昭和37年9月15日第三種郵便物認可　三菱電機技報　78巻4号（通巻875号）　2004年4月25日発行（毎月1回25日発行）

Changes for the Better

MITSUBISHI

三菱電機技報

Vol.78 No.4

2004 4

特集「安全・安心を支えるITソリューション」

ISSN　0369-2302　CODEN:MTDNAF

三菱電機技報 Vol. 78 No.4 2004

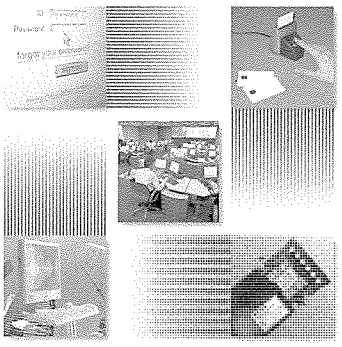
目　次

表紙

安全・安心を支えるITソリューション

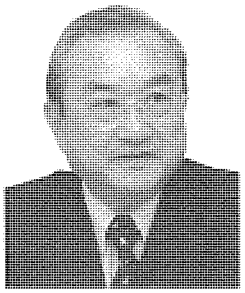
お客様情報システムの安全・安心を支えるITソリューションとして，この特集号では，“セキュリティ”と“高信頼性”に配慮した各種ソリューションを紹介しています。

この特集号の表紙では，従来からのID・パスワードによる個人認証に加え，ICカード(公開鍵(かぎ)基盤PKIに基づく電子証明書発行なども含む)や生体認証，耐タンパ(不正読み取り改ざん防止)セキュア装置，サーバベースコンピューティング(SBC)などを組み合わせた最新ソリューション技術や，大規模システムの二重化・運用監視・不正アクセス監視などの高信頼サービス技術により，お客様に安全かつ安心してご利用いただける情報システムをイメージしています。



巻/頭/言

安全・安心を支えるITソリューション特集に寄せて



中央大学理工学部情報工学科

教授　土居範久

経済産業省は2003年10月10日に「情報セキュリティ総合戦略」を発表した。基本目標は，世界最高水準の“高信頼性社会”の構築である。

これまで我が国の情報セキュリティ政策は経済産業省を中心として進められてきており，ISO/IEC15408に基づいたIT製品及びシステムの評価・認証制度を2001年4月から独立行政法人製品評価技術基盤機構を中心に創設し(運営委員会委員長：土居範久)技術的な対応をとるとともに，2002年4月からはISO/IEC17799とBS7799-2に基づいたISMS認証制度を情報処理開発協会を中心に開始し(運営委員会委員長：土居範久)マネジメント的な対応をとっている。我が国は2003年10月31日にCC(Common Criteria)承認アレンジメントへの加盟が認められたことから，我が国の企業は，CC承認アレンジメント参加諸国の政府調達に応じる際には，我が国のIT製品及びシステムの評価・認証制度に基づいて我が国で認証を取ればよく，産業界の活性化に役立つと期待している。ISMS制度の国際間での相互承認も英国との間で目下交渉中である。

これらの制度に加え，2003年4月には情報セキュリティ監査制度が経済産業省告示として発表され，10月10日にはこの制度の普及啓蒙を図るために特定非営利活動法人日本セキュリティ監査協会(会長：土居範久)が設立された。この制度は，ISMS制度が原則として127のコントロールについて包括的に監査・評価し認証するのに対し，コントロールを部分的に選択でき，保証だけでなく助言を与えることができるようにしたところ及び業種・業態ごとにカスタマイズできるところに特徴があり，ISMS制度の裾野を広げる制度である。これらを活用して，防衛庁では，37のコントロールを選び，独自のカスタマイズ化を進めている。また，総務省は，地方公共団体向けにカスタマイズしたものを12月25日に発表し，全国の地方公共団体がそれぞれの実情に応じた形で適切な情報セキュリティ監査に取り組むことを薦めている。

このように，順次，制度は整いつつあるが，いわば場当たり的に進められてきたところもあることから，情報セキュリティ政策を国家的な見地から見直し総合的に立てた戦略が「情報セキュリティ総合戦略」であり，経済・安全保障問題有識者，経営者，研究者からなる“産業構造審議会情報セキュリティ部会(部会長：寺島実郎)”と最前線のセキュリティ技術者，研究者，弁護士，自治体関係者などからなる“情報セキュリティ総合戦略策定研究会(委員長：土居範久)”との間でキャッチボールしながら集中的に検討し練り上げたものである。①しなやかな“事故前提社会システム”の構築(高回復力・被害局限化の確保)，②“高信頼性”を強みとするための公的対応の強化，及び③内閣機能強化による統一的推進を戦略の軸としており，国・自治体，重要インフラ，企業・個人に大別し，それぞれのセキュリティの向上を目指した42の具体策を提案している。①は“情報セキュリティに絶対はない”との前提の下で，事故の回避(予防)・被害局限化・回復の最適化を図った対応の徹底化を図る戦略であり，②は“高信頼性”を強みとするため，国家的視点から，技術基盤・制度基盤両面にわたる公的対応を強化する戦略である。最も重要で喫緊の課題である③内閣機能の強化から始め，これらの戦略が早急に実施に移されることを切に期待するとともに，これらの戦略の技術的側面を支えるITソリューション研究の更なる推進を期待する。

巻頭論文

三菱電機情報セキュリティソリューション


勝山光太郎*


小松田敏二**


飯島康雄***

要　旨

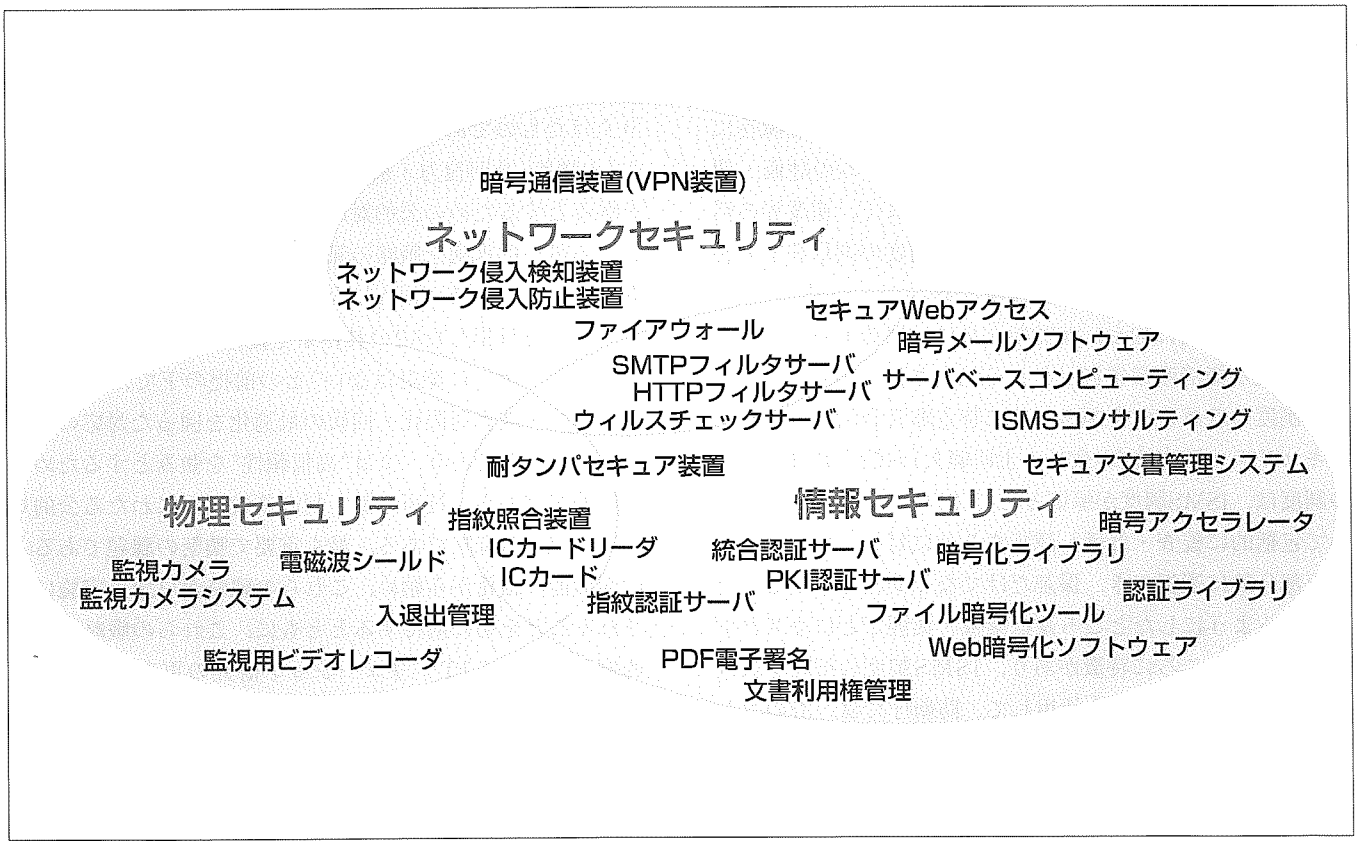
インターネットを代表とするいわゆるIT化の進展により，企業はビジネスリスクの一つとして，ITリスクとりわけ情報セキュリティリスクを考慮した経営を迫られている。

近年，マスコミで取り上げられることが多くなってきている個人情報の漏洩(ろうえい)事件や，MS-Blasterなどのウイルスにより情報システムがダウンするなどのリスクをどうコントロールしていくかが重要となる。さらに，法制度の面では，個人情報保護法や不正競争防止法において，情報の管理責任という意味で情報セキュリティ対策の実施がうたわれている。

情報セキュリティ対策を実施し情報資産を守るためには幾つかの側面があり，単に技術的側面だけでなく，設備や運用といった側面からもトータルにセキュリティ対策を実施することが求められている。経済産業省が2000年10月に発表した「情報セキュリティ総合戦略」においても，こうした観点から，ISMS(情報セキュリティマネジメントシステム)やセキュリティ監査の重要性が述べられている。

三菱電機グループでは，情報セキュリティ，ネットワークセキュリティ，物理セキュリティを連携させたトータルな取り組みをしており，お客様のニーズに合ったトータルセキュリティソリューションを提供している。本誌2002年4月号[1]では，“情報セキュリティ技術”を中心に，2003年4月号[2]では“ユビキタス社会に向けたセキュリティへの対応”を紹介してきたが，今回の特集号では“情報セキュリティソリューション”に焦点を当てて紹介する。

“情報漏洩防止ソリューション”や“公開鍵(かぎ)基盤PKI(Public Key Infrastructure)による認証サービス”など，安全・安心を支える多彩なソリューションがあり，経営リスクに対応した体系的対策・運用を可能としている。



三菱電機のトータルセキュリティ

三菱電機㈱は，情報セキュリティ，物理セキュリティ，ネットワークセキュリティのいろいろなコンポーネントを組み合わせ，お客様のニーズに合ったセキュリティソリューションをトータルに提供する。

*三菱電機㈱ 情報技術総合研究所 情報セキュリティ技術部長(工博)　**同社 インフォメーションシステム事業推進本部 情報セキュリティ推進センター長
***三菱電機インフォメーションシステムズ㈱ インターネットビジネスシステム部 インターネットセキュリティセンター長

1. まえがき

インターネットを代表とするいわゆるIT化の進展により，企業はビジネスリスクの一つとして，ITリスク，とりわけ情報セキュリティリスクを考慮した経営を迫られている。

個人情報の漏洩事件では，企業に対する損害賠償請求が起きたり，経営者の責任が問われることになる。また，MS-Blasterなどのウイルスにより情報システムがダウンするなどのリスクや，ネットワークからの不正侵入などのリスクは増大の傾向にある。

また，法制度は，システムの運用管理者やデータの利用者に責任を負わせる方向になってきている。

したがって，体系的に情報セキュリティ対策を導入し運用するために，ISMS(情報セキュリティマネジメントシステム)を実施し，認定をとる企業も増えてきている。

こうしたセキュリティ意識の高まりを背景に，今回の特集号では，安全・安心を支えるITソリューションと題し，三菱電機グループが取り組む情報セキュリティや物理セキュリティに関して幾つかの例を紹介している。採録されている論文の中には直接セキュリティに関連するものもあれば，セキュリティや高信頼に配慮したソリューションとして紹介しているものもある。

2章では最近のセキュリティに関するトラブルの例を取り上げ，**3章**では世の中の動きとしてOECD(世界経済協力機構)の情報セキュリティガイドラインや法制度，特に個人情報保護法及び不正競争防止法に関して述べる。**4章**ではISMS(情報セキュリティマネジメントシステム)，**5章**では当社のトータルセキュリティについて述べ，**6章**では情報セキュリティソリューションの中の幾つかの事例を紹介する。

2. 情報セキュリティに関するトラブル

情報セキュリティに関するトラブルは，セキュリティの3要素(機密性，完全性，可用性)と関連付けると以下のようになる(**表1**)。

(1) 機密性

機密情報漏洩，個人情報漏洩，不正アクセス

(2) 完全性

ホームページ改ざん

(3) 可用性

DoS攻撃(サービス不能攻撃)，ウイルス・ワーム

3. 世の中の動き

3.1 OECD情報セキュリティガイドライン

2002年にはOECDから情報セキュリティガイドラインが出され，その中では主に次のことが述べられている。

(1) 情報システム及びネットワークを保護する手段として，すべての参加者の間にセキュリティの文化を普及させること。

(2) 情報システム及びネットワークに対するリスク，それらのリスク対処のために有効な方針，実践，手段及び手続き並びにそれらの導入及び実施の必要性について認識を高めること。

(3) すべての参加者の間に情報システム及びネットワーク利用の形態における一層大きな信頼を醸成すること。

3.2 個人情報保護法及び不正競争防止法

法律がシステム運用者やデータ利用者に責任を負わせる方向になってきている。

具体的には，個人情報保護法では以下のような条項があり，何らかのセキュリティ対策実施を義務付けている。

個人情報保護法 第20条(安全管理措置)

「個人情報取扱事業者は，その取り扱う個人データの漏洩，滅失又は棄損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」

また，不正競争防止法でも次のような条項があり，何らかのセキュリティ対策が必要となる。

表1．情報セキュリティにかかわるトラブルの事例

要素	時期	対象	トラブル内容
ホームページ改ざん	2001/1	日本政府	科学技術庁，総務庁，総合研究開発機構(NIRA)，運輸省のWebサイトが相次いで改ざんされた。
	2003/3	米企業等	イラク攻撃に伴い，米国のWebサイトを中心に大量の改ざん。日本国内でも数例の事例。
不正アクセス	2002/2	宇宙関連	超高速インターネット衛星の受注に当たり，ライバル会社の機密情報を不正に入手。
	2002/8	宇宙関連	愛知県知立市の会社員所有のパソコンを踏み台にしたクラッキングを受けた。
ウイルス・ワーム	2001/7	全世界	"Code Red"ウイルス
	2001/9	全世界	"NIMDA"ウイルス
	2003/1	全世界	"SQL slammer"による被害。韓国では一時インターネットに障害も。
	2003/8	全世界	"MS-Blaster"ウイルス
DoS攻撃	2002/10	Root DNS Server	DoS攻撃を受け，13台のRoot DNS Serverのうち9台が機能低下。
機密情報漏洩	2002/8	防衛	防衛庁のシステムの，開発資料の一部が流出。
個人情報漏洩	1999	個人	宇治市で住民基本台帳の記載事項が流出。
	2002/5	美容	約37,000人の個人情報が流出。
	2002/5	製造	約45,000人の個人情報が流出。
	2002/8	食品	約50,000人の個人情報が流出
	2002/11	証券	約11,000人の個人情報が流出
	2002/11	個人	ウイルスにより，茨城県つくば市が運営するメーリングリストから個人メールアドレスが流出。

DoS：Denial of Service，DNS：Domain Name System

不正競争防止法 第14条(罰則)

(2003年の改正：営業秘密侵害に関する刑事罰の導入)

「秘密漏洩に対する対策を講じている企業から営業秘密を不正競争目的で取得・使用・開示する行為に対し，刑事罰（親告罪)を導入する(但し，秘密漏洩に対する対策を講じていない企業は，対象外)。」

ここでいう営業秘密は，秘密管理性，有用性及び非公知性という3要件をすべて満たす必要がある。秘密管理性の判断基準として以下の点がある。

(1) 当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること。

(2) 当該情報にアクセスできる者が制限されていること。

つまり，何らかの認証とアクセス制御が必要ということである。

4. ISMS(情報セキュリティマネジメントシステム)

3章で触れた法律にもあるように何らかのセキュリティ対策をすることが義務付けられているが，どこまでどのようにしたらよいのか分からないという企業が多いのが現状であろう。

そこで，セキュリティ監査を実施し，ISMSを構築し実践していくのが，大多数の企業がとる道と思われる。

情報セキュリティマネジメントの実施サイクルを**図1**に示す。基本方針や目標，実施規定，実施手順などを策定する。それを実際に導入する。そこでは教育や実際の対策(人的な面，設備的な面)を実施する。さらに運用では，実際に規定や基準どおりに運用されているかを監視し，事故があった場合には決められた対策を実施する。そして，内部監査等で実施状況を評価し，見直しを実行し，より高いセキュリティレベルへと向上していくサイクルとなる。

5. 三菱電機のトータルセキュリティ

三菱電機㈱では，要旨のイメージ図に示すように，単に情報セキュリティのソリューションのみならず，物理セキュリティ及びネットワークセキュリティを総合電機メーカーである特色を生かし，トータルに提供している。この章では，物理セキュリティとネットワークセキュリティについて簡単に触れ，**6章**で情報セキュリティソリューションの幾つかを紹介する。

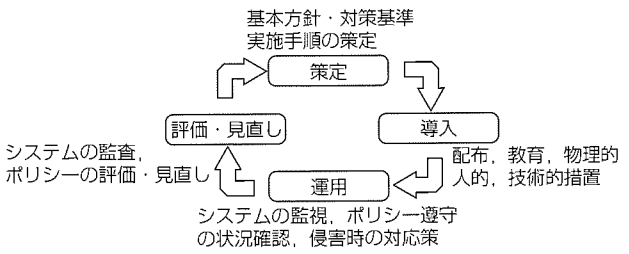


図1．情報セキュリティマネジメント実施サイクル

5.1 物理セキュリティ

物理セキュリティのコンポーネントとしては，本来建物への侵入を監視するなどの防犯や，広域の状況監視などに利用される監視カメラや監視用ビデオレコーダなどの製品がある。盗聴防止といった観点から，電磁波の漏洩を防止するペルセウスシールドといった製品もある。

ビルやオフィスなどの入退出管理では，ICカードや指紋認証などを利用した製品がある。特にビル向けの製品であるMELSAFETYは，高いシェアを持っている。

5.2 ネットワークセキュリティ

(1) 暗号通信装置(VPN装置)

VPN(Virtual Private Network)装置は，IPSECv2(Internet Protocol Security Version2)準拠で，暗号アルゴリズムとして米国標準暗号／認証アルゴリズムに加え，MISTY(注1)，Camellia(注2)をサポートしており，さらに暗号アルゴリズムのカスタマイズの要求にもこたえられる。

(2) IDS装置

IDS(Intrusion Detection System)装置は，ファイアウォールなどと組み合わせ，ネットワークからの不正侵入を検知し，防御する。侵入パターンであるシグニチャを管理装置から一元的に更新できるなどの特長がある。

(3) マネージドセキュリティサービス

セキュリティは，構築して完了ではなく，むしろ，スタートである。日々のセキュリティ監視，新たな脆弱(ぜいじゃく)性への対応，システム変更時のセキュリティチェックなどによって，セキュリティは維持される。三菱電機情報ネットワーク㈱(MIND)は，調査分析から，設計，導入，運用・監視及び評価というサイクルに対応したトータルなマネージドセキュリティサービスを提供している(**図2**)。米国RedSiren Technologies社(旧SRIコンサルティング社)との提携等で常に最新情報をサービスに反映し，24時間365日の統合管制センターICC(Integrated Control Center)をベースに絶え間ないサービスを提供している。

(注1) MISTYは，三菱電機㈱の登録商標である。

(注2) Camelliaは，日本電信電話㈱と三菱電機㈱の登録商標である。

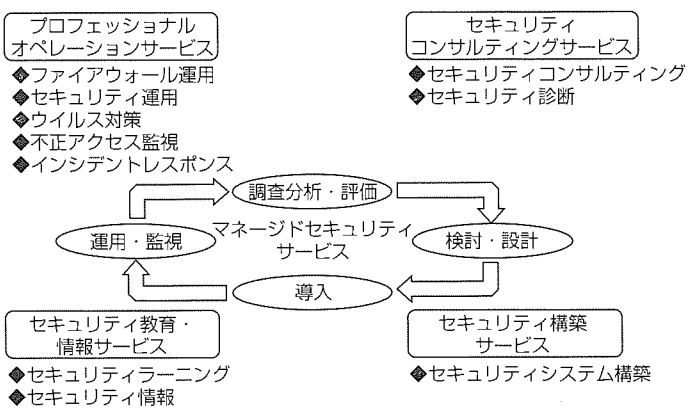


図2．MINDマネージドセキュリティサービス

なお，MINDでは，BS7799-2(情報セキュリティ管理システム仕様／認証規格)の認証を取得し，情報セキュリティマネジメントシステムの確立・維持によって，信頼されるサービスを提供している。以下に代表的なサービスを紹介する。

(a) セキュリティ診断サービス

システムのセキュリティ状態を擬似攻撃によって診断する。三菱統合セキュリティ診断ツール(ISAT)を使用したクロスサイト・スクリプティングによる脆弱性チェックなど，Webアプリケーションまで踏み込んだ診断も行う。診断結果は検出した脆弱性の対策も提示している。

(b) セキュリティ教育・情報サービス

初心者から専門家までに対応した総合的な情報セキュリティのeラーニングサービスを用意している。また，日々公開されるセキュリティ情報を複数の情報ソースからシステム管理者に代わって対象システム要件を踏まえて収集・分析し，その対処と合わせて提示している。

(c) 不正アクセス監視／インシデントレスポンスサービス

もはや，ファイアウォールだけではセキュリティを維持できなくなっているため，セキュリティホールへの攻撃を不正アクセス監視装置によって24時間監視を行う。万一の緊急事態発生時には，原因究明から対処までのインシデントレスポンスにも対応している。

6. 情報セキュリティソリューション

情報セキュリティソリューションも各種存在するが，ここでは，個人情報保護法の関連で注目を集めている“情報漏洩防止ソリューション”，そして，公開鍵基盤PKIについてヘルスケア分野を例として述べ，さらに，“セキュアWebソリューション”を紹介する。

6.1 情報漏洩防止ソリューション

情報漏洩防止ソリューションの一構成例を図3に示し，その特長を次に述べる。

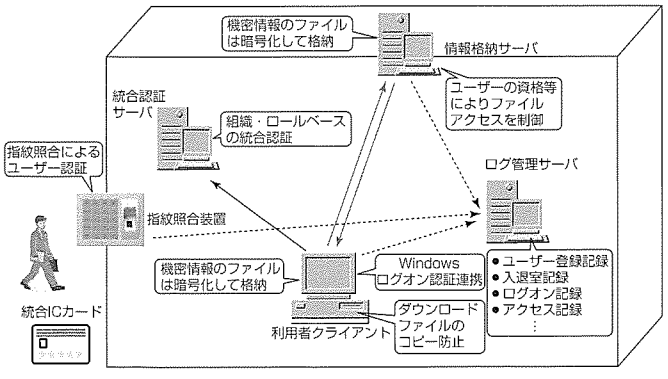


図3．情報漏洩防止ソリューションの構成例

(1) 利用者の統合的な認証

1枚のICカードですべてのシーンでの認証をカバー

- 部屋に入るときは指紋認証
- パソコンを使うときはログイン認証
- ファイルにアクセスするときはデジタル認証

(2) 情報の保護

世界最高水準の暗号技術MISTYでファイルを暗号化

- 利用クライアントの情報保護(ファイルの暗号化)
- 共有サーバの情報保護(サーバの暗号化，アクセス制御)
- コンテンツの情報保護
- ダウンロード後ファイルのコピー(カプセル化，外部出力防止)

(3) 簡単な導入・運用

- ユーザー認証情報の一括登録とICカード発行
- ログ管理サーバでの一元管理
- ISMS等認定取得のためのテンプレート

6.2 公開鍵基盤PKI

これまで，電子政府や電子自治体などで，GPKI(Government PKI)，又はLGPKI(Local Government PKI)としてPKI基盤が整備されてきている。一般にはブラウザを利用したアプリケーションでのSSL(Secure Socket Layer)の利用が進んできている。

今後PKI基盤の整備が進む分野の1つにヘルスケア分野がある。ここでは，ヘルスケアセキュリティにおけるPKI利用について述べる。

図4に示すように，今後ヘルスケア分野での電子化の促進に伴い，電子カルテ，処方箋(せん)，紹介状，レセプトなどに電子署名が必要となる。医療分野でのPKIについては，ISO17090で標準化が進んでいる。

電子署名を実現するために，証明書の発行が必要となる。

ジャパンネット㈱(Japan Net)は，PKIに基づく証明書の発行サービスを始め電子認証システムの運営管理サービス(ハウジング，ホスティング)等を提供している。証明書

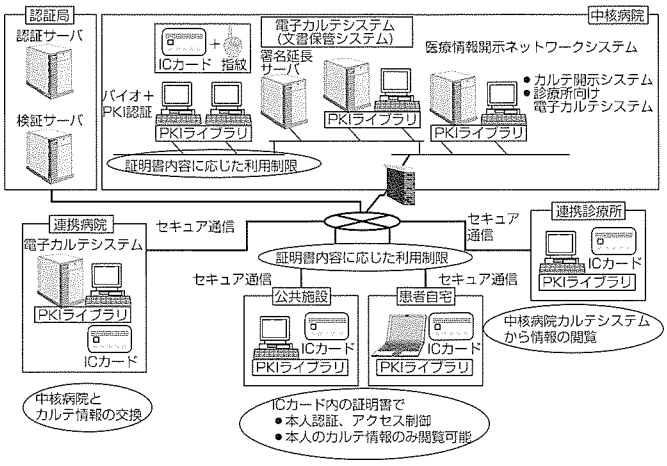
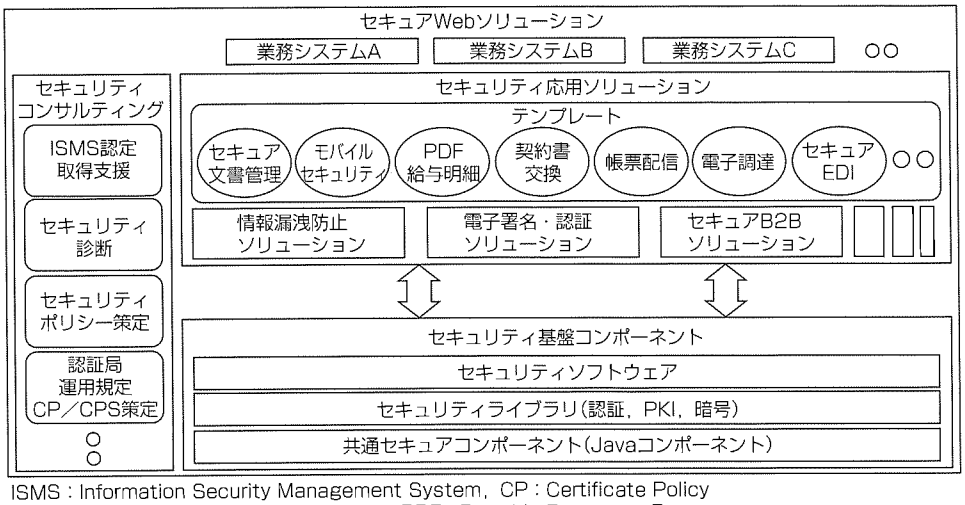


図4．ヘルスケアセキュリティ



ISMS：Information Security Management System，CP：Certificate Policy
CPS：Certification Practice Statement，PDF：Portable Document Format
PKI：Public Key Infrastructure，EDI：Electronic Data Interchange

図5．セキュアWebソリューション

発行サービスについては，特定認証業務の公的認定を取得し，府省・自治体などが実施する電子調達参加者向けの証明書発行も行っている。

6.3 セキュアWebソリューション

三菱電機インフォメーションシステムズ㈱(MDIS)では，Webベースシステムのセキュリティ上の課題を解決したり情報システムにセキュリティ機能を即応するためのフレームワークとして，“セキュアWebソリューション”を提供している。セキュアWebソリューションは，人的・物理的な側面も含めた情報セキュリティシステムを構築支援する“セキュリティコンサルティング”，PKI関連ライブラリを始めとする“セキュリティ基盤コンポーネント”，情報漏洩防止やセキュアなB２B環境及びこれらの活用ノウハウを集積した“セキュリティ応用ソリューション”から構成される(**図5**)。

7. むすび

三菱電機㈱のトータルセキュリティについて簡単に紹介するとともに，今回の特集テーマである“安全・安心を支えるITソリューション”の情報セキュリティに関する幾つかの例を述べた。企業のIT化が進む中，ITリスクとりわけ情報セキュリティリスクを経営の中でどう取り組んでいくか，経営者の意識が問われる時代となっている。今後，ISMSを導入する企業が増えると予想されるが，そのセキュリティ対策のためのツールやサービスに当社の情報セキュリティソリューションを積極的に提供していきたい。さらに，技術の方向や標準化の流れ，法制度をにらみつつ，今後とも最適なセキュリティソリューションを提供していく所存である。

参考文献

(1) 三菱電機技報：特集“情報セキュリティ”，**76**，No.4 (2002)
(2) 勝山光太郎，ほか：ユビキタスセキュアソリューション，三菱電機技報，**77**，No.4，239～242 (2003)

三菱情報漏洩防止ソリューション

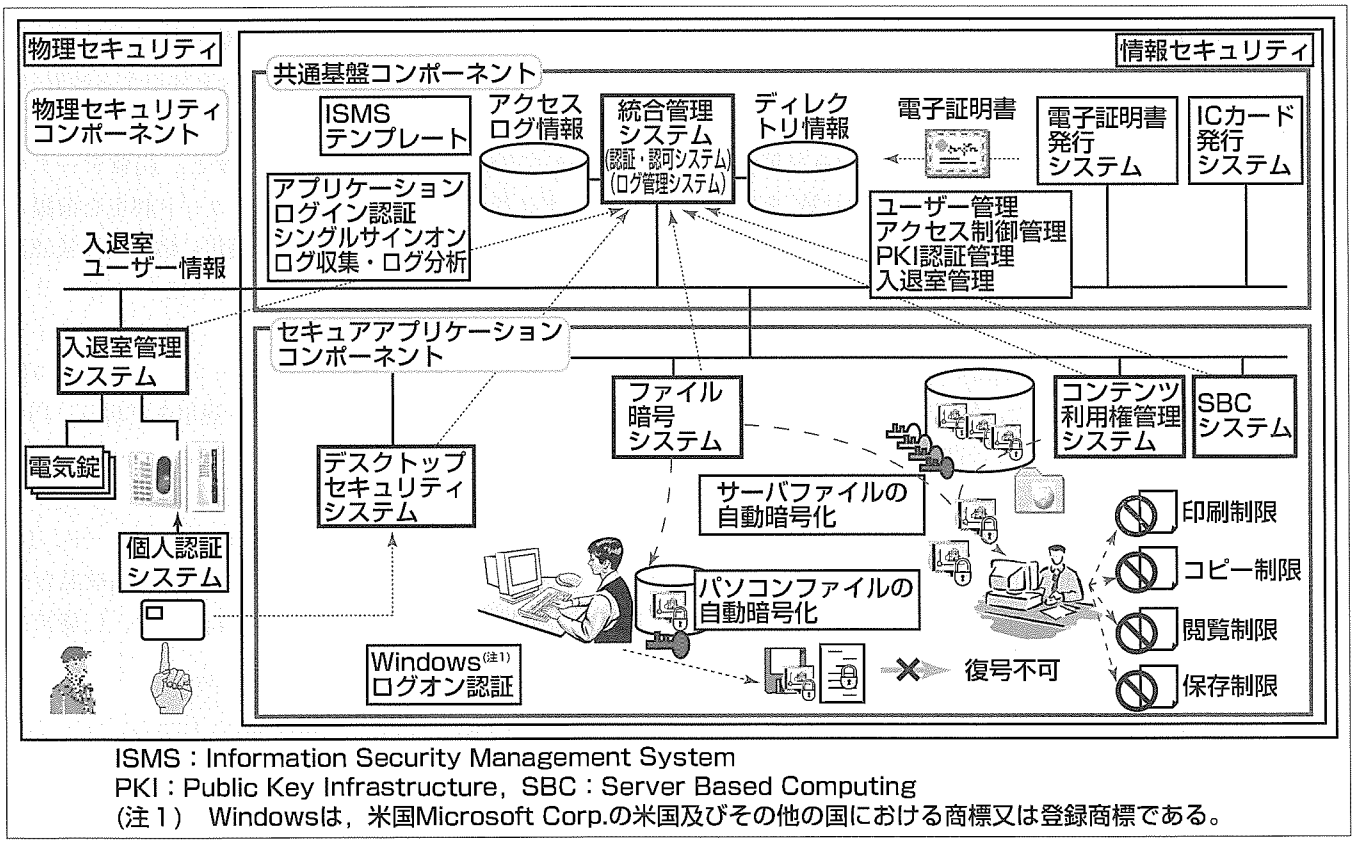
二井正雄* 伊藤英明***
中嶋春光**
近藤誠一**

要 旨

昨今，企業・組織のIT化に伴い，個人情報や企業情報などの機密情報が漏洩(ろうえい)・流出する事故が多発し，損害賠償に発展するなどの社会問題となっている。また，個人情報保護法や不正競争防止法などが施行され，法律面の整備も進んできている。こうした状況の中，今までは，外部からの不正アクセスからガードするためのネットワークセキュリティ対策に注力していたが，情報漏洩防止に対する取り組みとして，内部からの不正アクセスや情報漏洩に対する十分な情報セキュリティ対策が必要となってきている。

このような背景を基に，三菱電機㈱では，従来保有していた生体認証・電子認証などの認証技術や認証に基づいたアクセス制御技術，ファイルベースの暗号化技術，コンテンツ保護技術などの各種情報セキュリティ技術と，入退室管理システムなどの物理セキュリティ技術を連携・組み合わせることで，より強固な情報セキュリティマネジメントシステムを容易に構築できる“三菱情報漏洩防止ソリューション”を提供している。

また，ソリューションを構成する各コンポーネント間の機能連携やデータ連携の強化を図っており，大規模なイントラネットシステムから顧客管理システムなどの特定機能を利用する小規模なシステムまで，目的や規模に応じたシステム選択を容易とすることで，多様な業種・業態及び多様な用途にも迅速・的確に応じられる統合ソリューション化を目指している。



ISMS：Information Security Management System
PKI：Public Key Infrastructure，SBC：Server Based Computing
(注1) Windowsは，米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。

三菱情報漏洩防止ソリューションの構成概要

三菱情報漏洩防止ソリューションは，入退室管理システムや指紋照合システムなどの物理セキュリティコンポーネント，ユーザー管理やアクセス制御を統一的に管理する統合管理システムなどからなる共通基盤コンポーネント，及び情報システム利用認証や機密情報を自動暗号化するシステムなどのセキュアアプリケーションコンポーネントから構成されている。

*三菱電機インフォメーションシステムズ㈱ **三菱電機㈱ 情報技術総合研究所 ***同社 稲沢製作所

1. まえがき

情報のデジタル化やネットワークの進展によるIT社会の実現に伴い，社内外からの不正侵入・不正アクセスや端末の盗難・紛失などによる機密情報や個人情報の漏洩事故が頻発している。こうした情報の漏洩は，金銭的な損失だけではなく，企業イメージや信用・信頼の失墜が現実化しており，企業経営においても，競争力の低下をもたらすなど社会的問題となってきている。これに伴い，IT化の課題である情報化リスクに対して，不正アクセス禁止法・個人情報保護法・不正競争防止法などの法的整備や，情報セキュリティマネジメントシステム(ISMS)適合性評価制度及び情報セキュリティ監査制度などの情報保護対策を促す各種施策が実施され始めており，情報セキュリティの重要性が認知されつつある。信頼性の高い情報セキュリティへの取り組みを実現するため，暗号技術や指紋照合機能などの認証技術・アクセス制御技術，コンテンツ不正流出を防止するためのコンテンツ保護対策技術をベースに，情報資産の範囲やレベルに応じた最適な情報セキュリティ構築を支援するセキュリティコンポーネントシステム群として，三菱情報漏洩防止ソリューションを提供している。

2. 情報を適切に守る情報漏洩防止ソリューション

三菱情報漏洩防止ソリューションは，**図1**に示すコンポーネント群で構成され，ISMS認証取得をサポートするための標準テンプレート提供や取得支援コンサルテーションを行うとともに，情報セキュリティへの取り組み対策である人的・物理的・技術的対策のうち，“技術的対策”を提供するソリューションである。このソリューションは，物理セキュリティと情報セキュリティを融合させることで，認証基盤の統一を実現しており，入退室の認証情報と情報システムへの認証情報やログ情報を統一的に管理することができる特長を持っている。また，個人認証デバイスとして，ICカードや指紋照合装置だけでの認証レベルから，電子政府・電子自治体での導入実績も高いPKI(Public key Infrastructure)技術などを組み合わせた高度な認証レベルまで，ニーズに応じたセキュリティレベルでシステム構築を実現可能としている。次章以降にそれぞれ主なコンポーネントシステムへの取り組みを述べる。

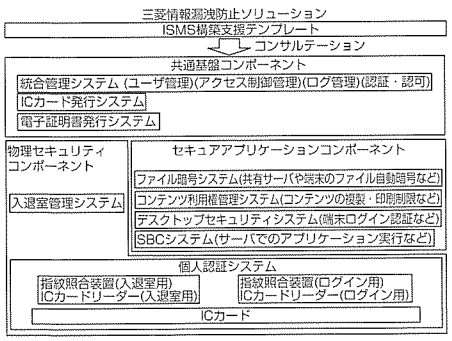


図1．三菱情報漏洩防止ソリューション取り組み概要

3. ソリューションを構成する主なコンポーネントシステムの概要と特長

3.1 入退室管理及び個人認証システム

情報セキュリティシステムの認証基盤と連携した入退室管理や指紋照合などの認証基盤であり，認証情報や通行ログ情報などの共有を可能とする。

3.1.1 入退室管理システム

このコンポーネントシステムは，三菱総合ビルセキュリティシステム“MELSAFETY”などのように，従来は，独立したシステムとして，IDコントローラが個人ごとのアクセス制御情報(入室可能な扉や時間帯)や通行履歴などを保持し，管理用装置では，IDコントローラに対する設定や履歴収集を行う機能を提供していた。

このソリューションでは，従来の管理用装置の機能を後述する統合管理システムでIDコントローラと直接接続を実現し，ユーザー管理を共通化するとともに，アクセス制御情報や通行履歴などの情報を統合した(**図2**)。

3.1.2 個人認証システム

情報セキュリティ用の個人認証システムとして，指紋で個人識別しアクセス制御ができる指紋照合装置がある。装置の種類としては，単体の指紋照合装置(三菱電機製品ではFPR-DTU)とICカードと指紋照合を併用する装置(同FPR-ICRU／S)がある(**図3**)。また，個人の指紋データをサーバで管理する指紋単体のタイプと，指紋データをICカードに登録して個人管理するICカード利用を前提とした併用タイプがある。システムの運用に応じて指紋認証やICカードでの認証が混在する場合もある。このソリューションでは，次に説明するデスクトップセキュリティシステムと組み合わせることで，ICカードと指紋照合の併用や単体のICカードリーダーでの相互運用を実現し，PKI技術を利用した高度な認証も可能とした。

3.2 デスクトップセキュリティシステム

ICカードによる認証から，ICカード＋パスワード，ICカード＋指紋照合，ICカード＋パスワード＋指紋照合やPKI認証などを組み合わせた多様な認証手段を，三菱デス

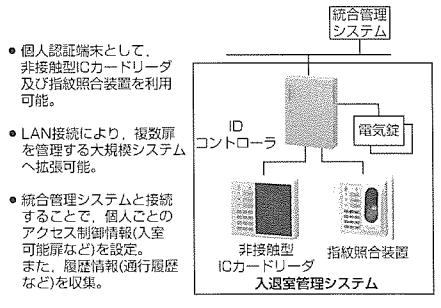


図2．入退室管理システムの構成及び特長

クトップセキュリティ“MISTYLOGON(注2)”などの認証システムとして提供している(図3)。本認証手段のアクセス制御機能を基に，端末へのログオン，Standard9－M ICカードと組み合わせたWindowsのSmartCardLogon，アプリケーション起動制御などを実現するとともに，ICカードの装脱着による端末ロックや抜き忘れ防止などの機能を提供している。また，ICカードへの各種情報や指紋登録を行うためのデスクトップ管理者機能も提供している。

3.3 統合管理システム

統合管理システムの概要を図4に示す。図中，統合管理システムは，認証・認可に必要とされるユーザー情報を統合管理し，各種セキュリティシステムや業務アプリケーションに対して，以下に示す機能を提供する。

(1) システムを利用するユーザー情報の設定・蓄積
(2) ICカード発行システム，入退室管理システムへのユーザー属性情報の配布
(3) 設定されたユーザー情報に基づいた認証・認可
(4) 認証・認可，入退室，コンテンツアクセス等のログの収集，保存，分析

3.3.1 ユーザー情報の統合管理

情報漏洩防止を実現するためには利用資格を持つ人のみが安全・確実に情報を利用できるシステムの実現が必要となっており，従来，個々に管理されていたユーザー情報を統合したアイデンティティ管理下に置くことが重要となる。そのため，物理セキュリティ及び情報セキュリティの各コンポーネントシステム及び業務アプリケーションで利用するユーザー情報，権限情報を一箇所で統合管理する。その結果，運用の効率化だけでなく，権限情報設定の根拠となるロール(役割)の集中管理によるセキュリティポリシーの統一化を実現することが可能となる。

