ISSN 0369-2302/CODEN:MTDNAF

MITSUBISHI ELECTRIC
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

8
2016
Vol.90 No.8

## 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.90 No.8 2016


目　次

特集「企業・社会の快適・安心・発展を支えるITソリューション」　IT Solutions for Optimized, Secure and Progressive Enterprises and Society



特許と新案



**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，最新技術を活用したICT(Information and Communication Technology)システムの開発と，それらシステムの稼働を安全に維持する運用管理サービス等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，オフィスビル，工場，家庭など，様々なところから，ノートパソコン，スマートフォン，タブレット等，ICTデバイスを用いて，セキュリティが確保された安心・安全なクラウド上のデータセンターのサーバにアクセスし，そのデータセンターが監視・運用されている様子をイメージで表している。

巻/頭/言

# IoTのもたらす新たな社会～循環型社会の実現に向けて～

## New Society by IoT － for Realizing Sustainable Society －

撫中達司
*Tatsuji Munaka*

モノのインターネット(Internet of Things：IoT)花盛りであるが，日ごろの生活の中でIoTを実感することはまだまだ少ない。全てのモノがインターネットに接続され，収集されたデータの活用によって新たなサービスが生み出されるとのことだが，一般消費者からIoTって具体的にはどのようなものですか，これまでのインターネットとは何が違うのですかと尋ねられたら，どう答えればよいだろうか。

IoTを支えるインフラであるインターネットは1990年代前半のWebブラウザの登場によって商業利用が拡大し，2000年代の携帯電話，スマートフォンの登場で世界中に広がり，我々の日々の生活に欠かせないものとなっている。インターネットは，第三次産業革命ともいわれ，モノづくりの生産性を向上させる仕組みの基本インフラとして，産業の発展に大きく寄与したことはいうまでもない。一方で，人々の生活が便利に，豊かになった代償として，環境問題という大きな課題を抱える結果となっている。

このような状況を踏まえ，IoTがこれまでと異なる価値をもたらすには，人々の生活を便利に，豊かにすることだけにとどまらず，再生可能エネルギー等の利用をより促進し，環境に配慮した循環型社会の実現に寄与するものでなければならないのではないだろうか。安心・安全，使いやすい，低価格などを実現する製造の仕組みに加え，共有によって繰り返し利用され，最後にはその形を変えて新たなモノへと循環されていくような社会を築くために，IoTが担う責務は大きい。

さて，ここで改めて“IoTとは”という質問に答える一例を紹介しよう。我々が日々生活で消費するモノは，製造，流通，消費，廃棄・再利用というライフサイクルを持つ。モノが消費され，廃棄・再利用される際，環境に配慮してゴミは最小限に，資源は最大限にすることが大切であることはいうまでもない。モノのライフサイクルの末端で機能するのが“ゴミ箱”である。IoTは全てのモノがインターネットに接続されるといわれているが，モノのライフサイクルの末端で機能するゴミ箱までがインターネットにつながり，IoTの一例として重要な役割を果たしている。

仕組みは至って単純である。ゴミ箱の中のセンサがゴミの量を常に測定し，一定量以上ゴミがたまると，“そろそろ回収が必要です”と自らゴミの回収の必要性を知らせてくれる。センサやインターネット接続のための電源はソーラー発電によって賄われる。このようなゴミ箱は“スマートゴミ箱”と呼ばれ，ロンドン五輪でも導入されており，また米国等海外では既に多くの場所で活用が進み，環境の美化に加え，回収の効率化による人件費を含めた運用費の削減，さらには回収車両の$CO_2$の削減など，多くの成果をもたらしている。ゴミ箱をさらに一歩進めて，ゴミと再生可能な資源とを分別した“資源の回収箱”とすれば，モノの共有，再利用を促進する循環型社会の実現に向け重要な役割を担えることになる。

IoTは消費者個別のニーズを満たすモノの効率的な製造，付随する新たなサービスの提供という点に大きな関心が寄せられている。しかし，モノが製造され，運搬されて消費者にわたって消費された後，最終的には廃棄又は再利用されるというライフサイクルを考えれば，製造から廃棄・再利用までの全てのライフサイクルが考慮されたモノづくり，そのためのサービスがIoTによってもたらされることが大いに期待される。

IoTによって，再生可能エネルギー等を活用した環境に優しいモノづくりが可能になり，モノを消費して廃棄するという時代から，共有され再利用できることがモノの価値判断となる。このような社会を実現することが，IoTに携わる我々に課せられた１つの命題ではないだろうか。

東海大学 情報通信学部 組込みソフトウエア工学科 教授
Professor, School of Information and Telecommunication Engineering, Embedded Software Technology, TOKAI University

特集論文

# 三菱電機スマート制御クラウドサービス“DIAPLANET”のIoTシステムへの適用

伊藤正裕*
田村孝之**
古谷　遼*

*Application of Cloud Services "DIAPLANET" to IoT System*

*Masahiro Ito, Takayuki Tamura, Ryo Furuya*

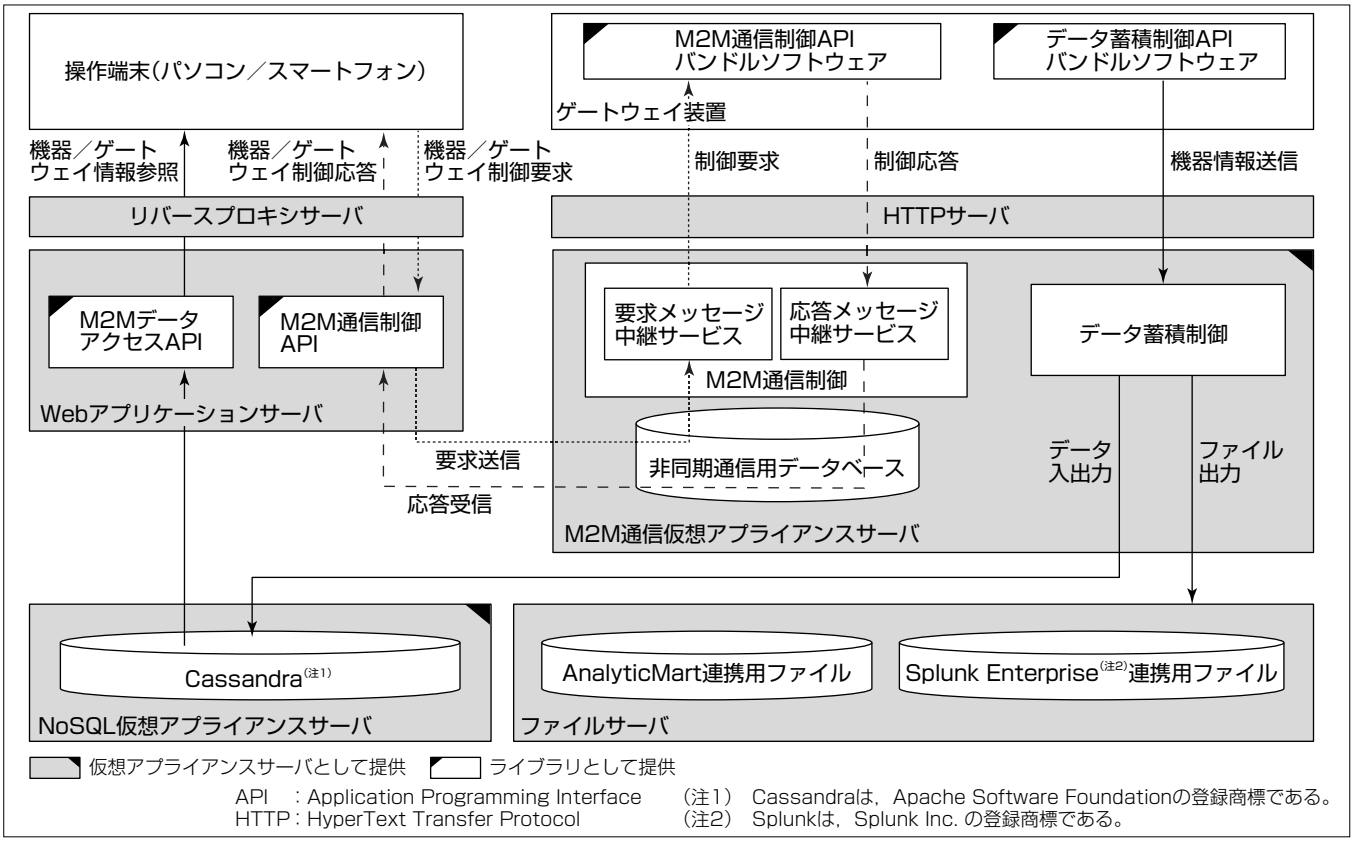
**要　旨**

モノのインターネットと呼ばれるIoT(Internet of Things)は，大量の機器からデータを収集して分析することで，マーケティング，機器の故障検知，AI(Artificial Intelligence)技術を利用した機器の故障予兆への活用や家庭電化製品を外出先から制御したり，機器の故障時に制御を保守拠点から行ったりする遠隔制御への活用が期待されている。

三菱電機は2015年４月から三菱電機スマート制御クラウドサービス“DIAPLANET”の提供を開始している。DIAPLANETのベースサービス(基盤)では，IoTシステムを構築するために必要なM2M(Machine to Machine)通信機能，データベース機能を提供している。M2M通信機能では，M2Mデータ蓄積機能とM2M通信制御機能を提供している。一方，データベース機能では，RDB(Relational Data Base)，冗長構成RDB，NoSQL(Not only SQL)，DWH(Data WareHouse)，リアルタイムデータ分析機能を提供している。用途に応じて機能を組み合わせることでIoTシステムを構築することが可能である。

IoTシステムの多くはデータ収集・分析及び遠隔制御を目的としている。これらのシステムの規模及び特性に応じてシステム構成を選択する必要がある。

今後，IoT及びM2Mシステムの標準化動向を見据えながらDIAPLANET完成度を高めて進化させていく。




## DIAPLANETが提供するIoTシステムに有効な機能

DIAPLANETはIoTシステムを構築するために有効な機能として，M2M通信仮想アプライアンスサーバ，M2M通信仮想アプライアンスサーバと通信するためのゲートウェイ装置にインストールするバンドルソフトウェアや，NoSQL仮想アプライアンスサーバ，その他RDB，DWH，リアルタイム分析仮想アプライアンスサーバなどを提供している。

*インフォメーションシステム統括事業部　**情報技術総合研究所(博士(工学))

## 1. まえがき

モノのインターネットと呼ばれるIoTは，大量の機器からデータを収集して分析することで，マーケティング，機器の故障検知，AI技術を利用した機器の故障予兆への活用や家庭電化製品を外出先から制御したり，機器の故障時に制御を保守拠点から行ったりする遠隔制御への活用が期待されている。当社は2015年４月から三菱電機スマート制御クラウドサービスDIAPLANETの提供を開始している。DIAPLANETのベースサービス(基盤)では，IoTシステムを構築するために必要なM2M通信機能，データベース機能を提供している。M2M通信機能では，M2Mデータ蓄積機能とM2M通信制御機能を提供している。一方，データベース機能では，RDB，冗長構成RDB，NoSQL，DWH，リアルタイムデータ分析機能を提供している。用途に応じて機能を組み合わせることでIoTシステムの構築が可能である[(1)]。

本稿では，DIAPLANETのIoTシステムへの適用分野，主要提供機能及び適用例について述べる。

## 2. DIAPLANETのIoTシステムへの適用

### 2.1 適用分野

DIAPLANETは，IoTシステムのデータ収集，遠隔制御及び両者を備えるシステム構築に対応している。

#### 2.1.1 データ収集

機器の障害検知，電力使用量計測，機器が持つ機能の使用頻度を収集してマーケティングなどに活用できる。

#### 2.1.2 遠隔制御

家庭電化製品を外出先から制御するリモートコントロール，機器の保守及び故障時のオンデマンドな保守情報収集などに活用できる。

#### 2.1.3 遠隔制御及びデータ収集

家庭電化製品のリモートコントロール及び電力使用量最適化制御などを行うHEMS(Home Energy Management System)，MEMS(Mansion Energy Management System)，さらに大規模なTOWNEMS(TOWN Energy Management System)などに活用できる。

### 2.2 IoTシステム向け主要提供機能

DIAPLANETでは，IoTシステムを効率よく構築するためにM2M通信機能及びデータベース機能を仮想アプライアンスサーバとして提供している。

#### 2.2.1 仮想アプライアンスサーバ

仮想アプライアンスサーバは，M2M通信制御，RDBなどの単機能をLinux[(注3)] OS(Operating System)にあらかじめインストール済みで，簡単な設定ですぐに使えるように準備された仮想サーバである。通常，RDBなどの機能を用いる場合には，サーバにOSをインストールし，そのOS上でRDB，セキュリティソフトウェア，監視システム用エージェントなどをインストールし，他のOSからアクセスできるようにネットワークのポートを開放したり，セキュリティの脆弱(ぜいじゃく)性を緩和するために不要なネットワークポートを閉じたり，不要なソフトウェアをアンインストールしたりしなければならない。しかし，仮想アプライアンスサーバでは，これらの処置があらかじめ実施されている。

(注３) Linuxは，Linus Torvalds氏の登録商標である。

#### 2.2.2 M2M通信機能

M2M通信機能としては，機器又はゲートウェイ装置に組み込めるM2Mバンドルソフトウェアとサーバ上で稼働するM2M通信機能仮想アプライアンスサーバを提供している。このM2M通信機能には，データ蓄積とM2M通信制御の２種類がある(**表１**)。

通信方式のポーリングとロングポーリング方式の違い，利点・欠点は**表２**に示すとおりである。

#### 2.2.3 データベース機能

DIAPLANETでは，用途に応じたデータベース機能を提供している(**表３**)。

NoSQLであるCassandraは，大規模データ格納のためにFacebook社が開発したDBであり，現在はオープンソース団体Apache Foundation[(注4)]に寄贈され進化中のソフトウェアである。KVS(Key Value Store)型データベースとも呼ばれ，データアクセスはキーを用いて行う。構造がシンプルであり高速アクセスが特長であるが，ト

**表１．M2M通信機能**

| 機能 | 特徴 |
|---|---|
| データ蓄積 | 機器側からサーバ側にデータを送信する機能及びその戻り値としてサーバ側の指示を機器側に返す機能を提供する。<br>通信方式としてポーリング方式を採用。 |
| M2M通信制御 | 制御端末からの指示を，サーバを経由して機器に送信する機能を提供する。<br>通信方式としてロングポーリング方式を採用。 |

**表２．通信方式の比較**

| 通信方式 | | 説明 |
|---|---|---|
| ポーリング | 方式 | ・機器及び制御端末からサーバ側にデータを送信し，結果を受け取る。 |
| | 利点 | ・高価なネットワーク機器であるファイアウォール，ロードバランサ装置のリソースを占有せず低コストである。 |
| | 欠点 | ・送信の都度，サーバに対し接続を行うため，Webサーバの負荷が高くなる。<br>・機器からの定期的なデータ送信の戻り時に制御情報が伝達されるので即時性なし。 |
| ロングポーリング | 方式 | ・通信開始時に機器からサーバ側に接続した後，サーバから機器側へ制御用のネットワークを張る。制御用セッションは，ネットワークのキープアライブ設定値より前にデータを送信することでセッションを維持し，サーバからの指示を即時に機器へ伝達できる。 |
| | 利点 | ・サーバからの指示は即時性を持って機器側に伝達できる。<br>・機器側に高価なグローバルIPアドレス付与は不要である。 |
| | 欠点 | ・ネットワークのセッションを常時張っていることによって高価なネットワーク機器であるファイアウォール，ロードバランサ装置のリソースを占有し，高コストである。 |

表３．データベース機能

| 提供機能 | 特長 |
|---|---|
| RDB | 汎用的にデータ格納，抽出，削除ができる。トランザクション制御が可能であり，データの信頼性が高い。オープンソースのPostgreSQL(注5)をベースとした商用版のPowerGres(注6)の仮想アプライアンスサーバを提供する。 |
| 冗長化RDB | PowerGresを二重化し，可用性に優れたRDB機能を提供する。 |
| NoSQL | 高速な書き込み処理と高い可用性を特長とする。トランザクション制御機能はない。Key Value Store型データベースであり，キーを用いてデータにアクセスする。３ノード以上で構成するオープンソースの分散型NoSQLであるCassandraの仮想アプライアンスサーバを提供する。 |
| DWH | 大福帳型データベースであるAnalyticMartの仮想アプライアンスサーバを提供する。大量にデータ蓄積されたデータベースからデータを高速に抽出することができる。 |
| リアルタイム分析 | テキストファイルやTCPポートなどからデータを取得し，都度分析を行う機能としてSplunk Enterpriseとの連携を提供する。 |

TCP：Transmission Control Protocol
（注５） PostgreSQLは，PostgreSQLの登録商標である。
（注６） PowerGresは，㈱SRAの登録商標である。

ランザクションの一貫性保証はない。DIAPLANETでCassandraを採用した理由は，主に，高速アクセスが可能であること，スケールアウトによるスケーラビリティの確保が容易であること，最小構成３ノードでの分散型データベースであることの３点であり，１ノードがダウンしてもデータベースシステムは止まることなく稼働し続ける可用性の高さにある。

（注４） Apacheは，Apache Software Foundationの登録商標である。

## 3. IoTシステムへの適用例

### 3.1 IoTシステムの分類

IoTシステムでは，センサ機器の数やこれら機器のセンサデータを集約してサーバ側にデータを送信するゲートウェイ装置の数，通信間隔，可用性，即時性，性能，コストなど，要件が多々ある。**表４**に示すとおりシステムを分類する。

### 3.2 DIAPLANET適用のIoTシステム構成例

DIAPLANETが提供する機能を用いて構築する**表４**の分類に基づくIoTシステムの構成例を次に述べる。

#### 3.2.1 データ収集：実験用途

実験用途では手軽に設計・構築が可能で効果の確認しやすい構成が求められる。この場合は，ゲートウェイ装置でなく汎用パソコンを用いてWebアプリケーションに向けてデータを送る簡単なプログラム作成で対応することが多い。データ分析では，データベース設計が不要ですぐに使えるSplunk Enterpriseを活用する（**図１**）。

#### 3.2.2 データ収集：小規模業務用途

DIAPLANETでは，ゲートウェイ装置に組み込むためのデータ蓄積制御API(Application Programming Interface)バンドルソフトウェア（組み込みLinux用，OSGi(注7)用）を提供している。このバンドルソフトウェアは定期的（ポーリング方式）にサーバ側にデータを送信する。このデータを受信するためのサーバ機能としてデータ蓄積制御機能仮想アプライアンスサーバを提供する。データ蓄積制御で受信したデータはPowerGres仮想アプライアンスサーバに格納することで，Microsoft Excel(注8)など汎用的な分析ソフトウェアを用いてデータ分析を行うことが可能である（**図２**）。

表４．IoTシステムの分類

| 分類 | 用途／条件 | ゲートウェイ数（台数規模は目安） | 構成例 |
|---|---|---|---|
| データ収集 | 実験 | ～数千程度 | 3.2.1 |
| | 業務 | ～数千程度 | 3.2.2 |
| | | 数千以上 | 3.2.3 |
| 遠隔制御 | 数分の遅延可 | ～数千程度 | 3.2.4 |
| | | 数千以上 | 3.2.5 |
| | 数分の遅延不可 | － | 3.2.6 |

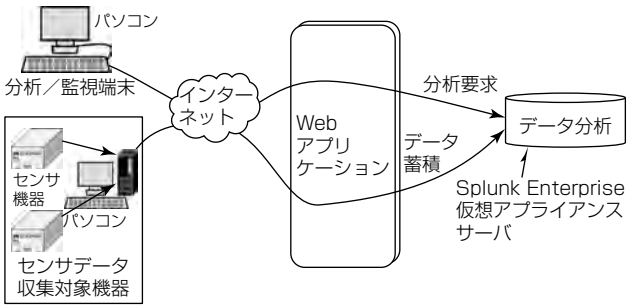



図１．データ収集：実験用途の構成例

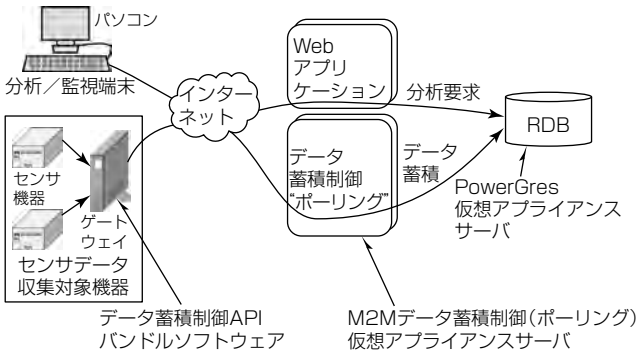



図２．データ収集：小規模業務用途の構成例

（注７） OSGiは，OSGi Allianceの登録商標である。
（注８） Microsoft Excelは，Microsoft Corp. の登録商標である。

#### 3.2.3 データ収集：大規模業務用途

センサからのデータが大量になる場合にはDWH機能であるAnalyticMart仮想アプライアンスサーバを用いる（**図３**）。

#### 3.2.4 小規模遠隔制御：数分の遅延可

即時性を求めず低コストで遠隔制御を行うにはデータ蓄積制御仮想アプライアンスサーバを用いる。データベースは，可用性を向上させるために冗長構成PowerGres仮想アプライアンスサーバを用いる（**図４**）。制御の流れは次のとおりである。

①制御端末からWebアプリケーションにアクセスする。
②WebアプリケーションはM2MデータアクセスAPIを

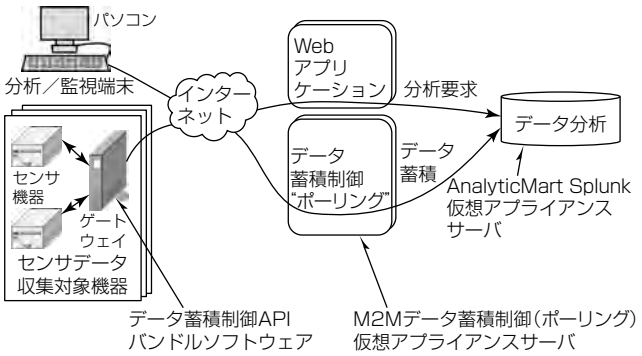



**図３．データ収集：大規模業務用途の構成例**

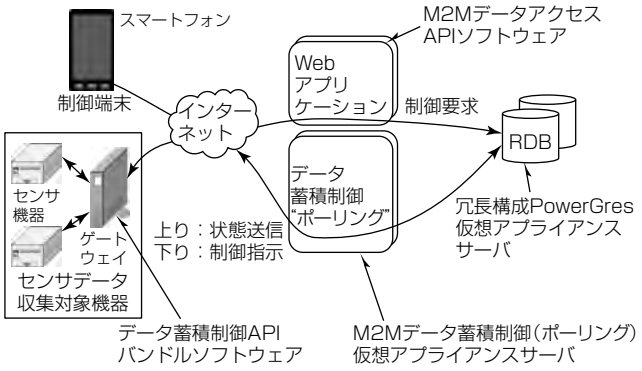



**図４．小規模遠隔制御：数分の遅延可の構成例**

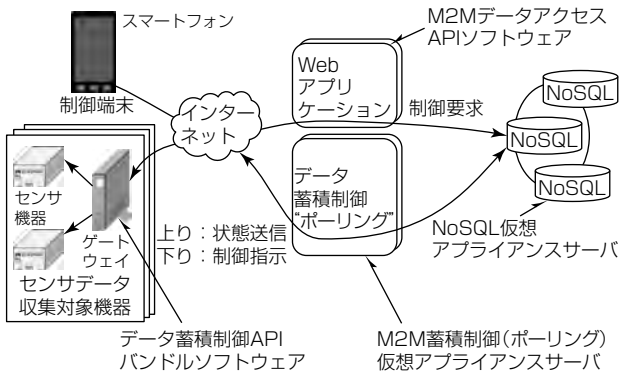



**図５．大規模遠隔制御：数分の遅延可の構成例**

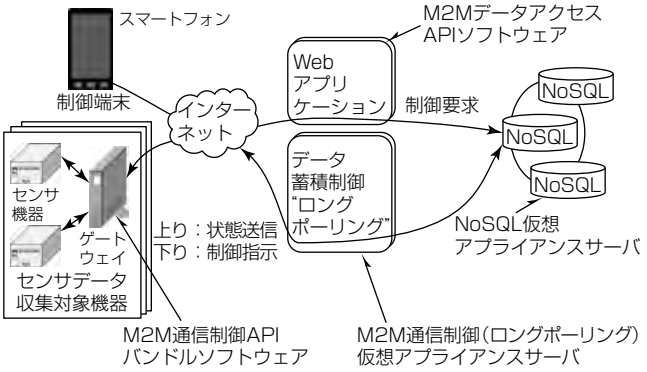



**図６．遠隔制御：数分の遅延不可の構成例**

通して機器への制御指示をデータベースに書き込む。また機器の状態をデータベースから取り出して制御端末に送信する。

③機器側ゲートウェイ装置は定期的に自らの状態をセンサ，データ蓄積制御APIバンドルソフトウェアを用いてデータ蓄積制御仮想アプライアンスサーバへ送信する。

④データ蓄積制御仮想アプライアンスサーバはデータベースに状態を書き込むとともに制御端末から書き込まれた制御指示をデータベースから得て戻り値として機器側に伝える。

### 3. 2. 5　大規模遠隔制御：数分の遅延可

小規模構成と異なりRDBでは多数の機器からのデータ処理に追いつけなくなる。これを回避するとともにデータベースシステムダウンによる影響を防止するために，RDBではなくNoSQL(Cassandra)仮想アプライアンスサーバを用いる(**図５**)。

### 3. 2. 6　遠隔制御：数分の遅延不可

数秒以内での制御の即時性が求められる場合にはM2M通信制御を用いる。機器の状態を確認するには，データ蓄積制御を併用する(**図６**)。機器の状態確認は**3. 2. 4項**，**3. 2. 5項**と同様の方法である。遠隔制御の流れは，次のとおりである。

①ゲートウェイ装置をネットワークに接続すると，M2M通信制御バンドルソフトウェアはM2M通信制御仮想アプライアンスサーバに接続する。この処理で，下り側のネットワークセッションを別に作成し，このセッションを切断することなく利用する。

②制御端末から遠隔制御の指示がなされると，対象とする機器の下りセッションに向けて制御指示が送られる。M2M通信制御バンドルソフトウェアはこれを受けて機器の制御を行う。

## 4. む　す　び

IoT及びM2Mシステムの世界的な動向として，IIC(Industrial Internet Consortium)やoneM2Mなどが規格の標準化を進めている。これら標準化動向を見据えながら，DIAPLANETをMEMS，TOWNEMS及び三菱電機製品のIoTシステムを支える基盤として実証実験などを通じて，完成度を高めて進化させていく。

## 参　考　文　献

(1) 伊藤正裕，ほか：三菱電機スマート制御クラウドサービス“DIAPLANET”，三菱電機技報，**89**，No.8，430～433 (2015)

特集論文

# 三菱電機スマート制御クラウドサービス“DIAPLANET TOWNEMS”

井上和樹*　高須賀史和*
吉田　諒**
塩井川幸保*

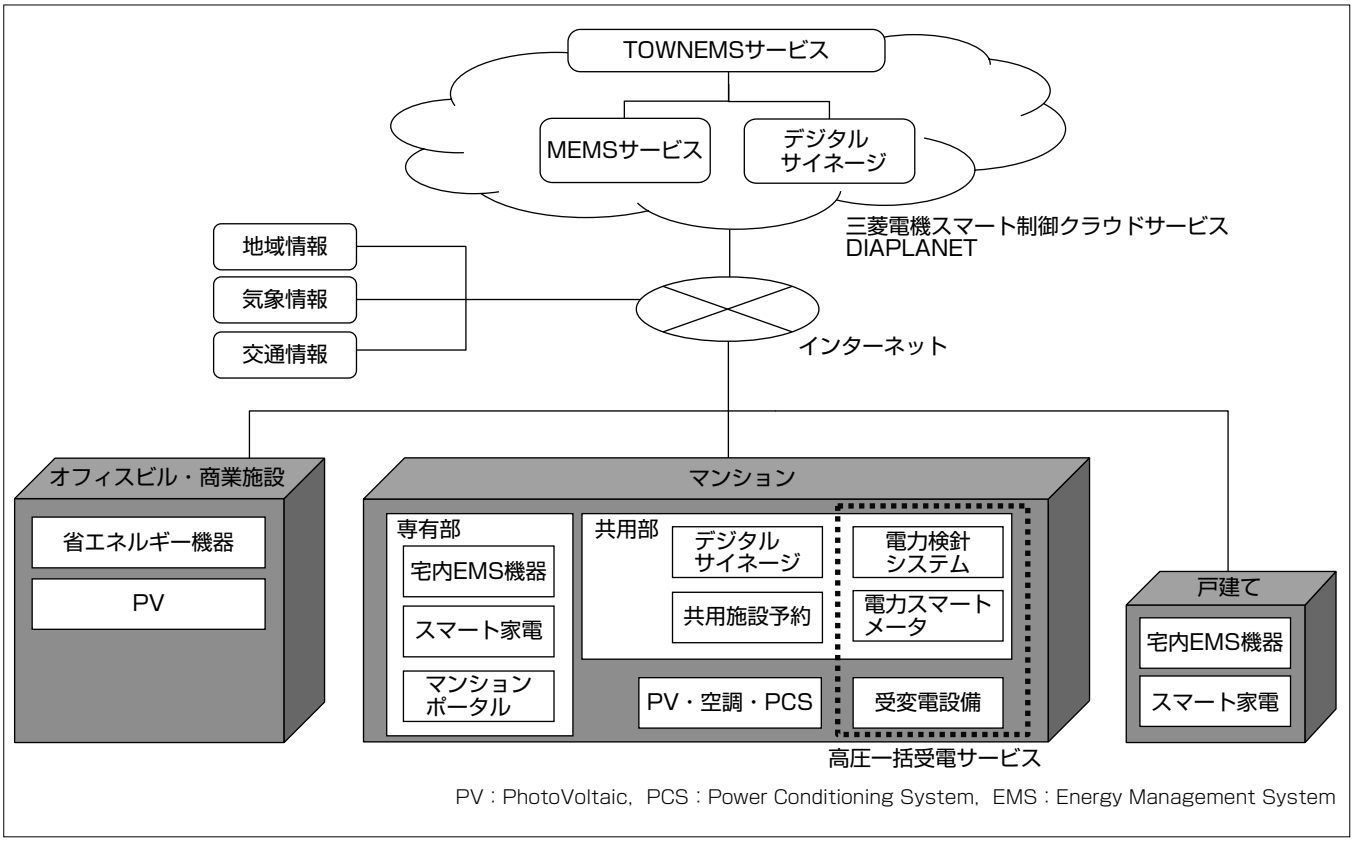
*"DIAPLANET TOWNEMS" : Cloud Services for Town Energy Management Systems*

*Kazuki Inoue, Ryo Yoshida, Yukiyasu Shioigawa, Fumikazu Takasuka*

**要　旨**

三菱電機は，IoT(Internet of Things)及びM2M(Machine to Machine)技術を利用して，複数の家電製品や産業用機器の遠隔制御，稼働状況確認，エネルギー管理などを実現するシステムをクラウド環境上で構築可能にするスマート制御クラウドサービス“DIAPLANET”上のSaaS(Software as a Service)サービスとして，“DIAPLANET TOWNEMS(TOWN Energy Management System)”サービスを2016年６月に販売開始した。

DIAPLANET TOWNEMSサービスは従来のDIAPLANET MEMS(Mansion Energy Management System)サービスとデジタルサイネージを統合した小規模コミュニティ向けのエネルギーマネジメントシステムである。“地域”単位での利用と，エネルギー関連に限らない“暮らし”の視点を取り入れることで，一人ひとりの行動の積み重ねが地域全体への貢献につながり，また，地域の生活環境が良くなることで，個人の生活も更に良くなるという相互作用を生むことを狙ったコンセプトとしている。“エネルギー”“セキュリティ”“アメニティ”の３つのキーワードを軸とし，エネルギー管理や家電コントロール，地域アメニティなどの多彩な機能を高度なサービスとしてマンション全体や街全体に提供する。現在はDIAPLANET MEMSサービスとデジタルサイネージの統合を実現しているが，今後，HEMS(Home Energy Management System)，BEMS(Building Energy Management System)など，他のEMSソリューションと組み合わせることによって，地域全体の最適なエネルギーソリューションの提供を目指していく。




## DIAPLANET TOWNEMSサービス

DIAPLANET TOWNEMSサービスは小規模コミュニティを対象にマンション，戸建て，オフィスビル，商業施設等の電力使用量を収集し，見える化を行う。また，家電コントロール，地域アメニティなどの生活に密着する多彩な機能を提供する。

