ISSN 0369-2302 CODEN:MTDNAF

MITSUBISHI
Changes for the Better

家庭から宇宙まで、エコチェンジ eco Changes

三菱電機技報

7 2013
Vol.87 No.7

企業・社会の快適・安心・発展を支えるITソリューション

三菱電機技報 Vol. 87 No.7 2013

目　次

表紙：企業・社会の快適・安心・発展を支えるITソリューション

三菱電機は，クラウド技術，情報セキュリティ技術などを適用したITソリューションを提供することによって，企業及び社会の快適・安心・発展に貢献していく。

表紙では，企業・社会を表すビル群，顧客のデータを預かり安全に守るデータセンターを配置し，それらがデジタルネットワークでつながり，ITが支えている様子をイメージ図で表現した。

巻/頭/言

クラウドサービス利用拡大への期待

The Expectation to the Expansion of the Use of Cloud Services

五月女健治
Kenji Saotome

だれもが，安価で安全に，しかも簡単にコンピュータ資源を活用できるようになるために，クラウドコンピューティングへの期待が大きい。クラウドは，水道や電気などの社会インフラのように，それがどこでどのように作り出されているか知ることなく，簡単に利用できる可能性があるからでもある。しかし，手放しで利用するというのはあまりにもリスクが大きい。だからと言って，当分はまったく無視すると，コスト競争の激しいビジネスの環境で勝ち抜くことが難しくなるかもしれない。クラウドという言葉を耳にして数年，どのような状況にあるか見ることにしよう。

クラウドの出現は，インターネット利用拡大によるところが大きい。1994年頃から，現在インターネットの世界を席巻(せっけん)しているIT企業の創業が相次いだ。クラウドという言葉は，2006年にグーグルのエリック・シュミット氏が，“Search Engine Strategies Conference”で自社のサーバ群を“クラウド”と表現したのが始まりとされ，その後，IT企業が，次々とクラウドサービスをスタートさせた。このようにクラウドの歴史はまだ浅いが，利用環境が整い始めて，その活用が広まっている。

クラウドの最大の不安は，セキュリティと信頼性である。

セキュリティについては，社外，さらには海外で管理されることへの不安が大きい。ひとつの例として，「米国愛国者法」がある。米国はクラウド先進国で，データセンターのほとんどを米国に設置している。2001年９月11日に発生した同時多発テロを契機に，「米国愛国者法」が制定され，捜査機関がデータセンター内のプライバシー情報の提出を求めることも可能になったのである。すなわち，米国にある自社の情報が，米国による捜査対象となる可能性があるということである。

信頼性においても，クラウドサービスの障害や利用者に自由にならない定期メンテナンスによるサービスの停止がある。障害については影響の小さい範囲でたびたび報告されているが，すべてのデータが失われ，大きな社会問題になった事件も起こっている。

しかし，クラウドの不安要素の解消や向き合い方が浸透して，クラウドの利用が進みつつある。

経済産業省，総務省から，クラウド提供者及び利用者への指針・ガイドラインが公開され，それを受ける形でいろいろな対策が具体化されている。

クラウド提供者の信頼性が大きな懸念材料となるが，安全・信頼性の情報開示基準を満たしているサービスを認定する“ASP・SaaSの安全・信頼性に係る情報開示認定制度”が発足した。これによって，利用者にとってはクラウドで提供されるアプリケーション(ASP(Application Service Provider)・SaaS(Software as a Service))の選択肢が広がり，サービス提供者にとってはユーザー獲得の機会を広げることが期待できる。

また，日本ユーザー向けに，海外のクラウド提供者が日本でデータセンターを開設する動きが進んでいる。日本のベンダーも，当然ながら日本にデータセンターを開設して，クラウドサービスの提供を開始し，データの在り場所についての不安が軽減されている。

情報を入手しづらい中小企業向けに，IPA((独)情報処理推進機構)は，“中小企業のためのクラウドサービス安全利用の手引き”を発行して，分かりやすいクラウド導入方法を示している。

大企業が，まずクラウドの活用を行うことは想像できるが，国や地方自治体のクラウド活用もすでに始まっている。2009年家電エコポイント制度が制定され，家電エコポイントシステムでクラウドサービスを採用し，短期間でシステムを完成させたという。

中小企業では，クラウドで提供されるWebメールやオンラインストレージの業務での活用が始まりつつある。オンラインストレージとは，クラウド上のストレージを貸出すサービスである。2011年３月11日の東日本大震災によって，BCP(事業継続性計画)が注目されているが，このBCP対策に有効な手段であり，利用が広がるものと思われる。中小企業も，このようなクラウドを利用することで，効果や課題が実体験でき，本格的なクラウド利用の足掛かりになれば，クラウドの利用はいっきに加速するであろう。

クラウド活用には，利用者である当事者の正しい認識が必要である。日本企業の競争力の維持・強化のためにもクラウド活用は不可欠であり，クラウド提供者は，利用者を啓蒙する責任を担っている。

◆法政大学経営大学院 イノベーション・マネジメント研究科 教授
Professor, Hosei Business School of Innovation Management

特集論文

イオンモール㈱向けITインフラBCP対策

片谷二郎* 岩崎郁来*
飯塚和貴* 渡辺直之*
加藤美彦*

The Business Continuity Planning in IT Infrastructure for AEONMALL Co.Ltd

Jiro Kataya, Waki Iizuka, Yoshihiko Katou, Ayana Iwasaki, Naoyuki Watanabe

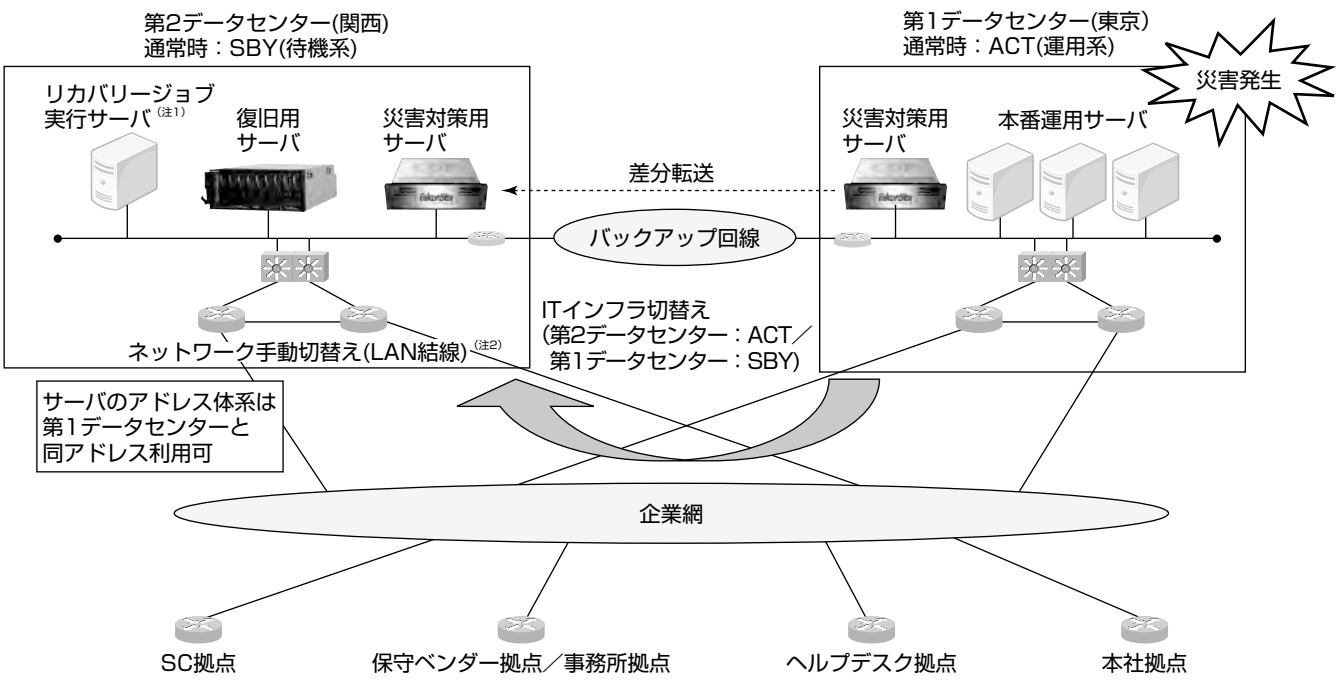
要　旨

東日本大震災以降，各企業で事業継続／災害対策が急務となり，検討・対応が推進されてきている。三菱電機インフォメーションシステムズ㈱(MDIS)の顧客であるイオンモール㈱でも，2011年からBCP(Business Continuity Planning)対策の検討を開始しており，ITインフラ全般にかかわっているMDISが中心となってBCP対策を進めることになった。

都内のデータセンター(以下“第1データセンター”という。)には約60システム(約200サーバ)が集約されており，全国のショッピングセンター(SC)及び関係場所(事務所，保守ベンダー拠点)約90拠点からネットワークを介して業務を行っている。利用規模はパソコン約2,000台，POS(Point Of Sale)端末約15,000台である。

MDISが推進したイオンモール㈱向けITインフラBCP対策プロジェクトでは首都圏直下型地震等の大震災(震度6以上)によって，関東近郊の社会インフラが途絶することで電源供給断などが発生し，第1データセンターが機能しなくなることを前提としている。MDISはITインフラBCP対策として，他社複数ベンダーが構築した45システム(120サーバ)を対象システムとし，これら全てを改修することなく，かつ同じオペレーションで統一的に関西地区のデータセンター(以下“第2データセンター”という。)に復旧する仕組みを構築した。ITインフラBCP対策システムの構築は2012年4月から約1年をかけて完遂し，運用を開始している。

なお，BCP発動後のITインフラの切替えは，第2データセンター内オペレータによって，“ネットワーク切替え(第1データセンター⇒第2データセンター)”と“システム復旧”を手動で実施する運用としている。



(注1)　仮想環境下でリカバリージョブを実行し，システム復旧を行う。
(注2)　災害時に第2データセンター側の専用ルータにLANケーブルを差しこむ(通常時：未結線)ことで，ネットワーク切替えを実現する。
日々の差分転送はバックアップ回線を通し，第2データセンターの災害対策用サーバに格納される。

ITインフラBCP対策システム

通常時は第1データセンターはACT(運用系)，第2データセンターをSBY(待機系)とし，非同期でデータ連携を行う。災害時は第2データセンターでネットワークの切替えとシステム復旧を手動で行うことでITインフラの切替えを行う。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

MDISはイオンモール㈱(以下“顧客”という。)と2005年にITアウトソーシング契約を締結し，IT全般にかかわる業務を担ってきている。主な業務はデータセンター，ネットワーク(WAN，データセンター内LAN，各拠点)，仮想化を含めたITインフラ，端末管理，システム運用・監視，ヘルプデスク，情報システム企画支援，情報システム管理等である。2010年から2011年には，約20社の各システムベンダーが構築した約50システムのサーバ仮想化統合を推進し，現在までに約60台の物理サーバを仮想化(VMware vSphere(注3))環境へ移行し運用している。

2011年の東日本大震災によってBCP対策の機運が顧客内部で高まる中で，顧客全社に先駆けてシステム部で対策を練ることになり，各システムが災害後も継続利用できる方法を検討することになった。そこで，ITアウトソーシング・物理サーバ仮想化を実現し，顧客ITインフラ全般に携わるMDISがBCP対策を進めることになった。

BCP対策に向けての課題は多種多様なシステムに対して，⑴現行システムへの改修を行わず(同一IPなど)統一的な方式を採用すること，⑵個別要件を満たすRPO(Recovery Point Objective：目標復旧時点)とRTO(Recovery Time Objective：目標復旧時間)を達成すること，⑶運用の簡易化及び拡張性のある構成にすることであった。

本稿ではこれらの課題を踏まえて取り組んだITインフラBCP対策システム構築の内容について述べる。

(注3) VMware vSphereは，VMware，Inc. の登録商標である。

2. 要件定義

2.1 改修を伴わない統一的な方式

BCP対策対象システムのほとんどが他ベンダー構築のシステムであった。そのため，第2データセンターに切り替えて運用する際に，サーバのホスト名，IPアドレスなど固有値を変更することの影響範囲を把握することが難しかった。また，サーバのホスト名，IPアドレスを変更することで，システム利用者が通常通りに利用できなくなってしまう。したがって，現行システムへの改修を行わないことが最善であった。

そして，システムごとにBCP対策方式が異なることは運用を煩雑化させるので，統一的な方式で全対象システムに対してBCP対策を実施する必要もあった。これらの要件から，システムに依存しないバックアップが可能で，サーバ固有値を変更することなく第2データセンターで復旧できるBCP対策システムとして，コスト面なども考慮し，FalconStorCDP(注4)を採用した。

(注4) FalconStorCDPは，FalconStor Software，Inc. の登録商標である。

2.2 RPO／RTOの取り決め

RPO／RTOの設定は，顧客が事業継続に必要とするシステムを把握することと，顧客の要望に応えることが可能かどうかを確認する上で重要な数値となる。

設定にあたっては，第3者的視点を持つために，“顧客影響度”“収益影響度”“業務影響度”“データ重要度”の4項目を定義し，システムごとに数値化(1～3)して，その合計値(最大12)から，RPO／RTO数値を取り決めた。その結果から，各システムを6段階のRPO／RTOレベルにグルーピングし，その中でRPO／RTO数値の降順に優先順位を設定した(**図1**)。

2.3 容易な復旧方法と継続的な運用

首都圏直下型地震等の大震災(震度6以上)発生時に，MDISがシステムの復旧操作を実施できない可能性を考慮し，誰でも容易に復旧操作を実施できることが重要である。実際にBCPが発動され，システム復旧を実施する場合，非被災場所である第2データセンターのオペレータが統一した手順に沿って復旧操作を行うことになる。

さらに，BCP対策には終わりはなく継続的運用をするために，バックアップデータを保護するストレージと復旧用のサーバを追加することが容易な構成とした。

3. ITインフラBCP対策設計

3.1 第2データセンター選定

第2データセンター選定もMDISの作業範囲にあり，最初に地震，原子力，水害等の災害リスクの低いエリアから耐震構造，給電方式，自家発電の対応時間等をベースに8つのデータセンターを候補として選定した。その上で，ネットワーク設備のキャリアフリー対応，運用サービス形態等に加え，顧客グループ全体で利用できるキャパシティを考慮するなど，グループ会社全体のBCP対策を考え，最終的に関西地区にあるデータセンターに決定した。

	A	B	C	D	E	F
RPO	1時間前	半日前	2日前	2日前	2日前	指定なし
RTO	1時間	半日	2日	1週間	2週間	2週間～
1	A1システム	B1システム	C1システム	D1システム	E1システム	F1システム
2	A2システム	B2システム	C2システム	D2システム	E2システム	F2システム
3	A3システム	B3システム	C3システム	D3システム	E3システム	F3システム
4	A4システム	B4システム	C4システム	D4システム	E4システム	F4システム
5	－	－	－	D5システム	E5システム	F5システム
6～	－	－	－	D6システム …	E6システム …	F6システム …

(高) 優先順位 (低)

RPO：データを戻す時点，RTO：システム復旧にかかる時間

RPO 災害発生時点 RTO

図1．RPO／RTO一覧

3.2 データ連携方式の検討

⑴ データセンター間データ連携方式

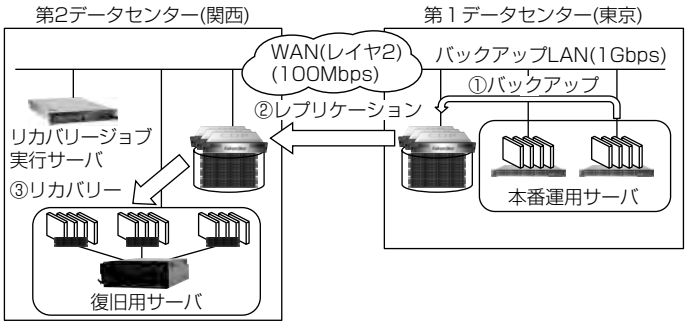
第2データセンターで運用するシステムは，第1データセンター内にバックアップ取得したデータを用いて復旧を行う。データセンター間のデータ連携方式として，①第1データセンター・第2データセンターをACT（運用系）・ACTにした双方向レプリケーションでのリアル同期方式，②第1データセンターはACT，第2データセンターをSBY（待機系）とする非同期の方式，そして③データ部のみを第2データセンターへバックアップする方式を検討した。結果，コスト面，運用，復旧時間等の要件から方式②を顧客のBCPデータ連携方式に決定した（**図2**）。

⑵ アプリケーション非改修及びバックアップ方法

複数システムのBCP対策で，バックアップを行うためにシステムごとにアプリケーションを改修することは膨大なコスト増につながる。そのため今回は，アプリケーションを改修することなく，システムごとに，OSを含むシステム全体をアーカイブとしてバックアップし，レプリケーションする方式を採用した。また，このバックアップデータを用いることでサーバ固有値を変更することなくシステムを復旧させることが可能である。

⑶ システム単位のデータ同期方法

第1データセンターと第2データセンターのデータ連携を非同期としたため，第1データセンターのバックアップ後にレプリケーションが実行されるようにするなど，決められたスケジュールでデータの同期を行える仕組みが重要である。 バックアップ，レプリケーションの回線の負荷を平準化させつつ，帯域内でシステムごとに異なるRPOを満たすデータ同期のスケジュールを設定した。



①バックアップ：システムをOSを含むDISK単位でCDPサーバへバックアップ
②レプリケーション：第1データセンターのCDPサーバから第2データセンターのCDPサーバへバックアップデータを転送する
③リカバリー：復旧用サーバへシステムを復旧させる
CDP：Continuous Data Protection

図2．データ連携方式

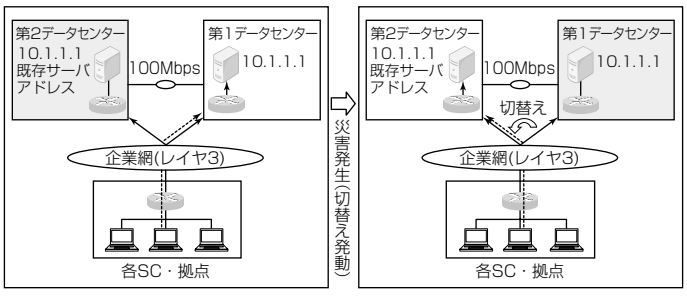


図3．ACT／SBY側によるネットワーク切替え

3.3 ネットワーク設計

⑴ 拠点ネットワーク

当初，第1データセンターと第2データセンターのネットワークアドレス体系は別とし，サーバのIPアドレスを同一とするために，各拠点にNAT（Network Address Translation：IPアドレス変換）用のファイアウォールを導入し，BCP発動時に各拠点でNAT用のファイアウォールに切り替えることで，異なったネットワークアドレス体系を意識することなくサーバへのアクセスを可能とする案で検討を進めていた。しかし，各拠点の作業者への教育やBCP発動時の連絡体制などに対する問題から，別の案を検討することとなった。

検討を重ねた結果，動的ルーティング（Border Gateway Protocol：BGP）を利用できる新ネットワーク網にネットワーク全体を変更し，第1データセンターと第2データセンターのネットワークアドレス体系を同一にすることに決定した。サーバIPアドレスを変更せず，かつ自動でネットワーク全体を切り替えることが可能となったため，第1データセンターが利用不能となった際，全拠点を一斉に第2データセンターに切り替えることができることになった（**図3**）。なお，既存ネットワーク網を新ネットワーク網に変更する作業として約3か月間，全国約90拠点の現場に赴き，夜間帯の工事で動的ルーティングに対応したネットワークへの変更を実施した。

⑵ データセンターネットワーク

第1データセンター内にバックアップLAN（1Gbps）を新設し，新設したLANを通してバックアップを行うことで，既存のネットワークに影響を与えない設計とした。

また，データセンター間にバックアップ回線（100Mbps）を新設し，新設したバックアップ回線を通してレプリケーションを実施する設計とした。

4. 工 夫 点

4.1 バックアップ・レプリケーションのスケジュール

リカバリーに使用するバックアップデータはレプリケーション終了後のデータとなる（**図2**）。そのため，レプリケーションが終了するまで，第2データセンターでは最新のバックアップデータを利用できない。したがって，バックアップ終了からレプリケーション終了までの間に災害が発生した場合，最新のバックアップ時点に復旧することができず，1つ前のバックアップデータが復旧時点となる。そのため，バックアップ及びレプリケーションのスケジュールは，バックアップ開始からレプリケーション終了を

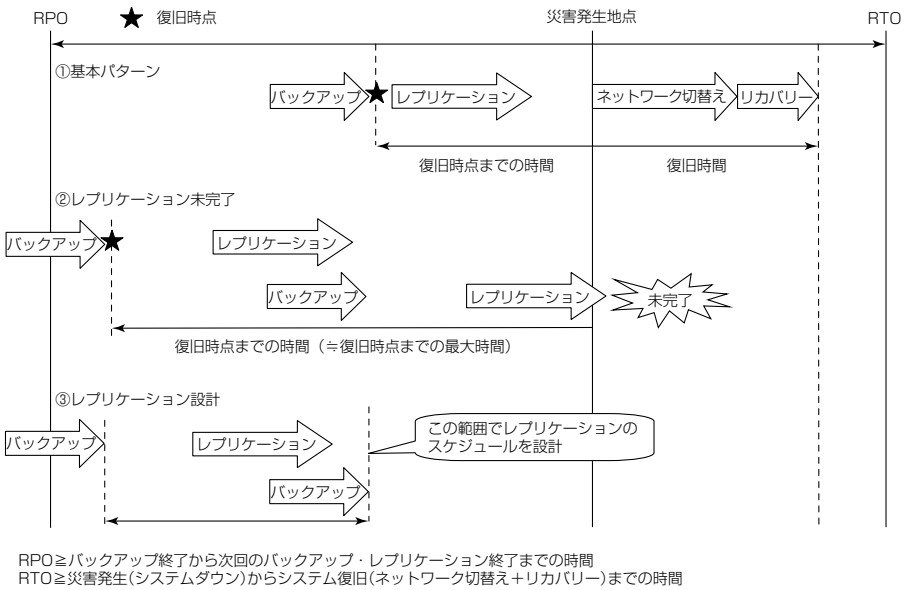


図4．バックアップ・レプリケーション設計

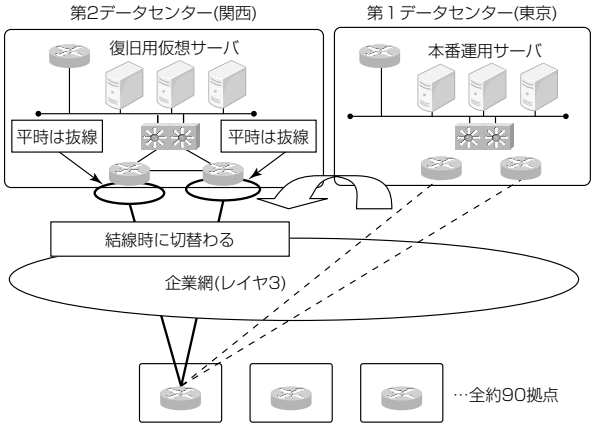


図5．新ネットワーク網によるネットワーク切替え

RPO内に収める設計をするのではなく，バックアップ終了から次回のバックアップを対象とするレプリケーションが終了するまでをRPO内に収める設計が必要である(**図4**②)。

また，レプリケーションは次回バックアップ終了時までに終了すればよいため，レプリケーションを行う回線の負荷分散を考慮したスケジュールを組んだ(**図4**③)。

全システムのスケジュールを1つの表にまとめることで時間帯ごとのレプリケーション数を数値として可視化し，時間帯ごとのレプリケーション数を均等とすることで，レプリケーションを行う回線の1日の負荷を均一とした。

4.2 BCP発動時のネットワーク切替え

当初，新ネットワークは通信の優先順位を第1データセンター＞第2データセンターとし，第1データセンターのネットワークが利用不能となった場合に，自動切替えで第2データセンターがACTになる方式としていた。しかし，この方式には，2つの課題があることが分かった。1つ目は，災害ではない通常障害でも自動で第2データセンターに切り替わってしまうこと，2つ目は，関東近郊の社会インフラが途絶し対象システムが利用できなくなったにも関わらず，第1データセンターのネットワークが落ちなかった場合に，自動切替えが発生しないことである。

そこで，通信の優先順位を第1データセンター＜第2データセンターとし，第2データセンターのネットワークが有効となった場合に，自動切替えで第2データセンターがACTになる方式として，第2データセンターのLANケーブルを通常時は抜いておく運用とした。

これらのことから，ネットワーク網が誤って自動で切り替わることがなく，BCP発動時には，非被災地の第2データセンターのオペレータがLANケーブルを結線するだけで，“ネットワーク切替え(第1データセンター⇒第2データセンター)”を実施できる仕組みを構築した(**図5**)。

5. むすび

BCP対策は費用対効果の観点から，被災によるビジネスに対する影響と，対策を講じるための費用のバランスをとることが重要であり，対象システム範囲とRPO／RTOを定量的に導き出すことが鍵となる。

今回の事例では，提案(2011年)から2年を掛け，顧客とMDISが一体となってITインフラBCP対策システムを構築した。BCPとは本来企業内の各組織が一体化して取り組む施策であり，システムごとのBCP対策では，設計思想のずれやコストのオーバーヘッドが大きくなることが懸念されるが，このプロジェクトでは，長年にわたるITアウトソーシング業務やサーバ仮想化を遂行したノウハウを活用したこと，汎用的なBCPシステムを採用したことによって，個々のシステム要件(RPO／RTO，データ量，仮想化サーバ可否，データベース有無等)を満たした上で，運用の統一，コスト抑制等の“全体最適”を実現することができた。

特に，今回採用したBCPシステムは，ディスク単位でのバックアップやリカバリーが可能なため，一般的なバックアップシステムに代わるものとしても非常に有効である。

MDISは今後もBCP対策機器の追加・変更，運用見直し等による各種マニュアルの改訂や定期訓練等，BCM(Business Continuity Management)の観点で，アウトソーサーの立場として継続的に対応し続ける。また，このプロジェクトを通して得たノウハウや，この事例のバックアップ方式をバックアップ提案例の1つとし，今後ともBCP対策ソリューションの提供に取り組んでいく所存である。

特集論文

災害対策として有効なデータセンターの活用

宮嶋智裕*
松尾英治**

Effective Use of Data Center for Disaster Recovery

Tomohiro Miyajima, Hideharu Matsuo

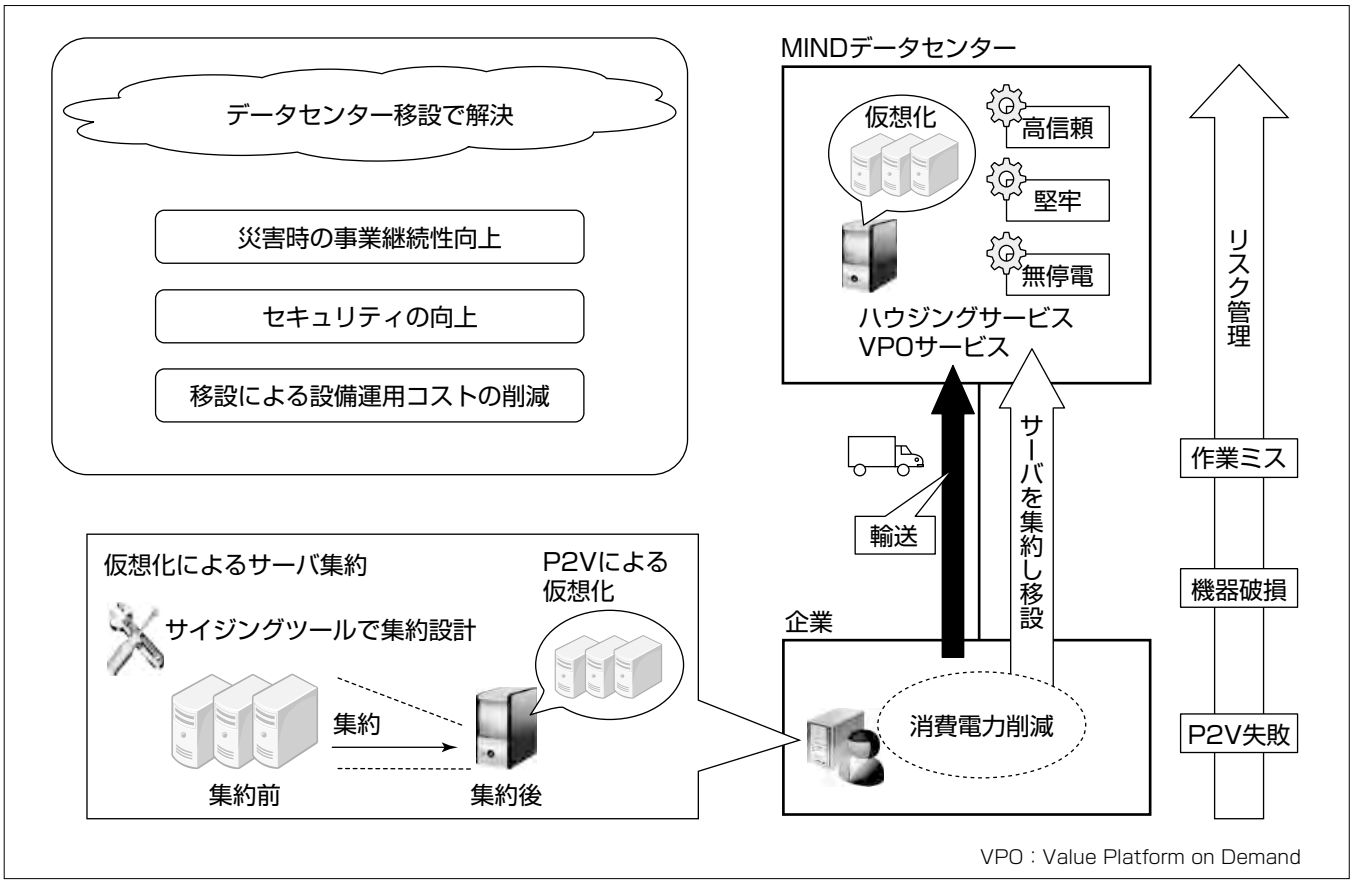
要　旨

データセンターという言葉は多くの企業で一般的に通用する言葉となっており，データセンターは既に企業の情報システムの中核を担う存在となっている。データセンターの市場規模は約１兆2,000万円と言われており[(1)]，今後も成長トレンドが続き，データセンターに関連する仮想化技術，クラウド技術などの発展が促されていくものと予想されている。

また，東日本大震災によってデータセンターに対する企業の見方が大きく変わり，今後データセンターは単なる企業の情報システムの設置場所という位置付けから，企業における，事業継続を検討するうえでも非常に重要な拠点へと変貌していく。

このように変化する状況のなか，三菱電機情報ネットワーク㈱(MIND)は1999年からデータセンター事業を東京都内で３拠点，名古屋，大阪に各１拠点の計５拠点で行っており，これまでの事業実績及び，豊富な経験を活用し，顧客の様々な要望に対してサービスを継続的に提供している。

データセンターを利用する場合，自社の設置環境から情報システムを移設するというケースが大半である。情報システムをデータセンターへ移設する場合，総コスト削減などのためにはサーバの仮想化が有効であり，仮想化では，サイジング技術，P2V(Physical to Virtual)技術が必要である。さらに移設に際してはリスク対策を事前に講じておくことが重要である。実際にデータセンターへ移設した事例を挙げて，データセンター利用によるコスト削減効果について述べる。



データセンターの利用例

企業でサイジングツールを利用し，サーバの集約設計を行い，P2Vで仮想サーバを構築する。その後，データセンターへの輸送ではリスク管理を行いながら実施することでデータセンターを有効に利用することが可能となる。

*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

データセンターとは耐震性に優れたビルに様々な通信回線を引き込み，自家発電設備や無停電電源装置(UPS)を備え，空調設備が完備された，機器の安定稼働を実現する施設である。このようなデータセンターを利用する企業がここ数年で増加しており，既にデータセンターを用いて企業のICT(Information and Communication Technology)環境を構築することが一般的となっている。

加えて現在では，単に自社の管理・保守するサーバをデータセンターに設置(ハウジング)するだけでなく，仮想化技術を用いてサーバを集約し運用コストの低減を行ったり，自社サーバの利用からデータセンター事業者が提供するサーバを利用するホスティングへ移行したり，データセンターを離れた拠点に複数用意するといった事業継続計画を考慮したりと，企業にとってデータセンターをどのように利用するかが重要になっている。

MINDではデータセンターを基盤とし，アプリケーション提供，セキュリティ対策，ネットワーク構築，日々の運用等の様々なレイヤで，サービスの提供を行っている。

本稿では某社が実際に仮想化技術を用いてサーバ集約を行い，データセンターへ移設した事例について述べる。

2. 災害対策としてのデータセンター利用

東日本大震災によってデータセンターに対する企業の見方が大きく変わった。しかし，ただ闇雲に情報システムをデータセンターに設置すれば，すべてがうまくいくわけでもなく，データセンターを利用するための課題をまとめた。

2.1 データセンターの必要性

2011年3月に発生した東日本大震災に伴い，企業の情報システムを継続稼働させる対策について変化が生じてきている。従来は機器障害に備えた取組みが主であったが，震災以降，社会インフラや金融システム等の重要なシステムと同様に，企業の情報システムについても電力，オフィスビル等のファシリティ全体を考慮した取組みへと変わってきている。

内閣官房情報セキュリティセンターが発表した“東日本大震災における政府機関の情報システムに対する被害状況”最終報告書[(2)]では，震災による被害は電力喪失による停電が最も多く，次に，ネットワーク障害，オフィスビル被害の順となっている。また，震災後に行われた計画停電についても，調査対象の半数が計画停電の実施対象に含まれたと述べられており，その内38%が勤務時間外に実施された計画停電への対応を行っている。計画停電の対応については，計画停電時の情報システム停止・再稼働の対応以外にも，システム利用者へのサービス停止の周知や，計画停電に向けた情報システムの改修と試験，ベンダーへの作業対応の要請などの作業が発生する。これらの作業は計画停電が計画された時点で，その実施有無にかかわらず行う必要があり，物理的な被害報告だけでは把握できない人的リソースへの負荷の増大が問題として挙がっている。

情報システムの停電対策の1つとしてオフィスビルに設置していた情報システムをデータセンターへ移設することが挙げられる。データセンターに情報システムを移設することで，オフィスビルが被災した場合でも情報システムを稼働し続けることが可能となり，また，計画停電の影響も，最小限にとどめることが可能となる。実際に，日本データセンター協会からは，東日本大震災の地震によるデータセンター被害・停止はなかったとの報告がされている[(3)]。

加えて，情報システムを利用するための広域ネットワークについても，回線キャリアの報告によると，特に被害が深刻であった地域を除いては2日程度で所要拠点間の中継が復旧したとのことである[(4)]。また回線キャリア各社で今後のルート分散等の堅牢(けんろう)化も検討されており，更なるネットワークの復旧時間短縮が期待される。

このように，広域のネットワークがつながっている環境であれば，データセンターに情報システムを移設することで，災害時であっても情報システムを継続して利用することが可能となる。

2.2 サーバ仮想化の手段

データセンターへの情報システムの移設が災害時に有効な対策であるものの，実際にデータセンターを利用するにあたり，コストの問題から躊躇(ちゅうちょ)するケースが少なくない。オフィス内のサーバ室を利用していた場合はデータセンターへの移設によって，利用ラック数，消費電力量などによって，相応のランニングコストが新規に発生することとなる。このコストを削減する方法として，サーバ仮想化技術によるサーバ集約が期待されている。

サーバ仮想化技術は，1つの物理サーバ上に，複数の仮想的なサーバを稼働させる技術であり，物理的なサーバ数を集約し，結果，ラック数，消費電力の削減が実現できる。

MINDでは，顧客のサーバ仮想化の導入に対し，2つのモデルに分け対応を行っている。1つは，顧客自身で仮想化したサーバをハウジングサービスで受け入れる対応であり，もう1つは，MINDがサービス提供しているIaaS(Infrastructure as a Service)型プラットフォームサービスVPO上に顧客の情報システムを受け入れる対応である。ハウジングとは異なり，サーバやストレージなどの機器をMINDが管理・運用を行うモデルであり，顧客はラックより細かいサーバ単位での契約が可能となる。

ハウジングで受け入れる場合，従来のハウジング同様に，顧客が仮想化したサーバをMINDデータセンターのハウジング領域に移設する。

VPOで受け入れる場合，MINDで用意した，仮想化した

サーバに顧客はシステムの移行を行うこととなる。

2.3 移設における検討課題と対策

データセンター移設でサーバ仮想化が有効ではあるが，この移設には何点か課題が存在する。情報システム運用者にとっては，①サーバ集約台数の見積り，②既存サーバから仮想サーバへの移行，③データセンターへの移設におけるリスク管理等が課題として挙がる。