(注2) MISTYLOGONは，三菱電機㈱が商標出願中である。

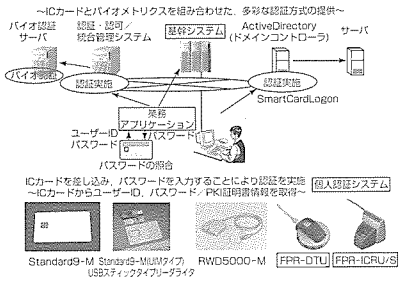


図3．ICカードシステムとデスクトップセキュリティシステムの概要

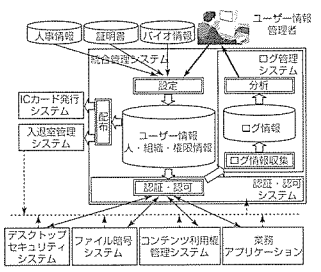


図4．統合管理システムの概要

3.3.2 ログ管理システム

ISMS認証取得をサポートするために，規定に従った項目のログを収集し，一箇所に統一形式で格納・整理して提供することを可能とする。また，接続された各種セキュリティシステムは，ユーザー情報の統合管理により，一つのユーザーIDで統一されるだけでなく，組織を基に統一したセキュリティポリシーによるアクセス制御が行われるため，収集・統合されたログの複合解析が可能となる。例えば，入室情報がないIDによる端末へのログイン防止など，因果関係による不正アクセスの検知に利用することが可能となる。

3.3.3 認証・認可システム

一つのユーザーIDをキーに，ユーザー情報，アクセス制御情報を統合管理し，認証・認可サーバにより，シングルサインオンを実現する。認証・認可結果は，構造化情報標準推進機構OASIS(Organization for the Advancement of Structured Information Standards)の標準化形式であるSAML(Security Assertion Markup Language)準拠のアサーションとして提供する。一度ログインするだけでファイル暗号システムや，コンテンツ利用権管理システム及び業務アプリケーションなどの各種サービスを自由に利用でき，利便性を向上させることができる。

3.4 ファイル暗号システム

機密情報ファイルの暗号化を行うシステムで，三菱ファイル暗号ソフトウェア“CRYPTOFILE(注3)”などがあり，クライアント機能とサーバ機能を提供している。クライアント機能は，クライアント端末内のドライブやフォルダを自動暗号化するとともに，リムーバルメディア利用を制限するなどの機能を提供し，端末の盗難・紛失やリムーバルメディアの流出・不正持ち出しによる情報漏洩を防止することができる。また，サーバ機能は，イントラネット内で，通常，複数の共有サーバ上に保管している機密情報を，個人の暗号鍵(かぎ)以外に，統合管理システムで管理される組織情報と共有サーバ上のフォルダへのアクセス制御情報を基に，業務に合わせファイルを自動的に共有暗号化する。暗号化された機密情報は，専用のアプリケーションから認証・認可システムを通じてのみアクセスが可能であり，機密情報のダウンロード・閲覧・保存などのアクセスコントロールを行うことで，不正なアクセスから機密情報を守るとともに，暗号化されたすべての機密情報ファイルを安全に復号する機能を提供している(図5)。

3.5 コンテンツ利用権管理システム

機密情報の中には，管理レベルの高い情報が多々ある。単純に暗号化するだけでなく，コンテンツ単位に適切なデータ保護対策が求められる。コンテンツ利用権管理システ

(注3) CRYPTOFILEは，三菱電機㈱の登録商標である。

表1．ソリューション適用事例

適用No	導入事例＼システム	入退室管理	個人認証	統合管理			ICカード発行	電子証明書発行	ﾃﾞｽｸﾄｯﾌﾟｾｷｭﾘﾃｨ	ファイル暗号		利用権管理	SBC
				ディレクトリ	ログ管理	認証認可				クライアント	サーバ		
①	某製造業パソコンファイルセキュリティ									●	●		
②	某製造業設計文書管理										●	●	
③	某医療機関シングルサインオン認証基盤		●	●		●	●	●	●				
④	某医療機関認証基盤		●					●	●				
⑤	某金融機関個人情報保護				●					●			
⑥	某金融機関セキュアデータ交換									●		●	
⑦	某自治体職員認証	●	●	●			●		●				●
⑧	某自治体個人情報保護			●		●					●		
⑨	某サービス業データセンター	●	●						●				

ムには三菱情報漏洩防止ソフトウェア“デジカプセルWeb(注4)”や三菱電機利用権管理ソリューション“DROSY(注5)”などがあり，以下のような攻撃から機密情報の不正流出を防止する。

(1) ファイルコピー
(2) ファイル保存(保存機能／コピー＆ペースト機能)
(3) 印刷
(4) 画面キャプチャ

この機能では，“コンテンツの暗号化”,“アプリケーション・OSの機能制御”という防御方法によって前記の攻撃からコンテンツを保護し，HTML(Hyper Text Markup Language)，JPEG(Joint Photographic Experts Group)などのWebコンテンツやPDF(Portable Document Format)，Microsoft(注6) Officeなどの電子文書コンテンツの不正流出を防止している(**図5**)。

3.5.1 コンテンツの暗号化

利用者に配信するコンテンツは，あらかじめその利用者以外は閲覧できないよう暗号化されており，利用者がコンテンツの閲覧権限を持つ場合のみ復号され閲覧することができる。このとき，復号されたコンテンツはメモリ上にのみ展開され，ローカルディスクやリムーバブルディスクに保存しないことによってコンテンツの不正流出を防止する。

3.5.2 アプリケーション・OSの機能制御

電子文書コンテンツを扱うアプリケーションのメニュー等を制御することによって，コンテンツのファイル保存，印刷及びコピー＆ペーストといった機能の使用を制限する。また，OSが提供する画面キャプチャ機能の使用を制限することによって，コンテンツの不正流出を防止することができる。

4. 情報漏洩防止ソリューションの適用事例

システム構築目的や規模に応じたシステム選択による代表的なシステム構築例を**表1**に示す。表中の事例①に示す製造業では，クライアントパソコンのモバイル利用を前提としたパソコンファイルへの不正アクセスや盗難・紛失対策のため，クライアントパソコンのファイル暗号化機能を導入し，自パソコンのディスクをドライブごと自動暗号化している。また，共有ファイル暗号化機能を社内のデータ交換にも利用している。今後，管理レベルの高い情報をサーバで管理するため，サーバ機能の導入を予定している。事例③に示す医療機関では，指紋＋PKIによる強固な認証と医療アプリケーションへのシングルサインオンを実現している。事例⑦に示す自治体では，職員の入退室管理のIDとパソコンのログインIDを一元管理し，職員の認証管理を実現している。

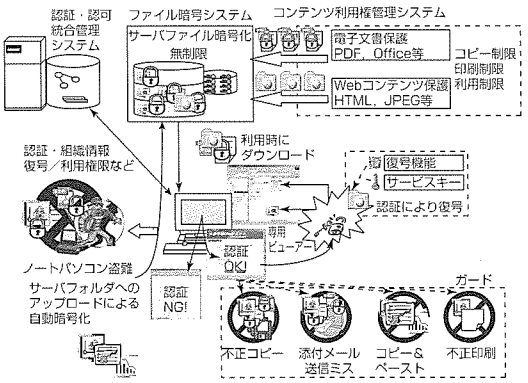


図5．ファイル暗号及びコンテンツ利用権管理システムの概要

5. むすび

情報セキュリティ技術を利用した機密情報の情報漏洩防止ソリューションを構成する主要なソリューションコンポーネントについて述べた。必要なソリューションを選択・組み合わせることで，外部漏洩・内部漏洩などの脅威から大切な機密情報を保護することができ，情報資産の範囲やレベルに応じた最適なISMSを構築・整備できることを示した。今後の展開として，物理セキュリティとの連携を更に強化し，暗号技術とコンテンツ保護技術を更に融合することで，使いやすくかつ強固な機密情報保護ソリューションへ拡張していく所存である。

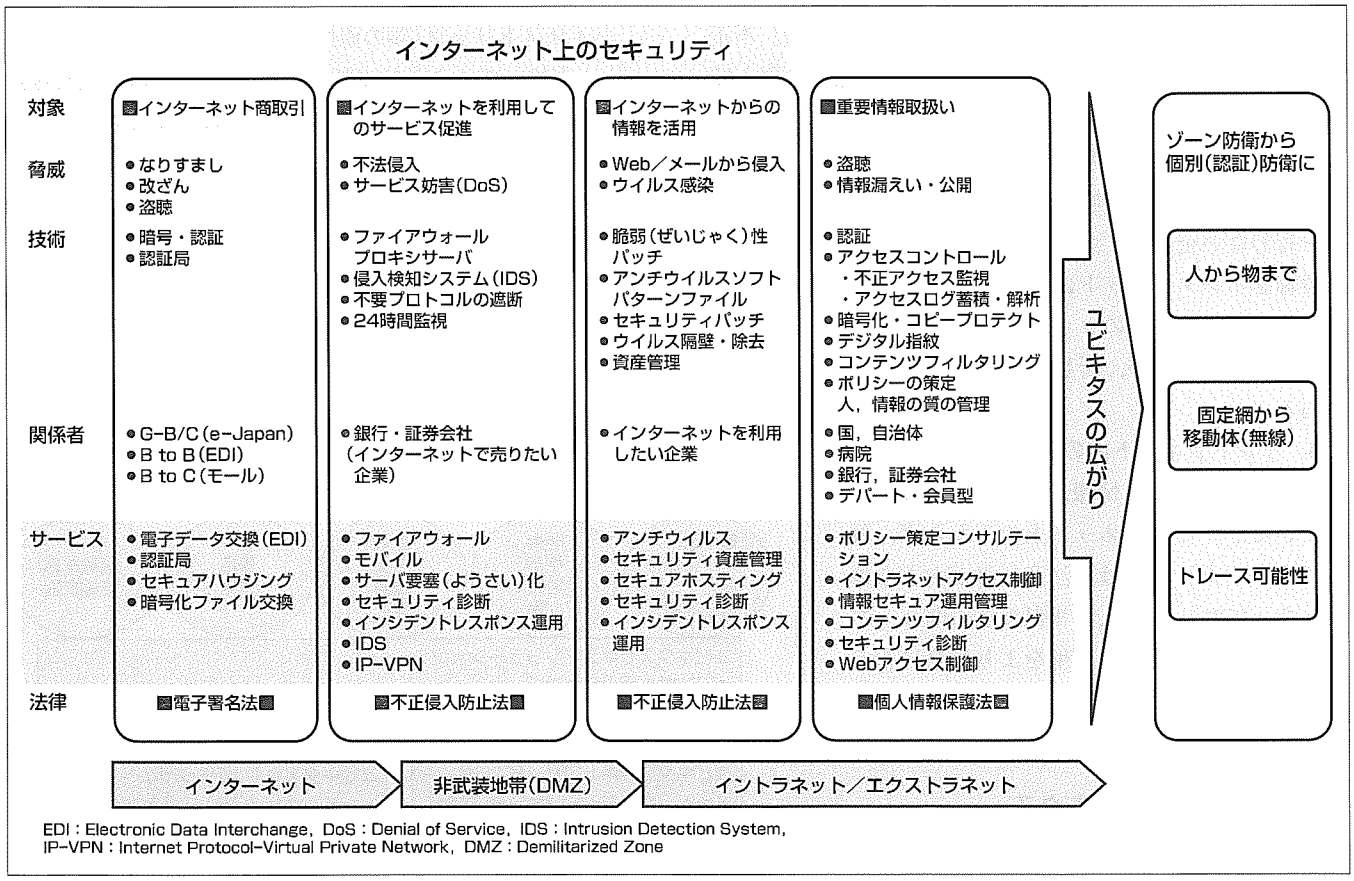
(注4) デジカプセルWebは，三菱電機㈱の登録商標である。
(注5) DROSYは，三菱電機インフォメーションシステムズ㈱の登録商標である。
(注6) Microsoftは，米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。

ユビキタスセキュアソリューション実現のための認証サービス

村木克己*
角野章之*
中村克巳*

要　旨

ユビキタスの時代が予感されている。この時代には，あらゆるものが電子的につながれ，相互のコミュニケーションがいつでもできる。自由が増せば悪用のチャンスも増え，恩恵が多いほど，この悪用による被害が増えていく。ユビキタスのセキュリティ対策は，今までの対策の積み重ねの上にユビキタスの時代の特徴を持った脅威に対する対策を付加することとなる。今まで，セキュリティキーワードは，①インターネット上の情報交換に対する盗聴，なりすまし，②サービス提供者への不正侵入，③インターネット利用者パソコンへのウイルス感染，④内部情報の漏えいであった。ユビキタス時代には今までの“インターネット”と“人”に加えて，“無線による常時接続通信”と“物”とが追加される形でソリューションの応用を広げていく。“いつでも，どこでも，何にでも”のユビキタスインフラの上で“今だけ，ここだけ，あなただけ”が価値を持つ。ユビキタスの時代のソリューションは，利便性を持つものが期待される半面，個々の価格は安価なものも多い。したがって，認証といった基本機能も，提供するソリューションに合ったものをアウトソーシングも含め安全かつ安価に入手することが成功の鍵(かぎ)となる。三菱電機の優れた暗号技術を使用し，電子署名法に基づく公的な認定を受けた“認証局サービス”，またその応用としての“アウトソーシングサービス”などをジャパンネット㈱(Japan Net)は提供している。



EDI : Electronic Data Interchange, DoS : Denial of Service, IDS : Intrusion Detection System,
IP-VPN : Internet Protocol-Virtual Private Network, DMZ : Demilitarized Zone

インターネット上のセキュリティ

インターネット上のセキュリティは，その応用対象により，場所を守るやり方(不法侵入やウイルス等の対策)と，対象を認識し情報を守るやり方(認証局，暗号アクセスコントロール等)がある。ユビキタス時代のセキュリティはインターネットの対応の延長にあるが，より細かく環境移動する人や物の位置変化までとらえられるため，場所依存の防御よりも人や物に対応した認証が中心になる。これによりユビキタスの中で独自のグループを作ることができる。

*ジャパンネット㈱

1. まえがき

インターネットで人間相互が結ばれた世界が実現し，その利便性を享受する中で，いよいよこれを物にまで拡張したユビキタスの時代の動きが見え出している。このような世界では，多くの場合見知らぬ物の，見知らぬ人が相互の関係を持って仕事を行う。そのような構造の社会ではセキュリティの確保は不可欠である。これは，法律に則り，適正な技術の適用とその絶え間ない安全な運用が鍵(かぎ)となる。

2. セキュリティサービスの変遷

セキュリティが必要とされる状態に応じて分類すると，以下のようにまとめることができる。

2.1 情報交換における脅威

インターネット上の情報交換についてはなりすまし，改ざん，盗聴が脅威で，電子署名法に則り暗号，認証，PKI(Public Key Infrastructure)という技術でこれに対応する。電子署名法は，“電子署名”があればこれを法的に従来の紙への署名と同等に扱うものである。

2.2 インターネット上のサービス提供時の脅威

従来の銀行サービス業務などをインターネットで行おうとすると，インターネットからの侵入が脅威となる。不正侵入防止法に則り，IDS，ファイアウォールなどの侵入監視を強化する。

2.3 インターネット利用の脅威

インターネット上で物を売るという直接のネットビジネスを行わない企業も，ネット上の情報を利用するために社内設備をインターネットに接続したことにより，多くの企業が無差別攻撃などのウイルスに悩まされた。ウイルス対策ソフトが有効だが，新しいウイルスに間に合わない場合がある。

2.4 イントラネット内の情報漏えい

そして今や，個人情報が漏えいする危険が出ているが，これはネット上のみならず，社内の人の不正行為又は不注意行為が大きな原因となっており，個人情報保護法に則り，アクセス管理など社内の運用をより厳格に行うなどの対策が必要である。ここでは個人の認証が鍵となる。

3. ユビキタス

ユビキタスの時代には，2章で述べたような脅威が無線でつながれた人々は無論，小さな物にまで広がる。IPv6(Internet Protocol Version 6)でいろいろな物が無線通信も含め常時接続された構造でのセキュリティは，インターネットの脅威が無論すべて当てはまり得る。ただし，今までの閉じた領域型の防御は無線など人や物が動き出す環境では有効性を失い，個別の相手の“場所によらない”認証が不可欠技術となる。すなわち“いつでも，どこでも，だれでも”の環境の上で有益となるソリューションは，“ここだけ，今だけ，あなただけ”の安全かつ厳格な囲い込みにある。

三菱電機のユビキタスセキュアソリューションを図1に示す。

4. 認証とは

認証とは本人(又は物)の確かにその人(又は物)であることを確認することであり，人を実印で確認することは今までも行われてきたが，インターネット上ではデジタルデータだけで確認する必要性がある。

4.1 記憶しているもの

パスワードは使いやすいが忘れやすい。覚えやすいものは他人に推測されやすい。盗まれても本人が気づかない。

4.2 持っているもの

カード，USB(Universal Serial Bus)トークンなど。本人の確認でなく所持者の確認となる。

4.3 自分そのもの

バイオメトリック(顔の画像，指紋，網膜，虹彩(こうさい)，声紋，デオキシリボ核酸(DNA)など)は本人を確認する強力な手段であり，日常生活ではほとんどの場合，これが本人確認の手段である。ただし，声紋も指紋もコピーができる。また，自分の特徴，たとえば指紋を直接的に相手のコンピュータに登録することは心理的にも負担がある。

4.4 電子署名

公開鍵を使った証明書による身元証明，つまり上記4.1節から4.3節までの方法がいわば1対1型で身元確認する方法であったが，それでは，社会に広く使える形(社会のいろいろの組織に属する各々違った人の集団を作る場合な

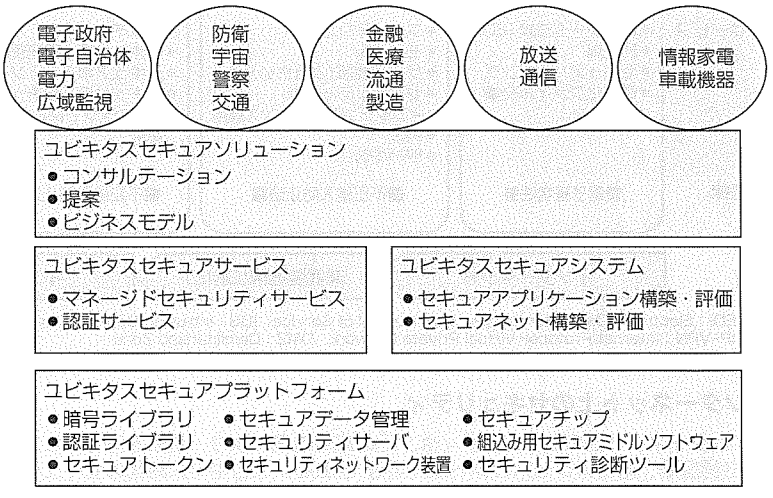


図1．三菱電機のユビキタスセキュアソリューション

ど)とするには，何組ものこれらの秘密情報の交換・変更などの管理が必要となる。インターネット上で行うには，更に暗号化が不可欠であり，その暗号鍵の管理も必要となる。公開鍵技術を使ってPKIを構築し証明書を信頼できる機関から発行を受けることによりこれらの問題が解決できる。ただし，このような証明書も暗号鍵を証明しているだけで本人とは限らず，盗用の危険がある。証明書をパソコンに入れておけば認証されるのはパソコンであり，ICカードに入れておけば認証されるのはICカードの所持者である。PKIは現在世界で広く使われ出しており，携帯電話にもWPKI(注1)(Wireless Public Key Infrastructure)が利用されるようになってきていることから，“重要な物”にはすべて“物”の認証が行われる時代が到来する。

5. Japan Netの電子証明書発行サービス

実務システムにおける電子証明書の利用が確実に増えつつあり，Japan Netでは以下に述べる電子証明書の発行サービスを行っている。

5.1 e-Japan対応電子入札用電子証明書発行サービス（特定認証業務）

“電子入札コアシステム”による電子入札が2003年4月から国土交通省で開始されたが，他の省庁や自治体でも電子入札が始まっている。Japan Netは，電子入札コアシステムによる電子入札で使用する電子証明書を発行している(図2)。この電子証明書発行サービスは，電子署名法で規定された特定認証業務である。また，政府認証基盤ブリッジ認証局と相互認証している。

5.2 一般向け電子証明書発行サービス

e-Japanと並ぶ電子証明書の大きな利用分野であるヘルスケア分野，金融分野などで使用する電子証明書，及びイントラネット，企業コミュニティ内での各種サーバ／クライアント用の電子証明書を発行するサービスである。ICカード，USBトークンを始めとした各種媒体に電子証明書を格納して提供している。

5.3 特定認証業務の認定取得支援サービス

電子署名法に基づく特定認証業務の認定取得のために必要な運用管理ドキュメント作成等，一連の業務に関する支援を行うサービスである。

6. Japan Netのセキュアアウトソーシングサービス

特定認証業務の認定基準を満たす高いセキュリティ環境の下で長年培ってきた運用アウトソーシングノウハウをベースとして電子認証局システムの運営管理(ハウジング，ホスティング)を行うサービスである。具体的な運用管理業務内容としては，①証明書に登録するユーザー情報及び発行管理のために使用するユーザー情報の登録，②電子証明書の生成，媒体への書込み及び電子証明書媒体の顧客指定場所への配布，③証明書の失効受付と失効処理及び失効情報の公開，④認証局システムのデータベースバックアップ処理，⑤証明書の有効期限管理と有効期限切れ前の利用者への通知，⑥認証局システムの24時間365日の稼働状況監視，⑦認証局システムの障害対応と障害履

(注1) WPKIは無線公開鍵インフラのことであるが，携帯電話に利用される証明書は，X.509に比べより小さなWTLS(Wireless Transport Layer Security)が利用される。

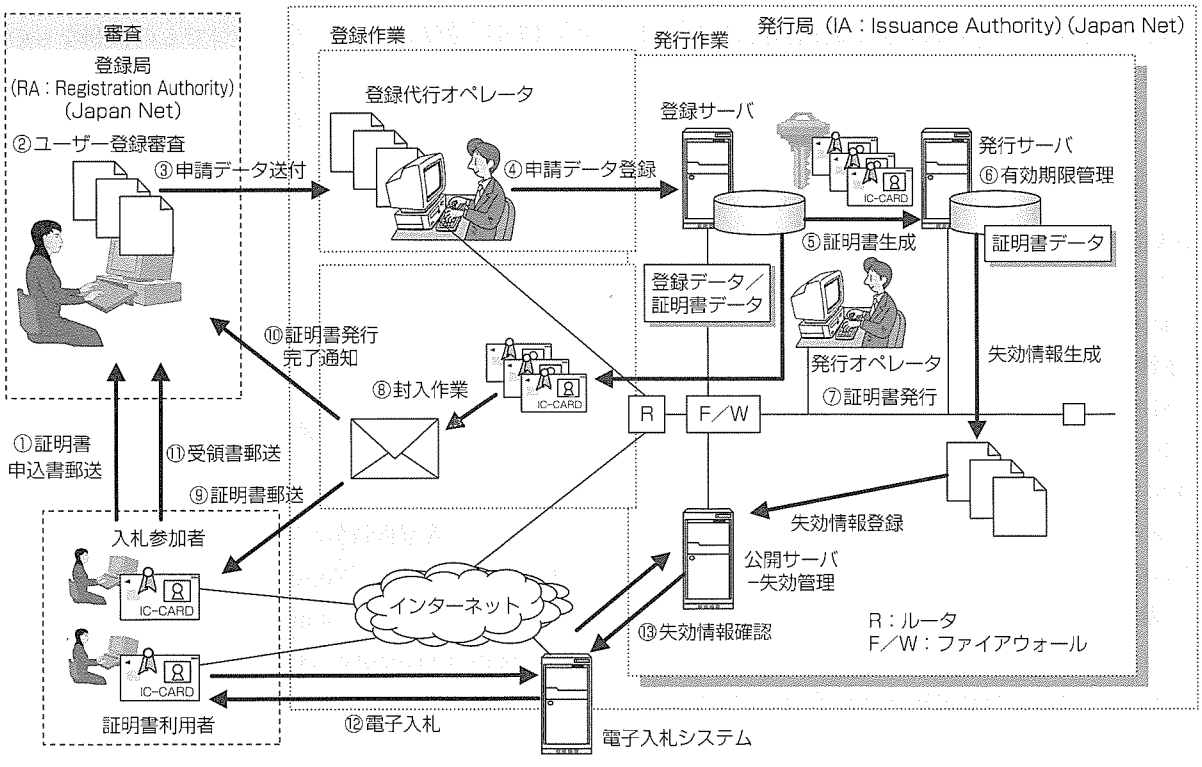


図2．電子証明書発行業務フロー

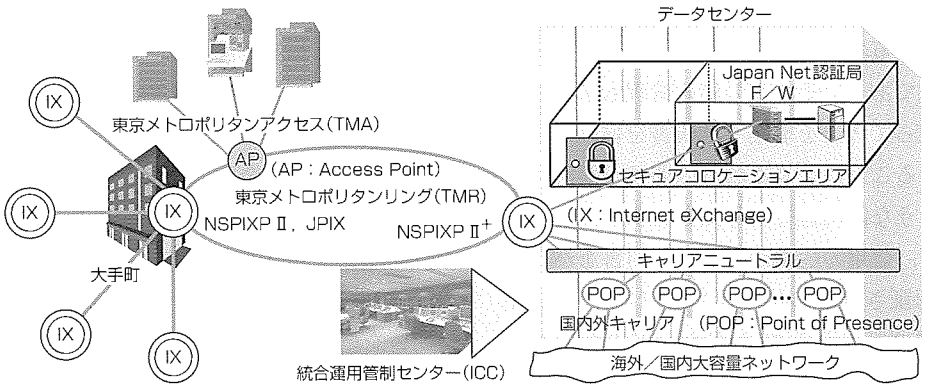


図3．Japan Netセキュアコロケーション

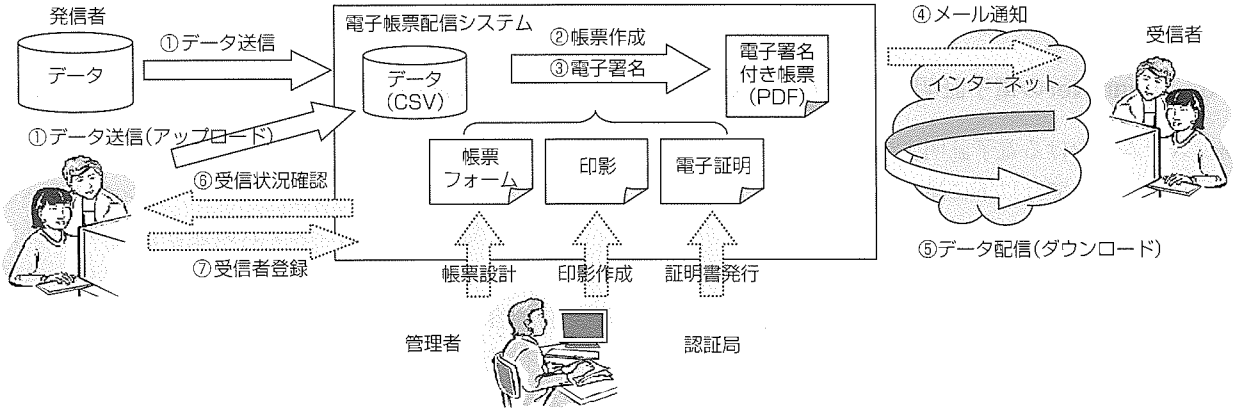


図4．電子帳票配信サービスの概念

歴管理，⑧認証業務全般にかかわる監査情報の保管，⑨認証局運用管理規程(CPS)他の運用ドキュメントの策定と維持管理，⑩証明書利用者に対するヘルプデスク業務等がある。

また，高いセキュリティを要求されるお客様に対してはセキュアコロケーションエリアでコロケーションサービスを提供し，サーバ類の設置と監視業務を行う(図3)。

7. 電子証明書を利用した応用サービス

三菱電機情報ネットワーク㈱(MIND)では，Japan Netが発行する電子証明書を利用した各種アプリケーションサービスを開発し展開している。

7.1 電子帳票配信サービス

今まで郵送していた請求書や帳票類を電子化してネットワーク配信することによりコスト削減を図りたいというお客様の要望に対応し，請求書や帳票類の電子データをPDF(Portable Document Format)化して，そのPDF文書に電子署名を付加し，インターネット上で配信するサービスである(図4)。

7.2 セキュア電子データ保管サービス

ストレージサービスの付加価値サービスの一つとして，電子データの真正性を確保し，かつ，長期保存できるサービスの提供を行うため，電子署名，タイムスタンプ，署名延長等の技術を使用して，セキュア電子データ保管サービスの提供を予定している。

8. むすび

ITが，だれでもどこでもいつでもの便利なものになるにつれて，現実にはセキュリティ，プライバシーがますます重要になっている。認証はその基本技術であり，PKIは現在最善の解決法と思われるが，それとて，鍵を盗まれないことが前提のものであり，これを本当に安全に管理・運用することがかなり難しいことも事実である。我々は，今後も，ユビキタス世界のソリューションを提供する企業にそのコンポーネントたる認証関連サービスをコストパフォーマンス良く提供していく所存である。

参考文献

(1) 勝山光太郎，ほか：ユビキタスセキュアソリューション，三菱電機技報，**77**，No.4，239～242（2003）

(2) Varshney, U.：Network Access and Security Issues in Ubiquitous Computing, CIS Department Georgia State University（2003）
http://weatherhead.cwru.edu/pervasive/Paper/UBE%202003%20-%20Varshney.pdf

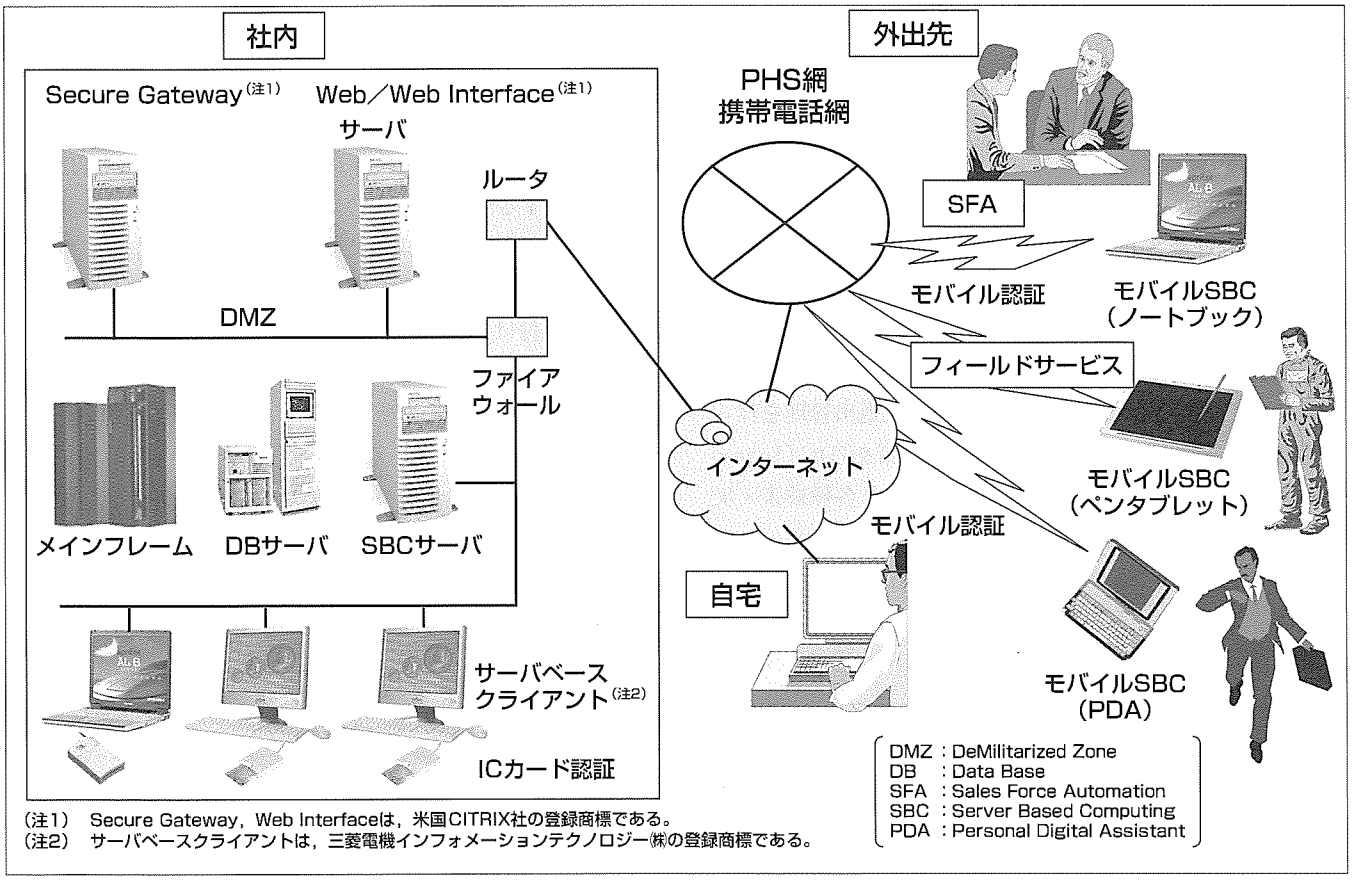
セキュリティ機能を充実させたサーバベースクライアントによるSBCソリューション

木幡康博*
冨安哲郎*
清水茂樹*

要　旨

安全な情報システムでは，機密性・完全性・可用性が求められる。情報システムのセキュリティ技術は，暗号技術や個人認証技術によりネットワーク上での盗聴，データ改ざん，なりすまし，不法侵入，データ破壊等の意図的な脅威から守ってくれる。ただし，セキュリティを保つためには，過失・故障・災害等の偶発的な脅威に対しても対策する必要があり，技術面だけでなく，人的対策としてのユーザー教育，モラルの徹底，制度的な対応として手順書等による運用面での徹底，ハードウェアの故障や地震・火災等の脅威に対して建物や設備に対する対策が必要である。これらを対策するためには，バランスのとれたセキュリティシステムを構築する必要がある。

特に，ユーザー教育やモラルの徹底等の人的対策や運用面での対策に頼るセキュリティに対しては，技術面でのセキュリティ向上が求められている。三菱電機インフォメーションテクノロジー㈱(MDIT)では，ソフトウェア，データをすべてサーバで管理する“サーバベースコンピューティング(SBC)ソリューション”により，運用や人的なセキュリティ上の脆弱(ぜいじゃく)さを技術的な仕組みとして対策し，いつでもどこでも安心してオフィスと同じ環境にアクセスできる，トータルなセキュリティソリューションを提供している。



(注1)　Secure Gateway，Web Interfaceは，米国CITRIX社の登録商標である。
(注2)　サーバベースクライアントは，三菱電機インフォメーションテクノロジー㈱の登録商標である。

SBCトータルソリューション

ユビキタス社会への期待が高まっている中で，社内・外出先・自宅などから，いつでも，どこでも，多様な通信サービス等を利用して，センターのSBCサーバに接続することによりオフィスと同じ環境を安心して使えるためのトータルソリューション(端末ソリューション，認証ソリューション，設計・構築ソリューション)が，“SBCトータルソリューション”である。図中のSecure GatewayとWeb Interfaceは，クライアントからWebブラウザを利用して安全にSBCサーバに接続するためのユーザー認証と暗号化を行うためのサーバである。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

企業での情報漏洩(ろうえい)の大部分は内部からの漏洩であると言われており，人的なセキュリティ対策をいかにして技術的な仕組みとして取り込めるかがセキュリティ対策上の大きな課題である。本稿では，SBCによる技術的な仕組みとして，人的なセキュリティを強化し，いつでもどこでもオフィスと同じ操作環境を提供するセキュアなSBCセキュリティソリューションについて述べる。

2. 情報システム・セキュリティでの問題点

(1) セキュリティの重要性

企業において，情報発信，情報収集，情報交換，ビジネス等にインターネットはなくてはならない存在となってきた。インターネットゆえに，世界中のハッカーから通信データの盗聴，改ざん，システムの破壊等の危険に常時さらされている。また，2003年8月に猛威を振るったMS Blasterウイルスは，史上最大規模の被害を与え，ウイルス問題は後を絶たない。さらに，個人情報漏洩に関する事件が多発しており，こうした被害から自社システムを守り社会への信用を得るために，情報システムのセキュリティ対策の重要性は言うまでもない。

(2) セキュリティ対策

安全な情報システムでは，機密性(盗まれない)，完全性(壊されない)，可用性(いつでも使える)が求められる。こうしたシステムの対策としては，代表的なリスクの原因からアプローチする方法として以下の対策が必要である。

①技術的対策としては，ネットワークセキュリティ対策が重要な要素であり，暗号と認証技術によりネットワークでのデータ破壊，改ざん，盗聴，不正アクセス，なりすまし等からセキュリティを保つ，②物理的セキュリティ対策としては，重要な情報資産を厳格な入退出管理を伴った耐震構造建物などに設置するなどの対策やIDC(Internet Data Center)でのバックアップ等により各種被害・災害等から守る，③人的セキュリティ対策としては，セキュリティ教育，モラルの向上，運用規約などにより，人的不注意によるデータ漏洩を防ぐ(図1)。

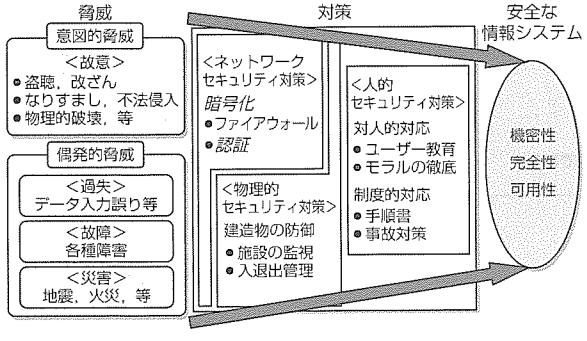


図1．安全な情報システムのためのセキュリティ対策

(3) 人的セキュリティ対策の重要性と課題

企業における情報漏洩の大部分は内部の人的ミスや故意によるものと言われており，人的なセキュリティ対策部分をモラルや人の運用のみに頼るのでなく技術的な仕組みでセキュリティを向上することが大きな課題となっている。

3. SBCでのセキュリティとは

(1) SBC方式の背景

情報システムの構築方式として，1990年代に入りホスト集中システムから，安価なサーバでシステムを構築できるクライアント／サーバシステム(C／Sシステム)に移行を開始した。1990年代後半からは，クライアント台数が増えることによる管理コストの増大とクライアント側のセキュリティ強化の面から，新たなサーバ集中方式としてインターネットとの親和性の高いWebシステムへの移行が進みつつある。しかしながら，C／SシステムからWebシステムへの移行は，システムの再構築が必要であり，多大な開発投資を必要とする。そこで，既存のC／Sシステムをそのまま利用してすべての業務をサーバで集中管理可能なSBCシステムが注目を浴びている。

(2) SBC方式の仕組み

C／Sシステムのクライアントとサーバの間にSBCサーバを置き，クライアント側にあったアプリケーションとデータすべてをSBCサーバ上に置いて動作させる。クライアントとSBCサーバとの間では，画面情報とキーボード，マウス等の情報だけが交換される。クライアント側では，画面を制御するSBCクライアントソフトウェアが動作するだけで，あたかも，端末でWindows(注3)が動作しているように見える。サーバ側では，複数のクライアントからの要求を受け付け，端末対応に論理的な仮想端末を生成し，各々が独立した端末として動作するよう制御する。これにより，システム独自のアプリケーションだけでなく，Excel(注3)，Word(注3)，Outlook(注3)等のOA系のアプリケーションもすべてサーバでの集中管理が可能となる(図2)。

(注3) Windows，Word，Excel，Outlook，Officeは，米国Microsoft Corp.の登録商標である。

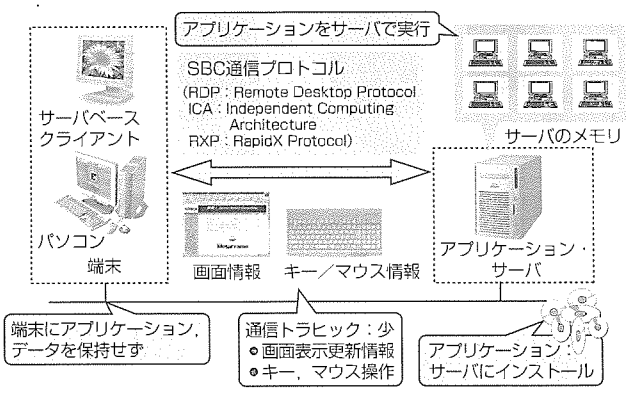


図2．SBCシステムの動作概要

(3) セキュリティに関する特長と効果

これまでの人的なセキュリティ対策は，従業員の教育，モラル，運用等に頼ってきたが，SBCでは，技術的な仕組みとして，以下のようなセキュリティを確保できる。

(a) 情報の不正持ち出し防止

データをすべてサーバで管理し，端末側ではサーバの仮想端末の画面表示が行われ，また端末のデータ入出力はサーバ側で制限をかけることが可能なので，端末を通した情報の不正持ち出しを技術的な仕組みとして防止できる。

(b) モバイル端末盗難紛失時のセキュリティ

モバイル端末に顧客情報等の会社機密情報をダウンロードした状態での端末の盗難・紛失は，機密情報の悪用により企業にとって大きな損害を与えることがある。モバイルパソコンにおいても，SBCでは，データがすべてサーバで管理されていることから，万一の時にも安心して使用できる。