*インフォメーションシステム統括事業部　**デザイン研究所

## 1. まえがき

スマートグリッドと国内での電力自由化によって，スマートメータの導入を始め，HEMS，MEMS，BEMS等が次々に開発され，スマートハウス，スマートマンション，スマートビルの導入が活発化している。さらに，家庭やビル，交通システムをITネットワークでつなげ，地域でエネルギーを有効活用する次世代社会システムであるスマートコミュニティやICT(Information and Communication Technology)などのテクノロジーを活用し，市民の生活の質を高め，環境負荷を抑えながら成長できる都市システムであるスマートシティの取組みも活発化している。こうした中で，当社は小規模コミュニティをターゲットとし，従来のDIAPLANET MEMSサービス(以下“MEMS”という。)とデジタルサイネージを統合したDIAPLANET TOWNEMS(以下“TOWNEMS”という。)を開発した。TOWNEMSは，マンション全体や街全体の快適な暮らしを実現するために，三菱電機スマート制御クラウドサービスDIAPLANET上で，エネルギー管理や家電コントロール，地域アメニティなどの多彩な機能を提供する。

本稿では，TOWNEMSのコンセプト，構成と提供機能，活用モデル，今後の展開について述べる。

## 2. コンセプト

### 2.1 地域単位のEMS

当社は高圧一括受電事業者向けのMEMSを提供している。MEMSはマンションのエネルギーマネジメント，各家庭の省エネルギー及び光熱費節約が中心であったが，TOWNEMSは，“地域”単位での利用と，エネルギー関連に限らない“暮らし”の視点を取り入れることで，小規模コミュニティへの適用を可能とした。一人ひとりの行動の積み重ねが地域全体への貢献につながり，また，地域の生活環境が良くなることで，個人の生活も更に良くなるという相乗効果を実現できると考えた。

### 2.2 サービスコンセプト

住民同士のコミュニケーションが希薄になりがちな大規模マンションで，TOWNEMSが地域と家族・個人をつなぎ，家庭と地域の情報共有を円滑にすることで，エネルギーにとどまらない地域全体の安心な暮らしを支える役割を担うことを目指した。

TOWNEMSではマンション共用部のデジタルサイネージ，自宅のテレビ，宅外のスマートフォンの3つの機器を選定し，これらを組み合わせることによって幅広い利用者に日常生活の中での自然な利用の機会を提供している。例えば，共用部のデジタルサイネージでは表示器の前を通り過ぎる際に地域のお知らせや地域のエネルギー需給状況を確認でき，自宅のテレビでは高齢者や子供にも使いやすい操作で毎月の電気代や回覧板を閲覧できる。さらに，スマートフォンを使って宅外からでも自宅の状況を確認でき，必要に応じて自宅のテレビにメッセージを送ることもできる。このように，それぞれの状況に合った利用シーンと提供機能の検討を進めた。また，機器それぞれに役割がありながらも，統一性のあるデザインや季節のイベントや時間帯によって，3つの機器の背景画像を連動して変化させ，TOWNEMS全体を通して共通のコンセプトを提供する。

## 3. TOWNEMSの構成と提供機能

TOWNEMSは“エネルギー”“セキュリティ”“アメニティ”の3つのキーワードを軸とした，次の機能を提供する。

### 3.1 “エネルギー”の機能

#### 3.1.1 電力使用量の収集・集計

TOWNEMSは住戸単位，マンション単位，街区単位の電力使用量を管理する。住戸単位では複数台の電力スマートメータのデータを自動検針器で収集するAルート方式と，Wi-SUN(Wireless Smart Utility Network)(注1)通信によって宅内EMS機器でデータを収集するBルート方式に対応している。自動検針器の導入が設置場所や設置距離によって困難である戸建て等はBルート方式で収集して機器構成を使い分けている。

収集したデータはHTTPS(Hypertext Transfer Protocol Secure)通信でDIAPLANETのクラウド環境にアップロードする。DIAPLANETのクラウド環境では街区，マンション，住戸のマスタ情報を管理しており，収集したデータを各単位で集計することで見える化のためのデータを生成する。また，受変電設備にデマンドコントローラを取り付けることによって，マンション全体やビル，商業施設等の一括した電力量情報の収集も可能になる。電力量収集・集計の構成を**図1**に示す。

(注1) Wi-SUNは，Wi-SUN Allianceの登録商標である。

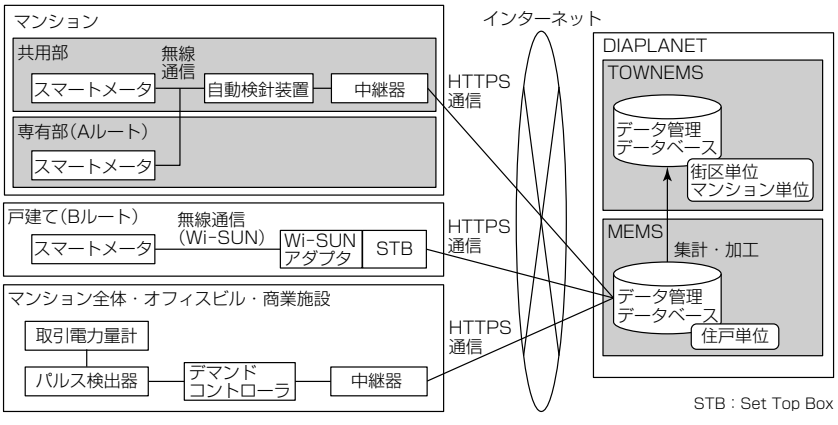



**図1．電力量収集・集計の構成**

### 3.1.2　電力使用量の見える化

**3.1.1項**で収集したデータを用いて，電力使用量の見える化を行う。見える化では住戸単位の情報をテレビ(**図2**)で，マンション，街区単位の情報をデジタルサイネージで表示する。

見える化を行う情報を次に示す。

⑴　30分，日，月単位の電力使用量と電気料金
⑵　時間帯別の電力使用量
⑶　使用量目標値と実績使用量の比較
⑷　節電ランキング(個人，街区単位)

⑴の電気料金については，利用者に電気代単価を設定してもらい電気料金(目安)を算出する。また，高圧一括受電事業者とサーバ間で連携し，前月の請求金額を取得することで，正確な電気料金を表示することにも対応する。高圧一括受電事業者との連携がない場合は通常の目安表示を選択することもできる。⑶の目標値との比較については，目標値のしきい値を超過する前に警告を通知する仕組みを備えており，利用者の節電行動を促す。

### 3.1.3　デマンドレスポンス

TOWNEMSでは高圧一括受電事業者向けのデマンドレスポンス(DR)と地域単位でのDRの機能を持つ。前者はマンション共用部に設置するデマンドコントローラによって，デマンドの監視を行い，目標デマンドを超過する前に警報を発信することで，デマンドのピークカットに対応する。マンションの専有部に対しても時間帯を指定してのDR要請の発信を可能とする。後者は自治体等の要請によって，夏・冬の電力逼迫(ひっぱく)時に地域を運営する管理者から地域単位に時間帯を指定したDR要請を発信可能とする。

## 3.2　“セキュリティ”の機能

離れて暮らす家族の安全を確認するためのツールとして見守り[1]機能を提供する。見守りの内容は住戸単位で収集した過去数日間の電力使用量をDIAPLANETのクラウド環境で分析し，設定したしきい値の範囲外となった際に，通常ではない生活行動と判定し，登録済みのユーザーにメールで通知するものである。

## 3.3　“アメニティ”の機能

### 3.3.1　共有情報の発信

マンションの管理組合や地域の自治会から発信するお知らせや回覧板，アンケートといった情報をインターネット経由で自宅のテレビ(**図3**)，スマートフォン，デジタルサイネージで閲覧できる。回覧板へのサインやアンケートの回答といった行為も自宅のテレビからの送信によって実施できるため，情報共有のスピードを上げることができる。

また，管理組合や自治会の管理者は閲覧状況を閲覧・管理することができるため，周知度を把握することができる。また，アンケートは回答項目ごとの集計を自動で行うため，管理者の業務負荷を軽減できる。


**図2．電力使用量(住戸)のテレビ画面イメージ**


**図3．回覧板のテレビ画面イメージ**

### 3.3.2　地域情報の発信

**3.3.1項**で述べた管理組合，自治会からの管理者機能だけではなく，地域に向けたお知らせ発信機能がある。この機能をショッピングモールや行政，地域運営者が利用することで地域イベントや近隣ショッピングモールからのお得な情報を発信でき，地域の活性化に貢献する。

### 3.3.3　家族伝言板

SNS(Social Networking Service)やコミュニケーションツールの発達によって，スマートフォン，パソコン間でのコミュニケーションが活発化している。パソコンやスマートフォンを所有していない子供や高齢者でも，テレビ，スマートフォン間でメッセージを送受信することによって，家族間のコミュニケーションの場を増やすことができる。

### 3.3.4　外部サイトとの連携

外部の情報提供サービスと連携して生活に密接する鉄道の運行情報，天気予報，災害情報をデジタルサイネージに表示する。また，地域情報や商店街，ショッピングモール等の広告を表示する機能を持っており，地域と住民をつなぐツールとしても利用できる。

# 4.　TOWNEMSの活用モデル

**3章**で述べた機能を活用して次のような利用シーンへの適用が想定される。

## 4.1　地域の環境エネルギー貢献と地域の活性化

省エネルギー・$CO_2$削減を目的としたスマートコミュニ

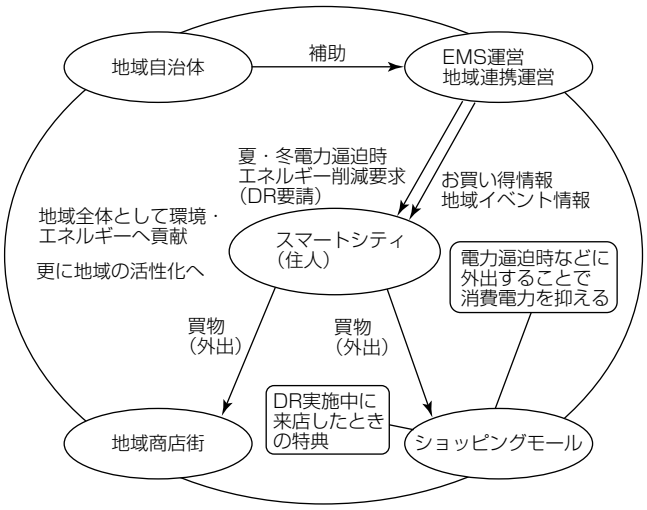



**図４．地域DRの運用モデル**

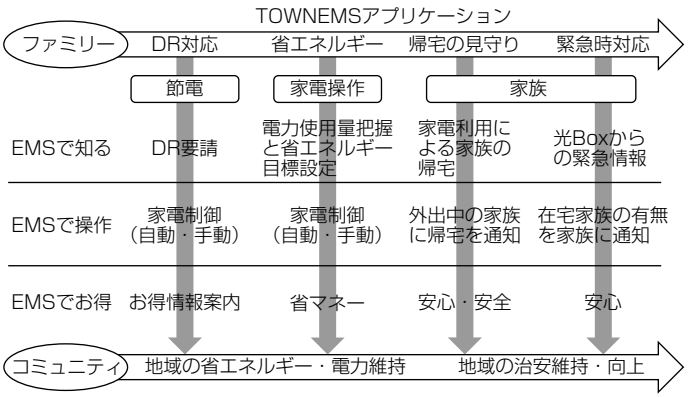



**図５．TOWNEMSの利用モデル**

ティで夏・冬の電力逼迫時に地域全体のエネルギーを削減する場合，地域住民に対して節電行動の呼びかけとしてTOWNEMSの地域DR要請を利用し，DR実施の時間帯を通知する。ただし，要請するだけでは地域住民の協力を得ることは難しい。そこで，地域情報発信の機能や広告の表示機能を利用し，DRを実施する時間帯と同じ時間に近隣の商店街，ショッピングモールのお得情報や地域イベントの案内を発信し，地域住民に該当時間帯の外出を促すことで，地域全体のエネルギーを削減する。また，商店街やショッピングモールは人の流れができることによって，売上増加や新規顧客獲得につなげることができる。

TOWNEMSは，このような利用シーンで環境・エネルギーへの貢献，地域の活性化へ貢献することができる。地域DRの運用モデルを**図４**に示す。

### 4.2　住民行動から地域へのつながり

利用者がTOWNEMSのサービスを受けることで，地域への貢献につながると考える。例えば，電力使用量，電気料金の見える化や目標値超過のアラームの機能を用いることで利用者の日々の節電意識向上と省マネーを手助けする。利用者の節電への意識が高まることによって，高圧一括受電事業者，地域からのDR要請を発信した際に住民の協力体制が築かれていき，利用者の一つ一つの節電行動が地域全体としての省エネルギー・$CO_2$削減につながると考える。

また，家族伝言板を利用して，子供の帰宅を知らせることで外出中の家族に安心・安全を伝えることができる。災害時には在宅中の家族の有無や外出中の家族の状況を連絡することで，家族の安全を確認できる。TOWNEMSの利用モデルを**図５**に示す。

## 5. 今後の展開

TOWNEMSでは既に電力スマートメータとの連携，検針，見える化をサービスとして実現している。2016年４月から開始された電力小売自由化，2017年４月から開始される都市ガス小売自由化によって，ガス会社による電力小売や電力会社によるガス小売が活発化していくものと考える。電気，ガス，水道などのエネルギーをトータルで管理，見える化を行うことによって，ニーズに合致したサービス提供を目指す。また，見守りの分析データとしてガス，水道のデータを加えることで，より精度の高い行動検出，見守りサービス提供を目指す。

ガス，水道メータとの連携方式は，まずはパルス検出器を介してのデータ連携を検討している。将来的なガス，水道のスマートメータの実用化に向け，スマートメータとの連携も視野に入れて検討を進めていく。

## 6. むすび

現在のTOWNEMSはMEMSとデジタルサイネージを統合した小規模コミュニティ向けのサービスである。今後，HEMS，BEMSなど他のEMSソリューションと組み合わせることによって，地域全体の最適なエネルギーソリューションの提供を目指す。

また，“エネルギー”“セキュリティ”“アメニティ”の機能の充実化によって，社会のニーズに合致した快適な暮らしを実現するソリューションを提供していく。

## 参考文献

(1)　塩井川幸保，ほか：三菱電機スマート制御クラウドサービス“DIAPLANET”MEMS，三菱電機技報，**89**，No.8，434～438（2015）

特集論文

# クラウドの活用を支援するハイブリッドクラウドサービス“CloudMinder”

村澤　靖*
今村和幸*
林　雅彦*

*Hybrid Cloud Service "CloudMinder" Supporting Customer's Cloud Computing Use*

*Yasushi Murasawa, Kazuyuki Imamura, Masahiko Hayashi*

**要　旨**

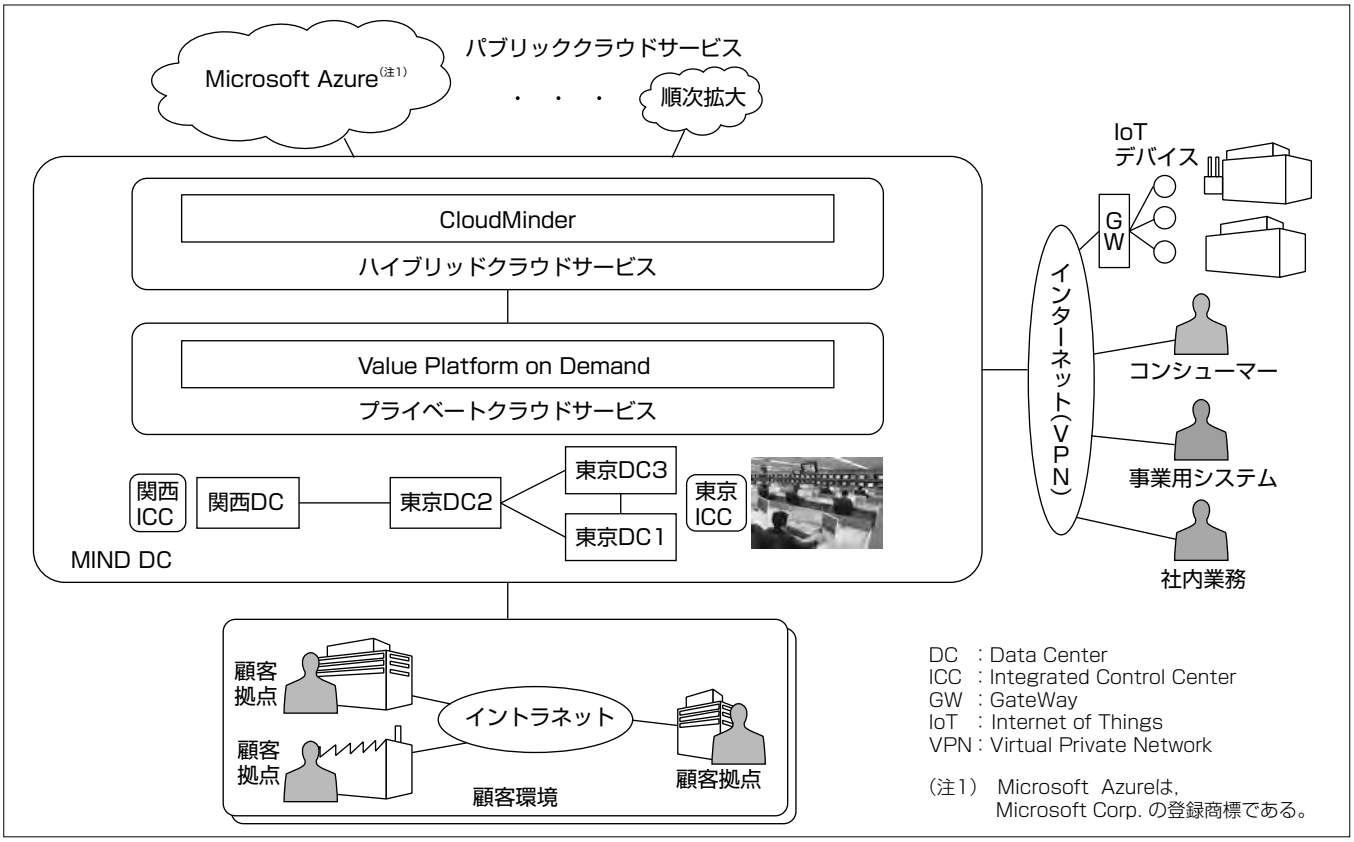
国内のクラウド市場では，プライベートクラウド，特にハイブリッドクラウドにおけるハブ機能や事業拡大の基盤としての役割が同市場の成長をけん引していくことが予想されている。

三菱電機インフォメーションネットワーク㈱(MIND)では，MINDデータセンター(以下“MIND DC”という。)の顧客が安心，安全かつ簡単にパブリッククラウドを利用できるハイブリッドクラウドサービス“CloudMinder”を2016年度から提供開始した。CloudMinderは，次の特長を持つサービスである。

(1) MIND DC内のプライベートクラウドとパブリッククラウドの連携
(2) 安心・安全を確保するセキュリティサービスの提供
(3) 豊富なプライベートクラウド運用実績に基づく運用サービス

MIND DCからパブリッククラウドへの接続ネットワークは，安定性やセキュリティを考慮し，閉域網での接続を提供している。あらかじめ広帯域のアクセスポイントをMIND DC内に設置し，複数の顧客がセキュアかつ帯域保証で利用可能な共有ネットワークを構築した。これによって低コスト，短期間での提供を実現した。

今後，接続ネットワークの延伸やセキュリティ・運用サービスの強化等，順次サービスの拡張を予定しており，MIND DCを核に顧客のクラウド利用に応えていく。




**ハイブリッドクラウドサービス“CloudMinder”の全体像**

ハイブリッドクラウドサービスCloudMinderは，MIND DC内のプライベートクラウドとパブリッククラウドを閉域網で接続し，パブリッククラウドのメリットを活用した顧客のハイブリッドクラウド環境の構築と運用を支援するサービスである。これによって，顧客はプライベートクラウドからパブリッククラウドまで，シームレスに活用することができる。

*三菱電機インフォメーションネットワーク㈱

## 1. まえがき

IDC Japan㈱によれば，2014年の国内プライベートクラウド市場は6,196億円，国内パブリッククラウド市場は1,942億円である。2019年に，それぞれ2014年比3.0倍(1.9兆円)，2.8倍(5,404億円)に達すると予測されている(1)(2)。プライベートクラウドに対する顧客の主な期待はITや業務の効率化であり，ハイブリッドクラウドにおけるハブ機能や事業拡大の基盤としての役割が同市場の成長をけん引していくことが予想されている。

MINDでは，これまで自社で運営するデータセンターを使って，顧客個別のシステムや運用の要件に応えたプライベートクラウドサービスを提供してきた。その一方で近年，短期利用での柔軟性等で優位性があるパブリッククラウドの利用を希望する顧客も増えてきた。パブリッククラウドの利用に当たっては，セキュリティへの不安，システム移行や日常運用に関する手間は解消できておらず，これらを軽減するサービスが求められている。このニーズに応えるため，MIND DCの顧客が安心，安全かつ簡単にパブリッククラウドを利用できるハイブリッドクラウドサービスCloudMinderを2016年度から提供開始した。

本稿では，CloudMinderのサービス概要とパブリッククラウド接続ネットワークを中心に述べる。

## 2. CloudMinderのサービス概要

### 2.1 CloudMinderのサービス提供イメージ

CloudMinderは，MIND DC内のプライベートクラウドとパブリッククラウドを閉域網で接続し，パブリッククラウドのメリットを活用する顧客のハイブリッドクラウド環境の構築と運用を支援するサービスである。**図1**にCloudMinerのサービス提供イメージを示す。

MINDがIaaS(Infrastructure as a Service)としてMIND DC内で提供するValue Platform on Demand(3)上の顧客システムと，Microsoftが提供するパブリッククラウドAzureを接続し，シームレスな活用を実現する。

### 2.2 CloudMinderの特長

(1) MIND DC内のプライベートクラウドとパブリッククラウドの連携
- ①柔軟かつ迅速な拡張性が求められるパブリッククラウド上のWebフロントエンドシステムとプライベートクラウドの基幹系システムの連携を実現
- ②パブリッククラウドをプライベートクラウドのDR(Disaster Recovery)用のバックアップシステムとして活用
- ③パブリッククラウドが提供するPaaS(Platform as a Service)機能(機械学習等)の活用

(2) 安心・安全を確保するセキュリティサービスの提供
- ①閉域網接続によるセキュアかつ高品質なネットワークによってプライベートクラウドとパブリッククラウドを接続
- ②日々発生するセキュリティの脅威から顧客の情報資産を守るアクセス制御，脆弱(ぜいじゃく)性診断等のサービスを提供

(3) 豊富なプライベートクラウド運用実績に基づく運用サービスの提供
- ①24時間・365日の監視サービスを提供
- ②パブリッククラウド利用の契約，利用料支払やリソース確認などの運用に関する手続きを代行

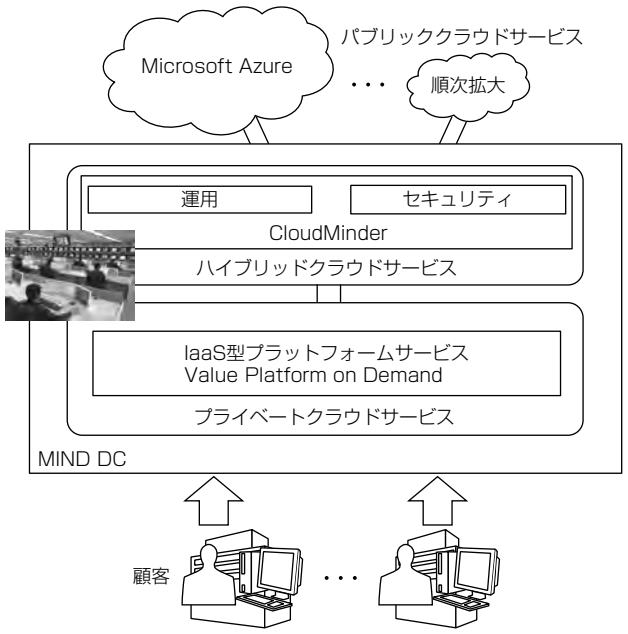



**図1．CloudMinderのサービス提供イメージ**

**表1．サービス項目**

| 項目 | サービス内容 |
|---|---|
| 対象パブリッククラウド | Microsoft Azure |
| 運用 | 利用契約代行，支払代行，監視等 |
| セキュリティ | アクセス制御，脆弱性診断等 |

### 2.3 CloudMinderの提供サービス

CloudMinderで提供するサービス項目を**表1**に示す。

パブリッククラウドの利用で，MIND DCの顧客のニーズが高い機能からサービス提供を開始した。対象パブリッククラウドや運用・セキュリティのサービス内容は順次拡大していく。

## 3. 想定する利用シーン

CloudMinderを利用することで，どのようなことが実現できるか，利用シーンに基づき述べる。想定している主な利用シーンの例を**表2**に示す。

(1) アクセス変動が激しいWebフロントエンドでの利用

パブリッククラウドの特長として，リソース増減が柔軟かつ迅速であることが挙げられる。例えば，インターネットを介して多数の利用者に期間限定の申込みを受付ける

表２．利用シーンの例

| 分類 | 例 |
|---|---|
| アクセス変動が激しいWebフロントエンドでの利用 | ・キャンペーンサイト<br>・多数のIoT機器の接続用サイト |
| 利用頻度が少ないデータや一時的に必要となるシステムでの利用 | ・アーカイブ<br>・評価，検証環境<br>・DR用サイト |
| パブリッククラウドが提供するPaaS機能の利用 | ・機械学習や深層学習によるデータ分析 |

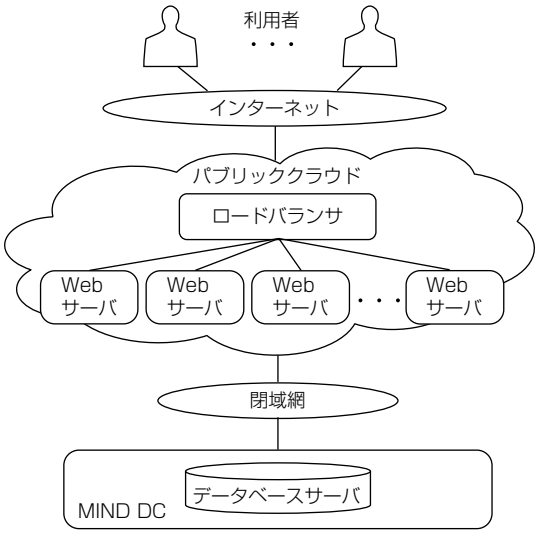



図２．キャンペーンサイトでの利用例

キャンペーンサイトは，**図２**に示すようにパブリッククラウド上にWebサーバを置き，MIND DC内のデータベースサーバと連携したシステムとすることで構築できる。これによって，急激なアクセス変動に柔軟に対応できるとともに，必要なリソースだけを調達することでコスト削減も期待できる。

⑵　利用頻度が少ないデータや一時的に必要となるシステムでの利用

パブリッククラウドでは比較的安価かつ大容量なストレージサービスが提供されている。例えば，大容量のCAD(Computer Aided Design)図面等の技術文書を管理するファイルシステムは，**図３**に示すように一定期間を過ぎたアクセス頻度の低いデータをパブリッククラウド上のストレージにアーカイブとして保管することが可能である。これによって，より安価で必要なだけのストレージ容量を調達することでコスト削減が期待できる。

⑶　パブリッククラウドが提供するPaaS機能の利用

主要なパブリッククラウドサービスプロバイダーでは，IaaS領域から機械学習や開発環境等，PaaS領域でのサービス提供へと注力するようになってきており，PaaS機能として新技術によるサービスが逐次導入されている。例えば，工場の製造ラインの稼働ログ等をMIND DCに収集・蓄積する生産情報分析システムは，**図４**に示すように，パブリッククラウドが提供する機械学習サービスにデータを分析させることで実現できる。これによって，新技術を容易に利用することができる。

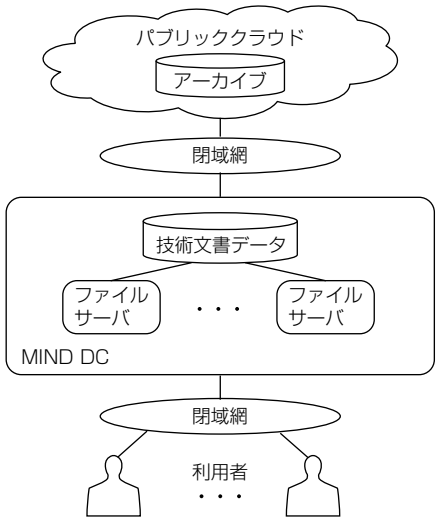



図３．技術文書アーカイブでの利用例

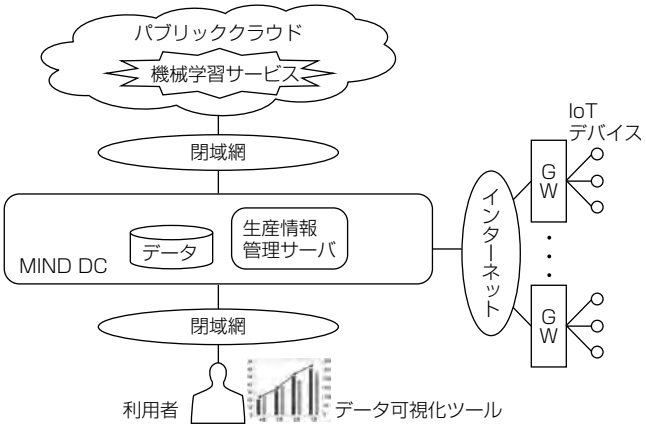



図４．生産情報のデータ分析での利用例

## 4. パブリッククラウド接続ネットワーク

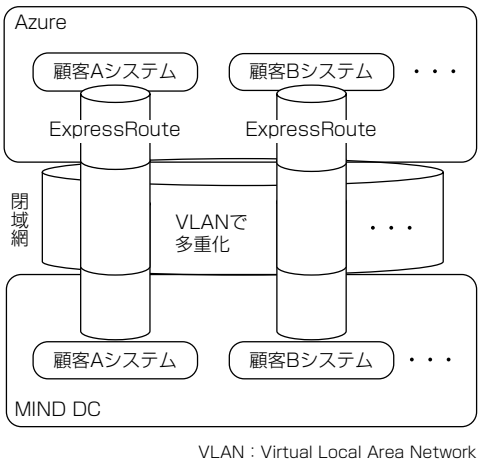
CloudMinderで構築したパブリッククラウド接続ネットワークについて，Microsoft Azure(以下“Azure”という。)を例として述べる。

### 4.1　接続ネットワークの構築

CloudMinderでは，安定性やセキュリティを考慮し，閉域網での接続を提供している。Azureでは閉域網での接続サービスとして，ExpressRoute(注２)⑷が提供されており，閉域網を使ってMIND DCからExpressRouteへ接続を行った。

顧客からの引き合いに応じて接続ネットワークを個別に構築した場合，提供料金が高くなる上に提供するまでの時間がかかるといった課題がある。そのため，Azureとの広帯域のアクセスポイントをあらかじめMIND DC内に設置した。**図５**にその構成を示す。顧客からの受注ごとに，VLAN(Virtual Local Area Network)によって顧客のシステム間をエンドtoエンドで接続する。敷設済みの回線に多重化することで低コスト・短期間(個別に構築する場合と比べて1/2以上に短縮)で，顧客は利用可能となる。

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




VLAN：Virtual Local Area Network

**図5．Azure接続ネットワーク構成**

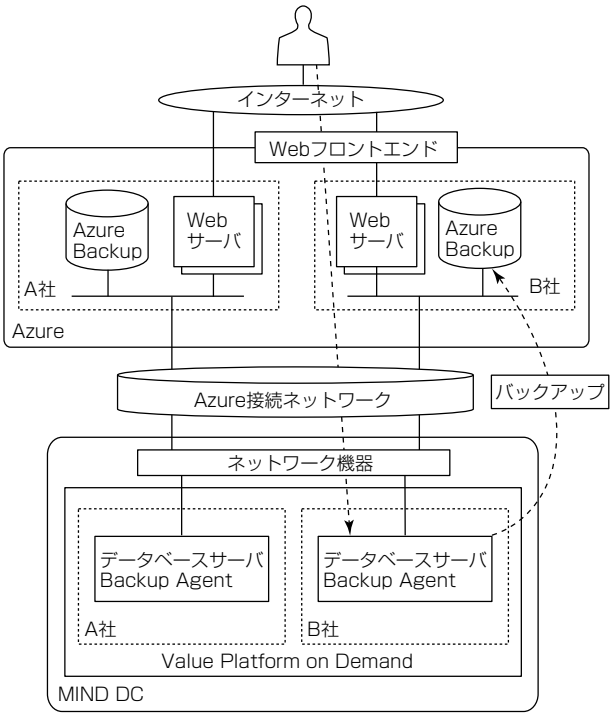



**図6．検証環境の構成**

### 4.2　接続ネットワークの検証

構築した接続ネットワークを経由して，Azureの各サービスとMIND DC内の“Value Platform on Demand”を接続し，Webフロントエンドとバックアップの２つの利用シーンを想定したシステムを構築し，検証を行った。検証環境の構成を**図6**に示す。Azureが提供するバックアップサービスAzure Backupも活用し，A社，B社のマルチテナント構成での検証環境を構築した。

