

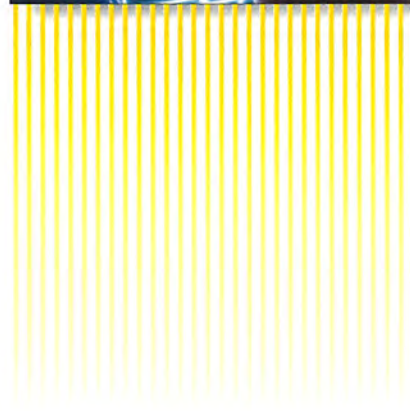
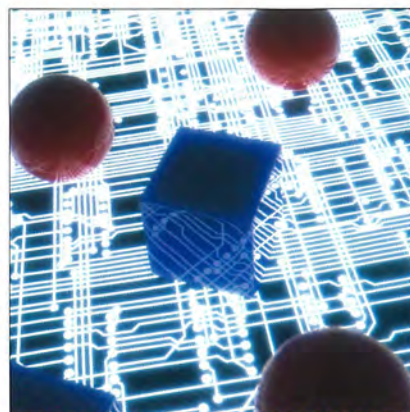
MITSUBISHI

三菱電機技報 Vol.82 No.7

2008

7

特集「企業・社会の発展を支えるITソリューション」



目次

特集「企業・社会の発展を支えるITソリューション」

- Do It Yourself IT 1
Haim Mendelson
- インフォメーションシステム事業のねらいと展望 4
伏見信也・中川路哲男
- ネットワークオペレーション業務を効率化する
運用監視ナビゲーションシステム 9
松下年伸・木村俊之
- ネットワーク運用管理サービスの高度化を実現する
企業向けポータルサイトシステム 13
増田裕紀・本部祐史
- EDIサービスシステムの高信頼化 17
吉田 稔・秦野克彦・松浦陽亮
- 紙文書の不正持ち出しをブロックする
“文書持ち出し監視／ドキュメント棚卸システム” 23
虎渡昌史・村上耕平・末沢康弘・伊藤俊之
- “ネカ録”最新シリーズによる遠隔・集中監視ソリューション 27
西村達夫・内村誠之
- “DIGUARD NET” 対応統合ID管理サーバを用いた
情報システム・入退室管理システム連携ソリューション 31
近藤誠一・堀 辰也・池田健一郎・伊藤英明
- 保健医療福祉分野の情報化を安全と標準で支える
ヘルスケアPKI対応ICカードミドルウェア 35
齋藤和美・米田 健・茗原秀幸・角野章之
- 1000万件のメールを1秒で検索する“LogAuditor Mail Saver” 39
大塚哲史・石川雅朗・加藤 守
- パソコンからの情報漏洩を防止する“CRYPTOFILE PLUS for Vista” 43
小田切信一
- 三菱電機オフィシャルウェブサイトを支える
企業ウェブサイト構築・運用ソリューション 47
磯西徹明・鈴木靖宏・大矢富保・安齋利典・柏谷俊彦
- システム構築のためのプラットフォーム活用標準“MIWESTA/PF” 51
朝倉耕一・村田謙一・花崎芳彦・松浦陽平・原田雅史
- 生花市場におけるせり総合システム市場くんシリーズ
“生花卸売システム” 55
野上泰弘・小池信成

IT Solutions for the Progress of Enterprises and Society

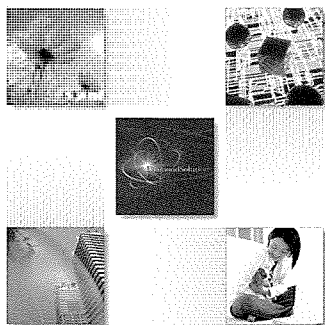
- Do It Yourself IT
Haim Mendelson
- Scope and Vision of Mitsubishi Electric Group's Information Systems and Network Services
Shinya Fushimi, Tetsuo Nakakawaji
- Navigation System for Improving the Efficiency of Network Monitoring and Operation
Toshinobu Matsushita, Toshiyuki Kimura
- Portal Site System for Enterprise that Achieves Upgrade of Network Management Service
Yuuki Masuda, Yuuji Honbu
- Progress of EDI Service System Reliability
Minoru Yoshida, Katsuhiko Hatano, Yosuke Matsuura
- Confidential Paper Documents Management System
Masashi Torato, Kohei Murakami, Yasuhiro Suezawa, Toshiyuki Ito
- Remote and Centralized Surveillance Solutions with “NECAROKU” New Series
Tatsuo Nishimura, Seishi Uchimura
- Information Systems and Physical Access Control Systems Integrated Solution Using ID Management Server with “DIGUARD NET”
Seiichi Kondo, Tatsuya Hori, Kenichiro Ikeda, Hideaki Ito
- Smart Card Middleware for Healthcare PKI
Kazumi Saito, Takeshi Yoneda, Hideyuki Miyohara, Akiyuki Sumino
- “LogAuditor Mail Saver” : Email Archive Solution with High-Speed Search up to 10 Million Emails per Second
Tetsufumi Otsuka, Masaaki Ishikawa, Mamoru Kato
- “CRYPTOFILE PLUS for Vista” : Provides File and Whole Disk Encryption Features
Shinichi Odagiri
- Corporate Web Site Solution
Tetsuaki Isonishi, Yasuhiro Suzuki, Tomiyasu Oya, Toshinori Anzai, Toshihiko Kasuya
- Platform Infrastructure Standard “MIWESTA/PF” for System Development
Kouichi Asakura, Kenichi Murata, Yoshihiko Hanazaki, Yohei Matsuura, Masafumi Harada
- “Flower Wholesale Trade System” of ICHIBAKUN Series
Yasuhiro Nogami, Nobushige Koike

特許と新案

- 「オペレータ業務支援システム」「呼制御データ検索
システム及び呼制御データ検索プログラム」 59
- 「携帯端末装置用プロテクタ」 60

スポットライト

データ交換プラットフォーム“BizOrder”



表紙：企業・社会の発展を支えるITソリューション

三菱電機は、「快適・安心・発展 “DiamondSolution”」をスローガンに、効率的な企業経営や暮らしやすい社会の実現を目指して、顧客に信頼されるITソリューションを提供している。

表紙では、DiamondSolutionのロゴを中央に配置し、ITが進歩することによって人々に与える快適さ・安心感を爽やかな花と女性に抱かれた犬で表現し、ITソリューションによって支えられている企業・社会の発展をIT網や高くそびえるビルなどのイメージで表現した。

Do It Yourself IT

Do It YourselfのIT



Haim Mendelson

Traditional implementations of Information Technology (IT) in the enterprise follow a structured top-down process. The reason is clear: since IT is the digital nervous system of the organization, its implementation requires careful analysis and design so it will be aligned with the organization's business strategy and process flows and so it will satisfy a host of functional and technical requirements. Buying cycles for enterprise IT products are notoriously long, expensive and complex, and are often followed by a painful and highly uncertain implementation process that consumes vast time and human resources.

Compare that to consumer Information Technologies, which are often adopted on a whim. While consumers may consider functionality and price (especially for high-ticket items), and some engage in extensive product research, the consumer buying process is certainly faster and more straightforward than business procurement. The most common implementations of new consumer IT are "Do It Yourself" (or, as we say in the United States, "DIY"), which means that products are either "ready to go" or they will remain unused. To bypass the painful implementation process, which is unacceptable for consumers, usability is key in the consumer world. The product has to be designed for usability and value, but once it proves its value, it may be adopted like wildfire. Apple's iPod/iTunes system is a good example: Buy the device, plug it in, download self-installing software – and you are ready to go. The system is sophisticated and complex, but the complexity is hidden behind the device and the user interface, so it's simple and easy to use from a consumer's point of view. And if you need assistance before or after you buy an iPod, you can get free help from a knowledgeable and pleasant "genius" at the Genius Bar in an Apple store near you. The results? Apple sold more than 50 million iPods in the past twelve months, more than four times the average number of Walkman units sold by Sony in its hey years.

This is not to say that the successful adoption of consumer IT is guaranteed. To the contrary: Many consumer products from the Apple Newton to Web TV have been flops. The failure rate of new consumer technologies is high because of fickle consumer tastes, the high threshold of usability consumers insist on, and their price sensitivity. But when it does take off, consumer IT

can quickly go through multiple design iterations. This means that a "cool" device like the iPhone – which opened up an entirely new market for Apple – could become ubiquitous in just a few months. In contrast, enterprises are naturally risk averse when their IT infrastructure is concerned and they insist on a low failure rate even if this leads to slower adoption – and a higher price. And because consumer IT tends to move at a faster "clockspeed"¹ than enterprise IT, it can serve as a test lab for the enterprise IT market.

Indeed, we are at the beginning of a cycle where enterprises adopt new technologies and business models that were originally developed for the consumer market, rather than for the enterprise IT market. Enterprise employees are also consumers, and their experience with consumer IT raises the bar for enterprise IT. As a result, enterprise IT is expected to change the way it delivers information to match the capabilities of new consumer technologies. And, once consumers get used to a new technology, they start pressuring their IT organizations, and through them – the vendors of enterprise IT, to bring it to the enterprise: "Why can't search on our Intranet be as easy as a Google search?" Gradually, consumer devices, entertainment and consumer service applications start influencing the way enterprise applications, information and content are developed and delivered. A good example of this trend is the adoption of Web 2.0 technologies, based on an "architecture of participation," in the enterprise. Blogs, wikis, RSS, tagging, prediction markets and Web-based social networks have been designed for the consumer market but are increasingly used in the enterprise. Knowledge workers are already bringing DIY IT to their organizations, putting together their own Web-based information feeds, publishing, personal productivity and collaboration tools without the assistance of IT personnel. The adoption of these technologies is driven by people's desire to socialize and interact, and these individuals are pushing their IT organizations to invest in tools that will facilitate further collaboration. Indeed, about 15% of employees surveyed by Forrester Research in 2007 used Web 2.0 tools for a business purpose, and their adoption increased to between a quarter and a third of employees at enterpris-

¹ See, H. Mendelson and J. Ziegler, *Survival of The Smartest*, Wiley, 1999.

es that had invested in Web 2.0 technologies. Interestingly, even within enterprises that were not considering an IT investment in Web 2.0 tools, three to eight percent of employees were nevertheless using them in pure “DIY” mode.

The growing desire and ability of individual employees to influence the use of IT in the enterprise challenge the traditional role of the IT organization, which can be both a blessing and a curse. As Tom Tabor, CIO of health insurer Highmark put it, “The good news is, we have choices. The bad news is, we have choices.”² The challenge is to put in place procedures and policies that enable the organization to support at the same time both “industrial strength,” structured and controlled IT, and DIY IT. At Highmark, employees often suggest new consumer technologies, but these technologies are required to go through a formal evaluation process by the IT

2 “Employees often use unauthorized technologies at work. Does that compromise security? Or enhance productivity? Two experts debate the issue.” The Wall Street Journal, October 22, 2007.

organization. Google, in contrast, believes in an almost pure DIY model: Employees are free to choose and download productivity and collaboration software by themselves and to just use it. While this does not apply, of course, to Google’s ERP system, Google believes that the adoption of consumer IT will help employees be more productive and reduce the company’s spending on enterprise IT.

In fact, the digital nervous system of an effective organization consists of both a highly-structured, process-driven backbone, and a horizontal, people-driven network that enables collaboration and knowledge-sharing.³ The modern IT organization has to support both. This means that it has to extend its traditional structure so it can function as well like an Apple store, helping employees to sort out the myriad options available to them, guiding them to the proper choice, helping to reduce the costs of installing DIY IT, and providing user-friendly assistance when things fall apart.

3 See Mendelson and Ziegler, Ibid.

《和訳》

これまでの企業のITシステムは、統制化されたアプローチによってトップダウンに構築されてきた。その理由は明快である。企業のITシステムは企業のデジタル神経網としての役割を担うので、その構造や運用は企業のビジネス戦略や独自のビジネスプロセスに整合しなければならず、そこから導かれる多くの機能要件・技術要件を満たすことが必要だからである。このため、その要件分析や設計には細心の注意が必要となり、結果として企業のIT製品購入のプロセスは恐ろしく時間がかかり、複雑で、費用がかさむものとなってきた。また、製品購入後のシステム構築においても、往々にしてトラブルが発生し、稼働までの見通しは不透明となり、膨大な時間と人的資源を浪費してしまうことも多い。

これを個人向けのIT製品と比べてみよう。元来、個人は思いつきで製品を購入するものである。もちろん、時間をかけて製品の機能や価格を比較してどれを買うか決めることもあるが(特に製品が高額の場合)、そのIT製品購入のプロセスは企業のIT製品購入プロセスに比べて明らかに速い直接的である。特に、個人向けIT製品は“Do It Yourself”(米国では“DIY”と省略される。)が可能な製品でなければならない。つまり、個人向けのIT製品は、買った人が自分ですぐに使える(ready to go)ものでなければならない、またそうでなければ永遠に使われないままで終わると言ってよい。買った製品を使って“システム構築”をすることなど、個人にとっては到底許容し難いからである。したがって、“買ってすぐに使える”という性質は個人向け製品市場においては不可欠な事項であり、個人向けのIT

製品は、その使い勝手とユーザーの利用価値を最優先事項として設計される。一方で、個人向け市場では、一旦製品の評価が定まると山火事の火のごときスピードで市場を席卷する。Apple社のiPodやiTunesはその良い例である。iPodを買ってこれをパソコンにつなぐと、ソフトウェアがダウンロードされ自動的にインストールされる。これでもう製品が使えるようになる。製品は洗練されているがそのソフトウェアは複雑そのものである。しかし、その複雑さはシンプルなハードウェアとユーザーインターフェースで遮蔽(しゃへい)されており、個人のユーザーから見れば実にシンプルで使いやすい製品になっている。また何か分からないことが出てきても、Appleストアのジーニアスパーと呼ばれるコーナーに行けば、何でも知っている愛想の良いジーニアス(天才)がいて、無料で何でも教えてくれる。その結果はどうか? この1年間で実に5000万台以上のiPodが売れた。この数は、ソニーが最盛期に売ったウォークマンの数の4倍以上である。

もちろん、個人向けIT製品のビジネスが必ず成功するわけではない。逆に、同じApple社のNewtonやWebテレビなど、大失敗した個人向けIT製品は枚挙にいとまがない。個人消費者の嗜好(しこう)は気まぐれに変化する一方、使い勝手への要求度は高く、価格にも極めて敏感であり、結果として個人向けIT製品ビジネスの成功率は極めて低いのである。しかし、一旦製品の販売が軌道に乗り始めると、あとは同じ製品をどんどん生産するだけでよく、iPhoneのような“カッコいい”製品(この製品もApple社の新しいビジネス分野を開拓した)は数か月の短期間であま

ねく市場に普及した。一方、企業ユーザーはことITに関してはリスクを回避する傾向にあり、時間がかかり高くつくと分かっているにもかかわらず失敗のリスクが小さければそれを選ぶ。その結果、個人向けITは企業向けITよりも速い“クロック速度^(注1)”で進んでいくこととなる。すなわち、個人向けIT市場は企業向けIT市場のテスト市場とも言えるのである。

実際、企業情報システムの一部に、個人消費者向けに開発されたITの新技術やビジネスモデルを採用しようとする動きが始まりつつある。企業の従業員は同時に個人消費者でもあり個人向けITの良さを経験し熟知している。この経験が企業ITと個人向けITの垣根を取り払い、企業の情報システムが個人向けの新IT技術を取り入れた形に変わってくる、との期待が生まれてきたのである。事実、従業員が一旦個人向けITに慣れてしまうと、その技術を自分の勤務先企業のITシステムに採用するように、自社のITシステム部門、さらにはその先の企業向けITベンダーに要求するようになってくる。例えば、「どうして社内の情報をGoogleのように簡単に検索できないのか？」といったような要求が生まれてくるのである。このようにして、個人消費者向けのハードウェア製品、娯楽製品、サービス等が企業情報システムのアプリケーションやコンテンツの開発に影響を及ぼし始めた。このトレンドの良い例が“参加型アーキテクチャ”によるWeb2.0の企業内の採用である。ブログ、Wiki、RSS、タグ付け、予測マーケット、Webベースのソーシャルネットワーク等、個人消費者市場向けに開発されてきた技術や製品・サービスが、今、企業の内部で採用されつつある。特に、知識労働者と呼ばれる人たちが、情報システム部門の助けなしにこれらの新技術を職場に持ち込んで“DIY”し、Webベースの情報発信や情報管理ツール、コラボレーションツールとして使い始めている。これは、社内のコミュニティ作りや従業員相互の情報交換への欲求が現場から生じてきたと言え、その結果、従業員は更なる本格的なコラボレーションの環境づくりを情報システム部門に要求するようになってきているのである。事実、Forrester Research社の調査によると、2007年には従業員の15%が企業内でWeb2.0のツールを使用しており、Web2.0環境を本格的に構築した企業においてはこの数字は25%から33%と更に大きい。面白いことに、Web2.0の

(注1) H. Mendelson and J. Ziegler, *Survival of The Smartest*, Wiley, 1999.を参照

社内環境整備には興味がないと答えた企業においても3%から8%の従業員がDIYによって(すなわち自分たちが勝手に)これらのツールを使っていると答えていることである。

従業員個人から企業情報システムへの新しい要求がボトムアップに発生し、またその影響力が増大した結果、情報システム部門にとっては有利不利両面の問題が生じている。医療保険会社のHighmark社のCIOであるTom Tabor氏が言うように「良い知らせは、新しいやり方ができたということ。悪い知らせは、新しいやり方ができてしまったということ」^(注2)である。問題は、「業界での競争力」としての構造化され統制されたITと、DIY型のIT双方を同時に社内を実現することである。Highmark社では、従業員が個人向けITを社内を利用したいと要求したとしても、情報システム部門がその採用を審査することになっている。Googleは逆で、ほぼ完全なDIYモデルを採用している。すなわち、従業員は何の制約もなく自由に生産性向上のツールやコラボレーションソフトウェア等をインターネットからダウンロードし、利用することが許されている。もちろん、GoogleのERPシステムはこのようなやり方の対象にはなっていないが、Googleでは個人向けITの採用によって従業員の生産性は向上し、全体として企業の情報システムへの投資額は減少すると考えられているのである。

実際、効率のよい企業の組織をつぶさに分析してみると、そのデジタル神経網は高度に構造化されたビジネスプロセス駆動型の基幹バックボーンと、共同作業や知識の共有化を行うための水平型、人間駆動型のネットワークから構成されていることが分かる^(注3)。現代の情報システム部門はこの両方を実現しなければならないのである。これが意味するところとは、企業の情報システム部門は従来の業務領域を拡大し、Appleストアのような役割を果たす必要があるということになる。すなわち、情報システム部門は、従業員に対していろいろなITを紹介し、どれを使えば良いのかの判断を助け、DIYのITをインストールする際にアドバイスし、何かことがあった際にも温かく支援の手を差し伸べることがその仕事となってくるのである。

(注2) “Employees often use unauthorized technologies at work. Does that compromise security? Or enhance productivity? Two experts debate the issue.” *The Wall Street Journal*, October 22, 2007.を参照

(注3) (注1)の文献を参照

インフォメーションシステム事業の ねらいと展望



伏見信也*



中川路哲男**

Scope and Vision of Mitsubishi Electric Group's Information Systems and Network Services

Shinya Fushimi, Tetsuo Nakakawaji

要 旨

三菱電機は、「快適・安心・発展 “DiamondSolution^(注1)”」をスローガンに掲げて、製品やサービスを提供している⁽¹⁾⁽²⁾⁽³⁾。

快適・安心・発展は、ITの活用面からの次の3つの取り組みに対応している。

- 快適 ↔ Realtime Management
- 安心 ↔ Risk Management
- 発展 ↔ Resource Management

(1) Realtime Management

ITを用いて、処理の即時化を進め、現在の業務状況を明らかにして経営の見える化を行うことによって、業務の効率化を図るための取り組み

(2) Risk Management

ITを用いて、セキュリティ事故、品質問題、コンプライアンス違反、災害などの事業上のリスクを識別し、適切な対応を図るための取り組み

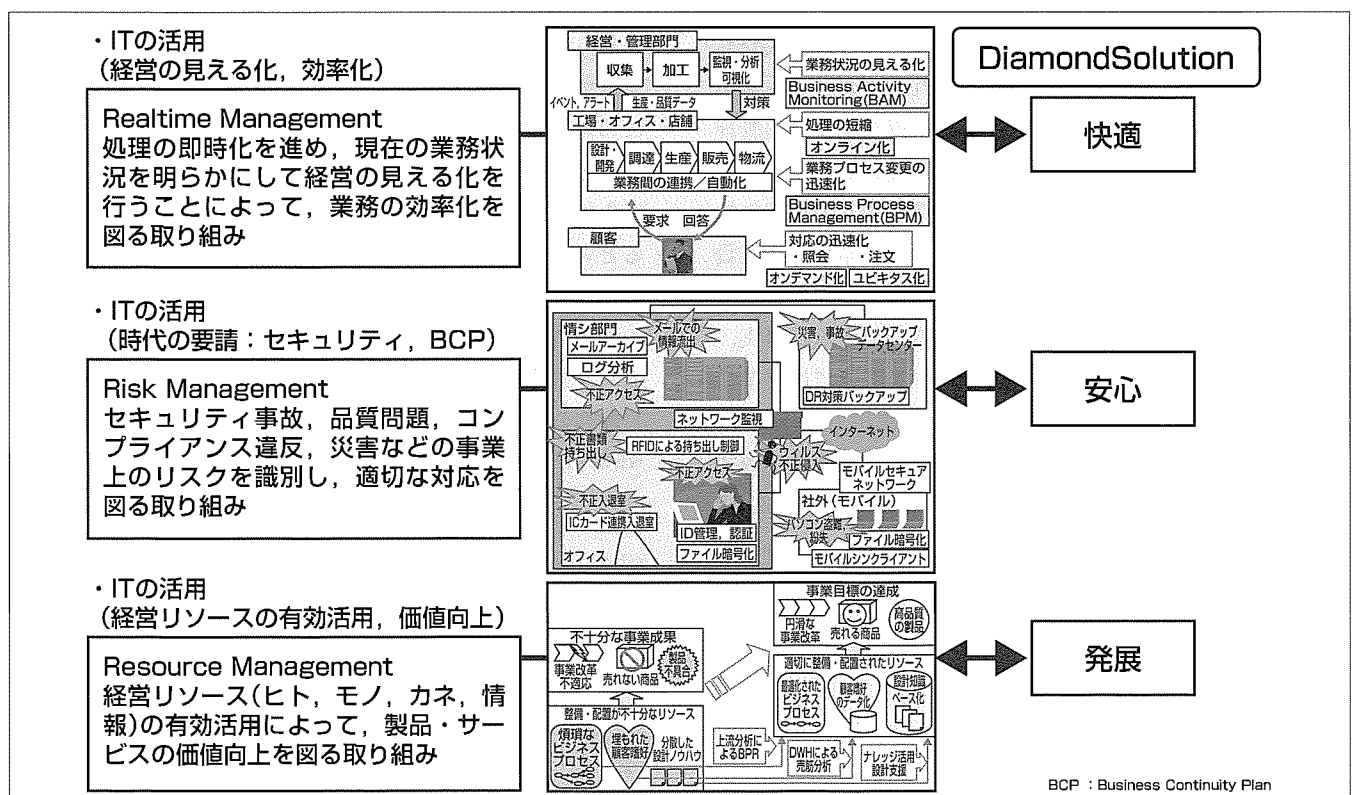
(注1) DiamondSolutionは、三菱電機株の登録商標である。

(3) Resource Management

ITを用いて、経営リソース(ヒト、モノ、カネ、情報)を有効活用することによって、製品・サービスの価値向上を図るための取り組み

これらの取り組みの具体例として、本特集号で紹介されている、リアルタイムの情報提供を可能とするネットワーク運用管理ポータルサイト、紙文書漏洩(ろうえい)リスクに対応した文書持ち出し監視システム、コンテンツをリソースとして活用する企業ウェブサイト構築・運用ソリューションがある。

将来に向けた上記3つのIT活用の取り組みとして、製造業での更なるデータの活用と連携、当社が2007年に発表したトータルセキュリティソリューション“DIGUARD(ディガード)⁽⁴⁾”の強化、グリーンITのための技術強化などがある。



快適・安心・発展の3つの技術面の取り組み

DiamondSolutionで掲げる“快適”“安心”“発展”は、それぞれ、ITの活用面からの3つの取り組み、Realtime Management, Risk Management, Resource Managementに対応している。

1. ま え が き

当社は、“快適・安心・発展を支えるITシステムの顧客との共創”を目指すDiamondSolutionをスローガンに、技術の強化を図ってきた。本稿では“快適”“安心”“発展”で意図している技術的な取り組みについて述べるとともに、それらの取り組みがどのように具体化しているかを、本特集号に掲載している製品／ソリューション／システムを中心に概観する。また、更なる発展に向けた技術強化の取り組みについても述べる。

2. 企業経営におけるIT活用

㈩日本情報システム・ユーザー協会(JUAS)が発表している“企業IT動向調査2008⁽⁵⁾”によれば、2007年度はIT予算を増加させた企業が61%であり、特に大企業でIT投資が加速されている。その背景にはIT活用の重要性の高まりがある。

IT活用には大きく3つの方向性がある。

第一の方向性は、オペレーションの効率化とそのための“見える化”に向けた適用である。その際のポイントは、いかにスピード感をもって、リアルタイムに状況対応ができるかである。業務自体を人手を介して数日かけて行うものから、要求が発生次第、ITを活用して自動的に処理が進むように変えるとともに、必要な情報がリアルタイムでレポートされ、経営に資することが求められる。

第二の方向性は、企業が抱える様々なリスクへの対策をとるための適用である。セキュリティ事故、品質問題、コンプライアンス違反に対する社会の目はより厳しくなっており、これらのリスクに適切に対応できないと、企業の存続を脅かす問題になりかねない。また、災害などの不測の事態に対して事業継続できる仕組みを準備することも重要性を増している。

第三の方向性は、企業の持つ強みを強化するための適用である。各企業は自分たちの保有する固有の経営リソース(差別化技術、業務ノウハウ、先端設備、人材など)を最大限に生かして強みを強化していくことが、持続的な競争優位を保つ上で重要である。保有するリソースを最大限に生かすために、ITを活用してビジネス・プロセスを見直したり、社員個人が暗黙知として保有する業務ノウハウを、形式知に変換し共有することが求められる。

3. 快適・安心・発展 “DiamondSolution”

3.1 DiamondSolutionのねらい

前述のIT活用の3つの方向性を、技術面からの次の3つの取り組みに整理する。

(1) Realtime Management

ITを用いて、処理の即時化を進め、現在の業務状況を

明らかにして経営の“見える化”を行うことによって、業務の効率化を図るための取り組み

(2) Risk Management

ITを用いて、セキュリティ事故、品質問題、コンプライアンス違反、災害などの事業上のリスクを識別し、適切な対応を図るための取り組み

(3) Resource Management

ITを用いて、経営リソース(ヒト、モノ、カネ、情報)を有効活用することによって、製品・サービスの価値向上を図るための取り組み

DiamondSolutionの掲げる“快適・安心・発展”は、これらの取り組みに対応している。すなわち、

● 快適 ↔ Realtime Management

● 安心 ↔ Risk Management

● 発展 ↔ Resource Management

である。

次に、これら3つの取り組みについて具体的に述べる。

3.2 Realtime Management：“快適”を支える技術

Realtime Managementの代表的な実現例としては、製造業におけるタテ(経営層から現場まで)とヨコ(顧客メーカー-サプライヤーを結ぶサプライ・チェーン/バリュー・チェーン)の両面での、リアルタイムな連携が挙げられる(図1)。

このリアルタイムな連携では、オンデマンド化(要求が発生する都度処理を起動)、ユビキタス化(どこからでも処理要求)などによって、ニーズの発生と処理実行のずれを減らす一方、BPM(Business Process Management)技術を活用して業務プロセスの変更を容易にし、また、BAM(Business Activity Monitoring)技術などによって、現在の業務状況や経営指標がその場で把握できる(“見える化”)。

本特集号におけるRealtime Managementの実現例として、“ネットワーク運用管理サービスの高度化を実現する企業向けポータルサイトシステム”がある(図2)。

三菱電機情報ネットワーク㈱(MIND)は、顧客ネットワークの運用管理サービスを行っており、このサービスにおける運用情報の提供は、従来は紙や電話での連絡が主であ

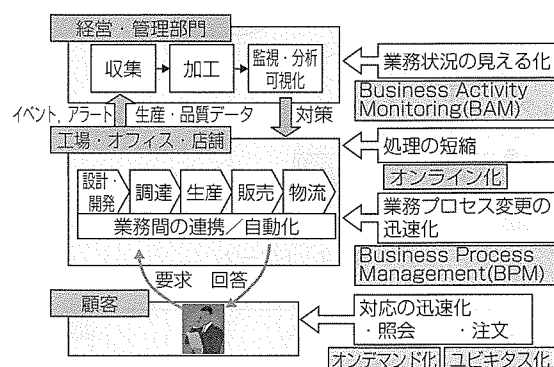


図1. Realtime Managementの実現例

図 2. Realtime Management を実現する運用ポータル

三菱電機技報・Vol.82・No.7・2008

3.4 Resource Management：“発展”を支える技術

Resource Managementの代表的な実現例としては、煩瑣(はんさ)なビジネス・プロセス、顧客嗜好(しこう)を内包したデータ、設計ノウハウなど、組織化されにくい情報を企業にとってのリソースととらえ、これらを活用するためのシステムが挙げられる(図5)。

このシステムでは、BPR(Business Process Reengineering)によってビジネス・プロセスを整理したり、DWH(Data WareHouse)を用いて顧客嗜好を分析したり、暗黙知である設計ノウハウを知識ベースを用いて形式知に変えたりする。

本特集号におけるResource Managementの実現例として、“三菱電機オフィシャルウェブサイトを支える企業ウェブサイト構築・運用ソリューション”がある。

このソリューションは、ウェブサイト構築のための素材である、コンテンツ、企業情報、社内のサービス、及びASP(Application Service Provider)が提供する社外のサービスをリソースとして、そのリソースを有効活用することで、企業価値向上に貢献する質の高い企業ウェブサイトの構築・運用を可能としている(図6)。

このシステムには、次のような機能が実現されている。

●Webコンテンツのワンソース・マルチユース化

コンテンツを一元的に管理し、コンテンツの新規作成、更新を容易にする。企業情報(会社概要、事業概要、製品情報等)のデータベースとコンテンツ管理システムとを連携させることによって、情報リソースを適切に管理し“ウェブ先行型の情報発信”を可能にする。

●ASPサービスのインテグレーション

顧客に利便性の高いインタフェース、ユーザビリティ、アクセシビリティを提供するためのサービス(キャプチャ画像付きサイト内検索など)が各種ASPで提供されている。これらのサービスも利用可能なリソースととらえ、既存のリソースとASPの提供するサービスをシームレスに連携することで、ユーザビリティ、アクセシビリティを一層向上させることができる。

これらの機能を用いて保有する情報リソースを最大限に活用し、またASPのサービスという外部のリソースも有

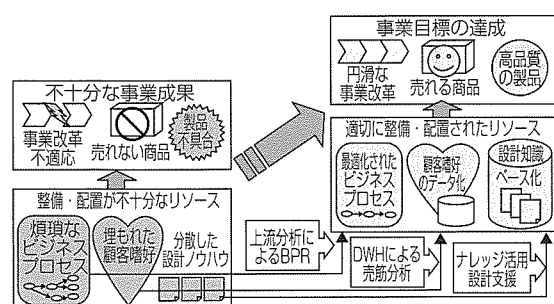


図5. Resource Management実現例

効活用して企業ウェブサイトを構築・運用することによって、企業価値向上＝“発展”が期待できる。

4. 将来に向けて

これまでに述べたDiamondSolutionを実現する3つの取り組みの将来に向けた方向性について述べる。

(1) 快適：Realtime Management

業務の見える化や、処理のオンデマンド化を図るべき範囲は、グローバル化や業務の合理化などの進展によって急速に広がっている。一方、現場の機器からは今でも大量に処理過程のデータが発生しているが、現状は一部のデータが集計・要約されるだけで、十分に活用されないままである。

今後は、より詳細なデータを、よりリアルタイムに連携させて業務にフィードバックすることが重要になってくると考えられる。

当社は、従来“DIAPRISM”に代表されるデータ分析技術やBAM技術で、大量の業務データを高速に分析して活用してきたが、Realtime Managementの拡大に向けて、SOA(Service-Oriented Architecture)やESB(Enterprise Service Bus)などの技術も活用し、更なる技術強化を図っていく。

(2) 安心：Risk Management

リスクのうちセキュリティについては、脅威の増加・多様化に伴って、あらゆる局面で対策が求められるようになっていく。その典型として、3.3節で、ID管理等の情報セキュリティと、ICタグや映像監視といった物理セキュリティの連携例を示した。

当社は、情報セキュリティと物理セキュリティが連携したトータルセキュリティシステムの構築に向け、独自の共通プロトコルによってシステム間の通信を実現するセキュリティ構築プラットフォーム“DIGUARD NET(ディガードネット)”を開発した。DIGUARD NETについては本特

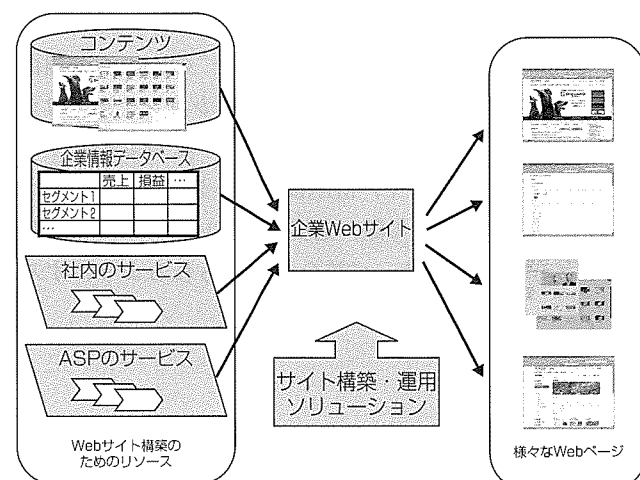


図6. Webサイト構築のためのリソースの活用

集号の“DIGUARD NET対応統合ID管理サーバを用いた情報システム・入退室管理システム連携ソリューション”で紹介している。

今後、トータルセキュリティのニーズは更に高まると想定されるため、DIGUARD NETを核として、セキュリティ技術を強化していく。

内部統制については、三菱電機インフォメーションシステムズ(株)(MDIS)が2006年から、“内部統制整備／評価支援ツール TOOLMASTER/IC”を提供しており、現在、当社を含む多数の企業で、内部統制報告制度の初年度の対応に向けて利用されている。今後、初年度対応で明確になった課題を解決するために、業務プロセスの見直しやIT全般統制の整備も含めた更なるニーズが高まると予想される。このため、内部統制整備／評価支援ツールだけでなく業務再構築の支援やITガバナンスの整備に向けた製品⁽⁶⁾、サービスを充実させていく。

“安心”に向けたもう一つの取り組みとして、社会のインフラである金融機関や交通機関等の大規模ミッションクリティカル・システムについて、着実な構築と安定的な運用に向けた技術強化を図っていく。具体的には、システム構築時の品質確保のための取り組み、障害の発生をすみやかに検知するシステム監視、障害が発生してもサービスを継続するためのシステムの冗長化技術、障害から短時間で確実に復旧するためのシステム回復技術などがある。この特集号では、MINDの“EDIサービスシステムの高信頼化”で、特にシステム監視について、その一端を紹介している。

(3) 発展：Resource Management

Resource Managementについては、最も基本的なリソースであるエネルギー使用量を低減するための、“グリーンIT”への取り組みが重要な課題となってきた。当社は、創立100周年の2021年を目標年とする、環境経営における長期ビジョン“環境ビジョン2021”を策定し推進しており、グリーンITへの取り組みもその一環として位置づけている。

グリーンITには、“IT機器・システムの省エネルギー”と、“ITを活用した社会の省エネルギー”の、2つの側面がある。我々は、三菱電機インフォメーションテクノロジー(株)(MDIT)のソリューション・サーバをはじめとするIT機器の省エネルギーや、MINDのデータセンターの省エネルギーを進める。この際、進展が著しいサーバの仮想化技術なども活用し、サーバ統合が進められるようにする。

同時に、工場やビルのエネルギー消費状況をITを活用して分析し、対応を図れるようにする。

なお、環境に関する情報を総合的に管理するために、従来MINDが、“環境統合情報システム(ECOrates)”を提供しており、今後とも法制度等にはすみやかに対応し、環境経営を支えていく。

リソースの活用のほかの観点として、企業・組織が自分たちのコア・コンピタンスに集中するために、社外のサービスを適切に利用することの必要性も高まっている。システム構築やサービス提供にあたっては、SaaS(Software as a Service)の活用も視野に入れ、最適な構成を追及していく。

