クラウドを利用した
システム運用に関するガイダンス
（要約版）

令和４年４月５日

内閣官房内閣サイバーセキュリティセンター
重要インフラグループ

改定履歴

改定年月日	改定箇所	改定内容
2021 年 11 月 30 日	―	・初版決定
2022 年 4 月 5 日	関連用語集	・用語集を一部修正

はじめに

本ガイダンスは、増加するクラウドサービスの選定や利用、サービスを使った環境の構築や運用などを行うに当たり、クラウドサービスの「利用者[1]」（以下「利用者」という。）がクラウドサービスの基本を理解し、クラウドサービスにおけるインシデント（企業にとって好ましくない事象や出来事）の発生を可能な限り抑制することや、インシデントが発生した際の対応及びステークホルダー（利害関係者）の連携によって事態の解決を図る重要性など、クラウドサービスの安全な運用に重点を置いた利用者向けの基本的なガイダンスの要約版です。

昨今、個別の動作環境（ハードウェアやソフトウェア）を準備して、自らコントロールする「オンプレミス」に代わり、クラウドサービスを活用したシステム構築や運用が主流となってきています。確かに、利用者にとってクラウドサービスを利用することは、調達や導入等の負担軽減に寄与しますが、利用者からシステム運用や責任そのものがなくなるわけではありません。クラウドサービスでは、クラウド事業者が提供する動作環境を活用していることから、利用者が制御できない環境や領域が存在するため、利用者の目に見えないところでクラウドサービスの更新や仕様変更が行われます。

そのため、クラウド事業者の作業によってインシデントが発生する場合もあり、利用者はクラウド事業者からWebサイトへの公開等により提供される情報の把握や変更管理などを適切に行う必要があります。インシデントによってはクラウド事業者もその原因が分からず、約款や利用規約などの取り決めにもない想定外の事態が発生する場合もあります。その場合は、クラウドサービスに係る全てのステークホルダー、関係機関や、サイバーセキュリティコミュニティが協力しながら、事案対応を行う必要があります。

クラウドサービスは約款による契約に基づいて提供されることから、利用者がクラウドサービスを活用し、顧客に対して何らかのサービス等を提供する事業を行っている場合、その顧客から見れば、利用者が当該サービス等の提供元となります。このため、クラウド事業者に起因するインシデントが発生した際、クラウド事業者は基本的には約款や利用規約で定めている範囲で責任を負う一方、それ以外の範囲については、利用者に責任が問われる場合があります。クラウドサービス利用に関して、初期の導入の容易さや負担軽減のメリットがある一方、オンプレミスと同等に利用者の責任は存在することから、システムの運用・維持体制の整備が不可欠であることを認識することが重要です。

我が国では、利用者が様々な情報技術を活用する場面において、自組織のみで対応が完結することは少なく、システムの構築や運用の全体や一部を外部に委託しているのが現状です。そのため、情報システム子会社やシステムインテグレータ（以下「SIer」という。）をはじめとしたステークホルダーを把握して、我が国全体（Cybersecurity for All）で対応することが欠かせません。

---

[1] クラウドサービスを利用する事業者のほか、地方公共団体も含む。

クラウドサービスの基本理解

変化の激しい現代社会において、早期に事業を立ち上げ、変化させるためにはクラウドサービスの活用は欠かすことができません。しかし、一言で「クラウドサービス」と言ってもその形態は様々で、利用者はどのようなクラウドサービスを活用するのか、適切に選定する必要があります。

NIST SP800-145[2]などでも定義されているように、ハードウェアや仮想化ソフトウェアなどの基盤となる環境を整備しているのが「IaaS(Infrastructure as a Service)」、そしてOSやアプリケーションを制御、支援するミドルウェアまでの環境を整備しているのが「PaaS(Platform as a Service)」、さらにアプリケーションまでの環境を整備しているのが「SaaS(Software as a Service)」です。クラウドサービスは後者になればなるほど、クラウド事業者が提供する範囲が広がり、利用者はより早く活用することが可能です。

