三菱電機技報　84巻7号（通巻950号）

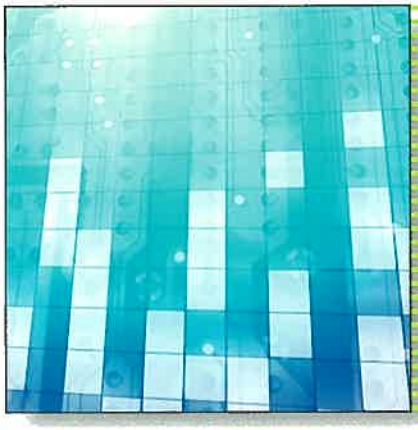
Changes for the Better

MITSUBISHI

三菱電機技報

Vol.84 No.7　2010 7

特集「クラウド技術を適用した企業情報システム」



eco Changes

家庭から宇宙まで、エコチェンジ

ISSN　0369-2302　CODEN:MTDNAF

三菱電機技報 Vol. 84 No.7 2010

目　次

特集「クラウド技術を適用した企業情報システム」

Cloud Computing Technologies for Enterprise Information Systems

特許と新案

表紙：クラウド技術を適用した企業情報システム

三菱電機は，効率的な企業経営の実現を目指して，高セキュリティ・高信頼なインフラ基盤技術をベースに，クラウド技術を適用した企業情報システムへの取組みを推進している。

表紙では，高度な情報通信サービスの要となる三菱電機情報ネットワーク㈱(MIND)の東京第3データセンターの写真を中央に配置し，その周囲に配したビジュアルイメージによって，企業情報システムに求められる“安全性”“信頼性”“利便性”“快適さ”を表現した。

巻/頭/言

クラウドコンピューティングの進展とその課題

Development of Cloud Computing and its Problem

辻　秀一
Hidekazu Tsuji

世の中は今，ネットワーク化の大きな流れの中にある。インターネットやワールドワイドウェブ上で多数の検索エンジンやポータルサイトによる情報提供サービスがあり，世界中のインターネット上の情報を，パソコンや携帯端末のブラウザを通して簡単に見ることができる。インターネットによって情報が瞬時に時間と空間を超えて低コストで伝達されるようになり，企業は少ない費用で自社のビジネス範囲を拡大することができるようになった。さらにインターネットやイントラネットに接続された企業情報システムによって情報共有やコラボレーションが可能となり，企業はサプライチェーン全体の在庫適正化，開発期間の短縮や，柔軟性の高い効率的な経営組織の実現を図ることで，企業競争力を向上させている。また，ネットワークを経由した各種アウトソーシングサービスの利用による組織強化やコスト削減によって，企業間競争の激化に立ち向かおうとしている。

このような社会環境やビジネス環境において，情報システムの効率化のためにインターネットを経由した様々なコンピュータ提供サービスやソフトウェア提供サービスが行われている。まず，顧客のサーバを預かり，インターネットへの接続や保守・運用サービスなどを提供するインターネットデータセンター(IDC)がある。また，各種の業務アプリケーションソフトウェアを提供するASP(Application Service Provider)や，ソフトウェアの機能のうちで必要な機能のみを必要なときに利用でき，利用する機能に応じた分だけの料金を支払うSaaS(Software as a Service)がある。さらに，最近ではこれらを発展させたクラウドコンピューティングによるサービスが提唱されている。これは，ネットワーク技術やデータベース技術に基づく高度な仮想化技術によって，特にリソースの所在を意識することなくコンピュータリソースを利用できるというコンセプトである。クラウドコンピューティングによって，ユーザーは自社内に情報システムのコンピュータ環境を持つ必要がなく，用意すべきものはブラウザやインターネット接続の最低限のインタフェースとサービス利用料金となり，処理が実行されるコンピュータ本体の維持管理の大半が不要となる。

この新しいサービスコンセプトのクラウドコンピューティングであるが，課題もいくつか挙げられている。まず初めの課題として企業情報システムのブラックボックス化への不安がある。クラウドサービス提供側の何らかの障害によるサービス停止や，顧客情報や経営情報の流出のリスクがある。また，法令に準拠したデータの保管や管理が行われるかどうかの不安もある。今後のクラウドコンピューティングの進展のためには，これらの課題を解決していくことが大変重要となる。サービス停止を招かないための仮想化技術や障害対策技術の更なる高度化，情報流出を食い止めるためのより安全で便利な認証技術の研究・開発，リアルなビジネス世界と整合性の取れたサービス規則の整備など，今後の進展に大いに期待したい。

◆東海大学　情報通信学部　組込みソフトウェア工学科　教授
Professor, Department of Embedded Technology, School of Information and Telecommunication Engineering, Tokai University

巻頭論文

クラウド技術を適用した企業情報システムへの取組み


伏見信也* 茂木 強**

Cloud Computing Technologies for Enterprise Information Systems

Shinya Fushimi, Tsuyoshi Motegi

要 旨

ITインフラやアプリケーションをサービスとしてユーザーに提供するというクラウドコンピューティング(以下“クラウド”という。)の流れが加速している。しかし，インターネットにアクセスできればだれでも利用可能なオープンなクラウド(パブリッククラウド)では，ユーザーが信頼性やセキュリティなどに不安を感じることもあり，企業情報システムでの利用が進展していない。そのため，企業情報システムにおけるクラウド利用に関しては，特定の限られたユーザー(企業内，企業グループなど)に閉じた形で導入し，ユーザーニーズに応じた高いサービスレベルを保証することが必要である。

三菱電機では，高セキュリティ・高信頼性を実現するインフラ基盤技術を保有しており，それを付加価値として，クラウド技術を適用した企業情報システムへの取組みを推進している。その具体的な例として，企業環境の変化に柔軟に対応するためのシステム間連携基盤，容易な運用管理を特長とする仮想化技術，セキュアな認証基盤とアクセス制御技術などのインフラ基盤技術を活用し，セキュリティや省エネルギーを付加価値としたSaaS(Software as a Service) 型サービスを実現している。また，三菱電機情報ネットワーク㈱(MIND)の豊富な実績に基づき，強固なセキュリティを確保したデータセンターによる運用管理サービスなどを提供している。

今後の更なる技術開発の取組みとしては，①復号情報の漏えいの心配を払拭(ふっしょく)するため，暗号化したまま個人識別情報を照合する秘匿照合技術，②仮想化技術を用いた情報システムの信頼性向上技術などの研究開発を行っており，安全性と信頼性を確保した付加価値の高い企業向けITサービスの提供を推進していく。

(注1) (財)金融情報システムセンター：金融機関等コンピュータセンター安全対策基準

クラウド技術を適用した企業情報システムへの取組み

当社では，高セキュリティ・高信頼性を実現するインフラ基盤技術を保有し，それを付加価値として，クラウド技術を適用した企業情報システムを提供する。また，当社の基盤技術を活用した製品と連携し，セキュリティ・省エネルギーを付加価値としたSaaS型サービスを実現している。さらに数年先を見据え，将来的な技術の研究開発を行っており，安全性と信頼性を確保した企業向けITサービスの提供を推進していく。

*インフォメーションシステム事業推進本部 技術企画部長(工博) **情報技術総合研究所 情報技術部門統括

1. まえがき

ITインフラやアプリケーションをサービスとしてユーザーに提供するというクラウドコンピューティング(以下“クラウド”という。)の流れが加速している。ITリソース調達の柔軟性や費用対効果の面から，企業情報システムのプラットフォームとしても魅力的である。しかし，不特定多数のユーザーがインターネット経由で利用できるパブリッククラウドは，信頼性やセキュリティなどのサービスレベルが明確に規定されていないことが多く，企業システムとしての利用を躊躇(ちゅうちょ)させる一因となっている。

当社では，高セキュリティ・高信頼性を実現するインフラ基盤技術をベースに，特定の限られたユーザー(企業内，企業グループなど)に閉じた形での利用を前提として，クラウド技術を適用した企業情報システムへの取組みを推進している。

本稿では，具体的なサービス内容とそれらを実現するための基盤技術，及び将来に向けた最新技術の研究内容について述べる。

2. クラウドの現状

2.1 クラウドとは

図1に示すように，従来の情報システムでは“ユーザーがハードウェアやアプリケーションを自前で購入・管理”していたものから，クラウドでは“情報システムをユーザー側で所有せず，サービスとして使用した分を支払う利用形態”となる。例えば，従来はパッケージソフトウェアを購入して利用していた形態から，クラウドではネットワーク経由でアクセスしてアプリケーションを利用する形態に変わる。

また，クラウドで利用できるサービスは，XaaS(X as a Service)という言い方で大きく3つに分類される(**表1**)。

2.2 クラウドへの期待と懸念

ユーザーから見たクラウドへの期待と懸念については，いろいろなメディアを通じて報告されている。一般に言われているところでは，期待としては，①ITリソースを柔軟に拡張，縮小できること，②サービス開始までの期間が短くて済むこと，③自前でシステムを構築しないので初期投資が抑制されコスト削減が図れること，というような点が挙げられている。

次に利用に際しての懸念事項を**図2**に示す。

図2から，①重要な情報を外部の事業者に預けるというセキュリティ上のリスク，②従来に比べて本当にコストダウンできるか，③サービスレベルが不明瞭(ふめいりょう)，又はサービスレベルが保証されていないというリスク，④社内システムとの連携の困難さなどがクラウドを利用する際の懸念材料になっていることがわかる。

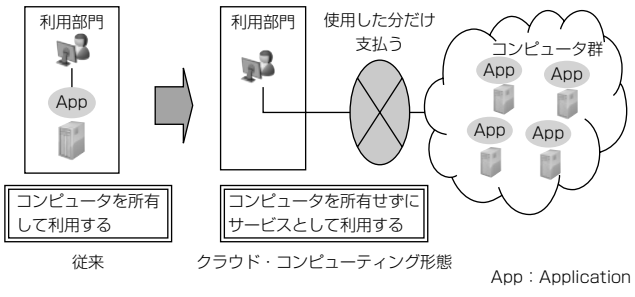


図1．クラウドコンピューティングの概念

3. 三菱電機グループの取組み

2. 2節で述べたような，クラウドの利用におけるユーザーの懸念を解消するために，次のような方策を実現することが必要となる。

(1) 個人情報などの重要なデータを安心・安全に保管できる強固なセキュリティ機能を持つデータセンターと，その運用管理基盤を提供できること

(2) 情報漏えい対策などのために，セキュアな認証基盤を提供できること(特定のユーザーだけがアクセス可能であることを保証するアクセス制御機能など)

(3) 社内の業務システムとの連携を容易に行うことができるシステム間連携手段を提供できること

(4) (1)～(3)で述べた基盤を活用し，サービスレベルを保証したSaaS型サービスとその基盤を提供できること。

三菱電機グループではこれらの実現に当たり，セキュリティ及び信頼性を担保するため，不特定多数のユーザーが利用するパブリッククラウドではなく，特定の限られたユーザー(企業内，企業グループ向けなど)によって独占的又は排他的に利用できる“プライベートクラウド／マネージドクラウド”を対象に，そのシステム構築や運用管理サービス，SaaS型サービスの提供を推進している(**図3**)。

表1．クラウドのサービス分類

サービス分類	内容
SaaS(Software as a Service)	アプリケーションを提供するサービス
Paas(Platform as a Service)	アプリケーションの開発環境，実行環境を提供するサービス
IaaS(Infrastructure as a Service)	ITリソース(仮想マシン，OS，ストレージ等)を提供するサービス

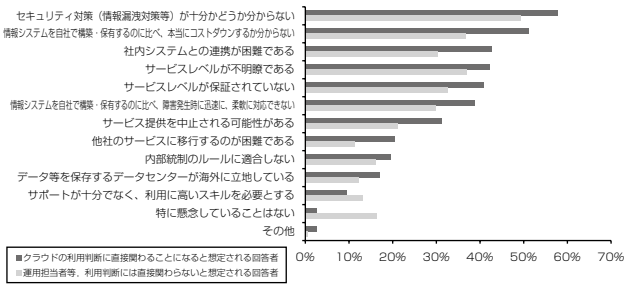


図2．クラウドコンピューティングの利用を控える理由／利用に当たっての懸念(1)

なお本稿では，自社内のデータセンターに情報システムを設置する形態を“プライベートクラウド”，社外のデータセンターに委託する形態を“マネージドクラウド”と呼ぶ。

三菱電機グループの具体的な取組み内容を**表2**に示す。太陽光発電システムを採用したMINDの最先端データセンター，仮想化やセキュア認証などの基盤技術，これらの技術に基づく各種SaaSサービスについて，次に代表的な事例を述べる。詳しい内容に関しては，この特集号の該当する論文を参照されたい。

3.1 高セキュリティ・高信頼を実現するインフラ基盤技術

3.1.1 データセンターにおける最先端技術

MINDの最新データセンターでは，重要なシステムを震災から保護するためにビル全体を免震構造とするとともに，集積度の高いシステムを収容するための高度な冷却技術を採用するなど，堅牢(けんろう)なファシリティを実現している。また，サーバ室へのアクセスに生体認証と共連れ防止のサークルゲートを組み合わせることで厳密な入退室管理を行い，高度な物理セキュリティを確保した。

ネットワークについては，マルチキャリアによる多様かつ高速な接続を準備するとともに，負荷分散・帯域制御等のトラフィック制御技術によってトラフィック増に対応する。これらに加え，各種の省電力設備の採用と太陽光発電システムの導入によって，地球環境に配慮しながらクラウド技術への適応を実現している。

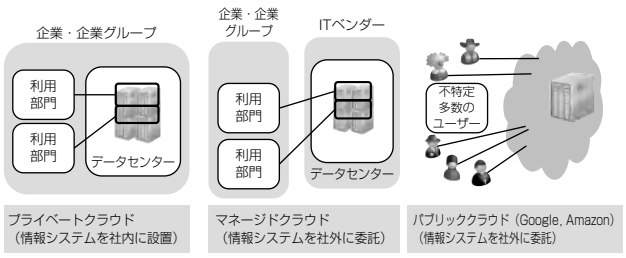


図3．当社の取組み形態

表2．三菱電機グループの取組み内容

分類	社名	取組み内容
高セキュリティ・高信頼を実現するインフラ基盤技術	MIND	データセンターにおける最先端技術
	MDIT	仮想化技術(VMINTEGRA)
	MDIS，MIND ジャパンネット㈱	セキュアな認証基盤技術
	MDIT	システム間データ連携基盤技術
SaaS型提供サービス	MDIS MDIT	グリーンITサービス (Green by Cloud)
	MDIS ジャパンネット㈱	ヘルスケアセキュリティサービス
	MIND	SaaS型セキュリティ診断サービス
将来技術	三菱電機㈱ (情報技術総合研究所)	秘匿照合技術 仮想化技術を用いた信頼性向上技術

MDIS：三菱電機インフォメーションシステムズ㈱
MDIT：三菱電機インフォメーションテクノロジー㈱
MIND：三菱電機情報ネットワーク㈱

3.1.2 仮想化技術

サーバ仮想化技術が急速に進歩しており，この数年で大企業を中心に仮想化によるサーバ統合が進展してきた。しかしまだ，サーバ統合におけるリソース設計，パフォーマンス評価，仮想環境構築ノウハウを持つ技術者は不足しており，そのために構築・運用コストは高く，仮想化による中小規模サーバ統合普及の阻害要因となっている。

三菱電機インフォメーションテクノロジー㈱(MDIT)は，これらの課題を解決するため，プラットフォーム統合ソリューション“VMINTEGRA(ヴイエムインテグラ)”を開発・製品化した。VMINTEGRAは，仮想化市場で高いシェアと実績のあるVMware社のVMware(注2) vSphere4に運用監視機能をパッケージした製品で，“簡単導入”“簡単運用”“安心サポート”の3つのコンセプトの下，中堅・中小企業でのサーバ統合の促進を目指している。

3.1.3 セキュアな認証基盤技術

企業や医療機関などに各種のサービスを提供する場合，アプリケーションやネットワーク等の様々なレベルで，利用者に応じたアクセス制御が重要であり，セキュアな認証基盤を確立する必要がある。

認証情報は個人情報であり，高度な機密情報であることから，それらは企業内のシステムに安全に保管した上で，外部のクラウドシステムと既存の企業内システム間での認証連携を実現する方式を確立した。認証機能やデータのアクセス制御機能の実装に当たり，SAML(Security Assertion Markup Language)やXACML(eXtensible Access Control Markup Language)といった標準仕様を採用し，オープンソースソフトウェアも活用しながら，再認証が不要なシングルサインオン機能を独自に開発し，実証実験を通してその有効性を確認した。

3.1.4 システム間データ連携基盤の構築

トランザクションHubとは，トランザクションデータを蓄積して，そのデータを再利用する業務アプリケーションとの間で交換する“データ交換の場”である。一般に，業務アプリケーションを単純にSaaS化すると，社内のシステムとSaaS化したシステムの間の連携が分断されてしまうという問題点がある。

業務アプリケーションはトランザクションHubを経由してデータを交換することで，他の業務アプリケーションの影響を受けない独立した部品となる。そのため，システムの交換，新たなシステムの追加，SaaS化等を容易に実現することが可能となる。

3.2 SaaS型提供サービス

3.2.1 グリーンITサービス“Green by Cloud”

2010年4月から施行された改正省エネ法では，“事業者単位”でのエネルギー管理が義務付けられるようになった

(注2) VMwareは，VMware, Inc. の登録商標である。

ため，ビルのオーナーだけでなく，そこに入居しているテナント事業者もエネルギー使用量を把握する必要がある。そこで当社では，ビルオーナーとテナントが協力して環境情報データの見える化等に取り組み，課題を解決するグリーンITサービス“Green by Cloud”の提供を開始した。これは，三菱電機グループの総合力を生かし，ビルや工場内の設備・機器，セキュリティシステムとITシステムをネットワークで接続し，建物を丸ごと省エネルギーする新しいサービスである。

Green by Cloudは，CO_2排出削減施策のPDCA（計画・実行・評価・改善）サイクルを支援するトータル環境経営ソリューション“DIALCS”，大量に発生する環境情報データを分析する環境経営ソリューション“MELGREEN”，及びこれらが動作する最先端のデータセンターをサービス基盤としている（**図4**）。このサービスによって，法規制の対応に加え，ビルオーナーはビルの付加価値向上，テナントは企業価値の向上というメリットが得られる。

3.2.2　ヘルスケアセキュリティSaaSへの取組み

ヘルスケア分野では，医療情報等の機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。三菱電機グループでは，厚生労働省等のガイドラインを遵守できる低コストのハイレベルセキュリティサービスを医療機関等に提供することを目指して，ヘルスケアセキュリティSaaSシステムの構築と評価を実施した。

これらの成果をベースに，円滑な医療情報交換や保存が義務付けられた医療情報の外部保存を行える環境の提供を実現していく。また，真正性を担保するための電子署名・タイムスタンプ付与をSaaS型サービスとして提供し，電子署名付き文書の文書交換や外部保存に対応したサービスと連携し，ワンストップで地域医療連携のニーズにこたえていく（**図5**）。

4. 更なる技術開発への取組み

従来以上の高セキュリティ・高信頼を実現するための研究開発として，暗号化したまま個人識別情報を照合する技術と仮想化技術を用いた信頼性向上技術について述べる。

4.1　クラウド時代の個人認証“秘匿照合技術”

近年，ネットワーク経由でサービスを利用するクラウドの進展によって，電子メール運用や文書管理をデータセンターに委託する需要が高まっている。この際に使われる本人認証は，事前に登録した個人識別情報と認証時に入力される個人識別情報を照合して行われるが，個人識別情報は厳格な保護が求められることから，暗号化した上でデータセンターに送られ管理される。しかし，これまで提案されている技術では，照合する際に復号が必要なケースや，暗号化情報からその一部が類推可能なケースがあるなど，復号情報の漏えいの可能性を完全には否定できないという問題があった。また，登録者数が多くなると認証に時間がかかるという問題を持つものもある。

三菱電機は，復号することなく暗号化したまま個人識別情報を照合する秘匿照合技術を開発した（**図6**）。これによって，データセンター内の個人識別情報の利用・管理を安全に効率良く行えるようになる。顔・指紋・筆跡・文字・

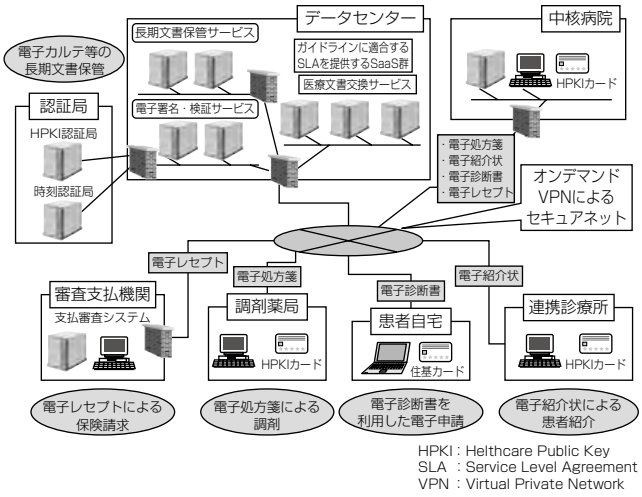


図5．ヘルスケアセキュリティSaaSの概念図

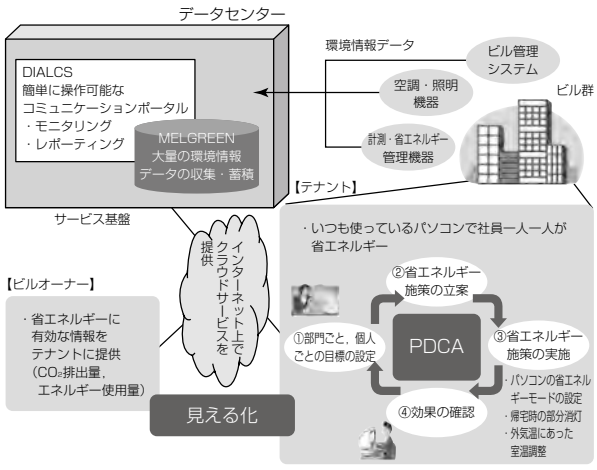


図4．Green by Cloudとサービス基盤

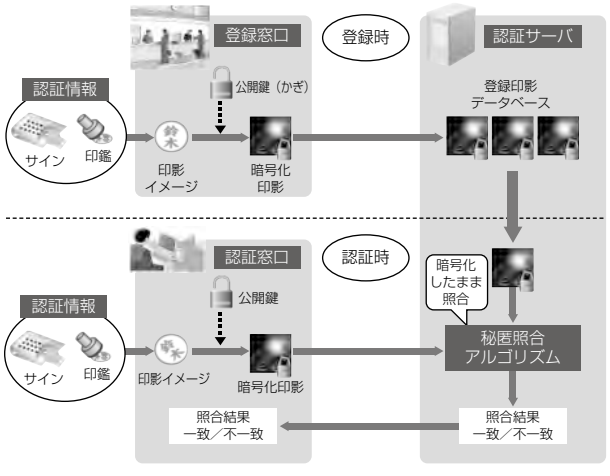


図6．秘匿照合技術

印影などの個人識別情報は，一般的に複数の特徴で表現される。例えば，顔は，輪郭，色，大きさ，目と鼻の位置関係など，複数の特徴を数値化し，その数字の組（特徴ベクトル）で表現される。本人認証は，認証時に取得した特徴ベクトルを登録時の特徴ベクトルと比較し，両ベクトルの距離から類似，又は一致した場合に同一人物と判定する。したがって，この特徴ベクトルは厳格な管理が必要であり，特徴ベクトルは暗号化され認証サーバに格納される。

この秘匿照合技術は，2つの暗号情報の算術演算が可能な準同型暗号を用い，暗号化された特徴ベクトル間の距離を，認証サーバとの1度のやり取りで照合する。これによって，照合の過程で特徴ベクトルが復号されることなく，データセンターにおける個人情報の秘匿が，少ない通信時間で実現できる。

4.2　仮想化技術を用いた情報システムの信頼性向上技術

重要な社会インフラを支える情報システムでは，サーバを2重系構成として信頼性を高めている。2重系サーバでは，稼働中のメインサーバが故障した際，待機サーバに切り替えて業務を継続できるが，故障したサーバが復旧するまでの間は信頼性が低下するので2重系へのすみやかな復旧が求められる。2重系以上の信頼性を持たせるには，業務ごとに予備専用のサーバを準備する3重系構成が必要であり，また，データの保存に，信頼性の高い高価な外部共有ディスクを用いる構成が採用されており，情報システム構築コストの増大に結びついている。三菱電機は，仮想化技術によって，システムを構成するサーバ群の空き資源を活用して，2重系構成を短時間で復旧する技術を開発した（**図7**）。この技術によって，3重系構成と同等の信頼性を確保しながら，予備専用サーバと外部共有ディスクを不要とし，システムの構築コストを抑制できる。

サーバの仮想化技術によって，サーバ群の空き資源（CPU（Central Processing Unit），メモリ，ディスクなど）を活用して故障したサーバと同等の処理ができる代替環境を自動で構築し，2重系構成に復旧する。これによって，3重系構成と同等の信頼性を確保しながら，予備専用サーバ群は不要となる。

また，各仮想サーバの実行環境であるOSやアプリケーションのみならず，代替環境の構築に必要な復旧用データもすべて，情報システムを構成するサーバ群の内蔵ディスクに格納する。復旧用データは，各仮想サーバで共通のOS部分と，固有のアプリケーション部分に分けて格納することで必要なディスク容量を削減しており，これによって，高価な外部共有ディスクを使用する必要がなく，システムを低コストで構築でき，万が一共有ディスクが故障した際の全業務停止のリスクも回避可能となる。

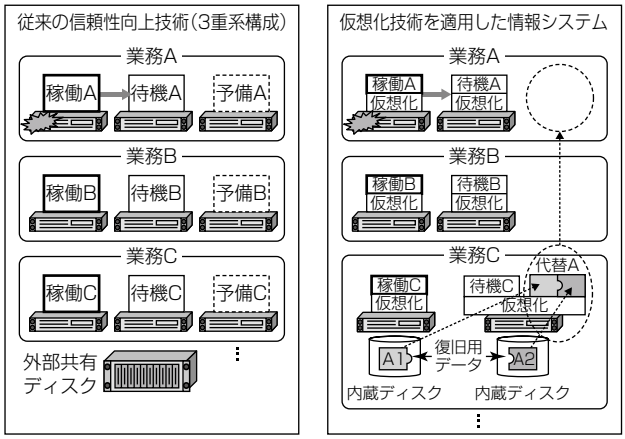


図7．仮想化技術を用いた信頼性向上技術

5. むすび

企業情報システムへのクラウド技術の適用に対する期待が高まっている一方，セキュリティや信頼性の面で不安を感じるユーザーも多く，これらの不安感を払拭するための努力が必要である。

三菱電機では，これまで培ってきた高信頼・高セキュリティのインフラ基盤技術に関する豊富な経験を生かすとともに，数年先を見据えた独創的な研究開発も並行して進めており，今後も付加価値の高い企業向けITサービスの提供を推進していく。

参考文献

(1)　経済産業省：情報システム・ソフトウェアの信頼性及びセキュリティの取組強化に向けて～豊かで安全・安心な高度情報化社会に向けて～―中間報告書―（2009）

特集論文

データセンターにおける最先端技術

稲坂朋義*
西宮哲進*

Advanced Technologies in Data Center

Tomoyoshi Inasaka, Tesshin Nishimiya

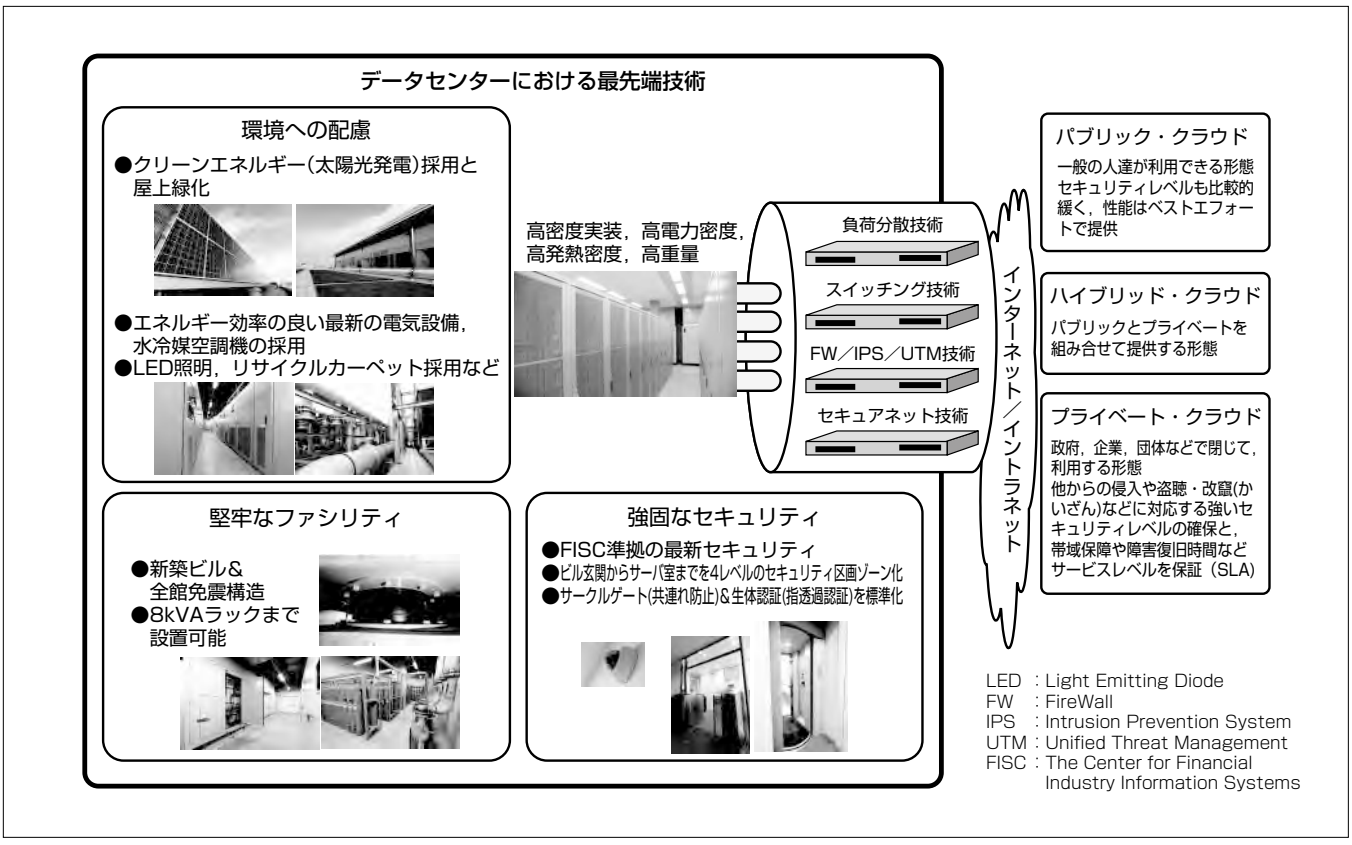
要　旨

情報システムの利用形態の一つとして，インターネットなどによって広域に分散したコンピューティングリソースを使って，ハードウェア，ソフトウェアやアプリケーションのサービスを利用者へ提供するクラウド技術を適用した情報通信システムが注目されている。その市場規模は，2012年度に2009年度の約8.3倍の2,065億円になると予想されている(1)。

このような情報化社会の変化を受けて，関係省庁の調査研究と，それに関連した実証実験を含む研究開発事業や，業界団体(ASP(Application Service Provider)・SaaSインダストリ・コンソーシアム，日本データセンター協会など)でのクラウド技術をキーワードとした活動が活発化してきている。

情報化社会の変化の潮流に合わせて，企業・官公庁が所有している情報システムをデータセンターへ移設・集約するニーズが高まっており，データセンター及びデータセンターに集約された情報システムと利用者をつなぐネットワークが，情報化社会のインフラとしてますます重要となる。また，情報システムがデータセンターに集約されることは，それにかかわる電力消費がデータセンターに集中することになるので，国内のCO_2排出量削減の観点からデータセンターには高い電力利用効率が求められる。

三菱電機情報ネットワーク㈱(MIND)では，1999年から10年以上にわたってデータセンター事業を展開しており，現在東京都内に3拠点，名古屋，大阪に各1拠点の5拠点で事業を行っている。これまでの事業実績と豊富な経験に基づいて，MINDが考える最先端のデータセンターの姿と，それを実現するインフラ，サービス，ネットワークの主要技術について述べる。



MINDデータセンターの特徴

データセンターは，コンピュータパワー集約にこたえられる堅牢(けんろう)なファシリティと強固なセキュリティを備えるとともに，情報システムの省エネルギーに貢献する高いエネルギー利用効率とクリーンエネルギーの採用などグリーンな環境への取組みを推進する。また，利用者がクラウド技術を適用した情報通信システム環境を安全・安心・快適に利用できるネットワーク環境を備える。

*三菱電機情報ネットワーク㈱

1. まえがき

情報システムが所有から利用へと変化することに伴い，情報システムのデータセンターへの移設・集約が進み，データセンター内の情報システムが大規模化(IT機器台数の増加)している。大規模化した情報システムを限られたスペースに収容するためには，情報システムを高密度に実装することが不可欠の要件となる。そのため高い電力密度，高い発熱密度に対応した，電力利用効率や冷却効率に優れた堅牢なインフラがデータセンターに要求される。加えて，クラウド技術を適用した情報システムは，利用者の増減や利用形態の変化によって，システム規模が変化することが前提であり，堅牢性を維持しつつ，迅速かつ柔軟に対応できることもデータセンターのインフラに求められる。

また，情報システムのデータセンターへの設置増加に伴って，データセンター内の情報システムと利用者をつなぐネットワークは，これまで以上にデータセンターへのトラフィックが集中することに加えて，外部からのアクセスの増加が想定され，高帯域確保や高セキュリティなどへの対応が重要になっている。

MINDでは，これらクラウド技術を適用した情報通信システムに対応して，データセンターに関する様々な技術に取り組んできている。本稿ではその概要について述べる。

2. データセンターのインフラ技術

2.1 概　要

データセンターのインフラには，ブレードサーバに代表されるように，高電力・高密度実装に対応できる電力供給能力・冷却能力と，建物・インフラ設備の高い堅牢性及び強固なセキュリティが求められる。

