

パブリッククラウドサービスK5による 社内システムの集約・統合

Migration of Internal Systems to FUJITSU Cloud Service K5

● 相澤 誠 ● 角間知博 ● 金丸章憲

あらまし

富士通では、社内システムの運用コストの削減および新規アプリケーションの開発期間やコストの最小化を目指し、パブリッククラウドサービスへの集約・統合を開始した。社内システムを効率的にパブリッククラウドに移行し安心・安全に運用するため、セキュリティの強化、クラウドサービスと接続するネットワーク環境(VPN接続)、共通インフラサービス、全社システム横串のインフラ統合監視や自動運用などクラウド化の技術的課題を解決できる「社内クラウドサービス」を整備した。この社内クラウドサービスの社内パイロットシステムによるクラウド移行検証・評価の結果、インフラ運用コストを30%削減、インフラ導入期間を4か月から2週間に短縮できた。

本稿では、富士通が提供するデジタルビジネス・プラットフォームFUJITSU Digital Business Platform MetaArcの中核となるクラウドサービスFUJITSU Cloud Service K5上に社内システムを集約・統合することを目的とした、社内クラウドサービスの整備や社内パイロットシステムによるクラウドへの移行の検証・評価と効果について述べる。更に、富士通社内システムの完全クラウド化に向けた移行計画と期待効果についても紹介する。

Abstract

Fujitsu has embarked on migrating its internal systems integrated on a public cloud service, aiming to minimize system operation costs, as well as the cost and period of the development of new applications. In order to migrate the systems efficiently to a public cloud while ensuring operational security and safety, we have developed an internal cloud service. It can address various technical challenges in cloud-computing, such as security enhancement as well as the development of a network environment for connecting to the cloud service (VPN connection), common shared infrastructure services, system-wide integrated infrastructure monitoring, and operational automation. An internal pilot system was introduced to assess and evaluate the migration operation, and we verified that the internal cloud service could achieve a 30% reduction in the cost of operating the infrastructure, while the new infrastructure would be introduced in a shorter period (from four months to two weeks). These are part of the efforts to integrate the internal systems on the FUJITSU Cloud Service K5, the pivot of the Company's digital business platform FUJITSU Digital Business Platform MetaArc. The paper describes this initiative to develop the internal cloud service and the evaluation of the system migration using the pilot system, with its results. The paper also presents the total cloud-migration plan for Fujitsu's own internal systems, and the expected effects.

ま え が き

富士通の社内システムは、これまで幾度もの改修を経て必要な機能を増やしてきた。それによりシステム構造の複雑化や、システムの個別最適化による業務システム同士が連携できない「サイロ化」といった問題が発生した。更に、運用コストの増大やビジネスニーズに柔軟に対応するためのシステム更改とコスト最小化などの課題を抱えていた。これらを改善するため、2009年から仮想化によるサーバ集約とアプリケーション集約の二通りで、全体最適化方針のもとで全社的なICT統合を進めてきた。しかし、これまでのところどちらも満足できる結果が得られていない。

社内システムへのICT投資に占める運用コストは、運用監視の効率化や自動化などによりコスト削減を進めているが、ほぼ横ばいである。運用維持にかかる固定費用は全体の8割となっており、戦略的投資まで予算が回せない状況に陥っている。

こうした状況の中で、社内システムの運用を抜本的に変革するために、富士通が提供するデジタルビジネス・プラットフォームFUJITSU Digital Business Platform MetaArcの中核となるパブリッククラウドサービスFUJITSU Cloud Service K5（以下、K5）⁽¹⁾への社内システムの移行を開始した。

本稿では、社内システムをK5上で安心・安全かつコストを適正化して利用していくため、まず各種インフラサービスの整備やインフラ運用の取り組みについて述べる。次に、社内パイロットシステムによるK5への移行の検証・評価から見えてきたセキュリティや性能などの課題や解決に向けた対応について説明する。最後に、今後本格的に移行を開始する社内システムのK5への移行計画についても述べる。

富士通社内システムの現状と課題

富士通では、2009年度からシステム効率化・TCO（Total Cost of Ownership）削減を目的に、全体最適化に向け仮想化によるサーバ統合や全体最適の視点によるアプリケーションの集約（システム再編）を実施してきた。

