会誌「情報処理」Vol.62 No.8（Aug. 2021）「デジタルプラクティスコーナー」

FUJITSUファミリ会論文

生命保険会社におけるパブリッククラウドの活用～機動的なシステムインフラ構築とコスト最適化を目指して～

白石征久[1]　佐田野直樹[1]　堀　仁人[1]

[1]T&D情報システム（株）

近年，少子高齢化の進行やライフスタイルの変化にともない，生命保険業界を取り巻く環境が大きく変わりつつある．当状況下において，デジタル技術を活用した成長戦略を実現するためには機動的なシステム開発態勢の構築が急務であり，迅速かつ柔軟にシステムを構築でき，コスト最適化に資するパブリッククラウドの活用に取り組むこととなった．パブリッククラウドの活用に向けては，サービスの継続性と情報漏洩などのセキュリティに関するリスク対策が重要な要素であり，外部機関の知見も加え，実証実験を含めた複数のステップを経て段階的に評価を行った．また，並行して社内の基準を整備し，可用性と機密性の観点からパブリッククラウドへの移行対象システムを選別，2019年度から約2カ年で社内システム（約70サーバ）を移行した．移行により，コスト削減，開発期間の短縮に加え拡張性や柔軟性など，パブリッククラウドのメリットを享受できた．

※本稿はFUJITSUファミリ会2020年度優秀論文受賞論文です．

1. 当社の概要と取り組み

T&D情報システム（株）（以下，当社）は，**図1**に示すとおり大同生命，太陽生命，T&Dフィナンシャル生命の生命保険会社3社を中核とするT&D保険グループのICT戦略を一手に担う会社である．その業務内容は，ICT戦略の立案実行をはじめ，システム開発，システム基盤の構築，システム運用とICTにかかわる全般にわたっている．

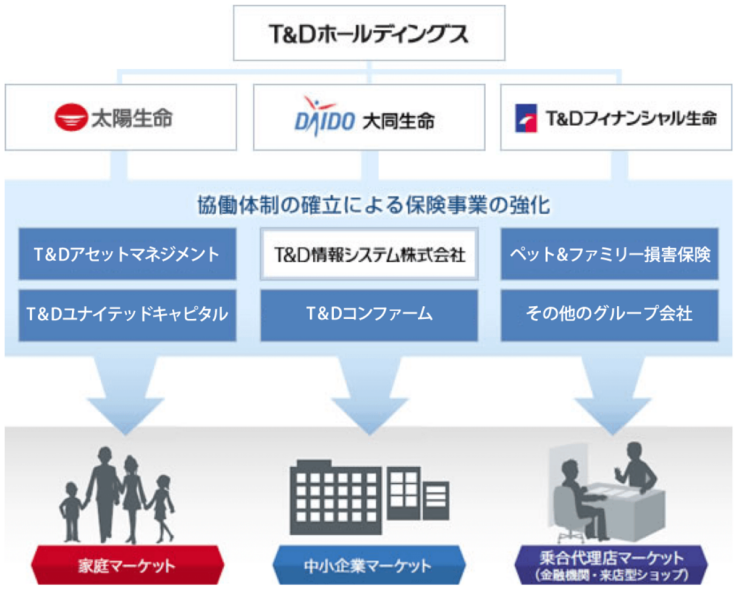


図1　T&保険グループ組織体制図

当社が受託している大同生命は法人向け市場，とりわけ中小企業経営者向けの保険商品の販売をコアビジネスとしており，主なお客さまは経営者やそのご家族，従業員である．近年では少子高齢化の進行やライフスタイルの変化による保障ニーズの多様化など，生命保険業界を取り巻く環境が大きく変わりつつある．このような事業環境の変化を背景に，業界各社では人工知能やオープンAPIといった革新的情報技術の活用を通じ，Fintechに代表される新たな顧客サービスの創出に着手している．

当社においては，昨今の著しい環境変化に即応しデジタル技術を活用した成長戦略などの実現に向け，「システム開発力の一層の強化」と「デジタル化の推進」をシステム開発の目指すべき姿として設定し，品質・生産性の向上，コスト最適化および新たな価値の創造など，各種施策に取り組んでいる．

迅速かつ柔軟にシステムを構築でき，コスト最適化に資する「パブリッククラウドの活用」は，機動的なシステム開発態勢の構築に必要な取組みとして捉え，2017年度から本格活用に向けた取り組みに着手した．

2. パブリッククラウド活用に向けた取り組み

2.1　パブリッククラウド移行の進め方

パブリッククラウドの本格活用に向けては，**図2**に示すとおりFISC安全対策基準やセキュリティガイドラインをもとに，外部の知見も加え，活用における概算効果やリスク対策を確認した上で，「1. 効果試算・リスク整理」「2. 実証実験・基準整備」「3. スモールスタート」「4. 本格活用」といった4段階のステップを経て，安全に社内システムを移行できるよう取り組みを開始した．

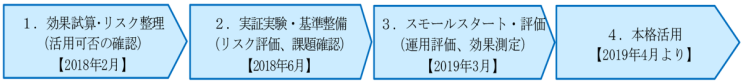


図2　パブリッククラウド移行の進め方

2.2　効果試算・リスク整理

（1）効果試算

パブリッククラウド環境の調査，分析および外部からの情報収集を踏まえて，パブリッククラウドの利用により，システムインフラ構築期間の短縮や処理集中時のリソース拡張など，システム構築および運用時において柔軟に対処できることが把握できた．また，データ分析およびAIなどの最新技術の活用，アジャイル開発環境や外部接続APIの利用により，機動的なシステム開発態勢に寄与できることが確認できた．

コスト面においても社内OAシステム☆1を対象にパブリッククラウドに移行した場合の効果シミュレーションを行い，現行比で約30％の継続費用の削減が見込める結果となった．

（2）リスク整理・対策

リスクの整理においては，FISC安全対策基準の「リスクフレームワーク」を元に，外部コンサルティング機関の知見も加えて，パブリッククラウド固有の想定リスク☆2を洗い出し，受託元の大同生命と協力して必要な対策案の策定に取り組んだ．

クラウド事業者が公的認証の取得や暗号化などのセキュリティ対策を強化したこと，およびFISCによる標準化の推進により，事前にリスク対策を行うことで多くのリスクは回避可能であった．ただし，パブリッククラウド障害時における対応および予期せぬサービス停止に対するリスクは，机上調査や外部からの情報収集では回避可能な判断が難しく，次フェーズ以降の実証実験やスモールスタートにて影響や発生頻度，対策の実行性を確認の上，評価することとした．

FISCの「金融機関におけるクラウド利用に関する有識者検討会報告書」では，パブリッククラウドの活用においては，業務特性や重要度に応じてリスクを管理する「リスクベースアプローチ」が推奨されており，当社においても想定リスクおよび対策案を踏まえ活用範囲を整理し，原則，機密性・可用性の低いシステムから順次活用する方向性とした．

