

セキュリティ強化と運用効率化を実現する グローバルウェブサイト統合基盤

野間口元輔*
桜井 剛*
中根史香*

Global Website Integrated Base for Realizing Enhanced Security and Efficient Operation

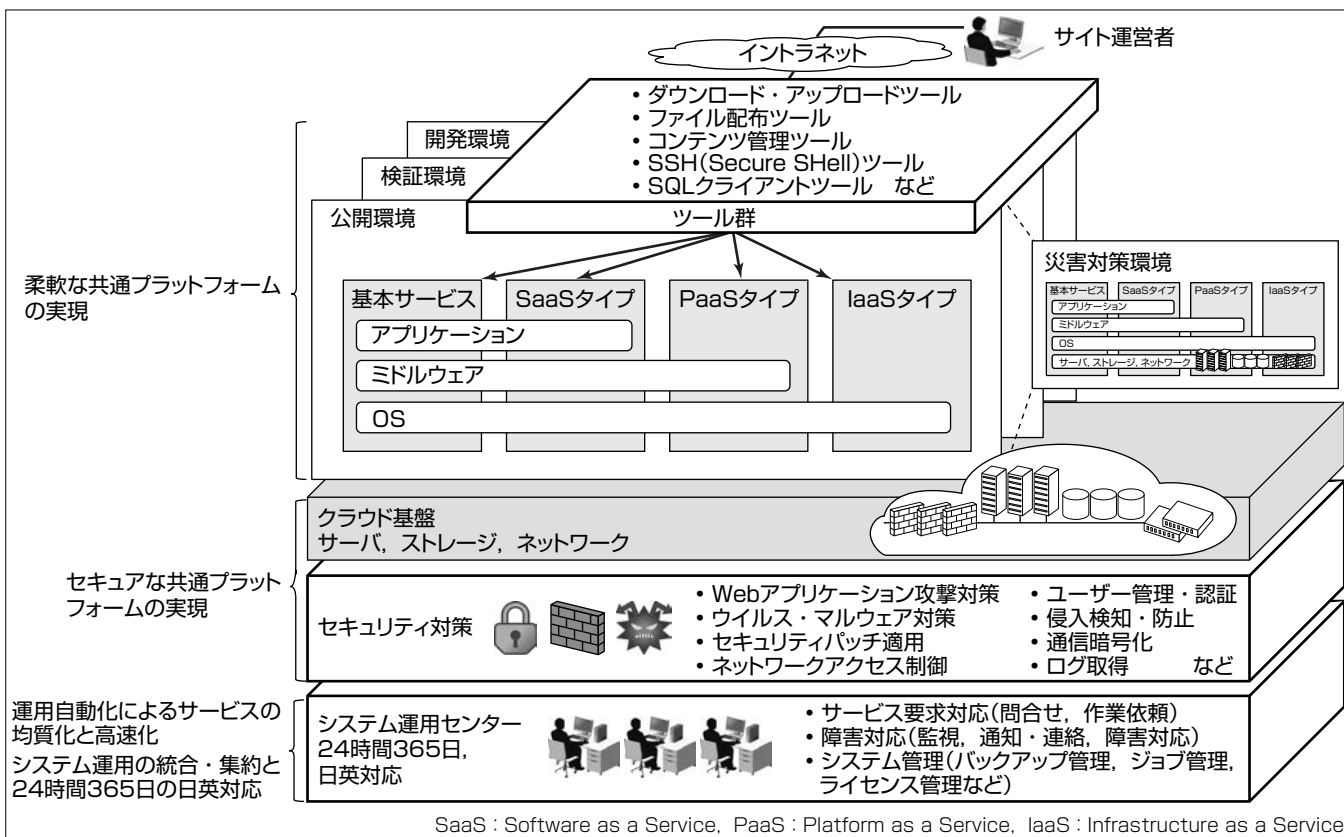
Gensuke Nomaguchi, Tsuyoshi Sakurai, Fumitaka Nakane

