「クラウドサービス提供における情報セキュリティ対策ガイドライン」の概要

総務省　サイバーセキュリティ統括官室 主査　佐々木（ささき）　弘和（ひろかず）

総務省では、安全・安心なクラウドサービスの利活用推進のため、平成26年（2014年）4月に、中小規模を含むすべてのクラウドサービス事業者において実施することが推奨される情報セキュリティ対策を取りまとめた「クラウドサービス提供における情報セキュリティ対策ガイドライン」を公表した。その後、クラウドサービスの提供・利用における環境の変化等を踏まえ、本ガイドラインの改定について検討を進め、令和3年（2021年）9月に同ガイドラインの最新版となる「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」を公表した*1。本稿では、同ガイドラインの概要について、ご紹介する。

1. 本ガイドライン作成の背景

クラウドサービスは、コスト面・運用効率性・拡張性などにおいて、オンプレミス環境と比較して様々な利点を有していることから、官民において急速に利活用が進んできており、社会経済活動を支える重要なICT基盤となっている。その一方で、クラウドサービスが関連するセキュリティに関する事案も多数報告されており、クラウドサービスを提供し、運用していく過程において、クラウドサービス自体のセキュリティを担保することが重要な課題となってきている。

また、クラウドサービスはその性質や提供形態から、オンプレミス環境では無かった新たなセキュリティ上のリスクを生じさせている。従来は、インフラまでも含めて、単独のクラウドサービス事業者がクラウドサービス利用者にサービスを提供する形態が一般的だった。しかし、現在ではインフラや実行環境などの基盤を提供するPaaS/IaaSと、アプリケーションサービスを中心にサービスを提供するSaaS等の様々なサービス提供形態があり*2、SaaS事業者が他者のPaaS/IaaSを基盤としてSaaSをクラウドサービス利用者に提供するなど、クラウドサービス事業者同士が連携してクラウドサービスを提供する事例が急増している。この提供形態の複雑化は、クラウドサービス事業者によるクラウドサービス全体の管理・統制を難しくする要因となっており、クラウドサービス事業者はこの状況を踏まえ、クラウドサービス事業者とクラウドサービス利用者との間における責任分担に関する考え方に基づき、双方の責任範囲を明確にした上で、自身の責任範囲においてクラウドサービスを安全・安心に提供するための情報セキュリティ対策を実施する必要がある。

本ガイドラインは、クラウドサービス事業者がクラウドサービスを提供する際の責任共有の考え方や、必要とされる情報セキュリティ対策等を整理して示すことにより、より安全・安心なクラウドサービスの利活用を推進することを目的とし、作成した。

2. 本ガイドラインの読者対象と活用方法

本ガイドラインは、民間事業者や行政機関などのあらゆる主体が利用するクラウドサービスに求められる情報セキュリティ対策を記載しており、その観点から本ガイドラインの読者対象としては、中小規模を含むSaaS/PaaS/IaaS等のすべてのクラウドサービス事業者を想定している。

クラウドサービス事業者は、取り扱うサービスの種類やデータなどを踏まえたリスク、自らの経営規模、利用でき

---

*1　「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」（案）に対する意見募集の結果及び「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」の公表
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html

*2　本ガイドラインにおけるIaaS/PaaS/SaaSの定義は以下のとおり。
IaaS：サービスの形で提供されるインフラストラクチャ。IaaS事業者は、演算機能、ストレージ、ネットワークほかの基礎的コンピューティングリソースを配置し、クラウドサービス利用者に提供する。
PaaS：サービスの形で提供されるプラットフォーム。PaaS事業者は、クラウドのインフラストラクチャ上で、アプリケーションを開発、実装、稼働できるようにするために、ミドルウェア等を提供する。
SaaS：サービスの形で提供されるソフトウェア。SaaS事業者は、クラウドのインフラストラクチャ上で稼働するアプリケーションをクラウドサービス利用者に提供する。

るリソース等を踏まえつつ、本ガイドラインを参照することで、自らが提供するクラウドサービスに適した情報セキュリティ対策を実施することが求められる。また、主な読者対象ではないが、クラウドサービス利用者においても、利用するクラウドサービスを選択する際の一定の指針や、利用するにあたって留意すべき情報セキュリティ対策の指針とすることが可能である。

