特集論文

MIND統合運用管制システムの二拠点化

本部祐史* 山田耕一**
生駒健二郎*
古川良寛*

Disaster Recovery System of MIND ICC Operation

Yuji Honbu, Kenjiro Ikoma, Yoshihiro Furukawa, Koichi Yamada

要 旨

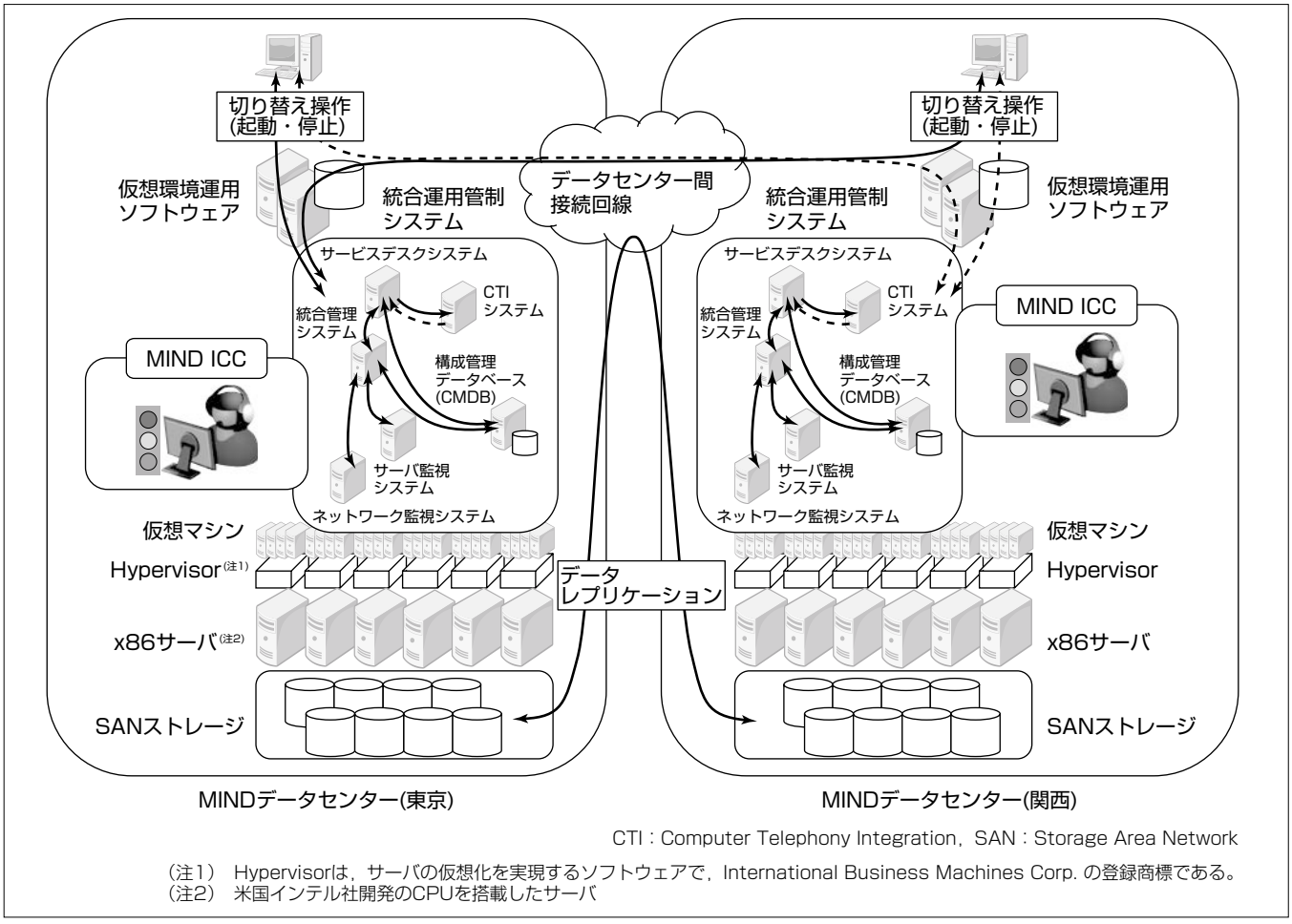
三菱電機情報ネットワーク㈱(MIND)の統合運用管制センター(MIND ICC)では，顧客のICT(Information and Communication Technology)システムの24時間365日の監視運用サービスを提供している。そのMIND ICCの円滑な業務遂行を支えているのが統合運用管制システムである。

