名古屋工業大学博士論文
甲第542号(課程修了による)
平成１８年３月２３日授与

博士論文

情報資産の効果的保護方法の研究

２００６年

児玉　充晴

目　次

第４章　情報漏えい対策システムへのＵＳＢキーの適用

第５章　情報漏えい対策システムへの指紋認証の適用

第６章　情報漏えい対策システムへのＳＢＣ方式の適用

第７章　国際業務システムへのＳＢＣ方式の適用

第1章 緒言

1.1 概要

情報資産を活用する情報システムが、単なる業務処理にとどまらず、戦略的な役目を果たすようになり、急速な技術革新とインターネットの普及によって、その効率性が飛躍的に高まっている。しかし、これらの恩恵に反して、ネットワーク化された情報システムの発展に伴い、不正アクセスや内部からの情報漏えいなどにより、故意か過失かを問わずさまざまなリスクの発生が社会的な問題として注目されている。さらに、クレジットカードの個人情報のような情報資産の流出など、経営的な問題にもおよぶ問題も表面化している[1]。このような問題に対処するためのセキュリティ対策は、個人情報保護法の制定に伴って重要性を増している。このことから、情報資産保護方法の研究は、社会的に見ても大変重要なテーマである。

本章では、1.2項で情報資産保護に関する社会動向を述べ、1.3項で情報資産保護に関する現状と問題点を整理している。1.4項で最近の研究動向と本論文の研究活動全般における位置づけを整理し、1.5項で本論文の構成と概要を示している。

1.2 情報資産保護に関する社会動向

情報資産に関する取り組みは、世界的に見ればすでに 1960 年代から始まっている。その背景には、このころから情報資産のコンピュータ処理が拡大したことにある。1970年代には、ヨーロッパ各国で情報資産のひとつである個人情報の保護に関する法律が次々と整備され、1980年9月には、経済協力開発機構（OECD）が「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択し、ヨーロッパ各国の情報資産保護に関する法律に対し、国際的な方針が示されている[2]。

日本でも情報資産の管理が重要視される状況を踏まえ、1988年に「行政機関の保有する電子計算機処理に関する個人情報の保護に関する法律」が施行され、1989年には「民間部門における電子計算機処理に係る個人情報の保護について」という指針が通産省によって定められている。その後、1997年には通産省が「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を制定している。さらには、1998年にプライバシーマーク制度が発足している[1]。

また、1980年代から実施されてきた「不正競争防止法」や「不正アクセス禁止法」の施行に見られるような情報資産保護の法整備も進み、また、各省庁からも「セキュリティ対策のためのガイドライン」が2004年までに順次出されるようになってきている。

この中で注目されるのが、2005年4月1日から施行された「個人情報保護法」である。これが全面施行されることで、5000件以上の個人情報を保有する事業者は「個人情報取り扱い事業者」として、個人情報の適切な管理を行う義務が生じることになる。法律違反に対する罰則は、6ヶ月以下の懲役または30万円以下の罰金というもので、罰則内容は必ずしも重いものではないが、個人情報の取り扱いに関する企業責任が、明確に示された点が重要である[2]。

以上のような法整備と平行して、企業においては情報資産を適切に保護するための統一方針である「セキュリティポリシー」を定めたり、グローバルスタンダードであるBS7799やISMSの資格取得を行う動きも出始めている[1]。情報資産を保護することが必要となった背景には次の社会情勢があげられる。

（1）労働力の流動化に伴う会社に対する社員の忠誠心の変化
（2）社員からアクセス容易でかつ情報資産保全ができる管理方法の必要性の向上
（3）ＩＴ技術の普及による情報漏えいの容易性の向上
（4）インターネットの普及による企業とユーザとの力関係の逆転

また、情報資産を管理する側の状況として、以下の点がリスクとしてあげられる。

（1）情報システムのオープン化によるぜい弱性の露呈
（2）１人１台パソコン（PC）にみられる情報システムの普及
（3）PCへのデータのダウンロードするタイプのOSの普及
（4）アウトソーシングや他店舗展開など情報資産の分散化に伴う管理の不徹底
（5）内部告発と企業情報の開示義務の位置づけの混在傾向の増大

以上の動向をベースとして、企業等において、効率的かつ有効な情報資産の保護対策が急務となる社会状況にあるものと考えられる。

1.3 企業等における情報資産保護の現状と問題点

企業等における情報資産保護の現状と問題点については、上場企業438社を対象に、総務省「情報セキュリティに関する実態調査結果の公表」（平成16年7月5日）に調査結果として詳しく示されている[3]。

詳しい分析内容を第3章3.3項で述べることとするが、要点を整理すると以下のようになる。

（1）セキュリティ対策のベースとなるセキュリティポリシーのノウハウが少ない。
（2）セキュリティポリシーを保障するための施設系での対策の裏づけが難しい。
（3）セキュリティ対策への費用が、パソコン１台あたり、平均2.1万円を中心としてせいぜい１万円～３万円程度である。このような金額で、どんな対策をどんな優先順位で実施したらよいかわからない。

これらの内容を総合すると、企業における情報資産保護への社会的な研究ニーズは、“コストパフォーマンスが良い既存の業務システムへの情報資産保護対策の研究”ということになるであろう。

1.4 最近の研究動向と本研究の位置づけ

企業内の重要な情報資産を保護するという観点において、従来、外部からの不正アクセス対策の研究が盛んに行われて来た。しかし、最近、顧客情報を始めとする企業機密の漏えいが多発するようになり[4][5]、企業のイメージがダウンするとともに、致命的な損害を被ることから、喫緊の社会問題となりつつある。これらの状況から、個人情報保護の社会情勢にも対応して、企業において、最近、セキュリティポリシーを策定して社員教育を行うところが多い[6]。

これらの情勢を踏まえて、標準ガイドラインや認定制度に基づく、セキュリティポリシー策定の方法と具体的適用方法の研究が内田により行われている [7]。また、リスク管理に基づくセキュリティ教育の研究[8]が桑原により行われ、セキュリティ品質設計における障害発生頻度と被害額検討の尺度の研究[9]も村上らにより行われている。
これらの研究により、セキュリティ管理の基本と人間によるセキュリティ管理のあり方が明らかにされて来た。しかし、公開鍵証明書を用いた病院向けの利用者認証システムの研究[10]が坂本により行われているように、既存システムへの情報漏えい対策の研究は緒についたばかりである。

このような研究成果を適用する側の一般企業においては、コスト高となる厳密なセキュリティレベルを求めている訳ではない。機密情報を扱うオフィスという環境下で内部情報を漏えいしないための、コストパフォーマンスの良い対策を求めているのである。今後の研究では、このような条件下での既存の情報システムに対するセキュリティ対策の工夫が必要となる。

最近のセキュリティ技術関係の、研究動向の分析結果の概要を表１に示す。調査対象は電子情報通信学会研究報告（情報セキュリティ：2004-05～2005-02）に記載されている合

計 135 報告である。この中では、基礎研究 63 件、実用化研究 40 件、応用研究 19 件であり、実導入までを包含した研究の少ないことがわかる。また、この研究動向の分析の結果、以下のような特徴が判明している。

（1）要素技術におけるある弱点部分に関する改善の研究が多い。
（2）方式の提案においてはシミュレーションが多く、実導入による効果の評価はきわめて少ない。
（3）外部からのアタックを想定されているケースが多く、内部からの情報漏えいが想定される研究は少ない。
（4）“セキュリティの強度上の欠陥を解消することによる軍事レベルのセキュリティ”までを求めない、一般企業のニーズに応えるような応用研究がきわめて少ない。

表1 最近のセキュリティ関係の研究動向の分析結果

Table 1 The analysis result of the recent research trend related to security.

No	分　　野	報告数
1	(基)　暗号方式関係	１７
2	(実)　攻撃回避方式関係	１２
3	(基)　セキュリティの関数や数値解析関係	１１
4	(基)　ネットワークセキュリティ関係（含無線ＬＡＮ他）	１１
5	(基)　セキュリティプロトコル関係	１０
6	(実)　攻撃検知、追跡方式関係	１０
7	(実)　共通鍵、鍵配送関係	9
8	(実)　署名方式関係	9
9	(応)　実装のためのモデル化方式検討関係	8
10	(応)　検出、モニタリングシステム攻撃関係	7
11	(基)　数値モデル、シミュレーション関係	6
12	(基)　乗算回路、素因数分解関係	4
13	(基)　一般数体篩法関係	4
14	(応)　電子投票の方式提案関係	4
15	その他　（リスク評価法、アクセス制御方式、バイオ認証、他）	１３

（注）（基）：基礎研究（63 件）　（実）：実用化研究（40 件）　（応）：応用研究（19 件）　合計：１３５件

本論文では、“たくさんあるセキュリティ対策技術を限られた予算の中でどう選択し、実現するか？”という社会のニーズにこたえるために、応用研究の先にある個別技術の実用化に重点を置くこととしている。具体的には図１に示す範囲の概念で研究を実施している。本論文は、個別技術を社会に適用する実用化研究であるため、図１にあるように電子情報通信学会寄りの研究部分もあるが、情報文化学会寄りの研究内容の傾向も大きい。このことから、研究内容ごとへの情報文化学的な考察も、関係する章（第２章、第７章）の中で記述している。

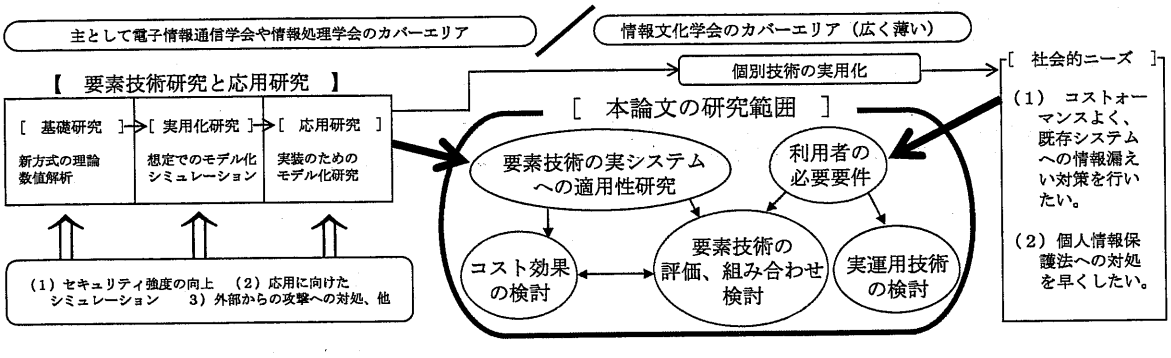


図1 本論文の研究範囲

Fig.1 The range of the research of this paper.

研究のターゲットとして、法的な規制を前にしてセキュリティ対策に戸惑っている一般企業に焦点をあてている。技術的にはコスト効果の高い要素技術を抽出し、その組み合わせや方式設計に重点を置いて研究している。また、保守運用性にまで視点を広げて研究し、社会への即効性ある効用を検証している。さらに、この研究の延長線上にある、社会インフラとしての共同利用型のセキュリティプラットフォームについても検討を加え、各企業で共同利用できるシステムの、今後のあるべき姿についての提言を述べている。

従来の工学系の論文では、既存技術の問題点を解決するというタイプのものが多い。本論文はこのタイプとは異なり、企業のニーズに基づいて、すでにある要素技術をどう研究・工夫してインテグレーションし、企業一般へ実際に活用してもらえるか？に重点を置いている。このことから、分野としては経営工学や総合工学の分野の論文という位置づけとなる。この観点から、第３章 3.2 項で、要素技術をニーズ要件に応じてインテグレーションしてシステムとして実現する方法論を抽象化・一般化して論じている。

1.5 論文の構成と概要

本論文の構成と研究内容の概要は以下のとおりである。

（1） 人間系による情報漏えい対策（第２章）

最近の情報漏えい事件の分析から、人間系での問題点から情報漏えいが発生していることを示している。また、セキュリティ教育の実態を調査した結果から、ｅ-ラーニングの必要性を研究している。この中で、受講証跡を残すｅ-ラーニング技術の必要性を明らかにして、その適用方法や導入コストについて述べている。さらに、最も安上がりである社員満足を生み出すマネジメント方法についても言及し論じている。

（2） 施設系による情報漏えい対策（第３章）

企業のニーズを技術で実現するための方法論を抽象化・一般化して論じている。これに基づき、セキュリティ対策に関する実態調査の結果を分析し、施設系での取り組みのポイントとセキュリティ対策へ投資できる金額の値ごろ感を導出している。また、現状のセキュリティ技術全体を整理して、投資できる金額の値ごろ感を前提として、本論文で研究対象とする技術要素を選定して絞込みを実施している。さらに、情報漏えい対策の高度化の道筋について論じて、主に第４章から第７章に検討するセキュリティ対策のための技術を抽出し、今後の発展性の方向を述べている。

（3） ＵＳＢキー（別紙：用語説明(4)）を利用した情報漏えい対策システム（第４章）

一般の企業が、まず簡単かつ安価にセキュリティ対策ができることを主眼に、ＵＳＢキーによるセキュリティ対策を研究する。１万円以下／パソコンを目標として、従来のＩＤ/パスワード方式で構築されたシステムへのオーバーレイでの導入を目指している。この中では、ＵＳＢキーを用いた方式設計の工夫のみならず、運用での工夫なども紹介し、さらに企業への導入効果について検証している。この結果、数千円／パソコンのコストでの、最大限のセキュリティ対策ができることを示している。

（4） 情報漏えい対策システムへの指紋認証の適用（第５章）

前章の発展形態として、安価なバイオメトリックス（別紙：用語説明(6)）による本人性確認方法として、指紋認証を取り上げ、２万円以下／パソコンを目標価格として、実現方法を検討している。ここでは実際に発生したセキュリティ事故から抽出された要件をもととして、指紋認証の既存システムへの適用性を技術検討している。その内容を実地テストで検証し実用化できることを提起している。さらに、運用における工夫やその副次効果などについて紹介し、企業での利用が可能であることを明らかにしている。

（5） 情報漏えい対策システムへのＳＢＣ方式（別紙：用語説明(1)）の適用（第６章）

情報漏えい対策として有効なＳＢＣ方式の適用について、保険代理店における情報

漏えい問題を取り上げ、代理店システムへのＳＢＣ方式の適用を試験検証している。さらに大手金融機関にＳＢＣ方式を導入して、大きな経済効果をあげうることを証明している。また、ペーパーレスシステムへの適用等、今後の発展形態についても論じている。

（6） 国際業務システムへのＳＢＣ方式（別紙：用語説明(1)）の適用（第７章）

前章の導入実績をふまえ、企業における国際業務システムへのＳＢＣ方式の適用について、損害保険会社に導入した実際の事例をもとに研究している。方式設計の内容を示すとともに、導入による検証結果を紹介し、ＳＢＣ方式が国際業務システムで使用できることを証明している。さらに、このシステムを安定的に利用するために、マルチホーミング（別紙：用語説明(14)）によるインターネットＶＰＮ（別紙：用語説明(12)）の通信品質の向上方法を提起している。さらに、情報共有の観点から、本章で述べる方式の有効性を論じている。

（7） 共同利用型セキュリティプラットフォームへの発展形態（第８章）

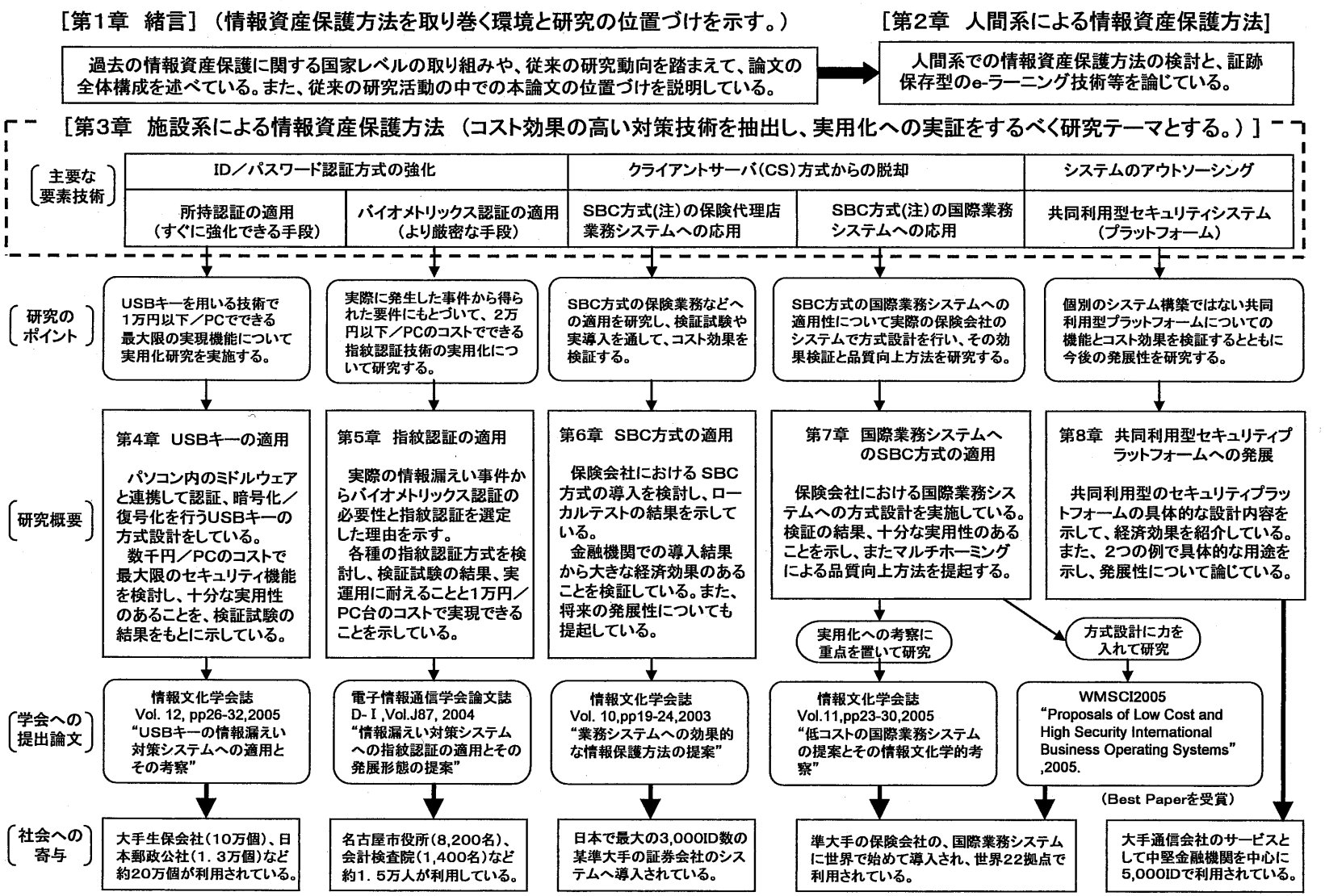
ブロードバンド常時接続が企業において多数導入されている現状をふまえて、セキュリティ処理機能をセキュリティプラットフォームにもたせて、企業間で共同利用する方式について研究している。セキュリティプラットフォームの構造を示すとともに、実際の利用におけるコスト検証の結果を紹介している。さらに、具体的な２つ用途の事例を提起して、このセキュリティプラットフォームの活用方法を示し、社会インフラとしての将来の発展について論じている。

（8） 結言と業績のまとめ

論文全体の締めくくりとしての研究成果や今後の課題をまとめて述べている。また、謝辞を示すとともに、業績としての査読つき論文、査読なし論文、表彰、著書、出願特許についても記載している。また最後の（参考）に本論文が社会に果たした役割について、導入実績と記事でまとめて紹介している。

論文全体の構成を図２に示す。ここでは、効果的な情報資産保護の研究の進め方のストーリーを述べている。人間系と施設系の関係を明らかにして、施設系でのセキュリティ対策に必要な技術要素を抽出している。この要素技術を実用化して、十分なコスト効果があるかどうか、実導入による検証を実施している。

図２では、さらにこの研究の目的と研究概要を簡記するとともに、学会の論文誌に採録された査読つき論文名や、社会への寄与についても簡単にまとめて示している。



（注）SBC（サーバベースコンピューティング）方式：クライアントパソコンとネットワークを介したサーバとのやり取りを、「マウスクリック」、「キーストローク」、「画面遷移の処理」に限ることで、速度の向上や、各種の制限の解消などのメリットを得ようという方式。ハードディスクを用いないので内部情報漏えいの対策になる技術で、海外の金融機関では多用されている。

図2　論文全体の構成

Fig.2　The composition of this entire paper.

1.6 まとめ

本章では、情報資産保護に関する法整備の状況と、最近の社会動向を整理している。また、過去の研究の動向から本研究の位置づけを明らかにして、“コストパフォーマンスが良い既存の業務システムへの情報資産保護対策の検討”という、研究のポジションを示している。さらに、本論文の指針になるように、論文構成と内容の概要を紹介している。

[参考文献]

[1] 小栗正嗣ほか,“個人情報保護全対策”,週刊ダイヤモンド,2005 年 3 月 12 日日号, pp. 31-57, Mar. 2005.

[2] “個人情報漏えい対策”,日経ビジネス,2004 年 12 月 20 日・27 日号, pp. 101-106, Dec. 2004,

[3] 総務省,“情報セキュリティに関する実態調査結果の公表”, pp. 44-45, pp. 60-61, Dec. 2004, http://www.soumu.go.jp/s-news/2004/040705_2.html.

[4] 岡村久道,“続発する個人情報漏えい事件”,日経バイト,2000 年 8 月号, pp24, Aug. 2002.

[5] “ワイド特集：ディジタル時代における企業機密の漏えい防止”, Telecom Forum, 2003 年 1 月号, pp. 7-12, Jan. 2003.

[6] 森宮 康,“情報管理一般について”,わが国における情報セキュリティの実態の概要, pp. 5-6, (財)日本情報処理開発協会,東京,2002.
http://www.jpdec.jp/security/01sec.htm.

[7] 内田昌宏, “特集 1：セキュリティ・ポリシー策定のためのガイドラインから手順まで”, Computer&Network LAN, 2003 年 2 月号, pp. 8-36, Feb. 2003.

[8] 桑原 悟,“組織の情報セキュリティ実現のための組織内外の役割とその逐行に必要な教育に関する検討”,情報処理学会,第 63 回全国大会予稿集, 3-621, 2001.

[9] 村上英世,坂本弘章,幸 徳雄,“セキュリティ品質の検討”,信学技報, vol. 102, pp. 103-109, July, 2002.

[10] 坂本憲弘,“公開鍵証明書を用いた国立大学病院保険医療情報利用者認証システムの開発”,信学論 (D-Ⅰ), vol. J84-D-Ⅰ, no. 6, pp. 830-839, June, 2001.

第2章　情報資産保護に関する人間系による情報漏えい対策

2.1 概要

情報漏えい対策の基本は「人」であり、企業においては、その忠誠心に基づく精神的規則として社員就業規則や外部委託規約などがある。しかし、現実的な情報漏えい対策としては、人に依存する部分とシステムに依存する部分（機械警備）に分けて分担を考える必要がある。人に依存する部分においては、セキュリティポリシーに基づく各種ルールの遵守が求められる[1]。また、問題発生時のリスク分析も重要な考慮の対象となる[2]。さらに社員教育や社員の心に悪心を起こさせないためのマネジメント法も大切である。

本章では、2.2項で実際に発生した事件の分析における人間系での問題点と対策について考察している。2.3項で企業のリスク分析に基づくセキュリティ対策費用の考え方について論じている。2.4項で証跡保存型のe-ラーニングシステムの開発内容とその所要費用を紹介している。また、2.5項で社員の心の満足を与えるマネジネント法についても論じている。

2.2 情報漏えい事件への分析と情報文化学的考察

情報資産の保護対策については、予防措置と事後措置に分けて検討する必要がある。

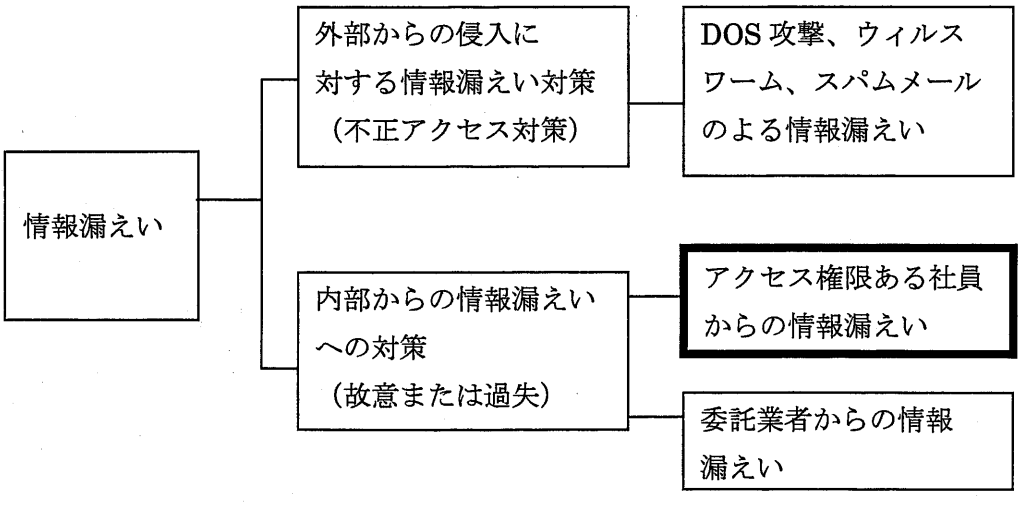


図1　情報漏えいの分類

Fig.1　The classification of information leakage.

本論文では、事後措置ではなく、予防措置に注目して情報資産保護方法の研究を行うこととしている。

予防措置については、図 1 に示すように外部からの侵入と内部からの情報漏えいに分けて検討することになる。本論文では、以下に示す実際の発生事件の分析に基づいて、“外部からの侵入”ではなく、社会的ニーズの高い“企業内部からの情報漏えい”に重点を置くとともに、図 1 の分類のうち、“アクセス権限ある社員からの故意または過失による情報漏えいへの対策”に焦点をあてて研究している。

本章での研究の基本検討は、新聞報道への分析をベースとしている。典型的な事件の報道例を表 1 に示す。この表にもあるように、最近の個人情報流出事件の経緯はほとんど似通っており、主に次の３つのパターンのあることがわかる[3]。

(1) 外部からの侵入ではなく、アクセス権を有している社員を介して情報漏えいが発生していること。
(2) 大規模情報漏えいではサーバ側から情報が抜き出され、小規模情報漏えいではクライアントパソコンから外部記憶媒体や印刷を介して漏えいしていること。

表1 2004 年 6 月に発覚した主な個人情報流出事件例

Table 1 The main individual information leakage events that came to light in June, 2004.

発生年月日	企業・団体	流出規模	コンテンツ	流出経緯	流出媒体
2004 年 6 月 2 日	阪急交通社	62 万件	氏名、住所、電話番号、生年月日、職種	アクセス管理用サーバから抜き取りか？	サーバ
2004 年 6 月 8 日	コスモ石油	92 万件	住所・電話番号など	下請け業者より流出	サーバ
2004 年 6 月 11 日	埼玉りそな銀行	424 件	氏名や電話番号、普通預金残高など	帰宅途中に私用カバンをなくし、中に入っていた顧客資料を紛失した内規違反	紙
2004 年 6 月 21 日	P&G、BSI	1 万件	視聴者情報	パソコンにCDを入れたまま廃棄	ディスク
2004 年 6 月 22 日	大和ハウス	35 万 7000 件	賃貸住宅のオーナーなどの住所、氏名、電話番号や土地に関する情報	オフィスからのパソコンの盗難	ディスク
2004 年 6 月 23 日	みずほ銀行	254 件	融資額や信用リスクの格付けなど	パソコンの置き忘れ	ディスク
2004 年 6 月 25 日	中央三井信託銀行	493 件	氏名、住所、預金の取引状況	嘱託社員が紛失、場所不明の内規違反	紙

(3) クライアント側からの情報漏えいの原因は、悪意のみならずミスも多いこと。

この３項目の共通点は、いずれも人間系での問題点が基礎にあることである。

本章では、この人間系での情報資産保護方法検討の前に、情報文化学的観点から見た、人間系での企業における情報資産保護の位置づけを明確にすることとする。

情報文化学でいう、理念系・人間系・施設系の主要３軸および社会系の４つの分野について、考察した結果を以下に示す[4]。

理念系においては、情報漏えいに伴う企業価値の減価に着目する必要がある。企業価値には、収益性や株価のように数値化できるもの以外に、ブランドやステイクホルダとの信用関係などの非数値化の要素もあげられる。この中で、「不十分な情報漏えい対策が原因で、収益性などの企業価値がどの程度低下しているか？（低下する恐れがあるか？）」という有形・無形のリスク分析に伴う“企業価値の減価評価”を検討する必要がある。

人間系においては、企業への忠誠心に基づく精神的規則としての社員就業規則などの遵守が求められる。この中で、人間系での問題発生を想定したリスク分析が、重点対策分野を定める上で必要であり、この重点分野への社員教育が効果的である。ただし、忠誠心に基づいて行われるセキュリティ教育は低コストではあり効果的であるが、情報漏えい対策として見た場合、人間が介在することから過失の可能性もあり、ある程度の限界が存在する。

施設系においては、企業システムが有するセキュリティ機能の最適設定が、人間系の持つ過失のような不完全さを補完するために必要となる。第３章 3.4 項に詳述するように、この機能の内訳として、認証とサーバアクセスコントロールを中心として様々な管理機能があげられる。施設系においては、システムの創設費のみならず業務システムの維持・運用のための人件費なども含む“広義の所要費用”と、“システムで達成すべきセキュリティ対策とそのセキュリティレベル”という観点での検討が重要となる[5][6]。

社会系においては、情報漏えいが発生する以下のような社会的な背景があげられる[7]。

(1) 企業のリストラや人材の流動化により、社員の企業への忠誠心が薄れる傾向にあること。
(2) 企業不祥事の多発に伴い、社員の内部告発の心理障壁が低下し、国も奨励していること。
(3) IT 技術の進展により、企業内の重要情報の入手が簡単になってきたこと。

この状況への対応として、本章 2.5 項で論じている社員の心の満足に向けた人間系に対する経営改善努力が企業に求められる。

本論文の表題にある、“効果的な”の言葉を因数分解すると、“現実的な情報漏えい対策をリーズナブルな費用で実現” するべく研究することになる。この観点から、上記の各系のうち人間系（人間警備）での対策を、施設系（機械警備）での対策との関係で考えることとしている。

大きな投資をもとに、施設系での対策を強化すると、高度なチェック機能をもとにセキュリティ管理が充実する。その結果、セキュリティに関して大幅な“人間系”への負担軽減が図れることになる。しかし、施設系であるコンピュータへの依存が高まる結果、セキュリティ教育へのニーズの低下、あるいはセキュリティポリシーやルールの軽視という現象を惹起することが懸念される。

会社の業務システムへのセキュリティ対策は、企業活動全般にわたる広範な対策の一部であり、全般的な対策はやはり人間系で行わざるを得ない。施設系への対策を行うと同時に、社員自らがセキュリティ対策を担うという、“Awareness”を全社的に高めることが必要となる。この具体的方法として、以下に示す個人の業績評価に基づく人事制度の適用が有効であると考えられる。

(1) セキュリティマネジメントを業務として実施する者を指定し、実施目標を事前に定めてその達成度を評価する。
(2) セキュリティルールを守る側の者については、ルールの理解、遵守、実践という項目に対して、組織内部の模範となりうるレベルの目標を定め、その達成度を評価する。

上記(2)においては、ルールの理解、遵守、実践のみならず、①問題発生時の対処策を案出できるレベル、②未然に問題発生を防ぐべく活動できるレベル、③ルールの定着に向けた施策を案出して組織内に展開できるレベル、という順にレベルをクラス分けし、目標設定する方法もセキュリティマインドの向上に対して有効であろう。施設系へのセキュリティ対策を契機として、会社にとって「全社的な人間系での運動論での対策」にしてゆくことが大切となる。

2.3 費用面から見た人間系での情報漏えい対策の考え方

人間系と施設系が連携する対策の最適解を検討するためには、前 2.2 項の理念系にある企業のリスクに伴う企業価値の減価評価が必要となる。この評価作業においては、主として社員のセキュリティ意識を含めた全社的なリスクの抽出・分析と、そのリスクに伴う逸失利益の検討を行うことになる。

企業の減価評価の進め方を図２に示す。トップの理解と支援のもとで、推進組織を旗揚げしてリスク要素を抽出し、その対応方針や対策実施計画の策定・推進するとともに、そ

の効果の測定が大きな柱となる。この結果としてリスク分野別に、“人間系と施設系の分担により実施すべき、所要強度でのセキュリティ対策”と、対策にかけても良い費用との関係が明確となる。

セキュリティ対策として支出すべき費用の分類の考え方は、図３に示すとおりである。人間系での、セキュリティ対策と、それを補完する施設系でのセキュリティ対策の仕切りのレベル設定が大切である[8]。この場合、過失ミスの防止や故意による情報漏えい防止する対策をどこまで実施するか？によって人間系での費用のかけ方が変わる。施設系でのセキュリティ対策を充実すればするほど、システム関係の費用は高コストになるが、自動化が進むおかげで、人間系である社員の負担（コスト）は低下し、教育コストも低下するという関係がある。しかし、施設系の対策を充実させるためのコストには際限がなく、一般的に高額になりがちである。このことから、比較的費用が安い社員への意識向上研修のような取り組みに重点を置く傾向になりやすい[9]。

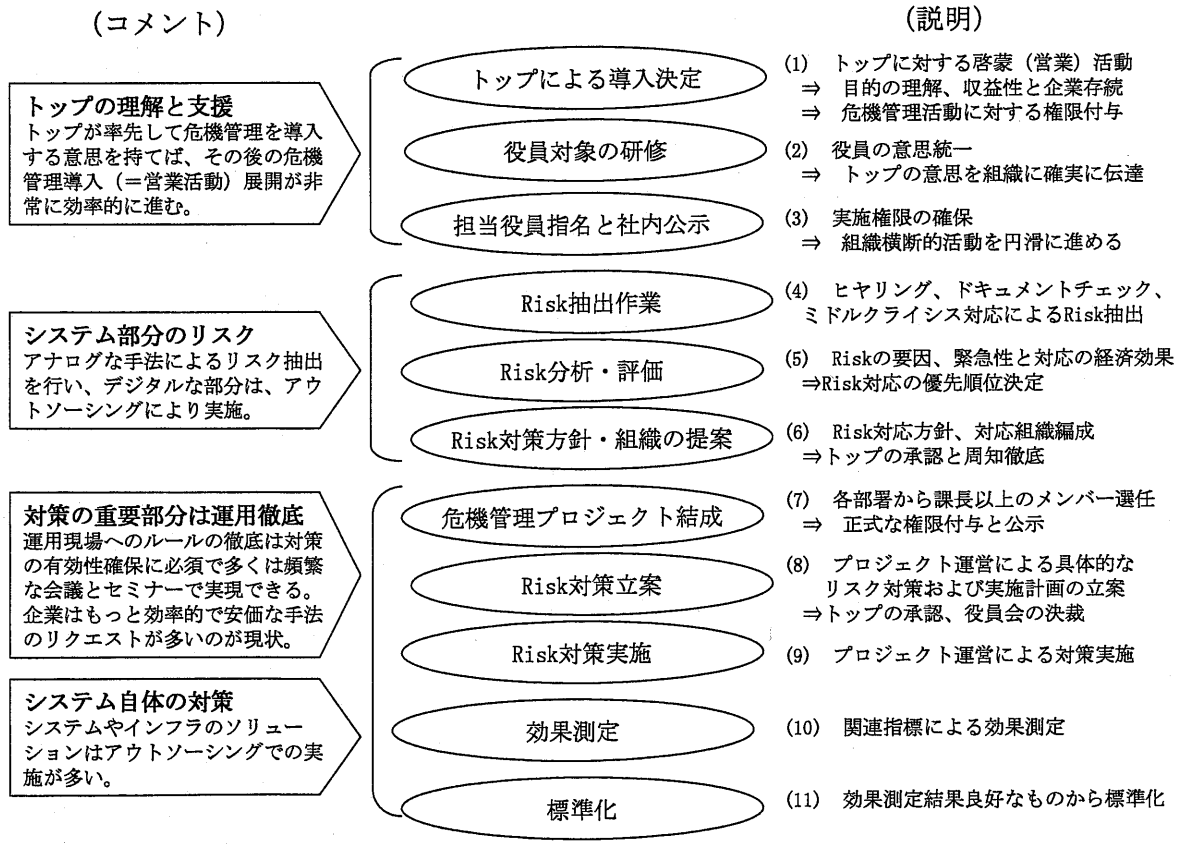


図2 リスク評価と対策検討のステップ

Fig.2 The steps of risk evaluation and measures examination.

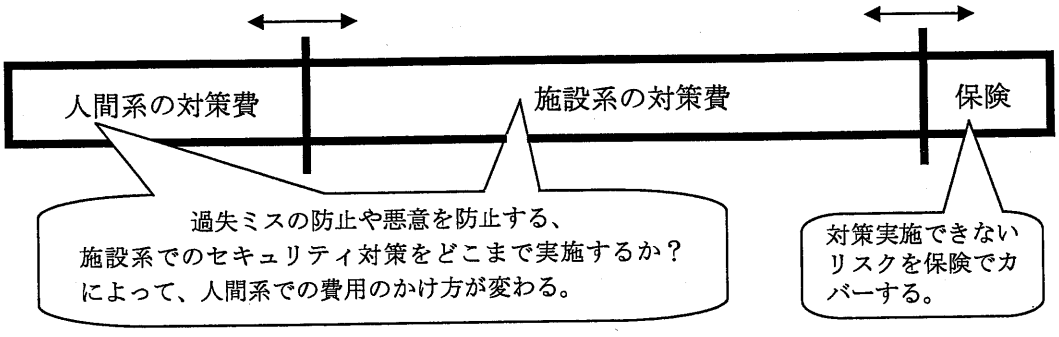
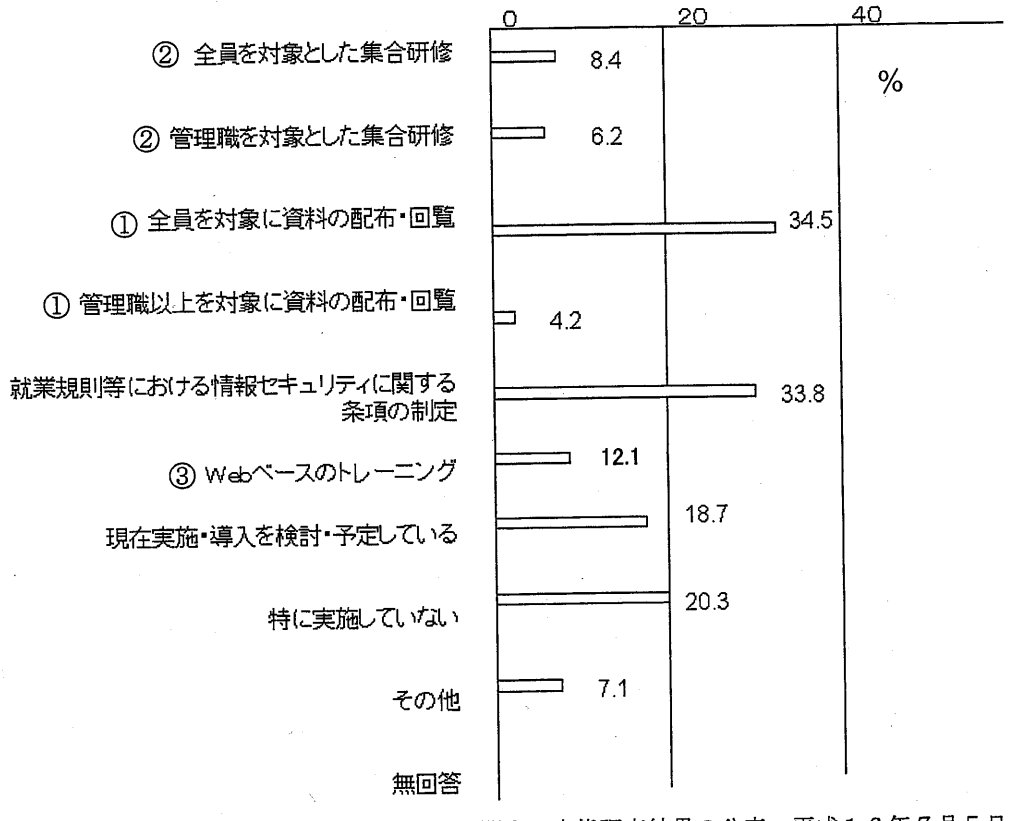


図3　セキュリティ対策の費用の内訳の考え方

Fig.3　The breakdown of the costs for security.



〔注〕総務省「情報セキュリティに関する実態調査結果の公表」平成１６年７月５日より転載

図4　情報セキュリティ教育の実施状況

Fig.4　The execution conditions of information security education.

総務省「情報セキュリティに関する実態調査結果の公表」の結果を図４に示す[10]。ここにあるように、上場企業においても、セキュリティに関する条項を制定して、資料を配

布回覧しているだけのところが多い（図４①）。また、セキュリティ教育を実施しているところは全体の１割以下で殆んど行われていない（図４②）。さらに、Ｗｅｂベースのトレーニングである e-ラーニングも１割強でしか行われていない（図４③）。

情報セキュリティ教育は、情報資産保護のためには安上がりな方法である。このことから、資料配布の対応レベルから、研修実施のレベルに今後強化されるものと考えられる。

集合研修は、実業務の時間を消費するとともに、交通費・宿泊費もかさむことが問題である。今後は e-ラーニングによる教育が、高速広帯域ネットワークの進展と１人１台パソコンの普及に伴い、急速に普及するものと考えられる。

この流れの中で、企業においては、以下の対策の検討が必要となる。

(1) 施設系への対策費と比較して費用が安い社員への教育を、企業活動で最もコストが高い人件費への圧迫が少ない方法で効率的に実施する。
　→ e-ラーニングの活用
(2) 万一事件が発生した場合、社員個人の問題に帰着させて極力企業を守りたい。このために、企業として社会的に責任を果たしている証拠とするべく受講証跡を残す e-ラーニングを導入して事前に対策措置しておく。
　→ e-ラーニングへの受講証跡の保存機能の付与

以上の検討経緯から、次項に述べる証跡保存型 e-ラーニングの開発検討を実施している。

2.4 証跡保存型 e-ラーニングの開発検討

社員にセキュリティ教育を受講させたとする証拠を残し、証拠データとして保存するためのシステムに必要となる要件は次のとおりである。

(1) 本人受講時の画像記録による、なりすましや離席のチェック。
(2) 受講時刻の確定のための配信された教育コンテンツで学習した時刻の確認。
(3) 教育内容をすべて受講したかの確認のための学習プログラムの「受講開始時点」「受講中にランダムに時刻を設定」「理解度テスト中」の３ポイントの記録。
(4) サーバ内での「誰に」、「いつ」配信したかの記録。

この概念を技術的に実現するシステムの概要構成を図５に示す。このシステムは、会社側で教材コンテンツを作成し、ストリーミング配信により、社員の保有する Web カメラつきパソコンに配信するものである。

まず、配信されている教材コンテンツに、それを学習している社員の顔画像を撮って保

存する。その顔画像は教材のタイムスタンプとともにサーバ側に送信され、証跡として保存するものである。これにより、万一、情報漏えいが発生しても、会社側の責任は軽減され、社員個人の責任に帰することが可能となる。

このシステムの構築するためのフローを図６に示す。この図では、特に社長方針に沿った、人事・教育・情報システム部門の利用企業としての役割と、専門技術集団としての提供者側の役割にわけ、その時系列での業務の流れを整理している。また、パイロット運用に入るまでのプロセスを図示している。“どこに居る誰にいつどれぐらいの容量の教材をどれぐらいの頻度で提供するのか？” が仕様検討のポイントである。このシステム開発においては、ストリーミング配信の技術に適合した、受講生の操作ストレスのない教材配信による受講の実現が技術検討の重点である。

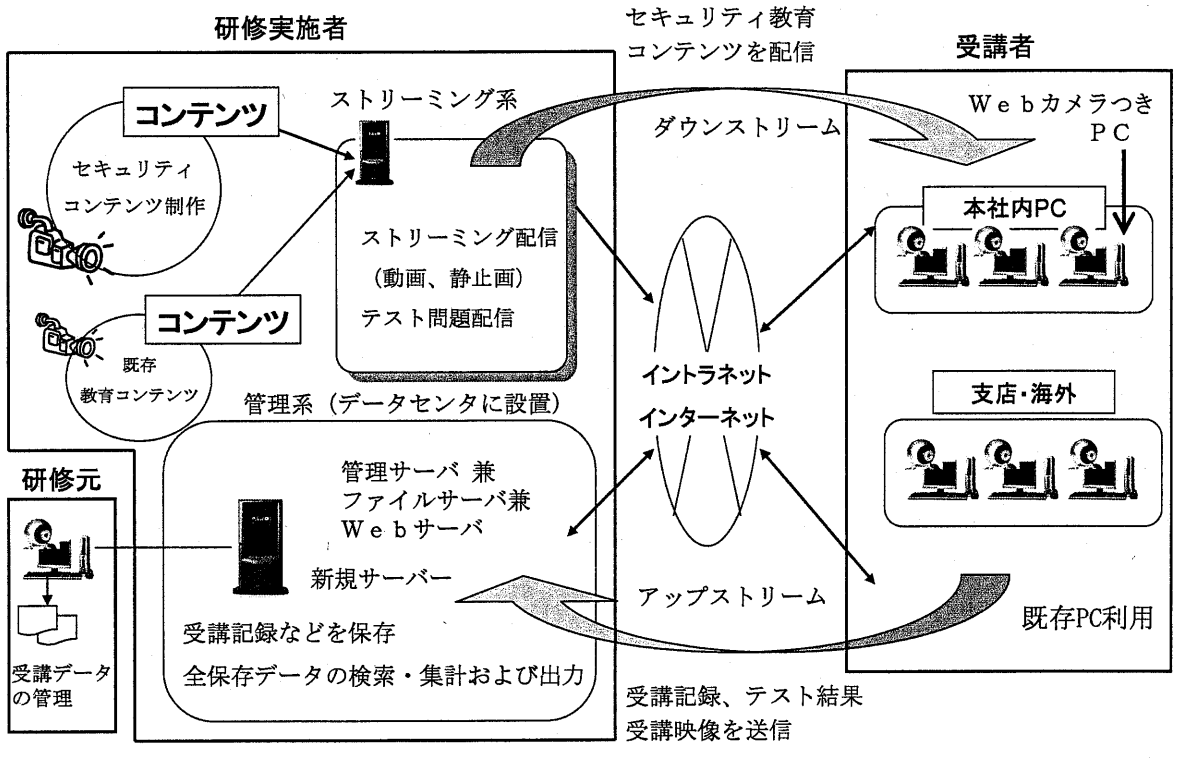


図5 システムの概要

Fig.5 The outline of this system.