3. ガイドラインの全体構成

本ガイドラインは、5つの章で構成されている。各章における記載内容は以下のとおりである。

Ⅰ. 序編

本ガイドラインの目的･位置付け･利用方法、クラウドサービス事業者とクラウドサービス利用者の責任範囲、本ガイドライン内で使用している用語の定義等を記載している。

Ⅱ. 共通編

SaaS事業者、PaaS事業者及びIaaS事業者に共通して求められる情報セキュリティ対策として組織的な取組み、情報資産の取扱い、契約や雇用における留意事項、開発や保守運用に係る対策等を取りまとめている。

Ⅲ. SaaS編

SaaS事業者に求められる情報セキュリティ対策を取りまとめている。

Ⅳ. PaaS/IaaS編

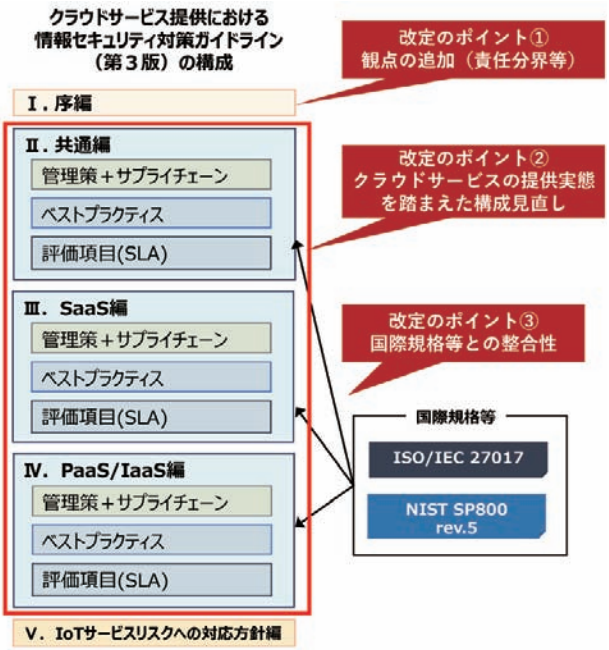
PaaS/IaaS事業者やデータセンタ等の情報処理施設に求められる情報セキュリティ対策を取りまとめている。

Ⅴ. IoTサービスリスクへの対応方針編

クラウドサービス事業者がIoTサービスを提供する場合を念頭に、IoTサービスリスクを詳しく解説するとともに、IoTサービスをモデル化するツールを提供し、これらのモデルに基づいて対処すべきリスクや分担すべき責任・役割を整理するための手順を取りまとめている。

本ガイドラインのメイン部分であるセキュリティ対策は、Ⅱ章からⅣ章にかけて、すべてのクラウドサービス事業者共通の対策、SaaS事業者に求められる対策、PaaS/IaaS事業者に求められる対策の3つに分類した上で記載しており、自身が提供するクラウドサービスの形態に応じて、読むべき箇所を明確化することで、より効率的に本ガイドラインを活用することが可能となる。

なお、第2版から第3版への改定においては、クラウドサービスを取り巻く環境の変化を踏まえ、全体構成の見直しやクラウドサービス提供における責任分界の在り方の追記、国際規格等との整合性を踏まえた情報セキュリティ対策の追加・修正を行った。



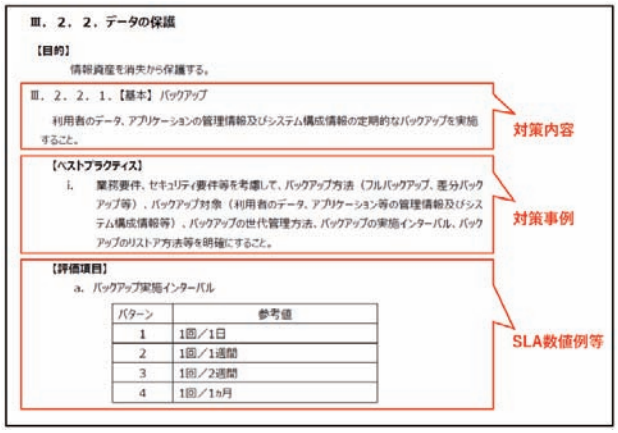
■図1. ガイドラインの章構成

4. 情報セキュリティ対策の例

Ⅱ章～Ⅳ章にかけて記載している情報セキュリティ対策の例を図2に示す。基本的な構成としては、「対策内容」を記載した上で、クラウドサービス事業者が対策を実施するに当たっての参考となるように、具体的な実施手法や注意すべき点を記載した「ベストプラクティス」を併記している。