従来，統合運用管制システムはMINDの東京都内のデータセンター内に設置しており，災害などによって，万一，システムの監視機能が停止するとMIND ICCの監視運用サービスを顧客へ提供できなくなってしまう恐れがあった。

東日本大震災の発生に始まり，首都直下型地震発生リスクの高まりを受け，MIND ICCでは，顧客が継続的に安心して監視運用サービスを利用できるよう，関西にあるデータセンターに統合運用管制システムのDR(Disaster Recovery)システムを構築し，2013年1月から運用を開始している。

また，並行して，実効性のあるBCP(Business Continuity Plan)の維持を目的とした事業継続管理(BCM：Business Continuity Management)規程を策定した。その規程に沿って，有事の際，限られた人員と時間でスムーズにシステムを切り替えて，サービスを再開するための定期的な要員の教育・訓練を日々行っている。

MIND ICCでは，システムと人の両面で磐石(ばんじゃく)な災害対策を実現し，顧客のICTシステムの監視運用サービスの安定的な提供を今後とも目指していく。



CTI：Computer Telephony Integration，SAN：Storage Area Network

(注1) Hypervisorは，サーバの仮想化を実現するソフトウェアで，International Business Machines Corp. の登録商標である。
(注2) 米国インテル社開発のCPUを搭載したサーバ

MIND統合運用管制システムの全体イメージ

統合運用管制システムは，通常，東京のデータセンターの仮想マシン上で稼働しており，東京，関西のMIND ICCのどちらからでも起動，停止を行うことができる。有事の際は，BCM規程に従って，操作可能なデータセンターから容易に切替え操作を行い，MIND ICCの監視運用サービスを顧客へ継続して提供することが可能なシステム構成になっている。

 *三菱電機情報ネットワーク㈱ **三菱電機㈱ 情報技術総合研究所

1. まえがき

MIND ICCでは，データセンター，ネットワーク，サーバ，セキュリティからアプリケーションに至るまで，顧客のICTシステムに対して24時間365日の高度な監視運用サービスを提供している。そのMIND ICCの日々の円滑な業務遂行を支えているのが統合運用管制システムである。

本稿では，この統合運用管制システムのDRシステムの構築，及び業務に従事する要員向けに策定した有事の際のBCM規程について述べる。

2. 開発の目的と方針

2.1 背景と目的

2011年3月11日東北地方を中心に太平洋沿岸に被害をもたらした東日本大震災の発生に始まり，首都直下型地震発生のリスクも高まっている。このような状況下で，三菱電機㈱では東京，関西のデータセンター内に，それぞれ基幹システムのメインシステムとDRシステムを構築するという二拠点化プロジェクトに着工した。これに合わせてMINDでは，どんな時でも顧客が安心して監視運用サービスを利用できる基盤・組織づくりを目指して，統合運用管制システムのDRシステムの構築プロジェクトを立ち上げた。

2.2 構築要件

統合運用管制システムのDRシステム構築に当たり，次の5点を要件として打ち出し，まずは三菱電機㈱の二拠点化される基幹システムを対象として要件検討を実施した。

⑴ 関西のデータセンター内にあるMIND ICCで，DRシステムを使って監視運用サービスを継続する。

⑵ 首都直下型地震によって，電力が1週間，通信が2週間停止する被害を想定する。

⑶ RTO(Recovery Time Objective)：4時間未満，RPO(Recovery Point Objective)：被災直前を目標とする(三菱電機㈱二拠点化システムの要件を考慮)。

⑷ 2012年6月に構築を開始し，三菱電機㈱の二拠点化システムが稼働する2013年1月までの6か月間でDRシステムを構築する。

⑸ 有事の際，管理者と連絡が取れなくても，東西のMIND ICCのオペレータが自立的にDRシステムへ切り替えることができる。

3. 統合運用管制システムの二拠点化

3.1 システムの構成と基本機能

現在の統合運用管制システムは，セキュリティレベルと可用性の高いMINDの東京のデータセンターに設置され，ITサービス管理のベストプラクティスを包括したデファクトスタンダードであるITIL(Information Technology Infrastructure Library)に基づき，監視運用業務の標準化・自動化を図り，2006年8月に稼働したシステムである。以降，今日に至るまで様々な機能拡張を行っている。統合運用管制システムは，主に次の6つのサブシステムから構成され，これらのサブシステムが相互に密接に連携することで，オペレータ作業の自動化，効率化を図るとともに，MIND ICCの円滑な業務遂行を支えている(**図1**)。