Webフロントエンドの検証では，インターネット経由でAzure上のWebサーバをアクセスし，Value Platform on Demand上のデータベースサーバからデータ読み出しを行った。バックアップの検証では，データベースサーバ内のBackup Agentプログラムにバックアップ情報の設定を行い，Azure上のバックアップ用ストレージへのリモートバックアップやリストアを行った。検証の結果，次のことを確認することができた。

(1)　ネットワークの安定性

MIND DCとAzure間におけるWebサーバとデータベースサーバ間のデータ通信やバックアップデータの送受信で，あらかじめ確保した帯域での安定した通信を確認した。

(2)　ネットワークのマルチテナント利用

A社，B社が物理的に共有したネットワークでも，セキュアな通信を確認した。

## 5. むすび

CloudMinderは順次サービスを拡張予定であり，最後にその方向性について述べる。

(1)　接続ネットワークの延伸

MIND DCの顧客だけでなく，オンプレミスの顧客のシステムに対するパブリッククラウドとの接続ネットワークを提供する。また，接続対象のパブリッククラウドも追加していく。

(2)　セキュリティ・運用サービスの強化

パブリッククラウドの利用拡大に応じて，社員が会社の管理下にないサービスを勝手に利用するシャドーITへの対策やIT全般統制への対応等が必要となる。これまでプライベートクラウドで提供しているログ管理，認証やバックアップ等のセキュリティ・運用サービスを強化していく[5][6]。

今後もMIND DCを核に，顧客がプライベートクラウドからパブリッククラウドまで，シームレスに利用可能とするサービスを提供していく。

## 参考文献

(1)　松本　聡：国内プライベートクラウド市場 2014年の実績と2015年～2019年の予測，IDC Japan㈱（2015）
(2)　松本　聡：国内パブリッククラウドサービス市場 2014年の実績と2015年～2019年の予測アップデート，IDC Japan㈱（2015）
(3)　IaaS型プラットフォームサービス Value Platform on Demand
http://www.mind.co.jp/service/idc_platform/platform/on_demand.html
(4)　Microsoft Azure ExpressRoute
https://azure.microsoft.com/ja-jp/services/expressroute
(5)　砂田英之，ほか：IT全般統制における特権ID管理システムの導入，三菱電機技報，**89**，No.8，470～473（2015）
(6)　村澤　靖，ほか：クラウドシステム構築のためのセキュリティ基盤(1) ―モデルシステムと実証実験―，三菱電機技報，**83**，No.7，411～414（2010）

特集論文

# 機密情報ファイル交換サービス “パッケージプラス トランスポーター”

鈴木　剛*
渡邉優介*

*Confidential Information File Exchange Service "PACKAGEplus Transporter"*

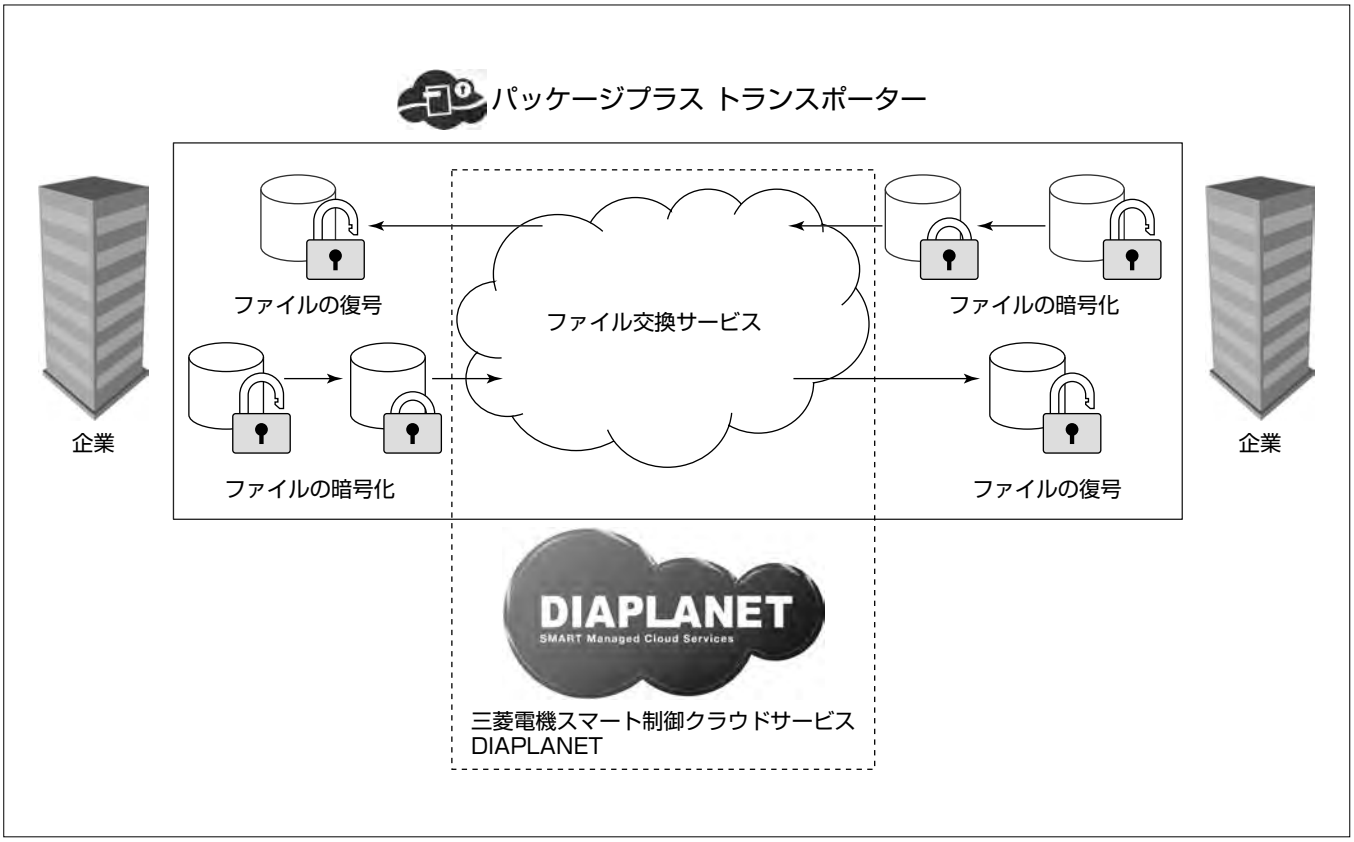
*Takeshi Suzuki, Yusuke Watanabe*

**要　旨**

㈱三菱電機ビジネスシステム(MB)は，機密情報ファイル交換サービス“パッケージプラス トランスポーター”の提供を2016年１月から開始した。パッケージプラス トランスポーターは，三菱電機の“関数型暗号(1)”を実装した三菱電機スマート制御クラウドサービス“DIAPLANET(2)”上で企業間における機密情報ファイル交換を実現する。

機密情報や個人情報の漏えい・改ざんは，ひとたび発生すると企業経営の根本を揺るがしかねない深刻な社会的な問題へと発展するケースが少なくない。一方，従来，紙や電子メディアで行われてきた企業間のデータ受渡しは，ネットワークを介したファイル交換サービスの利用が急速に高まりつつある。

MBでは，このような市場のニーズに応えるため，パッケージプラス トランスポーターによるファイル交換サービスを高セキュリティ・高信頼技術の強みを活用したDIAPLANETを使用して提供することで，企業間での機密情報の安心・安全なファイル交換を実現している。




**“パッケージプラス トランスポーター”のサービス提供範囲**

パッケージプラス トランスポーターは，企業と企業が行うファイル交換を，三菱電機スマート制御クラウドサービスDIAPLANET上で提供している。これによって，安心・安全なファイル交換を実現している。

## 1. まえがき

企業間のデータの受渡しは，紛失・盗難のリスク回避のため，インターネット等のネットワークを介したファイル交換サービスの利用が急速に高まりつつあるが，インターネットの安全性に対する懸念は解消されていない。機密情報や個人情報の漏えい・改ざんは，ひとたび発生すると企業経営の根本を揺るがしかねない深刻な社会的な問題へと発展するケースが少なくない。また，2016年１月から運用の始まった“マイナンバー(注1)”を含んだ特定個人情報の受渡しは，より安全な手段で行わなくてはならない。

MBでは，このような市場のニーズに応え，企業間で機密情報のファイル交換を安心・安全に実現するため，高セキュリティ・高信頼技術の強みを活用したDIAPLANET上でファイル交換を実行するサービスであるパッケージプラス トランスポーターの提供を開始した。

本稿では，このサービスの機能と特長，及び他社サービスにない特長について述べる。

(注１)　マイナンバーは，内閣府大臣官房会計課長の登録商標である。

## 2. パッケージプラス トランスポーターの概要

DIAPLANETは，これまでの大規模システム対応で培った高いレベルのセキュリティと信頼性によって，安心・安全な運用環境を“PaaS(Platform as a Service)”及び“SaaS(Software as a Service)”で提供する。パッケージプラス トランスポーターは，DIAPLANETの提供する“認証認可機能”と“暗号PaaS機能”を利用して企業間等の機密情報ファイルの交換を安心・安全に実現するサービスである。

このサービスでは，ファイル交換相手を設定する機能によって，指定した相手先だけが復号できるという堅牢(けんろう)なセキュリティを維持したファイル交換を実現している。さらに，このサービスでのファイル交換は，クライアント側の“Windows(注2)”アプリケーションで暗号化・復号の処理を行い，暗号化通信HTTPS(Hypertext Transfer Protocol Secure)を組み合わせることで，機密情報をより強固に保護する仕組みを採用した(**図１**)。

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

## 3. パッケージプラス トランスポーターの機能と特長

この章では，パッケージプラス トランスポーターが持っている，安心・安全に機密情報ファイル交換を行うための機能について述べる(**図２**)。

### 3.1　パッケージプラス トランスポーターを構成するツールと機能

このサービスは，機密情報の電子データを交換するための“ファイル交換ツール(通常版，簡易版)”，利用元と相手先の情報等を設定する“権限管理ツール”及びクラウド上で提供するサービスから構成される。各ツールが提供する機能は**表１**のとおりである。

### 3.2　“利用元”と“相手先”の概念

一般のファイル交換サービスでは，送信者と受信者の間で一対一のファイル交換を行うが，このサービスでは，**図３**に示すように利用元と複数の相手先との間でファイル交換が可能である。

利用元は，このサービスを契約した企業や部門であり，複数の相手先とファイル交換ができ，このファイル交換を管理する。相手先は，利用元とだけファイル交換ができる企業や部門である。

また，利用元側では，複数の担当者が利用できるように，担当者別に識別子(IDentifier：ID)を持つことができる。

### 3.3　ファイル交換ツール

機密情報ファイルを安心・安全に交換するためのクライアントツールである。用途によって，複数の相手先とファイル交換を行う利用元が使用する通常版と，相手先が使用

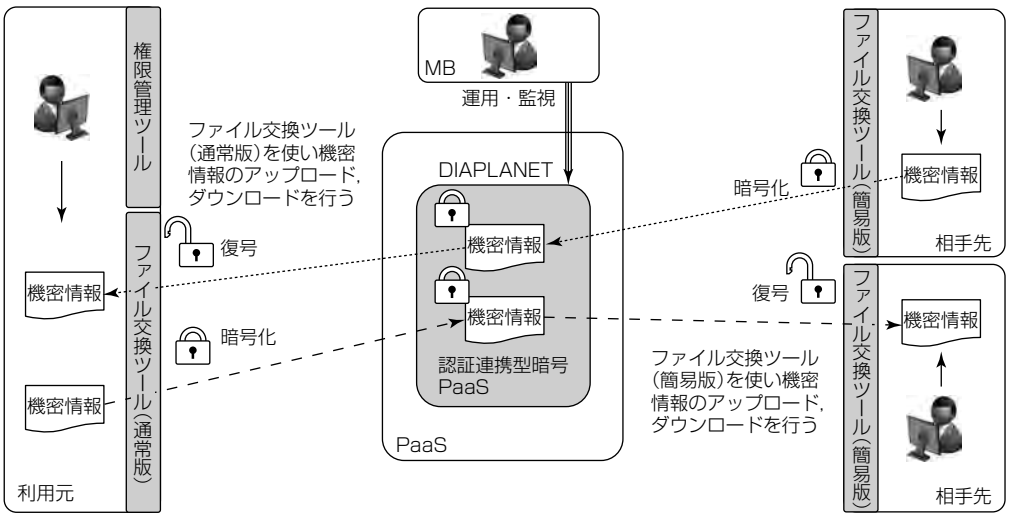



**図１．機密情報ファイル交換サービスの概念図**

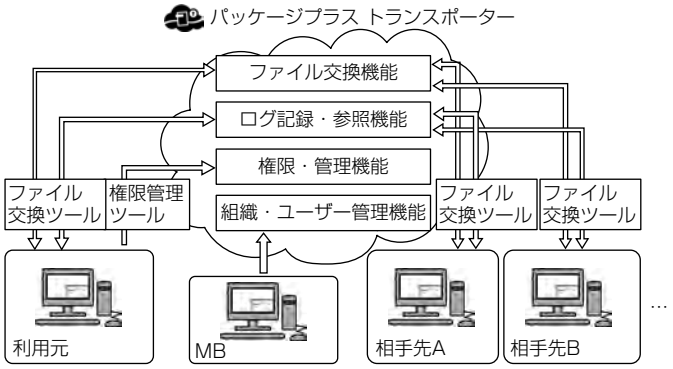



**図2．機密情報ファイル交換サービスの機能**

**表1．機密情報ファイル交換サービスの構成ツール**

| | ファイル交換ツール(通常版) | ファイル交換ツール(簡易版) | 権限管理ツール |
|---|---|---|---|
| 使用者 | 利用元，相手先 | 相手先 | 利用元(管理者) |
| 機能 | ファイルアップロード | | ファイル交換相手設定 |
| | ファイルダウンロード | | 利用者名変更 |
| | ファイル削除 | | 相手先名変更 |
| | ファイル暗号化・復号 | | ファイル領域の初期化 |
| | ファイル交換ログ参照 | | パスワードリセット |
| | ダウンロード通知 | | 変更ログ参照 |
| | 自動ダウンロード | | |
| | パスワード変更 | | |
| | 複数の相手とファイル交換 | — | — |
| | フォルダ管理 | | |

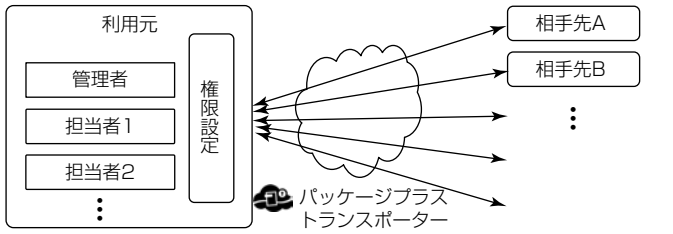



**図3．利用元と相手先の概念図**

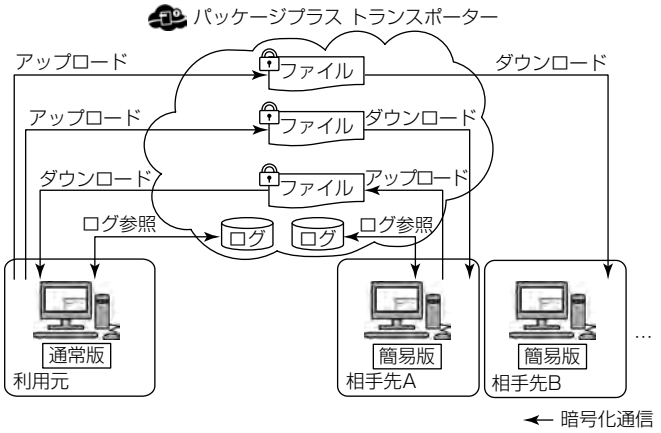



**図4．ファイル交換ツール利用の概念**

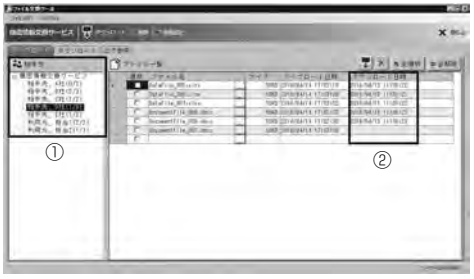



**図5．ファイル交換ツールのアップロード画面例**

**図6．ファイル交換ツールのダウンロード画面例**

する簡易版を用意している。利用できるファイル形式に制約はなく，パソコン等で使用できるファイルであればよい。機密情報のデータファイルだけでなく，プログラムファイル等の交換もできる。

**図4**にファイル交換ツール利用の概念を示す。ファイルを相手先に送信する場合には，ファイル交換ツールを使用してファイルをクラウド上のこのサービスの領域内にアップロードする。送信されたファイルを受信する場合は，ファイル交換ツールを使用してファイルをダウンロードする。

なお，簡易版はファイルの送受信先が1つの場合だけに使用できるように設定されており，操作を簡単に行うことができ，誤送信を防止している。それ以外の機能は通常版と同一である。

### 3.3.1　ファイル交換ツールの機能

利用元で使用する場合，ファイル交換ツールでは権限管理ツールで設定された，ファイル交換可能な全ての相手先を相手先セレクターで一覧することができ(**図5**①)，さらに相手先ごとのファイルのアップロード(送信)及びダウンロード(受信)の状況が確認できる。また，アップロード(送信)したファイルを相手先がダウンロード(受信)し保存したかどうかの状況も把握することができる(**図5**②)。

一方，ダウンロード画面では，相手先が送ってきたファイルの一覧が，相手先ごとに表示される(**図6**)。それらのファイルは，サーバ又はクライアント端末のローカルディスクのいずれかを選択して保存されるが，“環境設定”画面でのパラメータ設定によって，自動的にサーバやクライアント端末のローカルディスクに保存することもできる(**図7**)。

### 3.3.2　操作ログの記録・参照機能

ファイル交換ツールや権限管理ツールを操作した内容はログとして記録され，いつでも参照することができる(**図8**)。

### 3.4　権限管理ツール

“権限管理ツール”は利用元で使用するツールであり，相


**図7．環境設定画面**

**図8．操作ログ参照画面例**

手先の名称や，利用元の名称，利用元の担当者がファイル交換できる相手先を設定することができる(**図9**，**図10**)。また，“権限管理ツール”は，相手先からの要請等によってパスワードをリセットする機能や，利用する相手先が変更になった場合等にファイルの交換領域を初期化する機能を備えている。なお，利用元が設定した利用権限等の設定情報も，契約情報と同じようにクラウド上に保存される。

### 3.5　組織・ユーザー情報の管理

このサービスを利用する組織・ユーザーの情報は，MBが契約情報を基に登録し，クラウド上に安全に保管される(**図11**)。

### 3.6　他社サービスにない特長

⑴　機密性・完全性の確保

機密情報のファイル交換サービスは，暗号化通信によって通信経路を暗号化してファイルの送受信を行っている。万一暗号化通信に脆弱(ぜいじゃく)性問題が発覚してファイルが搾取されても，パッケージプラス トランスポーターの場合はファイル自体に関数型暗号が施されているため，情報漏えいや改ざんを防ぐことができる。また，他社のファイル交換サービスはクラウド上で暗号化・復号が行われるが，このサービスでは利用元で暗号化されたファイルは，指定した相手先が受信するまで復号されないため，ファイルの機密性・完全性を保つことができる(**図12**)。

⑵　個人情報を必要としない

このサービスでは，設定情報に個人情報がなくても利用できることを大きな特長にしており，氏名・メールアドレス等の個人情報は一切必要としていない。自分宛ファイルが送信された場合，メールでの通知があれば便利であるが，このサービスでは，クライアントツールのバックグラウンドでの常駐化機能(タスクトレイ)を備えることで，自分宛のファイルが送信された場合に，自動でダウンロードできる仕組み及びバルーンメッセージによる通知を表示する仕組みを持っている。

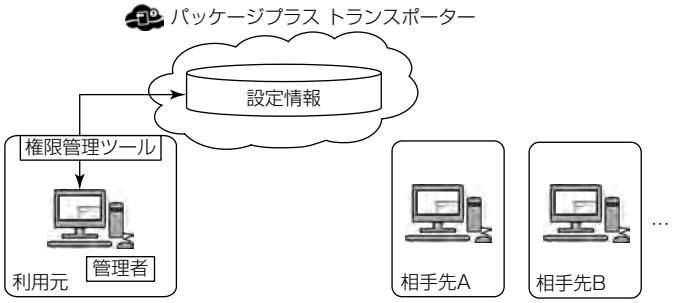



**図9．権限管理ツール**

**図10．権限管理ツールの設定画面例**

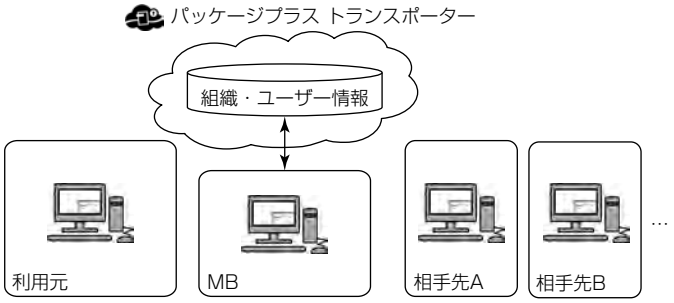



**図11．組織・ユーザー情報の管理**

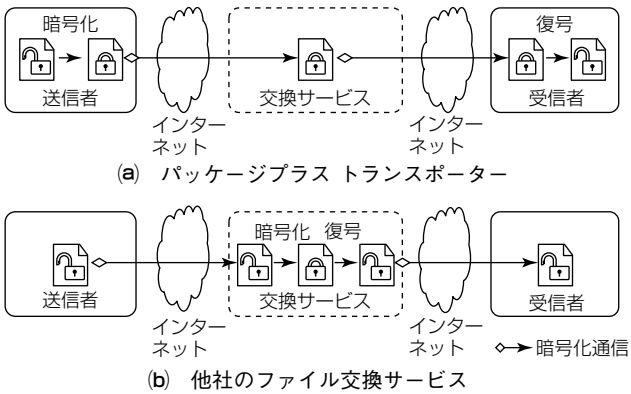



**図12．ファイル交換サービスの比較**

### 3.7　提供サービスの要件

このサービスが提供するサービスの要件は**表2**のとおりである。

表2．提供サービスの要件

| 要件 | 内容 |
|---|---|
| ファイル形式 | 制限なし |
| 使用容量制限 | 5GB/契約企業 |
| ファイル保持期間<br>（ダウンロード済みファイル） | 24時間<br>初回ダウンロードから24時間経過後に自動削除 |
| ファイル保持期間<br>（未ダウンロードファイル） | 30日間<br>初回アップロードから30日経過後に自動削除 |
| 利用者による<br>ユーザーID変更 | 不可能<br>サービス内で一意になる必要があるためMB管理 |
| 管理者による<br>操作ログの一元管理 | 不可能<br>操作ログ表示はログイン中ユーザーの操作に限定 |
| 管理者によるダウンロードファイル保存先の一元管理 | 不可能<br>ダウンロードファイルは操作ごとにユーザーが指定 |

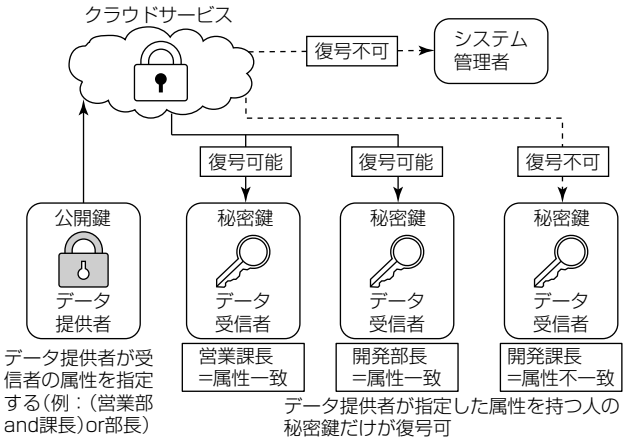



図13．関数型暗号のアクセス権限機能

## 4. 関数型暗号

関数型暗号は，三菱電機が開発した安全性と利便性を両立できる暗号化の仕組みであり，従来の暗号化技術を更に発展させた次世代の暗号化技術としてクラウド時代に求められる高度なセキュリティを実現している。従来の暗号化技術とは異なり，関数型暗号ではアクセス権限の機能を取り入れており，データ提供者が指定した属性を持つ社員の秘密鍵だけでデータの復号を可能としている。これが関数型暗号の大きな特長である（**図13**）。暗号化する場合に，例えば，そのデータの受信を許可する組織上の所属や役職をアクセス権限で定義しておくことによって，仮に復号のための鍵を持っていたとしても，人事異動等で該当の所属や役職等を離れた社員がデータを復号することができなくなるという仕組みになっている。**図13**の例では，復号できる条件を“営業部の課長，又は部長((営業部 and 課長) or 部長)”としているため，開発部の課長やシステム管理者は復号できない。また，人事異動等によって所属部門や職位が変更になり，条件を満たさなくなった場合も復号できない。

先に述べたように組織情報と関数型暗号を組み合わせると細かいアクセス権限を設定できるが，アクセス権限を強

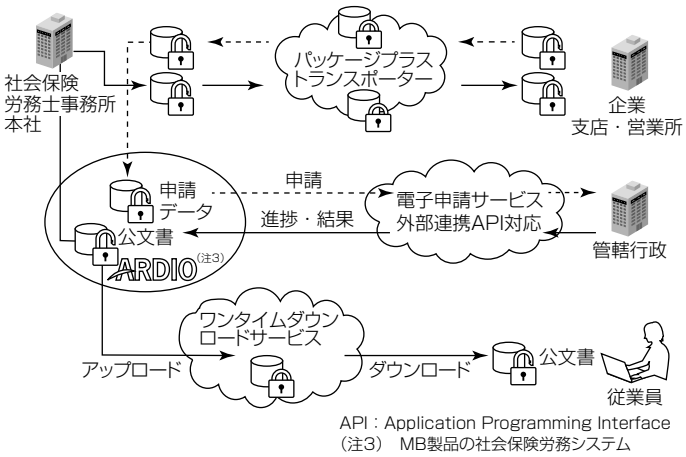



図14．パッケージプラスの機能全体図

化するためパブリックな共有クラウドサービスに組織情報を持ち込むと管理が煩雑になるという課題がある。そこで，パッケージプラス トランスポーターでは，利用元から相手先にデータ送信する場合は個人名宛に秘密鍵を送付する。逆に，相手先から利用元にデータ送信する場合は，個人名宛ではなく利用元の職名宛にファイルを送付する仕組みにして，職務上，アクセスが許可された属性を持つ社員だけがデータを復号できるようにしている。なお，復号に使用する属性を，複雑な組織情報ではなく，一部の役割に限定することによって，関数型暗号の特長を活用しつつ簡便に使用できるように考慮している。

## 5. むすび

今後もファイル交換の利用頻度は高くなることが予想され，より安心・安全なファイル交換等を行うための対策が必要となる。

MBでは，今後増加する電子申請・申告(e-Gov(注4)，“eLTAX”(注5))等のファイル交換をより簡単に，より安全に利用できる仕組みを“パッケージプラス”の製品ラインアップとしてそろえ，安心・安全なファイル交換サービスをサポートするソフトウェアを提供していく（**図14**）。

（注4） 電子政府の総合窓口(e-Gov)は，総務省行政管理局が運営する総合的な行政情報ポータルサイトである。
（注5） eLTAXは，一般社団法人地方税電子化協議会の登録商標である。エルタックス・地方税ポータルシステムの呼称で，一般社団法人地方税電子化協議会が開発・運用主体とする地方税の手続きを電子的に行うシステムである。

## 参考文献

(1) 三菱電機ホームページ：注目の研究・技術 関数型暗号
http://www.MitsubishiElectric.co.jp/corporate/randd/spotlight/spotlight15.html
(2) スマート制御クラウドサービス“DIAPLANET”，三菱電機技報，**90**，No.1，19(2016)
http://www.MitsubishiElectric.co.jp/corporate/giho/1601/pdf/1601007.pdf

特集論文

# 標的型攻撃対策サービス

庄谷卓也*
伊藤久繁*
大野一広**

*Advanced Persistent Threat Detection Service*

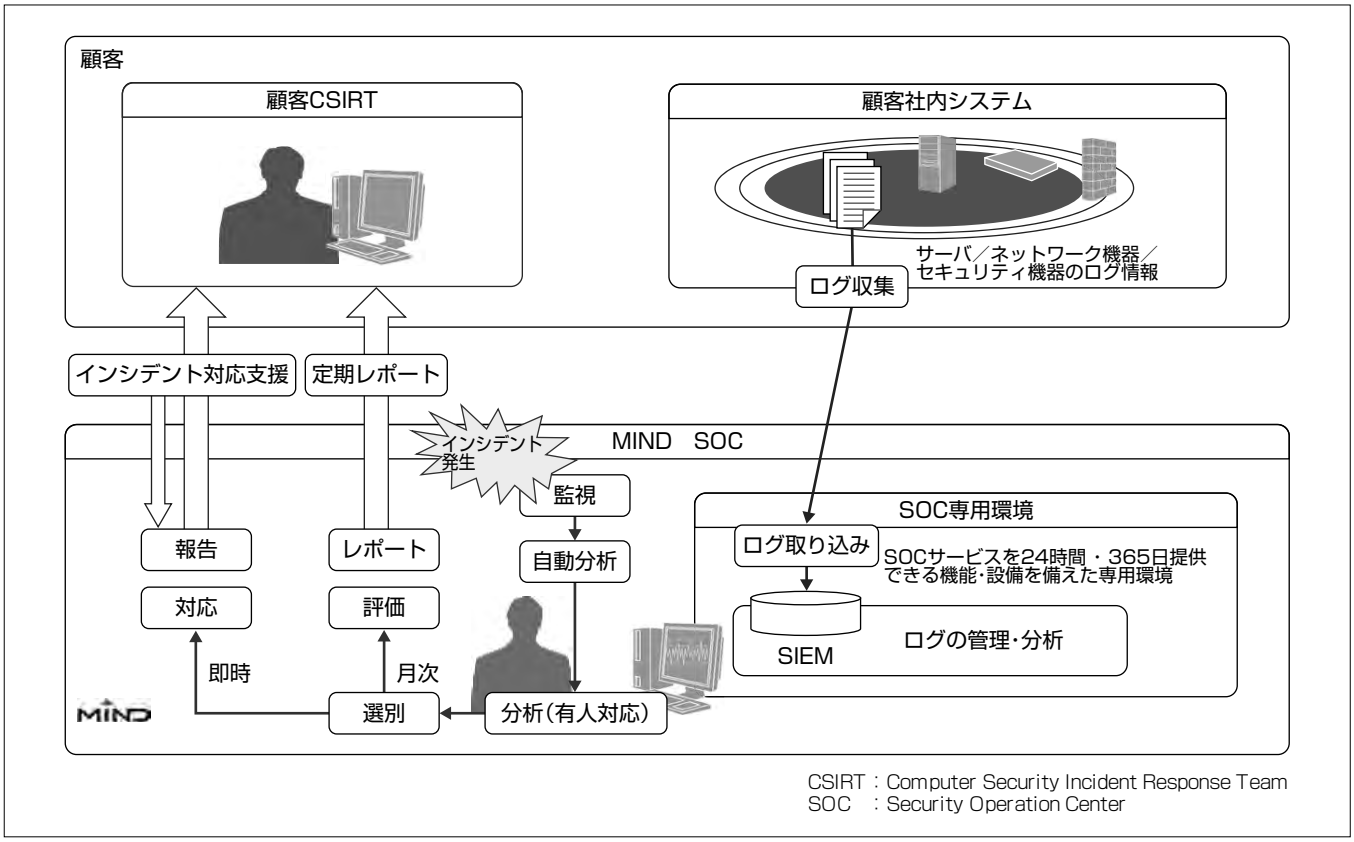
*Takuya Shoya, Hisashige Ito, Kazuhiro Ono*

**要　旨**

企業のイントラネットや工場内の制御システムに対して高度標的型攻撃(Advanced Persistent Threat：APT)と呼ばれる新しいサイバー攻撃が出現している。この攻撃は複数の手口を用いて標的の組織内へ侵入し，長期間にわたり攻撃活動を行う。その際，標的となる組織に特化した攻撃を行うため，従来のサイバー攻撃対策では対応が困難である。被害を受けた組織は機密情報の流出や生産設備の破壊など，企業の経営活動に深刻な打撃を受けることから早急な対策が必要となっている。