2.3.1 サーバ集約台数の見積り

情報システムを仮想化したサーバに集約する場合，何台の物理サーバに集約することができるか，台数を見積もる必要がある。仮想化したサーバでは１台の物理リソースを複数の仮想サーバで融通し合うことから，物理台数がそもそも不足した場合，仮想化したサーバ１台に割り当てるリソースも不足することとなる。そのため，物理台数の不足は，情報システムの安定した稼働に対して直接的に影響を与える。また，仮想化されたサーバが必要とするリソースは各々異なることから，仮想化したサーバをどの物理サーバに配置していくかについても検討が必要となる。これらを解決するための手法として，サイジング技術を用いることができる。

2.3.2 既存サーバから仮想サーバへの移行

サイジングを実施した後，既存サーバから仮想サーバへいかに移行するかも課題となる。情報システムを仮想サーバ上に新規に再構築するという対応もあるが，新たなサーバ構築には実構築作業など，長時間の作業を要することとなる。そのため，この解決としては，P2V技術を用いて短縮することができる。P2Vは，既存サーバの情報システムを，そのまま仮想サーバ上に移動させる技術であり，IPアドレスの見直し程度でシステムの移行を行うことができる。

2.3.3 データセンターへの移設におけるリスク管理

移設時に問題が生じた場合であってもシステムが適切に守られるように，移設に先立ったリスク分析が重要となる。リスク対象は，データ漏洩(ろうえい)，データ紛失等のセキュリティ以外に，情報システムの再稼働が予定時間内で終了するかなどの可用性の担保も含まれる。仮に移設中の機器に破損が生じた際，リスク対策を行っていない場合は，情報システムの再稼働に影響を与えることとなる。この解決策としては，移設計画でリスク管理を組み入れ，各作業に対し適切に分析を行うなどの対応を検討する必要がある。

3. 事例紹介

この章では，災害対策として情報システムをデータセンターへ移設した事例について示す。これは，サーバ仮想化技術を用いてサーバ台数の削減を実施し，その仮想化したサーバをハウジングサービスでMINDデータセンターへ移設した例である。

3.1 某社システムのデータセンターへの移設(ハウジング)

某社では，2011年の震災を受け，オフィス内のサーバ室に設置していた情報システムのほとんどをデータセンターへ移設した。オフィスビルの被害はほとんどなく，広域ネットワークの被害も同様にほとんどなかった。しかし，某社所在地が計画停電の地区に含まれており，その対応として情報システム運用者の負荷が増加したことが課題となった。運用者の通常業務に支障をきたすおそれが高かったことから，計画停電対策，並びに，今後同様の災害が生じた際のリスク軽減として，データセンターへの移設が実施された。

3.2 移設課題への対応と結果

某社が実際に行った移設における課題への取組みは次のとおりである。

⑴ サーバ集約台数の見積り

２週間程度移設対象の実稼働状況についてサイジングツールを用いて収集し，サーバの利用状況を分析した。これによって，少なくとも50台のサーバを３台に集約可能であることを算出し，最終的には70台のサーバを５台に集約するに至った。

⑵ 既存サーバから仮想サーバへの移行

仮想サーバへの移行にはP2Vを利用した。事前に検証環境でシステムの仮想サーバへの移行を実施し，P2V後であっても情報システムの稼働に問題がないことを検証した。⑴でのサイジングによって性能に対する検証がなされていることから，P2V後の検証では機能試験を中心に行い，性能などの非機能の試験については，本番稼働前に１週間程度，仮想サーバ移行後の情報システムを実環境として用い検証した。

⑶ データセンターへの移設におけるリスク管理

リスク分析では，プロジェクトで定めた各移設ステップに対し，実作業のレベルまで工程を分解し手順化を実施した。その手順で，移設後にサーバが起動しなかった際の代替手段の確立や，輸送時による盗難対策等のリスクが存在しないか，仮に問題が生じた場合であっても復旧が可能かを検討した。

3.3 移設における効果

これらの作業の結果，大きな問題もなくデータセンターへの情報システムの移設が完了した。なお，移設で，某社ではオフィス内のサーバ室の見直しも実施し，空調を含め某社で29kWの利用電力の削減が実現された(**図１**)。

さらに移設の効果としては，災害発生時における作業負荷の低減，グリーンIT促進などが考えられ，また，データセンターを利用する問題として挙げられる全体の運用コストについても，オフィス内サーバ室の空調，UPSといった設備等の見直しによって移設以前と同等に抑えることができた。

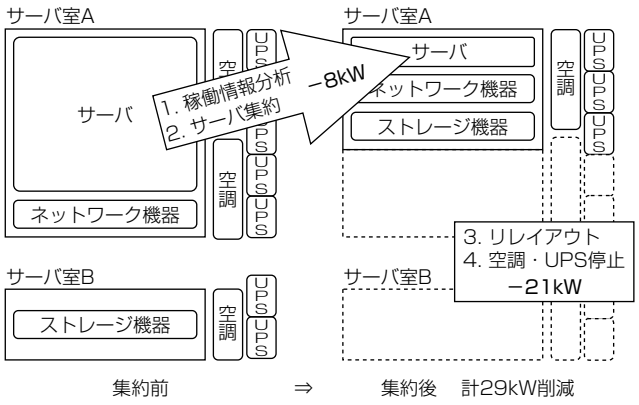


図1．サーバ集約による情報システムの変化と利用電力の削減

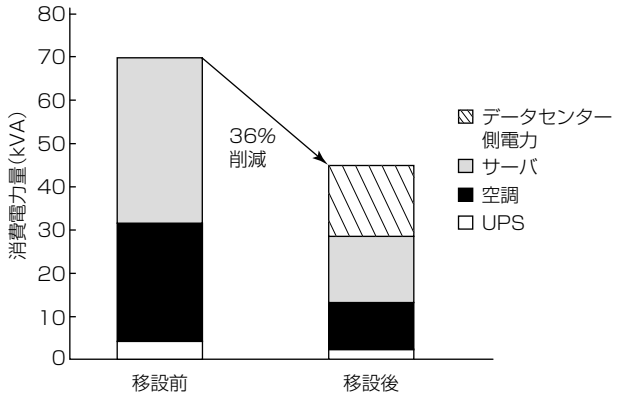


図2．移設前後のデータセンター含めた全体消費電力量の変化

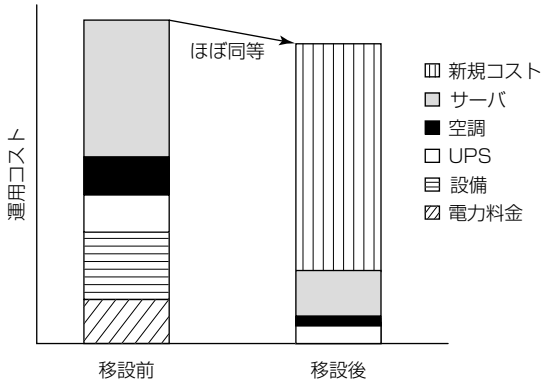


図3．移設前後の全体運用コストの変化

災害発生時における作業負荷の低減では，計画停電に対する作業担当者の負担軽減が図れ，また，緊急時に備え自家発電装置を設置する必要もなくなった。

某社では，データセンターに情報システムを移設する前は，計画停電に備え情報システムの停止・再稼働作業を4人体制で行うことを検討していた。この作業は，1回の停電について3時間を要し，計画停電が毎日行われた場合計1.6人/月の作業増となることから，大きな負担として問題となっていた。仮に自家発電装置導入で対応したとしても，装置のレンタル費，及び燃料費（1回の停電について3時間稼働させた場合）に月約80万円の出費となる。

グリーンITの促進では，移設によってデータセンター側で増えた消費電力を含めても，全体でおよそ36%の削減を実現した（**図2**）。CO_2で換算した場合，年間で100t以上の排出量削減となる。

全体運用コストでは，データセンター利用料として新規にコストが生じるものの，移設に伴い電力や機器，賃貸等の費用削減が期待されることから，全体としては従来と同等以下に抑えられる見通しとなった（**図3**）。

費用削減は，データセンター移設による自社サーバ室運用費の削減と，仮想化によるサーバ集約の機器維持費の削減に分けられる。自社サーバ室運用費の削減は，消費電力削減による電力料金削減，自社サーバ室のリレイアウトによる空調機とUPSの設備維持費，賃貸費用の削減からなる。サーバ集約による機器維持費の削減は，サーバのリース費用削減とデータセンターでの利用ラック数削減による利用料削減からなる。

4. むすび

3章の事例はMINDと某社協力の下で行われており，実施したサイジング，P2V，リスク管理等のノウハウについてはMIND VPOでも活用されており，データセンター利用の敷居を下げている。

今後，企業がビジネスを維持・拡大を図るうえでデータセンターの位置付けは非常に重要なものになることに疑いの余地はなく，MINDでは今後も魅力あるデータセンターのサービス開発・提供に取り組み，安心して利用できるICTのインフラサービスを提供し続けていく。

参考文献

(1) ITアウトソーシング市場展望 2012年度版，㈱ミック経済研究所（2012）
(2) 内閣官房情報セキュリティセンター：東日本大震災における政府機関の情報システムに対する被害状況調査及び分析（最終報告書）（2012）
http://www.nisc.go.jp/inquiry/pdf/shinsai_report.pdf
(3) 日本データセンター協会：東日本大震災を踏まえたデータセンター ファシリティ スタンダードの検証と見直し（2012）
http://www.jdcc.or.jp/pdf/20120315JDCC_facility_standard_digest.pdf
(4) NTTコミュニケーションズ㈱：NTTコミュニケーションズにおける東日本大震災の影響と対応（2011）
https://www.ntt.com/b-advance/feature/201109/index.html

特集論文

IT−BCP対策ソリューション

土井丈志*

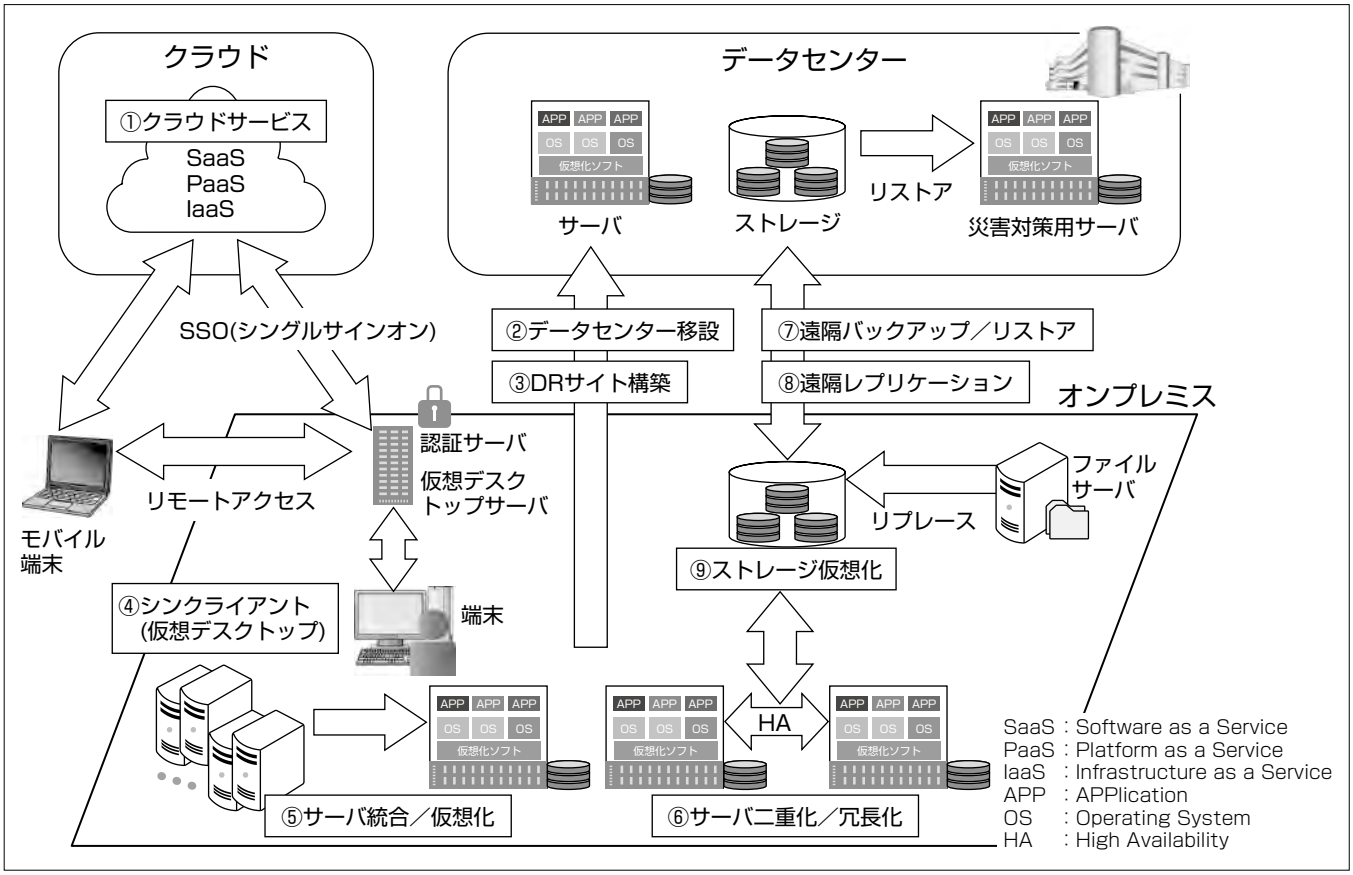
IT−BCP Recovery Solution

Takeshi Doi

要　旨

東日本大震災以降，各企業では災害対策の必要性が認識され，事業継続計画(Business Continuity Plan：BCP)の策定や改善が進められている。情報システムは，企業活動を支える重要な役割を担っているため，情報システムの停止やデータ消失は事業継続に大きな影響を与えることになる。IT−BCPとは災害など予期せぬ事象が発生した場合でも情報システムを継続し，早期復旧を可能とするための行動計画や準備体制のことを指している。情報システムを停止させないための事前対策としてはシステムの二重化，データセンター内へのシステム設備の移設，システムのクラウドサービスへの移行等の予防的措置を講じておくことが有効である。また，計画停電や交通機関の停止等による間接的被害への対応など多くの課題に対しての検討，対策が必要である。

多岐にわたるIT−BCPで最優先で準備・実施しておくべき対策は，情報システムが停止した時の早期復旧，再開を目的とした災害復旧(Disaster Recovery：DR)対策である。㈱三菱電機ビジネスシステム(MB)では，最重要となるデータの消失を回避するためのバックアップデータの遠隔地保管や，早期復旧を目的としたDRサイト構築による2拠点化等の対策ソリューションを中心として，仮想化を始めとする効果的な技術を活用しながら，顧客のニーズにこたえられるIT−BCP対策ソリューションの提供に取り組んでいる。



仮想化とデータセンター活用による情報システムのIT−BCP対策

①クラウドサービスや②データセンターへの移設，③DRサイト構築で情報システムの停止を回避する事前対策を行う。④デスクトップ仮想化による在宅勤務環境の構築，仮想化による⑤サーバ統合，⑨ストレージ仮想化によるコスト削減，⑥サーバ二重化による可用性向上を実現する。システムが停止した時の復旧を目的とした災害対策としてDRサイト内のストレージに⑦遠隔バックアップや⑧レプリケーションによるデータ転送を行い，災害対策用サーバでシステムの早期復旧・再開を実現する。

*㈱三菱電機ビジネスシステム

1. まえがき

東日本大震災後，企業のIT-BCP対策に対する取組みに変化が起きている。理由としてはBCPに対する意識が高まったことや，技術の進化による対策ソリューションの多様化等が挙げられる。特に震災後は予防的措置だけで災害全てに対応することは困難という認識からシステムが停止した場合のDR対策への取組みが注目されている。

本稿では多岐にわたるIT-BCP対策の中からDR対策に焦点を置き，早期復旧するためのDR対策ソリューションの特長やDR対策に効果的な技術について述べ，最後に導入事例について述べる。

2. IT-BCP対策

IT-BCP対策は災害などが発生した場合でも情報システムを停止させないための事前対策と，停止した時の復旧・再開のためのDR対策に大別される。

2.1 事前対策

事前対策には情報システム設備のデータセンターへの移設やシステムのクラウドサービスへの移行等がある。また，震災後に発生した計画停電や交通機関の停止による間接的被害に対応するためのリモートアクセスやデスクトップ仮想化等の在宅勤務環境の整備も事前対策の一つである。

2.2 DR対策

DR対策でのデータ復旧方法には技術の進歩もあり多くの方法があるが，大きく分けると次の3つに分類できる。

⑴ バックアップ媒体の輸送による遠隔地保管
⑵ レプリケーションによる遠隔地保管
⑶ DRサイト構築によるサイト間フェールオーバー

⑴のバックアップ媒体の遠隔地保管はDR対策では一般的な方法でデータ消失を防ぐためには有効な対策であるが，この方法は復旧に多くの時間が必要となり早期復旧を要する場合には不向きである。早期復旧を実現するには⑵のレプリケーション技術による遠隔地保管や⑶のDRサイトを構築してサイト間でシステムを切り替えるといった対策が必要である。

DR対策は復旧すべき情報システムごとに災害発生からいつまでにシステムを再稼働すべきかの目標復旧時間（Recovery Time Objective：RTO）や，災害からさかのぼっていつの時点のデータに復旧するかの目標復旧時点（Recovery Point Objective：RPO）を定める必要がある（**図1**）。

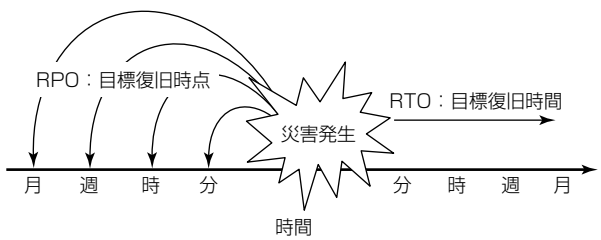


図1．DR対策におけるRPOとRTOの関係

3. 早期復旧を目的としたDR対策モデル

災害時の早期復旧を目的としたDR対策は，レプリケーション技術を使って遠隔地にデータを保護する方法と，これに加えてDRサイトを構築しシステムを切り替えて再開する方法がある。この2つの方法を組み合わせたDR対策ソリューションを復旧時間目標別に3つにモデル化（**表1**）して，それぞれの機能や特長を述べる。

3.1 対策モデル1：バックアップレプリケーション

各サーバのバックアップをバックアップストレージに集約し，ネットワーク経由でバックアップデータをDRサイト側のストレージにレプリケーションする（**図2**）。

災害発生時にはOSやアプリケーション等の環境構築済みの代替機にバックアップデータをリストアする。バックアップストレージは，レプリケーションソフトウェアをインストールしたストレージや，レプリケーション機能を持った専用ストレージを使用する。この方法の特長はメインサイト側サーバのバックアップの運用を変えずに追加する形で対策を施すことが可能な点である。

3.2 対策モデル2：ソフトウェアレプリケーション

メインサイト側サーバとDRサイト側サーバにレプリケーションソフトウェアをインストールしてサーバ間でレプリケーションを行う。メインサイト側サーバで更新された業務データをネットワーク経由でDRサイト側サーバのディスクへ直接レプリケーションする（**図3**）。災害発生時にはDRサイト側サーバでシステムの切り替えを実施する。バックアップからのリストアが必要ないため比較的短時間でシステムを再開することが可能である。このモデルの特長はサーバ1台だけの災害対策にも採用できる点である。ただし，レプリケーション対象は業務データだけのため，

表1．早期復旧を目的としたDR対策モデル

対策モデル	モデル1	モデル2	モデル3
対策ソリューション	バックアップレプリケーション	ソフトウェアレプリケーション	ストレージ統合・レプリケーション
RTO	数日	1日	数時間
RPO	1日	数分～数時間	数分～数時間
保護対象データ	バックアップデータ	本番データ	本番データ・OS・アプリケーション
導入コスト	低	中	高

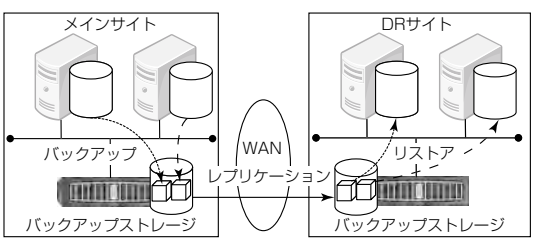


図2．バックアップレプリケーション

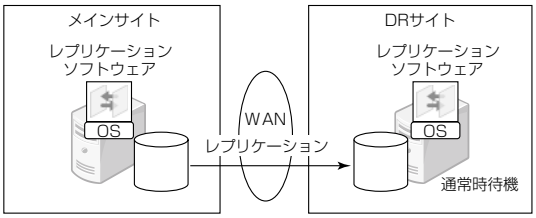
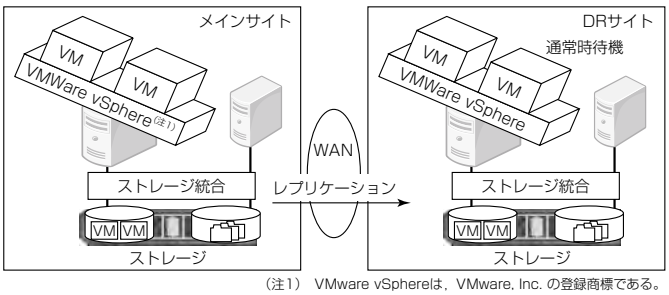


図3．ソフトウェアレプリケーション



（注1） VMware vSphereは，VMware, Inc. の登録商標である。

図4．ストレージ統合・レプリケーション

メインサイト側サーバでOSやアプリケーション等の更新を行った場合にはDRサイト側サーバも手動更新をする必要がある。

3.3 対策モデル3：ストレージ統合・レプリケーション

レプリケーション機能を持ったストレージ間でレプリケーションを行う。メインサイト側で複数サーバのストレージ統合環境を構築し，ストレージには各サーバのOSやアプリケーションを含めたデータが保管される。メインサイト側ストレージ内で更新されたデータをDRサイト側ストレージへレプリケーションする（**図4**）。

災害発生時には，DRサイト側の各サーバでシステム切り替えを実施する。このモデルの特長は，ストレージ統合された複数サーバのOSやアプリケーションを含めた更新データがDRサイト側ストレージに同期されるため，短時間で複数サーバのシステムの再開が可能な点である。また，複数サーバを同一の方法でレプリケーションするため運用の統一化を図ることができる。ただし，複数サーバのデータを全てストレージに格納するため高信頼のストレージが必要となり導入コストは割高となる。

4. DR対策に効果的な技術

DR対策で必要となるバックアップやWAN（Wide Area Network）でのデータ転送を実現するために効果的である技術や，DRシステム構築時にコスト削減効果を得ることができる仮想化技術について述べる。

4.1 レプリケーション

レプリケーションとは，本番サーバのデータを待機サーバやストレージに複製してデータを同期させる技術である。レプリケーションにはリアルタイムに同期させる方式と非同期方式，一定間隔で差分データをまとめて転送する方式がある。DR対策の基本である遠隔地へのデータ複製には欠かせない技術である。レプリケーション環境は，システム規模，対象データ量，コスト等を勘案して適切なレプリケーションソフトウェアを選定し，必要なストレージを準備し構築する。

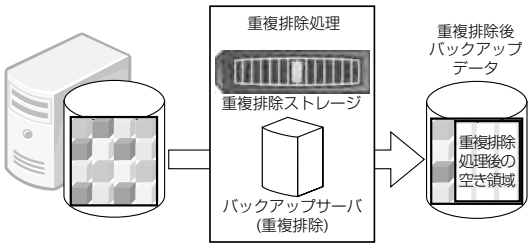


図5．重複排除

4.2 重複排除

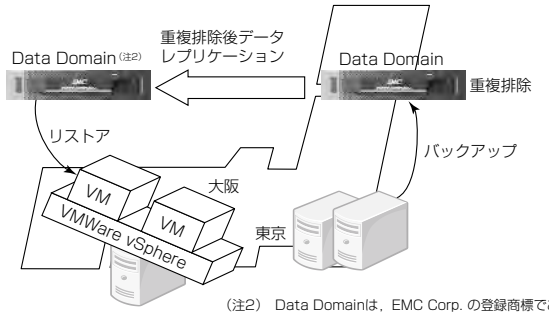
重複排除とは，データの中で重複している部分をあらかじめ排除し，実際にディスクに格納するデータ量を小さくする技術である（**図5**）。重複排除に対応したバックアップソフトウェアを利用することによってバックアップディスクの使用量削減，バックアップ時間の短縮といったメリットが期待できる。ネットワークで遠隔地にデータを送る場合に，事前に重複排除処理を行って送るべきデータ量を縮小することで回線の帯域幅を抑えることが可能である。重複排除はDR対策では非常に有効な技術であり今後も進化していく技術と考えられる。

4.3 イメージバックアップ

イメージバックアップとは，ディスクのビット列をそのままバックアップする方式で，ディスクをまるごとイメージでバックアップする。リストアは専用のリカバリーCDでサーバを起動後，バックアップイメージ全てをディスクにリストアする。従来のデータバックアップからの復旧方法に比べて圧倒的に速く手順もシンプルなため，復旧時間の短縮を目的とするバックアップとして有効である。

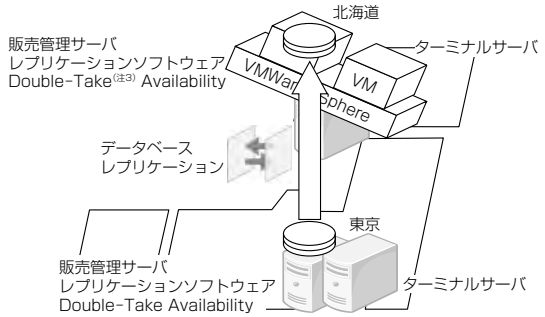
4.4 仮想化技術

DR対策に有効な仮想化技術としてサーバ仮想化が挙げられる。サーバ仮想化によって，1台の物理サーバ上に複数の仮想サーバを稼働させることができる。DRサイトの構築には基本的に本番サーバと同数の待機サーバを用意する必要があるが，待機サーバを仮想化で構築することによって物理サーバ数を減らすことができ，ハードウェア費用や省スペース化といったコスト削減が可能である。さらに，仮想化はシステムのハードウェア依存性を排除することが可能なため本番サーバと同等の機器でなくても待機サーバ環境を構築することが可能である。また，仮想化の特長であるカプセル化によってハードウェア構成，OS，アプリケーション，データがファイルとしてディスクに格納される。仮想サーバ全体がファイル化されるため，そのファイルをバックアップやレプリケーションを活用し遠隔地へ保管すれば仮想サーバ全体の保護が可能となる。



(注2) Data Domainは，EMC Corp. の登録商標である。

図6．バックアップデータレプリケーション



(注3) Double-Takeは，Vision Solution, Inc. の登録商標である。

図7．ソフトウェアレプリケーションによる2拠点化

5. 導 入 事 例

3章のDR対策モデルをベースにしたIT-BCP対策ソリューション導入の2つの事例を述べる。

5.1 バックアップレプリケーションDR対策事例

5.1.1 概　　要

複数サーバのデータ消失回避と低コストが要件であったため，**3．1節**の対策モデル1：バックアップレプリケーションを採用し，かつ待機サーバを仮想化で1台に集約している事例である。メインサイトは東京にあり大阪にDRサイトを新規に構築し，バックアップ保管に重複排除バックアップストレージData Domainを採用し両拠点に設置した(**図6**)。東京側のストレージで重複排除処理によってバックアップデータの重複している部分をあらかじめ除去しバックアップデータサイズを縮小し，ストレージのレプリケーション機能で大阪側のサイトへバックアップデータの複製を実施する。

災害発生時は，大阪のData Domainから待機サーバへリストアを行い業務再開する。

5.1.2 導 入 効 果

メインサイトの東京側で重複排除によるバックアップデータ量の削減を行うことによってバックアップ時間の短縮とネットワーク負荷低減を実現した。また，待機サーバを仮想化で1台に集約することによってコスト削減が図られている。

5.2 ソフトウェアレプリケーションDR対策事例

5.2.1 概　　要

販売管理システムの1日以内の業務再開と可能な限り災害発生前の最新データへの復旧が要件であったため，**3．2節**の対策モデル2：ソフトウェアレプリケーションを採用し，かつ待機サーバを仮想化で1台に集約している事例である。メインサイトは東京にあり北海道にDRサイトを新規に構築し，販売管理サーバのデータベースのデータをレプリケーションソフトウェアDouble-Take Availabilityで北海道側の待機サーバへ非同期レプリケーションを行う(**図7**)。災害発生時は北海道側の待機サーバに手動で切り替えを行い業務を再開する。

5.2.2 導 入 効 果

データベースの更新データを即時に北海道側待機サーバへレプリケーションを行うため，災害直前のデータに復旧可能なこととリストア作業が不要なため短時間で業務の再開が可能である。また，待機サーバを仮想化で1台に集約することによってコスト削減が図られている。

6. む　す　び

現在の企業活動には情報システムは不可欠であり，不測の事態による情報システムの停止は企業活動に大きな影響を与える。IT-BCP対策は一度実施すれば終わりではなく，システムの更新や技術の変化によって対策の見直しや改善を継続的に行っていく必要がある。

情報システムを停止させないための予防対策や災害発生時の事前対策は保険的要素が多く，顧客は必要最低限の投資コストで安心を得られる対策ソリューションを望んでいる。

今後も時代に応じた技術や製品を取り入れながら，顧客ニーズに対応できるIT-BCP対策ソリューションの提供に取り組んでいく所存である。

参 考 文 献

(1) 巻頭特集，3.11の教訓を生かした災害に強いBCP策定のポイントとITソリューションとは，MELTOPIA，No.175（2012）
http://www.mitsubishielectric.co.jp/meltopia/backnumber/2012/04/case01.html
(2) (独)情報処理推進機構：事業継続のための高回復力システム基盤導入ガイド(概要編)，SEC Report（2012）
http://www.ipa.go.jp/sec/reports/20120508.html
(3) (独)情報処理推進機構：情報システム基盤の復旧に関する対策の調査報告書（2012）
http://www.ipa.go.jp/sec/reports/20120725.html
(4) 経済産業省：ITサービス継続ガイドライン改訂版（2012）
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2011_IoformationSecurityServiceManagementGuidelineKaiteiban.pdf

特集論文

ワークスタイル変革を支援するコミュニケーション＆コラボレーションサービスへの取組み

手束裕司*

Communication ＆ Collaboration Services for Work Style Revolution

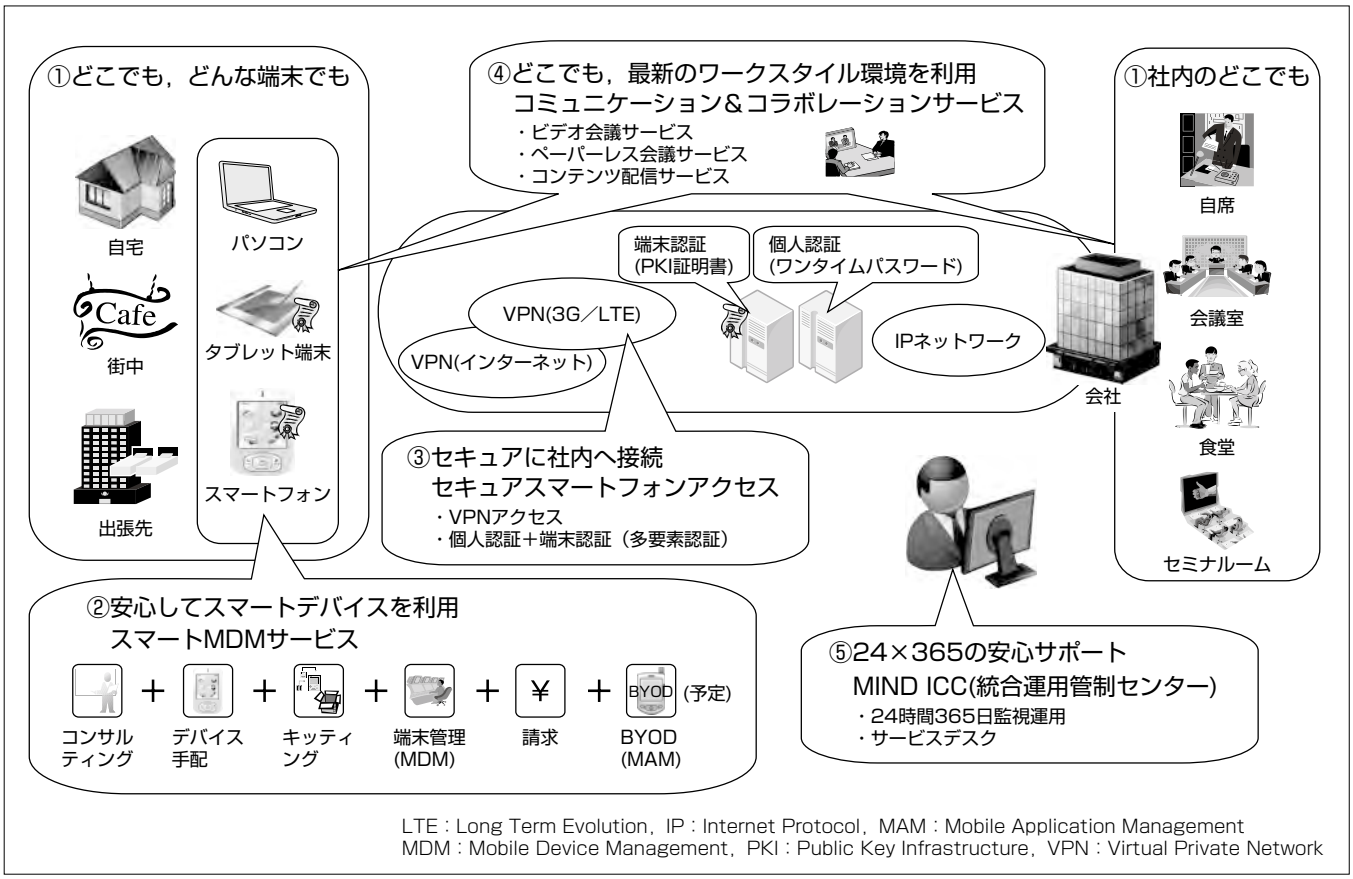
Yuji Tetsuka

要　旨

スマートフォンやタブレット端末の利用が世界中で急速に広まっている。世界市場では2012年携帯電話新規出荷台数のうち約4割は既にスマートフォンになっており(1)，日本市場では更に加速して，新規出荷台数の約7割がスマートフォンになっている状況である(2)。

このような市場におけるスマートデバイスの普及と並行して，ワークライフバランスの実践や従業員の業務効率や生産性の向上を目的とした在宅勤務やサテライトオフィス等，企業における従業員の働き方について変化が起こっている。さらに，2011年の東日本大震災以降，事業継続性(Business Continuity Planning：BCP)の観点から，社外でも社内と同様の環境で業務を行えるIT(Information Technology)環境を求める声が高まっており，企業におけるワークスタイル変革が注目されている。

三菱電機情報ネットワーク㈱(MIND)では，企業のワークスタイル変革を支援するソリューションとして，スマートデバイスを安全に利用するための“スマートMDMサービス”，業務効率の向上を目的としたコミュニケーション＆コラボレーションサービスとして，“スマートデバイス対応ビデオ会議サービス”“ペーパーレス会議サービス”“コンテンツ配信サービス”を提供している。そして，現在，個人所有のデバイスを業務で利用するBYOD(Bring Your Own Device)の提供へ向けたサービス開発に取り組んでいる。



LTE：Long Term Evolution，IP：Internet Protocol，MAM：Mobile Application Management
MDM：Mobile Device Management，PKI：Public Key Infrastructure，VPN：Virtual Private Network

スマートデバイスの管理とコミュニケーション＆コラボレーションのトータルサービス

どこからでも，どんな端末でも，セキュリティを確保して社内へ接続し，ビデオ会議，ペーパーレス会議，コンテンツ配信等の最新のワークスタイル環境を利用することによって，業務効率の向上を実現する。さらに，MINDの運用管制センターであるICC(Integrated Control Center)によって24時間365日のサポートを提供する。

*三菱電機情報ネットワーク㈱

1. まえがき

スマートフォンやタブレット端末等，スマートデバイスの普及が急速に進んでいる。世界市場では2014年にはスマートフォンの出荷台数が従来の携帯電話の出荷数を超え，タブレット端末については，2015年にノートパソコンの出荷台数を上回ると予測されている(1)。さらに，コンシュマライゼーションの流れを受けスマートデバイスを企業の業務で利用しようとする動きが急速に広まっている。

