# 情報システムに係る政府調達における
# セキュリティ要件策定マニュアル

## 別冊．クラウド設計・開発編

2022 年 7 月 29 日

内閣官房 内閣サイバーセキュリティセンター

目次

# 1章　マニュアルの概要

この章では、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル別冊. クラウド設計・開発編」（以下「本書」という。）を作成した背景、その目的・位置づけ及び活用範囲について述べる。

## 1.1　背景

急速に進化し発展したクラウドサービスは、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きく、政府情報システムにおいても、クラウドサービスを利用することで様々な課題が解決されることが期待されている。

国内では、「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（平成 29 年５月 30 日閣議決定）及び「デジタル・ガバメント推進方針」（平成 29 年５月 30 日高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議決定）で、クラウド・バイ・デフォルト原則、すなわち、政府情報システムを整備する際に、クラウドサービスの利用を第一候補とすることとし、「デジタル・ガバメント実行計画」（平成 30 年１月 16 日 e ガバメント閣僚会議決定）において、「政府情報システムにおけるクラウド・バイ・デフォルトの基本的な考え方、各種クラウド（パブリッククラウド、プライベートクラウド等）の特徴、クラウド利用における留意点等を整理する」こととされたほか、平成 30 年６月７日には、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」が各府省情報化統括責任者（CIO）連絡会議で決定された。

このような流れを受けて、令和元年９月に改定された、政府情報システムにおけるセキュリティ要件を示す「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（以下「SBD マニュアル」という。）に加えて、政府情報システムにクラウドサービスを利用するケースを想定した場合のセキュリティに関する議論が進められてきた。

## 1.2　目的

クラウドサービスを利用して政府情報システムを構築する際、オンプレミスで構築する情報システムとは構成や責任範囲等異なる点が多いことから、本書ではクラウドサービスの特徴に着目したセキュリティ観点の注意事項を整理し、クラウドサービスにおいて設定すべき基本的なセキュリティ対策の項目や実装の指針を示している。これにより、クラウドサービスを利用して情報システムの構築を行う政府機関等の情報システム担当者のクラウドサービスに対する理解のベースラインを引き上げるとともに、クラウドサービスを利用して情報システムを構築する際に必要となるセキュリティ対策の確認や受入テスト時等の確認項目として本書を活用することで、政府機関等におけるクラウド活用の企画・設計段階からのセキュリティ確保を支援することを目的としている。

## 1.3 位置づけ

本書は、SBD マニュアルの別冊として位置付ける。

SBD マニュアルは、政府が調達する情報システムに対して求めるべき必要なセキュリティ要件を調達仕様書に盛り込むことで、その後の設計・開発等において本来必要な要件の抜け漏れを防止することを目的としている。したがって、セキュリティ要件について、個別の設定項目等を示すものではない。

他方、本書においては、SBD マニュアルで定めたセキュリティ要件に則り、クラウドサービスの基本的設定項目等を示すことで、設計・開発時のセキュリティ対策の実装を支援することを目的としている。なお、本書では、クラウドサービスの設計・開発時における基本的なセキュリティ対策に焦点をあてており、運用・保守時のセキュリティ対策については本書の対象としていないため、別途検討する必要がある。

下図に、SBD マニュアルと本書のそれぞれの位置づけを示す。

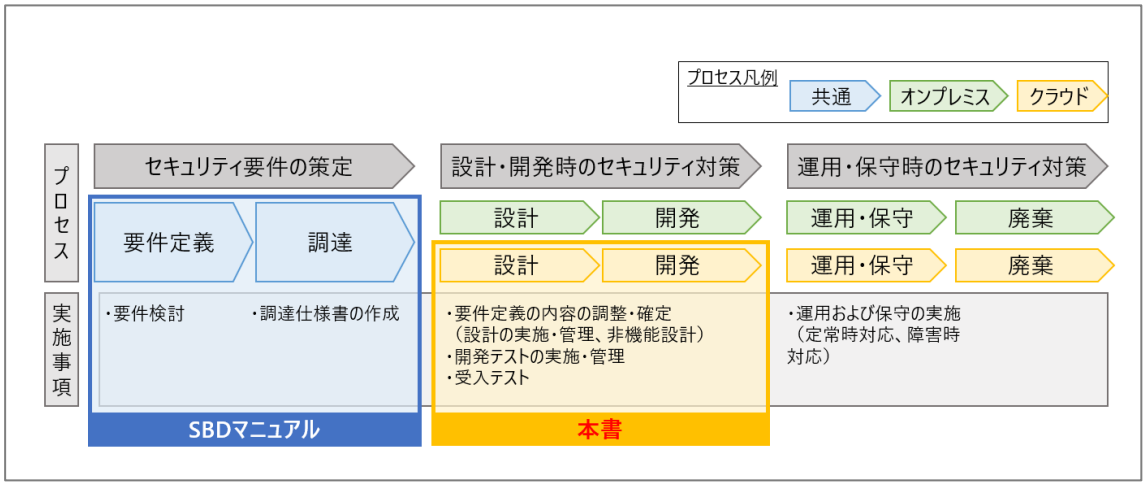



**図 1　本書の位置づけ**

## 1.4 想定読者

本書の想定読者は、クラウドサービスを利用した情報システムの構築に関わる機関等の担当者（以下「機関等の担当者」という。）及びクラウドサービスを利用した情報システムの構築を受託している事業者（以下「受託者」という。）である。なお、上述の通り、本書ではクラウドサービスの設計・開発時における基本的なセキュリティ対策に焦点をあてており、運用・保守時のセキュリティ対策については本書の対象としていないが、クラウドサービスの運用・保守のみを担当する機関等の担当者や事業者についても本書を参考とされたい。

## 1.5 活用範囲

比較的大規模な政府情報システムの構築にクラウドサービスを活用する場合は、クラウドサービスに精通している専門家が当該システムの構築に参画することが想定される。一方で、中小規模の政府情報システムにおいてクラウドサービスを活用する場合は、このような専門家の参画が困難となることが想定される。

本書が想定する情報システムは、クラウドサービスに精通した専門家が当該システムの構築に参画することが難しく、機関等の担当者や受託者が中心となって構築することが想定される中小規模の政府情報システムである。ただし、大規模な政府情報システムを構築する際にも本書を参照することで適切なセキュリティ対策を実施可能な場合があると考えられる。そのため、システムの規模を問わず、必要に応じて本書を参考とされたい。

なお、特に大規模な政府情報システムを構築する際は、セキュリティ対策の抜け漏れや設定ミス等を防ぐため本書で記載する対策を個別に実装するのではなく、共通化可能な範囲でセキュリティ確保のための初期設定を実装しておくことが重要である。

## 1.6 本書の全体構成

本書は全７章で構成されている。

各章の主な記載内容とそのねらいについては以下の通りである。

１章 マニュアルの概要

本書の目的・位置付け・想定読者等を記載している。本書の目的等の前提について把握することで、以降の内容の理解を助ける。

２章 本書の利用方法

本書の利用タイミングや具体的な利用方法を記載している。また、本書が対象としているクラウドサービスの概要や設定項目に関する考え方等についても記載している。

３章 クラウドサービスの概要とセキュリティ脅威

一般的なクラウドサービスの概要や、オンプレミスの違い及びクラウドサービス利用時におけるセキュリティに関する脅威を記載している。

クラウドサービスを利用する上で理解しておくべき基本的な事項としてクラウドサービスの特徴やクラウドサービス特有のセキュリティ脅威を把握することで、４章において記載するセキュリティ対策の目的や必要性の理解が容易になると考えられる。

４章 クラウドサービスにおいて設定すべきセキュリティ対策

クラウドサービスにおいて設定すべきセキュリティ対策について、クラウドサービスの形態ごとに整理し記載している。各セキュリティ対策について、セキュリティ対策の内容やセキュリティ対策を実施しない場合のリスクを示すとともに、具体的な設定値の参考となるよう、米国の政府機関・企業等が協力して設立された非営利団体 CIS（Center for Internet Security）が発行するセキュリティ対策のベストプラクティスである、CIS Benchmarks[1]において関連する項番を示している。CIS Benchmarks は、クラウドサービスをはじめ、ネットワーク機器やデータベース、OS 等の製品ごとに、セキュリティに関して望ましいと考えられる設定項目を記載している一連の文書群である。

機関等の担当者が設計書に適切なセキュリティ対策が含まれているかを確認する際に本章を参照することで、CIS Benchmarks のカテゴリを参考にした基本的な設定項目が当該設計書に含まれているか、その必要性も含め確認できる。また、受託者が作成したテスト計画やテスト項目に適切なセキュリティ対策が含まれているかを機関等の担当者が確認する際に調達仕様書とあわせて本章を参照することで、当該テスト項目におけるセキュリティ対策の抜け漏れ等の確認を行うことができ、システムの受け入れを検討できる。

５章 クラウドサービスの事故事例

クラウドサービスのセキュリティ対策に関する理解を深めるため、近年増加しているクラウドサービスの事故について、代表的な事例の概要を解説している。また、これら事例の原因等に鑑みて、４章で記載したセキュリティ対策を実施することで、当該事例における脅威をどのように防止・軽減できるかについても記載している。機関等の担当者は本章を参考に、４章に記載のある対策がセキュリティ事故を防止するためにどのように有効となるかを確認し、セキュリティ対策の必要性を十分に理解することが重要である。

６章 用語定義

本書において使用している用語の定義を記載している。なお、「４章 クラウドサービスにおいて設定すべきセキュリティ対策」記載の各項目を理解する上で特に必要となる用語の定義は、４章冒頭部分に記載している。

７章 参考資料

本書の参考となる資料について記載している。当該資料について本書とあわせて参照し、クラウドサービス利用に関するセキュリティ対策について検討することが望ましい。

[1] 参考：CIS Benchmarks
https://www.cisecurity.org/cis-benchmarks/

# 2章　本書の利用方法

この章では、本書の利用タイミング、及び本書の使い方について述べる。

## 2.1　本書の利用タイミング

本書の利用タイミングは、クラウドサービスを利用した政府情報システムの設計・開発時を想定している。具体的には、政府機関等における情報システムの調達プロセスにおいて、クラウドサービスを利用した情報システムの構築に係る受託者の決定後、調達仕様書に記載されるセキュリティ要件に基づき、受託者が設計書を策定する以降のタイミング（受入テスト時含む）で利用されることを想定している。

なお、クラウドサービスを既に利用している情報システムにおいても、定期的なセキュリティ設定の確認を実施する際に、本書を活用することも可能である。

## 2.2　本書の使い方

本書は、クラウドサービスにおける基本的なセキュリティ対策の理解を助けるとともに、設計・開発時に機関等の担当者が参照するセキュリティ項目や、受入テストの確認項目を提供している。

また、クラウドサービスを利用中は設定の誤りを防止するための対策として、定期的にセキュリティ設定の確認が必要となるが、本書を活用することも考えられる。

具体的な使い方の例は以下の通りである。

なお、本書に記載のウェブサイトのアドレスは、令和４年３月時点のものであり、今後、廃止又は変更される可能性があるため、最新のアドレスを確認した上で利用すること。

（１）　受託者が作成する設計書に適切なセキュリティ対策が含まれているかを確認するための利用

クラウドサービスを利用した情報システムの構築を行う受託者が決定した後、当該受託者は仕様書に基づいて設計書を作成することとなる。その際、機関等の担当者は、当該設計書に適切にセキュリティ対策が含まれているかを確認することが重要である。

本書の４章を参照することで、クラウドサービスの基本的なセキュリティ対策を、その設定方法とともに把握することが可能となる。これにより機関等の担当者は、受託者が作成した設計書に、実施すべきクラウドサービスの基本的なセキュリティ対策が含まれているかを確認することができる。

（２）　受入テストの項目に考慮すべきセキュリティの観点が含まれているかを確認するための利用

受託者はクラウドサービスを利用した情報システムを構築する際、設計書に基づきテスト計画を作成する。その際、機関等の担当者は受託者が作成したテスト計画に含まれるテスト項目の内容を確認し、セキュリティ確保のための設定に関する内容が当該項目に正しく含まれているかを確認することが重要である。

調達仕様書と共に本書の４章を参照することで、受託者が作成したテスト計画やテスト項目に必要なセキュリティ対策に関する項目が正しく含まれているかを確認することができる。

（３） クラウドサービス利用中における定期的なセキュリティ設定の確認に利用

クラウドサービスを利用した情報システムにおいては、サービス仕様の変更や構成変更等によりセキュリティ対策の設定内容等に変更が生じる可能性があるため、定期的にセキュリティ対策の見直しが必要である。

本書の 4 章を参照することで、クラウドサービスにおける基本的なセキュリティ対策を把握することが可能となり、機関等の担当者は、定期的に確認すべきセキュリティ対策の項目について本書を活用し検討することが可能となる。

本書の利用方法の例について、下図に示す。

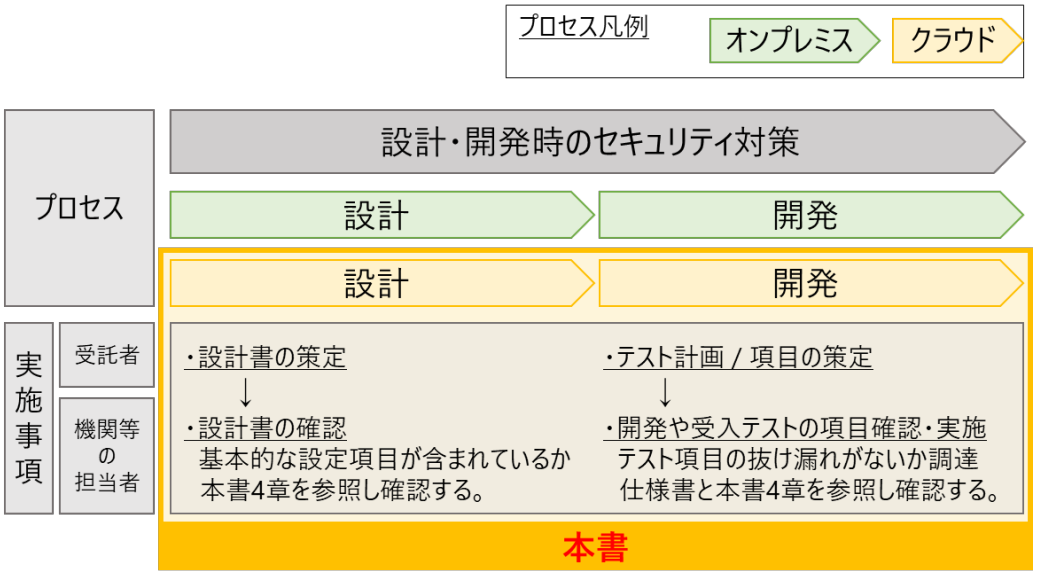



**図 2　設計・開発プロセスにおける本書の利用方法例**

## 2.3 本書が対象とするクラウドサービス

（１） 対象とするクラウドサービス

本書では、ISMAP クラウドサービスリスト への登録状況等や CIS Benchmarks の発行状況

等を踏まえ、以下の５つのクラウドサービスについて取り上げている（表１参照）。また、本書は対象とするクラウドサービスの利用を強制するものではなく、いずれのクラウドサービスを利用する場合であっても共通して適用することが可能なセキュリティ対策を中心に記載している。そのため、他のクラウドサービスを用いて政府情報システムを構築する場合であっても、本書の考え方を活用することができる。

**表 1　本書が対象とするクラウドサービス**

| | クラウドサービス名 | クラウドサービス事業者 | クラウドサービス形態 | ISMAP クラウドサービスリストにおける登録番号 |
|---|---|---|---|---|
| 1 | Amazon Web Services（AWS） | Amazon Web Services, Inc. | PaaS/IaaS | C21-0008-2 |
| 2 | Google Cloud Platform（GCP） | Google LLC | PaaS/IaaS | C21-0004-2 |
| 3 | Microsoft Azure（Azure） | 日本マイクロソフト株式会社 | PaaS/IaaS | C21-0012-2 |
| 4 | Google Workspace | Google LLC | SaaS | C21-0005-2 |
| 5 | Microsoft 365 | 日本マイクロソフト株式会社 | SaaS | C21-0013-2 |

（２） 対象とするクラウドサービスの利用形態

本書が対象とするクラウドサービスは、「SaaS」、「PaaS」、あるいは「IaaS」の形態をとるものである。

SaaS は「サース」と呼び、インターネット経由でソフトウェアを提供するクラウドサービスの形態である。SaaS は、業務等で利用する様々なアプリケーションを利用者に提供する。当該アプリケーションが稼働しているサーバ、ミドルウェア、ネットワーク設備等の IT インフラストラクチャを含む多くの部分はクラウドサービス事業者の管理対象となる。そのため、利用者はソフトウェア等をインストールする必要がなく、手軽に利用できるとともに、常に最新のバージョンを使えるメリットがある。

PaaS は「パース」と呼び、インターネット経由でプラットフォームを提供するクラウドサービスの形態である。PaaS は主にデータベースや開発フレームワーク等のミドルウェアや OS を提供する。利用者はアプリケーションを開発、配備、実行するためのプラットフォームを利用することができる。PaaS を用いることで、自組織でプラットフォームを準備するコストを抑え、手軽に開発環境を用意することができる。

IaaS は「アイアース／イアース」と呼び、インターネット経由でコンピューティングリソースを提供する等クラウドサービスの形態である。IaaS は、サーバ、ストレージ、仮想化基盤であるハイパーバイザ等の環境を利用者に提供する。また、クラウドサービス事業者の責任において、これらの機器を稼働させるためのネットワーク設備や電源設備等の IT インフラストラクチャの整備を実施している。

### （3） セキュリティ対策の分類に関する考え方

本書の４章では、クラウドサービスの形態ごとに、基本的なセキュリティ対策を記載している。その際、4.1 では PaaS/IaaS において設定すべきセキュリティ対策を記載し、4.2 では SaaS において設定すべきセキュリティ対策をそれぞれ記載している。

このように PaaS/IaaS を対象にする対策と SaaS を対象にする対策を分けて記載するのは、PaaS/IaaS と SaaS とでは、具体的な各クラウドサービスにおける機能等の差異の大小が異なると考えられるからである。つまり、本書が対象とする PaaS/IaaS では利用するクラウドサービスが異なっていても提供しているサービスの大要は大きく異ならない（いずれのクラウドサービスにおいても ID 及びアクセス管理等の共通の機能は提供される）。一方、SaaS では、提供するサービスの内容によって設定すべき事項が大きく異なると考えられる。

以上の理由から、本書の 4.1 では PaaS/IaaS において CIS Benchmarks のカテゴリを参考にした基本的な設定すべきセキュリティ対策を、個別のサービスに依らず、以下の６つの機能分類の観点から記載している。

