ヌーラボサービスの安全な利用方法を知るための

クラウドサービスのセキュリティ専門用語
～IDaaS、ログ・レポート、アクセス制限～

nulab

はじめに

本資料を読むと得られること

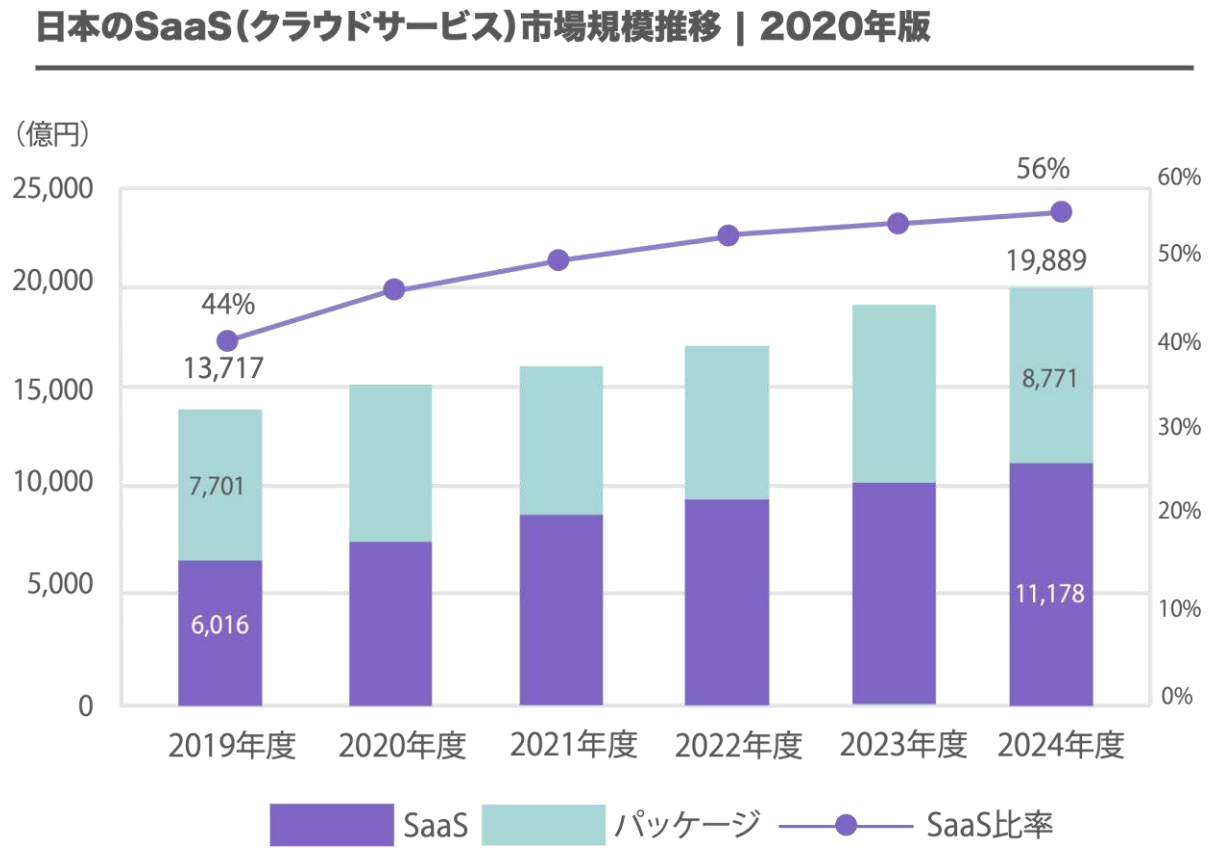
近年、在宅勤務が浸透してきた中で
ヌーラボサービスをはじめとしたクラウドサービスの導入が進みました。

そして、それらのクラウドサービス導入検討時に
経営者や情報システム担当と円滑なコミュニケーションをはかり
安全な利用を行うためにも**セキュリティ専門用語の理解**は欠かせません。

本資料の前半ではクラウドサービスの**セキュリティに関わる基礎知識**をお伝えし、
後半では**「IDaaS」「ログ・レポート」「アクセスログ」**について解説していきます。

