ASCJ クラウドセキュリティガイダンス& ベストプラクティス概要

1.0 版

目次

1 なぜクラウドなのか

1.1 背景としての DX

近年、多くの企業経営者が DX の必要性を認識している。そこには技術革新、人々の価値観、ライフスタイル、自然環境の変化に伴い、かつてとは比較できないほどのスピードで変化し続けているビジネス環境において、自らの事業を変革しなければ生き残ることができない、という危機感が背景にある。具体的には、ベンチャー企業や他業界・業種からの新規参入者が最新のデジタル技術を駆使した新しいビジネス・モデルを展開し、既存産業を浸食・破壊ししつつある状況を脅威に感じているものと推察される。一方、DX を積極的に進め、既存マーケットにおける競争力の維持、新たな顧客セグメントの開拓、異業界・業種への参入に成功している事例も増えてきている。

このような中、クラウドの「俊敏性」「柔軟性」「コスト効率」といった特徴が注目されるようになり、DX 推進に不可欠な IT 環境として選ばれている。

1.2 クラウドのメリット

パブリッククラウドを実際に利用している企業が挙げるクラウドの一般的な利点について以下に述べる。

- **構成管理や運用保守労力の削減**
  クラウドを利用する場合、クラウドサービス事業者の責任範囲における保守運用作業（物理機器のメンテナンス、OS パッチ適用、バックアップ作業など）は、クラウドサービス事業者が対応する。そのため、クラウドサービス利用者が従来行っていた作業範囲や作業負担が低減でき、結果として従来の運用・保守にかかっていた労力の削減につなげることが可能である。

- **システムリソース調達の柔軟性、および調達コストの抑制**
  サーバ等のシステムリソースを数分で調達可能なため、従来に比較するとシステム開発期間が短縮される。また、クラウドではシステムリソースを必要な時に調達し、不要な時に開放することができるため、常に業務ピーク時の負荷状況に合わせた過剰なリソースを確保する必要がなく、状況に合わせてシステムリソースをコントロールすることで余剰なコストを発生させないことが可能である。

- **最新テクノロジーへのリーチ、および、開発スピードの俊敏性**
  クラウドサービス事業者は、クラウド上で利用できる新機能やサービス・オプションを毎年多数リリースする傾向にある。中には、機械学習、IoT、音声認識、感情認識等もあり、こうした最新テクノロジーの基礎部分を企業自ら開発する必要がなく、機能を用いて自社の商品開発に注力することが可能である。

- **バックアップの利便性、および業務継続性**
  クラウドサービス事業者は、距離が一定程度離れたデータセンターを複数使いサービスを提供していることが多く、クラウドサービスとして提供されるバックアップ機能を用いることで、バックアップの隔地保管が可能となるケースがある。

また、業務継続の目的での DR サイトについても、クラウドサービス事業者が国内・海外に展開しているデータセンター群や障害検知・復旧機能を用いることで、データセンター設置、DR サイト切替機器の調達・設置等を行うことなく DR サイトを構築することが可能である。DR サイトは、平常時には最小リソースで運用し、必要となった際にスケールアップさせることも可能である。

- **セキュリティ機能の提供**
  クラウドサービス利用者がセキュアにクラウドを利用するための充実した機能の提供をい進めており クラウドサービス事業者自身が培ってきたセキュリティ対策技術の一部を脅威検出サービスとして提供しているケースもある。また、ホワイトペーパー等によるクラウドサービスが提供する機能の利用におけるナレッジの提供を行っている。
  企業が独自にこういったセキュリティ機能を準備し保有するには、費用と労力の他、専門性が必要となるため容易なことではないが、クラウドではクラウドサービス事業者が提供するセキュリティ機能を用いながらセキュリティ対策を強化していくことも可能である。

1.3 クラウド導入の壁

企業へのクラウドの導入において、マネジメントやシステム開発現場の双方において様々な課題があり、それら課題によってスムーズに進まない、もしくは、時間を要する傾向がある。一般的に起こり得る課題を以下に挙げる。