(c) 通信の暗号化

SBCでのC／Sシステム間の通信はセキュアな鍵(かぎ)交換により接続の各セッションごとにすべて暗号化されており，データの盗聴，改ざんを防止できる。

4. SBCでのセキュリティソリューション

4.1 サーバベースクライアント

MDITでは，セキュアなSBC専用端末として，以下の3種類のサーバベースクライアントを提供している(**図3**)。

- TX110(モニター体型)
- TX210(Box型，モニタ別)
- TX110-TP(モニター体型，タッチパネル付き)

サーバベースクライアントは，ディスクを持たず，SBC対応ソフトのみが動作するSBC接続専用端末である。ディスク，ファン等の駆動部品を持たないことで高信頼，省スペース，静寂な端末設計であり，こうした専用端末を使用すると可用性を大きく高められるとともに人的なセキュリティを技術的な仕組みとして確保できる。

(1) 情報不正持ち出し防止強化

FDD等のリムーバブルデバイスを持たないので，不正データ持ち出し防止を更に強化できる。

(2) ウイルス対策

全社員の端末ウイルスソフトを常に最新状態に保つ必要があるが，SBC専用端末ではディスクを持たないことからウイルス感染の危険がない(サーバ側のみウイルスソフトを最新に保つだけでよい)。

(3) ブラウザからの不正アクセス対策

ブラウザの脆弱性に対する修正情報が頻繁に発行される中で，各担当者が自己パソコンのブラウザを最新状態に保つ必要があるが，SBCでは，サーバ側のみ修正情報を適用するだけでよい。

4.2 認証ソリューション

SBCでは，常にサーバにログインして動作し，ネットワーク上でのデータは常に暗号化されていることから，ログイン認証を強化することでセキュリティを一層強化できる。MDITでは以下の多彩な認証ソリューションを提供している(**図4**)。

(1) SBC専用端末用ICカード接続認証EasyLogin

SBC専用端末上には，サーバへの接続情報を設定することなくサーバ接続時にICカードをリーダーに挿入しICカードの暗証番号(PINコード)を入力するだけで自動的にサーバ接続できる製品を提供する。物理的なICカードを持っており，本人しか知り得ないPINコードによる2段階認証によりセキュリティを強化できる。また，端末もICカード認証がOKとならないと端末自体の操作もできないようになっていることから，セキュリティが高い。ICカードの中にサーバ接続情報とサーバへのログイン情報を持つことにより，公開鍵基盤PKI(Public Key Infrastructure)のように証明書管理する特別なサーバを必要とせずに認証管理も簡単に行える。さらに，Windowsが提供するPKIを用いたスマートカードログオンの仕組みも同時に提供する。

(2) パソコン用ICカードソリューションEasyLogin-Web

SBCの端末としては，専用端末だけでなくパソコンでも利用できる。パソコンでは，WebからSBCサーバに接続してSSL(Secure Socket Layer)を利用したセキュアな接続が可能である。これにより，モバイルで出張先から会社のSBCサーバに接続して，オフィスと同じ環境で使用することができる。こうした環境では個人認証が特に重要となる。WebのSBC接続画面に対してICカードをセットし，ICカードのPINコードを入力するだけでサーバ接続可能なソリューションを提供している。

(3) パソコン用指紋認証によるWeb接続ソリューション

三菱電機㈱稲沢製作所製の指紋付きICカードリーダライター装置を用いた指紋認証ソリューションを提供する。

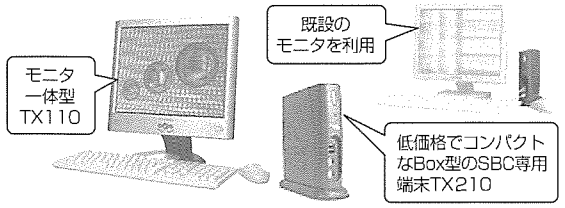


図3．セキュア端末ソリューションTX110, TX210

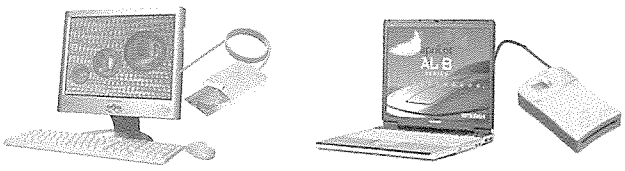


図4．SBC認証ソリューション(ICカード，指紋)

パソコンからWebを利用してSBCサーバに接続するときの個人認証として，指紋を入力するだけでSBCサーバに接続できる。この製品は，ICカードの暗証番号であるPINコードの代わりに，指紋認証により指紋付きICカードの持ち主本人の指紋と照合できて初めてICカードの内部情報を読み出せるようになっており，バイオメトリクスを用いた2段階の個人認証なためICカードより更にセキュアな認証ソリューションと言える。さらに，指紋装置だけを用いサーバ側で指紋照合するソリューションも用意している。

4.3 文書利用権管理システムとSBC連携ソリューション

機密性の高い文書管理において，SBCだけではセキュリティ性を守れない場合も想定される。ある人に文書のアクセス権が付与されている場合(例えばメールの添付文書などの場合)，SBC単体では防止しきれないケースでも三菱電機利用権管理ソリューション<DROSY>(注4)を使用し文書を暗号化することにより第三者にそのファイルが渡った場合でも不正閲覧を防ぐことができる。また，機密文書の印刷などに対しても，利用者の資格に応じた利用制限(例えば印刷不可とする等)を文書ファイルごとに設定可能であり，情報漏洩防止が図れる。SBC環境においてサーバベースクライアントのICカードソリューションとDROSYを連携することで，より強固にセキュリティを保持し，利用者へ負担を強いることのないシステム環境を構築できる(図5)。

4.4 セキュアなSBC設計・構築・保守サービス

SBCは，サーバですべてのプログラムが動作し個人ファイルも含めてすべてサーバで管理することから，可用性の高いシステム構築が求められる。サーバのロードバランス設計，アクティブディレクトリのセキュリティポリシー設計，ストレージ設計，ネットワーク設計が重要であり，各種SBCシステム設計・構築・保守サービスを取りそろえている。

4.5 モバイルSBCソリューション

いつでもどこでも多様な通信手段を用いてSBCサーバに接続することで，社内でも外出先でも自宅でもオフィスと同じ環境を安心して利用できるモバイルSBCソリューションを提供している。

5. 事　例

(1) 経理業務アウトソーシング会社納めSBC構築事例

経理業務のアウトソーシングを受ける会社であるため，お客様の個人情報を大量に扱っていることから，お客様からも理解できる形でのセキュリティ強化が必要であった。そこで，SBCとサーバベースクライアントを導入し，お客様の個人情報漏洩防止のためにセキュリティを強化した(図6)。

(注4) DROSYは，三菱電機インフォメーションシステムズ㈱の登録商標である。

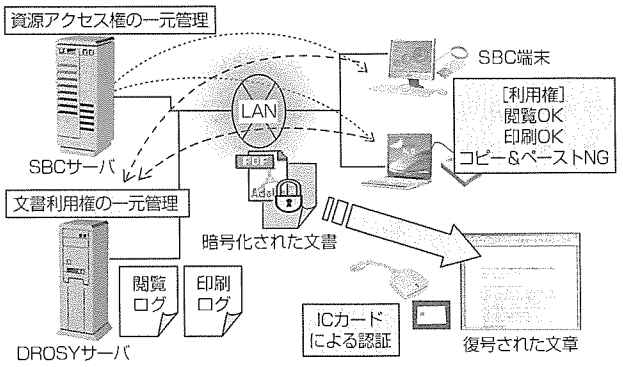


図5．DROSYにおける文書利用権管理システム

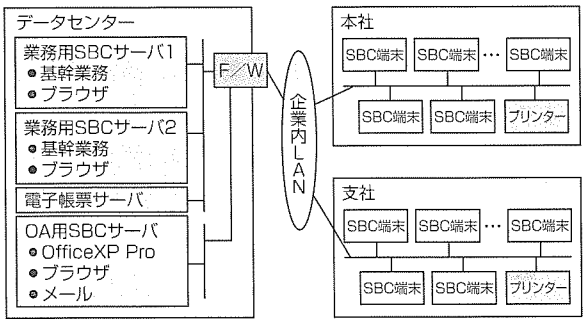


図6．経理業務アウトソーシング会社納めSBC構築事例

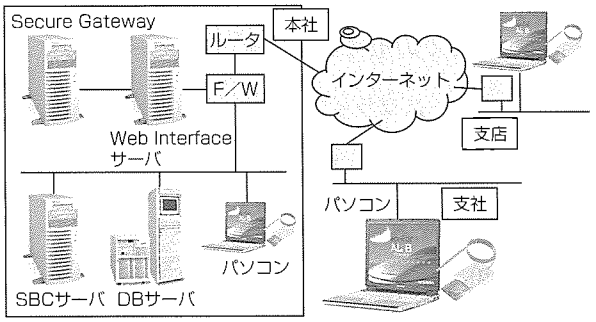


図7．SBCによるWeb対応インターネット接続事例

(2) SBCによるWeb対応インターネット接続事例

SBCのWeb接続機能を利用し，既存のC/Sシステムをそのままwebブラウザから接続可能とし，ICカードソリューションEasyLogin-Webを利用して個人認証することで，各支店・支社から本社のSBCサーバにインターネット接続でのセキュアなアクセスを可能にした(図7)。

6. むすび

運用/人的なセキュリティ面を技術的な仕組みとして向上させ，いつでもどこでも接続すればそこがオフィスとなるSBCセキュリティソリューションを紹介した。

SBCは，単にセキュリティ強化だけでなく，運用管理コスト削減においても非常に効果のあるソリューションであり，サーバ，端末，ソフトウェア，構築を含むトータルなSBCソリューションに更なる改善をしていく所存である。

ネットワークセキュリティソリューション

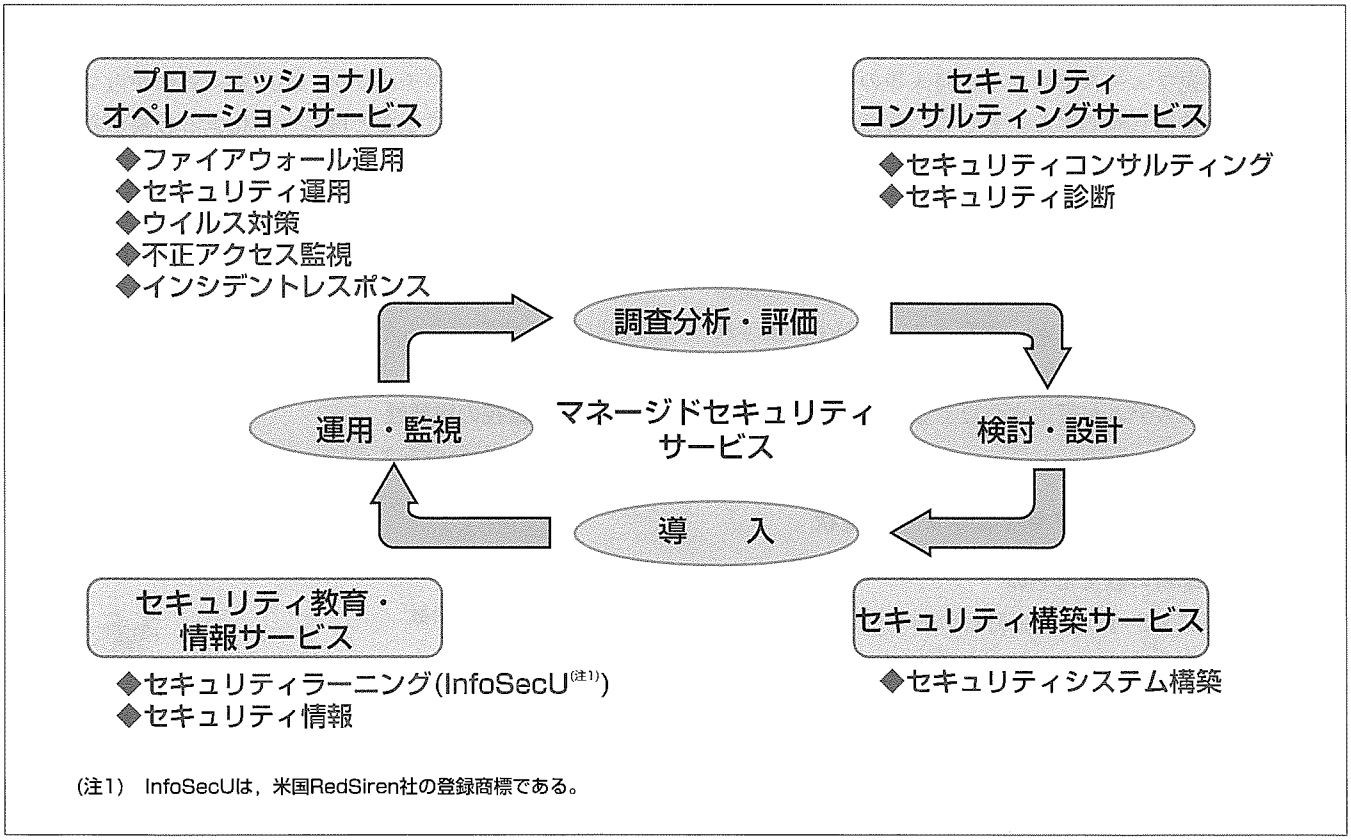
吉田　稔*
寺沢　茂*
山﨑義直*

要　旨

情報システムはネットワークの発達，とりわけ，インターネットの発展によって，利便性を持つことができた。その一方で，ウイルス，ワームや，サービス不能攻撃DoS(Denial of Service)等の不正アクセスの脅威にさらされているのも事実である。過日繁殖したMS-Blasterを見ると，対象ソフトウェアの脆弱(ぜいじゃく)性の公開からワームが現れるまでの時間は以前(NIMDAは脆弱性公開から6か月かかった)に比べ大きく短縮している(MS-Blasterは1か月で出現)。それだけ，迅速な対応が要求されていることが分かる。不正アクセスの手法も多様化し，これらに対応して，情報システムを守らなくてはならない。

ネットワークセキュリティで重要なことはライフサイクルに従って新たな脆弱性，脅威への対応を維持していくことである。これには，ネットワークセキュリティの高度な専門技術が必要になる。例えば，日々，多くのセキュリティ情報を収集し，自社システムに対処が必要か否か，緊急を要するか否かを判断しなくてはならない。これを自社で行うには，要員の確保・育成が必要で，時間とコストがかかる。ところが，脅威は待ってくれない。

このような状況に対し，三菱電機情報ネットワーク㈱(MIND)は，お客様に代ってネットワークセキュリティを実践するサービスを用意している。MINDマネージドセキュリティサービスは，ネットワークセキュリティのライフサイクル全般をカバーする各種サービスを用意している。



MINDマネージドセキュリティサービスの構成

MINDマネージドセキュリティサービスは，ネットワークセキュリティライフサイクルに対応したサービスを用意している。個々のサービスは互いに関連・連携し，システムのセキュリティという広い視野で提供されている。例えば，不正アクセス監視サービスでは，ファイアウォール情報，パッチ適用情報，セキュリティ診断結果等を考慮して監視を実施している。

*三菱電機情報ネットワーク㈱

1. まえがき

企業活動の基盤として，情報システムの重要性はますます高くなっている。情報システムは，インターネットの進展やブロードバンド化により，ネットワーク接続され，外部とのインタフェースが増えている。言い換えれば，利便性を享受する反面，リスクに直面していると言える。すなわち，ウイルスやワーム，システムへの不正侵入などのリスクにさらされていることになる。このようなアタックから情報システムの安定稼働を維持するため，ネットワークセキュリティを抜きにしては情報システムの“安全”“安定”は考えられなくなっている。

本稿では，**2章**で，ネットワークセキュリティのライフサイクルについて紹介し，**3章**でワームを通して得たセキュリティの現状を述べる。**4章**ではネットワークセキュリティのソリューションとしてのマネージドセキュリティサービスを紹介する。

2. ネットワークセキュリティのライフサイクル

ネットワークセキュリティには4つのフェーズからなるライフサイクルがある(**図1**)。調査・分析フェーズでは，情報システムの現状のリスクを分析し，検討・設計フェーズでセキュリティシステムを設計する。導入フェーズでは，セキュリティシステムを構築し，実際の運用をスタートさせる。運用監視フェーズでは，不正侵入等のチェック，新たな脆弱性を監視し対処する。そして，新たなリスクに備え，調査・分析フェーズに戻り，ライフサイクルを回していく。

重要なことは“セキュリティシステムを構築して完了”ではないということである。日々，新たな脆弱性が公開され，新たなウイルスやワーム，攻撃パターンが生み出されている(**図2**)。これらに対処していかなくては，構築したセキュリティシステムが役に立たなくなってしまうのである。

3. ネットワークセキュリティの現状

3.1 MS-Blasterの教えたもの

2003年8月にMS-Blasterと呼ばれるワームが大繁殖した。このワーム騒動は2点の教訓を残している。

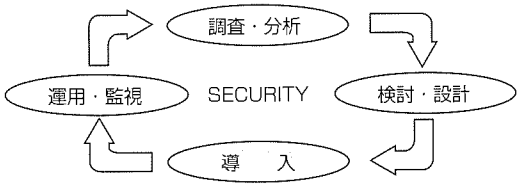


図1．ネットワークセキュリティのライフサイクル

3.1.1 脆弱性への迅速な対処

2001年にも，NIMDAというワームの大繁殖があった。NIMDAはMicrosoft IIS(注2)の脆弱性を利用したもので，この脆弱性の公開から6か月後にワームが登場している。一方，MS-BlasterはRPC(Remote Procedure Call)の脆弱性を利用したワームで，その脆弱性が公開されてからわずか1か月余りで登場している。すなわち，脆弱性の公開から実際に被害が出るまでの時間が1/6に短縮されている。もちろん，今回もこの脆弱性への対処をしていた情報システムには感染の被害はなかった。この事実は，情報システムにとって重要な脆弱性が公開された際には早い対処が必要であるということを伝えている。これには，日常からセキュリティ情報に注意し，対象となる脆弱性が自システムにあるかどうかを見極め，パッチ適用などの迅速な対処をする必要がある。

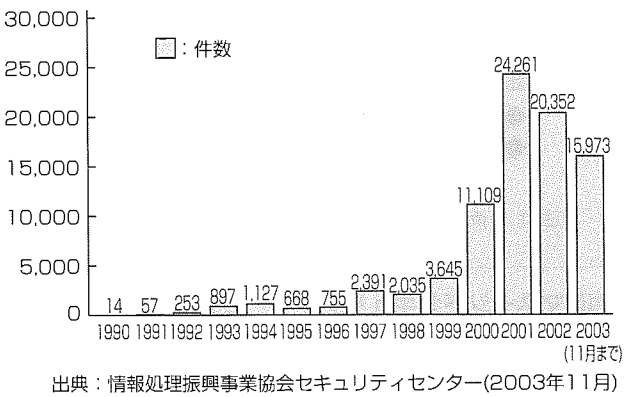
3.1.2 内部からの感染

MS-BlasterはRPCの脆弱性を利用したものであるため，ファイアウォールで外部からの侵入は防いでいたにもかかわらず，感染し，被害を受けた企業が多かった。外部からの感染には防御していたが，内部からの感染に対し無防備だったのである。実際には，外部から持ち込まれたパソコン，媒体を経由して感染したものである。ネットワークセキュリティでは“内部は安全”という思い込みがあった。内部からの不用意な行動を制御することが必要である。持ち込まれたパソコンのチェック，不用意に外部からソフトウェアを導入しないことなどはルール化する必要がある。また，内部からのアクセスにも不正アクセス監視システムIDS(Intrusion Detection System)を置き，監視するなどの対処も効果がある。MS-Blasterの場合は意図した感染ではなかったが，情報漏洩(ろうえい)などの事件の70%は内部による犯罪であるという事実にも目を向けるべきである。

3.2 運用監視の重要性

上記の例でも分かるように，ネットワークセキュリティ

(注2) IISは，米国及びその他の諸国におけるMicrosoft Corp.の登録商標である。



出典：情報処理振興事業協会セキュリティセンター(2003年11月)

図2．ウイルス届出件数の推移

への対処は迅速化，対象の拡大へ向かっている。しかし，しっかりしたセキュリティ運用監視をしていれば，防げていることも事実である。ファイアウォールを設置し外部ネットワークとの通信のフィルタリングを行うこと，IDSを導入し不正アクセスを監視すること，セキュリティ情報に注意し公開された脆弱性には迅速に対処することが肝要である。社内ネットワークへの接続にはウイルスやワームの感染がないことを事前チェックする等を確実に実施することで，被害は必ず防げるのである。一方，セキュリティ運用監視が不備であるため情報漏洩やサービス不能攻撃DoS(Denial of Service)の踏み台にされた場合，社会的な信用とともに，多大な損害を被ることになる。

3.3 セキュリティサービスの活用

ネットワークセキュリティのライフサイクルを回していくには，そのための体制が必要である。例えば，不正アクセス監視システムでアラームが上がった場合，そのアラームが緊急性を要するものか否かを迅速に判断し，対処を決めなくてはならない。また，現在，年間5万件ものセキュリティ情報(脆弱性情報)が公開されている。これらの情報を収集し，理解し，自社システムに必要な情報か否かでふるいにかけ，緊急な対処が必要か否かを判断しなければならない。これらへの対処には，ネットワークセキュリティの専門家かそれに準じるノウハウを持った人材と体制が必要である。これは時間とコストのかかることである。しかし，脅威となるアタックは待ってくれない。このようなネットワークセキュリティの実践を自社でできない場合は，専門家が提供するサービスを利用することによって質の高い対処を実践することができる。

4. マネージドセキュリティサービス

三菱電機情報ネットワーク㈱(MIND)は，ネットワークセキュリティのライフサイクルをカバーする“マネージドセキュリティサービス”を提供している。以下にその内容を紹介する。

4.1 MINDマネージドセキュリティサービスの特長

MINDマネージドセキュリティサービスの特長を以下に示す。マネージドセキュリティサービスは，表面に現れた情報だけでなく，その周辺にある様々な情報(機器の設定環境，パッチ情報等)を駆使し，トータルに判断・実施されるものである。また，セキュリティの基本は24時間365日の運用監視体制である。当然のことながら，セキュリティに休みはない。さらに，常に新しい情報，技術に沿ったセキュリティサービスであることが必要である。そして，サービス提供業者自身がネットワークセキュリティの管理がしっかりできていなくてはならない。これらの考えに基づいてMINDマネージドセキュリティサービスは提供されている。

MINDマネージドセキュリティサービスの特長は，次のとおりである。

(1) 情報システムの設定環境，状況を考慮し，トータルなセキュリティソリューションを提供する。

(2) 24時間365日の統合運用監視センターを基盤としている。

(3) 米国RedSiren社(旧SRI Consulting)の技術ノウハウを活用したサービスである。

(4) BS7799-2及びISMS適合性評価制度の認証を受けたセキュリティ管理システムの下で提供される安心できるサービスである。

4.2 マネージドセキュリティサービスの紹介

以下に幾つかの特長あるサービスを紹介する。

4.2.1 セキュリティ情報サービス

日々公開されるソフトウェアや各種機器の脆弱性情報をお客様に代って収集し，お客様システムへの影響の有無，緊急性を判断し，その対処を含めて報告するサービスである。緊急の場合は，即刻，その内容と外部接続の切断，パッチの適用などの対処をお客様に報告する。緊急性のないものは，月次で報告する。このサービスは表面的なシステム構成を知るだけでは実施できない。お客様システムの動き，情報の流れを知った上で提供される専門家によるサービスである。

4.2.2 監視アラームへの対応

構築したセキュリティ監視システムを使用し，24時間365日情報システムの異常を検知し，その対処を報告する。その代表的なサービスが不正アクセス監視サービスである。不正アクセス監視サービスでは，監視システムからのアラームへの対応スピードがポイントとなる。IDSは，センサに不正アクセスのパターンを持ち，監視している通信がこのパターンに一致した場合にアラームを上げて通知する。したがって，疑いのあるパターンはすべてアラームとして通知する。この通知内容と対象システムを考慮してその緊急度を判断しなくてはならない。これは高度の専門技術を必要とする作業である。MINDマネージドセキュリティサービスでは，IDSによるセキュリティ監視に二つの技術を加味して対応している。いずれも迅速な判断と対処へのアプローチで，被害の防止，最小化をねらったサービスである。

一つは不正アクセス防御システムIPS(Intrusion Prevention System)の導入である。IPSは，IDSの機能に加え，様々な異常を検知し，異常パケットの廃棄，セッションのリセットなど防御機能も持つシステムである(**図3**)。急激なトラフィックの増加，異常なアドレスを持つパケット，使用を禁止しているサービスへのアクセス等，設定に従ってセキュリティ異常を検知し，即時に対処を行うことができる。

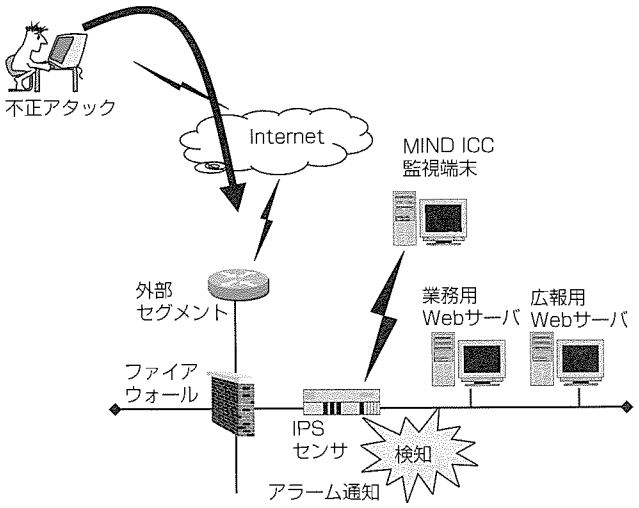


図3．IPS導入例

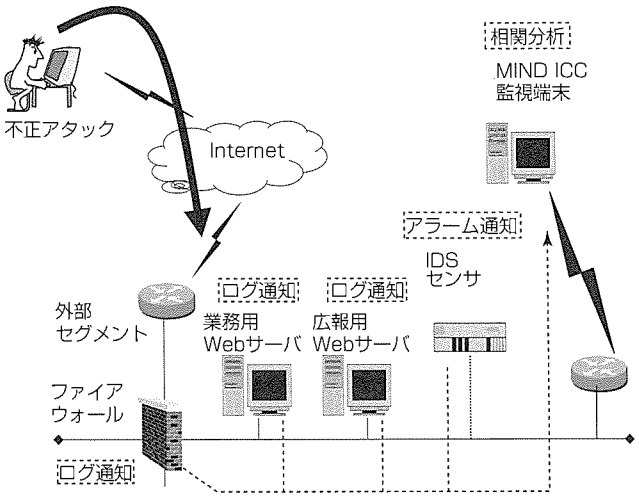


図4．相関分析システムの構成

二つ目は相関分析システムの導入である。これは，アラームが上がった場合，セキュリティ専門家が行う解析を自動的に行うシステムである。相関分析システムでは，マネージャーが，IDSだけでなく，ファイアウォールやサーバのログをリアルタイムに収集している。IDSからアラームが上がると，相関分析システムが関連するファイアウォールのログ，サーバのログを分析し，その危険度を判断する(図4)。危険であると判断した場合にアラームとして通知する。IDSでアラームとなっても，ファイアウォールで廃棄している場合は，相関分析の結果，アラームとはならなくなる。逆に，サーバで異常パケットを検知していれば，アラームとして緊急な対処が必要となる。セキュリティ専門家は，相関分析の結果を見て，対処を判断し，お客様へ報告を行うことになる。アラームの分析を自動化することで，迅速な判断と対処が可能となる。

4.3 セキュリティ診断サービス

ネットワークシステムのセキュリティレベルは，日々の脆弱性公開だけでなく，操作ミスや不用意な設定変更によって低下する。これをチェックするには定期的なセキュリティ診断が有効である。セキュリティ診断サービスは，お客様のシステムに擬似的な攻撃を試みてシステムのセキュリティ度を診断するサービスである。これも，単に診断ツールを使用しその結果を報告するだけでは不十分である。対象システムの構成，情報の流れ，運用を考慮しセキュリティレベルを判断しなくてはならない。

従来型の外部からネットワークレベルまでの擬似攻撃を行う診断に加え，Webアプリケーション専用のWebアプリケーション診断が増えている。Webアプリケーションが増えた一方，クロスサイト・スクリプティングなどの不正情報入手手段が既知になっており，アプリケーションレベルでのリスクが増大している。これらの脆弱性を，ツールだけでなく，ノウハウを持った専門家が診断を実践するサービスである。これにより，自社システムのセキュリティレベル，リスクを対処とともに事前に知ることができる。

4.4 セキュリティ教育サービス(e-Learning)

ネットワークセキュリティは，一部の人の努力で実現できるものではなく，全員で築き，維持するものである。したがって，各社員の立場に対応したセキュリティ教育が必要である。セキュリティ教育サービスISU(Information Security University)は米国Carnegie Melon Universityとの提携で生まれたWebシステムを使用した教育システムで，利用者のスケジュールに合わせて受講することができる。その理解度のチェックのための修了試験も用意されている。

5. むすび

ネットワークセキュリティはますます重要になっていく。しかし，守る情報資産の重要度(価値)とかける費用とのバランスが重要である。今後も，最新のセキュリティ技術を取り入れ，“安全”“安心”を少しでも多く提供できるようにサービスの充実を図っていく。

セキュリティ技術を活用したトータルWebインテグレーションフレームワーク“セキュアWebソリューション”

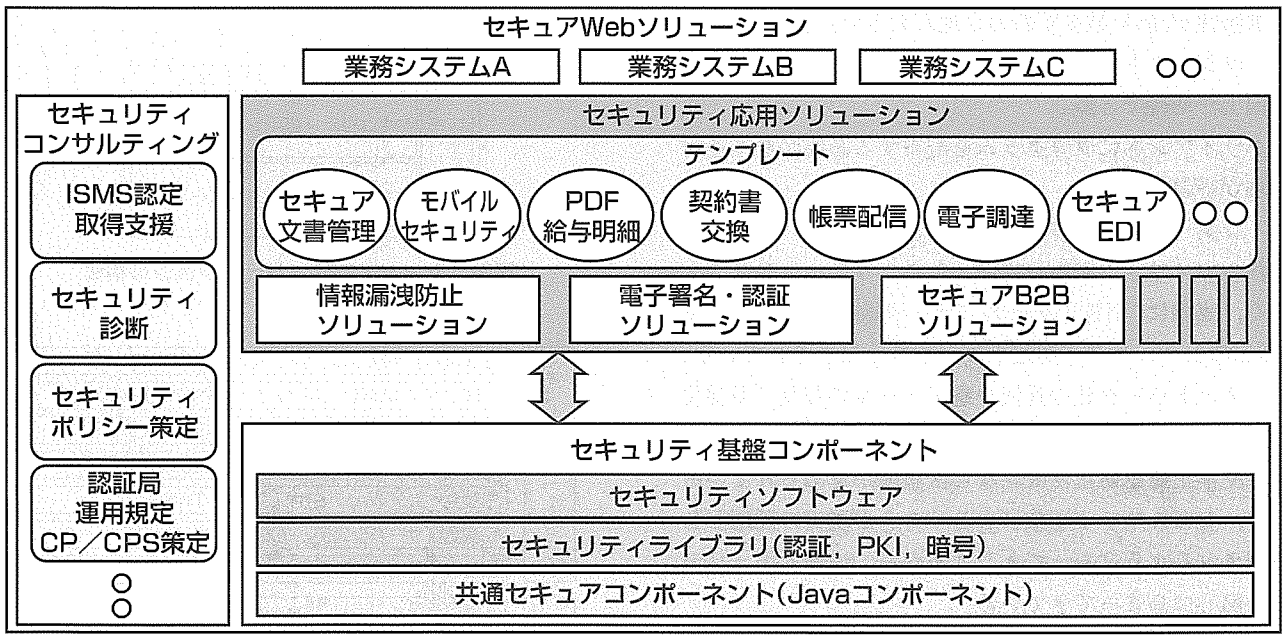
田名網淳夫* 角野章之**
遠藤 淳* 釜坂 等***
鷲津 忍*

要 旨

インターネットの普及，Java仕様の成熟化などによりWebベースのシステムニーズが拡大しており，これまで困難とされていた基幹系システムをWebベースで再構築する事例も増えている。Webベースのシステムは，プラットフォーム依存度が低く，システム開発費用・運用費用を抑制できるなど多くの利点が挙げられる。一方で，Webは情報公開・共有技術として開発されたものであるため，サーバへの不正アクセスやデータの盗聴などセキュリティ上のリスクが多いことも事実である。また，セキュリティに対する企業の関心が高くなり，すべてのシステムにセキュリティが求められているといっても過言ではない。

三菱電機インフォメーションシステムズ㈱(MDIS)では，Webベースシステムのセキュリティ上の課題を解決したり情報システムにセキュリティ機能を実装するためのフレームワークとして，“セキュアWebソリューション”を提供している。セキュアWebソリューションは，人的・物理的な側面も含めた情報セキュリティシステムを構築するためのセキュリティコンサルティング，PKI(Public Key Infrastructure：公開鍵(かぎ)基盤)関連ライブラリを始めとするセキュリティ基盤コンポーネント，情報漏洩(ろうえい)の防止やセキュアなB２B(Business To Business)環境及びこれらの活用ノウハウを集積したセキュリティ応用ソリューションから構成される。

MDISのセキュアWebソリューションは，これまでに蓄積したWeb技術とセキュリティ技術を活用して，特にセキュリティリスクに対する企業情報システムの多様なニーズにも対応できる安全で安心なWebベースのシステムインテグレーションサービスを提供する。



ISMS：Information Security Management System，CP：Certificate Policy，
CPS ：Certification Practice Statement，PDF：Portable Document Format，
PKI ：Public Key Infrastructure，EDI：Electronic Data Interchange

セキュアWebソリューションの体系図

この図は，セキュアWebソリューションの体系を示したものである。情報セキュリティシステムの構築コンサルティングサービスとセキュリティ基盤コンポーネントや情報漏洩防止，電子署名・認証，セキュアB2Bなどの各ソリューションを活用して，顧客ニーズにフィットした業務システムを迅速に構築するセキュリティ応用ソリューションを提供する。

*三菱電機インフォメーションシステムズ㈱ **三菱電機情報ネットワーク㈱ ***三菱電機㈱ 情報技術総合研究所

1. まえがき

インターネットの普及，ハードウェアの高性能化と低価格化，J2EE(Java2 Enterprise Edition)に代表されるJava仕様の成熟化などにより，急速なWeb技術の普及が進んでいる。“企業グループ全体での最適化”“プロセス統合による業務改善”“汎用機からのリプレース”など企業内の大規模な基幹系システムの再構築でも積極的にWeb技術が採用されつつある。政府においても，経済産業省が高度な電子政府システム実現のために発足させた“ITアソシエイト協議会”の中間報告の中で，Webアプリケーションを中心としたモデルが示されている。

MDISでは，得意とする情報セキュリティ技術とWeb技術の体系化を進めている。

本稿では，このセキュアWebソリューション体系の構成要素について述べ，その中のセキュリティ応用ソリューションの事例を紹介する。

2. セキュアWebソリューション

2.1 背　景

Webベースのシステムには多くのメリットが挙げられる。

(1) ネットワーク型システムに適している。
(2) ミドルウェアやプラットフォームの依存度が低い。
(3) 拡張性が高い(技術革新の余地が大きい)。
(4) オブジェクト指向開発に適しており，生産性・保守性の向上が期待できる。
(5) クライアントにプログラムを配布する必要がなく運用管理が容易である。
(6) インターネットを容易に活用できる。

これらのメリットがある反面，セキュリティ上のリスクも多く，実際に“不正アクセス”“データ改ざん”“データ流出”などのセキュリティ関連事故が数多く報告されている。また，ネットワーク化の進展や電子メールの普及，多様化する雇用形態などの社会環境の変化に伴って個人情報保護法成立や不正競争防止法改正など法整備が進められていることや，セキュリティ事故によるリスクが現実の問題として認識されるようになってきたことから，情報セキュリティへの関心は高まってきている。

このようなニーズにこたえるために，セキュリティ技術を活用したトータルなWebインテグレーションフレームワークを，セキュアWebソリューションとして体系化した。このソリューションを提供することにより，以下のようなメリットを生み出し，ITによる企業の業務革新を安全・安心なシステムで実現することを可能とする。

(1) セキュリティを考慮した共通セキュアコンポーネントを再利用することで，セキュリティの高いシステムを効率的に構築
(2) 暗号，署名・認証などのライブラリを活用して高度なセキュリティ機能を実装
(3) 文書管理やB2Bなどのソリューションにセキュリティ機能を組み込むことで新たな付加価値を創出

2.2 セキュアWebソリューションの構成

セキュアWebソリューションは，**図1**に示すように，大きく3つのパートから構成されている。

それぞれの詳細は次のとおりである。

2.2.1 セキュリティ基盤コンポーネント

セキュリティ基盤コンポーネントは，セキュアなシステムを構築するための文字どおり基盤をなすコンポーネント群である。単体でセキュリティ機能を実現している暗号やPKIを応用したソフトウェア製品，システム(アプリケーション)にセキュリティ機能を実装するためのライブラリ製品，セキュアなシステムの構築に利用できる共通セキュアコンポーネントで構成される(**図2**)。

それぞれのコンポーネントは，PKI技術や暗号アルゴリズムMISTY(注1)を始めとした三菱電機グループのセキュリティ技術を活用した特長的なソフトウェアである。システム構築に必要なソフトウェア上のセキュリティを“共通セキュアコンポーネント(Javaコンポーネント)”としてまとめ，再利用することでシステム構築における生産性を高めることができる。

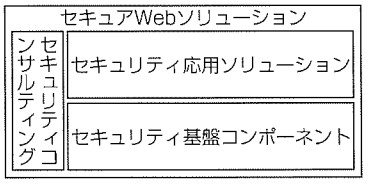
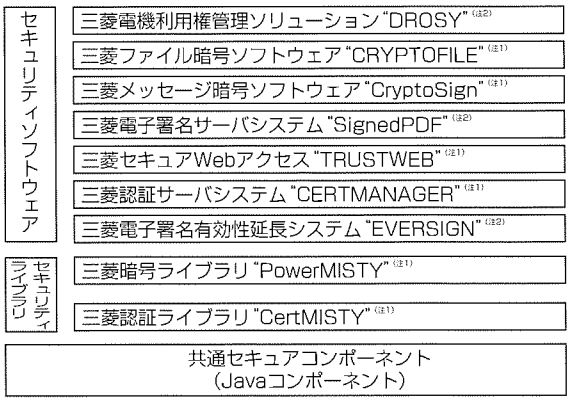


図1．セキュアWebソリューションの構成



(注1) MISTY，CRYPTOFILE，CryptoSign，TRUSTWEB，PowerMISTY，CERTMANAGER，CertMISTYは，三菱電機㈱の登録商標である。
(注2) DROSY，SignedPDF，EVERSIGNは，三菱電機インフォメーションシステムズ㈱の登録商標である。

図2．セキュリティ基盤コンポーネント

2.2.2 セキュリティ応用ソリューション

セキュリティ応用ソリューションは，要旨のイメージ図に示したように，セキュリティ基盤コンポーネントと，企業や官公庁・自治体における情報の漏洩を防ぐための情報漏洩防止ソリューション，電子文書を安全に扱うための電子署名・認証ソリューション及び企業間のセキュアなデータ交換を行うためのセキュアB2Bソリューションなどを活用して高度な情報セキュリティシステムを構築するためのソリューションである。また，各種業務システムの構築ノウハウをテンプレートとして蓄積しているので，顧客ニーズにフィットしたシステム化を短期間に構築できる。

2.2.3 セキュリティコンサルティング

セキュリティコンサルティングは企業や官公庁・自治体などの情報セキュリティシステムを人的・物理的な側面も含めて構築するコンサルティングサービスであり，現在は次の4つのサービスメニューを用意している。

(1) ISMS認定取得支援(ISMS構築運用支援サービス)

これまで企業などの組織におけるセキュリティは外部の脅威への対策がクローズアップされていたが，社会的な環境変化やネットワーク化の発達などにより，内部の脅威への対策も重要視されてきた。これらのセキュリティを総合的・体系的に管理することが組織の安全と信用に不可欠であることから，ISMS(情報システムマネジメントシステム)の導入が盛んになっている。

このようなニーズに対し，“ISMS構築・運用の支援”及び“ISMS適合性評価制度に基づく認定取得の支援”を行うコンサルティングサービスを用意している。認定取得の実績も多数あり，豊富な実績を基にコンサルティングを提供している(図3)。

(2) セキュリティ診断(情報セキュリティベンチマークサービス)

ISO17799等の国際基準に適合しており，セキュリティポリシー，物理的セキュリティから運用管理のセキュリティまで，10種のセキュリティ領域をカバーしたベンチマーク分析を実施している。企業における情報セキュリティ投資のレベルを判断する材料として利用することができ，定量的な他社との比較を行うこともできる。

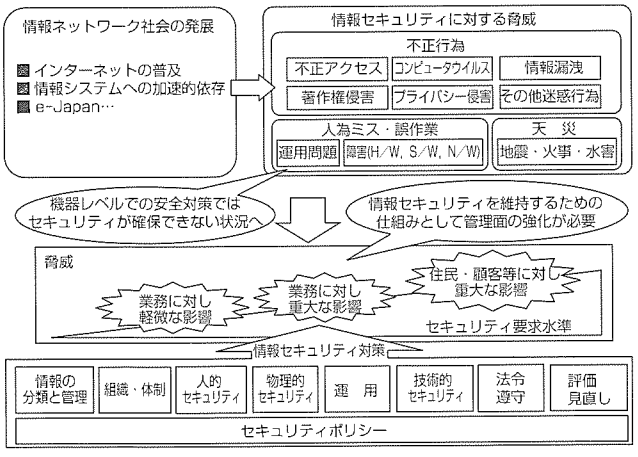


図3．ISMS構築運用支援サービスのイメージ

(3) セキュリティポリシー策定(セキュリティポリシー・ベストプラクティスパッケージ)