三菱電機インフォメーションネットワーク㈱(MIND)は標的型攻撃への対応として，新たに“標的型攻撃対策サービス”の提供を開始した。このサービスはサーバやネットワーク機器などの各種ログを用いてMINDが独自に開発したログ分析ルールによって監視を行う。このログ分析ルールは標的型攻撃の攻撃パターンに沿い，攻撃の各フェーズを幅広くカバーしていることが特長である。これによって，従来のセキュリティ対策の中心であった入口対策だけでなく，組織内部で行われる攻撃者との通信，内部情報の調査，機密情報の送信などの出口対策まで含めた総合的な監視が可能となる。

MINDでは標的型攻撃の検知技術の開発を三菱電機とともに進めており，複数のフェーズにわたって発生する攻撃活動をシナリオ化する手法を導入し，より検知能力の高い標的型攻撃対策を実現していく。




**標的型攻撃対策サービスの概念図**

MINDの標的型攻撃対策サービスでは，顧客システムのサーバやネットワーク機器，セキュリティ機器などのログをSIEM(Security Information and Event Management)と呼ばれる分析システムに一元的に収集し，SIEMに設定した分析ルールによって多角的な観点でログ分析を行うことで標的型攻撃を検知する。攻撃を検知した際は，セキュリティの専門要員が顧客のCSIRTと連携し，インシデント対応をサポートする。

*三菱電機インフォメーションネットワーク㈱　**三菱電機㈱ 情報技術総合研究所(博士(工学))

## 1. まえがき

企業への標的型攻撃は高度化・巧妙化が進み，従来用いられてきたファイアウォールの設置やウイルス対策ソフトの導入などでは十分な対策が困難になりつつある。標的型攻撃の被害は機密性の高い情報の流出や工場設備の破壊など，より深刻度が高く，企業にとって早急に対策すべき脅威となっている。しかし，標的型攻撃は組織内部に入り込んで行われる種類の不正アクセスであることから，分析の観点が多岐にわたる。そのため企業は対策を行うために，分析する人員の養成や費用の確保など多大な負担を要している。

そこでMINDでは，高度化・巧妙化する標的型攻撃に対する企業を支援するため，新たに標的型攻撃対策サービスを立ち上げた。このサービスでは標的型攻撃で発生する攻撃活動の流れを複数のフェーズに分解し，フェーズごとに発生する攻撃の活動を検知する多層的な監視を実現している。監視技術にはMIND独自のノウハウに加え，三菱電機の研究成果を活用している。

本稿では標的型攻撃対策サービスとそれらを実現する技術について述べる。

## 2. 標的型攻撃対策サービス

### 2.1 標的型攻撃対策サービスの立ち上げ

MINDは1998年からセキュリティサービスを提供しており，ICC(Integrated Control Center)と呼ばれる統合運用管制センター内にあるSOCを利用した“プロフェッショナルオペレーションサービス(CyberMinder)”では，セキュリティの専門要員が24時間・365日体制でファイアウォールやIDS(Intrusion Detection System)などの運用・監視サービスを提供している。

近年の標的型攻撃の脅威の高まりを背景に，MINDでは標的型攻撃に対応できる新しいセキュリティサービスの開発検討を行い，2015年11月に標的型攻撃対策サービスの提供を開始した(**図1**)。

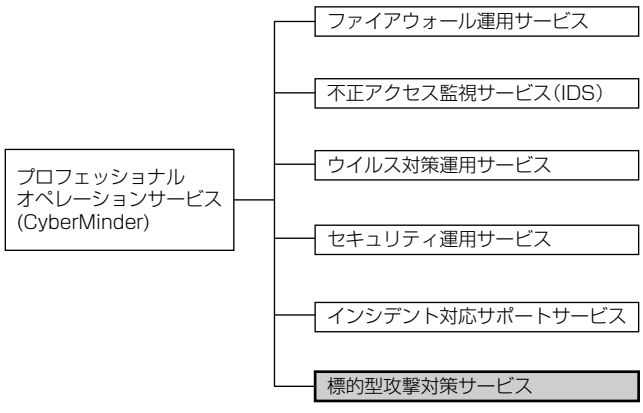



**図1．MINDのセキュリティ運用・監視サービスのメニュー**

### 2.2 標的型攻撃への対策アプローチ

#### 2.2.1 ログ分析による攻撃検知

対応困難な標的型攻撃を検知する方法を検討する中で，MINDでは標的型攻撃が行われた際にシステムの各種機器(サーバ，ネットワーク機器，セキュリティ機器など)のログに様々な痕跡が残る事象に注目した。システムのログ収集を行い，ログのリアルタイム分析によって攻撃の痕跡を発見することで，標的型攻撃の活動を早期に検知することができると考えた。

ログ分析によって標的型攻撃の痕跡を捕らえる仕組みとしてSIEMと呼ばれる分析システムを導入し，複数の機器のログや危険URL(Uniform Resource Locator)などのセキュリティ情報をリアルタイムで関連付けて分析できるようにした。

#### 2.2.2 SIEMによる分析と専門要員による分析

SIEMでは，ログの分析ルールを設定し，収集したログに対して多角的な分析を加えることが可能である。検知精度が高く網羅性のある分析ルールをSIEMに設定することが，標的型攻撃対策サービスの品質に大きく影響する。このサービスの分析ルールについては，MINDの15年以上にわたるセキュリティ監視のノウハウと三菱電機の研究成果を活用して開発を行い，実際にMIND社内で試行して効果を確認した。また，危険URLなどのセキュリティ情報については，セキュリティベンダーの提供する情報を定期的に収集する仕組みを導入し，分析ルールと組み合わせて活用できるようにした。

このサービスでは，SIEMの分析ルールで検知したイベントをそのまま顧客に通知するのではなく，SOCの専門要員がSIEMの出力結果に対して分析を加え，正常な活動を誤検知した可能性や攻撃の深刻度などを総合的に判断した上で，顧客への通知を行う。

#### 2.2.3 攻撃検知後の早期対応

標的型攻撃の活動を検知した際は，顧客のセキュリティ担当窓口へ即時連絡を行う。SOCの専門要員が，攻撃の検知内容や攻撃の進行状況を伝え，その後の顧客のインシデント対応をサポートする。

昨今の標的型攻撃では，攻撃者は長期期間にわたりシステム内に潜伏し，継続的な攻撃を実施するため，攻撃の早い段階で活動を検知することで，実際に被害が発生する前に攻撃をくい止めることが可能となる。

### 2.3 サービス提供方法

標的型攻撃対策サービスを提供する場合，監視対象システムとなる顧客システム内にMINDが提供するログ収集サーバを設置する。ログ収集サーバをMINDのICCに設置されたSIEMと接続することで，ログをリアルタイムで分析することが可能となる。顧客側は，既存機器のログをログ収集サーバに転送するだけで，新たな機器を購入する必要はない(**図2**)。

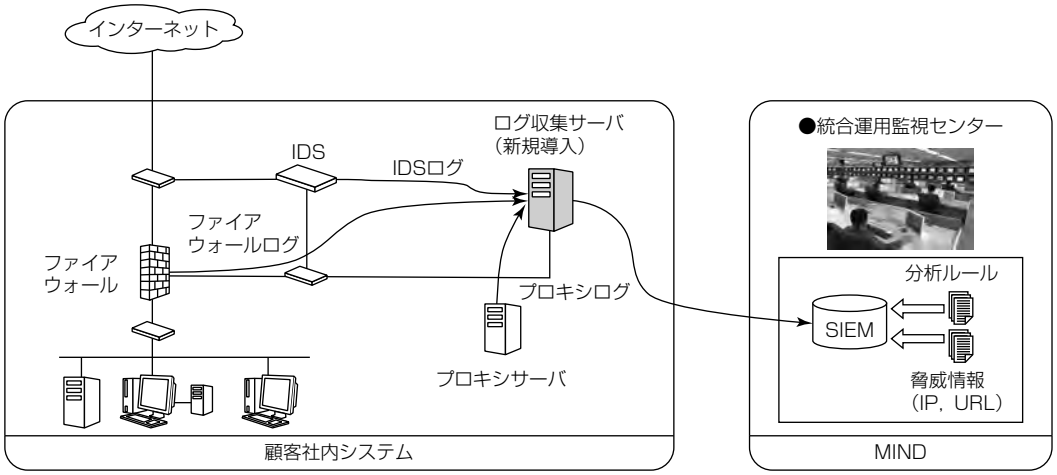



**図２．標的型攻撃対策サービスの提供方法**

## 3. 標的型攻撃の検知技術

### 3.1 高度化・巧妙化する標的型攻撃

**表１**はIPA（(独)情報処理推進機構）が提案する標的型攻撃のフェーズである[1]。このうち組織内部のネットワークで発生する攻撃活動は“③初期侵入”“④基盤構築”“⑤内部調査”“⑥目的遂行”の４つが該当する。近年の標的型攻撃は特にAPT（Advanced Persistent Threat）と呼ばれる高度な手口を駆使する攻撃が増加している。APTは標的とする組織を明確に定める，標的用にカスタマイズされたマルウェアを用いて攻撃活動を行う，１つの標的に対して執拗（しつよう）に再侵入を繰り返すなどが従来の標的型攻撃と異なる。標的となる対象も不特定多数から官公庁[2]，エネルギー企業[3]などの特定の組織が多大な被害を受けた事例が数多く報告され，APTの対策が急速に必要とされている。

従来，組織のセキュリティ対策としてはファイアウォールやウイルス対策ソフトなどの入口対策が主流であったが，APTは組織の内部侵入後の活動が主であり，入口対策だけでは監視できず，十分な対策にはならなくなった。そのため，組織内部の監視を強化するとともに情報の流出を監視し，被害を最小限にとどめる出口対策の必要性が高まっている。

### 3.2 検知技術の開発における課題

標的型攻撃の検知技術を開発するには，個々の攻撃を理解するとともに標的型攻撃における攻撃活動の全体像を把握する必要がある。しかし，各所で報告されている標的型攻撃の事例は，各攻撃の目立つ箇所を重点的に取り上げる傾向があるため，これらの事例を単純に集約して検知技術の軸となる項目を抽出した場合は網羅性に欠ける可能性が高い。また，標的型攻撃の事例は多数発生するため，どの事例が検知技術の開発対象として取り入れるべき高度なものであるか，既存の技術で対応可能な平凡なものであるかの比較が容易ではない。そのため，標的型攻撃を網羅的に分析する基準を設定する必要があった。

**表１．標的型攻撃のフェーズと攻撃活動**

| フェーズ | 攻撃活動 |
|---|---|
| ①計画立案 | 標的となる企業・組織を探索，調査 |
| ②攻撃準備 | 攻撃者が利用するサーバの設置 |
| ③初期侵入 | 標的型メールや悪意のあるWebサイト閲覧を介してマルウェアが感染 |
| ④基盤構築 | 感染した端末にバックドアを作成，攻撃者と通信を行いマルウェアが動作開始 |
| ⑤内部調査 | 組織の内部システムの機密情報の所在を探索，特定してデータを取得 |
| ⑥目的遂行 | マルウェアが攻撃者へ機密情報を送信 |
| ⑦再侵入 | バックドア経由で侵入し④⑤⑥を実施 |

### 3.3 検知技術の開発手順

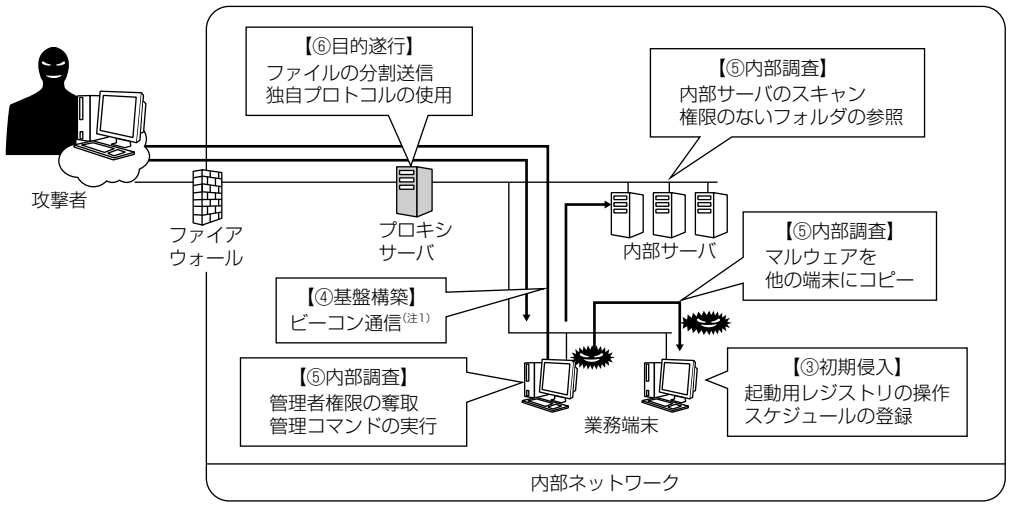
検知技術の開発は次の３つのステップで進めた。

ステップ１：網羅的な評価基準による標的型攻撃の事例調査

ステップ２：標的型攻撃の検知方式の検討

ステップ３：SIEMシステムへの実装

ステップ１では標的型攻撃の攻撃活動の分析モデルとして**表１**の標的型攻撃のフェーズを用いる。このモデルを基に標的型攻撃の事例をフェーズごとに発生した攻撃活動，攻撃活動の発生順序，痕跡の発生する機器，攻撃の実現性などの観点から分類する。これによって多数の事例と攻撃フェーズの特徴に基づいた検知技術の検討が容易となる。痕跡の発生する機器は攻撃活動の具体的な手口を解析することで導出する。攻撃者は攻撃活動中に端末の内部情報へのアクセスやネットワークを経由した通信などを行うことから，攻撃の手口の具体的な手順を明らかにすることで多数存在する機器の中から監視すべき対象の特定が可能になる。**図３**に組織内のネットワークで発生する攻撃活動と手口の一例を示す。③初期侵入では，マルウェアに感染した端末の起動用レジストリの操作が行われ，端末の再起動後もマルウェアが継続して動作するようスケジュールの登録が行われる。④基盤構築では，マルウェアが攻撃者の




（注1） ビーコン通信は，攻撃者がマルウェアに感染した端末の死活監視を行い，遠隔操作が可能な端末を把握する活動

**図３．標的型攻撃で発生する攻撃の手口**

用意したサーバとWebアクセスの経路を利用してビーコン通信を行い，新しい攻撃ツールなどをダウンロードする。⑤内部調査では，攻撃基盤を利用し，内部サーバや端末を探査し，管理者権限の奪取や，マルウェア感染を広げたりしながら，機密データを探す。⑥目的遂行では，内部調査で取得した機密データを，ファイル分割することや，独自プロトコルを利用するなどして，見つからないように外部に持ち出す。

ステップ２ではステップ１の結果を基に標的型攻撃で行われる攻撃活動の検知方式を検討する。このステップでは攻撃の手口の解析結果から得られた装置間の通信記録や各装置の内部情報(設定ファイル，ログファイル，一時ファイル，レジストリなど)から攻撃の特徴となる情報を抽出し，その特徴の検知アルゴリズムを設計する。

ステップ３ではステップ２で設計した標的型攻撃の検知アルゴリズムを標的型攻撃対策サービスで運用するSIEM上で動作する分析ルールとして実装する。

### 3.4　標的型攻撃の検知方式

標的型攻撃の検知方式として④基盤構築フェーズで発生するビーコン通信を例に述べる。ビーコン通信は攻撃者がマルウェアに感染した端末の死活監視を行い，遠隔操作が可能な端末を把握する活動である(**図４**)。ビーコン通信の主な特徴は，次の２点である。

⑴　短い周期で継続して発生する。
⑵　一定の間隔で通信が発生する。

多くのマルウェアでは，ビーコン通信は**図４**の四角形で示すパターンで発生する。ビーコン通信は攻撃者とマルウェアとの間で最短５秒に１回程度の周期の通信が継続する。ビーコン通信は攻撃者との間で死活確認が完了するまで数分間から数時間の通信が継続するが，人間が行うWebサイトへの通信は**図４**の丸印で示すパターンのとおり短時間で完結する。そこで，同一の宛先へ多数発生した通信の継続をルール化して人による通信と区別する。また，**図４**のパターンに示すとおりビーコン通信の間隔はマルウェアによって差があるが，通信の間隔はほぼ一定である一方，人による通信は不定期であることに着目し，同一の宛先に対する一定間隔の通信を抽出する方式をルール化する。これらのとおり標的型攻撃で行われるビーコン通信を時間軸と通信間隔の両面から監視する。さらに，MINDのサービス運用経験から得られた通信プロトコルの特徴を反映することで誤検知を抑制する。

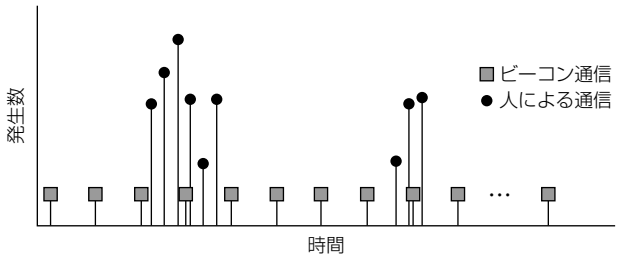



**図４．ビーコン通信のイメージ**

## 4.　標的型攻撃対策サービスの今後

標的型攻撃を検知するための特徴と考えられる通信や端末の内部情報は，正常な活動によって同種の通信や内部情報が発生することで誤検知となる場合がある。例えば，⑤内部調査フェーズで攻撃者が行う重要書類の存在するフォルダへのアクセスとアクセス権限のない正規ユーザーのフォルダへのアクセスは同一の特徴を持つ。しかし，マルウェアが感染した端末からファイルサーバ内の重要書類へアクセスした場合，④基盤構築フェーズでビーコン通信を検知した端末であったことを事前に把握できれば重要書類へのアクセスが標的型攻撃である可能性が高くなると考えられる。

標的型攻撃のフェーズごとに攻撃活動を監視する現在の

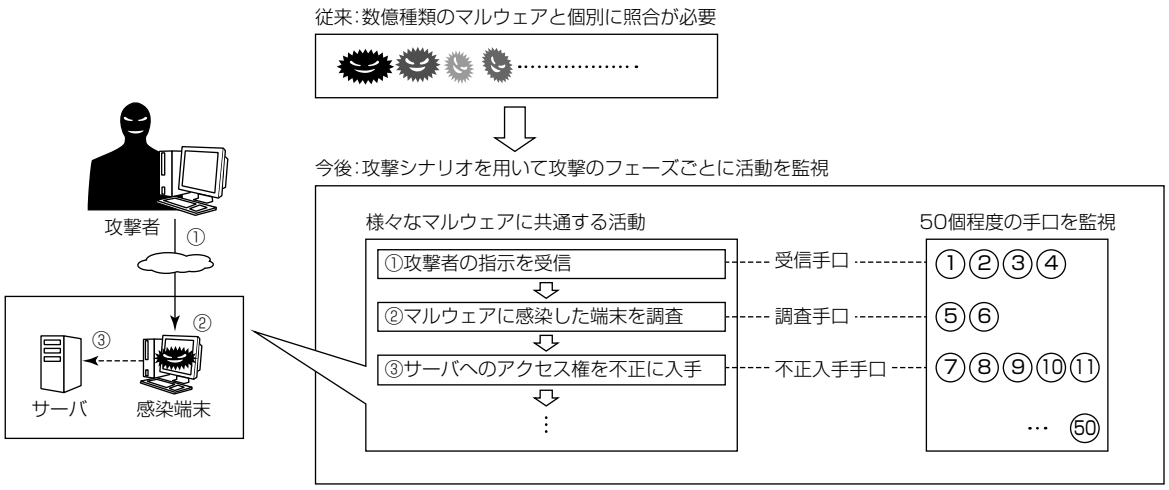



**図５．シナリオを用いた標的型攻撃対策**

技術に加え，攻撃シナリオに基づくサイバー攻撃検知技術を三菱電機が開発した[4]（**図５**）。この技術ではマルウェアの活動の分析から分類した標的型攻撃の目的達成のために必ず実施される50個程度の攻撃の手口を監視する。さらに，攻撃の手口が**図５**に示す“①攻撃者の指示を受信”“②マルウェアに感染した端末を調査”“③サーバへのアクセス権を不正に入手”など一連の流れとして想定される攻撃シナリオに沿ったものかを相関分析して確認する。この技術によって，仮に攻撃の手口と類似した正規ユーザーの活動が発生した際も，攻撃シナリオに沿った活動でなければ正規の活動であると識別が可能になり，より精度の高い検知を可能にする。現在は，専門要員で行っているこの判断をSIEMの分析ルールに組み入れることで，今後この手法をより広くサービスで活用していく。

## 5. むすび

企業における重大な脅威となっている高度な標的型攻撃への対応として，MINDマネージドセキュリティサービスに追加した標的型攻撃対策サービスについて述べた。高度な標的型攻撃は従来行われてきた入口対策では検知が困難である。そこで，組織内に侵入後のマルウェアの活動や機密情報の流出などを監視し，被害を最小限にとどめる出口対策が組織にとって重要となっている。

今後MINDでは標的型攻撃の出口対策の高度化に取り組み，企業の経営活動に打撃を与える不正アクセスの対策を支援するサービスの提供を継続していく。

## 参考文献

(1) (独)情報処理推進機構(IPA)セキュリティセンター：「高度標的型攻撃」対策に向けたシステム設計ガイド(2014)
http://www.ipa.go.jp/files/000046236.pdf
(2) サイバーセキュリティ戦略本部：日本年金機構における個人情報流出事案に関する原因究明調査結果(2015)
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
(3) FireEye, Inc.：CYBER THREATS TO THE NORDIC REGION (2015)
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf
(4) 三菱電機ニュースリリース2016年2月17日：「サイバー攻撃検知技術」を開発
http://www.MitsubishiElectric.co.jp/news/2016/0217-f.html

特集論文

# サイバーセキュリティに対する包括的対策

田中　朗*
惣名和啓*
末永信治*

*Comprehensive Security Operations for Cybersecurity*

*Akira Tanaka, Kazuhiro Somyo, Shinji Suenaga*

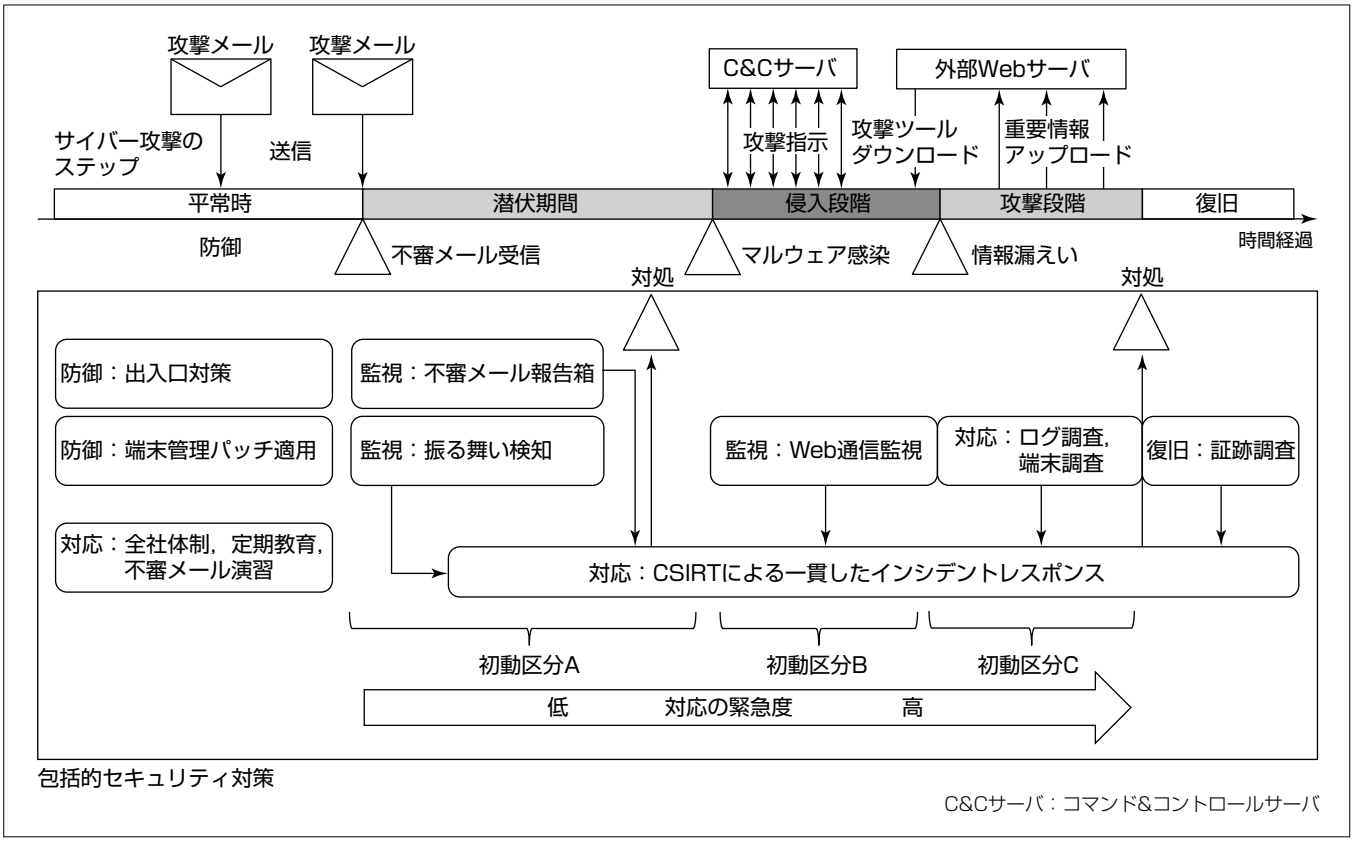
**要　旨**

企業におけるサイバーセキュリティ対策はこれまでの防御対策中心から監視，対応に重点を置いた，事故前提の組織的，技術的対応が必要な時代になってきている。万が一のインシデント発生時の対応体制としてCSIRT（Computer Security Incident Response Team）設置が要請されているものの，運用まで整備できている組織は多くない。

三菱電機インフォメーションネットワーク㈱（MIND）では各種セキュリティ機器を使用した出入口対策，パッチ適用，ウイルスソフトウェアパターンの自動更新などの端末管理対策及び教育，訓練等の防御を中心とした対策を実施してきている。

さらに昨今の高度なサイバー攻撃に対して，サイバー攻撃の各ステップを分析し，監視，対応対策を強化する包括的セキュリティ対策を全社プロジェクトとして推進して運用を開始した。

一貫したインシデントレスポンス体制整備及びセキュリティ専門家をアサインしたCSIRTを新設し，防御対策をすり抜けてきた不審な活動の監視機能を追加した。また，監視の結果を活用して防御対策にフィードバックすることによって導入済みのセキュリティ対策を有効活用すること，及び経営層を含めた対応訓練を実施することで，日々変化する攻撃に対してプロアクティブな防御活動を行い，重要情報漏えい発生のリスクを軽減できている。




包括的セキュリティ対策

C&Cサーバ：コマンド&コントロールサーバ

**サイバー攻撃のステップと包括的セキュリティ対策による対応**

サイバー攻撃のステップに対応した包括的セキュリティ対策による対応を示す。早期の段階である潜伏期間に対処を完了することを目標として監視機能の強化及びインシデントレスポンス体制を整備した。侵入段階，攻撃段階では対応の緊急度が高くなり，より迅速な対応が求められ，端末調査や証跡調査による発生事象の調査が必要であることを示す。

*三菱電機インフォメーションネットワーク㈱

## 1. まえがき

企業でサイバーセキュリティは経営リスクの重要な項目になりつつあり，“サイバーセキュリティ経営ガイドライン⑴”では経営的観点でセキュリティ対策を適切に実施するために，セキュリティ責任者であるCISO(Chief Information Security Officer)を中心に経営とセキュリティの現場が連携してPDCA(Plan，Do，Check，Act)を実施することが求められている。

MINDでは従来実施している防御を前提としたセキュリティ対策を基本に，サイバー攻撃に対応した監視機能の強化及びCSIRT設立によって，組織的，技術的レベルアップを包括的セキュリティ対策として推進した。

本稿では包括的セキュリティ対策で整備した運用を含めた施策について述べる。

## 2. サイバー攻撃の整理

### 2.1 攻撃メールによる侵入方法

サイバーセキュリティ対策を適切に実施するには，攻撃手法を理解することが必要である。サイバー攻撃の侵入経路としてはUSBメモリなどの媒体を介しての攻撃もあるが，電子メールとWebページへのアクセスが多く利用されている。現在，初期侵入に最も多く利用されている電子メールによる攻撃手法について分析する。

電子メールを利用した初期侵入方法は，次の４つに分類される。

⑴ マルウェアと呼ばれる悪意を持った実行可能なプログラムをメールの添付ファイルで送付する方法
⑵ Office文書やPDF(Portable Document Format)文書又は画像ファイルを添付ファイルで送付する方法
⑶ 実行可能なプログラムをダウンロードするWebのアクセス先を示すURL(Uniform Resource Locator)をメール本文に記載して送付する方法
⑷ 不正Webサイト又は改ざんされたWebサイトのURLをメール本文に記載して送付する方法

⑴から⑷の侵入方法とそれらが攻撃に利用する脆弱(ぜいじゃく)性との関連を**表１**に示す。

最近では文書ファイルに見せかけた実行可能なプログラムが添付される方法もあるが，実体がプログラムである場合は方法⑴と分類する。この分析の結果，ソフトウェアの最新セキュリティパッチを適用することによって，防止できる対策は，方法⑵と⑷であり，方法⑴と⑶に対しては他の対策が必要であることが分かる。

**表１．侵入方法と攻撃に利用する脆弱性**

| 侵入方法 | 利用する脆弱性 |
|---|---|
| ⑴ 実行プログラム添付 | ユーザー操作 |
| ⑵ 文書ファイル添付 | ソフトウェアの脆弱性 |
| ⑶ URLリンク記載 | ユーザー操作 |
| ⑷ URLリンク記載 | ソフトウェアの脆弱性 |

### 2.2 攻撃のステップ分け

初期侵入をきっかけに攻撃は段階的に進められていくが，一般的にサイバー攻撃の手順は攻撃側の視点で整理されている。ここでは防御側での視点で，観測される事象の違いに合わせたステップ分けを行った。

⑴ 潜伏期間

不審メールを受信してユーザーが実行するまでの期間を潜伏期間と定義した。ユーザー操作によってメールに添付されたマルウェアを実行するか，文書ファイルを開封する，又はURLのリンクをクリックすることによってエンドユーザーのパソコンに感染して，初期侵入が成功する。

⑵ 侵入段階１

エンドユーザーのパソコンに初期侵入したプログラムは，許可されている社内からインターネットへのWebアクセスを利用してC&Cサーバに定期的に接続し，攻撃者からの指示を受け取る。

⑶ 侵入段階２

C&Cサーバから送られる攻撃者の指示に従い，追加の攻撃用プログラム(攻撃ツール)を外部Webサーバからダウンロードしてパソコンにインストールを行う。

⑷ 侵入段階３

攻撃ツールを利用して，社内ネットワークやサーバの情報収集を行い，ターゲットとなる重要なサーバ及びデータを見つける。

⑸ 攻撃段階１

重要なサーバ及びデータを発見して取得したら，外部Webサーバに重要情報のアップロードを実行して目的を達成する。

⑹ 攻撃段階２

さらに他の社内パソコン，サーバへの感染，侵入を繰り返していくことによって被害が拡大する。また，攻撃ツールやアップロードしたデータなどの痕跡を消去することによって活動の履歴を消去し，事後調査を困難にする活動も行う場合がある。

⑺ 事後調査・復旧

侵入から攻撃の段階で検知できた場合には，攻撃活動を調査し防御対策を決定して対処を行うことで，被害拡大を防止して攻撃を終了させる。その後，企業・組織は取得されているログ等を利用して被害の発生状況の事後調査とシステム，データの復旧を行う。情報漏えいが発生した場合は社外への公表等を含めた対応が必要である。

侵入段階から攻撃段階までは連続して実行され，比較的短時間で行われるが，長期間にわたり継続する場合もある。これら一連の攻撃の発生から重要情報の漏えいによるセキュリティ事故発生までのステップを**図１**に示す。