また，ワークライフバランスや事業継続性の観点から，企業における従業員の働き方に変革が起こっており，社外でも社内と同様の環境で業務を遂行できるIT環境の整備が求められている。

スマートデバイスは，ノートパソコンに比べ操作性が良くかつ携帯電話に比べて多くのアプリケーションを利用できることから，このようなワークスタイルの変革に対応するためのツールとしての利用が注目されている。

本稿では，急速に導入が進んでいるスマートデバイスの業務利用における課題と解決策，ワークスタイル変革を支援するスマートデバイスを活用したコミュニケーション＆コラボレーションサービスについて述べる。また，次のステップとして注目を浴びている個人所有のデバイスを業務で利用するBYODの動向と実現方式についても述べる。

2. スマートデバイスの業務利用

2.1 スマートデバイスの業務利用の動向

企業がスマートデバイスを業務で利用しようとする動きは急速に広まっており，現在，日本国内の法人契約の携帯電話加入者数におけるスマートフォンの割合は1割強であるが，2016年には法人契約のスマートフォンが5割を超えると予測されている(3)。特に携帯通信事業者から新規に発売される携帯電話はスマートフォンが主流となっており，従来の携帯電話を入手するにも選択肢が少なくなってきていることも企業におけるスマートフォン導入の促進要因となっている。

2.2 スマートデバイスの業務利用における課題

スマートデバイスは携帯電話の延長線上で開発されたものであるが，機能としてはパソコンの要素を併せ持っている。そのため，スマートデバイスを業務で利用する場合には次の課題を解決する必要がある。

2.2.1 情報及びアプリケーションの適切な管理

スマートデバイスは従来の携帯電話と比べ，多くの情報やアプリケーションをデバイス内部に持っている。スマートデバイスでは，それらの情報とアプリケーションを簡易に利用することができるため，利便性が評価され普及しているが，企業で利用する場合には，デバイス内部に持つそれらの情報やアプリケーションを適切に管理する必要がある。

2.2.2 セキュリティ対策

スマートデバイスは常にネットワークに接続されており，一部のスマートデバイスのOS(Operating System)はオープンソースであるため，その脆弱(ぜいじゃく)性をターゲットとしたマルウェアも出現している。また，悪意のあるアプリケーションがアプリケーションストアから提供され容易にダウンロードができるなど，従来の携帯電話では考慮する必要のなかったセキュリティ対策を講じる必要がある。

2.3 スマートデバイスを安全に利用するための対策

スマートデバイスを安全に利用するためには，スマートデバイス利用におけるセキュリティガイドラインの策定とデバイス管理という大きく2つの対策を講じる必要がある。

2.3.1 セキュリティガイドラインの策定

セキュリティガイドラインでは，スマートデバイスを社員に配布するための基本的な考え方(誰が，どのような目的で，どのように利用するか)，スマートデバイスの機能の制限(カメラ，メモリカードの使用制限など)，利用するアプリケーションの制限(ホワイトリスト管理，ブラックリスト管理)，パスワードの管理(有効期限，文字種類･組合せの設定)等，利用方針及び利用基準を決める必要がある。

2.3.2 デバイスの管理

スマートデバイスの管理は次の3つの対策を講じる必要がある。

(1) 紛失・盗難時の情報漏洩(ろうえい)防止対策

スマートデバイスは外出先で利用することが多いため，万一紛失や盗難にあった場合に企業の機密情報や顧客情報が外部に漏れないように対策を講じる必要がある。対策としては，デバイス内部の情報の暗号化に加え，スマートデバイスがセキュリティガイドラインに準拠するようMDMによる管理が必要となる。MDMによって，デバイスで利用できるアプリケーションの制限やカメラなどの機能制限，万一デバイスを紛失した際に遠隔からデバイスをロックしたり，デバイスの設定を初期化し全てのデータを消去(ワイプ)したりすることが可能になる。

(2) ウイルス対策

スマートデバイスを社内のシステムへ接続する際にウイルスなどを持ち込ませないようにするために，それぞれのスマートデバイスのOSに対応したウイルス対策ソフトを導入する(注1)。さらに，ウイルス対策ソフトが常に最新の状態になっているかMDMを利用して管理する。

(3) 不正アクセスの防止と通信の保護

社内への不正アクセスや通信経路の盗聴を防ぐ対策として，VPNを用いて暗号化されたネットワークで接続する。社内ネットワークへの接続の際には個人認証と電子証明書による端末認証等の複合的な認証を実施する。

(注1) 一部ウイルス対策ソフトを提供しないOSがある。

2.4　スマートデバイスを安全に利用するためのソリューション

MINDでは，スマートデバイスを安全に利用するために“スマートMDMサービス”を提供している。このサービスを利用することによって，セキュリティガイドライン策定の支援から，スマートデバイスの手配，スマートデバイスへのセキュリティポリシーの設定，MDMによる24時間365日の遠隔運用管理，利用状況のレポート，請求までをワンストップで行い，顧客のスマートデバイスのライフサイクルを適切に管理することができる（**図1**）。さらに，MINDでは，“セキュアスマートフォンアクセスサービス”として，外出先から社内へのVPN接続サービス，個人認証及び端末認証の認証サービスを提供している。

3. ワークスタイル変革に合わせたコミュニケーション＆コラボレーションサービス

3.1　ワークスタイル変革でのスマートデバイスの有用性

ワークスタイル変革にはいろいろな考え方があるが，この章では，“時間と場所に制限されない働き方”と定義する。具体的には在宅勤務など社内外を区別せずに業務を行い，かつ社内でも自席を意識せずに社内のどこにいても業務を行える働き方である。

ワークスタイル変革を実践する上で重要となるのは，社外や自席以外で業務を行う際に業務効率や生産性を低下させないことであり，自席と同様の使い勝手で不自由なく業務を遂行できるIT環境を提供することである。そのようなIT環境を実現する上で，スマートデバイスはノートパソコンに比べ，重量が軽く，起動が速い，携帯電話と比べ画面が大きく，業務アプリケーションの利用が可能である等，外出先や自席以外で利用するには利便性が高く適したツールである。また，スマートデバイスは，メール，スケジュール，業務システム等，社内リソースの利用に加えて，営業活動時の迅速な製品カタログの閲覧やプレゼンテーションの実施，外出先でのビデオ会議への迅速な参加等，これまでのパソコンでは準備に時間がかかった業務を短時間で実現することができ，商談の機会損失の削減，業務効率の向上を図ることが可能である。

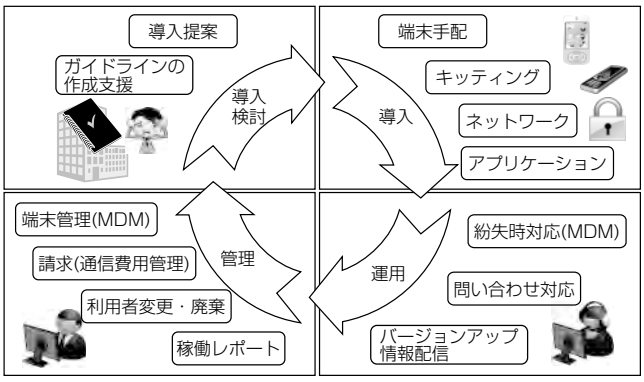


図1．スマートMDMサービス

3.2　スマートデバイスを活用したコミュニケーション＆コラボレーションサービス

MINDではワークスタイル変革を支援するコミュニケーション＆コラボレーションサービスとして，スマートデバイスを活用したビデオ会議サービス，ペーパーレス会議サービス，コンテンツ配信サービスを提供している。さらに，現在，インスタントメッセージ，プレゼンス，メール，電話，オンライン会議が1つのインタフェースで利用できるUC（Unified Communication）サービスの開発を進めている。

3.2.1　スマートデバイス対応ビデオ会議サービス

従来のビデオ会議システムは，会議室に据置きのビデオ会議システム同士で会議を行うか，パソコンにビデオ会議用のアプリケーションをインストールし利用するのが一般的であったが，このサービスではタブレット端末を利用して，出張先や自宅からでも簡単にビデオ会議に参加できる環境を提供している。これによって，いつでも，どこからでも迅速に会議に参加でき，業務効率の向上を図ることができる（**図2**）。

3.2.2　ペーパーレス会議サービス

会議で配布する資料をPDF（Portable Document File）のファイル形式であらかじめサーバへ保存しておき，会議では出席者がタブレット端末を利用して該当のファイルを閲覧し会議に参加できるサービスである。資料にはコメントや下線等の書き込みが可能であり，出席者各自が書き込んだ資料はサーバにそれぞれ保管され，会議終了後に自席のパソコンから閲覧することが可能である（**図3**）。紙の大幅な削減につながり，グリーンITにも貢献する。

3.2.3　コンテンツ配信サービス

配信する動画や静止画をコンテンツサーバに保存しておき，タブレット端末などのスマートデバイスから閲覧でき

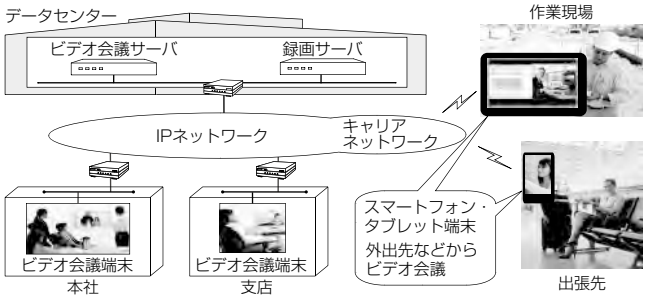


図2．スマートデバイス対応ビデオ会議サービス

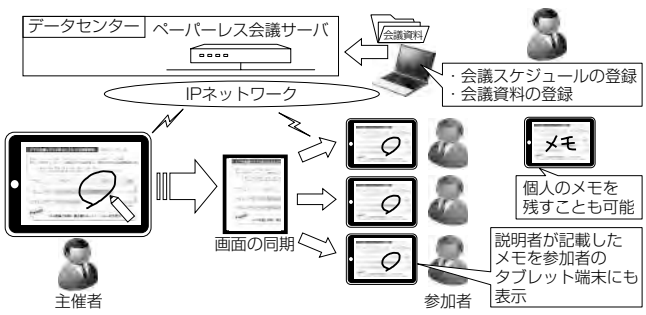


図3．ペーパーレス会議サービス

るサービスである。社員のトレーニング，経営幹部の社内メッセージの動画配信，営業活動における製品カタログ配布等いろいろな場面で利用が可能である。オンラインでの利用に加え，あらかじめダウンロードすることによってオフラインで利用することもできる(**図4**)。

4. BYODの動向と実現方式

4.1 BYODの概要

BYODとは，個人所有のデバイス(パソコン，スマートフォン，タブレット端末等)を企業内に持ち込み業務用として利用することである。BYODはコンシュマライゼーションの流れを大きく反映したものであり，会社が支給したデバイスでは性能や使い勝手等に満足できないため，個人所有のデバイスを業務用に利用したいという従業員からの要望と，企業側はデバイスを支給し定期的に買い換えるコストを削減できるという利点から欧米を中心に広まっている。日本でもBYODを導入している企業の事例が出始めているが，企業文化の違いやセキュリティ，プライバシーへの懸念もあり導入は欧米の企業に比べまだ慎重であると言える。ただし，企業の情報システム部門が認めていないデバイスを無断で社内に持ち込み利用する事象が現在問題視されており，このような事象を“シャドーIT”と呼んでいる。シャドーITの存在は企業のセキュリティ管理上，極めて重要な課題であり，BYOD対策の導入がその解決策の一つになる。

4.2 BYODを実現するための技術

BYODを実現するには，セキュリティポリシーの設定などMDMによるスマートデバイス自体の管理に加え，デバイスには個人のプライベートな情報と企業の情報が混在するため，企業はプライベートな情報には関与せず企業情報だけを管理する情報管理の仕組みが必要になる。

この仕組みを実現するための技術として現在注目されているのがMAMである。MDMがデバイスのセキュリティや資産管理を主体に実施するのに対し，MAMはデバイスにインストールされているアプリケーションの保護や管理を実現する技術である。MAMの実現方式としては，次の2つの方式がある。

4.2.1 サンドボックス／コンテナ方式

デバイスの内部を業務領域とプライベートな個人領域に分離し，相互の通信を遮断するとともに，万一デバイスを紛失した際にも業務領域だけを一括で削除できる方式である。同方式は自社開発のアプリケーションを業務領域に入れる際にSDK(Software Development Kit)による開発が伴うなどの導入の課題もあるが，業務領域と個人領域をそれぞれ一括で管理できるなど運用管理が容易である。

4.2.2 アプリケーションラッピング方式

個々の業務用アプリケーションをラッピングという技術で保護し，外部からの影響を受けないようにする方式である。アプリケーションを起動する際にパスワードを要求したり自動的にVPNを起動したりセキュリティ機能を付加することも可能である。同方式は自社開発のアプリケーションであっても容易にラッピングすることができ，アプリケーションごとにセキュリティ設定が可能であるなど運用管理の柔軟性が高い。

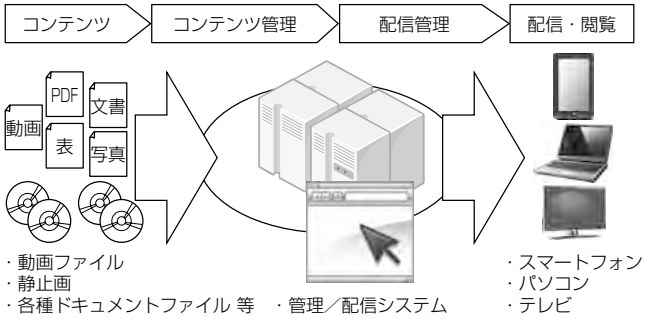


図4．コンテンツ配信サービス

現在，このサンドボックス／コンテナ方式とアプリケーションラッピング方式の技術を融合させ，セキュリティの強化と運用管理の容易性を併せ持った製品も市場に出てきている。

MINDでは，現在，BYODへの対応として，ニーズ調査，技術調査，製品調査，製品検証を行いサービスの提供へ向け開発を進めている。

5. むすび

今後，ワークスタイルの変革が進むとともに，社内外を問わずに業務を円滑に遂行する環境が求められ，スマートデバイスはワークスタイル変革を実現するための必須のツールとなる。さらに，これまでパソコンでは実現できなかった迅速性や機動性を求められる業務に対して，操作性に優れるスマートデバイスの活用が期待される。

ワークスタイル変革でスマートデバイスを活用するには，スマートデバイスを安全に利用する仕組みと，業務効率を向上させるためのコミュニケーション＆コラボレーション環境が必要である。

MINDでは，スマートデバイスを安全に利用するためのスマートMDMサービス，業務効率を向上させる各種コミュニケーション＆コラボレーションサービスを提供し，今後，さらにBYODやUC等，新たなサービスの開発にも取り組み，顧客のワークスタイル変革を支援していく所存である。

参考文献

(1) ㈱矢野経済研究所 プレスリリース：世界のスマートフォン・タブレットに関する調査結果2012（2012）
(2) IDC Japan プレスリリース：2012年第3四半期 国内携帯電話／スマートフォン市場規模を発表（2012）
(3) IDC Japan プレスリリース：国内ビジネスモビリティ市場予測を発表（2012）

特集論文

仮想環境構築・運用自動化技術

小笠原大治* 堀口真理子*
河野義哉* 金木佑介**
遠藤 司*

Automation Technology for Virtual Machine Construction and Operation Process

Daiji Ogasawara, Yoshiya Kono, Tsukasa Endo, Mariko Horiguchi, Yusuke Kaneki

要 旨

多くの企業でサーバの仮想化が進むにつれ，大量にVM（Virtual Machine）を構築する要求が増えてきている。そこで三菱電機インフォメーションシステムズ㈱（MDIS）は，大量のVMを迅速に構築する“仮想環境構築・運用自動化ソフトウェア”を開発した。

このソフトウェアは，大量のVM生成とOS設定，アプリケーションの導入・設定といった従来人手で行っていた作業を，あらかじめ定義した情報を基に自動化する。

このソフトウェアの主な特長は，次の3つである。

⑴ 大量のサーバの構築自動化

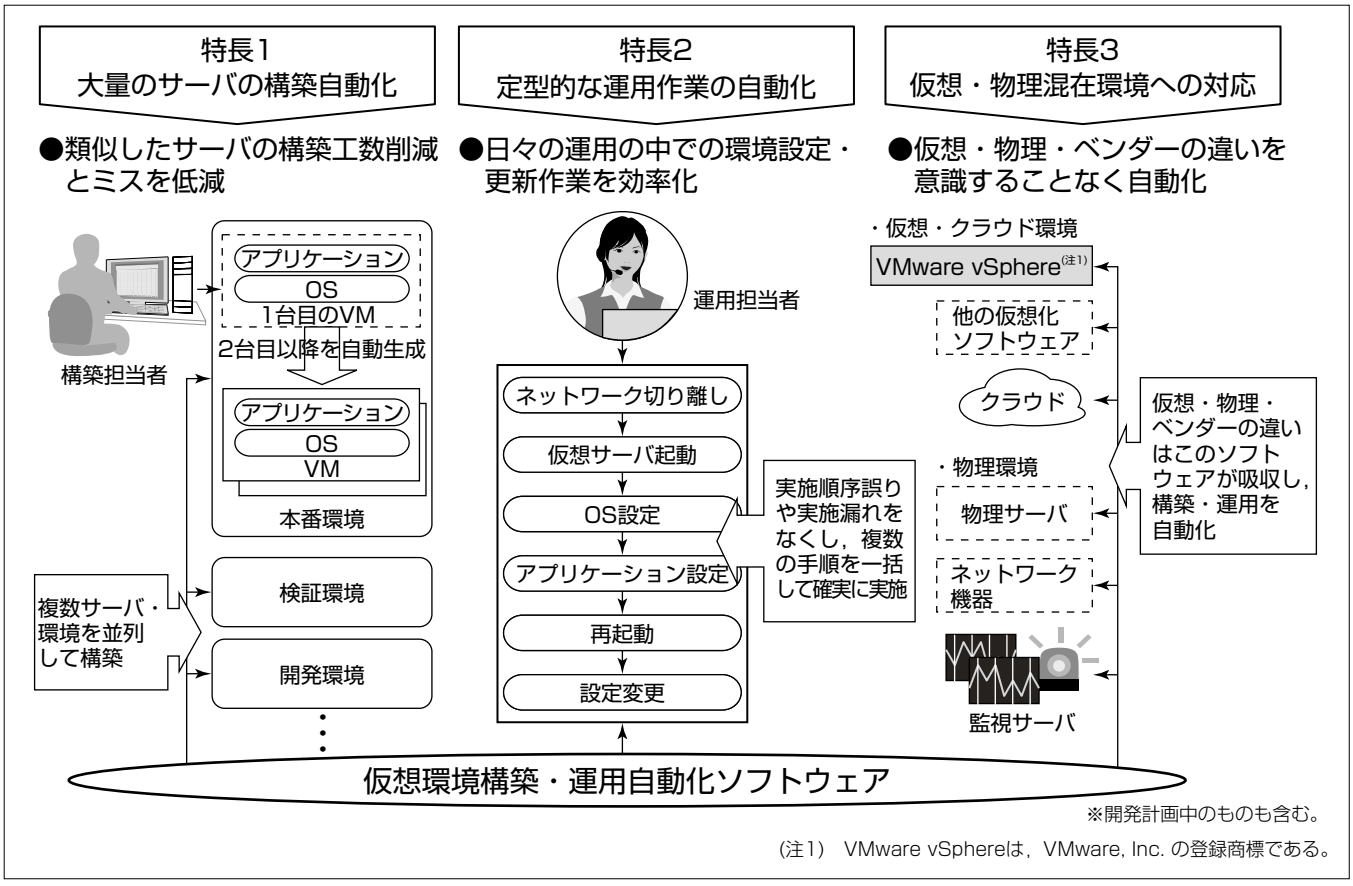
1台目のVMを雛形（ひながた）として2台目以降のVMを自動生成する機能と複数台のサーバを並列に構築する機能によって，類似したサーバを大量に構築する際の工数と所要時間を大幅に削減し，OSとアプリケーションの設定ミスを低減する。

⑵ 定型的な運用作業の自動化

大量のサーバを構築した後の，日々の運用の中でのOS・アプリケーション環境の設定・更新作業を自動化し，運用作業の効率化と手順誤り・漏れをなくす。

⑶ 仮想・物理混在環境への対応

仮想・物理混在環境での構築・運用を自動化する。各々の環境を制御するために各ベンダーが提供しているAPI（Application Programming Interface）の違いをこのソフトウェアで吸収しているため，マルチベンダー環境にも対応できる。



※開発計画中のものも含む。

（注1） VMware vSphereは，VMware, Inc. の登録商標である。

仮想環境構築・運用自動化ソフトウェアの特長

大量のサーバの構築自動化，定型的な運用作業の自動化，仮想・物理混在環境への対応の3つの特長を持つ。アプリケーション導入手順や設定ファイル等のテンプレート情報を，対象サーバに応じた処理情報に整形することで，複数台の対象サーバの環境構築と運用を効率的に行う。なお，このソフトウェアの技術は現在特許出願中である（出願番号：特願2013-30940）。

 *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

多くの企業でサーバの仮想化が進み，構築・運用すべき仮想マシン数が大幅に増えてきている。しかし，その運用管理費用は横ばいのため，数年前と比べ同じ人数(費用)で2倍近い台数のサーバをミスなく構築・運用することが必要になってきた[1]。そこでMDISは，大量のサーバの構築・運用の工数削減とミス低減を狙い，“仮想環境構築・運用自動化ソフトウェア”を開発した。

本稿では，このソフトウェアの主な特長と適用事例・効果について述べる。

2. 仮想環境構築・運用時の課題

2.1 大量サーバ構築時の工数削減とミス低減

システム構築作業では，本番システムだけでなくアプリケーションやシステムの開発環境と検証環境も構築するのが一般的である。さらに，BCP(Business Continuity Planning)用に本番とほぼ同じ構成の災害対策システム(BCP環境)を構築することが増えている。

人手で類似した構成のサーバを多数構築する場合，設定誤りを引き起こしやすい。100台以上のサーバの構築設定を手作業で行うと，IPアドレスを誤って設定してしまうことは，十分起こり得る[2]。

構築作業の自動化を実現すれば，構築作業全体の工数削減とミス低減を狙うことができる。

2.2 運用の効率化と運用容易性の向上

大量にサーバを持っていると，日々の運用の中でのOS・アプリケーション環境の設定・更新作業も増えるため，その効率化が必要である[3]。

例えばインターネットからのアクセスを分散して処理しているWebサーバが10台あり，これらすべての環境設定を実施したい時，1台1台ネットワークから切り離し，手作業で設定を行わなければならない。大量のサーバをインターネット公開しているオフィシャルサイトの運用では，この設定作業を3日に1回実施しているケースもある。

このような定型的な作業を自動化すれば，時間や工数の削減を狙うことができる。

また，運用の中では非定常的な作業も発生する。非定常的な作業は，低頻度ではあるが作業項目が多岐にわたったり，担当者が作業に未習熟であったりするため，対応が容易ではない。

例えば被災時のBCP環境への切替え作業は非定常的な作業である。被災時には緊急性が求められ，環境切替え方法を確認する時間が十分に確保できないことや，担当者が不在の可能性も考えられる。

非定常的な作業だからこそ，即座に判断・行動できる仕組みを用意すれば，運用容易性を高めることができる。

2.3 仮想・物理混在環境への対応

サーバの仮想化が進展している一方で，すべてのシステムを仮想環境へ移行しないケースもある。そのため仮想・物理サーバが混在した環境での運用管理が求められる。また，サーバOSの種類によって，OS・アプリケーション環境を設定するためのベンダー提供コマンド・APIが異なるため，環境ごとに多くの技術知識や経験を習得するなどの対応が必要である。そこで，構築・運用を自動化する際は，仮想・物理の混在及びOSの差異を意識させないことで利用者の利便性を更に高めることができる。

3. 仮想環境構築・運用自動化ソフトウェア

“仮想環境構築・運用自動化ソフトウェア”は，あらかじめ定義した情報を基に，大量のVM生成とOS設定，アプリケーションの導入・設定といった，従来人手で行っていた作業を自動化するソフトウェアである。

このソフトウェアを利用して，類似したサーバを複数構築・運用する場合の使い方を**図1**に示す。

(1) VMテンプレート作成

元となるVMと，VM作成後に配置したいアプリケーション・設定ファイルの雛形を作成し，テンプレート領域へ配置する。

(2) パラメータ定義

複数のサーバで共通なパラメータ(VMテンプレート名など)と，サーバ固有のパラメータ(IPアドレス，ホスト名等)を登録する。

(3) 処理フローの作成

サーバの電源入・電源切・VMへのファイルコピー・運用コマンド実行等，このソフトウェアが提供する操作を組み合わせて，従来人手で行っていた作業を登録する。

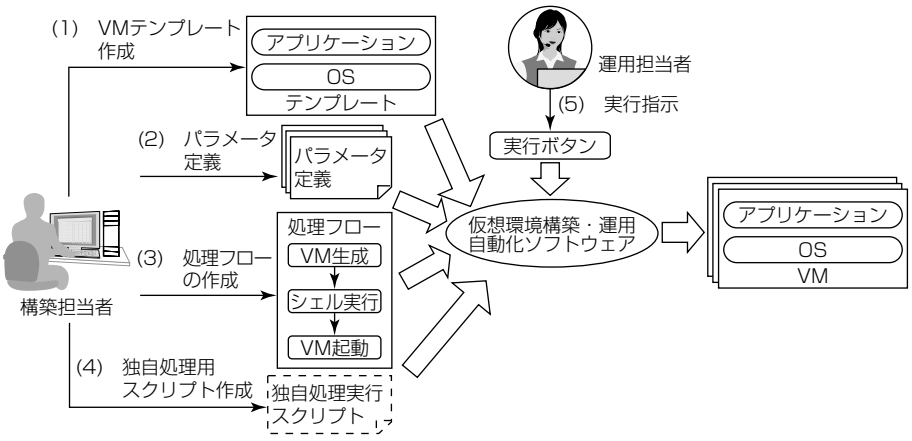


図1．仮想環境構築・運用自動化ソフトウェアの使い方

⑷ 独自処理用スクリプト作成

利用者が作成したアプリケーションを導入したい場合は，個別に独自処理を実行するスクリプトを作成する。

⑸ 実行指示

このソフトウェアの管理画面から生成対象サーバを選択し，実行を指示する。

4. 特　　長

このソフトウェアの3つの特長を次に述べる。

4.1 大量のサーバの並列構築を自動化

4.1.1 VM・OS・アプリケーション構築自動化機能

VM・OSからアプリケーションまで，システム構築手順を自動実行する，このソフトウェアの中心機能である。具体的には元となるVMを複製し，複製したVMに対しMAC(Media Access Control)アドレスとネットワークへの接続設定を行い，VMとOSを起動(電源入)する。VMの起動後，OSに対しIPアドレス・サブネット・ゲートウェイ等のネットワークカードごとの設定と，ホスト名変更を行い，適宜OSを再起動して，設定を反映させる。OSの設定終了後，アプリケーションを導入するためのファイル群を各VMへコピーし，アプリケーションを導入するためのスクリプトを実行する。

この機能によって，ホスト名とIPアドレスだけが異なるVMを多数構築する場合，2台目以降の構築はほぼ全自動で実施できる。

4.1.2 並列実行機能

複数のサーバに対する構築処理を並列で実行する機能である。これによって，1台1台順に構築する場合と比べ，構築にかかる時間を大幅に短縮できる。並列処理数を手動調整することも可能なため，仮想化ソフトウェアの並列処理数の限界値に合わせて，可能な限り並列処理を実行することで，構築時間を短縮することができる。

4.2 定型的な運用作業の自動化

4.2.1 一括実行・順序実行機能

定型的な運用作業を複数のサーバに対し一括，又は順序に従い実行する機能である。

一括実行機能を活用することで，各VMに対し時間がかかる運用作業をまとめて指示できる。実行指示した作業はバックグラウンドで処理されるため，実行指示した管理端末の電源を切り，翌朝実行結果を確認するという使い方もできる。

また，運用作業順序に依存関係がある場合は，順序付けを行うことで，前の作業が終了してから次の作業を自動で実行することができる。幾つかのサーバで処理が失敗した時は，失敗したサーバだけを処理対象とする機能も持つ。

これらの機能によって，大量のサーバに対する運用作業を効率的に行うことができる。

また，被災時のBCP環境への切替え作業のような，非定常的だが，定型的な運用作業を自動化することで，運用容易性を高めることができる。

4.2.2 テンプレート化支援機能

定型的な運用作業を自動化するために，ユーザーが記述する個別スクリプトファイルとOS・アプリケーション用の設定ファイルのテンプレート化を支援する機能である。ファイル中の動的に値を変更したい箇所(IPアドレスなど)をパラメータとして定義し，テンプレート用のフォルダへ保存しておく。このソフトウェアがこのテンプレートを使った運用作業を実行する時に，パラメータに適切な情報をセットし，VMへのコピーと実行作業を自動で行う。

この機能ではパラメータに加え，条件分岐(if文)と繰り返し(foreach文)の制御構文も記述することができる。

図2はこの機能の動作例である。httpd.confという設定ファイルのテンプレートに対し，IPアドレスとドキュメントルート文字列が設定される。

4.2.3 管理画面開発用通信インタフェース

このソフトウェアは，定型的な運用作業の自動化を指示する画面を利用者が自由に開発できるよう，通信インタフェースを公開している。インタフェース形式は，インターネットでのサービス公開インタフェースとして一般的なREST API(REpresentational State Transfer API)を採用することで，特定の開発言語に縛られることなく自由に開発することができる。

このソフトウェアが標準で提供する管理画面(**図3**)もこのAPIを使っている。

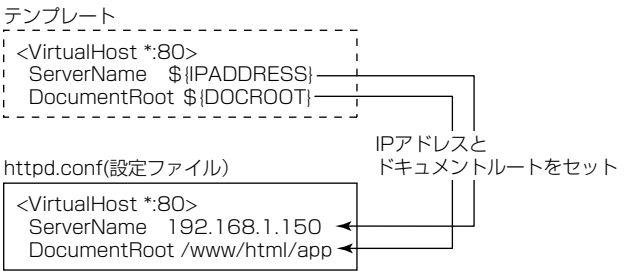


図2．テンプレート化支援機能

図3．管理画面

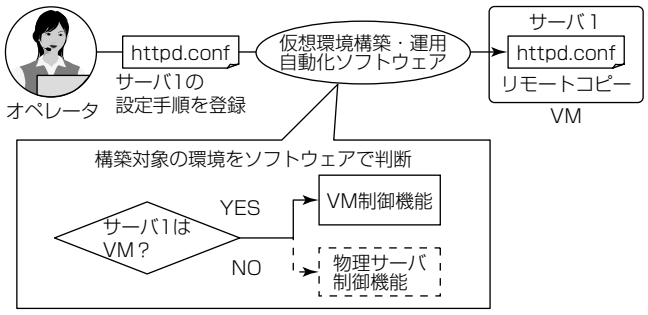


図4．仮想・物理混在環境での動作

4.3　仮想・物理混在環境への対応

4.3.1　VM・物理サーバ制御機能

このソフトウェアは，構築対象がVMか物理サーバかを意識することなくサーバを制御することができる。具体的にはVMの生成・削除・電源入・電源切・一覧取得とOSの再起動・ファイルのリモートコピー・リモート実行といった代表的な制御機能を抽象化し，ベンダー製品ごとの違いを知らなくともVM・物理サーバを制御できる。

図4は，この機能の動作例である。

このソフトウェアは構築・運用対象の環境に応じた制御手順を選択することができる。そのため，**図4**の例のようにhttpd.confという設定ファイルをサーバ1へリモートコピーしたい時，オペレータはサーバ1がVMか物理サーバか知らなくとも，サーバ1へリモートコピーを実施できる。

5. 適用事例と効果

大手上場企業の商品紹介Webシステムでの適用事例について述べる。このシステムは本番環境とそれに類似した環境(検証環境，開発環境，BCP環境)を複数運用している(**図5**)。そのため大量サーバの構築工数削減とミス低減，運用の効率化が課題であった。このソフトウェアを活用することで，大量のサーバの構築や定型的な運用作業を自動化し，課題を解決することができた。

(1)　大量のサーバの構築自動化

この適用事例では，環境構築後に本番環境の設定変更が発生し，対応するBCP環境の作り直しも数回発生した。BCP環境も大量のサーバを持つため，すべてを手動で作り直すことは非常に手間がかかる。しかしこのソフトウェアを適用することで，BCP環境の作り直し作業をすべて自動でかつミスなく実施でき(**図5**の①)，その結果，BCP環境の再構築工数を大幅に削減できた(**図6**)。

(2)　運用の効率化と運用容易性の向上

適用事例では，被災時のBCP環境への切替え作業を仮想化ソフトウェアやこのシステムの専門知識がないオペレータでも迅速・確実に実施できることが求められた。

そこでBCP環境への切替え手順をこのソフトウェアへ登録し，画面開発用インタフェースを使って被災時専用画面

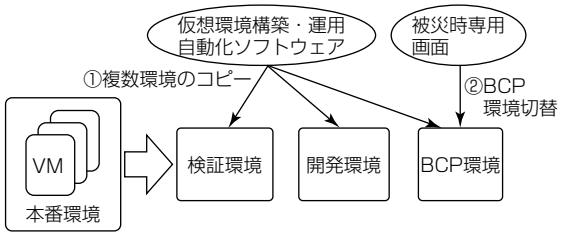


図5．適用事例

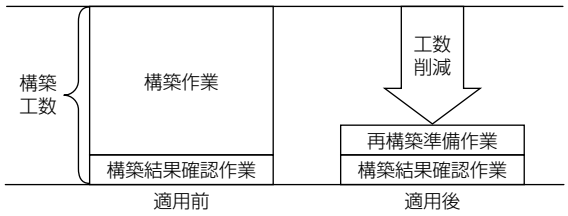


図6．BCP環境の再構築工数削減効果イメージ

を提供した。その結果，オペレータは専用画面上のボタンを押すだけで切替え指示を確実に行うことができる(**図5**の②)。また，幾つかのVMで処理が失敗した時は，“失敗したVMだけ再構築の処理対象にしたい”と指示するだけで，このソフトウェアが自動で対象を判断し切替え作業を再開することができるようになった。

さらに，目標復旧時間(被災した後，迅速にBCP環境へ切り替わるまでの目標時間)についても，このソフトウェアの並列実行機能を活用することで，顧客の目標を達成した。

6. むすび

先に述べた適用事例を皮切りに，ITシステムの構築・運用の自動化を希望する顧客がMDISでも急速に増えてきている。

今後サーバ仮想化だけでなくネットワークやストレージの仮想化が進展すると，仮想化ソフトウェアを使ったITシステムの構築・運用の自動化が今まで以上に可能となる。これは“Infrastructure as Code”[4]とも言われており，より大量のサーバの構築・運用が効率良く行えるようになる。MDISもこの潮流に追随するために，更なる構築・運用自動化の機能拡充と対象プラットフォームの拡大を図っていく。

参考文献

(1)　IDC：Green IT: Where's the Competitive Advantage for CIO's?，Doc # DR2008_3MEW（2008）
(2)　林　喜男：人間信頼性工学－人間エラーの防止技術，海文堂（1984）
(3)　一般社団法人　日本情報システム・ユーザー協会：ソフトウェアメトリクス調査2010（2011）
(4)　Theo Sohlossnagle，et al.：Infrastructure as Code，InfoQ http://www.infoq.com/presentations/infrastructure-as-code