5. む す び

本稿では、DiamondSolutionで掲げている“快適”“安心”“発展”と結びついた、3つの技術的な取り組み、Realtime Management, Risk Management, Resource Managementについて述べるとともに、それらの取り組みの具体的な実現について述べた。

今後も、更なる“快適”“安心”“発展”に向けて、技術強化を進めていく。

参 考 文 献

- (1) 高木正博，ほか：インフォメーションシステム事業のねらいと展望，三菱電機技報，**81**，No.7，436～440（2007）
- (2) 高木正博，ほか：インフォメーションシステム事業のねらいと展望，三菱電機技報，**80**，No.4，236～240（2006）
- (3) 下間芳樹，ほか：インフォメーションシステム事業のねらいと展望，三菱電機技報，**79**，No.4，236～240（2005）
- (4) 竹田昌弘，ほか：三菱電機トータルセキュリティソリューション“DIGUARD”，三菱電機技報，**82**，No.4，245～248（2008）
- (5) ㈱日本情報システム・ユーザー協会(JUAS)：第14回企業IT動向調査2008（2008）
<http://www.juas.or.jp/project/survey/it08/press-zu2008.pdf>
- (6) 近藤誠一，ほか：情報セキュリティガバナンスシステム，三菱電機技報，**82**，No.5，353～356（2008）

ネットワークオペレーション業務を効率化する 運用監視ナビゲーションシステム

松下年伸*
木村俊之**

Navigation System for Improving the Efficiency of Network Monitoring and Operation

Toshinobu Matsushita, Toshiyuki Kimura

要 旨

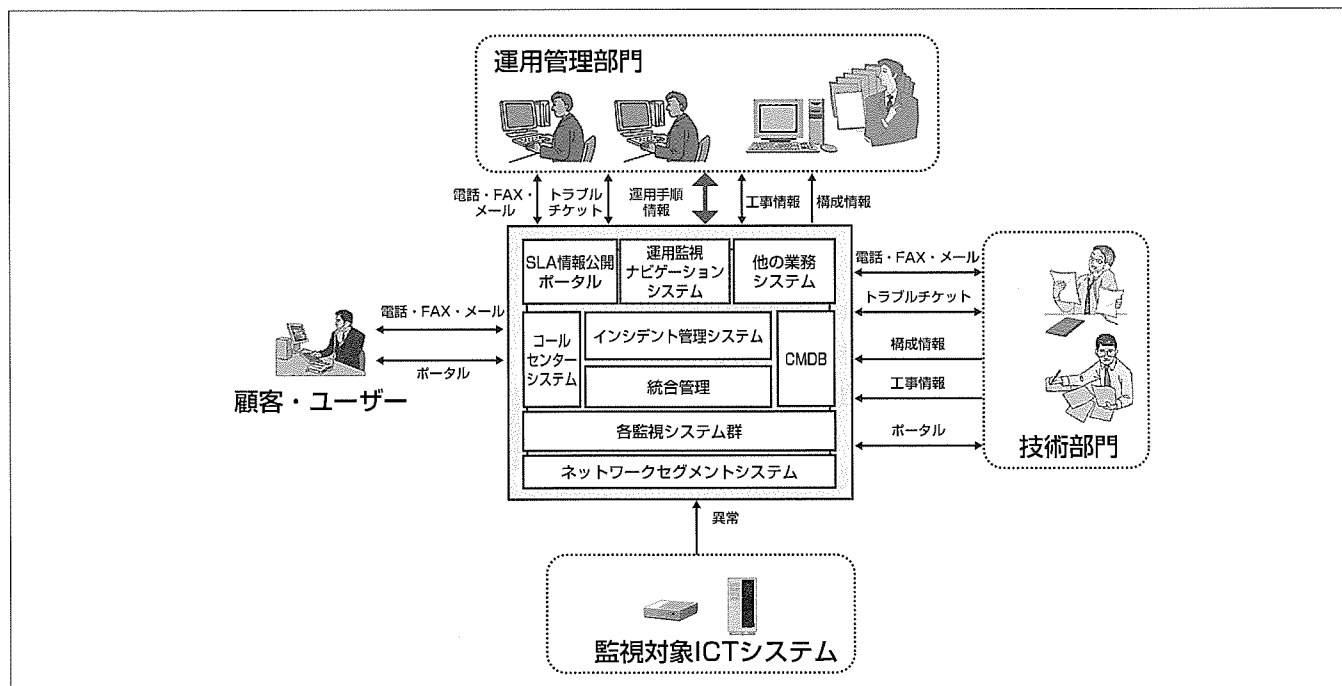
企業活動のICT (Information and Communication Technology) への依存度の高まりや規模の拡大に伴い、その基盤となるICTシステムの運用に対する要求は多様化し、高度で複雑なものとなっている。それに伴い運用管理業務自体にも監視システムやインシデント管理システム、資産管理システムなどの運用業務用システムが導入され効率化や可視化などが進んでいる。一方で、システム障害に対応する運用管理部門には、高度な専門知識や24時間365日の有人体制、複雑化した個々のユーザーニーズにこたえるための個別の運用規則などが不可欠となっている。そのため、専門技術者の不足や育成費用の増加、個人のスキル差によって生じるサービスレベルや作業負荷の不均衡化などの様々な課題を抱えている。

今回開発した運用監視ナビゲーションシステムは、ICTシステムの運用管理業務の中でも障害発生時の対応業務を対象に、多様化複雑化する業務規則や操作手順をシステム化し、業務フロー形式で作業過程をトレースしながら運用管理者に業務内容をナビゲートするシステムである。また、そのナビゲーションの過程で正確な作業記録を自動的に蓄

積する仕組みも兼ね備えている。システムの開発に当たっては、三菱電機㈱情報技術総合研究所が開発したプロトタイプを基に三菱電機インフォメーションシステムズ㈱ (MDIS) が製品開発を行った。

また、ファーストユーザーでの運用管理システムへの適用事例では、すでに導入されていたサービスデスクシステムやCMDB (Configuration Management Database) との連携機能の追加実装や現場の意見を基にした操作性の改善などの工夫を行った。

今回は運用管理業務の担当者へのナビゲーション機能を主とした開発であったが、今後は蓄積した作業履歴を利用した進捗 (しんちよく) 管理機能や対処時間の自動計測機能など、サービスレベルの維持や管理、検証に寄与する機能追加を検討する。これによって、コンピュータシステムの運用・管理業務に関する体系的なガイドラインであるITIL (Information Technology Infrastructure Library) の考え方を取り込み、運用管理業務の継続的な改善を実現するシステムを目指す。



運用管理業務用システム群における運用監視ナビゲーションシステムの適用イメージ

統合化された運用システムの1つのサブシステムとして、インシデント管理システムをはじめとする他のサブシステムと連携し、運用管理部門に対してインシデントの内容に応じた運用手順情報や操作手順、参考情報等の詳細な業務要領情報を提供する。

1. ま え が き

企業活動のICTへの依存度の高まりや規模の拡大に伴い、その基盤となるICTシステムの運用に対する要求は多様化し、高度で複雑なものとなっている。それに伴いシステム障害に対応する運用管理部門には、高度な専門知識や24時間365日の有人体制、複雑化した個々のユーザーニーズにこたえるための個別の運用規則などが不可欠で、専門技術者の不足や育成費用の増加、個人のスキル差によって生じるサービスレベルや作業負荷の不均衡化などの様々な課題を抱えている。

本稿では、実際の適用事例を交えて、ICTシステムを運用管理する現場が抱える課題や、運用監視ナビゲーションシステムの機能、適用事例における工夫点、今後の展開などについて述べる。

2. 運用管理の現場が抱える課題と開発の目的

2.1 個人スキルへの依存

ICTシステムの運用管理の業務は、顧客とのSLA (Service Level Agreement) 契約に基づき一定の障害対応レベルを維持する必要がある。そのためには、対応する担当者の技術レベルやノウハウも一定レベルを維持する必要があるが、マルチベンダー化やシステムの複雑化によって実際の現場での障害対応能力は、個人のスキルに依存する傾向が強くなってきており、作業負荷や作業品質に担当者による偏りが発生して業務品質の維持が困難になってきている。

2.2 人材育成の期間や費用の増大化

ICTシステムの運用管理部門では、前節で述べたような個人のスキルの差による問題を解消するために要員教育に注力しているが、その結果として教育期間の長期化や育成指導者の負荷増大化などの問題が生じている。また、24時間有人体制を実現する交代制のシフト勤務を強いられる特殊な職場で人員変動も多くなり、問題を一層顕著にしている。

2.3 開発の目的

運用監視ナビゲーションシステムの開発では、障害対応業務で個人に求めるスキルの低減や個人差の排除、教育期間の長期化や規定が遵守されない等の現場が抱える課題の解決を開発目的とした。その実現手段として、対応業務規則や操作手順をシステム化して業務フロー形式で運用管理者にナビゲートする機能や、ナビゲーションの過程で正確な作業履歴を自動的に蓄積する仕組みが必要と考えた。

3. 運用監視ナビゲーションシステムの機能

3.1 業務手順の自動選定表示機能

故障箇所や故障内容、顧客との契約内容によって異なる業務手順の選定を複数のキーワード(例えば故障機器のホ

スト名など)によって自動的にを行い、業務手順を業務フロー形式で表示する機能である(図1)。障害対応の初期段階での担当者による個人差の排除を実現する。

3.2 業務状況管理機能

業務フロー図が表示された画面をマウスでクリックするだけの簡易な操作で作業内容や作業時刻等の実績を入力できる仕組みと、業務フロー図の変色という視覚的表現によって業務状況を表示する機能である(図2)。

3.3 詳細情報表示機能

基本機能として、業務フロー図による業務手順のナビゲーションと合わせ、状況に応じた具体的な操作説明を文章でナビゲートする。さらに、操作上必要となる構成情報やマニュアルなどCMDBやファイルサーバ上の関連資料をリンク表示し様々なビューを起動する外部アプリケーションの起動機能やバッチファイルによる外部コマンド実行などの作業補助機能を備えている。

3.4 作業履歴記録機能

業務状況管理機能によって入力された作業実績を作業履歴としてサーバのデータベース上に長期保管するとともに、表示中のインシデント(顧客からの問い合わせや監視システムからの警報など)に関する作業履歴情報を画面に表示する。

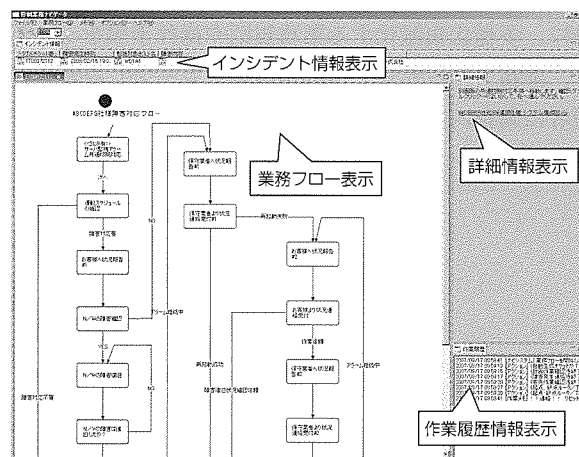


図1. クライアントの画面構成

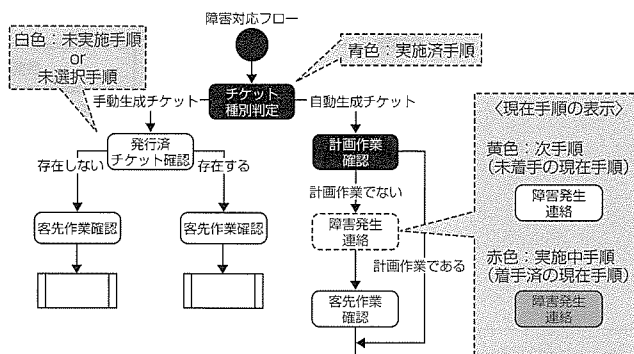


図2. 業務フローと状況表示

4. 開発時の課題解決と実装上の工夫点

4.1 開発時の課題

研究開発時のプロトタイプから実際の運用現場に向けた製品化開発での主な課題として、取り扱い可能な業務フロー数の増大と業務フローを動的にシステムへ取り込んで取り扱える柔軟さの必要性が挙げられた。このような課題を解決するために業務フローのメンテナンスを容易に行うための業務フロー策定ツールの選定や、システムへの取り込みや管理を容易にする仕組みなどシステムの運用機能の検討、基本部分のアーキテクチャの見直しなどを行う必要があった。

4.2 ツールの選定

業務フロー作成に利用する業務モデリングツールは、複数社の製品が対象に挙がったが、情報技術総合研究所が持つ業務プロセスモデリング技術の活用を前提に、汎用性の確保を考慮し次のような要件を基に選定を行った。

- UML(Unified Modeling Language)の記述が可能で、業界の標準形式であるXMI(eXtensible Markup Language Metadata Interchange)形式でのデータの取り扱いが可能であること
- データのカスタマイズが可能であること
- システムへ取り込むための開発が容易なこと
- 複数ユーザーの編集に対して整合性が取れること

その他、製品価格や使用実績の有無を考慮した結果、この要件を満たすスパークスシステムズジャパン社のEnterprise Architect^(注1)という製品を採用した。

4.3 運用機能の追加実装

ナビゲーションの基となる業務フローのデータは、データ管理者によってサーバ上で一元的に管理する必要があった。ただし、データの変更頻度は低いことから、クライアントアプリケーションの設計では、処理速度や通信トラフィックを優先し、リアルタイムにデータを参照するのではなくあらかじめクライアント上へダウンロードしたデータを使用して動作する仕組みを採用した。そのため業務フロー

(注1) Enterprise Architectは、スパークスシステムズジャパン㈱の商標である。

データの運用管理には次のような仕組み(図3)を検討し、追加実装した。

操作者が少数に限定されるサーバ上のデータ管理は、明示的にWebブラウザ向けのメンテナンス画面を通じて行う機能を実装した。対象者が多数となる個々のクライアントパソコンへのデータ展開は、自動的にサーバからダウンロードし差し替える機能をクライアントのアプリケーションの機能として追加実装した。これによって、新規顧客や運用対象システムの追加、契約内容の変更などによって業務フローデータのメンテナンスが発生した場合にも、利用者は意識することなく常に最新のデータに基づくナビゲーションを受けられる運用を実現した。

4.4 アーキテクチャのポイント

システムの中心的なサブシステムであるクライアントに搭載する“業務フローナビゲーション”の開発に当たって、土台となるフレームワークやアプリケーション部分のアーキテクチャのポイントについて次に述べる。

(1) GUIアプリケーション

クライアントアプリケーションは、業務フローの表示などGUI(Graphical User Interface)を持ったアプリケーションであることから、GUIを使ったアプリケーションを構築する際に一般的に用いられる構造であるMVC(Model-View-Controller)構造を採用し、モデルの永続化にはDAO(Data Access Object)方式を用いた。このDAOを実現しているのが、情報技術総合研究所が開発したナビゲーションライブラリである。また今回の開発では、単一の業務フローを扱い、クライアントパソコン上だけで動作するデスクトップアプリケーションであったプロトタイプをRDBサーバと組み合わせて実用可能な形態のソフトウェアとした。

(2) EclipseRCPフレームワーク

実装フレームワークとしては、リッチクライアントアプリケーションの代表的な構築基盤であるEclipseRCP(Rich Client Platform)フレームワークを利用した。また、ViewとControlはGEF(Graphic Editing Framework)をベースとすることで、効率的な開発を行った。

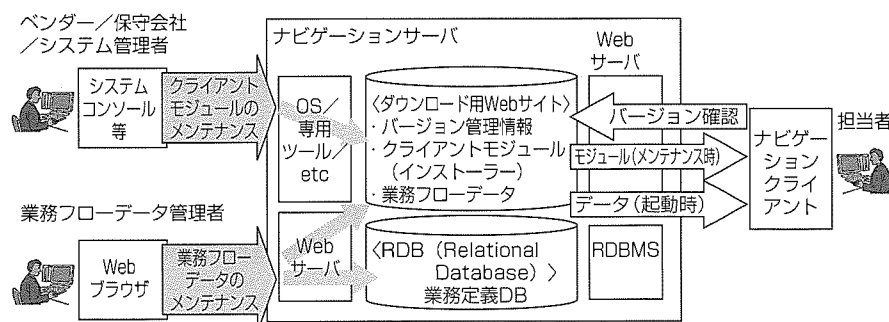


図3. ソフトウェアメンテナンスの仕組み

4.5 適用事例での実装上の工夫

(1) サービスデスクシステムとの連携

運用監視ナビゲーションシステム導入に当たっては、既設の運用管理用システムでサブシステム間の連携などある程度の統合化が完了していたため、その統合化された仕組みの中にうまく組み込むことで、操作性や有効性を向上するよう検討を行った。その結果、インシデント管理機能を備え業務の中心的なサブシステムとなっていたサービスデスクシステムとの連携機能を実装することで、スムーズな導入と様々な効果を実現した。

連携のポイントは次の2点である。

①ナビゲーションシステム起動操作の簡易化

運用監視ナビゲーションシステムでは、障害発生箇所のシステム識別子やサービスの種類、故障機器を特定するホスト名などをキーとして業務フローを決定する必要がある。また、これらはすべてサービスデスクシステムがインシデント情報として保持している情報であり、サービスデスクシステム上からのインシデント指定をもってナビゲータを起動することで、マウス操作1つで容易に正確な起動を可能とした。

②作業履歴の信頼性向上

運用監視ナビゲーションシステム導入前の障害対応業務では、サービスデスクシステムへの作業履歴の入力は各担当者に委ねられていたため、情報の正確さや信頼性に担当者ごとで個人差が生じていた。このため、場合によっては事後に履歴情報をメンテナンスする作業が発生していた。

運用監視ナビゲーションシステムでは、マウスでのクリックによって業務手順の確認を進めるだけで、作業実績が履歴情報として収集されるため、その情報をサービスデスクシステムへ自動挿入する連携機能を実装することで、信頼性の高い作業履歴の記録を実現した(図4)。

(2) 操作性の改善

運用監視ナビゲーションシステムは、担当者が業務手順を必ずトレースすることで、画一的な作業品質を確保するシステムである。しかし、プロトタイプでは担当者の熟練度によっては省略が可能であった作業が省略できなくなることで作業効率の低下を招き逆効果となるケースも指摘された。また、担当者のミスや勘違いによる手戻りへの対応などの柔軟性が必要であることも実際の現場への適用で初めてわかった。このため、次の機能を追加することで、操作性の改善を図った。

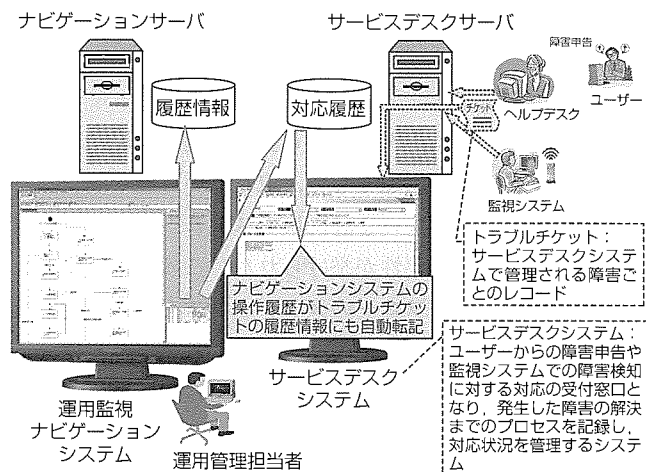


図4. サービスデスクとの連携

①スキップ機能

業務手順には、確実に実施しなければならない不可欠の作業と、何らかの代替作業によって明白となる確認作業のように不可欠でない作業が存在する。このため運用監視ナビゲーションシステムでは、業務手順のスキップ機能を実装した。これによって、業務フロー上の各手順に省略許可の目印となる“SKIP”マークを事前に設定することができ、その業務手順の実行結果としてスキップ状況の容易な確認が可能となった。

②Undo機能

担当者はナビゲーションに従って実施結果を入力していくが、誤って先の手順へ進んでしまった場合には、ある時点まで立ち返る必要が生じる。そういった事態に備えて運用監視ナビゲーションシステムでは、Undo機能を実装した。また、取り消し操作自体は作業履歴に記録することで、柔軟な操作性と正確な履歴情報の両立を実現した。

5. む す び

今回の開発では、運用管理担当者へのナビゲーション機能を中心としたシステムに留まった。今後はナビゲーションシステムのサーバに蓄積した作業履歴を利用した進捗管理機能や対処時間の自動計測機能など、サービスレベルの維持や管理、検証に寄与する機能開発にも取り組み、ITILの考え方に基づいた運用管理業務の継続的な改善を実現するシステムを目指していきたい。

参 考 文 献

- (1) 村澤 靖, ほか: ITIL準拠運用監視ナビゲータの開発, 情報処理学会第68回全国大会 (2006)

ネットワーク運用管理サービスの高度化を 実現する企業向けポータルサイトシステム

増田裕紀*
本部祐史*

Portal Site System for Enterprise that Achieves Upgrade of Network Management Service

Yuuki Masuda, Yuuji Honbu

要 旨

三菱電機情報ネットワーク㈱(MIND)では、企業向けネットワークサービスとして、企業内のデータ系・音声系ネットワークの構築・運用サービスや、外出先からのイントラネットアクセスを可能とするモバイルネットワークサービスなど、様々なサービスを提供している。

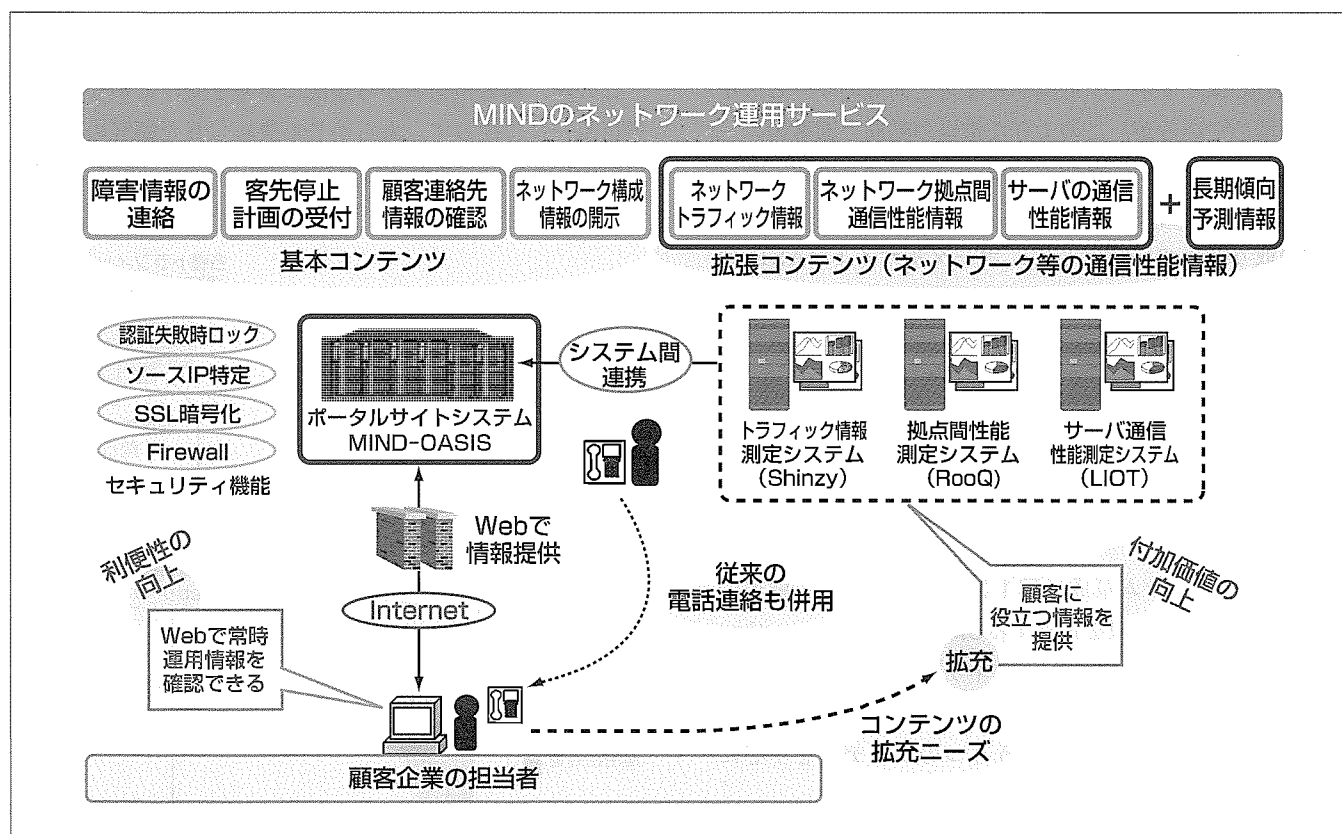
従来、これらネットワークサービスを提供していくためのユーザーとのインタフェースは電話やメールが中心であり、また運用情報を提供する媒体も紙、又は電子ファイルのメール送付がほとんどであった。

MINDでは、2006年に新ICC(統合運用管制センター)を立ち上げ、その一環として、ユーザーとの新たな運用インタフェースを実現するため、ポータルサイトシステム

“MIND-OASIS”(以下“OASIS”という。)を構築し、各種運用情報のWebによる提供を開始した。

OASISでは、顧客ネットワークの障害情報やネットワーク構成情報の開示といった従来電話や紙媒体で提供していた各種運用情報をWeb画面で開示する。また、ネットワークのトラフィック量や拠点間の通信応答性能など、ネットワークの性能を中長期的な視点から分析する各種システムとの連携を実現している。

現在は、顧客への公開を順次進めており、運用情報の公開ニーズを把握しつつ、顧客企業の情報システム部門にとってメリットのある“付加価値の高い運用情報”を拡充していくことで、運用管理サービスの高度化をめざしている。



企業向けポータルサイトシステム“MIND-OASIS”の概要図

障害の発生情報やネットワーク構成情報といった各種運用情報を基本コンテンツとし、さらにネットワークのトラフィック量などの通信性能情報を拡張コンテンツとして、インターネットを通じて顧客に提供する。

1. ま え が き

MINDのネットワークサービスでは、企業のニーズに合わせ、通信キャリアの広域回線や各メーカーの通信機器、及び種々の通信制御技術を組み合わせ、顧客の情報システムを支えるネットワークを設計・構築・運用している。

本稿では、このネットワークサービスにおける運用管理水準向上の施策として新たに開発した顧客企業向けポータルサイトシステムOASISの概要について述べる。

2. 開発の背景

国内のネットワークサービス市場では、各通信事業者が企業の拠点間を広域回線で接続するサービスを従来提供しているが、ここ数年は“マネージドサービス”という名称で、構築・運用の範囲を拡大する通信事業者が増えてきている。このマネージドサービスは、広域回線の提供が主体であった従来型のサービスに加え、ネットワーク機器の提供と監視・保守、及びネットワークのトラフィック測定などを行い、企業のネットワーク運用負荷軽減を目的としたものが多い。

このような動向の中で、企業の情報システム部門としては、これらマネージド型のサービスを提供する通信事業者の中から自社ネットワークの運用を安心してアウトソースできる信頼性の高い通信事業者を選択する必要がある。

MINDでは、マネージド型サービスと同等のサービスを従来提供しているが、このような市場の動向と顧客のニーズにこたえるために、更なる運用サービスの高度化、充実化に取り組む必要性が出てきた。

この取り組みの一環として、ポータルサイトOASISの開発を行い、“運用情報(なかみ)の充実”及び“伝達手段(つたえかた)の改善”という観点からサービスレベルの向上をめざしている。

3. OASISのアーキテクチャと基本機能

3.1 アーキテクチャ

(1) システム構成

OASISのシステム構成は図1に示すとおり、①顧客のネットワーク構成情報を管理するCMDB(Configuration Management Database)^(注1)、②ネットワークの障害情報管理用データベース、③顧客がインターネットを通じてアクセスするWebサーバ、という3つのシステムを中心に構成される。

また、④ネットワークの各種トラフィック測定を行う個別Webシステムとの連携を実現している。

(注1) CMDBとは、IT運用管理のガイドラインとして普及しているITIL(Information Technology Infrastructure Library)で定義される構成情報管理データベースである。

(2) セキュリティ

このシステムでは、各種運用情報をインターネット経由で顧客へ開示するというシステム形態であることを考慮し、セキュリティ面での各種安全性対策を行っている。

具体的には、SSL(Secure Socket Layer)による通信の暗号化、Firewallによる不正アクセス防止、このシステムに接続するソースIPアドレスとログインIDの合致検証、及びログイン認証失敗時(3回以上)のアカウントロックを可能としており、外部からの攻撃や侵入防止に備えている。

3.2 基本機能

OASISでは次の4つの基本機能を提供する。

(1) 障害情報の開示

従来、ネットワーク上で発生する障害情報の顧客担当者への伝達は電話連絡が中心であった。

OASISの障害情報開示機能は、顧客ネットワークにおける障害の内容を障害発生後、すみやかにWeb画面へ開示する。個々の障害はインシデント番号を採番して管理しており、このインシデントごとに障害の発生箇所や発生時間のサマリー、及び時系列での詳細な障害対応内容を画面上に表示することが可能となっている。

(2) 計画停止情報の受付

顧客が入居しているビルの計画停電などによって、MINDが遠隔監視するネットワーク機器の停止が発生し、MINDのICCでもアラームを検知する場合がある。

この際、顧客担当者から事前に連絡を受けていないと、運用ルールに従って、あらかじめ決められた顧客の連絡先にICCのオペレータが連絡を行う。

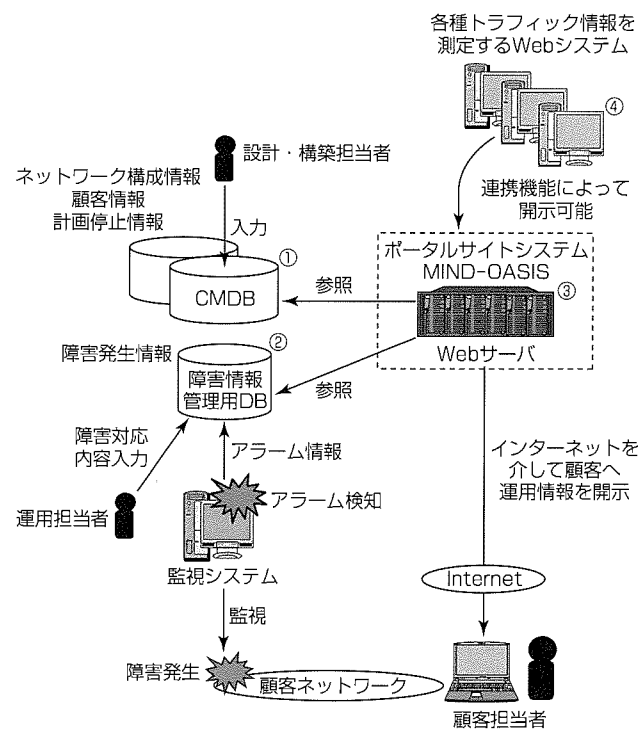


図1. OASISのシステム構成

このため、顧客・MIND双方にとって不要な状況確認作業が発生することになる。

計画停止情報の受付機能では、Web画面上から顧客担当者が該当拠点の停電やビル工事の情報を入力し、MINDに伝達することが可能である。

(3) 顧客情報の確認

ネットワークの運用では、障害発生時の連絡や計画停止工事の連絡など、MINDのネットワーク運用担当者と顧客担当者が日常でコミュニケーションをとるケースが発生する。

しかしながら、顧客内の人事異動などで運用担当者の変更が発生するケースがあり、この変更情報を日常から正しく管理していくのは、伝える側の顧客、及び管理する側のMIND双方にとって難しいのが実情である。

OASISの顧客情報確認機能では、サービスの契約時に取り決めた顧客側の運用窓口担当者氏名、電話番号、メールアドレス、及び複数の窓口担当者の連絡優先順位、といった運用情報をWeb画面から常時確認することが可能となっている。

(4) ネットワーク構成情報の開示

ネットワークの運用で、全国各拠点に導入している通信回線の速度やネットワーク機器の種別といった構成情報を正しく把握しておくことは、ネットワークの増強計画を立案していく上で必要となる。

従来、顧客側でこのネットワーク構成情報を把握する手段は、MINDが提供するネットワーク構築時の完成図書が中心であった。OASISのネットワーク構成情報開示機能では、Web画面からすみやかに回線速度やルータ機器名といった構成情報を確認することが可能となっている。

4. 拡張機能

基本機能で提供する運用情報をベースとし、OASISでは、ネットワークの通信性能測定情報など、MINDが運用サービスの付加価値として位置付ける各種性能情報を開示する。

4.1 ネットワーク性能情報の開示

従来MINDでは、ネットワークのトラフィック情報測定システム(システム名称:Shinzy)を構築し、Webで顧客に開示するサービスを提供していた。

OASIS構築に伴い、次に述べるShinzyの開示方式変更、及び、ネットワーク性能情報の拡充を図る拠点間通信性能測定システム(システム名称:RooQ)の開発を行った。

(1) ネットワークトラフィック情報

MINDのネットワークサービスでは、ネットワークに流れるトラフィックの量を測定し、通信回線の帯域に対する利用率を顧客企業に開示することでネットワークの増強計画立案に活用してもらっている。

前述のとおり、OASIS構築に伴って、このトラフィック情報を測定するShinzyをOASISの画面から顧客へ開示可能とするため、両システムに連携機能を持たせた。

これによって、顧客担当者はOASISにログインし、ネットワーク性能情報メニューから、Shinzyが測定するトラフィック量のグラフ画面を閲覧することが可能となっている(図2)。

(2) 拠点間の通信性能情報

従来、ネットワークの性能測定手法は前述したShinzyによるトラフィック量の測定が主であった。

OASIS構築に伴い、より高度なネットワーク性能の分析を可能とするため、顧客拠点間(例:本社~A支社)の通信レスポンス時間とパケットロス率を測定するRooQを開発した。このRooQでは、顧客ネットワークの本社又はデータセンターのような中心拠点に設置しているルータにRooQシステムが定期的にログインし、全国各拠点に設置しているルータに対してping^(注2)を実行することで、中心拠点~支社、支店などの拠点間の通信レスポンス時間とパケットロス率がどの程度発生しているかを把握することができる仕組みとなっている(図3)。

(注2) pingとは、IPネットワークでパケットの通信先までの到達を確認するためのプロトコルである。

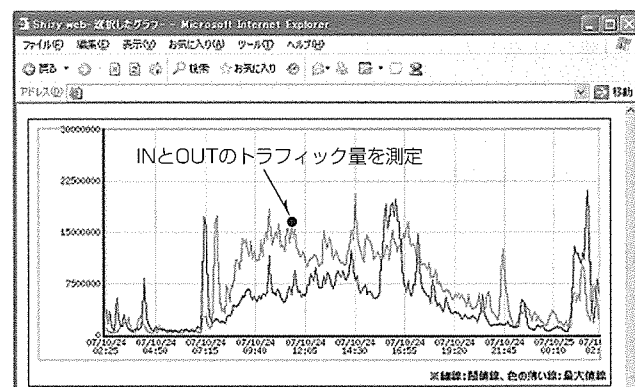


図2. Shinzyによるネットワークトラフィック情報画面

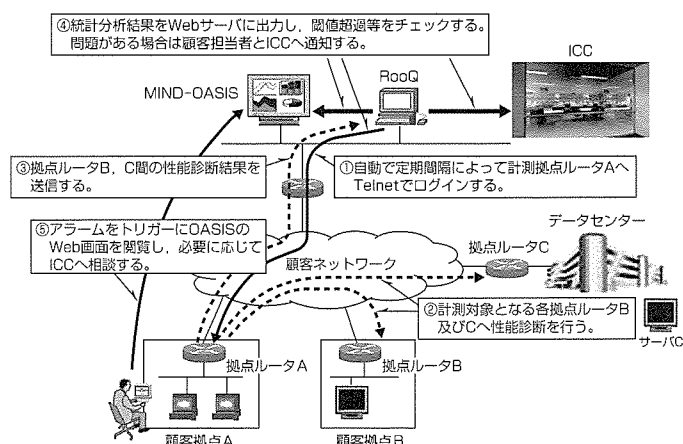


図3. RooQによる拠点間通信性能測定の仕組み

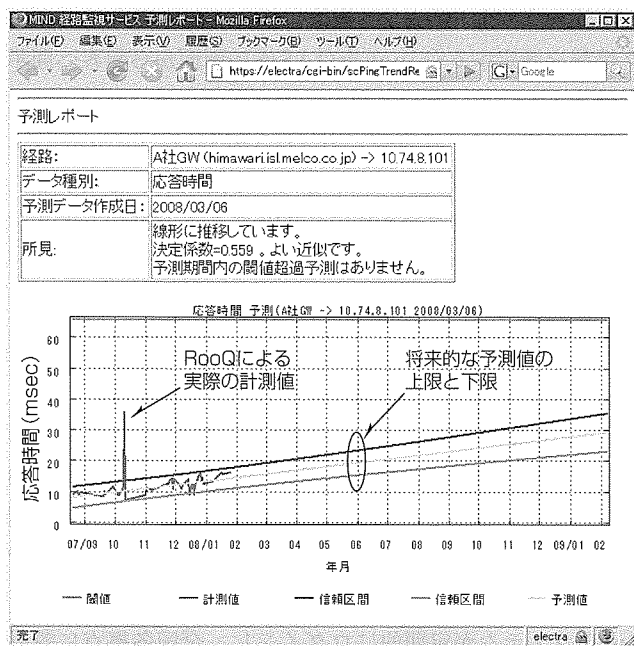


図4. 長期傾向予測の測定画面

4.2 ネットワークトラフィック情報の長期傾向予測

この機能は、前述した“ネットワークトラフィック情報”、及び“拠点間の通信性能情報”の補助的な機能として位置付けられる。

この長期傾向予測の機能はShinzy及びRooQそれぞれのシステムにプラグインするプログラムであり、各システムが収集、蓄積したデータを基に統計分析を行い、1年単位での将来的なデータの変化を予測してグラフに表示することが可能となっている(図4)。

