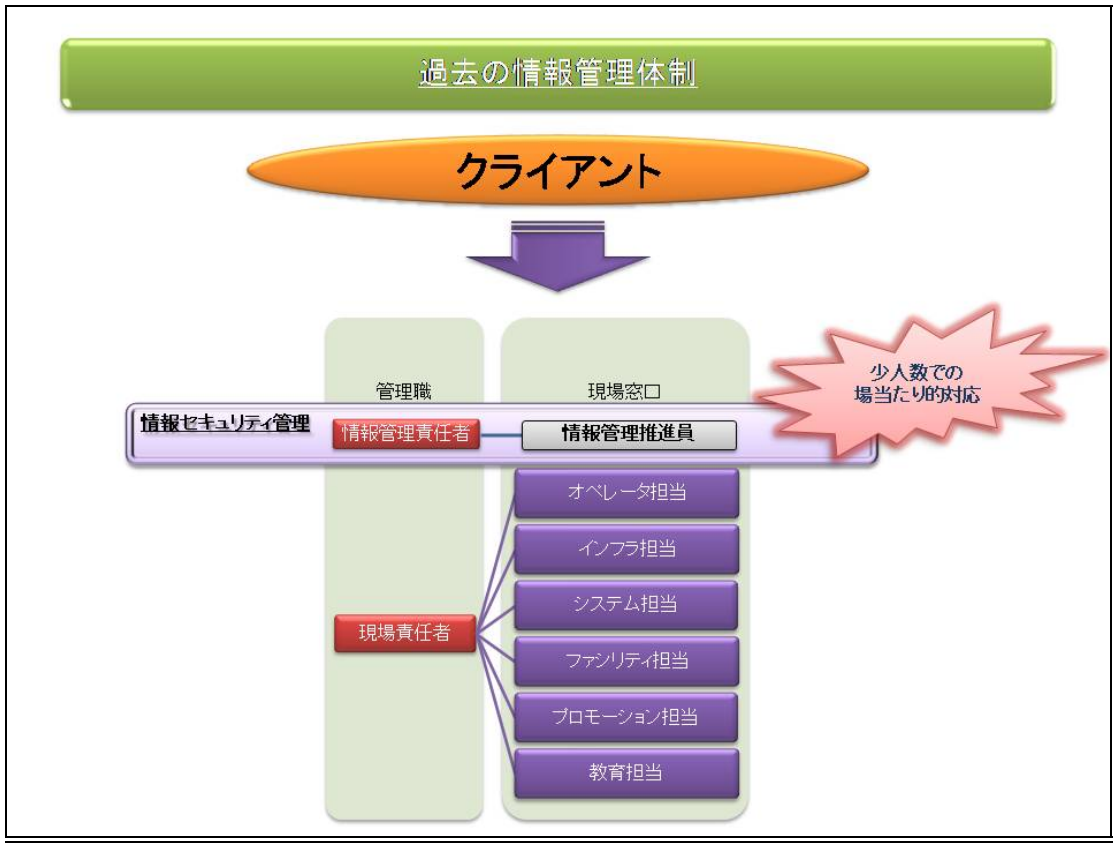
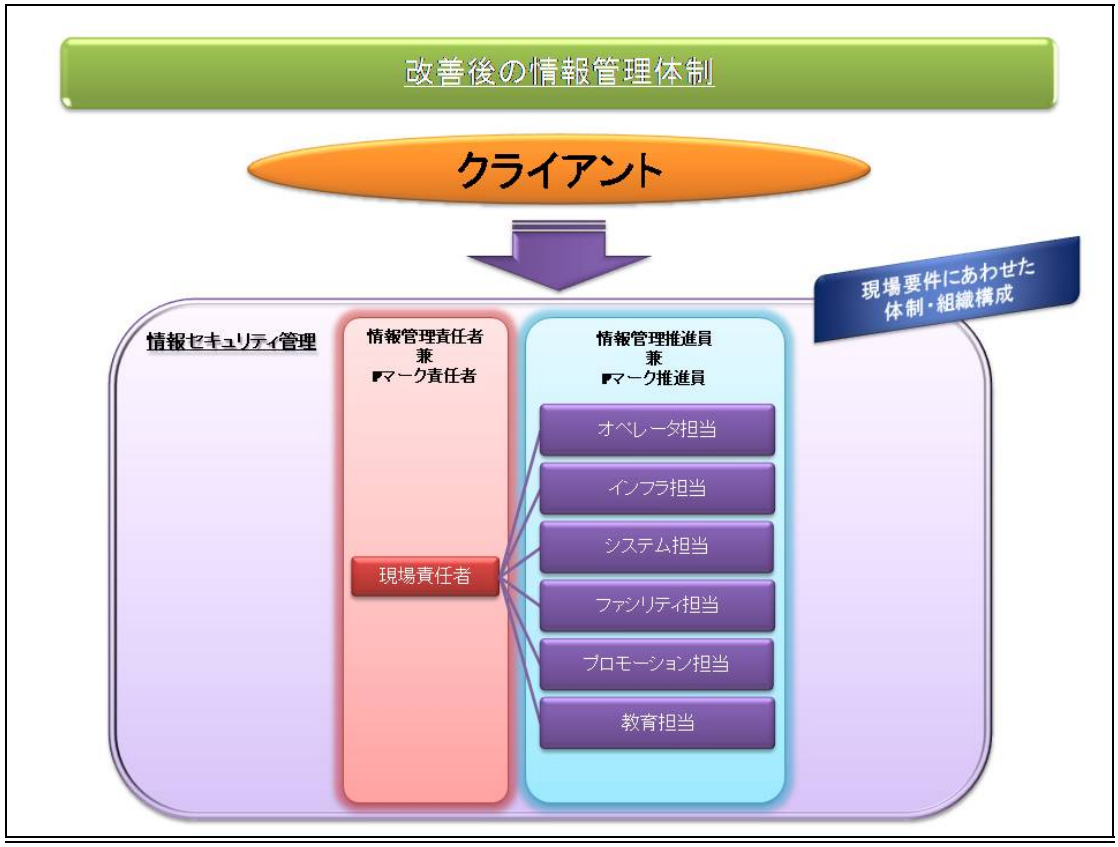