2.3　実証実験・基準整備

（1）実証実験（PoC）

実証実験はMicrosoftAzure（以下，Azure）を利用し，VirtualMachines（IaaS）およびAzureSQLDatabase（PaaS），AzureSynapseAnalytics（PaaS）を対象に行い，システムインフラ構築における期間短縮，システムリソースの柔軟な変更などが想定どおり可能であることが確認できた．

コスト面では，不要な時間帯のサーバ停止やリソース削減に加え，サービスの複数年契約やOSライセンスの持込み特典などを用いることで，当初想定よりも大幅なコスト削減効果を見込むことができた．

（2）社内基準の作成・整備

第1段階にて整理したパブリッククラウド固有の想定リスクと対策より，利用者対策，事業者選定に加え，移行システム選定の3つの観点からパブリッククラウド利用時における社内基準を作成した．基準の作成は受託元の大同生命が担当し，当社においては基準作成に向けた情報収集および各種対策の実効性を確認した．

移行システムの選定基準においては，「リスクベースアプローチ」に基づき，機密性および可用性の観点よりパブリッククラウドへの移行基準を策定した．

機密性においては，**表1**のとおり扱う情報の重要度に応じて移行基準を取り決め，「特定個人情報」以外はパブリッククラウドへの移行を認めた．また，可用性においては，**表2**のとおりシステムの重要度に応じて移行基準を取り決め，条件付きとなるが「最重要な情報システム」においてもパブリッククラウドへの移行を認める基準とした．

表1　機密性「扱う情報の種類」に関する基準

<table>
<tr><th>項番</th><th colspan="3">情報の種類</th><th>当社パブリッククラウド移行基準</th></tr>
<tr><td>1</td><td rowspan="4">重要な情報</td><td rowspan="3">個人情報</td><td>特定個人情報</td><td>（×）クラウド移行不可</td></tr>
<tr><td>2</td><td>センシティブ（機微）情報</td><td>（△）クラウド移行可
［条件］
・サーバ暗号化対策を実施。
・クラウド移行の適切性、
安全対策状況を事前付議し協議。</td></tr>
<tr><td rowspan="3">3</td><td>特定個人情報・センシティブ（機微）情報以外の個人情報</td><td rowspan="3">（○）クラウド移行可
［条件］
・サーバ暗号化対策を実施。</td></tr>
<tr><td colspan="2">経営機密に関する情報</td></tr>
<tr><td colspan="2">部門の業務遂行にあたり、漏えい、改ざんおよび紛失により業務の継続性が損なわれる情報</td></tr>
<tr><td>4</td><td>その他の情報</td><td colspan="2">上記以外の情報、および社外に開示した情報</td><td>（○）クラウド移行可
・制限なし</td></tr>
</table>

表2　可用性「システムの重要度」に関する基準

<table>
<tr><th>項番</th><th colspan="2">情報システムの種類</th><th>当社パブリッククラウド移行基準</th></tr>
<tr><td>1</td><td>最重要な情報システム</td><td>当日中に復旧を必要とする情報システム（お客さまや複数の金融機関に大きな影響を与える決済システムなど）。個人情報のうち、特定個人情報、センシティブ（機微）情報を扱う情報システム。</td><td>（△）クラウド移行可
［条件］
・日本国内複数地域のデータセンターでサーバを冗長化
・クラウド移行の適切性、
安全対策状況を事前付議し協議。</td></tr>
<tr><td>2</td><td>重要な情報システム</td><td>当日中に復旧する必要はないが、経理上および対外的に影響がある情報システム。</td><td>（○）クラウド移行可
［条件］
・システムのバックアップを日々取得</td></tr>
<tr><td>3</td><td>その他の情報システム</td><td>上記以外の情報システム</td><td>（○）クラウド移行可
・制限なし</td></tr>
</table>

2.4　スモールスタート

（1）社内システムの移行

実証実験では確認できない運用監視やジョブ管理などのシステム運用面の実行性および認証処理を含めた既存システムとの相互連携，応答性能の確認を目的として，機密性・可用性の低い社内システム（サーバ：2台）を対象にAzure環境に移行した．

システム運用，各種機能，リスク対策の観点より評価を行い，パブリッククラウド固有の想定リスクの対策が有効であることを確認した．

（2）予期せぬサービス停止への対応

実証実験およびスモールスタートの期間を通じて，課題としていた予期せぬサービス停止は発生しなかったが，大規模障害によりシステム停止が長引くリスクを想定し，「最重要なシステム」と一部の「重要なシステム」を東日本・西日本リージョン☆3に冗長化することで，リスク発生時の影響を極小化できると判断した．一部の「重要システム」とは，停止時の代替手段がなく，お客さま対応もしくは決算・資金決済業務にて利用するシステムおよび利用者の範囲が全社に及ぶシステムを対象とした．

2.5　本格活用

実証実験およびスモールスタート評価期間中の新たな課題やリスクの発生がなかったことから，リスク対策に対しての有効性を確認することができたため，サービスレベルの維持が可能であり，コスト削減効果が期待できる社内OAシステムを対象にAzure環境への移行に取り組むこととした．

移行対象のシステムは約70台であり，文書管理システムやDWHシステムなど，センシティブ情報を保持しているシステムも含まれる．プロジェクトは2019～2020年度の2カ年とし，機密性・可用性の低いシステムからで順次Azure環境に移行する計画とした．

また，パブリッククラウドへの移行にあたって，新たなITの開発・目利きなどが可能な人材（クラウド・エンジニア）の育成が急務であり，当案件の対応と合わせて，新たなITの調査・研究・実証実験を推進することで育成に取り組んだ．

3. パブリッククラウド環境の構築とセキュリティ対策

3.1　クラウド環境の構築

（1）セキュアな通信経路の確立

情報漏洩などに対する万全なセキュリティ対策，意図しないサービス停止へ柔軟に対応できるよう，社内OAシステムの移行に先立ち，Azure環境に当社専用環境を構築した．

移行対象となるシステムの中には個人情報やセンシティブ情報が含まれることから，今回Azure環境に構築する環境は外部環境から遮断する必要性があった．社内からの接続がインターネット経由の接続とならないよう配慮し，当社データセンタとAzureリージョン間に専用線を敷設，「ExpressRoute」サービスを利用することでセキュアな通信環境を整備した．また，PaaSはパブリックIPに対しての接続となるため，通常はインターネット経由での接続となるが，「マイクロソフトピアリング」サービスを利用することで専用線経由での利用を可能とした（**図3**太枠部）．

（2）東西リージョンの作成

メインで利用する東日本リージョンが障害となり業務継続が困難となった状態を想定し，西日本リージョンにも専用線を敷設，東日本リージョンと同等の環境を構築した．西日本リージョンに切替対象となるシステムをレプリケーションし，有事の際にデータをリストアすることで，早期に業務復旧が図れる環境とした（図3二重線部）．