4.3 サーバ通信性能情報の開示

企業情報システム全体の管理という観点では、メール、DNS(Domain Name System)、Proxyなど、ネットワークとともにインフラの基盤を構成するサーバの通信性能状態を日常から把握しておくことが必要となる。

これを実現するため、MINDではネットワークサービスのオプションとして、サーバの通信性能管理を実現する測定システム(システム名称:LIOT)を構築した。

このLIOTでは、顧客の拠点LAN(Local Area Network)内に専用の測定器(Agent)を設置し、Agentへ対象サーバ間の通信応答時間を定期的に測定することで、サーバごとの通信性能を定量的に把握することが可能である(図5)。

この機能によって、メールやWeb利用の遅延発生時に

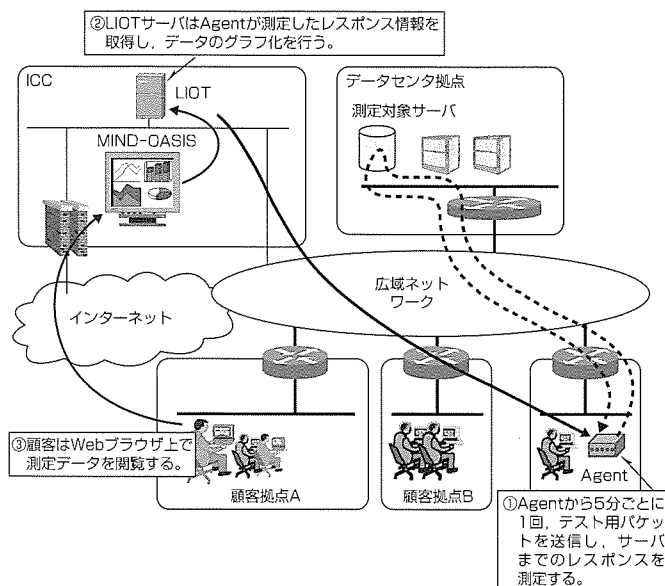


図5. LIOTによるサーバ通信性能測定の仕組み

原因がネットワーク側にあるか、サーバ側にあるかの切り分けが可能となり、かつ、ネットワークとサーバを含めた情報システム全体の増強計画を立案していくことが可能となる。

5. む す び

企業向けポータルサイトシステム“MIND-OASIS”で実現する各種機能について述べた。

顧客企業の情報システム部門に役立つ運用情報を提供していくことがこのシステムの役割であるため、顧客への公開を推進しつつ、情報システム部門が必要とする運用情報についての要望を把握し、顧客企業にとって真に付加価値のある運用情報ポータルをめざしていく。

参 考 文 献

- (1) 西宮哲進, ほか: お客様の利用感を監視し、快適・安心を提供する新ネットワーク性能監視サービスソリューション, 三菱電機技報, 80, No.4, 273~276 (2006)
- (2) 猪股義晴, ほか: サービスレベルと信頼性を向上させた新統合管制センターによるITILプロアクティブ運用管理サービスソリューション, 三菱電機技報, 80, No.4, 289~292 (2006)

EDIサービスシステムの高信頼化

Progress of EDI Service System Reliability

Minoru Yoshida, Katsuhiko Hatano, Yosuke Matsuura

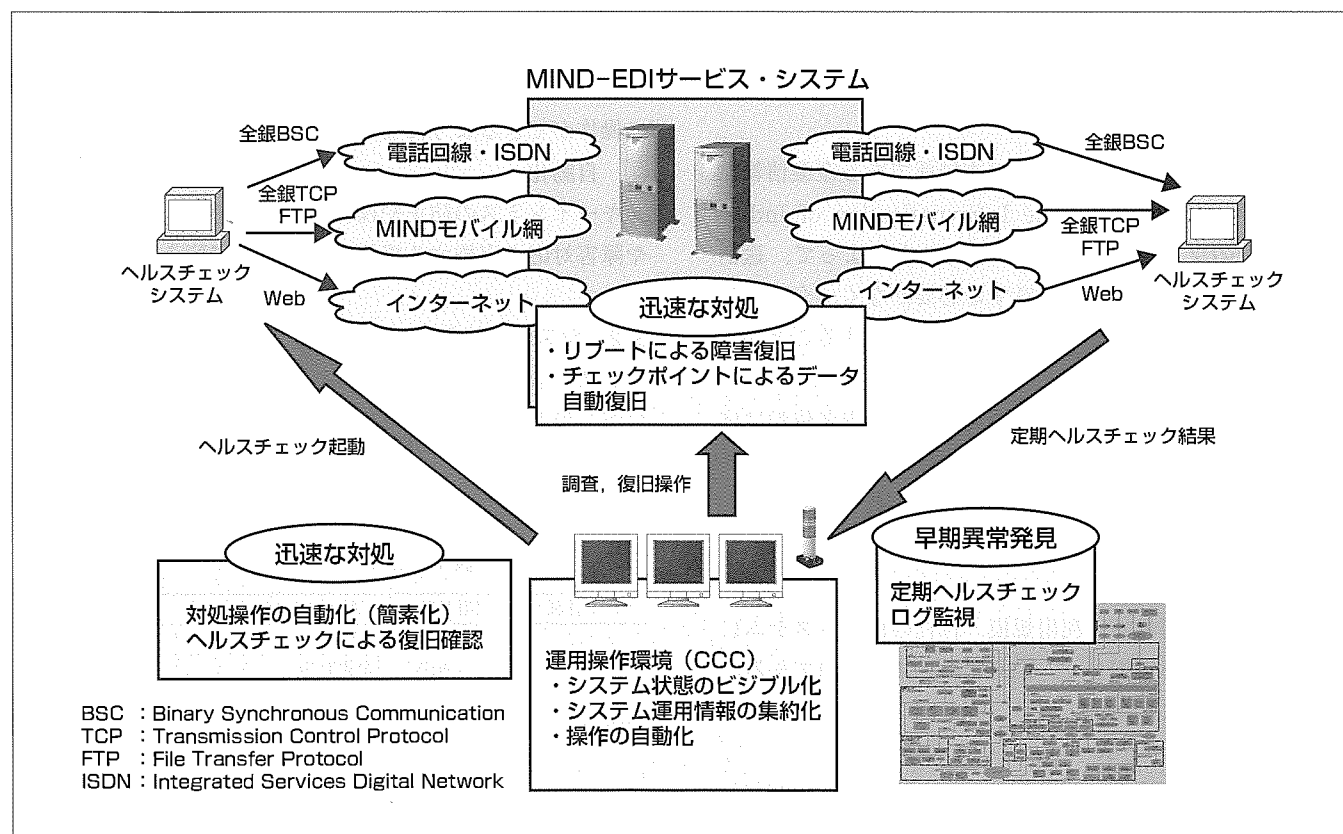
要 旨

EDI(Electronic Data Interchange)サービスシステムのダウンサイジングを機会に信頼性の向上機能を盛り込んだ。

サービス停止時間を極小とするため、システムの異常を早期発見し、迅速に対処する機能を実現した。早期発見のため従来システムにおける監視のように、想定した異常の発生を検知する“点監視”から、一連の処理がすべて正常に完了していることを監視する(言い換えれば、どこかに異常が発生したかを監視する)“線監視”に変えた。これはヘルスチェックと呼ぶシステムで、ネットワークを含めてEDIシステムをブラックボックスと見なし、擬似利用者がデータを投入し、その処理結果のデータを確認することで正常稼働を確認する。さらに、処理パターンを網羅することで、“線監視”から“面監視”へと進めている。定期的にヘ

ルスチェックを行うことで、システムの監視を行っている。ヘルスチェックは異常時の対処を含めてCCC(Command Control Center)を中心に実現されている。CCCは情報のビジュアル化、集約化、操作の自動化をめざした運用環境である。異常範囲はCCCによってネットワーク構成図上に表示され、操作員は障害解析シートに従って、原因を絞り込み、復旧を行う。復旧のための操作もCCCでボタンやネットワーク構成図上のサーバをクリックすることで迅速に行える。

新システムでは最悪の場合でもリポートでサービスを再開させることができる。新システムの処理ではチェックポイントを取りつつ動作しているため、リポート復旧時は処理中のデータの復旧も自動化されている。



EDIサービスシステムの高信頼化

MIND(三菱電機情報ネットワーク㈱)-EDIサービスの高信頼化技術を示す。新たな監視システムとしてヘルスチェックを実装した。これは擬似利用者がEDIシステムの正常稼働を監視するものである。監視結果はCCCという運用操作環境で表示される。正常時はもちろん、異常時の操作もすべてCCCで行われる。

1. ま え が き

新サービスの実装や機能追加を柔軟に実施できる環境を構築するために、EDIサービスシステムをメインフレームからサーバシステムにダウンサイジングした。新システムへの移行は2006年2月から2007年4月にかけて、順次、無事故で完了することができた。本稿では、ダウンサイジングを機に追加した高信頼化機能と新システムへの移行の際に駆使した技術について述べる。

2. MIND-EDIサービス

2.1 サービス機能

MIND-EDIサービスの目的は、企業に対して、受発注情報などの企業間のデータ交換を効率よく安全に行える環境を提供することである。EDIシステムは企業間に位置し、あとで述べる高信頼性を背景に、利用者へ次の利便性を提供している。

(1) ネットワークの集約

利用者はデータ交換相手のネットワーク設備を意識せずに、EDIサービス・アクセスポイントとのネットワークを用意すればよい。

(2) 蓄積交換

利用者はデータ交換相手のシステムの運用方式(稼働日時、送受信方式)を意識せずに、データを送受信することができる。

(3) 仕分処理、コード変換

利用者は送信データの形式を日本標準である産業情報化推進センター(Center for the Informatization of Industry: CII)のフォーマットに合わせることによって、送信先ごとにデータファイルを用意する必要がなく、全送信先へのデータを1つのファイルにまとめて送信することができる。

このほか、利用者データ異常時の連絡、利用者依頼に応じたデータの再送、ヘルプデスク、EDI推進サポート(新規加入時の伝送試験、Web-EDI新規加入者への操作説明会の実施等)も行っている。

2.2 多様な利用形態

利用者は、利用目的、利用規模、自社の情報システムに応じた利用形態を選択して、EDIサービスを利用できる。その内容を表1に示す。

2.3 電子帳票サービス

EDIサービスと連携したサービスとして、電子帳票配信サービスを提供している。このサービスは利用者が送信したデータをあらかじめ登録した形式の帳票に埋め込み、その結果を電子署名付きPDF(Portable Document Format)として配信するものである。電子署名を施すことによって、受信者は改竄(かいざん)のないことを確認することができ

る。また、受信したデータをCSV(Comma Separated Values)ファイルとして、ダウンロードすることもできる。

3. 新システムの高信頼化

利用者へ安全安心なサービスを継続的に提供するにはその基となるシステムの稼働状況を把握し、適切に対処することが第一である。そのため、異常を早期発見し、迅速に対処して定常稼働状態に戻すための機能を新システムに盛り込んだ。

3.1 C C C

EDIサービス新システムでは運用操作環境としてCCCを構築した。運用員はすべての操作をCCCで行う。EDIサービスシステムはデータセンターに設置されており、CCCとはネットワーク接続されている。CCCはEDIサービスシステムの運用思想を具現化したもので、情報のビジュアル化、システム運用のための手段の集約化、操作の自動化をコンセプトとしている。

(1) ビジュアル化

ネットワーク構成図に次節で述べるヘルスチェックの結果を表示し、異常の場合はその影響範囲を明示する。利用者データの処理状況、システムの負荷状況も表やグラフで図示することができる。

(2) 集約化

システム運用のために必要な情報(環境情報、マニュアル等)、操作機器を集約している。運用者はCCCですべての操作ができるようになっている。

(3) 自動化

キーインミスの防止や操作の迅速化を目的に、運用操作や障害対応で実施する操作をボタン等で行えるようにしている。

3.2 システム状態の把握(監視)

システムの信頼性向上には異常を早期発見することがその第一歩となる。そのために新システムに盛り込んだ技術について述べる。

表1. EDIサービスメニュー

データ仕様	利用形態	通信プロトコル	備 考
CII仕様	ファイル転送	FTP	MINDモバイル網使用
		全銀TCP	
		全銀BSC	
任意	Webアクセス	HTTPS	CSVファイルの送受可 添付ファイル(任意)の送受可 注文残管理機能
	FAX	FAX	
任意	ファイル転送	FTP	MINDモバイル網使用
		全銀TCP	
		全銀BSC	
任意	Webアクセス (電子帳票配信サービス)	HTTPS	電子署名付きPDFファイル CSVファイルの送受可

HTTPS: Hyper Text Transport Protocol Security

3.2.1 ヘルスチェック

(1) 点監視から線監視・面監視へ

従来のシステムでは、異常(例：処理停止)を想定し、その異常を示すイベント(例：該当プロセスのダウン)の発生を監視していた。これはシステムの処理の流れ(線)の上の特定の点を監視していることになる。ほかの原因で障害が発生した場合、これを検知することができなかった。例えば、プログラムのバグによってプロセス内で処理が滞った場合、プロセスダウンの監視では異常を検知できない。

新システムでは、正常であるかどうかを監視することとした。すなわち、一連の処理の流れ(線)すべてで異常がないことを確認することにした。逆に言えば、処理の流れ(線)の上のどこかで異常があれば、それを検知できるようにしたのである。さらに、このシステムの処理の流れを網羅することで“面監視”へと進めている(図1)。

(2) ヘルスチェックの仕組み

“線監視”“面監視”を実現するのがヘルスチェックである。ヘルスチェックの目的は、利用者から見てシステムが正常に稼働していることを確認することにある。

ヘルスチェックシステムは、擬似利用者がEDIシステムをブラックボックスと見なしてデータを投入し、その処理結果で正常稼働を確認している。次にその仕組みを述べる(図2)。

- ①擬似送信利用者がデータを自身の利用形態に従ってEDIシステムに送信する。宛先は擬似受信利用者を指定する(例：ファイル転送利用者の場合はメールボックスに送信する)。
- ②EDIシステムではこのデータを処理する。この結果、指定された宛先すなわち擬似受信利用者が受信できる状態になる(例：ファイル転送利用者の場合はメールボックスに格納される)。
- ③擬似送信利用者がデータ送信後、一定時間経過すると擬似受信利用者は自身の加入形態に応じてデータを取り込む(例：ファイル転送利用者の場合は自身のメー

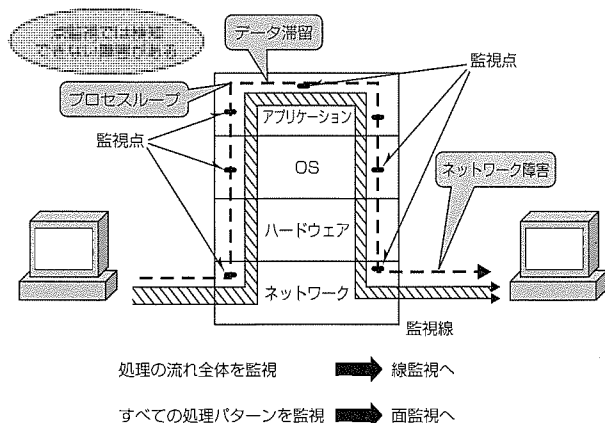


図1. 点監視と線監視, 面監視

ルボックスからデータを引取る)。

- ④擬似受信利用者は受信したデータの内容が正しいかどうかを確認する。擬似受信利用者は異常を検知すると、ヘルスチェック対象範囲を示す識別子と異常であることをCCCへ通知する。
- ⑤CCCでは異常の通知があると、パトライトを緑の点灯から赤の点滅に変え、警告音を鳴らす。ネットワーク構成図上のヘルスチェック対象識別子に対応するルートを青から赤に変更する(図3)。

上記処理を24時間365日繰り返し、システムの稼働状況を監視している。ヘルスチェックは正常稼働を確認すると、CCCにその旨通知する。CCCではこれを受けて、パトライトを緑に戻し、ネットワーク構成図上のルート表示を青

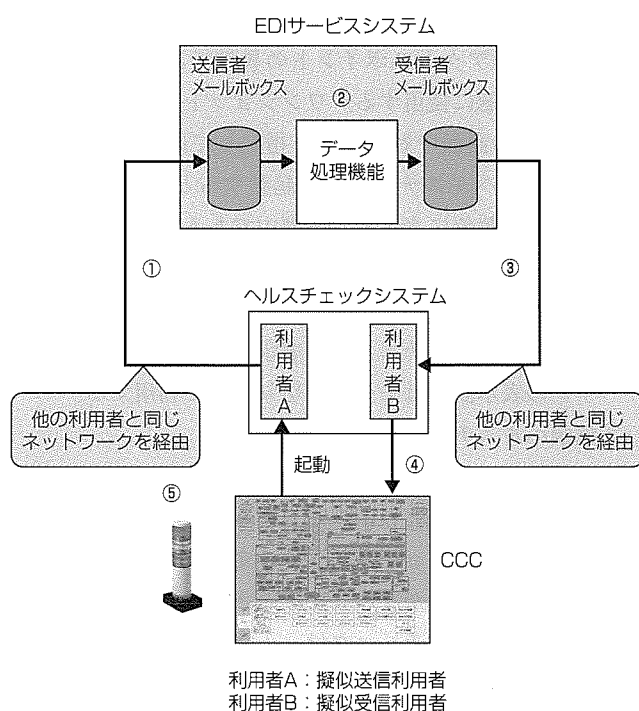


図2. ヘルスチェックの仕組み

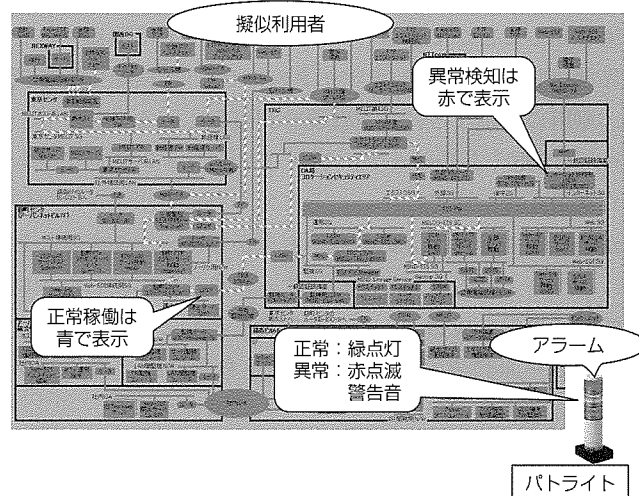


図3. ヘルスチェック結果表示画面(CCC)

に戻す。

EDIサービスへの利用者加入形態はファイル転送型、Web型、FAX型があり、ファイル転送型ではその通信プロトコルも多種にわたる。これらの全パターンに対応してヘルスチェックが用意されている。

(3) 3種のヘルスチェック

ヘルスチェックはその用途に応じて3種類用意している。

①定期ヘルスチェック

定期ヘルスチェックはシステムの稼働状態を常時監視するのが目的で、定期的に起動している。利用度が大きいサービス、経路に対して実施しており、すべて自動化している。

②ワンショットヘルスチェック

ワンショットヘルスチェックは特定の経路の正常・異常を確認する場合に使用する。例えば、障害の原因がFTPのアクセスポイントの異常であった場合、その復旧確認に使用する。ワンショットヘルスチェックはCCCの画面で対象経路を指定して起動する。ワンショットヘルスチェックを起動すると、CCCは処理中経路を黄色に表示し、処理中であることを示す。ワンショットヘルスチェックの結果が正常の場合は該当ルートが青で表示し、異常の際は赤く表示する。ワンショットヘルスチェックの表示画面と定期ヘルスチェックの表示画面はモードを切り換えて利用する。

③拡張ヘルスチェック

拡張ヘルスチェックは、EDIサービスの全サービス、全経路が正常かどうかを確認することを目的とし、システムのバージョンアップ等の変更が利用者へのサービス提供に影響がないことを確認するのに使用している。拡張ヘルスチェックは、正常確認が自動化されていないFAX送信など、人手による起動、確認も含んでいる。

3.2.2 ログ監視

システムが出力するログを監視することで、システムの状態を知ることができる。ヘルスチェックでは検知できない異常(利用者が送信したデータのエラー)の検知や影響範囲、原因の特定などにログ監視を利用している。しかし、サーバOSやミドルウェア、アプリケーションプログラムでログ形式は一律ではない。そこで、異常を示すキーワードがログ上の特定位置にあるかどうかをチェックすることで、エラー・警告の発生を監視する仕組みを作成した。ログ監視で異常を検知すると、警告音とともに情報をログ監視コンソールに表示する。異常発生を受けて、操作員がCCCから該当サーバに遠隔アクセスし調査を行う。

3.2.3 その他の監視

その他、機器の表示ランプの定期チェック、日々の処理負荷の定量的把握を行っている。EDIシステムへの入出力

データ量、システムに滞留しているデータ量等は日々記録に残している。これらの情報はシステムのキャパシティ管理に活用している。

3.3 異常時の対処

内部規程としてシステムの停止は2時間以内としている。この目標を維持するための仕組みについて述べる。

(1) システムの復旧

システムの運用者はパトライトの表示、警告音によって異常の発生を知り、CCCのネットワーク構成図によって異常範囲を即座に把握できる。これを受けて、異常を示すサーバのログやステータス情報によって、原因を絞り込んでいく。これらの作業はほぼルーチン化しており、作業シート等によって手順が標準化されている。具体的なコマンド等の操作はCCC上でボタン化されている(図4)。

新システムでは、ハードウェア障害(ハードウェアは二重化構成)以外では、最悪の場合でもシステムのリポートによってサービスが再開できることを確認した。リポートに必要な時間を考慮に入れ、復旧作業タイムチャートにチェックポイントを設定しており、チェックポイントでは2時間以内の復旧を目標に、リポートの可否を判断している。

(2) 利用者データの復旧

システムをリポートさせたあと、異常発生時に処理中のデータの復旧を行う。新システムでは、定常的に利用者データの処理にチェックポイントを埋め込んでいる。障害発生後、リポートすると、チェックポイントで処理中途であったデータの有無をシステム起動時にチェックし、必要なリカバリ処理を自動的に行う仕組みになっている。

(3) 復旧確認

システムのリポートが完了しても、外部とのデータ入出力はヘルスチェックを除いて停止させている。システムが稼働し、利用者データの復旧が完了すると、ヘルスチェックを起動する。ヘルスチェックで正常稼働を確認後、外部

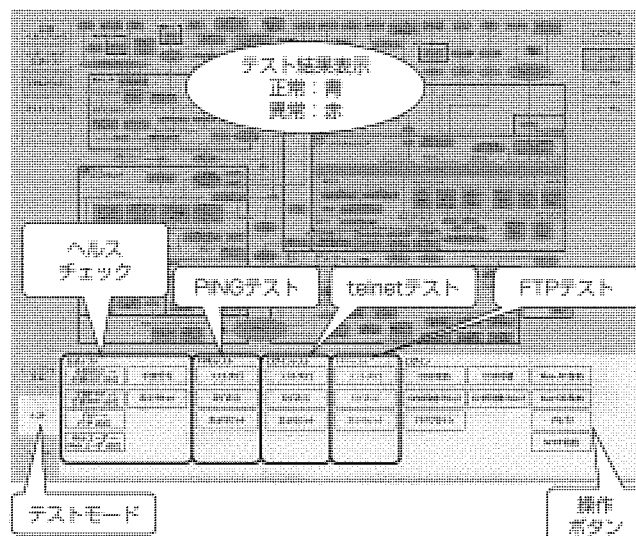


図4. CCC操作画面

とのデータ入出力を再開させる。

(4) その他

障害の原因調査よりサービス再開を優先するのは当然であるが、障害の再発は断じて防止しなくてはならない。原因調査に必要な情報はリブート前に可能な限りセーブするように、シャットダウン処理が組み込まれている。サービス復旧後、原因調査を行い、再発防止策が定められ、周知、実施される。

4. 新システムへの移行

多数の利用者へ影響を及ぼすことなく移行を完了させるため、様々な検証を行って移行に臨んだ。

4.1 利用者インタフェースの継承

新システムへの移行に伴い、FTP利用者、全銀TCP/BSC利用者がアクセスするサーバが変更になる。次のように、この変更が利用者に影響を及ぼさないようにした。

FTP利用者に対しては、事前にFTPプロキシサーバを設置した。この時点でFTP利用者からは直接EDIシステムへアクセスしないようにした。これによって、移行はFTPプロキシサーバからEDIシステムへの転送先を変更することで可能とした。

新旧システムの設置場所(データセンター)が異なるため、全銀TCP/BSC利用者のアクセスポイント(発呼先電話番号)の変更が必要であった。これに対しては、NTTの着呼の転送機能を利用した。移行当日に、アクセスポイントへの着呼を新アクセスポイントへ自動転送するように交換機の設定を行った。これによって全銀TCP/BSC利用者にとって、アクセスポイントの変更は不要になる。新システムへの移行完了後、すべての全銀TCP/BSC利用者に新アクセスポイントへの移行(発呼先の変更)を文書で依頼した。交換機の履歴情報等で旧アクセスポイントからの着呼自動転送実績をチェックし、旧アクセスポイントの利用がゼロになった時点で、旧アクセスポイントを廃止、解約した。

図5に新システムへの移行の流れを示す。利用者データ

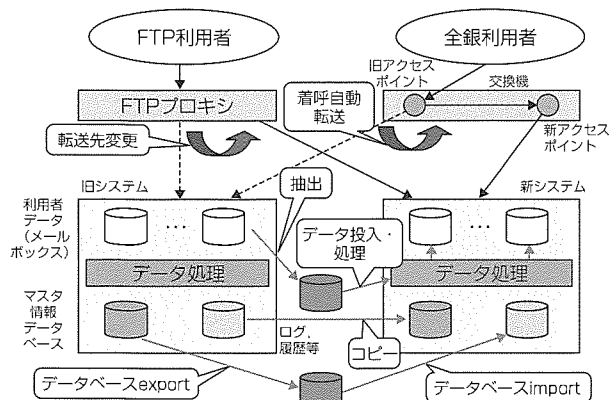


図5. 新システムへの移行

の移行では、利用者データのステータスを継承するため、旧システムから抽出したデータファイルを入力ファイルとして新システムに投入し、新システムで処理させ、利用者メールボックスにセットしている。

4.2 サービス継続性の検証

サービスの継承をサービス機能、利用者情報、利用者データの3点に分けて検証した。

(1) サービス機能の継続性(利用者インタフェースの移行)

利用者からみたサービス機能(利用者インタフェース)の継承は新システムでの拡張ヘルスチェックで確認を行った。

(2) 利用者情報の継続性(マスタ情報の移行)

利用者の利用形態、取引関係等の情報(マスタ情報)の継続性は、3か月分の実データを新システムで処理し、その結果を旧システムの結果と比較することで確認を行った。

(3) 利用者データの継続性(利用者データ、課金情報を含むログデータの移行)

移行開始時点でEDIシステムのメールボックスや保管庫に残っているデータの継続性は、新旧システム上のファイル数とその大きさの一致で確認した。

4.3 移行手順の確認

4.3.1 移行手順

移行は図6に示す手順で行った。作成した移行仕様で正しく移行できることは前節のサービスの継続性で述べた方法で確認を行っている。移行はEDIサーバ本体の移行(2006年2月)と全銀サーバの移行(同年11月)の2段階で実施した。

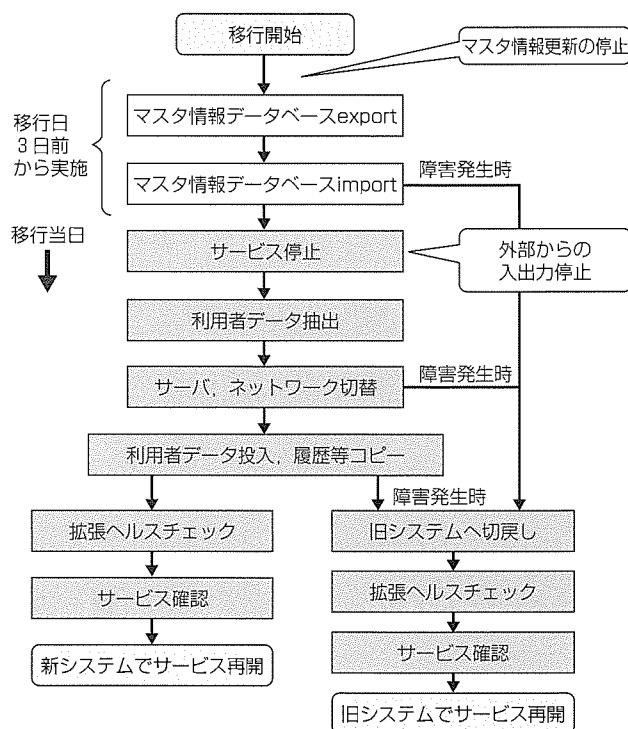


図6. 移行手順

移行は日曜日に実施した。利用者情報は多量であるため、旧システムからのexport、新システムへのimportは1日では完了させることはできない。そのため、移行当日の3日前に利用者情報の更新処理を停止(禁止)させ、移行を3日前から開始し、移行日前日には完了させている。

移行当日、不慮の事故等で新システムのままではサービスを継続できない場合がないと言い切れない。そのために、移行を中止し、旧環境へ戻し、サービスを継続できるようにしておかなくてはならない。この旧システムへの切戻し手順も作成し、確認をしている。

図6のサービス確認では、サービス利用に必要な全画面が正しく表示されていることを確認している。

4.3.2 リハーサル

移行手順は実際に移行当日と同じ作業を行うリハーサルによって確認した。また、リハーサル後は旧システムに戻し、旧システムでサービスを継続するため、切戻しの確認も行うことになる。そのほかに、リハーサルは移行当日の所要時間の実測という点でも重要である。また、予想外の事象(利用者からのアクセス)が実際に発生し、その対処も移行当日の手順に盛り込むことができた。

移行当日は、最悪の場合を想定し、旧システム環境に切戻し、旧システムでサービス再開するための所要時間を考

慮し、チェックポイントを定め、各ステップで経過を確認しつつ進めた。移行完了は拡張ヘルスチェック等で確認した。

5. む す び

移行後、障害が発生したこともあったが、即時に検知し、ここまで述べた対処によってすべて2時間以内でサービスを復旧している。障害履歴・問い合わせ履歴という財産を活用し、より安全、安心なサービス、利用しやすいサービスの提供を進めていく。

参 考 文 献

- (1) 神代トシコ, ほか: 企業ICTシステムを支える安全安心なシステム運用サービス, 三菱電機技報, 81, No.7, 481~484 (2007)
- (2) 秦野克彦, ほか: 安全なシステム移行のためのシステム試験, 情報処理学会第68回全国大会, 講演論文集(1), 講演番号7A-4 (2006)
- (3) 佐藤雅之, ほか: End-to-End監視によるアプリケーション監視システム, 情報処理学会第67回全国大会, 講演論文集, 講演番号5E-5 (2005)

紙文書の不正持ち出しをブロックする “文書持ち出し監視／ドキュメント棚卸システム”

虎渡昌史* 伊藤俊之***
村上耕平*
末沢康弘**

Confidential Paper Documents Management System

Masashi Torato, Kohei Murakami, Yasuhiro Suezawa, Toshiyuki Ito

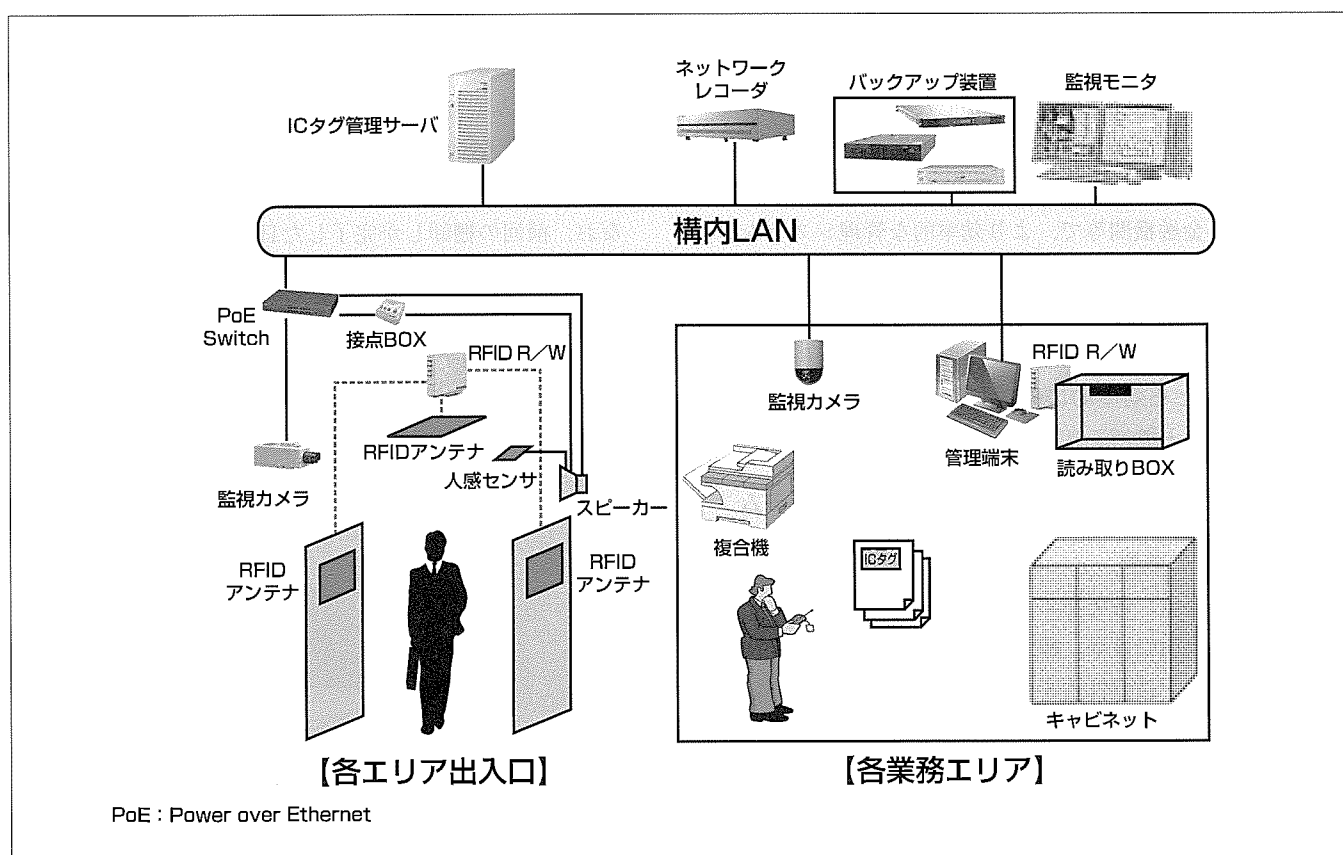
要 旨

個人情報保護法の施行や内部統制への取り組みが進む中、企業ではセキュリティに対する要求が高まっており、その対象は電子データに限らず印刷物の紙文書にもおよび。電子データはシステムやツールで均質な統制が実現可能であるが、紙文書に対しては人手に頼るところが多いため、確実性の面や管理負荷の面で問題がある。

三菱電機インフォメーションシステムズ㈱(MDIS)では、RFID(Radio Frequency IDentification)技術を活用することで、この問題を改善するための新たなドキュメント管理ソリューション(文書持ち出し監視／ドキュメント棚卸システム)を開発した。このシステムは、RFIDアンテナを内