在宅勤務によるクラウドサービス導入の広がり①

リモートワークの進展や、デジタル変革などの変化に迅速に対応できるシステム環境の構築を理由とした在宅勤務が浸透してきた中で、クラウドサービスの導入が進んでいます。

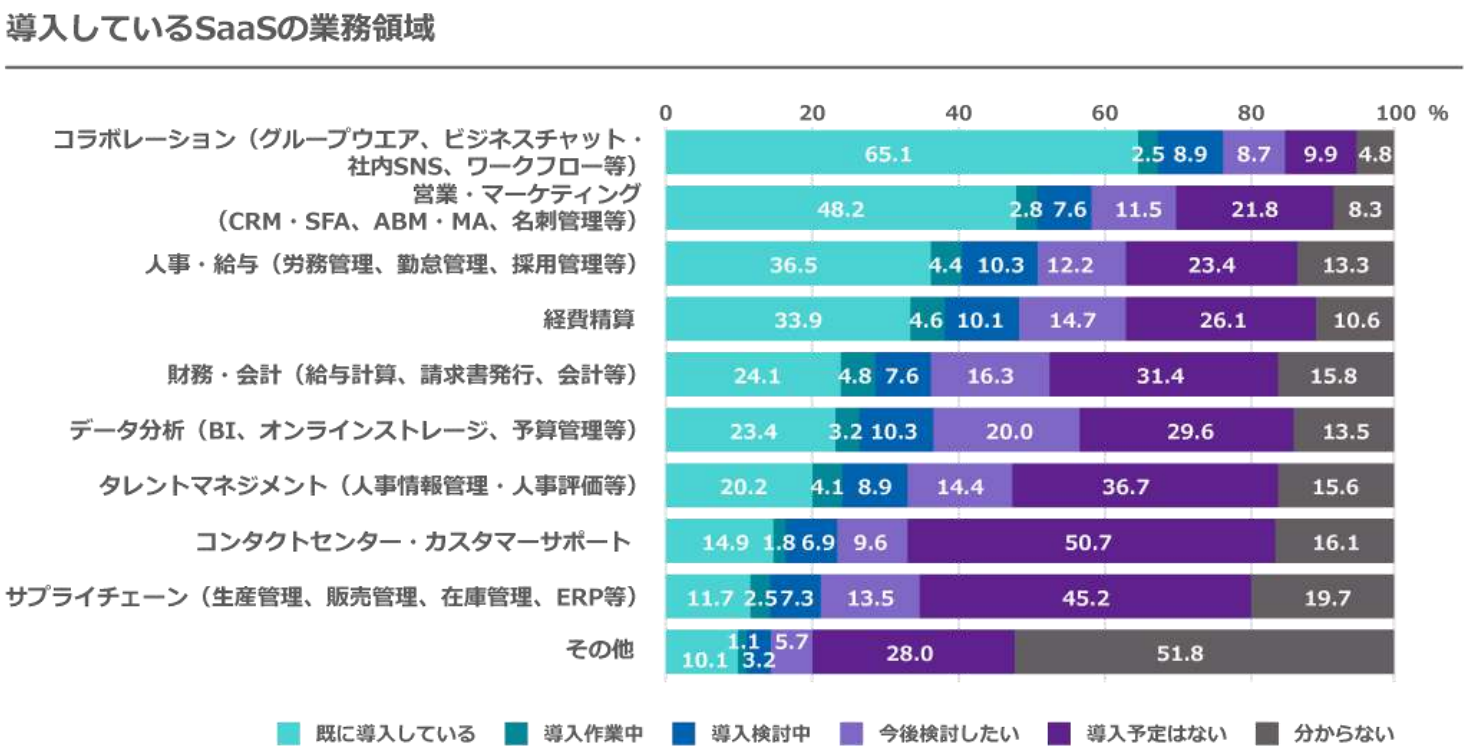


参照：富士キメラ総研『ソフトウェアビジネス新市場 2020年度版』*2019年度実績、2020年度見込み、以降予測

クラウドサービスを導入する企業は年々増えてきており、今後さらに多くの企業で導入されることが予想されています。

在宅勤務によるクラウドサービス導入の広がり②

近年では多岐にわたる業務領域でクラウドサービス（SaaS含む）が使われるようになっています。



参照：WalkMe株式会社『SaaS導入後の課題が、「ユーザーへの定着化」であると72.9%が回答』

連絡やタスク管理を効率化できるコラボレーション分野から、生産管理や販売管理等のサプライチェーン分野まで、**様々な業務でクラウドサービスが活用**されるようになりました。