● 仮想化によるサーバ統合

富士通は、グループ会社を含めた5,808台のサー

バを物理サーバ、仮想サーバによって2015年度末までに3,136台に集約し、2,672台のサーバを削減してきた。しかし、2011年度比で依然として約6割が物理サーバであるほか、仮想化できたケースでも基本的には業務システム単位でサーバ集約したレベルであり、十分な効率化ができていない。また仮想化した物理サーバは、各業務システムの最大ピーク負荷に耐えられるように設計されている。このため、平均負荷で考えるとCPUは30%前後、メモリは50～70%の使用率であり、リソースを有効活用できていない。

● アプリケーションの集約(システム再編)

2010年度から事業軸と業務のブロックごとに業務改革を実行し、システムの統合・再編を進めてきた。しかし、事業部門をまたがる機能は業務改革が進んでおらず、現行を踏襲するためシステムが複雑に連携した構造のままになっている。アプリケーションの集約に向けて、ESB（Enterprise Service Bus）を整備しデータ連携の標準化を進めてきてはいるが、システム相互に更改が必要であるため、投資規模の大きさが原因で予定よりも大幅に遅れている。

こうした状況の中、富士通が提供しているパブリッククラウドサービスK5への社内システムの移行を契機に、前記した仮想化によるサーバ統合やアプリケーション集約を更にドラスティックに推進することにした。それを実現するために、セキュリティや運用コストを適正化した社内クラウドサービスの整備や、社内パイロットシステムを使用したパブリッククラウド上への移行検証・評価を開始した。

社内クラウドサービスによる標準化・共通化

社内システムをK5上で稼働させるに当たり、社内システムの情報セキュリティ規定や運用品質の担保、および運用コストを適正化するために運用環境を整備した。また今後、5年間で段階的に移行させるために、既存のデータセンターとK5間のネットワーク接続や社内事業所からのシステム利用を実現する社内イントラネットとの接続など、社内データセンターの運用を標準化・共通化・自動化できる社内クラウドサービスを設計・構築した。

● 社内システム専用ドメイン

K5契約単位に与えられるドメインに対して、社内システム専用セキュリティ（アクセス制御、ウイルス対策など）、ネットワーク接続、共通サービスなどの環境を整備した。こうして社内クラウドサービスを構築・提供することにより、パブリッククラウド上でも安心・安全、かつ適正な運用コストで利用できるサービスを実現した。社内システム専用ドメインの全体概要を図-1に示す。

以下、社内クラウドサービスを構成するセキュリティ、アクセス制御、ウイルス対策、ネットワーク接続、共通サービスについて説明する。

● 仮想化環境におけるセキュリティの考え方

K5は、社内・社外を区別せず、安全な領域はないという「ZERO-TRUST」の考えに基づき全てのゾーンを多層防御し、標的型攻撃などの脅威に対応した設計となっている。

また、ビジネスや商品開発目的で利用する開発サーバ用途では、開発業務の即時性を考慮し、セキュリティレベルの変更により対応できるように設計した。

● アクセス制御

社内システムは、ユーザープロジェクトという単位でドメインにより管理される。このユーザープロジェクトは、FWaaS（Firewall as a Service）でネットワークアクセスを制御し、セキュリティグループでサーバアクセスを制御するといったよ