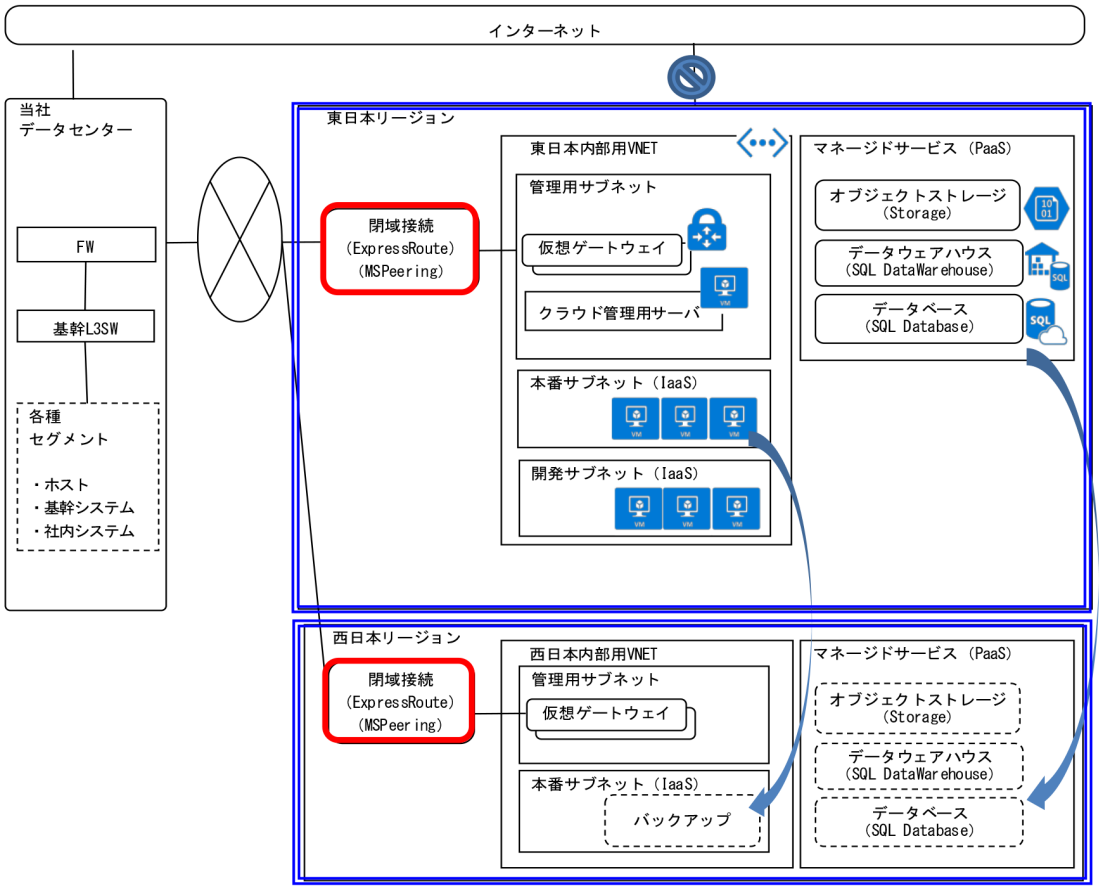


図3　Azure環境の構成図

3.2　クラウドにおけるセキュリティ対策

（1）外部機関によるセキュリティアセスメント

Azure環境への移行前に外部機関によるセキュリティアセスメントを行い，構築した当社システム基盤の環境にセキュリティホールが存在しないことを確認した．

セキュリティアセスメントには大きく2つの観点があり，1つ目はCIS[☆4]やAzureベストプラクティス[☆5]などの基準に応じて，当社システム基盤の各種オブジェクトの設定値が正しく設定されていることである．2つ目はFISC安全対策基準やISMSなどの基準と照らし合わせ，当社のクラウドにおける運用態勢が確立されていることである．

なお，セキュリティアセスメントは，大規模なネットワーク環境の変更および新しいサービスの利用の都度実施する運用とし，環境変更時にセキュリティレベルが低下しないよう徹底している．

（2）CASBの導入

セキュリティアセスメントにて安全性を確認した当社システム基盤の環境が，意図せず変更されていないことを継続的に監視するため，クラウドサービスの利用状況を可視化・監視するサービス「CASB」を導入した．

「CASB」はセキュリティアセスメントと同様に，CISベンチーマークおよびAzureのベストプラクティスなどの基準をベースとして，当社要件を踏まえた検知ルールをカスタマイズし，設定値に変更があった際は速やかに管理者に通知する仕組みとしている．

たとえば，仮想マシンにパブリックIPが付与されていた場合に検知するルールを作成することで，意図しない設定変更によるリスクに早期に気付くことができる．

4. 社内OAシステムのAzure移行

4.1 移行方針

Azureへの移行は，大きくIaaSを活用した単純マイグレーション（以下，IaaS移行）とPaaSを活用したシステム更改（以下，PaaS移行）に大別して行った．前者はハードウェア保守期限が迫っており，OSやそのほかソフトウェアの保守期限に余裕があるサーバを対象とし，後者はハードウェアおよびソフトウェアともに保守期限となるサーバを対象とした．

移行対象となる多くのサーバは，OSがWindows Server 2012で構成されていたため，作り直しによる開発工数の抑制を目的としてIaaS移行を選択し，ハードウェア，ソフトウェアともに保守期限となるDWHシステムは，PaaS移行を選択した．

前述のとおり，原則機密性・可溶性の低いシステムから順次移行することとし，2019～2020年度にかけて，4段階に分割して移行を行う計画とした．段階ごとの移行対象システムは**表3**に記載のとおりであり，影響度の低いシステムから移行を行うことで，問題発生時の影響を最小限に抑えるとともに，移行時のノウハウやプロセスを後続の段階に活かし，作業品質の向上を図れるよう工夫した．当社におけるAzureの活用イメージを**図4**に示す．

表3　移行フェーズごとの対象システム

移行フェーズ	移行対象システム	主な対象サーバ	サーバ台数	移行区分
第一段階	システム開発用（下図[A]）	・各種開発用サーバ	17台	IaaS
第二段階	可用性の低いシステム（下図[B]）	・システム運用系サーバ（ウイルス管理サーバ、ログ収集サーバなど、サーバ共通で利用する運用基盤）	14台	IaaS
第三段階	影響範囲が部門限定的なシステム（下図[C]）	・部門固有システム（不動産、主計部計算用サーバなど）	12台	IaaS
		・部門固有システム（DWHサーバ）	9台	PaaS
第四段階	影響範囲が全社的なシステム（下図[D]）	・全社利用システム（文書管理サーバ、社内ポータルなど）	17台	IaaS