クラウドサービス導入

クラウド型サービスの特徴は、コストを必要最小限に抑えた上で、利用開始や障害対応に関してスピード感のある運用ができる点にあります。

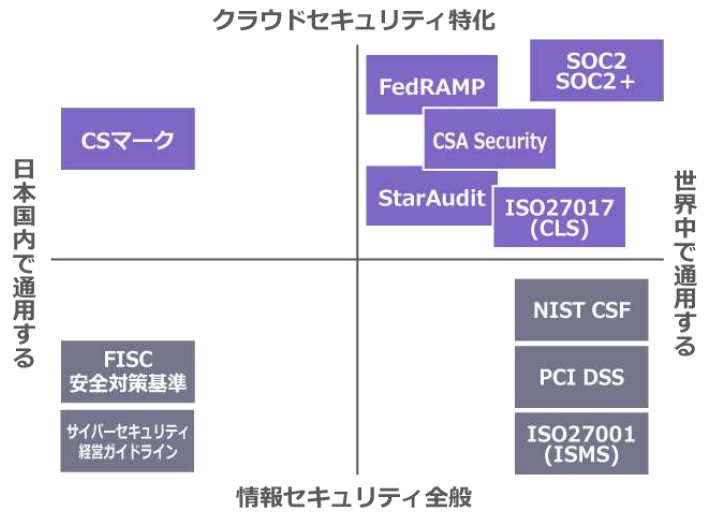
クラウド型オンプレミス型の比較

	クラウド型	オンプレミス型
導入のしやすさ	○ **最短即日** （オンラインでの契約手続きのみで利用可能。また、契約前に試用ができるものが多い）	× 数ヶ月 （サーバーの調達、ネットワークの構築、サーバーやソフトウェアのセットアップ、メンテナンス計画の策定などが必要）
運用にかかる手間	○ メンテナンスはクラウド事業者が対応	× サーバーの保守やバックアップ、ソフトウェアのアップデートなどメンテナンス作業が必要
セキュリティへの懸念	△ 安全性はクラウド事業者の運用に依存する （※次ページより解説）	○ 自社内の閉じたネットワーク環境下で 運用するなど、安全性をコントロールできる

クラウド利用におけるベンダーの選定ポイント

信頼性や安全性の高いクラウドサービスを提供するベンダーの選定が重要です。

関連した認証・認定制度



参照：ニュートン・コンサルティング株式会社『クラウドサービスに特化したセキュリティ基準 ～各ガイドラインや認証制度の比較』

クラウドサービスの安全性

ベンダーが提供しているクラウドサービスごとに公表されている**「サービスの稼働率、データバックアップ対策、障害発生頻度、障害時の回復時間などのサービスの品質保証」**を確認する。

利用者へのサポート体制

サービスの使い方や分からないことがあった際にどのような**支援（ヘルプデスクやFAQなど）**が提供されているか、連絡方法やサポート料金なども含めて確認する。

ベンダーの信頼性

ベンダーが公表している**情報セキュリティ方針**、関連した**認証・認定制度の取得状況**、**個人情報保護法**といった関連法を遵守しているかなどを必ず確認する。

付帯するセキュリティ対策

サイバー攻撃に対して**通信の暗号化**や**マルウェアウイルス対策**、不正ファイアウォールに代表される**ウイルス侵入対策検知**、**通信やデータの暗号化**、**セキュリティパッチの適用やアクセスログの提供**など、 具体的な対策が公開されているか確認する。

ITツール導入時のセキュリティ社内対策

社内で扱うデータの種類ごとに価値やリスクの違いとセキュリティ対策を確認しましょう。

取り扱う情報の重要度を明確化

「漏えい・改ざん・消失」「サービス停止」等の**トラブルが起こった場合の対応、賠償額、費用面での負担を想定し、情報の重要度を考える。**
その重要度合いによって、クラウドサービスに求めるセキュリティレベルと社内の対策内容が変わる。

