クラウドマイグレーションのためのガイド

第 1.0 版

平成 24 年 6 月

ジャパン・クラウド・コンソーシアム　クラウドマイグレーション検討ワーキンググループ

目次

委員名簿

主査	(株)日立製作所	樋野 匡利
委員	(株)IDC フロンティア	内山 大輔
委員	(株)IDC フロンティア	石橋 誠之
委員	ITC 近畿会 SaaS/クラウド研究会	生田 勝
委員	アラクサラネットワークス(株)	新 善文
委員	伊藤忠テクノソリューションズ(株)	中島 淑乃
委員	(株)インターネットイニシアティブ	新 麗
委員	(株)インテック	永見 健一
委員	(株)ＳＴＮｅｔ	勝賀瀬 修
委員	(株)エヌティティデータ	江森 恭太
委員	エプソン販売(株)	渡辺 将司
委員	(株)ジェーエムエーシステムズ	長澤 浩
委員	首都大学東京 産業技術大学院大学	瀬戸 洋一
委員	(社)情報通信技術委員会	田村 潤三
委員	ソフトバンクテレコム(株)	有賀 祥平
委員	(株)東芝	瀬尾 尚史
委員	東芝ソリューション(株)	岩崎 孝夫
委員	東芝ソリューション(株)	大友 雅裕
委員	東芝ソリューション(株)	望月 祐之
委員	21 世紀ＩＴＣクラブ	野田 和生
委員	日本 CIO 協会	米田 日出海
委員	日本情報経済社会推進協会	小坂 周一郎
委員	日本電気(株)	高橋 博
委員	日本ヒューレット・パッカード(株)	薗川 元樹
委員	日本ヒューレット・パッカード(株)	丸山 昌平
委員	日本ヒューレット・パッカード(株)	高山 卓
委員	日本ヒューレット・パッカード(株)	山下 和也
委員	日本ヒューレット・パッカード(株)	向井 純太郎
委員	日本マネジメント総合研究所	戸村 智憲
委員	(株)野村総合研究所	稲月 修
委員	バリオセキュア･ネットワークス(株)	稲見 吉彦
委員	(株)日立システムズ	新貝 知晃
委員	(株)日立システムズ	加藤 俊路
委員	(株)日立製作所	大西 治
委員	(株)日立ソリューションズ	藤岡 秀樹
委員	ヒューリット･マネジメント･フォーラム	川野 太
委員	プライスウォーターハウスクーパース(株)	一山 正行

委員	三菱 UFJ リース(株)	宮崎 明大
委員	(株)山忠	米田 久行
委員	リコージャパン(株)	赤澤 義秋
事務局	(株)日立コンサルティング	伊藤 泰樹
事務局	(株)日立製作所	秋沢 充
事務局	(株)日立製作所	白川 幸博
事務局	(株)日立製作所	三宅 滋
事務局	(株)日立製作所	青木 隆史
事務局	(株)日立製作所	鈴木 芳生

(社名五十音順、2012 年 6 月時点)

- 利用者自身の責任で利用下さい。ジャパン・クラウド・コンソーシアムならびに執筆関係者は、本ガイドラインの利用によって生じるいかなる損害についても責任を負うものではありません。
- 出典を明記するなど著作権法の規定する引用の範囲内でご利用下さい。
- 本ガイドに記載の商品名・サービス名は、一般に各社の商標または登録商標です。
- 本ガイドは 2012 年 6 月時点のものであり、記載された内容は今後、断りなく変更される可能性があります。

ジャパン・クラウド・コンソーシアムは、団体、業種の枠を超えてクラウドサービスの普及・発展を産学官が連携して推進するために設立された民間団体です。総務省、経済産業省および農林水産省がオブザーバとしてコンソーシアムの活動を支援しています。

1. はじめに

1.1. 本ガイドの目的

情報システムを自社や自組織で所有せずに、外部の事業者が提供する計算リソースを必要な時に使用するクラウドサービスが注目を集めている。情報システムにクラウドサービスを活用することで、その上で動作する業務や経営の効率向上を図っていくことは、今後、ますます拡大していくと考えられる。

クラウドサービスの活用は、利用形態や契約形態の変化を引き起こすだけでなく、海外からの利用やモバイル端末からのアクセスなど情報システムの利用場面の変化をも引き起こしていく。これまでは、情報システムを立ち上げ・運営していくには、企画、設計、構築、運用といった一連のプロセスにしたがった作業が必要であったが、クラウドサービスを利用する場合には、利用形態、利用場面、契約形態の変化にしたがって、各プロセスにおいて検討・確認すべき点も変わってくる。

そこで、ジャパン・クラウド・コンソーシアム クラウドマイグレーション検討ワーキンググループ(以下、WG)では、既存の情報システムの全て、あるいは一部を、クラウドサービスにマイグレーション（移行）する際に、円滑に実施するための支援を目的として、ガイドを作成することとした。具体的には、本ガイドでは、移行にあたって、検討・確認すべき点や検討の参考になる情報を提示している。

なお、本ガイドで提示した項目は、クラウドサービスへの移行にあたって、クラウドに特化した部分のみに着目して検討・確認すべき項目を列挙しておくことを意図したものである。ガイドの活用にあたっては、対象となる情報システムや業務の特徴などを十分に把握した上で、必要となる部分のみを検討するなど適切に活用して頂きたい。

1.2. 対象読者と対象範囲

本ガイドは、クラウドサービスの利用者を対象読者としている。すなわち、クラウドサービスの導入・移行を検討している企業、団体、組織において、導入・移行作業に関わる関係者、または、導入の決定に関わる関係者を対象としている。また、対象範囲としては、クラウドサービスの形態として IaaS(Infrastructure as a Service)、PaaS(Platform as a Service)、SaaS(Software as a Service)の全てが対象であり、特に限定は置いていない。

1.3. 本ガイドの構成

本ガイドでは、2 章に情報システムを立ち上げ・運営していくプロセス観点で検討・確認すべき項目をまとめた。すなわち、企画、設計、構築、運用のプロセスにおいて、検討・確認すべき点、あるいは、参考情報をまとめた。また、3 章では、プロセス観点以外の検討項目として、海外拠点を活用する場合の検討項目や注意点を提示した。

なお、本ガイドでは、移行時の検討項目については、以下のガイドラインを参考とした。また、本ガイドで用いる技術用語については、「クラウドサービス利用者の保護とコンプライアンス確保のためのガイド（案）[1]」（ASP・SaaS 普及促進協議会）の技術用語の解説、「クラウド・コンピューティング時代の SAM の考え方[2]」（JIPDEC）の用語の解説等を参照頂きたい。

[1] http://www.aspicjapan.org/feedback/pdf/attachment_jp_01.pdf
[2] http://www.isms.jipdec.or.jp/sam/doc/JIP-SAM113-10.pdf

[参考にしたガイドライン]

策定者	ガイドライン名称	公開時期
総務省	地方公共団体における ASP･SaaS 導入活用ガイドライン http://www.soumu.go.jp/main_content/000061414.pdf	2010 年 4 月 1 日
総務省	公共 IT におけるアウトソーシングに関するガイドライン http://www.soumu.go.jp/denshijiti/pdf/060213_03.pdf	2003 年 3 月
総務省	ASP･SaaS の安全・信頼性に係る情報開示指針 http://www.soumu.go.jp/main_content/000018194.pdf	2011 年 12 月 16 日
総務省	ASP･SaaS における情報セキュリティ対策ガイドライン http://www.mhlw.go.jp/shingi/2008/07/dl/s0730-18l.pdf	2008 年 1 月 30 日
経済産業省	クラウドサービス利用のための情報セキュリティマネジメントガイドライン http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html	2011 年 4 月 1 日
経済産業省	SaaS 向け SLA ガイドライン http://www.meti.go.jp/committee/materials/downloadfiles/g80207c05j.pdf	2008 年 1 月 21 日
情報処理推進機構（IPA）	中小企業のためのクラウドサービス安全利用の手引き http://www.ipa.go.jp/security/cloud/documents/cloud_tebiki_V1.pdf	2011 年 4 月 25 日
情報処理推進機構（IPA）	欧州 ENISA のクラウドのセキュリティに関するガイドラインの翻訳 http://www.ipa.go.jp/security/publications/enisa/index.html	2010 年 10 月 25 日
特定非営利活動法人 ASP・SaaS・クラウドコンソーシアム （ASPIC）	クラウドサービス利用者の保護とコンプライアンス確保のためのガイド～経営層による的確なリスクマネジメントのために～ http://www.aspicjapan.org/feedback/pdf/attachment_jp_01.pdf	2011 年 7 月 12 日
総合行政ネットワーク運営協議会	総合行政ネットワーク ASP ガイドライン（3.5 版） https://www.lasdec.or.jp/cms/resources/content/7638/C-7-1_AspGuideline_200905211.pdf	
Cloud Security Alliance（CSA）	Security Guidance for Critical Areas of Focus in Cloud Computing http://www.cloudsecurityalliance.org/guidance/csaguide.pdf	2009 年 4 月 1 日
National Institute of Standards and Technology （NIST）	Effectively and Securely Using the Cloud Computing Paradigm http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-pmell-day3_cloud-computing.pdf	2009 年 10 月 7 日

[参考文献]