図２．現在の情報管理体制



以上の情報管理体制強化によって、その権限範囲は拡大し、次に述べる施策の実行に至った。

（1）情報セキュリティ強化施策の一括管理

情報管理に対する基準を確立するため、情報管理細則や、クライアントの情報セキュリティ強化要求を整理し、遵守すべき規則や、作成すべきエビデンスを社内イントラネット上に専用サイトを構築・公開するといった「見える化」を行った。

また、全ての情報セキュリティ強化施策は、情報管理責任者、情報管理推進員にて審議・承認・管理を実施した。

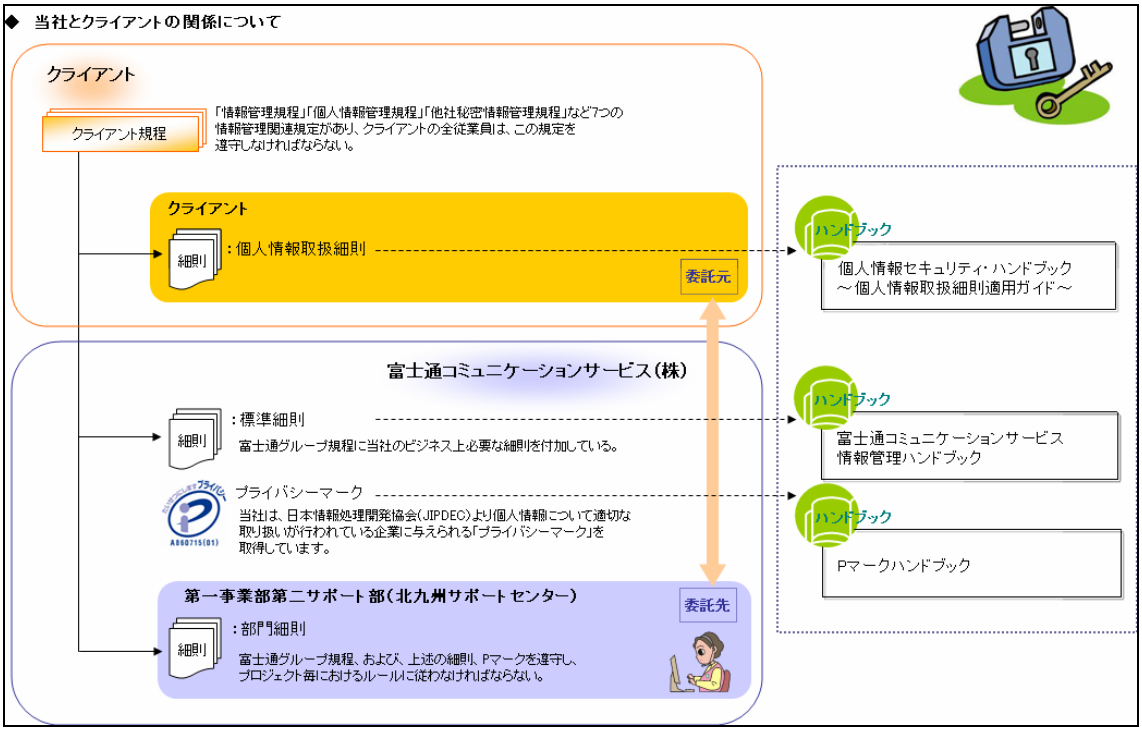
（2）情報管理教育の整備

情報管理教育については、教育資料や教育カリキュラムの見直しを実施した。

その後、各細則を理解し易く要約したハンドブックと、応用事例を用いた資料で教育を実施し、「業務を行う上で必要な、情報セキュリティに対する理解と知識」の取得を推進した。（図３）

教育講座終了後は、全ての確認テストに合格するまで、情報を取り扱うことが可能な有資格者とは認めず、現場への配属は行わないこととした。

図３．情報セキュリティ教育資料



（3）セキュリティ意識向上施策

前述の 2 つの施策や教育を行う過程で、情報セキュリティとは、個人の倫理観や判断に依るものではなく、遵守すべき規則、細則であると意識付けを行い、違反については懲戒免職も含めた罰則についても説明を行った。

また社内イントラネット上で、全従業員に対して、毎月 16 項目からなる「セキュリティチェック確認表」の起票を義務付けた。

そのほか、目視でセンター内の人員が判別できるようにネックストラップを色分けしている。（図４）

図４．ネックストラップの区分（来館者：黄、従業員：赤、情報管理担当：青）

４．２　物理的な要素に対する取り組み

新事業所ビルの設計段階から、情報管理責任者、情報管理推進者が参画。
設計業者、施工業者、センター管理スタッフと連携し、動線、各エリアのセキュリティレベル設定を反映した設計を実施。

（１）入退出管理

ビル内の全エリアに、５段階からなるセキュリティレベルを設定（図５、６、７）し、自身がどのセキュリティレベルに入るのかを目視で確認できるようにした。（図８）

最高レベルの四次セキュリティに関しては、ビルセキュリティカードの盗難などを考慮し、確実な本人認証が行われるよう、手のひら静脈認証装置を導入した。（図９）

図５．５段階のセキュリティレベル設定

北九州サポートセンターのセキュリティレベル設定

LEVEL 0	セキュリティ外エリア Non Security Area	セキュリティ設定されていないエリアです。 ご来客用のカウンター、受付用応接室などがあります。	-
LEVEL 1	一次セキュリティエリア First Security Area	全スタッフ及び受付をして頂いたカード所有のお客様の行動エリアです。 ビル共有部分（リフレッシュ、エレベーター、喫煙室、会議室）があります。	アート製 V-LINE VM-10A
LEVEL 2	二次セキュリティエリア Second Security Area	プロジェクト関係者のみが入室可能エリアです。 個人別の私物収納ロッカーがあります。	セコム社製 ワイヤレス・セキュリロック
LEVEL 3	三次セキュリティエリア Third Security Area	プロジェクト関係者のみが入室可能エリアです。 サポートエリア、検証エリア、フィードバックエリアなどがあります。	アート社製 V-LINE VM-10A
LEVEL 4	四次セキュリティエリア Forth Security Area	プロジェクト関係者の中でも、限られた者のみが入室可能なエリアです。 FAX・コピーエリア、引取りPC室等があります。 マシンルームでは生体認証（静脈認証）にて高いセキュリティを確保しています。	施錠管理 富士通フロンテック社製 手のひら静脈認証 入退室装置