特集論文

クラウド環境でのSAP基幹システムのフルアウトソーシングサービス

百本征弘* 佐藤雄蔵*
丸山隆久*
関 吉隆*

Full Outsourcing Service for SAP System on Cloud Environment

Yukihiro Momomoto, Takahisa Maruyama, Yoshitaka Seki, Yuzo Sato

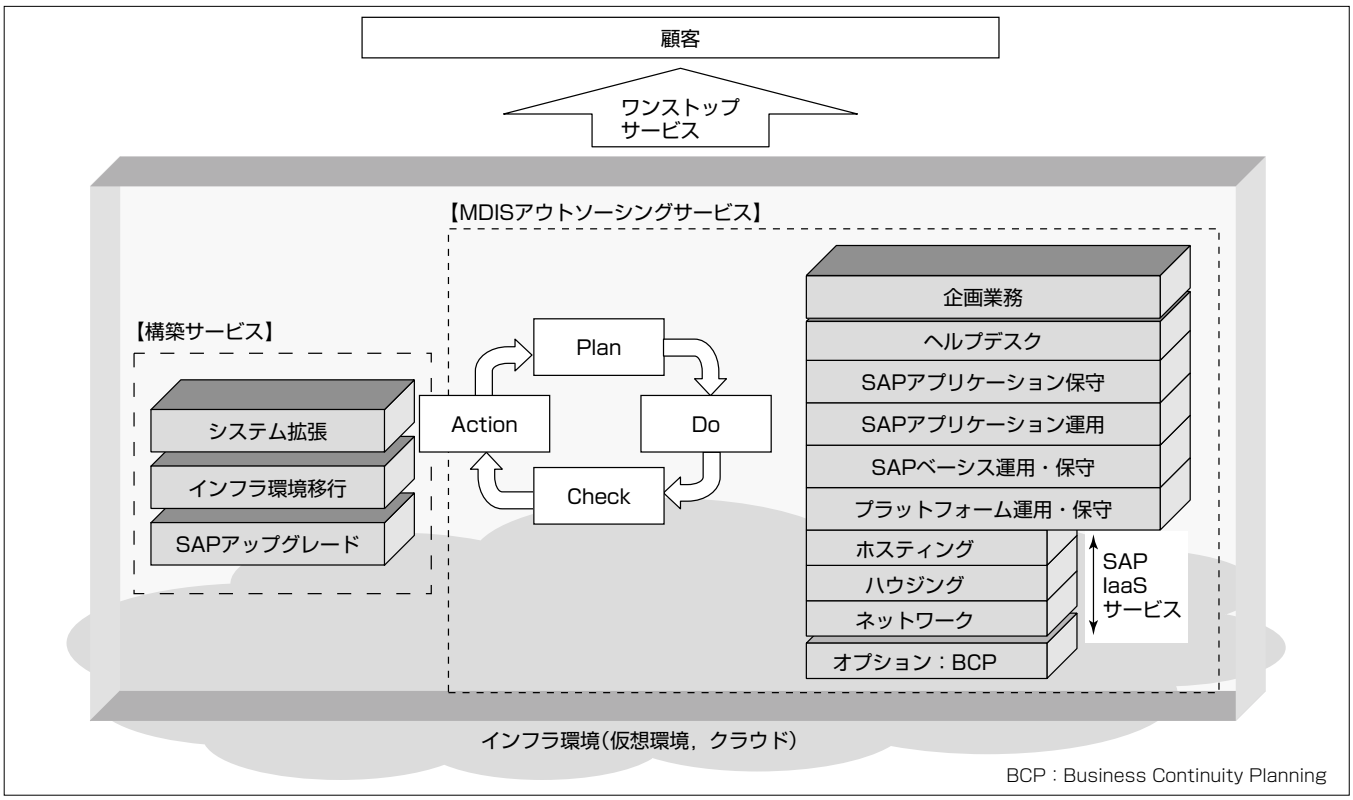
要 旨

三菱電機インフォメーションシステムズ㈱(MDIS)では，製造業顧客向けに，企業向けエンタープライズソフトウェア最大手のSAP社ERP(Enterprise Resource Planning)製品を核としたソリューション(以下“SAPソリューション”という。)を主に提供している。SAPソリューション提供では，情報システムの運用を含めたTCO(Total Cost of Ownership)削減，さらにはアウトソース化ニーズの高まりもあり，顧客向けサービスの向上を目的として，運用保守の提供やハウジング・IaaS(Infrastructure as a Service)化にも取り組んでいる。

MDISのSAPソリューション事業では，蓄積されたノウハウを活用し，構築から運用までの“ワンストップサービス”を提供する柱として，アプリケーションからインフラまでシステム全般の運用保守に対するフルアウトソーシングサービスをメニュー化し提供している。

サービスの特長としては，顧客ごとに必要なサービスを選択・組み合わせることによってプラットホームからアプリケーション・ビジネス領域まで対応できること，SLA(Service Level Agreement)によるサービスマネジメント対応であること，グローバル対応であること等が挙げられる。

また現在，MDISのSAPソリューション事業のクラウド対応としては，仮想化環境構築(プライベートクラウド)及びIaaS上でのSAPシステム構築，さらにはこれら環境へのシステム移行サービスがある。仮想環境利用で，I／O(Input／Output)性能を十分に引き出すためには仮想ソフトウェア・SAPの設定及びディスクレイアウト設計が重要であり，IaaSサービス活用では，パッケージ化されたハードウェア構成や運用を維持しつつ，メモリチューニングや運用環境面での対応によって補完していくことが重要である。



MDISのインフラ環境提供及び運用保守サービス

基幹システム再構築，SAPシステム導入済み顧客に対するSAPアップグレードやインフラ環境移行サービス，さらにはSAPシステム安定運用を実現するアウトソーシングサービスを，ワンストップで提供している。インフラ環境面では，物理サーバ及び仮想サーバを，顧客管理下の設備に設置するオンプレミスの形式に加えIaaSによるサービス提供を，アウトソーシングサービスでは，運用保守サービスから稼働評価の上での改善提案や追加開発への対応までをサービス提供する。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

MDISでは，製造業向けソリューションとして，SAP社ERPパッケージを基軸としたSAPソリューション事業を展開している。事業の特長としては，三菱電機㈱の基幹システム構築及び運用ノウハウを基にした製造業向けソリューションの展開，インフラ面ではマルチベンダー対応，フルアウトソーシング対応等が挙げられる。

ここ数年，運用コスト削減，及びハードウェアの自社での所有からサービス化への移行ニーズが高まる中で，クラウドコンピューティングの概念が具体的なサービスとして出始め，SI(System Integration)構築からサービス活用への転換が起きている。また，セキュリティ対策やBCP対策として，基幹システムを安全な場所へ設置するニーズも高まっている。この背景の下，SAPソリューション事業でもクラウド対応に取り組んでいるが，サービス型のインフラ提供ではSAPシステム固有のサイジング基準を満足することが必要であり技術検証が必須となっている。

本稿では，MDISが提供するSAPシステムのフルアウトソーシングサービスの内容，サービス型インフラ提供に関する取組み及び実プロジェクトでの事例について述べる。

2. フルアウトソーシングサービス

MDISではSAPシステムをコアとしたアウトソーシングサービスを約10年間，複数の顧客に提供している。この実績からSAPのインフラ，アプリケーションに関する技術，知識を蓄積してきており，これを基盤としてSAPシステムを対象としたAMO(Application Management Outsourcing)及びITO(Information Technology Outsourcing)のサービスメニュー，サービス提供体制を整備している。顧客は，MDISのサービスを利用することで，情報システム部門の人員を最小化することが可能となり，その人員をより付加価値の高い業務に割り当てることができる。

AMOサービスでは，問合せ対応のアプリケーション保守からシステム運用全般まで，さらには顧客システムの将来像のプランニングまで含めた改善を提案・提供している。

またAMOではアカウントマネージャーを設定し，顧客志向を取り入れた企画・運用サービス提供を行っている。一方ITOサービスでは，インフラレベルのホスティングサービスの提供だけではなく，専門スキルを持つSAPのBASIS(パッケージ運用・改善)分野に特化したエンジニアを配置して，システム全体を包含した運用サービス提供を行っている。

MDISのSAPシステムアウトソーシングサービスのメリットとして，次の点が挙げられる。

(1) 顧客に合わせたサービスの選択・組合せが可能

インフラからアプリケーションまで，サービスメニューの中から必要なサービスを選択・組み合わせることで顧客の要求に合ったサービスを提供できる(**表1**)。

(2) SAP専門要員の配置による安定したサービス提供

SAPシステムの運用保守に必須のSAP製品に精通した要員を配置している。SAP専門のアウトソーシングサービス提供体制を**図1**に示す。

(3) サービスの見える化

サービスごとのSLAと実績データを継続的にモニタリングし，SLA未達のサービス，課題があれば改善を実施することができる。

(4) 24時間×365日対応のグローバルサポート

国内外ユーザーへの対応，製造業顧客のシステム稼働時間要件への対応が可能である。

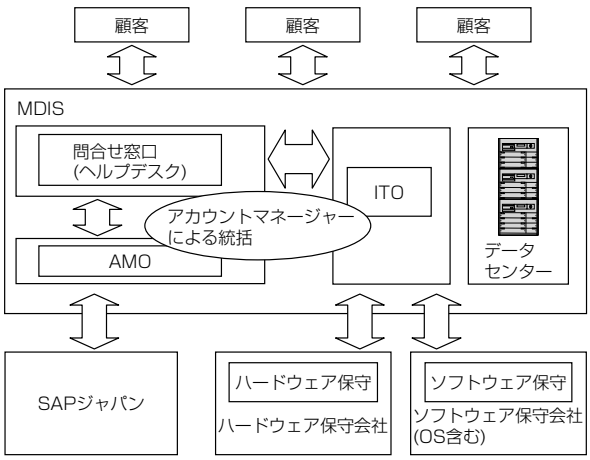


図1．アウトソーシングサービス提供体制

表1．SAP基幹システムを対象としたMDISのアウトソーシングサービス

分類	サービスメニュー		アウトソーシングサービスパターン			メリット	参考：アウトソーシング未実施時の対応
			フルアウトソーシング	運用保守＋インフラ提供	保守中心(インフラは顧客)		
AMO 対象：アプリケーション SAP：生産，販売，在庫購買，会計，原価アドオン	企画業務		MDIS	顧客	顧客	(1) 顧客体制・予算からサービスメニューを顧客要件に合わせて，自由に選択 (2) 料金＝基本＋チケットでの従量制 →顧客IT部門の固定費用から，サービス活用による変動費用とすることで顧客コスト削減	顧客IT部門で運営 SAPスキル習得必要 ＝体制固定 ＝固定費用
	ヘルプデスク			MDIS			
	SAPアプリケーション保守				MDIS		
	SAPアプリケーション運用				顧客		
ITO 対象：データセンター，ネットワーク，ハードウェア，OS，ミドルウェア SAP：BASIS(ベーシス)	SAPベーシス運用・保守		MDIS	MDIS	MDIS	(1) SAPを対象とした，大／中／小規模用パックを準備。パック選択によって，システム構築をオーダメイドからレディメイドにすることで，工期，コストの削減が可能 (2) オプションでBCP対応メニューを提供	顧客IT部門で運営 SAPスキル習得必要 ＝体制固定 ＝固定費用
	プラットフォーム運用・保守			顧客	顧客		
	ホスティング	SAP IaaS サービス		MDIS			顧客資産で運営 ＝顧客ごとの構築
	ハウジング						
	ネットワーク						
	オプション：BCP						

3. サービス型SAPインフラ

3.1 インフラ提供方法

インフラ環境としては，従来のオンプレミス中心から，規模感／用途／稼働要件／運用要件等に応じて自社資産を持たないサービス型環境も提供しサポートしている(**図2**)。現在MDISのSAPソリューション事業で推進するクラウド環境は，仮想化(プライベートクラウド)及びIaaSの活用である。

3.2 SAP ERP環境の仮想化及びIaaS対応への取組み

企業の情報システムインフラの選択肢が増えている状況下で，MDISのSAPソリューション事業でも，サービス提供型インフラとして，①仮想化技術検証(2010年度)，②IaaSサービスメニュー化(2011年度)，③実サービス化(2012年度)と，段階的に取り組んできた。

3.2.1 SAP仮想化技術検証

2010年から社内モデルによる実機検証を通した実現性の検討を行ってきた。検討にあたっては，仮想化ソリューションとしてVMware vSphere(注1)を対象とし，SAP社技術情報の仮想化ガイドラインに基づくインフラ設計，SAP環境の物理環境から仮想環境へのシステム移行(P2V(Physical to Virtual))，仮想環境上でのSAP本稼働を踏まえた性能面・運用面の評価を実施した。

実現性検討の結果，システム性能に影響を及ぼすのはディスクI／Oの負荷増であり，仮想サーバごとに競合しない設計とすること，及びP2Vによるシステム移行ではイメージ形式でバックアップを取得するツールを用いたシステム移行が可能であり有効であることを確認し，その成果をSAPシステム仮想化ガイドとしてまとめた。

(注1) VMware vSphereは，VMware Inc. の登録商標である。

3.2.2 IaaSを利用したSAP構築・運用

IaaS利用にあたっては，SAPシステムとしての特長を考慮し，サイジング結果及び非機能要件を中心としたFit&Gap評価(適合性評価)を行い，数百ユーザー程度の小規模システムに対し，IaaSサービス提供可能な構成を構築できると判断した。ここで主なFit&Gap評価項目は，①拡張性(ユーザー数やトランザクション数，及びそれを踏まえたCPU／メモリ拡張性)，②ストレージ性能(I／O処理能力)，③バックアップ(処理時間・業務停止時間等)，④可用性(連続運転性)，⑤コストといった点である。

定型化された機器構成や運用の中で，低価格化・環境提供の短納期化・顧客運用負荷軽減といった点はサービス化の目処(めど)が立ったが，SAPシステムとしての非機能要件を満たし，SAPシステムとしての運用実現にあたっては，以下の点の個別対応が必要であった。

(1) 大規模データベースにおけるバックアップ運用

基幹系システムで求められる高稼働率やグローバルへの対応のため，データバックアップで停止する時間を極小化することが必要である。IaaSサービスでは通常，システム稼働状態によらずに定時起動でバックアップ処理が実行されることもあり，バックアップに伴う許容停止時間やリカバリーポイントを踏まえ，SAPシステム用にDBMS(Database Management System)機能によるオンラインバックアップの雛形(ひながた)を作成し，運用要件を満たすソリューションとした。

(2) SAP及びDBMSのパラメータ設計・設定

IaaS環境では，ストレージは共用で利用するため，I／Oが多く発生する業務では性能への影響も懸念される。この課題には，必要なメモリを搭載した上で，サーバ上のメモリを有効活用できるようなSAP及びDBMSのパラメータ設計を行い，ディスクI／Oを極小化させることで対処した。

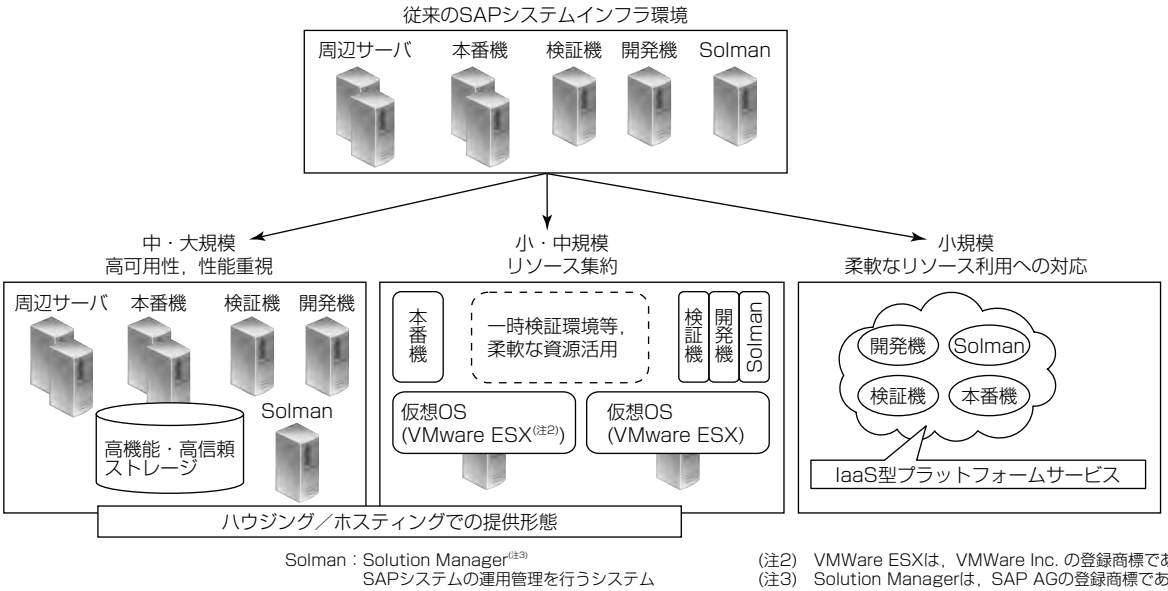


図2．MDISの提供するSAPシステムのインフラ環境

4. 事　例

SAP導入済みの顧客システムをクラウド環境に移行する場合，①仮想環境へシステム移行する場合，②IaaS環境へシステム移行する場合の2つの場合があり，それらの事例について述べる。

4.1 SAP本番システムの仮想環境への移行事例

この事例での顧客は，ハードウェアは顧客自身で購入して自社に機器を設置し，アプリケーション保守をMDISが実施していた。

システム移行は，SAPの最新バージョンアップに伴うIT基盤強化，ハードウェア保守期限対応，TCO削減，BCP対策等を目的としたものである(**図3**)。本番環境を含めた仮想化へのニーズ，重要システムに対する性能や可用性要件も考慮し，IaaSサービスではなく，顧客が購入済みの機器上に仮想環境を構築するという方法を選択した。その結果，仮想化によるサーバ集約，及び，データセンターへのシステム移行に伴う顧客運用負荷軽減を実現することができた。

仮想環境へのシステム移行にあたっての技術的ポイントを次に挙げる。

(1) 移行元・移行先のOSバージョン及び移行元環境の特性(仮想化された環境か否か)によって，移行手順は異なる。確実なシステム移行実施には，各組合せによる移行検証が必要である。

(2) SAP利用環境におけるSAP社及びVMware社推奨設定情報から，Ethernet(注4)やSCSI(Small Computer System Interface)関連仮想ドライバではスループットを最適化する仮想ドライバの選定が必要である。

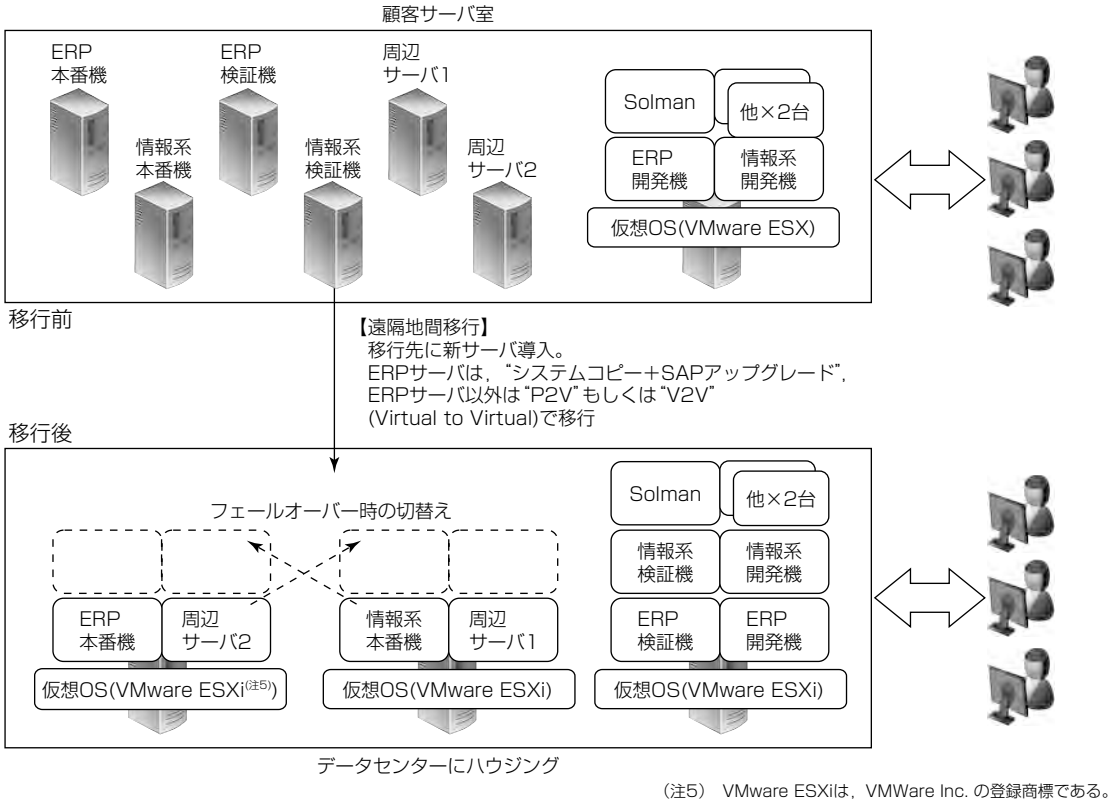
なお，移行後の機器レイアウトの最適配置を考慮したディスクレイアウト設計，及び新旧の構成差異を踏まえた環境移行が必要である。今後，これらの事項もSAPシステム仮想化ガイドにまとめ，導入設計及び移行手順の標準化を推進していく。

(注4) Ethernetは，富士ゼロックス㈱の登録商標である。

4.2 SAPシステムのIaaS環境への移行事例

この事例の顧客システムでは，冗長化構成のサーバ及びストレージをデータセンターに設置し，またこの顧客はインフラ運用保守及びアプリケーション保守としてMDISアウトソーシングサービスを利用していた。

この顧客の情報システム部門の方針としては，従来型のハードウェア所有から運用のサービス化を志向し，情報系から順次クラウド化を進めているという状況にあった。今回，インフラ運用負荷軽減とBCP対策もねらい，SAPシステムのクラウド化を実施した。その際，サービスメニューベースへの運用見直し，さらにはSAP対応モデルへの適用性も踏まえ，IaaS環境へのシステム移行とした(**図4**)。ただし，対象システムが基幹系システムであり，安定したバッチ処理性能が要求されることから，1台の物理サーバに複数顧客システムが同居する形態ではなく，顧客専用の



(注5) VMware ESXiは，VMWare Inc. の登録商標である。

図3．仮想環境へのシステム移行事例

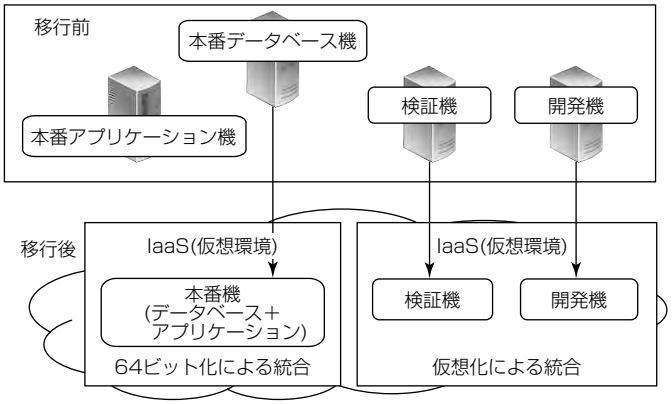


図4．IaaS環境へのシステム移行事例

サーバ上に仮想環境として提供されるIaaSモデルを採用した。また，IaaSモデルの場合，必要に応じて構成増強ができるため，最低限のインフラ構成とすることとした。

移行にあたっては，最低限の構成を実現するために運用を見直し，サーバ冗長構成の簡易化や，リカバリー用スナップショットの取得タイミングの削減を行った。システム的には，DBMSの64ビット化を新たに行うことで，メモリ空間拡大を可能とし，本番データベースサーバとアプリケーションサーバの統合及び稼働実績を踏まえたサーバ台数削減を実現した。

一方クラウドサービスのストレージ部分は共用で利用するものであり，競合時の負荷にも対応できるように，システムに余裕を持たせることが重要である。今後はオンメモリ化の実施など，より一層クラウド環境に見合った構成への変更が必要と考えている。

5. むすび

MDISのSAPソリューション事業では，従来のハードウェアを導入し，SI構築を行うというモデルに加えて，稼働後の効率的な運用を意識したサービス提供型のモデルの重要性が増してきている。そのためのソリューションが，基幹システムのフルアウトソーシングである。フルアウトソーシングでは，顧客のパートナーとしてインフラの運用を行うとともに，ライフサイクルに対応したサービスを継続的に提供していくことが重要である。今後は，対象領域をSAPシステム中心から非SAPのアプリケーション領域へと拡大し，またインメモリやモバイルソリューションといった新技術クラウド環境にも取り組み，アウトソーシングサービスでの提供を目指していく所存である。

参考文献

(1) 松田昇平，ほか：ITサービスインテグレーション“BizFLEX”，三菱電機技報，**85**，No.8，449～452（2011）

特集論文

企業の安心・便利を支えるクラウドID管理サービス“DIASMILE”

勝山尚彦* 佐藤雅之**
濱田 剛*
大沼聡久*

DIASMILE：Cloud-based ID Management Service to Provide Security and Convenience for Companies

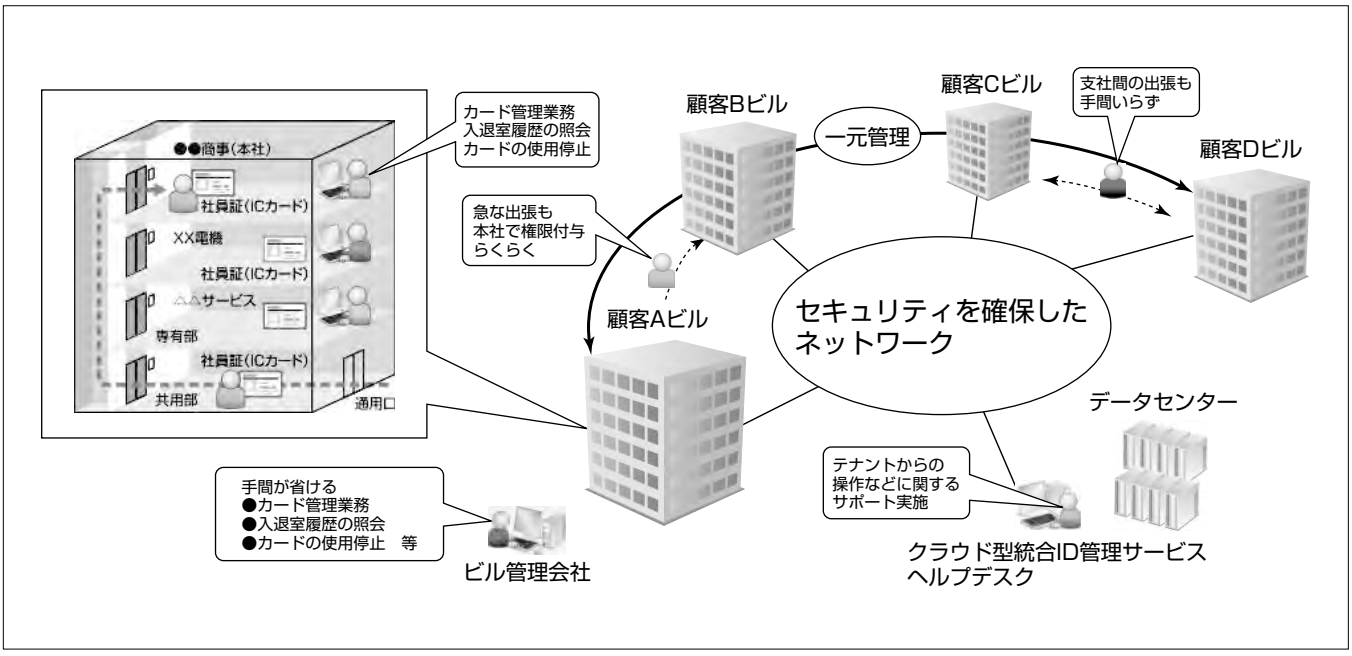
Naohiko Katsuyama, Tsuyoshi Hamada, Akihisa Oonuma, Masayuki Sato

要 旨

不正競争防止法の改定，個人情報保護法，日本版SOX法（米国企業改革法）の施行，サイバー攻撃の激化によって，企業におけるセキュリティ強化のニーズは高まっている。情報システムでは，シングルサインオンなど複数のシステムを統一して認証することによって，利用者の利便性を向上させるとともに，セキュリティの強化を進めてきた。一方入退管理システムやセキュアプリンターを始めとする物理セキュリティシステムについては，機器が拠点ごとに導入されてきた経緯もあり，その管理についても拠点独自で進めているケースが多い。これらの機器の管理者は，組織変更や人事異動による配置転換が発生した場合，それぞれの物理セキュリティシステムに対して，都度メンテナンスを行う必要がある。その結果，管理負荷が増大するとともに，変更漏れなどによるセキュリティリスクも拡大してきている。

クラウドID管理サービス“DIASMILE”（以下“DIASMILE”という。）は，従来ビル管理会社が運用していた入退管理システムのIDカード管理を利用者（テナント）に開放し，利用者が直接行えるようにすることで，利用者の利便性を向上させるサービスである。DIASMILEでは，複数の物理セキュリティシステムを統合的に管理する考え方のもと，入退管理システムなどをインターネット経由で接続する。これによって，従来はビルごとに設置されていた入退管理システムや従来のID管理ソリューションでは対応できなかった専有部と共用部の一元管理や，分散した企業の入退管理を一元的に行うことが可能となった。DIASMILEのベースとなる統合ID管理ソリューション“iDcenter”は，三菱電機グループ11万人が利用する情報システム基盤に導入され，三菱電機グループ内の様々な情報システムに対する統合ID管理としての機能を提供してきた。その大規模システムの実績を踏まえて，DIASMILEでは，各利用者が独自に利用できる基盤を構築可能とし，利用者に開放するサービス提供を実現した。その結果，企業における生産拠点や営業拠点の物理セキュリティシステムを一元的に管理するニーズへの対応が可能となった。

今後は，各拠点にある様々な物理セキュリティシステムと接続可能とするように機能を拡充し，利便性，安全性の向上を図っていく。



クラウドID管理サービス“DIASMILE”の全体イメージ

利用者（テナント）は，ビルの共用部，及び自社の専有部を通行する自社社員の個人情報，カード情報，通行権限などに対する管理業務を自席から行うことが可能である。また，他ビルに入居する支社などに関する管理業務も一元的に行うことが可能である。これによって，複数のビルに跨（またが）った場合でもカードの一枚化やセキュリティポリシの統一が可能となり，セキュリティリスクの低減や管理業務の負荷低減，利便性を向上させることができる。

*三菱電機インフォメーションテクノロジー㈱ **三菱電機㈱ 情報技術総合研究所

1. まえがき

不当競争防止法の改定や，個人情報保護法，日本版SOX法の施行によって，企業は，営業機密，個人情報，財務情報の漏洩(ろうえい)による損害賠償や社会的な責任を問われるようになった。また，サイバー攻撃の激化によって情報漏洩のリスクが高まっている。そこで，企業は情報を保護するため，セキュリティポリシーの強化・徹底，建物への不正侵入を防止する物理セキュリティ対策と情報システムへのネットワーク経由の不正侵入を防止する情報セキュリティの対策を強化している。

物理セキュリティの主要な対策である入退管理システムについては，機器が拠点ごとに導入されてきた経緯もあり，そのID管理も拠点ごとに行われているケースが多い。組織変更や人事異動が発生した場合に，それぞれの入退管理システムに対するメンテナンスを行う必要があり，ビル管理会社や企業の管理部門の管理負荷が増大するとともに，変更漏れによるセキュリティリスクも拡大してきている。

クラウドID管理サービス“DIASMILE”は，ビル管理会社などが運用していたID管理を利用者(テナント)が直接行えるようにしてビルの専有部と共用部の一元管理を可能にすると共に，企業が各拠点に分散していたID管理を一元的に行うことを可能にする。

本稿では，入退管理システムの課題，課題解決に必要な機能，及びそれらの機能を備えたDIASMILEについて述べる。

2. 入退管理システムの運用の現状と課題

従来の入退管理システムは，ビルごとで導入及び管理が行われてきた。そのため，施設管理部門や管理部門から委託を受けたビル管理会社が管理を担当していた。近年，通行権限の設定や通行履歴の閲覧等，利用者(テナント)自身による実施が利用者にとってのメリットとなるような運用は，利用者で実施できるようにすることで，ビル管理会社の運用負荷を軽減することが求められてきた。しかしながら，利用者自身が運用を行う場合は，利用者の情報をほかの利用者から秘匿するなどセキュリティの確保が課題となる。

一方，従来の入退管理システムは企業内ネットワークに接続されていないため，本社と複数の拠点(支店や工場等)を持つ企業では，それぞれの拠点の入退管理システムは，個別に通行権限が管理されていた。入退管理システムを拠点ごとに運用しているため，複数の拠点間で異動が発生した場合に，通行権限の設定変更の負荷が高く，設定ミスが発生する要因の一つとなる。また，複数の拠点の組織を兼務する人や複数の拠点の組織を横断するプロジェクトに属する人の通行権限の設定も各拠点で個別に行う必要があり，組織やプロジェクトの情報を活用した効率的で安全な通行権限設定も困難となる。企業で統一的なセキュリティポリシーを策定した場合でも，各拠点で個別に適用する必要があり，セキュリティポリシーが適切に拠点に適用されているかを確認する負荷も大きい。

次に，IDカードの運用・管理について考える。複数のテナントが入居するテナントビルでは，一般的にビルに導入されている入退管理システムはビル所有者が所有する。その場合，利用者はビル所有者から提供されたIDカードで入退管理システムを利用する。このような環境では，テナントビル内に支店などの拠点を持つ企業が社員証といった全社統一のIDカードをビルの入退管理システムで利用することができない。利用者は，社員証とビルの入退管理システム用のIDカードを管理する必要があり，IDカードの紛失といったセキュリティ事故の発生，事故発生時におけるIDカードの識別番号による個人の特定が困難といったセキュリティ上のリスクが存在している。また，異なる拠点に出張した場合，同じ会社にも関わらず，社員証で入館できず，利便性が損なわれる。

これまで述べたように，入退管理システムの現状の運用における課題は次の4点に集約される。

(1) ビル管理会社の入退管理システム設定作業の負荷軽減
(2) 複数のIDカード利用による利便性の欠如と紛失等によるセキュリティリスクの増大
(3) 拠点間を跨ぐ組織や異動及び出張における通行権限設定の運用負荷の増大
(4) 運用が各拠点単位で実施されていて，セキュリティポリシーの統一的な適用や適用の確認が困難なことによる，セキュリティリスクの増大

3. クラウドID管理に必要な機能

3.1 運用形態に対するニーズ

1章で述べた入退管理システムに対する課題を解決するためには，“テナント開放”“複数拠点の一元管理”といった運用形態に対するニーズを満たす必要がある。

(1) テナント開放

テナント開放とは，テナントビルのような入退管理システムの利用者(テナント)と所有者が異なる場合で，利用エリアの通行権限設定や利用カードの管理を利用者自身が行う運用形態である。これによって，**2章**で示した課題(1)，課題(2)に対応することが可能となる。

(2) 複数拠点の一元管理

複数拠点の一元管理とは，複数の拠点(支店や工場等)を利用する企業で，セキュリティ管理部門が策定したセキュリティポリシーに基づき，全ての拠点で設置されている入退管理システムの設定を行う運用形態である。これによって，課題(3)，課題(4)に対応することが可能となる。

3.2 機能要件

3.1節で述べたニーズを満たすために必要とされる機能について述べる。

3.2.1 テナント開放を実現するための機能

⑴ 管理権限付与

管理権限付与機能は，テナント開放の中核を成す。この機能によって，テナントビルに入居している各利用者(テナント)に対して，入退管理システムに対する管理者権限を与えることができる。管理者権限が与えられた利用者は，入退管理システムに対して通行権限設定や通行履歴の閲覧，利用するカード情報の登録が可能になる。このとき，利用者は社員証といった自社保有IDカードを登録でき，ビルから貸与されるカードや他拠点のカードとの2枚持ちから開放され，共通カードの利用が可能になる。この機能によって，入退管理システムへの登録作業の時間短縮やカードの1枚化による利便性の向上，又はカード紛失といったセキュリティ事故に対するリスク軽減が可能になる。

⑵ アクセス制限

アクセス制限機能は，任意の利用者(テナント)が管理する情報に関して，ほかの利用者からのアクセスに対する保護・秘匿を行う。この機能によって，それぞれの管理情報に対する利用者間の相互アクセスを禁止し，不正な通行権限設定による侵入や機密情報の漏洩といったセキュリティ事故を防ぐことができる。

3.2.2 複数拠点の一元管理を実現するための機能

⑴ 役割による通行権限設定

通行権限設定機能は，組織，資格といったある役割によって指定されたグループに対して通行権限設定を行う。企業内で機密情報に対するアクセス制御を実施する場合には，組織や資格等の役割によってアクセス制御を行う方が，個人単位でアクセス制御を行うより，セキュリティポリシーを適切に反映でき，異動に伴う設定変更も少なくすることができる。入退管理システムにおける通行権限設定も同様であり，機密情報を管理する部屋に入室するための通行権限は，組織や資格等の役割で設計・管理・運用する必要がある。この機能によって，個人単位での入退管理システムの通行権限の設定が不要となり，設定ミスの防止や運用負荷の軽減ができる。

⑵ 設定の自動化

設定自動化機能は，通行権限の設定変更や入退管理システムへの反映を自動的に行う。⑴の“役割による通行権限設定”で，組織構成の変更によって組織の役割が変わった場合や組織に所属する社員に異動や変更があった場合，入退管理システムに対して通行権限の変更情報を自動反映する。この機能によって，従来手動で変更していた通行権限設定が自動的に行われるため，設定ミスの防止や運用負荷の軽減が実現される。