著者	文献名称	発行時期
一般財団法人日本情報経済社会推進協会 (JIPDEC)	クラウド・コンピューティング時代の SAM の考え方 http://www.isms.jipdec.or.jp/sam/doc/JIP-SAM113-10.pdf	2010 年 6 月
特定非営利活動法人 ASP・SaaS・クラウドコンソーシアム （ASPIC）	SaaS サービス検索 http://www.aspicjapan.org/search/index.php	
財団法人マルチメディア振興センター	ASP･SaaS の安全・信頼性に係る情報開示認定制度 (安全・信頼性の情報開示基準を満たしているサービス一覧) http://www.fmmc.or.jp/asp-nintei/service.html	2009 年 2 月より実施
日経 BP 社　ITpro Active	クラウドサービス総覧 2011 年版　SaaS 編 http://itpro.nikkeibp.co.jp/active/2011saas/index.html	
OASIS(Organization for the Advancement of Structured Information Standards)	SAML(Security Assertion Markup Language) V2.0 https://www.oasis-open.org/jp/specs/#samlv2.0	2005 年 3 月
Micorosoft, IBM, VeriSign	Web Services Federation Language (WS-Federation) http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-fed/WS-Federation-V1-1B.pdf	2006 年 12 月
Micorosoft	Understanding WS-Federation http://msdn.microsoft.com/en-us/library/bb498017.aspx	2007 年 5 月 28 日
OASIS(Organization for the Advancement of Structured Information Standards)	Web Services Security v1.1 https://www.oasis-open.org/jp/specs/#wssv1.1	2006 年 2 月
OpenID ファウンデーション・ジャパン	OpenID Authentication 2.0 - 最終版 http://openid-foundation-japan.github.com/openid-authentication.html	2010 年 1 月 19 日
総務省	自治体クラウド開発実証事業成果 http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/index.html	2011 年 9 月 7 日
経済産業省	輸出管理クラウドコンピューティングと日本の競争力に関する研究会 報告書 www.meti.go.jp/press/20100816001/20100816001-3.pdf	2010 年 8 月 16 日
American Institute of CPAs	内部統制（SSAE16） http://www.aicpa.org/Pages/Default.aspx	
一般財団法人日本情報経済社会推進協会 (JIPDEC)	ISMS 適合性評価制度 http://www.isms.jipdec.jp/isms.html	

2. クラウドマイグレーションの各プロセスで検討すべき項目

本章では、クラウドサービスへのマイグレーション（移行）を行う際に、プロセス観点で検討・確認すべき項目をまとめた。

2.1. クラウドマイグレーションのプロセスと検討の前提

本ガイドでは、クラウドマイグレーションのプロセスを、開発の一般的なプロセスとして知られている企画、設計、構築、運用とし、プロセスにおいて必要となる検討項目を 2.2 節に整理した。また、セキュリティなど、クラウドサービスへの移行を検討する際に、特に利用者からの質問が多い項目に関しては、2.3 節において個別項目ごとの整理も行った。海外拠点活用に関しても、特記検討すべき内容が多いことから、本章とは別章（3 章）でまとめることとした。

なお、当初はクラウドサービスの提供形態（IaaS、PaaS、PaaS など）で検討内容が大きく異なると想定していたが、共通した検討項目も多く、明快な切り分けは容易でないため、本ガイドでは提供形態での分類は行わなかった。

2.1.1. 検討の枠組みと前提

本節では、2.2 節の検討の枠組みを示す。2.2 節では、クラウドマイグレーションのプロセスにおいて検討・確認すべき項目を、実施項目と検討事項の形で整理した。全体を俯瞰して把握しやすくするために、各節の冒頭に表形式で示した後、詳細を補うために文章形式で示している。特に、対応方法まで明らかになっている課題については、対応方法を記載しているガイド等を参考情報として示した。

2.1.2. クラウドマイグレーションのプロセス

本ガイドでは、以下のマイグレーションのプロセスに沿って、実施項目・検討事項をまとめた。

企画フェーズは、クラウド移行の企画を行うフェーズである。セキュリティなど各種要件を定め、構想・企画書を作成するフェーズである。設計フェーズは、クラウドサービスとオンプレミスとの接続部分やデータの設計を行い、設計書・仕様書にまとめるフェーズである。構築フェーズは、作成した設計書・仕様書に基づいて、構築を行うフェーズである。また、事前テストやデータ移行等も行うフェーズである。運用フェーズは、上流工程での検討に基づいて、運用管理や変更管理を行うフェーズである。また、契約の変更・終了では、クラウドサービスを終了させる場合、あるいは、さらに他のクラウドサービスへ乗り換える際に必要となる検討を行う。

2.2. クラウドマイグレーションプロセスにおいて検討すべき項目

本節では、企画/設計/構築・テスト・移行・教育/運用/契約の変更・終了といったマイグレーションプロセスにおいて、検討すべきことを示す。

2.2.1. 企画フェーズ

企画フェーズでは、下表に示す実施項目にしたがってマイグレーションを進めていく。以降では、実施項目ごとに、マイグレーションにおいて特に注意して検討・確認すべき事項を説明する。

#	実施項目	検討・確認事項
(1)	対象業務・対象システムの分析	業務の特殊性　（業務要件、ピーク変動性）
		データの特殊性
		システムの特殊性　（停止可能時間、運用）
		システム基盤の共通性
		周辺システムとの関連性
(2)	利用クラウドサービス調査	SaaS 調査
		IaaS／PaaS 調査
		トライアル利用
		データ移行方法
		BCP(Business Continuity Planning)／DR(Disaster Recover)対応
		SLA(Service Level Agreement)確認
(3)	新業務・新システムイメージの具体化	自社要件への対応
		周辺システム・既存ネットとの接続方法
		帳票作成・プリント
		運用の変更点
(4)	導入効果の算定	費用対効果
		導入のメリット
(5)	リスクの洗い出し	信頼性・性能
		セキュリティ　（データの保全）
		コンプライアンス　（監査対応）
		サービス継続性
		移行中止の判断
(6)	その他	推進体制
		スケジュール
		サービス利用の停止
		社内コンセンサス

(1) 対象業務・対象システムの分析

- **業務の特殊性（業務要件、ピーク変動性）**

システム移行を企画する際には、移行システムと対象業務の要件を分析し、クラウドサービスの利用メリットを検討する必要がある。

- SaaS 移行の場合、自社独自の業務要件がほとんどない業務内容であるかを確認
- 業務量が事業の拡大・縮小あるいは季節などで大きく変動する業務は、クラウド向き
- インターネット経由になると応答時間が数秒以上かかる場合があることに注意

現行利用しているシステムの以下の点については、特に確認しておくとよい。

- 業務量の明確化（業務量、伸び率、ピーク率、ピークの予測可否）
- 当該業務の入力、出力量、要求応答時間
- 業務停止時の影響評価（クラウド選定時の参考とする）
- 業務プロセスの SaaS サービスとの適合性の確認（新規に SaaS 化をする場合）
  - 業務プロセスを既存クラウドサービスに合わせることも評価する

また以下の確認や整理も行うとよい。

- クラウドへ移行する際に、改善したい課題事項を整理
- 既存システムの設計ドキュメント等の確認（設計当初と現システムの差異明確化）
- 非機能要件（可用性、性能、拡張性、運用・保守、移行、セキュリティ）等の現状確認とクラウド移行後の要件

- **データの特殊性**

クラウドへの外出しが可能な機密レベルのデータであるかを、以下に注意して確認する。

- 情報の重要度の確認
- セキュリティポリシの確認
  - 個人情報の有無
  - データ配備場所の制限（法規制の確認。詳細は 3 章を参照のこと）
    （個人情報はオンプレミスに配置し、リンク情報でクラウド上のデータとリンクさせる等）
  - ユーザ ID の整理等
- バックアップの必要性の確認
- 初期構築時の移行データ量

なお、高い機密性が必要であればプライベート接続をネットワーク要件に加える

- **システムの特殊性（停止可能時間、運用）**

自社設置クラウドのケースを除き、リモート運用が基本となるため、以下に注意の上で外出しできるシステムかどうか判断する。

- 業務の停止可能時間の制約
- システム運用の確認（テープ運用、帳票出力有無、特殊装置、装置ハンドリング有無）
- トラブル時の対応等の考慮

- **システム基盤の共通性**

以下を調査の上で既存システム基盤の共通性を分析し、クラウド上に標準化できるかどうか判断する。

- OS(Operating System)、ソフトウェアプロダクト等の現状
- 業務システムの更改時期や更改コスト概算等

- **周辺システムとの関連性**

周辺システムと大量データのやりとりを行うシステムはネットワーク遅延の問題を発生する可能性が高いことから、周辺システムとのデータ連携が少ないシステムがクラウド向きである。そのため、既存システムについて以下を調査しておく。

- システム間接続の有無
- 送受データの量、タイミング、応答時間等
- ユーザ認証等の連携有無

(2) 利用クラウドサービス調査

- **SaaS 調査**

以下の観点にも注意した上で、対象業務に適合するクラウドサービスがあるか調査し、候補となるクラウドサービスを比較検討する。

- 国内法令等改正に対応したアプリケーションのアップデートの計画・実施状況
- 業務要件・システム要件に沿ったカスタマイズの可否
- クラウドサービスの機能要件、契約条件の他、サポート体制（国内にサポート拠点があるか、電話、メール、オンサイトなどどういったサポートが期待できるか）

＜参考情報＞

SaaS サービス検索（ASP･SaaS・クラウド　コンソーシアム）

http://www.aspicjapan.org/search/index.php

安全・信頼性の情報開示基準を満たしているサービス一覧　（財団法人マルチメディア振興センター）

http://www.fmmc.or.jp/asp-nintei/service.html

クラウドサービス総覧 2011 年版　SaaS 編　（日経 BP 社　ITpro Active）

http://itpro.nikkeibp.co.jp/active/2011saas/index.html

- **IaaS/PaaS 調査**

以下の観点で、対象システムに適合するクラウドサービスがあるかを調査し、候補サービスを比較検討する。サービスの機能要件、契約/価格条件の他、サポート体制も調査する。