図６．１Ｆフロアセキュリティ

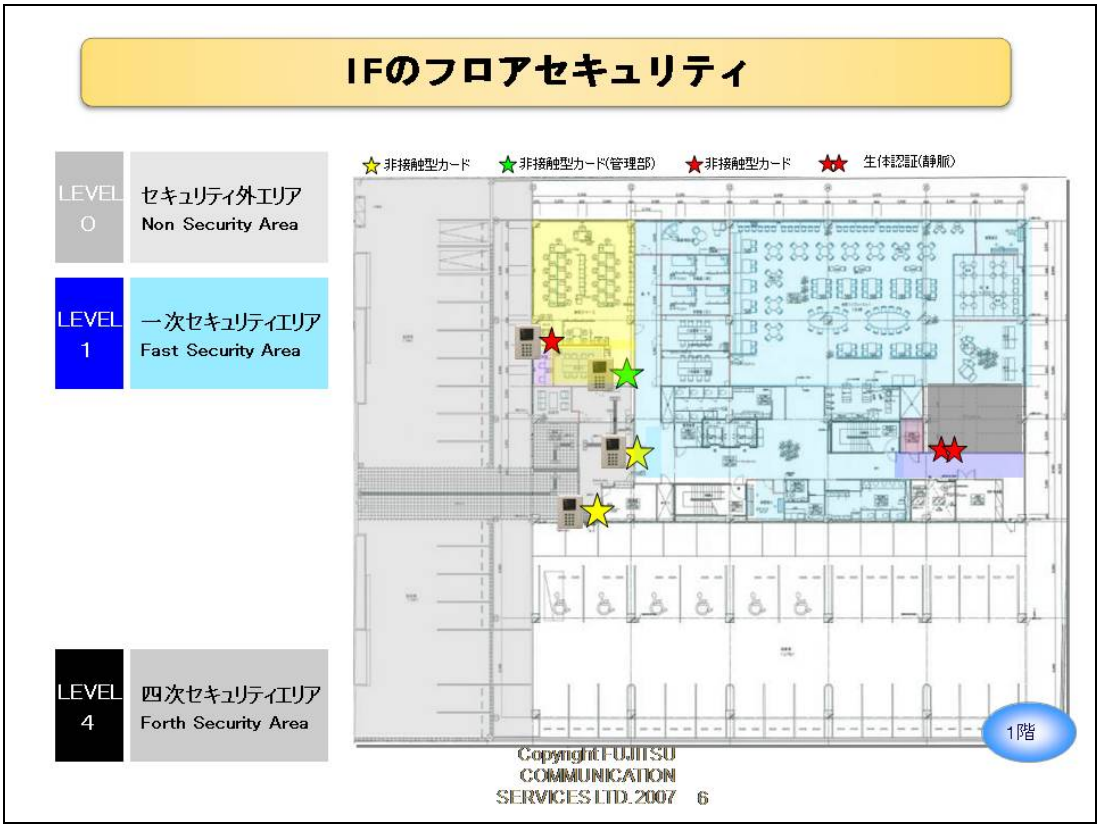


図７．２Ｆフロアセキュリティ

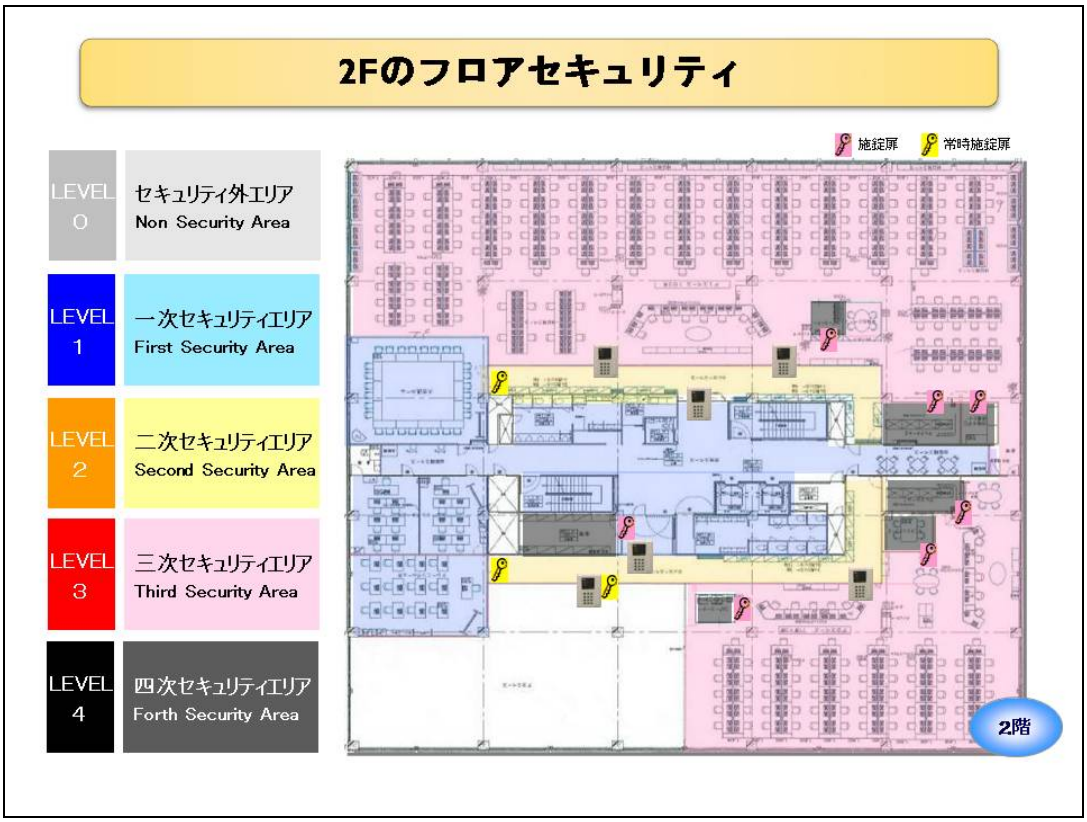


図８．セキュリティレベルの可視化

図９．手のひら認証装置

（２）私物の持ち込み制限

携帯や鞄などの私物は、全てセキュリティレベル２の中に設置したロッカーで管理し、業務エリアであるセキュリティレベル３への持込を禁止とした。（図１０）

また、毎月ロッカーの中を点検するチェックデーも実施している。

図１０．私物収納用ロッカー

（３）監視の強化

業務エリア内においては、監視カメラの死角をなくすように全 14 台を配置し、現場管理者の座席前で 24 時間モニタ監視をしている。（図１１）

また、現場管理者席による目視での監視と、コミュニケーションの活性化を目的とし、床上を 20 センチ上げたハイアリーナ席（図１２）を設置した。

図１１．業務エリア内の監視カメラ

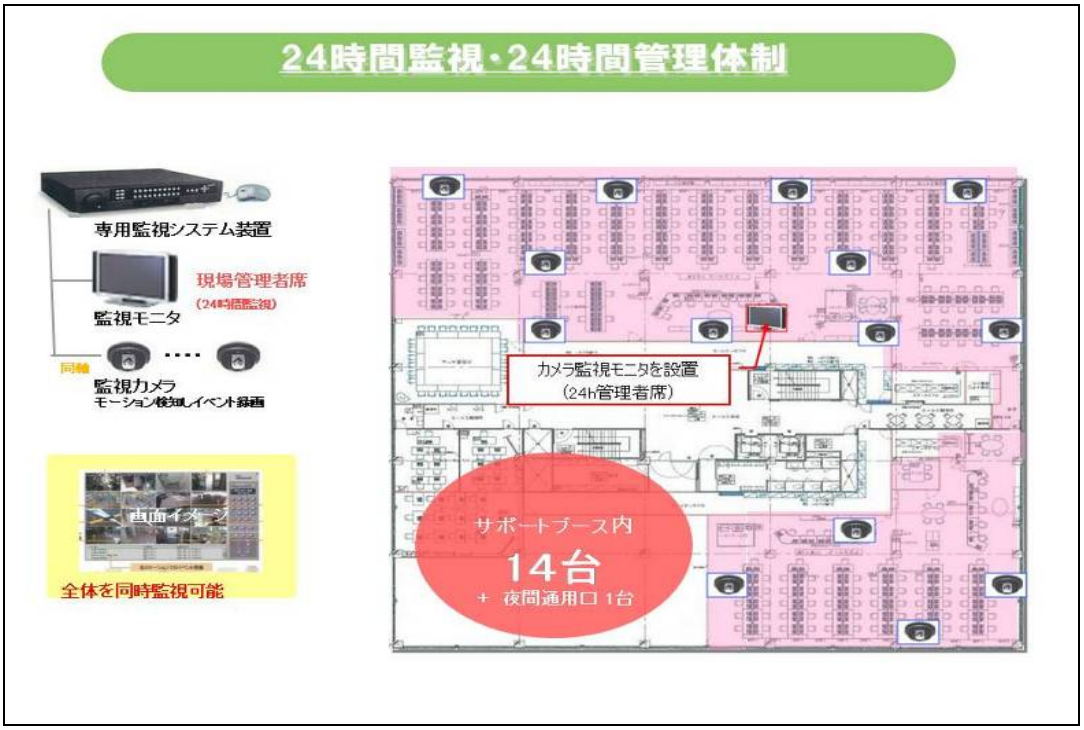


図１２．ハイアリーナ席

（４）機材の使用制限

コピー機、プリンタなど、情報の複製、発信が可能な機材については、業務エリア内に施錠可能なスペースとしてラピセルを設置。（図１３）

