コラム３

クラウド時代の
セキュリティマネジメント
『SaaS利用時の注意点、意識していますか？』

共通対策評価フレームワーク分科会

初版　2022年6月13日

Cyber Security Initiative for Japan

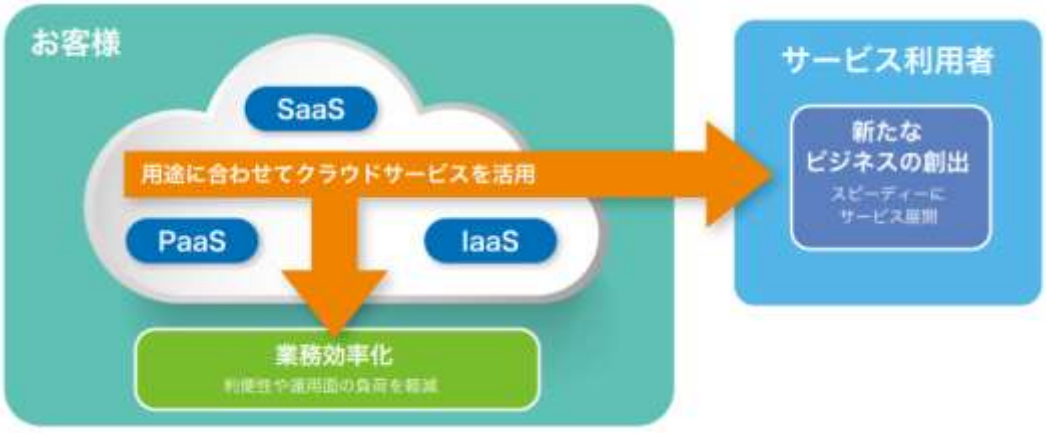
0.クラウドサービスのセキュリティとは

■ クラウドサービスの正しい理解と必要なセキュリティを認識する

クラウドサービスは、サービスによってさまざまな機能が提供されており、サービスごとに必要なセキュリティ対策が異なります。そのため、利用するクラウドサービスを理解し、必要なセキュリティ対策を自組織に合わせて最適化した上で利用する事が重要です。

SaaS	クラウドのインフラストラクチャ上で稼働しているプロバイダ由来のアプリケーション
PaaS	クラウドのインフラストラクチャ上にユーザが開発したまたは購入したアプリケーションを実装できる環境が利用者に提供される
IaaS	演算機能、ストレージ、ネットワーク、その他の基礎的コンピューティングリソースを配置できる環境が利用者に提供される

（出典：独立行政法人情報処理推進機構「SP 800-145 NISTによるクラウドコンピューティングの定義 The NIST Definition of Cloud Computing」より抜粋）



1.なぜ組織はSaaSを導入するのか？

組織がMicrosoft 365やGoogle WorkspaceなどのSaaSを導入する理由は、ビジネスや業務の推進に大きく貢献するからです。

メリット

- クラウドサービスのため どこからでもアクセスできる
- 自社でシステム構築が不要
- システム運用の負荷を軽減できる

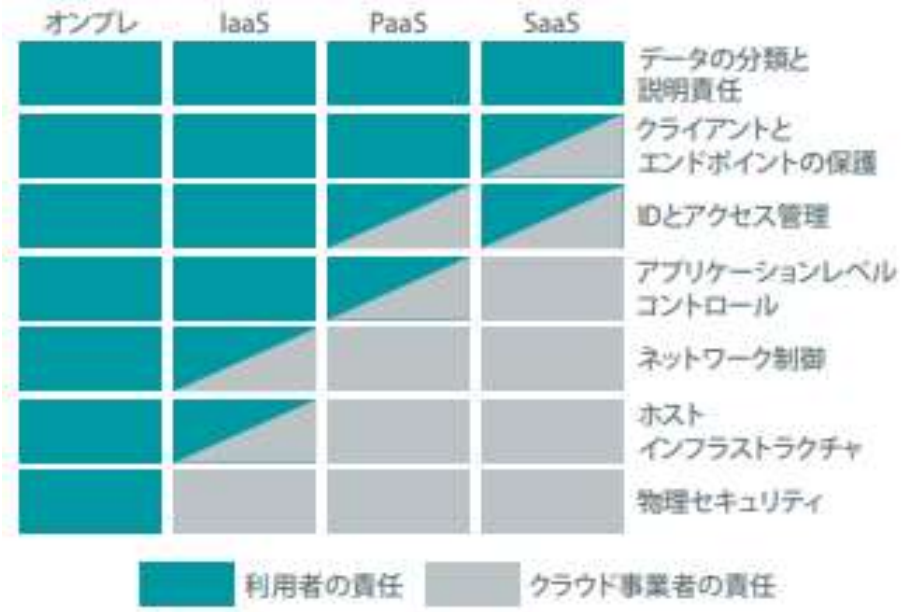
デメリット

- 利用する組織が求めるセキュリティレベルに達しているかどうかが把握しにくい
- リスクマネジメントが運用しにくい

1.なぜ組織はSaaSを導入するのか？

SaaSは責任共有モデルに基づいたセキュリティ対策を行うことが基本です。
SaaS導入時の注意点として、図に示すクラウドサービスの責任範囲のうち利用者側が責任を持つ３点の項目を抑えておきましょう。