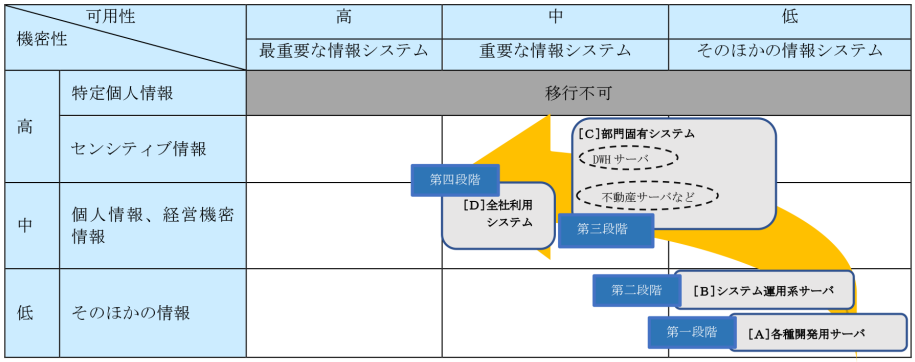


図4　当社におけるAzure活用イメージ

4.2　移行方式およびシステム冗長化

（1）AzureSiteRecovery サービスを利用したIaaS移行

IaaS移行では，クラウド事業者（マイクロソフト社）が提供する，オンプレミス環境の仮想マシンをAzure環境にレプリケーションし，移行を行うAzureSiteRecovery（以下，ASR）サービスを利用した．

ASRでは，OS以上のレイヤ（OS，ミドルウェア，アプリケーション，データなど）の整合を保った移行が行える（**図5**参照）ため，移行における工数を大幅に削減した移行を実現することができた．

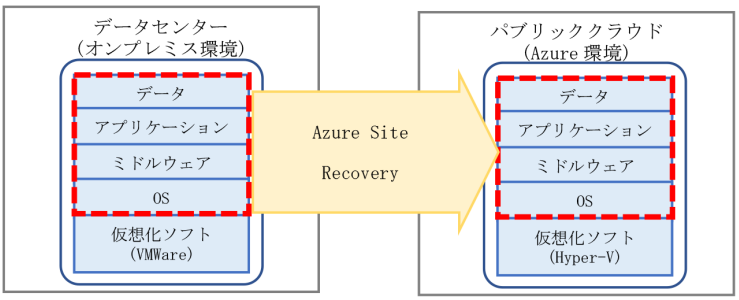


図5　Azure Site Recovery移行イメージ

（2）Azureにおけるシステム冗長化対策

オンプレミス環境のサーバは，仮想化基盤の障害発生時に待機系の仮想化基盤に移動し，継続稼動するよう設計されており，共通設備（ネットワーク機器・負荷分散装置など）や電源設備はシステムで共有する構成としている（SLA：99.9%）．

Azureにおける冗長化構成のオプションは，「HDD」「SSD」「可用性セット」「Site Recovery」の4種類（**表4**）あり，オンプレミス環境と同等の可用性をAzure環境で実現させるため，各システムの可用性要件に基づきオプションを選択，構築することでオンプレミス環境と同等の稼働率を確保する構成とした．

表4　Azureにおける冗長化オプション

オプション	概要	SLA	切替方法	障害時の対応	利用システム	コスト
HDD	・仮想マシンを HDD に配置。	なし	自動	・別仮想マシンに自動切替え （切替時間：約 15 分） ※15 分は目標値。	・各種開発用サーバ	低
SSD	・仮想マシンを SSD に配置。	99.9%	自動		・システム運用系サーバ ・部門固有システム	中
可用性セット	・同一リージョン内かつ共通設備が別の仮想化基盤で冗長化。 ・負荷分散装置を利用し、処理を冗長化しているサーバに分散。	99.95%	自動	・可用性セットを組んだ別マシンに自動振替え。 （切替時間：数十秒程度） ※負荷分散装置のヘルスチェック間隔に準ずる	・全社利用システム（文書管理サーバ、社内ポータルなど） ・一部の部門固有システム（DWH サーバなど）	高
Site Recovery	・別リージョンに仮想マシンを冗長化。 （日本の場合、東日本と西日本のデータセンターに仮想マシンを冗長化）	なし	手動	・別リージョンの仮想マシンに手動切替。 （切替時間：数時間程度） ※マシンの切替のみの時間は 30 分〜1 時間程度		

4.3　移行作業（IaaS移行）

（1）移行の進め方

移行にともない，移行対象サーバのIPアドレスおよび仮想化アーキテクチャ（VMware→Hyper-V）が変更となる．移行後の環境で各サーバの提供するサービスが継続的に利用できるよう，**図6**のとおり「現行調査」「初期移行」「切替テスト」「本番移行」の4ステップで，安全かつ着実にAzure環境への移行を進めた．

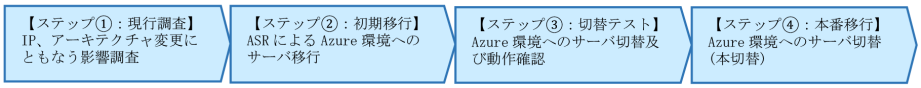


図6　IaaS移行の流れ

（2）現行調査

IPアドレスや仮想化アーキテクチャの変更にともない，移行対象サーバおよび関連サーバ，利用端末の観点から影響調査を行った．影響調査では，既存ドキュメント（設計書や運用手順書類）に加え，サーバや端末のミドルウェア定義，各種プログラム資源を確認，変更することで切替え漏れを防止した．

（3）初期移行

ASRサービスを使用し，オンプレミス環境の移行対象サーバのサーバイメージをAzure環境にレプリケーションした．差分データ量の多いサーバは，レプリケーション時に発生する通信量が多く，業務時間中にレプリケーションが行われた場合，回線の逼迫によるレスポンス劣化の影響が懸念された．そのため，レプリケーションで使用する通信量を時間帯により制御することで，業務に影響を与えることなく，日々の差分データのレプリケーションを実施した．

（4）切替テスト

移行対象サーバのホスト名を変更しない移行方針のため，テストについては，オンプレミス環境のサーバを停止した上で，Azure環境に切替える必要があった．

ASRのテストフェールオーバ機能（レプリケーションしている任意の断面からサーバをリストアする機能）を用い，Azure環境にリストアしたテスト環境に切替えた上で，移行対象サーバの疎通確認，機能確認および性能確認を行った．

①切替テスト時の通信制御

Azure環境へ切替後，利用者は意識することなくテスト環境にアクセスできる状態となる．そのため，Azure環境のサーバに対してAzureNetworkSecurityGroup（NSG）というAzureの仮想ファイアウォールの機能を利用し，疎通確認対象の関連サーバおよび切替テストで利用する端末のみ通信を許可することで，テスト環境に対して意図せぬ更新が発生しないよう制御を行った．