- クラウドサービスの機能要件
- 契約条件
- 価格条件（仮想サーバの単価の他、ディスク利用料、ネットワーク転送量などを調査する。複数の課金体系が混在しているので、価格シュミレーションを行う）
- 自社保有パッケージ・ミドルウェアライセンスの利用可否の確認
- 提供 API(Application Programming Interface)（他社のクラウドとの互換性を確認し、 ロックインされるリスクをチェックする）
- サポート体制

＜参考情報＞

クラウドサービス総覧 2011 年版　IaaS/PaaS 編（日経 BP 社　ITpro Active）

http://itpro.nikkeibp.co.jp/active/2011iaas/index.html

- **トライアル利用**

トライアル利用の可否、およびその内容と期間を調査する。トライアル利用が可能な場合は、トライアルにより以下を確認する。

  - IaaS の場合はスペック上期待される性能が出るか
  - ネットワーク遅延の影響
  - 移行方法と課題の洗い出し
  - サポートの対応レベル
  - 提供されているクラウドサービスのカスタマイズの可否、API の利用方法

- **データ移行方法**

クラウドに既存データを移行する方法を確認する。

  - 移行ツールの有無
  - 大容量外部記憶装置を使ったデータ移行の可否の確認

- **BCP/DR 対応**

対象業務の BCP/DR 対応方針を整理する。

クラウドサービスが利用できなくなった時の対応方針の確認、および、データのバックアップ有無や代替サイトの利用可否などクラウド事業者のサービス内容を確認する。

- **SLA 確認**

SLA の有無と SLA で保証している内容を確認する。

  - 稼働率
  - サポート内容（移行時、運用時）
  - レポートの提供
  - 問題発生時の責任範囲

(3) 新業務・新システムイメージの具体化

- **自社要件への対応**

SaaS 移行の場合、既存業務とのギャップを確認して、SaaS に合わせて業務を変更するか、あるいは SaaS をカスタマイズないし、自社周辺システムに機能追加して現行業務を成り立たせるかを見極める。

既存業務の分析結果を踏まえて、システム設計・業務設計（システム運用を含む）に必要となる以下に示すような要件を整理し、決めておく。

  - 信頼性
  - 性能（応答時間など）
  - セキュリティ
  - ID 利用権限
  - データ移行

- **周辺システム・既存ネットとの接続方法**

自社システムとクラウドをつなぐ方法を見極める。

- データの連携方法
  - リアルタイム連携の必要性と連携方法
  - バッチ連携でのインポート・エクスポート可能なデータ形式
  - クラウドサービス側の制限による、データの真否チェックや名寄せの手法と、データ形式の差の吸収手段
  - 端末周辺機器とのデータ入出力方法
- ネットワーク接続手段
  - プライベート接続の可否
  - インターネット VPN(Virtual Private Network)でのセキュリティ確保

- **帳票作成・プリント**

既存システムでの帳票作成・プリント機能がクラウド環境下でどう実現できるかを検討する。

- SaaS、IaaS、PaaS 共通の検討項目
  - Windows 以外の操作端末からの印刷手段を検討
  - ロケーションフリーな運用に対して帳票出力の必要性の検討
- SaaS の検討項目
  - 印刷手順、作業量の変化（手順増加やファイル一次保存によってセキュリティリスクが高まる）
  - デザインの自由度、変更手段の有無

- **運用の変更点**

クラウド移行に伴い運用面で大きく変わる事項や設計フェーズで検討すべき項目を洗いあげる。

- 業務運用面で検討すべき項目
  - クラウドのユーザ（ID）管理ルール、ID 利用権限
  - 端末周辺機器の選択方法
- システム運用面で検討すべき項目
  - 自社要員とクラウド事業者との役割分担
  - 移行後システムの運用体制
  - 端末周辺機器のドライバ管理手法
  - システム監視方法
  - バックアップ・リカバリ方法

(4) 導入効果の算定

- **費用対効果**

クラウドを利用する場合と、自社保有する場合の費用差を計算する。具体的には、それぞれ以下の観点で、利用予定期間の総費用を計算した上で、コスト面で比較する。

- クラウド利用時の費用
  - 初期費用
  - 利用費用 （月額・年額）

- 移行費用 （プログラム移行、データ移行）
- ネットワーク費用（インターネット回線の増速が必要な場合/専用線を引かなければいけない場合）

- 自社保有の場合の費用
  - 機器購入・環境構築・更改・保守・滅却費用
  - プログラムライセンス購入・保守費用 （OS、ミドルウェア）
  - データセンタ（DC：Data Center)利用費用
  - 自社内設置の場合、場所代、電気代、空調代など
  - 機器監視費用 （監視要員費用、監視サービス利用費用など）
  - 各種契約更新手続きのための作業工数
  - 業務アプリケーション保守費用 （不具合対策費、機能追加費、マニュアル更新費など）

- **導入のメリット**

クラウド採用のメリットを整理し、コスト換算できるものは実施する。

- 機器調達期間の短縮
- 開発期間の短縮 （PaaS・SaaS 利用時）
- 機器障害による業務・サービス停止時間リスクの削減
- 機器管理、ライセンス管理などが不要
- SaaS 利用時のセキュリティ面での対策費用、要員が不要
  => 運用コストの削減 （IPS(Intrusion Prevention System)/ IDS(Intrusion Detection System)運用、パッチ当て、動作確認など）
- 需要変動に合わせて、最適なリソースの確保が容易
- 機器を自社ビルに設置する場合に比較して、耐災害性が高い
  => 事業継続性の向上
- サービス提供にあたって、高速インターネット回線の準備が不要
- シェアドサービスを利用することによる環境負荷の低減
- パブリッククラウド利用に伴う、業務活動のユビキタス性の向上

(5) リスクの洗い出し

- **信頼性・性能**

クラウド環境でのシステム停止時間や応答時間について、想定される値を見積っておく。また、移行後に性能不足や稼働率低下が発生した際の対応方法と所要時間・費用を見積っておく。

- リソース（サーバやストレージ）のアップグレード
- ベストエフォートであるインターネットから専用線への移行

- **セキュリティ （データの保全）**

データの保管方法を設定し、データの漏えい・改竄対策などクラウド事業者のセキュリティ対策レベルを確認し、以下に示す自社が対策するべき事項を洗いあげておく。

- データのバックアップサイクルと保管場所（同一 DC 内、他 DC 利用）
- アカウント管理方法、アクセス認証、アクセスログ取得

- ウィルス対策、サイバー攻撃対策

- **コンプライアンス　（監査対応）**

J-SOX や個人情報保護に関するシステム監査に対応したクラウド側の整備状況を確認する。

- 監査証跡の取得範囲、クラウド事業者の監査対応内容
- 対策レベルの第三者認定（SSAE16(Statement on Standards for Attestation Engagements No.16)、86 号監査、プライバシーマーク）

- **サービス継続性**

クラウド事業者のサービス停止（倒産等）が発生した事態への対応方法を検討しておく。

- サービス終了にあたっての事前通知期間を確認し、その期間で別サービス・オンプレミスへ移行する手段を検討する
- データやソフト資産の引き渡しと事業者内情報の廃棄の取り決め
- SaaS 事業者のエスクロー（データやアプリケーションの第三者預託）の有無

- **移行中止の判断**

設計・開発段階で、移行中止を判断するポイントを検討しておく。

- 設計時に、セキュリティポリシなどにしたがった設計ができない場合
- 開発コストが想定コストを上回り、クラウド利用のメリットがなくなる場合

(6) その他

- **推進体制**

設計フェーズを円滑に推進するためには以下の体制作りが必要である。

- 業務担当（社内メンバー）のアサイン
- 移行支援ベンダ（移行 SIer(System Integrator)や業務プログラム開発会社など）の協力体制
- クラウド事業者候補の担当窓口の確保（サービス内容や先行事例の情報提供、相談）

- **スケジュール**

以下について、業務移行に見合った概略スケジュールを作成する。

- 設計・開発・テスト・データ移行・運用
- 利用者教育

- **サービス利用の停止**

サービス利用を停止・解約する場合に、データやプログラムの処理について、以下を確認しておく。

- データやプログラムの持ち出しが可能なこと。
- データやプログラムの持ち出し後に消去されたことが確認・保証できること。

- **社内コンセンサス**

クラウド採用のメリットについて、直接コスト以外の費用削減や質的効果を、経営層に随時情報提供しておくことが望ましい。

2.2.2. 設計フェーズ

設計フェーズでは、下表に示す実施項目にしたがってマイグレーションを進めていく。以降では、実施項目ごとに、マイグレーションにおいて特に注意して検討・確認すべき事項を説明する。

#	実施項目	検討・確認事項
(1)	導入プロセスの決定	導入プロセスの決定
(2)	機能仕様策定	業務仕様の策定
		カスタマイズの範囲の決定
		システム仕様の具体化
(3)	性能の検討	キャパシティプランニング、性能計画
		マルチテナントによる制限等の取り込み
		ネットワーク仕様
		ユーザ/システム間インタフェース仕様の策定
		導入するサービスレベルの策定
		必要となる性能の見積り
(4)	ネットワークの検討	ネットワーク仕様の策定
		ネットワーク上のセキュリティ設計
(5)	プロトタイプでの調査	事前調査
(6)	運用方式の検討	ハードウェア仕様との対応
		データの保管場所ポリシの策定
		運用管理ポリシの策定
		運用に関する情報の提供内容と手段
		運用の役割分担
		バックアップ/リカバリ
		他システムとの連携
		BCP 対策との整合性
		定期保守
		検証環境から本番機への適用方法
		セキュリティ監査，ISO(International Organization for Standardization)・ISMS (Information Security Management System)認証時の対応および手続きの確認
		運用スケジュール
(7)	セキュリティ仕様の策定	セキュリティレベルの検証
		現行システムとの対応
		ID 利用権限、アクセス管理（ロール制御）等の設計
		社内認証システムとの連携方式の検討
		シングルサインオンの検討
(8)	データ移行方式の検討	データ移行の対象と実現方式
		移行ツール（アプリケーション切り替え設計）
		データ変換プログラム開発