MINDの最新データセンターとして2009年4月に開設した東京第3データセンター(以下“東京第3iDC”という。)の概要を**表1**に示す。

表1の項目の中で，8kVAラックを実現する高密度・高電力に対応するエネルギー利用効率に優れた冷却技術，セキュリティ対応，環境への配慮，グリーンITについて次に述べる。

表1．東京第3データセンターの概要

項目	内容
ファシリティ	新築ビル＆全館免震 8kVAラック
セキュリティ	FISC準拠 共連れ防止＆生体認証
ネットワーク	マルチキャリア MIND Multi iDC Network
グリーンIT	高エネルギー利用効率 太陽光発電，LED照明

iDC：internet Data Center

2.2 堅牢なファシリティ(高密度・高電力対応冷却技術)

冷却効率を良くするには，次のような対策が必要である。

(1) 空調機からの冷気を，ラックに収容された冷却対象機器へできる限りロスなく与えること
- ●冷却対象機器から排出される暖気の，冷気への混入防止
- ●不必要箇所への冷気漏れ防止など

(2) 冷気の温度をできるだけ均一にすること
- ●温度むら等による一部の冷やし過ぎの排除

(3) 冷気風路を確保すること
- ●電源ケーブルや通信ケーブルの敷設ルートの最適化

(4) 暖気リターン風路を確保すること
- ●天井のリターン口の最適配置など

また，冷却システムに最適なラック配置とするためには，高発熱ラックの集中配置の排除，発熱量の均等化などが必要である。

MINDで採用した高効率冷却技術について**図1**に示す。

高効率冷却技術の適用によって，8kVAラックの配置を可能としている。

さらに，ラック当たり8kVA以上についても，そのラックを強制的に冷却して暖気をサーバ室内に排気しない個別冷却技術を適用して，配置を可能としている。

2.3 強固なセキュリティ

官公庁の情報システムや企業の基幹システム，クラウド技術を適用したサービス提供システムなど，情報システムを収容するデータセンターには，強固な物理セキュリティの確保が要求される。東京第3iDCは，FISC(㈶金融情報システムセンター)が定めている“金融機関等コンピュータシステムの安全対策基準”の“設備基準”の不可欠事項をすべてクリアしており，金融機関等のコンピュータシステムを収容できるセキュリティレベルを確保している。

セキュリティレベルの強化と利用者の利便性は相反するので，多くの人が立ち入る比較的セキュリティレベルの低いエリアは利便性を優先し，情報システムを収容するサーバ室は利便性を多少犠牲にしてもセキュリティを優先させるコンセプトによって，東京第3iDCでは**図2**に示すように，4段階のセキュリティレベルで管理している。

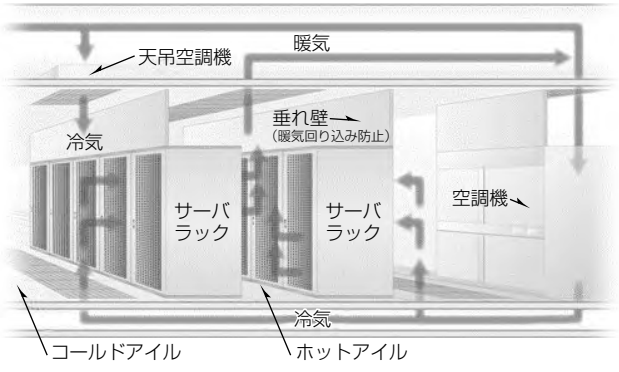


図1．冷却システム構成例

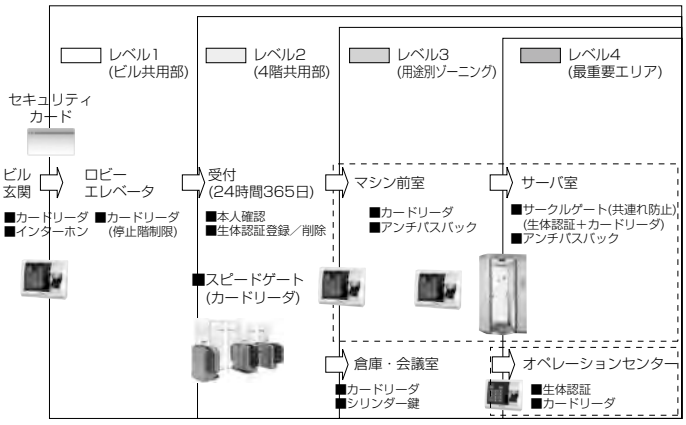


図2．4レベルの物理セキュリティ管理

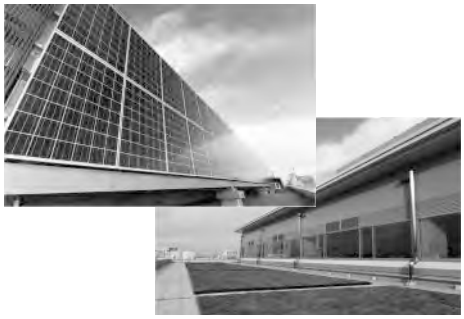


図3．太陽光発電システムと屋上緑化

サーバ室は最もセキュリティレベルの高い“レベル4”に設定して，生体認証による本人確認と，サークルゲートを使った共連れ防止による不許可者入室の排除と，ラックの二重鍵(かぎ)採用，サーバ室内の監視カメラによる不審行動監視などによって，強固な物理セキュリティを実現している。

2.4　環境への配慮

IT機器の消費電力量が，2025年度には2005年度比5.2倍(2,400億kWh)，国内総発電量の約20%を占めると予測されている[(2)]。クラウド技術を適用した情報通信システムの進展に伴い，これらのIT機器は，データセンターに集約される方向にあり，エネルギー利用効率に優れたデータセンターがこれまで以上に求められる。

東京第3iDCは，先に述べた冷却技術の適用や最新鋭の省電力設備の導入による業界最先端の高い電力利用効率の実現に加えて，自然エネルギー利用の太陽光発電システムの導入や屋上緑化など，地球環境に配慮したグリーンIT対応データセンターである(**図3**)。

3. データセンターのネットワーク

3.1　概　　要

データセンターでは，サーバの統合化及び仮想化に伴い，トラフィック集中や輻輳(ふくそう)にも耐えられる可用性の高い帯域制御と負荷分散技術，及び安定性のある高信頼なリモートアクセス環境が必要になる。また，クラウド技術を適用したシステムの安全・安心の確保には，高度なネットワークサービス品質の提供が必要になる。

ここではMINDのトラフィック制御にかかわる技術について述べるとともに，特に安全にかかわるリモートアクセス環境について詳しく述べる。

3.2　高トラフィックに対応するネットワーク

サーバの統合化が進めば，データセンター内へのトラフィックが増加し，通信遅延や帯域不足が発生する。また，サーバの仮想化が進めば，ネットワークリソースの状況把握や，最適なリソース配分が重要となる。

このため，次のようなネットワーク制御技術を用いた運用を行っている。

(1)　ネットワークの帯域制御技術

データセンター内に入ってくるネットワーク・トラフィックやパケットの測定を行い，一部のユーザーによる帯域の逼迫(ひっぱく)や帯域の占有を防ぐために，帯域の最高速度の規制値を制御し，ユーザーごとの帯域保証を行うことで安定した通信を確保する。また，最低速度でも保証値を制御することで，トラフィック量に見合った課金の提供も可能とし，ユーザーニーズに対応する。

(2)　WAN高速化技術

利用者とデータセンター間のアプリケーション通信の遅延などから回線の実効速度が低下するため，回線帯域を増強することなく，アプリケーション遅延に対応したネットワークの最適化を実現することで，投資コストを抑えた安価で安定した通信サービスを提供する。

(3)　トラフィック負荷分散技術

データセンター内に入ってくるネットワーク・プロトコルやアプリケーション・トラフィックを管理し，ユーザーごとの仮想サーバやその他のリソースへ分散する。これによって，特定の仮想サーバへアクセスが集中することによってシステムの性能が低下したり，システムダウンするのを防ぐことができ，利用者へ安定したサービス品質を提供するとともにリソースの利用効率向上にもつながる。

3.3　リモートアクセス環境

モバイル端末の普及に伴い，リモート環境からのアクセス利用が拡大し，多数の仮想サーバごとに様々なユーザーがアクセスするようになる。また，リモートアクセス環境では，セキュリティ面に不安を持つユーザーも多い。このため，データセンター内の仮想サーバまでのアクセス方法やユーザー認証が重要になる。

MINDは，他社に先駆け1997年から，リモート環境から社内へアクセスするモバイルネットワークサービス[(3)]を提供しており，認証技術，認証システムの運用ノウハウ技術を蓄積してきた。仮想サーバごとにこれらのユーザー認証技術を活用し，より強固なセキュリティを確保することができる。

図４．SecurIDカード

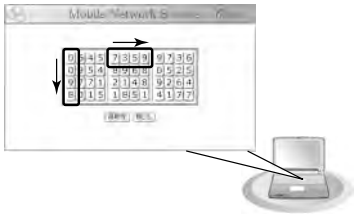


図５．マトリクス認証

図６．ikey2032

図７．PUPPY

代表的な認証方式としてワンタイムパスワード方式がある。他人の覗(のぞ)き見に対抗したい場合などには，１分ごとにパスワードが変わるトークンコードと，ユーザーが記憶している暗証番号とのセットで認証するSecurIDカード(注1)（**図４**）や認証媒体などを持ち歩きたくない場合は，毎回異なるマトリクス表の中から特定位置の数字をパスワードとして使用し認証するマトリクス認証(注2)（**図５**）によって実行するものである。

また，USB(Universal Serial Bus)メモリ媒体を活用した認証方式もある。成りすまし防止などを行いたい場合は，SafeNet社製のikey2032(注3)（**図６**）を利用した公開鍵暗号方式によってパスワードを暗号化し認証するUSBトークン認証がある。本人認証を行いたい場合は，SONY製のPUPPY(注4)（**図７**）を活用し，パソコンのUSBスロットに差し込んだ指紋認証装置から秘密鍵を読み出し，パスワードを生成するUSBメモリ上での指紋認証がある。ほかにも発信者の電話番号を登録する認証，又は固定パスワード認証などがある。

(注１)　SecurIDは，RSA Security Inc.の登録商標である。
(注２)　マトリクス認証は，㈱シー・エス・イーの登録商標である。
(注３)　ikey2032は，SafeNet社の登録商標である。
(注４)　PUPPYは，ソニー㈱の登録商標である。

4. むすび

昨今，厳しい経営環境の中で，各企業はコスト削減や資源効率化のキーワードとして，クラウド技術を適用した情報通信システムに期待しており，その構築基盤としてデータセンターの重要性はますます高くなる。

現在は，クラウドコンピューティングサービス市場の約80%以上をSaaS(Software as a Service)型サービスが占めるが(1)，今後カスタマイズ機能の提供を目的としたSaaS型サービスのPaaS(Platform as a Service)化が進むと考える。

また，大企業は情報保護の観点から，一般共用のパブリックな形態よりも単一組織内で利用するプライベートな形態を好む傾向にあり，プライベートクラウド市場が大企業を中心に成長していくものと考える。プライベートクラウド市場の成長に合わせて，カスタマイズ用プラットフォームとしてのPaaSや，仮想サーバやストレージを提供するIaaS(Infurastructure as a Service)のサービス基盤として，ネットワークやデータセンターはなくてはならないものとなっていく。

クラウド技術を適用した情報通信システムを収容するデータセンターの技術について述べたが，所有から利用への変化と，クラウド技術を適用した情報通信システム化の潮流に対する利用者の要望にこたえられるよう，データセンターのインフラ，ネットワーク，サービスなどの開発・提供に取り組んでいく。

参考文献

(1)　国内クラウド関連市場規模の現状と中間予測報告，ノークリサーチ PRESS RELEASE，2009年8月25日
http://www.norkresearch.co.jp/pdf/2009cloud.pdf
(2)　グリーンITイニシアティブの推進，経済省
http://www.csaj.jp/seminar/2008/081006_meti.pdf
(3)　工藤和仁，ほか：いつでも，どこでも簡単・安心に利用できるモバイルネットワークサービスソリューション，三菱電機技報，**79**，No.4，275～278（2005）
(4)　稲坂朋義，ほか：グリーン対応データセンター，三菱電機技報，**83**，No.7，429～432（2009）
(5)　国内SaaS/XaaS市場規模予測を発表，IDC Japan プレスリリース，2009年7月22日
http://www.idcjapan.co.jp/Press/Current/20090722Apr.html

特集論文

企業インターネットシステム構築・運用サービス“Internet-S³”

青木君仁* 前田純一*
佐藤 仁* 鈴木敏也*
緑 理一郎*

"Internet-S³" : Internet System Solution Service

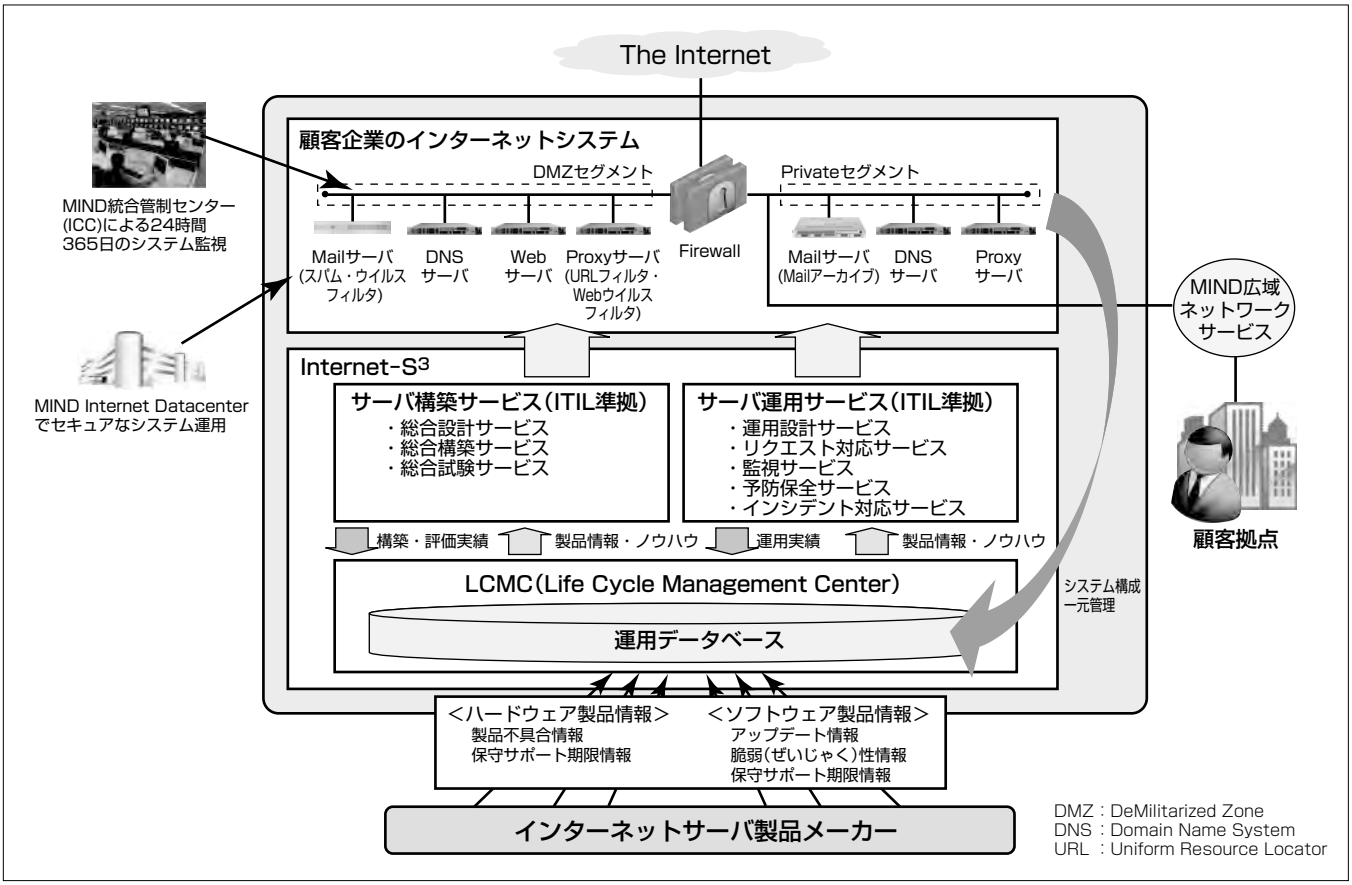
Kimihito Aoki, Hitoshi Sato, Riichiro Midori, Junichi Maeda, Toshiya Suzuki

要 旨

電子メールやWebブラウズなどのインターネット利用環境は，今や企業活動に不可欠のITビジネス基盤となっており，セキュアかつ高信頼であることが求められている。このため，各企業のITビジネス基盤は，電源，空調，耐震の対策，情報セキュリティ対策，ハードウェア故障対策，ソフトウェア不具合対策，システム変更時の誤操作対策など，数多くの脅威に対応する必要があり，情報システム部門はその運用負荷に悩んでいる。

三菱電機情報ネットワーク㈱（MIND）のInternet System Solution Service（Internet-S³：インターネット・エス・キューブ）は，MINDのネットワークサービス，データセンターサービス，サーバプラットフォームサービスを三位一体で提供し，顧客企業のセキュリティポリシーに合わせたインターネット利用環境の設計・構築から，MINDのインターネットデータセンターによるシステム運用まで，ワンストップのアウトソーシングサービスを提供する。

このサービスは，MIND統合管制センター（ICC）による24時間365日の監視，予防保全，キャパシティ管理，オンライン診断，インシデント対応など，MINDの豊富な経験に裏付けられた安全，安心な運用を特長としており，各サーバのライフサイクル情報を管理するLCMC（Life Cycle Management Center）を基盤とし，ITIL（Information Technology Infrastructure Library）に準拠したシステム運用を，企業の情報システム部門向けの業務アウトソーシングサービスとして提供する。



Internet-S³のサービスイメージ

企業のインターネット利用環境を構成するMail，Proxy，DNS，Webなどのサーバ群，及びこれらのサーバにセキュリティ機能を付加するアンチウイルスやスパムフィルタなどの各種セキュリティサーバを設計・構築する。また，MINDのデータセンターやLCMCによる製品・サービスのライフサイクル管理を基盤として，ITILの管理プロセスに準拠した安全・安心な運用サービスを提供する。

*三菱電機情報ネットワーク㈱

1. まえがき

Internet-S³は，メール，Proxy，DNS，Webといった企業のインターネット利用環境を構成するサーバ群を顧客企業の要求に合わせて設計・構築し，MINDデータセンター，MIND統合管制センター(ICC)で運用を行う情報システム部門向けの業務アウトソーシングサービスである。

2. Internet-S³サーバ構築サービス

サーバ構築サービスは，各顧客企業向けに最適化したインターネット利用環境を提供するため，総合設計，総合構築，総合試験の3つのサービスで構成される。

2.1 総合設計サービス

顧客要求を基にした機能設計，性能計算，信頼性設計，ネットワーク構成設計，機器選定を行う。特に信頼性設計では可用性を確保するために，異常検知から復旧確認までの仕組みやデータバックアップ・リストア手順の作成を重点的に行う。成果物は，基本設計書，性能目標値・信頼性設計書，機器一覧表，ネットワーク構成図，ラック構成図，IPアドレス管理表がある。

2.2 総合構築サービス

総合設計サービスによるシステム全体の基本設計を基に，サーバ個別の機能設計，機器手配，構築，設置，単体動作試験を実施する。構築に当たっては，外部からの攻撃リスクを回避・低減できるよう，ログインユーザーの制限，複雑なパスワードの使用，不要なサーバプロセスの停止，不具合がないことを確認した最新ソフトウェアの使用，ソフトウェアのバージョン情報隠蔽(いんぺい)，アクセス制限といった対処を行う。

サービス対象となる代表的なサーバを**表1**に示す。

表1．総合構築サービス 対象サーバ

対象	構築サービス
メールサーバ	ソフトウェア：Postfix ＜オプション＞ (1) POP3サーバの構築(機能追加) ソフトウェア：Dovecot (2) ウイルス対策機能(セキュリティ向上) ソフトウェア：IMSS(注1) (3) スパムフィルタ機能(生産性向上) アプライアンス製品：IronPort(注2) (4) メールアーカイブ機能(内部統制) ソフトウェア：GUARDIANWALL(注3)
Proxyサーバ	ソフトウェア：Squid アプライアンス製品：BlueCoat(注4) ＜オプション＞ (1) ウイルス対策機能(セキュリティ向上) (2) URLフィルタリング機能(生産性向上)
DNSサーバ	ソフトウェア：BIND ＜オプション＞ (1) コンテンツ機能とキャッシュ機能のハードウェア分離 (セキュリティ向上，性能向上) (2) スレーブサーバの構築(可用性向上)
Webサーバ	ソフトウェア：Apache(注5) ＜オプション＞ (1) SSLサーバ証明書の手配／導入(暗号化通信対応)

IMSS ：InterScan Messaging Security Suite
BIND ：Berkeley Internet Name Domain

(注1) IMSSは，トレンドマイクロ㈱の登録商標である。
(注2) IronPortは，Cisco Systems, Inc. の登録商標である。
(注3) GUARDIANWALLは，キヤノンITソリューションズ㈱の登録商標である。
(注4) BlueCoatは，BlueCoat Systems, Inc. の登録商標である。
(注5) Apacheは，The Apache Software Foundationの登録商標である。

2.3 総合試験サービス

総合設計サービスの設計値を満足していることの確認を目的とする。メール送受信，社内外Webブラウズなどの機能が正常動作すること，リクエスト処理数や応答時間，同時接続数などの性能目標を達成していること，システムの異常発生を検知できること，異常箇所に応じた縮退稼働の動作が設計どおりであることなどを評価する。

3. Internet-S³サーバ運用サービス

サーバ運用サービスは，5つのサービスで構成される。運用サービス体系を**図1**に示す。

3.1 運用設計サービス

構築が完了したサーバに対して顧客の要件を満たすように運用プロセス，ルールを設計し，次のドキュメントを整備する。

(1) 運用仕様書

システム監視(監視対象，監視方法，監視結果報告)，セキュリティパッチ適用や検索エンジン，パターンファイル更新，バックアップ，障害対応，各種設定変更などについて，実施内容を定義した仕様書である。

(2) 運用体制図

運用時における顧客とMINDの連絡体制を定めた資料である。

(3) 保守サポート契約表

ハードウェア及びソフトウェアの保守サポートに関して，保守対象品一覧とベンダー窓口，契約内容，期限を明確に

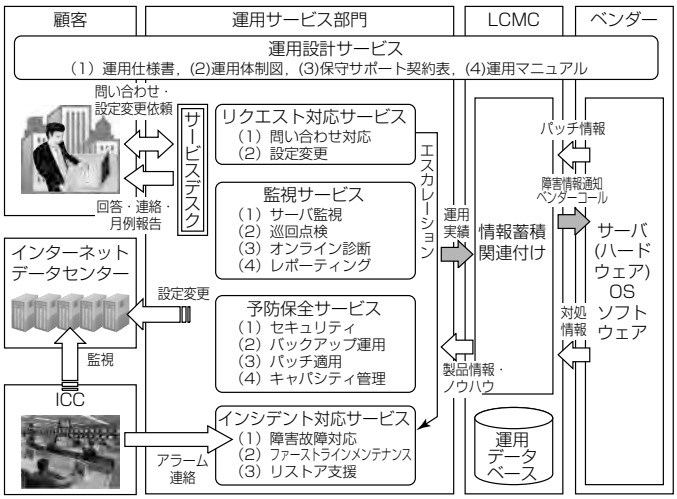


図1．運用サービス体系図

した資料である。

⑷ 運用マニュアル

サーバの操作及び点検手順を説明した資料である。

3.2 リクエスト対応サービス

顧客からの依頼(リクエスト)に基づき，問い合わせ対応や定型的な設定変更及び設定変更に伴う構成管理(ドキュメント改訂)を実施する。主な設定変更は，アカウント登録改廃，DNS登録改廃，SSL(Secure Socket Layer)証明書更新，ファイアウォールポリシー変更などがある。リクエストごとに作業手順書兼チェックリストを準備し，常に作業実施者，チェック者の2名体制で行うことによって，確実なサービスを提供する。

3.3 監視サービス

⑴ サーバ監視サービス

24時間365日の監視体制を持つMIND統合管制センター(ICC)でハードウェアやソフトウェアの稼働状態を監視し，あらかじめ規定した異常を検知した際は所定の連絡先に異常検知を連絡する。サーバ監視サービスには，①稼働監視：ICMP(Internet Control Message Protocol)，Port応答監視，②リソース監視：CPU(Central Processing Unit)使用率，メモリ・ディスク使用量の監視，サーバプロセスの稼働監視，エラーログ監視など，③サービス監視：応答性能監視，メールラウンドトリップ監視などがある。

⑵ 巡回点検サービス

主にハードウェア障害を発見するために，データセンターに常駐する作業員がハードウェアのLED(Light Emitting Diode)状態を毎日1回点検する。

⑶ オンライン診断サービス

パッチ適用サービスやインシデント対応サービス実施後に，システムを停止させることなくメール送受信やWebブラウズなどの操作を行い，その成否や応答速度によって，システム全体の正常性を診断する。

⑷ レポーティングサービス

運用中のシステムの状況として，イベント処理件数や未処理件数，機器のCPU使用率，メモリ・ディスク使用量などの推移について月次レポートを作成し送付する。

3.4 予防保全サービス

⑴ セキュリティサービス

サーバのセキュリティ強度を確保するために，定期的なパスワード変更を実施する。また，日々進化するウイルスやスパムメールの脅威に対応するために，パターンファイルやシグネチャファイルの更新状況を定期的に確認する。

⑵ バックアップ運用サービス

サーバ内のシステムデータや業務データを，運用マニュアルに従って週次や日次でメディアにバックアップする。実行結果を適時確認し，バックアップ失敗時には原因調査を実施し，必要に応じてクリーニング，機器再起動，保守ベンダーコールを実施する。

⑶ パッチ適用サービス

公開されたパッチ情報やバージョンアップ情報を適宜入手し，適用が必要なリストを作成し顧客に提示する。顧客から適用許可を得たパッチ，ファームウェア／ソフトウェアの適用作業を実施する。

⑷ キャパシティ管理サービス

CPU，メモリ，ディスク，回線などのリソース使用量を計測・蓄積し，統計的にシステムの余剰能力を把握する。必要に応じて，システムのメンテナンスや増強，リプレースの提案を行う。

3.5 インシデント対応サービス

⑴ 障害故障対応サービス

監視サービスからの異常検知や顧客からの申告を基に，あらかじめ定められた対応フローに従い，検知内容の通報，機器状態の確認，ログ取得，機器再起動，保守業者のコール，保守作業の現地立会いを実施する。

⑵ ファーストラインメンテナンス

必要に応じて，データセンターに常駐している作業員が顧客の許可の下，機器の電源OFF／ON，ケーブルの抜き差しを実施する。

⑶ リストア支援サービス

バックアップ運用サービスで取得したバックアップデータのリストア作業を支援する。

4. Internet-S^{3}の特長

Internet-S^{3}の特長は，データセンター事業者であるMINDが，ネットワークサービスとサーバプラットフォームサービスを合わせて，三位一体で提供する点である。24時間365日の運用，ITILに準拠したITマネジメントサービス，LCMCによる安全・安心サポート，オンライン診断による正常性確認などのシステム管理業務を，顧客企業の情報システム部門に代わってワンストップで提供する。

4.1 データセンター事業者の運用サービス

MINDデータセンターは，無停電電源設備や非常用電源設備，震度7クラスに対応する耐震構造，消火設備，空調設備，有人監視や監視カメラに加えてICカードや生体認証による入退室管理設備を備えており，充実したファシリティとセキュリティを提供する。また，国内のISP(Internet Service Provider)とはJPIX(JaPan Internet eXchange)，dix-ieでGigabit接続，海外とはPacnet，Sprint，Open Computer Networkと高速回線で接続し，バックボーンも含めた完全二重化構成によって，企業のビジネスユースに耐え得る高速で安定したインターネット接続環境を持つ。

さらに，ICCによるサーバ監視サービスを備え，安全・安心な運用を提供する。

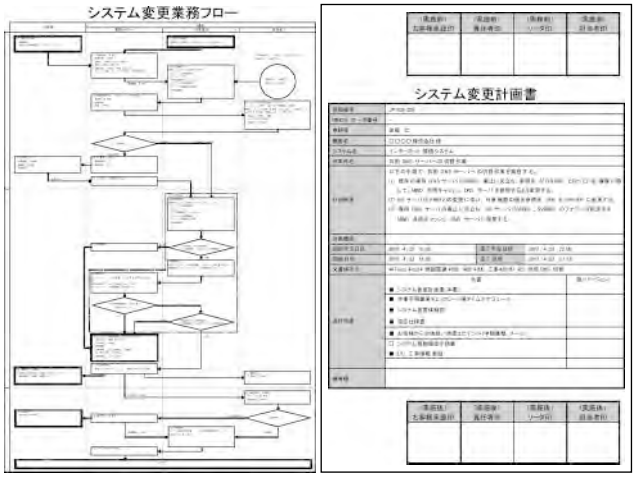


図2．システム変更業務フローとシステム変更計画書

4.2 ITILに準拠したITマネジメントサービス

Internet-S³を提供するスタッフは，ITILの資格取得が義務付けられており，ITILの各管理プロセスに準拠した運用サービスを提供する。特に障害原因の発生源となりやすいシステム変更に関しては，管理規程で作業内容のレビュー・承認が厳密に実施される。レビューは担当者が作成したシステム変更計画書に対して，リーダーレビューと管理者レビューの2段階で実施される。リーダーレビューでは主に技術面から見た作業の正当性がチェックされ，管理者レビューではリスク面や影響範囲がチェックされる。作業手順書には関係者及び顧客への状況報告を実施するための“チェックポイント”と，作業が予定時間どおりに進まない場合や想定した結果とならない場合に，システムを作業前の状態に戻すための“切り戻しポイント”が必ず明記される。

システム変更時の業務フロー及びシステム変更計画書の例を**図2**に示す。

4.3 LCMC

LCMCは，インターネットシステムを構成するアプライアンス製品や，オープンソースの各種サーバのライフサイクルを管理する組織である。メーカーや保守ベンダーから提供されるアップデートプログラムやサポート期限情報を取得し，運用データベースに蓄積するとともに，MINDの運用実績から得た各種製品特性を基に，各サーバへのアップデートプログラムの適用，予防保全修理，リプレースなどを計画し，システムの安定稼働をサポートする。

4.4 オンライン診断

Internet-S³では，多数のサーバや通信機器で構成されるインターネットシステム全体の正常性確認を行う“オンライン診断サービス”を提供する。これは，インターネットシステムを構成する各種サーバ環境と広域ネットワークからLAN環境までの構築・運用をワンストップで行うMINDだからこそ提供できるサービスである。

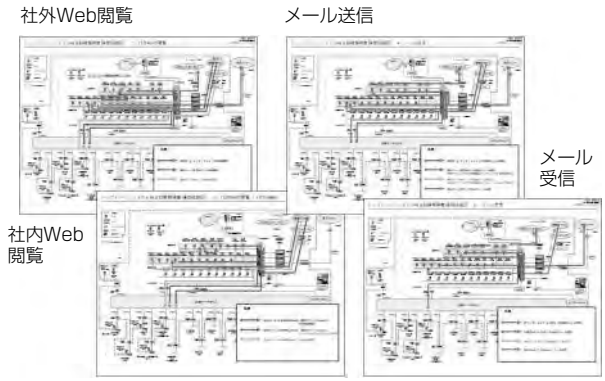


図3．通信経路図

ネットワーク全体構成図から利用プロトコルと全通信経路を洗い出す。洗い出した通信経路(**図3**)の正常性を確認するため，提供サービスとサーバ機能から試験手順を作成して一枚のシートにまとめたものが“総合試験要領書”である。試験手順は入力するコマンドと正常結果を具体的に記載するとともに，正常範囲の応答時間も明記して性能劣化の有無を確認する。

4.5 業界標準製品の採用

Internet-S³では，MINDの“キャリアニュートラル”“ベンダーニュートラル”の方針に則(のっと)り，業界標準の商用製品やオープンソーステクノロジーを採用する。実際に顧客企業のインターネットシステムを設計・構築する際には，MIND自身の導入・運用実績も加味して，顧客企業の要求を満たす製品やオープンソースを選定する。また，新製品や未経験の製品に関しては，ベンダーからの情報に加え，自社の検証環境で運用試験を行うことによって，顧客に提供しても問題がないことを確認する。

5. むすび

MINDでは，2000年から企業のインターネット利用環境の構築・運用サービスを行っており，製造業や官公庁を中心に100社以上への提供実績がある。

一方，昨今の仮想化やクラウド技術の進展には目覚ましいものがあり，企業の情報システム基盤への活用に大きな期待が寄せられている。MIND Internet-S³は，顧客企業の要求に合わせて構築・運用を行う現行サービスに加え，情報システム部門向けの業務アウトソーシングサービスとしての役割を維持しつつ，仮想化やクラウド技術を活用した低コストで流動性の高い標準サービスを展開し，企業のビジネス基盤として安全・安心なインターネット利用環境を提供し続けていく。

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管理サービス，三菱電機技報，**81**，No.7，481～484（2007）

特集論文

プラットフォーム統合ソリューション“VMINTEGRA 2.x”

萱野重実*
山田健策*

Platform Consolidation Solution "VMINTEGRA 2.x"