4. クラウドID管理サービスDIASMILE

3章に示した課題を解決するための機能を備えたシステムがクラウドID管理サービスDIASMILEである。

4.1 DIASMILEとは

DIASMILEは，テナントビルに入居する利用者(テナント)自らが入退管理システムの通行権限管理，通行履歴管理，カード管理等運用を行える機能を提供するサービスである。利用者は，クラウド上に設置されたID管理システムに対してセキュリティを確保したネットワークに接続された端末からアクセスして管理業務を行うことができる。サービスヘルプデスクを用意し，サービス利用者に対して利用方法等に関するサポートも行う。**図1**にDIASMILEのイメージを示す。

4.2 システム構成

DIASMILEのシステム構成を**図2**に示す。

サービスの利用者(テナント)は，インターネットに接続された自席の端末から，サービスにアクセスが可能である。一方，入退管理システムは，このサービスを提供するサーバとセキュリティを確保したネットワークで接続されており，入退室の権限情報や通行履歴情報を送受信する。現状，このサービスでは，連携する入退管理システムとして，三菱統合ビルセキュリティシステム“MELSAFETY-G”を対象としているが，今後対象範囲を拡大していく。

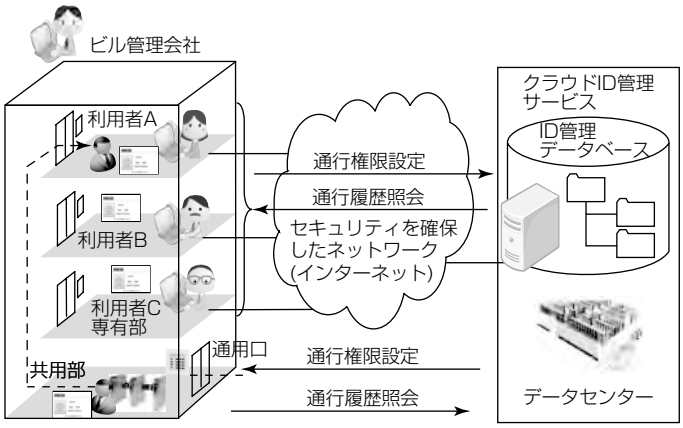


図1．DIASMILEのイメージ

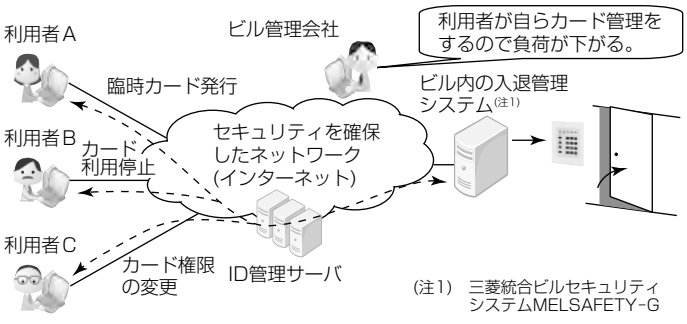


図2．DIASMILEのシステム構成

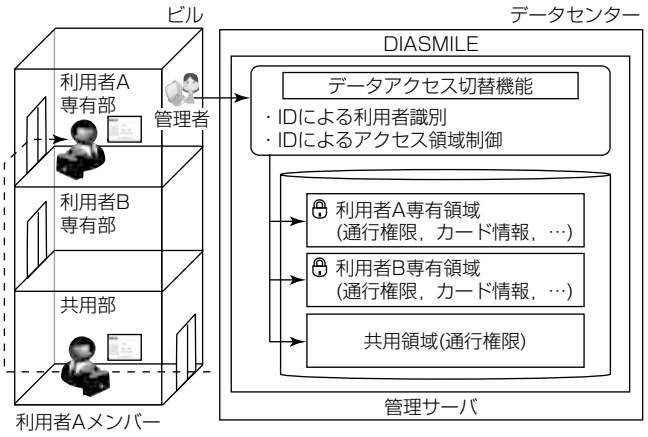


図 3．管理権限の付与及びアクセス制御機能

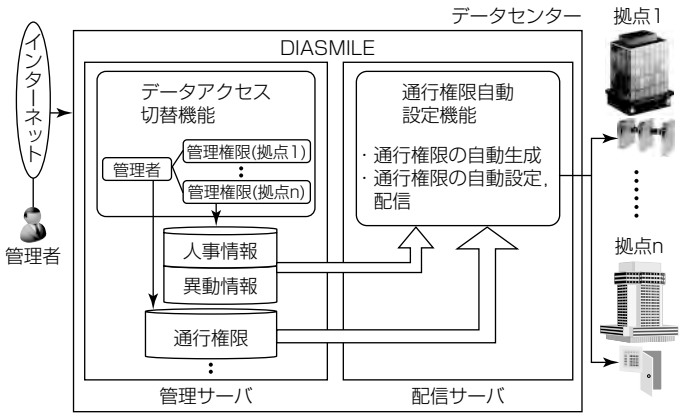


図 4．通行権限管理の集約と自動化の機能

4.3 特　　長

DIASMILEの特長は，次のとおりである。

⑴ 利用者への入退管理システム操作の開放

DIASMILEは，利用者への入退管理システム操作の開放に当たって，管理権限の付与とアクセス制御を行う機能を実現した。この機能は，IDによって利用者を識別し，システム上でアクセス可能なデータ領域を制御する。システムで扱うデータを格納するデータ領域には，共用領域と専有領域があり，前者では共用部の通行権限を管理し，後者では利用者ごとの人事情報やカード情報，専有部の通行権限を管理する。また専有領域では，共用部の通行権限と人事情報との関連付け情報も管理しており，この関連付け情報によって，共用部の通行権限を参照可能としている。

図 3 に，管理権限の付与及びアクセス制御機能について示す。

⑵ 役割による通行権限の設定

役割に対する通行権限設定を行うため，ロールによる通行権限の設定機能を実装した。ロールとは組織やプロジェクト，資格といったある役割で指定されるグループを指す。これによって，従来は個人ごとに行っていた通行権限設定を組織などに対して設定することが可能となるため，設定作業や通行権限の棚卸し作業の省力化ができるとともに，設定ミスや設定漏れを解消することができる。また，通行権限の設定は従来と同様に個人に割り当てることも可能であり，組織と個人を混在して割り当てることもできるため，柔軟な通行権限の設定ができる。例えば情報システムエリアについては，情報システム課に所属しているメンバーと，各部門のOA管理者を入室可能にさせるといった設定ができる。

⑶ 設定と配信の自動化

DIASMILEは，データセンタ上の管理サーバに，異動情報を含む人事情報，通行権限の情報を集約，一元管理している。管理者がインターネットに接続された自席の端末から異動情報などを入力すると，組織などに割り当てられた通行権限設定を自動的に個人単位の設定に分解し，各拠点の入退管理システムへ自動的に反映する。これによって，企業では，設定のミスや漏れが解消され，手作業による負荷削減，システム管理コストの削減が可能となるとともに，セキュリティポリシーの統一が可能となる。**図 4** に通行権限管理の集約と自動化，及びそれらを実現可能とする機能について示す。

5. む　す　び

DIASMILEのベースとなる統合ID管理ソリューション“iDcenter”は，三菱電機グループ11万人が利用する情報システム基盤に導入され，三菱電機グループ内の様々な情報システムに対する統合ID管理としての機能を提供してきた。その大規模システムでの実績を踏まえて，DIASMILEでは，各利用者が安全に，それぞれが独自に利用できる基盤の構築を可能としたサービス提供を実現した。その結果，企業における生産拠点や営業拠点など，離れた拠点間の物理セキュリティシステムを一元的に管理するニーズへの対応が可能となった。今後は，各拠点にある様々な物理セキュリティ機器と接続可能とするようにオプションを拡大していくことで，利便性，安全性の向上を図っていく。

参 考 文 献

⑴ 木幡康博，ほか：確実なセキュリティ運用を実現する統合ID管理システム“iDcenter”，三菱電機技報，**83**，No.9，559～562（2009）

⑵ 木幡康博，ほか：大規模情報系システムにおける統合ID管理ソリューションの適用，三菱電機技報，**86**，No.7，399～403（2012）

特集論文

サイバー攻撃対策トータルソリューション

辻　宏郷*　　酒巻一紀**
雲田憲太郎**
伊串亮二**

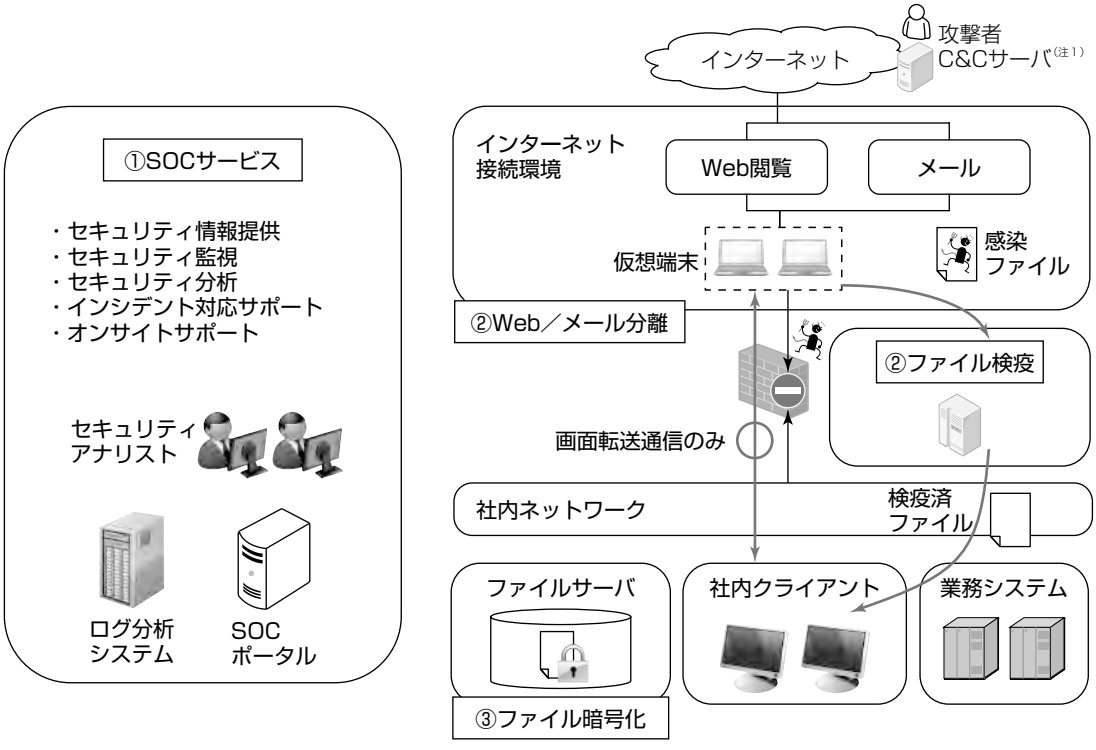
Total Solution to Protect against Cyber Attacks, Targeted Attacks and APT

Hirosato Tsuji, Kentarou Kumota, Ryouji Igushi, Kazunori Sakamaki

要　旨

近年，特定の組織を対象として，知財情報や個人情報等の重要情報の窃取を目的としたサイバー攻撃を仕掛ける標的型攻撃が多発している。これらの攻撃は，従来から施されてきた入口対策だけで防御することは困難であり，“入口対策”を強化するとともに，侵入したマルウェアによる外部との通信や重要情報の持ち出し・閲覧を防止する“出口対策”や，侵入したマルウェアによる内部での活動（情報収集・窃取・破壊等）を早期に検知し，可能であれば活動を阻止する“内部対策”の実施が必要である。

三菱電機インフォメーションシステムズ㈱（MDIS）が提供する“サイバー攻撃対策トータルソリューション”では，セキュリティインシデント発生時の対応組織であるSOC（Security Operation Center）を支援するSOCサービスを提供する。標的型攻撃やAPT（Advanced Persistent Threats）におけるマルウェアの侵入リスク低減と，マルウェアに侵入された場合の活動抑止を目的として，インターネット接続環境（社外Webアクセスや社外とのメール送受信）を社内ネットワークから分離するWeb／メール分離，社外から社内ネットワークに持ち込まれる全てのファイルを検査し，標的型攻撃コードを含むマルウェアを除去してファイルの無害化を行うファイル検疫，マルウェアによって重要情報を含むファイルが持ち出されたとしても，その内容を閲覧・利用不可とするファイル暗号化などを提供し，複数の対策を組み合わせた“多層防御”によって，マルウェアの侵入と活動，情報漏洩（ろうえい）を防止する。



（注1）　C&C(Command & Control)サーバ：標的組織に侵入したマルウェアを遠隔操作するサーバ

サイバー攻撃対策トータルソリューション

特定組織を対象とした情報窃取目的のサイバー攻撃（標的型攻撃）対策として，①インシデント対応組織であるSOCを支援するSOCサービス，②インターネット接続環境を社内ネットワークから分離するWeb／メール分離と社外から社内に持ち込まれる全ファイルの検疫，③重要情報を含むファイルが持ち出されたとしても内容を閲覧・利用不可とするファイル暗号化等，複数の対策を組み合わせた多層防御ソリューションを提供する。

*三菱電機インフォメーションシステムズ㈱（博士（工学））　**同社

1. まえがき

近年，特定の組織を対象として，知財情報や個人情報等の重要情報の窃取を目的としたサイバー攻撃を仕掛ける標的型攻撃が多発している[(1)(2)(3)]。これらの攻撃に対しては，従来サイバー攻撃対策として施されてきた入口対策だけで防御することは困難であり，入口対策の強化に加えて，出口対策や内部対策の導入が必要不可欠である。MDISでは，これらの攻撃から企業を守るトータルソリューションを提供している。

本稿では，サイバー攻撃対策トータルソリューションの全体像及び主要構成要素である①SOCサービス，②Web／メール分離とファイル検疫，③ファイル暗号化について述べる。

2. サイバー攻撃の多様化・高度化

2.1 サイバー攻撃と標的型攻撃，APT

“サイバー攻撃”とは，サイバー空間を介して行われる，コンピュータやネットワークの運用妨害，破壊，乗っ取りやデータの改ざん，窃取を目的とした攻撃である。従来から存在するサイバー攻撃は，主に不特定多数を対象として無差別攻撃を仕掛けるもので，攻撃しやすい公開サーバを狙ったDDoS(Distributed Denial of Service：分散型サービス不能）攻撃やWebサイトの改ざんを試みるものであった。これに対して，2005年頃から，特定の組織を対象とし，重要情報の窃取や破壊を目的として，メールや外部メディア(CD-ROM(Read Only Memory)やUSB(Universal Serial Bus)メモリ等)を介して組織内に侵入する攻撃が試みられるようになった。日本国内では，2011年に大手重機メーカーや国会，官公庁を対象とした情報窃取型のサイバー攻撃が発生し，世間の注目を集めた。このようなサイバー攻撃を，“標的型攻撃”，標的型サイバー攻撃，新しいタイプの攻撃と呼ぶ。また，政府機関や重要インフラを対象とし，長期にわたって繰り返し目的を達成しようと標的型攻撃を試みる攻撃主体やその攻撃を，“APT”と呼ぶ。持続的標的型攻撃，標的型諜報(ちょうほう)攻撃と呼ばれることもある。

2.2 標的型攻撃における攻撃手法

標的型攻撃のうち，情報窃取を目的とした攻撃手法は，事前準備から侵入，情報窃取に至るまでのプロセスがあると分析されており，それぞれの段階で次に示す攻撃手法が試みられる。

(1) 攻撃準備段階

標的の情報を窃取する前の準備段階として，標的組織の情報を事前調査する。そのために，標的の関連組織へ攻撃を行い，初期侵入の基として，組織間でやり取りしたメールなどの情報を収集する。これを利用して，標的組織への初期侵入の成功率を上げる。

(2) 第1段階：初期侵入段階

初期侵入段階では，メールやCD-ROM，USBメモリ等を用いて，標的組織の深部にマルウェアを送り込む。例えば，標的型攻撃メールの場合は，マルウェアを仕込んだ文書ファイルを添付したメールや，マルウェア感染を目的としたWebサイトへのリンクを貼ったメールを送信する。組織内の一人のパソコンを感染させることで目的は達成される。

(3) 第2段階：攻撃基盤構築段階

攻撃対象システムへの侵入に成功した場合，最初に攻撃者が用意しているC&Cサーバとのバックドア(裏口)通信経路を確保する。通常業務で使用しているHTTP(Hyper-Text Transfer Protocol)通信などに偽装して通信を行うため，ファイアウォールなどでの検知・遮断が困難である。このバックドアを用いて，システム内調査に必要な機能や新たなマルウェアのダウンロードを行い，攻撃基盤を構築する。

(4) 第3段階：システム調査段階

攻撃基盤を使用し，重要情報の場所など，システム内情報を捜索する。攻撃者はバックドアを通して侵入したマルウェアと通信を行い，システム情報を確認しながら情報の捜索を継続する。アカウント情報を管理するサーバを乗っ取り，重要情報へのアクセスに必要なユーザーIDやパスワード，管理者権限等の窃取を行う。

(5) 第4段階：攻撃最終目標の遂行段階

目的の情報を窃取し，バックドアから搬出する。入手した情報を基に再度攻撃を仕掛けたり，攻撃対象組織内に構築した攻撃基盤を維持したまま，何度も侵入・情報窃取を繰り返したりする場合もある。

2.3 入口対策の限界

従来型サイバー攻撃への対策としては，マルウェアの侵入を防止する“入口対策”に主眼が置かれていた。しかしながら，標的型攻撃ではゼロデイ(非公開)の脆弱(ぜいじゃく)性を悪用した未知のマルウェアが用いられることがあり，既知のマルウェアだけに対応している従来型アンチウイルスによる検出・侵入防止は困難である。また，初期侵入したマルウェアによる追加機能のダウンロードについても，利用中サービスの正常通信に偽装して行われるため，従来技術では検出できない。したがって，従来型の入口対策だけでは，標的型攻撃を防御不可能であり，新たなサイバー攻撃対策が必要となっている。

3. サイバー攻撃対策トータルソリューション

3.1 標的型攻撃対策の全体像

2章に示した通り，標的型攻撃におけるマルウェアの侵入を完全に防止することは不可能なため，侵入され得ることを前提とした対策が必要である。すなわち，“入口対策”

を強化するとともに，侵入したマルウェアによる外部との通信や重要情報の持ち出し・閲覧を防止する“出口対策”や，侵入したマルウェアによる内部での活動（情報収集・窃取・破壊等）を早期に検知し，可能であれば活動を阻止する“内部対策”の実施が必要である[4]。MDISが提供するサイバー攻撃対策トータルソリューションでは，複数の対策を組み合わせた“多層防御”によって，マルウェアの侵入と活動，情報漏洩を防止する。次節以降で述べる各ソリューションと対策箇所の関係を**表1**に示す。

3.2 SOCサービス

マルウェアの侵入によって，セキュリティインシデント（セキュリティの重大な事故に至る可能性がある出来事）が発生するため，インシデント対応の組織として，SOCやCSIRT（Computer Security Incident Response Team）の組成と効率的運用が必要となってくる[5]。SOCは，セキュリティの運用監視（アラーム受付，ログ分析，機器の設定管理）を担当し，インシデント発見（インシデントとなる可能性のある事象の抽出とCSIRTへの報告，定常状態の把握）の役割を担う。CSIRTはインシデントの対応（影響有無の確認，対処が必要な場合の原因究明や復旧作業）を行う。MDISは，SOCの構築支援及び運用サービス（SOCサービス）を提供する。主要提供機能を，次に示す。

(1) セキュリティ情報提供

ポータルサイトを通して，セキュリティ監視状態や外部団体からのアラート・警告等の情報を提供する（SOCポータル）。SOCポータルの画面例を**図1**に示す。

(2) セキュリティ監視

セキュリティ機器やシステムの監視（稼働監視，パフォーマンス監視，障害監視，検知内容の通知）及び運用（定められた手順に従った設定変更や緊急措置）を行う。主要箇所に設置したセンサからのアラームを受信し，攻撃の兆候を早期に発見する（入口対策，出口対策，内部対策）。

(3) セキュリティ分析

セキュリティ監視対象のログを収集・蓄積し，ログ分析システムを用いて異常とその予兆を抽出し，影響を分析・報告する。インシデント発生時，ログの調査分析を行う。

(4) インシデント対応サポート

インシデント発生時の初動対応，事象調査や復旧措置のアドバイス（対応方法の提示やリモート支援）を行う。

(5) オンサイトサポート

カスタマーエンジニアによるオンサイト情報採取（ウイルス検体採取など），回復支援や調査支援を行う。

表1．主要ソリューションと対策箇所の関係

	入口対策	出口対策	内部対策
SOCサービス	○	○	○
Web／メール分離	○	○	−
ファイル検疫	○	−	−
ファイル暗号化	−	○	○

図1．SOCポータルの画面例

3.3 Web／メール分離とファイル検疫

標的型攻撃におけるマルウェアの侵入リスク低減と，仮にマルウェアに侵入された場合のマルウェアの活動抑止を目的として，次の対策ソリューションを提供する。

(1) Web／メール分離[6]

インターネット接続環境（社外Webアクセスや社外とのメール送受信）は，社内クライアントからはリモートデスクトップとして利用することとし，画面イメージだけを表示する。社内から社外への通信はリモートデスクトップに必要なプロトコルだけを許可し，攻撃の出入口を遮断する。これによって，社内へのマルウェア侵入のリスクを低減する（入口対策）とともに，社内に侵入したマルウェアによる外部のC&Cサーバとの通信，重要情報の持ち出しを防止する（出口対策）。

(2) ファイル検疫

Web／メール分離を実施したとしても，業務上の必要性から，やむを得ずインターネット上のファイルや社外から受信したメールに添付されたファイルを社内ネットワークに持ち込みたい場合がある。このため，インターネット接続環境から社内ネットワークに持ち込まれる全てのファイルを，サンドボックス機能（仮想環境上での実行）などを用いて検査する。標的型攻撃コードを含むマルウェアに感染していた場合，マルウェアを除去するファイル変換機能によって，ファイルの無害化を行う（入口対策）[7]。ファイル検疫システムの内部構成を**図2**に示す。

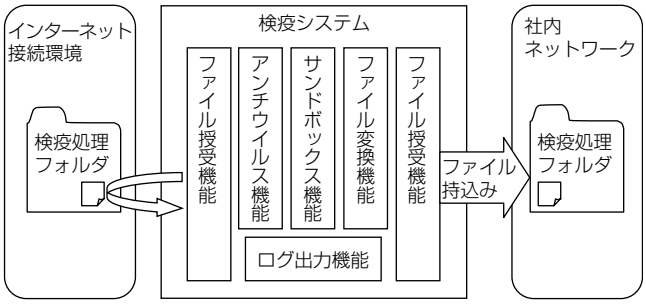


図2．ファイル検疫システムの内部構成

3.4 ファイル暗号化

マルウェアによってファイルが持ち出されたとしても，その内容の閲覧・利用を防止することを目的として，重要情報を含むファイルを暗号化する(出口対策)。ファイル暗号化は，侵入したマルウェアがファイルサーバ上の重要情報を収集し，次段階の攻撃に必要なシステム情報を収集することを防止する効果もある(内部対策)。MDISが提供するファイル暗号化ソリューションは，次に示す特長を備えている。

(1) ファイルサーバ上のファイル自動暗号化

既存のファイルサーバ上の所定のフォルダを暗号化対象フォルダと指定し，該当フォルダに重要情報を含むファイルを収納することによって，ファイルを自動的に暗号化する。暗号化されたファイルは，正規の利用者本人であることを確認した場合だけ，復号して利用可能である。ファイルサーバ上の暗号化フォルダやフォルダ保存によって暗号化されたファイルの例を**図3**に示す[8]。

(2) 関数型暗号を用いたグループ共有情報の暗号化

組織の職制に従って複数の利用者が存在する場合であっても，きめ細かいアクセス(開示)条件を設定して暗号化するために，三菱電機㈱と日本電信電話㈱が共同開発した関数型暗号アルゴリズム[9]を採用している。関数型暗号は，“(所属＝システム部)AND((役職＝部長)OR(役職＝課長))”という条件式を設定してファイルを暗号化し，社員に“所属＝システム部，役職＝部長”等の属性を設定した復号鍵を発行するといったように，条件式を設定した暗号化と復号が可能である。

(3) 復号鍵の集中管理による組織変更への柔軟な対応

人事異動が発生した場合，個人ごとに発行する復号鍵を用いる従来型の公開鍵暗号アルゴリズムでは，暗号化ファイルを一旦復号した後，新しい人員配置に対応した再暗号化が必要になる。これに対して，関数型暗号では暗号化ファイルはそのまま利用可能である。ただし，異動対象者に発行した復号鍵を回収し，新たな属性を設定した復号鍵を再発行・配布する必要があるため，復号鍵をサーバで集中管理し，認証(本人確認)に成功した場合に一時貸与する。これによって，人事異動の際にはサーバ上の復号鍵を更新するだけでよく，組織変更への柔軟な対応が可能となった。

図3．暗号化フォルダと暗号化されたファイルの例

4. むすび

サイバー攻撃，特に標的型攻撃やAPTから企業を守るため，入口対策の強化，出口対策及び内部対策の実施に必要となる施策の全体像及びその主要構成要素について述べた。その他，振る舞い検知型マルウェア対策ソフトウェア，ID・パスワード管理，DLP(Data Loss Prevention：情報漏洩防止)等，有効なサイバー攻撃対策技術が存在する。

今後は，本稿で述べた技術を含む複数の対策技術を最適に組み合わせた“多層防御”によって，サイバー攻撃に対抗するネットワークセキュリティを実現するソリューションを提供していく予定である。

参考文献

(1) (独)情報処理推進機構(IPA)：「新しいタイプの攻撃」の対策に向けた設計・運用ガイド，改訂第2版（2011）
http://www.ipa.go.jp/security/vuln/newattack.html

(2) (独)情報処理推進機構(IPA)：標的型サイバー攻撃の事例分析と対策レポート（2012）
http://www.ipa.go.jp/security/fy23/reports/measures/index.html

(3) (独)情報処理推進機構(IPA)：2012年版10大脅威～変化・増大する脅威！～（2012）
http://www.ipa.go.jp/security/vuln/10threats2012.html

(4) 金融情報システムセンター：金融機関におけるサイバー攻撃への態勢整備について，金融情報システム，平成25年冬号（2013）

(5) 早貸淳子：金融機関に関連するインシデントの動向と対策，組織内CSIRTの機能と役割，金融情報システム，平成25年冬号（2013）

(6) (独)情報処理推進機構(IPA)：情報セキュリティ技術動向調査 タスクグループ報告書（2010年下期）（2011）
http://www.ipa.go.jp/security/fy22/reports/tech1-tg/indexb.html

(7) 田中　覚，ほか：サイバー攻撃の入口対策に関する考察，電子情報通信学会2013年総合大会，D-9-31（2013）

(8) 日経BP社：[ITpro EXPO 2012] 三菱電機，標的型攻撃対応のファイル暗号化システムを参考出展，ITproニュース（2012）
http://itpro.nikkeibp.co.jp/article/NEWS/20121010/428946/

(9) 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，報道発表資料（2010）
http://www.mitsubishielectric.co.jp/news/2010/0728.pdf

特集論文

情報セキュリティを支えるデータ分析フレームワーク“AnalyticMart”

小出健太*
村松祐一郎*

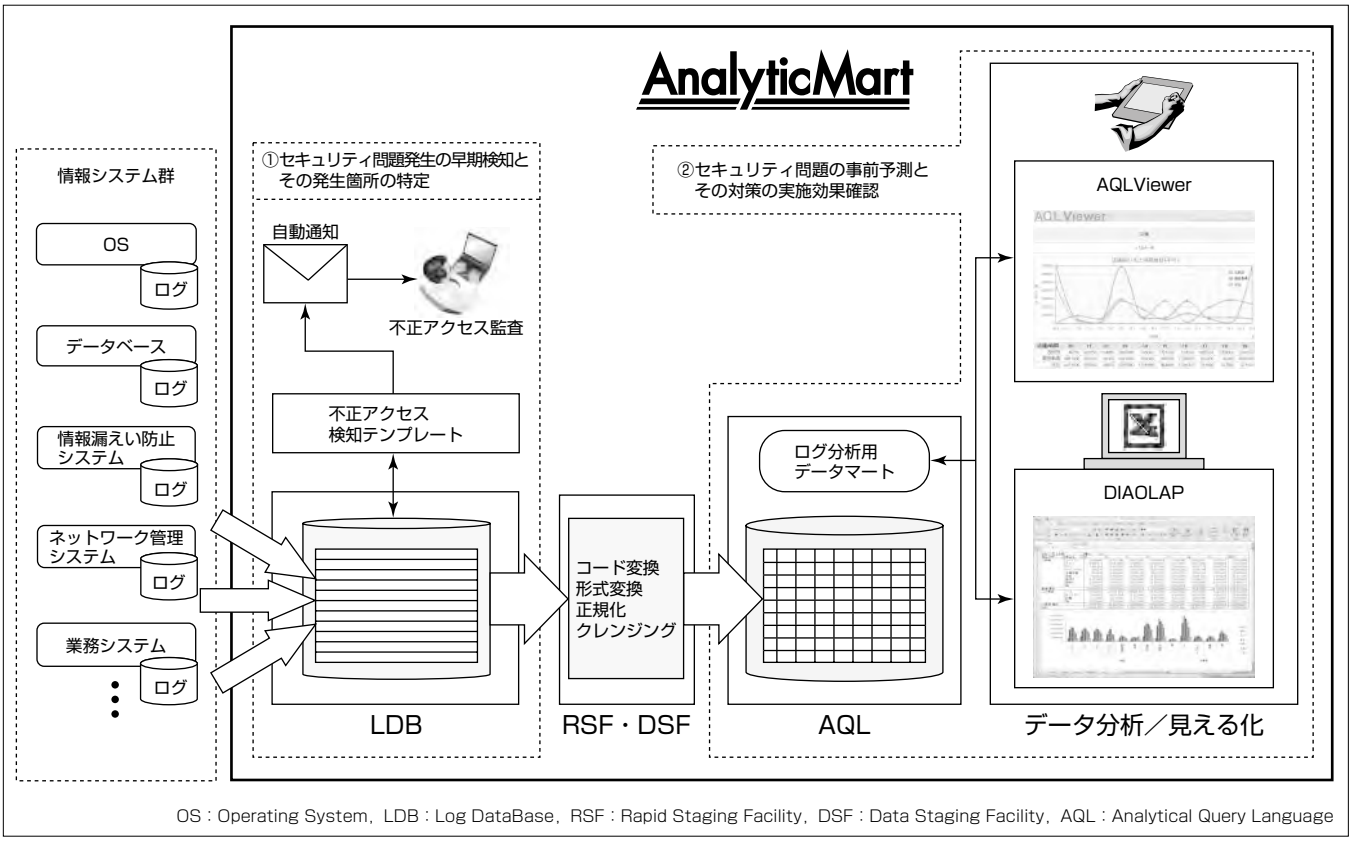
Data Analysis Framework "AnalyticMart" for Foundation of Information Security

Kenta Koide, Yuichiro Muramatsu

要　旨

昨今，内部統制やセキュリティ問題に対応するため，情報セキュリティ対策がますます重要になってきている。情報セキュリティ対策のためにはセキュリティログを十分に監視し活用することが必須であるが，セキュリティ問題発生時の即応性(課題①)や，セキュリティ問題の事前予測と対策(課題②)という複合的なデータの運用が必要であり，セキュリティログを十分に活かしきれていないという問題があった。これに対して，三菱電機インフォメーションテクノロジー㈱(MDIT)ではデータ分析フレームワーク“AnalyticMart”を発表し，これらデータ活用の課題への対応を図っている。

“AnalyticMart”では，課題①の“セキュリティ問題発生の早期検知とその発生箇所の特定”のために，ログデータベース“LDB”への多様なセキュリティログの蓄積と不正アクセス検知テンプレートによる自動的なセキュリティログの監視機能を提供している。また，課題②の“セキュリティ問題の事前予測とその対策の実施効果確認”のためには，情報分析ツール“DIAOLAP”による高度な非定型分析と，分析・表示ツール“AQLViewer”による簡易な操作による定型分析と見える化の機能を提供している。特にAQLViewerはノートパソコンよりも携帯性の高いタブレット端末に対応することで，多種多様な情報セキュリティ対策の現場での活用を実現している。



OS：Operating System，LDB：Log DataBase，RSF：Rapid Staging Facility，DSF：Data Staging Facility，AQL：Analytical Query Language

“AnalyticMart”の機能構成

各情報システムから集められたログ情報はLDBに集積され，同時にRSF・DSFによってデータ化されてAQLに蓄積される。LDBへの蓄積情報は蓄積タイミングでの自動的に監視対象となり，AQLへの蓄積データは分析に使用される。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

セキュリティ分野におけるデータ活用は，セキュリティ事故による企業価値の毀損を防ぐためや，内部統制等の外的要因によって，欠かせないものとなっている。これら内部統制におけるITでの対応としては，各情報システムから出力されるアクセス・操作・メール等の履歴や，情報漏えいや誤送信といった事件が発生した場合の追跡，ヒヤリハットによって，事件発生のリスクが高い箇所を特定し，事前対策を取ることが必要となる。しかし，情報セキュリティ分野のデータ，特に中心となるセキュリティログは多種多様に存在する上，日常的に増え続ける性質があり，取りこぼしが許されないものであることから，管理コストが高く，多様な分析を行う必要があるといった問題が存在し，重要度に比して導入難度が高く，敬遠されがちであった。

MDITでは，データ活用を包括的に支援する，データ分析フレームワークAnalyticMartを提供している。このAnalyticMartを用いることで，セキュリティ分野におけるデータ活用の問題点を解決することができる。

本稿ではセキュリティデータ活用として，データ分析／見える化を容易に実現するDIAOLAP及びAQLViewerを中心にAnalyticMartの特長と機能について述べる。

2. AnalyticMart

2.1 AnalyticMartとは

AnalyticMartは，販売分析，顧客分析，ログ分析，環境データ分析といった多様で形式の異なるデータの分析を，統一したアーキテクチャで効率よく低コストで実現でき，かつ中小規模から大規模まで，規模に合わせたデータ分析システムの構築・運用を可能とするフレームワークである。

2.2 AnalyticMartの特長

⑴ 多様なデータの分析・蓄積に対応するデータベース

AnalyticMartは，高速処理技術[1]が組み込まれた2つのデータベース“LDB”“AQL”によって，プロセッサ数に応じたスケーラビリティの高いシステムを提供している。同時に，データベース間をつなぐETL(Extract，Transform，Load)ツールを組み合わせることによって，販売／経理データに代表される構造化データから，システムへのアクセスログのような非構造化データまで様々なデータの分析を実現している。

①LDB

LDBは，非構造化データを蓄積するのに最適なDBMS(DataBase Management System)であり，テラバイト超の大規模ログにも対応可能な高速蓄積と正規表現指定による高速検索機能を持つコンポーネントである。

②AQL

AQLは，データ分析プラットホームとして10年以上の実績を持つ高性能DBMSであり，集計・分析に適した構造化データの保存と，高速なデータ検索・集計が可能なコンポーネントである。

③ETLツール

AnalyticMartでは2つのETLツール“RSF”と“DSF”を提供している。RSFは，企業内に存在する様々なログデータを収集・加工する高機能ETLツールである。DSFは加工済みデータに対して，高速にソート，JOIN(列の結合)を行う簡易ツールとして用意されている。

⑵ 短期間の構築ですぐに使えるシステム

親しみやすく簡単に扱えるBI(Business Intelligence)ツール(DIAOLAP，AQLViewer)や，目的別の各種テンプレートによって，短期間の構築で運用できるシステムを提供している。

①DIAOLAP

AQLのヘビーユース向け分析用フロントエンドである。詳細は**3. 2. 1項**で述べる。

②AQLViewer

AQLのライトユース向け分析用フロントエンドである。詳細は**3. 2. 2項**で述べる。

③各種テンプレート

近年求められるログへの即時対応をサポートする。主に以下の4種を用意している。

・不正アクセス検知テンプレート
・ISMS(Information Security Management System)テンプレート
・環境データ見える化テンプレート
・情報漏えい対策テンプレート

⑶ スモールスタート可能性と拡張性

AnalyticMartは柔軟なコンポーネント構成とすることができ，要旨の図に示すAnalyticMartの機能構成で，LDB周辺までを含めてデータの蓄積のみのスモールスタートから始め，ETLツールやAQLを駆使しての，様々なデータの統合分析へ徐々に構成を拡張させることも可能である。

