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 2015
Vol.89 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. 89 No.8 2015

目　次

表紙：企業・社会の快適・安心・発展を支えるITソリューション

三菱電機は，クラウド技術，情報セキュリティ技術など，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。

表紙の写真は，三菱電機インフォメーションネットワーク㈱(MIND)の統合運用管制センター(Integrated Control Center：ICC)である。統合運用管制センターでは，専門エンジニアが24時間365日，国内・海外の顧客のICTシステムに対する監視・運用サービスを提供し，顧客の負荷を軽減するとともに事業活動の基盤としての高品質なICTサービスを実現する。

巻/頭/言

スマートマシンが拓く新たなソリューション

Future Solutions Created by Smart Machines

工藤　司
Tsukasa Kudo

スマートグラスやスマートウォッチなどの様々なウェアラブル端末が登場し，今後の普及が予想されている。ヘッドマウントディスプレイなどのウェアラブル端末は以前から存在していたものの，普及には至っていなかった。これが一転して大きな関心を集めた背景にはデバイス自体もさることながら，近年，これらの使用環境が大きく変化していることが挙げられる。

第一はスマートマシン（自律的で学習するマシン）としての進化がある。GPS（Global Positioning System）を始めとするセンサの装備や，学習機能の進展などによってユーザーの状況や環境を認識してアシストすることで，ユーザーフレンドリなデバイスになっている。この結果，生活の様々な場面でパートナーとして使用することが可能になってきた。

第二はネットワークへの接続環境である。Bluetooth(注1) LE（Low Energy）などのテザリング機能の普及によって，各種の機器がスマートフォンなどの手持ちのモバイル端末経由で容易にインターネットに接続できるようになった。これは，ウェアラブル端末を常にネットワークに接続して使用できる実際的な環境が整ってきたことを意味している。

そして，第三はソーシャルメディアやビッグデータを始めとするクラウドサービスの普及である。例えば，NoSQL（Not only SQL）データベースによって実世界の多様なデータを保存し，多くのユーザーが活用できるようになった。この結果，簡易な端末でも，インターネットにつながれば様々なサービスを受け，情報を発信できるようになっている。

この動向は，どのようなITソリューションを生み出すのだろうか。1つは人と機械の垣根がなくなっていくことが予想されている。すなわち，IoT（Internet of Things）と呼ばれるように，機械も人も全てのモノがインターネットにつながる世界が始まろうとしている。ここでは，人間だけでなく機械も記事を投稿する。例えば，車の発信する運行情報をビッグデータとして活用すれば，渋滞を回避するための経路をガイドできる。こうなると，ネットワークの向こうの相手が，機械なのか人なのかということは意味を持たなくなってくる。

同様に，バーチャルな世界と実世界の垣根がなくなっていくことが考えられる。例えば，我々の周囲では家電や車を始め，見えない所でコンピュータが稼働している。また，流通分野ではネットで予約したものを実店舗で受領して電子決済するように，消費者が流通経路を意識せずに購入するオムニチャネルが進展している。一方で，ウェアラブル端末でも衣類など外から見えないところに組み込まれた製品が販売され，コンタクトレンズなどに組み込む研究も行われている。すなわち，我々のあらゆる生活の中で意識せずに機械を使用したり，アシストを受けたりする世界が来ることが予想される。

現在，IT革命と呼ばれる時代が続いている。この時代はインターネットを基盤として，世の中に多くの変革をもたらしてきた。これまでの時代を振り返ると，電子商取引，ユビキタス，クラウド，ビッグデータと幾つもの波が次々に押し寄せてきた時代であると見ることができる。すなわち，技術が市場を創り，その市場が新たな技術の創造を促すサイクルを構成してきたと言える。こうして，米国を中心に独創的な企業が誕生してきた。

ここで，IT革命以前の時代に戻って考えると，SFとして語られてきたことの多くが，当たり前のように我々の周囲に存在し，又は手の届くところにやってきている。もちろん，影の部分がありセキュリティやプライバシーなどの問題もまた存在する。しかし，大きな情報産業の市場を生み，我々が想像すらしていなかった快適で便利な生活をもたらしてきたことも事実である。

日本では少子高齢化や地方の衰退などに見られるような困難な社会的課題を抱えているが，新たな技術の波を捉えて，これらの課題を解決する革新的なソリューションを構想する力，これが今日の日本に最も必要なものではないだろうか。

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

◆静岡理工科大学 総合情報学部 人間情報デザイン学科 教授
Professor, Department of Human-Computer Interface Design, Faculty of Comprehensive Informatics, Shizuoka Institute of Science and Technology

特集論文

三菱電機スマート制御クラウドサービス“DIAPLANET”

伊藤正裕* 河村美嗣***
原田雅史* 児玉 拓***
田村孝之**

"DIAPLANET"：Mitsubishi Electric Cloud Services for IoT/M2M Systems

Masahiro Ito, Masafumi Harada, Takayuki Tamura, Yoshitsugu Kawamura, Taku Kodama

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”の販売を2015年4月から開始した。このサービスの特長は，次のとおりである。

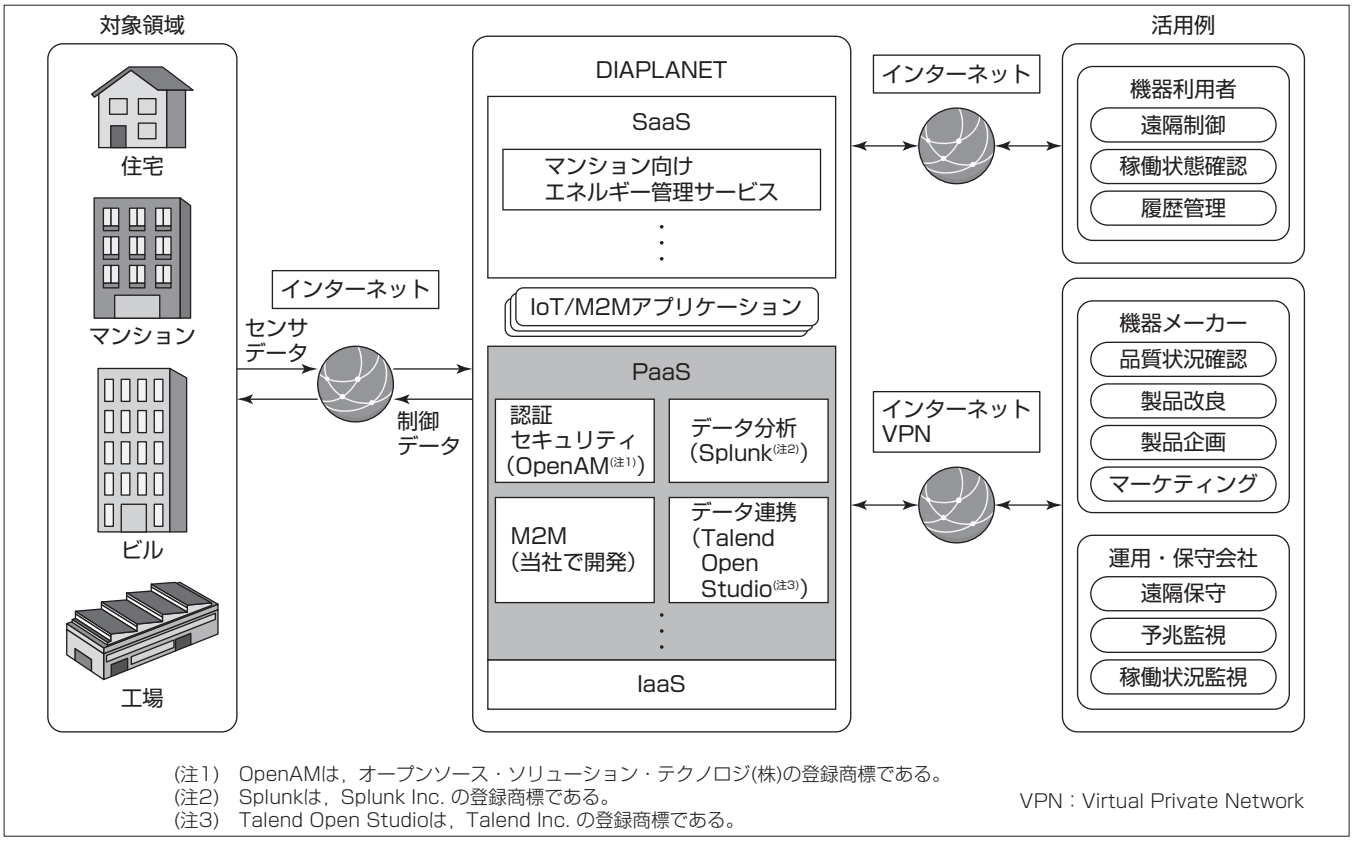
(1) 豊富なPaaS(Platform as a Service)機能によって，IoT/M2Mシステムを効率的に構築できる。

(2) トライアル支援サービスによって，少ない費用で対象システムの事前検証を行うことができる。

(3) 安心・安全なクラウド基盤を提供できる。

DIAPLANETは，要旨の図に示すように，IaaS(Infrastructure as a Service)，PaaS，SaaS(Software as a Service)の3つの層で構成している。利用者は，PaaS層で提供する各サーバ機能を使用して，短期間でIoT/M2Mシステムを構築することができる。PaaS層の中核となるM2Mサーバ機能は，機器からのセンサデータを蓄積する機能と機器を制御するためのデータ通信機能を提供する。接続する機器が増加した場合もスケールアウト方式で対応可能である。

また，利用者は，今後充実化していくSaaS層で提供するサービスを利用することで，サービスインまでの時間をさらに短縮することができる。



(注1) OpenAMは，オープンソース・ソリューション・テクノロジ(株)の登録商標である。
(注2) Splunkは，Splunk Inc. の登録商標である。
(注3) Talend Open Studioは，Talend Inc. の登録商標である。

VPN：Virtual Private Network

DIAPLANETを使用したIoT/M2Mシステムの全体構成

DIAPLANETは，インターネットを介して住宅，マンション，ビル，工場などの家電や機器からのデータを受信して蓄積するとともに，制御コマンドを送信してそれらを制御する機能を提供する。一方，各利用者がスマートフォンなどを用い，DIAPLANET上のPaaS層で提供する機能を使用して，エネルギー管理，蓄積されたデータの分析，機器類の遠隔制御・保守，予兆監視などを行うアプリケーションを開発することができる。

*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)) ***同研究所

1. まえがき

近年，クラウドコンピューティング（計算機（ハードウェア，ソフトウェア）を所有せず，それらをサービスとしてオンデマンドで利用する）の普及が進んでいる。一方，計算機技術の進展に伴い，企業活動を支えてきた従来の企業情報システムとは異なった，大量の機器やセンサなどからの膨大なデータを処理し，それらの機器を最適制御するような新しいパラダイムの情報システム構築が可能になり，IoT/M2Mシステム構築は成長市場になりつつある。爆発的に増加する等，変動が大きいデータを広範囲にわたって定常的に蓄積・処理する必要があるため，IoT/M2Mシステムは，計算機リソースの増減に柔軟に対応できるクラウド上に構築されるのが一般的である。このような背景から，当社では豊富なPaaS機能を備えたIoT/M2Mシステム構築支援環境と安心・安全な運用環境をリーズナブルな価格で利用できるスマート制御クラウドサービスDIAPLANETを開発し，2015年4月から販売を開始した。

本稿では，DIAPLANETを構成する3つの層のうち，基盤となるIaaS層と中核となるPaaS層，特に，IoT/M2Mシステムを構築する際のキーとなるM2Mサーバについて機能と特長を述べるとともに，クラウド管理方式とセキュリティの実現方式について述べる。

2. DIAPLANETの概要

DIAPLANETは，不特定多数のユーザーが利用するパブリッククラウドに位置付けられ，PaaS層及びSaaS層を提供するサービスモデルである。DIAPLANETの中核はPaaS層であり，IoT/M2Mシステムを効率的に構築するために必要となるミドルウェアを仮想サーバとして提供している。

SaaS層では，IoT/M2Mシステムをサービスとして提供するが，当面のターゲットは，MEMS（Mansion Energy Management System）に代表される各エネルギー管理システムである。

基盤となるIaaS層は，物理サーバ，物理ストレージ，物理ネットワークから構成される。物理サーバ上には仮想化基盤ソフトウェアがインストールされており仮想サーバを作成することができ，高可用性も実現している。

3. IaaS層の機能と特長

DIAPLANETのIaaS層の構成を**図1**に示す。IaaS層は，利用者に仮想サーバを提供する複数の計算ノード，クラウド全体を管理する管理ノード及び計算ノードにディスクを提供するストレージノードで構成している。計算ノードでは，仮想サーバは仮想ルータによって内部ネットワークと外部ネットワークを分離しており，仮想サーバ間はVLAN（Virtual Local Area Network）によって隔離している。ストレージノードは，仮想サーバに対して仮想ディスクを提供するプライマリストレージとスナップショット，インストールイメージなどを格納しておくセカンダリストレージで構成している。

3.1 仮想化基盤の導入

DIAPLANETではパソコンサーバ上に仮想化基盤としてCitrix社のXenServer(注4)を導入し，その上に複数の仮想サーバを生成する方式を採用している。それによって，パソコンサーバのリソースが有効活用できる。仮想サーバにインストールされるOS（Operating System）はCentOS(注5) 6，Red Hat Enterprise Linux(注6)6及びWindows(注7) Server 2012から選択する。これら以外は個別対応になる。

（注4） XenServerは，Citrix Systems，Inc. の登録商標である。
（注5） CentOSは，CentOS Ltd. の登録商標である。
（注6） Red Hat Enterprise Linux(注8)は，Red Hat，Inc. の登録商標である。
（注7） Windowsは，Microsoft Corp. の登録商標である。
（注8） Linuxは，Linus Torvalds氏の登録商標である。

3.2 高可用性の実現

DIAPLANETでは，仮想化基盤が提供する機能を利用することで，最小限のダウンタイム（数秒から十数秒程度）での高可用性を実現している。XenServerが提供するXenHA（High Availability）の構成例を**図2**に示す。ハートビート用に独立した媒体（LAN（Local Area Network）とストレージ）を使用することで，サービスの二重起動などのスプリットブレイン現象の発生を低減させる特長がある。また，障害の程度に応じて同じパソコンサーバ上や別のパソコンサーバ上で再起動できる。

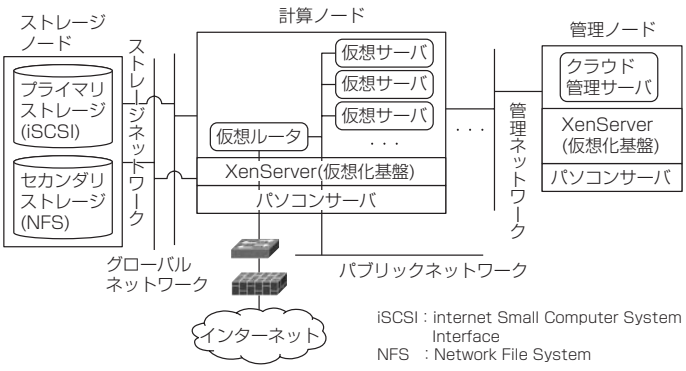


図1．DIAPLANETでのIaaS層の構成

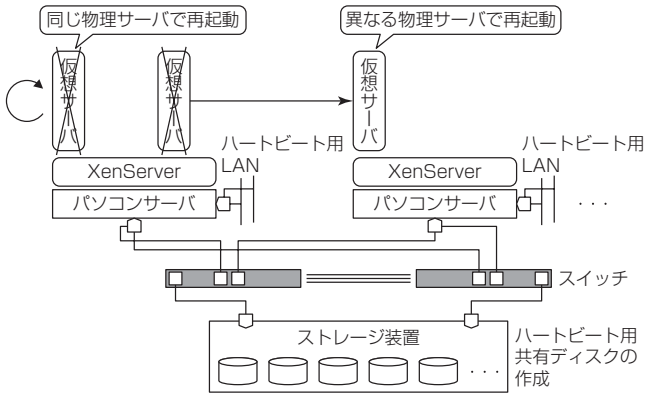


図2．高可用性を実現する構成

4. PaaS層の機能と特長

PaaS層では，システムを構築する際にクラウド管理ソフトウェア(**5. 1節**)を用いる。クラウド管理ソフトウェアによって，OSや必要なミドルウェアがインストールされた仮想サーバを画面から簡単に選択できる。ユーザーは，この仮想サーバ上にアプリケーションを構築していく。PaaS層の構成例を**図 3** に示す。

PaaS層で提供する仮想サーバは，一般的なミドルウェアが搭載された仮想サーバ(**4. 1節**)とIoT/M2Mシステム対応で当社で開発したM2Mサーバ(**4. 2節**)で構成している。さらに，PaaS層のOSには，あらかじめ監視用エージェントをインストールしているとともに管理者や運用者向けアカウントの作成，不要サービスの停止，ファイアウォールやリモートログインの設定など，セキュリティポリシーに準拠した対処を実施済みである。

4. 1 一般仮想サーバ

システム構築を行う際に，使用される頻度が高いミドルウェアは，OSS(Open Source Software)製品中心にデファクトスタンダードとして認知され日本国内での使用実績が高いものの中から次の製品を選定した。今後，このレパートリーを増やしていく予定である。

- 統合監視サーバ(Zabbix(注9))
- 統合認証・認可サーバ (OpenAM，OpenDJ(注10))
- Web/APサーバ(Apache Http Server(注11)／Apache Tomcat(注11))
- NoSQLデータベース(Apache Cassandra(注11))
- リレーショナル データベース(PowerGres(注12))
- データ分析サーバ(“AnalyticMart”)
- データ分析・可視化サーバ(Splunk)
- データ連係サーバ (Talend Open Studio)など

(注9) Zabbixは，Zabbix SIA社の登録商標である。
(注10) OpenDJは，オープンソース・ソリューション・テクノロジ㈱の登録商標である。
(注11) Apache Http Server，Apache Tomcat及びApache Cassandraは，Apache Software Foundationの登録商標である。
(注12) PowerGresは，SRA OSS，Inc. の登録商標である。

4. 2 M2M仮想サーバ

IoT/M2Mアプリケーションには，接続機器数の増加に応じ，多数の機器からのデータ収集や多数の機器に対する制御を柔軟に処理することが求められる。IoT/M2MアプリケーションのためのアーキテクチャやインタフェースはoneM2M等による標準化が進められているものの実装が確立していないのが現状である。

DIAPLANETでは上記の課題を解決するために，IoT/M2Mアプリケーションに対して次の2つの機能をM2M仮想サーバ及びAPI(Application Programming Interface)ライブラリとして提供している。

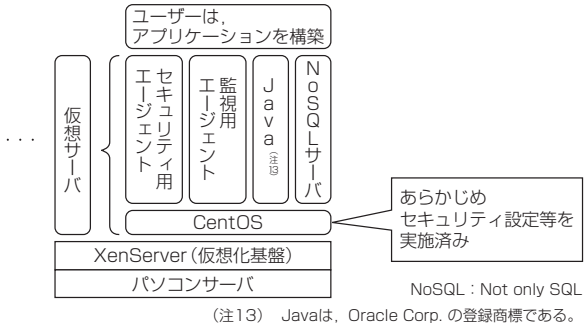
(1) 多数の機器からデータを収集しDIAPLANET上のNoSQLデータベースに格納するデータ蓄積機能
(2) DIAPLANET上のWeb/APサーバから多数の機器を遠隔制御する制御通信機能

M2M仮想サーバを用いたIoT/M2Mシステムの構成を**図 4** に示す。現行では，Web/APサーバとGW(Gateway)向けにAPIライブラリを提供しており，各機器は，GWのミドルウェアであるOSGi(注14)上で動作するGWのアプリケーションを介してM2M仮想サーバと通信する。今後は，各機器がGWを介さずに直接M2M仮想サーバと通信する方式に対応する。

(注14) OSGiは，米国OSGi Allianceの登録商標である。

4. 2. 1 データ蓄積機能

データ蓄積機能は，機器から受け取ったデータをスケールアウトに対応したNoSQLデータベースであるCassandraに格納することで，機器台数の増加に対応する。



(注13) Javaは，Oracle Corp. の登録商標である。

図 3．DIAPLANETでのPaaS層の構成

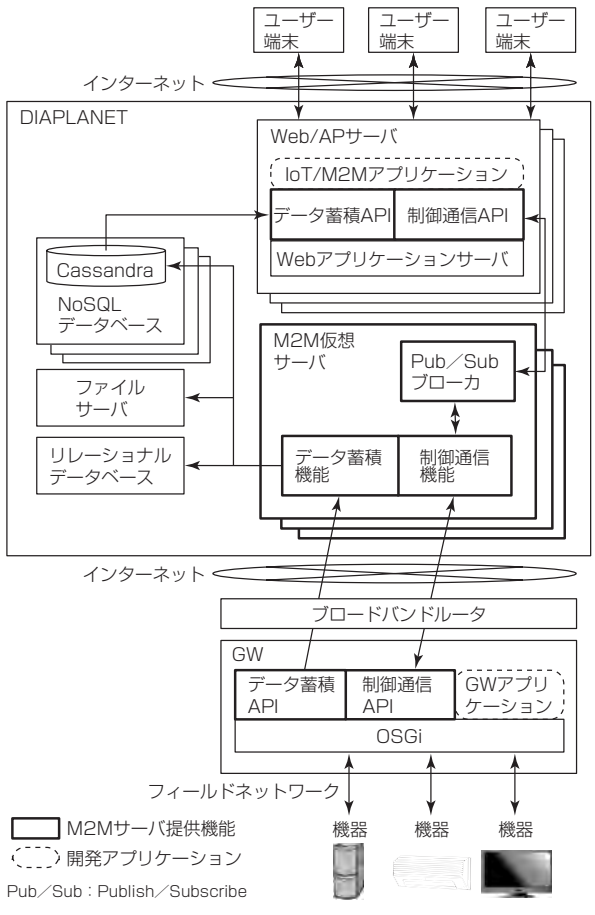


図 4．M2M仮想サーバを利用したシステム構成

機器データを蓄積するためのデータベーススキーマは汎用的な形式(機器ID(IDentifier)，時刻，データ形式，及び生データ)を用意し，様々な機器データに対応できるようにした。機器固有のデータ形式を格納した場合，読み出し時に生データの解析を行う。

また，データの保存先としてリレーショナルデータベースやファイルサーバを追加指定することも可能であり，一般ミドルウェアとも容易に連携できる。

4.2.2 制御通信機能

住宅・ビル・工場などの環境では，機器に対するインターネット側を起点とする通信は，ブロードバンドルータ等によって遮断される場合があるため，遠隔制御指令の送受信方法が課題である。そこで，制御通信機能では，機器側から通信を開始する通信方式によって，インターネット側から遠隔制御通信を行う手段を提供する。

機器側から通信を開始する通信方式にはポーリング方式やロングポーリング方式，WebSocket方式などが存在するが，IoT/M2Mアプリケーションが個々のプロトコルに依存する設計を行うとプログラムの煩雑化を招き保守性が損なわれる。APIライブラリによって個々のプロトコルの詳細を隠蔽することでアプリケーションと通信方式の分離を図った。

一方，機器側から通信を開始することで，M2M仮想サーバをスケールアウトさせた場合に，機器が接続するM2M仮想サーバが一意に定まらなくなるという課題が生じる。そのため，遠隔制御指令を発行するWeb/APサーバとM2M仮想サーバの間はPublish／Subscribe方式で連携し，機器IDに基づいて指令を配信するようにしている。

5. クラウド管理方式とセキュリティ

5.1 クラウド管理の容易性

DIAPLANETでは，仮想サーバを管理するクラウド管理ソフトウェアとしてCitrix社のCloud Platform(注15)を採用している。このソフトウェアは，OSSのApache Cloud Stack(注16)をベースにしており，海外を始め複数の国内クラウドサービスベンダーに採用されている。このソフトウェアでは，複数の仮想化基盤をサポートしているが，先に述べたとおりDIAPLANETでは親和性を考慮し仮想化基盤にはCitrix社のXenServerを採用した。

CloudPlatformでは仮想サーバの作成，変更，削除などの管理作業はWebブラウザを用いて直感的に行うことができる。管理画面の一例を**図5**に示す。

(注15) Cloud Platformは，Citrix Systems，Inc. の登録商標である。
(注16) Apache CloudStackは，Apache Software Foundationの登録商標である。

5.2 高いセキュリティの実現

安心・安全なクラウド環境を実現するために次の取組みを行っている。

(1) 総務省による“ASP(Application Service Provider)・SaaSにおける情報セキュリティ対策ガイドライン”に準拠し，さらにデータセンターを運営している当社のセキュリティ基準を加えることで，高いセキュリティ管理レベルを実現した。

図5．CloudPlatformの管理画面の一例

(2) 物理セキュリティ対策としては，次の2つを実現した。
①当社が運営しているデータセンター内に配備して，運用管理を実施
②システム管理者のメンテナンス操作は，管理者接続用VPN経由でのみに制限して不正侵入のリスクを低減

(3) 情報セキュリティ対策としては，次の3つを実施した。
①ウイルス及び脆弱(ぜいじゃく)性対策などの総合的セキュリティとしてTrend Micro Deep Security(注17)を導入し，すべての仮想サーバの安全性を確保
②あらかじめセキュリティ設定をした仮想サーバを提供することで設定漏れリスクを低減
③定期的なセキュリティ診断の実施

(注17) Trend Micro Deep Securityは，トレンドマイクロ㈱の登録商標である。

6. む す び

DIAPLANETが提供するPaaS層やSaaS層を使用することでIoT/M2Mシステムの早期立ち上げや安全な運用を行うことができる。現在，次の強化開発を実施しており，より高度なサービスを順次提供していく。

(1) 機器との接続性の強化(当社製機器との接続保証，WebSocketやMQTT(Message Queuing Telemetry Transport)など代表的な通信プロトコルのサポートなど)

(2) IaaC(Infrastructure as a Code)技術を使用したシステム運用を行うことで，仮想サーバ提供までのリードタイムの短縮や仮想サーバ構成の自由度向上の実現

(3) IoT/M2Mシステムのサービスインを大幅に短縮するSaaS層の充実

参 考 文 献

(1) 西村達夫，ほか：未来の小規模コミュニティ向けIT基盤，三菱電機技報，**89**，No. 7，411～414（2015）
(2) 児玉　拓：クラウドを利用したサービス事業者向け見守りシステム，三菱電機技報，**88**，No. 8，442～445（2014）

特集論文

三菱電機スマート制御クラウドサービス“DIAPLANET” MEMS

塩井川幸保*
鷲尾元太郎**
田村孝之***

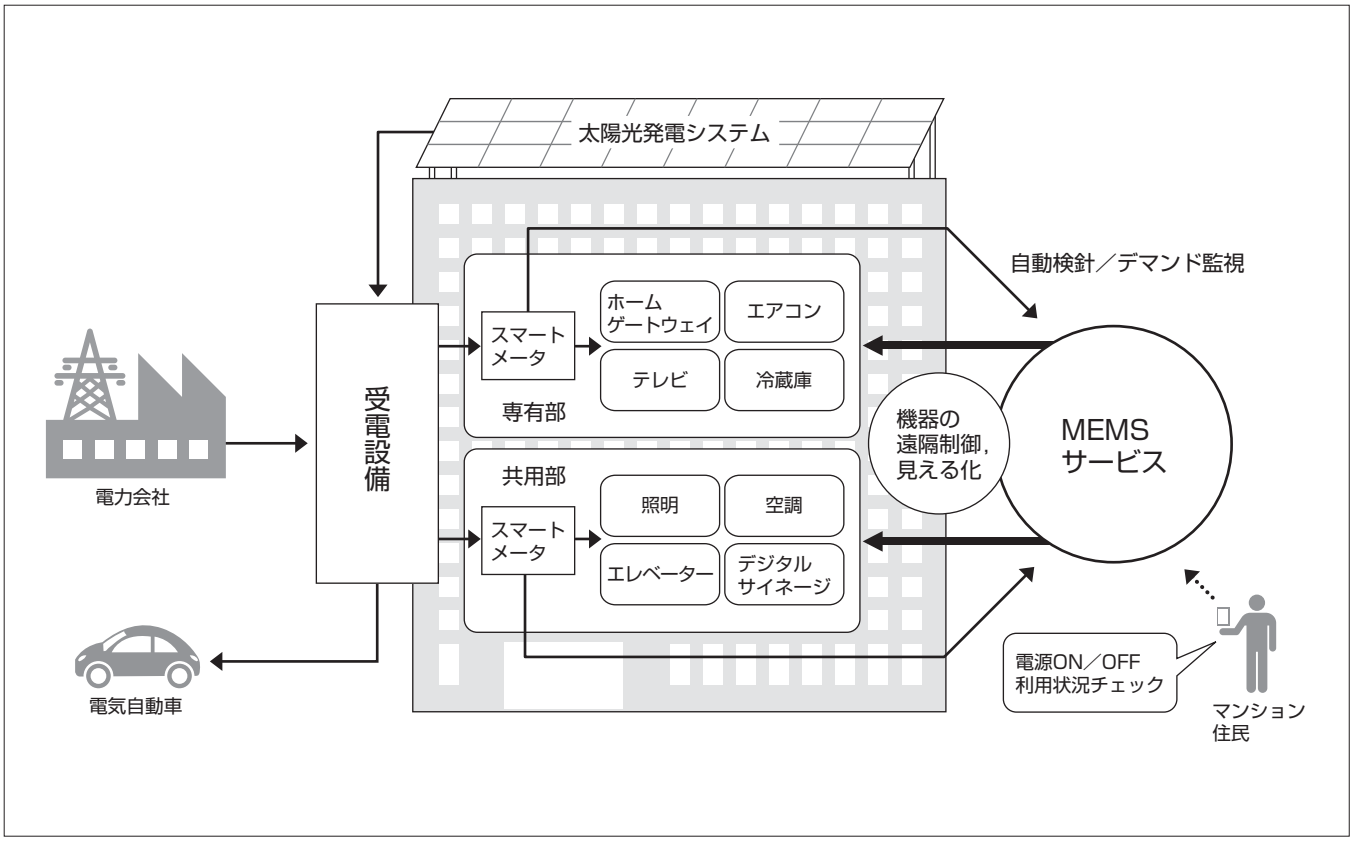
"DIAPLANET" MEMS：Mitsubishi Electric Cloud Services for Mansion Energy Management Systems

Yukiyasu Shioigawa, Gentaro Washio, Takayuki Tamura

要　旨

昨今のエネルギー市場では，原子力発電の再稼働が不透明な中，エネルギーを無駄なく，賢く利用するエネルギー管理への関心が高まってきている。MEMS（Mansion Energy Management System）は，経済産業省主導のスマートマンション導入加速化推進事業によって普及が促進され，アグリゲータ主導でMEMSの導入が進んでいる。MEMSとは，マンション建物内の電力使用量を計測して蓄積し，マンション内や外部からの電力使用量を“見える化”する。さらに照明や空調の遠隔制御や，全体の電力消費の“ピーク抑制”をする等の機能を持つ。

三菱電機のMEMSは，複数の家電製品や産業用機器の遠隔制御，稼働モニタリング，エネルギー管理などをワンストップでシステム構築する三菱電機スマート制御クラウドサービス“DIAPLANET”上で実現している。これによって，スマートマンションとしての付加価値を向上させ，高いセキュリティと信頼性を持つサービスをトータルで提供する。MEMSはスマートコミュニティソリューションの１つであり，今後はHEMS（Home EMS），BEMS（Building EMS）など他のEMS（Energy Management System）ソリューションと組み合わせることによって最適なエネルギーソリューションを提供し，安心・安全なスマートコミュニティ向けサービスに発展させていく。



マンションエネルギーマネジメントシステムの概念図 (1)

当社が提供するマンションエネルギーマネジメントシステム（MEMS）の概念図である。スマートメータから電力使用量を収集して様々なデバイスで見える化を行う。また専有部，共有部に設置された機器の遠隔制御が可能である。

*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　***同研究所（博士（工学））

1. まえがき

原子力発電の再稼働が不透明な中，電気エネルギーの管理が注目されており，各需要家へのエネルギーの安定供給を目的としたEMSの導入が進んでいる。当社では，スマートコミュニティソリューション事業として，タウンEMSなどのマイクログリッドモデルへの応用・転用を進めている。この中で高圧一括受電事業者，マンションデベロッパーに対しクラウドサービスをコアとした集合住宅向けのEMSサービスの提供を行っている。

本稿では，三菱電機スマート制御クラウドサービスDIAPLANET（**図1**）でSaaS（Software as a Service）として提供するMEMS（**図2**）について述べる。

2. MEMSの導入効果

2.1 設備投資の負担軽減

MEMSの利用によって，マンションデベロッパーは導入時の受電設備などマンションの設備投資に関するコストを削減することができる。

またMEMSはクラウドサービスであり，高圧一括受電事業者が従来必要としたサーバの設備投資，管理も不要となる。

2.2 高圧一括受電事業者の検針業務効率化

スマートメータでの自動検針によって，手動検針の場合に要していた人件費の削減と検針ミス撲滅による品質向上を図ることができる。また検針員が立ち入らないため，保安性も向上する。

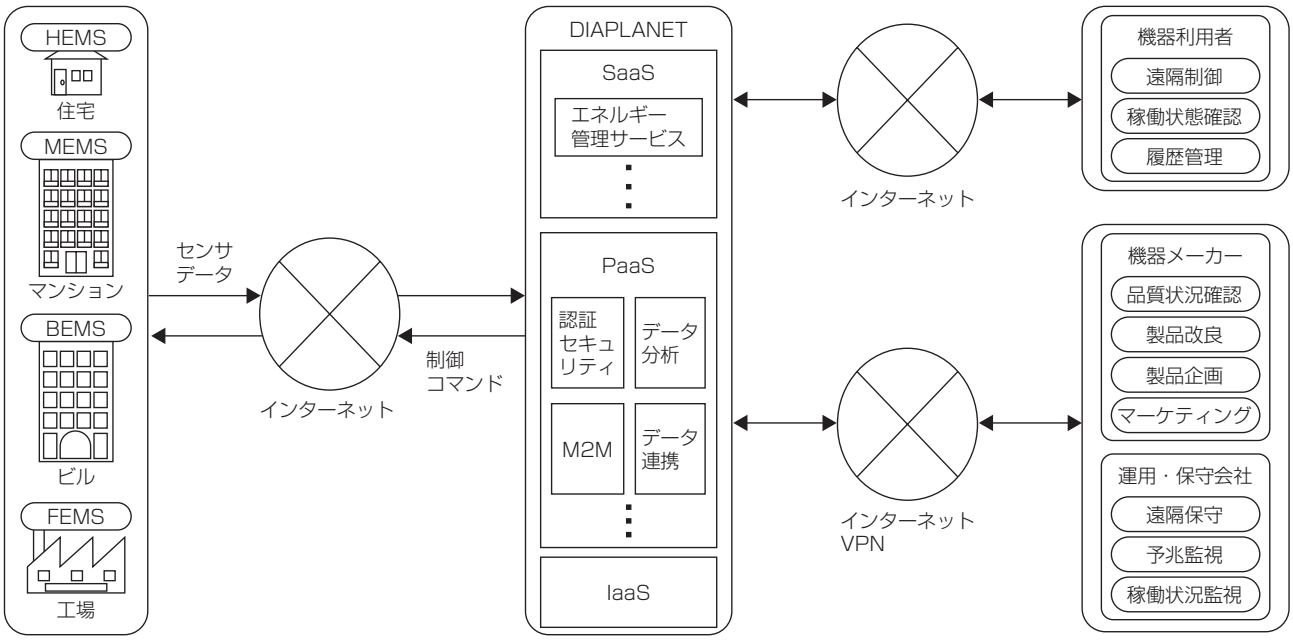


図1．DIAPLANETを使用したIoT（Internet of Things）/M2M（Machine to Machine）システムの全体構成[2]