特に同時アクセス数とコンテンツ配信サーバの能力、アップロードの情報量、受講側の回線の容量のチェック、オンデマンド方式にするか、一斉同報方式にするかの前提条件が大きな技術的実現検討のポイントとなる。以下に設計検討のポイントを列記する。

(1) ネットワーク回線の種類と帯域（太さ）

(2) 既存ユーザ端末

機種、OS、AP、USB、HDD、メモリーカード等

(3) 既存サーバ機器

機種、OS、ブラウザ、AP、HDD／メモリー容量、周辺機器、同時アクセス数

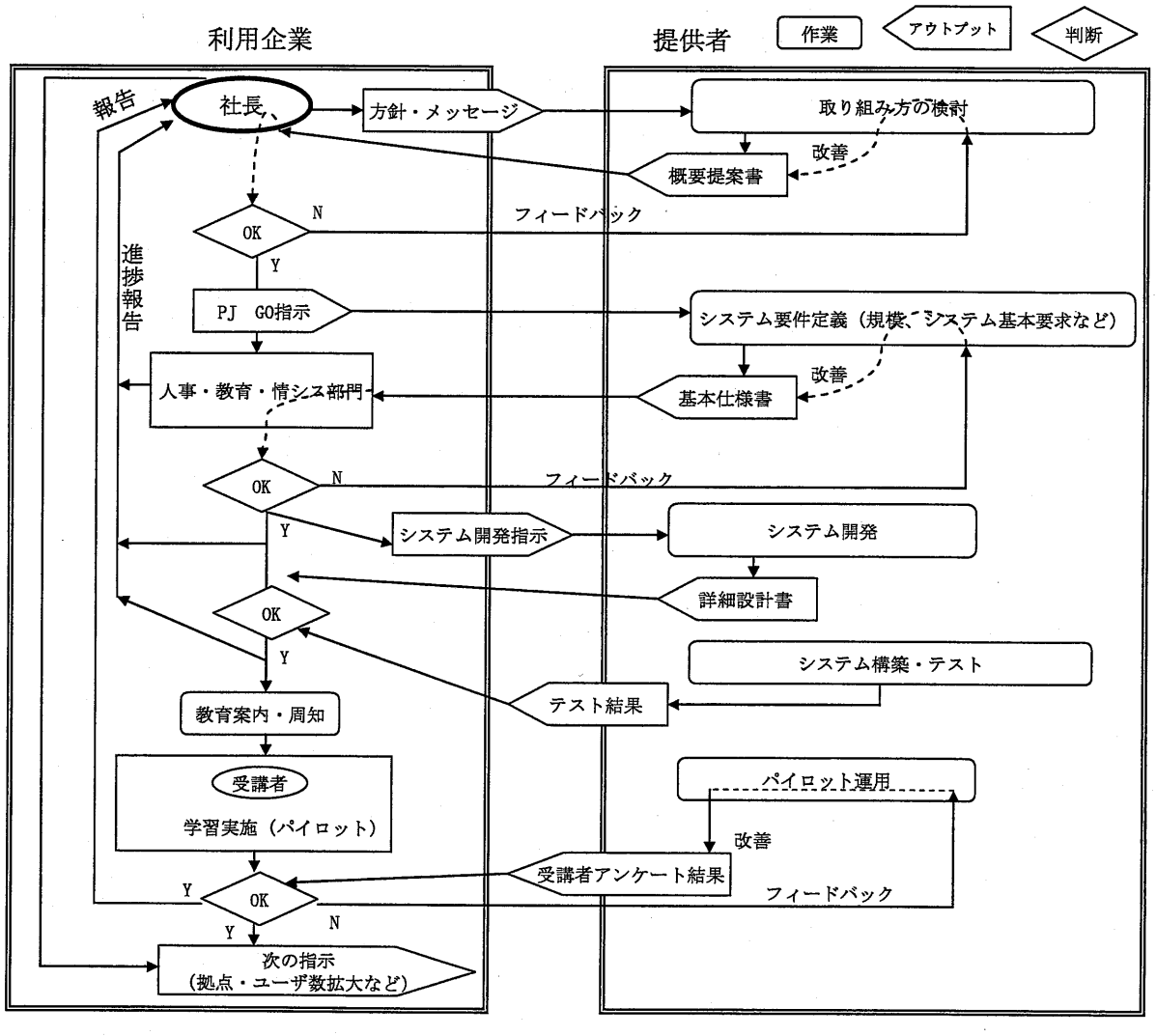


図6 システムの構築フロー

Fig.6 The construction flow chart of this system.

また、以下の方式の要件決定が、システム設計上、重要である。

(1) コンテンツの配信は蓄積型か、リアルタイム型か

(2) 受講者画像のアップロード量　(3) 受講記録の要件　(4) 受講者の認証方式

(5) システムの信頼性レベル（２重化、バックアップなど）
(6) 配信映像の画素数　　(7) ストリームの同時配信数
(8) 受講申請や受講記録のドメイン管理
　　個人別、部門別、役割別、役職別、拠点別、地域別
(9) 将来の拡張性

このシステムを運用するための手順は、実用化において重要な検討要素となる。そのシステム運用のフローを図７に示す。図７のプロセス検討では、専門事業者を提供者とコンテンツ作成者に分けて、その業務分担と情報のやり取りを示している。

ここでは利用企業の意図に沿ったコンテンツ仕様の作成と、その出来型のチェックに重点を置いている。ここで用いられる教材は、セキュリティポリシーに基づいて、図 2 に示すリスク分析を経て、初めてコンセプト形成がなされる。その内容を設計仕様書の形にし、これに基づいて、コンテンツ内容の合意形成がされるように工夫している。

コンテンツがサーバにアップされた後でも、受講生の反応を収集分析することにより、次のコンテンツへ反映するというフィードバックをしている。

この e-ラーニングのシステムは、以下の主要条件のもとで提供されている。

① ユーザ数：3000、　　② 同時接続数：100（ベストエフォート）
③ ストリーミングのエンコード速度：300kbps/stream、蓄積型
④ 符号化：MPEG－４符号化　　⑤ ブラウザ：Window Media Player
⑥ ユーザ認証：ID／パスワード　　⑦ 画素数：240（縦）x 380（横）
⑧ 拠点数：350　　⑨ ID/パスワードによる本人認証

このシステムを実導入した結果、コンテンツ制作料金を除くと、初期費用 200 万円、ランニングコスト 20 万円／月のコストになることが判明した。これを創設費に換算すると、約 4000 円／パソコンになる。これは、社員に対する教育が、第３章以降に示す施設系での対策と比較すると、きわめて安上がりな方法であることを示している。

今後、施設系でのセキュリティ対策が十分ではない企業のリスクヘッジと、経営陣の保身という観点で、このシステムは普及するものと考えられる。

2.5 社員へ心の満足を与えるマネジメント方法

昨今の、年功序列型の企業経営側と社員との関係の変化およびＩＴ技術の発展に伴い、社会的に次のような雇用上の変化があらわれている。

(1) 企業のリストラや労働力の流動化により、企業と社員の関係が変化してきており、終

身雇用が保証されなくなった。

(2) 社会の説明義務を求める意識が大きくなり、役所など権力的な揉み消しが通用しなくなってきた。　→　波風立てずに我慢していればよいとは思わなくなった。

(3) IT 技術の普及により、通信の盗聴や情報漏えいが容易に行えるようになってきている。
→　無条件の忠誠心の期待はできなくなった。

このことから、人間系での情報漏えい対策は社員に対する心の満足を図る経営が行われた上で実施されるべきである。この経営努力はセキュリティ対策として、最も安上がりな方法である。人は「自分のことをよく知ってくれる上司」に対して、その配慮に対するお礼の意味で、よく尽くすものである。この場合、マズローの唱える欲求の階層に分けて考えるとよい。図８に示す段階でそれぞれマネジメント上の工夫・対処することとなる[11]。

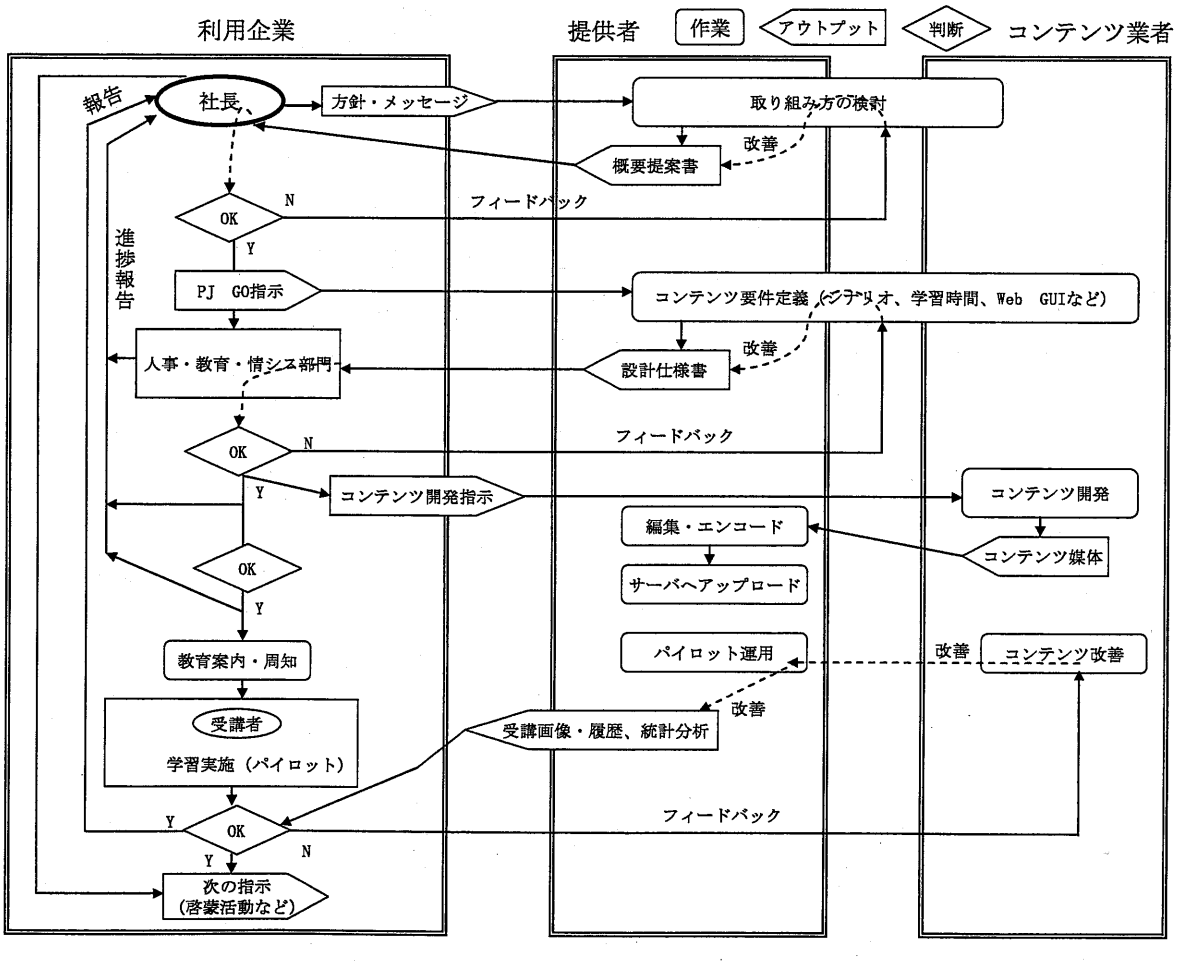


図7　運用のフロー図

Fig.7　The flow chart of operation of this system.

(1) 自分のやりたいことを知ってもらえてやらせてもらえること。（自己実現欲求）
(2) 自分の活動の成果をほめてもらえること。（自尊の欲求）
(3) 仲間として認めてもらえること。（所属の欲求）

この中で、(2)や(3)への取り組みも効果があるが、最も効果的な(1)の“自己実現欲求を満足できる”ように、職場環境を整えると自発的な活気のある職場となる。このためには、自己実現欲求データが大切になる。すなわち、社員に対して“自分はどこから来て、どこに行くのか？”という、自己のたな卸しと将来展望を計画させることである。また、上司は、“仕事としてのニーズ”と、“個人個人の欲求というシーズ”をマッチングさせることが業務となる。仕事に人を割り付けるのではなく、“人の持つ希望などの特性にあわせて仕事を割り付ける”という概念の植え付けも大切なことである。

このようなマネジメント法を実践している企業では“この会社を利用してこんなスキルを持つ人になれる”とする情報を広く世間に発信することができる。これにより、人材の採用においても、優秀な人材をこの会社に集めることが可能となる。

自分のやりたいことが仕事としてできるとなると、そうでない場合と比較して、大幅なパフォーマンス向上が図れる。このような社員の心の満足を与えるマネジメント方法が、もっとも安上がりな社員のロイヤリティ向上方策であると考えられる。

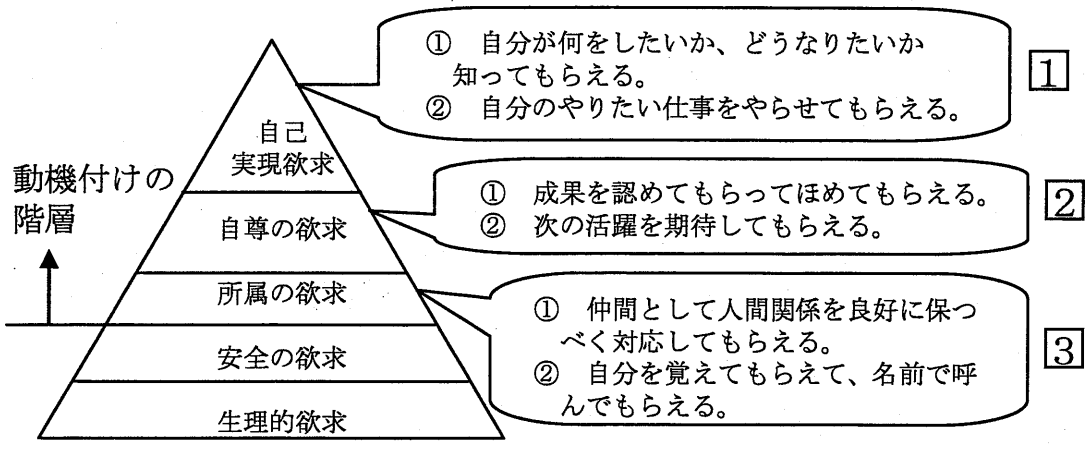


図8 マズローの欲求段階理論の活用法

Fig.8 The use method of desire stages theory by Mazror.

2.6 まとめ

本章では、人間系における情報資産保護方法の考え方を、最近の発生事件への分析および情報文化学的な考察から導き出している。特にアクセス権限ある社員からの情報漏えい

のリスクに着目して、企業の減価評価方法を用いて人間系と施設系での対策の最適解を導き出す方法について述べている。

また、企業のリスクヘッジを安いコストで行う人間系での対策の観点で、証跡保存型 e-ラーニング方式の開発の必要性とその開発内容を紹介している。ここでは、社員教育が経済効果の高いセキュリティ対策であることを示している。

今後は、人間系での対策として最も効果的な、社員への心理的なマネジメント方法について、経営心理学としての人間系での対策にまで高める必要がある。この中では、社員の心の満足を実現することが、人間系でのセキュリティ対策として最も重要な経営課題になりうることを、もっと鮮明にするべく研究することになろう。

[参考文献]

[1] 森　慎一, 塩谷幸治, 新川晃太郎, “情報セキュリティ, ネットワークセキュリティ”, セキュリティポリシーの考え方, pp. 79-80, 株式会社エスシーシー, 東京, 2001.

[2] 上園忠弘, “情報システムのリスク分析”, 情報システムのセキュリティ, 第 3 章, 株式会社トッパン, 東京, 1995.

[3] “それでも止まらない情報漏洩”, 日経コンピュータ, 日経 BP 社, pp. 64-70, Aug. 2005.

[4] 片方善治監修, 情報文化学会編, 情報文化学ハンドブック, 森北出版, 東京, pp. 55-56, 2001.

[5] 崎村夏彦, “個人情報流出事件が急増, 内部反抗防止策が不可欠に”, パッケージソフト＆ソリューション総覧, 日経 BP 社, pp. 24-26, Aug. 2004.

[6] “特集セキュリティ, ネットワーク 100 の新常識”, 日経コンピュータ, 日経 BP 社, 東京, pp. 75, Nov. 2004.

[7] 安田直義, “企業における情報感知のあり方”, コンピュータ＆ネットワーク LAN, 株式会社オーム社, 東京, pp. 25, Dec. 2002.

[8] “社員監視時代が始まる”, 日経コンピュータ, 日経 BP 社, pp. 54-56, Sep. 2004.

[9] 加藤慶信, “顧客情報のネット流出を防げ”, 日経コミュニケーション, 日経 BP 社, 東京, pp. 35-42, Jan. 2005.

[10] 総務省, “情報セキュリティに関する実態調査結果の公表”, pp. 20, Dec. 28th, 2004. http://www.soumu.go.jp/s-news/2004/040705_2.html.

[11] 児玉充晴, “職場でのコミュニケーションのコツ”, 利益を生み出すビジネス手法と事例 108, 日経 BP 企画, 東京, pp. 146-147, May, 2005.

第3章　施設系による情報漏えい対策

3.1 概要

本論文では「既存システムへコスト効果良く情報漏えい対策を行いたい。」とする企業に対してソリューションを提供することを研究目的としている。このためには、施設系でのセキュリティ対策の研究項目を絞り込んで、企業の実態に応じた実システムへの適用性を実証研究することが大切である。

本章では、3.2項で企業ニーズを技術で実現するための方法論を抽象化・一般化して論じている。これに基づいて、3.3項でセキュリティ対策に関する実態調査の結果を分析し、施設系での取り組みのポイントとセキュリティ対策へ投資できる金額の目安を導出している。3.4項および3.5項で現状のセキュリティ対策技術を整理するとともに、本論文で研究対象とする技術要素を絞り込んでいる。さらに、3.6項で情報漏えい対策の高度化の道筋について事例も含めて説明し、今後のセキュリティ対策発展の方向を述べている。

3.2 企業ニーズをシーズに結びつける方法論

一般的に企業のニーズは、図 1 に示すような段階を経て、システムとして実現されることになる。このプロセスにおいては、品質・コスト・納期の3要素に重点をおいて、導入から保守･運用までの全般の検討を行うこととなる。

要素技術をシステムとしてインテグレーションする場合においては、本論文の第4章～第8章でも提起しているような、要素技術の組み合わせ検証や要素技術が有していない機能の開発も行われる場合が多い。ここでは、既存システムが有している機能の調査に基づいて、要素技術の最適な組み合わせを目指すことになる。この検討では、将来の発展過程のロードマップが重要である。本章の3.6項の図14がセキュリティ対策のロードマップの例である。本論文では 3.3 項で、企業の持つコストニーズや機能ニーズを、現状調査の結果に基づいて論じている。また、要素技術を図 10 に示すように分類整理し、図 11 に示すニーズに沿って、そのシステムへの適用方法を体系立てて検討している。

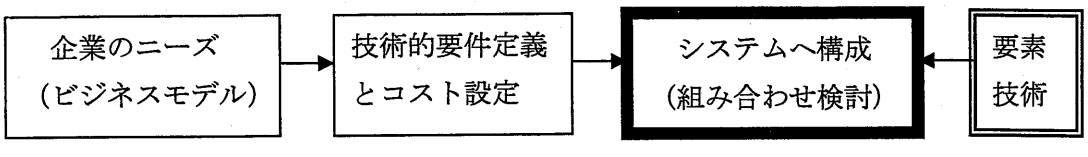


図 1　ニーズ実現のプロセス

Fig.1　The process to achieve the needs.

図１に示す、「技術的要件定義」から「システムへ構成」への検討内容を、第４章で示す「ＵＳＢキー」をもとに例示すると次のようになる。

（技術的要件定義）
(1)　とりあえずの対策なのでコストはＰＣ１台当たり１万円以下であること。（コスト）
(2)　このコストで実現できる記憶認証以外の認証手段であること。（品質）
(3)　他社での採用実績があって、保守・運用も含め安定して使えること。（品質・納期）
(4)　セキュリティ対策の範囲を可能な限り大きくカバーしていること。（品質）

（システムへの構成：要素技術の組み合わせ検討）
(1)　コスト要件を満たす“所持認証”を適用しＩＣカードより安いＵＳＢキーを採用する。
(2)　ＰＣのＯＳとアプリの間に介在させるミドルウェアと、安価なＵＳＢキーの連携で、最大限のセキュリティ機能を実現してコスト効果を高める。
(3)　ＵＳＢキーの利用においてセキュリティを向上させるための運用上の工夫を行う。

図１における「企業のニーズ」を分解すると、一般的に図２のような構造となる。この図の中で、セキュリティ対策における「(4)対策費への値ごろ感」については、トラブル発生確率と企業価値減価との関連で決まる場合が多い。また、図３に示す実地検証でコスト効果が証明され、“○ヶ月で元が取れる”というような結果に基づいて値ごろ感が醸成されることもある。特に、図２の「(2)業績向上、コスト削減施策」の実施においては、実地検証は必要なプロセスになる場合が多い。さらに、「(5)他社での実施状況」は自社での実施に向けての大きな判断材料となる。

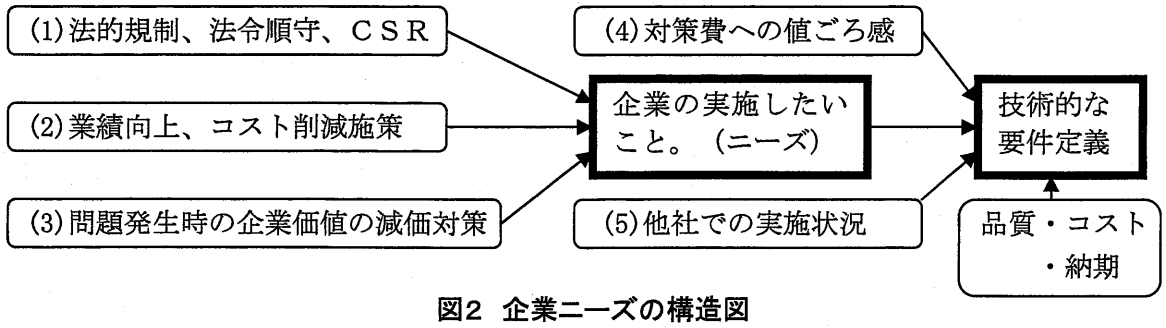


図2　企業ニーズの構造図

Fig.2　The structural chart of corporate needs.

企業ニーズは業種業態によっても異なり、また、社会変化や他社の動向によってきわめて流動的である。この企業ニーズを的確に捉えるためには、ニーズを有する企業と、シーズを有するシステムベンダが一緒になって、コンセプト作りから始めることが有効である。ニーズや実現方法が明らかな場合は問題ないが、これが漠然としている場合が多い。この

ことからニーズへの想定に基づき、所要システムを仮定して「何ができるか?」をまず設定することから始めることになる。これをベースに、ブレインストーミングによるアイデア出しを行い、ＰＤＣＡサイクルを回してゆくことになる。この検証のためには、検証試験モデルの設定と実地検証が重要な役目を果たすことになる。図３にその構造を示す。

たとえば外食チェーンの場合、実験店が設定され、導入容易性、導入効果、コストの回収効果、店員の行動や思考に与える影響、店員への教育方法、システム運用方法、保守方法などが検討されることになる。一方ベンダにおいては、更なる研究開発テーマを明確化でき、仮定ではない要件がはっきりした、お客つきのコスト効果の高い開発が可能となる。

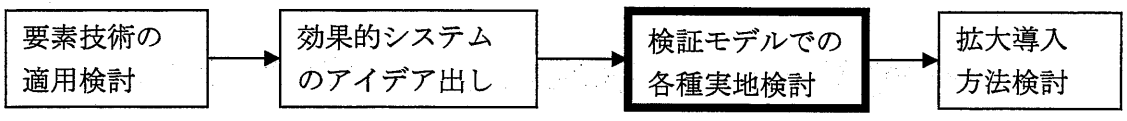


図3　検証モデルでの実地検証のプロセス

Fig.3　The process of on-the-spot inspection in verification models.

3.3 情報セキュリティ調査にもとづく現状分析

3.3.1 調査対象

総務省が実施した実態調査の対象企業は上場企業 438 社であり、規模分布は図４のとおりである[1]。調査期間は平成 16 年 2 月 22 日～3 月 15 日である。社員数から判断して中堅企業を中心に従業員数 1000 人未満の一般企業も含まれていて、本論文の対象とする企業規模も含まれていることがわかる。

3.3.2　セキュリティポリシー関する分析

セキュリティポリシーについて、図５に示すように、策定のための知識 ・ノウハウがないと訴えるところがその理由のトップで約半数を占めている（①）。また、社員の認識不足（②）や予算の問題でできない（③）とする企業も約１／３にのぼる。さらに、図６に示すように、セキュリティポリシーが機能していない理由として、セキュリティポリシーを実現する手段がなく、実現性に欠けるためとしている（④）。

このことから、“知識・ノウハウもお金もなく、セキュリティポリシーをどのようにして実現してするのか？”がわからない、とする一般企業が多く存在することがわかる。

“少ない予算という条件において、たくさんあるセキュリティ技術から何を選択して、既存の業務システムが持つセキュリティ機能を活用しつつ、どのように情報資産保護を進めるのか？”の道筋作りは、研究テーマとして大変社会的意義のあることである。

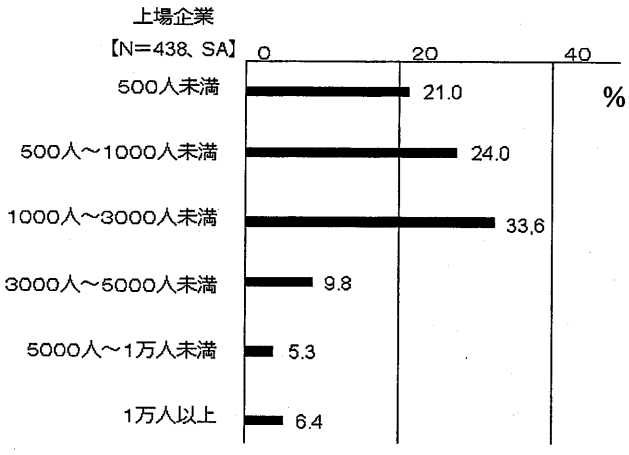


図 4 調査対象企業の規模分布

Fig.4 The scale distribution of investigated object enterprises.

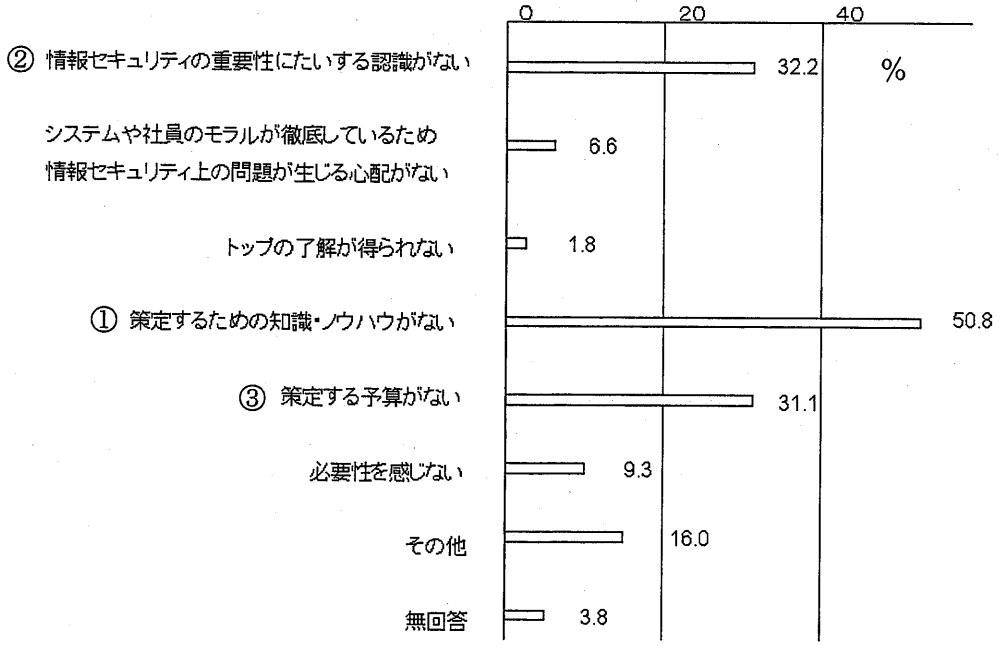


図5 セキュリティポリシーを策定していない理由

Fig.5 The reasons why security policy is not settled on.

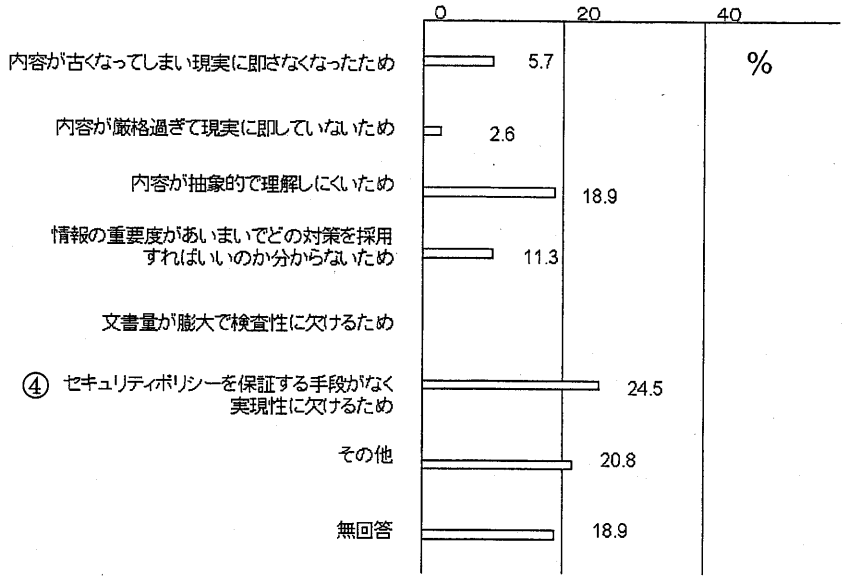


図6 セキュリティポリシーが機能していない理由

Fig.6 The reasons why security policy doesn't function.

3.3.3 セキュリティ対策への投資額分析

図7に示すセキュリティ対策に投資できる金額と図8に示すパソコン（PC）の台数分布から加重平均をすると、おおむね2.1万円／PC程度の支出となる。図7、図8の分布がある程度分散していることを考慮すると、PC1台当たり1～3万円程度が支出の値ごろ感と考えられ、本論文のセキュリティ対策の費用の範囲としている。

この分析結果から、本論文では「コストパフォーマンスよく、既存システムへの情報漏えい対策を行いたい。」とする企業に対してソリューションを提供することを主眼とする。具体的には、これに適合するようにセキュリティ対策の研究項目を絞り込んで、セキュリティ技術の適用性を研究することになる。

3.4 既存のセキュリティ技術の整理と研究の方向性

施設系におけるセキュリティ機能においては、認証とアクセスコントロールを中心として様々な管理機能が必要となる。情報漏えい対策に必要な情報管理の典型的な基本構造の例を図9、図10に示す。サーバ内では、“何を守る必要があるのか”という観点から、情報源となるファイルの分類整理を行うとともに、ファイル毎の登録･廃棄権、改変権、印刷権、閲覧権などの属性付与ルールを設定する必要がある。特に、重要な情報資産保護については、端末での個人認証、クローズドネットワーク、サーバでのユーザ認証を中心に様々な管理機能の適用を行う必要がある。

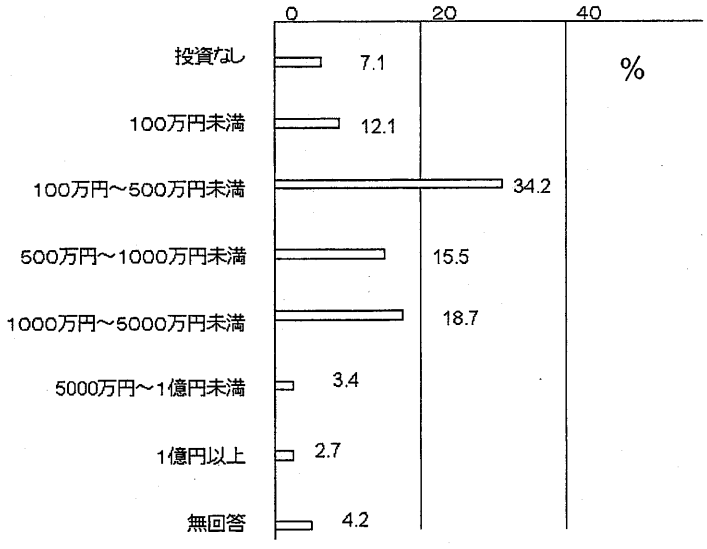


図7 情報セキュリティ対策関連の投資額

Fig.7 Amount of investment related to information security measures.

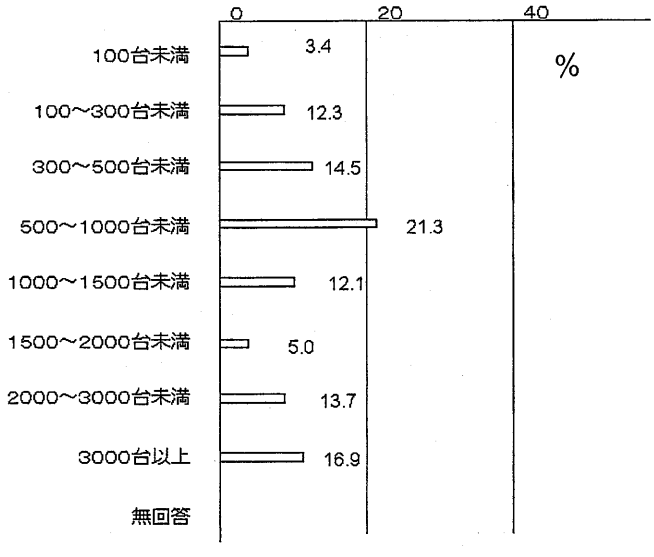


図8 クライアントパソコンの所有台数

Fig.8 The number of ownership of client personal computers.

これら情報漏えい対策に必要な機能の内容は、ネットワーク側とサーバ・コンテンツ側に分けて、表 1 のように整理できる[2][3]（注）。この中で、ネットワーク側の(1)～(6)の機能について、内部情報漏えいという観点よりは外部からのアタック対策が重要という事情もあり、実現している企業が多い。一方、サーバ・コンテンツ側の(7)～(9)の機能について

表 1 情報漏えい対策に関する主なセキュリティ機能

Table 1 The main functions about the measure against information leak.

	項目	内容
ネットワーク側	(1) アクセス制御	レイヤ2/3/4の情報に基づくネットワーク機器のアクセス制御
	(2) 暗号化	IPの通信をセキュアに行うためでIPsecやSSLが代表的
	(3) ネットワークにログオン時のユーザ認証	RADIUSサーバでのネットワークログオン時の認証やLANにおけるEAP認証が代表例
	(4) LANのメンバーシップのための認証	LANスイッチのポートベースでのハードウェア情報に基づくユーザー認証が代表的
	(5) DHCPサーバにおけるユーザ認証	IPアドレスの配信時でのユーザー認証
	(6) ファイアウォールにおけるユーザ認証	ファイアウォールを通過するパケットに対する認証
サーバ・コンテンツ側	(7) アクセスに対する認証	ID/パスワード認証が一般的だが、バイオ認証の必要性が増大
	(8) アクセスログの蓄積	イベントログ、SYSLOG、アカウンティングログを管理・保存
	(9) 認可における制御	参照、更新、削除、登録などの権限をユーザの資格に応じて付与
	(10) アクセスデータの蓄積	メールや外部送信データそのものを蓄積

実現していない企業が多く、多発する事件の直接的原因となっている。なお、“(10)アクセスデータの蓄積”による対策については、高価な専用システムを必要とすることから、特殊事情のある会社での実施にとどまっている。

(注) 表1の技術内容は第3章から第8章で論じる技術的なベースになることから、本論文の最後に“(別紙) 本論文で述べる技術の説明”として詳細に説明している。

以上の観点から、本研究では表 1 の(7)～(9)クライアントとサーバ間のアクセス系に重点を置いて、企業のセキュリティ対策の発展形態に合わせて、情報漏えい対策のあり方について研究している[4]。

本論文ではセキュリティ対策の発展形態として、①所持によるセキュリティ対策、から②生体認証によるセキュリティ対策、へ、さらには、③情報そのものをPCにダウンロードさせないセキュリティ対策、から、④グローバル情報システムにおけるセキュリティ対策への展開に着目して、第4章から第7章で記述している。

3.5 セキュリティ技術の全体と研究対象要素技術の選定・絞込み

情報漏えいを発生させないための、施設系のシステムが持つべき“セキュリティ対策の構造”を図９に示す。企業内の業務システムの中核に認証機能を配置し、情報源とアクセス者との間に介在させ、情報源自体を保護する構造である。この中ではセキュリティポリシーが同じでないと情報流通においては機能しないという特徴がある。また、端末およびユーザ認証に基づきファイルの操作権限が与えられることになる。ここでは、この構造をアクセス者、ネットワーク、情報源に区分して、情報源の重要度に応じて整理している点が特徴である。

セキュリティ対策の基本は、情報資産保護の観点から守るべき情報資産を定義し、その資産にアクセスできる者を特定することにある。その資産に対するアクセス者の権限の規定も必要となる。たとえば、その情報資産の閲覧権、更新権、廃棄権、印刷権などの設定のことである。

このような認証においては、さまざまなアクセスルートごとに設定することができる。基本的には、端末での認証、ネットワーク認証、サーバ認証、ファイルやＷｅｂコンテンツアクセス認証などがある。（別紙：2 技術説明）

本論文では、この中でコストが安く簡単に実現できる“端末”と“サーバ”での認証に重点をおいて研究を進めている。

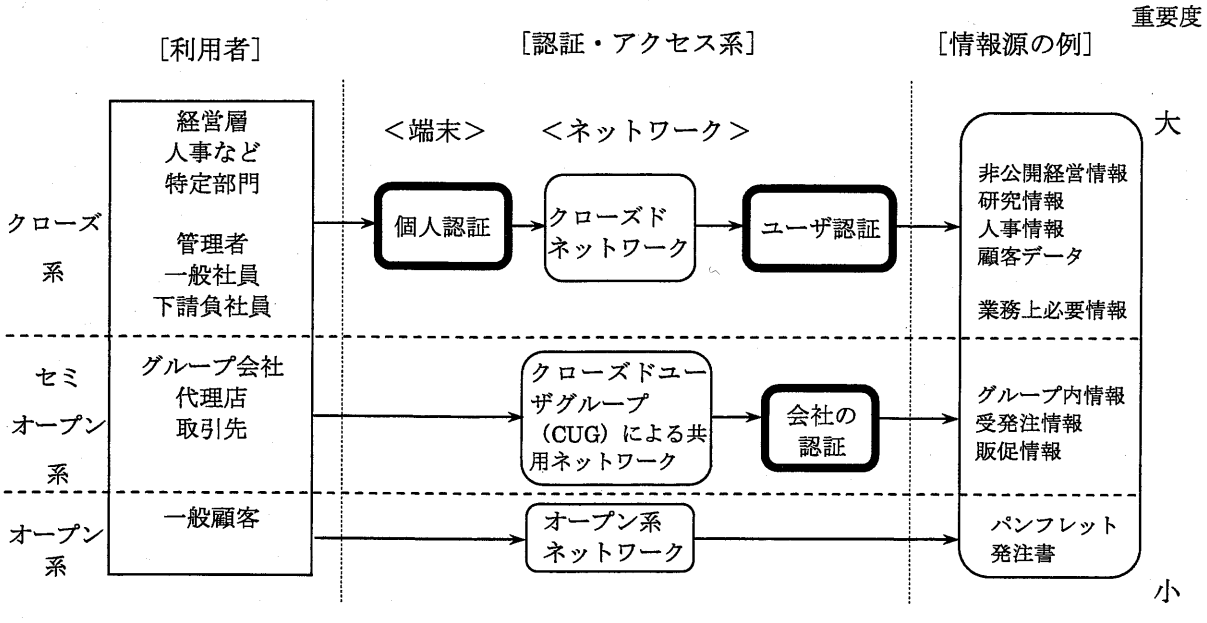


図9 情報管理の典型的な基本構造の例

Fig.9 The sample of the typical basic structure of information management.