⑴ ネットワーク監視システム

ネットワーク監視システムは，マルチベンダーの多種多様のネットワーク機器を対象として，PING(Packet Internet Groper)による死活監視，トラップ監視，性能監視等を行う。

⑵ サーバ監視システム

サーバ監視システムは，マルチベンダー，マルチOSのサーバ機器を対象として，PINGによる死活監視，ポート監視，リソース監視，ログ監視，性能監視等を行う。

⑶ 統合管理システム

統合管理システムは，それぞれの監視システムで検知したアラート(注3)を一元的に管理し，構成管理データベース(Configuration Management Database System：CMDB)と連携することでアラートの影響を受ける顧客，システム，アラートの重要度，影響度等の判別を行う。

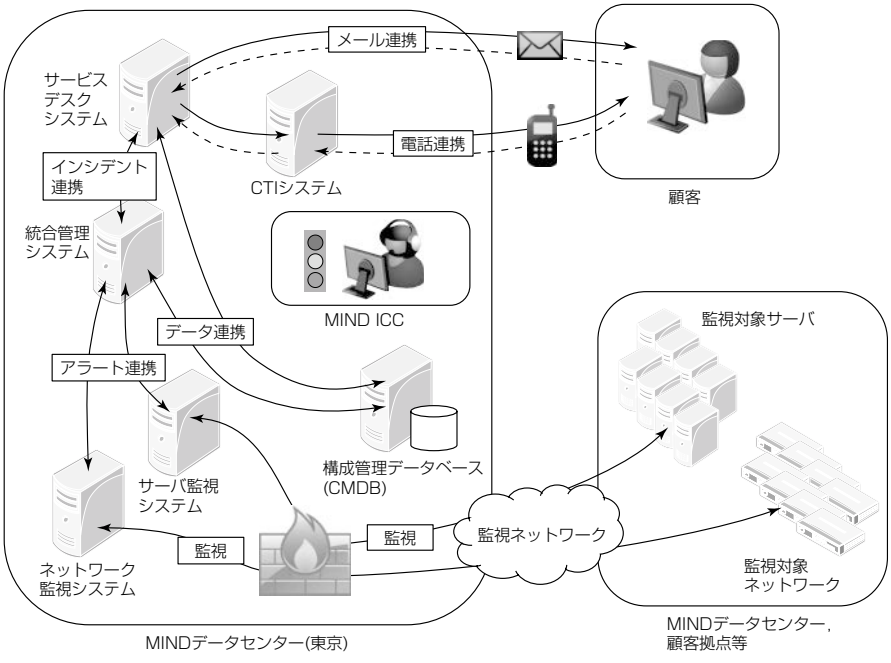


図1．統合運用管制システム構成

⑷ CTIシステム

CTIシステムは，電話の受発信を管理し，担当オペレータへの電話着信の振り分け，音声ガイダンスの発信を行う。

⑸ サービスデスクシステム

サービスデスクシステムは，統合管理システム，CTIシステム，CMDBと連携し，全ての検知アラート，及び電話やメールによる顧客からの問合せをインシデントとして管理し，担当オペレータへのインシデントの振り分け，専門部隊へのエスカレーション，インシデントの対処状況等の一元管理を行う。

⑹ 構成管理データベース(CMDB)

CMDBでは，ネットワーク機器，サーバ機器，顧客情報，運用情報等，監視運用サービスを提供するために必要な情報の一元管理を行う。

(注３) 注意，警告を促す表示，通知メッセージ

3.2 二拠点化実現に向けたVPOサービスの採用

東京のデータセンターで稼働しているこれらのメインシステムと同等のDRシステムを直線距離で約400km離れた関西のデータセンターに短期間で構築し，いつ発生するか分からない災害に備えて，DRシステムを維持し続けるためには，サーバの移行や再構築を容易に行うことができるサーバの仮想化技術と，高速かつ確実なデータレプリケーション技術の適用が有効である。