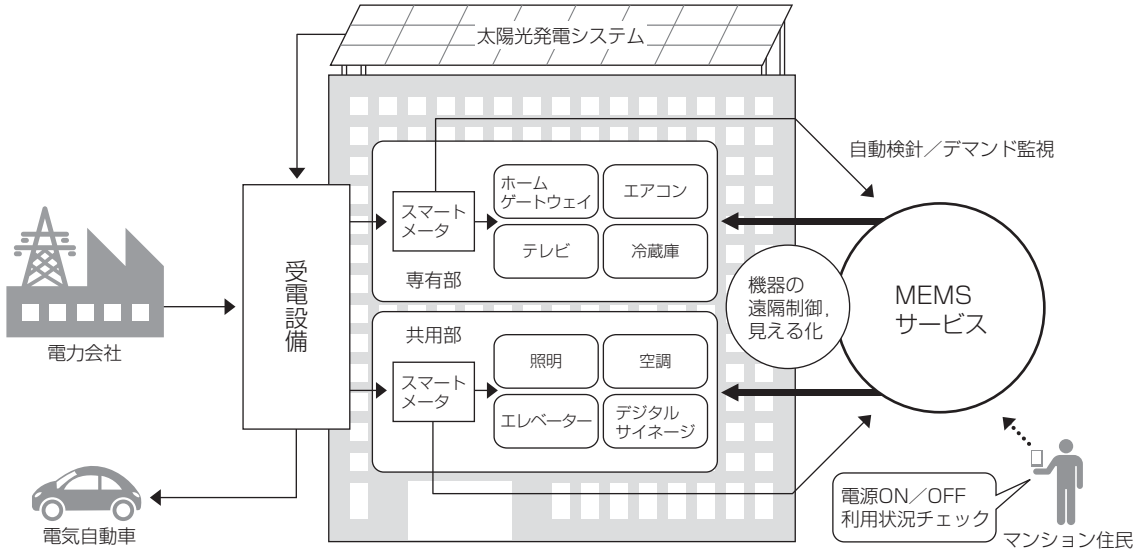


図2．MEMSの概念図[1]

2.3 デマンドピークの管理

マンション全体の電力使用量がピーク時に契約電力を超えることによって追加費用支払いのリスクが生じる。デマンド制御によってマンションの専有部，共用部の電力消費を抑制し，ピークカット・ピークシフトなどを実現することが可能となる。

2.4 資産価値の向上

MEMSの導入によって，マンションデベロッパーは低コスト・高利便性・高付加価値マンションの提案ができるようになる。また，経済産業省の“スマートマンション評価制度”の認定取得も可能である。**図3**にMEMSのステークホルダとその関連を示す。

3. MEMSのシステム構成と提供機能

3.1 システム構成

MEMSのシステム構成を**図4**に示す。マンションは専有部(各戸)と共用部からなり，それぞれに電力使用量見える化のための計測機器や，節電時の制御対象となる家電機器，空調・照明機器がある。MEMSでは，これらの多様な機器のデータ管理や制御を実現するため，機器固有のデータ形式の解析や制御コマンドの発行が必要になる。

専有部，共用部にはそれぞれゲートウェイ装置(以下“GW装置”という。)を設置し，クラウドサーバへの電力計測値送信と，クラウドサーバからの遠隔制御指示受付を行う。クラウドサーバは，GW装置からのHTTPS(Hypertext Transfer Protocol Secure)接続を受け付け，受信したデータのKVS(Key-Value Store：書き込み性能を重視したデータベース)への格納と，KVSのデータを基に見える化のために集計した結果をRDB(Relational Data Base) へ格納する。

見える化サービスは，インターネットを介してスマートフォンなどのユーザー端末からアクセスされるほか，専有部に設置されたWebブラウザ搭載型インタホンからもアクセスできる。

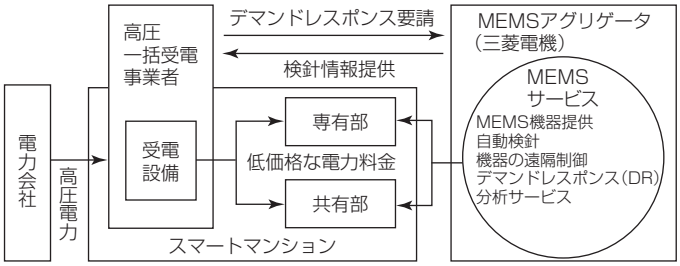


図3．MEMSのステークホルダとその関連[1]

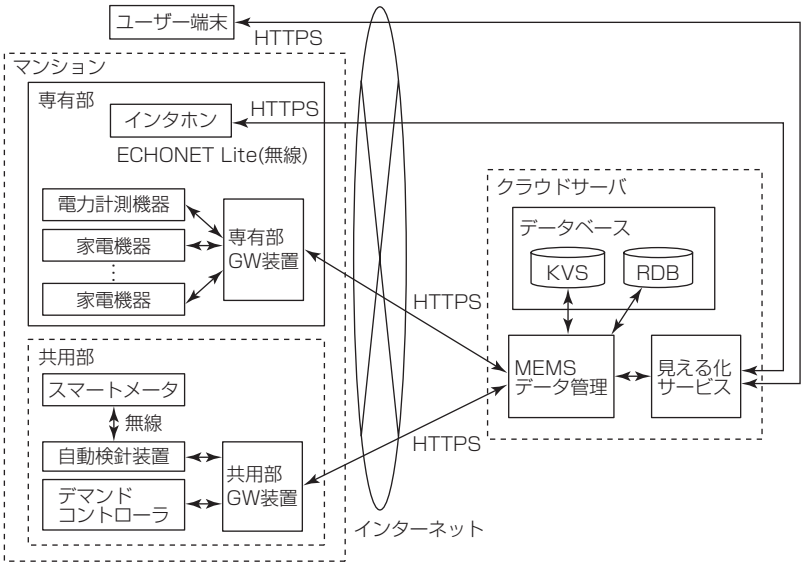


図4．MEMSのシステム構成

3.2 提供機能

3.2.1 ユーザー種別

マンションの専有部と共用部では見える化サービスの機能が異なることから，一般のエンドユーザー(マンション居住者)とマンション管理者の区別を設ける。さらに，高圧一括受電事業者と契約して安価な電力を購入するケースでは，高圧一括受電事業者に対しても業務支援機能を提供するため，一般のエンドユーザー，マンション管理者，高圧一括受電事業者の3種類のロール(役割)が必要になる。各ロールに対応した機能を提供することに加え，データへのアクセス権や機器に対する制御権の管理を行っている。次に，各ロールに対する提供機能を述べる。

3.2.2 エンドユーザー向け機能

エンドユーザーに対しては，専有部の電力使用量をグラフ表示するとともに，節電への動機付けとして，戸宅別電力使用量の前月と今月の比率を基に，マンション内での節電ランキングを表示する機能を提供する。また，高圧一括受電事業者からの節電要請や，マンション管理者からの通知メッセージを表示する。これによって，エンドユーザーとマンション管理者の情報共有を支援する。

さらに，ECHONET Lite(注1)標準に準拠した宅内の家電機器は，個別の電力使用量の一覧表示と，それらの機器を外部から電源操作する機能も提供している。**図5**にエンドユー

図5．エンドユーザー向けの見える化画面(イメージ図)

図6．高圧一括受電事業者向けの業務画面(イメージ図)

ザー向けの見える化画面(イメージ図)を示す。

(注1)　ECHONET Liteは，エコーネットコンソーシアムの登録商標である。

3.2.3　マンション管理者向け機能

マンション管理者に対しては，共用部の空調・照明機器を対象とした電力使用量の表示や制御を行う機能を提供する。

さらに，DRに対応するため，共用部の機器の電源を一定期間自動遮断する機能も提供する。

3.2.4　高圧一括受電事業者向け機能

高圧一括受電事業者に対しては，事業者が契約するマンション全体の電力使用量を表示し，必要に応じてDRの節電要請メッセージを各マンションあてに発行する機能を提供する。節電要請は地域や電力会社単位で発行することが多いため，マンションの属性に基づいて発行先を検索し，一括処理するようにしている。また，節電要請は未来の指定期間に対して発行するため，現在のDRの状態と今後の予定を閲覧することもできる。

さらに，高圧一括受電事業者はマンションのスマートメータの設置・管理を行うため，検針時のデータ取得結果に関するイベントログ情報の監視や，スマートメータ機器交換等の保守作業に必要な管理情報の閲覧・編集機能も提供している。**図6**に高圧一括受電事業者向けの業務画面(イメージ図)を示す。

4.　今後の展開

4.1　柔軟なシステム構成の実現

専有部では，拡充が想定されるECHONET Lite標準に準拠した機器との接続を可能とするために，複数種類の装置の接続をGW装置で行い，ユーザーのニーズに柔軟に対応することを目指していく。

さらに，共用部では，当社製品だけでなく他社製品をも含むシステム構成を可能とする予定である。

4.2　スマートマンションとしての付加価値向上

MEMSでユーザーがコストメリットを実感しにくいという課題があり，電力使用量の見える化・家電機器の制御に加え，新たな付加価値の創出が必要となっている。

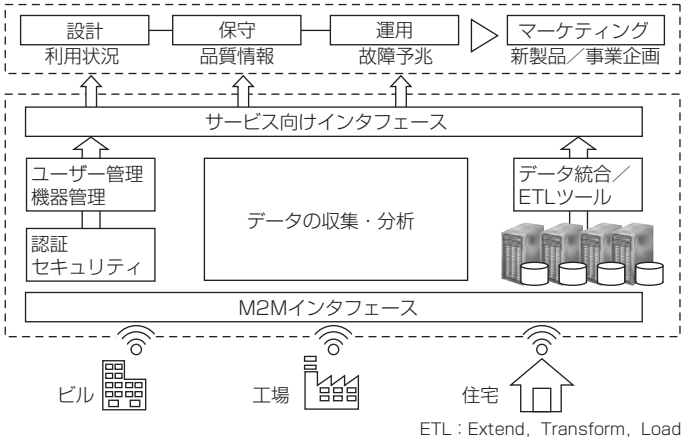


図7．DIAPLANETの将来活用イメージ[4]

今後は，生活情報ポータルとして次のようなサービスコンテンツを提供し，総合的なマンションの付加価値向上を図っていく。

コンテンツの提供媒体としては，パソコン，スマートフォンのほかテレビ，デジタルサイネージも活用する予定である。

(1)　行動検出・通知サービス[3]

電力使用量に基づき行動を検出・通知するサービスを検討中である。このサービスは次の①，②の判定方法による行動検出アルゴリズムを用いて実現する予定である。将来的には，居住者の見守りサービスとしての応用を予定している。

①過去指定日数の平均電力使用量の変化による判定

②電力変動分析による判定

(2)　コミュニケーションサービス

お知らせ，回覧板，アンケートなどの掲示による住民間，住民・マンション管理者間のコミュニケーションサービスを提供する。

(3)　生活情報提供サービス

地域のイベントなどの情報提供を行うことで，地域コミュニティの活性化を促進する。また，共用施設の予約，閲覧サービスを提供し，電子錠による施設管理を行う。

(4)　デジタルサイネージを活用した情報提供サービス

マンション及び地域のエネルギー情報，天気，交通・災害情報など住民の安心・安全な暮らしを支援する情報を提供する。

4.3　ビッグデータ活用サービス

機器から収集する電力使用量，稼働情報などのビッグデータを活用して，次のサービスを将来的に提供していく。

これらのサービスは，DIAPLANETのビッグデータ分析機能を強化することで実現する。**図7**にDIAPLANETの将来活用イメージを示す。

(1)　エンドユーザー向けサービスとして，収集した詳細な電力使用量を基に，節電アドバイスを行う。電力自由化

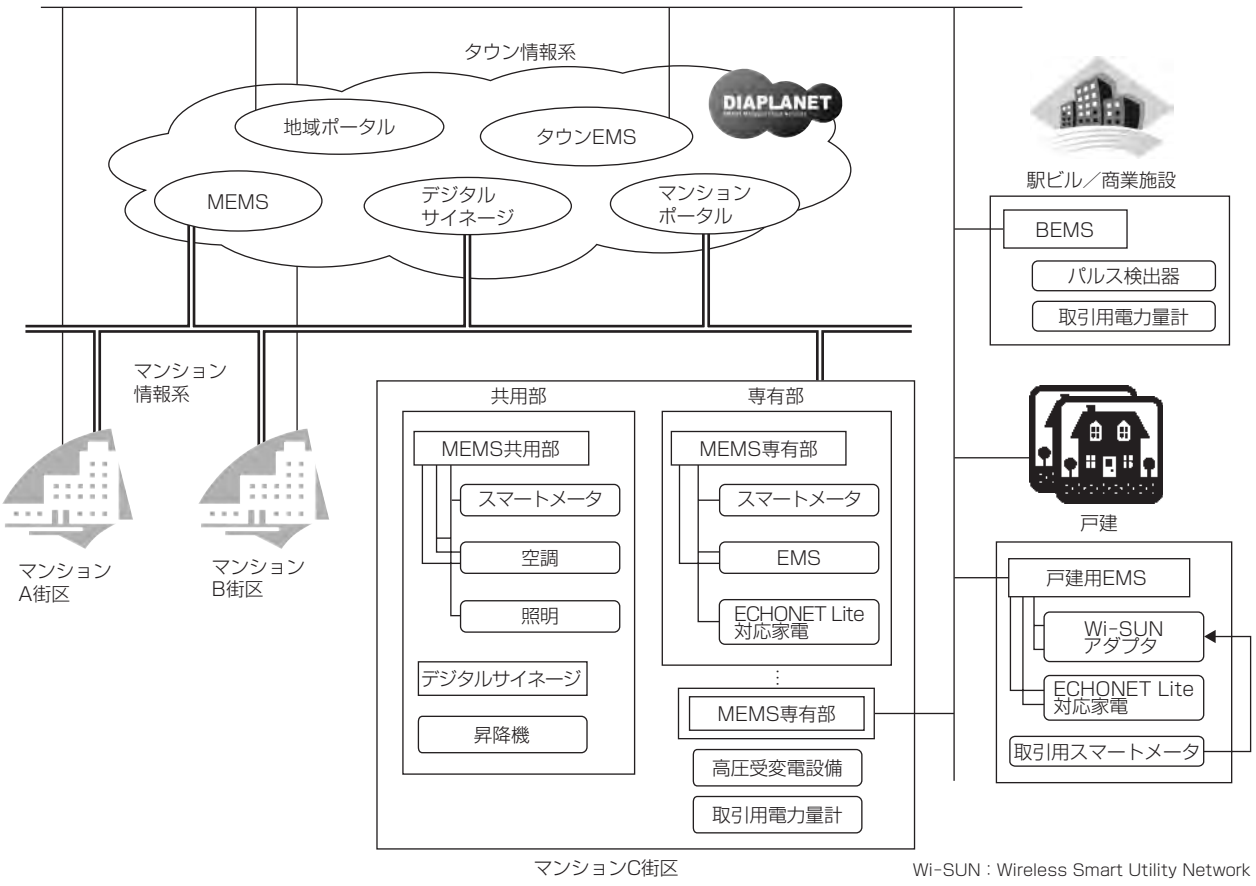


図8．小規模スマートコミュニティ向けサービスの将来イメージ[4]

を見据えた最適な料金体系ナビゲーションなどを提供する。

(2) 高圧一括受電事業者に対して，機器，設備の稼働監視を行い稼働状況レポート，故障予兆レポートを作成し，遠隔拠点からの効率的な設備管理サービスを提供する。

5. むすび

MEMSの概要及び取組みについて述べた。MEMSはスマートコミュニティソリューションの1つであり，今後は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最適なエネルギーソリューションを提供していく。各EMSソリューションはDIAPLANETのSaaSとして実現し，DIAPLANET上で統合して提供することで小規模スマートコミュニティ向けサービス(**図8**)へと発展させていく。

参考文献

(1) 三菱電機ホームページ：三菱電機スマート制御クラウドサービスDIAPLANET
http://www.mitsubishielectric.co.jp/business/itsolution/ondemand/diaplanet/index.html

(2) 三菱電機ニュースリリース IS No.1501：三菱電機スマート制御クラウドサービス「DIAPLANET」発売のお知らせ
http://www.mitsubishielectric.co.jp/news/2015/0129-b.html

(3) 児玉　拓：クラウドを利用したサービス事業者向け見守りシステム，三菱電機技報，**88**，No. 8，442～446（2014）

(4) 西村達夫，ほか：未来の小規模コミュニティ向けIT基盤，三菱電機技報，**89**，No. 7，411～414（2015）

特集論文

クラウドを利用した大規模動画配信システム

菊池正人* 細田洋佑*
岡村 基* 小池重男**
池原 勉*

Large-scale Movie Streaming System Based on Cloud Service

Masato Kikuchi, Motoi Okamura, Tsutomu Ikehara, Yousuke Hosoda, Shigeo Koike

要 旨

三菱電機インフォメーションシステムズ㈱(MDIS)では，大規模動画配信システムを，アマゾンのクラウド(Amazon Web Service：AWS)を利用することで低コスト，かつ短期間で構築した。

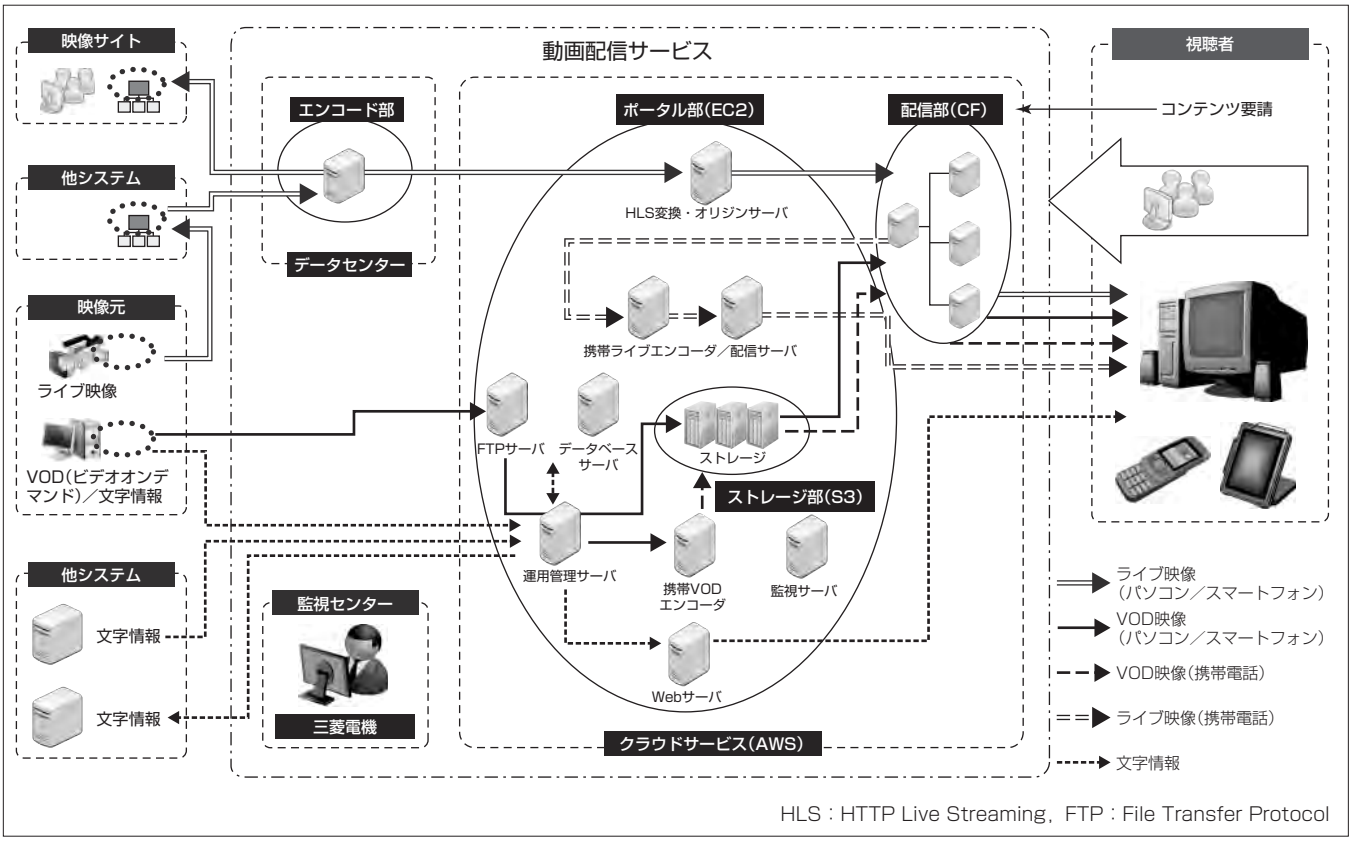
このシステムの特長は，入力した1種類のライブ映像をシステム内で3種類の配信方式に変換することによって，パソコン・携帯電話・スマートフォン向けにライブ映像を提供できることである。また，パソコンライブ映像の最大同時視聴者数を40,000人とする大規模配信を可能としている。

運用面では，クラウド内で持つ監視サービスに加えてオープンソフトウェアであるZabbix(注1)を併用することでシステムの各種異常を自動で検知して保守要員等にメールで通知する監視機能を実現し，従来の有人監視からシステムによる無人監視に切り換えている。

可用性では，クラウドのインスタンス(仮想サーバ)の稼働率が99.95%なので，このシステムの目標稼働率である99.99%を実現するためにクラウド内のデータセンター間で冗長化するシステムを構築している。

また，AWSサービスの特徴である利用時間による課金への対応として，時間帯で自動台数制御を行う方式を採用した。その他，データベースフェールオーバーの遅延，ライブ・オンデマンド映像配信，アクセス数集計等，幾つかの課題に対応している。

(注1) Zabbixは，Zabbix SIA社の登録商標である。



HLS：HTTP Live Streaming，FTP：File Transfer Protocol

大規模動画配信システム

ライブ映像の配信では，外部からライブ映像のデータを受信し，EC2(Amazon Elastic Compute Cloud)の各インスタンス上で各メディア向けの変換を行う。変換処理を行ったライブ映像データは，AWSのCDN(Contents Delivery Network)サービスであるCF(Amazon CloudFront)を利用して配信する。一方，オンデマンド映像は，S3(Amazon Simple Storage Service)に一旦格納して，CFで配信する仕組みである。

*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事業推進本部

1. まえがき

MDISでは，2010年11月にオンプレミスと社外CDNサービスを組み合わせた大規模動画配信システムを開発し，ライブ映像・オンデマンド映像をパソコン・携帯電話で一般ユーザーが視聴できるサービスを提供した。それがこのシステムの前身である。

このシステムでは，①システムコスト削減のため，オンプレミスからクラウドへ移行，②近年のユーザー数拡大への対応のため，パソコンライブ映像の同時視聴者数を20,000人から40,000人に拡張，③利用者が増加しているスマートフォン向けのライブ・オンデマンドサービスを追加，の3つを目的としてシステムを短期間で再構築し，2014年8月からサービス提供を開始している。

本稿では，クラウド（AWS）を利用した大規模動画配信システム構築における課題とその解決策について述べる。

2. システムの特長

このシステムの特長は，20種類の異なるライブ映像をパソコン・携帯電話・スマートフォン向けに提供できることである。配信方式としてHDS（HTTP（HyperText Transfer Protocol） Dynamic Streaming）とHLS（HTTP Live Streaming）を用意することで，パソコン・スマートフォン（全てのAndroid(注2)端末とiOS端末）をサポートしている。また，携帯電話に関しては配信サーバと携帯電話側アプリケーションを一対とした独自方式とした。

一方，オンデマンド映像の配信に関しては，スマートフォンでの視聴を考慮して，前身のシステムが採用したWMV（Windows Media(注3) Video）形式からMP4（MPEG（Moving Picture Experts Group）-4）形式に変更した。また，携帯電話への配信は，3つのキャリアブランド（docomo(注4)，au(注5)，SOFTBANK(注6)）に対応するため，パソコン向けのオンデマンド映像から自動的にそれぞれの形式に変換・蓄積することによって，ほとんどの携帯電話で視聴可能となっている。

（注2） Androidは，Google Inc. の登録商標である。
（注3） Windows Mediaは，Microsoft Corp. の登録商標である。
（注4） docomoは，日本電信電話㈱の登録商標である。
（注5） auは，KDDI㈱の登録商標である。
（注6） SOFTBANKは，ソフトバンク㈱の登録商標である。

3. クラウド化における課題と解決策

この章では，先に述べたシステムの目的，特長を実現するための設計上の留意事項を**3. 1節**で述べ，**3. 2節**から実装上の主要課題と解決策について述べる。

3.1 設計上の留意事項

設計時点で特に留意した事項は次の5項目である。

⑴ 設備投資の最小化

エンコード部での最新機器の採用とクラウドサービスの活用によって，初期設備を通信環境（回線・ルータ），運用・監視用パソコン，入力画像エンコード機器のみとした。

⑵ パッケージ利用とライセンス管理対策

構築スピードとコストの面から，携帯電話サービス対応，映像視聴用画面処理，映像配信・変換処理には既存パッケージをクラウド上で動作検証，チューニングを実施した上で利用した。なお，一部パッケージのライセンス管理で認証に物理メディアが必要であったが，パッケージのカスタマイズによって物理メディアでの認証を不要とし，クラウド上での利用を可能とした。

⑶ クラウドサービス停止時の対策

クラウドサービス（AWS）全体が停止した場合でも，最小限のライブ映像サービスが継続できるように，オンプレミス環境上のエンコード部から第三者の映像配信サービスへ映像を提供できる機種を選定して，設計した。

⑷ 映像画質のHD化への対応

現状は縦横比4：3のSD（Standard Definition）画質での映像サービスであるが，近い将来に16：9のHD（High Definition）画質での映像サービス開始が想定されるため，映像入力インタフェース，エンコード機器，Web画面設計などでHD化対応を前提とした設計を行った。クラウド内のサーバリソースについても，HD化による負荷増加に柔軟に対応可能な構成とした。

⑸ 更なる大規模動画配信への対応

今回構築したシステムでは，配信部からの同時配信人数を最大40,000人としているが，スマートフォンを中心とした同時配信人数の更なる拡張にも耐えられる構成とした。

配信規模拡張への対応として実施した項目は次のとおりである。

①配信部

現状でも十分な配信容量を保持しているが，バースト的な配信要求急増時に備え，配信部の利用制限値を見直し，今後の定常的な要求増加にも対応可能とした。

②ポータル部

クラウド内サーバリソースについてはスケールアップ（インスタンス増強），スケールアウト（インスタンス数増加）のどちらの方法でも能力増強が可能な構成とした。

3.2 可用性向上への対策

このシステムの目標稼働率は，99.99%であるが，クラウド部の公称インスタンス稼働率は99.95%である。そこで，次の3項目の対策を実施して，動画配信サービス全体としての稼働率99.99%を確保する設計を行った。

⑴ ポータル画面用Webサーバの耐障害性対策

全体で最大10台の冗長構成を採用した。5台ずつを異なるデータセンター上に分散して配置することで，Webサーバ単位での冗長構成のみではなく，クラウドで利用するデータセンターを含めて耐障害性を向上させた。

⑵ ライブ配信用オリジンサーバ切換え時の対策

動画配信ソースデータの提供元となるオリジンサーバについても，異なるデータセンター上に分散配置したホットスタンバイ構成として，障害発生などによる切換え時の映像配信タイムラグの短縮を図った。

(3) ポータル部の文字情報連携処理の二重化対策

他システムとの通信を伴うポータル部の文字情報連携処理は，接続先システム側の制約によってプライベートIP(Internet Protocol)での通信が必要であったが，クラウド側の制約もあり，完全な二重化構成での実装ができなかった。対応策として，稼働系と待機系を別のデータセンター上に配置するコールドスタンバイ構成を採用した。

3.3 監視の無人化(自動化)に向けた対策

このシステムでは，24時間無人監視を目的に，自動監視機能を搭載する設計とした。AWSには監視サービス(CloudWatch)が提供されているため，AWS上のサーバインスタンスの稼働状況を監視することでメトリクスを取得することができる。メトリクスとはサーバのリソース値を意味し，CPU(Central Processing Unit)使用率，ディスクI／O(Input／Output)回数，ネットワーク流量，データベースコネクション数などを取得できる。取得されたメトリクスはAWSコンソールに蓄積され，しきい値を超えている場合に警告メールを自動送信する。またAWSコンソールにログインすることによって，これらのメトリクスを，**図1**のようなグラフ上で確認することができる。

このシステムでは，CloudWatchに加え，統合監視ミドルウェアであるZabbixとの連携による監視も行っている。

監視システムの構成を**図2**に示す。

CloudWatchとZabbixの連携によって次の3つの機能を実現した。

(1) CloudWatchとZabbix連携による監視対象の拡大

CloudWatchでは，メモリ使用率やディスク使用率など，一部取得できないリソース情報があるが，監視対象インスタンスへZabbixエージェントをインストールすることで，これらのリソース情報を監視可能にした。一方，RDS

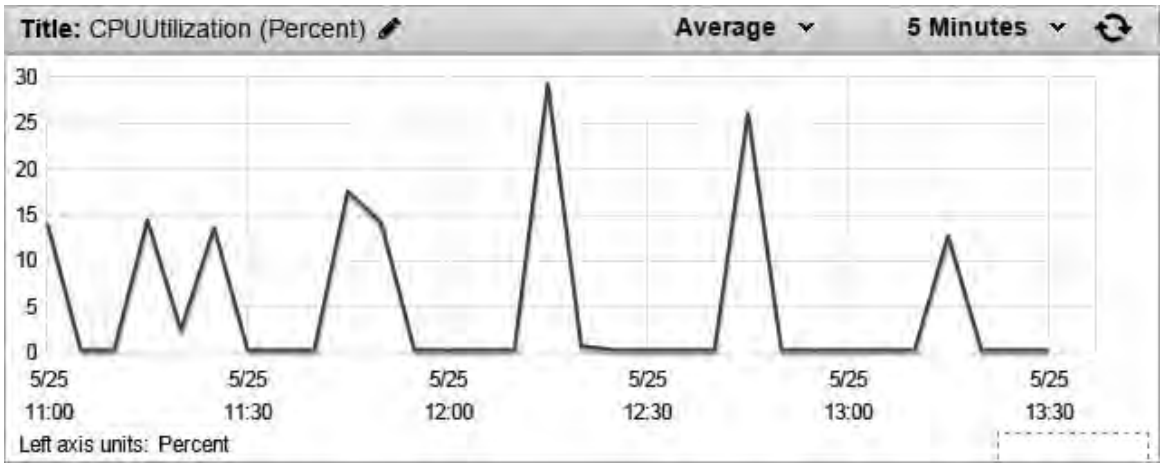


図1．AWSコンソール上でのメトリクスグラフ(CPU使用率)

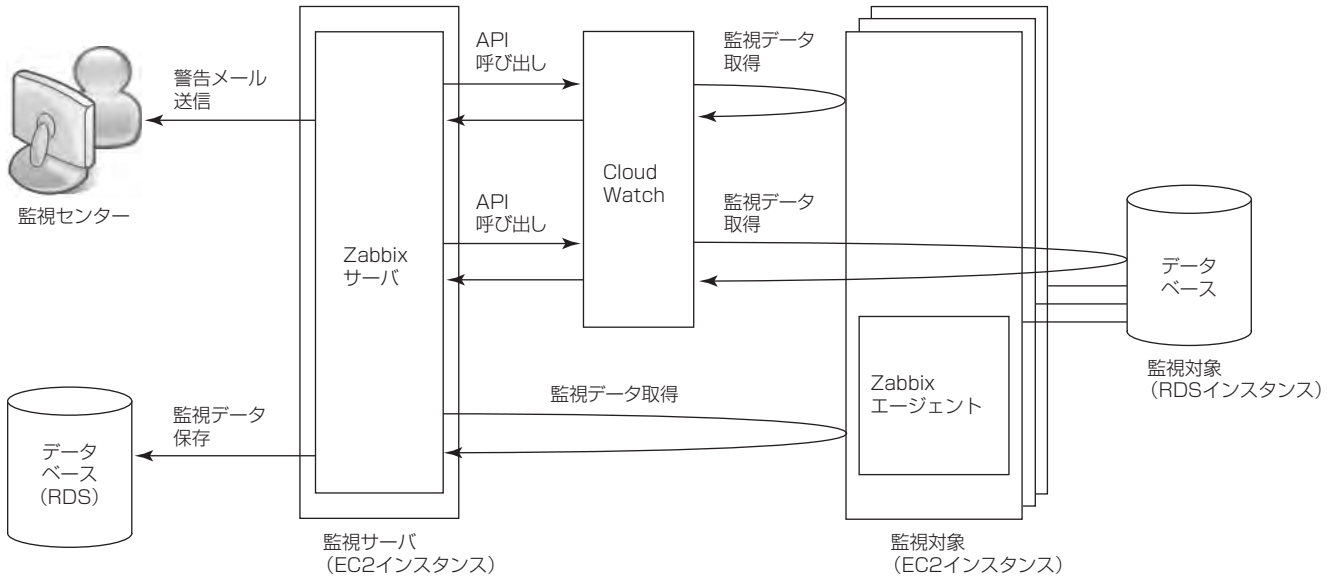


図2．監視システムの構成

(Amazon Relational Database Service for Oracle Database)など，OSへのログインができず，Zabbixエージェントを導入できないインスタンスについては，Zabbixエージェントでリソース情報を取得することができないため，CloudWatch経由で情報を取得することで対応を図った。このように，CloudWatchとZabbixを連携させることで，両者単独では監視できない，保守サポートに必要な監視データを取得できるようにした。実際に監視している項目の一部を**表1**に示す。