		移行手順・方式計画（一括、部門別など）
		移行スケジュール
(9)	調達仕様の提示	RFP の作成と提示
(10)	サービス仕様・SLA の評価	サービス仕様の評価
		サービス品質の評価
		サービスレベルの検討
		セキュリティ監査報告事項、監査手順の確認
(11)	事業者の安全・信頼性評価	評価基準に基づいた安全性・信頼性評価
		認証基準等の確認
(12)	契約の締結	責任範囲の明確化

(1) 導入プロセスの決定

- **導入プロセスの決定**

ユーザ企業の情報システムについて、企画フェーズの検討事項を基に、どのシステムを、どのような導入プロセスで、いつまでにクラウド化するのかを決定する。特に、クラウド化によって柔軟な仕様変更の実現が求められている場合には、導入プロセスにはアジャイルな手法の採用も検討する。

(2) 機能仕様策定

- **業務仕様の策定**

企業戦略などの企業ニーズから、クラウド化を行う特定業務に関する業務仕様をまとめる。

- **カスタマイズ範囲の決定**

以下の手順で、クラウドサービスをカスタマイズの上で利用する範囲を決定する。

- 自社業務と導入候補のクラウドサービス間のフィット&ギャップ分析の実施
- カスタマイズのコストも考慮して、クラウドサービス利用時のコストを検討
- フィット&ギャップ分析の結果とコストから、カスタマイズ範囲を決定

なお、クラウドサービスでは提供されないが業務として必要な機能、あるいは、修正量が多すぎるなどコスト観点からカスタマイズでの対応が困難な場合には、個別に対応方法を検討する。

- **システム仕様の具体化**

クラウド事業者の提供サービスをカスタマイズせずに使用する機能、および、カスタマイズの上で使用する機能に関して、システム仕様をまとめる。

(3) 性能の検討

- **キャパシティプランニング、性能計画**

以下の項目に注意して、キャパシティプランニングを実施する。

- ユーザ数
- 保存データ量
- 処理量など

また、ユーザ数やデータ容量の増加に柔軟に対応できるような負荷分散・スケールアウト方法についても

検討しておく。

- **マルチテナントによる制限の確認**

以下に示すような、マルチテナントによる制限がないか確認しておく。

- クラウド間の仕様制限
- マルチテナント時の接続性 （ex. 同時接続数の制限）
- 他ユーザからの影響 （ex. 多数のユーザが同時利用した場合の応答性低下）

- **ネットワーク仕様**

データ転送のボリューム、タイミング、フォーマット等により利用するネットワークの仕様を検討する

- **ユーザ/システム間インタフェース仕様の策定**

以下に関して、インタフェース仕様を策定する。

- 利用するクラウドサービスと利用者間のインタフェース仕様
- 利用するクラウドサービスと他システム（既存の Web サービスなど）との間のインタフェース仕様

- **導入するサービスレベルの策定**

必要な機能にしたがって、導入するサービスを決定する。IaaS/PaaS/SaaS など、どのサービスレベルが必要かを確定する。

- **必要となる性能の見積り**

性能計画で検討したクラウドサービスについて、クラウド事業者から提供されている SLA, サービスメニュー、サービス契約などを基に、必要なサービスを見積る。

(4) ネットワークの検討

- **ネットワーク仕様の策定**

距離、セキュリティレベル、インタフェース/回線種別といった条件を整理し、技術条件とサービス内容を検討する。

- 専用線、VPN、インターネット利用等の通信方式
- 必要な性能、転送量、帯域、品質
- 複数拠点の接続とマルチキャストなどのサービス
- 通信事業者のサービス

- **ネットワーク上のセキュリティ設計**

通信の内容、相手、コストから、セキュリティレベルを設定し、設定したセキュリティレベルにしたがった上で、以下に注意して設計を行う。

- ネットワークレベルでの暗号化の必要性
- 暗号化プロトコルの選定
- 電子署名、電子証明書等の必要性
- アクセスログ記録および管理方法

セキュリティレベルによっては暗号化が必要となるが、暗号化を行う場合には、その運用方式についても検討する。特に、鍵の管理や暗号の危殆化（暗号アルゴリズムの安全性が低下した状況、または、それによりシステムの安全性が脅かされる状況）については注意が必要である。仕様、セキュリティ要件から、通信事業者のサービスを選定する。また、運用方法と運用コストに関しても検討しておく。

(5) プロトタイプでの調査

- **事前調査**

クラウドサービスは事業者ごとに提供するサービスの内容に特徴があるため、性能を含めて見込みで策定した仕様に基づいたサービス導入はリスクが高い。そのため、できるだけ事前にサービスのテスト導入やプロトタイプによる検証により、ターゲットシステムに対応可能なことを確認しておく。

(6) 運用方式の検討

- **ハードウェア仕様との対応**

以下のハードウェア仕様を確認した上で、障害発生時にも SLA が満たされるかを確認する。

- 物理サーバ仕様
- 仮想サーバ仕様
- ストレージ仕様
- ネットワーク機器仕様
- 通信回線仕様

- **データ保管場所ポリシの策定**

バックアップデータの保管場所・保管方法として、以下のいずれの方法を取るのかを、BCP 対策にも照らし合わせながら検討する。

- クラウドサービスの仕様に準ずる
- ユーザ企業が保管場所を指定
- 遠隔地

- **運用管理ポリシの策定**

コストも考慮した上で、以下の検討を行う。

- ユーザ企業自身の運用管理に関する基本的な考え方
- 運用に関する権限
- 運用品質
- 運用ルール
- 障害対応方針等

- **運用に関する情報の提供内容と手段**

クラウド事業者から提供される監視、障害等の運用に関する情報について、その内容と報告提供のタイミングおよび手段について検討する。

- 死活監視報告
- リソース監視報告

- 異常アクセス監視報告
- セキュリティレポート
- 障害レポート
- 性能レポート
- 稼働レポート　等

- **運用の役割分担**

クラウド事業者と自社の運用範囲を明確にし、役割分担、体制、連絡手段を検討する。

- **バックアップ/リカバリ**

バックアップのタイミング、世代、他の DC へのバックアップの必要性やスナップショット保管の必要性等について、リカバリ時のシステム停止可能時間等も含めて検討する。

- バックアップ時に仮想マシンの停止が必要か
- バックアップ時にアプリケーションの停止が必要か
- バックアップサイクルと保管世代数
- 遠隔地バックアップの必要性と手段・手法
- スナップショットの必要性と手段・手法
- ディザスタリカバリ（DR）環境と構成
- 目標復旧時点(RPO: Recovery Point Objective)、目標復旧時間(RTO: Recovery Time Objective)等

- **他システムとの連携**

クラウドシステム障害発生時の関連する他システムへの対応について、以下の項目を検討する。

- システム間の役割分担および境界
- お互いの連絡体制
- 障害時の対応方法
- 障害復旧時のリカバリ手順

- **BCP 対策との整合性**

事業継続計画（BCP）にて検討されているものとの整合性を以下の観点で検証する。

- 採用する運用設計仕様で災害発生後の業務運用が可能か
- 想定される復旧時間については妥当か
- データの保全性・信頼性は確保されているか
- 計画されているコストとの乖離はないか

- **定期保守**

クラウドサービスに含まれる以下の定期保守項目と内容について確認する。

- パッチ適用
- （自前）ソフトのアップデート
- ハード／ソフト保守項目
- バックアップテープ等の消耗品交換の保守項目およびその費用負担

- 定期保守によるクラウドサービスの停止状況

- **検証環境から本番機への適用方法**

ユーザアプリケーションを更新する場合について、検証環境で更新したアプリケーションの本番機への適用方法を、以下に注意した上で検討しておく。

- 作業分担
- 手続き
- バックアップ要件　等

- **セキュリティ監査、ISO・ISMS 認証時の対応および手続きの確認**

運用設計、クラウド事業者との契約内容が運用要件を満たしていることを確認する。また、クラウド事業者が提供する性能レポート、セキュリティレポート、およびユーザ企業の各種レポート等により以下の認証監査対応に問題がないことを確認する。

- セキュリティ監査
- ISO 認証監査
- ISMS 認証監査
- プライバシーマーク認証監査　等。

- **運用スケジュール**

以下について、クラウドサービス移行後の恒常的な運用スケジュールを策定する。

- 定期監視
- 定期保守（アップデート、パッチ適用、ハード保守等）
- 定例報告
- ハード／ソフトバージョンアップのロードマップ　等

(7) セキュリティ仕様の策定

- **セキュリティレベルの検証**

ビジネスプロセス等の要件から決定したセキュリティ要件（セキュリティポリシ）を満たしているかを確認する。できる限りサブシステムあるいはサービスプロセスの単位で必要なセキュリティ要件を検証する。

- **現行システムとの対応**

現行のレガシーシステムから変更されるシステムあるいはサブシステムについて、以下を検証する。

- インタフェースでやりとりされるデータ
- インタフェースの通信プロトコル等の通信方式
- （可能なら）システム内でのデータの取り扱い方法

- **ID 利用権限、アクセス管理（ロール制御）等の設計**

企画フェーズで検討した ID 利用権限の定義にしたがって具体的に設計することを原則とする。もしも相違がある場合は相違点について明記して検証できるようにする。

- **社内認証システムとの連携方式の検討**

社内認証システムのインタフェースと利用するクラウドサービスの認証インタフェースを比較し、データの取り扱い、セキュリティレベルについて比較する。また、認証のプロトコルや手順についてシーケンスを確認する。特に、利用するクラウドサービス側で認証に用いるユーザ ID や利用権限についてのデータベースやキャッシュが存在する場合、社内認証システムでの ID 利用権限の変更や削除を行った場合に、どの程度の遅延でクラウドサービス側の ID 利用権限の情報を更新できるかを確認する。