FAX 機についてはクライアントのセキュリティ要件で設置不可と定められているため、代替システムで運用し、業務エリア内には設置しない。

図１３．ラピセル

（５）資産の管理

業務用 PC、周辺機器などはインフラ担当の情報管理推進員が、設置場所、設定の一括管理を実施し、ノート PC には盗難防止として 362 台全てに、セキュリティワイヤーの取り付けを義務化した。（図１４）

図１４．ノート PC の盗難防止用セキュリティワイヤー

業務用機器の持ち出しは原則禁止し、業務上機器の移動が必要な場合は情報管理責任者、もしくは情報管理推進員の承認を必要とする。

また、業務用 PC の移動や可搬媒体の使用は全て台帳管理し、情報管理上エビデンスとして保存され、3 ヶ月ごとに全ての機器に対して、定期棚卸しを実施する。

以上の資産管理体制で、機器の盗難、紛失による情報漏洩を防止する。

４．３　システム的な要素に対する取り組み

以下に説明するシステムに関する取り組みは、社内のセキュリティ要件や、クライアントのセキュリティ要件など、各々に個別対応するのではなく、双方の要件を満たすよう考慮し、かつ現場の業務効率化に対する要望も事前にヒアリングした上で、総合的に判断し、実施したものである。（表１）