⑵ メトリクス保存期間の拡大

CloudWatchで取得したメトリクスをAWS上で保存する場合，最長2週間までしか保存されない。そのため，このシステムではCloudWatchで取得したメトリクス，及び，Zabbixエージェントによって取得した監視データをZabbixサーバに接続されたRDSインスタンスに一元的に保存する設計とした。その結果，最長5年間保存できるようになり，稼働状況調査や障害調査時に，過去の監視データをさかのぼって参照できるようになった。

⑶ 障害検出時のインスタンスの自動制御

Zabbixでは外部チェックと呼ばれる機能によって，監視データがしきい値を超過した場合等をトリガー条件に設定して，外部コマンドを実行することができる。また，AWSにはAWS CLI(Command Line Interface)と呼ばれるコマンドラインベースのAPI(Application Programming Interface)が提供されており，APIの呼出しによってインスタンスの制御が可能である。このシステムではZabbixの外部チェック機能を用いてAWS CLIを呼び出すスクリプトを実行するようにした。これによって**表2**に示すようなインスタンスの自動制御が可能となった。

表1．監視項目

監視項目	CloudWatch単独での監視	Zabbix単独での監視
CPU使用率	○(注7)	○(注7)
メモリ使用率	×	○
ディスク使用率	×	○
RDS監視	○	×
ELB監視	○	×
ログ監視	×	○

○：監視可　×：監視不可

ELB：Elastic Load Balancing

（注7） CPUの全体使用率は，CloudWatch，Zabbixともに監視可であるが，CPUの詳細情報(user，system，iowait，load average等)に関しては，CloudWatchは監視不可，Zabbixは監視可である。

表2．Zabbixによるインスタンス制御(一部の例)

項目	トリガ条件	制御方法
インスタンスの再起動	Zabbixサーバからインスタンスへping疎通に失敗した場合	Zabbixサーバから該当インスタンスに停止コマンドを実行して，インスタンスを再起動させる
待機系インスタンスへのフェールオーバー	ZabbixサーバからAWSインスタンスへのweb監視で異常を検知した場合	ZabbixサーバからRoute53(DNS)のCNAMEレコードを待機系インスタンスのホスト名に書き換えるコマンドを実行して，AWSへのアクセスを，現用系から待機系へ切り換える

3.4 データベースフェールオーバー遅延対策

このシステムでは，外部システムから送信される文字情報をその都度データベースに格納し，1分周期で表示情報を更新して提供する必要があった。

このシステムでのデータベースは，AWSのRDSサービスを信頼性向上のためMulti-AZ(Availability Zone)配置オプションを利用して構築したが，このRDSの冗長化構成ではフェールオーバー時にDNS(Domain Name System)への付け替え等が発生する関係で，フェールオーバーに数分かかることがあり，情報更新が滞るという課題があった。

そこで，Webサーバ側の処理を見直して，データベースから情報取得して表示データを生成する部分については，最後に受け取った情報を再利用して情報表示を継続する仕組みにすることで対応した。

3.5 インスタンスの稼働制御によるAWS課金対策

AWSではインスタンスを利用した時間に応じて課金される。そのため，システムの負荷に関係なく常に全てのインスタンスを稼働させてしまうと，無駄なランニングコストがかかるという課題があった。必要な時に必要な数だけインスタンスを使用するためのAWSの標準機能として，自動スケーリング機能がある。これは，インスタンスの負荷があらかじめ設定した基準に達した場合に，EC2インスタンスの負荷に合わせてインスタンスのスペックを上下させ，インスタンス数を増減させるものであるが，このスケーリングは起動開始から起動完了となるまでに数分を要していた。

また，このシステムには，1日を通して定期的に視聴者数が急増して負荷が高くなる時間帯があり，その時間帯に限りインスタンス数を増やしたいが，急激な負荷増大には，自動スケーリング機能のスピードが追い付けないという課題があった。その対策として，AWSのAPIにインスタンスを起動／停止できるものがあり，これを用いてインスタンス数を増減させる方式を採用した。

1日24時間を3パターンに分け，日中を全てのインスタンス稼働，夜間を半数のインスタンス稼働，深夜を必要最低限のインスタンス稼働とした。それによって，常に全てのインスタンスをフル稼働させることがなくなり，ランニングコストを削減し，AWSの無駄な課金が生じないようにした。

3.6 アクセス数集計の精度向上への対策

このシステムでは同時視聴者数の把握として，視聴されたアクセス数から同一IPアドレスでアクセスされた場合と同一チャネルをアクセスした場合は，1回とカウントする仕様で5分ごとに統計情報を収集する仕組みが要求されていた。

また，ライブ映像に関しては，外部システムが直接配信ポイントを参照してライブ視聴する仕組みを提供するが，システム内でのアクセス数をカウントする方法では，その

表3．ライブ映像サービス提供対象と配信形式

サービス対象	配信形式	備考
パソコン，一部スマートフォン	HDS	Android2.2以前
スマートフォン	HLS	
携帯電話	独自形式	docomo機種のみ

ような直接参照されるアクセス数が除外されてしまうという課題があった。この課題に対しては，AWSが提供するサービスの1つである，配信部（CF）の各サーバのアクセスログをS3に収集する機能を利用して，それらのアクセスログを解析することによって統計情報を算出する仕組みを構築することで対応を図った。

また，このログ収集は，AWSの仕様では60分程度で配信部の各サーバからS3に格納されるとされていたが，実際には，24時間以降に格納されるサーバがあることが判明したため，このシステムでは，72時間後にログ解析を行う仕組みとしている。

3.7　ライブ・オンデマンド映像の多様な配信形式への対応

ここでは，多彩な機種で動画視聴を可能とするために行った設計上の留意事項について述べる。

3.7.1　ライブ配信形式

このシステムはSD-SDI（Standard Definition-Serial Digital Interface）で受け取った映像・音声を最終的に**表3**に示す形式で視聴者へサービス提供している。

HDSでの提供先は規格の定義がなく，代表的なAndroid搭載機器での検証を実施し，ユーザーエージェントによる対象機器の判定と配信形式の選択を実施している。

携帯電話は，先に述べたとおり，クラウド上での動作確認及び入力映像対応カスタマイズを経てライブ配信パッケージをdocomo製品のみに対応させた。

なお，パソコン，携帯電話については配信形式に合わせた再生プレーヤーアプリケーションの更新も実施している。

主にスマートフォン向けに配信しているHLSについては，クラウド内インスタンスにHDSからの変換処理を実装しており，変換が不要なHDSに比べて即時性が損なわれる面があるが，変換処理に利用するインスタンスのチューニング及び無線環境での利用が大多数であることなどから，パソコンライブとの差異は目立つものとはなっていない。

表4．オンデマンド映像サービス提供対象と配信形式

サービス対象	配信形式	備考
パソコン，一部スマートフォン	MP4ファイル	
携帯電話	独自形式（7種類）	docomo，au，SOFTBANK

3.7.2　オンデマンド配信形式

ライブ配信に対して，オンデマンド配信では元映像はライブ映像からの取得ではなく，ダイジェスト版への編集後にMP4ファイルとしてこのシステムへ登録後，配信する方式としている。基本はMP4ファイルをそのまま配信しているが，携帯電話のみ**表4**に示すとおり，機種個別対応の変換実施後に配信している。

4. むすび

クラウドサービスを利用した大規模動画配信システムの構築は，ビジネスシーンで要求が高まってきている分野である。今回の事例・構築ノウハウをいかして今後のシステム構築に取り組んでいく。

特集論文

仮想環境でのストレージ運用の自動化

遠藤　司*
小笠原大治*
河野義哉*

Automated Storage Operation under Virtualized Environments

Tsukasa Endo, Daiji Ogasawara, Yoshiya Kouno

要　旨

近年，物理サーバやストレージの仮想化によるリソースの運用効率化が進んでいる一方，仮想環境の運用コストの増加が課題となっている。三菱電機インフォメーションシステムズ㈱(MDIS)では，大量の仮想マシンの構築・運用を自動化する仮想環境構築自動化ソフトウェア“Biz FLEX VC”を開発し，この課題に対応してきた。今回，仮想マシン構築時にストレージのボリューム割当て作業を自動化する機能を更に追加し，仮想環境でのストレージ運用の効率化を図った。

仮想環境でストレージの運用コストが増加する原因として，次の3点が挙げられる。

⑴　ボリューム増加による運用負荷の増大

仮想環境の拡大に伴い，ストレージのボリュームも増加の一途をたどっている。ボリュームの増加はストレージの運用業務の負荷を増大させ，運用コストを増加させる。

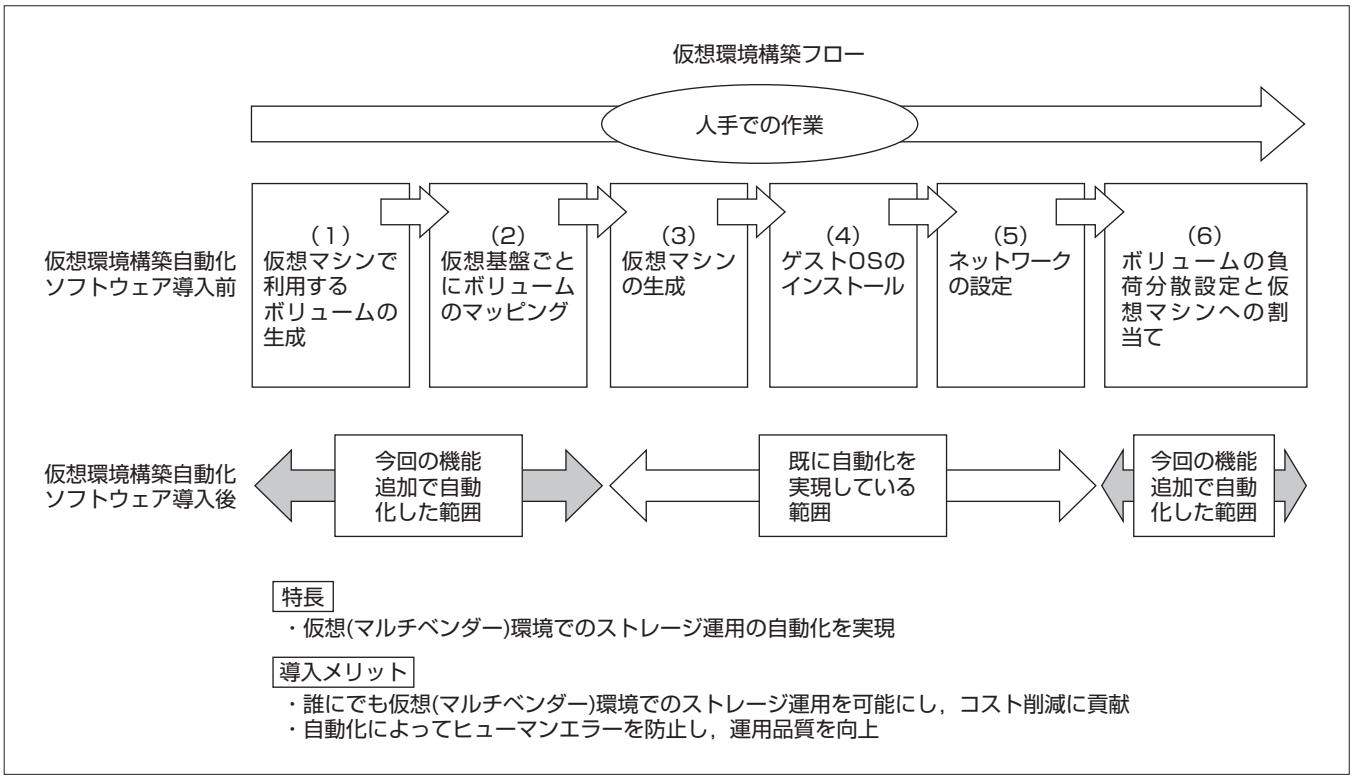
⑵　手作業による仮想基盤とストレージの間の煩雑な処理

仮想基盤とストレージの双方にまたがる処理の自動化は進んでおらず，各製品ベンダーから提供される運用ツールを用いて煩雑な作業を行わなければならない。このような作業はヒューマンエラーを引き起こし，手戻りの原因となる。

⑶　ストレージのマルチベンダー化に対応した運用要員の増加

マルチベンダー化したストレージを運用するには専門的な知識が必要となる。そのため，これらの知識・技術を持つ特定の担当者への業務集中による対応の遅れを回避するため，要員を増やして運用体制を強化する必要がある。

この課題に対応するため，MDISでは仮想(マルチベンダー)環境でストレージの運用を自動化するためのソフトウェアを開発した。これによって，ストレージ運用業務の効率化を実現し，ストレージのボリューム割当て作業における担当者の作業時間を約1/20に削減することができた。



ストレージのボリューム割当て作業の自動化

仮想(マルチベンダー)環境でのストレージ運用の自動化を実現することによって，仮想マシンの生成からストレージボリュームの割当てまでの一連の処理を自動化し，ストレージ運用の効率化を実現した。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

近年，物理サーバやストレージの仮想化によるリソースの運用効率化が進んでいる[1]一方で，仮想環境の運用コストの増加が課題となってきている[2]。MDISでは，大量の仮想マシンの構築・運用を自動化する仮想環境構築自動化ソフトウェア“BizFLEX VC”を開発し，この課題に対応してきた。

今回，仮想マシン構築時にストレージのボリュームの割当て作業を自動化する機能をこのソフトウェアに追加し，仮想環境でのストレージ運用の効率化を図った。本稿ではこの機能について述べる。

2. ストレージ運用の課題

仮想環境でストレージ運用コストが増加する原因として，次の3点が挙げられる。

(1) ボリューム増加による運用負荷の増大

仮想環境の規模が拡大することで仮想マシンの台数が増加しており，仮想マシンに割当てられたボリュームの数も増加の一途をたどっている。ボリュームの増加は，ボリュームの構築やバックアップ，性能・容量の監視，構成管理などのストレージの運用業務の負荷を増大させ，運用コストの増加を引き起こす。

(2) 手作業による仮想基盤とストレージの間の煩雑な処理

仮想基盤上に生成した仮想マシンに対してストレージのボリュームを割当てるといった，仮想基盤とストレージの双方に跨る処理の自動化は実現されていない。現状では，**図1**のように，各製品ベンダーから提供されている運用ツールを利用し，双方の環境に対して交互に手作業で必要な処理を行っている。このような作業は，入力誤りによる設定ミスなどのヒューマンエラーを引き起こす原因となり，手戻りによって運用コストが増加する。

(3) ストレージのマルチベンダー化に対応した運用要員の増加

ストレージ製品は，ベンダーや機種ごとにボリュームやストレージプールの構造など，内部のアーキテクチャが大きく異なる。一例として，**図2**に記憶装置，ストレージプール，ボリュームの製品間の構造の違いを示す。ストレージプールやボリュームの生成といったストレージの運用業務を行う場合，利用するストレージのストレージプールがどのような構造になっているのか，ストレージプールとボリュームの関係は

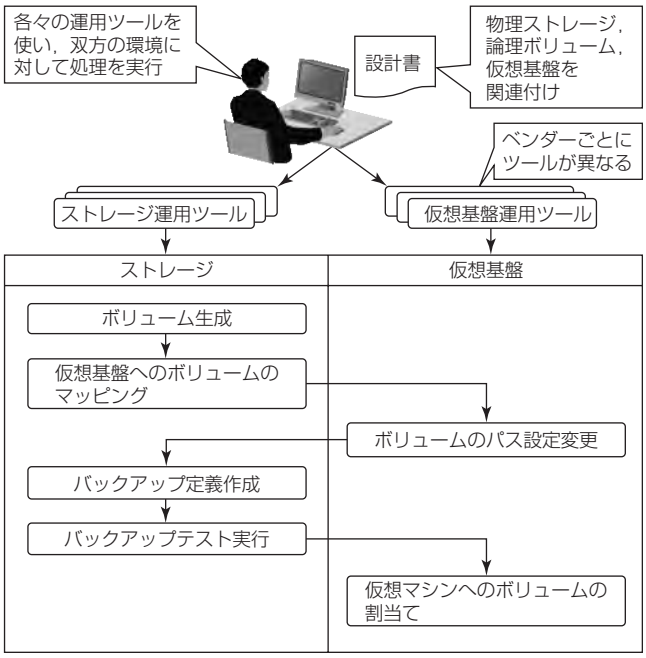


図1．仮想マシンへのボリューム割当て作業のフロー

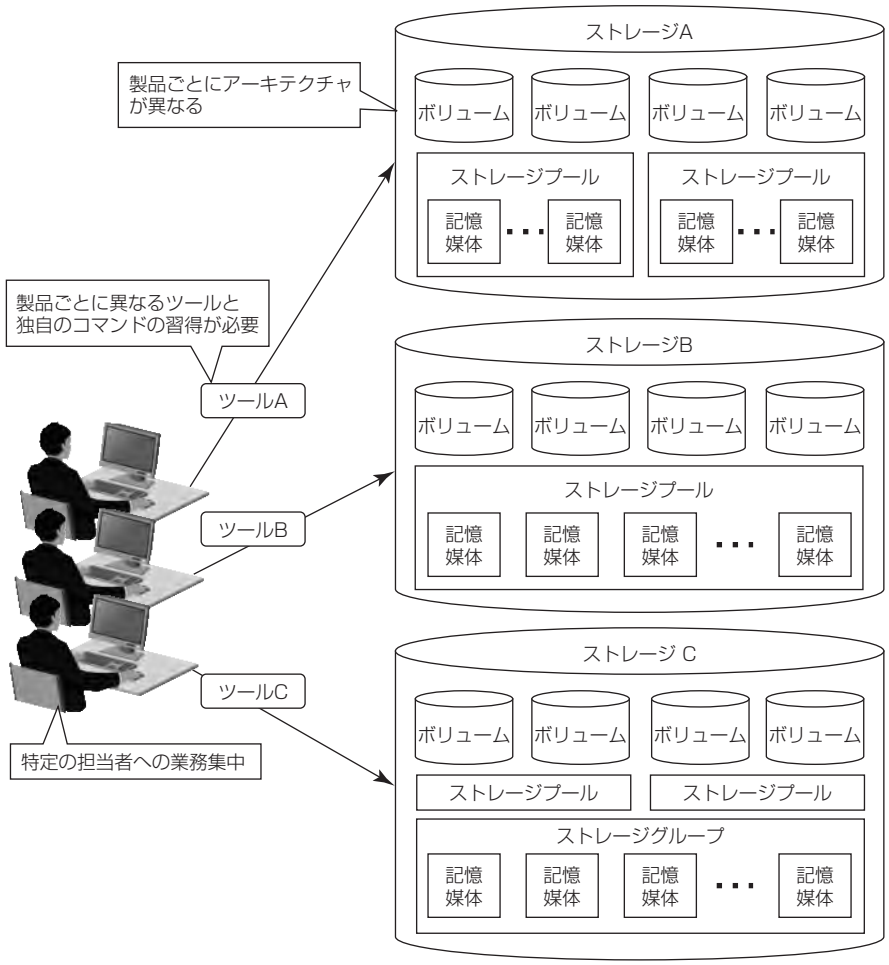


図2．ベンダーごとのストレージの構造の違い

どうなっているかなど，ストレージのアーキテクチャを理解し，さらに，各製品ベンダーから提供される機種ごとのツールや製品独自のコマンドの扱い方を理解する必要がある。ストレージの運用にはこのような専門的な知識や技術が必要であるが，知識・技術の習得には個人差があるため誰もが同じ作業を行えるようにはならない。特定の担当者への業務集中による対応の遅れを回避するため，運用要員を増して運用体制を強化する必要があり，運用コストが増える。

3. 課題への対策

3.1 仮想(マルチベンダー)環境での自動化機能

先に述べた3つの課題を解決するために，仮想(マルチベンダー)環境でストレージ運用を自動化するためのソフトウェアを開発した。このソフトウェアによって，ストレージ運用担当者の増加への対応や煩雑な作業によるヒューマンエラーの防止，さらに，マルチベンダー化したストレージに対する知識・技術の属人化の排除が可能となる。

このソフトウェアは，ストレージのベンダーに依存しない統一されたユーザーインタフェース(**図3**)で設定された個々のパラメータをベンダー固有のコマンドに変換して自動実行することで，**図1**のようなベンダー依存の運用ツールや**図2**のようなストレージの構造の違いに起因する運用業務の煩雑さ，属人性を排除することができる。

このソフトウェアが統一されたユーザーインタフェースとして提供する機能を**表1**に示す。

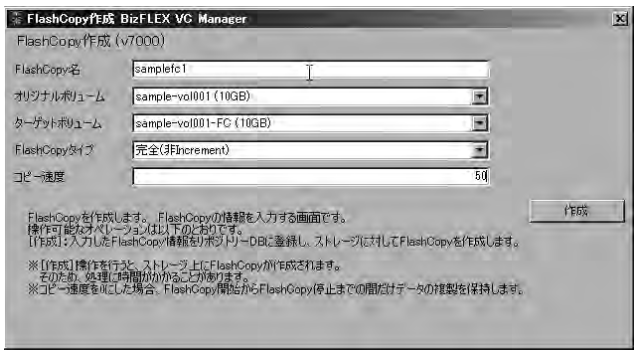
3.2 自動化機能の実現方式

各ストレージ製品はボリュームの生成，削除や仮想基盤へのマッピングなどの処理を行うためのインタフェース(API(Application Programming Interface)，コマンドラインなど)を提供している。通常，これらのインタフェースはストレージの製品ごとに異なるため，同じ命令で同じ処理を行うことはできない。

そこで，このソフトウェアは，統一されたユーザーインタフェースとストレージの構造の違いを吸収したリポジトリーデータベースを提供することで，運用業務担当者が製品ごとの違いを意識することなくストレージに対する処理を実行できるようにした。

運用業務担当者は，統一されたユーザーインタフェースからボリューム名やボリュームサイズなど各ストレージに共通なパラメータを入力し，処理を実行する。

処理実行の指示を受けたこのソフトウェアは，入力されたパラメータとリポジトリーデータベースの情報を基に，運用業務担当者がどのストレージに対して処理を実行しようとしているのかを決定し，入力されたパラメータ以外に処理を行うために必要なストレージ独自のパラメータを補完し，これらのパラメータをベンダー固有のコマンドと組み合わせて実行する(**図4**)。



(a) バックアップ定義作成

(b) ボリューム生成

図3．ユーザーインタフェース例

表1．ストレージ運用自動化機能

ストレージ管理	ストレージを管理する機能で，入力パラメータから対象ストレージのベンダーの特定や，ストレージへの接続を行う。
ボリューム生成	ボリュームサイズやLUN(Logical Unit Number)の番号を指定してボリュームの作成，及び作成したボリュームの削除を行う。ボリューム作成時にマッピング先の仮想基盤を指定した場合は仮想基盤へのマッピングを自動的に行う。
ボリューム変更	ボリュームのマッピング先の変更やボリュームのマッピングの削除を行う。
バックアップ	ボリュームのバックアップの定義の作成やバックアップの実行，停止，削除を行う。

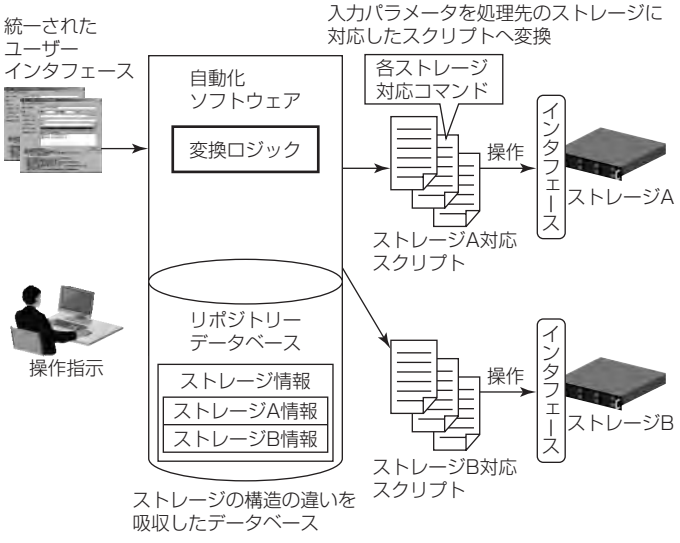


図4．自動化機能実現の仕組み

4. 導 入 効 果

このソフトウェアの導入効果を測定するために，ストレージのボリュームの割当て作業をベンダー提供の運用ツールを利用して行った場合と，このソフトウェアを利用して行った場合のそれぞれの作業時間を測定して比較した。その結果，このソフトウェアを利用することで，ボリュームの割当て作業における運用業務担当者の作業時間を約1/20に削減できた。

この結果を基に，大規模な仮想環境でこのソフトウェアを導入した場合の効果についても試算した。某上場企業で，この自動化ソフトウェアを利用した場合の工数の削減効果を**図5**に示す。この案件では，本番環境構築後の設定変更をBCP(Business Continuity Plan)環境へ効率的に反映させるため，仮想環境を活用して年に10回，80台の仮想マシンから成るBCP環境を繰り返し構築するといった運用を行っている。この環境で，ボリュームの割当て作業を自動化した場合，ボリュームの割当て作業では約6％，仮想マシンの自動生成による削減効果(13％)と合わせた場合は約19％の工数の削減効果があると想定された。

なお，このソフトウェアを導入することで以下の効果も期待できる。

統一されたユーザーインタフェースによって，パラメータ設計書があれば誰でも簡単な操作でマルチベンダーのストレージに対する操作を実行することが可能となり，属人性を排除することができる。さらに，今後操作対象のストレージが増えた場合も画面上の操作は変わらないので，従来の運用業務担当者が業務を担当することができるため，新たな運用要員の確保は不要である。

また，このソフトウェアの自動化対象は，複数のベンダーや機種に跨る複雑な処理であるので，従来の手作業では仮想マシンの生成からボリュームの割当てまでの一連の作業を実施した際に，コマンドの入力誤りのようなヒューマンエラーが発生しやすくなっていた。このようなヒューマンエラーが発生すると，誤りの特定や修正に多くの時間がかかってしまう。このソフトウェアの導入によってこのようなヒューマンエラーを防止し，運用品質を向上させることができる。

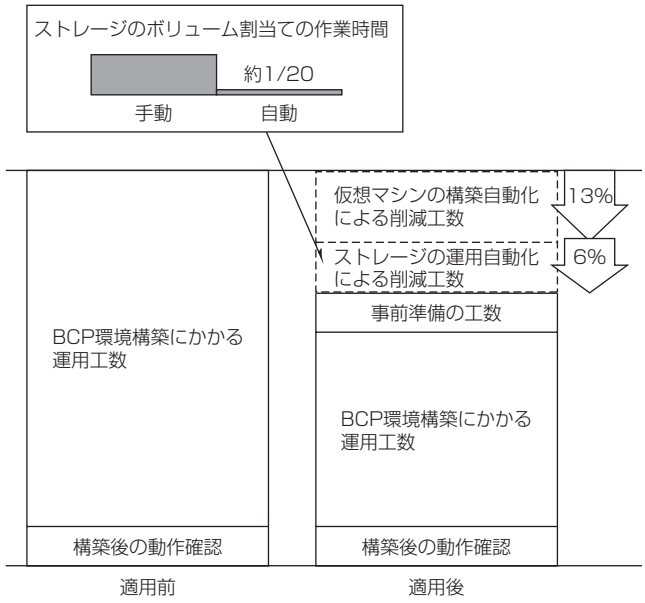


図5．運用工数の削減効果

5. む す び

システムの仮想化の流れは拡大傾向にあり，仮想基盤だけではなくストレージやネットワークも含めた仮想環境の運用効率化が今後ますます要求されることが想定される。MDISでは，これらの要求にこたえるべく，対応ベンダー拡充によるマルチベンダー製品対応の強化や，条件分岐を含めた複雑な運用プロセスの自動化，試験の自動化などの検討を進めている。

今後も引き続き仮想環境の運用自動化の開発を継続し，運用業務の効率化に貢献していく。

参 考 文 献

(1) 一般社団法人 日本情報システム・ユーザー協会：ソフトウェアメトリックス調査2014（2014）
(2) 日経BP社：システム運用実態調査2013報告書（2013）

特集論文

スケールアウトによる負荷分散を実現するデータ分析フレームワーク“AnalyticMart”

戎　直哉*
和田貴成*
山岸義徳**

High Scalability Data Analysis Framework "AnalyticMart"

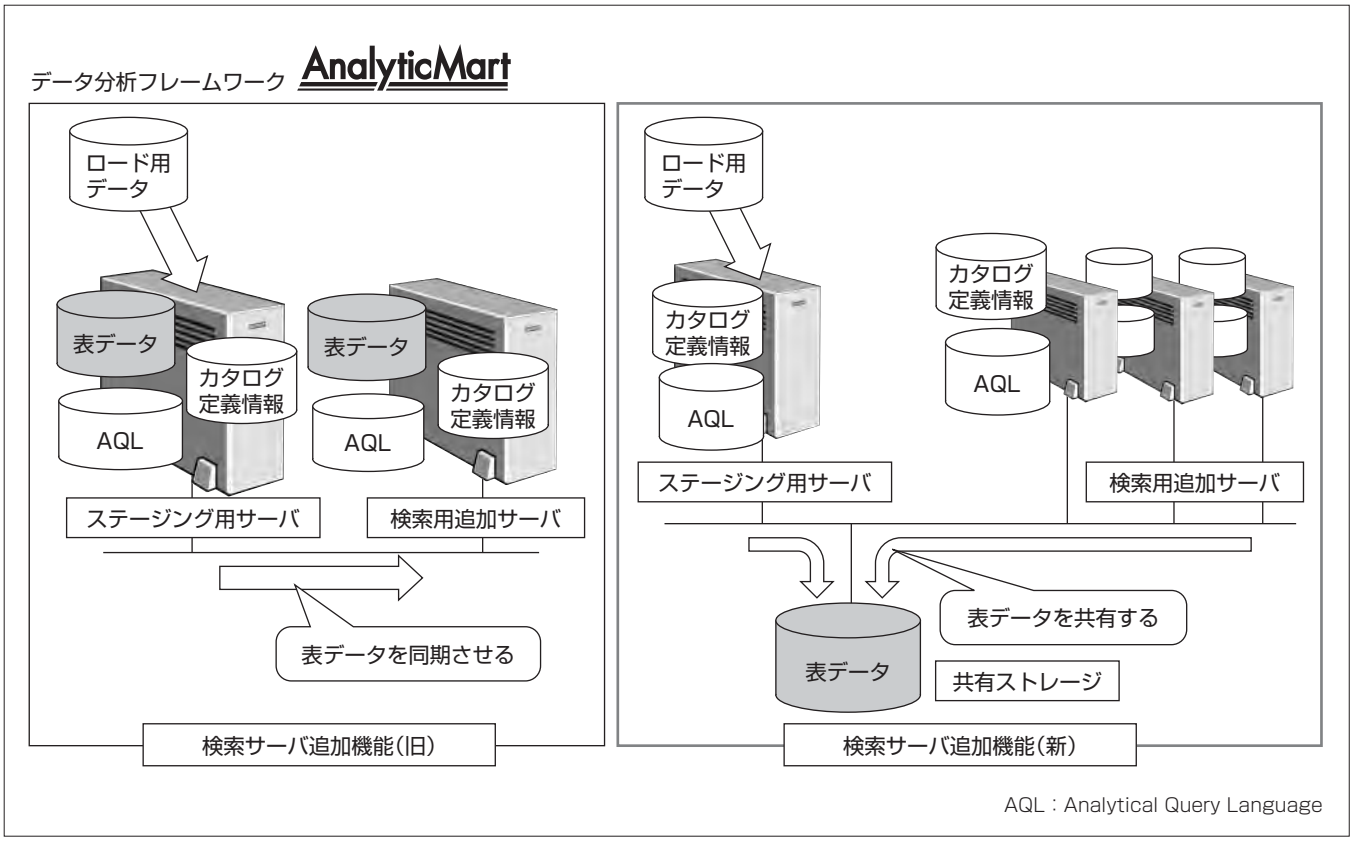
Naoya Ebisu, Takashige Wada, Yoshinori Yamagishi

要　旨

近年，データ分析の重要性の高まりによって，データ分析システムの利用者数が増大するとともに，発生したデータの分析結果への短時間での反映が求められるようになってきた。頻繁にデータ投入が行われる環境で，多数の利用者からの検索処理を遅延なく実行するためには，処理負荷の分散を実現することが必須の要件となる。

三菱電機インフォメーションネットワーク㈱（MIND）が提供する“AnalyticMart”はデータ分析を低コストで実現できる製品（フレームワーク）で，負荷を分散する機能として，“検索サーバ追加機能”を提供してきた。従来の“検索サーバ追加機能”は，対象のソースから適切なデータの加工・抽出・ロードを行うデータステージングと検索集計処理の負荷を2台のサーバで分散することを目的としているため，利用者数が増加した場合の拡張性や運用性に課題があり，より多くの利用者への対応が困難であった。

データ分析システム利用者数増加の課題に対応したデータ共有型の“検索サーバ追加機能”は，データロード用のステージング用サーバと複数の検索用追加サーバが，共有ストレージ上の表データを共有する構成である。利用者数の増加に応じて，容易に検索用追加サーバを増設（スケールアウト）することができ，全体のスループットを向上させることが可能である。



検索サーバ追加機能の新旧比較

検索サーバ追加機能は，データステージングと検索集計処理の負荷を分散させ，システムのスケーラビリティ向上を実現する機能である。ステージング用サーバと検索用追加サーバで，表データを同期させる従来の構成に加えて，ステージング用サーバと複数の検索用追加サーバで共有ストレージ上の表データを共有する構成を新たに提供する。

*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

1. まえがき

DWH(Data WareHouse)に代表されるデータ分析システムは，従来，情報システム部門など一部の部門が活用してきた。しかし，近年，データ分析の重要性の高まりによって，マーケティング部門や経営企画部門などに活用範囲が拡大し，システムの利用者数が増加している。また，発生したデータをリアルタイムで分析に利用したいという要望もあり，データの投入頻度も増す傾向にある。このように，データのロードが頻繁に行われ，かつ，同時に多数のユーザーからの検索要求が発生するシステムでは，処理負荷の分散を実現することが必須となる。MINDが提供するデータ分析フレームワークAnalyticMartでは，負荷分散を実現するために“検索サーバ追加機能”を提供してきた。しかし，従来の“検索サーバ追加機能”では，拡張性や運用性の課題があり，より多くのデータ分析システム利用者への対応が困難であった。

