クライアントパソコンの入れ換えに併せた社内ネットワーク環境のセキュリティ向上対策について

富士火災海上保険（株）

■ 執筆者Ｐｒｏｆｉｌｅ ■

武藤　範嗣

1993 年　富士火災海上保険（株）入社
　　システム部
2006 年　現在　ＩＴ統括部運用グループ所属
　　端末・ネットワーク運用担当

■ 論文要旨 ■

富士火災海上保険株式会社では，従来のクライアントパソコン（以下パソコンという）の老朽化に伴い全パソコンの入れ換えを行った．その際，従来のパソコンでは対応できていなかった様々なリスクに対して，パソコンへのソフトウェアインストールだけでなくサーバを構築してシステム構築を行い，社内ネットワーク全体としてのセキュリティを向上させた．

ここではパソコンの入れ換えにあたって，どのようにリスクの分析を行いセキュリティ対策の方法を選択したか，また，セキュリティ対策の運用方法について述べることとする．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社の概要

当社は 1918 年に設立の損害保険会社である．当社では業務の効率化の手段として，全社員に対して 1998 年から順次パソコンを配布した．現在では全国約 190 ヵ所の事業所から約 6,500 人の社員が社内ネットワークを介して，基幹システムや情報系データベースから顧客情報にアクセスし，メールによる情報伝達を行っている．

これまでパソコンの OS は Windows NT 4.0（以下 NT という）を標準 OS と定め，パソコンを追加購入する場合も OS は NT で使用してきた．しかし，マイクロソフト社における NT のサポート終了や初期に配布したパソコン（全体の３割以上を占める）の老朽化を契機として，使用 OS の変更と新パソコンへの移行スケジュールを検討することとなった．