- **シングルサインオンの検討**

ディレクトリサービスなど、既存のレガシーシステムで利用しているサインオン機能を分析し、サービスの ID 利用権限等の認証サービスと連携したシングルサインオンが実現できるか検討する。たとえば、独立した ID 権限認証サービス利用やシングルサインオンサーバの導入等の候補が考えられる。シングルサインオンを実装する場合、必要な ID フェデレーションを準備する。

(8) データ移行方式の検討

- **データ移行の対象範囲と実現方式**

移行対象システムのデータベースについて、以下を明確にした上で、移行対象とするデータを決定する。

- 現在保存されているデータのフォーマットおよびデータ自体
- 現在保存されているデータの期間
- データベースのアクセスインタフェース

さらに、移行データの容量、移行手順の検討を行うと共に、移行作業を管理する人材のアサインも行う。

- **移行ツール（アプリケーション切り替え設計）**

移行ツールの候補を選出した後、以下に注意した上で、実際に利用する移行ツールの決定と移行計画の検討を行う。

- 動作環境
- 動作性能
- 制限事項の有無

- **データ変換プログラム開発**

レガシーシステムのデータが独自形式の場合、利用するクラウドサービスのデータ形式との整合性を検証し、必要に応じて以下の開発を行う。

- データ形式変換ツール
- データベース形式変化ツール

- **移行手順・方式計画（一括、部門別など）**

移行対象システムの利用形態を分析し、特に以下の項目に注意した上でシステム停止に対するインパクトの最も少ない移行計画を検討する。

- 休業日でのシステムの一括切り替え
- 一定期間の新旧システム共存の要否
- 新旧システム共存の場合のデータ保存方法

- 移行期間中のデータ交換やメールなどでの中継　等

- **移行スケジュール**

企画フェーズの決定にしたがって、移行計画の具体的な設計を行う。上記の移行方式の検討結果を基に、詳細なスケジュールを立案する。

(9) 調達仕様の提示

- **RFP の作成と提示**

機能仕様策定プロセスで定義した要求機能を RFP として提示する。RFP には以下が含まれるようにする。

- コンプライアンスレベル
- 情報機密レベル
- 非機能要件（データ移行要件）
- 非機能要件（性能要件，運用要件）

(10) サービス仕様・SLA の評価

- **サービス仕様の評価**

採用対象としているクラウド事業者のクラウドサービスが、移行対象システムのサービス仕様を満たしているか評価する。特に、以下を注意して評価する。

- 稼働率
- 移行時や運用時のサポート有無

- **サービス品質の評価**

サービス品質に加えて、サービス品質に関する情報開示が十分に行われているかといった点に注意して、クラウドサービスを選択する。

- **サービスレベルの検討**

以下に注意して、サービスレベルの検討を行う。

- SLA の対象範囲

  「公共 IT におけるアウトソーシングに関するガイドライン」（総務省）を参考に、SLA の範囲を決定する。導入当初は、範囲が広くなりすぎないように注意する。

- 責任範囲明確化

  利用者とクラウド事業者間の責任範囲の明確化を行う。責任範囲明確化については、「ASP･SaaS の安全・信頼性に係る情報開示指針」（総務省）が参考になる。

- SLA 実現方法の明確化

  クラウドサービスの内容と品質を確認した上で、SLA を実現するための手順を明確化する。クラウドサービスだけでは SLA が満たせない場合など、必要に応じてカスタマイズの検討を行う。

  SLA 実現方法については、「ASP･SaaS の安全・信頼性に係る情報開示認定制度」（財団法人マルチメディア振興センター）が参考になる。

- サービスレベル参考値の導出
  クラウドで扱うデータに対して、機密レベル等でパターン化を行う。パターン化には、「総合行政ネットワーク ASP ガイドライン（3.5 版）」（総合行政ネットワーク運営協議会）が参考になる。
  作成したパターンに対して、サービスレベルの参考値の導出を行う。参考値導出には、「SaaS 向け SLA ガイドライン」（経済産業省）が参考になる。

- **セキュリティ監査報告事項、監査手順の確認**

設計フェーズで策定したセキュリティ仕様を用いて、セキュリティ監査報告事項の確認を行う。また、監査報告の手順を確認し、必要に応じて手順の見直しを行う。
セキュリティ監査報告については、「ASP･SaaS における情報セキュリティ対策ガイドライン」（総務省）が参考になる。

(11)事業者の安全・信頼性評価

- **評価基準に基づいた安全性・信頼性評価**

企画フェーズで実施したリスク評価基準に基づき、採用対象のクラウド事業者の安全性・信頼性を評価する。特に、サービスが停止した場合の対応方法として、以下の点を確認しおくとよい。

- 具体的なリスク回避手段
- 代替クラウドサービスへの移行手段

- **認証基準等の確認**

移行対象のシステムが必要とする認証基準等を調査し、クラウド事業者がそれらを取得しているか確認する。

(12)契約の締結

- **責任範囲の明確化**

整理した SLA を基に、クラウド事業者との契約締結を行う際には、以下の点に注意した上で、利用者とクラウド事業者と間の責任範囲を明確にする。

- 具体的な構築体制・運用体制
- クラウド事業者側との連絡手段

2.2.3. 構築・テスト・移行・教育フェーズ

構築・テスト・移行・教育フェーズでは、下表に示す実施項目にしたがってマイグレーションを進めていく。以降では、実施項目ごとに、マイグレーションにおいて特に注意して検討・確認すべき事項を説明する。

#	プロセス	実施項目	検討・確認事項
(1)	構築	システム連携	認証
			連携のためのインタフェース開発
(2)		アプリケーション開発	業務アプリケーション
(3)	テスト	機能確認と運用手順の検証	テストデータ生成
			機能要件の確認
			運用要件の確認
			アプリケーションのテスト
(4)	移行	データ移行	事前検証
			移行検証
(5)	教育	業務マニュアルに沿った教育・研修	利用者教育の実施

(1) システム連携

- **認証**

既存システムや他のシステムと連携する場合は、連携のための仕組みやセキュリティ対策などを上流の設計に基づき対応する。

- 社内システムとの連携では、シングルサインオンの実現のため既存ディレクトリと連携したフェデレーション環境を構築する。
- クラウドサービス間連携では、各サービスの認証方法を確認し、必要であればサービス間での ID 連携の仕組みを作る。
- データの同期方法、利用要件の確認やドメインの変更を伴う場合の中継やプロキシの設置など連携のためのインタフェースを確認すること。
- データの機密性確保のためデータの所在や受け渡しによるリスクにも注意すること。
- ネットワーク環境については企業のポリシにあった接続方法について準備する。必要な場合は、社内のネットワークポリシの設定を変更する。

サービスレベルは低いほうに足を引っ張られることを十分に注意する。

＜参考情報＞

ASP/SaaS における情報セキュリティガイドライン（ASP/SaaS の情報セキュリティ対策に関する研究会）

なお、既存システムや他のシステムとの連携を行わない場合も上流の設計に基づき利用者の ID 登録を行うこととなるが、管理者等の運用時の ID 管理をもれなく配慮する。

- **連携のためのインタフェース開発**

以下に注意した上で、連携のためのインタフェース開発を行う。

- 相互運用性を維持するためにも標準ベースの技術を意識する。
- SaaS アプリケーション側の障害時シナリオを考慮する。
- SaaS アプリケーション側の仕様変更時に検知する仕組みを考慮する。

- たとえば、デフォルトの文字コードが変更になるなど、設計時にはわからなかった事象であっても、変更を検知の上でエラーとするようにする。

＜参考情報＞

以下に示す代表的な仕組み／技術標準が参考になる。

SAML(Security Assertion Markup Language)

WS-Federation

OpenID

OASIS(Organization for the Advancement of Structured Information Standards)

http://www.oasis-open.org/jp/specs/index.php

(2) アプリケーション開発

- **業務アプリケーション**

必要に応じアプリケーションの開発を行うが、特定環境へのロックインを回避するためプラットフォームから独立させ、環境間の移植に手間がかからないように注意する。できるだけコーディングが最小限あるいは不要である環境を推奨する。階層を明確に分離し、変更が必要になった場合にその影響が最小限になるようにする。

上流の設計に基づき業務アプリケーションの開発を行う際、クラウド特有の制限事項やアプリケーション配置方法等を理解すること。たとえば、トラフィック課金やサービス課金など課金方式を理解し、安価に抑えるよう注意をする。課金方法や帯域、データの重要度によってデータの配置にも注意する。

- **その他のアプリケーション開発**

必要に応じて、以下に示すような運用上必要となるアプリケーションの開発を行う。

- クラウド上のデータ確認や一括データ更新のためのアプリケーション
- 障害等を迅速に検知するためのアプリケーション
- 利用者から不具合の報告があった際の、その状況を確認するためのアプリケーションなど

(3) 機能確認と運用手順の検証

- **テストデータ生成**

テスト用データを準備する。運用テストおよび本番データ移行がスムーズかつ確実に行えるように、可能な限り本番に近い準備をする。

- **機能要件の確認**

テスト仕様書に基づき機能テストを実施し、SLA を満足しているか確認する。特にバックアップ／リカバリの確認や高負荷テスト、冗長性／可用性テスト、障害許容性の確認を行う。また、システム拡張や縮小時の方式を確認するためキャパシティ状況の把握からスケールアウトの実施までのプロセスにしたがってテストする。

