三菱電機技報 85巻8号(通巻963号)

ISSN 0369-2302 CODEN:MTDNAF

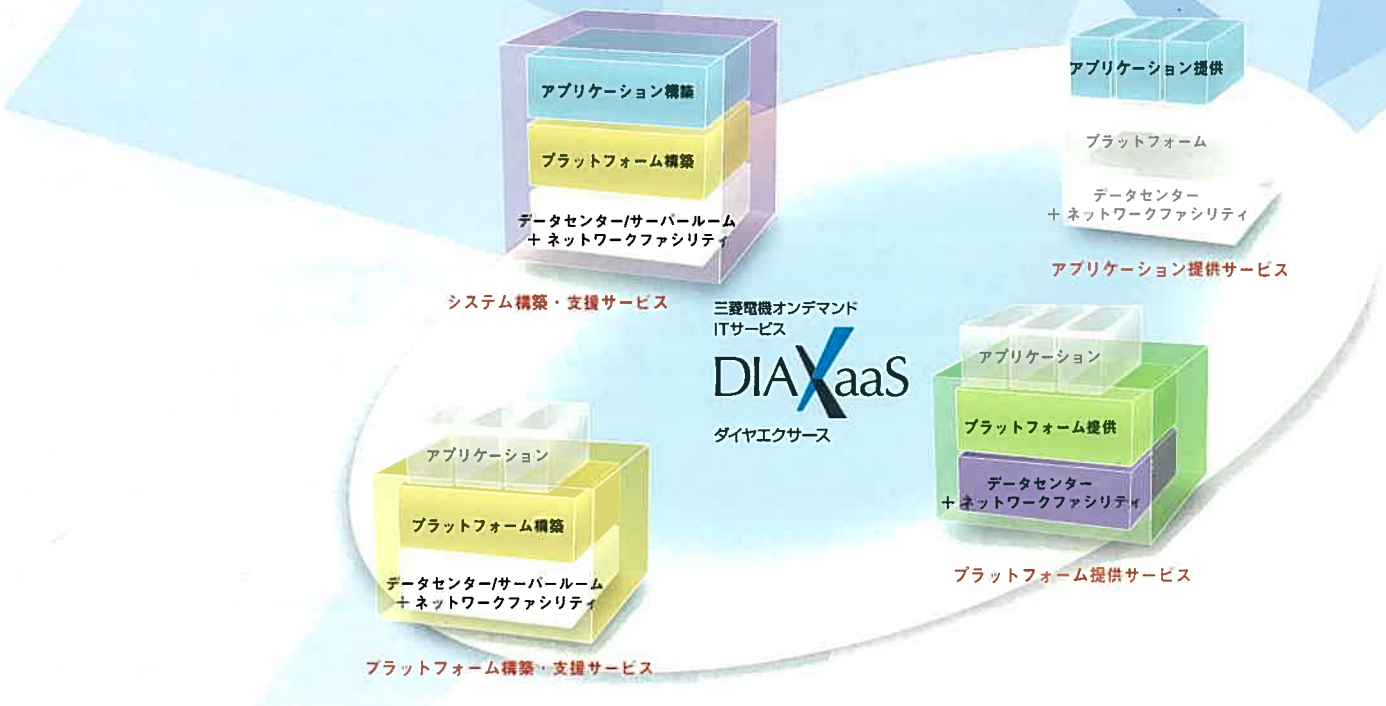
MITSUBISHI
Changes for the Better

家庭から宇宙まで、エコチェンジ

三菱電機技報

8
2011
Vol.85 No.8

特集「企業の発展を支えるオンデマンドITサービス“DIAXaaS”」



三菱電機技報 Vol. 85 No.8 2011

目　次

表紙：企業の発展を支えるオンデマンドITサービス“DIAXaaS”

三菱電機では，クラウド時代のITサービスとして，オンデマンドITサービス“DIAXaaS(ダイヤエクサース)”を提供している。

DIAXaaSは，セキュリティや信頼性の面で，企業ユーザーが求める高いレベルのサービスを実現しており，企業の情報システムを支えるとともに企業の発展に貢献していく。

表紙では，DIAXaaSのロゴマークを中央に配置し，その周辺に4つの代表的なサービスメニューを示した。

巻/頭/言

クラウドを支える技術の重要性

Why Technologies are Vital to Cloud Computing

前川　徹
Toru Maegawa

クラウド・コンピューティング(以下“クラウド”という。)が情報処理のパラダイムを変えようとしている。おそらくこれに異を唱える人はほとんどいないだろう。しかし，クラウドを支える技術の重要性については意見が分かれる。ITのコモディティ化の進展によって，技術はもはや重要ではないという専門家がいる。例えば，次のような主張である。

ハードウェアは完全にコモディティ化しており，数万円で十分パワーのあるIAサーバを手に入れることができる。必要があれば，低コストでハードディスクやメモリを増強することも可能だ。こうしたマシンを何台か調達し，この上にLinux(注1)とXen(注2)をインストールすれば仮想化環境が整う。さらにEucalyptus(注3)やHadoopなどを必要に応じて組み込めばクラウド環境を構築できる。こうして個人でも簡単かつ安価にクラウド環境を構築できるのだから，IT系企業であればどこの企業でも，より大規模で高性能なクラウド環境を容易に構築できるだろう。したがって，クラウドはもはや技術の問題ではない。

この主張は正しいのだろうか。たしかに，個人でもある程度の知識とスキルがあれば，それなりのクラウド環境を構築することはできるし，企業であればより大規模なクラウド環境を構築できる。しかし，こうしたクラウド環境を企業向けのサービスの基盤として提供できるのか，あるいは，ビジネスとして利益を生み出す事業にすることができるのかとなると，これは別の問題である。

企業ユーザーがクラウドを利用するにあたって，最も懸念する問題は，クラウドの情報セキュリティと信頼性である。ネットのあちら側にあるデータは安全なのか，なりすましや不正アクセス，盗聴による漏えいや改竄(かいざん)のおそれはないのか，サーバやネットワークの不具合によってサービスが中断されるのではないか等々。

クラウドに蓄積する情報の種類や重要性によって，あるいはクラウド上で処理する業務によって，求められる情報セキュリティや信頼性のレベルは異なるだろうが，個人が簡単かつ容易に構築できるクラウド環境では，こうした企業のニーズを満たすことは難しいだろう。高度な情報セキュリティ技術と情報システムの運用技術がなければ，企業ユーザーが要求するセキュリティと信頼性は実現できない。

もう１つは，数多くの企業が参入しつつあるクラウド市場で，競争優位を獲得できるのかという問題である。他社のサービスにはない特長や機能・性能を備えたクラウドを構築するという戦略をとる場合でも，他社よりコスト・パフォーマンスに優れたサービスを提供するという戦略をとる場合でも，それを支える重要な要素は技術である。

例えば，ユーザーからみたクラウドの最大の魅力は，情報システムの調達，開発，運用に必要なコストが，オンプレミスの情報システムと比べて極めて安価なことにある。この低コスト実現のキーワードが“規模の経済”(注4)であり，それを生み出しているのも技術である。

無償で利用できるOSSで実現できる仮想化も規模の経済を実現する一要素であるが，それだけではまったく不十分である。例えばSaaS(Software as a Service)の場合，１つのインスタンスで複数のユーザーにサービスを提供できるマルチテナント方式の採用が規模の経済を生み出す。ユーザーごとに異なったインスタンスを割り当てるシングルテナント方式に比べて，マルチテナント方式の方が保守運用コストは圧倒的に小さい。ソースコードを修正することなくカスタマイズできる仕組みがあれば，管理するソースコードは１つで済み，保守管理が圧倒的に容易になる。これも高度な技術がなければ実現できない。

クラウドではデータセンターを効率よく管理運用する必要がある。大量のコンピューティング・リソースを集中管理することによって，サーバ１台あたりの運用管理コストを下げることができるが，これも優れた自動管理システムがなければ実現できない。最先端の巨大なデータセンターでは一人で数千台のサーバを管理しているが，単にサーバやネットワークの障害を監視するだけではなく，障害の未然防止，自動復旧やリソースの最適管理を行う技術がなければ，これは実現できない。

以上のように，企業向けクラウドでは，高いセキュリティと信頼性，効率のよい運用管理を実現するために高度な技術が不可欠であり，今後一層の技術発展を期待したい。

(注１)　Linuxは，Linus Torvalds氏の登録商標である。
(注２)　Xenは，Citrix Systems, Inc. の登録商標である。
(注３)　Eucalyptusは，Eucalyptus System, Inc. の登録商標である。
(注４)　生産量や販売量の増加に伴って平均費用が低下し，その結果として利益率が高まること。規模に関する費用逓減(収穫逓増)とも言う。

◆サイバー大学 IT総合学部　教授
Professor, Faculty of Information Technology and Business, Cyber University

特集論文

オンデマンドITサービス“DIAXaaS（ダイヤエクサース）”のセキュリティ技術

小湊　晃*　米田　健†
酒井康行**
樋口　毅***

On-demand IT Service "DIAXaaS" and its Security Technology

Akira Kominato, Yasuyuki Sakai, Tsuyoshi Higuchi, Takeshi Yoneda

要　旨

三菱電機では，クラウド時代のサービスを“オンデマンドITサービス”と位置づけて，2010年7月，“DIAXaaS（ダイヤエクサース）”を発表した(2)。DIAXaaSは，企業情報システムにおけるサービス利用に向けて，企業ユーザーが求める高いレベル（セキュリティ，信頼性）のサービスを提供しており，次の特長を持つ。

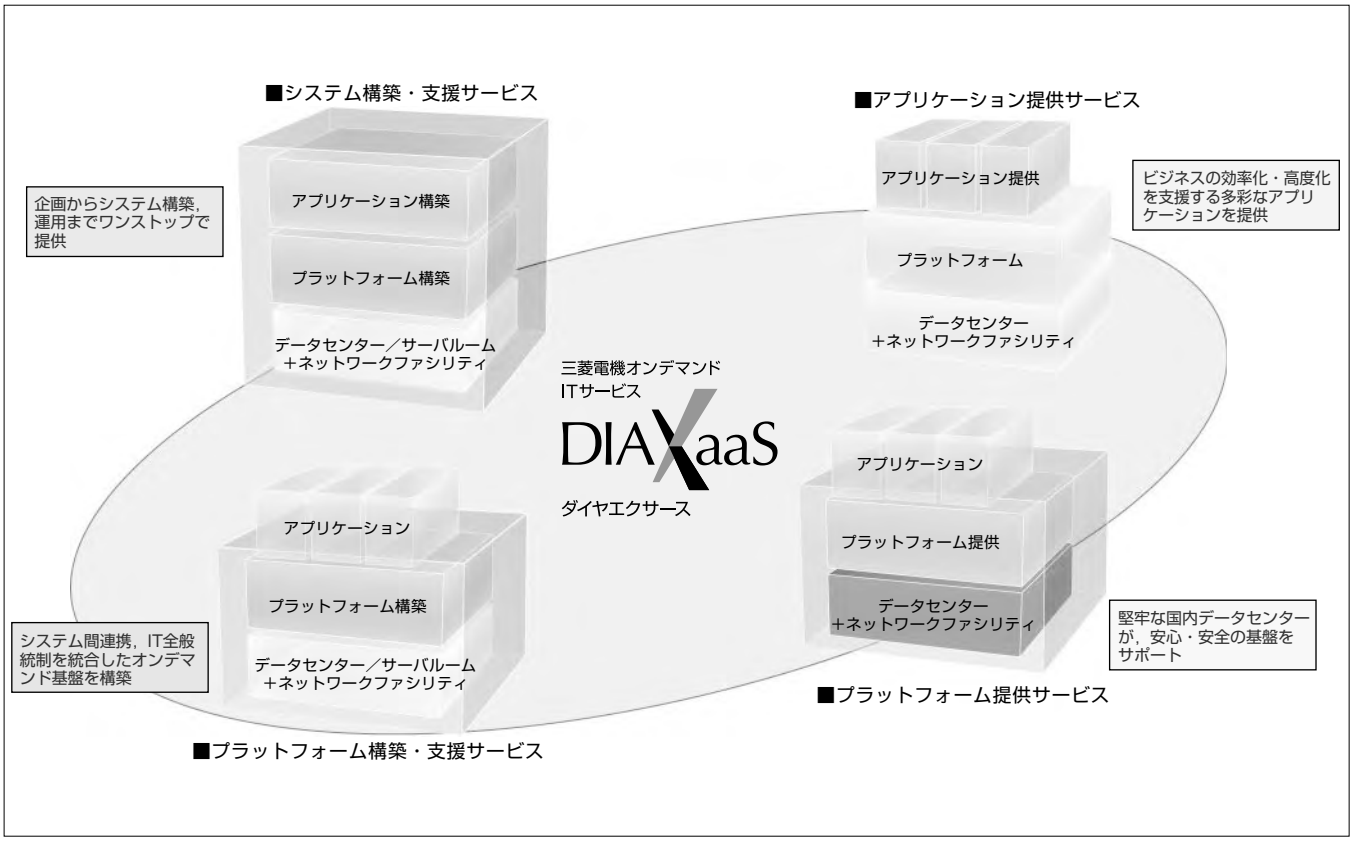
(1)　総務省医療情報向けガイドラインに準拠した高いセキュリティ管理レベル

(2)　データセンターの高信頼基盤と運用管理技術

本稿では，セキュリティを中心としたクラウド技術への取組みについて述べる。DIAXaaSでは，当社がサービス提供する基盤上でセキュリティを確保するためのネットワークセキュリティ，改ざん防止のためのデータセキュリティ，認証認可技術等に取り組んでいる。特に認証認可技術については，IDマッピングや認証連携等のクラウドに適応した様々な機能を実現した基盤を構築しており，詳細について述べる。

さらに，セキュアで利便性が良いサービスを提供するための研究成果として，“IDマッピング自動登録方式”“新世代暗号方式”について述べる。

最後に，セキュリティ技術と関連する“データセンターの高信頼基盤”“セルフサービスポータルによる運用管理”について述べる。



三菱電機オンデマンドITサービス“DIAXaaS（ダイヤエクサース）”のサービスメニュー

DIAXaaSは，三菱電機グループが提供するオンデマンドITサービスの統合ブランドで，企業に求められるセキュリティと信頼性の高いサービスを，アプリケーション，プラットフォームから，構築・支援まで，4つのサービスメニューに分けて提供する。その中でプラットフォーム提供サービスは，高速で信頼性の高いインターネット環境を提供する三菱電機情報ネットワーク㈱（MIND）のデータセンターとネットワーク上に構築している。

*インフォメーションシステム事業推進本部　**情報技術総合研究所（博士（工学））　***同研究所　†インフォメーションシステム事業推進本部（工博）

1. まえがき

企業がクラウドコンピューティング(以下“クラウド”という。)技術を活用して，データを企業内や企業グループで一元管理したり，外部事業者に預けたりする時代が到来している。一方，情報の機密性確保や災害時などにおける事業継続性に関する社会的重要性が高まっており，データの保管や種々のITサービスを利用する際に，セキュリティと信頼性の確保がますます重要となっている。

当社では，ITのサービス化に伴うセキュリティと信頼性の課題を解決するため，クラウド技術基盤の強化に積極的に取り組んでいる。

本稿では，三菱電機オンデマンドITサービスDIAXaaSにおけるセキュリティを中心とした取組みについて述べる。

2. DIAXaaSのサービス

当社では，クラウド市場に向けて，政府の実証事業・実証実験で実績を積み重ねた暗号・認証技術，及びMINDが運営する高信頼データセンターを活用したクラウド技術基盤を組み合わせ，クラウド時代のサービスを“オンデマンドITサービス”と位置づけて，2010年7月，DIAXaaS(ダイヤエクサース)を発表し，販売を開始した。提供サービスを**表1**に示す。

3. セキュリティに対する取組み

この章では，クラウド化に伴うセキュリティの脅威と安全なサービスを提供するための取組みについて述べる。またDIAXaaSのセキュリティ技術と認証認可基盤について述べる。

3.1 セキュリティの脅威

企業と外部事業者がネットワークで接続された環境で，外部からのアクセスに関する3大脅威が“盗聴”“改ざん”“なりすまし”である。

表1．DIAXaaSのサービス一覧

サービス名	提供会社
アプリケーション提供サービス	
FAXOCRサービス　MELFOS on Demand	MDIS
SaaS型Webセキュリティ診断サービス　WebMinder on Demand	MIND
オンデマンド電子署名サービス　@Sign on Demand	ジャパンネット㈱
SaaS型環境情報共有サービス　ECOrates on Demand	MIND
SaaS型電子帳票配信サービス　帳票Express on Demand	MIND
プラットフォーム提供サービス	
IaaS型プラットフォームサービス　Value Platform on Demand	MIND
システム構築・支援サービス	
ITサービスインテグレーション　BizFLEX	MDIS
プラットフォーム構築・支援サービス	
オンデマンド基盤構築ソリューション　Fine Platform Solutions	MDIT

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

(1) 盗聴
ネットワークを盗聴し，データを不正に取得する。

(2) 改ざん
他人や自分のデータを後から不正に変更する。

(3) なりすまし
他人の権限で操作を不正に行う。

3.2 セキュリティ対策

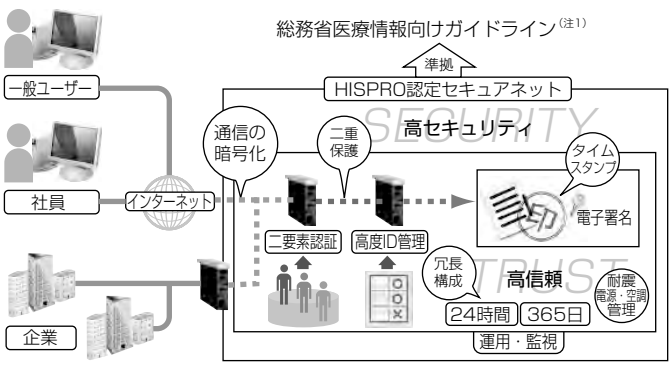
3.1節で述べた脅威に対して，ASP(Application Service Provider)・SaaS(Software as a Service)事業者が，提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として，ASP・SaaS普及促進協議会より“ASP・SaaSにおける情報セキュリティ対策ガイドライン(2008.4)”(以下“ASP・SaaSガイドライン”という。)が公表されている。一般的なサービス事業者ではガイドラインに準拠したサービスが提供されていくと考えられる。

当社では，さらに，機微な個人情報や企業機密を扱うサービスを提供するため，“ASP・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(2009.7)”(以下“医療ガイドライン”という。)に準拠したセキュリティレベルに対応するため，**3.3節**以降に示すような取組みを行っている(**図1**)。

3.3 DIAXaaSのセキュリティ技術

(1) 盗聴防止のためのネットワークセキュリティ

ASP・SaaSガイドラインでは，通信の暗号化が求められているが，IP(Internet Protocol)通信の暗号化またはHTTP(Hyper Text Transfer Protocol)通信の暗号化のいずれかの対策を実施すればよい。一方，医療ガイドラインでは，IP通信の暗号化など通信レベルの暗号化とHTTP通信の暗号化などコンテンツレベルの暗号化の両方の対策を実施する必要がある。MINDが提供する“セキュアネットワークサービス”は，インターネットVPN(Virtual Private Network)サービスで，暗号通信プロトコルはキャリアやプロバイダに依存することなく，チャネルごとの通信を実現している。また，ジャパンネット㈱の“電子証明書発行



(注1) 総務省が策定したASP・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(2009.7)

図1．DIAXaaSのサービス基盤

サービス”を利用して，SSL(Secure Socket Layer)用の証明書を発行し，HTTP通信の暗号化によるデータの保護を行うことができる。なお，セキュアネットワークサービスは，医療ガイドラインが参照している，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”に準拠していることを一般社団法人保健医療福祉情報安全管理適合性評価協会(HISPRO)によって認定されている。

⑵ 改ざん防止のためのデータセキュリティ

ASP・SaaSガイドラインでは，原本性確保が推奨されているものの，対策は不可欠ではない。一方，医療ガイドラインでは，原本性確保に関して，電子署名による本人認証とタイムスタンプによる時刻認証の両方の対策が求められている。そのために，三菱電機インフォメーションシステムズ㈱(MDIS)では，電子署名とタイムスタンプを実装した製品として“電子署名モジュールMistyGuard<SignedPDF>シリーズ”を提供している。また，ジャパンネット㈱では“CryptoTime 時刻認証サービス”を提供している。

⑶ なりすまし防止のための認証技術・ID管理技術

ASP・SaaSガイドラインでは，利用者のアクセス制御となりすまし対策が求められており，ID／パスワード，ICカードなどが認証方式として示されている。一方，医療ガイドラインでは，ID／パスワード+ICカード，ID／パスワード+生体認証のような二要素認証が求められている。当社は，厚生労働省の“社会保障カード(仮称)の制度設計に向けた検討のための実証事業”に参加し，ID／パスワード+ICカードによる二要素認証を実現している。また，ID情報として，資格の情報を付与し，資格に応じて操作・閲覧先を限定する仕組みを実現した。

⑷ マルチテナント環境でのセキュリティ基盤の取組み

DIAXaaSでは先に述べた3つの取組みに加え，マルチテナント環境で，ほかの利用者による盗聴やアクセス侵害等を防止する取組みを行っている。具体例としては，マルチテナント環境で，盗聴防止のためにファイアウォールから仮想マシンまでのネットワークを論理的に分離し専用ネットワーク化する対策や，仮想環境のセキュリティ設定に関するガイドラインの作成，及びガイドラインに則した設定自動化ツール・監査ツールの活用による対策を行っている。

3.4 クラウドに適した認証認可基盤

今後，サービス利用の流れが進むと，ユーザーを適切に認証し，許可されたユーザーだけがSaaSにアクセスできる仕組みがますます重要となる。当社では，クラウドに適応する次のような機能を持つ“認証認可基盤”を開発し，DIAXaaSのサービス基盤に適用するとともに，企業向けにソリューションとして提供している。

⑴ 複数SaaS間に跨(またが)るシングルサインオン機能

ユーザーが複数のSaaSを利用する場合，SaaSごとに異なるユーザーID(以下“ID”という。)／パスワードの入力が必要になり，操作が煩雑な上，推測可能なパスワードが使われる可能性が高まる。そこでDIAXaaSのサービス基盤上で提供するSaaSで一度正しいID／パスワードを入力すると，その認証状態を保持し，別のSaaSへアクセスする際にID／パスワードの入力が不要となるリバースプロキシ型のシングルサインオン(SSO)機能を実現した。また，企業内の既存システムと異なるドメインでサービス提供するSaaS間で，SAML (Security Assertion Markup Language)連携機能を用いたSSO機能を実現しており，経済産業省の“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”で実証済みである。

⑵ パスワード認証とPKI認証

SSOは，SaaSへのアクセス制御の要(かなめ)となるため，強力な認証方式のサポートが求められる。パスワード認証に加え，ICカードの電子署名機能を用いるPKI(Public Key Infrastructure)認証をサポートした。サービスを利用する一般ユーザーはパスワード認証，ユーザー企業の管理者はPKI認証というように，複数の認証レベルをサポートした。

⑶ 従来のIDの継続利用機能

既存のシステムを新たにSaaSとして提供する場合，既にID体系が決定しており，また利用する企業側でも既にID体系が決定している。互いに異なる企業内のID，SaaSのIDをそのまま管理，利用するために，IDの読替えをして認証するIDマッピング機能を実現した。

⑷ ユーザーの役割に応じたSaaSアクセス制御

資格や職位等の役割に応じて，SaaSへのアクセスを管理，制御する仕組みを実現した。ユーザーの認証成功後，その役割によって利用可能なSaaSにのみアクセスできる。

⑸ SaaSに対するユーザー属性情報の提供制御

さらに個々のSaaSでは，ユーザー属性にもとづくSaaS固有のアクセス制御を設ける必要がある。このアクセス制御を実現するため，認証認可基盤からSaaSに提供するユーザー属性情報をSaaSごとに定義できる仕組みを実現した。

図2に認証認可基盤の医療分野での利用例を示す。ある医師が大学の医局と病院の双方に所属している場合でも，1つのユーザーIDと1つのICカードによって，それぞれの所属先が契約するSaaSに認証認可基盤を通してアクセスできることを表している。また，認証認可基盤からSaaSへは契約IDや資格等の属性の情報が送信されるため，SaaSではその属性に対応した権限によるアクセス制御を実現できる。

3.5 今後のセキュリティ技術への取組み

今後，複数のクラウド事業者の同時利用・連携・移植・移行が頻繁に行われるようになると，IDやデータについて，運用管理の複雑化や，受渡しの際のセキュリティの維

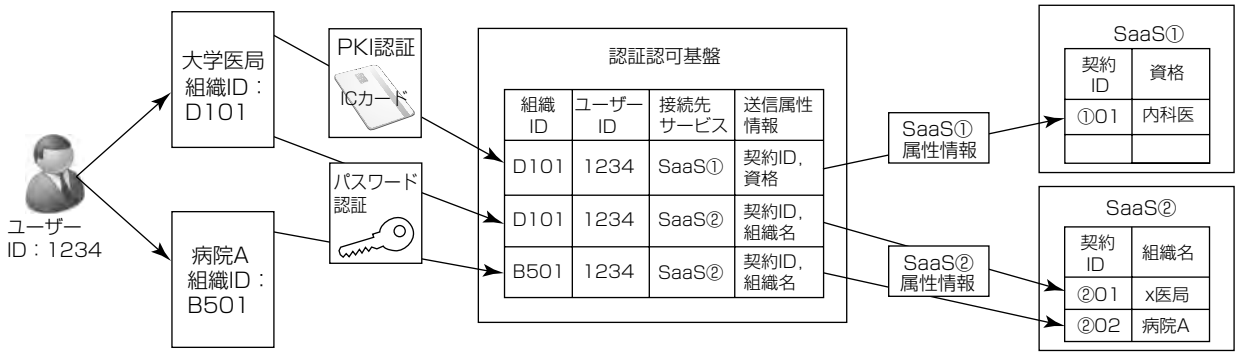


図2．認証認可基盤の利用例

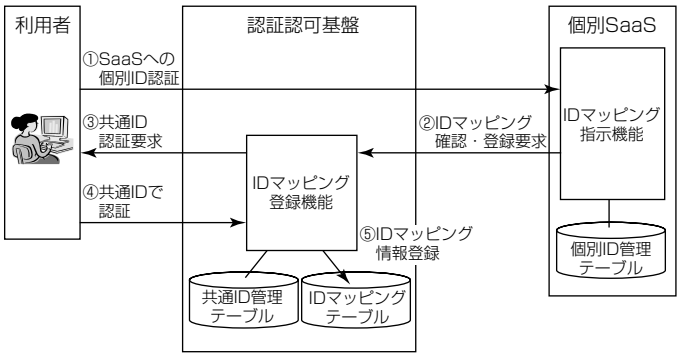


図3．IDマッピング自動登録方式

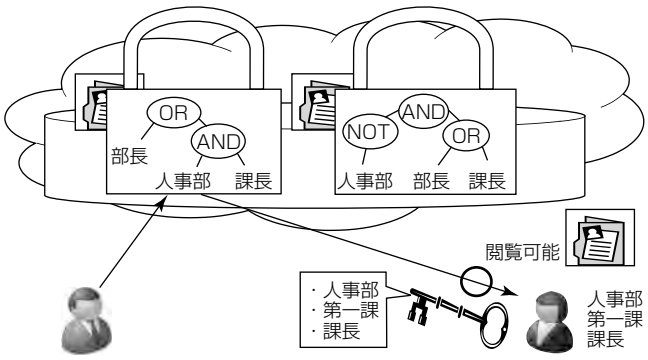


図4．新世代暗号方式の利用例

持が課題となる。当社では，これらの課題を解決するためのクラウド関連技術の研究開発に取り組んでいるが，ここでは“IDマッピング自動登録方式”“新世代暗号方式”について述べる。

3. 5. 1　IDマッピング自動登録方式

3. 4節で述べたように，SSO環境で，サービスごとに異なるIDを維持したまま，共通IDで利用可能とするための技術としてIDマッピングがある。

今後，外部サービスの活用が進むと，組織や社員のユーザーID情報の管理が複雑化し，登録作業の負荷増大，管理者による登録ミスや漏洩(ろうえい)への対策が課題となる。

図3に，認証認可基盤でIDマッピングテーブルを自動的に登録する方式を示す[3]。利用者は，最初の段階ではIDマッピングテーブルが生成されていないので，SaaSへの個別ID認証を行う。その後，共通IDでの認証要求が行われ，SaaS側の“IDマッピング指示機能”と認証認可基盤の“IDマッピング登録機能”が連携して，IDマッピングテーブル登録を自動化できる。その後の操作では，利用者は，共通ID又は個別IDによる1回の認証だけで良い。

この方式の実現によって，複数のSaaSに関するIDマッピングテーブルの登録が自動化できるため，管理者による登録作業負荷の削減，及び登録ミスの抑止，なりすましや改ざん等の不正を防止できる。また，個別のSaaSにはIDマッピング情報を持たないため，個別SaaSが外部からのアタックを受けても共通IDの漏洩を防ぐ効果もある。膨大なID情報を管理する企業や公的機関への適用が考えられる。

3. 5. 2　新世代暗号方式

クラウドへ機密性の高いデータを預けることで，セキュリティ対策が複雑化することが課題となっていくが，データを暗号化したまま交換することができるようになれば，セキュリティ対策の格段の効率化が図れる。

日本電信電話㈱と当社は，共同で“クラウド時代の高度なセキュリティ対策を実現する新世代暗号方式”を開発し，2010年7月に発表した[4]。この暗号方式は，暗号－復号のメカニズムの中に高度なロジック(論理)を組み込むことが可能であり，暗号機能によってきめ細かいデータ送受信制御を実現できることを特長としている。データごとにきめ細かくアクセス条件(開示範囲)が設定された暗号データをクラウド上で管理して，そこで設定されたアクセス条件を満足する属性情報をもつ利用者のみがそのデータを復号・閲覧できるような機能を提供できる。企業における機密情報管理システムや公的機関による個人情報データベース管理などへの応用が考えられる。

図4に企業における機密情報管理システムでの新世代暗号方式の利用例を示す。図中左側の文書では，“部長または人事部の課長のみが閲覧可能”という条件式が文書とともに暗号化されてクラウド上で管理されており，その条件式を満足する人事部第一課の課長が，その属性情報に応じた自分の復号鍵を用いて，クラウド上にある暗号化機密情報を入手，復号して閲覧可能となる状況を表している。

4. 高信頼基盤と運用管理技術への取組み

当社では，様々なクラウド技術への取組みを実施しているが，この章では，セキュリティ技術との関連性が高い“データセンターの高信頼基盤”“セルフサービスポータルによる運用管理”について述べる。

4.1 データセンターの高信頼基盤

企業がデータセンターにデータを預ける場合，災害や障害によって，データの紛失やサービスの継続が停止する事態を避けるため，データセンターでは次の対策が必要となる。

⑴ 災害対策，事業継続関連対策

MINDでは，耐震設備や電源・空調管理を備えた，堅牢（けんろう）性・信頼性の高いデータセンターを首都圏の流通拠点に設置，グローバル対応の24時間×365日オンサイト運用保守サービス，広域バックアップサービスなどの災害対策，事業継続関連サービスの提供等の取組みを行っており，“ASP・SaaS・ICT（Information and Communication Technology）アウトソーシングアワード2009”のIDC（Internet Data Center）部門で大規模分野グランプリを受賞している。

⑵ 4段階の物理セキュリティレベル管理

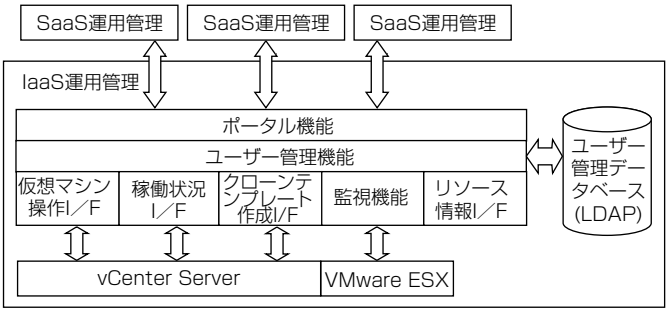
データセンターの物理セキュリティレベルを，ビル入館，ロビー，マシン前室，サーバ室の4段階に分けた物理セキュリティ管理を行っている。最もセキュリティレベルが高いサーバ室では，生体認証，サークルゲートを使った共連れ防止等を実現している。これら管理の仕組みは，FISC（金融情報システムセンター）の“金融機関等コンピュータシステムの安全対策基準”に準拠している。

⑶ システムやネットワークの最適化技術

データセンターでは，システムやネットワークの冗長化やバックアップを施している。また，マルチキャリア対応の高信頼ネットワークを有し，サーバの統合化によるトラフィック集中で発生する通信遅延や帯域不足を防ぐため，“ネットワーク帯域制御技術”“WAN（Wide Area Network）高速化技術”“負荷分散技術”で最適化を図っている。

4.2 セルフサービスポータルによる運用管理

今後，各企業がプライベートクラウドの構築・運用や，IaaS（Infrastructure as a Service）事業者の基盤上に複数のSaaSを運用していくようになると，IaaSとSaaSそれぞれの運用管理について，役割の明確化が重要となる。その際，IaaSの運用管理をIaaS事業者に一任すると，SaaS事業者にとってはIaaSの状態が把握できないことが課題となる。そのため，三菱電機インフォメーションテクノロジー㈱（MDIT）では，クラウド環境でも，個別のSaaS単位で，サービス運用管理の仕組みを提供できるよう，“セルフサービスポータル”を開発した（**図5**）。