そこで，次期 OS を Windows XP（以下 XP という）と定め，全業務アプリケーションの XP 対応と全パソコンの一斉入れ換えを決定した．

１．２　移行前のパソコン環境

移行前のパソコン（以下旧パソコンという）について，パソコンの環境設定と利用環境を図１に示す．

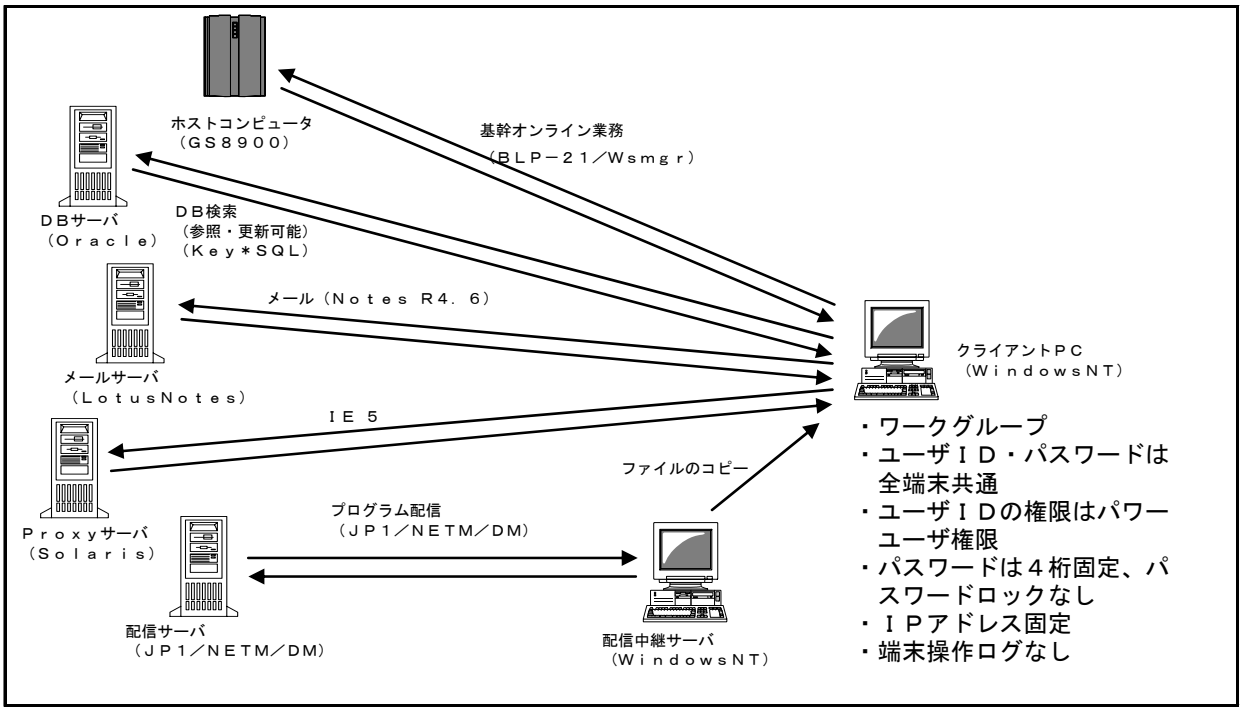

図１　移行前の PC 環境図

図１のとおり，旧パソコンはワークグループ構成としており，ドメイン構成と違って各パソコンの設定情報は各パソコンで管理していた．しかし，パソコン運用上，全パソコンで共通のユーザ ID・パスワードを使用し，また，パスワードを定期的に変更するようにした場合の運用管理の煩雑さを懸念して，パスワードの定期的な変更やパスワードの誤入力によるアカウントロックを行わなかった．

また，サーバの名前解決を各パソコンの HOSTS ファイルにて管理することで使用者ごとへの柔軟な対応が可能であったが，反面，全サーバの IP アドレスを誰でも確認できるとい

うことや，イレギュラーな HOSTS ファイルの存在によってサーバ入れ換えによる HOSTS ファイルの一斉入れ換えが難しくなるといった問題点を含んでいた．

社内システムには情報系業務としてＯｒａｃｌｅ（以下オラクルという）を利用した DB 検索システムがある．このシステムには DB への参照だけでなく更新機能を含んでいるにも係わらず，パソコン側にもサーバ側にもアクセスログを取得する仕組みがなかった．

クライアントへのプログラム配布は，各部署に設置しているパソコンのうちの１台を配布中継サーバとし，配布サーバからは配布中継サーバのみに配布していた．その他のパソコンは起動時にそれぞれの部署に設置している配布中継サーバから内製のコピーツールを利用して受信していた．このように変則的な配布システムにした目的は配布システムのライセンス費用を抑えることであり，その点については目的を達成できたが，その代わり，全パソコンへの配布状況を一元管理できないとか，パソコンをログオンしてからプログラム配布が開始されるため，ログオンしてすぐにパソコンが使用できないといった弊害があった．また，旧パソコンへのプログラム配布は，配布中継サーバからファイルをコピーする仕組みだけであり，ファイルを実行する機能がなかったため，セキュリティパッチの配布をおこなうことができなかった．

なお，これらホストコンピュータや各種サーバの運用保守は全てアウトソーシングしており，機器の設置場所もアウトソーシング先のデータセンタに設置している．また，パソコンを設置している事業所とデータセンタ間は原則として１～４Mbps の広域イーサにて接続されている．

１．３　パソコンの入れ換え

旧パソコンの入れ換えにあたって，クリアすべき条件は以下のとおりであった．

① システム開発～パソコン展開までを 2005 年４月～2006 年３月までに行うこと．
② セキュリティの向上に配慮すること．
③ 現在利用可能な業務はセキュリティ上問題ない範囲ですべて移行すること．
④ 利用者にとって便利となる機能を追加すること．
⑤ 機器の運用管理の負担が増加しないこと．

パソコン入れ換えの検討を開始したのが 2004 年 10 月なので，新パソコンで実施するセキュリティ対策と業務システムの操作イメージを作ったうえで，ソフトウェアの選定・ハードウエアの構成を決定するまでに６ヵ月間しかなかった．特にセキュリティ対策については既存のシステムとして存在しないため，何をするべきか，どこまでするべきかが解らず，更に運用上の負担も考慮して検討しなければならなかった．システム要件と開発要件を確定するまでの流れはおおよそ以下のとおりであった．

① 現状のシステム構成のまとめと実現したい機能の洗い出し　　１ヵ月
↓
② リストアップした『実現したい機能』を基に『実現するべき機能』の選定とシステム構成のアウトライン作成　　２ヵ月
↓
③ 類似機能のソフト間での機能比較とシステム構成の確定　　２ヵ月
↓

④　システム要件を基に開発ベンダの決定　　１ヵ月

なお，『利用者にとって便利となる機能』の一つとして社屋内の無線 LAN 化を検討した．無線 LAN は手軽に接続できるようなイメージや社屋外に漏れる電波から盗聴されるといったイメージからセキュリティ的には危険なイメージがある．しかし，現在の無線 LAN では，通信の暗号化やアクセスポイントでの MAC アドレスによるフィルタリングなど，正しく詳細に設定することによって有線 LAN よりも安全な通信環境を構築することができる．しかし，今回の検討では無線 LAN 化のためのアクセスポイントの設置・設定費用や展開・運用時に発生しうる接続不良のリスクを考慮して，無線 LAN 化は行わないこととした．