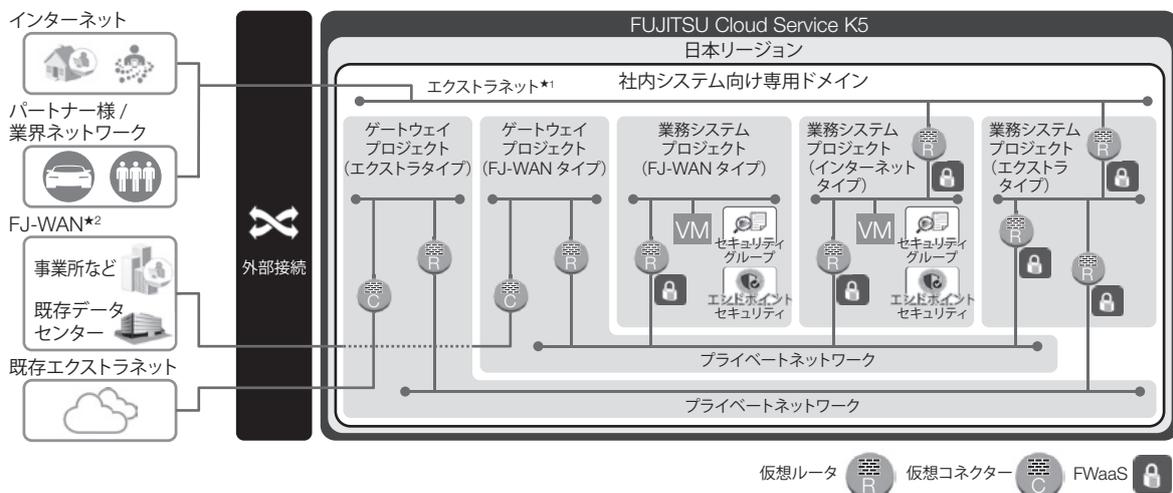
うに、アクセス制御を組み合わせることでセキュリティを担保している。

FWaaSは、ユーザープロジェクトの仮想ルータに対して適用され、特定のIPアドレス（またはサブネット）、またはポート（ホワイトリスト形式）で外部接続およびプロジェクト間の通信を制御する。従来のFW同様、FWaaSの管理権限を社内クラウドサービス運用部門に限定することで、セキュリティを強化している。

セキュリティグループは、Web、DB（データベース）など仮想マシン（以下、VM）の利用用途に応じて、内部、外部のトラフィックを制御するFWとして役割を果たす。具体的には、Ingress（外部からの通信）ルールに従ってVM自身の受信ポートを制御し、Egress（内部からの通信）ルールに従ってVM自身から送信する通信を制御している。このセキュリティグループの管理権限をセンター運用SEに限定することで、サーバ単体のセキュリティを維持した運用を担保している。アクセス制御の構成を図-2に示す。

● ウイルス対策

社内システム情報セキュリティ規定に則り、エンドポイントセキュリティ（ウイルス対策）を実施している。ウイルス対策ソフトウェアとしてMcAfee社の製品を採用し、各プロジェクトから通信可能な共通プロジェクトに組み込むことで、各業務システム（運用サーバ、開発・検証用サーバ、