蔵した各業務エリア出入口のゲート設備及び管理端末によって、IC(Integrated Circuit)タグを添付した紙文書の不正持ち出しを監視することができる。

ICタグの利用は管理番号の目視やバーコード読み取りによる方法に比べてより効率的な持ち出し管理ができるほか、ドキュメントの定期的な棚卸が容易に行えるようになり、不正持ち出しの検出をより確実なものとしている。また、監視カメラシステムと連動することで持ち出し時の証跡記録としての利用のほか、不正持ち出しに対する抑制効果の面でも有効な仕組みとなっている。



“文書持ち出し監視／ドキュメント棚卸システム”のシステム構成

各業務エリアの出入口にゲート設備を設置して、紙文書の不正持ち出しを監視する。不正持ち出し時には、ゲートでの警報と所定の情報の記録を行う。また、監視カメラによる録画から、持ち出し時の状況を容易に検索することができるよう、録画情報へのインデックス付けを行う。ゲートでの検出漏れを補完するために、管理端末で定期的に紙文書の棚卸作業を実施する。

1. ま え が き

個人情報保護法の施行や内部統制への取り組みが進む中、企業ではセキュリティに対する要求が高まっており、その対象は電子データに限らず印刷物の紙文書にもおよぶ。電子データはシステムやツールで均質な統制が実現可能であるが、紙文書に対しては人手に頼るところが多いため、確実性の面や管理負荷の面での対策が十分に機能しにくい側面があった。

紙文書に対する統制を強化するためには、紙文書の持ち出しに関する管理方式を確立して運用する必要があるが、従来のような管理番号の目視やバーコード読み取りによる方法では、不正持ち出し防止策としての有効性や管理負荷の点で問題があった。

本稿では、紙文書の不正持ち出し防止を強化しつつ、管理負荷の低減を可能とするシステムについて述べる。

2. システム化の背景

紙文書による情報の流出を防ぐためには、安易な印字出力やコピーの抑制はもちろん、記載内容に応じたセキュリティ管理上の等級を定め、その等級に応じたアクセス管理／持ち出し管理を徹底する必要がある。特に、機密度の高い情報が記載された紙文書に対しては、各文書へのアクセスを制限するとともに、閲覧や持ち出しに対するトレーサビリティを高め、外部流出の危険性の高い不正持ち出しを防止することが重要となる。しかしながら、紙文書の場合は、電子データの場合と比べて識別や所在確認の自動化が難しく、対象となる紙文書の増加に伴って管理負荷が増大するため、金融機関等で、より効率的な管理システムの開発が望まれていた。

そのため、不正持ち出しに対する管理方法として、紙文書の不正持ち出し時に検知することと、紙文書が持ち出されていないことを効率的に確認できる“文書持ち出し監視／ドキュメント棚卸システム”を開発した。

3. 文書持ち出し監視／ドキュメント棚卸システム

3.1 システムの概要

このシステムは、各業務エリアの出入口で持ち出しを検知するゲート設備のほか、紙文書の登録／棚卸作業を行う管理端末、ゲート設備付近を監視する監視カメラ、それらを管理するサブシステムによって構成している。

(1) 紙文書の登録

ユーザーは、管理対象となる紙文書にICタグを貼り付けて、管理端末を通じてシステムにそのICタグを登録する。登録されたICタグによって文書を識別し、棚卸時の存在確認や不正持ち出し等の検出に利用する。

(2) 紙文書の棚卸

登録された紙文書はその所在を確認するために定期的に棚卸作業を実施する。この棚卸は、管理端末に接続された読み取りBOX(図1)に紙文書をかざすことで簡単に行うことができ、棚卸結果は一覧として出力可能である。

(3) ゲートでの不正持ち出し監視

業務エリアのゲート通過時に、持ち出しを許可されていない紙文書の有無を判別し、不正持ち出しが検出された場合には警報を鳴らすなどの必要な処置を取る。

(4) 監視カメラによる記録

ゲートの出入りは、監視カメラで24時間録画しており、検出したICタグによる識別情報をインデックスとして録画情報に記録し、この識別情報によって録画情報の検索・再生を行うことができる。

3.2 紙文書の棚卸

紙文書を紛失していないこと、不正に持ち出されていないことを確認するため、定期的な棚卸作業を実施する。システムを有効に機能させるためには、この棚卸作業が効率的、かつ確実に行えることが不可欠であり、専用の読み取りBOXによって紙文書に貼り付けられたICタグを読み取ることでこれに対処している。

読み取りBOXには、一度に複数の紙文書をかざすことが可能で、かざす方向は関係なくICタグを読み取ることができる。そのため、大量の紙文書でも短時間で読み取ることができる。存在するはずの紙文書がない場合には、ICタグの読み取り結果と一致しないため、簡単に棚卸ができるのみでなく、棚卸の際の虚偽の報告による隠蔽(いんぺい)も困難である。

なお、前回の棚卸しが完了した日時を記録しているので、不正持ち出しが判明した場合には、その日以降に範囲を絞って、録画情報等による調査を実施することになる。

3.3 ゲートでの不正持ち出し監視

ゲート設備(図2)は紙文書の不正持ち出しを検知するために設置する。ゲート設備は左右の壁及び天井にRFIDア

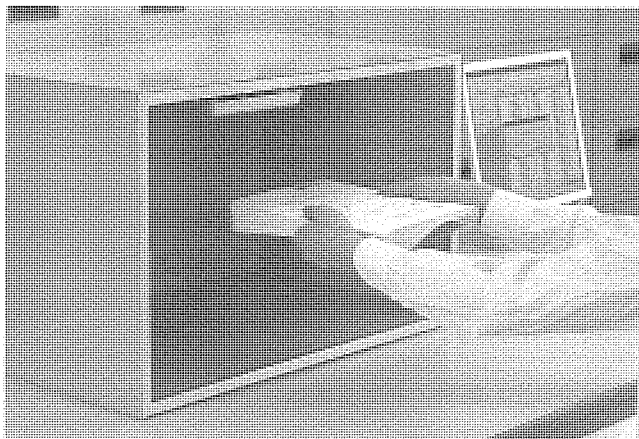


図1. 読み取りBOX

ンテナを配置する。UHF(Ultra High Frequency)帯のRFIDを使用することで遠距離でもICタグが読めるため、既存の壁に直接RFIDアンテナを設置してもよい。

各ゲートでは、人感センサによってゲートの通過を検知し、RFIDアンテナによってICタグの読み取りを行う。ICタグを検出した場合、その識別情報によって持ち出しを許可されているかどうかを判別し、許可されていない場合には不正持ち出しとして警報を出力する。また、所定の情報をシステム上に記録し、監視カメラでの録画情報に対応したインデックスとして識別情報を記録する。

3.4 監視カメラによる記録

各業務エリアの出入り口には固定型の監視カメラを設置し、出入りの状況を録画する。

出入口に設置される固定型カメラは、高画質な映像で監視し、逆光時や夜間の低照度時でも鮮明な映像が取得できる。また、必要に応じて旋回型カメラを設置して広範囲を監視することも可能である。旋回型は、最大400倍のズーム機能と毎秒540度の高速水平エンドレス回転機能を持つものを使用する。

設置したカメラは24時間365日で稼働しており、録画したすべての画像をネットワーク経由でレコーダに保存する。保存された録画画像は、インデックス情報によって検索し、監視モニタ上に再生表示することができる。なお、レコーダに保存された画像は、自動的にテープへバックアップされるため、長期間の保存にも対応できる。

監視カメラを設置することで、持ち出し時の証拠として録画情報が利用できるようにするほか、不正持ち出しの抑止効果を目的としている。

4. UHF帯RFIDの利用

4.1 他の方式との比較

このシステムを実現する上でUHF帯のRFIDを採用しているが、UHF帯のRFID以外の次の方式と比較した。

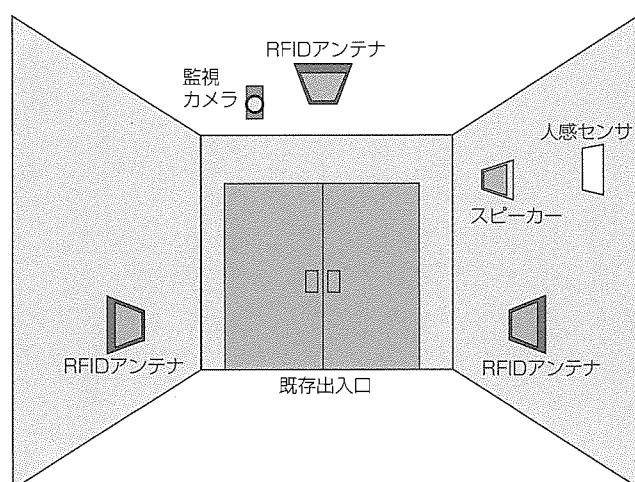


図2. ゲート設備

- ・二次元バーコード
- ・他の周波数帯を使用したRFID

二次元バーコードでは、バーコード部分を光学的に読み取らせる必要があり、棚卸作業時に読み取り効率が悪い。また、ゲート通過時の検出に関しても読み取り機がバーコードを視認できなければ検出できないため、持ち出し時に検知することは難しい。

RFIDタグは光学的な遮蔽(しゃへい)物があっても読み取ることが可能である。ただし、UHF帯以外の周波数帯では電波の到達距離が短いため、通常の出入口に設置する場合、ゲートの間隔を狭める必要がありゲート設備には不向きである。

UHF帯のRFIDでは3m程度離れていてもICタグの読み取りが可能である。そのため、既存の出入口を邪魔することなく設置できる。

特に三菱電機製のUHF帯RFIDでは最大7mの読み取り距離を誇り、1枚のアンテナで広い範囲にある複数のICタグを同時に読み取ることが可能である。

4.2 ICタグの読み取り率向上

ゲート通過時に不正持ち出しを検知するためには、確実にタグを読み取る必要がある。ただし、ゲートを通過するユーザーがどのように紙文書を持つかは限定することが難しい。紙文書の持ち方によってICタグのポジションが異なってくるため、様々なシチュエーションでICタグを読み取れるようにする必要がある。そのため、RFIDアンテナの設置をゲートの左右及び天井の3か所に配置することでゲート通過時におけるICタグの読み取り率を向上させた。

また、RFIDリーダライタの最大出力でゲート設備を構築した場合、読み取り範囲が広範囲にわたり、ゲート通過者が紙文書を持っていない場合でも、業務エリアに置いてある紙文書を誤検知して警報を鳴らす事態が発生する。そのため、このシステムでは環境に応じて出力を変更し、読み取り範囲を調整してゲート付近のみ検知させることとした(図3)。

4.3 電波干渉回避

1 拠点に複数のゲート設備や管理端末を設置する場合、多数のRFIDリーダライタを設置する必要がある。ICタグ読み取り時における電波干渉が発生する可能性がある。電波干渉が発生するとリーダライタから電波を出力させることが一時的にできなくなり、ICタグを読み取れない。電波干渉を回避して常に正しくICタグを読み取れる設計をしなければならない。干渉回避の方法として次の対策を行った。

- ・使用する周波数を分ける
- ・電波輻射(ふくしゃ)時間を限定する
- ・電波を遮断して影響範囲を狭める

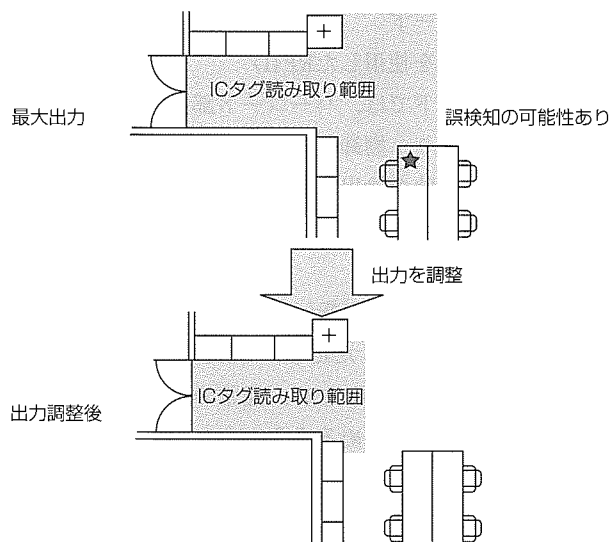


図3. 読み取り範囲の調整

周波数を分ける対策に関しては、三菱電機製のRFIDリーダライタでは複数の周波数帯が利用でき、同時に複数のアンテナを利用できる。ただし、使用できる周波数帯には限界があるため、いかに有効利用できるかが課題となる。ゲート通過時に確実にICタグを検知する必要があるため、ゲート設備で使用するリーダライタの周波数を優先させた。

輻射時間を限定する対策に関しては、ゲート通過時のみ電波を輻射してICタグを読み取ることにした。また、各ゲートが同時に動作しても干渉しないようシミュレーションで最適な輻射時間とした。同様に管理端末についても輻射時間調整を実施した。電波の遮断対策に関しては、管理端末での読み取りBOXに電波吸収体を使用し不要な電波の放射をおさえることで、近接距離での管理端末稼働を実現した。

このような対策を行ったうえで、システム設置後にゲートの同時通過試験や複数の管理端末での読み取り負荷試験を実施し、電波の干渉問題が発生せずにICタグを読み取れることを確認した。

5. む す び

このシステムは三菱東京UFJ銀行で採用され、システム部門で2007年10月から本格的に運用されている。数10万枚のICタグが管理可能で、RFIDリーダライタは70台以上、RFIDアンテナは170台以上となり、UHF帯RFIDを用いた文書持ち出し監視システムとしては国内最大級の規模となる。

これまでの情報セキュリティソリューションは情報システムの上でのセキュリティ管理が中心であり、紙媒体に出力された文書まで対策をすることはほとんどなかった。このシステムによって、今まで難しかった紙文書のセキュリティ上の管理をシステムで実施することができ、紙文書的不正持ち出し防止を強化しつつ、管理負荷の低減が可能となる。今後、紛失や持ち出しの許されない重要書類や物品を扱う企業や団体などの管理システム構築に展開していく予定である。

参 考 文 献

- (1) 三菱電機広報発表：2007年10月25日 三菱東京UFJ銀行に国内最大級の大規模セキュリティシステムを納入
<http://www.mitsubishielectric.co.jp/news/2007/1025.htm>
- (2) 三菱電機：“技術に驚き”をテーマとした新聞広告、第33弾 UHF帯RFIDシステム
http://www.mitsubishielectric.co.jp/info/ad/series_keytech01/index.html
- (3) みずほ情報総研(株)：UHF帯電子タグシステムの相互干渉特性把握及び運用方法の検討，経済産業省委託事業報告書
http://www.meti.go.jp/policy/it_policy/tag/2006_UHF_research_1.pdf

“ネカ録”最新シリーズによる 遠隔・集中監視ソリューション

西村達夫*
内村誠之*

Remote and Centralized Surveillance Solutions with “NECAROKU” New Series

Tatsuo Nishimura, Seishi Uchimura

要 旨

“ネカ録^(注1)”は三菱電機インフォメーションテクノロジー(株)(MDIT)が提供するネットワークカメラに対応した監視カメラ用録画・配信サーバである。カメラメーカーを選ばず自由に組み合わせて表示／録画が可能で、IP (Internet Protocol) ネットワーク経由での統合的な遠隔監視が可能であることを特長としている。今回、小規模から大規模システムまで幅広く対応できるよう機能強化を図った。

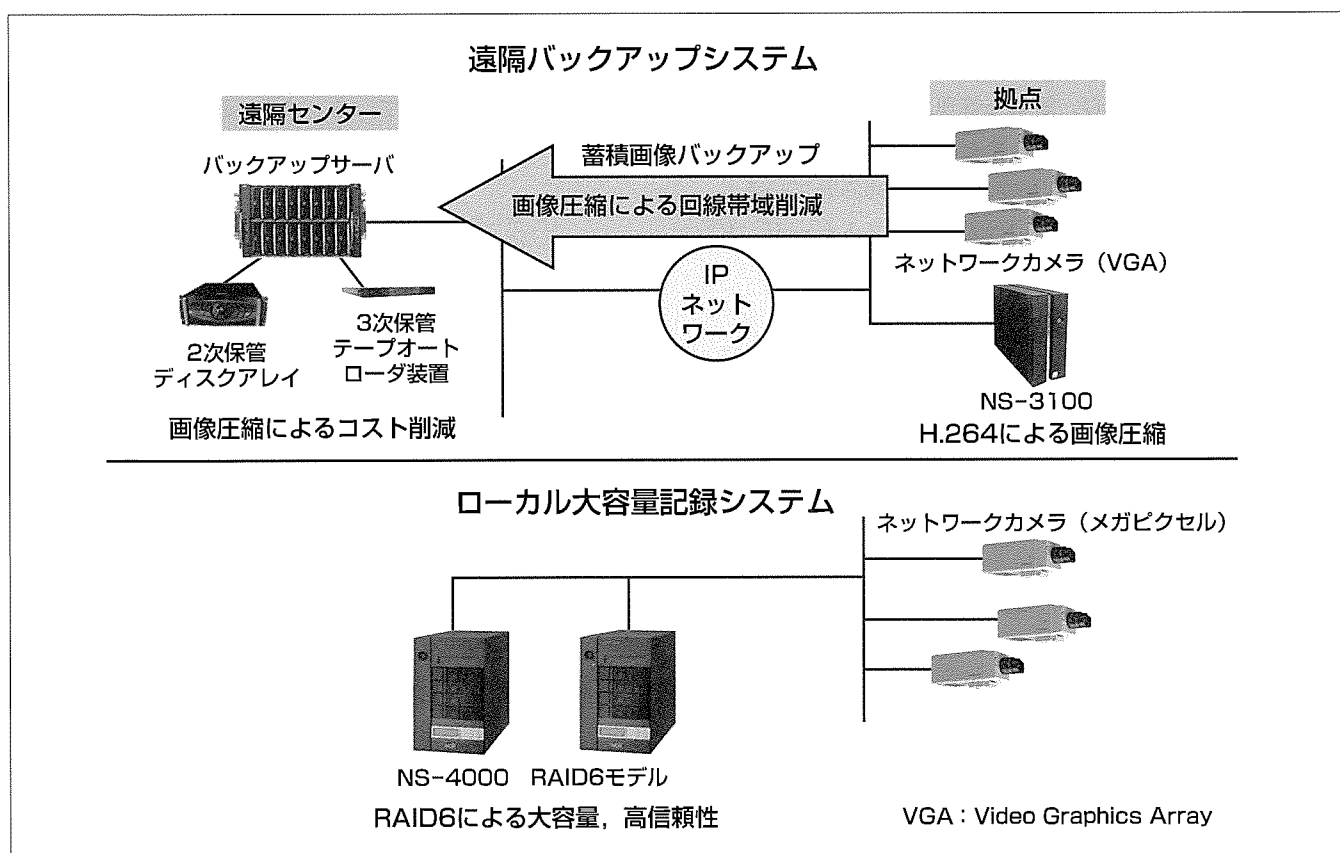
小規模な店舗でも複数台のカメラを設置するなどストレージの大容量化が進み信頼性の要求も高まっている。そこでRAID (Redundant Arrays of Independent Disks) 6を採用した大容量／高信頼ストレージを開発した。

(注1) ネカ録は、三菱電機インフォメーションテクノロジー(株)の登録商標である。

適用領域の拡大に対応し、小規模システムではだれでも簡単に操作でき、大規模システムでは多数のカメラを容易に制御・監視できるスーパーマルチビューアを開発した。

また、画像の増加に対応するため最新画像圧縮技術MPEG (Moving Picture Experts Group) -4 AVC/H.264を採用した。これによって従来の4倍の圧縮率を実現し、ストレージコストや回線コストの削減を図った。

MDITでは、これらネカ録の特長を生かし、全国に展開する拠点の監視画像を、センターのテープ装置へ長期保存可能な遠隔センターバックアップシステムも多数構築している。



ネカ録による監視システム構成例

遠隔バックアップシステムには、高速CPU (Central Processing Unit) を搭載し、MPEG-4 AVC/H.264トランスコードによる画像圧縮効率を向上した“NS-3100”を各拠点に設置して、回線帯域を削減、センターストレージコストを削減する。ローカル大容量記録システムではRAID6を採用した“NS-4000”によって大容量／高信頼システムを実現する。

1. ま え が き

近年、セキュリティへの関心が高まる中、監視カメラも従来のアナログカメラシステムから、ネットワークカメラを活用するデジタルシステムへ移行しつつある。MDITの録画サーバ“ネカ録”は、ネットワークカメラを使った監視カメラシステム用の録画サーバで、①ネットワークカメラの種類を選ばず自由に組み合わせて接続できる、②一店舗だけの小規模なシステムでも簡単に利用できる、③デジタル化によってIPネットワークで接続できるという特長があり、全国規模での展開も容易である。

本稿では、ネカ録の最新機能とそれを支える技術について述べる。

2. 背 景

2.1 適用領域の拡大

監視カメラシステムは、セキュリティ意識の高まりとともに、適用領域が広がってきている。例えば、小規模な店舗などでも複数台の監視カメラを設置し始めている。問題が発生した場合に関連する画像を取り出すためには、その画像を適切に管理、保管しておく必要がある。また、専用のオペレータなどは期待できない家族経営の小売店などでは、特別なスキルを持たない店舗経営者が管理しなければならない場合も多い。カメラの高画質化に伴い、録画データも増え、ストレージコストも無視できないレベルになってきている。これらから、簡単な管理、ストレージコストの低減が一層求められている。また、狭い店舗での設置を考え、省スペースな筐体(きょうたい)も求められている。これらの課題を解決するためには大容量のストレージ、ビューアの操作性向上が重要となる。

2.2 大規模システムへの対応

一方、金融機関などでは、各店舗に数十台、さらにATMにも監視カメラが設置されている。従来は各店舗、各拠点で管理していたが、法規制強化、保存期間の長期化、管理コストの低減などに対応するため、遠隔センターから監視したり、一括バックアップを行う大規模システムが求められつつある。

この場合、課題となるのは画像データを店舗から遠隔センターに伝送する回線コストである。実用的な時間内に伝送するには相当の回線帯域が必要になる。そのためには、画像圧縮技術と、高度なシステム構築技術が必要になる。

3. 大容量／高信頼ストレージモデル

メガピクセルカメラへの対応が進み、必要な記憶容量は確実に増大している。しかし、容量を増やすとHDD(Hard Disk Drive)が故障した場合の被害も増大する。大容量でかつ安心して使用できるストレージを内蔵したモデ

ルが必要となってきた。 “省スペースで大容量／高信頼性モデル”という要求にこたえるため、RAID6を採用した大容量／高信頼ストレージを内蔵した“NS-4000”を開発した。その特長を以下に述べる。

3.1 RAID6構成

一般に大容量で信頼性を確保するためには、3～4台のHDDを組み合わせて仮想的な1台のHDDとして構成するRAID技術を使用する。RAIDにはその構成方法、信頼性によってRAID1からRAID5の5種類がある。従来は4台のHDDによるRAID5構成とし、うち1台のHDDが故障しても録画が継続できるようにしていた。新モデルNS-4000ではRAID6構成とし、4台のうち2台のHDDが故障しても録画画像は消えずに保持できるようにした(図1)。これによって、1台が故障して交換中に、別の1台が故障しても録画済みの画像は保持され、新しい画像の録画も止まることなく、非常に信頼性の高いシステムが提供できるようになった。

3.2 筐体のコンパクト化と大容量化

幅152mm、奥行319mm、高さ235mm(突起部を除く)のコンパクトな筐体に、最大4TBの大容量HDDを内蔵し、長期間の録画やカメラ台数が多い構成にも対応できるようにした(図2)。

3.3 ホットスワップへの対応

さらに監視カメラシステムは24時間稼働が求められるため、HDD故障時でも電源を切ることなく交換できるホットスワップ機構を備えている。また、交換後も一切の操作

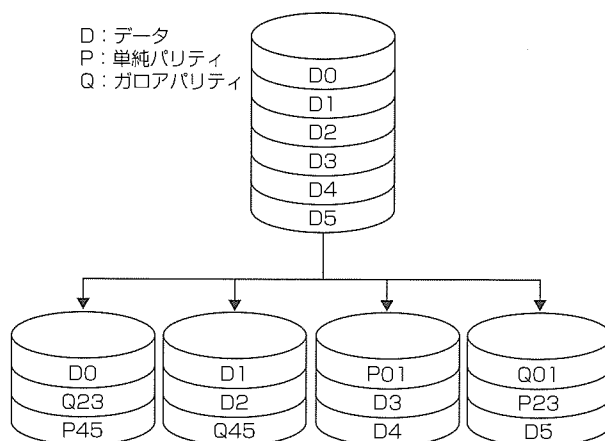
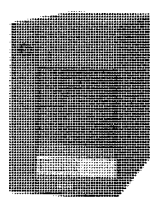


図1. RAID6動作概要図



HDD物理容量(TB)	4	3	2
HDD実効容量(TB)	RAID5 3	2.25	1.5
	RAID6 2	1.5	1
ネットワーク(RJ-45)	1000M×1		
消費電力(W)	100		
サイズ(mm)	幅152×奥行319×高さ235		
質量(kg)	10		

図2. NS-4000の外観、仕様

をせず、自動的に新HDDに必要なデータが再生成される自動再構築機構を備えた。

4. スーパーマルチビューア

現在撮影中のライブ画像は、必要な時に必要なカメラの画像に簡単に切り替えて表示できなければならない。さらに問題発生時に、過去の画像を簡単に検索して表示する機能も要求される。

4.1 カメラ配置図連携機能

ライブ画像画面の横にカメラの配置図を表示し、画像表示中のカメラの位置が視覚的にわかるようにした。また、配置図上のカメラアイコンをクリックすることによって、該当カメラライブ画像を拡大表示する機能を実現した。この機能によって配置図とライブ画像の連携を可能とした(図3)。

4.2 再生機能強化

ネカ録には、カメラ画像のほかに、各種信号入力(動き検知、センター入力、カメラ停止など)も同時に記録している。これらの信号履歴と連携して、各信号の通知時の録画画像を検索して再生可能とした。さらに、入退出管理装置などの外部機器による履歴や、監視画像を解析しての行動認識・顔認証なども連携する。この機能によって、例えば深夜の異常なドア開閉時の監視画像を素早く検索し再生するといった応用が可能となる。

4.3 表示レイアウト設定機能強化

ビューアの表示レイアウトで、各カメラの画像の表示位置・サイズを任意に指定可能とし、ユーザーの用途に合った見やすいレイアウトでの画像監視を可能とした(図4)。

5. 画像圧縮技術MPEG-4 AVC/H.264 トランスコーダ

通常のネットワークカメラは、カメラ側でモーションJPEG(Joint Photographic Experts Group)方式によって画像を圧縮し、録画サーバではそのまま録画していた。例えばJPEGでは、一般的なVGA10コマ/秒、5台カメラの構成では、データ量は1.25Mバイト/秒となり、1か月で約

3TBとなってしまふ。

圧縮率を向上させるために、JPEG系に加えてMPEG系での記録にも対応した。現在、MPEG系で最も圧縮率が良く、高画質なMPEG-4 AVC/H.264を採用し、JPEGから直接MPEG-4 AVC/H.264形式へ圧縮するトランスコーダを開発した。

5.1 高圧縮率

モーションJPEG画像をMPEG-4 AVC/H.264形式へ変換することで、圧縮率を4～6倍向上させた。これによって、ネカ録への長期保管が可能となる。例えばあるシステムで1TBの物理HDD容量でJPEG形式によって3か月録画可能であった場合、MPEG-4 AVC/H.264で圧縮することで実質4TB相当(1年以上)の記録ができることになる。

また回線の帯域確保とコスト低減も可能となる。例えばあるシステムで全拠点のバックアップに100Mbpsの回線が4本必要であった場合、MPEG-4 AVC/H.264で圧縮することで100Mbps回線1本にでき、回線コストの大幅な削減が可能になる。

5.2 汎用ファイルフォーマット

変換後のファイルは汎用的な“MP4”フォーマットとし、MPEG-4 AVC/H.264のデコード機能を持つ汎用的な動画再生プレーヤーで再生可能な形とした。このため、表示には専用のアプリケーションが不要となっている。

6. 遠隔バックアップシステム

2006年2月の預金者保護法施行を契機とし、金融機関内の監視システムについては財金融情報システムセンター(FISC)のガイドラインが浸透し、録画データを長期保管(2年間)するシステムが増えている。銀行のATMコーナーは300以上の拠点を持つこともめずらしくなく、広域網を介して多数の拠点にあるネカ録内の録画画像を遠隔で同時にバックアップしたいというニーズが高い。

MDITが提供するバックアップシステム構成を、図5の監視センター内の構成を例に述べる。

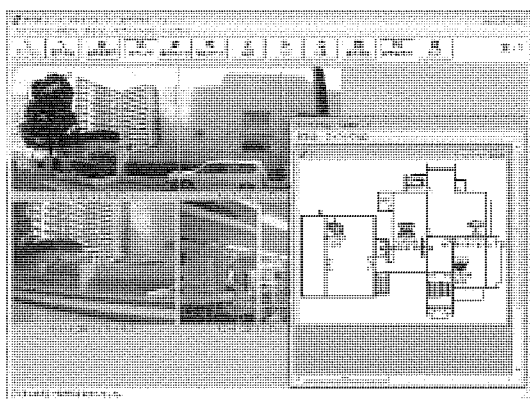


図3. 配置図表示例

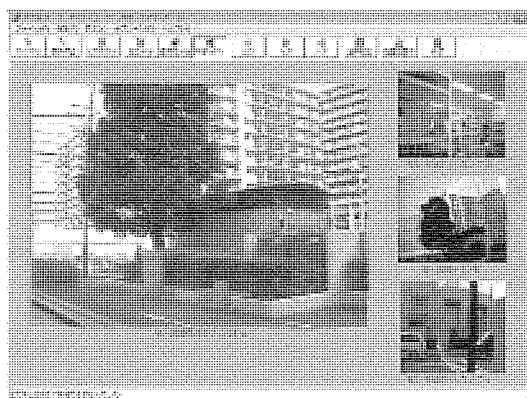


図4. 表示レイアウト例

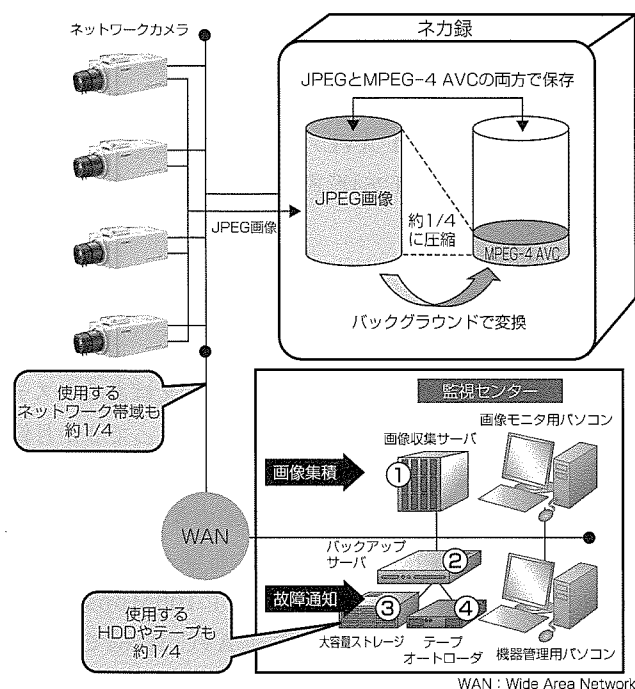


図5. 遠隔バックアップシステム

(1) 画像収集サーバ(1次記憶)

各拠点から毎日画像を吸い上げて1日分の録画データのみ一時的に記録する。吸い上げた画像ファイルは②のバックアップサーバのファイル共有機能で③のストレージ(2次記憶)に格納される。収集サーバはブレードサーバで構成され、1台のブレードが故障してもほかのブレードで代替運転できるよう制御する専用ソフトウェア“ネカ録画像集積ソフトウェア”を用意した。

(2) バックアップサーバ

2次記憶の大容量ストレージ、3次記憶のテープオートローダを管理している。バックアップソフトウェア(Backup Exec^(注2)等)もこのサーバ上で動作する。

(注2) Backup Execは、VERITAS Software 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。

(3) 大容量ストレージ(2次記憶)

3か月程度の画像を記憶し、テープから戻さずに高速検索できる。10~15TBの容量を持つ。

(4) テープオートローダ(3次記憶)

Backup Exec等によって大容量ストレージ内の録画データを毎日大容量のテープに書き込む。テープ媒体によって2年以上の長期保存が可能となっている。

このような構成の遠隔保管センターで、今回、ネカ録画像集積ソフトウェアをMPEG-4 AVC/H.264に対応させ、MPEG-4 AVC/H.264へ変換した画像を定期的に遠隔センターのサーバへバックアップする機能を実現した。この遠隔バックアップは、従来はモーションJPEG形式の画像のみを対象としていたが、MPEG-4 AVC/H.264形式を新たに追加することで狭帯域の回線しか持たないユーザーに対しても遠隔バックアップへの道が開かれるものと期待している。

7. む す び

今回、遠隔バックアップシステムなどシステムのニーズにこたえるために、NS-4000大容量/高信頼ストレージモデル、スーパーマルチビューア、MPEG-4 AVC/H.264トランスコーダを開発した。今後それぞれの製品を更にブラッシュアップし、使いやすく高信頼性のシステムを構築していきたいと考えている。

参 考 文 献

- (1) ISO/IEC 14496-10:2004, Advanced Video Coding (Second edition) (2004-3)
- (2) 大久保 榮 監修, 改訂版 H.264/AVC 教科書, インプレスR&D (2006)

“DIGUARD NET” 対応統合ID管理サーバを用いた 情報システム・入退室管理システム連携ソリューション

近藤誠一* 伊藤英明†
堀 辰也**
池田健一郎***

Information Systems and Physical Access Control Systems Integrated Solution Using ID Management Server with “DIGUARD NET”
Seiichi Kondo, Tatsuya Hori, Kenichiro Ikeda, Hideaki Ito

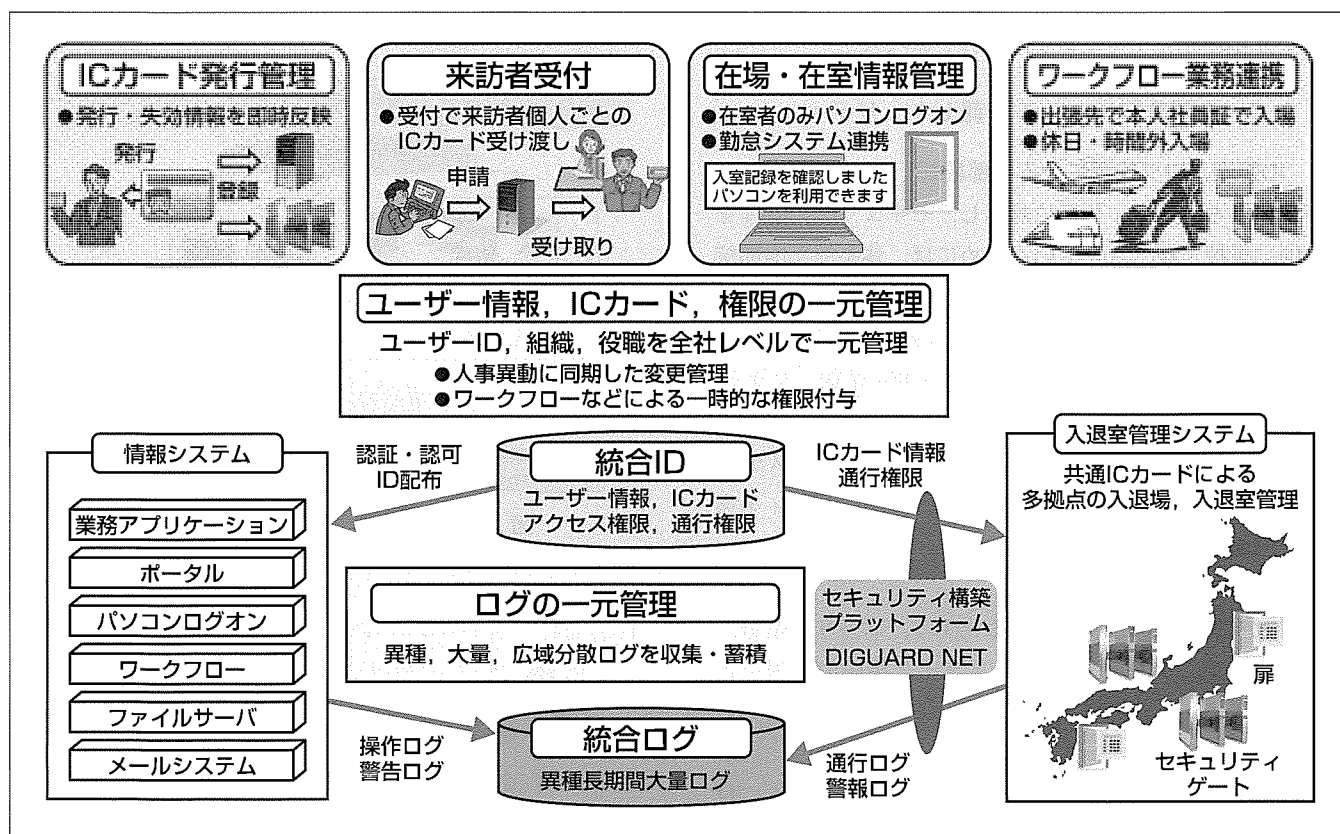
要 旨

増加、多様化するセキュリティ脅威に対して、ユーザー認証、アクセス制御、ログ監査などの情報システムを対象としたセキュリティ対策や、人の通行を物理的に制限する入退室管理システムなどの導入が進められている。情報システムにおけるなりすまし・不正防止のための在席状況の確認や、情報システムで変更管理する人事情報と連動した入退室管理システムの通行権限自動設定といった相互連携が、セキュリティ向上、運用性向上、内部統制強化につながる。しかし、一般に、入退室管理システムを含む設備管理と情報システムは独立して構築、運用されているため、連携システム導入には、個別に対応する必要があった。