企業における情報漏えい対策に必要となる施設系の対策技術要素を、クライアント、回線、ネットワーク、認証、社内ネットワーク、サーバ、文書管理の各技術要素に分けて分類を実施した。その結果を図 10 にまとめて示す。この図に示す太字の下線部分が本論文での研究対象技術である。

初めてセキュリティ対策を行う企業においては、これらの技術要素のうち、どれから導入したらよいのか迷うところが多い。このことから、当面の初歩的な取り組みを以下の３つの要素に分類して対象となる技術を定義した。その内容を図 11 に示す。

(1) セキュリティ教育　　(2) 内部情報漏えい対策　　(3) 外部からのアタック

特に中小企業で情報漏えい対策の遅れている場合での、限られた予算の中で取り組むための要件と当面の対処策として必要となる技術要素を示している。図 11 の太枠の部分が本論文が対象としている要素である。

上記の検討を深堀りするために、セキュリティ強度とコストの関係をマッピングしている。その結果を図 12 に示す。この図では、今回の研究対象とした要素技術を太い○印で示している。また、第８章で示す今後の発展形態を□で示している。この中では、コストが安く、比較的既存技術にオーバーレイしやすい技術要素をピックアップしている。第４章から第７章で取り上げる技術要素が、３万円以下／パソコンというコストパフォーマンスのよい領域に含まれていることがわかる。また、番外ではあるが、第２章に示すコスト効果の高い教育ツールであるｅラーニングについても、この表に含めてマッピングしている。

今回取り組む研究の範囲の考え方を図 13 に示す。図 12 の関係をシンプル化してコンセプトとして研究の意義を示している。1.4 項に示すように軍事機密といった、コスト対効果ではない厳密さを求める領域の研究は、論文になりやすく学会でのテーマとなりやすい。しかし 一般企業でのセキュリティ対策を求めるニーズには合致しないケースが多い。

今後は、従来の研究の範囲を超えて、より要素技術を実用化してゆく研究が必要である。身の丈にあったコスト対効果を追求する一般企業においては、費用対効果の良いセキュリティ要素技術を用いた情報資産保護対策を求めている。ここが本論文の研究テーマとなる。

3.6 セキュリティ対策の高度化の道筋

情報漏えい対策を行う上での、対策システムの導入には高度化のための順序がある。一般企業における高度化のためのステップは、図 14 に示す道筋が一般的である[5]。

ステップ１：社外からの企業内システムへのアタックに対して、ファイアウォールによる防御を行う。

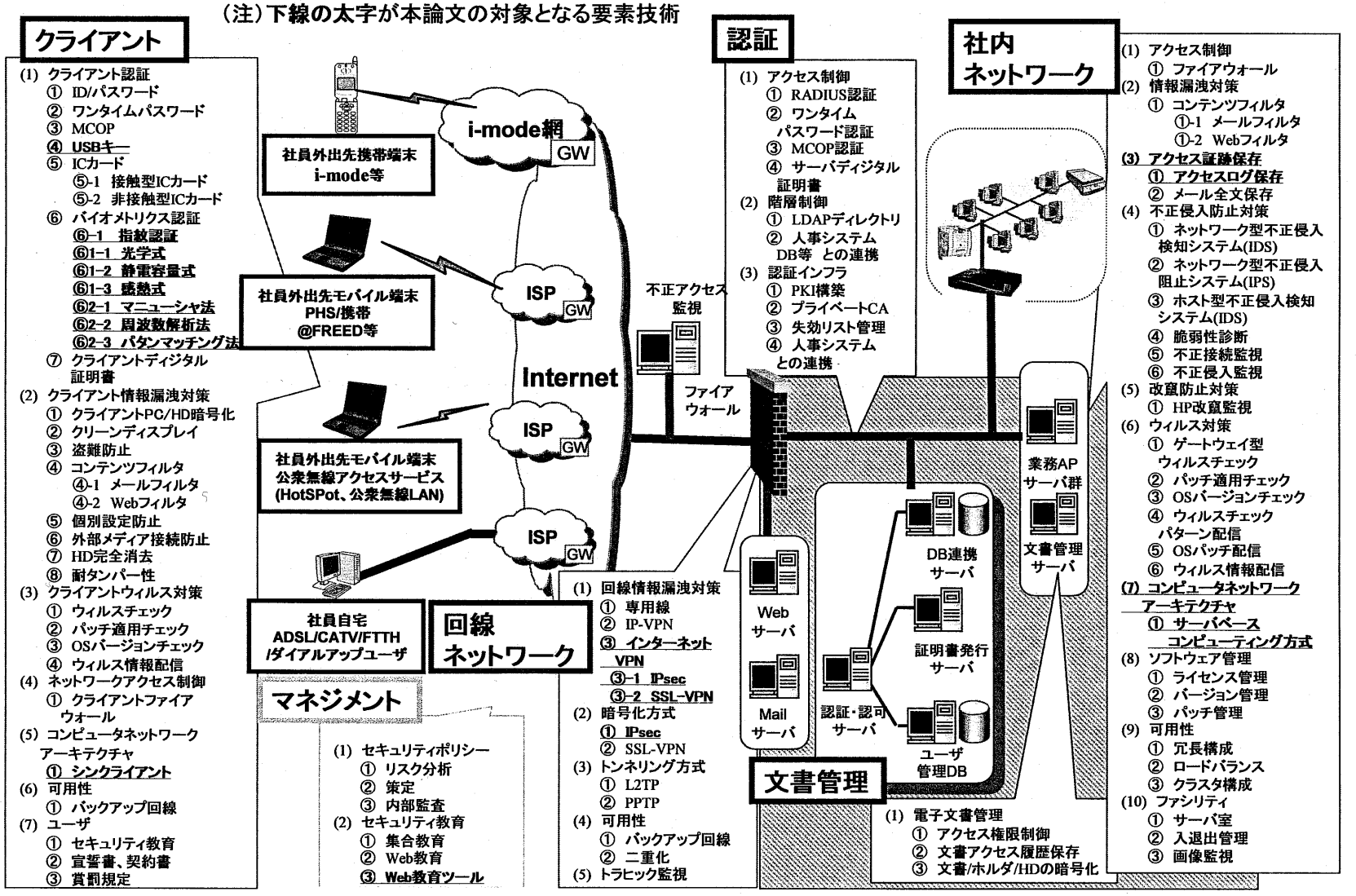


図 10 セキュリティ対策のための技術要素の分類

Fig.10 The classification of technological elements for security countermeasures.

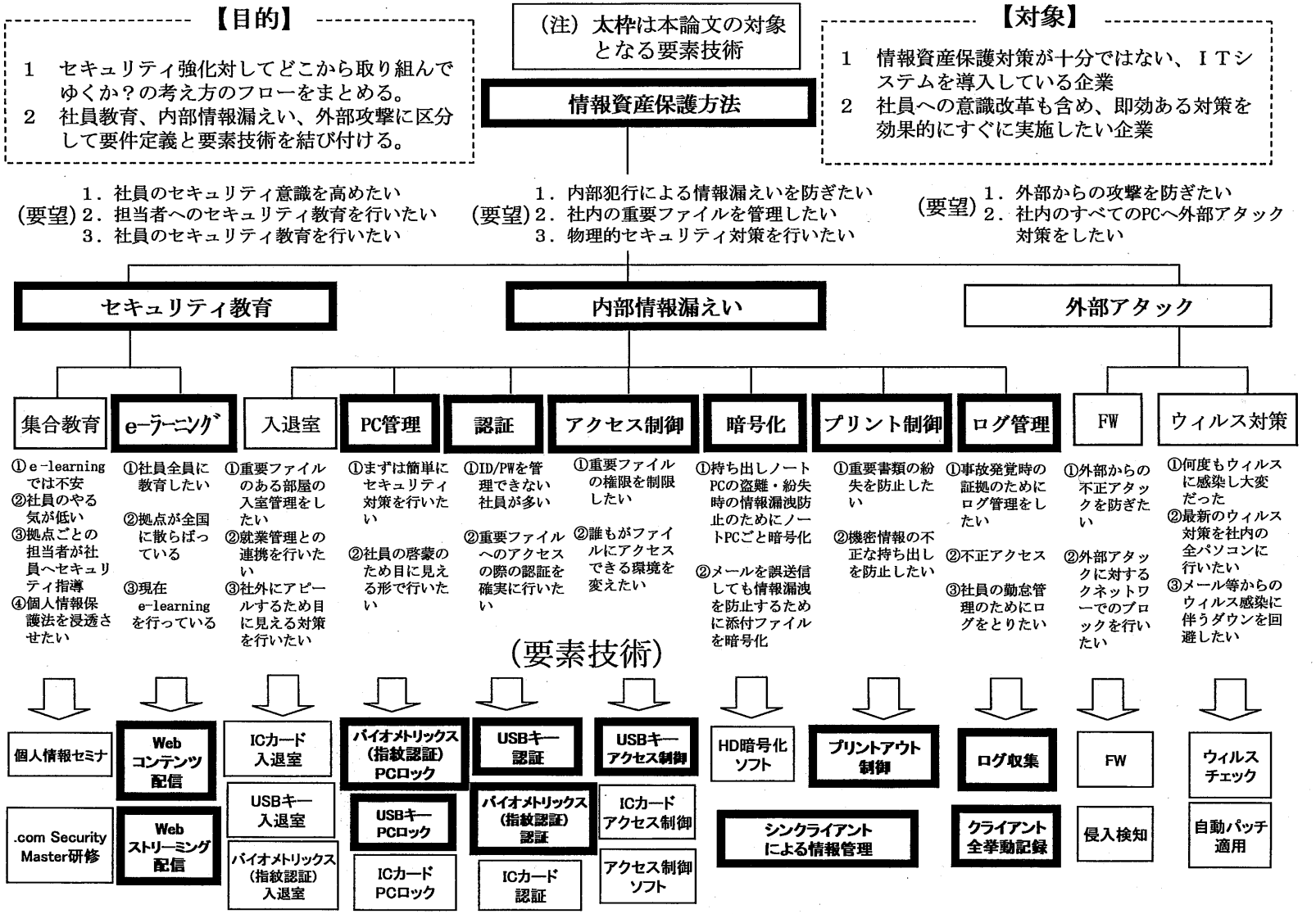


図 11　情報資産保護対策検討の道筋

Fig.11　The route of rudimentary examinations of security countermeasures.

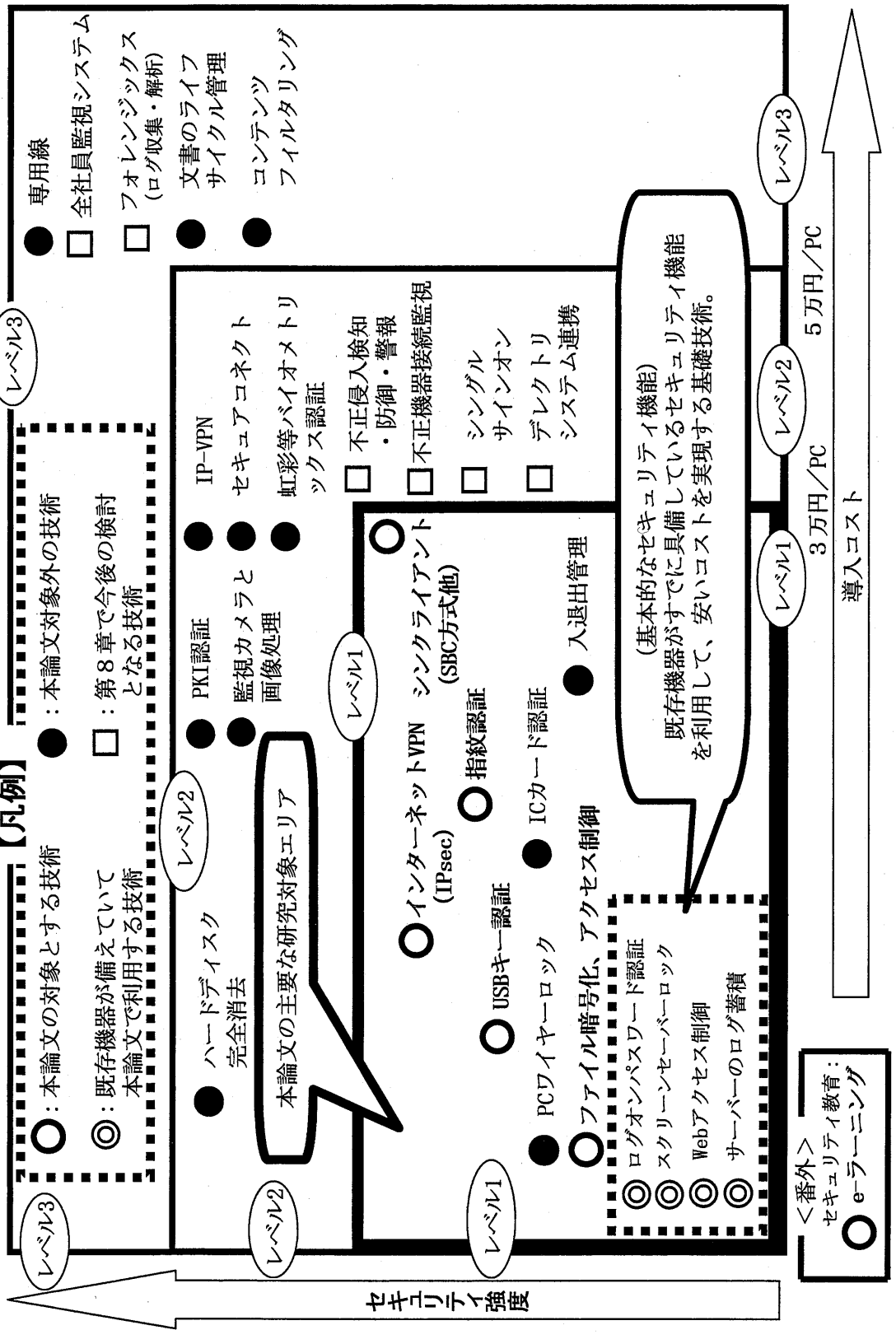


図 12　各技術要素のセキュリティ強度とコストの関係

Fig.12　The relation between security strength and cost of technological each elements.

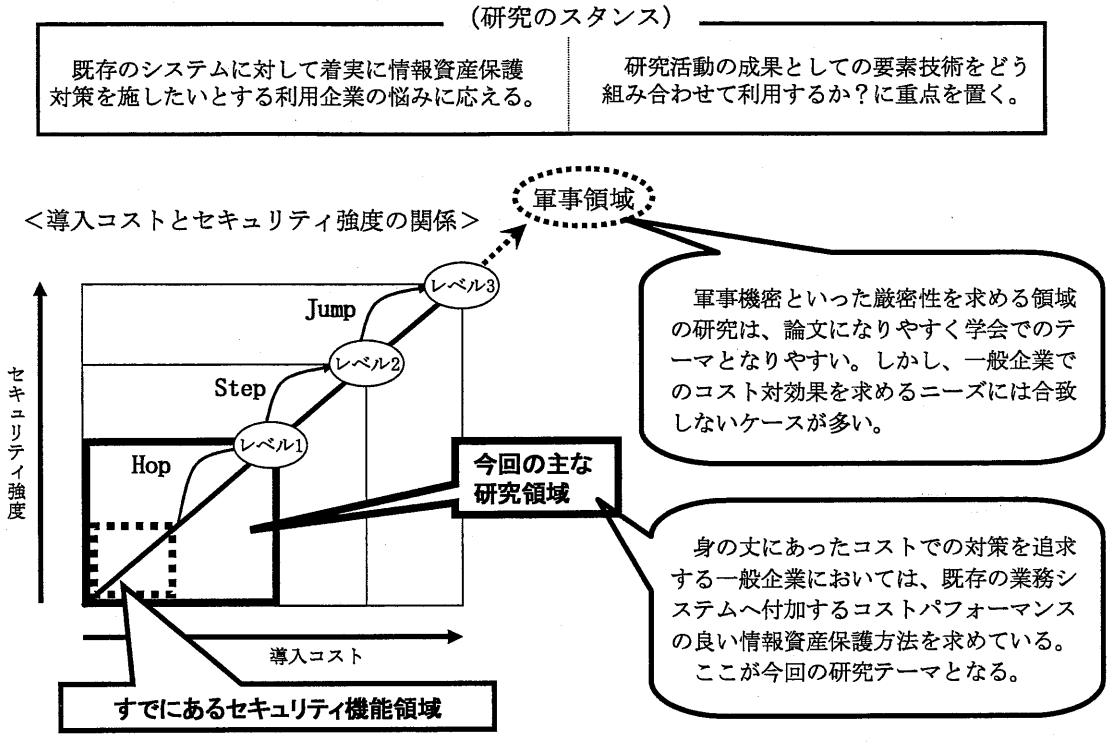


図 13 導入コストとセキュリティ強度から見た今回の研究範囲

Fig.13 The range of research analyzed from introduction cost and security strength.

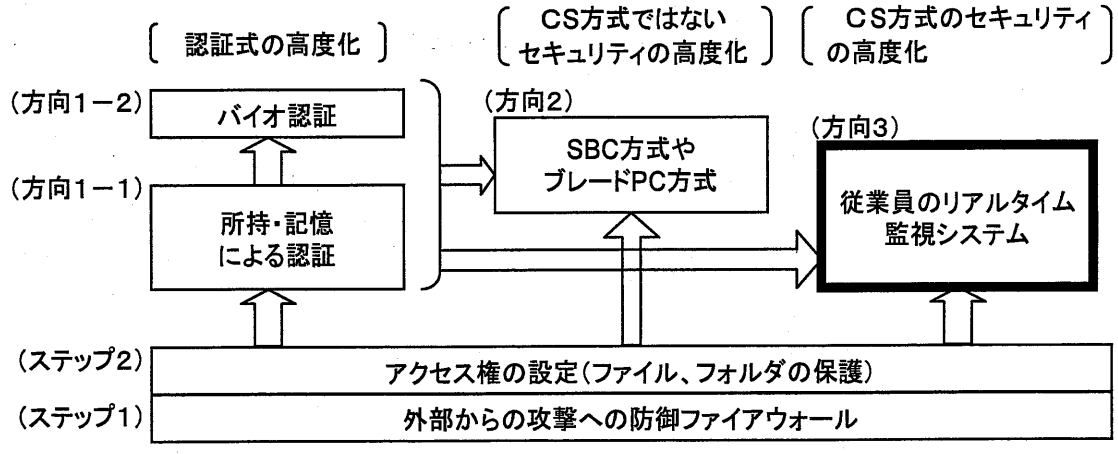


図 14 情報漏えい対策の高度化の方向

Fig.14 The direction of upgrade of information leakage measures.

ステップ２：社内の重要情報の特定とアクセス権を設定する。

方向 1-1：ＩＤ／パスワードの記憶による本人認証を高度化して、所持（ＩＣカード、ＵＳＢキー（別紙：用語説明(4)））と必要に応じてPINコードを設定する。

方向 1-2：本人認証をバイオ認証とする。

方向２：ＣＳ方式（別紙：用語説明(3)）を用いず、ＳＢＣ方式（別紙：用語説明(1)）を採用して、クライアント側からの情報漏えいを防止する。

方向３：ＣＳ方式をそのまま採用し、利用者に対するリアルタイム監視システムを導入して情報漏えい対策とする。

本論文では、ステップ２を主体として、方向 1-1、方向 1-2 および方向２の発展系を研究対象とした[8]-[10]。 なお、方向３については、第８章で述べる発展形に含めて記述している。セキュリティ対策取り組みの基礎となる、ステップ２の具体的な進め方の例を表２に示す。実際に情報漏えい事件をおこした企業が、当局の指導のもとに実施した対策と、その発展形をまとめて示している。事件を契機として表２の“② 開拓時代”と“③ 発展期”の対策が必要となった。これにより、既存システムのセキュリティ機能高度化のために、第５章に示す指紋認証システムへの導入検討を実施することとした。

表2 セキュリティ対策のステップアッププランの実際

Table 2 An actual conditions of a step-up plan of security countermeasures.

	① 無法時代	② 開拓時代	③ 発展期	④ 充実期
問題	サーバ上のファイルはフリーパスでアクセス可能なものが多い。	ＩＤ／パスワードだけでは、アクセスしたのが本人だと立証不可能	誰がいつファイルにアクセスしたか不明	ＨＤＤやＭＯなどにダウンロードし、外部に持ち出せる。
対策	ファイルアクセスに制限を設ける。	指紋認証システムを導入する。	ログを残すソフトをサーバ／端末に導入	特にアライアンスへはＳＢＣ方式を導入
具体的活動	各ユーザフォルダ毎に必要なアクセス権を調査し、段階的に付与する。 半年毎に一斉チェックを行う。	各担当の端末に指紋認証システムを開発して実装する。 導入による運用性を検証する。	ログを残すソフトの比較を実施、別環境で検証を実施してから導入を判断する。	ＳＢＣ方式を導入することで生じるメリット／デメリットを分析し、導入の判断を行う。
効果	アクセスできる範囲を限定。重要情報へのアクセス拒否など、情報の重要度に合わせた管理が行える。	アカウントにハッキングして、重要な情報にアクセスを行うのを阻止。本人がアクセスしたという証拠にもなる。	誰がファイルにアクセスしたかを把握する。不正なアプリケーションソフトの導入も検知できる。	ファイルが端末に保存できないので、ファイルの持出不可となり、高速アクセスも期待できる。

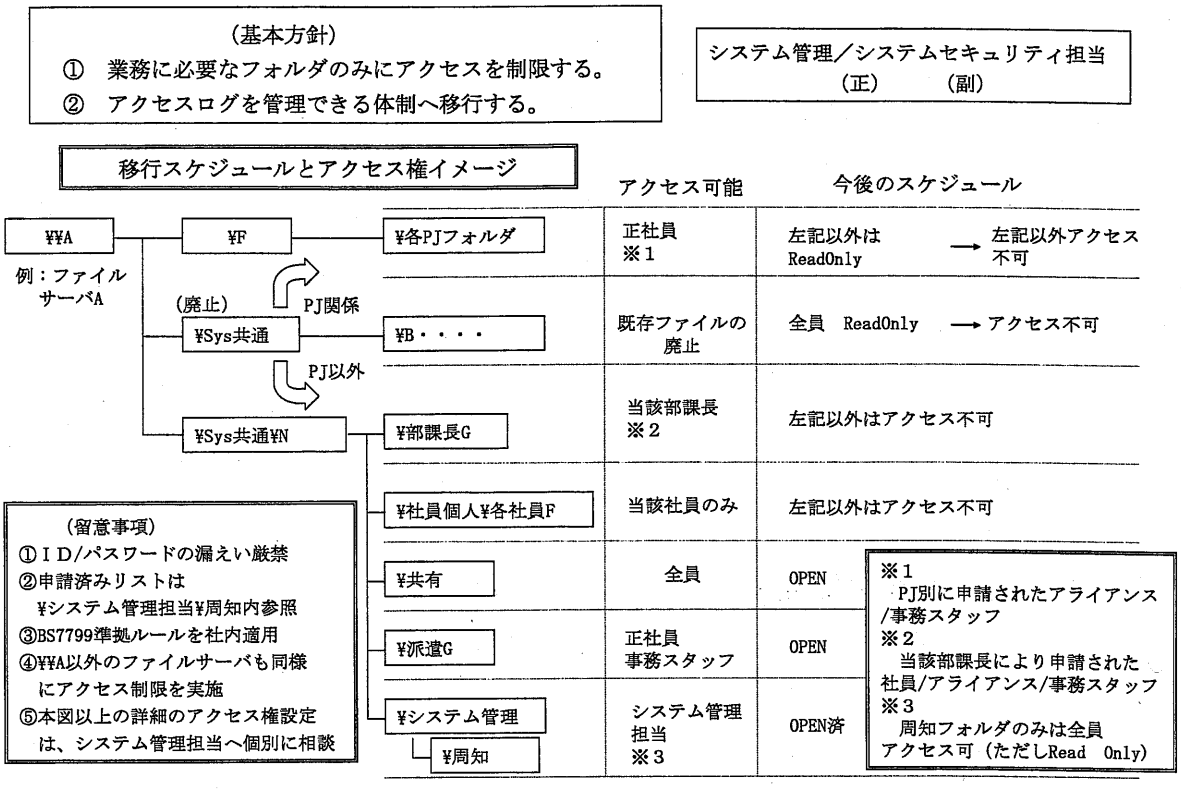


図 15 ファイル管理方法の実際の例

Fig.15 An actual example of the method of file management.

表２の“① 無法時代”に対する、ファイル管理の具体的な方法を図 15 に示す。このモデルの職場には部課長、正社員、アライアンス社員、派遣社員の４種類の権限の違うメンバが混在していたことから、権限に応じたファイル分けを検討した事例である。

なお、表２の“④ 充実期”に必要となるＳＢＣ方式の導入について、本論文では第６章と第７章でその検討内容を示している。

3.7 まとめ

本章では国が実施した情報セキュリティ調査にもとづいて、一般企業が「たくさんあるセキュリティ技術から、何を選択して、少ない予算の中から、既存のセキュリティ機能を活用しつつ、どのようにセキュリティ対策を進めるのか？」の道筋作りが研究テーマとして重要であることを示した。安価で導入容易な端末認証に注目して、コストパフォーマンスのよいセキュリティ技術を抽出して、バイオメトリックス認証（別紙：用語説明(6)）やＳＢＣ方式（別紙：用語説明(1)）の利用に向けた発展の方向を示した。

今後の技術の発展にあわせて、手のひらの静脈パターンによる個人認証のようなバイオメトリックス認証（別紙：用語説明(6)）やブレードPC（別紙：用語説明(8)）のような各種のシンクライアント方式（別紙：用語説明(7)）の適用研究も今後の課題となる。

本章にある、セキュリティの要素技術を網羅した分類整理方法と、発展のステップの考え方が、セキュリティ対策に迷っている企業の一助になれば幸いである。

[参考文献]

[1] 総務省，“情報セキュリティに関する実態調査結果の公表”，pp. 44-45, pp. 60-61, Dec. 28th, 2004. http://www.soumu.go.jp/s-news/2004/040705_2.html.

[2] 岡村康一郎，“インフラから見た情報漏洩・隠蔽防止のテクノロジー”，コンピュータ&ネットワークLAN, 2002年12月号, pp. 26-30, Dec. 2002.

[3] 相原弘明，“アプリケーションから見た内部情報漏洩防止のためのテクノロジー”，コンピュータ&ネットワークLAN，2002年12月号, pp. 31-35, Dec. 2002.

[4] 藤田康幸，“不正アクセス禁止法について”，情報セキュリティ，bit 別冊，共立出版，東京，pp. 312-321, 2000.

[5] “社員監視時代が始まる”，日経コンピュータ，日経BP社, pp. 54-56, Sep. 2004.

[6] McNurlin, Barbara and Ralph H. Sprague Jr., 1989.
Information Systems Management In Practice, Second Edition, Englewood Cliffs, New Jersey: Prentice Hall, pp. 353-370, 1989.

[7] Don McIntosh, Rich Born, “Server-based Computing: Back to the Future Solves Enterprise Desktop Problems”, ICMIT 2000, pp. 732-737, 2000.

[8] Andrej Volchkov, “Server-based Computing Opportunities”, IT Pro Mar./Apr. 2000.

第4章　情報漏えい対策システムへのUSBキーの適用

4.1 概要

最近、企業内部からの顧客情報をはじめとする機密情報の漏えいは、ブランドイメージの低下や信用失墜のみならず経営の根幹にかかわる重大な問題になりつつある。この中で、多くの一般企業のように、セキュリティ対策への大きな投資が困難なところでは「安価でかつ最大限の対策が簡単にできること」というニーズが強い。このことから、本論文では、1万円以下／パソコンを目標コストとしている。また、パソコンおよびサーバがすでに備えているセキュリティ機能を活用した、安価なＵＳＢキー（別紙：用語説明(4)）を用いた情報漏えい対策システムを工夫している。さらに、実際の企業に導入して得られたコスト効果および導入・運用上の工夫も実施している。

本章では、4.2項で企業のＩＴ化の現状をふまえて必要となるセキュリティ対策項目を整理している。4.3項でこの項目を満足するためのＵＳＢキーを用いた各種機能の実現方法について記述する。4.4項で本システムの導入・運用上の工夫やその効果について説明する。

4.2 セキュリティ対策要件の整理

4.2.1 認証ツールとしてのUSBキーの選定理由

セキュリティ対策においては、本人認証が重要であり、その方法として「知識」、「所持」、「バイオメトリックス」（別紙：用語説明(6)）の３つによるものが代表的である[1]、現状の企業の情報システムの多くは「知識」によるＩＤ／パスワード認証を基本とする形態で構築されている。しかし、「知識」だけでは十分なセキュリティ対策となっていないのが現状である。

一方、「バイオメトリックス」においては、コスト高や本人拒否への対応および社員の抵抗感などの問題があり[2]、厳密な本人認証までを求めない中小企業での普及にまで至っていない。

「所持」による本人認証の場合、主としてＩＣカードやＵＳＢキーが用いられる。ＩＣカードにおいては社員証などとの併用で適用されるケースもあるが、リーダライタのようなデバイスが必要で高コストである。また、中小企業ではＩＣカードによる社員証があまり普及していないことから、今回、検討対象外としている。

このことから「所持」による本人認証を、ＵＳＢキーを用いて検討することとする。な

お、ＵＳＢキーには、「知識」による PIN コード入力（別紙：用語説明(5)）と「所持」の２段階認証する機能を持たせることは可能である。しかし、本論文では、パスワード管理稼働の低減を目的としたことから、「所持」のみで検討している。

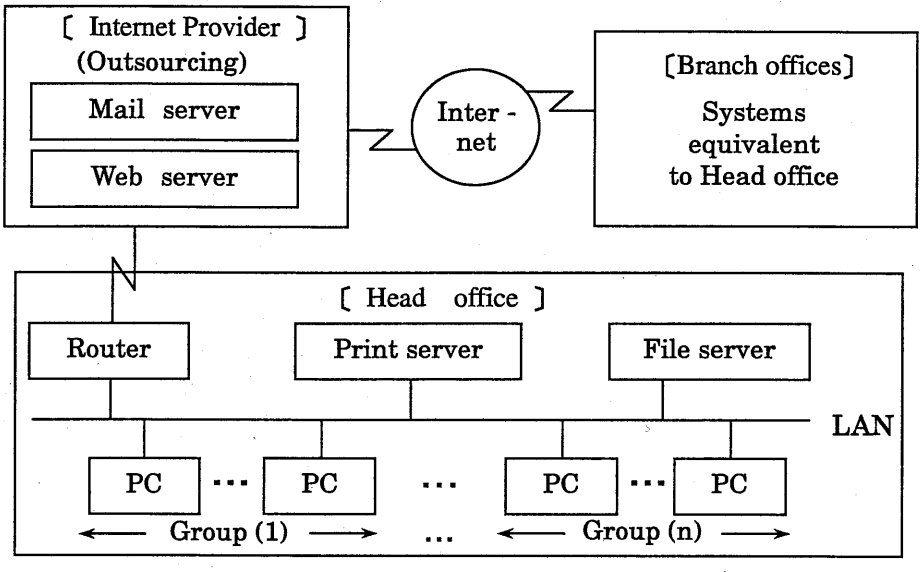


図1 検討対象とした情報システムの構成モデル

Fig.1 The functional model of information systems in this study.

4.2.2 適用対象および必要となる検討項目

一般企業においては、セキュリティポリシーが明文化されているところはまだ少なく[3]、実際のセキュリティ対策として、社長やシステム管理者の個々の判断に頼るケースが多い。

本論文では、セキュリティポリシーにおける、「アクセス制御」と「運用管理」の部分の一部を、本章で提言するシステムで実現して、セキュリティポリシー遵守におけるシステム管理者や利用者の負担軽減を図ることを目的としている。

また、一般企業のセキュリティに対する投資力が 100 万円～500 万円／年程度であることを勘案して[4]、パソコン（PC）１台あたり１万円以下の投資で最大限の対策が実現できることを検討の主眼としている。

本章で検討するＵＳＢキーは、耐タンパ性を強化しているとともに、市販部品を組み合わせて、低コストで各種セキュリティ機能を工夫している点が特徴である。なお、本章の 4.3 項で述べるセキュリティ機能の実現方法については、最近、各種市販され始めたＵＳＢキーの提供事業者などから公表されているものは見あたらない[5]-[7]。

今回、検討対象とした企業層の従業員規模は 30 名～300 名程度であり、年間の売り上げ高は数億円から数十億円である。これは、この企業層が情報システム担当者の設置される

規模でありながら、セキュリティへの意識が比較的遅れているからである[8]。今回対象とした一般企業における典型的な情報システムの機能モデルを図 1 に示す。インターネットプロバイダのサーバをアウトソーシングで利用して、電子メールとＷｅｂを中心とする業務システムを構築している。本支店において、ＬＡＮに接続されたPCからＬＡＮ上のサーバおよびインターネット経由で接続されるプロバイダのサーバを利用する形態を想定している。この形態を利用している導入対象企業８社のシステム管理者からのヒアリングにより抽出した、内部情報漏えいへの不安の順位とＵＳＢキーを用いて実現できるセキュリティ対策の項目を表 1 に示す。また、実現すべき項目として、ＵＳＢキーそのものの低コスト化や耐タンパ性向上、安全なＵＳＢキーの生成・配布・キー情報の保管方法等があげられ、さらにスムーズな導入・運用方法の実現も重要な項目となる。

表1 不安の順位とUSBキーによる対策内容

Table 1 The uneasiness ranking and measures by an USB key.

	Uneasiness ranking which administrators have.	Measure functions by USB key	Item number
1	Injustice in the time of logon	Automatic logon by attestation of an USB key	4.3.4.1
2	Peeping by others when leaving a seat	(1)Automatic logoff by USB key detach (2) Lock by a screen saver	4.3.4.2
3	Injustice access to important information	(1) Automatic encryption of files (2) Secret memory of file password in an USB key	4.3.4.3 ～4.3.4.5
4	Injustice download from web pages	Web access and its process control by password in an USB key	4.3.4.6
5	Injustice acquisition of printed matters	Print control by password in an USB key	4.3.4.7

4.3 検討項目に対する実現方法の検討

4.3.1 USBキー本体に対する検討

ＵＳＢキーは図２に示すように、ＵＳＢインタフェース内蔵のワンチップマイクロプロセッサ、不揮発性メモリ（8KB)、大容量キャパシタによる電流平滑化回路で構成されている。すべての処理ソフトはファームウェアとして不揮発性メモリ内に格納し、安価なワンチップマイクロプロセッサで処理が行えるよう構成している。サイズは 34mm×16mm×8mm（除コネクタ部）と、親指サイズの小型化を実現している。

一般のＵＳＢキーは ABS 樹脂製のシェル内にプリント基板を配置する形態が多い[12], [6]。この形態では、シェルをこわされるとプリント基板が取り出し可能であり、プ

リント基板における信号の解析が安易となる。

これに対し本ＵＳＢキーでは、この基板自体をEVA樹脂を主体とするプラスチックを用いて多層一体成型をしている。内部のプリント基盤を敢えて薄く脆弱にするにより、取り出そうとするとこわれる可能性を高くし、耐タンパ性を高めている。

また、ＵＳＢインタフェースにおいては通信内容を解析されないように、通信コマンド単位に、時刻をキーとするワンタイムパスワードでのミクロな制御を行う暗号方式を適用している。ＵＳＢキー内の情報処理方法が、処理プロセスの電流値変化で推定されることも考えられる。このため、本ＵＳＢキー内の電流平滑化回路を用いて、消費電流解析の面からの耐タンパ性の向上を図っている。

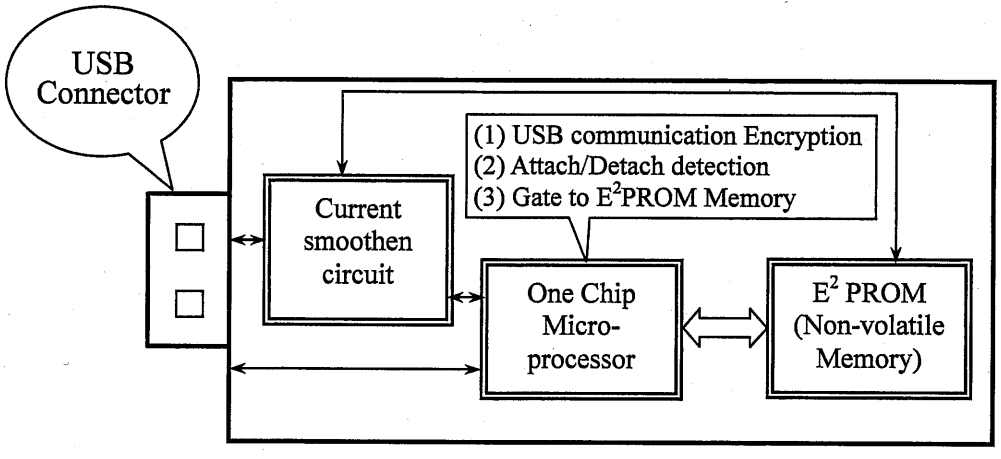


図2　USBキー内の構成

Fig.2　The Composition in an USB key.

4.3.2 ミドルウェアの構成と関連する機能

ＵＳＢキーに格納された情報と処理ソフトは、PCにインストールされるミドルウェアとの連携により機能する。このミドルウェアはＵＳＢキーを用いる本システム導入時にPCにインストールされる。ミドルウェアは利用するアプリケーションとPCのOSの間の処理に割りこんで、暗号化／復号化を主とするセキュリティ機能を実現するための処理を行う。

このミドルウェアとＵＳＢキーが果たす機能概要を図３に示す。また、ミドルウェアとの関連で処理される各種のセキュリティ機能要素とその関連を図４に示す。これらを利用したセキュリティ機能の実現方法を、以下の4.3.3項、4.3.4項に示す。

なお、図３～図８の図中に示すＡ～Ｖの各要素について、以下の文章では(A)～(V)の記号を用いて処理方法を説明する。

4.3.3 鍵情報の生成、保管と機能設定方法

ＵＳＢキーに関するキー情報の生成とその保管方法を図５で①～④の順に示す。キー生

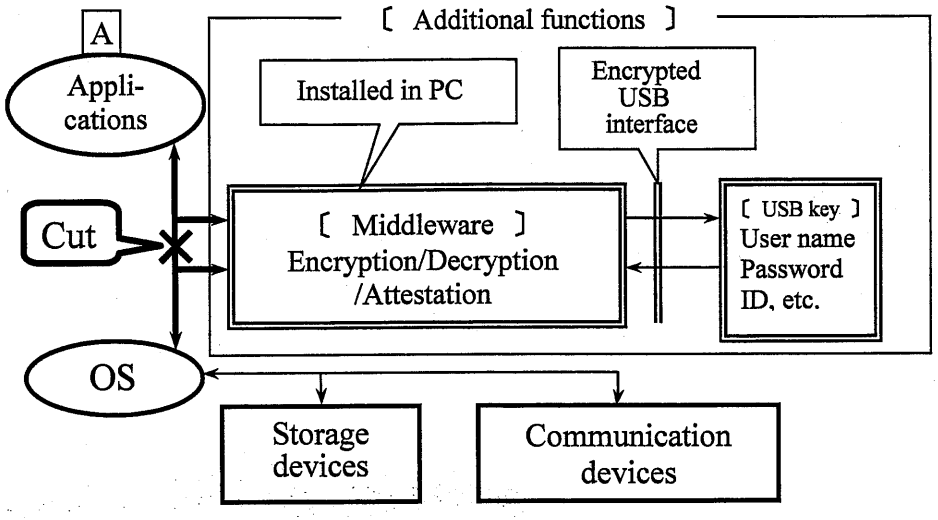


図3　パソコンに付加されるミドルウェアとUSBキーの機能概要

Fig.3　The additional functions of Middleware and USB key to PC.

成用ソフトにより、キーの基本情報（ユーザ名、ID、パスワード）(G)から公開鍵、秘密鍵、ハッシュ値が作成される（①）。ハッシュ値を用いるのは、ＵＳＢキーの正当性をチェックするためであり、ユーザ名、ID、パスワードから 20byte の情報として生成される。この時生成された公開鍵はファイルサーバにユーザ名とともに保管され、アクセス管理に利用される（②）。

公開鍵、ハッシュ値はキー生成ソフトにより独自暗号方式で暗号化され、ユーザ名、IDとともにＵＳＢキー内のメモリエリア(U)に保管され、秘密鍵も同じく暗号化されてＵＳＢキー内の(S)に保管される（③）。

この情報はバックアップとして PC 内に保管することが危険なため、フロッピーディスク等の外部記録媒体にとって保管することとしている（④）。このバックアップファイルはＵＳＢキー紛失時等で再作成が必要となった場合に利用される。

なお、キーの基本情報となるパスワードについては自動生成することも可能である。この処理においてはカオス擬似真性乱数を用いることにより、パスワードのくり回し発生を極小にしている。

4.3.4 各種セキュリティ機能の実現方法

4.3.4.1 自動ログオン・ログオフ機能

ＵＳＢキーが PC に接続されている状態で OS を起動をすると、ミドルウェア(K)はログオン画面(D)を表示するとともに、ＵＳＢキー内(U)に記録されたハッシュ値を読み出す。ま

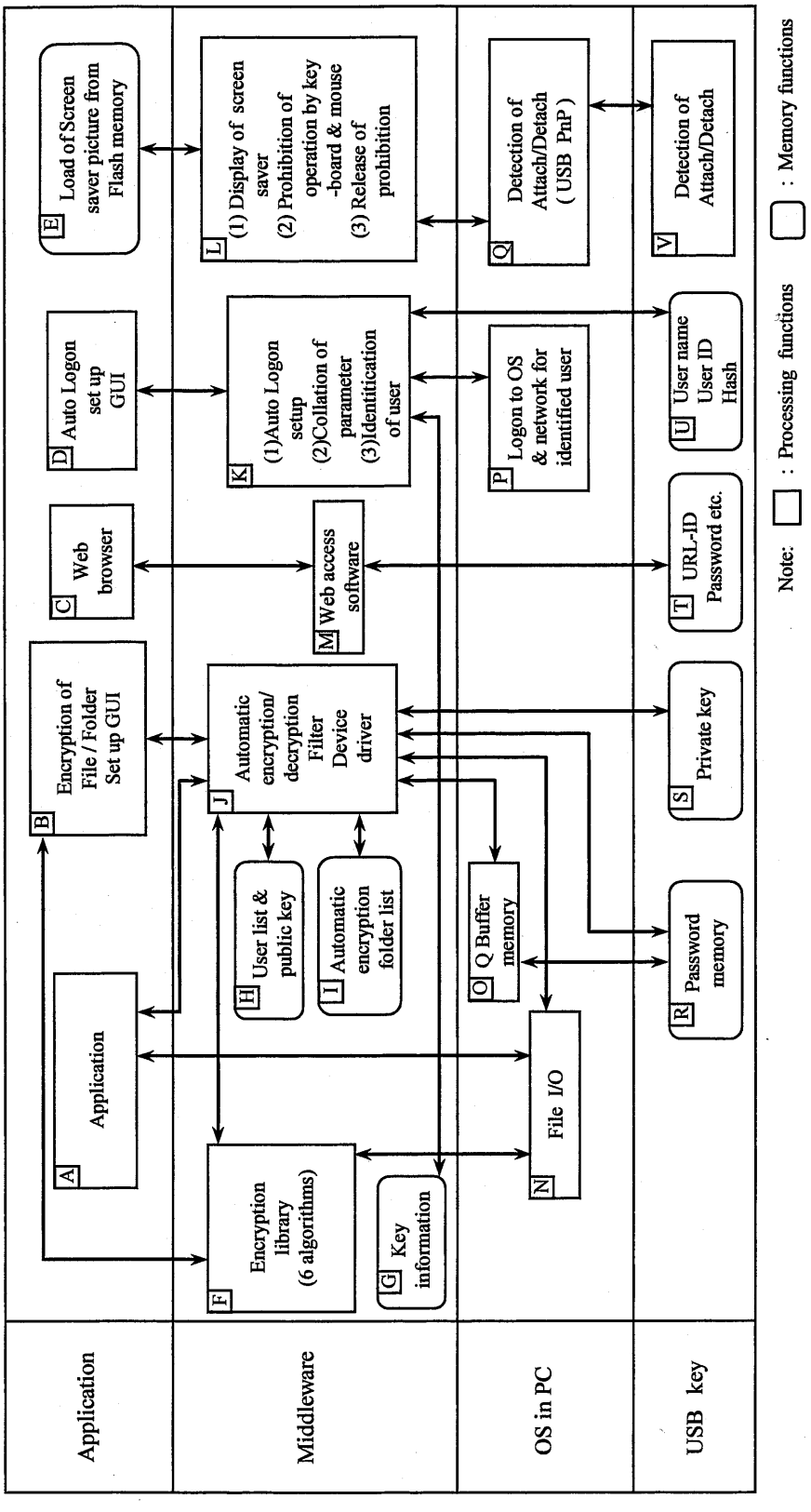


図4 ミドルウェアとUSBキーに関する各種機能と処理

Fig.4 The various functions and process relations relevant to Middleware and an USB key.

た、(K)はキー情報(G)に暗号化して持っているユーザ名、ID、パスワードからハッシュ値を計算する。この計算結果が、ＵＳＢキー内(U)に記録されたハッシュ値と合致していれば、OS のログオン機能(P)を呼び出し、ログオンする。

自動ログオフが設定されている状態でＵＳＢキーが抜かれた場合、ミドルウェア(L)は、PC の OS が持つＵＳＢインタフェースのプラグアンドプレイ(PnP)機能であるＵＳＢキー内の(V)とＵＳＢデバイスドライバ(Q)の連携によりＵＳＢキーが無いことを検知し、OS からログオフする。

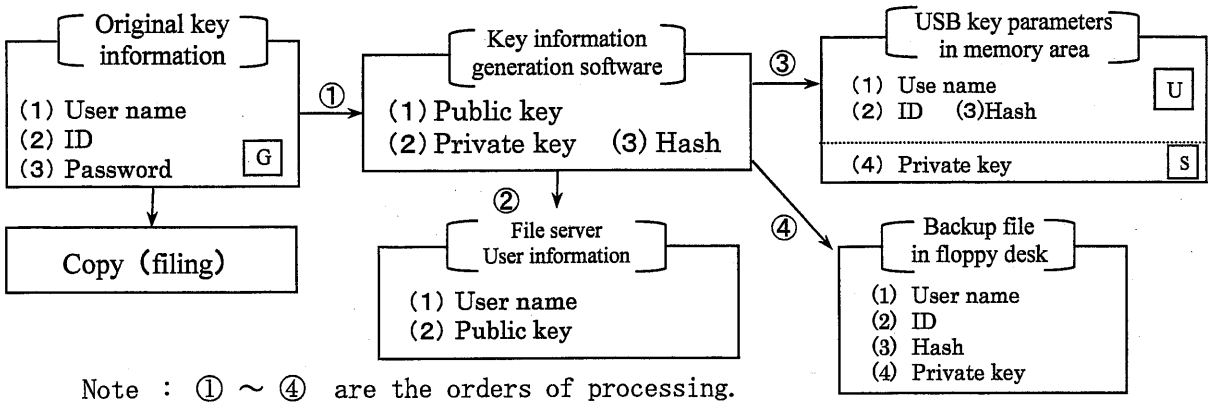


図5 キー情報生成と保管方法

Fig.5 The generation and filing methods of key information.