２．パソコンの入れ換えとセキュリティ対策

２．１　セキュリティ向上の検討

セキュリティの向上を検討するにあたって，まず，どのようにすれば『セキュリティが確保されている』といえるかであるが，以下の５要件が必要と考えられる．

①　機密性 ‥‥‥‥ 権限のない人が情報を見ることができないようにすること．
②　完全性 ‥‥‥‥ 権限のない人が情報を更新できないようにすること．
③　可用性 ‥‥‥‥ 権限があればいつでも利用可能な状態であること．
④　真正性 ‥‥‥‥ 情報が正しいことを保障すること．
⑤　責任追跡性 ‥‥ いつ誰が利用したか追跡できるようにすること．

これらの要件を実際のネットワーク構成やパソコンの中で，どのようにすれば満たすことができるかを『セキュリティの要件』として以下にまとめる．

①　本人認証 ‥‥‥ 利用者の正当性を確認．
②　アクセス制御 ‥ 利用者の権限を制御．
③　改ざん防止 ‥‥ データの真正を確保．
④　機密保持 ‥‥‥ 情報の持ち出しを防ぐ（盗聴・盗難の防止）．
⑤　否認防止 ‥‥‥ システムを利用したことについて，否認できないようにする．
⑥　ウィルス対策 ‥ ウィルスによる破壊・不正アクセスを防ぐ．

実際にセキュリティ対策を検討する時には，ネットワーク構成上のどこにどのような問題点があるかを検討する．その問題点が上述のどのセキュリティの要件に対するリスクであるかが明確になれば，対策方法の指針は決まってくる．

２．２　リスク分析

現状のネットワーク構成やパソコンに対してリスクを分析し，セキュリティの要件を当てはめた後，そのリスクに対してどのような対策方法で対処するかを検討する必要がある．このとき，どのリスクに対しても防止措置をとることがセキュリティ上は理想的と思われるが，防止のためのシステム構築費用や運用費用，システムの使い勝手を考慮すると必ずしも全体的には理想的とはならないといえる．そこで，リスク対策の対策レベルとして以下の４段階に分けて検討することとする．

①　検出→記録 ‥‥ リスクを検出するだけに留め，危険を記録しておく．
②　抑止→監視 ‥‥ リスクを抑止する措置をとり，危険を監視する．

③　防止→遮断 ‥‥ リスクの防止措置をとり，危険を遮断する．

④　回復 ‥‥‥‥‥ 正常状態への回復措置のみ検討する．

これによって，リスクを回避するための対策としては，運用担当者の作業負荷を軽減しつつ，システムの使い勝手の確保と最大限の費用対効果を得ることができる．

２．３　対象範囲の確定

上記２．１，２．２を基にセキュリティの対象範囲とリスク分析を行い，表にまとめてセキュリティ対策を行う対象範囲の確定と対策方法の選定を行う．以下にモデルケースとして作成した表の一部を表１に示す．