このような問題を解決するため、ユーザー情報、ICカ

ード情報、権限情報などの“統合ID”と、情報システムの操作ログ、入退室管理システムの通行ログなどの“統合ログ”を一元管理し、三菱電機標準のセキュリティ構築プラットフォーム“DIGUARD NET(ディガードネット)”を利用して、データ収集・変更管理・情報提供を行う情報システム・入退室管理システム連携ソリューションを開発した。

連携ソリューションとして、人事システムと連動したICカード発行管理、来訪者向けに一時的なICカードを即時発行する来訪者受付、在室者のみにパソコンログオンを可能とする在室管理、及び、出張者、休日出勤者等に一時的な権限を与えるワークフロー業務連携などを提供する。



情報システム・入退室管理システム連携ソリューション

ユーザー情報、ICカード、権限、ログを、情報システムと入退室管理システム間で一元管理し、DIGUARD NET を利用してデータ収集、変更管理、情報提供を行う連携ソリューションを提供する。その結果、認証手段であるICカードの共通利用、変更管理の局所化・即時化、統合ログ管理によって、利便性向上、安全性向上、運用性向上を実現する。

1. ま え が き

IT利活用の進展に伴い、セキュリティ脅威は増加・多様化の一途をたどっている。機密情報漏えい事故に対する対策として、パソコン、サーバなどのユーザー認証、アクセス制御、ファイル暗号化などの情報セキュリティや、人の通行を物理的に制限する入退室管理システムの導入が進んでいる。入退室管理システムは、単に、機材や紙文書の盗難、破壊に対する対策としてだけでなく、機密情報が格納された情報機器の閲覧、コピーの抑止や、通行ログを解析することによる機密情報漏えい事故が発生した際の犯人の特定に利用されている。しかし、これまでは、個別の脅威に対して個別に対策が施されていたため、ID／パスワード、ICカードといった本人認証手段の導入コストや、人事異動時の変更に要する運用コストの重複が発生していただけでなく、認証手段やアクセス許可を得るための手順が複雑になることによって、利便性、モラルの低下を招く危険があった。特に、来訪者、社内出張者、ICカード非携帯者／紛失者に対する入場許可といった例外処理に対しては、人手による運用を要するだけでなく、人為的な誤りによるセキュリティ上のリスク発生の危険があった。

本稿では、三菱電機セキュリティ構築プラットフォームDIGUARD NET⁽¹⁾を利用した情報システム・入退出管理システム連携ソリューションについて述べる。

2. 内部統制における情報セキュリティ

2.1 ID管理、ログ管理による内部統制

多様なセキュリティ脅威に対応し、セキュリティ管理を継続的に維持・向上させていくためには、体系的な内部統制の仕組みが有効である。内部統制を実現するフレームワークであるCOBIT(Control Objectives for Information and related Technology)⁽²⁾では、ユーザー情報、アクセス権限の統合ID管理、各システムのログを集積・監査する仕組みの構築が示されている。これらを情報システム、入退室管理システムに適用し、“見える”セキュリティを実現した内部統制の構成を図1に示す。

(1) 統合ID管理

“だれが何をできるか”見える化する。ユーザー情報、情報機器、コンテンツのIDと、アクセス権限の管理を行う。

(2) 統合ログ管理

“だれが何をしたか”見える化する。情報システムに対する操作、入室・退室のログを収集して、一元管理する。ログは、コンプライアンス・セキュリティ基準のためのエビデンス、セキュリティ対策の実施状況確認、不正・異常検知、不正行為の事後追跡といった用途で活用される。

2.2 統合ID管理サーバ

ユーザー情報、及び、ユーザーに割り当てられるアクセス権限の管理を行う統合ID管理サーバの全体構成を図2に示す。統合ID管理サーバは次の機能を持つ。

(1) 認証機能

ID／パスワード、ICカード、指紋、PKI(Public Key Infrastructure)などの認証手段による本人認証、及び、これらを組み合わせた複合認証を行う。

(2) 認可機能

ロールベースアクセス制御RBAC(Role-Based Access Control)モデル⁽³⁾に基づいて、組織、役職といったユーザー属性情報をもとに、アクセス権限の有無を判定する。

(3) ID投入機能

人事システムから抽出したユーザー情報、組織情報等のIDのバッチ投入、Web画面インタフェースからのオンライン投入、及び、アクセス権限の設定を行う。

(4) IDライフサイクル管理機能

企業活動で発生する変化に即座に追従するため、IDを多バージョン管理し、事前投入、赴任までの猶予期間管理、過去のログの整合性検査を可能とする。

(5) ID配布機能

管理しているIDを入退室管理システム、業務システム、LDAP(Light weight Directory Access Protocol)、

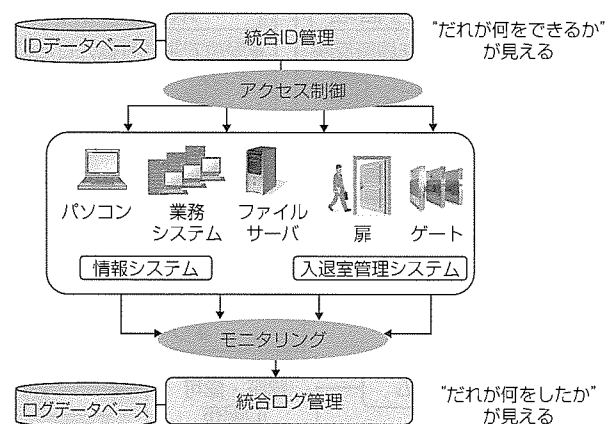


図1. ID管理、ログ管理による内部統制

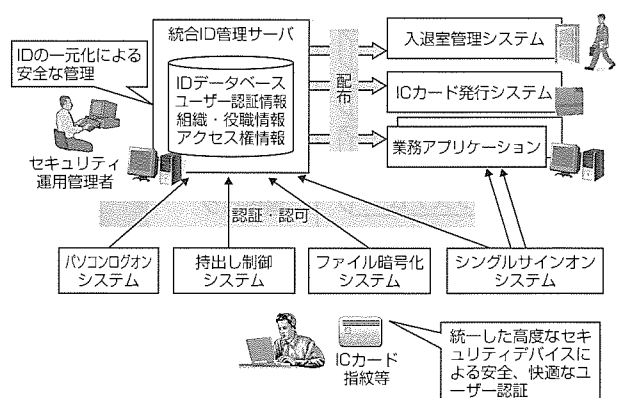


図2. 統合ID管理サーバ構成図

Microsoft Active Directory^(注1)等へ配布する。

(6) ログ収集・蓄積機能

パソコン、サーバ、入退室管理システムが出力するログを、エージェントを用いて収集・蓄積する。

2.3 セキュリティ構築プラットフォームDIGUARD NET

トータルセキュリティシステムの構築に向け、三菱電機独自の共通プロトコルによってシステム間の通信を実現するセキュリティ構築プラットフォームDIGUARD NETを開発した。図3にDIGUARD NETを利用したトータルセキュリティシステムを示す。入退室管理、映像監視の物理セキュリティや、ファイル暗号化などの情報セキュリティの連携に必要なID情報、ログ情報、画像情報などを、共通プロトコルを用いて相互に通信し、ニーズに応じたセキュリティシステムの構築が可能である。また、セキュリティだけでなく、勤怠管理などの業務システム、昇降機、空調、照明などのビル設備との連携も可能である⁽¹⁾。

3. 情報システム・入退室管理システム連携ソリューション

3.1 ICカード発行管理

セキュリティの観点から社員証等の身分証としてICカードを利用する事例が増加している。社員への発行が遅れると、本人にとって機会損失、利便性が損なわれるだけでなく、代替手段に要する運用コスト、セキュリティリスクが発生する。また、退職・紛失時に、失効処理が遅れると、回収されていないICカードが不正に利用されるリスクが発生する。このシステムでは、図4に示すように、人事異動に連動したICカードの発行・失効管理、及び、Webブラウザを用いた、即時発行／失効処理機能を提供する。人事システムから、人事異動発令時に発行／失効情報を投入し、発令日、赴任日といった猶予期間を含むユーザー情報を多バージョンで管理し、指定日からの認証、及び、失効を実現する。

3.2 来訪者受付

企業内では、継続的に勤務する従業員、派遣社員のほかに、業務打ち合わせ、資産の搬入／搬出／メンテナンスの

(注1) Microsoft Active Directory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。

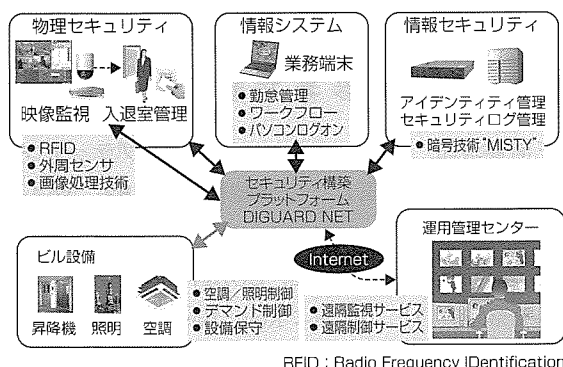


図3. DIGUARD NETを利用したトータルセキュリティシステム

ために企業外の来訪者が入退室する。これらの来訪者に対して指定時間に、指定場所のみ、一時的に入室を許可することが必要となる。図5に、来訪者受付システムを示す。このシステムでは、次の手順で来訪者の入場を許可する。

- ①従業員が来訪者予約画面から入場期間、入場を認める場所を指定して、統合ID管理システムに登録する。
- ②受付担当者が、来訪者到着時に、申請された場所に該当するICカードを、DIGUARD NETを介して入退室管理システムに登録して利用可能にし、貸し出す。
- ③来訪者は、受け取ったICカードを利用して指定された場所に入場／入室する。
- ④来訪者ログを管理者画面から確認する。

3.3 在場・在室管理

入退場／入退室の記録をDIGUARD NETを介して収集・蓄積して、指定した時間、場所の在場・在室者を、管理者画面から検索を可能にする。在場・在室情報を利用した情報システム連携の例を次に示す。

●パソコンログイン連携

在室者情報を、Microsoft Active Directory等のユーザー認証を制御するシステムに設定することによって、在室者に限定したパソコンログイン、退場者のパソコンの自動ログオフ等を行う。

●スケジュール管理連携

本人が記入した予定表に加えて、現在の在場・在室情報をリアルタイムで表示することによって、スケジュールに対する現在状況の確認、予定外の行動の把握を第三者が行うことが可能となる。

●就業管理連携

勤怠管理システムに入退室時刻を投入することによって、就業時間入力の補助、整合性確認が可能となる。

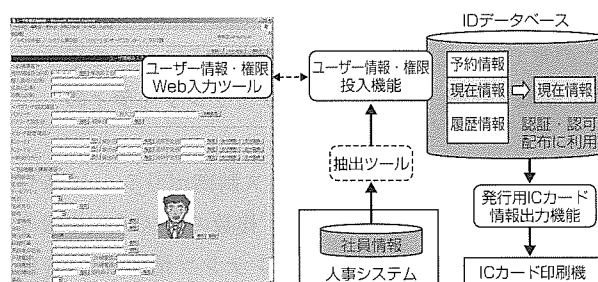


図4. ICカード発行管理

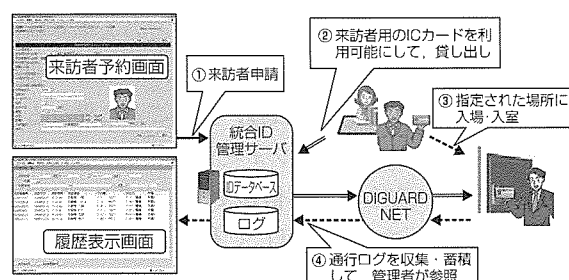
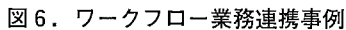


図5. 来訪者受付システム



3.4 ワークフロー業務連携

出張時、休日・時間外入場、システム障害発生等の緊急時に、普段は持たない権限を一時的に付与する機能を提供する。図6に、出張先での入場を申請するワークフローの例を示す。拠点が分散し、従業員の勤務地が固定している企業では、セキュリティ強化のため、入退室可能な場所を勤務地に限定する対策が施される。そこで、この機能を用いて拠点間の出張者の入場を本人の社員証で可能にする。

- ①出張者、又は、受け入れ者が出張先、期間・拠点を指定した入場申請を提出する。
- ②入場を認める権限を持つ人が承認する。
- ③DIGUARD NETを介して、入場申請情報(期間、場所)に基づいて、入退室管理システムの設定を行う。

4. DIGUARD NETを利用した入退室管理連携

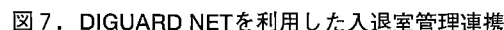
3章で述べた情報システム－入退室管理システム連携ソリューションは、図7に示すように、各システムで管理する次の情報をDIGUARD NETを利用して授受することで実現した。

- ①ユーザー情報、権限情報
- ②通行イベント
- ③装置管理情報

この章では、これらの情報の連携方式について示す。

4.1 組織・役職・申請に基づくアイデンティティのライフサイクル管理

統合ID管理サーバは、アクセス制御ポリシーに基づいた企業全体の統制を行うために、複数のシステムで扱うユーザー情報、情報機器情報、コンテンツ情報のID管理を統一的に行う仕組みを提供する。特に大企業では、認証・認可を必要とする多様なシステムが、地理的に分散して配置されているため、入社・異動・退職などの人事異動情報や、出張・訪問者への一時的な権限付与・取消しに即座に対応する必要がある。そこで機種、拠点ごとに異なるデータ形式の差異を吸収した共通フォーマットで、広域に分散した各システムに安全かつ高信頼で配布するDIGUARD NETの共通プロトコルを利用して実現した。また、大規模な人事異動時の大量変更情報のバッチ投入、来訪者、出張者向けの小規模リアルタイム投入の両者に対応して、ユ



ーザー情報の多様な変化に追随するアイデンティティのライフサイクル管理を可能とした。

4.2 通行イベントの収集・蓄積

入室・退室といった通行イベントを入退室管理システムから即時に提供するDIGUARD NETの共通プロトコルを利用して、在室管理、ログ収集・蓄積機能を提供する。通行イベントは、3.3節で示したように、即時情報として在場・在室管理で利用される。また、情報システムの操作ログと合わせて、異種・広域のログとして収集し、内部統制の監査などで利用する。

4.3 管理情報の監視・設定

DIGUARD NETを介して授受する装置の管理情報を利用して、入退室管理システムの稼働状況の監視、設定情報の変更を行う。全国レベルで広域分散された拠点に管理者を配置した常時管理が必要になる。また、4.1節、4.2節で示した即時の権限設定、即時の通行イベントの利用前に必要となる対象入退室管理システムの現在状況把握に、管理情報が用いられる。

5. む す び

情報システムと入退室管理システムを連携させたソリューションとして、ICカード発行管理、来訪者受付、在場・在室管理、ワークフロー業務連携について述べた。DIGUARD NETを介したユーザー情報、権限情報、通行イベント、稼働状況の授受を、異種広域分散環境で実現することによって、これらの機能を提供した。今後は、映像監視や、他のビル管理設備との連携を図っていく予定である。

参考文献

- (1) 三浦健次郎, ほか: セキュリティ構築プラットフォーム“DIGUARD NET”, 三菱電機技報, **82**, No.4, 249~254 (2008)
- (2) IT Governance Institute, COBIT 4.1 (2007)
- (3) Ferraiolo, D.F., et al.: Role-Based Access Control, Second Edition, Computer Security Series, ARTECH HOUSE (2007)

保健医療福祉分野の情報化を安全と標準で支える ヘルスケアPKI対応ICカードミドルウェア

齋藤和美* 角野章之†
米田 健**
茗原秀幸***

Smart Card Middleware for Healthcare PKI

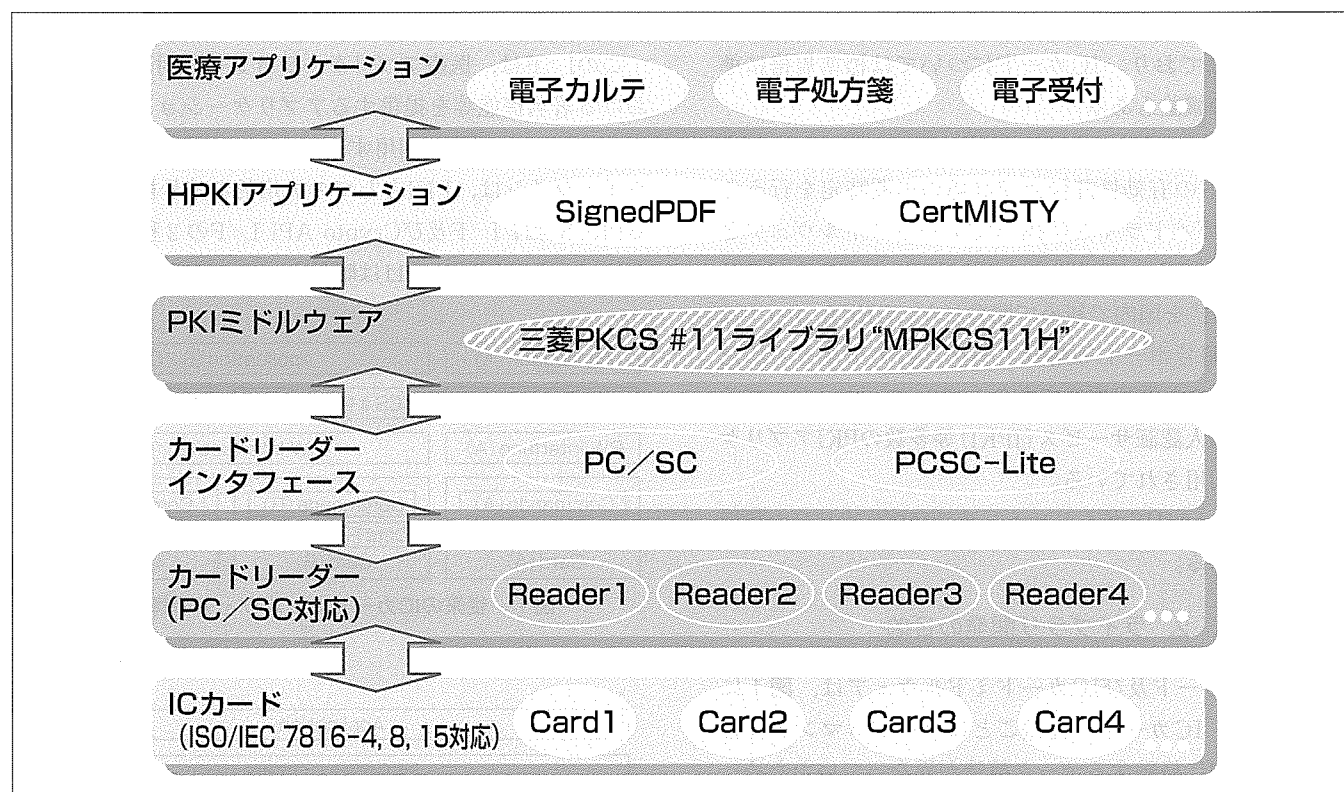
Kazumi Saito, Takeshi Yoneda, Hideyuki Miyohara, Akiyuki Sumino

要 旨

近年、保健医療福祉分野では電子カルテに代表される情報システム化に伴い、ICカードを利用したヘルスケアPKI (Healthcare Public Key Infrastructure: HPKI) による電子署名の利用が普及しつつある。保健医療福祉分野は公的な分野であるため、特定のベンダーに依存しない標準的なICカードが求められる。ICカードの国際標準規格として、ISO/IEC 7816-4, 8, 15が制定されている。これら標準規格に準拠することで、カードインタフェース(I/F)やデータ構造がベンダーに依存しない。保健医療福祉情報システム工業会(JAHIS)は、医療従事者を対象とした“HPKI対応ICカードガイドライン”を2008年中に標準ガイドラインとして制定予定である。この仕様は標準的なICカードを採用し今後国内のヘルスケア分野への適用が見込まれる。

我々は、この仕様に準拠する三菱ICカードミドルウェア

アとしてPKCS #11ライブラリ“MPKCS11H”を国内で初めて開発した。PKCS #11は、ICカードのような暗号トークンにアクセスするためのAPI(Application Program Interface)を定めた業界標準であり、ブラウザや公的個人認証サービス等多数のアプリケーションに利用されている。MPKCS11Hは、通信及びカードI/FにPC/SC(Personal Computer/Smart Card), ISO/IEC 7816-4, 8, 15を採用した。JAHISガイドライン準拠のICカードを用いて、秘密鍵(かぎ)による署名生成や証明書の取得が可能である。署名時のユーザー認証に関してISO/IEC 7816-15とPKCS #11の間で仕様の対応付けが困難な箇所が見られたが、安全性を保持しつつ解決した。今後は、ヘルスケアほか汎用用途に向けた機能拡張を実施していく。



三菱PKCS #11ライブラリ“MPKCS11H”の位置付け

MPKCS11HはJAHISガイドライン準拠ICカードを用いて、秘密鍵による電子署名生成やエンドエンティティ等の証明書取得機能を持つ。PC/SC, ISO/IEC 7816-4, 8, 15等の標準I/Fを使用し、カードやカードリーダーはベンダーに依存しない。三菱電子署名ソフトウェア“MistyGuard”^(注1) <SignedPDF^(注2)> や三菱認証ライブラリ“CertMISTY”^(注1)等を介して医療従事者による電子カルテや電子処方箋等の電子署名をサポートする。

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

(注2) SignedPDF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。

*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(工博) ***三菱電機㈱ 本社 †ジャパンネット㈱

1. ま え が き

近年、電子カルテや電子処方箋等の保健医療福祉分野における情報システム化に伴い、HPKIに対応するICカードの議論が活発である。HPKIは、ヘルスケア分野の公開鍵基盤である。ヘルスケア分野は公的な分野であるため、特定のベンダーに依存しない標準的なICカードが求められる。海外では既にドイツのHPC(Health Professional Card)等の標準的なICカードが運用されている。標準的なICカードは、国際標準規格ISO/IEC 7816-4⁽³⁾、8⁽⁴⁾、15^{(5)(注3)}に準拠するICカードであり、カードI/Fやカード内のデータ構造がベンダーに依存しない。欧米諸国では既にIDカードとしても一般的に利用されている。例えば、ベルギーのBELPIC(BELgian Personal Identity Card)、フィンランドのFINEID(FINnish Electronic IDentification)、アメリカのPIV(Personal Identity Verification)である。国内ではJAHISで医療従事者を対象としたHPKI向けのICカードに対するガイドライン“HPKI対応ICカードガイドライン”⁽¹⁾(以下“JAHISガイドライン”という。)が2008年中に国内で初めてISO/IEC7816-4、8、15準拠の標準ガイドラインとして制定される予定である。JAHISガイドラインは、今後国内の保健医療福祉分野への適用が見込まれる。また、昨年からは厚生労働省で、年金手帳、健康保険証、介護保険証等として利用するための社会保障カード(仮称)の検討が行われており、ICカードについては標準規格に準拠すべきとの議論もある。

我々は、このような国内外の動向に迅速に対応し、標準的なICカードの有効性評価及び課題の早期特定を行うため、JAHISガイドライン準拠のICカードミドルウェアとして標準的なICカードに対応するPKCS #11ライブラリ“MPKCS11H”を国内で初めて開発した。PKCS #11⁽²⁾は、ICカードや暗号ボード等暗号トークンにアクセスするためのAPIを定めた業界標準であり、インターネット・ブラウザや公的個人認証サービス(JPKI)等多数のPKIアプリケーションに利用されている。

本稿では、JAHISガイドライン及びMPKCS11Hの特徴について述べる。

2. ライブラリ開発の目的

従来のICカード及びICカードミドルウェアは、図1に示すように、ICカードの種類ごとにカードコマンド仕様やICカード内に格納するデータ構造が異なっていたため、異なる種類のICカードに対してPKCS #11ライブラリを個別に開発する必要があった。その結果、PKCS #11ライブラリを用いて開発したアプリケーションは、特定メーカー

(注3) ISO/IEC 7816-15は、RSAセキュリティ社によって規定されたPKCS #15を基に策定された。

の特定ICカードしか利用できず、ICカードの選択肢が限定されていた。そこで、図2に示すように標準コマンド及び標準データ構造を前提としたPKCS #11ライブラリを開発し、アプリケーションを変更することなく、異なるメーカーのICカードを利用できる可能性を切り開くことを目的とした。この開発によって、ICカードの選択肢が広がり、性能、価格及び機能に関する顧客要件への柔軟な対応が可能となることが期待される。

標準コマンド及び標準データ構造といっても選択の自由度が高く、あらゆる選択肢に対応して動作を保証するPKCS #11ライブラリを実装することは困難であるため、今回はHPKI等特定用途に必要な十分な機能サブセット及びデータ構造(プロファイル)を定めたJAHISガイドラインを具体的なターゲットとし、実装上の課題の洗い出しを実施した。

3. JAHISガイドライン

JAHISガイドラインは、HPKIにおける相互運用性確保のため、アプリケーションプログラムとのインタフェース、PKIカードアプリケーションの構造、PKIカードアプリケーションのコマンド仕様を定めている。前述のHPKIアプリケーションの構造図とJAHISガイドラインの規定範囲との関係を図3に示す。

3.1 アプリケーションプログラムとのインタフェース

このI/Fは、医療アプリケーション等に対してHPKIにおける署名機能等を提供するアプリケーションがHPKI対応ICカードの機能を利用するためのI/Fである。JAHISガイドラインは、PKIとしての汎用的な暗号機能を提供するPKCS #11 I/F及びCrypto API I/Fの2種類のI/Fを定めている。PKCS #11は暗号トークンの汎用I/Fであり、

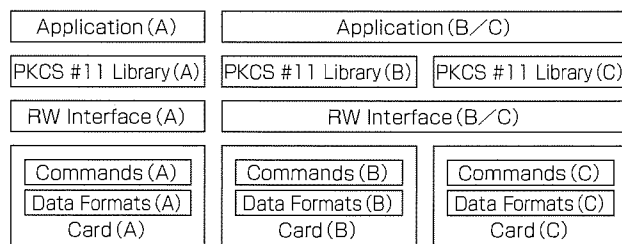


図1. 従来のICカードミドルウェアの構造例

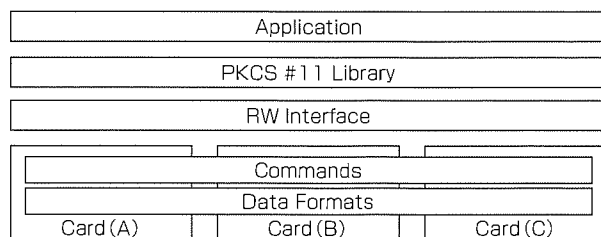


図2. 標準的なICカードミドルウェアの構造例

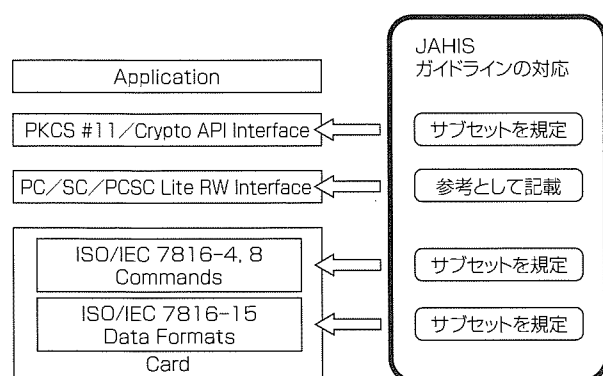


図3. JAHISガイドラインの規定範囲

RSAセキュリティ社によって規定された。Crypto APIはマイクロソフト社が規定した暗号化や署名等の機能を提供するI/Fである。いずれもインターネット・ブラウザや公的個人認証サービス(JPKI)のAPIとして採用されている。アプリケーションはこれらによって、ICカード内に格納されている公開鍵証明書の読み出し機能、電子署名生成機能を利用できる。

3.2 PKIカードアプリケーションの構造

ICカード内に格納する公開鍵証明書や秘密鍵等のデータ構造は、ISO/IEC 7816-15又はJIS X 6320-15⁽⁷⁾の国際/国内標準仕様が採用されている。JAHISガイドラインには、否認防止用秘密鍵1つとエンドエンティティ証明書、ルートCA自己署名証明書、サブCA証明書1、サブCA証明書2の4種類の公開鍵証明書を格納する場合のデータ構造の例が記載されている。

3.3 PKIカードアプリケーションのコマンド仕様

ICカードの機能を利用するためのカードコマンド仕様であり、ISO/IEC 7816-4、ISO/IEC 7816-8又はJIS X 6320-4、JIS X 6320-8⁽⁶⁾の国際/国内標準仕様が採用されている。このコマンドはPKCS #11やCrypto API等の暗号モジュールで利用される。相互運用性確保に必要となるカードコマンドとして公開鍵証明書等のデータをICカードから読み出すREAD BINARY、ICカード内の秘密鍵を用いて署名を行うPERFORM SECURITY OPERATION等が規定されている。

4. 三菱HPKI対応PKCS #11ライブラリの特徴

三菱HPKI対応PKCS #11ライブラリ“MPKCS11H”は、JAHISガイドライン準拠のHPKI対応ICカードを利用することができ、同ガイドラインのPKCS #11 I/Fに準拠し、ICカードの証明書取得、秘密鍵による署名生成等の機能を提供するライブラリである。

MPKCS11Hのサポート機能を次に示す。署名アルゴリズムは、JAHISガイドライン規定のCKM_RSA_PKCSをサポートする。公開鍵証明書はX.509 Ver.3形式に対応す

る。プラットフォームは、Microsoft Windows^(注4) XP、Windows Vista^(注4)、Linux^(注5) (Debian^(注6) 4.0)である。PC/SC対応のICカードリーダーに対応している。

MPKCS11Hは電子署名等のHPKIアプリケーションからの利用を想定している。ICカードへのアクセスは、JAHISガイドラインで規定されたISO/IEC 7816-4, 8のカードコマンドのサブセットを使用して行っている。ICカード内のデータ構造についても同様にJAHISガイドラインで記載されたISO/IEC 7816-15のサブセットに対応する。

4.1 ICカードリーダー及びカード通信の標準化対応

MPKCS11はICカードリーダーとの通信I/FとしてPC/SC(Microsoft Windows)、PCSC-Lite(Linux)を使用している。PC/SCやPCSC-LiteはPS-232CやUSB(Universal Serial Bus)等の物理的I/Fや、ICカードリーダーのI/Fに依存しない汎用的なAPIである。JAHISガイドラインはこれらプラットフォームを参考にしている。

4.2 ISO/IEC 7816-15符号化データ復号機能

HPKI対応ICカードに格納されているデータのうち、公開鍵証明書や秘密鍵等の格納場所を示すディレクトリ情報等はISO/IEC 7816-15の規定に従ってASN.1(Abstract Syntax Notation One)形式で符号化されている。MPKCS11Hはこれらのデータを利用するため、符号化データの復号機能を実装している。

4.3 秘密鍵及び証明書管理機能

MPKCS11Hでは、鍵長2048ビットまでのRSA^(注7)秘密鍵、X.509 Ver.3の公開鍵証明書に対応している。

秘密鍵に関しては、ラベル、ID、公開鍵(modulus及びpublicExponent)による検索が可能である。また、検索された秘密鍵を用いて、署名を生成することができる。署名アルゴリズムはCKM_RSA_PKCSに対応する。CKM_RSA_PKCSはPKCS #1 v1.5規定の署名アルゴリズムのうち秘密鍵演算とブロックタイプやパディングを付加するブロックフォーマットを行うアルゴリズムである。秘密鍵は安全性の観点からICカードの外部に取り出すことはできない。

証明書に関しては、ラベルやIDによる検索が可能である。また、検索された証明書は、ICカードから取り出すこともできる。

4.4 署名時のパスワード認証要否情報取得機能

ISO/IEC 7816-15では署名等による秘密鍵等のプライベートオブジェクトに対してアクセスする際に行う認証の頻度を示すuserConsentという属性が規定されている。しか

(注4) Microsoft Windows, Windows Vista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5) Linuxは、Linus Torvalds氏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6) Debianは、Software in the Public Interest, Inc.の登録商標である。

(注7) RSAは、RSA Security Inc.の登録商標である。

し、今回の実装で参照したPKCS #11 v2.01には対応する属性が規定されていない。そこでPKCS #11の最新の規約v2.20で新規に規定されたCKA_ALWAYS_AUTHENTICATE属性を仕様に取り込むこととした。

CKA_ALWAYS_AUTHENTICATE属性は、PKCS #11の秘密鍵オブジェクトにおける属性の一つであり、この値が真であれば、署名又は復号ごとに毎回認証が要求されることを示す。JAHISガイドラインの例では、秘密鍵に対しuserConsentは1、CKA_ALWAYS_AUTHENTICATE属性は真に設定され、署名ごとに毎回認証が要求される。今回の実装でも、userConsentに1が設定されている場合はCKA_ALWAYS_AUTHENTICATE属性を真に対応付けしておりJAHISガイドラインに準拠する。さらにuserConsentにそれ以上の値が設定されている場合、すなわち認証は署名回数ごとでよい場合もCKA_ALWAYS_AUTHENTICATE属性を真とすることによって安全性を損ねない。

このようにCKA_ALWAYS_AUTHENTICATE属性を真に対応付けることによって、HPKIアプリケーションは署名時に認証が必要か否かを知ることが可能となった。HPKIアプリケーションは安全性を重視してユーザーに対しパスワード入力を毎回促すか、あるいは操作性を重視して通常は代行し必要時のみ入力を促すか等を選択可能である。

4.5 ユーザーパスワード変更機能

ユーザーパスワードの変更機能は、JAHISガイドラインでは標準化対象範囲外の機能である。しかし実運用ではICカード発行時に共通のパスワードを設定し、後日ユーザーが各自個別のパスワードに変更する状況が一般的であるので、この機能を提供する。カードコマンドには、HPCやBEPICのパスワード変更コマンドに利用され、かつISO/IEC 7816-4に規定された標準的なコマンドであるCHANGE REFERENCE DATAを採用した。

4.6 データキャッシュ機能

MPKCS11Hでは、ICカードがリーダーライターに挿入されるとアプリケーション情報や証明書等ICカード内のデータをメモリ上に保存し、そのキャッシュデータを用いて処理するデータキャッシュ機能を提供する。この機能によってSELECTやREAD BINARY等のカードコマンド実行回数は必要最小限に抑えられるため、快適なユーザーレスポンスが得られる。キャッシュデータはICカード操作終了時に削除される。

5. む す び

JAHISによって策定された“HPKI対応ICカードガイド

ライン”に準拠するPKCS #11ライブラリ“MPKCS11H”について述べた。MPKCS11Hは、通信I/FにPC/SCを用い、ICカードとのI/FにはJAHISガイドラインで規定されたISO/IEC 7816-4, 8, 15のサブセットを採用した。MPKCS11H経由でICカードを用いるアプリケーションは、JAHISガイドライン準拠のICカードであればアプリケーションを変更することなく利用が可能となる。

JAHISガイドラインに準拠するHPKI対応ICカードを用いて、ICカード内に格納された秘密鍵による署名生成や証明書の取得が可能である。署名時のユーザー認証の頻度に関してはISO/IEC 7816-15とPKCS #11間で仕様の対応付け困難な箇所が見られるが、安全性を損ねないよう実装を工夫した。また、JAHISガイドラインに規定された機能に加えて、運用上有用な機能であるユーザーパスワード変更機能も標準的なコマンドを用いて実装した。さらに、データキャッシュ機能を搭載することによってカードコマンドの使用回数を抑えて処理の高速化に対応した。