★1：複数の企業内ネットワーク（イントラネット）を相互接続したネットワークシステム
 ★2：富士通グループ専用の広域ネットワーク

図-1 社内システム専用ドメインの全体概要

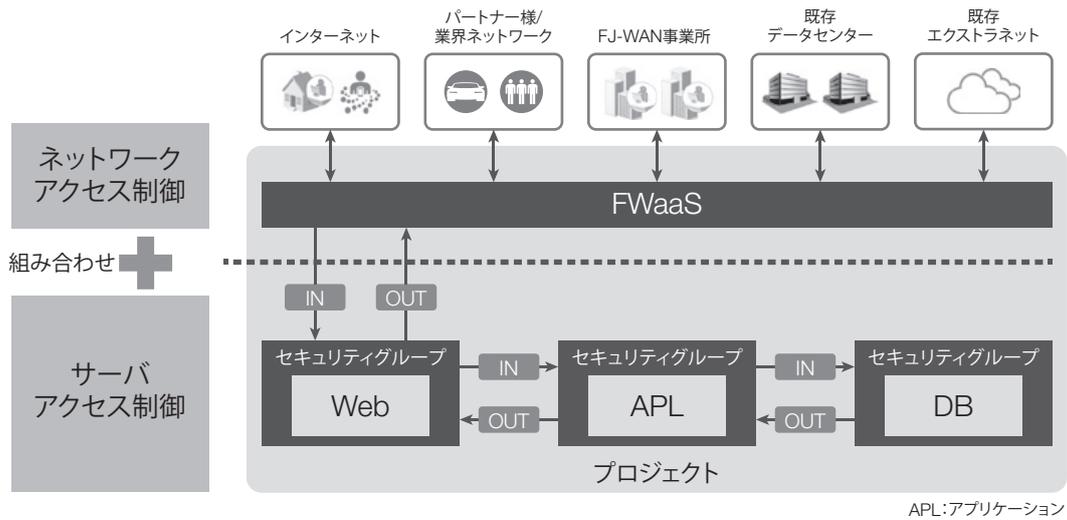


図-2 アクセス制御の構成

部門用サーバ)を対象にウイルス対策機能を提供している。

● セキュリティセルフチェック

インターネットから直接アクセスがある機器を対象に、セキュリティの担保を目的として、セキュリティ診断を定期的実施している。

● 社内イントラネットとのネットワーク接続

既存データセンターとの連携性とシステム移行の効率性を担保し、ネットワーク帯域管理を効率化するため、ゲートウェイプロジェクトを構築し、社内イントラネット接続用ルータ (L3スイッチ) で共有できるように設計した。これにより、各プロジェクトと社内イントラネット間の容易なネットワーク接続と管理を実現した。

● 共通インフラサービス環境

社内システムのインフラ運用を効率化するために、以下に示す共通サービスを整備・提供している。

- ・名前解決サービス (DNS: Domain Name System)
- ・時刻同期サービス (NTP: Network Time Protocol)
- ・PROXYサービス (社外Webへのアクセス)
- ・メールサービス (メール中継)
- ・インフラ監視サービス (サーバ監視)
- ・ログ管理サービス (サーバなどのログ管理)
- ・RBAサービス (RBA: Systemwalker Runbook Automation, パッチ適用などのメンテナンス自動化)

中でも、インフラ監視サービス、ログ管理サービス、およびRBAサービスは、OpenStackベースのオートスケール、フェイルオーバーに対応して機器の増減に動的に対応できるように設計・構築されている。

● インフラ監視サービス

前述のオートスケール、フェイルオーバーなどは、クラウド機能に対応したシステム運用監視機能であり、K5の標準サービスでは未提供であるため、社内システム用にシステム監視機能を共通サービスとして構築し、提供している。

このサービスは、Zabbix社のZabbixを組み込んだSystemwalker Centric Manager (CMGR) によってオートスケール時の監視対象の自動追加を、Systemwalker Service Quality Coordinator (SQC) によってサーバリソースおよび富士通製ミドルウェアの性能監視を実現している。共通インフラサービス環境の構成を図-3に示す。

● セルフサービスポータル整備

VM配備の時間短縮および運用コストの更なる削減に向けて、社内CSM (Cloud Service Management) 製品を使ったセルフサービスポータルの整備を行っている。セルフサービスポータルは、人手による作業をベースに行っているVM配備の作業を効率化するだけでなく、今後の社内システム移行を円滑に実施するものである。