本稿では，複数台のサーバを追加することによって負荷分散を容易に実現する“検索サーバ追加機能(データ共有型構成)”の機能や利点などを中心に述べる。

2. AnalyticMartでのスケールアウトへの対応

2.1 AnalyticMart

AnalyticMartは，販売分析，顧客分析，ログ分析，環境データ分析といった多様で形式の異なるデータの分析を，統一したアーキテクチャで効率よく低コストで実現できるフレームワーク[(1)]である。AnalyticMartが提供する統一した分析基盤によって，中小規模から大規模まで，規模に合わせたデータ分析システムの構築・運用を実現することができる。AnalyticMartではAQLと呼ばれる標準の構造化データ用データベースを使用しているが，そのアーキテクチャはデータ分析向けに最適化されたものである。AQLの特長[(2)]を次に挙げる。

(1) 高度な圧縮技術によるディスク容量の削減

元データを1/5から最大1/40のサイズに圧縮し，ストレージ容量の大幅な削減ができる[(3)]。

(2) 高速集計・検索

必要な列に限定した選択的な読み出し処理，圧縮・伸張処理の並列実行によって，高速な集計・検索性能を実現する。

2.2 検索サーバ追加機能

負荷分散を実現するための機能として，AnalyticMartでは，検索サーバ追加機能を提供してきた。従来の検索サーバ追加機能の構成を**図1**に示す。検索サーバ追加機能は，データロード処理を専用に行うステージング用サーバ1台，及び，データ分析システム利用者からの検索・集計の要求を処理する検索用追加サーバ1台の合計2台から構成されるシステムである。この機能では，ステージング用サーバにロードされた表データ，及びカタログ定義情報(データベース全体の管理情報)を，定期的に検索用追加サーバに反映することによって，サーバ間でのデータ同期を実現している。表データの同期処理は，圧縮された増分データのみを配布することによって，短時間でのデータ同期が可能となる。

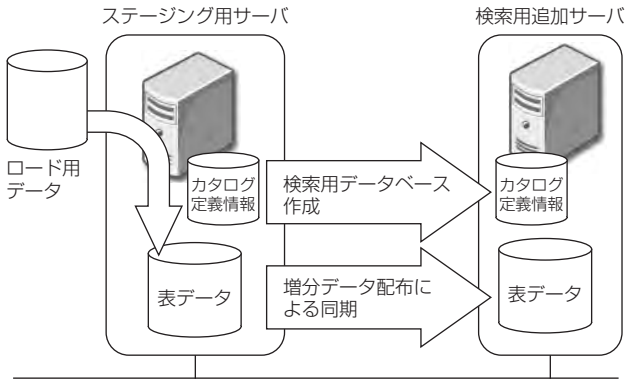


図1．従来の検索サーバ追加機能

2.3 検索サーバ追加機能の課題

従来の検索サーバ追加機能は，ステージング処理と検索・集計処理の負荷分散が目的であり，データ分析システム利用者数が増加した場合には，検索用サーバをより高性能のものに置き換えて対応しなければならないという課題があった。1台のサーバで性能を向上させることは限界があるため，データ分析システム利用者数の増加に対応するためには，複数台のサーバを追加することによって負荷分散を実現する機能(スケールアウト)が必須となる。

2.4 スケールアウトを実現するための課題

サーバ間で表データを同期させる従来方式で，検索用追加サーバを複数台追加する構成にした場合，運用性について次のような課題が発生すると考えられる。

(1) 表データ同期中のサーバ間でのデータ不整合を防止するために，同期が完了するまで検索ユーザーは待ち状態となる。そのため，検索用追加サーバが複数台存在する場合は，長時間の待ち状態が頻繁に発生する可能性がある。

(2) 検索用追加サーバの増設時には，ステージング用サーバから，増設したサーバ全てにデータを配布する必要があるため，サーバ増設に要する時間が長くなる。

(3) システム全体では，“データ規模×サーバ台数”に相当するストレージ容量が必要となる。

これらの課題を解決するために，新たな検索サーバ追加機能として，“データ共有型構成”の開発を行った。

3. 新検索サーバ追加機能(データ共有型構成)

3.1 システム構成

新しく検索サーバ追加機能として提供する“データ共有型構成”を**図2**に示す。この構成は，データロード処理を

専用に行うステージング用サーバ(1台),データ分析システム利用者からの検索・集計の要求を処理する検索用追加サーバ(複数台),及び,それらのサーバからアクセスが可能な共有ストレージで構成される。

ステージング用サーバがロードする表データは,共有ストレージ上に配置し,複数の検索用追加サーバと共有する。カタログ定義情報は,各々のサーバ上で管理する。

3.2 AQL分散実行機能

AQLでは,ユーザー定義情報,表定義情報などのカタログ定義情報をメモリ上に配置することによって,検索・集計時の高速処理を実現している。ディスク上のカタログ定義情報は,AQL起動時にメモリ上に展開され,カタログ定義情報の更新時には,メモリ上の定義情報とともに,ディスク上の定義情報が更新される。データ共有型構成では,各検索用追加サーバで同様の仕組みを実現するため,カタログ定義情報は各サーバに配置し,各サーバでカタログ定義情報の更新を実行する方式を採用した。この方式を実現するためには,複数サーバ上のカタログ定義情報を同期させて更新する必要があるが,各サーバで独立して更新処理を行うと,運用の負荷が増すとともに,不整合が生じる原因となり得る。そのため,ユーザーはステージング用サーバ上でのみカタログ定義情報の更新を行い,同じ内容が各検索用追加サーバで実行される機能(AQL分散実行機能)を開発した。

AQL分散実行機能の構成を**図3**に示す。AQL分散実行機能は,ステージング用サーバから自身及び各検索用追加サーバに対してカタログ定義操作命令(例:表作成)を送信する"分散操作実行ユーティリティ"と,分散操作実行ユーティリティから受信したカタログ定義操作命令を各サーバ上で実行する"分散操作サービス"の2つのコンポーネントで構成される。

3.3 データ共有型構成の特長

データ共有型構成の特長を次に挙げる。

(1) 共有ストレージ上に配置された表データは全てのサーバで共有するため,サーバ間の表データの同期が不要である。そのため,表データ同期による検索ユーザーの長時間待機が発生しない。

(2) 検索用追加サーバの増設時に表データの配布が必要ないため,システム拡張に要する時間が,従来の構成より短縮できる。

(3) 表データはステージング用サーバ,及び,検索用追加サーバで共有する仕組みのため,ストレージ容量を従来の構成より削減できる。

以上の特長によって,データ分析システム利用者数が増加した場合の拡張性や運用性の課題が解決できる。

3.4 スケールアウトに関する性能評価

複数の検索用追加サーバによって負荷分散が実現できることを検証するための評価を実施した。

(1) 評価環境

ステージング用サーバ,及び,検索用追加サーバは,メモリ8Gバイト,CPU(Central Processing Unit)4個を搭載したサーバで評価した。

(2) 評価目的

検索処理を連続して実行するジョブが複数同時に要求された場合に,検索用追加サーバの増設に応じて,システム全体のスループットが向上することを確認する。

(3) 評価方法

評価では,19個の問合せを連続実行するジョブを30個同時に実行し,全てのジョブが完了するまでの時間を測定した。なお,各検索用追加サーバで同時に実行するジョブ数は,均等となるように配分した。

(4) 評価結果

検索用追加サーバの台数を変化させた場合のシステム全体のスループットを**図4**に示す。検索用追加サーバの台数が増加すると,スループットの向上は確認できたが,4台目の場合はスループットの向上率は低下する結果となった。

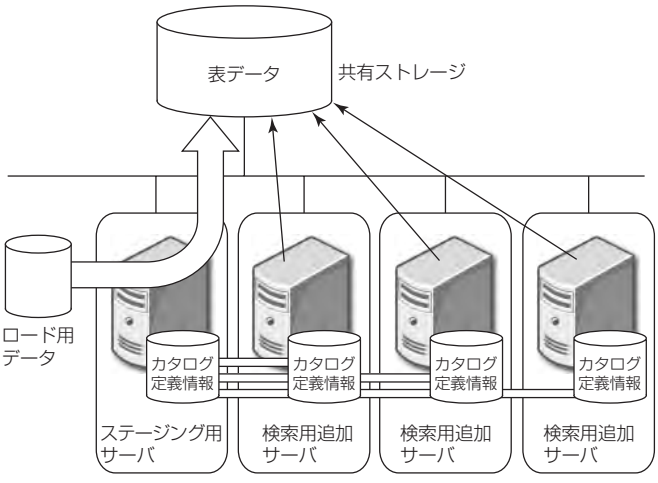


図2. データ共有型構成

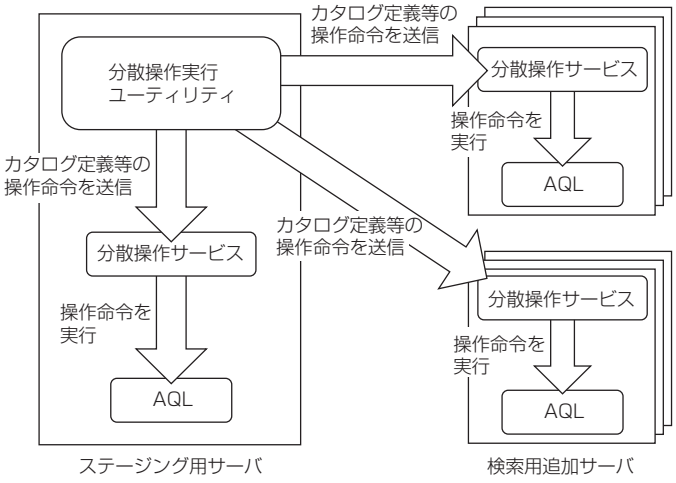


図3. AQL分散実行機能の構成

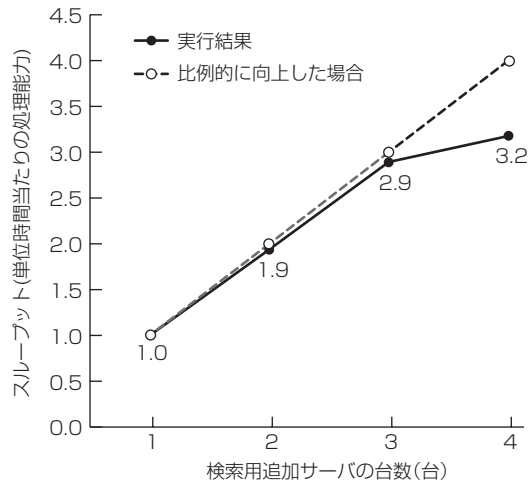


図4．検索サーバ追加時の性能比較(検索サーバ1台の処理時間を1とした場合)

(5) 考察

評価の結果，検索用追加サーバ3台まではサーバ台数に比例しておおむね期待どおりのスループットが得られた。しかし，サーバ台数4台からスループットが向上しない傾向を示している。この主な原因は，1か所の共有ストレージに対して，ステージング用サーバ，及び，複数の検索用追加サーバから同時にアクセスされる仕組みにあると考えられる。検索内容によっては，共有ストレージから大量のデータが検索用サーバに転送されるため，ネットワーク負荷が上がるとともに，複数サーバから集中的に要求を受けた共有ストレージのI／O(Input／Output)処理性能の限界によって，スループットが低下したと推測される。これらの問題を解決するためには，十分なネットワーク帯域の確保とI／O処理性能の高いストレージを採用する必要がある。

4. 各構成の比較

従来の検索サーバ追加機能の構成とデータ共有型構成について，各構成の特徴を比較する(**表1**)。

利用者数の増加に関する拡張性については，従来構成の検索サーバ追加機能は，検索サーバをより高性能のものに置き換える方法のみで拡張に対応しているため，スループットの向上に限界がある。一方，データ共有型構成はスケールアウト方式による拡張が可能であるため，サーバ台数に応じてスループットが向上する。

表1．各構成の特徴の比較

構成	利用者数の増加に関する拡張性	ストレージ故障時のシステムの連続稼働に関する可用性
従来構成	× スループットの向上に限界がある	○ すぐに縮退運転が可能となる
データ共有型構成	○ サーバ台数に応じてスループットが向上する	× すぐにシステムを復旧できない

一方，ストレージ故障時のシステムの連続稼働に関する可用性に関しては，従来構成の検索サーバ追加機能は，全てのデータを各サーバに配置して管理しているため，すぐに縮退運転が可能である。これに対して，データ共有型構成は，表データを共有ストレージ上に配置して全てのサーバで共有する仕組みであるため，単一障害点(共有ストレージ)が存在する。そのため，共有ストレージが，万一障害等で停止した場合，復旧までシステムは稼働できない。

これらのことから，検索サーバ追加機能を適切に使い分けることが望ましい。

5. むすび

複数台のサーバを追加することによってスケールアウトを容易に実現する“検索サーバ追加機能(データ共有型構成)”の機能と特長などについて述べた。この構成では，利用者数増加に応じて検索用追加サーバを増設することによって，全体のスループットを向上させることが可能である。

今後は，故障したサーバの縮退などを容易に実現する手段，及び，ステージング用サーバと複数台の検索用追加サーバを一元的に管理する手段の実現を検討していく。

参考文献

(1) 小出健太：情報セキュリティを支えるデータ分析フレームワーク“AnalyticMart”，三菱電機技報，**87**，No. 7，405～408（2013）
(2) 山岸義徳，ほか：高速集計検索エンジンとセンサデータベースへの応用，三菱電機技報，**83**，No.12，709～712（2009）
(3) 郡　光則：データウェアハウス向け高性能データ圧縮方式，情報処理学会論文誌，**47**，No. SIG13，58～73（2006）

特集論文

マルチテナント利用を実現する大規模データ分析共用基盤の構築

井ノ口裕也* 渡邊健太*
三屋誓志郎* 埋金進一**
福島愼一*

Construction of Large-scale Data Analysis Base to Realize Multi-tenant Use

Yuuya Inokuchi, Seishiro Mitsuya, Shinichi Fukushima, Kenta Watanabe, Shinichi Umegane

要　旨

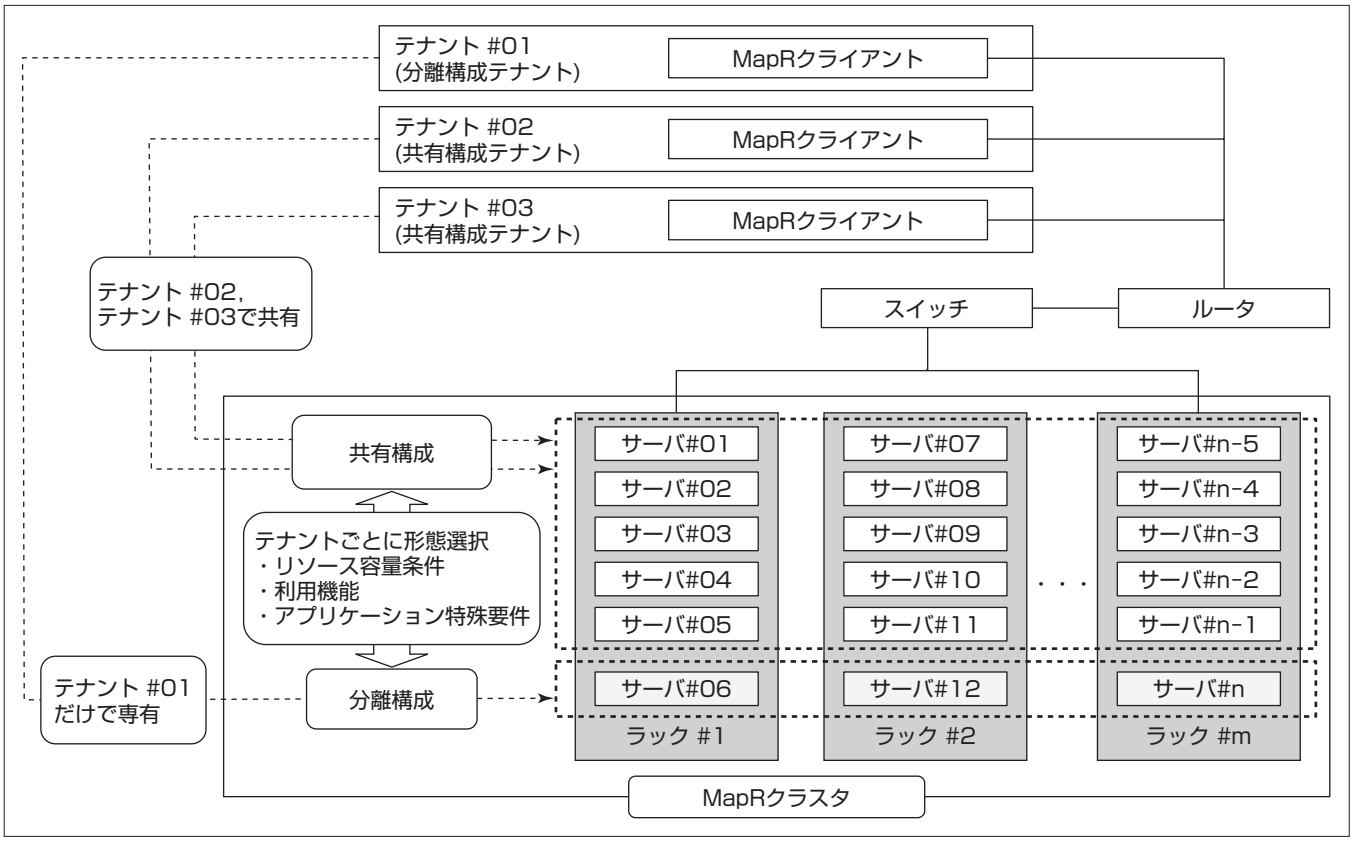
近年，コンピュータシステムが扱うデータ量は増加の一途をたどっており，膨大なデータを活用し，新たな価値を生み出すことが脚光を浴びてきている。

これらのデータを扱う手段の１つとしてJ. Dean等の論文[1]をベースにオープンソフトウェア（Open Source Software：OSS）として実装されたHadoop[注1]がある。Hadoopは複数マシンでの分散処理を実現でき，従来のデータベース，データウェアハウスでは取り扱うことができなかったデータ量を扱うことができる。さらに，分析の用途が増加するにつれ，Hadoopクラスタを共用するニーズが発生したが，既存のHadoopディストリビューション（Hadoop本体と利用に必要なアプリケーション等をまとめたもの）では用途ごとのリソース管理に幾つかの課題があった。

三菱電機インフォメーションシステムズ㈱（MDIS）と㈱ノーチラス・テクノロジーズは，高速化や高信頼性に加えてマルチテナント運用向け機能を持つHadoopディストリビューションであるMapR[注2][2]を用いて複数用途を共存させるマルチテナント利用を実現する大規模データ分析共用基盤の構築に取り組んだ。

専有サーバを割り当てる構成（分離構成），又はマルチテナントで共有する構成（共有構成）かを選択可能とするなど，テナント要件に沿って柔軟な構成を実現している。また，ログ運用，アプリケーションの制限ルールの設定，クラスタ拡張のための情報収集などの運用方針を整理した。MDISでは，この実績を基に，2015年６月から“MapRクラスタ構築サービス”の提供を開始している。

（注１） Hadoopは，The Apache Software Foundationの登録商標である。
（注２） MapRは，MapR Technologiesの登録商標である。



マルチテナント対応大規模データ分析共用基盤

大規模データ分析基盤をマルチテナント対応として構築したシステム構成図である。テナントごとにクラスタの一部を占有又はマルチテナントによるリソース共有といった，テナントの要件に沿った柔軟な構成をとることが可能なシステムとなっている。

*三菱電機インフォメーションシステムズ㈱
**㈱ノーチラス・テクノロジーズ

1. まえがき

近年，コンピュータシステムが扱うデータ量は増加の一途をたどっている。今までは処理しきれずに捨てていたデータを活用し，新たな価値を生み出すことが，ビッグデータの取組みとして脚光を浴びてきている。その基盤として複数マシンでの分散処理を実現するHadoopの構築を行う企業が増加している。

サーバ数が数十台，データ量が数百TB(TeraByte)の大規模データ分析基盤構築に際して，企業内の複数の部門が共用すること(マルチテナント運用)によるコスト削減やリソースの有効活用が求められるが，既存のHadoopディストリビューションでは複数アプリケーション間のリソースの競合を抑制する機能や，利用部門(テナント)ごとのディスク使用量を制限する機能が不足しており，マルチテナント運用を行うことが困難であった。

この問題を解決するため，MDISでは既存Hadoopと完全互換で，マルチテナント運用向け機能(以下“マルチテナント機能”という。)を持つHadoopディストリビューションであるMapRを用いてマルチテナント利用を実現する大規模データ分析共用基盤を構築した。

本稿では，従来のHadoopディストリビューションでの課題について述べ，その課題を解決するために実現すべきマルチテナント機能を定義した上で，その実現に向けたマルチテナント機能設計のポイントを述べる。さらに，運用上の留意事項についても述べる。

2. 従来の大規模データ分析基盤の課題

既存のHadoopディストリビューションでは，次に挙げる4つの課題があり，複数部門で大規模データ分析基盤を共用するマルチテナント運用を行うことが難しい状況にあった。

(1) テナントごとのディスク使用量制限機能の欠如

テナントごとのディスク使用量を制限できず，特定テナントによる大量データ利用が他テナントに影響を及ぼす可能性がある。

(2) テナント間でのリソースの競合による処理の遅延

クラスタを構成する全てのサーバに分散してデータを蓄積し，全てのサーバで処理を実行する構成のみの実装となっている。この方式は，全サーバのリソースを有効に活用できる点では有利であるが，複数処理の同時実行によってリソースの競合が発生する可能性があり処理時間の見積りが難しい。確実に規定時間内に処理を完了させるためには，リソースの競合が発生しないようにテナント間で利用サーバを分離する必要があるが，既存のHadoopディストリビューションでは，利用サーバを分離するために複数のHadoopクラスタを構築する必要があった。

(3) 耐障害性の不足

多くのテナントでの利用を展開するには，極力システム停止を伴わない運用が必要であり，耐障害性の向上は必須である。既存のHadoopディストリビューションの標準構成では単一障害点が存在するため，Hadoopディストリビューション以外のミドルウェアなどを利用して，独自に多重化構成を構築する必要があった。

(4) Hadoop固有APIのみの提供

既存のHadoopディストリビューションでは大規模データを扱うAPI(Application Programming Interface)としてHDFS(Hadoop Distributed File System)(注3)インタフェースしか提供されず，データアクセスの処理を新たに作りこむ必要があった。

(注3) Hadoopが利用している分散ファイルシステムである。OS(Operating System)のファイルシステムを代替するものではなく，その上に独自のファイル管理システムを構築するもので，アプリケーションからローカルファイルと同様のインタフェースでアクセスすることはできない。

3. 目標とするマルチテナント機能拡張要件

Hadoopの商用ディストリビューションであるMapRは，高速化や高信頼性に加えてマルチテナント機能を持っていることを特長としている(2)。MapRを用いて，次に挙げる3つのマルチテナント機能拡張要件を満たすことを目標として，従来の課題を解決することに取り組んだ。

(1) マルチテナントに対して，テナントごとにデータ管理機能を持たせて，かつ利用サーバを分離できるHadoopシステムを提供する。

(2) マルチテナント機能を，単一クラスタ上に構築する。

(3) データアクセスの分離とテナント間のリソースの利用をMapR及びLinux(注4)の標準機能で構築する。

(注4) Linuxは，Linus Torvalds氏の登録商標である。

4. マルチテナント機能設計のポイント

4.1 前提条件の設定

まずはマルチテナント機能を利用する範囲や利用するユーザーを定義した。システム設計・運用設計で要件の発散を排除するために重要なプロセスであるため，設計の初期段階で検討を行った。

(1) マルチテナント機能を利用する範囲の設定

今回構築したシステムは，社内利用であり，部門やプロジェクトごとに1テナントずつを割り当てる想定で設計した。社内ネットワークで接続され，ユーザーは提示されたルールを守ることを前提としたため，ルール無視のユーザーの誤使用を排除する対策等は実施していない。

(2) マルチテナント運用関係者の役割の明確化

マルチテナント運用関係者の役割(ロール)とそれぞれが利用できる機能を定義した。

具体的には設定ファイルの変更やリソースの払出しが可

能なインフラ担当者，クラスタの通常運用を行うMapR運用者，テナント側の接続環境を構築するテナントインフラ担当者，ファイルI／O(Input／Output)やアプリケーション実行が可能なテナント利用者である。

4.2　マルチテナント機能の実現方式

2章で述べた課題(1)～(4)を解決するために採用したマルチテナント機能実現のための具体的な方式を次に述べる。

4.2.1　テナントごとのデータアクセス制限の設定

テナントごとに利用可能なディレクトリを割り付け，アクセス権を適切に設定することによってテナント間のデータアクセスを分離した。既存のHadoopディストリビュージョンでもこのデータアクセスの分離までは実現可能であるが，クラスタ全体のストレージを1つのファイルシステムとして扱っているため，テナントごとのデータ使用量を制限することはできなかった。MapRでは“ボリューム”という概念でファイルシステムを分割管理しており，ボリュームごとにディスク使用量の上限値を設定できる[(2)]。これによって，ボリュームをテナントごとのディレクトリに割り付けることでテナントごとのデータ使用量を制限することを可能とした。また，MapRでは，ボリュームごとにスナップショットを生成する機能を持っており[(2)]，ユーザーがデータ処理で誤操作をした場合の復旧手段としてテナントごとにこの機能を提供することとした。

4.2.2　テナント間の利用サーバの分離

従来のHadoopでは，各テナントの利用サーバを分離するためには複数のクラスタに分割した構成にする必要があった。次に示すように，MapRの持つ機能を適切に組み合わせて活用することによって，単一のクラスタ構成で利用サーバ間の分離を柔軟に行うことを可能とした。

(1)　分離構成と共有構成の定義

今回構築したクラスタでは，リソースを割り当てる構成として次の2種類の構成を定義した。

①分離構成

1つのテナントに対して専有サーバを割り当てる構成である。他テナントとのリソース競合を回避できる構成であり，応答性能の要件が高い場合に選択する。

②共有構成

マルチテナントでサーバを共有する構成である。リソースを効果的に活用できるが，競合によって性能面の保証ができなくなる。応答性能の要件が高くない場合に選択する。

テナントごとにこれらを選択でき，かつ共存できるよう設計した。利用するアプリケーションの要件に応じてどちらを選択するかを決定する。

分離構成と共有構成の比較を**表1**に示し，それぞれのイメージを**図1**に示す。

(2)　分離構成の実現方式

分離構成を実現するには，テナント間で，データの分離と処理の分離を実現する必要がある。構築したシステムでは，MapRの“ボリュームトポロジー”機能と“ラベル”機能[(2)]を組み合わせることによって，分離構成を実現している。

表1．分離構成と共有構成の比較

項目	分離構成	共有構成
他テナントへの影響	ほとんどない	性能，容量面で影響がある
小規模なリソースの割当て	最低でも3台分のサーバリソースを割り当てる必要がある。小規模なリソース割り当ては不可	小規模なリソースを割当て可能
テナント追加	専有サーバを確保する必要があり，共有構成と比べて工数と時間が大きくかかる	既存リソースに余裕があれば，分離構成と比べて容易
クラスタ構成	1クラスタ(注5)	1クラスタ

(注5)　既存のHadoopで分離構成相当の機能を実現するには，テナント間のリソース競合を回避するためにテナントごとに別々のクラスタを構築する必要があった。この設計では1クラスタ構成でテナント間のリソース競合を回避できるため，既存のHadoopに比べコスト削減となる。

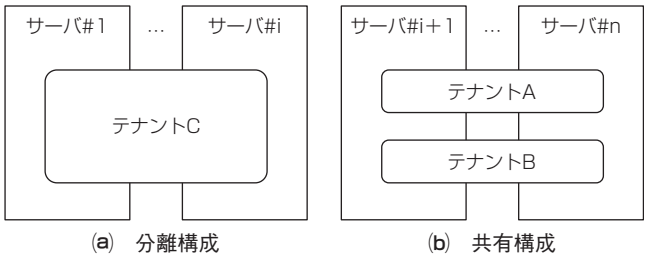


図1．分離構成と共有構成

①データの分離

“ボリュームトポロジー”機能を用いてデータの分離を行った。ボリュームトポロジーは，ボリュームのデータをどのサーバに格納するかを設定する機能である。各テナントのデータの保存位置を分離したサーバ内に限定することで，ディスクI／O，ネットワークI／Oの競合による性能劣化を防止する。

②処理の分離

“ラベル”機能を用いて処理の分離を行った。ラベルは，アプリケーションを実行するサーバをグループ化する機能である。テナントごとに，アプリケーションを実行するサーバを特定ラベルを付けたサーバに限定することでCPU(Central Processing Unit)，メモリの競合による性能劣化を防止する。

ボリュームトポロジーとラベルによるデータ・処理分離イメージを**図2**に示す。

先に述べたように，この設計での分離構成では，MapRの設定を変えることによってクラスタ内の物理的なサーバ台数を変化させずに，テナントが利用するサーバ台数を変化させることができる。この妥当性を確認するために，分離構成の設定によって利用可能サーバの台数を変化させた場合と，物理的にクラスタ内の接続サーバ台数を変化させた場合での

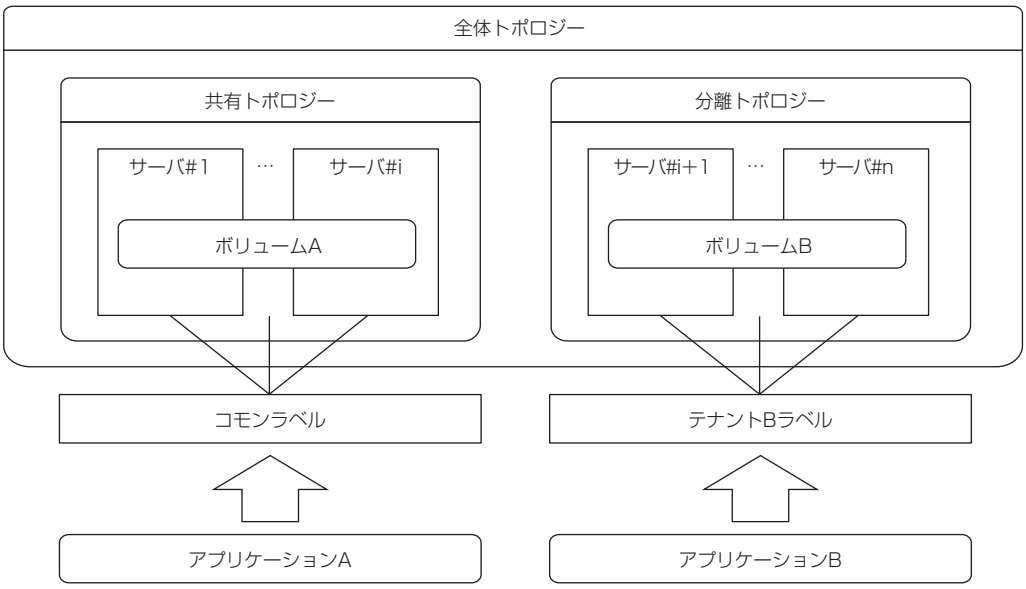


図2．ボリュームトポロジーとラベルによるデータ・処理分離

ベンチマークテストプログラムの応答性能の比較を行った。その結果，両者でほぼ同等の結果を得ることができ，分離構成によって有効にリソース分離ができていると考えられる。

4.2.3　耐障害性の向上

マルチテナントに対して安定した運用を提供するために，三重化冗長構成として二重までの障害に耐えうる構成としている。2台以下のサーバ，2台以下のハードディスク，2つ以下の管理サービスの同時障害が発生してもシステム停止が起こらないように設計した。これは，ファイルのレプリカ数(多重度)を“3”にすること，各管理サービスを三重化構成にすることによって実現している。前者は既存のHadoopから持つ機能，後者はMapRが提供する機能である[2]。また，管理サービスの配置設計では，各管理サービスを別ラックのサーバに分散させて1ラック全体障害発生時のシステム停止を回避するために，分離構成を構築するサーバでは管理サービスを動作させない構成として，分離構成利用テナントと共有構成利用テナント間で管理サービスに伴う影響を最低限にする等の構築上の工夫を行っている。

4.2.4　APIの拡張

この実現方式では，ファイルシステムに対し，従来のHDFSインタフェースに加えてNFS(Network File System)(注6)で接続する機能を提供している[2]。UNIX(注7)ファイルシステムと同様の操作でデータ入出力することができ，多くの既存アプリケーションをそのまま利用することが可能である。

NFSの構築では，HDFSインタフェースと同様にアクセス権を設定してテナント間のアクセス権の分離を実現している。また，NFSゲートウェイサービスを行うサーバをテナントごとに分散して割り付け，それぞれのマウントポイントに接続可能なクライアントマシンを制限することで負荷分散とセキュリティ向上を実現する設計とした。

(注6)　主にUNIX系OSで利用される分散ファイルシステムとそのプロトコルである。サーバのストレージをネットワーク経由でマウントすることによってローカルファイルと同様にアクセスすることができる。
(注7)　UNIXは，The Open Groupの登録商標である。

5.　マルチテナント運用上の注意点と対応策

5.1　ログの運用

各テナントのアプリケーション実行における障害発生時等の問題の解析・解決のためにテナントへログを提供する。ログ提供でもテナント間のアクセス権の分離が必要であるが，テナント間のアクセス権の分離ができないログもあり，ログの種類によって次の運用とした。

(1)　OSのログ，MapRデーモンのログ

テナントごとの分離が不可能なため，テナントにはそれらのログは公開せず，テナントの要請によってシステム管理者側でログ内容を確認する運用とした。

(2)　アプリケーション実行時のログ

他テナントがログをアクセスできないようにアクセス権を設定した上で各テナントから参照可能とした。なお，ログはクラスタ内で散在しており参照処理が煩雑であるため，MapRの持つ集中ロギング機能[2]を活用して，テナントへの便宜を図っている。

5.2　テナント運用形態の選択

新たにテナントを追加する際，テナント間のリソースの分離を適切に実現するために，分離構成とするか，共有構成とするかを決める必要がある。

追加テナントに対して，リソース容量条件，利用する機能，アプリケーションの特殊要件等のヒアリング項目を明確にし，どちらの利用形態が適しているかを判別できるようにした。基本的には他テナントへの，又は他テナントか