- ID およびアクセス管理
- ログの記録と監視
- ネットワーク
- 仮想マシン
- ストレージ
- データベース

また、本書の 4.2 では、SaaS において設定すべきセキュリティ対策を、本書が対象とする SaaS ごとに記載している。

また、本書では、PaaS/IaaS 向けの対策、SaaS 向けの対策ともに、クラウドサービスを利

用する上での基本的なセキュリティ対策を、一定の機能分類に基づき記載しているが、一般にクラウドサービスのセキュリティを考える場合、機能面での対策以外にも、ガバナンス面、マネジメント面、データ保護や脆弱性およびインシデント管理など、種々の観点を考慮する必要がある。この点については本書ではなく、CSA 発行の CCM（Cloud Control Matrix）なども参照されたい[2]。また、近年、IaaS や SaaS、PaaS といった類型では分類が難しい様々な XaaS も増えており、上記で取り挙げたもの以外に特徴的な機能（例えば機械学習に関する機能やコンテナ管理機能を提供するもの）を持つものもある。このようなサービスについてはクラウドサービス事業者の公式ドキュメントや、公式で案内されるセキュリティに関するベストプラクティスを参照し、セキュリティ対策を検討・実装していくことが望ましい。

### （4） 設定項目に関する考え方

先述の通り、本書の 4 章ではクラウドサービスにおける基本的なセキュリティ対策として実施されるべきものを記載しているため、すべてのセキュリティ対策における設定項目を網羅するものではない。

なお、各対策を実施するための設定項目の内容は CIS Benchmarks の Level1[3]に相当する内容となっており、より高度なセキュリティ対策が求められる場合は、クラウドサービスおよび構築対象の情報システムのセキュリティ脅威を踏まえたリスク評価を行った上で必要なセキュリティ対策を検討する必要がある。また、合わせて CIS Benchmarks の Level2 やクラウドサービス事業者等が公開している公式ドキュメント等を参考とすると良い。

本書で参照している各クラウドサービスの CIS Benchmarks のバージョンについては以下の通りであるが、CIS Benchmarks は新たなセキュリティ脅威に対応するため、常に更新されている。したがって、本書を参考すると共に最新の CIS Benchmarks もあわせて確認する必要がある。

- Amazon Web Services
  CIS Amazon Web Services Foundations Benchmark v1.4.0 - 05-28-2021
- Google Cloud Platform
  CIS Google Cloud Platform Foundation Benchmark v1.2.0 - 05-01-2021
- Microsoft Azure
  CIS Microsoft Azure Foundations Benchmark v1.3.1 - 07-21-2021
- Google Workspace
  CIS Google Workspace Foundations Benchmark v1.0.0 - 01-29-2021
- Microsoft 365

[2] 参考：CCA ジャパン「CCM V4.0.2 日本語版（2021/08/20）」
https://www.cloudsecurityalliance.jp/site/?page_id=2048

[3] CIS Benchmarks に記載されている各設定項目のほとんどは Level 1 あるいは Level 2 のいずれかに分類される（一部の特定項目については、その他に分類される）。Level 1 は基本的なセキュリティ要件を指し、Level 2 は追加のコスト等を要する可能性がある発展的なセキュリティ要件を指すとされる。

CIS Microsoft 365 Foundations Benchmark v1.3.0 - 06-02-2021

CIS Benchmarks は本書が対象とする５つのクラウドサービス以外についても広く対象としてベストプラクティスをまとめているため、政府情報システムの構築において、本書が対象とするクラウドサービス以外を利用する場合は、各クラウドサービスに対応する CIS Benchmarks を参照するのが望ましい。

（５） その他留意事項

「1.3 位置づけ」にて記載の通り、本書は設計・開発時の基本的なセキュリティ対策の実装を支援することを目的としている。そのため、本書では、可用性が損なわれないための対策等は記載しているが、障害等発生時の自動復旧に関する設計の考え方やオートスケーリング等をはじめとする高可用性設計を必要とする設計技法を考慮した記載はしていない。また、運用時における変更管理に関する考え方等も記載の対象としていない。このような高可用性を考慮した設計技法や運用・保守時に必要となるセキュリティ対策については、可能な限り設計・開発段階から実装することが望ましいため、クラウドサービス事業者が提供する公式ドキュメント等を参考に検討すること。更に、クラウドサービスを利用する際は、運用・保守時の対策についても別途検討を行うことが重要である[4]。

また、クラウドサービスを提供する際には、初期設定で利用する場合に最もセキュリティが高くなるように設計することや利用者のセッション管理としてログアウトを行った時点でセッション識別子を無効にしたり、セッション識別子はランダムな識別子を生成するようにしたり、一定時間経過後にセッションを遮断したりする等の観点を取り入れる等の検討が望ましい[5]。

なお、クラウドサービスを利用する際はクラウドサービス事業者が提供するサービスの利用規約や利用に当たっての注意事項等を事前に公式ドキュメント等を参考に確認をすることも重要となる[6]。

[4] 参考：内閣サイバーセキュリティセンター「クラウドを利用したシステム運用に関するガイダンス」（令和３年 11 月 30 日）
https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html

[5] 参考：総務省「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」
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html

[6] 参考：内閣サイバーセキュリティセンター「クラウドを利用したシステム運用に関するガイダンス(別紙)」
https://www.nisc.go.jp/policy/group/infra/cloud_guidance_attach.html

# 3章　クラウドサービスの概要とセキュリティ脅威

この章では、クラウドサービスの概要やそのセキュリティに関する特徴とともに、クラウドサービスが有するセキュリティに関する脅威について述べる。また、クラウドサービスを利用するにあたり責任共有モデルにて示される責任分界の観点から利用者の責任について述べる。

## 3.1　クラウドサービスの特徴

クラウドサービスは、使用するコンピューティングリソースがインターネット経由で提供され、セキュリティ対策においても、従来のオンプレミスの情報システムにはなかったクラウドサービス独自の特徴がある。そのため、クラウドサービスを用いた情報システムを構築する際には、これらの特徴に留意することが重要である。ここでは、このようなクラウドサービスにおけるセキュリティに関する特徴を踏まえて重要となる観点について解説する。

組織の内外をつなぐ通信経路の増加

オンプレミスによって構築される情報システムでは、組織内から組織外への通信経路は少数の箇所に限定することが一般的である。そのため、外部からのセキュリティ脅威を意識する上では、組織内と組織外をつなぐ少数の箇所についてセキュリティ対策を考えることで、セキュリティレベルを向上させることができる。

一方、クラウドサービスを利用した情報システムは、各クラウドサービス事業者が提供する様々な種類のサービスから構成されることが多く、組織内と組織外をつなぐ通信経路が多数存在する。そのため、オンプレミスの場合と比較すると、外部からのセキュリティ脅威を考慮して対策を実施しなければならない箇所が多くなり、セキュリティ対策の管理も複雑化することとなる。その結果、対策を実施すべき箇所の見落としがないかを、より厳格に確認することや、利用している各サービスに対応した適切な対策の実施を検討することが重要となる。

機器等の物理的な制御や保護を行う機会の減少

オンプレミスによって構築される情報システムでは、情報システムの管理者がサーバ装置やネットワーク機器等を物理的に管理することが可能であるため、それらの機器等が設置されている場所へ直接赴き、システムを管理するためのアクセスや、媒体の保護を実施することができる。

一方で、クラウドサービスにおいては、クラウドサービス事業者の責任においてサーバ装置やネットワーク機器等の物理的な管理が実施される。また、利用者はこれらの機器等の物理的な位置を把握していないことも多く、機器等の物理的な制御や保護には基本的に関与しない。クラウドサービス事業者は例えば、機器等が設置されている施設への入館制限や、老朽化した機器等の交換等を実施することになるが、利用者からはこれらの実施を直接確認す

ることができないことが多い。そのため、当該クラウドサービス事業者に対する第三者認証や内部統制保証報告書等により、適切なセキュリティ対策の実施を確認することが重要となる。

また、クラウドサービス事業者が管理するサーバ装置等の機器は、日本国内に設置されているとは限らず、リージョンやゾーンで分けて世界中に分散している可能性がある。その際、クラウドサービスで取り扱うデータが法制度や実施体制が十分でない、法の執行が不透明である、権力が独裁的である、国際的な取決めを遵守しないなどのリスクの高い国に保存される可能性があり、データセンター内のデータが外国の法執行機関の命令により強制的に開示される、データセンターの他の利用者等が原因でサーバ装置等の機器が機関等のデータを含んだまま没収されるなどのリスクが存在する。そのため、クラウドサービスを利用する際に選択できるリージョンやゾーンを制限することや利用者が管理する暗号鍵を用いてデータを暗号化するなどの対策も重要である。

セキュリティに関する設定見直しタイミングの増加

オンプレミスで構築した情報システムにおける、セキュリティに関する設定の見直しのタイミングは、一般的にシステムの改修や更改を実施する場合に多く見られる。

一方、クラウドサービスを利用した情報システムでは、クラウドサービス事業者が主導する形で自らの提供するサービスに関する仕様変更や機能追加を行うことがあり、これらがクラウドサービスの利用者のセキュリティに関する設定に影響を与える可能性がある。

そのため、クラウドサービスの利用者は、自らが利用するサービスについて最新の情報を収集し、仕様変更や機能追加が発生する場合は、関連する情報システムのセキュリティに関する設定や業務内容等への影響の有無等を確認することが重要である。

## 3.2 クラウドサービス形態ごとの責任共有モデル

クラウドサービスには様々の形態が存在するが、2.3(2)に記載の通り、本書では「SaaS」、「PaaS」、「IaaS」の３つの代表的な形態を対象とする。

クラウドサービスでは、クラウドサービスの利用者とクラウドサービスを提供する事業者のそれぞれがクラウドサービスを運用する上での責任を共有するという、「責任共有モデル（Shared Responsibility Model)」の考え方が採用されるのが一般的である。

責任共有モデルにおける、利用者あるいはクラウドサービス事業者それぞれの責任範囲は、クラウドサービスの形態に応じて異なるものの、クラウドサービスの利用者がクラウドサービスで取り扱うデータそのものや、クラウドサービスへアクセスするデバイスのセキュリティに関する設定等については、いずれのクラウドサービスの形態においても、利用者側の責任範囲であると考えられる。また、クラウドサービスで提供される各種サービスの設定を適切に実施する責任はクラウドサービスの利用者側が有することに留意が必要である。

各クラウドサービスの形態における責任共有の考え方は以下の通りである。

SaaS では、アプリケーション、ミドルウェア、OS、当該クラウドサービスが稼働しているサーバの仮想化ソフトウェアやハードウェア等の管理について、クラウドサービス事業者が責任を持つとされる。

PaaS では、ミドルウェア、OS、当該クラウドサービスが稼働しているサーバの仮想化ソフトウェアやハードウェア等の管理はクラウドサービス事業者側の責任であり、PaaS で提供されているミドルウェア等を利用して構築したアプリケーションの管理はクラウドサービスの利用者側の責任であるとされる。

IaaS では、クラウドサービスが稼働しているサーバの仮想化ソフトウェアやハードウェア等の管理はクラウドサービス事業者側の責任であり、IaaS で提供されるこれらのリソースを利用して構築したアプリケーション、ミドルウェア、OS 等の管理はクラウドサービスの利用者側の責任であるとされる。

なお、オンプレミスにおいては、アプリケーション、ミドルウェア、OS、情報システムが稼働しているサーバの仮想化ソフトウェアやハードウェア等の全ての管理を情報システムの管理者が責任を持って実施することとなる。

以上のようなクラウドサービスの形態ごとの責任共有のあり方を下図に示す。なお、ここでは基本的な責任共有モデルのあり方に関する例を示しているが、責任共有モデルの具体的な内容については、各クラウドサービス事業者や提供されるサービスによって異なる可能性があることに留意する必要がある。


**図 3　クラウドサービスの形態ごとの責任共有モデルの例**

## 3.3　クラウドサービスにおける責任共有に係る留意点

上述のように、クラウドサービスにおいては責任共有モデルが採用されており、その内容はクラウドサービスの形態ごとに異なる。クラウドサービスの利用者が適切にセキュリティ対策を実施する上では、この責任共有モデルに関する理解が不可欠となるが、クラウドサービスを用いた情報システムを実際に構築する際には、当該モデルの適用に関して特に留意すべき点が存在する。

まず、クラウドサービスにおいて各種設定を行う管理コンソール（例：AWS における AWS Management Console）はクラウドサービス事業者によって提供される機能であるものの、その設定を実施する責任はクラウドサービスの利用者にあるという点である。管理コンソールは、クラウドサービスにおける各種操作を効率的に行うための便利なツールである一方、一つの設定ミスによってシステムに関する重要な変更が行われる可能性もある（例：本来組織内にのみ閉じた環境を想定していたシステムがクリック１回でインターネット上に公開されてしまう）。本来、管理コンソールはクラウドサービスの利用者が主体的に管理すべきものであるが、管理コンソールの機能自体はクラウドサービス事業者によって提供されるものであることから、管理主体としての意識がクラウドサービスの利用者に根付いていないことも多い。その結果、管理コンソールにお

ける各種設定ミスが発生することが考えられる。クラウドサービスの利用者は、管理コンソールにおける設定実施の責任が自らにあることを認識の上、自組織内の管理者や開発者にその旨を周知し、本書４章記載の各種対策を実施するのが望ましい。

次に、情報システムを構築・運用する上では、単一のクラウドサービス形態でのみサービスを利用するだけでなく、複数のクラウドサービス形態を組み合わせる場合があるという点にも留意が必要である。例えば、あるシステムを構築する際に、ウェブサーバの構築には IaaS を利用し、データベースの構築には PaaS を利用し、システムにおける認証基盤には SaaS を利用するということが考えられる。このように複数のクラウドサービス形態を組み合わせる際には、クラウドサービスの利用者は多数の事業者とクラウドサービスに関する責任を共有することになる。その際、各種クラウドサービス事業者との責任共有のあり方が複雑化するために、利用者が認識している責任共有の範囲と、実際の契約等において規定されている責任共有の範囲に齟齬が発生する可能性がある。このような認識の齟齬は、本来であればクラウドサービスの利用者が設定すべきセキュリティ対策であるにもかかわらず、自らの責任範囲外であると誤認識していることで設定を実施していない等による設定ミスを招く可能性がある。このような事態を防ぐために、情報システムの構成要素のどの部分について、各種クラウドサービス事業者と自らがそれぞれどのような責任を有しているのかを常に把握しておくことが重要である。

## 3.4 クラウドサービス利用時の脅威

近年、クラウドサービスにおけるアクセス権の設定不備等に起因する不正アクセスや情報漏えい等の事例が実際に確認されており、内閣サイバーセキュリティセンター（NISC）からも注意喚起[7]がなされ、クラウドサービスの利用状況や各種設定の確認・見直しの必要性が指摘されている。

オンプレミスでは、組織内のネットワーク等の「信用できる領域」と、インターネット等の組織外部の「信用できない領域」が明確であるため、「信用できる領域」に情報を格納し、それらの境界部分に対してファイアウォールや IDS/IPS 等を用いて防御を固めるのが一般的である。一方、クラウドサービスでは、様々な場所・デバイス・ネットワーク等からアクセス可能であるため、オンプレミスのように防御すべき境界が明確ではない。したがって、クラウドサービス上に存在する情報を守るためには、情報へのあらゆるアクセス方法・権限等を考慮に入れる必要があるが、それらを網羅することは難しく、抜け漏れが生じてしまうことが多い。結果として、クラウドサービス利用者の設定ミスや、組織内外問わず悪意を持った攻撃者による不正アクセスに起因する情報漏えい事故が相次いでいる。

クラウドサービス利用者は、サービス利用にあたってはさまざまな脅威が存在する認識をあらたにするとともに、クラウドサービス利用に伴う事故防止に細心の注意を払う必要がある。下表

[7] 内閣サイバーセキュリティセンター 「Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について」（2021 年 1 月 29 日）
https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf

に、クラウドサービス利用時における脅威の例を示す。

なお、本書の５章ではクラウドサービスにおける具体的な事故事例や、事故を防ぐために必要と考えられる対策を解説している。

**表 2　クラウドサービス利用時の脅威例**

| No. | 脅威の種類 | 説明 |
|---|---|---|
| 1 | データ侵害 | 要機密情報の外部公開や、不正閲覧、窃取 等 |
| 2 | 設定ミスと不適切な変更管理 | データに対する不必要なアクセス権限の付与や、セキュリティ制御の無効化等のクラウド環境での設定ミス、セキュリティパッチの未適用 等 |
| 3 | クラウドセキュリティアーキテクチャと戦略の欠如 | セキュリティを考慮せずにクラウド利用を推進することによる、適切なセキュリティアーキテクチャの実装不備 等 |
| 4 | 認証情報、アクセス管理システム、暗号鍵等の不十分な管理 | 認証情報、アクセス管理システム、暗号鍵等を適切に管理していないことによる、データへの意図しないアクセスの発生 等 |
| 5 | アカウントハイジャック | 悪意のある攻撃者が、クラウドサービスに関する高権限のアカウント等を悪用する 等 |
| 6 | 内部者の脅威 | 組織が管理する情報資産へアクセスする権限を現在持っているか、あるいはかつて持っていた個人がその権限を悪用し、組織に悪影響を及ぼす可能性のある行為を行う（例：知的財産の窃取）等 |
| 7 | 安全でないインタフェースと API | 一般的にシステムの中で最も外部にさらされる部位である、API やインタフェースにおける設計の不備や、API キーの不正利用 等 |

| | | |
|---|---|---|
| 8 | クラウドサービスを用いたシステムの管理不備 | クラウドサービス利用者が、セキュリティ設定やデータの取り扱いに関する知識を有していないために、データの管理が不十分になる　等 |
| 9 | クラウドサービス事業者が管理する範囲における脆弱性や障害 | クラウドサービス事業者が管理責任を有している領域において、脆弱性のあるシステム設計が実装されることで、障害が発生する　等 |
| 10 | クラウドサービス利用の可視性の不備 | 組織内でクラウドサービスの利用状況が可視化されていないことで、本来は許可されていないアプリケーションの利用や、アプリケーションの悪用が行われる 等 |
| 11 | クラウドサービスの悪用・乱用・不正利用 | 悪意のある攻撃者による、クラウドサービス事業者のドメインを利用したなりすまし攻撃 等 |

参考：日本クラウドセキュリティアライアンス（CSA ジャパン）

「クラウド重大セキュリティ脅威 11 の悪質な脅威」（2019 年 10 月 31 日）

（ https://www.cloudsecurityalliance.jp/site/wp-content/uploads/2019/10/top-threats-to-cloud-computing-egregious-eleven_J_20191031.pdf ）