4.3.4.2 スクリーンセーバーロック機能

自動ログオフが設定されていない状態で、利用者がＵＳＢキーを PC から抜くと、ＵＳＢキー内の(V)が切り離されたことを、ＵＳＢデバイスドライバ(Q)が PnP 機能により検知する。この情報をミドルウェア(L)が受けとって、スクリーンセーバー画面(E)を表示するとともに、キーボード、マウスの操作を無効とする。

ＵＳＢキーを PC へ挿入すると、それを(V)と(Q)の連携で検知し(L)において逆の処理を行い、もとの画面を表示して PC の操作を有効とする。

4.3.4.3 パスワードメモリ機能

この機能の処理プロセスを図６の①～⑤に示す。利用者のパスワードメモリ機能の呼び出し操作により(①)、ミドルウェア(J)はＵＳＢキー内のパスワードメモリ(R)に複数蓄積されている ID／パスワードをパスワード名とともに読み出し(②)、一覧表として PC へ表示する。利用者はこの表から必要な ID／パスワードを選択する。この時(J)は OS の Q バッファ(O)において、選択された ID／パスワードを一時格納する(③)。

次に、ID／パスワードを要求しているアプリケーション(A)上でペーストコマンド入力を実行する(④)。これにより、(O)→(J)→(N)→(A)のルートで ID／パスワードが自動入力され

る(⑤)。ペーストコマンド入力操作を利用者に要求するのは、自動での誤入力を防止するために利用者による確認を行う必要があるからである。

4.3.4.4 手動暗号化機能

本システムでは、暗号ライブラリ(F)で６種類の共通鍵暗号アルゴリズムを選択できるようにしている。これは、暗号強度と処理速度の兼ね合いを利用者が選択できるようにするためである。利用者は、暗号化が必要なファイルを指定して、そのファイルをミドルウェア(J)であらかじめ設定した共通鍵暗号アルゴリズムにより暗号化する。暗号化したファイルは電子メールに添付したり、ＵＳＢメモリなどのリムーバブルディスクに格納したりして相手先に送られる。

図７は利用者がＡ氏向けの平文ファイルを暗号化して送り、Ａ氏が復号するプロセスであり、図中①～⑧の順を用いて以下に処理方法を示す。

利用者により、暗号化指定された平文ファイル(①)は、カオス擬似真性乱数により自動生成したワンタイムパスワードを共通鍵として用いて、設定されている共通鍵アルゴリズムにもとづき(J)において暗号化される(②)。

次にインポートされているユーザ一覧表(H)が(J)→(B)のルートで PC に表示され、利用者がアクセス権限のあるユーザ名または階層的ユーザグループを指定する．図７の例ではユーザとしてＡ氏を指定している。

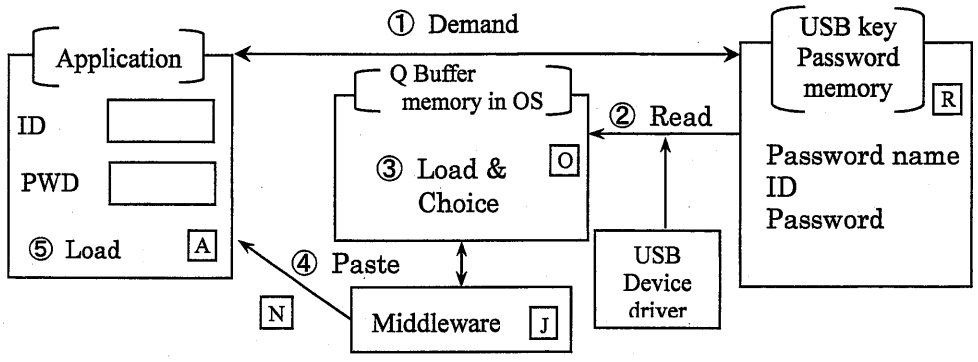
ミドルウェア(J)はその権限あるユーザの公開鍵をファイルサーバから呼び出して、前述のワンタイムパスワードを暗号化し(③)、ユーザ名（平文）とともにタグとして一体化して、暗号化された本文ファイルに添付する(④)。この時、アクセス権のある者の人数分のタグを付けて暗号化ファイルとすることが可能である。

復号には、上記の逆の処理を行う。受信者のミドルウェア(J)は自分向けの平文のユーザ名のタグが受信ファイルに添付されているかどうかをチェックする。これが存在する場合は、自分のＵＳＢキー内の(S)から秘密鍵を取り出して(⑤)、ワンタイムパスワードを復号する(⑥)。このワンタイムパスワードでファイル本体を復号して(⑦)、自分向けの平文ファイルを得る(⑧)。上記処理方法により、自分向けのタグが無い場合や、ＵＳＢキーが接続されていない場合は復号することは不可能である。

4.3.4.5 自動暗号化機能

これは、ユーザに暗号を意識させず、暗号化／復号化を実現する機能である．予め自動暗号化対象フォルダをフォルダリスト(I) で指定しておき、その指定されたフォルダ内のファイルは全て前項の方法で暗号化しておく。

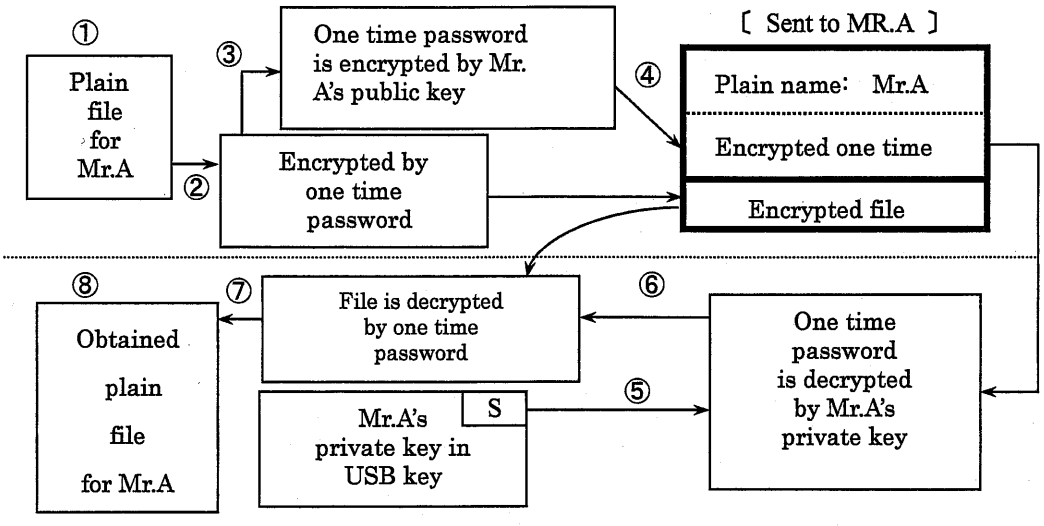
ファイルは、ファイル I/O (N)→ミドルウェア(J)→アプリケーション(A)のルートで処理



Note : ① ～ ⑤ are the orders of processing.

図6 パスワード呼び出しとロードの処理プロセス

Fig.6 The processing method of password calling and loading.



Note : ①～⑧ are the orders of processing.

図7 A氏向けのファイルの暗号化と復号化の方法

Fig.7 The encryption and decryption method of the file for Mr.A.

されて、利用者には通常の見え方であるようにし、利用者はアプリケーションやファイルのフォーマットによらず、今までどおりの操作法で読み書きできるようにする。この場合、ファイルのアイコンに暗号化されていることを示すマークを付加することも可能である。

ミドルウェア(J)はアプリケーション(A)がファイルの入出力を(N)で行うときに、(A)と(N)の間に介在して、読み出しに際しては自動的に復号化し、書込みに際しては自動的に暗号化する。 (J)は、自動暗号化設定されていないファイルへのアクセスの場合は何もしない。

自動暗号化設定されているファイルの場合は、処理をいったん(J)に引き取って実施する。処理方法は前項手動暗号化の場合と同じであるが、自動暗号化の場合(J)には、ファイルの

データが一括で与えられるわけではなく、ファイルポインタとともに、ファイルのRead／Writeブロック単位で与えられ、暗号化／復号化はその単位に順次実施される。

4.3.4.6 ウェブアクセス管理機能

この機能のプロセスを図８の①～⑧で示す。利用者が業務システムのURLをWebブラウザ(C)に入力して表示させる場合、通常はWebページからセキュリティ対策としてユーザ名、ID、パスワードの入力が要求される。

ミドルウェア(M)は、業務システムのURLが入力され(①)、URLが示すサイトへのアクセスが実行されているかどうかを常駐プログラムにて監視している(②)。もしそのアクセスが実行された場合、(M)は入力されたURLをURL-IDに変換する(③)(④)。このURL-IDをもとにＵＳＢキーにアクセスし(⑤)、(M)はＵＳＢキー内のメモリ(T)のID、パスワードを読み出して(⑥)、自動的にWebページが求める覧へ入力し(⑦)、ユーザ名／ID／パスワード入力後のWebページを表示する(⑧)。ここでは利用者にID／パスワードを見られないようにしている。

(M)でURLを(③)(④)のプロセスにてURL-IDに変換しているは、長いURL情報の場合、ＵＳＢキー内のメモリエリアを多く占有することとなるので、これを防止するためである。URL-IDは1byteの情報量で、(M)において自動生成している。また、(M)の常駐プログラムが起動するのは、(C)を起動した時点としている。

Webサーバ側では、アクセス後のログオン、ログオフ、アップロード、ダウンロードの4つの操作に対して、利用者毎に操作できる権限を規定しており、その操作はタイムスタンプとともにサーバ内にログを蓄積することで不正への監視を実施している。

4.3.4.7 印刷管理機能

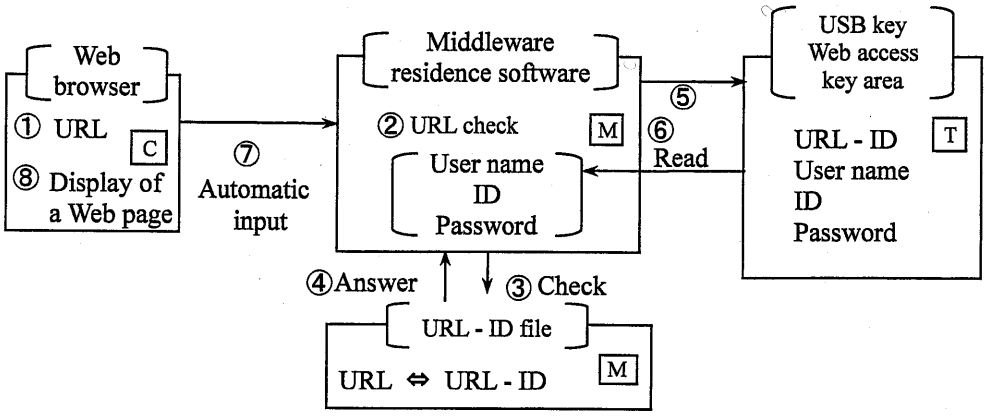
利用者が印刷コマンドを実行すると、図７の①～④のプロセスで印刷すべきファイルを暗号化し、印刷サーバへ転送する。印刷サーバに自分を含む指定された利用者が自分のＵＳＢキーを持参して挿入する。次に、印刷キューとして蓄積された自分のファイルが、図７の⑤～⑧のプロセスで復号され、印刷が実行される。

なお、暗号化されていないファイルは通常通りの印刷処理が行われ、復号化されるまでにキューとして蓄積されるファイルとは別系統の処理が行われる。

4.4 企業への導入効果と導入、運用上の工夫

4.4.1 導入の効果

今回のシステム導入で、パスワードを忘れた利用者に対するヘルプデスクにおける対応稼働（OSの再インストール等）が大幅に削減された．一方、ＵＳＢキーの管理や紛失時の



Note : ① ～ ⑦ are the orders of processing.

図8 Webページ表示コントロールの処理方法

Fig.8 The processing method of web pages display control.

再発行処理などの負担は増加する。しかし、図９に示す管理センタ（Administration Center）の業務をアウトソーシングしたため、この稼働増を抑えることができた。

今回検討対象としたPC300台規模の会社において、ヘルプデスク担当者２名の稼働の約30%削減（人件費約300万円／年の減）ができるという実証データを得ることができた。これは、アウトソーシングも含めた本対策のための投資を１万円／PCと仮定すると、導入コストが300万円となり、１年程度で初期投資が回収できることを示している。

なお、初期導入費用に換算した大略のコスト比は、個人別に権限規定したＵＳＢキー（50%）、ミドルウェアのカスタマイズ（30%）、図９の運用アウトソーシングサービス（4年分）（20%）であることが判明した。

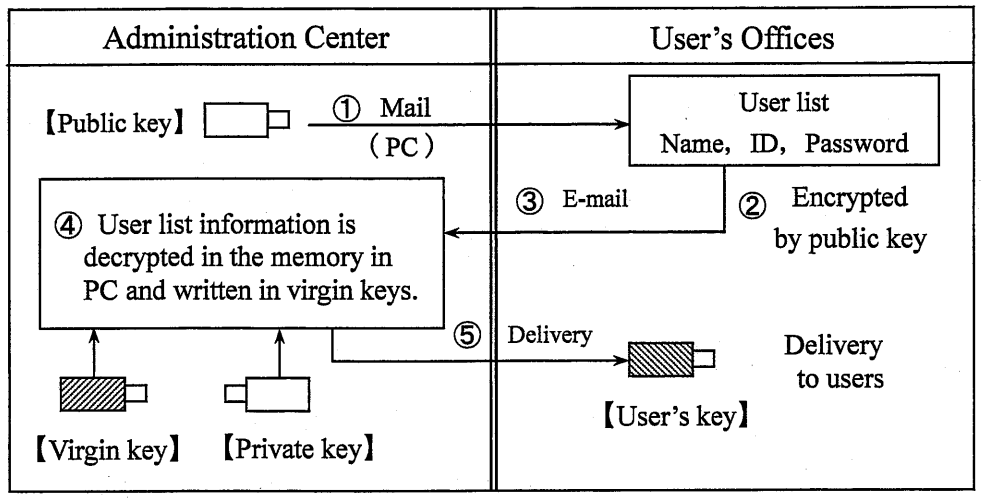
4.4.2 導入時および運用上の工夫のポイント

本システムの導入にあたっては、ＵＳＢキーにもりこむ機能が利用者それぞれで異なるため、その機能設定を容易に行う必要がある。今回、質疑応答形式による要件定義ツールを開発して、個人別設定の自動化を図り、導入時の稼働負担の軽減を実現した。

一般に企業における社内情報へのアクセス権限は、職制によって規定され管理されている。今回、企業の職制 DB を要件定義ツールおよびシステム内に取りこむことで、アクセス権限者指定の煩雑さが解消できた。

ＵＳＢキーの新規発行や、紛失時の再発行の業務処理フローを、図９の①～⑤を用いて以下に示す。管理センタから利用者のオフィスへ、ユーザリストを暗号化するための公開鍵を郵送する(①)。ユーザリストはその公開鍵で暗号化され(②)、電子メールの添付ファイルとして管理センタへ送られる(③)。

管理センタでは操作者に秘密の情報がわからないようにするために、PC内のメモリ上で、



Note : ① ～ ⑥ are the orders of processing.

図9 USBキー生成・配布の処理フロー

Fig.9 The processing flow of the USB key generation and delivery.

秘密鍵を用いて暗号を復号して、操作者を介さずバージンキーからＵＳＢキーを生成する(④)。ここで作成されたＵＳＢキーは送付書を付けて利用者オフィスへ配送される(⑤)。

一般の企業活動においては、PC を社外に持ち出すケースが多い。この場合、ＵＳＢキーと PC を別々にしておくことは PC 紛失時の情報漏えい対策として有効である。このことから、外部持ち出し用のカバンを特注して、ＵＳＢキーをさしたままの PC が、カバンに入らない工夫も実施した。また、利用者のＵＳＢキーを集中保管し、朝に払い出し、夕方に戻すルールもセキュリティ管理上有効であった。

4.5. まとめ

本論文では、一般企業において、内部情報漏えいを防止するためのコストパフォーマンスの良いセキュリティ対策を検討した。この中では、PC にインストールされるミドルウェアを用いて、PC やサーバの既存のセキュリィ機能との連携を検討し、安価であるが処理機能が限定されるＵＳＢキーの適用方法を工夫した。

しかし今後は、次期ステップとして以下のような PKI 認証（別紙：用語説明(16)）の利用等も含めた機能について、コスト効果もふまえた効率的な実現方法の検討が課題である。

（1） ディジタル証明書の発行要求とインポート
（2） Web 取引データの保護
（3） インターネット利用制限と利用履歴の保存、等

また、「所持」や「記憶」による本人認証では、万一の場合の裁判証拠性が小さいことを考慮する必要がある。このことから、次章で示す、より本人認証機能の高いバイオメトリックス認証へのグレードアップ検討が重要となる。本論文が、コストパフォーマンスの良いセキュリティ対策を望む中小企業において、参考になることを期待している。

なお、第９章（参考）に示すように、このＵＳＢキーの社会での利用は、すでに幅広く行われつつある。日本生命の外交員向けの１０万個の利用をはじめとして、総合商社や警察など、業種業態を問わず各方面への導入実績あげることにより、法人の情報資産保護に寄与している。

[参考文献]

[1] “認証の三要素”,本人認証技術の現状に関する調査報告書,pp. 3,情報処理振興事業協会セキュリティセンタ-,東京, 2003. http://www.ipa.go.jp/security/fy14/reports/authentication/uthentication2002.pdf

[2] 瀬戸洋一, “生態認証技術の市場動向”,生態認証技術, pp. 8-14, pp. 22, 共立出版株式会社,東京, 2002.

[3] 河内,宇佐美, “情報セキュリティ対策の状況調査結果（別添.)”, pp. 17, 総務省政策統括官（情報通信担当）情報流通振興課, May, 2002. http://www.soumu.go.jp/ s-news/2002/020509_2.html

[4] 河内,宇佐美, “情報セキュリティ対策の状況調査結果（別添.)”, pp. 25, 総務省政策統括官（情報通信担当）情報流通振興課, May, 2002. http://www.soumu.go.jp/s-news/2002/020509_2.html

[5] http://www.aladdin.co.jp/etoken/index.html

[6] http://www.msol.co.jp/it/msolock/lock/index.html

[7] 山口雅治,細田泰弘,佐藤能行,小杉 哲,菅生 清,青野正宏,” 情報セキュリティ高度化のためのデ-タ保護技術に関する研究（委託研究)”,アー5「セキュアモジュールと連携した認証機能の実現方法の研究開発」,通信・放送機構, 2002. http://www.shiba.tao.go.jp/kenkyu/itakua/seika/37/37yokou37.pdf

[8] 市川正紀, “ セキュリティマネジメントに関するユーザー調査 (1)”,インターインテリジェンス,東京, Oct. 2003. http://www.itmedia.co.jp/survey/0310/15/svn06.html

第5章　情報漏えい対策システムへの指紋認証の適用

5.1 概要

オープン系ネットワークの進展や労働人口の流動化など、企業をとりまく環境の変化とともに、近年、「社内からの情報漏えい対策」の重要性がクローズアップされている。この中で、一般の企業においても、個人認証をより強化したコストパフォーマンスの良いセキュリティ機能の強化は大きな課題である。この場合、第４章で述べた一般企業で利用されているＵＳＢキー方式（別紙：用語説明(4)）より、さらに個人認証機能の高くしたいとするニーズが実際の事件を契機に出ている。

このことから、本章では目標価格１～２万円／パソコンの低コストを条件としてバイオメトリックス認証（別紙：用語説明(6)）の適用を研究している。本論文では実際に発生した情報漏えい事件をモデルとして、司直の見解に基づきセキュリティ機能に必要な要件を整理している。また、実際に導入した指紋認証を用いたセキュリティシステムに対する検証を行った結果、実用的なセキュリティ対策が可能であることが判明したので記述する。

本章では、5.2項で現状のセキュリティ対策の状況と実際の事件などから導出された必要要件を考察している。また、5.3項でバイオメトリックス認証のうち、指紋認証を選定した理由を論じ、指紋認証を用いた対策システムの具体例を示している。5.4項で今回のテストシステムの概要とその検証方法を示している。また、5.5項で導入の検証結果を示している。

5.2 内部情報漏えい対策の要件検討

実際に発生した事件に基づくセキュリティ要件の考察を行い、必要条件を検討する。現実に発生した事件とは“職場を同じくする下請負会社の社員が、ノートパソコンのハードディスクにＬＡＮ経由でサーバにアクセスして顧客情報をコピーし、不正に持ち出して悪用するおそれがあった”というものである。

これに対して、司直と対応した経験から導出された情報漏えい対策の基本は、次の２点に集約される。

(1) 事件発生に伴う被害が明確であること。
(2) 決定的証拠をもとに被疑者本人と情報漏えいの過程が特定できて裁判で勝てること。

この場合、「被疑者がハードディスクにコピーしたことを示すユーザ認証（別紙：2 技術説明）に基づく時刻と痕跡」を証拠として、裁判所へ提出することが被害者側に求められ

る。この事件モデルにおいて、一般的なセキュリティ対策システムに要求される要件を表1に、事件に伴う必要要件を表2に示す。

表1 情報漏えい対策に関する主なセキュリティ機能

Table 1 The main functions about measure against information leak.

	項目	内容
ネットワーク側	(1) アクセス制御	レイヤ2/3/4の情報に基づくネットワーク機器のアクセス制御
	(2) 暗号化	IPの通信をセキュアに行うためでIPsecやSSLが代表的
	(3) ネットワークにログオン時のユーザ認証	RADIUSサーバでのネットワークログオン時の認証やLANにおけるEAP認証が代表例
	(4) LANのメンバーシップのための認証	LANスイッチのポートベースでのハードウェア情報に基づくユーザー認証が代表的
	(5) DHCPサーバにおけるユーザ認証	IPアドレスの配信時でのユーザー認証
	(6) ファイアウォールにおけるユーザ認証	ファイアウォールを通過するパケットに対する認証
サーバ・コンテンツ側	(7) アクセスに対する認証	ID/パスワード認証が一般的だが、バイオ認証の必要性が増大
	(8) アクセスログの蓄積	イベントログ、SYSLOG、アカウンティングログを管理・保存
	(9) 認可における制御	参照、更新、削除、登録などの権限をユーザの資格に応じて付与
	(10) アクセスデータの蓄積	メールや外部送信データそのものを蓄積

表2 事件に伴う情報漏えい対策システムへの必要要件

Table 2 The requisites to information leak measure systems.

項番	必要事項	必要条件	(注)
1	裁判で決定的証拠となりうる本人性の確認	バイオメトリックスによる個人の特定	(7)
2	アクセスへのトレーサビリティの確保	個人を特定したアクセス制限とアクセスログの蓄積	(8)
3	参照、媒体への記録、印刷の制限	文書管理が行えるシステムなどの適用	(9)

(注) (7)～(9)は表1の項目で関係する部分を引用している。

表２の 1 項の本人性を確認する手法としては「知識」によるもの、「所持」によるもの、本人の生体的、行動的特徴である「バイオメトリックス」（別紙：用語説明(6)）によるものが挙げられる[1]。個人の認証においては、ID/パスワード（知識）やＩＣカード（所持）では“厳密な本人認証の観点において、裁判の決定的証拠にならない”ことを重視する必要がある。このことから、表 1 の“(7)アクセスに対する認証”において、バイオメトリックス認証が必要要件となる[2][3]。

この場合、端末側の個人認証とサーバ側でのユーザ認証において、従来用いられているID/パスワード方式への適用容易性を確保することがコストパフォーマンスの観点で重要である。このことから今回の実施例では、“指紋認証データから本人も知らない非公開なパスワードに変換して適用する方式”を既存システムへのアドオン型で採用した。

表２の 2 項のトレーサビリティについては、一般的にサーバが標準的に備えている表 1 の“(7)アクセスに対する認証”と“(8)アクセスログの蓄積”機能により安価に実現可能であり、5.3 項に示す実施例で適用した。（別紙：2 技術説明）

表２の 3 項の各種制限要件については、表 1 の“(9)認可における制御”の実現が必要となる。今回はサーバが標準的に備えている「フォルダへのアクセス権の設定」により“参照に関する制限”を実現している。しかし、“媒体への記録や印刷の制限”については、高価なシステムの適用が必要であり、第８章に述べる発展形態の実現が今後の課題である。（別紙：2 技術説明）

5.3 指紋認証システムによる対策の実施例

5.3.1 指紋認証を選定した理由

表２の 1 項に示したバイオメトリックス認証において、指紋認証を選択した理由は以下の通りである[3][4]。

(1) 机の上などに指紋は残り、物的証拠に利用できること。
(2) 本人である決定的な証拠として、裁判で採用された長い歴史があり、警察に十分なデータベースとして積みあがっていること。
(3) センサのコストが安く、小型であること。
(4) 業務に使用する社員への適用であることから、犯罪者チェックといった心理的抵抗感が少ないこと。
(5) 指紋センサユニットは個人使用であり、他人接触嫌悪感の問題がないこと。
(6) 万一、個人認証に失敗しても、対象が社員であるため、対面での本人確認と、システム管理者支援による指紋データの再登録などの対応が可能であること。

(7) ２０代～５０代中心のオフィスワーカーが対象であることから、高齢者のような指紋データのとりづらい特殊事情を持つ者が比較的少ないこと。
(8) 他のバイオメトリックス方式と比較して最も導入実績があること[5]。

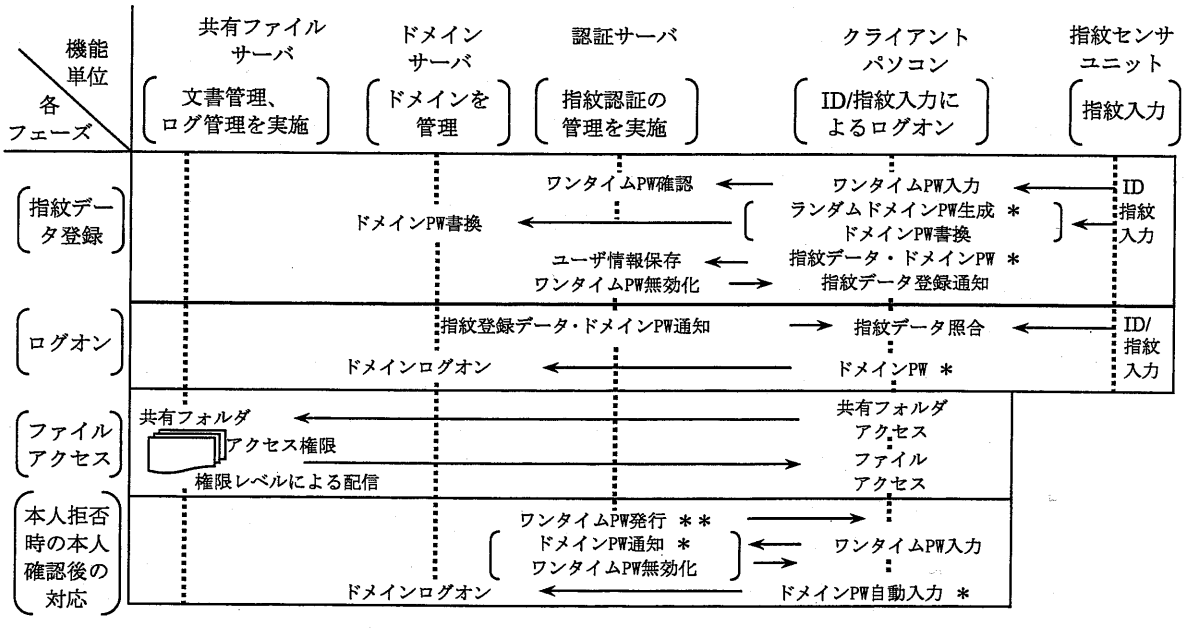
5.3.2 指紋認証タイプの検討

セキュリティにかける予算に限度のある一般企業がオフィスで利用できることを前提とすると指紋認証タイプとして次の条件を満足する必要がある。

(1) クライアントパソコンに接続できる小型のユニット形式であること。
(2) 指紋認証アルゴリズムの使用料も含めたセンサユニットのコストが安く（２万円以下)、市販されていること[6]。

これに適合する指紋認証のセットは、現状４つのタイプしか市場に存在しなかった。

４つのタイプとは、感熱式ラインセンサを用いた周波数解析法のタイプ、２社のセンサメーカーの光学式エリアセンサを用いたマニューシャ法の２つのタイプ（A）と（B)、静電容量式エリアセンサを用いたマニューシャ法のことである[7]-[10]。ここでは、表３に示すようにそれぞれ順にタイプ１～タイプ４と称している。



[凡例]　PW：パスワード　　ユーザ情報：ID、指紋登録データ、ドメインPW
＊：利用者へは非公開　　＊＊：システム管理者による操作

図1 指紋認証システムにおける処理フロー

Fig.1 The process flow in the fingerprint authentication system.

5.3.3 検証システムの処理方法

今回、検証対象とした指紋認証システムの処理フローを図１に示す。また、ログオン時の処理方法を図２に示す。この処理方法では、図２に示すようにログオン時のクライアントパソコンに入力されたID/指紋データをクライアントパソコンにおいて、認証サーバに登録されているユーザ情報を取り出して照合確認後、本人へも非公開なパスワード（ドメインパスワードとしてランダムに生成される）を認証サーバから取得する形式をとっている。この照合確認プロセスを認証サーバにおいて行うことも可能であるが、今回は認証サーバの負荷を考慮してクライアントパソコンにおける照合方式を採用した。また、図１、図２に示す一連の通信および各サーバ、クライアントパソコンのファイルには、“3DES 暗号”を適用した。

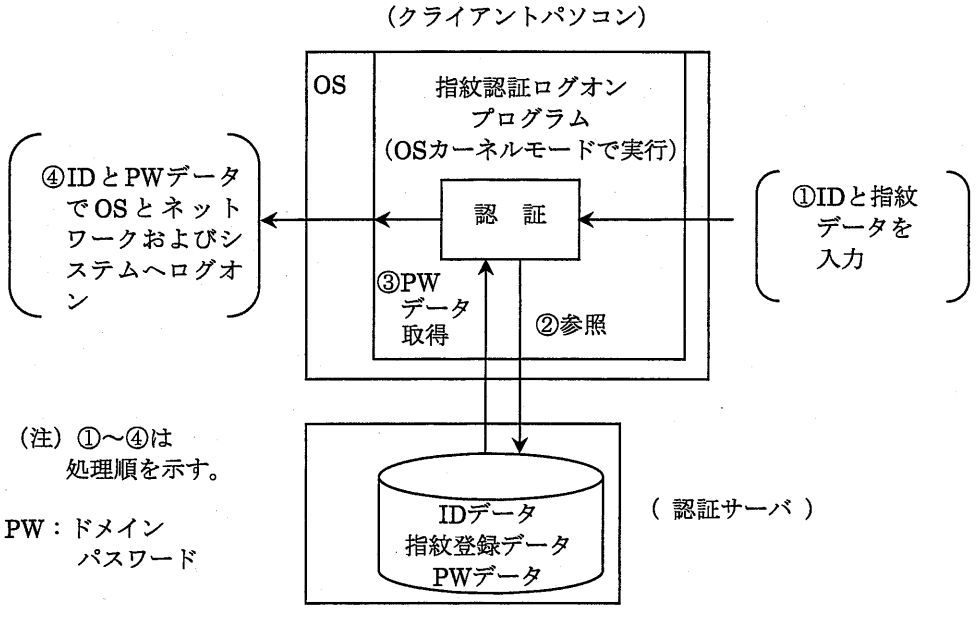


図2 ログオン時の処理方法

Fig.2 The processing method at the time of logon.

このログオン時の認証プロセスにおけるタンパフリー性を確保するために、次の 2 つの方法を適用している。

(1) クライアントパソコンの OS として、ログオン時におけるセキュリティ管理機能を持つ OS を適用する。
(2) クライアントパソコンのアドミニストレータ権限を利用者に開放しない。

これにより、利用者によるOSのカーネル書き換えを不可能にするとともに、カーネルモードで動作する指紋認証のログオンプログラムへの利用者の介入を防止している。

今回、指紋の経時変化、経年変化への耐性を向上させることを目的として、最新の認証された指紋データについて、所定の条件で認証サーバ内の指紋登録データへの置き換えを行い、本人拒否を少なくする工夫を行っている。

5.4 導入効果の検証方法

5.4.1 比較検証の前提条件

今回の検証においては、100万回の入力テストを実施している。これは、1つの認証管理単位を 1,000 人として毎実働日に1回認証するものと仮定し、さらにその業務システムの使用寿命を4～5年（実働日約 1,000 日）としたためである。

（1,000 回／日×1,000 日＝100 万回）

今回の検証においては、他人受容率（FAR）を最大で 0.01%としている。本システムにおいては、図2に示すように、ID と指紋入力を併用している。もし、なりすましを意図したとしても、他人の ID を投入した後に、続けてその ID にたまたま一致する他人受容が発生しないと、なりすましは不可能である。

このようになりすましへのリスクが極めて低いことから、FAR の評価について、今回のテストでは対象外とし、タイプ1～4の仕様に決められている数値を所与のものとして用いた。

他人受容率（FAR）が低い場合、本人拒否率（FRR）が高くなるという相関がある。タイプ1～4で FAR が 0.01%以下と低く、FRR の評価が重要となる。他人受容に伴うなりすましリスクが極めて小さい中で、一般企業では、本人拒否による本人データ再登録のための運用コスト増、あるいはシステム利用できない機会損失リスクが重視されるのも、FRR の評価が重要となる点である。本人拒否率（FRR）の比較検証の条件は、エアコン完備のオフィスを前提として、次の通りに設定している。

(1) 対象者は２０代～４０代を中心とする男女オフィスワーカー２５名（男性１８名、女性７名）である。このうち指紋の薄い者２名、乾燥指の者１名、高齢者２名を含んでいる。
(2) いずれも利き指での測定とし、タイプ３のみ標準と指定されている親指、その他は人差し指でテストする。
(3) 指紋入力操作に慣れてからのテストを行い、FAR はタイプ1、タイプ3で 0.01%、タイプ2で 0.001%、タイプ4で 0.0001%に設定されている。
(4) 社員は最悪の場合でも、指紋認証に成功するまで、4回は連続して操作をすることと

している。

(5) センサ表面のクリーニングについては、入力に失敗した時のみ実施する。

(6) 指紋の経時変化は考慮せず、指紋を登録した日にテストする。これは、本システムが指紋の変化に追随して本人拒否を少なくする機能を有しているためである。

(7) 指の状態を“通常”、“多湿”、“乾燥”の3状態に変化させる。これは、指の状態が、冷たい飲み物に触れて湿る場合や、長時間紙に触れて乾く場合を想定しているためである。

(8) FRRの算定条件として、指の状態が“通常”、“多湿”、“乾燥”であるときのFRRを2:1:1の割合で合算し、それぞれを加重平均して、結果としている。

(9) “多湿”は手洗い直後の状態を想定して、水で湿らせたガーゼを触った直後にテストする。“乾燥”はエアコンのフル稼動時の状態を想定して、指にパウダーをまぶした後にふき取ってテストする。

(10) 経時変化に対する耐性について、指紋の登録直後認証を行った場合、認証がうまくいく可能性は極めて高く、実際の運用環境とは違いがある。評価は長期間にわたって行うことが望ましいが、今回は時間的制約があることから、『認証操作を連続して行わない』というポリシーにて評価を実施する。

(11) 各指紋認証システムで使用している指紋センサでは、運用によりセンサ表面が汚れ、結果として指紋認証に失敗する場合が出てくるため、定期的なクリーニングが必要となる。しかし、1入力毎にクリーニングを実施するのは現実的ではないため、本評価では、指紋認証に失敗した際に初めてクリーニングを行うという方法をとる。クリーニング後に指紋認証に失敗した場合には、再度クリーニングを実施する。

5.4.2 検証システムの概要

今回用いた検証システムの概要を図3に示す。クライアントPCを用いて指紋認証によりWindowsのドメインにログオンするための検証システムとしている。動作環境は次の通りである。

(1) クライアントPCのソフトウェア構成

① Windowsの起動時、及びログオン待機時に実行され指紋による認証を行うログオンプログラムを用いている。OSの違いにより、NT版（WindowsNT/2000/XP）、9x版（Windows95/98/Me）に分けており、NT版ではスクリーンセーバの制御も行う。

② Windows95/98/Meで、指紋認証を用いた解除ができるスクリーンセーバのプログラムを適用している。

③ 指紋の新規登録・再登録・追加を行うためのユーティリティプログラムを用いている。

④ タスクトレイに常駐し、ユーティリティの起動、バージョン情報の確認などの機能

を提供する常駐アイコンプログラムも用いている。

⑤ クライアントPCソフトウェア群のインストール、アンインストール、アップデートを行うインストーラプログラムを用いており、シリアル版指紋センサユニットを使用するWindows95/NT用とUSB版指紋センサユニットを使用するWindows98/Me/XP/2000用に分かれている。

(2) クライアントPCの動作環境

① ハードウェア

メモリ64MB以上、HDD50MB以上の空き、USB 1ポート以上（※1）、シリアルポート1ポート以上（※2）

※1 WindowsXP、2000、Me、98SE、98の場合

※2 Windows95、NT4.0の場合

② OS

WindowsXP（HomeEditionは除く）※1、Windows2000SP2（※2）、WindowsMe（※2）、Windows98SE（※2）、Windows98SP1（※2）、Windows95OSR2（※2）、Windows95SP1（※3）、WindowsNT4.0SP6（※3）

※1 WindowsXP HomeEditionはドメインへの参加機能を備えていないためサポートしない。

※2 Internet Explorer5.0以上必須。Internet Explorer6.0以上推奨。

※3 Internet Explorer5.0以上必須。Internet Explorer5.5SP2以上推奨。

(3) ネットワーク環境

① Windowsドメインネットワーク環境として、TCP/IPを使用するWindowsNTドメインの下のネットワーク環境を対象としており、ワークグループは対象外としている。一台のクライアントPCで複数のドメインを切り替えて使うことも可能とし、最大のドメイン数は1ユーザあたり4ドメインまでとしている。

② 管理サーバでは使用ポート番号としてTCP/IPの32772番を使用するため、このポート番号に対するアクセスを可能としている。

5.5 比較検証の結果

指紋センサとして比較評価に用いた4つのタイプのユニット諸元を表3に示す。照合精度と登録する指については公称値を用いている。

(1) タイプ1では1,000人の事業所でも加重平均して年1回以下のFRRであり、タイプ2においても、年2回以下のFRRであるという結果となり、十分な実用性を有している。

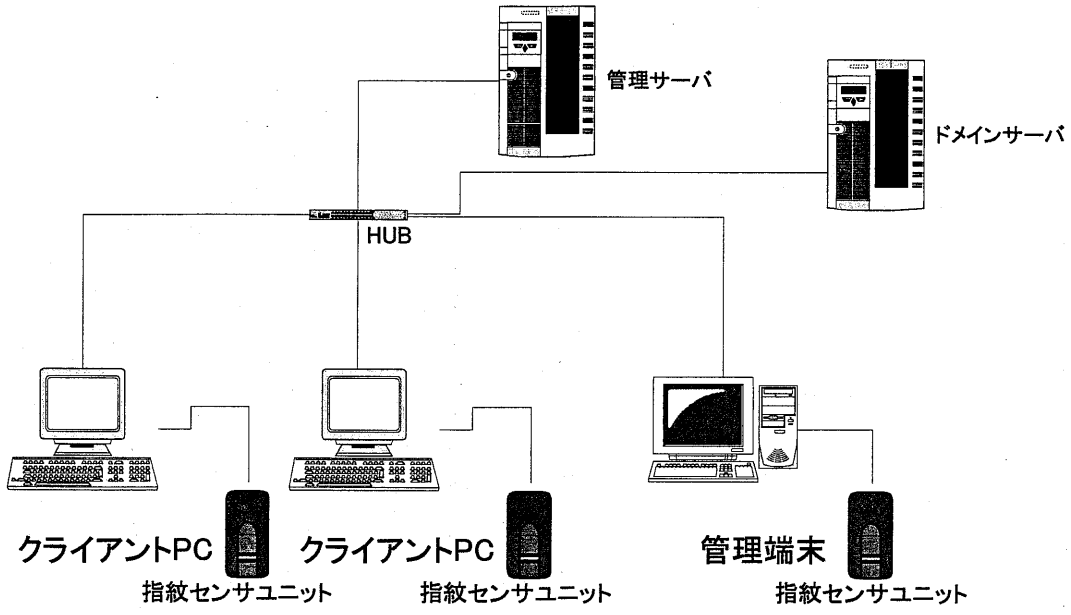


図3 検証システムの概要図

Fig.3 The outline figure of this verification system.

表3 比較対象の指紋認証ユニット

Table 3 The Compared fingerprint attestation units.

認証タイプ	登録時 入力回数	照合制度 (公称値)	登録する指 (公称)
タイプ1 感熱式ライセンサ 周波数解析法	3	FRR 0.1% FAR 0.01%	効き指の人差し指
タイプ2 (A) 光学式エリアセンサ マニューシャ法	2	FRR 0.1% FAR 0.001%	効き指の親指
タイプ3 (B) 光学式エリアセンサ マニューシャ法	4	FRR 1.4% FAR 0.01%	効き指の人差し指
タイプ4 静電容量式エリアセンサ マニューシャ法	3	FRR 0.5% FAR 0.0001%	効き指の人差し指

(注) 登録時入力回数とは、指紋の登録時に必要となる指紋入力回数である。
一般的に回数が多いほど認証精度が向上する。

(2) 1,000 人の事業所で FRR が毎日(0.1%)発生するのは困るが、月 1 回程度 (0.022%)の発生を許容すると仮定すると、タイプ 3 について加重平均しても 0.0266%であり、ほぼ許容できることがわかる。

(3) タイプ 4 は静電容量式であることから、指の状態に対し、クリティカルなところが見られ、加重平均すると実用レベルには達していない。

以上の結果から、タイプ 1 ～ 3 について一般のオフィス環境における比較的厳しい条件下においても、システム運用管理者のもとで、十分な実用性のあることが判明した。

なお、ログオンでの認証に失敗した場合、ID と指紋データの再入力がシステム側から要請される。今回のテストのように 4 回入力しても失敗する頻度はかなり少なく、“対面で本人を確認して再登録を行う運用方式”でも認証失敗時の対応として、運用上問題にならないと考えられる。

表 4 実運用での本人拒否率(FRR)比較(%)

Table 4 The Failure Rate of Refusal(FRR) comparison under real employment. (%)

認証タイプ	状態	入力 1	入力 2	入力 3	入力 4	加重平均	結果
タイプ 1 感熱式ラインセンサ 周波数解析法	通常	0. 8000	0. 0000	0. 0000	0. 0000	0. 0003	約33万回に 1回の認証失敗
	乾燥	15. 2000	1. 3376	0. 0107	0. 0001		
	多湿	63. 2000	20. 7296	0. 1658	0. 0013		
タイプ 2 (A) 光学式エリアセンサ マニューシャ法	通常	0. 8000	0. 0000	0. 0000	0. 0000	0. 0007	約15万回に 1回の認証失敗
	乾燥	65. 6000	21. 7792	0. 1742	0. 0014		
	多湿	42. 4000	9. 1584	0. 0733	0. 0006		
タイプ 3 (B) 光学式エリアセンサ マニューシャ法	通常	4. 0000	0. 0000	0. 0000	0. 0000	0. 0266	約3800回に 1回の認証失敗
	乾燥	79. 2000	32. 9472	1. 3179	0. 0527		
	多湿	56. 8000	17. 2672	0. 6907	0. 0276		
タイプ 4 静電容量式エリア センサマニューシャ	通常	20. 0000	0. 3200	0. 0026	0. 0000	0. 7808	約130回に 1回の認証失敗
	乾燥	59. 2000	23. 4432	4. 6886	0. 9377		
	多湿	91. 2000	50. 7072	10. 1414	2. 0283		

今回さらに、以下の副次的効用もあることが判明した。

(1) ログオン時に指紋をとられることで、「悪いことはできない」という心理的障壁効果が生まれたこと。
(2) ログオン時に従来必要だったパスワードの投入が不要となり、パスワードを覚える必要がなく、定期的なパスワードの変更も不要であること。
(3) 各ファイルへのアクセス時にパスワード入力が不要であること。
(4) 社員の入退室管理と併用することでより一層セキュリティレベルが向上すること。

導入に伴う不便な点は、パソコンを外部へ持ち出す場合や家庭におけるリモートアクセスでの利用時に、指紋センサユニットが必要となる点である。

以上のような、システムのセキュリティ性能の向上およびセキュリティ意識向上の効果が比較的低コストで得られたことは、今後情報漏えい対策のシステムの導入を検討する企業では十分参考になるものと考えられる。

5.6 まとめ

本論文では、企業内部の情報漏えい対策について、実際に発生した事件をモデルとして、企業として必要なセキュリティ要件を、司直の見解も含めて整理した。また、それを実現する指紋認証による情報漏えい対策システムが、１～２万円／パソコンのような比較的安価で実用になることを示した。

この中では、情報漏えい認証システムの導入に伴う社員の利便性の向上や、セキュリティ意識の向上が図られたことも見逃せない効用である。犯罪捜査に多用される指紋を毎日投入させて行動を見張る情報漏えい認証システムの一般社員への犯罪抑止効果は、心理的にも大きいものと考えられる。

本章で述べた指紋認証方式の、今後の課題としては、第８章の 8.3 項に示すセキュリティプラットフォームへの社会基盤としての認証情報の流通の実現があげられる。また、携帯電話への搭載などの展開についても今後の検討が必要である。

なお、この指紋認証方式はすでに社会での利用が進みつつあり、第９章の（参考）に示すように、名古屋市役所をはじめ、合計 1.5 万個以上の指紋センサユニットがパソコンのセキュリティ対策として利用されている。

[参考文献]

[1] “認証の三要素”, 本人認証技術の現状に関する調査報告書, pp. 3, 情報処理振興事業協会セキュリティセンター, 東京, 2003. http://www.ipa.go.jp/security/fy14/reports/authentication/uthentication2002.pdf

[2] 杉浦　淳ほか, “指紋識別に基づくユーザインターフェース”, 情報処理学会インタラクション’99, pp. 169-176, march, 1999.