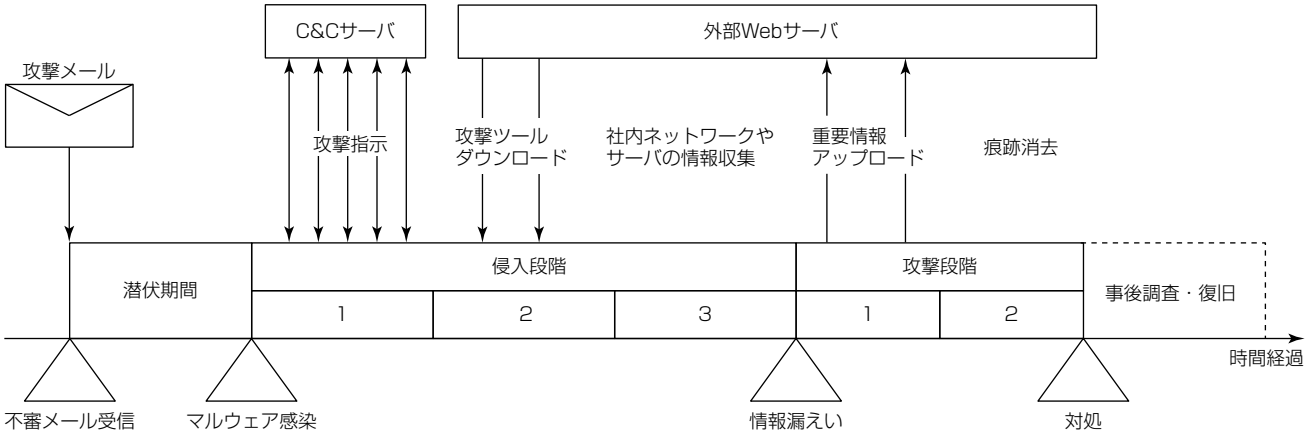



**図1．攻撃のステップ**

## 3. 包括的セキュリティ対策

### 3.1 対策の検討

攻撃のステップを整理した後，対策の網羅性評価を実施した。評価に当たっては，米国のCybersecurity Framework[(2)]を参考にして，“識別”“防御”“監視”“対応”“復旧”の各機能による対策状況を確認した。

“識別”“防御”については出入口対策，端末管理，体制など必要な対策が適用済みであった。また，“復旧”については重要システムのバックアップ等の対策が実施済みであった。しかしながら，サイバー攻撃を想定した“監視”“対応”については，**2. 2節**で述べた攻撃のステップ分けでの侵入段階と攻撃段階を検知する監視機能が不足していること及び監視した結果の対処を行う専門的な組織体制が不十分であることが明らかとなった。

これらの評価結果を受けて，従来のセキュリティ対策と包括的セキュリティ対策で強化した項目の一覧を**表2**に示す。

なお，評価の過程で，導入したセキュリティ製品では，侵入段階のC＆Cサーバの通信検知だけでなく，攻撃段階の通信検知も可能な機能を持ったものがあることが明確になった。これらについては，検知アラームによってどの段階かを判断して，対応を変える必要がある。

### 3.2 強化対策

MINDではネットワークやサーバ，クラウドの運用監視及びセキュリティの運用監視を既にサービスメニューで提供しており，今回の標的型攻撃対策サービス等でも，それら既存の監視機能を取り込むことで対応を図った。

また，攻撃段階になる前に検知して対応することが最も重要であり，防御対策に偏った対策では，攻撃者がそれを回避する手法を日々開発している現在ではリスクを下げることができないのが実状である。その現状を踏まえMINDで実施した，４つの主な強化対策について次に述べる。

#### 3.2.1 専門家グループCSIRTの設置

CSIRTと呼ばれるセキュリティの専門家によるグループを組織し，１名の専任者と７名の兼務者を配置した。CSIRTは，監視によって検知されたインシデントへの対応を中心業務とするため，ネットワーク，サーバ，セキュリティの各分野からの技術者をメンバーとして構成した。

緊急時にはCSIRTから経営層に直接報告を上げることができるようにし，経営層への情報伝達のスピードアップを図っている。また，情報システム部門やセキュリティ管理部門などの関連部門と連携フローを定義し，万が一のインシデント発生時での対応手順を定義した。

対応手順は，潜伏期間，侵入段階，攻撃段階に対応させて，発生事象の緊急度に応じて初動区分をAからCまでの３つに分けてそれぞれ定義した。潜伏期間は初動区分Aとして，感染防止を目的とした対応を行う。既に初期侵入を許している侵入段階では，緊急度を上げて対処する必要があるため，初動区分Bとして対応する。場合によってはインターネットを一部又は全面遮断するかどうかの判断も行う。更に緊急度の高い攻撃段階では，初動区分Cとしてインターネットの部分遮断ないし全面遮断が必要な事態であるとした対応を実施する。万が一自社で検出できずに外部からの指摘で情報漏えいが検知された場合は，既に攻撃段階に入っているため初動区分Cとして扱って対応する。

また，攻撃は急速に進んでいくため，発生状況の正しい把握を迅速にできることが重要である。不審な外部との通信が発生している端末の特定，トリガーとなったメールの洗い出し，マルウェアの取り出し，該当のメールが何通で誰に着信しているかなど，緊急に調査すべき事項の手順を定めている。

不審メールを開封前に止められるかは時間との戦いなので，事前の準備作業が重要であり，これらを全てフローに定義した。

表2．包括的セキュリティ対策一覧

| 区分 | 対策内容 | MINDの対応状況 |
|---|---|---|
| 識別：端末，台帳管理 | 接続端末識別 | 端末一元管理システムによる端末の管理 |
| | システム管理 | 資産管理，ソフトウェアライセンス管理等 |
| 防御：出入口対策，端末管理，体制・教育・訓練 | ウイルスメール対策 | ２種類のウイルスチェックソフトウェアによる入口対策 |
| | スパムメール対策 | 専用アプライアンス製品によるスパム隔離 |
| | Webウイルス対策 | Proxyサーバによるウイルスチェック |
| | Webフィルタ | ProxyサーバでURLフィルタリング(カテゴリ，レピュテーション) |
| | パッチ適用 | 端末一元管理システムによるパッチ自動配信 |
| | 端末アンチウイルス | 自動更新，Webレピュテーション機能 |
| | 全社体制 | リスク管理委員会(経営層)，リスク検討会，事故対策本部 |
| | CSIRT体制(注1) | CSIRT新設(技術専門家８名体制，兼務含む) |
| | 従業員教育 | 全社教育(年１回)，新入社員教育 |
| | 不審メール対処演習 | 標的型攻撃メールを全社員に送信する演習実施(年２回) |
| 監視：検知機能 | 外部からの攻撃監視 | 不正アクセス監視サービス |
| | 振る舞い検知(注1) | 専用アプライアンス導入 |
| | Web通信監視(注1) | 標的型攻撃対策サービス |
| | 不審メール報告箱(注1) | ユーザーからの報告受付，CSIRTで対応 |
| 対応：インシデントレスポンス・調査 | メール／Web通信ログ | ログサーバによるログ保管，ログ分析 |
| | 端末調査 | 情報システム部門／ヘルプデスクで一次受付，対応 |
| 復旧：バックアップ，証跡 | システムバックアップ | 重要システムは冗長化，定期バックアップ取得 |
| | 通信履歴(メール) | メールアーカイブ機能 |
| | 通信履歴(Web) | Web全通信ログ記録装置の導入 |

(注１)　今回強化した対策

#### 3.2.2　振る舞い検知の導入

既存のパターンマッチングによるウイルス検知ソフトウェアでは発見できない未知のマルウェアが添付されているメールが近年増加しているが，この問題はメール受信者がメールを開封する前，すなわち潜伏期間中に対処することができれば被害発生を未然に防ぐことができる。そのためのサンドボックス技術を利用した振る舞い検知装置を今回導入した。社内のネットワーク通信状況をモニタリングして不審な振る舞い動作及びメールの添付ファイルの動作をチェックすることで未知のマルウェアを検知することができる。検知装置の導入時には誤認識による多数のアラームが発生したが，攻撃ステップを分析した結果によってマルウェア添付の不審メール検知に監視対象を絞ることで，発生するアラーム数を削減した。なおC＆Cサーバとの通信も検知可能であり，アラーム発生時には初動区分に合わせた対応を実施する。

#### 3.2.3　Web通信監視

侵入段階から攻撃段階ではWeb通信が頻繁に行われる。Web通信のログから攻撃の有無を検知するために，SIEM(Security Information and Event Manager)を使って攻撃に利用される特徴的な通信を抽出する標的型攻撃対策サービスを導入した。

#### 3.2.4　不審メール報告箱

振る舞い検知機能で検知することができない未知のマルウェアは，少なからず存在しており，エンドユーザーに到達する不審メールを完全に除去することはできない。このため，エンドユーザーが受信した不審メールをCSIRTに連絡できる仕組みを不審メール報告箱というもので運用している。

### 3.3　攻撃ステップと包括的対策による対応

包括的セキュリティ対策として実施した内容が，**２章**で述べたサイバー攻撃のステップの中でどこの箇所に位置付けられるか，その関係を**図２**に示す。図から，出入口対策や端末管理対策に加えてサイバー攻撃に対する監視とCSIRTによる一貫したインシデントレスポンス連携によって，サイバー攻撃の全てのステップをカバーできていることが分かる。

## 4.　運用状況と成果

2015年度からCSIRTによる運用を開始し，不審メールの対応を中心に日々の活動を実施している。インシデント対応を通じて得られた知見を活用して事前のセキュリティ強化対策にフィードバックすることで，侵入する不審メールの削減を達成している。

### 4.1　運用監視状況

運用する中で，MINDでは多い日には１日に3,000通ものマルウェア添付メールが送られてきており，平均１人当たり0.7通受信していることが明らかになった。これらは従来のウイルスチェックソフトで検知できずに通過していたメールである。なお，ウイルスソフトベンダーも未知のマルウェアには順次対応を進めており，多くの未知のマルウェアはウイルス検知ソフトウェアで半日から２日程度の遅れで検知できるようになっている。

### 4.2　監視のフィードバック

運用監視によって得られた不審メールの特徴を基に，既存のセキュリティ対策の設定を変更することで防御できることが分かり，スパムメールフィルタの機能で特定の不審

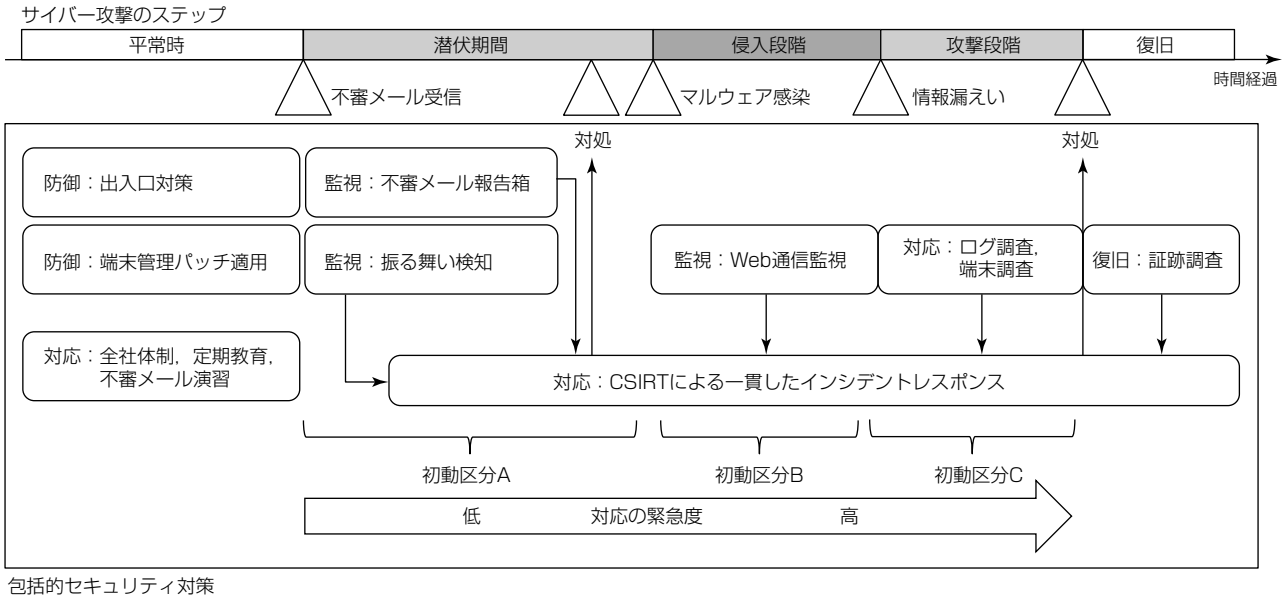



**図2．攻撃ステップと包括的対策による対応**

メールを隔離することに成功している。

また，運用監視業務を通じて，既存の出入口対策の機能を最大限に活用することも重要であることを把握した。

### 4.3 対応事例

2015年12月に，日本国内に多数のマルウェアが送信されたが，その際にMINDでは先に述べたフィードバックによる対策強化を実施した。その結果，2016年２月末から３月にかけて発生した多数の不審メールの受信を隔離することができ，エンドユーザーへの配信を防止することができた。これによって，メール受信者が開封して感染してしまうリスクを低減するとともにCSIRTが対応しなければならない不審メールの絶対数を減らすことにもつながり，その時間を他の強化策の検討に充てることができるようになった。

### 4.4 対応訓練

インシデントレスポンスのフローを定義しただけでは，緊急時に短時間で効果的な対応を行うことは難しい。そのため，未知のマルウェアの感染発生時の連絡訓練を，経営層を含む全社員に実施し，万が一のインシデント発生時に適切にかつ迅速な対応ができる体制が構築できていることを確認した。その訓練の過程で，現状のフローのままでは時間がかかるステップが明確になり，現在，改善を図っている。

## 5. むすび

サイバーセキュリティの脅威への対応は重要な経営課題の１つとして取組みの必要性が叫ばれているが，何をどこまで，どのようにすれば良いかの具体的な対策は明示されていないのが実態である。また，サイバーセキュリティの専門技術を持った人材の不足はユーザー企業における課題となっている。そのため監視や初動対応などの技術的な業務は信頼できる専門業者に委託し，ユーザー企業側では自社内にリスクの軽重を判断できる人材を育成していくことが望ましい。

## 参考文献

(1) 経済産業省：サイバーセキュリティ経営ガイドライン，Ver. 1.0 (2015)
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

(2) Natural Institute of Standards and Technology：Framework for Improving Critical Infrastructure Cybersecurity，Ver. 1.0 (2014)
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

特集論文

# スマートデバイスによる業務効率向上を実現する“MINDセキュアモバイルマネジメント”

手束裕司*

*"MIND Secure Mobile Management" for Achieving Improvement of Work Efficiency with Smart Device*

*Yuji Tetsuka*

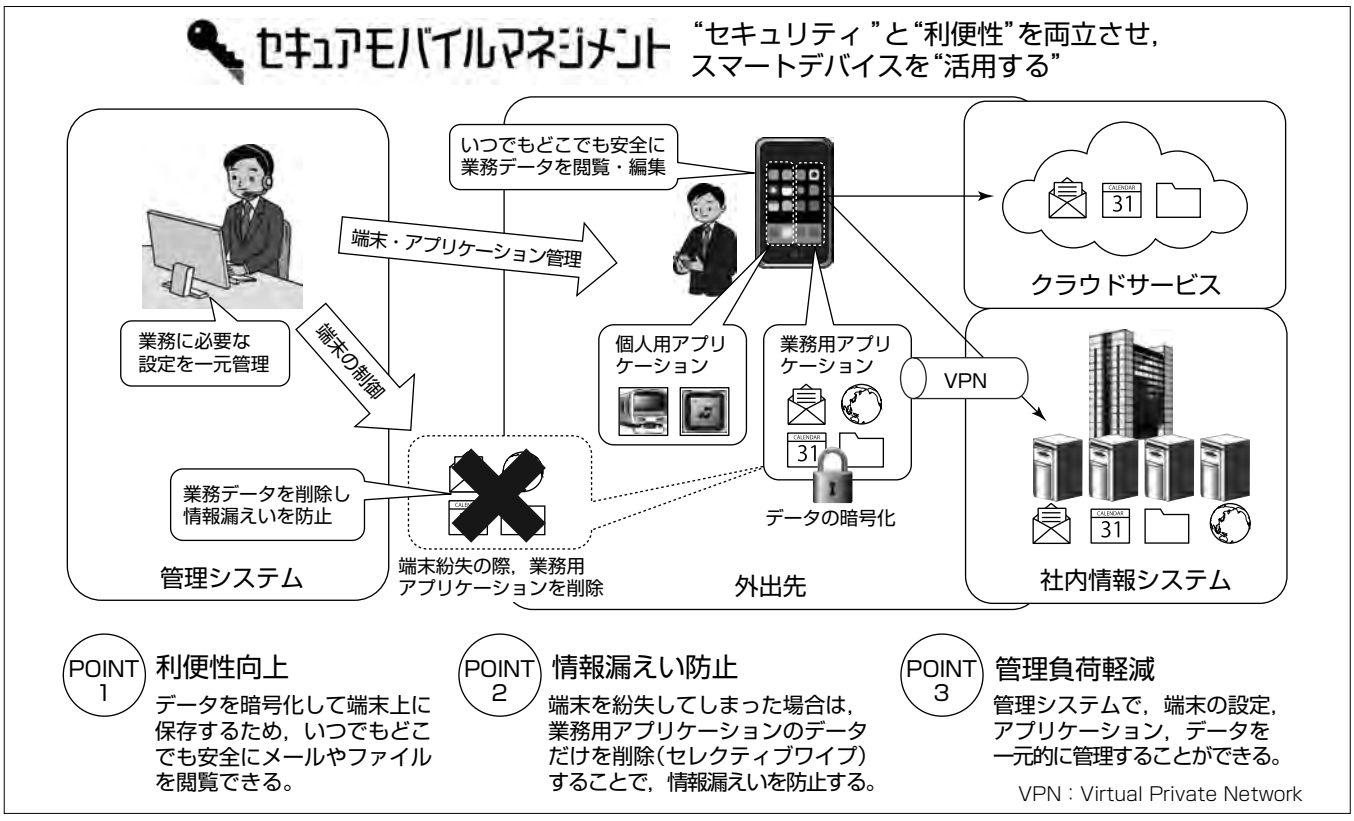
**要　旨**

スマートフォンやタブレットなどのスマートデバイスの普及が世の中で進む中，それらのスマートデバイスを業務で利用する動きが年々加速している。2013年には企業の半数以上がスマートフォンを業務で利用しており，その数は年々増加している。

スマートデバイスの業務での利用方法は，“店舗や製造現場などで業務システムの一部としての利用”と“情報システムツールとしての利用”との大きく２つに分類される。業務システムとしての利用では，紙マニュアルの電子化や，店舗での受発注など多くの事例が出ている。一方で，情報システムツールとしての利用については，メールの送受信やスケジュールの閲覧が主であり，利用者も経営幹部や一部の営業社員などにとどまっており，企業として，ワークスタイル変革を実現するまでの活用には至っていない。

情報システムツールとしてスマートデバイスを活用するためには，“セキュリティを確保するための技術”と“業務アプリケーションを利用するための技術”が必要となる。その２つの技術を実現するのがEMM(Enterprise Mobility Management)であり，EMMは従来デバイス管理として利用されているMDM(Mobile Device Management)に，アプリケーション管理のMAM(Mobile Application Management)，コンテンツ管理のMCM(Mobile Contents Management)を併せ持つ技術である。

三菱電機インフォメーションネットワーク㈱(MIND)では，情報システムツールとしてのスマートデバイスを“利用する”から“活用する”に変革するためのソリューションとして，EMMをサービス型で利用してもらえるソリューションとして“MINDセキュアモバイルマネジメント”を提供する。これによって，企業におけるスマートデバイスの活用を支援する。




## MINDセキュアモバイルマネジメント

MINDセキュアモバイルマネジメントは，スマートデバイスの管理製品であるMDM，MAM，MCMの３つの機能を併せ持つEMM製品をサービス基盤としたスマートデバイスの管理・活用ソリューションである。スマートデバイスの業務利用で重要となる“セキュリティ”と“利便性”を両立させ，企業でスマートデバイスを“利用する”から“活用する”へ変革することを支援する。

*三菱電機インフォメーションネットワーク㈱

## 1. まえがき

スマートフォンやタブレットなどのスマートデバイスの普及が世の中で進む中，それらのスマートデバイスを業務で利用する動きが年々加速している。2013年には企業の半数以上でスマートフォンを業務で利用しており(1)，その数は年々増加している。

スマートデバイスを業務で利用することは，企業で一般的なことになってきているが，その利用方法は，“店舗や製造現場などで業務システムの一部として組み込んで利用する”と“情報システムツールとして利用する”との２つに大別される。前者の業務システムの一部として利用するケースは，航空会社における紙マニュアルの電子化，店舗での受注端末，倉庫での在庫管理などいろいろな場面での利用が実現されている。一方，情報システムツールとしての利用については，メールの送受信やスケジュールの閲覧が主となっており，営業社員の生産性向上や外出先からの業務利用などまだまだ十分に活用されておらず，ワークスタイルを変革するまでの利用方法には至っていないのが現状である。また，情報システムツールとしてスマートデバイスを導入したが，社内での展開が一向に進まないケースも多く出ている。

本稿では，情報システムツールとしてのスマートデバイスの活用に関し，その課題と解決策を述べる。

## 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での課題

企業におけるスマートデバイスの業務利用は2010年ごろから本格的に始まり，2011年には約３割の企業で何らかの形でスマートデバイスを業務で利用し，2012年には約４割，2013年には約５割の企業で利用している(1)。スマートデバイスの業務利用が進む一方で，その情報システムツールとしての用途はメールの送受信やスケジュールの閲覧にとどまり，また，利用者も企業の経営幹部など一部の人に限られ，全社的に展開している企業は多くはない。その第１の理由として挙げられるのが，従来の携帯電話に比べスマートデバイスの本体価格と通信料金が高額なことであり，第２の理由は，企業がスマートデバイスを導入する際に最大の懸念事項として挙げるセキュリティ対策である。スマートデバイスは従来の携帯電話に比べ，デバイスの中に多くのデータとアプリケーションを保持している。各種アプリケーションはデバイス内のデータにアクセスし，クラウドサービスなど外部のサービスとのデータ交換を可能とする。また，アプリケーションは個人が自由にダウンロードすることが可能であり，中には情報漏えいにつながるような不正なアプリケーションも存在する。企業の情報システム部門にとっては，セキュリティリスクを回避するため利用者を限定したり，MDMのようなデバイス管理のシステムを導入したり，対策を講じている。

スマートデバイスの業務利用に当たっては，ワークスタイル変革に伴う生産性の向上を目的とする企業が多いが，先に述べたとおり価格の面から社内での利用者が限られていること，セキュリティ対策を重視するがあまり利便性が損なわれ，利用したいと思う人が増えないことなど，その本来の目的を達成できない場合がある。特に導入目的を明確に策定せずに導入することで，本来の目的である生産性向上に代わり，“スマートデバイスを導入すること”自体が目的となっているような場合には，スマートデバイスの展開が進まず，生産性の向上が図れない。

### 2.2 スマートデバイスを業務で活用するための技術と導入ポイント

スマートデバイスを業務で活用するためには，“セキュリティを確保するための技術”と“業務アプリケーションを利用するための技術”の大きく２つの技術が必要となる。

“セキュリティを確保するための技術”としては，データ及び通信の暗号化，個人及びデバイスの認証，マルウェアの検知及び駆除，デバイスにインストールするアプリケーションの制御及び保護，さらにスマートデバイス紛失時の対策としてはGPS(Global Positioning System)によるデバイスの捜索，遠隔からのデバイスのロック及び内部データの削除などが挙げられる。

これらのセキュリティ対策を採用するに当たっては，企業のセキュリティポリシーに基づき，スマートデバイス利用時のリスクを分析し，そのリスクに合わせて適用する技術を採用することが必要である。過度のセキュリティ対策を実施することは，**2. 1節**で述べたとおり利用者の利便性を損ね，本来のスマートデバイスの導入目的である生産性の向上を実現することはできない。

一方の“業務アプリケーションを利用するための技術”であるが，情報システムツールとしての利用と考えた場合には，社内メールの送受信，スケジュールなどのグループウェアの利用，各種システムの利用(閲覧・入力・申請・承認)，ファイルストレージからのファイルの閲覧及び編集が主な用途として挙げられる。また，これらのシステムは，①自社保有のオンプレミス型として社内又はデータセンターに設置している場合，②Microsoft Office365(注1)やGoogle Apps for Works(注2)などのクラウドサービスを利用している場合，③その両方を利用している場合に分けられる。

スマートデバイスの導入では，“セキュリティ”と“利便性”のバランスを取り，それぞれを両立させることのできる仕組みが必要となる。“MINDセキュアモバイルマネジメント”は，スマートデバイスにおけるセキュリティと利便性の両立を実現したソリューションである。

MINDセキュアモバイルマネジメントを実現するため

の技術がEMMであり，EMMの構成要素であるMDM，MAM，MCMについて次に述べる。

（注１） Microsoft Office365は，Microsoft Corp. の登録商標である。
（注２） Google Apps for Workは，Google Inc. の登録商標である。

### 2.2.1 MDM（モバイルデバイス管理）

MDMは，企業のセキュリティポリシーに合わせてスマートデバイスの設定などを一元的に管理する製品又はサービスであり，パスワードの設定や，利用するアプリケーションの制限などスマートデバイス自体を管理する仕組みを提供する。

この機能によって，企業の情報システム部門では配布したスマートデバイスのハードウェアの一元的な管理，スマートデバイスごとにインストールしたアプリケーションの管理，アプリケーションのバージョン管理など，統合的にスマートデバイス及びスマートデバイス内にインストールされているアプリケーションの管理を行うことができる（**図１**）。さらに，万が一のスマートデバイスの紛失時には，拾得者が操作できないよう遠隔からロックを実施したり，デバイス自体を初期化して一切のデータを削除（ワイプ）したりすることによって情報漏えいを防止することが可能である。拾得されたスマートデバイスの90％は，拾得者がデバイスの中身にアクセスを試みているとの調査結果も出ており，この対策は必要である。

ただし，MDMによる遠隔からのロックや初期化はオンラインの状況で実施する必要があることや，スマートデバイス自体を管理する仕組みであるため，スマートデバイス内に保管している業務データだけを削除するようなことはできない。

現在，個人所有のスマートデバイスを業務用として利用するBYOD（Bring Your Own Device）を実施する企業が増加しているが，MDMの機能だけでは会社による個人データの管理や，紛失時の個人データを含めた全データの削除など，プライバシーや運用面での課題が存在する。

### 2.2.2 MAM（モバイルアプリケーション管理）

MAMは，スマートデバイスにインストールする業務用のアプリケーションを管理する機能であり，ソフトウェア製品として提供されるのが一般的である。利用する機能はコンテナ機能とラッピング機能の２つが代表的であり，アプリケーションに対して他のアプリケーションからのアクセス制限やデータ保護の設定を行うことによって，業務用のアプリケーションやスマートデバイス内に保管しているデータを安全に利用できるようにする。コンテナ機能は，スマートデバイスの内部をコンテナと言われる単位で特定の領域に分離し，同じコンテナ内部のアプリケーションであれば相互にデータの交換を可能にするが，コンテナ外部のアプリケーションとのデータの交換は制限するというものである。なお，コンテナ内部は暗号化をすることで，万が一スマートデバイスを紛失した際にも情報の漏えいを防ぐことができる。一方，ラッピング機能は，アプリケーション単位にセキュリティの機能を付加するものであり，この機能によって，個人アプリケーションから業務アプリケーションへのアクセスを制限し，個人アプリケーションが業務データを取り込むことを禁止したり，業務アプリケーションが社内のサーバなどへ接続する際には，自動的にVPNを設定して暗号化通信を行うなど，業務データの保護を可能にしている（**図２**）。

### 2.2.3 MCM（モバイルコンテンツ管理）

MCMは，先に述べたMDMやMAMとは異なり，スマートデバイスを業務でセキュアに活用するための機能であり，ソフトウェア製品として提供される。MCMによって，スマートデバイスから，社内のメールサーバやクラウド型メールシステム，クラウドストレージや専用のファイル共有型システムなどへ安全にアクセスできる環境を提供する。セキュリティ対策は，スマートデバイスの中にデータを保管する際にはファイルごとに暗号化を行ったり，コピーや印刷の禁止などのアクセス制限をかけたり，コンテンツの秘匿レベルに合わせてセキュリティの強度を管理することで実現する。さらに，専用のファイルストレージで管理する場合には，誰が，いつ，どのドキュメントを閲覧・編集したかのログを管理することが可能であり，不正

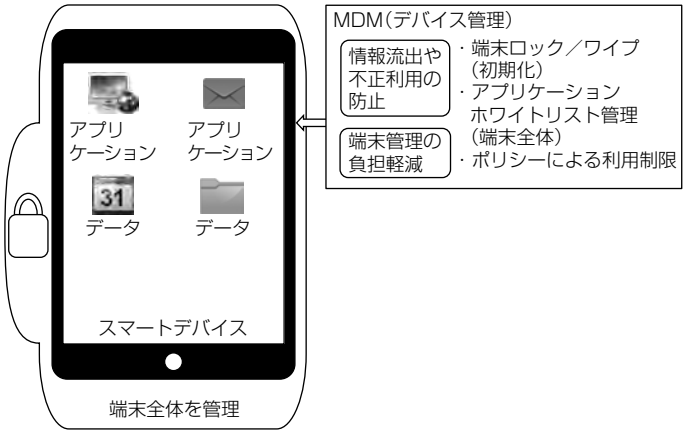
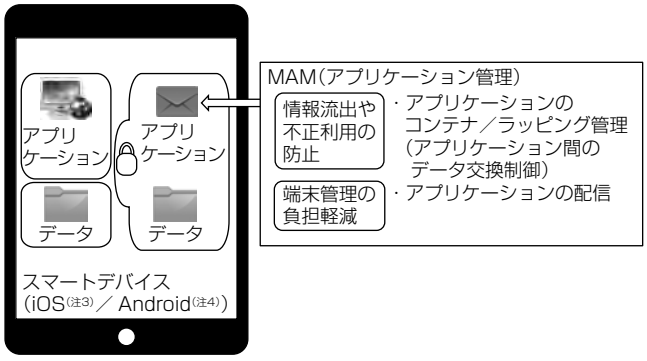



図１．MDM




（注３） iOSは，Cisco Systems，Inc. の登録商標である。
（注４） Androidは，Google Inc. の登録商標である。

図２．MAM

にダウンロードしているファイルを遠隔から削除することもできる。MCMによって，電子メールの送受信やグループウェアの利用，ファイルサーバやクラウドストレージと連携して業務データや文書ファイルの閲覧・編集などを簡易にかつ安全に行うことが可能となる(**図3**)。

MCMの活用としては，商品カタログや価格表など常に情報を最新に保つ必要のある情報を共有のファイルストレージに保管しておき，営業社員がスマートデバイスでこれらの情報にアクセスして活用する場面などが想定される。また，プレゼンテーション資料を共有のファイルストレージに保管し，営業社員が顧客への提案の際に事前にダウンロードして提案活動を行うことにも利用できる。MCMはスマートデバイスの中にデータを保管することができるため，通信の電波が届かない室内でのプレゼンテーションもあらかじめデータをダウンロードしておくことによって可能になる。

### 3. MINDセキュアモバイルマネジメント

スマートデバイスの管理は，MDMによるデバイスの管理から始まり，その後，アプリケーションの管理であるMAM，そしてスマートデバイスを活用するためのソリューションであるMCMがソフトウェア製品又はサービスとして市場に登場した。EMMはこれら3つの機能を併せ持ち，デバイスの管理からアプリケーションの管理，そして業務で活用するためのメールやグループウェアなどのアプリケーション連携を包括的に提供するものであり，企業でセキュリティを確保しながらスマートデバイスを活用するためのソリューションとして近年注目を集めている。

MINDは“スマートフォンマネージ”という名称でMDMサービスを提供しているが，これに加え，EMMの機能を“MINDセキュアモバイルマネジメント”という名称でサービスとして提供する(**図4**)。なお，EMMは市場ではソフトウェア製品として提供されており，サービスとしての提供は例が少ない。MINDは，各企業のスマートデバイスの利用環境に合わせて，最適なEMMの機能を導入しやすい“サービス”として提供することによって，企業の情報システムツールとしてのスマートデバイスの活用を支援する。