# 4章　クラウドサービスにおいて設定すべきセキュリティ対策

この章では、クラウドサービスの形態ごとに設定すべきセキュリティ対策について述べる。

PaaS/IaaS に関しては、各クラウドサービス共通で設定すべき基本的なセキュリティ対策を記載している。なお、各クラウドサービスにて独自に実装されている機能等で個別に設定すべきセキュリティ対策については、各対策カテゴリにおいて「各クラウドサービスにおいて考慮すべき設定」として記載している（4.1.1(11)、4.1.3(2)、4.1.4(4)、4.1.5(3)が該当）。

設定すべきセキュリティ対策の個別説明の凡例は以下の通り。

| | |
|---|---|
| 対策の内容 | セキュリティ対策の内容を記載 |
| 対策を実施しない場合のリスク | 本対策を行わない際に起こりうる状況等、対策を実施すべき理由等を記載 |
| 設定参考資料 | 設定時に参考となるCIS Benchmarksの項番を記載<br>※　共通で設定すべき対策については、該当するクラウドサービスにおけるCIS Benchmarksの記載が無いクラウドサービスの場合においても、対策を検討することが望ましい |

SaaSに関しては、各クラウドサービスにおいて提供内容が大きく異なり設定すべき事項も異なるため、サービスごとに設定すべき基本的なセキュリティ対策を記載している。

なお、本章を理解するための共通認識となる用語定義は以下の通り。本書全体において言及している用語の定義については、６章「用語定義」を参照すること。

| 用語 | 本書における定義 |
|---|---|
| アカウント | クラウドサービスの利用者がクラウドサービスを使用するための権利や資格のこと。<br>各アカウントには、その利用者の認証情報が紐づく。<br>本書では具体的には以下を指す。<br>● AWSにおける「IAMユーザー」<br>● GCPにおける「Googleアカウント」<br>● Azureにおける「ユーザー」<br>また、上記と比較してより高い権限を有する「管理者アカウント」についても「アカウント」に含まれるものとする。<br>※　各クラウドサービスにおけるアカウントやアクセス権限の詳細は、4.1 |

| | |
|---|---|
| | 記載の「コラム：AWS、GCP、Azure におけるアカウントの概要」を参照すること。 |
| 管理者アカウント | クラウドサービスの様々な設定変更等が可能な権限を持つアカウントのこと。また、管理者アカウントのみが有する、設定の変更等が可能な強力な権限を管理者権限という。<br>管理者アカウントは、本書では具体的には以下を指す。<br>● AWS における「AWS アカウント（ルートユーザー）」、ならびに「AWS アカウント（ルートユーザー）」より生成した、「IAM ユーザー」であって、管理者権限を持つもの。<br>● GCP における「Google アカウント」であって、管理者権限を持つもの。<br>● Azure におけるグローバル管理者や所有者等のロールが割り当てられた「ユーザー」。<br>※ 各クラウドサービスにおけるアカウントやアクセス権限の詳細は、4.1 記載の「コラム：AWS、GCP、Azure におけるアクセス権」を参照すること。 |
| IAM ロール | AWS において、主にアプリケーション等が特定のリソースに対してアクセスするために割り当てられる権限設定のこと。例えば、AWS において稼働している各サービスの連携を行うために、データベース等のアクセス権限を含んでいる IAM ロールをあるアプリケーション等に割り当てること等が想定される。 |
| サービスアカウント | GCP において、アプリケーション等が特定のリソースに対してアクセスするために割り当てられる権利や資格のこと。 |
| サービスプリンシパル | Azure において、アプリケーション等が特定のリソースに対してアクセスするために割り当てられる権利や資格のこと。 |
| 認証情報 | 認証を実施するために必要な情報のことで、具体的には、識別コード（ID）、主体認証情報（パスワード等）、アクセスキー、サービスアカウントキー等を指す。 |
| アクセスキー | AWS でプログラム等の認証に用いられる情報のこと。アクセスキーID とシークレットアクセスキーから構成されている。識別コード（ID）、主体認証情報（パスワード等）による認証と同様の処理をアクセスキーID とシークレットアクセスキーを用いて行うことができる。 |
| サービスアカウントキー | GCP で用いられる、サービスアカウントの認証のために使用される情報のこと。 |
| サービス | 本書においては、各クラウドサービス上で個別の用途のために提供されている製品等のことを指す。 |

| | |
|---|---|
| リソース | クラウドサービスを構成する資源や要素（CPU、メモリ）を指す。 |
| サブスクリプション | Azure で用いられる、リソースをグループ化したもの。 |
| インスタンス | クラウドサービス上に構築された仮想サーバのこと。 |
| プロジェクト | GCP のサービスで作成するリソースの管理単位のこと。 |

## 4.1 PaaS/IaaS において設定すべきセキュリティ対策

どのようなクラウドサービスであっても、クラウドサービスへ接続するデバイスの安全性の確保、さらには利用者が管理する情報等の取扱いは、利用者の責任により実施する必要がある。

上記に加えて、PaaS ではプログラミング環境やデータベース等のミドルウェアに対して、クラウドサービス事業者が提供する認証機能、ログ管理機能といったセキュリティ機能を利用者側で設定する必要があり、IaaS では仮想マシン上で動作している OS を含めたすべてのソフトウェアの管理を利用者側で行う必要がある。

また、「3.1 クラウドサービスの特徴」に記載のとおり、クラウドサービスは頻繁に仕様変更や機能追加が行われることがあり、利用者のセキュリティに関する設定に影響を与える可能性がある。そのため、最新の情報を収集するとともに、セキュリティに関する設定や業務への影響等の有無を確認することが特に重要である。また、クラウドサービスを利用する際に選択するリージョンやゾーンによっては、国内法以外の法令及び規制が適用されるリスクが存在するため、選択できるリージョンやゾーンを制限することや利用者が管理する暗号鍵を用いてデータを暗号化するなどの対策も重要となる。利用者が管理する暗号鍵を用いて暗号化する対策については、適切な暗号鍵の管理とクラウドサービス利用開始時から運用の全期間を通じて暗号化を実施していることを前提とした場合、暗号化消去として利用することができるため、特に重要となる。

なお、本節においては、PaaS/IaaS で設定すべき基本的なセキュリティ対策をカテゴリごとに分類し、各対策を実施するための設定項目について記載している。なお、以降で記載する設定項目はすべてのセキュリティ対策における設定項目を網羅するものではないため、必要に応じて、追加のセキュリティ対策等を検討すること。

### 4.1.1 ID およびアクセス管理

ID およびアクセス管理は、適切なエンティティ（人または物）に対し、アプリケーションやデータ等のリソースへの適切なアクセス権限を付与し認証するために必要となる。

クラウドサービスでは、オンプレミス環境と異なり、インターネットを通して様々なコンピューティングリソースがクラウドサービス事業者から利用者へ提供される。利用者のデータについても、インターネットを通してクラウドサービスに保存される。このことにより、利用者は使用するデバイスや場所に依存せず、インターネットの接続環境があればクラウドサービスを利用することが出来るようになる。一方で、クラウドサービスにおいては、インターネットと組織内環境との境界が曖昧になることから、オンプレミス環境で実施していた従来の境界防御によるアクセス制御だけでは、不正アクセスによる情報の改ざんや漏えい等のリスクが高まる。このようなリスクに対し、クラウドサービスではそれぞれのリソースに対して誰を認証し、誰に使用を承認する（アクセス権限を持たせる)かを制御することは、特に重要なセキュリティ対策となる。

なお、クラウドサービスごとにアカウントに関する考え方や名称が異なるため、それぞれのアカウントの概念について、下図に示す。

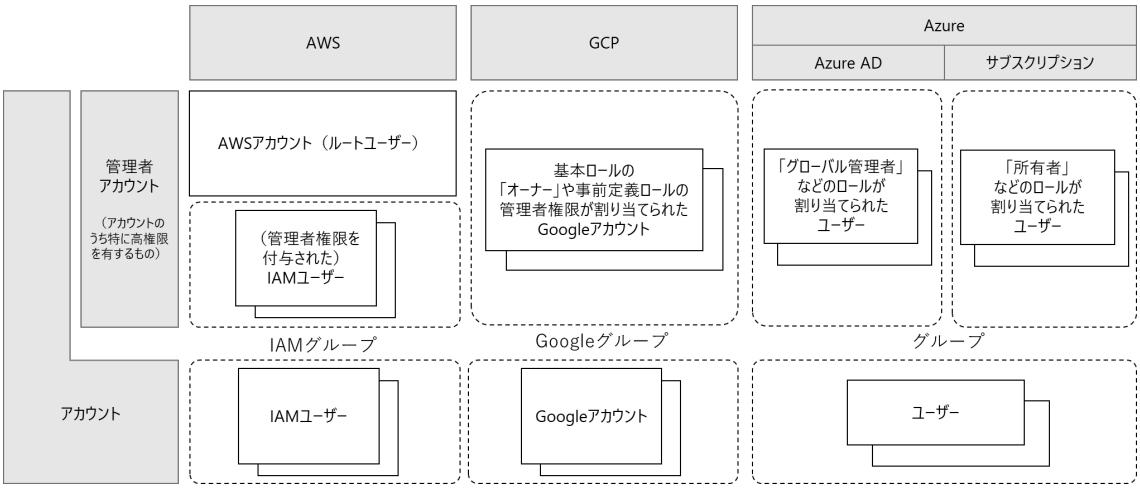
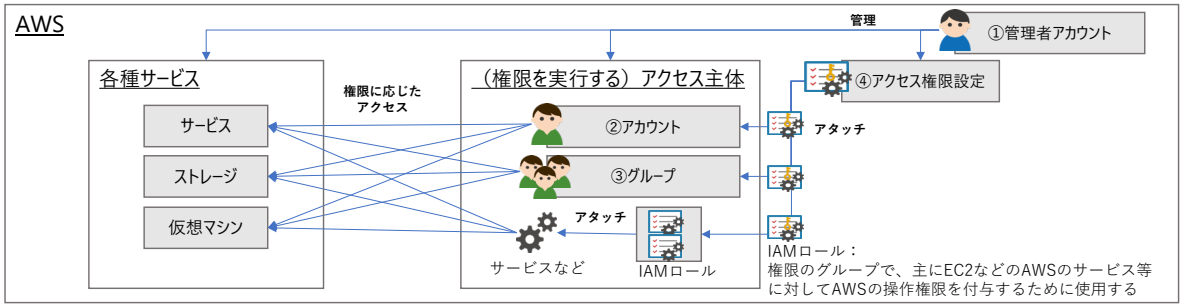



**図 4　本書におけるクラウドサービスごとのアカウントの概念図**

コラム： AWS、GCP、Azure におけるアカウントの概要

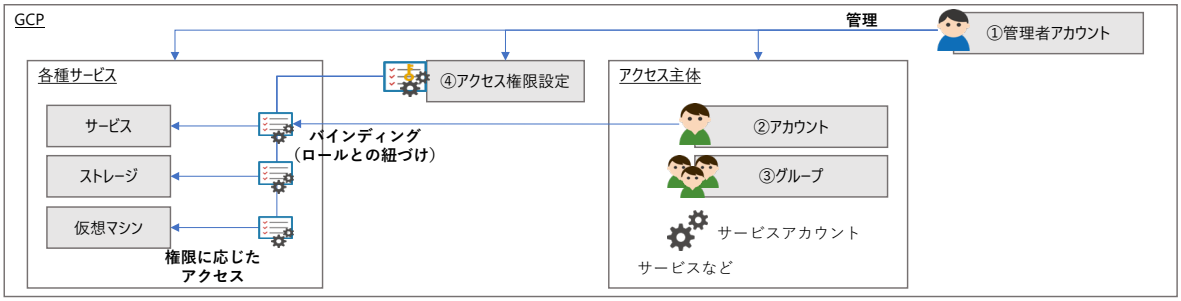
それぞれのクラウドサービスのアカウントの概要を以下に示す。

［AWS］



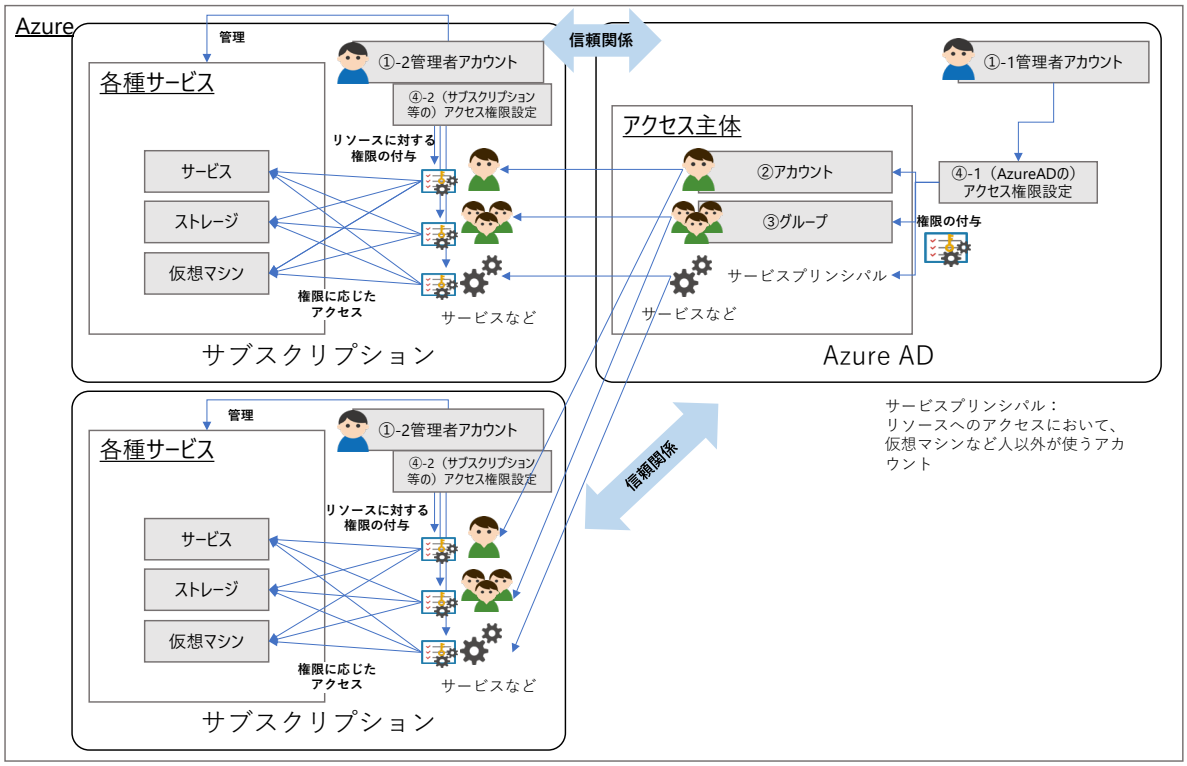

| 上記の概念内の用語 | AWSでの用語 | 補足 |
|---|---|---|
| ①管理者アカウント | AWSアカウント（ルートユーザー） | すべての AWS サービスとリソースに対して完全なアクセス許可を持つ。 |
| | （管理者権限を付与された） IAMユーザー | AWSアカウントによって作成されるユーザー。IAMユーザーにポリシーをアタッチ（割り当て）することで、権限が付与される。 |
| ②アカウント | IAMユーザー | |
| ③グループ | IAMグループ | 複数のIAMユーザーの集合。IAMグループに対してIAMポリシーを割り当てることができ、複数のIAMユーザーにまとめて権限設定を行うことができる。 |
| ④アクセス権限設定 | IAMポリシー | AWSサービスのリソースに対するアクセス権限の集合であり、IAMユーザー、IAMグループ、IAMロールに割り当てることができる。 |

［GCP］




| 上記の概念内の用語 | GCPでの用語 | 補足 |
|---|---|---|
| ①管理者アカウント | （管理者権限を付与された） Googleアカウント | 個人、または組織により管理される個別のアカウント。管理者のロールを割り当てることで、管理者権限が付与される。 |
| ②アカウント | Googleアカウント | |
| ③グループ | Googleグループ | 複数のGoogleアカウントやサービスアカウントの集合。 |
| ④アクセス権限設定 | ロール | GCPのリソースに対するアクセス権限の集合であり、Googleアカウント、Googleグループ、サービスアカウントなど割り当てることができる。 |

［Azure］




| 上記の概念内の用語 | Azureでの用語 | 補足 |
|---|---|---|
| ①-1管理者アカウント | 「グローバル管理者」などのロールが割り当てられたユーザー　※AzureADの管理を行う | Azure AD上で管理されているユーザー。管理者のロールを割り当てることで、管理者権限が付与される。 |
| ①-2管理者アカウント | 「所有者」などのロールが割り当てられたユーザー<br>※Azureリソース（ストレージなど）の管理を行う | |
| ②アカウント | ユーザー | |
| ③グループ | グループ | 複数のユーザーの集合。Azure AD管理者により管理される。 |
| ④-1アクセス権限設定 | Azure ADロール | Azure ADでの設定に対する権限。<br>設定としては、ユーザーの作成や編集などがある。 |
| ④-2アクセス権限設定 | Azureロール | リソースに対する権限。ロールには役割に応じたアクセス権限が設定されており、ユーザー等に割り当てることでリソースへのアクセス制御を行う。 |

(1)　組織が許可したアカウントの管理

| | |
|---|---|
| 対策の内容 | 組織が許可したアカウントのみを利用するように管理する。例えば、個人の私的に利用しているアカウント等の利用を許可しない。 |

| | |
|---|---|
| 対策を実施しない場合のリスク | 例えば、個人の私的に利用しているアカウント等を業務に使用することで、私的な利用と業務での利用が混同し、設定ミスや操作ミスが発生する可能性が高まるとともに、アカウントの窃取等による不正アクセス等による情報漏えい等につながる可能性がある。 |
| 設定参考資料 | (GCP) 1.1 |

(2) 管理者アカウントに対する多要素認証の利用

| | |
|---|---|
| 対策の内容 | 管理者アカウントに対して多要素認証を有効とし、管理者アカウントのセキュリティ強度を高める。 |
| 対策を実施しない場合のリスク | 多要素認証を利用せずに管理者アカウントの認証情報が窃取等されてしまうと、簡単に管理者アカウントを不正利用されてしまう。管理者アカウントは高権限を有しているため、データの漏えいや改ざん、不正アプリケーションの導入及び、システムの停止・破壊等につながる可能性がある。 |
| 設定参考資料 | (AWS) 1.5、1.10<br>(GCP) 1.2<br>(Azure) 1.1 |