また、システム担当者が情報管理を兼務していることで、各セキュリティ要件を深く理解したうえで対策を講じることができた。

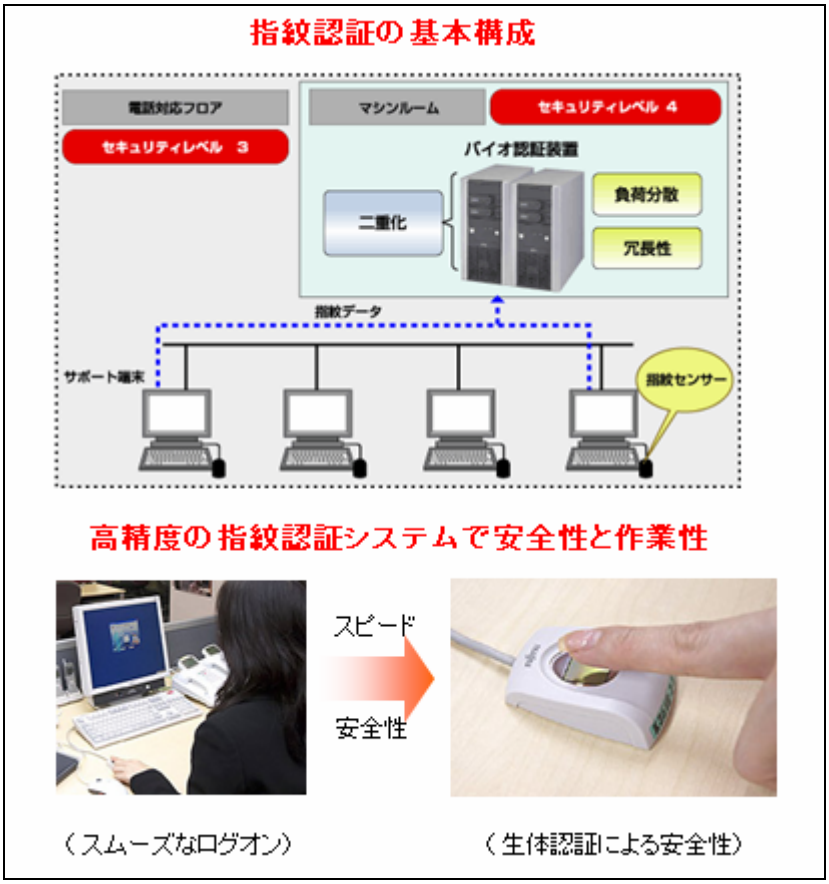
表１．現場からの改善要求と導入ソリューション

現場の改善要求	導入ソリューション
各種システムのパスワードが多く、Windows パスワードを忘却することがあるため、代替えログオン方法がほしい。	指紋認証
どの PC でログオンしても環境設定が同じであってほしい。 PC が故障し、修理したとしても環境が元通りであってほしい。	移動プロファイル フォルダリダイレクト
Winny などの危険なアプリケーションを使えなくし、意図せず使われるようなことがないように、PC を制御してほしい。	ファイルスクリーン
プリンタインストールの有無で PC が管理されていると、どの席から印刷できるかわからないので、ユーザーによる制御をしてほしい。	プリントサーバ
PC でメールを受信すると他の席に座った場合に参照できないので、サーバ内で管理するメールボックスを簡単に参照できる仕組みがほしい。	Exchange Server
Windows の Update を各自が手動で実施しなくても、自動的に適用される仕組みがほしい。	Windows Server Update Services
仮に資産紛失などの事故が発生した場合も、あとから追跡できる仕組みがほしい。	監視カメラ
資産紛失が発生しても情報が漏洩しないようにしたい。	ハードディスク暗号化

（１）指紋認証装置の導入

指紋で本人を認証する生体認証装置を用いてシステムにログオンすることから、成りすましのような不正アクセスを防止でき、かつログオン時のユーザー名、パスワード入力を省けるようにした。（図１５）

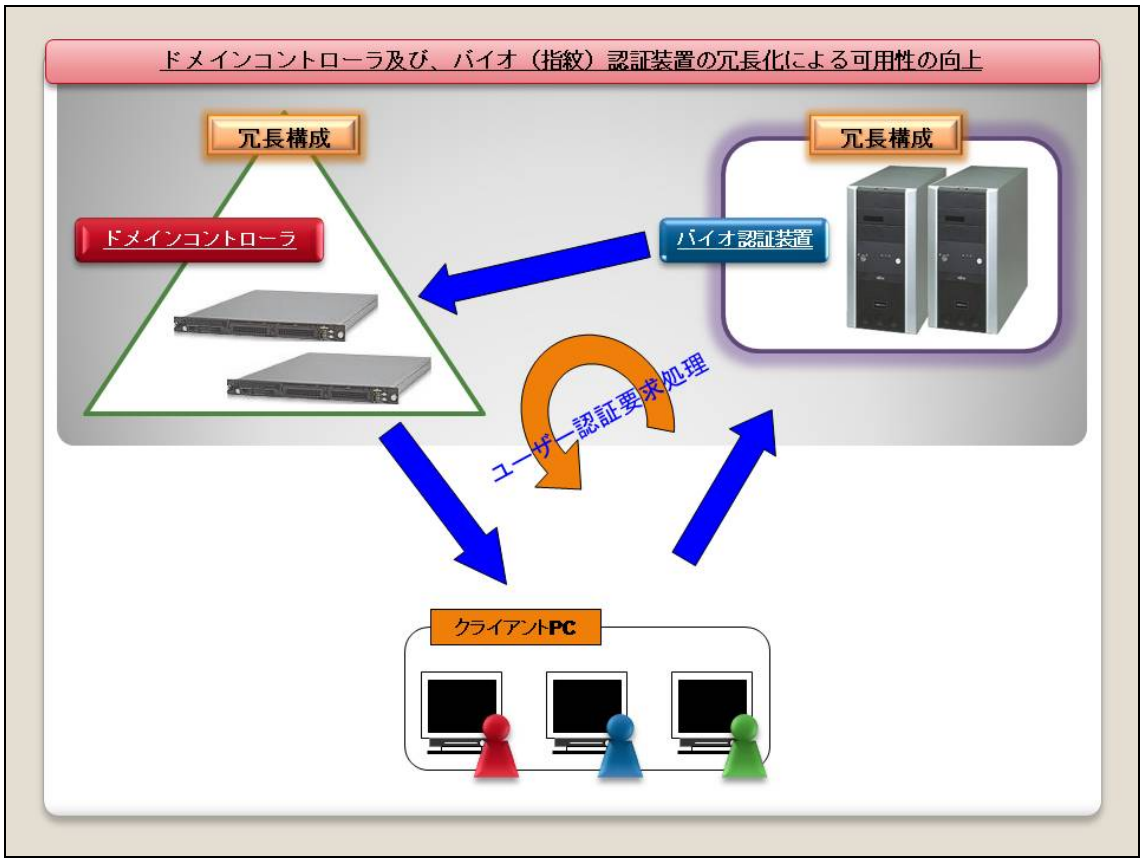
図１５．指紋認証装置による本人認証



（２）本人認証基盤の冗長化

本人を認証する際に使用する生体認証装置及び、ドメインコントローラは２基の装置を用いて、それぞれ冗長化構成を整えることで、万が一の障害時も業務を停止することなく、サービスを継続できるようにした。（図１６を参照）

図１６．本人認証基盤の冗長化構成図



（３）移動プロファイル、フォルダリダイレクトの導入

業務用 PC においては、様々なセキュリティ要件へ対応するため、スクリーンセーバーによるパスワードロックや、USB デバイスの使用禁止など、情報漏洩対策を施している。