想定されるリスク	リスクの対象		リスクの実行例	リスクへの対策方法	リスク対策のレベル（高←ﾚﾍﾞﾙ←低）			リスク対策により発生する問題点	リスク対策の可否
	対象となる物	対象の形・方法			防止	監視	記録		
盗難	装置	パソコン	社内への侵入による持ち去り	営業時間外の入退室を禁止	○			強制力に乏しい	
	データ	ﾊｰﾄﾞﾃﾞｨｽｸ(PC)		セキュリティワイヤによるＰＣの固定	○			ワイヤの鍵の運用管理が煩雑になる	一部対策済み
		紙		未使用時は施錠できるﾛｯｶｰ等にて保管	○			施錠管理のルール	一部対策済み
		フロッピー		監視カメラによるフロア内監視		○			
		ＣＤ・ＭＯ		第三者による入退室時の持ち物検査		○		運用ｺｽﾄ? 時間外の運用?	
		ＭＴ・ＭＴＣ		入退室の機械管理			○	社員しか管理できない	一部対策済み
		メール	廃棄対象物の持ち去り	特定業者との契約による廃棄	○			引き渡すまでの管理をどうするか	
				廃棄物を廃棄業者へ引き渡すまで施錠管理する	○			保管場所の問題	一部対策済み
				廃棄前に裁断・データ消去を行う	○			FD･CDなどの媒体の裁断は?	一部対策済み
			プリントアウトして持ち去り	顧客情報などの印刷を禁止	○			業務上、不可能	
				プリンタの印刷ログを収集する			○	各プリンタからの収集方法と保存期間	
			ＦＤ・ＣＤへのコピーによる持ち去り	ＦＤデッキ、ＣＤ－Ｒ等の使用禁止	○			ﾛｯｸ方法はｿﾌﾄｳｪｱorﾊｰﾄﾞｳｪｱ?	
				ＦＤ・ＣＤ－Ｒ等の使用を許可制にする		○		承認者のモラルの影響が大きすぎる	
				ＦＤデッキ、ＣＤ－Ｒ等の使用ログの取得			○	ｾｷｭﾘﾃｨ対策用のｻｰﾊﾞ構築が必須	
			MT･MTCなどへのコピーによる持ち去り	通常のﾕｰｻﾞIDで媒体へのｱｳﾄﾌﾟｯﾄを禁止	○				
				媒体へのｱｳﾄﾌﾟｯﾄは第三者による承認が必要とする		○			
				バッチログの保存と管理			○		
			メールに添付して持ち去り	社外へのメールはデータの添付を禁止する	○			業務上、不可能	
				社外ﾒｰﾙは第三者（上長・検査部）による検閲を行う		○		第三者不在時の対処をどうするか?	
				ﾒｰﾙは全て第三者（上長・検査部）による検閲を行う		○		第三者不在時の対処をどうするか?	
				社外へのメールの添付データについては容量制限する		○		添付文書の内容を確認する必要がある	
				送信データの履歴を採取する			○	圧縮ﾃﾞｰﾀ・暗号化ﾃﾞｰﾀの取扱い?	

表１　リスク分析とセキュリティ対策対応表（一部）

このようにして，運用上のバランスを考慮しつつ，採り得るべきセキュリティの対策手法を新パソコンの仕様の中に取り込んでいった．

３．セキュリティ対策

３．１　セキュリティ対策手法の効果と範囲

上述の手法にしたがって，当社でのセキュリティ対策を検討した結果，図２のような環境となった.