(3) 管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し

| | |
|---|---|
| 対策の内容 | 管理者アカウントに紐づく連絡先を登録し、最新の状態を保つとともに、クラウドサービス事業者からの通知を組織内の複数人が受け取れるように設定する。 |
| 対策を実施しない場合のリスク | クラウドサービス事業者側のモニタリングにより利用規定に違反していると判断された活動が確認された場合、単一の連絡先のみが登録された状態であると、規定違反に気がつくのが遅れ、アカウントの停止及びサービスの停止につながる可能性がある。また、同様のモニタリングによりセキュリティ侵害の可能性を示す活動が検知された際、クラウドサービス事業者からの連絡に気がつくのが遅れることで利用者側にて必要な対応の実施が遅れ、情報漏えいやサービス停止等の発生や被害の拡大を引き起こす可能性がある。 |
| 設定参考資料 | (AWS) 1.1、1.2 |

(4) 必要最低限の管理者権限の割当て

| | |
|---|---|
| 対策の内容 | 管理者権限の付与は必要最低限とし、重要な設定変更等の操作が可能となる管理者権限をむやみに使用せず、必要な操作のみを許可する権限 |

| | |
|---|---|
| | 等を付与する。 |
| 対策を実施しない場合のリスク | 本来必要としていない担当者にまで管理者権限を割り当ててしまうことで、本来アクセスすることのできないデータ等にアクセスが可能となってしまい、情報の漏えい等につながる可能性がある。 |
| 設定参考資料 | (AWS) 1.16<br>(GCP) 1.5 |

(5) グループを利用した権限の設定

| | |
|---|---|
| 対策の内容 | 権限の設定は利用者ごとに適用するのではなく、グループの役割や与えられる権限に応じて可能な限りグループへ適用する。 |
| 対策を実施しない場合のリスク | グループを利用した権限割り当てを使用せず、アカウントごとに権限を割り当てると、管理が複雑化する可能性がある。管理が複雑化すると、付与すべき権限を間違える等のミスが発生し、本来アクセス制限されるべきデータ等にアクセスできる状態や、本来アクセスできる必要のあるデータ等にアクセスできなくなる状態を引き起こし、情報漏えいの発生や通常の運用及びサービス提供等に支障をきたす可能性がある。 |
| 設定参考資料 | (AWS) 1.15 |

(6) 管理者アカウントに関する復旧手段の確保

| | |
|---|---|
| 対策の内容 | 管理者アカウントにアクセスできなくなった場合に備えて、確実な復旧手段を確保する（秘密の質問等）。 |
| 対策を実施しない場合のリスク | 管理者アカウントへのアクセスに必要な認証要素（知識情報、所持情報、生体情報）が紛失/破壊されてしまうと、管理者アカウントへのアクセスができなくなってしまう。その際、復旧方法が設定されていないと、管理者アカウントが必要な操作等を実施できなくなり、通常の運用及びサービス提供に支障をきたす可能性がある。 |
| 設定参考資料 | (AWS) 1.3 |

(7) すべてのアカウントへのパスワードポリシーの適用

| | |
|---|---|
| 対策の内容 | 管理者アカウントに限らず、管理者権限をもたないアカウントを含むすべてのアカウントに対して、以下の例にパスワードポリシーを適用する。<br>例：<br>● パスワード長を 14 文字以上とする<br>● 一度利用したパスワードの再利用を禁止する |

| | |
|---|---|
| | ● パスワードをリセットする際に知識認証以外の認証方法を要求する<br>● パスワード変更時、利用者にパスワード変更通知を送付する<br>● システムの利用者に定期的に再認証の実施を求める　等 |
| 対策を実施しない場合のリスク | アカウントに対して適切なパスワードポリシーが未設定の場合、アカウントのセキュリティ強度が脆弱となる可能性がある。セキュリティ強度の脆弱なアカウントは、ブルートフォース攻撃によるログイン試行等が行われる可能性が高くなり、不正アクセス等が成功してしまうと、情報漏えいやデータの破壊等につながる可能性がある。 |
| 設定参考資料 | (AWS) 1.8、1.9<br>(Azure) 1.5～1.7 |

(8) アクセスキー、サービスアカウントキー等の適切な管理

| | |
|---|---|
| 対策の内容 | 各種サービスへのアクセスを認証するために作成される認証情報であるアクセスキー(AWS)やサービスアカウントキー(GCP)、API キー等は、作成することの必要性を検討するとともに、作成したキーが不正に利用されていないことの定期的な確認及びキーの更新等の管理を行う。<br>例えば、AWS の場合、AWS アカウント（ルートユーザー）は多くの高権限を持ち不正利用時のリスクが大きいため、AWS アカウント（ルートユーザー）に関連するアクセスキーは設定しない、削除する等があげられる。 |
| 対策を実施しない場合のリスク | 作成するアカウントと同様の権限を有するアクセスキー(AWS)やサービスアカウントキー等(GCP)を適切に管理しないと、これらの不正利用により情報漏えいやデータの破壊、サービス停止等につながる可能性がある。 |
| 設定参考資料 | (AWS) 1.4、1.11、1.13、1.14<br>(GCP) 1.4、1.7、1.9～1.10、1.13～1.15 |

(9) 管理者アカウントと日常的に使用するアカウントの分離

| | |
|---|---|
| 対策の内容 | 管理者アカウントと日常的に使用するアカウントを分離し、管理者アカウントは日常業務では使用しないようにする。 |
| 対策を実施しない場合のリスク | 日常的な業務に管理者アカウントを使用していると、本来必要としない管理者権限の不正利用や意図しない設定の変更等によるデータの破壊やサービス停止等を引き起こす可能性がある。 |
| 設定参考資料 | (AWS) 1.7 |

| | |
|---|---|
| | |

(10) アカウント・権限・認証情報の定期的な見直し

| | |
|---|---|
| 対策の内容 | 不要となったアカウントや権限及び認証情報を定期的に確認し、不要なアカウントや権限及び認証情報は随時削除する。 |
| 対策を実施しない場合のリスク | 不要となったアカウントや権限、認証情報を残していると、アカウントの窃取や権限及び認証情報の不正利用等のリスクが高まり、情報漏えいやデータの破壊につながる可能性がある。 |
| 設定参考資料 | (AWS) 1.12<br>(Azure) 1.3 |

(11) 各クラウドサービスにおいて考慮すべき設定

AWS

1. AWS サポートセンターへのアクセス設定

| | |
|---|---|
| 対策の内容 | AWS で発生したセキュリティインシデントの通知や対応、技術サポート等を利用できるようにするため IAM ユーザーに AWS サポートセンターへのアクセス権限を設定する。 |
| 対策を実施しない場合のリスク | AWS サポートセンターへのアクセス権限を有するアカウントを作成しない場合、AWS で発生したセキュリティインシデント等の確認ができず、サービス停止等への対応が遅延する可能性がある。 |
| 設定参考資料 | (AWS) 1.17 |

2. IAM に保存されているサーバ証明書の管理

| | |
|---|---|
| 対策の内容 | IAM に保存されている TLS 証明書のうち、有効期限が切れた証明書については削除する。 |
| 対策を実施しない場合のリスク | 有効期限が切れて無効になった証明書を誤って使用すると、アプリケーションやウェブサイトの信頼性が損なわれる可能性がある。 |
| 設定参考資料 | (AWS) 1.19 |

3. IAM Access analyzer の有効化

| | |
|---|---|
| 対策の内容 | 利用する全てのリージョン（AWS のデータセンターが集積されている物理的ロケーション）において IAM Access analyzer（AWS におけるアクセス制御ポリシーを分析し、意図していないアクセスの可否を検出す |

| | |
|---|---|
| | るための機能）が有効化され、リージョン内の各リソースに適用されているポリシーの分析・監視が行われていることを確認する。<br>なお、複数リージョンをまとめて有効化することはできない為、リージョンを複数利用する場合は、個別に有効化の設定を行う。 |
| 対策を実施しない場合のリスク | 外部からのアクセスが検知されたリソースを確認する際、組織が許可したアクセスか不審なアクセスかを特定するのに時間を要し、対応が遅れる可能性がある。 |
| 設定参考資料 | （AWS）1.20 |

GCP

1. サービスアカウントのロール設定

| | |
|---|---|
| 対策の内容 | 以下のロールを利用者に割り当てる際、プロジェクト単位で割り当てるのではなく、特定のサービスアカウントに対して割り当てる。<br>● Service Account User（iam.serviceAccountUser）<br>● Service Account Token Creator（iam.serviceAccountTokenCreator） |
| 対策を実施しない場合のリスク | iam.serviceAccountUser または iam.serviceAcountTokenCreatorccountUser をプロジェクト単位で利用者に割り当てた際、利用者が持つその他の権限との組み合わせによっては、将来作成される可能性のあるサービスアカウントを含め、プロジェクト内のすべてのサービスアカウントへのアクセスを間接的に許可し、本来意図しない不要な権限を付与することになり、データの漏えいや改ざんにつながる可能性がある。 |
| 設定参考資料 | （GCP）1.6 |

Azure

1. Azure AD 管理ポータルへのアクセス制限

| | |
|---|---|
| 対策の内容 | Azure AD 管理ポータルへのアクセスを管理者のみに制限する。 |
| 対策を実施しない場合のリスク | 権限を持たない者が Azure AD のユーザー一覧等のデータにアクセスが可能となり、情報の漏えい等につながる可能性がある。 |
| 設定参考資料 | （Azure）1.15 |

| | |
|---|---|
| | |

2. Azure AD へのデバイス追加設定

| | |
|---|---|
| 対策の内容 | 業務で使用するデバイス（例：PC、タブレット等）を Azure AD に追加する際に多要素認証が行われるようにする。 |
| 対策を実施しない場合のリスク | Azure AD へのデバイス追加時に多要素認証が実施されないと、なりすましによってデバイスが追加され、不正に組織内の情報を閲覧・窃取されてしまう可能性がある。 |
| 設定参考資料 | （Azure）1.20 |

3. Azure AD におけるセキュリティの既定値群の有効化

| | |
|---|---|
| 対策の内容 | Azure AD で「セキュリティの既定値群」を有効にする。<br>※ セキュリティの既定値群とは、「管理者に対して多要素認証を必須にする」等、既に構成されているセキュリティ設定のこと。 |
| 対策を実施しない場合のリスク | アカウントに関するセキュリティ対策を個別に行うと、本来設定しなければならない対策等の抜け漏れが発生し、セキュリティの確保が困難になる可能性がある。 |
| 設定参考資料 | （Azure）1.22 |

### 4.1.2 ログの記録と監視

クラウドサービスにおけるログの取得は、オンプレミス環境と同様に悪意ある第三者等による外部からの不正侵入や不正操作等の情報セキュリティインシデントの予兆、検知や、情報セキュリティインシデントが発生した際の原因究明等に利用するため特に重要となる。したがって、クラウドサービスにおけるログの取得についてもオンプレミス環境と同様に適切に取得できるよう設定するとともに、改ざんや消失等が起こらないよう、適切に保全する必要がある。

クラウドサービスでは、様々なログを取得し記録する仕組みが提供されている。また、ログの取得と記録にとどまらず、ログを監視しアラートを通知するサービスや、ログを分析できるサービス等も提供されており、ログを統合的に管理できる仕組みが提供されている場合が多い。

なお、このようなクラウドサービスで提供されている仕組みを活用しログの管理を行う場合、ログ取得に関する設定等が適切に実施されていることが重要である。設定が不足している、あるいは設定内容が誤っている場合、取得すべきログが取れない、監視が行われない、通知がされない、等の事象によりセキュリティインシデントに対する迅速な検知や対処、被害の最小化、未然に防ぐための対策等ができなくなる可能性がある。

これらのログ取得に関連する設定は、基本的には初期設定で有効化されているが、特定のサービスにおいては、初期設定では有効化されていなかったり、ある機能では有効化されていても他の機能では有効化されていなかったりする場合もある。また、取得するログの種類については利用者が自ら選択しなければならない場合もある。そのため、利用者自らがログ取得に関する設定内容を確認し、必要に応じて設定を実施あるいは変更することが重要である。設定する内容は各サービスにおいて異なる可能性があるため、本項で示すセキュリティ対策を参考とするとともに各クラウドサービスの公式ドキュメント等を参照することが望ましい。

コラム： クラウドサービスにおけるログの管理について

クラウドサービスではログの管理に関する様々な仕組みを提供している。ログの管理における主な仕組みの概要を以下に記載する。

① 収集

クラウドサービスにおいて収集可能なログは多岐にわたり、各クラウドサービスは多岐にわたるログを効率的に収集するための仕組みを提供している。利用者は各サービスでログを取得するための設定を行い、必要なログを収集する。なお、クラウドサービスやログの種類によっては、初期設定で収集されるログもあるため、取得すべきログの種類等についてはクラウドサービス事業者が提供する公式ドキュメント等を確認することが望ましい。

② 蓄積

収集されたログはクラウドサービス内で蓄積される。その際、クラウドサービスの種類や契約内容によってログの保存期間が異なるため、利用者は自らが構築するシステムの要件に鑑みてログの保存期間の設定を変更する必要がある。また、蓄積したログが何者かに改ざんされてしまったり、運用に関わる者によって誤って削除されてしまったりすると、後述の活用や分析の実施が困難となるため、ログへのアクセス制御や暗号化の実施を検討するのが望ましい。

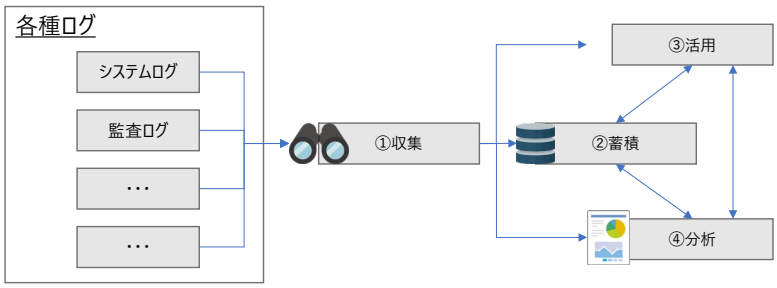
③ 活用

収集、蓄積されたログは様々な方法で活用される。活用の例としてはリソースモニタリング、ログをトリガーとしたアラート発信、レポーティング等が挙げられる。ログを活用する仕組みは、同じクラウドサービスで提供されている場合もあるが、異なるクラウドサービスのサービスやソフトウェア等を利用することもできる。

④ 分析

蓄積されたログは様々な目的で分析される。例えば、不審なアクセスや操作の検出、リソース状況の把握等が挙げられる。分析と活用の目的や仕組みは類似していることから、分析と活用を連動させた仕組みとしてクラウドサービスから提供される場合や、分析と活用を 1 つの仕組みとして提供される場合がある。

クラウドサービスのログ管理イメージ




各クラウドサービスにおけるサービスの例

| クラウドサービス | ① 収集 | ② 蓄積 | ③ 活用 | ④ 分析 |
|---|---|---|---|---|
| AWS | Cloud Trail<br>Cloud Watch | S3<br>Cloud Watch Logs | メトリクスフィルタ<br>（Cloud Watch Logs） | Elasticsearch<br>OpenSearch |
| GCP | Cloud Logging | シンク | Cloud Monitoring | - |
| Azure | Azure Monitor | Azure Monitor<br>（Log Analyticsワークスペース、Storageアカウント） | Azure Monitor<br>(Aleart) | Azure Monitor<br>(Log Analytics) |

(1) ログの有効化及び取得

| | |
|---|---|
| 対策の内容 | ログの取得が必要となる各サービスにおいてログを取得するために必要な設定を有効化し、適切なログ取得が可能となるようにする。 |

| | |
|---|---|
| 対策を実施しない場合のリスク | ログが適切に取得できていないと、セキュリティインシデントが発生した際、過去に遡って不審なアクセスや操作を確認することが困難となり、被害の全容把握や原因を調査できず被害が拡大する可能性がある。 |
| 設定参考資料 | (AWS) 3.1、3.6<br>(GCP) 2.1、2.12、3.8<br>(Azure) 2.11、5.1.1、5.1.2、5.1.5、5.3 |

(2) ログの一元管理

| | |
|---|---|
| 対策の内容 | 各サービスで取得するログの監視や通知をログの一元管理機能を用いて行う。 |
| 対策を実施しない場合のリスク | 各サービスのログを個別に監視し通知を受けると、運用管理が煩雑となり、必要なログの取得漏れや不審な挙動を示すログを見逃してしまう可能性がある。 |
| 設定参考資料 | (AWS) 3.4<br>(GCP) 2.2 |

(3) ログの保護

| | |
|---|---|
| 対策の内容 | 取得したログに対してアクセス制御、改ざん防止設定を実施する。 |
| 対策を実施しない場合のリスク | ログが保護されていない場合、攻撃者によって不正アクセスの痕跡等を削除、改ざんされる可能性がある。その場合、被害の全容把握が困難となり原因を特定できず被害が拡大する可能性がある。 |
| 設定参考資料 | (AWS) 3.3<br>(GCP) 2.3<br>(Azure) 5.1.3 |

(4) ログの監視/通知の設定

| | |
|---|---|
| 対策の内容 | 重要な設定変更や管理者アカウントでのログイン等、重要な操作に関するログの監視や通知を設定する。 |
| 対策を実施しない場合のリスク | 重要な操作に関するログの監視や通知の設定がされていないと、不審な活動の見逃しや、検出までの時間を要することから、セキュリティインシデントの被害が拡大する可能性がある。 |
| 設定参考資料 | (AWS) 4.1～4.5、4.8、4.12～4.15<br>(GCP) 2.4～2.11<br>(Azure) 5.2.1～5.2.9 |

### 4.1.3 ネットワーク

クラウドサービスは、クラウドサービス単体の利用のほか、自組織のオンプレミスのシステムや他のクラウドサービスとの接続を行い連携することを前提とした利用が考えられる。このようなクラウドサービスの多様な利用の仕方について、目的や用途に応じて様々な接続構成が考えられるが、基本的には不特定多数がアクセスできるインターネットを経由した接続が想定される。

適切なネットワーク接続設定がなされない状態でクラウドサービスを利用した場合、本来は公開することを意図していない情報がインターネット上に公開されたり、機微な情報を扱っている通信が盗聴されたりする等の被害が発生する可能性がある。

このため、クラウドサービスの利用において、ネットワークのセキュリティ対策には十分留意する必要がある。なお、一般的なネットワークのセキュリティ対策としては利用する目的に応じたネットワークセグメントの分離や、ウェブアプリケーションを保護する機能、DDoS攻撃に対応するための機能の利用、ファイアウォール等によるアクセス制御等が重要となるが、これらの機能における設定等については、クラウドサービスの利用環境に応じて異なるため、各クラウドサービスの公式ドキュメント等を参考にしながら構築する環境にあわせて検討する必要がある。