3. AnalyticMartを使ったセキュリティ対策

この章では，AnalyticMartを使ってセキュリティ対策を行うにあたってのセキュリティの問題を改めて整理し，AnalyticMartでの解決策(対応機能)及び，セキュリティ対策の実際の運用について述べる。

セキュリティ分野について，データを使って捉えるべき課題は大きく分けて次の2つがある。

⑴ セキュリティ問題発生の早期検知とその発生箇所の特定
⑵ セキュリティ問題の事前予測とその対策の実施効果確認

3.1 セキュリティ問題発生時の早期検知とその発生箇所の特定

セキュリティ問題の発生は，できる限りの早期検知と発生箇所の確実な特定が必要となる。セキュリティログの日

常的な監視は問題の発生有無確認につながり，蓄積は問題が発覚した後の追跡のために必須である。AnalyticMartではこれらの対策のため，LDB及び不正アクセス検知テンプレートを提供している[2]。LDBにはセキュリティにかかわるログを全て蓄積することができる。LDBへ日常的に蓄積されるログに対して，不正アクセス検知テンプレートは，“ログイン失敗が短時間に何度も発生している”“深夜に機密ファイルへ定期的なアクセスが行われている”といった，不正アクセスが疑われるログを自動的に発見し，ユーザーへメール通知する機能を備えている。これによって，問題発生の迅速な検知が実現される。この通知メールには発生したログそのものの情報も記載されており，LDBにアクセスすることで実データやその周辺データに関して追跡調査を行うことができ，問題発生箇所を特定することが可能となる。

3.2 セキュリティ問題の事前予測とその対策の実施効果確認

セキュリティ問題は発生してしまうと社会的信用の失墜につながってしまうため，問題を未然に防ぐことが重要になる。セキュリティ問題を未然に防ぐためには，セキュリティログの分析による問題発生要因や危険な箇所の予測・特定とそれらへの対策実施・実施効果確認が必要になる。同時に，セキュリティの現場は多岐にわたるため，得られたセキュリティについての知見をどのような現場でも見える化できる工夫が必要になる。AnalyticMartでは，DIAOLAPとAQLViewerという2つのツールによってセキュリティログの分析と見える化を実現している。これら2つのツールはともに分析と見える化を行うAnalytic Martのフロントエンドである。両者にはAQLのヘビーユース向け(DIAOLAP)と，ライトユース向け(AQLViewer)という用途の違いがあり，セキュリティログに対して，知見を得るための非定型分析はDIAOLAPによって行い，得られた知見の展開や各種の現場での情報セキュリティデータ活用ではAQLViewerを活用するといった用途による使い分けを想定している。

3.2.1 DIAOLAP

DIAOLAPはAQLのヘビーユース向けとして，セキュリティログを情報システムセキュリティの部門が詳しく分析を行うような用途に向いている。その特長を次に述べる。

(1) インタフェースにExcel(注1)を採用

Excelのアドオンツールとして提供しており，使い慣れたExcelからシームレスに利用できる。セキュリティログを時間帯別，ユーザー別，操作種別，対象別に，アクセス回数や失敗回数で集計(ピボットテーブル)し，グラフで表示するといった手間のかかる処理の自動化をサポートしている。

(2) 高度な非定型分析と表示ウイザードの提供

柔軟な呼び出し形態とExcelの分析機能による高度な非定型分析を実現している。データ呼出し条件の設定には，ウイザードで時間や場所といった変数を指定していく形式を採用し，容易な操作を提供している。これによって，多様な環境に潜在するセキュリティリスクを簡単な操作で洗い出していくことができる。

(3) ドリルスルー機能の提供

作成した集計表からセキュリティリスクやその予兆を発見したときに，ドリルスルー機能によって，その原因となる明細のデータにさかのぼって表示することができる。これによって，絞り込んだデータの実体であるセキュリティログを確認し，問題発生の前後に何が起こっているのかなどの確認が容易にできるようになる。

(注1) Excelは，Microsoft Corp. の登録商標である。

3.2.2 AQLViewer

AQLViewerはAQLのライトユース向けとして，セキュリティログの分析結果を，情報セキュリティにかかわる各現場で手軽に素早く提示することや，現場の情報システムやセキュリティに精通していないユーザーが分析結果を閲覧するような用途に向いている。AQLViewerは，DIAOLAPの提供する機能をライトユース向けにスリム化しつつ，同等レベルの分析能力を維持している(**図1**)。その特長を次に述べる。

(1) Webブラウザでの表示

クライアントの表示は標準のWebブラウザだけで実行可能としている。これによって，この機能はライセンスフリーで展開することができ，セキュリティ対策のコスト低減や，多数のライトユーザーへ定型の分析結果を展開したい場合，分析結果閲覧のためにインストールするソフトウェアの費用を低減できるといった効果がある。

(2) 容易なインタフェース

図2にあるように，DIAOLAPでは分析結果としてグラフを得るまでの操作に，ログインからグラフ表示操作まで含めて8ステップの作業が必須であった。AQLViewerでは，これらステップを整理して細かな設定を行う6ステップをサーバ側であらかじめ事前定義情報として作成して保存しておくことでクライアント側での作業量を低減し，4ステップでのグラフ表示を実現した。クライアントから閲覧する際は，定型となる事前定義情報の選択と，データ絞

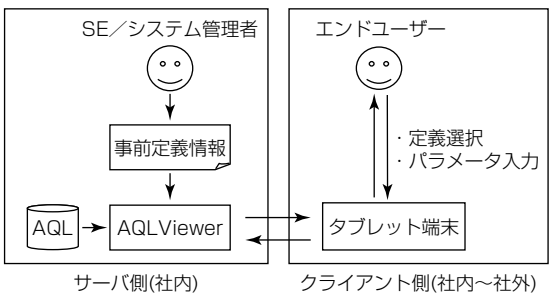


図1．AQLViewerの構成

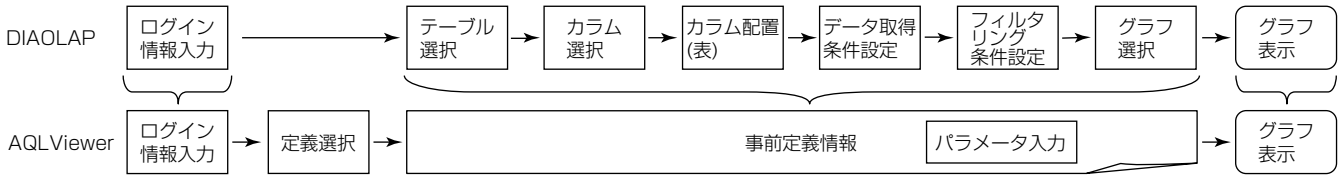


図2．DIAOLAPからAQLViewerへの操作削減

り込みパラメータの設定(年月日での範囲絞り込みや，特定サーバ／ファイルへのアクセス，特権ユーザーの指定等)を実施するだけでグラフが表示される。これらのパラメータ設定内容は事前定義情報内で全て決定されるため，パラメータ指定が必要なければ，定義の選択のみでグラフが表示されることになる。また，クライアント側では定型の表示のみとなって自由度が下がることになるが，サーバ側の事前定義情報にはクエリの自由記述や4種のグラフ表示の選択といった設定が可能であり，AQLViewer全体としてはDIAOLAPに近い表示の自由度を確保している。

(3) タブレット端末への対応

近頃利用され始めた，ノートパソコンより携帯性に優れたタブレット端末に対応している。これによって，ノートパソコンでも手狭な場所での操作や，移動先での突然の閲覧，早急に分析結果を出さなければならない場合など，多くの場面で蓄積・分析した情報セキュリティのデータを活用することができる。また，指先での操作や視認性の悪い場所での操作に対応して，大型ボタンの配置や押すべきボタンの配色を目立たせるといった工夫を行い，タブレットの特性を活用するユーザーインタフェースとしている。

3.3 AnalyticMartを用いたセキュリティ対策の運用

ここまで，AnalyticMartによるセキュリティ分野のデータに対するアプローチを述べてきた。最後に，実際にAnalyticMartを用いたセキュリティ対策を運用する際のデータの流れとその効果を，**図3**に沿って述べる。

最初に，各情報システムからセキュリティのデータを取り出すため，ISMSテンプレートを用いて自動的にセキュリティログをLDBへ蓄積するシステムを構築する。蓄積されるセキュリティログは不正アクセス検知テンプレートによって常に監視され，問題があればユーザーへ即座にメール通知される。問題発生後に，問題となったログそのものを確認したい場合も，通知メールの内容からLDBの該当ログをスムーズに表示し，詳細を確認することができる。問題が発生しない日常では，LDBに蓄積されたデータはRSF・DSFによって分析用に整理され，AQLに保存される。これによってログの高速な分析システムが整う。ユーザーは非定型のログ分析をDIAOLAPによって行い，セキュリティの脆弱(ぜいじゃく)性が存在していないかを確認する。確認したログについて問題があれば，ドリルスルーによってより生のデータに近いものを確認し，不正アクセス検知テンプレートへの監視事項追加や，その他の対策へつなげることができる。既知となっているセキュリティ状況の指標についてはAQLViewerで定型化しておき，タイムリーに見える化したデータを入手できる。特に，セキュリティがかかわる場面は幅広いため，監査のサイトツアーでの実データ提示や，サーバラック裏などの手狭な場所での閲覧，データの説明時にデータを手元から示すといった様々な状況が想定される。そのため，セキュリティ分野のデータ活用でタブレット端末に対応したAQLViewerは有用なツールである。

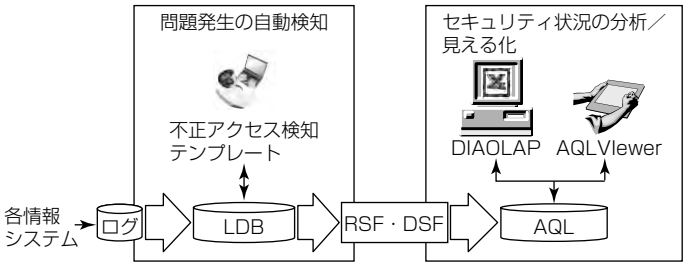


図3．AnalyticMartでのセキュリティ対策の流れ

4. むすび

多種多様なデータの分析基盤となるAnalyticMartのセキュリティ分野への適用と，その効果について述べた。本稿では主に，分析と見える化を行うフロントエンドツールについて述べ，用途に沿って使い分けるツールを提供していること，またそれぞれのツールの特長について述べた。

AnalyticMartを用いることで，セキュリティ問題発生の早期検知とその発生箇所の特定，及びセキュリティ問題の事前予測とその対策の実施効果確認が可能となる。今後は使い勝手の向上や使用環境の拡充を進め，より多くの場面で活躍できるプラットホームにしていく予定である。

参考文献

(1) 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）
(2) 和田貴成，ほか：統合ログ管理ソリューション“AnalyticMart for LogAuditor”，三菱電機技報，**86**，No.7，391～394（2012）

特集論文

最新モデル“ネカ録4.0”の機能強化

中野卓朗*

Functional Enhancement of Latest Model "NECAROKU 4.0"

Takuro Nakano

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。三菱電機㈱の“MELOOK-DGシリーズ”を始めとするマルチベンダーのカメラサポート，大容量HDD(Hard Disk Drive)による長期間録画，録画サーバ上で映像の展開と比較を行う動体検知等，他社を差別化する機能を備えている。しかし，近年，監視カメラシステムでは，JPEG(Joint Photographic Experts Group)と比較して，2～10倍の圧縮率がある動画圧縮技術H.264/AVC(Advanced Video Coding)のサポートが進んでおり，同じHDD容量でも長期間録画が可能になってきているため，従来のネカ録が持つ長期間録画機能という優位性が失われつつあった。この背景の下，“ネカ録4.0”では，従来のネカ録とH.264/AVCの特長を生かした次の機能強化を実施した。

(1)　新カメラサポート

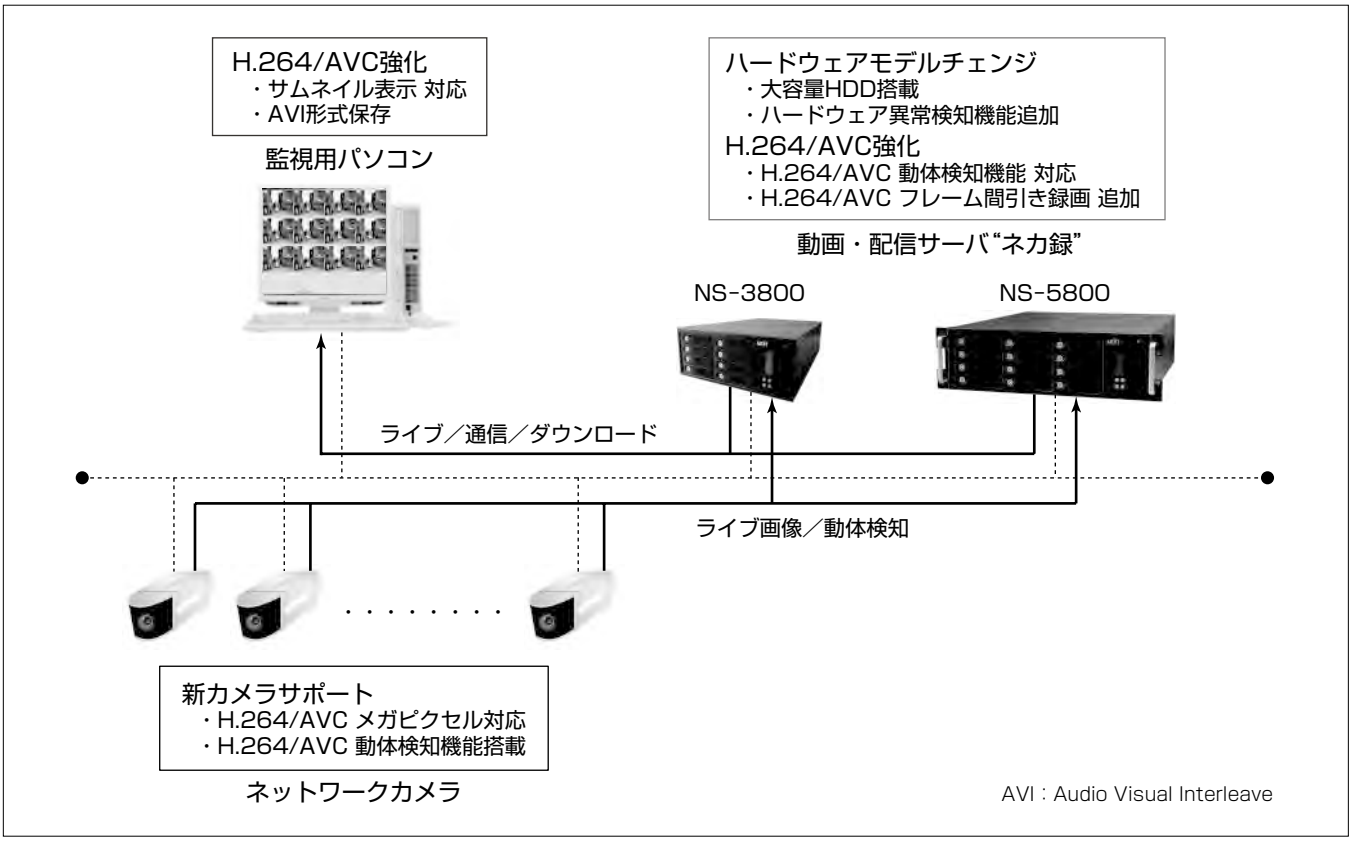
H.264/AVC高圧縮を生かし，メガピクセル(100万画素以上の解像度)で撮影可能な新しいカメラに対応

(2)　ハードウェアのモデルチェンジ

長期間，複数のカメラ画像を安心して保管できる大容量HDDの搭載。ファン異常・電源縮退・温度異常等のハードウェア異常検知機能による信頼性の確保

(3)　H.264/AVCの機能強化

動体検知，フレームの間引き録画等，JPEGでだけ実現していた機能をH.264/AVCに対しても実現



“ネカ録4.0”の機能強化ポイント

ネカ録4.0では，H.264/AVCに対応したメガピクセルや動体検知機能を持つ新しいネットワークカメラ(左下)をサポートした。また，大容量HDD，ハードウェア異常検知機能を完備したネカ録ハードウェア(右上)に一新した。ソフトウェアとしてH.264/AVCの動体検知，フレーム間引き録画機能に対応し，監視用パソコン(左上)で動作する監視ツールでは，ダウンロードしたH.264/AVC録画映像に対するサムネイル表示などの機能強化を行った。

*三菱電機インフォメーションテクノロジー㈱

1. まえがき

ネカ録は，大容量HDD，RAID(Redundant Arrays of Inexpensive Disks)ホットスワップ対応を特長として，機密性が高く高品質な映像の長期間録画が求められる金融，工場，データセンター分野等の大中規模企業をターゲットとしている。アナログカメラからネットワークカメラ化への急速な変化期の中で，ネットワークの市場動向に目を向け，新たな技術を取り入れていくことで，ネットワークカメラ市場だけでなく，セキュリティの強化を必要とする新たな市場でも活用可能な付加価値の創造を目指している。

最新モデル“ネカ録4.0”では，ネカ録ハードウェアを一新し，ディスク容量を増加，新カメラをサポート，高圧縮率動画形式H.264/AVCの録画方法を拡張(動体検知，フレームの間引き)等の機能強化を図った。

本稿では，ネカ録4.0の最新機能について述べる。

2. 市場動向とネカ録の方向性

2.1 市場動向

ネットワークカメラによる監視システムは，IP(Internet Protocol)ネット利用での設置性が高く，画質も良く，遠隔監視が容易で操作性に優れており，2013年にはIP系がアナログ系を追い越すと予想されている。また，2010年から需要が回復してきており，**図1**に示す通り，ネットワークレコーダ市場は2011年から年率20%以上の伸長率で，ネットワークカメラ市場も今後，年率10%以上の伸びが予想されている[1]。

カメラに関しては，各カメラメーカーとも，2011年から，H.264/AVCサポートが進んできている。近年では，メガピクセルでH.264/AVC対応のカメラが発売され，H.264/AVCに対応したカメラのラインアップが充実してきている。また，ネカ録の競合製品にあたる各社レコーダも，これに対応してきている。

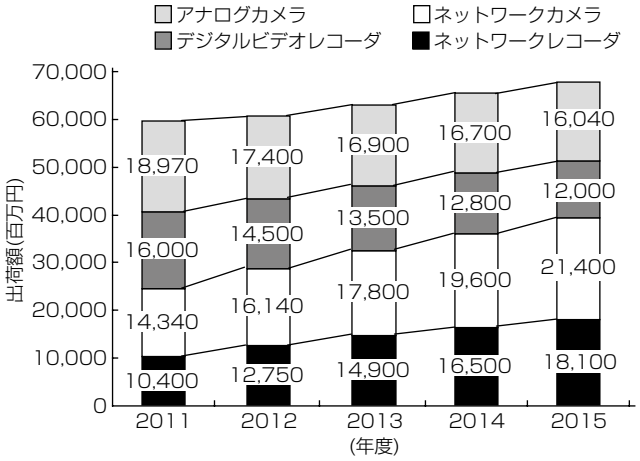


図1．監視カメラと録画装置の出荷金額推移[1]

2.2 ネカ録に求められていること

市場動向から，ネカ録では，新ネットワークカメラの迅速なサポート，H.264/AVCに対する機能強化が求められている。また，ネカ録は，金融，工場，データセンター分野等の大中規模企業をターゲットとしており，このような分野では，セキュリティを強化するために，カメラ台数が増加する傾向にある。さらに，高精細かつ滑らかな映像を長期間保存できることが要求される。すなわち，高品質でかつ長期間の映像データを蓄えられるだけの十分な記憶容量の確保が必要になってきている。

2.3 ネカ録の方向性

ネカ録は，ネットワークカメラ市場だけでなく，セキュリティ向上を必要とする新たな市場のシステムに対しても連携可能となる製品を目指している。そのためには，市場動向に目を向け，セキュリティに関して魅力ある製品にしていく必要があり，**2.1節**の最新の市場や技術動向，ネカ録の適用範囲も考慮すると次の機能強化が求められている。

(1) 新ネットワークカメラのサポート
(2) 十分な記憶容量の確保
(3) H.264/AVCに対する機能強化

ネカ録は，これらの背景の下，最新技術に対する機能強化を行い魅力ある製品の商品化を進めている。

3. ネカ録の機能強化

この章では，最新モデル“ネカ録4.0”で機能強化した内容について述べる。

3.1 新ネットワークカメラのサポート

2章で述べたように，ネカ録には，H.264/AVCに対応した新しいネットワークカメラの迅速なサポート，対応機種の拡大が求められている。これに対して，ネカ録4.0では，次のH.264/AVCに対応したカメラを新規にサポートした。

(1) 三菱電機

コンパクトボディの“NC-6400”と360度旋回監視可能な“NC-6500”に対応

(2) SONY

従来では，JPEG画像にしか対応していなかったがH.264の映像にも対応

(3) AXIS

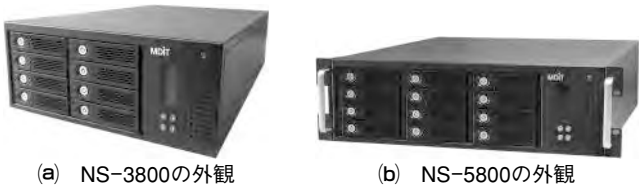
全方位カメラ“M3007”に対応

また，これらのカメラは，高精細な画像を撮影できるメガピクセルに対応している。メガピクセルに対応したネットワークカメラは，人物の表情，車のナンバー，受け渡した資料，紙幣の種類等を明瞭に捉えることが可能である。

このような新しいネットワークカメラのサポートを図ることで，**表1**に示すようなH.264/AVC映像で高品質な映像の保管を可能にするカメラレパートリーを増やすことができた。

表1．ネカ録4.0でサポートしているH.264/AVCとメガピクセルに対応したネットワークカメラ一覧

メーカー名	機種名
三菱電機	NC-6100，NC-6400，NC-6500，NC-6700，NC-8000（X-8000経由），NC-8600（X-8000経由）
SONY	SNC-DH260C，SNC-DH280，SNC-ER580，SNT-EX104
AXIS	P1353，P1346，P1347，P3346，M3007
Panasonic	DG-SW355，DG-SP304V，DG-SP305
Canon	VB-M40，VB-M600VE
サンヨー	VCC-HD2500，VDD-HD3300



(a) NS-3800の外観　(b) NS-5800の外観

図2．ネカ録新製品

3.2 ネカ録ハードウェアを一新

ネカ録4.0では，ラックマウント型の上位機（NS-5800），デスクトップ型の中位機（NS-3800） 2機種を新機種としてフルモデルチェンジを行った（**図2**）。下位機（NS-1800）も順次，モデルチェンジしていく予定である。

次にモデルチェンジの特長を述べる。

3.2.1 ネカ録4.0で追加された特長

(1) 大容量HDD

近年，拠点あたりのカメラ台数の増加，保存期間の長期化，メガピクセルカメラへの対応等によって，必要な記憶容量及び録画性能は確実に増大している。そのため，フルモデルチェンジしたネカ録4.0では，HDD容量の拡張を図った。上位機種の“NS-5800”では最大36TBの大容量HDDを内蔵し，従来機のNS-5700と比較して，約1.5倍の記憶容量とした（**表2**）。また，中位機種のNS-3800では，従来機の“NS-3500”と比較して約3倍とした（**表3**）。これによって，メガピクセルの映像データの長期間の録画に対しても，余裕を持って対応できるようになった。

(2) ハードウェア異常検知の強化

さらに，ハードウェア異常検知についても機能強化を図った。従来機で対応していなかった“RAID縮退通知”“ファン異常通知”“電源縮退通知”“メモリ異常通知”“温度異常通知”といったハードウェア異常検知機能を強化した。これによって，ハードウェア障害発生を迅速に認識でき，深刻な問題に発展する前に，原因の追究や対策を施すことが可能になった。

(3) ハードウェアセキュリティ強化による漏洩（ろうえい）リスクの低減

ネカ録4.0の外装には，従来サポートされていなかったHDD単位でのロック機構がついており，管理者が所持している鍵がないと抜き差しできないようになっている。これによって，漏洩リスクの低減を図っている。

表2．上位機−新機種（NS−5800）と従来機種（NS−5700）の比較

	NS-5800	NS-5700
HDD構成	3.5インチHDD 12Bay	3.5インチHDD 12Bay
搭載容量	3TB×12（36TB：最大） 2TB×12（24TB）	2TB×12（24TB：最大） 2TB×8（16TB） 1TB×8（8TB）
冗長機能	RAID6	RAID5／6（いずれかを選択）
セキュリティ	ロック機構搭載	未搭載

表3．中位機−新機種（NS−3800）と従来機種（NS−3500）の比較

	NS-3800	NS-3500
HDD構成	3.5インチHDD 8Bay	3.5インチHDD 4Bay
搭載容量	3TB×8（24TB：最大） 2TB×8（16TB） 2TB×4（8TB） 1TB×4（4TB）	2TB×4（8TB：最大） 1TB×4（4TB） 500GB×4（2TB） 500GB×2（1TB）
冗長機能	8台構成はRAID6 4台構成はRAID5	RAID5／6（いずれかを選択） （500GB×2はRAID1）
セキュリティ	ロック機構搭載	未搭載

3.2.2 従来のネカ録から引き継いだ特長

(1) 冗長構成

大容量HDDサポートに伴い，HDD故障などでデータを失った時のリスクが高まってしまうという課題が残る。これに対しては，ネカ録4.0でも，従来機と同様に，2台のHDDが同時に故障しても連続運転・復旧可能なRAID6をサポートし，信頼性・可用性の向上を図った。また，復旧時では，ホットスワップ型で，システムを停止することなしにHDDを入れ替えることができる。これによって，大容量でかつ安心して利用できるHDDの提供が可能になった。

3.3 H.264/AVC 機能強化

ネカ録4.0では，次世代動画圧縮技術H.264/AVCに対応したカメラをサポートしており，カメラから送信されるH.264/AVC画像の直接録画とライブ表示・再生が可能である。H.264/AVCは，JPEGと比較して圧縮効率が非常に高いため，同じHDD容量で2～10倍の長期間録画が可能である。各ネットワークカメラメーカーのH.264/AVCサポートが進む中，今後の主流はH.264/AVC機能となることが考えられるため，ネカ録4.0では，H.264/AVCに対する次の機能を新たに追加した。

(1) H.264/AVC動体検知

動体検知とは，ライブ映像を配信するとともに，現在の映像と1フレーム前の映像を比較して動きに違いがないかを検知するための機能である。H.264/AVCの映像に対するこの機能を実現することで，H.264/AVCの映像でも，動体検知をトリガーにした“録画・通知・プリセット位置の移動”等の従来のネカ録が持っている機能と連動することが可能になる。

従来のネカ録では，ネカ録の中で，H.264/AVCの動体検知を行うためには，正確な画像差異を計測する必要があり，H.264/AVC形式の映像データを，BMP（BitMap）形式

表 4．ネカ録のH.264/AVC動体検知への対応カメラサポート状況

メーカー名	機種名
三菱電機	NC-6100，NC-6700
AXIS	M1054，M1114，M3203，M5014，P1347，P3346，P5534等
Canon	VB-M40，VM-M600VE

などの可逆圧縮の画像形式に変換する必要があった。この変換は，ネカ録のCPUに大きな負荷がかかるため，これまで実現することができなかった。しかし，近年，各カメラメーカーでH.264/AVCが主流になり，H.264/AVC機能も充実してきており，ネットワークカメラの中に動体検知の機能を持つカメラも発表されてきた。

そこで，ネカ録4.0では，ネットワークカメラが持つ動体検知機能と連動することによって，H.264/AVCに対する動体検知をトリガーにした“録画・通知・プリセット位置の移動”等の機能を実現した。現在，“ネカ録4.0”では，**表 4** に示すネットワークカメラでこれらの機能を利用することが可能となっている。

⑵ H.264/AVC フレームの間引き録画

間引き録画とは，ライブ表示される全ての映像データを録画するのではなく，指定の間隔で，一部の映像だけを録画する機能である。この機能は，ライブ映像は滑らかに表示したいが，一定の間隔で一部の映像が録画されていれば良いという状況で利用される。これは，長期録画の要求に対して有効な録画機能である。従来のネカ録ではJPEGだけサポートしており，H.264/AVCでは利用できなかったが，ネカ録4.0では，H.264/AVC映像の間引き録画に対応した。

H.264/AVCはJPEGと異なり，複数の連続する画像をグループとして管理するGOP(グループ・オブ・ピクチャー)方式でデータが管理されている。ネカ録で利用されるGOPは，IフレームとPフレームから構成され，GOPの基準となるデータをIフレーム，そして，直前のフレームとの差分をPフレームと呼んでいる。Pフレームは差分データであるので，IフレームにPフレームを重ねることで１つのフレームとなる。つまり，Pフレームを絡めることでIフレームだけ並べた映像より，映像データを軽量化できる映像圧縮方式である。この特長を踏まえて，ネカ録4.0では，Iフレームだけを保存し，Pフレームを間引くといった録画方法で，H.264/AVCの間引き録画を実現した。これによって，H.264/AVCでもディスクの使用量を抑えることができ，より長期の録画にも対応できるようになった。

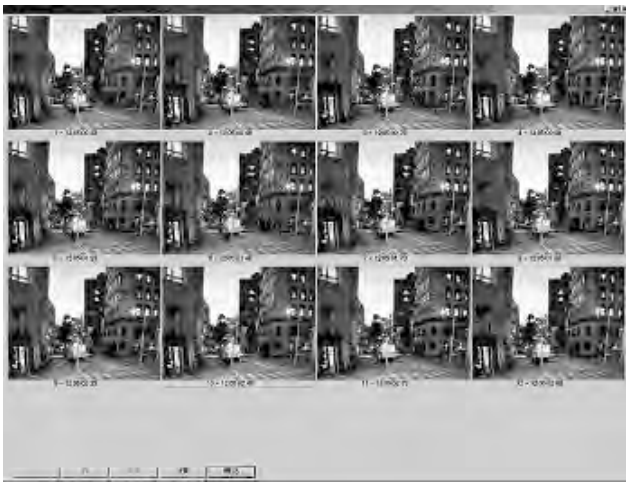


図 3．サムネイル表示

⑶ H.264/AVCダウンロード再生機能の拡張

ネカ録では，録画を中断することなしに日時を指定してパソコンなどへ録画データをダウンロードすることが可能である。ダウンロードしたデータは独自のプレーヤーで再生／コマ送り表示することができる。このプレーヤーには，ダウンロードした録画データを一覧表示するサムネイル機能（**図 3**）があるが，従来JPEGでだけ対応されておりH.264/AVCではサポートされていなかった。ネカ録4.0では，この機能をサポートすることで，コマ送りで１枚ずつ画像を確認する場合と比較して，ユーザーの視認スピードが高まり，ユーザビリティを向上させることができた。

また，H.264/AVC形式のダウンロードデータに対しても，AVI形式に変換する機能を追加し，ネカ録独自のプレーヤーを使わずに再生することも可能になった。

4. むすび

最新モデル“ネカ録4.0”では，ネカ録ハードウェアを一新し，ディスク容量を増加，新カメラのサポート，高圧縮率動画形式H.264/AVCの録画方法を拡張(動体検知，フレームの間引き)等の機能強化を図った。これらの付加価値を基に，三菱電機製品との連携を強化していくことで，新たな市場の開拓を目指していきたい。今後も，付加価値の創造に努め，ネカ録の機能充実を図っていく所存である。

参考文献

⑴ 2012 セキュリティ関連市場の将来展望，㈱富士経済（2012）

特集論文

三菱電機アプリケーション構築フレームワーク“DIAECOR”

鈴木和行* 秋間孝道*
山本孝史*
小坂一樹*

MITSUBISHI ELECTRIC Application Solution Framework "DIAECOR"

Kazuyuki Suzuki, Takashi Yamamoto, Kazuki Kosaka, Takamichi Akima

要 旨

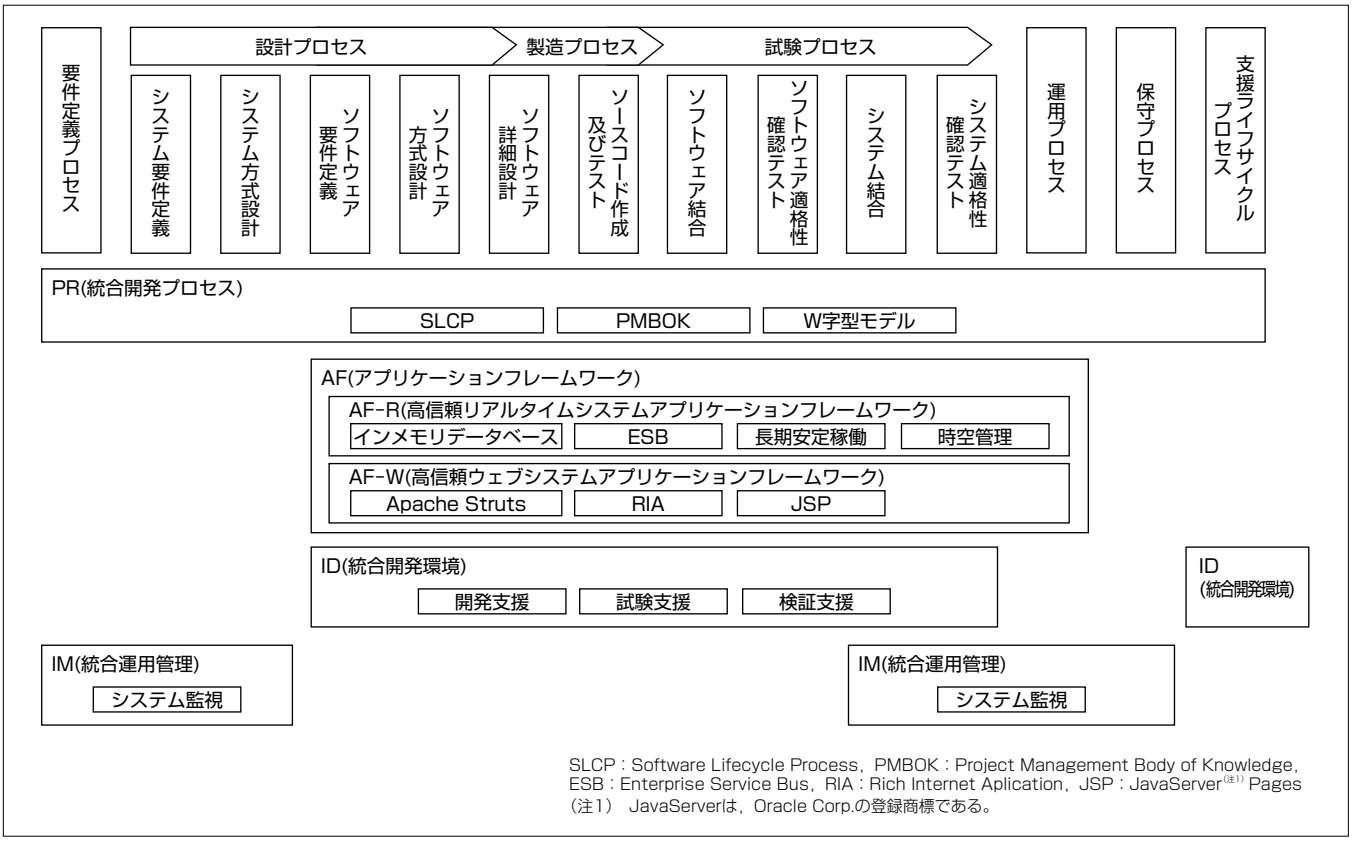
三菱電機アプリケーション構築フレームワーク“DIAECOR（ダイヤエコール）”は，社会インフラを支える“高信頼・高品質”な情報システムを実現するための統合フレームワークである。

国際標準のSLCP-JCF2007（Software Lifecycle Process-Japan Common Frame 2007）(1)に対応可能な開発プロセスと，高信頼な分散処理型アーキテクチャを実現する実行モジュールによって，24時間365日稼働し続ける高品質なミッション・クリティカルな情報システム（無停止社会インフラ情報システム）を構築可能にしている。

三菱電機は，長期にわたり“高信頼・高品質”を必要とされるミッション・クリティカルな情報システムを構築し続けてきており，そこで得られた様々な課題に対する解決策を“DIAECOR”に集約して製品化した。

DIAECORは，ウェブ系システム，及び，リアルタイム系システムに対応することが可能であり，それらを効率的に開発するため円滑な開発プロセスを提供する“PR：統合開発プロセス”，アプリケーション構築の基盤を提供する“AF：アプリケーションフレームワーク”，開発の自動化を支援する“ID：統合開発環境”，そして，高度なシステム運用を実現する“IM：統合運用管理”の4つの製品群を提供している。