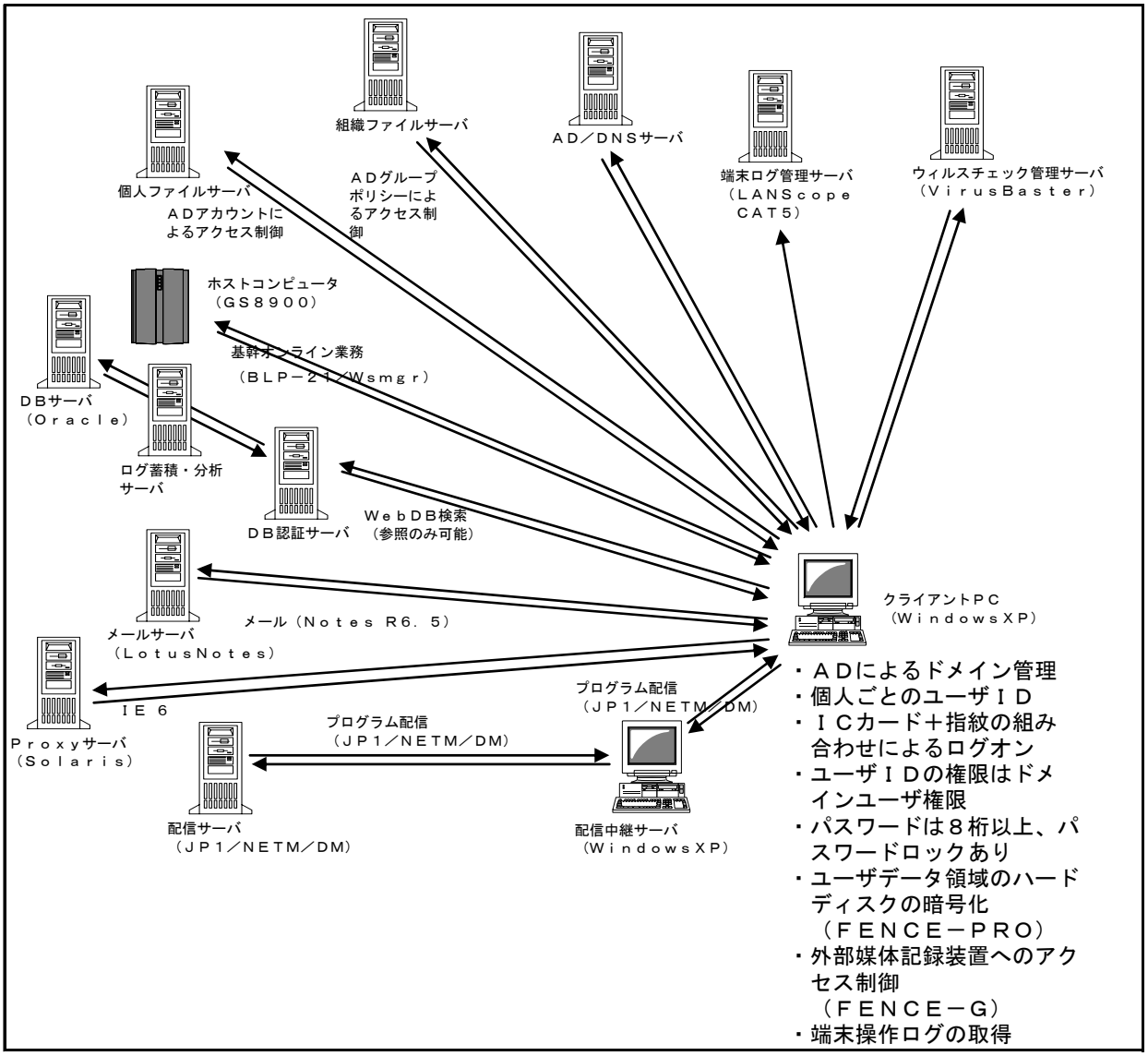

図２　移行後の PC 環境図

新パソコンの環境でセキュリティ向上のために設置したサーバを以下に挙げる.

・Active Directory（以下 AD とする）/DNS サーバ

・ファイルサーバ

・ウィルスチェック管理サーバ

・端末ログ管理サーバ

・ログ蓄積・分析サーバ

これらのサーバはすべてデータセンタに設置し，ハードウェアの運用保守はアウトソーシングした.

また，セキュリティ向上のソフトウェアとして，以下のソフトウェアを導入した．

・指紋認証システム

・ファイル暗号化ソフト

・漏洩抑止ソフト

この他，各事業所とデータセンタ間のネットワークを二重化した．その際，増設した回線は可能な限り元の回線ベンダと異なるベンダを利用することとして，一方の回線ベンダ内で設備障害が発生しても通信が可能となるように敷設した．

３．２　セキュリティ対策手法の選択

セキュリティ向上のために設置したサーバやシステムの役割について，以下に解説する．

（１）　AD/DNS サーバ・指紋認証システム

４台のサーバで多重化した AD によるドメイン環境を構築した．ドメインネットワークとすることで全社員に対し，個々のユーザ ID を割り当てて運用する環境を整えることができた．

なお，ログオン時のユーザ ID・パスワードの運用方法として，個人のユーザ ID とパスワードを IC カードに登録し，これらの情報を引き出す手段として，指紋認証を使用するようにした．こうすることで，使用者にユーザ ID とパスワードを通知する必要がなくなった．そのため，使用者が簡単なパスワードや類推しやすいパスワードを使用する，パスワードをパソコンや机に貼付する，あるいは，自分のユーザ ID とパスワードを他人に教えて不正に使用させることを防止することができる．

また AD のグループポリシーの機能を利用して，パソコンに様々なセキュリティ上の制限を設けている．例えば，OS やソフトウェアをインストールしているディスク領域をユーザから見ることができないようにしている．また，業務上不要な OS の機能や管理ツールの起動や各種設定の変更をできないようにしている．その他にも様々な制限事項をサーバ側で一括反映させることで，パソコンの設定内容を統一すると同時に，使用者が勝手に設定を変更する自由を奪うことで設定内容を維持することが可能となった．

更に，旧パソコンでは HOSTS ファイルで行っていたサーバの名前解決について DNS を使用するように変更した．システム開発など，個々の特殊環境については HOSTS ファイルを使用するにしても，一般的には DNS を使用することで，各サーバの設置情報の特定を防ぐことができる．

（２）　ファイルサーバ

ファイルサーバには『個人ファイルサーバ』と『組織ファイルサーバ』の２種類があり，パソコンの入れ換えにあたっての条件であった『利用者にとって便利となる機能』として，全社員が利用できるファイルサーバを設置することとなった．

『個人ファイルサーバ』は AD サーバで管理しているユーザ ID ごとに割り当てられた個人専用のエリアを提供しており，基本的に各ユーザデータの保存場所としての位置付けである．つまり，個人情報の入ったデータを個々のパソコンに保存させるのではなく，ファイルサーバに保存させることで極力個人情報の拡散を防ぐことが目的である．