らの影響度によって判断する。

5.3 共有構成における運用方針

(1) クラスタのチューニング方針

共有構成ではどのようなアプリケーションが動作するかの予測が不可能であるため，パラメータは最も汎用性があるデフォルト値を採用した。なお，個別チューニングによる応答性能の向上が必要なテナントについては分離構成を選択することでパラメータのチューニングを可能としている。

(2) アプリケーションの制限ルールの設定

共有構成では，サーバのリソースを有効に利用できるメリットはあるが，サーバを共有するテナント間でのリソースの競合が発生する可能性が高くなる。通常は，Hadoopの機能でリソース利用はテナント間で適切に制御されるが，アプリケーションの利用方法によってはHadoopでは制御しきれないケースがある。そのため，他テナントに影響を与えないようにするアプリケーションの制限ルールを定めた。具体的には，Linux上の別アプリケーションを起動する場合の使い方の制限，一時ファイル等の出力先としてのLinuxローカルのファイルシステムの利用禁止等である。

5.4 アラートの監視

MapRでは問題を検知した際にアラートを発生させるが，そのアラートが特定テナントにのみ影響があるのか，又はクラスタ全体に影響があるのかを判別することが難しい。

発生する可能性のあるアラートをリスト化し，運用時に影響範囲を判断できるようにガイドを作成した。

5.5 クラスタの拡張方針の策定

マルチテナント運用を継続するには，運用中のテナントの処理量・データ量の増加や新規テナントの追加に備えてクラスタの拡張を検討する必要がある。拡張検討のために，日々の運用で，監視対象とするリソースと拡張基準を策定した。

主な監視対象は次の5点であり，定期的に監視することとした。なお，これらが拡張基準となるしきい値を超えた際には，クラスタの拡張を検討することとしている。

(1) CPU利用率(サーバごと)
(2) メモリ利用率(サーバごと)
(3) ディスクI／O(サーバごと)
(4) ネットワークI／O(サーバごと)
(5) ファイルシステム利用率
(全体，サーバ，ボリュームごと)

6. むすび

今回，MapRを利用して，データ用ディスク容量が数百TB規模のマルチテナント向け大規模データ分析共用基盤を設計・構築することができた。これまでは，この規模のシステムを単一テナントでしか利用できなかったが，このマルチテナント向け共用基盤を用い，ログの分析システムとIoT(Internet of Things)関連データ処理システムの2つの大容量データ処理テナントを同一プラットフォームで稼働させる運用を2015年4月から開始している。また，このノウハウを活用して2015年6月から“MapRクラスタ構築サービス”を開始している。

今後，今回開発した大規模データ分析共用基盤の技術をベースとして様々な適用分野を探っていくとともに，データ分析のためのアプリケーションの拡充を図っていく予定である。

参考文献

(1) Dean, J., et al.：MapReduce：Simplified Data Processing on Large Clusters, Proc. of Operating System Design and Implementation(OSDI), 137～150 (2004)
http://static.googleusercontent.com/media/research.google.com/ja//archive/mapreduce-osdi04.pdf
(2) MapR公式ドキュメント
http://doc.mapr.com/display/MapR3/Home

特集論文

大規模データ分散処理技術を活用したバッチ高速化ソリューション

中島賢弘* 佐藤彰洋*
武石富士見*
佐藤啓紀*

Batch Speeding−up Solution by Distributed Processing Technologies

Takahiro Nakajima, Fujimi Takeishi, Hiroki Satou, Akihiro Satou

要　旨

バッチ処理は，多くの企業の基幹業務システムで現在でも重要な役割を担い，取り扱うデータ量は増え続けている。データ量増加に伴いバッチ処理時間は増大し，処理時間の短縮は企業が抱える重要な課題の１つとなっている。

三菱電機インフォメーションシステムズ㈱(MDIS)では，大規模データの分散処理を支えるフレームワークであるHadoop(注1)技術に着目し，この課題を解決するための“バッチ高速化ソリューション”を立ち上げた。

このソリューションのサービス構成は次のとおりである。

⑴　高速化診断サービス

現行バッチ処理のボトルネック箇所を診断し，このソリューション適用による改善効果を提示する。

⑵　高速化設計・構築サービス

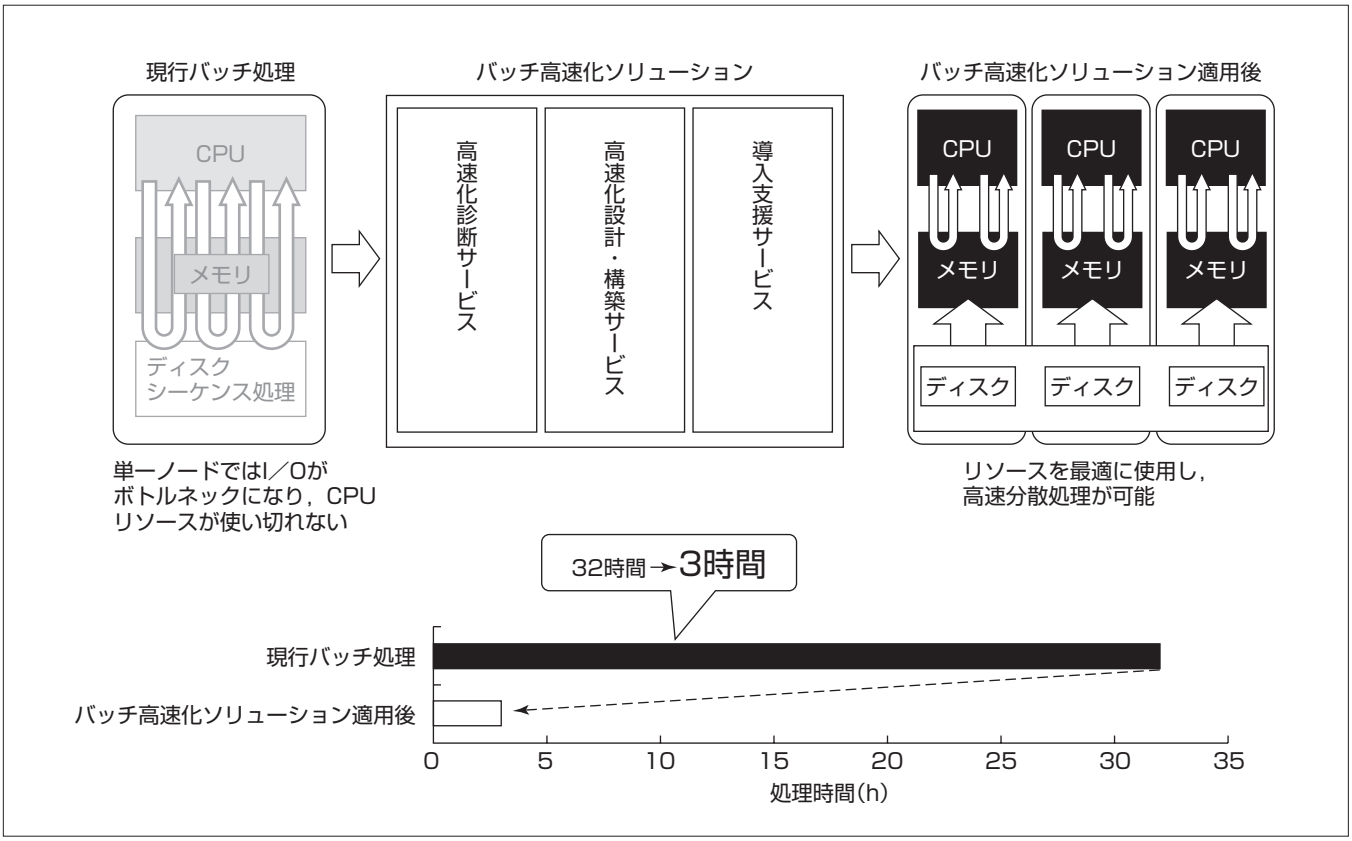
診断結果を基に現行バッチ処理を詳細分析し，高速化処理設計と高速化モジュール構築を行う。

⑶　導入支援サービス

高速処理環境の構築と稼働までの支援を行う。

このソリューションを，年次バッチ処理の時間短縮が長年の課題であった顧客システムに適用し，ディスク，CPU(Central Processing Unit)，メモリなどのリソース全体の効率化，及び分散処理化などを行うことで，現行32時間掛かっていた処理を３時間に短縮し，約1/10の大幅な性能改善を達成した。

（注１）　Hadoopは，The Apache Software Foundationの登録商標である。



バッチ高速化ソリューションと適用事例

ディスクI／O（Input／Output）ネックが原因で処理時間に課題を抱えているバッチ処理に対し，バッチ高速化ソリューションを適用することで，ディスク，CPU，メモリなどのリソース全体の効率化及び処理の分散化によって処理時間短縮を実現した。顧客システムへ適用した事例では，32時間の処理を3時間に短縮することができた。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

バッチ処理の多くは，長年にわたり企業の基幹業務システムを支えている。業務を支援するシステム化範囲の拡大や扱うデータ量の増加に伴い処理時間が増大し，夜間日次バッチ処理がオンラインサービス開始時間までに終わらない等，企業にとって大きな課題となっている。

MDISではこの課題を解決するために，近年大規模データの分散処理を支えるソフトウェアフレームワークとして注目され，企業への導入が進むHadoop技術に着目し“バッチ高速化ソリューション”を立ち上げた。

本稿では，このソリューションの概要，バッチ処理に課題を抱える顧客システムへの適用事例と適用ポイント，及び適用後の効果について述べる。

2. バッチ高速化ソリューションの概要

このソリューションでは，①高速化診断サービス，②高速化設計・構築サービス，③導入支援サービスを提供している。処理性能に問題がある現行バッチ処理に対し，このソリューションを適用することで，顧客に手間をかけることなくバッチ処理の高速化を実現する。

2.1 高速化診断サービス

高速化診断サービスでは，このソリューション適用による改善効果を次の2段階で提示する。

2.1.1 簡易診断サービス

対象データ量，処理概要から簡易的な改善効果有無を無償で診断する。

2.1.2 詳細診断サービス

対象データ量，処理概要，現行処理時間，現行リソース(設計書やプログラムソースなど)の情報を基に詳細診断を行う。対象バッチ処理のボトルネック箇所の解析を行い，このソリューション独自の“見込み処理時間計算式”で高速化後の見込み処理時間を算出し，改善効果を提示する。なお，改善効果については，ハードウェア構成パターン(サーバスペック，ノード数)別に導入に必要なハードウェア概算費用も併せて提示する。

2.2 高速化設計・構築サービス

高速化設計・構築サービスは，高速化診断サービスでインプットにした情報を基に，処理対象データの流れに着目した高速化設計と高速化モジュール構築を行うサービスである。

高速化モジュールを構成するソースコードの一部は，高速化設計書から自動生成可能である。また，現行資産を活用した構築を実現しているため，仕様検討など顧客に手間をかける時間を，通常の新規構築の場合と比較して大幅に削減することができる。

2.3 導入支援サービス

導入支援サービスでは，Hadoop環境の構築，高速化設計・構築サービスで開発したモジュールの導入，稼働までの支援を行う。

3. バッチ高速化事例と適用ポイント

このソリューションを適用した顧客では，年度始めに処理時間の長い年次バッチ処理を実施するため，土日(休日)から月曜日(営業日)にまたがって基幹業務システムのオンラインサービスを停止しなければならず，通常業務に支障をきたしていた。

このソリューションの適用によって，年次バッチ処理(全体40時間処理)のうち，特に時間がかかっていた32時間のバッチ処理を3時間に短縮することができた。

次に，顧客に対し提供した高速化診断サービス(詳細診断サービス)，高速化設計・構築サービスの具体的な内容，適用に当たって工夫したポイント，及び高速化後の性能の結果について述べる。

3.1 高速化診断事例と適用ポイント

3.1.1 高速化処理対象選定

ボトルネック箇所の高速化が可能かどうかを見極めるため，次に述べる2段階のアプローチによって高速化すべき対象を絞り込んだ。

1段階目：各処理の処理時間測定による高速化候補の選定

2段階目：高速化候補と高速化しない現行処理間の結合度調査

1段階目で各処理の処理時間の測定結果に基づき，処理時間がかかるものから高速化処理対象の候補とした。Hadoop環境上でバッチ処理を実施する場合，現行環境(データベースサーバ)とHadoopサーバ間のデータ転送時間がオーバーヘッドとなる。そのため，現行処理時間が短い処理は，このオーバーヘッド時間を考慮すると高速化の効果が見込めない可能性が高いので高速化対象としない。

このソリューションでは高速化効果が見込まれるしきい値(処理時間)を設定しており，しきい値による分類で年次バッチ処理の全250処理中25処理を高速化対象候補とした。この25処理の合計処理時間は，全処理時間40時間中32時間(約82%)を占めており，有効な高速化候補であることが分かる。

次に2段階目では，高速化候補の25処理と高速化対象外の225処理の結合度を調査した。結合度とは，処理間の依存関係を示す度合いであり，例えば処理Aの結果が処理Bの処理内容に影響を及ぼす場合は結合度が高いと言える。結合度を調査した理由は，高速化処理環境と現行処理環境は異なる環境での処理であり，処理間の結合度が高い場合には，高速化による効果が期待できないためである。

調査した結果，高速化候補の25処理と高速化対象外の225処理で，結合度は低いことが判明したため，25処理を高速化対象として確定した。この適用例では，結合度が高

い高速化対象はなかったが，顧客のバッチ処理の全体像を把握した上で，単純に時間のかかる処理を選定するのではなく，現行処理との結合度を見極めた上で対象を選定することが重要である。

3.1.2 高速化後性能の見極め

選定した25処理に対し，このソリューション独自の“見込み処理時間計算式(注2)”を用いて，バッチ処理高速化後の見込み処理時間を算出した。その結果，25処理の見込み処理時間は高速化前の32時間に対して高速化後は5.6時間との結果になり，適用によって処理時間に相当の短縮が見込めると判断した(**図1**)。

(注2) このソリューション立ち上げに当たり，バッチ高速化のプロトタイプを作成し，インプットデータ量，処理内容を基に複数パターンについて検証して処理時間を実測した。実測結果から基礎数値(データ量単位の処理時間)を求め，計算式を策定している。

3.2 高速化設計・構築事例と適用ポイント

高速化バッチモジュールの処理は，現行バッチ処理が直接データベースに処理を実施する(**図2**(a))のに対し，**図2**(b)に示すとおり①データ抽出処理(データベース→Hadoop(HDFS(Hadoop Distributed File System)))，②変換処理(Hadoop処理)，③データ反映処理(Hadoop(HDFS)→データベース)の3ステップ処理となる。

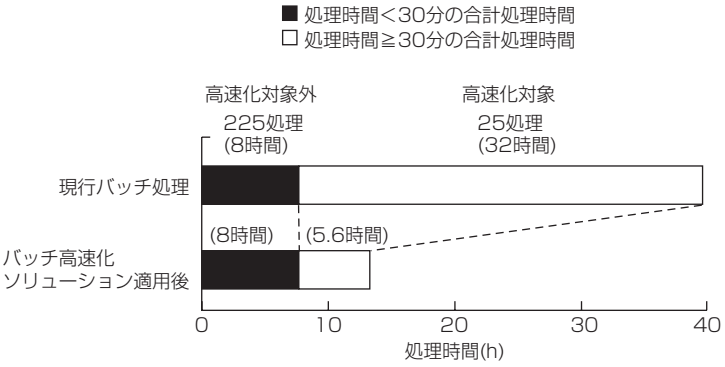


図1．バッチ処理時間の比較

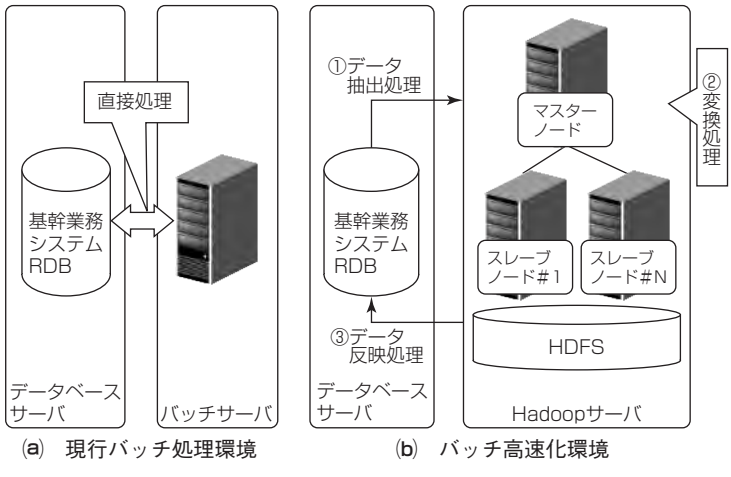


図2．バッチ高速化構成イメージ

次に，これら3つの構築ポイントについて述べる。

3.2.1 データ抽出処理とデータ反映処理の最適化

先に述べたとおり，データ抽出処理とデータ反映処理は，Hadoop環境で処理する場合にはオーバーヘッド時間となる。特にデータ反映処理は既存のデータベースサーバ環境の書き込み性能に大きく依存する。このソリューションでは，このオーバーヘッド時間を最小化する①データベースサーバとHadoopサーバ間の転送量削減，②抽出・反映方式の最適化の2つの工夫を行っている。

①の転送量削減については，処理対象テーブルの中に処理に必要な項目と不要な項目があることに着目し，抽出・反映に必要な項目のみを対象とすることで実現している。

②の抽出・反映方式の最適化については，幾つかの方式を数種類のデータパターンごとに実測し，最適な抽出・反映方式を選定することで実現している。

抽出方式は，方式1：sqoop(注3)，方式2：SQL(Structured Query Language)*Plus(注4)，方式3：WindGate(注5)を候補として，各方式による抽出時間を測定し，どのデータパターンでも最速であった方式1を今回の事例では採用した。

一方，反映方式は，方式1：sqoop，方式2：PL(Procedural Language)/SQL(注6)，方式3：SQL*Loader(注7)を候補として，反映時間を測定し最適手法を選定した。反映方式の場合は，処理対象テーブルの全件数に対する更新件数の比率によって最適手法は異なり，この更新件数比率をしきい値として，手法を選定している。更新件数がしきい値未満の場合は方式2が最速であり，しきい値以上の場合は方式3が最速である。このソリューションの反映方式ではデータ特性によって方式を切り分けて対応している。今回の事例では更新件数の割合がしきい値未満であったため，方式2を採用している。

さらに，抽出・反映処理については構築時の生産性向上をねらい，高速化設計書を読み取って処理を実行するソースコードを自動生成する機能を実現している。

(注3) データベースとHadoopの間でデータ転送を行うためのコマンドラインインタフェースアプリケーションである。
(注4) Oracle社によるデータベース操作のためのユーティリティである。
(注5) ノーチラス・テクノロジーズ社が開発したデータベースと連携するコンポーネントである。
(注6) Oracle社がデータベース言語SQLを独自に拡張したプログラミング言語である。
(注7) 外部ファイルのデータをOracle Databaseの表に取り込むユーティリティである。

3.2.2 変換処理の実現方式について

変換処理の高速化バッチモジュール構築には，ノーチラス・テクノロジーズ社が提供するOSS(Open Source Software)“Asakusa Framework(注8)(注9)(以下“AsakusaFW”という。)”を活用している。高速

化モジュールを構築する場合，分散処理を意識したプログラミングが必要となるが，AsakusaFWは分散処理を意識することなくプログラミングが可能であり，高速化モジュールを自動生成することができる。ただし，AsakusaFWによるプログラムは現行のバッチプログラムと構造やコーディング方法が大きく異なるため，現行のバッチプログラムを単純に機械変換して作成できるわけではない。そのため，このソリューションでは，**図3**に示すとおり，開発プロセスの中で次の3つの手段によって，バッチ処理高速化環境構築をする際の顧客への負担を少なくした。

⑴　現行バッチ処理内容の解析作業の効率化

このソリューションでは，独自の解析シートを用いて現行のバッチプログラムを解析する。解析シートは，高速化設計移行時に，現行のバッチプログラムの業務仕様を漏れなく移行すること，及び業務仕様に関係がない処理は排除することを目的として，必要な処理と不要な処理の分別の指標を示している。例えば，必要な処理はSQLなどのデータを加工する処理であり，不要な処理は変数に値を格納するような処理である。この解析シートを用いることで解析作業の効率化を図っている。解析作業はこのように既存リソースを主体としているため，顧客から現行仕様をヒアリングする必要がなく顧客の負担，変換コストを削減している。

解析結果は，“現行バッチ処理データフロー図”“プロセス処理内容”となる。

⑵　データフロー図を用いた高速化設計

AsakusaFWではデータフロー制御，データ操作，データ結合など処理特性に合わせた“演算子”が用意されており，演算子を組み合わせることでバッチ処理を構築する。

このソリューションでは，⑴のアウトプットの“現行バッチ処理データフロー図”“プロセス処理内容”をインプットとして，演算子を最適に組み合わせることで“高速化バッチ処理データフロー”を作成する。**図4**に現行バッチ処理のデータフロー図と高速化バッチ処理データフロー図の作成イメージを示す。移行設計後(**図4**の右側)は，データベースの内容はデータモデルに格納して取り扱い，業務処理はAsakusaFWの演算子に置き換えを実現する設計としている。また，各演算子に具体的な処理内容を定義し，現行処理内容の高速化設計を行う。設計には高速化設計書を用意しており，AsakusaFWのプログラム構造に準拠した定形フォーマットとなっている。

⑶　ソースコードの一部自動生成による構築作業の効率化

高速化モジュールのソースコードについては，高速化設計書から一部自動生成可能であり，開発コストを抑える工夫をしている。高速化設計書は先に述べたとおり，AsakusaFWの構成に準拠した構成となっているため，効率的な構築を可能にしている。

(注8)　Asakusa Frameworkは，Hadoop上で大規模な基幹バッチ処理を行うためのフレームワークである。
(注9)　Asakusa Frameworkは，㈱ノーチラス・テクノロジーズの登録商標である。

3.2.3　ジョブ構成の最適化

バッチ高速化ジョブは，**3.2節**で述べたとおり①データ抽出処理，②変換処理，③データ反映処理の3ステップの処理で成り立つ。ジョブ構成は**図5**のように段階的に各処理を実行することでデータベースサーバ，又はHadoopサーバに負荷が集中しないように工夫している。

3.3　高速化後の性能の結果について

3.1.2項で述べたとおり，高速化診断サービス段階では現行32時間の処理は5.6時間に削減可能であると見込んでいた。

これに対して，実際にはさらに，**3.2.1項**で述べた抽出・反映処理の転送量の削減，**3.2.3項**で述べたジョブ構

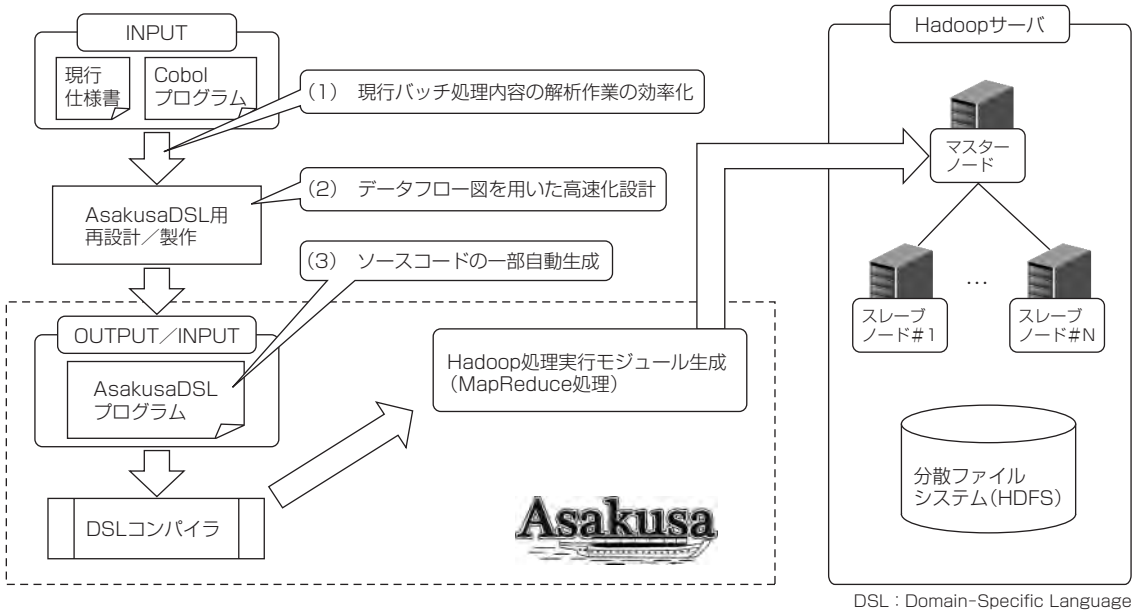
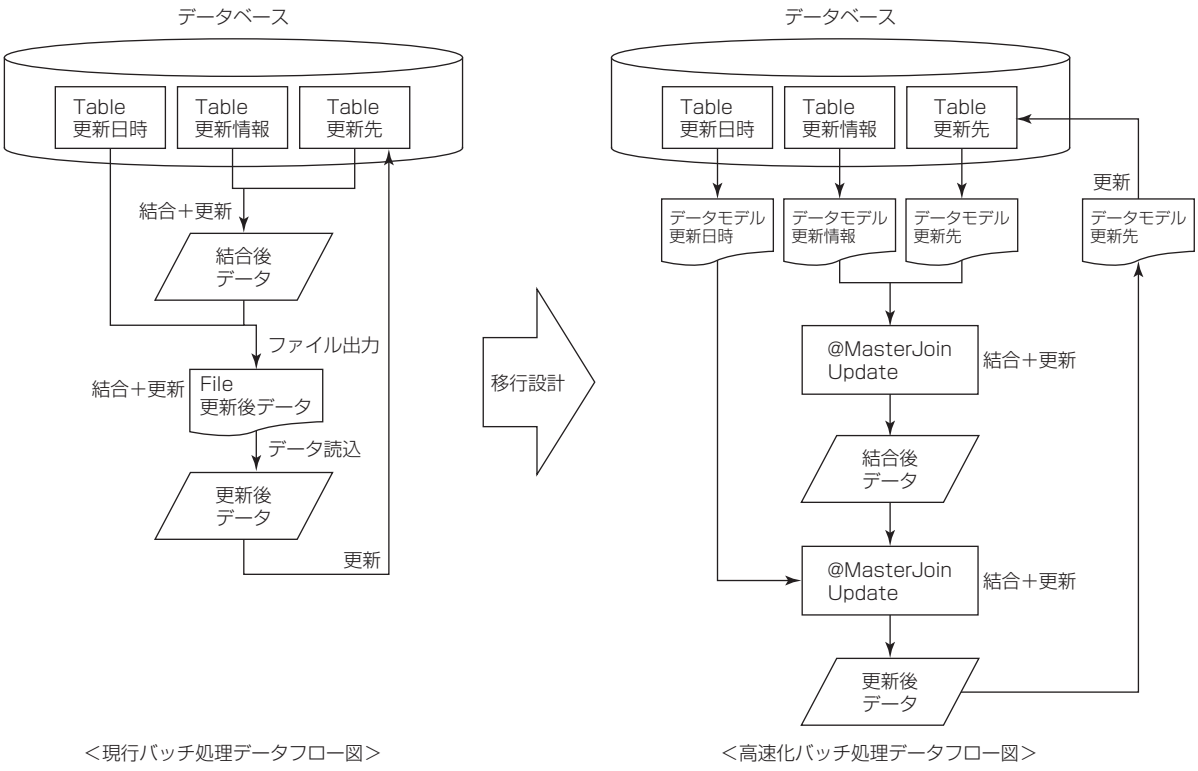


図3．変換処理の実現方式



＜現行バッチ処理データフロー図＞　　＜高速化バッチ処理データフロー図＞

図４．データフロー図の作成イメージ

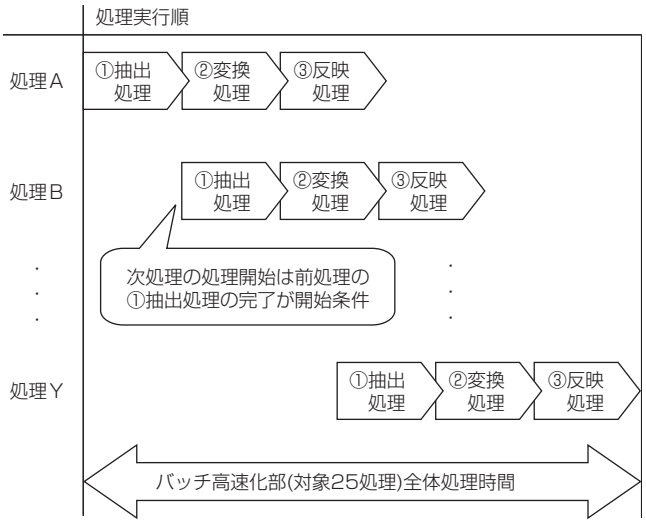


図５．高速化処理の実行順イメージ

成の最適化を実施する等，設計フェーズ，構築フェーズでも高速化するための様々な工夫を行うことによって，構築後の実測値では処理時間を３時間にまで短縮することができた。

4. む　す　び

今後，このソリューションの有効性を更に高めるためには，高速化設計・構築の自動化範囲の拡大，データベースとHadoop間の転送処理を高速化する必要がある。

また，現行バッチ処理を高速化することによって，月次集計しかできなかった業務データの日次集計，リアルタイム集計が可能になり，経営的判断を行う上で必要なデータをタイムリーに提供できるようになる。顧客にバッチ高速化ソリューションを導入することによってどのような効果や付加価値をもたらすことができるか，研究を更に深めてこのソリューションの価値向上に努めていく所存である。

一方，このソリューションで培った“高速にデータ加工するノウハウ”は，今後ビッグデータ分析を行う前処理であるデータクレンジング等への応用が可能であり，またHadoop環境はデータ分析基盤への活用が可能である。このソリューションを応用していくことで，適用範囲の更なる拡大・展開を進めていく。

特集論文

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

米沢みどり* 稲葉浩樹***
高梨郁子** 熱田裕毅*
角 正徳*

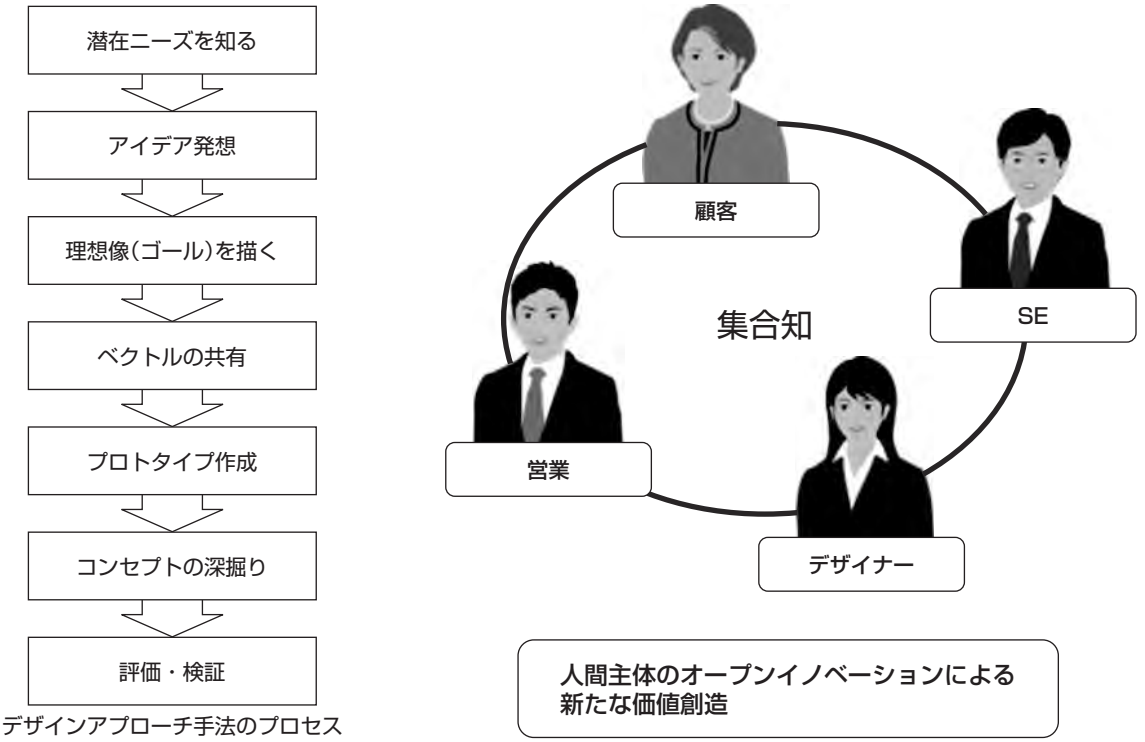
Concept Creation of Next-generation Airport Service Using Design Approach Method

Midori Yonezawa, Ikuko Takanashi, Masanori Kado, Hiroki Inaba, Hiroki Atsuta

要 旨

デザインアプローチ手法とは，あるべき理想の姿を描いて現実的な解に落とし込んでいく手法の１つである。デザイナーが形を創出する思考プロセスを一般に応用した手法で，従来型の課題解決型手法であるリサーチアプローチに比べ，新規事業開発やイノベーションによる新たな価値創出に有効であるとされている。三菱電機では，社内教育プログラムの中で，20年以上前からコンセプトメイキング手法としてデザインアプローチを展開してきた。2008年にアメリカのIDEO社が同様のプロセスからなるデザインシンキング(デザイン思考)手法を提唱し，ここ数年注目されている。

三菱電機インフォメーションシステムズ㈱(MDIS)では，2007年から三菱電機のデザイン研究所，情報技術総合研究所，先端技術総合研究所と共同でシステムエンジニア(SE)，営業，デザイナーによる社内プロジェクトを組み，デザインアプローチ手法を用いて次世代空港サービスのコンセプトを創出し，空港情報サービス事業に展開してきた。その一例である日本航空㈱の国内線自動チェックイン・発券機では，旅客の目的に合わせた使いやすいインタフェースや，用途を限定したスリムな筐体(きょうたい)にコンセプトが反映されている。MDISでは，パブリック情報，スマートIT(Information Technology)，流通，交通など様々な事業領域で，システム開発における超上流フェーズの手法の１つとして，デザインアプローチ手法を事業に展開している。



デザインアプローチ手法のプロセス

デザインアプローチ手法のプロセスと特長

デザインアプローチ手法は，最初に理想像を描いてから，自社の強み，業界動向などのフィルタをかけてゴールに導く手法である。システムエンジニア(SE)だけでなく，営業，デザイナー，時には顧客も交えた異なるメンバーの英知を集めた相乗効果としての集合知によって，新しい価値の創造が期待できる。