パブリッククラウド上で社内システムを効率的に運用するためのVM配備に必要な設定作業を組

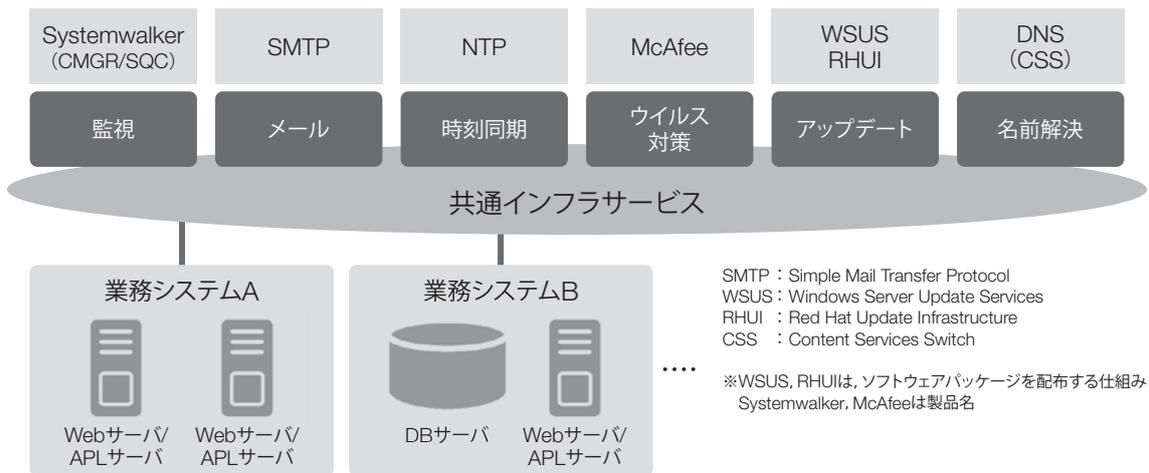


図-3 共通インフラサービス環境の構成

み込むことで、運用コストの削減を見込んでいる。更に、開発を目的としたVM利用においては、頻繁にVM配備・廃棄のオペレーションが発生するため、人手による作業には限界がある。したがって、製品開発を効率的に進めていくためにも、富士通ではできるだけ早い段階でセルフサービスポータルを提供できるように取り組んでいる。

グローバルICTガバナンス

本章では、社内クラウドサービスのグローバル展開について述べる。今回、日本国内で提供しているK5上に社内クラウドサービスを構築した。このサービスは、富士通の社内システム情報セキュリティの規定や運用コストを適正化する共通サービスを提供しており、社内データセンターのインフラ運用を標準化・共通化・自動化している。今後、社内システムのK5への移行を日本国内から順次進めていく。

社内システムの移行は、日本に限定されるのではなく、グローバルレベルで実施される。そのため、各国・各地域の法規制や制度などに対応し、海外におけるK5上での社内クラウドサービスの整備が必要となる。今回の日本国内に構築した社内クラウドサービスの構築・運用ノウハウは、海外における社内システムのK5への移行を加速するだけでなく、これまで実現できていなかったグローバルレベルでの社内データセンターの運用を可能にする。これらは、グローバルでのICTガバナンスを実現する意味でも大きな意義があり、是非とも達成

したい目標である。

社内パイロットシステムによる検証と評価

社内システムのK5への移行を本格的に進めるに当たり、先行して二つのシステム（パイロットシステム）による移行検証を実施した。本章では、K5の機能やリソースの有効活用に向けた取り組み、移行における課題・対策について述べる。

● パイロットシステムの移行概要

ICT投資予算管理システムと、ICT機器を管理する統合現品管理システムの2システムをパイロットシステムとし、オートスケール機能・マルチテナント製品を活用し、六つのVMを最小で三つに集約した。パイロットシステムの移行の概要を図-4に示す。

● オートスケール機能の活用

パイロットシステムは、通常時とピーク時では負荷にばらつきがあり、これまではピーク時を想定したシステム構成としていた。これは、通常時はリソースに余剰があることを意味している。通常時のシステム構成をリソースの基本とし、ピーク時は負荷に合わせて増強ができればリソースの有効活用が可能となる。

パイロットシステムのCPU使用率を調査した結果、ICT投資予算の締め日などの定期的に発生するシステムの高負荷と、不定期に発生するシステムの高負荷があることが確認できた。CPU使用率の状況を図-5に示す。CPU使用率の変化に合わせて、しきい値による動的なスケールアウトと、ス