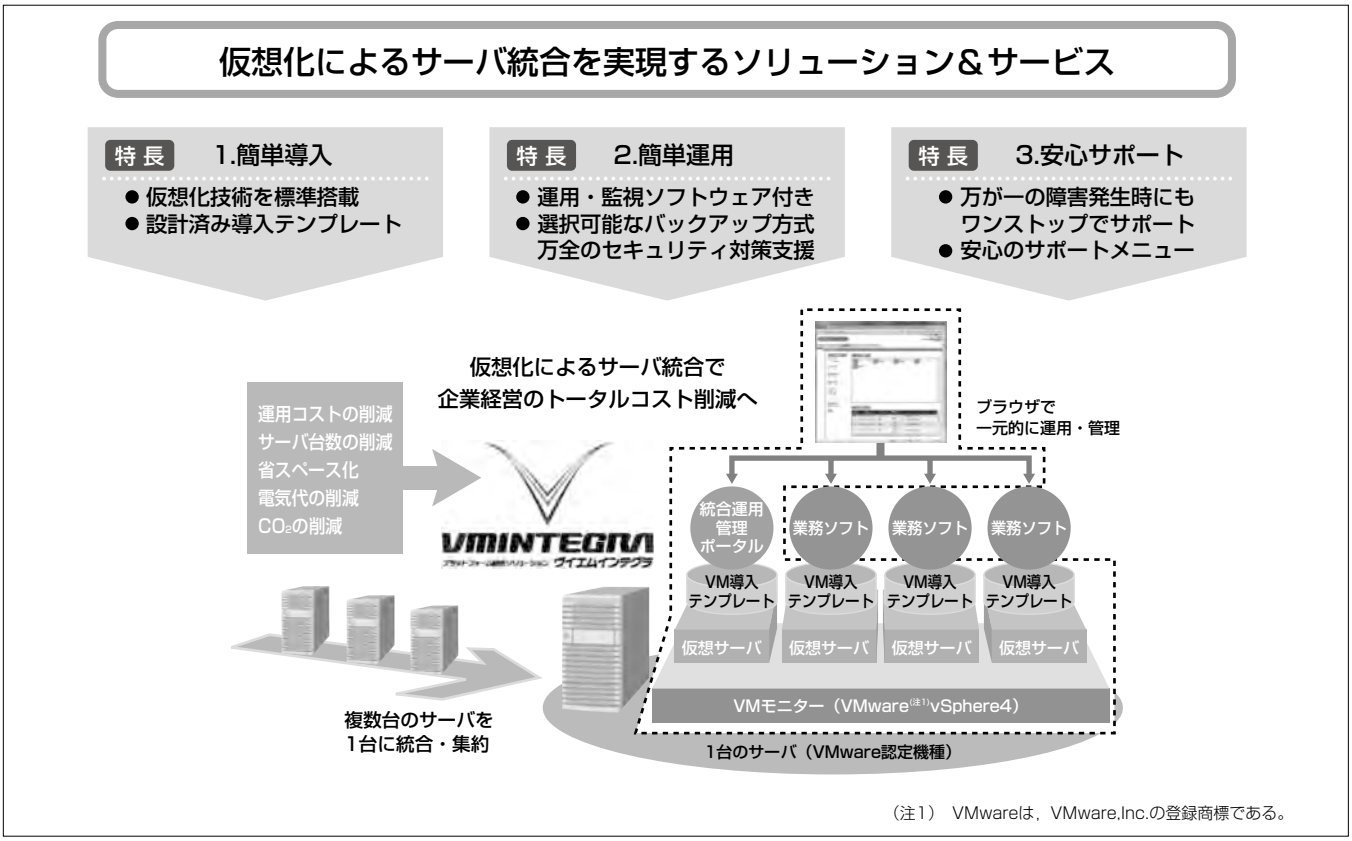
Shigemi Kayano, Kensaku Yamada

要　旨

昨今進んでいるプロセッサのマルチコア化を背景に，１台のハードウェア上に複数のOSを稼働させる仮想化技術が急速に進歩しており，この数年で大企業を中心に仮想化によるサーバ統合が進展してきた。仮想化によるサーバ統合は，サーバ台数の削減，運用コストの削減，セキュリティレベル向上，グリーンIT対応（電気代とCO_2の削減）など様々な利点がある。しかし，サーバ統合におけるリソース設計，パフォーマンス評価，仮想環境構築ノウハウを持つ技術者はまだ不足しており，そのために構築・運用コストは高く，仮想化による中小規模サーバ統合普及の阻害要因となっている。

三菱電機インフォメーションテクノロジー㈱（MDIT）は，これらの課題を解決するためプラットフォーム統合ソリューション“VMINTEGRA（ヴイエムインテグラ）”を開発し，2009年１月から出荷している。VMINTEGRAは，“簡単導入”“簡単運用”“安心サポート”の３つの特長の下，中堅・中小企業でも導入しやすいパッケージ製品をねらいとしている。

さらに，市場ニーズにこたえて，可用性向上及びハードウェアからアプリケーションまでを一括監視できる運用・監視機能などの強化を図ってきた。これによって，専任の情報システム運用者がいない，又は少ない中堅・中小企業におけるサーバ統合の促進を目指す。



（注1） VMwareは，VMware,Inc.の登録商標である。

中堅・中小企業でも簡単に導入・運用が行えるプラットフォーム統合ソリューション“VMINTEGRA”

運用コスト削減，サーバ台数削減，電気代の削減など様々な利点があるとされている“仮想化によるサーバ統合”をベースとした，簡単導入，簡単運用，安心サポートを特長とするソリューション製品である。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

1台のハードウェア上で複数の計算機システムを動作させる仮想化技術が進歩し，この数年で大規模なサーバ統合が伸展してきた。ハードウェア仮想化によるサーバ統合は，グリーンIT対策，運用コスト削減などのメリットがある。しかし，サーバ統合におけるリソース設計，パフォーマンス評価，仮想環境構築ノウハウを持つ技術者はまだ不足しており，そのために構築・運用コストは高く，仮想化による中小規模サーバ統合は普及していない。

2. VMINTEGRAとは

“VMINTEGRA”は，仮想化市場で高いシェアと実績のあるVMware社のVMware vSphere4に運用・監視機能をパッケージした製品で，情報システム担当者が少ない中堅・中小企業でも簡単に導入・運用を行えるプラットフォーム統合ソリューションである。MDITが2009年1月に製品化し，仮想化によるサーバ統合普及を推進している。

また，2009年10月に“VMware Japan Partner Award 2009”のSpecial Awardである“Packaged Solution”を受賞した。

2.1 VMINTEGRAの特長

システムライフサイクルは，企画・導入，構築，運用・管理フェーズに大別される。VMINTEGRAは，企画・導入と構築では“簡単導入”，運用・管理フェーズでは“簡単運用”“安心サポート”を特長としている。

2.1.1 簡単導入

著名なパッケージベンダーと共同で，VMINTEGRA上でのパッケージ稼働評価・リソース設計を行っている。そして，これらのリソース情報を基にしたパッケージ専用テンプレートや，よく使われる構成の汎用(はんよう)テンプレートを提供している。

小規模なサーバ台数であればVMINTEGRAヒアリングシートと呼ぶ現状調査シートを使って，大規模なサーバ台数であればサーバ負荷調査を実施するアセスメントサービスによって，必要なリソースを導き出す。このリソース情報を基に，最適なテンプレートを適用して容易に導入が行える。

2.1.2 簡単運用

仮想化されたシステムを簡単に運用・監視できるように，統合運用環境Centportalと監視マネージャーCentmonitorを提供している。統合運用環境Centportalは，情報システム管理者向けにも，業務を行う一般ユーザー向けにも，ログインユーザーごとに必要な機能を容易に設定できるブラウザベースの運用環境である。

2.1.3 安心サポート

メインフレームやオフィスサーバであれば，ハードウェアを提供するメーカーがハードウェア，OS，ミドルウェアまでトータルでサポートを行ってきた。しかし，パソコンサーバによるオープンシステムでは，ハードウェア，OS，ミドルウェアなどを提供するベンダーが異なるため，障害発生時の障害部位の切り分け及び問い合わせが複雑になっている。VMINTEGRAでは，ハードウェアから仮想環境，その上で動作する仮想サーバ，運用管理，セキュリティ，バックアップまで含めたプラットフォーム全体をトータルでサポートする。これによって，ユーザー及びシステムインテグレーターは安心してシステム構築，運用に専念できる。

3. VMINTEGRA2.x(注2)

VMINTEGRAは，初版出荷以来，市場ニーズにこたえシステム可用性向上及び運用・監視機能の強化を行ってきた。その強化ポイントについて述べる。

(注2) VMINTEGRA2.xとは，バージョン2から派生する各バージョンを示す。

3.1 高可用性モデル

仮想化によるサーバ統合では，1台のハードウェアに多くの仮想サーバが稼働するという構成上，トータルな故障率は下がる反面，そのハードウェアが故障すると搭載されているすべてのシステムが一斉に止まることになる。そのため，堅牢(けんろう)性が求められるシステムでは，可用性を向上できる構成が必要となる。

一般的に可用性を向上するためには，ハードウェアを複数配置し，1台が故障した場合に他のハードウェアで代替して稼働させることで実現する。VMINTEGRAでは，高可用性モデルとして次のような3方式を提供している。

3.1.1 ゼロスペア構成

ゼロスペア構成は，名称のとおり“待機サーバなし”という意味である。また，ゼロスペア構成では共有ストレージ“あり”と“なし”を選択できる。**図1**にゼロスペア構成を示す。

(1) 共有ストレージ“あり”

VMwareの仮想サーバはディスクファイルとなっている。A系，B系ともに，この仮想サーバを共有ストレージに置き，両方から仮想サーバが認識できる設定にしておく。A系で稼働させる仮想サーバは通常はA系で起動し，B系で稼働させる仮想サーバはB系で起動する。A系で障害が発生した場合には，B系上で本来のB系の仮想サーバに加えA系の仮想サーバも手動で起動させることで可用性を向上させる。

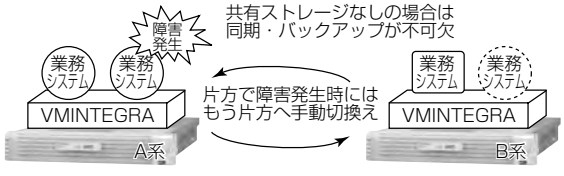


図1. ゼロスペア構成

⑵ 共有ストレージ“なし”

共有ストレージ“なし”では，業務システム全部の仮想サーバを，A系，B系のローカルディスクに配置する。共有ストレージ“あり”と異なり，業務システムが稼働すると仮想サーバの仮想ディスクのイメージが変更されるため，この情報を同期させる必要がある。同期の方法としては，仮想ディスクのイメージをバックアップしてもう片方にリストアする。

ゼロスペア構成は，一方に障害が発生した場合に，もう一方のサーバで業務システム全部を稼働させることから，片方のサーバ上ですべての業務システムが稼働できるようなリソース設計を行う。

3.1.2 N＋1冗長構成

N＋1冗長構成は，ゼロスペア構成と異なり，1つの待機サーバを配置する。**図2**にN＋1冗長構成を示す。

A系で障害が発生した場合には，待機系でA系の業務システムを稼働させる。これによって，ゼロスペアのように1台のサーバですべての業務システムが稼働できるようなリソース設計を行う必要はなく，A系，B系ともにリソースの限度まで業務システムを集約させることができる。この構成の特長は，障害が発生して縮退した際もパフォーマンスの低下がないことである。障害発生時の業務システムの切替えは，ゼロスペア構成と同様に手動で行う必要がある。

3.1.3 HA構成

HA(High Availability)構成(**図3**)は，共有ストレージ“あり”ゼロスペア構成とハードウェア配置は同じであるが，VMware vSphere4のHA機能を用い，サーバハードウェア同士がお互いの死活監視を定期的に行うことで，一方のサーバハードウェアに障害が発生した場合に，自動的にもう一方のサーバハードウェア上で業務システムを自動的に再起動する。サーバ管理者が不在であっても，最小限のダウンタイムで復旧が可能となる。

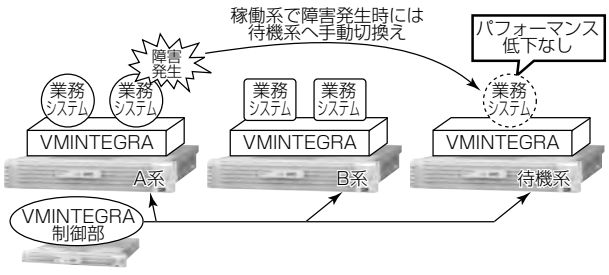


図2．N＋1冗長構成

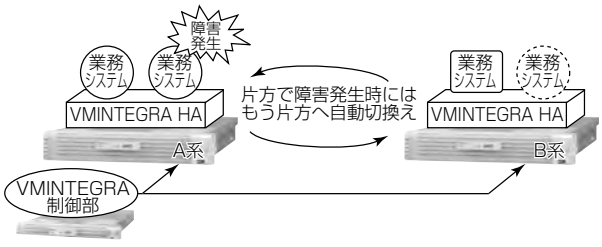


図3．HA構成

VMINTEGRAは導入ユーザーの可用性要求に応じて，片系がダウンしたときに手動で業務システムを再起動するタイプから，片系がダウンしたときに自動認識して自動で業務システムを再起動するタイプまで，運用方法，導入価格でモデルを選択できるようにしている。

3.2 運用・監視機能の強化

システムライフサイクルで一番長いのが運用フェーズである。仮想化によってサーバ台数を削減したのち，運用コストを削減するための機能が必要となる。VMINTEGRAでは顧客の要望にこたえて運用・管理機能の強化を行っている。

通常サーバはセキュリティ強化のため，施錠された無人のサーバ室で運用されることが多い。物理的に離れている場所から日々の運用・監視が行え，統一されたユーザーインタフェースで簡単に操作できるように，運用・監視機能を統合運用環境Centportalに集約した(**図4**)。

3.2.1 情報システム管理者向け

情報システム管理者に対しては，監視機能，VMモニタ機能，バックアップ機能，シャットダウン機能を提供する。

⑴ 監視機能

監視機能は，仮想化したサーバハードウェアの電源，温度，ファンなどの異常検出，VMware，仮想サーバの死活監視のほか，LAN(Local Area Network)上に接続されるIT機器の監視が可能である。

図5のように，監視対象のハードウェア，VMware，OSがアイコンとして表示され，それらが正常稼働している場合は緑色，軽度障害を起こしている場合はピンク色，停止している場合は赤色などのように色分けされるため，システム全体の稼働状況を一目で把握することが可能である。さらに，メールによる通報の仕組みも提供しており，管理者がシステムを常に監視していなくても，メール受信によって監視が可能である。

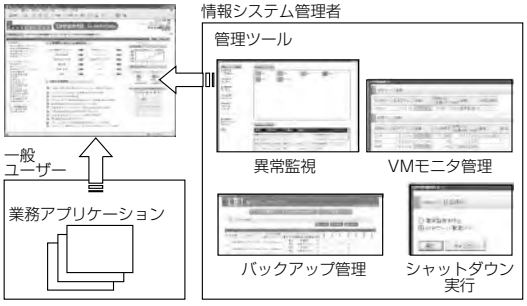


図4．統合運用環境Centportal

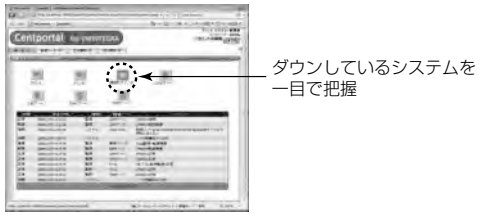


図5．Centmonitorによる監視画面

さらに，VMINTEGRA2.1ではデータベース及び業務アプリケーションの異常監視を可能とした。これによってハードウェアからミドルウェア，業務アプリケーションまで一括した監視が可能となり運用負荷軽減が図れる。**図6**にアプリケーション監視方式を示す。

監視対象マシンではアプリケーションがログを出力しており，そのログを監視しているログ監視エージェントがログを取り込み，必要な情報だけをフィルタリングし，監視マネージャーCentmonitorに送信する。

アプリケーションが生成するログとしては，ログファイルが1つである“逐次追加型”と，日付やサイズによってローテーションされる“ローテーション型”双方に対応可能とした。いずれの場合も前回からの差分を取り込む。

フィルタリング処理ではログ形式を項目の並びで定義し，取り込んだログデータ1行ごとに項目のデータ値を判定して選択処理する。この処理を定義するフィルタリング規則を外部ファイルとすることで，外部ファイル内の規則を修正するだけで様々なログ形式に柔軟に対応可能とした。

またCentmonitorへの送信処理は，業界標準インタフェースであるSNMPを採用することで拡張性に富む仕様とした。

このような方式で，簡単な設定だけで幅広いアプリケーション監視を可能とした。

(2) VMモニタ機能

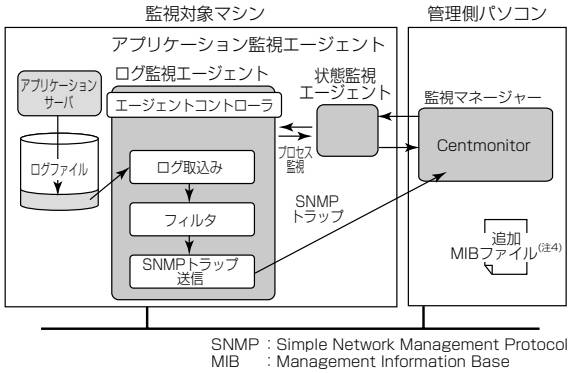
日々の運用では，変更しないCPU(Central Processing Unit)，メモリ，ディスクなどのリソース設定を誤操作させないように隠蔽(いんぺい)し，使う必要のある仮想サーバの電源オン／オフ，CD-ROMドライブの割付けなどを統合運用環境上に提供する。また仮想サーバごとに管理者が異なる場合，操作してはいけない仮想サーバを操作画面から隠蔽し，誤操作防止を実現した。

(3) バックアップ機能

VMwareの仮想サーバはディスクファイルとなっている。これを丸ごとバックアップするイメージバックアップと，従来どおりのOS内にあるファイルレベルのバックアップを行える機能をオプションとして提供する。このバックアップスケジュール操作，バックアップ成功・失敗の確認もCentportalから行える。

(4) シャットダウン機能

通常，VMware操作では，仮想サーバをシャットダウンし，VMware自体をシャットダウンし，サーバハードウェアの電源を切る操作を行う。VMINTEGRAでは，この一連の操作をCentportalからワンクリックで簡単に行える。さらに，VMINTEGRA2.1では，シャットダウンさせる仮想サーバの順番を設定することを可能とした。全仮想サーバのシャットダウン完了後，Active Directory(注3)サーバをシャットダウンさせるといった設定が可能である。また，この機能はUPS(Uninterruptible Power Supply)からのシャットダウン要求にも連携可能である。



(注4) MIBファイルとは，SNMPプロトコルで使うオブジェクトの構造体を記述したテキストファイルのこと。

図6．アプリケーション監視方式

3.2.2 一般ユーザー向け

一般ユーザー向けには，販売管理・生産管理といった業務系アプリケーションを，ブラウザインタフェースであってもクライアント・サーバ型インタフェースであっても，同じメニュー画面から起動させることを可能とした。

これらの運用・監視機能強化によって運用負荷の軽減が可能となる。

(注3) Active Directoryは，Microsoft Corp.の登録商標である。

4. むすび

最近，クラウドコンピューティングというキーワードが新聞・IT系雑誌・Web上に頻繁に出てきている。このクラウドコンピューティングには，CRM(Customer Relationship Management)，SFA(Sales Force Automation)，メール，オフィス系アプリケーションなどを提供するパブリッククラウドや，企業が自らの業務をサービスとして企業グループ内に提供するためのインフラを整備するプライベートクラウドなどがある。このクラウドコンピューティングのコンセプトは“手間いらずで，コンピュータ資源を必要なときにネットワーク経由で使用できるシステム形態”であり，まさにこれを実現する技術として仮想化技術が注目されている。しかし，単にサーバを仮想化しただけでは，クラウド(雲)上にあるシステムの運用・管理は困難である。VMINTEGRAが提供するブラウザベースの統合運用環境Centportalは，このプライベートクラウドの運用・監視を担うために，更に運用・監視機能の強化を図っていく。

参考文献

(1) 仮想化によるサーバ統合を実現するソリューション＆サービス“VMINTEGRA”，三菱電機技報，**84**，No.1，20（2010）

特集論文

企業環境の変化に対応するシステム間データ連携基盤

河井弘安*
三浦　隆*
草場信夫*

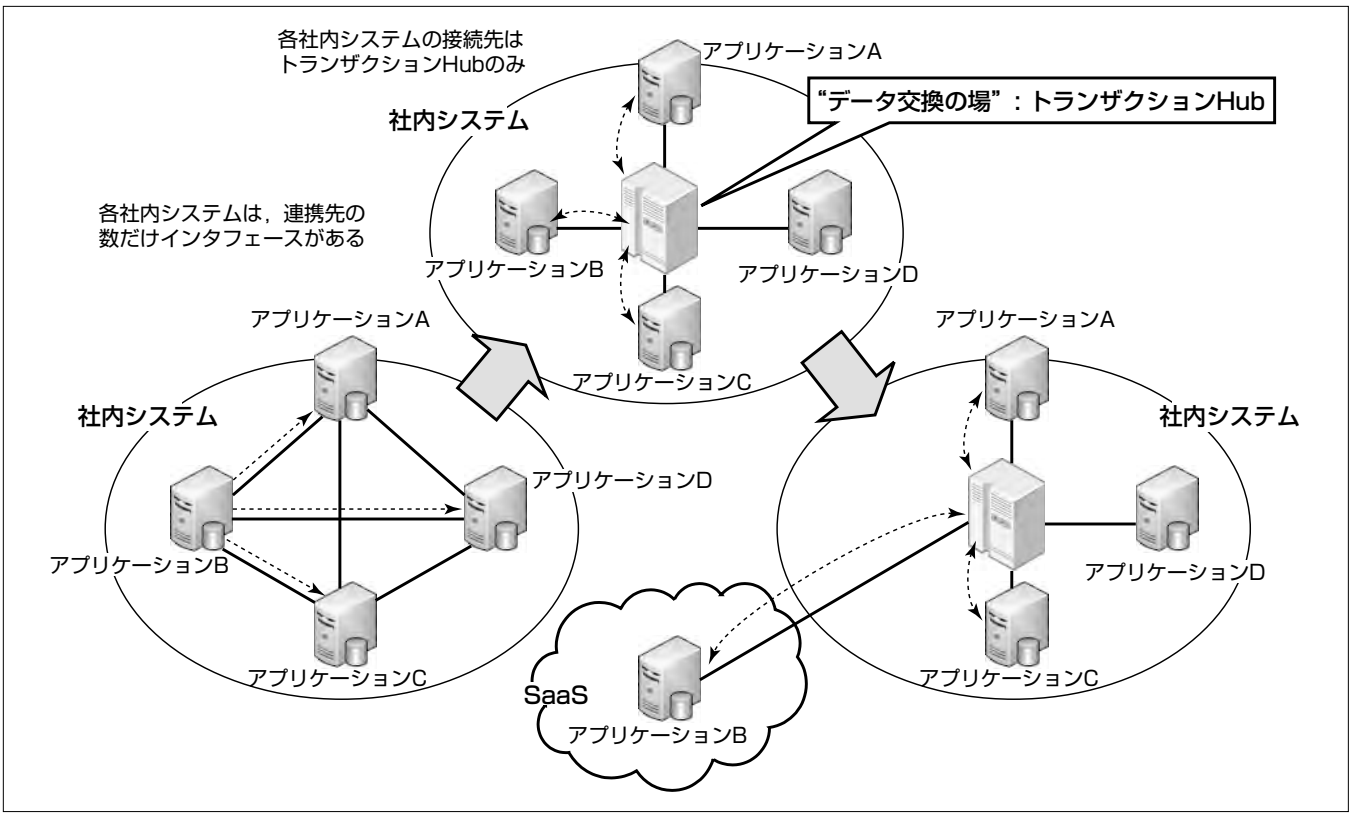
Infrastructure for Multi System Linkage in the Cloud Computing Era

Hiroyasu Kawai, Takashi Miura, Nobuo Kusaba

要　旨

近年，業務システムにクラウド，特にSaaS（Software as a Service）の利用が拡大している。SaaSの利用企業数を示す直接的な統計はないが，SaaSの市場規模が年率20%で拡大していることから(1)，間接的にユーザー企業のSaaS利用の拡大が進んでいることが分かる。しかし，社内システムのアプリケーションが相互に依存しているために，業務システム上のアプリケーションを単純にSaaS化すると，その連携が分断されてしまう。また，SaaS化するアプリケーションに連携するすべての業務アプリケーションを修正しなければならないなどの問題に直面する。

このような問題を解決するために，三菱電機インフォメーションテクノロジー㈱（MDIT）は，ETL（Extract Transform Load）ツールを活用して，クラウド技術の適用を支えるデータ連携基盤であるトランザクションHubをユーザー企業向けに構築した。トランザクションHubは，“もの”の移動をとらえるトランザクションデータを蓄積して，そのデータを再利用する業務アプリケーションとの間で交換する“データ交換の場”である。トランザクションHubを社内システムに導入することにより，業務アプリケーションはトランザクションHubを経由してデータを交換する。その結果，業務アプリケーションは連携先業務アプリケーションの影響を受けない独立した部品となる。このように，トランザクションHubにより相互依存性を排除された社内システムでは，レガシーシステムからオープン系システムへのダウンサイジング，システムの交換，新たなシステムの追加，SaaS化などを容易に実現できる。トランザクションHubを導入することにより，SaaSを含めた選択肢の中から，企業環境の変化に柔軟に対応できる最適な社内システムを構築できる。



データ連携基盤としてのトランザクションHubによるアプリケーション連携の変遷

MDITが構築したトランザクションHubを社内システムに導入することにより，業務アプリケーション相互の連携を疎結合にする。疎結合になることにより，業務アプリケーションは独立した部品となり，連携先のアプリケーションの変更や取替えによる影響を受けなくなる。このような社内システム連携を構築することで，業務アプリケーションのSaaS化を容易に行える。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

近年，業務システムにクラウド技術を利用する企業の数は増加傾向にある。クラウドには種々の定義があるが，本稿では，いわゆるSaaSを対象とする。

SaaSとは，業務を遂行するために外部企業が提供するソフトウェアのサービスを利用すること，業務そのものを外部企業に委託することを言う。サービス提供ベンダー数の増加やネットワーク環境の改善などによって，以前に比べてSaaSを容易に利用できるようになった。しかし，単純に業務システム上のアプリケーションをSaaS化すると様々な問題が発生する。その1つがデータ連携である。

本稿では，MDITがETLツールを活用して，データ連携基盤をユーザー企業向けに構築した事例について述べる。このデータ連携基盤は，社内システムにクラウド技術を適用する際に直面するデータ連携の問題を解決する。

2. 業務アプリケーションのSaaS化の進展と問題点

業務システムにクラウド，特にSaaSの利用が拡大している。SaaSの利用企業数を示す直接的な統計はないが，SaaSの市場規模は，年率20%で拡大している。これは，間接的にユーザー企業のSaaSの利用の拡大が進んでいることを示していると言える。また，ネットワーク帯域の拡大がこれを後押ししている。ここ数年で企業内ネットワークや社外ネットワークの回線の速度が飛躍的に向上した。従来は遠距離通信に専用線を使い帯域を確保していたが，現在ではインターネット網でも十分な通信速度が得られる。

ユーザー企業の情報システム部門によるコストメリット追求も，クラウド技術利用拡大に寄与していると言われている。自社にとって独自性の強いシステムか，より汎用(はんよう)的なシステムかといった視点でのシステムの選別が進み，企業の独自性が少ない業務アプリケーションは外部のサービスを利用するか，又は業務そのものを外部企業に委託する流れが加速している。

このようにクラウド技術利用の障壁はかなり低くなっているが，業務アプリケーションを単純にSaaS化すると大きな問題に直面する。

1つ目の問題点は，業務アプリケーション間の連携が分断されてしまう点である。今日の企業の業務は，1つの業務アプリケーションでは完結せずに複数のアプリケーションから構成される。例えば，**図1**に示すように3つのアプリケーションA，B及びCを利用して業務を行っている場合を考える。アプリケーション間の連携数は，連携先の数だけ存在する。この状態のままでアプリケーションCと同等の機能を持つアプリケーションDというサービスを利用すると，SaaS化前の社内システム(アプリケーションAとC，BとC)との連携が分断されてしまう。

2つ目の問題点は，業務アプリケーションが連携先のアプリケーションに依存しているために，連携先のアプリケーションがSaaSに変更された場合，連携元アプリケーションも修正しなければならないことである。連携先アプリケーションに依存するとは，連携元のアプリケーションが連携先の情報を保持し，それに基づいて処理していることを言う。具体的には相手先サーバのアドレスや，データレイアウトなどである。

図1の例では，アプリケーションAとBはSaaS化前のアプリケーションCに依存した設計となっているため，何らかの方法でSaaSベンダーが提供するアプリケーションDと連携するための修正が必要となってしまう。このことは，SaaS／ASP(Application Service Provider)利用実態調査の結果にも現れている[2]。SaaS採用前後で“一度採用すると他サービスに移行しにくい”という問題点が上位に挙げられている。これは，社内アプリケーションが，利用するSaaSに依存した連携を構築しているために，他のサービスへ移行すると，連携する社内アプリケーションを修正する多大なコストが必要になることを示していると言えよう。

3. データ連携基盤の構築

あるユーザー企業では，将来の社内システムのクラウド技術活用を想定して，業務アプリケーション間の“データ交換の場”の必要性を感じていた。そこで，ホスト上の販売物流システム，生産管理システム，原価計算システムをダウンサイジングするに当たり，MDITは業務アプリケーションの“データ交換の場”であるデータ連携基盤，トランザクションHubを構築した(**図2**)。このトランザクションHubで交換されるトランザクションデータとは，“もの”の移動をとらえるデータである。“もの”とは製商品や原材料といった物だけでなく，人の異動，金銭の移動も含み，企業内には伝票データや人事異動データなど様々なトラン

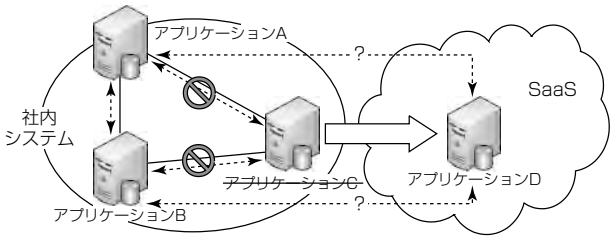


図1．業務アプリケーションのSaaS化の問題点

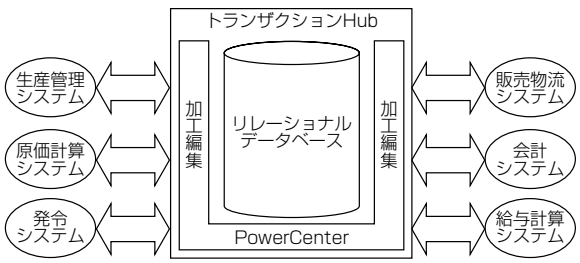


図2．データ連携基盤：トランザクションHub

ザクションデータが存在する。今回構築したトランザクションHubは，製商品や原材料の移動情報を蓄積する。

“データ交換の場”とは，1つのコンピュータ内での複数のプログラムのやり取りであればデータベースである。複数のプログラムは，データベースを介してデータをやり取りして相互の依存性を排除している。この考えを複数のコンピュータ上にある複数のアプリケーションがデータを交換する状況に応用して，“データを交換する場”がトランザクションHubである[3]。このデータのやり取りのために，トランザクションHubは，データを格納するサービス，及び取得するサービスを提供する。

3.1 トランザクションHubの特長

トランザクションHubは，社内システムに2つの疎結合を実現する。ここで言う“疎結合”とは，接続相手に依存しない連携のことを言う。具体的には，業務アプリケーション間の疎結合と業務アプリケーションとトランザクションHubとの間の疎結合である。

(1) 業務アプリケーション間の疎結合

業務アプリケーション間の疎結合は，業務アプリケーションが連携するときにトランザクションHubを介することで実現する。連携元のアプリケーションは，あらかじめ決められたフォーマットでトランザクションデータをトランザクションHubに格納する。格納されたトランザクションデータを再利用するアプリケーションは，必要なデータを必要なタイミングでトランザクションHubから取得する。データを格納，利用する業務アプリケーションはトランザクションHubのみと非同期で連携する。

格納するトランザクションデータは，可能な限り明細データとした。これは，トランザクションデータを再利用するアプリケーションの必要とするデータの粒度が各々異なるためである。例えば，原価計算システムでは月次で集計されたデータでよいが，在庫管理システムでは日々の製商品，原材料の動きをとらえる必要がある。

トランザクションデータを格納するとき，データはすべて挿入のみとする。トランザクションデータを再利用するアプリケーションは，損益計算システムなど会計系システムも含まれている。追跡可能性と検証性を高めるため，修正や訂正などは伝票処理と同様に赤黒修正を行う。

このように，あらかじめ決められたフォーマットの明細レベルのトランザクションデータを，業務アプリケーション間で非同期に共有することによって，データを格納する側はだれがいつデータを使用するかを意識する必要がなくなる。データを再利用する側も，だれがいつデータを格納したかに依存しない。

(2) 業務アプリケーションとHubとの疎結合

トランザクションHubは，業務アプリケーションとの疎結合を実現するために3階層アーキテクチャを採用した（**図3**）。データストア層，Hub層，インタフェース層である。データストア層にはリレーショナルデータベースを採用した。Hub層は，トランザクションHubの主機能の実装を行い，文字コード変換，データマッピング，データの粒度変換を行う。この機能の実現には，ETLツールであるPowerCenter(注1)を利用した。インタフェース層は，格納要求サービス，取得要求サービスのAPI（Application Program Interface）を提供する（**図4**）。このAPIは，業務アプリケーションからトランザクションHubとの連携の実装やHubそのものの実装を隠蔽（いんぺい）する。アプリケーションは，このAPIを通してトランザクションHubにデータの格納や取得を要求するので，トランザクションHubがどのようなシステムかといったことや，どのようにデータを連携しているかを意識しなくてよい。

3階層アーキテクチャは，トランザクションHubそのものの拡張性，保守性を向上させる。トランザクションHubの機能を階層化して階層間のデータの授受の方式を決めることで，それぞれの階層の実装方式を変更しても他の階層への影響を最小限に抑えることができる。例えば，インタフェース層をファイル交換によるバッチ処理で実現しているとき，将来の要求に対してデータベースとの直接連携やWebサービスなどのリアルタイム連携への変更が短期間で実現できる。業務アプリケーションからのトランザクションデータの粒度の変更要求に対しては，Hub層の修正のみで対応できる。このように3階層アーキテクチャを採用することによって，トランザクションHubへの変更要求に対して柔軟に対応できる高品質なシステムを提供した。