- **データの分類と説明責任**
- **クライアントとエンドポイントの保護**
- **IDとアクセス管理**



2.SaaSにおけるインシデント事例

■概要

2020年の末から2021年の初めにかけて、大手SaaSベンダが提供する顧客管理サービスを利用する組織において大規模なセキュリティ事故（情報漏えい）が相次ぎました。

■発生原因

利用者がデータに対して適切なアクセス権限を付与していなかったことが原因でした。
不正アクセス被害に遭ったわけではなく、**「利用者が不適切な設定項目に気付かなかった（知らなかった）」**ことに起因します。

■インシデント事例の教訓

- SaaSにおける**「データの適切な分類やアクセス権の設定」は利用者側が責任を持っている**
- 意識して設定したつもりでも、不適切な設定項目に気付かなかった（知らなかった）
  ⇒**わずかな設定ミスが大規模な情報漏えいに繋がってしまう**

- **データの保護責任は利用者にあり、定期的にデータへのアクセス権が適切であるかを確認する必要がある**

3.攻撃者視点から見たSaaSの「狙いドコロ」

SaaSは“利用者がインターネットに繋がっていればいつでもどこでも利用可能”という特性上、どうしてもオンプレミス環境よりも不正アクセスのリスクは高くなります。

■攻撃者が狙うポイント

利用者の認証情報（ID・パスワードなど）の窃取

⇒利用者側で管理が必要な認証情報の量に比例して利用者のアカウント管理が煩雑になり、パスワードの使い回しや推測しやすいパスワードを設定してしまう傾向にあることも、攻撃者が利用者を狙う理由の1つです。

■対策

①セキュリティを強固にする視点と、②ユーザの利便性を向上させることでセキュリティを強固にする視点の両方から、対策を検討することが重要です。

①多要素認証の導入

⇒ID、パスワード認証に加え、生体認証やOTP等を導入し、認証を強化

② SSO（シングルサインオン）の導入

⇒ユーザのアカウント管理の煩雑さを解消

4.SaaSにおけるセキュリティ対策

SaaSにおけるセキュリティ対策の一例を、取り組みやすさに応じて紹介します。
SaaSの導入時・運用時のセキュリティ対策方針の策定基準例としてご活用ください。

【フェーズ1】
すぐに現状を確認する必要があるもの

- 保有するデータに対する適切なアクセス権限（公開範囲）の設定
- アカウント情報（ID/PW）の適切な管理（多要素認証の採用など）
- 説明責任の確保（原因の特定が可能な形でのログ取得・ログ管理）

【フェーズ2】
日々の運用時において計画的に実施する必要があるもの

- 第三者によるセキュリティリスクの評価（次項に記載の**「共通対策評価フレームワーク」**等）
- 認証情報の一元管理（SSOの導入など）
- 保有するデータに対する適切なアクセス権限の定期的な見直し（棚卸し）
- 利用するSaaSのアップデート履歴を常時確認する

【フェーズ3】
組織の目標として中長期的に取り組みが推奨されるもの

- 利用サービスのアクセス制御や運用基準の策定（文書化を含む）
- 組織内の利用者一人ひとりに対する教育の実施

5.CSIJが簡易なクラウド評価の枠組みを提供

共通対策評価フレームワークとは・・・

　企業が安全にITの利活用やDX推進を進める中で、今現在のシステム利用状況や管理状況を見える化し、課題を浮かび上がらせることで、あるべき姿とのフィットギャップを示し、安全な運用を継続し続けるための指標となることを目的に、セキュリティ企業の知見を集めた共通評価フレームワークとして公開します。

- クラウド環境を利用しようと検討中の企業
- クラウドを利用しているが、安全性に不安のある企業
  - クラウドセキュリティのチェックを行う部署・担当の方
  - クラウド利用を検討・推進している部署・担当の方
  - クラウドサービスの企画、推進を行う方
  - 情報システム部門のリーダー、担当者　など

[出典]「共通対策評価フレームワーク分科会」サイバーセキュリティイニシアティブジャパン
https://www.csi-japan.org/evaluation

簡易セキュリティ評価を体験ください

共通評価フレームワーククラウド版を見てみる
⇒評価分科会活動ページへ

簡易クラウド評価を始めてみる（無料）
⇒発起3社にご相談ください

・株式会社ラック
・NRIセキュアテクノロジーズ株式会社
・グローバルセキュリティエキスパート株式会社

CSIJ

Cyber Security Initiative for Japan