- **運用要件の確認**

業務運用設計にしたがい、人の動きも含めて運用が可能であることを事前に確認しておく。

- IaaS についてはサードベンダ製ソフトのクラウド向けサポートの実態（サポートセンタへの障害

インプット実施状況、実運用上機能すること等）を確認する。

- 運用開始直前状態のベンダ提供サービスの性能と内訳（DC 所在地、応答時間の確認等）を把握しておく。
- パブリッククラウドの場合のアクセス端末制御、セキュリティ確保が機能するか実機で確認をしておく。
- サービスの継続のため必要な監視項目を確認しておく。
- 本番、ステージング、テスト等の環境において、クラウドサービス利用時にも変更・リリース等の運用ができることを確認する。
- クラウドサービス側で提供する仕組み・サービスの有無に関わらず、ユーザの業務運用視点で運用ができることを確認する。
- セキュリティ事故があった場合を想定し、その対応を含めてリハーサルを行うこと。また、IT サービスの契約範囲での運用の確認とユーザ企業の運用管理との境界・連携を確認する。

- **アプリケーションのテスト**

SaaS と連携する機能については、仕様書等の机上確認だけではなく、実機での網羅的なテストを実施しておく。また、SaaS 側の障害発生時の対応手順については事前に確認をしておく。

- 機能テスト

  IaaS/PaaS を構成するハイパーバイザやソフトウェアバージョン、提供モジュールによって動作しない場合が考えられるので、網羅的な機能テストを実施しておく。

- 性能テスト

  リソースは共用利用なので、スペック等の机上確認だけでなく、実際のアプリケーションを稼働させて性能検証（応答性能や処理時間等）を行うとよい。また、過度な利用による追加料金の発生の可能性などを事前に確認しておく。

(4) データ移行

- **事前検証**

移行方式の検討結果に基づき検証を行う。データ移行を行う際はインターネットの帯域幅を検証し、移行時間を算出する。また、変更度合いや回線負荷を考慮し、他のツール利用、メディアでのファイル移行等を検討する。部分的な移行を計画している場合は、移行計画通り行えるか検証を行う。場合によっては移行の中断、移行スケジュールの変更を検討する。

＜参考情報＞

総務省自治体クラウド開発実証事業成果

http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/index.html

- **移行検証**

移行後のデータの検証を行う。

(5) 業務マニュアルに沿った教育・研修

- **利用者教育の実施**

以下の教育・トレーニングを実施する。

- ヘルプデスクに対するトレーニングを実施する。

- クライアント環境への設定、管理者教育等を展開する。
- エンドユーザに対するトレーニングを実施する。

2.2.4. 運用フェーズ

運用フェーズでは、下表に示す実施項目にしたがってマイグレーションを進めていく。以降では、実施項目ごとに、マイグレーションにおいて特に注意して検討すべき事項を説明する。

#	実施項目	検討・確認事項
(1)	運用体制	組織・体制
(2)	運用管理	インシデント・問題管理
		変更・リリース管理
		契約・財務・構成管理
		システム監査、セキュリティ監査、内部統制
(3)	導入効果の評価	費用対効果の評価
		導入のメリット
(4)	情報収集と検討	組織の IT 戦略に合致したサービスの検討

(1) 運用体制

- **組織・体制**

クラウドサービス提供ベンダにロックインされず、IT サービスの最適化を継続できる管理体制とし、不要な IT インフラ管理体制を縮小しコスト削減に努める。

(2) 運用管理

- **インシデント・問題管理**
  - インシデント・問題の切り分け

    システムや利用者からのインシデントに対して、クラウドサービス側の問題か、それ以外かの切り分けを行い、クラウドサービス側の問題の場合の対応体制・プロセス等を予め定めておく。
  - セキュリティリスク

    クラウドサービスはオープンで共用の環境のため、セキュリティリスク（情報漏えい、ウィルス感染等）に対しては、迅速な対応が必要となるため、管理体制・プロセス等を予め定めておく。

- **変更・リリース管理**
  - アプリケーション変更

    システムの変更管理は、オンプレミス側のアプリケーションからそのアプリケーションと連携するクラウドサービスまで含めたトータルでの管理が必要となる。オンプレミス側のアプリケーションを変更すると、連携しているクラウドサービスが正常に動作しなくなる可能性があるため、事前の検証が必要。
  - サービス提供者側での変更

    サービス提供側で変更が発生する場合、クラウドサービスと連携しているアプリケーションの稼働検証が必要となる。また、以下の項目についても確認しておく。
    - サービス提供者側からの変更内容の説明

- 無停止でのサービスやデータの引き継ぎが可能であるか否か
- データの所在変更があるのか
- 変更が契約範囲内であるか

- **契約・財務・構成管理**

クラウドを含めたトータルでの管理が必要であり、特に、クラウド側に対して、SLA,SLM が守られているか、性能に問題がないかの観点での評価を行う。また、従量課金のクラウドサービスを使う場合には、利用状況によって料金が変動するため、以下の点に注意する。

- 月々の利用量と支払い額の確認
- 他サービス提供者との比較評価（自システムに適用可能な、より安価なサービスがないか確認する）

- **システム監査、セキュリティ監査、内部統制**

クラウドを含めたトータルでの管理が必要であり、クラウド部分についてもブラックボックス化しないように、監査等の対応を行う。特に、パスワードの管理や変更が適切に行われているか監査すること。

＜参考情報＞

内部統制（SSAE16）、システム監査、セキュリティ監査

(3) 導入効果の評価

- **費用対効果の評価**

クラウドを利用する場合と、自社保有する場合の費用差を算定する。企画時に算定した効果と比較し定量的評価を行う。

- **導入のメリット**

企画時に期待したメリットが正しく実現されているか、定性的評価を行う。

(4) 情報収集と検討

- **組織の IT 戦略に合致したサービスの検討**

クラウドサービスの市場動向をよく確認して、自組織の IT 戦略に合致したサービスを検討するために、次の観点で情報収集を行う。

- 技術やベンダサービスの変化に対応したオンプレミス、パブリッククラウド、プライベートクラウドの住み分け検討
- Request for Change(RFC：変更要求)の発行

2.2.5. 契約の変更・終了

契約の変更・終了時には、下表に示す実施項目、検討事項を検討しておく必要がある。

#	実施項目	検討・確認事項
(1)	サービス利用の終了、サービス提供者の変更	サービス移行
		データ、ログの削除

(1) サービス利用の終了、サービス提供者の変更

- **サービス移行**

XML、CSV など移行データのフォーマットや移行データを格納する媒体などを確認し、データ移行の方法、期間、費用を検討する。移行作業は、クラウド事業者との作業分担と責任分界点を明確にした上で行う。

円滑なサービスの移行のためには、クラウドサービス事業者（SaaS 事業者）が講ずる措置について確認しておくとよい。確認項目としては、たとえば、以下があげられる。

- サービスを引き継ぐ事業者との打合わせの実施
- 移行するデータの内容の説明
- 利用を終了するサービス（SaaS）における案内画面表示や次のサービスへの自動リンクの設定など

- **データ、ログの削除**

クラウド事業者（SaaS 事業者）のサーバなどで処理・蓄積され、サービス停止後も残存しうるデータの処理方法（物理的破壊、など）を確認する。利用者データの返却とクラウド事業者のストレージからの完全な消去が不可欠であり、消去のエビデンスを受領する。

2.3. セキュリティ、性能などの観点に関する検討項目

2.2 節ではクラウドへのマイグレーションにおいて検討・確認すべき事項を、マイグレーションのプロセスにしたがって列挙した。ただし、このようなまとめ方では、複数の観点での検討・確認事項が混在して書かれてしまうため、本節ではセキュリティ、性能などクラウドの課題として一般的に認識されている観点ごとに、個別に検討・確認事項をまとめた。具体的には、セキュリティ、性能、可用性/サービス継続性、ビジネス上のメリットという 4 つの観点ごとに、実施項目と検討・確認事項を表形式でまとめた。なお、本節での検討・確認事項はサマリとなっており、詳細は（表のリンク部に記載した）2.2 節の該当部分を参照のこと。

(1) セキュリティ

#	ﾌﾟﾛｾｽ	実施項目	検討・確認事項	リンク
1	企画	対象業務・対象システムの分析	・データの機密レベルを分析し、外出しができるか判断する。	2.2.1 節(1)
2		新業務・新システムイメージの具体化	・既存業務の分析を踏まえて、システム設計・業務設計に必要なセキュリティ要件を整理し決めておく。	2.2.1 節(3)
3		導入効果の算定	・特に SaaS 利用時には、SaaS 利用に伴って必要となる費用も考慮して効果を算定する。	2.2.1 節(4)
4		リスクの洗い出し	・データの保管方法を設定し、データの漏えい・改竄対策などクラウド事業者のセキュリティ対策レベルを確認し、自社が対策するべき事項を洗いあげておく。	2.2.1 節(5)
5	設計	ネットワークの検討	・必要とされるセキュリティレベルを考慮し、インターネット/VPN/専用線の利用を検討する。 ・セキュリティ要件を満たす通信事業者を選定する。 ・暗号化を行う場合には、方式を検討する。	2.2.2 節(4)

