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。

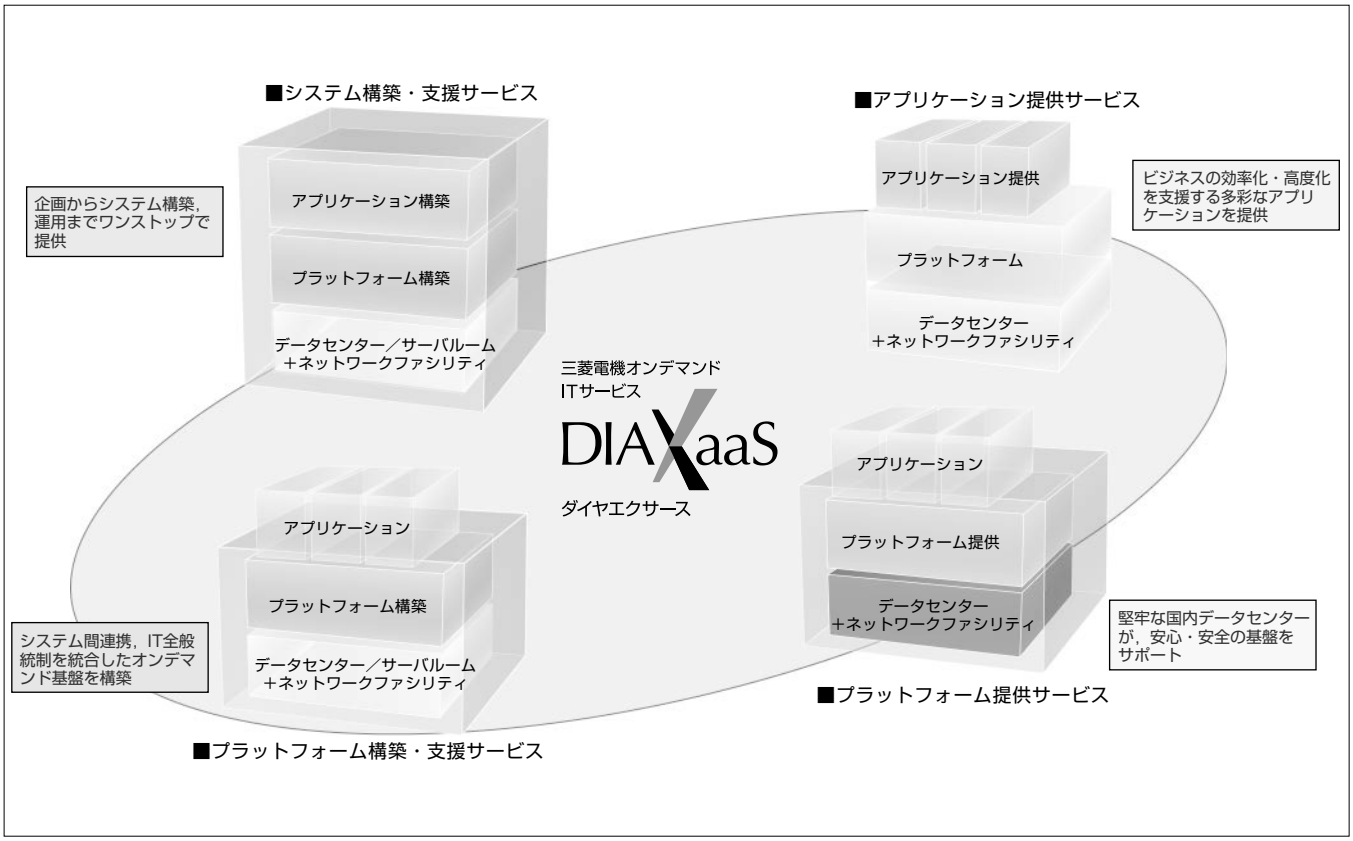
(1) 総務省医療情報向けガイドラインに準拠した高いセキュリティ管理レベル

(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

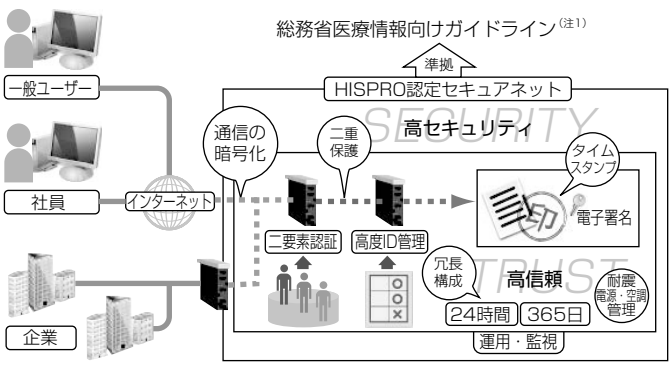
3.1節で述べた脅威に対して，ASP(Application Service Provider)・SaaS(Software as a Service)事業者が，提供するサービス内容に即した適切な情報セキュリティ対策を実施するための指針として，ASP・SaaS普及促進協議会より“ASP・SaaSにおける情報セキュリティ対策ガイドライン(2008.4)”(以下“ASP・SaaSガイドライン”という。)が公表されている。一般的なサービス事業者ではガイドラインに準拠したサービスが提供されていくと考えられる。