[3] 佐藤宏介ほか, “自分がパスワード, -バイオメトリック本人確認-”, 信学会誌, Vol. 82, No. 4, pp. 340-345, 1999.

[4] 内田　薫ほか, “指紋識別を用いた情報システム”, 信学技報, OFS98-26, pp. 13-18, Sep. 1998.

[5] 瀬戸洋一, “生態認証技術の市場動向”, 生態認証技術, pp. 18-21, 共立出版株式会社, 東京, 2002.

[6] 川上潤司, “レポート2：セキュリティの主役となるバイオメトリックス(生態認証)”, 日経情報ストラテジー, 2002年10月号, pp74-79, Oct. 2002.

[7] D. Inglis et al, A Robust, 1.8V, 250 ” W, Direct Contact 500dpi Fingerprint Sensor”, IEEE ISSCC98, SA 17.7, pp. 285-286, Feb. 1998.

[8] O’ Gorman, L “Figerplint Verification, Biometrics, Personal Idetification”, Network Society (Ed. By Tain), pp. 43-64, Kluwer Academic Publishers, 1999.

[9] Jain, A. et. al, “On-Line Fingerprint Verification”, IEEE Transactions on pattern anaiysis and machine Intelligence, Vol. 19, No. 4, pp. 302, Apr. 1997.

[10] 浅井ほか, “マニューシャネットワーク特徴による自動指紋照合-照合過程-”, 信学論, Vol. J72-D-2, No. 5, pp. 733-740, 1989.

第6章 情報漏えい対策システムへのSBC方式の適用

6.1 概要

最近、個人情報保護法遵守が社会情勢となりつつあり、既存の業務システムに対する効果的なセキュリティ対策は企業等において急務となっている。本章では、従来のＷｅｂコンピューティング方式（別紙：用語説明(2)）に代わって、「セキュリティの確保」や「情報処理の高速化」が経済的に実現できる“ＳＢＣ方式（別紙：用語説明(1)）”に着目し、業務システムへの適用性検討を実施している。

日本における従来のＳＢＣ方式の業務システムへの導入目的としては、処理の高速化と管理コストの低減によるＴＣＯ（Total Cost of Ownership）の削減が主であり、セキュリティの向上という目的でのＳＢＣ方式の導入はほとんど検討されてこなかった[1]-[3]。日本では、社会的な体面上セキュリティを主目的にすることへのはばかりがあるのかもしれない。

今回、損害保険会社（以下「保険会社」と略す）と代理店の間の業務システムを例にとり、日本では例のない、顧客情報の不正利用対策としてのＳＢＣ方式の適用性を検討している。この中では、コストパフォーマンスの観点から、３万円以下／パソコンを目標価格として検討を進めている。

本章では、6.2項でＳＢＣ方式の業務システムへの適用性を検討している。6.3項で保険代理店システムにおけるセキュリティ上の問題点とＳＢＣ方式の適用性検討の内容を示す。6.4項で処理速度のベンチマークテスト結果およびモデルシステムへのＳＢＣ方式導入の評価結果を紹介する。6.5項で今後の発展形態としてのペーパーレスシステムについて検討したので、その内容を提起する。

6.2 SBC方式の適用性検討

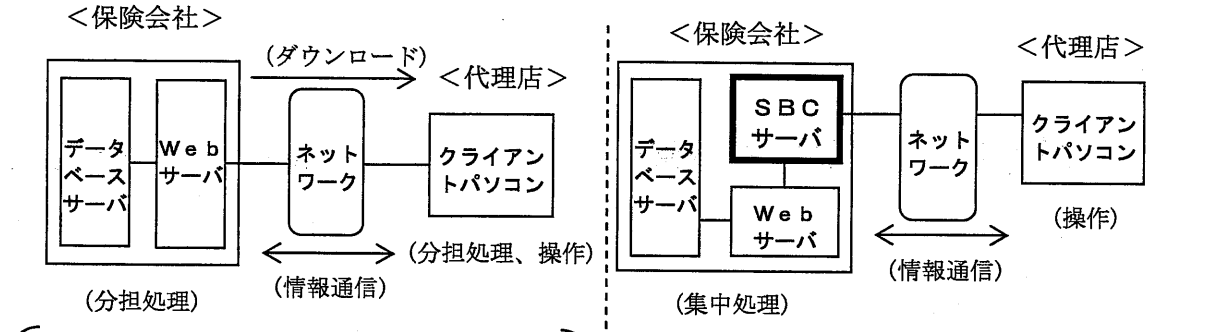
近年のダウンサイジングやパソコンの低価格化、高機能化の流れに沿って、企業における業務システムにおいて、メインフレーム上のシステムをクライアントサーバ（ＣＳ）方式（別紙：用語説明(3)）のシステムへ移植する動きが盛んに行われてきた。しかし、クライアントサーバ方式は分散システムであるがゆえに、クライアントパソコンの性能や、クライアントパソコンとサーバを結ぶネットワークの帯域幅にパフォーマンスが大きく左右されるという構造的な問題をかかえている。また、クライアントパソコン毎にプログラムをインストールしなければならないという保守面の負担も問題である[4]。

これらの問題点を解決するために、Ｗｅｂサーバとインターネットブラウザを利用した、Ｗｅｂコンピューティング方式が1990年代後半から、業務システムの主流になりつつある。この方式を用いた保険会社と代理店を例とした情報処理方法を図１（１）に示す。本方式における、サーバとクライアントパソコンの両方で情報処理が行われるしくみが、セキュ

リティの向上と処理の高速化の阻害要因である。

このＷｅｂコンピューティング方式の問題を解決するために、最近登場したのが、ＳＢＣ方式である[5]-[7]。この方式は、クライアントパソコンとネットワークを介したサーバとのやり取りを、「マウスクリック」、「キーストローク」、「画面遷移の処理」に限ることで、速度の向上などのメリットを得ようというものであり、クライアントパソコン内のハードディスクを用いないことがセキュリティを高める要因である[8][9]。

ＳＢＣ方式の特徴をＷｅｂコンピューティング方式と比較した保険会社と代理店を例とした情報処理方法を図１(2)に示す[10]。また、両方式の比較を表１に示す。



(1) Ｗｅｂコンピューティング方式の情報処理方法　　(2) ＳＢＣ方式の情報処理方法

図1 情報処理方法の特徴比較

Fig.1 The comparison of features of method of processing information.

6.3 保険会社と代理店間の業務システムの問題点とSBC方式の適用性検討

6.3.1 代理店業務システムの問題点

保険会社はオンライン計上により、契約管理を簡便化することと、紙ベースでの契約情報（保険証券控）を代理店に残さないことを目的として、代理店を自社の業務システムのネットワークに組み込もうとしている[11]。代理店もこのネットワークから様々なメリットを受けられるため、営業フロントへのパソコンの導入を推進しつつある。

このネットワークに参加し、Ｗｅｂコンピューティング方式などで構築された業務システムを利用すればするほど、顧客情報が代理店のパソコンのハードディスクに蓄積される

表1 Webコンピューティング方式とSBC方式の特徴

Table1 The features of the Web-computing method and the SBC method.

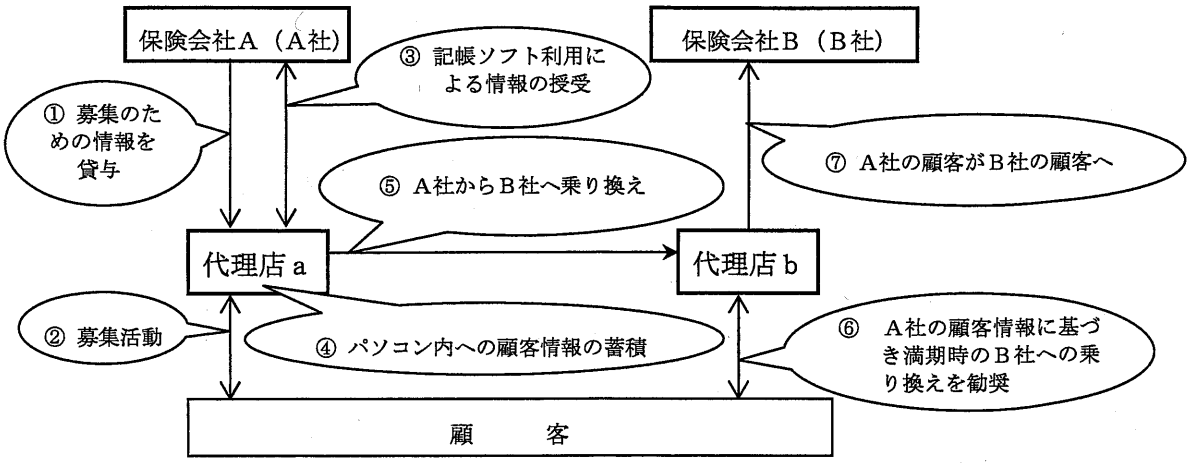
特徴	Ｗｅｂコンピューティング方式	ＳＢＣ方式
長所	(1) インターネットブラウザさえあれば、クライアントサーバ方式と比較して、既存の各種業務システムへ簡単に適用可能である。 (2) 業務システムがＷｅｂサーバで一元的に管理されることから、保守運用性が向上する。	(1) 既存業務システムへのフロントエンドプロセッサとしての導入が容易であり、情報処理速度が向上する。 (2) クライアントパソコンのＯＳやブラウザの種類に依存しないため、旧式パソコンでも適用可能である。 (3) 業務システムの新規導入やバージョンアップ時に、クライアント側での作業は発生せず、保守運用性が高い。
短所	(1) ハードディスクがないと動作しないという、クライアント側に依存した業務ソフトが多数ある。 (2) インターネットのブラウザの種類やＯＳのバージョンを限定しなければ、動作保証ができない。 (3) 処理速度がネットワークの帯域幅に大きく依存するシステムが多い。	(1) クライアント側のプリンタのドライバがＳＢＣサーバ内にあることから、推奨プリンタを指定するか、事前の動作確認作業が必要である。 (2) 高速処理を阻むシステム構成上のボトルネックの発見・解消に高いサーバ技術を持つ人材が必要である。

ことになる[4]。この顧客情報として、住所、氏名、年齢、電話番号、保険対象家族名、無事故歴、車の型式のような10数項目の個人の情報があげられる。

ある法人が保険会社の代理店となる場合、「損害保険代理店委託契約書」が締結される。この契約書では、“募集に必要な物品や情報は保険会社の所有である”としている[11]。しかし保険会社では、代理店のパソコンに蓄積された顧客情報が、代理店契約に違反して不正利用されることを恐れている[11]。

この違反行為の例として、代理店ａが保険会社Ａの代理店から保険会社Ｂの代理店ｂになる場合に、顧客情報が不正利用される可能性のあることがあげられる。このプロセスを図２に示す。ここでは、代理店ａに蓄積されたＡ社の顧客情報を利用して、Ｂ社の商品にふさわしい顧客へ募集活動がなされた場合を契約違反としている。代理店ａが乗合代理店である場合、代理店ｂになることなくＡ社の顧客情報をもとにＢ社の商品を販売することもこの契約違反の範囲に含めることができる。

保険会社においては、システム化の進展に伴い上記のような顧客情報漏えいへの対策が



(注)　①～⑦はプロセスの順序を示す。　Note：①～⑦shows the order of the process.

図2　顧客情報が不正に利用されるプロセス

Fig.2　The process where customer information is illegally used.

急務であり、セキュリティに関する業務システムのしくみ上からの問題解決が必要となっている。

6.3.2 代理店の実態とSBC方式の効用

損害保険業界では、IT投資が代理店の責任で行われていることから、パソコンの性能やOSブラウザの種別が統一されていない。また通信回線へのコスト負担も代理店の責任で行われていることから、ネットワークの形態も区々である。電話回線とモデムによる56kb/s程度の狭帯域のダイヤルアップ回線が一般的に多用されており、低い通信速度による処理速度の遅さが問題である。

これらを踏まえ、ＳＢＣ方式を適用することによる効用は以下の通りまとめられる。

(1) 代理店のパソコン内に顧客情報が残らないことによるセキュリティの向上
(2) 既存の低速通信のままでの処理の高速化
(3) 既存パソコンの継続的な活用による移行容易性確保と、導入・運用コストの削減

6.4 SBC方式の導入効果の検証結果と考察

6.4.1 処理速度のベンチマークテスト結果

本項では、性能の異なる３種類のパソコンでの処理速度の向上効果についての比較を実施している。検証システムの基本構成は図１の通りであり、検証に用いた各種の前提条件

や仕様は以下の通りである。

(1) サーバとして、OS：Windows 2000 Server　Service Pack 2、CPU：Pentium Ⅲ 1GHz、256KB キャッシュデュアル方式、メモリ：2GB SDRAM×2 を用いる。
(2) ネットワークとして低速のモバイル環境を想定し、PIAFS32kb/s を用いる。
(3) ベンチマークテスト用のソフトとして“xl Bench97.xls” を用い、http://www.vector.co.jp/soft/dl/win95/hardware/se063747.html よりダウンロードしている。各テストの詳細内容は、この URL に示している通りである。

処理時間のベンチマークテストを行った結果を表２に示す。全般的に見て、ＳＢＣ方式はＷｅｂコンピューティング方式よりかなりの速度で処理可能なことがわかる。しかし、表２の７項“描画”や５項“移動”において、クライアントパソコン上で起動した場合よりサーバ上で起動した場合の方が処理速度が遅くなっているケースが多い。これは画面の差分情報が大きくなりネットワークを通じて送信するプロセスで時間がかかるためで、ＳＢＣ方式は、変化する画像情報のない情報処理に適用すると効果の高いことがわかる。

6.4.2 保険業務モデルシステムでの検証の結果

代理店の業務システムのうち、通信が多用される保険業務の情報処理プロセスとしては、保険料計算、設計書作成、申込書作成、名寄せ、既契約の参照、帳票の参照、契約規定参照、商品情報参照があげられる。この中で頻繁に利用される保険料計算をモデルシステ

表2　両方式のベンチマークテストの結果

Table2　The results of benchmark test of both methods.

	テスト項目	SBC 方式〔秒〕	Webコンピューティング方式〔秒〕		
		CPU: Pentium 100MHz Memory: 32MB	CPU: Pentium 166MHz Memory:48MB	CPU: Pentium 120MHz Memory:48MB	CPU: Pentium 100MHz Memory:32MB
1	再計算	5	13	15	23
2	業務様式	1	4	5	12
3	グラフ	7	14	20	37
4	罫線	2	9	11	24
5	移動	9	6	7	35
6	ソート	1	6	8	13
7	描画	50	19	22	48

ムとして取り上げ、次の条件に基づいて、6.3.2項に示す(2) (3)の処理速度とコスト削減効果を検証した。

(1) クライアントパソコンとしてOS：Windows95、CPU：MMX Pentium(266MHz)、メモリ：32MB、HDD：6GBを用いた。
(2) 通信回線として56kb/sダイヤルアップ回線を用いた。実質回線速度は44kb/sである。
(3) サーバとして、6.4.1項に示す(1)と同じものを用いた。
(4) 保険料計算ソフトのソフトサイズは22KBであり、計算を開始して結果が出るまでの時間を計測した。

上記(4)の測定結果は、Ｗｅｂベースコンピューティング方式の場合5秒であるのに対し、ＳＢＣ方式では0.5秒であった。

今回はさらに、グループウェアの導入を前提として、ＳＢＣ方式の適用効果を測定した。上記(1)～(3)を測定条件として、グループウェアの起動ソフトのダウンロードが開始から終了するまでの時間を計測した。この起動ソフトのサイズは2MBである。この処理時間として、Ｗｅｂベースコンピューティング方式の場合10分を要したのに対し、ＳＢＣ方式では7秒であった。これらの結果から、本方式について処理待ち時間の大幅な短縮効果のあることがわかる。

なお、ＳＢＣ方式では、印刷についてもＳＢＣサーバ内で処理を行っている。代理店側で利用する各社のプリンタドライバがすべてサーバ内で動作し、印刷が支障なく行われるかどうかの導入事前確認に時間を要することが、この方式の煩瑣な点であることが判明した。

上記の条件下で、ＳＢＣ方式導入の実コストとして、約3万円／パソコンの費用で実現できている。3万円の内訳は、ＳＢＣ方式のライセンス料が1.6万円、その他はサーバ等の対応費用である。ただし、今回の場合、ＳＢＣサーバやパソコンなどは既設の設備を流用しているため、創設費が安くなっている。新規のシステム構築の場合は、数万円～20万円／パソコン程度の費用が必要になる。構築検討の人件費であるＳＩ（システムインテグレーション）費用が、システムの複雑さに応じて、実際に必要となる金額の変動要因の大きな要素である。また、毎年のサーバ等の保守費も、構築費に上乗せで数千円／パソコン程度は見込む必要がある。

6.4.3 大手金融機関における導入検証の結果

大手金融機関へＳＢＣ方式を導入してその効果をさらに究明した。この金融機関の全国数十支店のネットワーク構成は、現在フレームリレー網を用いているが、これをＩＰ－ＶＰＮ網に更改するに当たり、ＳＢＣ方式の導入を実施したものである。

約2,000名の従業員を抱えるこの企業の現状の問題点は以下のとおりである。

(1) 業務で利用するアプリケーションが多く、クライアント端末の設定に稼働がかかる。
(2) サーバへのアクセス頻度が高いため、レスポンスが低下し業務効率が悪い。
(Notes 等を利用しているが非常にスピードが遅い。)
(3) ネットワークの設計・保守・運用に労力と時間をかけており、顧客情報などをクライアント PC に落とすなど、セキュリティ対策にも不安がある。
(4) エンドユーザのレスポンスを確保に必要な帯域が、大幅に肥大化しコスト高になっている。(Web, Mail 等のサービスでアウトソース出来るところはしたい。)

端末パソコン（約 3,000 台）に、ＳＢＣ方式を導入した結果での、コスト削減効果を以下に列記する。

(1) トラフィックの正規化と最小化によりネットワークコストを削減した。
導入前：1,800 万円／月 → 導入後：1,450 万円／月 削減効果額：350 万円／月
(2) ＳＢＣ方式により常時発生していた端末設定作業がなくなった。
導入前：118 万円／月 → 導入後：0 円／月 削減効果額：118 万円／月
(3) 端末の業務アプリケーションのレスポンスを大幅に向上し業務稼働を削減した。
① Notes での全社通知文章の添付ファイル（23KB 相当）を開く時間の短縮効果。
導入前：76 秒／回 → 導入後：10 秒／回 レスポンス向上効果額：165 万円／月
(1 ヶ月短縮時間 22 分／人／月として 1,500 人分を稼働効果に換算)
② Notes の本社実績表の添付ファイル（570KB）を開くまでの時間の短縮効果
導入前：167 秒／回 → 導入後：33 秒／回 レスポンス向上効果額：223 万円／月
(1 ヶ月短縮時間 44.6 分／人／月として 1,000 人分を稼働効果に換算)
(4) ハードディスク（ＨＤＤ）が不要のパソコン端末の耐久期間が、4 年から 6 年にすることによる買い替え費用を削減した。(全端末台数 3,000 台)
年間の費用削減効果：8 万円／台 ×3,000 台 ×1/6＝4,000 万円／年

上記の下線部分を合計すると、年間で約 1.3 億円の削減金額になる。
本件の場合、6.4.2 項に示すようにＳＢＣ方式の端末への実導入費用が約３万円／台必要である。これ以外に新規サーバ構築が必要であることから、回線費用を除く全体の導入費用は約３億円であった。これから、年間の削減額を考慮すると、約 2.3 年で導入費用が回収できることを示しており、ＳＢＣ方式の経済効果の大きいことが証明できた[2][3]。

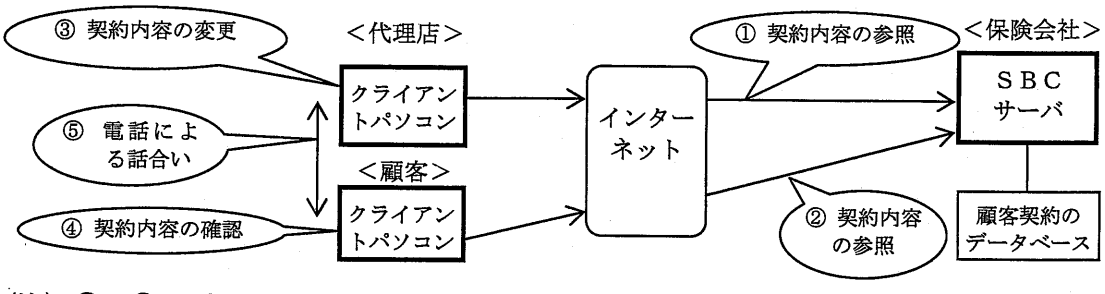
6.5 今後の発展形態

従来の保険会社の業務に対して、森林資源保護の観点から、ペーパーレス化が叫ばれて久しいが、いまだに紙ベースのプロセスが多い[12]。例えば、ある大手保険会社では年間 400 トンの紙を消費しており、本社ビルやシステムセンタに保管されている契約書の紙の量は地下２階分全体を占有するような例があるほど膨大である。今回、ＳＢＣサーバで一元

処理されるというＳＢＣ方式の特徴を利用して、代理店と顧客がサーバ内の新しい契約内容を確認し、打合わせる方法への代理店業務システムの発展形態を検討した。

図３にそのプロセスの概念を示す。契約更新時に代理店がＳＢＣサーバの管理者となり、種々の条件をシステムへ投入して新しい契約内容を作成する。顧客と代理店はそれを画面でチェックして電話で契約交渉を進めることが可能となるものである。顧客が承諾した契約内容は紙へ印刷されることなく、保険会社のデータベースに電子的に保管され、将来にわたり顧客も参照可能となる。なお、この交渉に用いられる電話は、今後、IP 電話が活用されるものと考えられる。この例で示したＳＢＣ方式による遠隔相談と電子的書類保管の機能については、今後、他の各分野に幅広く適用されるものと考えられる[13]。

ＳＢＣ方式はシンクライアント方式（別紙：用語説明(7)）の１つの方式であるが、これ以外にブレードPC 方式（別紙：用語説明(8)）、ＳＣＮ（ストレージセントレックネットワーク）方式（別紙：用語説明(9)）、Sun Ray 方式（別紙：用語説明(10)）が新たに普及している方式がある。ＳＢＣ方式だけではない、これらの方式の特長に応じた、企業での業務システムへの適用が今後の発展形態となる。



(注) ①～⑤はプロセスの順序を示す。　Note：①～⑤ shows the order of the process.

図3　ペーパーレスシステムのプロセス概念図

Fig.3　The process concept chart of the paperless system.

6.6 まとめ

本論文では、“施設系”であるＬＡＮ／ＷＡＮ系コンピュータシステムへのセキュリティ対策の１つの方法として、ＳＢＣ方式の適用性を検討した。ベンチマークテストや保険代理店のモデルシステムによる検証により、セキュリティの向上と処理の高速化が経済的に実現できることを示している。また、ＳＢＣ方式導入が、一般企業の支出できる値ごろ感である約３万円程度で、既存設備を利用して実現できることが判明した。さらに、ＳＢＣ方式を大手金融機関に導入した結果、新規構築においても、約 2.3 年で導入費用が回収でき

る経済効果のあることが証明できた。

このような事例は、顧客情報や売上げ情報などの情報漏えいや不正利用対策を、経済的に実現したい企業にとって、参考になるものと考えられる。また、ＳＢＣ方式の特徴を生かしたペーパーレスシステムは、各方面での広範な利用により、今後の森林資源保護の一助になるものと期待している。

今後の課題として、各種のシンクライアント方式（別紙：用語説明(7)）の特長に応じた業務システムへの適用があげられる。

なお、本章で述べているＳＢＣ方式を適用したセキュリティ対策は、第９章の（参考）に示すように、3,000 ID という金融機関での大規模な導入で実績をあげている。

[参考文献]

[1] MetaFrame ユーザー事例集, http://www.citrix.co.jp/solutions/casestudy/ index.html, June, 2003.

[2] MetaFrameXP 実践ガイド, OPEN DESIGN Books, ＣＱ出版社, 東京, pp. 20-23, 2002.

[3] MetaFrameXP 初級管理者ガイド, 毎日コミュニケーションズ, 東京, pp. 25-30, 2002.

[4] メタフレームとは, http://www.pbsystems.co.jp/products-page-meta-kokon.htm, May, 2003.

[5] Server-based Computing, 日経コンピュータ, 東京, pp. 183-188, 2002.

[6] 印丸哲, “アプリケーション管理技術の最新テクノロジー②”, コンピュータ＆ネットワーク LAN, 東京, pp. 16-22, 2002.

[7] 西郷健, 奥野克仁, “アプリケーション管理技術の最新テクノロジー①”, コンピュータ＆ネットワーク LAN, 東京, pp. 10-15, 2002.

[8] 松田利夫, “古き（レガシー）を活かす新しい ASP の潮流”, コンピュータ＆ネットワーク LAN, 東京, pp. 5-9, 2002.

[9] MetaFrame の必要性と全機能一覧, http://www.kcs.ne.jp/syouhin/citrix/mfrole0.htm

[10] シンクライアントシステム 基礎講座, http://www.keyman.or.jp/search/30000031_1. html, Oct. 2001.

[11] 大塚英明, 東京損害保険代理店協会法制委員会, “損害保険代理店委託契約書コンメンタール （中）”, 東京損害保険代理業協会, pp. 9-12, pp. 100, 2002.

[12] 日本損害保険協会における環境活動について, http://www.jqa.jp/06manage/15_iso_news/ 32/06.html, June, 2003.

[13] 岡田潤之, 河東 勇, 清水茂樹, “サーバベースコンピューティング（SBC）ソリューション”, 三菱電機技報, Vol. 77, No. 4, 2003.

第7章　低コストの国際業務システムの提案とその考察

7.1 概要

国際通信のコストが高いことから、「日本と海外拠点をＬＡＮ／ＷＡＮ接続した全社的な業務システム」の実現は一部の企業に限られてきた。本章では、これを低コストで実現する１つの手段として、通信コストの安いインターネットＶＰＮ（別紙：用語説明(12)）と、伝送される情報量の少ないＳＢＣ方式（別紙：用語説明(1)）を組み合わせる方式を提案する。

実際の業務システムへ、この方式を適用して検証した結果、簡単な業務について利用可能であることが判明したのでその内容を紹介する。また、本章では、本方式の通信品質を改善させるための方法の概念を提起し、その内容を論じる。さらに、本システムの企業活動における、より創造的な利用用途について考察する。

本章では、7.2項で現状の問題点と過去の研究動向を整理している。7.3項で本研究のモデルケースとした業務システムとその必要要件を示し、今回提案する方式による技術的実現方法について論じている。7.4項で本システムの設計内容を示す。7.5項で本方式の実用性についての検証テストを、ローカルテストと実地テストに分けて実施したので、そのテスト方法と結果および考察を紹介する。また、7.6項で本方式の通信品質の改善方法の概念を説明し、その効果に対する評価を実施している。さらに7.7項では情報文化学的観点からの利用用途を情報共有の分類にもとづいて考察し、より創造的な企業活動への適用などについて述べている。

7.2 現状の課題と研究の動向

企業活動の国際展開が進む中、日本と海外拠点との情報通信はますます重要になっている。企業においては、海外拠点のクライアントパソコンからＬＡＮ／ＷＡＮを介してシームレスに日本のサーバにある業務システムを利用したいとするニーズが高い。

これに対応するために、通信事業者から、フレームリレー、国際仮想専用線（ＩＰ-ＶＰＮ）のようなＬＡＮ間接続のための国際通信サービスが提供されている。しかし、料金が高いことから高コストに見合う業務への適用に限られており、一般企業において、国際的なＬＡＮ／ＷＡＮ接続が十分普及していないのが実情である[1]。

従来のクライアントサーバ（ＣＳ）方式（別紙：用語説明(3)）を用いた業務システムでは通信回線で伝送される情報量が多く、通信コストが高くなるという問題があった[2]。最近、Ｗｅｂコンピューティング方式（別紙：用語説明(2)）を用いて回線への負荷を軽減しようとする動きもある。しかし、既存システムをＣＳ方式からＷｅｂコンピューティング方式へ再構築するための費用と時間がかかるという問題がある。このことから、この方式の適用は新規システムにとどまるケースが多く、既存システムの更改も活発に行われてはいない。

前述の問題を解決するため、本章では、コストの安いインターネットＶＰＮと伝送される情報量の小さいＳＢＣ方式を組み合わせる方式を提案する。

従来、このような方式へのニーズは大きいものの、実現した事例は極めて少なく、あまり普及はしていない[2]-[4]。これは、主にインターネットＶＰＮの国際区間において、しばしば伝送遅延揺らぎやパケットロスのような、通信品質の劣化が起きることが大きな理由の一つである[5]。このことから、この品質劣化の影響を少なくする方法の検討は有意義である。

本論文では、複数経路を利用するマルチホーミング技術（別紙：用語説明(14)）を用いて、パケットロスや伝送遅延揺らぎの影響を少なくする方法の概念を提案する。従来、西園や林らによりインターネットを用いた複数経路のデータ伝送方式の検討が行われてきた[6][7]。この研究ではネットワーク品質の異なる複数経路へパケットを分配して伝送する場合の、スループット特性の検討が主に行われている。また、堀池らにより、複数の経路にIPパケットを拡散して通信することによる、セキュリティ向上方法の研究も行われている[8]。しかし、従来の研究では、インターネットＶＰＮを複数経路で利用した通信品質の改善の検討は行われていない。また、現状のインターネットＶＰＮゲートウェイ装置でも、実現されているものは見当たらない。このことから、本章で示す通信品質向上の提案は、新しい視点を提起するものであり、意義のあるものと考えられる。

7.3 必要要件と実現方法の技術検討

7.3.1 モデルケースとしたシステムの要件

本論文では、ある損害保険会社で実際用いられている海外業務を行うシステムを事例としている。現状では、国内のセンタと海外拠点を接続する専用ネットワークはない。海外拠点からeメール、FAX、電話で寄せられた情報をもとに、日本本社で専任のオペレータが、必要なデータベースメンテナンス業務を行っている。このような実施方法は極めて煩雑であり、また、入力されたデータベースのチェックを海外拠点でリアルタイムに行えないという問題もある。

今回、センタのサーバにあるデータベースの様式を海外拠点のパソコンに次々に表示させて参照し、その様式へのデータの入力や修正を行う業務について、後述する7.5.2項のローカルテストの結果に基づき検証の対象業務とした。このモデルに対して、実現すべき要件は以下のとおりである。

要件(1)：利用に耐えうる安価なネットワークを採用し、ランニングコストを抑えること。
要件(2)：既存の業務システムへの変更コストを少なくして、海外拠点から本社サーバのアプリケーションを利用できること。
要件(3)：成りすましや盗聴を防止できる安全な通信が確保できること。

要件(4)：このモデルの最長距離である東京とロンドン間において、我慢できるレベルで業務システムが使えること。

7.3.2 インターネットVPNの適用性検討

前項の要件(1)を満たすために、本論文では、安価であるが、品質面、安全面で問題のあるインターネットＶＰＮの適用を前提として、前項の要件に対して以下の対策をとることとした。

① 要件(1)への対策の一つとするべく、SLA（Service Level Agreement）（別紙：用語説明(13)）により、通信品質を保証しているISP（Internet Service Provider）をアクセスポイントとして採用する。これにより、Tier1と呼ばれる高速・広帯域バックボーンに直結されたインターネット網の高い通信品質が利用可能となる。

② 要件(2)への対策の一つとするべく、ＶＰＮゲートウェイにグローバルアドレスを設定し、既存プライベートアドレスとデータを、このグローバルアドレスをヘッダとしてカプセル化する。これにより、既存のプライベートアドレスをそのまま利用できるようにする。

③ 要件(3)への対策とするべく、インターネットＶＰＮゲートウェイにおいて多用され、頑強なセキュリティ性能を有するIPSecプロトコル（別紙：用語説明(15)）を適用する。今回はESPトンネリングモードと、3DES暗号を用いてＶＰＮゲートウェイ間を接続するとともに、ＶＰＮゲートウェイ装置の認証も併せて行うこととした。

7.3.3 SBC方式の適用性検討

従来から用いられているクライアントサーバ（ＣＳ）方式（別紙：用語説明(3)）の業務システムに対して、要件(1)、(2)への対策の一つとするべく、ＳＢＣ方式についての適用性を検討した。これは、クライアントパソコンとネットワークを介したサーバとのやり取りを、「マウスクリック」、「キーストローク」、「画面遷移の処理」に限ることで、通信回線で伝送される情報量を少なくできる特長に着目したためである[9]-[11]。

ＣＳ方式では、業務ソフトはAPサーバ内にあり、実行の都度クライアントパソコンのハードディスクへダウンロードされて処理が行われる。処理の都度ダウンロードがードが発生するため、処理速度がネットワークのスループットに依存する。一方、ＳＢＣ方式では、業務ソフトはAPサーバとＳＢＣサーバ内にあり、クライアントパソコンには、業務ソフトはダウンロードされず、情報処理もＳＢＣサーバ内で実行され、その実行結果の画面情報がクライアントパソコン側に送出される。この仕組みの適用により、既存のアプリケーションやデータベースに大きく手を加えることが不要となり、7.3.1項の要件(2)への対策の一つにすることができる[12][13]。

本章で評価対象のモデルとしたシステム構成を図1に示す。この構成で7.3.1項の要件(4)をどこまで満たすことができるかの検証試験を、7.5項で行うこととしている。

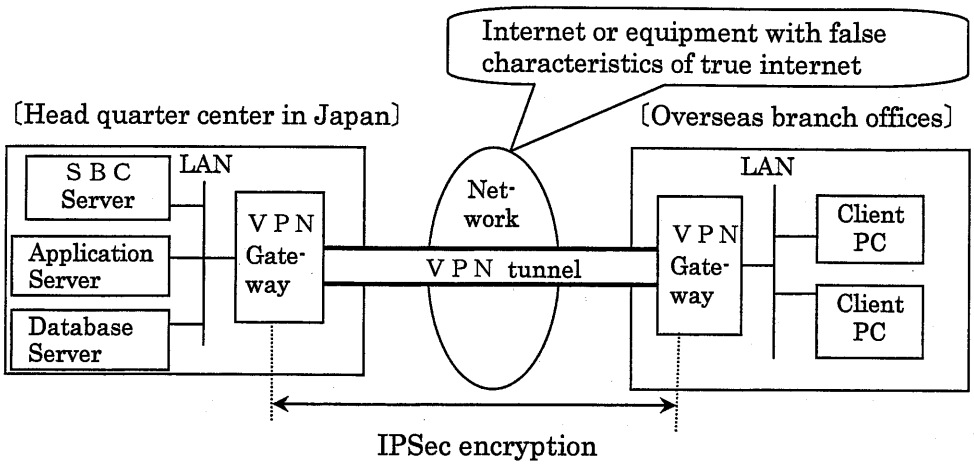


図1　評価モデルシステムの構成

Fig.1　The composition of the valuation modeling system.

7.4 SBC方式を用いた国際業務システムの方式設計

7.4.1 導入システムの基本構成

国際業務のシステムについて、図２に既存のシステム構成を、図３に目標とするシステム構成をそれぞれ示す。図３の太線の部分が今回の主な新規構築部分である。大手町のＩＣカードプラットフォームを新規にアウトソーシングして、このプラットフォームがすでに有しているインターネットＶＰＮを利用した点に特徴がある。本社ビルにＳＢＣのシステムを用いて、海外 22 拠点から本社サーバ（業務システム）を操作できるシステムを構築する。支店間通信は直接行わない。

海外 22 拠点のクライアント端末にＩＣカードプラットフォームのクライアントソフトをインストールし、インターネット～ＩＣカードプラットフォームのサーバ（大手町プラットフォーム）間の通信を IPSec 暗号化（別紙：用語説明(15)）する。

本社に新規導入するＳＢＣサーバ側とＩＣカードプラットフォーム側の IP アドレスは、ＩＣカードプラットフォーム側の指定アドレス 10.63.16.X/24 を使うこととし、既存ＬＡＮへ接続する IP アドレスは既存のプライベートアドレスを用いている。

ただし、ＩＣカードプラットフォーム指定アドレスである 10.63.16.X/24 は既存営業拠点にて使用中のため、既存国際部ＬＡＮからＳＢＣサーバへ接続する場合は NAT アドレスを利用することとしている。ここで用いる既存のアドレス体系を表１にまとめて示す。

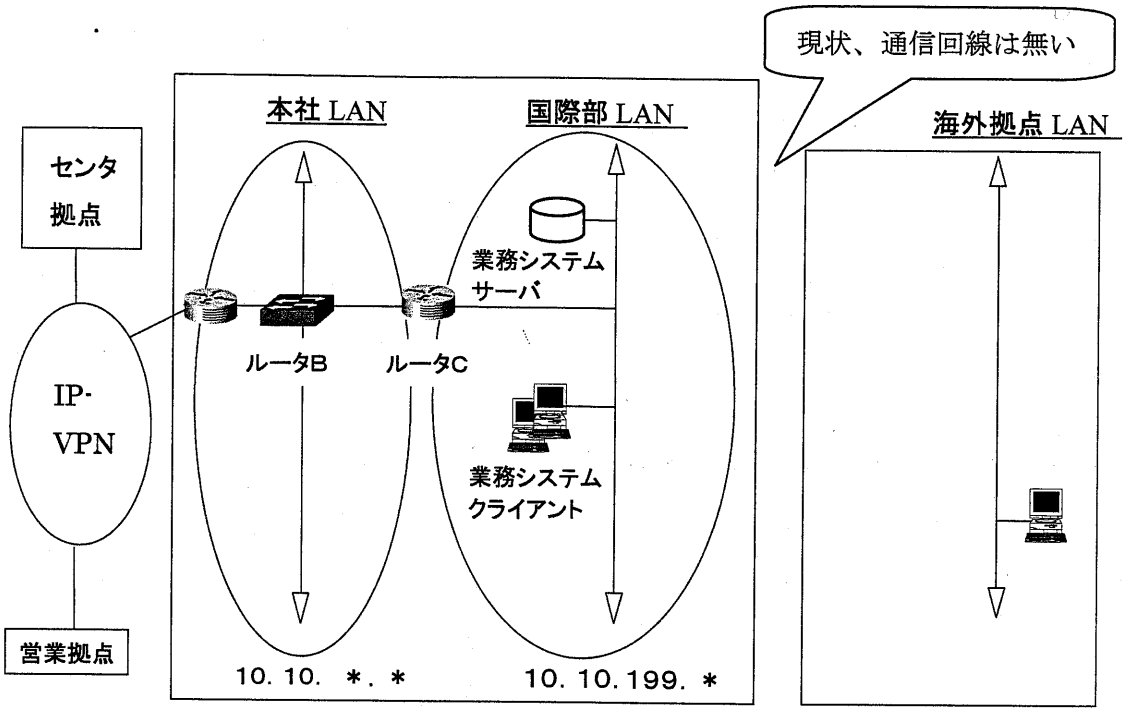


図2 既存システムの構成

Fig.2 The composition of existing system.

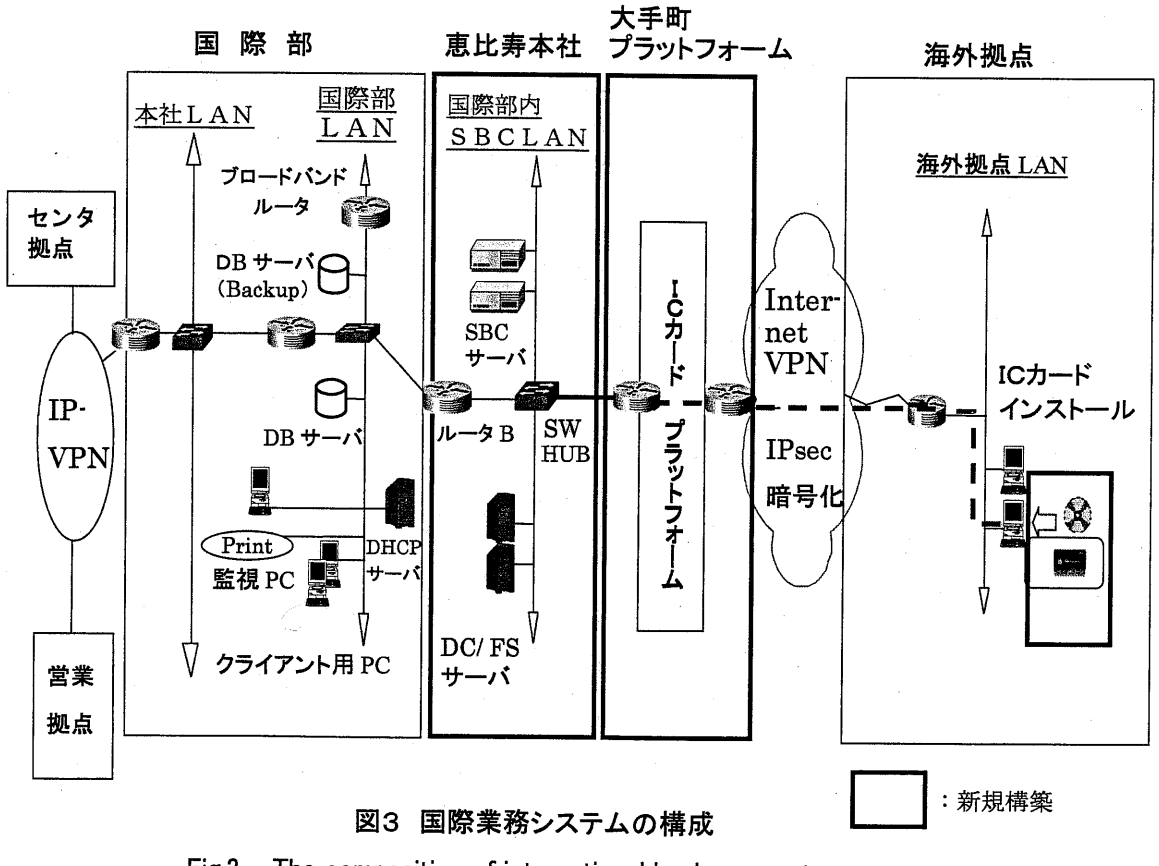


図3 国際業務システムの構成

Fig.3 The composition of international business system.

表1　既存の IP アドレス一覧

Table 1　The existing Internet Protocol addresses list.

IP アドレス	用途	ホスト名	備考
10.10.199.0	ネットワーク		
10.10.199.1	ローカル・ルータ	KGRT01	小容量ルータ
10.10.199.2	ブロードバンド・ルータ	KGRT02	汎用品
10.10.199.21	DB サーバ(D 社)	KGSV01	
10.10.199.22	DB サーバ(メイン)	KGSV02	
10.10.199.23	DB サーバ(C 社)	KGSV03	
10.10.199.24	ローカル DNS(Primary)	KGSV04	DHCP サーバ
10.10.199.65	プリンタ	KGPR01	汎用品
10.10.199.99	Work Group PC		
10.10.199.129～254	クライアント用 PC(DHCP)	KGCL～KGCL25	
10.10.199.255	ブロードキャスト		

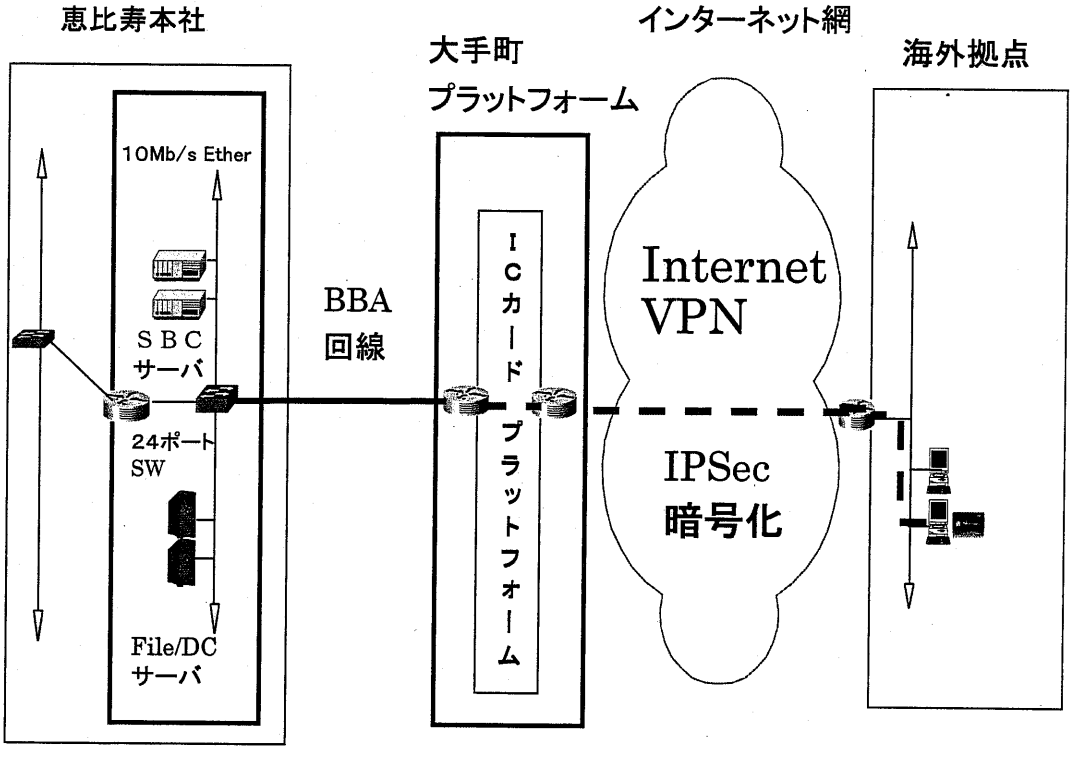


図4　ネットワーク構成図

Fig.4　The figure of network composition.