パスワード・ID管理の徹底

複数人でパスワードやIDは共有せず、強固なパスワード（「できるだけ長く」「複雑で」「使いまわさない」）を使用させる。
「多要素認証を使用する」設定などがある場合、活用して認証機能を適切に設定・管理する。

利用者の権限決め

情報の重要度によって、「従業員の誰でもあらゆる操作ができる」状態は望ましくないため、**どの人に・どのような権限（閲覧、変更、削除など）を与えるか**決めて適切に管理する。

セキュリティ意識を高める教育

社内研修、外部セミナー、eラーニングなどを用いた学習やセキュリティに関するテストを実施し、**従業員のセキュリティへの意識を高める。**

国内企業の事例① ～経済産業省～

クラウドサービスを導入した企業のセキュリティ対策　～メールのファイル添付でよく起こるPPAP対策のためのBacklog活用～

Backlog導入前は、**メールに添付されたzipファイルの解凍とパスワードメールの検索に費やす工数**に悩んでいました。

取引先のベンダーによっては課題管理表をメールで送るときにzipファイルに圧縮して暗号化し、さらにパスワードを別メールにして送付されることがよくあります。この際の、まずzipファイルを保存して、パスワードメールを探して、zipファイルにパスワード入れて解凍して、最後にファイルを共有フォルダに入れて…という**一連の煩雑な事務作業も効率化したかった**のです。

Backlogは課題の担当者、状態、期日などが管理項目として設定されており、課題管理とガントチャートが紐づいているので、**以前のようにベンダーにWBSなどの表を用意してもらい、メールで送付いただく手順がなくなりました**。

経済産業省

国内企業の事例② ～株式会社アピリオ～

クラウドサービスを導入した企業のセキュリティ対策　～アクセス管理機能でファイル共有が安心・安全に～

メールのトラブルで一番多いのが「ファイルの添付」です。たとえば、添付ファイルの暗号化によって、メールが届かないということも起こりがちです。

Backlogを使えば、ファイルを添付した課題のリンクや、ファイル機能によるリンクの共有など、リンクベースでファイル共有ができるので、こうしたトラブルを回避できます。さらに、ファイルのアクセス権限まで管理できるので、**仮にお客様が誤って外部にリンクを共有しても、セキュリティ事故につながらないので安心です。**

お客様のなかでも大企業はファイル管理が厳しいのですが、Backlogのおかげで助かっています。ファイルにアクセスしなくなったメンバーは、プロジェクトメンバーから消すことで簡単に権限を剥奪できるので、セキュリティ管理という面でBacklogを高く評価しています。

情報技術コンサルティング
株式会社アピリオ

3つのセキュリティ対策

代表的な３つのセキュリティ対策と各仕組みをご紹介します。

IDaaS
（アイダース / Identity as a Service）

ノウハウを持ったクラウドサービスベンダーがIDaaSとして提供しているサービスを利用し、各クラウドサービスを利用する際の認証を堅牢なIDaaSに任せることで、不正アクセスのリスクを減らせる。さらに、各クラウドサービスのアカウントをIDaaSのアカウントをもとに自動生成することでアカウント管理の手間を簡略化できる。