*三菱電機インフォメーションシステムズ㈱ **同社(博士(工学))
***三菱電機㈱ インフォメーションシステム事業推進本部

1. まえがき

2020年の東京オリンピック開催を控え，来日外国人の増加に対応するため，国土交通省は首都圏空港(成田，羽田)の2015年の発着回数を74.7万回と2011年の1.5倍に拡大し，更なる機能強化を計画するなど，日本の空港を取り巻く環境は大きく変わろうとしている。

このような中，空港の将来像を描き，利用者にとって便利で使いやすい情報サービスを提供するため，MDISでは社内プロジェクトを発足させて次世代空港サービスについて検討を行ってきた。

本稿では，そのプロセスと得られた成果について述べる。

2. 目　的

MDISでは，航空会社のチェックインシステムから，空港のフライトインフォメーションシステム，デジタルサイネージまで旅客向け空港情報サービスに関わる広汎なソリューション事業を行っている。

2007年に次世代空港プロジェクトを発足させ，特に2009年から2013年までの5年間はデザインアプローチ手法を用いて将来ビジョンを描き，その成果を実際のビジネスに展開するための継続的な検討を行ってきた。プロジェクトメンバーは空港システムを担当するSE，営業に加え，研究所からデザイナー，研究者が参画し，横断的な編成を取った。

既存の空港情報サービスの発展形のみならず，新規事業分野も含めたソリューションを検討し，ビジネスに展開することを目的とした。

3. 方　法

次世代空港サービスのコンセプトを創出するに当たり，デザインアプローチ手法を用いた[1]。デザインアプローチ手法とは，あるべき姿から理想を描いて現実的な解に落とし込んでいく手法である。デザイナーがユーザー視点から形を創出する思考プロセスを一般に応用した手法で，従来型の課題解決型手法であるリサーチアプローチに比べ，新規事業開発やイノベーションによる新たな価値創出に有効であるとされている。2008年に，アメリカのデザインファームであるIDEO社が同様のプロセスからなるデザインシンキング(デザイン思考)手法を提唱し，広く一般にも注目されるようになった[2]。

三菱電機では，全社的な社内教育プログラムの1つとして1980年代始めからコンセプトメイキング講座を実施しており，その中でワークショップの形でデザインアプローチ手法を教えている。次世代空港プロジェクトでは，社内の事業企画書に反映させるコンセプトを次のプロセスで創出した。

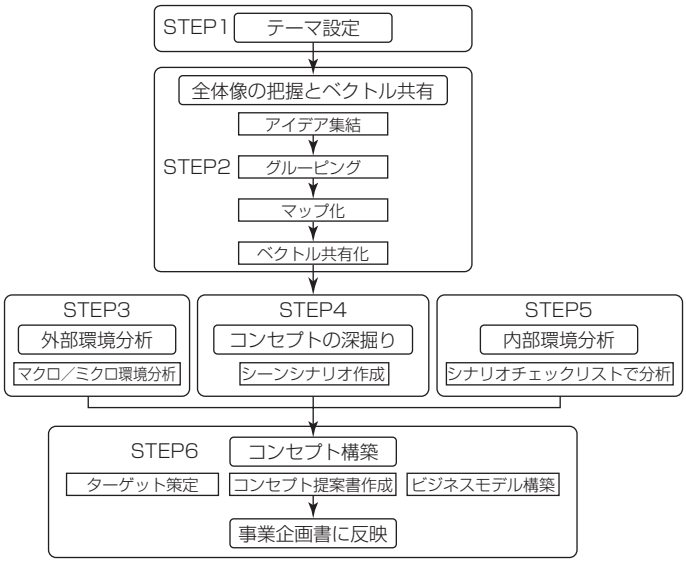


図1．コンセプト創出のプロセス

STEP 1 ：テーマ設定
STEP 2 ：全体像の把握とベクトル共有
STEP 3 ：外部環境分析
STEP 4 ：コンセプトの深掘り
STEP 5 ：内部環境分析
STEP 6 ：コンセプト構築

アイデア発想，分類には，KJ法[3]を始めとして様々な手法があるが，あるべき姿の全体像を把握するため，2軸によるマップを作製した。メンバー全員で検討し，マップ化することによってプロジェクトメンバーの共感を得られやすくし，完成したマップは事業企画書などにも用いることができる。STEP 4 まではアイデアを広げる発散と深掘りのプロセスであり，STEP 5 の内部環境分析で絞り込みを収束させる。実際にはSTEP 2 からSTEP 5 までの発散，収束を何度か繰り返すことによって，コンセプトをブラッシュアップさせた(**図1**)。

3.1　STEP 1 ：テーマ設定

空港のあるべき姿と，理想的なサービスを導き出すため“理想のターミナルサービス”をテーマとした。

3.2　STEP 2 ：全体像の把握とベクトル共有

プロジェクトメンバー全員が集まり，集中的にアイデアミーティングを実施した。1件1葉のチップに述べたアイデア約230件をディスカッションしながらグルーピングし，マップを作成した。メンバーが互いに異なる視点から意見を交わしながらアイデアを発展させていくという，この段階の集合知が最も重要である。その後デザイナーが中心となり，軸の名称やグループ名称，レイアウトなど何度も推敲(すいこう)を重ね，マップをブラッシュアップした。

縦軸を“パーソナル向けサービス～パブリック向けサービス”，横軸を“移動の経由地として利用する場合のサービス～施設として利用する場合のサービス”とし，アイデア

全体を“スムーズに利用できるサービス”“快適に過ごせる空間，施設”など大きく15のグループとして配置した(**図 2**)。

3. 3　STEP 3 ：外部環境分析

空港を取り巻く環境を把握するため，2020年までの外部環境分析表を作成した。社会環境から航空行政，エアラインの動向，観光業の動向，鉄道事業，道路交通まで幅広い分野を分析した。

3. 4　STEP 4 ：コンセプトの深掘り

マップを作る過程で出た様々なアイデアを，幾つかのまとまったソリューションとしてブラッシュアップするため，シナリオライティング手法を用いて検討した。

具体的には，外部環境分析結果を反映した時代設定の上にビジネスマン，熟年夫婦の旅行者，外国人旅行者など11のペルソナ(サービス対象モデル)を想定してシナリオを作成し，それぞれのアイデアの特長と技術的ポイントなどを整理した(**図 3**)。

3. 5　STEP5：内部環境分析

実際に事業に結び付けるアイデアを絞り込むために内部環境分析を行った。それぞれのシナリオについて，チェックリストを用いて，空港ビル，エアライン，利用者属性別の重要度，自社の技術適用度，協業の可能性などのフィルタで評価し，事業化のステップを策定した。

3. 6　STEP 6 ：コンセプト構築

次世代空港サービスのコンセプトを“フライトビジョン”(**図 4**)として，事業企画書に反映させた。また，コンセプト構成要素の中の重要なアイデアは特許出願し，パンフレット，ウォークスルーCG(Computer Graphics)(**図 5**)を作成して客先への提案を開始した。

2010年からは，フライトビジョンのコンセプトを実際にエアライン，空港ビルの具体的な商談に反映させ，受注した案件では幾つかのコンセプトを実現することができた[(4)]。

また，作成したマップをベースに，エアライン，空港ビルと共同で，デザインアプローチ手法を用いて，実際の空港利用者の声や運営スタッフのニーズを盛り込んだ，より精度の高いコンセプトを創出した。

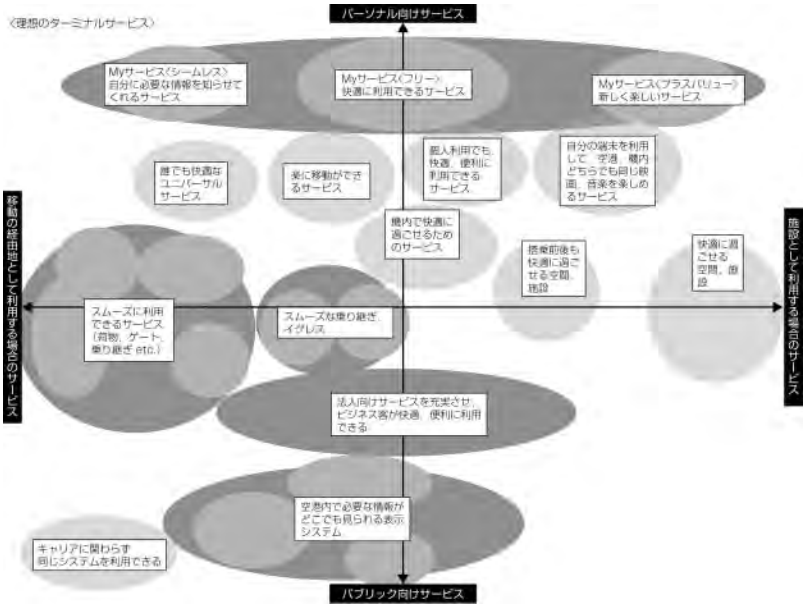


図 2．次世代空港サービスの全体像

5W-1H	シナリオ			ポイント
■いつ：平日の朝7時～8時 ■どこで：羽田空港 ■誰が：ビジネスパーソン2人 ■何を：急なディレイを ■なぜ：どこでもFISで ■どうした：どこにいても随時に確認できる			今日は部下の白鳥さんと福岡の支店に出張だ。羽田では特に待合せはせず，乗る便だけ決めて福岡空港で落ち合うことにした。	
	羽田空港駐車場	M	車で羽田空港へ。駐車場にも運航案内があるから安心だ。	●FIS 40インチ液晶で随時に表示 エアライ，空ビル別々でなくいつでもどこでも最新の運航情報が表示される 空港内の店舗や駐車場，アクセス駅，その他全国の主要な駅にも設置
	ゲート内カフェ	M	落ち着かないから早めにゲートを通過しゲート内のカフェで寛ぐことにしよう。	
		A	カフェオレを注文してソファーに座ると，横にある表示が突然点滅し出した。何かと思って目をやると，福岡行きにディレイが！白鳥さんはどうしたかな？電話してみよう。	
	空ビル内マーケットプレイス		「もしもし，今どこ？僕はゲート内に入っちゃったんだけど，たった今ディレイの案内があったよ。」	
		K	「私は今マーケットプレイスの資生堂にいます。たった今お店の前の表示にディレイが出たから，もうしばらくここで買い物してから中に入りますね」ふっふっふ，あと30分あるからゆっくり買い物しちゃおっと。	
			やれやれ，会議に遅れるな。念のためここで遅延証明をもらっておこう。支店長にも連絡しないとな。	
	博多駅	A	「もしもし，前田です。台風の影響で福岡便が30分遅れています。営業会議先に始めてください。」	●FIS(インタラクティブ) 携帯をタッチするだけで，端末から遅延証明が発行される。
			「前田くんか，ご苦労様。私も今支店に向かう途中の博多駅でフライト情報を目にしたよ。 今日は帰れないと思って覚悟しておいてくれよ。」	

FIS：Flight Information System

図 3．シナリオの一例

CIDS：チェックインカウンター案内表示器，BIDS：ブース案内表示器

図 4．コンセプトの一例

図５．次世代空港ウォークスルーCG

図６．日本航空国内線自動チェックイン・発券機

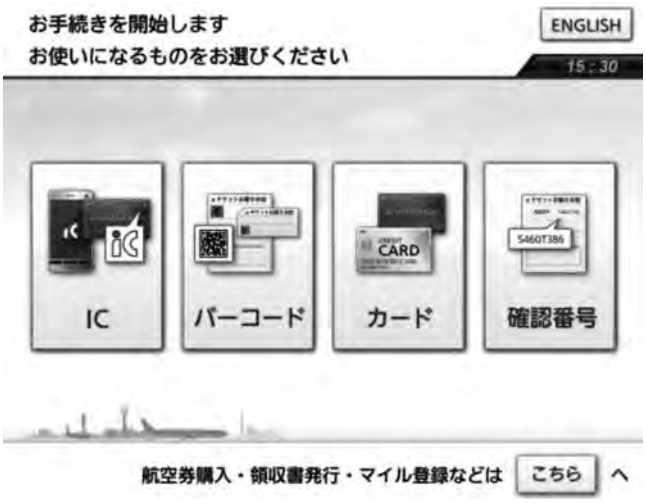


図７．日本航空国内線自動チェックイン・発券機表示画面例（トップ画面）

4. 応　用　例

2013年３月から全国の空港で利用されている日本航空国内線の新しい自動チェックイン・発券機では，用途を限定したスリムな筐体デザイン，シンプルなトップ画面と簡単な操作で間違えにくい画面遷移，認証媒体（二次元バーコード，JALマイレージバンクカードなど）をかざすだけで

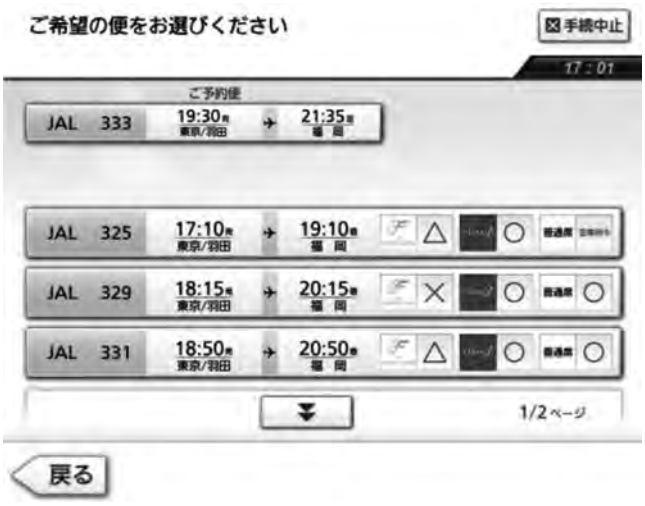


図８．日本航空国内線自動チェックイン・発券機表示画面例（便選択画面）

顧客の状況に応じた機能選択画面を表示するインタフェース，などにフライトビジョンのコンセプトを反映させることができた。この自動チェックイン・発券機はビジネスパーソンから旅行者まで広く利用されている（**図６**，**図７**，**図８**）。

5. む　す　び

次世代空港プロジェクトでは，デザインアプローチ手法を用いて長期的な視点からあるべき姿を描くことで，関係者のベクトルを合わせ，その後の開発効率化，提案力強化，特許取得などの成果につなげることができた。また，フライトビジョンのコンセプトの一部は既に実現されている。

変化の激しいIT業界では，システムインテグレータは顧客の求める仕様に応じたシステムを構築するだけでなく，上流からのコンサルティングも含めた提案が求められるようになってきている[(5)]。MDISでは，2014年度からサービス提供型事業における超上流フェーズの手法の１つとして，更にブラッシュアップしたデザインアプローチ手法を全社的に取り入れ，公共分野，スマートIT分野，流通，交通など，ITに関わる広汎な領域で事業への展開を行っている。

参　考　文　献

(1) 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コンセプト構築，デザイン学会2014年春季大会梗概集（2014）
(2) デイヴィッド・ケリー，ほか：クリエイティブ・マインドセット，日経BP社（2014）
(3) 川喜田二郎：続 発想法 KJ法の展開と応用，中公新書（1970）
(4) 実践デザイン・シンキング,日経BP社（2014）
(5) 紺野　登：ビジネスのためのデザイン思考，東洋経済新報社（2010）

特集論文

証券業界での通話録音システムとコミュニケーション基盤の統合

石川智子* 藤田喜広*
光永博文*
津村哲郎*

Unified Communication with Voice Logging System for Securities Business

Tomoko Ishikawa, Hirofumi Mitsunaga, Tetsurou Tsumura, Yoshihiro Fujita

要　旨

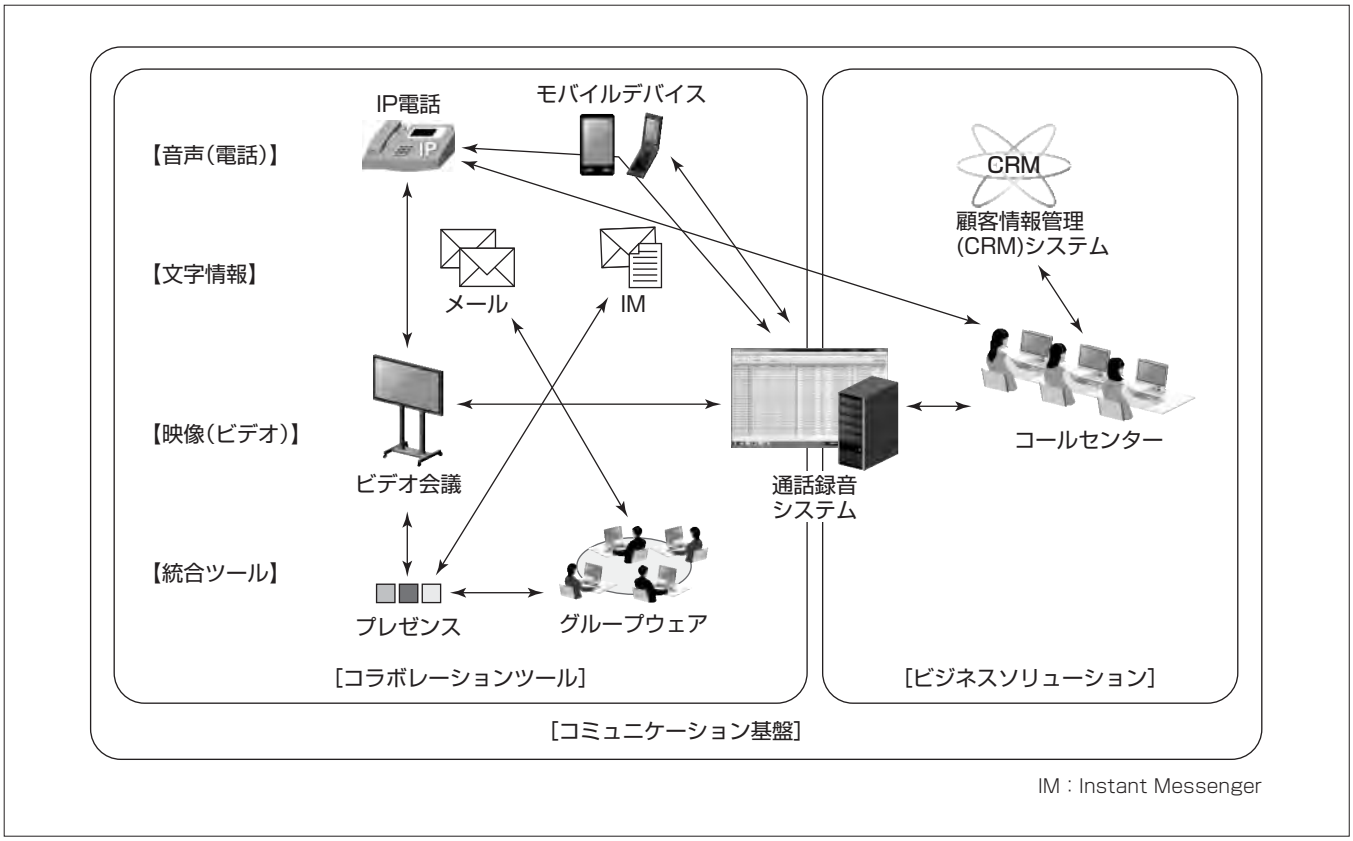
証券会社では，業務効率化や社内コミュニケーションを円滑にするコミュニケーション基盤（電話やビデオ会議などのツールやコールセンター等のソリューション）を統合して，顧客への迅速かつ正確な対応，及び多様な顧客ニーズにワンストップで応えられる仕組みを整備し，顧客満足度の向上に努めている。

三菱電機インフォメーションシステムズ㈱（MDIS）では，ベリントシステムズ社製の通話録音パッケージImpact360(注1)を中心として，これらのコミュニケーション基盤の連携を図り，統合化するとともに，証券業務に重要な商取引通話の確実な録音と必要なときに必要な人が聞き起こすことが可能な仕組みを整備し，証券会社の要望に対応してきた。コミュニケーション基盤の統合化によって，基盤ごとに録音・確認する仕組みから，一括して録音・確認できる仕組みにすることで業務効率の向上を図っている。

これまでに，IP（Internet Protocol）電話，コールセンター，顧客情報管理（Customer Relationship Management：CRM）システム，ビデオ会議，モバイルデバイスといったコミュニケーション基盤を構成する要素とImpact360の統合を実現し，業務効率化や社内コミュニケーションの円滑化に貢献している。

今後は，更に様々なコミュニケーション基盤との統合を推進していく。

（注１）　Impact360は，Verint Systems Inc. の登録商標である。



コミュニケーション基盤と通話録音システムの位置付け

証券業務でのコミュニケーション基盤には，コラボレーションツールとビジネスソリューションがある。これら同士，及びそれぞれと通話録音システムとを連携することによって，顧客対応の迅速化，社内業務の効率化に貢献できる。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

証券会社では，IP電話，携帯電話・スマートフォン，コール制御，通話録音，コールセンター，ビデオ会議などのツールやシステムを連携させて，業務効率化や社内コミュニケーションの円滑化を目指している。

本稿では，通話録音ソリューション(ベリントシステムズ社製Impact360パッケージ)と次に挙げるサービスとの連携について述べる。

⑴ コラボレーションツール(IP電話，ビデオ会議システム，モバイルデバイス等)
⑵ コールセンター
⑶ 顧客情報管理(CRM)システム

2. 証券業界における電話利用業務の現状と課題

2.1 ユニファイドコミュニケーションへの期待

2007年に施行された金融商品取引法などで法規制が強化されたことや，セキュリティやコンプライアンスに対する社会認識の変化などによって，通話録音システムが，証券会社を始め多くの金融機関に導入されるようになった。

また，ネットワークの広帯域化・低価格化，ストレージシステムの大容量化・低価格化に伴い，音声／イメージ／映像などの従来に比べて大量のデータを扱うマルチメディアが，ビジネスの現場で急速に普及しつつある。

これらの技術革新を背景に，通話録音システムと異なるコミュニケーション基盤(コールセンターやビデオ会議システムなど)をIT(Information Technology)ネットワークで統合したユニファイドコミュニケーションの活用が注目されている。ユニファイドコミュニケーションの活用によって，業務の効率化や社内コミュニケーションの円滑化を図りたいというニーズが高まっている。

2.2 証券業務における現状と課題

2.2.1 証券業務の現状

⑴ 膨大な電話対応業務

証券会社の業務は電話による取引が非常に多く，大手の証券会社では通話件数が数十万件/日に上る。また，商取引以外も電話による定型業務が多く，その多くはコールセンターで対応している。

⑵ 多様化する証券業務間での相互コミュニケーション

証券業務としては大きく，

①有価証券売買の仲介や代理業務
②有価証券の証券会社自己資金での売買業務
③企業が株式等を発行する場合の買取業務
④有価証券を売りさばく業務

が挙げられ，それぞれ多くの人が関わっているが，複数のコミュニケーション基盤が個別に使われているため，統一したコミュニケーションを取ることが難しい。

2.2.2 証券業務における課題

⑴ コールセンターの電話対応業務の迅速化

商取引のほか，株価照会や住所・氏名・届出印の変更，カード紛失対応などの定型業務を含む大量の電話に対し，迅速に対応しなければならないという課題がある。コールセンターでは業務に対応したスキルを持つ担当者に自動振り分けするシステムの利用が進んでおり，このようなコールセンター業務の中で録音した通話内容を確認して迅速に正確に対応したいというニーズが高まっている。

⑵ モバイルデバイスへの通話録音の対応

近年では，各営業所やコールセンターの電話だけでなく，証券業務でも携帯電話やスマートフォン，タブレットなどモバイルデバイスが利用されている。モバイルデバイスの通話録音は，固定電話とは別の仕組みが必要であり，検索・再生の操作が固定電話とモバイルデバイスとで異なり煩雑であるという課題があり，固定電話とモバイルデバイスの通話録音を同じインタフェースで検索・再生することが要望されている。

⑶ コラボレーションツールを利用した業務の内容記録と確認

社内業務では，業務の効率化やコミュニケーションの円滑化を目的として，電話だけでなくネットワークを利用したビデオ会議やグループウェアといったコラボレーションツールも利用されている。しかし，これらのコラボレーションツールによる業務内容を記録し，後日確認する手段がない。

3. コミュニケーション基盤の統合に対する現在の取組み

MDISでは，通話録音ソリューションとしてベリントシステムズ社製Impact360を採用しており，今回，Cisco社製品，Genesys社製品，顧客情報管理システム，ビデオ会議システム，音声テキスト化システム，モバイルデバイスとImpact360を連携させて，証券業務の課題を解決するシステムを構築した。

3.1 基盤連携の核となる通話録音システム

3.1.1 IP電話との連携

Cisco Unified Communications Manager等を利用したIP電話システムにおいて，Impact360は呼制御情報，発信者番号及び着信者番号などのCTI(Computer Telephony Integration)情報をIP電話システムから受け取り，通話の開始・終了・保留・転送を把握し，通話ごとのコンタクト情報(発信者番号，受信者番号，内線番号，通話時間，保留回数，保留時間など)を作成する(**図1**)。

なお，障害などでCTI制御情報が取れない場合の通話については，通話履歴データ(課金情報の基となるもの)と突き合わせをしてCTI情報を作成するリカバリーツールを開発した。

3.2 コールセンターでの電話対応業務の迅速化

3.2.1 コールセンターとの連携

コールセンター業務では，顧客からの通話に音声自動応

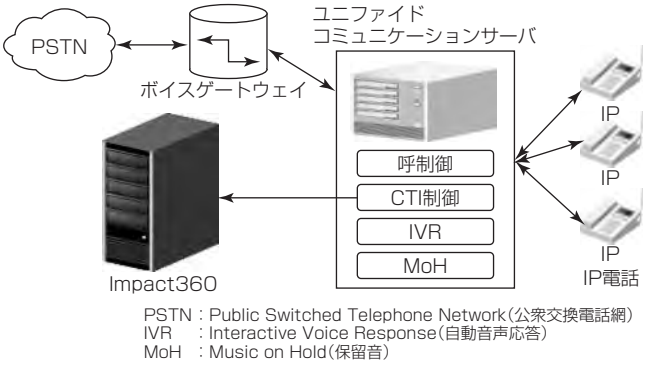


図1．IP電話とImpact360の連携

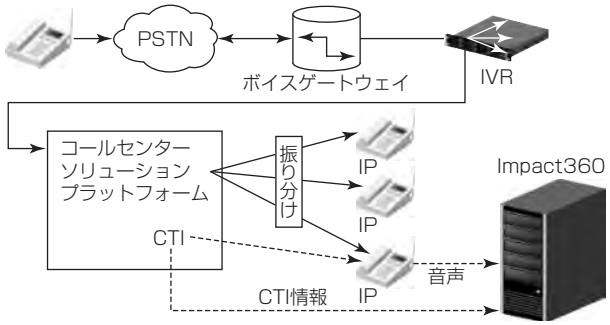


図2．コールセンターソリューションプラットフォームとImpact360の連携

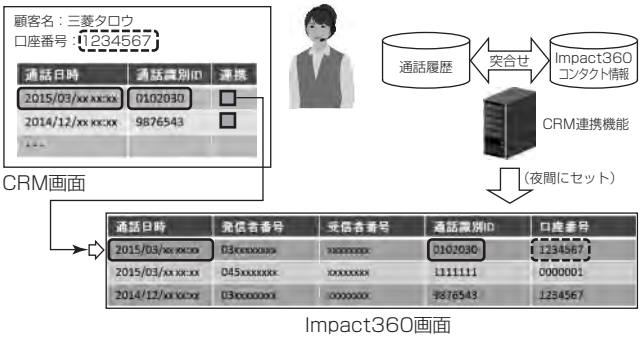


図3．CRMシステムとImpact360の連携

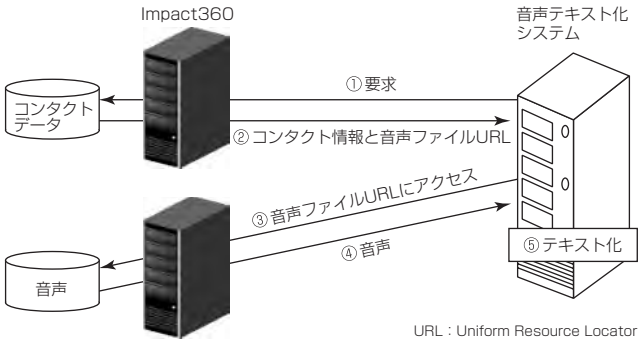


図4．音声テキスト化システムとImpact360の連携

答装置（Interactive Voice Response：IVR）が応答し，選択した照会内容に対応するスキルを持った要員を自動的に選択するなどの機能を持ったコールセンターソリューションが利用されており，コールセンターソリューションとしてGenesys社製システムを利用している証券会社は少なくない。

IVRからコールセンターソリューションプラットフォームに転送されてきた電話を一旦キューに入れ，照会内容に対応できるスキルを持つオペレータに接続し，空いているオペレータがいない場合には，“混み合っているのでお待ちください”という旨のメッセージを流して顧客に待ってもらう仕組みとなっている。呼が成立した時点で，接続した内線番号を含むCTI情報をImpact360に通知し，Impact360はコールセンターソリューションプラットフォームから受け取ったCTI情報を基にコンタクト情報を生成する。

コンタクト情報の中には店舗情報などの顧客特有の情報もあり，カスタマイズ可能なCTI領域を利用して，顧客がどこの支店へかけた電話を処理したかといった情報や，照会内容の情報などをコールセンターソリューションプラットフォームからImpact360に渡している（**図2**）。

3.2.2　CRMシステムとの連携

リテール業務では，一般的に，顧客情報を管理するためにCRMシステムを導入している。CRMシステムで管理する顧客情報と通話録音とを紐（ひも）付ける機能を開発し，必要なときに，すぐに再生して通話内容の確認ができるようにすることで，顧客への迅速で正確な対応が可能となる。

顧客情報と通話録音とを紐付けるために，通話を特定できる情報，例えば，通話時刻や通話識別IDをCRMシステムから通話録音システムに送り，通話録音システムは該当する録音データを検索・特定してCRMシステムに渡す。このようにして，CRMシステムの画面上から通話録音した音声を確認することができる。また，コンタクト情報の中の口座番号は，顧客管理情報を突き合わせて，夜間にセットしておくことで，後日，口座番号で録音データを検索することもできる（**図3**）。

3.2.3　音声テキスト化システムとの連携

通話録音システムから音声ファイルを取得して音声認識を行い，テキストに変換することができる。証券会社では通話録音されたデータから音声のテキスト化を行い，禁止用語（NGワード）を抽出して注意喚起することで，コールセンターのオペレータや営業員へのコンプライアンス強化を図っている（**図4**）。

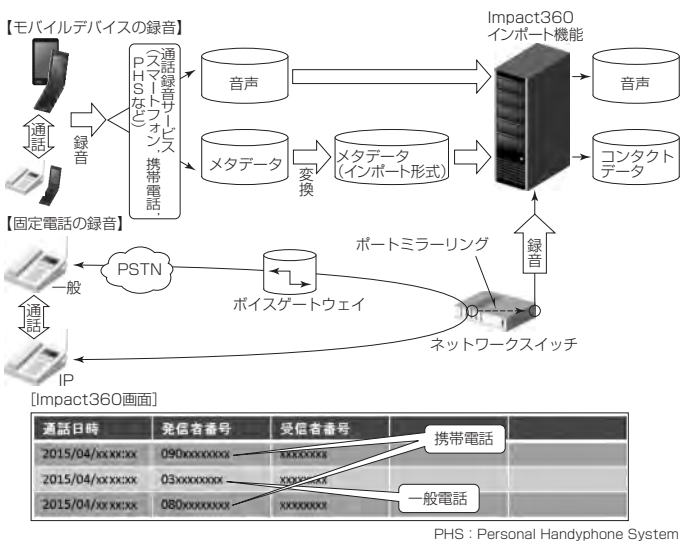
将来的には顧客からの問合せの傾向を捉え市場ニーズを的確に把握することで，競合他社との差別化を図る戦略ツールとして活用することを目指している。

3.3　モバイルデバイスへの通話録音の対応

3.3.1　モバイルデバイスとの連携

Impact360は，電話とボイスゲートウェイ間を流れる音声を，ネットワークスイッチのポートをミラーリングする機能を利用して録音サーバに取り込み，録音する。一方，モバイルデバイスによる通話については，まったく別の経路を通るので，録音サーバで音声を取得することができず，録音することができない。

それに対して，MDISでは通信サービス会社等が提供す



PHS：Personal Handyphone System

図５．モバイルデバイスとImpact360の連携

るモバイル通話録音サービスを利用して，そのサービスで録音された音声とコンタクト情報（発信者番号などのCTI情報のメタデータ）をImpact360に取り込むことによって，１つのインタフェースで固定IP電話とモバイルデバイスの通話録音を検索・再生できるようにした（**図５**）。モバイル通話録音サービスのコンタクト情報とImpact360のコンタクト情報は形式が違うため，変換ツールでフォーマット変換した後Impact360が提供しているインポート機能で取り込んでいる。

これによって，Impact360の画面から社内電話での通話も，スマートフォン・携帯端末での通話も一元管理でき，同一のインタフェースで検索・再生することができる。

3.4　コラボレーションツールを利用した業務の内容記録と確認

3.4.1　ビデオ会議システムとの連携

社内でのコミュニケーション効率化，円滑化の１つの手段として，ビデオ会議システムを利用して遠隔地との会議を実現した。各拠点のビデオ会議端末の音声をImpact360の録音サーバで録音し，Impact360のセンターサーバで集中管理する（**図６**）。

4.　コミュニケーション基盤統合の動向

これまで，証券会社では，業務の効率化を目的としたコミュニケーション基盤の統合と，通話録音システムの構築・利用によるコンプライアンス強化がなされてきたが，今後は，災害時の事業継続という観点から，場所を問わずに業務が継続できるコラボレーションツールの活用が今まで以上に重要視されてくると考えられる。つまり，“いつでも，どこでも”をキーワードとするモバイルデバイスの業務利用が，より推進されると考える。

国内のユニファイドコミュニケーション／コラボレーション市場に関する調査によると，2013年の市場規模は前年比約４％増の2,050億円程度であり，2014年以降は企業