また、対策を実施する際に、その実施レベルを定量的あるいは具体的に評価できる指標がある場合は、「評価項目」として参考となる指標を記載している。これらの指標は、SLA（Service Level Agreement）の合意事項として活用することも想定される。

これらの対策内容については、「基本」「推奨」の2段階で分類しており、自身のクラウドサービスに求められるセキュリティレベルに応じて、「基本」とされる対策だけを実施するのではなく、「推奨」とされる対策についても実施し



■図2. 情報セキュリティ対策の記載凡例

ていくことを検討する必要がある。参考までに、本ガイドラインにおける「基本」「推奨」の定義は以下のとおりである。

「基本」対策：クラウドサービスを提供するに当たり、基本的に実施することが求められる情報セキュリティ対策

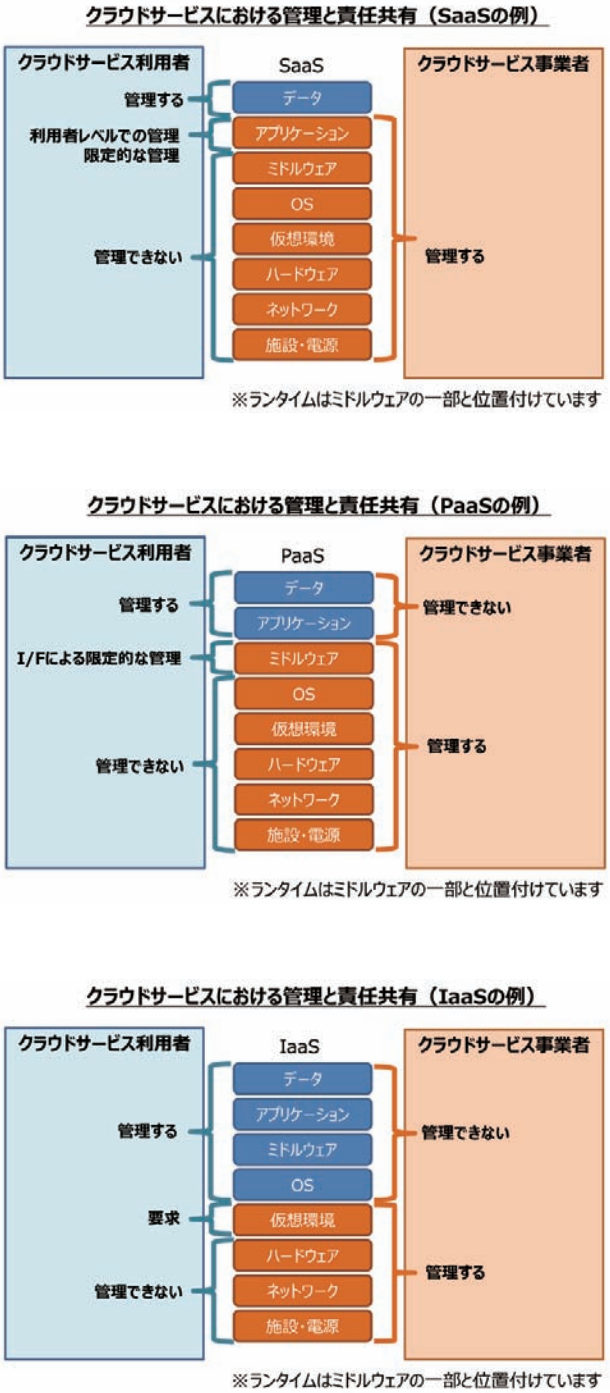
「推奨」対策：より高いセキュリティレベルが求められるクラウドサービスを提供するに当たり、「基本」対策に加えて付加的に実施することが望まれる情報セキュリティ対策

5. 本ガイドラインの特徴

本ガイドラインの特徴として、SaaS、PaaS、IaaSにおけるクラウドサービス利用者・クラウドサービス事業者間の責任分界の考え方や、複数のクラウドサービスを連携して利用者に提供する場合の責任分界の考え方について記載している。これらの責任分界を示したモデルは、一般に「責任共有モデル」(Shared Responsibility Model) と呼ぶが、この考え方はこれまでのオンプレミス環境でのシステムとは異なるものとなっており、この責任共有モデルについてクラウドサービス事業者及びクラウドサービス利用者の理解が不足していると、情報セキュリティ管理が不十分な箇所が生じ、情報漏洩などのセキュリティ事故が発生する可能性が高くなる。