ログ・レポート

クラウドへの不正アクセスやマルウェア感染の可能性をアクセスログ・監査ログから把握し、対処する

アクセス制限

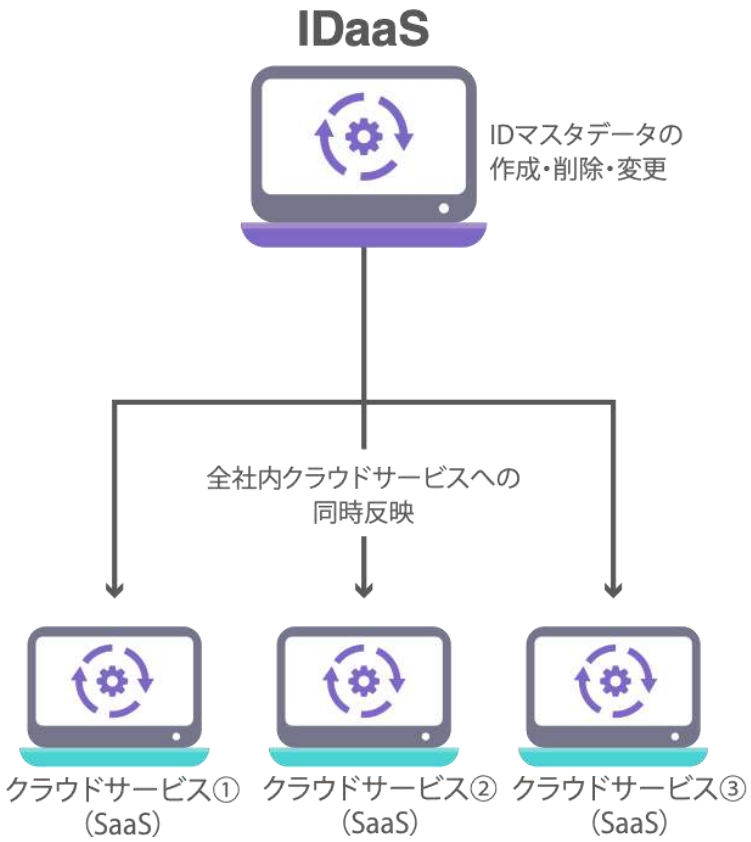
クラウドにアクセスできるIPアドレスや端末に制限をかけ、アクセスできる場所・機器を限定する

1. IDaaS - ①アカウントの一元管理

IDaaSを利用することで、業務で使用するクラウドサービスへの認証のセキュリティレベルの基準を保ちつつ、アカウントの管理を容易にします。

ID認証：ログインユーザーの本人確認＆アクセスの許可

ログインしようとしているユーザーに許可されている本人かどうかIDとパスワードなどを要求し、利用可能な状態にする



IDの同期：ユーザーアカウントの情報を一元管理

IDaaSとクラウドサービス（SaaS）がアカウントの情報を同期できる場合、IDaaS側の各ユーザーのアカウント情報がクラウドサービス側にも自動で反映されるため、手間を減らし対応漏れを防ぐ

対策例

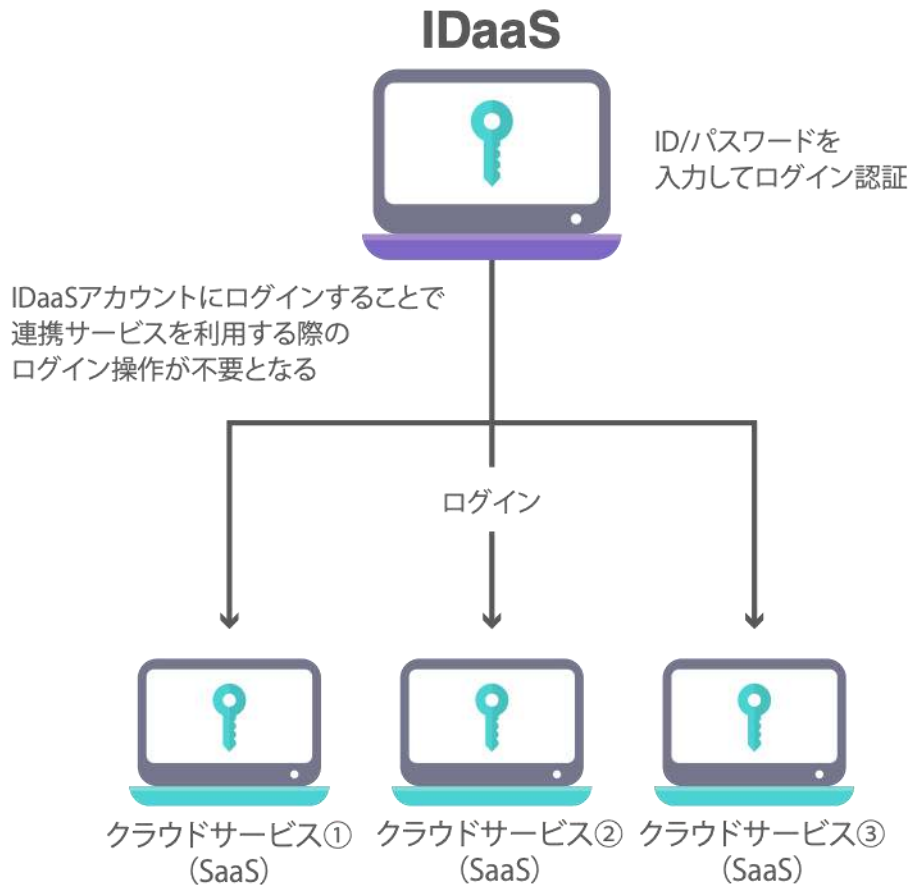
IDaaS未使用時は、社員の入退社時のSaaSアカウント作成/削除は、システム管理者が各サービス毎に行う必要があった。
IDaaSの利用により、IDaaSのアカウントを作成・削除することで、連携サービスも利用開始・停止が行えるようになり、管理者の負担が減った