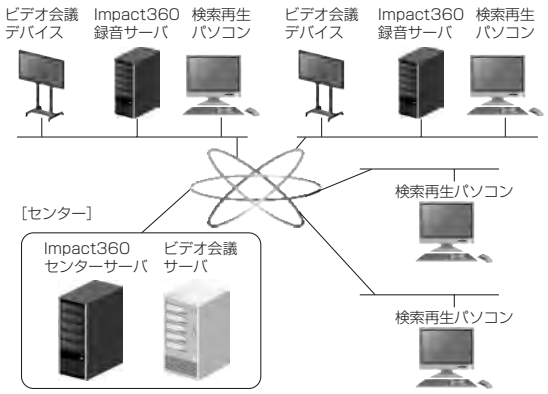


図６．ビデオ会議システムとImpact360の連携

モバイルソリューション，ビデオコラボレーション，ソーシャルビジネスなどが市場を牽引（けんいん）するとして，2013～2018年の年間平均成長率を約３％，2018年の市場規模を2,370億円程度と予測している[(1)]。また，ユニファイドコミュニケーション／コラボレーションアプリケーションのSaaS（Software as a Service）化を加速すべきとも分析しているが，半年前の調査時点では，SaaS化と企業モバイルソリューションなどのソリューションパッケージの開発が重要であると分析していたことから，半年で企業利用のモバイルソリューションパッケージが整備されつつあると推察できる。実際に，スマートフォンや携帯電話の通話録音サービスについては，通信事業社のみならず“通信システムソリューション”を手がけてきた会社がサービスを提供しており，MDISはこれを利用してスマートフォンや携帯電話とImpact360の連携を実現している。

5.　む　す　び

MDISは，証券会社等の金融機関で全国100拠点を超えるような大規模な通話録音システムを多数構築してきた。IP電話等と連携して通話を録音する基本機能の実現はもちろんのこと，通話録音システムを安定かつ安心して利用してもらうための運用，性能，セキュリティ，信頼性，拡張性などの非機能面におけるノウハウを強みとしている。

MDISとしては，さらにImpact360と他のコミュニケーション基盤を統合してレパートリーを増やし，様々なシーンに対応できる基盤を提供していき，Impact360だけでなく，ユニファイドコミュニケーションの核となり得る製品を利用してコミュニケーション基盤統合の効果範囲を広げていく。

条件の厳しい証券会社での実績を基に，他の業界にも進出したいと考えている。

参　考　文　献

(1)　IDC Japan：国内ユニファイドコミュニケーション／コラボレーション市場予測（2014）
http://www.idcjapan.co.jp/Products/research_UnifiedCom.html

特集論文

IT全般統制における特権ID管理システムの導入

砂田英之*
長田康志**

Implementation of Unrestricted Privilege ID Management System under IT General Control

Hideyuki Sunada, Yasushi Nagata

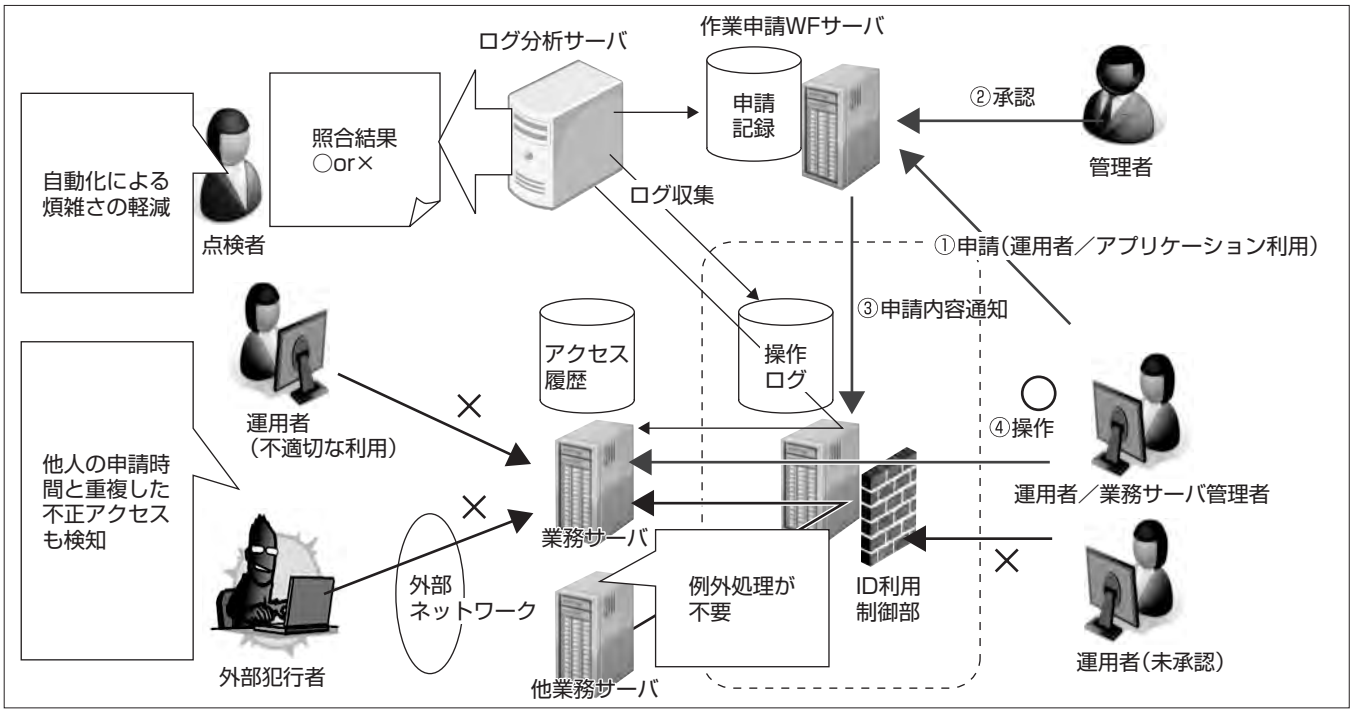
要　旨

近年，IT（Information Technology）が企業活動の中核を担うにつれ，財務統制の一環として実施されるIT全般統制で，その監査要求が年々厳しくなってきている。一部上場企業における個人情報の不正入手等を防止するため，IT運営管理基準を設ける対策が肝要である。さらに監査要件としての証憑（しょうひょう）取得や障害時の事後対応作業負荷の軽減，作業ミスの撲滅を図るため，PDCA（Plan-Do-Check-Action）サイクルを軸とした予防的な取組みとして，国際規格の１つであるITサービス管理システム（ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）20000-1/ITSMS（IT Service Management Standard））の重要性が増している[1]。

2008年から始まった三菱電機㈱のIT全般統制の監査では，システム構築・運用時に使われる一切の制限がない特権ID（Identification）による不正アクセスがないかを，Windows(注1)，データベース，ミドルウェアであるERP（Enterprise Resource Planning）システムのアクセス履歴を証憑として監査する。しかし，年々その基準が厳格になり，証憑を取得する作業が煩雑でかつ時間がかかることや，職務権限内で持ち出し許可されていない情報へのアクセスは点検できないという問題があった。この課題に対し，従来は申請ワークフロー（以下“WF”という。）と連携し，申請記録とアクセス履歴を照合して点検する方式で対応していた。この仕組みを用いても，業務サーバ間のアクセス点検の例外処理が必要なことや，申請された利用時間と重複した不正アクセスは検知ができないといった課題が残る。

本稿では，これらの課題を解決するため，アクセス履歴，申請記録，操作ログの照合を毎月行い，複数の本番サーバ上のアクセスログ点検作業を自動化して事象発生後に特権IDによる不正アクセスを効率的に“発見”する方式と，それが運用上問題ないことを検証するために行う負荷試験について述べる。

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



特権ID管理システムのシステム構成と作業フロー

作業フローは，①運用者が特権IDの利用を管理者へ申請，②管理者が作業日時，作業内容，作業対象サーバを確認して承認，③ID利用制御部へ自動的に申請内容を通知，④運用者が作業を開始し，申請時間内に作業を終了の4ステップからなる。この一連の作業は監査ログとして各業務サーバに蓄積され，ID利用制御部で蓄積された操作ログを点検することで，“不正アクセスの有無”を検知する。

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

1. まえがき

2008年から始まった三菱電機㈱のIT全般統制では，特権ID管理の監査対象がWindowsからデータベース，ミドルウェアのERPシステムへと範囲が広がり，開発者が本番機にアクセスできない規定も新たにできた。そのため，アウトソーシングサービス提供元である三菱電機インフォメーションネットワーク㈱(MIND)が本番機のメンテナンス作業を行い，特権ID管理における“承認”とその“申請書及び監査ログ収集”及び“月次での不正アクセスの点検”が必須の通常業務となった。手作業では数台のサーバしか対応できないため，今後MINDのクラウド事業の拡大によってその数が急速に増加する場合，システムの変更管理の煩雑化を防ぎ人為ミスを防ぐ運営手段の構築が急務となった。

2013年から今回の特権ID管理システムの開発に着手し，200台のサーバに適用するというシステム要件の下，システムの信頼性を担保するための負荷試験の方式を考案し，実施した。

本稿では，この開発に採用したアクセスログ点検方式及びその運用実証の一環としての負荷試験について述べる。

2. 従来技術

2.1 アクセスログ点検方式

⑴ 申請記録とアクセス履歴による照合

申請WFによって登録された申請記録(業務の種類と作業予定時刻を含む)と監査対象サーバのアクセス履歴を照合し，不正アクセスの有無を点検する仕組みで対応していた(**図1**)。これによって運用者本人の権限内であっても，不適切なタイミングでの操作を容易に検知することができる。

⑵ 課題

特権IDによるアクセスには，業務サーバ間のアクセス同様，利用期間を限定できないものがあり，これらを“アクセス許可”“アクセス不許可”と適切に判断するためには例外処理が必要であり，自動化することが困難であった。さらに，申請記録があっても作業予定時刻と外部犯行者による不正アクセスが偶然同じタイミングで行われた場合には，従来方式では適切に区別できない。

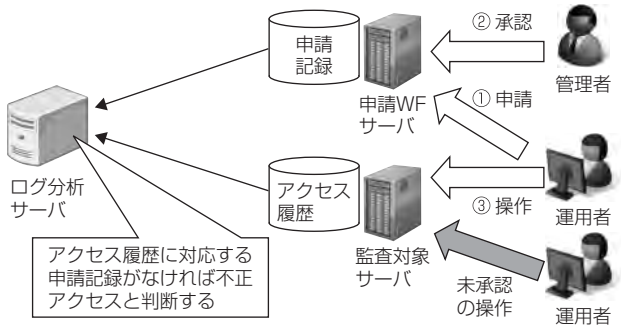


図1．システム構成(従来技術)

2.2 負荷試験

⑴ 仮想化基盤を活用した負荷試験

多重接続の負荷試験を実施する場合，必要台数分の物理マシンを準備することは非効率であり，仮想マシンで実現するケースが増えてきている。一時的に仮想マシンを複製して試験環境を構築することで，試験に係る費用を抑制できるほか，設置場所の問題や管理コンソールによる一括操作によって試験の効率化を図ることができる。

⑵ 課題

大量の仮想マシンを試験環境に用意する場合，テンプレートとなる仮想マシンを用意し，それを複製する方法を採用していた。しかし，この方法では複製時にホスト名を指定できるが，インストールされているソフトウェアによってはホスト名(又はIPアドレス)が変更された場合に再設定／再インストールが必要になるという問題があった。これに対して，プロビジョニングスクリプトの実行等，仮想マシンの作成時に初期設定を行う方法が仮想環境で準備されているが，バックグラウンドで実行されるため，画面がアクティブにならず，画面インタフェースを持つ操作の自動化が困難であるという課題があった。また，運用者の操作の自動化も本試験の効率化のために必要であったが，これも同様に課題となっていた。

3. 解決策

3.1 アクセスログ点検方式

3.1.1 操作ログとの照合による点検方式

監査対象サーバへはID利用制御部を経由してアクセスし，ID利用制御部では申請記録に基づき，サーバへのアクセス制御を行い，操作ログを残す構成とする。運用者は事前に利用申請して，監査対象サーバへアクセスする。また，他の業務サーバ(アプリケーション)から監査対象サーバへのアクセスも同様に，ID利用制御部を経由して監査対象サーバにアクセスする構成とする。なお，点検時にはID利用制御部を経由したアクセスを，正当なアクセスとして取り扱う(**図2**)。

3.1.2 実現方式

⑴ 特権IDの利用申請と申請記録

監査対象サーバの運用者は，作業を実施する前に申請WFで利用申請を行う。申請WFでは，管理者に対して利用申請があったことを通知し，管理者の承認手続きによって，申請記録(**表1**)を保存する。

⑵ ID利用制御部を経由した対象サーバへのアクセス

ID利用制御部では，運用者の認証及び各種利用プロトコルの中継を制御する機構を持つ。運用者の認証後，申請記録と適合するアクセスであれば，指定された特権IDで対象サーバとの認証を行いアクセスを中継する。利用時間やプロトコルが異なるなど不適合な場合は，アクセスをブ

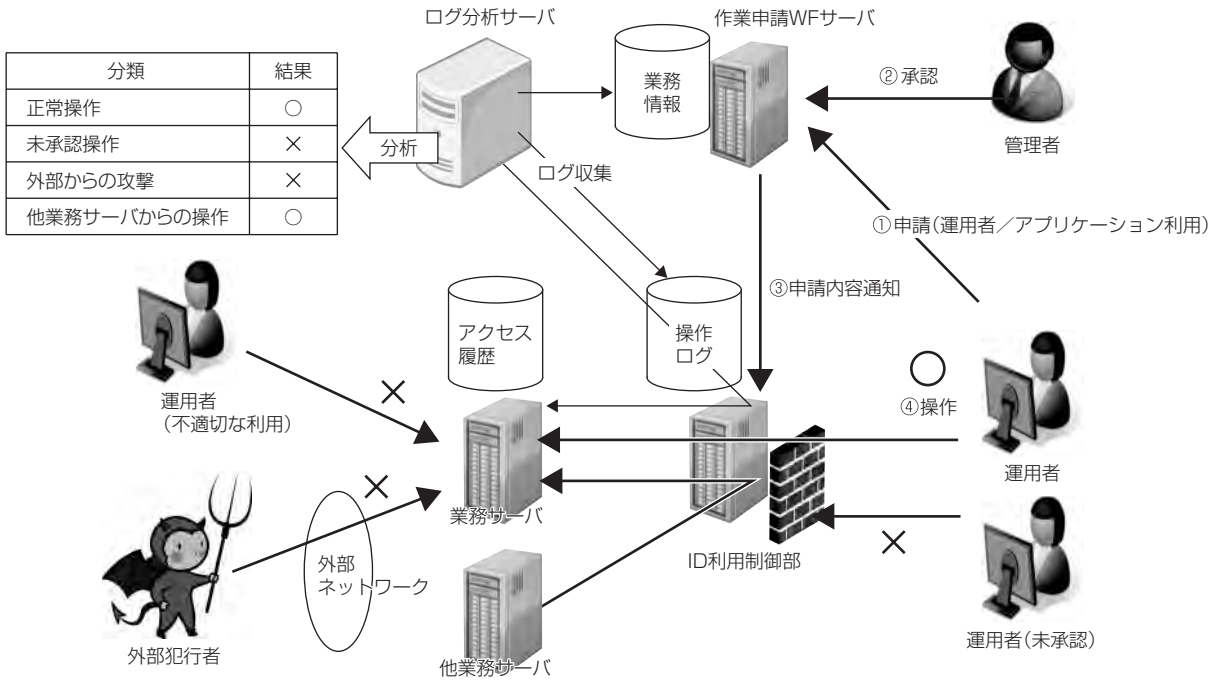


図 2．システム構成(解決策)

表 1．申請記録(承認状態)

項目	内容
特権ID	作業時に利用する特権ID
運用者ID	運用者の識別情報
対象サーバ情報	サーバのホスト名など
目的	作業の目的
利用期間	作業開始～終了の予定日時
操作内容	利用プロトコルなど

表 2．操作ログ

項目	内容
特権ID	サーバへの認証に使ったID
運用者情報	運用者の識別情報
アクセス日時	アクセスを中継した日時など
操作内容	利用プロトコルなど

表 3．アクセス履歴

項目	内容
特権ID	サーバへの認証に使ったID
操作内容	“ログイン”などの操作内容
アクセス日時	操作の実施日時

ロックする。**表 2** は操作ログの内容である。

(3) アクセス履歴

監査対象サーバ上のOS(Operating System)のセキュリティ監査ログ等の機能によって，運用者の操作内容がアクセス履歴(**表 3**)として記録される。

ID利用制御部を経由した場合は，申請記録と適合したアクセスのみが許可され，アクセス履歴に記録されたレコードの日時に対応する申請記録・操作ログの両方がそろった状態で保存される。一方，内部・外部犯行者による不正アクセスでID利用制御部を経由しない場合には，操作ログが残らないため，不正なアクセス等であることが判断できる。**表 4** は，アクセス状態と各種記録の状況及び，それらに基づく判定結果を整理した一覧である。

表 4．アクセス状態と各種記録の対応

アクセス状態		記録			判定	備考
		申請書	アクセス履歴	操作ログ		
ユーザー操作	承認(正常)	あり	あり	あり	○	正当アクセスと判断
	承認(不正)	あり	あり	なし	×	不正アクセスと判断(運用ルール非適合)
	未承認(正常)	なし	−	なし	×	ID利用制御部がブロック
	未承認(不正)	なし	あり	なし	×	不正アクセスと判断
業務サーバ	承認(正常)	あり	あり	あり	○	正当アクセスと判断(点検時例外処理不要)
	承認(不正)	あり	あり	なし	×	不正アクセスと判断(乗っ取り等の可能性あり)
	未承認(正常)	なし	−	なし	×	
	未承認(不正)	なし	あり	なし	×	
外部犯行	承認時間内	あり	あり	なし	×	不正アクセスと判断
	承認時間外	なし	あり	なし	×	不正アクセスと判断

このように，IT全般統制での監査における不正アクセスの点検作業は，アクセス履歴に対応する申請記録及び操作ログがそろっているかどうかで正当・不正を判断でき，例外処理の必要がなく自動処理が可能である。

3.2 負荷試験

(1) 初期設定方式

個別に仮想マシンの初期設定を行うことは煩雑であるため，今回はキー操作可能なスクリプトを採用し，ホスト名をキーとした設定ファイルに実行内容を指定することで対応した。1台の仮想マシンでスクリプトを実行し，スクリプトの処理によってリモートデスクトップで他の仮想マシ

ンのスクリプトを逐次起動し，指数関数的にスクリプトの実行台数が増加するよう設定して，設定に掛かる時間の短縮を図った。

⑵　メンテナンス操作シミュレーション

運用者の操作シミュレーションも初期設定と同様にスクリプトで実現した。環境を共通化するため，各仮想サーバのホスト名の命名ルールを“VMnnn（nnn＝000～150）”と定めて，nnnの仮想マシンはnnn＋１の仮想マシンに対して，メンテナンス操作のシミュレーション（スクリプトによって実施）を行うように設定した。

これによって各環境の共通化が図れるとともに，１台目の仮想マシンでスクリプトを実行するだけで，設定及びメンテナンス操作の自動化が可能となる。

4. 評　　価

4.1　新点検方式による効果

不正アクセスの検出で，作業の煩雑さや本人の権限がないアクセスしか検出できないことが課題になっていた。従来技術でも，申請WFと連携することによって，本人の権限内であっても不正なタイミングや操作によるアクセス検出が可能であったが，業務サーバ間のアクセスや他人の申請記録（利用時間）と重複した不正アクセスを検出できない課題が残っていた。この方式を用いることで，申請記録，操作ログ，アクセス履歴の対応関係を照合して，先に述べた不正アクセスの検出が可能となる。また例外処理がないため，処理の自動化ができ作業を効率化することが可能となった。

4.2　負荷試験とその効率化

特権ID点検（ログ収集）の実現に当たり，対象サーバ（顧客の本番機）を想定し，監査ログを特権ID点検システムで収集するためのエージェントを開発した。

通常運用の試験23項目，異常試験５項目に加え，200台規模での動作を検証するための負荷試験を実施した。負荷試験では，最大150台のWindowsサーバを構築して，エージェント導入，ログ収集，サーバ削除をクラウド環境で構築することで，負荷試験のための準備を数時間以内にすることができ，試験の効率化を図ることができた。

今回，これらの試験環境の構築方法を活用し，ログ収集対象サーバの台数を最大150台まで段階的に増やして負荷試験を行った。**表５**に試験のシステム要件をまとめた。

この負荷試験は，クラウド環境で監査ログ収集対象Windowsサーバを構築して，サーバ起動時にログ収集エージェントを導入し，さらに運用者の操作シミュレーション（ログイン，ログオフ操作の繰り返し）を自動化するスクリプトを作成することで実施した。

表５．システム要件

分類		内容	
機能要件	特権ID管理	WF機能	WFによる監査サーバ利用の申請及び承認
		アクセス制御機能	利用申請に基づく監査サーバへのアクセス許可／不許可
	特権ID点検	ログ収集機能	監査対象サーバ及び特権ID管理システムからのログ収集
		点検機能	監査ログから不正アクセス抽出と結果の出力
		保管／削除機能	指定期間を経過したファイルの削除
非機能要件	規模	監査対象サーバ数	200台規模
	性能	ログ確認	前日のログを確認可能
		点検時間	数時間以内に完了

その結果，ログ収集エージェントによる操作シミュレーションに対応するログが全て収集されたことを確認できた。さらに，試験手順をスクリプトで自動化し，作業の効率化，試験時間の短縮と試験にかかるコストの最小化が可能となり，150台接続時に次の内容で試験を実施することができた。

＜負荷試験の実績＞

⑴　構築（150台）：3.0時間

⑵　操作シミュレーション・ログ確認：2.0時間

⑶　消去（150台）：0.5時間

⑷　作業時間：合計5.5時間

⑸　利用料金：約５万円

5. む　す　び

業務サーバ間のアクセスや他人の申請記録と重複した時間帯でのアクセスも含めた不正アクセスの検出方式について述べた。この技術は監査上“発見的統制”と呼ばれ，事象発生後，特権IDによる不正アクセスを効率的に“発見”するためのものである。今後，ログ自体の改ざん対策，Windows以外のOSの監査ログ収集とその点検方式の開発，仮想化環境での監査ログの点検，特権IDでの不正アクセスのリアルタイム検知技術も含め，検討を進めていく。

負荷試験では，クラウド環境の操作は標準のポータル画面から実施したが，一度に構築・削除可能なサーバ台数に制約があり，構築・削除に数時間を要してしまった。今後は，クラウドのAPI（Application Programming Interface）を活用し，一度の操作で大量のサーバの構築・削除を実現し，より短時間で負荷試験の環境を準備する方式について検討していく。

参 考 文 献

⑴　経済産業省 企業内ITC・ITガバナンス研究会：ITCプロセスにおける情報システムの信頼性向上へのアプローチ（2008）
http://www.itc.or.jp/foritc/itccommunity/search/dlfiles/S07002_syousai.pdf

特集論文

クラウドを利用した保守支援システム“PACKAGE PLUS Park”

鈴木　剛*
高橋裕幸*

Cloud-based Maintenance Support System "PACKAGE PLUS Park"

Takeshi Suzuki, Hiroyuki Takahashi

要　旨

㈱三菱電機ビジネスシステム(MB)で取り扱うパッケージでは，様々な保守サービスを提供している。

社会保険労務システムや人事総務系パッケージのバージョンアップ保守サービスでは，法改正対応の際，CD-ROM(Compact Disc Read Only Memory)による改訂モジュール配布，システムエンジニア(SE)訪問によるシステム入替えを行っている。法改正対応が発生するごとに，改訂モジュールの提供回数が増加して保守コストも増加している。

一方，ソフトウェア保守サービスでも，近年システム構成が複雑化していることで，障害発生から復旧までに多くの人件費が費やされる事案が増加してきている。

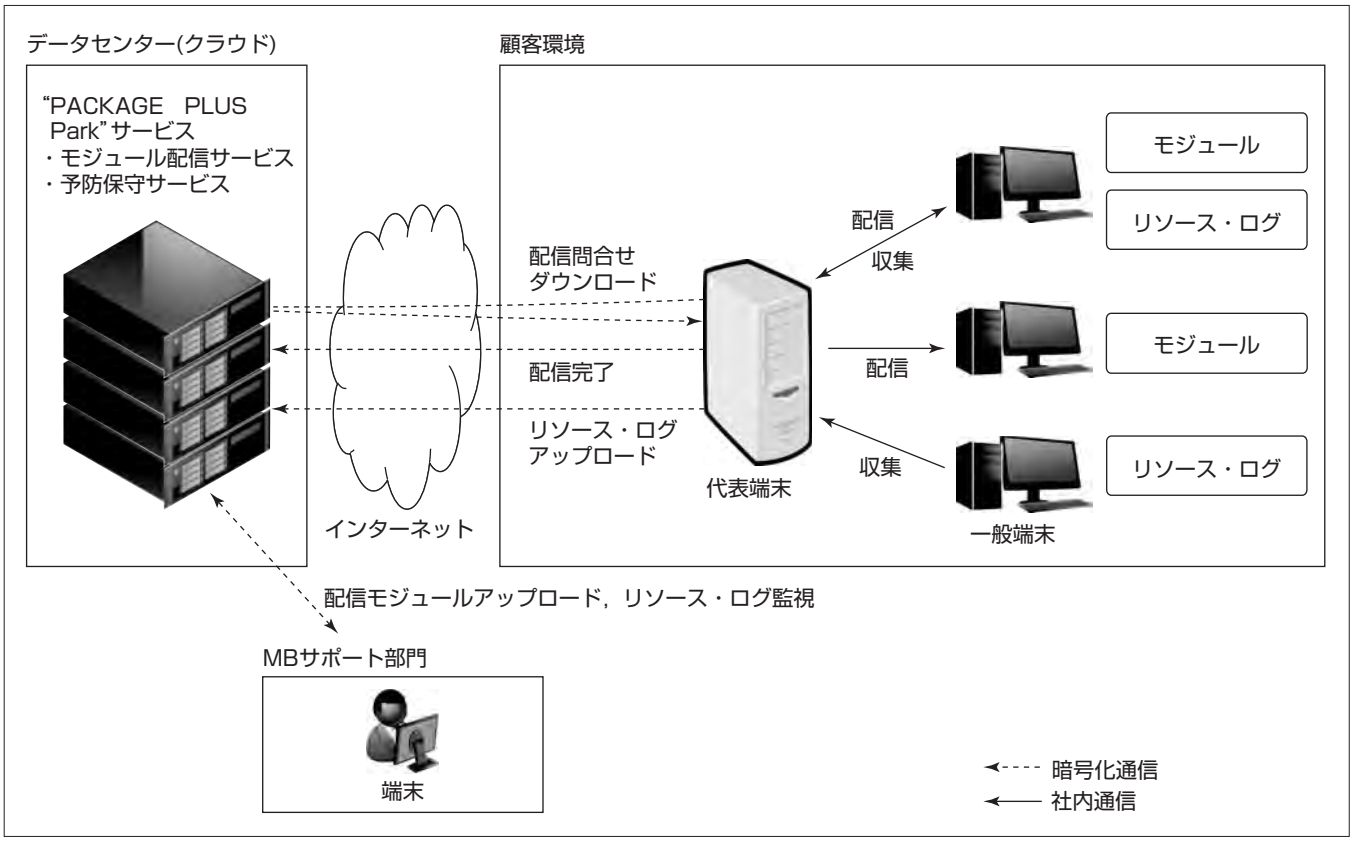
これらの保守コスト増加を防ぐため，MBでは保守支援システム“PACKAGE PLUS Park”を開発してサービス提供を開始した。PACKAGE PLUS Parkの主なサービスは次の2つである。

(1)　モジュール配信サービス

法改正に対応した改訂モジュールをインターネット経由で配信するサービスである。インストール開始までのプロセスを完全自動化することで，人的作業を削減・効率化して，システムの入替え作業を迅速化する。

(2)　予防保守サービス

顧客のハードウェアリソースの使用状況とシステムログを収集して，24時間自動監視することでトラブルにつながる予兆を検知するサービスである。トラブルにつながる可能性がある予兆を検知した際には，MBのエンジニアが適切に対処し，障害発生を未然に防ぐことで顧客システム運用の安定化に貢献する。



PACKAGE PLUS Parkのシステム構成

PACKAGE PLUS Parkシステムは，データセンターで稼働するPACKAGE PLUS Parkサービス(モジュール配信サービス・予防保守サービス)，顧客環境の代表端末，一般端末及びMBサポート部門の端末で構成している。顧客の代表端末はPACKAGE PLUS Parkサービスとインターネット経由で通信し，一般端末は顧客社内で代表端末と通信し，端末ごとにモジュール配信とリソース・ログ収集の両方又は一方を実行する。MBの端末はPACKEGE PLUS Parkサービスとインターネット経由で通信し，配信モジュールアップロードとリソース・ログ監視を行う。

*㈱三菱電機ビジネスシステム

1. まえがき

近年，社会保障の充実やワークライフバランスの推進などを目的とし，次のような法改正が実施されている。

⑴ 税制改正（保険料率改定や消費税法改正等）

⑵ 労働法改正（パートタイム労働法，36協定）

今後も消費税率変更，マイナンバー法，労働者派遣法，ストレスチェック義務化などの法改正が控えている。各種業務パッケージ製品を提供しているMBとしては，法改正に合わせてパッケージ製品を改訂し，確実に顧客に提供する使命がある。法改正に対応した改訂モジュールの提供回数増加に伴う保守コストも膨らむことが予想されるため，保守コストの増加を抑えることを目的としたPACKAGE PLUS Parkシステムを開発した。PACKAGE PLUS Parkサービスの提供環境は，立ち上げ時の初期コスト抑制と，利用者が増加した場合の柔軟なリソース拡張が可能なクラウドを利用した。

本稿では，最初に，PACKAGE PLUS Parkを開発する背景となった保守業務における課題を述べ，次にその解決策として開発したPACKAGE PLUS Parkの主な機能とその導入効果について述べる。

2. パッケージ保守業務の課題

2.1 改訂モジュールの配布

MBの提供するバージョンアップ保守サービスでは，従来，各種業務パッケージの法改正対応を行った際，パッケージを導入している顧客に対し，改訂モジュールを格納したCD-ROMを配布している。発送したCD-ROMを基に顧客が入替えを行うパッケージ製品と，SEが顧客まで持参してインストールと説明を実施しているパッケージ製品がある。

例えば，社会保険労務システムの場合には，税制改正や年末調整の他，電子申請の仕様変更等，年に数回の法改正対応が発生している。その都度改訂モジュールを格納したCD-ROMの作成・発送を行っているため，毎年多大なコストがかかっている。その他のパッケージ製品でも，CD-ROMの作成や配布，顧客環境へのインストールに伴う作業が発生しており，改訂モジュールの配布に伴うトータルコストの増加を抑えることが課題となっている。

また年末調整システムでは法改正仕様が9月中旬頃に確定するが，顧客での利用開始は11月となるため対応期間が短い。この1か月半程度で法改正対応と，CD-ROM作成，インストールを行っており，CD-ROM配布に伴う作業の迅速化，効率化も課題となっている（**図1**）。

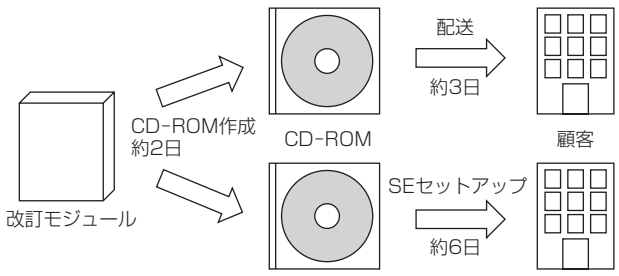


図1．現状のCD-ROM配布

2.2 受動的保守

MBでは様々なソフトウェア保守サービスを提供しているが，基本的には障害発生後に復旧作業を行うサービスである。発生した障害が深刻な場合は，システムの停止時間が長くなり，顧客の業務が停止する。障害発生後に対応するという，後手の保守も課題となっている。

3. モジュール配信サービス

法改正対応のCD-ROM等，改訂モジュール配布に関する課題の解決策として，クラウドを利用したモジュール配信サービスを開発した。

モジュール配信サービス（以下“配信サービス”という。）とは，事前に顧客環境へインストールしたエージェント（ユーザーの代理で通信処理を行うソフトウェア）が配信サービスへ定期的に問い合わせ，未導入の改訂モジュールが存在した時には自動でダウンロードする仕組みである。エージェントがモジュールをダウンロード後，インストーラを自動起動する設定も可能である。これらは全てバックグラウンドで動作し，かつ定期タスクで処理をする。したがって，改訂モジュールの完成後から，顧客のインストール開始までのプロセスを完全自動化することができる。

一般的なインターネット経由配信の中には，ブラウザから対象のモジュールを選択しダウンロードする方式もあるが，現状のCD-ROM配布に比べ顧客側での運用業務の変更が必要となり，手間も増えるため採用しなかった。

この結果，改訂モジュールを配布する顧客数分のCD-ROMを作成する作業が，配信サービスのサーバへアップロードする作業に置き換わり，顧客への改訂モジュール配布が，CD-ROM配布からダウンロード形式に替わる。つまり改訂モジュールの出荷から顧客への配布までの作業が迅速化され，従来の人手による作業が自動化されて効率化へとつながる（**図2**）。また，顧客訪問が必要な一部のパッケージ製品でのSEセットアップも，CD-ROM作成・持参等が不要となるため，作業を効率的に進めることができる。

今後顧客のPACKAGE PLUS Park導入が進むことでCD-ROMの作成から発送までのコストと，SEセットアップコストの増加を抑えることが可能となる。

3.1 顧客のパソコン構成

顧客環境のエージェントは端末ごとに配信サービスへ直

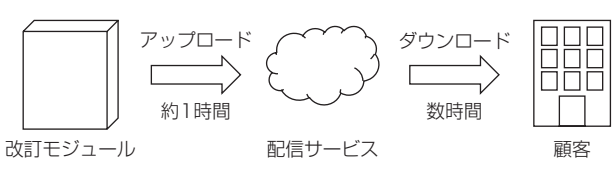


図2．モジュール配信サービス

接問い合わせるという構成はとらない。顧客環境ごとに1台の代表端末を設置し，複数の一般端末(パッケージ製品を導入したパソコン)は，その代表端末を経由して配信サービスを受ける構成とした(**図3**)。

しかし，顧客によってはパッケージを導入したパソコンが1台で，一般端末を複数設置しない場合もある。この場合は代表端末に一般端末の役割も持たせることで，1台での構成も可能である。

3.2 モジュール配信方式

モジュール配信方式は，代表端末のエージェントのみが配信サービスへ問い合わせ，改訂モジュールをダウンロードし，一般端末のエージェントに配信する仕組みである。配信サービス提供側から見ると代表端末のみからのアクセスとなり，ネットワークトラフィックを抑え，配信サービスのハードウェア要件を抑えることに貢献する。