その中で、ほとんどのセキュリティ要件は、Windows が標準で備えているグループポリシーという機能で対応が可能であり、特別な投資を必要としなかった。

その機能の中でも、ログインしたユーザーの環境設定情報をサーバへ格納し、業務用 PC に情報を残さない移動プロファイルとフォルダリダイレクトを採用した。（図１７）

図１７．移動プロファイルによるフォルダリダイレクト

（４）印刷の制限

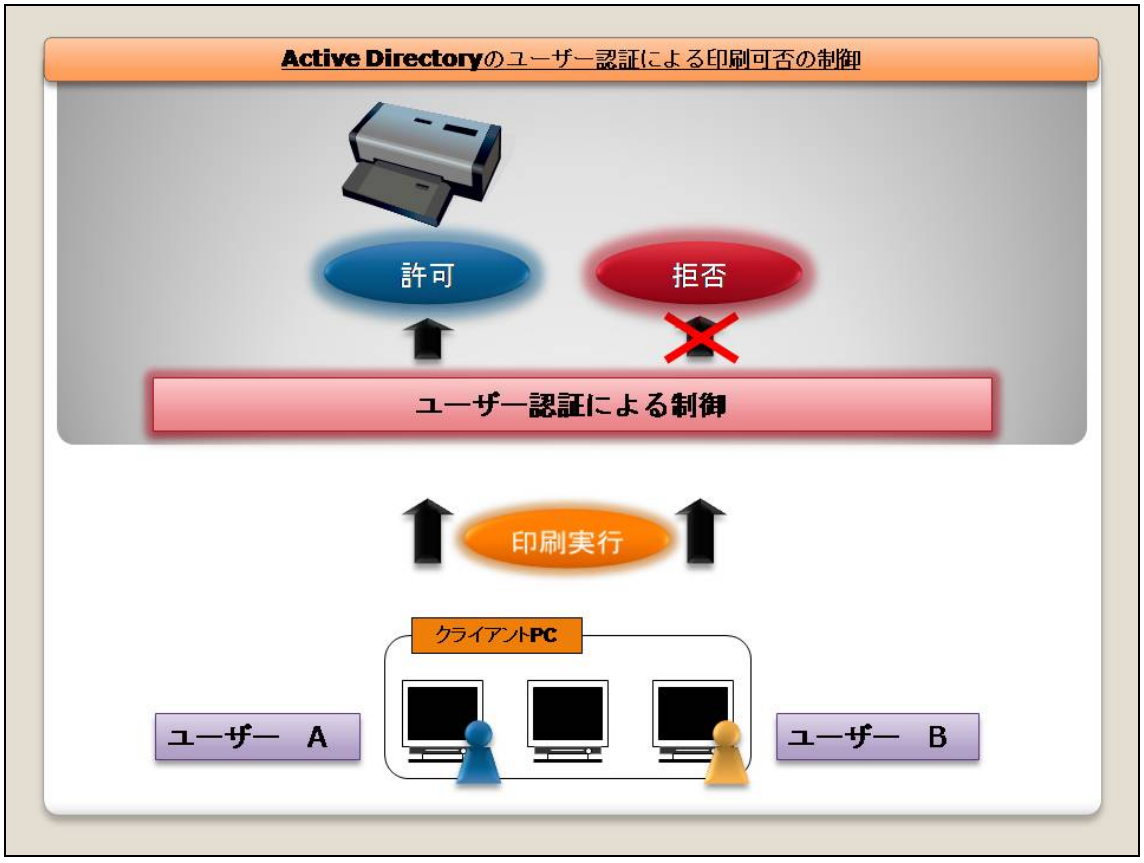
セキュリティ要件の中には、不必要な印刷を制限することが定められており、当初、その要件を満たすために、プリンタをインストールする端末とインストールしない端末に分けて運用していた。

しかし、印刷を必要とするユーザーがプリンタをインストールしていない PC に着席した場合に、作業が進まないという弊害を起こしていた。

そのため、Windows Server のプリントサーバ機能を用いて、本人認証の情報を活用することにした。

この場合、管理者が印刷を許可するユーザーと拒否するユーザーを定めておけば、仮にプリンタがインストールされている端末でも、許可されたユーザーでしか印刷ができない。（図１８）

図１８．ユーザー認証による印刷制限



（５）ファイルスクリーン

ユーザーごとの環境情報には、ファイルスクリーンを設定しており、特定の拡張子を持つファイルを保存することはできない。

仮に許可していない拡張子のファイルを保存すると、警告メッセージの表示とともに、システム管理者への通知が自動的に行われる。

当然ながら、実行形式（exe、bat など）のファイルは無効にしており、ファイル交換ソフトなどを保存・実行することはできない。

（６）セキュリティパッチの適用

Windows や Office の脆弱性を修正するパッチの配布についても専用の配布サーバを導入し、ユーザーが意識することなく、最新のセキュリティ状態を保つことができる。また、ウィルス対策ソフトも専用サーバを設けており、常に最新の定義ファイルに更新されている。

（７）ハードディスクの暗号化

業務用 PC すべてに対して、BIOS パスワードなどのセキュリティを施すだけでなく、万が一の事故に備え、ハードディスクの暗号化を施した。

（８）可搬媒体でのデータ持ち出し禁止

メールボックス内データ等の、外部への持ち出しを禁止する為、以下を実施した。

・可搬媒体の使用を規制する為、BIOS 設定と、専用ツールを使用し、クライアント端末のデバイスを無効化した。

・業務上、可搬媒体の使用が必要な一部の端末は、セグメントを分離し設置。

・可搬媒体を使用する場合は、事前に使用用途を情報管理責任者に申請し、承認を得た人物のみが、承認を得た内容でのみ使用可能であるが、そのつど、可搬媒体管理台帳への記入と、情報管理推進者の承認、立会いの下でのみ実施するものとした。