また、これまで 3 つの分類で語られることが多かったクラウドサービスですが、昨今ではさらに細分化されています。例えば、様々な環境で利用可能なアプリケーションの開発ができるCaaS(Container as a Service)や、サーバレスでアプリケーション開発ができるFaaS(Function as a Service)等の形態が存在し、それらを組み合わせてシステムが構築されるようになり、より複雑化しています。

クラウドサービス活用のステークホルダーの把握

利用者にとっては、クラウド事業者からクラウドサービスを直接調達する場合や、販売者や構築者を介して調達する場合など、クラウドサービスの活用には様々なステークホルダーが存在します。利用者はステークホルダーを把握し、締結された契約の相手方、その契約内容(約款、利用規約等[3])及び契約に基づく責任範囲を把握する必要があります。システム上のステークホルダー(表 1)に加え、データを取り扱うステークホルダー(表 2)についても把握する必要があります。なお、以下のステークホルダーについてはあくまでも例示であり、サービスによっては全てのステークホルダーが存在しない(利用者とクラウド事業者のみの)場合もあります。例えば、受託開発の場合、受託開発に加えてライセンスを利用する場合、利用規約に同意して利用する場合等、ステークホルダーの構成は様々です[4]。

---

[2] NIST(アメリカ国立標準技術研究所)によるクラウドコンピューティングの定義
https://www.ipa.go.jp/files/000025366.pdf

[3] 約款、利用規約、利用条件等があり、取引条件を記載した文書を指す。

[4] 自治体の SNS 利用と個人情報へのアクセス
https://cio.go.jp/sites/default/files/uploads/documents/dp2021_04.pdf

表 1　システム視点でのステークホルダー例

項目	説明
利用者	クラウドサービスやシステムを利用する組織
販売者	クラウドサービスやシステムを販売する組織
構築者	クラウドサービスを活用してシステムを構築する組織 (利用者の子会社や SIer など)
設置者	クラウド構築者を支援して、実作業や設置を行う組織 (SIer や SIer の委託企業など)
運用者	構築されたシステムの運用を支援する組織 (SIer や SIer の委託企業など)
クラウド事業者	クラウドサービスを提供している組織 ※組織によっては日本国内には販売拠点や一時的なサポートを行う体制しかない場合があり、最終的なサポートの判断や解決策の提供などは、国外の拠点から行う場合もあるため、各ステークホルダーはクラウド事業者の国内外の体制の確認を行うとともに、クラウド事業者は体制について開示する必要があります。
顧客	利用者がクラウドサービスを利用してシステムを構築し、何らかのサービス等を提供する対象者

表 2　データ視点でのステークホルダー例

項目	説明
保有者	クラウドサービスに保存するデータを保有している者(独自にデータを作成した者等)
保存者	保有者のデータを保存している者(所有者の業務や作業などの委託事業者)
保管者	保有者のデータを保管している者(クラウド事業者)
使用者	保有者のデータを利用する者(情報収集者や保有者の許諾を得て利用する者)
加工者	保有者のデータを編集・修正する者

「責任共有モデル(Shared Responsibility Model)」について

クラウドサービスを活用する際、「責任共有モデル(Shared Responsibility Model)」の理解が大前提となります。これは、利用者とクラウド事業者が、責任分界点を定めるだけではなく、運用責任を共有し合っているという考え方です。

この責任範囲はクラウドサービスを提供するクラウド事業者やサービス内容によっても異なるため、利用者はその違いを事前に確認する必要があります。しかし、どのようなクラウドサービスでも、組織としての活用の目的や指針、設定や接続する端末の安全性の確保、さらには管理する(又は生み出される)データなどの取扱は、概ね利用者側の責任です。また、先に述べたとおりクラウドサービスの活用に当たっては多数のステークホルダーが存在し、一般的に利用者側に責任がある領域も外部へ委託している場合や外部からの支援を受けている場合があります。そのため、責任共有モデルは構築者や設置者などの