今後は、JAHISガイドラインの改定が行われた際に迅速に対応するとともに、一枚に複数の秘密鍵が格納されたICカードへの対応や、任意のデータを格納可能なデータオブジェクトへの対応、及び暗号アルゴリズムの追加等の汎用用途に向けた機能拡張を実施していく。

参 考 文 献

- (1) JAHIS HPKI対応ICカードガイドライン, 保健医療福祉情報システム工業会 カードシステム委員会(2008)
- (2) PKCS #11 v2.20, <http://www.rsa.com/rsalabs/node.asp?id=2124>
- (3) ISO/IEC 7816-4:2005 Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange
- (4) ISO/IEC 7816-8:2004 Identification cards—Integrated circuit cards—Part 8: Commands for security operations
- (5) ISO/IEC 7816-15:2004 Identification cards—Integrated circuit cards—Part 15: Cryptographic information application
- (6) JIS X 6320-8:2006 ICカード—第8部:セキュリティ処理コマンド
- (7) JIS X 6320-15:2006 ICカード—第15部:暗号情報アプリケーション
- (8) IC・IDカードの相互運用可能性の向上に係る基礎調査シーズ編報告書, 独立行政法人情報処理推進機構(2007)

1000万件のメールを1秒で検索する “LogAuditor Mail Saver”

大塚哲史*
石川雅朗**
加藤 守**

“LogAuditor Mail Saver”: Email Archive Solution with High-Speed Search up to 10 Million Emails per Second
Tetsufumi Otsuka, Masaaki Ishikawa, Mamoru Kato

要 旨

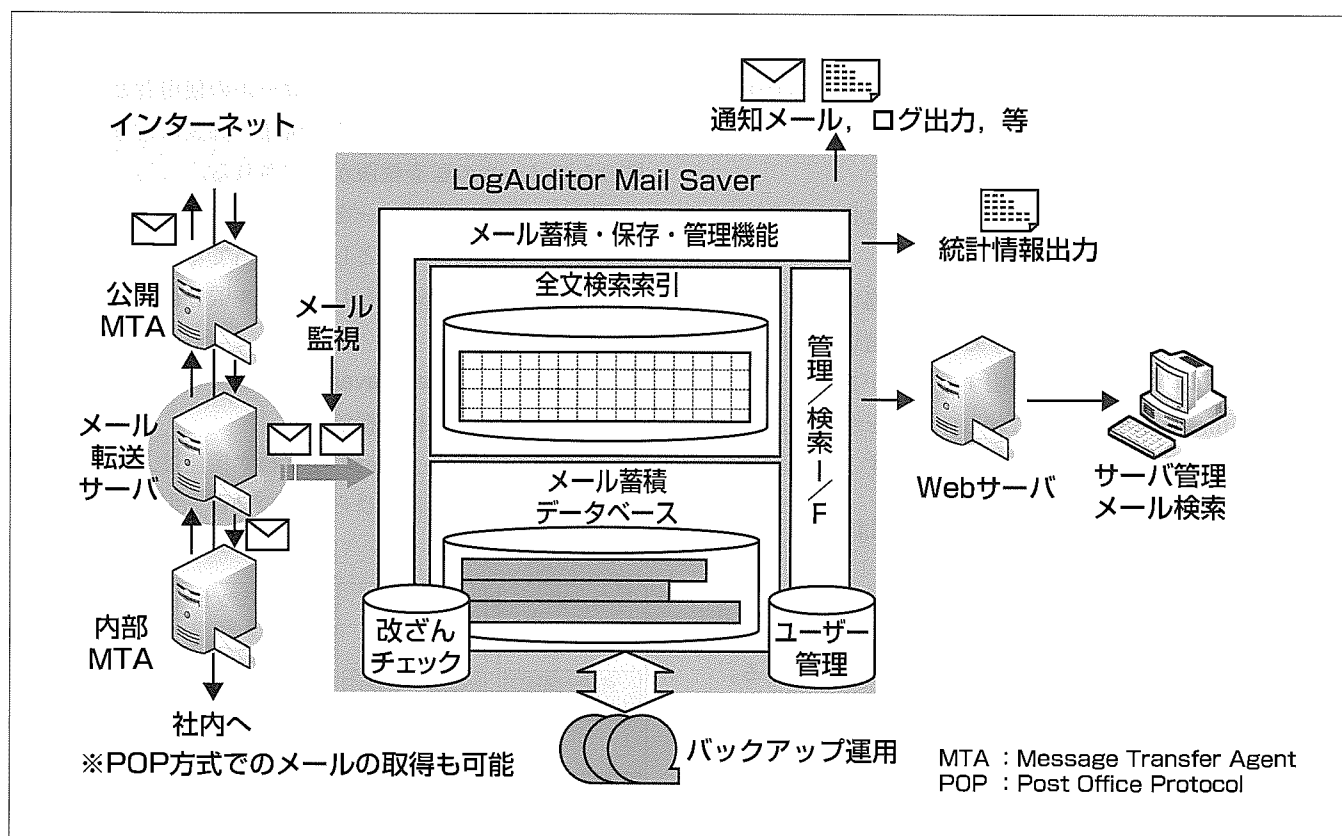
ビジネスツールとして日々利用されている電子メールには、企業の様々な情報はじめ、重要な情報が数多く含まれている。メールは容易に利用できる反面、情報漏洩(ろうえい)などの要因にもなり得る。メールの運用監視策としてメールを長期間保管し、必要な時に監査できるメールアーカイブシステムが不可欠となっている。メールアーカイブシステムの課題としては、大量のメールを保管するためのストレージコスト、大量のメールから目的のメールを取り出すための検索速度、利用者の権限の範囲内で参照するセキュリティの確保などの点にあった。

三菱電機インフォメーションテクノロジー(株)(MDIT)が提供するメールアーカイブソリューション“LogAuditor^(注1)”

Mail Saver”は、三菱電機独自の技術によって、大量のメールの高速蓄積、データ圧縮によるストレージ容量削減、高速全文検索を実現した製品であり、次の特長がある。

- (1) 1 Tバイトのメール(平均メールサイズ約100Kバイトのメールで約1000万通に相当)の中から目的のメールを1秒で検索可能な高速全文検索
- (2) 全文検索索引を含めたアーカイブデータを元メールから最大20%圧縮してストレージ容量を削減
- (3) ユーザー/ロール/メールセットビューの組み合わせによって、利用者に与えられた権限の範囲でメールの検索/表示が可能なユーザー管理を実現

(注1) LogAuditorは、三菱電機インフォメーションテクノロジー(株)の登録商標である。



“LogAuditor Mail Saver”のシステム構成

LogAuditor Mail Saverは大量のメールを蓄積・保存し管理する機能、大量の非定型データの圧縮・蓄積機能を提供するメール蓄積データベース、高速全文検索エンジンの全文検索索引から構成され、管理/検索用フロントエンドとしてWebブラウザで動作する運用管理画面、検索画面を提供する。

1. ま え が き

ビジネスツールとして日々利用されている電子メールには、企業の様々な情報をはじめ、重要な情報が数多く含まれている。メールは容易に利用できる反面、情報漏洩などの要因にもなり得る。内部統制、リスク管理、コンプライアンスの観点から、メールを長期間保管し、必要に応じて迅速にメールを取り出せるメールアーカイブシステムが必要となってきている。

メールアーカイブシステムとは、送受信したすべてのメールを1か所にまとめて保存するシステムを指す。通常は保存してから一定期間は効率的な検索が可能なハードディスクに保存し、一定期間後に順次バックアップメディアへの保存を行うという運用がとられる。

本稿では、従来のメールアーカイブシステムにおける課題、MDITで製品化したメールアーカイブシステムLogAuditor Mail Saverの特長、及び、製品を支えるデータ高速処理技術について述べる。

2. メールアーカイブシステムの課題

メールの容量は添付ファイルなどを伴って増加傾向にあり、送信されるメール数は1998年から2006年までの間に3倍に増加しているという調査結果⁽¹⁾もある。最近では、大企業で送受信されるメールは、年間で数十テラバイト規模に及ぶ事例も見られる。大量のメールを取り扱う必要があるため、従来のメールアーカイブシステムでは次のような課題があった。

- 監査や追跡調査に必要なメールの検索に長時間を要し、効率的な追跡調査が困難
- 長期保管に必要なストレージコストが高い
- すべてのメールを一括保管するため、適切な権限によってメールの参照範囲を制限する必要がある

LogAuditor Mail Saverはこれらの課題を解決し、大量のメールの長期保管と迅速な検索を可能とする。

3. LogAuditor Mail Saverとは

3.1 LogAuditor Mail Saverの特長

LogAuditor Mail Saverは、大量のメールの蓄積・保存・検索を可能とするための機能を提供する製品である。蓄積するメールはメール転送サーバから取得するSMTP (Simple Mail Transfer Protocol) 方式とジャーナル機能で蓄積されたメールを取得するPOP方式でのメールの取得が可能である。主に、次のような特長がある。

(1) 大量メールデータの高速全文検索

1 Tバイトのメール(平均メールサイズ約100Kバイトのメール約1000万件)のヘッダ・本文・添付ファイルの内容を対象として、約1秒で検索する高速全文検索エンジンを

搭載し、長期保存している大量メールへの高速検索を可能としている。

(2) メールストレージコスト削減

従来のメールアーカイブシステムでは、全文検索索引を含めるとストレージ容量が元メールサイズの1.5倍程度に増大するものもあり、大量のメールを長期保存するには、数十テラバイトにも及ぶ大規模なストレージシステムが必要であった。LogAuditor Mail Saverは、全文検索索引の効率化、データ圧縮技術によって、全文検索索引を含め、元メールより約20%容量を削減でき、大量メールの長期保存に対するストレージ容量の大幅な削減を可能としている。

(3) ユーザー管理機能

メールアーカイブシステムへのアクセス管理のみならず、昨今の内部統制、セキュリティ管理要件に対応するため、ユーザー/ロール/メールセットビューの組み合わせによって、利用者に与えられた権限の範囲でメールの検索/表示が可能なユーザー管理を実現している。これによって、上長が部下の送信メールのみを監査する運用を可能とし、人事異動、組織変更などに伴うユーザー管理の変更に柔軟に対応可能である。

図1に、2つの課から構成される営業部で、部下のメールのみを監査する権限の設定例を示す。営業一課ビューとして、営業一課員から送信されたメールのみを検索対象とする設定を行い、営業一課ビューを使用するロールとして営業一課長ロールを設定する。ロールの使用者として営業一課長自身を設定することで、営業一課長は営業一課の課員のみのメールの監査権限が設定される。

同様に、営業二課ビューを設定し、営業一課、営業二課ビューを営業部長ロールとして割り当てることで、営業部長が営業部員のみを対象としたメール監査権限が設定される。

3.2 LogAuditor Mail Saverの主要機能

(1) 漏れのない全文検索機能

LogAuditor Mail Saverの全文検索機能は、カタカナの拗音(ようおん)/促音、ひらがなの拗音/促音、英字の大

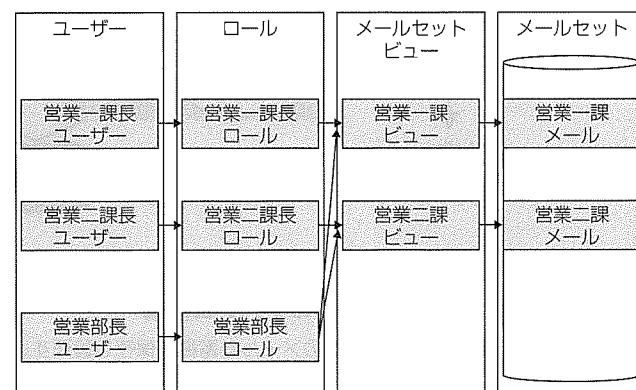


図1. ユーザー管理

文字／小文字，文字の全角／半角などの異表記を同一視した検索や，検索キーワード内の途中の空白や改行を無視した検索にも対応し，漏れのない検索を実現している（図2）。

(2) メール監視機能

メール内容の監視機能によって，メールのアーカイブ時にあらかじめ設定した監視条件に合致するメールが送信されたことを検知し，ログ出力や管理者への通知等を行うことが可能である。これによって，情報漏洩などの事故発生時に迅速かつ効率的に対応が可能となる。

(3) メールの証拠能力を保証する改ざんチェック機能

メール蓄積データベースは，追記型データベースで構成され，上書き，更新ができないシステムとなっている。また，アーカイブ時にハッシュ値を取得し，後日現在のメールデータとハッシュ値を照合することによって，改ざんの有無を検出し，アーカイブメールの真正性を保証することが可能である。

(4) バックアップ機能

メールを月／日単位などの時系列的な“範囲”に分割して管理し，“範囲”を単位としたバックアップ／リストア，削除が可能である。オンラインでの保存期間を過ぎた“範囲”をテープなどにバックアップして削除し，必要に応じてリストアできるようにすることで，ストレージの効率的利用が可能となる（図3）。

(5) 統計情報出力機能

“LogAuditor Basic／Enterprise⁽²⁾”と連携することで，メールアドレス別送受信件数，日付別送受信件数，時間帯

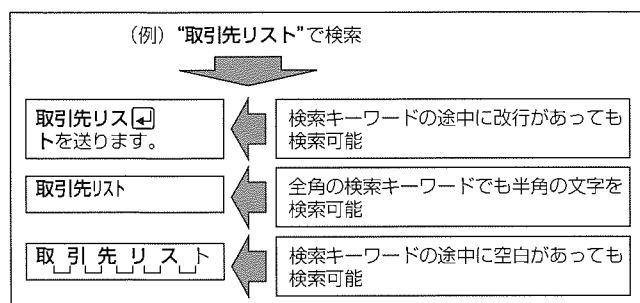


図2. 異表記検索

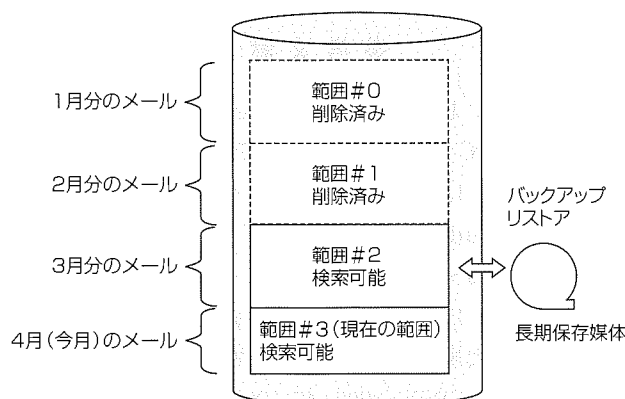


図3. 範囲の概念

別送受信件数などをレポート出力することが可能である（図4）。

(6) Webブラウザによる管理／検索

LogAuditor Mail Saverの管理／検索については，Webブラウザによる画面操作で完結する形で設計されており，クライアント側は，Webブラウザ以外は不要となっている（図5）。

また，管理／検索機能インタフェースとしてJava^(注2) API(Application Program Interface)を提供しており，必要に応じてユーザインタフェースの変更，他のシステムとの連携等に柔軟に対応が可能である。

4. LogAuditor Mail Saverの高速処理技術

LogAuditor Mail Saverは当社独自の大規模データ高速処理アーキテクチャSISA(Scalable Intelligent Storage Architecture)に基づき，大量のメールの高速処理と効率的な管理を実現した。次にその主要技術について述べる。

4.1 構成

メールアーカイブには以下のような特徴がある。

- サイズが可変長であり，従来のデータベースでは効率的に管理できない

（注2）Javaは，米国Sun Microsystems, Inc. の登録商標である。

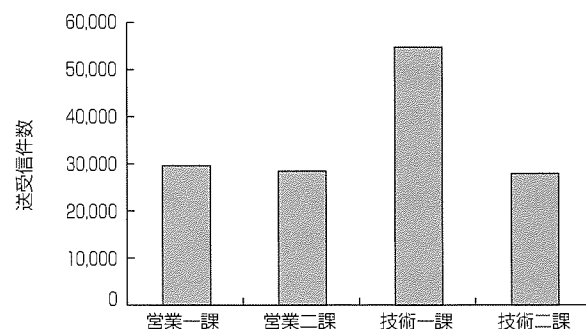


図4. レポート出力力

メールセットビュー	営業一課 営業二課 営業三課
期間(送信日時)	2007年10月1日から 2007年11月11日まで
並び替え(送信日時)	●指定なし ○昇順 ○降順
送信アドレス(From)	
受信アドレス(To, CC)	
件名(Subject)	
添付ファイル名	
添付ファイル有無	●指定なし ○あり ○なし
キーワード (本文, 添付テキスト)	
最大件数	1000件

図5. 検索画面イメージ

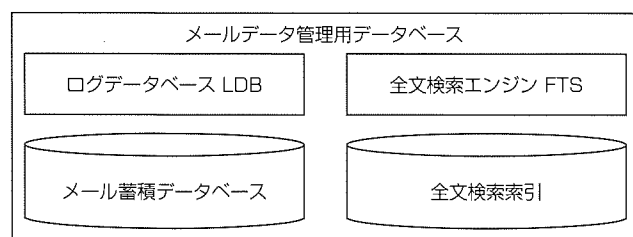


図6. メール管理用データベースの構成

- メール件数が多く、通常のファイル管理ではオーバーヘッドが大きい
- 大量に蓄積されるため、圧縮によるストレージ容量削減が必要
- 時系列に追加されるため、更新は不要
- 日付、件名、アドレス等の属性による検索やキーワード検索機能が必要

このようなメールアーカイブの特徴に対応するために、ログデータベース (Log DataBase : LDB)⁽²⁾ と高速全文検索エンジン (Full Text Search : FTS)⁽³⁾ という2つの技術を組み合わせた当社独自のメールデータ管理用データベースを構築した。図6に構成を示す。

LDBは、時系列的に追加される可変サイズの非定型データを効率的に管理可能な追記型データベースであり、メールを保管するメール蓄積データベースを管理する。高速全文検索エンジンFTSは、キーワード検索を可能とする全文検索索引の管理を行う。

蓄積時にはメールをメール蓄積データベースに自動的に圧縮して保管すると同時に、メールからテキストと属性情報を抽出して全文検索索引を生成する。検索時には全文検索索引によってメールIDを取得した後、そのメールIDによってメール蓄積データベースからメールを取得することが可能である。

4.2 高速全文検索

全文検索エンジンFTSはブロック化n-gram索引方式によって高速化を実現している。ブロック化n-gram索引は、広く利用されているn-gram索引のデータ配置に独自の工夫を加えたものであり、次の特長を備えている。

- 最小限のデータ読み出し
- I/O単位の最適化(バッファサイズの範囲で最大のI/O実行)
- 一方向のデータ読み出し(シークを最小化)
- 複数ストレージへの分散

全文検索索引、メール蓄積データベースともに、複数ストレージへのデータ分散配置と並列処理によって高速化が図られている。全文検索索引では索引の読み出し処理や照合処理を並列に実行し、メール蓄積データベースでは読み出し処理/圧縮・伸張処理を並列化する。これによって、プロセッサ数やストレージ数に応じて処理速度を向上させ

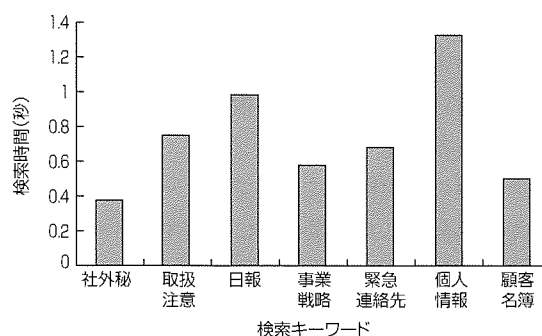


図7. メール1Tバイトの検索時間

表1. アプライアンス・モデルのラインアップ

	小規模向け	中規模向け	大規模向け
モデル			
アーカイブ領域	300Gバイト (最大:2.7Tバイト)	1.8Tバイト (最大:7.6Tバイト)	3.6Tバイト (最大:7.6Tバイト)
メール保存期間	1～3年を想定	1～3年を想定	1～2年を想定
ユーザー数	2,000ユーザーまで	5,000ユーザーまで	10,000ユーザーまで

ることができ、データ規模に応じた処理速度を実現している。

図7に検索時間の一例を示す。1Tバイトのメール(平均メールサイズ約100Kバイトのメール約1000万件)を約1秒で検索することが可能である。

5. む す び

メールを長期間保存し、迅速に取り出すことができるメールアーカイブソリューションLogAuditor Mail Saverについて述べた。今後、内部統制やリスク管理の強化はより重要性が増すと予測されるため、更なるスケーラビリティの拡大強化及び検索・分析機能の充実化を図る予定である。

また、LogAuditor Mail Saverのアプライアンス・モデルとして、LogAuditor Mail Saver AMを製品化している。アプライアンス・モデルでは、ユーザー規模に応じて、ハードウェアも含め、小規模向け、中規模向け、大規模向けの3タイプにサイジングし簡易な導入を可能としている(表1)。

参 考 文 献

- (1) Granz, J, F., et al.: The Expanding Digital Universe, IDC White Paper (2007)
- (2) 郡 光則, ほか: 多種多様なログの統合管理を実現する“LogAuditor Enterprise”, 三菱電機技報, 80, No.10, 615～618 (2006)
- (3) 郡 光則, ほか: 検索機能を備えたストレージシステムによる大規模並列全文検索, 電子情報通信学会技術研究報告, CPSY-2002-47 (2002)

パソコンからの情報漏洩を防止する “CRYPTOFILE PLUS for Vista”

小田切信一*

“CRYPTOFILE PLUS for Vista”: Provides File and Whole Disk Encryption Features

Shinichi Odagiri

要 旨

情報技術(IT)は金融、物流、医療、交通等、様々な社会システムの“神経系”を担うインフラに成長した。高度にネットワーク化された情報社会では便利になった反面、一企業の事件や事故が社会全体に波及することもある。近年、情報漏洩(ろうえい)の事故は多発しており、このような事故が起きると、損害賠償の支払いだけでなく、企業の信頼を失い、時には事業継続が危ぶまれることもある。顧客の信頼を得られる企業として存続し続けるには、情報管理上の事故を最小限にとどめる情報セキュリティ対策が必要である。モバイルパソコンの紛失、電子ファイルの不正コピー、電子メールでのファイル誤送信などの様々な脅威から機密情報を守る対策の第一歩は、機密情報の電子ファイルを暗号化することである。

三菱電機インフォメーションシステムズ(株)(MDIS)では、世界最高水準の暗号技術“MISTY^(注1)”“Camellia^(注2)”を採用

したファイル暗号ソフトウェアとして、Windows Vista^(注3)対応のMistyGuard^(注1)<CRYPTOFILE^(注1) PLUS for Vista>(以下“CRYPTOFILE PLUS”という。)を開発した。

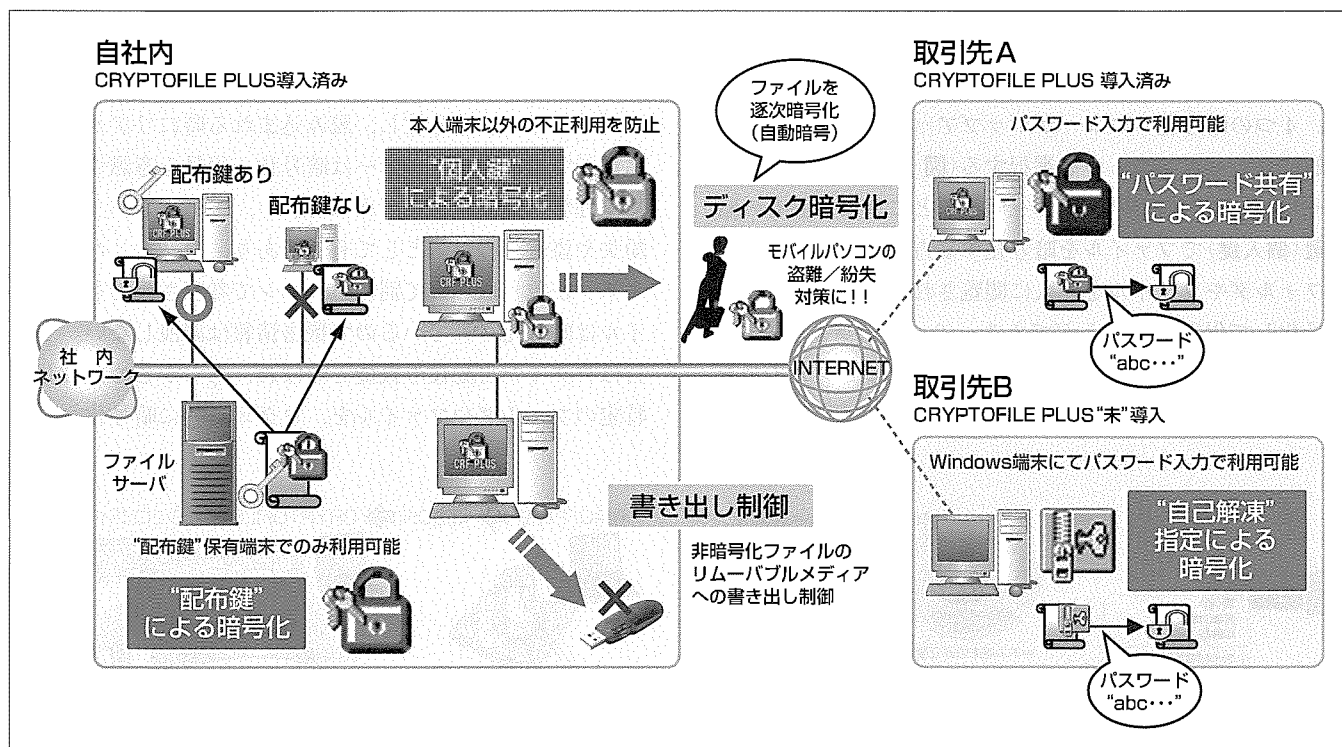
CRYPTOFILE PLUSで機密情報の電子ファイルを暗号化することによって、外部媒体への書き出しや、インターネット経由での外部送信の際に、第三者への情報漏洩を防ぐことができる。また、パソコン内のフォルダやファイルを常に暗号化しておくことで、パソコンの紛失や盗難に対して、第三者からの不正利用を防御できる。

本稿では、CRYPTOFILE PLUSの機能と導入効果を中心に、製品の特長、実現方式、事例について述べる。

(注1) MISTY, MistyGuard, CRYPTOFILEは、三菱電機(株)の登録商標である。

(注2) Camelliaは、日本電信電話(株)と三菱電機(株)の登録商標である。

(注3) Windows Vista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。



CRYPTOFILE PLUSの機能概要

CRYPTOFILE PLUSは、世界最高水準の暗号技術 MISTY, Camelliaを採用したファイル暗号ソフトウェアである。利用シーンに合わせて様々な暗号化機能を提供しており、“個人鍵(かぎ)”による暗号化で本人以外の利用を防止したり、“配布鍵”による暗号化で鍵を持つメンバーとだけ暗号化ファイルを共有したり、“パスワード共有”による暗号化や“自己解凍”指定によって暗号化したファイルを取引先へ安全に送信することができる。また、ハードディスクの自動暗号化でモバイルパソコンの紛失/盗難対策も行える。さらに、暗号化しなければ、USB(Universal Serial Bus)メモリ等へファイルを書き出せないように制御することも可能である。

1. ま え が き

企業・組織のIT化に伴い、各種情報の一元管理が可能となった一方で、個人情報や企業情報などの機密情報が漏洩・流出する事故が多発している。モバイルパソコンの紛失、電子ファイルの不正コピー、電子メールでのファイル誤送信などの脅威から機密情報を守る対策の第一歩はファイルの暗号化である。MDISでは、最新OSであるWindows Vistaに対応したファイル暗号ソフトウェア製品としてMistyGuard<CRYPTOFILE PLUS for Vista>を開発した。本稿では、CRYPTOFILE PLUSの特長、実現方式、事例について述べる。

2. CRYPTOFILE PLUSの特長

CRYPTOFILE PLUSは、高度な安全性と高速なソフトウェア実装性能を特長とする、世界最高水準の暗号技術MISTY, Camelliaを採用したファイル暗号ソフトウェアである。

CRYPTOFILE PLUSで機密情報の電子ファイルを暗号化することによって、外部媒体への書き出しや、インターネット経由での外部送信の際に、第三者への情報漏洩を防ぐことができる。また、パソコン内のフォルダやファイルを常に暗号化しておくことで、パソコンの紛失や盗難に対して、第三者からの不正利用を防御できる。

次に、この製品の特長について述べる。

2.1 多彩なファイル暗号方式

ファイルやフォルダを選択してマウスを右クリックすると、4つの暗号化メニューがポップアップ表示されるので、目的に合わせてメニューを選択する(図1)。1つ目のメニュー“ファイルの暗号化”はユーザーごとに異なる固有の暗号鍵(個人鍵)でファイルを暗号化する方式であり、個人用のフォルダやファイルを他人に閲覧されたくない場合に、暗号化して保護することができる。2つ目のメニュー“共有ファイルの暗号化”はパスワードを設定してファイルを暗号化する方式である。暗号化したファイルは、パスワー

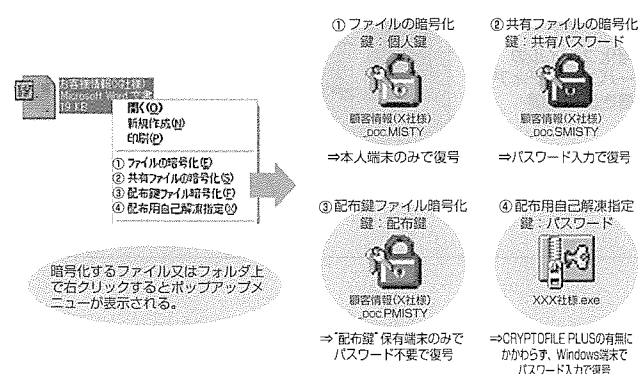


図1. ファイルの暗号化メニュー

ドを知っている者だけが復号できるので、CRYPTOFILE PLUSをインストールしている社内/社外の関係者と安全にファイルを共有したり送受信したりすることができる。3つ目のメニュー“配布鍵ファイル暗号化”は関係者だけにあらかじめ配布された暗号鍵(配布鍵)でファイルを暗号化する方式である。配布鍵を持っている者だけが復号できるので、社内の共有ファイルサーバに暗号化ファイルを安全に保管しておくことができる。なお、配布鍵はあらかじめ各自のパソコンに登録しておく必要があるが、配布鍵ファイルの作成者が設定したパスワードを知らなければ登録できないようになっている。4つ目のメニュー“配布用自己解凍指定”はパスワードを設定してファイルを暗号化する方式の一種で、暗号化ファイルとそれを復号するためのプログラムが結合した自己解凍型の実行ファイルを作成する。このため、CRYPTOFILE PLUSをインストールしていないパソコンでも、パスワードを知っていればファイルを復号することができる。インターネット経由で取引先にファイルを送信する際に、データを暗号化して安全に送信する場合に有効である。なお、この自己解凍型の暗号化ファイルは、復号時のOS環境が日本語でなければ、英語の画面を表示して復号できるようになっている。

2.2 ファイルの自動暗号化機能

CRYPTOFILE PLUSは3種類の自動暗号化機能をサポートしている。1つ目は逐次暗号化機能と呼ばれ、OSやプログラムのフォルダ(C:\¥Windows, C:\¥Program Files等)を除いて、ハードディスク上のファイルを常に暗号化しておく機能である。ファイルが書き込まれる時にリアルタイムに暗号化し、読み込まれる時にリアルタイムに復号するので、ユーザーは暗号化/復号を意識することなく通常の業務操作を行える(図2)。モバイルパソコンの紛失や盗難への対策として有効であり、たとえ、ハードディスクが抜き取られて別のパソコンで参照されても、ファイルは暗号化されているので機密情報は漏洩しない。2つ目はログイン自動復号機能と呼ばれ、あらかじめ定義した特定のフォルダやファイルを、ログオフ時に暗号化しログ

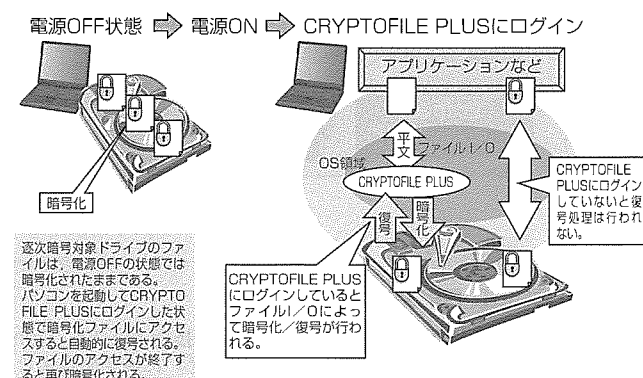


図2. 逐次暗号化機能

オン時に復号する機能である。業務中は作業のために常に復号しておき、パソコンシャットダウン時は忘れずに暗号化する場合に有効な機能である。3つ目は定期自動暗号化機能と呼ばれ、あらかじめ定義した特定のフォルダ内を単位の定期間隔で監視し、暗号化されていないファイルが見つければ、個人鍵や配布鍵で自動暗号化する機能である。ユーザーがファイル暗号化の操作をしなくても、ファイルが特定のフォルダ下であれば、自動的に暗号化されて第三者のアクセスから保護される。

2.3 暗号化していないファイルの持ち出し抑止

CRYPTOFILE PLUSは、暗号化操作をした時だけ、リムーバブルメディア(USBメモリ、SDカード、フロッピーディスク、外付けハードディスク等)へのファイル書き込みを許可し、それ以外の場合は、リムーバブルメディアへの書き込みを抑止する機能を持っている。この機能を有効にした場合、ユーザーは暗号化していない平文のファイルをリムーバブルメディアにコピー／移動／新規作成することはできない。マウスの右クリックメニューで暗号化を実行した時だけ、リムーバブルメディアへ暗号化ファイルを書き込むことができる。なお、リムーバブルメディア上にすでに存在するファイルの読み込みは、今までどおり、普通に実行できる。この機能はリムーバブルメディアの紛失や盗難の対策に有効な機能である。

2.4 ファイル操作履歴の記録

CRYPTOFILE PLUSは、ファイルの読み込み／書き込み／削除／移動／リネームを監視しており、ログファイルに履歴を記録する機能を持っている。監視対象はローカルディスクだけでなくリムーバブルメディアやファイルサーバ(共有フォルダ)へのアクセスも含まれる。ログファイルはCSV(Comma Separated Values)形式のテキストファイルで、“年月日、時分秒、コンピュータ名、IP(Internet Protocol)アドレス、ログインユーザー名、プログラム名、ファイル名、操作種別”の操作履歴情報が記録される。このログ情報は、許可されていない操作を検出したり、セキュリティ事故発生時の原因を特定したりするためのデータとして、有力なツールである。

2.5 運用面の利便性

CRYPTOFILE PLUSのインストーラは、システム管理者が、各種機能の有効／無効や自動暗号化するフォルダ、設定変更を許可する場合のパスワード等を定義して作成する。そして、作成したインストーラを各部門の取りまとめ者(ユーザー管理者)に配布して、社内のパソコンへ展開する。ユーザー管理者には多くの保守ツールが用意されており、個別のパソコンの事情に合わせた設定変更や維持管理の作業負担を軽減している。また、ユーザーが暗号鍵をなくしたり暗号化パスワードを忘れて復号ができなくなった場合に、暗号化ファイルを復号する特別な保守ツ

ルも用意されている。さらに、すべてのパソコンで設定変更が必要となった場合の作業負担を軽減するツールも用意されている。システム管理者は、変更情報を定義した暗号化ファイルを作成し、このファイルを市販のファイル配信ツールで、各パソコンの所定のフォルダ下に配信することによって、一斉に設定変更することも可能である。

3. CRYPTOFILE PLUSの実現方式

図3に示すように、CRYPTOFILE PLUSはOSのユーザーモードとカーネルモードで暗号化機能を実現しており、逐次暗号化機能はカーネルモードで動作するフィルタドライバで処理している。フィルタドライバは、OS起動時(ファイルシステムドライバロード時)に登録され、この時点から、すべてのファイルI/OはCRYPTOFILE PLUS逐次暗号化フィルタドライバを経由することになるが、未だ暗号化処理は開始されない。ユーザーID／パスワードでWindowsへのログインが完了しCRYPTOFILE PLUSユーザーとしての認証が完了すると、暗号鍵がCRYPTOFILE PLUS逐次暗号化フィルタドライバに設定され、AES(鍵長128ビット)による逐次暗号化処理が行われるようになる。なお、暗号化していないファイルのリムーバブルメディアへの持ち出し抑止機能やファイル操作ログの機能も、このフィルタドライバがすべてのファイルI/Oを監視することで実現している。