LDAP：Lightweight Directory Access Protocol

図5．セルフサービスポータル構成図

このポータルは，仮想化ミドルウェアであるVMware社の“vCenter Server”と“VMware(注2) ESX”に対応しており，仮想マシンの作成，起動，停止，監視等を行う。特にマルチテナント環境下では，パフォーマンスの監視が重要になるが，画面インタフェースによって，遠隔からも容易に操作・表示ができるという特長を持つ。

IaaS事業者がSaaS事業者向けに運用管理の仕組みを提供する際にも，このポータルサービスによって，今までの運用管理の仕組みの延長で対応でき，運用管理業務を効率化できる。仕向先としては，データセンター，プライベートクラウド構築事業者，IaaSやSaaSの運営事業者が挙げられる。

（注2） VMwareは，VMware Inc. の登録商標である。

5. むすび

当社グループでは，セキュリティと信頼性の確保を目標とし，高度な技術を適用したクラウド技術基盤を開発した。この基盤をベースに，金融，医療から一般製造業等，様々な業種や分野に向け，IaaSやSaaS等を活用した最適な情報システムを提案・構築していく。また，情報セキュリティ技術や運用管理技術等の更なる強化，DIAXaaSサービスメニューの拡充を行い，安心・安全なオンデマンドITサービスを提供していく所存である。

参考文献

⑴ 伏見信也，ほか：クラウド技術を適用した企業情報システムへの取組み，三菱電機技報，**84**，№7，370～374（2010）

⑵ 三菱電機ニュースリリース：三菱電機オンデマンドITサービス「DIAXaaS」提供のお知らせ，7/21（2010）

⑶ 牧　和宏，ほか：IDマッピング情報の登録方式に関する一考察，情報処理学会第73回全国大会，4E-2（2011）

⑷ 日本電信電話㈱，三菱電機㈱：クラウド時代の高度なセキュリティ対策を実現する新世代暗号方式を開発，三菱電機ニュースリリース（報道発表資料），7/28（2010）

特集論文

IaaS型プラットフォームサービスによる仮想環境のための構築プロセスと実現方法

江見雅仁*
樋口　毅**

Process and Methods for Building Virtual IT Environment Based on IaaS Platform Service

Masahito Emi, Tsuyoshi Higuchi

要　旨

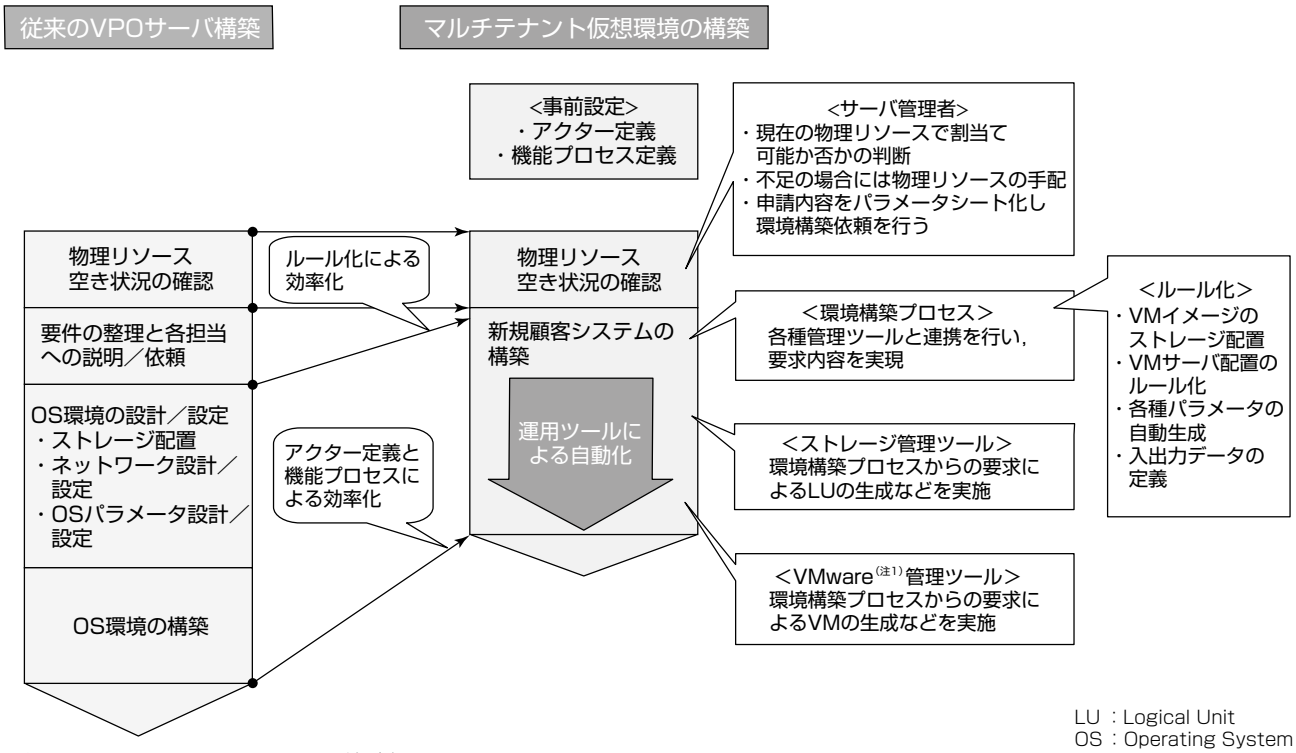
三菱電機情報ネットワーク㈱(MIND)は，オンデマンドITサービス“DIAXaaS”のサービスとして，2010年9月にIaaS(Infrastucture as a Service)型プラットフォームサービス“Value Platform on demand(VPO)”の販売を開始した。

VPOは，物理サーバと共用設備を組み合わせたサービスで，いままでのサーバホスティング要件で顧客別に提供していたエリアやラック，電源，保守メンテナンス，資産管理等の管理の煩雑さや専有化による割高感を解消し，ICT(Information and Communication Technology)資源の“所有から利用”への流れに沿ったサービスとした。

現在，VPOの新サービスとして，物理サーバ1台に対して複数の顧客が利用する“マルチテナント”化した仮想環境の提供を予定している。そのため，マルチテナント仮想環境の短納期提供の実現を目指し，今までの環境構築手順とは異なる構築プロセスと実現方法について検討を行い成果を得た。

構築プロセス機能を明確化／フロー化したこととルール化された構築方式よる手順の標準化が特長である。

今後は，運用自動化ツールを活用し，仮想環境の構築自動化を進めて，この検討結果を実サービスに適用する。



従来方式と比較したマルチテナント仮想環境構築の効率化イメージ

マルチテナント環境の構築は，事前に役割の明確化(アクター定義)や作業内容の明確化(機能プロセス定義)を行い，運用ツールによる自動化で短納期を実現する。

*三菱電機情報ネットワーク㈱　**三菱電機㈱ 情報技術総合研究所

1. まえがき

MINDでは，VPOを2010年9月に立ち上げた。

今回，物理サーバをマルチテナント化した仮想環境を提供するにあたり，一般的な仮想環境提供の短納期化（申請受付後，翌営業日等）の実現を目指し，従来の物理サーバ提供の構築手順によらない，仮想環境構築時のプロセスや実現方式について検討した。

本稿では，その結果について述べる。

2. 仮想環境構築プロセス

物理サーバをマルチテナント化し，各仮想環境を提供するサービスを実現するに当たり，申込みから提供までを短期間に実施することが重要となる。構築プロセスを機能別に分類し，処理を明確にすることで，仮想環境構築に熟知していない担当者でも短期間での環境構築が可能となる。また，分類・処理の標準化を進めることで，運用ツールによる自動化が容易となる。

構築では，構築プロセスフローならびに，物理リソース配置やパラメータ情報のルール化を行い，構築ノウハウの属人化を低減し標準化を進めた。

2.1 アクター定義

仮想環境を構築するためには，構築作業担当者が環境準備のための物理リソースの状況を確認し，手配有無の判断や手続，運用ツールを使った処理を行う。これらの構築のプロセスを明確にするために，だれが（何が）どのような処理を行うかを定義し，役割分担を明らかにする必要がある。

だれが（何が）どのような処理を行うかを定義したものが，**表1**の“アクター定義”である。アクターとは，構築時に必要な判断，処理をするための人や機能を指している。

2.2 機能プロセス定義

機能プロセス定義とは，仮想環境構築に必要な構築項目を分類し，分類した構築項目を“機能プロセス”として定義することである。定義したプロセスは次の5つである。

①物理リソース空き状況の確認

環境構築や物理リソース追加を実施する前に，物理リソースの空き状況を確認し，必要に応じて物理サーバの追加を行う。

②新規顧客システムの構築

新規顧客からのIaaS環境利用の申請を基に，顧客用の仮想リソース確保並びにVMの生成を実施する。

③既存顧客システムへの仮想リソース追加

既存顧客からの新しいVM利用の申請を基に，既存顧客が使っている仮想リソースの拡張並びにVMの生成を実施する。

④既存顧客システムからの仮想リソース削除

既存顧客からの不要になったVM削除の申請を基に，申請のあったVMの削除並びに仮想リソースの縮小を行う。

⑤既存顧客システムの削除

既存顧客からのIaaS環境利用終了の申請を基に，顧客用のシステムの削除並びに仮想リソースの開放を実施する。

これら5つのプロセスそれぞれの処理要件を明確にし，どのアクターがいつ・どのような処理をするかをフロー化することで，仮想環境構築における分類・処理が標準化される。

①の“物理リソース空き状況の確認”プロセスを例として，各アクターでの処理要件をフロー化して説明したものが**図1**である。

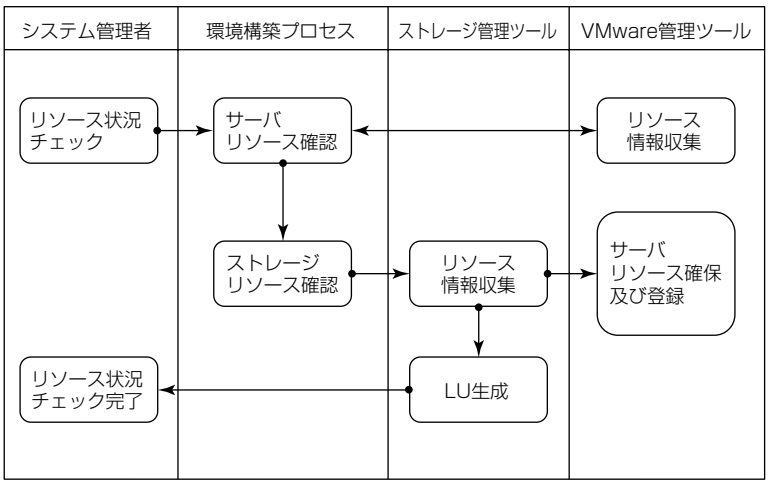


図1．物理リソース空き状況の確認フロー

表1．アクター定義

アクター	説明
顧客	システムの生成や追加を申請
システム管理者	顧客からの申請を受け付け，次を実施 ・現在の物理リソースで割当て可能か否かの判断 ・不足の場合には物理リソースの手配 ・顧客からの申請内容をパラメータシート化し，環境構築依頼を行う
環境構築プロセス	システム管理者からの要求を受け付け，各種管理ツールと連携を行い，要求内容を実現
ストレージ管理ツール	環境構築プロセスからの要求に基づき，LUの生成などを実施
VMware管理ツール	環境構築プロセスからの要求に基づき，VMの生成などを実施

表2は**図1**の各アクターが行う処理要件をまとめたものである。

アクターを5つに分類し，それぞれが行う処理要件を**表2**のように定義することで，前工程の結果内容や指示内容が明確になり，効率的に構築作業を進めることができる。

3. 仮想環境構築方式

仮想環境を短期間で構築するためには，機能プロセス定義で定めた各々の処理内容について，作業担当者が個別に判断していた内容を，だれでも(若しくは自動で)環境構築ができるよう次の項目をルール化する。

・VMイメージのストレージ配置
・VMサーバ配置
・各種パラメータの自動生成
・入出力データの定義

3.1 VMイメージのストレージ配置

新規顧客のシステムを構築する場合，その顧客専用の論理ボリュームを生成するために必要な容量の空きが複数のRAID(Redundant Arrays of Inexpensive Disks)グループに存在した場合，どのRAIDグループに生成するかについては，**表3**のとおり3つの考え方がある。

これまでの物理サーバに対する論理ボリューム割当ての考え方は，最も空き容量が小さいRAIDグループに配置するものであり，仮想環境にストレージを配置する場合でも，ストレージや仮想化ソフトウェアの機能で移行が可能である点を考慮し，最も空き容量が小さいRAIDグループに配置することとする。

3.2 VMサーバ配置

配置対象となる物理サーバは，プライベート型(顧客専用)とシェアード型(マルチテナント)で異なる。

いずれの場合であっても，各仮想マシンに割り当てる物理リソース量(CPUリソース量とメモリリソース量)を基に各物理サーバの空き物理リソースを計算し，最も空き物理リソースがある物理サーバに配置することとする。これは，CPUやメモリ量はオーバーコミット(物理容量を超えて各仮想マシンにリソース量を割り当てる)を実施しないことを前提としているため，いずれの物理サーバに配備してもよいが，負荷を均等化させることで，物理サーバの消費電力を抑える効果が得られるためである。

消費電力を重視した場合，物理サーバごとに仮想リソースを最大限割り当て，使用しない物理サーバを作り出して，電源をオフにすることも可能であるが，現時点では，電源

表2．確認フロー(図1)におけるアクターの処理

アクター	処理内容
顧客	内部で物理リソースを確保するための処理であるため，該当なし
システム管理者	①物理リソース状況の確認 顧客の申請(新規構築，VM追加)に必要となる物理リソースが確保可能か否かを確認する。 ②物理サーバの手配／追加 不足している物理リソース分を確保できるだけの物理サーバを手配／追加登録する。 ③ストレージの手配／追加 不足している物理リソース分を確保できるだけのストレージを手配／追加する。
環境構築プロセス	①物理サーバ上仮想リソースの確認 現在の空き仮想リソースと要求仮想リソース量を比較する。 ②ストレージ仮想リソースの確認 現在の空き仮想リソースと要求仮想リソース量を比較する。
ストレージ管理ツール	①ストレージの空きの確認 現在の空き仮想リソースと要求仮想リソース量を比較する。 ②LU拡張／LU生成 LU拡張，あるいはLU生成を実施する。
VMware管理ツール	①仮想リソースの空きの確認 現在の空き仮想リソースと要求仮想リソース量を比較する。 ②物理リソースの確保／登録 登録追加された物理サーバを確保／登録する。

表3．ストレージ配置の考え方

考え方	利点	欠点
最も空き容量が小さいRAIDグループに配置	将来，大きな空き容量を必要とした顧客のシステムを構築する際，まとまった領域を提供する事が可能である。	ディスクへのアクセス頻度の偏り(使用されているRAIDグループとされていないRAIDグループの偏り)が大きくなるため，物理リソースに余裕のある段階からアクセス集中による性能劣化が発生する可能性がある。
最も空き容量が大きいRAIDグループに配置	ディスクへのアクセス頻度の偏りの可能性が小さくなる。	細かい空き容量を持ったRAIDグループが存在する可能性が出てくるため，大きな容量を必要とした顧客のシステムを複数のRAIDグループにまたがった論理ボリュームを提供する形態になる可能性があり，管理が複雑になる可能性がある。
最もアクセス頻度が小さいRAIDグループに配置	ディスクへのアクセス頻度の偏りの可能性が小さくなる。	利用領域は少ないが，アクセス頻度が高い顧客が存在した場合，必ずしもアクセス頻度の均等化が実現できるわけではない。

表4．設定パラメーター一覧

パラメータ	生成方法
論理ボリューム名	顧客からの申請情報を基にシステムで一意のものを事前定義し，それを利用する。
論理ボリュームサイズ	顧客から申請された各VMに指定されたサイズを基に計算する。すべてのVMに対して計算した和を必要ボリュームサイズとする。ただし，スナップショットを利用したバックアップ(VCBやVDRによるバックアップ)を取得することを想定する場合には，変更量を勘案する。
ポートグループ名	顧客からの申請情報を基にシステムで一意のものを事前定義し，それを利用する。
VLAN ID	顧客用に割り当てるIDの範囲(例えば，101～4000など)を事前定義し，現在割り当てられていない最も小さい番号を自動的に割り当てる。
データストア名	顧客からの申請情報を基にシステムで一意のものを事前定義し，それを利用する。
仮想リソースプール名	顧客からの申請情報を基にシステムで一意のものを事前定義し，それを利用する。
仮想リソースプールのCPU上限値	各VMに指定されているCPU周波数の和である。
仮想リソースプールのメモリ上限	各VMに指定されているメモリ量の和である。
VMカスタマイズ名	顧客名は，顧客からの申請情報を基にシステムで一意のものを事前定義し，それを利用する。
VMのゲストOS(Windows(注2))のフルネーム	ホスト名は，各VMに指定されているホスト名を利用する。

(注2)　Windowsは，Microsoft Corp. の登録商標である。

VCB：VMware Consolidated Backup
VDR：VMware Data Recovery
VLAN ID：Virtual LAN ID

表5．アクター間の入出力定義

機能 / 入出力	物理リソース空き状況の確認	
入出力1	システム管理者・環境構築プロセス間	CPU使用量
		メモリ使用量
		ストレージ装置識別情報
		ディスク使用量
		OS種別
		OSバージョン
		OS地域情報
入出力2	環境構築プロセス・ストレージ管理ツール間	ストレージ管理ツールログオンユーザー名
		ストレージ管理ツールログオンパスワード
		ストレージ装置識別情報
		ディスク使用量
入出力3	環境構築プロセス・VMware管理ツール間	vCenterサーバ識別情報
		vCenterサーバ接続ログイン名
		vCenterサーバ接続パスワード
		CPU使用量
		メモリ使用量

断にする物理サーバが存在するほどの余剰物理リソースを事前に確保することは想定していないため，均等に配置する方式とする。

3.3　各種パラメータの自動生成

顧客ごとに仮想スイッチのポート名などの命名規則や仮想リソース量の計算方法を事前に決めておくことで自動生成が可能となる。**表4**に各設定に必要となるパラメータを示す。

3.4　入出力データの定義

各フローにおけるアクター間の入出力内容を定義し，授受するデータ項目や内容を標準化する。**2．2節**で述べた機能プロセス定義の各項目での入出力は，①の“物理リソース空き状況の確認”を例にとると，**表5**のとおりとなる。

4．むすび

VPOの新サービスであるマルチテナント化した仮想環境の提供で，短納期で仮想環境構築が実現できる，プロセスの定義や実現方式のルール化を整理した。今後は，運用自動化ツールを使った環境で，今回整理したプロセス定義や実現方式の妥当性を検証し，2011年度にリリースするVPO新サービスへ適用する。

特集論文

オンデマンド基盤構築ソリューション“Fine Platform Solutions”

伊藤正裕* 萱野重実*
草場信夫*
山田健策*

"Fine Platform Solutions"：On-demand Platform Integration Solutions

Masahiro Ito, Nobuo Kusaba, Kensaku Yamada, Shigemi Kayano

要　旨

近年，IT(Information Technology)インフラやアプリケーションをサービスとして提供するクラウド・コンピューティング(以下“クラウド”という。)が伸展してきている。三菱電機インフォメーションテクノロジー㈱(MDIT)は，クラウドの特性を活(い)かしながら，基幹系システムの稼働に耐えうるITインフラ環境を構築するために，オンデマンド基盤構築ソリューション“Fine Platform Solutions”を提供している。Fine Platform Solutionsは，オンデマンド基盤の企画検討，要件分析，設計，構築，運用支援，保守までワンストップで提供する。

Fine Platform Solutionsの特長は次のとおりである。

①現状システムを正しく把握しオンデマンド基盤の要件を明確にする“アセスメントサービス”

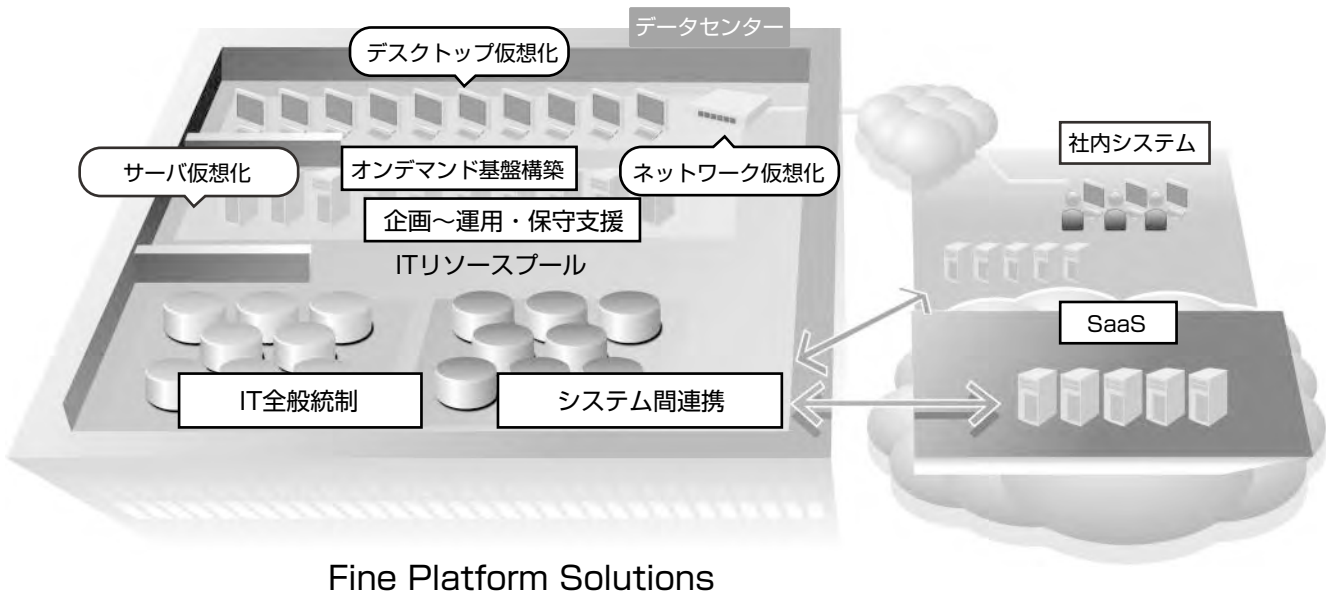
②マルチベンダーハードウェア及びミドルウェア製品による設計，構築

③オンデマンド基盤を利用者自らが容易に運用管理するための“セルフサービスポータル”構築

④外部とのデータの“つなぎ”を可能とする“システム間連携”の設計，構築

⑤“いつ，どこで，だれが，どのような操作をしたか”という履歴(ログ)を，監査証跡として一元管理し，常に把握することができる“IT全般統制”の設計，構築

今後は，クラウドの特質の１つである“ITリソースの自動管理”を実現するなど，更なる効率化を目指し，基幹業務処理に耐えられる性能を維持しながら，各種機能を強化していく。



SaaS：Software as a Service

オンデマンド基盤構築ソリューション“Fine Platform Solutions”

Fine Platform Solutionsは，サーバ，デスクトップ，ネットワーク，ストレージといったITリソースのプール化を実現するためのオンデマンド基盤構築ソリューションである。外部とのデータの“つなぎ”を可能とする“システム間連携”，セキュリティ対策を万全とし，安心な運用を実現するための“IT全般統制”等の機能も実現することができることを特長としている。

*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，ITインフラやアプリケーションをサービスとして提供するクラウドが伸展してきている。ITインフラのクラウド化は，サーバ，デスクトップ，ネットワーク，ストレージといったITリソースのプール化によって，必要な時にリソースを確保し，不要になれば開放して再利用に備えることが容易に行え，ITコスト削減，迅速なIT環境の提供を可能とする。

本稿では，企業内に構築するITインフラのクラウド基盤の構築・運用の課題を示し，その解決策としてオンデマンド基盤構築ソリューションFine Platform Solutionsについて述べる。

2. オンデマンド基盤

2.1 プライベート・クラウドのメリット

ITインフラのクラウド化では，ITリソースの配置形態によって，ほかの企業とITリソースを共用するパブリック・クラウドと企業自らがITリソースを占有するプライベート・クラウドがある。プライベート・クラウドは，自社でITリソースを占有することから，自社のセキュリティポリシーの適用が可能であること，サービスレベルの独自定義が可能なことから，企業の基幹系業務を稼働させるITインフラとして需要が高まっている(**表1**)。

2.2 オンデマンド基盤とは

サーバ仮想化とプライベート・クラウドの違いには明確なものはない。サーバ仮想化は，

・必要な時に，ハードウェアを準備せずに仮想サーバの作成が可能
・導入，電気代などのコスト削減／CO_2排出量の削減が可能
・設置スペースの削減が可能
・新サーバでは稼働しない旧OS(Operating System)システムの延命が可能

といったメリットがあるが，運用の統合・自動化，システム連携，IT全般統制を付加すると，仮想化効果が更に向上する。MDITは，これをオンデマンド基盤と称している。

MDITでは，三菱電機オンデマンドITサービス“DIAX-aaS”のもと，IaaS(Infrastructure as a Service)及びPaaS(Platform as a Service)対応のオンデマンド基盤構築ソリューションFine Platform Solutionsを提供している。

3. Fine Platform Solutions

3.1 プライベート・クラウド構築課題と解決法

クラウドの特性を活かしたプライベートなITインフラ構築には，現在，様々な課題がある。

(1) ITリソースの柔軟な活用を可能とする設計が必要

ITリソースを統合し集中管理することになるため，現状を正しく把握した上で，将来を見据えてのIT機器の選定，可用性及び災害対策を考慮したシステム設計を行うことが必要となる。

(2) オンデマンド・セルフサービスの実現

オンデマンド基盤の特長を活かすには，必要な時に自分自身で，迅速にリソースを確保／開放するための仕組みとユーザー・インタフェースが必要となる。しかも，このユーザー・インタフェースでは，ログインしているユーザーがどのリソースを操作できるのか，どこまでの操作が許されるのかといった権限を意識した作りとなっている必要がある。

(3) 外部SaaS(Software as a Service)システムとの連携

アプリケーションを新たなプラットフォーム(ハードウェア，OS)に追従させるための維持コストを削減するとともに，最新機能を開発投資せず享受するために，社外サービスであるSaaSを活用することが重要となる。そのために，既存システムとSaaSを無理なく連携させる手段が必要となる。

(4) クラウド故のセキュリティ対策

クラウドでは，システム作成／削除，ITリソース変更などが容易に行え，システムの利便性は向上する。しかし，承認されていないシステムの生成，必要なシステムが故意に削除される，ほかへの影響を無視したITリソースの変更などの危険性もある。さらに，様々な端末からネットワーク経由でアクセス可能とすることで，不正アクセスの不安も出てくる。これらセキュリティの課題は，パブリック・クラウドだけでなく，プライベート・クラウドでも同様である。クラウドの特性を活かした便利なITインフラを構築し運用するためには，しっかりとしたIT全般統制が必要である。

表1．パブリック・クラウドとプライベート・クラウドの比較

配置形態	メリット	デメリット
パブリック・クラウド	・設備の初期投資が不要 ・ＩＴリソースの拡大・縮小が容易	・全く知らない他社とＩＴリソースを共有するため，セキュリティが不安 ・サービスレベルはクラウド事業者のメニューからの選択のみ ・ＩＴリソースの設置場所がどこの国かを含めて不明な場合がある
プライベート・クラウド	・自社のセキュリティポリシー適用が可能 ・サービスレベルの独自定義が可能 ・ＩＴリソース利用は，自社に閉じるための安心感あり ・ＩＴリソースの設置場所が明確	・設備の初期投資が必要 ・ＩＴリソースの拡大は，自社で用意したリソースが上限

3.2 提供するサービス

Fine Platform Solutionsは，プライベート・クラウドを構築・運用する際のこれら課題を解決するために，MDITが持つ技術と実績による仮想化技術，システム間連携技術，ログ収集・蓄積・分析技術を総合的にワンストップで提供する(**図1**)。

3.2.1 アセスメントサービス

オンデマンド基盤構築の第一歩は，現状を正しく把握し既存システムをどのように統合化するか，将来の拡張をどのように計画するかである。これを定量的なデータとして可視化するために，既存システムのCPU(Central Processing Unit)／メモリ／ディスク／ネットワーク負荷を処理が増大する月次処理を挟んで収集し，分析する必要がある。これを実現するために，Fine Platform Solutionsでは，“CentAnalyzer”を開発し，データ収集・分析するサービスを提供している。

CentAnalyzerは，**図2**のように，Windows(注1) OSであれば，WMI(Windows Management Instrumentation)を用い，Linux(注2) OSであれば，SSH(Secure SHell)を用いて，パフォーマンス情報をデータベースに収集する。WMI，SSHを用いることで，測定対象のサーバには情報収集エージェントを入れることなく，情報の採取が行える。また，データ収集後，要件に基づき統合後の最適システム構成案や予測負荷を自動算出する。自動算出では，仮想化オーバーヘッド，プロセッサ性能差，仮想サーバ割当て優先度付け等を考慮している。このようにして収集したデータは，ローカルデータベースに格納することで情報漏洩(ろうえい)を防ぐとともに，収集したデータの分析・加工を容易にし，多角的な分析・統合計画の支援を可能としている。レポートの例を**図3**に示す。

(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。

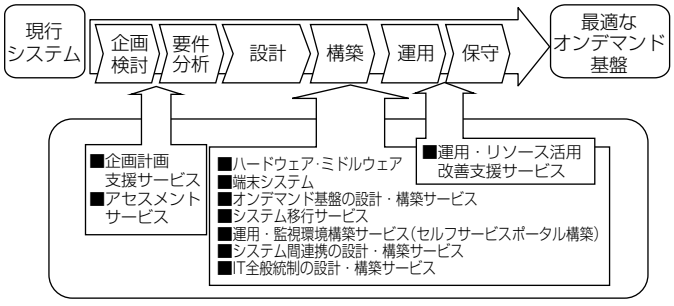


図1．Fine Platform Solutionsが提供するサービス

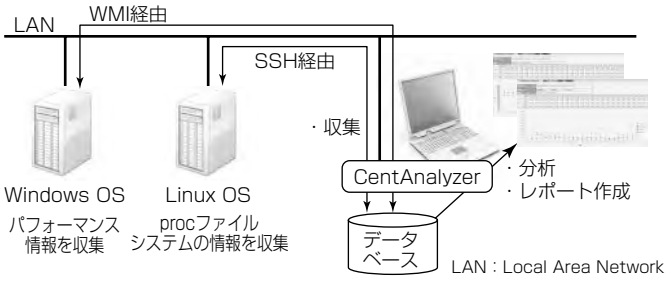


図2．CentAnalyzerの仕組み

3.2.2 オンデマンド基盤の設計・構築サービス

オンデマンド基盤の運用で，“運用統合・自動化”技術が不可欠である。

(1) 運用の統合化

管理部門が統合的に管理することで，利用部門は割り当てられたリソースプール内で，仮想サーバ作成，ITリソースの変更を行える。また，物理サーバ，仮想サーバ，その他IT機器類を統合的に運用・監視することで，管理部門，ユーザー部門ともに運用コストの削減が可能となる。さらに，仮想化されたサーバを統合運用しリソースの空き／不足を監視することによって，リソースの最適配置が可能となり，無駄なサーバ追加などコストを抑制することができる。

(2) 運用の自動化・可用性向上

仮想化によるHA(High Availability)を用いることで物理ハードウェア障害発生時にほかのサーバで仮想サーバの自動立ち上げが可能となる。

Fine Platform Solutionsでは，これらオンデマンド基盤を顧客要件にあわせ，最適なハードウェア，ミドルウェアを選択し，マルチベンダー対応で設計・構築することが可能である。

3.2.3 セルフサービスポータル

クラウドの特質として，必要な時に自分自身で，迅速にリソースを確保／開放することが必要とされる。これを実現する機能が“セルフサービスポータル”である。MDITは，導入顧客の要件に合わせてセルフサービスポータルを構築するためのフレームワークを提供する。このフレームワークは，仮想化ミドルウェアVMware社ESXサーバに対応している。基本機能として，VMware(注3)のAPI(Application Programming Interface)を駆使してゲストOSの起動，停止，再起動や，ゲストOSの作成，ゲストOSなどの

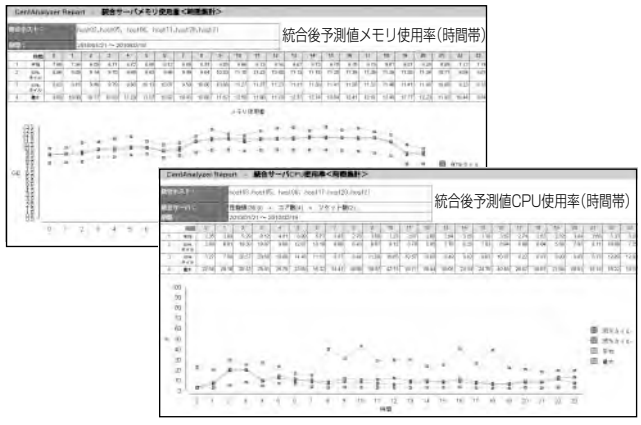


図3．アセスメントサービス：分析レポート(サンプル)