要 旨

企業のウェブサイトは様々な情報を発信可能であるとともに、顧客と直接つながる窓口としても欠かせない存在となっており、企業活動や事業活動の基盤としてその重要性はますます高まっている。三菱電機グループ国内外各社(以下“グループ各社”という。)でもウェブサイトは様々な企業活動、事業活動に活用されており、今後ますます利用範囲の増大と利用用途の多様化が見込まれる。

一方で、インターネット上の脅威は年々高まっており、ウェブサイトへの攻撃や内部データ流出などのセキュリティリスクを抱える中、グループ各社ではセキュリティ対策レベルの地域差、独自にシステム運用やセキュリティ対策を実施していることによるシステム運用の非効率性が生じている。三菱電機の宣伝部(以下“宣伝部”という。)はこ

の課題に対応するために、セキュリティ技術やクラウド技術を活用し、様々な利用形態に対応するための柔軟かつセキュアな共通プラットフォーム(グローバルウェブサイト統合基盤)を構築し、グループ各社へのサービス提供を開始している。グループ各社の数百のウェブサイトを同時に運営しながら、サイト運営者からの構成変更やシステム運用に対する要望に迅速かつ高品質で応えるため、三菱電機インフォメーションシステムズ(株)(MDIS)では、運用自動化を導入するとともに、システム運用センターによるグローバルなシステム運用の統合・集約と24時間365日の日英対応(日本語/英語対応)を行うことで、提供するサービスの均質化とサービス提供の高速化を実現した。



SaaS : Software as a Service, PaaS : Platform as a Service, IaaS : Infrastructure as a Service

グローバルウェブサイト統合基盤のシステム

グローバルウェブサイト統合基盤では、クラウド技術を活用し、OS(Operating System)/ミドルウェア/アプリケーションの種類や必要数を自由に選択できるサービスを提供する。柔軟な拡張性ととも、三菱電機要求基準を満たすセキュリティと内部統制のための機能を標準実装するなど一般のクラウドサービスにはない機能に対応している。システム運用センターによるグローバルなシステム運用の統合・集約を実現し、24時間365日の日英対応での運用支援を行っている。

1. ま え が き

三菱電機ウェブサイト⁽¹⁾は宣伝部が主体となって先進技術を取り入れつつ、様々な企画や施策を実行して進化するとともに⁽²⁾⁽³⁾、ビジネス拡大を促進するツールとしての活用を推進している。一方、グループ各社でもウェブサイトを経営する様々な企業活動、事業活動に活用しているが、各社が独自にセキュリティ対策を実施しているため対策レベルに差が出るとともに、システム運用の非効率性が生じている。これらの課題に対応するために、宣伝部は様々な利用形態に対応するための柔軟かつセキュアな共通プラットフォーム(グローバルウェブサイト統合基盤)を構築・提供してグループ各社に広く展開することで、グループ全体としてのシステム運用の効率化、及びセキュリティレベルの向上を図っている。MDISでは、このグローバルウェブサイト統合基盤を構築し、サービスの均質化とサービス提供の高速化を実現した。

本稿では、グループ各社向けに提供を開始したグローバルウェブサイト統合基盤について述べる。

2. 現状の課題

2.1 プラットフォーム統合への要求

グループ各社で運営されているウェブサイトは、各社が独自にセキュリティ対策を実施しているため、対策レベルに差が出るとともに、システム運用が非効率になっている。そこで、グループ各社のウェブサイトを経営するためにセキュアなプラットフォームに統合するとともに、システム運用業務を集中化してシステム運用の効率化を図っていく必要がある。また、利用用途の多様化や最新技術導入に応えることのできる柔軟なプラットフォームであることが求められている。

2.2 現状の課題

プラットフォーム統合推進のためには、グループ各社での次の課題を解決する必要がある。

- (1) 新しいニーズやサイト統合の要望に応えるため、機能拡張が容易で、最新技術の搭載に対応する必要がある。
- (2) 利用用途に応じたOS/ミドルウェア/アプリケーションの種類や必要数などを柔軟に拡張できる必要がある。
- (3) 国・地域で対策レベルに違いがあり、高度化するサイバー攻撃によるセキュリティ事故が起きる可能性があるが、そのリスクを最低限まで減らす必要がある。
- (4) グループ各社が独自にシステム運用やセキュリティ対策を実施していることによって、グループ全体としてみるとシステム運用が非効率となっている。