（注1） PowerCenterは，Informatica Corp.の登録商標である。

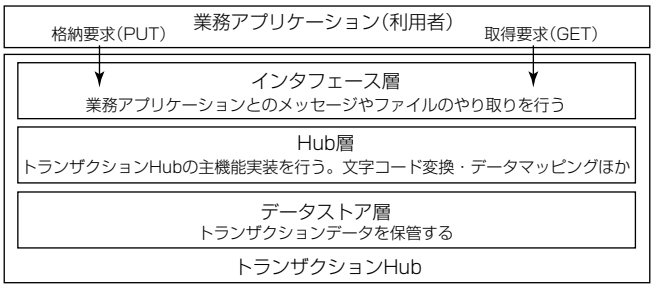


図3．トランザクションHubの3階層アーキテクチャ

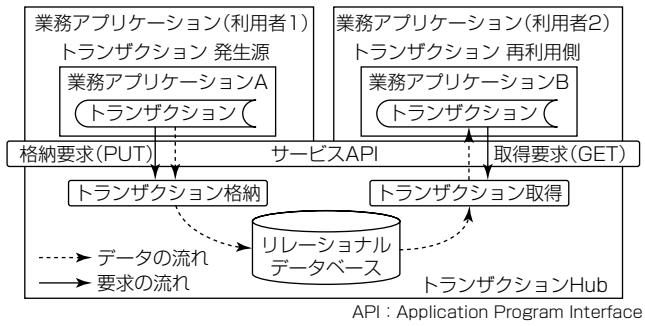


図4．サービスAPIによるトランザクションHubの隠蔽

3.2 サービス指向アーキテクチャとの違い

一般的にSOA(Service Oriented Architecture：サービス指向アーキテクチャ)やESB(Enterprise Service Bus)は次の特徴を備えていると言われている。

①標準化されたインタフェースで内部を隠蔽する
②個々のサービスは独立して稼働する
③サービスの実装方法や稼働しているプラットフォームを問わない
④実際にサービスがどこにあっても関係ない

トランザクションHubもこれらの特徴を持っているが，大きな違いは，連携するデータフォーマットを共通化した点にある。“もの”の移動情報であるトランザクションデータのレイアウトはどうあるべきかを突き詰め，汎化(はんか)を行い，フォーマットを決定した。汎化は，単に各業務アプリケーションが使用するフォーマットの最小公倍数を取るのではなく，トランザクションデータのモデル化から行った。具体的には，“もの”の移動を5W1Hでとらえる。何を，いつ，だれが，どこに，なぜ，どのように“もの”を移動したかを表現する。この汎化モデルは，移動を表現するFromとToの情報が含まれているため，UML(Unified Modeling Language)などを使用して表現すると，左右対称のきれいなクラス図となる。トランザクションデータの共通レイアウトを採用することで，業務アプリケーションはデータを再利用する他の業務アプリケーションに依存することなく，データをトランザクションHubに格納できる。

4. データ連携基盤の効果

将来のSaaS化を見据えた社内システムにおいて，業務アプリケーションの相互依存性をなくして，連携するデータのレイアウトを共通化するトランザクションHubの活用は大きな効果をもたらす。

(1) 業務アプリケーションの部品化による効果

業務アプリケーションが疎結合になることによって，業務アプリケーションは独立した部品となる。部品化することによって，その業務に最適な部品(アプリケーション)を利用することができる。パッケージソフトウェア，独自に開発したプログラムなど，適材適所に導入することを可能にする。

部品化した業務アプリケーションは，修正や入替えを行っても他の業務アプリケーションには影響しない。したがって，業務アプリケーションのSaaSへの移行も容易に行うことができる。**2章**で述べた，業務アプリケーション連携の分断や1つのアプリケーションの変更が連携先に波及するというような問題は発生しない。

その結果，社内システムをレガシーシステムからオープンシステムへ，オープンシステムからSaaSへと段階的に緩やかな移行を可能にする(**図5**)。業務アプリケーション

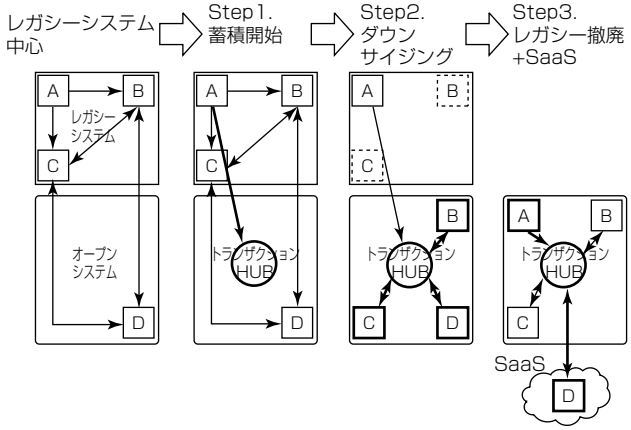


図5．レガシーシステムからSaaSへの段階的に緩やかな移行

を一気にSaaS化するのではなく，まずはトランザクションHubでデータを一元的に管理する基盤を構築する。次に，業務アプリケーションの連携をトランザクションHubを経由させる。業務アプリケーション間の依存関係を排除した上で，SaaS化するシステムを見極めて外出しにするというステップを踏むことが可能となる。

(2) PowerCenterの利用の効果

トランザクションHubにPowerCenterを活用することによって，データの流れを可視化できる。Metadata Manager(注2)によるメタデータ管理機能を利用してメタデータを横断的に収集分析し，データの出自や変換ロジックを把握してトランザクションHubの信頼性の向上を図ることができる[4]。

(注2) Metadata Managerは，Informatica Corp. の登録商標である。

5. むすび

MDITは，企業環境の変化に対応するシステム間データ連携基盤であるトランザクションHubを構築した。トランザクションHubは，業務アプリケーション間を疎結合にして部品化する。業務アプリケーションの部品化は，企業内業務アプリケーションを緩やかに段階的にSaaS化するというシナリオを可能にする。その結果，SaaSを含めた選択肢の中から，企業環境の変化に柔軟に対応できる最適な社内システムを構築できる。

参考文献

(1) 国内SaaS／XaaS市場 2008年の分析と2009年～2013年の予測アップデート，IDC Japan（2009）
(2) SaaS／ASP利用実態調査2009－2010，日経マーケット・アクセス，日経BPコンサルティング調査部（2009）
(3) 椿正明：名人椿正明が教えるデータモデリングの“技”，翔泳社（2005）
(4) 高山茂伸，ほか：メタデータ管理で拡がるデータ統合ソリューション，三菱電機技報，**81**，No.7，477～480（2007）

特集論文

グリーンITサービス“Green by Cloud”

村田謙一* 冨永博史***
平井規郎** 佐藤節雄†
高橋 洋***

Green IT Service "Green by Cloud"

Kenichi Murata, Norio Hirai, Hiroshi Takahashi, Hiroshi Tominaga, Setsuo Sato

要 旨

法規制改正によって，温室効果ガス排出量規制管理対象が拡大され，温室効果ガス排出量の増加が著しいオフィスビルの省エネルギー活動の推進が不可欠となってきている。オフィスビルの省エネルギーの課題は，ビルオーナーとテナントが協働して省エネルギーを進める改善のPDCA（Plan Do Check Action）サイクルを回す仕組みがないことである。省エネルギーを推進する責任はビルオーナーにあるが，テナントがエネルギーを消費している。一方，テナントは省エネルギー推進に必要なエネルギー消費量等を把握できず，簡単に把握できる仕組みを求めている。

そこで三菱電機では，ビルオーナーとテナントをつなぎ，これらの課題を解決するサービスをクラウド技術の適用によって実現し，グリーンITサービス“Green by Cloud(注1)”としてデータセンターを活用して提供する。

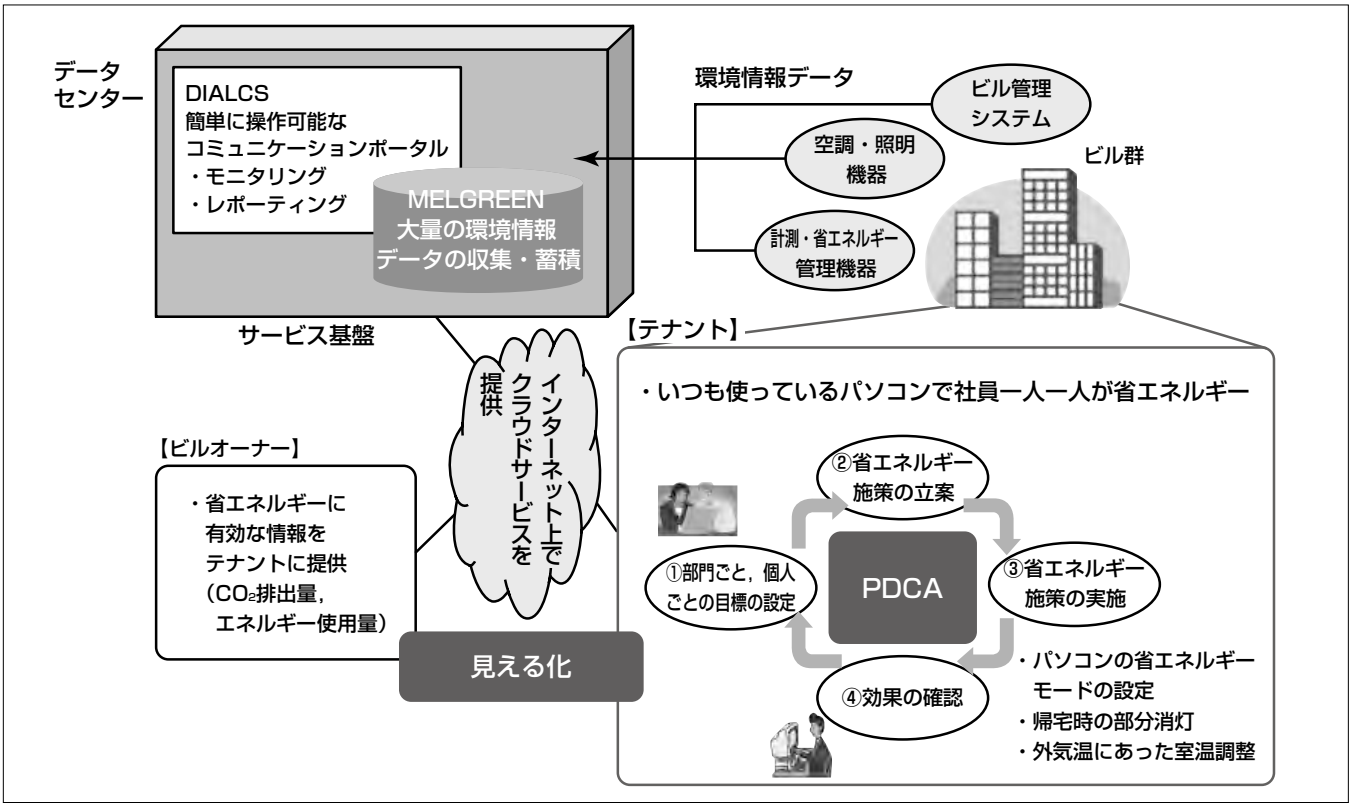
Green by Cloudは，①コミュニケーションポータル機能を提供するトータル環境経営ソリューションDIALCS（ダイアエルシーエス：LCS（Low Carbon Society）），②多拠点で大量(注2)に発生する環境情報データを一元管理し，高速に分析する環境経営推進ソリューションMELGREEN，③クラウド技術を適用した環境を備えたデータセンターの3つから構成される。

実際にオフィスビルの一部エリアに適用し，消費電力量の計測や対策を実施した結果，4.0%の削減効果を確認できた。このサービスによって法規制に対応できるばかりでなく，ビルオーナーはビルの付加価値向上，テナントは企業価値の向上というメリットも得られる。

今後，三菱電機はこのサービスをワンストップで提供し，顧客のグリーン化への取組みをサポートするとともに，企業全体のグリーン化を支援するサービスを目指していく。

（注1） Green by Cloudは，三菱電機㈱が商標登録出願中である。

（注2） 約6億件：ビル10棟で計測ポイント10,000点を1時間間隔で7年間採取した場合のデータ件数



三菱電機のグリーンITサービス

三菱電機は，環境情報データをビルの設備・機器からデータセンターに構築したサービス基盤であるMELGREEN，DIALCSに取り込み，建物を丸ごと省エネルギー化するサービスをグリーンITサービス“Green by Cloud”として提供する。

*三菱電機㈱ 本社 **同社 情報技術総合研究所 ***三菱電機インフォメーションシステムズ㈱ †三菱電機インフォメーションテクノロジー㈱

1. まえがき

本稿では，クラウド技術を用いて省エネルギー化のための各種機能を提供するグリーンITサービス“Green by Cloud”について，そのサービス基盤である“トータル環境経営ソリューションDIALCS”“環境経営推進ソリューションMELGREEN”及びデータセンターの特長や実現方法について述べる。また，実際のオフィスビルで実証実験を行った適用事例についても述べる。

2. Green by Cloud

2.1 背　景

基準年1990年に対する2008年度の国内温室効果ガス排出量を部門別に見ると，産業分野，交通分野に比較して，家庭部門，業務部門（＋41.3%）の増加が顕著である。業務部門の代表的なものとしてオフィスビルが挙げられ，その省エネルギーの推進が不可欠となってきている（**図1**）。オフィスビルにおける省エネルギーの課題は，ビルオーナーとテナントが協働して省エネルギーを進める改善のPDCAサイクルを回す仕組みがないことである。省エネルギーを推進する責任はビルオーナーにあるが，実際にエネルギーを消費するのはテナントという関係にある。ビルオーナーにとって，オフィスビル貸借契約は流動性が大きく，また多拠点のビルを管理するため，環境情報データ量の増減に柔軟に対応できる仕組みが必要である。一方，テナントも同じく貸借契約は流動性が大きいという課題を持っており，エネルギー消費量等を把握するため，導入期間が不要かつ従業員教育が不要で，必要な期間だけアクセスが可能な仕組みを求めている。

2.2 Green by Cloudとは

2.1節の背景から三菱電機では，ビルオーナーとテナントをつなぎ，これらの課題を解決するサービスをクラウド技術の適用によって実現し，グリーンITサービス[1] Green by Cloudとしてデータセンターを活用して提供する。Green by Cloudは，**図2**に示すように，ビルや工場内の“設備のデータ”“人のデータ”“ITのデータ”をきめ細かい単位で収集し，一元管理・分析・見える化等を行うことによって，建物を丸ごと省エネルギー化する新しいサービスである。

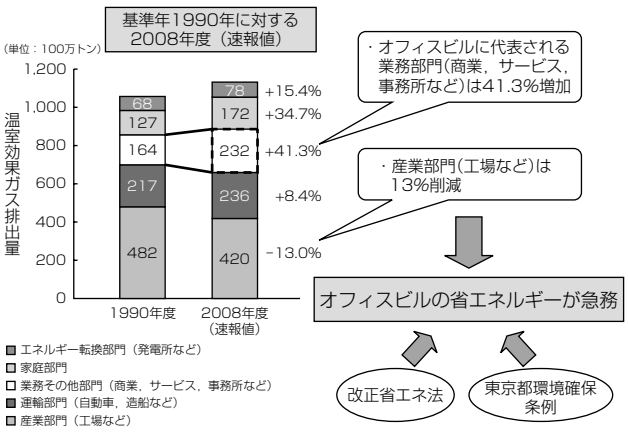


図1．日本における温室効果ガス排出量（部門別）[2]

3. Green by Cloudのサービス基盤

Green by Cloudは，トータル環境経営ソリューションDIALCS，環境経営推進ソリューションMELGREEN及びクラウド技術を適用した環境を備えたデータセンターの3つのサービス基盤から構成される（**図3**）。オフィスビルから収集した環境情報データをDIALCSやMELGREENに取り込み，各種の分析を行い“見える化”した上で，インターネットを介してテナントに情報を提供する。

3.1 DIALCS

DIALCSは，三菱電機インフォメーションシステムズ㈱（MDIS）が，2003年度から展開しているビルテナントサービスをベースに開発した新しい環境経営ソリューションである。

一般的なエネルギー管理においては，一連のPDCAサイクルを適切に運用することによって，事業者が目標を達成する仕組みを持つことと，継続的に改善が可能であることを内外に示すことが重要である。

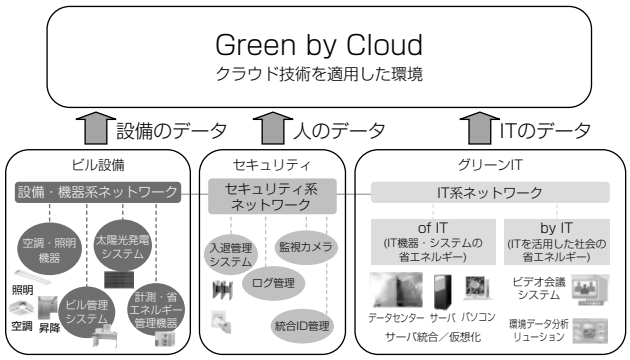


図2．Green by Cloud

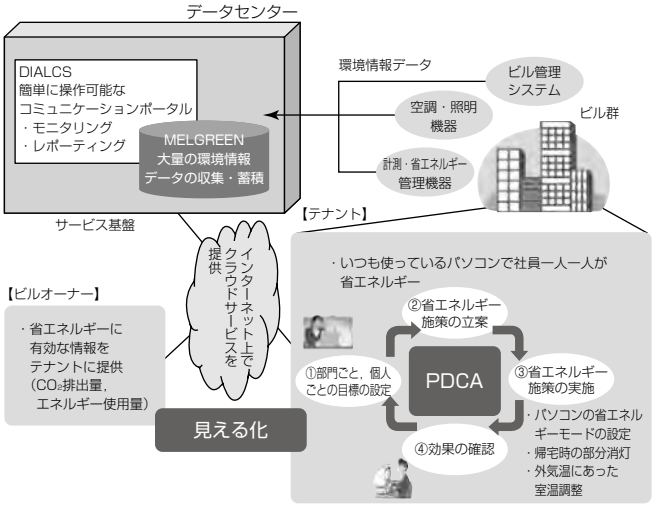


図3．Green by Cloudサービス基盤とサービス

今回の省エネ法改正では，規制対象範囲が改定前の事業所単位から事業者単位に拡大されている。今回の改正で新たに管理対象になった事業者は，今まで専任のエネルギー管理者を配備してないため，環境経営のPDCAサイクルの運営ノウハウ・運営体制に課題を抱えている。

DIALCSは，事業者による環境経営のPDCAサイクルの運用を支援するツールであり，利用者に対して啓蒙（けいもう）を図ることで省エネルギー活動を促進していく。さらに，あとで述べるMELGREENの分析機能と組み合わせることで，事業者の省エネルギーの改善対策の立案を支援することも可能である。

オフィスビルに特化しない汎用（はんよう）的なデータベース構造を保持しており，小規模な拠点を多数保持する特定連鎖化事業者や，公共団体などへも適用可能となる。

DIALCSの機能は次のとおりである（**図 4**）。

⑴　環境情報データの収集機能

収集する計測機器において，協業関係にある㈱エイチ・エル・シー製の電力線通信（PLC）エネルギー収集装置との連携もサポートしている。実際の事業者は拠点ごとに様々なエネルギー計測装置を導入しており，今後もエネルギー収集機能のレパートリーを充実していく。

⑵　レポート出力機能

改正省エネ法などの環境法令で各事業者が報告を義務付けられる帳票[3][4][5][6]を，収集・蓄積した環境情報データから自動生成する。事業者の業務の省力化と報告内容の客観性確保を図る。

⑶　コミュニケーションポータル機能

事業者の各階層が必要とする環境情報データを一つの画面上に表現し，情報コックピットとして環境経営判断を支援するとともに，利用者に対しては省エネルギーのための啓蒙を促進する。

多くの事業者では，このような大量の環境情報データを社内の基幹ネットワークを経由して通信することは許可されないため，今後DIALCSでは，各拠点内はPLC通信，広域はPHS（Personal Handyphone System）などを経由して，サービス環境にあるDIALCSサーバに集約する機能の拡充を図っていく。このようにすることで，企業の基幹ネットワークと完全に独立した環境情報データ専用のネットワーク構築が可能となり，企業への展開が加速するものと考えている。

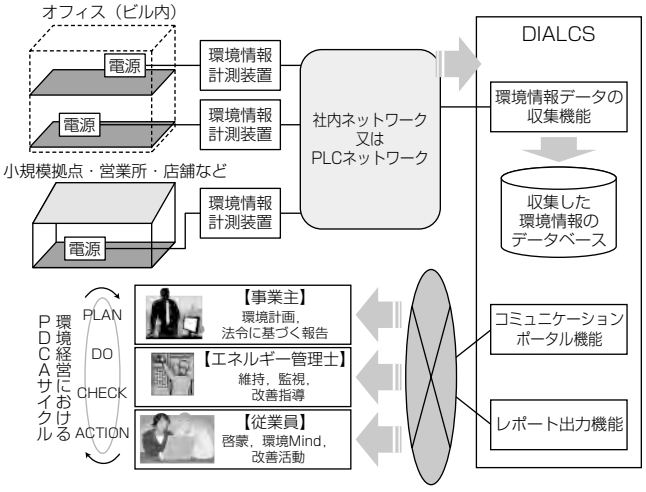


図 4．DIALCSの機能

3. 2　MELGREEN

MELGREENは，三菱電機インフォメーションテクノロジー㈱（MDIT）が展開する環境経営推進ソリューションであり，オフィスや工場，データセンターなど多拠点で発生する様々な環境情報データをインターネット経由で収集，一元管理し，企業の省エネルギーや温暖化対策などに必要となる情報をタイムリーに提供する。

MELGREENは，次の特長[7]を持つ。

⑴　環境情報コックピットは，大量データを分析した結果を見える化し，省エネルギーや温暖化対策立案の支援を行い，環境負荷低減とコスト削減を同時に実現する。

⑵　環境情報以外のデータ（セキュリティ，ビル管理，財務データなど）と環境情報データを統合分析し，人の動態と空調電力量との相関などのような高度な分析が行える。

⑶　膨大な環境情報データを長期間保管し，１億件３秒の高速集計，高速検索ができる。

⑷　テンプレートの活用によってシステム導入期間の短縮を実現する。

一方，クラウド技術を適用した環境で，一般のデータベースを用いて省エネルギーサービスを提供するには，次の課題があった。

⑴　多拠点に設置された大量のセンサから収集した環境情報データを１件ずつ追加するためロードに時間がかかる。

⑵　複数の利用者に対してサービスを提供する必要がある。

⑶　大量のデータを蓄積するためストレージが圧迫される。

MELGREEN の環境統合データベースでは，次の機能によってこれらの課題を解決した（**図 5**）。

⑴　多拠点で同時刻に計測されたデータの到着遅延を制御し，１レコードに結合してロードすることによって，セ

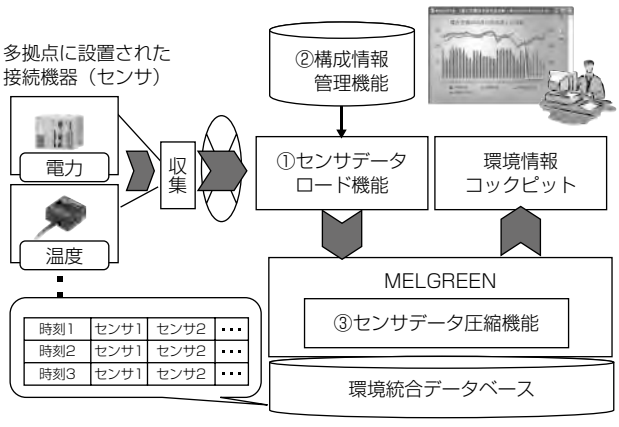


図 5．MELGREENの機能

ンサ数に依存することなくロード速度を高速化するセンサデータロード機能(**図5①**)

(2) センサと機器の階層関係を環境統合データベースと分離し，利用者ごとに管理する構成情報管理機能(**図5②**)

(3) 環境情報データに最適な圧縮モデルによって，少量単位でロードされる大量のデータを効率よく圧縮するセンサデータ圧縮機能(元データの1/5～1/50に圧縮)(**図5③**)

3.3 データセンター

三菱電機は，仮想化技術，セキュリティ技術をクラウド技術とともに活用し，Green by Cloudのサービス環境をデータセンターに構築する。サービスの提供方法としては，ビルオーナー等の事業者内に構築し提供する場合と三菱電機情報ネットワーク㈱(MIND)のデータセンターから提供する場合の選択が可能である。

4. Green by Cloudの適用事例

Green by Cloudの適用事例として，約1,400m^{2}のエリアに約220人が在席しているオフィスビルでの実証実験について述べる。対象エリアでは，テナントとして省エネルギー活動に取り組んでおり，従来は“どの機器に”“いつ”“どのぐらいの”電力が消費されているのか不明であった。今回，照明機器，コピー機，机上パソコン，給茶機など約60計測点に計測機器を設置し，5分ごとに消費電力量の計測とデータ収集を実施した。計測結果から電力量の構成比は，照明59%，パソコン16%，コピー機9%，その他16%の比率(空調機器は除く)となっており，まず割合の多い照明を中心にMELGREENによって分析を実施した。入退出システムから収集した在席者数の時刻による変化と合わせて分析することによって，在席者1名当たりの照明消費電力量の時刻による変化がわかった。早朝，及び19時以降が大きな値となっており，この時間帯に不必要な照明が点灯されている(**図6**)。また，退社時の照明装置の消費電力量は自動的に一括消灯される時刻20時，22時のうち，22時に大きく低下する(**図7**)。これは，退社時の部分消灯を実施していないことが原因と考えられる。この2つの分析結果から，退社時の不在エリア消灯の実施という運用ルールを在席者全員に通達することによって，照明の消費電力量(会議室の照明を除く)は1.9%低減された。

また，その他機器の分析を通じて最も無駄な電力は，利用者のいない夜間，休日のコピー機の待機状態での消費電力量であることがわかった。この問題点に対しては，平日の最終退場者，及び休日コピー機利用後の利用者による主電源OFFという運用ルールを在席者全員に通達することによって，コピー機の消費電力量は22%の削減効果が確認された。その他，パソコンに省エネルギーモードを設定する等の対策も合わせて実施した。その結果，対策前後のそれぞれ一週間の消費電力量を比較すると，エリア全体で4.0%の削減効果があった。

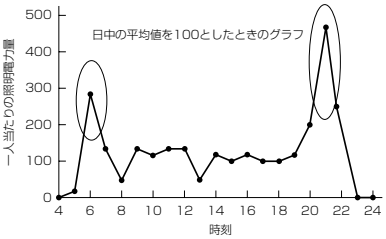


図6．在席者1人当たりの照明消費電力量の変化

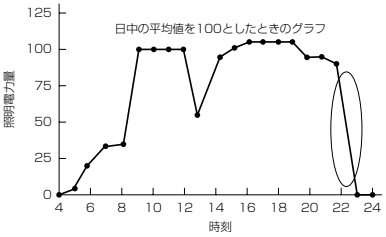


図7．1日の照明消費電力量の変化

5. むすび

Green by Cloudは，環境情報データをビルオーナーとテナントが共有することによって，改善のPDCAサイクルを回す仕組みを提供し，継続的なビルの省エネルギーの推進を支援するとともに，帳票出力等によって法規制対応を可能とする。加えて，ビルオーナーにとっては，ビルの付加価値向上，収益の拡大，テナント側にとっては，コスト削減，企業価値向上というメリットも得られる。今後，三菱電機はこのサービスをワンストップで提供し，顧客のグリーン化への取組みをサポートするとともに，企業全体のグリーン化を支援するサービスを目指していく。

参考文献

(1) 伏見信也，ほか：三菱電機グリーンITソリューション，三菱電機技報，**83**，No.7，408～412（2009）

(2) 環境省：2008年度(平成20年度)の温室効果ガス排出量(速報値)について

(3) 関東経済産業局：平成21年度改正省エネ法説明会 説明資料(実務編)

(4) 経済産業省：改正省エネ法(工場・事業場)説明資料(2009年7月)

(5) 経済産業省 資源エネルギー庁：エネルギーの使用の合理化に関する法律 第15条に基づく定期報告書 記入要領

(6) 経済産業省 資源エネルギー庁：改正省エネ法の概要2010

(7) 松井陽子，ほか：省エネルギーのPDCAの管理基盤 環境経営ソリューション“MELGREEN”，三菱電機技報，**83**，No.7，413～416（2009）

特集論文

ヘルスケアセキュリティSaaSへの取組み

茗原秀幸*
長浜隆次**
田口拓也***

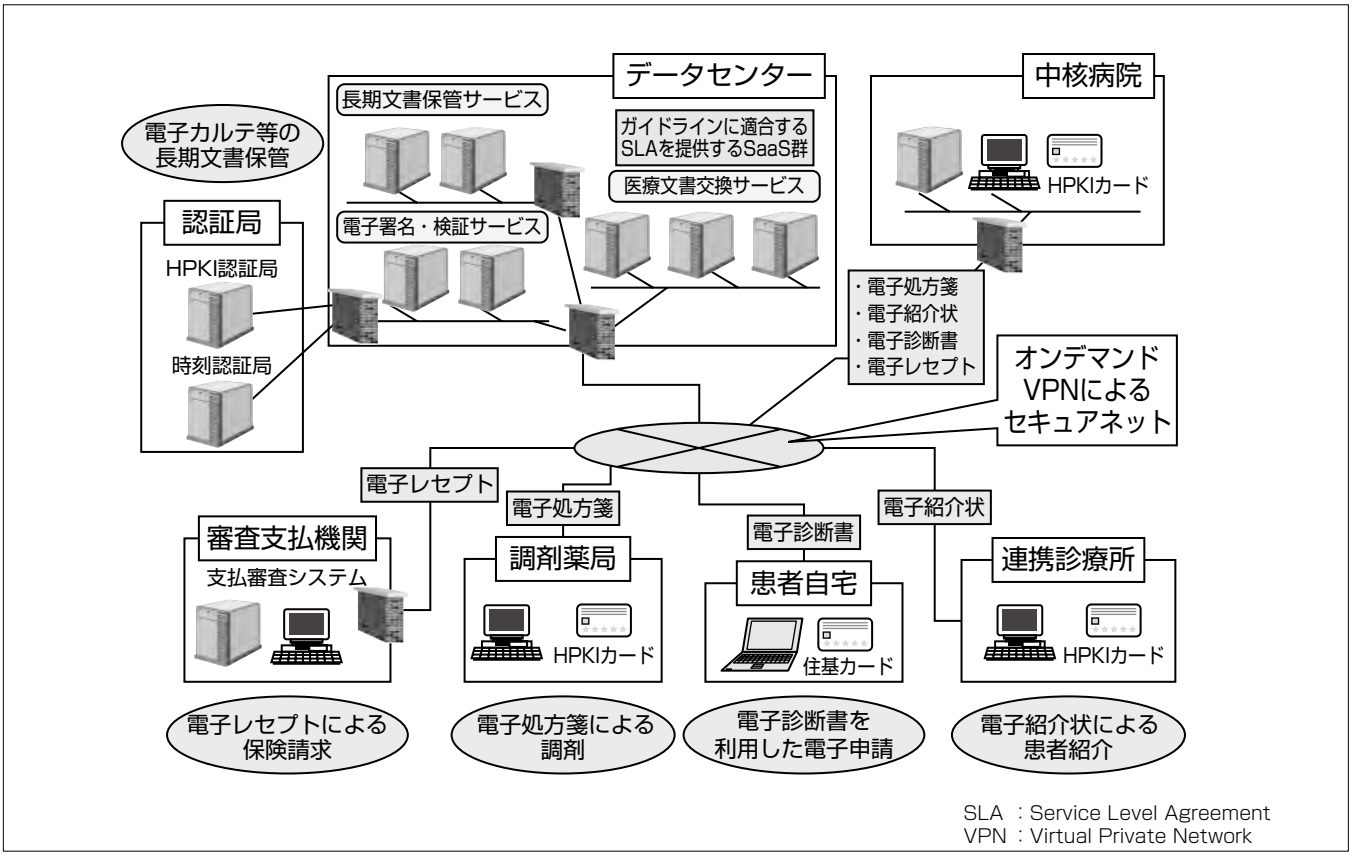
Our Activity on Healthcare Security SaaS

Hideyuki Miyohara, Ryuji Nagahama, Takuya Taguchi

要　旨

ヘルスケア分野では，機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。医療機関等が遵守すべきガイドラインとして，厚生労働省が医療情報システムの安全管理に関するガイドラインを制定し，その遵守を求めている。これに対応し，医療機関などへのサービス提供を行う事業者に対しても，経済産業省及び総務省のガイドラインが制定された。三菱電機グループでは，これらの要求事項を遵守できる低コストのハイレベルセキュリティサービスを医療機関などに提供することを目指して，ヘルスケアセキュリティSaaS(Software as a Service)システムの構築と評価を実施した。構築に当たっては，職能団体の要求事項をヒアリングし，小規模な医療機関などでも簡単に利用可能なサービスとしての要件を明確化した。また，クラウド技術を適用し，①ハイレベルセキュリティを確保したIaaS(Infrastructure as a Service)，②PKI(Public Key Infrastructure)認証による成りすまし防止やID管理を適切に行うPaaS(Platform as a Service)，③これらの基盤上で，医療分野向けのガイドラインに適合した電子署名，検証サービスを提供するSaaSを構築した。

このシステムでは，厚生労働省が推進する署名用HPKI(Healthcare PKI)証明書や認証用HPKI証明書も利用可能な設計となっており，保健医療福祉情報システム工業会(JAHIS)策定のガイドラインに準拠したHPKI電子署名，HPKI認証基盤を提供することができる。今後は自社サービスのみならず，他社の提供するSaaSに対するIaaS，PaaSの提供や，SaaS間連携を実施し，医療情報分野に対するハイレベルセキュリティサービスを提供していく。