図４．セルフサービスポータル操作画面

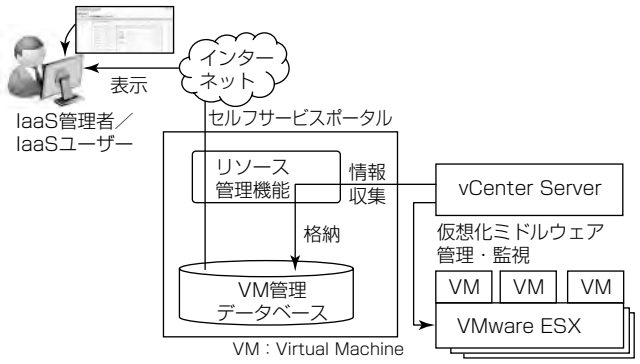


図５．情報表示の高速化

負荷の監視，データベースなどのアプリケーションを監視する機能を提供する(**図４**)。

ゲストOSなどの負荷状況監視は，ユーザーが要求する度にVMware vCenter Serverに問い合わせを実施すると，システム負荷が高くなるため，定期的に情報を採取し，内蔵のデータベースに情報を保管するなど工夫をして実装している。これによって，多数のユーザーからの要求を即座にポータル上に表示することを可能とした(**図５**)。

(注３)　VMwareは，VMware，Inc. の登録商標である。

3.2.4　システム間連携の設計・構築サービス

従来のシステムでは，関連する複数のシステムの間はスパゲティ状態で密結合している場合が多い。今後，システムを改修／拡張／更なる連携を進める上で，密結合は問題となる。将来の拡張性を考慮して疎結合化することは，システムの一部をパブリック・クラウド上のSaaSに置き換える場合にも有効である。Fine Platform Solutionsでは，外部との データの“つなぎ”の機能として“トランザクションHUB”を提供する。トランザクションHUBは，システム間のデータの流れを，統一されたやり方，統一されたインタフェースで扱え，データの“つなぎ”の構築／運用／保守を容易にする(**図６**)。

3.2.5　IT全般統制の設計・構築サービス

Fine Platform Solutionsでは，“いつ，どこで，だれが，どのような操作をしたか”というコンピュータの操作やアクセスの履歴(ログ)を，監査証跡として一元管理し，常に把握することができる機能を提供する。システムを統合化し管理するオンデマンド基盤では，大量な何種類ものログ

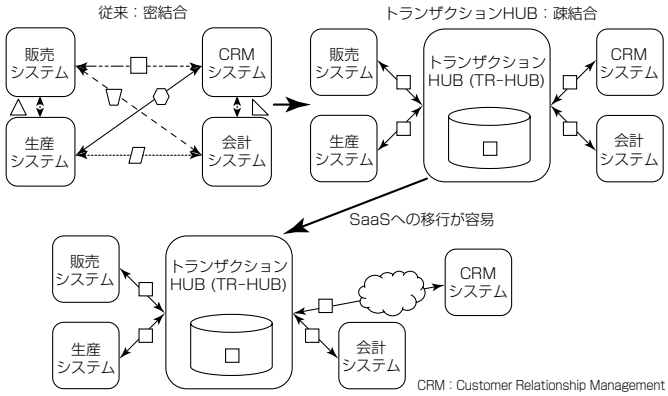


図６．トランザクションHUBによるシステム間連携

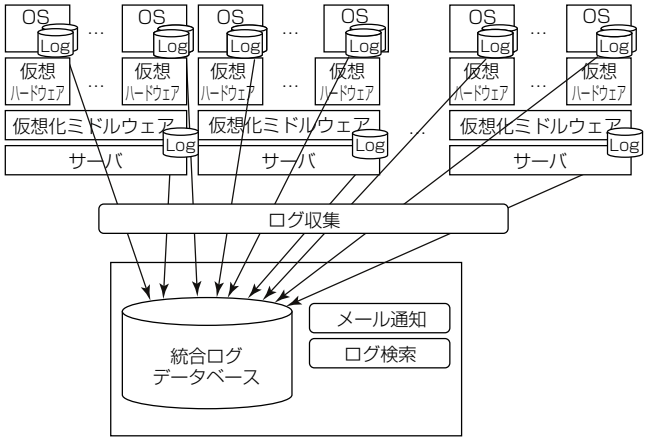


図７．IT全般統制対応ログ管理

が出力される。これら大容量のログの蓄積，分析を高速に行うために，“データ圧縮技術”(データ量を1/10 以下に圧縮し，ストレージコスト低減と高速化を実現)，“並列処理技術”(データ規模に応じた処理速度と高スケーラビリティの実現)，“高速文字列照合技術”(ログ形式判別や，索引を使用しない検索を高速に実現)等の当社独自の高速処理技術を採用しオンデマンド基盤に適用した(**図７**)。

4. むすび

MDITは，プライベート・クラウド構築対応で，オンデマンド基盤構築ソリューションFine Platform Solutionsを提供している。今後，クラウドの特質の１つである“ITリソースの自動管理”を実現するなど，さらなる効率化を目指し，基幹業務処理に耐えられる性能を維持しながら，各種機能を強化していく。

参考文献

(1)　河井弘安，ほか：企業環境の変化に対応するシステム間データ連携基盤，三菱電機技報，**84**，No. 7，387～390（2010）
(2)　多種多様なログを統合し一元管理する“LogAuditor”，三菱電機技報，**81**，No. 1，23（2007）

特集論文

ITサービスインテグレーション“BizFLEX”

松田昇平* 川口正高*
安福哲男* 平井 譲*
大野次彦* 魚住光成**

IT Service Integration "BizFLEX"

Shohei Matsuda, Tetsuo Yasufuku, Tsugihiko Ohno, Masataka Kawaguchi, Yuzuru Hirai, Mitsunari Uozumi

要 旨

クラウド・コンピューティングの台頭によって，企業・組織の情報システムにおいても，仮想化技術によるシステムの統合，IaaS(Infrastructure as a Service)の活用によるハードウェアインフラの非保有，SaaS(Software as a Service)による業務システムのサービス利用など，システム調達の選択肢が大幅に拡大しつつある。

三菱電機インフォメーションシステムズ㈱(MDIS)はクラウド技術活用によるシステム調達形態の変化に対応するために，ITサービスインテグレーション“BizFLEX”を2010年7月より提供している。

BizFLEXは，企業・組織の情報システムをクラウド技術を用いて革新するためのソリューション群である。

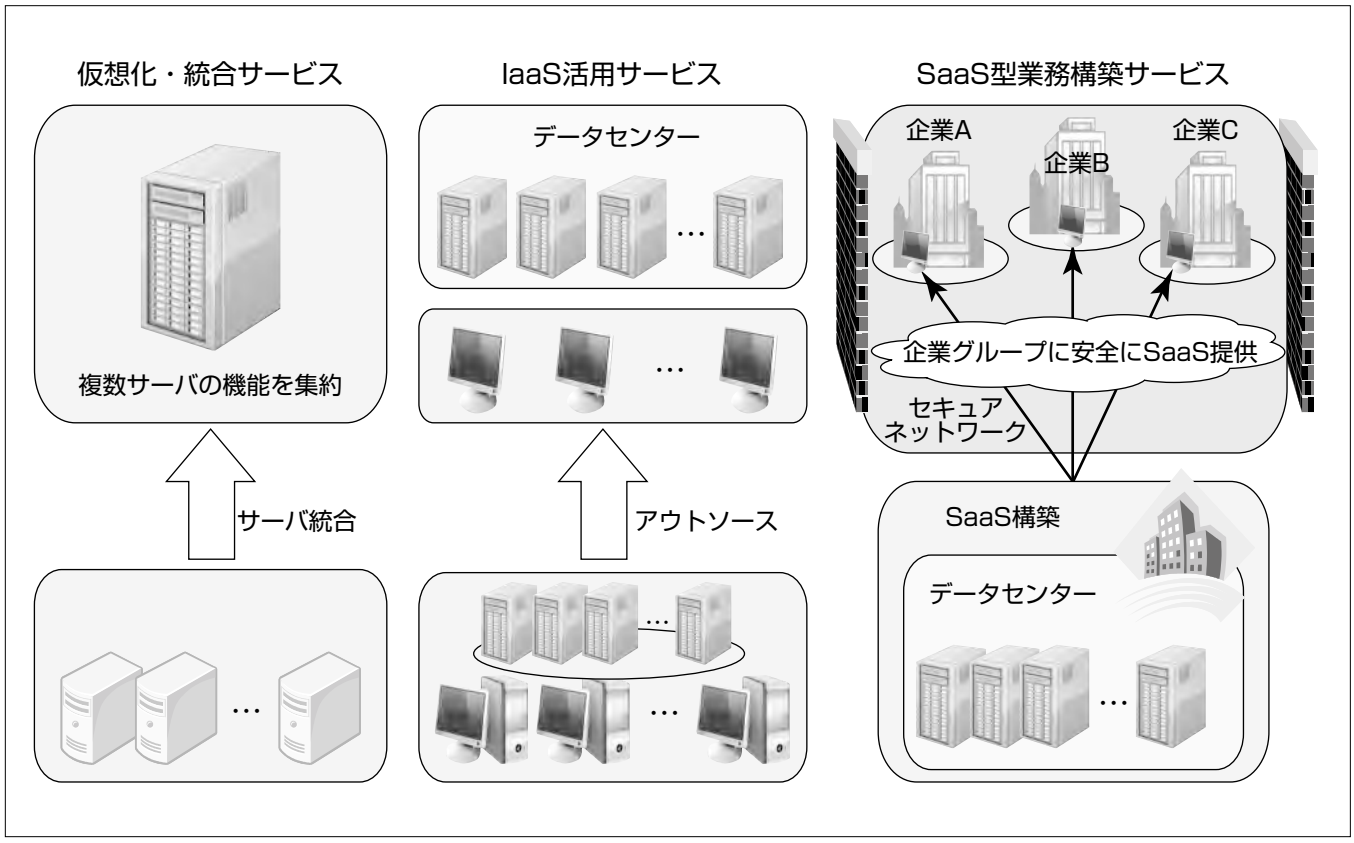
BizFLEXでは，提供するシステム企画・構築・運用サービスを，大きく3つに分けてとらえる。

(1) 仮想化・統合サービス
(2) IaaS活用サービス
(3) SaaS型業務構築サービス

BizFLEXの適用によって，次のような効果が期待できる。

・事業部門の運用負荷の低減
・初期導入費用と期間の圧縮
・全社横断的な情報活用
・十分なセキュリティ・レベルの確保

MDISではクラウド技術を活用したシステム企画・構築・運用に対応するために，インフラの提供とアプリケーションの構築の両面で，一層の技術力強化及び必要なパートナーとの連携を進めていく。



BizFLEXの代表的なサービス

ITサービスインテグレーションBizFLEXは，仮想化・統合からSaaS構築まで，企業情報システムの調達に際してITサービスの企画・構築・運用をワンストップで提供するためのソリューション群である。大きくは上で述べた3つの形態に対応したシステム企画・構築・運用サービスからなる。

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

1. まえがき

近年の，いわゆるクラウド・コンピューティングの台頭によって，企業・組織の情報システムにおいてもシステム調達の選択肢が大幅に拡大しつつある。すなわち，これまでのシステム機能ごとに自社保有・自社構築することを中心としたシステム調達から，仮想化技術を用いて複数のシステムをまとめて共通ハードウェアインフラの上に構築して効率化を図る形態や，社外のサービス・メニュー化されたIaaSの上にシステム構築することによって，ハードウェアインフラ調達のオーバヘッドを低減し迅速なシステム構築を可能とする形態，さらには，1つの企業だけでなく共通の目的を持つ企業グループが情報システムの機能をサービスとして共有し，グループ全体として更なる効率化を図る形態などに拡大している(**図1**)。

これらの形態は，一つ一つを見ると従来からあるサービスの適用の発展形だが，“所有から利用へ”の考え方の下，仮想化技術や複数の企業ユーザーを管理する技術などによって，リソースのより高度な共有を図る点が革新的である。

MDISでは，このようなクラウド技術活用によるシステム調達形態の変化に対応するために，2010年7月より，ITサービスインテグレーションBizFLEXを提供している。

本稿では，BizFLEXの概要，技術的な特長及び事例について述べる。

2. BizFLEXとは

BizFLEXとは，企業・組織の情報システムを，クラウド技術を用いて革新するためのソリューション群である。

BizFLEXでは，提供するシステム企画・構築・運用サービスを，大きく3つに分けてとらえる(**扉図**)。

(1) 仮想化・統合サービス
(2) IaaS活用サービス
(3) SaaS型業務構築サービス

以下に，各サービスの概要を述べる。

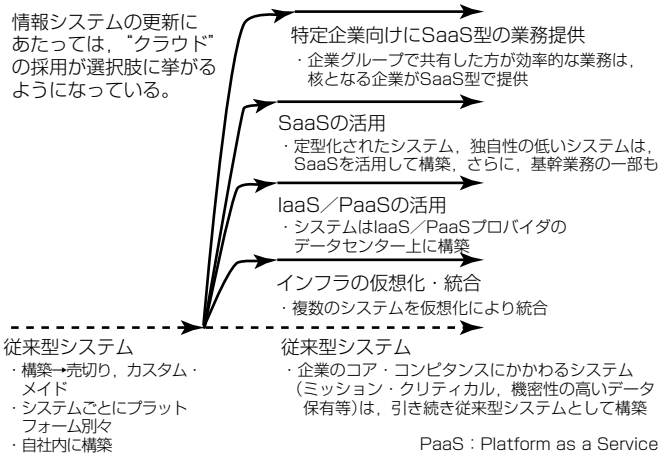


図1．情報システム調達の選択肢の拡大

2.1 仮想化・統合サービス

仮想化・統合サービスは，複数のサーバに個別に構築されていたシステムを，仮想化技術によって統合する。

クライアント－サーバ・コンピューティングの普及以降，情報システムごとにサーバを用意することが普通になったため，企業内のサーバ数は膨れ上がってきた。多数のサーバは，おのおの運用管理が必要であり，情報システム部門や業務部門の負担となっている。一方，システム別にサーバを立てるため，企業全体としての処理能力は，一般的に過剰になっている。

BizFLEX仮想化・統合サービスは，企業の保有する複数のシステムの用途や必要処理能力を見極めた上で，仮想化技術によってサーバを統合する。仮想化ミドルウェア(ハイパーバイザ)として，ヴイエムウェア社のVMware(注1)，マイクロソフト社のHyper-V(注2)が利用可能であり，さらに，KVM(Kernel-based Virtual Machine)などの仮想化ミドルウェアについても個別対応をしていく。

仮想化・統合サービスでは，複数の現行のシステムの運用をどのように共通化し，どのように仮想化環境にマッピングするかの設計が重要であり，システムの特性によっては仮想化に含めない判断も必要である。例えば，独自のスケジュールで連続稼働が不可欠の業務については，サーバ・インフラを共用することによって，そのスケジュールが統合されたシステム全体の運用に影響を及ぼす可能性があり，統合には向かない。また，仮想化環境へのマッピングのためには，現行システムの負荷状況の見極めも重要であり，BizFLEXではそのための性能予備調査もサービスに含んでいる。

システムを仮想化・統合すると，システム運用は共通化されて全体としては単純化するが，一方で，これまで存在しなかった仮想化ミドルウェア層の運用管理が必要になる。BizFLEXでは，このような仮想化環境全体の運用管理の設計・構築も提供する。

(注1) VMwareは，VMware，Inc. の登録商標である。
(注2) Hyper-Vは，Microsoft Corp. の登録商標である。

2.2 IaaS活用サービス

IaaS活用サービスは，情報システムのハードウェアインフラ部分を社外のIaaSサービスを用いて構築・運用する。

IaaSの活用にあたっては，システムの要件に沿った適切なIaaSサービスを選択することが重要である。情報システム部門は，ユーザー部門に対して提供するサービスのSLA(Service Level Agreement)に応じて，IaaSプロバイダが提供するサービスのOLA(Operational Level Agreement)を見極める必要がある。BizFLEXでは，要求されるサービスレベルに対するIaaSプロバイダの充足レベルを調査し，選定を支援する。特に，BizFLEXでは，安心・安全なIaaSとして，三菱電機情報ネットワーク㈱(MIND)

の“Value Platform on Demand”を活用して，信頼性の高いシステムを構築することができる。

2.3 SaaS型業務構築サービス

SaaS型業務構築サービスは，複数の企業からなる企業グループに対して，類似の業務を共通化して切り出し，一元的にSaaS型でサービス提供するシステムを構築・運用する。

業務システムを一元化することで，システム構築のための重複投資を避けることができ，システム運用も一元化できるので，必要な要員を削減することができる。また，システムを，より大きな範囲で共有するため，リソースの利用効率が高まることが期待できる。さらに，業務システムの一元化によって，企業グループ全体に対するITのガバナンスも働かせやすくなる。

一方，SaaS型業務システムでは企業ごとにある程度は異なる業務を，共通部分と可変部分に分けて整理する必要があり，現行システムの分析と再設計が通常の再構築以上に重要となる。また，複数の企業を１つのシステムで収容するため，セキュリティや信頼性の点でも従来とは異なる配慮が必要である。

BizFLEXでは，業務システムの共通化によるSaaS化，複数の企業を一つのシステムの中で分離しつつ共存させる認証・認可基盤の構築，サービス化されて社外から提供されるようになった機能と各社の社内に残った機能のサービス連携技術等を活用して，SaaS型業務システムの構築を行う。

3. BizFLEXを支える技術

クラウド技術を応用した情報システムを構築する上で，従来と異なる検討が必要なポイントの一つは，一式のリソースを複数の利用者グループ(＝テナント)で効率的に分け合うための，“マルチテナント”技術である。

これまで独立にサーバを立てていたシステムを仮想化・統合したり，SaaS型で業務サービス化したりする場合は，１つの物理的なシステムの上に異なる特性を持った複数の論理的なシステムを相乗りさせるアーキテクチャが必要である。このようなアーキテクチャ技術がマルチテナント技術である。

次に，代表的なマルチテナント技術として４つのアーキテクチャを示す(**図２**)。

(1) アプリケーション方式：アプリケーションが複数のテナントを識別する方式である。アプリケーションを適切に作れば高い効率が期待できるが，作成の負担が大きい。

(2) データベース分離方式：アプリケーションが最小限のテナントの識別を行い，個々に独立のデータベースを割り当てる方式である。従来型のアプリケーションを，少ない改修でマルチテナントに対応させることができる。

(3) 複数インスタンス方式：１つのOS(Operating System)の上でアプリケーションを複数起動し，各々をテナントに割り当てる方式である。アプリケーションの改修は少なくて済むが，インスタンス間で，OSリソースの競合がないことが条件となる。

(4) プラットフォーム仮想化方式：１つのコンピュータ上でVM(Virtual Machine)を使って複数のOSを起動し，それぞれでアプリケーションを動作させる方式である。既存のアプリケーションにほとんど手を加えることなく，マルチテナントに対応することが可能だが，VMによるオーバヘッドや，ストレージの分割ロスなどがある。

BizFLEXでは，現行システムの性能評価や，アプリケーションの構造などに着目して，これらの中から最適な方式を選択する。

4. 事　例

BizFLEXのモデル・ケースとなったSaaS型業務構築サービスの事例として，MDISが構築を担当した三菱電機㈱のオフィシャルサイトにおける共通業務サービス化(**図３**)について述べる。

三菱電機オフィシャルサイトは，単に情報発信を行うだけでなく，顧客からの相談のサポート，展示会・セミナ参加受付・管理，会員制サイトの構築・管理といった双方向の業務を行う場でもある。従来は，このような業務を行うシステムは，必要となる都度，事業部門や関係会社が個別に構築してきた。しかし，このようなシステムはインター

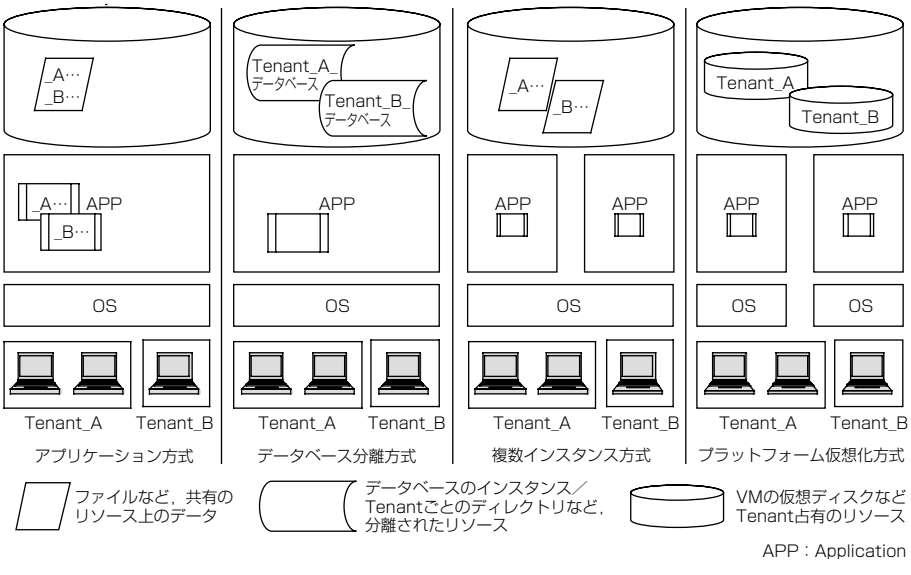


図２．マルチテナント化の方式

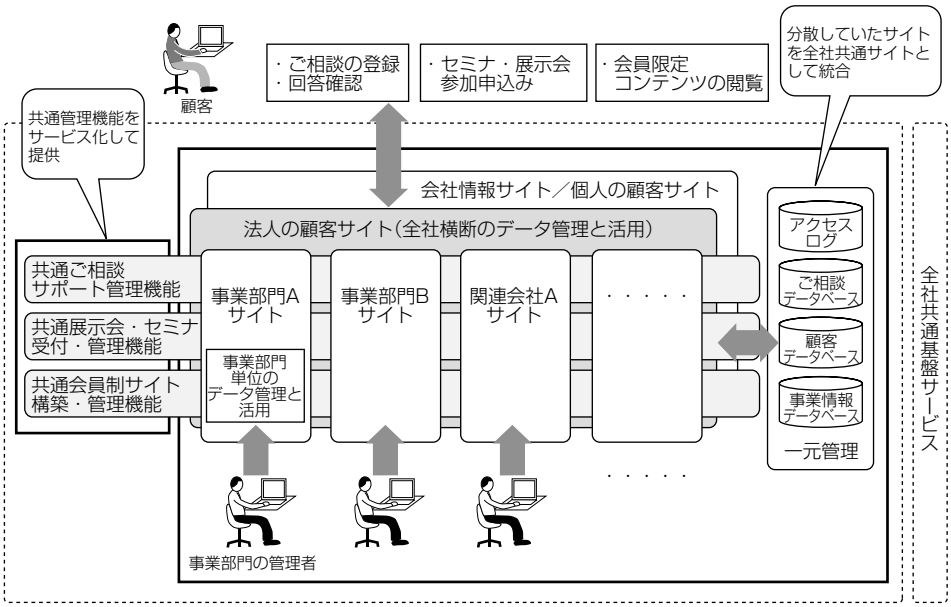


図3．オフィシャル向けサイトでの共通業務のサービス化

ネットに公開されるため，高いセキュリティが必要であり，運用管理にも手間がかかっていた。

これに対して，三菱電機オフィシャルサイトの再構築にあたっては，相談サポート，展示会・セミナ受付・管理，会員制サイト構築・運営の各業務を共通サービス化し，三菱電機宣伝部が一元的に運用するようにした。

得られた効果は次のとおり。

- 事業部門の運用負荷の低減：これまで個別に行っていて事業部門や関連会社の負担となっていた運用を，宣伝部で一元化することで，事業部門の運用負荷が低減した。
- 初期導入費用と期間の圧縮：事業部門や関係会社は，サーバ・インフラなどを準備する必要がなく，業務も標準化されているため一から検討する必要がない。
- 全社横断的な情報活用：全社で蓄積されている顧客情報などを共有して使うことができるため，個々の部門で行うよりも高度な分析が可能となった。
- 十分なセキュリティ・レベルの確保：個別に構築するとセキュリティ・レベルの確保の負担が大きく，手戻りも発生しやすいが，標準のサービス化されたシステムは必要十分なセキュリティ対策を含んでおり，セキュリティ・レベルの確保が容易である。

このようなシステムを構築するために，次のような技術上のポイントに注力している。

(1) アプリケーション方式マルチテナント

このシステムでは，サービスの共通化による運用やリソース利用の効率化に加え，蓄積する顧客情報を横断的かつ様々な角度から分析ができることが重要である。このため，**3章**で述べたマルチテナント技術の4つのアーキテクチャのうち，1つのアプリケーションで複数の顧客をサービスするアプリケーション方式を採用している。

(2) 業務の標準化

従来個別に行っていた業務を見直して，業務を標準化して切り出した。各業務について，基本機能とオプション機能に分けて整理した。例えば，セミナ募集自体は基本機能として提供するのに対して，その際アンケートを行うかはオプション機能とした。

(3) SLAベースの課金と責任分担の明確化

共通サービスの利用部門には課金して費用徴収を行うが，そのためにSLAを明確にして，これに基づいて課金を行うことにした。また，運用の中で事業部門／関係会社独自の部分は，各部門／関係会社で対応してもらう必要があり，責任分担を明確化した。

(4) 共通機能／共通データの一元管理

アクセスログの採取等は一元化し，システム全体としての管理にも使えるようにするとともに，顧客データベースなどは共通化して一元管理とした。

5. むすび

今後，企業・組織の情報システムは，クラウド技術を活用して大幅に見直されていくものと考えられる。また，企業活動のグローバル化に伴い，海外の拠点に対して均質なサービスを行うための手段としても，クラウド技術の活用が重要になってくる。

MDISではクラウド技術を活用したシステム企画・構築・運用に対応するために，インフラの提供とアプリケーションの構築の両面で，一層の技術力強化及び必要なパートナーとの連携を進めていく。

参考文献

(1) 伏見信也，ほか：クラウド技術を適用した企業情報システムへの取組み，三菱電機技報，**84**，No. 7，370～374（2010）
(2) 磯西徹明，ほか：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，三菱電機技報，**84**，No. 7，407～410（2010）
(3) 三菱電機オンデマンドITサービス“DIAXaaS”，三菱電機技報，**85**，No. 1，19（2011）

特集論文

アプリケーション構築サービスを支えるWebアプリケーション自動生成技術

天沼敏幸*
浅見可津志*
大野次彦*

Web Application Generator for Application Building Service

Toshiyuki Amanuma, Katsushi Asami, Tsugihiko Ohno

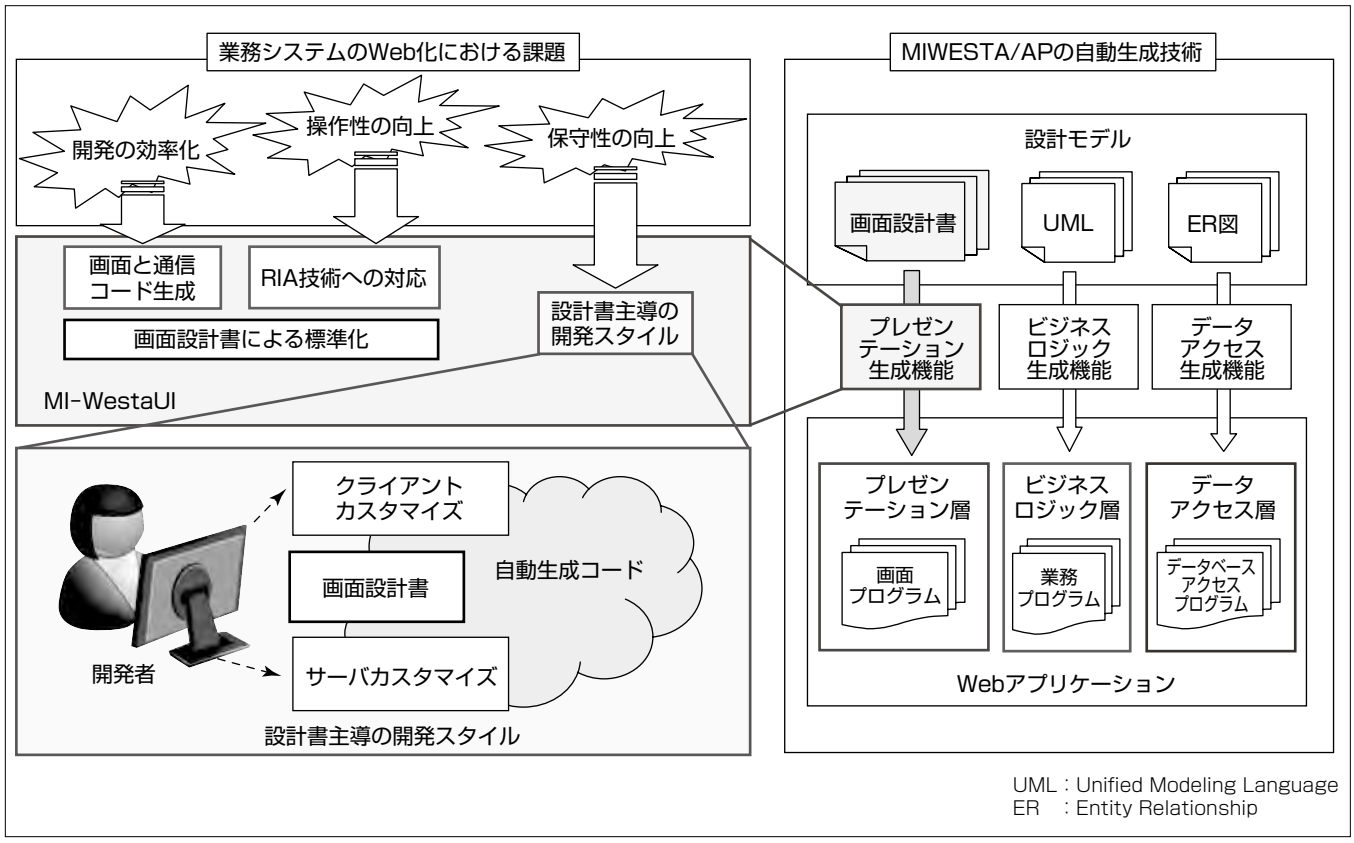
要　旨

クラウドコンピューティング技術の台頭によって，業務システムをプライベートクラウドなどのWeb環境に対応させる動きが活発化している。三菱電機インフォメーションシステムズ㈱(MDIS)では，早くからWebアプリケーション開発標準を体系化し，MIWESTA/AP(MDIS Web Development Standard for Application)としてWebアプリケーション構築技術の蓄積，整備を図ってきた。近年では，MDISがITサービスインテグレーション“BizFlex”を展開するに伴い，更なる生産性向上を目指し，自動生成技術を強化している。

業務システムのWeb化における一般課題として開発の効率化，操作性の向上，保守性の向上が挙げられる。MIWESTA/APでは論理3階層アーキテクチャの各階層に対応した自動生成機能があり，特にユーザーインタフェースについては，プレゼンテーション層の自動生成機能(MI-WestaUI)でその課題に対応し，画面設計書による標準化，画面と通信コード生成，RIA(Rich Internet Applications)技術への対応，設計書主導の開発スタイルの諸機能を実現している。実プロジェクトへの適用結果ではMI-WestaUIを含むMIWESTA/APの自動生成技術によって，業務システム全体の開発量の約6割のコード自動生成を実現している。

今後は機能強化を図るとともに，ユーザーインタフェース実装技術の分野で利用が進みはじめたJavaEE(Java(注1) Enterprise Edition)のJSF(Java Server Faces)について，RIA生成機能への対応を予定している。

(注1)　Javaは，Oracle corp.の登録商標である。



業務システムのWeb化における課題とMIWESTA/APの自動生成技術の対応

業務システムのWeb化における課題として開発の効率化，操作性の向上，保守性の向上がある。MIWESTA/APは論理3階層アーキテクチャに対応しており，特にユーザーインタフェースについてはプレゼンテーション層の自動生成機能(画面設計書による標準化，画面と通信コードの生成，RIA技術への対応，設計書主導の開発スタイル)によって，業務システムのWeb化における課題に対応している。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

MDISではWebアプリケーションの開発標準を体系化し，MIWESTA/APとして，Webアプリケーション構築技術の蓄積・整備を図ってきた[1]。近年ではITサービスインテグレーションBizFlexを展開するに伴い，更なる生産性の向上を目指し，自動生成技術を強化している。

MIWESTA/APが対象とする業務システムは数百画面をもつユーザーインタフェース中心のシステムであることが多い。ユーザーインタフェースについては，操作性への要求が高く，ユーザーからの改善要望が集中しやすい。MIWESTA/APの自動生成技術は，そのような業務システムをWebアプリケーションで効率的に開発するための機能提供を目標としている。

本稿では，MIWESTA/APの自動生成技術の全体像を紹介し，その中でプレゼンテーション層の自動生成機能(MI－WestaUI)[2]を中心に，業務システムのWeb化における課題とそれを解決するMI－WestaUIの実現方式及び実システム適用による改善点について述べる。

2. MIWESTA/APの自動生成技術

MIWESTA/APはWebアプリケーションをプレゼンテーション層，ビジネスロジック層，データアクセス層の論理3階層で構成するアーキテクチャに対応している。

MIWESTA/APの自動生成方式の特徴は，上流側からの設計成果である設計モデルから，Webアプリケーションの論理3階層の各層に対応したプログラムを生成する点にある(**図1**)。

プレゼンテーション層では，画面設計書からブラウザに表示される画面及び通信に使用するデータ構造とサーバ側で送受信するコードを生成する。ビジネスロジック層では，UMLで記述された設計書からJavaコードを生成する。データアクセス層では，ER図から作成したデータベース定義に基づきデータベースアクセス用Javaコードを生成する。これらの機能を利用し，データベース定義からWebアプリケーション開発の足場となるデータベースメンテナンス用プログラムを一括生成する機能も提供している。