ステークホルダーを踏まえた上で理解する必要があります。

クラウドサービスを安全に利用していくためには、責任範囲を区別する責任分界点の明確化、インシデント発生時の対応等をあらかじめ検討する必要があります。こうした背景を踏まえ、米国 NSA[5]は 2020 年 1 月にクラウドサービスの脅威・脆弱性と責任共有モデルを示しています。(図 1)

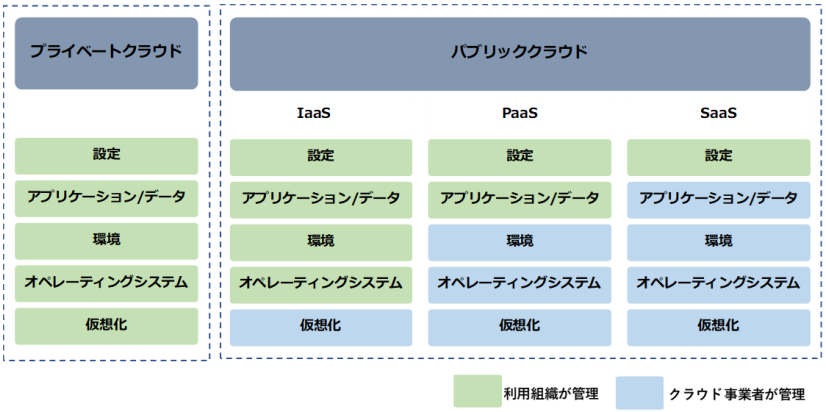

図 1　NSA によるクラウドサービスにおける責任共有モデル

利用者は SaaS としてサービスを利用しているつもりでも、その背景には、IaaS や PaaS を提供する別のクラウド事業者が存在している場合があります。そのため、利用者はクラウドサービスのステークホルダーを正しく理解する必要があります。

この場合は、特にクラウド事業者や構築者においても事前の協議を行い、対応や責任範囲の明確化を行い、対応範囲と責任の落とし穴を生じさせないようにしておく必要があります。また、クラウド事業者のデータセンターが海外にある場合などは、当該国の法令や政府機関の対応、データの取扱やサービスの支援内容など細心の注意を払う必要があります[6]。

クラウドサービス活用の注意点

・クラウドサービスの選定

クラウドサービスの選定に当たっては、組織の活用目的に最も合致したサービスを、利用者が主体となって選定します。この際、利用者は共存共栄ができる、信頼できるクラウドサービスを選定する必要があります。有事の際のインシデント対応において共に連携できること、クラウド事業者側のログデータ等、クラウドを活用して提供するサービスの重要度に応じた、インシデント対応に必要な情報が即座に提供されること、想定外のインシデントでも問題解決のための提案ができること等、クラウド事業者のサポート方針やサポートレベルを見極めなければなりません。また、日頃から顧客及びセキュリティコミュニティに向けての積極的なセキュリティ情報発信が行われているかも重要な評価項目です。SaaS の機密性やデータ安全に関して、ISMAP(日本)や FedRAMP(米国)といった認定制度があり、選定の際の参考となります。

---

[5] アメリカ国家安全保障局(National Security Agency)

[6] 内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン(令和３年度版)」遵守事項 4.2.1(3)(e)「国内法以外の法令及び規制が適用されるリスク」について参照

そして利用者は、クラウド事業者が公開している情報(各種認証など)を把握した上で、構築者や設置者との要件定義を行い、クラウドサービスを活用したシステムや環境を整備します。

なお、クラウド事業者は情報の非対称性などにも深く考慮し、利用者や構築者、設置者などに対してもクラウドサービスに関する情報を、丁寧かつ分かりやすく公開、提供し続ける必要があります。

・設定不備や脆弱性に係る診断

設定不備や脆弱性に係る診断を行うことで、利用者が守るべきデータをはじめとした情報資産を適切に守ることができているのか確認し、インシデントの防止を図ることができます。構築者や設置者が独自に行う場合もあれば利用者主導で行う場合もあり、全てのステークホルダーが設定や脆弱性対応の重要性を理解し、対応に努める必要があります。