ＬＡＮの方式は Ethernet であり、通信ネットワークではシンプルで管理容易な、Static のルーティングを用いている。ＳＢＣサーバとＤＢ間はＳＱＬ通信（1433）（別紙：用語説明(17)）を利用している。

また、管理端末とＳＢＣサーバ間は、ＳＢＣ方式で用いられるＩＣＡ通信（別紙：用語説明(11)）（TCP:1494、UDP:1604）を用いている。海外クライアントとＩＣカードプラットフォームゲートウェイ間は、ブロードバンドルータが標準的に具備している、IPSec（1443）を適用している。

ＩＣカードプラットフォームサーバがある大手町プラットフォームから本社ビル間はＢＢＡ（ブロードバンドアクセス）回線を利用している。帯域は 10Mb/s、接続方式は 10Base-T(Ether)である。また、ＩＣカードゲートウェイーＳＢＣサーバ間の通信はＩＣＡ通信を適用している。図４にこれらの諸元を設定したネットワーク構成を示す。

7.4.2 システム全体の設計内容

7.4.2.1 SBC方式を適用するための設計内容

ＳＢＣ方式は、ハード・ソフト一体型の規格化サーバユニット方式により、この方式の利点を最大に引き出して、実現するものである。この方式では、アプリケーションをＳＢＣサーバ上で動作させ、クライアントの入力をＳＢＣサーバ上のアプリケーションへ送信し、ＳＢＣサーバ上で動作しているアプリケーションの画面（差分）をクライアントに返信する。

本システムでは海外のクライアントに対しての作業を可能な限り排除し、サーバをデータセンターで一元管理することにより、管理負荷の削減を考えている。ＳＢＣ方式を使用することにより、以下に示すような特徴を生かしたシステムを構築する。

① クライアント毎にアプリケーションをインストール（アップデート）する手間を省くことができる。
② ＳＢＣサーバ、クライアント間を流れるデータが少ない。
③ クライアントにかかる負荷が小さい。

上記の特長点に加えてハード＆ソフト一体型のサーバユニットと独自ツールを利用することにより、ＳＢＣ方式のメリットを最大限に活用可能としている。

サーバ群をＳＢＣサーバ２台、ドメインコントローラ（別紙：用語説明(21)）兼ファイル（ＤＣ／ＦＳ）サーバ２台で構成し、ＳＢＣサーバのセグメントと業務システムサーバのある国際部のセグメントはルータ経由で接続し、不必要な通信に制限をかける。また、ＳＢＣサーバのセグメントのIPアドレス体系が社内ネットワークのIPアドレス体系に干渉しないようにするため、ＳＢＣサーバから業務システムサーバへの通信に対してルータで静的 NAT 変換（別紙：用語説明(17)）を行うこととする。図５にこの構成を示す。

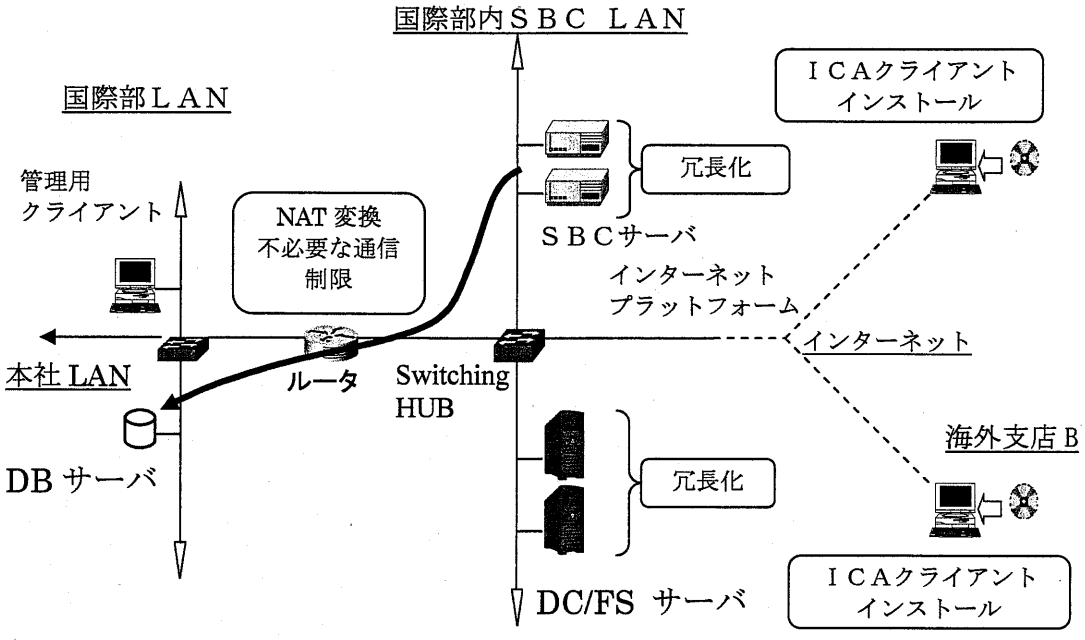


図5　冗長化構成とLAN間トラフィック制御

Fig.5　The dual composition and Traffic control between LANs.

国際部のセグメントに、管理用クライアントPCを用意してネットワークの管理を一元実施できるようにしている。

ドメインコントローラ兼ファイル（ＤＣ／ＦＳ）サーバに使用ユーザを登録し、業務システムを使用するための認証に使用する。また、ユーザごとの設定値等のユーザプロファイルはＤＣ／ＦＳサーバ上に保存することで、２台のＳＢＣサーバのどちらを使用しても同じプロファイルが適用されるように設計している。

ＳＢＣサーバ２台でのロードバランスを行い、またＤＣ／ＦＳサーバは Co－Standby Server を使用することでユーザデータ、設定を含めた冗長化を確保している。

7.4.2.2 ネットワークの構成

本システムでは、ＳＢＣサーバ及びドメインコントローラ兼ファイル（ＤＣ／ＦＳ）サーバを１つのＴＣＰ／ＩＰセグメント上に構築している。これは海外からの接続を受けるため、既存セグメントと別セグメントにすることでセキュリティの確保をするためである。また、ＩＣカードプラットフォーム経由で接続させる機器には指定されたIPアドレスを振る必要があり、そのアドレスと既存アドレスが影響しないようにするためである。図６にこの構成を示す。

既存セグメントとＳＢＣサーバセグメントはルータで接続し、ルータにはＡＣＬ設定（別紙：用語説明(19)）を行い不要な通信は不許可としている。本システムではＳＢＣサーバから

業務システムのＤＢサーバへＳＱＬ通信（ポート 1433）のみ必要となるため、２台のＳＢＣサーバから既存の２台の業務システムのＤＢサーバへの通信とその応答のみ許可としている。

またＳＢＣサーバ２台はルータに静的 NAT（別紙：用語説明(17)）の設定を行い、既存セグメントからの接続は静的 NAT で割り当てた IP アドレスを使用している。

不用意な通信を防ぐため、このルータにはデフォルトゲートウェイの設定を実施していない。ＳＢＣサーバのセグメントには、海外クライアントからのＳＢＣサーバへのＩＣＡプロトコルでの通信（別紙：用語説明(11)）と、ユーザプロファイルやユーザデータ等のＳＢＣサーバからファイルサーバへの通信が主に流れるようにしている。

ＩＣＡプロトコルの通信は、検証試験により１名に付き約 30kb/s であることがわかっている。今回の最大接続数は 30 ユーザなので 900kb/s が必要である。ＳＢＣサーバとファイルサーバ間の通信はファイルの送受信なので早いほど好ましいが、本システムでは事前検証の結果、保存されるファイルは大きくても 1MByte 程度と予想されている。これにより既存セグメントと同様の、100Base-TX での接続で十分と判断し、100Base-TX のスイッチによる接続としている。

ただし、ＤＣ／ＦＳサーバではネットワークを利用して２台でディスクのミラーを行う方式を採用しているため、ミラー用のネットワークとしてＤＣ／ＦＳサーバ２台をクロスケーブルで接続し、専用のネットワークを構成している。

既存セグメントでは 100Base-TX を基本としており、ＳＢＣセグメントも上記から 100Base-TX となる。したがってルータは 100Base-TX での接続ができる機種としている。

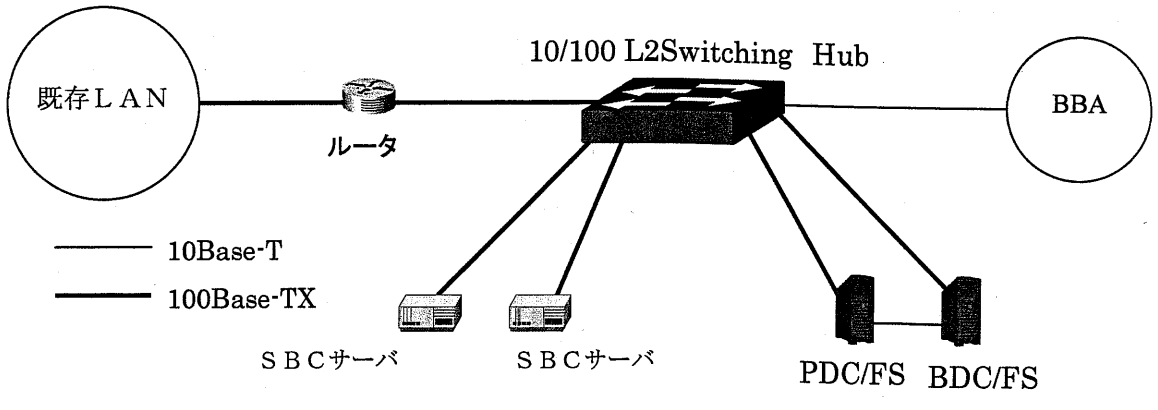


図6　ネットワーク構成

Fig.6　The network composition between LAN and BBA.

事前検証では、１ユーザあたり 50kbyte 程度のＳＱＬデータ（別紙：用語説明(18)）が断続的に流れるのみであり、パケットの流通量も最大でも 50pps 程度であることが判明している。最大 30 ユーザが接続するとして 50×30=1.5kpps である。このため本システムではカタログスペックが 20kpps であるルータを選択している。

7.4.2.3 SBCサーバの構成

ＳＢＣサーバとして、クライアント PC に対してターミナルサービスを提供する機能がプリインストールされたアプライアンスサーバを利用している。

本システムでは、OS に Windows2000Server を採用し、Meta Frame1.8 SP3 に独自ツールを加えたものを使用している。

今回、ＳＢＣサーバの“Load Balancing Services オプション”を使用することで負荷分散を実現し、１台にかかる負荷を抑えるとともに冗長化を実現している。

事前テストにおいては PentiumⅢ933MHz×２の環境で、通常作業時の１ユーザのＣＰＵ使用率最大が約４％未満であった。本システムでは、最大 30 ユーザが同時使用することを想定していることから、ＣＰＵ使用率は、4%×30=120%である。本システムでは PentiumⅢ1GHz の約 1.5 倍以上の処理能力が期待できる Xeon2.4GHz×2 を選択している。この場合、30 ユーザ同時使用時に 80%となり、ロードバランスを考慮しない状態で１台のサーバに接続が集中した場合でも、ＣＰＵ使用率が 80%未満に抑えられることが期待できる。

メモリについては、事前テストにおいて、１ユーザ接続時に最大約 30MB のメモリ使用が確認できている。この結果から、１台のサーバに最大 30 ユーザ接続した場合を想定し、システム用のメモリを 256MB と仮定すると 256MB+30MB×30=1156MB であり、このときの使用率が 80%未満になるよう考えると、1.5GB 必要になる。本システムでは、拡張性を考慮し、2GB の容量を準備している。

ＨＤＤ（ハードディスク）の容量は、システムの容量を約 8GB、ユーザプロファイルの容量を約 10MB と想定した場合でも 10GB で十分と考えられるが、導入当時の入手性とコストパフォーマンスから 32GB とし、イメージバックアップ用として同容量のＨＤＤをもう１台用意している。

7.4.2.4 ドメインコントローラ兼ファイル(DC／FS)サーバの構成

アプリケーションを使用するユーザの個人認証を行うため、ドメインコントローラを使用している。海外からの接続ということを考慮し、セキュリティ強化のため認証のためのユーザは本システム専用に登録する。そのため、ドメインは本システム用に新規に構築を行う。また、ドメインコントローラ（別紙：用語説明(21)）は、冗長化と負荷分散のため PDC，BDC の２台構成とする。

ドライブをｃ：、ｄ：とし、ｃ：ドライブはシステムデータ用、ｄ：ドライブはユーザデータ用とし、共有ファイル等のファイルサービスを提供する。また、Co-Standby Server を使用することでこのファイルサービスに冗長化を付加している。

仮想的なサーバ名を用意し、そのサーバ名でアクセスすると、Co-Standby Server の機能により、主となるサーバに問題があった場合でも副サーバに自動的にアクセスし、冗長化が実現するように設計している。また、各々のｄ：ドライブを同様に Co-Standby Server の機能で定期的にミラーリングし、ファイルの冗長化も実現している。

本方式では負荷分散のため、そのときの状況により２台のＳＢＣサーバのどちらかにログインすることになる。どちらのＳＢＣサーバに接続しても同じユーザプロファイルが使用されるように移動プロファイルを利用している。また、移動ユーザプロファイルでは、ログオン、ログオフ毎にファイルコピーがされるので、設定データ以外の個人データの保存場所として共有フォルダを用意し、その下にユーザ毎のフォルダを用意、ログオン時にｚ：ドライブとしてマッピングする。移動ユーザプロファイル領域およびマッピングする共有フォルダは Co-Standby Server により冗長化されているｄ：ドライブに作成する。

今回使用するサーバ機種は省スペース性を重要視し、ハードディスクドライブが最大で２台のものを選択している。そのためハードディスクの今後の増設を見込むことが難しいため、ユーザデータ用のドライブは今後のデータの増加を考慮に入れ、実験当時の手に入る最大の 72GB としている。また、システム領域用のドライブは 10GB で十分であるが、コストパフォーマンスに優れる 32GB としている。

7.4.2.5 クライアントからのアプリケーションの利用

クライアントからＳＢＣサーバ上のアプリケーションを利用する方法として、サーバ上のデスクトップ環境をそのまま利用する方法と、アプリケーションの画面のみ開いて、指定したアプリケーションのみを使用する方法がある。

本システムでは、デスクトップ環境は使用せず、セキュリティの高いアプリケーションのみを使用する方式にしている。この場合、シームレスウィンドウ機能により、ローカルマシン上のアプリケーションを使用している場合と同じように表示され、ユーザにＳＢＣサーバ上のアプリケーションであることを認識させないようにしている。また、想定したアプリケーション以外を不用意に利用されることを防ぐことができる。

本システムではＳＢＣサーバ上で業務システムクライアントソフトを公開アプリケーションとして登録し、その公開アプリケーションをＩＣＡクライアントソフトの Program Neighborhood により選択、起動できるようにする。本システム公開時では、業務システムクライアントソフトを含め、表２に示すアプリケーションを公開している。

表2 公開しているアプリケーション

Table 2 The applications that have been opened for the inside jobs.

公開名	主な用途	コマンドライン
業務システム Client	国際業務支援アプリケーション	"C:¥ProgramFiles¥Microsoft Office ¥ART¥Office¥MSACCESS.EXE" "c:¥kgnet¥KaisaCS.ade"
My Documents	サーバ上に保存したファイルをクライアントにダウンロードする。	"C:Program Files¥APP_ explorer.exe" Z:¥
Net101	イントラネット閲覧	"C:Program Files¥Internet Explorer ¥IEXPLORE.EXE"
Share	海外ユーザの共通ファイル保存場所	"C:Program Files ¥APP_ explorer.exe""X:¥"

デスクトップ上では起動用のショートカットを作成しており、ＩＣカードプラットフォームの接続を確認するとともに、ＳＢＣサーバと接続が可能なことを確認して Program Neighborhood を起動するようにしている。これにより、ＩＣカードプラットフォームのパスワード入力、接続確立までのタイムラグによる Program Neighborhood のタイムアウトを防いでいる。

また、Program Neighborhood の設定により、アプリケーションセットマネージャの選択や新規作成、カスタムＩＣＡコネクションの新規作成メニューが表示されないようにしている。これにより、ＳＢＣサーバ上以外のアプリケーションの使用を防ぐことが可能になる。これらの設定はインストール時に設定されるように、あらかじめインストール時に設定されるようにファイルを構成しておくようにしている。

ＩＣカードプラットフォームの仕様により、ＳＢＣの代替えアドレスの設定が必要な場合があるので、インストーラ構成を２種類用意し、クライアントの設定によりインストールするインストーラ構成を選択する事としている。

印刷は、公開アプリケーションから直接行うことはせず、保存したファイルを公開アプリケーション「My Documents」を使用してクライアント PC にダウンロードし、必要に応じて印刷を行うようにしている。　また、不要なアクセスを制限するためサーバの c:¥,d:¥,e:¥ドライブが表示されないようにグループポリシーを適用し、各ドライブのルートにあるファイル、フォルダを隠し属性に設定している。

アプリケーション起動時にＳＢＣサーバへのログインを必須とし、この認証に前項で説明した、ドメインコントローラ兼ファイルサーバ上のユーザを使用することで個人認証を実現し

ている。クライアントでＳＢＣサーバ上のアプリケーションを使用する時に、透過的にクライアントのドライブを使用できるようにするため、ドライブマッピングと呼ばれる機能を使用している。また、各ユーザのデータ格納のためファイルサーバ上のユーザ専用フォルダをマッピングしている。ＳＢＣサーバ上のアプリケーション使用時のドライブは図７のようになる。

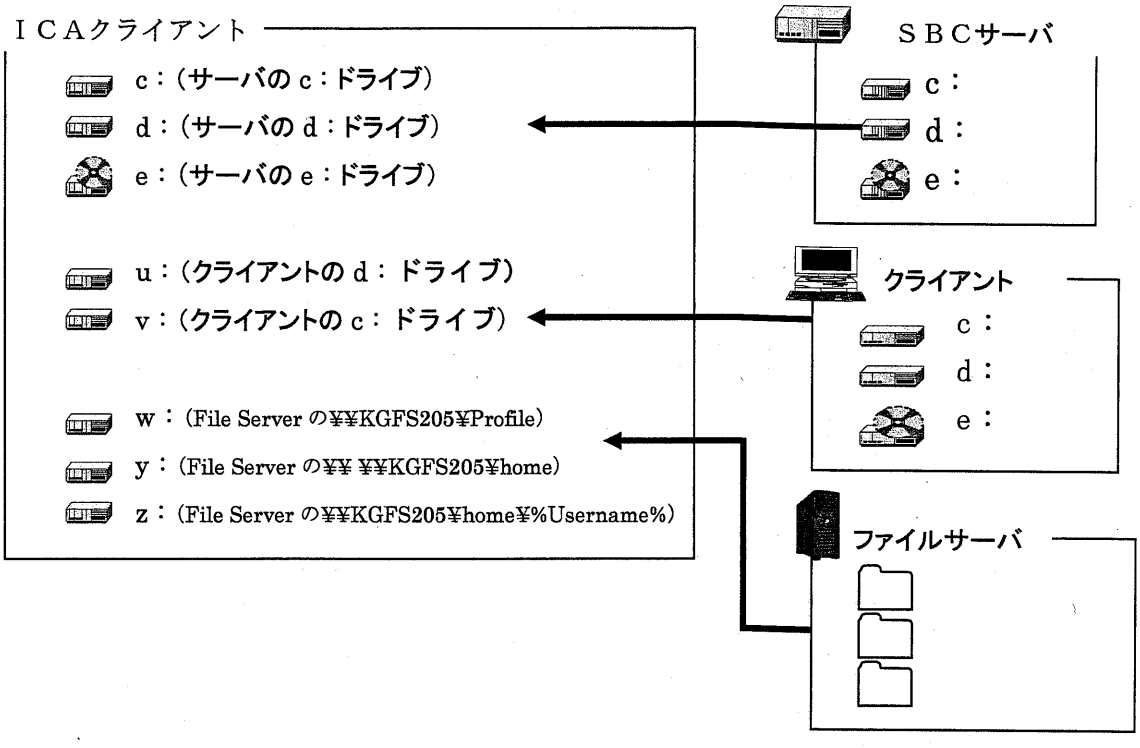


図7　アプリケーション使用時のドライブの構成

Fig.7　The composition of PC drives when the application is used.

7.4.2.6　運用方法の考え方

ＳＢＣサーバは安定運用させるため定期的にリブートを行う。過去の実態から、１週間に１度のリブートとし、リブートは自動的に行われるように各サーバで設定している。

使用者が各国にいることから未使用時刻を特定することが難しいため、本システムでは実際に運用を行う日本の事情に合わせることとしている。サーバに関係なくファイル保存時、ログイン時等のタイムスタンプを統一するために各サーバの時刻を合わせるようにしており、時刻はサーバを設置する日本時間を基準として定期的に自動的に合うように設定している。

ＳＢＣサーバのセグメントと既存セグメント間の不要な通信を抑えるため、まず既存のタイムサーバとＳＢＣサーバの時刻の同期を行い、その後ＳＢＣサーバとＳＢＣサーバセグメント

にある他の各サーバの時刻を同期する方式にしている。

ＳＢＣサーバと既存タイムサーバの時刻の同期には、既存のシステムで使用しているＮＴＰプロトコル（net time/sntp コマンド）（別紙：用語説明(20)）を使用している。またＳＢＣサーバとＳＢＣサーバセグメント内の時刻同期には Windows 標準の net time コマンドを使用している。

7.4.3 ICカードプラットフォームを利用するための設計

ＩＣカードプラットフォームとはＩＣカードを利用したハイセキュアな認証、接続サービスである。ＩＣカードプラットフォームを利用することで、クライアントとＩＣカードプラットフォームセンター間で IPSec 暗号化を形成し、インターネット経由での高速で安価な通信を安全に行うことが出来る。また、接続には専用ＩＣカードを利用するため、成りすましによるアクセスを防ぐことができる。

ＩＣカードプラットフォームでのサービスは、クライアント、ＩＣカードプラットフォーム、国際部内ＳＢＣ－ＬＡＮで構成される。ＢＢＡのＩＣカードプラットフォーム側にルータを設置し不要な通信に制限をかけることにより、ＩＣカードプラットフォーム－国際部内ＳＢＣ－ＬＡＮ間のセキュリティを確保している。国際部内ＳＢＣ－ＬＡＮのアドレス体系は 10.63.16.0/24 としている。しかし、ＩＣカードプラットフォームの仕様により、クライアントが 10.*の IP アドレスを持つ場合は、クライアントが認識する国際部内ＳＢＣ－ＬＡＮの IP アドレス体系として 172.16.16.0 が仮想的に与えられるようにしている。

このため、クライアントの設定に２種類の設定が必要になり、クライアント側のインストーラを２種類用意することで対応している。

クライアントから国際部内ＳＢＣ－ＬＡＮへ接続しようとすると自動的に認証が開始され、ＩＣカードプラットフォームへの IPSec 暗号化が確立する。

ＩＣカードリーダは原則としてＵＳＢ接続の物品を使用し、ＵＳＢポートが無い等の理由があるときのみ PC カードタイプを利用することとしている。ＩＣカードプラットフォームの対象クライアント環境は以下のとおりであり、今回はこのクライアント環境に適合させている。

OS：Windows 98／Windows Me／Windows 2000 Professional(SP2)
　　Windows ＸＰ Home Edition／Professional Edition（すべて日本語版のみ）
CPU：Intel(R)Pentium(R)プロセッサ 266MHz 相当以上
メモリ：64MB 以上　　空きハードディスク：25MB 以上
その他：CD-ROM ドライブ要、USB ポートまたは PC カードスロット要

7.4.4 BBA(ブロードバンドアクセス)回線を用いた設計

ＢＢＡ回線は、高速広帯域なアクセス回線を低廉な料金で提供する回線サービスであり、イーサネットによるビル間伝送を低コストで実現できることと、異拠点間において同一ＬＡＮ環境を実現することを目的に、この通信サービスを選択している。

本システムでは、ルータ等の機器をなるべく除外した簡易な構成にするため、本社ビルと大手町プラットフォームビルをＢＢＡブロードバンドアクセスーイーサ型で接続している。また、約３０ユーザの通信が主な通信となるため、帯域としては 30kb/s×30=900kb/s 程度必要となる。今後の人数の拡張を考えてもコストが最も低い 10Mb/s で十分であることから伝送用契約者回線群（ビル間伝送）に 10Mb/s を選択し、さらに契約者回線（ポート）に 10BASE-T を選択している。

7.5 検証試験内容とその結果への考察

7.5.1 検証試験の進め方とシステム諸元

今回、7.3.1 項に示す業務に対してインターネットＶＰＮ（別紙：用語説明(12)）を擬似ネットワークに置き換えて試験するローカルテストを行った。次に、この結果に基づき、ロンドンのクライアントパソコンから東京のセンタのサーバに対して、実際のインターネットＶＰＮを介した実地テストを実施した。

今回、7.3.3 項の図１の構成に用いたシステムの諸元は以下のとおりである。

(1) クライアントパソコン：CPU；PentiumⅢ、700MHz、メモリ 196MB、OS；Windows 2000 professional
(2) ＳＢＣサーバ：CPU；Xeon 2.4GHz×2、メモリ 2GB、OS；Windows 2000 professional、同時接続数 30
(3) ＶＰＮゲートウェイ：IPSec を利用、3DES での暗号化、IKE を利用した共通鍵によるＶＰＮゲートウェイ認証、ISDN バックアップ
(4) 擬似ネットワーク：伝送帯域の設定、固定の伝送遅延を付加

7.5.2 ローカルテストの方法とその結果

7.3.3 項の図１に示す擬似ネットワークの伝送遅延を 100ms、300ms、500ms、800ms の４点に変化させて作業遅延時間を測定した。これは、東京ーロサンゼルス間の固定遅延時間として 100ms を、東京ーロンドン間の固定遅延として 300ms を想定したためである。更に遅延揺らぎが発生する場合を想定して、500ms と 800ms についても調査することとした。

また、回線速度として、32kb/s、64kb/s、512kb/s の３点で調査をした。これは ISP への接続回線として、それぞれダイヤルアップ回線、ISDN 回線、ブロードバンド常時接続回線を想定したものである。

今回、以下の２つの表に対して、キーボード入力後のパソコン画面への表示の遅延時間を測定した。

(1) 5 項目の簡単な表（ファイルサイズ：15KB）を順々に表示させる。(Test1)
(2) 30 項目の複雑な表（ファイルサイズ：70KB）を順々に表示させる。(Test2)

遅延時間の測定は、ストップウォッチによる手作業で行った。テストの結果を表 3 に示す。Test1 で 2～3 秒程度の作業遅延が発生している時に、一般社員のデータ入力者にとっては 1～1.5 ストロークのテンポの遅れとして感じられた。この程度ならば、作業者にとって大きな違和感を感じない程度である。しかし、4～5 秒以上の遅れとなると、待つことによるかなりのストレスを感じるということがわかった。

このことから、ロンドンでブロードバンド接続されたインターネットＶＰＮの通信状態が良好な場合である表 3 の(A)の条件の場合に、Test1 の作業に対して実施可能であるものと想定できる。ロンドンー東京の通信状態を想定した場合、表 3 の(B)、(C)の状態になる可能性がある。この場合で遅延時間が 3 秒程度であり、何とか作業できるものと想定できる。

クライアントパソコンの画面に表示させる表内への入力結果の表示遅延は、Test1、Test2 とも 1～2 秒程度であった。このことから、Test2 において、表示までに 10 数秒の時間を要するものの、表への入力、修正作業は十分実施できるレベルであることが判明した。

なお、ＣＳ方式の場合で、64kb/s の回線速度において同様のテストを行った結果、Test1 の作業の場合、伝送遅延時間が 300ms で 48 秒、伝送遅延時間が 500ms で 63 秒の作業遅延となり、一般業務ではほとんど使えないという結果が得られた。

7.5.3 ロンドンにおける実地テストの結果

ローカルテストで行った作業がロンドンのクライアントパソコンから、東京本社のサーバに対して、実地において実施可能かどうかを調査した。今回は、両端の ISP にブロードバンド接続された実回線のインターネットＶＰＮを用いている。

まず、イギリスーアメリカー日本の経路で、往復の伝送遅延時間とパケットロスについて測定した。ここでは ICMP（Internet Control Message Protocol）のサブコマンドである ping コマンド（32byte、TTL=30）を用いている。ロンドンから 1 分間で一つの ping コマンドを東京の OCN のルータに対して発信して、エコーとして応答する往復時間を 100 サンプルごとに 3 日間サンプリングでデータを取って評価した。

平常時の一般的なロンドンー東京間のスループットは平均 220kb/s（160kb/s～320kb/s の範囲）、固定遅延時間は 320ms であり、また、ホップ数は 30 であった。今回、ICMP のサブコマンドである Tracert コマンドで調べた通信ルートにおいて通信事業者の SLA で定めている“日米間の網内遅延 130ms 以下”とする高い通信品質を適用することができた。

今回得られた ICMP エコー特性のうち、最も測定結果として悪かった夕方の往復伝送遅延時間分布を図 8 に示す。この夕方の時間帯はアメリカ東海岸、イギリスともビジネスタイムであり、その影響によるものと想定される。

表3 ローカルテストでの作業遅延時間の測定結果

Table 3 The measurement results of operation delay time in the local tests.

Transmission delay time(ms)	100			300			500			800		
Access speed(kb/s)	32	64	512	32	64	512	32	64	512	32	64	512
Test1(sec)	5	3	2	5	3 (B)	2 (A)	5	4	3 (C)	6	6	5
Test2(sec)	17	15	14	17	16	15	17	16	15	18	16	15

Note: Delay time measurement when displaying a table one by one.

Test1:Table of 5 items(15KB), Test2:Table of 30 items(70KB)

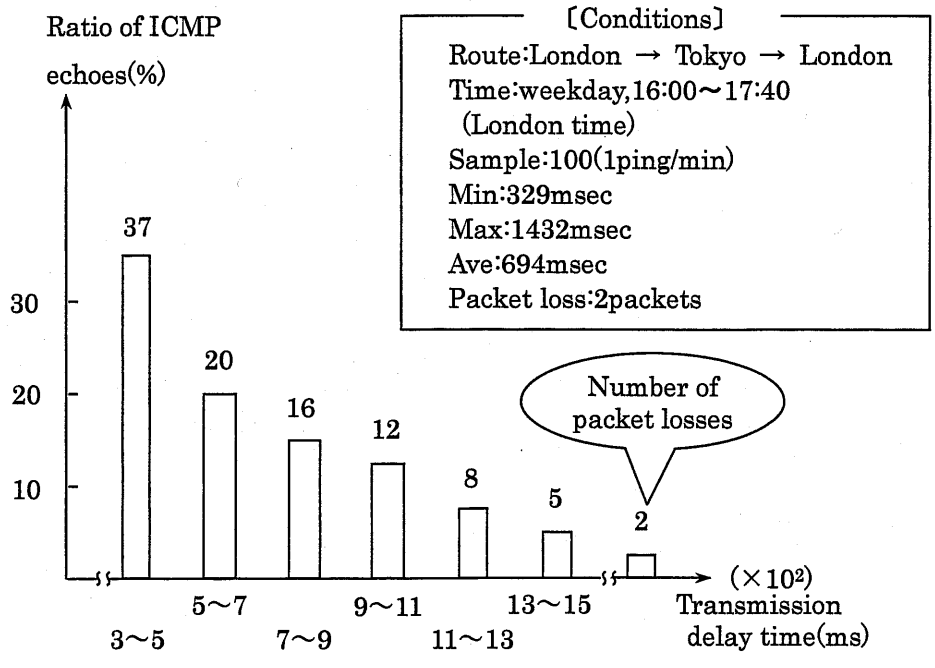


図8 最悪時の往復伝送遅延の分布

Fig.8 The distribution of round trip transmission delay at the time of worst.

ロンドン事務所のクライアントパソコンからTest1について一般社員が作業をした。その結果、表3の(A)と同様、1～1.5ストロークのテンポの遅れで、ほぼ定常的に使えるという結果が得られた。ただし、図8のような通信品質の劣化が発生する可能性の高い夕方の時間帯を避けるよう配意した。

また、64kb/s の ISP へのアクセス回線に接続した場合についても調査した。その結果、若干ストレスはあるものの、表３の(B)の結果と同様に、何とか使えることがわかり、ＶＰＮゲートウェイが持つ ISDN バックアップ機能の場合でも利用できることが判明した。

7.5.4 本方式の経済的効用の検討

インターネットＶＰＮで本システムを構築する場合の費用を、通信事業者が提供する国際仮想専用線（ＩＰ-ＶＰＮ）を利用して構築する場合の費用と比較した。費用は通信網構築のコストも含めたランニングコストとして比較する。計算の前提条件を以下のとおりである。

(1) センタ側アクセス回線：512kb/s
(2) 海外拠点アクセス回線：64kb/s
(3) 海外拠点数：22 拠点
(4) ルータやＶＰＮゲートウェイ等機器代、設計費、工事費、保守運用費を算入
(5) 回線料金や ISP へ支払う料金を算入

この結果、従来の国際仮想専用線で構築した場合の約 7,000 万円／年のランニングコストを大幅に削減できた。具体的には、第９章の（参考）の記事にもあるように、約 600 万円／年へと、約 10 分の１にコスト低減（約 6400 万円／年のコスト削減）できることが判明した。

また、ＳＢＣ方式を適用したことから、次のコスト効果も期待できる。

(1) パソコンの OS やスペックに依存せずクライアントとして適用できることから、新規購入コストをかけず既存パソコンで統一的な利用環境が実現できること。
(2) アプリケーションのバージョンアップなど、パソコン毎に必要となる作業コストが不要となること。

ＳＢＣ方式部分のみの導入に要した実コストは、第６章の 6.4.2 項に示したコストと同じ約３万円／PC である。しかし、この費用には、7.4 項に述べるインターネットＶＰＮ構築費用、ＩＣカード認証プラットフォームおよびＢＢＡ回線などのランニングコストは含んでいない。また、ＳＢＣサーバなどのサーバやその２重化費用なども必要である。このことから、実際にかかった費用を創設費換算したところ 1.6 億円必要であった。しかし、上記に示した年間 6400 万円の費用削減効果のみを見ても、約 2.5 年で投資が回収できることを示しており、それ以外のコスト効果を勘案すると、大きな経済効果のあることがわかる。

7.6 通信品質の改善方法の検討

7.6.1 本方法の仕組みの概念

マルチホーミング（別紙：用語説明(14)）とは、同じアドレスの宛先に対して、複数の経路で通信を行う技術である。従来のマルチホーミングの目的は、広帯域化とロードバランシングによる負荷分散や信頼性確保である[14][15]。

本論文では、インターネットＶＰＮで発生する伝送遅延揺らぎやパケットロスの品質劣化の影響を少なくするために、この技術を利用することを提案している。今回提案する方法の概念を図９に示す。この図では、三つのＶＰＮを用いる場合の伝送遅延揺らぎの品質改善方法を例として示している。以下、プロセス順に本方法を説明する。

(1) 送信側端末から、パケットが時刻順に①②③と発信される。送信装置(S)は三つのＶＰＮに対して、同時に三つの同じIPパケットを送出する機能を有する。
(2) この三つのIPパケットは途中のＶＰＮトンネルに存在する遅延揺らぎの影響を受けて受信装置(R)に到着する。
(3) 受信装置(R)ではIPパケットの到着順を監視し、早く到着した初めてのIPパケットを採用し、すでに採用された遅く到着したIPパケットを廃棄する。
(4) 受信装置(R)で①②③の順にIPパケットを組み立てなおして受信端末へ送信する。

これにより、遅延揺らぎの影響を少なくすることができる。また、いずれかのＶＰＮでパケットロスが発生しても、他のＶＰＮにより到着するIPパケットで補完することができる。本方法では、すべてのＶＰＮにおいて通信品質が全く同時に劣化すると効果は小さい。このため、多少コストはかかるが、ＶＰＮ毎にISPをそれぞれ別々に設定し、極力経路を分散させることが望ましい[16][17]。

今回示す方法は、現在実用化されているマルチホーミングの目的の一つである“信頼性の向上”の機能を包含している。今後、もう一つの目的である“広帯域化”と本方法との組み合わせることについての検討を行うことも有用であると考えられる。

7.6.2 本方法による通信品質改善効果の評価

本方法において劣化のない通信品質が得られる確率P(0)は式(1)であらわされる。この式における設定パラメータは以下のとおりである。

m：適用するＶＰＮの総数
ＶＰＮ(k) ：m本のＶＰＮのうちk番目のＶＰＮ
Pd(k)：ＶＰＮ(k)における通信品質劣化の発生確率

$$P(0)=1-\prod_{k=1}^{m}Pd(k) \quad \cdots(1)$$

次に遅延揺らぎの時間帯ごとの品質改善特性について検討する。設定パラメータは以下のとおりである。

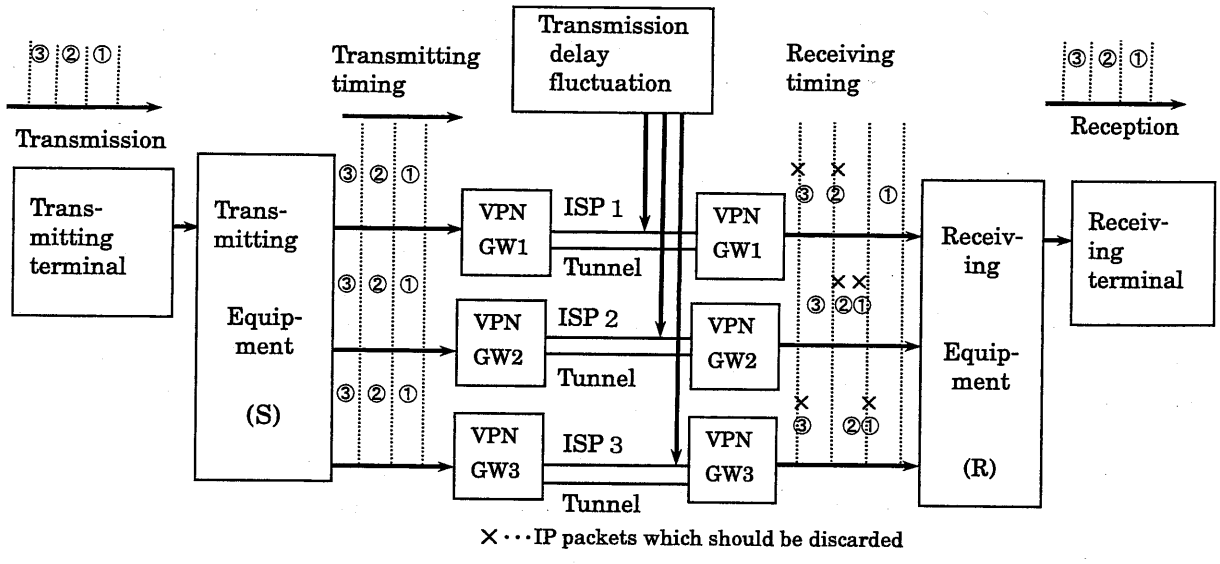


図9 伝送遅延揺らぎの影響を少なくする方法

Fig.9 A method to lessen the influence of transmission delay fluctuation.

T(i)：固定遅延時間からタイムオーバーでパケットロスとなるまでをｎ個に分割して得られるｉ番目の遅延時間帯

P(i,k)：ある遅延時間帯 T(i)におけるＶＰＮ(k)の遅延揺らぎの発生確率

P(i)：本方法を用いた場合の T(i)における遅延揺らぎの発生確率

以下に P(i)の算出方法を示す。i=1 の場合である P(1)は次の式であらわすことができる。

$$P(1)=1-\prod_{k=1}^{m}P(1-P(1,k)) \quad \cdots(2)$$

次に一般式としての P(i)は以下のとおりとなる。

$$P(i)=1-\prod_{k=1}^{m}(1-\sum_{j=1}^{i}P(j,k))-\sum_{j=1}^{i-1}P(j) \quad \cdots(3)$$

図８の品質劣化が二つまたは三つのＶＰＮにおいてそれぞれ発生している場合の、式(3)で示される品質改善の効果を図 10 に示す。

ここでは、ある T(i)での P(i,k)が、例えば P(1,1)=P(1,2)=P(1,3)=0.37 のように図８に示す同じ品質劣化の数値になるものとして、単純化して計算している。図 10 の結果から、ｉが大きくなるほど大きな品質改善効果のあることがわかる。

図10では同じ特性の劣化がすべてのＶＰＮで起きるという稀なケースでの通信品質の改善効果を示しているが、一般的には、通信品質のよいＶＰＮで伝送されたIPパケットが通常採用されるであろう。そのＶＰＮにおいて一時的に品質劣化が起きた時に、“他のＶＰＮのIPパケットで補完する”という形態が一般的な動作パターンになるものと考えられる。

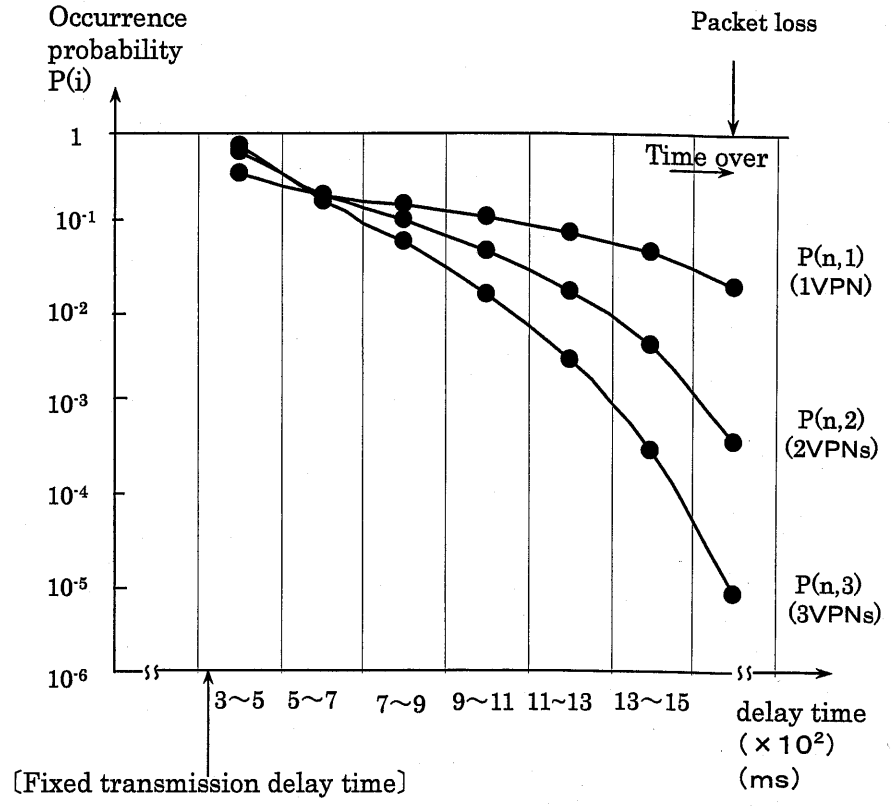


図 10　図8に示す品質の劣化の発生確率の改善状況

Fig.10　The improvement situation of generation probability of deterioration in quality shown in Figure 8.