企業や官公庁・自治体向けのセキュリティポリシー策定をサービスメニューとして用意している。LGWAN(Local Government Wide Area Network：総合行政ネットワーク)にも対応しており，実績を基にした具体例及びサンプル文書を提示し，運用・保守性の高い情報セキュリティポリシー策定を支援する。

(4) 認証局運用規定CP／CPS策定(特定認証業務認定取得支援サービス)

このサービスは，電子署名法で定める認証業務を行う認証局の構築に必要な証明書のポリシー及び認証局の運用規定の作成支援をするものである。認証局構築の実績に基づいた“業務設計”“トラステッドロール提案”及び“審査基準提案”を行いながら，認証局としてのCP及びCPSの作成を支援する。

3. システム事例

3.1 電子帳票配信サービス

セキュリティ応用ソリューションのシステム事例として，三菱電機情報ネットワーク㈱(MIND)向けにMDISが構築した“電子帳票配信サービス”がある(図4)。これはMINDが展開しているEDIサービスの付加価値サービスの一つであり，MDISの企業間電子商取引システム“EDIFOAS／B2B(注3)”と電子署名ソフトウェア“SignedPDF”を活用し，帳票配信テンプレートを使って短期間に構築した(2004年サービス開始予定)。

これまでのEDIは発注・仕入れ・請求など取引データの送受信をオンライン化することで業務を効率化していたが，実業務では依然として請求書や帳票などのビジネスドキュメントが紙で存在している。電子帳票配信サービスは，これらビジネスドキュメントの発送など，ハンドリングを含めた業務の効率化を実現することができる。取引によって発生する請求書や帳票などのビジネスドキュメントはPDFファイルとして電子帳票化し，電子署名によって文書の真正性を確保することで，安心・安価・確実・迅速に配信することが可能となる。

例えば，EDIによって受信した受注データを利用して，締め日ごとに請求書を電子署名付きPDFで生成する。請求書が配信可能になったことを支払元(発注側)に電子メールで通知し，支払元はWebを利用して請求書をダウンロードする。ダウンロードデータはHTTPS(Hyper Text Transfer Protocol Security)によって暗号化されているた

(注3) EDIFOAS／B2Bは，三菱電機㈱の登録商標である。

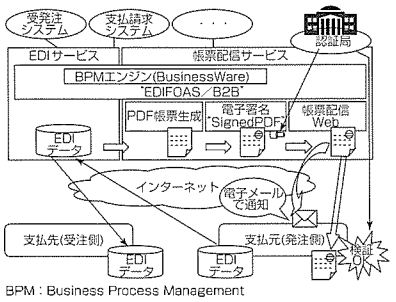


図4．MINDの電子帳票配信サービスのイメージ

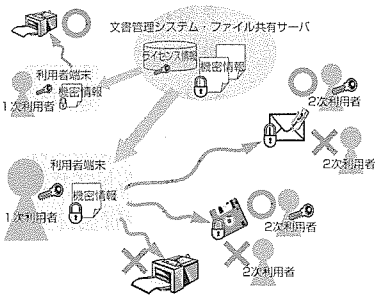


図5．"DROSY"の利用権管理機能

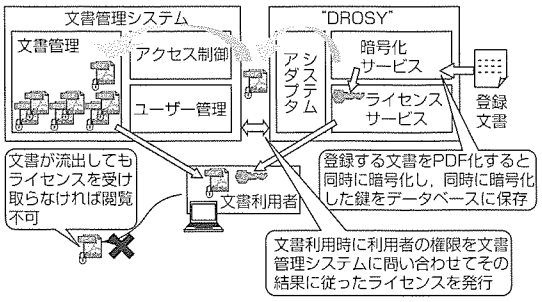


図6．共有文書機密管理システムの事例

め盗聴される心配はなく，請求書自身も電子証明書を使用した電子署名によって真正性を確認できる。また，支払先(受注側)もWebによって請求書のダウンロード状況を確認することができる。電子帳票はユーザー・フォーマットごとに対応し，支払い通知や買掛一覧などEDIに関連する帳票配信をサービスとして提供する。

"EDIFOAS／B2B"にはBPM(Business Process Management)エンジンとしてVITRIA(注4)社のBusinessWare(注4)が組み込まれているため，EDIを中心に様々な付加価値サービスを拡張することができる。また，ebXML(electronic business eXtensible Markup Language)やWebサービスにも対応することによってサービスの幅を広げていく予定である。

3.2 共有文書機密管理システム

情報漏洩防止を目的としたセキュリティ応用ソリューションのシステム事例として，MDISが某製造業向けに構築した共有文書機密管理システムがある。このシステムは，社内共有文書の閲覧を許可された利用者だけに限定するもので，情報漏洩防止ソリューションのコンポーネントの一つである三菱電機利用権管理ソリューション"DROSY"を活用して構築した。

"DROSY"は，DRM(Digital Rights Management)技術を応用した再配布コンテンツのセキュリティを確保するためのソリューションで，PDFやMicrosoft(注5) Office文書を暗号化し，認証された利用者にだけライセンス(復号鍵＋利用情報)を配布して暗号化した文書の閲覧を可能とする。ライセンスは，利用者ごとにパーソナライズ(個別化)しているため，万が一，他の利用者がこのライセンスを不正に入手したとしても利用することはできない。暗号化した文書はメモリ上でのみ復号し，平文を作らないことにより不用意な情報の漏洩を防ぐ。また，利用者の閲覧権限は回数，期間などで限定できるので，様々な利用形態に適応できる。"DROSY"のサーバ側ソフトウェアはJ2EEで作られており，ユーザーインタフェース及び外部システムインタフェースもすべてWebベースにしている(図5)。

従来，文書管理システムなどで文書のセキュリティを確保するためには，オペレーティングシステムやソフトウェアのファイルアクセス制御機能を使っていたが，この"DROSY"を活用することで文書管理システムなどから文書を取り出した後も常にユーザーの利用権限をチェックすることができ，万が一，故意・過失によって文書ファイルが流出した場合でも，内容の漏洩を阻止することができる。

DROSYは，既に文書管理システムが導入されているユーザーにも容易に導入することができる。例えば，共有文書をPDF化する業務フローにDROSYで暗号化する処理を追加することで，共有するPDF文書に利用制限を設定することができる。また，文書管理システムで利用者認証にLDAP(Light weight Directory Access Protocol)サーバを利用している場合，DROSYもこれを利用して文書管理システムのアクセス権をそのまま引き継ぐことが可能である。これにより，文書セキュリティシステムを導入した後も，ユーザーは，従来の処理フローと変わりなく，文書を利用することができる。万が一，ユーザーが手元にダウンロードしたPDF文書が媒体や電子メールで外部に流出しても，文書管理システムにおいて利用者の閲覧権限を確認しなければそのPDF文書を開くことはできない(図6)。

機密情報の共有において，これまではセキュリティの観点から共有する範囲を限定していたケースでもDROSYを導入することによりセキュアな情報共有が可能になり，セキュリティの確保と生産性向上の両立を図ることができる。

4. むすび

今後，システムのWebベース化や業務システムでのインターネット利用の拡大，Webサービスの普及などによって，これまで以上に情報システムにおけるセキュリティの確保が必要になる。この意味でも，SIベンダーとしては，安全で安心なソリューションを確実に提供することがますます重要になってくる。進化する環境とニーズに応じてセキュアWebソリューションをより一層充実させ，安全・安心と利便性を両立させた情報システムソリューションを提供していく所存である。

(注4) BusinessWare，VITRIAは，米国Vitria Technology. Inc. の登録商標である。

(注5) Microsoftは，米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。

顧客ニーズの抽出・活用を迅速・安全に支援するWebマーケティングソリューション“ActiveMarketer”

土田泰治* 相川勇之**
磯西徹明*
稲垣尚史*

要 旨

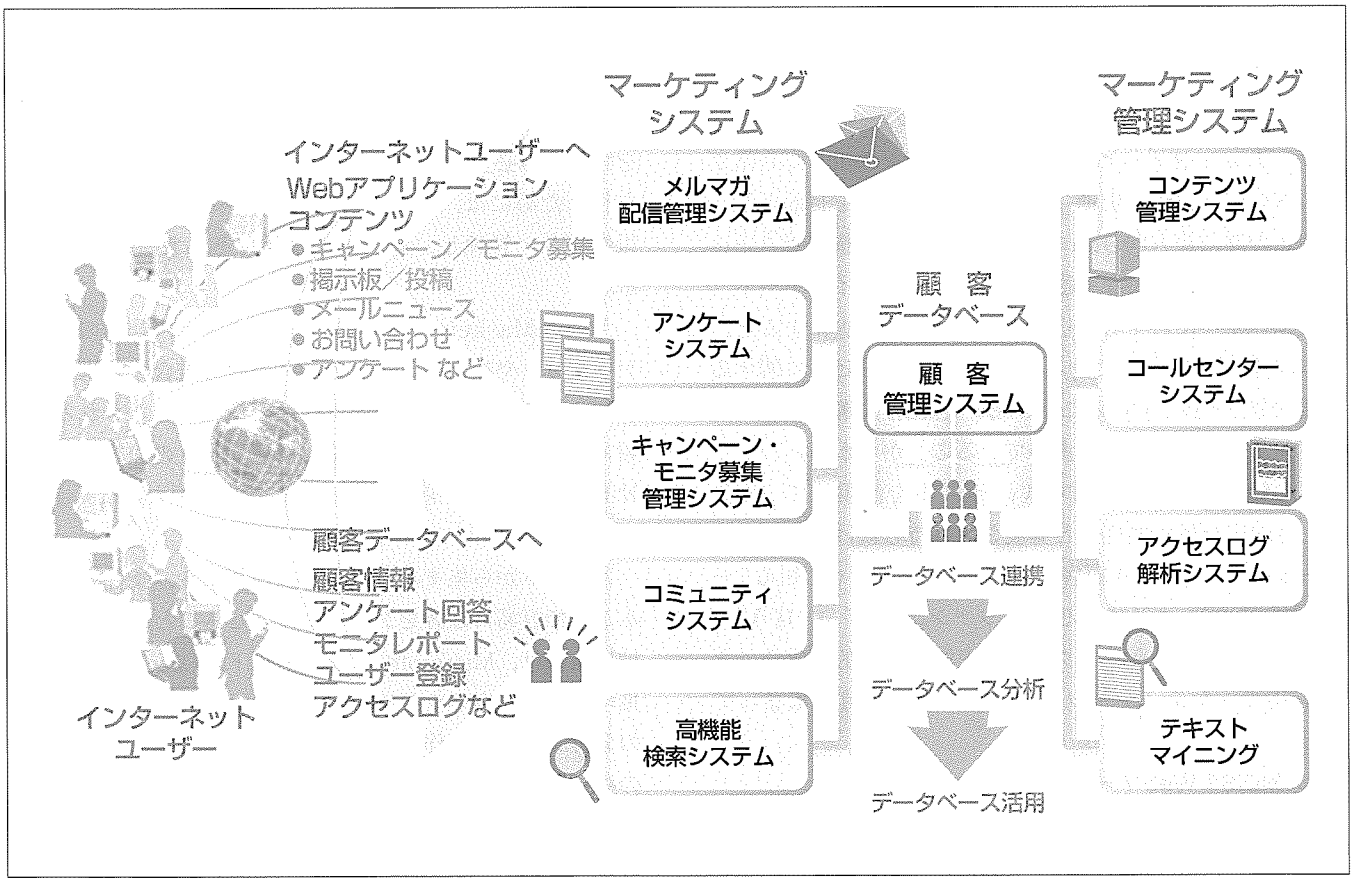
インターネット・ユーザーに対する㈱UFJ総合研究所の調査によると，“企業のWebサイトが消費者との関係強化に役立っている”という回答が約9割，“一般企業のWebサイトをよく見ている又はたまに見ている”という回答が約8割あり，企業のWebサイトは“企業と消費者との関係強化のためのコミュニケーションツール”として一定の役割を果たしている。

しかしながら，企業のWebサイトはカタログなどの情報提供機能が中心のため，顧客のニーズや製品開発に結び付く情報の収集ができていないのが実情である。

三菱電機インフォメーションシステムズ㈱（MDIS）のDiamondStream(注1) ActiveMarketer(注2)（以下“ActiveMarketer”という。）は，顧客データベースを中心にアンケートやメルマガなどのサブシステムを連動させ，戦略的なWebマーケティングを実現するソリューションである。能動的に顧客をサイトに呼び込み，顧客の情報や意見を集め，顧客情報の獲得→顧客の囲い込み→顧客からの意見聴取→顧客から集めたデータの活用という流れでマーケティングを行うことができる。

ActiveMarketerは，顧客へ情報を安全・的確に配信するメルマガ配信機能，顧客の意見を聴取しやすいアンケート機能，顧客情報を統合して管理する顧客データベース機能，顧客の意見から特徴的な情報を簡単に取り出せるテキストマイニング機能など，顧客ニーズの抽出・活用を迅速・安全に支援するWebマーケティングの必要機能を網羅している。

（注1） DiamondStreamは，三菱電機㈱の登録商標である。
（注2） ActiveMarketerは，三菱電機インフォメーションシステムズ㈱の登録商標である。



ActiveMarketerの構成

ActiveMarketerは，顧客データベースを中心にメルマガ配信管理システム，アンケートシステム，テキストマイニングなどが連携しており，各システムが顧客データベースと連携してWebマーケティングが行えるため，顧客ニーズの抽出・活用が迅速・安全に対応可能となる。

*三菱電機インフォメーションシステムズ㈱ **三菱電機㈱ 情報技術総合研究所

1. まえがき

インターネットの進展により，ネットワークのブロードバンド化，常時接続化されることにより，家庭や職場でWebを見ている時間が長くなり，Webが消費者と企業との関係強化に役立ってきている。

本稿では，能動的に顧客をサイトに呼び込み，顧客の情報や意見を集め，顧客から集めたデータを活用してマーケティングを行うWebマーケティングソリューションActive Marketerを紹介する。

2. Webマーケティングソリューションの市場動向と取り組み

2.1 Webマーケティングの市場動向

一般に新しいサービスや商品は，その世帯普及率が15%を超えると，その需要は顕在化し，大きなビジネス市場を形成すると言われている。総務省の調査では，ブロードバンドの世帯普及率が約22.3%(2003年5月)に達し，まさにブロードバンドインターネットを中心とした新市場が形成されようとしている。この普及は，利用するユーザー層の多様化，ユーザー数とその利用時間の増加と利用シーンの拡大を生み，一般消費者を対象とする企業に様々なビジネスチャンスを与えている。

このようなブロードバンドインターネットの進展に伴い，企業のWebサイトは，単なる情報発信の一手段からリッチコンテンツやマーケティングツール等を活用した企業ブランドの向上，販売促進，宣伝，商品開発等を目的とし，顧客との間に双方向One-To-Oneの関係を構築できるe-ビジネスの最も重要な手段となりつつある。インターネット・ユーザーに対する㈱UFJ総合研究所の調査によると，Webの利用目的として約9割が“商品・サービスに関する情報収集”を挙げていることから，消費者の購買行動において非常に重要な役割を占めていることが分かる。

この動向の中で，企業のWebサイトを活用して一度獲得した顧客を優良顧客へと発展させ維持し続けられるソリューション，つまり顧客が商品やサービスを“知る”→“興味を持つ”→“理解する”→“ファンになる”→“買う”→“人に勧める”というサイクルを効率的，効果的に実施できるWebマーケティングソリューションに注目が集まっている。

2.2 MDISのWebマーケティングへの取り組み

MDISでは，このような背景の中で，戦略的にWebサイトを構築し，積極的にメルマガ配信やアンケート，キャンペーンやモニタ募集などを実施し，様々なデータを集め，そのデータを活用してマーケティングを行うWebマーケティングソリューションActiveMarketerを開発し，これを核とした“企業Webサイト及びマーケティングサイトの構築サービス”を提供している。

電子メールやWebアンケート等を応用した従来のマーケティングツールは，アプリケーションごとに顧客情報を持っているため，アプリケーション間でのデータ連携が困難で，収集したデータの集計から分析までに時間がかかるなど貴重なデータを十分に生かすことができなかった。

ActiveMarketerは，それぞれのアプリケーションのデータが別々に存在するのではなく，各アプリケーションの顧客情報を連携・統合させることにより，アンケート回答結果，モニタレポート，製品に対する意見・感想，メルマガへの反応等を関連付けることが可能となり，多種多様なニーズに沿った分析ができる。

このActiveMarketerは，主婦層を対象とした三菱電機のマーケティングサイトである“シュフレー”などで活用されており，冷蔵庫，ファンヒーター，オーブンレンジ等の家電製品の宣伝活動，製品開発等に結び付く情報収集に効果を上げている。

3. ActiveMarketerの特長

この章では，ActiveMarketerの特長的機能である顧客データベース，メルマガ配信管理システム，アンケートシステム及びテキストマイニングについて紹介する。

3.1 顧客データベース

Webサイトの多様化により，会員ページや特定商品・サービスの専用ページなど複数のサイトやページで顧客情報を管理する必要性が増えている。効果的なマーケティングを行うためには，複数サイトやページに分散した顧客情報を統合・管理し，総合的に活用できる機能が必要である。

ActiveMarketerの顧客データベースは，複数のアプリケーションや複数のサイトの顧客情報を統合・連携して管理しているため，あるサイトの顧客情報が更新されると，顧客データベースの顧客情報と関連サイトの顧客情報が自動的に更新され，常に最新の顧客情報に保たれている(図1)。

各サイトから集まる幅広い顧客情報から，条件を指定することで容易に顧客をグループ化させることも可能である。抽出結果は，Microsoft(注3)Excel(以下，Excel)で自由に編集可能で，顧客のランク付け評価や，マクロを使った顧客の分析レポートの作成も簡単にできる。また，グループ化の結果は，再度顧客情報へ反映させ，メルマガ配信の送付先を決定するなどに利用できる。

3.2 メルマガ配信管理システム

メルマガ配信管理システムは，サイトに登録した会員へのメールマガジンの配信や株主などの投資家向け情報の配

(注3) Microsoftは，米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。

信，マスコミへのニュースリリースの案内など様々なメール配信シーンに対応している。メルマガ配信管理システムは，的を絞ったメール配信ができるよう，年齢や性別といった配信先条件を事前に設定登録することが可能で，顧客データベースとの連携により常に最新の対象者にメールを配信できる。この配信先条件の事前登録機能によりオペレータは顧客情報を見なくても配信ができ，配信オペレータの誤操作による顧客情報の漏洩(ろうえい)などを起こすことなくメルマガの配信が可能である。不正メールアドレス，重複メールアドレスチェック機能により，無駄なく，安全・的確にメールマガジンを配信することができ，また，エラー設定で配信エラーとなったメールアドレスに対して配信停止や顧客データベースからの自動削除を行うことができ，常に有効なメールアドレスを保存管理できる。

また，顧客データベースとも連携しているので，常に最新の顧客属性を利用した情報配信ができる。パーソナライズ(顧客の名前などをメールに埋め込む)や，オプトイン情報(属性情報にマッチした内容の差し込み)の設定で，個人向けメールマガジンの作成が容易にでき，配信後メールに埋め込まれたURLのクリックカウント集計機能を利用することで，詳細な関心度も把握でき，更なる顧客の関心をひくメールマガジンの配信が可能となる。

3.3 アンケートシステム

アンケートシステムは，バリエーション豊富な質問が設定でき，背景画像指定やレイアウトなどによる意匠設定，HTML(Hyper Text Markup Language)記述による拡張設定など多彩な編集機能を搭載している。また，Webブラウザからの操作で，だれでも簡単に完成度の高いアンケートページが作成できる。過去のアンケートから現在実施中のアンケートまで回答データをすべてデータベースに格納し，必要に応じて指定した回答データを引き出せる。また，アンケートを複数同時に実施できる。この回答データは自動的にデータベースに登録されるので，管理者は，実施期間を問わずいつでもアンケート情報を閲覧できる。また，集計データは必要な情報のみ抽出できるので，無駄なく分析できる。CSV(各項目のデータをカンマで区切った形式のファイル)出力機能により，Excelなどでデータ分析を行うこともできる。テキストマイニングとの連携でアンケートの自由回答欄からニーズ等の抽出も可能となっている。

3.4 テキストマイニング

大量に蓄積された電子メールやアンケートデータ中には，顧客の“生の声”がテキストデータとして含まれている。テキストマイニングとは，大量のテキストデータから有用な情報を抽出してマーケティングや顧客満足度の向上に活用するための技術である。

Webを利用するアンケートは，紙のアンケートと比較して大量の回答を迅速に収集可能であり，また，自由意見のテキストの記述量が多いなどの特徴がある。このような大量テキストの分析を人手で行うには限界があり，テキストマイニングの利用価値が大きい。

従来のテキストマイニングは，指定された単語及び単語の組合せをテキスト中から抽出して統計的に分析を行うので，類似の内容を表わす複数の表現が分析対象中に存在する場合には，あらかじめ類義語辞書を作成する必要があり，このような類義語辞書を対象分野ごとに構築するための時間と経験が必要という課題があった。

そこで，三菱電機㈱は，テキストの分析作業を効率化するための概念抽出型テキストマイニング方式を開発した[(1)(2)]。この方式の特長は，テキスト中に同時に出現する単語や複合語の関係から言葉の関連性を自動抽出することにより，分析対象文書ごとに作成していた類義語辞書を不要にしている点である。自動抽出した言葉の関連性は概念ベクトルという内部形式で表現する。この概念ベクトルを索引として用いることにより，入力した検索文と類似する内容を持つテキストを検索する概念検索や，“さわやか”と“爽快”という言葉を同一の回答グループとするような各種の相関分析が可能になる。

図2はエアコンのアンケートを対象とする分析結果で，アンケートの選択式回答欄のうち，“非常に満足”と回答した顧客がどのような理由で満足しているかを顧客の年代別に分析した例である。分析の対象となるテキストは，シス

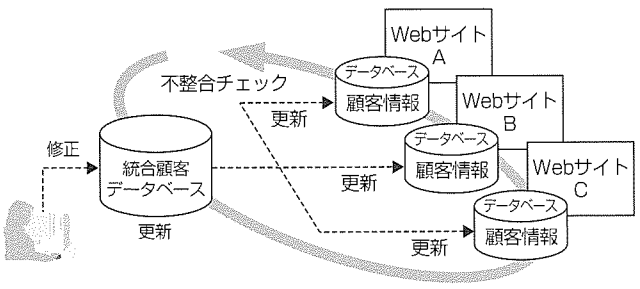


図1．顧客データベースの考え方

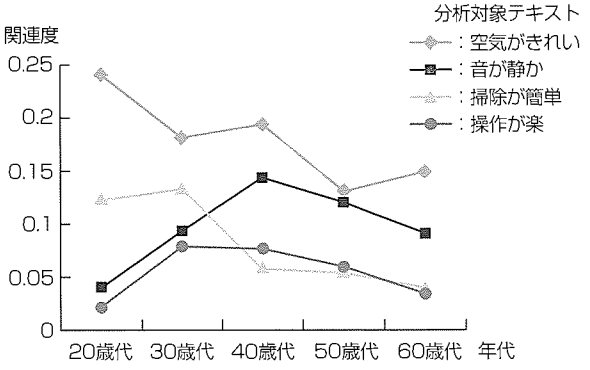


図2．エアコンアンケートの分析結果例

テムが提示する候補から選択する方法と，分析者の新たな発想で自由入力する方法の両方が可能である。関連度は各年代別意見と指定テキスト内容を含む意見との関連性の強さを示す指標であり，上記の概念ベクトルを基に計算する。図の結果から，“若年層は空気清浄機能及び掃除の簡単さに対する満足度が高く，中高年齢層は作動音の小ささに対する満足度が高い”ということが分かる。

この概念抽出型テキストマイニング方式を利用することで，アンケートから容易に顧客意見や要望が抽出でき，製品の次機種開発企画などに有効活用できる。この方式は㈱アイプラネットの“MINING Plus”ソリューションサービスにおいても活用されている。

4. ActiveMarketerの活用事例

ActiveMarketerは，三菱電機の主婦向けサイト“シュフレー”(http://www.MitsubishiElectric.co.jp/shufu/)などで利用されている(図3)。シュフレーは，三菱電機の家電事業（主に白物家電)の“機種拡販支援”と“新商品開発支援”を目的としており，アクセス数は60～100万月間ページビュー，月間サイト訪問者数は6～10万人である。会員は，立ち上げからわずか1年半強で約4万人強を獲得している。シュフレーでは，2週間に1回以上メルマガを発行している。シュフレー以外にも，携帯電話事業など他事業向けに計4種類のメルマガを2週間に1回配信している。また，メルマガとタイアップして，アンケート・キャンペーンを定期的に実施しており，シュフレー関連で月に5回，その他自動車機器事業関連でも月に数回実施している。これらの努力により，日経BP社Webブランド調査によるサイトブランドランキングでは，701位(2001年2月)から89位(2003年8月)に大幅にアップした。

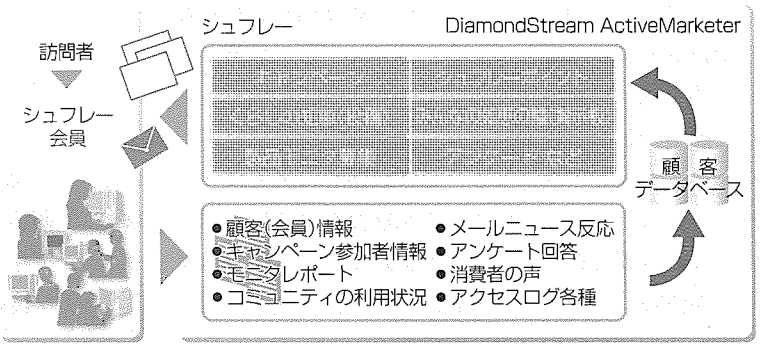


図3．主婦向けサイト“シュフレー”の概要

シュフレーでは多数の会員情報を扱うが，会員が安心して情報提供を受けられるよう，三菱電機としても会員の個人情報保護には万全を期している。

5. むすび

これからの企業Webサイトは，従来のように製品情報を表示するだけでなく，メールなどで積極的に情報を提供し，アンケートを利用して顧客から意見を吸い上げ，その顧客の意見からいろいろな情報を吸収してビジネスを推進することが重要となる。これまでに培った情報提供・配信技術や情報収集技術，情報分析技術を生かし，今後とも，Webマーケティングシステムを開発・提供していく所存である。

参考文献

(1) 相川勇之，ほか：概念抽出型テキストマイニングによるアンケート分析手法の提案，情報処理学会デジタル・ドキュメント研究会，DD38-1 (2003)
(2) 高山泰博，ほか：eCRM向け概念抽出型テキストマイニング，電子情報通信学会報告，NLC2002-93研(2003)

知識情報活用エンジンを搭載した統合ドキュメント管理システム“Manedge Leader”

岡村博之* 中谷壮志*
稲葉 豊*
小島栄之*

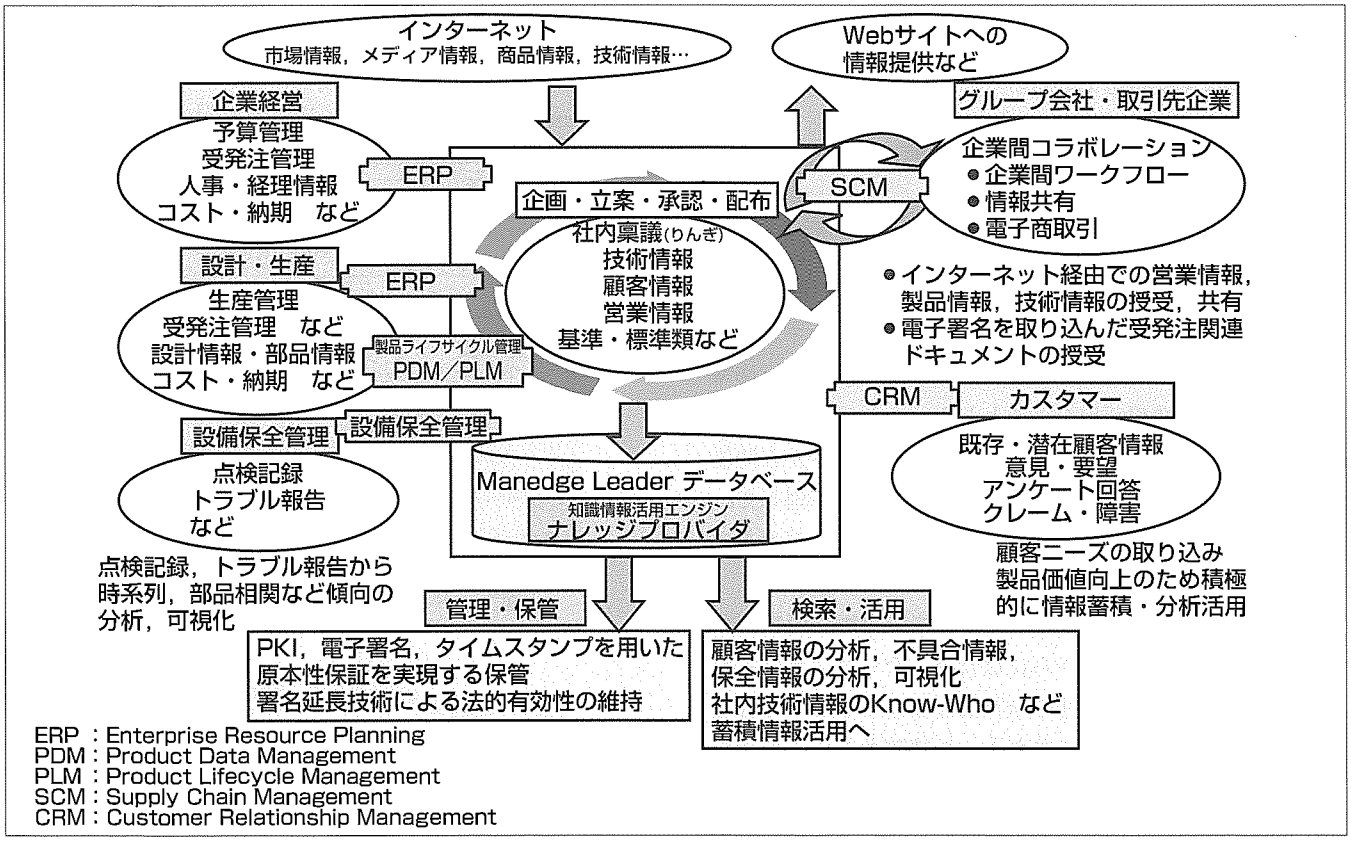
要 旨

景気低迷が長引き企業各社の経営状況は一層の厳しさを増しているが，激化する競争を勝ち抜くためには，様々な面での全社的な最適化が必要とされている。このような状況の中で，社内に蓄積された膨大なドキュメントの中から必要な情報を取り出して全社的に活用するためのシステム構築が求められている。

三菱電機統合ドキュメント管理システム“Manedge Leader(注1)”は，社内に分散している各種ドキュメントを取り込んで一元管理し，三菱電機㈱研究所の成果である知識情報活用エンジン“ナレッジプロバイダ”を採用したことで，多種多様な文書・データから必要情報の抽出を可能とし，従来及び他社製品にない全文検索，概念検索，テキストマイニングなど，三菱電機㈱独自の方式を用いた高度な情報検索，効率的な情報活用を可能とした。その結果，大量の文書中に埋もれたノウハウなどの知識を抽出したり，例えばアンケートの情報を分析してマーケティングなどに活用したりすることが可能になった。

Manedge Leaderを導入することで，企画，研究開発，設計，品質管理，資材，さらには営業・サービスといった各種部門から発生する情報を全社的な資産として一元管理することができ，部門間をまたがった情報共有とその活用により，製品企画・設計の効率化，品質向上，資材調達価格の低減，顧客ごとの製品補修履歴のトレースなどを実現することができる。また，企業内の重要情報を取り扱うことから電子署名や署名延長，電子文書の利用管理といった高度なセキュリティ機能を組み合わせることができ，安全で快適な企業内，企業間のコラボレーションを実現可能にしている。

（注1） Manedge Leaderは，三菱電機インフォメーションシステムズ㈱の登録商標である。



統合ドキュメント管理システムManedge Leaderの概念

知識情報活用エンジン“ナレッジプロバイダ”を採用したManedge Leaderデータベースに各種ドキュメントの情報が一元管理され，高度な情報検索，効率的な情報活用が可能である。また，既存の関連するシステムと連携し，ERP，SCM，CRM，PDM，PLM，企業間コラボレーション，社内外情報の蓄積・分析・活用など様々な業種・分野に適用できる。なお，Manedgeは，ManagementとKnowledgeを組み合わせた造語である。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

景気低迷が長引き企業各社の経営状況は一層の厳しさを増しているが，そのような中，激化する競争を勝ち抜くためには，様々な面での全社的な最適化が必要とされている。ドキュメント管理システムにおいても，最近は，ワークフロー対応，全文検索機能などを付加したエンタープライズ型の統合ドキュメント管理システムのニーズが高まってきている。

(1) 社内に蓄積された膨大なドキュメントを知識情報資産として共有し，これを全社的に活用して競争力を向上させたい。

(2) 設計品質管理を確実に行い，品質ロスコストを削減させたい。

(3) 団塊の世代が持つ技術，ノウハウをドキュメントとして残し，若い世代に確実に伝承させたい。

(4) 情報の漏洩(ろうえい)を防ぎ，コンテンツを保護したい。

これらは，まさに企業にとって緊急の課題である。三菱電機インフォメーションシステムズ㈱(MDIS)が開発した三菱電機統合ドキュメント管理システムManedge Leaderは，三菱電機㈱及びMDISの長年の経験とノウハウを生かし，三菱電機㈱の研究所が独自に研究開発したナレッジマネジメント機能及びセキュリティ機能を搭載し，このような課題の解決を支援している。

2. Manedge Leaderの機能，特長

Manedge Leaderは，登録・閲覧・検索・ワークフロー・アクセス権管理といったドキュメント管理機能に加え，三菱電機㈱の知識情報活用エンジン“ナレッジプロバイダ”を搭載したことにより，全文検索，概念検索，テキストマイニングなど，三菱電機㈱独自の方式を用いた高度な情報検索，効率的な情報活用を可能とした。これにより，登録時の属性設定や検索用キーワード設定の煩わしさから開放され，企業内で発生する多種多様な文書を一元管理して，必要なときに必要な情報を効率良く抽出することができるようになった。

Manedge Leaderを導入することで，企画，研究開発，設計，品質管理，資材，さらには営業・サービスといった各種部門から発生する情報を全社的な資産として一元管理することができ，部門間をまたがった情報共有とその活用により，製品企画・設計の効率化，品質向上，資材調達価格の低減，顧客ごとの製品補修履歴のトレースなどを実現することができる。また，電子署名や署名延長，電子文書の利用権管理といった高度なセキュリティ機能を付加することで，安全で快適な企業内，企業間のコラボレーションを実現可能にしている。

Manedge Leaderの主な特長を，以下に簡単に紹介する。

(1) ドキュメント管理機能

図1は，ドキュメント管理機能の画面例である。紙文書(手書き，モノクロ／カラー)，電子文書(ワープロ，画像，CADなど)など，各種業務で作成される様々なドキュメント，既存文書や外部から入ってくる多様な形態の文書を保管し，新規登録～改訂～廃棄までのライフサイクル管理を実現する。既存のファイルサーバから文書を自動的に取り込んで登録することも可能であるため，既存のデータを逐一登録しなおすことなく，すぐにManedge Leaderを導入し，活用できる。また，ワークフロー機能(起案～承認～発行～受領)により，文書の承認管理・授受管理をサポートする(図2)。

(2) 検索機能と検索結果の活用

一般的な属性による検索のほか，全文検索・概念検索など，必要な情報を的確に抽出し，それを活用するための様々な機能が用意されている。

全文検索では，紙文書・電子文書など，ドキュメントの形式を問わず，ページ単位で検索が可能である。これまで検索の対象にできなかった文書中に埋め込まれた画像内の文字や，ベクトルで描かれた文字，手書き文字にも対応する(図3)。また，検索結果は該当箇所が強調表示(赤枠表示)されるため，該当箇所がひと目で分かるようになっている。

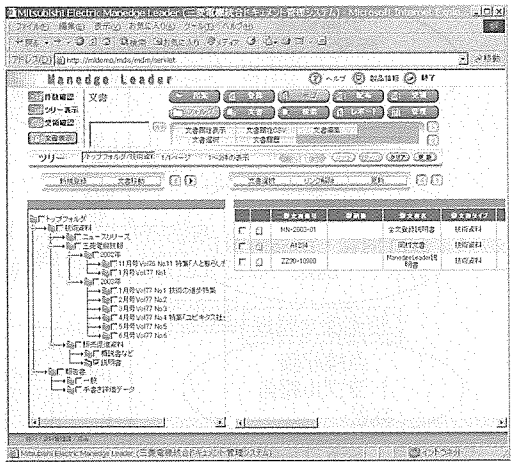


図1．ドキュメント管理機能の画面例

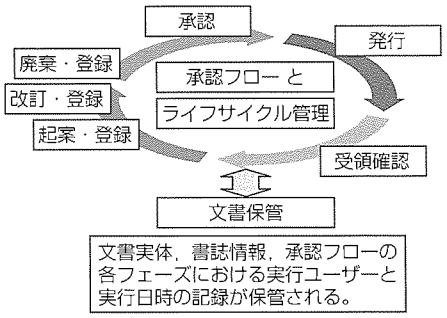


図2．承認フローとライフサイクル管理

概念検索では，キーワードを意識せずに自然な文章で検索できる。文書内容に応じた概念を自動学習するため，類義語辞書をあらかじめ人手を使って作成する手間が不要である。例えば，“ワープロ”という単語を指定して“ワードプロセッサ”や“文書編集装置”などの表現が異なる類似文書を的確に検索する。また，高精度な日本語形態素解析により，検索に最適な索引を生成し，漏れの少ない検索を実現する。

検索結果として多数の文書がヒットした場合，従来の単なる結果の一覧表示だけでは分かりにくいため，対象データを図・画像・地図などの上にマッピングして表示することで，直感的に傾向を把握したり，検索結果の絞り込みを行うことも可能である。

テキストマイニングでは，顧客アンケートなどの膨大な文書の中に記述されている内容を傾向や相関関係などの視点で分析することで，営業戦略の立案，マーケティングなどに役立つ新たな情報の創出が可能となる。

性能面では，規模に応じて最大256台のパソコンサーバによる大容量ストレージを構成することができ，この場合，1,000億文字(新聞記事1,000年分に相当)の文書から，1秒程度で全文検索することが可能である。

(3) オープンアーキテクチャ

Webアーキテクチャ(3層構造)を採用し，また，すべてのコア機能をAPIとしてオープンにしているので，ERP，SCM，CRM，PDM，PLMといった周辺システムとの連携が容易であり，多様なビジネスニーズに対応できる十分な拡張性を持っている。

(4) セキュリティ機能

他の製品と組み合わせることにより，重要なデータの漏洩や改ざん，持ち出しを防ぐために，電子署名や電子公証，電子文書の閲覧制御・印刷制限・コピー制限といった利用権管理(DRM)など，高度なセキュリティ機能を実現することが可能である。これにより，安全で快適な企業内，企業間コラボレーションを実現可能にしている。

3. Manedge Leaderの適用例

3.1 ファイルサーバ連携と電子メール登録

情報共有のための適用例として，ファイルサーバ連携機能と，現在開発中である電子メール自動登録機能を紹介する。

ファイルサーバ連携機能とは，既に共有サーバ等に保管されている電子データをそのままManedge Leaderのデータとして利用し，情報を共有するものである(図4)。これにより，既存のデータを逐一登録しなおすことなく，すぐにManedge Leaderを導入し，活用することができる。Manedge Leaderは，指定されたファイルサーバの指定されたフォルダ下にある電子ファイルから検索用インデックスデータと表示用データを自動生成し，登録する。ユーザーは，Manedge Leaderで検索・参照することにより，Manedge Leader本体に登録されているデータか共有サーバ等に保管されていた電子ファイルかなど，元のドキュメントの所在を意識することなく利用することが可能になる。そのため，従来の共有サーバではファイルごとに個別に検索していた業務が，Manedge Leaderの持つ強力な検索，活用機能を利用できるようになり，検索業務の大幅な効率化が図れる。

電子メール自動登録機能では，特定のメールアドレスに送信することにより，そのメールの本文をファイル化し，また，添付ファイルも個別のファイルの登録データとして自動的に登録し，検索対象とする。最近は，メールによる情報のやり取りが一般的になり，多くの情報がメールにのみ記録として残ることが多い。しかしながら，従来，メールの本文や添付データを検索対象とする場合，メール本文をテキストファイルとして保存し添付ファイルと個別に登録するという方式で登録していたため，手間がかかり情報共有が促進されていなかった。しかし，メールの宛先(あてさき)にManedge Leader専用のメールアドレスを追加しておくだけで自動的に登録されるため，メールの情報も共有することができる。

3.2 設計・品質関連ドキュメントの管理

製造業における損益改善のための対策として，品質ロスコストの削減が重視されてきている。品質対策には過去に起こった不具合の再発防止が大切であり，そのためには，設計・品質関連のドキュメントを共有・有効活用すること