(1) ロードバランサの接続設定

| | |
|---|---|
| 対策の内容 | ロードバランサの接続に用いる通信を TLS1.2 以降に設定する。 |
| 対策を実施しない場合のリスク | 安全でない暗号プロトコルを用いることで、通信内容が盗聴される可能性がある。 |
| 設定参考資料 | (GCP) 3.9 |

(2) 各クラウドサービスにおいて考慮すべき設定

GCP

1. レガシーネットワークの利用停止

| | |
|---|---|
| 対策の内容 | レガシーネットワーク（単一の IP アドレス範囲のみをもつことができるネットワーク）を利用している場合、利用を停止する。<br>なお、現在、新規でのレガシーネットワーク作成は実施できない。 |
| 対策を実施しない場合のリスク | レガシーネットワークでは、ネットワークを複数に分割して作成することができないため、ネットワークトラフィックの多いプロジェクトで、可用性に悪影響を与える可能性がある。 |

| | |
|---|---|
| 設定参考資料 | （GCP）3.2 |

2. DNSSEC の有効化

| | |
|---|---|
| 対策の内容 | Cloud DNS（GCP 上で提供されている DNS サービス）の DNSSEC を有効にする。<br>また、DNSSEC の署名には強力な暗号化アルゴリズム（SHA-2 以降）が用いられていることを確認する。 |
| 対策を実施しない場合のリスク | DNS ハイジャック等の攻撃により、攻撃者が偽の DNS レスポンスを発行し、悪意のある Web サイトに誘導する可能性がある。 |
| 設定参考資料 | （GCP）3.3～3.5 |

Azure

1. Network Watcher の有効化

| | |
|---|---|
| 対策の内容 | Network Watcher（仮想ネットワーク内のリソースの監視等を行う機能）を有効にする。これにより、仮想マシンとデバイスの間の通信の監視やネットワークの診断、トラフィックの分析等を行う。 |
| 対策を実施しない場合のリスク | ネットワーク内の監視が行えず、パフォーマンスの低下やネットワークの問題の検知が遅くなる可能性がある。 |
| 設定参考資料 | （Azure）6.5 |

コラム：安全でない状態で公開されたクラウドサービスへの攻撃

パロアルトネットワークス社の調査によると、パブリッククラウドで構築された脆弱性のあるインスタンス(ハニーポット)をインターネットに公開したところ､24 時間以内にその 80%、１週間以内にその 100%への侵害が確認された。インスタンスには SSH、Samba、Postgres、RDP のアプリケーションが導入され、弱い認証情報が意図的に設定されていた。

この事実は、設定ミスや、安易な認証情報の設定等により、インスタンスが安全でない状態でインターネットに晒された場合、たとえそれが数分であったとしても、短い時間で攻撃者により発見され、攻撃される可能性を示している。

参考：Palo Alto Networks, Inc 「パブリッククラウドのハニーポット観測結果: 脆弱な

SSH、Samba、Postgres、RDP を数百台デプロイして攻撃アクティビティを分析」（2021 年 11 月 29 日）（https://unit42.paloaltonetworks.jp/exposed-services-public-clouds/）

### 4.1.4 仮想マシン

クラウドサービスにおける仮想マシンは、必要なリソースを自由に選択することができ、オートスケールを使用した自動的なリソースの増減ができる等の特徴から、効率的な運用や、可用性の担保といったメリットがある。

一方で、仮想マシンに係るセキュリティ対策については利用者の責任において実施する必要がある。具体的には、稼働している全ての仮想マシンに対して脆弱性対策を行っているか、仮想マシンの設定がセキュリティに関する問題になっていないか等を確認する等、管理の徹底に十分留意する必要がある。

(1) 最新の OS パッチの適用確認

| | |
|---|---|
| 対策の内容 | 仮想マシンの OS に対して最新のセキュリティパッチが適用されていることを確認する。 |
| 対策を実施しない場合のリスク | セキュリティに関する脆弱性へ対応済みの最新のセキュリティパッチが適用されていないと、脆弱性を突いた攻撃のリスクが高まり、データの漏えいや改ざん、システムの停止・破壊等につながる可能性がある。 |
| 設定参考資料 | (Azure) 7.5 |

(2) 不正プログラム対策ソフトウェアの導入

| | |
|---|---|
| 対策の内容 | 仮想マシンの OS 上で動作する不正プログラム対策ソフトウェアを導入する。不正プログラム対策ソフトウェアを導入することにより、仮想マシンの OS 上でのアクティビティを監視し、不正プログラムの実行を検出・ブロックすることができる。 |
| 対策を実施しない場合のリスク | 不正プログラム対策ソフトウェアを導入しないと、不正プログラムを実行されるリスクが高まり、データの漏えいや改ざん、システムの停止・破壊等につながる可能性がある。 |
| 設定参考資料 | (Azure) 7.6 |

(3) 攻撃対象となるネットワークポートへのアクセス制限

| | |
|---|---|
| 対策の内容 | 外部からの不正アクセスや DDoS 攻撃等に使用される可能性のあるネットワークポートを制限する。(以下対策例)<br>例:インターネットからの RDP や SSH のアクセスについて接続元制限を行う。不要な UDP ポートを無効にする。 等 |
| 対策を実施しない場合のリスク | インターネットに公開されているネットワークポートのアクセス制限が適切に行われていないと、ブルートフォース攻撃による不正アクセスや DDoS 攻撃が成功し、情報漏えいやサービス不能等につながる可能性がある。 |
| 設定参考資料 | (AWS) 5.1、5.2<br>(Azure) 6.1～6.3、6.6 |

(4) 各クラウドサービスにおいて考慮すべき設定

GCP

1. インスタンスのサービスアカウントの設定

| | |
|---|---|
| 対策の内容 | 初期設定のサービスアカウントを使用しない。 |
| 対策を実施しない場合のリスク | 初期設定のサービスアカウントは高権限であるため、当該サービスアカウントが悪用された場合、プロジェクトのすべてのデータ等にアクセスされ、データの漏えいや改ざん、システムの停止・破壊等につながる可能性がある。 |
| 設定参考資料 | (GCP) 4.1、4.2 |

2. インスタンス固有の SSH キーの利用

| | |
|---|---|
| 対策の内容 | プロジェクト共通の SSH キーではなく、インスタンス固有の SSH キーを使用する。 |
| 対策を実施しない場合のリスク | プロジェクト共通の SSH キーを用いると、プロジェクト内のすべてのインスタンスへのログインに使用できる。そのため、当該 SSH キーが漏えいした場合、プロジェクト内のすべてのインスタンスに影響を与えることとなり、データの漏えいや改ざん、システムの停止・破壊等につながる可能性がある。 |
| 設定参考資料 | (GCP) 4.3 |

3. OS Login の有効化

| | |
|---|---|
| 対策の内容 | OS Login（IAM を使用してインスタンスへの SSH アクセスを Google アカウントと連動して管理することができる機能）を有効にする。 |
| 対策を実施しない場合のリスク | OS Login を有効にしない場合、SSH によるアクセスが可能な利用者を Google アカウント/グループと別に管理する必要があるため、SSH キーも個別に管理することになる。そのため、Google アカウントを削除する際に、Google アカウントと SSH キーの削除を独立して実施する必要があるため、キーの削除漏れ等の可能性が高まる。 |
| 設定参考資料 | （GCP）4.4 |

4. インタラクティブシリアルコンソール接続の無効化

| | |
|---|---|
| 対策の内容 | インタラクティブシリアルコンソールを用いた接続を無効にする。<br>インタラクティブシリアルコンソールとは、マウス等を用いずにテキスト入力によってインスタンスの操作を行う方法のうち、対話型の形式のものを指す。起動やネットワークの問題のデバッグ、不具合のあるインスタンスのトラブルシューティング時の利用が想定されているが、IP 許可リスト等によるアクセス制限に対応していない。 |
| 対策を実施しない場合のリスク | 任意の IP アドレスからインスタンスへの接続を試行することが可能となる。そのため、アクセスに必要な情報（※）があれば、誰でもインスタンスに接続することが出来るようになり、攻撃者による不正アクセスに利用され、データの漏えいやサービス不能等につながる可能性がある。<br>※ SSH キー、ユーザー名、プロジェクト ID、ゾーン、およびインスタンス名 |
| 設定参考資料 | （GCP）4.5 |

5. IP フォワーディングの無効化

| | |
|---|---|
| 対策の内容 | インスタンス間での転送機能（IP フォワーディング）を無効にする。 |
| 対策を実施しない場合のリスク | 意図しないインスタンスに対してデータパケットの転送が行われることで、データの損失や漏えいにつながる可能性がある。 |
| 設定参考資料 | （GCP）4.6 |

Azure

1. Azure Managed Disks の利用

| | |
|---|---|
| 対策の内容 | Azure Managed Disks（Azure の仮想マシンで使用されるディスク領域機能）を利用し、仮想マシンで使用されるディスク領域の暗号化を実施する。 |
| 対策を実施しない場合のリスク | 暗号化が実施されないことで、保存されているデータの安全性が低下してしまう可能性がある。 |
| 設定参考資料 | （Azure）7.1 |

2. Azure Virtual Machine 拡張機能の管理

| | |
|---|---|
| 対策の内容 | 組織として承認された拡張機能（Azure Virtual Machine 上で展開後の構成、自動化タスクを提供する小さなアプリケーション）のみがインストールされていることを確認する。 |
| 対策を実施しない場合のリスク | 拡張機能に脆弱性が発見された際、当該拡張機能を利用していることを組織が把握していない場合、適切な処置がなされず、攻撃者による不正アクセスに利用され、データの漏えいやサービス不能等につながる可能性がある。 |
| 設定参考資料 | （Azure）7.4 |

### 4.1.5 ストレージ

クラウドサービスのストレージは手軽に利用を開始することが可能であり、データに対する柔軟な冗長化のオプションや低遅延によるデータ転送等、利便性の高い機能や設定が提供されていることも多い。

一方で、利用するストレージの仕様を理解していないことによる設定ミスや、初期設定の見落とし等によるセキュリティ設定の不備といったセキュリティインシデントの発生が多く、重要な情報の外部流出という結果を招く可能性がある。したがって、クラウドサービスのストレージを利用するにあたっては、利用用途を明確にするとともに十分なセキュリティ対策を実施する必要がある。

(1) 匿名/公開アクセスの禁止

| | |
|---|---|
| 対策の内容 | 利用者の認証を必要としないアクセス(匿名/公開アクセス)が必要ない場合は、当該設定を無効化する。 |
| 対策を実施しない場合のリスク | 利用者の認証を必要としないアクセス(匿名/公開アクセス)を許可してしまうと、インターネットから誰でもストレージにアクセスできてしまうため、情報の漏えいや不正利用等につながる可能性がある。 |
| 設定参考資料 | (AWS) 2.1.5<br>(GCP) 5.1<br>(Azure) 3.5 |

(2) ストレージアクセスの通信設定

| | |
|---|---|
| 対策の内容 | ストレージに対しての通信が、https で暗号化されるようにする。 |
| 対策を実施しない場合のリスク | ストレージに対して暗号化されていない通信でアクセスすることで、通信内容が盗聴される可能性がある。 |
| 設定参考資料 | (Azure) 3.1 |

(3) 各クラウドサービスにおいて考慮すべき設定

AWS

1. Amazon RDS の暗号化

| | |
|---|---|
| 対策の内容 | Amazon RDS (Amazon Relational Database Service) を使用する場合、暗号化を有効にする。 |
| 対策を実施しない場合のリ | 暗号化が実施されないことで、保存されているデータの安全性が低下してしまう可能性がある。 |

| | |
|---|---|
| スク | |
| 設定参考資料 | （AWS）2.3.1 |

2. MFA Delete の有効化

| | |
|---|---|
| 対策の内容 | S3 バケットで MFA Delete（バージョン ID を指定する削除操作時に多要素認証を必須とする設定）を有効にする。<br>バージョン ID とは、バージョニングで用いられる、ファイルごとに付与される ID のこと。この ID により、ファイルを上書き・削除する際にも元のファイルを保持することで誤った削除を防止する。 |
| 対策を実施しない場合のリスク | バージョン ID を指定する削除操作は、完全にオブジェクトを削除することが出来てしまうため、多要素認証を用いた承認プロセスを設けないと誤ってデータを紛失する可能性がある。 |
| 設定参考資料 | （AWS）2.1.3 |

3. Amazon EBS の暗号化

| | |
|---|---|
| 対策の内容 | Amazon EBS（AWS 上で提供されているストレージサービス）の暗号化を有効にする。 |
| 対策を実施しない場合のリスク | 暗号化が実施されないことで、保存されているデータの安全性が低下してしまう可能性がある。 |
| 設定参考資料 | （AWS）2.2.1 |

Azure

1. ストレージアカウントのアクセスに使用する認証情報の管理

| | |
|---|---|
| 対策の内容 | ストレージアカウント（Azure における Azure Storage の管理単位のこと）において、定期的に認証情報の再生成を行う。 |
| 対策を実施しない場合のリスク | ストレージアカウントの認証情報が漏えいした場合に悪用される可能性が高くなる。 |
| 設定参考資料 | （Azure）3.2 |

2. 制限付きアクセス権の有効期限設定

| | |
|---|---|
| 対策の内容 | Azure Storage（Azure で提供されるストレージ機能）のリソースへの制限付きアクセス権限を付与する際は、指定した期間のみとする。 |

| | |
|---|---|
| | （Shared Access Signature（SAS）トークンの有効期間をできるだけ短く設定する必要がある） |
| 対策を実施しない場合のリスク | 不必要に長期間の権限を設定すると、攻撃者に利用され、ストレージに保存されているデータの漏えいや改ざんにつながる可能性がある。 |
| 設定参考資料 | （Azure）3.4 |

3. 論理削除機能の有効化

| | |
|---|---|
| 対策の内容 | Azure Storage の「論理的な削除」を有効にすることで、データ消去時の復元が可能となるようにする。 |
| 対策を実施しない場合のリスク | 利用者が誤って削除コマンドを実行する、あるいは攻撃者が故意に削除コマンドを実行することで、データが消失する可能性がある。 |
| 設定参考資料 | （Azure）3.8 |

### 4.1.6 データベース

クラウドサービスでデータベースを構築するためには、仮想マシンにデータベースソフトをインストールする方法に加えて、クラウドサービス事業者が提供するサービスを利用する方法がある。目的や用途に応じて様々な構成が考えられるが、特に後者については、設定等の容易さというメリットがある。ただし、使用するクラウドサービスによって、提供されているデータベースサービスの種類や設定内容等が異なる。そのため、クラウドサービス事業者が提供するデータベースサービスを利用する際には、どのような種類のサービスが利用できるのか、また構築しようとしているシステムの要件に鑑みた考慮事項はないか等を事前に検討することが重要となる。なお、クラウドサービス事業者が提供するデータベースのサービス例は以下の通り。

- リレーショナルデータベース型：Amazon RDS、Azure SQL Database、Cloud SQL
- データウェアハウス型：Amazon Redshift、Azure Synapse Analytics、BigQuery
- NoSQL 型：Amazon DynamoDB、Azure Cosmos DB、Datastore
- キャッシュ型：Amazon ElastiCache、Azure Cache for Redis

データベースの利用に際しては、不正な操作によってデータを窃取、消去あるいは改ざんされるという脅威が存在する。このような脅威に対する一般的なセキュリティ対策として、以下の実施を検討する必要がある。

- ファイアウォール等を用いたり、ネットワークを分離したりしてデータベースへのアクセス自体をできる限り制限するための「アクセス制御」
  (例)
  - SSL接続の有効化（Azure　4.3.2）（GCP　6.4）
  - データベースの公開設定（GCP　6.5）
- データ漏えいや改ざん等を防止するための暗号化等の「データ保護」
  (例)
  - データベースの暗号化設定（Azure　4.1.2）
- 不正アクセスを検知するためのセッションの詳細情報を取得する等の「ログの取得」
  (例)
  - サーバへの接続試行のログ取得設定（GCP　6.2.3）（Azure　4.3.4）
  - セッション詳細情報のログ取得設定（GCP　6.2.4）（Azure　4.3.5）
  - 監査機能の有効化（Azure　4.1.1）
  - 監査ログの保持期間設定（Azure　4.1.3）

なお、上記の対策以外にも、使用するデータベースや構成に応じて必要となる設定内容が異なるため、各クラウドサービス事業者の公式ドキュメント等を参考にしながら使用するデータベースにおける必要なセキュリティ設定を行う必要がある。

## 4.2 SaaS において設定すべきセキュリティ対策

SaaS は業務等で利用する様々なアプリケーションの機能をサービスとしてネットワーク経由で利用するモデルである。従来、アプリケーションはオンプレミスのサーバ上で構築し、自組織にて管理することが主流であったが、近年では、導入が手軽であることや、柔軟なプラン設定によりコスト削減を行えること等のメリットを背景に SaaS の普及が進んでいる。その結果、自組織のサーバでアプリケーションの管理を行うことなく、クラウドサービス事業者が SaaS で提供するアプリケーションを利用する組織も増加している。

オンプレミスで自らアプリケーションの構築を実施する場合、アプリケーションの管理に関する一連の事項は自らの組織で責任をもって実施する必要がある。一方、SaaS では、クラウドサービス事業者が提供するアプリケーション、OS・ミドルウェアのアップデートやサーバ等のメンテナンス等はクラウドサービス事業者の責任で実施される。そのため、利用者はクラウドサービスを動かす基盤についてのセキュリティ対策を実施する必要はない。ただし、SaaS の利用者において設定可能な項目については、利用者がセキュリティ対策を実施する必要がある。

このように SaaS においては、基盤等に関するセキュリティ対策の多くをクラウドサービス事業者が実施するが、アカウントや認証に関する管理、権限の設定、データの管理等クラウドサービスを利用する上で利用者が設定しなければならないセキュリティ対策については利用者の責任で行う必要がある。

また、「3.1 クラウドサービスの特徴」に記載のとおり、クラウドサービスは頻繁に仕様変更や機能追加が行われることがあり、利用者のセキュリティに関する設定に影響を与える可能性がある。そのため、最新の情報を収集するとともに、セキュリティに関する設定や業務への影響等の有無を確認することが特に重要である。また、クラウドサービスを利用する際に選択するリージョンやゾーンによっては、国内法以外の法令及び規制が適用されるリスクが存在するため、選択できるリージョンやゾーンを制限することや利用者が管理する暗号鍵を用いてデータを暗号化するなどの対策も重要となる。

なお、SaaS として提供されるサービスの種類は、グループウェア、ビジネスチャット、Web 会議ツール等、その用途によって多岐にわたる。また、用途が同様のサービスであっても、セキュリティ対策のための設定項目等の詳細については個別のサービスによって異なることが多い。以上のような理由から、本項においては設定すべきセキュリティ対策をクラウドサービスごとに分けて記載する。本書の対象としていない SaaS については、クラウドサービス事業者が提供している公式ドキュメント等を参考に、必要なセキュリティ対策を講ずる必要がある。