3. 対 応 策

2.2節で述べた課題に対応できるプラットフォームにす

るため、クラウド技術を活用し、OS/ミドルウェア/アプリケーションの種類や必要数を自由に選択できる柔軟なサービスを提供するためにSaaS/PaaS/IaaSの各基盤を整備し、統合を容易にするための柔軟な拡張性を確保した。さらに、一般的なセキュリティ対策はもちろんのこと、全てのサービスに対して三菱電機要求基準を満たすOS環境と専用設計ミドルウェアを搭載し、内部統制のための機能を標準実装するなど一般のクラウドサービスでは提供されない機能にも対応した。これによって、様々なサービス形態に対応する柔軟かつセキュアな共通プラットフォームを実現した。三菱電機要求基準を満たすセキュリティを確保しながら、ウェブサイトにも最適化されたプラットフォームを柔軟に組み合わせて提供できるのは、他社にはない独自の技術である。また、数百のサイトを同時に運用しながら、グループ各社のシステム運用の要望に迅速かつ高品質で応える必要があり、運用自動化によるサービスの均質化と高速化を実現した。さらに、グローバルにシステム運用を統合化する必要があったため、統合運用センターとなるシステム運用センターを設置し、システム運用の統合・集約と24時間365日の日英対応を実現した。

3.1 柔軟な共通プラットフォームの実現

従来は、利用用途に応じた設定変更を行うたびにウェブシステム全体の影響確認を行う必要があり、頻繁なシステム設定の変更が難しく、柔軟性の確保が困難であった。これに対し、プラットフォーム全体の設定とサイト固有の設定を階層化する設計としたことで、サイト固有の設定変更による影響を局所化した。その結果、サイト運営者からの設定変更ニーズに柔軟に応えることが可能となった。

3.2 セキュアな共通プラットフォームの実現

グループ各社に対してセキュアな共通プラットフォームを提供するため、ネットワークや利用者環境におけるセキュリティ強化や、ある利用者の影響がほかの利用者に及ばないように利用者ごとの影響を分離するための対策を施した。次に、その対策内容を述べる。

3.2.1 セキュアな共通プラットフォームの提供

セキュアな共通プラットフォームを提供するために、ファイアウォール(FW)やウイルス対策ソフトウェアに加え、WAF(Web Application Firewall)を導入してウェブアプリケーションの脆弱(ぜいじゃく)性への対策を図るとともに、IPS(Intrusion Prevention System)を導入して外部ネットワークからの攻撃や不正アクセスへの対策を実施し、セキュリティの高度化を実現した。また、アクセスログ保持期間の設定やセキュリティポリシー等は、三菱電機要求基準にのっとり設定し、各アプリケーションのアクセスログを集約して一元管理する等の仕組みを導入した。さらに、プラットフォームでのネットワークセグメントを環境(公開・検証・開発等)及び機能(ウェブ・アプリケー