・運用体制の確保

これまで述べてきたように、クラウドサービスだからと言って、必ずしも利用者の運用負荷が軽減されるわけではありません。そのため利用者は、(兼任であったとしても)クラウド事業者や運用者などとの連携を行う窓口、運用に関する責任者、作業を指示又は実施する担当者、脅威や脆弱性情報、クラウドサービスの更新情報などを収集し、展開する担当者を任命し、CSIRT のように組織的に運用できる体制を確保します。

・仕様変更に対する十分な対応

クラウドサービスは利用者や構築者などの見えないところで更新や仕様変更が行われるため、利用者はクラウド事業者から案内された内容を理解、評価し、適切に対応する体制を整えておく必要があります。

なお、クラウド事業者側も更新や仕様変更についてその説明責任を果たす必要があります。特に仕様変更に当たっては、クラウド事業者が、利用者が設定・運用しているデータへのアクセスコントロールや権限、手段、機能等が変わることのないように考慮した上で仕様変更を行い、利用者のデータや情報資産の安全性を確保する必要があります。もし、クラウド事業者による仕様変更によってデータや利用者全体に悪影響を及ぼすことが判明した場合、クラウド事業者は即座に応急処置や緩和策などの提示を行い、利用者に対応を促すよう周知する必要があります。

・サービス利用約款の把握

技術的な側面だけではなく、法律的な側面についても対応が必要です。2020 年に施行された改正民法の規定を踏まえ、利用者はまずクラウド事業者と行う取引が「定型取引」に該当するものなのかを確認し、サービス利用約款や利用規約等に定型約款の規定が適用されるのか否かを確認する必要があります。いずれの契約形態であっても、契約締結後、利用約款等の変更が利用者にとって利益になる場合も不利益になる場合もありますので、想定される事態に備えて法務部門等と相談していただくことが望まれます。

なお、クラウド事業者においても、提供するクラウドサービスが不特定多数との取引を目的とした定型取引としての性質を有するのであれば、サービス利用約款が定型約款に該当する可能性があることを忘

れてはなりません。

さらに、クラウド事業者は定期的に約款、規約などの変更を行う場合があり、利用者は、約款の性質によってクラウド事業者との取引における法律的な側面を継続的に監視する必要があります。クラウド事業者の変更内容によっては利用者と構築者や運用者との個別契約の締結や既存の契約の変更を行わなければならない場合があり、双方で協議し解決に向けて努める必要があります。

なお、利用者は約款や規約などのクラウド事業者との契約については、できる限りの確認を行い、またクラウド事業者は約款や規約などの変更に当たっては、その変更点を示したり、解説を行ったり、変更された約款や規約などの効力発生要件を明らかにするなどして、利用者や運用者などに対して、情報が適切に伝わるよう発信する必要があります。

クラウドサービス活用のインシデント対応に備えて

クラウドサービスの活用に限らず、利用者はインシデントを想定し、備える必要があります。発生しうる代表的なインシデントは、「システムやサービスの脆弱性を狙った攻撃」、「OSINT 等を活用した攻撃」、「装置故障などによるシステム障害」、「クラウドサービスの故障」、そして「設定の不備」が挙げられます。

まず、利用者や構築者などは、過去にクラウド事業者(できればクラウド事業者の競合企業も含め)で発生したインシデントを確認し、インシデントを「想定内のインシデント」とするように努め、事前に対応や対策を練ることが大切です。また利用者はクラウド事業者や運用者などが提供しているサポート(保守・運用)契約を事前に確認し、SLA(Service Level Agreement)や SLO(Service Level Objective)、オンサイト(訪問対応が可能な)サポートの有無など、事前にインシデント発生時の対応を確認します。特に重要なシステムにおいてクラウドサービスを活用する場合は、事前に経営層を含めて当該サポート契約の締結について協議し、クラウド事業者や運用者と契約を行うことが望ましいでしょう。