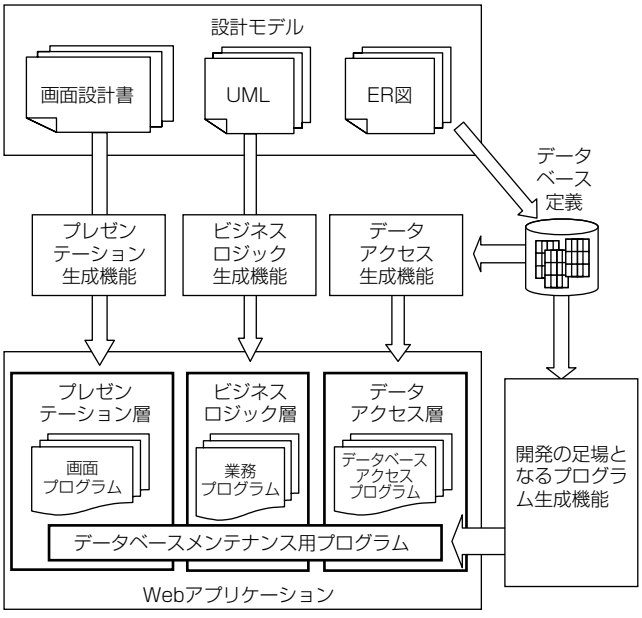


図1．MIWESTA/APの自動生成技術

3. 業務システムのWeb化における課題

3.1 開発の効率化

大規模なWebアプリケーションを開発する際に問題となるのは，開発環境での実装の自由度が高く，品質や開発スピードが開発者個人のスキルに大きく依存する点である。実際の開発では，開発規約によって標準化を図るようにしているが，徹底は困難で開発の効率化を妨げる要因となる。対策としては，画面の設計モデルを作成する時点で標準化を実施し，それをそのまま実装コードに反映する方式が考えられる。

3.2 操作性の向上

一般に業務システムを標準的なHTML(HyperText Markup Language)の機能だけで実装した場合，操作性が低下することが多い。画面のデザインや操作性への要求は高く，ユーザーからの改善要望が集中しやすいところである。そのため，操作性の向上を目的として各種のRIA(Rich Internet Applications)技術の活用は不可欠であるが，導入にあたっては，個別のRIA製品に精通したプログラミング技術者を確保しなければならないという課題がある。

MI－WestaUIの特長の一つは，実装に依存しない画面設計モデルから，特定のRIA技術に対応した実装コードを生成する点にあり，開発者のスキルに依存しない。

3.3 保守性の向上

ユーザーインタフェースの開発では，試験工程での不具合修正や仕様変更によって，数百の画面の一括変更が必要になるケースが多い。これは，保守フェーズでの改良開発でも同様である。そのため，大量の画面を繰り返し変更できる方式や，開発者の負担を伴わない方式によって画面の設計モデルと実装コードを一致させる開発スタイルをサポートする必要がある。

4. MI－WestaUIの実現方式

この章では，業務システムのWeb化における課題に対応するためにMI－WestaUIが提供している諸機能(**図2**)について，その実現方式を交えて述べる。

4.1 画面設計書による標準化

通常，画面の開発では次に示す①から④の設計項目について，設計時と実装時の2段階で，設計レベルの詳細化を行う。この過程では担当者間の解釈の齟齬(そご)などによ

って誤りが混入することが多い。

MI-WestaUIでは，標準化された画面設計書によって，設計の時点で，実装まで含めた開発手順の標準化を実施している。設計者に対しては，アプリケーションフレームワークの機能を前提にすることで，実装に関する知識がなくても，詳細レベルの設計ができるようにしている。

MI-WestaUIの画面設計書では，Excel(注2)の形式で，次に示す画面設計項目を指定する。

①画面レイアウト－画面上の部品配置及び表示ラベル
②入出力項目-部品に対応するデータ名，初期値
③入力制約－入力データのエラー検出のための規則
④アクション明細-サーバ通信時の呼出し方法

MI-WestaUIは画面設計項目が入力されたExcelシートを基に，実装コードを自動生成する。

生成されたコードは，MI-WestaUIが提供するEclipse(注3)上の開発環境で自動的にコンパイルされる仕組みになっており，そのままアプリケーションサーバを利用した試験作業に移行できる。

また，画面設計書の設計情報は，Eclipse上の“UIモデルエディター”(**図3**)でグラフィカルに表示することができ，プログラマが設計情報を確認しながら実装作業を実施できる。

(注2)　Excelは，Microsoft Corp. の登録商標である。
(注3)　Eclipseは，Eclipse Foundation，Inc. の登録商標である。

4.2　画面と通信コード生成

MI-WestaUIでは画面設計書から，ブラウザの画面コード，サーバとの送受信メッセージ及び通信コードを自動生成することによって，プレゼンテーション層の開発を効率化している。また，MI-WestaUIによって生成される通信機能は，**図4**に示すようにWebサービス(HTTP(Hyper Text Transfer Protocol) SOAP(Simple Object Access Protocol))として動作するため，通常のWebアプリケーションのように通信に伴う画面全体の再表示が発生しない。

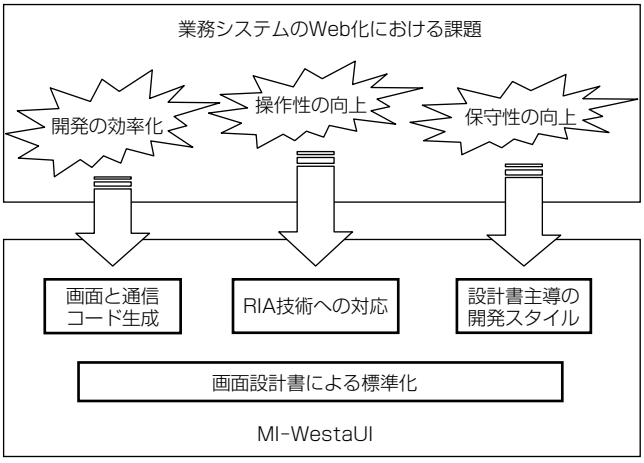


図2．業務システムのWeb化における課題と対策

図3．UIモデルエディター

4.3　RIA技術への対応

MI-WestaUIの自動生成機能は，様々なRIA実装技術に対応するため交換可能な方式になっており，現在は，RIA技術で最も普及しているFlex(注4)に対応している。Flex部品群の実装コードを自動生成することによって，Flexに精通していない開発者でも高度な操作性を持つ画面を容易に構築することができる。

操作性の向上の一例として，入力制約違反時のメッセージ表示で該当項目が指摘されるユーザーインタフェースを示す。入力制約は**図5**に示すように，必須チェック，テキスト属性(半角，全角ほか)，最大・最小桁等主な項目を画面設計書に指定することによって記述する。入力制約チェックの実装コードはMI-WestaUIによって生成されるが，制約違反時のメッセージは，部品のラベル設定から自動で合成されて表示される。この例ではメッセージの“ユーザー名”の部分が部品のラベル設定に当たる。

(注4)　Flexは，Adobe Systems, Inc. の登録商標である。

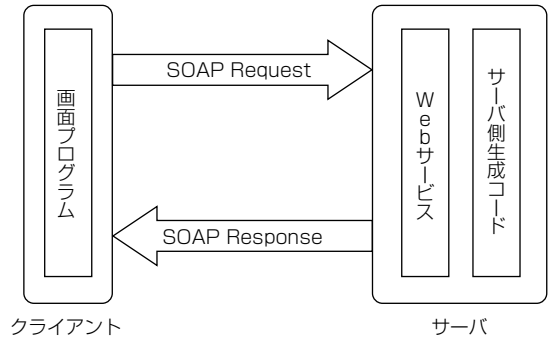


図4．MI-WestaUIによって生成される通信機能

図5．必須チェックの表示と設定例

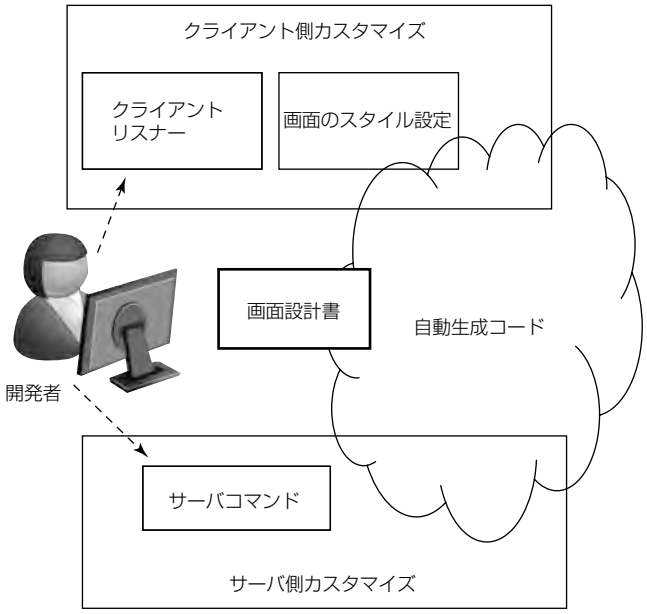


図6．MI-WestaUIの開発スタイル

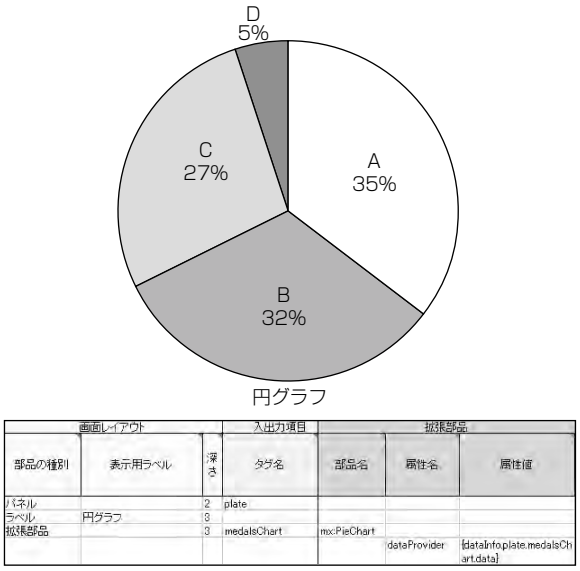


図7．拡張部品及び拡張属性の記述例

4.4　設計書主導の開発スタイル

MI-WestaUIでは，頻繁な画面の仕様変更に対応するため，修正が発生した場合に，画面設計書を修正し，画面を自動生成する手順を繰り返す開発スタイルを想定している（**図6**）。そのためには開発者が画面のカスタマイズの目的で独自に記述したコードを，自動生成の再実行で上書きしないことが前提となる。したがって，開発者がカスタマイズのために記述する以下のコードを自動生成部分から分離する方式にしている。

①クライアントリスナー（クライアント側における標準外の操作性を向上する画面ごとのコード）

②サーバコマンド（サーバ側のメッセージ送受信，ビジネスロジックの呼出しの画面毎コード）

③画面のスタイル設定

このように，標準化された部分は自動生成によって開発効率を下げずに変更を繰り返すことができ，一方，カスタマイズ部分は局所化され，変更が把握しやすいという利点がある。また，結果として画面設計書とコードは一致した状態が保たれる。

5. 実システム適用における改善

MI-WestaUIを含むMIWESTA/APのフレームワークを利用したシステム開発では，全体開発量の約6割のコードを自動生成することができた。また，プロジェクト適用の結果に基づき，機能追加，性能向上，操作性の改善を行った。実システム適用における機能追加では，Flexで利用可能なカスタム部品を利用したいという要望があった。

MI-WestaUIの画面設計書では，業務システムで利用頻度の高い約30種類の標準部品を選択できるが，カスタム部品の情報を記述することはできなかった。そこで，プロジェクト適用時の柔軟性に配慮し，拡張部品及び拡張属性を記述できるようにした。これによってサードパーティから提供されるカスタム部品の利用も可能となっている。Flexのチャートコンポーネントの一つである円グラフを利用する例を**図7**に示す。設計仕様書の部品名に拡張部品であるmx:PieChartを直接記述することによって，標準部品と組み合わせた画面を構成している。

6. むすび

Webアプリケーションの実装技術の進展にはめまぐるしいものがあり，MIWESTA/APでは，新技術を体系化するために継続的な取組みを行っている。ここで述べたWebアプリケーションのユーザーインタフェース実装技術の分野では，JavaEEのJSFが利用されるようになってきており，今後のMI-WestaUIの実装技術対応として，JSF実装のRIA生成機能開発を予定している。

参考文献

(1) 川口正高，ほか：オープン環境のシステム構築を高品質・短納期で実現するWebシステム開発標準“MIWESTA”，三菱電機技報，**81**，No. 7，489～492（2007）

(2) 渡邉圭輔，ほか：Webアプリケーションユーザーインターフェイス構築技術，三菱電機技報，**82**，No. 12，783～786（2008）

特集論文

スマートフォンで社内に安全にアクセス “セキュアスマートフォンアクセスサービス”

柘場純一*
木岡宣明*

"Secure Smartphone Access Service"：Service for Secure Access to Office

Junichi Haseba, Yoshiaki Kioka

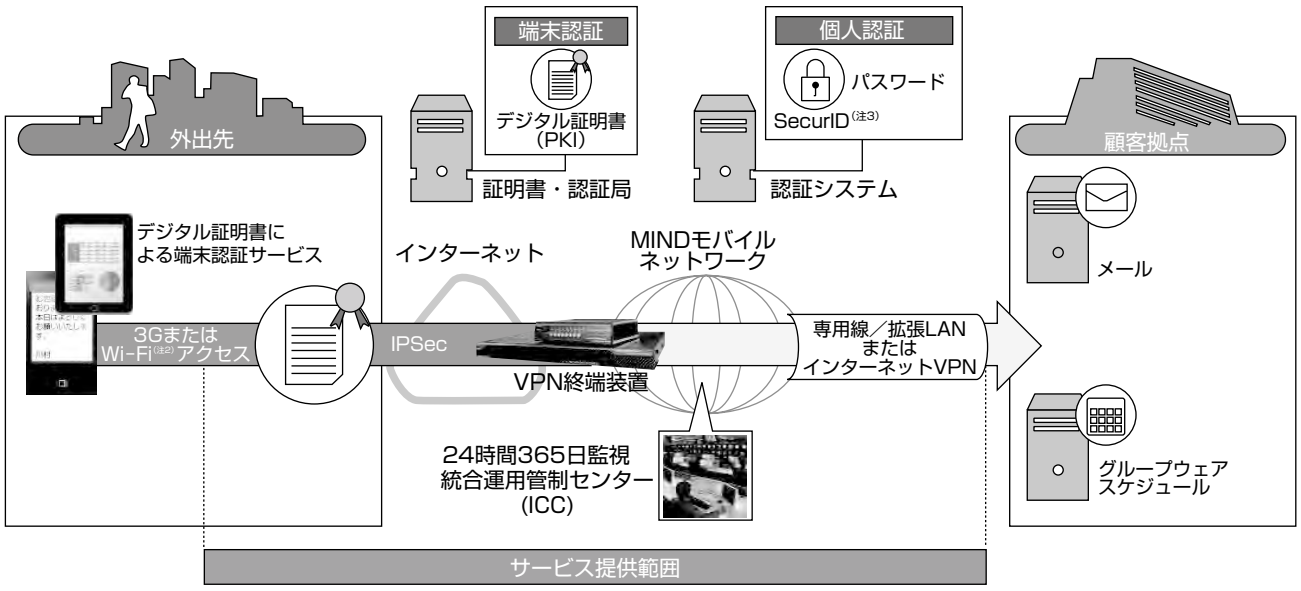
要　旨

三菱電機情報ネットワーク㈱(MIND)のモバイルネットワークサービスは，顧客の業務システムを社内利用と同様にリモートから安全・安心にアクセスできるリモートアクセスサービスを提供し，企業ユーザーから高評価を得ている。ネットワークの設計・構築・稼働後の運用保守，アウトソーシングまでをMINDがワンストップで提供し，ユーザーはモバイル端末を用意するだけでリモートから社内業務システムが利用可能となる。iPhone／iPad(注1)の市場投入を皮切りに，モバイル端末の利用ニーズは，従来のモバイルパソコン主体から手軽で操作性が優れた端末として注目されているスマートフォン／タブレット端末に移ってきている。

一方，セキュリティ面では，従来のモバイルパソコンと同等のセキュリティレベルを維持しつつ，スマートフォン／タブレット端末特有のセキュリティ対策を必要とすることから，導入に踏み切れない企業も少なくない。

MINDは，それらの課題を“セキュアスマートフォンアクセスサービス”“スマートフォンマネージサービス”を提供することで解消し，スマートフォン／タブレット端末でも利便性とセキュリティを兼ね備え，快適・安心に利用できるリモートアクセスを実現した。“セキュアスマートフォンアクセスサービス”は，現行のモバイルネットワークサービスのユーザーID認証及び暗号化通信に加え，証明書による“端末認証”を組み合わせ，許可された端末のみ社内の業務システムにアクセス可能にしている。スマートフォンマネージサービスは，スマートフォン／タブレット自体の端末管理を可能とし，紛失時に遠隔で端末ロック・データ消去を可能とした。

（注１）　iPhoneとiPadは，Apple Inc. の登録商標である。



（注2）　Wi-Fiは，Wi-Fi Allianceの登録商標である。
（注3）　RSA SecurIDは，EMC Corp. の登録商標である。

3G　：3rd Generation
IPSec：Security Architecture for Internet Protocol
PKI　：Public Key Infrastructure
VPN　：Virtual Private Network

“セキュアスマートフォンアクセスサービス”の概要

セキュアスマートフォンアクセスサービスは，データ通信を暗号化（IPSec）しデジタル証明書による端末認証とユーザーIDとパスワードによる個人認証を組み合わせて，強固なアクセス制御機能を実現している。

*三菱電機情報ネットワーク㈱

1. まえがき

MINDのモバイルネットワークサービスは，1997年サービス開始当初から，顧客の業務システムを社内アクセスと同様にリモートから安全・安心に利用できることが特長で，ネットワークサービスの設計・構築・稼働後の運用保守，アウトソーシングまでをワンストップサービスとして提供している。今回，スマートフォン／タブレット端末を利用可能とした“セキュアスマートフォンアクセスサービス”と“スマートフォンマネージサービス”の提供を開始した。

本稿では，スマートフォン／タブレット端末利用における利便性とセキュリティを兼ね備えた“セキュアスマートフォンアクセスサービス”とスマートフォン／タブレット自体の端末管理を可能とした“スマートフォンマネージサービス”の特長やサービス内容について述べる。

2. 市場動向

2.1 スマートフォン／タブレット端末の市場動向

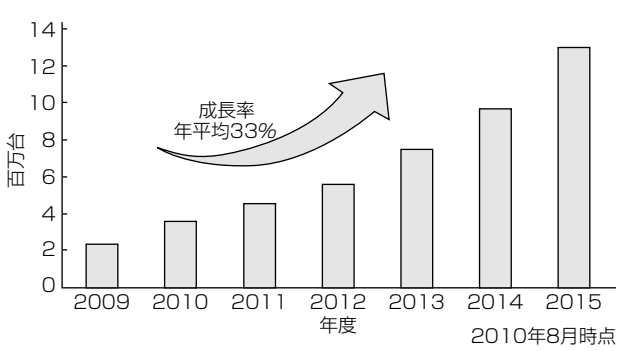
iPhoneの市場投入を皮切りにコンシューマー市場でスマートフォンが急速に普及し，国内のスマートフォン／タブレット端末の市場は，年平均33%のペースで成長している。2015年には1,300万台まで増えると予測されている（**図1**）。

モバイルパソコンに比べ手軽に持ち運べるというスマートフォン／タブレット端末の利便性から，企業でも社内の業務システムを利用するモバイル端末として顧客ニーズが高まっている。

2.2 顧客ニーズとセキュリティ課題

企業で，スマートフォン／タブレット端末は，モバイルパソコン並みの情報処理能力を持った多機能携帯端末ととらえられ，メールやグループウェアを外出先から効率的に活用できる新たなモバイル端末としての利用ニーズは高い。

一方で，企業が適用しているモバイルパソコンのセキュリティレベルを維持しつつ，スマートフォン／タブレット端末特有のセキュリティリスクを回避することが課題となっており，本格展開にまで至っていない企業も少なくない。



出典：日本スマートフォン市場分析2010，(株)ROA Group

図1．スマートフォン市場の規模予測（2009～2015年）

従来のモバイルパソコンに対して，スマートフォン／タブレット端末に特有な次のようなセキュリティリスクが考えられる。

(1) 端末が個人所有物であるケースが多くなり，場所や周りを気にせず利用する機会が増える。そのため，通信やユーザーID／パスワードの盗聴による脅威や企業が許可していない端末から不正アクセスされるリスクが大きくなる。

(2) 端末がモバイルパソコンと電話を兼ね備えた機能を保有しているため，企業の機密データだけでなくアドレス帳などの個人情報も保有することが多い。そのため，紛失・盗難時や多種多様なアプリケーションソフトウェアの利用時等における個人情報漏洩（ろうえい）の事故が発生するリスクが大きくなる。

2.3 企業が求めるスマートフォン／タブレット端末導入に必要なセキュリティ機能

企業がスマートフォン／タブレット端末導入に求めるセキュリティ機能を次に挙げる。

(1) 企業が貸与または許可した端末のみアクセスを許可
(2) 企業が許可したユーザーのみ社内へのアクセスを許可
(3) 業務システムとのデータ通信は暗号化
(4) 利用したアクセスログなどの収集管理
(5) スマートフォン／タブレット端末の状態管理
(6) 紛失による情報漏洩の防止と遠隔制御の実現
(7) 管理者が許可したアプリケーションソフトウェア以外の使用禁止

このような背景から，企業がモバイルパソコン利用に適用している情報漏洩対策のセキュリティ機能を継続しつつ，不許可端末の利用防止や端末の状態管理など，スマートフォン／タブレット端末に関する特有のセキュリティ対策について，モバイルネットワークサービスの機能拡充を図る必要があった。

3. リモートアクセスソリューション

3.1 セキュアスマートフォンアクセスサービス

ユーザーの社内システムへのアクセス制御機能（**2．3節**(2)），データ通信の暗号化機能（**2．3節**(3)），利用したアクセスログ等の収集管理機能（**2．3節**(4)）は，モバイルネットワークサービスの既存の認証システムと連携した仕組みを実現することで可能とした。

端末のアクセス制御機能（**2．3節**(1)）は，既存の認証システムにはなく，スマートフォン／タブレット端末の端末認証機能を加える必要があった。個々のスマートフォン／タブレット端末を識別し，3GモデルやWi-Fiモデルの機種に依存せず認証可能な仕組みとして，端末識別情報に紐（ひも）づけたデジタル証明書による端末認証を搭載した。デジタル証明書による認証の仕組みは次のとおりである（**図2**）。

①端末識別情報を基に指定端末のデジタル証明書を発行

する。

②発行されたデジタル証明書を指定端末にインストールする。インストール時に指定端末であるかを証明書認証局で認証し，認可されればインストールされる。

③デジタル証明書がインストールされたスマートフォン／タブレット端末からVPN(Virtual Private Network)クライアントソフトウェアを利用しIPSec集線装置に接続する。IPSec集線装置で，アクセス許可されたデジタル証明書であるかの認証を実施する。アクセス許可された端末であれば認可し，許可されていない端末であれば拒否する(端末認証)。

④認証システムで，ユーザーID及びパスワードの認証を実施する。アクセス許可されたユーザーID及びパスワードであれば認可し，許可されていないユーザーID及びパスワードであれば拒否する(個人認証)。

⑤端末認証及び個人認証で許可された端末かつユーザーのみ，アクセス回線経由で業務用サーバにアクセス可能となる。

3.2 スマートフォンマネージサービス

スマートフォン／タブレット端末の状態管理(**2. 3節**(5))，紛失による情報漏洩の防止や遠隔制御(**2. 3節**(6))，管理者が指定したアプリケーションソフトウェア以外の使用禁止(**2. 3節**(7))を実現し，管理者に代わってMINDが“スマートフォンマネージサービス”として提供する。

このサービスは，複数のスマートフォン／タブレット端末を企業のセキュリティポリシーで管理・監視・制御することを可能としている。また，利用端末の機種やインストールされているアプリケーションなどの情報を収集する機能を有し，インベントリ情報を可視化できる。**図 3** にスマートフォンマネージサービスを示す。

このサービスの機能は，①セキュリティ機能，②ポリシー管理機能，③端末管理機能の 3 つに分類される。それぞれの主な機能を**表 1**，**表 2**，**表 3** に示す。

スマートフォンマネージサービスは，Apple社から提供されているiPhone／iPad iOS4.0で制御可能な端末管理“モバイルデバイスマネジメント(MDM)”の仕組みを利用

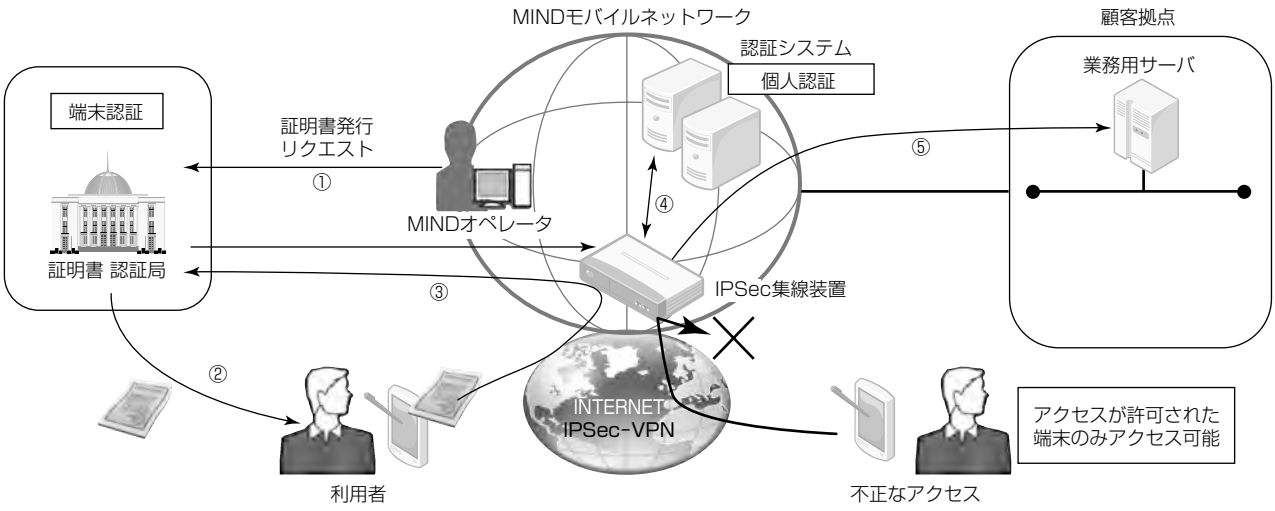


図 2．デジタル証明書による認証

エンドユーザーに配布されたスマートフォン端末を遠隔制御・状態管理し，情報漏洩防止を実現
⇒ 盗難・紛失時の端末ロックやデータ消去
⇒ 許可されたアプリケーションソフトのみ利用，不許可アプリケーションソフトを削除

顧客に代わり，管理者から命令を送信(運用代行)，
日常運用はもちろん，いざという時にも，すばやく確実に対応！

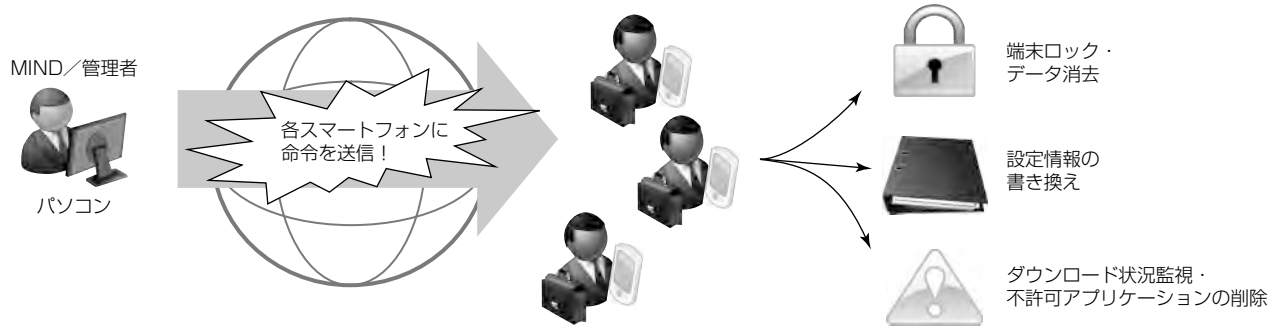


図 3．スマートフォンマネージサービス

表1．主なセキュリティ機能

機能名	内容
リモートワイプ	データ消去(工場出荷時に初期化)
リモートロック・アンロック	ロック・アンロックの実行
必要なパスコード数	最小パスコード長の設定
パスコード更新頻度	パスコードの更新頻度の設定
許容される失敗数	パスコードの失敗回数の設定

表2．主なポリシー管理機能

機能名	内容
アプリケーションのインストール	新たなアプリケーションのインストール可否
カメラの使用	カメラの利用可否
画面キャプチャ	画面キャプチャの実行可否
Safari(注3)の利用	Safariの利用可否
YouTube(注4)の利用	YouTube利用の実行可否

(注3)　Safariは，Apple Inc. の登録商標である。
(注4)　YouTubeは，Google Inc. の登録商標である。

表3．主な端末管理機能

機能名	内容
Wi-Fi設定	Wi-Fiのアクセスポイント情報の設定
ネットワーク接続	ネットワーク接続に関する設定追加
VPN設定	VPN構成の情報設定

している。MDMの動作を**図4**に示す。

①モバイルデバイス管理サーバ(MDMサーバ)の情報を含む構成プロファイルをデバイスに送る。送信手段としては，3G回線やWi-Fi又は送信用パソコンからUSB(Universal Serial Bus)で送信する。

②送信された構成プロファイルをデバイスにインストールしてMDMサーバから管理されることを許可する。

③デバイスにインストールされるとデバイス情報がMDMサーバに配送され，管理対象のデバイスとして登録される。

④管理対象として登録されたデバイスに対し，APNs(Apple Push Notification service)サーバを介し対象デバイスに通知が行われ，その後MDMサーバからデバイスのポリシーコントロールが行われる。

⑤対象デバイスへのポリシー設定は，管理者がMDMサーバから対象デバイスに指示・要求することで行われる。

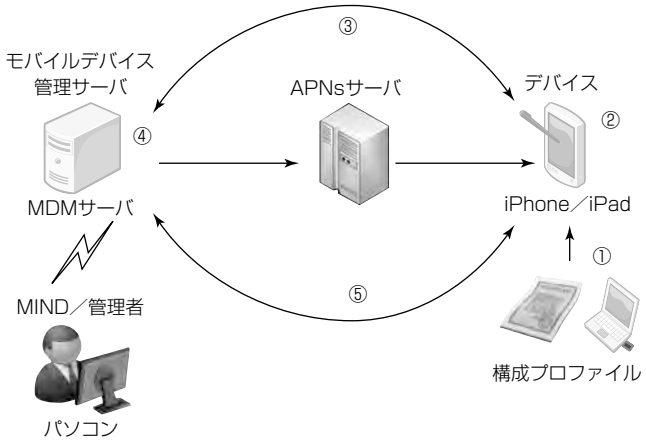


図4．モバイルデバイスマネジメントの動作

“セキュアスマートフォンアクセスサービス”“スマートフォンマネージサービス”が提供する機能によって，モバイルパソコンと同等のセキュリティポリシーやソリューションを適用することができ，手軽で操作性を損なわないというスマートフォンの特長を生かしつつ，リモートから社内の業務システムを安心・安全に利用できる。

4. 今後の課題

スマートフォン市場では，iOSを内蔵したiPhone／iPad以外にAndroid(注5)OSを内蔵したスマートフォン／タブレット端末も多く出荷されている。現在MINDが提供している“セキュアスマートフォンアクセスサービス”“スマートフォンマネージサービス”は，iPhone／iPadに対応しているが，Android OSのスマートフォン／タブレット端末も今後サポートする予定である。Android OSでのサービス提供機能の検証を行い，サービスメニューの拡充を図っていく。

(注5)　Androidは，Google Inc. の登録商標である。

5. むすび

ITの技術進歩や利用環境の多様化から，リモートアクセスの分野でもITシステムにおけるネットワークサービスが複雑化している。常に利用者のワークスタイルにあったサービス提供を心掛ける必要があり，今後も顧客ニーズをとらえ，快適・安全に利用できるネットワークを継続提供していく所存である。

特集論文

スマートデバイス向け証明書発行サービス

小俣三郎*
田口拓也*
向江勇気*

Certificate Issuing Service for Smart Device

Saburo Omata, Takuya Taguchi, Yuki Mukae

要　旨

近年，iPhone／iPad(注1)及びAndroid(注2)を搭載したスマートデバイスが普及してきている。これらは個人ユーザーの一般利用だけではなく，企業においても重要な情報ツールとなりつつある。一方，スマートデバイス携帯時の盗難・紛失等による個人情報漏洩(ろうえい)やなりすましといったセキュリティ上の観点からも，スマートデバイス自体を認証する端末認証のニーズが高まってくる。