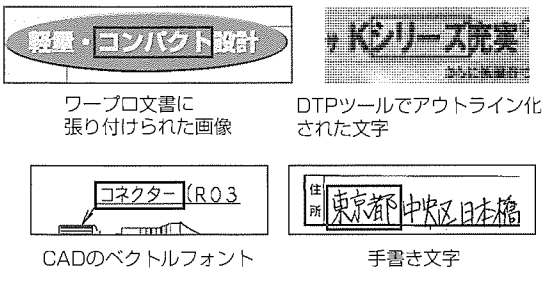


図3．全文検索で検索できる文字列

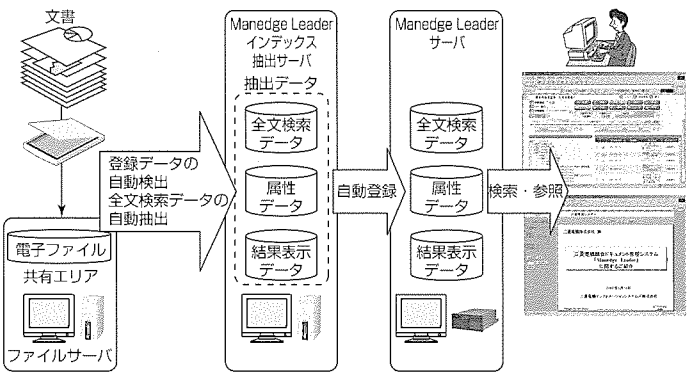


図4．ファイルサーバ連携機能

が前提となる。Manedge Leaderでは，蓄積された知識情報の中から不具合を発生させる要因を抽出し，早期に対策を施すことで品質の向上につなげることができる。

(1)　システムの活用イメージ

システム活用のイメージを図5に示す。品質の確保のためには，以下の運用を徹底し，同じ不具合を繰り返さないための環境構築が求められる。

- 社内基準に従った業務の遂行
- 確実なデータ共有(最新版管理)と的確な情報検索
- 十分なレビューの実施

これらを満たした業務環境構築のため，Manedge Leaderで以下のような様々なドキュメントを登録・管理する。

- 設計基準，品質基準等の社内基準類
- 過去に発生した不具合に対する報告書，対策・影響などが記されたドキュメント
- 各種設計成果物(ワープロデータ，イメージデータ，図面データ，他)

これらの情報の中から必要な情報を多彩な検索機能を用いて抽出し，業務に活用していくことができる。

例えば，自分が設計している内容が社内の基準に従ったものになっているかどうかを確認したい場合，これまでは各種基準ファイルの中から，該当するページを探す必要があり，検索に時間を要した。Manedge Leaderでは，確認したい内容をキーワードに指定した全文検索を実行することで，自分が確認したい対象のドキュメントと該当ページを即座に参照することができる。また，類似設計における過去のトラブルに関する情報を収集したい場合も，大量なドキュメントの中から関連情報を的確に検索することができる。このような類似情報の検索には，概念検索機能が有効な手段となる。

さらに，Manedge Leaderでは，該当ファイルを検索するだけでなく，検索結果として得られた情報の分析へと発展させることができる。情報の分析には，テキストマイニング，日本語解析技術，ドキュメントのXML(Extensible Markup Language)変換技術等を駆使し，設計段階における品質の作り込みを支援する。

品質向上を支援するためのManedge Leaderの有効な機能は検索機能だけではない。品質の確保に必要なドキュメントのレビューを，電子承認，配布・授受管理などの承認フロー機能を用いて対応することができる。承認フローを採用した運用ルールを徹底することで，承認前に関係者に対するレビューを確実に実施し，承認後は関連部門に対し配布を行うことで，間違って変更前の古いデータを使って作業を進めてしまうといったミスを防止することができる。このような作業のベースとなるドキュメント類を共有管理する場合は，最新版，改版，旧版等の版管理機能が不可欠となる。

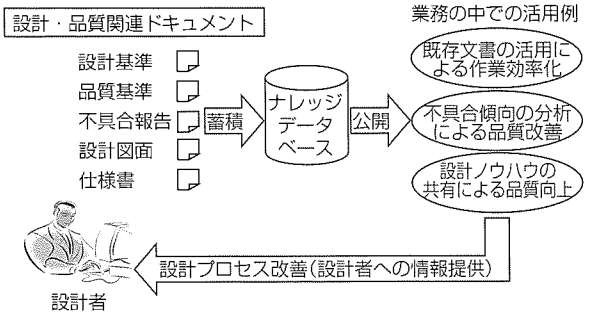


図5．設計・品質関連ドキュメントの活用イメージ

(2)　今後の展開

今後は，従来の検索機能に加え，業務に応じた多様な支援機能が求められるようになる。たとえば設計業務の場合には，以下のような拡張機能が必要となる。

(a)　設計者が作成した仕様書や図面を自動チェックし，設計基準からの逸脱や障害要因となる箇所を指摘する機能

(b)　仕様書を作成する際に，設計者を誘導する参考情報を設計者の習熟度に応じてガイダンスする機能

(c)　大量の蓄積文書から，重要な設計ノウハウを抽出・整理して活用を容易にするためのノウハウ獲得支援機能

Manedge Leaderは，情報抽出技術及び分析技術の高度化により上記の機能を実現し，次世代ナレッジマネジメントへの対応を視野に入れた拡張を図っていく。

4. むすび

Manedge Leaderは，ナレッジマネジメント機能を大幅に強化し，企業内にドキュメントの形で蓄積された潜在知識を全社的に共有し，企業の競争力強化の活力源として有効活用する知識情報活用環境の構築に適した製品である。

今後もますます多様化・高度化していくお客様の要求にこたえるため，三菱電機㈱の研究所と連携して先進的技術を取り入れながら，経営課題の解決に役立つより効果的・効率的な情報活用ソリューションを提供していく所存である。

高信頼性を実現した次期衛星配信ソリューション

福田　隆*　吉田　浩**
石川康雄*　名古屋　翼***
鷹取功人**

要　旨

三菱電機インフォメーションシステムズ㈱(MDIS)では，宇宙通信㈱(SCC)が提供するDirecPC(注1)サービスを通信インフラとして，企業内通信を中心に衛星情報システムの構築と運営サービスを進めてきた。代表的な適用事例としては，某證券会社向けファイルミラー配信・映像配信システム，某流通会社向けBGM(Back Ground Music)・プロモーション映像配信システム，某報道機関向けニュース配信システムなど多数ある。

この実績を踏まえ，サービス基盤をより強固にするため，2003年4月からスーパーバードD号機(東経110度CS：Communication Satellite)を用いた新しい衛星情報配信サービス基盤の開発を宇宙通信㈱と共同で進めた。

スーパーバードD号機は，BS(Broadcast Satellite)衛星と同位置にある衛星であるため，多数の視聴者を持ち，かつ，アンテナが共有できることから，

(1)　既存のBSユーザーへも通信サービスが容易に実現可能

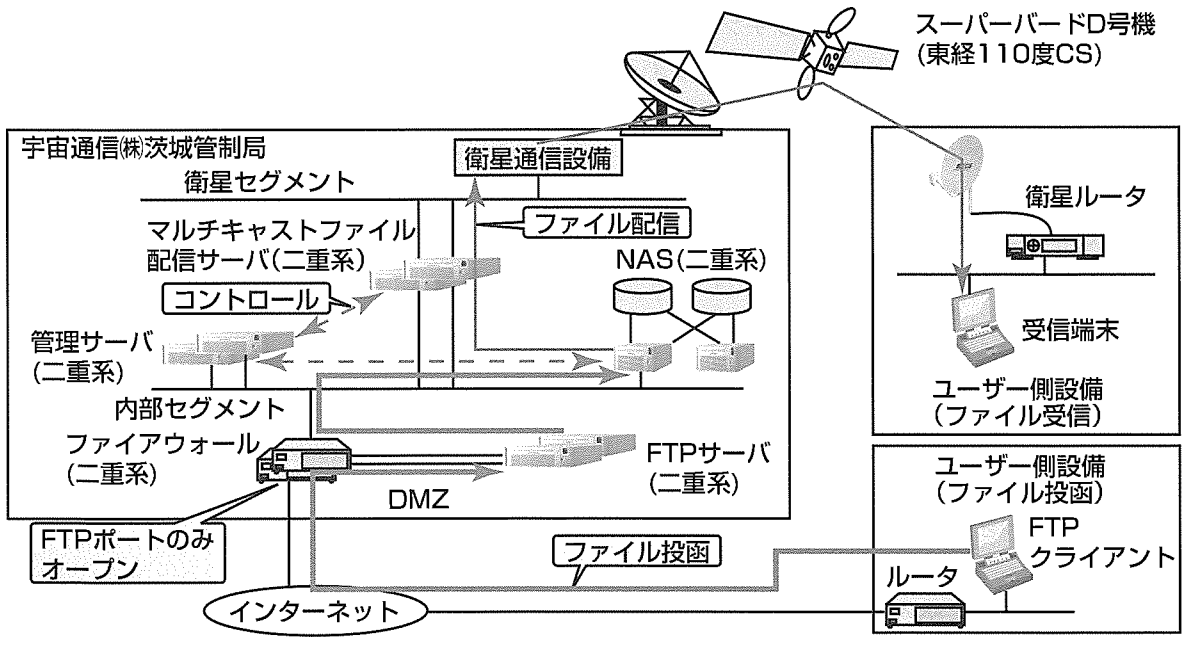
(2)　BS／CS共有化による機器・工事の低価格化が実現可能

(3)　BSとCSを共に利用可能な新たなサービスが提供可能

などのメリットがある。

本稿では，まずCS110度通信サービス“V-DRIVE110”の概要を説明し，次に従来サービス以上の運用性・利便性・信頼性の向上をねらい安全・安心な衛星配信サービスを実現するための帯域制御，優先度制御，高信頼性配信，再送方式，二重化システム，セキュリティなどの特長的機能について解説する。最後に上記を活用したソリューション例を紹介する。

(注1)　DirecPCは，米国HNS(Hughes Network Systems)社の登録商標である。



DMZ(DeMilitarized Zone)　：Web，DNS(Domain Name System)，FTPなどの公開サーバをインターネット側からの不正な攻撃から守るため，ファイアウォールにより設けられたセグメント。

FTP(File Transfer Protocol)　：ネットワーク上のクライアントとホストコンピュータとの間でファイルの転送を行うためのプロトコル(又はそれを実装したコマンド)。

NAS(Network Attached Storage)　：ネットワークに直接接続する形式のストレージデバイス。いわゆる専用ファイルサーバ。

“V-DRIVE110／IP”ファイル配信サービス基盤の全体構成

V-DRIVE110／IPファイル配信サービス基盤は，システム全体を管理するユーザー管理及びシステム管理サーバ，ユーザー(送信側)の送信ファイル及びエンベロープファイルを受け付けるFTPサーバ，投函された送信ファイル及びエンベロープファイルを格納するNAS，マルチキャスト配信サーバ，ファイアウォール及び衛星通信設備からなる。衛星通信設備以外が今回のMDISの開発範囲である。

*三菱電機インフォメーションシステムズ㈱　**三菱電機㈱ 情報技術総合研究所　***宇宙通信㈱

1. まえがき

近年，地上回線の高速化・低価格化が急速に進み，従来衛星通信の特長であった高速性・低価格性が薄れてきた。一方，衛星通信には地上回線の弱みである大容量同報配信，地域格差に依存しない配信性能・配信品質の提供といった独特のメリットがあり，衛星通信の用途・効果が明確な業務形態においては今後も有望な市場である。特にCS110度衛星通信サービスにおいては，既存BS利用者が潜在ターゲットユーザーとして見込まれることから，新たなビジネスチャンスが期待できる。

参考：BSアナログ視聴者…1,500万人以上
BSデジタル視聴者… 392万人
BSアナログ放送は2011年までに終了
(平成14年末実績　出典：平成15年版情報通信白書)

本稿では，まずCS110度通信サービスV-DRIVE110の概要を説明し，次に2003年4月から宇宙通信㈱と共同開発したV-DRIVE110／IPファイル配信サービス基盤の機能・特長を解説する。最後に，上記を活用したソリューション例を説明する。

2. CS110度通信サービスV-DRIVE110の概要

2.1 衛星を用いたデータ配信のこれまで

衛星を用いたデータ配信は，多地点へのコンテンツファイル一斉配信，音楽・映像のストリーム配信など多くのメリットが認識されている。また，インターネットの普及により衛星系もIPネットワークに対応することが要求され，その代表事例が宇宙通信㈱の提供するDirecPCサービスであった。DirecPCサービスは，米国HNS(Hughes Network Systems)社により開発されたシステムであり，ファイル配信・ストリーム配信・TCP／IP通信を一つのキャリアに統計多重したもので秀逸なサービスであったが，デジタル衛星放送方式そのものがレガシーなDSS(Digital Satellite System)方式であり，欧州及び日本で標準的なDVB(Digital Video Broadcasting)方式とは異なっていた。また，DirecPCサービスを受信するにはHNS社製のPCI(Peripheral Components Interconnect)ボードをパソコンに挿すか同社製専用の受信機を購入するしかなかった。

2.2 V-DRIVE110サービスについて

宇宙通信㈱では，更に衛星利用の利便性を増すために，2003年2月からV-DRIVE110サービスを開始している。V-DRIVE110サービスは，東経110°というBSと同じ軌道位置に打ち上げられているスーパーバードD号機(東経110度CS)の左旋偏波を利用する。このため，利用者は新たに左旋対応の受信装置LNB(Low Noise Block down converters)を用意するのみでこのサービスが利用でき，BS用の既存アンテナ鏡面と屋内配線を共用する。

このスーパーバードD号機はBSと同様の高い送信機能を持っており，日本の本州内であれば45cmφ程度のアンテナで受信が可能である。また，他のCSを受信するときのように偏波面の調整も不要である。

このV-DRIVE110のアップリンク設備は，茨城県のSTC(SCC Teleport Center)にあり，国内最大級の13mφアンテナと2kWのクライストロンから構成されている。スーパーバードD号機のALC(Automatic Level Control)機能との組合せにより，悪天候時でも回線の切断が起こりにくく，信頼性の高いデータ送信を可能としている。V-DRIVE110サービスは，このような利点を持つスーパーバードD号機上でDVBプラットフォームを構築，MPEG-TS(Transport Stream：MPEG映像のパケットストリーム)を用いた映像配信サービス，IP over TS機能を用いたデータ配信サービスを実現している。このプラットフォームは基本的にはMPEG映像伝送の仕組みであり，1Mbps程度の低レートのSDTV(Standard Definition TeleVision)映像から，15Mbps程度のHDTV(High Definition TeleVision)映像の伝送が可能である。このことにより，利用者は廉価な低レートのサービスから高品質画像まで選択できるようになっている。また，利用者は，一台2万円程度のデジタルCS通信用チューナーIRD(Integrated Receive and Decoder)を用途に応じて選択でき，NAGRA社の限定受信機能に対応している製品の場合は，送信局側からの鍵(かぎ)管理の仕組みにより，特定のIRDのみ映像の視聴が可能になる。

またDirecPCサービスのように利用者は独自のネットワークでコンテンツを茨城の送出センターに持ち込む形態だけでなく，都内にあるアクセスポイントまで配信情報を伝送するだけで，全国拠点への配信が可能となる。

図1にV-DRIVE110の仕組みを示す。

2.3 V-DRIVE110／IPサービスについて

V-DRIVE110／IPサービスは，このV-DRIVE110サー

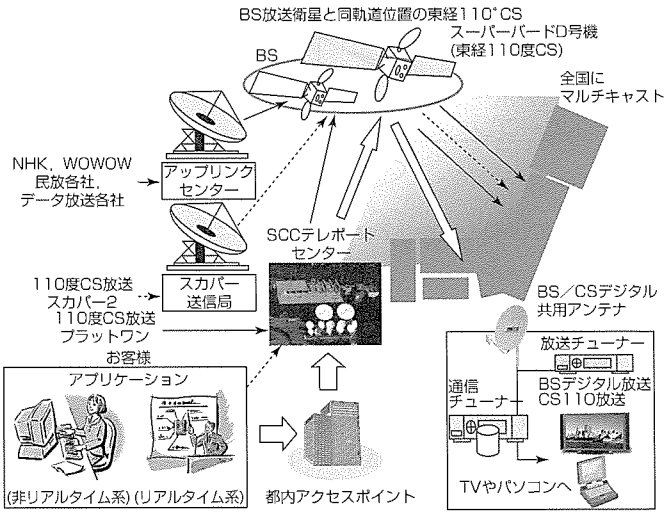


図1．V-DRIVE110の仕組み

ビスの映像のTSパケット中にIPパケットをカプセレーションして伝送する仕組みである。

受信形態は，映像パケットにカプセレーションされたIPパケットをIP受信機である衛星ルータで受信し，LAN側へ送り出す形である。また，利用者の用途によっては，ハードディスク付きのIP受信機を用意し，映像等のコンテンツを蓄積し，定期的にローカル再生する等の利用も考えられる。伝送プロトコルは，衛星の同報性を生かしたUDP(User Datagram Protocol)伝送，又はマルチキャストが主体となる。

図2にV－DRIVE110の受信側システムのイメージを示す。

3. V-DRIVE110／IPファイル配信サービス基盤の特長

次に，このシステムの特長及び主な機能について紹介する。

このシステムは，スーパーバードD号機(東経110度CS)を利用してSCC社が提供するIPマルチキャスト通信プラットフォーム上にファイル配信機能とストリーム配信機能を提供するものである。このシステムを利用するユーザーは，従来のDirecPCサービスと同様，エンベロープファイルと呼ぶファイルに配信方法や配信日時，受信拠点先を指定することにより，指示したスケジュールに従って大容量データを全国規模で多地点に定期的又は随時，同報配信することが可能である。

3.1 システム構成

このシステムは，衛星管制局に置かれた衛星情報配信システム(サーバ群)と各受信拠点に設置された受信端末(パソコン)で構成する。衛星情報配信システム側(サーバ群)には，システム全体を管理するユーザー管理／システム管理サーバ，IPマルチキャスト配信サーバ及びユーザー(送信側)の送信ファイル／エンベロープファイルを受け付けるFTPサーバなどがある。受信端末側では，受信したファイルに基づいてプログラムの自動実行が可能なIPマルチキャスト受信ソフトウェアがある。

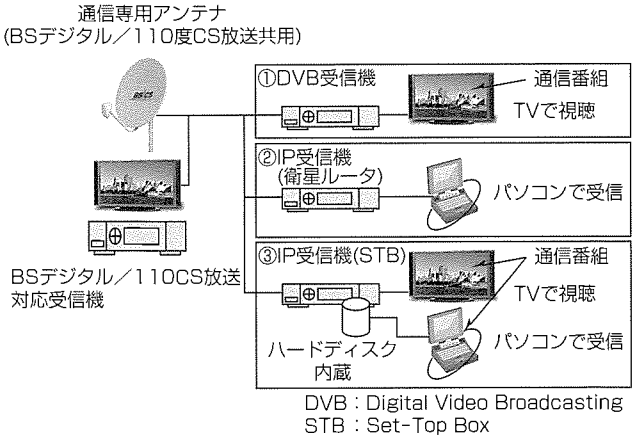


図2．V-DRIVE110の受信側システムのイメージ

3.2 システムの特長

今回，欧州及び日本で標準的なDVB方式に準拠したIPマルチキャスト通信を利用しているため，受信局側に安価な衛星ルータを利用してシステム構築が可能となり，従来システムに比べて標準化・低コスト化が図れる。また，このシステムでは，従来サービス以上の運用性・利便性・信頼性の向上をねらい，安全・安心な衛星配信サービスを実現するための以下のような特長的機能を提供する。

(1) 帯域制御

限られた衛星通信帯域を複数ユーザーでいかに効率的に利用するかが運用上重要になる。そのため，あらかじめユーザーごとに利用可能な帯域幅を設定し，その帯域を超えないようユーザーごとの帯域制御を行う。また，複数ユーザーの同時利用により衛星帯域を超える場合には，ユーザーの優先度の条件によって各ユーザーの帯域を動的に制御可能である。

(2) 優先度制御

同一ユーザーが要求する配信予約ごとに優先順序を指定できるため，通常時は同一優先度による複数均等配信を行うとともに，速報のような緊急性の高い配信については，高優先度指定による予約順序を追い越した配信も可能となっている。これにより，他ユーザーへの配信には影響を与えず，各ユーザーに与えられた帯域の中で優先配信，均等配信ができるようになっている。

(3) 高信頼配信

高信頼な配信保証を実現するため，ファイルデータにはエラー訂正符号FEC(Forward Error Correction)を付加して配信することが可能である。ユーザーはエンベロープファイルからFEC量を指定することが可能であり，配信用途に合わせた信頼度を設定することができる。FECはファイル配信だけでなくストリーム配信時にもリアルタイムで生成するため，遅延のない映像配信が可能である。

(4) 再送方式

天候不良等によるファイル配信時のエラーに備えて，このシステムでは3つの再送方法をユーザーが指定できる。受信端末から衛星配信システムへの上り通信回線がある場合には，回数指定による再送モードや各サイトの受信状況を確認してレポートファイルを生成する確認モードがある。また，上り回線がない場合には，送達確認を行わず，指定した回数だけ同一ファイルの配信を繰り返すベストエフォートなモードを選択可能である。

(5) 二重化システム

配信システム自体の信頼性については，従来のサービスでは，システム障害が発生した場合，利用者やシステム管理者が再度配信要求を行う必要があったが，今回のシステムでは，サーバ，ディスク装置を二重化し，ダウンした場

合でも，自動的に待機サーバへ処理を復元し，中断した配信を自動的に再開する高信頼な配信システムを実現している。

(6) セキュリィティ

前述のとおり，ユーザーは，インターネット経由でこのシステムのFTPサーバに配信したい実ファイル及び配信方法・配信日時・配信拠点先を指定するエンベロープファイルを投函することで，衛星経由でのマルチキャスト配信を実現する。そのため，インターネットとこのシステムネットワーク間にはファイアウォールを設け，FTPサーバをDMZ(DeMilitarized Zone)に配置する構成をとっている。また，FTPポート以外のポートはクローズし，かつ，ユーザー認証を行うことで，セキュリティ的に強固なネットワークとしている。

(7) 利便性向上

従来のサービスでは，ユーザーは予約登録後(エンベロープファイル投函後)にファイル配信の状態(ジョブ)を知ることができなかった。今回のシステムでは，ユーザーがFTPサーバを通して処理状態を確認することを可能とすることで，ユーザーの利便性を向上させた。

3.3 今後のシステム拡張について

今回開発したシステムは主にファイル配信機能が中心であったが，今後は，ストリーム配信に関する機能拡充や運用性向上など，更なるプラットフォーム強化を行い，適用分野の拡大を進める予定である。

4. ソリューション例

地上回線の低価格化・高性能化に伴い，ユーザーは文字だけでなく“映像”“音声”“画像”など多様な情報を同時に求めるようになっており，この傾向は今後ますます強くなってくる。一方，クローズドな情報の要求も高まってきている。例えば，

(1) フランチャイズ店舗向け商品情報・広告配信サービス
(2) 情報配信任意団体がその会員に対して行う会報等関連情報の配信サービス
(3) 予備校が予備校生に対して行う授業映像配信サービス
(4) 流通業者がカード会員に対して行う会員向け商品情報配信サービス

などがある。

衛星通信は，対象が不特定多数で，かつ配信する内容がオープンとなる放送と異なり受信者を限定するため，クローズドで秘匿性が高く，かつ地域格差のない一斉同報配信，高品位映像配信ができるため，上記目的のためには最適なネットワークと言える。

ソリューションの一例として，フランチャイズ店舗向け商品情報・広告配信サービスを図3に示す。このサービスは，衛星通信の特長である一斉同報配信を利用するため，

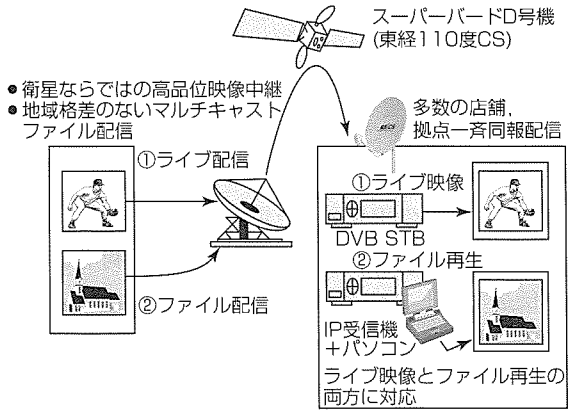


図3．フランチャイズ店舗向け商品情報・広告配信サービスのシステム構成イメージ

- 店舗間で地域格差がない
- 店舗間で情報到達の時間差がない
- 店舗数に関係なく通信コストが一定

といった利点があり，店舗差別が生じない公平な情報サービスが提供できることにある。配信する情報は，商品情報，イベント案内，カタログなどの様々なコンテンツが考えられ，動画・音声を活用したアクティブな商品プロモーションを行うことができる。また，標準機器の使用，アンテナ工事の容易化(従来に比べて小型アンテナが利用できる)により，一店舗当たりの初期導入費用を低減できるといった顧客メリットがある。

これに加えて，BS／CS衛星放送との共存が図れることから，例えば，イベント，リアルタイム広告キャンペーンのライブ中継を行うことができるので，より集客効果を高めるサービスを行うことが可能となる。

5. むすび

衛星通信は，一斉同報性，地域格差のない通信回線である点，耐災害及び衛星放送との共存性といった地上回線の弱点を補う特長を持つネットワークである。

これに加えて，この衛星情報配信サービス基盤は，MDISが得意とするマルチキャスト配信技術，二重化技術などを核に開発を進めており，セキュリティを含む高信頼性システムを実現している。また，サービスの長所・短所を完全に把握しており，ユーザーに対して最適なソリューションを提供することができる。

今後は，受注事例を増やしてシステム構築ノウハウを蓄積するとともに，コンテンツセンター機能やアプリケーション拡充に努める所存である。また，地上回線と融合したハイブリッドネットワークの構築・提供及び納入後の運用サービスまで含めたトータルソリューションに対応できる“総合衛星情報サービス”を指向していく。

ヘルスケアセキュリティソリューション

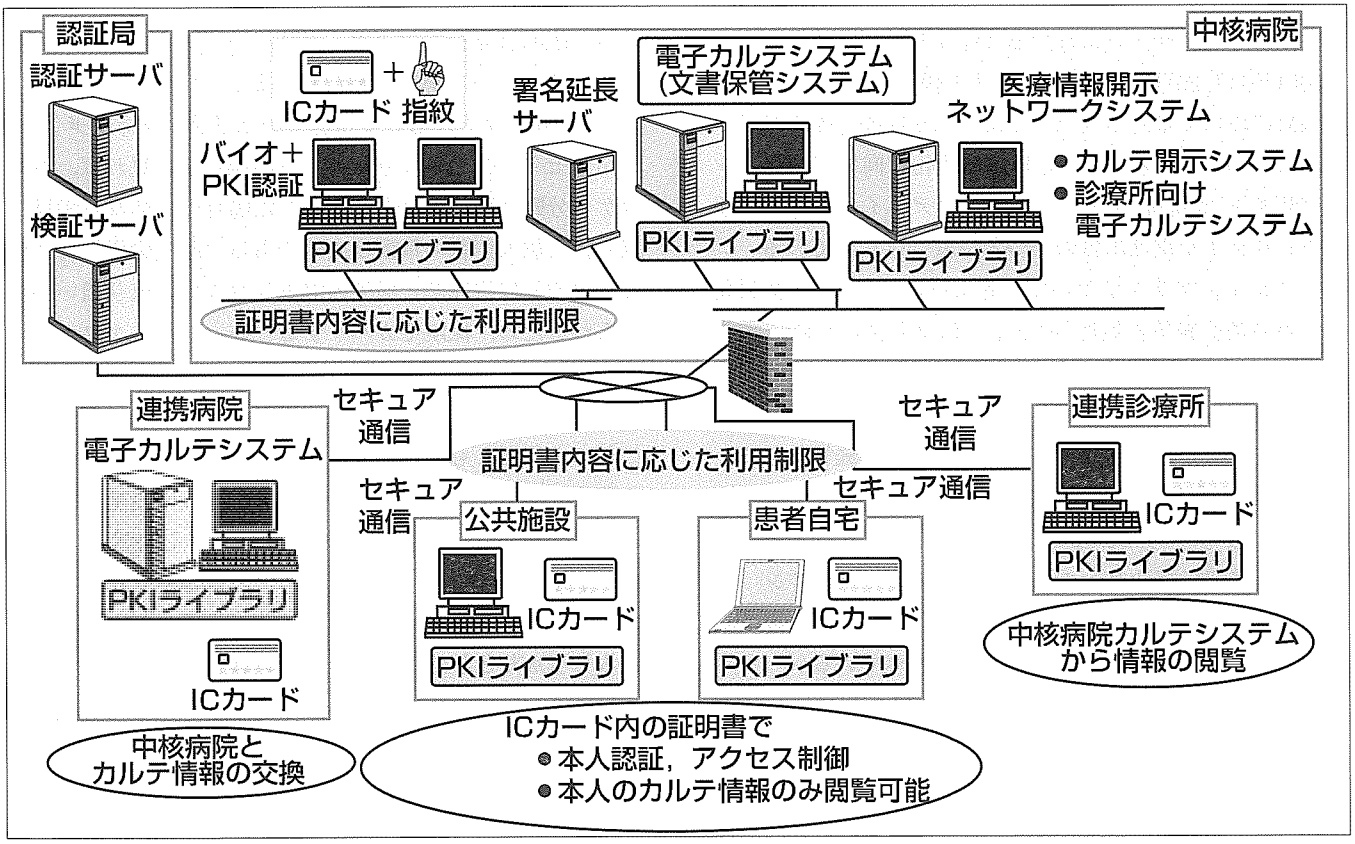
宮崎一哉*
茗原秀幸**
佐納成重***

要　旨

2001年の“保健医療分野の情報化に向けてのグランドデザイン”に始まり，e-Japan重点計画2003でも保健医療分野の情報化推進がうたわれるなど，保健医療等ヘルスケア分野の情報化が本格的に展開されつつある。ヘルスケア分野で情報化を実施する場合，取り扱う個人情報が極めて重要であり，外部から攻撃を受けた場合の影響も極めて重大であることから，情報セキュリティへの十分な配慮が必要となる。

ヘルスケア分野において高度な安全性を実現するには，ヘルスケアに対応した公開鍵(かぎ)基盤PKI(Public Key Infrastructure)を活用することとなる。“ヘルスケアセキュリティソリューション”は，原本の長期保存を可能とする署名延長サーバ，電子文書の送受を保証する電子公証サーバ，証明書や電子署名などの検証処理を実行する検証サーバなど，PKIにおける複雑な一連の処理を個々のクライアントやアプリケーションに代わって実施する各種セキュリティサーバ群を提供することを特長とする。

ヘルスケアセキュリティソリューションが提供する各種セキュリティサーバを利用することにより，クライアントやアプリケーションにPKIを意識させない安全なヘルスケアシステムを容易に構築することが可能となるばかりでなく，PKIの処理に伴う複雑な運用管理をサーバに一元化することが可能となるため，システムトータルコストの大幅な削減を期待することができる。



ヘルスケアセキュリティソリューション

ヘルスケアセキュリティソリューションは，ヘルスケアに対応したPKI(公開鍵基盤)技術により，高度な安全要求に耐え得るセキュリティ基盤を提供する。各種のセキュリティサーバ群をバックエンドとして提供することにより，個々のクライアントシステムに高度な処理や複雑な運用を課することなく，安全なヘルスケアシステムを構築することが可能となる。

*三菱電機㈱ 情報技術総合研究所　**同社 インフォメーションシステム事業推進本部　***三菱電機インフォメーションシステムズ㈱

1. まえがき

保健医療福祉等ヘルスケア分野の情報化が本格的に展開されつつある。このことは，e-Japan重点計画2003で“患者の選択の尊重と情報提供，質の高い効率的な医療提供体制，国民の安心のための基盤づくりを実現するという基本的考え方に基づき，電子カルテ，遠隔医療，病院事務の電算処理等の保健医療分野の情報化を推進する”ことがうたわれていること，関連の標準やガイドラインの提唱，実証実験等が盛んに実施されていることなどからうかがい知ることができる。

ヘルスケア分野での情報化を考える場合，取り扱う個人情報の重要度，又は外部から攻撃を受けた場合の影響の重大度が共に極めて大きいため，他分野にもまして情報セキュリティへの十分な配慮が必要となる。

本稿では，ヘルスケア分野における情報化の背景と動向について情報セキュリティ関連を中心に紹介し，ヘルスケア分野に安全と安心をもたらすソリューションとその中でも今後特に重要となってくるキーコンポーネントについて解説を加え，最後に一部の導入事例について紹介する。

2. ヘルスケアセキュリティの背景と動向

2.1 日本における制度化とグランドデザイン

(1) グランドデザインにおけるセキュリティ

2001年11月29日に「医療制度改革大綱」が政府・与党改革協議会において策定された。また，保健医療情報システム検討会において“保健医療分野の情報化に向けてのグランドデザイン”が策定された。グランドデザインでは，情報セキュリティが重点項目の一つと位置付けられている。

アクションプランにおいて情報セキュリティは“情報化のための基盤整備の促進”のトップに位置付けられ，電子情報セキュリティ，個人情報保護，認証制度に関する基盤整備を実施していくこととなっている。特に，国，学会，医療界，産業界が役割分担を行って取り組む施策として，“個人認証・資格認証基盤整備”と“ネットワークセキュリティの確立”が挙げられている。

(2) 個人情報保護法とヘルスケア分野のガイドライン

グランドデザインの第一次提言において，医療分野における個人情報保護に関し以下のように述べている。

“情報セキュリティ及び個人情報保護は，保健医療分野のみの問題ではなく，高度情報通信社会における共通の社会基盤である。したがって，保健医療分野における対応は，e-Japan重点計画に記載された施策に加えて，保健医療分野の特殊性を配慮して対策を立てる必要がある。”

ヘルスケア分野においては，医学の進歩，公衆衛生の確保の視点からの個人情報の利用が不可欠であり，適切な保護と適正な利用の確保の両面から十分な配慮が必要になる。個人情報保護法の成立・施行を受け，厚生労働省は，医療分野におけるガイドラインなどの策定を検討している。

(3) 電子保存三原則と外部保存

1999年4月22日に，厚生省の局長通知“診療録等の電子媒体による保存について”によって，カルテの電子保存が可能になった。基準として真正性・見読性・保存性の確保が電子保存の条件とされた。また，2002年3月29日に，厚生労働省の局長通知“診療録等の保存を行う場所について”によって，カルテの外部保存の道が開かれた。しかしながら，2003年12月時点では，ネットワーク経由でのデータセンターなどに対する外部保存については大きな制約が課されている。厚生労働省は，医療情報ネットワーク基盤検討会において，今後の方向性を検討している。

2.2 ヘルスケア分野におけるPKIガイドラインの検討

㈶医療情報システム開発センター(MEDIS-DC)は，2001年度から医療用セキュリティ技術委員会の活動として“保健医療福祉分野における公開鍵基盤を用いた証明書の発行・利用に関する運用についての指針を提供する”ガイドラインの策定を行っている。このガイドラインには，人，組織，それらの属性に関する電子署名用途又は認証用途の証明書に関する指針が定められる。

2003年12月時点で公表されているガイドライン(暫定版)には，証明書，証明書失効リスト，属性証明書のプロファイルや証明書発行局の運用，ポリシー，タイムスタンプ等についてのルールが記載されている。

2.3 ヘルスケアにおける情報セキュリティマネジメント

情報セキュリティマネジメントの観点から見れば，ヘルスケア分野と他の分野とを比較した場合の大きな差異は，取り扱う個人情報の重要度の差である。厚生労働省によれば，診療録は犯罪歴と同等の機密レベルでの取り扱いが求められるため，保険でカバーするといったリスクファイナンスの考えだけでは十分な対応ができない。また，金融分野で一般的に採用されている情報セキュリティ対策を施すことで十分だとも言い切れない。しかしながら，医療機関の機能分担や院外処方の普及，医療と福祉の連携など地域連携のニーズは増大しており，ITを活用した診療の高度化，情報連携の強化，業務の効率化が緊急の課題となっている。情報化の推進には，ヘルスケア分野において求められるしっかりとしたリスク管理を実施し，安全に情報交換，情報連携を行うための仕組みを構築することが必要である。

3. ヘルスケアセキュリティソリューション

保健医療現場における情報化が推進されるのに伴い，医療情報システムに対してセキュリティ機能を組み込むための製品群へのニーズが高まってきている。三菱電機㈱では，このニーズにこたえるために，医療情報システムにPKIを利用したセキュリティ機能を組み込むためのヘルスケアセ

キュリティソリューションを提供している(要旨のイメージ図)。

PKIを利用する場合，認証局が発行する証明書が必要となる。証明書の利用者が多く，利用者の入れ替わりが多い大学病院などでは，自前で認証局を運営したいとの要望がある。“三菱認証サーバシステムMistyGuard(注1)<CERTMANAGER(注1)>”はこの要望にこたえる製品である。CERTMANAGERでは，認証局自身の秘密鍵をFIPS140-2レベル3の認定を日本で初めて取得した“三菱耐タンパセキュアボードTURBOMISTY(注2)”へ安全に保管することが可能となっている。また，認証局の運営に必要となる認証局実施規定(CPS)を策定するためのコンサルティングも用意している。

図1にヘルスケアセキュリティ製品群を示す。

病院全体の医療情報システムを1社で構築することはまれで，電子カルテシステムはA社，医事会計システムはB社というように，各業務に特化した複数のベンダーが参画することが多い。そのため，システムごとに開発言語やシステム設計思想が異なってくる。病院全体としてのシステムのセキュリティを考えた場合，これら複数ベンダー間での一貫したセキュリティ機能の提供が望まれる。“三菱認証ライブラリCertMISTY(注1)”やその上位コンポーネントは，これら異なるベンダー間においてもPKI技術を用いた“電子署名”や“ユーザー認証”といった機能が柔軟で，容易にシステムへ組み込むことが可能なライブラリ製品群となっている。

ヘルスケア分野における電子署名の対象としては，処方箋(せん)や紹介状，カルテ等が想定される。処方箋は医療機関と薬局間，紹介状は医療機関間で交換され，カルテは病病連携や病診連携の場合に医療機関間で交換されることになる。異なる組織やシステム間でデータ交換をする場合，記述形式としてXMLが注目されており，医療分野でもXMLによる情報交換形式が提案されている。

XML文書に対して電子署名を行うための製品として，各種アプリケーションにXML署名機能を組み込むためのXML署名ライブラリを提供している。署名された電子カルテ等の文書は実際には長期間保存されることとなる。“三菱署名有効性延長システムMistyGuard<EVERSIGN(注2)>”は，電子署名付き文書の長期保存を可能とする製品である。

また，PKIにおける複雑な機能をサーバシステムとして提供するDVCS(Data Validation and Certification Server)検証サーバ，XKMS(XML Key Management Specification)認証サーバ，XKMS検証サーバといった製品群も，今後レパートリーへ追加する予定である。

一方，PKIをユーザー認証に使う場面としては，医療情報システムに医療従事者がログインする場面や，患者が本人のカルテ情報を閲覧するためにログインする場面等が想定される。このような場合，医療従事者は院内に設置された任意の端末を利用することが多く，患者も院内や公共施設に設置された公共端末を利用することがあり，利用者の端末を固定できない。そのため，ユーザー認証で利用する証明書や秘密鍵は持ち運びが可能な媒体に格納しなければならない。ICカード(Standard-9M)は，携帯性に優れ，かつ耐タンパ性を持つため秘密鍵を安全に管理できることから，証明書や秘密鍵を格納する媒体として最適である。

ID／パスワードよりも確実なユーザー認証を実現したいが第一段階からのPKIの導入は難しいというユーザーに対しては，ICカードを利用した指紋照合装置(FPR-ICRU-DT/MB-J9)によるユーザー認証コンポーネントを用意している。この指紋照合装置は，ICカードに指紋データを格納しておくことで装置内において照合処理を行うことができるという特長を持っている。PKI用と同一のICカードを利用できるため，次の導入ステップで医療情報システムをPKI対応に発展させることが可能となっている。

ヘルスケア分野でのPKIとしては，MEDIS-DCが証明書のプロファイルを規定している。三菱電機㈱が提供するヘルスケアセキュリティソリューションは，このプロファイルに従った証明書の発行や利用が可能となっている。

(注1) MistyGuard，CERTMANAGER，CertMISTYは，三菱電機㈱の登録商標である。

(注2) TURBOMISTY，EVERSIGNは，三菱電機㈱が商標出願中である。

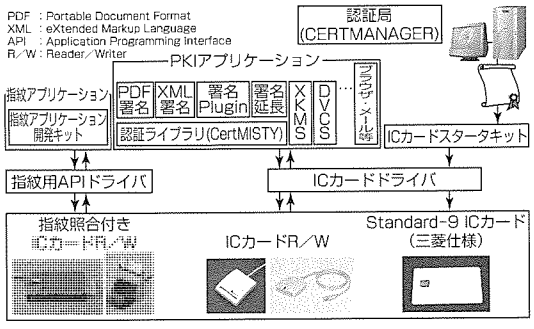


図1．ヘルスケアセキュリティ製品群

4. ヘルスケアセキュリティを支える最新コンポーネント

4.1 電子文書長期保存システム

2001年4月1日の電子署名法の施行により電子署名に法的な裏付けが与えられて以来，電子文書の真正性確保のために電子署名を用いることが一般的となりつつある。法制度的に数年から数十年といった長期間の保存義務が課せられる文書も各分野に多数存在し，ヘルスケア分野も例外ではない。電子署名には1年ないし3年の有効期間があり，そのままでは長期保存には耐えることができない。電子文書の有効性を長期間保つためには，署名有効性延長機能が不可欠な機能となる。署名延長サーバは，電子署名の存在時刻や検証情報を改ざん不可能な状態で保存するための長期署名フォーマットを自動生成し，長期経過後の電子署名

の有効性を確認可能とする(図2)。

4.2 電子認証・検証サーバシステム

PKI基盤に立脚した安全な情報化がヘルスケア分野でも期待されているが，PKI基盤技術を用いたシステムの構築や運用は極めて複雑となりがちであり，このことが導入を遅らせる要因となっていた。例えば電子署名や証明書の検証処理は複雑で重たい処理であり，検証プログラムをすべての利用者の計算機に導入するにはコストが高くつき，また検証のためには証明書や失効情報を各利用者が常に最新の状態に保つ必要があるため，運用コストも高くなる。