②段階的なテスト範囲の縮小

第1段階では，移行段階における最初のフェーズであることから，プログラムのバリエーションを踏まえた機能確認，全機能に対する性能確認を対象とした．

第1段階の移行結果に問題がなかったこと，およびASRの移行では，OS以上のレイヤに変更がなく，プログラムレベルでの動作変更は不要であることから，第2段階移行は，**表5**に示すとおりテスト種類ごとに確認内容を極小化し，テストの効率化を図った．

表5　テスト種類ごとの確認範囲

テスト種類	テストの確認ポイント（移行時の環境変更点）	テストの確認範囲	
		見直し前	見直し後
疎通確認	移行対象サーバの IP アドレス変更	**全接続先システムとの疎通確認**を行い、新 IP アドレスへの接続経路及び環境設定に問題がないことを確認。	**変更なし** 移行に伴う環境変更点や、テスト時における課題事項から、必要と判断。
機能確認	仮想化アーキテクチャの変更	**保有する全機能に対し、バリエーションを考慮した確認**を行う。 これまでと異なる仮想化アーキテクチャに対し、各種処理（シグナル）が正常に伝わることを確認する。	システムが保有する全機能に対し、**正常系１ケースを確認**することで網羅性を担保。
性能確認	物理的な機器設置場所・ハードウェアの変更	**システムが保有する全機能に対し、レスポンスの確認**を行う。	**代表機能の処理性能を確認**することで十分性を担保。

（5）本番移行

初期移行時に全量データを移行しているため，本番移行は差分データのみ反映，データ転送時間を最小限とすることで，移行後の稼動確認に十分な作業時間を確保するよう計画した．ASRにて前日からの差分をレプリケーションした最新の同期断面よりサーバイメージをリストアし，本番環境の構築を行った．IPアドレス変更にともなう移行対象サーバ，関連サーバおよび端末の変更資材をリリース後，保有する全機能の正常性確認を行い，Azure環境への移行を完了させた．また，本番移行においては，作業日あたり最大3サーバを上限とすることで，移行時の作業品質を確保した．

4.4　IaaS移行における課題と対応

（1）現行調査不足による関連システムの切替え漏れ

当移行においては，移行時にIPアドレスの変更を行うため，関連システムにおいても対応が必要となるが，テスト時に連携が正常に行えないケースが散見された．オンプレミス環境とAzure環境間のファイアウォールや，サーバ自身のファイアウォール機能の通信定義の考慮漏れが多く，現行調査の不足を露呈するものであった．

そのため，ネットワークのパケット情報取得コマンドを用い，移行対象サーバの通信情報を1カ月間取得し分析，網羅的に関連システムの影響を確認するよう改善した．

また**表6**に記載のとおり，調査に必要となる項目をまとめた調査シートを作成し，各担当者の個別知識に頼ることなく画一的な調査が可能となるようにした．

表6　現行調査シート　調査項目

項番	調査項目	主な調査観点
1	事前条件確認 （ASR前提条件確認）	.NET FrameworkやsshのバージョンなどASRを行ううえで、前提条件を満たしているかの確認
2	設計書・ドキュメント調査	・サーバ・ネットワーク設計書、運用設計及び夜間バッチなどのジョブ定義書の確認
3	システム環境情報調査	・OS バージョン、CPU、メモリなどのシステム情報、導入サービス一覧の整理
4	ソフトウェア情報	・Web/AP/DBサーバのソフト調査(IIS,Apache,SQLserverなど)
5	ネットワーク情報	・各サーバのNICに紐づくIPアドレス調査
6	通信要件	・DB連携(DB_LINK)や性能要求有無の確認 ・各ミドルウェアのIPアドレス保有有無調査 ・netstatコマンド取得結果の整理、確認
7	運用要件 （バックアップ）	・バックアップ取得時間の調査 ・保有世代数、遠隔地保管有無の調査
8	運用要件 （サーバ監視）	・死活監視、サービス監視、リソース(CPU,メモリ,ディスク使用率)監視有無の調査
9	サーバ資産調査	・移行対象サーバ及び関連サーバ/端末に対して、IP アドレス変更対象資材の調査。
10	NW機器通信制御設定	・移行対象サーバと関連サーバ/端末間のNW機器通信制御有無の調査 （ルーティング設定やファイアウォール定義有無の調査）
11	現行調査後変更確認	・現行調査完了後の移行対象サーバのシステム変更履歴の確認

（2）移行後の性能劣化

Oracleデータベースリンクによる大量データの結合に関して，データベース検索による性能確認時，特定の画面において検索性能が著しく劣化する事象が発生した（オンプレミス：16秒，移行後：40秒）．

当処理は，オンプレミス環境に存在するデータベースが，移行対象サーバのデータベースとリンクしており，Web画面から投入した検索SQLが，リンク先のデータベースとFULL OUTER JOIN（完全外部結合）する処理であり，検索時に大量データの通信が発生していることが原因であった．処理構成イメージを**図7**に示す．

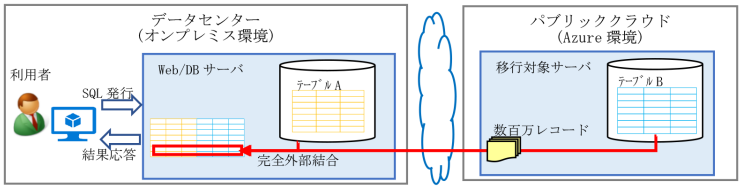


図7　処理構成イメージ

本原因における対応として，リンク先のテーブル保持データを整理し，授受するデータ量を削減することによって処理性能を改善した．

サーバ間で大量のデータ送受信を行う処理構成の場合，拠点が離れることにより，性能劣化が発生する可能性が高い．今後は，現行調査フェーズで当該処理の有無を確認し，保持データの整理など，事前に処理構成の見直しを行うことが必要である．

（3）メモリ保持メンテナンスへの対応

Azure環境に移行後，サーバ間伝送やデータベースへのロード処理が異常終了することがあり，調査の結果，Azure環境上のサーバに対してのセッション確立不可もしくは強制切断が発生していた．

Azureでは，クラウド事業者側の保守作業のため，任意のタイミングで最大30秒程度の停止を伴う「メモリ保持メンテナンス」があり，原因は当作業とサーバとのセッション確立が競合したことによるものであった．

メンテナンス時間は利用者側で指定することができないため，Azure環境に構築・移行する際は，「メモリ保持メンテナンス」を考慮した処理構成とする必要がある．

4.5　移行作業（PaaS移行）

（1）システム構成の検討

現行DWHシステムは，複数の物理サーバで構成したクラスタにPostgreSQL系のDWHソフトウェアを組み込んでいた．移行にあたり，同様の構成をIaaSの仮想マシンで実現することも可能であったが，移行方針に則りサービスとして利用できるPaaSのAzureSynapseAnalytics（以下，AzureDWH）を採用することとした．