- **経営層およびマネジメント層における課題**
  - 準拠すべき各セキュリティ規準について、クラウドと紐づけた解釈・判断が困難であり、各種ステークホルダーや監督・規制当局に対する説明責任を果たせるか不安である。
  - クラウドを利用する際に取るべきセキュリティ対策とその充足性に関して説明が困難であり、リスク管理部門や上位層からの理解が得られない。
  - 従量課金制のため、事前のコスト試算とは異なる実績となる可能性が高く、運用中の予期せぬコスト増加が不安でありとともに、費用対効果が得られるか不明確である。
- **システム開発現場における課題**
  - クラウドを用いた設計や構築を行ううえで必要な知識・スキルを不足なく、かつ十分なスピードで習得することが困難であり、オンプレミスをベースにしたセキュリティ要件に対して、クラウド上で取るべきセキュリティ対策に置き換えることが困難である。
  - クラウドのナレッジを十分に有する人材が不足しており、レビュー体制を整えることが難しい。
  - マネジメント層が抱える漠然とした不安に対して、セキュリティ対策の充足性を説明することが困難である。

これらの課題はクラウドを導入する企業だけの課題だけではなく、外部委託の依存度が高い日本においては、その企業を支援するコンサルティングファームや SIer の課題にもなっている。

2 ASCJ の背景と目的

日本においても 2018 年 6 月、各府省庁情報化統括責任者（CIO）連絡会議にて「政府情報システムにおけるクラウドサービスの利用に関わる基本方針」が発表され、クラウド・バイ・デフォルト原則（政府情報システムを構築する際は、第一候補にクラウドサービスの利用を検討するという方針）が打ち出され、クラウドの活用を強く推奨している。それに呼応する形で、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録する制度である政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program (ISMAP)）が発表され、2020 年度から運用が開始される。この制度によりセキュリティ水準の確保とクラウドサービスの効率的な選定が可能となることが期待されている。

このように、クラウド活用が推奨され、それを支える制度も整いつつある一方で、世の中ではクラウドサービス利用者に起因するセキュリティインシデントが後を絶たない状況であり、クラウドサービス利用者はオンプレミスとは異なるリスクを把握、適切に管理し、セキュリティやコンプライアンスに対応していくことが一層求められている。

このような背景をうけ、ASCJ では、DX の土台となるクラウドについて、クラウドを利用する企業や組織が、安心・安全にクラウドサービスを採用し、継続的に利用していくための適切なリスク管理の在り方等について、セキュリティシステムの新たな姿を検討していくことを目的として活動している。

これを目的とし、前述のクラウド導入における課題の解消の手助けとして、ASCJ では本書の他に以下のドキュメントを提供している。

Cloud Risk Control Framework

クラウド導入の際に考慮するべきリスクとリスク管理策について、課題となり得る国内・グローバルの公知の基準とリスク管理策を整理し、対策の優先度やシステム開発・運用の方針を検討する際のポイントをまとめた資料。

ACSJ 技術文書

リスク管理策を実現する アマゾン ウェブ サービス（AWS）の解説：

リスク管理策を実装するために利用可能な AWS サービス（AWS が提供する機能）の紹介およびその特性をまとめた資料。

サンプルアーキテクチャ：

機能選定や実装するリスク管理策の優先度を検討する際のポイントとして、サンプルとなる具体的なアーキテクチャとそのアーキテクチャで取り得るリスク管理策をまとめた資料。

3 Cloud Risk Control Framework Overview

Cloud Risk Control Framework (以下 CRCF)は、クラウド特有のセキュリティに限らず、システムセキュリティ全般および IT 戦略も対象範囲に含め、クラウドを安全に利用・活用する際に考慮すべきリスクとコントロールを抽出しまとめたフレームワークである。

3.1 CRCF の構成

CRCF は、「Risk Control Matrix」と「Control Reference」の2つのシートで構成されている。

3.1.1 Risk Control Matrix の概要

Risk Control Matrix では、クラウドを安全に利用・活用する際に考慮すべきリスクと、システム検討フェーズから運用フェーズにおける検討ポイントをコントロールとして挙げ、それぞれのリスクとコントロールの関連性を整理している。

Risk Control Matrix の縦軸

グローバル標準として、ISO27017 においてもリスク分析を実施するための参考として紹介され、日本においてもクラウドサービスを利用する企業で広く活用されている ENISA(欧州ネットワーク情報セキュリティ庁)のクラウドセキュリティガイドライン「クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項」をベースに、オンプレとは異なるクラウドのセキュリティリスクを挙げている。

- ポリシーと組織的なリスク
  - ロックイン
  - ガバナンスの喪失
  - コンプライアンスの課題
  - 他の共同利用者の行為による信頼の喪失
  - クラウドサービスの終了または障害
  - クラウドプロバイダの買収
  - サプライチェーンにおける障害
- 技術的なリスク
  - リソースの枯渇（リソース割当の過不足）
  - 隔離の失敗
  - クラウドプロバイダ従事者の不正－特権の悪用