ユーザーモードで動作するアプリケーションでは逐次暗号化以外の暗号化を処理している。配布用自己解凍型暗号化ファイルにはCamellia(鍵長128ビット)、それ以外の暗号化ファイル(個人鍵、配布鍵、パスワードによる暗号化)にはMISTY(鍵長128ビット)を採用し、信頼できる高い技術で暗号化を実現している。

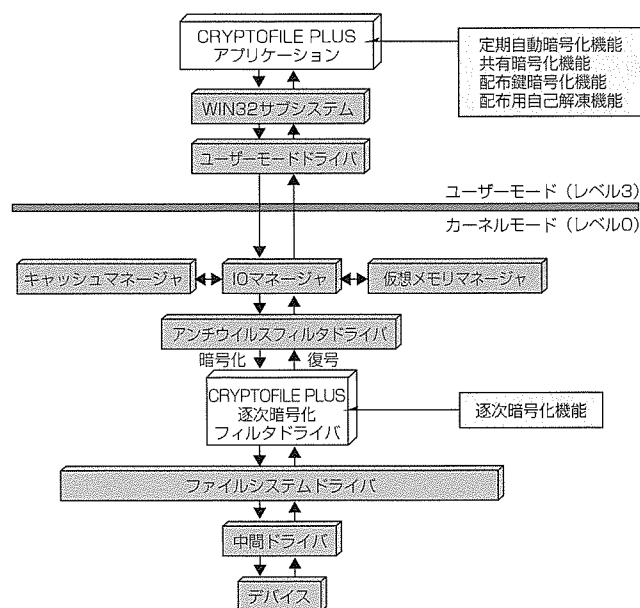


図3. 各種暗号機能の処理レイヤ

4. CRYPTOFIELD PLUSの適用事例

図4にCRYPTOFIELD PLUSの典型的な適用事例を示す。

4.1 ノートパソコン(モバイルパソコン)からの情報漏洩防止

紛失や盗難のリスクに備えて、持ち運びできるすべてのノートパソコン(モバイルパソコン)に逐次暗号化を設定しておけば、機密情報が漏洩する心配がなく安心である。ハードディスク上のファイルは常に自動的に暗号化されているので、どこかに置き忘れたり、だれかに持ち去られたりしたとしても、パソコン内の機密情報ファイルを第三者が閲覧することはできない。また、逐次暗号化機能には、パソコンの利用者が暗号化/復号を全く意識する必要がないというメリットがある。ユーザーは、面倒な手間や負担を感じることもなく、今までどおりに快適に業務操作を行える。ワープロソフト等のアプリケーションでファイルの作成や上書き保存、また、エクスプローラでのファイル移動やコピー等のファイル操作を行うだけで、ハードディスク上のファイルは常に自動的に暗号化されて安全に保管することができる。

4.2 リムーバブルメディアからの情報漏洩防止

USBメモリや外付けハードディスク等のリムーバブルメディアに、自由に、ファイルをコピーしたり、書き出ししたりできると、機密情報が漏洩するリスクが高くなる。そこで、CRYPTOFIELD PLUSの機能で、暗号化していないファイルのリムーバブルメディアへの書き出しを抑制する。このように設定しておく、ユーザーは、アプリケーションやエクスプローラの操作でリムーバブルメディアへファイルを書き出すことができない。リムーバブルメディアからファイルを読み込むことしかできなくなる。リムーバブルメディアへ書き出すにはCRYPTOFIELD PLUSの暗号化操作をしなければならないので、リムーバブルメディアへの持ち出しは必ず暗号化する運用を徹底することができる。

また、リムーバブルメディアは、CRYPTOFIELD PLUSの機能で暗号化メディアにフォーマットすることもできる。暗号化メディアにしておけば、ローカルディスクの逐次暗号化の場合と同様に、リムーバブルメディアへのファイル書き込み時に自動的に暗号化され、読み込み時は自動的に復号される。ユーザーが暗号化を意識しなくても自動的にファイルが暗号化されるので、リムーバブルメディアを紛失した場合に、そのメディアの中に保存したファイルやバックアップ・データから機密情報が漏洩することを防止できる。

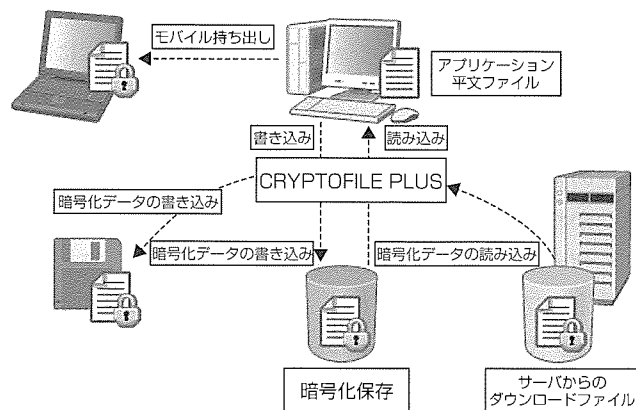


図4. CRYPTOFIELD PLUSの適用事例

4.3 プロジェクトメンバーのみでの情報共有

特定のプロジェクト内でのみ共有する機密データを部外者に漏洩させないようにするには、プロジェクトメンバーのみに配布した暗号鍵(配布鍵)でファイルを暗号化しファイルサーバに保管する。復号にも、配布鍵を使用するため、鍵を持たない部外者は復号できず、鍵を持つプロジェクトメンバーだけがファイルサーバからダウンロードして復号し機密情報を共有することができる。頻繁に暗号化/復号を繰り返して更新するような共有ファイルは、パスワードで暗号化するよりも配布鍵を指定して暗号化する方が、入力が少なく簡単に操作できる。

4.4 自分以外の第三者による不正利用の防止

自分以外の者が、個人のファイルに不正にアクセスして勝手に閲覧されないようにするには、個人鍵で特定のフォルダを定期自動暗号化しておく。当該フォルダ下にあるファイルは、分単位の定期間隔で監視され、暗号化されていないファイルが見つければ個人専用の暗号鍵で暗号化される。本人であれば暗号化ファイルのダブルクリックで簡単に復号できるが、第三者は復号することができない。なお、定期自動暗号化のフォルダには、ファイルサーバ上の共有フォルダを指定することも可能である。

5. む す び

情報漏洩対策は、社会的責任として、企業規模にかかわらず必要なことである。CRYPTOFIELD PLUS for Vistaは、企業の情報セキュリティを守るソフトウェア製品として期待されているので、今後も更なる機能強化を図っていく所存である。

磯西徹明* 安齋利典**
鈴木靖宏* 粕谷俊彦**
大矢富保**

Tetsuaki Isonishi, Yasuhiro Suzuki, Tomiyasu Oya, Toshinori Anzai, Toshihiko Kasuya

今後、放送と通信の融合が促進され、メディアのシームレス化が進むとともに、企業ウェブサイトは会社機能の中核を担うと考えられる。MDISはこうした目まぐるしい社会環境の変化に応じて高いサービスレベルを確保した企業ウェブサイトの構築・アプリケーション開発・運用保守ソリューションを提供し、企業ウェブサイトの価値向上、発展に寄与していく。



1. ま え が き

宣伝部の企画、運営する三菱電機オフィシャルウェブサイトMDISは、

- ①安定的かつ迅速な最新情報の発信
- ②ウェブマーケティングツールを活用した販売促進支援
- ③信頼性の高いセキュアなウェブサイトの実現

を目的として、インフラ／システム構築・運用・保守、アプリケーション開発・保守及びコンサルティングを実施している。また品質改善、業務効率化、信頼性向上のためのPDCA(Plan-Do-Check-Action)を実践することによって、ウェブサイトの信頼性及び情報セキュリティの維持・向上を実現した。本稿では、三菱電機オフィシャルウェブサイトの概要とそれを支えるMDISの企業ウェブサイト構築・運用ソリューションについて述べる。

2. 社会環境の変化

近年、個人情報保護法(2005年4月)、会社法(2006年5月)、改正消費生活用製品安全法(2007年5月)等の法整備・法改正があり、企業ウェブサイトはあらゆるステークホルダーに対する社会的責任の意思表示、不特定多数に対する情報発信の場として位置付けられ、セキュリティレベルと信頼性の向上が求められている。またコンピュータ事業者のテレビ局との連携強化やテレビ局のネット配信への進出というような放送と通信の融合が進みつつあり、コンピュータ、通信、放送、それぞれの業界の生き残りをかけた覇権争いが激化している。そのため情報の垣根がなくなり、メディアのシームレス化が進んでいく。こうした状況下で、企業ウェブサイトはもはや単なる情報発信の場にとどまらず、企業価値向上のための自社情報発信“メディア”として、情報の帰着点、集約点となる必要性がでてきている。

3. 三菱電機オフィシャルウェブサイトの概要

宣伝部で実施している三菱電機オフィシャルウェブサイトの企画、運営にあたっての方針及び施策について述べる。

3.1 企業情報発信力強化(サイトマネジメント)

従来、“会社概要”“環境報告”のような企業情報は、まず印刷物のためにまとめた情報をウェブサイトに転用してきた。このサイクルでは最新の情報発信にはならないため、企業情報を印刷物先行ではなくウェブ先行の情報提供に切り替え、発信力を強化した。これによってすべてのステークホルダーに対して常に最新の詳細情報を提供できるようになっている。また、様々な企業情報をウェブサイトに集約し、一元的に管理するワンソースマルチユース化を図ることで、統一的な情報提供を可能とした。さらに、ステークホルダーに対して三菱電機に関する理解を一層深めても

らう目的で、社会・生活に貢献している三菱電機の技術と動きのあるリッチなコンテンツで伝える“キー・テクノロジーサイトTechno-Spiral(テクノスパイラル)”を公開している(図1)。

3.2 ウェブマーケティングツールとしての活用

三菱電機では、オフィシャルウェブサイトを通じて、①メール配信による顧客との接点創出、②キャンペーンなどでの新規顧客の誘引、③顧客データベースを利用した特定顧客向けの情報発信、④顧客の囲い込みなどを実施し、すべてのプロセスを連携させる運用支援体制を確立している。これによって顧客の関心度を高め、アクセス頻度などを含めたユーザーニーズの収集を行いつつ、製品企画／販売戦略へフィードバックすることで、顧客とのWin-Winの関係を築いている。

3.3 先進的技術を取り入れたユーザビリティの向上

高いユーザビリティ、アクセシビリティを実現するために、デザインガイドラインを策定し、グローバルヘッダの統一やオフィシャルウェブサイト全体の制作基準、SEO(Search Engine Optimization)／LPO(Landing Page Optimization)のための留意事項等を定義している。また、アクセスログ解析・分析、ユーザーアンケート調査による定量評価に加え、三菱電機㈱デザイン研究所や外部コンサルティング等専門家による感覚的な評価を含む定性評価も実施している。これら各種の評価を活用して、PDCAサイクルを継続して実施し、常にレベルの高いユーザビリティへと改善を進めている⁽²⁾。またキーワードでサイト内を検索する機能にキャプチャ画像を付けることで(図2)、ページの見つけやすさを向上させ、初心者や高齢者などウェブに不慣れな人々でも目的のページを簡単に見つけられる機能(MARSFINDER^(注1))やアクセシビリティに関するJIS X8341-3対応の、HTML(HyperText Markup Language)からテキスト版のウェブページを自動生成する機能(SimpleWeb^(注2))、会社情報ではメニューの中から印刷したいページを選ぶことや表紙や目次を付けて全ページ一括印刷

(注1) MARSFINDERは、Marsflag社の登録商標である。

(注2) SimpleWebは、ソシオメディア㈱の登録商標である。



図1. 会社情報サイトとTechno-Spiral



図2. キャプチャ画像付きサイト内検索画面

ができる機能(サイトプリントシステム^(注3))といったような先進的な技術を導入し、利便性の向上を図っている。

3.4 情報セキュリティの確保(ウェブインフラ)

オフィシャルウェブサイトでは、多岐にわたる企業活動を顧客へ正確かつタイムリーに発信する一方で、顧客へのサービスを向上させるために個人情報の取得・管理・活用も行っている。宣伝部は長年にわたりオフィシャルウェブサイトの運営に関し、技術的なセキュリティ対策と組織全体のマネジメントの両面から情報セキュリティマネジメントの確立をめざしてきた。その結果、2005年9月29日第三者審査登録機関である(株)日本情報セキュリティ認証機構(JACO-IS)から“三菱電機オフィシャルウェブサイトの開発・運用・保守業務”についてISMS(Information Security Management System)認証を取得し、2006年10月23日にはISMS認証の国際規格ISO/IEC 27001及びこれに対応した日本工業規格JIS Q27001への移行審査に合格している。また三菱電機としては(財)日本情報処理開発協会から個人情報の適切な取り扱いを行う事業者と与えられる“プライバシーマーク”の認定も受けている。企業活動で重大な問題が発生した際、すぐさまオフィシャルウェブサイトでの情報提供の危機管理対応についての検討も進めており、ワークフローや重要度に応じた緊急告知表示の範囲等を策定中である。

4. 三菱電機オフィシャルウェブサイトを支えるサイト構築・運用ソリューション

オフィシャルウェブサイトは、宣伝部で企画／運営、デザイン、施策立案を実施し、それを支えるために、土台となるインフラ整備、システム構築、アプリケーション開発、運用／保守をMDISが実施してきた。次にMDISの提供するソリューションについて述べる。

4.1 企業ウェブサイト向けワンソースマルチユースサイト構築ソリューション

MDISは、コンテンツ管理システムとデータベースを組み合わせてワンソースマルチユースを実現したウェブサイト^(注3) サイトプリントシステムは、(株)COMの商標である。

ト構築サービスを提供する。コンテンツ管理システムは、ウェブサイトのコンテンツを一元的に管理し、コンテンツの新規作成、更新を迅速に行うことができ、かつその履歴を管理するシステムである。テンプレート機能を利用するとだれが作成しても同レベル、同品質のコンテンツを作成することができるという利点がある。さらにCSS(Cascading Style Sheet)の選択による自由度の高いレイアウト表示やアクセス解析用スクリプト埋め込みの自動化、ウェブページ及び印刷用ページの同時生成機能を実現している。またデータベースと組み合わせることでウェブページそのものや画像データのワンソースマルチユースも可能である。特に企業情報(会社概要、事業概要、製品情報等)をデータベース化し、コンテンツ管理システムと連携させることによって、企業価値向上につながる、迅速かつ的確な“ウェブ先行型の情報発信”を行えるようになる。

4.2 企業ウェブサイト向け効果測定ソリューション

MDISは、顧客との接点創出から顧客獲得、顧客への情報発信までをトータルにカバーするウェブマーケティングとアクセスログ解析システムを組み合わせたソリューションを提供する。

このソリューションによって、問い合わせや展示会・セミナーの申し込みから顧客データ管理、顧客へのメール配信までを行いつつ、様々な施策／リニューアルによるアクセス数の変化や検索エンジンからのユーザー流入率などの効果を評価できる。評価結果から課題を洗い出し、ウェブサイト改善に役立てることで、企業ウェブサイトを発展させることが可能である。

4.3 ASPサービスのインテグレーション

顧客に利便性の高いインタフェース、ユーザビリティ、アクセシビリティを提供するため、3.3節で示したようなサービス(キャプチャ画像付きサイト内検索など)が各種ASP(Application Service Provider)で提供されている。MDISはこれらサービスを企業ウェブサイトを導入するためのインテグレーションを提供している。既存のリソースとASPの提供するサービスをシームレスにすることでユーザビリティ、アクセシビリティを一層向上させることができる。

4.4 ウェブサイト運用保守・監視ソリューション

企業のウェブサイトは高度なスキルとサービス改善の仕組みが組み込まれた高レベルなシステム運用保守が必要となる。MDISはITIL(Information Technology Infrastructure Library)をベースとした高レベルな運用保守・監視ソリューション⁽³⁾を提供する。これはSLA(Service Level Agreement)の締結及びSLAを基にした品質改善、業務効率化、信頼性向上のためのPDCAを実践し、企業ウェブサイトの信頼性向上、情報セキュリティレベルの維持、レベルアップを行うものである。

表1. 三菱電機オフィシャルウェブサイトの具体的施策及び効果

項番	項目	具体的施策	効果
1	企業情報発信力強化 (サイトマネジメント)	①アニュアルレポート、環境・社会報告書等 会社情報のウェブ先行型発信と刊行物の整理 ②企業／事業情報の集中管理と運営母体の組織化 ③企業／事業情報のワンソースマルチユース化 (データベース化)推進 ④キーテクノロジーサイト“Techno Spiral”の新設・充実 ⑤関係会社製品情報の取り込み及び各製品サイトへの 導線確保。お問い合わせの設置等による商談機 会の創出 ⑥SEO対策、LPO対策	①ウェブ先行型発信による最新企業／事業情報の統一提供 ・会社情報サイトリニューアル後のアクセス数が従来比で2.5倍(CSR(Corporate Social Responsibility)1.7倍、環境報告1.4倍、 社会貢献活動1.4倍、資材調達4.8倍)、採用情報は学生のアレントリー数増加 ・ウェブ先行型情報発信：“アニュアルレポート”・“環境・社会報告”をウェブで発信し紙資源を有効活用等 ②情報の一元管理と組織化による円滑な情報発信の実現、及びシナジー効果による情報発信力強化 ・週刊ダイヤモンド2007年9月15日号：“ウェブサイト価値ランキング2007”電子・電機業界第7位(全体49位) ・日経パソコン2007年10月8日号：“企業サイトランキング2007”17位 ・第1回企業ウェブグランプリ(2007年12月17日発表)の“クロスコーポレート＆コラボレーション部門”で第2位 ・日興アイ・アール株“2007年度 全上場企業ホームページ充実度ランキング調査”で18位 ③CMS(コンテンツ管理システム)導入によるワンソースマルチユース化(サイト用ページとプリント用ページの同時生成)、コンテンツの作成・修正時間の短縮化、サイト管理システムによる必要ページのプリント ④ウェブコンテンツによる技術の分かりやすい訴求・認知向上 ⑤各製品サイトのアクセス・問い合わせの増加 ⑥SEO：検索結果の上位掲出、適切な誘引とアクセス増加、LPO：効果確認中
2	ウェブマーケティング ツールとしてのオフィ シャルウェブサイト	①デザインガイドラインによるフォーマットの統一とクオリティの標準化 ②会員制サイト構築(DB構築管理、ポイント管理) ③メール配信・キャンペーン・アンケート等のウェブマーケティング (誘引・顧客DB化・情報収集・ポイント制による囲い込み等) ④アクセスログ解析、動線分析などによる効果測定	①ページ品質の向上とコーポレートイメージの確立 ②会員によるマーケティング母体の確保 ③ユーザーとの接点創出からサイトへの誘引、顧客データベースに基づく販促支援／開発支援、 顧客の問い合わせのすべてのプロセスを連携させる運用支援体制を確立 ④閲覧状況把握とサイト構築への反映
3	先進的技術を取り入れ たユーザビリティ向上	①テキスト版ウェブの提供 ②キャプチャ画像付き検索結果一覧表示機能の提供 ③会社情報コンテンツの選択／一括プリント機能の提供 ④デザイン研究所・外部コンサルティング等専門家の定量的・定性的評価によるPDCAサイクル	①高齢者、障害者等への配慮(アクセシビリティ向上) ②ウェブサイトの使いやすさ向上(ユーザビリティ向上) ③刊行物削減とニーズにあったプリントの提供 ④ユーザビリティの継続的改善
4	情報セキュリティの確保 (ウェブインフラ)	①技術的なセキュリティ対策と組織全体のマネジメント ②統合運用監視システム導入 ③ウェブサイトの危機管理対応ワークフロー作成 ④PMO(Project Management Office)によるプロジェクト管理 ⑤障害管理のPDCAサイクル実施	①ISMS取得及びISO・IECとJIS規格への移行と三菱電機としてのプライバシーマーク取得による安心できるサイトの実現 ②運用監視作業の効率化及びコスト削減 ③危機管理対応構築の準備 ④障害発生件数の減少

5. 三菱電機オフィシャルウェブサイト施策及びソリューションによる効果

宣伝部は絶えず三菱電機オフィシャルウェブサイトに対する施策を行い、定量・定性評価を継続的に実施し、PDCAサイクルを回すことでサイト改善を実施している。これまでに実施してきた三菱電機オフィシャルウェブサイトの具体的施策及び効果を表1に示す。その結果、月間ページビュー数、会員数、メール配信数は年々上昇している(図3)。2006年度後半から2007年度にかけては、多彩な企業情報を発信する“会社情報”サイトをリニューアルし、それぞれのサイトのシナジー効果を高めたことによって、“企業サイトランキング2007(日経パソコン2007年10月8日号)”で17位を獲得している。

6. む す び

今後、宣伝部ではウェブサイトの位置付けの変化に対応して、オフィシャルサイトを自社情報発信“メディア”として活用しつつ、情報の帰着点、集約点(情報のハブ)とするため発展させていく。それに向け、企業価値向上のため企業情報の充実を図るとともに商談機会を創出し、三菱電機及び関係会社の事業活動に貢献することをめざしている。

さらにオフィシャルウェブサイトを宣伝、広報、IR(Investor Relations)、採用、営業支援等の情報発信の核とし、ビジネスインフラの一角として社員が最新の情報をビジネスに活用するための“ビジネスエンジン”として展開していく予定である。加えて、IT新改革戦略・u-Japan政策の目標年度、通信・放送法改正、第4世代携帯電話導入

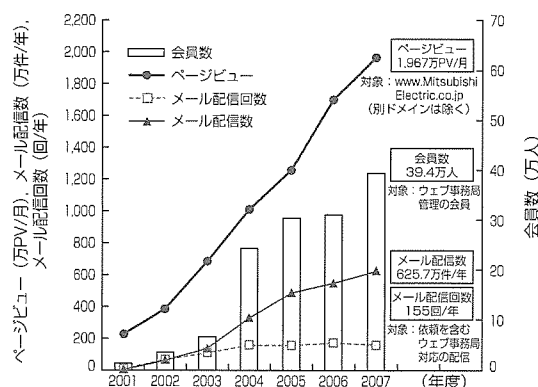


図3. 三菱電機オフィシャルウェブサイトの施策による効果

の2010年、地上波デジタル放送本格化の2011年以降に向けた検討も開始した。

MDISは宣伝部との連携を強めながら、先進的なソリューションを確立し、めまぐるしく変化する社会環境に対応した企業ウェブサイトを支える構築・運用ソリューションを市場に展開する。

参考文献

- (1) 三菱電機オフィシャルウェブサイト：
<http://www.MitsubishiElectric.co.jp/>
- (2) 三菱電機(株)デザイン研究所 編：こんなデザインが使いやすいを生むー商品開発のためのユーザビリティ評価ー，工業調査会 (2001)
- (3) 磯西徹明，ほか：安全，安心を実現する高レベルWebサイト運用保守・監視ソリューション，三菱電機技報，80，No.4，257～260 (2006)

システム構築のためのプラットフォーム活用標準“MIWESTA/PF”

朝倉耕一* 松浦陽平***
村田謙一** 原田雅史***
花崎芳彦***

Platform Infrastructure Standard “MIWESTA/PF” for System Development

Kouichi Asakura, Kenichi Murata, Yoshihiko Hanazaki, Yohei Matsuura, Masafumi Harada

要 旨

三菱電機インフォメーションシステムズ㈱(MDIS)では、オープンシステムの黎明(れいめい)期からWebシステムの開発標準を体系化し、“MIWESTA^(注1) (MDIS Web Development Standard)”としてソリューション技術の蓄積・整備を図ってきた。“MIWESTA”は、現在アプリケーション開発標準“MIWESTA/AP”と、プラットフォーム活用標準“MIWESTA/PF”の2つで体系化されている。

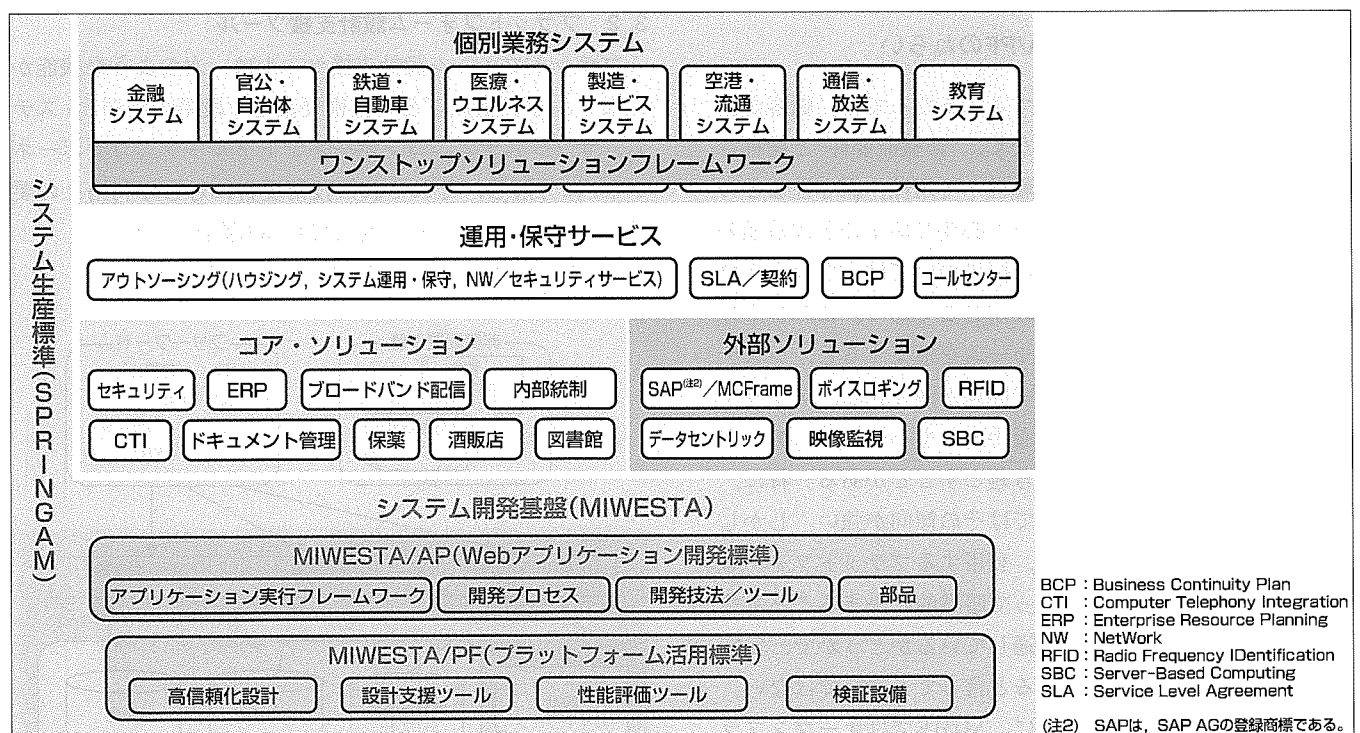
MIWESTA/APは、Webアプリケーションソフトウェアを開発するためのフレームワークである⁽¹⁾。

MIWESTA/PFは、上記のWebアプリケーションソフトウェアを開発する上での基盤となるオーブンプラットフォームの選定・活用にかかわる標準であり、IHV(Independent Hardware Vendor)製品やISV(Independent Software Vendor)製品を組み合わせて所定の品質や性能

(注1) MIWESTA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。

を確保することを目的としたものである。

“オープン化”の進展に伴って、利用可能なプラットフォーム製品の選択肢が拡大し、より安価な製品で、より効率的なシステムの構築が可能になってきた。しかし、反面、これを選定する上での広範な知識と活用ノウハウが必要となっており、とりわけ、性能や信頼性などの非機能要件に関する設計技術の点で、標準化の果たす役割は大きい。MIWESTA/PFでは、プラットフォーム製品の選定・活用に関する基準を制定し、その基準に沿った形でシステムを構築する場合の設計手法ガイドとそれを支援するツール群とによって、製品活用技術の標準化を実現している。本稿では、このうちのプラットフォーム製品の選定から構成設計(コンピューティング・モデル設計)までを支援するプラットフォーム設計支援ツールと、物理構成を確定するために必要なサイジング(性能設計)の手順について述べる。



システム開発の標準フレームワーク“MIWESTA”の構成図

MIWESTAは、システム開発基盤の総称である。MDISのシステム生産標準である“SPRINGAM”の下で、Webシステムの開発標準をフレームワーク化し、Webアプリケーションソフトウェアの開発/実行基盤(プラットフォーム)とに分けて開発・構築技術を蓄積・整備している。“MIWESTA/PF”は、このうちの実行基盤の方をサポートする。TOGAF(The Open Group Architecture Framework)のテクノロジー・アーキテクチャのレイヤを対象に、製品選定基準、高信頼化設計手法、各種支援ツール、検証設備などによって関連技術の体系的整備を図っている。

1. ま え が き

Webベースシステムや“オープン化”の進展に伴って、オープンプラットフォームの活用が急速に拡大した。このオープンプラットフォームは、IHV製品、ISV製品などの組み合わせによって構成されるマルチベンダー環境であることのほか、技術の進歩に伴う製品サイクルの短縮化や選択肢の拡大などによって、従来のような経験知をベースとした設計・構築が困難な環境でもある。他方、情報システムの高度化とネットワーク化による社会インフラ化によって、システムの障害や不具合が社会的又は企業全体に重大な影響を及ぼすようになり、システムの構築にあたっては、性能、セキュリティ、信頼性・可用性、保守性などの“非機能要件”に対する考慮が今まで以上に必要になっている。このような問題を背景に、コンピューティング・モデルなどによるテクノロジー・アーキテクチャ層のモデル化や、対象用途別にプラットフォーム(開発/実行基盤)までをフレームワーク化する動きが加速してきており、MDISのWebシステム開発基盤(MIWESTA)でも、“MIWESTA/PF”としてこれを開発・整備した。MIWESTA/PFでは、プラットフォーム製品の選定・活用に関する基準を制定し、その基準に沿った形でプラットフォームを構築する場合の設計ガイドとそれを支援するツール群とによって、オープンプラットフォームを活用するために必要な設計技術の蓄積と再利用を図っている。

2. MIWESTA/PFのねらい

情報システムを設計・構築するにあたっては、顧客が望む機能要件を実現するだけでなく、“非機能要件”と総称される性能、セキュリティ、信頼性・可用性、保守性などの品質特性に対しても十分な考慮が必要であることは前述のとおりである。この“非機能要件”については、プラットフォーム設計段階からの作り込みが必要であり、これを十分に検討しないままプラットフォームを構築すると、システム試験や運用試験などの段階で問題が顕在化し、アプリケーションソフトウェアの大幅な手直しやハードウェアのグレードアップなどの事態を引き起こすことがある。特に、性能や信頼性・可用性についてはその傾向が強い。しかしながら、これらの品質特性は、利用するプラットフォーム製品の選定や組み合わせによって暗黙的に決まることも多く、その製品の活用技術に精通しているかどうかで、安定運用や短期構築の可否が決まると言っても過言ではない。これらの課題を解決するために、MDISではオープンプラットフォームの設計(論理設計/物理設計)を支援するツールを開発した。本稿では、このうちのプラットフォーム製品の選定から構成設計(コンピューティング・モデル設計)までの論理設計を支援するプラットフォーム設計支援ツ

ールと、物理構成を確定するために必要なサイジング(性能設計)の手順について述べる。

3. プラットフォームの論理設計

3.1 論理設計の概要

プラットフォームの設計にかかわる課題に対処するためには、プラットフォーム・レベルでの組み合わせをモデル化・パターン化したコンピューティング・モデルによって対象システムの論理構成を定義し、それをベースとして性能、拡張性、可用性、保守性、セキュリティなどの非機能要件の実現手段を付加していくプロセスを確立することが必要となる。

MIWESTA/PFでは、これらの一連の設計作業を“プラットフォーム論理設計”として整理し、プラットフォーム設計ガイドとプラットフォーム設計支援ツールとによって、このプロセスを統制/支援している。

プラットフォーム設計ガイドは、基本構造(ベースモデル)の選定から物理構成の決定に至るまでのプロセスについて、留意すべき非機能要件をリスト化するとともに、それを実装するために必要な設計手法や設計上の要点をまとめたものである。一方、プラットフォーム設計支援ツールは、非機能要件をキーとして、蓄積された事例構成(構築実績及びベースモデル)を参照するためのツールであり、プラットフォーム設計ガイドと連携してプラットフォームの設計に必要な製品情報や技術情報を提供する。

3.2 プラットフォーム設計支援ツール

プラットフォーム設計支援ツールは、次のような機能からなり、事例構成ごとの技術要素を4段階の階層(システム、サブシステム、コンポーネントグループ、コンポーネント)に分解し、それぞれの技術要素に対して利用上の要件や知見をデータベース化している(図1)。

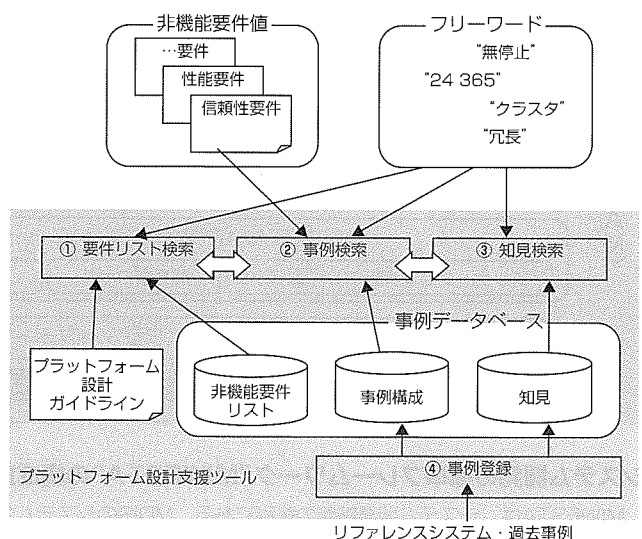


図1. プラットフォーム設計支援ツールの機能構成

(1) 非機能要件検索

フリーワードで非機能要件を検索し、マッチした要件と、その要件を具体化した事例、事例を構成するための要件などを提示する。また、登録された要件値で事例を絞り込む機能を持つ。

(2) 事例検索

フリーワードで事例を検索し、マッチした事例と、その事例が使用している製品や構成要素などを提示する。

(3) 知見検索

フリーワードで知見を検索し、マッチした知見と、その知見にひも付けられる事例を表示する。

(4) 事例登録

システム事例ごとにベースモデルの構成や、知見、設計要件・要件値などを事例データベースに登録する。

なお、これらの機能は、一般的なWebブラウザから利用できるようになっており、全社又は事業所共通の開発支援環境としての利用を想定している(図2)。

プラットフォーム設計ガイドと連携してプラットフォーム設計支援ツールを活用することによって、次のような効果が期待できる。

- プラットフォーム設計作業の定型化・効率化
- 非機能要件に対する設計漏れや設計誤りの削減
- プラットフォーム製品情報・設計情報の組織的共有
- 構成製品の統制によるトラブル対応力の向上

4. プラットフォームの物理設計

4.1 性能評価ツールを用いた物理設計とサイジング

MIWESTA/PFでは、プラットフォーム論理設計でのアウトプットに基づいて、具体的な機種の決定やコンポーネントの配置を含むプラットフォームの物理構成を設計するものとし、これを“プラットフォーム物理設計”と呼ぶ。プラットフォーム物理設計のポイントは、システムに要求される性能が確保できるよう、システムを構成するサーバな

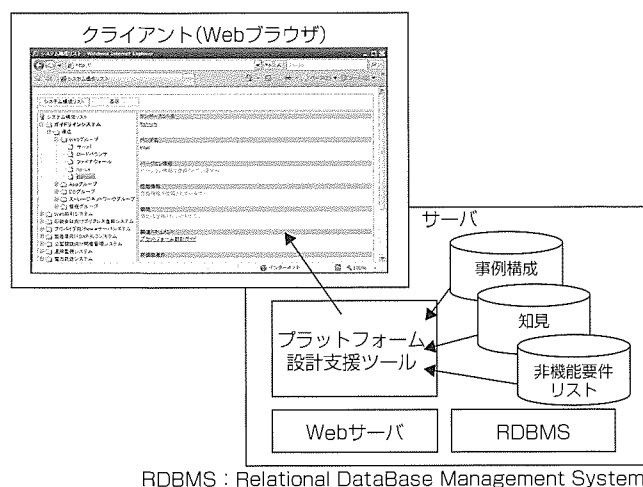


図2. プラットフォーム設計支援ツールのシステム構成

どに対して適切なサイジングを行うことである。

システムの性能は、プラットフォームの構成のみに起因するものではなく、使用するミドルウェアやアプリケーションにも大きく依存するため、これらを加味する必要がある。MIWESTA/PFでは、MIWESTA/APに準拠したアーキテクチャを採用したシステムに対して、サイジングを支援するための性能評価ツールが用意されており、ツールによって収集・蓄積された性能基礎データを使用することで、対象システムの概略性能が確認できる。