### 4.2.1 Google Workspaceにおいて設定すべきセキュリティ対策

Google Workspaceとは、Gmail、Googleカレンダー、Googleドライブ等のサービスをパッケージングしたグループウェアである。クラウドサービスにファイルを保存・共有し、複数の利用者によって同時に作業が可能である等、コラボレーションに優れている。一方で、複数利用者との共同作業に際しての設定ミス等によりデータの漏えい等が発生する可能性があるため、外部公開・共有設定等のセキュリティ設定を適切に行う必要がある。

また、記載事項以外にも検討することが望ましい事項については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

https://support.google.com/a/answer/7587183

https://support.google.com/a#topic=4388346

(1) 認証に関するセキュリティ強化

Google Workspaceでは、管理者アカウントにて管理コンソールへログインすることにより、アカウントの管理やセキュリティ設定、サービス（Gmailや Googleカレンダー等）の設定を行うことができる。また、利用者としてサービスを利用する際には利用者用のアカウントにてログインを行う。

本来 Google Workspaceを利用する権限を持たない者によるなりすましや不正アクセス等によりアカウントの乗っ取りが成功した場合、データの漏えいや改ざん等につながる可能性があることから、各アカウントの認証に関するセキュリティ対策が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

※（）内は参考とすべきCIS Benchmarks の項番。

- 管理者アカウントでの多要素認証プロセスを必須にする。(Google Workspace 1.1)
- パスワードポリシーは強力なパスワードの使用が強制されるように設定する。（Google Workspace 1.4)
- セッションの継続時間を設定する。（通常の業務環境とは異なる環境下で作業している利用者に対して、セッションの継続時間を短くすることで、機密性の高いリソースにアクセスできる時間を制限する。）（Google Workspace 1.6)

また、上記以外にもアカウントの不正使用を防止、監視するためにレポートの定期的な確認や管理者へのメールアラート設定等も検討することが望ましい。これら設定については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

管理者アカウント

https://support.google.com/a/answer/9011373

利用者用のアカウント

https://support.google.com/a/answer/7587183?hl=ja&ref_topic=7559287#Accounts

(2) アプリケーションの権限設定

Google Workspace では、データを安全に共有するために、利用者がサードパーティのアプリケーションや SNS 等に対して、Google アカウントで利用できるさまざまな機能へのアクセス権を付与することができる。

例えば、スケジュールをシェアすることが出来るサードパーティのアプリケーションの場合、空き時間のあるメンバーを当該アプリケーションにて表示するために、Google カレンダーへのアクセスが求められる。また、サードパーティのメールアプリケーションから Google Workspace で管理しているメールアドレスを自動的に補完するような場合、ディレクトリデータ（Google コンタクトのディレクトリ内に登録されている組織内外の連絡先データ等）へのアクセスが求められる。

しかし、安全性の低いサードパーティのアプリケーション等は、OAuth 等最新のセキュリティ規格を使用していないことからアカウントの流出等のリスクが高い。また、データへのアクセスについても、無制限にアクセスを許可すると本来アクセス権限を有していない第三者から不正アクセスをされ、外部への漏えいにつながる可能性があることから、適切な権限の設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- 安全性の低いサードパーティのアプリケーションからのアクセスを無効にする。（Google Workspace 2.1）
- ディレクトリデータへのアクセスを制限する。（無制限にアクセスできないようにする。）（Google Workspace 2.2）

また、上記以外にもサードパーティのアプリケーションや SNS 等と Google アカウントとの連携をする場合は追加の設定等も検討することが望ましい。これら設定については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

Google でサードパーティ製のアプリやサービスとのデータ共有を安全に行う方法

https://support.google.com/accounts/answer/10130420?hl=ja

(3) Google カレンダーの外部共有設定

Google カレンダーでは、会議および予定の調整を行うことが出来る。また、複数人での

利用を想定して設計されたサービスであるため、スケジュールの共有を容易に行うことが出来る。

しかし、組織外部とGoogleカレンダー情報を共有する際に、誤操作により情報の漏えいにつながる可能性がある。Googleカレンダーの情報には、会議の参加者情報や場所、会議内容の説明等が含まれるが、説明に重要な情報が記載されている場合もあることから、組織外部とGoogleカレンダー情報を共有する際のセキュリティ対策が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- Googleカレンダーの外部共有オプションを設定し、共有する情報をコントロールする。（共有する情報を「空き時間情報のみ（予定の詳細は非表示）」と設定することで、Googleカレンダーで予定が追加されている時間と空いている時間を確認することはできるが、予定の名前や詳細を表示することはできないようにする）（Google Workspace 3.1、3.3）
- 組織外部のゲストユーザーを招待する際に警告を表示する。(Google Workspace 3.2)

また、上記以外にも組織内部のGoogleカレンダーの共有範囲の設定や、アドオンの利用許可設定等も検討することが望ましい。これら設定については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

Google Workspace管理者ヘルプ（Googleカレンダー）

https://support.google.com/a/topic/9201?hl=ja&ref_topic=9197

(4) Googleドライブのセキュリティ設定

Googleドライブでは、パソコンやスマートフォン、タブレット等のデバイスを使い、様々なデータをどこからでも簡単に共有し、またバックアップを行うことが出来る。

しかし、Googleドライブの共有設定が適切に行われないことで、操作ミスや意図的な行為により本来権限のないファイルにアクセスが可能となり、格納している情報の漏えいにつながる可能性がある。したがって、アクセス制御等の適切なセキュリティ設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。（Google Workspace 4.1）
- ファイルの外部公開や、組織外との共有を制限する。(Google Workspace 4.2、4.3)
- 共有ドライブの設定変更を管理者のみに制限する。（Google Workspace 4.6）

- 共有ドライブのファイルへのアクセスは管理者が許可した利用者のみに制限する。（Google Workspace 4.7）
- ファイルへのリンクの共有方法を制御する。（「リンク共有のデフォルト」をオフにすることで、ファイルの所有者とその所有者がファイルを共有している利用者だけがファイルにアクセスできるようにする）（Google Workspace 4.8）

また、上記以外にもGoogleドライブ内ファイルのデバイス間の同期設定等も検討することが望ましい。これら設定については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）
Google Workspace管理者ヘルプ（ドライブ）
https://support.google.com/a/topic/2490075?hl=ja&ref_topic=9197

(5) Gmailのセキュリティ設定

Google WorkspaceのGmailでは、組織のドメインを使用したメールアドレスを使用してメールの送受信を行うことが出来る。

しかし、メールを介した攻撃やなりすましにより、データの漏えいや改ざん等につながる可能性があり、フィッシングやマルウェアに対する保護等の設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- Gmailにおける委任機能（メールの閲覧、送信、削除の実施権限を他の利用者に委任することができる機能）の利用を管理者に限定する。（Google Workspace 5.1）
- Gmail labs（正式な機能ではないが、Gmail上で試験的に提供されている機能）が有効になっていないことを確認する。（Google Workspace 5.2）
- DKIMを設定する。（Google Workspace 5.3、5.14）
- メールを検疫しスパムメール等を隔離する設定を行う。（Google Workspace 5.4）
- 悪意のある可能性のある添付ファイルからの保護設定を行う。（Google Workspace 5.5～5.7）
- 悪質な可能性のあるリンクをクリックした際に警告を表示するよう設定を行う。（Google Workspace 5.8～5.10）
- 類似したドメイン名を利用したドメイン偽装メールや、認証されていないなりすましメールを受信した際、迷惑メールフォルダへの移動や警告を表示するよう設定を行う。（Google Workspace 5.11～5.13、5.15）
- 利用者からのすべての送信メールがGoogle Workspaceの送信ゲートウェイを経由するよう設定を行う。（Google Workspace 5.18）

また、上記以外にもメールの暗号化等も検討することが望ましい。これら設定については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

Google Workspace 管理者ヘルプ（Gmail の高度なセキュリティ）

https://support.google.com/a/topic/2683828?hl=ja&ref_topic=2683865

### 4.2.2 Microsoft 365 において設定すべきセキュリティ対策

Microsoft 365 とは、デスクトップアプリケーションの Office 365、ストレージサービスの OneDrive、コラボレーションツールの Microsoft Teams 等がパッケージングされたサービスである（使用できる内容は契約するプランに応じて異なる）。

場所を問わず様々な業務が可能となる一方で、外部からの不正アクセスやデータの漏えいへの対策として、セキュリティ設定を適切に行う必要がある。

なお、 Microsoft 365 には E3、E5 等複数のプランがある。プランによって設定できる対策に違いがあり、E3 に比べて E5 の方が脅威対策等、提供される機能が多くなっている（例えば、Microsoft Teams のチャットにおけるデータ損失防止（DLP）機能は E5 のみ）。本書では基本的なセキュリティ対策を記載するという観点から、「Microsoft 365 E3」にて対策可能なものを記載する。

また、記載事項以外にも検討することが望ましい事項については、クラウドサービス事業者が提供しているドキュメント等を参照すること。

（参考）

https://docs.microsoft.com/ja-jp/microsoft-365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide

#### (1) Azure AD の認証に関するセキュリティ強化

Microsoft 365 サブスクリプションには Azure AD サブスクリプションが含まれており、オンプレミスの Active Directory と統合して、アカウントとパスワードの同期や、シングルサインオンの設定を実施することが出来る。

Azure AD は、インターネットを経由したアクセスによって認証情報を管理する。その際、設定ミス等により多要素認証を回避されることで権限を持たない者によるなりすましが成功し、データの漏えいや改ざん等につながる可能性があることから、アカウントの認証に関するセキュリティ対策が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

※（）内は参考とすべき CIS Benchmarks の項番。

- 管理者権限を持つすべての利用者に多要素認証を設定する。(Microsoft 365 1.1.1)
- グローバル管理者が１人しかいない場合、内部不正の発見が困難となることから、グローバル管理者を複数人設定する。（Microsoft 365 1.1.3）
- 利用者自身によるパスワードリセットを有効にする。（Microsoft 365 1.1.4）
- Azure AD のパスワード保護を有効にする。（強力なパスワードの使用が強制されるようにする）（Microsoft 365 1.1.5）
- 多要素認証をサポートしていない Basic 認証である「レガシー認証」を遮断する。（Microsoft 365 1.1.6）

- オンプレミスの Active Directory と Azure AD のパスワードハッシュを同期し利用者の持つパスワードの数を 1 つにすることで漏えい等の機会を低減する。（Microsoft 365　1.1.7）
- Azure AD での「セキュリティの既定値群」を有効化する。(Microsoft 365　1.1.12)

※ セキュリティの既定値群とは、「管理者に対して多要素認証を必須にする」等、既に構成されているセキュリティ設定のこと。

(2) 各サービス・アプリケーションの認証に関するセキュリティ強化

Microsoft 365 の各サービス・アプリケーションの認証において、Basic 認証が使用されている場合、多要素認証が使用できない状態となっている可能性がある。そのため、本人以外のログインが容易になり、なりすましや不正アクセス等によりアカウントの乗っ取りが成功し、データの漏えいや改ざんにつながる可能性があることから、適切な認証の設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- Exchange Online において「先進認証」（前述の「レガシー認証」と比較して、より安全に利用者の認証を行う認証方法）を有効にし、メール（Exchange）で多要素認証等の強力な認証機能が利用できるようにする。（Microsoft 365　1.2）
- Skype for Business Online において「先進認証」を有効にし、コラボレーションツール（Skype for Business Online）で多要素認証等の強力な認証機能が利用できるようにする。（Microsoft 365　1.3）
- SharePoint において「先進認証」を有効し、データ共有アプリケーション(SharePoint)で多要素認証等の強力な認証機能が利用できるようする。（Microsoft 365　1.4）
- Office365 の利用者の認証にはできる限り多要素認証を設定する。知識認証のみの認証とする場合、パスワードの有効期限を設定しないことが望ましい（利用者に定期的なパスワード変更を求めることは、実際にはパスワードの安全性を低下させる可能性がある）。（Microsoft 365　1.5）

(3) アプリケーションの権限設定

Microsoft 365 では、利用者は Microsoft Word、Excel、PowerPoint の各アプリケーションにアドインをインストールすることが出来る。アドインによって、ドキュメントの編集等を実施する際の利便性が高まる。一方で、脆弱性のあるアドインが使用されることで、本来意図していない操作が実施され、データの改ざんや漏えいが発生する可能性がある。

また、Microsoft 365 において提供されるサービスである Forms では、アンケート作成を容易に行うことが出来る。ただし、攻撃者が Forms で正規のアンケートサイトを見せかけた偽のウェブページを作成した上で、フィッシングメールにて当該ページへの誘導を行い、個人情報や認証情報を収集する可能性がある。

さらに、Microsoft 365 において提供されるサービスである Sway では、レポートやプレゼンテーション等をインターネット上で作成し、共同編集をすることが出来る。ただし、共有設定の誤操作によって、プレゼンテーション等に含まれる重要情報を外部へ漏えいしてしまう可能性がある。

上記のようなセキュリティに関する問題を防止するために、Microsoft 365 において提供されている各種アプリケーションを利用する際は、適切な権限設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- 組織で未確認の脆弱性を含む可能性のあるアドインが利用者によってインストールされるのを防ぐために、利用者による Word、Excel、PowerPoint アドインのインストールを制限する。（Microsoft 365　2.9）
- Forms の内部フィッシング対策機能(フィッシングの試みをスキャンする保護機能)を有効にする。（Microsoft 365　2.10）
- Sway の組織外への共有機能を無効にする。（Microsoft 365　2.11）

(4) データ管理設定

Microsoft 365 では、各種アプリケーションを用いて組織内外の関係者とデータを共有することが出来る。しかし、これらのデータの管理方法を誤ると、データが意図せず削除されてしまったり、意図していない相手にデータを公開してしまったりする可能性がある。

このようなデータ管理に関する事故を防止するために、適切なデータ管理設定を行う必要がある。

以下に設定すべき基本的なセキュリティ対策を記載する。

- データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。（Microsoft 365　3.4）
- Microsoft Teams の会議を録画する場合、録画データが OneDrive あるいは SharePoint に保存されるようにする。(録画データが OneDrive あるいは SharePoint に保存されることで、事前に許可された者にのみデータが公開されるようになる)（Microsoft 365　3.8）

(5) メール（Exchange）のセキュリティ設定

Microsoft 365 が提供する Exchange では、メールの送受信を行うことが出来る。

ただし、メールを介したマルウェア攻撃やなりすましにより、データの漏えいや改ざんが発生する可能性があり、フィッシングやマルウェアに対する保護等の設定が必要となる。

以下に設定すべき基本的なセキュリティ対策を記載する。

- マルウェアが含まれている可能性がある特定の実行可能ファイル（.exe 等）を遮断

する。（Microsoft 365　4.1）

- スパム対策を設定する。（Microsoft 365　4.2）
- 攻撃者によるデータの流出や他の利用者への攻撃に悪用されないように、メール転送の設定を行う。（Microsoft 365　4.3、4.5）
- DKIM を設定する。（Microsoft 365　4.11）
- SPF を設定する。（Microsoft 365　4.12）
- DMARC を設定する。（Microsoft 365　4.13）
- マルウェアを送信した組織内の利用者への通知を有効にする。（Microsoft 365　4.14）

(6) 監査ログの設定

Microsoft 365 が提供している監査ログ機能では、各種アクティビティのログの確認や検索を行うことができ、例えば、「利用者が特定のドキュメントを表示したか」、「メールボックスからアイテムを削除したか」等を確認することが出来る。

これらの監査ログに関する機能の多くは初期設定で有効になっているが、適切な設定となっている旨については利用者が自ら確認することが重要である。

以下に設定すべき基本的なセキュリティ対策を記載する。

- Microsoft 365 の監査ログ検索を有効にする。（Microsoft 365　5.1）
- メールボックス監査を有効にする。（Microsoft 365　5.2）
- 設定変更やマルウェアの検出等のレポートを定期的に確認する。（Microsoft 365　5.3、5.5～5.11、5.14）
- 不要なゲストユーザーが存在していないかを定期的に確認する。（Microsoft 365　5.15）

(7) ストレージの有効期限設定

Microsoft 365 の SharePoint では、ストレージの外部共有機能を使用することで組織内の利用者が組織外の利用者とデータを共有することが出来る。

ただし、アカウントが窃取された場合、攻撃者が外部に共有リンクを送信することでデータへ不正にアクセスされてしまう。このような不正アクセスの被害拡大を防止するために設定すべき基本的なセキュリティ対策を以下に記載する。

- 外部共有リンクの有効期限を設定する。（Microsoft 365　6.3）

(8) モバイルデバイスの管理

Microsoft 365 の Intune では、モバイルデバイスとモバイルアプリケーションの管理を行うことが出来る。例えば、iOS/iPadOS デバイスや、Android デバイス等の安全な管理や、

デバイスとアプリが組織のセキュリティ要件に準拠していることの確認を行うことが出来る。

以下に設定すべき基本的なセキュリティ対策を記載する。

- モバイルデバイス管理ポリシーの設定（Microsoft 365　7.1）
- モバイルデバイスでのパスワードの再利用を禁止する。（Microsoft 365　7.2）
- モバイルデバイスでのパスワードを無期限に設定する。（Microsoft 365　7.3）
- ジェイルブレイク等がされたモバイルデバイスからの接続を制限する。（Microsoft 365　7.4）
- モバイルデバイスに複雑なパスワードを要求する。（Microsoft 365　7.6）
- モバイルデバイスが未使用時にロックされるように設定する。(Microsoft 365　7.7）
- モバイルデバイスの暗号化を有効にする。（Microsoft 365　7.8）
- モバイルデバイスのロック解除時に複雑なパスワードを要求する。（Microsoft 365　7.9、7.10）
- モバイルデバイスにアンチウイルスソフトを導入し、ファイアウォールを有効にすることを要求する。（Microsoft 365　7.11）
- モバイルデバイスのロックを解除するために、パスワードの使用を義務付ける。（Microsoft 365　7.13）

# 5章　クラウドサービスの事故事例

この章では、クラウドサービスのセキュリティ対策に関する理解を深めるため、近年増加しているクラウドサービスの事故について、代表的な事例の概要を解説する。一般に、クラウドサービスを使った情報システムにおいてインシデントが発生する場合、責任共有モデルに基づき、事業者側の責任範囲に起因するケース、利用者側の責任範囲に起因するケース、両者にまたがるケースなどが考えられるが、本章では利用者側の責任範囲（利用者で設定したセキュリティ設定・構成）に起因する事例について記載する。また、これら事例の原因等に鑑みて、４章で記載したセキュリティ対策を実施することで、当該事例における脅威をどのように防止・軽減できるかについても記載する。