本稿では，それぞれの製品群について，開発の背景や特長について述べる。



三菱電機アプリケーション構築フレームワーク“DIAECOR”の構成

“DIAECOR”は“PR：統合開発プロセス”“AF：アプリケーションフレームワーク”“ID：統合開発環境”“IM：統合運用管理”から構成され，SLCP-JCF2007の開発プロセスに対応可能な製品群となっている。

*インフォメーションシステム事業推進本部

1. まえがき

社会インフラを担う情報システムは，24時間365日停止することなく稼働し続けるために，高信頼・高品質なソフトウェアで構成されなければならない。また，十数年にわたる長期間の安定した運用を行うために，アーキテクチャに一貫性があり拡張可能なソフトウェアプラットフォームの採用，ハードウェアやOSに依存しない機構を持つアーキテクチャ，安定した運用・保守を継続できる機構が必要である。一方で，情報システムのライフサイクル全般で人に依存しない高品質なシステム構築を行うため，プロセスの標準化，国際標準・業界標準技術の採用，作業の自動化による品質向上の仕組みや手戻りの発生を抑える開発モデルも必要である。

当社は社会インフラ情報システムの開発に関する課題を解決するために，統合フレームワーク“DIAECOR”を開発した。

DIAECORは統合開発プロセスDIAECOR(PR)，アプリケーションフレームワークDIAECOR(AF)，統合開発環境DIAECOR(ID)，統合運用管理DIAECOR(IM)の4つの製品群からなる。また，アプリケーションフレームワークは，高信頼リアルタイムシステム向けDIAECOR(AF-R)と高信頼ウェブシステム向けDIAECOR(AF-W)の2つの製品群で構成されている。本稿では，PR，AF，ID，IMそれぞれの製品群の特長について述べる。

2. 統合開発プロセス(PR)

2.1 統合開発プロセス(PR)の概要

PRは社会インフラ情報システムを構築するために要求される開発プロセスはもちろんのこと，運用・保守も含めたプロセスと成果物の定型文書を提供し，プロジェクト作業で高い品質を実現・維持することを可能としている。

2.2 統合開発プロセス(PR)の特長

2.2.1 SLCPに対応したプロセス

近年の大規模な情報システムの調達では，ソフトウェアの開発から運用・保守に至るまでのプロセスの国際規格であるSLCPに適合することが求められている。そのため，開発プロセス自体をSLCPに対応させる必要がある。

PRはSLCP-JCF2007に対応したプロセスと文書の雛型(ひながた)を組み合わせた開発プロセスを提供している。開発者は雛型文書を利用することでSLCPに対応したプロジェクトの迅速な立ち上げと推進が可能であり，開発フェーズを明確にした開発を支援している。

2.2.2 PMBOKを取り入れたプロセス

プロジェクトマネジメントにおける知識体系として事実上の国際標準であるPMBOKは，スコープ，時間，コスト，品質，人的資源，コミュニケーション，リスク，調達を総合的に管理するための知識エリアを定めている。

PRは提供する規約・基準を，SLCPに加えてPMBOKの知識エリアとの対応を行っているので，従来のQCD(Quality，Cost，Delivery)による管理だけではない，体系化されたプロジェクト運営を可能にしている。

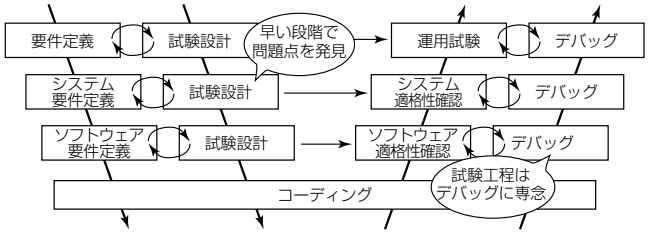


図1．W字型モデル

2.2.3 W字型モデルを採用したプロセス

一般的な開発プロセスでは，現在も試験フェーズの最初に試験計画を行うV字型モデルが主流であるが，V字型モデルの場合，設計の誤りや抜けが試験フェーズで検出された場合に大きな手戻りとなる。

一方PRの開発プロセスは，要件定義と並行で試験設計を行うW字型モデル(**図1**)を取り入れたプロセスを採用しているため，設計の段階でリソースを重点的に投入するフロントローディングを可能とし，試験段階での手戻りを抑制することで，品質の向上を図ることができる。

3. アプリケーションフレームワーク(AF)

3.1 アプリケーションフレームワーク(AF)の概要

AFは，アプリケーション開発者に対して，共通的に利用されるであろう機能やライブラリを提供するものであり，高信頼・高品質で一貫したアーキテクチャを持ち，拡張可能なソフトウェアプラットフォームとなっている。

AFはウェブシステム向け(AF-W)とリアルタイムシステム向け(AF-R)の2つの製品群で構成されており，それぞれの特長は次のとおりである。

3.2 ウェブシステム向け(AF-W)の特長

AF-Wは業界標準のJavaEE(Java Enterprise Edition)アーキテクチャに準拠した，高信頼ウェブシステム向けソフトウェアプラットフォームである。AF-Wを利用することでJSPを用いたHTML(HyperText Markup Language)ベースのアプリケーションや，Flex(注2)を用いたRIAを簡単に作成することが可能となる。

(注2) Flexは，Adobe Systems Inc. の登録商標である。

3.2.1 高品質な業界標準アーキテクチャ

AF-Wはトランザクション管理やエラー制御等，ウェブシステムで必須の機能をあらかじめシステム基盤機能として組み込んだフレームワーク(**図2**)である。Apache Strutsをベースとして一般的なModel／View／Controllerアーキテクチャを採用していることで，誰にでも比較的容易にフレームワークを活用することが可能である。人に依存しない開発を可能にすることで，トータルライフサイクルコストの低減も実現している。

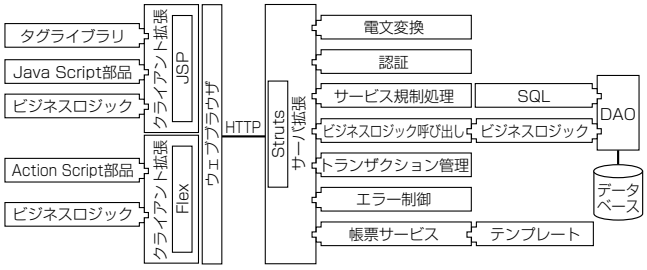


図 2．AF-Wのアーキテクチャ

3. 2. 2　RIAへの対応

AF-Wは，従来のFlexが持っているコンポーネントに加えて，社会インフラ情報システムでよく利用されるDIAECOR独自のコンポーネントを追加している。これらのコンポーネントを活用することによって，更に表現力に優れたウェブアプリケーション(RIA)の開発を可能にしている。

加えて，IDで提供するドキュメント連携機能を用いた設計書の自動生成を行うことで，設計品質の向上も図っている。

3. 3　リアルタイムシステム向け(AF-R)の特長

AF-Rは高信頼かつ高性能を求められる分散処理型ミッション・クリティカル・システムを実現するために必要な，データ管理機構，構成管理機構，ノード間結合機構等を備えたソフトウェアプラットフォームである。

3. 3. 1　長期安定稼働を可能とするアーキテクチャ

AF-Rでは，数年～十数年以上の長期間にわたって，システムを停止させることなく保守作業やハードウェア更新作業ができるよう，プラットフォーム抽象化機構を独自に組み込んだアーキテクチャとなっている。これによって，コンピュータシステムにおける長期ライフサイクルの維持保守活動を可能としている。

このプラットフォーム抽象化機構は，ハードウェアやOSを抽象化するレイヤ(PAL)，サービスの提供を行うレイヤ(DSL)とユーザーデータを抽象化するレイヤ(ADL)に分割した構成(**図 3**)で実現しており，ハードウェアやOSに変更・更新があっても上位のアプリケーション層は変更が不要となる。

3. 3. 2　データ同期インメモリデータベース

AF-Rでは高信頼かつ高性能な分散処理を実現するため，サーバ間の同期機能を備えたメモリ上の高速なデータ保持機構を提供している。

秒間30万件以上の検索を可能とするために一般的なリレーショナルデータベースとは異なるキーバリュー方式でデータを保持することで，メモリアクセスの性能向上だけでは実現できない，更なる高速性を備えている。また，信頼性を実現するためのサーバ間リアルタイム同期機能を保持しており，一台のサーバがダウンした場合でも他のサーバで処理を継続することが可能となっている。

さらに，同期処理を標準的なサービスバス(ESB)を利用して行うことで，隣接装置への同期だけでなく，拠点間の同期も可能となり，分散能力を向上させている。

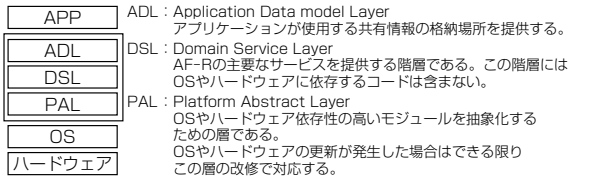


図 3．AF-Rの基本構造

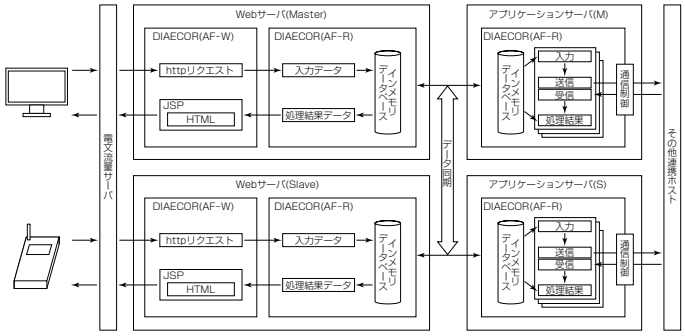


図 4．AF-WとAF-Rの連携

3. 3. 3　時空管理機能

情報システム開発では，限られたサーバ台数しかない状況で複数の実行環境を構築したい場合があるが，利用するリソースが競合するなど，構築や運用が難しかった。

AF-Rでは，リソースが競合しない複数の実行環境を構築する機能を提供しており，この実行環境を“時空”と呼んでいる。時空の特長は，これらに加え，時間の進む速度を時空ごとに変更できることで，例えば2倍の速度にした時空では，試験時間を半分にすることが可能となる。

3. 4　AF-WとAF-Rの連携機能

ウェブシステムではセッションと呼ばれる接続情報の維持管理が必須である。一般的なウェブシステムでは何らかの原因でセッションの接続が切れてしまうと処理が中断されるため，従来技術ではミッション・クリティカルな高信頼ウェブシステムの構築が難しかった。

DIAECORではこのような課題を解決するために，AF-WとAF-Rを**図 4** の形で組み合わせることを可能にしている。この連携機構によって，セッション情報をインメモリデータベースに保存・同期することができ，処理中のウェブサーバが停止した場合でも，フェールオーバー後のバックアップサーバで処理を継続し，ユーザーにシステム異常を気付かせることなく処理を継続することができる。

4. 統合開発環境(ID)

4. 1　統合開発環境(ID)の概要

IDは，PR，AFを導入する際の，品質・信頼性向上とトータルライフサイクルコスト削減を実現するためのツール・機能を統合した開発環境であり，設計支援，試験支援，分析支援のツール類を提供する。

4.2 統合開発環境(ID)の特長

4.2.1 設計支援

設計支援では，システム設計者が利用するツールとして，仕様書を自動生成するツールとソースコードを自動生成するツールを提供している。

仕様書生成ツールでは，画面仕様書，及び帳票仕様書を自動的に作成することができる。また，ソースコードの自動生成ツールでは，JSPの自動生成，エンティティの自動生成等が可能である。

DIAECORではSLCPのプロセスを重視しており，単にツールを提供するだけではなく，そのツールの使い方やプロセスを規定している。先に述べた画面や帳票の仕様書自動作成機能などは，GUI(Graphical User Interface)を利用して画面設計を行うことや，Excel(注3)を利用して帳票設計を行うことで仕様書を自動生成することができるが，さらに，**図5**で示した設計作業の流れの中での活用方法が規定されていることから，トレーサビリティの向上に加え，設計プロセスの順守も促している。

(注3) Excelは，Microsoft Corp. の登録商標である。

4.2.2 試験支援

試験支援では，仕様書から試験設計書を自動生成する機能，試験の自動実施機能，試験実施時に必要な各種ビューア等を提供している。

試験設計書を自動生成することで，設計と試験設計を同時に行えるため，試験自体の品質向上につながる。また，試験の自動化機能によって繰り返し試験を行えるので，デグレードの防止につながる。

各種ビューアは，リアルタイム系の目に見えない内部処理のメモリ状況やメッセージを可視化することを可能にしており，試験の自動化機能と組み合わせることで，機能試験，例外試験の自動テストと結果の検証を容易にしている。

4.2.3 分析支援

分析支援ではログから情報を収集する機能と分析する機能等を提供している。

ログの出力に関しては，作成したプログラムに対して，アプリケーションフレームワークと連携したログ出力機構を自動的に追加する機能を保持している。

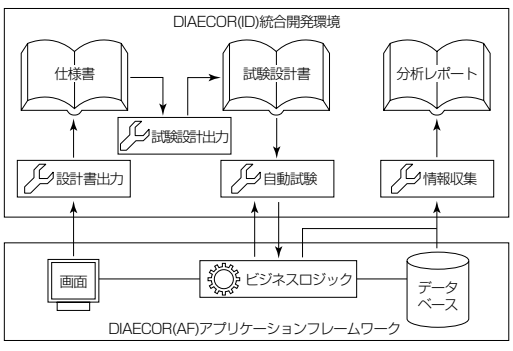


図5．統合開発環境(ID)

この機能を利用することで，実行状況やSQL文のログ出力等が自動的にできるようになるため，製作時に発生しがちなデバッグ文の埋め込みや削除といった工数が不要になり，開発者は機能の製作や試験に注力することが可能となる。

さらに，複雑化するシステムの性能試験を効率的に行うために，高負荷の状態で出力される大量のログからも効率的に目的とするログを探し出す機構とツールを備えている。

5. 統合運用管理(IM)

5.1 統合運用管理(IM)の概要

IMは従来高額であった運用監視アプリケーションを安価に実現するために，オープンソースを活用して社会インフラ情報システムに必要な運用管理機構を組み込み，DIAECORだけで安定した運用・保守を提供可能としている。

5.2 統合運用管理(IM)の特長

5.2.1 稼働状況の監視

IMは，システムの稼働状況を監視し，システムの運転状態に即した様々な状況をアラームやメールでリアルタイムにシステム管理者に通知する。また，システムを構成するCPU，メモリ，ディスク，ネットワーク等のリソース使用状況がリアルタイムでグラフ化されシステムの稼働状況を瞬時に把握することを可能にしている。

5.2.2 クライアント資産を管理

IMは，クライアント端末の資産を遠隔管理する機能を提供している。最近はウェブシステム全盛であるが，現在もクライアント側に特定のファイルを配信したいという要求がある。具体的には，専用クライアントソフトウェアによって，端末にインストールされている各種クライアントソフトウェアや外字フォント等の管理を行い，これらのモジュールの配信やバージョン管理を行うことができる。

また，クライアント端末でのソフトウェアの実行，インストール，マシン再起動等，クライアント側が無人の状態での管理を可能としている。

6. むすび

DIAECORはデータ同期インメモリデータベースを始めとする機能の追加やAF-Wとの連携によって，ミッション・クリティカルな情報システムへ適用できる統合フレームワークとなり，今まで以上に高信頼・高品質を要求される社会インフラ情報システムへの適用が見込めるようになった。

今後は，高信頼・高品質な分散環境と開発プロセスを備えたクラウド基盤を目指すため，機能追加や他システムとの連携強化を目指していく。

参考文献

(1) (独)情報処理推進機構：共通フレーム2007 第2版，オーム社（2009）

特集論文

汎用双方向型Web画面自動生成技術

河村美嗣*　小笠原淳子***
田村孝之**
宮嵜弘治***

General-purpose Bidirectional Web Screen Automatic Generation Technology

Yoshitsugu Kawamura, Takayuki Tamura, Kouji Miyazaki, Atsuko Ogasawara

要　旨

近年，情報システムの形態はWebブラウザをクライアントとしてサーバなどを利用するWebコンピューティングが主流となっている。また，システム開発では，社会の急速な変化に対応することが求められており，短期間／低コスト／高品質にシステムを構築するために，より一層の開発生産性と品質の向上が求められている。

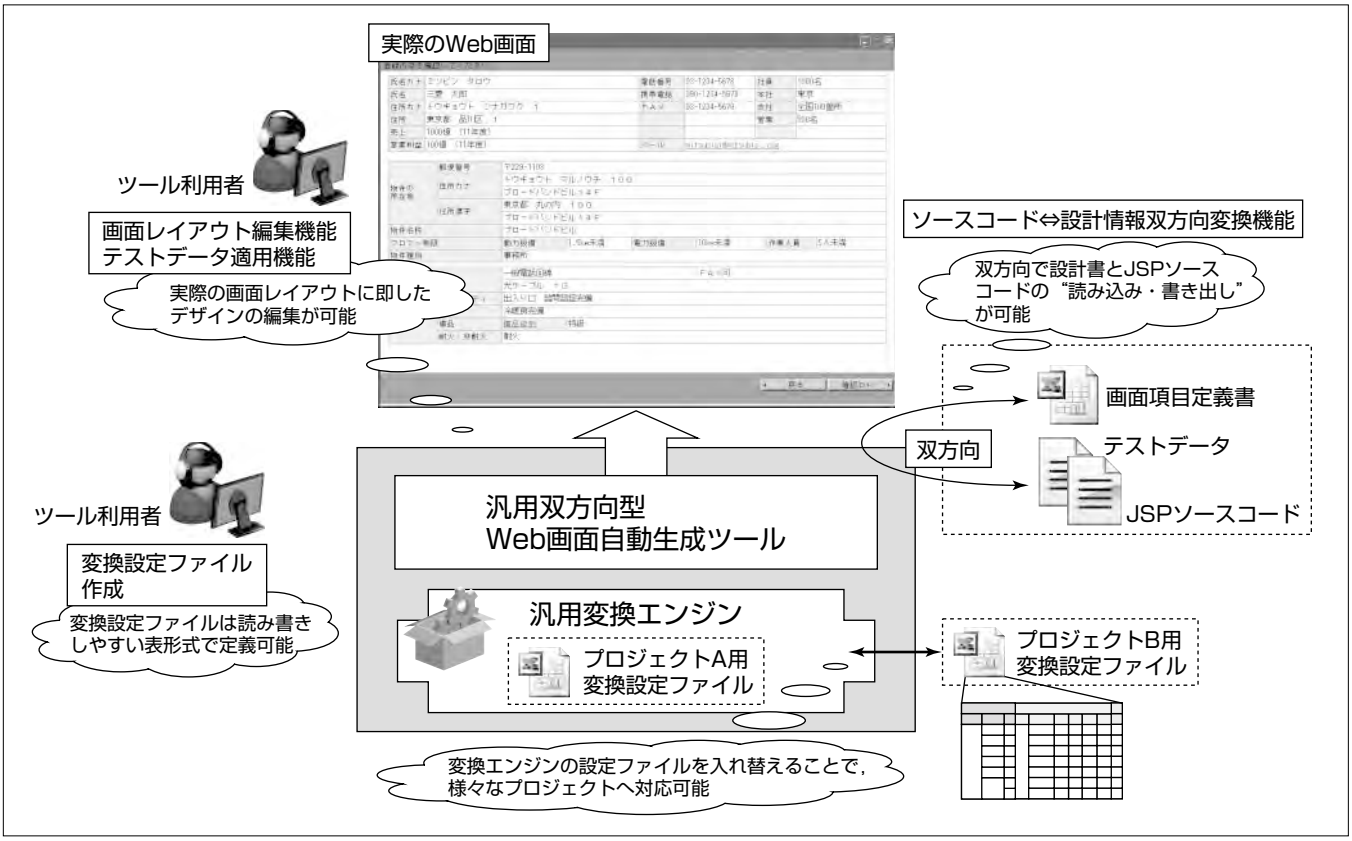
このような背景から，三菱電機インフォメーションシステムズ㈱(MDIS)及び三菱電機㈱では，Web画面開発の効率化を目的に，双方向型Web画面自動生成技術とこの技術を実装した双方向型Web画面自動生成ツールの開発を行ってきた[(1)(2)(3)(4)(5)]。このツールを使用することで，ユーザーの要求を取り込んだWeb画面のレイアウトを容易に作成でき，また，作成した画面レイアウトから設計書やJSP(JavaServer(注1) Pages)ソースコードを自動生成することで，システム開発における生産性と品質の向上を実現している。

しかし，これまでの双方向型Web画面自動生成技術は，プロジェクト固有の仕様書やソースコードのフォーマットに依存する部分が多く，他プロジェクトには容易に適用できないという課題があった。

その課題に対して，今回，このツールを容易に他プロジェクトへ適用可能にするため，双方向型Web画面自動生成技術のコア部分である変換エンジンを汎用化した“汎用双方向型Web画面自動生成ツール”を開発した。

この汎用化によって，他プロジェクトへ適用可能にする際の工数を汎用化前と比較し三分の一以下である5人日以内へ短縮可能という効果が得られている。

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



汎用双方向型Web画面自動生成技術

この技術は，画面レイアウトから設計書やJSPソースコードを自動生成して開発工数の削減を可能にする双方向型Web画面自動生成技術のコア部分である変換エンジンを汎用化することで，他プロジェクトへ容易に適用可能にする。この技術を実装した汎用双方向型Web画面自動生成ツールの利用者は，プロジェクト向けの変換エンジンを作成することなく，変換設定ファイルを作成することで，ツールを新プロジェクトへ適用可能にすることができる。

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

1. まえがき

近年，情報システムの形態はWebブラウザをクライアントとしてサーバなどを利用するWebコンピューティングが主流となっている。また，社会の急速な変化に即座に対応したシステムの開発が求められ，短期間／低コスト／高品質にシステムを構築する必要性が高まり，顧客からはより一層の開発生産性と品質の向上が求められている。

このような背景から，三菱電機インフォメーションシステムズ㈱及び三菱電機㈱では，Web画面開発の効率化を目的に，双方向型Web画面自動生成技術とこの技術を実装した双方向型Web画面自動生成ツールの開発を行ってきた。このツールを使用することで，ユーザーの要求を取り込んだWeb画面のレイアウトを容易に作成でき，また，作成した画面レイアウトから設計書やJSPソースコードを自動生成することで，システム開発における生産性と品質の向上を実現している。

しかし，これまでの双方向型Web画面自動生成技術はプロジェクト固有の仕様書やソースコードのフォーマットに依存している部分が多く，他プロジェクトへ容易に適用できなかった。他プロジェクトへの適用に時間がかかると，要件定義の初期段階に，このツールの特長である画面レイアウトや画面遷移イメージの共有を容易に行う機能を利用できなくなる。この機能の利用によって短期間かつ高品質に要件を確定し，プロジェクト全体の工数削減効果を大きくするには，他プロジェクトへの適用期間を，プロジェクトへの参画決定から要件定義開始までに，短縮する必要があった。

そこで，双方向型Web画面自動生成技術のコア部分である変換エンジンを汎用化することで，このツールを容易に他プロジェクトへ適用可能にした。本稿では汎用化方式の詳細について述べる。

2. 双方向型Web画面自動生成技術とは

双方向型Web画面自動生成ツールは，ソースコード及び画面仕様書とツール内部の設計情報との双方向変換機能，画面レイアウト編集機能と，テストデータを利用したソースコード(JSP)とHTML(HyperText Markup Language)の双方向変換機能から構成されている。

2.1 ソースコード／設計情報の双方向変換機能

ソースコードであるJSPファイルと，設計情報であるExcel(注2)ファイルを双方向に変換する機能である。このツールはJSPファイルの読込機能，書出機能と，Excelファイルの読込機能，書出機能を全て備えている。ソースコードから設計情報に変換したい場合は，JSPファイルを読み込み，その後Excelファイルを書き出す。逆に変換したい場合は，まずExcelファイルを読み込み，その後JSPファイルを書き出す。

(注２) Excelは，Microsoft Corp. の登録商標である。

2.2 画面レイアウト編集機能

Web画面をグラフィカルな編集画面で作成／編集できる機能である。このツールには，Web画面の作成に必要な部品を配置するためのボタンが用意されており，マウス操作で部品を選択し画面レイアウト編集エリアへ配置することで，Web画面を容易に作成することができる。作成した画面レイアウトは，Webサーバを必要とせずにプレビューで確認することができる。また，プレビュー時に画面遷移を確認することもでき，実際のアプリケーションの動きに即した画面設計が行える。さらに，業務要件に合わせて画面項目の表示・非表示制御を行う場合，このツール上で様々なパターンのデータを適用した場合の画面項目の表示・非表示結果を確認することができる。

2.3 テストデータの適用

一般的なWebアプリケーションでは，画面上に動的にデータ(例えば顧客氏名や住所等)を表示する。そのため，Web画面デザインの要件を詰めていく際には，様々なテストデータが表示された状態のサンプル画面を作成し利用する。

このツールは，テストデータとJSPソースコードを合成／分離する機能を備えており，テストデータを表示したまま画面レイアウトの編集が可能である。また，テストデータを差し替えることで，様々なテストデータを適用した場合の画面デザインを簡単に確認することができる。この機能によって，要件定義段階で作成したWeb画面デザインからそのままJSPソースコードを生成することができ，効率的な開発が行える。

3. 他プロジェクトへ適用する際の課題と対応策

2.1節で述べた双方向変換機能を実現するための変換エンジンは，プロジェクトで用いる仕様書やソースコードのフォーマットに合致するよう，開発する必要がある。そのため，このツールを様々なプロジェクトへ適用するにあたっては，**図1**に示すような変換エンジン個別開発方式が考えられる。これは，プロジェクトごとの仕様書やソースコードのフォーマットに対応する変換エンジンを開発するという方式である。

しかし，変換エンジン個別開発方式では，変換エンジンをプロジェクトごとに新規に開発する必要があるため，開発工数がかかるという問題があり，そのため，このツールでは，変換エンジンを個別に開発するのではなく，変換エンジン自体を汎用化するというアプローチを採用することとした。

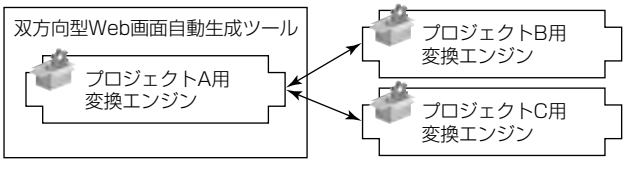


図1．変換エンジン個別開発方式

4. 汎用化実現方式

このツールで採用した汎用化実現方式を**図2**に示す。これは，汎用変換エンジンを開発して，プロジェクトごとに外部で定義したプロジェクト固有の変換設定ファイルを入れ替えるという方式である。

変換設定ファイルには，表形式の変換規則設定ファイル，スクリプト形式の変換スクリプトファイル，変換設定ファイルの自動単体テスト用のテストデータ定義ファイルの三種類のファイルが含まれている。次節より，それぞれの変換設定ファイルの詳細について述べる。

4.1 変換設定ファイル形式の選択

汎用変換エンジンは，変換設定ファイルを読み込み，ソースコード／設計情報の双方向変換を実現する。変換設定ファイルには，ソースコードと設計情報の変換関係の情報を定義する。変換関係を定義するためには，構造化されたデータが表現可能であり，プログラムにとって読み書きが容易であることが望ましい。一方，変換設定ファイルを記述し作成するのは，このツールの利用者であるため，人にとっても読み書きが容易であることが望ましい。

これらの条件を満たすファイル形式を選定するにあたって，**表1**に示すファイル形式について比較検討を行った。ファイル形式としてはCSV(Comma Separated Values)，XML(eXtensible Markup Language)，JSON(JavaScript(注3) Object Notation)，Excelの4形式を列挙し，それぞれ構造化データの表現力と，人，プログラムからの読み書きのしやすさを比較した。比較の結果，データ構造化とプログラムからの読み書きのしやすさでは，XML，JSON形式が優れていることが分かる。しかし，今回はこのツールの利用者にとって読み書きがしやすいことを重視し，Excel形式を選択した。

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

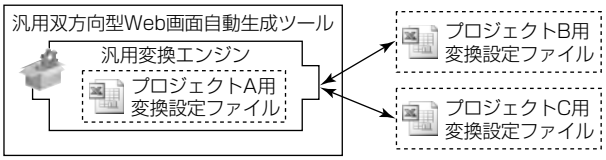


図2．汎用変換エンジン＋変換設定ファイル方式

表1．変換設定ファイル形式の比較

形式	書式	データの構造化	読み書きの容易性	
			人	プログラム
CSV	カンマ区切り	×	△	○
XML	マークアップ	○	△	○
JSON	JavaScript構文	○	△	○
Excel	Excelブック	△ セル結合で表現	◎ 操作性，罫線，色付けに優れる	△ Excelのインストールが必要 入出力処理がやや重い

4.2 1：1又は1：多対応関係の定義

ソースコード／設計情報の双方向変換で，単純な変換規則は，1：1又は1：多の対応関係で表現できる。

1：1又は1：多の対応関係を記述した表形式の変換規則設定ファイルの書式を**図3**に示す。変換規則設定ファイルは，左部分がソースコードに記載のJSPタグ名や属性名，中央部分が画面レイアウト編集に利用するHTMLタグ名や属性名，右部分が設計書の列番号の定義となっている。また，セルを結合することで，構造化されたデータを表現している。

このツールは，このファイル内に記述された対応関係を読み込み，双方向変換時にソースコードに記述されているJSPタグ名や属性名と一致する設定を左部分から探し，同一の行に定義されている対応関係を利用してHTMLや設計書へ変換する。また，逆変換も同様の処理を行うことで実現可能である。

4.3 その他の対応関係の定義

1：1又は1：多の対応関係では定義不可能な変換処理が必要な場合，表形式の変換規則設定ファイルに加えスクリプト形式の変換スクリプトファイルで定義する。

変換スクリプトファイルの書式を**図4**に示す。**図4**では，JSPタグを受け取りHTMLタグを返す処理を持つVisual C#(注4)のメソッドで，JSPからHTMLへの変換処理を定義している。

このツールは，変換スクリプトファイルを読み込み，変換時にコンパイルして実行することで，複雑な変換に対応する。また，逆変換については，逆変換用のスクリプトを読み込み，同様の処理を行うことで実現可能としている。

(注4) Visual C#は，Microsoft Corp. の登録商標である。

4.4 変換設定ファイルの単体テストの自動化

これまで述べてきた変換設定ファイルは，実際にプロジェクトへ適用する前に，想定通りの変換動作をするかテストする必要がある。このテスト工程は，ツールのサポー

図3．変換規則設定ファイル書式

```
public class JspElementConverter{
  public HtmlNode convertElement(HtmlNode node){
    // ここに変換ロジックを記述
  }
}
```

図4．変換スクリプトファイル書式

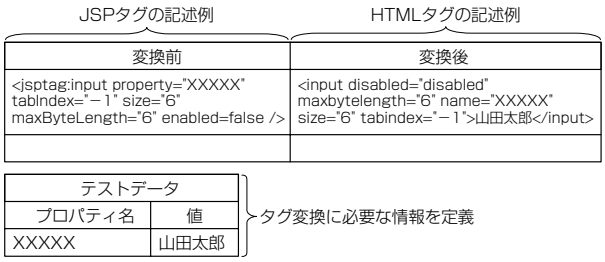


図5．テストデータ定義ファイル書式

トがない場合，無視できない工数がかかると考えられる。そのため，変換設定ファイルの単体テストをツールで自動化し，工数削減を図っている。

図5に自動単体テスト用のテストデータ定義ファイルの書式を示す。単体テストでは，JSPタグとHTMLタグの双方向変換が想定通りに動作するかどうかをテストする。そのためのデータとして，テストデータ定義ファイル内に変換前JSPタグの記述例と，変換後HTMLタグの記述例を定義する。また，JSPに外部から与えるパラメータを，テストデータとして，プロパティ名と値のペアで定義する。

テストツールは，変換規則設定ファイルと変換スクリプトファイルとテストデータ定義ファイルに記述された情報を利用して，実際に双方向変換を実施し，テストデータ定義ファイルに記述された通りの変換が実施されたかどうかの結果を画面に表示する。この結果を確認することで，変換規則設定ファイルと変換スクリプトファイルに記述された内容が正しいかどうかを判断できる。

5. 評　価

このツールをプロジェクトの初期段階である要件定義段階から使用するためには，プロジェクトへの参画決定から要件定義開始までのおよそ1週間で，このツールの準備を完了する必要がある。そのため，プロジェクトへ適用する際の工数の目標値として5人日以内を設定した。

汎用変換エンジンの効果を測定するため，双方向型Web画面自動生成ツールをあるプロジェクトへ適用する際の工数を，汎用化前後で比較した結果を**表2**に示す。

汎用化前は，プロジェクト向けの変換エンジンとして約2KLのプログラムを作成する必要があり，適用完了までにかかった合計工数は約14人日であった。

汎用化後は，変換エンジンの開発は不要であり，プロジェクト向けの変換設定ファイルだけを定義すればよい。変換設定ファイルの書式は用意されているため，作成時に外部設計／内部設計の工程は不要となる。また，単体テストの自動化によって，テスト工数の削減も見込める。

評価に利用したプロジェクトでは，変換設定ファイルの記述量は約20行×15ファイルであり，適用完了までにかかった合計工数は約4.5人日であった。

この結果から，汎用化によって工数を三分の一以下である4.5人日へ短縮することができ，目標値を達成できた。これによって，このツールをプロジェクトの初期段階から使用できることが見込める。

表2．汎用化前後の工数比較

作業内容	汎用化前	汎用化後
仕様確認	1.0人日	1.0人日
外部設計／内部設計	4.0人日	0.0人日
変換エンジン開発	4.0人日	0.0人日
変換設定ファイル作成	0.0人日	1.5人日
単体テスト	4.0人日	1.5人日
結合テスト	1.0人日	0.5人日
合計工数	14.0人日	4.5人日

6. むすび

Web画面の開発工数を大幅に削減可能とする双方向型Web画面自動生成技術と，この技術を実装した双方向型Web画面自動生成ツールの，汎用化における実現方式とその効果に関して述べた。

これまでの双方向型Web画面自動生成技術は，プロジェクト固有の仕様書やソースコードのフォーマットに依存している部分が多く，プロジェクトごとに変換エンジンを開発する必要があり，他プロジェクトへ容易に適用できないという課題があった。そこで変換エンジンを汎用化することで，他プロジェクトへ容易に適用可能とした。評価の結果，他プロジェクトへ適用する際の工数を三分の一以下に短縮可能という効果が得られた。

現在，このツールが入出力可能なソースコードの言語はJSPだけであるが，今後，PHP(PHP：Hypertext Preprocessor)やASP(Active Server Pages)等その他の言語のソースコードを入出力可能とするように拡張開発し，さらに，適用範囲を拡大していく予定である。

参考文献

(1) 河村美嗣，ほか：双方向型Web画面自動生成ツールの開発，情報処理学会，第73回全国大会講演論文集，No.1，221～223（2011）
(2) 杉浦啓介，ほか：双方向型Web画面自動生成ツールの開発とその効果～設計書とソースコードの双方向変換～，情報処理学会，第74回全国大会講演論文集，5A-6（2012）
(3) 河村美嗣，ほか：双方向型Web画面自動生成ツールの開発とその効果～汎用化による適用範囲の拡大～，情報処理学会，第74回全国大会講演論文集，5A-7（2012）
(4) 大島正晴：双方向型Web画面自動生成技術，三菱電機技報，**86**，No.1，68（2012）
(5) 大島正晴，ほか：双方向型Web画面自動生成技術，三菱電機技報，**86**，No.6，349～352（2012）