ヘルスケアセキュリティSaaSの概念図

医療情報における安心・安全を確保しつつ，円滑な医療情報交換や保存が義務付けられた医療情報の外部保存を行える環境を提供する。真正性を担保するための電子署名・タイムスタンプ付与をSaaSサービスとして提供した上で，電子署名付き文書の文書交換や外部保存に対応したサービスと連携し，ワンストップで地域医療連携のニーズにこたえることができる。認証や署名のフレームワークでは，HPKI環境が利用可能である。また，将来は住民基本台帳カードに格納された公的個人認証基盤との連携も視野に入れている。

*三菱電機㈱ 本社　**三菱電機インフォメーションシステムズ㈱　***ジャパンネット㈱

1. まえがき

ヘルスケア分野では，機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。医療機関等が遵守すべきガイドラインとして，厚生労働省が医療情報システムの安全管理に関するガイドラインを制定し，その遵守を求めている。これに対応し，医療機関等へのサービス提供を行う事業者に対しても，経済産業省の“医療情報を受託管理する情報処理事業者向けガイドライン”，及び総務省の“ASP（Application Service Provider）・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン”が制定された。三菱電機グループでは，これらの要求事項を遵守できる低コストのハイレベルセキュリティサービスを医療機関等に提供すること目指して，ヘルスケアセキュリティSaaSシステムの構築と評価を実施した。

本稿では，ヘルスケア分野における要求事項とそれに対応したヘルスケアセキュリティSaaSの実装方式について述べる。

2. ヘルスケア分野の情報システムにおける要求機能

2.1 ガイドライン

厚生労働省の“医療情報システムの安全管理に関するガイドライン”（以下“ガイドライン”という。）では，インターネット経由での医療情報の送受信に対して，盗聴，セッション乗っ取りなどを防止する対策をとることが必要とされており，その中で次の例が明記されている。

①IPSec（Security Architecture for Internet Protocol）とIKE（Internet Key Exchange）の適用によるセキュアな通信路を確保すること

また，署名又は記名・押印が義務付けられた文書等で，記名・押印を電子署名に代える場合，次の②～④の条件を満たす電子署名を行う必要があると明記されている。

②厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

③電子署名を含む文書全体にタイムスタンプを付与すること

④上記タイムスタンプを付与する時点で有効な電子証明書を用いること

2.2 要求機能の整理

医療分野の情報システムにおける要求機能の検討に当たっては，**2.1節**のガイドラインをベースとし，職能団体の要求事項（次の(4)，(5)）も含め，次のように整理した。

(1) ガイドラインに準拠したセキュアなネットワーク上でのサービス（ガイドライン①に対応）

(2) 電子医療文書等への電子署名並びにタイムスタンプ付与サービス（ガイドライン②，③に対応）

(3) タイムスタンプ付き電子署名文書の検証サービス（ガイドライン④に対応）

(4) 医療機関（組織）並びに医療機関に所属する個人が識別可能な認証サービス

(5) 従量課金が可能な課金方式

3. SaaSサービスとしての要求機能

ヘルスケアセキュリティSaaSでは，小規模な医療機関等でも簡単に利用可能なサービスをねらいとし，ガイドラインに準拠したセキュアなネットワーク上で，高いセキュリティとアプリケーション基盤サービスを安価な料金で提供することを目標としている。

(1) ガイドラインに準拠したセキュアなネットワーク上でのサービス

ガイドラインで要求されるセキュリティ基準をクリアしているセキュアネットワークサービス（三菱電機情報ネットワーク㈱（MIND）が提供）をSaaSサービスのネットワーク基盤とし，セキュアネットワーク上にヘルスケアセキュリティSaaSポータルサイトを作成する。

(2) 電子医療文書等への電子署名並びにタイムスタンプ付与サービス

電子医療文書はPDFを想定し，PDF（Portable Document Format）への電子署名並びにタイムスタンプ付与サービスとし，電子署名機能及びタイムスタンプ付与機能を**表1**のように整理した。なお，性能については，クライアントレスポンスとして8秒以内とした。

(3) タイムスタンプ付き電子署名文書の検証サービス

タイムスタンプ付き電子署名PDFファイルをSaaSサービス上にアップロードして，電子署名並びにタイムスタン

表1．SaaSサービスとしての要求機能(1)

要求機能	内容
電子署名機能	・クライアントパソコン上のPDFファイルに対し，ICカード内の証明書（署名アルゴリズム：SHA1withRSA，鍵長：1,024ビット）を使用して電子署名（ES形式（CMS署名に証明書を特定する属性が付いたもの））が付与できること ・署名行為はクライアントパソコン上で実施し，PDFファイルへの署名付与はSaaSサービス側で実施できること ・クライアントパソコン上にはICカード及びブラウザのみ必要とし，PDFファイルは一度，SaaSサービス上にアップロードすることで署名を付与できること ・電子署名付きPDFはクライアント側にダウンロードされ，ダウンロード後はSaaSサービス上から削除すること
タイムスタンプ付与機能	・電子署名付きPDFへRFC3161に準拠したタイムスタンプ（署名アルゴリズム：SHA1withRSA，鍵長：2,048ビット）が付与できること ・PDFファイルは一度，SaaSサービス上にアップロードすることでタイムスタンプを付与できること ・タイムスタンプ付きPDFはクライアント側にダウンロードされ，ダウンロード後はSaaSサービス上から削除すること

CMS：Cryptgraphic Message Syntax　RSA：Rivest Shamir Adleman
ES：Electronic Signature　SHA：Set Hash Algorithm
RFC：Request for Comments

プを検証し，ブラウザ上に検証結果を表示し，アップロードされたPDFファイルは検証結果表示後，SaaSサービス上から削除する。

⑷ 医療機関(組織)並びに医療機関に所属する個人が識別可能な認証サービス

SaaSサービスのアクセス認証としては，SSL(Secure Socket Layer)クライアント認証又はID／Password認証とし，ユーザー管理機能及び認証／認可機能を**表2**のように整理した。

⑸ 従量課金が可能な課金方式の検討

課金方式については，従量制，固定性，不定期課金があり，SaaSサービスとして必要な課金方式を検討した。また，認証情報によって，医療機関(組織)と医療機関に所属する個人を特定し，だれが，いつ，何のサービスを使用したかを特定できるようにする必要がある。

4. ヘルスケアセキュリティSaaSの実装方式

先に述べたガイドラインに準拠したヘルスケアセキュリティSaaSを実現するために，**図1**に示すようなIaaS，PaaS，SaaSの概念定義を実施し，国内のデータセンターで提供されるIaaSを利用して，電子署名・電子署名検証サービス，PaaS上のSSO(Single Sign-On)，ユーザー管理，課金管理機能の開発を行った。

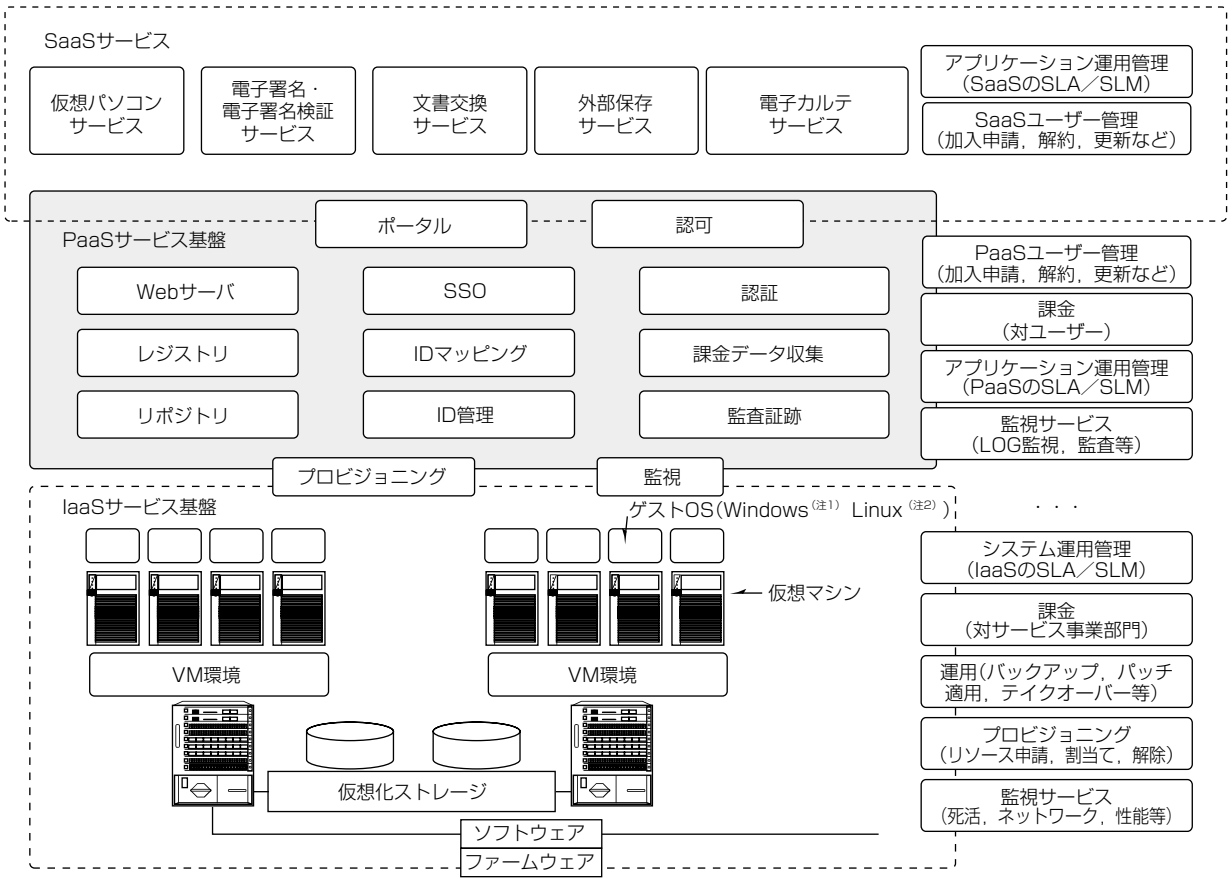
4.1 電子署名・電子署名検証サービス

“電子医療文書等への電子署名並びにタイムスタンプ付与サービス”及び“タイムスタンプ付き電子署名文書の検証サービス”のSaaS化を実現するため，PDFデータへの電子署名及び電子署名検証については，三菱電機インフォメーションシステムズ㈱(MDIS)製SignedPDFシリーズを利用

表2．SaaSサービスとしての要求機能(2)

要求機能	内容
ユーザー管理機能	・SaaSサービス加入者として，医療機関(組織)並びに医療機関に所属する個人を管理できること ・ユーザ管理機能としてGUIを用意し，SaaSサービス加入者情報(認証情報含む)の登録，変更，削除等をCSVファイルで実施できること ・GUIからはSaaSサービス加入者の検索や，認可／認証機能への認証データ反映を実施できること
認証／認可機能	・SSLクライアント認証に加え電子証明書のSubject属性を認証情報とし，認証情報による認証並びにSaaSサービス加入者を特定できること ・ID／Password認証ではID／Passwordを認証情報とし，認証情報による認証並びにSaaSサービス加入者を特定できること ・認証情報からヘルスケアセキュリティSaaSポータルサイトへの認可を実施し，認可されたサービスのみをポータルサイトに表示すること ・認可されて，ヘルスケアセキュリティSaaSポータルサイトに表示されたサービスは，再度認証することなく利用できること(SSO機能)

GUI ：Graphical User Interface
CSV ：Comma Separated Value



(注1) Windowsは，Microsoft Corp. の登録商標である。
(注2) Linuxは，Linus Torvalds氏の登録商標である。

SLA ：Service Level Agreement
SLM ：Service Level Management

図1．ヘルスケア分野向けサービスの概念図

した。ただし，既存製品ではガイドラインの要求事項であるタイムスタンプ機能は未実装なため，今回の，CAdES(Cryptographic Message Syntax Advanced Electric Signatures)対応のタイムスタンプ機能を新たに追加した。電子署名に使用する電子証明書は，厚生労働省が推進する署名用HPKI電子証明書を利用可能とした。また，署名検証サービスでは，クライアントへのCRL(失効リスト)のダウンロードを不要とし，将来のCRL肥大化に対応できる設計となっている。

4.2 ヘルスケアセキュリティ用PaaS

“医療機関(組織)並びに医療機関に所属する個人が識別可能な認証サービス”を実現するため，ユーザー管理機能及び従量課金機能を実装した上で，次の特長を持つヘルスケアセキュリティ用PaaSの開発を行った。

4.2.1 ICカードを用いたSSLクライアント認証

ガイドラインに準拠した電子証明書を利用可能としたSSL(Secure Socket Layer)クライアント認証を実装した。これによって，認証局で本人確認を行った電子証明書の保有者のみがSaaSを利用できることになる。IPSec＋IKEによるネットワークセキュリティの確保とあいまって，成りすましや不正アクセスを防止でき，ハイレベルなセキュリティを確保できる。このPaaSでは，厚生労働省が推進する認証用HPKI証明書も利用可能な設計となっており，保健医療福祉情報システム工業会(JAHIS)策定のガイドラインに準拠したHPKI認証基盤を提供することができる。

4.2.2 SSO

医療機関のデータ保管やデータ交換など，将来的に新たなSaaSサービスを提供することを前提として，医療機関での利便性を考慮し，**4.2.1項**で述べたSSLクライアント認証を行ったあとには，複数のSaaS間で再認証が不要なSSO機能を実現した。SSO機能のコアシステムには，オープンソースソフトウェア(OSS)を採用した。OpenSSOをベースに，リバースプロキシとSAML(Security Assertion Markup Language)2.0の両方をサポートする形で実現されており，SaaSサービスごとにいずれかの形態でSSO機能を利用できる。

システム構築に当たってはOSSを活用したため，導入及び維持管理費用が抑えられる。また，ユーザー管理機能によって，SaaS側で独自に割り振ったIDとPaaSのIDをマッピングし変換することが可能となり，異なるIDを持つSaaSサービス間のSSOも可能になっている。この際，各SaaSは他のSaaSのIDを知る必要がなく，PaaSのIDと連携することでSaaS間の独立性と機密性を担保している。また，課金管理機能とSaaSが連携することで，PaaS運営者が課金代行をすることが可能となり，利用サービスをまとめた一括請求なども利用可能となる(**図2**)。

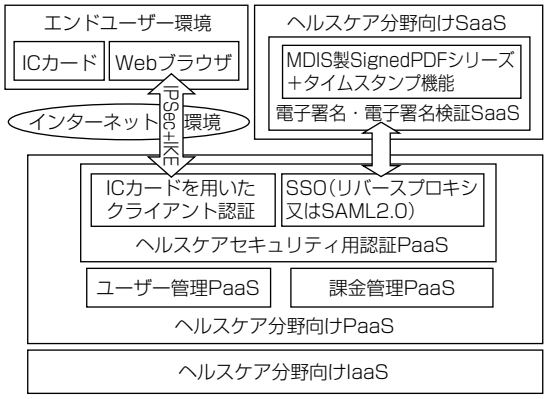


図2．ヘルスケア分野向けサービス構成

4.3 ヘルスケアセキュリティ用IaaS

医療情報を取り扱うこのサービスでは，データの保存場所は国内法の影響が及ぶ範囲であることが不可欠であるため，IaaSは国内に設置し，海外へのデータ流出がないことを担保する必要がある。また，可用性や信頼性の確保が大前提であるため，SaaS，PaaS事業者からのIaaSのSLA(Service Level Agreement)に対する要求レベルは非常に高いものになる。三菱電機グループでは，IaaS，PaaS，SaaSのトータルサービスを提供するため，ハイレベルセキュリティを担保するSLAに対応したIaaSを構築し，機微な情報を扱う分野にも適応できるようにした。仮想化技術を採用し，仮想化サーバ，仮想化ストレージ，仮想化ネットワークを提供するとともに，統合管制センターによる稼働監視，運用自動化が可能である。

5. むすび

今回の構築によって，医療分野の各種ガイドラインに準拠したSaaSサービスの提供に目処(めど)が立った。今後は署名対象ファイルの多様化(XML(eXtensible Markup Language)，ODF(Open Document Format)など)を行うとともに，外部保存サービス，電子カルテサービス，地域連携サービスなどSaaSサービスの多様化を図り，医療分野のユーザーニーズにこたえていく。また，自社サービスのみならず，他社の提供するSaaSに対するIaaS，PaaSの提供や，SaaS間連携を実施し，医療情報分野に対するハイレベルセキュリティサービスを提供していく。

参考文献

(1) 厚生労働省：医療情報システムの安全管理に関するガイドライン第4.1版（2010）
(2) 保健医療福祉情報システム工業会：JAHISヘルスケアPKIを利用した医療文書に対する電子署名規格（2008）
(3) 保健医療福祉情報システム工業会：HPKI対応 ICカードガイドライン第2版（2010）

特集論文

SaaS型セキュリティ診断サービス

今川大輔* 藤井誠司***
河内清人**
佐伯保晴***

SaaS Security Assessment Service

Daisuke Imagawa, Kiyoto Kawauchi, Yasuharu Saeki, Seiji Fujii

要 旨

企業活動にインターネットが不可欠である一方，不正アクセスによるセキュリティ事故が後を絶たない。その対策としてセキュリティ診断の必要性が叫ばれて久しいが，従来の診断は技術者が専用ツールを駆使する必要があり，広く利用されていないのが現状である。

この課題を解決するため三菱電機情報ネットワーク㈱(MIND)は，SaaS(Software as a Service)(注1)型セキュリティ診断サービスを開発した。このサービスでは，MINDの診断ノウハウを反映した診断ツールによる自動診断機能が提供される。ユーザーはポータルサイトを通じて簡単な設定を行うだけで，この機能をいつでも利用でき，“所有から利用へ”を実現したサービスとなっている。

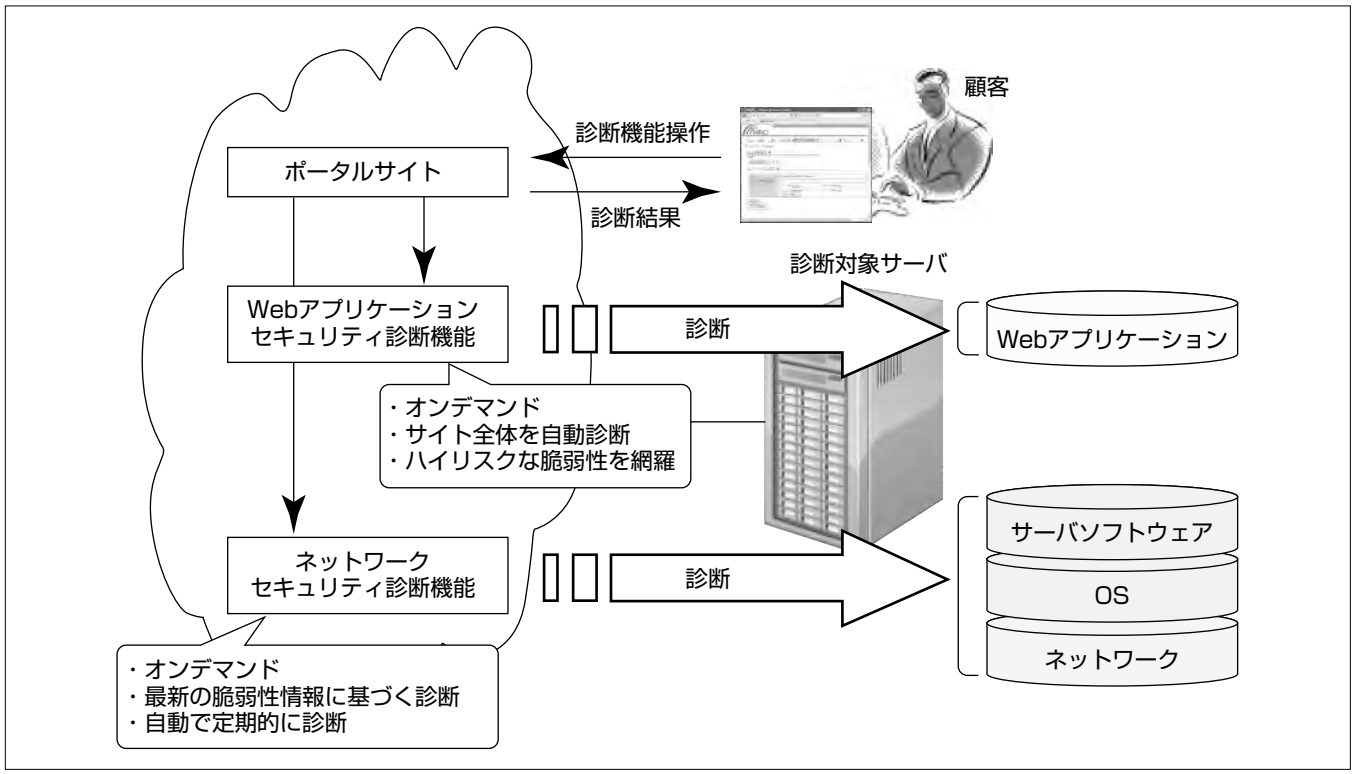
MINDは現在，SaaS型セキュリティ診断サービスとして，Webアプリケーションセキュリティ診断とネットワークセキュリティ診断を提供している。

SaaS型Webアプリケーションセキュリティ診断サービスは，①必要に応じユーザー自ら診断が可能，②診断開始ページの指定だけでサイト全体を診断，③再現診断機能によって脆弱(ぜいじゃく)性修正後の確認が容易，④従来は技術者が実施していた，OWASPが公開している高リスクな脆弱性を自動診断，という特長がある。

一方SaaS型ネットワークセキュリティ診断サービスは，サーバのOSやサーバソフトウェアに対する脆弱性診断を行う。SaaS型Webアプリケーションセキュリティ診断サービスと組み合わせることで，OSからWebアプリケーションまでサーバ全体に対する診断を提供可能である。

MINDは今後，SaaS型Webアプリケーションセキュリティ診断サービスの高精度化と，脆弱性管理機能の強化に取り組み，企業のセキュリティ事故防止に役立つサービスを提供する予定である。

(注1) ユーザーが必要とするソフトウェア機能をサービスとして提供する形態。



SaaS型セキュリティ診断サービスの概念図

MINDは，セキュリティ診断機能をサービスとして提供するSaaS型セキュリティ診断サービスを提供している。現在MINDでは，Webアプリケーションセキュリティ診断サービスとネットワークセキュリティ診断サービスをSaaS型サービスとして提供しており，ユーザーのサーバの脆弱性をOSからWebアプリケーションまで診断可能である。

*三菱電機情報ネットワーク㈱(理博) **三菱電機㈱ 情報技術総合研究所 ***三菱電機情報ネットワーク㈱

1. まえがき

サーバやWebアプリケーションへのセキュリティ対策の必要性が叫ばれて久しいが，不正アクセスによるセキュリティ事故は後を絶たない。さらに昨今は，情報漏えいやWebサイトの改ざんによるウイルス配布サイトへのリンク埋め込みなど，Webサイト管理者が加害者として責任を問われる場合も多く，そのため，自社のサーバやWebアプリケーションが最新の脆弱性に対し対策ができているかを確認するセキュリティ診断の必要性はますます高まりつつある。

しかし従来のセキュリティ診断は，専門的な技術を身につけた診断技術者による作業が必要であった。そのため，必要性は認識されつつも，セキュリティ診断の普及がなかなか進んでいないのが現状である。

そこで，MINDはセキュリティ事故の防止に貢献することを目指し，だれでも簡単に使える診断サービスとしてSaaS型セキュリティ診断サービスの開発に取り組んでいる。現在MINDでは，SaaS型Webアプリケーションセキュリティ診断サービスとSaaS型ネットワークセキュリティ診断サービスを提供している。

SaaS型セキュリティ診断サービスでは，だれでも使えるようにMINDの診断ノウハウが反映された診断ツールが自動診断を行う。ユーザーはポータルサイトを通じて，診断ツールに簡単な設定を行うだけで，必要なときにいつでも簡単に診断を行うことができる。

本稿では，これらMINDのSaaS型セキュリティ診断サービスと，それらを実現する技術について述べる。

2. SaaS型セキュリティ診断サービス

ここでは，現在MINDが提供しているSaaS型Webアプリケーションセキュリティ診断サービスとSaaS型ネットワークセキュリティ診断サービスについて述べる。

2.1 SaaS型Webアプリケーションセキュリティ診断サービス

このサービスは，インターネット上に公開されたユーザーのWebアプリケーションの脆弱性を自動診断するサービスである（**図1**）。このサービスは，SaaS型セキュリティ診断サービスの“ユーザーが必要なときにいつでも簡単に診断を行うことができる”という特長に加え，次の特長がある。

(1) サイト全体をスピーディに診断

サイト全体を巡回して各ページを自動で診断する。1ページ当たり約30秒で診断可能である。さらに，診断結果は利用者向けポータルサイト上で即時確認可能である。

(2) 検出された脆弱性への再現診断

診断で検出された脆弱性が正しく修正されたか，再度診断を行いたいというニーズは多い。そこで，過去に検出された脆弱性が，正しく修正されたかを容易に確認できる再現診断機能を提供している。

(3) 主要な脆弱性をカバー

他社に先駆け，Webアプリケーションが必ず対策すべき脆弱性として広く認知されているOWASP Top 10[(1)]脆弱性に対応した診断を実施可能である。

OWASP Top 10とはWebアプリケーションセキュリティ向上のために活動する非営利団体OWASPが公開している，Webアプリケーション上で知られるハイリスクな脆弱性の上位10項目である。OWASP Top 10はクレジットカード業界のセキュリティ対策基準であるPCI-DSS[(2)]でも，Webアプリケーションに対する診断項目として採用されており，対策が不可欠の脆弱性として世の中に広く認知されている。

表1にOWASP Top 10（2010年版）に記載されている脆弱性の一覧を示す。このサービスは，ストレージ暗号化に関する脆弱性（表中網掛け）を除き，全項目を診断する。

2.2 SaaS型ネットワークセキュリティ診断サービス

SaaS型ネットワークセキュリティ診断サービスは，ユーザーがインターネット上に公開しているサーバやネットワーク機器に対し，OSやサーバソフトウェアにおけるセキュリティ上の問題点を検査する。

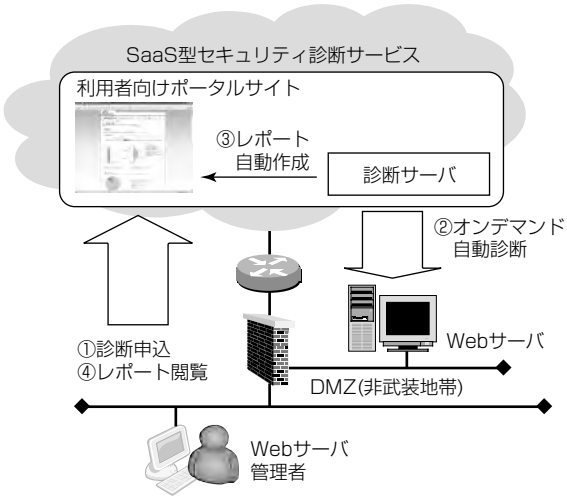


図1．SaaS型Webアプリケーションセキュリティ診断サービス

表1．OWASP Top 10の脆弱性

順位	脆弱性の名称
1	インジェクションの不具合（SQLインジェクション等）
2	クロスサイトスクリプティング
3	不完全な認証管理とセッション管理
4	安全でないオブジェクトの直接参照
5	クロスサイトリクエストフォージェリ
6	セキュリティ設定の不備
7	安全でない暗号化保存
8	URLアクセスの制限失敗
9	トランスポート層の不十分な保護
10	未チェックのリダイレクト・フォワード

URL：Uniform Resource Locator

この診断サービスは，日々発見される最新の脆弱性情報に基づき，一日一回など，高い頻度で繰り返しネットワーク診断を自動実施可能な点が特長である。

このサービスを利用することで，ユーザーは新たな脆弱性に対しても被害を受ける前に対処することが可能となる。

この診断サービスとSaaS型Webアプリケーションセキュリティ診断サービスによって，OSからWebアプリケーションまですべての階層をSaaS型でカバー可能である。

3. SaaS型セキュリティ診断を支える基盤技術

ここでは，MIND SaaS型セキュリティ診断サービスを実現する技術であるWebアプリケーションセキュリティ自動診断技術とMINDクラウド技術基盤について述べる。

3.1 Webアプリケーションセキュリティ自動診断技術

OWASP Top 10のうち，“不完全な認証管理とセッション管理”“クロスサイトリクエストフォージェリ”及び“URLアクセスの制限失敗”といった脆弱性は，MINDが他社SaaS型Webアプリケーション診断サービスに先駆けて自動診断を実現している。この診断を実現するために，MINDと三菱電機が共同で診断方式の開発を行った。

SaaS型Webアプリケーションセキュリティ診断サービスでは，実際の攻撃を模擬した診断用データをWebアプリケーションに入力し，それに対するWebアプリケーションの応答の中に脆弱性を示す特徴が現れているかを調べることで，脆弱性の有無を判定する。

脆弱性を診断するためには，擬似攻撃を実施した結果として，Webアプリケーション機能を不正に呼び出せたことを確認する必要がある。しかし，応答を分析し，擬似攻撃に成功したかを自動で判断することは従来困難であった。

この課題を解決するため，正当な権限のもとアクセスしたときに返されるページの内容と，擬似攻撃によって不正にアクセスしたときのページの内容とを比較し，同じ内容が返されていた場合に擬似攻撃に成功したと判定する方式を開発した。

しかし，単純なページ比較では，広告等，診断とは無関係にページ内容が変化する場合に判定誤りを起こす可能性がある。そこで，ページ間の類似度を定量評価する方式を開発し，類似度に基づいてページ内容が同一かどうかを判定することで，コンテンツの多少の変化に対して影響を受けないようにしている。

3.2 MINDクラウド技術基盤

このサービスを提供するため，診断サーバ，Webポータルサーバ，及び管理サーバで構成されている。各サーバは，**図2**に示すとおり，MIND iDC(internet Data Center)のクラウド技術基盤上の仮想マシンとして動作する。各仮想マシンには，SAN（Storage Area Network)で接続されたストレージが仮想ハードディスクとして割り当てられ，仮想L2スイッチを経由して，ファイアウォールなどの外部ネットワーク機器と接続されている。

クラウド技術基盤を利用することで，システムの構築に当たり，次の効果を得ることができた。

⑴ 短期間でシステム構築ができる

クラウド技術基盤では，ハイパーバイザーに要求するだけで，必要な性能を持った仮想マシンが生成される。ネットワークも既設ケーブルを仮想化して共有するため，物理的に新たなケーブルを配線する必要がない。そのため，ハードウェア調達や施設工事にかかる時間が不要となり，従来の約半分の期間(2か月)で必要なシステムを構築できた。

⑵ 顧客数の増加に対し，柔軟に対応できる

システムを仮想マシン上で構築することで，ハードウェアのリプレースなく，柔軟にサーバの処理性能を向上させていくことができる。そのため，サービス初期は少ないコンピュータ資源のみを使用するスモールスタートとし，顧客数の増加に応じて，段階的に使用するコンピュータ資源を増加させていくという運用を容易に行えるようになった。

4. SaaS型セキュリティ診断サービスの今後

最後に，MIND SaaS型セキュリティ診断サービスの今後の計画として，Webアプリケーションセキュリティ診断サービスの高精度化，及び脆弱性管理機能の強化について述べる。

4.1 SaaS型Webアプリケーションセキュリティ診断サービスの高精度化

SaaS型Webアプリケーションセキュリティ診断サービスが検出できる脆弱性の数は，Webアプリケーション内で診断ツールが巡回できる画面数と診断項目数に左右される。MINDは，より高い精度でWebアプリケーションの脆弱性を検出できるよう，①巡回できる画面数の増加，②診断項目数の拡充に取り組んでいく。

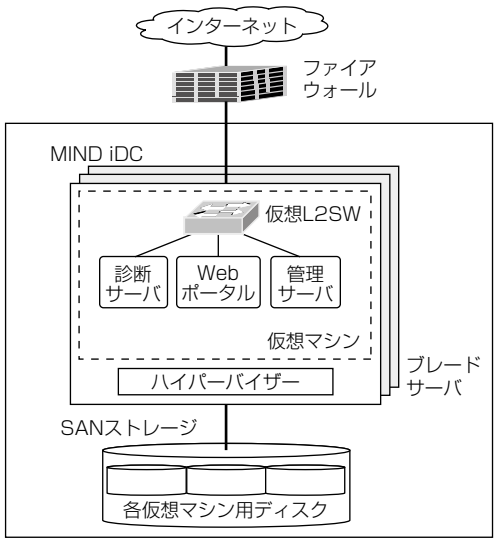


図2．MINDクラウド技術基盤

4.1.1 巡回できる画面数の増加

SaaS型Webアプリケーションセキュリティ診断サービスでは，診断対象サイトを自動巡回し，到達できた各ページを診断するため，到達できないページは診断対象から漏れてしまう。このようなページが発生する主な原因として，JavaScript(注2)によるページ移動が挙げられる。

JavaScriptによるページ移動は，ページ内のJavaScriptがブラウザを操作することで行われるページ移動を指す。このようなページ移動に対し，現在の診断システムでは，静的にJavaScriptを解析して移動先URLを推測するが，連結や置換等の文字列操作で生成されるURLまで認識することはできていない。

この課題を解決するため，今後は，従来の静的な解析に加え，動的な解析，すなわち，診断ツール内でJavaScriptを実際に動作させることで，移動先ページのURLを取得する方式についても検討を進めていく予定である。

自動巡回機能を継続的に改良する一方，ユーザーが必要に応じ，診断対象ページURLを追加できるよう，自動巡回できた範囲を簡単に確認できるようにする仕組みも必要である。例えば，巡回中にWebアプリケーションから返されたエラー画面などを自動認識し，エラーによって巡回が中断したページをユーザーに提示する機能などが有効と考えている。

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

4.1.2 診断項目数の一層の拡充

2.1節で述べたとおり，現在のSaaS型Webアプリケーションセキュリティ診断サービスでは，OWASP Top 10で示されるハイリスクなWebアプリケーションの脆弱性に対応した診断サービスを提供している。

より高いセキュリティを求めるユーザーに対応するため，今後も継続して診断項目の拡充に努めていく予定である。それと並行し，既存の診断項目に対しても，診断アルゴリズムの改良に取り組んでいく。