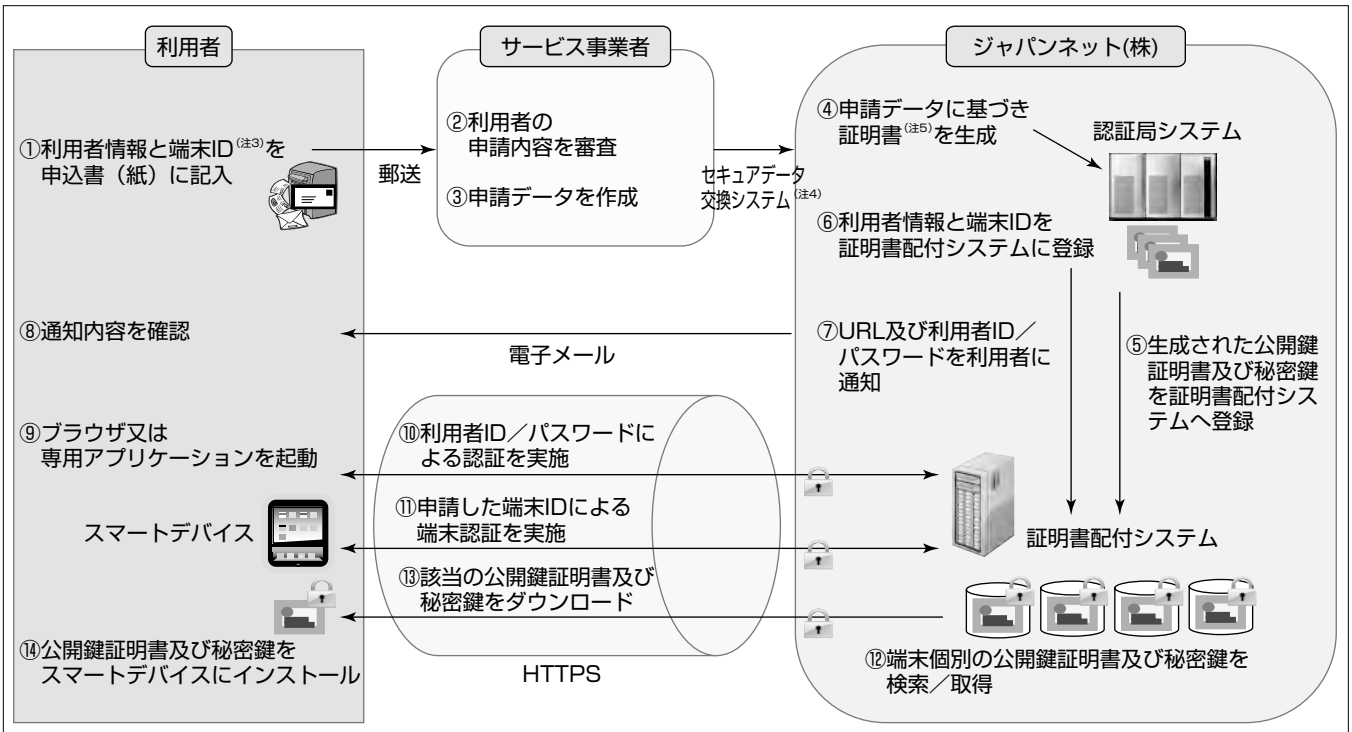
そこで，ジャパンネット㈱では，スマートデバイスに対して安全かつ確実に電子証明書を発行・配付することを目指して，スマートデバイス向け証明書発行サービスの検討を実施した。検討に当たっては，iPhone／iPad及びAndroidの仕様を調査し，方式の統一を図った。

本稿では，スマートデバイス向け証明書発行サービスの実現方法などの技術的特長を述べる。

スマートデバイス向け証明書発行サービスでは，事前にスマートデバイスの端末ID(IDentifier)情報を利用者から申請し，その端末IDに基づいて証明書を発行する。また証明書配付システムでは，なりすまし等を防止するために，①利用者ID／パスワードによる利用者認証，②端末IDによる端末認証という二要素認証を実施するよう，システムを設計した。

今後は，サービスフローの詳細を確定させ，オンデマンドITサービスとして主に企業向けのスマートデバイスに対する証明書発行サービスを提供していく。

（注１）　iPhone，iPadは，Apple Inc. の登録商標である。
（注２）　Androidは，Google，Inc. の登録商標である。



(注3)　端末ID：MACアドレスなどのスマートデバイス固有の端末識別情報またはそれらの組み合わせ
(注4)　セキュアデータ交換システム：データ送受信のためのWebシステム
(注5)　証明書：PKIにおける公開鍵証明書

HTTPS：Hyper Text Transfer Protocol Security
MAC　：Media Access Control
URL　：Uniform Resource Locator

スマートデバイス向け証明書発行サービスの概念図

企業におけるスマートデバイス利用拡大に伴い，スマートデバイスでのPKI（Public Key Infrastructure）利用のための電子証明書を発行するサービスを提供する。スマートデバイスのポータビリティを考慮し，盗難・紛失等による個人情報漏洩やなりすましのリスクを低減するため，利用者認証及び端末認証による二要素認証を導入した上で電子証明書を配付する。

*三菱電機情報ネットワーク㈱

1. まえがき

ポータビリティ，操作性の高さ，機能の豊富さから，近年多くの企業がiPhone／iPadやAndroid端末といったスマートデバイスに注目している。スマートデバイスを用いることで業務の効率化を期待できる一方で，個人情報漏洩やなりすまし等のセキュリティ上の問題も顕在化するおそれがある。そこで注目されているのが，PKIを利用した端末認証である。

三菱電機グループのジャパンネット㈱は，官公庁・自治体が実施している電子入札や電子申請への参加者（一般企業や団体 等）を電子的に特定するために使用する電子証明書の発行サービス事業を行っている。また，医療や金融，一般ビジネス分野における認証や署名用途で使用する各種の電子証明書の発行サービスを行っている。現在発行している電子証明書は人物を特定するための証明書であるが，最近のスマートデバイスは様々な場面で利用されるケースが増えており，今後は利用する端末を特定するための端末認証用証明書の必要性が高まってくる。

本稿では，スマートデバイス向け証明書発行サービスに関する実現方法などの技術的特長について述べる。

2. 証明書の利用法及び検討方針

2.1 証明書の利用法

端末認証用証明書の利用法として，パソコンでは一般的に広く利用されているHTTPS（SSLクライアント認証），及びVPN（SSL-VPN(注6)及びIPSec(注7)）での利用を想定している。これらの機能はiPhone／iPadでも標準機能として搭載されており，例えばHTTPSによってSSLクライアント認証を必要とするサービスに接続して情報を取得することや，SSL-VPNで外出先から社内ネットワークに接続し，Webメール，グループウェア，スケジュール管理等のWebアプリケーションにアクセスすることで社外から安全に業務を行うことが可能になる。

2.2 実現方法などの検討方針

iPhone／iPadでもAndroid端末でもL2TP(注8)，PPTP(注9)，IPSecをサポートしている。ただしAndroid端末では標準機能でSSLクライアント認証ができないことや，独自の認証局を信頼点として設定するために複雑な操作を必要とするという課題がある。

（注6） Secure Sockets Layer-Virtual Private Networkの略。SSLを利用したVPNの一種。
（注7） Security Architecture for Internet Protocolの略。IPパケット単位で改ざん防止や秘匿機能をもったプロトコル。
（注8） Layer 2 Tunneling Protocolの略。VPNのためのトンネリングプロトコル。
（注9） Point to Point Tunneling Protocolの略。Point to Point Protocolを拡張したトンネリングプロトコル。

このような証明書の利用法及び課題を踏まえながら次の方針で検討する。

①ユーザーの利便性を損なわない
②スマートデバイスの種類に依存しない

3. スマートデバイス向け証明書

3.1 端末IDの確認方法

このサービスの利用者は，証明書の発行申込みを行う際に，まず発行対象となるスマートデバイスが固有に持っている端末IDを確認して申請する必要がある。端末IDを確認する方法に関しては，iPhone／iPadの場合，設定画面またはiTunes(注10)の画面に**表1**に示すような端末IDが表示される。Android端末の場合，設定画面または機種によって表示可否の差はあるが，専用アプリケーションを実行することによって端末IDを表示できる。

（注10） iTunesは，Apple Inc. の登録商標である。

3.2 端末IDの種類と証明書格納情報

今回検討した証明書発行サービスでは，iPhone／iPadまたはAndroid端末自体に対して電子証明書を発行するが，電子証明書のSubjectというエリアに個々のスマートデバイスの端末ID情報を格納することとしている（**表2**）。ただし，利用者が複数サービスで同じ証明書を利用するケースでは，証明書内に端末IDを格納することで第三者が証明書に格納された端末固有情報を収集，分析することができる場合もあり，結果として端末固有情報を追跡される可能性もある。そのため端末IDを格納するか否か，及び格納する場合でもどの端末IDを格納するか，についてはサービス事業者または利用者によって選択可能としている。また，スマートデバイスの利用年数に応じて，証明書の有効期間も1，2，3，5年から選択可能とし，**表1**に示すIDを証明書のSubjectエリアに格納する。

表1．端末ごとの端末ID及び表示方法／取得方法

端末のOS	取得可能な端末ID	端末での表示方法／取得方法
iOS（iPhone／iPad）	UDID（Unique Device Identifier）	iTunesで表示可能
	IMEI（International Mobile Equipment Identity）	設定画面またはiTunesで表示可能
	ICCID（Integrated Circuit Card ID）	設定画面またはiTunesで表示可能
	MACアドレス	設定画面またはiTunesで表示可能
Android（Galaxy Sの例）	IMEI（or MEID）	OSによって提供される機能で取得可能（android.telephony.TelephonyManagerクラスのgetDeviceId()メソッド）
	MACアドレス	設定画面で表示可能
	IMSI（International Mobile Subscriber Identity）	OSによって提供される機能で取得可能（android.telephony.TelephonyManagerクラスのgetSubscriberId()メソッド）

4. 証明書配付システム

この章では，証明書配付システムの認証方式及び配付方式について述べる。証明書配付システムでは**図1**のように利用者からの申込みに応じて証明書を生成し，配付システムに登録後，利用者認証及び端末認証を経て証明書を配付する。

4.1 利用者及び端末の認証方式

この証明書発行サービスは，次の手順にしたがってスマートデバイス向け証明書を生成する。

⑴ 認証局システムで鍵ペア(秘密鍵と公開鍵)を生成する。

⑵ 生成した公開鍵に対して利用者からの申込み内容に沿って証明書を生成する。

⑶ 証明書と秘密鍵を合わせてPKCS#12(注11)データとしてスマートデバイスに配付する。

手順⑴においては，鍵ペアを認証局が生成する方法と，スマートデバイスが生成する方法が考えられるが，今回は次の理由によって，認証局システムで鍵ペアを生成することにした。①ハードウェア性能などによって，乱数(または乱数の種)として物理乱数など安全性の高い乱数を使用することが可能で，鍵ペアの品質を安定できること，②鍵紛失時に鍵を復元可能とするためのキーアーカイブが可能であること，③スマートデバイス側での利用者によるCSR(Certificate Signing Request)の生成操作が不要。

手順⑶において，PKCS#12データをスマートデバイスへ配付する際は，利用者のなりすまし，及びスマートデバイスのなりすましを防止する必要があるため，利用者ID／パスワードによる利用者の認証，及びスマートデバイスを個別に識別・特定することによる端末認証をともに実施することとしている。

iPhone／iPadのOSであるiOSでは，多数のデバイスの構成情報を一括で設定するために，構成プロファイルと呼ばれるXML(eXtensible Markup Language)(注12)ファイルを使った設定方式[1][2][3]がOSの標準機能として搭載されている。

この機能の一つとして，サーバがスマートデバイスの各種端末ID情報(UDID，IMEI，ICCID，MACアドレス等)を取得する機能がある。この機能によってサーバが認証する必要のある端末IDを細かく指定して要求することができ，またはサービスの種類に応じてサーバが必要とする端末IDのみを認証するといった認証方式が可能である。

一方Androidでは，iOSのようなサーバによる構成プロファイルを利用した端末IDの取得機能はないが，android.telephony.TelephonyManagerクラスから端末IDを取得[4]してサーバに送信するアプリケーションを事前に作成してインストールすることによって，サーバ側ではiPhone／iPadかAndroid端末かを区別する必要なく同じプロトコルで認証及び証明書配付を実施できるようにした。

(注11) Public-Key Cryptography Standard #12の略。RSAセキュリティ社考案の秘密鍵及び証明書を保管するフォーマットの定義。

(注12) 文書やデータの意味や構造を記述するためのマークアップ言語の一つ。

表2．スマートデバイス向け証明書のプロファイル例

領域名		規定内容と設定値
基本部		
version		2(v3)
serialNumber		1001(例)
signature		sha1WithRSAEncryption(ハッシュ，暗号アルゴリズム)
validity		
	notBefore	有効期間(1 or 2 or 3 or 5年)
	notAfter	
issuer		c＝JP（国名）
		o＝Enterprise Premium Service(JNのサービス名称)
		cn＝EnterPrise Premium CA(JNの認証局システム名)
subject		c＝JP
		o＝ABC Corporation(会社名英語(オプション))
		ou＝XYZ Department（部署名英語(オプション))
		ou＝xxxxxxxx(所属又は固有番号等英語(オプション))
		cn＝xxxxxxxx(デバイス識別子英語)
subjectPublicKeyInfo		証明書所有者の公開鍵情報
	algorithm	rsaEncryption(暗号アルゴリズム)
	subjectPublicKey	RSA公開鍵値(1,024bit or 2,048bit)

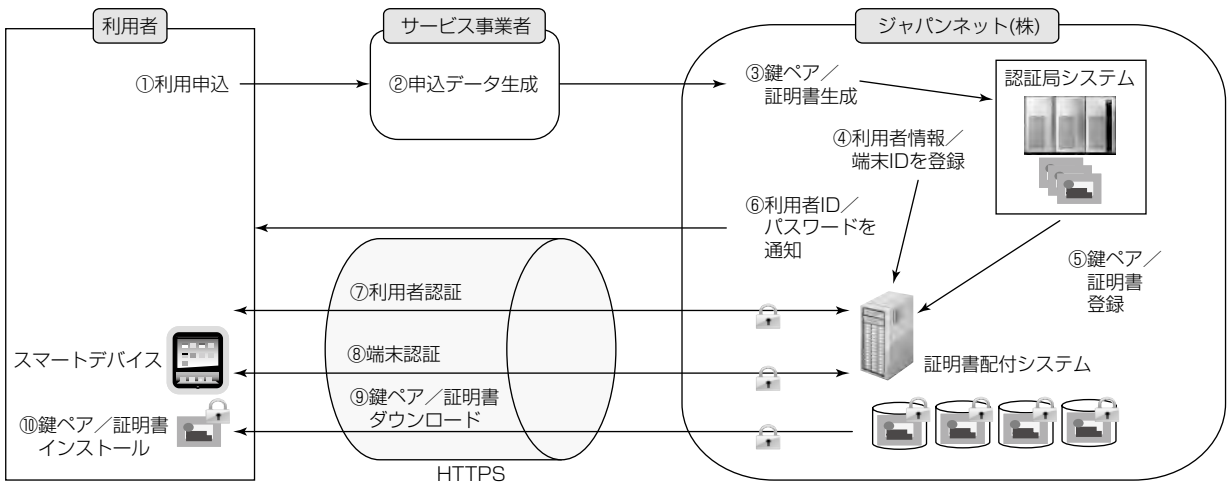


図1．証明書配付システム

4.2 証明書の配付方式

iPhone／iPadでは，無線経由のプロファイル配信とプロファイルによるデバイスの一括設定が可能であり，①認証フェーズ，②証明書の登録フェーズ，③デバイスの構成フェーズという3つのフェーズで構成されるプロトコルを標準でサポートしている。このうち②の証明書の登録フェーズでは，iPhone／iPad側で証明書申請のためのCSRを作成して認証局に送信することで証明書の発行を行うようになっている。

ジャパンネット㈱では，先に述べたとおり認証局で鍵ペアを生成する方式を採用しているため，iPhone／iPadにおける無線経由のプロファイル配信とデバイスの構成のプロトコルをそのまま適用することはせず，①の認証フェーズのうち，サーバがiPhone／iPadの端末IDを取得する機能，及び②の証明書の登録フェーズのスキームを組み合わせることによって，**図2**のような独自の証明書配付方式を採用することにしている。

iPhone／iPadでは，先に述べた構成プロファイルを使って証明書を端末に配付することが可能であるが，Android端末には標準でこのような機能はない。ただし，AndroidはOSとしてPKIの機能自体は持っており[5]，アプリケーションとしては実装可能である。

そこで，ユーザーインタフェースや認証，証明書配付のプロトコルを統一するため，Android端末用のアプリケーションを開発し，擬似的にiOSと同様にXMLを処理することによって，XMLデータとして送られてきたPKCS#12データを端末にインストールさせることにした。

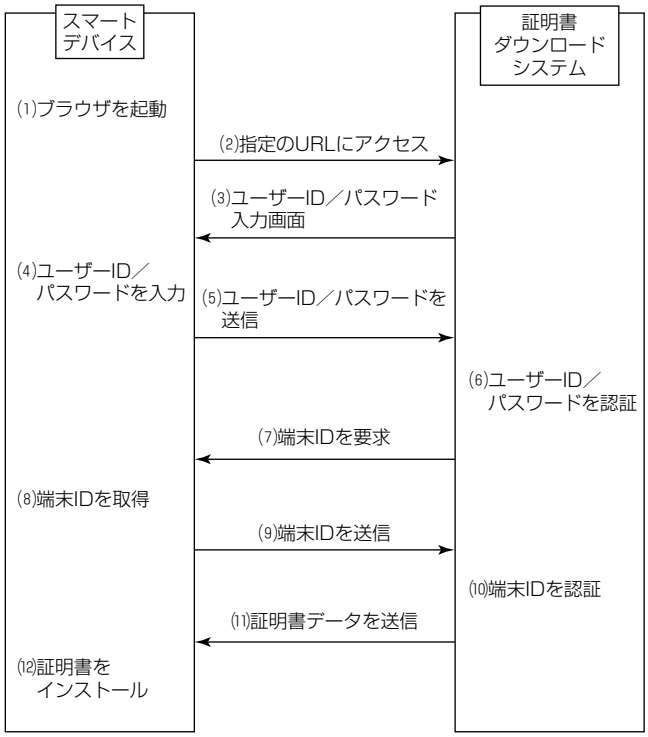


図2．iPhone／iPadの認証方式及び証明書配付方式

5. むすび

iPhone／iPad及びAndroid端末のようなスマートデバイス用OSの機能やユーザーインタフェースなどの特徴を考慮した上で，利用者の利便性を重視した端末認証用証明書の発行サービスの検討内容を述べた。この検討内容は，①証明書配付時に利用者認証及び端末認証の二要素認証を実施し，②iPhone／iPadまたはAndroid端末のOSの種類によらず，同じプロトコル，同じユーザーインタフェースで証明書のインストールが実施できることを特長としており，また，配付可能期間などの運用上必要なパラメータを他社と比較して細かく設定できるようにするなどの工夫をした。今後は，この検討結果を踏まえてシステムの構築及びサービスの提供を行う。

iPhone／iPad及びAndroid端末のようなスマートデバイスが今後，医療，金融，一般ビジネス分野の場において広く普及していくと考えている。また同時に，そのスマートデバイスのポータビリティ性ゆえに，セキュリティがより重要になってくると想定しており，デバイスを認証するための電子証明書のニーズも一層高まってくると考えている。

例えば，医療分野ではスマートデバイスの利用による医療の高機能化が期待されており，在宅医療，在宅介護，訪問薬剤師，電子カルテ，救急病院間の情報共有システムへの適用，又は医師による遠隔診断や治療補助，看護師による急病患者のトリアージ（重症度と緊急性によって傷病者を分別し，治療の優先度を決定すること）等，高い注目を集めている。

今まで人物を認証するための様々な電子証明書を発行してきているが，これまで培ってきた認証局ノウハウを最大限に活（い）かしながら，端末認証用の電子証明書発行に取り組むことによって，電子証明書発行サービス事業の据野を拡大するとともに，安心・安全な社会を下支えすることを目指していきたい。

参考文献

⑴ Apple Inc.，無線経由のプロファイル配信と構成（2010）
⑵ Apple Inc.，iPhone OSテクノロジーの概要（2009）
⑶ Apple Inc.，iPhone OS エンタープライズ配備ガイド，第2版（2010）
⑷ public class Telephony Manager, http://developer.android.com/reference/android/telephony/TelephonyManager.html
⑸ package java. security, http://developer.android.com/reference/java/security/package-summary.html

特集論文

FAXOCRサービス“MELFOS on Demand”

上田　稔*　小野健一*
石川浩通*
滝田健司*

FAXOCR Service "MELFOS on Demand"

Minoru Ueda, Hiromichi Ishikawa, Kenji Takita, Kenichi Ono

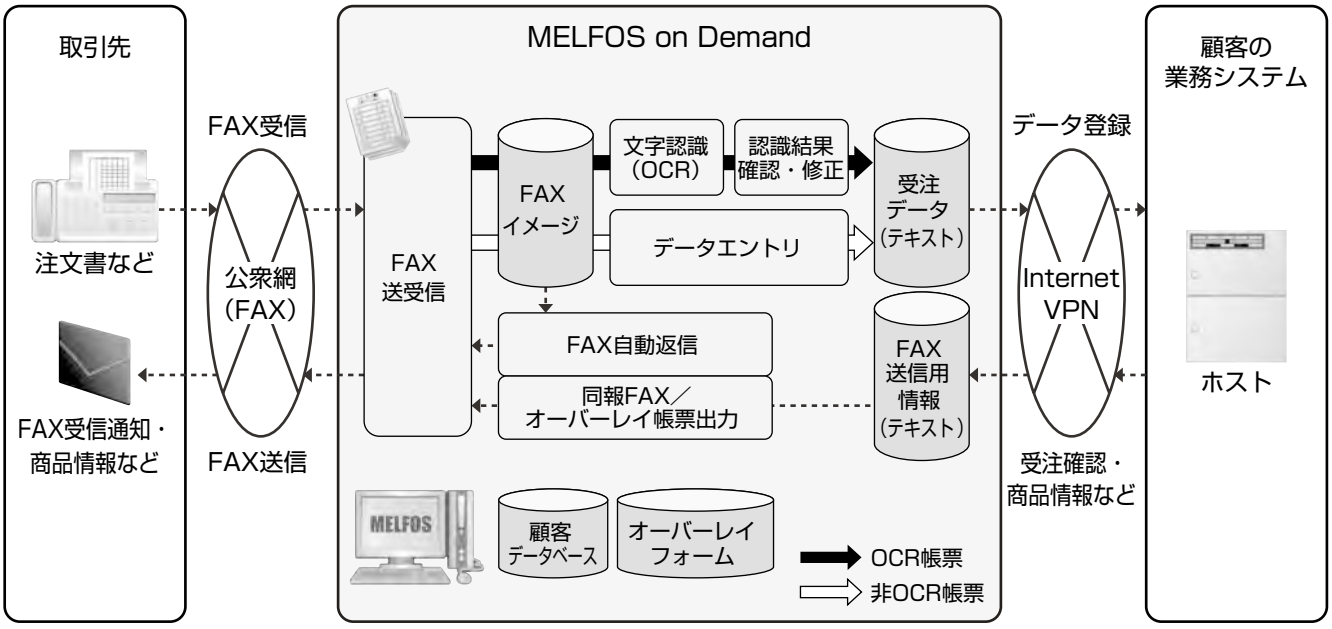
要　旨

IT（Information Technology）アウトソーシングの国内市場は，平均約4％の右肩上がりの成長を続けており，企業内におけるITリソースへの利用者マインドは“所有”から“利用”へと大きく転換しつつある。特にSaaS（Software as a Service）に代表されるオンデマンドITサービスは，運用コスト削減や業務効率化，最新技術の容易な活用，業務量の変動に応じたITリソースの投入等のメリットがあるため企業ユーザーから導入の期待が大きい。

“三菱FAXOCRシステム MELFOS”（以下“MELFOS”という。）は，1999年の販売開始以後，FAX特有の悪条件に対応した自社開発の認識エンジンを強みとして着実に実績を重ね，200社以上の豊富な販売実績がある。一方で，業務量が少ない顧客，繁忙期に極端に業務量が集中する顧客への導入がなかなか進まないという問題があった。

このような背景から，オンデマンドITサービス市場に対応した“MELFOS on Demand”の事業化を計画し，2010年6月に三菱電機インフォメーションシステムズ㈱（MDIS）初のサービス事業として広報発表し，2010年10月にサービス提供を開始した。迅速なサービス開始を目指し，既存のシステム導入型MELFOSのソフトウェア資産を最大限に活用しながら，サービス提供基盤の設計・構築を進めた。

“MELFOS on Demand”は，MELFOS独自の認識技術などの優位性を継承するとともに，業務に併せて必要なサービスのみ利用することを可能としており，これまでFAXOCRシステムの利用が難しかった顧客への提供が可能となった。



OCR：Optical Character Recognition

MELFOS on Demandを活用したFAX受注業務の流れ

①取引先からのFAX受信は“FAX受信サービス”で行われる。受信したFAXは画像ファイルとなる。②“文字認識（OCR）サービス”によって，認識が行われ，結果がテキスト情報で出力される。③認識結果は受注データとしてInternet－VPN（Virtual Private Network）経由でサービス利用顧客のシステムへ伝送される。伝送する前に“認識結果確認・修正サービス”を利用して確認・修正を利用顧客側で行える。又は“データエントリーサービス”によってMDISが確認・修正をしてから顧客側業務システムに渡すこともできる。④FAX受信時に“FAX自動返信サービス”によって受付通知をFAX送信できる。⑤“同報FAX／オーバーレイ帳票出力サービス”によって顧客側システム出力のテキスト情報を帳票にオーバーレイしてFAX送信できる。

*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FAXOCRシステム MELFOSは，ファクシミリ送信された手書きの文字を自動認識し，コンピュータで処理可能なデータに変換するシステム製品である。1999年の販売開始以降，FAXに特有な文字の傾斜やかすれがあっても文字の読み取りに強く，200社以上の豊富な販売実績があるロングセラー製品となっている。また，MDISの技術，導入実績，社会貢献度が高く評価され，2009年6月に画像電子学会から“画像電子技術賞”を受賞した。

“MELFOS on Demand”は，このMELFOSが持つ機能を，初期費用を抑えたSaaS型サービスで提供するものである。

本稿では，“MELFOS on Demand”の提供を開始するにあたり実施したビジネスモデルの検討やサービス提供基盤(設備)構築の課題解決方法について述べる。

2. オンデマンドITサービス市場への対応

2.1 ITアウトソーシングの国内市場の動向

2007年度から2013年度まで平均4.3%の右肩上がりの成長を続け，2013年度には，3兆1305億円に到達すると予測されている(**図1**)[(1)]。これは，企業内におけるITリソースへの利用者マインドが“所有”から“利用”へ大きく変化した表れである。

ITアウトソーシング市場での，企業におけるASP(Application Service Provider)サービスやSaaSの利用比率については，2007年度が12.6%であったのに対し，2009年度では20%と増加しており，“今後利用予定”も含めると38.6%と着実な浸透が伺える[(2)]。

サービス利用のメリットとしては，①コスト削減や業務効率化を実現できる，②最新技術を手軽に利用できる，③業務量や負荷の変動リスクの回避，④事業継続計画(Business Continuity Plan：BCP)の導入等がある。一方，課題としては，①既存システムとの連携が難しい，②重要データを社外に持ち出すことによる漏洩(ろうえい)リスクといった点が挙げられている[(3)]。

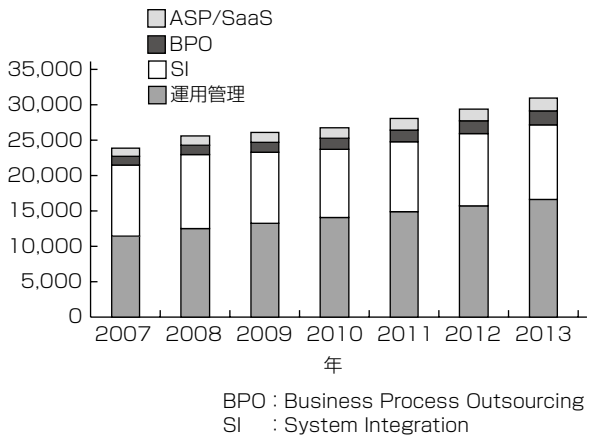


図1．ITアウトソーシングサービス市場の動向[(1)]

2.2 MELFOS事業分野での顧客ニーズの変化

MELFOSの既存顧客や事業分野でも，2009年頃から同様な変化が生じつつある。例えば，ワールドワイドで“FAXサービス”を展開する事業者の登場によって，このようなサービスを活用したいというニーズの増加や，エントリー業務自体を自社運用ではなく，アウトソーシングしていく動きなどが出てきた。

2.3 MELFOSの“on Demand”化

これらの背景によって，MELFOSのサービス型事業への対応を目指し，これまで蓄積してきた優位性のある技術の有効活用を基本として，サービス型の“MELFOS on Demand”の方式検討を進めた。

3. 新たな利用範囲の分析

“MELFOS on Demand”の提供を開始するにあたり，**2章**で述べた市場及び顧客のニーズ変化の分析とともに，これまでのシステム導入型のMELFOS事業で採用が進まなかった原因の分析を行い，次のような新たな利用範囲を定義した。

3.1 業務量視点での分析

特定の数日や時間(締め日，締め時間)に極端に業務量が集中する業務では，ピークとなる特定の期間に対応したFAX回線数キャパシティを用意すると，平準時には余剰な設備となる(**図2**の新利用範囲1)。また，システム導入時の初期費用は，最低でも数百万円になるため，業務量が少ない顧客の場合は，投資対効果が十分に得られず導入が進まない(**図2**の新利用範囲2)。

“MELFOS on Demand”の場合は，MDISがシステム設備(ITリソース)を提供するため，少ない初期費用で利用可能

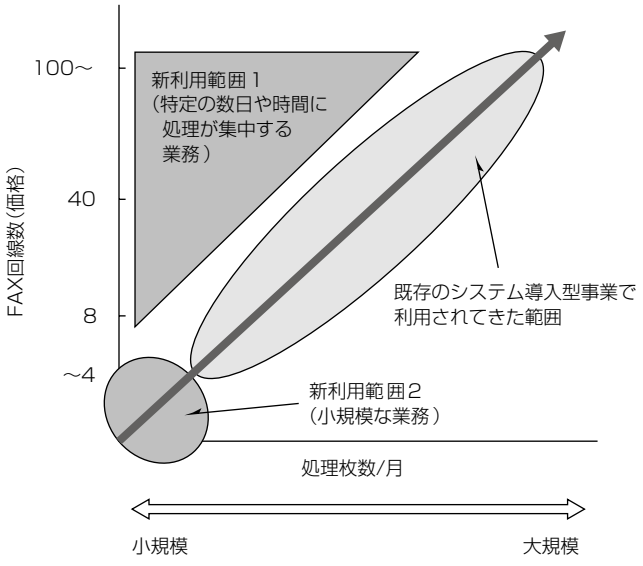


図2．業務量視点での分析

であり，かつ業務量(使用量)に応じた“従量制の費用”となり，“ピークに合わせた余剰な設備”を持つ必要がなくなる。

3.2 システム運用視点での分析

システムを自社導入した場合，導入した設備の管理・運営を自ら行っていく必要があるが，サービス型の場合は，設備の管理・運営をサービスプロバイダが行うため不要である。従来は，単にこのシステム運用負荷の軽減を焦点としたニーズが主となっていたが，最近はこれに加え，BCPの重要性の高まりや，サーバ仮想化技術を用いることによるシステム復旧の容易性／バックアップ保持の容易性／スケールアウト(サーバ増設)の容易性に対する期待が増えてきている。さらには，受注エントリー等の“業務処理まで含めたBPO(Business Process Outsourcing)”のニーズに対応したエントリーサービスを提供することで，従来のシステム導入型(SI型)では利用が難しかった顧客でも容易に利用ができることになる。

4. サービス提供基盤の検討

SaaS型サービスでは，サービスプロバイダが持つITリソースを複数ユーザーが共用する“マルチテナント方式”であることが求められ，1台のサーバでより多くのテナントを稼働させることによって，低廉な利用料金を実現できる。

4.1 マルチテナントのためのデータ分離方式

マルチテナントを実現するためには，データ分離をアプリケーション～データベース～OS(Operating System)間のどの階層で実現するかによって，次の方式が考えられる。

(1) アプリケーションによるデータ分離

システムを構成するすべてのプログラムをマルチテナントに対応した処理に改修する方式

(2) データベースでのデータ分離

1つのOS上で，複数のシステムを起動してシステムで最小限のテナントの識別を行い，テナントごとに独立したデータベースを割り当てる方式

(3) OSでのデータ分離

1つのコンピュータ上で複数の仮想化したプラットフォーム(マシン，OS)を起動し，それぞれでシステムを稼働させる方式

各方式には，それぞれのメリット／デメリットがあるが，MELFOSの持つシステムごとのカスタマイズ性の高さを維持した上で，タイムリーなサービス開始(スピードを重視)を考慮して比較検討した結果，既存のMELFOSソフトウェアモジュールの改修が不要で，テナントごとのカスタマイズが容易な(3)のOSでのデータ分離，すなわち“プラットフォーム仮想化”の方式を選択した(**図3**)。

4.2 認識(OCR)処理部のマルチテナントの実現

一方，プラットフォーム仮想化方式のデメリットとして，仮想マシンを使用することによるITリソース効率の低下が懸念される。特にMELFOSの心臓部であるOCR処理部は，CPU(Central Processing Unit)使用率が高いプログラムである。このOCR処理部に関して，同一コンピュータ上で稼働数をどのように確保するかが，サービス実現に向けての最重要課題であった。

当初の検証では，CPU使用率に着目し，CPUのコア数と稼働可能なテナント数との関係の確認を進めたが，CPUコア数を増やしても処理可能なテナント数が頭打ちとなってしまう結果が得られた(**図4**の結果1)。分析を進めた結果，最終的にディスクI/O(Input/Output)がボトルネックとなっていることが判明し，高速なディスク装置を採用することによって，稼働可能なテナント数の目標が実現可能となった(**図4**の結果2)。

