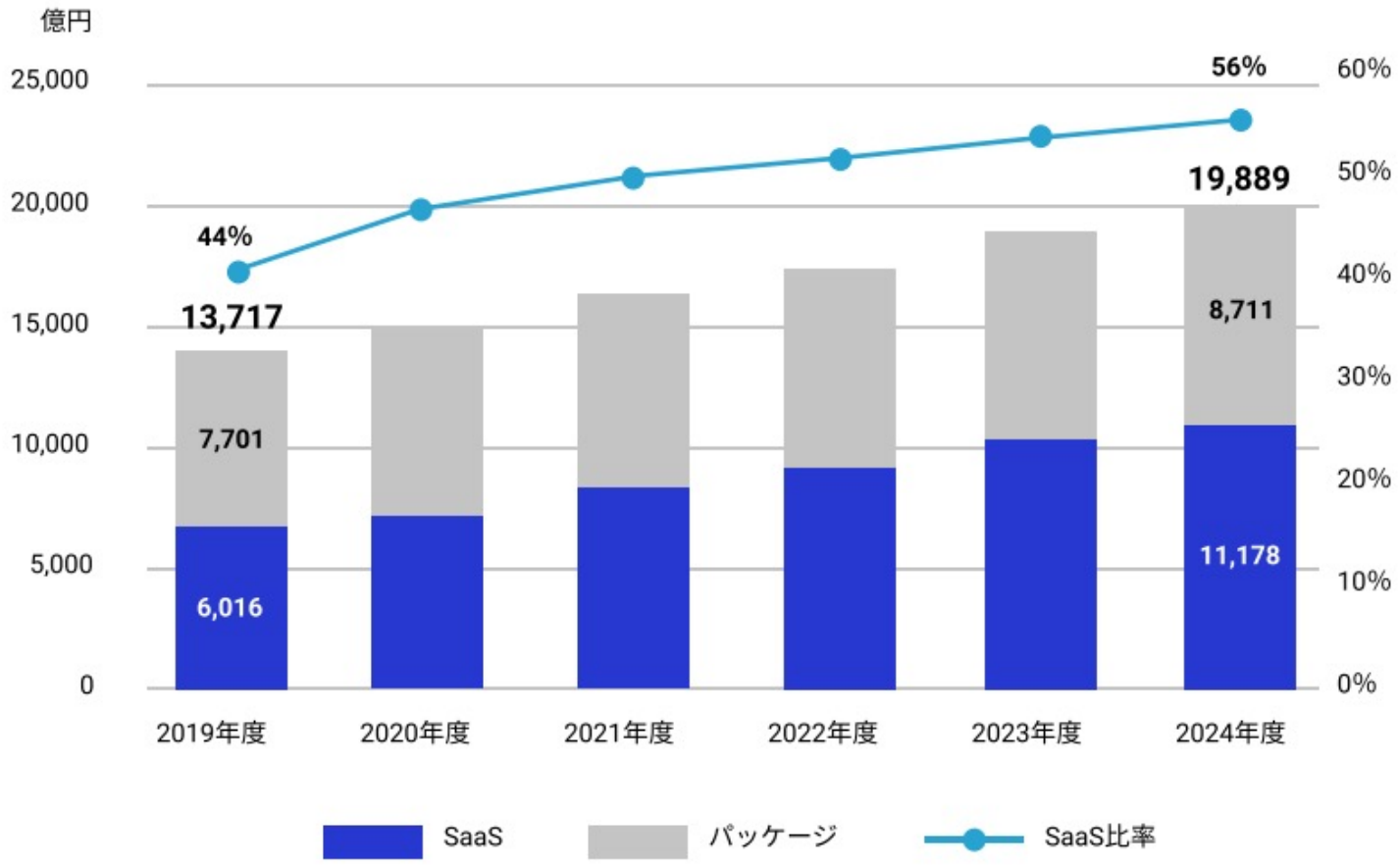
Microsoft × BOXIL SaaS

# SaaSセキュリティの実態と課題解決ガイド

# 日本の SaaS 市場規模推移

SaaS 市場は年平均成長率約13%の勢いで急成長しており、2024年には約1兆1,200億円へと拡大する見通しです。




2019年度～2024年度

**パッケージ比率**

56.1% ▸ **43.8%**

**SaaS比率**

43.9% ▸ **56.2%**

SaaS比率も大幅に上昇

出所　富士キメラ総研
「ソフトウェアビジネス新市場 2020年版」
＊2019年度実績、2020年度見込、以降予測

# SaaS のセキュリティリスクの高まり

一方、SaaS の浸透にともない、SaaS の種類、はたらく場所、デバイスが多様化し、セキュリティリスクが高まっています。

