基盤システム更新への取り組み

1. はじめに

企業活動においてクラウドサービスが不可欠な存在になった今日では，クラウドサービスを便利に，かつ，安全に使用できるシステム環境が欠かせない．

情報システム部では，将来的に社内システムや社外クラウドサービスをデバイスフリーでシームレスに利用できるITインフラ基盤（ハイブリッドクラウド）の構築に向けた取り組みを進めている．

本稿では，旧来のオンプレミス型システムから，先進的なクラウド型システムへの刷新に取り組んだ基盤システムの更新について述べる．

2. 概要

基盤システムとは，グループウェアやメールシステムなどの「基盤情報システム」ならびに，受注生産システムなどの「基幹システム」における業務アプリケーションを除く，基幹サーバ，基幹ネットワーク，セキュリティシステムなどといった共通基盤のシステムを指す．いわば「ITインフラ（Information Technology Infrastructure）」と呼ばれるものである．

従来使用していた基盤システムは，16年前の設計思想に基づき構築されたものであり，クラウドサービスの利用を考慮していなかった．

そこで，「クラウドをベースに据えたシステムへ刷新する」，「今後，少なくとも10年間は大きな更新を行わずに，使い続けられるシステムを構築する」という考えのもと，機密性，先進性，可用性，継続性，経済性などの観点から，次の4つの方針を定め，更新に取り組んだ．

① グループウェアやメールシステムは，常に進化や柔軟性が求められることから，最新のサービスを使えるように「パブリッククラウド」へ全面移行する．

② ネットワークは，通信の安定性とセキュリティの確保がより求められることから，インターネット網と閉域網を両立させたネットワークへ「再構成」する．

③ 通信機器は，現状のセキュリティレベルを下げることはできないことから，当社独自のセキュリティ設定ができる様に「オンプレミス」を継続する．

④ サーバは，機器の安定稼働やデータ保全が何より重要であることから，システムの維持継続を優先し「プライベートクラウドとオンプレミス」を組み合わせた構成へ移行する．