さらに、インシデントが発生すると、利用者や運用者、構築者などは、インシデントの原因究明に努める必要があります。それぞれの組織でインシデント対応が行えるように、あらかじめクラウド事業者に提供可能なログやその内容(例えば、ログの種類や提供期間、費用、教育の有無など)について確認をしておくとよいでしょう。なお、インシデント発生時にどこの組織に調査や解析などをお願いするのか、事前に見当をつけておくことも大切です。

ステークホルダー連携によるインシデント対応

インシデント発生後は、先のステークホルダーに加えて、監督官庁や法執行機関、(個人情報の漏えい・滅失・毀損に関する場合は)個人情報保護委員会などとの連携が加わります。また、メディアからの問合せや法的解釈が求められる場合に備え、広報や法務に関係する担当者や部門とも連携を行います。先に

述べたクラウド事業者や運用者などの窓口の把握だけではなく、自組織の広報や法務に関係する窓口についても事前に把握し、いつでも連携できる体制を整備します。さらに、自組織やシステムの関係者だけではなく、国内外の研究者や技術者から連絡を受けることにより、インシデントが発見される場合があります。状況によってはこのようなステークホルダーとの連携が追加されることも認識しておくことが大切です。

インシデント発生後、インシデントの性質により、またクラウド事業者・運用者などからの情報提供・情報公開が行われていないなどの場合、原因(サイバー攻撃や設定不備、脆弱性など)の特定ができず、利用者で対応できなくなるおそれがあります。特に、想定外のインシデントが発生した際に、リスク情報の提供などがステークホルダーにおいて必要なときには、クラウド事業者は秘密保持に配慮しつつ、事業遂行に係る社会的責任を踏まえた対応として、利用者とその顧客に情報の提供や連携を行う必要があります。また、利用者や構築者、運用者、クラウド事業者などは「日本シーサート協議会」(NCA)などのコミュニティに参画し、ステークホルダー全体でインシデントの解決に向けた取組を行えるように、事前に連携体制を確保します。利用者はインシデント情報(TLP(Traffic Light Protocol)を設定)の共有をできる限り行い、クラウド事業者も国内外で差が生じることのないよう情報を提供し、インシデント対応が完了するまで支援を続けます。特にコミュニティに対しては、利用者に限らずクラウド事業者も積極的に情報共有や連携を行う必要があります。

なお、コミュニティに情報共有や連携を行っている中で、我が国のサイバー空間の安全性に大きな影響を及ぼすおそれのある場合は、速やかに内閣サイバーセキュリティセンター(NISC)などの政府機関に情報共有を行い、国を挙げてサイバー空間の安全確保に努め、早期のインシデント解決につながる対応を官民の枠を越えて行います。

おわりに

本文書はクラウドサービスの基本的な内容や姿勢を明記したものであり、今後このガイダンスは利用者、クラウド事業者などの全てのステークホルダーの連携によって、より一層安全性の確保のために研鑽していくことが大切です。技術や活用方法など様々な変化が生じれば、このガイダンスも継続的に見直していく必要があり、完成に向けた継続的な議論や取組が必要です。

クラウドサービスの活用が欠かすことができない時代であるからこそ、普段から、そして特にインシデントが発生したときは、コミュニティを含む全てのステークホルダーが健全に連携し合う必要があります。クラウドサービスのステークホルダー連携こそが、我が国のサイバー空間の安全に貢献できると言っても過言ではありません。

「Cybersecurity for All」、誰も取り残すことなく、全てのステークホルダーがクラウドサービスの理解に努める一方で、情報の非対称性を理解した上でそれぞれが説明責任を果たし、誰もが安心・安全にクラウドサービスを活用できる社会を実現していくよう努める必要があります。

関連用語集

クラウドコンピューティング

利用者がサーバやストレージ等のリソースを物理的、仮想的に共用し、インターネットを介してサーバ、アプリケーション等をどこからでも必要に応じて利用可能とするコンピュータ活用方式。実装方式として、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド等がある。