IaaSの仮想マシンを利用する場合，現行DWHシステムと同様の構成・DWHソフトウェアを選択することができるため，既存定義情報などを流用でき，移行負荷を軽減できる．その反面，サーバの構築，DWHソフトウェアの導入・設定が必要であり，またOS・ソフトウェアの保守ライフサイクルにあわせて更改対応が必要となる．

PaaSのDWHサービスを利用する場合，SQL Server系のDWHソフトウェアであるため，移行時に定義情報などの変換が必要となる．しかし，OSやミドルウェアのレイヤを考慮する必要がなく，スペックを選択後1時間足らずで利用を開始することができ，保守ライフサイクルにあわせた更改作業から開放されるというメリットの方が大きいと判断した．

なお，移行先のPaaS選定にあたっては事前にAzureDWH上にテーブルを作成し，サンプルデータのロードおよび検索テストを実施し運用面・性能面で問題がないことを確認した．IaaSの仮想マシンを使用する場合，実機での事前検証は費用・期間などの面で対応が難しいが，PaaSを使用することで利用した分の従量課金のみ，即日環境準備が可能となり事前検証を効率的に行うことができた．

また，大規模なクラウド障害などが発生した際にも継続して業務が行えるよう，**図8**に示すとおり，通常使用する東日本リージョンとは異なる西日本リージョンに遠隔地バックアップを取得する構成とした．東日本リージョンでトラブルが発生した際には，**図9**に示すとおり西日本リージョンでサービスを起動しデータを復元することで業務継続を可能とした．

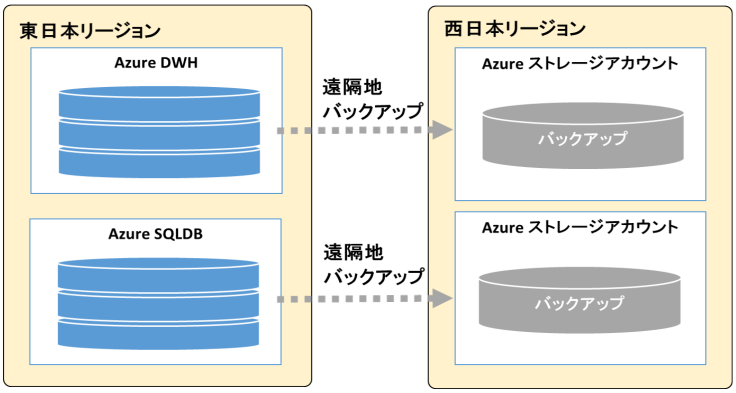


図8　AzureDWHにおけるバックアップ方式

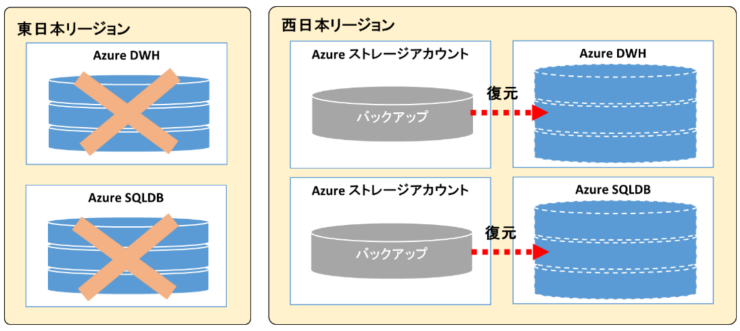


図9　障害発生時の復元イメージ

（2）セキュリティ対策

AzureDWHの初期構築状態では，インターネットから誰もがアクセスできる状態となっている．移行データには保険契約情報などのお客さま情報や経営に関する機密情報などが含まれるため，専用線経由でのアクセスのみAzureDWHを利用できるよう対策を実施した．

また，移行データにおける病歴・健康診断結果などのセンシティブ情報は，個人を特定できない形に加工，暗号化を実施した．セキュリティ上，十分な対策を取っており情報漏洩の可能性はきわめて低いが，お客さま情報を保護するため二重・三重のセキュリティ対策を行った．

（3）移行作業

①定義情報の移行

現行のDWHシステム（PostgreSQL系）とAzureDWH（SQL Server系）では製品が異なるため，DDL（テーブル定義）やフォーマット情報などの定義情報はそのまま移行することができない．現行DWHシステムとAzureDWHの定義情報の相違点を洗い出し，変換対応表を作成した．この変換対応表をもとに定義置換ツールを作成し，定義情報の移行を効率的に行った．

②データの移行

現行のDWHシステムとAzureDWHで製品は異なるが，RDBMSであるため通常のデータベース移行と同様に，データ移行はExport→Importで実施した．移行後はまったく同じデータが移行できており，どちらのDWHでも同じ結果が得られることを確認するために全データの一致確認を実施した．DWHシステムで保有するデータが約1TB，10億レコードと非常に多いため，確認作業に多くの時間を費やした．データ移行・比較方式を**図10**に示す．

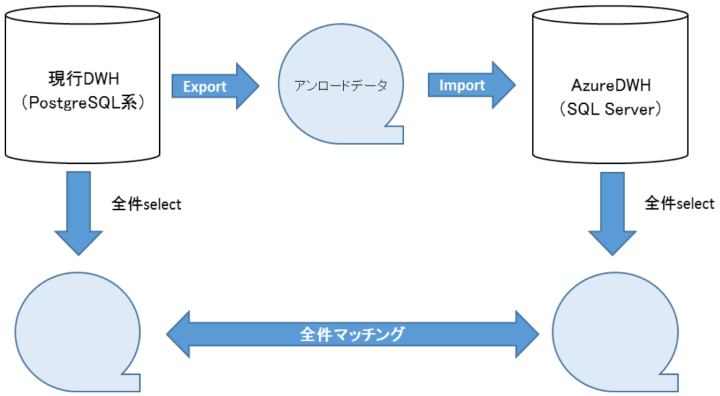


図10　データ移行・比較方式

4.6　PaaS移行における課題の検出と対応

データ移行後，本番環境と同等のテーブル構成・データ件数での機能確認および性能確認を実施した．機能面では特に問題なく，現行DWH・AzureDWHで同等のデータ抽出ができることを確認したが，性能面での課題を検出した．具体的には特定の定型SQLを連続実行するWebツールを実行すると，トータルでの処理時間に差が出るという内容だった．

事前の性能検証時点ではWebツールとAzureDWHの接続ができず，Webツールから発行されるSQL単体の性能検証を実施していた．そのため，連続実行すると性能差が出るという点を検知できていなかった．**表7**に性能差の発生イメージを示す．

表7　性能差の発生イメージ

	単体実行		連続実行	
	現行 DWH	AzureDWH	現行 DWH	AzureDWH
SQL①	5 秒	5 秒	5 秒	5 秒
SQL②	5 秒	5 秒	1 秒	5 秒
SQL③	5 秒	5 秒	1 秒	5 秒
SQL④	5 秒	5 秒	1 秒	5 秒
合計	20 秒	20 秒	8 秒	20 秒