4.2 脆弱性管理機能の強化

現状のSaaS型セキュリティ診断サービスは，Webアプリケーションやサーバ機器の“現在”の脆弱性の状況を報告する。しかし，セキュリティレベルを維持し続けるためには，日々の運用にセキュリティ診断を組み込み，脆弱性を早期に発見して，被害が発生する前に必要な対策を完了させる必要がある。このように管理サイクルとして診断と対策を継続的に行う“脆弱性管理”の考え方が重要となる。

脆弱性管理業務の中では，SaaS型サービスを使ったセキュリティ診断は単なる1ステップにすぎない。例えば，診断実施後には，検出された脆弱性に対するリスク評価や取るべき対策(パッチ適用，アプリケーション修正等)の決定，及び対策の実施が必要である。さらに，スケジュールや作業要員の管理といった業務全体の管理も行わなければならない。

これら脆弱性管理業務は，管理サイクルを早めれば早めるほど，またユーザーのネットワークが大規模になればなるほどユーザーにかかる負担は増大していく。

SaaS型ネットワーク診断サービスでは，診断システムが，検出された脆弱性の修正状況の表示など，脆弱性管理の支援機能を一部提供している。今後はSaaS型Webアプリケーションセキュリティ診断でもこれらの機能を提供するとともに，両者を統合して管理できるようにしていく予定である。

5. むすび

昨今のセキュリティ診断のニーズの高まりを受け，だれでも容易に利用可能なセキュリティ診断としてMINDが開発したSaaS型セキュリティ診断サービスについて述べた。

SaaS型セキュリティ診断サービスでは，診断ツールの機能がサービスとしてユーザーに提供される。ユーザーは，Webポータルを通じて簡単な設定を行うだけで，必要なときにいつでも診断を実施可能である。

今後MINDは，SaaS型Webアプリケーションセキュリティ診断の高精度化に取り組むとともに，脆弱性管理機能の強化に取り組み，企業のセキュリティ事故防止に役立つサービスを提供する予定である。

参考文献

(1) OWASP：OWASP Top 10-2010
http://www.owasp.org/index.php/Category : OWASP_Top_Ten_Project
(2) PCI Security Standards Council：PCI DSS-PCI Security Standards Council,
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

特集論文

既存パッケージのSaaS化への取組み

野本泰宏*
服部佐次郎*

Approach of Existing Package on Making to Software as a Service

Yasuhiro Nomoto, Sajiro Hattori

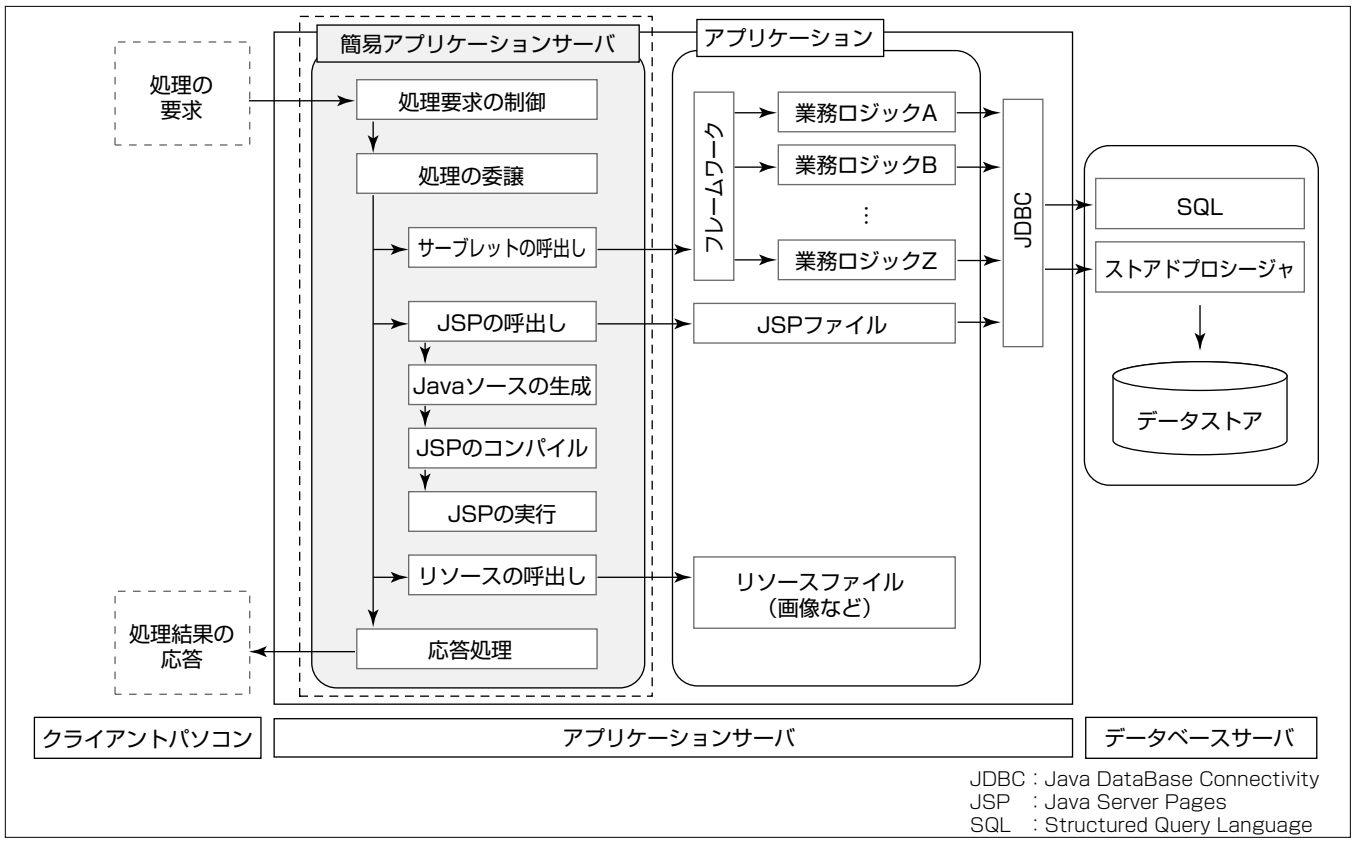
要　旨

近年，ハードウェアや仮想化技術などの進歩を受けて，SaaS(Software as a Service)，PaaS(Platform as a Service)，IaaS(Infrastructure as a Service)のような新しいコンピュータの利用形態が広がり始めており，インターネットを活用したITサービスが急速に拡大してきている。これらの新たな利用形態では，高いスケーラビリティを持つ仮想サーバ群を，“必要なときに”“必要なだけ”サービスとして利用できるところに特長があり，特にSaaSについては，アプリケーションの提供方法に大きな変革をもたらしつつある。

このような動向に対応するため，既存のアプリケーションパッケージをSaaS化するための検討を行い，小売店向け販売管理パッケージによる検証を実施した。このパッケージは，アプリケーションサーバ上で業務ロジックを実行する構造の業務アプリケーションパッケージである。インターネットを介して動作する既存のアプリケーションパッケージの大半はこれと同じ構造を持つが，IaaSなどの実行環境を提供するベンダーによってアプリケーションサーバの仕様が異なっており，SaaS化に向けた移植性が問題となっている。

今回，SaaS化を検討するに当たっては，移植性の問題への対処方法として，アプリケーションサーバ機能の共通化を図ることとし，この実現性を検証するために，IaaSベンダーが提供する仮想化環境上に検証用の“簡易アプリケーションサーバ”を構築して，動作確認を実施した。

その結果，この方式の有効性を確認することができ，同様の構造を持つ業務アプリケーションパッケージを汎用(はんよう)的なIaaS環境下で動作させるための方法を確立できた。



簡易アプリケーションサーバによるアプリケーションソフトの動作イメージ

アプリケーションパッケージの業務ロジックは，仮想化環境上に構築した検証用の“簡易アプリケーションサーバ”の下で，Webベース・アプリケーションとして動作する。
簡易アプリケーションサーバは，該当する業務アプリケーションを呼び出し，処理を実行後，処理結果をクライアントパソコンへ返却する。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

三菱電機㈱及び三菱電機インフォメーションシステムズ㈱(MDIS)では，様々な用途・業種に向けて業務アプリケーションパッケージを開発し，それを活用したビジネスを展開している。

本稿では，近年の技術動向及び市場動向を踏まえ，これらの業務アプリケーションパッケージをSaaS向けのシステムとして実現するための方式を，小売店向けの販売管理パッケージで検証した内容について述べる。

この方式は，仮想化された環境下に，業務アプリケーションパッケージに共通なアプリケーションサーバ機能を構築することで，既存のアプリケーションパッケージへの改修を最小に抑えるようにしているところに特長がある。この方式は，アプリケーションサーバ上で動作する多くの既存パッケージに適用できるものである。

今回，その実現性を検証するために，検証用の“簡易な”アプリケーションサーバ機能(以下“簡易アプリケーションサーバ”という。)を構築し，IaaSベンダーが提供する仮想化環境下での動作確認を行った。

2. SaaS化に向けた課題と指針

既存パッケージのSaaS化に当たっては，新しい実行環境への移植を可能な限り効率的に実現する必要がある。

このためには，移植対象となるパッケージ・アプリケーションへの改修を最小に抑え，現行のパッケージで実現している機能や操作性を損なうことなく実行できるようにすることが最も重要な課題となる。

インターネットを介して動作する既存の業務アプリケーションパッケージの大半は，アプリケーションサーバ上で業務ロジックを実行する構造となっており，SaaS化に際してもこの論理的構造を踏襲できる。しかしながら，アプリケーションサーバの仕様はベンダーごとに異なるほか，提供されるバージョンによっても異なり，その都度パッケージ側の改修が必要となる。

このため，個々の既存パッケージごとに，IaaSなどのベンダー環境に移植するための改修が必要となり，SaaS化するためだけに多くのコストと工期をかけることになる。

また，専用のネットワークで実行されていた業務アプリケーションをSaaS化する場合には，このほかにも①信頼性・可用性の確保，②セキュリティを中心としたデータベースの管理方法，③応答性能の確保などの技術課題のほか，④課金方法，⑤SLA(Service Level Agreement)など，多くの課題が存在するが，まずは，この移植効率の問題を解決する必要がある。

今回の検討では，この問題に対処するための方法として，アプリケーションサーバ機能の共通化と仮想化を採用し，次の点を検討指針とした。

(1) アプリケーションに手を加えない

今回検証した小売店向け販売管理システムなどの業務アプリケーションパッケージは，これまでの豊富な経験から，多くのノウハウと資産を継承している。

これらの資産を損なうことのないよう，アプリケーション(業務ロジック)には一切手を加えずに動作をさせる。

(2) 快適な操作性と応答性能の継承

中核となる基本入力機能は，応答性能及び操作性の良さを実現した既存パッケージと同等レベルに維持することが絶対条件となる。

(3) 信頼できるシステムの提供

インターネットを前提とした業務システムの特性上，セキュリティや可用性の問題が，関連する業務に甚大な支障を及ぼす可能性が高く，セキュアで高信頼なシステムであることが不可欠となる。

(4) アプリケーションとサーバの独立性の保持

アプリケーション又はアプリケーションサーバのいずれか一方に大幅な改修を実施したとしても，可能な限り他方は影響を受けないようにする。

(5) 他のアプリケーションパッケージへの適用

検証対象とした小売店向け販売管理パッケージだけではなく，将来的に他のアプリケーションへ適用することを見据えて，多種多様な環境での動作を目指す。

これらの点を踏まえて，その実現性を検証するための“簡易アプリケーションサーバ”を構築し，IaaSを提供するベンダーの仮想化環境下で動作検証を実施することとした。

3. 簡易アプリケーションサーバの構築

3.1 検証対象パッケージの基本アーキテクチャ

検証対象とした小売店向けの販売管理パッケージは，アプリケーションサーバにWebSphere(注1)(以下“WAS”という。)を使用することを前提としている。

WASは，JavaEE(Java Platform, Enterprise Edition)(注2)の仕様に準拠したアプリケーションサーバであるが，検証対象パッケージでは，業務ロジックを除き，ソースを自動生成するため，必要とするJavaEE API(Application Programming Interface)は極めて少ない。

3.2 簡易アプリケーションサーバの概要

実装は，今回の検証対象パッケージに必要な機能に限定した(**表1**)。サーブレットの実行など，必要最低限の機能は提供する一方，HTTPS(Hyper Text Transfer Protocol Security)，JSP(JavaServer Pages)(注3)タグへの対応など，不要な機能は一切実装していない。

(注1) WebSphereは，IBM Corp.の登録商標である。
(注2) Javaは，Sun Microsystems, Inc. の登録商標である。
(注3) JSPとJava Serverは，Sun Microsystems, Inc. の登録商標である。

3.3 簡易アプリケーションサーバのアーキテクチャ

簡易アプリケーションサーバ上でのアプリケーションソフトの動作イメージを**図1**に示す。

基本的な動作原理はJavaEEに準拠しており，クライアントアプリケーションからのリクエスト要求に応じたサーブレットを呼び出す。

サーブレット以降の処理は，パッケージ側のフレームワークが担当し，要求された業務ロジックを実行する。

処理結果は，JSPで生成したXML(eXtensible Markup Language)でクライアントアプリケーションに返送される。JSPの動作は，Javaソースを動的に生成し，コンパイルしたクラスファイルを実行することで実現した。

今回の検証対象パッケージでは，データの更新処理にEJB(Enterprise JavaBeans(注4))を採用しているが，このEJBは，検証対象パッケージ独自のフレームワークによって制御されている。このため，簡易アプリケーションサーバでは，EJBの実行に関する機能を実装していない。

これを補うため，EJBを制御しているフレームワークに対して，簡易アプリケーションサーバ上で実行する場合，EJBを通常のJavaBeansとして扱うようにフレームワークの改修を施した。

また，操作性を確保するため，1つのバッチファイルの起動，終了をするだけでサーバの起動，停止を実行できるようにし，バッチファイルを複数起動したり，コンソール管理画面からの操作などをしたりせずに済むようにした。

今回構築した簡易アプリケーションサーバでは，検証対象のパッケージに不要な処理はすべて実装を見送った結果，軽量・簡易な機能となり，仮想化環境にもかかわらず実用に足る応答性能を得ている。

なお，簡易アプリケーションサーバは100%Javaで記述されており，特定のOSやハードウェアに依存することなく多種多様な環境で稼働させることができる。

表1．簡易アプリケーションサーバのJavaEE対応状況

分類	機能	動作	備考
基本動作	アプリケーションの管理(EAR,WAR)	×	独自体系による，アプリケーションの配置と管理方式
	サーブレットの実行	○	URLに応じたサーブレットの実行が可能
	EJBの実行	×	実装せず。ただし，EJBを通常のJavaBeansとして扱うことで実行可能
	静的リソースの返却	○	画像ファイル，テキストファイルなどを返却可能。
	JSPの実行	△	ソース自動生成ツールで出力されたJSPのみ実行可能。JSPタグ，一部ディレクティブへは未対応
	マルチスレッド実行	○	指定スレッド数にて同時実行可能。指定スレッド以上のリクエストは，キューイング
	HTTPセッション管理	×	実装せず
	コネクション・プール	△	実装せず。ただし，オープンソースなどによって代替可能
管理	web.xml定義	△	アプリケーションサーバの定義ファイルに，サーブレットURLなどを定義
	Webアプリケーション再起動	×	Webアプリケーション単位での再起動は不可。サーバの再起動が必要

○：基本的な動作は可能
△：一部動作は未実装。又は，代替手段によって動作可能
×：未実装。動作せず
EAR：Enterprise ARchive
WAR：Web ARchive
URL：Uniform Resource Locator

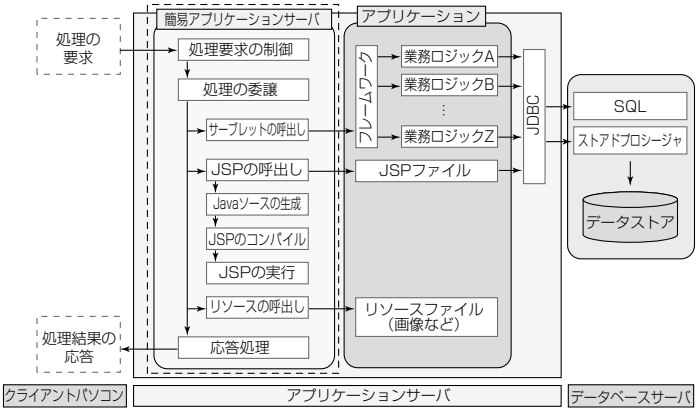


図1．アプリケーションソフトの動作イメージ

(注4) JavaBeansは，Sun Microsystems, Inc.の登録商標である。

4. 検　証

4.1 検証の方法

詳細な検証を行うためにVMware(注5)による仮想化環境を社内設備として構築し，開発した簡易アプリケーションサーバが，SaaS化に向けた指針を満たしているかどうかの検証を行った。

また，多種多様な環境での動作の検証を行うために，IaaSとして提供されている汎用的・一般的な商用プラットホームの下で検証を行うこととし，国内，海外を問わず幅広いベンダーからこれを選定して実施した。

(注5) VMwareは，VMware, Inc.の登録商標である。

4.2 検証の結果

(1) 仮想化環境での検証

検証用の仮想化環境では，簡易アプリケーションサーバ上で，対象アプリケーションが正常に動作することが確認できた。また，異なるバージョンのアプリケーション，並びにアプリケーションサーバを適用し，他方へ影響が発生せず，十分な独立性が確保できていることが検証できた。

操作性を確保するために必要な応答性能についても確認したが，従来のアプリケーションサーバ上での動作と比較すると，多少応答性能で劣ることが明確になった。これは，今回の製作で実装を見送った機能(コネクション・プール)の影響と考えられる。

(2) IaaS環境での検証

IaaS環境でも，簡易アプリケーションサーバ自体は問題なく動作した。ただし，帳票出力を行う場合，帳票サーバからプリンターへ印刷指示を行う方式については，方式の

変更が必要である。

現行の方式では，VPN(Virtual Private Network)等によって帳票サーバからプリンターを認識できる場合は印字可能であるが，パブリックなネットワークを介した場合，帳票サーバ側からプリンターが認識できないため，印字することができなくなるという問題がある。

4.3 検証課題への取組み

簡易アプリケーションサーバの動作検証に対しては，おおむね良好な結果が得られたが，一方で未実装の機能が原因で，期待した結果が得られなかった事項もある。

これらの事項への対処が今後の課題であり，仮想アプリケーションサーバとして実装が求められる次のような機能を中心に，この解決を図っていく。

(1) アプリケーションの管理／web.xml定義

アプリケーションサーバは，JavaEEに準拠した形式でアプリケーションの配置，管理を行っている。今回は，検証対象パッケージに都合の良い形式で管理したが，他のパッケージへの適用を考えた場合には変更が必要である。

今後，JavaEEに準拠した形式での管理体系に変更していく。

(2) EJBの実行

EJBは登場以来，まだ立場が曖昧(あいまい)な状況にある。最近のEJBは，かなり進化はしたものの，従来のJavaオブジェクトを動作させるなどの点で，否定的な面もうかがえる。また，EJBの動作理論上，EJBで実行した場合，通常のJavaオブジェクトより応答性能が低下するというデメリットもある。

EJBについては，先に述べた方式を取ることで業務ロジックは十分に動作するため，今後とも実装は不要と考えるが，更なる検証が必要である。

(3) HTTPのセッション管理

検証対象パッケージでは，リッチ・クライアント方式を採用しており，通信ごとに必要な情報を交換し合うため，HTTPセッションが不要であった。ただし，リッチ・クライアント方式ではない一般的なアプリケーションでは，サーバとのやりとりを頻繁に行う必要があるため，HTTPセッションが多く使われることになる。

今後，他のパッケージへの適用に向けて，HTTPセッション管理の実装を進めていく。

(4) コネクション・プール

データベースとのコネクションは，必要に応じて確立する方法を取ると，接続・切断のオーバーヘッドによって応答性能が劣化する。これを解消するために，多くのアプリケーションサーバでは，都度コネクションを切断せずに保持する機構(コネクション・プール)を備えている。

検証に使用した簡易アプリケーションサーバにはこの機能を実装しなかったが，実用化に当たっては，オープンソースであるTomcat(注6)アプリケーションサーバのコネクション・プール機構を実装する方向で検討を進めていく。

(5) Webアプリケーションの再起動

多くのアプリケーションサーバでは，サーバを再起動することなく，一部のアプリケーションのみを再起動(再読み込み)することが可能である。これは，Java VM(Virtual Machine)に用意されたクラスローダーをアプリケーション・サービスごとに用意することで実現されている。

今回の簡易アプリケーションサーバでは，この機能を実装していないため，同一アプリケーションサーバ上で複数のアプリケーション・サービスを提供した場合に，各サービス単位での保守がしにくくなる可能性がある。

(注6) Tomcatは，Apache Software Foundationの商標である。

5. むすび

今回の検証によって，アプリケーションサーバ上で動作する小売店向け販売管理パッケージのソフトウェアを，汎用的なIaaS環境下で動作させるための方法が確立できた。

これによって，このパッケージの機能をSaaSとして提供するための方法に技術的な目処(めど)が立ったほか，アプリケーションサーバのバージョンアップに伴うアプリケーションパッケージ側の改修を最小に抑えることについても大きく前進した。

このソリューション技術は，既存の業務アプリケーションパッケージのSaaS化に有効であるほか，業務アプリケーションパッケージの維持開発費を軽減する方法としても，十分な効果が期待できる。

今後は，優良なベンダーの選定やデータベースの管理をはじめとしたサービス化への課題にも取り組み，より利便性の高いサービスの実現を目指していく所存である。

特集論文

企業価値向上と商談機会創出に貢献する三菱電機オフィシャルウェブサイトの再構築

磯西徹明*
安齋利典**
大矢富保**

Reconstructuring of Mitsubishi Electric Official Website Contributing to Business

Tetsuaki Isonishi, Toshinori Anzai, Tomiyasu Oya

要　旨

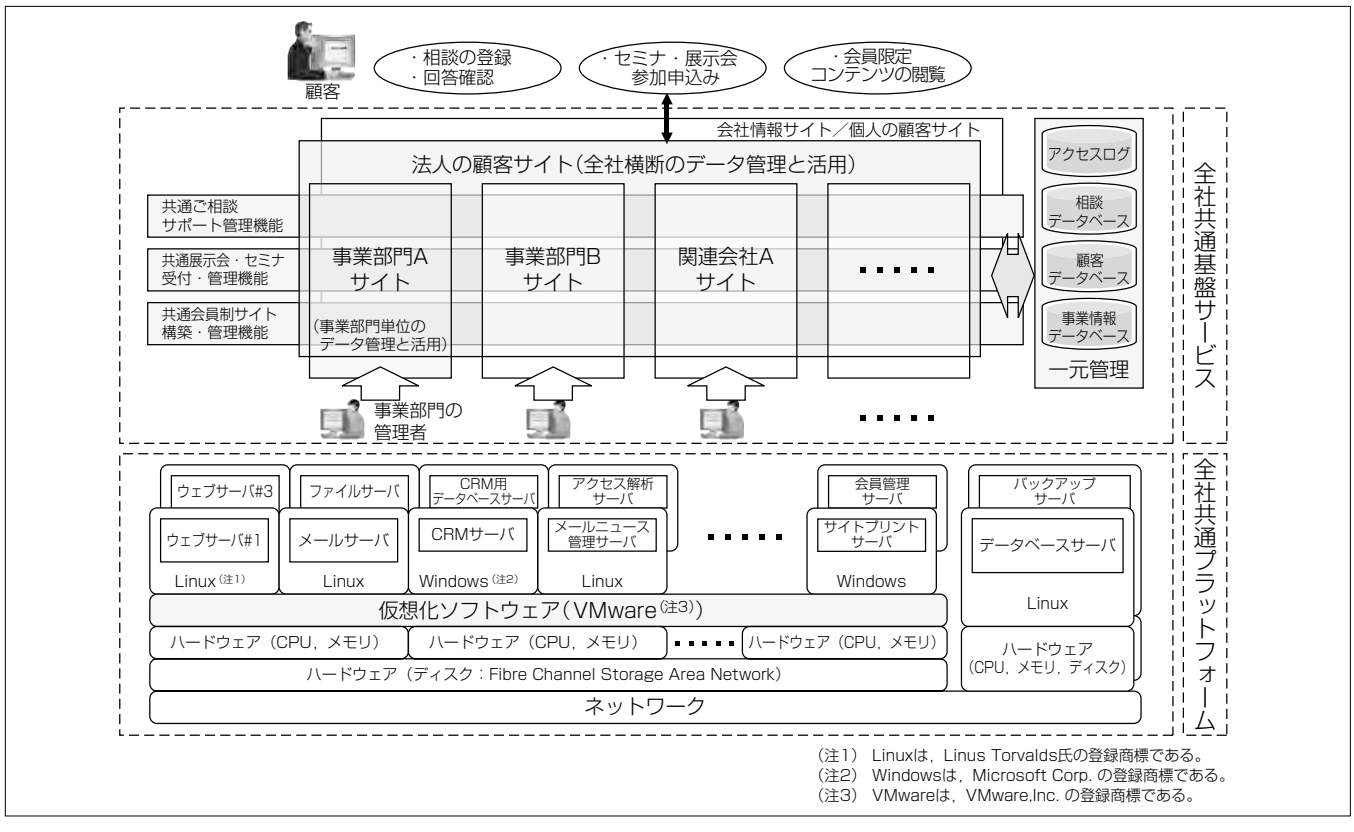
IT技術の進歩に伴い，インターネットは単なる情報発信や情報共有手段ではなく，すべての人々の生活になくてはならない社会インフラへと変化している。その基盤の上に成り立つ企業ウェブサイトは，企業のあらゆる活動にとって必要不可欠なものとなり，企業目的を達成するための手段として大きな役割を担うようになってきた。

三菱電機オフィシャルウェブサイト(1)（以下“当社サイト”という。）は，三菱電機宣伝部がシステムインフラ，コンテンツ・サイトマネジメント，ウェブマーケティングの機能を一元的に統括・管理し，三菱電機の“企業価値向上”と“商談機会創出”を目的として運営している。

この当社サイトは，2001年に全面的見直しを行い，全社統合的なオフィシャルサイトとして立ち上げ，先進技術を取り入れつつ，様々な企画，施策を実行し，発展させてきた(2)。

その後，政府による通信と放送の融合施策，デジタル放送本格化などによって，インターネット環境が激変して広告宣伝と企業ウェブサイトのあり方が大きく変わるとの予想の下，新たな環境に適合した次世代のプラットフォームとビジネスに活用できる種々サービス提供を行う“オフィシャルウェブサイトの中長期的再構築”を開始した。この再構築では，サーバ仮想化技術やクラウド技術を活用し，2009年から3か年計画で次の4つの重点施策を推進中で，初年度にかなりの成果を挙げることができた。

(1) サーバの整理統合・運用管理の効率化
(2) 危機管理，コンプライアンス対応の強化
(3) 多様化するメディアと表現方法への対応
(4) BtoB(Business to Business)マーケティング基盤構築による商談機会創出



（注1） Linuxは，Linus Torvalds氏の登録商標である。
（注2） Windowsは，Microsoft Corp. の登録商標である。
（注3） VMwareは，VMware,Inc. の登録商標である。

再構築中の三菱電機オフィシャルウェブサイトの機能と構成

三菱電機オフィシャルウェブサイトの再構築では，システムの効率化，可用性向上，CO_2削減等を目的とし，仮想化技術を用いてサーバ統合を進めている。また，ビジネスに活用できる相談サポート，会員制サイト構築・管理機能等の共通機能をサービス化し，事業部門単位で機能，リソースを選択的に使用できるようにした共通基盤サービスを整備している。ウェブサイトを通じて収集・蓄積した種々データは，全社横通しで活用できる。

*三菱電機インフォメーションシステムズ㈱　**三菱電機㈱ 本社

1. まえがき

IT技術の進歩に伴い，インターネットは単なる情報発信や情報共有手段ではなく，人々の生活になくてはならない社会インフラへと変貌(へんぼう)している。その基盤の上に成り立つ企業ウェブサイトは，企業のあらゆる活動にとって必要不可欠なものとなり，多数の人々と直接コンタクトできる強力な手段として，企業目的を達成するための大きな役割を担うようになってきた。

また近年，CPU(Central Processing Unit)とネットワークの高速化，ディスク・メモリの大容量化，低価格化がますます進み，さらにサーバ，ストレージ等の仮想化技術の進歩に伴い，“所有から利用へ”というサービス化の流れが進展し，クラウド技術を利用して自社内の各部門にサービス提供する動きも出てきている[(3)(4)]。

本稿では，①サーバ仮想化技術を応用したシステムの統合と効率化，②事業部門単位で機能とリソースが選択的に活用できる共通基盤サービスの提供とその社内標準化，③全社的視点でのサイト全体の最適化をねらいとする“三菱電機オフィシャルウェブサイトの中長期的再構築”の3か年計画(2009～2011年度)と，これまでの実績・成果について述べる。

2. 三菱電機オフィシャルウェブサイトの現状と課題

2.1 役割と背景

当社サイトは，宣伝部が全社最適化の観点でシステムインフラ，コンテンツ・サイトマネジメント，ウェブマーケティングの機能を一元的に統括・管理しているのが特徴であり，三菱電機の“企業価値向上”と“商談機会創出”を目的として全社的なガバナンスの下で運営している。

2001年に当社サイトの全面的見直しを行って以来，様々な企画と施策を繰り返し発展させてきた[(2)]。また，政府のu-Japan政策，通信・放送法改正，地上デジタル放送本格化等を睨(にら)み，2011年以降は，放送と通信の融合が実現し，本格的ユビキタス社会になり，インターネット環境が激変することによって広告宣伝と企業ウェブサイトのあり方が大きく変わると2007年度末に予想した[(5)]。そして，この予想に基づき，当社サイトは，新たな環境に適合した次世代のプラットフォームとビジネスに活用できる種々サービスの提供が不可欠と考え，**図1**に示すように，新たなフェーズに移行するための種々施策を実行している。

2.2 機能と構成

当社サイトは現在，国内向けとして会社情報・個人の顧客・法人の顧客サイト，海外はグローバル・地域ポータルと海外事業サイト，及び一部の関連会社サイトから構成されている。国内向けサイト全体は，およそ10万ページからなり，扱う製品の機種は，個人向け39機種，法人向け104機種に上り，月間2,000万ページビュー以上(事業部門独自運営部分等を除く)の大規模なものとなっている。

さらに，サイト内には，**表1**に示すようなセキュリティを維持しながら安定的に運用するために，多岐にわたる機能が搭載されている。

これらの機能は，宣伝部が管理・運営するサーバ群と各事業部門独自に管理・運営しているサーバ群，そしてApplication Service Provider(ASP)のサーバ群によって提供されており，ウェブサーバだけでなく，**表2**に示す様々なサーバ群が密に連携することによって動作している。

2.3 課　題

当社サイトは，宣伝部で企画運営しているが，それを支える基盤となるネットワーク等のインフラ整備，システム構築，アプリケーション開発，システム運用保守は，三菱電機インフォメーションシステムズ㈱(MDIS)が担当している。

個人情報保護法，会社法の施行等によって，2006年ごろから企業ウェブサイトの社会的役割が変化し，システムの信頼性への強い要求や運用保守費用の削減等，様々な課題が山積し，より安全・安心・安定なシステム運営に向けた早急な課題解決が必要となった。

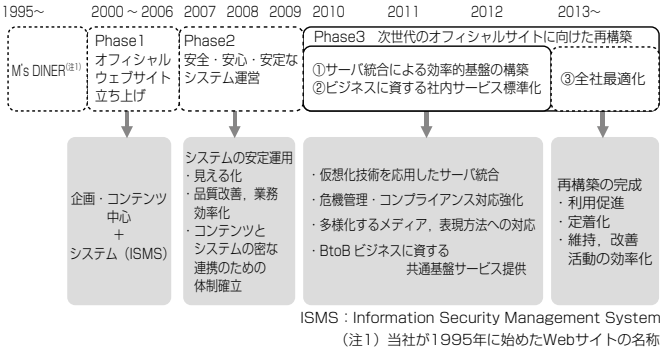


図1．三菱電機オフィシャルウェブサイト構築の変遷

表1．オフィシャルサイトの機能例

分類	機能の種類
サイトトップページからリンクされている重要機能	ニュースリリース機能，重要なお知らせ機能，消費生活用製品安全法に基づく事故報告機能など
個人情報管理を伴う機能	会員制サイト機能，製品登録サービス機能，　メールニュース配信機能，アンケート機能，お問合せ・ご相談対応機能，展示会・セミナー開催・募集機能など
ユーザーの利便性向上のための機能	サイト内検索機能，サイトプリント機能，動画・地図配信機能，モバイル端末へのコンテンツ配信機能など

表2．オフィシャルサイトの代表的サーバ

分類	代表的サーバ
基本サーバ	ウェブサーバ，ファイルサーバ，バックアップサーバ，データベースサーバ，運用監視サーバなど
アプリケーション及び管理サーバ	メールサーバ，メールニュース管理サーバ，アンケート管理サーバ，コンテンツ管理サーバ，コンテンツ・アプリケーション検証サーバ，アクセス解析サーバ，検索サーバ，サイトプリントサーバなど

そこで，当社サイトのシステムにかかわるプロジェクト管理と品質改善，生産性向上に取り組んだ結果，システム運営業務の見える化，システム障害発生数と運用コストの削減等，大きな成果が得られるとともに，将来に向けた全社的視点の検討ができるようになった[5]。そして，2008年から始めたこの検討の結果，見えてきた課題は，次の3点に集約される。

⑴ サーバ数とCO_2排出量の増加とリスクの増大

当社サイトの機能が増加するにつれ(現在，全社で約100システムが稼働)，アプリケーションとサーバがほぼ1対1のサイロ型システム構成では，ハードウェアが増え続けると同時にCO_2排出量も増え続ける。また，リプレースや新機能導入の都度，時間とコストがかかると同時に障害発生のリスクが増大する。

⑵ 危機管理，セキュリティレベルの不均質化と非効率性

まだ事業部門などが運営するサーバが分散しており，会社不祥事，製品不具合発生時を含む危機管理が全社統合的にできにくい。また，セキュリティレベルが不均質であるとともに，重複管理によってコスト増を招いている。