なお、事例は、PaaS/IaaS に関連するものと、SaaS に関連するものについてそれぞれ記載する。また、各解説は実際に発生した事例を参考に記載しているものの、原因や対策等の重要な点をより有効に理解するために、一部推測等が含まれている場合がある。

各事例について、以下の３つの項目を記載する。

事例の概要

クラウドサービスに関連して発生したセキュリティ事故事例の発生状況や被害等の概要。

考えられる要因

当該事故が発生する要因と考えられる、クラウドサービスのセキュリティ設定に関する不備等の概要。

有効な対策の例

４章に記載した対策のうち、各事例の防止や被害の軽減等に有効であると考えられる対策。なお、本箇所に記載する対策のみを実施することで、類似の事例を完全に防止することができるとは限らないことに留意すること。

【PaaS/IaaS に関連する事故事例】

## 事例 1：外部からアクセス可能なネットワークポートを使用した不正アクセス

事例の概要

ある組織では、仮想マシンを用いて外部向けウェブサイトを構築していた。その際、仮想マシンへのアクセス可能な RDP や SSH のネットワークポートへの通信を制限しないままでウェブサイトを運用していた。更に、仮想マシンへアクセス可能な管理者アカウントは脆弱なパスワードを使用していた。また、ウェブサイトに関連するシステムへの外部からのアクセスログについて、初期設定から変更せずに取得していた。

ある日、外部に公開していた RDP のネットワークポート経由でウェブサイトのシステムへの不正アクセスが発生し、顧客情報を含む大量の情報が漏えいした。また、システムに関連するログの一部が保存されておらず、事故発生後の調査が不十分となった。

考えられる要因

- 仮想マシンの管理者アカウントの資格情報に一般的なアカウント名（例えばよく知られている Administrator 等を使用）や脆弱なパスワードを使用しており、強固な認証方式を採用していなかったとともに、不要なアカウントの管理がなされていなかった。
- 業務上不要で、本来はアクセス制御しておくべきネットワークポートが不適切に広範囲に開放されており、外部からの不正アクセスが容易な状態となっていた。
- 外部向けウェブサイトで利用しているアプリケーション、仮想マシン、ネットワークにおいて、ログ取得に関する設定が不十分だったため、一部のログが適切に取得されていなかった。あるいは、ログの取得はされていたものの、適切な管理のための設定が実施されていなかった。

有効な対策の例

本書 4.1 に記載の以下対策が有効と考えられるが、機能面の対策以外の観点も考慮し検討を行う必要がある。

- 4.1.1(7)　すべてのアカウントへのパスワードポリシーの適用
- 4.1.1(10)　アカウント・権限・認証情報の定期的な見直し
- 4.1.2(1)　ログの有効化及び取得
- 4.1.2(2)　ログの一元管理
- 4.1.2(3)　ログの保護
- 4.1.2(4)　ログの監視/通知の設定
- 4.1.4(3)　攻撃対象となるネットワークポートへのアクセス制限

### 事例 2：システム構築時に使用した管理者アカウントの認証情報の漏えい

事例の概要

ある組織では、PaaS/IaaS を用いて業務システムを構築しており、当該システムの構築時に管理者アカウントを複数使用していた。その後、一部の管理者アカウントは担当者の異動により不要となったが、無効化されないままの状態で残存していた。また、当該管理者アカウントは、本来は付与する必要のない機微な情報の編集や削除等の非常に強い権限を有していた。さらに、当該管理者アカウントは ID とパスワードによる知識認証のみによってログインできるようになっており、パスワード長の設定はしていなかった。

その後、不要となった管理者アカウントの ID 及びパスワードが外部に漏えいし、当該認証情報を用いた、業務システムへの不正アクセスが行われた。その結果、データの不正な閲覧やリソースの不正使用が発生した。

考えられる要因

- 業務上必要な範囲を超えた権限を管理者アカウントに付与していた。
- アカウントの要否や付与されている権限に関して、定期的な見直しが実施されていなかった。
- パスワード長が設定されていない等、管理者アカウントに関するパスワードポリシー設定が不適切であった。
- 管理者アカウントへのログイン時に、多要素認証が利用されていなかった。

有効な対策の例

本書 4.1 に記載の以下対策が有効と考えられるが、機能面の対策以外の観点も考慮し検討を行う必要がある。

- 4.1.1(2)　管理者アカウントに対する多要素認証の利用
- 4.1.1(4)　必要最低限の管理者権限の割当て
- 4.1.1(7)　すべてのアカウントへのパスワードポリシーの適用
- 4.1.1(10)　アカウント・権限・認証情報の定期的な見直し

【SaaS に関連する事故事例】

## 事例 3：意図しないファイル共有

事例の概要

ある組織では、SaaS のオンラインストレージを活用して組織の特定の担当者とファイル共有を実施している。セキュリティに関する設定を特に意識せずに利用していたところ、要機密情報を含む重要なファイルが、本来意図していない組織内及び組織外の第三者によって閲覧できる状態であった。

考えられる要因

- ファイル共有のアクセス制限が不適切であり、特定の URL にアクセスすれば任意の第三者が当該ファイルを閲覧できるようになっていた。
- データ損失防止（DLP）のための設定が不適切であった。

有効な対策の例

本書 4.2 に記載の以下対策が有効と考えられるが、機能面の対策以外の観点も考慮し検討を行う必要がある。

[Google Workspace]

- 4.2.1(4)　Google ドライブのセキュリティ設定
  - データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。（Google Workspace 4.1）
  - ファイルの外部公開や、組織外との共有を制限する。（Google Workspace 4.2、4.3）
  - 共有ドライブの設定変更を管理者のみに制限する。（Google Workspace 4.6）
  - 共有ドライブのファイルへのアクセスは管理者が許可した利用者のみに制限する。（Google Workspace 4.7）
  - ファイルへのリンクの共有方法を制御する。（「リンク共有のデフォルト」をオフにすることで、ファイルの所有者とその所有者がファイルを共有している利用者だけがファイルにアクセスできるようにする）（Google Workspace 4.8）

[Microsoft 365]

- 4.2.2(4)　データ管理設定
  - データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。（Microsoft 365　3.4、3.5）
- 4.2.2(7)　ストレージの有効期限設定
  - 外部共有リンクの有効期限を設定する。（Microsoft 365　6.3）

## 事例 4：メール経由でのマルウェア感染

事例の概要

自組織で利用している SaaS のメールサービスで、外部の組織から窃取されたメールアカウント名やメール文面等の情報を用いたなりすましメールを受信した。なりすましメールには特定の実行可能ファイル（.exe)が添付されていた。

送信元アドレスのドメインが正規のドメインと異なっていたものの、メールアカウント名やメール文面等の情報が実際にやりとりしたメールと類似していたため、なりすましメールであると気が付けずに添付されたファイルを開いてしまった。その結果、利用しているデバイスがマルウェアに感染し、重要な情報の漏えいが発生した。

考えられる要因

- 送られてきたメールに対しドメイン認証に基づくなりすまし判定を行い、なりすましと判定した場合の受信拒否や隔離、受信者への注意喚起等の対応がされず、受信者が正規のメールであると判断してしまった。（なりすましメールであることに気がつくことができなかった要因）
- 受信したメールに添付されていたファイルを検閲する機能が有効化されておらず、受信者が悪意のあるマクロ等を含むファイルを開き実行できる状態であった。（デバイスがマルウェアに感染してしまった要因）

有効な対策の例

本書 4.2 に記載の以下対策が有効と考えられるが、機能面の対策以外の観点も考慮し検討を行う必要がある。

[Google Workspace]

- 4.2.1(5)　Gmail のセキュリティ設定
  - DKIM を設定する。(Google Workspace 5.3、5.14)
  - メールを検疫しスパムメール等を隔離する設定を行う。(Google Workspace 5.4)
  - 悪意のある可能性のある添付ファイルからの保護設定を行う。(Google Workspace 5.～5.7)
  - 類似したドメイン名を利用したドメイン偽装メールや、認証されていないなりすましメールを受信した際、迷惑メールフォルダへの移動や警告を表示するよう設定を行う。(Google Workspace 5.11～5.13、5.15)

[Microsoft 365]

- 4.2.2(5)　メール（Exchange）のセキュリティ
  - マルウェアが含まれている可能性がある特定の実行可能ファイル（.exe 等）を遮断する。(Microsoft 365　4.1)

- DKIM を設定する。(Microsoft 365　4.11)
- SPF を設定する。(Microsoft 365　4.12)
- DMARC を設定する。(Microsoft 365　4.13)

# 6章　用語定義

アルファベット順・50 音順

| | |
|---|---|
| API | Application Programming Interface の略称。ソフトウェアやプログラム等の連携のために用いるインタフェースのこと。API を用いることで、あるソフトウェア等における機能の一部を他のソフトウェア等において使用することができる。 |
| Basic 認証 | HTTP で定義されている認証方式であり、ユーザー名とパスワードを Base64 でエンコードする、簡易的な認証方法とされる。 |
| CIS Benchmarks | 米国の政府機関・企業等が協力して設立された非営利団体 CIS（Center for Internet Security）が発行するセキュリティ対策のベストプラクティス。クラウドサービスをはじめ、ネットワーク機器やデータベース、OS 等の製品毎に、セキュリティに関して望ましいと考えられる設定項目を記載している。 |
| DKIM | DomainKeys Identified Mail の略称。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメール等の迷惑メールへの対策の一つとして利用可能。 |
| DLP | Data Loss Prevention の略称。情報の紛失や外部への漏えい等を防止するための技術や仕組みのこと。 |
| DMARC | Domain-based Message Authentication, Reporting, and Conformance の略称。電子メールにおける送信ドメイン認証技術のこと。 |
| DNS | Domain Name System の略称。ドメイン名（電子計算機を識別する名称）と IP アドレスを対応付けて、自動的に変換するシステムのこと。 |
| DNSSEC | DNS 応答に添付された署名を受信側で検証することにより、正しい相手から届いた正しいデータであることを確認できるようにするための技術のこと。 |
| DNS ハイジャック | 既存のドメインを管理する権限を有していない者が、DNS サーバへの不正なアクセス等により、ドメイン名を不正に変更する攻撃手法のこと。 |
| IaaS | インターネット経由でコンピューティングリソースを提供するクラウドサービスの形態。IaaS は、サーバ、ストレージ、仮想化基盤であるハイパーバイザ等の環境を利用者に提供している。また、これらの機器を稼働させるためのネットワーク |

| | |
|---|---|
| | 設備や電源設備等の IT インフラストラクチャの整備を実施している。 |
| IDS | 通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステムのこと。 |
| IPS | サーバ装置や通信回線に対する攻撃や侵入等の不正行為を検知して阻止する仕組みのこと。 |
| OAuth | 複数のウェブサービス間で認証情報を連携するための規格。 |
| PaaS | インターネット経由でプラットフォームを提供するクラウドサービスの形態。PaaS は主にデータベースや開発フレームワーク等のミドルウェアや OS を提供している。 |
| SaaS | インターネット経由でソフトウェアを提供するクラウドサービスの形態。SaaS は、アプリケーションや、当該アプリケーションが稼働しているサーバ、ミドルウェア、ネットワーク設備等の IT インフラストラクチャを含む多くの部分をクラウドサービス事業者が提供している。 |
| SPF | Sender Policy Framework の略称。電子メールの送信元ドメインが詐称されていないかを検査するための仕組み |
| SSH キー | SSH（Secure Shell）の通信を用いてリモートアクセスを実施する際に必要となる認証情報のこと。 |
| アドイン/アドオン | アプリケーションへ機能を追加するためのプログラムのこと。 |
| アクセス権限 | アカウントやグループが仮想マシンやサービス等のリソースを利用する（プログラムの実行や、データの参照、追加、変更、削除等）資格のこと。 |
| アクセス制御 | あるアカウントやグループのアクセス権限に基づき、データやリソース等へのアクセスを認可及び制限するための仕組みのこと。 |
| オートスケーリング | クラウドサービスにおいて利用しているサーバ等の負荷に応じて、自動的に使用サーバ等の規模を増減させる機能のこと。 |
| クラウドサービス | 事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであ |

| | |
|---|---|
| | って、情報セキュリティに関する十分な条件設定の余地があるものをいう。 |
| サードパーティ | ある製品等自体の開発元・販売元ではない企業のことを指す。 |
| ジェイルブレイク | デバイスにおいてソフトウェアの実行環境に施している制限を非正規な方法で撤廃し、自由にソフトウェアを導入・実行できるようにすること。 |
| ストレージ | データを保管するシステムや装置のこと。データを保存するための領域をクラウドストレージ、あるいはオンラインストレージ等と呼ばれるサービスの形態で提供される場合もある。 |
| 脆弱性 | 機器・システムやその利用環境におけるセキュリティに関する欠陥のこと。 |
| 責任共有モデル | クラウドサービスの利用者とサービスを提供する事業者のそれぞれが、クラウドサービスを運用する上での責任を共有するという考え方 |
| 多要素認証 | 知識情報、所持情報、生体情報の３つの要素のうち２つ以上の異なる要素を組み合わせて行う認証方式のこと。MFA（Multi Factor Authentication）と呼称する場合もある。 |
| ハニーポット | 攻撃者による不正なアクセスを受けることを前提としているシステム等のこと。攻撃者を誘引し、攻撃者の行動や目的を調査するために設計される。 |
| フィッシング | 詐称した電子メール等で偽の Web サイトに誘導し、クレジット番号等の情報の入力をおこなわせ窃取する攻撃手法のこと。 |
| ブルートフォース攻撃 | 同一 ID に対してパスワードを変えながらログインを試行する攻撃のこと。総当たり攻撃とも呼ばれる。 |
| マルウェア | さまざまな脆弱性や情報を利用して攻撃をするソフトウェア（コード）の総称のこと。ウイルスのほか、ワーム、スパイウェア、スパム、トロイの木馬等さまざまな種類のマルウェアが存在している。 |
| リモートデスクトップ | 自らの手元にある機器から、RDP 等によりネットワークを経由して他のデバイスを操作するための仕組みのこと。 |
| ロードバランサ | 外部ネットワークからの大量のアクセスを一元的に管理し、複数のサーバに割り振り負荷を軽減する装置のこと。 |

# 7章　参考資料

本書における参考となる資料は以下の通り（50 音順にて記載）。

- 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　総務省
- 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 2013 年度版
  2013年　経済産業省
- クラウド重大セキュリティ脅威 11 の悪質な脅威
  2019年　日本クラウドセキュリティアライアンス
- クラウドを利用したシステム運用に関するガイダンス
  2021年　内閣サイバーセキュリティセンター
- 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル
  2019年　内閣サイバーセキュリティセンター
- 政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）
  2021年　内閣サイバーセキュリティセンター
- 政府情報システムにおけるクラウドサービスの利用に係る基本方針
  2021年　各府省情報化統括責任者（ＣＩＯ）連絡会議決定
- 政府情報システムのためのセキュリティ評価制度（ISMAP）管理基準
  2020年　内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省
- デジタル・ガバメント実行計画
  2022年　閣議決定
- デジタル・ガバメント推進標準ガイドライン
  2022年　デジタル社会推進会議幹事会決定決定

# 参考.クラウドサービスにおいて設定すべきセキュリティ対策一覧

PaaS/IaaS において設定すべきセキュリティ対策

| 対策 | | 対策の内容 | 設定参考資料 |
|---|---|---|---|
| 4.1.1 ID およびアクセス管理 | | | |
| | (1) 組織が許可したアカウントの管理 | 組織が許可したアカウントのみを利用するように管理する。例えば、個人の私的に利用しているアカウント等の利用を許可しない。 | (GCP) 1.1 |
| | (2) 管理者アカウントに対する多要素認証の利用 | 管理者アカウントに対して多要素認証を有効とし、管理者アカウントのセキュリティ強度を高める。 | (AWS) 1.5、1.10<br>(GCP) 1.2<br>(Azure) 1.1 |
| | (3) 管理者アカウントに紐づく最新の連絡先の登録と定期的な見直し | 管理者アカウントに紐づく連絡先を登録し、最新の状態を保つとともに、クラウドサービス事業者からの通知を組織内の複数人が受け取れるように設定する。 | (AWS) 1.1、1.2 |
| | (4) 必要最低限の管理者権限の割当て | 管理者権限の付与は必要最低限とし、重要な設定変更等の操作が可能となる管理者権限をむやみに使用せず、必要な操作のみを許可する権限等を付与する。 | (AWS) 1.16<br>(GCP) 1.5 |
| | (5) グループを利用した権限の設定 | 権限の設定は利用者ごとに適用するのではなく、グループの役割や与えられる権限に応じて可能な限りグループへ適用する。 | (AWS) 1.15 |
| | (6) 管理者アカウントに関する復旧手段の確保 | 管理者アカウントにアクセスできなくなった場合に備えて、確実な復旧手段を確保する（秘密の質問等）。 | (AWS) 1.3 |

| | | | |
|---|---|---|---|
| | (7) すべてのアカウントへのパスワードポリシーの適用 | 管理者アカウントに限らず、管理者権限をもたないアカウントを含むすべてのアカウントに対して、以下の例にパスワードポリシーを適用する。<br>例：パスワード長を 14 文字以上とする<br>一度利用したパスワードの再利用を禁止する<br>パスワードをリセットする際に知識認証以外の認証方法を要求する<br>パスワード変更時、利用者にパスワード変更通知を送付する<br>システムの利用者に定期的に再認証の実施を求める　等 | （AWS）1.8、1.9<br>（Azure）1.5～1.7 |
| | (8) アクセスキー、サービスアカウントキー等の適切な管理 | 各種サービスへのアクセスを認証するために作成される認証情報であるアクセスキー（AWS）やサービスアカウントキー（GCP）、API キー等は、作成することの必要性を検討するとともに、作成したキーが不正に利用されていないことの定期的な確認及びキーの更新等の管理を行う。<br>例えば、AWS の場合、AWS アカウント（ルートユーザー）は多くの高権限を持ち不正利用時のリスクが大きいため、AWS アカウント（ルートユーザー）に関連するアクセスキーは設定しない、削除する等があげられる。 | （AWS）1.4、1.11、1.13、1.14<br>（GCP）1.4、1.7、1.9～1.10、1.13～1.15 |
| | (9) 管理者アカウントと日常的に使用するアカウントの分離 | 管理者アカウントと日常的に使用するアカウントを分離し、管理者アカウントは日常業務では使用しないようにする。 | （AWS）1.7 |
| | (10) アカウント・権限・認証情報の定期的な見直し | 不要となったアカウントや権限及び認証情報を定期的に確認し、不要なアカウントや権限及び認証情報は随時削除する。 | （AWS）1.12<br>（Azure）1.3 |
| | (11) 各クラウドサービスにおいて考慮すべき設定 | | |
| | AWS | | |
| | 1.AWS サポートセンターへのアクセス設定 | AWS で発生したセキュリティインシデントの通知や対応、技術サポート等を利用できるようにする | （AWS）1.17 |