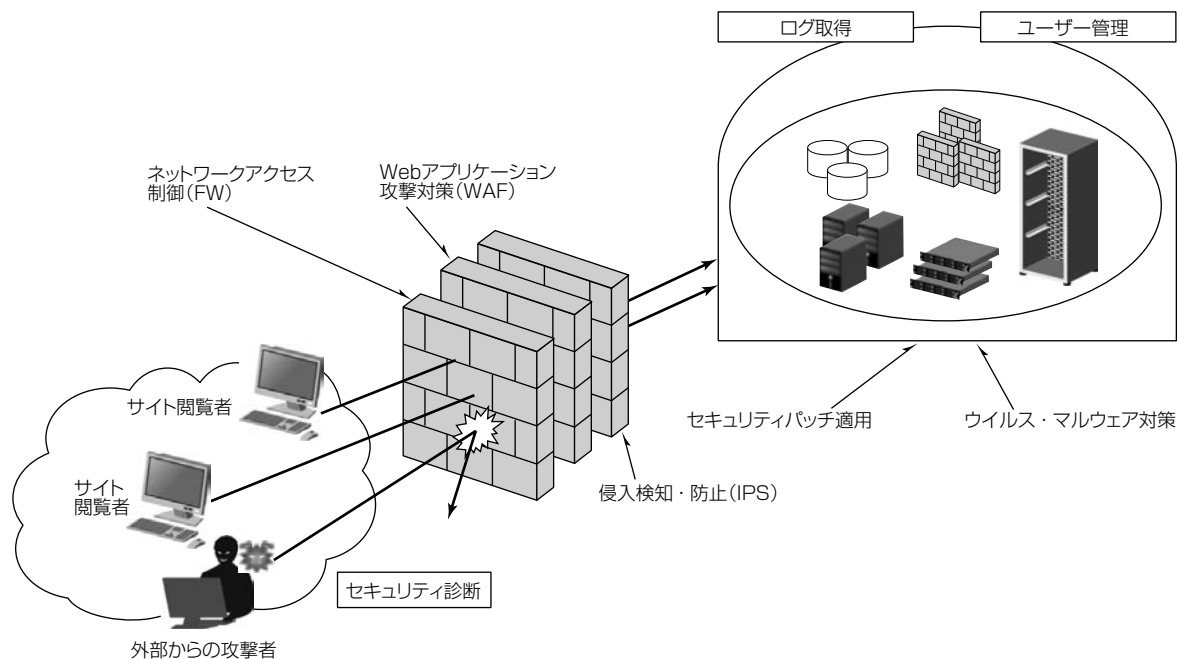


図1. セキュリティ構成

ション・データベース等)ごとに細分化し、環境間でのアクセスを必要最小限にすることでセキュリティの高度化を図るとともに、定期的なセキュリティ診断やセキュリティパッチの適用を行うことでセキュアな共通プラットフォームの提供を実現した(図1)。

3.2.2 サービス利用環境の一元化

サイト運営者の端末からプラットフォームへのアクセスは直接行わず、Windows Server 2012 R2^(注1)のリモートデスクトップサービス^(注2)(4)機能を利用してサービス利用時のアクセス経路を一元化させた。また、システム操作点検・監査ソリューション(ESS REC^(注3))を導入することで、操作証跡の取得や禁止操作に対する抑止力を高めることが可能となり、セキュリティレベルの均一化を実現した。

(注1) Windows Server 2012 R2は、Microsoft Corp.の登録商標である。

(注2) Windows ServerでMicrosoft Corp.が提供しているRemote Desktop Protocolのサーバサービス。

(注3) ESS RECは、エンカレッジ・テクノロジー株の登録商標である。

3.2.3 利用者ごとの影響を分離したプラットフォームの提供

グループ各社が利用する際の利用者ごとの相互の影響を最小限に抑えるため、リソースプール機能を用いて、ITリソースの分離・ストレージ及びネットワークI/Oの制限・ネットワークによるアクセス制限等を実装した。これらの対処によって、リソース利用過多や誤操作等による利用者ごとの影響を分離したセキュアなプラットフォームの提供を実現した。

3.3 運用自動化によるサービスの均質化と高速化

3.3.1 運用自動化の必要性

グループ各社全体では数百のウェブサイトが様々な利用

用途で存在しているが、これらをグローバルウェブサイト統合基盤に統合して全て同時にシステム運用を行っていくためには、サービス利用者ごとの構成やシステム運用依頼に対する対応履歴など多岐にわたる管理要素を常に最新化しておくことが重要であるが、管理要素の維持には非常に手間がかかることが予想された。一方、ウェブシステムの特性上、サービス利用者からの設定変更の要望やセキュリティパッチの適用などが頻繁に発生する中、サービス品質を維持しつつシステム停止時間を最小限に抑えながら対応することが求められており、これらを同時に実現するためには運用の自動化は必須であった。以前はこれらを1台1台手動で対応していたため、膨大な時間を必要とし、さらにサービス品質が運用者のスキルに依存していたが、自動化を実現して作業を均質・高速化することによって、数百のウェブサイトを同時に運営することが可能となる。また、OS/ミドルウェア/アプリケーションの種類や必要数、及びCPUやメモリなどリソースの柔軟な拡張性を確保するためには、拡張に合わせてライセンスなどの費用が発生するシステム構成になることを回避する必要があった。