6		運用方式の検討	・クラウド事業者から提供されるセキュリティレポートの内容、タイミング等について検討する。 ・クラウド事業者が提供するセキュリティレポート、およびユーザ企業の各種レポート等により、セキュリティ監査，ISO，ISMS の認証、監査対応に問題ないことを確認する	2.2.2 節(6)
7		セキュリティ仕様の策定	・ビジネスプロセス等の要件から決定したセキュリティ要件（セキュリティポリシ）を満たしているかを確認する。 ・社内認証システムのインタフェースと利用するサービスの認証インタフェースを比較し、データの取り扱い、セキュリティレベルについて比較する。	2.2.2 節(7)
8		調達仕様の提示	・企画フェーズでまとめた運用要件，セキュリティ要件について，コンプライアンスの観点から J-SOX 法や個人情報保護法などを勘案し，RFP として提示する。 ・企画フェーズでまとめたセキュリティ要件のうち，情報機密事項につき，RFP として提示する。	2.2.2 節(9)
9		サービス仕様・SLA の評価	・クラウド事業者との間で責任範囲および責任分界の明確化を行う。 ・クラウドを利用する場合のセキュリティ監査報告手順を確認する。 ・機密レベル等のパターンに対応する SLA を対応づける。	2.2.2 節(10)
10		事業者の安全・信頼性評価	・企画フェーズでのリスク評価に基づき、採用対象クラウド事業者の安全性・信頼性が必要な基準を満たしているか評価する。 ・移行対象システムが必要とする認証基準等のリストを作成し、クラウド事業者が取得している基準と照合する。	2.2.2 節(11)
11	構築	システム連携	・既存システムや他のシステムと連携する場合は連携のための仕組みやセキュリティ対策などを上流の設計に基づき対応する。	2.2.3 節(1)
12	テスト	機能確認と運用手順の検証	・特に、パブリッククラウドの場合は、アクセス端末制御、セキュリティ確保が機能するか実機で確認をしておく。 ・セキュリティ事故があった場合を想定し、その対応を含めてリハーサルを行うこと。	2.2.3 節(3)
13	運用	運用管理	・SaaS/クラウドはオープンで共用の環境のため、セキュリティリスク（情報漏えい、ウィルス感染等）に対しては、迅速な対応が必要であり、管理体制・プロセス等を予め定めておく。 ・SaaS/クラウドを含めたトータルでの管理が必要であり、ブラックボックス化しないように、監査等の対応を行う。特にパスワードの管理や変更が適切に行われているか監査すること。	2.2.4 節(2)

(2) 性能

#	ﾌﾟﾛｾｽ	実施項目	検討・確認事項	リンク
1	企画	対象業務・対象システムの分析	・利用メリット明確化のために、移行システムと対象業務の要件を分析する。現行システムの以下の点は、特に確認しておくとよい。 (1) 業務量（業務量,伸び率,ピーク率,ピークの予測可否） (2) 当該業務の入力、出力量、要求応答時間 ・周辺システムとのデータ連携が少ないシステムがクラウド向きである。周辺システムと大量データのやりとりを行うシステムはネットワーク遅延の問題を発生する可能性が高いため、・システム間接続の有無、・授受データの量、タイミング、応答時間等、・ユーザ認証等の連携有無を調査しておく。	2.2.1 節(1)
2		利用サービスの調査	・トライアル利用の可否、およびその内容と期間を調査し、以下の観点で試行する。(1) IaaS の場合はスペック上期待される性能が出るか確認 (2) ネットワーク遅延の影響確認。	2.2.1 節(2)
3		新業務・新システムイメージ具体化	・既存業務の分析を踏まえて、システム設計・業務設計（システム運用を含む）に必要な要件（応答時間など）を整理し決めておく。	2.2.1 節(3)
4		リスクの洗い出し	・クラウド環境でのシステム停止時間や応答時間について、想定される値を見積っておく。また、移行後に性能不足が発生した際、対応方法と所要時間・費用を見積っておく。	2.2.1 節(5)
5	設計	性能の検討	・ユーザ数、保存データ量、処理量などから、キャパリシティプランニングを実施する。 ・性能計画として、ユーザ数の増加やデータの増加に柔軟に対応できるような負荷分散・スケールアウト方法を検討する。 ・データ転送のボリューム、タイミング、フォーマット等により利用するネットワークの仕様を検討する ・性能設計で計画した、サービスが提供されているかを SLA, サービスメニュー、サービス契約などから、必要なサービスを見積る。	2.2.2 節(3)
6		ネットワークの検討	・距離、セキュリティレベルといった条件を整理し、技術条件とサービス内容（必要な性能、転送量、帯域、品質等）を検討する。 ・暗号化を行う場合、符号化/復号化時の性能に注意する。	2.2.2 節(4)
7		プロトタイプでの調査	・クラウドサービスは各社ともサービス内容がまちまちであり、性能を含めて見込みで仕様を策定し、サービス導入という流れではリスクが高い。そのため、サービスのテスト導入とプロトタイプの作成により、ターゲットシステムに対応できることを事前に確認する。	2.2.2 節(5)
8		運用方式の検討	・クラウド事業者から提供される性能レポートについて、その内容と報告提供のタイミングおよび手段について検討する。	2.2.2 節(6)
9		データ移行方式の検討	・移行ツールの候補を選出し、動作環境、動作性能、制限事項を検証し、移行計画に適合するツールを決定する。	2.2.2 節(8)
10		調達仕様の提示	・企画フェーズでまとめた性能要件，運用要件など移行後の運用に	2.2.2 節(9)

			関する非機能要件を RFP として提示する。	
11	テスト	機能確認と運用手順の検証	・業務運用設計にしたがい、人の動きも含めて運用が可能であることを事前に確認しておく。運用開始直前状態のベンダ提供サービスの性能と内訳を把握しておく。 ・テスト仕様書に基づき機能テストを実施し、SLA を満足しているか確認する。特にバックアップ／リカバリの確認や高負荷テスト、冗長性／可用性テスト、障害許容性の確認を行う。 ・SaaS と連携する機能については、仕様書等の机上確認だけではなく、実機での網羅的なテストを実施しておく。リソースは共用利用なので、机上確認だけでなく実際のアプリケーションを稼働させて性能検証（応答性能や処理時間等）を行うとよい。	2.2.3 節(3)
12	運用	運用管理	・SaaS/クラウドを含めたトータルでの管理が必要であり、特に SaaS/クラウド側に対して、SLA や SLM (Service Level Management)が守られているか、性能に問題がないかの観点での評価を行う。	2.2.4 節(2)

(3) 可用性/サービス継続性

#	ﾌﾟﾛｾｽ	実施項目	検討・確認事項	リンク
1	企画	導入効果の算定	・クラウド採用のメリットを整理し、可能なものはコスト換算する。可用性/サービス継続性に関しては、「機器障害による業務・サービス停止時間リスクの削減」、「機器を自社ビルに設置する場合に比較して耐災害性が高いことによる、事業継続性の向上」といったメリットがある。	2.2.1 節(4)
2		リスクの洗い出し	・クラウド事業者のサービス停止（倒産等）が発生した事態への対応方法を検討しておく。	2.2.1 節(5)
3	設計	運用方式の検討	・設計した運用方式を既存の BCP 比較し、整合性を確認する。	2.2.2 節(6)
4	テスト	機能確認と運用手順の検証	・テスト仕様書に基づき機能テストを実施し、SLA を満足しているか確認する。特にバックアップ／リカバリの確認や高負荷テスト、冗長性／可用性テスト、障害許容性の確認を行う。 ・業務運用設計にしたがい、人の動きも含めて運用が可能であることを事前に確認しておく。特に、サービスの継続のため必要な監視項目を確認しておく。	2.2.3 節(3)
5	運用	運用体制	・サービス提供ベンダにロックインされず、IT サービスの最適化を継続できる管理体制とし、不要な IT インフラ管理体制を縮小しコスト削減に努める。	2.2.4 節(1)

(4) ビジネス上のメリット

#	ﾌﾟﾛｾｽ	実施項目	検討・確認事項	リンク
1	企画	対象業務・対象システムの分析	・システム移行を企画する際には、移行システムと対象業務の要件を分析し、クラウドサービスの利用メリットを検討する。	2.2.1 節 (1)
2		導入効果の算定	・クラウドを利用する場合と自社保有する場合の費用差を計算する。 ・クラウド採用のメリットを整理し、可能なものはコスト換算する。	2.2.1 節(4)
3		その他	・クラウド採用のメリットについて、直接コスト以外の費用削減や質的効果を、経営層に随時情報提供しておくことが望ましい。	2.2.1 節(6)
4	設計	機能仕様策定	・自社の業務とクラウドサービス間のフィット＆ギャップ分析を実施し，カスタマイズ範囲や，クラウドサービス利用時のコストを検討する。 ・フィット＆ギャップ分析結果，およびクラウドサービスの導入／利用コストの観点から，カスタマイズ範囲を決定する。クラウド側で提供されない機能については個別に対応方法を検討する。	2.2.2 節(2)
5	運用	導入効果の評価	・クラウドを利用する場合と、自社保有する場合の費用差を算定する。企画時に算定した効果と比較し定量的評価を行う。 ・企画時に期待したメリットが正しく実現されているか、定性的評価を行う。	2.2.4 節(3)

3. プロセス観点以外で検討すべき項目

DR のバックアップ先に海外拠点を使うなど、海外拠点を活用したクラウドサービスへの注目が高まっている。この場合、拠点が立地する国と日本国内では、法律や商習慣が異なる場合があるため、事前に情報収集しておくことが必要である。

ここで、海外拠点を利用する場合であっても、2 章で検討したクラウド移行のプロセスとしては、国内拠点のみを利用する場合と大きな違いはない。したがって、本章では海外拠点を利用する際に、特に検討・確認しておくべき項目のみを 2 章とは別にまとめることにした。

3.1. 検討の枠組みと前提

本章では、海外拠点を利用する場合について、法規制対応など情報収集する観点を抽出し、抽出した観点ごとに、検討・確認すべき項目を記載した。さらに、該当項目に関して対応方法や参考情報がある場合には、それらの情報も記載することにした。