クラウドサービスを選ぶ時のチェックリスト

- 第三者機関による監査・セキュリティ認証があるか
- サービス提供年数はどれくらいか
- IDaaSが連携できるサービスが、自社で利用しているサービスのどの程度をカバーしているか

1. IDaaS - ②シングルサインオン

シングルサインオンの機能により、**一つのID/パスワード**を用いてID認証するだけで**対応しているクラウドサービス(SaaS)全てを利用**することができます。



対策例

・シングルサインオンを利用することで、複数のサービス間で同一のパスワードを使い回したり、複数のパスワードをメモ書きで保管しておくといった、パスワード流出のリスクを下げられる

・利用するパスワードが一つだけで忘れづらくなるため、システムごとのパスワードリセットに伴うシステム管理者の作業負担が軽減する

クラウドサービスを選ぶ時のチェックリスト

・多要素認証（P.13）やアクセス制限（P.15）等がしっかりと対策されているか

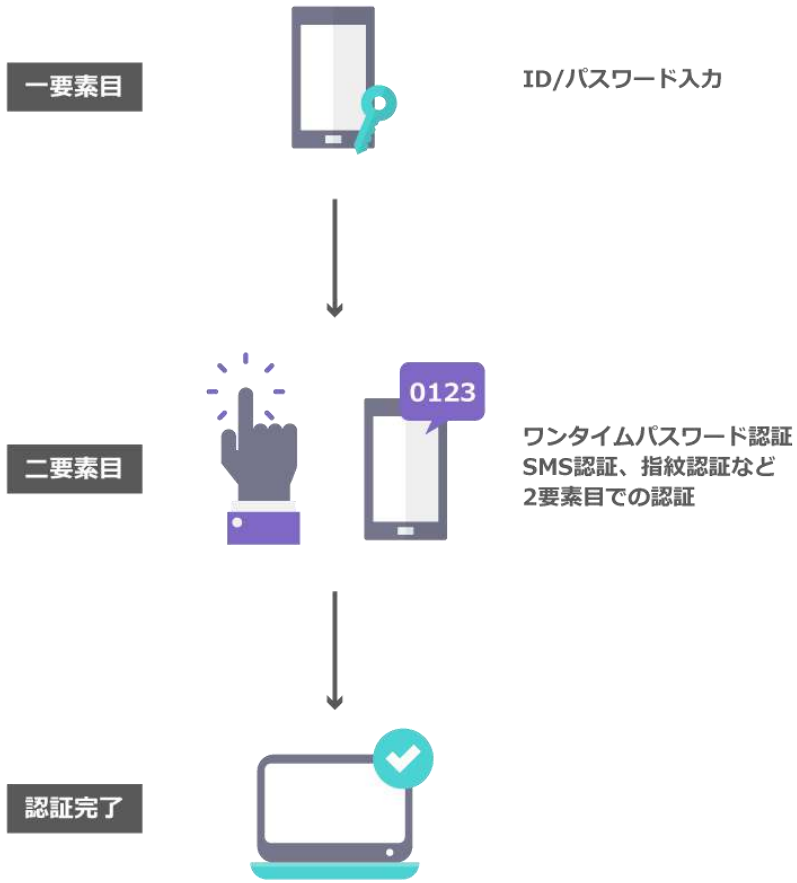
・可用性が高い（システムが停止する率が低い）サービスであるか

・万が一の障害発生時の方針や代替策は用意してあるか

・既存または導入予定のクラウドサービスへのシングルサインオンに対応しているか

1. IDaaS - ③多要素認証

「**ユーザーの記憶（ID/パスワード）**」「**ユーザーの持ち物（スマホ等）**」「**ユーザーの生体情報（指紋等）**」などから２つ以上合わせる多要素認証により、セキュリティを強化します。