⑶ ビジネスに必要な新機能導入の非効率性

事業部門，関連会社ごとにビジネスに必要なツールを独自に開発，又は導入していたのでは効率が悪い。また，全社的視点で事業部門間を横断したデータ連携とその活用が難しい。

3. オフィシャルウェブサイトの再構築

3.1 再構築の概要

全社の事業部門に対して，次世代のプラットフォームとビジネスに活用できる種々サービスの提供を目指すとともに，**2. 3節**で述べた新たな課題解決に向け，2009年度から“オフィシャルウェブサイトの中長期的再構築”を開始した。この再構築は，①サーバ統合による効率的基盤の構築(統合化)，②ビジネスへの活用を目指したサービス提供と社内標準化(標準化)，③全社的視点での当社サイトの最適化(最適化)の3つのステージに分け，サーバ仮想化技術とクラウド技術を活用して構築を推進している。

次に統合化と標準化を目的とした3か年計画(2009～2011年度)における4つの重点施策を示す。

⑴ サーバの整理統合・運用管理の効率化

サーバ仮想化技術を活用し，2011年度末までに現行60台超のサーバを30台に削減するとともに，グリーンIT化の推進によってCO_2削減14%(2008年度比)を目指す。

⑵ 危機管理，コンプライアンス対応の強化

一部分散している事業部門運営サーバの統合・管理によって，セキュリティの均質化，高度化を推進し，コンプライアンス強化と危機管理のレベルアップを図る。

⑶ 多様化するメディアと表現方法への対応

サイトプリントシステム[1]導入等，多メディアに対応したワンソースマルチユース化を推進する。

⑷ BtoBマーケティング基盤構築による商談機会の創出

ユーザー情報の取得，その全社横断的活用と定量的効果測定可能な共通基盤サービスを開発し，全社に提供する。

3.2 サーバ統合による効率的基盤の構築

今回の再構築では，60台を超える多数のサーバを仮想化技術によって統合し，リプレースや新規サービス導入の際のコスト削減，サーバ台数削減による運用保守費用の削減が可能となる基盤構築を第一の目的とした。この際，当社サイトの可用性，性能・拡張性，運用保守性，移行性，セキュリティ，環境・エコロジー，将来の社内サーバ統合，新サービスの導入などを考慮し，基盤となるサーバ仮想化ソフトウェア(VMware)，物理サーバ(VMware社認定ハードウェア)，ストレージ(Fibre Channel SAN(Storage Area Network))を選定した。また，性能と可用性の観点から物理サーバ，仮想サーバの配置を考えたシステム設計を行うとともに構築を進めている。

2009年度は，3か年計画の初年度ではあったが，次のような大きな成果が得られた。

⑴ 60台超のサーバのうち，仮想化対象サーバ28台を6台(2台/セグメント)の物理サーバに統合し，ウェブサーバ，ファイルサーバ，メールサーバ，メールニュース管理サーバ，アクセス解析サーバ，サイトプリントサーバ(新規追加)，相談受付とサポートのためのCRM(Customer Relationship Management)サーバ(新規追加)などが仮想環境で稼働を開始した。

⑵ コールドスタンバイ機(物理サーバ)と合わせVCS(Veritas Cluster Server) for VMware ESXによって，ハードウェア障害及びアプリケーション障害が発生した際に即時に復旧可能なホットスタンバイ機能の部分導入が完了し，**図2**に示すように，全体的に可用性と信頼性が向上した。

⑶ MDISが開発したITシステムの環境負荷評価手法に基づき効果を試算した結果，この計画終了段階では，サーバ60台超が25台に，年間CO_2排出量57.2tが30.9tに削減できる目処(めど)が立ち，計画を上回る成果が見込まれる。

稼働状態の分類			可用性	可用性向上策	再構築前	再構築後	サーバ(例)
①	サービス停止なし	縮退 短	高	LB + HS	−	1	ウェブサーバ
②		縮退 中		LB + CS	−	1	
③		縮退 長		LB	1	−	−
④	障害時復旧機能あり	停止 短		HS	2	2, 3	ファイルサーバ，メールサーバ，コンテンツ管理サーバ，アクセス解析サーバ
⑤		停止 中		CS	3	3, 4	
⑥	障害時復旧機能なし	停止 長	低	なし	4	−	−

LB ：負荷分散装置
HS ：ホットスタンバイ
CS ：コールドスタンバイ
1～4：再構築前のサーバ可用性レベル
HS，CS機能は，VCS for VMware ESXによって実現

図2．サーバ仮想化技術による可用性向上策

利用者の目的＼提供サービス	基本サービス	共通基盤					ホスティング	オプション					依頼対応				
		相談受付・管理	相談サポート・管理	メールニュース／アンケート配信・管理	展示会・セミナ開催・募集	会員向けサイト提供	データベース利用（選択）独自Webアプリケーション開発環境提供	動画の利用	独自運用アップロードツール利用	範囲限定検索の利用	アクセス解析	独自ドメインサイト提供	アクセス解析レポーティング	メールニュース配信	キャンペーンの抽選	アンケートの実施	展示会セミナの開催・募集
コンテンツの掲載をしたい	○																
問い合わせ・資料請求・相談フォームをサイトに追加したい	○	○															
相談サポートサービスデスク機能を実現したい	○	○	○														
メールニュースの配信をしたい（期間限定・依頼ベース）														○	△		
メールニュースの配信をしたい（継続的・独自運用）	○			○											△		
展示会の募集をウェブでやりたい（独自作成・運用）	○				○											△	
展示会の募集をウェブでやりたい（依頼ベース）																	○
会員制サイトを作りたい	○					○											
共通基盤にない独自のWebアプリケーションを運用したい	○						○										
動画を使ったプロモーションをしたい	○							○									
独自運用で素早いコンテンツの更新を行いたい	○								○								
サイトや事業部，製品単位で独自のサイト内検索窓をつけたい	○									○							
アクセスログを使った効果測定を行いたい（継続的）	○										△		△				
アクセスログを使った効果測定・レポーティングを行いたい（期間限定）	○												○				
独自ドメインを利用したサイトを運用したい												△					
ウェブを使ったキャンペーンの抽選をしたい															○		
ウェブを使ったアンケートとその集計をしたい（依頼ベース）																○	

○：目的に対応した不可欠サービス、△：必要に応じて選択するサービス

図3．オフィシャルウェブサイトに関わる社内提供サービス

(4) 静的コンテンツの内容の妥当性（最新情報か，誤りはないか）とページ数の確認，動的コンテンツ（CGI（Common Gateway Interface）プログラム等）のセキュリティ脆弱（ぜいじゃく）性の確認等，リスク管理の観点で当社サイトのコンテンツの棚卸しを実施した。また，静的コンテンツの新ウェブサーバへの移行が完了し，稼働を開始した。

3.3 ビジネスへの活用を目指したサービスの提供と社内標準化に向けて

今回の再構築では，サーバ統合と併行して，ビジネスへの活用を目的としたユーザー情報の取得と蓄積，それらの事業部門単位での活用と全社横断的活用，そして定量的効果測定が可能な共通基盤サービスを開発し，社内の事業部門に提供する施策を推進している。

2009年度は，マルチテナント型の①相談受付・管理・分析（テキストマイニング）・サポート機能，②会員制サイト構築・管理機能，③展示会／セミナ開催・募集・管理機能等を開発・導入し，社内各事業部門に向けたサービスの提供を開始した。これらの社内標準サービスを使用することによって，社内事業部門はセキュリティレベルの高い，高品質なウェブサイトを短期間で構築できるだけでなく，全社横断的なデータ活用が可能となる。また，これらの運用は，全社一元的に管理している宣伝部が行うため，事業部門の負担が軽減され，セキュリティレベルの均質化が実現できる。

現在宣伝部では，従来提供しているサービスを含め，**図3**で示すように提供サービスを整理し，事業部門が共通に活用できる運用業務及び管理の社内標準化，SLA（Service Level Agreement）を基にした費用徴収，責任分担の明確化，共有運用体制の整備等を進めている。

4. むすび

2011年以降は，企業の広告宣伝と企業ウェブサイトのあり方が大きく変わり，当社サイトがビジネスの重要な武器となると考え，“オフィシャルウェブサイトの中長期的再構築”を推進してきた。本稿で述べたように，当社サイトは統合化・社内標準化の道を歩み始めたばかりである。今後は，最新のIT技術を活用しながら，あらゆるステークホルダーにとって必要不可欠な“情報ハブ”として，また，当社ビジネスを牽引（けんいん）する“ビジネスエンジン”として発展させていく所存である。さらに，最近ビジネスへの活用が注目されているYouTube，Twitter等のソシアルメディアの活用にも目を向け，当社サイトのソシアル化も含め検討していく。

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) 磯西徹明，ほか：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，三菱電機技報，**82**，No.7，469～472（2008）
(3) 丸山不二夫：クラウドの成立過程とその技術的特徴について，情報処理，**50**，No.11，1055～1061（2009）
(4) 浦本直彦：クラウドコンピューティングにおけるセキュリティとコンプライアンス，情報処理，**50**，No.11，1099～1105（2009）
(5) 安齋利典，ほか：マネジメントシステムを活用した三菱電機オフィシャルウェブサイト運営，三菱電機技報，**82**，No.10，638～641（2008）

特集論文

クラウドシステム構築のためのセキュリティ基盤(1) ーモデルシステムと実証実験ー

村澤　靖*　澤部直太***
高畑泰志**
津國　剛***

Security Platform for Cloud Computing Based Systems—Testbed Experiments—

Yasushi Murasawa, Yasushi Takahata, Takeshi Tsukuni, Naota Sawabe

要　旨

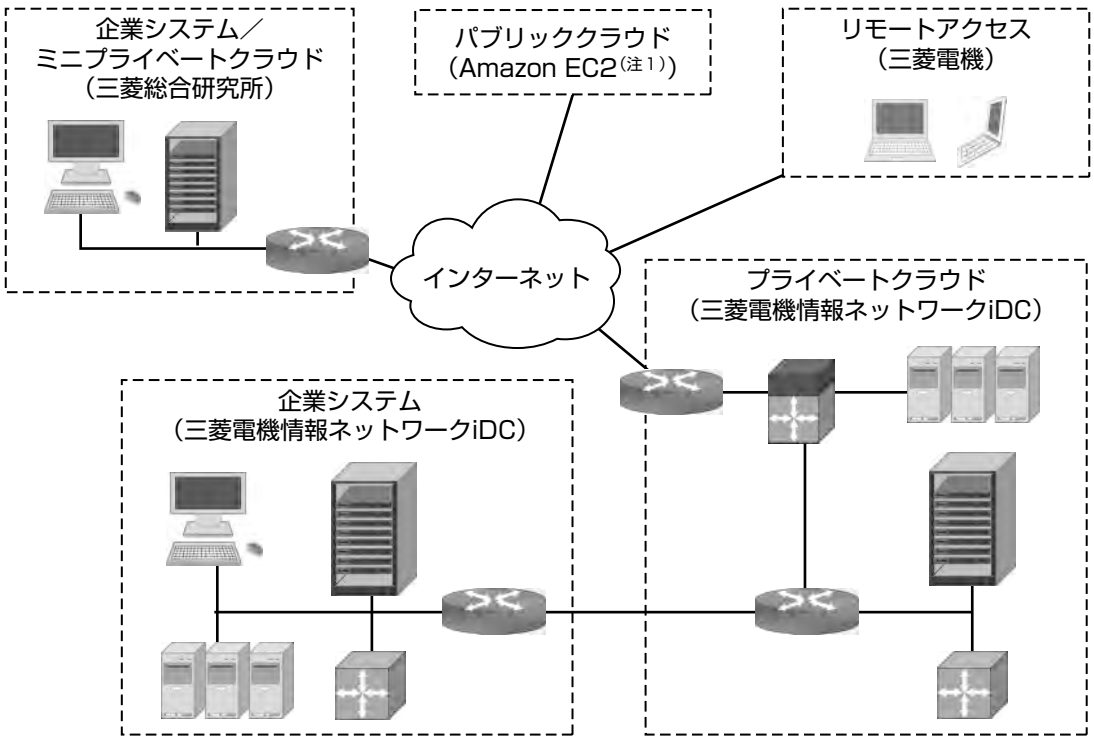
クラウドコンピューティングは，ITリソース調達の柔軟性や費用対効果などの面から，企業システムのプラットフォームとしての普及が期待されているが，セキュリティ上の課題が残されていることなどによって，企業システムとしての利用は一部に留(とど)まっている。クラウド環境へ移行したシステムを利用するに当たっては，従来の企業システムと同様に，データやネットワークなど様々なレベルでの利用者に応じたアクセス制御が必要である。その際，アカウント情報は個人情報であり，高度な機密情報であることから，アカウント情報を保護した上で実現する必要がある。

我々は，企業システムのクラウド環境への移行期を想定し，企業システムが置かれた企業環境と，プライベートクラウド，パブリッククラウドからなるクラウド環境及びリモートアクセス環境からなる実証実験システムを構築し，次の観点から検証した。

(1)　企業システムとクラウド間の認証連携の実現
(2)　データの利用者権限管理の実現
(3)　仮想ネットワークによるアクセス制御の実現
(4)　大規模ユーザー環境への対応の実現
(5)　システム運用者に対するシステム操作制御の実現

検証では，企業ユーザーがクラウド環境で社内外のユーザーとファイルを共有するシーンを想定したファイル共有アプリケーションを使って，企業が業務でクラウド環境を利用する各種場面を想定したシナリオを実施し，実装した認証基盤やデータ利用権管理機能などの有用性を確認した。

本稿では，実証実験システムとその実証実験の概要を中心に述べる。なお，認証基盤及び仮想ネットワークについては，別稿で詳しく述べる。



（注1）Amazon EC2は，Amazon Technologies, Inc. の登録商標である。

iDC：internet Data Center

実証実験環境の全体像

実証実験環境は，企業環境とクラウド環境に大きく分かれている。クラウド環境は，プライベートクラウドとパブリッククラウドから構成した。パブリッククラウドは，Amazon EC2 (Elastic Compute Cloud) サービスを利用した。また携帯電話などリモートアクセスも可能とした。

*三菱電機㈱ 情報技術総合研究所　**同社 同研究所(情報学博士)　***㈱三菱総合研究所

1. まえがき

企業システムは，ホストコンピュータを用いた業務システム，クライアント・サーバシステムを経て，現在ではWebコンピューティング技術の活用によって，業務の効率性の向上や法規制，各種の脅威などに対応するものとなってきている。一方，ここ数年で台頭してきたクラウドコンピューティングについては，ITリソース調達の柔軟性や費用対効果などの面から，企業システムのプラットフォームとしては非常に魅力的である。しかし，クラウド環境におけるセキュリティ実装の不明確さなどによって，データ保護への懸念などの課題が残されており，企業システムとしてクラウド環境を利用することを躊躇(ちゅうちょ)させる原因となっている。仮に，クラウド環境の利用を考慮する場合，一般には既存のIT資産があることから，すべてのシステムを一度にクラウドに移行することは少ないと考えられる。現実的には，既存システムを機能別，役割別にサブシステムに分割し，クラウド環境が同等の機能を提供している部分から移行していき，既存サブシステムとの連携を図るといった移行シナリオを用いることが想定される。クラウド環境へ移行したシステムを利用するに当たっては，従来の企業システムと同様に，データやネットワークなど様々なレベルでの利用者に応じたアクセス制御が必要である。その際，アカウント情報は個人情報であり，高度な機密情報であることから，アカウント情報を保護した上で実現する必要がある。この課題に取り組むため，実証実験システムを構築して検証した結果について述べる。

2. 実証実験システム

2.1 実証実験環境の全体像

実証実験環境の全体像を**図1**に示す。

システムは，企業環境とクラウド環境に大きく分かれており，**表1**に示すようにそれぞれ企業システム，及びプライベートクラウド，パブリッククラウドから構成した。パブリッククラウドの構築に当たってはAmazon EC2サービスを利用した。また，携帯電話やモバイル端末からインターネット経由でリモートアクセスも可能とした。

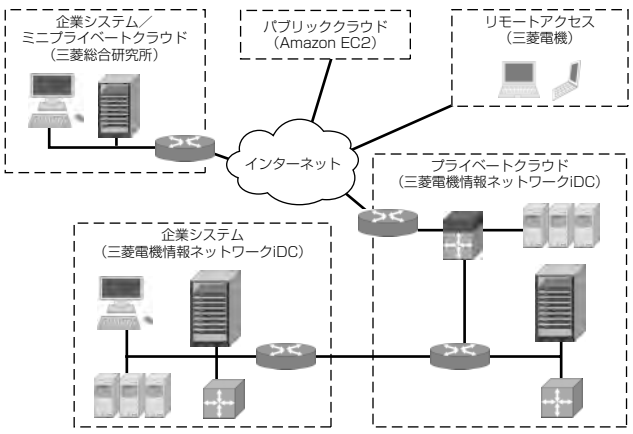


図1．実証実験環境の全体像

ソフトウェアはOSS(Open Source Software)をできる限り活用するとともに，認証機能やデータのアクセス制御機能の実装に当たり，SAML(Security Assertion Makeup Language)やXACML(eXtensible Access Control Markup Language)といった標準仕様を採用した。また，仮想ネットワーク[1]やPUZZLET認証[2]といった三菱電機の保有技術も活用した。

2.2 各サブシステムの構造

企業システム，プライベートクラウド，パブリッククラウドのシステム構造は共通であり，その概略構成を**図2**に示す。

(1) 企業システム

企業システムでは，ブレードサーバ上に仮想化ソフトウェアとしてVMware(注2)を搭載し，シングルサインオン機能を実現するOSS のOpenSSO(Single Sign-On)を使った認証認可サーバ，Webサービスによるアプリケーション連携機能を実現するOSSのServiceMixを使ったESB(Enterprise Service Bus)サーバなどを動作させた。10万人分のアカウント情報を認証認可サーバ内に保管した。また，大規模ユーザー環境に対応するため，ロードバランサを使ってサーバの処理を負荷分散している。

(2) プライベートクラウド

プライベートクラウドでは，ブレードサーバ上に仮想化ソフトウェアとしてXen(注3)を搭載し，企業システムと同様，認証認可サーバ，ESBサーバやロードバランサなどから構成している。また，インターネットアクセス用にDMZ(DeMilitarized Zone)を構築し，メールサーバなどを個別に設置した。

表1．各サブシステムの説明

分類	システム名	説明
企業環境	企業システム	従来の企業システムの中核部分が動作するシステム。利用者のアカウント情報を保管している。
クラウド環境	プライベートクラウド	従来の企業システムの一部が移行した社内向けサブシステムの位置付け。社内利用のデータを保管している。
	パブリッククラウド	従来の企業システムの一部が移行した社外向けサブシステムの位置付け。社外とやり取りするデータを保管している。

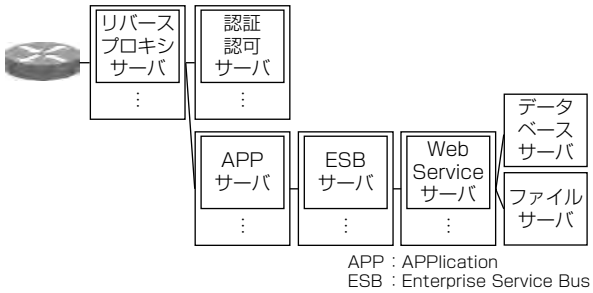


図2．各サブシステムの構造

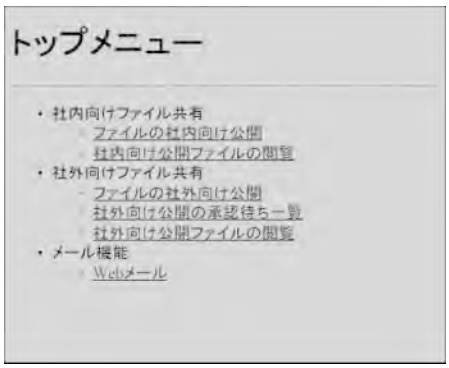


図3．トップメニュー画面

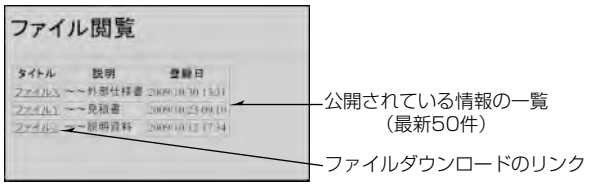


図4．ファイル一覧画面

(3) パブリッククラウド

パブリッククラウドは，Amazon EC2サービスを利用して，固定IP(Internet Protocol)アドレスを割り当てた7台のサーバ上に，企業システムと同様認証認可サーバ，ESBサーバなどを動作させた。

(注2) VMwareは，VMware, Inc.の登録商標である。
(注3) Xenは，Citrix Systems, Inc.の登録商標である。

2.3 評価用アプリケーション

今回，評価用業務アプリケーションとして，社内ユーザーがクラウド環境で社内外のユーザーとファイルを共有するシーンを想定したファイル共有アプリケーションを開発した。社内ユーザーが他の社内ユーザーへファイルを公開したり，社外ユーザーへ上長承認を経てファイルを公開したりするためのユーザーインタフェースを提供する。トップメニューを**図3**に，ファイル一覧画面を**図4**に示す。

ファイルの閲覧やワークフローなど，アプリケーションで共通的に利用する機能はサービスとしてWeb Serviceサーバ上で動作する。アクセス元アプリケーション，及び利用者の権限の組合せによって各サービスへのアクセスを制御するサービス認可も実装した。

3. 実証実験

実証実験は，企業が業務でクラウド環境を利用する各種場面を想定した10個のシナリオに基づく検証を行った。その概要について述べる。

(1) 企業システムとクラウド間の認証連携

企業システム及びクラウドの相互間で，認証及び認可が適切に連携できることを検証した。企業システムで認証されたユーザーAが，プライベートクラウドへ再認証することなくアクセスするシナリオの一部を次に示す。

①ユーザーAが企業システム上のパソコンからファイル共有アプリケーションにログオンする(**図3**が表示される)。
②ユーザーAは“ファイルの社内向け公開”を選択し，ファイルXを作成し，ファイルXに対して，ユーザーBはアクセス許可，ユーザーCはアクセス不可の設定を行う。
③ユーザーAはファイルXを登録すると，ファイルXがプライベートクラウド内に保管される(ユーザーAでプライベートクラウドへ認証連携機能によってシングルサインオンが実行される)。

シナリオに沿った操作を実施し，システム動作時に出力されるアプリケーションやミドルウェアのログによって，想定した機能が動作していることを確認した。

(2) データの利用者権限管理

プライベートクラウド，パブリッククラウドで，ユーザー単位でデータの利用が適切に制御できることを検証した。ユーザーCには参照不可の設定がされているプライベートクラウド上のファイルXが保護されていることを確認するシナリオの一部を次に示す。

①ユーザーCが企業システム上のパソコンからファイル共有アプリケーションにログオンする(**図3**が表示される)。
②ユーザーCは“社内向け公開ファイルの閲覧”を選択する(**図4**が表示される)。
③ユーザーCはファイルXを指定するが，ファイルを読み出すことができない。

シナリオに沿った操作を実施し，システム動作時に出力されるアプリケーションやミドルウェアのログによって，想定した機能が動作していることを確認した。また，②において，“社外向け公開ファイルの閲覧”を選択することで，パブリッククラウド上のファイルについても同様に確認した。

(3) 仮想ネットワークによるアクセス制御

IPv6を活用した仮想ネットワークによって，クラウド環境に配置される各サーバへのアクセスが適切に制御されることを検証した。具体的には，企業システム～プライベートクラウド間通信路を論理的に分割し，pingによるサーチによって，あらかじめ許可された組合せの装置間だけが通信可能で，他の組合せでは通信不可能となるように制御できていることを確認した。

(4) 大規模ユーザー環境への対応

大規模ユーザー環境での実証実験システムの動作を評価するため，1万ユーザーがアクセスし，ファイル一覧画面表示の認証連携機能に関する応答性能(応答時間)やエラー発生率を測定した。測定に当たっては，**図5**に示すようにユーザー操作をシミュレーションする性能負荷ツールによ

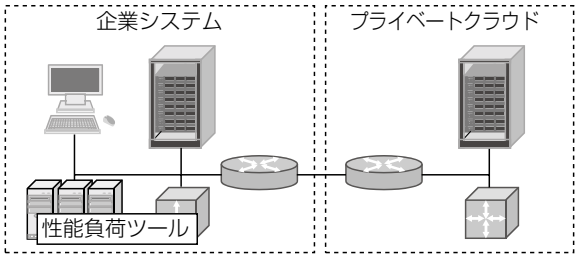


図5．スケーラビリティ検証での構成

表2．スケーラビリティ検証結果

性能指標	目標	測定値
応答性能(ms)	3秒以内	358.0
エラー発生率(%)	0.05未満	0.01

って，企業システムからプライベートクラウドのリソースへのアクセスを実施した。

表2に示すようにそれぞれ目標性能を満たすことを確認した。

(5) システム運用者に対するシステム操作の制御

企業システムのクラウド環境移行時に想定されるセキュリティ脅威の1つとして，クラウドのシステム運用者が管理者権限でクラウドを利用するケースが想定される。この実証実験では，高度なセキュリティ機能が付加されたSELinuxの機能を利用した。プライベートクラウドのシステム運用者によるファイルへのアクセスを防ぐセキュリティポリシーを設定し，OSのログによって想定した機能が動作していることを確認した。

4. むすび

クラウドコンピューティングの普及によって，**図6**に示すようにこれまで企業内に閉じていたシステムが，今後アカウント情報は企業内で管理した状態で，外部のクラウド環境に移行すると考えられる。業務の遂行に必要な共通機能は，サービスとしてクラウド環境で提供され，グループ企業間などでクラウド環境を共同利用する形態も進展すると考えられる。今回の実証実験によって，このような新たなシステム形態で必要となる次の機能を検証することができた。

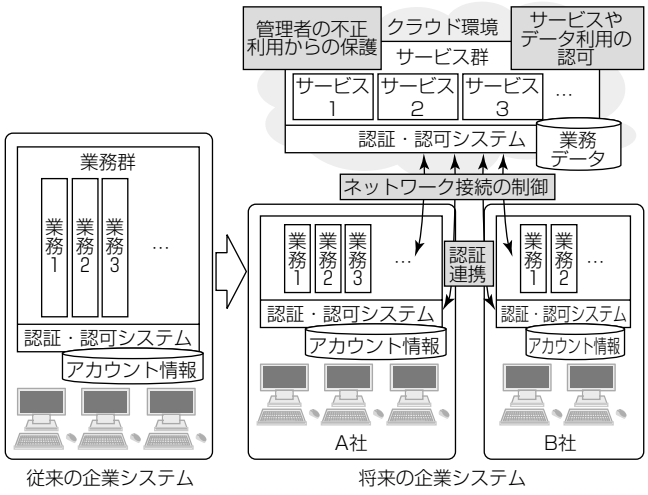


図6．将来の企業システムの形態

(1) アカウント情報を企業システム内のみに保管するとともに，セキュリティ要件に応じた複数の認証機能を提供するセキュアなシングルサインオン

(2) 企業システム又はクラウド上に配置されたサービス，データへのアクセス制御

(3) アドレス資源の豊富なIPv6を活用した仮想ネットワークによるネットワークレベルでのアクセス制御

(4) 管理者権限を持っているシステム運用者の操作の制御

実適用に向けては，信頼性や運用性などの非機能面についても検証が必要であり，今後取り組んでいく。

なお，この研究開発は，経済産業省平成21年度“新世代情報セキュリティ研究開発事業[3]”によって実施したものである。

参考文献

(1) 平井　肇，ほか：分散型仮想ネットワークにおける転送効率化方式の検討と試作機開発，電子情報通信学会技術研究報告，**107**，No.525，265～270（2008）

(2) 桜井鐘治，ほか：背景配列の移動量を用いた個人認証方式ののぞき見に対する安全性評価，情報処理学会論文誌，**49**，No.9，3038～3050（2008）

(3) 経済産業省：平成21年度“新世代情報セキュリティ研究開発事業（クラウドコンピューティングセキュリティ技術研究開発）”公募仕様書（2009）

特集論文

クラウドシステム構築のためのセキュリティ基盤(2) ―認証基盤―

白木宏明*
原田篤史**
大沼聡久*

Security Platform for Cloud Computing Based Systems―Authentication Infrastructure―

Hiroaki Shiraki, Atsushi Harada, Akihisa Onuma

要　旨

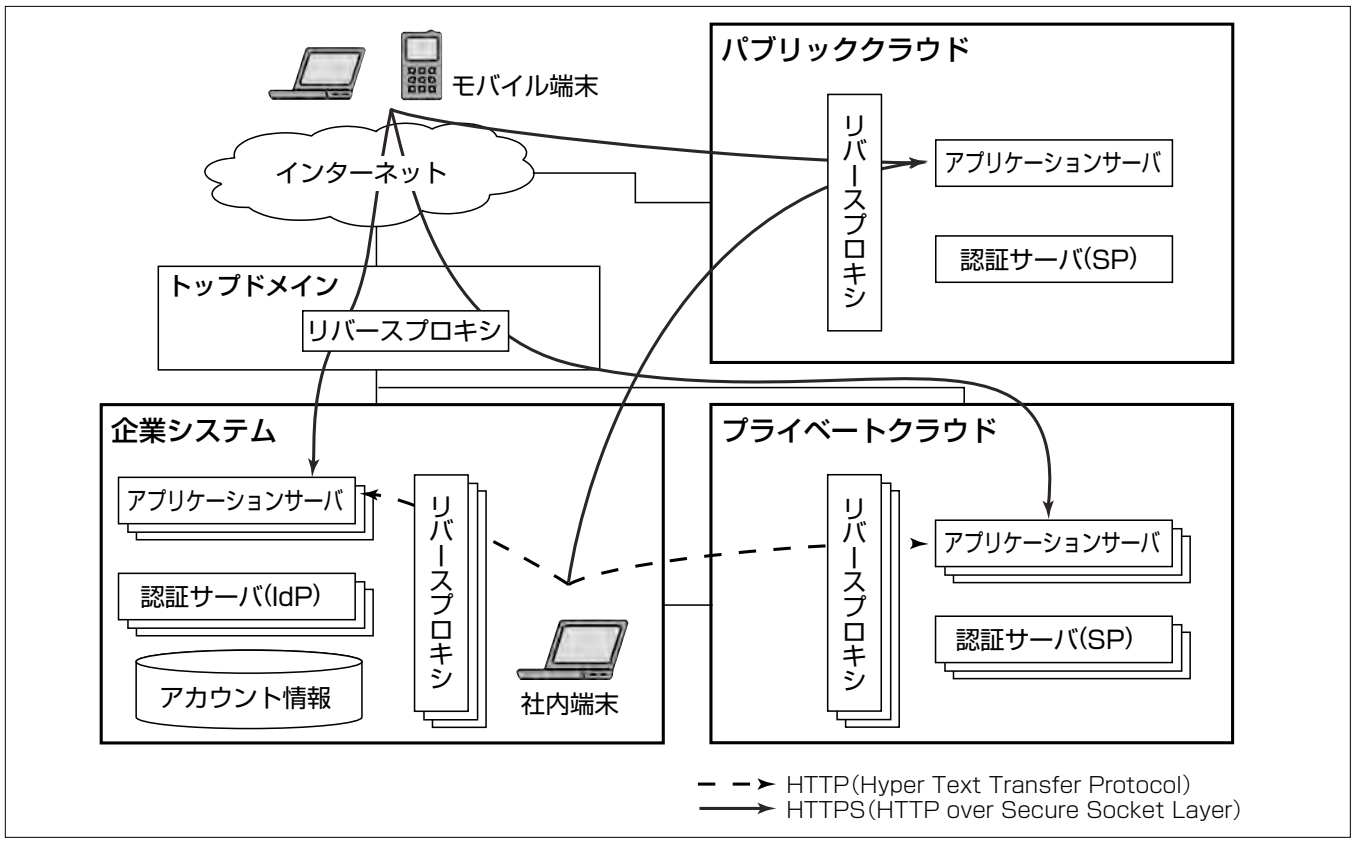
クラウドコンピューティングは今後，利用の拡大が期待されている[(1)]。しかし，クラウド環境を構築する際には，認証・認可や機密情報の管理等のセキュリティ上の問題が存在する。具体的には，機密情報であるアカウント情報を組織の外部となるクラウド環境中に保持することは避けるべきであり，かつ利用者の権限に応じてクラウド環境上のリソースに対するアクセスを制限しなければならないということである。

これらを解決するためには，クラウド環境上のシステムは，企業内システムでの認証システムと連携し，クラウド環境上の認証やリソースのアクセス制御を実現する必要がある。既存の企業内システムとクラウド環境間でアカウント情報の連携と保護を実現する手段を提供することが不可欠となる。

今回の“クラウド環境活用に向けた企業内既存システムとの連携実証実験”で，認証とアカウント情報を企業内に集約しつつ，クラウド環境上で認証・認可及びアクセス制御を実現することができる認証基盤の研究開発を行い，セキュリティ要件を満たすことの検証を目的として実証実験を実施した。

実証実験では，次の要件から評価を実施した結果，先に示したセキュリティ上の問題が解決されており，十分に実システムでの使用に耐え得ることを確認することができた。

(1) 企業内システムからクラウド環境へのシングルサインオン
(2) インターネットからクラウド環境へのシングルサインオン
(3) 認証情報に基づいたクラウド上のアプリケーションによるアクセス制御



認証基盤実証実験のシステム構成

クラウド環境活用に向けた認証基盤のシステム構成は，企業システムのクラウド移行を想定した企業システムとプライベートクラウド，パブリッククラウドからなる。アカウント情報は，企業システム内で管理を行う。クラウド環境上のアプリケーションを利用する場合には，企業システム上の認証サーバで認証を行い，その認証に基づきアクセス制御を実施する。

*情報技術総合研究所　**同研究所(情報学博士)

1. まえがき

現在，ITリソース調達の柔軟性や費用対効果などの面から，クラウド環境は企業システムのプラットフォームとして非常に魅力的であるが，セキュリティ実装の不明確さなどの課題が残されているため，企業システムとしてのクラウド環境の利用は制限されている[2]。