MINDセキュアモバイルマネジメントはセキュリティと利便性の両方を兼ね備えたサービスであり，次にその特長を整理して列挙する(**図5**)。

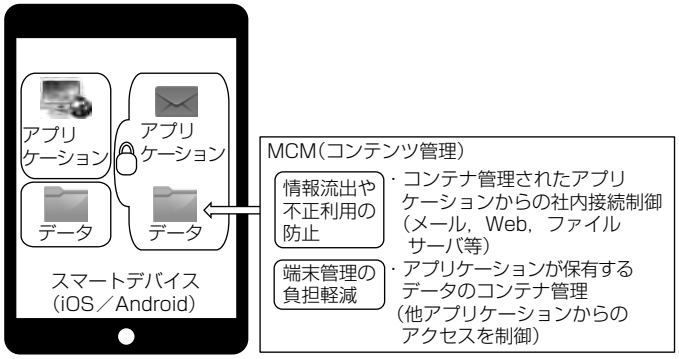



**図3．MCM**

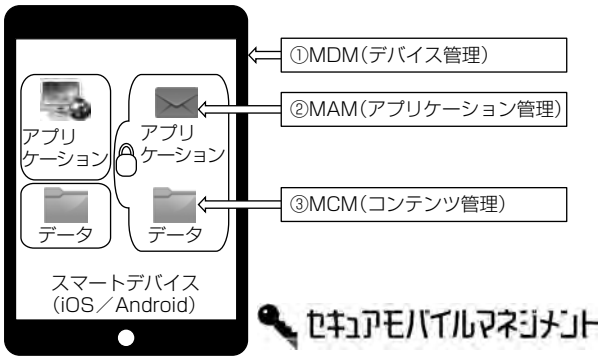
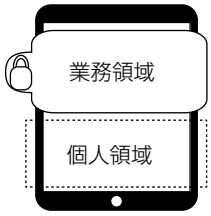
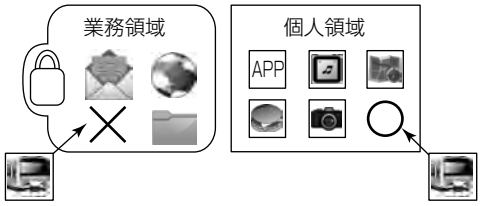


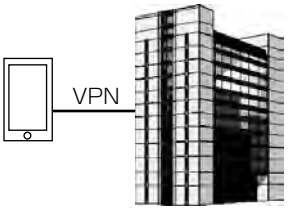

**図4．MINDセキュアモバイルマネジメント**



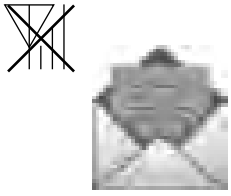

業務領域と個人領域との分離



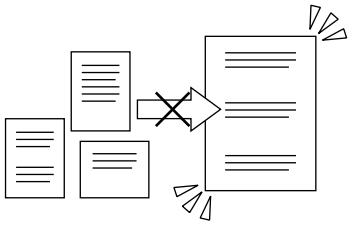

業務領域には業務アプリケーションだけを，個人領域は自由に利用



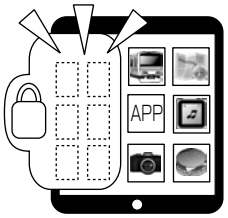

業務アプリケーションはVPNによる社内接続



オフラインでの閲覧・編集が可能



コピー &ペースト機能の制限




業務領域だけ初期化(ワイプ)

**図5．MINDセキュアモバイルマネジメントの特長**

(1) セキュリティの特長

①スマートデバイス内部を業務領域と個人領域にコンテナ機能で分離し，業務領域は暗号化によって保護する。

②業務領域は暗号化によって保護され，さらに遠隔から業務領域だけを削除することによって，デバイスの紛失時にも個人領域には影響を与えずに企業の情報漏えいを防ぐ。

③業務領域と個人領域の間でのデータの交換，文書のコピー／貼付けなどを一切禁止し，個人領域からの情報の漏えいを防ぐ。

(2) 利便性の特長

①アプリケーションごとに自動的にVPNを設定して暗号化通信を行うことで，セキュリティを確保しながら，VPN設定の手間を省き，迅速なアプリケーションの利用を可能にする。

②業務領域の暗号化によって，デバイス内にデータを保持し，オフラインで利用することができる。これによって，電波の届かない環境でのスマートデバイスを利用したプレゼンテーションや，メールやファイルの編集などが可能となり，生産性の向上につながる。

## 4. むすび

MINDセキュアモバイルマネジメントは，2016年度中のサービス提供開始を予定している。このサービスの提供によって，企業がスマートデバイスを“利用する”から“活用する”へと進化を遂げ，ワークスタイル変革そして生産性の向上を達成することを支援する。

また，スマートデバイスの業務利用とともに企業で急速に広まっているのがOffice365などのSaaS(Software as a Service)の利用である。ワークスタイルの変革に伴いスマートデバイスから，直接SaaSを利用する業務形態が今後増加していくものと思われる。これに対して，MINDではスマートデバイスの業務利用を含め，クラウドサービスをセキュアに活用するためのソリューションとして“MINDセキュアクラウドアクセス”を提供することも検討中である。今後，MINDセキュアモバイルマネジメントとMINDセキュアクラウドアクセスを組み合わせ，企業が安全にかつ利便性を損なわずに，スマートデバイスからクラウドサービスを活用する仕組みを提供していく。

## 参考文献

(1) (独)情報処理推進機構： 2014年度 情報セキュリティ事象被害状況調査 報告書 (2015)
http://www.ipa.go.jp/files/000043418.pdf

特集論文

# “MINDスマートオフィスソリューション”のサービス化に向けた実践と検証

堀内哲朗*
栃木秀明*
舘本恭昌*

*Practice and Verification of "MIND Smart Office Solution"*

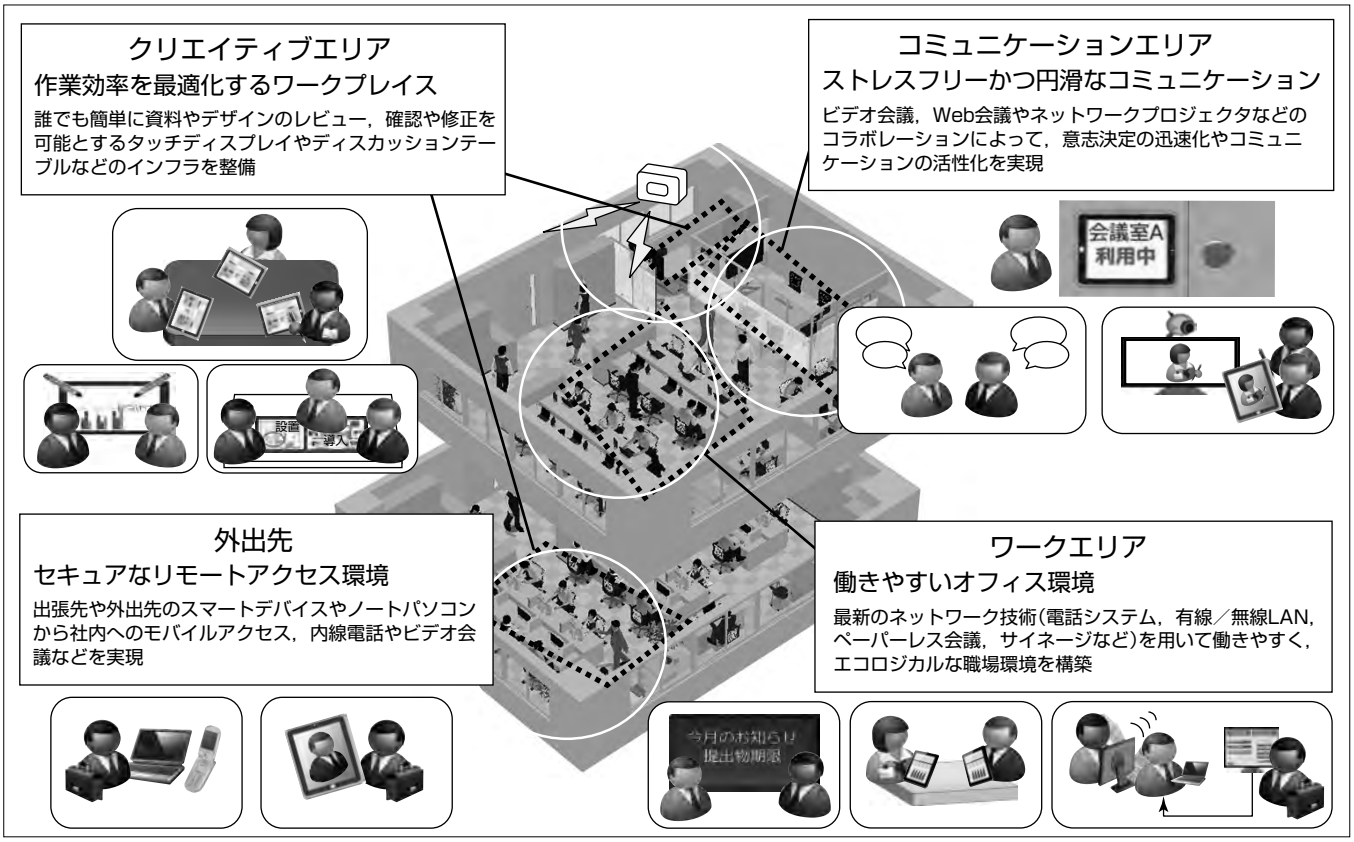
*Tetsuro Horiuchi, Hideaki Tochigi, Yasumasa Tachimoto*

**要　旨**

日本では今後，類を見ない少子高齢化が予測されており，それに伴い労働人口は大幅に減少することが見込まれている。労働人口の減少は労働力の減少に直結するため，競争力の引上げに向けて企業での一人当たりの生産性向上は必須である。三菱電機インフォメーションネットワーク㈱(MIND)では，顧客の業務効率化・生産性向上を実現するソリューションとして，“MINDスマートオフィスソリューション”の提供を開始した。

MINDスマートオフィスソリューションは“コンサルティングサービス”“ICT(Information and Communication Technology)ツール・空間・運用提供サービス”“移転・統廃合マネジメントサービス”の３つのメニューからなり，サービス化に当たっては，まず社内サンプル部門を対象に実践と検証を行い，そこで得た経験とノウハウを顧客に提供していくことにした。MINDでの実践では抽出した課題を解決して新しいワークスタイルを実現するためのワークショップを重ね，“紙を持たない働き方の実現”“新たなコミュニケーション空間の創出”や“時間と空間の制約からの解放”を目標に定めて様々な施策を実施し，その結果，紙文書の削減など幾つかの取組みで定量的・定性的な効果を確認できた。

MINDでは今回の経験とノウハウを活用しつつ，ソリューションによってもたらされる効果を形骸化させないため，継続してPDCA(Plan，Do，Check，Action)サイクルを回しながらノウハウを蓄積し，広く顧客に対しソリューションを提供していく。




**“MINDスマートオフィスソリューション”のオフィスイメージ**

MINDスマートオフィスソリューションは，顧客の様々な要望や課題を解決するため，いつでも(情報の共有ができる)，どこでも(仕事ができる)，だれでも(同じ業務ができる)をコンセプトに，“快適なワークスペース”と“多彩なワークスタイル”実現のため，コンサルティングからICTツール・空間・運用の提供，移転・統廃合マネジメントまでワンストップで対応する。

*三菱電機インフォメーションネットワーク㈱

## 1. まえがき

日本の65歳以上の人口は2010年の23.0％から2060年の39.9％へと，かつてない少子高齢化が予測されている。それに伴い15～64歳の生産年齢人口は2013年12月時点では7,883万人，2060年には4,418万人へと大幅に減少することが見込まれている(1)。このような少子高齢化による労働人口の減少は，労働力の減少に直結するだけでなく，企業の持つ知識や技能の継承にも影響が出ることが危惧されている。企業ひいては日本の競争力を引き上げて豊かな社会を維持していくためには，非労働人口の就業の掘り起こしとともに，一人当たりの生産性向上は必須である。すなわち，一人当たりの就労時間を増やすことなく大きな成果を出すため，効率的かつ誰であっても専門的な業務をこなせる生産性の高い職場環境が求められている。

このような背景の下，MINDでは多彩なワークスタイルと快適なワークスペースを実現することで顧客の業務効率化・生産性向上を実現するソリューションとして，MINDスマートオフィスソリューションの提供を開始した。

本稿では，MINDスマートオフィスソリューション及びそのサービス化に当たって，MINDでそのソリューションを実践・検証した結果について述べる。

## 2. MINDスマートオフィスソリューション

MINDスマートオフィスソリューションは大きく分けて３つのサービスメニューで構成している。①顧客の働き方や働く場所を分析し，顕在する課題とその解決策について検討・提言を行うコンサルティングサービス，②ワークスタイル革新を実現する各種ICTツールやシステム，空間を構築・運用する提供サービス，③事務所の移転，リニューアルや統廃合などの取りまとめを行うマネジメントサービスの３つである。

なお，各サービスは単独・組合せのどちらでも提供可能であり，コンセプトの検討，空間デザインから構築・運用・取りまとめまで全てに対応することもできる。

### 2.1 コンサルティングサービス

コンサルティングサービスは，“会議が活性化せず多くの意見が出ない”“レビュー会議における配布資料の無駄を解消したい”“事務所以外で仕事ができず効率が悪い”“場所にとらわれずに働ける環境がほしい”といった顧客の抱える課題や将来に向けた要望を踏まえて業務やオフィスの現状調査・分析を行い，ワークショップや実証実験などの手法を用いつつ，解決に向けたコミュニケーション分野のプランニング作成やワークスタイル変革を支援するサービスである。

具体的な要件が固まっていない顧客であっても，ワークスタイルやワークスペースの改革を検討したいという要望があれば，ヒアリングを実施した上，あるべきイメージやロードマップなどのプランニングを提供する。

### 2.2 ICTツール・空間・運用提供サービス

ICTツール・空間・運用提供サービスは，ワークスタイルやワークスペース変革のため，様々なツールやシステム，働く空間を構築・提供するとともに，顧客の日常“運用”をサポートするサービスデスクを提供するサービスである。具体的なツールの例としては，“ビデオ会議”“ペーパーレス会議”“デジタルサイネージ”“インタラクティブプロジェクタ”“電話システム”等が挙げられ，それらを組み合わせた働く空間として顧客のニーズに合わせた“受付”“会議室”“研修室”“オフィス”“ショールーム”の構築支援を行うとともに，そのツールや空間を使いこなすための日々の運用支援をサービスデスクとして提供する。

### 2.3 移転・統廃合マネジメントサービス

移転・統廃合マネジメントサービスでは，事務所の移転，リニューアルや統廃合等のプロジェクトで，顧客とゼネコン，ビルオーナーなどに対し，プロジェクト完遂までのマネジメントを提供するサービスである。他事業者が提供する部分も含めて，移転調整や各種オフィスインフラ，ファシリティ調整を一括で取りまとめることが可能であり，移転・統廃合等における顧客の実務レベルでの負荷を大幅に軽減し，移転や統廃合に関わる企画・計画・決済業務に専念できるようにする。

## 3. ソリューションの実践と検証

MINDスマートオフィスソリューションのサービス化に当たっては，まずMIND自身にソリューションを適用して実践と検証を行う環境を作り上げ，そこで得た課題解決の経験とノウハウを活用して顧客に提案・提供を行っていくことにした。

この章では，ソリューションの効果算定とノウハウ蓄積のため，まずMIND社内のサンプル部門に対して実践と検証を行った結果について述べる。対象となった部門と取組み期間は次のとおりである。

(1) 対象部門：SE部門，35名，１フロア307m²（共有スペース込），2016年３月末にオフィスの移転完了
(2) 取組み実施期間：2015年４月～2016年３月

### 3.1 コンサルティングサービスの実践

MINDでの実践に当たり，まずコンサルティングサービスを実践して当該部門の現状の働き方を調査・分析し，課題を解決するための取組みと目標について検討を行った（**図１**）。ヒアリングによって当該部門が抱えている様々な課題をリストアップし，その要因を分析するとともにそれらの課題のグループ化を実施し，最終的に主要課題として次の５つを抽出した。

①情報の保管・検索手段にばらつきがある。


**図1．ワークショップ光景**

②紙文書が氾濫し，スペースが有効活用されていない。
③レビュー・ワークの準備に時間がかっている。
④会議や日常業務に無駄・手間が顕在化している。
⑤情報の共有が徹底されていない。

次いでこれらの課題解決に向け，ワークショップを重ねて解決策の検討を行った結果，最初に目指すべき取組みの目標は次の3つとした。

⑴ 紙を持たない働き方の実現(課題①②⑤の解決)

無駄な紙文書を排除し，情報を共有しやすい，ほしい情報をすぐに探せる快適で働きやすいオフィスを実現する。

⑵ 新たなコミュニケーション空間の創出(課題③④の解決)

コミュニケーションの活性化や意思決定の迅速化を促す新しい空間を実現する。

⑶ 時間と空間の制約からの解放(課題②④の解決)

日常業務・作業等が，いつでも，どこでも，だれでも容易に実施できる環境を実現する。

### 3.2 ICTツール・空間・運用提供サービスの実践

**3.1節**で述べた3つの目標実現に向け，実際にICTツール・空間・運用提供サービスを実践し，効果を確認することにした。

#### 3.2.1 紙を持たない働き方の実現

この部門で持っている紙文書の個人・共有を合わせた総量は調査開始時で98.4fm(ファイルメータ：書類量を計測する単位。1fm＝書類約10,000枚)であり，これは一人当たりに換算すれば約2.9fmであった。この値は，一般の民間企業の平均とされる6.7fm[2]と比べて，低い数値ではあったが，実際にヒアリングを行った結果，多くの時間と業務がいまだ紙文書の制約を受けており，それが課題につながっているという声が上がった。そのために，まず紙文書及び紙文書を用いた業務を減らすことで，新しい働き方を目指すことにした。当該部門における紙を用いた業務と文書を分類した(**表1**)。

紙文書の分類結果を踏まえ，原本必須の請求書や領収書等を除いた多くの文書について削減を目指し，その取扱いについて検討を実施した。最初の3か月で対応方法のガイドライン策定とそれぞれに対応する文書の仕分，それ以降で実際に紙文書の削減を実行した。また，並行して紙を持たない，発生させない働き方を実現するため，ICTツールの導入や仕組み作りに取り組むことにした。具体的に実施した施策は次のとおりである。

**表1．紙文書とそれに関わる業務**

| | |
|---|---|
| 紙文書の種類 | 申請書／申込書／請求書／領収書，<br>契約書／規程／認許書類／公文，名刺，<br>提案資料／パンフレット／完成図書，書籍 |
| 紙文書を扱う業務 | 文書／資料作成，レビュー／報告，印刷／配布／回覧 |

・紙文書の削減のためのガイドライン策定
・不要文書の廃棄と廃棄ルールの徹底
・文書，名刺の電子化
・保管が必要な文書の外部への保管(倉庫活用)
・ペーパーレス会議システムによる会議，打合せ資料の電子化
・電子化したファイルの部門サーバ保管フォルダ共有
・回覧・掲示文書のデジタルサイネージによる代替

#### 3.2.2 新たなコミュニケーション空間の創出

この部門では2016年3月末に移転を予定していた。そこで移転を機に，従来の会議室や打合せスペースと紙文書削減によって生み出されたスペースを合わせ，コミュニケーション空間を拡充することにした。これらのコミュニケーションを行うためのエリアは従来同様に会議室・打合せコーナーとして利用するだけではなく，幾つかのICTツール・システムと組み合わせて各業務の用途に特化した空間としても構築し，業務分析で挙げられた課題の解決を目指すことにした。

移転に当たって，ICTツールなどを活用し，新しいコミュニケーション空間として設けたエリアの内容は次のとおりである。

・大画面のマルチディスプレイ，全卓にタブレット型ディスプレイとマイクを設置し，従来よりも画像，音響の視認性や臨場感を考慮した大型会議室(**図2**(a))
・ディスカッションテーブルによって複数人が同時にデ

(a) 大型会議室

(b) クリエイティブエリア

(c) レビューエリア


(d) 会議室予約システム

**図2．新しいコミュニケーション空間**

ザインワーク等の作業可能なクリエイティブエリア(**図2**(b))

・ネットワーク対応の電子黒板を導入した遠隔地と板書共有が可能なレビューエリア(**図2**(c))

また，各エリアに会議室予約システム(**図2**(d))を設置して利用をチェックイン制とすることで空予約を防止し，利用効率の向上を実現した。併せて全エリアにビデオ会議システムを導入し，遠隔地と気軽にコミュニケーション可能な環境を構築した。

### 3. 2. 3　時間と空間の制約からの解放

さらに，ヒアリングで挙げられた幾つかの無駄や手間という課題を解決するため，“いつでも(情報の共有ができる)どこでも(仕事ができる)だれでも(同じ業務ができる)”というコンセプト実現に向けて，新たに幾つかのICTツール及び空間の活用手法を導入し，時間や空間にとらわれない働き方を目指していくことにした。

時間と空間の制約から抜け出す新しい働き方に向けて，導入したICTツールや空間の活用手法は次のとおりである(**図3**)。

(1) 無線LANとパーソナルタブレット活用によって，全員のノートやメモ帳をタブレット端末に置き換え，ペーパーレス促進及び電子化によって検索性や情報共有が向上した。

**図3．新しい働き方を実現するオフィス環境**

⑵ オフィス各所へ大型ディスプレイとワイヤレスプレゼンテーションシステムを導入し，様々な場所でいつでも簡単に資料投影ができるようにした。
⑶ シンクライアントによる，この部門への出張者が自席と同じように作業可能な出張者用エリアを構築した。
⑷ 作業や資料作成等の効率向上を狙い，外部の音を遮断して集中が可能なコンセントレーションエリアを設置した。

### 3.3 ソリューションの検証

**3.2.1項**については，2016年３月時点で紙文書は当初の98.4fmから37.5fmへ62％削減，キャビネットは28本から10本へ64％削減となった。キャビネット１本当たり，利用スペースを含めて約１m²と想定すると，この場合，約18m²(フロアの約６％相当)のスペースを生み出したことになる。また，既存紙文書の削減だけでなく，部門全体のコピー・印刷費用合計は2014年度924千円から2015年度567千円に削減された。単純な費用削減だけでなく，紙文書のコピー・印刷作業の削減，すなわち働き方そのものが，会議やレビュー資料のコピー・印刷の手間を省いた，紙を持たない働き方へと変化したことが確認できた(**図４**)。

⒜ 従来のオフィス

⒝ 施策実施後のオフィス

**図４．紙を持たない働き方への変化**

**3.2.2項，3.2.3項**については，実践後間もないため具体的な効果を検証するまでには至っていない。しかし，実践直後に実施した部員への効果予想アンケートの集計結果では，先に述べた各施策によって実施前と比べて平均7.5％の業務時間削減，すなわち業務効率化が期待できるという回答が出ており，引き続き検証を行っていく。

また，そのアンケートでは電子化・ツールの導入によって情報の共有を進める一方で，膨大な情報の中から必要な情報を素早く取り出すための“情報の検索性”という点が依然として課題であり，改善検討が必要との回答も多く，引き続きこれらの課題解決に向けて取り組んでいく。

## 4. むすび

企業が抱える課題を解決し，生産性向上につなげていくためには，ワークスタイル及びワークスペース革新への取組みは必須である。MINDではそれらを実現するソリューションとして，MINDスマートオフィスソリューションをMINDの一部門に対して適用し，短期間ではあったが，実践と検証を行うことで紙文書の削減や新たなコミュニケーション空間の実現などについて，幾つかの成果を確認することができた。このソリューションは既に提供を開始している。MINDでの検証結果がそのまま当てはまるわけではないものの，得られたノウハウや経験を活用することで様々な顧客にも一定の効果は見込めると考える。

このソリューションで特に重要なのは，コンサルティングサービスでの継続した取組みに向けたプランニングであると考える。例えば，保有する紙文書をいくら削減しようとも，働き方が従来同様に紙文書を中心としたものであれば，いずれ紙文書の量は元に戻ってしまう。せっかくの取組みや成果を一過性のものとして終わらせないためには，新しいワークスタイルをいかに定着させ，いかにして継続していくか，また，何のために取り組むのかという目的意識を共有・浸透させることが重要であり，MINDでは引き続きそのためのPDCAサイクルを実践しながらノウハウを蓄積し，広く顧客へサービスを提供していく。

## 参考文献

⑴ 総務省：平成26年版 情報通信白書(2014)
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/index.html
⑵ ㈱エフエム・ソリューション：オフィス内の文書量に関する実態調査報告(2014)
http://www.fm-solution.co.jp/topics/pdf/RM-Report_2014.pdf

特集論文

# 空港向けフライトインフォメーションシステムソリューション及びグローバル化への取組み

長田光平*　今宿誠己*
志村和生*
寺崎浩隆**

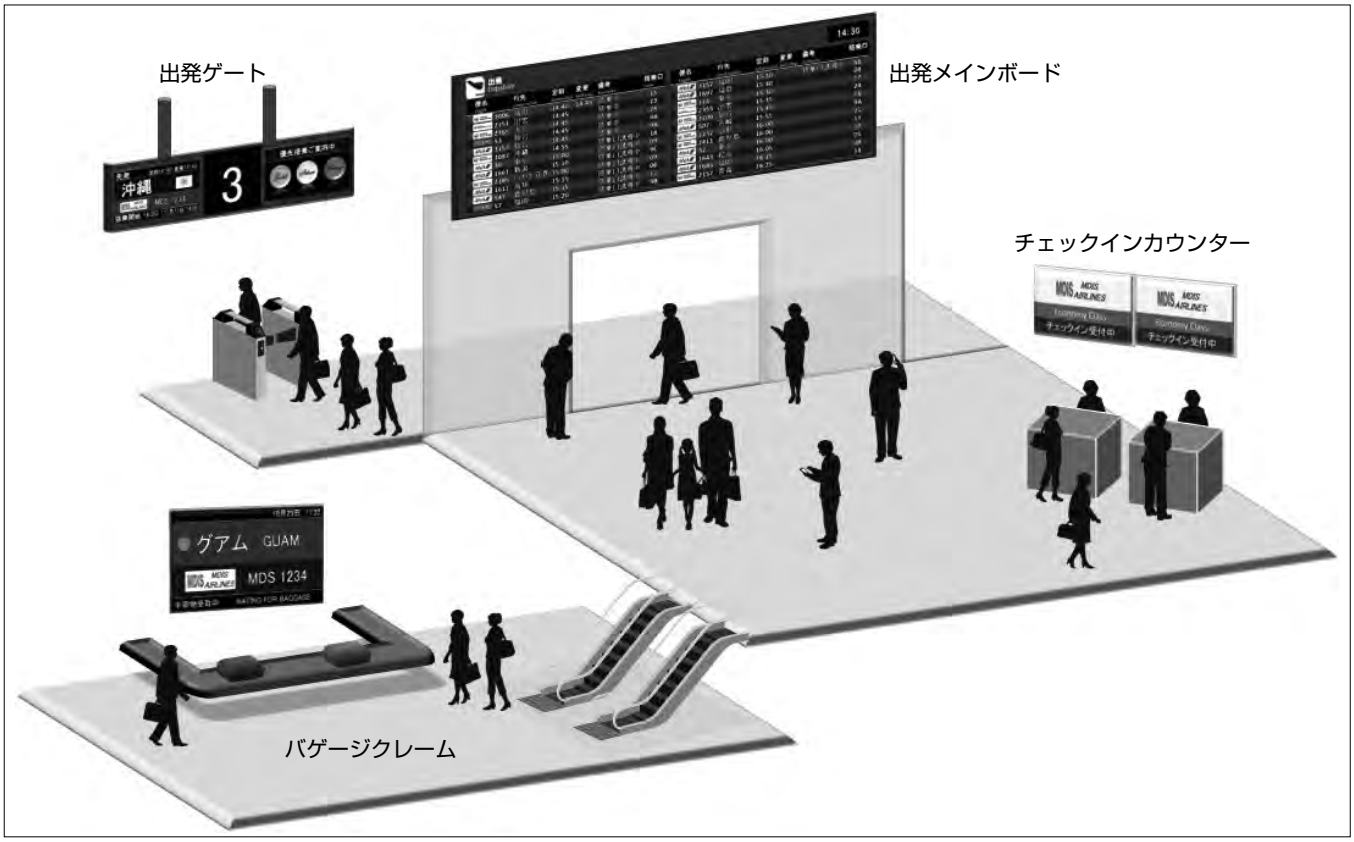
*Flight Information System Solution for Airports and Effort for Global Market*

*Kohei Osada, Kazuo Shimura, Hirotaka Terasaki, Masaki Imajuku*

**要　旨**

フライトインフォメーションシステム(Flight Information System：FIS)は，空港を利用する旅客，来港者及び空港スタッフに対して，空港に関する情報(航空機の離発着情報であるフライト情報，搭乗手続きを行うチェックインカウンターの案内情報，各種案内情報)を旅客が発着するフロアにある大型映像表示器や液晶ディスプレイなどで表示するシステムである。三菱電機インフォメーションシステムズ㈱(MDIS)では，人に優しい空港を実現することをコンセプトにして利用者目線を考慮したシステム設計，表示器の設置レイアウト，画面デザイン，表示デバイスの選定，設置工事までFISソリューションとして提供している。近年の航空業界ではLCC(Low Cost Carrier)の台頭によって訪日外国人が増加し，旅客への空港案内のニーズ(多言語化や商業施設案内等)が多様化してきている。そのため，MDISでは旅客への空港案内のニーズに対応するため多言語化機能やデジタルサイネージ(Digital Signage：DS)機能を持ったFISパッケージを開発した。また，近年の空港は24時間化へ動き出しているため，ディスプレイの省エネルギー化を達成する三菱電機の特許を使用して環境対策を実現している。

今後，FISソリューションの付加価値向上，空港内トータルソリューションの実現を目指し，国内空港だけでなくグローバル市場でFISパッケージを販売するため，海外への提案活動にも力を入れていく。




**フライトインフォメーションシステムの空港内運用イメージ**

フライトインフォメーションシステムは空港内のあらゆるシーンで，フライト情報などを大型映像表示器や液晶ディスプレイへ表示し，空港を利用する旅客，来港者及び空港スタッフにリアルタイムで情報提供するシステムである。

*三菱電機インフォメーションシステムズ㈱　**三菱電機㈱ インフォメーションシステム統括事業部

## 1. まえがき

MDISでは，空港に関する情報を旅客，来港者及び空港スタッフに提供・表示するフライトインフォメーションシステム(FIS)のシステム設計から設置工事までを行うFISソリューションを提供している。

本稿では，FISソリューションとグローバル化への取組みについて述べる。

## 2. FISソリューション

### 2.1 機　能

FISは旅客，来港者及び空港スタッフに発着する航空機の出発時刻，行先，搭乗ゲート番号，到着時刻などのフライト情報や各種案内情報等の空港利用におけるあらゆるシーンで必要な情報を提供するシステムであり，フライト情報案内機能，チェックインカウンター案内機能，各種案内表示(DS)機能及び外部システム連携機能の4つの機能を持つ(**図1**)。

#### 2.1.1 フライト情報案内機能

フライト情報案内機能による情報提供は，次のとおりである。

(1) 出発便向けの案内

出発フロアを主な設置場所として，出発旅客や見送りの来港者向けに空港から出発する航空機の出発便情報を表示する。空港のシンボルとなる大型映像表示器や単体の液晶ディスプレイを出発旅客の動線上に配置することで，どこからでも出発便の情報を入手できる。出発便の搭乗口では，搭乗口ごとに表示器を設置することで，旅客が搭乗する航空機へ正確に案内する。

(2) 到着便向けの案内

到着フロアを主な設置場所として，空港に到着する航空機の到着時刻及び変更時刻などの到着便情報や，通関中，手荷物受取中，入国審査中などの到着旅客の状況を表示する。出迎えの来港者へ情報を提供することで，航空機がいつ到着するのか，旅客がどれくらいの時間で出てくるのかを知らせ，待ち時間のストレスがないよう案内する。

#### 2.1.2 チェックインカウンター案内機能

チェックインカウンター案内機能は，航空会社が受付業務を行っているカウンター情報(ファーストクラスはどこのカウンターで搭乗手続きを行うかといった情報等)を表示するシステムである。これによって，出発旅客に搭乗手続きを行うカウンターを案内する。また，各航空会社の個別の案内も自由に登録・案内表示することもできる。

#### 2.1.3 各種案内表示(DS)機能

出発便・到着便といった航空機の発着情報だけではなく，手荷物品の制限や検疫など，旅行者への注意喚起等の情報提供を行う。また，地震，火災などの緊急時の案内や，搭乗口までの距離，移動に必要な時間，店舗などの広告と