対策例

・IDやパスワードのみでクラウドサービスが利用できる場合、それが漏洩すれば第三者に不正利用される懸念があるが、多要素認証によって本人が特定できない限り利用できないようにすることで対策した

クラウドサービスを選ぶ時のチェックリスト

・多要素認証に対応しているか

・多要素認証の各要素は何か（代表例：「ID/パスワード＋ワンタイムパスワード」「ID/パスワード＋SMS認証」）

※ワンタイムパスワード:認証時に発行される一度限り有効なパスワードのこと

・2つ以上、もしくは3つ以上の複数の要素で認証ができるか
※SMSしか使えない、というケースはないか

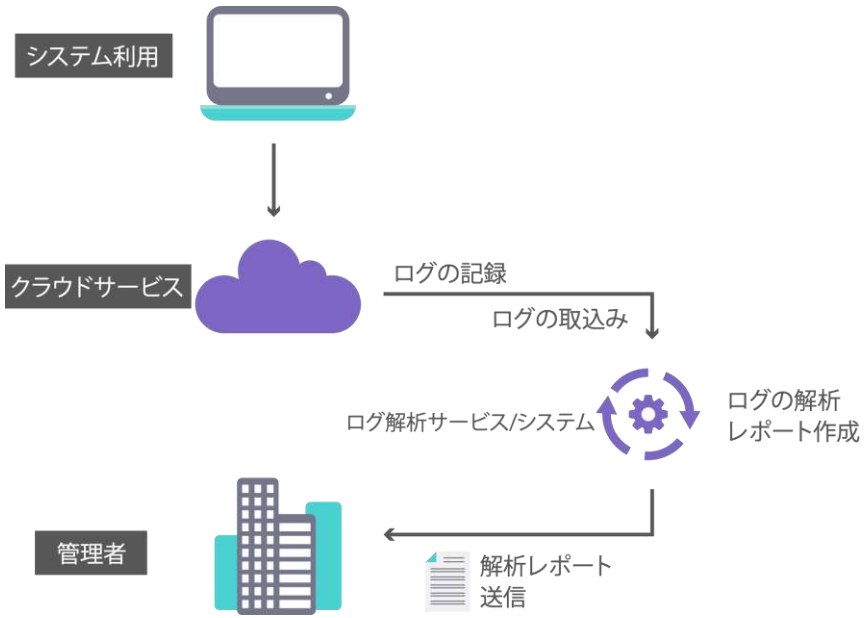
・多要素認証を強制できるか

2. ログ・レポート（アクセスログ、監査ログ）

ログ・レポートにより、**クラウドサービスへの不正行為など**をアクセスログ・監査ログから把握し、対処しやすくします。

アクセスログ：アクセスした人の履歴

クラウドサービスにアクセスした接続元のIPアドレスや日時、エラーの状態、アクセスしたファイル名、ダウンロードしたファイル名、入力されたURLの内容、アクセス元ブラウザの種類などが記録される



監査ログ：「いつ」「誰が」「何をしたか」の行動履歴

アクセスログよりも詳しく、操作内容やそれに伴うシステムの動き、データの移り変わりなどが時系列に沿って記録される

対策例

左図の「クラウドサービス」における、クラウドサービスの利用で不正行為やマルウェア感染の危険性があるが、ログ・レポートでアクセスログや監査ログをレポーティングしてもらうことで、不正行為などが把握できるようになり、速やかに対策が打てるようになる