また，災害発生時に，システムに精通したシステム管理者と連絡が取れないことを想定して，誰でも容易にDRシステムへ切り替えられるように運用支援ツール，自動オペレーションの仕組みを導入しておくことが必須である。さらに，MIND ICCは24時間365日のサービスを提供していることから高い可用性を実現する必要がある。

これらの統合運用管制システムの二拠点化の実現に必要不可欠な要件を満たすため，MINDが提供するIaaS(Infrastructure as a Service)型プラットフォームサービス“Value Platform on Demand”(VPOサービス)を採用した。MINDのVPOサービスは，サーバ，ストレージ，ネットワークといった物理的なインフラストラクチャの提供から，複数のデータセンターに跨(またが)る仮想化されたシステム構成にも対応しており，二拠点化が前提となる今回のプロジェクトの要件に合致するものである。

3.3 VPOサービスの適用方式

VPOサービスの適用に当たっては，統合運用管制システムに求められる高い可用性の実現と，短期間での構築という要件を満たすために次の**3.3.1項，3.3.2項**に示す通り，ハードウェア，及びソフトウェアはMIND ICC専用の設備と他のユーザーも使用している共用設備を適材適所に配置し，プライベートクラウド環境を構築するという方式を採用することとした。

3.3.1 専用設備

⑴ 仮想サーバ(x86サーバとHypervisor)

メインシステム，DRシステムのインフラ基盤となる仮想サーバである。可用性と他のユーザーとは独立したメンテナンス性を向上させるために専用設備とした。

⑵ 仮想環境運用ソフトウェア

DRシステムへの切替え発動時の容易な操作をサポートする運用ソフトウェアである。今回のプロジェクトの方針，要件を満たすためには，他のユーザーとは独立して切り替え，監視運用サービスを再開させる必要があるため専用設備とした。

3.3.2 共用設備

⑴ SANストレージ

仮想マシンを保管するSANストレージである。オンデマンド(注4)性，将来的な拡張性を考慮した仕組みが確立している共用設備を利用することとした。また，複数のSANストレージ間でのデータレプリケーション機能を持っている。

⑵ データセンター間接続回線(データレプリケーション)

東西のデータセンター間でSANストレージ内のデータを同期するための回線である。実績のある共用の10GBの広域回線を利用することとした。

(注４) 要求に応じてサービスを提供すること

3.4 システムの構築手順

システムの構築手順は次のとおりである。

⑴ MINDのVPOサービスを活用して，東京のデータセンターにメインシステム用，関西のデータセンターにDRシステム用のプライベートクラウド環境を構築した(**図2**)。

⑵ 共用の10Gbpsの広域回線を使って，ほぼリアルタイムに東西のSANストレージ内のデータレプリケーションを実現できる環境を構築した。

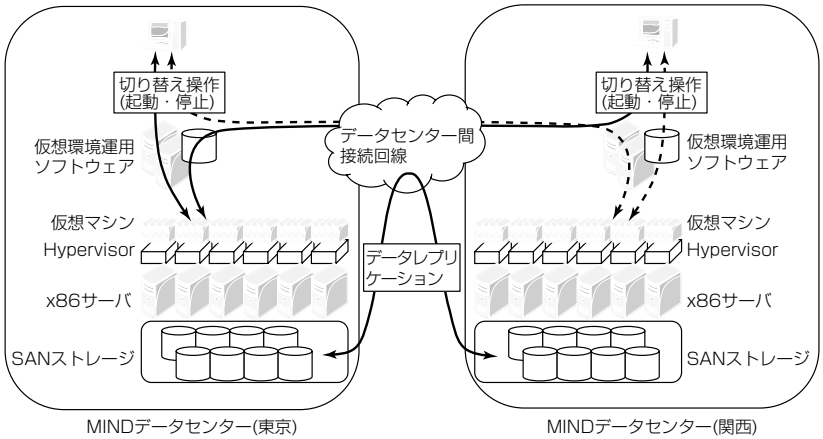


図2．VPOサービスを活用したプライベートクラウド環境

⑶ 東京のメインシステムを順次プライベートクラウド環境に移行，又は再構築した。この時点でSANストレージのレプリケーション機能によって，東京側のメインシステムのデータイメージが関西側にレプリケーションされ，DRシステムのデータイメージが完成した。