『組織ファイルサーバ』は，一定の組織単位に分割したエリアを提供しているも

のであり，それぞれの組織内に所属する社員間でのみ，データの共有が可能となっている．もともと当社内にもファイルサーバは存在していたが，一部の本社部門のためだけに本社ビル内に設置しており，一般的にはファイル共有を行う環境がなかった．そのため本社部門以外では，各組織に設置しているパソコンの設定を勝手に変更してファイル共有を行っている場合があった．しかし，ほとんどの場合はセキュリティへの考慮がなく，社内ネットワークの中ならどこからでもアクセスできる状態となっていたり，組織改変や人事異動の際には共有したまま放置されてしまうような状態であった．そこで，AD で管理しているユーザアカウントに組織情報を連携させることで，『組織ファイルサーバ』のアクセス権限を設定することで，組織改変や人事異動にもタイムリーにアクセス権の変更を反映できるようにした．また，ファイルサーバの設置場所を他のサーバと同様にデータセンタ内に設置することで，機器管理やバックアップも含めたデータの管理についてもコントロールが可能となった．

大容量のファイルサーバを構築するとバックアップの処理時間が問題となる．今回『組織ファイルサーバ』を構築検討する上で，バックアップの処理時間を試算した際には８時間程度となった．バックアップデータの真正性と運用上の利便性を考慮すると，バックアップ処理でファイルサーバを８時間停止することは難しい．そこで『組織ファイルサーバ』のバックアップには OPC（One Point Copy）によってサーバ内のデータを論理ボリュームごと別ボリュームへとコピーし，コピー後のボリュームをバックアップ処理専用のサーバで処理を行うこととした．これによってデータのバックアップ処理でサーバ機能をほとんど停止することなく，ファイルサーバの機能を提供することが可能となった．ただしこの仕組みの欠点はディスク容量が実運用の２倍必要となることである．そのため，ディスク容量不足によるディスクの増量はコスト面から見ると容易ではなくなるので，不要データの削除など，データ管理を厳しく行う必要がある．

（3） ウィルスチェック管理サーバ

旧パソコンの環境にもウィルスチェックソフトは導入していた．しかし，ウィルスのパターンファイルの更新は業務アプリ同様にプログラム配信のシステムで配布しており，個々のパソコンでの配布状況を確認することができなかった．また，中にはパソコンの処理効率を上げるために，意図的にウィルスチェックソフトを停止する者がいた．そこで，新パソコンではウィルスチェックソフトの管理サーバを構築し，ウィルスチェックソフトだけをサーバで個別管理するようにした．

ウィルスチェック管理サーバはウィルスチェックソフトをインストールしている個々のパソコンに対して，パターンファイルの更新やバージョン管理を行うだけでなく，パソコンにインストールしているウィルスチェックソフトの設定も一括管理しているため，画一的に設定変更やユーザによる勝手な設定変更によるリスクを防止することができる．また，パソコン側でウィルスチェックソフトの停止を行うにはパスワード入力が必要となっており，ユーザによるウィルスチェックの停止が行えないようになっている．

（4） 端末ログ管理サーバ

新パソコンから実現しているセキュリティ機能として，各パソコンで端末操作ロ

グを取得し，この情報をサーバに蓄積するシステムを導入した．

これは，パソコン側で『いつ』『誰（ユーザ ID）が』『どこ（コンピュータ情報）で』『何をしたか』をウィンドウごとに取得し，操作ログを随時サーバへと送信する仕組みとなっている．パソコン操作時にネットワークに接続されていない場合でも，パソコン内に操作ログが蓄積され，ネットワークに接続されたタイミングでサーバへとデータが送信される仕組みとなっているため，外部へ持ち出した際の操作ログについても取得できる仕組みとなっている．

しかし，この仕組みの限界はあくまでも操作履歴の追跡までであり，操作しているデータの内容については一切確認できない点である．つまり，特定の時間に特定の人物が特定の端末で特定のファイルについて何らかの操作を行っているということまでは判別できるが，そのファイルの内容までは判らないのである．

したがってこのシステムのセキュリティとしてのポイントは，問題発覚時の追跡システムというよりは，実際には，常に操作内容を監視されているという使用者への心理的プレッシャーの方にあるといえる．

（5） ログ蓄積・分析サーバ

前述のとおり，旧パソコンでの DB 検索システムは共通のログオン ID でオラクル DB に直接ログオンしており，また，使用していたソフトウェアの機能上，更新することも可能であった．そこで，新パソコンでの改善要件として，ユーザごとに個別のアカウントでログオンし，DB へのアクセスログを取得することが挙げられた．