（社内検討時の）チェックリスト

・ログの監視のために、別途ログ解析のシステムの運用が必要かどうか

・ログの保存期間や対象範囲はどのくらいか

・ログレポートの目的は何か？（不正アクセスや不正利用の早期発見）

・自社のセキュリティ対策に必要なログの種類は何か？

3. アクセス制限

アクセス制限とは、クラウドサービスにアクセスできる**IPアドレスや端末に制限**をかけ、アクセスできる場所・機器を限定することです。

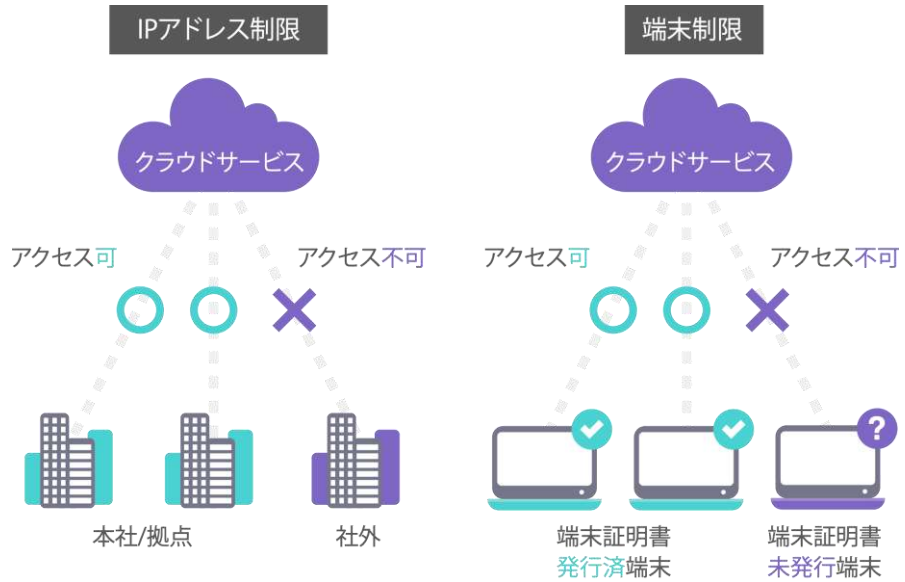
IPアドレス制限：本社や拠点以外からのアクセスを防止

アクセス可能なIPアドレスを指定して、決められた場所（ネットワーク）以外からはアクセスできなくする

端末制限：アクセスできる端末を限定する

アクセス可能な端末（PCやスマホ）に端末証明書を発行して、証明書のある端末でしかクラウドにアクセスできないようにする

※IDaaSでシングルサインオンできるクラウドサービスは、MDMという端末管理サービスとIDaaSとの組み合わせ次第で端末制御ができる



対策例

正規のIDの持ち主が許可されていないプライベートの端末でのアクセスを防ぐことができる

クラウドサービスを選ぶ時のチェックリスト

- IP制限機能が搭載されているか
- 端末制限機能が搭載されているか
- 社外でのクラウドの利用が必要か
- アクセス制限の条件をどの程度にするか

＼シンプルでスケーラブルなセキュリティ対策／

ヌーラボ製品のセキュリティとガバナンスを強化できる Nulab Passとは？

サービス概要・Nulab Passについて

サービス概要

Backlog・Cacoo・TypetalkとNulab Passを併用することで、より強固なセキュリティ対策のもとアカウント管理を強化することができます。大切な業務データをNulab Passで安全に管理しましょう。

Nulab Passの基本機能

①ビジネスを効率化させるシングルサインオン （参考：P.12）

Nulab Passが提供する「SAML※認証によるシングルサインオン」はお客様がご利用のIDプロバイダーを介してヌーラボサービスのアカウントを認証し、利便性を高めます。

※SAML･･･クラウドサービス間で認証情報を交換するための標準規格。シングルサインオン(SSO)を実現するために使われます。SAMLはセキュリティアサーションマークアップ言語の略
※IDプロバイダー･･･ユーザーIDを保存、管理する認証機関です。外部の信頼できるサービスへ認証情報を提供します

②SAMLでデータを保護する （参考：P.11）

SAMLに準拠することで、認証のセキュリティレベルをヌーラボのサービスの外側にあるIDプロバイダーにまかせることでき、結果的に自社のセキュリティ基準を満たすことに繋がります。

③監査ログ （参考：P.14）

ヌーラボサービスですでに提供しているアクセスログよりも詳しい、メンバーの操作内容やそれに伴うシステムの動きなどをログとして残します。

サービス詳細はこちら

会社概要・お問い合わせ

nulab

backlog by nulab　cacoo by nulab　typetalk by nulab　nulabpass

ヌーラボ製品は世界の10,000以上もの組織から
信頼され、愛用されています。

社名　：　株式会社ヌーラボ

所在地：　福岡県福岡市中央区大名1丁目8-6 HCC BLD.

代表　：　橋本正徳

設立　：　2004年3月

問合せ：　https://nulab.com/ja/contact/