性能差が発生した原因は現行のDWHシステムとAzureDWHのDBMSの仕様相違によるもので，現行のDWHシステムでは，SQLのアクセスプランのキャッシュ効果から，短時間に同テーブルへ連続発行される2回目以降の処理時間が高速化することが判明した．AzureDWHは大規模データの並列処理に特化しており，現行のDWHシステムと同様のキャッシュ機能がなく，SQL連続発行時に性能差が生じていた．

対応の検討にあたりWebツールから実行されるSQLを分析した結果，インデックスを使用したアクセスプランの最適化が有効であることを確認した．対応策として，Webツールから利用する対象のテーブルをPaaSの通常のRDBMSであるAzureSQLDatabase（以下，AzureSQLDB）にも格納し，Webツール実行時の参照先をAzureSQLDBとする方針とした．AzureDWHでの結果セットのキャッシュなどのチューニングも検討したが，BIツールからの非定型検索処理やデータロード処理の性能に影響するケースがあるため，用途に応じてDBMSを分離することが最適と判断した．対応前後の構成を**図11**に示す．

当対応により，Webツールからの連続実行時の処理性能は現行同等以上となり，性能面での課題を解消することができた．

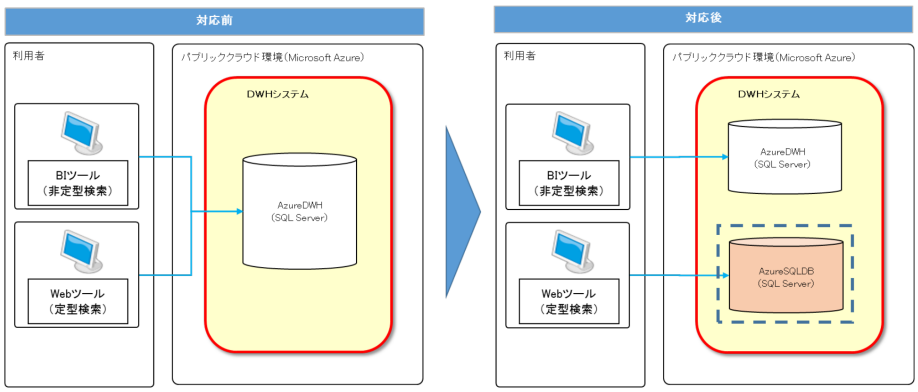


図11　対応前後の構成

5. 評価

5.1 定量評価

（1）コスト削減

オンプレミス環境の社内OAシステムをAzure上の仮想マシンもしくはサービスに移行することで，5年ごとに発生するハードウェア更改の費用も含め現行比で最大50%減のコストメリットを享受することができた．**図12**に示すとおり，クラウドの場合，物理的な機器導入や設備関連の費用がなく，また更改時はソフトウェア保守切れ対応のみでハードウェア作業が不要であり並行期間中の二重負担などもない．

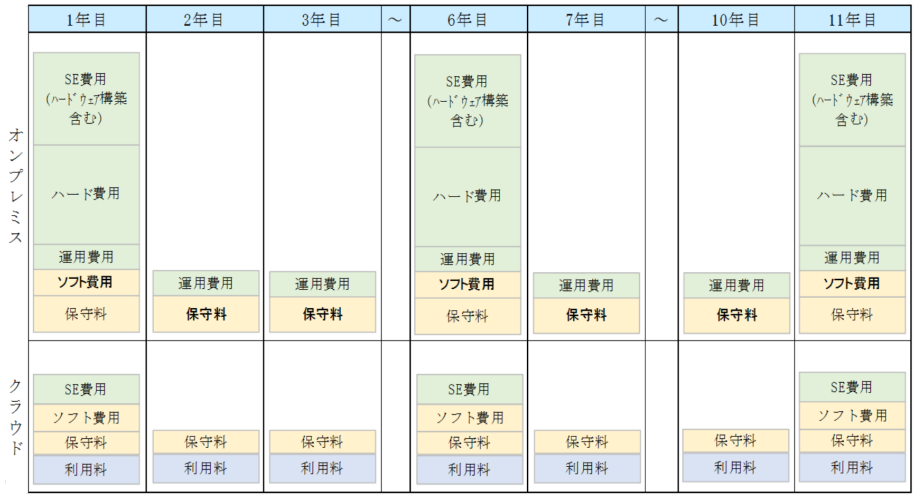


図12　コストの比較

さらにPaaSを採用するDWHシステムは，ソフトウェアのバージョンアップやバグフィックスもクラウド事業者側の作業となり，ハードウェアやソフトウェアの保守期限によるシステム更改作業が不要となった．また，データセンタの停電作業やハードウェアのファームアップ，ハードウェアに起因した障害対応などがクラウド事業者側で行われることで，年間10人月相当の内部工数の削減に繋がっている．

（2）開発期間の短縮

一般的に新規システム構築時においては，プログラムとは別にサーバ導入が必要であり，サーバ導入時には機器搬入・電源配備・ネットワーク敷設といった物理作業のほか，OSインストール，初期設定などの手配・作業が必要である．パブリッククラウドを利用することで，上述したシステムインフラ構築に伴う作業期間を短縮し，**図13**に示すとおりサーバ構築において約8週間の作業期間を約2週間に削減することができた．

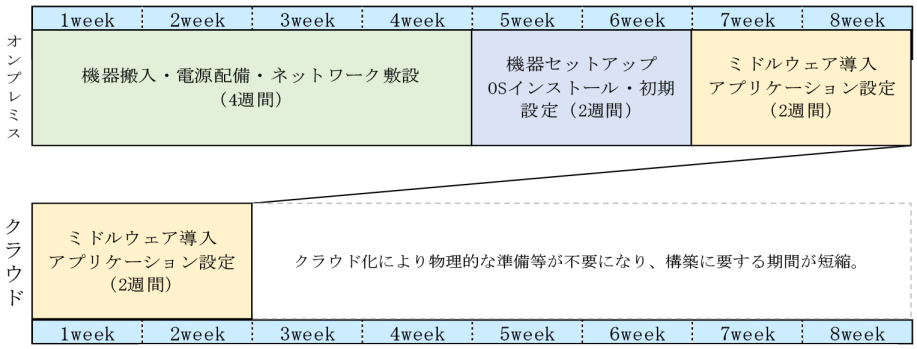


図13　開発期間の短縮

5.2　定性評価

（1）拡張性・柔軟性の向上

物理的なシステムリソース（CPU，メモリ，ディスク）を意識することなく，リソースの変更を短時間で行えるため，処理集中時など，システムの利用頻度に合わせた柔軟な対応が可能となった．ユーザ検証環境やシステム開発環境など，常時起動する必要がないシステムは，利用時のみの起動とし，コスト削減にも繋げることができた．