セキュリティ上の問題の一つとして，クラウド環境における認証・認可といったアカウント管理の機能が挙げられる。アカウント情報は個人情報を含む高度な機密情報であることから，組織から見て外部となるクラウド環境に保存することは避けるべきである。また，アカウント情報を含む各種の機密情報は，利用者サイドでアクセスコントロールすべきであり，システム上の特権ユーザーであるクラウド事業者に対するアクセスも制限する仕組みが必要である。このような機密情報の保護を実現した上で，既存の企業システムでの認証結果に基づきクラウド環境上のシステムと連携する手段，すなわち，認証連携を実現する。

クラウド環境におけるセキュリティ上の不安要素のうち，特にアカウント管理に焦点を当て，認証とアカウント管理機能を企業に集約しつつ，認証情報の連携によってクラウド上システムで利用できる認証基盤を研究開発し，実証実験システムを構築して検証した結果について述べる。

2. 認証技術の動向

2.1 認証連携技術

認証連携(IDフェデレーション)技術は，ドメインを跨(またが)ったシステム間でのSSO(フェデレーテッド・シングルサインオン)や，ログアウト(グローバル・ログアウト)を実現するために，システム間で認証情報を伝播(でんぱ)する技術のことである。

2.1.1 主要技術

IDフェデレーションにおける主要技術としてSAML(Security Assertion Markup Language)，OpenID，CardSpaceがあり，**図1**に示すような関係となっている。

それぞれ独立して仕様が策定されたため，技術分野として共通する領域があり，これらの仕様間の相互接続を実現するための取組みが行われている。

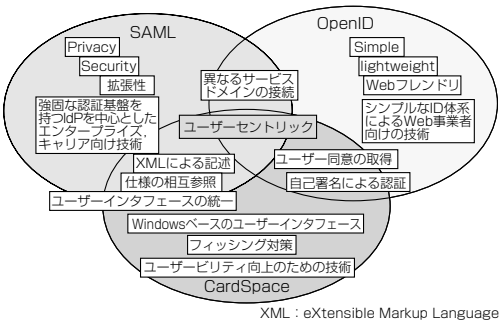


図1．IDフェデレーション主要技術の関係[2]

(1) SAML

SAMLはLiberty Allianceで策定されOASIS(Organization for the Advancement of Structured Information Standards)で標準化された技術仕様であり，認証，認可，属性といったセキュリティ情報をサービス間で交換するための表現形式及びプロトコルを規定している。強固な認証基盤を持つIdP(Identity Provider)を中心に高いセキュリティを必要とする企業，キャリア向けの認証連携の技術として主に用いられている[4][5]。

(2) OpenID

OpenIDはURL(Uniform Resource Locator)を利用し，サイトを越えて使用できる認証方式であり，シンプルでWebとの親和性が高いことから，ポータルサイトやブログなどWeb事業者向けの技術として主に利用されている[3]。

(3) CardSpace

Microsoft社が開発したインターネット上でのID管理，制御，交換のためのシステムである。.NET Framework 3.0の一部としてWindows Vista(注1)，XP等で使用可能な，ユーザービリティ向上のための技術である[4]。

(注1) WindowsとWindows Vistaは，Microsoft Corp.の登録商標である。

2.1.2 標準化の取組み

2009年6月に，IDフェデレーション技術を含めたID管理技術に関する標準化を目的としたカンターラ・イニシアティブ[3]が設立された(**図2**)。合わせて，これまで個別に活動してきたID管理技術の議論の場を1か所にまとめ，より広い視点からオープンに議論できる場を提供することも目的としている。

実質的な活動の中心は分科会活動で，ワークグループ(WG)とディスカッショングループ(DG)の2種類から構成される。WGは文書の発行，他団体への技術仕様のドラフト提出が可能であるが，DGは文書発行，提出する権限はなく，気軽に参加可能なフリーディスカッションの場として設立されている。

2.2 今後の動向

IDフェデレーションのプロトコルは，**2.1.1項**で述べた3技術に収束しつつあり，現在は各プロトコル間での相互運用の検討・実証実験の動きが盛んになっている。

クラウド環境において認証連携は不可欠な技術要素であ

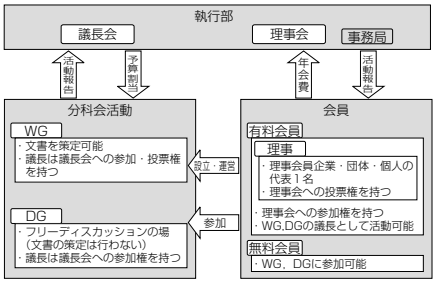


図2．カンターラ・イニシアティブの組織[2]

り，これらの標準化・相互運用の動きとともに，基盤技術としての利用が進むものと期待される。

3. 実証実験システム

3.1 認証基盤及びシステム構成

機密情報の保護が不可欠であるドメイン間の認証連携方式には，高いセキュリティを提供するSAML2.0[4]を用いた。また，クラウド環境内のシステムを隠蔽(いんぺい)するために，リバースプロキシ型シングルサインオン環境[6]をオープンソースソフトウェア(OSS)のOpenSSO Enterprise 8.0 Update1[7](以下“OpenSSO”という。)を使用し認証基盤を構築した。SAML2.0による認証連携をサポートしており，独自の認証機能をプラグインモジュールとして追加することが可能であるため，OpenSSOを採用した。

また，実証実験システムでは，企業システムのクラウド移行を想定した企業システム／プライベートクラウド／パブリッククラウドの3つの構成とした(**図3**)。なお，プライベートクラウドは，グループ企業への業務委託による運用を想定している。

3.2 評価方針

このシステムで，企業システムにアカウント情報と認証機能を集中することで，クラウド上にアカウント情報を持たない認証基盤を構築し，認証連携を実システムへ適用するための次の要件を満足することを検証する。

(1) 企業内システムからのシングルサインオン

企業内システムにID／パスワード認証でログインしたユーザーが，再度認証を要求されることなくクラウド上のアプリケーションにアクセス可能である。

(2) インターネットからのシングルサインオン

モバイル端末からクラウド上のアプリケーションにアクセスする際，PKI(Public Key Infrastructure)認証／PUZZLET認証[8]が行われる。

最初の認証後，企業システム又は別のクラウド上のアプリケーションに対して，再度認証を要求されることなくアクセス可能である。

(3) ユーザーを識別したサービス提供

アカウント情報を持たないクラウドにシングルサインオンしたユーザーのIDを，クラウド上のアプリケーションが利用可能である。

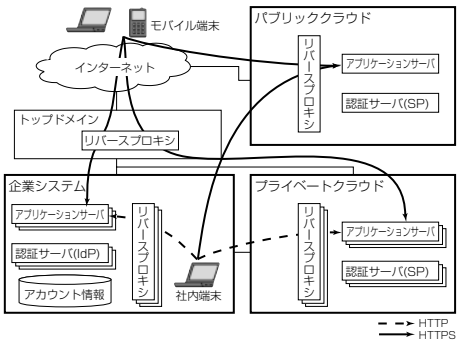


図3．システム構成

なお，企業システム内の認証はID／パスワード方式を採用しているが，セキュリティ上の観点から，インターネットからクラウド上のアプリケーションへのアクセスを許可する場合には，より強固な認証方式を採用することが望ましい。そこで，モバイル端末に対してはPKI認証(クライアント証明書を用いた認証)とPUZZLET認証(三菱電機独自のモバイル認証)を切り換えて利用できるようにした。

3.3 実証方法

実証実験システムでは，認証基盤上に評価用業務アプリケーションとして，社内ユーザーがクラウド環境において社内外のユーザーとファイルを共有するシーンを想定したファイル共有アプリケーションを開発した[1]。

(1) 処理概要

企業システムの社内LAN上の端末から，又はインターネット上のモバイル端末から，各ドメインのWebアプリケーションが利用可能である。すべてのドメインへのアクセスについて，必ず企業システムの認証サーバへリダイレクトされ，認証が行われる。一度認証をパスしたあとは，その認証セッションが継続する間，再度の認証を求められることなく任意のドメインのアプリケーションにシングルサインオンが可能である。認証は必ず企業システムの認証サーバが提供する認証機能を用いて行われ，アカウント情報は企業システム内にしかないことが特徴である。

ドメイン間のシングルサインオンは，SAML2.0のプロトコルを利用して実現している。企業システムの認証サーバがIdPとして認証機能を提供し，クラウド上の認証サーバがSP(Service Provider)としてサービスを提供する。ユーザーがクラウド上のアプリケーションにアクセスすると，クラウド上の認証サーバ(SP側)によって認証済みかどうかのチェックが行われ，認証がまだ行われていなければ，SAML2.0プロトコルに従って企業システムの認証サーバ(IdP側)にユーザー認証の実施を要求する。IdPはユーザー認証を実施し，ユーザーの認証情報(SAMLアサーション)をSPに送信する。SPは認証情報を検証し，ユーザーが認証に合格したことを確認すると，ユーザーにSP側のアプリケーションへのアクセスを許可する(シングルサインオン)。ここで，クラウド上のSPにはアカウント情報が存在しないため，ユーザーは認証セッションが継続する間のみ有効な一時アカウントを利用する。ユーザーIDはIdPからSPに送信され，アプリケーションで利用可能だが，アカウント情報として保存されることはない。

(2) 検証シナリオ

3.2節の要件を検証するためのシナリオは次のとおりである。

①企業システムを経由してプライベートクラウド上のシステムを利用

②プライベートクラウド上のシステムを直接利用
③パブリッククラウドのシステムを利用
④プライベートクラウドを経由して企業システムを利用
⑤プライベートクラウドを経由してパブリッククラウドのシステムを利用

3.4 実証実験結果

3.3節⑵に示した5個のシナリオを実施した結果，**3.2節**で取り上げた要件を満足していることが検証できた。次に，検証結果をまとめる。

⑴ シナリオ①の結果から，企業内システムとプライベートクラウドのアプリケーション間のシングルサインオンが可能であることを確認できた。

⑵ シナリオ②③④⑤の結果から，社内・社外等のアクセス場所に合わせた認証が行われることを確認できた。

⑶ シナリオ④⑤の結果から，プライベートクラウドと企業内システム／パブリッククラウド間のシングルサインオンが可能であることを確認できた。

⑷ シナリオ①②③の結果から，プライベートクラウドとパブリッククラウド環境で，企業内の認証システムから渡されたユーザーのIDを利用可能であることを確認できた。

3.5 評　価

3.2節で述べた⑴～⑶の検証項目については，機能，性能面ともに問題なく動作することが検証できた。今回の評価結果について述べる。

⑴ アカウント情報管理

クラウド環境上にアカウント情報を持たずに，安全な企業内でアカウント情報の管理を行うことで，セキュリティ的に問題なくクラウド環境上のシステムを利用可能なことを検証することができた。

⑵ 企業，クラウド間のシングルサインオン

複数の企業システムと複数のクラウド環境上のシステム間における様々な形態のシングルサインオンが可能なことを検証することができた。

⑶ OSSの利用技術

複数の企業システムと複数のクラウド環境上のシステム認証連携の基本的なプロトコルであるSAML2.0について，利用者の要件に合わせた形での利用技術を確立することができた。また，今回のようなID管理，認証連携システムを構築するために商用ソフトウェアを利用すると高額であるため，OSSを利用したが，その有効性の検証や技術蓄積が限られていた。この検証によって，OSSを利用して独自の認証連携システムを安価に構築する技術を確立できた。

4. むすび

企業間連携の標準プロトコルであるSAML2.0を利用し，企業内システムのID情報を用いて，アカウント情報を持たないクラウドとの連携を可能にする認証基盤の構築を行い，実システムでも十分に利用可能なことが検証できた。また，複数の企業システム及びクラウド上に構築したシステム間での認証連携が可能となり，企業システムをクラウド上に移行させる上で基本的な認証連携の技術ノウハウが蓄積できた。

今回の実証実験では，アカウント情報を企業内で一元管理し，クラウド上に構築した認証システムは，その情報を用いて認証を行っていた。しかし，実際にクラウドを用いる場合，不特定多数の企業がシステムを共有するケースが多くなる。その際，各企業内で管理しているアカウント情報を利用する形で認証を行うケースも増えていくであろう。

クラウド環境利用の拡大をめざして，クラウド上におけるシステム構築技術開発を進めるに当たり，次に示す課題を解決していく。

⑴ OpenIDによる認証連携

OpenIDは，Web事業者向けの認証連携技術として，SAMLと並び普及が進んでいる。将来，様々なWeb事業者が展開するクラウド環境との連携を考えた場合，認証手段の一つとして組み込んでいく必要がある。

⑵ アカウント情報連携の構築手法

各企業内で管理しているアカウント情報をクラウドから利用するため，アカウント情報に対しリンクを張ることで認証を行う方式の実装及び検証を行っていく。

なお，この研究開発は，経済産業省平成21年度“新世代情報セキュリティ研究開発事業”によって実施したものである。

参考文献

⑴ 村澤　靖，ほか：クラウドシステム構築のためのセキュリティ基盤(1)－モデルシステムと実証実験－，三菱電機技報，**84**，No.7，411～414（2010）
⑵ 経済産業省：平成21年度“新世代情報セキュリティ研究開発事業（クラウドコンピューティングセキュリティ技術研究開発）”公募仕様書（2009）
⑶ カンターラ・イニシアティブ
http://kantarainitiative.org/
⑷ 日本PKIフォーラム，PKI-Jジャーナル2007(最終号)
⑸ OASIS，SAML仕様
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20
⑹ IPA：大規模サイトのネットワークセキュリティ
http://www.ipa.go.jp/security/fy14/contents/enterprise/pdf/enterprise.pdf
⑺ The OpenSSO Project
https://opensso.dev.java.net/ja/
⑻ 桜井鐘治，ほか：背景配列の移動量を用いた個人認証方式ののぞき見に対する安全性評価，情報処理学会論文誌，**49**，No.9，3038～3050（2008）

特集論文

クラウドシステム構築のためのセキュリティ基盤(3) ー仮想ネットワークー

清水直樹* 高畑泰志**
都築宗徳*
平井 肇*

Security Platform for Cloud Computing Based Systems—Virtual Network—

Naoki Shimizu, Munenori Tsuzuki, Hajimu Hirai, Yasushi Takahata

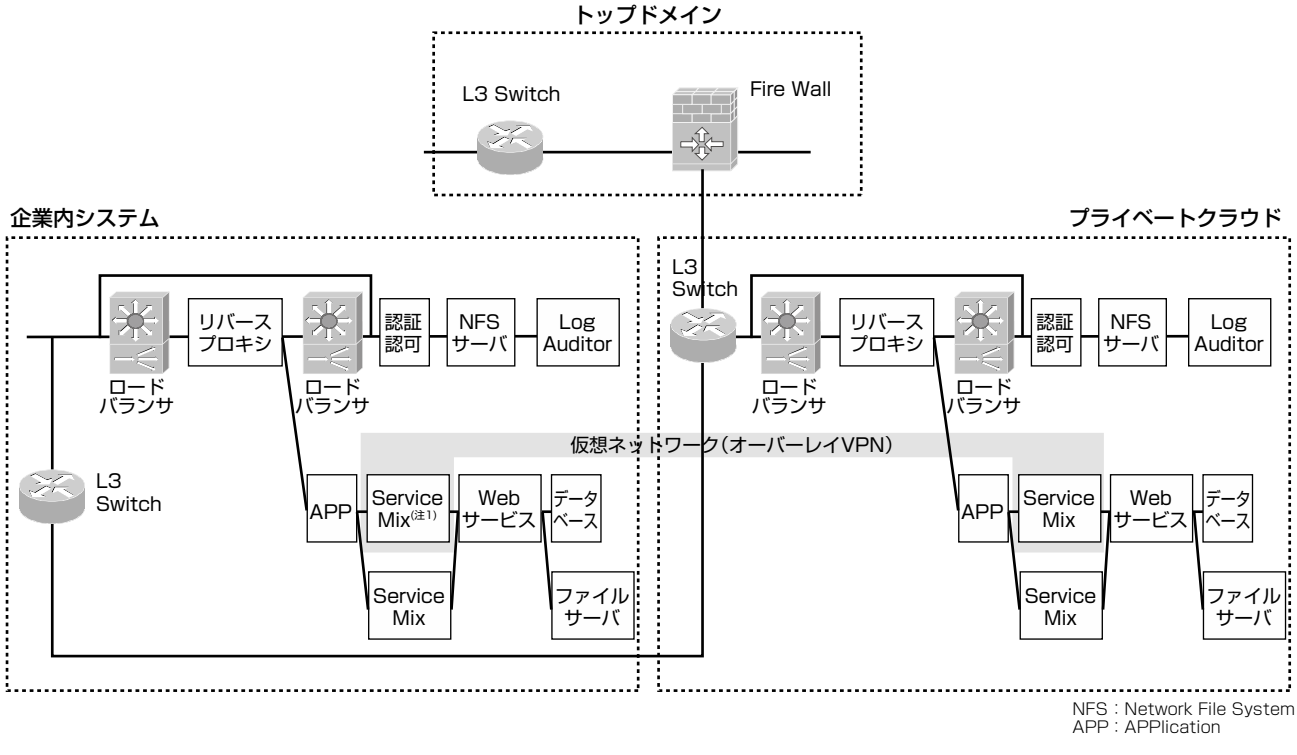
要 旨

クラウド環境は，企業の情報システムとして期待されているが，セキュリティの面で課題が残されている。通常，クラウド環境はネットワーク経由で利用されることから，ネットワーク上のデータ転送の面でもセキュリティを向上させることが必要である。

ネットワーク仮想化技術は，物理ネットワークとは独立した仮想ネットワークを構築し，仮想ネットワークで接続された機器間でセキュアに通信することを可能にする。三菱電機では，要求が発生した場合に動的にオーバーレイネットワーク(オーバーレイVPN(Virtual Private Network))を構築し，VPN内でのみ通信することが可能なオンデマンドグループ通信を実現するネットワーク仮想化技術“分散型仮想ネットワーク”を提案し，研究開発を行ってきた。

今回，“クラウド環境活用に向けた企業内既存システムとの連携実証実験”で，分散型仮想ネットワークをネットワーク仮想化技術に適用し，クラウド環境におけるネットワーク仮想化の実証実験を行った。

実証実験においては，企業内システムとプライベートクラウドにまたがるオーバーレイVPNを分散型仮想ネットワークによって構築した。オーバーレイVPNに接続する装置間では，企業内システムとプライベートクラウドの境界を越えて仮想ネットワーク上の通信が行える一方で，オーバーレイVPNに接続しない装置間では仮想ネットワーク通信を行うことができず，仮想ネットワークによって論理的にネットワークが分割されていることを確認した。



ネットワーク仮想化実証実験の論理接続図

クラウド環境活用に向けた企業内既存システムとの連携実証実験で，分散型仮想ネットワークによって企業内システムのService Mixとプライベートクラウドの Service Mix各1台について，企業内システムとプライベートクラウドにまたがるオーバーレイVPNを構築した。オーバーレイVPNを構成するService Mix間でのみ仮想ネットワーク上の通信が可能である。

*情報技術総合研究所 **同研究所(情報学博士)

1. まえがき

ネットワーク仮想化技術は，ネットワーク的に同じものを分割し，またネットワーク的に異なるものを結合して仮想のネットワークを構成し，仮想ネットワークで接続された資源をセキュアに利用することを可能にする。

近年台頭してきたクラウドコンピューティング環境(以下“クラウド環境”という。)は企業情報システムとして期待される一方で，セキュリティ上の課題があることからその利用が拡大していないのが現況である。クラウド環境はネットワークによって接続されたコンピュータ資源を利用者がその空間的配置などを意識せずに利用するシステムであり，クラウド環境の利用はネットワーク経由であることから，ネットワーク仮想化の適用によってクラウド環境利用におけるセキュリティを向上させることが可能である。

本稿では，クラウド環境活用に向けた企業内既存システムとの連携実証実験で行ったネットワーク仮想化手法の調査と，クラウド環境におけるネットワーク仮想化実証実験について述べる。

2. ネットワーク仮想化手法

ネットワーク仮想化手法は，暗号化等によって情報を秘匿することによって他者との独立を実現する方式と，ネットワークを多層化して他者との独立を実現する方式に分けることができる。情報の秘匿によるネットワーク仮想化技術の多くは，インターネット経由でVPNを構成することを目的としており，代表的な技術としてIPsec(Security Architecture for Internet Protocol)-VPN，SSL(Secure Socket Layer)-VPNなどが挙げられる。一方，ネットワークを多層化する仮想化方式は，専用の伝送／交換機器が必要となることから通信キャリアのネットワークを含めて主には閉域網でVPNを構築する技術であり，代表的な技術としてVLAN(Virtual Local Area Network)，IP-VPN，オーバーレイVPNなどが挙げられる。

当社では，P2P(Peer to Peer)技術に基づいたオーバーレイVPNの技術である分散型仮想ネットワーク[(1)(2)]を提案し研究開発を行ってきた。分散型仮想ネットワークはアプリケーション層で物理的なネットワークと独立した仮想の上位層ネットワーク(オーバーレイネットワーク)を構築するので，閉域網に限らず自由にネットワーク仮想化を実現することが可能である。今回の実証実験では，ネットワーク仮想化手法として分散型仮想ネットワークを適用した。

3. ネットワーク仮想化実証実験

3.1 分散型仮想ネットワーク

分散型仮想ネットワークの目的はオンデマンドグループ通信の実現である。オンデマンドグループ通信は，企業における業務など利用者の行動に応じた特定メンバー間の通信が可能なグループをオンデマンドで構成し，

(1) 関係者外への漏えいのない安全なグループ通信
(2) 時限プロジェクトなど期限付きネットワークのための動的なグループ構成
(3) ユーザーの属性に基づくアクセス制御

を実現する。例えば**図1**に示すように各プロジェクトや拠点に対応するグループを生成して，同一グループに属する端末間でのみ通信することが可能になる。

3.2 分散型仮想ネットワークのパケット転送

多くの端末を収容するスケーラビリティとネットワークの障害に耐え得る信頼性を持たせるため，分散型仮想ネットワークではオーバーレイネットワークの構築と管理に特化した専用装置DVC(Distributed Virtual network Controller)をネットワーク上に分散配置してオーバーレイネットワークを構築する。

図2で各DVCは隣接するDVCとP2P技術によって接続されており，リング状のDVCのネットワークが構成されている。そして各DVCにユーザー端末が接続される。

分散型仮想ネットワークではID情報を用いてユーザー端末間のパケット転送を行う。ID情報は通信グループのIDとユーザーのIDからそのユーザー端末が接続するDVCを検索するためのデータベースである。このデータベースは通信グループIDとユーザーIDのハッシュ計算値を検索キーとして構成されており，DVC間で分散管理される。ハッシュ計算値によるデータベースが分散管理されることから分散ハッシュテーブル(Distributed Hash Table：

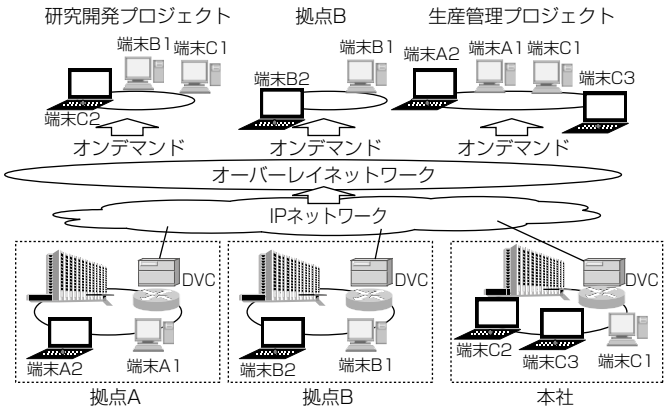


図1．オンデマンドグループ通信

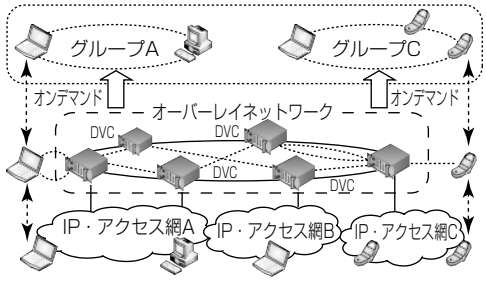


図2．分散型仮想ネットワーク

DHT)[3]と呼ばれる。

図3に示すように，ユーザー間で通信する場合に送信パケットは，

①送信元端末aは，あて先端末bへのパケットを自分の送信元接続DVCであるDVC1に送信

②DVC1からあて先端末bのID情報を管理するDVC2までは，DHT探索によって転送

③DVC2であて先端末bの接続先DVCがDVC3と判定され，DVC3まで転送

④DVC3からあて先端末bに転送

という手順であて先端末まで届けられる。

グループIDとユーザーIDをキーとしたあて先情報管理が行われているので，同一グループに所属しない端末間のパケット転送についてはあて先DVCの検出に失敗する結果となり，同一グループ内に閉じたセキュアな通信が可能となる。

3.3　分散型仮想ネットワークを構成する技術

分散型仮想ネットワークは仮想ネットワーク制御ソフトウェア，仮想ネットワークドライバ，仮想ネットワーク管理ソフトウェアの3種類のソフトウェアによって構成される。**図4**に各ソフトウェアの接続構成を示す。

3.3.1　仮想ネットワーク制御ソフトウェア

仮想ネットワーク制御ソフトウェア(以下“制御ソフトウェア”という。)は，IPネットワーク上にオーバーレイネットワークを構成し，仮想ネットワークを用いた通信機能を実現するためのソフトウェアであり，パケットの中継処理を行うサーバとして設置する。制御ソフトウェアはID情報のデータベースを管理し，ID情報に基づいて端末ごとに通信の可否を判定してパケットのルーティングを行う。制御ソフトウェアが動作する装置がDVCである。

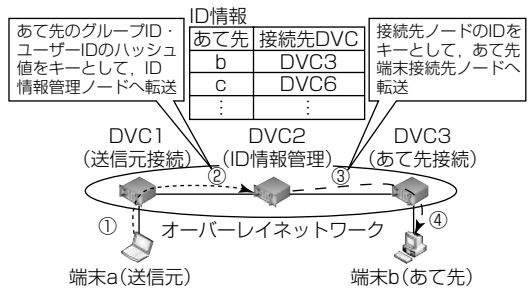


図3．分散型仮想ネットワークのパケット転送

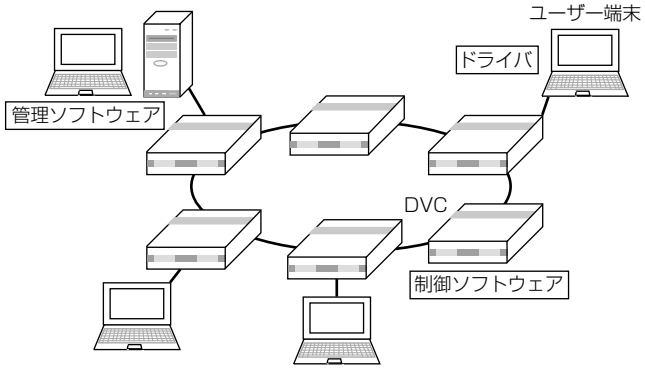


図4．仮想ネットワークソフトウェアの接続構成

3.3.2　仮想ネットワークドライバ

仮想ネットワークドライバ(以下“ドライバ”という。)は，ユーザーアプリケーションから受信したパケットをカプセル化して仮想ネットワークに送出するためのソフトウェアである。仮想ネットワーク通信を行う各端末にインストールして用いる。ドライバはホストの内部に仮想的なネットワークインタフェース(NIC)を生成するので，ユーザーアプリケーションに手を加える必要はなく，インタフェースを変更するだけで仮想ネットワークを使用することができる。

3.3.3　仮想ネットワーク管理ソフトウェア

仮想ネットワーク管理ソフトウェア(以下“管理ソフトウェア”という。)は，制御ソフトウェアとドライバによって構成される仮想ネットワークの接続状態の収集と可視化をするソフトウェアである。管理ソフトウェアが収集した情報はウェブブラウザを用いて画面表示することができる。

3.4　実証実験構成

図5に実証実験の仮想ネットワーク構成を示す。物理ネットワーク上では，企業内システム内，プライベートクラウド内の各装置はレイヤ2スイッチ(L2SW)によって相互に接続されている。また，企業内システムとプライベートクラウドはレイヤ3スイッチ(L3SW)で接続されている。物理ネットワーク上ではすべての装置が接続された状態であり，通信可能なネットワークとなっている。

DVCは企業内システムにDVC1，プライベートネットワークにDVC2が配置されている。VN(Virtual Network)管理は管理ソフトウェアが動作する仮想ネットワーク管理である。

ネットワークの仮想化は図中のService Mixに適用した。Service Mixはオープンソースの ESBである。ここではService Mixが動作する装置をService Mixと呼んでいる。

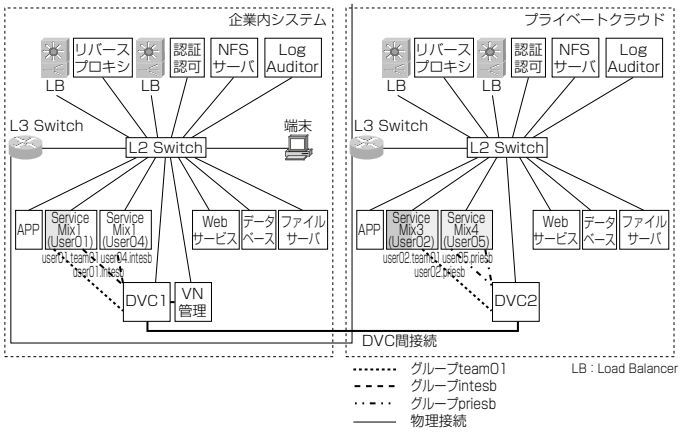


図5．実証実験の仮想ネットワーク構成

企業内システムのService Mix1(S.M.1)とService Mix2(S.M.2)が参加するグループintesb，プライベートクラウドのService Mix3(S.M.3)とService Mix4(S.M.4)が参加するグループpriesb，企業内システムとプライベートクラウドにまたがったS.M.1とS.M.3が参加するグループteam01の3個のオーバーレイネットワークを構成している。各Service Mixには所属するグループに対応する仮想ネットワーク用の名前が与えられる。2個のグループに所属するS.M.1とS.M.3は各グループに対応した2個の名前を持っており，通信するグループに応じて使い分けられる。

3.5 実証実験結果

実証実験ではアプリケーションとしてpingを使用し，企業内システムのService Mixからプライベートクラウドの Service Mixをpingによってサーチすることによって，ネットワーク仮想化の効果について確認を行った。企業内システムのS.M.1からプライベートクラウドのS.M.3に対して実行したグループteam01を使用したpingでは，両S.M.ともグループteam01に所属しており，仮想ネットワーク上をパケットが転送され，pingのReplyがS.M.1に到着することが確認できた。一方，S.M.1からプライベートクラウドのS.M.4に対して実行したpingでは，グループteam01，グループpriesbのいずれのグループを使用した場合にもpingの応答は返らず，仮想ネットワークによって両S.M.が遮断されていることが確認できた。また，企業内システムのS.M.2からプライベートクラウドのS.M.3／S.M.4に対して実行したpingについても応答は返らず遮断されていることが確認できた。

クラウド環境ではネットワークで接続されたコンピュータ資源が多数の利用者によって使用されるため，関係しない装置間を遮断することは不正行為の防止などセキュリティの向上において効果的である。また，クラウド環境は仮想マシンによって構成されることも多く，ネットワーク仮想化による論理的な遮断はクラウド環境におけるセキュリティ向上に効果的であると考えられる。

4. むすび

今回の実証実験では，プライベートクラウド環境を併用する企業ネットワークで，ネットワーク仮想化の実験を行った。具体的には仮想ネットワーク制御ソフトウェア(制御ソフトウェア)と仮想ネットワーク管理ソフトウェア(管理ソフトウェア)を使用して，企業システムとプライベートクラウド間の通信路を論理的に分割できることを確認した。

実験結果から，制御ソフトウェアによってあらかじめ許可された組合せの装置(Service Mix)間だけが通信可能で，他の組合せでは通信不可能となるように制御できていることを確認できた。また，管理ソフトウェアによって通信可否の組合せ(アクセスリスト)の集中管理と，組合せに基づく通信制御を可視化できることを確認した。

この実験の構成はネットワーク仮想化機能を確認するための最小限の構成となっており，実際のネットワーク構成を考慮してクラウド環境への本格的な展開を図るためには更なる機能拡張が必要である。本稿の締めくくりとして，今後の検討課題となる主要な拡張機能について述べる。

(1) 様々な機器，接続環境への対応

ロードバランサやVLANなどの導入によって，機器構成とネットワーク構成の対応が複雑化している現実のネットワーク環境下でも，ネットワーク仮想化機能を利用できるようにする。

(2) 管理機能の高度化

物理層，仮想層の両方を統合的に管理するネットワークリソースマネジメントを実現するため，管理ソフトウェアの機能を拡張し，物理層のネットワーク構成管理や経路制御も統合的に行えるようにする。

(3) セキュリティ

今回の実証実験では各ホストに専用ソフトウェアを載せて通信することが前提であり，ホストの設定に頼ることがセキュリティ上の弱点となり得る。例えば仮想ネットワークインタフェースをプロキシサーバやルータのような外部の通信機器に集約し，ホストからの通信を強制的に仮想ネットワークへ通すような構成が考えられる。

なお，この研究開発は，経済産業省平成21年度“新世代情報セキュリティ研究開発事業(4)”によって実施したものである。

参考文献

(1) 平井　肇，ほか：分散型仮想ネットワークにおける転送効率化方式の検討と試作機開発，電子情報通信学会技術研究報告，**107**，No.525，265～270（2008）
(2) 斉藤泰孝，ほか：分散型仮想ネットワークの基本コンセプト，電子情報通信学会2007年総合大会講演論文集，No.B-7-55（2007）
(3) Stoica，I.，et al.：Chord： A Scalable Peer-to-peer Lookup Service for Internet Applications，SIGCOMM Computer Communication Review，**31**，149～160（2001）
(4) 経済産業省：平成21年度“新世代情報セキュリティ研究開発事業(クラウドコンピューティングセキュリティ技術研究開発)”公募仕様書（2009）