- 管理用インターフェースの悪用（操作、インフラストラクチャアクセス）
- データ転送途上における攻撃
- データ漏えい（アップロード時、ダウンロード時、クラウド間転送）
- セキュリティが保護されていない、または不完全なデータ削除
- DDoS 攻撃（分散サービス運用妨害攻撃）
- EDoS 攻撃（経済的な損失を狙ったサービス運用妨害攻撃）
- 暗号鍵の喪失
- 不正な探査またはスキャンの実施
- サービスエンジンの侵害
- 利用者側の強化手順と、クラウド環境との間に生じる矛盾

- 法的リスク
  - 証拠提出命令と電子的証拠開示
  - 司法権の違いから来るリスク
  - データ保護に関するリスク
  - ライセンスに関するリスク
- クラウドに特化しないリスク
  - ネットワークの途絶
  - ネットワークの管理（ネットワークの混雑、接続ミス、最適でない使用）
  - ネットワークトラフィックの改変
  - 特権の（勝手な）拡大
  - ソーシャルエンジニアリング攻撃（なりすまし）
  - 運用ログの喪失または改ざん
  - セキュリティログの喪失または改ざん（フォレンジック捜査の操作）
  - バックアップの喪失、盗難
  - 構内への無権限アクセス（装置その他の設備への物理的アクセスを含む）
  - コンピュータ設備の盗難
  - 自然災害

これら ENISA のクラウドのセキュリティリスクの他に、クラウドを活用するにあたり考慮が必要となるポイントをリスクとして3つ追加している。

- IT 戦略およびガバナンス
- コストマネジメント（ROI、および TCO）
- クラウドサービス導入の失敗（開発、移行、運用設計）

Risk Control Matrix の横軸

システム化検討・要件整理、基本システムの検討、クラウドサービス事業者の選定、システムの継続的な構築・運用という 4 つの大きなカテゴリに分け、それぞれのカテゴリ内での検討ポイントをコントロールとして記載している。

3.1.2 Control Reference の概要

Control Reference では、クラウドサービス利用者がクラウドサービスの利用・活用を検討する際に検討すべきコントロールの観点をまとめている。あわせて、国内およびグローバルの主要な基準とガイドラインを、その特性や偏りを排除したうえで、各コントロールに対してマッピングしている。そのため、各基準・ガイドラインの特性や専門性を必要とする場合には、Control Reference にてマッピングを参照し、その項目で求められる具体的な対応内容を基準・ガイドライン文書にて確認することが必要となる点に留意いただきたい。その他、CEF 利用時における留意事項や前提については、CEF 内を参照のこと。

Control Reference の縦軸と横軸

このシートでは Risk Control Matrix の横軸を縦軸（B 列、C 列）として利用し、各コントロールで考慮すべき内容を D 列に記載している。また、様々な公知のガイドラインや基準内の「必須」とされる項目やシステムの基本的な対策とされる項目とマッピングしている。これらの項目は全て必ず対応しなければならないものではなく、クラウドサービス利用者の業界やシステムの特性に合わせ、セキュリティ目標を定め、必要となる対策を検討のうえ、選択・適用するものである。なお、自社として選択・適用しないコントロールについては、企業やシステムの成長・変化に伴い、対応すべきコントロールが変化した際に見直しやすいよう「対応しない理由」を明確にしておくことを推奨する。

現在マッピングに使用している公知のガイドライン、基準、技術文書は以下の通り。

- 内閣サイバーセキュリティセンター（NISC）
  「政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）」
- NIST
  「連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策 SP 800-53 rev.4」

- Cloud Security Alliance
  「Cloud Controls Matrix Version 3.0.1」
- Amazon Web Services
  「AWS : セキュリティプロセスの概要」
  「AWS のリスクとコンプライアンス」
  「PCI DSS スコーピングおよび AWS 上でのセグメンテーションのためのアーキテクチャの設計」
  「DDoS に対する回復性に関する AWS のベストプラクティス」
  「AWS Cloud Adoption Framework の概要」
  「AWS Well-Architected フレームワーク」

3.2 コントロール概要

Risk Control Matrix の横軸および Control Reference の縦軸は、大きく4つのカテゴリにわけ、それぞれ C1～C4 というラベルで分類している。