なお、本ガイドでは国内ユーザが海外拠点を活用したクラウドへ移行する際に、検討・確認すべき項目を対象とした。 業種や業界などについての限定を置かない一般的な検討項目を記載しており、HIPPA[3]など個別事業法がある場合には、その個別事業方法を優先した検討を行うことを想定している。

3.2. 海外拠点を利用する場合に検討すべき項目

本節では、法規制/商習慣/性能/セキュリティ/保守/その他 の 6 観点に関して、検討・確認すべき項目、および対応方法がある場合には、その対応方法を記載した。

3.2.1. 法規制

法規制の観点では、以下の 6 項目に関する検討・確認が必要である。

#	観点	検討・確認項目
(1)	法規制	個人情報保護
(2)		機密データ
(3)		輸出管理
(4)		監査対応（システム監査）
(5)		監査対応（業務監査）
(6)		税制

(1) 個人情報保護

域外へのデータ移行が制限される地域のクラウドサービスを利用する場合、サービス終了時などの必要な時に、作成したデータを引き出せない場合がある。そのため、このような事態に備えた検討をしておく必要がある。

対応方法としては、複製データを他拠点で保管しておく、あるいはデータ移行制限地域内で収集した情報は地域内でのみ利用するといったことが考えられる。

[3] Health Insurance Portability and Accountability Act: アメリカの医療機関における患者情報の機密性、統合性、および可用性を維持することを目的に定められた法律

(2) 機密データ

国によっては、政府当局がデータに対して調査権限を有する。そのため、機密データであっても差し押さえのリスクがあり、またサーバごと押収される可能性もあるため、サービスが利用できなくなる可能性がある。したがって、サービスが利用できなくなった際の対応を検討しておく必要がある。

対応方法としては、サービス利用、データアクセスが不能となる状況への対策、BCP/BCM(Business Continuity Management)の検討を行うといった方法が考えられる。

(3) 輸出管理

PaaS、IaaS 上にアプリケーションを構築する場合、外為法の遵守が必要となる。

対応方法としては、外為法において特定の技術（暗号化技術等）を外国で提供、もしくは外国企業・外国人に提供する際には経産相の許可が必要と定められており、対象かどうかの確認を行う。

なお、輸出管理については「クラウドコンピューティングと日本の競争力に関する研究会」報告書も参照のこと。

(4) 監査対応（システム監査）

監査への対応を検討しておく必要がある。

対応方法の検討には、自国から監査情報を閲覧できるのか、あるいはクラウド事業者が監査情報を出してくれるのか確認する必要がある。もし、情報が得られない場合は、ユーザ自身でログを取得するといった対応が必要となる。

(5) 監査対応（業務監査）

業務に SaaS（メール等のサービスを含む）を利用する場合には、システム監査に加えて、業務に対しての監査への対応を検討しておく必要がある。

対応方法の検討にあたっては、アーカイブサービスがあるかの確認が必要である。もし、サービスがない場合には、ユーザがアーカイブを取得する必要がある。

(6) 税制

消費税や売上税等、各国で課税制度が異なり、価格に含まれていない場合もあるため、サービス事業者への支払い方法・支払い金額についての検討が必要である。

対応方法の検討には、各国の課税制度や、サービス事業者との契約内容を事前に確認しておく必要がある。また、必要であれば各国の源泉徴収制度の運用方法も事前に確認しておく必要がある。

税金については、http://aws.amazon.com/jp/agreement/ などのクラウド事業者のホームページの情報も参考のこと。

3.2.2. 商習慣

商習慣の観点では、以下の項目に関する検討・確認が必要である。

#	観点	検討・確認項目
(1)	商習慣	決済

(1) 決済

海外事業者のサービス利用時に、国内の商取引の通例の決済方法が利用できるか、検討が必要である。

対応方法としては、サービス利用規約を参照して、決済方法（ex. 法人向け決済、円建て決済の可否）を事前確認しておくことがあげられる。

3.2.3. 性能

性能の観点では、以下の 5 項目に関する検討・確認が必要である。

#	観点	検討・確認項目
(1)	性能	応答性能
(2)		処理性能
(3)		データ転送性能
(4)		マルチクラウドの SLA 保証
(5)		品質

(1) 応答性能

距離が大きく離れることによる、遅延時間の拡大への影響を検討する必要がある。

対応方法としては、性能に関して SLA を締結する（SLA を満たせる事業者と契約する）ことがあげられる。

(2) 処理性能

サービス利用時に、コール数に上限を設けるといた制限が API にかけられている場合がある。

そのため、サービス仕様書などに記載されている制限事項を事前確認して、高負荷時などにも業務要件を確保できるか検討する必要がある。

(3) データ転送性能

初期ロードやアーカイブサービス開始時など、大量データをバルクで送る場合、ネットワークに十分な帯域が確保できなければ転送時間が増大してしまう。特に、海外拠点利用時は、遠隔地への大量データ転送が必要となるため、初期ロードやアーカイブサービス開始時における、データ転送方法には十分な検討が必要である。

対応方法としては、たとえば初期ロード時については、国際スピード郵便等を用いたテープ/ハードディスク搬送も検討する。また、アーカイブサービスについては、差分データの転送でも対応できるか確認する。

(4) マルチクラウドの SLA

マルチクラウドで国をまたがってサービスを使う場合、一番低い SLA に律則されることになる。

対応方法としては、SLA のミニマムラインを定義し、それを満たすクラウド事業者を選択する。

(5) 品質

時差等で自国と海外拠点の負荷ピークが異なる場合、自国ビジネスアワー内にサービスの品質（ex. 応答時間）が悪化する可能性がある。

対応方法としては、自国のビジネスアワーへの影響を事前に確認し、影響の少ない事業者を選択する。あるいは、複数地域の DC を使い、高負荷時は切り替えを行うといった方法も考えられる。

3.2.4. セキュリティ

セキュリティの観点では、以下の 2 項目に関する検討・確認が必要である。

#	観点	検討・確認項目
(1)	セキュリティ	マルチクラウドのセキュリティ
(2)		ネットワーク

(1) マルチクラウドのセキュリティ

マルチクラウド、すなわち複数のクラウドサービスの組み合わせで自社サービスを実現する場合で、かつ国をまたがってサービスを使う場合、セキュリティレベルの統一が困難な場合がある。

対応方法としては、セキュリティのミニマムラインを定義し、それを満たすクラウド事業者を選択することがあげられる。

(2) ネットワーク

ベストエフォート型のネットワークを選択した場合、経路を特定することはできない。そのため、経路上のサーバやネットワーク装置のキャッシュにデータが残ってしまうとデータ漏えい等の問題が生じる可能性がある。

対応方法としては、以下が考えられる。すなわち、ベストエフォート型のネットワークを選択する場合には VPN を前提とするか、暗号化の上で通信を行う。あるいは、重要なデータについては、経路が特定される専用線に変更するといった方法も考えられる。

3.2.5. 保守

保守の観点では、以下の 2 項目に関する検討・確認が必要である。

#	観点	検討・確認項目
(1)	保守	保守品質
(2)		カスタマサービス（ヘルプデスク）

(1) 保守品質

国ごとでの保守品質の均一化が困難な場合がある。そのため、保守品質均一化のための検討が必要となる。

(2) カスタマサービス（ヘルプデスク）

現地語でしか対応ができない場合、カスタマサービスの品質が確保できないという問題が生じる。

対応方法としては、クラウド事業者を選択する際には、自社で対応可能な言語をサポートする事業者の範囲内で検討すると言ったことが考えられる。

3.2.6. その他

法規制/商習慣/性能/セキュリティ/保守以外では、以下の 4 項目の検討・確認が必要である。

#	観点	検討・確認項目
(1)	その他	現地対応
(2)		契約・申し込み
(3)		ネットワーク
(4)		調達

(1) 現地対応

国によって時差があり、休日が異なるため、運用時間や対応日を考慮する必要がある。

対応方法としては、事前に現地情報を入手して、利用制限のある日時・時間帯の対応方針を検討しておく必要がある。特に、対応時間に制限がある場合（ex. 9:00-17:00）には、国内時間で対応してもらえるか確認する必要がある。

(2) 契約・申し込み

契約書の翻訳版が提供されていても、翻訳版と基の契約書（現地語版）に齟齬がある場合には、基の契約書（現地語版）が優先される。そのため、契約書の原版を確認する必要がある。

(3) ネットワーク

たとえば、新興国や途上国では衛星回線しか利用できない地域があるなど、国・地域によってネットワークのインフラ整備状況が異なるため注意が必要である。

対応方法としては、対象国のインフラ状況を考慮して、利用するネットワークを選択する必要がある。

(4) 調達

国内と同等のハードウェアやソフトウェアが、現地で調達できない可能性がある。

対応方法としては、代替製品の使用の検討があげられる。また、グローバルに調達可能な製品のみを採用しておくといった対応も考えられる。

4. おわりに

本ガイドは、2011 年 4 月から 2012 年 3 月までの、JCC クラウドマイグレーション WG の活動結果をまとめたものである。本ガイドは、クラウドへのマイグレーションを行う際に、注意すべき点を列挙しており、何をサービスプロバイダに確認し、何を利用者自身が検討しなくてはいけないか等の参考情報として活用することによりサービスの品質を適格に把握し、効率よく導入していけるようガイドしていくことを目的としている。サービスプロバイダ側の設定ミスや操作ミスによってサービス停止やデータ消失が発生する事例も発生していることから、プロバイダ側の機能や運用体制まで理解した上で、導入検討を行うことはますます重要となっている。

創造的で多様なサービスが展開される社会に向けては、クラウドが有する低コスト、迅速な立ち上げ、柔軟なリソース割り当てといったメリットを利用したシステム構築やサービス開発が求められており、本報告書の活用により、クラウド活用がさらに進むことを期待したい。