（2）可用性の向上

オンプレミス環境の社内OAシステムは，同一データセンタ内の複数機器で冗長化しているが，拠点災害を想定した他拠点への冗長化は行っていない．Azureで提供されているサービスを利用することで，有事の際は西日本リージョンへの切替えを可能にし，可用性の向上が図れた．

（3）生産性の向上

Azureでは仮想マシンの複製機能を用いて，パラメータの設定作業などを行うことなく，本番環境と同等の環境を迅速に構築することができる．複製した環境を利用することで，システム開発におけるテストおよびテスト準備に要する期間の短縮が可能となる．

また，障害時においても，本番環境から分離された環境での検証を迅速に行うことでき，生産性の向上に繋がった．

（4）クラウド関連スキルの向上（クラウド・エンジニアの育成）

クラウド・エンジニア育成に向けては，専用の育成フレームワーク（**表8**）を定め，フレームワークに沿って計画的にスキル習得を行った．具体的には，必要なスキル要素を，3種類（「インフラ構築」「インフラ運用」「セキュリティ」）に分類し，それぞれの要素につき成熟度（初級，中級，上級）を定め，各人が年度ごとに目標を立て，IaaS移行やPaaS移行の案件対応や社外研修，Off-JTを通じてスキル向上を図った．

スキル評価は外部機関による第三者評価とし，2019年度においては，目標としていた人数の初級認定を達成することができ，達成者全員がAzure関連の資格☆6を取得することができた．2020年度は中級認定に向けて計画的にスキルを向上に取り組んでいる．

表8　クラウド・エンジニア育成フレームワーク

クラウド・エンジニア成熟度レベル		スキル要素		
		インフラ構築	インフラ運用	セキュリティ
上級	**【最適化、管理】** 先進事例を把握し、各リソースを組み合わせて、自社システムの最適化が可能	・自社のシステムインフラを含めた全体最適の設計。 ・最新のサービスも活用したインフラの設計・構築。	・自社のシステム運用の全体最適・自動化などの設計。 ・最新のサービスを活用したシステム運用の自動化・実装。	・既存セキュリティ機能を含めたAzure利用時の最適な設計。 ・Azure のサービスを活用した、セキュリティ対策の実装。
中級	**【設計者】** サーバ/ストレージ/NW、運用など、各種設計が可能	・要件に適した構成設計及びサイジング設計。 ・Azure 移行作業、リスク対策などを確認したうえでの移行計画の策定。	・非機能要件に合わせたサービスの停止起動、バックアップなどの運用設計。	・ネットワーク設定や暗号化など、Azure 利用時のセキュリティの設計。 ・AzurePortal のアクセス権限設計。 2020 年度目標
初級	**【担当者】** 手順作成～作業・確認まで一連の実務作業が可能	・システム基盤の構築、変更及び、作業結果の確認。 ・準備から結果確認まで一覧の移行作業の実施。	・ログ監視などの運用ツールの作成、実行。 ・Job の自動化スクリプトの生成、実行。	・ネットワーク設定、暗号化の設定作業。 ・アカウント、アクセス権限作成、変更。
	【作業者】 クラウドに関する共通知識習得し、手順書の作業が可能	・インフラ構築やサーバ移行に必要な IaaS の概要の理解。 ・手順書に従った Azure 上でのサーバ構築、移行作業の実施。	・リソース及び死活監視の概要理解。 ・AzurePotal やコマンドレットでのシステムの起動、停止などの定例的な運用の実施。	・Azure 利用時のリスク、事業者のセキュリティ対策の理解。 ・手順書に従ったストレージなどの暗号化対策の実装。 2019 年度目標
前提スキル		一般的なシステムインフラの基礎知識		

6. 今後に向けて

今回のパブリッククラウドの活用により，機動的なシステム基盤構築のための下地を作ることができ，コスト面においても効果のある施策であった．しかしながら，今回の移行では既存システム機能を保証したIaaS移行が中心であり，クラウドのメリットを全面的に享受できているとはいえない．今後に向けては，各システムが求められている機能に応じてクラウドネイティブに作り変えていくことでさらなる「システム開発力の一層の強化」と「デジタル化の推進」に取り組んでいきたい．末筆ながら，本更改にあたり多大なご支援・ご協力を賜ったソリューションベンダ各社殿，メーカ各社殿，関係各社の皆様に心から感謝の意を表するとともに，本稿がユーザ企業，システム業界に携わる方々の参考となれば幸甚である．

脚注

☆1　社内OAシステム：ポータルや文書管理など，社内共通で利用するシステムおよびBIなどでデータ参照するDWHシステムの総称．

☆2　パブリッククラウド固有の想定リスク：ネットワーク分離やデータ消去などの情報漏洩対策，サービス停止時における対処や統制管理など，利用者対策と事業者選定の観点より，パブリッククラウド利用時のリスクを洗い出し（合計58項目）．

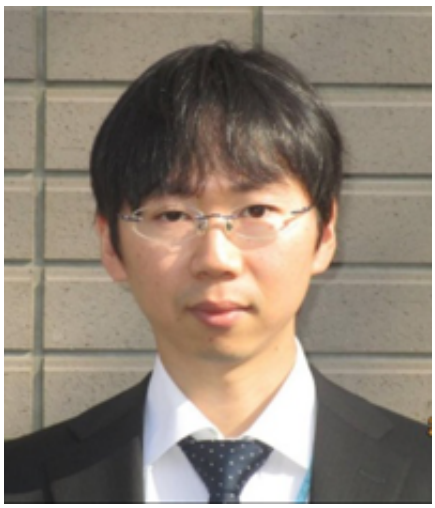
☆3　東日本・西日本リージョン：データセンタを設置している完全に独立した地域のこと．Azureは全世界に52のリージョンを保持しており，国内では東日本リージョンと西日本リージョンの2リージョンが存在する．

☆4　CIS：インターネット・セキュリティ標準化団体が定めている「Azureセキュリティベンチマーク」（全92項目）．

☆5　Azureベストプラクティス：「Azureセキュリティのベストプラクティス」（全14項目）．

☆6　マイクロソフト社の認定プロフェッショナル（MCP）のAzureに関する資格試験．

白石征久（非会員）shiraishi.yukihisa.661712@daido-life.co.jp
2004年入社．2020年現在，テクニカルサポート二部．IT基盤管理二課 課長代理．



佐田野直樹（非会員）sadano.naoki@daido-life.co.jp
2008年入社．2020年現在，テクニカルサポート二部．IT基盤開発課 課長代理．

堀　仁人（非会員）hori.yoshito.541712@daido-life.co.jp
2010年入社．2020年現在，テクニカルサポート二部．IT基盤管理二課．

採録決定：2021年3月10日
編集担当：斎藤彰宏（日本アイ・ビー・エム（株））