C1：システム化検討・要件整理

C2：基本システムの検討

C3：クラウドサービス事業者の選定

C4：クラウドサービス利用における継続的構築・運用

経営戦略および IT 戦略の立案後、C1 からスタートする。システム導入時においては、C1 から C4 へ順に行うが、システムの本番稼動後は C1～C4 の要素を定期的、もしくはトリガーとなる経営戦略立案、法令・基準の改定、システムへの機能追加等のイベントが発生した場合に該当する項目を随時実施していく。

3.2.1 [C1]システム化検討・要件整理

「C1：システム化検討・要件整理」では、まず、システム化対象業務や取り扱う情報を明確化(C1-1)したうえで、全社の経営戦略および IT 戦略との整合性を確認する(C1-2)。

次に、後続で整理するシステム要件の軸となる企業のポリシー・ガイドライン(C1-3)および事業継続計画および災害復旧計画(C1-4)を明確にする。また、システム化実施後に効果を測定するため、経営戦略と IT 戦略の両面から評価する KPI を定めること(C1-5)の他、説明責任を果たすために必要となる責任者と窓口の明確化（C1-6)を実施する。

C1-7 では、システム構築・運用体制の確認を実施する。クラウドを用いた設計・構築・運用においては、クラウドコンピューティングの基礎知識や一般的なインフラ知識だけではなく、クラウドサービスを安全に使いこなすための様々な知識とスキルが求められる。しかしながら、そういった人材のは企業内外問わず少ない傾向にあるため、システム化検討段階から、人材の確保が可能か確認・検討する必要がある。

C1-8 では、クラウド人材の育成・教育について検討する。クラウドを活用し DX を進めるためには、前述の知識とスキルに加え、当事者として自社サービスを作り上げていくスキルも求められる。このような幅広い知

識とスキルを持つ人材を育成するには時間を要するため、システムの運用・改善のフェーズの体制も見据え、システム化検討段階から人材育成・教育計画の検討をはじめることを推奨する。

C1-9 では、システムで扱う情報の重要性とその保護についての考え方を徹底させ、情報の安全性を確保するための人的セキュリティ対策について確認する。

C1-10～C-14 では、稼働率や性能、拡張性、完全性等のシステム要件のベースを整理する。検討項目自体はクラウドに特化したものではない。しかしながら、クラウドでは達成困難な要件となる可能性が否定できない。また、クラウドで達成するためには必要となるコンポーネント、構成（アーキテクチャ）に影響を与える要件となる可能性が考えられ、ひいては構築・ランニングコストへ大きく波及する可能性がある。そのため、クラウド利用を検討する際には、これらの項目を早い段階で明確化することが求められる。

3.2.2[C2]基本システムの検討

「C2：基本システムの検討」では、「C1：システム化検討・要件整理」で整理した要件を満たす具体的な構築方針・移行方針を検討し定める。検討する際、IT 戦略を念頭に、各クラウドサービス事業者がベストプラクティスとして提唱する移行パターン（例えば、「AWS への移行:ベストプラクティスと戦略」）等と照らし合わせ、どのような構成とするかを検討するとともに、クラウドとの親和性を確認する。このフェーズでは、構成だけではなく、アプリケーションのポータビリティについてもあわせて検討する(C2-1)。IaaS ベースでの単純移行とした場合であっても、移行後にクラウドサービスが提供する最新技術を用いたサービスの活用し、データ活用を進めるには、アプリケーションのポータビリティを高めておくことが鍵となるためである。アプリケーションの要件次第で、想定するシステム構成が変動するため、このタイミングで行うことが望ましい。

次に、対象システム単体だけではなく、他システムとのデータ連携・共有や、将来的なデータ活用を見据えたデータ保管・処理を考慮した構成を検討する(C2-2)。

その後、システムが必要とする構成が見えてきたタイミングで、IaaS/PaaS/SaaS 等クラウドサービスの選択(C2-3)を実施し、代替策の検討(C2-4)、出口戦略の検討(C2-5)を行う。

出口戦略を定めるの背景には、クラウド利用におけるリスクの 1 つであるクラウドサービス利用者側で制御できないイベント（長期メンテナンスによるサービス停止、サービスの提供終了、料金の上昇等）による影響がある。特に、法令や公的基準の改定に対してクラウドサービス側がタイムリーに対応できないケースにおいては、クラウドサービス利用者側への影響が甚大となり得ることから、事前に対策を検討しておく必要がある。一般的な対策例としては、システムの閉塞、別クラウドサービスやオンプレへの移行/切替等があげられる。また、その対策を行うにあたり必要となる時間を考慮し、出口戦略の発動条件を事前に検討することが肝要である。