| | | | |
|---|---|---|---|
| | | ため IAM ユーザーに AWS サポートセンターへのアクセス権限を設定する。 | |
| | 2. IAM に保存されているサーバ証明書の管理 | IAM に保存されている TLS 証明書のうち、有効期限が切れた証明書については削除する。 | (AWS) 1.19 |
| | 3. IAM Access analyzer の有効化 | 利用する全てのリージョン（AWS のデータセンターが集積されている物理的ロケーション）において IAM Access analyzer（AWS におけるアクセス制御ポリシーを分析し、意図していないアクセスの可否を検出するための機能）が有効化され、リージョン内の各リソースに適用されているポリシーの分析・監視が行われていることを確認する。<br>なお、複数リージョンをまとめて有効化することはできない為、リージョンを複数利用する場合は、個別に有効化の設定を行う。 | (AWS) 1.20 |
| | GCP | | |
| | 1. サービスアカウントのロール設定 | 以下のロールを利用者に割り当てる際、プロジェクト単位で割り当てるのではなく、特定のサービスアカウントに対して割り当てる。<br>・Service Account User<br>(iam.serviceAccountUser)<br>・Service Account Token Creator<br>(iam.serviceAccountTokenCreator) | (GCP) 1.6 |
| | Azure | | |
| | 1. Azure AD 管理ポータルへのアクセス制限 | Azure AD 管理ポータルへのアクセスを管理者のみに制限する。 | (Azure) 1.15 |
| | 2. Azure AD へのデバイス追加設定 | 業務で使用するデバイス（例：PC、タブレット等）を Azure AD に追加する際に多要素認証が行われるようにする。 | (Azure) 1.20 |
| | 3. Azure AD におけるセキュリティの既定値群の有効化 | Azure AD で「セキュリティの既定値群」を有効にする。<br>※セキュリティの既定値群とは、「管理者に対して多要素認証を必須にする」等、既に構成されているセキュリティ設定のこと。 | (Azure) 1.22 |

| | | |
|---|---|---|
| 4.1.2 ログの記録と監視 | | |
| (1) ログの有効化及び取得 | ログの取得が必要となる各サービスにおいてログを取得するために必要な設定を有効化し、適切なログ取得が可能となるようにする。 | (AWS) 3.1、3.6<br>(GCP) 2.1、2.12、3.8<br>(Azure) 2.11、5.1.1、5.1.2、5.1.5、5.3 |
| (2) ログの一元管理 | 各サービスで取得するログの監視や通知をログの一元管理機能を用いて行う。 | (AWS) 3.4<br>(GCP) 2.2 |
| (3) ログの保護 | 取得したログに対してアクセス制御、改ざん防止設定を実施する。 | (AWS) 3.3<br>(GCP) 2.3<br>(Azure) 5.1.3 |
| (4) ログの監視/通知の設定 | 重要な設定変更や管理者アカウントでのログイン等、重要な操作に関するログの監視や通知を設定する。 | (AWS) 4.1～4.5、4.8、4.12～4.15<br>(GCP) 2.4～2.11<br>(Azure) 5.2.1～5.2.9 |
| 4.1.3 ネットワーク | | |
| (1) ロードバランサの接続設定 | ロードバランサの接続に用いる通信を TLS1.2 以降に設定する。 | (GCP) 3.9 |
| (2) 各クラウドサービスにおいて考慮すべき設定 | | |
| GCP | | |
| 1.レガシーネットワークの利用停止 | レガシーネットワーク（単一の IP アドレス範囲のみをもつことができるネットワーク）を利用している場合、利用を停止する。<br>なお、現在、新規でのレガシーネットワーク作成は実施できない。 | (GCP) 3.2 |
| 2.DNSSEC の有効化 | Cloud DNS（GCP 上で提供されている DNS サービス）の DNSSEC を有効にする。<br>また、DNSSEC の署名には強力な暗号化アルゴリズム（SHA-2 以降）が用いられていることを確認する。 | (GCP) 3.3～3.5 |
| Azure | | |

| | | | |
|---|---|---|---|
| | 1.Network Watcher の有効化 | Network Watcher（仮想ネットワーク内のリソースの監視等を行う機能）を有効にする。これにより、仮想マシンとデバイスの間の通信の監視やネットワークの診断、トラフィックの分析等を行う。 | （Azure）6.5 |
| 4.1.4 仮想マシン | | | |
| | (1) 最新の OS パッチの適用確認 | 仮想マシンの OS に対して最新のセキュリティパッチが適用されていることを確認する。 | （Azure）7.5 |
| | (2) 不正プログラム対策ソフトウェアの導入 | 仮想マシンの OS 上で動作する不正プログラム対策ソフトウェアを導入する。不正プログラム対策ソフトウェアを導入することにより、仮想マシンの OS 上でのアクティビティを監視し、不正プログラムの実行を検出・ブロックすることができる。 | （Azure）7.6 |
| | (3) 攻撃対象となるネットワークポートへのアクセス制限 | 外部からの不正アクセスや DDoS 攻撃等に使用される可能性のあるネットワークポートを制限する。（以下対策例）<br>例：インターネットからの RDP や SSH のアクセスについて接続元制限を行う。不要な UDP ポートを無効にする。 等 | （AWS）5.1、5.2<br>（Azure）6.1～6.3、6.6 |
| | (4) 各クラウドサービスにおいて考慮すべき設定 | | |
| | GCP | | |
| | 1.インスタンスのサービスアカウントの設定 | 初期設定のサービスアカウントを使用しない。 | （GCP）4.1、4.2 |
| | 2.インスタンス固有の SSH キーの利用 | プロジェクト共通の SSH キーではなく、インスタンス固有の SSH キーを使用する。 | （GCP）4.3 |
| | 3.OS Login の有効化 | OS Login（IAM を使用してインスタンスへの SSH アクセスを Google アカウントと連動して管理することができる機能）を有効にする。 | （GCP）4.4 |

| | | | |
|---|---|---|---|
| | 4.インタラクティブシリアルコンソール接続の無効化 | インタラクティブシリアルコンソールを用いた接続を無効にする。<br>インタラクティブシリアルコンソールとは、マウス等を用いずにテキスト入力によってインスタンスの操作を行う方法のうち、対話型の形式のものを指す。起動やネットワークの問題のデバッグ、不具合のあるインスタンスのトラブルシューティング時の利用が想定されているが、IP 許可リスト等によるアクセス制限に対応していない。 | (GCP) 4.5 |
| | 5.IP フォワーディングの無効化 | インスタンス間での転送機能（IP フォワーディング）を無効にする。 | (GCP) 4.6 |
| | Azure | | |
| | 1.Azure Managed Disks の利用 | Azure Managed Disks（Azure の仮想マシンで使用されるディスク領域機能）を利用し、仮想マシンで使用されるディスク領域の暗号化を実施する。 | (Azure) 7.1 |
| | 2.Azure Virtual Machine 拡張機能の管理 | 組織として承認された拡張機能（Azure Virtual Machine 上で展開後の構成、自動化タスクを提供する小さなアプリケーション）のみがインストールされていることを確認する。 | (Azure) 7.4 |
| 4.1.5 ストレージ | | | |
| | (1) 匿名/公開アクセスの禁止 | 利用者の認証を必要としないアクセス（匿名/公開アクセス）が必要ない場合は、当該設定を無効化する。 | (AWS) 2.1.5<br>(GCP) 5.1<br>(Azure) 3.5 |
| | (2) ストレージアクセスの通信設定 | ストレージに対しての通信が、https で暗号化されるようにする。 | (Azure) 3.1 |
| | (3) 各クラウドサービスにおいて考慮すべき設定 | | |
| | AWS | | |
| | 1.Amazon RDS の暗号化 | Amazon RDS（Amazon Relational Database Service）を使用する場合、暗号化を有効にする。 | (AWS) 2.3.1 |

| | | | |
|---|---|---|---|
| | 2.MFA Delete の有効化 | S3 バケットで MFA Delete（バージョン ID を指定する削除操作時に多要素認証を必須とする設定）を有効にする。<br>バージョン ID とは、バージョニングで用いられる、ファイルごとに付与される ID のこと。この ID により、ファイルを上書き・削除する際にも元のファイルを保持することで誤った削除を防止する。 | （AWS）2.1.3 |
| | 3.Amazon EBS の暗号化 | Amazon EBS（AWS 上で提供されているストレージサービス）の暗号化を有効にする。 | （AWS）2.2.1 |
| | Azure | | |
| | 1.ストレージアカウントのアクセスに使用する認証情報の管理 | ストレージアカウント（Azure における Azure Storage の管理単位のこと）において、定期的に認証情報の再生成を行う。 | （Azure）3.2 |
| | 2.制限付きアクセス権の有効期限設定 | Azure Storage（Azure で提供されるストレージ機能）のリソースへの制限付きアクセス権限を付与する際は、指定した期間のみとする。（Shared Access Signature（SAS）トークンの有効期間をできるだけ短く設定する必要がある） | （Azure）3.4 |
| | 3.論理削除機能の有効化 | Azure Storage の「論理的な削除」を有効にすることで、データ消去時の復元が可能となるようにする。 | （Azure）3.8 |

SaaS において設定すべきセキュリティ対策

| 対策 | | 対策の内容 | 設定参考資料 |
|---|---|---|---|
| 4.2.1 Google Workspace において設定すべきセキュリティ対策 | | | |
| | (1) 認証に関するセキュリティ強化 | 管理者アカウントでの多要素認証プロセスを必須にする。 | (Google Workspace 1.1) |
| | | パスワードポリシーは強力なパスワードの使用が強制されるように設定する。 | (Google Workspace 1.4) |
| | | セッションの継続時間を設定する。（通常の業務環境とは異なる環境下で作業している利用者に対して、セッションの継続時間を短くすることで、機密性の高いリソースにアクセスできる時間を制限する。） | (Google Workspace 1.6) |
| | (2) アプリケーションの権限設定 | 安全性の低いサードパーティのアプリケーションからのアクセスを無効にする。 | (Google Workspace 2.1) |
| | | ディレクトリデータへのアクセスを制限する。（無制限にアクセスできないようにする。） | (Google Workspace 2.2) |
| | (3) Google カレンダーの外部共有設定 | Google カレンダーの外部共有オプションを設定し、共有する情報をコントロールする。（共有する情報を「空き時間情報のみ（予定の詳細は非表示）」と設定することで、Google カレンダーで予定が追加されている時間と空いている時間を確認することはできるが、予定の名前や詳細を表示することはできないようにする） | (Google Workspace 3.1、3.3) |
| | | 組織外部のゲストユーザーを招待する際に警告を表示する。 | (Google Workspace 3.2) |
| | (4) Google ドライブのセキュリティ設定 | データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。 | (Google Workspace 4.1) |
| | | ファイルの外部公開や、組織外との共有を制限する。 | (Google Workspace 4.2、4.3) |
| | | 共有ドライブの設定変更を管理者のみに制限する。 | (Google Workspace 4.6) |
| | | 共有ドライブのファイルへのアクセスは管理者が許可した利用者のみに制限する。 | (Google Workspace 4.7) |

| | | | |
|---|---|---|---|
| | | ファイルへのリンクの共有方法を制御する。（「リンク共有のデフォルト」をオフにすることで、ファイルの所有者とその所有者がファイルを共有している利用者だけがファイルにアクセスできるようにする） | （Google Workspace 4.8） |
| | (5) Gmail のセキュリティ設定 | Gmail における委任機能（メールの閲覧、送信、削除の実施権限を他の利用者に委任することができる機能）の利用を管理者に限定する。 | （Google Workspace 5.1） |
| | | Gmail labs（正式な機能ではないが、Gmail 上で試験的に提供されている機能）が有効になっていないことを確認する。 | （Google Workspace 5.2） |
| | | DKIM を設定する。 | （Google Workspace 5.3、5.14） |
| | | メールを検疫しスパムメール等を隔離する設定を行う。 | （Google Workspace 5.4） |
| | | 悪意のある可能性のある添付ファイルからの保護設定を行う。 | （Google Workspace 5.5～5.7） |
| | | 悪質な可能性のあるリンクをクリックした際に警告を表示するよう設定を行う。 | （Google Workspace 5.8～5.10） |
| | | 類似したドメイン名を利用したドメイン偽装メールや、認証されていないなりすましメールを受信した際、迷惑メールフォルダへの移動や警告を表示するよう設定を行う。 | （Google Workspace 5.11～5.13、5.15） |
| | | 利用者からのすべての送信メールが Google Workspace の送信ゲートウェイを経由するよう設定を行う。 | （Google Workspace 5.18） |
| 4.2.2 Microsoft 365 において設定すべきセキュリティ対策 | | | |
| | (1) Azure AD の認証に関するセキュリティ強化 | 管理者権限を持つすべての利用者に多要素認証を設定する。 | （Microsoft 365 1.1.1） |
| | | グローバル管理者が 1 人しかいない場合、内部不正の発見が困難となることから、グローバル管理者を複数人設定する。 | （Microsoft 365 1.1.3） |

| | | | |
|---|---|---|---|
| | | 利用者自身によるパスワードリセットを有効にする。 | （Microsoft 365 1.1.4） |
| | | Azure AD のパスワード保護を有効にする。（強力なパスワードの使用が強制されるようにする） | （Microsoft 365 1.1.5） |
| | | 多要素認証をサポートしていない Basic 認証である「レガシー認証」を遮断する。 | （Microsoft 365 1.1.6） |
| | | オンプレミスの Active Directory と Azure AD のパスワードハッシュを同期し利用者の持つパスワードの数を 1 つにすることで漏えい等の機会を低減する。 | （Microsoft 365 1.1.7） |
| | | Azure AD での「セキュリティの既定値群」を有効化する。 | （Microsoft 365 1.1.12） |
| | (2) 各サービス・アプリケーションの認証に関するセキュリティ強化 | Exchange Online において「先進認証」（前述の「レガシー認証」と比較して、より安全に利用者の認証を行う認証方法）を有効にし、メール（Exchange）で多要素認証等の強力な認証機能が利用できるようにする。 | （Microsoft 365 1.2） |
| | | Skype for Business Online において「先進認証」を有効にし、コラボレーションツール（Skype for Business Online）で多要素認証等の強力な認証機能が利用できるようにする。 | （Microsoft 365 1.3） |
| | | SharePoint において「先進認証」を有効し、データ共有アプリケーション（SharePoint）で多要素認証等の強力な認証機能が利用できるようする。 | （Microsoft 365 1.4） |
| | | Office365 の利用者の認証にはできる限り多要素認証を設定する。知識認証のみの認証とする場合、パスワードの有効期限を設定しないことが望ましい（利用者に定期的なパスワード変更を求めることは、実際にはパスワードの安全性を低下させる可能性がある）。 | （Microsoft 365 1.5） |
| | (3) アプリケーションの権限設定 | 組織で未確認の脆弱性を含む可能性のあるアドインが利用者によってインストールされるのを防ぐために、利用者による Word、Excel、PowerPoint アドインのインストールを制限する。 | （Microsoft 365 2.9） |

| | | | |
|---|---|---|---|
| | | Forms の内部フィッシング対策機能（フィッシングの試みをスキャンする保護機能）を有効にする。 | （Microsoft 365 2.10） |
| | | Sway の組織外への共有機能を無効にする。 | （Microsoft 365 2.11） |
| | (4) データ管理設定 | データ損失防止（DLP）機能を使用し、組織外部の相手と共有できるデータを管理する。 | （Microsoft 365 3.4） |
| | | Microsoft Teams の会議を録画する場合、録画データが OneDrive あるいは SharePoint に保存されるようにする。（録画データが OneDrive あるいは SharePoint に保存されることで、事前に許可された者にのみデータが公開されるようになる） | （Microsoft 365 3.8） |
| | (5) メール（Exchange）のセキュリティ設定 | マルウェアが含まれている可能性がある特定の実行可能ファイル (.exe 等) を遮断する。 | （Microsoft 365 4.1） |
| | | スパム対策を設定する。 | （Microsoft 365 4.2） |
| | | 攻撃者によるデータの流出や他の利用者への攻撃に悪用されないように、メール転送の設定を行う。 | （Microsoft 365 4.3、4.5） |
| | | DKIM を設定する。 | （Microsoft 365 4.11） |
| | | SPF を設定する。 | （Microsoft 365 4.12） |
| | | DMARC を設定する。 | （Microsoft 365 4.13） |
| | | マルウェアを送信した組織内の利用者への通知を有効にする。 | （Microsoft 365 4.14） |
| | (6) 監査ログの設定 | Microsoft 365 の監査ログ検索を有効にする。 | （Microsoft 365 5.1） |
| | | メールボックス監査を有効にする。 | （Microsoft 365 5.2） |
| | | 設定変更やマルウェアの検出等のレポートを定期的に確認する。 | （Microsoft 365 5.3、5.5～5.11、5.14） |

| | | | |
|---|---|---|---|
| | | 不要なゲストユーザーが存在していないかを定期的に確認する。 | （Microsoft 365 5.15） |
| | (7) ストレージの有効期限設定 | 外部共有リンクの有効期限を設定する。 | （Microsoft 365 6.3） |
| | (8) モバイルデバイスの管理 | モバイルデバイス管理ポリシーの設定 | （Microsoft 365 7.1） |
| | | モバイルデバイスでのパスワードの再利用を禁止する。 | （Microsoft 365 7.2） |
| | | モバイルデバイスでのパスワードを無期限に設定する。 | （Microsoft 365 7.3） |
| | | ジェイルブレイク等がされたモバイルデバイスからの接続を制限する。 | （Microsoft 365 7.4） |
| | | モバイルデバイスに複雑なパスワードを要求する。 | （Microsoft 365 7.6） |
| | | モバイルデバイスが未使用時にロックされるように設定する。 | （Microsoft 365 7.7） |
| | | モバイルデバイスの暗号化を有効にする。 | （Microsoft 365 7.8） |
| | | モバイルデバイスのロック解除時に複雑なパスワードを要求する。 | （Microsoft 365 7.9、7.10） |
| | | モバイルデバイスにアンチウイルスソフトを導入し、ファイアウォールを有効にすることを要求する。 | （Microsoft 365 7.11） |
| | | モバイルデバイスのロックを解除するために、パスワードの使用を義務付ける。 | （Microsoft 365 7.13） |