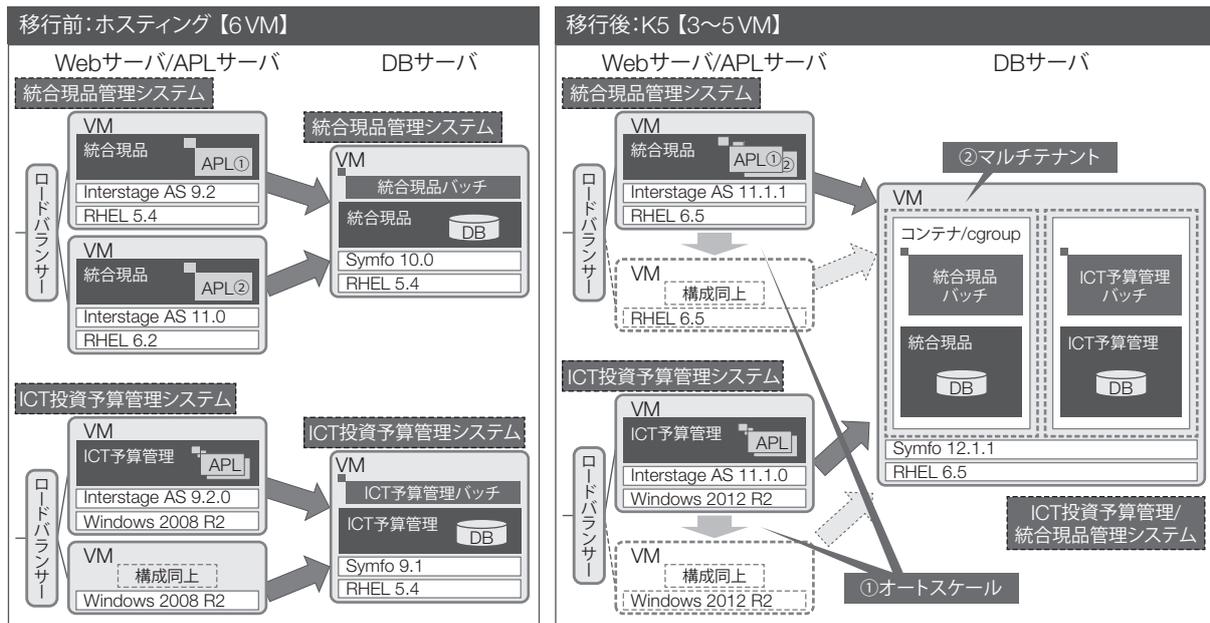


図-4 社内パイロットシステムの移行の概要

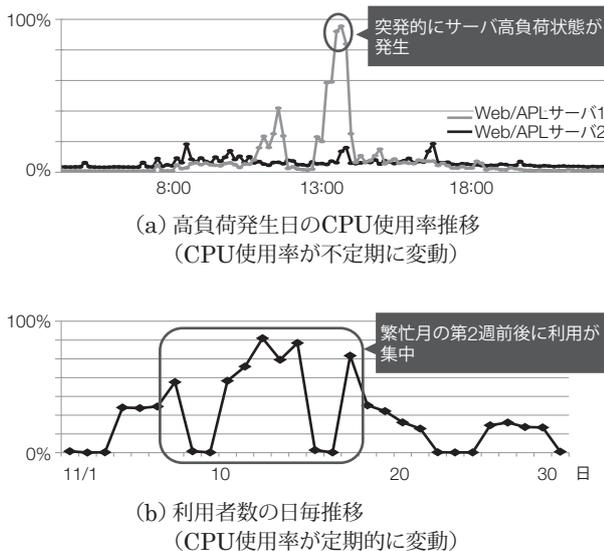


図-5 社内パイロットシステムのCPU使用状況

ケジュールによる計画的なスケールアウトを組み合わせることで、VM構成の適正化（リソースのスリム化）を実現した。

● マルチテナント製品の活用

DBサーバを、FUJITSU Software Symfoware Server Consolidation Option機能と、Red Hat Enterprise Linux (RHEL) 6.5のcgroup機能でマルチテナント化し、二つのパイロットシステムのDBサーバを集約した。

今回、各システムにおけるCPUの使用比率を設定した。高負荷時(全CPUの使用率が100%のとき)はあらかじめ設定した範囲で処理が実施されるが、通常時(CPUの使用率が100%に満たないとき)は設定比率を超えるCPUの使用が可能である。二つのシステムのCPU推移を図-6に示す。

● 標準ポリシー適用によるセキュリティ対策

これまで、社内イントラネットはセキュアな環境と位置付けられていたが、K5ではZERO-TRUSTの考えに基づいたセキュリティ対策を実施している。今回のパイロットシステムでは、セキュリティグループの作成に必要な通信ポリシーを設定するため、SEはシステム内外の通信情報を全て洗い出すなど、新たな作業を強いられることとなった。これに対し、通信ポリシーを既存社内データセンター間などのセンターが把握可能な情報（標準ポリシー）とSEが把握可能な情報に分け、前者を一元管理・自動化することで、センターおよびSEそれぞれの作業を軽減させた。なお、パイロットシステムでは、SEが洗い出す通信ポリシー数が1,389から482に削減された。