以降の C2-6、C2-7 では、初期コスト、運用コストの検証を行う。検討項目自体はクラウドに特化したものではないが、クラウドの特徴の１つである「従量課金」という観点から、データ量、リクエスト量の増減を考慮した数年間に渡った運用コストの検証が求められる。

3.2.3[C3]クラウドサービス事業者の選定

「C2：基本システムの検討」にてクラウドを利用する方針となった場合に、「C3：クラウドサービス事業者の選定」を行う。このフェーズでは、クラウドサービス事業者のガバナンス・コンプライアンスや、SLA を含む提供サービス仕様を確認したうえで、複数のクラウドサービス事業者を比較(C3-1)後、利用するクラウドサービスを選定する。

C3-2 から C3-13 では、クラウドサービス事業者との契約内容の他、委託先管理としてのモニタリング手段や、クラウドサービス利用者側の業界特性に応じて必要とするコンプライアンス認証取得状況、準拠法、管轄裁判所、契約解除・終了時の対応等の確認を行う。

準拠法(C3-8)および管轄裁判所(C3-9)については、契約で定められる内容によっては、係争に発展した場合に海外の法制度や裁判制度にあわせた対応が求められるほか、対応可能な弁護士の確保等、多額の費用が掛かる可能性がある。また、クラウドサービス事業者が何らかの訴訟や犯罪操作にクラウドサービス事業者が巻き込まれた場合に、捜査機関によってサーバの差し押さえが発生する等の事態が想定されるため、どの国の法律・法令が適用されるのか、管轄裁判所はどこになるのかを事前に確認する必要がある。

契約解除・終了時の対応(C3-13)については、データの不正利用や情報漏洩等につながる可能性があるデータ消去が特に留意すべきポイントとなるため、クラウドサービス事業者によりデータ消去を行ったことを確認する手段が提供されるかを確認する必要がある。確認手段が提供されない場合には、クラウドサービス事業者側でのデータの取り扱いやメディア破棄時のルールおよび管理方法が適切であることを各種ホワイトペーパーや SOC レポート等で確認のうえ、クラウドサービスが提供するデータ保護や利用状況の証跡取得の仕組みを用いてクラウドサービス利用者側が実装可能なデータ破棄の統制例を確認することも有用である。

C3-14 から C3-23 は、クラウドサービス事業者が実施しているセキュリティに関わる統制状況の確認となる。一般的に、第三者によるコンプライアンス認証および証明を用いて確認する内容となる。例えば、2020 年度から運用開始予定の ISMAP（統制状況の確認は 2021 年度以降を予定）や、SOC レポート等を用いて確認することが可能である。この際、結果だけではなく、クラウドサービス事業者が行っている統制の内容を確認することが重要である。また、これらコンプライアンス認証および証明では、クラウドサービス事業者の責任範囲のみをカバーしている点に留意すること。クラウドサービス利用者側の責任範囲については、クラウドサービス利用者側のセキュリティに係る統制が必要となるため、別途確認、検討し、必要に応じて C4 以降の設計に盛り込むこと。

C3-24～C3-26 では、クラウドサービス利用者が必要とするセキュリティ関連機能をクラウドサービスが提供しているかを確認する。

C3-27 では、クラウドサービスが提供する機能のうち、既存システムの他、自動化ツールやコミュニケーションツールを含めたサードパーティー製アプリケーションと連携するための機能について、クラウドサービスの独自仕様になっていないかを確認する。

3.2.4[C4]クラウドサービス利用における継続的構築・運用

「C4：クラウドサービス利用における継続的構築・運用」では、クラウドサービス事業者を選定後、C2 で定めた構築方針・移行方針をベースに、C1 で整理した要件と C3 で選定したクラウドサービスの特徴・仕様を組み合わせて、具体的にシステムの設計に落とし込む。

検討項目自体はクラウドに特化したものではないが、全項目に対して、選定したクラウドサービス責任分界点および利用対象機能の仕様を考慮した設計が必要となるほか、クラウドサービスを利用するからこそ新たに発生する運用イベントの整理や、クラウドサービスが提供する機能を組み込んだ運用オペレーションの自動化の検討など、クラウドサービス利用時に留意すべき観点を加えている。

各項目に関連する AWS サービスやアーキテクチャ例については、技術文書「AWS 環境におけるクラウドセキュリティへの取り組み方」を参照のこと。