４．４　ローコスト化への取り組み

以下の施策は、前項までに説明した各施策の導入に対し、コスト面からの選定理由として、関連する部分があるが、本項では独立した施策として説明する。

情報セキュリティ強化に必要な費用をローコスト化する方法として、以下２つの施策を実施した。

（１）導入・導入検討時の施策

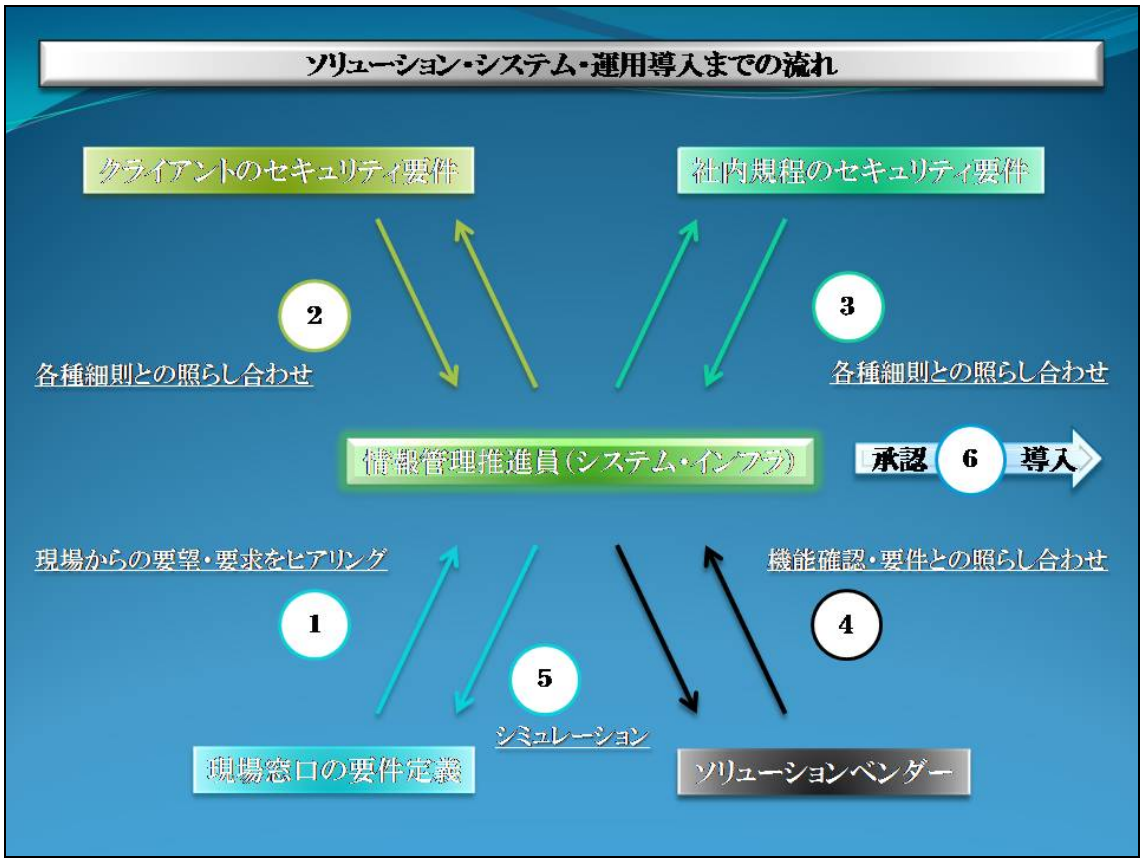
情報セキュリティ強化に対する設備投資は、クライアント要求などを勘案した中長期的な情報管理計画に沿って実施されるため、現場に対しての影響を軽視する傾向にあった。

そこで今回は、将来的に現場業務の効率化を促し、費用対効果を高める設備投資ができるよう、新たに以下の導入フローを構築、採用した。（図１９）

これは、各セキュリティ要件と現場の改善要求を基に、情報セキュリティ強化と、現場

の業務パフォーマンス向上を兼ね備えたシステム・ソリューションの導入を可能とし、併せて導入を予定しているシステム・ソリューションを関連部署やクライアントへ事前に報告することから、将来的なリスクもヘッジしている。

図１９．システム・ソリューション導入フロー



上記結果として、今回導入したシステム・ソリューションは前項の取り組みで紹介した「現場からの改善要求と導入ソリューション」（表１）のとおりである。

（２）情報セキュリティ強化施策の成果物を利用することによるローコスト化

情報セキュリティ強化施策によって作成された、各エビデンスの活用や、整理された情報の活用が、現場の業務を効率化し、中長期的に費用を削減できるよう取り組んだ。

具体的な成果物利用例は以下のとおりである。（表２）

表２．成果物の利用例

資料名称	利用例（今後も含む）
人的付与情報一覧	入社・退職時の各種システム登録・解除作業 社員教育履歴確認システムへの流用 社員パフォーマンスカルテへの流用 勤怠データベースへの流用 要員数の把握や、体制図の作成など
人的処理フロー	
人的付与情報管理台帳	
物的付与情報一覧	定期資産棚卸しに利用 オペレーターの資産検索システムへ流用 修理保守手配時の仕様情報確認 費用情報を元に来期予算の作成 MAC アドレスを元にしたアクセス制限
物的処理フロー	
物的付与情報管理台帳	
規程・細則一覧	情報管理教育資料への活用

５．効果

今回設定した４つの取り組みに対する効果と、実施結果について以下に考察する。

５．１　情報管理体制強化に対する取り組み効果

プロジェクト内全ての情報管理施策とエビデンスの一括管理が実施されたことで、情報管理の状態を常に把握でき、社内外の情報管理監査や、資産管理を迅速且つ効率的に対応することが可能となった。

また、情報管理のために、現場で実施する定期チェックの遅延が減少した。

５．２　物理的な要素に対する取り組み効果

プロモーション（来客向けサポートセンター見学会）とセキュリティの両要求を満たしたフロアレイアウト設計によって、2006 年 10 月の事業所移転から現在まで、複数回にわたって実施したプロモーションにおいて、非常に高い評価を得ており、2007 年 8 月 6 日に「第 20 回　日経ニューオフィス賞」を受賞した。

静脈認証装置など、今回の施策で導入した入退室管理システムで、高いセキュリティを確保し、社内外から高い評価を得た。

また、各エリアのセキュリティレベル設定は目視によって確認できることから、それが個人の情報セキュリティに対する意識向上効果としても現れており、業務エリア内への私物持込禁止徹底などを実現した。