3.3.2 運用自動化の実現

運用の自動化に当たっては図2に示す各種ツールを選定し採用した。ツールの選定に当たってはOSS(Open-Source Software)を中心に選択することによって、ライセンス料を発生させることなく、低コストでOS/ミドルウェア/アプリケーションの種類や必要数、及びCPUやメモリなどのリソースを拡張することも同時に実現した。

運用管理ツールにはRedmineを採用して、サービス利用者からのシステム運用依頼に対する対応履歴、及び発生障害・障害予兆事象に対する対応履歴の管理を行う。

OS・ミドルウェアの構成変更、アプリケーション更新に伴う構成変更の管理はGitlab^(注4)(バージョン管理)／Jenkins(作業自動化)／Ansible^(注5)(環境構築自動化)を連携させることで実現し、実行結果を自動でRedmineへ反映することによって、一元管理を行う。一方、ハードウェア、ミドルウェアの監視はZabbix^(注6)に集約し、Zabbixでの監視結果もRedmineに反映するようにした。これによって、グローバルウェブサイト統合基盤上の全ての構成情報・構成変更情報をRedmine上で一元的に管理することを可能にしている。なお、これらの運用自動化のためのツール類は、3.4節に述べるシステム運用センターの中核機能として位置付けられている。

(注4) GitLabは、GitLab B.V.の登録商標である。
 (注5) Ansibleは、Red Hat, Inc.の登録商標である。
 (注6) Zabbixは、Zabbix LLCの登録商標である。

3.4 システム運用センターによるシステム運用の統合・集約と24時間365日の日英対応

この節ではグループ各社のシステム運用を統合・集約し、24時間365日の日英対応を行うシステム運用センターの実現に際し、重要なポイントとなった手法について述べる。

3.4.1 システム運用の統合・集約

各社のウェブサイトは利用用途の多様化が進んでおり、サイト運営のために必要なシステム運用は多種多様である。そのため、統合・集約に際して重要なポイントと考えたのは、サイト運営の様々な要望を吸い上げ、迅速なサービス