また、プラットフォーム物理設計段階での性能設計手順や性能評価ツールを利用した検証・評価方法などを解説した性能設計ガイドを用意しており、これらによってサイジングを含むプラットフォーム物理設計を支援している。

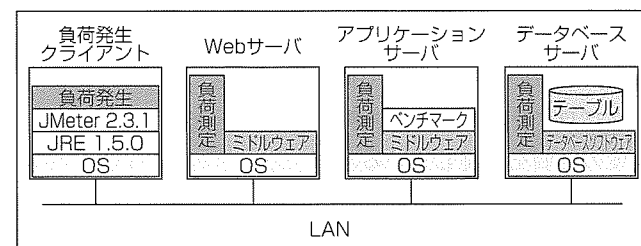
MIWESTA/PFの性能評価ツールは、プラットフォーム物理設計段階での設計性能の検証・評価を目的としたものであり、MIWESTA/APで規定されているアーキテクチャに準拠したベンチマークプログラム、負荷発生プログラム及び負荷測定プログラムから構成されている。図3にツールの全体構成例を示す。

現時点で準備されているベンチマークプログラムは、Web 3 階層型の受注システムをモデル化したものである。負荷発生プログラムは、性能に大きな影響を及ぼすデータベースの検索処理と更新処理の実行比率を自由に設定可能であるが、代表的な次の3つの形態に対して測定及び収集を行っている。

- 閲覧ミックス 検索処理：更新処理=95：5
- 買物ミックス 検索処理：更新処理=80：20
- OLTP(On-Line Transaction Processing)ミックス 検索処理：更新処理=50：50

このベンチマークプログラムでは、次のような性能基礎データが簡単に収集・蓄積できるようになっており、単に性能測定・評価を行うだけではなく、収集したデータとその時の構成機器情報などをデータベース化して、サーバの機種候補選定などに利用できる。

- (1) アプリケーション側の性能基礎データ収集項目
各処理の実行回数、応答時間、スループットなど



JMeter2.3.1：Java[®]アプリケーションの時間性能測定/負荷生成ツール
JRE1.5.0：Javaプログラムの実行環境
(注3) Javaは、Sun Microsystems, Inc. の登録商標である。

図3. 性能評価ツールの構成例

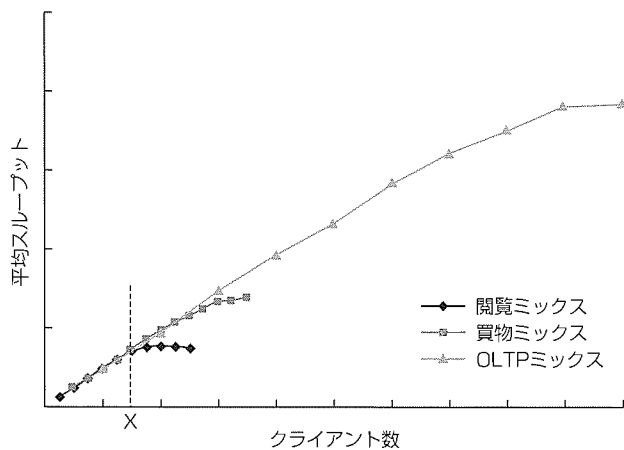


図4. 平均スループット

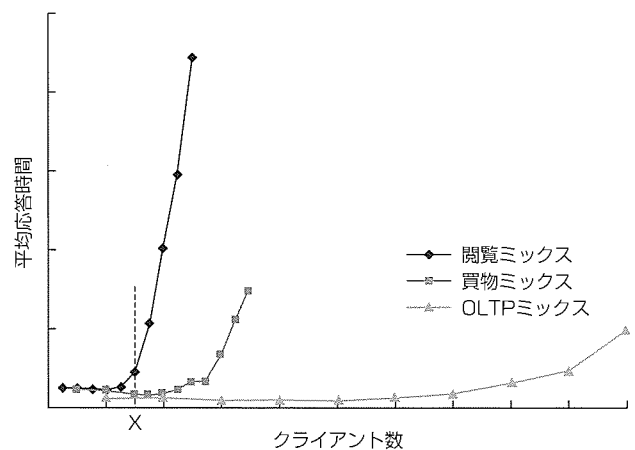


図5. 平均応答時間

(2) プラットフォーム側の性能基礎データ収集項目

CPU(Central Processing Unit)使用率, メモリ使用率, ディスク使用率, ネットワーク使用率など

(3) その他の補助的なデータ収集項目

ミドルウェアのリソース使用率など

4.2 性能基礎データの事例

図4から図6に, ツールを用いて測定・収集した性能基礎データの一例を示す。図4及び図5は, 評価対象システムに対して閲覧・買物・OLTPミックスに相当する負荷をかけた場合の, 平均スループット及び平均応答時間を示したグラフである。

この例では, 同時接続クライアント数がXを超えると閲覧ミックスでの平均スループットと平均応答時間が急速に悪化することがわかる。このときの各サーバの負荷状態として, 例えば図6に示すようなCPU使用率, メモリ使用率, ディスク使用率が得られ, どのサーバの, どのリソースがボトルネックになっているかがわかる。図6の場合はデータベースサーバのCPUがボトルネックであることを示しており, データベースサーバのサーバ増設(スケールアウト)やより性能の高いサーバへの変更(スケールアップ)が必要であることがわかる。

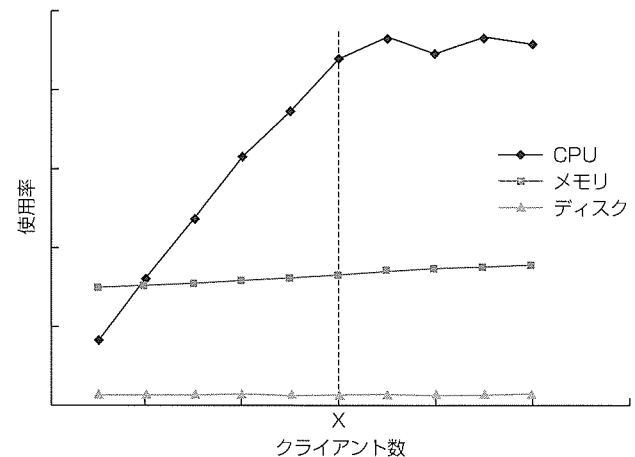


図6. データベースサーバ負荷(閲覧ミックス)

5. む す び

このように, MIWESTA/PFでは, 非機能要件のリスト化とその構築技術の標準化を行っており, 今回, プラットフォーム設計支援ツールと性能設計手順について述べた。現在, 複数の実システムで採取した性能データとベンチマークプログラムで採取した性能基礎データからサイジング精度の評価を実施している。

今後, プラットフォーム設計支援ツールは, 事例の拡充と性能設計との連携を計画している。

また, プラットフォーム性能設計手順では, 複数のプラットフォームと幅広いアプリケーション種別に対応可能でなければならない。性能に影響を及ぼす項目として, 本稿で述べた要因以外に計算機リソースを含めたシステム・アーキテクチャ, アプリケーションの違いに起因するビジネス・ロジックの複雑さ, データベーステーブルの構成や大きさなどが挙げられる。上流段階で正確なサイジングを可能にするためには, これらをパラメータ化して取り込むことが課題である。

参 考 文 献

- (1) 川口正高, ほか: オープン環境のシステム構築を高品質・短納期で実現するWebシステム開発標準“MIWESTA”, 三菱電機技報, 81, No.7, 489~492 (2007)
- (2) 金木佑介, ほか: Webシステムの性能評価に関する一手法, 情報処理学会論文誌, 48, No.SIG18, 99~107 (2007)

生花市場におけるせり総合システム 市場くんシリーズ“生花卸売業システム”

野上泰弘*
小池信成*

“Flower Wholesale Trade System” of ICHIBAKUN Series

Yasuhiro Nogami, Nobushige Koike

要 旨

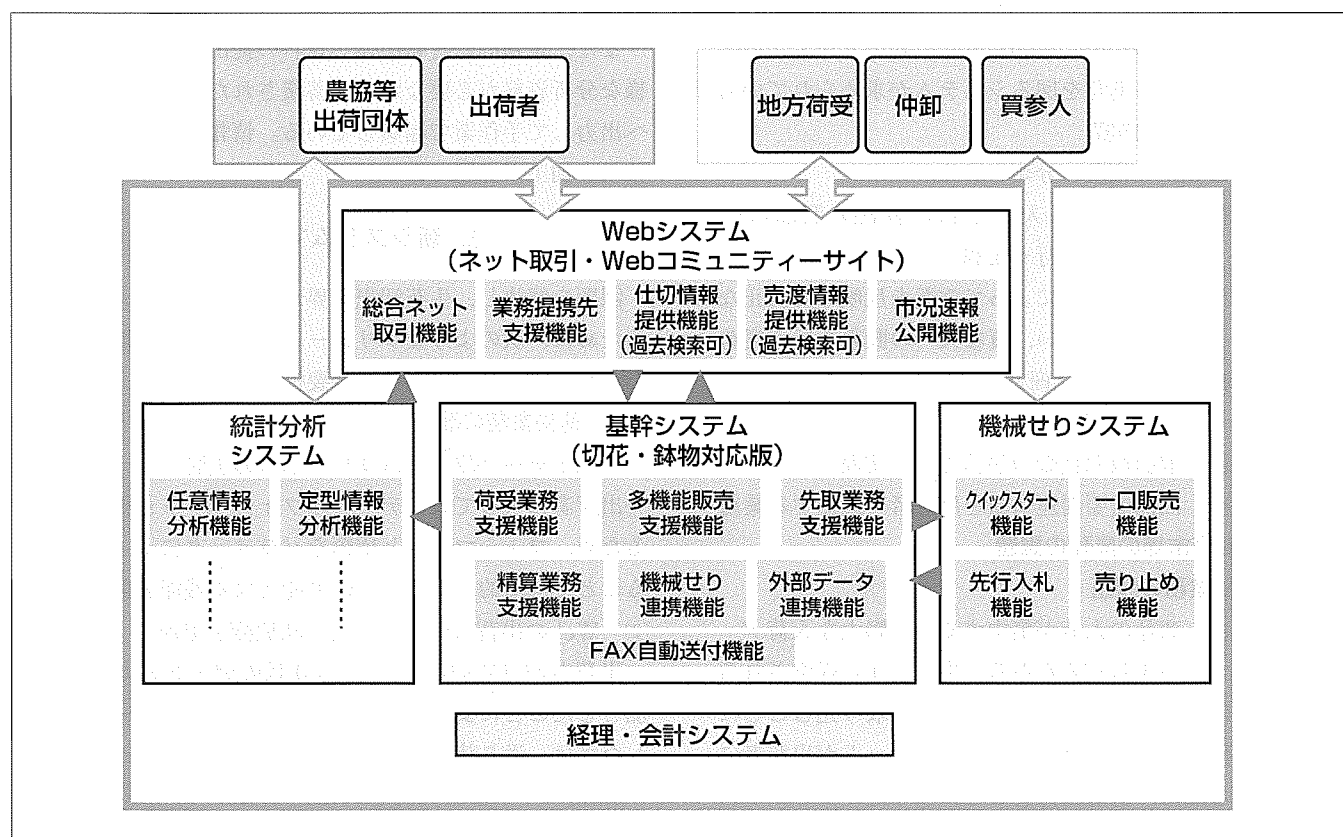
(株)三菱電機ビジネスシステム(MB)では、生花卸売市場における、基幹システム、統計分析システム、ネット販売などから構成される市場くんシリーズ“生花卸売業システム”を開発・販売している。

この度、某生花卸売市場のシステムリプレースに際して、従来の手せり対応のシステムから、機械せり対応のシステムに変更し、同業他社との差別化、各部門・部署での作業効率向上、Web対応のネット販売による顧客サービスの向上等を実現した。

システムの導入効果を次に挙げる。

- 操作が簡易な機械せり機によって、せりの時間を短縮
- Webシステムによって利用者の求める情報が即時に参照可能
- 商品の販売から出荷までの時間短縮
- 蓄積されたデータの分析と有効活用

このシステムの導入によって、効果的かつ効率的な顧客サービスが実現できて、顧客満足度の向上に寄与することを確信している。



生花卸売市場のシステム構成

基幹システムで入荷処理された商品データを、せり応札機に送信して機械せりを行う。買参人によって応札されたデータを即時に処理して、せり結果はWebシステムを通じて出荷者(商品の生産者、及び農業組合等)や買参人(仲卸業者、及び売買参加者)にリアルタイムで情報が公開されるサービスを実現する販売管理総合システムである。

1. ま え が き

“市場くんシリーズ”は、中央卸売市場や地方卸売市場の卸売業及び仲卸業をターゲットにした販売管理パッケージシステムで、1997年から販売を開始した。2004年には、生花卸売業向けに機能を特化した、市場くんシリーズ“生花卸売業システム”を開発し、販売を開始した。この生花卸売業システムは、荷受・販売・精算を対象にした基幹業務システムであった。今回このシステムを改版するにあたり、顧客向けサービスを新たなセールスポイントとするため、インターネットを利用して、出荷者(商品の生産者、及び農業組合等)、卸売会社(出荷者から入荷された商品をせり等で販売する)、買参人(仲卸業者、及び売買参加者)のネット取引・売買情報及び市況速報等を提供するコミュニティサイトの機能追加を行った。

本稿では、今回開発した生花卸売業システムの特長と、このシステムの導入によってどのように業務改善することができたかについて述べる。

2. 生花卸売市場の業務内容とシステムの課題

2.1 卸売業界の状況

全国の卸売業界は、2009年4月から施行される取引手数料の自由化に伴い、顧客確保のための競争が激化することが予想される。そのため、業務効率化と顧客サービス向上によって他社との差別化を図るシステムが求められている。

2.2 卸売業の業務内容

大別すると5つの業務に分類される。

- ①荷受業務：出荷者から入荷された多種の商品の受入・検品を行う業務
- ②販売業務：せり取引等によって需要を反映した公正な値決めを行い、買参人への販売を行う業務
- ③分荷業務：販売された商品を仕分けして買参人へ搬送・出荷する業務
- ④精算業務：取引販売代金の決済を行う業務
- ⑤報告業務：商品需要関連情報を出荷者へ通知する業務

2.3 生花卸売市場の業務の課題

2.3.1 荷受業務の課題

繁忙期には、商品の入荷が集中するので膨大な入荷データを短時間で入力する必要がある。出荷者から提供される入荷データは、データ変換してシステムに取り込むことによって入力作業が軽減できるが、フォーマットが出荷者によって異なるため、新規出荷者ごとに取り込みプログラムの開発が必要となり、コスト増となる。

荷受業務の改善は、データ入力負荷の軽減と開発コストの削減が課題である。

2.3.2 販売業務の課題

せりは、品目別に並行して複数レーンで行われる。買参

人は、常時、複数レーンのせり商品と見本品の色を確認しながら応札する必要がある。そのため、購入チャンスを見逃さない仕組み作りが要求されている。

また、現状では、応札を行うには来場する必要がある、来場が少ない遠方の買参人の応札頻度を高くするための利便性向上も課題である。

2.3.3 分荷業務の課題

せり販売された商品に販売ラベル(購入者の買参人コードを印字したシール)を貼り付けて買参人別に仕分け、搬出している。ラベルが発行されるまでの印字待ち時間と、印字されたラベルから商品を探して貼り付ける作業に時間を要している。作業時間の短縮が課題である。

2.3.4 精算業務の課題

買参人は売上伝票をもとに商品の確認を行い、精算窓口で代金の支払いを行うが、せり直後は窓口が非常に混雑する。卸売会社側は、当日発行した売上伝票を買参人別に仕分けする作業に時間を要している。精算の集中回避と伝票仕分けの時間短縮が課題である。

2.3.5 報告業務の課題

出荷者は、安定した価格で販売する卸売会社へ商品を出荷したいため、商品販売結果をいち早く求めている。現状では、すべてのせりが終了しないと情報が公開されないため、せり中でも公開できる仕組み作りが要求されている。

また、定期的に管轄団体へ資料の提出を行うが、毎年多様な分析資料が必要なため、蓄積されたデータをパソコンへ出力して手作業で編集している。情報の速報性と情報の柔軟な加工が課題である。

3. 新システムでの解決策

課題を解決し、生花卸売業界が求めるシステムを提供するために、次のようなソリューションの設計・開発を行った。図1にシステムの機器概要構成を示す。

3.1 荷受業務の改善

(1) 汎用データ取り込みプログラムの実装

出荷者によって入荷データのフォーマットと種類が異なるため、フォーマットと種類をパラメータによって設定することで汎用的に取り込みが可能となる機能を開発した。

(2) Webの出荷者サイトに送り状機能を追加

出荷者向けWebサイトに送り状のデータ入力機能を付加としたことによって、出荷者は一度送り状データを入力した後は、送り状の作成と送付作業が不要となった。

Webサイトから入力された送り状データが即時に入荷データとして扱われることによって、迅速な情報の収集と、データ入力負荷の軽減が実現できた。

3.2 販売業務の改善

(1) 全レーンにサブモニタ(42インチ液晶)を導入

全レーンのせり時計スクリーン(図2)下に42インチのサ

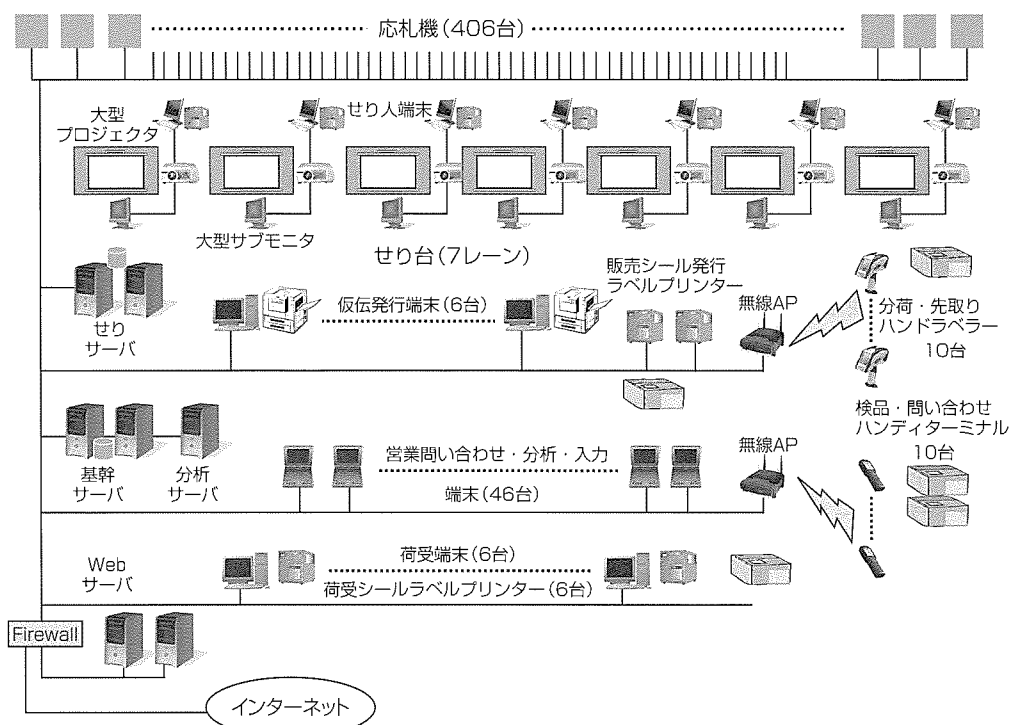


図1. システムの機器概要構成



図2. せり時計スクリーンのイメージ



図3. オークションルームとサブモニタ

ブモニタ(図3)を設置し、せり品のイメージ写真を表示することで、開花時のイメージ、色のイメージを画面で確認可能とした。

(2) 高機能型応札機の導入

購入希望商品が同時に2レーン以上のせり台で流れたときにもせり台の切替をすることなく購入を可能とした。また、事前に応札機で応札内容を先行登録して自動的に応札することを可能とした。

液晶画面を大型化することで落札データを1画面あたり300件表示可能とし、当日購入商品の一覧・購入金額合計の確認をせり席で行うことを可能とした。

(3) Web先行入札機能の導入

せり前日に、インターネットで上場商品を対象に応札価格を設定することで、せり当日の機械せりに連動した先行応札を可能とした。市場に来場しなくてもせり応札ができるため、遠方の買参人の応札機会を増すとともに、すべて

の買参人の利便性を向上させた。

(4) ネット販売の実現

30分ごとに上場する商品の情報を更新して、インターネットでの購入を可能とした。ロット購入単価の設定表示を行うことで、多数購入する買参人に対して、より安価に商品の提供を行うことを可能とした。携帯電話からの接続も可能である。

(5) D2/D3品のネット販売の実現

D2(次々回せり入荷予定品)及びD3(次々々回せり入荷予定品)の情報を公開し購入可能にすることによって、買参人は計画的な購入が可能となった。

(6) 孫番号管理機能の導入

買参権を持たない購入希望者もネット取引ができるように、買参人の申請によって買参人孫番号を付与し、買参人経由でネット購入に参加することを実現した。

(7) ハンドラベラー活用による先取り機能

無線LAN対応ハンドラベラーを活用し、先取り取引（せり前に買参人が商品を予約購入する販売業務）を商品置き場で可能としたことによって、入力処理の軽減をはかった。

(8) 購入明細発行機の設置

せり中でも購入商品を確認できる仕組み作りを実現するために、オークションルームに購入明細を随時発行できる端末の設置を行った（せりで使用するIDカードを活用し、カードスキャナでIDカードの情報を読み取って、買参人の購入明細を印字）。

3.3 分荷業務の改善

(1) 無線LAN対応ハンドラベラーの導入

無線LAN対応ハンドラベラーを使用することによって、せり販売されたデータを、場所を選ばずどこからでも要求に応じてリアルタイムに問い合わせすることが可能となった。

かつて熟練者が行っていた分荷作業を、商品バーコードをスキャンすることで、詳細情報が参照可能となりだれでも分荷作業を可能とした。

ハンドラベラーは、①移動ができる無線対応、②片手で操作可能なスキャナー一体型、③片手で長時間操作が可能な重量、④ランニングコストが少ない感熱紙対応、⑤シール剥離（はくり）機内蔵、⑥高速印字（1秒以内/1枚）、⑦導入実績が豊富といった点を考慮した。

(2) 検品用ハンディターミナルの導入

商品の集荷後に不足品・分荷間違い商品のピックアップが即時に判別できるように、商品確認の際に離れた場所でも迅速にスキャンできるハンディターミナルを導入して、迅速な検品作業を行えるようにした。

3.4 精算業務の改善

(1) 本伝票発行機の設置

精算所の横に本伝票発行機を設置し、買参人が自分で印字することで、精算所の混雑解消と事務作業の軽減を可能とした。

3.5 報告業務の改善

(1) オープンな環境の会員制コミュニティサイトの構築

Webサイトから情報収集・情報発信を可能とした。買参人向けには販売情報をWeb画面上で公開し、より早い情報の公開が実現でき、ダウンロード機能によってデータの2次利用を可能とした。

出荷者向けには、仕切情報をWeb画面上で公開し、より早い情報の公開を実現した。ダウンロード機能によってデータの2次利用を可能とした。

(2) ブログによる情報発信

消費者に商品を身近に感じてもらえるようブログ（Weblog）による消費者向け情報発信を実施した。

(3) 高速OLAPの導入

高速のOLAP（On-Line Analytical Processing）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（株）（MDIT）製の“DIAPRISM”を導入することで、大量データ分析の高速化を図り、DIAOLAP for Microsoft Excel^(注1)（Excel上で実行するBIフロントエンドアドイン）の利用によって自由に分析が可能となり“いつでも、だれでも、即時に”を実現した。

4. む す び

生花卸売業界は、出荷者と買参人に対する迅速な情報提供と公正な取引の提供が強く求められており、顧客のニーズを吸収できる業務パッケージの提供は不可欠である。

今回開発した統合システムをベースに、ユーザー規模とニーズに合わせたサブシステムの提供を行うとともに、様々な企業独自のカスタマイズに対応可能なシステムとして改版を継続する。卸売会社の業務形態に対応するために、更なるシステムの充実と操作性と利便性の向上を行い、生花卸売業務だけでなく、青果版・鮮魚版と幅を広げてパッケージシステムを提供することによって、卸売業界への社会的貢献を果たしていきたい。

（注1） Microsoft Excel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。



特許と新案***

三菱電機は特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社 知的財産渉外部
電話(03)3218-9192(ダイヤルイン)

オペレータ業務支援システム 特許第3827704号(特開2006-276754)

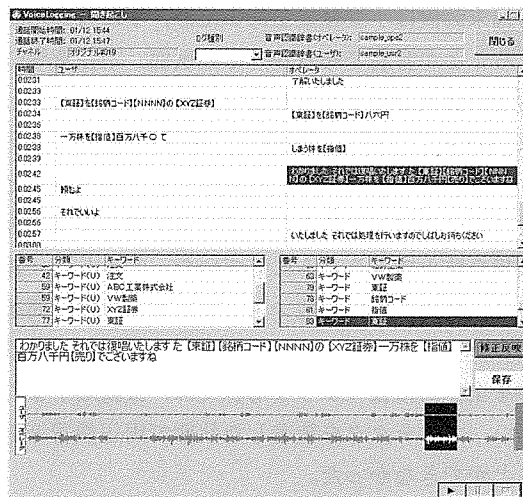
発明者 岩山洋明

この発明は、「オペレータ業務支援システム」に関するもので、音声テキストデータに変換して表示するときに特定のキーワードを強調表示することによって、オペレータの作業効率を向上させる特徴がある。

従来、コールセンター業務におけるオペレータ支援システムとして、ユーザーからの問い合わせ内容や回答内容を業務ログとして作成するときに、音声認識の結果をテキスト表示する機能があった。しかし従来の機能では、音声認識結果がテキスト表示されるだけだったため、オペレータ作業を効率的に行わせるための工夫はされていなかった。

この発明では、オペレータがユーザーからの電話を受け付けると、録音を開始し、通話の進行に伴いリアルタイムで通話内容を表示する。そのとき、あらかじめ指定した特定のキーワードと一致する内容は、強調表示する。一例としてキーワードを、【】で囲んだり、色、フォントの種類、文字の大きさを変更して、強調表示をする。またオペレータは聞き起こし時に強調表示する新たなキーワードを自由

に指定することができる。このキーワードは、業務目的に合わせて、複数の単語の組み合わせ、文書、固有名詞などを指定できるため、オペレータは重要な部分をより短時間で認識でき、作業効率を向上させることができる。



呼制御データ検索システム及び呼制御データ検索プログラム 特許第4091645号(特開2008-124758)

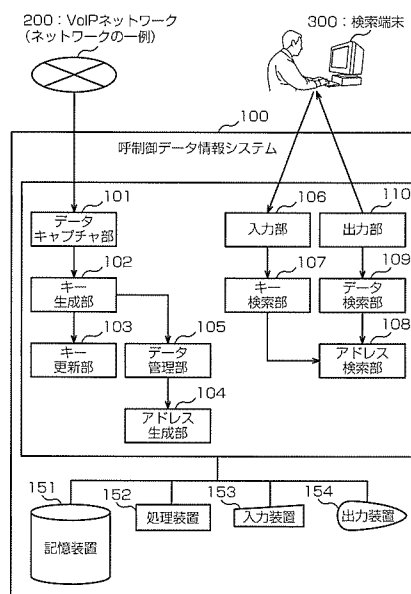
発明者 小杉英司, 北山浩二

この発明は、VoIP(Voice・over Internet Protocol)の呼制御データの高速検索方式に関する発明で、キーファイルに同一の呼識別子のキーが存在するときは、キーを追加することで、特定の事象があった呼の検索を容易にすることを特徴とする。

昨今、VoIPの代表的なアプリケーションであるIP電話が普及し加入者が増加してきたことから、VoIPに対して従来の電話網と同等の信頼性が求められるようになった。そのためトラブル発生時に、リアルタイムに発生する大量のVoIPパケットの中からトラブルの原因となったパケットを効率的に検出して、そのトラブルに迅速に対処する必要が生じている。

この発明では、特定の事象があったことを示す属性データを含むキーを呼制御データの呼識別子ごと、かつ単位時間ごとに生成し、生成したキーをキーファイルに保存し、過去のキーファイルに同一呼識別子のキーが保存されている場合には、同一呼識別子のキーに、新しいキーの属性データを追加する。それによって、多数の呼の中から、検索条件として指定した時刻に特定の事象があった(例えば午

前10時に開始された)呼で、当該時刻より後に検索条件として指定した事象があった(例えば午前10時10分より後に異常切断した)呼を容易かつ高速に抽出することができる。





特許と新案***

三菱電機は特許及び新案を有償開放しております

有償開放についてのお問合せは
三菱電機株式会社 知的財産渉外部
電話 (03) 3218-9192(ダイヤルイン)

携帯端末装置用プロテクタ 特許第3678593号 (特開2000-183556)

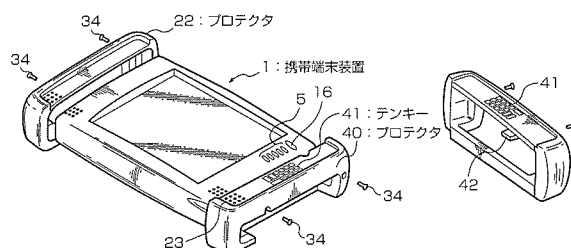
発明者 船越 勇, 富田 修

この発明は、携帯端末装置用プロテクタ、特に落下による衝撃での装置破損を防止し、かつプロテクタ取付時における携帯端末装置の操作性、機能性を損なわないようにするための構造に関するものである。

携帯端末装置は小型軽量であるため、手に持った状態で使用することが容易であるが、その反面、不注意等によって使用者が装置を落としてしまい、衝撃で破損してしまうおそれがある。このため従来は、装置の角部(コーナー)を被うようなプロテクタを取り付けたり、装置本体と衝撃吸収材とを一体成形するなどして、落下時の衝撃を吸収させ、破損を防止できるようにしていた。しかし、一体成形にすると、装置本体の製造コストや小型化の面で問題がある。プロテクタを着脱可能にすれば解消するが、装置の角部近傍を全体的に被うような形状では、接続端子まで被ってしまい、プロテクタを装着した状態で周辺機器等を使用することができなかった。

この発明では、保護部材であるプロテクタに端末の各側面をはめ込むことで、装置の角部を被い、かつ接続端子、操作部及び表示部を被わないように開口部を設けた形状と

することで、プロテクタを取り付けた状態でも周辺機器等を使用でき、機能性を損なうことがない。また、保護部材を2層構造とし、装置と接する内層部に剛性を持たせたことで、プロテクタを取り付けたまま机上で使用する際、装置中央部が浮いた状態となり、筐体(きょうたい)が撓(たわ)むのを抑えることができ、外層部を柔らかい部材で形成することで、落下による衝撃を吸収できる。さらに、プロテクタの上面にテンキーを配置し、プロテクタ取付時に装置本体のテンキー用端子へ接続する構造としたので、プロテクタの未使用スペースを有効利用しつつ、ユーザーへテンキーの入力手段を提供した。



〈本号記載の商標について〉

本号に記載されている会社名、製品名はそれぞれの会社の商標又は登録商標である。

〈次号予定〉三菱電機技報 Vol.82 No.8 特集「エコファクトリー化技術」

<p>三菱電機技報編集委員</p> <p>委員長 杉山 武史</p> <p>委員 小林智里 増田正幸 滝田英徳 岩崎慎司 糸田 敬 世木逸雄 江頭 誠 河合清司 種子島一史 安井公治 逸見和久 光永一正 河内浩明 橋高大造</p> <p>事務局 園田克己</p> <p>本号取りまとめ委員 河内浩明</p>	<p>三菱電機技報 82巻7号 2008年7月22日 印刷 (無断転載・複製を禁ず) 2008年7月25日 発行</p> <p>編集人 杉山 武史 発行人 園田 克己 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</p> <p>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</p> <p>定 価 1部945円(本体900円)送料別</p>
<p>三菱電機技報 URL 三菱電機技報に関するお問い合わせ先</p>	<p>URL http://www.mitsubishielectric.co.jp/corporate/giho/ URL http://www.mitsubishielectric.co.jp/support/corporate/giho.html</p>
<p>英文季刊誌「MITSUBISHI ELECTRIC ADVANCE」がご覧いただけます</p>	<p>URL http://global.mitsubishielectric.com/company/rd/advance/</p>

企業間の電子データ交換では、取引先企業によって転送プロトコルやデータ形式が様々で管理が煩雑であり、さらに社内のレガシーシステムとの連携を行うには多大なコストがかかります。これらデータ交換の課題をデータ交換プラットフォーム“BizOrder^(注1)（ビズオーダー）”が解決します。BizOrderは、電子商取引や社内システム連携で交換される文書などの情報を、それぞれのシステムに合わせて自動的に変換。いままでデータ交換のために費やされていた時間とコストを大幅に低減します。

■ 製品の特長

(1) 豊富な対応データ形式・プロトコル

SMTP/POP3形式の電子メール、DB、FTP、HTTPなど様々な入出力インタフェースに対応。入出力ファイル形式もCSV、固定長テキスト（マルチレコードフォーマット形式にも対応）、タブ区切テキスト、XML、Excel^(注2)に対応しています。特に最近では、データ交換のフォーマットとしてExcelが非常に多く使われています。BizOrderでは、Excelファイルの受信・取込み、生成・送信を簡単に定義で行うことができます。また、セル結合や複数のワークシートなど様々なパターンに対応します（図1）。

(2) EDI連携機能

BizOrderは、様々なEDI機能と連携が可能です。

● XML-EDI^(注3)対応

XMLはデータ構造を汎用的に記述できる言語でデータ交換に最も適したデータ形式です。このXMLを用いたEDIとして2007年に経済産業省が“流通ビジネスメッセージ標準”を公開し、大手スーパー、卸が採用を表明しています。これによって今後、XML-EDIの普及が加速していくことが予想されます。BizOrderは簡単にXMLフォーマット変換を行うことが可能です。

また、XML-EDIの通信プロトコルであるebXML及びJX手

順との連携オプションを提供いたします。

● インターネットEDI

従来の全銀手順、JCA手順といった公衆回線を利用したEDIからインターネットをベースにしたEDIへの移行が急速に進んでいます。通信プロトコルはレガシー系からインターネット系に切り替わっても、送受信するデータ形式は従来どおりといった事例が多く存在します。BizOrderは、インターネット系プロトコルに対応すると同時にレガシー由来のマルチレコードフォーマット形式の送受信もサポートします。これによって通信プロトコルが変わっても安価で迅速に対応が可能となります。

(3) 開發生産性

● データ交換テンプレート

BizOrderはデータ交換を自動で行うための“フロー制御テンプレート”を提供しますので簡単に自動化ソリューションを導入することができます。またSOAをベースとしているため導入後のカスタマイズも容易に行えます。

(4) 運用性

● 統合的なEDI処理

昨今のデータ交換ではXML-EDI、インターネットEDI、全銀・JCA手順といった様々な形態が入り乱れて運用されています。BizOrderはこれらEDIとの連携手段を提供し、様々な形態のEDIを一括管理できる機能を提供します。

● データ受信時のエラーチェック

データの数字や文字の許容範囲などを自動的にチェックし、異常がある場合にはシステム管理者に電子メールで通知しますので、データエラーの有無を目視で確認することもなく、チェックの省力化が可能です。

● 送受信履歴ビューア

データの受信、送信が成功したか失敗したかの履歴をブラウザベースのツールでチェックすることが可能です。また、バックアップデータも見ることができデータ送受信管理を容易に行うことができます（図2）。

（注1） BizOrderは、三菱電機インフォメーションテクノロジー㈱の登録商標です。

（注2） Excelは、米国Microsoft Corp.の米国及びその他の国における登録商標または商標です。

（注3） XML-EDI：インターネット上の高機能記述言語／電子商取引に関する情報の書式を統一して、企業間で電子的に交換する仕組み

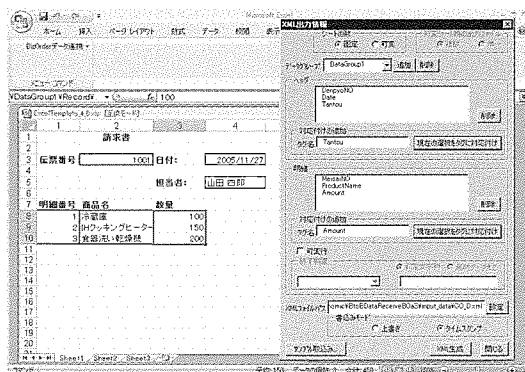


図1. Excel連携

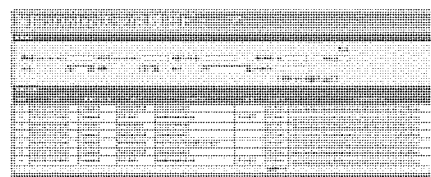


図2. 送受信履歴ビューア