上記の方針に基づいた更新の概要図を**図1**に示す．

3. 基盤システム更新の内容

前述の4つの方針に基づき，各基盤システムの更新に取り組んだ．

3.1 ユーザ認証基盤の刷新

ユーザ認証基盤とは，全てのパソコンやサーバへのログイン認証や，社内システムのアクセス制御といった「アカウント管理」を担っている根幹の仕組みである．

しかし，従来のユーザ認証基盤は，前述の通り16年前の設計思想で構築されたものであり，クラウドサービスの利用を前提としたアカウント管理の要件を満たせていなかった．

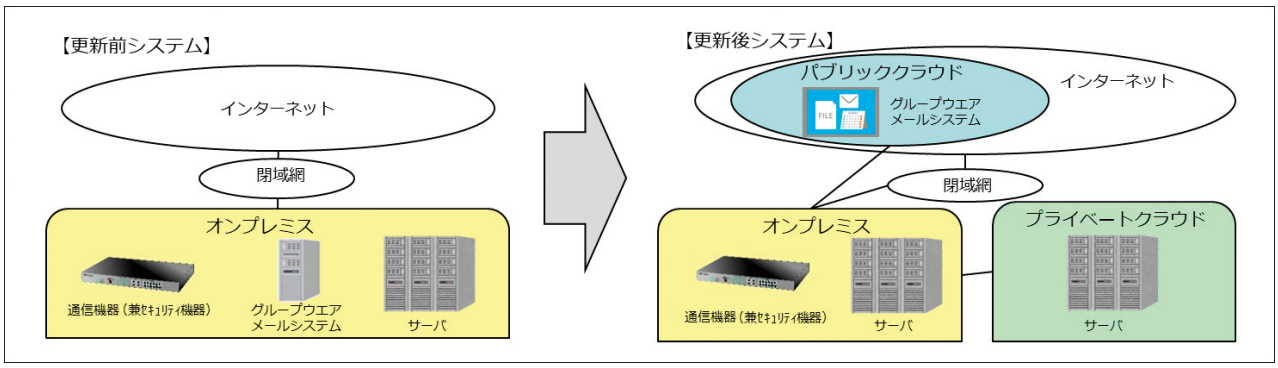

図1　基盤システム更新概要図

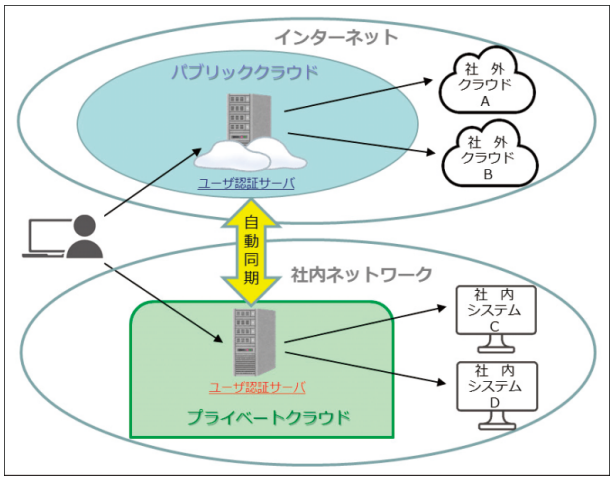

図2　ハイブリッド ID環境構成図

この問題を解決するために，新たなユーザ認証基盤はオンプレミスからクラウドベースへ刷新を図った．

この新しいユーザ認証基盤では，社内ネットワーク内のプライベートクラウドと社外ネットワークのパブリッククラウドの両方にユーザ認証サーバを配置し，ユーザ情報を自動的に同期する「ハイブリッド ID環境（図2）」を構築した．

これにより，一度のユーザ認証処理で社内システムと社外クラウドサービスがシームレスに利用可能となる「シングルサインオン（SSO:Single Sign On）認証」を実現できた．

3.2　コミュニケーション基盤の変更

ユーザ認証基盤の刷新に伴い，グループウェアとメールシステムをクラウドサービスへ全面移行した．クラウドへ全面移行したことにより，最新のコミュニケーション基盤の提供が可能となった．また，クラウドストレージの導入により，メールで送れなかった大容量ファイルを送受信できるようになった．

3.3　ネットワーク基盤の再構築

ユーザ認証基盤とコミュニケーション基盤のクラウド移行に伴い，通信経路やアクセス制御方法が変更となるため，ネットワーク全体の設計，構成を見直し，再構築を行った．

また，ネットワーク通信量の増加に対応するため，主要回線の帯域幅を約3倍に拡大した．さらに，旧閉域網の拠点を新閉域網に移行し，全48拠点のネットワーク機器を最新の通信規格であるIPver6（Internet Protocol Version 6）に対応した機器へ更新した．これにより，ネットワークのパフォーマンスとセキュリティが向上し，クラウド移行後の運用を効率的に行うことが可能となった．

3.4　セキュリティ基盤の強化

基幹ネットワークは，社外ネットワーク側および社内ネットワーク側の双方にUTM（Unified Threat Management）機器を設置し，重要なデータを防御する「ゼロトラスト・セキュリティ（Zero Trust Security）」の仕組みを実現した．

これにより，外部から内部への悪意ある攻撃や，内部から外部への不正送信など，様々な脅威に対して効果的な防御ができるようになり，より堅固なセキュリティレベルを確保できた．

3.5　サーバ基盤の新規構築

可用性が求められるサーバは，オンプレミスからプライベートクラウドへ移行し，24時間安定稼働できるサーバ基盤を構築した．また，重要なサーバや通信機器に対しリモート監視ができるシステムとその運用体制を新たに構築した．

4. まとめ

今回の基盤システム更新により，クラウドサービスを便利に，また安心・安全に利用できる環境が整った．

今後も，様々なシステムやサービスを，場所やデバイスを問わず，より便利に，そして高度に利用できる情報システム（図3）の実現に向け，更なる拡充に取り組んでいく．

宮本　昂輝（情報システム部）

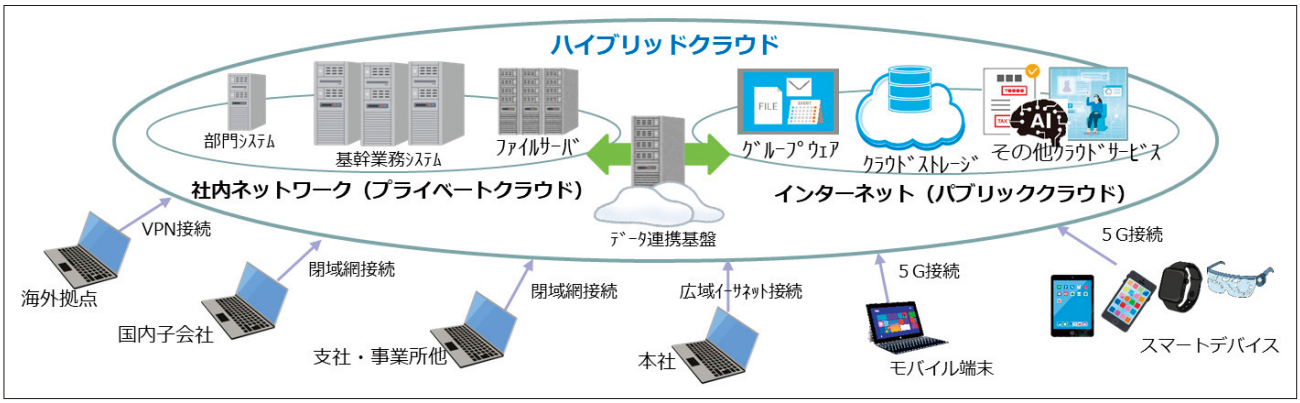

図3　当社情報システムの将来構想図