7.7 利用用途への情報文化学的考察

7.7.1 情報共有に関する考え方

本システムは、国際ネットワークを通じた情報共有の手段を提供しているということができる。この情報共有の方法を以下に情報文化学的に考察してみる。この中では、ＳＢＣ方式の利点を見出すとともに、インターネットＶＰＮの通信品質向上の必要性について検討している。さらにより創造的な企業活動への適用についても論じている。

(1) 理念系

情報文化の構造の一要素として、情報の価値は重要で、特に企業活動においては、情報の価値を財とみなすことができる[17]。本論文で紹介している企業における情報共有は、情報の財として価値を維持向上させるための、企業構成員による活動と言える。この財としての情報をコアコンピタンスとして、商流、物流、情報流が形成され、企業の存在価値が確立される。

(2) 人間系

企業が有する財としての情報の質と量をより向上させるためには、現場から経営層までの風通しの良い組織形態を形成し、それに合わせて情報共有方法を進化させることは重要である。また、社員参加型の共同作業環境を整備することや、社員同士のコミュニケーションの効率化も、企業発展には欠かせないものである。

(3) 施設系

本論文では企業における財としての情報を低コストで効率よく流通させるための“施設系”の技術的発展を中心に述べている。この“施設系”の革新は、それを利用する“人間系”の意識変革や“理念系”の進化を促すインパクトを有していると考えられる。

7.7.2 情報共有形態の分類

7.4.1項に示す“施設系”である保険会社の国際業務システムに対する必要要件は“理念系”および“人間系”からのニーズにもとづいている。この業務システムのデータベースをアップデートするモデルは、「効率的な情報共有をしたい」とする社員の要求を満たす典型的なものと言えよう。

ＬＡＮ／ＷＡＮ接続にもとづくコンピュータシステムに対して、情報共有の観点から、情報共有形態を分類すると以下の通りとなる。

形態１：時々刻々変化する情報のトレーシングと情報の更新およびその共有
（例）作業に用いる共有データベースの更新
形態２：新規又は能動的に変化させた情報の提供とその情報共有
（例）会議資料や議事録などファイルの提供による情報共有
形態３：同一の情報をもとに討議して新たな情報を創出することを目的とする創造的な情報共有　（例）同一の情報を見ながらのＴＶ会議とその情報の更新・共有

7.3.1項に示すモデルとした業務システムは形態１の例となる。今回提起しているＳＢＣ方式の形態１～３への適用は7.3.3項に述べた通り、クライアントパソコンのハードディスクに記録されない方式であることから、内部情報漏えいと言った“人間系”でのセキュリティの観点からも有効である。

7.7.3 創造的情報共有へのシステムの適用性検討

最近の企業活動においては、形態１、形態２をベースとして形態３への要求が高くなる傾向

にある。特に、海外の生産拠点において、日本との間での情報量の多いデータを用いた、リアルタイムでの意思疎通を求める要求には大きいものがある。

例えば三次元ＣＡＤ図面の修正に関する情報共有や討論は、電話や電子メールでは困難である。このことからＴＶ会議によりお互いの画面上で三次元ＣＡＤ図面や相手の映像を見ながら、「リアルタイムでの音声と手書き書きこみデータに基づいて、遠隔打合せを行いたい」という要望が出されることが多い。

この場合、手書きで書きこみされた三次元ＣＡＤ図面は出席者の音声や画面上の映像により合意確認された後、この会議に参加しているオペレータの手で三次元ＣＡＤの電子データに修正がほどこされる。このプロセスはＣＡＤデータを利用する開発の業務フローの一環に組みこまれていて、ＴＶ会議終了後、即座にＣＡＤデータが更新され情報共有が行われる。

このような、三次元ＣＡＤを利用しさらに出席者の映像も映し出せる、開発業務フローに組みこまれたＴＶ会議システムを、海外に進出したある電子装置製造メーカーの日本本社と海外拠点へ導入し、その効果を検証した。その結果、開発担当者の出張費用の大幅な削減を実現するとともに、開発期間を３割程度短縮することが可能であることが判明した。

ここで用いられる音声情報や画像情報については、通信品質への要求条件の厳しいデータ伝送が必要である。このことから、インターネットＶＰＮを伝送路とするＬＡＮ／ＷＡＮシステムを適用したＴＶ会議システムの通信において、7.6項に述べている通信品質の改善を行なうことは極めて有効となる。

7.8 まとめ

本論文では、インターネットＶＰＮとＳＢＣ方式を組み合わせて、海外から日本のセンタのサーバへＬＡＮ／ＷＡＮ接続でアクセスして、簡単な業務が実施可能であることを示した。このシステム構築において、国際仮想専用線（ＩＰ-ＶＰＮ）を用いる場合の、約10分の１のランニングコストで実現できた意義は大きい。

更に、本論文ではマルチホーミングを用いたインターネットＶＰＮの通信品質劣化の影響を少なくする方法の概念を提起した。また、情報文化学的観点からの情報共有の分類をこころみている。この中で同一の三次元ＣＡＤデータについてＴＶ会議システムを利用して討議し修正するといった、より創造的な企業活動への本システムの適用が有効であることを示した。

今後の課題として、ＳＢＣ方式以外の他のシンクライアント方式の国際ネットワークへの適用性検討と、マルチホーミング技術による通信品質向上実験による実証確認があげられる。本論文が国際業務システムの高度化の一助になることを期待している。

なお、本章の実導入の内容は記事として公開されている。第９章の（参考）にこのシステムの構築の経緯や効用を紹介する。今後、このようなシステムのますますの利用が期待される。

[参考文献]

[1] 野崎　保, “グローバルオーダールーティングシステム”, システムマンスリー, pp. 4-7, 野村総研, 東京, May, 2001.

[2] MetaFrame ユーザー事例集, http://www.citrix.co.jp/solutions/casestudy/index.html, June 2003.

[3] http://www.jnx.ne.jp/_download/Oct02_nsg.pdf

[4] http://business.rakuten.co.jp/infoseek/mcscorp/010165/

[5] 中野功一, “ＶＰＮ, ゼロから始めるＶＰＮ”, pp. 40-47, 株式会社アスキー, 東京, 2003.

[6] 林　孝典, 山崎真一郎, 森田直人, 相田　仁, 武市正人, 土居範久, “インターネットを用いた複数経路データ伝送方式の性能評価”, 信学論(B), vol. J84-B, no. 3, pp. 523-533, Mar. 2001.

[7] 西園敏弘, “異速度回線からなるマルチリングパケット伝送方式の評価”, 信学論(B), vol. J69-B, no. 12, pp. 1647-1655, Dec. 1986.

[8] 堀池唯人, 齊藤孝紀, 長田慎二, 宮崎正光, 桧垣博章, “盗聴に頑強な通信路のための IP 通信拡散手法”, 信学技報, IN2002-86, Nov. 2002.

[9] 松田利夫, “古き(レガシー)を活かす新しい ASP の潮流”, コンピュータ＆ネットワーク LAN, pp. 5-9, 株式会社オーム社, 東京, Nov. 2002.

[10] MetaFrame の必要性と全機能一覧, http://www.kcs.ne.jp/syouhin/citrix/ mfrole0.htm.

[11] シンクライアントシステム基礎講座, http://www.keyman.or.jp/search/30000031_1.html, Oct. 2001.

[12] MetaFrameXP 実践ガイド, OPEN DESIGN Books, ＣＱ出版社, 東京, pp. 20-23, 2002.

[13] MetaFrameXP 初級管理者ガイド, 毎日コミュニケーションズ, 東京, pp. 25-30, 2002.

[14] “ブロードバンドＶＰＮを成功させるコツ”, ゼロから始めるＶＰＮ, pp. 36-39, 株式会社アスキー, 東京, 2003.

[15] 河井保博, “広がる“2 本目”のネット接続”, 日経インターネットテクノロジー, pp. 101-111, 日経 BP 社, 東京, Jan. 2002.

[16] “マルチホーミングの効きめ、格安ブロードバンドとの相性は？信頼性向上に効果はあるか”, 日経コミュニケーション, 日経ＢＰ社, 東京, Sep. 2002.

[17] 平賀十志男, “マルチホーミングでインターネット接続を強化する”, 日経コミュニケーション, 日経ＢＰ社, 東京, Oct. 2003.

[18] 片方善治監修, 情報文化学会編, 情報文化学ハンドブック, 森北出版, 東京, pp. 15, 2001.

第8章　共同利用型セキュリティプラットフォームへの発展形態

8.1 概要

本論文の第４章から第７章までは、個別の企業ごとでのセキュリティ対策システムの構築方法について述べている。比較的セキュリティ意識が高く大きな投資も可能な企業においてはこのような方法はとりうる選択肢となる。しかし、一般企業においては、個別のシステム構築は大きな負担となる。本章ではこれをふまえて、セキュリティ処理機能をセキュリティプラットフォームにもたせて、複数企業で共同利用する方式について研究している。この中では、具体的な用途を事例として２つ提起してセキュリティプラットフォームの活用法を示すとともに、将来の展望を論じている。

本章では、8.2項でセキュリティプラットフォームの構造を示し、8.3項でそのプラットフォームの適用方法と、実際の検証でのコスト効果を含めた結果を述べている。さらにこのプラットフォームの発展的利用形態の事例として、8.4 項で常時監視セキュリティ対策システムへの適用方法を、8.5 項でＳＢＣ方式を用いたプラットフォーム上での協調作業システムを紹介している。8.6 項でこのセキュリティプラットフォームの今後の課題を示すとともに、社会的なセキュリティ基盤としての発展の方向性を論じている。

8.2 セキュリティプラットフォームの概要

8.2.1 セキュリティプラットフォームの定義

セキュリティプラットフォームとは、セキュリティに関する情報を集めて組織化するところ（収集・構築）、保存しておくところ（蓄積）、流通するところ（流通）、情報を取り出し利用するところ（利用）となる共通基盤とみなすことができる[1]-[3]。これにより、セキュリティプラットフォームは、情報コンテンツなどの構築・蓄積・流通・利用の利便性を支援する機能を有するものと考えられる[4]。

8.2.2　セキュリティプラットフォームへの要求条件

人間が社会生活や活動を展開する際に、「いつでも、どこでも、誰とでも、自由に情報のやりとりができる」という手段を提供するために、情報の生成、蓄積、伝達、処理などの各過程において、セキュリティプラットフォームには様々の基本要件が課される[5]-[7]。情報流通の階層化の概念とその中におけるセキュリティ機能の位置付けを図１に示す。情報を伝送するネットワークの１つ上の階層で共同利用型の各種サービスの１

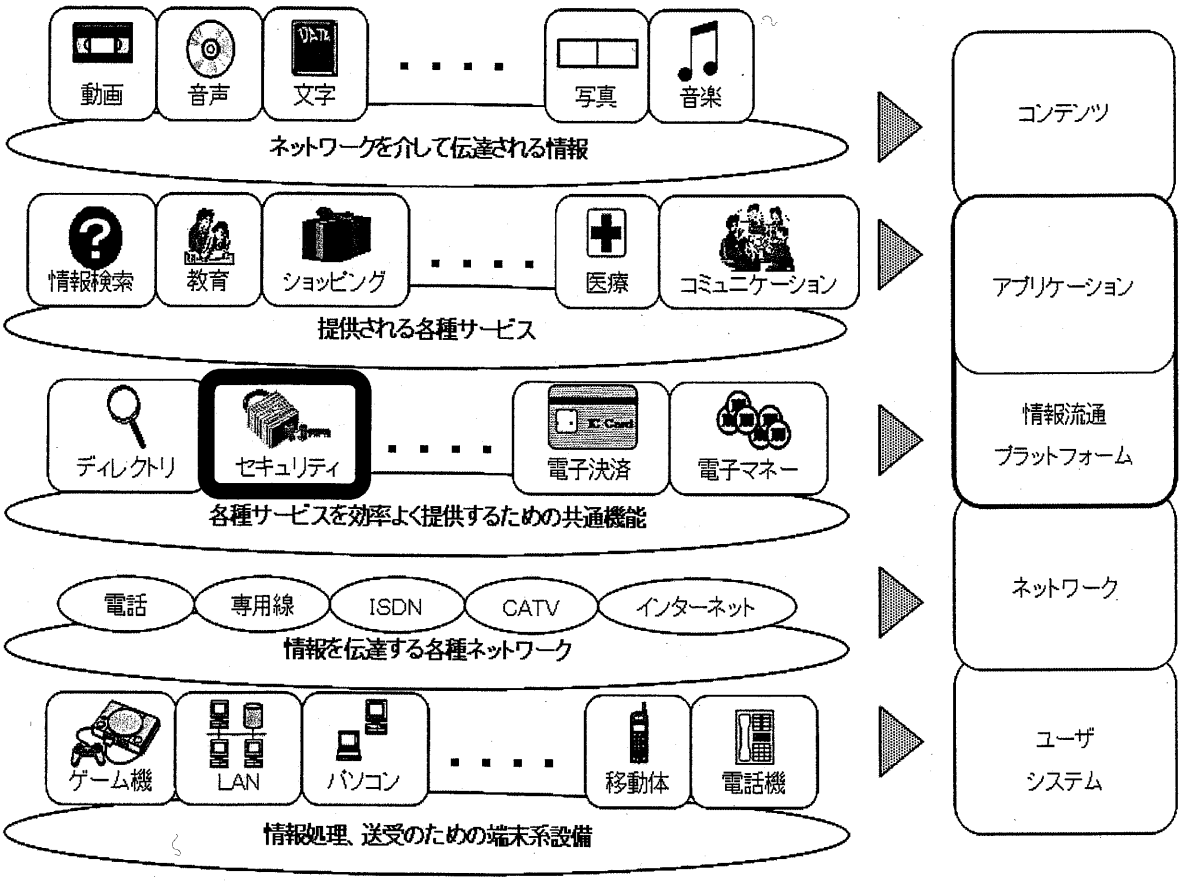


図1 情報流通の概念

Fig.1 The concept of information flow.

つとして提供される。この図は一般公衆型の利用形態を主に示しているが、企業に閉じた形態または、企業間での利用の形態でも同じ概念で適用可能である。

8.2.3 セキュリティプラットフォームの構造

図1に示すセキュリティ機能の部分を細部の機能を構造図として図2に示す。“① ネットワーク系セキュリティ”、“② 認証系セキュリティ”、“③ トランザクション系セキュリティ”の3階層をサービス階層とする形態となる。業界向けのカスタマイズは必要になるが、基本となる機能の階層別分類は変わらない。上位の階層になるほどカスタマイズが必要となる傾向にある[5]。

8.3 共同利用型セキュリティプラットフォームの適用方法とその効果

第4章から第7章の研究においては、比較的セキュリティ意識が高く、ノウハウや経

験および投資力のある一部の企業を対象としている。今後は情報漏えい対策のニーズの高まりに伴い、ノウハウの少ない企業が安価なシステム導入を模索するものと想定される。ネットワークのブロードバンド常時接続が企業において多数導入されている現状を踏まえて、事前に標準化されたパッケージ型アウトソーシングスタイルとしての共同利用型のセキュリティプラットフォームを検討する。図３にその構成例を示す。

この構成では、ネットワークを介したサーバ類の共同運用を行うことにより、セキュリティポリシーにおけるシステムコンセプトの統一と、低コスト化を可能としている。また、広域ＬＡＮにおけるＶ—ＬＡＮやＶＰＮのような閉域網の適用により、ネットワークセキュリティを確保している[8]。この部分は、図２の ”① Network Security” のレイヤに相当する機能部分である。

共同利用管理サーバで、ユーザ企業毎のドメインを認識させ、また、共同利用ファイルサーバでは、場合によっては、第５章で述べた指紋データから変換された秘密のパスワード（ドメインパスワード）とユーザＩＤによるアクセス管理を実施させている。この部分は、図２の ”② Authentication Security” のレイヤに相当する機能になる。さらに、ＳＢＣ方式をＦＥＰ（フロントエンドプロセッサ）として各社で共同利用している。

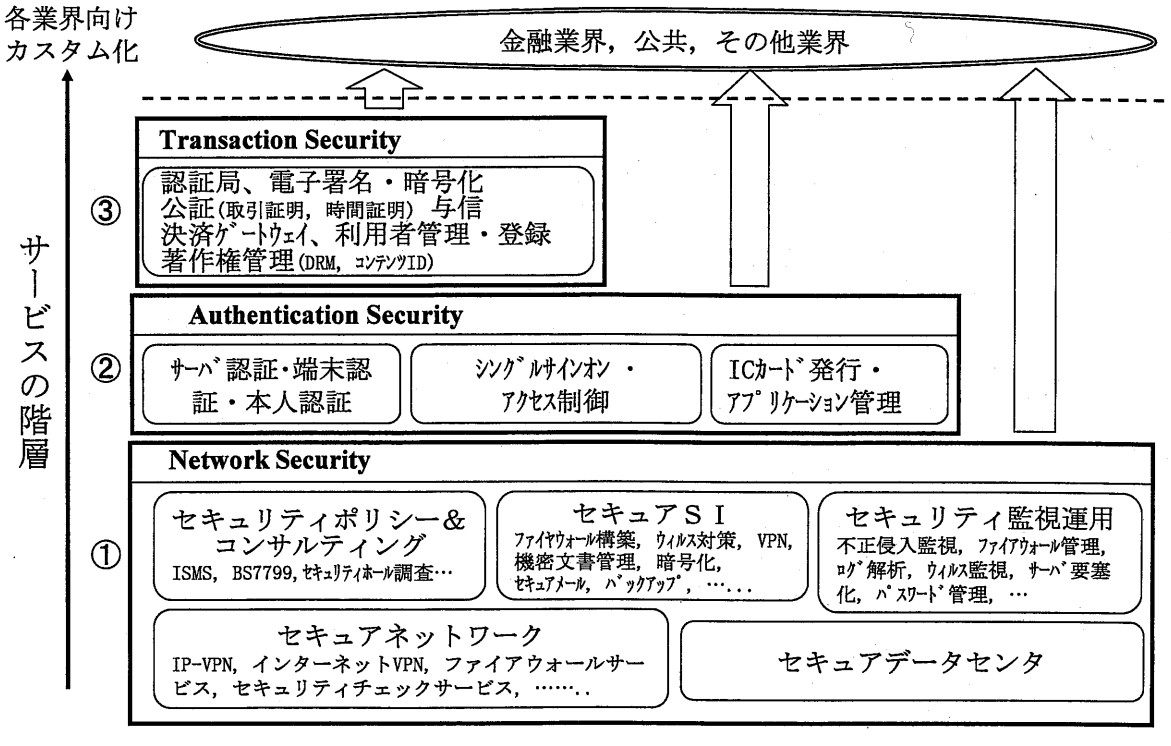


図2　セキュリティプラットフォームの構造

Fig.2　The structure of a security platform.

共同利用ファイルサーバおよび共同利用管理サーバのハードは各社で共同利用しているが、処理はユーザ企業個別としている。ファイルサーバにおけるストレージについては、各社で共同利用する形態としている。なお、通信および各サーバ、クライアントパソコンのファイルに暗号を適用している場合が多いことから、認証サーバ、ドメインコントローラ（別紙：用語説明(21)）のサーバを物理的にデータセンタ内に設置することも可能である。この部分は、図２のセキュアデータセンタの機能内容に相当する。

このセキュリティプラットフォームでは、図２に示す機能のうち、図２①のネットワークのパイプと、データセンタにある情報の格納庫をインフラとして、図２②の認証機能を提供する形態をモデルとしている。また、①のレイヤにある共通化されたセキュリティポリシーやセキュリティ監視・運用やセキュアＳＩ機能もあわせて具備している。ただし現状のところ、図２③の高度なトランザクションのセキュリティ機能や、②のアプリケーション管理機能までは提供していない。

このプラットフォームでは、共同利用であるがゆえの大幅な監視運用コストの低減が実現できる。この監視運用の業務内容として、(1)不正アクセスおよびアクセス状況の監視、(2)セキュリティポリシーの変更と運用、(3)セキュリティホールの修正、(4)非常時の検出と運用停止、などが必要となる。

図３の構成では、共同利用型ファイルサーバへＳＢＣ方式を適用している。この方式は、クライアントパソコン内の OS やブラウザのバージョンに関係なく動作するという特長があるため、共同利用型プラットフォームには有用である。今回、“媒体への記録の制限と印刷の制限機能”を実現するため、この方式が持つ「クライアントパソコンにデータがダウンロードできない仕組み」に注目し、このプラットフォームへ適用している。

このセキュリティプラットフォームでは 、“認可における制御”というファイルマネジメント機能については、一般に市販されている文書管理システムを適用することも可能である。しかし、現状の文書管理システムでは、(1)文書のＷｅｂ化が必要である、(2)ＰＤＦファイルにする必要がある、などの文書管理システム固有の制約のある場合が多く、さらにコストが高いことから、適用については今後の技術開発の進展を踏まえた研究課題である。

このプラットフォームを、大手証券会社の社内システムに適用して、その効果を検証した。この証券会社の例では、図３の左に示す”企業 ”とは支店のことであり、図の左に示す“ｎ”はｎ＝30 である。パフォーマンスマネジメントとトラフィックマネジメントをアウトソーシングして、自社で実施する場合と比較して、年間で約 1,000 万円の経済効果を実現している。これはアウトソーシングによる集約実施効果の現れである。

以上は、基本となるプラットフォームの構成を述べているが、利用用途ごとに、以下の 8.4 項、8.5 項に示すようなこのプラットフォームのカスタマイズが必要となる。

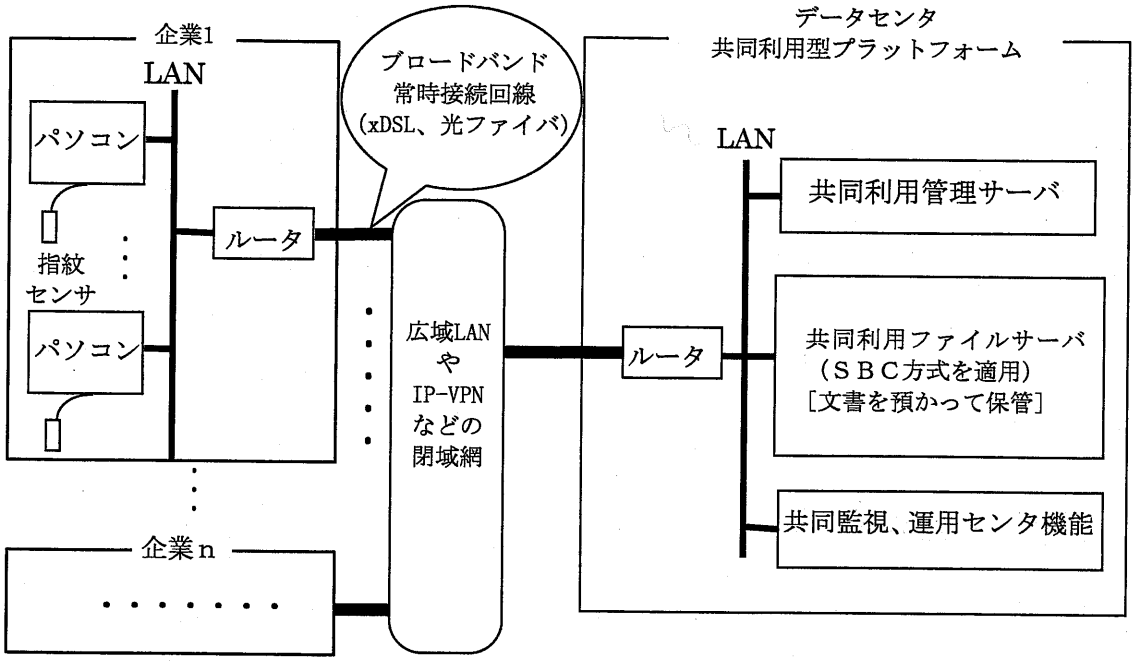


図3 共同利用型セキュリティプラットフォームの構成例

Fig.3 An example of composition of a joint use type security system.

8.4 常時監視セキュリティ対策システムへの適用

常時監視セキュリティ対策システムでは、すべてのクライアント側の操作をログとして収集し、常時監視した上で、情報分析管理するものである。その機能を表1に、その構成概要を図4に示す。このシステムは既存のシステムが有しているセキュリティ対策機能も含めて、ワンストップで統合化することによりコストダウンを実現している。

表1および図4に示す機能については、図3に示す“共同利用管理サーバ”および“共同監視運用センタ”の有するメカニズムで実現される。また、ファイルの一元管理については、“共同利用ファイルサーバ”を利用して実現可能となる。

このシステムにおいては、禁止ルールを定めて、これに対する違反を検出して利用者本人への警告はもとより、アラームを発出したり、その状況を管理者に通知したりする機能を有する。違反状況の統計機能をもとに分析することにより、次の情報漏えい対策を検討することも可能となる[9]。また、個人情報保護法案にある事件発生後のトレーサビリティの確保を、2.2項に示す事後追跡として実施することが大切となる[10]。

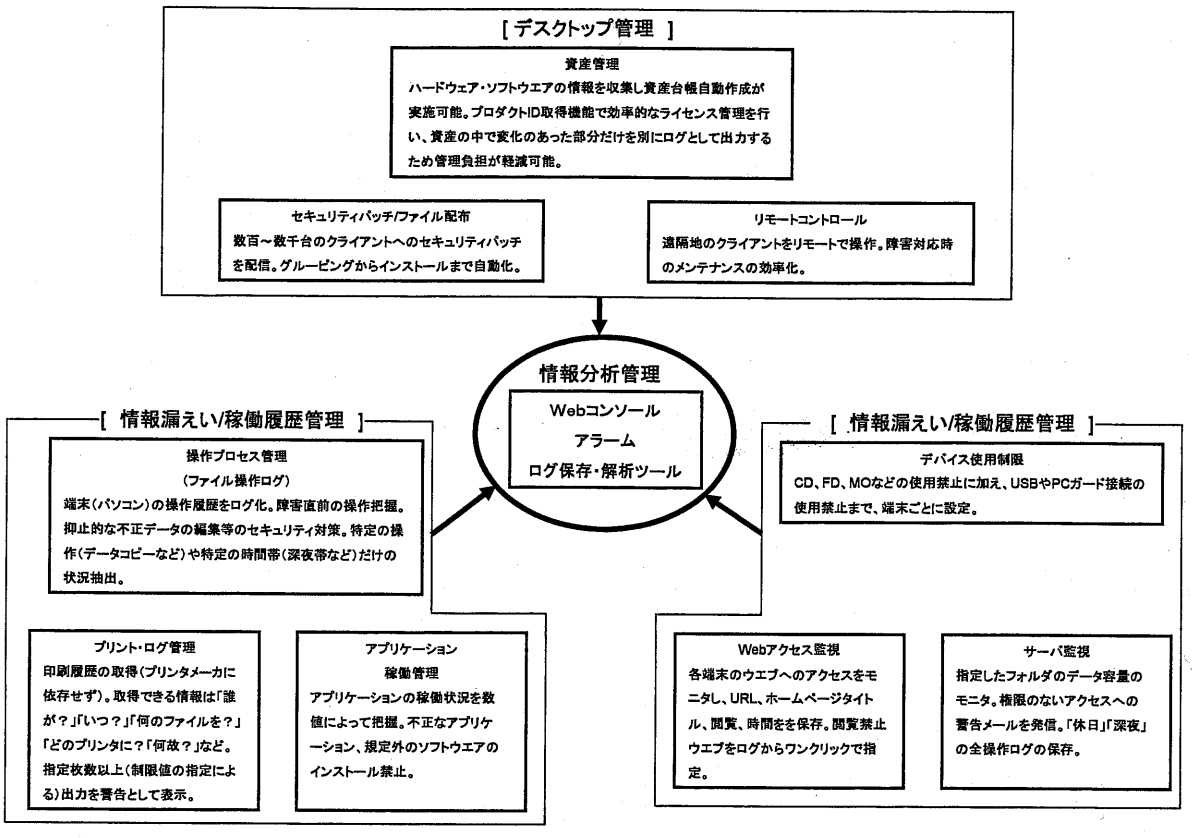
表1 リアルタイム監視システムの機能

Table1 The functions of the real-time monitoring system.

大項目	中項目	小項目
資産管理	ハードウェア資産管理	①CPU ②HDDの全体容量／空き容量 ③IPアドレス ④MACアドレス ⑤ドメイン名 ⑥メモリサイズ ⑦シリアルNo. ⑧マシン機種名 ⑨マシンメーカ名 ⑩コンピュータ名 など20種類以上を自動取得
	ソフトウェア資産管理	①インストールアプリケーション ②OSバージョンとプロダクトID取得 ③全EXE情報取得 ④アプリケーションのバージョン ⑤MS-Officeのプロダクト ID取得 ⑥不正ライセンスの検出 ⑦HotFix情報取得 ⑧ウィルスソフト情報の取得
	資産の変化を知る管理	①ハードウェアの追加／削除を自動検出 ②未稼働PCを自動検出 ③リース切れPCの自動検出 ④勝手なソフトウェアのインストールを自動検出 ⑤フィル多機能で任意の情報を抽出
操作プロセス管理（ファイル操作ログ）	セキュリティ管理	①PC操作履歴をログ化 ②権限の無いファイルアクセスを監視 ③ファイルのコピー、削除、名前の変更などファイルの流れをログ化
	モラル向上／リテラシー管理	①商用以外のソフトウェア操作を管理・指導可能 ②ゲームソフトの稼働監視 ③端末の稼働時間及び稼働状態を視覚的に集計 ④PCの私物化、環境変更の監視
	障害管理	①障害発生までの操作履歴をログ化 ②管理対象アプリケーションだけのログを保持
アプリケーション稼働管理	アプリケーション稼働集計	①グループ別に、アプリケーションの使用時間を集計 ②管理対象アプリケーションの選択 ③管理期間を設定
	アプリケーションの稼働禁止	①商用以外、使用禁止アプリケーションの起動禁止が可能 ②特定のアプリケーションの使用時間の制限
	アプリケーション要・不要管理	①未使用アプリケーションの検出により要・不要の判断
プリント・ログ管理	プリンタ別集計	①プリンタ単位で印刷枚数を集計 ②プリンタを適材適所へ配置
	ドキュメント別集計	①印刷ドキュメント（ファイル名）別に、誰が何枚印刷したかを管理（セキュリティ対策） ②ペーパーレス化の推進 ③ISOに則った印刷枚数管理
	プリントアラーム	①グループ別に印刷枚数を管理し、グループ課金が可能 ②印刷制限枚数を設定して、アラームとして印刷超過ログを保存
Webアクセス監視／デバイス使用制限	Webのアクセスログ管理	①誰がどのWebサイトをどれだけの時間閲覧しているかを監視 ②キーワードに抵触したサイトへのアクセス履歴のみログ化
	不正なWebサイトの閲覧を禁止	①キーワードに抵触したサイトへの閲覧を禁止 ②禁止サイト設定は日本語のキーワードで登録可能
	記憶媒体のデバイス禁止	①CD、FD、USBなどのリムーバブルメディアの使用を制限してデータの持ち出し禁止
サーバ監視	サーバ容量管理	①管理対象のフォルダの容量を監視し、容量制限を超過したものにアラーム発生
	サーバアクセスログ管理	①指定フォルダ／ファイルへのアクセスログを記録 ②権限の無いアクセス（編集・実行・削除・移動・コピーなど）をログオンアカウント別にログ化 ③複数のサーバを一括で統合管理
セキュリティパッチ・ファイル配置	セキュリティパッチの配信機能	①パッチが適応されていない端末を自動的にグルーピング ②権限に依存せず自動インストール可能 ③Push型で配信し、未配端末へは自動的にPull型で配信
	各PCへファイルを配布	①PC、グループ単位で任意のファイル配布 ②スケジューリングして自動配布 ③配布ログで結果を取得し、未配布PCへは自動再送
	エージェントモジュール	①エージェントモジュールのバージョンをチェックして、自動的に最新のバージョンにアップデート
リモートコントロール	リモートで障害対応	①リモートPCの操作 ②リモートPCの設定変更 ③リモートPCのファイルコピー／削除 ④リモートで再起動（ログオン／ログオフ） ⑤リモートPCのファイルを編集
	リモート運用指導	①リモートPCのデスクトップにコメントを追記して操作指導 ②教育現場でのPC操作指導
情報分析管理	Webコンソール	①Webブラウザ上から必要な情報を必要な時に参照可能 ②変化のあった部分だけのレポート、統計／集計レポートなどの情報分析の実行

図4 リアルタイム監視システムのプラットフォームで実現すべき機能構成

Fig.4 The composition of the real-time monitoring system.



本システムの導入により、“常に監視されている”という意識を社員に植え付け問題行動を抑止することが可能となる。ただし、このシステムでの社員監視機能を使いこなすには、情報システム部のみならず、総務部、法務部、経営企画室などのセキュリティに関係する各部のミッションと役割を有機的に結合する必要がある。この組織の上に監視機能や監視のあり方のポリシーを定めないと十分機能させることはできない。また、このポリシーを社内規定に盛り込んで、社員に告知しておく必要がある。

「社員は勤務中心といえども私的領域がある」という判例があることから、黙って監視することはできない。また、監視により得られる情報もまた社員の個人情報である。このことから、社員規定に盛り込むべき必要があり、その項目の例を表2に示す。

このシステムをプラットフォームサービスにすることで、レディメイドの機能としての利用が可能となる。パソコンを 1,000 台保有するクラスの企業で、実際かかるフルアウトソーシング費用がパソコン1台あたり約 4,000 円／月であることが判明した。この

ことから、アウトソーシングする前と比較して、３～４割の費用削減ができることが明らかになった。また、パフォーマンス報告サービスなどをランニングコスト化できるため、運用のための人件費もカットでき、更なる経済化が可能となる。さらに、社員を監視するシステムであることから、アウトソーシングして第３者に委ねることで、隠し事のない透明性の確保も実現できた。

表2　監視を行う場合の新規に社内規定とすべき項目

Table2　The items that should be newly assumed to be an internal rule.

1	（監視の宣言） 懲戒や人事といった従業員に不利益な決定に使うことを明記する。	6	（社員に禁止する行為） アプリケーションの使用禁止ならなるべく具体的なアプリケーション名まで書く。
2	（監視の方法） 運用体制、誰が管理者を任命するか、管理者にどのような権限を与えるか、など	7	（監視ログの保管期間） ２年など具体的に決める。
3	（監視する項目） 例えば、メールの宛て先だけか内容も含むのか、など。	8	（本人の開示要求への対応） 監視で得た情報は監視される本人への開示義務があるため。
4	（監視する時間帯） 具体的な時間帯を明記する。	9	（問題行動を発見した場合の対応方法） 従業員への警告方法など。
5	（苦情処理の対応） 総務部で受け付ける、など。	10	（処分を行う場合の根拠） 当社○○規定の○条に基づき懲戒、など。

8.5 プラットフォーム上のSBC方式による協調作業システム

8.5.1 背景

ここ数年で製造業をはじめとする非ＩＴ系の業界でも、多くの作業をコンピュータ上で行うことが増えてきた。一方で、１つの会社、１つの拠点に閉じないかたちでの共同作業が増えている。一例として挙げられるのは自動車業界で、複数の会社によって供給される部品を組み立てることによって最終製品をつくりあげるような形態である。また建築業界のように、大規模なプロジェクトを複数会社でジョイントベンチャーを組んで行うことが慣習となっている業界もある。

このような状況で協調作業を行う場合、遠隔地をネットワークで結んで、作業にかかわる人が直接集まることなく参加できるという環境が求められつつある。

しかし非ＩＴ系の業界では、計算機システムを管理できる管理者を自社内に持たない場合も多く、計算機システムの構築・運用を外部に委託するケースが増えている。

そのような要求にこたえるとともに、セキュリティ機能の共有化を目指して、ＳＢＣ方式をベースとする、アプリケーション共有のプラットフォームの適用を検討し、提起している。[10][11]

8.5.2 SBCベースのアプリケーション共有システム

本システムではアプリケーションの動作する Windows サーバと実際のユーザが操作するクライアントとの間に、フロントエンドサーバを置き、サーバからクライアントに向かう画面のデータを複数のクライアントに同時に配信する方式である。構成を図５に示す。図５に示すフロントエンドサーバで通信情報を仲介することにより、ＳＢＣサーバを利用する形態としている。本システムでは、複数のクライアントから送られる操作情報の中から、現在アプリケーションを操作する権利を持っているクライアントの操作情報だけをサーバに送る。これにより、アプリケーションは単一のユーザが操作しているのと全く同じ状況になる。

本システムでは、対象となるアプリケーションをＣＡＤ等のグラフィカルなものと想定し、単一のデータまたは図面を複数人のユーザが共同で編集するような協調作業を想定している。複数人というのは２人から 10 人程度で、それぞれのユーザはほぼ対等な権利を持っているという前提で設計をしている。

本システムを用いるとネットワークを介して遠隔地でデータをリアルタイムに共有することができる。さらにデータの実体は１つで、それを複数のユーザが直接操作できるので、あらかじめデータのコピーを各ユーザの手元に配布するような形態の共有とは異なり、作業後に作業の結果を統合するという余計な手間がかからない。

また前述のように、同時にアプリケーションを操作するのは単一のユーザだけに制限されている。このようにシステム側でアプリケーションへのアクセスを制御することで、アプリケーションそのものを複数ユーザに対応させるような改造を施すことなく、アプリケーション共有のメリットを享受することができる。

さらに、アプリケーションの画面を共有するだけでは伝えにくい、「ここ」に着目しているといった情報を伝達するため、また共同作業の途中経過を何らかのかたちで残しておくために、アプリケーションの画面に透明なウインドウをかぶせ、それに簡単な絵や文字を書く「オーバーレイ」機能を実装している。オーバーレイは複数のユーザが同時に書き込むことが可能な設計になっている。それにより、アプリケーションを操作して

いるユーザに対して他のユーザから指示をすることが可能である。

これをサポートする機能として次のものがあげられる。

(1) シングルサインオン機能

1度認証を受けるとその後、本システム内に存在するすべてのサーバに対して認証が不要となる機能である。Liberty Alliance の仕様を用いて、アカウントの分散管理を行っているため、アカウントはそれぞれのサーバの管理主体によって別々に管理され、それをフロントエンドサーバで連携させる。そのため、シングルサインオン用に新たなアカウント体系をつくる必要はなく、既存の体系をそのまま利用することができる。図6にその構造を示す。この図では、フロントエンドサーバの認証サーバで認証されていることに基づいて、サービスサーバに対して代理認証を求める形態を示している。

(2) セッション管理機能

前述の複数ユーザによる協調作業は一種の会議であることから、そのような会議の開催を助け、円滑に進行させるために、次のような機能を有している。

① セッション予約、自動召集

あらかじめ会議を予約し、参加が予定されているメンバを登録することができる。登録されたメンバの元には、開催予定時刻が近づくと自動的にシステムから召集のメッセージが届く。その召集のメッセージに応答することで、参加者は円滑に協調作業への参加の準備を整えることができる。

② SIP（別紙：用語説明（22））によるセッション管理

召集などの機能は、SIP のプロトコルを利用している。これにより、音声会議やビデオ会議など、アプリケーション共有機能と同時に用いられる可能性のある他のアプリケーションとの親和性を実現している。

③ セッションディレクトリ

協調作業の予約を行うため、本システムはセッションディレクトリと呼ばれるデータベースを装備している。セッションディレクトリは協調作業の予約、予約内容の確認、予約の変更・取り消しに加え、過去の協調作業の情報を参照することや、現在進行中の情報を参照すること、さらにはそれらの情報から、現在行われている協調作業に参加するためのインタフェースを提供することができる。

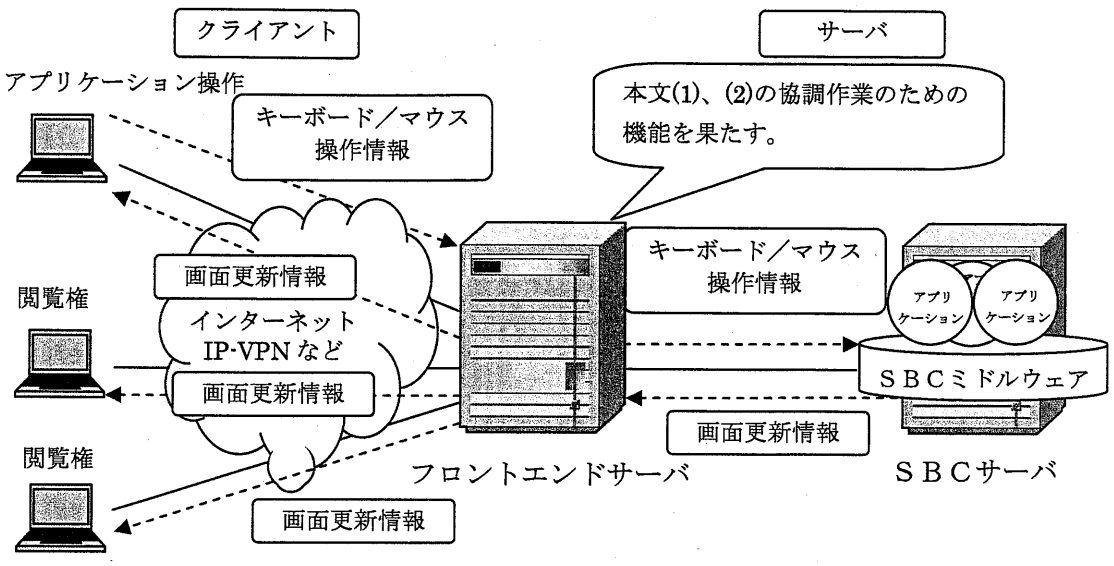


図5　SBC方式によるアプリケーション共有方法

Fig.5　The method of sharing application by the SBC method.

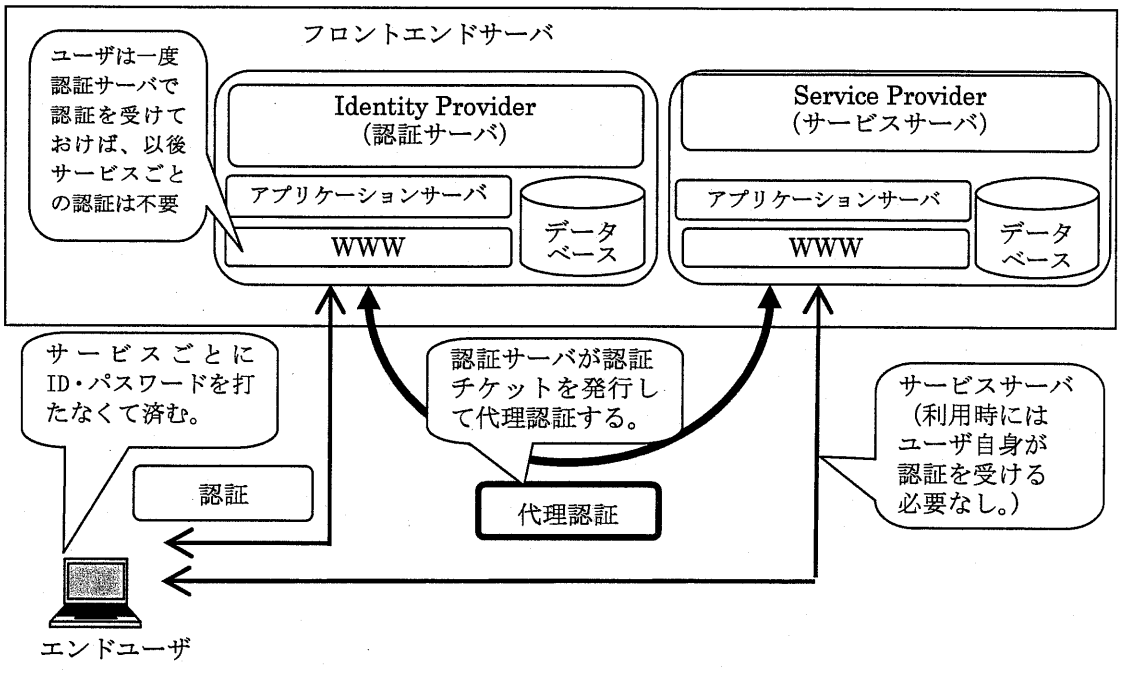


図6　シングルサインオンのための構造

Fig.6　The structure for single sign-on.