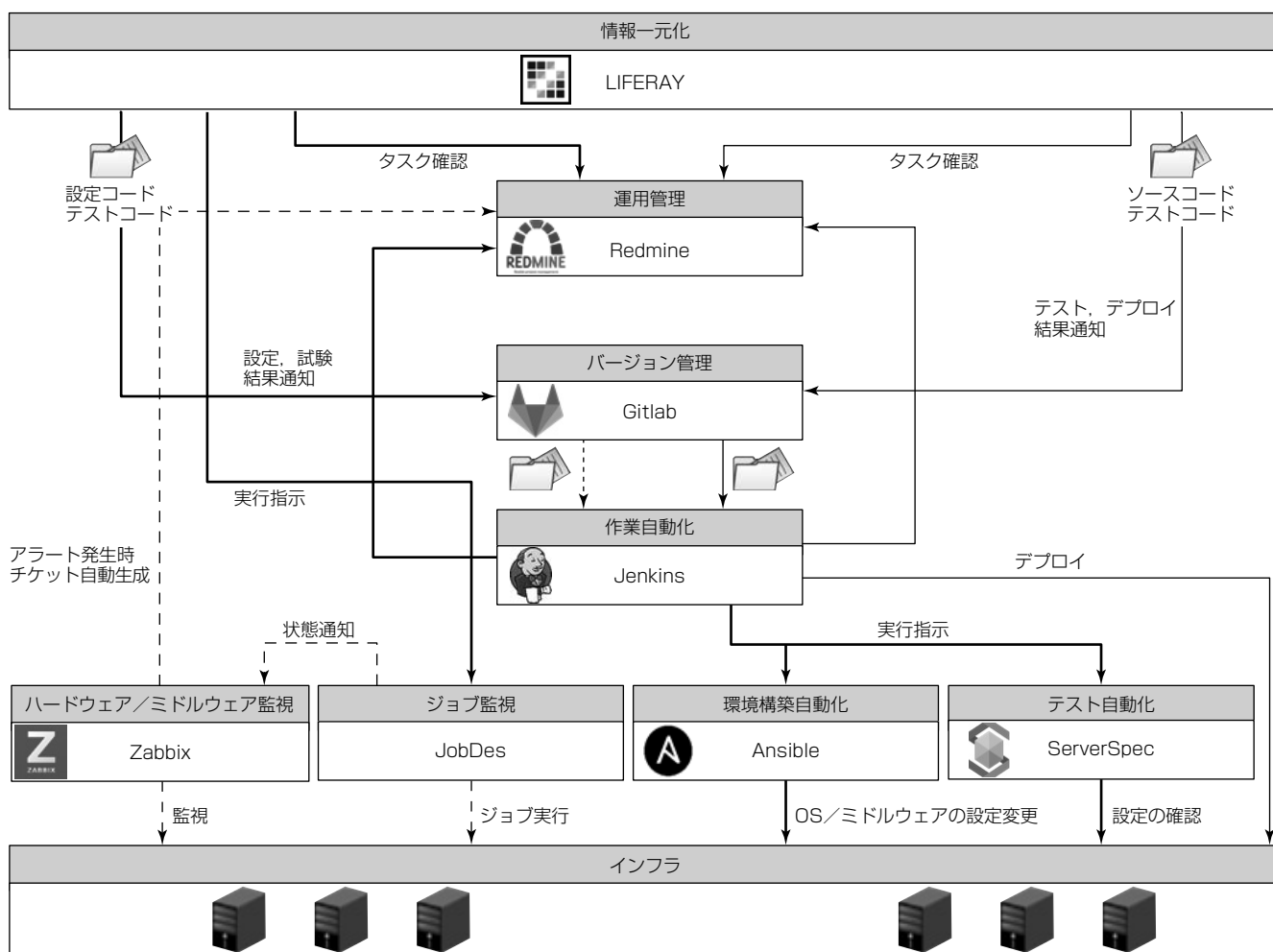


図2. 運用自動化構成

表1. 提供サービスと業務

| 提供サービス | 役割と業務 | 窓口 | | サービス要求対応 | | | | システム管理 | | | |
|--------|-------------|-----|-----|----------|-----|-----|-----|--------|-----|-----|-----|
| | | 業務1 | 業務2 | 定型 | | 非定型 | | 定型 | | 非定型 | |
| | | | | 業務1 | 業務2 | 業務1 | 業務2 | 業務1 | 業務2 | 業務1 | 業務2 |
| 定型作業 | ユーザーアカウント更新 | ○ | ○ | ○ | ○ | | | | | | |
| | Webサーバの設定変更 | ○ | | ○ | | | | | | ○ | |
| | コンテンツ配置・削除 | ○ | | ○ | | | | ○ | | | |
| 非定型作業 | 運用サービス相談 | ○ | ○ | | | ○ | | | | | |
| | 調査・情報提供 | ○ | | | | ○ | | ○ | | | |