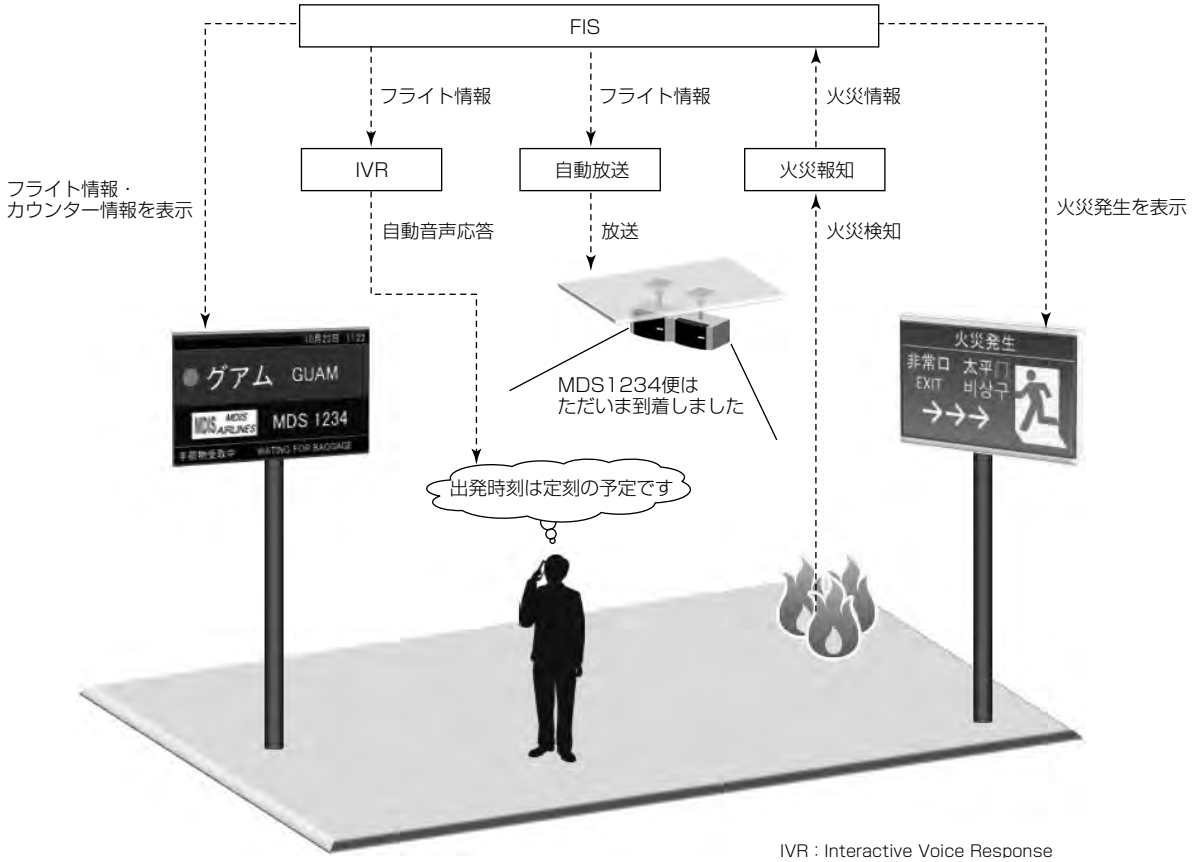



**図1．FISと外部システムの連携**

いった情報提供を可能とする。

### 2.1.4 外部システム連携機能

様々な外部システム(IVR，自動放送，火災報知)と連携することで，FISの表示器に連携している外部システムの情報を表示する。また，表示器による情報提供だけではなく，FISの情報を放送によって提供することも可能である。

## 2.2 特　長

FISソリューションのコンセプトは，“人に優しい空港を実現する”である。空港内の“誰が”“いつ”“どこで”“どのような”情報を必要とし，それに対して“どのように”分かりやすく伝えるか。この問題解決のため，最新技術の採用はもちろん，多言語化対応や省エネルギー等の環境対策も考慮した利用者目線での設計を特長として行っている。次にその詳細及び取組みについて述べる。

### 2.2.1 利用者目線を考慮したシステム設計

FISは，空港を利用する様々な人に必要な情報を提供できることを目的としている。また，空港の空間や設備を考慮して表示器の設置場所から表示器のデザイン，画面設計，設置場所に応じた表示内容まで利用者目線を考慮した設計を行う。

### 2.2.2 高信頼性・可用性

(1) サーバシステム

FISが停止してしまうと空港を利用する旅客及び空港スタッフを混乱させ，更に航空機の発着に影響を与える可能性がある。そのため，システムの中核となるシステムサーバは冗長化構成とし，信頼性向上を図っている。バックアップサーバを設置することで，万一システムサーバが停止した場合でもバックアップサーバに切り替えて運用を継続することができるように配慮している。

(2) 専用STBを用いた表示制御

システムサーバからデータを受信し，表示媒体へ表示するための表示制御装置には，専用のSTB(Set Top Box)を採用している。このSTBは，MDISも設計段階から携わり開発した装置である。その特長は，次の４点である(**図２**)。

(1) ファンレス・ディスクレス

故障の要因となる送風機(ファン)や記憶装置のための可動部(ディスク)がないため，長寿命であり，耐久性に優れている。

(2) データ蓄積型

万一システムサーバの停止やネットワーク不通の状態になっても，表示を維持して運用を継続できる。

(3) 個別設定不要

IPアドレスだけでどの表示器の画面も表示できるため，導入が容易である。また，メンテナンスによる交換時の作業量も軽減できて保守性もある。

(4) 同期機能

STB間で同期を取ることが可能なことから，表示の切替えタイミングを表示器間で同期することができる。表示切替えの同期によってタイムラグ等による表示器間の不整合を起こさない仕組みとなっているため，ストレスを感じさせないサービスを提供できる。

### 2.2.3 視認性の向上

空港は様々な人が利用するため，どんな人に対しても見やすい表示を行うことが必要である。FISソリューションでは，次の事項によって視認性向上を図っている。

(1) 画面設計

表示する項目，文字高，色合いで，表示器の設置場所や案内したい目的に合わせた構成を提供する。

(2) ユニバーサルフォント

健常者だけでなく，高齢者や障がい者にも視認しやすいようユニバーサルフォントによる情報の表示を行う。

(3) 大画面表示器

DLP(Digital Light Processing)表示器やマルチディスプレイを採用することで，視認性の高い表示，必要十分な情報量の表示を行うことができる。マルチディスプレイ構成では，コンテンツを拡大表示する方法は様々あるが，FISソリューションでは，ディスプレイ１面に対し表示制

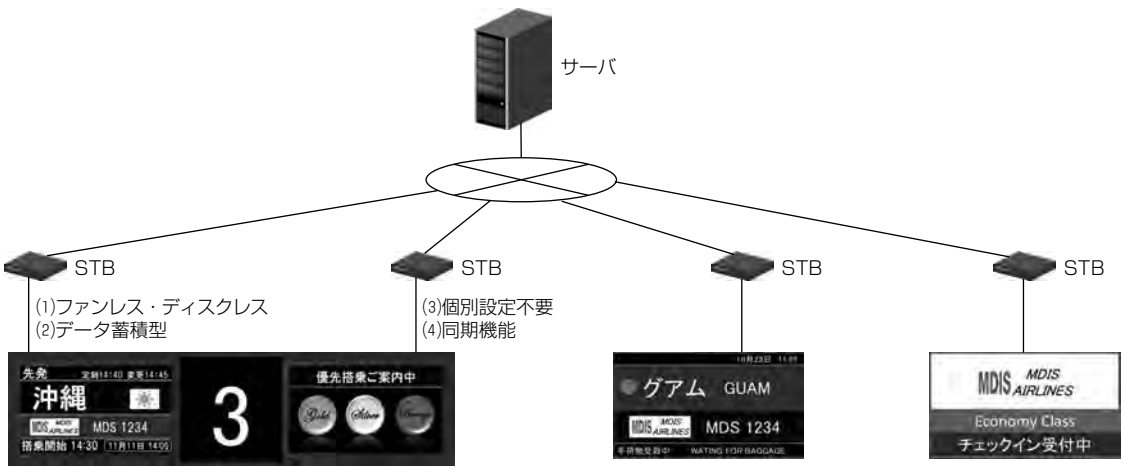



**図２．専用STBを用いた表示制御**


**図３．輝度調整機能**

御装置(STB)１台の構成を採用し，拡大表示しないシステムを構築する。これによって，表示時に解像度を落とさない鮮明な表示を可能とする。

### 2.2.4　多言語による表示

従来は，日・英の２か国語表示を標準仕様としていたが，外国人利用客の増加に伴い多言語表示での案内が必須となってきた。FISソリューションでは，日・英・中・韓の４か国語表示を基本としたシステムを提供している。

### 2.2.5　省エネルギー

液晶ディスプレイを採用するシステムが増加してきたことに伴い，システム運用で，省エネルギー，機器の寿命延長を目的とし，三菱電機が取得した特許[1]を適用したシステムを構築している。このシステムは，液晶ディプレイ上に表示する案内がある場合は輝度を上げて表示を行い，表示する案内がない場合は輝度を下げるというものであり，液晶ディスプレイの稼働を維持しつつ，省エネルギーを実現できることが利点である(**図３**)[2]。また，液晶ディスプレイの電源を切ると案内する情報がないのか故障なのか液晶ディスプレイの状態では判別できないという問題が生じるが，このシステムではその問題を回避できる。

## 3.　グローバル化への取組み

### 3.1　FISパッケージの開発

当社のFISは第１世代(クライアント／サーバ方式)，第２世代(STB方式)と進化し，日本国内市場向けに機能拡張を行ってきた。第２世代は約10年前に開発したシステムであり，現在の多様なニーズを満たせない部分が出てきている。また，日本以外に目を向けると空港の新設／拡張が計画されている国々があり，MDISではFISを中国市場向けに販売することを進めている。そのため，国内向けには最新技術を用いた新しいソリューションの提供，国外向けには中国仕様の標準要件に適合した機能開発を目的にFISパッケージの開発を行った。

### 3.2　FISパッケージの特長

FISパッケージの主な特長は次のとおりである。

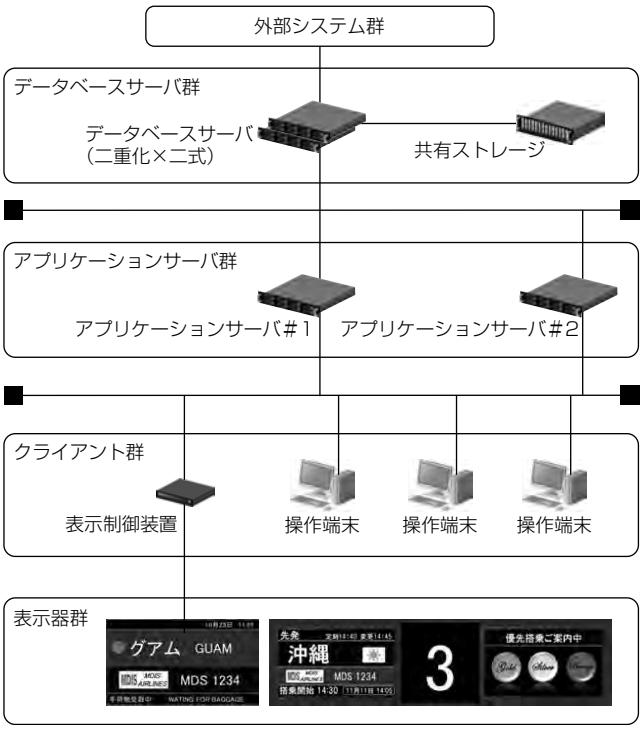



**図４．３層アーキテクチャシステム構成**

(1)　システム統合

これまで別システムであったフライト情報案内システム，チェックインカウンター案内システム，DSシステムを１つのシステムに統合した。統合することによってFIS機能の差別化を行った。これによって，フライト情報表示を行う表示器でも運用者がDS表示に切り替えることができるようになり，表示器の表示内容の自由度を向上させた。

(2)　表示制御装置のパソコン化

FISパッケージでは表示制御装置をSTBからパソコンに変更した。STBより性能が高く，汎用性の高いパソコンを採用することによって，高解像度の画像や高負荷の動画コンテンツの再生，プッシュ型ブラウザへの表示等が可能となった。パソコンを採用することで価格競争力の強化と，最新技術への追随を容易にした。

(3)　３層アーキテクチャ

システム統合によって，サーバ構成の見直しや空港に離発着する航空便数の増加に対応したシステム拡張が必要となっている。また，中国市場では管理する表示器数が日本より多い構成となっているため，３層アーキテクチャによってスケーラビリティの向上を図っている(**図４**)。

(4)　カスタマイズ性の高いフライト案内画面

従来システムではFISで表示する画面レイアウトは運用者が変更できない仕様(ベンダーだけ変更可能)となっていた。FISパッケージでは，画面デザイン編集ツールを開発することによって，運用者でも容易に画面のレイアウトを変更できる機能を追加した。なお，画面デザインの編集は中国市場向けの要件である。これによって，運用者が各空

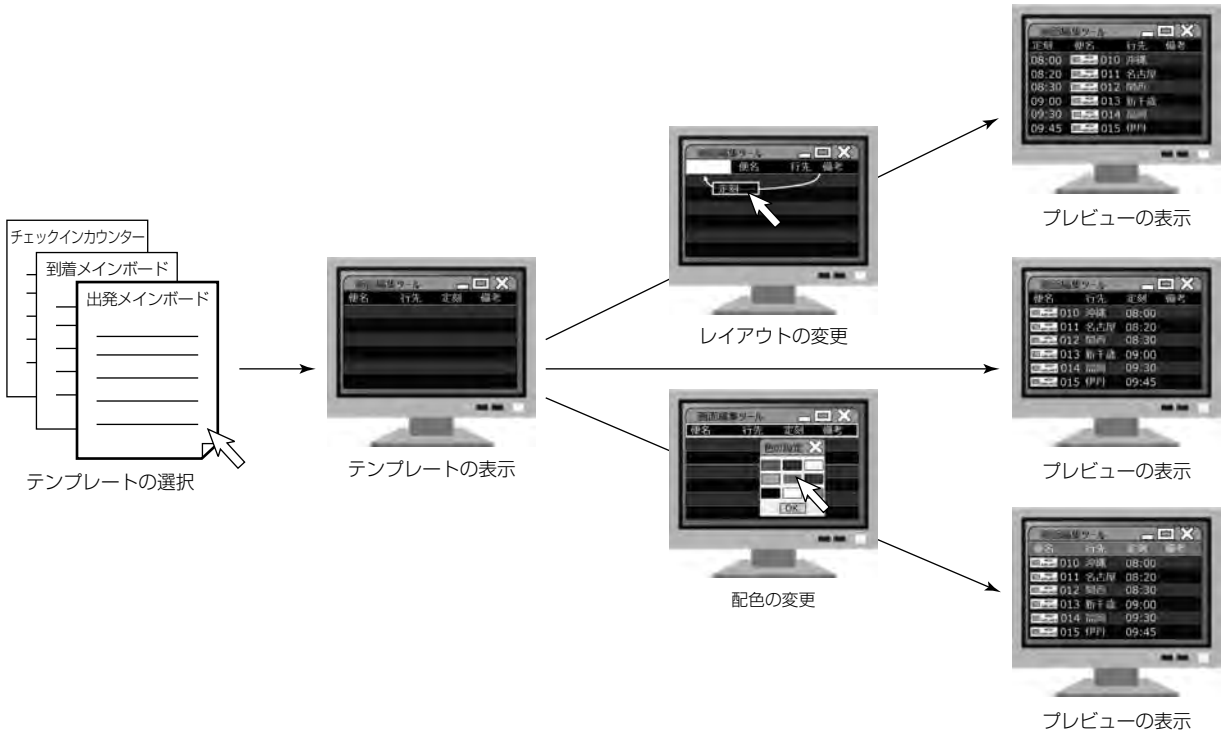



**図５．画面デザイン編集ツール**

港の状況に合わせてタイムリーに画面レイアウトを変更することができるようになった(**図５**)。

⑸　操作端末の多言語化への対応

従来システムでも表示器は日・英・中・韓の４か国語に対応していたが，操作端末の多言語対応化が課題であった。FISパッケージでは，中国市場向けに，日・英・中を基本とした操作端末の多言語化への対応を行い，その他の言語もサポート可能としている。

## 4. 今後の展開

### 4.1　ソリューションの今後の展開

テロや犯罪などの空港を取り巻く問題は多く，空港利用者に安心・安全を提供するためのセキュリティ対策は最重要課題となっている。

MDISでは，監視カメラなどによる侵入検知システムや外周警備システム，映像解析システム等とのシステム連携によってFISソリューションへ付加価値を加え，空港内トータルソリューションの実現を目指し，顧客にとって使いやすく，安心・安全に空港を利用してもらえるソリューションの更なる開発を目指していく。

### 4.2　グローバル化に向けた今後の展開

MDISでは現在グローバル化への対応として，アジア地域の市場調査を実施し，アジア市場で要求される機能の抽出を行っている。これによって，FISパッケージの機能を拡張していくとともに，空港内トータルソリューションとして海外への販売活動にも注力していく。

## 5. むすび

MDISのFISソリューション及びグローバル化への取組みについて述べた。MDISでは2007年から次世代空港プロジェクト“フライトビジョン”を発足させ，現在も継続的なFISソリューションの機能拡張を進めている[(3)(4)]。今後も2020年の東京オリンピックに向けてFISの重要性が高まることが予想されるため，DS機能の強化や空港セキュリティとの連携を目指し，拡張性の高いシステムを構築していく。

## 参考文献

⑴　渡辺一博：表示輝度制御装置及び表示輝度制御プログラム，特許第4352096号（2010）
⑵　渡辺一博，ほか：那覇空港におけるフライト情報表示設備の省エネルギー化，三菱電機技報，**86**，No.1，20（2012）
⑶　MDIS：空港表示システム フライトビジョン
http://www.mdis.co.jp/products/flightvision/
⑷　米沢みどり，ほか：デザインアプローチ手法による次世代空港サービスのコンセプト創出，三菱電機技報，**89**，No.8，462～465（2015）

特集論文

# 快適・安心・発展を提供するITソリューション開発運用基盤

山足光義* 大澤伸行*
米沢みどり* 高畑泰志**
小笠原大治*

*System Development and Operation Environment for IT Solution Providing Comfort, Safety and Growth*

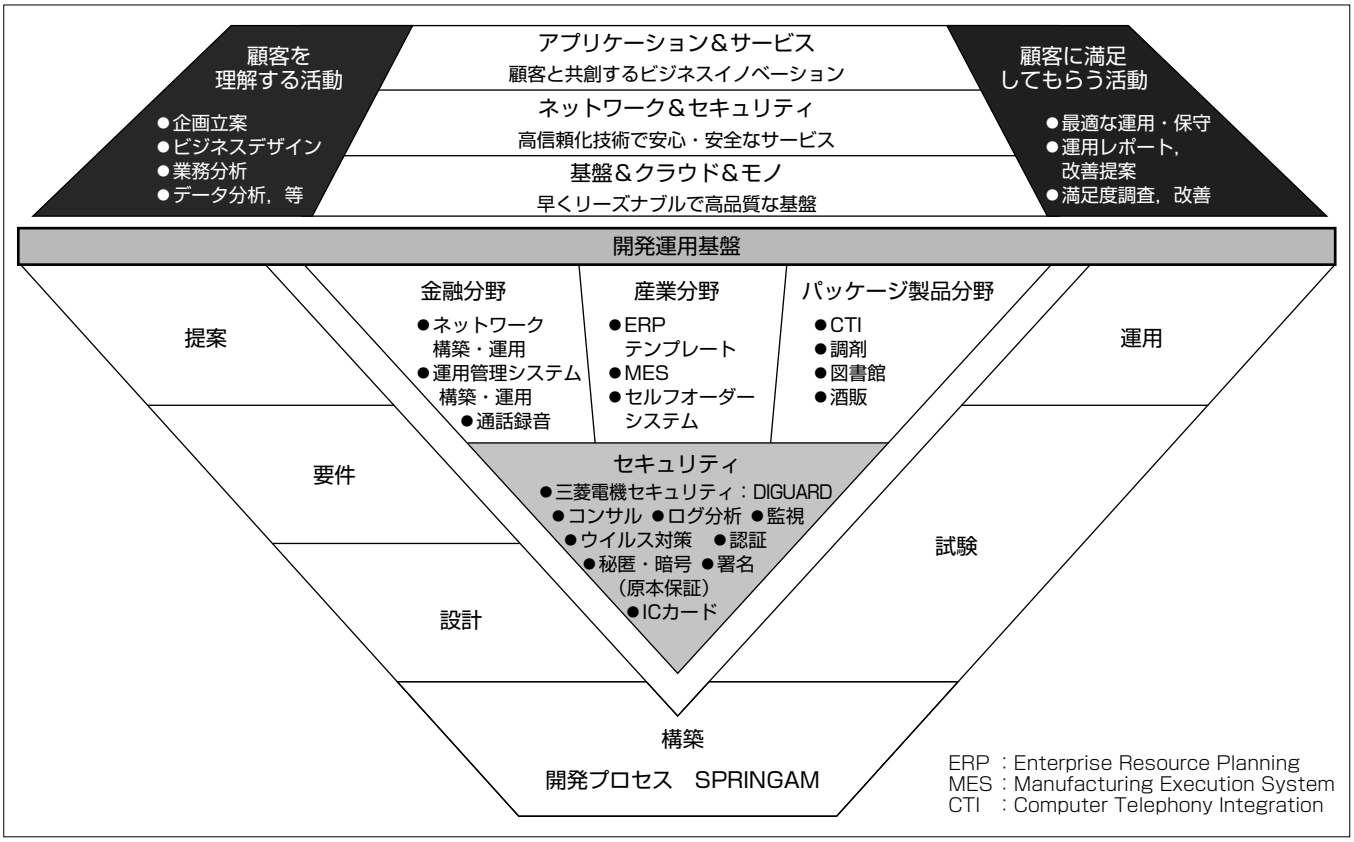
*Mitsuyoshi Yamatari, Midori Yonezawa, Daiji Ogasawara, Nobuyuki Oosawa, Yasushi Takahata*

**要　旨**

IT技術が私たちの生活に広く浸透し，既にIT技術なしでの生活が考えられない状況の中，“快適・安心・発展を支えるIT技術”は，全ての企業で必須となっている。快適・安心・発展をどのような形で提供するかは，企業によって千差万別である。三菱電機インフォメーションシステムズ㈱(MDIS)では，顧客の立場に立って，最適な快適・安心・発展が提供できるよう，“ダイヤモデル”という概念に基づいたITソリューションを提供している。

ダイヤモデルは，顧客を理解し，顧客に満足してもらえる快適・安心・発展を提供するための価値を創造する活動と，その価値をV字型モデル(開発運用基盤)で実現する活動の2つで構成している。顧客に提供する価値としては，“顧客と共創するビジネスイノベーション”“高信頼化技術で安心・安全なサービス”“早くリーズナブルで高品質な基盤”の3つの階層的な価値を設定する。“デザインアプローチ(1)”による共創，脆弱(ぜいじゃく)性対策支援デスクなどによる安全・安心対策，自動化技術による生産性向上を，V字型モデルの開発プロセスを通して，先進的な開発運用基盤で実現している。

MDISでは，金融分野，産業分野，パッケージ製品分野等でITシステムを開発しているが，それらの開発に，この基盤を適用し，“快適・安心・発展”を提供できるよう，基盤の最新化と整備・展開に取り組んでいる。




**ITソリューション開発運用基盤の概念モデル**

MDISでは，顧客ごとに個別に価値を提供するため，顧客を理解する活動を起点として，V字型モデルの開発プロセスを通し，様々な分野でITソリューションを開発・提供し，最終的に顧客に満足してもらうことを目指した活動を展開している。その活動をダイヤモデルとして体系化し，モデルに沿った開発運用基盤の整備，開発を進めている。

*三菱電機インフォメーションシステムズ㈱ **同社(情報学博士)

## 1. まえがき

近年，IT技術が社会のすみずみに普及し，快適・安心・発展を支えるIT技術がもはや当たり前のように考えられるようになってきた。MDISでは，快適・安全・安心を具体的にどのようにして提供するべきかを“価値”という形で捕らえ，その価値をMDISが顧客の立場で考え，提供できるようにするための活動を“ダイヤモデル”という概念で体系化している。このダイヤモデルを支えているのが，開発運用基盤，すなわち，MDISのシステム生産標準である“SPRINGAM[(1)]”であり，SPRINGAMが提供する各種標準化ガイド及び活用ソフトウェア群である。

**2章**でこのダイヤモデルの３つの階層(①アプリケーション＆サービス，②ネットワーク＆セキュリティ，③基盤＆クラウド＆モノ)について，**3章**で①の価値である顧客と共創するビジネスイノベーションについて，**4章**で②の価値である高信頼化技術で安心・安全なサービスについて，**5章**で③の価値である早くリーズナブルで高品質な基盤についてそれぞれ説明し，このダイヤモデルの特長及び開発運用基盤について述べる。

## 2. ダイヤモデル

MDISでは，開発運用基盤の整備をダイヤモデルを通して，常に最新化している。ダイヤモデルは，顧客に満足してもらえるITシステムを常に提供できるようにするため，顧客を理解し，顧客に合った価値を創造する活動と，その価値を開発運用基盤で実現する活動の２つから構成される。

ダイヤモデルには，アプリケーション＆サービス，ネットワーク＆セキュリティ，基盤＆クラウド＆モノの３つの階層がある。アプリケーション＆サービスでは，顧客のビジネスを向上させるという最も重要な視点から，“顧客と共創するビジネスイノベーション”を設定した。そして，ネットワーク＆セキュリティでは，安心して提供できるという点を重視した“高信頼化技術で安心・安全なサービス”を，また，基盤＆クラウド＆モノでは，情報システム開発で最も基本となる“早くリーズナブルで高品質な基盤”を価値として設定した。

これらの価値を顧客ごとに具体化していくため，まずは，顧客を理解する活動を実施する。この活動はデザインアプローチというMDISの特長ある手法を取り入れて行っている。この手法によって顧客の潜在ニーズを見える化し，顧客が本当にほしい魅力的な要件を定義したシステムを提案することができる。これらの活動を通して，顧客と共創するビジネスイノベーションという価値を生み出している[(2)]。また，提案するシステムではセキュリティを重視し，脆弱性に敏速に対応できる脆弱性対策支援デスクやログ分析による不正な挙動検知など安心・安全なサービスを提供する。さらに，システム開発には品質を担保するため，実績のある製品とその製品を利用した開発手順を開発フレームワークとして整備している。開発者スキルの未成熟に起因する不具合混入を低減させるとともに，仕様書からプログラムソースを自動生成させたり，設計書から試験仕様を自動生成させる等，自動化技術を様々な開発フェーズで取り入れて低コスト化も実現している。これらの活動を通して，顧客に満足してもらえるシステムの提供を図っている。

## 3. 顧客と共創するビジネスイノベーション

この章では，顧客と共創するビジネスイノベーションを実現するためのデザインアプローチについて述べる。デザインアプローチは，顧客をよく理解することで，システムに期待される要件を明らかにし，魅力的なシステム提案に結び付けていくMDIS独自の新しい手法である。従来の課題解決型の手法であるリサーチアプローチに対して，デザインアプローチは，あるべき姿，理想像を考えてから現実的な解に落とし込んでいく手法であり，具体的には，ユーザーエクスペリエンス，バックキャスティング，フィット＆ギャップ分析の３つのプロセスから構成される(**図1**)。

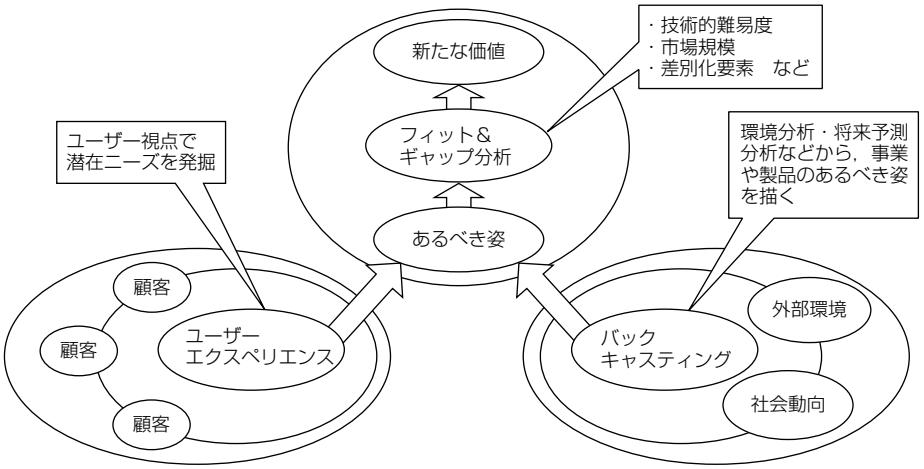



**図1．デザインアプローチ**

ユーザーエクスペリエンスが，ユーザー視点で潜在ニーズを発掘するプロセスである。顧客も巻き込んで，現行システムやプロトタイプを用いたユーザーの行動観察(エスノグラフィ)などを実施し，顧客自身も気が付かなかったようなニーズを発掘する。バックキャスティングは，マクロ環境分析，将来予測分析などを実施するプロセスである。これら２つのプロセスを通して，事業や製品のあるべき姿，将来ビジョンを描いていく。この段階では技術的な制約などを考慮せず，本来あるべき理想的な姿を自由に発想することが重要である。最後に実現可能なソリューションに落とし込むために，フィット＆ギャップ分析のプロセスを実施する。ここで技術的難易度，市場規模，差別化要素などのフィルタリングを行うことで，初めて実現性のある新たな価値の提案が可能となる。

これらのプロセスを実際の商談で実践し，コンセプトをまとめあげるために有効な各種テンプレートや具体的なノウハウを標準化ガイドの形で整備することで，独自の体系を構築してきた。これによって，従来の課題解決型の手法であるリサーチアプローチだけでは得られない新しいイノベーションが期待できるようになった。このプロセスを継続的に実践し，有効性が確認できた手法やノウハウを開発運用基盤に適宜追加し，充実化を図っている。

## 4. 高信頼化技術で安心・安全なサービス

この章では，高信頼化技術で安心・安全なサービスを実現するための“脆弱性対策支援デスク”について述べる。

近年ますます激化・複雑化するセキュリティへの脅威から，顧客の安心・安全を確保するためには，問題を迅速に解決することが非常に重要になってきている。特に，日々大量に発生する脆弱性問題は，最近事例が増加している特定の個人や組織・情報を狙った標的型攻撃の入口や踏み台としても利用される場合が多い。このため，脆弱性問題の発覚後，情報収集と対策の検討を素早く行い，顧客への対応を的確に行う必要がある。

顧客への対応の迅速化対策のため，開発運用基盤の１つとしてMDIS社内に脆弱性対策支援デスクを設置している(**図２**)。支援デスクでは，脆弱性情報の収集，対象や影響確認，原因確認，対策検討と脆弱性に関する情報を一元管理し，顧客に提供したシステムが安心・安全に稼働できるよう，敏速な対応ができる環境を構築している。

支援デスクでは，日々大量に発生する脆弱性情報から，顧客が必要とする情報のみを抽出する作業の効率化も進めている。これは，国内外の脆弱性関連情報とその対策情報を日々大量に提供しているJVN(Japan Vulnerability Notes)データベース(注1)から，顧客が利用しているシステム構成に応じた脆弱性情報だけを，ほぼ自動で抽出するシステムを構築することで実現した。脆弱性が発見された場合，顧客対応のシステムエンジニアと連携し，いつ修正を提供するかなどの調整を顧客も含めて行い，敏速な対応を実施している。今後もこれらの取組みを通じ，顧客の信頼を得るため，セキュリティ対策の強化を進めていく。

(注１)　JPCERT(Japan Computer Emergency Response Team)コーディネーションセンターと(独)情報処理推進機構(IPA)が共同で運営

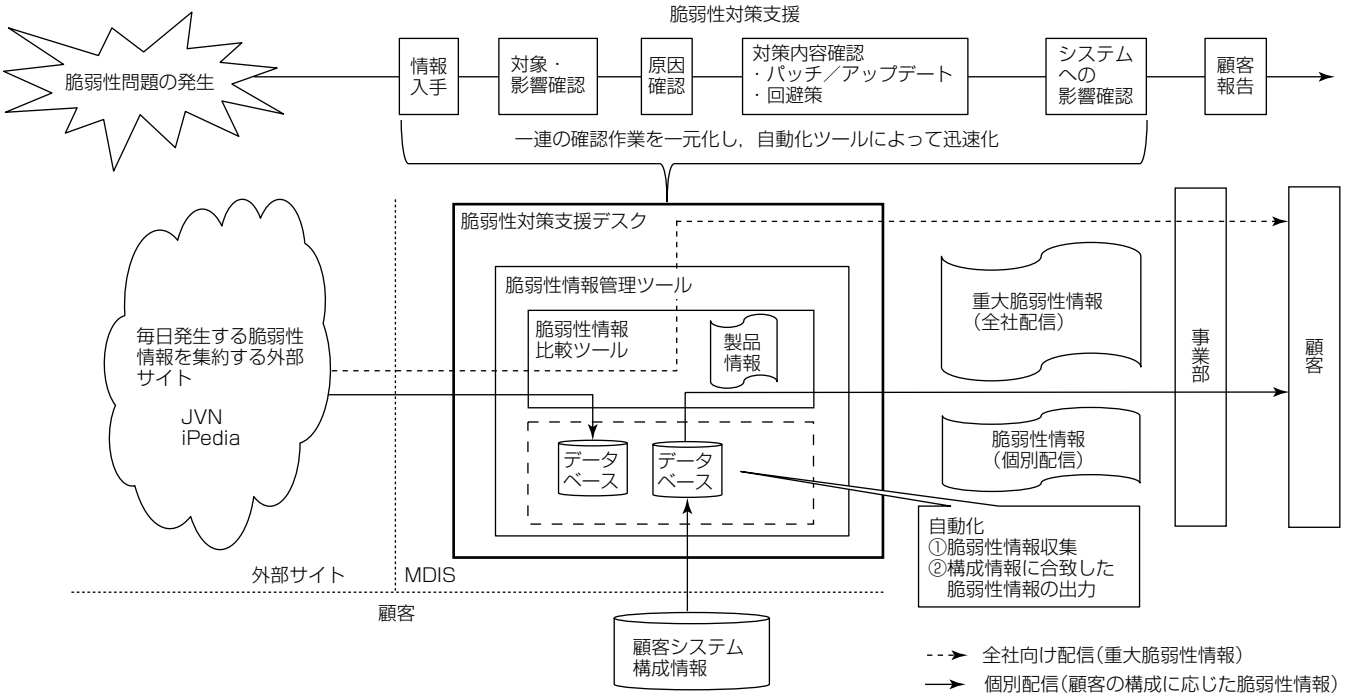



**図２．脆弱性対策支援デスク**

## 5. 早くリーズナブルで高品質な基盤

この章では，早くリーズナブルで高品質な基盤を実現するための自動化による生産性向上への取組みについて述べる。システム開発の生産性向上を実現するために，設計から試験，さらにはシステムの構築・運用まで，様々な開発フェーズで自動化技術を利用しているが，ここではその中でもベースとなる見える化とシステム構築作業の自動化，及びシステム運用の自動化について述べる。