ユーザごとに個別のアカウントを割り当てる方法としては AD サーバとの連携で対応し，DB へのアクセスログの取得としてログ蓄積・分析サーバを構築した．

（6） ファイル暗号化ソフト・漏洩抑止ソフト

パソコンの中だけで完結するセキュリティ対策ソフトウェアとして，ファイル暗号化ソフトと漏洩防止ソフトがある．

ファイル暗号化ソフトはその名前どおり，ハードディスクのデータを暗号化するソフトウェアであり，Windows のログオン時に連動して自動的にデータを復号する仕組みとなっている．XP にはファイルの暗号化が標準機能として存在するが，標準機能では使用者が常に暗号化ファイルであることを意識し，必要に応じて自ら暗号・復号処理を行う必要があるため，利便性の点で劣っている．しかし今回当社で導入した暗号化ソフトにも不十分な点がある．それは OS の下で稼動するソフトウェアであるため，Windows 自体のシステムファイルを暗号化することができず，そのため暗号化を行うことができる領域が制限されることである．そこで前述のとおり，AD のグループポリシーによって使用者から見ることのできるディスク領域を制限することで使用者が暗号化できない領域にデータを保存することができないように工夫をした．

漏洩防止ソフトとはフロッピーディスクや CD-R，USB メモリといった外部媒体へのデータ保存をソフトウェアによって禁止するものである．ソフトウェアによってデータの保存先を制御するメリットとしては，フロッピーディスクやＣＤ，USB メモリからの読み込みに制限をかけることなく，書き込みだけを制御できる点である．また，想定外の機器を現地にて不当に持ち込み接続されたとしても，ソフトウェアの制御であればほとんどの場合書き込みを抑止することが可能である．

このように漏洩防止ソフトを導入し，基本的には外部媒体へのデータ保存を抑止しているが，監督省庁への資料提出や団体顧客へのデータ提供など，業務上外部媒体へのデータ保存が必要である場合がある．そこで，USB 接続のソフト解除キーによって外部媒体への保存をしているという操作ログを残してデータの書き出しができるような仕組みを導入している．このように，USB 接続のソフト解除キーの持ち出し管理と操作履歴の保存を行うことによって，パソコンからのデータの持ち出しを完全に防止していないものの，一定の抑止効果を持たせている．

３．３　セキュリティ対策の運用

このように，セキュリティ対策として様々なサーバとソフトウェアを準備し，新パソコンの使用環境を整備したが，最終的には当初の計画どおりに運用ができなければ全く意味がなくなってしまう．そして今回の入れ換えのように，パソコンの運用環境が劇的に変化する場合，新しい仕組みの使用方法や新環境の運用ルールをある程度でも使用者に通知しておくことで運用についてもスムースに移行できると考えた．

そこで，新パソコンへの入れ換えに先立って，新パソコンで実現しようとしている新機能や新しく予定している運用ルールについて，回を分けて社内の掲示板のシステムに『PC リプレイス NEWS』（図３参照）として掲示し，通知を行った．