これを解決するためには，処理／運用とも少数のサーバに集約することが効果的である。検証処理の実行はもちろん，検証のために常に最新の状況に保っておく必要のある情報の運用をサーバに一本化できるようになる。各利用者は，検証の必要のある電子署名や証明書の検証をサーバに依頼し，その結果を確認すればよい。

このような検証機能を提供するサーバシステムが，DVCS検証サーバやXKMS検証サーバである。後者はXMLを利用したプロトコルで，アプリケーション間やクライアント／サーバ間を連結するWebサービスに対応するものである。XKMSには証明書の登録／発行にかかわる機能を提供するXKMS認証サーバもあり，いずれも情報セキュリティに関連する処理を個々のアプリケーションから意識せずに利用できるようにするための役割を果たす(図3)。

5. 事 例 紹 介

5.1 国立神戸大学医学部附属病院

国立神戸大学医学部附属病院では，看護支援システムへのログインに指紋照合装置によるユーザー認証を採用しており，CERTMANAGERを利用してMEDIS-DCの下位認証局を構築している。ヘルスケア分野において電子署名と指紋照合を組み合わせたICカードシステムを日本で初めて導入した事例である。第一ステップでは，下位認証局から発行された証明書は2002年度のMEDIS-DCの実証実験でインシデントレポートに対する電子署名に利用されている。第二ステップでは，院内システムでの電子署名の実現を予定している。

5.2 医療法人鉄蕉会 亀田総合病院

医療法人鉄蕉会 亀田総合病院では，安房鴨川地域を中心に，医療機関や患者を結ぶ医療ネットワーク(PLANET)を構築し，地域医療機関間での医療情報共有や患者へのカルテ開示システムを構築し運用している。PLANETに登録した患者は自宅のパソコンのほかに，市役所等に置かれた公共端末を利用しインターネット経由でカルテ情報を閲覧することが可能となっている。カルテ情報という個人情報を扱うことから，PLANET登録患者に対しては証明書

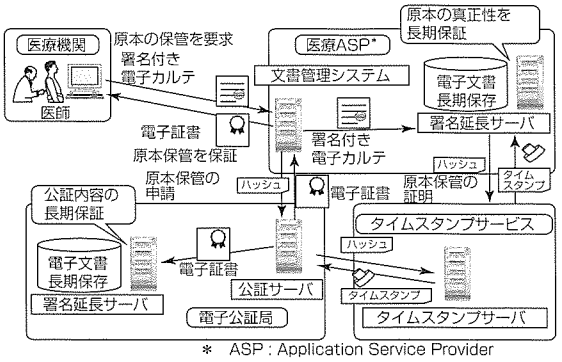


図2．電子文書長期保存システム

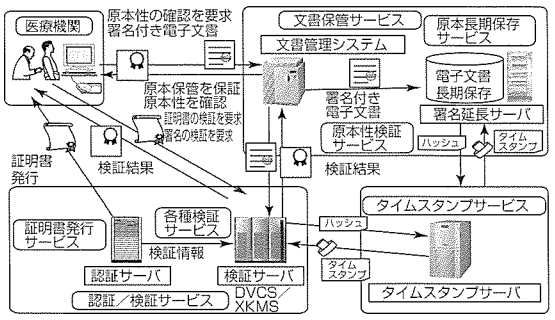


図3．電子認証・検証サーバシステム

と秘密鍵をICカードに格納して発行し，PKI技術を用いた個人認証を行っている。また，インターネット上を流れるデータに対しては，暗号化によりデータを秘匿することで第三者に情報が漏れないようにしている。この証明書は，亀田総合病院で運用／管理する認証局が発行している。

5.3 国立岐阜大学医学部附属病院

2004年6月に移転予定の国立岐阜大学医学部附属病院の新病院における電子カルテシステムやインシデントレポートシステムでは，ユーザー認証を行うために，証明書と秘密鍵を格納したICカードを全職員に対して発行することになっている。また，入院中の患者に対してもベッドサイド端末からカルテ情報を閲覧可能とすることになっており，ここでもICカードを用いたユーザー認証を行う。岐阜大学医学部附属病院でも，院内で認証局を構築／運用し，証明書の発行業務を行う。更に今後の岐阜地区での医療機関間や医療機関と患者間といった地域連携を視野に入れ，電子署名，医療機関間での転送データの保護，外部からのアクセス制御等の機能拡張が可能な構成となっている。

6. む す び

ヘルスケアセキュリティソリューションでは，各種のセキュリティサーバ群をPKIバックエンドとして用意しているため，個々のクライアントやアプリケーションに負荷の高い処理や複雑な運用を課することなく，高度な安全要求に耐え得るセキュリティ基盤を提供できる。

今後，このような高度な安全性を要求する領域は拡大するものと予想されるため，ヘルスケア分野を越えて適用できるソリューションとして発展させる所存である。

中堅企業向け人事・総務部門トータルシステム“セキュアALIVE Solution”

庭山正志*
森口隆史*
大石浩之*

要　旨

中堅企業におけるIT化は，販売・仕入れ・在庫管理・経理・財務系システムを中心として各社ともほぼ導入・対応が完了しており，“利活用”の段階に入っている。

一方，人事・総務系のシステムは，給与計算などのシステム化は済んでいるものの，人事・総務部門と社員の間で行われる間接業務が非定型かつ各社の制度や考え方が異なるため，システム化しにくいファジーな部分としてIT化は困難とされてきていた。景気低迷で売上げが伸びにくいという時代の潮流もあり，経営者は，今，人事・総務部門の改革に着目し，効率アップ・経費節約を期待している。

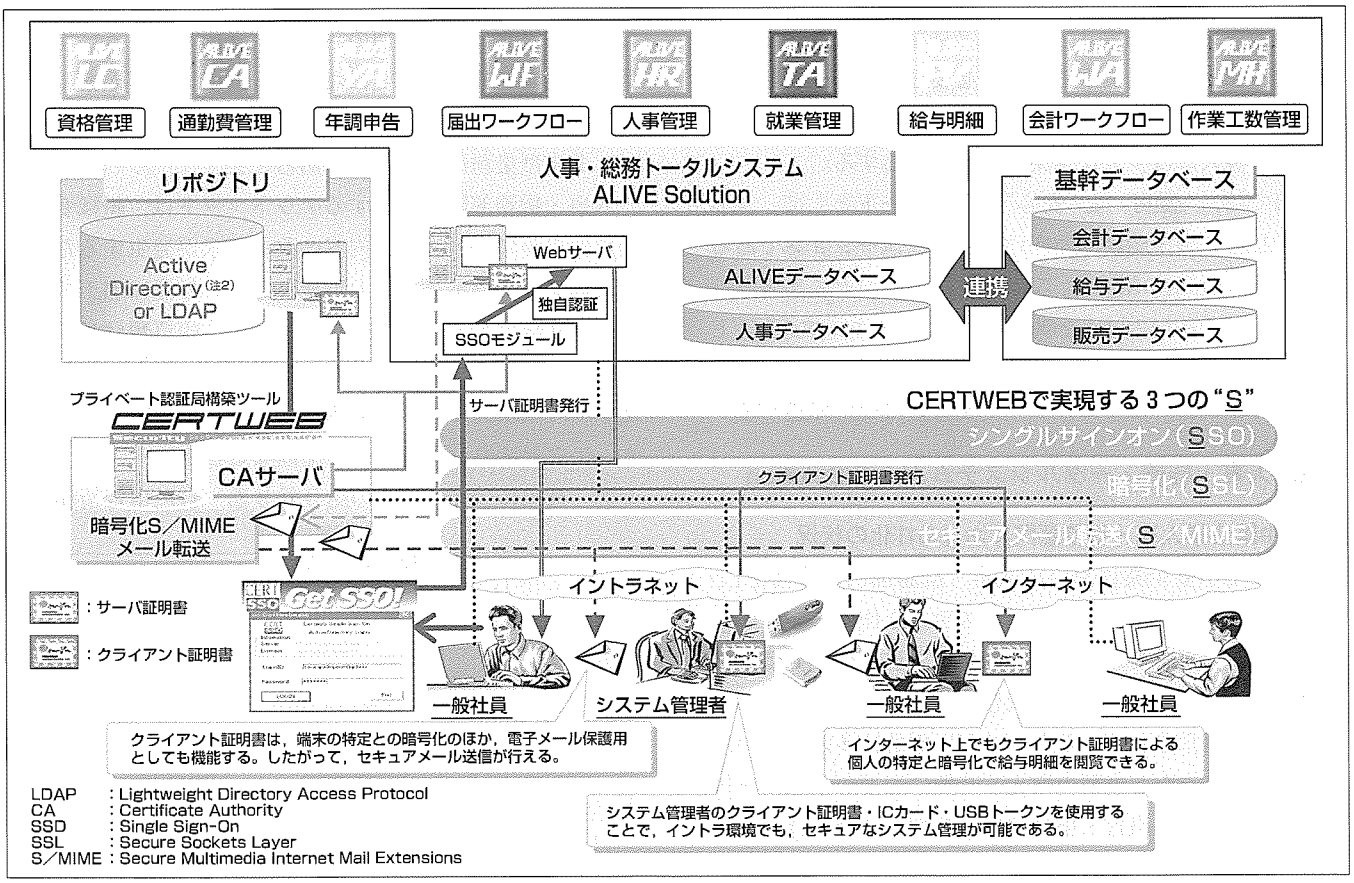
㈱三菱電機ビジネスシステム(MB)は，人事・総務部門の日常業務のIT化と社員に対する徹底した間接業務の効率化を目標とし，2003年6月，人事システムを中心とした9つの業務システムからなる人事・総務トータルシステム“ALIVE Solution(注1)”の販売を開始した。

人事・総務部門が取り扱うデータは給与や家族情報などプライバシー保護に関する配慮が必要となるが，一般企業にとって“セキュリティ基盤構築”は非常に難解・高価であるため，導入には多大な企業努力を必要とする。

MBでは，人事・総務部門トータルシステムALIVE Solutionに，MB独自のプライベート認証局構築ツール“CERTWEB(注1)”を組み合わせたセキュアALIVE Solutionを実現しており，中堅企業のお客様に“便利”で“安心”なシステムを“安価”に提供している。

(注1)　ALIVE Solution及びCERTWEBは，㈱三菱電機ビジネスシステムの登録商標である。

(注2)　Active Directoryは，米国及びその他の国における米国Microsoft Corp.の登録商標である。



セキュア ALIVE Solutionの概念図

基幹データベース群と連携した9業務からなる人事・総務トータルシステムALIVE SolutionにMBが提供するプライベート認証局構築ツールCERTWEBを組み合わせることにより，社内システムのセキュリティとして必要な3つの“S”(シングルサインオン・SSL暗号化通信・セキュアメール転送)を実現している。

*㈱三菱電機ビジネスシステム

1. まえがき

2003年7月に政府から発表された「e-Japan戦略Ⅱ」によると，我が国は“第一期：IT基盤整備”から“第二期：ITの利活用”へ差し掛かっており“元気・安心・感動・便利”社会を目指すとある。

中堅企業におけるIT化も，販売・仕入れ・在庫管理・経理・財務系システムを中心として，各社ともほぼ導入／対応が完了しており，“利活用”の段階に入っている。

一方，人事・総務系のシステムは，給与計算などのシステム化は済んでいるものの，人事・総務部門と社員の間で行われる間接業務が，非定型かつ各社の制度や考え方が異なるため，システム化しにくいファジーな部分としてIT化は困難とされてきていた。

MBは，人事・総務部門の日常業務のIT化と社員に対する徹底した間接業務の効率化を目標とし，1998年3月からWebアプリケーション技術を駆使した“Web就業管理システム”を社内システムとしてスタートさせた。その後，順次システムのレパートリーを増やすとともに，パッケージ製品としての機能を盛り込み，2003年6月，人事システムを中心とした9つの業務システムからなる人事・総務トータルシステム“ALIVE Solution”の販売を開始した。

人事・総務部門が取り扱うデータは給与や家族情報などプライバシー保護に関する配慮が必要となるが，一般企業にとって“セキュリティ基盤構築”は非常に難解・高価であるため，導入には多大な企業努力を必要とする。

本稿では，“便利”と“安心”をキーワードとして，MBが開発した人事・総務部門向け最新ソリューションであるALIVE Solutionの紹介と，これにMB独自のセキュア認証システム“CERTWEB”を組み合わせた“セキュアALIVE Solution”により短期間で効果的な人事・総務部門向けソリューションと，セキュリティ実現方式について述べる。

2. 人事・総務トータルシステムALIVE Solution

2.1 中堅企業人事・総務部門におけるIT化の状況

これまで中堅企業において人事・総務部門の業務をIT化するということは給与計算のシステムを作ることというのが従来の考え方であり，それ以外の業務については手作業で処理されているか，又は統合性のない業務個々の小システム群で運営されているケースが圧倒的に多い。このため，異動や年末など書類の増える時期に遠方から紙ベースで送られてくる届出書・申請書類が締切りに間に合わなかったり書類から複数のシステムへ同一データの手入力を余儀なくされたりし，人事・総務部門に大きな負荷がかかっている。この結果として人事・総務部門の業務は非効率・不正確・不便なものとなり，ITを利活用しているとは言えない状況に陥っている。

2.2 ALIVE Solutionのねらい

人事・総務部門のIT化は，“計算”だけでなく“人を支援する”ことを実現しなければならない。

ALIVE Solutionのねらいは，人事・総務部門の日常業務の統合的なIT化による作業の効率化と，遅配・誤送など誤りの大幅軽減によるクレーム処理の最小化を実現することにある。また，IT化によって単に人事・総務部門だけが楽になるということではなく，一般社員側すなわちエンドユーザー側へのサービスの充実や使いやすさなども重要なねらいの一つとなる。

2.3 ALIVE Solutionの基本コンセプト

(1) 人事・総務部門と一般社員の要求を最大限取り込む

実際の業務に精通した人事・総務部門の要求を最大限反映させるとともに，一般社員の間接業務遂行における問題点・改善点・要望を取り入れ，事務の合理化・効率化・正確性の向上・使い勝手を十分に考慮したシステムとする。

(2) 効率的で使いやすいこと

マスタ入力・データ入力の二重入力を徹底排除するために，人事・総務部門で扱うマスタを論理的に1つに統合し，マスタに対して一度データを入力すれば，他の者はそれを流用できるようにする（図1）。また，人事・総務部門だけでなく，社員番号・氏名・所属・原価負担部門その他公開できるデータは，他部門の者でも引き出せるようにする。業務担当者が異動で変更になっても，引き継ぎが楽にできるように操作を簡単にすることも重要である。

(3) 非定型業務に対応可能であること

人事・総務部門が作成するアウトプットは，組織変更や制度変更等により次々に内容の改訂要求が発生するため，表計算ソフトウェアに出力可能として，任意に加工できることを前提とする。定型的な出力画面・帳票類は必要最低限とし，検索条件・抽出条件・出力項目・出力順序等の設定が随時縦横無尽に実施できることが必要である。

(4) アクセスコントロールが堅固なこと

(a) 社内に公開できない給与賞与額・自己申告情報・家

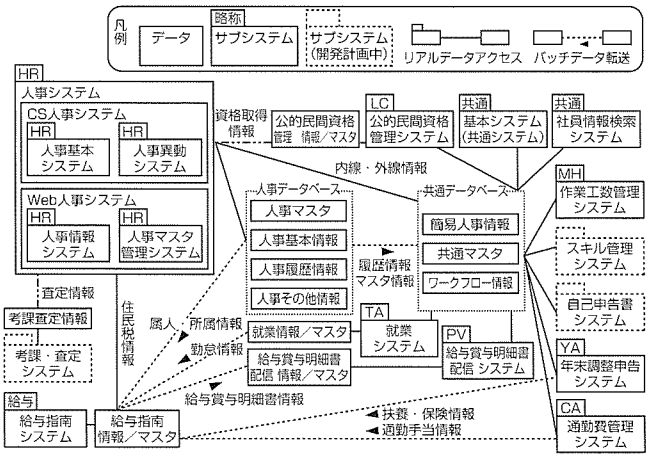


図1．ALIVE Solution データ関連図

族情報等のデータに対して一般社員がアクセスすることができないようにすること。

(b) 取締役・支店長・部長・課長など，複数の階層ごとにデータへのアクセス権限を設定できること。

(c) サインオン時の成功・失敗の履歴を採取し，不正アクセスに対する追跡が可能となっていること。

(5) 人事・総務部門本来の仕事に役立つこと

(a) 社員に対する各種サービスの向上

(b) 社員の経験・保有能力等のタイムリーな把握と分析

(c) 経験・能力分析による研修・教育の方向性の明確化

(d) 社員異動における適材適所の実現

(e) 人事・総務部内業務の効率化促進と正確性向上

(f) 経営幹部からの要請への迅速な対応と積極的補佐

(g) ペーパーレス化・効率化等を通じた費用節減

2.4 ALIVE Solutionで実現可能なIT化の例

ここでは，特長的な一部のシステムについて紹介する。

(1) ALIVE YA(Web年末調整申告システム)

年末調整の時期，申告書類を間違いなく本人に作成してもらうのは，人事・総務部門にとって手間のかかる仕事である。税務署から用紙をもらってくることからスタートし，間違いなく本人の居場所に申告書用紙を届け，記入方法についての集中的な問い合わせに電話等で回答し，集まった申告書の記載内容にも間違いがないことをチェックし，変更情報を人事システムに手入力することが必要となる(図2)。

Web年末調整申告システムでは，申告書はイントラネットの中に電子的に存在する。したがって，社員はどこにいようとも自分の申告書を取り寄せればよいため，人事・総務部門が用紙を郵送・配布する必要がない。また，前年度のデータや家族の生年月日等からあらかじめ必要項目は申告書に表示されており，保険内容や税金の計算について迷うことなく，一年に一度しか行わない資料の作成を手助けしてくれる。

税務署による要請で本人が捺印(なついん)した申告用紙が必要であるため，印刷作業は社員自身が行う。

本人が申告書を作成し終わると，人事・総務部門のデータベースに内容が集計され，給与計算システムに反映される。人事・総務部門はこれまでと同様に内容にミスがないかのチェックはするが，入力画面に注意事項が表示され，入力プログラムで最低限必要なチェックは自動的にかかっていることと，データ収集後に昨年分との比較チェックをシステムで実施できるため，導入前に比べ確認作業と本人とのやり取りは大幅に減少する。

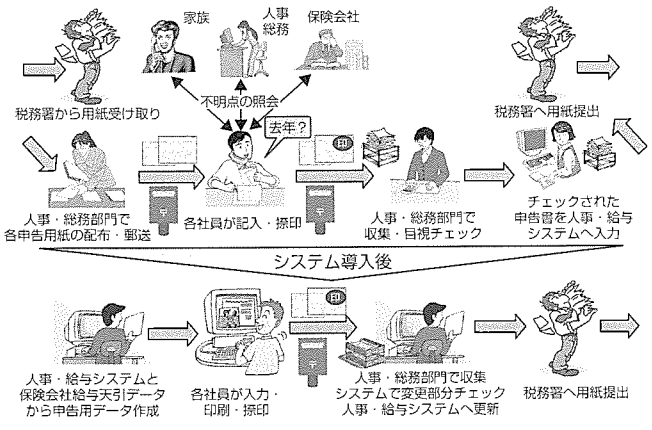


図2．ALIVE YA(Web年末調整申告)

(2) ALIVE PV(Web給与賞与明細配信システム)

給与明細書は，通常，社員全員分を印刷して封筒の形に折り込み，社員の手元に送付する。毎月の人事異動に合わせて，しかも実際に転勤した月日と支給日に合わせて確実に給与明細を配る必要がある。Web給与賞与明細配信システムでは紙の支給明細書は存在せず，イントラネットを使って社員がいつでもどこにいても明細書を見ることが可能となっている。16日付けで異動の辞令が出て25日の給料日には，転勤先でも，又は引継ぎで元の場所にいても，間違いなく給与明細書を見ることができる。また，通知先に自宅や携帯のメールアドレスを指定することもでき，会社以外でも明細を見ることができる。このように人事・総務部門での給与明細の準備・印刷や，辞令と実際の転勤日を考慮して間違いなく本人のもとに届けるという業務を大幅に改善することが可能である。

(3) Web社員情報公開サービス

社員間のコミュニケーションを支援する仕組みとして，イントラネット上で名前や所属部署等で検索すると，該当社員の顔写真・勤務地・座席表・社員番号・メールID・所属・役職・資格・内線電話番号・入社日・自己紹介等を参照できる機能がある。社員が異動した場合には所属や勤務地は異動データに基づいてシステムが自動的に変更し内線番号等は本人が直接修正できるようになっているため，社員に対するサービスが向上し，人事・総務部門は異動時における業務を軽減することが可能となる。

3. 社内システムに必要なセキュリティ

3.1 社内システムにおけるセキュリティの必要性

ALIVE Solutionのように社員の様々な情報へのアクセスがブラウザを通じて参照できることは，非常に“便利”である反面，セキュリティの面では大きな危険性が伴う。セキュリティ対策は，何もインターネットにおけるウイルス対策だけではなく，社内システムにも施しておく必要がある。なぜならば，同僚や上司・業務担当者のパスワードをなぜか知っているというケースも多く，LAN上のデータを解析・盗聴するツール等も簡単に手に入ることから，外部からよりも内部漏洩(ろうえい)の方が多いからである。これではとても“安心”して業務を行うことはできない。

セキュリティ基盤構築は直接的な利益を生むものではなく，反対に被害発生の未然防止という観点から，“何事も

起きない"ということを目標としているものである。

一方，内部漏洩はなかなか表面化しないこと，技術面では非常に難解であり，投資コストは一般に高価になることから，中堅企業においてはなかなか整備が進まないのが実情である。

3.2 ユーザーID・パスワード管理の限界

セキュリティ確保の一番の課題は，通常行われているIDとパスワード方式だけでは脆弱(ぜいじゃく)であるということである。パスワードの管理について，セキュリティポリシーとして一般的に以下のことが要求される。

(1) 8文字以上のパスワードにする。
(2) 大文字小文字記号数字を混ぜたものにする。
(3) パスワードは定期的に変更する。
(4) 変更時，一度使用したパスワードは使用しない。
(5) システムごとに違うパスワードを設定する。
(6) パスワードは紙に書かず記憶すること。

これらのポリシーを守ることは，複数システム対応となれば人間技では不可能であり，結果としてパスワードの推測・漏洩につながっている。また，現在のコンピュータ能力で，8文字程度のパスワードであればツールを使って4分以内，文字を10文字に増やしたとしても約3時間で解読されてしまうと言われていることから，IDとパスワード方式は限界に来ていると言わざるを得ない。

4. セキュアALIVE Solution

4.1 CERTWEBで実現する3つの"S"

社内システムにおけるセキュリティ対策の基本的なポイントは，セキュアな利用者認証方式と，LAN上のデータの暗号化，そしてメールやファイルの暗号化の3つが挙げられる。

セキュアALIVE Solutionは，ALIVE SolutionとMBのプライベート認証局構築ツールCERTWEBを組み合わせることにより，社内システムに必要な以下の3つの"S"を，簡単・安価・短期間に実現することができるソリューションである(図3)。

4.2 シングルサインオン(SSO)

公開鍵(かぎ)暗号基盤(PKI)技術をベースに，CERTWEBからクライアントに対して発行される"デジタル証明書"を利用することにより，IDとパスワードによる利用者認証だけではなく，ハードウェア(ディスク・ICカード・USBトークン)による利用者認証が可能となる。この証明書は，暗号化メールの受信用としても機能する。

1回の認証で複数のアプリケーションへアクセス可能となるシングルサインオン機能は，ALIVE Solutionの中では単体で実現しているが，他のアプリケーションも含めたシングルサインオンを実現するために，CERTWEB独自モジュールをアプリケーションに埋め込むことで実現する。他社アプリケーションなどで独自モジュールを埋め込むことができないものに対しては，ディレクトリからセキュアに取り出したIDとパスワードをキーボードエミュレーション機能により擬似入力し利便性を向上することができる。

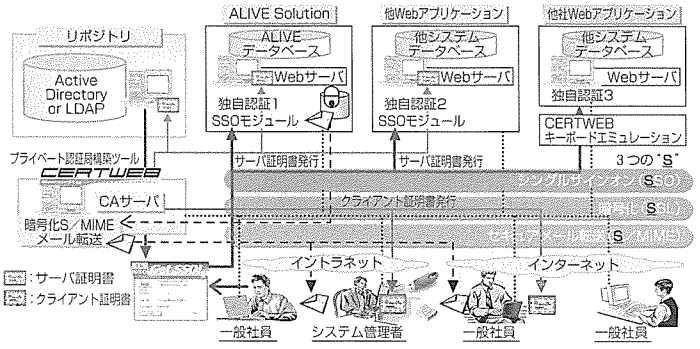


図3．CERTWEBで実現する3つの"S"

4.3 暗号化(SSL)

社内の回線上において平文でデータが送受信されていることは，セキュリティ上の大きな脅威である。

CERTWEBは，セキュアなWebサーバアクセス開始時に必要となるデジタル証明書の発行を可能とし，SSL(Secure Sockets Layer)による暗号化通信機能を実現する。これにより，WebサーバとクライアントはHTTPS(Hypertext Transfer Protocol Security)による送受信となり，LAN上のデータを解析することは不可能となる。さらに，クライアントを特定してよりセキュアな送受信を行いたい場合は，クライアントのデジタル証明書により，暗号化通信を実現することができる。

4.4 セキュアメール転送(S/MIME)

ALIVE Solutionの給与賞与明細配信メールを暗号化して送信する場合，送信先(一般社員)の公開鍵が必要となるが，ALIVE SolutionからセキュアWebサービスを利用してCERTWEBにメール情報を送信すると，CERTWEBに格納された各一般社員の公開鍵を利用して，暗号化メール(S/MIME)を一括して転送することができる。この機能により，一般社員は，CERTWEBに登録されている公開鍵に対応する秘密鍵を1つ管理するだけで，社内の複数のサーバ又は他の一般社員からの暗号化メールを受け取ることができる。

5. むすび

システムが便利になればなるほど安心を確保することが重要になっていく。MBはセキュアALIVE SolutionにWeb人事考課・査定システム等のパッケージ化を計画しており，今後さらに中堅企業向けに便利で安心な最新ソリューションを提供していく所存である。

金融基幹系向け“高信頼ブロードバンドネットワークソリューション”

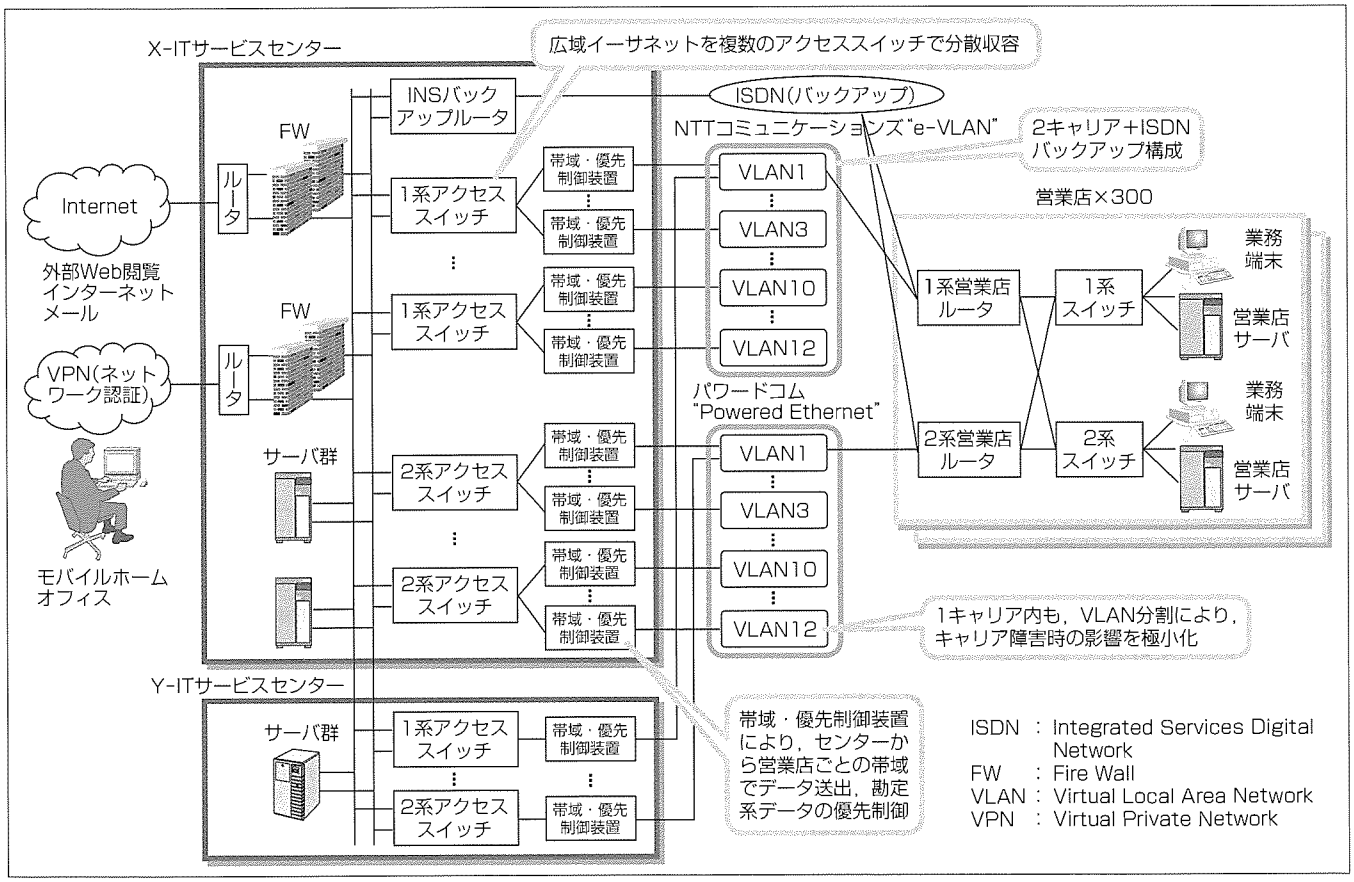
止部久仁彦* 重野俊浩*
大月英雄*
井上紀明*

要 旨

三菱電機インフォメーションシステムズ㈱(MDIS)は，“高信頼ブロードバンドネットワークソリューション”により，従来難しいとされていた大手都市銀行ネットワークのブロードバンド化を，広域イーサネット及びVLAN(Virtual Local Area Network)構築技術を応用して短期間に実現可能としている。特に，マルチキャリア採用による高信頼性の確保，帯域・優先制御装置導入による勘定系など重要トラフィックの保護，ブロードバンド化対応の運用管理システム構築等がその特長と言える。

㈱東京三菱銀行への導入では，“高い信頼性が必要な勘定系システムの通信に都市銀行では初めて広域イーサネットサービスを採用した”ことが評価され，同行は日経コンピュータの第7回情報システム大賞・先進技術賞[1]を受賞し，現在は金融系ブロードバンドネットワーク構成のモデルになっている。同行は，このブロードバンドネットワークを活用した行内業務革新も推進しており，本部・支社・営業店，さらにはモバイル活用を前提とした行外の行員個人までがブロードバンドネットワークで結合され，ITシステムを活用した業務の効率化，特に情報検索・入手にかかる時間の短縮化をテーマとして取り組んでいる(MDISはそのIT化も支援している)。

今後は，高信頼ブロードバンドネットワークソリューションを他業種へ展開していくとともに，音声ブロードバンドネットワーク化への取り込みや，海外及び社外接続等においても安価で高速・安全なサービスを提供していく。



(株)東京三菱銀行営業店ブロードバンドネットワーク全体構成

広域イーサネットは，NTTコミュニケーションズの“e-VLAN”及びパワードコムの“Powered Ethernet”を採用し，二系統化してキャリア障害時のリスク分散を図っている。また，帯域・優先制御装置により，センターと営業店間の帯域制御及び重要データの優先制御を実現し，広域イーサネット内では，複数のVLANに分割することでネットワーク障害時の営業店への影響範囲を最小限にしている。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

三菱電機インフォメーションシステムズ㈱(MDIS)は，“高信頼ブロードバンドネットワークソリューション”により，従来難しいとされていた大手都市銀行ネットワークのブロードバンド化を，広域イーサネット及びVLAN構築技術を応用して短期間に実現可能としており，このソリューションを適用した㈱東京三菱銀行の営業店ブロードバンドネットワーク“BEGIN-Ⅳ”は2003年4月から本稼働を開始している。

BEGIN-Ⅳ構築の背景には，融資稟議(りんぎ)書の電子化，支店収益管理情報をオンラインでリアルタイムに参照・分析できる国内経営情報・収益管理システム構築等の開発案件の増加や，e-ラーニング，TV会議システム等を利用した業務革新の動きがあり，ネットワーク容量拡大の強いニーズがあった。また，広域イーサネット，IP-VPN(Internet Protocol-Virtual Private Network)，ダークファイバ，法人向けADSL(Asymmetric Digital Subscriber Line)等，キャリアの安価で大容量な新通信サービスが出始めた時期でもあった。

本稿では，㈱東京三菱銀行に導入した高信頼ブロードバンドネットワークソリューションの設計コンセプト，信頼性確保のための取り組み，及びブロードバンドを活用した同行の業務革新に関する取り組み等を紹介する。

2. 銀行営業店のブロードバンドネットワーク構築

2.1 ネットワーク設計コンセプト

㈱東京三菱銀行の営業店ブロードバンドネットワーク設計に当たっては，以前の“BEGIN”ネットワークの利点(マルチキャリア，二系統化，自動迂回(うかい)機能等による高信頼性)を生かしつつ，以下のような高速性及びハイパフォーマンス性を実現することを基本方針とした。

(1) ネットワークの大容量化

今後のアプリケーションデータ増大に対応可能な回線容量を確保できるネットワークとする。今までの64kbps～1.5Mbpsの専用線及びデジタルアクセス回線の利用から，メガビット／ギガビット級のキャリア新サービス利用へ移行する。

(2) アベイラビリティの確保

ユーザーニーズに合わせて，適時，必要な回線容量を提供する(回線増速作業を容易に実施可能とする)。そして，今後のデータ統合に向け，データ・音声・画像をブロードバンドネットワークに収容可能とする。

(3) セキュリティの確保

今後のモバイル，関連会社など行外との接続を視野に入れ，セキュリティ，運用管理機能を強化する。

(4) 高信頼性の確保

勘定系基幹業務も対象とするネットワークのため，信頼性の維持・強化を図る。

2.2 高信頼ネットワークの構築

新たなBEGIN-Ⅳネットワークを構築するに当たって，既存の専用線ベースのネットワークと同等の信頼性を確保することに最大のポイントを置いて設計した。

(1) キャリア新サービスの選定

広域イーサネットサービス，IP-VPN，ダークファイバ，法人向けADSLの新サービスを検討したが，**表1**に示すように，短期間での開発，既存ネットワーク設計の変更量最小化及び設計自由度を重視し，最終的に高速性と使用ルーティングプロトコルに制約のない広域イーサネットサービスを選択した。その結果，既存のネットワーク設定を大きく変更することなく，新ネットワークへ移行できた。

(2) キャリア回線構成の冗長化＋INSバックアップ

キャリア内の詳細な網構成は公開されていないため，網の信頼性に不安があり，次の対応をとった。

(a) 二系統の回線にそれぞれ別キャリアを採用し，片系キャリアに障害が発生しても営業店業務を停止しないネットワーク構成とした。

(b) 広域イーサネットサービスの安定性を確認するまで，

表1．キャリア新サービスの比較

	広域イーサネット	IP-VPN	ダークファイバ	法人向けADSL
サービスの特長	市販LAN機器(L2SW)で構成した低料金／高速LAN間接続サービス	市販LAN機器(ルータ)で構成した低料金／高速LAN間接続サービス	波長分割多重化装置(WDM)で構成した超高速専用線	メタル高速伝送(ADSL)を利用した低料金／高速足回り回線
提供エリア	ほぼ全国展開完了	ほぼ全国展開完了	提供エリア限定的順次全国展開	ほぼ全国展開完了
適用技術	LANスイッチ(L2SW) VLAN	ルータ(L3SW) MPLS	波長分割多重 WDM	メタル高速伝送 ADSL
容量(bps)	1M～1G	64k～135M	2.4G以上	最大8M 場所により変動大
適用回線	光	光・メタル	光	メタル
収容可能システム	IP含む LAN系システム	IPのみ	ESCON(注1)，LAN ATM等多種システム	IPのみ
価格設定(円/kビット)	容量に依存 最低帯域保証 35円(10M契約)	容量に依存 最低帯域保証 105円(1.5M契約)	距離と容量に依存 帯域保証 6円(100M契約) 初期導入費用が高い	容量に依存 帯域保証なし 16円(8M契約)
導入時の制約	制約なし	迂回(うかい)方式：BGP-4 アドレス：数に制限	制約なし	迂回不可 同時接続端末台数
ターゲットユーザー	中大規模ユーザー(1M以上の専用線)の乗換え多い	小中規模ユーザー(64k程度の専用線)の乗換え多い	データセンター間の大容量転送	主に中小企業のインターネット接続用アクセス回線
評価	必要帯域1M以上の拠点向き(営業店，拠点間の大容量化)。制約なく，移行／テスト負荷小。	必要容量1.5M程度の拠点向き。	ギガクラスを必要とする大容量拠点向き。マルチプロトコル・媒体使用が可能。	速度変動・ばらつきが大きく信頼性に問題あり(勘定系システムでの利用は困難)。

LAN：Local Area Network，IP-VPN：Internet Protocol-Virtual Private Network，
L2SW：Layer2 Switch，L3SW：Layer3 Switch，MPLS：Multi Protocol Label Switching，
WDM：Wavelength Division Multiplexing，ADSL：Asymmetric Digital Subscriber Line，
IP：Internet Protocol，ATM：Asynchronous Transfer Mode，BGP-4：Border Gateway Protocol-4

(注1) ESCONは，米国IBM社の登録商標である。

既存ネットワークで使用していたINSバックアップ回線を継続使用することとした。また，回線切換え時間の短縮と運用負荷軽減のため，広域イーサネットのキャリア切換え及びINS切換えはすべて自動で行う方式とした。

(3) 二系統化の徹底

ネットワーク上の1箇所の障害による影響を極小化するために，ネットワークの二系統化を徹底して実施した。ネットワークを構成する機器の二重化だけではなく，データセンターと接続するキャリアの局も複数局に分散させた。また，データセンター内の管路も複数に分散させ，1箇所の障害の影響がネットワーク全体に及ぶことを徹底的に排除した。NTTコミュニケーションズは2局から，パワードコムは4局から回線を引き込み，局の分散化を図った。また，データセンター内では広域イーサネットの引き込み回線を4台のルータで分散収容した(2系も含めると合計8台)。

(4) VLAN分割によるリスク分散

広域イーサネットでは，通常1つの企業に1つのVLANを設定するが，複数VLANに分割する方式をあえて採用した。複数VLANに分割することによってセンター引き込み回線も分割できる。ルーティングプロトコルEIGRP (Enhanced Interior Gateway Routing Protocol)との整合性を考慮し，営業店約300店舗を約30店舗ごとにグループ化し，12のVLANに分割した。これにより1つのVLANに障害が発生しても残り270店舗には影響しない構成とした。また，隣り合う支店は別VLANに収容し，VLAN障害時にも近隣の営業店に影響が及んで顧客の利便性が大きく低下するのを防止した。

(5) 帯域・優先制御による回線処理の安定化

センター回線と営業店回線の速度差吸収及び優先制御の目的で，帯域・優先制御装置を導入した。ルータはルーティング制御機能だけの使用に留め，帯域・優先制御はこの専用装置できめ細かい帯域・優先制御ができるようにした。図1に帯域・優先制御機能を示す。

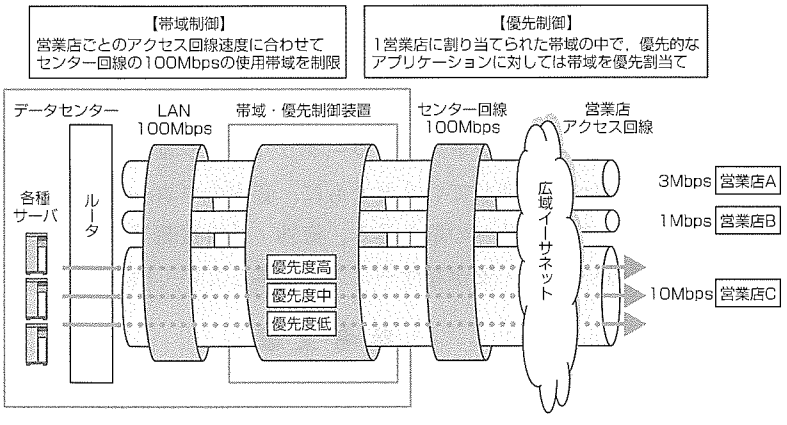


図1．帯域・優先制御機能

広域イーサネットのセンター側は100Mbpsのイーサネット回線，営業店側は1～10Mbpsのアクセス回線のため，両者の速度差が大きい。このままの状態でセンターのサーバから営業店の端末にデータを連続送信すると，速度差が大きいため，網内でフレーム廃棄が発生することがある。そのため，センター側で帯域を制御し営業店ごとの回線速度でデータを送出することにより，網内のフレーム廃棄に起因する回線効率低下を防止する対策を講じた。

新ネットワークでは，e-ラーニングやTV会議などの高帯域なデータとATM(現金自動預け払い機)等の低帯域な勘定系データが混在するため，高帯域を利用するアプリケーション動作時にも重要な勘定系データを優先させるように配慮した。