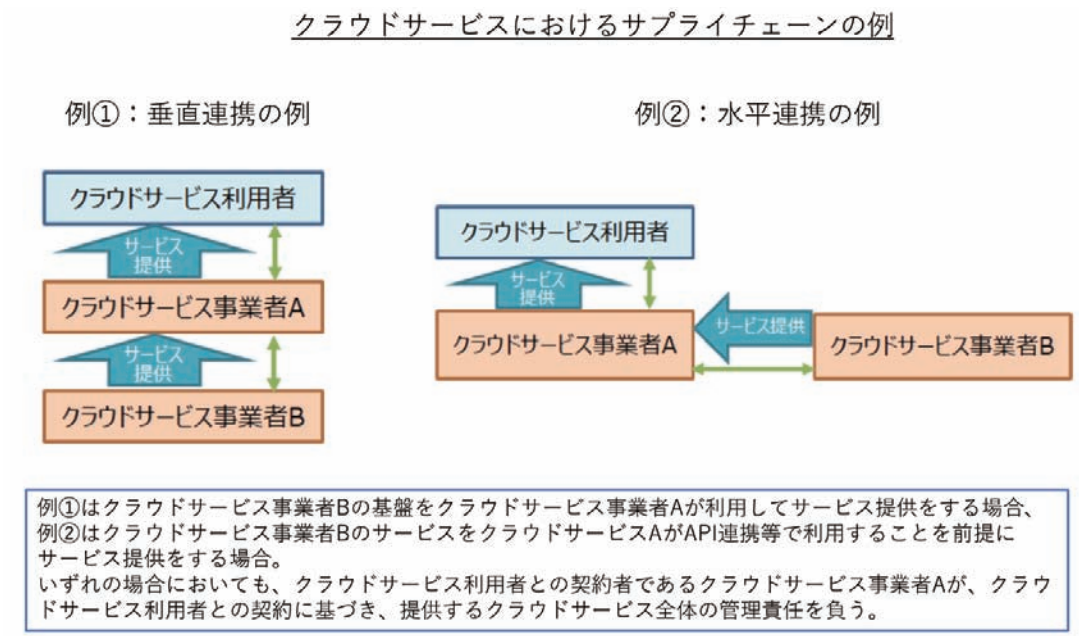
クラウドサービスにおいては、クラウドサービス事業者が管理する部分、クラウドサービス利用者が管理する部分の両方が存在しているが、双方における責任範囲・内容は一律に決まるものではないため、クラウドサービスの内容やクラウドサービス利用条件・環境ごとに、両者で責任範囲と内容について合意し、契約で明示することが重要となる。

また、昨今では多数のクラウドサービスが複合的に連携した上で、一つのクラウドサービスとして提供するケースが



■図3. クラウドサービスにおける管理と責任共有の例

増えており、そのケースにおける責任分界についてはクラウドサービス事業者として十分な留意が必要となる。本ガイドラインにおいては、その提供形態として典型的なパターンにおける責任分界の例を紹介している。



■図4.　クラウドサービス提供におけるサプライチェーンの例

6. おわりに

本稿では、クラウドサービス提供における情報セキュリティガイドラインの概要をご紹介したが、個別の対策内容等の詳細は、ガイドライン本文を参照いただきたい。総務省としては、本ガイドラインを活用し、中小規模を含むすべてのクラウドサービス事業者におけるセキュリティ対策を推進することにより、安全・安心なクラウドサービスの利活用推進に継続的に取り組んでいく。

他方、昨今ではクラウドサービス利用者において公開範囲設定を誤るなど適切にクラウドサービスを利用できていないことに起因し、結果的に情報流出のおそれに至る事案も発生している。このような事態が発生しないようにするためには、利用者における適切な設定の促進及び事業者における利用者に設定不備を起こさせないための取組みが重要となる。このため、総務省では、利用者におけるクラウドサービスの安全な利用の促進について、現在、事業者・利用者を含む幅広い主体で検討しており、今後、クラウドサービス事業者・利用者向けの適切な設定のための指針として示していくことを予定している。

ITUが注目しているホットトピックス

ITUのホームページでは、その時々のホットトピックスを“NEWS AND VIEWS”として掲載しています。まさに開催中の会合における合意事項、ITUが公開しているICT関連ツールキットの紹介等、旬なテーマを知ることができます。ぜひご覧ください。

https://www.itu.int/en/Pages/default.aspx