

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)

2021年 9月

総務省

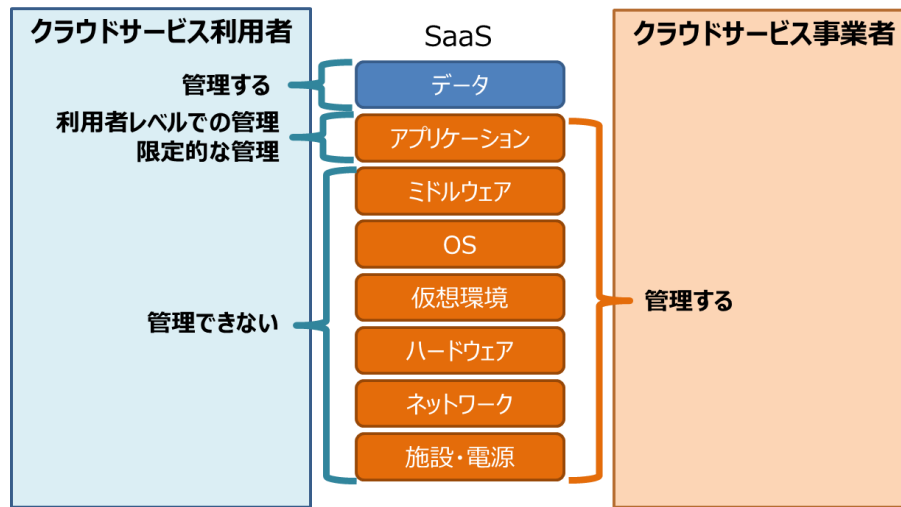
I. 6. クラウドサービス事業者とクラウドサービス利用者の責任

クラウドサービスは、組織外部での利用が前提であり、クラウドコンピューティング環境によって管理する内容も異なるため、従来のオンプレミス環境での情報セキュリティ対策に加え、クラウドコンピューティング環境特有の情報セキュリティ対策が必要となる。しかしながら、クラウドサービスを利用するにあたってのリスクに対する認識度合いによっては、機能の追加や改修などのバージョンアップ等の頻度が多いクラウドサービス特有のリスクへの対応が疎かになり、情報セキュリティ管理が不十分になりがちである。クラウドサービスのセキュリティに関する設定が十分でなかったために、意図せず、クラウドサービスで管理している機密情報を無認証状態で外部に公開してしまい、機密情報を漏洩させてしまった事例が相次いで報告されている。

クラウドサービスは市場で普及してからの歴史が長く、技術も成熟化しつつあるにもかかわらず、セキュリティインシデントが多発している要因の一つとして、クラウドサービス利用者が対応すべき情報セキュリティ対策が曖昧になっていることが挙げられる。例えば、クラウドサービス事業者は、クラウドサービスで管理する情報資産を外部からアクセスするための権限設定機能を提供し、クラウドサービス利用者は、外部からアクセスを許可するかの判断を行い、そのための権限を設定する。クラウドサービスの情報セキュリティを高めるためには、クラウドサービス事業者とクラウドサービス利用者が協力して、クラウドサービスに対する責任を共有する必要がある。この責任を共有するという考え方(責任共有モデル)を多くのクラウドサービス事業者が採用している。ただし、責任共有モデルにおける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・内容は一律に決まるものではなく、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、両方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である。また、双方の責任範囲において、クラウドサービス利用者がセキュリティ上のリスクを判断できるように、クラウドサービス事業者はクラウドサービス利用者に対して、クラウドサービスの内容やクラウドサービス利用条件・環境等について適切に情報提供をする必要がある。

本ガイドラインでは、この責任共有モデルを採用し、各クラウドサービスモデル(SaaS/PaaS/IaaS)における責任分担の一般的な考え方を示す。この責任分担は、クラウドサービスの実装方式(パブリッククラウド、プライベートクラウド等)には依存しない。