(6) 擬似環境による事前検証

広域イーサネットサービスは，キャリア新サービス開始直後で実績がまだ余りなかったことと，新しい帯域・優先制御専用装置を導入したことから，その事前検証としてMDIS社内の検証のみではなく，㈱東京三菱銀行のITサービスセンター内に擬似環境を構築し，実際のキャリア回線を使って事前検証を念入りに実施した。その結果，広域イーサネットサービスのキャリアごとのスループット差異，実アプリケーションを使った帯域・優先制御機能等を検証することで，使用しているグループウェア等のトラフィック特性に合った帯域・優先制御装置の最適設定方法等をあらかじめ確認することができた。

既存ネットワークの設計ポリシーの継承及び擬似環境による念入りな事前検証等により，プロジェクト開始から3か月目で擬似環境の評価，4か月目で試行営業店への展開，5か月目で本格展開を実施し，約半年間で営業店300店舗へのネットワーク展開を完了するという非常に短期間でプロジェクトを遂行することができた。さらに，既存の専用線ベースのネットワークと比較して，ランニングコストを増やすことなく大容量化を達成した。

㈱東京三菱銀行は，“高度な信頼性が必要とされる勘定系システムの通信インフラに都市銀行では初めて広域イーサネットサービスを採用した”ことが評価され，日経コンピュータの第7回情報システム大賞・先進技術賞[1]を受賞し，現在は金融系ネットワーク構成のモデルになっている。

3. ブロードバンドネットワークの活用事例

3.1 銀行における業務革新への活用

ブロードバンドの企業内活用は，将来的には様々な業務システムに適用されていくと思われるが，当面はそのリッチコンテンツ化の特長を生かした情報共有・活用の活性

化が中心となる。ブロードバンドネットワークの整備を終えた㈱東京三菱銀行でも，プロジェクト“OPEN”と称してこれを活用した大胆な業務革新に取り組んでいる。ブロードバンドネットワークで結合されたITシステムを活用し，業務の効率化，特に情報検索・入手にかかる時間の短縮化を最大のテーマとしている。**表2**にOPEN業務一覧，**図2**にOPENシステムの構成を示す。ここでは，以下の代表的な3つの業務について紹介する。

3.2 行内ポータル

行内ポータルのコンセプトは，行内のすべての業務及び情報入手・提供の“入り口”である。行員がパソコンを起動してログイン認証を受けると，最初にポータルトップ画面が表示される。メール／スケジューラ機能や，外部のWWWサイトの閲覧，行内業務システムの起動はこのトップ画面から行うことを基本としている。情報発信用には，全行共通用と所属部門用の掲示板がある。また，“トップメッセージ”と呼ぶストリーミング画像を配信し，頭取など経営層からのメッセージ(動画)を自席で見ることができる。このストリーミング配信は，ブロードバンドネットワークを活用したこのシステムの最大の特長でもある。

3.3 ナレッジベース

“時間短縮”をテーマとしたこのプロジェクトでは，“ナレッジ共有”の仕組みにも力を入れている。ナレッジベースとして採用したツールでは，“ベストプラクティス”と呼ばれる共有価値の高い文書を事務局で準備し，システム稼働後直ちに利用できるナレッジベースを構築した。さらに，参照した文書の貢献度を評価する機能を活用して情報提供者に評価を還元する仕組みを構築した。これにより，ナレッジの質の向上を図っている。

一方，登録した文書や様々な情報データベースを検索する機能も強力なものとし，情報検索・入手にかかる時間の短縮も図っている。

3.4 モバイル

情報セキュリティの観点からモバイルへの取り組みには慎重であったが，行員からの強い要望でモバイルパソコンを導入することになった。自宅のADSL回線又は高速モバイルカードから，三菱電機情報ネットワーク㈱(MIND)のモバイルサービスを利用して行内環境に接続し，ポータル画面の参照やメール・スケジューラを利用できる。

モバイルアクセスに当たってはセキュリティの確保に十分配慮しており，ワンタイムパスワードによる個人認証に加え，HDD(Hard Disk Drive)の暗号化，行外でのファイル持出し防止などの機能も取り込んでいる。

表2．OPEN業務一覧

名称	主な業務	特長
行内ポータル	全行統一のポータルトップ ●お知らせ(全行／部門) ●トップメッセージ(動画配信) ●各種業務の起動メニュー	行内への情報提供を行うとともに，すべての業務起動をこの画面からできるようにして，ポータルを全行業務標準として推進。
メール／スケジューラ	メール送受信／スケジュール管理・公開・予約	—
ナレッジベース	コミュニティ(部門)単位でのノウハウの共有活用 ●提案書など文書の共有	行内の情報共有化の基幹ツールとして利用。
e-ラーニング	パソコンを利用して専用教材を用いた自己学習	自席利用のほか，モバイル利用による自宅からの学習も可能に。
TV会議	パソコンを利用した拠点間を接続したTV会議	海外拠点との利用も考慮。
モバイル	行外からのポータルアクセス メール／スケジューラ利用	ファイルの暗号化，FDDへのコピー禁止などのセキュリティ対策を重視。
インターネット接続	外部インターネットサイトの利用	—
共通認証	個人の認証と，OPEN各業務システムへのシングルサインオン	ユーザー認証，ユーザー権限に応じたアクセス権を制御。

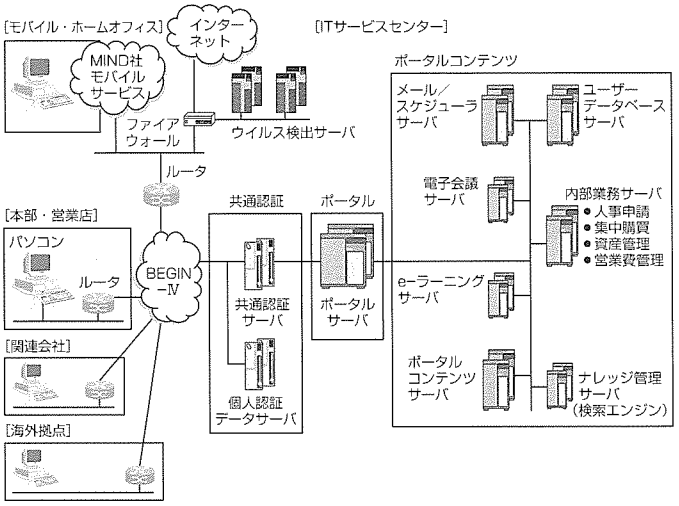


図2．OPENシステムの構成

3.5 プロジェクトOPENの効果

OPENによる，ポータル，ナレッジ，モバイルなどを活用した行内業務の“大胆な改革”はまだスタートしたばかりであるが，行内共通情報サイトとしてその存在を確たるものとしている。今後もブロードバンドネットワークを有効に活用したITシステムのリリースが計画されており，大胆な業務改革が更に加速されていくものと思われる。

4. むすび

銀行業務システムの構築には，高いレベルの安全・安心が要求される。この目的を達成したMDISの先進的な高信頼ブロードバンドネットワークソリューションを今後は他業種へも展開していくとともに，音声のブロードバンドネットワーク化への取り込み，海外・社外接続等においても安価で高速・安全なサービスを提供していく所存である。

参考文献

(1) 勘定系に広域イーサネット，信頼性を徹底追求，日経コンピュータ 2003.2.24，50～51 (2003)

ビル資産価値とテナント向けサービスの向上を提供する“ビル情報サービスソリューション”

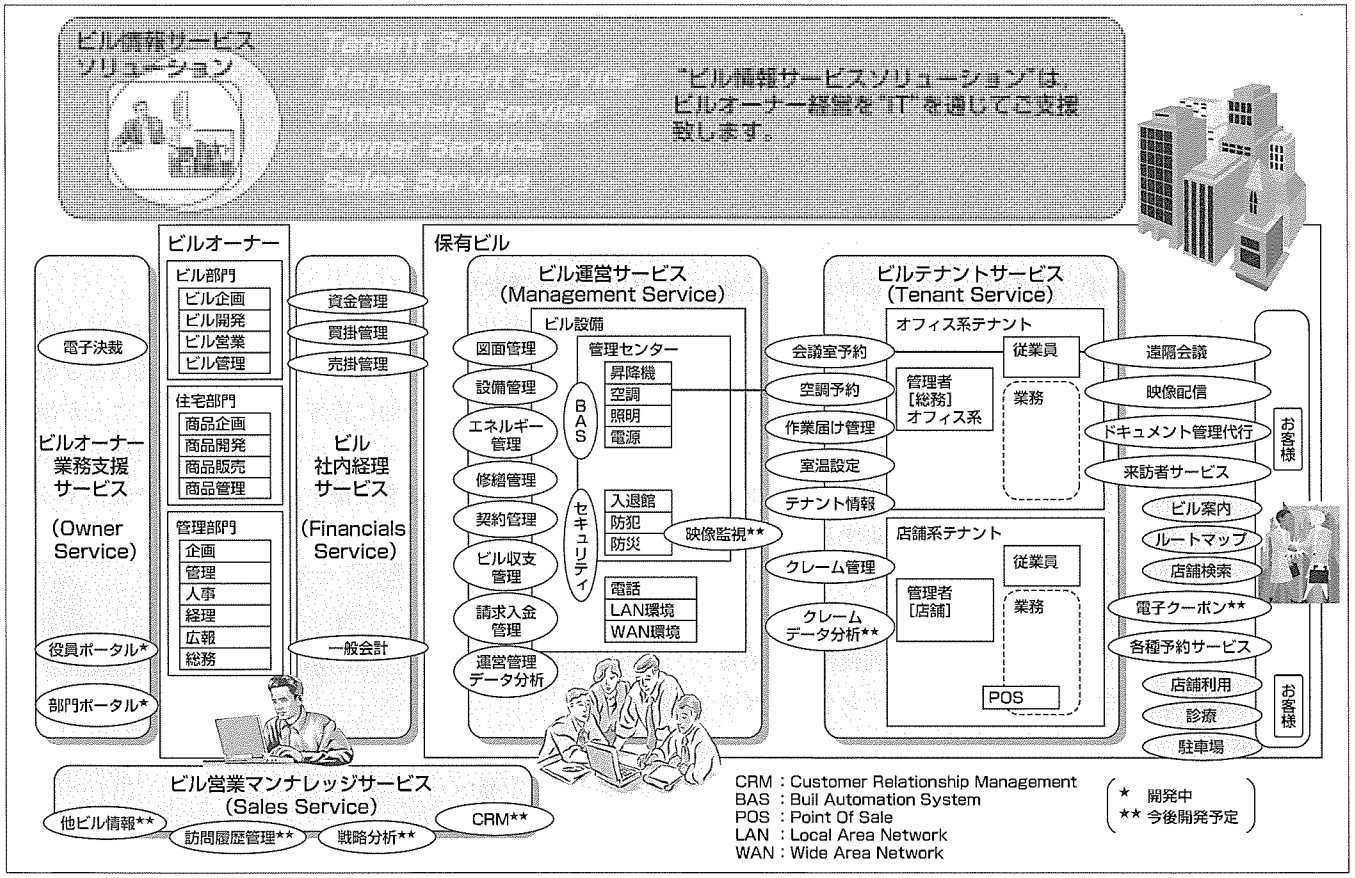
白鳥喜久*
石川和範*
滝口和男*

要　旨

不動産市場は，バブル崩壊に伴いキャピタルゲインが消滅し，企業のリストラとあいまって賃料の下落やテナントの転出が続いたことからビルは供給過剰となっており，ビル経営は所有から収益性の重視へと事業環境が変化している。

三菱電機インフォメーションシステムズ㈱(MDIS)は，従来から大手不動産会社を中心としてビル賃貸業務全般についてのIT化を推進してきたが，これまで蓄積してきた技術と業務ノウハウを集大成し，ビル経営をトータルに支援する“ビル情報サービスソリューション”として提供することにした。このソリューションは，保有ビルの運営・サービスを支援する2つのサブソリューションとオーナー会社の業務を支援する3つのサブソリューションから構成され，インターネットから利用することができる。

近年，企画から開発・契約・維持管理・分析といった一連の不動産ライフサイクルに対して統合的なソリューションの提供への注力が始まっている。このソリューションは，保有ビルのプロパティマネジメントを柱に，ビルオーナー会社業務までを包括的にカバーしており，顧客要件に合わせた組合せの柔軟性及び次ステップに対する継続性と発展性が確保され，安心してシステム導入を図ることができる。また，テキストマイニング技術やナレッジ技術を応用した経営改善のためのデータ分析情報の提供や，優良テナント誘致のための営業マンへの有効情報提供などの機能強化を計画しており，新たな付加価値の創造を目指している。



ビル情報サービスソリューションの全体像

ビル情報サービスソリューションは，①テナントサービスの向上を支援する“ビルテナントサービス”，②ビル設備の資産価値を維持・保全する“ビル運営サービス”，③ビル賃貸業の経理を支援する“ビル社内経理サービス”，④ビル賃貸業の決裁業務を効率化する“ビルオーナー業務支援サービス”，⑤優良テナントの誘致を支援する“ビル営業マンナレッジサービス”の5つのサブソリューションで構成される。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

ビルテナント管理業務に代表されるビル情報サービス分野では，国内企業のリストラや外資系企業の撤退等により需要が低迷し，賃貸相場も弱含みとなってきている。また，大規模ビルの竣工(しゅんこう)がピークを迎え，投資拡大による収支改善も厳しくなったことから，営業力や商品企画力の向上による収益強化に目が向いている。

本稿では，ビル経営に関して不動産業界が抱える課題に対して，このソリューションの目的とこれによる解決策を紹介する。

2. 不動産業界におけるIT化の動向

平成12年11月に"投資信託及び投資法人に関する法律"が改正されたことに伴い，不動産投資信託の組成が可能となり，ビルオーナーの委託を受けて不動産物件の運営を代行するプロパティマネジメントに対する関心が高まっている。このような業界動向を受けて，近年，SAP社(注1)"不動産事業管理ソリューション"など，企画から開発・契約・維持管理・分析といった一連の業務を不動産ライフサイクルととらえた統合的なソリューションが提供され始めた。今後，複数ベンダーの参入が予想されるが，市場は未成熟でありビジネスチャンスは大きい。

3. ビル情報サービスソリューション

このソリューションは，保有ビルごとのプロパティマネジメントを柱に，ビルオーナー会社業務までの全体をカバーしており，5つのサブソリューションから構成される。各サブソリューションは，顧客のニーズに合わせ柔軟に組み合わせて提供することが可能である。

3.1 ビルテナントサービス

バブル崩壊以降，不動産は所有から利用・活用の時代へと変化している。ビルオーナーにとっては，入居テナントの確保と，ビル管理業務の効率化による収益性のアップがますます重要となっている。この課題を解決するために，

(1) テナントサービス向上による顧客満足度の向上

(2) ビル管理者業務の効率化

を目的として，ビル内での日常業務に対し利便性を高めるための各種機能を提供する。**図1**にビルテナントサービスの概要を示す。

3.1.1 インフォメーションサービス機能

ビル入退館，停電，共用設備のメンテナンス等のビル管理者と入居テナント間の依頼や各種連絡，また，ビルガイド，各種申請書などの掲示物参照が，インターネットにつながるオフィス端末から利用できる。また，蛍光灯交換，スポットクリーニングなどの重要な連絡は，メールでも通知されるため，見落としや処理の遅れを防ぐことができる。日常業務の利便性向上とビル管理者とのコミュニケーションの円滑化により，テナントからの安心感と信頼感が得られる。

3.1.2 空調機能

各区画の空調の運転時間変更，温度変更，運転開始・運転停止などについてのテナントからの空調要求を受け付け，BMS(Buil Management System)経由でBAS(Buil Automation System)とリアルタイムに連携する。空調運転のコアタイムパターンをテナント単位に保管し，3か月先までの基本スケジュールが定期的に展開されるため，入力を繰り返すことなく先の予定を見ながら日々のきめ細かな運転制御が可能となる。

3.1.3 会議室予約機能

会議室の予約，変更，取消し，照会が可能で，会議室に付属する備品，付帯設備，利用料金等も一元管理されており，利用者と管理者間での情報共用が可能である。会議室ごとの予約可能時間帯，請求口座などをマスタ情報として保持しており，予約実績データからテナントの請求処理に連携することができる。

3.1.4 外部システムとの連携機能

テナントの契約管理，請求管理，BMSなどは，個々に導入済みのケースも多いが，これらの周辺システムと連携して柔軟なシステム導入が可能である。

今後，テキストマイニング技術などを適用し，クレームデータや利用実績からビルのリニューアル計画へのフィードバックなど，経営に役立つ情報提供機能の装備を目指している。

3.2 ビル運営サービス

近年，複雑化・大規模化するビル施設におけるビルの運営管理・維持保全業務では，コスト削減など施設及び環境を経営的視点から総合的に管理・活用していくことが課題である。このソリューションは，以下3点を目的とする建物資産・運営の効率化を支援するための機能を提供するこ

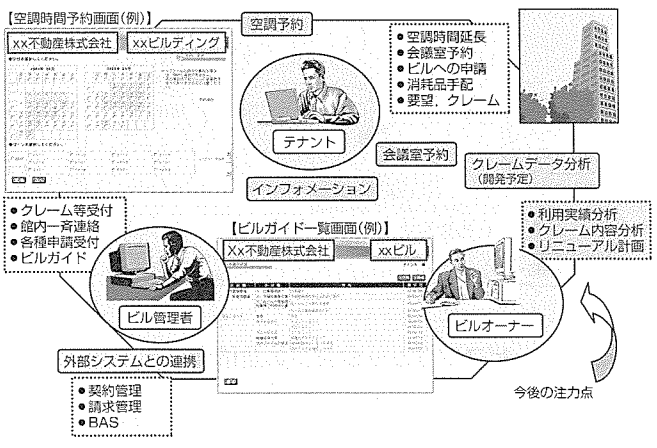


図1．ビルテナントサービスの概要

(注1) SAPは，独国SAP AG社の登録商標である。

とで課題を解決し，最適なファシリティ環境を実現する。

(1) 建物資産の一元管理による資産価値の適正化

(2) 施設の長期活用に対応した合理的な保全計画

(3) テナント請求業務等の契約管理業務の効率化

図2にビル運営サービスの概要を示す。

3.2.1 資産管理系機能

(1) 設備管理・図面管理機能

組織が保有するあらゆる資産(建物・面積・設備・保守履歴等)を体系的に管理する各種台帳機能により，常に最新かつ正確な資産情報を提供する。各種資産情報を検索・加工・分析することにより，資産価値の適正化，資産の有効活用を図ることが可能となる。また，これらの資産情報と電子図面・書類が連動して取り出せるようになっており，管理者の負荷低減と管理業務の合理化へとつながる。

(2) エネルギー管理機能

検針・採取したエネルギーデータ(電気，空調等)を基にトレンドグラフ等を作成し，エネルギー運用の効率化を支援する。コスト実績を管理し，中長期にわたる運用コストの改善計画立案が可能となる。

(3) 修繕管理機能

建物設備の中長期の修繕更新計画値に基づき，予算の立案，実績管理が行える。工事の時期・費用・管理項目等を年度別，ビル別等のシミュレーションで行い，最適計画の立案を支援する。これらの機能により，計画的な予防保全を可能とし，施設の長寿命化・修繕費用最小化を図ることが可能となる。

3.2.2 契約管理系機能

テナント契約，テナント請求・入金管理，収支管理まで，きめ細かくカバーし，テナント管理業務の効率化を支援する。契約管理と請求・入金管理を連動させることにより契約更新及び変更をシステムに反映させ，請求・支払業務の自動化を実現した。また，収支管理では，ビル別，テナント別等，様々な視点で収益管理(コスト管理)が可能となり，ビル経営を支援するための情報を提供できる。

このソリューションは，資産管理系機能と契約管理系機能の各機能コンポーネントが有機的に結び付き，ビル運営全般にわたるソリューションを提供している点に特長がある。

3.3 ビル社内経理サービス

現状ではビル賃貸業務にフィットした経理パッケージはなく，独自のアプリケーションシステムとして手作りするか，既存ERP(Enterprise Resource Planning)パッケージに多くのカスタマイズを加える必要があり，費用と期間を抑えたシステム構築が課題である。このソリューションは，ビル賃貸業務向けの経理システムの提供を目的として，下記の5機能を提供する。ビル賃貸業務の経理システムは関連する契約管理・請求入金管理・修繕管理・ビル収支管理と整合することがポイントであり，これを組み込んだ機能を提供することにより，ビル賃貸業の経理に適合するシステム導入が可能となる(図3)。

(1) 一般会計

グローバルなデータ管理で会計管理，データ収集，情報アクセス，財務レポート生成など

(2) 買掛管理

支払請求入力から支払手続きまでの管理，定期支払は契約情報から自動生成など

(3) 売掛管理

受注から入金のプロセスに対する請求と回収の財務管理など

(4) 発注管理

発注申請，工事請負書，注文書，注文請書の出力，工事費支払管理など

(5) 統合分析

財務レポート作成や予算編成，計画作成，財務分析などの管理会計をサポート

3.4 ビルオーナー業務支援サービス

ビルオーナー会社業務のIT化については，必要に応じて個別に進められてきた状況と見られるが，結果的に様々なプラットフォームの氾濫(はんらん)やユーザー利用環境の不統一が起こり，必要とする情報の検索に多くの時間を

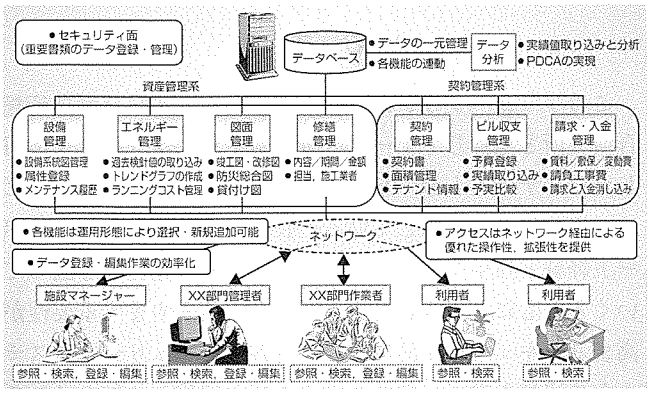


図2．ビル運営サービスの概要

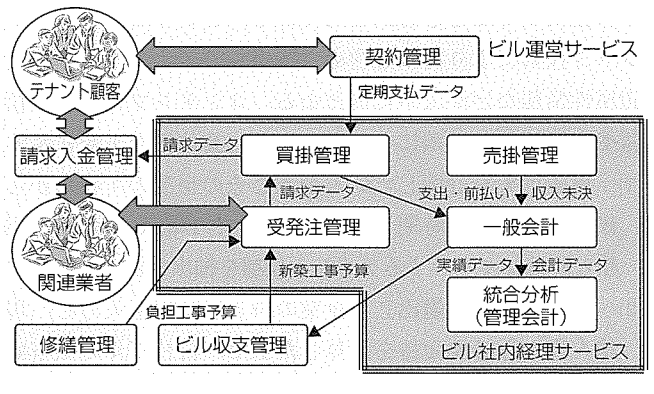


図3．ビル社内経理サービスの概要

割かれている。このため，重要な決裁業務の滞りで機会損失を招くおそれが出てきている。

これらの課題を解決するために，このソリューションでは，次の目的で次項の2つの機能を提供している(図4)。

(1) 個別のシステムから該当部門や役員が必要とする情報をタイムリーに提供し，業務の効率化を図る。

(2) インターネット環境下で，いつ，どこからでも決裁や承認業務を行えるようにし，決裁業務の滞りを防ぐ。

3.4.1 ビルポータル機能

様々なプラットフォームで構築された既存システムをこの機能を使って融合させることで，タイムリーな情報提供を可能とする。ポータルシステムとしての玄関の位置付け以外に，抽出条件を任意に設定しておくことでシナリオ実行型(プッシュ型)で情報を提供することが，大きな特長である。例えばワーストテンプロジェクトの表示など，重要なチェック事項を常に目に留まるようにすることもできる。

この機能は，部門別，個人別，役員向けにと，用途に応じた情報を関連付けて表示することが可能で，不動産会社の財産である情報の有効活用が図られる。

3.4.2 電子決裁機能

決裁文書の作成から承認業務，役員決裁までを行うワークフロー機能であり，文書の重要度等により決裁ルートを自由に設定・変更することができる。また，回覧機能を使って部下の意見を聴いて承認することや他役員の同意を得ることも可能で，これは一般のワークフロー機能にない特長である。インターネット環境からの利用が可能であり，都合の良いときに決裁や承認業務を実施できるため，業務の滞りが出ない。また，職制と職位で文書単位にアクセス権限の指定が可能となっており，セキュリティの確保が図られている。

3.5 ビル営業マンナレッジサービス

新規インテリジェントビルの乱立や空室率の上昇といった"不動産戦国時代"の到来に伴い，優良顧客をテナントとして勧誘・獲得することがビルオーナーにとっての大きな課題である。このソリューションは，テナント獲得のための営業活動を効率良く行うために必要な情報をビル営業マンに提供することを目的としており，シナリオ実行型のナレッジ技術により将来を含めた空室へのテナント候補と周辺属性情報などが入手可能となる。コンテンツは自社内情報や市販情報の種類により異なるが，具体例を下記に示す。

(1) 事業拡大を計画している企業とその企業の所在地から候補企業と移転時期予想を割り出し，自社ビルの空室面積と時期にマッチするテナント候補を抽出するコンテンツ

(2) 自社ビルから退出した企業の再入居時期を入力し，現状人員から必要面積を計算した上で，自社ビルの空室面積と時期にマッチするテナント候補を抽出するコンテンツ

(3) 上記テナント候補の周辺属性情報として，取引業者であった場合は発注額を参照でき，退出した企業であれば退出理由を参照できるコンテンツ

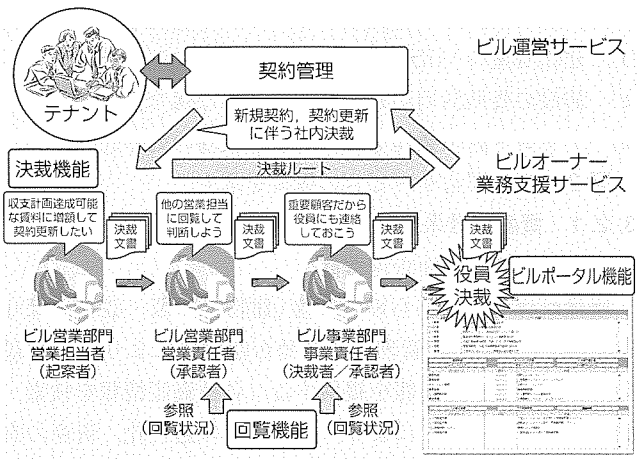


図4．ビルオーナー業務支援サービスの概要

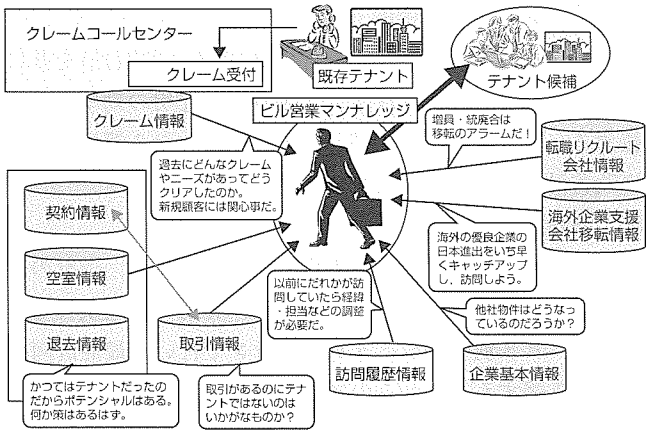


図5．ビル営業マンナレッジサービスの概要

営業マンは，情報の保管場所やシステムを意識することなく，抽出したい切り口で検索したり，最新情報にアップデートされたタイミングで自動的に必要な情報を入手することが可能になる。また，一度登録した抽出条件はテンプレートとして営業の資産として繰り返し活用できる。これにより，裏付けのある確度の高い情報をタイムリーに入手し，勧誘・獲得を進めることが可能となる(図5)。

4. むすび

このソリューションは，今後は，三菱電機㈱情報技術総合研究所と連携してデータ分析技術やナレッジ技術を応用したビルテナントサービスやビル営業マンナレッジサービスの機能拡充を計画している。長年の大手不動産でのサポート経験と技術を生かし，サービス内容の充実化を図っていくとともに，ビル経営にとっても今後ますます重要性が高まるセキュリティ面についても各種セキュリティシステムとの連携を進め，安全で安心なビル情報システムインテグレーションの提供に取り組んでいく。

高信頼性・拡張性を実現した“三菱電機ビルテクノサービス㈱情報センターシステム”

佐藤利明*
五十嵐敏之**

要　旨

三菱電機ビルテクノサービス㈱は，“より快適なビルの空間環境づくりを通じ，豊かな人間社会の実現に貢献する”を企業理念として，“トータルビルシステム事業”を展開している。その中で，情報センターシステム（以下，MIC(注1)）はこれら事業の中核と位置付けられ，日本全国で約20万台の昇降機，約30万台の冷熱空調機器のデータを管理・活用し，お客様からの問い合わせや修理依頼・故障時の緊急対応や設備機器の遠隔監視などを行い，ビルオーナーや利用者に安全・安心をお届けしている。MICの業務はエレベーターの閉じ込め救出に代表されるように緊急を要する業務が多く，これらに迅速かつ確実に対応するため24時間365日連続稼働の高い信頼性が要求される。

高い信頼性は主に以下の3点に集約される。

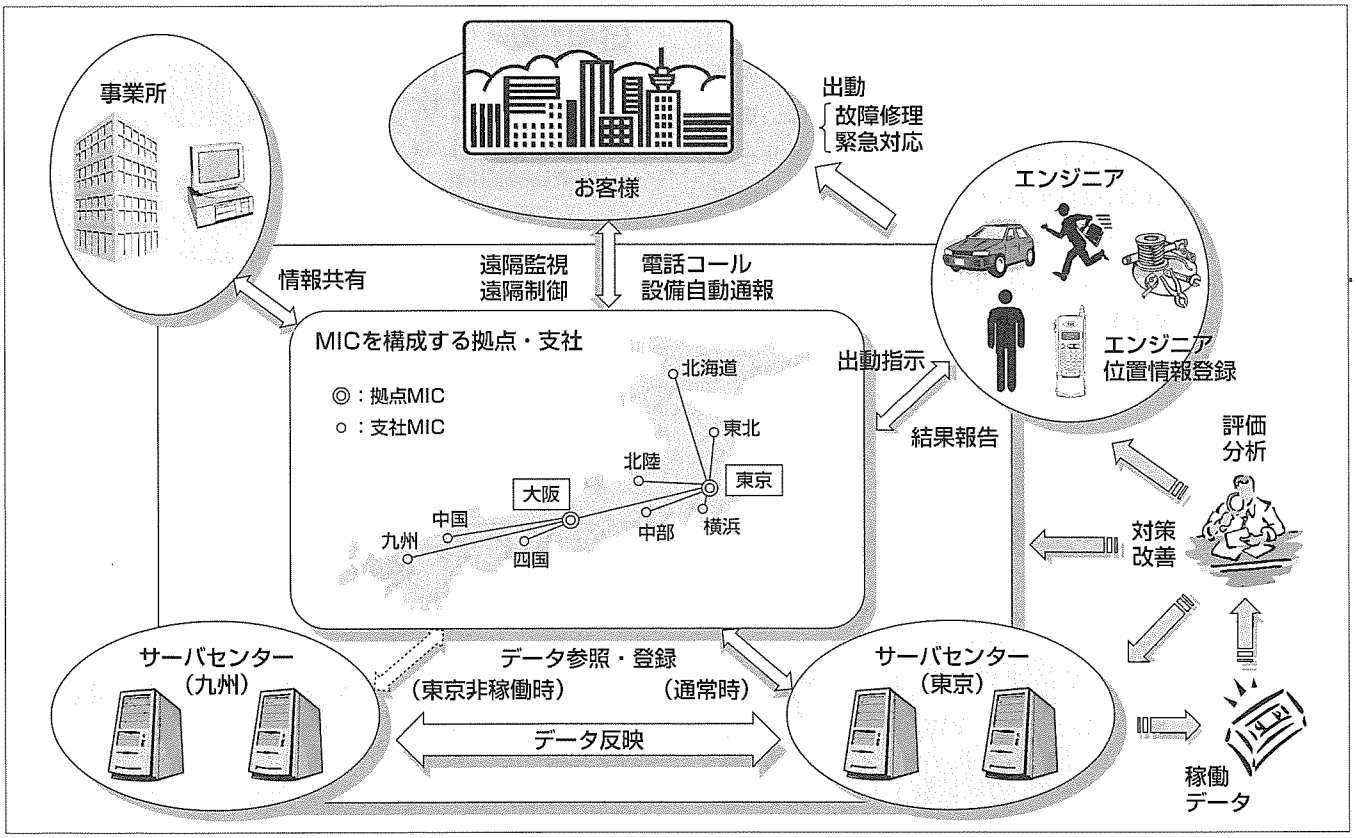
- お客様の電話を確実に受信できること
- システムメンテナンスや機器の故障・地域被災の影響でサービスが止まらないこと
- ハードウェアやソフトウェアの障害を最小限に抑え，止まらずに業務を継続できること

これらを実現するために以下の工夫を施している。

- 受信業務や監視業務に不可欠なサーバの二重化
- 電話受信拠点の相互代行機能
- 顧客データを遠隔地に二重化し内容は直ちに反映
- 各機器と常駐プログラムを常時監視し，問題があった場合は自動通知する仕組みを導入

さらに，システム全般にわたる継続的な稼働評価を実施することにより，正確な各種業務量の把握を可能とした。その結果，エレベーターの機能拡張を始めとするお客様サービスの更なる向上を見越した拡張性の見極めやシステム増強時期等の予測も可能とした。

（注1）　MICは，Mitsubishi Electric Building Techno-Service Information Center Systemの略称である。



三菱電機ビルテクノサービス(株)情報センターシステム(MIC)の全体図

MICでは，お客様からの電話コールを確実に受信し，設備を常時遠隔監視している。拠点MICと支社MICは受信業務の代行が可能で，サーバセンターを2局遠隔配置とし，ノンストップを実現している。また，システムの稼働評価を定期的に実施し，将来的な機能拡張を見越したキャパシティの見極めに万全を期している。

*三菱電機インフォメーションシステムズ㈱　**三菱電機ビルテクノサービス㈱

1. まえがき

三菱電機ビルテクノサービス㈱MICでは，エレベーター内の閉じ込め故障等への対応のため24時間365日連続稼働の高い信頼性が要求される。本稿では，高信頼性を実現するための工夫及び本稼働後の稼働評価と改善の具体例について述べる。

2. MICの概要

MICでは，全国で約20万台の昇降機，約30万台の冷熱空調機器を対象として，図1に示すような以下の業務を行っている。

(1) お客様からの問い合わせに対する電話対応
(2) お客様からの修理依頼や故障時の緊急対応のためエンジニアに出動を指示し，一連の処置が完了するまで管理
(3) ビルの設備機器を回線経由で常時遠隔監視

3. 高い信頼性と拡張性の実現

MICの業務は，エレベーターの閉じ込め救出を始め，建物設備の遠隔監視など，安全の確保に不可欠な業務が集中しており，24時間365日連続稼働の高い信頼性が不可欠である。さらに，地域被災や台風などによる局所的な業務の集中があっても問題なく処理を継続できる仕組みが必要で，以下の工夫をしている。

3.1 電話コールを確実に受信

全国のMICでは，平日夜間・休日は東京と大阪の二大拠点で電話の代行受信を行っている。これら拠点では，電話を受信するCTI(Computer Telephony Integration)サーバを二重化して，故障時は待機系のサーバに切り換える構成としている(図2)。また，集中豪雨などにより支社MICに電話コールが集中しても，拠点MICや事業所で受信を可能とすることでお客様からの応答待ちをなくし，確実な受信を可能としている。

3.2 ビルの遠隔監視

ビルの遠隔監視は，MICの遠隔監視受信装置を通して，REP(REceive Panel)サーバで行っている。REPサーバの故障はビルの遠隔監視不可に直結するため，REPサーバもCTIサーバ同様に二重化し，故障時は待機系のサーバで確実に監視を行うことができる構成としている。

3.3 顧客データの多重化

業務データは集中型とし，サーバセンターで管理しているが，完全に同一機器構成のサーバセンターを東京と九州に二組配置し，地域被災も考慮した構成としている。普段はいずれか一方のサーバセンターで業務を行い，更新された顧客データは，高速なフレームリレー網を通して1分以内でタイムリーに同期合わせを行っている。データベースの同期合わせはOracle(注2)の機能を活用し，高速・正確にデータの反映を可能とし，切換えに要する時間も旧システムと比べ約5分の1に短縮している(図3)。

(注2) Oracleは，Oracle Corp.の米国及びその他の国における登録商標である。

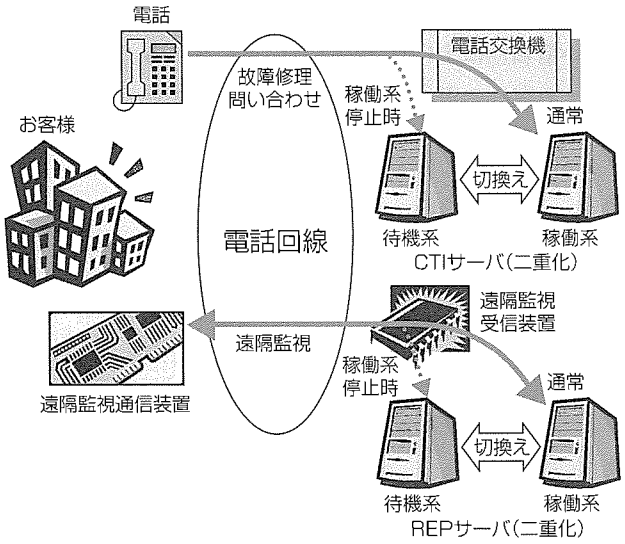


図2．サーバの二重化

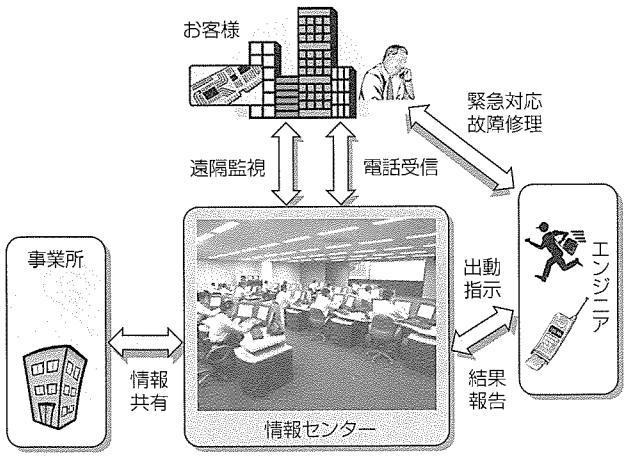


図1．MICの概要

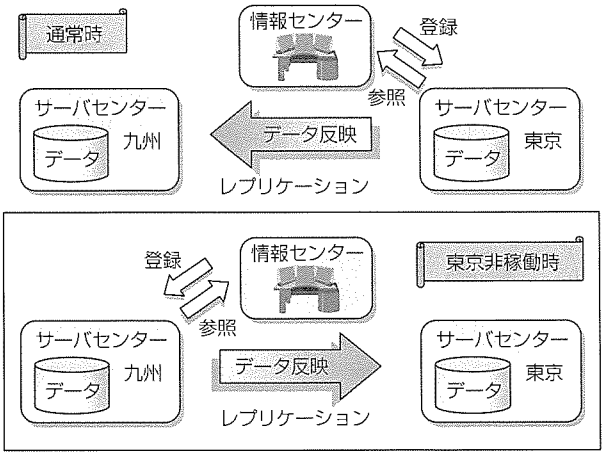


図3．顧客データの多重化

3.4 日々の運用監視による障害回避

MICを構成する機器は全国にわたり，その数は数百台規模にのぼる。これらの運用負荷を軽減するため，運用監視ソフトウェアを導入することにより問題箇所の自動検出と障害発生時のメール通知が自動化され，監視業務の省力化及び運用コスト低減を実現している。

4. システム稼働評価と負荷改善

MICでは，前述の高信頼性・拡張性だけでなく，日々増大する顧客データ，年々拡張する顧客ニーズの多様化・高度化にも十分に余裕を持って対応できるだけのキャパシティを持たなければならない。設計時点で将来までの顧客データの伸びは考慮されているものの，例えば，顧客サービス向上のため，エレベーターの監視内容の細分化によって業務データが増加したり，計画値を超過してデータ件数が増加するケースもある。このような予測を超えたデータ量の伸びがあっても，従来と同等のレスポンスを確保しサービスレベルを維持し続けることが課題となる。この解決のため，MICを構成する各サーバ／クライアントの稼働データを定期的に採取し，評価・分析している。これらデータ採取は，従来，クライアントやサーバ単体に限ったデータ採取が主体であった。MICでは，システムを構成する機能の異なったサーバそれぞれに焦点を当てて，機器全般にわたる稼働データを採取・分析している(**図4**)。これにより稼働状況の推移と影響を正確に見極めることが可能となり，効果的な改善策の実施に結び付けることができる。以下に具体的な事例の一部を記述する。

本稼働後6か月経過時点で稼働データを採取し評価・分析した結果，**表1**の網掛け部分を改善課題としてピックアップした。

(1) 機能拡張により業務データ件数の伸びが一部設計値を大きく上回っている(**図5**)。
(2) データベースサーバのCPU利用率が想定より高負荷となっている。
(3) 画面の応答性能が一部悪くなっている。
(4) その結果，想定していた時期より前に処理能力の限界に達してしまう見通しとなった。
(5) 一方，APPサーバの負荷は設計当初の計画どおりであった。