特集論文

山手線トレインネット実証実験

東野裕一*
荒川直樹**
山村直史***

Trainnet Experiment for Yamanote Line Train

Yuuichi Higashino, Naoki Arakawa, Tadashi Yamamura

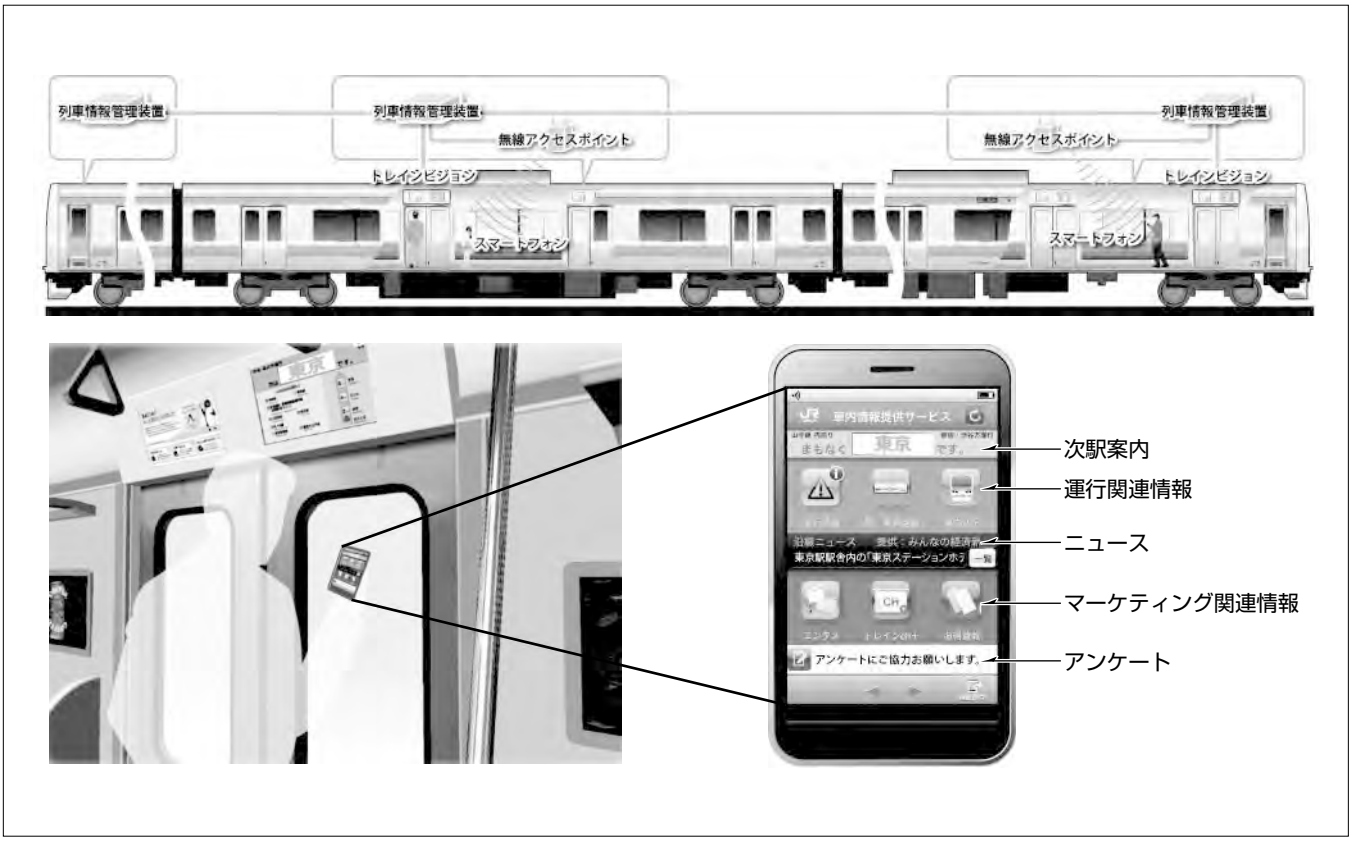
要　旨

社会インフラである鉄道では，乗客へのサービス向上としてLED(発光ダイオード)や液晶ディスプレイを用いた情報提供サービスが導入されており，列車の行き先情報や輸送障害発生時の運行情報等が提供されている。

三菱電機では，東日本旅客鉄道㈱と共同で，鉄道車両内の乗客に対するパーソナルな情報提供サービスを実現するシステムの研究開発を行っている。パーソナルな情報提供サービスとは，列車を利用して移動するユーザー(乗客)に対し，自分が乗車している列車に関する情報や移動先に関係する様々な情報を個人に必要な情報に最適化して提供するサービスである。乗客はネット上の膨大な情報とリアル(列車)を自分で紐(ひも)付ける必要がなく，かつ必要な情報に素早くアクセスすることができる。車両内でこれらの情報を受信するための端末は，乗客が持つ携帯電話を活用する。またデータ通信には携帯電話に搭載される近距離無線通信を用いる。そのため，これまで携帯電話に搭載される様々な近距離無線通信技術を検証してきたが，昨今のスマートフォンの普及によって携帯電話に搭載される近距離無線通信方式として無線LANが選択できるようになった。

今回，車両内に無線LANネットワークを構築し，乗客のスマートフォンに無線LANによる情報提供を行うシステムを開発した。このシステムを用いて，東日本旅客鉄道㈱山手線でフィールド試験“山手線トレインネット(注1)実証実験”を行い，その有効性を検証することができた。

(注1)　トレインネットは，東日本旅客鉄道㈱の登録商標である。



鉄道車両内におけるパーソナルな情報提供サービス

列車の運行情報や沿線情報等，利便性の高い情報を乗客の持つスマートフォンに提供するサービスである。列車位置・停車駅・乗車率等の乗車中の列車に関する情報，移動先に関係する地域情報，エンタテインメント情報等を提供する。“列車情報管理装置”からリアルタイムに取得するデータを活用し，無線アクセスポイントを経由してスマートフォンに情報を配信する。

*営業本部　**インフォメーションシステム事業推進本部　***伊丹製作所

1. まえがき

近年，インターネット上のコンテンツ閲覧行動をリアルな店舗での消費行動に結びつけるO2O（Online to Offline）の取組みが盛んに行われている。スマートフォンの普及によって，移動中でもオンラインで様々な情報検索が容易な時代となり，地図情報サービスなどネットとリアルの紐付けも日常的となっている。

当社では，東日本旅客鉄道㈱と共同で，鉄道車両内における乗客に対するパーソナルな情報提供サービスについての研究開発を行っている。鉄道という社会インフラを利用するユーザー（乗客）の安心・便利・快適な移動を情報提供サービスによってサポートすることが目的である。当社は，サービス実現にあたり乗客が持つ携帯電話を情報提供ツールとして活用することに着目して，これまで携帯電話を使った近距離無線通信による情報配信技術を検証してきた。昨今，スマートフォンの登場によって携帯電話での無線LANによるデータ通信が普及し，大容量のデータ配信が可能となった。

本稿では，今回開発したスマートフォン向けのシステム及びこのシステムを用いて東日本旅客鉄道㈱山手線で行ったフィールド試験“山手線トレインネット実証実験”の取組みについて述べる。

2. 情報提供サービスを実現するシステム

2.1 パーソナルな情報提供サービス

鉄道車両内におけるパーソナルな情報提供サービスとは，列車を利用して移動するユーザー（乗客）に対し，自分が乗車している列車に関する情報や移動先に関係する様々な情報を個人に必要な情報に最適化して提供するサービスである。乗客はネット上の膨大な情報とリアル（列車）を自分で紐付ける（検索キーワードを設定する）必要がなく，必要な情報に素早くアクセスすることができる。“自分が乗った列車が本当に目的地にたどり着く列車なのか？”などといった乗客の不安を解消し，安心な移動をサポートする。また“目的地の一つ前の駅でアラームを通知する”などといった日々の鉄道利用に便利なサービスも提供する。さらに，移動先に関係する様々な情報を提供し，乗車時間を有効に活用できる快適な移動をサポートする。

2.2 システムの構成

このサービスを実現するシステムの構成を**図1**に示す。自分が乗った列車に関する情報は①列車情報管理装置から受信した列車データが基になる。②情報提供装置はリアルタイムに受信する列車データ（走行位置や運行情報等）を加工・管理し，携帯電話からのリクエストに応じて情報を配信する。移動先に関係する様々な情報は，③コンテンツ管理システムから登録された情報を配信する。移動先に関係する沿線情報やエンタテインメント情報等が列車の進行に応じて選択され，配信される。例えば大崎から渋谷・新宿方面に向かって走行しているときは，渋谷に関係する情報が提供され，渋谷を過ぎると新宿に関係する情報が配信される。つまり乗っている列車の情報を基に情報の絞込みが行われている。情報を受信する装置には特殊な情報端末は使用せず，乗客の持つ携帯電話を活用している。

2.3 近距離無線通信による情報配信

2.3.1 モバイルFeliCaによる情報配信

車両内という公共空間では，ユニバーサルなサービスが求められることから不慣れな人でも簡単に使えることが必要である。そこで，“おサイフケータイ(注2)”の用途で搭載されたモバイルFeliCa(注3)に着目した(1)。モバイルFeliCaは，非接触ICカード技術“FeliCa”を携帯電話に搭載したものであり，近距離無線通信による情報配信が可能である。リーダー／ライター装置に携帯電話をタッチするだけで情報を配信することができ，改札を通るときに交通系ICカードをタッチする行為との親和性もあると考えた（**図2**）。2006年秋ごろからは第2世代のモバイルFeliCaが搭載され，通信速度の向上（212kbpsから424kbpsに向上）と“アドホック通信”機能によって，画像などの大容量データも送信できるようになった。

しかし，モバイルFeliCaは“おサイフケータイ”のイメージが強く，利用者にとっては“情報取得の手段”というなじみが薄かった。また情報を取得する際にリーダー／ライター装置にタッチするという行動が伴うため，車両内の混雑

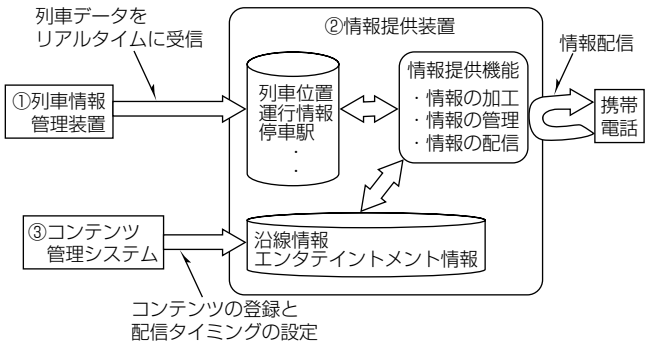


図1．システムの構成

図2．モバイルFeliCaによる情報配信

状況では利用に躊躇(ちゅうちょ)してしまうという心理的なバリアや物理的にタッチできないという課題があった。さらに，各キャリア全てに対応して標準的に配信する方法にも課題があった。

(注2)　おサイフケータイは，㈱NTTドコモの登録商標である。
(注3)　FeliCaは，ソニー㈱の登録商標である。

2.3.2　無線LANによる情報配信

当時(2006年頃)，無線LANは携帯ゲーム機などには既に搭載されていたが，携帯電話への搭載が進んだのは，iPhone(注4)が発売された2008年頃からである。2009年にはAndroid(注5)端末が発売され，スマートフォンと呼ばれるようになり，一挙に携帯電話での無線LANによるデータ通信が普及した。これによって携帯電話の近距離無線通信として無線LANが選択できるようになった。無線LANであれば，携帯電話だけでなく，携帯ゲーム機や音楽プレーヤー等にも配信が可能であり，より幅広いユーザーが利用できる(**図3**)。

(注4)　iPhoneは，Apple Inc.の商標である。
(注5)　Androidは，Google Inc.の登録商標である。

2.4　コンテンツの管理

沿線情報やエンタテインメント情報は，コンテンツ管理システムからコンテンツデータを登録することで配信される。データはWeb形式であるため，既にWebコンテンツを持っている場合はそれを流用することができる。またコンテンツを配信する日時や位置(列車位置)等の配信条件を設定することができ，登録したコンテンツは，実際の配信イメージをプレビューで確認することができる(**図4**)。

図3．無線LANによる情報配信

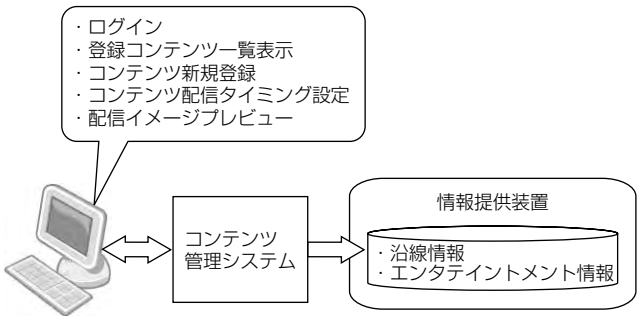


図4．コンテンツ管理システム

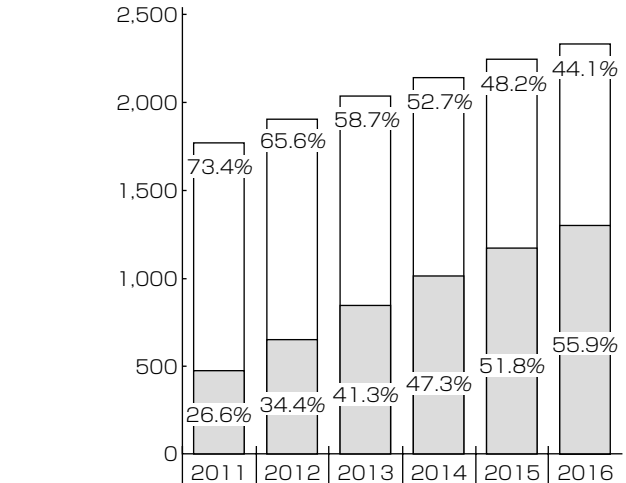
3.　スマートフォンを用いた情報提供

3.1　携帯電話市場の動向

無線LANが搭載された携帯電話の普及状況は，スマートフォンの普及状況に見ることができる。世界市場における携帯電話販売台数に占めるスマートフォンの比率は，2011年は約27%に達している(2)。比率は今後も拡大を続け，2015年には世界市場で5割を超える見通しとなっている(**図5**)。また，スマートフォンの販売台数は，2011年の4億7,000万台から，2016年には13億台となり，年平均22.5%の成長が予測されている。携帯電話の新規契約はスマートフォンが中心という状況であり，若年層を中心にスマートフォンへの移行が進んでいる。スマートフォンがパソコンとほぼ同等のWeb閲覧機能を持っていることが，スマートフォン購入の重要な動機となっていると考えられている。

3.2　山手線でのフィールド試験

東日本旅客鉄道㈱との共同研究開発の一環として，2011年10月上旬から約1か月間，山手線1編成で“山手線トレインネット実証実験”という呼称でフィールド試験を実施した(3)。車両内に無線アクセスポイントを設置し，乗客の持つスマートフォンに情報を配信した。トレインネット対応列車に乗車し，車両内の専用Wi-Fi(注6)ネットワーク“Trainnet”に接続することで誰でもサービスを利用できる。スマートフォン用アプリケーションを用いることで，“車両の外”では携帯電話回線を利用した試験列車の走行位置の提供(試験列車は1編成だけであったため，探すことができるようにした)やサービスの利用方法を案内し，“車両の中”では無線LAN接続による情報提供サービス(ただし，インターネットには接続できない)を行う構成とした(**図6**)。



	2011	2012	2013	2014	2015	2016
その他携帯電話	1,303	1,248	1,194	1,127	1,083	1,026
スマートフォン	472	655	841	1,012	1,165	1,303
合計	1,775	1,903	2,035	2,139	2,248	2,329

出典：平成24年度版情報通信白書

図5．世界の携帯電話販売台数に占めるスマートフォンの販売台数の推移(推計)

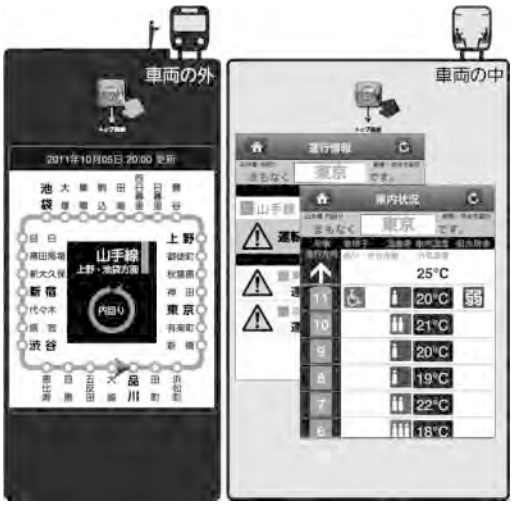


図6．“山手線トレインネット”のサービス構成

(a) 第1回実証　(b) 第2回実証

図7．トップ画面のデザイン

提供したトップ画面のデザインを**図7**(a)に示す。画面のヘッダ部には常に自列車に関する情報が表示されるようになっており，走行位置に応じて“次は○○駅です”，“間もなく○○駅です”，“ただいま○○駅です”のいずれかの状態がリアルタイムに表示される。これによって，目的駅への到着を常に意識しながら移動先に関する様々な情報を閲覧することができる。このように場所に応じたリアルタイムな情報をタイムリーに提供する点がこのサービスの特長である。

また，トレインネット上のコンテンツ閲覧行動をリアルな店舗での消費行動に結びつけるO2Oの取組みとして，駅内店舗，駅周辺施設で利用できる電子クーポンを配信した。利用者はトレインネット利用時に電子クーポンのイメージを保存し，リアルな店舗で提示することで割引などの特典を受けることができる。

アクセスログの評価から当初の想定よりも多くのユーザーが利用したことが確認できた。またコンテンツ別に見ると，“車内状況”“お得情報”“駅･乗換路線”が特にアクセスが多い傾向にあった。“車内状況”は，車内の混雑率や温度がリアルタイムに見られるため，目新しさを感じる一方で，“乗る前に見たい”という意見が多く得られており，乗車前に提供する仕組みを構築することで更に有益な情報と感じることが期待できる。システム面では，インターネットに接続できないことへの不満が多く得られた。

2012年に行った2回目の実証実験では，トレインネット利用時にインターネットへの接続を可能とし，この課題を解決した。これによってインターネット上のサービスと連携したサービスも提供可能となり，サービスのバリエーションを増やすことができた。また複数編成へのサービス提供にも対応し，約4か月半の実証期間でコンテンツの運用管理についても検証を行うことができた。トップ画面のデザインは，**図7**(b)に示すように，白い背景にカラフルなクリスタルボールをデザインすることで，ポップで楽しそうな印象を与えるデザインとした。

(注6)　Wi-Fiは，Wi-Fi Allianceの登録商標である。

3.3　今後の展開

このサービスは双方向型の情報提供サービスであるため，情報配信を行うだけでなく，鉄道利用時の乗客からの意見や感想等の情報を収集することも可能である。提供サービスの利用状況や乗客から収集した情報を分析し，サービスを改善していくことで，サービス品質の維持・向上を図ることができる。また，これまでの成果を基に，列車だけでなくバス，駅，空港等，様々な社会インフラへの応用・展開が可能と考える。

4. むすび

鉄道車両内でのパーソナルな情報提供サービスを実現する上で，携帯電話に搭載される様々な近距離無線通信による情報配信方法を検証してきた。スマートフォンの登場によって，近距離無線通信として無線LANが選択できるようになり，今回，車両内に無線アクセスポイントを設置した情報提供システムを開発した。また開発したシステムを山手線に搭載し，フィールド試験を行うことでシステム面及びサービス面で様々な検証を行い，その有効性を確認することができた。今後は，このシステムの実用化と様々な社会インフラへの応用・展開に取り組んでいく。

参考文献

(1) 松本貴之，ほか：車両内における個人向け情報提供システム(InfoPic)の開発，JR EAST Technical Review，No.33，23～26（2010）
(2) 総務省：平成24年度版情報通信白書，161（2012）http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/pdf/n2020000.pdf
(3) 松本貴之，ほか：車両内での個人向け情報提供サービス「トレインネット」，JR EAST Technical Review，No.41，19～24（2012）

特集論文

薬局経営の業務効率化を支援する“調剤Melphin/DUO”

山口英二* 平田基晴*
井川 大* 大森智美*
土田泰治*

Melphin/DUO：Speedy，Simple and Safety Prescription System for Customer Satisfaction

Eiji Yamaguchi, Dai Igawa, Taiji Tsuchida, Motoharu Hirata, Tomomi Oomori

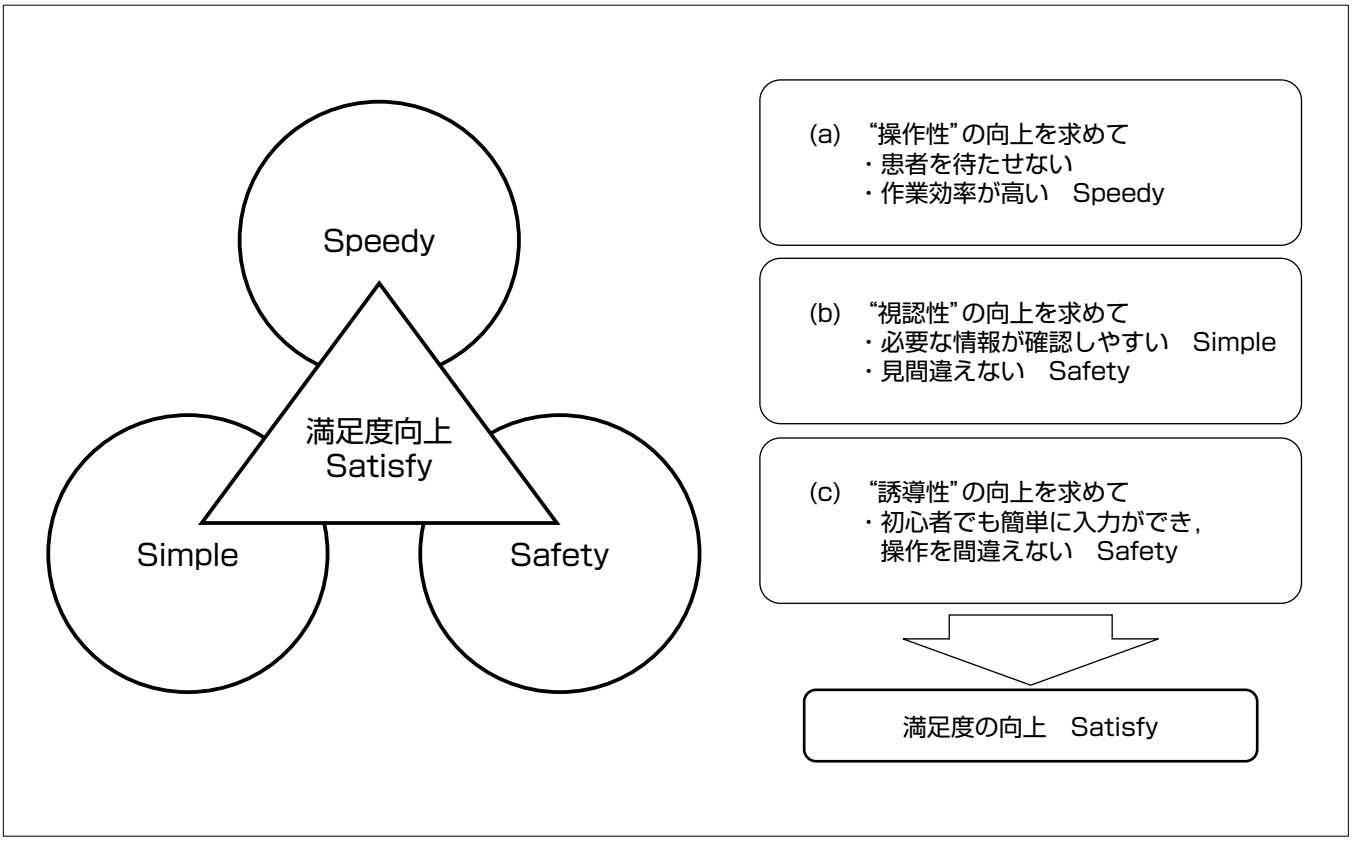
要 旨

三菱電機インフォメーションシステムズ㈱(MDIS)は，1980年代から約30年にわたり，三菱保険薬局システム“調剤Melphin”を開発し，調剤薬局をサポートしてきた。

調剤薬局業界は，医療費削減を目的とした医薬分業政策に乗って急成長を続けてきており，平成15年度には分業率が50%を超えた。その後平成23年度には64%を超えたが，分業率が鈍化してきており，市場は成熟期に近づいていると考えられる(1)。そのよう状況のなか，MDISは更なる拡販を目指し，操作性を大幅に向上させた新製品“調剤Melphin/DUO(デュオ)”を開発した(2)。

“調剤Melphin/DUO”は薬局業務の主要機能である“処方せん入力”の操作性に対して，現行製品の長所を維持しつつ，大きく改良を加えたものである。

開発にあたって，“調剤Melphin”のコンセプトである“3S”に，“満足度の向上(Satisfy)”を加えて，新たなコンセプト，“3S＋S”を定めた。その後，“使いやすさ”をテーマとした有識者によるブレーンストーミング及び薬局員へのインタビュー結果からコンセプトを具体化して，具体化した項目を，成果物がコンセプトに適合しているか確認するためのチェックリスト(以下“コンセプト適合リスト”という。)としてまとめ，要件定義から試験の全フェーズで，“コンセプト適合リスト”によるチェックを繰り返し，コンセプトに沿った開発を完遂した。



“調剤Melphin/DUO”のコンセプト展開

“調剤Melphin/DUO”の開発にあたって，“調剤Melphin”の製品コンセプトである“3S”に，“満足度の向上(Satisfy)”を加えて“3S＋S”のコンセプトを定めた。“3S”は“Speedy”“Simple”及び“Safety”で，それぞれ“操作性”向上，“視認性”向上及び“誘導性”向上へ展開できる。これらの機能向上を実現することで，ユーザーの“Satisfy”(満足度の向上)を図り，更なる拡販を目指す。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

三菱電機グループは，1980年代から約30年にわたり，三菱保険薬局システム“調剤Melphin”を販売し，調剤薬局をサポートしてきた。現在では，全国でのシェア約14%で，業界第3位に位置している。

“調剤Melphin”は，MDISが開発し，三菱電機インフォメーションテクノロジー㈱(MDIT)から全国の代理店を通して調剤薬局向けに販売している製品であり，MDISでは，“調剤Melphin”シリーズの更なる拡販によって，業界2位へ躍進することを目標とし，様々なユーザー拡大施策を行っている。

本稿では，拡販を目指し，操作性を大幅に向上させた新製品，“調剤Melphin/DUO”(以下“DUO”という。)で取り組んだコンセプトの展開方法，システムへ組み込んだ内容と成果について述べる。

2. 調剤Melphin/DUOの開発

2.1 調剤Melphin/DUO開発の経緯

“調剤Melphin”シリーズは，現行製品の“調剤Melphin/Neo(ネオ)”(以下“Neo”という。)の発売から5年が経過し，市場からは新製品の早期投入を求められていた。新製品の開発にあたっては，まず“3S＋S”のコンセプトを定めた。コンセプトの“3S”は，“調剤Melphin”のコンセプトである“Speedy”“Simple”“Safety”の3つの頭文字を表し，“＋S”は“3S”を実現することで得られる“Satisfy”を意味する。

2.2 コンセプトの展開

コンセプトに適合した製品を実現するために，今一度原点に立ち戻って，“調剤Melphin”の強みである“使いやすさ”の更なる向上を差別化戦略として掲げ，GUI(Graphical User Interface)及び画面操作性の向上に重点を置きつつ，Neoが持つ処方せん入力のGUIイメージを刷新し，他社製品を凌駕(りょうが)する“使いやすさ”を備えることを目標とした。

目標の実現に向けては，薬局の窓口業務の大半を占める“処方せん入力”の使いやすさをテーマとした有識者によるブレーンストーミング及び薬局員へのインタビューによって，“使いやすさ”の具体的な要件を抽出し，コンセプトに合わせてそれぞれ，“Speedy”：操作性向上，“Simple”：視認性向上，“Safety”：誘導性向上に展開した。

2.3 コンセプト適合リスト

目標を満たす製品を実現するためには，要件定義からシステム試験までの全フェーズで，仕様書やプログラムが目標から外れていないことを常に意識する必要がある。そのために，バイブルとなるチェックリストとして，“コンセプト適合リスト”を作成した。

3. コンセプト適合リストの作成方針

“コンセプト適合リスト”の作成にあたっては，“3S”のコンセプトそれぞれについて展開した，“使いやすさ”の要件(操作性向上，視認性向上，誘導性向上)を基に，まず具体的な確認ポイントを定めた。

3.1 操作性向上

操作性を向上させることで，“Speedy”な操作ができるようにする項目を，確認ポイントとしてまとめた。

⑴ 入力の簡素化

入力を簡素化することで，入力の手間を減らし，高速化を図る。具体的には，Neoでは複数画面にわたって操作する必要があった機能を，1画面で操作が完結するように見直し，ユーザー操作の回数を減らす工夫を実施した。

⑵ Neoの継承

Neoでは，処方せん入力で，キーボードだけで入力可能であることが好評であったため，マウス入力方式に加え，キーボード入力方式を踏襲した。

⑶ ショートカットの充実

主要機能に対してショートカットを設け，作業効率を高めた。

3.2 視認性向上

視認性を向上させ，表示内容の理解度を高めるようにする項目を，確認ポイントとしてまとめた。

⑴ シンプルな画面構成

画面構成をシンプルにして見やすくすることで，表示内容を早くかつ正しく理解できるようにする。

⑵ 視覚的な効果

強調したい箇所の色やサイズを変え，目立たせる。

3.3 誘導性向上

操作上の誘導性を向上させることで，ユーザーによる処方せんデータなどの誤入力を防ぎ，より“Safety”なシステムを目指す項目を，確認ポイントとしてまとめた。

⑴ 画面構成の分かりやすさ

項目ごとにまとまった配置にするなど，画面構成を分かりやすくして，ユーザーの誤操作を防ぐ。

⑵ 操作ミスの防止

入力補助機能を充実させたり，メッセージを読むだけで必要な操作が分かるようにエラー及び警告を表示することで，操作ミスを防止し，適切な操作に誘導する。

3.4 コンセプト適合リストの作成

3.1節から**3.3節**の確認ポイントを基に更にブレークダウンし，具体的な確認項目を検討して作成した“コンセプト適合リスト”の一部を，**表1**に示す。左端の欄に，コンセプトそれぞれについて展開した，“使いやすさ”の要件である，“操作性向上”“視認性向上”及び“誘導性向上”を置き，右へいくほどブレークダウンされ，より具体化された内容

表1．コンセプト適合リストの一部

コンセプト要素	要件	実現方式	確認項目
視認性（見やすさ）	画面構成	シンプルな画面構成	関連情報がグルーピングされている。 グループは大・中・小に3分類し，大分類が3つ迄を目安とする。
		強調性	見たい画面のサイズ・色が他画面より際立っている。
		ワイドモニター対応	横スクロールせずに表示できる。
		入力・表示項目の配置	最小限の目・手の動きに配慮した配置になっている。 ※画面左上→右下への入力 類似・関連情報が近い位置に配置されている。 比較すべき項目は横並びに配置されている。
		ユーザーによる配置変更	フリーレイアウトが可能である。 画面配置パターンをあらかじめ用意し，ユーザーがパターンを選択できる。
	視覚化	フォント	小さすぎず大きすぎないフォントサイズである。 強調したい項目は，フォントの種類・サイズを変える。
		属性のアイコン表示	一目で属性や意味が判断できるイメージ（アイコン）表示になっている。
		色合い	確認事項・注意事項を見落とさないよう，安全性へ配慮した色使いになっている。 ※エラー：赤・黄・青
		複線，背景色	入力箇所の色やグループが色分けされ，人間の本能的な認知となっている。
		項目タイトルと入力項目の明確化	入力項目が一目でわかる配色になっている。 システム的に統一されている。
操作性	入力の簡素化	入力方法	マウス操作が楽（制御コード不要）である。 キーボード入力だけでも入力可能である。 IME制御が考慮されている。 西暦・和暦チェックが考慮されている。
		項目移動	オートマチックエンターが可能である。 左→右，上→下への入力が考慮されている。

IME：Input Method Editor

となり，右端の欄はコンセプトに沿っているかどうかの確認項目となっている。

3.5　コンセプト適合リスト活用による効果

“コンセプト適合リスト”によるチェックの効果を次に述べる。

(1)　コンセプトからのぶれ防止

“コンセプト適合リスト”を用いて，開発の各フェーズで仕様書，プログラムをチェックすることによって，コンセプトに沿った製品を実現することができた。

また，“コンセプト適合リスト”によって，具体的なチェック項目を共有することで，プロジェクトメンバー間の意思統一が図れ，メンバーに依存することなくコンセプトからのぶれを防ぐこともできた。

そのうえ，“コンセプト適合リスト”をバイブルとして共有することで，課題が発生した際にも，課題解決の指針となり，課題解決にかける打合せなどの時間を削減することができた。

(2)　操作性，誘導性の向上

“操作性向上”及び“誘導性向上”の例を**図1**に示す。“コンセプト適合リスト”によって，Neoの長所を引き継ぎつつ，Neoの課題を克服した。特に，処方せん入力の複雑な手順については，“コンセプト適合リスト”を利用して繰り返して操作手順を見直した結果，入力を誘導する画面を作成するなどの工夫によって，**図2**に示す通り，手順数を26回の操作から3回の操作へと約1/8に大幅に削減できた。

◆ワイド画面に対応。特記・患者コメントなど患者情報を常に表示
◆項目ごとにまとめた配置とタイトルごとに色区分け
◆制御コード入力のような分かりにくい機能は，“サイドメニューバー”による操作誘導で，現状よりマニュアルレスで作業が可能

図1．操作性，誘導性の向上

(3)　視認性の向上

“視認性向上”の例を**図3**に示す。Neoでは，監査結果を判断するために，複数画面を確認する必要があったが，DUOでは必要な情報を1画面にまとめることで，視認性を向上させた。

Neo

No	入力・操作手順	操作(回)
1	処方せん入力画面を起動する。	1
2	処理モードに[新規]を選択する。	1
3	医療機関・診療科・保険医を選択する。	1
4	基本料の制御行コードを[Ctrl]+[Delete]で削除する。	1
5	薬歴料の制御行コードを[Ctrl]+[Delete]で削除する。	1
6	服薬情報等提供料の制御行コード"8.1010"を入力する。	6
7	指導量のみの算定用薬品コードを入力する。	4
8	分量"1"を入力する。	1
9	材料の用法コード". ザイ"を入力する。	2
10	[F12]で確定する。	1
11	対象調剤日入力画面が表示される。	−
12	対象調剤日を入力する。	6
13	[F12]で確定する。	1
合計		26

DUO

No	入力・操作手順	操作(回)
1	薬歴選択画面で算定対象の薬歴を選択する。	1
2	指導料のみ算定画面を起動する。	1
3	医療機関・診療科・保険医を確認する。	−
4	[F12]で確定する。	1
合計		3

図 2．操作手順数の削減

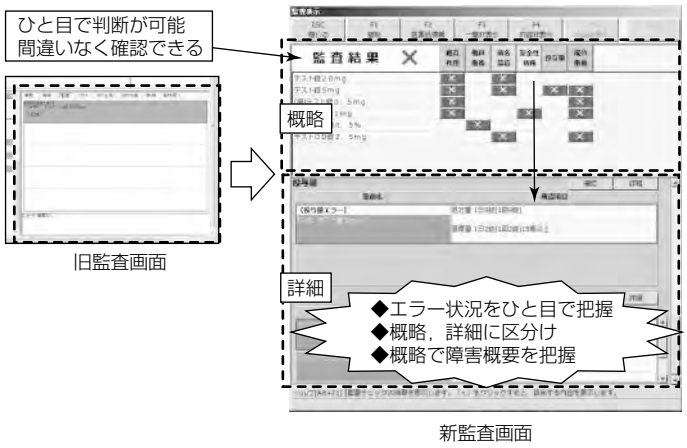


図 3．視認性の向上

⑷ GUI評価の見える化

“コンセプト適合リスト”によってチェック項目を明確にすることで，定量的な評価がしづらいGUIでも，定量的に効果を評価できるようになった。

例えば，システム設計では，Neoの適合度とDUOの適合度を比較し，DUOの適合度が高くなるようにした。具体的には，コンセプト適合リストの要件ごとに，Neoの適合数とDUOの適合数を比較し，Neoの適合数が高かった場合，DUOのシステム設計を見直して，DUOの適合数が高くなるようにした。このように，チェックと見直しを繰り返すことで，全要件で，DUOの適合数の方が高いシステム設計を実現した。また，適合数によって，“使いやすさ”が向上したことを定量的に評価できた。

4. む す び

今回の開発では，主に処方せん入力機能を中心に，GUI及び画面操作性の向上を目指した。今後は，処方せん入力以外の機能に対しても，コンセプトを基に適合リストを作成し，機能追加・改良する計画である。また，近年はネットワーク環境が目覚しい進歩を遂げており，次版以降，“3S＋S”に“N”(Network)を加えたコンセプトに拡張し，プライベートクラウド(企業の社内向けサービスを提供する形のクラウド)などに取り組むことも検討している。さらに，今後は販売面や保守面にも視野を広げ，改善を実施することで，次世代DUOの販売拡大に取り組み，業界2位への躍進を目指していく。

参 考 文 献

⑴ 日本薬剤師会：医薬分業進捗状況
http://www.nichiyaku.or.jp/?p=11219
⑵ 三菱電機㈱：ニュースリリース2013年1月29日：三菱保険薬局システム「調剤Melphin/DUO(デュオ)」発売のお知らせ（2013）
http://www.mitsubishielectric.co.jp/news/2013/0129-b.html