今回、物理的なシステムセキュリティ強化のために実施した施策の効果をまとめると、以下のようになる（表３）

表３.物理的なセキュリティ強化に対する効果一覧

導入施策	物理的なセキュリティ強化に対する効果
センターエリア内のセキュリティレベル設定 セキュリティレベルの可視化	部外者の不正な侵入を防止、 従業員のセキュリティ意識の向上
2 次セキュリティレベルエリアのファシリティ完備 ロッカー定期点検の実施	3 次セキュリティエリア（業務エリア）への私物の持込禁止を徹底。 情報漏えい防止
監視カメラによる 24 時間監視（業務エリア内）	業務エリア内の監視を強化。 部外者の不正な侵入を監視。 資材、機材の盗難防止。 情報漏えい防止。
ハイアリーナ席の設置	
業務エリア内の施錠可能スペースを設置 （ラピセル）	情報の複製、発信が可能な機材の使用者制限。 本人確認が可能。 情報漏えい防止
セキュリティワイヤーの設置	資材、機材の盗難防止。 資産の盗難による情報漏えい防止
セコム社製ワイヤレスセキュリティロック採用	部外者の不正な侵入を防止、監視。 従業員のセキュリティ意識の向上。 各監視システムのログにより、事件・事故にも迅速に対応を可能とする。
アート社製　V-LINE　VM-10A 採用	
富士通製手のひら静脈認証装置採用	

５．３　システム的な要素に対する取り組み効果

今回、システムセキュリティ強化のために実施した施策効果をまとめると、以下のようになる。（表４）

表４．システムセキュリティ強化に対する効果一覧

導入ソリューション	システム的なセキュリティ強化に対する効果
移動プロファイル フォルダリダイレクト	サーバ内にユーザー情報が格納されるため、ローカル PC にデータが保存されない。また、重要な情報もすべてサーバのバックアップ対象に含まれるため、事件・事故への対策も図れる。
ファイルスクリーン	意図しないファイルの複製や保存・実行をなくした。
プリントサーバ	印刷の可否をユーザー情報で制御できるため、誰がどの PC にログオンしても同じセキュリティが保てる。
Exchange Server	メールのデータはすべてサーバ内に格納されるため、ローカル PC へのデータ保存を抑制できた。
Windows Server Update Services	業務用 PC は、常に最新のセキュリティ対策を施している状態となる。
指紋認証	ユーザーパスワードの流出が発生しても、本人認証のプロセスを崩すことがない。
ハードディスク暗号化	資産の盗難や、紛失が発生した場合でも情報漏洩を防止できる。

５．４　ローコスト化への取り組み効果

上述した施策に対するコスト削減効果の中から代表的なものをまとめると、以下のとおりである。（表５）

表５．コスト削減効果一覧

ソリューションやエビデンス	削減効果	削減コスト
移動プロファイル	ローカル PC 設定工数の削減。	5 分×250 名/日
プリントサーバ	ローカル PC 設定工数の削減。	10 分×314 台
人的付与情報一覧 人的処理フロー 人的付与情報管理台帳	各種システムへの流用し、各業務におけるデータの参照時間や、入力時間を削減した。	250 名×システム数 ×入力工数
	要員数把握や入社・退職時の各種システム登録・解除作業の処理時間を短縮。	入社・退職人数×15 分
	勤怠管理、評価データ管理、パフォーマンス管理の管理工数を削減。	–
Exchange Server	メールサーバーログオン時間の短縮。 ローカル PC の設定工数削減。 アドレス帳の一元管理。	5 分×250 名/日
Windows Server Update Services	Windows Update 実施時間短縮。	20 分×314 台/月
指紋認証	ログオン時間短縮。 パスワードリセット工数の削減。	1 分×250 名/日
物的付与情報管理台帳	オペレーターの資産検索時間の短縮。 修理保守手配時の仕様情報確認工数の削減。 費用情報を元に来期予算の作成工数を削減。	–
	資産棚卸し工数の削減	1035 台×10 分 ×4 回/年

５．５　結果考察

前項で説明した内容から、当初設定した情報セキュリティ強化のための 4 つの課題に対し、十分な効果を得ることができたと判断する。

これは、事業所移転という機会を逃さず、現場の情報管理担当者が、設計段階から情報セキュリティ強化のために参画し、様々な工夫をもって各施策に取り組んだ結果である。

今回の取り組みで、我々自身が特に評価するものを以下に考察する。

（１）情報管理体制の強化を最優先

個別の課題に対する施策を計画・実施する前に、それを管理する情報管理体制を強化し、その後の作業に以下のようなアドバンテージを持たせることに成功した。

・各分野から担当者が参画したことで、将来的に各業務へ与える影響を多面的に予測できた。

・様々な観点からセキュリティ強化施策を実施したことで、適用範囲の拡大へ繋がった。（費用面、人員面）
・情報管理業務における PDCA サイクルを構築し、今後の継続した情報セキュリティ強化を可能とした。

（2）独自のローコスト化

情報セキュリティ強化のために必要な機材や、ソリューション導入の費用自体を削減することは困難である。

しかし、情報セキュリティ強化施策によってもたらされたエビデンスや、整理された情報を活用し、現場の業務効率化を実現した。

これは相対的ではあるが、情報セキュリティ強化に対するコストを、中長期的な費用対効果の向上によってローコスト化したといえる。

また、実現するにあたって、現場のマネージメントや業務プロセスを理解し、必要とする情報を把握する必要があったが、情報管理担当者が常に現場と連携し、業務の可視化を推進したことは高く評価できる。

６．終わりに

北九州サポートセンターの事業所移転が無事終わり、情報セキュリティ強化施策も一応の効果を挙げる事ができたが、これで情報セキュリティ強化が終わったわけではない。

現在、既に我々は、データ保護のためのソリューション導入や、新システム要件を満たすためのインフラ環境整備に取り組んでいる。

また、当社に限ったことではなく、コールセンターに対する情報セキュリティ強化の要求は益々厳しいものとなっており、今後は内部統制に関連して、業務内容の可視化やリスクコントロールといった、新たな要求も対応していく必要があると考えられる。

そのような中、本論文の内容が、コールセンターの担当者の方々をはじめ、各企業の担当者の方々に少しでも参考になれば幸いである。

最後に、当社北九州サポートセンターの事業所移転の際に、多大なご支援をいただいた富士通株式会社殿に、深く感謝いたします。