4.3 FAX送受信部のマルチテナント対応

MELFOSではサーバ内蔵型のFAXボードをハードウェアとして使用しており，これを制御するFAX送受信部は仮想マシン上では稼働できない。このため，密結合であるOCR処理部とのコンポーネントの分離を行い，異なるマシン上での稼働を可能とした(**図3**)。

また，1サーバで処理可能なFAX送受信量は，自(おの)

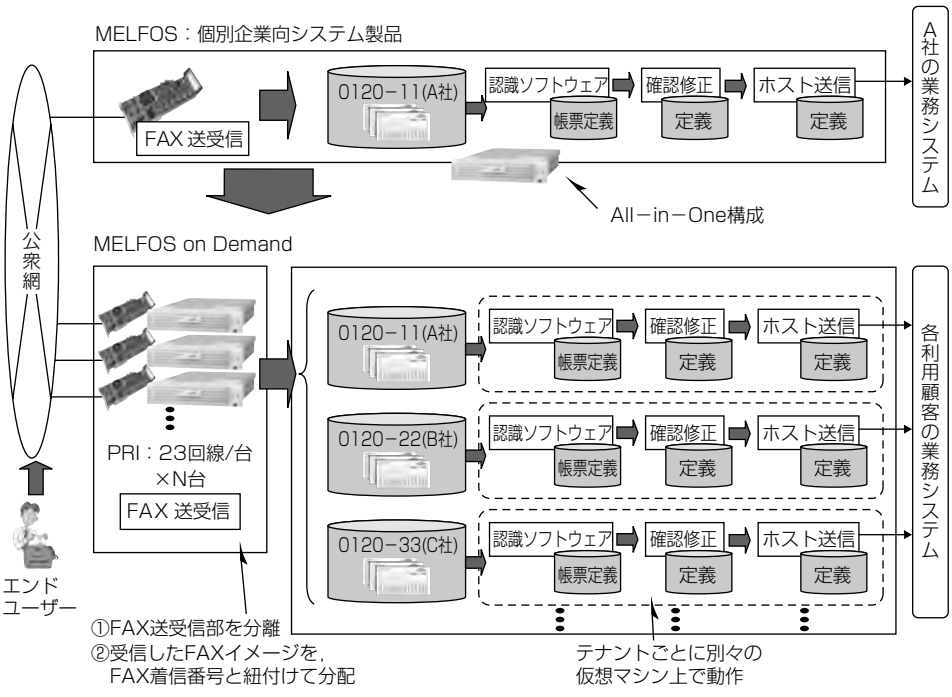


図3．実現したサービス提供基盤

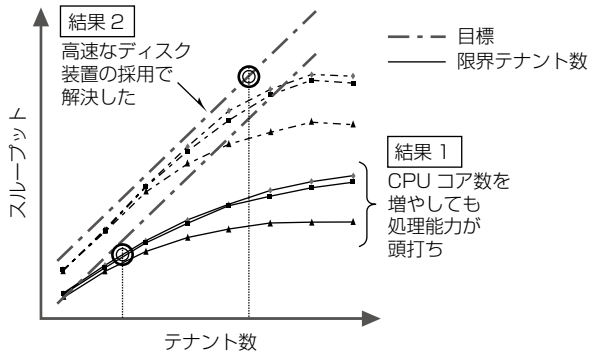


図４．OCR処理部の性能測定

ずと限界がある(サーバに搭載するFAXボードの回線数に左右される)。このためFAX回線は，回線集積度の高いPRI回線(Primary Rate Interface。国際電機通信連合が標準化したISDN(Integrated Services Digital Network)回線のインタフェース規格。通信速度は1.544Mbps。23通話回線相当)を採用することとした。使用業務量の少ない複数テナントを同一のFAX回線／サーバで共用するため，各テナントで異なったものになるFAX着信番号(ダイヤルイン番号)情報を，受信したFAXイメージと紐(ひも)付けて後続処理であるテナントごとに独立したOCR処理部に渡す機能を開発し，FAX回線のマルチテナント化を実現した(**図３**)。

さらに，FAX送受信処理量の急激な変動に対する設備の増強が間に合わない場合を考慮し，他社のFAX送受信サービスを活用することを視野に入れた連携機能の開発も同時に行った。

5. MELFOS on Demandの特長と機能

先に述べた事項を含め，“MELFOS on Demand”の特長と機能を次に述べる。

5.1 特　長

(1) 初期費用が少なくIT資産を抑制

FAX回線やFAXOCR用サーバが不要で初期導入コストやIT資産を抑制可能であり，締め日・締切り時刻などで処理が集中する業務でも余剰な設備は不要となる。

(2) MELFOSの評価の高い機能・性能を継承

従来のMELFOSの認識エンジンがそのままサービスで利用可能であり，人手での全件エントリーと比較して1/3から1/10の大幅な効率化ができる。また認識結果確認・修正サービスは，“急ぎ”の処理や“複雑な運用”を利用顧客が自社で実施できることを目的として提供を行っている。

5.2 機　能

従来のMELFOSを基本的に踏襲し，さらには必要な機能を必要な分だけ使うニーズの高いサービス型の特性を考慮し，“MELFOS on Demand”では次のサービスを提供している。

(1) FAX送受信サービスは，ニーズに応じて受信のみ／送信のみの利用が可能である。FAX送受信サービスは，あらかじめ登録してある帳票に指定の文字，イメージをオーバーレイしてFAX送信する。

(2) FAX自動返信・転送サービスは，FAX受信時に，あらかじめ設定された内容にしたがってFAX送信元への返信やFAX転送を自動で行う。

(3) 文字認識(OCR)サービスは，FAX受信した帳票から認識対象の文字をテキスト化(OCR)する。OCR専用帳票が必要になる。

(4) データエントリーサービスは，文字認識(OCR)サービスを活用し，認識結果確認修正まで実施したデータを出力する。文字認識ができないFAXへのこのサービス提供も行う。

(5) 同報FAX送信サービスは，あらかじめ登録してある帳票に指定の文字，イメージをオーバーレイして，指定された複数の送信先に同一内容をFAX送信する。

(6) FAX送受信データ照会サービスは，FAX送受信した履歴やイメージを画面で照会できる。

(7) 認識結果確認・修正サービスは，利用顧客が，自社の端末でMELFOSの認識結果確認・修正機能を使用できる。

6. むすび

“MELFOS on Demand”は既存製品の資産を最大限に活用し，MDIS初のサービス事業として迅速なサービス開始を実現した。広報発表以降，ユーザーから多数の引き合いを頂いており，MELFOS事業の裾野(すその)を拡(ひろ)げる成果は着実に得られつつある。今後，サービスメニューのより一層の拡充や，信頼性の更なる向上のため，サービス稼働基盤強化等の施策を継続して実施していく。また，CTI(Computer Telephony Integration)事業分野全般を視野に入れ，SaaS型コールセンターサービスなどの新しいサービスと融合することによって，さらに新しい形でのCTIサービスを創出していく。これらを通じて，“IT資産のコスト削減”“ビジネス環境の変化に応じて，サービス利用規模のタイムリーな拡充・縮小が可能”“BCPが万全”という，ITサービスならではのメリットを生かしていきたいと考えている。

参考文献

(1) 矢野経済研究所：日経ソリューションビジネス2009年9月30日号，日経BP社，329（2009）
(2) 総務省：平成21年「通信利用動向調査」の結果（2010）
(3) 経済産業省：平成21年情報処理実態調査結果報告書（2010）

特集論文

SaaS型電子帳票配信サービス“帳票Express on Demand”

吉田　稔*
大矢真一*
川上暢美*

SaaS-type Electronic Form Delivery Service "Form Express on Demand"

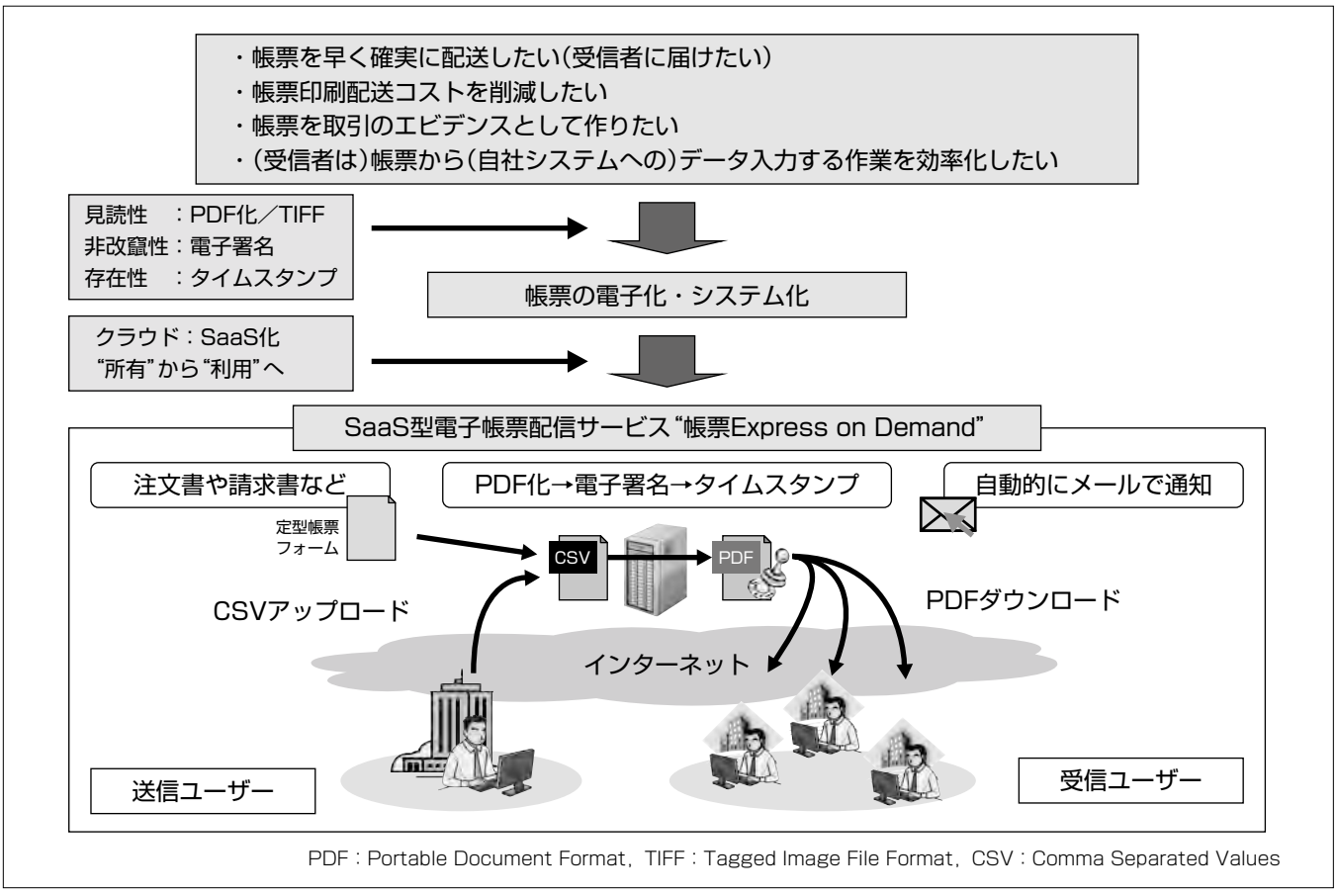
Minoru Yoshida, Shinichi Ohya, Masami Kawakami

要　旨

国内の企業間取引では，注文書，買い掛け明細書等，企業間での帳票の配送は日常業務になっている。これを電子化し送受信することで，郵送などに比べ，業務の効率化とコストダウンを実現し，さらにシステムによる配送先の管理と自動配信を行うことで，誤送信をなくすことができる。

帳票を電子化し，そのまま企業間で送受信するためには，帳票イメージを作成し配信するシステムが必要である。これには，自社システムとして開発・構築する方式(所有方式)と，これらをアウトソーシングサービスを利用することで実現する方式(利用方式)とがある。一方，アプリケーションシステムを複数のユーザーで共有する環境を提供するSaaS(Software as a Service)型サービスが種類，量ともに増えており，ユーザーの利用範囲も拡大している。これらの状況から，コスト削減を目的に，情報システムは“所有”から“利用”へのシフトが大きな潮流となっている。

三菱電機情報ネットワーク㈱(MIND)では，帳票の電子化ニーズにこたえて，SaaS型電子帳票配信サービス“帳票Express on Demand”の提供を開始した。帳票Express on Demandは，①コスト削減，②高いセキュリティ(電子署名による改竄(かいざん)防止など)，③帳票配信業務のスピードアップ，④電子データのまま保存可能(電子署名，タイムスタンプの付与による保証)，⑤運用管理(受信確認，受信の督促)機能を特長としている。



SaaS型電子帳票配信サービス“帳票Express on Demand”とその背景

企業間では多くの帳票が配送されている。帳票は印刷・封入され，紙で配送されているのが実情である。業務効率化，コストダウン，誤配送の防止等，ユーザーの要望を解決するためには，帳票の電子化，システム化が必要であるが，これらには様々な課題がある。これらの課題を解決するソリューションとして帳票Express on Demandサービスの提供を開始した。

*三菱電機情報ネットワーク㈱

1. まえがき

国内商取引では，見積書，注文書，買い掛け明細書など定常的に企業間で配送されている帳票は多い。これらの帳票は企業の情報システムで作成され，紙に印刷し，郵送されているのが実情である。企業にとって，帳票を電子化することは様々なメリットがある。しかし，帳票はエビデンスとしても重要な意味を持ち，エビデンスであることを維持して電子化すること，さらに，それをシステム化し運用することの負担が帳票電子化の課題となっていた。一方，セキュリティを維持しつつ，コンピュータシステム基盤やアプリケーションを共同利用するクラウドサービスが立ち上がりつつある。

本稿では，従来の課題を解決した帳票電子化のソリューションとして，SaaS型電子帳票配信サービス“帳票Express on Demand”について述べる。

2. 帳票の電子化

2.1 帳票電子化の課題

帳票を電子化しエビデンスとしても利用する場合，いくつかの要件があり，2005年4月1日施行のいわゆるe-文書法に帳票などの文書を電子データで扱うに当たっての要件が示されている。

1点目は非改竄性(改竄されていないこと)である。電子化された帳票は容易に変更を加えることができるので，電子化された帳票が，確かに発行者が作成したものであることを客観的に示す必要がある。2点目は存在性(発行日に作成されたものであること)である。意図的に後で作成されたものでないことを示すことである。3点目は見読性(紙の帳票と同様に，見て内容が理解できること)である。電子化された帳票を表示させ，客観的に内容が理解できるものである必要がある。これらの要件が帳票電子化の課題である。

2.2 解決策

帳票Express on Demandでは，これらの課題を主に暗号技術を用いて以下のように解決している。

(1) 非改竄性

非改竄性は電子署名技術によって担保している。帳票Express on Demandでは，送信者の電子証明書(公的に認定されている第三者機関である電子認証局が発行したものを採用)を用いて配信帳票ファイルに電子署名を付与している。これによって，発行者が作成したものであること，改竄されていないことを認証できる。合わせて，ユーザーが非改竄性を確認する手段も提供しており，受信者が配送された帳票ファイルを開いた際にこの非改竄性が自動的にチェックされ，結果が画面上に表示される。

(2) 存在性

帳票Express on Demanでは，帳票ファイルにタイムスタンプを付与することで存在性を担保している。タイムスタンプは，時刻認証局(TSA：Time Stamp Authority)が帳票のメッセージ・ダイジェストに標準時刻を付加し，その上でTSA自身の電子署名を付与することで実現している。TSAはRFC3161[3]にしたがって運用され，標準時刻を維持していることが保証されている(**図1**)。受信者が配信された帳票ファイルを開いたときにタイムスタンプの確認も自動的に行われ，作成日時が画面に表示される。

(3) 見読性

帳票Express on Demandでは見読性を維持するため，帳票ファイルとしてPDFを採用している。電子化された帳票は長期にわたって保管され，参照されるため，表示するソフトウェアが長期にわたって存在し，稼働が維持される必要がある。日本経済団体連合会の2004年3月の報告では，税務書類に使用するファイルはPDFまたはTIFFが推奨されている。

3. SaaS型電子帳票配信サービス

帳票Express on Demandは先に述べたように帳票をPDF化し，電子署名，タイムスタンプを付与して電子帳票としている。

3.1 サービス概要

帳票はその書式である帳票様式と帳票様式に埋め込まれる帳票データに分けられる。帳票Express on Demandでは，標準様式としていくつかの帳票様式が用意されており，利用者はその中から自社に合致するものを選択する。送信者は選択した帳票様式に加え，帳票に押印する印影とその押印位置の設定を含めて自社の帳票様式として帳票Express on Demandシステムへあらかじめ登録しておく。送信者は帳票データを作成し，サービス提供元である帳票Express on Demandシステムへ送信する。帳票Express on Demandシステムで帳票様式と帳票データから電子帳票が作成され，指定された受信者へ配信される。電子帳票

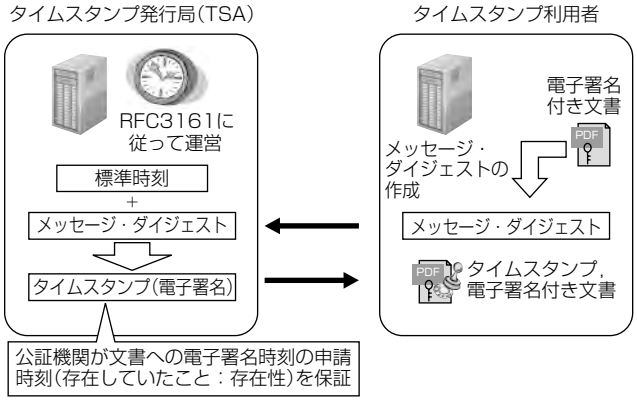


図1．タイムスタンプ付与処理

の送受信はインターネットを介して行い，特別なネットワーク環境を用意する必要はない。

図 2 に電子帳票の作成，配信の流れを示す。

⑴ 帳票データのアップロード(**図 2** ①)

送信者は，標準様式から選択した自社帳票様式にしたがって，自社で帳票データを作成する。これはCSVファイル形式で，帳票様式，宛先を指定するデータも含む。帳票データのサンプルが用意されており，そのガイドにしたがって作成できる。送信者はインターネットを介し，帳票Express on Demandシステムにログインし，作成した帳票データをアップロードする。

⑵ 電子帳票作成(**図 2** ②③④⑤)

帳票Express on DemandシステムはアップロードされたCSVファイルを解析し，宛先ごとに仕分し，指定された帳票様式に帳票データを埋め込み，電子帳票を作成し，これをPDFファイル化する。作成したPDFファイルに電子署名，タイムスタンプを付与し，受信者メールボックスに格納する。さらに受信者に電子メールで受信すべき電子帳票ができあがったことを通知する。帳票Express on Demandシステムでは，PDFファイル化，電子署名付与，タイムスタンプ付与の処理をMDIS社製ソフトウェアの“MistyGuard<Signed PDF Server>”をベースに実現している。

⑶ 帳票受信(**図 2** ⑥)

受信者は，帳票Express on Demandシステムからの通知メールを見て帳票Express on Demandシステムにログインし，未受信帳票をダウンロードする。受信者は通知されてから14日間であれば何回でもダウンロードを行うことができる。受信者がダウンロードしたPDFファイルを開くと，付与された電子署名，タイムスタンプを用いて，自動的に改竄チェック処理，時刻確認処理が起動され，結果が画面に表示される。これによって受信者は確かに送信者が送信した帳票であること(改竄されていないこと)，作成時刻を確認することができる。この確認処理は改竄チェックツール(SignedPDF Verifier)によって行われる。受信者はSignedPDF VerifierをあらかじめMDISのWebサイトからダウンロードしておく必要がある(ダウンロードは無償)。また，受信者は，送信者が作成した帳票データをCSVファイルとしてダウンロードすることもできる。これによって，受信者は帳票データを自社システムに直接(人手によって再入力することなく)取り込める。

3.2 管 理 機 能

帳票Express on Demandはグループという単位で運用管理される。グループは複数の送信者と複数の受信者で構成される。例えば，帳票配信企業とその受信企業をグループとすると，送信企業の各拠点(事業所，工場等)が送信者，各拠点から電子帳票を受信する企業が受信者となる。

3.2.1 ユーザー管理

帳票Express on Demandサービスへの加入に際しては，グループ管理者を指定する。加入処理が完了すると，グループ管理者にIDとパスワードが発行される。グループ管理者は帳票Express on Demandシステムにログインし，以下のユーザー管理機能を使用できる。

⑴ 送信者，受信者の登録，削除

帳票Express on Demandサービスを利用する送信者，受信者をシステムに登録する(**図 3**)。管理者画面にログインし，登録情報を入力するが，サービス利用開始時など，大量のユーザー登録が必要になる場合には，登録情報をCSVファイルに作成し，アップロードすることで代用できる一括登録機能も用意されている。

⑵ グループ内“お知らせ”機能

グループ管理者は，グループ内のユーザーがログインした直後のトップ画面に任意の文字列を掲載できる。グループ内受信者に配信時刻の変更，新規帳票の配信計画等の連絡を行える。

⑶ 仮パスワードの発行，変更の督促

サービス利用者がパスワードを忘れたときの仮パスワードの発行やパスワードの定期変更の督促を行える。グルー

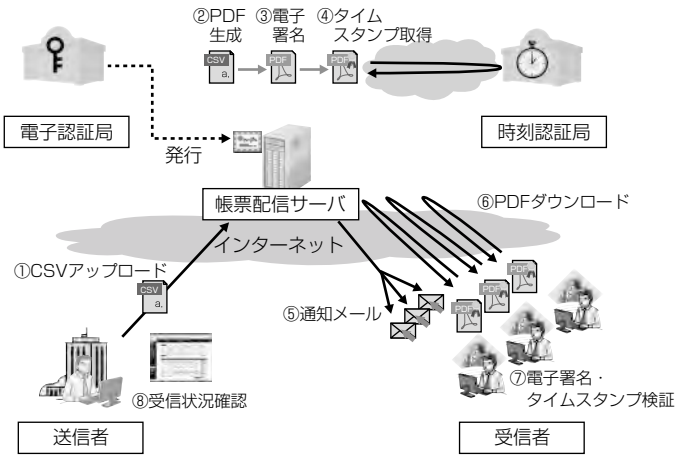


図 2．電子帳票の作成・配信の流れ

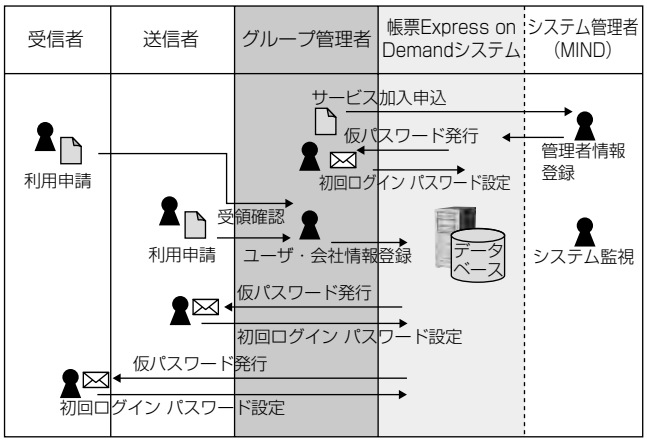


図 3．ユーザーの登録の流れ

プ管理者がパスワードの督促を指定すると，グループ内のユーザーがログインした際，パスワードの変更依頼画面が表示され，受信者にパスワードの変更を促す。

3.2.2 配信管理

⑴ 配信完了日時の確認

送信者は帳票の配信状態を知ることができる。すなわち，帳票Express on Demandシステムは，受信者がダウンロード完了した日時を記録しており，送信者はこれを検索し，確認できる。

⑵ ダウンロードの督促

受信者が帳票Express on Demandシステムからの通知メールを受けてから3日間ダウンロードせずに放置すると，受信者へダウンロードの督促メールが自動的に送信される。この督促メール送信までの日数は，グループ管理者が設定・変更できる。送信者は自動送信とは別に，配信管理画面から受信者を特定し，督促メールの送信をシステムに指示きる。

⑶ 配信の停止・再開，データ削除

送信者は自身が作成・配信した帳票の内容を確認できる。すなわち，帳票Express on Demandシステムによって作成されたPDFファイルを送信者自身もダウンロードすることができる。また，送信したデータの配信の停止，再開を操作できる。さらに，配信データの削除も行える。導入当初や新規帳票の試験等に役立てられる。

4. カスタムプラン

帳票Express on Demandでは上記の標準機能に加え，企業のきめ細かいニーズに対してカスタムプランを用意している(**図4**)。

⑴ 独自帳票

カスタムプランでは，標準様式で対応できない独自様式の帳票の配信をサポートする。MINDが送信者より依頼を受けて，独自帳票様式とそれに対応した帳票データを定義する。帳票様式を帳票Express on Demandシステムに登録し，送信者はその帳票様式を指定した帳票データを作成し，アップロードする。業務で使用中の紙の帳票があれば，その様式を容易に電子化でき，短期間で独自の帳票様式を作成できる。また，カスタムプランでは，グループ内のユーザーがログイン後に操作する画面上のロゴをカスタマイズする(例えば送信者企業のロゴを入れる)こともできる。

⑵ アプリケーション連携

送信者側システムで帳票データ作成処理を自動化している場合，帳票データの帳票Express on Demandシステムへのアップロードも，人手による操作ではなく自動化したいというニーズがある。カスタムプランでは，これに対応しアプリケーション連携機能を用意している。送信者側アプリケーションは，作成した帳票データを宛先，ファイル名等，あらかじめ定められたルールに従って帳票Express on Demandシステムへファイル転送できる。

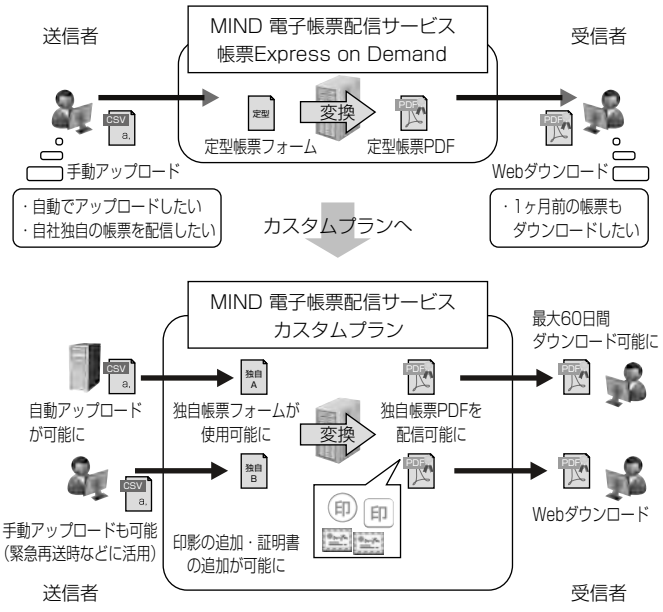


図4．カスタムプラン

⑶ 配信データの保管延長

配信データは帳票Express on Demandシステムに通常14日間保管される。受信者側の事情等によって更に保管が必要な場合はその期間を延長できる。

5. むすび

“所有”から“利用”へのユーザーニーズにこたえてSaaS型電子帳票配信サービス“帳票Express on Demand”の提供を開始した。今後もユーザーの声を聞く機会を増やし，その要望をサービスに反映し，改善拡張し，使いやすいサービスを目指していく。

参考文献

⑴ 吉田　稔，ほか：EDIをベースとした電子情報交換・保存サービスソリューション，三菱電機技報，**79**，No.4，293～296（2005）

⑵ 税務署類の電子保存に関する報告書，日本経済団体連合会情報通信委員会（2004）

⑶ Adams，C.，et al.：Internet X.509 Public Key Infrastracture Time-Stamp Protocol(TSP)，Internet Engineering Task Force(IETF) Networking Group，Request for Comment 3161（2001）

特集論文

既存パッケージのSaaS化に向けた課題と解決策

前田和俊*
鈴木　剛*

Challenges and Solutions for Existing Packages toward SaaS

Kazutoshi Maeda, Takeshi Suzuki

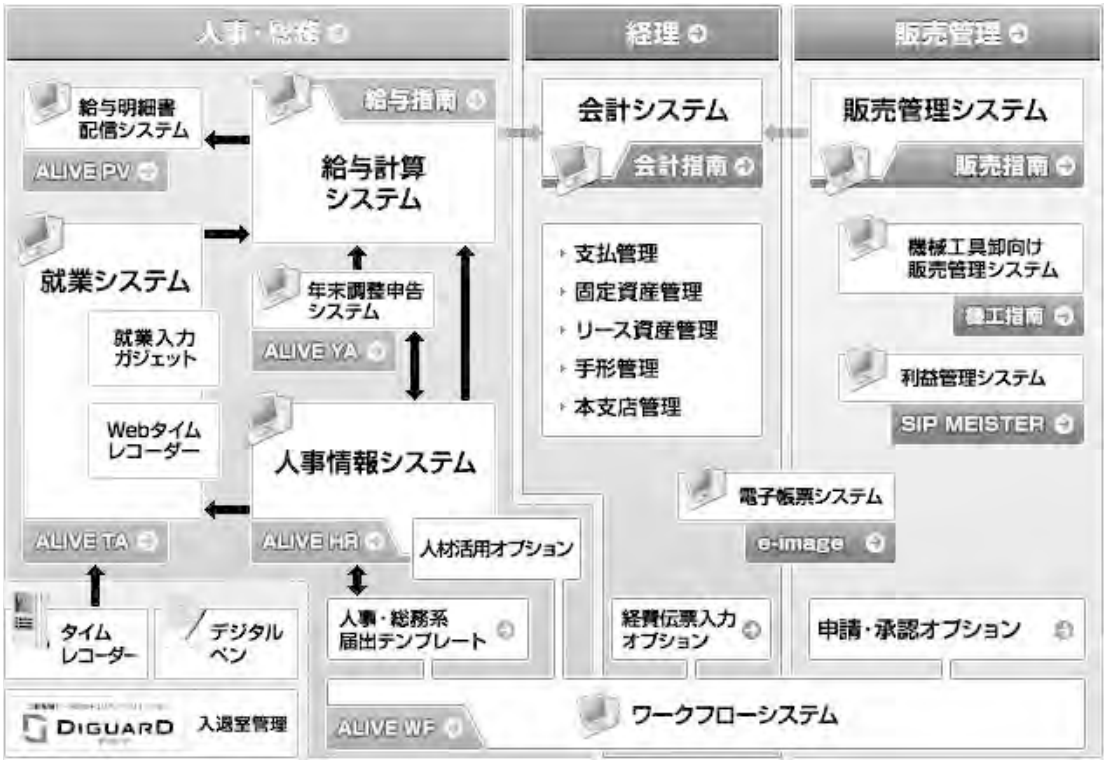
要　旨

㈱三菱電機ビジネスシステム(MB)では，人事・総務系業務パッケージの“ALIVEシリーズ”と，基幹系パッケージの“指南シリーズ”を開発・販売している。

MBではSaaS(Software as a Service)化に向けた様々な技術検討を実施しており，本稿では，両シリーズのユーザーインタフェースを実現するために開発したフレームワークと共通ソフトウェアコンポーネントを述べ，SaaS化に向けたこのフレームワークの課題と解決策について述べる。

ALIVEシリーズで使用するフレームワーク“radish”には，ユーザーインタフェースを受け持つ各種のコンポーネント群があるが，パッケージとしてイントラネット環境での使用を前提としている。事前検証によって，ネットワークトラフィックに関する課題があり，パッケージをそのままSaaS化することは困難であることを確認した。解決策としてコンポーネントの軽量化に取り組んでおり，その試作評価結果について述べる。

また，指南シリーズは操作の応答性能を重視して，クライアントサーバ方式を採用している。クライアントサーバ方式のSaaS化に向けた課題と取組みについて述べる。



http://www.melb.co.jp/as/index.html

“ALIVE・指南シリーズ”の構成

幅広い業種・業務で培ってきたノウハウと技術力を基盤に，ユーザーの抱える現場のニーズを解決するシステムを提供している。効率的・機能的な業務改善を目的としたパッケージであり，パッケージ単独の導入はもちろん，必要なパッケージを自由に組み合わせて最適なシステムにカスタマイズすることも可能である。

*㈱三菱電機ビジネスシステム

1. まえがき

ALIVEシリーズは，総務系の業務を対象とした人事・総務のトータルシステムで，2002年から販売を開始した。

指南シリーズは，経理系の業務を対象とした会計・給与計算システムと，販売管理業務を対象とした販売管理システムで，1998年から販売を開始した。

両シリーズとも各種機能追加，法改正対応，オープン化を進めるための開発言語の変更を行い，顧客ニーズにあわせ商品性を向上させてきた。

本稿では，既存パッケージのALIVEシリーズと，指南シリーズを概観し，ALIVEシリーズのSaaS提供に向けた課題と解決策を中心に，両パッケージのSaaS化への取組みについて述べる。

2. 既存パッケージの概要

2.1 ALIVEシリーズ

ALIVEシリーズは，人事・総務部門の業務効率化と，戦略的人材活用をサポートする業務パッケージである。

ALIVEシリーズの構成は次のとおりで，ALIVE TAの就業入力画面を**図1**に示す。

①ALIVE TA：就業システム
②ALIVE HR：人事情報システム
③ALIVE WF：ワークフローシステム
④ALIVE PV：給与明細書配信システム
⑤ALIVE YA：年末調整申告システム