I. 6. 1. SaaS における管理と責任共有



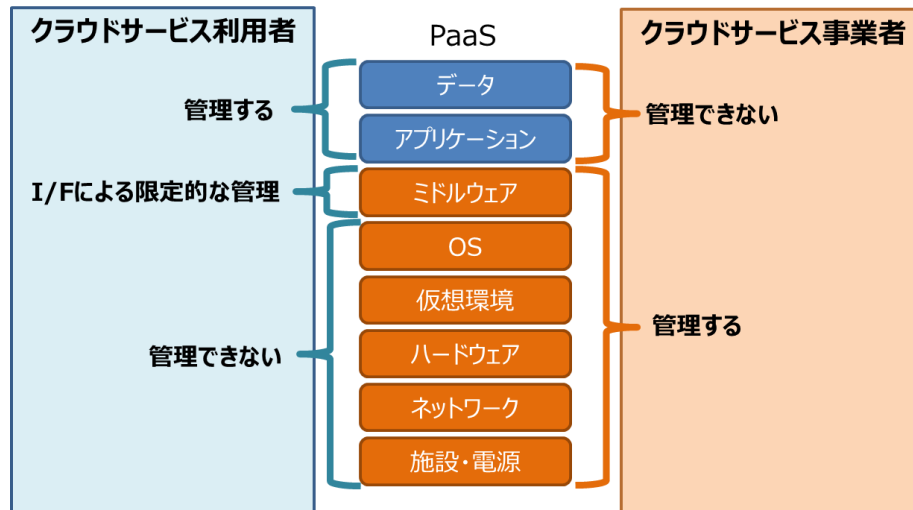
※ランタイムはミドルウェアの一部と位置付けています

SaaS を利用するクラウドサービス利用者は、クラウドサービス事業者が提供するアプリケーションを利用するためのデータやアプリケーション上で生成したデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。アカウント管理などの限定的な管理権限をクラウドサービス事業者から付与され、外部からのアクセス権限を設定する場合がある。

（注）アプリケーションのバージョンアップや機能の追加により、設定が不適切なものとなってしまう、情報漏洩に至ることが想定されるため、クラウドサービス事業者は、クラウドサービス利用者がバージョンアップによる情報セキュリティへの影響を見定めることができるよう、適切な情報提供を行う必要がある。

クラウドサービス事業者は、契約・SLA に基づくサービスをクラウドサービス利用者に提供するために、アプリケーション層以下の実装、設定、更新及び運用を管理するとともに、クラウドサービス利用者に限定的な管理権限等を提供する場合がある。

I . 6. 2. PaaS における管理と責任共有



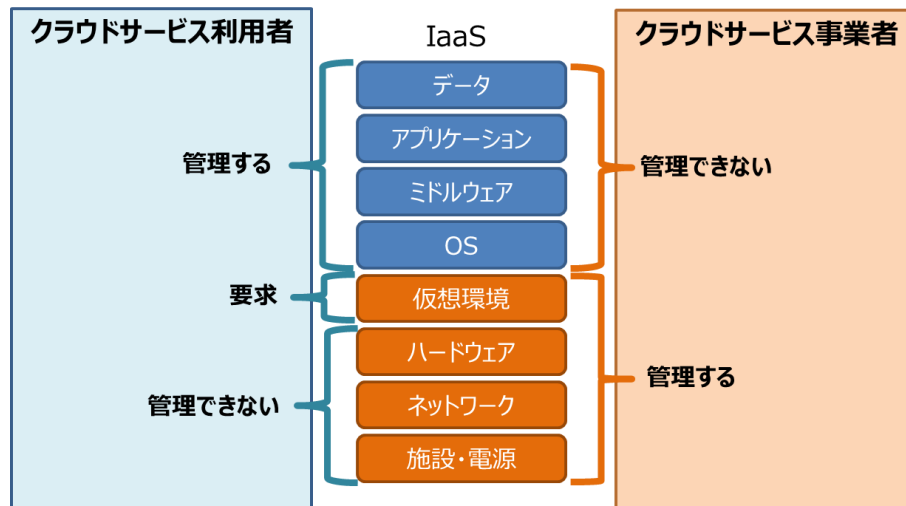
※ランタイムはミドルウェアの一部と位置付けています

PaaSを利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLAに基づいて、アプリケーションの開発、アプリケーションに対する管理を行う。クラウドサービス利用者は、クラウドサービス事業者が提供するプログラミング環境やSQL⁷等のユーティリティインターフェースを利用してミドルウェア層を利用する。また、クラウドサービス利用者は、クラウドサービス事業者が提供するセキュリティ機能（データバックアップ機能、認証機能、データ暗号化機能、ファイアウォール機能、ログ管理機能等）を正しく理解して設定する必要がある。

クラウドサービス事業者は、ミドルウェア層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

⁷ SQL(Structured Query Language)はミドルウェア層にあるデータベースを操作するための言語。データベースにデータを検索、挿入、更新、削除等する際に利用する。

I . 6. 3. IaaS における管理と責任共有



※ランタイムはミドルウェアの一部と位置付けています

IaaS を利用するクラウドサービス利用者は、クラウドサービス事業者との契約・SLA に基づき、ゲスト OS⁸等が動作するための仮想環境の構築と管理をクラウドサービス事業者に要求できる。クラウドサービス利用者は、仮想環境上で動作している OS を含めたすべてのソフトウェアの管理を行う。OS やミドルウェア層での障害対応や、ミドルウェアに対するパッチ適応やぜい弱性対応などは、クラウドサービス利用者の責任となる。

クラウドサービス事業者は、仮想環境層以下の実装、設定、更新及び運用を管理するとともに、データセンター内のネットワークインフラも管理する。

⁸ 一つの物理コンピュータ上で別のコンピュータをエミュレートする仮想環境において、仮想環境で動いている OS のこと。物理コンピュータ上で動いている OS はホスト OS と称す。例えば、Windows 上で Mac を動かす場合、ホスト OS が Windows、Mac がゲスト OS となる。ゲスト OS を動かすためには、必要な環境設定をホスト OS に施す必要がある。