● 多重化による性能対策

K5では、TCO削減の一環としてOSやミドルウェアの標準化、CPUコア数・メモリ組み合わせのパターン化など標準構成を適用している。また、K5

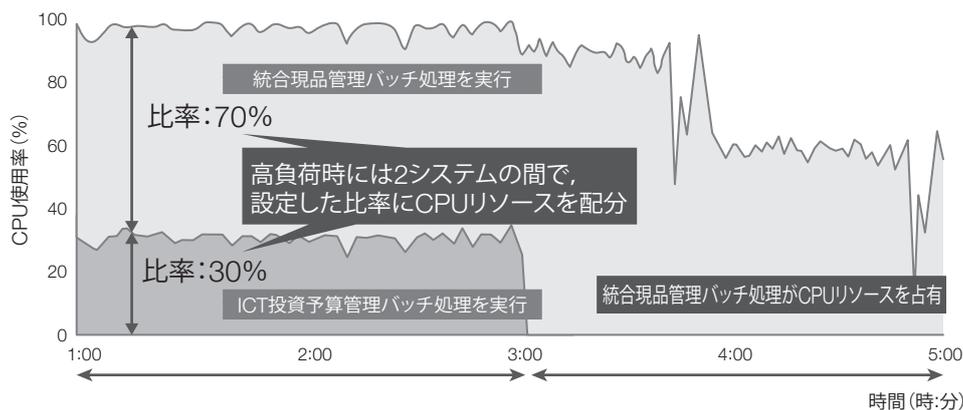


図-6 システム高負荷発生時のCPU使用率推移

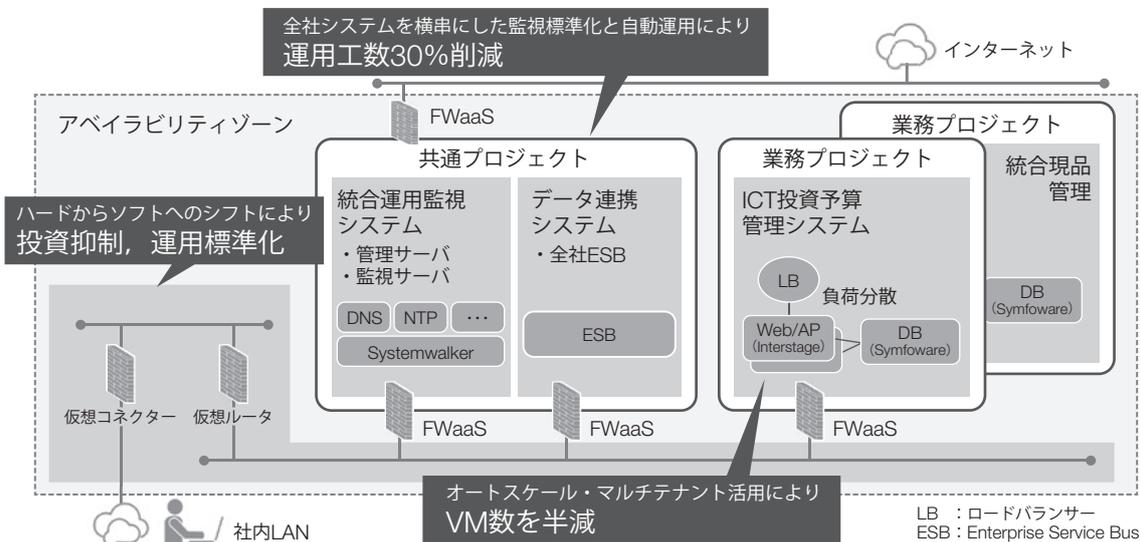


図-7 パイロットシステムによる検証の成果

で採用しているサーバスペック（CPU周波数）は、既存のものに比べて50～70%程度である。そのため、CPU周波数が低いことに起因する処理速度の低下が発生する場合、アプリケーションの改修が必要となる。今回、パイロットシステムにおいて性能劣化が発生したが、処理を多重化（コア数を有効活用）するようアプリケーションを改修することで対応した。

● **パイロットシステムによる検証の成果**

社内パイロットシステムでは、オートスケール機能の活用およびマルチテナント製品の活用により、移行前と比較しVM数を半減させた。また、全社システムを横串にしたインフラ監視の標準化と自動運用により、運用工数を30%削減した。更に、システム構築時に発生するサイジングや調達作業