2.2 指南シリーズ

指南シリーズは，経営活動をサポートする基幹系パッケージである。

指南シリーズの構成は次のとおりである。

①会計指南：会計システム
②給与指南：給与計算システム
③販売指南：販売管理システム

3. ALIVEシリーズのSaaS化

この章では，ALIVEシリーズのシステム概要，ALIVEシリーズで利用するフレームワークradish，及びSaaS化におけるradishの課題と解決策について述べる。

3.1 ALIVEシリーズの構成

ALIVEシリーズは，社内イントラネットを前提としたWebシステムである。社内のサーバにインストールしたOS(Operating System)上でALIVEを稼働させ，利用者はブラウザからHTTP(HyperText Transfer Protocol)プロトコルでALIVEにアクセスする。**図2**に，現状のALIVEのイントラネット構成を示す。

SaaSでは，インターネット経由の利用が前提となる。データセンターの仮想マシンにインストールしたOSの上でALIVEを稼働させる。利用者はブラウザからインターネットを経由しALIVEにアクセスする。ALIVEでは人事データを取り扱うため，通信経路上での盗聴などを防止する必要があり，HTTPS(HTTP over Secure Socket Layer)で通信を行う。**図3**に，ALIVEのSaaS構成を示す。

3.2 ALIVEシリーズのフレームワークradish

radishは，ALIVEシリーズで使用しているMBが開発したJava(注1)フレームワークである。

radishの中に，Webシステムのユーザーインタフェースを受け持つradish Web UIコンポーネント群があり，その中の1つに入力補助機能を提供する入力コンポーネントがある。HTML(HyperText Markup Language)のInputタグのテキストボックスは入力値の型や範囲をチェックする機能を持たないが，radish Web UIの入力コンポーネントによって，JavaScript(注1)による入力値チェックやフォーマット変換の機能を付加する。

(注1) JavaとJavaScriptは，Oracle Corp. の登録商標である。

図1．ALIVE TAの就業入力画面

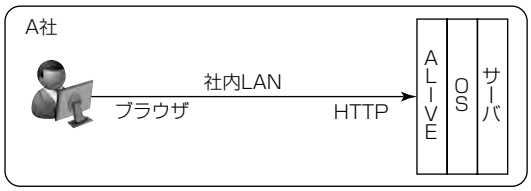


図2．ALIVEのイントラネット構成

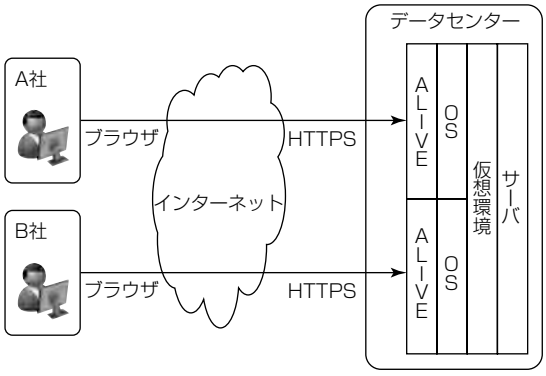


図3．ALIVEのSaaS構成

入力値のチェックはAjax(Asynchronous JavaScript and XML(eXtensible Markup Language):サーバとの非同期通信)でサーバで処理を行っている。そのため,サーバ側に固有のチェック処理を記述し,テキストボックスから呼び出すことで,ビジネスロジックにかかわるチェック処理を,HTMLに記述することなく実現可能としている。

図4に,時間入力コンポーネントの例を示す。1行目は入力途中の状態で,8時53分の出勤を入力するために"8.53"と入力している。この状態でフォーカスを移動すると,2行目のように"08:53"と自動でフォーマット変換し表示する。3行目の"8.61",4行目の"abc"のように時間表現としては不正な入力をした場合,テキストボックスの背景色を変え,入力値の不正を表現する。

3.3 SaaS化に向けた課題

SaaS化に向けた検証の一例として,ALIVE TAをインターネット経由で利用したときと,イントラネット内で利用したときの性能比較,パケット量の調査結果について述べる。

検証環境は,**図3**の構成で,仮想マシンはCPU(Central Processing Unit):1Core,メモリ:4GBを割り当てた。インターネット経由の利用はMB社内から,イントラネット利用はデータセンター内の別仮想マシンからアクセスすることで,アクセス経路のみが異なる環境を構築した。

3.3.1 ネットワークトラフィックの課題

就業入力画面をインターネット経由で利用した場合,今回検証した環境では,イントラネット環境に比べ,最大2.5倍の応答時間を要した。インターネット経由で応答時間が長くなる原因として,回線速度やサーバ性能のほか,ネットワークトラフィックが多いこともあげられる。

現行のALIVEは**3.2節**で述べたとおり,コンポーネントでHTML標準のテキストボックスに機能を付加している。機能の実装にはJavaScriptを多用しているため,HTMLが巨大化している。

表1に,テキストボックスのみを表示したサンプルHTMLに関して,radishによる変換処理前,処理後のHTML容量を示す。テキストボックスが1個あるHTMLの容量は161バイトであるが,このHTMLをradish上で実行すると,テキストボックスのほか,formタグに対する初期処理などが追加され,3,266バイトとなる。

図4. 時間入力コンポーネント

JavaScriptで機能を付加したHTMLをクライアントに転送するネットワークトラフィックの削減が,SaaS提供する際の応答性能を維持するための課題となる。

3.3.2 ユーザビリティの課題

SaaSでは,システム導入作業が現状のパッケージ販売とは異なるため,導入時の操作指導に関しても対応が必要となる。より理解しやすいマニュアルを整備するとともに,より直感的に利用可能なユーザビリティへと改善する必要がある。

3.4 解 決 策

3.4.1 ネットワークトラフィック削減の解決策

SaaS提供するために,radish Web UIコンポーネントが生成するJavaScriptや機能の見直しをすることで,ネットワークトラフィックの削減を目指し,radishの改善版を試作評価した。

現行版のradishでは,コンポーネントの振る舞いに必要なJavaScriptを各コンポーネントが個別に生成している。この動的に生成しているJavaScriptのうち,共有可能な処理を関数として1つ生成し,各コンポーネントから呼び出すことで,JavaScriptの生成量を減らしHTMLサイズを縮小した。

表2に,radishによって機能付加したHTMLに関して,クライアントに出力される容量を示す。テキストボックスが1個の場合,改善版のHTMLは現行版の−52%と悪化している。しかし,テキストボックスが10個の場合は32%,20個の場合は50%と,テキストボックスの数が多くなるほど,共有化による効果が現れる。

実際のHTMLにはデザインに関連する記述や,表示文字列等が含まれるため,一概には言えないが,項目数の少ない画面で転送量が問題になることは少なく,改善による効果は大きい。

3.4.2 ユーザビリティの解決策

具体例として,ガジェットのようなシンプル機能を用意することで,SaaS導入時における操作指導などの利用者の負担を減らすことも可能となる。ALIVE TAパッケージの最新版では,就業入力ガジェット(**図5**)を追加している。

表1. HTML容量

テキストボックス数	処理前(byte)	処理後(byte)
1個	161	3,266
10個	684	9,895
20個	1,274	17,305

表2. radish改善によるHTML削減効果

テキストボックス数	現行版HTML量(byte)	改善版HTML量(byte)	削減量(byte)	削減効果(%)
1個	3,266	4,972	−1,706	−52
10個	9,895	6,731	3,164	32
20個	17,305	8,701	8,604	50

図5．就業入力ガジェット

この機能によって，Windows Vista(注2)以降のクライアントOSで，デスクトップに表示可能なガジェットとして，出勤・退勤を1クリックで入力できる。

(注2) Windows Vistaは，Microsoft Corp.の登録商標である。

4. 指南シリーズのSaaS化

この章では，指南シリーズで採用している入力コンポーネント“MBInput”とSaaS化に向けた取組みについて述べる。

4.1 指南シリーズの構成

指南シリーズは，クライアントサーバ方式を採用しており，利用端末ごとにソフトウェアをインストールする。

4.2 指南シリーズ共通コンポーネントMBInput

MBInputは，業務アプリケーションにおける項目入力の標準化を目的としてMBが開発した指南シリーズ共通の入力コンポーネントである。売上入力で使用する入力コンポーネントには，伝票情報を片手にテンキーのみで操作できる機能と，1伝票を数秒で登録可能とする性能が求められる。MBInputのコンポーネントは，上で述べたような入力業務で求められる機能と性能の両方を兼ね備えており，ユーザーインタフェースで重要な役割を担っている。

MBInputの特長を次に示す。

- 複数の入力項目の形式を1つのコンポーネントでサポート
- 指定された型に対応した入力値制御，入力けた数・範囲指定が可能
- Enterキーによるフォーカス移動
- フォーカス取得時の背景色変更機能
- 優れた入力応答性

図6に，販売指南の売上入力の画面イメージを示す。入力項目はすべてMBInputで作成している。

4.3 課題と解決に向けた取組み

指南シリーズは，**4．2節**に示したとおり入力時のユーザーインタフェースが重要であり，Webシステムとして作り直す場合も，MBInputが持つ機能・性能のすべてを実現する必要がある。このためALIVEシリーズよりSaaS化の課題が多く，次で述べるように，早期提供開始，セキュリティ，コスト，機能・性能等の要件を満たすことができる提供方式を検討している。

図6．販売指南の売上入力画面

SaaSでは，インターネット経由でソフトウェアを利用するため，セキュリティや提供コストを考慮するとWebシステムの方が都合がよい。リッチクライアント方式を採用すれば機能・性能を満たせるが，対応開発のための期間とコストを要する。

機能・性能要件を満たした上で，顧客のSaaS化ニーズに俊敏に対応するため，現時点では，既存のクライアントサーバ方式の資産を活(い)かしてSaaS提供する方向で技術課題を抽出中である。

5. ソフトウェア以外の課題

SaaSサービスを提供する際に，ソフトウェア以外に次のような大きな課題が挙げられ，これらについても取組みを進めている。

5.1 サーバのサイジング

ALIVE TAなどの業務処理が特定の時間に集中する場合に，同一の物理サーバにいくつの仮想環境を動作させることが可能か検証し，ガイドラインを設定する必要がある。

5.2. サービス環境構築の迅速化

認証認可の設定，ポート，ファイアウォール等，仮想ネットワークの設定や仮想サーバを容易に設定できる環境やツールを準備し，サービス開始までの導入期間，コストを削減する必要がある。

6. む す び

SaaS提供には，本稿で述べた課題のほか，アプリケーションのマルチテナント対応，マルチテナントでSaaS提供する場合のセキュリティ課題，インターネット回線使用時の性能確保等，既存パッケージとは異なる技術課題が存在する。今後，これらの課題に取り組み，変化の激しい市場環境で，顧客ニーズに俊敏にこたえられる製品，サービスを提供していく所存である。

小規模オフィス向けアプライアンス“SmartSecurityOffice”

地里木拉提 特里瓦尔迪*
平島栄一*
石川純一*

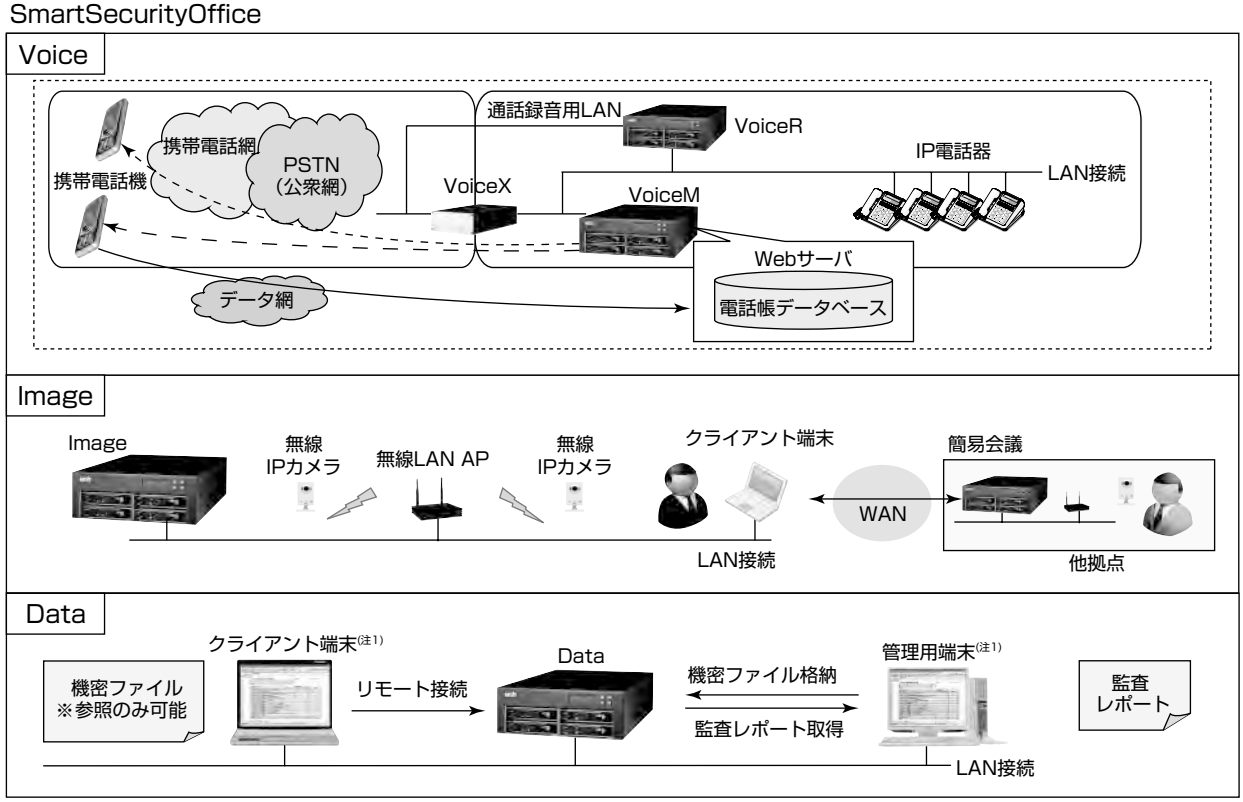
Appliance "SmartSecurityOffice" for Small Offices

Dilmurat Tilwaldi, Eiichi Hirashima, Jyunichi Ishikawa

要　旨

近年，大企業だけでなく，中小企業でも“取引リスク”“社会リスク”等の“経営リスク”が意識されるようになり，内部統制への対応やコンプライアンス強化が図られつつある。一方，一般に中小企業では，セキュリティ対策への意識が低く，また，投資余力がないという課題を持つ。さらに，中小企業では，IT(Information Technology)の人材不足などで，リスクへの対応と業務効率を両立させることが難しい場合がある。

三菱電機インフォメーションテクノロジー㈱(MDIT)が開発・販売している小規模オフィス向けアプライアンス“SmartSecurityOffice”は，Voice(通話録音)，Image(録画録音)，Data(文書アクセス制御)の3製品からなり，これらの課題に対するソリューションを提供するものである。Voiceは，Web電話帳機能によって情報漏洩(ろうえい)防止と携帯電話同士間の通話録音を実現する。Imageは，ノイズキャンセル機能とリップシンク機能を搭載することで録画品質を確保し，可搬型のマイク付き無線IP(Internet Protocol)カメラの採によって緊急的・スポット的な録画を可能にする。Dataは，格納された機密文書ファイルの閲覧・編集を可能としつつ，外部持ち出しを禁止する機能を提供する。



(注1)　クライアント端末，管理用端末は，本製品の対象外　　AP：Access Point，LAN：Local Area Network，WAN：Wide Area Network

“SmartSecurityOffice”3製品の全体像

SmartSecurityOfficeは，Voice，Image，Dataの3製品からなる。VoiceではWebサーバを利用したV字発信によって携帯電話機間の通話録音を実現する。V字発信はVoiceMサーバ内蔵のWebサーバにアクセス(図中の実線)し，VoiceMから発呼する(図中の破線，点線)機能である。Imageは窓口，応接室など接客業務を録画録音する。Dataは重要ファイルの印刷・コピーを禁止した共有閲覧機能や重要ファイルへのアクセス履歴管理機能を持つ。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

大企業だけでなく，中小企業でも“取引リスク”“社会リスク”などの“経営リスク”への対応が重要となってきている。これに対し，内部統制へのIT投資が図られつつあるが，中小企業では，セキュリティに対する意識が低く，また，ITの人材不足，初期投資コスト，ITリテラシーなどの制約によって，思うような対策が進んでいないのが大きな課題となっている。

2. SmartSecurityOffice

“SmartSecurityOffice”は，従業員20～30名程度の小規模オフィスを対象としたセキュリティ機能に特化したアプライアンス(専用コンピュータ)製品である。この製品のねらいは，Voice，Image，Dataの3つのアプローチから職員一人ひとりのコンプライアンスや顧客対応力を向上させ，企業を経営リスクから守るとともに貴重な収益向上の契機を逃さない対応を可能とすることである。また，この製品はユーザー環境に合わせた設定を出荷時に行うこと，及び専用管理ツール群によって，顧客自身による短期間での導入と運用を可能としている。これによって，システムエンジニアによるシステム構築が不要であり，安価なソリューションを提供している。

3. SmartSecurityOfficeのVoice

3.1 製品コンセプト

SmartSecurityOfficeのVoice(以下“SSOVoice”という。)は，携帯電話機のデータレス化及び通話録音を実現した製品である。PBX(Private Branch eXchange)機能を持つVoiceX，CTI(Computer Telephony Integration)機能を持つVoiceM，通話録音機能を持つVoiceRの3サーバで構成する。社員がVoiceMのWebサーバ上に電話帳を保存し，Web経由で電話帳にアクセス・電話をかける形で使用する。利用シーンとしては社員が私有する携帯電話機内の電話帳データを使わずにWeb電話帳のデータを参照し電話をかけることや，管理者が携帯電話機の録音を聞き，職員の管理や指導を的確に行うことを想定している。

3.2 特　長

本製品は，Web電話帳機能と携帯電話機間の通話録音機能を特長とする。Web電話帳機能は，社員が携帯電話のWebブラウザからVoiceMサーバにアクセスし，VoiceM内のWeb電話帳データを閲覧し相手先に発信する機能を持つ。通話録音機能は，外線通話を全自動で録音する機能を持つ。

3.3 使用技術

(1) Web電話帳機能

Web電話帳機能はCTI機能を持つVoiceMで実現する。VoiceMは，音声パケットを処理できるSBC(Session Border Controller)型B2BUA(Back-to-Back User Agent)方式のSIP(Session Initiation Protocol)サーバとWebサーバを内蔵している[1]。従来のSIPサーバは電話機を制御する機能が主で，電話帳機能は電話機内の機能であったため，電話帳のデータを集約することはできなかった。しかし，VoiceMはWebサーバを内蔵し，Webブラウザで電話帳データを閲覧・発呼する機能を備えた。これによって，Webブラウザを使用できる携帯電話機やスマートフォンなどの携帯端末からの電話帳操作を可能とした(**図1**)。

Web電話帳から発呼するときは，携帯電話ブラウザからVoiceMにアクセスし，認証後に電話帳を閲覧する。Web電話帳に表示された電話番号をクリックするとWebサーバからSIPサーバに発呼命令を送信し，SIPサーバが発呼命令に基づき発呼する。発呼は携帯電話機ではなく，VoiceMから行っているので，まず操作した携帯電話機に発信し，次にクリックした電話番号に発信する。これらの通話はそれぞれ独立した通話であるが，
SIPサーバ内で2つの通話を接続するので見かけ上は1つの通話に見える。

(2) 携帯電話の通話録音機能

通話録音はVoiceRでスイッチングハブのミラーポートからパケットをキャプチャし，音声ファイルとして録音する。すべての外線通話を自動的に録音する。通話はWebブラウザからVoiceRにアクセスすることで再生できる(**図1**)。

3.4 今後の課題

従来のSIPサーバは電話機制御が主であり，通話ログなどは保存しない，又は保存しても有効活用できていない。SSOVoiceは通話ログの取得・閲覧機能を持つので，今後は通話ログをログ管理システムなどと連携して管理することでCRM(Customer Relationship Management)機能を付加するなど，製品価値の向上を検討する。

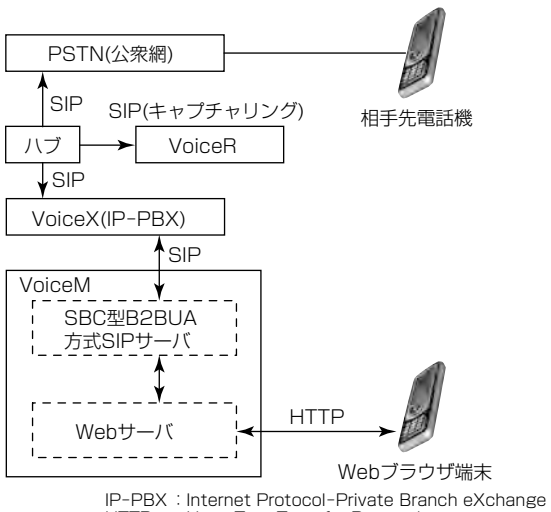


図1．VoiceMの内部構成と各機器との接続

4. SmartSecurityOfficeのImage

4.1 製品コンセプト

SmartSecurityOfficeのImage(以下“SSOImage”という。)は，可搬型マイク付き無線カメラによって，応接室，窓口カウンターの接客状況，社内の会議などを録画録音する。利用者は専用の簡易会議ビューアソフトウェアをパソコンにインストールすることによって，録画録音している映像，会議参加者の映像をビューアでライブ表示できる。また録画録音した映像や簡易会議を選択して再生できる(**図2**)。この製品の主な利用シーンを次に示す。

(1) 応接室などでの顧客との商談や交渉の様子を録画録音し，職員の動作を確認することで，顧客対応時における指示やアドバイスを行うことが可能である。

(2) 窓口での顧客対応の様子を録画録音し，後日，身に覚えのないクレームを受けた場合などに，こちらの対応に落ち度のないことを示す証拠として活用できる。

(3) 受付やエントランスに設置し，外部からの不審者や内部の怪しい動きを監視することが可能である。

4.2 特　　長

(1) 可搬型のマイク付き無線IPカメラを採用

通常のネットワーク監視カメラシステムでは，各機器の接続や設定などにあたってLAN工事が必要である。カメラの設定場所を変えた場合，改めてLAN工事を行う必要がある。SSOImageでは，可搬型の無線IPカメラを採用しているため，カメラを設置していない場所でもLAN工事などが不要で，緊急的・スポット的にいつでもどこでも録画録音が可能である。しかもカメラは小型でマイク内蔵であり，付属のバッテリーとカメラを付属の接続ケーブルで接続し，1つのカメラ・ケースの中に設置するため，顧客との接点(窓口カウンター・応接室等)でも目立つことなく利用可能である。

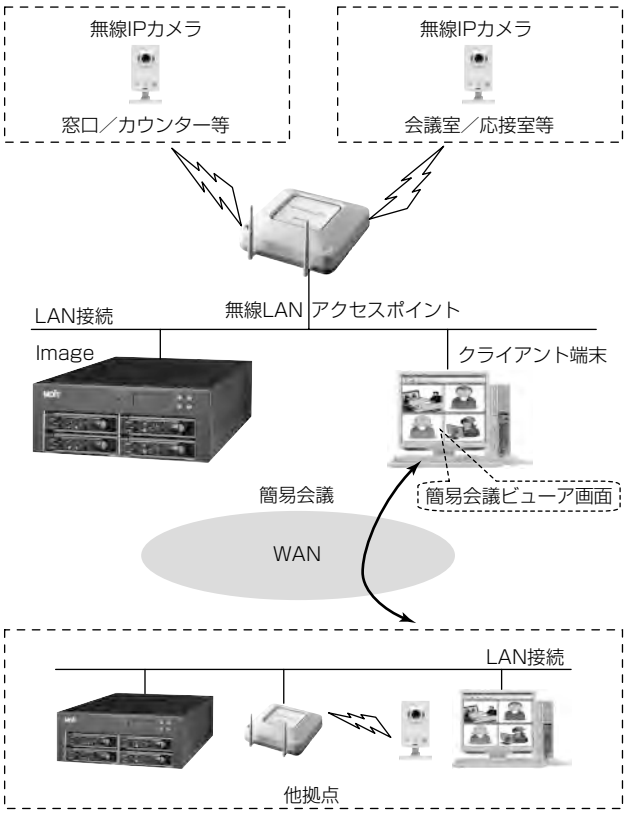


図2．SSOImageの構成

(2) ノイズキャンセル機能とリップシンク機能搭載

通常のマイク付きネットワークカメラでは，音声を録音した際，雑音が入ってしまい再生音が聞き取りにくくなる。それを防ぐため，この製品ではノイズキャンセル機能を利用している。また，通常の録画サーバでは，映像と音声がずれて再生されてしまう。これを改善するため，リップシンク機能を利用している。

(3) 簡易的な会議システムとして利用可能

全社的に導入すると，社内拠点間で簡易的な会議システムとしても利用可能であり，出張による交通費，移動時間を削減できる。会議画像自体をそのまま議事録として保存でき，事務効率を向上できる。

4.3 使 用 技 術

SSOImageは，MDITの“ネカ録”をベースとして開発したアプライアンス製品である[(2)(3)(4)]。ネカ録の保有技術以外では，次の技術を使用している。

(1) 簡易会議ビューア

既存のネカ録では，録画録音した複数台のカメラ映像を同じ画面上に同時に再生するのは不可能であった。SSOImageでは，既存のネカ録製品では持てない簡易会議ビューアを開発した。簡易会議ビューア専用ソフトウェア(クライアント用ソフトウェア)をクライアント端末にインストールすることによって，録画録音している映像を最大9画面までビューアで同時にライブ表示可能である。さらに，録画録音した9台までの映像を同時に再生可能である。

(2) ノイズキャンセル機能とリップシンク機能

騒音の中でも再生音を聴き取りやすくするため，ノイズキャンセル機能を使用している。この機能は周波数帯域限定によって実現している。また，映像を録画録音した場合，通常の録画サーバでは，映像と音声がずれて再生されるという問題への対応が必要である。この製品では，リップシンク機能を使用し，画像と音声の差異調整によってこの問題を解決している。

4.4 今後の課題

録画録音した映像の検索性を高めるために，録画データにインデックスを付ける機能や，会議ごとのデータバックアップ機能を追加することなどを検討中である。

5. SmartSecurityOfficeのData

5.1 製品コンセプト

SmartSecurityOfficeのData（以下“SSOData”という。）は，各企業が保有する機密情報を格納するための“情報管理ボックス”である。顧客情報，経理情報等が記録された機密文書ファイルを管理者が格納し，一般ユーザーが参照する形で使用する。保険業，不動産業等で顧客一覧などの情報をこの製品に格納しておき，営業マンが参照するといった利用シーンが考えられる（**図3**）。

5.2 特　長

最大の特長は，格納された機密文書ファイルの閲覧・編集を可能としつつ，外部持ち出しを禁止している点にある。また，機密文書ファイルへのアクセスログを常時保存しており，管理者は監査レポートの形でこれを確認する事が可能である[5]。情報漏洩が発生した際の調査に利用できるほか，不正行為の心理的抑制効果も期待できる。その他，機密文書ファイルの暗号化，USB（Universal Serial Bus）デバイス制限，クリップボード制限などの仕組みを備えている。

5.3 使 用 技 術

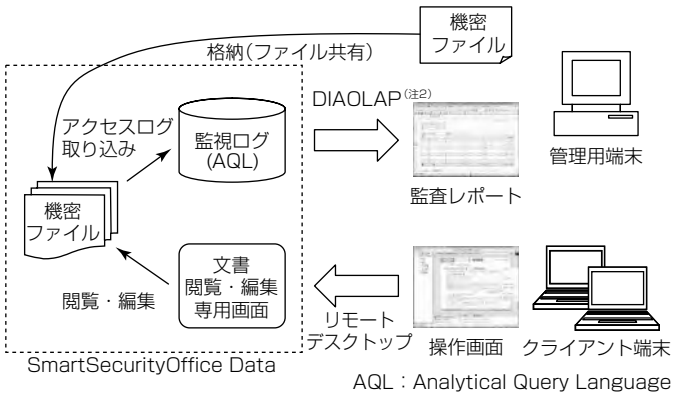
クライアントからの機密文書ファイル閲覧・編集を可能とすることと外部持ち出し防止を両立することは，一般的なファイルサーバでは実現できない。ファイルに対して読み込み可能の権限を付与した時点で，そのファイルはクライアント側にコピーが可能となり外部への持ち出しができてしまう。そこで次の技術を用いてこの要件を実現させている。

(1)　リモートデスクトップ

機密文書ファイルの外部持ち出しを防止するためには，機密データ自体をクライアント側にダウンロードさせないことが必要である。そこで，クライアント・サーバ間を流れるデータを，画面の画像情報とキーボードなどの入力情報に制限することとし，仕組みとしてWindows(注3)のリモートデスクトップを使用している。

(2)　文書閲覧・編集専用画面

リモートデスクトップ接続によって，クライアント側への機密文書のダウンロードは防止可能となるが，サーバ上でのコマンド操作で機密文書ファイルをほかのファイルサーバにコピーすることは可能である。そのため，文書持ち出し防止を実現するにはまだ不十分である。そこで，リモートデスクトップ接続時に可能な操作を制限することが必要であり，文書閲覧・編集専用画面を開発した。文書閲覧・編集専用画面は，一般ユーザーがログオンした際にWindowsスタートメニューの代わりに起動されるものである。この画面では任意の機密文書ファイルを開き，ログオンユーザーのアクセス権限に応じて閲覧・編集・上書き保存を行うことが可能だが，それ以外のコマンド起動・ファイルコピーといった操作はできない。そのほか，システム改変の防止，操作の簡略化にも有効であり，また，通常実行されるスタートアップ処理が行われないため，素早いログオンが可能となる。



（注2）　DIAOLAPは，三菱電機(株)のデータ分析ツールである。

図3．SSOData動作概要

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

5.4 今後の課題

監査レポートを改良し，よりユーザーの利用形態に合わせたものとすることや，不審ファイルアクセスの自動検知機能を追加することなどを検討中である。

6. む　す　び

大企業では“取引リスク”“社会リスク”への対策が進んでいるが，従業員20名から30名程度の企業へのセキュリティ対策の浸透はこれからである。“SmartSecurityOffice”は，家電ライクで，ITの専門知識が不要であり，小規模オフィス向けのセキュリティソリューションとして今後機能拡張を検討していく。

参 考 文 献

(1)　渡辺　透，ほか：IP-PBXにおけるCTIサービス機能の実現に関する課題と考察，情報処理学会マルチメディア，分散，協調とモバイル（DICOMO2010）シンポジウム，1011～1018（2010）
(2)　三浦敏広，ほか：進化した監視カメラ用録画・配信サーバ“ネカ録”，三菱電機技報，**83**，No.7，449～452（2009）
(3)　西村達夫，ほか：“ネカ録”最新シリーズによる遠隔・集中監視ソリューション，三菱電機技報，**82**，No.7，449～452（2008）
(4)　西村達夫，ほか：ATM向け映像監視・保管システム，三菱電機技報，**81**，No.7，445～448（2007）
(5)　郡　光則，ほか：多種多様なログの統合管理を実現する“LogAuditor Enterprise”，三菱電機技報，**80**，No.10，615～618（2006）

H.264/AVCカメラに対応した“ネカ録3.0”

内村誠之*
萩原聖貴*

“NECAROKU 3.0”: Recording and Distributing Server for Network Cameras with H.264/AVC Transcoder

Seishi Uchimura, Kiyotaka Hagiwara

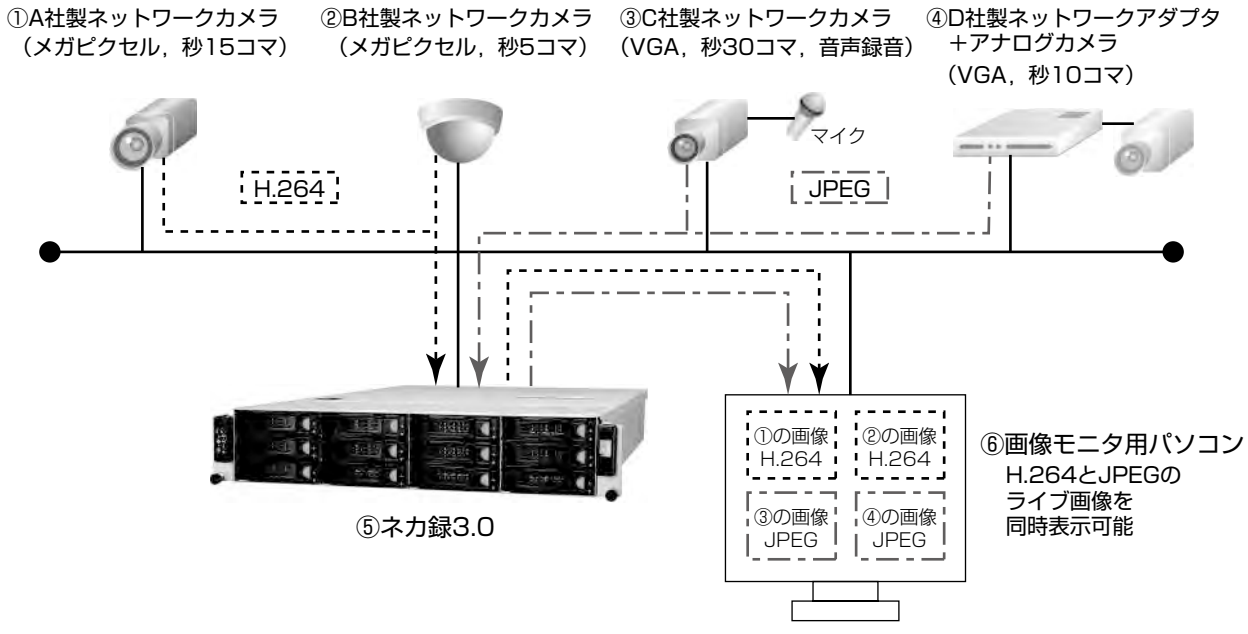
要　旨

“ネカ録”は，三菱電機インフォメーションテクノロジー㈱（MDIT）が提供するネットワークカメラに対応した監視カメラ用録画・配信サーバである。様々なメーカーのネットワークカメラを自由に組み合わせて表示／録画が可能なこと，IP（Internet Protocol）ネットワーク経由での統合的な遠隔監視が可能なこと，長時間・大容量の録画に対応可能なことを特長としている。