サービス・業務はイメージ

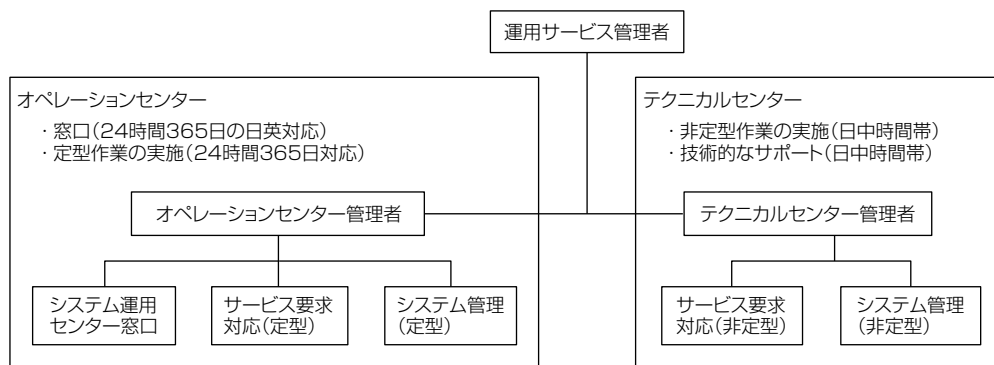


図3. システム運用センター体制

改善を行うプロセスを実現することである。

迅速なサービス改善のためには、運用設計書・業務マニュアル・実行体制といった運用リソースの頻繁な変更が必要であるが、それらの規模が大きくなると、変更を適切に行うことが難しくなる。その理由は、複数のサービスに関係する共通業務が増え、各業務の関係が複雑化し、変更時に整合性を取ることが難しくなるためである。そのため、運用ドキュメント間の整合性が崩れ、業務の実態が業務遂行者以外には分からない状態に陥るケースも多い。

この対策としてシステム運用センターでは、サービスの定義ドキュメントにサービスごとに必要な業務を明記し、複数のサービス提供に必要な“共通業務”を整理して“見える化”した(表1)。また、窓口(サイト運営者向けの連絡窓口)、サービス要求対応(サイト運営者からの要望・質問への対応)、システム管理(障害未然防止、障害時の復旧)という3つの役割を厳密に定義し、各役割の業務を明確に規定する形で運用設計を行った。業務を体制に割り当てず、抽象化した“役割”に割り当てることによって、設計変更を伴わない体制見直しを可能とし、迅速なサービス改善プロセスを実現した。

3.4.2 24時間365日の日英対応

24時間365日の日英対応実現に際して重要なポイントと考えたのは、対応するサービスの提供範囲を明確にして利用者・サイト運営者にそれらが容易に分かるようにすることと、利用者の要望に合わせた形でそのサービス提供範囲を徐々に拡大することの2点である。

まず、対応するサービス提供範囲を明確化にするため、定型業務を24時間365日対応にするという基本方針を定め、定型業務を24時間365日対応で迅速に遂行する“オペレーションセンター”と、技術的なサポートや非定型業務を着実に遂行する“テクニカルセンター”の2つの実行体制を構築した。また、実績のある標準的なサポートデスクサービスを利用して窓口を設置し、24時間365日の日英対応体制を実現した(図3)。

一方、利用者の要望に合わせたサービス提供範囲拡大の

ために、非定型業務の中で要望が多いものを定型化してオペレーションセンターへ移管するプロセスを定義した。また、スムーズな業務移管のため、システム運用センターの情報集約基盤である運用管理システムに運用リソース情報を集約し、変更時のルールを厳密に定め、迅速な業務移管を実現した。

4. むすび

2016年に構築を終え、2017年から宣伝部がサービス提供を開始したグローバルウェブサイト統合基盤は、安心・安全なプラットフォームとしてグループ各社での活用が加速しており、三菱電機、及びグループ各社で今後更なる企業活動、事業活動への活用が期待されている。また、今後はデジタルマーケティングへの活用も期待されており、宣伝部では様々なニーズに柔軟に応え三菱電機のグローバル戦略推進を支援するためのプラットフォームとなるよう、更なる強化を行っていく計画である。それに向けて、MDISでは引き続き最新のIT技術やクラウド技術、セキュリティ技術を活用しながらグローバルウェブサイト統合基盤の強化を進めていくとともに、システム運用の高度化・効率化を進めていく。

参考文献

- (1) 三菱電機ウェブサイト(国内)
<http://www.MitsubishiElectric.co.jp/>
- (2) 野間口元輔, ほか: 運営効率化とビジネス貢献に向けたオフィシャルサイトの中・長期的再構築, 三菱電機技報, **86**, No.12, 687~690 (2012)
- (3) 磯西徹明, ほか: 企業価値向上と商談機会創出に貢献する三菱電機オフィシャルウェブサイトの再構築, 三菱電機技報, **84**, No.7, 407~410(2010)
- (4) Microsoft リモート デスクトップ サービスの概要
[https://technet.microsoft.com/ja-jp/library/cc725560\(v=ws.11\).aspx](https://technet.microsoft.com/ja-jp/library/cc725560(v=ws.11).aspx)