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

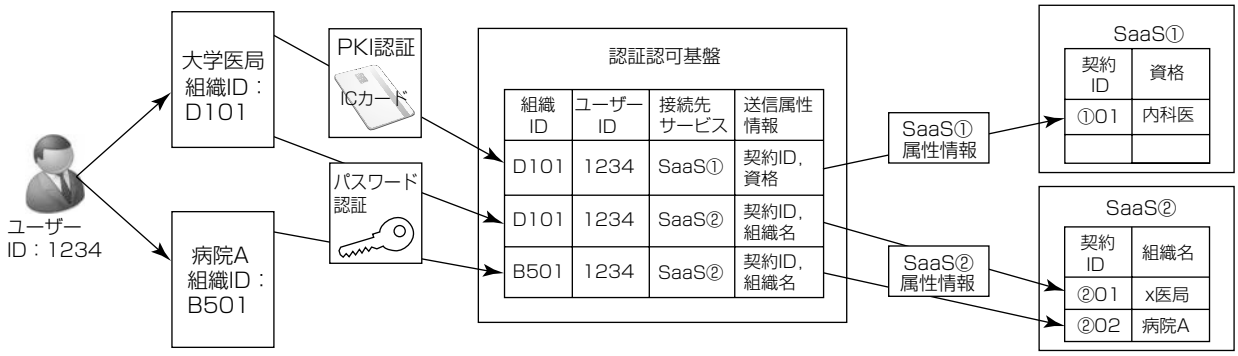


図2．認証認可基盤の利用例

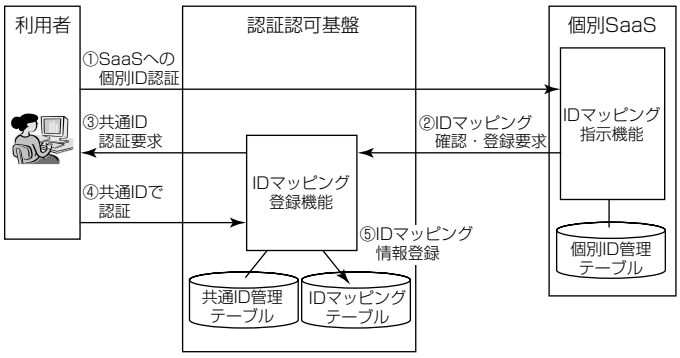


図3．IDマッピング自動登録方式

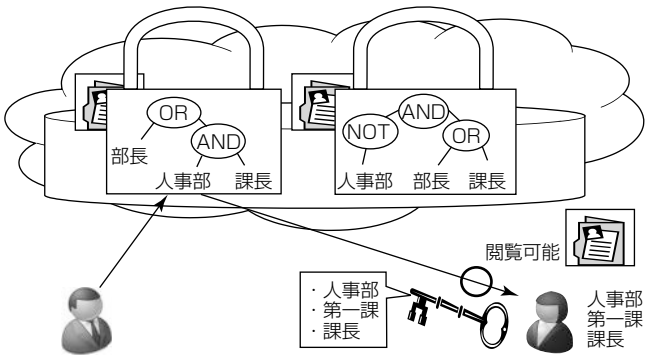


図4．新世代暗号方式の利用例

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

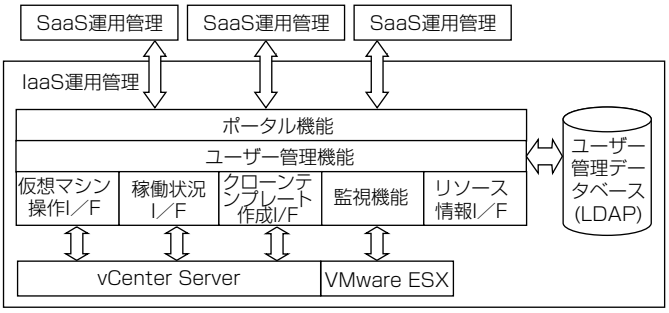
データセンターの物理セキュリティレベルを，ビル入館，ロビー，マシン前室，サーバ室の4段階に分けた物理セキュリティ管理を行っている。最もセキュリティレベルが高いサーバ室では，生体認証，サークルゲートを使った共連れ防止等を実現している。これら管理の仕組みは，FISC（金融情報システムセンター）の“金融機関等コンピュータシステムの安全対策基準”に準拠している。

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）