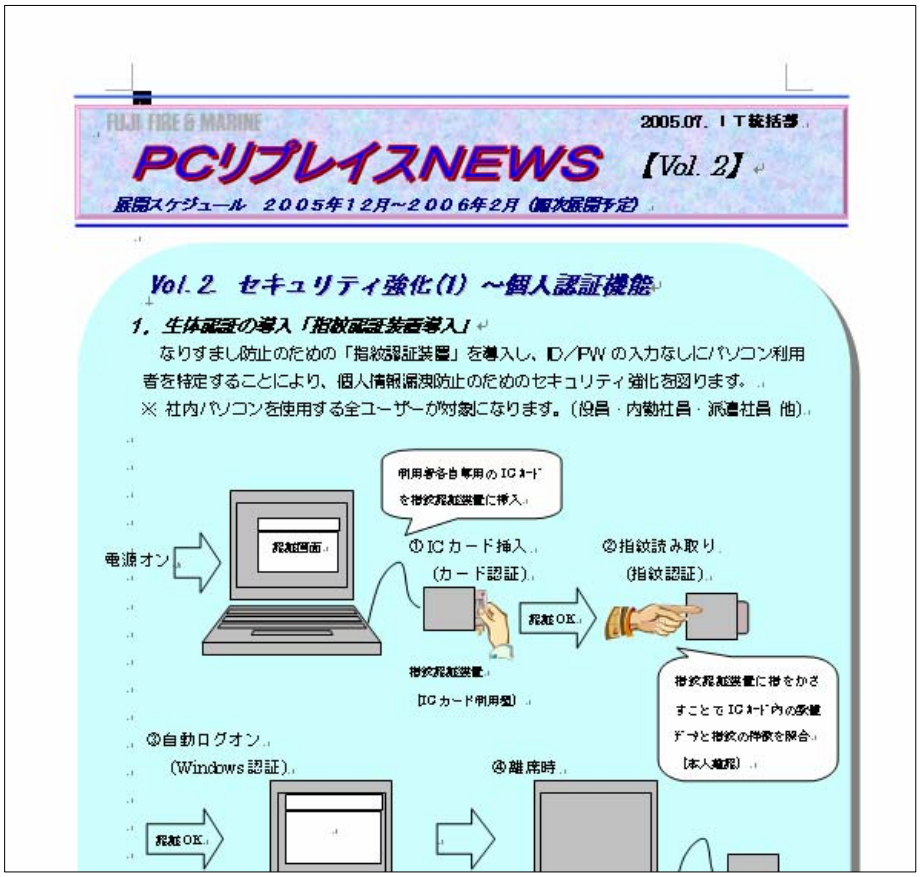

図３　『PC リプレイス NEWS』

『PC リプレイス NEWS』は１か月に１～２回程度の割合で合計８回に分けて掲載を行った．『PC リプレイス NEWS』は使用者全体に新パソコンへの興味を持ってもらう機会となり，また，会社としてのセキュリティ対策を周知する効果があったと思われる．

『PC リプレイス NEWS』で掲載した新しい運用ルールについては，新パソコンの入れ換えを行う前に文書化し，社内システムの掲示板に掲載するとともにパソコンの入れ換え作業の通知と併せて通知することで使用者への周知徹底を図った．

４．今後の課題

４．１　セキュリティの監視

これまでに述べてきたとおり，新パソコン内のシステム設計にあたって，リスクとなりうる様々なパソコンの操作を監視し，記録するようにしている．しかし，従来のシステムにはこのような端末の操作記録を点検・監視するといった運用フェーズがなかったため，現状ではログ解析の手順や手法も含めたトータルでの監視体制が十分な状態とはいえない．

また，これらの記録された各種のログの保存期間を現状では１年間としているが，１年間で蓄積される全パソコンの操作ログのファイル容量についても現状では不明である．

したがって，監査要件で特定のデータが流出した経路を調査する必要が発生した場合，現状ではどれくらいの時間が必要となるかは不明である．

このように，セキュリティの監視手法と体制の強化は今後の運用上の課題といえる．

４．２　セキュリティ問題への対応

新パソコンで構築した各種システムのシステム設計・構築作業を行っていく中で，当然のことながら各システムのバックアップやリストアについて，実機による単体テストや総合テストを実施している．しかし，これらは主にハード障害を想定した対応である．つまり，ウィルスの混入など社内ネットワーク全体に影響を与えるようなセキュリティ上の問題が発生した場合の対処方法やシステム復旧方法についても，社内ネットワーク全体での復元方法を想定しておく必要がある．

４．３　リスクの変化とセキュリティ対策の見直し

このように新パソコンではパソコン単体での機能だけでなく，パソコンを管理するサーバの新規設置や使用ルールの変更によって，セキュアな環境であること自体をパソコンの機能の一部として環境構築を行った．しかし，OS のセキュリティホールや業務システム上の新機能の追加，パソコン使用者による想定外の利用方法など，運用環境の変化を止めることはできない．そのため，定期的に運用環境の変化に合わせてセキュリティ対策の見直しを計画する必要がある．

５．おわりに

このようにして新パソコンでのセキュリティ向上対策は予定どおり開発が進行したが，業務アプリケーションの操作性や現地でのパソコン入れ換え作業で問題が発生しないことを慎重に確認するために試行実施期間を延長した．そのため，実際に入れ換えを開始したのは当初の計画より遅れて 2006 年５月からとなった．９月には全パソコンの入れ換えが完了し，11 月現在では順調に新パソコンが運用されている．

しかし，セキュリティ対策の本質はセキュリティの品質を維持することであり，これか

らも教育や改善を継続していくことが重要だと考えている.

最後に，新パソコンの入れ換えに係わったすべてのスタッフと，弊社の試みに対して執筆の機会を与えていただいたFUJITSUファミリ会に対し，厚くお礼申し上げます.

以　上