から解放され、インフラ導入期間を8分の1（4か月を2週間）に短縮した。K5移行の取り組み成果を図-7に示す。

社内システムのK5への移行計画と期待効果

2015年度から日本国内の社内システムのK5への移行を本格的に開始し、2015年度末で19のシステムが稼働中である。現在、今後5年間を目途に国内外の社内システムのK5への移行計画を完了させるため、全ての社内システムの実態調査を実施している。また、業務系システム以外にもビジネス、製品・ソリューション開発を目的に複数の個別開発系クラウド環境（約13,000のVM）が存在している。これらの開発系クラウド環境についても、各部門と連携してK5への移行を推進中である。

富士通は、グループ国内外全ての社内システムを次世代クラウド基盤へ刷新することにより、グループ全体で5年間で約350億円のTCO削減を達成すると2015年2月に発表した⁽²⁾。社内システムをクラウドに移行する最大の効果は、サーバやストレージ、ネットワークなどのインフラ設備の調達やインフラ構築・運用作業が軽減され、インフラ構築費用や運用コストが削減できる。また、スケーラビリティを活かし、業務量に応じた柔軟なリソースの変更が可能となる。これにより、業務のピーク時に合わせたリソース量から平常時のリソース量に削減できるため、インフラ運用コストを削減できる。更に、個別に社内システムのインフラを維持する必要がなくなるため、社内ICT要員の人件費も削減できる。

従来、ICT運用に携わっていた人員は社内実践で培ったノウハウや技術を持っているため、パワーシフトすることでビジネスなどへの貢献による副次的な効果も期待できる。しかし、社内システムのクラウド移行に向けては課題もある。クラウド移行を計画しているシステムの多くは、ハードウェアやOS、ミドルウェアなどのプラットフォームを利用する「IaaS (Infrastructure as a Service) 型」であり、幾度もの改修を経て複雑化したアプリケーションの運用コストを削減するためには対策が必要である。

今後、レガシーシステムを一度解体し、本当に必要なシステムだけをクラウド上に構築する「モダナイゼーション (近代化)」やビジネスや事業戦略に連動したシステムの再構築、およびそれらに合わせてPaaS (Platform as a Service) を活用することで、アプリケーションを標準化・共通化・自動化してTCOを削減するクラウドネイティブな開発手法についても検証していく予定である。

む す び

本稿では、社内システムをパブリッククラウドに集約・統合するための社内クラウドサービスや社内パイロットシステムによるクラウド移行の検証・評価と効果について紹介した。

今後、本格的に社内システムをK5に移行・運用していく中で、社内クラウドサービスを成長させるとともに、K5で提供されるIaaS・PaaSを社内

システムに適用することにより、知見やノウハウも数多く蓄積していくことになる。これらは、K5品質の向上やPaaSなどの新たな製品・サービスの強化につながると同時に、富士通のクラウドビジネスにも必ず貢献できると考えている。もちろん、お客様に提供するクラウドサービスを事前に使用することで、お客様に安心して利用していただけだけでなく、社内で得られた知見やノウハウをお客様に価値として提供できるはずである。そのためにも、富士通グループ全体で実施する社内システムのK5への移行プロジェクトを必ず成功させる所存である。

参考文献

- (1) 富士通：デジタルビジネス・プラットフォーム「MetaArc」を提供。
<http://pr.fujitsu.com/jp/news/2015/09/29.html>
- (2) 富士通：グループ国内外すべての社内システムを次世代クラウド基盤へ刷新。
<http://pr.fujitsu.com/jp/news/2015/02/18.html>

著者紹介



相澤 誠 (あいざわ まこと)

IT戦略本部
デジタルビジネスプラットフォーム推進室
社内システムのK5移行展開の推進に従事。



角間知博 (かくま ともひろ)

(株) 富山富士通
クラウドサービス企画統括部
社内向けクラウドサービスの企画、設計に従事。



金丸章憲 (かなまる あきのり)

富士通CIT (株)
コーポレートシステム統括部
知財システムおよびコーポレート共通システムの企画・開発・運用に従事。