クラウドサービス

クラウドコンピューティングを活用して提供されるサービス。代表的なサービスモデルとして IaaS/PaaS/SaaS がある。

パブリッククラウド

クラウドサービスの提供方式のひとつ。CPU、ストレージ、メモリ等のコンピュータリソースの利用率を最適化するために、一般ユーザや複数の利用者でリソースを共用して実装されるクラウドコンピューティング方式。

プライベートクラウド

クラウドサービスの提供方式のひとつ。クラウド事業者が１つの組織に対してクラウドサービスを提供するものであり、当該組織外のユーザは利用することができない、その組織専用に実装されるクラウドコンピューティング方式。

ハイブリッドクラウド

パブリッククラウド、プライベートクラウド等、複数の提供方式を組み合わせて実装されるクラウドコンピューティング方式。パブリッククラウドで Web サービスを構成し、認証情報はプライベートクラウドに保管して Web サービスの認証処理を行うといった例が挙げられる。

オンプレミス

従来型のシステム構築手法で、自組織の施設内(事務所内や自組織で保有するデータセンター内等)にシステムを設置する方式のこと。

IaaS(Infrastructure as a Service)

クラウドサービスモデルのひとつ。利用者に CPU、ストレージ、メモリ等のコンピュータリソースが提供される。利用者はそのリソース上に OS 等を構築することができる。

PaaS(Platform as a Service)

クラウドサービスモデルのひとつ。IaaS に加えて、OS、基本機能、開発環境等もサービスとして提供される。利用者はそれらを組み合わせて情報システムを構築することができる。

SaaS(Software as a Service)

クラウドサービスモデルのひとつ。PaaS に加えて、利用者に特定のアプリケーション(メールサービスやファイルサービス、グループウェア等)の機能がサービスとして提供されるもの。

SLA(Service Level Agreement)

サービスレベル合意書。クラウド事業者と利用者との合意事項で、クラウド事業者は SLA に含まれるサービスレベル(稼働率や性能等)を満たすことを利用者に保証する。そのため SLA を満たせなかった場合は違約規程として返金規約等がある。

SLO(Service Level Objective)

サービスレベル目標。クラウド事業者が、合意した SLA を履行するために、稼働率、セキュリティ、サポートといった項目ごとに、パフォーマンスの目標値を設定したもの。クラウド事業者が設定する目標値のため SLO には違約規程がなく、SLO の内容について利用者に開示されない場合もある。

TLP(Traffic Light Protocol)

情報共有の促進を目的に作られた、適切な組織又は人に共有するための標示。情報共有の範囲を 4 色で示す。

TLP:RED	公開不可、関係者限定
TLP:AMBER	限定公開、関係者が所属する組織内で共有可能
TLP:GREEN	限定公開、コミュニティ内で共有可能
TLP:WHITE	制限なく共有可能

定型約款

「ある特定の者が不特定多数の者を相手方として行う取引で、その内容の全部又は一部が画一的であることが当事者双方にとって合理的なもの」を定型取引という。2020 年に施行された改正民法では、定型約款は「定型取引の契約内容とすることを目的に、特定の者によって準備された条項の総体」として定義されている(2020 年改正民法 548 条の 2 第 1 項柱書)。

執筆協力

本ガイダンス執筆協力一覧（五十音順：敬称略）

アマゾン ウェブ サービス ジャパン合同会社
株式会社エヌ・ティ・ティ・データ
グーグル・クラウド・ジャパン合同会社
クラスメソッド株式会社
グローバルセキュリティエキスパート株式会社
シスコシステムズ合同会社
株式会社セールスフォース・ジャパン
株式会社ディー・エヌ・エー
一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会
日本マイクロソフト株式会社
弁護士　北條　孝佳
楽天グループ株式会社
株式会社ラック
立命館大学 情報理工学部 情報理工学科　教授　上原　哲太郎

以上