また，サイズが大きなファイルをダウンロードすると，配信サービス環境と顧客環境のネットワーク帯域を専有してしまうおそれがある。そこで配信ファイルを独自方式で分割して配信する方式にした。エージェントが配信サービスで分割されたファイルをダウンロードし，ファイル結合とハッシュ値チェックを行い，元のファイルに復元する(**図4**)。通常の配信に比べ時間を要するが，CD-ROM発送よりは大幅に短縮される。これらの処理は全てバックグラウンドで行うため，顧客による画面操作は必要とせず，運用の負担はない。ファイルを分割して配信することによって1回の通信量を減らすことができるため，配信サービス側で使用するハードウェアリソースを低減したままで，多数の顧客への同時ファイル配信を実現している。

その他，配信の前後に，指定したファイルの実行機能を付加し，データベースに項目を追加するスクリプトやバッチファイルの実行，インストーラの自動起動を可能とした。これらの実装によって配信サービスは改訂モジュールのファイルサイズや，ファイル種類に関係なく導入できる。

セキュリティ面では，通信の暗号化，分割ファイル結合時のハッシュ値チェック，分割ファイルの改ざんチェック，DNS(Domain Name System)キャッシュポイズニング(DNSサーバに偽の情報を覚えこませる攻撃手法)対策として返答サーバのIP(Internet Protocol)アドレスチェックを行っている。

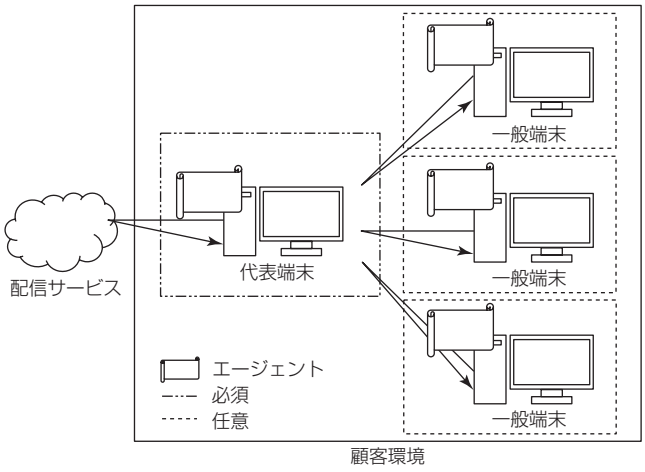


図3．顧客環境の構成

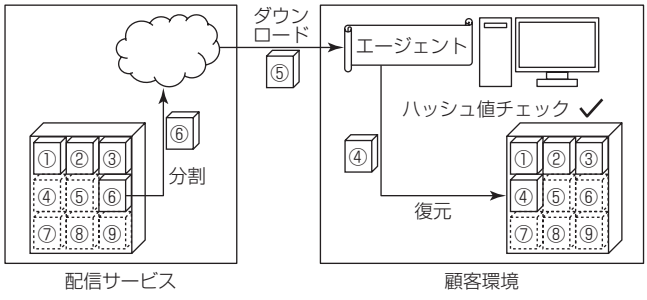


図4．モジュール分割配信の仕組み

4. 予防保守サービス

受動的な保守の解決策として，予防保守サービスを開発した。トラブルにつながる予兆を早期に検出・解決し，障害発生を未然に防ぐことを目指している。配信サービスではハードウェアリソースの使用量が少なく，アイドル時間が長いため，予防保守サービスで監視機能を稼働させることで，リソースを有効活用できる。またPACKAGE PLUS Parkは，顧客環境の各端末にエージェントを導入する構成であるため，エージェントにモジュール配信に加えて予防保守の役割を与えることで付加価値を提供できる。

予防保守サービスでは，顧客端末のリソース・ログを監視する。その結果，トラブルの予兆を検知し，システム停止の原因となり得る障害が発生する前に対処する能動的な保守サービスの提供が可能となる。

次に予防保守サービスのリソース・ログ監視機能と，月次レポート作成機能について述べる。

4.1 リソース・ログ監視機能

リソース・ログ監視機能で，顧客の端末から次の情報を予防保守サービスで収集してリアルタイム監視を行う。

(1) 端末リソース情報(CPU(Central Processing Unit)・メモリ・ハードディスク)
(2) ログ情報(ソフトウェア・ハードウェア等)

そして，ハードディスクの空き容量不足に陥る，CPU使用率100%が継続するなどの，故障につながる状態変化や潜在的な障害を早期に検出する機能である。

リソース・ログ監視機能が障害の予兆を検出した場合に

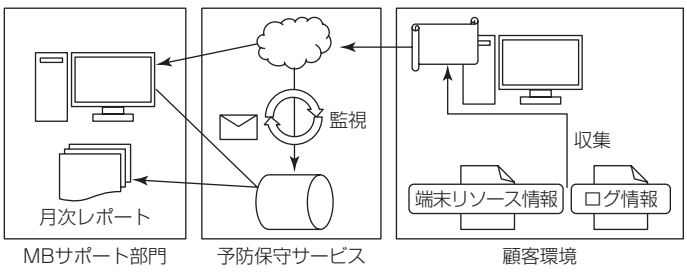
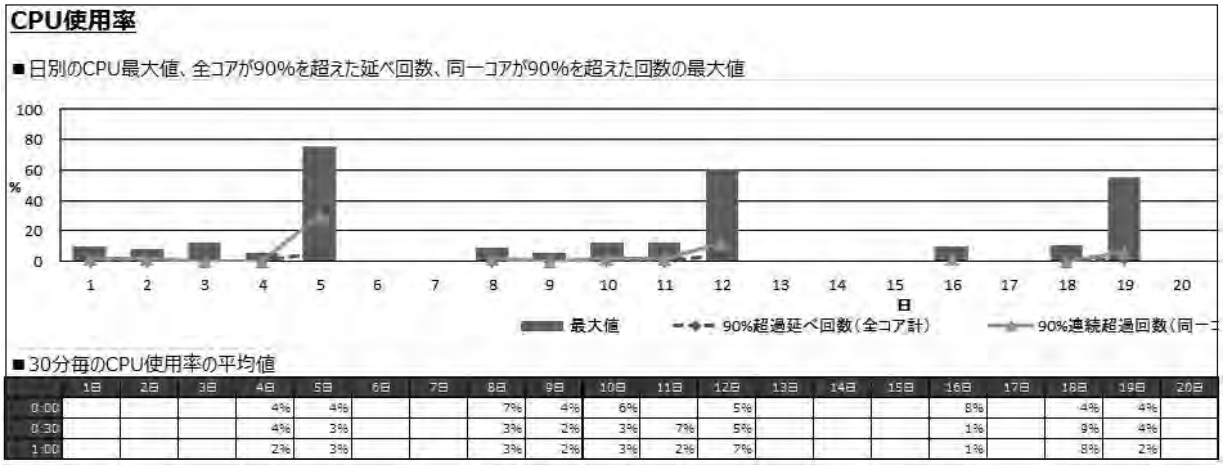


図5．月次レポート作成機能



	1日	2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日
0:00				4%	4%			7%	4%	6%		5%				8%		4%	4%	
0:30				4%	3%			3%	2%	3%	7%	5%				1%		9%	4%	
1:00				2%	3%			3%	2%	3%	2%	7%				1%		8%	2%	

リソース別に，日別平均値推移と，日別時間別（30分単位）の明細を端末ごとに出力する。

図 6．端末リソース情報のレポート

リソース障害件数統計

発生状況	件数
前月以前に発生した未対応障害件数	19
前月以前に発生した未対応障害の内、当月対応済の障害件数	16
当月発生した障害件数	9
当月発生した障害の内、対応済の障害件数	9

リソース障害対応情報

NO	コンピュータ名	発生日時	障害タイトル	障害内容	処置内容	処置日	処置状況
1	client-7	2015/4/3 13:08	MELB：client-7：Cドライブ空き容量不足	ユーザー企業：MELB コンピューター：client-7 内容：Cドライブの空き容量が95%を超えた	Cドライブの空き容量確保のため下記を実施。 ①VM環境(LINUX、Win2008R2)を削除 ②ダンプファイルを削除	2015/4/3	完了
2	client-8	2015/4/15 13:08	MELB：client-8：Cドライブ空き容量不足	ユーザー企業：MELB コンピューター：client-8 内容：Cドライブの空き容量が95%を超えた	バックアップ取得のため一時的に使用量が増 処置不要	2015/4/15	完了
3	Server-1	2015/4/1 7:03	MELB：Server-1：CPU使用率100%のまま1時間経過した	ユーザー企業：MELB コンピューター：Server-1 内容：CPU使用率100%の状態1時間経過	サーバー監視用ツールがCPUを専有していたため 低リソースで動作するよう設定変更した	2015/4/1	完了

監視機能によって検出したリソース情報の明細。件数のサマリーと障害・処置内容を出力する。

図 7．リソース情報監視ログのレポート

は，MBのサポート部門へのメール通知と，リアルタイムモニタ画面へのアラート表示が行われ，予防保守に向けた迅速な対応を可能としている。

ログ情報の監視では，転送量を最低限にするため前回アップロードからの差分ログのみを抽出収集する。収集したログは予防保守サービスのサーバ上で一定期間保持・管理する。ログ閲覧機能を使用すれば，監視で検出されたログの確認が可能である。また，実際のログファイルをダウンロードすることで，対象ログの前後に出力されているログも参照可能とした。さらに，関連する各種ログを時系列にマージして閲覧できる機能を備えた。これによってログを横断的に調査することが容易になる。

4.2　月次レポート作成機能

リソース・ログ監視機能で収集した顧客ごと，端末ごとの情報が予防保守サービスのサーバへ蓄積される。これらの情報を月次で分析・集計し，端末ごとに月次レポートを作成する（**図 5**）。作成したレポートは予防保守の結果として顧客へ提供する。

分析・集計・出力処理ではサーバの負荷が高くなるため，別のサーバで分析・集計処理して定期タスクで夜間に出力処理を行う仕組みとした。出力したレポートは予防保守サービスのサーバ上に保存するが，顧客を特定する情報は保持しない。顧客名等はHTML5（HyperText Markup Languageの第 5 版）のWebストレージ（データをブラウザ側に蓄積する仕組み）で保持し，ダウンロード時に帳票に埋め込む処理を追加している。このように顧客情報を保持せず，漏洩（ろうえい）リスクを極力減らす対策を施している。

なお，作成する月次レポートは次の 3 種類がある。

(1)　端末リソース情報（**図 6**）
(2)　リソース情報監視ログ（**図 7**）
(3)　ログ情報監視ログ（**図 7** と同様）

5. む　す　び

現在，システムの多様化と同様に，保守サービスも多様化してきている。しかし，システム停止による業務への影響を極力減らすことは相変わらず重要である。PACKAGE PLUS Parkの導入によって，ソフトウェア保守，ハードウェア保守，システム導入のトータルコストを削減し，その費用を製品品質や保守サービスの更なる向上に充当していきたい。

PACKAGE PLUS Parkには，システム改善，セキュリティ対策を継続的に実施し，技術や環境変化への対応や改善を図るとともに，今後，マルチテナント化やシステム内権限管理の強化を実施し，モジュール配信サービス及び予防保守サービスの外販を目指していく。

特集論文

無停止型サーバftServerの公衆インターネット網を用いた遠隔監視システム

渡辺和也*
冨塚　潔*
尾崎勝広*

Remote Support System via Internet for Fault-tolerant Server "ftServer"

Kazuya Watanabe, Kiyoshi Tomizuka, Katsuhiro Ozaki

要　旨

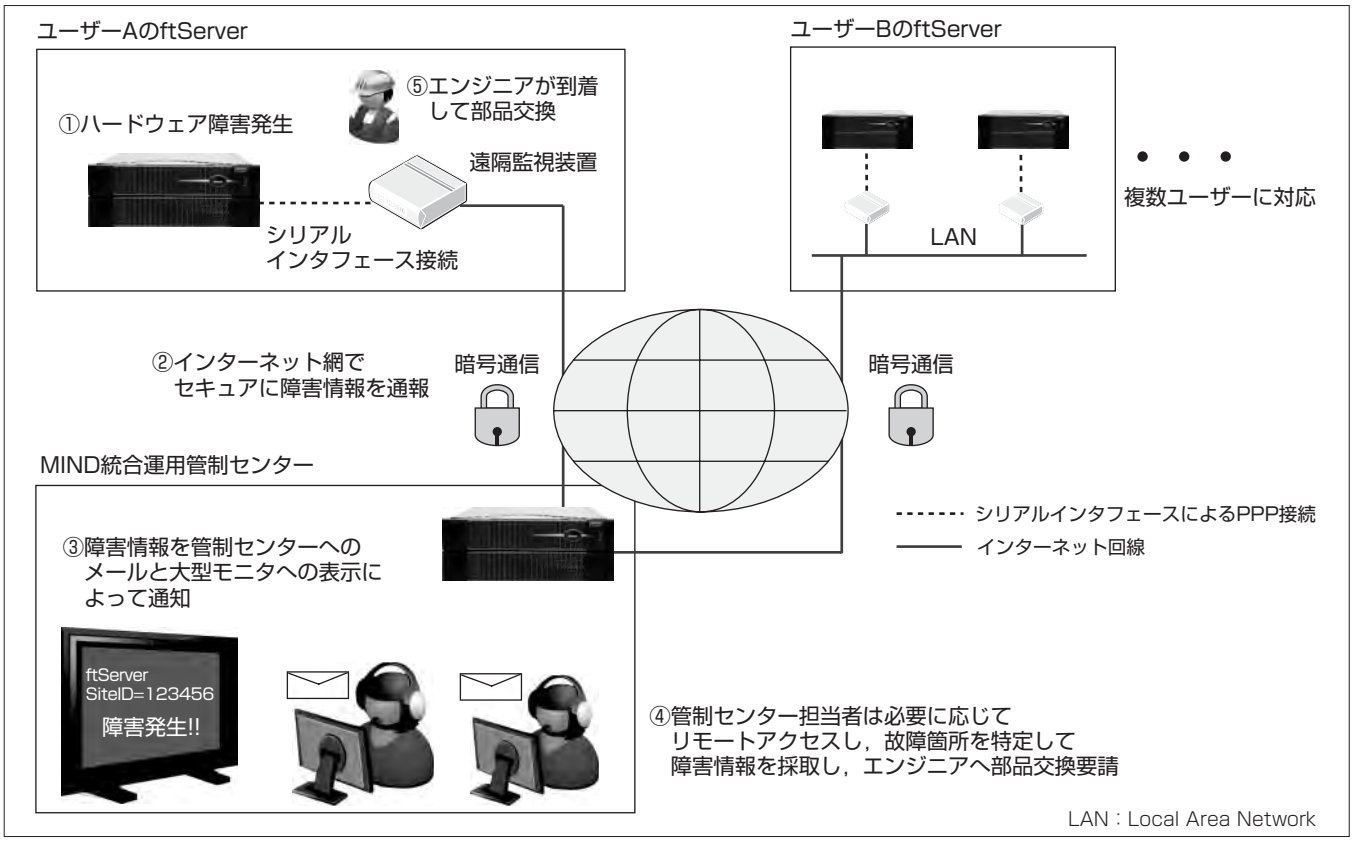
三菱電機インフォメーションネットワーク㈱(MIND)では，止められないシステムに対して無停止型サーバ“ftServer”(注1)の販売・保守を行っている。

ftServerは二重化したハードウェアが完全同期しながら動作するため，片方が故障しても動作し続けて無停止を実現している。しかし，二重故障によるシステムダウンを防ぐためには迅速なハードウェア障害の検知と故障部品の交換が重要である。MINDでは，ハードウェア障害が発生すると，電話回線を用いてMIND統合運用管制センター(以下“管制センター”という。)へ自動通報し，管制センターからリモートアクセスで診断して部品交換の手配をする仕組みを提供している。しかし専用の電話回線の敷設が必要なことや，PBX(Private Branch eXchange)を介さない回線に限られるなど，設置条件に合わない場合もあり，別の手段による仕組みを提供することが課題となっていた。

そこで公衆インターネット網を用いた遠隔監視システムを開発し，2015年2月から保守サービスを開始した。

ユーザー側にはftServerを監視するための遠隔監視装置を配置し，ftServerとシリアルインタフェースでPPP(Point-to-Point Protocol)接続することで既存のネットワーク構成に影響を与えない。また遠隔監視装置と管制センターを公衆インターネット網で接続するに当たり，公開鍵認証基盤(Public Key Infrastructure)を用いてセキュリティを担保した。ユーザー側に公衆インターネット環境さえ準備すれば，安価で容易にセキュアで高可用性を維持するための保守サービスを提供することが可能である。

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



公衆インターネット網を用いた保守サービスの流れ

遠隔監視装置からftServerのハードウェア障害をポーリング監視し，障害を検知したら管制センターに通知する。管制センター担当者はターミナルソフトウェアを用いてリモートアクセスし，故障箇所を特定して部品交換の手配をする。ユーザーが用意するものは公衆インターネット環境のみで，既存の公衆インターネット環境を流用することができる。このように容易に高可用性を維持するための保守メニューを実現した。

*三菱電機インフォメーションネットワーク㈱

1. まえがき

近年の経済活動のグローバル化や24時間化に伴い，“ミッションクリティカルアプリケーション”，つまり停止してしまうとビジネスに莫大(ばくだい)な損害をもたらす重要なアプリケーションが急増している。

そこでMINDでは，止められないシステムに対して無停止型サーバftServerの販売・保守を行っている。

MINDでは，従来の保守サービスに加え，公衆インターネット網を用いた遠隔監視システムを開発し，2015年２月からサービスを開始した。

本稿では，公衆インターネット網を用いた遠隔監視システムの実現方法等について述べる。

2. 無停止型サーバftServer

ftServerは，ミッションクリティカルなシステム，又は24時間365日稼働が必要なシステムのためにハードウェアを二重化した無停止型サーバである[(1)(2)]。特長として次の３点が挙げられる。

(1) ハードウェアの二重化による無停止の実現

1台のftServerには，CPU(Central Processing Unit)・メモリ・チップセットのモジュールとPCI(Peripheral Component Interconnect)とPCIに接続するHDD(Hard Disk Drive)やLANのモジュールからなるエンクロージャが２台内蔵されている。

この２台のエンクロージャをロックステップと呼ばれる完全同期処理によって二重化している。各エンクロージャは同期しながら同じ処理を並行して実行し，OS(Operating System)などの上位層からは１台のハードウェアが動作しているように見える。エンクロージャは互いの障害検知と故障部分の特定機能を搭載しており，万一の障害発生時には故障部分を切り離し，正常な部分で処理を継続する(**図１**)。

(2) シングルシステム同様の操作性

OS・アプリケーションは１台のハードウェアが動作しているように認識するので，OS・アプリケーションのライセンスは１つのライセンス(注2)で運用可能である。エンジニアはシステムの二重化を意識することなく容易にシステムを構築・運用することができる(**図２**)。

(3) 無停止での故障部品の交換

正常運転時は１台のサーバとして動作するが，障害発生時は故障部分をエンクロージャ単位で切り離した上で連続して動作することができる。切り離したエンクロージャはシステムを停止させることなく交換し，復旧できる(**図３**)。

ftServerは先に述べたように，ハードウェア障害が発生しても継続して処理を行うことが可能である。しかし，二重故障が発生した場合のシステムダウンを防ぐためには，障害部位をいち早く検知し，故障部品を交換して二重化状

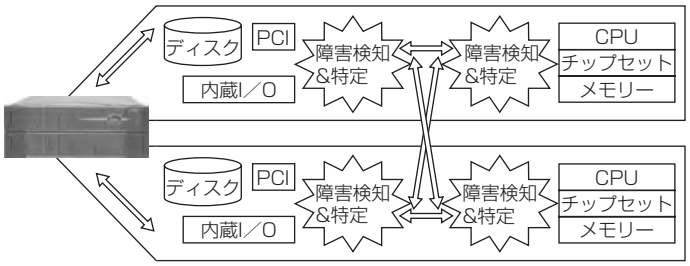


図１．ハードウェアの二重化による無停止の実現

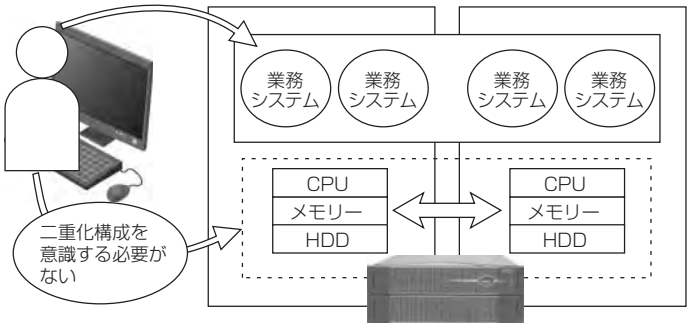


図２．シングルシステム同様の操作性

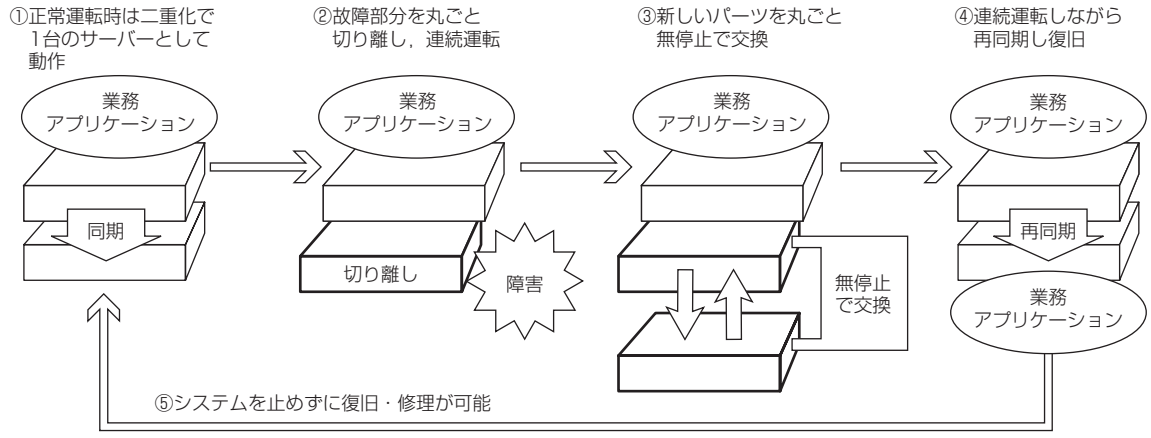


図３．無停止での交換

態へすみやかに復旧することが必要である。

（注２） アプリケーションによっては複数ライセンス必要な場合もある。

3. 公衆インターネット網を用いた遠隔監視のニーズ

MINDが従来提供している次の３つの監視の仕組みとそれぞれが抱える課題について述べる。

⑴ LEDランプの目視による監視

ftServerのフロントパネルのLED（Light Emitting Diode）を目視することによって二重化状態かハードウェア障害状態かを判別することができる。しかし，障害の発生を見落とした場合，もう一方が故障すると二重故障となりシステムダウンが発生するという課題がある。

⑵ ハードウェア障害警告機構による障害発生通知

ハードウェア障害警告機構は，サードベンダー製のネットワーク対応型警告灯とMIND製の障害検知ソフトウェアを連携させることによって，ハードウェア障害が発生すると警告音と警告灯によって障害の発生をユーザーへ伝えることができる。先に述べた⑴の方法に比べると障害の発生に気づきやすいが，警告音の聞こえる範囲や警告灯の見える範囲に制限がある。また，エンジニアがログを採取して障害部位の特定を行ってから部品の手配となるため，復旧までのリードタイムが長くかかり，この間に二重故障が発生するリスクがある。

⑶ ASNによる自動通報

ASN（ActiveService(注3) Network）はftServerのハードウェア障害を電話回線経由によって管制センターへ自動通報する仕組みである。管制センターでは，ASNによって障害が通報されるとユーザーへ障害発生の連絡をするとともに，リモートアクセスで障害解析・故障部位の特定を行って部品とエンジニアの手配を行う。このことによって，二重化状態に復旧するまでのリードタイムを短縮し，先に述べた⑴，⑵に比べ二重故障のリスクを低減することができる。

しかし，設置条件などによって電話回線を敷設できない場合があることや，敷設費用や回線固定費を懸念してASNを使用しないユーザーが増えており，導入が容易で安価な公衆インターネット網を用いたASN相当の監視が求められていた。

（注３） ActiveServiceは，Stratus Technologies Bermuda Ltd. の登録商標である。

4. 公衆インターネット網を用いた遠隔監視システム

MINDでは，ASN相当の監視のニーズを満たすための，公衆インターネット網を用いた遠隔監視システムの開発を行った。

4.1 システム構成

システム構成を**図４**に示す。

⑴ ユーザー拠点

ユーザー拠点にはftServerごとに遠隔監視装置を設置する。遠隔監視装置とftServerをシリアルインタフェースでPPP接続することでIP通信を可能とした。その際にftServerの業務用ネットワークに変更を加える必要がないようにするために，遠隔監視装置とftServerにクラスCの固定のプライベートIPアドレスを割り当てている。

遠隔監視装置に搭載された監視ソフトウェアによって監視を行い，公衆インターネット網を通じて管制センターの中継サーバへ監視結果を送信する。中継サーバとのセキュアな通信は，クライアントゲートウェイ機能を搭載することで実現した。

⑵ 管制センターの中継サーバ

管制センターの中継サーバでは，遠隔監視装置が監視しているftServerの監視結果を受信して管制センターの大型モニタを通じて管制センターの担当者に障害を通知する。

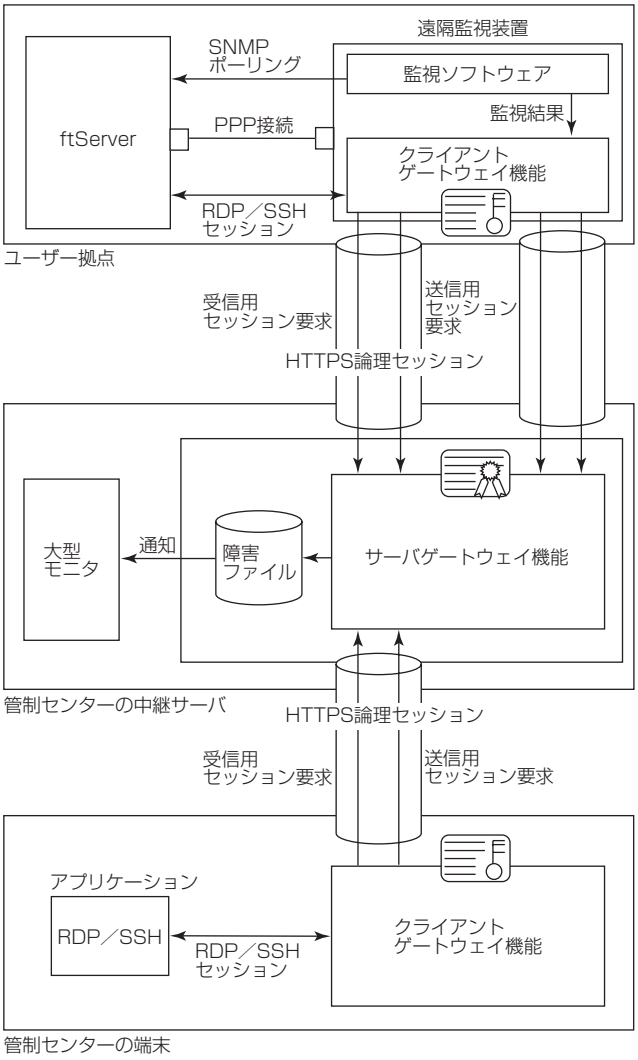


図４．システム構成

また，サーバゲートウェイ機能を搭載することで，管制センターの端末とユーザー拠点に設置した遠隔監視装置の通信をセキュアに中継することができる。

(3) 管制センターの端末

管制センターの端末はWindows(注4)端末である。管制センターの端末は，中継サーバと遠隔監視装置を経由してユーザーのftServerへアクセスすることができる。遠隔監視装置と同様に，中継サーバとのセキュアな通信は，クライアントゲートウェイ機能を搭載することで実現した。

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

4.2 監視の仕組み

遠隔監視装置にはOSとして組み込みLinux(注5)，アプリケーション基盤として組み込みJava(注6)を採用した。

監視方法は，SNMP(Simple Network Management Protocol)でポーリング監視を行うJavaアプリケーションを搭載し，シリアルインタフェースでPPP接続されたftServerに対して，SNMPでポーリング監視を実施している。監視結果は遠隔監視装置内にファイルとして記載され，CIFS(Common Internet File System)によって中継サーバと共有される。

また，遠隔監視装置は自分自身が正常に動作していることを一定時間ごとに中継サーバに報告する。このことによって，中継サーバは，遠隔監視装置から報告が途絶えた場合，遠隔監視装置自体又はユーザー拠点と管制センター間のネットワークの異常を，管制センターの担当者に通知する。

(注5) Linuxは，Linus Torvalds氏の登録商標である。
(注6) Javaは，Oracle Corp. の登録商標である。

4.3 セキュアな通信接続

公衆インターネット網を活用するに当たり，セキュリティの確保は最重要課題である。

このシステムでは公開鍵認証基盤(Public Key Infrastructure)を最大限活用することによって，遠隔監視装置，管制センターの中継サーバ及び端末間の安全な通信や確実なデバイス認証を実現した。

公開鍵認証基盤では，電子証明書の定期的な更新が必須となる。このシステムではサーバ証明書を商用認証局から1年ごとに更新する運用として，遠隔監視装置にインストールしたクライアント証明書についても1年ごとに更新する運用とした。

4.3.1 通信プロトコル

公衆インターネット網上の通信はすべてHTTPS(Hyper Text Transfer Protocol over SSL(Secure Socket Layer)/TLS(Transport Layer Security))とした。通信をHTTPSのみにすることで，次に挙げる3点のメリットが得られる。

(1) ユーザー側での導入が容易

Webブラウザで使用されている暗号通信方式であるため，公衆インターネット上のWebサイトを閲覧できるネットワーク環境があれば，ユーザー拠点のFirewallやProxyサーバ等のセキュリティのインフラに追加設定などを行うことなく導入可能である。

(2) 中継サーバのシンプルなセキュリティ設計

中継サーバはHTTPSに対応したポート(443/tcp)のみを接続許可し，その他のポートは接続を禁止する設定にすれば良い。また，HTTPSが持つ接続先検証や認証の仕組みを利用できる。

(3) 効率的な開発

このシステムでは，HTTPS関連のライブラリとして，遠隔監視装置では組み込み用Java，管制センターのWindows端末では.NET Framework(注7)を採用し，中継サーバではIIS(Internet Information Server)(注7)のライブラリを採用した。Java，.NET Framework及びIISは世間一般で広く利用されているため，各ベンダーから提供される新たな暗号方式や脆弱(ぜいじゃく)性対策モジュールに対して迅速に対応できる。

(注7) .NET FrameworkとIISは，Microsoft Corp. の登録商標である。

4.3.2 ゲートウェイ機能

先に述べたように通信プロトコルとしてHTTPSを採用したが，HTTPSはリクエスト・レスポンス型のプロトコルであるため，双方向通信を行うRDPやSSHなどのプロトコルには向かない特性がある。

この点については，**図4**に示すように，クライアントゲートウェイで，1つのアプリケーションの通信に対して送信用のHTTPSセッションと受信用のHTTPSセッションを張り，2本のセッションを束ねて論理的な1本の双方向通信のセッションとすることで解決した。この論理的なセッションの上で，このシステムに必要なRDP・SSH・CIFS・SMTP(Simple Mail Transfer Protocol)の各プロトコルのデータをHTTPSデータに載せ，中継サーバと通信している。

サーバゲートウェイは，クライアントゲートウェイから送信されるHTTPSデータから各プロトコルのデータを取り出し，各プロトコルに対応した処理を行う。例えば，RDPやSSHの場合は接続先のクライアントゲートウェイに対して再度HTTPSデータにRDPやSSHのデータを載せてデータを中継する。

接続先のクライアントゲートウェイは，サーバゲートウェイから送信されたHTTPSデータから，各プロトコルのデータを取り出し，対応するアプリケーションへ送信する。

4.3.3 デバイス認証

もう1つの重要なセキュリティ面の課題は，不正なデバイスによる接続防止である。このシステムでは，クライアント証明書及びデバイスID(IDentification)を用いた2要素認証を採用している。

ftServerには，ユニークなサイトIDが割り当てられ，こ

のサイトIDをCN(Common Name)としてクライアント証明書が発行される。クライアント証明書は，工場出荷時に遠隔監視装置にインストールされるとともに中継サーバに記録される。

デバイスIDは，遠隔監視装置の工場出荷時にキーとしてランダム値が発行され，中継サーバに記録される。遠隔監視装置と中継サーバが通信を開始する際には，クライアント証明書とデバイスIDによる認証が行われ，どちらか一方でも異なる場合は通信できない。管制センターの端末も同様である。

さらに管制センターからは，リモートデスクトップやターミナルソフトウェアで，CNを含むホスト名指定での接続操作を可能とした。

4.4 遠隔監視装置へのモジュール自動配布

各ベンダーから提供される脆弱性対策モジュールを迅速に配布する方法や，クライアント証明書を1年ごとに配布する仕組みが必要となり，このシステムではモジュールの自動配布の仕組みを開発した。モジュールを配布する場合は，中継サーバにこのシステムの配布規則に則(のっと)ったモジュールを配置すると，遠隔監視装置はそれを検知し，適用可否を判断した上でモジュールのダウンロードとインストールが実施される。それによって，ユーザー操作は不要となり，迅速にモジュールの適用が可能となり，最新の状態を維持することができる。

5. むすび

無停止型サーバftServerの公衆インターネット網を用いた遠隔監視システムの実現方法について述べた。

この開発によって，ユーザーの既存の業務ネットワーク環境に影響を与えず，かつ既存の公衆インターネット環境を活用することで，安価で容易にセキュアで高可用性を維持するための保守サービスを提供することが可能となった。

この開発ではftServerを対象とした監視システムとなっているが，遠隔監視装置に搭載する監視ソフトウェアの仕組みを変更すれば他製品への応用も可能と考えている。

今後はこのシステムの適用の拡大を検討していく。

参考文献

(1) 平島栄一，ほか：無停止型サーバによるCC-Link IEコントローラネットワークの高信頼化，三菱電機技報，**88**，No. 8，481～484（2014）
(2) 三菱電機インフォメーションネットワーク㈱：フォールトトレラント・サーバ
http://www.mind.co.jp/businessplatform/ftserver/index.html