このプラットフォームを適用することにより、企業が自前で構築するよりも高いコスト効果を得ることができる。これは、共同利用型プラットフォームとしてのレディメイド機能を利用でき、自前構築に必要なＳＩ（システムインテグレーション）費用が大幅にカットできるからである。

本方式については、コンセプトレベルの提起であることから、実証試験が今後の課題である。また、ＳＢＣ方式以外に、ブレードPC 方式（別紙：用語説明(8)）のような、他のシンクライアント方式（別紙：用語説明(7)）がある。これらの特長に応じた適用性検討も必要で、これも今後の検討課題である。

8.6 まとめ

本章では、共同利用型セキュリティプラットフォームが具備すべき機能と構成について説明し、その効用を明らかにしている。また、その基本機能に基づく用途別の発展形態について、２つの例をとらえて紹介している。

セキュリティプラットフォームとしての社員への常時監視システムについては、今後、監視、管理機能の集中化により、コストパフォーマンスがよく保守運用性の高いシステムに発展するものと考えられる。さらに、ＳＢＣ方式も含めたシンクライアント方式の発展系としての、“アプリケーションの共同利用システム”の実現により、遠隔共同作業の普及の一助になるものと期待している。今後は、操作性などの試験検証のような実用レベルのバージョンアップへの取り組みが課題となる。

当面、共同利用型セキュリティプラットフォームの業務システムへの広範な適用のための機能として、以下の機能の高度化が今後必要である。

① ファイルマネジメント
② トラフィックマネジメント
③ 高品質インターネットゲートウェイ
④ サーバマネジメント
⑤ イントラネットセキュリティマネジメント
⑥ パフォーマンスマネジネント
⑦ デスクトップマネジネント
⑧ ＩＴ資産アウトソーシング

本論文では、セキュリティ対策自体についての社会基盤としての高度化の方向については触れていない。欧米においては認証機能の標準化作業が行われており、日本も積極的に参加している。特にISO/IEC JTC1/SC37 において国際的な標準化作業が活発に行われている[12]。

この活動により、バイオメトリックス認証技術全般を包含した、認証ハードウェア、認証モデル、データフォーマットなどの標準化が早期に実現するものと考えられる。

今後、セキュリティプラットフォームへこの標準化内容を取り込んでいくことにより、セキュリティ対策を進めるための社会基盤に発展するものと期待している。

本章で示したセキュリティプラットフォームの経済効果について、社会で認知されだしている。第９章の（参考）に示すように、金融機関を中心に、合計 5,000 ID 以上の導入実績をあげており、今後、さまざまな業界での利用が期待される。

[参考文献]

[1] 根来龍之, 木村　誠, “ インターネット・プラットフォームビジネスの産業発展への貢献”, 経営情報学会誌, Vol. 9, No. 3, pp. 67-87, Dec. 2000.

[2] Dsvid Ticoll, Alex Lowy, Ravi Kalakota, “JOINED AT THE BIT”, Don Taoscott, Alex Lowy, David Ticoll (Ed.), BLUEPRINT OF DIGITAL ECONOMY”, McGraw-Hill, pp. 19-33, 1998.

[3] 国領二郎, “ネットワーク上の顧客間インタラクション”, マルチメディア社会システムの諸相, 高木晴夫・木嶋恭一編, 日科技連, pp. 51-72, 1997.

[4] 勝間田　仁, “仮想ローカルディスクをベースとしたシームレスな情報共有プラットフォーム”, 情報処理学会, 研究報告, IPSJ, SIG Technical Report May 2003.

[5] 森川郁也ほか, “オペレーションシステムの異組織相互接続のためのセキュリティプラットフォーム”, 信学技報, TM2000-11, pp25-30, May 2000.

[6] OMG, The Common Object Request Broker, “Architecture and Specification”, Revision 2.3.1, Oct. 1999.

[7] ITU-T, Security Architecture for Open System Interconnection for CCITT Application-X.800, 1991.

[8] 今井田伊佐宗ほか, “ユーザポリシーに基づく VPN 間通信のセキュリティ制御方式”, 信学技報, SSE2000-122, IN2000-73, CS2000-53, pp43-48, Sep. 2000.

[9] “社員監視時代が始まる”, 日経コンピュータ, 日経 BP 社, pp. 54-56, Sep. 2004.

[10] 大野靖夫, 池亀正和, 櫻井公人, 鵜飼純一, 吉尾猛, 頼富教子, 平松健太郎, “Meta FrameXP オーバビュー”, Meta FrameXP 初級管理者ガイド, 第１章, 毎日コミュニケーションズ, 東京, 2002.

[11] 山本勝之, 相場宏二, 大野靖夫, 牧野博, 岡島強, 柴田俊治, “サーバ・ベース・コンピューティング（ＳＢＣ）のメリット”, Meta FrameXP 実践ガイド OPEN DESIGN Books, 金子俊夫(編), pp. 7-26, CQ 出版社, 東京, 2002.

[12] 瀬戸洋一, “標準化の動向”, 生態認証技術, pp. 143-149, 共出版株式会社, 東京, 2002.

第9章 結言

本論文では、一般企業の情報資産保護を目的として、特に内部情報漏えいに対するセキュリティ対策について研究している。情報資産保護方法を人間系と施設系での対策に分け、特に施設系での対策の発展の方向にそって研究を進めている。

コスト効果の高いセキュリティ要素技術を抽出し、企業の業務システムへのＵＳＢキー（別紙：用語説明(4)）、指紋認証、ＳＢＣ方式（別紙：用語説明(1)）などの各種技術の適用を研究している。本論文では、以下に簡記するような研究成果をあげている。

(1) 人間系でのセキュリティ対策を研究して、証跡保存型のｅ-ラーニングの有効性を示すとともに、社員の心の満足を得るマネジメント手法までを提起した。
(2) 一般企業の実態に基づき、コスト効果の高いセキュリティ対策を整理して、導入のステップアップ方法を研究し提起した。
(3) ＵＳＢキーのような数千円／PC で実現できるセキュリティツールを研究し、企業での当面のセキュリティ対策の多くの部分をカバーしうることを証明した。
(4) より高度なセキュリティ対策としての指紋認証が、企業利用として２万円／PC 以下で実用化できることを証明した。
(5) ＳＢＣ方式がセキュリティ対策として、比較的低コストで既存の業務システムに適用でき、大きな経済効果を生むことを実際の導入結果で証明した。
(6) ＳＢＣ方式を、ＬＡＮ間接続された国際業務システムに、安価に適用できることを証明した。また、インターネットＶＰＮの品質向上方法を研究し提起した。
(7) 共同利用型セキュリティプラットフォームの経済効果と適用の広がりを事例で紹介した。また、セキュリティの社会基盤になりうることを示した。

これらの研究成果として、本章の最後に（参考）で示しているような、社会へ受け入れられる導入実績をあげることができている。

本論文において残された主な課題と展望は次のとおりである。

(1) 人間系での対策として最も効果的な、社員への心理的なマネジメント方法について、経営心理学としてのレベルにまで高める必要がある。（第２章関連）

(2) ＵＳＢキーによるＰＫＩ利用のためのディジタル証明書の発行要求などの、さらにセキュリティ強度をあげるための各種機能について、コスト効果もふまえた効率的な実現方法の検討が課題である。（第４章関連）

(3) 指紋認証については、セキュリティプラットフォームへの社会基盤としての認証情報の流通の実現があげられる。また、携帯電話への搭載などの展開についても、今後の技術検討が必要である。(第５章関連)

(4) ＳＢＣ方式以外のシンクライアント方式（別紙：用語説明(7)）の企業の業務システムに対する適用検討が必要である。(第６章関連)

(5) 前項をうけて、さらに国際業務システムへの適用性検討が必要である。また、マルチホーミング技術による通信品質向上については、今後、実験による実証確認を実施する必要がある。(第７章関連)

(6) 共同利用型セキュリティプラットフォームにおける文書管理および第８章の２つの事例についての実証試験およびプラットフォーム機能の高度化研究が今後の課題となる。さらに、セキュリティプラットフォームについて、欧米での認証機能の標準化作業をふまえて、社会基盤に発展させるための研究が今後の課題である。(第８章関連)

最後に、本論文が、コスト効果の高い情報資産保護対策を望む一般企業において、参考として利用されることを期待している。また、本章の（別紙）に示す導入実績がますます拡大し、情報資産保護の方面での社会貢献につながることを期待している。

[謝辞]

本研究は筆者が、NTT コミュニケーションズ㈱在職中に研究した内容を、社会人として入学した名古屋工業大学大学院工学研究科博士後期課程（情報工学専攻）の３年間で、梅崎研究室に在籍してまとめたものです。

本研究に当たっては、指導教授であります梅崎太造教授から３年間大変お世話になりました。ここに深く感謝いたします。入学からお世話になりました岩田彰教授、論文審査でお世話になりました北村正教授からはそれぞれ貴重なご助言ご指導をいただきました。また、梅崎研究室の伊藤ふさ江秘書と小島明美秘書にも、事務的なサポートをいただきました。ありがとうございました。

第５章の執筆にあたって、快く情報提供に応じていただいた㈱ディー・ディー・エスの三吉野健滋社長および山村雅典部長に、この場を借りて深く感謝致します。さらに佐藤幸男教授にはまとめに当たってご助言いただきました。ありがとうございました。

また、第６章の執筆にあたって、情報提供に応じていただきアドバイスをいただいた、早稲田大学法学部大塚英明教授およびアイネットエージェンシー㈱の小林薫前取締役にこの場を借りて深く感謝致します。

さらに、NTT コミュニケーションズ（株）の三瓶澄夫氏、黄智永氏には、第７章の執筆にあたって快く情報提供に応じていただきました。ありがとうございました。

最後に、職場で本研究の実施について暖かく見守っていただいた、NTT コミュニケーションズ㈱の中川雅行取締役および職場の皆様方に深く感謝致します。

[業績のまとめ]

査読付き論文一覧

(1) 児玉充晴，梅崎太造，佐藤幸男，“情報漏えい対策システムへの指紋認証の適用とその発展形態の提案”，電子情報通信学会，論文誌，ＤＩ，Vol. J87-D-I No. 2, pp. 278-286, 2004.

(2) 児玉充晴，梅崎太造，“業務システムへの効果的情報保護方法の提案”，情報文化学会誌，Vol. 10, pp. 19-24, 2003.

(3) 児玉充晴，梅崎太造，“低コストの国際業務システムの提案とその情報文化学的考察”，情報文化学会誌，Vol. 11, pp. 23-30, 2005.

(4) Mitsuharu Kodama, Taizo Umezaki, “Proposals of Low Cost and High Security International Business Operating Systems”, The 9th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI) 2005, Vol. II, pp. 89-94, 2005.
(Best Paper 賞を受賞)

(5) 児玉充晴，梅崎太造，竹林春海，“USB キーの情報漏えい対策システムへの適用とその考察”，情報文化学会誌，Vol. 12, pp. 26-32, 2005.

査読なし論文一覧

(1) Jun Yamagata, Hajime Takashima and Mitsuharu Kodama, “ Multi-Point Fault Locating method in Digital Repeated Line”, Japan Telecommunication Review, Oct. 1980.

(2) 児玉充晴，高島　元，山縣　淳，“スタッフ多重変換系の多段累積ジッタ特性”，昭和 56 年電子通信学会総合全国大会，1981.

(3) 児玉充晴, “インターネット時代の新しいビジネス手法”, 日本ベンチャー学会会報, Vol. 10, pp. 4-5, June, 2000.

(4) 児玉充晴, 木村裕一, “超撥水加工法の開発および事業化, NTT 技術ジャーナル”, pp. 82-83, Nov. 1995.

(5) 児玉充晴, “技術開発と金融を融合した新ビジネスの創出”, NTT 技術ジャーナル, pp. 70-71, Jul. 1995.

著書

著者：児玉充晴　　出版社：日経ＢＰ企画　　出版：2005 年 5 月
書名：図解　利益を生み出すビジネス手法と事例 108

表彰

発明考案　ＮＴＴ社長表彰　　昭和 62 年 10 月
“ 超高率マルチメディア多重変換装置 ”　　(下記の(1)の特許)

出願特許　　(注)　(1)以外は単独出願

(1) 登録番号　2727547　高速ディジタル用時分割多重化装置
(2) 特許公開平 07－221742　オンライン符号誤り測定器
(3) 特許公開平 07－280793　水質自動検査装置
(4) 特許公開平 08－254528　連続水質監視装置
(5) 特許公開平 08－035058　撥水性有機膜の形成方法および装置
(6) 特許公開平 08－283703　固体表面の撥水加工方法
(7) 特許公開平 08－285709　光ファイバ変位センサ
(8) 特許公開 2002－032662　契約希望者紹介システム及び方法

（参考） 社会への導入実績と関連記事

1　ＵＳＢキーの主な導入実績　（第４章関連）

Ｎｏ	導入先	個数	Ｎｏ	導入先	個数
1	日本生命保険	１００，０００	4	外資系生命保険会社	1,000
2	大手総合商社	7,000	5	信用金庫	５００
3	警察本部	6,000	6	貿易会社	２５０

2　指紋認証センサユニットの主な導入実績　（第５章関連）

Ｎｏ	導入先	ユニット数	Ｎｏ	導入先	ユニット数
1	名古屋市役所	8,200	4	関東の某市役所	1,400
2	日産フィナンシャルサービス㈱	2,400	5	東海の某市役所	1,300
3	会計検査院	1,400	6	名古屋の不動産会社	1,000

3　会社情報システムへのＳＢＣ方式の適用
（第６章関連）

みずほインベスターズ証券㈱の顧客情報に関わる情報システムにＳＢＣ方式を導入し、内部情報漏えい防止をした。3000IDのシステムであり、日本の金融機関では最大規模である。

4　国際業務システムへのＳＢＣ方式の導入
（第７章 関連）

あいおい損害保険㈱の海外事業のリスク管理のため、世界２２拠点の駐在員がリアルタイムかつ安全に業務情報を共有するシステムを世界で初めて実現した。

5　ＳＢＣ方式のプラットフォームサービスの主な利用実績（第８章関連）

Ｎｏ	導入先	ＩＤ数	Ｎｏ	導入先	ＩＤ数
1	マニュライフ生命	1,400	4	クレシア	７００
2	エース損保	1,300	5	日産フィナンシャル	４５０
3	メディサイエンスプランニング	９３０	6	マスミューチュアル生命	２００

報道記事1：
リアルタイムの情報伝達を目的にMetaFrame（注）を導入，みずほインベスターズ証券

本論文　第6章の金融機関への導入事例を示す。

2002年5月17日　［高橋睦美］
出典：http://www.itmedia.co.jp/enterprise/0205/17/02051705.html

（注）ＳＢＣ方式をCitrix社が商品化した商品名

みずほインベスターズ証券は，全国に59支店，約2000人の従業員を抱える証券会社。みずほファイナンシャルグループの一員として，リテールやホールセール，資産運用など

の事業を展開している。

その同社は2001年11月，コールセンターを開設するとともに，顧客情報を一元管理し，店舗とコールセンター，インターネットという3つのチャネルで共有するための新 CRM/営業支援システムの稼働を開始。顧客個々の情報に応じた営業活動や顧客対応に活用している。

同システムの構築に際して課題となったのは，複数のチャネルの間でリアルタイムに情報を共有するためのツールだった。検討を重ねた末，同社が選択したのは，シトリックス・システムズ・ジャパンのサーバベースコンピューティングソフトウェア，「MetaFrame」だった。

CS，Webアプリケーション，MetaFrameの3択

みずほインベスターズ証券の副参事役を務める加納佳明氏は，5月17日，エスシー・コムテクスとシトリックス・システムズ・ジャパンが都内のホテルにて開催した「MetaFrame World 2002」にて，CRMと営業支援の双方の性格を兼ね備えた新システムの構築からカットオーバー，運用に至るまでを紹介した。

みずほインベスターズ証券では以前より，独自に作り込み，ユーザインタフェースに工夫を凝らしたCRMシステムを運用させていた。新システムはこれを拡張し，電話であろうとメールであろうと，あるいは対面の場合でも，すべての顧客情報を一元的に管理し，問い合わせに的確に回答できる仕組みを提供することを目的としたもの。それだけに，情報の一元的な管理とリアルタイム性の確保がポイントとなった。

ここで同社が検討した選択肢は3つあったという。1つは，おなじみのクライアント／サーバ（CS）型システムを採用し，データベースのレプリケーションを各拠点に配置するというもの。2つめは，データベースと連携させたWebアプリケーション。そして3つめが，MetaFrameだ。

同社ではこれら3つの選択肢を，リアルタイム性（パフォーマンス）やユーザインタフェース，既存システムへの影響や運用・管理といった保守面，それに構築に要する期間など，さまざまな側面から検討した。

例えばCS型の場合，従来のインタフェースは維持できるものの，2000台に上るクライアントPCそれぞれでアプリケーションの修正やアップデートを行うことを考えると，手間は膨大なものとなる。また，データベースのレプリケーションによってWAN回線に負荷がかかり，情報のリアルタイム性とレスポンスの両立が難しい。

一方Webアプリケーションを採用すれば，メンテナンス作業はサーバに対してのみ行えばよく，保守面での負担は軽減される。だが従来のアプリケーションと同等のインタフェースをWebブラウザで表現するのは困難だ。しかもその開発，およびチューニングに要する期間も相当に上ると予想された。さらにWebアプリケーションでも，データ量の多い文書を開いたり，検索したりとなると，CS型同様にWAN回線がボトルネックとなる可能性

が高かった。

結果として同社は，MetaFrame を用いて CRM システムを稼働させる案を採用した。もちろん最初に ICA クライアントを配布，導入する必要はあるが，その後のアップデートはサーバサイドで行える。既存のユーザインタフェースをそのまま生かしながらも，回線を流れるのは画面表示のみ。したがって WAN 回線の増強も必要ない。

加納氏によれば，唯一ネックとなったのは「実績の点だった。そのため，まずモデル店舗を２店選び，プロトタイプを導入して検証を行った」と言う。結果は良好だった。

システム構築のポイントは……

現在同社は，NTT コミュニケーションズの IP-VPN 網を用いて本店，支店やコールセンターなど全国 62 カ所を接続。クライアントは，セキュリティを確保した IP-VPN 網経由で，データセンターに配置された MetaFrame Server にアクセスしている。

なおこの MetaFrame Server は，最大で 1750 ユーザが同時に接続しても余裕を持って対処できるよう，35 台のクラスタ構成（コンパックコンピュータ ProLiant DL360 を採用）とした。サーバはギガビットイーサネットで接続され，ロードバランシングを行っている。

加納氏は，「快適なレスポンスが得られており，リアルタイム性のある情報伝達が実現できている。またアプリケーション管理に関しては，修正，変更作業はサーバ側のみで行えるため，特にメリットを実感している」と述べている。

しかも同システムは，コールセンターやインターネット接続の再構築といった他の作業と並行しながら，約５カ月という期間でサービスインに至った。印刷や IME などに関してまだ改善の余地はあるものの，おおむね満足できるシステムに仕上がっていると言う。次のステップとして，このシステムをモバイル環境からも利用できるよう，拡張と認証システムの追加などを進めているところだ。

最後に同氏は，MetaFrame を用いたシステム構築時の留意点に触れた。サイジングやユーザプロファイルの方式，冗長構成やセキュリティといったポイントに加え，加納氏は「事前に十分な試験を行うことが重要だ」と述べている。

「未知の問題点を洗い出すため，１万件以上の単体試験を行ったほか，各支店の協力を得て，本番環境でも機能テストや過負荷試験を入念に行った」（同氏）。

報道記事2:
あいおい損害保険㈱の国際業務システムへMetaFrameを導入

本論文　第7章の導入事例を示す

（2003年6月12日(木)　日本経済新聞掲載）

出典：http://www.ntt.com/ip/news_11/index.html

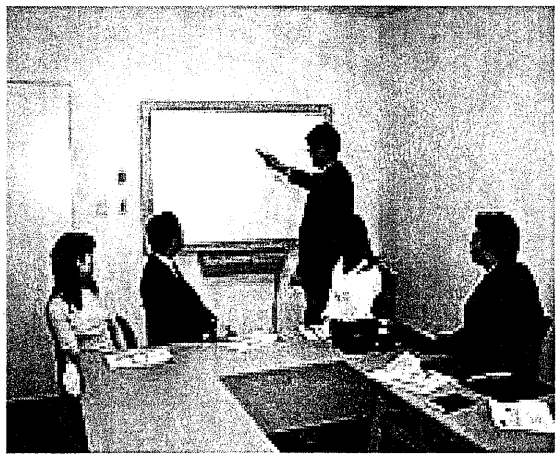
海外事業のリスク管理のために、あいおい損害保険(株)が求めたのは世界22拠点の駐在員がリアルタイムに、そして、安全に業務情報を共有できるネットワークでした。NTTコミュニケーションズは、リモートアクセスサービスと独自のICカード技術を利用することにより、専用線を敷設するときの実に10分の1のコストで、高度な情報秘匿性を持つグローバルネットワーク構築を実現。あいおい損害保険の海外展開における事業費削減に貢献しました。

損害保険事業をグローバルに展開しているあいおい損害保険株式会社（以降あいおい損保）では、世界22拠点の駐在員とリアルタイムでそして安全に業務情報を共有する必要がありました。同社は、事業費削減と顧客サービスの向上を目指し、海外ネットワークインフラ開発にもコストパフォーマンスを徹底的に追求する姿勢で臨みました。この革新的な業務インフラを実現させたのは“Arcstar Remote Accelerator”と“SAFETYPASS”のICカード技術を拡張したNTTコミュニケーションズの「グローバルセキュアNWシステム」です。本システムにより、開発コストの大幅な抑制と、専用線を敷設した場合の約10分の1のランニングコストを達成。さらには万全のセキュリティ対策を実現しています。

万全のセキュリティと大幅なコスト削減の両立

生き残りをかけた業界再編が加速する中、あいおい損保は統合一番手として、平成13年の合併以来、経営基盤の強化と事業の効率化に取り組んで来ました。海外進出においても、自社設立の子会社展開だけにこだわらず、現地の優良損保会社と提携することで、ワールドワイドで質の高い保険サービスを効率的に提供しています。

「従来、海外業務では拠点との情報共有を、ファクス・電子メールや国際郵便に頼っていた」あいおい損害保険株式会社 国際部 欧米グループ 次長 久保田卓氏は述べる。「紙やメールによるやり取りでは、海外から資料や報告書が届くと、それを専任のオペレーターが本社のシステムに手で入力していました。これでは現場と本社で二重の手間になっていることに加えて、入力された情報をチェックする人員も別途必要となっていたのです」と問題を振り返る。　システムの構築を手掛けた同社 国際部 担当課長 野崎知茂次氏は「このような人手やペーパー等の媒体を介する方式では、タイムリーな情報メンテナンスが困難ということもあり、報告漏れの検証にも手間取っていたのが実状。そこで海外駐在員からも情報入力を可能とし、しかもデータベースを一元化することで、合理化と情報精度の向



あいおい損害保険株式会社
国際部 欧米グループ 次長
久保田 卓 氏

上を考えた」と述べる。

「しかし、フロアー端末の LAN 接続や隣の支店とネットワーク接続するように容易な話ではない。当社の海外拠点は、世界 22 箇所に存在する。セキュアにデータをやりとりしなくてはならないとはいえ、全てを専用線で結ぶとなると、莫大なコストとなってしまう」と同氏はグローバルネットの課題を語る。

そこで、同社はコストパフォーマンスの良い回線を利用しながら、安全性確保の為にシステム自体を Web ベースに置き換えた SSL での暗号化を検討した。しかし、Web ベースのシステムに再構築するには、時間と費用がかり過ぎてしまう。さらに高度化した情報管理に耐え得る画面作りが困難である。別方式として、既存のクライアント・サーバ型（CS 型）のシステムを暗号化通信にて拠点接続させることも検討した。だが、送受信されるデータ量が多く、国際間で非現実的な回線帯域を確保する必要があった。「ナローバンドでも利用でき、既存システムの作り替えが少なくて済むターミナルサーバ方式の検討を進めていた時に、IC 認証技術でコストパフォーマンスの高い“SAFETYPASS”の組み込みを提案され、すべての懸案が一気に解決しました」と野崎氏は IC 認証技術を絶賛する。

全員で同じ情報をリアルタイムに共有

あいおい損保が採用したグローバルセキュア NW システムは、海外とのネットワーク遅延を最小限に押さえ、遠隔地からの入力も行っている。入力データそのものを送受信するのではなく、画面情報の変更部分のみを同期させるため、広帯域を必要としないというメリットがある。野崎氏は「専用線以外の回線も利用することでセキュリティに充分配慮した。IC 認証技術と高度暗号化に加え、“Arcstar Remote Accelerator”を用いることで情報秘匿性が更に高まった。もちろんそこには、数多くのグローバルシステムを手掛けている NTT コミュニケーションズのブランド名が大きな安心感につながっています」と、システム採用の理由を語る。

地球の裏側の拠点と通信することで、セキュリティ以外に問題点となるのが、データ遅延の発生である。野崎氏は「開発過程で色々と試しましたが、遅延は各拠点のインフラ整備状況や物理的な距離に左右されます。しかし、“Arcstar Remote Accelerator”は遅延対策も充分考慮されており非常に頼もしい」と感想を述べる。

あいおい損保では、グローバルセキュアNWシステムの導入によって、様々な効果が生まれることを期待している。その一つは、リスク管理の強化である。従来は、多種多様に紙ベースで報告される各種リスク情報を本社・国際部にて、統一フォーマットへ落とし込みを行っていた。国際電話や電子メールで拠点と確認をしながらの作業となり、双方での業務負担が増加傾向にあった。久保田氏は「今後は、同じシステムを全員で利用できるようになったことで、拠点側で従来同様に行っていた作業を、新システムに移行させるのみで、ほぼ入力作業が完結してしまう。むしろ一元化したデータベースやパターン入力の利用により、現場の省力化にも繋がる。もちろん情報活用の場面では、地域別のリスク総量が瞬時に把握出来る等、従来と比較にならない躍進を遂げている」とシステムを評価する。

あいおい損保では同システムを７月まで試験稼動させ、その後本格運用を開始する。今後さらにメニューを追加していくことで、顧客サービスの向上を図っていく考えである。

（この記事内の用語の説明）

Arcstar リモートアクセラレーター:

事業ＬＡＮやリモート端末からＬＡＮ環境へのアクセススピードを、ＬＡＮ端末と同等スピードまで飛躍的に向上させる。ハードウェア&ソフトウェア一体型のサーバユニットのため、導入も管理も容易で、特に、ＳＢＣ方式（(別紙：用語説明(1)）である MetaFrame の性能を安定的に最大限に引き出せるように最適化されており、独自に開発したセッション管理システムを搭載している。

セーフティパスビジネス:

企業とその社員間(BtoE)や企業間(BtoB)、事業会社とその代理店・販社などの特定会員間における情報のやり取り並びに決済を、ＩＣカードと最先端の暗号化技術(IPSec)（別紙：用語説明(15)）を用いて極めて安全性高く、簡便に実現できるハイセキュアな認証・接続サービスである。ＩＣカード社員証としても利用可能である。

（別紙）

本論文で述べる技術の説明

1 用語説明

（1）サーバベースコンピューティング（ＳＢＣ：Server Based Computing）方式

クライアントパソコンとネットワークを介したサーバとのやり取りを、「マウスクリック」、「キーストローク」、「画面遷移の処理」に限ることで、速度の向上や、各種の制限の解消などのメリットを得ようというものである。クライアントパソコン内のハードディスクを用いないことがセキュリティを高める要因である。この方式は、一般的に、“シンクライアントソリューション”や“ＳＢＣ方式を Citrix 社が商品化した商品名であるメタフレーム（MetaFrame）”と呼ばれることがある。

（2）ウェブコンピューティング（Web Computing）方式

クライアントサーバ方式の問題点を解決するためにできた、Web サーバとインターネットブラウザを利用したクライアントパソコンを用いた業務処理方式である。Web サーバとクライアントパソコンの両方で情報処理が行われるしくみである。方式上、セキュリティと処理の高速化の課題がある。

（3）クライアントサーバ（ＣＳ：Client Server）方式

クライアントパソコンで処理実行の都度クライアントパソコンのハードディスクへソフトやデータがサーバからダウンロードされて処理が行われる方式である。処理の都度ダウンロードが発生するため、クライアントパソコンの性能や、クライアントパソコンとサーバを結ぶネットワークの帯域幅にパフォーマンスが大きく左右されるという構造的な問題をかかえている。また、クライアントパソコン毎にプログラムをインストールしなければならないという保守面の負担も問題である。

（4）ＵＳＢ（Universal Serial Bas）キー

パソコンのＵＳＢインターフェースを持つセキュリティデバイスのことである。デバイス内にＩＣチップを持ち、パソコンのミドルウェアと連携してセキュリティ機能を果たすものである。装着している間だけネットワークへのログオン、暗号化領域へのアクセスなどを可能とする手軽なセキュリティツールである。「所持」による本人認証のみならず、パスワードを入力要求する PIN（Personal Identification Number）コード

（次項）による「記憶」や指紋認証等との抱き合わせを行うものも、商品化されている。

（5）PIN（Personal Identifier Number）コード

銀行カードの番号や社員番号あるいはシステムに対応した暗証番号で加入者確認のために使用する識別子（暗証番号等）として使われる。ＵＳＢキーやＩＣカードに内蔵され、所持認証と記憶認証の組み合わせで使用されるケースが多い。

（6）バイオメトリックス（Bio Metrics:生体）認証

本人の身体的特徴から本人を特定する技術である。指紋、声紋、手のひら静脈、筆跡、掌紋、DNA，虹彩、頭の形などの本人の特徴を認識して認証するものである。

（7）シンクライアント（Thin Client）方式：

ユーザ側端末の CPU・Memory・HDD などはすべてサーバ側に実装され、ユーザ側にはデータ・アプリケーションを置かない端末を用いる方式のことを指す。シンクライアント側メリットとしては、セキュリティ強化、可用性の向上・最適なオフィス環境の実現があげられる。（1）項の SBC 方式もこの一つで、以下の（8），（9），(10)項を含めた４つの方式がある。

（8）ブレード（Blade）PC 方式：

パソコンを構成するために欠かせない CPU・Memory・HDD などの主要な部品を、１枚のブレード（基盤）に集積し、マシンルームにまとめて設置することで、安全な情報管理と運用のトータルコスト削減を実現するクライアント PC 一元管理システムのこと。クライアントには「マウスクリック」、「キーストローク」、「画面遷移の処理」の情報に限ることで、セキュリティを高めるコスト削減を図る方式のことである。

（9）ストレージセントレックネットワーク（SCN:Storage Centric Network）方式

クライアント端末は起動時にセンタのストレージ上の OS、AP にアクセスして、起動後は各端末上の CPU、メモリを占有して使用する方式のことである。ネットワークへの負荷がかかる難点があるが、可用性が高い方式である。

(10) サンレイ(Sun Ray)方式：

各端末では、サーバ側の CPU、メモリをシェアして使用し、画面データ、キー入力データが、ネットワーク上で転送される UNIX 版の方式である。

(11) ICA（Independent Computing Architecture）通信（プロトコル）

ＳＢＣ方式のうちMetaframeと呼ばれる方式で使われているＳＢＣサーバとクライアントPC側のパソコン端末の間で利用される通信方式のこと。マウス情報、キーボード情報、ディスプレイ情報が通信される。ICA プロトコルはこの通信で使われるＳＢＣ方式を実現するために開発された、分散Windowsプレゼンテーション・プロトコルである。もともと、細い回線でも快適なパフォーマンスを実現するために開発されたプロトコルであるため、電話回線など平均約20kb/sしか使用しないという狭帯域を使ったアクセス時にその威力を最大限に発揮する。

(12) インターネットVPN（Virtual Private Network）

インターネットを用いて、認証や暗号化の技術により、他者が侵入しないような通信のパイプを設定して、その中を専用線的に企業などの通信で使おうとする安価な通信方式である。

(13) サービスレベルアグリーメント（SLA：Service Level Agreement）

サービス提供業者がお客にサービスを提供するに当たって、そのサービスの品質を契約として規定するもの。回線サービス業者であれば、エラー率、不稼働率という品質レベルを規定し、その品質を下回った場合のペナルティを契約項目としている。

(14) マルチホーミング（Multi-Homing）技術

インターネットサービスプロバイダ（ISP）を複数契約し、広帯域化とロードバランシングによる負荷分散や信頼性確保を行う。たとえば一方のISPのスループットなどの品質にネックが発生した場合、他方のISPで品質劣化をカバーするような目的で利用される。コストを安くバックアップを実現できるのがポイントである。

(15) IPSec（IP Security）プロトコル

TCP/IPレベルで通信経路の暗号化を行うプロトコルの一つであり、インターネットを介してデータをやり取りする場合に、外部のユーザにもそれらのデータを盗まれる可能性が出てくるため、通信経路を丸ごと暗号化する方法のこと。IPSecであれば、アプリケーションに依存することなくできてしまうので、業務で使用する独自アプリケーションなどのデータも安心して送ることができる。

(16) 公開鍵（PKI:Public Key Infrastructure）認証

公開鍵基盤（PKI）を用いた認証方式である。公開鍵暗号方式を利用して、暗号化して送られたデータが公開鍵で復号できる性質を利用して認証を行う方法のことである。

(17) NAT（Network Address Translation）アドレス

インターネットのグローバル IP アドレスとプライベート IP アドレスを相互変換するための技術である。1 つの IP アドレスを複数の端末で共有することができるが、複数の端末が同時にグローバル IP アドレスを利用することはできないという欠点がある。この欠点は IP マスカレードで解消されている。

(18) SQL（Structured Query Language）通信

データベースのデータの検索や変更、削除といった処理を行うための言語を用いた通信のことである。SQL に対応した代表的なデータベースサーバには、Oracle、Microsoft SQL Server、Adaptive Server などがある。

(19) ACL（Access Control List）設定

ユーザやグループに対して、ファイル、ディレクトリ、およびそのほかのリソースへのアクセス許可が定義されたデータのセットのことである。Active Directory サービスでは、保護対象のオブジェクトに格納されるアクセス制御エントリ（ACE）のリストを ACL とよんでいる。

(20) NTP（Network Time Protocol）プロトコル

ネットワークを介してコンピュータの内部時計を設定するためのプロトコルである。定期的に NTP サーバに対して時刻の参照を行ない、コンピュータの内部時計を正常に設定する役割を持っている。

(21) ドメインコントローラ（Domain Controller）

ユーザやアプリケーションによる認証や検索といった要求に応えるサーバのことで Active Directory のデータベースを保持している。Windows NT 4.0 までのドメインコントローラには，PDC と BDC という 2 種類が存在し，情報の変更は PDC に対してしか実行できなかった。しかし，Windows 2000 におけるドメインコントローラは 1 種類であり，いつでもドメインコントローラに昇格させたり降格させたりすることができる。

(22) SIP（Session Initiation Protocol）プロトコル

VoIP（Voice over IP）などの世界で広く用いられるようになりつつあるシグナリングプロトコルで、IETF (Internet Engineering Task Force) で標準化が行われている。IP 電話、ビデオ会議などを実現するプロトコル(RFC3261)でテキストベースのためシンプルで拡張性が高いことから、IP 電話の標準的なプロトコルとして主流となりつつある。

2 技術説明（システムの要素別のセキュリティ技術の説明）

2.1 ネットワーク・インフラから見た情報漏えい技術

（1） アクセス制御

レイヤ2/3/4の情報を元にしてアクセス制御を行う。IPファイアウォール、またはネットワーク機器のアクセス制御機能が代表的である。

（2） 暗号化

データを暗号化することにより、IPの通信をセキュアに行う。そのための技術としては、IPSecやSSLなどがある。同一インフラ上に複数のトラフィックをセキュアに運ぶ技術として重要な役割を果たす。

従来はネットワーク機器を設定監視するために、TELNETやSNMPおよびHTTPが使用されてきた。これらはクリア・テキストであるため、最近はSSH、SNMPv3、HTTPSなどといった新しい技術が実装された機器も増えてきている。

（3） 侵入検知システム

侵入検知システム（IDS）はもともとリアルタイムに不正アクセスを検知するシステムである。インフラとしてのIDSは、すべてのパケットを監視し、ネットワーク経由の侵入や攻撃を検知する方法である。スイッチやルータのトラフィックを監視するために、ポート・ミラーリングですべてのパケットをIDSにフォワードする場合が多い。

（4） ユーザ認証（ネットワーク認証、VLAN、DHCP）

以下では、レイヤの低いほうから順に説明する。

① ネットワーク加入のための認証

ダイヤルアップ・リモートアクセス・サーバによる認証が代表的である。認証サーバは通常RAIDUSサーバを用いる。従来のLANネットワークは、接続すればだれでもが利用できるものが一般的だったが、LANにおいても接続時の認証のニーズが高くなっている。 たとえば、IEEE802.1XによるEAP認証はネットワーク認証の標準プロトコルであり、無線LANのアクセス・ポイントやLANスイッチなどに実装されはじめている。基本的には、ポートへのアクセス制御である。

② DHCPサーバからのIPアドレス配布による認証

DHCPサーバは、クライアントからの要求に対して、自動的にIPアドレスを割当

てる。標準仕様では認証がないため、通常は端末からリクエスト送信すると不特定多数の端末にIPアドレスが割当てられる。しかし、IPアドレスの配信にユーザ認証を手順に加えることにより、IPアドレス配布による認証が可能となる。

③ ファイアウォールを通過するための認証

ファイアウォールを通過するパケットに対して、ルールを適用する前にユーザ認証を用いることにより、処理の簡素化とセキュリティの向上が可能となる。これらを全て自社で用意するとなると、専任の担当者を配置し、その担当者の人件費と教育費などコストも考慮する必要があるため、昨今はサービス・プロバイダやシステム・インテグレータが、セキュリティのアウトソーシング・サービスを提供している。これらを利用することによって管理コストの低減が望めるが、その反面、外注による社内情報の流出の恐れも懸念事項となる。

2.2 アプリケーションから見た情報漏えい技術

情報漏えいに対する対策としては、以下のように2つの考え方がある。（図3）

ブロッキング： コンテンツ（情報）にアクセスする人を限定する。
トラッキング： コンテンツ（情報）にアクセスした人の履歴を残す。

（1） ブロッキング

ブロッキングでは、アプリケーションを利用する人を限定する機能を付加することにより、不正に対する防止機能、検出機能を発揮する。

① 認証

人を特定する認証により、情報にアクセスする人を限定する。その方法としては、ID／パスワードを使用するケースがもっとも一般的である。多くの業務システムや、特定ユーザのみにサービスするシステムのほとんどは、認証機能を有している。

利用するシステムが多くなっていくにつれ、一人のユーザが複数のIDとパスワードを管理する必要が出てきている。これに伴い、IDとパスワードの管理がずさんになっていることが多い。そのため、シングル・サインオンと呼ばれる製品も見られるようになってきた。これと同時に管理側の問題として、ユーザ管理を統合する動向が進みつつある。また、より個人を厳密に特定する方法としてワンタイム・パスワード、デジタル証明書、バイオメトリクスによる認証も用いられるようになった。

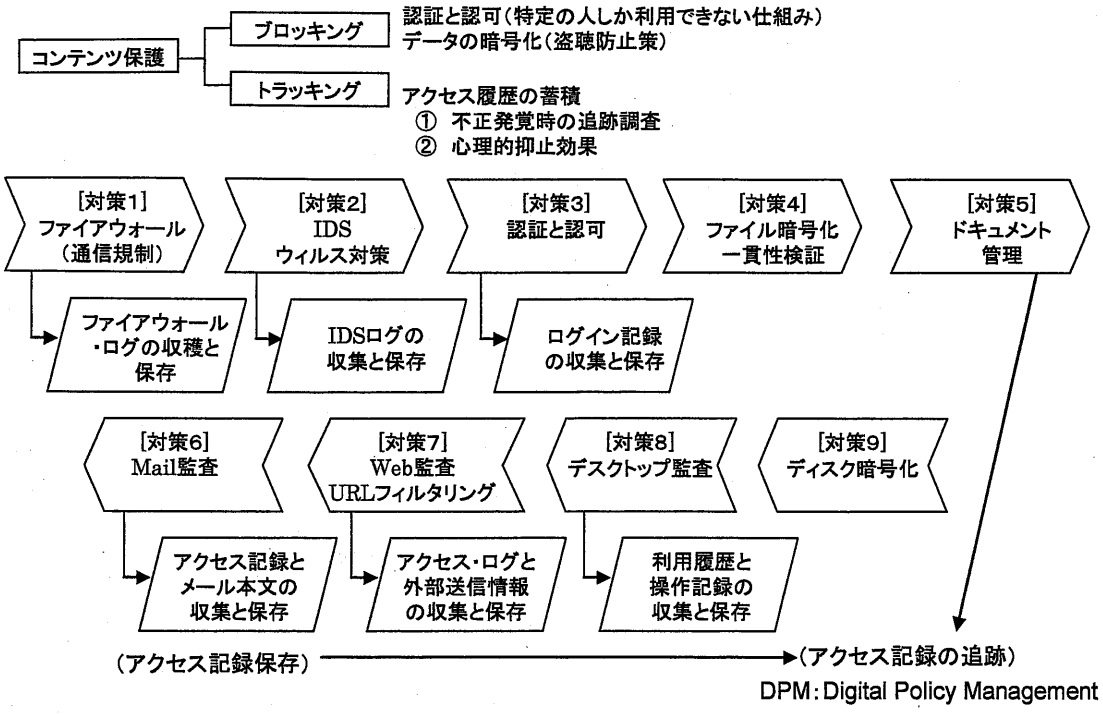


図1 コンテンツ保護の方策

Fig.1 The contents of the protection methods.

② 認可

個人に対して利用できる情報を特定するという、認可またはアクセス・コントロールがある。これは、認証された他人の情報を勝手に改ざん、持ち出しされないために実施するものである。たとえば、ある情報（ファイル、Web ページなど）に対して、参照や更新、削除などの権限を、ユーザの資格に応じて許可するなどの制御を行う。

③ 暗号

前述の手段にさらに取るべき対策として、情報に対するデータ保護や、盗聴の防止のためにデータの暗号化を行うこともある。具体的には、ファイルの暗号化、通信データの暗号化、メールの暗号化、などがある。

（2） トラッキング

トラッキングでは、アクセス履歴やアクセス・データを蓄積、保存することにより、不正に対する抑止機能（監視されているという心理的抑止機能）や検知機能（不正発覚時の追跡調査が可能）を有する。

① アクセス・ログ（システムで管理される情報）の蓄積

イベント・ログ、SYSLOG、アカウンティング・ログなどを管理、保存することにより、不正を検出するものである。

② アクセス・データ（利用者が使用するデータそのもの）の蓄積

メール、外部送信データなどのデータそのものを蓄積することにより、不正発覚時の追跡調査を可能にするものである。

2.3 サーバにおける情報漏えい技術

（1） アプリケーション・サーバでのセキュリティ対策

一般のアプリケーション・サーバの場合、それぞれの機能に対して機密レベルによって異なる。一般に公開されている Web コンテンツのように、だれでもアクセスを許可し、個人情報などが流れにくいサーバであれば、アクセス・ログのみの機能しか有しなくてもよい。

しかし、業務アプリケーションといった、個人を特定する必要があり、なりすましなどのリスクを伴うサーバであれば、認証、認可、データの暗号化、アクセス・ログの蓄積などの機能を有する必要がある。また、最近では、DRM と呼ばれるコンテンツ自体に保護をかけ、コピーの禁止や印刷の禁止、参照可能な有効期限を管理するなどの対策がとられるようにもなってきている。

（2） メール・サーバでのセキュリティ技術

情報漏えいにおける手段として、電子メールが悪用されやすいこともあり、最近では非常に多くの企業でメール・データの監査製品の導入が進んでいる。これらの監査製品は、メール情報を添付ファイルを含めすべて履歴として残す機能や、メールのキーワードにより送信を拒否、あるいは配送ルートを変更して送信する機能を有している。

（3） 外部の Web アクセス制御技術

Web 監査製品では、ユーザごとにどこの Web サーバにアクセスしているのかの履歴を収集してレポートする機能や、http コンテンツに対するウィルス・チェックなどを行う。http コンテンツ監査機能は、http 送信内容をキーワードで検索し、フリーメールやチャット、掲示板への書き込みなど、機密情報や不適切な情報と思われる情報が外部に送出されるのを防ぐ。また、レポート機能では、検索エンジンに入力されたキーワードの一覧、Web 利用の多い端末、外部転送の多い端末、大量データのダウンロードを行った端末などをレポートすることができる。

2.4 デスクトップ環境における情報漏えい技術

（1） ログオン認証によるディスクの暗号化

最近のノートPCは、持ち歩きが容易になり、利便性が向上してきたが、一方でその利便性の故に、紛失、盗難などのリスクを伴ってしまう。その対策として、パソコンの起動時に認証を行い、ディスクの全部または一部を暗号化しておくことによって、たとえ盗難にあっても情報を盗み出されることのないような対策を講じるようになってきた。また、このような製品を導入しておくことにより、故障などによる廃棄においても、その内容が外部に漏えいしにくくなる。製品としては、部分的な暗号化の機能をもつものから、ディスク全体を暗号化し、認証が行えなければOSすら起動しない製品もある。また最近のパソコンでは、BIOSによりパスワードを入力しないと起動しないシステムも多くなっている。

（2） デスクトップでの監査技術

情報に対するアクセス履歴は、一般にサーバ側で取得するものであるが、サーバ側でのアクセス履歴の取得内容については、サーバ側のシステムに依存し、取得可能な情報も限られる。さらに、クライアント間の通信による履歴情報も取得することができない。そこで、クライアントPC側で監査情報を収集できる製品がある。

このようなクライアント側の製品については、今まではセキュリティ対策だけで利用者パソコンへのソフトウェア導入は避けられてきたが、CPU、メモリ、OSの性能など利用環境も充実され、ウィルス・プログラムなどの導入も一般的になってきたこともあり、以前に比べて導入に抵抗感はなくなってきた。また利用者にとっても、利便性が向上する機能を付加することにより、以前よりも、かなり導入しやすくなっている。機能としては、クライアント側にエージェント・ソフトを事前に導入することにより、デスクトップ環境で利用したアプリケーション、利用したファイル、利用時間などの統計情報をサーバで管理することが可能となる。