⑷ 仮想環境運用ソフトウェアや自動オペレーションツールを使って，東京側のメインシステムの停止，関西側のDRシステムの起動，切替えが東西のMIND ICCのどちらからでも容易に実行できることを確認し，システム構築を完了した。

3.5 VPOサービス適用のメリット

VPOサービスの適用によって，6つのサブシステムから構成される大規模なシステム構築作業をわずか6か月で完遂することができた。また，“RTO：2時間，RPO：被災直前”を実現して目標を達成できた。VPOサービスは，事前検証によって，サーバ，ストレージ等の設備，構成アイテムの互換性が確保されており，また，その構築手順が確立されているため，オンプレミスで構築するよりも初動コストと構築期間を低減し，かつシステムの堅牢（けんろう）性向上を図ることができる。

一方，運用面では，従来MIND ICCのシステム開発者がサーバ，ネットワークの管理も合わせて行っていたが，その管理をより専門性の高いIaaS運営のエキスパートがサポートすることによって，MIND ICCではサーバ，ネットワーク管理に関わる作業負荷を低減することができ，本来の専門分野である統合運用管制システムの開発，維持に注力することができるようになる。

4. BCM規程

有事の際，限られた人員と時間でスムーズにシステムを切り替えて，サービスを再開するとともに，実効性のあるBCPを継続的に改善していく事業継続管理（BCM）が必要であると考え，MIND ICCでは，独自のBCM規程を策定した。現在，定期的に事業環境とBCPの適合性を確認，見直しを検討するPDCA（Plan，Do，Check，Act）活動を実施している。

BCM規程には，主に次のような指針を定めている。

⑴ 被災想定

被災想定は，管理者不在の休日夜間に，首都圏で震度6弱以上の大震災が発生し，東京都内にあるMINDのデータセンターが全て利用できない状況を想定した。また，メインシステムが設置されているデータセンターは，電力供給が停止し，被災から15時間で非常用電源も停止することを前提としている。

⑵ 災害時基本行動指針

災害時基本行動指針は，従業員及び家族の健康・安全の維持・確保を第1とし，次に顧客への影響の最小化，最後にMINDの経済的被害の最小化と続く。また判断に迷った場合は，刑法，企業理念，基本方針に反する行為，それが周知の事実となった場合に，会社又は個人が批判を受ける可能性のある行為でなければ，個人の判断で行動することを認めている。

⑶ 災害対応

災害対応（DRシステム切替え）は，災害が発生してからDRシステムへの切替えが完了するまでの体制・役割，フローを記載している。従業員及び家族の健康・安全の維持・確保を行った上で，管理者と連絡が取れない場合でも，東西のMIND ICCのオペレータが自立的に判断し，非常用電源が停止するまでに，仮想環境運用ソフトウェアなどを利用し，手順書に従って作業するだけで，メインシステムの停止，DRシステムの起動を実行できるようになっている。

⑷ 復旧対応

復旧対応（メインシステムへの切り戻し）は，災害発生後の状況に左右されるため，事前の計画策定は困難である。したがって，切り替え後に，メインシステムの状況，電力供給，通信，公共交通機関等，社会インフラの復旧状況，人員，体制の状況，リスク，顧客システムの稼働見込み等を考慮し，経営層の意思を確認した上で時期を決定し，復旧計画を策定，実行することを記載している。

⑸ BCMライフサイクル

実効性のあるBCPとするためには，平常時の教育，事業継続訓練等の活動を通して，ビジネス状況，事業継続を取り巻く環境の変化に対応できるよう，定期的にビジネスとBCPの適合性の確認を行い，必要に応じて，被災想定，対象業務，RPO，RTOの見直しを行うことを記載している。

5. むすび

現在も継続して，BCPに関する教育，訓練，マネジメントレビュー等の事業継続管理活動を行うとともに，三菱電機㈱の関係会社などの顧客システムへの展開など，二拠点化対象システムの適用範囲拡大を推進している。

MIND ICCは，システムと人の両面で磐石な災害対策を実現し，顧客のICTシステムの監視運用サービスの安定的な提供を今後とも目指す所存である。

参考文献

⑴ 猪股義晴，ほか：サービスレベルと信頼性を向上させた新統合管制センターによるITILプロアクティブ運用管理サービスソリューション，三菱電機技報，**80**，No.4，289～292（2006）