### 5.1 見える化

市場での多くのシステム開発では，新規システムの開発より，老朽化したシステムの更改や既存システムの機能拡張等の開発の占める割合が大きくなってきている。この既存システムをベースとしたシステムの開発を，品質を維持したまま迅速に行うためには，現行システムを常に見える化できることが重要である。特に仕様書と稼働中の現行システムとの間に乖離(かいり)がある場合は必須である。また，見える化は，システム構築の自動化を実現するためのシステムの基本データ収集という視点からも重要であり，開発運用基盤では特に力を入れている項目である[3]。見える化によって自動抽出したシステムの情報は，データベースに蓄積し，下流の様々な開発フェーズや構築，運用の自動化のための情報として利用している(**図3**)。

開発運用基盤が提供する見える化機能の大きな特長に，マルチ言語対応がある。対象システムは，通常，Java(注2)，Visual Basic(注3)，Microsoft社の.NET Framework向けのVisual Basic .NETなど様々なプログラミング言語で更に様々なバージョンの言語仕様でプログラミングされているため，特定の言語に依存せずに，“プログラム呼出し”“画面遷移”などの情報を獲得することができる機能はシステムの構造を把握する上で必須である。この機能を実現するため，システムから見える化すべき項目を洗い出して抽象化し，抽象化した概念と各言語の特徴を対応付けて定義した。これによって，マルチ言語をサポートした様々な見える化ツールを開発した。

それらツールによるボトムアップからの分析とガイドによって業務フローを明確化するトップダウンからの分析の両方によって，不要機能抽出等，システム全体の見える化を実施している。

(注2) Javaは，Oracle Corp. の登録商標である。
(注3) VisualBasicは，Microsoft Corp. の登録商標である。

### 5.2 システム構築作業の自動化

サーバ仮想化技術はシステム統合を容易にし，リソースの有効活用を実現した。しかし統合することでサーバ数が増加し，ネットワークも複雑化して構築作業時のパラメータ等の設定誤りや管理者が容易に他のサーバを削除できてしまうというリスクが顕在化している。そこで，MDISでは仮想サーバの構築作業やネットワーク設定，仮想サーバへのストレージ割当てなど，従来，手順書を基に人手で1台ずつ行っていた構築作業をソフトウェアの利用やプログラムの実装で自動化する技術に取り組んでいる。これによって，手作業による設定誤りや誤削除などの人的ミスを軽減し，大量サーバの確実な構築を実現していく(**図4**)。

### 5.3 システム運用の自動化

構築したシステムの運用業務は，顧客ごとのポリシーや採用するベンダー製品に依存して，その運用内容が異なるため，顧客ごとに最適な運用手順書を作成するとともに，オペレータの育成と確実な運用作業遂行体制の提案を行い，これによって顧客システムの安定稼働を支えている。MDISでは，更なる安心を提供するため，①日次作業自動化(システムログ監視)，②月次作業自動化(待機系仮想サーバとの同期)，③臨時作業自動化(サイバー攻撃検知

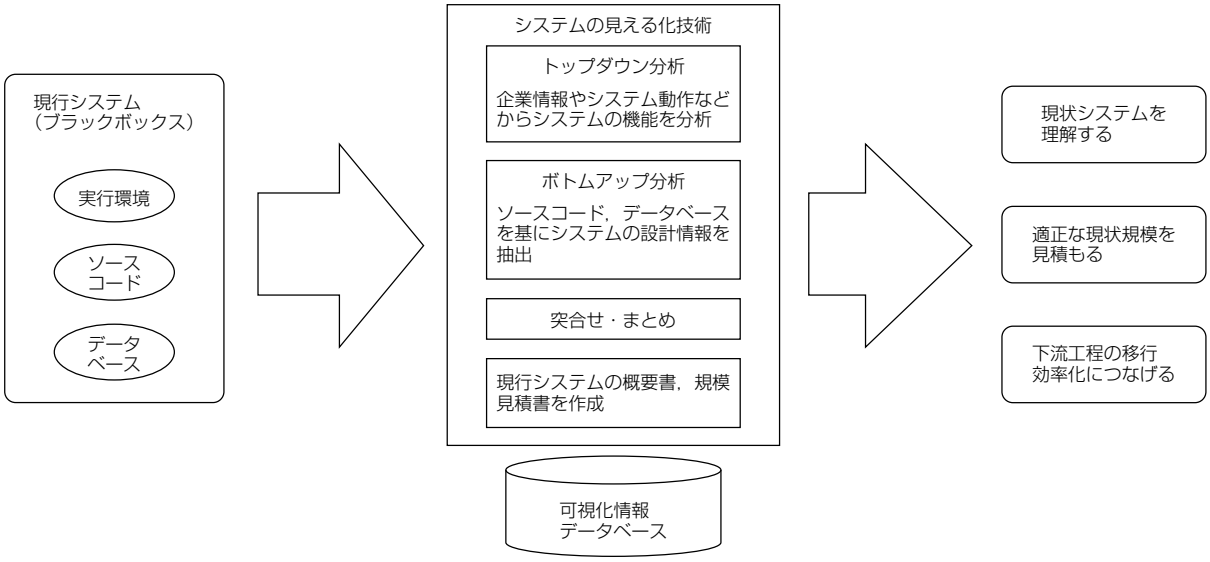



**図3．見える化技術概要**

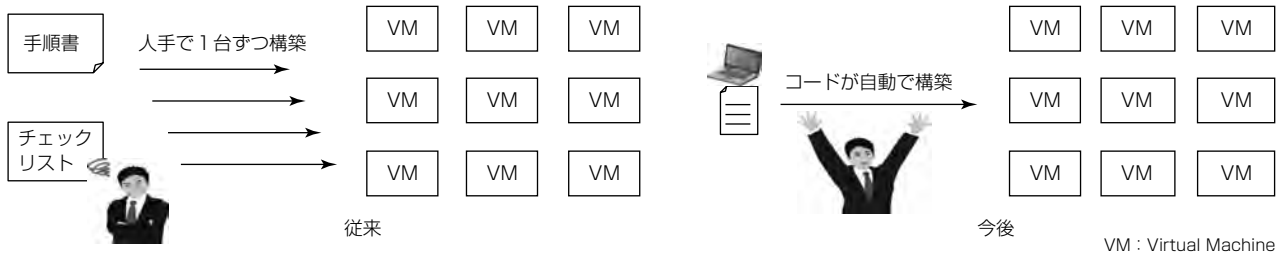



**図４．システム構築作業の自動化**

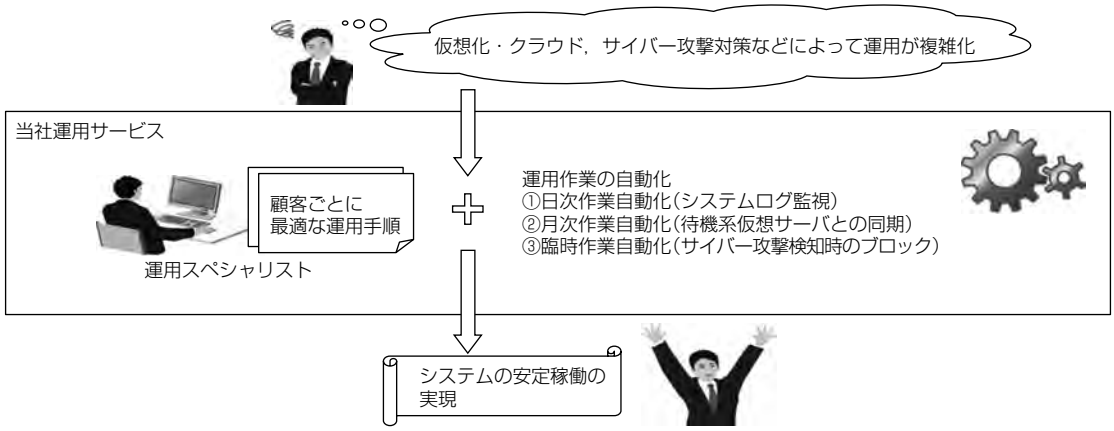



**図５．運用作業の自動化**

時のブロック)などに取り組んでいる。仮想化・クラウド活用によるサーバ台数増や，サイバー攻撃対策によって複雑化の一途をたどる顧客のシステム運用作業を，MDISの運用スペシャリストとこれら自動化技術を組み合わせることで，顧客システムの安定稼働の実現を支えていく(**図５**)。

## 6. む　す　び

オンプレミスのシステム構築を実現する開発運用基盤について，ダイヤモデルと価値を実現する開発運用基盤の特長について述べた。現在，新しい開発運用基盤として，クラウド上でのシステム構築を実現する開発運用基盤，さらに，これらの２つを連携させたハイブリッドシステムを構築する開発運用基盤を整備している。クラウド上のシステム構築では，アジャイルをベースとし，様々なサービスを連携させる連携基盤を提供する。ハイブリッドシステムの構築では，暗号化技術をベースにした，よりセキュアで安全性を実現した連携機能を提供する。これらの３つの開発運用基盤を，“スリーダイヤモデル”として今後注力していく。また，本稿で述べた開発運用基盤も，React(注4)などの最新のOSS(Open Source Software)製品等を都度取り入れ，より洗練された開発手順(開発フレームワーク)として継続整備していく。

(注４)　Reactは，Facebook Inc. の登録商標である。

## 参　考　文　献

(1)　藤原良一，ほか：プロセス改善による高品質ITソリューションの提供に向けたCMMIレベル5達成への軌跡，三電電機技報，**80**，No.9，953～598 (2006)
(2)　米沢みどり，ほか：デザインアプローチ手法による次世代空港サービスのコンセプト創出，三電電機技報，**89**，No.8，462～465 (2015)
(3)　堀田朋子，ほか：大規模な現行システムを効率的に見える化する技術，三電電機技報，**88**，No.8，471～477 (2014)

特集論文

# 高可用性を実現する“MIND HAシステム”

平島栄一*
佐藤彰洋*
渡辺和也*

*"MIND HA System" for High Availability*

*Eiichi Hirashima, Akihiro Sato, Kazuya Watanabe*

**要　旨**

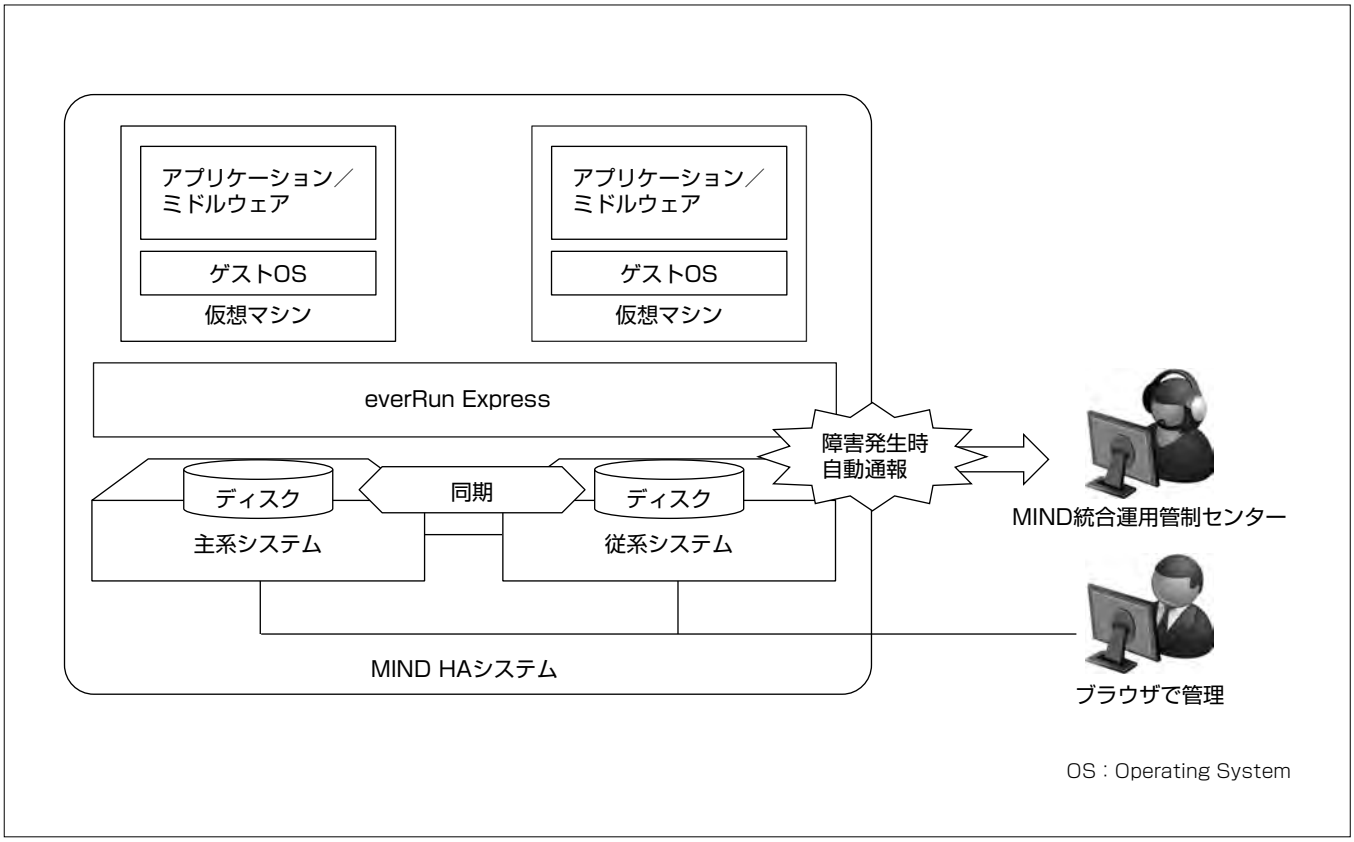
三菱電機インフォメーションネットワーク㈱(MIND)では，ユーザーのIT(Information Technology)プラットフォームの可用性・保守性を向上させるための高可用性サーバ製品を提供している。高可用性サーバ製品としては，中・大規模で停止するとビジネスに多大な損害をもたらすビジネスクリティカルなシステムや，停止してはならないミッションクリティカルなシステムをターゲットに無停止型サーバftServer(注1)の販売と保守を行ってきた。

2015年度には高可用性サーバ製品として新たに，小規模ではあるが停止するとビジネスに多大な損害をもたらすようなビジネスクリティカルなシステムをターゲットに2台のサーバと高可用性ソフトウェア製品“everRun(注1) Express”を組み合わせて構成した“MIND HA(High Availability)システム”の販売を開始した。HAクラスタシステムは，ハードウェアの冗長化によってハードウェア故障によるシステム停止時間を短縮した稼働率の高いシステムであるが，MIND HAシステムは従来のHAクラスタシステムと比較して次の特長を持つ。

・低コストでの導入
・従来のHAクラスタシステムよりも高い可用性
・容易な運用
・保守窓口の一元化

このシステムによって低コスト・短期間で，保守性も高いHAクラスタシステムの導入が可能である。

(注1)　ftServer，everRunは，Stratus Technologies Bermuda Ltd.の登録商標である。




**MIND HAシステム**

MIND HAシステムは，2台のサーバとeverRun Expressのシンプルな組合せで構成しており，低コストかつ短期間で高可用性の仮想化基盤を実現できる。OSやユーザーのアプリケーションはHA機能によって保護された仮想マシン上にインストールして使用する。また，仮想マシンのインストールやシステムの設定・操作はWebブラウザから実行する。MIND HA システムは，MIND統合運用管制センターでの遠隔監視による保守サービスを提供している。ハードウェア障害発生時の対応としてMIND統合運用管制センターへ自動通報を行っている。

*三菱電機インフォメーションネットワーク㈱

## 1. まえがき

近年の経済活動ではグローバル化・24時間化に伴い，停止するとビジネスに損害をもたらすような重要なアプリケーション，いわゆるビジネスクリティカルアプリケーションが増加している。従来は，ビジネスクリティカルアプリケーションはサーバの台数が10台を超えるような，中・大規模なシステムで構築・運用し，対処されてきた。MINDでは，このような中・大規模なシステムのビジネスクリティカルアプリケーションや，より重要性の高いミッションクリティカルアプリケーションを使用するユーザーのITプラットフォームの可用性・保守性の向上をターゲットとして，無停止型サーバftServerの販売・保守を行ってきた。

一方で，サーバの台数が1～2台の小・中規模なシステムでも，可用性を向上させたいとの需要が高まってきている。これは，現在のITシステムがあらゆるビジネスの根幹を支えており，規模の大小に関わらず重要性が高いためで，これらのITシステムに予期せぬ障害が発生した場合のビジネスへの影響は大きい。しかし，重要性が高くてもシステムの規模から，高可用化に必要な初期導入コストや運用コストを抑制したいというニーズも高い。このニーズに対応するために，MINDでは2015年度に高可用性サーバ製品として新たに小・中規模でビジネスクリティカルなシステムをターゲットにしたMIND HAシステムの販売を開始した。

本稿では，従来のシステムにおける課題について触れた後，このシステムの特長と機能，課題の解決策について述べる。

## 2. 従来のHAクラスタシステムの課題

ビジネスクリティカルなアプリケーションが動作するシステムを高可用化するための解決策の1つとして，HAクラスタシステムの採用がある。HAクラスタシステムは，ハードウェアの冗長化によってハードウェア故障によるシステム停止時間を短縮した稼働率の高いシステムである(**図1**)。HAクラスタシステムは，稼働する主系システムと待機用の従系システムを2台のサーバと共有ストレージ装置で構成している。HAクラスタシステムには，2台のサーバの両方にOSとクラスタソフトウェア，ビジネスアプリケーションをインストールする。通常時は主系システム上でビジネスアプリケーションが稼働し，データは共有ストレージ装置に書き込まれている。この主系システムをクラスタソフトウェアが常時監視しており，サーバのディスクやネットワークの故障，電源断などのハードウェアの障害発生をクラスタソフトウェアが検知して，自動的に主系から従系にシステムを切り替えるという仕組みになっている。この後，従系システムのアプリケーションは共有ストレージ装置からデータを読み出して，処理を引き継いでいく。

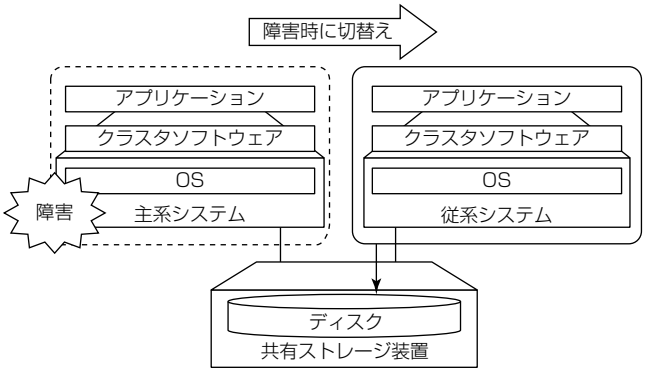



**図1．従来のHAクラスタシステムの構成**

従来のHAクラスタシステムには，次に述べる4つの課題がある。

### 2.1 高コスト

従来のHAクラスタシステムは中・大規模なシステムをターゲットにしているので，システム構成が複雑である。また，主系・従系システムや共有ストレージ装置のハードウェアOS・クラスタソフトウェアから構成されているため，高い初期導入コストが必要である。加えて，各ハードウェアやソフトウェアの機能が多いので構築と検証のための作業時間を多く確保する必要があり，構築期間や構築コストが増大しがちである。

### 2.2 単一障害点の存在

2台のサーバと共有ストレージ装置を用いて構築するHAクラスタシステムは，単一障害点(Single Point Of Failure：SPOF)を内包している。単一障害点とは，1つの装置故障によって，システムが停止する箇所のことである。HAクラスタシステムでの単一障害点はデータ格納用に使用する共有ストレージ装置である。この共有ストレージ装置が故障すると，データ損失が発生して，HAクラスタシステム全体が停止することになる。

### 2.3 ユーザーでの難しい運用

HAクラスタシステムでは，主系システムが故障しても従系システムに自動的に切り替わる仕組みとなっているため，主系システムが故障して従系システムに切り替わったことに気づかず運用を継続してしまうことが起こり得る。その場合，さらに従系システムが故障するとHAクラスタシステム全体が停止してしまう。このようなシステムの停止を防ぐためには，障害発生をいち早く検知し，故障部分を交換して二重化状態へ速やかに復旧させることが重要である。

しかし，障害発生をいち早く検知するためには，監視要員の定期的な目視確認による監視が欠かせない。また，その検知した障害の速やかな復旧のためにはスキルのある復旧要員の待機が必要である。さらに，重要なシステムであれば24時間365日対応での体制構築が必要になるなど，ユーザーでの運用が難しい場合が多い。

### 2.4　分散した保守窓口

HAクラスタシステムで障害が発生した場合には，障害の切り分けを行い原因の分析や原因に応じた各ベンダーへの問合せが必要となる。このとき，ベンダーはハードウェア(サーバ・共有ストレージ装置)とクラスタソフトウェアごとに存在するので保守作業が煩雑になる。

MIND HAシステムでは，これら４つの課題を解決する。

## 3. MIND HAシステム

MIND HAシステムは，２台のサーバと高可用性ソフトウェア製品everRun Expressとの組合せで実現した製品である。everRun Expressは２台のサーバにインストールし，１つの仮想化基盤として動作する。仮想化基盤上にはHA機能によって保護された仮想マシンを構築することができる。この章ではMIND HAシステムの４つの特長と**２章**の課題の解決策について述べる。

### 3.1　低コストでの導入

MIND HAシステムはシンプルな構成で共有ストレージ装置が不要であるため，機器コストを低減できる。またMINDで既に評価済みの構成をセットアップして出荷するので，ユーザーはこのシステムの到着後すぐに仮想マシン構築とアプリケーションの設定に着手できる。仮想マシンへの二重化ソフトウェアのインストールや既存アプリケーションの修正は不要で，HAクラスタシステムに非対応のアプリケーションであっても簡単に二重化を実現できる。これらの特長によって，構築コストの低減や構築期間の短縮を実現し，**2. 1節**で述べた高コストの課題を解決する(**図２**)。

### 3.2　従来のHAクラスタシステムよりも高い可用性

MIND HAシステムは，共有ストレージ装置を使用せず内蔵ストレージだけで動作するので，従来のHAクラスタシステムで単一障害点であった共有ストレージ装置を排除できる。この特長によって，**2. 2節**で述べた単一障害点存在の課題を解決する。さらに，ディスクやネットワークが故障した場合，everRun Expressは無停止で従系システムに切り替えるので，高い可用性を実現する(**図３**，**図４**)。

一方，サーバのCPU(Central Processing Unit)や電源を始めマザーボードやRAID(Redundant Arrays of Inexpensive Disks)コントローラの故障や電源断などでサーバ停止が発生した場合にも，従系システムに自動的に切り替えて処理を継続する(**図５**)。

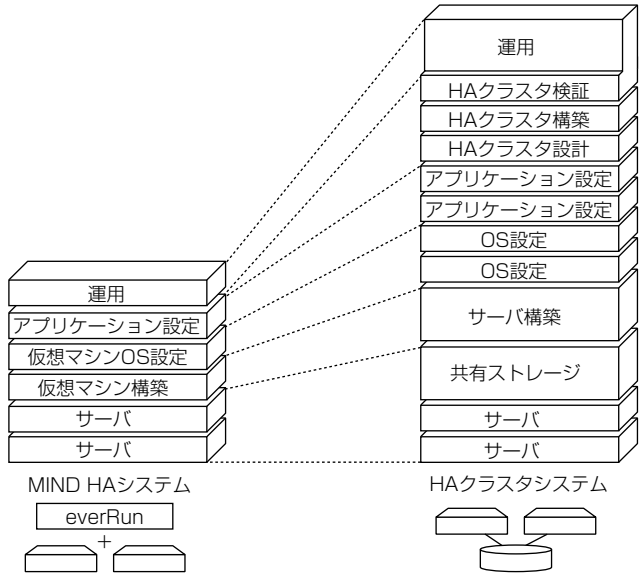
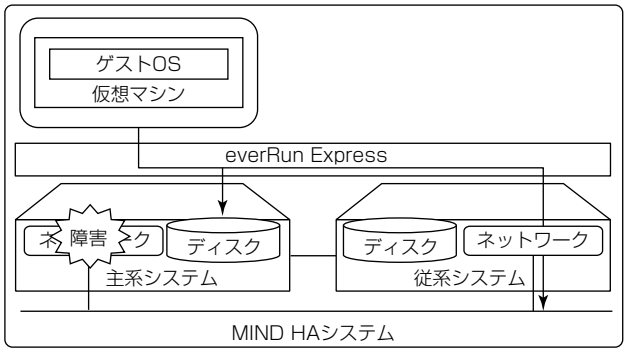
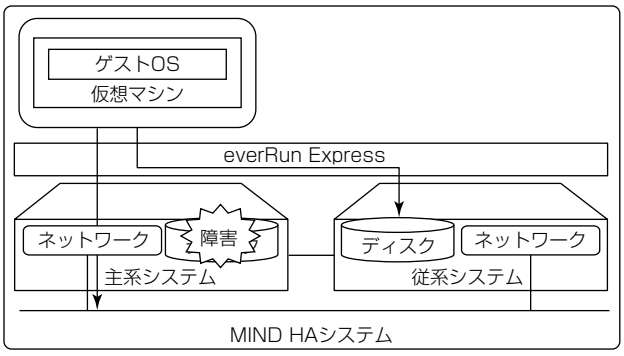



**図２．コスト比較**



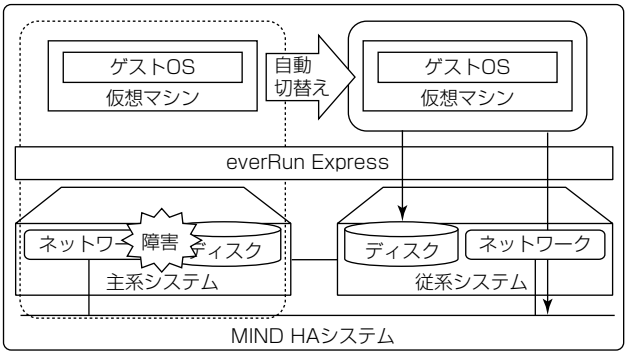

ネットワークで障害が発生した場合，従系システムのネットワークで仮想マシン内のシステムは継続動作

**図３．ネットワーク故障時の切替え動作**




ディスクで障害が発生した場合，従系システムのディスクで仮想マシン内のシステムは継続動作

**図４．ディスク故障時の切替え動作**




サーバ故障(CPU・電源等)が発生した場合，瞬時に従系システムで自動復旧し，仮想マシン内のシステムは継続動作

**図５．電源・CPU故障時の切替え動作**

### 3.3 容易な運用

MINDではMIND HAシステムの標準保守メニューとして，インターネット遠隔通報サービスを提供している。このインターネット遠隔通報サービスではこのシステムと遠隔監視装置を接続し，MIND統合運用管制センターで24時間365日監視する。そのため，このシステムのためのユーザー側での監視体制構築は不要で，容易な運用を実現する。

障害発生時には自動的にMIND統合運用管制センターに通報され，そこからエンジニアがリモートで障害を解析する。リモートでの障害解析によって，現地でのログ採取などを省略することができるので平均復旧時間(Mean Time To Repair：MTTR)の短縮を実現する。この特長によって，**2. 3節**で述べたユーザーでの難しい運用の課題を解決する。

### 3.4 保守窓口の一元化

MIND HAシステムは，2台のサーバとeverRun Expressとの組合せで実現した製品であるが，保守はMINDで一元的に受け付け，システムの復旧まで支援する。これによって，ユーザーやシステムインテグレータは自らの専門領域であるビジネスアプリケーションの構築や運用・保守に注力できる。この特長によって，**2. 4節**で述べた分散した保守窓口の課題を解決する。

## 4. インターネット遠隔通報サービス

MIND HAシステムでは保守メニューとして，インターネット遠隔通報サービスを標準で提供している。インターネット遠隔通報サービスでは，このシステムは遠隔監視装置と接続され，MIND統合運用管制センターで24時間365日監視される(**図6**)。

このシステムのハードウェアで障害が発生したときはMIND統合運用管制センターに自動通報され，そこからエンジニアがリモートで障害を解析し，復旧までの時間を短縮する。

インターネット遠隔通報サービスは，次に述べる2つの機能を持つ。

### 4.1 監視及び通報機能

各サーバと遠隔監視装置を接続し，SNMP(Simple Network Management Protocol)でポーリング監視を行う。監視結果はMIND統合運用管制センターに送信され，監視結果が異常である場合は同センターの担当者に障害を通知する。

### 4.2 リモートアクセス機能

MIND統合運用管制センターの端末から遠隔監視装置を経由して，ユーザーのMIND HAシステムにアクセスできる。このインターネット遠隔通報サービスは，2014年度に開発したftServerの遠隔監視システムを拡張開発することで実現している。

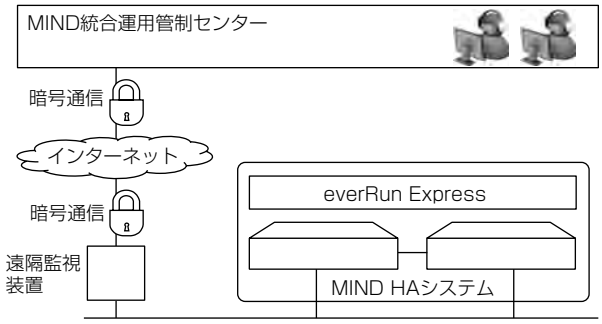



**図6．インターネット遠隔通報サービス**

**表1．監視対象とリモートアクセス先の拡張開発**

| | 監視対象 | リモートアクセス先 |
|---|---|---|
| 今回 | everRun Express，サーバ管理モジュール | everRun Express管理画面(HTTP)，サーバ管理モジュール管理画面(HTTPS)，everRun OS(SSH) |
| 従来 | ftServer 1台 | ftServer(SSH，RDP) |

SSH：Secure SHell，RDP：Remote Desktop Protocol

拡張開発では，監視対象とリモートアクセス先を追加した(**表1**)。監視対象では，2014年度に開発したftServerの遠隔監視システムの監視対象が1台のftServerだけであったが，拡張開発によってeverRun Expressとサーバ内蔵のハードウェア管理・監視を行うサーバ管理モジュールを監視対象にした。一方，リモートアクセス先では，従来ftServerへはSSHやRDPでのアクセスを実施していたが，拡張開発によってeverRun Express管理画面及びサーバ管理モジュール管理画面並びにeverRun OSへアクセスできるようにし，HTTP(HyperText Transfer Protocol)，HTTPS(Hypertext Transfer Protocol over SSL(Secure Sockets Layer)/TLS(Transport Layer Security))及びSSHでのアクセスを実現した。

## 5. むすび

MIND HAシステムの特長と機能について述べた。このシステムによって低コスト・短期間で，保守性も高いHAクラスタシステムの導入が可能である。今後は，より高性能・大容量なサーバを評価済みラインアップに加えることで，高可用ITプラットフォームの更なる拡大を狙う。

## 参考文献

(1) 渡辺和也，ほか：公衆インターネット網を用いた無停止型サーバftServerの遠隔監視システムの開発，三菱電機技報，**89**，No.8，478～482 (2015)
(2) 三菱電機インフォメーションネットワーク㈱：高可用性プロダクツMIND HAシステム
http://www.mind.co.jp/service/idc_platform/platform_products/ha/