次に，これらの改善課題をクリアするために実施した対策とその効果を**表2**に示し，その改善策の内容を実施順に説明する。

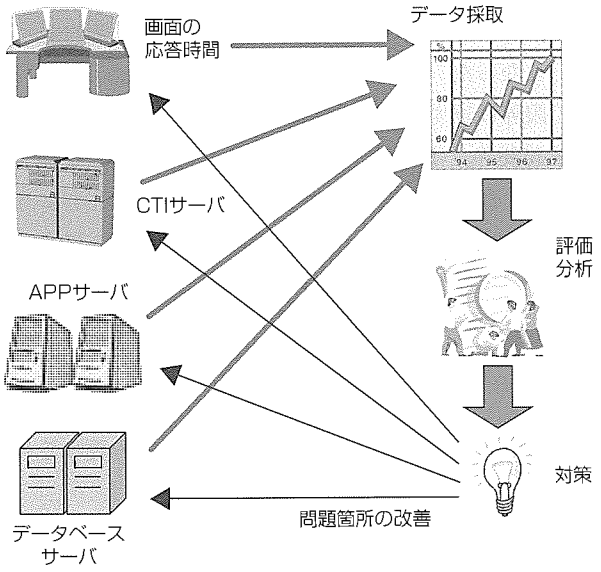


図4．稼働評価

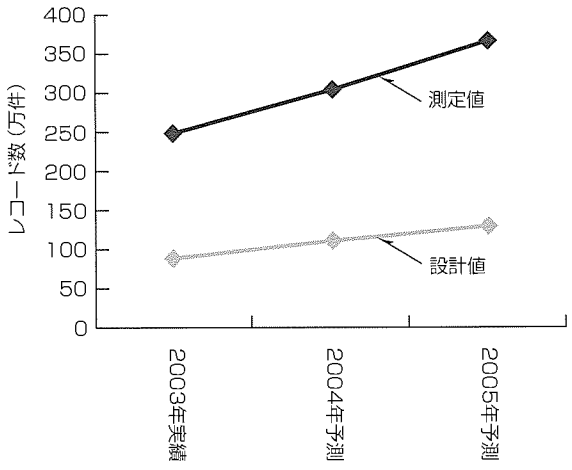


図5．設計値と異なる業務データの例

表1．稼働データ採取項目と稼働後6か月の評価

No.	項目		データ採取方法	評価ポイント	評価
1	業務データ件数集計		データベースから件数を集計	件数が想定値より多くないか データベースの領域を圧迫していないか	改善要
2	業務画面の応答性能		ログから応答時間を算出	応答時間が遅くなっていないか	改善要
3	APPサーバのCPU利用率		Windows(注3)パフォーマンスモニタ	稼働率が許容値より高くなっていないか	問題なし
4	データベースサーバ	CPU利用率	UNIX(注4)のsar	稼働率が許容値より高くなっていないか	改善要
5		メモリ使用状況	Oracleの分析ツール	メモリの有効利用がなされているか	問題なし
6	CTIサーバのCPU利用率		Windowsパフォーマンスモニタ	稼働率が許容値より高くなっていないか	問題なし

(注3) Windowsは，米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。
(注4) UNIXは，米国The Open Groupの登録商標である。

4.1 業務アプリケーションの改善

データベースサーバのCPU利用率の伸びが想定よりかなり高い上昇傾向にあることが判明した。分析の結果，処理の内容を細分化することでCPU利用率を低減可能であるとの結論に到った。実際に，業務アプリケーションの処理を分割・再構成した結果，**表2**のNo.1及び**図6**の①に示すようにCPU利用率を軽減することができた。

4.2 データベースの配置改善

画面応答性能が悪くなってきたためクライアント側処理を分析したところ，データベースからの応答時間が従来に比べて遅くなっていることが判明した。分析の結果，下記が明らかとなった。

(1) あるテーブルのアクセスがボトルネックになっていて，原因は設計当初の想定件数を上回るデータ量である。

(2) データベースサーバの稼働データから入出力に費やす待ち時間が次第に遅くなっている。

(3) 画面側の処理時間は同じであるが，データベースサーバ側の処理時間が次第に遅くなっている。

このことから，原因としてデータベース断片化の影響を疑った。データベースは日々データが更新されることで，次第にDisk上の断片化が進行する。その結果，入出力に要する時間が次第に遅くなり，応答性能に影響を及ぼす可能性がある。さらに，領域の使用効率も悪くなりDisk容量が不足する危険があった。これを解消するために，必要なテーブルに限定し，計画より早期にデータベースの再構成を実施した。この結果，定常的にかかるDiskのI／O待ちの削減に一定の効果を上げ，無駄な領域の削減を達成した。これに加えこれまで蓄積してきた業務データの保持期間を最適化することで，**表2**のNo.2とNo.3に示すように，画面応答性能を従来の半分以下に短縮することができた。さらに，データベース断片化解消の恒久対策としても，定期的にデータベース再構築を行う仕組みを導入した。

4.3. ハードウェアの改善

上記の改善を施してきたものの，業務拡張による業務データの伸びは依然として残り，データベースサーバのCPU利用率の伸びは2004年中に処理能力が限界に近づく見通しとなった。これは，当初の想定である2005年より1年早く限界に達する計算となる。とはいえ業務データの伸びは業務要件上不可避の側面もあるため，CPUを従来より1.5倍高速なものに置き換え，**図6**の②に示すようにCPU利用率を低減した。これにより，**図6**の③に示すように，CPU処理能力の限界が2008年以降に伸び，今後の業務拡張にも備えた十分なキャパシティを確保した。

表2．負荷改善項目と効果

No.	項目	改善箇所	効果
1	業務アプリケーションの改善	①データベースサーバCPU利用率	21%削減
2	データベースの配置改善	②データベースサーバI／O待ち	43%削減
3		③画面の応答時間	57%削減
4	ハードウェアの改善	④データベースサーバCPU利用率	32%削減

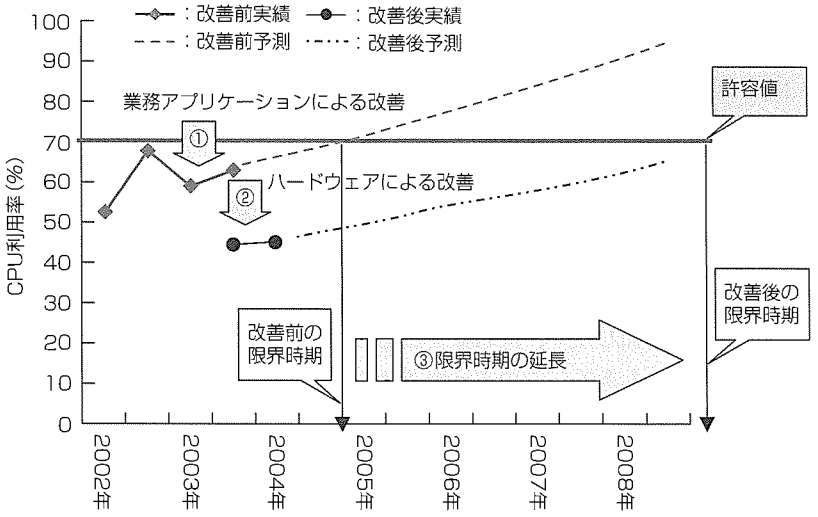


図6．データベースサーバ処理能力限界時期の変化

5. 今後の課題

(1) 各種サーバ二重化における切換所要時間の更なる短縮

(2) CTIサーバの稼働評価と改善対策

(3) 日々更新されるデータ領域の最適化配置

6. むすび

MICの高信頼性を確保する工夫及び稼働評価と改善事例について述べた。今後も，一層の利便性・情報の提供など，さらに使いやすい機能を拡充し，いままで以上にビルオーナー・利用者へ更なる安心を提供する所存である。

オープンネットワークを活用したビル設備システムコントローラ

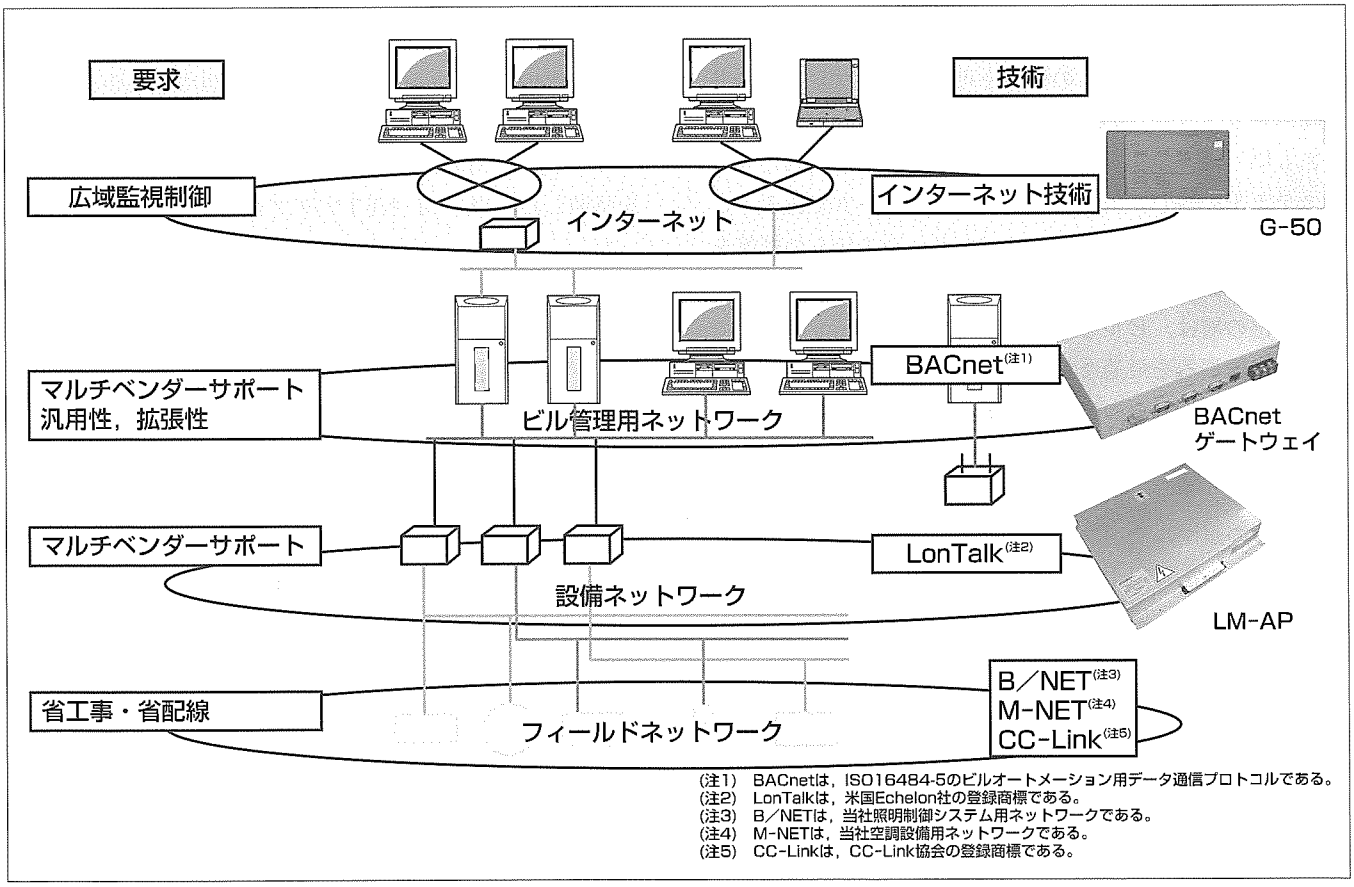
小宮紀之*
久代紀之*
鈴木繁樹*

要　旨

保守・メンテナンス作業の合理化を目的に，ビル・店舗に設置された空調・照明等各種設備機器を遠隔から監視・保守する設備機器監視システムの導入が国内外で活発化している。これらシステムの本格普及に際し，すべての機器を自社開発品で賄うクローズドなシステム構成から，インターネットを始めとする各種オープンなネットワークを用い他社・自社製品を自在に組み合わせるオープンなシステム構成が，低コスト化を目的に強く要求されている。

三菱電機では，このようなシステム構成に必要なオープンネットワーク対応ビル設備システムコントローラと基本技術を開発してきた。

本稿では，ビル設備システムのネットワーク階層と近年の動向，及びオープンネットワークに対応したこれらの基本技術，システムコントローラ群について述べる。



(注1)　BACnetは，ISO16484-5のビルオートメーション用データ通信プロトコルである。
(注2)　LonTalkは，米国Echelon社の登録商標である。
(注3)　B／NETは，当社照明制御システム用ネットワークである。
(注4)　M-NETは，当社空調設備用ネットワークである。
(注5)　CC-Linkは，CC-Link協会の登録商標である。

ビル設備システムのネットワーク階層と対応製品

ビル設備システムに用いられるネットワークは、図のように4階層に分類できる。フィールドネットワーク内のコントローラ間の接続を行う設備ネットワーク以上の階層の各種ネットワークではマルチベンダー化への要求が高まっており、その実現のため、ネットワークのオープン化が進んでいる。これらオープンネットワークに対応した各種ビル設備システムコントローラを開発した。

*住環境研究開発センター

1. まえがき

ビル・店舗の空調・照明等各種設備機器を遠隔から監視・保守する設備機器遠隔監視システムの導入が国内外で活発化している。すべての機器を一社の製品で賄うのではなく，より低コストな部材を自由に選択してシステムを構築することが可能なマルチベンダーシステムへの要求が高まってきている。そして，その実現のため，ビル設備システムのオープンネットワーク化が進められている。

本稿では，2章でビル設備システムのネットワークの動向について概観し，3章で設備ネットワーク，ビル管理ネットワークのオープン化対応技術，4章でインターネット対応技術について述べる。

2. ビルオープンネットワークの動向

ビル設備システムは4階層のネットワークで構成される。

最下位層は，設備機器フィールドネットワークであり，設備機器，操作器(リモコン)，センサの接続を行う。この階層に対する要求は，インテリジェントな設備機器間を接続するための拡張性，ビル内に分散的に配置される設備機器，操作器，センサ間配線の省工事化である。

第2階層は，設備制御ネットワークであり，各設備機器フィールドネットワーク内のコントローラ間の接続を行う。マルチベンダーシステムの構築を可能とするプロトコル共通化，ネットワークの省配線化が要求される。

第3階層は，空調・照明等の設備ごとに構成されたサブシステムを接続し，統合管理するネットワークである。この階層に対する要求は，マルチベンダーシステムの構築を可能とするプロトコル共通化である。

最上位の層は，ビルを遠隔から管理するネットワークである。設備機器を最適な状態に保ち省エネルギー運用する手段として設備機器の遠隔運用が注目されており，そのための情報通信手段として，インターネットが使用される。

複数のベンダーの機器を組み合わせて最適なシステムを構築するのがマルチベンダーシステムであり，マルチベンダーシステムを実現するためにネットワークのオープン化が進んでいる。設備管理ネットワークのオープン化技術として，LonTalk(LON(注6))，BACnetがある。

LonTalk(LON)は，第2階層のネットワークを対象としている。ネットワークの標準仕様には設備機器を制御の対象としてモデル化したオブジェクト仕様が含まれており，物件ごとのインタフェース設計が効率的にできる。また，小規模な機器の場合は，市販の通信チップ(Neuron Chip(注6))の内蔵機能を使用することで，簡単にネットワーク機器を実現することができる。

BACnetは，大規模ビルでの設備システム間の相互接続ネットワークとして適用が進んでいる。BACnetも同様にオブジェクト仕様が定められている。BACnetのオブジェクトは，汎用性・記述性に富むが，反面，ビル物件ごとに定義すべき内容が多く，システムインテグレータの負荷が大きい。そのため，中小規模ビルでは，BACnetでなく，LonTalk(LON)を用いて設備システムをビル管理システムに接続する場合も多い。

(注6) LON，Neuronは，米国Echelon社の登録商標である。

3. 設備管理ネットワークのオープン化技術

3.1 LON対応システム

LON(Local Operating Network)は米国Echelon社によって開発された設備制御用ネットワーク(空調，照明，配電，セキュリティ，他)で，米国，欧州ではデファクトスタンダードになりつつあるものである(プロトコル：LonTalk)。

3.1.1 LONシステムの課題

LONを設備ネットワークへ適用する場合や既存システムに適用する際には，次のような課題があった。

(1) 標準構成では制御点数が少ない(62点)

(2) ネットワーク設定，メンテナンスのための専用ツールが不可欠

(3) ツール機能実現のためには高価なソフトウェア開発キットが不可欠

(4) 既存のシステム・機器の資産が活用できない

これらの課題を解決するために，LON通信管理ミドルウェア(LON Management Middleware：LMM)と，それを搭載したLON／M-NETアダプタ(LM-AP)の開発を行った。

3.1.2 LON通信管理ミドルウェア(LMM)

LMMは大規模システムへの適用やLON機器のアドレス設定，接続設定やメンテナンス等のネットワーク管理を組込機器から行う通信管理ミドルウェアで，以下の特長を備える(図1)。

(1) LON管理点数の大幅拡張(62→4,096点)

(2) ツール機能(ネットワーク管理機能)の低コスト実現

3.1.3 LON／M-NETアダプタ(LM-AP)

LM-APは，当社ビル用マルチエアコンの室内機50台をまとめてLONシステムに接続可能とするアダプタである。LMMの搭載により，50台：制御点数約1,000点の監視・制

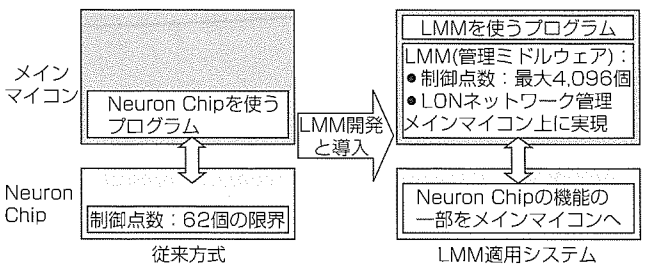


図1．従来方式とLMM方式

御を実現している(図2)。

LM-APでは，LON標準機能に加えて当社ビル用マルチエアコン独自の機能(立ち上げ，メンテナンス機能等)をLONで取り扱う拡張機能も用意している(図3)。

3.2 BACnet対応システム

BACnetは，国際標準(ISO16484-5)のビル設備機器管理ネットワーク用通信プロトコルである。国内での実現形態はBACnetに接続されるゲートウェイ(Icont)を用意し，そこから各社独自のネットワークシステムへと接続するのが一般的である。

3.2.1 BACnet適用システムの課題

(1) BACnetオブジェクト，オブジェクトと自社設備システムとの対応を物件ごとに作り込むため，カスタマイズコストが膨大

(2) Icontはパソコンベースで製作されるため，コストが高く，耐久性に課題

これらの課題を解決するために，当社では，組込機器によるオブジェクトや接続設定が容易なBACnetゲートウェイを開発した。

3.2.2 BACnetゲートウェイ

既存設備システムを丸ごとBACnetに接続可能とするゲートウェイであり，以下の特長を持っている。

(1) 物件ごとのカスタマイズの容易化を実現

Webサーバ機能を搭載し，BACnetオブジェクト，設備ネットワークオブジェクト，相互接続設定，その他各種設定をすべてWeb経由で実施可能とし，エンジニアリング低コスト化を実現した。また，設備ネットワーク部の交換を容易にしたソフトウェア構造により，各種設備ネットワークへ容易に対応可能とした。

さらに，LON対応のゲートウェイでは，LMMを搭載することにより，LON端末間の接続設定等もWebから可能とした(図4，図5)。

(2) ハードウェアの小型・低コスト化，高信頼性化を実現

類似又は同等機種が多数接続されることが多いという設備ネットワークの特性を考慮したネットワーク相互のデータ交換方式の開発により省メモリ，高速動作を実現した。また，組込機器での実現により高信頼性を確保した。

3.2.3 適用製品

(1) BACnet-B／NETゲートウェイ

当社照明制御システムB／NETを丸ごとBACnetに接続するゲートウェイで，約2,000台の照明機器を制御できる(図6)。

(2) BACnet-LONゲートウェイ

当社照明制御システムMELSAVE-NET(LON)を丸ごとBACnetに接続可能で，LMMを搭載し，大規模システム対応，LON側端末機器の接続設定対応を実現した。

4. インターネット対応遠隔監視システム

4.1 遠隔監視システムの課題

ISO14001などの導入や地球温暖化問題により省エネルギー意識が向上し，最適運転，最適機器メンテナンス，最適運用計画による省エネルギーを実現する遠隔監視システムへの要求が高まっている。遠隔監視システムを構築する上で，下記のような課題を解決する必要がある。

(1) 通信費削減

監視機器の高機能化，監視アプリケーションの高度化により，データ量が増大している。

(2) 監視側マンマシンソフトウェアの開発費の低減

物件ごとに異なるカスタマイズが必要なマンマシンソフトウェア開発費が大きく，システムコストが増大している。

(3) 現地作業削減によるメンテナンス費用の低減

初期設定，プログラムの入替えなど，現地で行うメンテナンスに時間がかかっている。

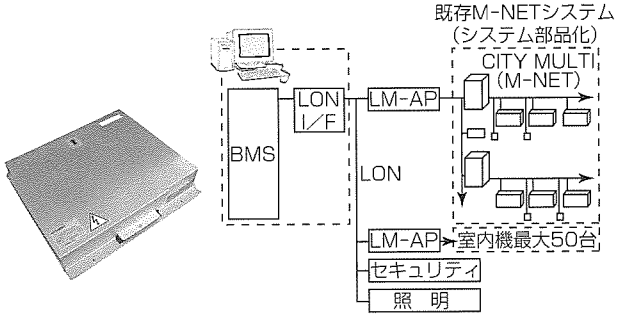


図2．LM-APの外観とLM-APを適用したシステム構成

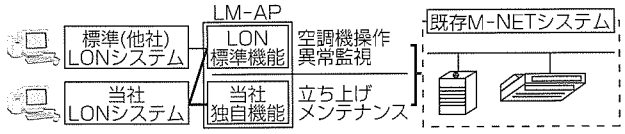


図3．LM-APの拡張機能

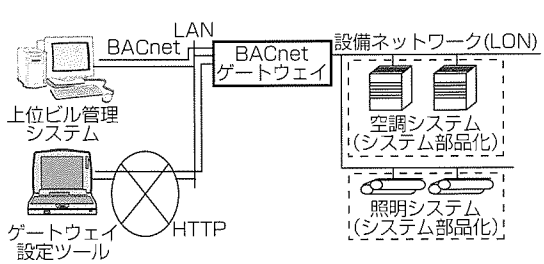


図4．BACnetゲートウェイを適用したシステム構成

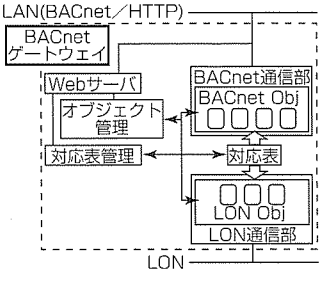


図5．BACnetゲートウェイの概略構造

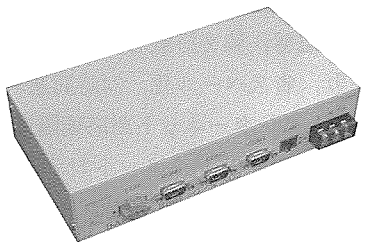


図6．BACnet-B／NETゲートウェイの外観

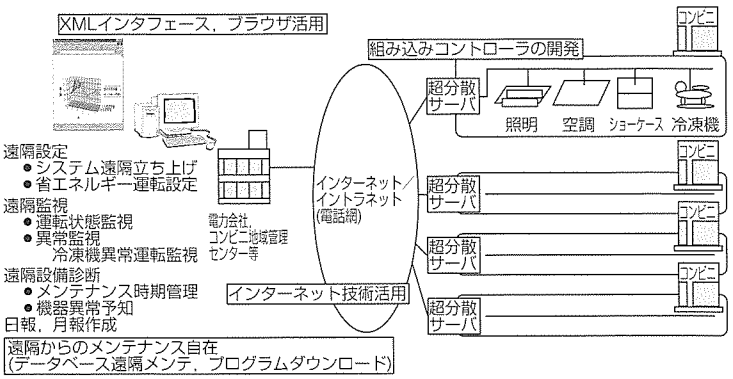


図7．インターネット対応遠隔監視システム

表1．仕　様

MPU	型名	M32R/E(ルネサス32ビットワンチップ)
	動作周波数(MHz)	66
SDRAM(Mバイト)		24
Flash ROM(Mバイト)		16
電源電圧(V)		100
質量(kg)		1.4
寸法(mm)		(W)210×(H)160×(D)64
液晶モニタ	サイズ(インチ)	5.7(STNカラー)
	画素数(ピクセル)	320×240
	表示色(色)	256
外部I／F		RS-232C，Ethernet(10Base-T)

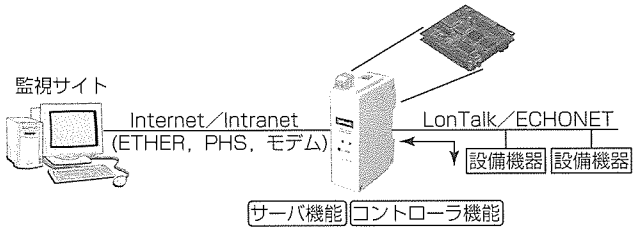


図8．OpenDuetの概要

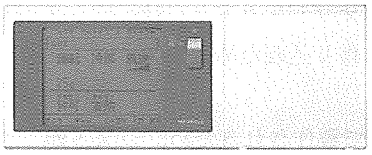


図9．G-50の外観

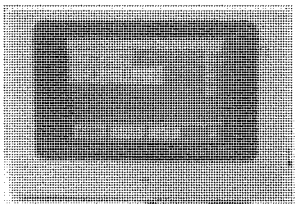


図10．省エネルギーモニタの外観

(4)　現地コントローラの小型化と高信頼性

現地コントローラの省スペース化，24時間運転への要求が高い。

4.2　課題解決策

(1)　インターネット技術の徹底活用

現地と遠隔サイト間にインターネット技術を活用することにより，ブロードバンドなど安価で高速なネットワークを使用することを可能とした。

(2)　XMLインタフェース，ブラウザ活用

現地と遠隔サイト間のインタフェース記述言語にXML(eXtensible Markup Language)を採用し，マンマシンにブラウザ等の表現能力の高いソフトウェアを採用することで，マンマシン開発コストを低減することを可能とした。

(3)　遠隔メンテナンスを支援するアプリケーションフレームワークの開発

上記XMLインタフェースを介して現地設置された機器を管理するデータベースの生成・削除，設定，及びプログラムの遠隔ダウンロードを可能とするアプリケーションフレームワークの開発により，メンテナンス費用削減を可能とした。

(4)　組み込み型コントローラの開発

上記解決策を搭載した組み込み型コントローラの開発により，省スペース化，24時間連続運転を可能とした。

4.3　インターネット対応遠隔監視コントローラ

図7にインターネット対応遠隔監視システムを，また，開発した組み込み型インターネット対応コントローラOpenDuetの概要を**図8**に，仕様を**表1**に示す。OpenDuetは，サーバ機能とコントローラ機能を持ち，インターネットを介して設備機器の遠隔管理を可能とする。また，32ビットマイコン(M32R/E)，ROM16Mバイト，RAM 24Mバイトという非常にシンプルな構成をとっている。

4.4　適用製品

(1)　集中コントローラG-50

ビル用マルチエアコンの集中コントローラにインターネット対応としブラウザを用いた空調機の操作・監視を可能とした(**図9**)。

(2)　省エネルギーモニタ(実証試験用開発品)

この技術を適用したホームコントローラを試作した。家庭内機器の遠隔監視と，省エネルギーアプリケーションの遠隔からの入れ替えを実現した(**図10**)。

5.　むすび

ビル設備システムネットワークのオープン化に対応するビル設備システムコントローラと基本技術を開発した。本稿で紹介した各種コントローラは汎用性が高く，ビル・店舗からホームユースまで，幅広く適用可能である。

参考文献

(1)　東芝セミコンダクター社：ニューロンチップTMPN 3150／3120，東芝セミコンダクター社 (1999)

(2)　電気設備学会：BACnet™ ビルディングオートメーション用データ通信プロトコル，電気設備学会 (2000)

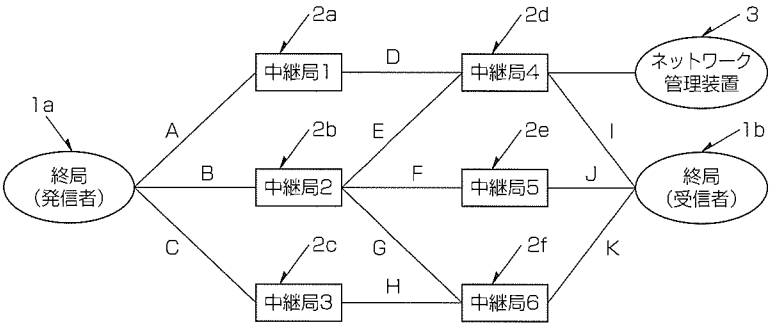
ネットワーク・ルーティングシステム　特許第3435885号(特開平8-265436)

発明者　河上　浩

この発明は，ネットワークにおける経路選択を行うルーティングシステムに関するものであり，特に通過忌避する中継局又は通過忌避するドメインを転送経路を選択する際の前提条件としたルーティングシステムに関するものである。

従来のネットワーク・ルーティングシステムでは，メッセージの機密保護や信頼性の事由で通過を忌避したい中継局又はドメインがあっても，メッセージ発信者がそれを避ける経路を明示することができなかった。

この発明では，①発信局は，通過忌避中継局又は通過忌避ドメインがメッセージの所定の箇所に記述されている場合は，通過忌避中継局と通過忌避ドメインを通過しない経路を抽出し，転送経路が存在すればその中から個々のルーティングシステムに依存した選択手段により転送経路を決定し転送経路に沿った隣接局に送信する。②中継局でも同様に，通過忌避中継局又は通過忌避ドメインが受信メッセージの所定の箇所に記述されている場合は，通過忌避中継局と通過忌避ドメインを通過しない経路を抽出し，転送経路が存在すればその中から個々のルーティングシステムに依存した選択手段により転送経路を決定し転送経路に沿った隣接局に送信する。この方式を採用することにより，発信者が通過忌避したい中継局又はドメインを指定することが可能となり，メッセージの機密保護に有効となる。



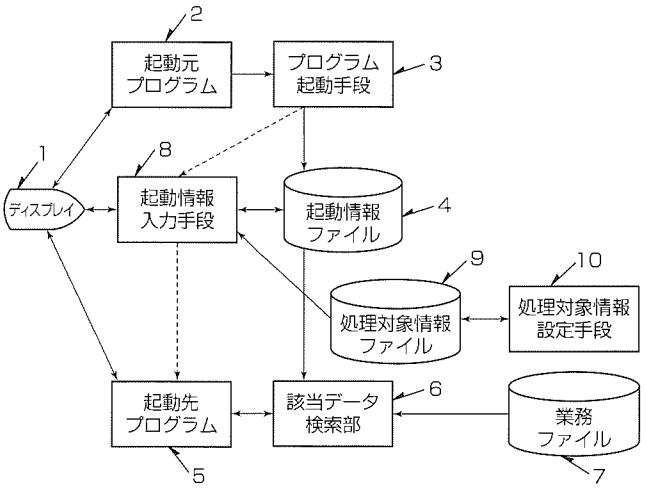
プログラム起動方式　特許第3386300号(特開平9-152962)

発明者　工藤　司，児島直人，秋間孝道

この発明は，１つのシステムにおいて処理の対象となるデータが１つであり，処理の対象となるデータに対して複数のプログラムを起動するプログラム起動方式に関するものである。

従来のプログラム起動方式では，例えば，自治体における住民情報システムのオンライン処理のように，同一の住民に対して所得証明発行・納税証明発行・住民票発行・印鑑登録証明発行等の複数の画面機能を切り換えながら処理を行う場合，プログラムを起動するたびに，処理の対象を特定するための項目である処理対象項目とその値をユーザーが指定しなければならなかった。

この発明では，あるプログラムから他のプログラムを起動するときに，起動先プログラム(5)における処理対象項目の値を特定できる情報が，処理対象情報ファイル(9)及び起動情報ファイル(4)から起動情報入力手段(8)に渡されているか否かを起動情報入力手段(8)は判別し，渡されていない場合に，起動先プログラム(5)で必要とする情報を入力させる。これにより，起動元プログラム(2)側で自動的に起動元プログラム(2)と同じユーザーに対して処理を行うことができ，ユーザーに指定誤りによる処理の無駄，漏れを防ぐことができる。



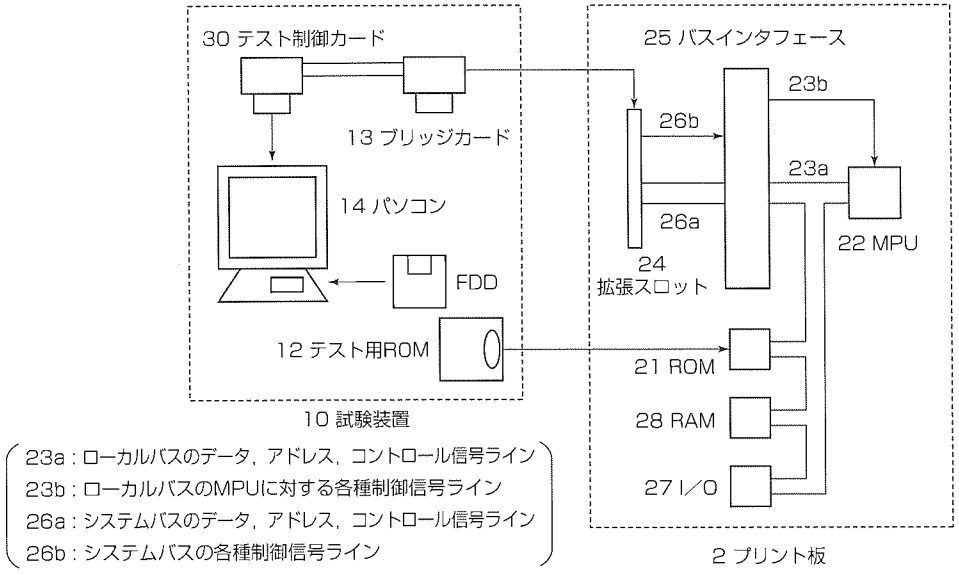
MPU搭載プリント板用試験装置　特許第3220018号(特開平10-55287)

発明者　潘　少賢

この発明は，マイクロプロセッサ(MPU)を搭載したプリント板の拡張スロットに接続してプリント板に搭載された構成全体の試験を行い，障害が発生したときにはその障害発生箇所を特定するMPU搭載プリント板用試験装置に関するものである。

従来の試験装置は，MPUを取り外し，そこにデバッグツールを接続して試験を行い，障害箇所を特定する方法であり，MPU自身及び拡張スロットやMPU制御部分を含めたMPU制御やMPUを取り外すことができないタイプのプリント板に対しては試験を行うことができなかった。

この発明では，プリント板(2)に装着するテスト用ROM(12)と，テスト制御プログラムを実行することでプリント板の試験の実行を行うパソコン(14)と，プリント板の拡張スロット(24)に接続するブリッジカード(13)及びパソコンの入出力I／Oカードであるテスト制御カード(30)とを持ち，テスト制御カードは，制御信号ライン(23b)，(26b)を操作してMPU(22)にテストプログラムを1BUSサイクルずつ実行させ，障害発生時に各バス信号ラインの状態を保持し，その障害箇所の内容を表示させることができる。



〈次号予定〉三菱電機技報 Vol.78 No.5 特集「最新の映像技術と社会インフラシステムへの応用」

三菱電機技報　78巻4号　2004年4月22日　印刷
(無断転載・複製を禁ず)　2004年4月25日　発行
編集人　三嶋吉一
発行人　松本敬之
発行所　三菱電機エンジニアリング株式会社　e-ソリューション&サービス事業部
〒102-0073　東京都千代田区九段北一丁目13番5号
日本地所第一ビル　電話(03)3288局1847
印刷所　株式会社　三菱電機ドキュメンテクス
発売元　株式会社　オーム社
〒101-0054　東京都千代田区神田錦町三丁目1番地
電話(03)3233局0641
定価　1部735円(本体700円)　送料別

URL　http://www.MitsubishiElectric.co.jp/giho/
三菱電機技報に関するお問い合わせ先　cep.giho@ml.hq.melco.co.jp

スポットライト

IT資産管理システム“ASSETnavi（アセットナビ）”

企業内のコンピュータやソフトウェアの急増に伴い，IT資産の正確な把握，ソフトウェア・ライセンスの遵守，システムのセキュリティ対策，IT投資の有効活用が重要な課題となっています。それにつれて，システム管理者やライセンス管理者の負荷は増大しています。

“ASSETnavi(注1)”は，そのような管理負荷を軽減するためのシステムです。ASSETnaviが提供するIT資産管理は，面倒なライセンス管理業務からの解放と，全社レベルでのTCO削減を実現します。ASSETnaviを導入することにより，社内のIT資産を人事情報やライセンス情報と結び付けて検索／集計できるようになります。

ASSETnaviは，Java(注2)ベース・WebベースのIT資産管理システムです。資産管理に必要な情報を必要なときにだれもが分かりやすいインタフェースで提供しますので，Webブラウザさえあれば，社内のどこからでもIT資産情報・人事情報・ライセンス情報などを簡単に検索／集計できます。

社員一人一人がコンピュータの配置状況，情報やライセンスの過不足を把握することにより，社内のIT資産を適材適所に配置できます。また，企業イメージの低下につながるライセンス違反を防止でき，管理コストの削減などを実現できます。

ASSETnaviは，クオリティ㈱のQNDPlus(注3)と連携します。QNDPlusで収集された膨大なデータを取り込み，必要な情報のみを検索／集計できます。

ASSETnaviは，ミドルウェアとして当社製のWebDBを使用しています。WebDBは，Webブラウザからデータベースを検索／更新／集計するためのJavaアプリケーションです。データベースを検索／更新／集計するための設定や画面デザインなどは，WebDBのメンテナンス機能を使用して自由に変更できます。WebDBを使用すれば，プログラミング言語の知識を持たない人でも，低コストで既存のシステムにデータベースを検索／更新／集計する機能を追加できます。

■機能

(1) データインポート機能

QNDPlusのデータ，人事情報などを取り込み，加工します。

(2) ログイン機能

(3) 検索／集計機能

データインポート機能で取り込んだデータを基に，ハードウェア，ソフトウェア，ライセンス情報などの検索／集計を行います。人事情報・組織情報と関連付けての表示が可能です。

(4) ライセンスメンテナンス機能

OSとソフトウェアのライセンス情報をメンテナンスします。

(5) マスタメンテナンス機能

社員マスタ・部門マスタなどをメンテナンスします。

(6) QNDデータ参照機能

QNDPlusの生データを検索します。

(7) ASSETnavi管理機能

(8) ASSETnavi保守機能

■ASSETnaviのデータの流れと画面

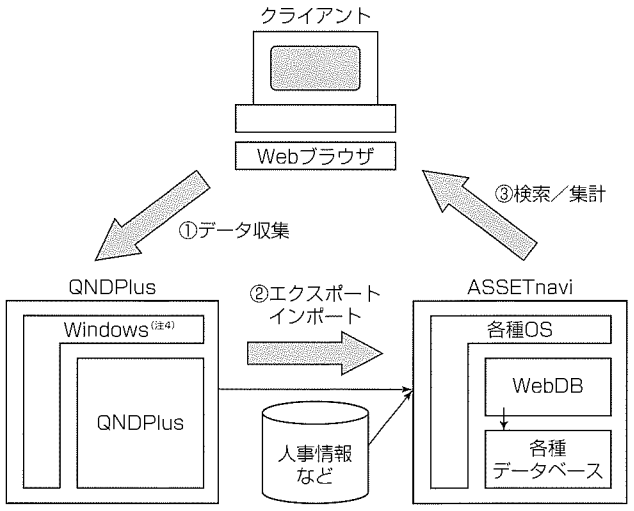


図1．データの流れ

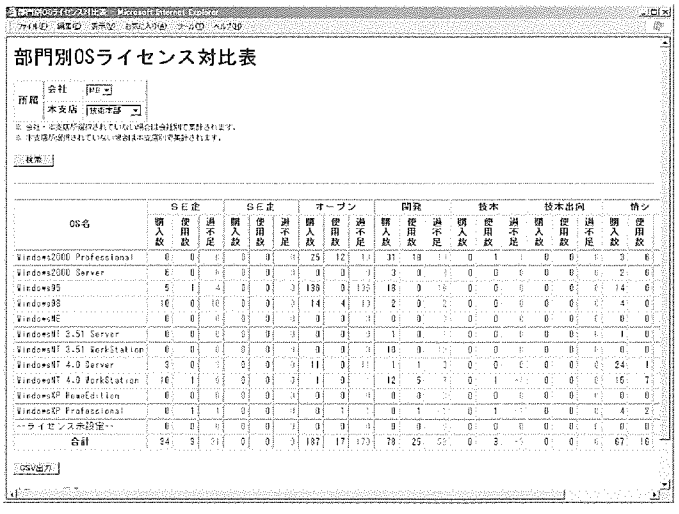


図2．部門別OSライセンスの購入数／使用数の対比画面

(注1) ASSETnaviは，㈱三菱電機ビジネスシステムの登録商標です。
(注2) Javaは，米国及びその他の各国におけるSun Microsystems, Inc. の商標又は登録商標です。
(注3) QND，QNDPlusは，クオリティ㈱の登録商標及び製品です。
(注4) Windowsは，米国Microsoft Corp.の米国及びその他の国の登録商標です。

住　所：〒169-0075 東京都新宿区高田馬場4-9-12
会社名：株式会社三菱電機ビジネスシステム　お問い合わせ先：IT事業部　古川　TEL 03-5389-4301