監視カメラシステム市場では，よりクリアで高精細な映像，長時間録画，設置カメラ台数の増加，コスト低減のための録画サーバ台数削減を求める傾向が強まっている。このため，録画サーバとしては，録画画像の大容量化への対応や画像圧縮性能の向上が必要となっている。

今回，ネカ録の最新バージョン“ネカ録3.0”で，動画圧縮規格H.264/AVC（Advanced Video Coding）形式のカメラ画像サポートなど，高画質での長時間録画を実現させるための機能強化を図った。

ネカ録3.0では，１台のネカ録でJPEG（Joint Photographic Experts Group）形式とH.264/AVC形式のカメラの混在を可能とした。多メーカーのカメラをサポートしているため，設置条件や録画条件に応じて多種のカメラを選定して混在させた場合でも，同時録画及びライブ画像表示が可能となる。



ネカ録3.0による監視システムの構成例

H.264/AVC画像配信カメラ（①，②），JPEG画像配信カメラ（③），JPEG画像配信ネットワークアダプタ＋アナログカメラ（④）の画像をネカ録3.0（⑤）に配信し，画像モニタ用パソコン（⑥）でライブ画像を同時に表示することが可能となる。

*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，セキュリティへの関心が高まる中，監視カメラシステムの市場は着実に成長を続けている。

MDITの監視カメラ用録画・配信サーバ“ネカ録”は，様々なメーカーのネットワークカメラを組み合わせて接続できること，長時間・大容量の録画に対応可能なこと，ネットワーク経由での統合的な遠隔監視が可能なことを特長としている。

ネカ録の最新バージョンである“ネカ録3.0”では，更なる大容量・長時間録画に関する機能を中心に強化を行った。

本稿では，ネカ録3.0の最新機能について述べる。

2. 背　景

セキュリティ意識の高まり，利用範囲の拡大，デジタル化へのシフトによって，金融機関，データセンター，ビル，店舗，交通機関等で，監視カメラシステムの需要は拡大すると予想されている。

例えば，金融機関では，紙幣の種類・枚数や人物の顔等の監視対象を正確に判別したいという要望が高まっており，監視カメラの録画装置には，高画質かつなめらかな映像で長時間録画できることが求められている。また，セキュリティ強化のため，1システムあたりのカメラ設置台数は増える傾向にある。これらの要求から，監視カメラシステムごとの総録画画像容量は，増加の一途をたどっている。

ネカ録は，H.264/AVCトランスコーダーを搭載して画像容量を圧縮するAVCモデルと，大容量HDD(Hard Disk Drive)内蔵によって，大容量・長時間録画を最小限のシステム構成，最小限のコストで実現できるような取組みを行ってきたが，更なる対応が必要となってきた。

3. ネカ録3.0の概要

今回新たに開発したネカ録3.0では，大容量・長時間録画に関する機能強化として，①ネットワークカメラのH.264/AVC形式のサポート，②内蔵HDD容量の拡張，③対応可能カメラ台数の拡張，の3点を行った。

3.1 H.264/AVC形式のサポート

ネットワークカメラから配信される画像形式として，従来のJPEG形式に加え，H.264/AVC形式をサポートした。H.264/AVC形式とは，国際標準策定団体ITU-T(International Telecommunication Union-Telecommunication Standardization Sector)とISO/IEC(International Organization for Standardization/International Electrotechnical Commission)の動画圧縮規格であり，MPEG-2(Moving Picture Experts Group-phase 2)の2倍以上の圧縮効率を実現するものである。この形式をサポートすることによって，録画可能時間が従来の3倍以上となった。

3.2 内蔵HDD容量の拡張

ラックマウントタイプの最上位機種“NS-5700”に，24TB(Tera Byte)ディスク(2TB×12本)内蔵モデルを追加した。これによって，最大録画可能容量が従来比の約1.5倍となった。各機種の搭載HDD容量・本数，対応RAID (Redundant Array of Inexpensive Disks)種の組合せも見直し，**表1**のとおりとした。各製品の外観を**図1**に示す。

3.3 対応可能カメラ台数の拡張

録画容量の拡張に伴い，1台のネカ録で対応可能なカメラ台数を32台から64台に拡張した。

4. ネカ録3.0の機能

4.1 H.264/AVC形式のサポートカメラ

ネカ録はマルチベンダーのカメラをサポートしているが，画像配信仕様は各カメラメーカー間で異なるため，それぞれの仕様に合わせて開発し，順次サポートしていくことになる。JPEG画像では，10社12種の仕様をサポートしているが，H.264/AVCに関しては，今回は3社をサポート対象とした(**表1**)。この3社は，今回の開発開始時点でH.264に対応していたカメラメーカーの中から，ネカ録との組合せでの過去の出荷実績，市場シェア，H.264サポートの性能・仕様の3点を考慮した上で決定した。

表1．ネカ録3.0の主な仕様

型名		NS-5700	NS-3500	NS-1500
物理ディスク容量		24TB／16TB／8TB／5TB	8TB／4TB／2TB／1TB	1TB／500GB
RAID		RAID6／5	RAID6／5／1	−
最大録画時間		約17,100	約5,400	約780
消費電力		～480VA/470W	～200VA/190W	75VA/70W
サイズ(mm)		485(W)×721(D)×88（H)	250(W)×401(D)×100(H)	215(W)×231(D)×89(H)
重量(kg)		～26.8	8.9	4.2
最大接続カメラ数		64		
画像圧縮方式		H.264/AVC，JPEG(モーションJPEG)		
解像度(横×縦)		1280×960(SXVGA)，640×480(VGA)，320×240(QVGA)		
接続可能カメラ	JPEG形式	三菱電機，パナソニック(I-Pro(注1)，BB)，ソニー，キヤノン，AXIS，TOA，サンヨー，ビクター，エルモ，東芝		
	H.264/AVC形式	AXIS，パナソニック(I-Pro)，サンヨー		

SXVGA：Super eXtended Graphics Array，QVGA：Quarter Video Graphics Array
(注1) I-Proは，パナソニック㈱の登録商標である。

(a) NS-5700

(b) NS-3500

(c) NS-1500

図1．ネカ録3.0の製品外観

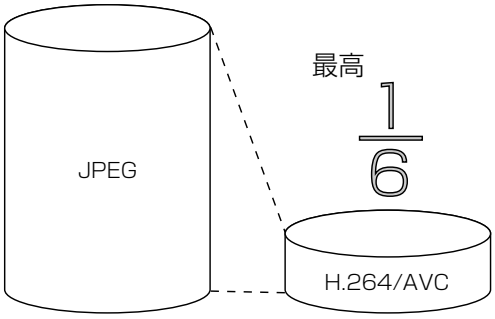


図2．画像容量比較

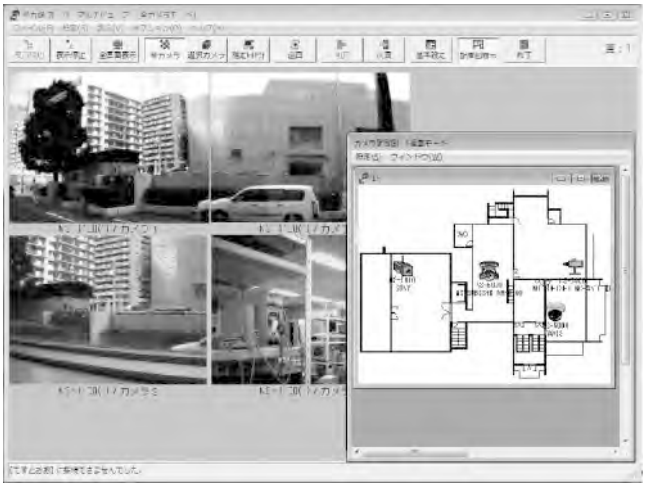


図3．監視画面の表示例

4.2 H.264/AVC形式サポートのメリット

H.264/AVC形式の画像容量は，JPEG形式と比較し1/3～1/6程度となる(**図2**)。これによって，録画画像保存容量と使用ネットワーク帯域を大幅に節減することができる。

4.3 サポート機能・仕様

H.264/AVC形式の画像に対してサポートする機能及び仕様は，従来JPEG画像に対してサポートしていた仕様と基本的に同一とした。ただし，動き検知などの実現難易度の高い一部の機能に関しては，今回はサポート外とし，今後の検討項目とした。

4.4 H.264/AVC形式とJPEG形式の混在

1台のネカ録で，JPEG形式とH.264/AVC形式のカメラの混在を可能とした。ネカ録内の画像管理形式を，両形式の画像の共通管理が可能な形に変更し，録画・検索処理を合わせて変更した。また，ビューアの表示画面でも，**図3**のようにJPEG形式とH.264/AVC形式のカメラの混在表示を可能とした。

4.5 H.264/AVC形式の表示性能

一般的に，JPEG形式と比較してH.264/AVC形式のデコードには非常に大きな負荷がパソコンにかかる。この点では，CPU(Central Processing Unit)の性能・機能を有効に使用するネカ録独自の工夫を施し，従来のJPEG形式の表示性能とさほど遜色ない表示性能を実現した。

4.6 H.264/AVC形式画像の保存

ネカ録内の録画画像をパソコンにダウンロードした場合は，ネカ録専用のファイル形式で保存されるが，標準的なパソコンにプリインストールされている汎用的な再生プレーヤーで再生可能なMP4(MPEG-4 Part14)形式に変換しての保存も可能とした。

4.7 従来ネカ録との高い互換性

ネカ録内ソフトウェア・管理ソフトウェア・ビューアソフトウェアとも，従来製品の拡張の形とし，ユーザーインタフェースの変更は必要最小限に留(とど)めた。そのため，導入作業や監視業務は，従来と同じ手順で行うことができる。

また，ネカ録3.0用のコマンダー／スーパーマルチビューアからネカ録2.0の管理／監視は可能となるので，ネカ録2.0／AVC／ネカ録3.0混在システムで，統合管理／監視が可能となる。

5. むすび

今回は，大容量・長時間録画に関する機能強化を中心に行った。今後の課題としては，次の3点を中心に考えている。

①ユーザビリティ向上，運用管理の簡易化

監視カメラシステムの市場では，アナログカメラからネットワークカメラへの移行が進んでいる。アナログでは実現不可能な映像の高精細化や，LAN(Local Area Network)／WAN(Wide Area Network)を介した遠隔監視・大規模監視の実現がその牽引(けんいん)要素になっている。一方で，中小規模案件を中心にアナログカメラの採用も依然として多い。導入／運用コストやユーザビリティが主な理由である。このため，アナログカメラシステムからの移行を推進するためには，さらなるユーザビリティ向上，運用管理の簡易化が必要と考えている。

②サポートカメラ機種の拡張

マルチベンダーのカメラサポートはネカ録の特長であるが，適応可能なシステム範囲を広げるため，更にサポート機種を増やしていきたい。H.264/AVC形式のカメラサポートでは，順次ほかのメーカーのカメラもサポートしていく。JPEGカメラに対しても，特長あるカメラがあれば新規サポートを検討していきたい。また，ネットワークカメラの共通規格ONVIF(Open Network Video Interface Forum)をサポートしたネットワークカメラも市場に登場しはじめているので，ONVIF規格のサポートも視野に入れていく。

③大容量・長時間録画に関する機能強化の継続

よりクリアで高精細な映像，長時間録画，設置カメラ台数の増加，コスト低減のための録画サーバ台数削減を求める市場の傾向は今後も続くと思われるので，大容量・長時間録画に関する機能強化は今後も継続していく。大容量HDDや高圧縮形式への対応を検討するとともに，運用開始後の保存可能容量の柔軟な変更への対応も検討していきたい。

参考文献

(1) 三浦敏広，ほか：進化した監視カメラ用録画・配信サーバ“ネカ録”，三菱電機技報，**83**，No.7，449～452（2009）
(2) 西村達夫，ほか：“ネカ録”最新シリーズによる遠隔・集中監視ソリューション，三菱電機技報，**82**，No.7，449～452（2008）
(3) 西村達夫，ほか：ATM向け映像監視・保管システム，三菱電機技報，**81**，No.7，445～448（2007）
(4) 大久保　榮 監修：改訂版H.264/AVC教科書，インプレスR&D（2006）
(5) ISO/IEC 14496-10:2004，Advanced Video Coding (Second Edition)（2004）

HGWの装置アーキテクチャと構成技術

布施雅明* 西尾俊介*
高田佳典**
藤原秀治***

Architecture and Technology of HGW

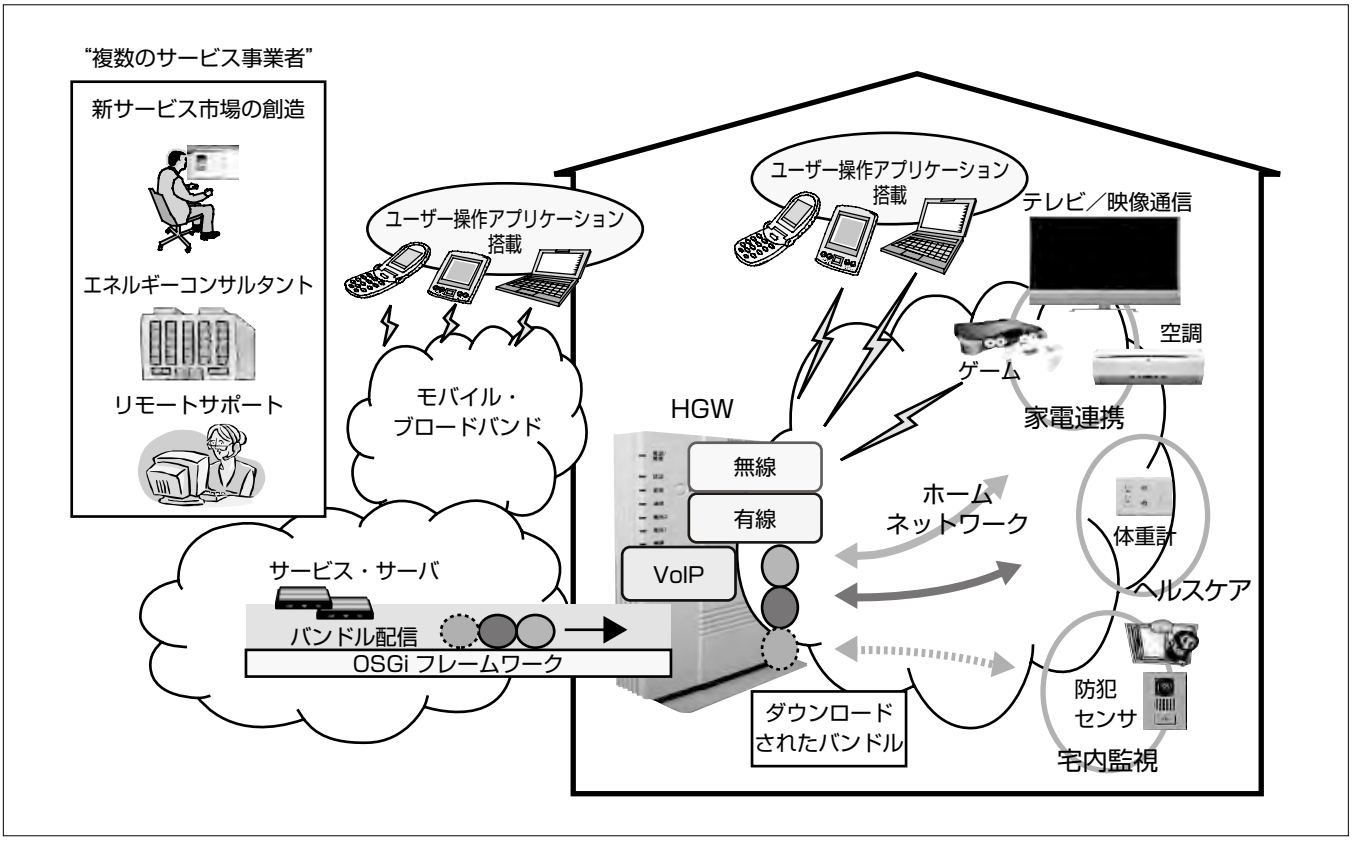
Masaaki Fuse, Yoshinori Takada, Hideharu Fujiwara, Shunsuke Nishio

要　旨

次世代ネットワーク(Next Generation Network：NGN)普及の次ステップとして，新たな付加価値を生み出すサービスの提供が始まりつつある。とくに，映像，センサ，カメラなど高度化する宅内機器とネットワークを連携させるホームICT(Information and Communication Technology)サービスの実用化が注目を集めている。ホームICTでは，多様なプロトコルを持つ宅内機器を宅内に配置したHGW(Home GateWay)が終端し，HGWがネットワーク内のサービス・サーバと連携することで，遠隔ユーザー間での映像共有などの家電連携，センサによる宅内監視，IT機器のリモートサポート，ヘルスケアなど，多様なサービスを提供する。ホームICTでは将来にわたって進化する宅内機器やサービスに柔軟に対応する必要があり，まただれもが簡単な操作で，便利に安全に利用できなければいけない。このため，HGWはNGNの基本機能であるVoIP(Voice over IP)機能やブロードバンド・ルータ機能のほか，各種サービスやプロトコルに柔軟に対応するプラットフォーム機構，ネットワークが配信するアプリケーション(バンドル)を実行するためのOSGi(注1)フレームワーク機構，各種アプリケーションサービスの暴走などからライフラインとしてのVoIP機能をガードする機構等が要求される。

本稿では今回三菱電機で開発したHGWの装置アーキテクチャと構成技術について述べる。

(注1)　OSGi(Open Service Gateway initiative)は，OSGi Allianceの登録商標である。



ホームICTにおけるHGWの位置付け

ホームICTではHGWがネットワーク内の各種サービス・サーバと連携することで，家電連携，宅内監視，リモートサポート，ヘルスケア，エネルギーコンサルタント等，多様なサービスを提供する。このため，HGWはネットワーク内のサービス・サーバがアプリケーションを配信するOSGiフレームワーク機構をサポートする。

*コミュニケーション・ネットワーク製作所　**情報技術総合研究所　***三菱電機マイコン機器ソフトウエア㈱

1. まえがき

三菱電機はホームICTを実現する宅内装置HGWに関する技術の標準化活動，技術研究に取り組み，現在開発を推進している(1)。

本稿では，今回開発したHGWの装置アーキテクチャと構成技術について述べる。**2章**では各種サービスやプロトコルに柔軟に対応可能な装置のアーキテクチャを示し，**3章**では装置実現のキーとなる，各サービスの連携・調停技術，VoIPの堅牢(けんろう)性技術，高速パケット転送技術について述べる。

2. HGWの装置アーキテクチャ

2.1 装置アーキテクチャ

HGWは将来にわたって進化する宅内機器やサービスに柔軟に対応する必要があり，まただれもが簡易に利用でき，また安心な暮らしをサポートできなければいけない。このため，HGWではNGNの基本機能であるVoIPやブロードバンドルータ機能のほか，各種サービスやプロトコルに柔軟に対応するプラットフォーム構成とする必要がある。これらの要求条件を実現するため，1GワイヤフルレートのIP(Internet Protocol)パケット高速転送が可能なパケット転送エンジン上で，複数の機能を独立に構成・動作可能にする装置アーキテクチャを実現した。

2.2 ソフトウェア・アーキテクチャ

ソフトウェアは，POSA(2)で紹介されているアーキテクチャ・パターンが広く知られているが，今回のHGW装置の開発にあたり，次に示す2つの要件を考慮して独自のソフトウェア構成を定義した。

①スケーラビリティ

日進月歩で進化する新しい技術の取り込みを容易にするため，機能の独立性，拡張性を確保する。

②ポータビリティ

他装置へのポータビリティを確保する。一例として，ONU(Optical Network Unit)にHGWの電話機能を搭載する場合，ルータ機能とVoIP機能に，ONU固有機能を搭載(プラグイン)することで新規装置を実現できる。

図1に示すようにHGWのソフトウェア構成は，マネージャー層，ミドルウェア層，サービス層，アプリケーション層の4階層の構成とした。

(1) マネージャー層

装置固有のハードウェア制御，競合制御を行う装置管理部と，上位層に対してデータベース機能，サービス連携・調停機能を提供するプロパティ管理部がある。これらの詳細については**3.1節**で述べる。

(2) ミドルウェア層

上位層と密に連携し，上位層が機能を実現するためのプロトコル制御を提供する。

(3) サービス層

HGWがユーザーに提供する各種サービスを実現する。

(a) 無線LANサービス

802.11nなどの無線LAN機能を提供するサービスである。

(b) ホームサーバサービス

DLNA(Digital Living Network Alliance)など，ホームICT機能要素を提供するサービスである。

(c) ルータサービス

ブロードバンドルータ機能に加え，通信事業者特有のサービスを実現するHGWの核となるサービスである。

(b) VoIPサービス

アナログ固定電話，及び，IP電話機能を実現するサービスである。

(e) 保守サービス

通信事業者特有の保守機能を提供するサービスである。

(4) アプリケーション層

サービス層が提供するAPI(Application Program Interface)を使って，装置の設定や高度な応用サービスを提供する。

(a) ユーザーインタフェース

GUI(Grapchical User Interface)やテレフォニー機能によって装置の設定や制御を行う。

(b) バンドル

OSGiプラットフォーム上で動作するアプリケーション(以下“バンドル”という。)が，サービス層を駆使することで，家電連携，宅内監視，ヘルスケアなどホームICTサービスをエンドユーザーに提供する。

3. HGWの構成技術

3.1 サービス連携・調停技術

HGWは各種サービスやプロトコルの拡張に柔軟に対応する必要があり，マネージャー層にプロパティ管理部を実

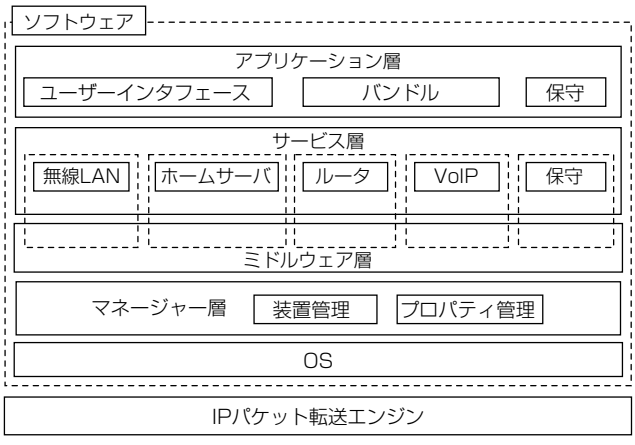


図1．HGW装置アーキテクチャ

装した。プロパティ管理部はデータベース機能とともに，サービス間を接続する通信機能を提供する。この通信機能によって，サービス層に実装するソフトウェアコンポーネントがプラグイン可能となり，スケーラビリティ，ポータビリティを実現する。

図2にプロパティ管理部の動作の一例を示す。無線LANサービスとVoIPサービスは値の変化を知りたい属性をあらかじめプロパティ管理部に購読要求しておく。ルータサービスが属性値を変更すると，無線LANサービスとVoIPサービスに変化通知がなされ，その後，必要な処理を行うことができる。無線LANサービスが存在しない装置を新たに開発した場合，このサービスから購読要求がなされないため，ほかのサービスに変更を加えることなくソフトウェアを構成できる。また，新たなサービスを追加した場合も，新たなサービスから購読要求がなされることで，自動的に必要な属性の変化が通知される。

先に述べたメカニズムは，スケーラビリティ，ポータビリティの観点で柔軟であるが，個々のサービスが完全に独立しているため，装置全体の動作の調停を行うことができない。そこで，プロパティ管理部のメカニズムの長所を維持して装置全体の動作調停機能を実現するために，装置競合制御マトリックスによる解決を図った。

装置競合制御マトリックスには，装置全体の競合制御条件が記述され，プロパティ管理部のデータベースと論理的にリンクしている。サービス層のプログラムは，ある処理を実行するとき，その処理を実行して良いかを装置管理部に問い合わせる。装置管理部は，サービス層が実行したい処理をキーに装置競合マトリックスを検査し，結果をサービス層に返す。

図3に装置競合制御の一例を述べる。緊急呼（110番など）通話中となりVoIPサービスはプロパティ管理部に緊急呼属性を有に設定要求する。その後，ユーザーインタフェースを介して装置のリセットが保守サービスに要求された場合，保守サービスは装置リセットを行ってよいか否かを装置管理部に問い合わせる。装置管理部は装置競合制御マトリックスを検査し，緊急呼通話中であるため，保守サービスに実行不可を返す。

3.2 VoIP堅牢性技術

HGWのアプリケーション層に属するバンドル部は，仮想マシン（VM），OSGiフレームワークを搭載し，ホームICTを実現する上で必要となるプラットフォームを提供する。また，OSGiフレームワークのみでは実現できないHGW固有の機能を提供するためにNI（Native Interface）を実装している。

ホームICTの各種サービスは，HGWが提供するこのプラットフォーム上で動作するバンドルが提供する。バンドルは，HGWが提供する様々なNIの機能，例えば，HGWの各種設定を行う機能，DLNA機能等を用いて，目的のホームICTサービスを提供する。バンドルは，公開されたAPI仕様に基づき，アプリケーションベンダーが製作し，同仕様に基づいた各社のHGW上で動作する。したがって，バンドルそのものの品質は，HGWベンダーがコントロールすることは不可能であり，その品質等に起因した異常動作により，HGWが提供する他のサービスに及ぼす脅威が考えられる。本HGWではこの脅威への対策をとっており，以下VoIPへの影響を防ぐために実施している内容について述べる。

バンドルはHGW内の各種リソースをNI経由で使用する。例えば，CPU（Central Processing Unit）であり，メモリであり，その他機能独自のリソースである。バンドルの暴走などによって，これらリソースが必要以上に消費され，直接的，間接的に，VoIPに脅威を与える可能性がある。緊急呼を実現するVoIPは宅内のライフラインであり，HGW上で動作するバンドルが異常動作しても，VoIPに影響を与えない構成とする必要がある。**図4**にHGWのバンドル部の構成と脅威の概念図を示す。

バンドルの異常動作によるVoIPに関連する影響は以下のように分類ができる。

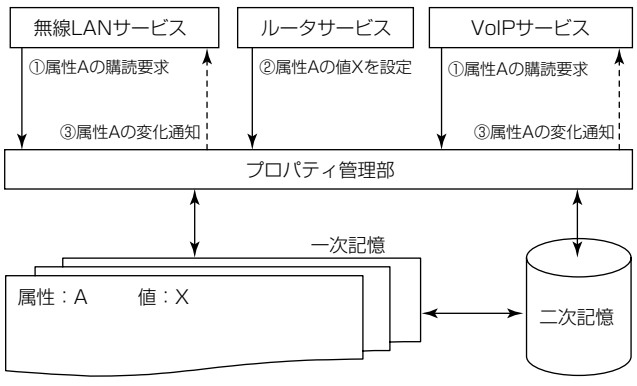


図2．プロパティ管理部

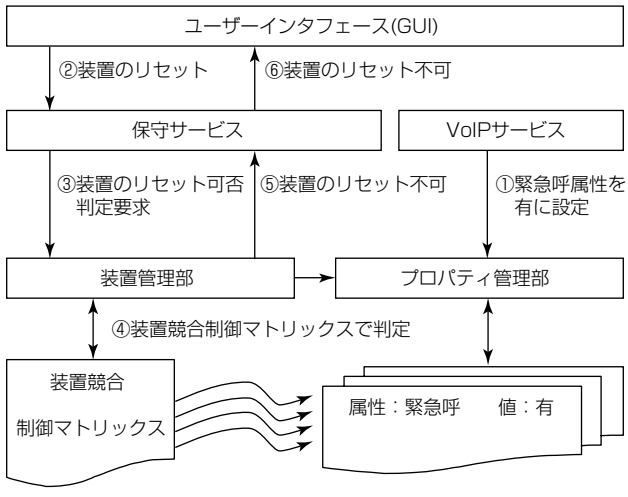


図3．装置競合制御

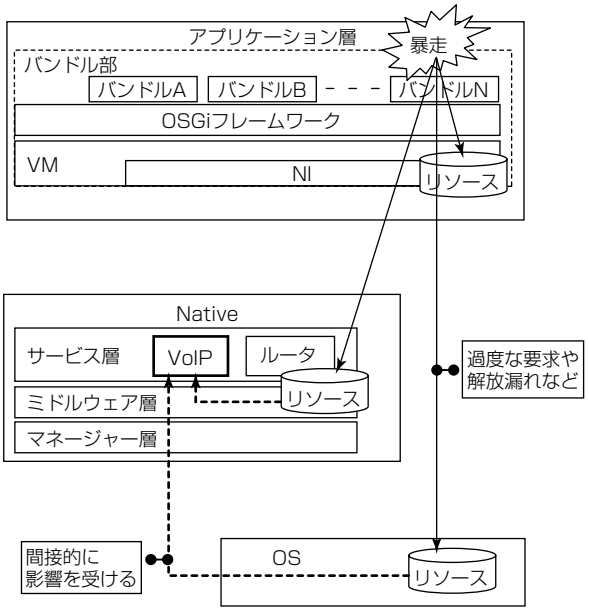


図4．バンドル部の構成と脅威

⑴ CPU占有による，VoIP通信品質の低下
⑵ 大量メモリ消費による，VoIP処理失敗
⑶ バンドルが連続でNIを呼び出し，サービス層以下のリソースを占有することによるVoIP通信品質の低下
⑷ バンドル暴走によるVMの強制終了時の，各種リソースの解放漏れ。VMが再起動した際の，解放漏れリソースの影響によるVoIP処理失敗

三菱電機はこれらVoIPに対する脅威に対応するため，次の対策を実装した。

＜対策1＞

HGWのOSは，プロセスごとの優先度設定機能を持たせている。VoIPプロセスの優先度を高く設定し，VMプロセスの優先度を低く設定することで，VoIPプロセスのCPUリソースを確保し，通信品質の低下を防ぐ。

＜対策2＞

VMは最大メモリサイズを設定可能で，そのサイズを超えてメモリを確保することは不可能なように設計されている。メモリ不足による脅威は，この機構によってガードする。

＜対策3＞

NI呼出しを監視する機構を設け，n回/秒以上の呼出しを制限する。これによって，バンドルが暴走し，NIを必要以上に呼び出したとしても，VoIPに影響を与えないようにする。

＜対策4＞

3．1節で述べたプロパティ管理部でVMプロセスの起動・停止という状態を管理する。一方，サービス層のプログラムは，プロパティ管理部へVMプロセスの起動／停止状態の購読要求を行い，状態の変化を通知してもらうよう依頼する。VMが停止すると，プロパティ管理部はその状態を購読依頼されているすべてのプログラムに状態変化通知として発行する。この通知を受けたプログラム側は，VMが停止して，不要となった各種リソースを解放する。これらによって，リソース解放漏れによるVoIPへの影響を防ぐ。

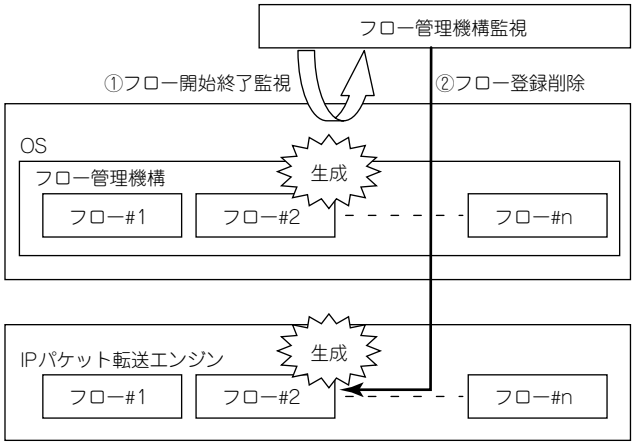


図5．ファスト・パス制御の概念

3．3　高速パケット転送技術

家庭内に接続される機器の性能向上に伴い，HGWには高い処理性能が要求される。このため，HGWではファスト・パス制御機能により高速パケット転送を実現した。ファスト・パス制御ではOS標準のフロー管理機構によるフローの生成・削除を，フロー管理機構監視機能を用いて外部から監視し，フローの生成・削除を検出した場合には，IPパケット転送エンジン機構に登録する。IPパケット転送エンジンは登録されたフローに該当するパケットに対して，OSのプロトコルスタックを使わずにパケット転送のみに特化した高速転送処理を実現する（**図5**）。

4．むすび

今回開発したHGWの装置アーキテクチャと採用したキー技術を述べた。今後，次世代に向けたHGWの機能拡張を行うとともに，開発した技術の他装置への適用を行う予定である。

最後に，この開発にあたり，多大なるご指導をいただいた関係各位に深く感謝の意を表す。

参考文献

⑴ 牧野豊司，ほか：ホームICTへの取組み，三菱電機技報，**84**，No.8，449～452（2010）
⑵ Buschmann, F：Pattern-Oriented Software Architecture Volume 1，A System of Patterns. Chichester，Wiley，ISBN 0471958697（1996）