・コラボレーション
・バックオフィス
・営業・マーケ など

SaaSの種類

×

・オフィス
・自宅
・外出先 など

はたらく場所

×

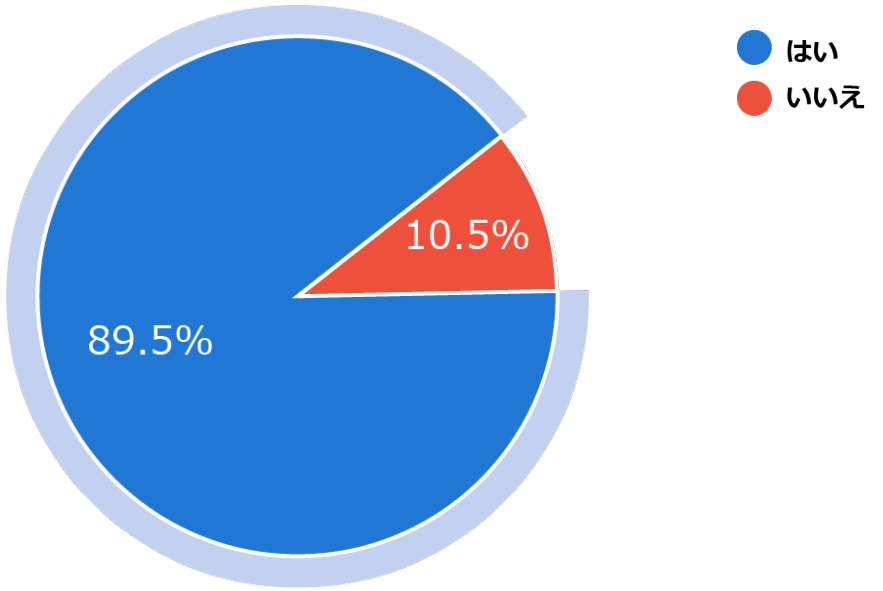
・PC
・スマートフォン
・タブレット など

デバイス

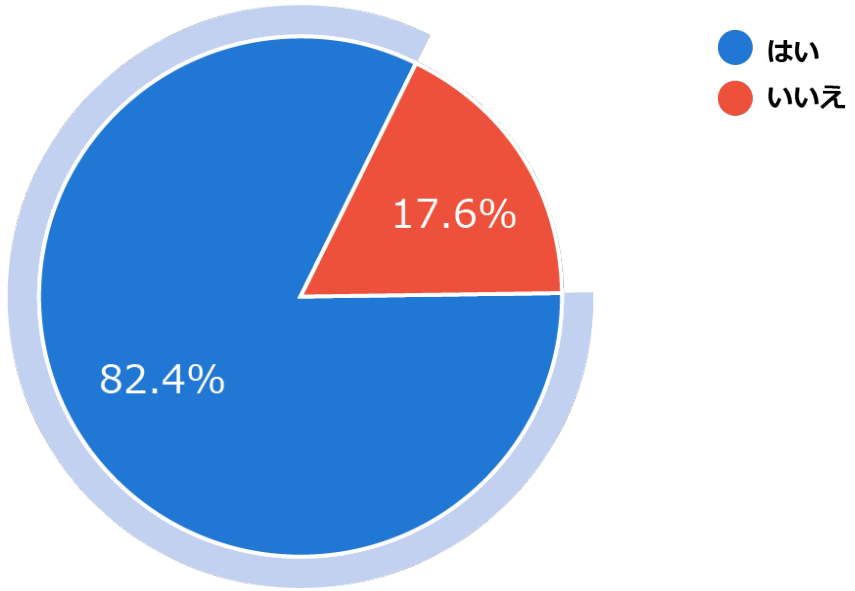
# SaaS セキュリティ実態調査（SaaS 提供者）

SaaS 提供者の約90%がユーザーに対してセキュリティ機能を提供しており、そのうち約82%が十分なセキュリティ機能を提供できていると回答しています。

あなたの企業で提供している SaaS/IT ソフトウェアは、ユーザーに対してセキュリティ機能を提供していますか。



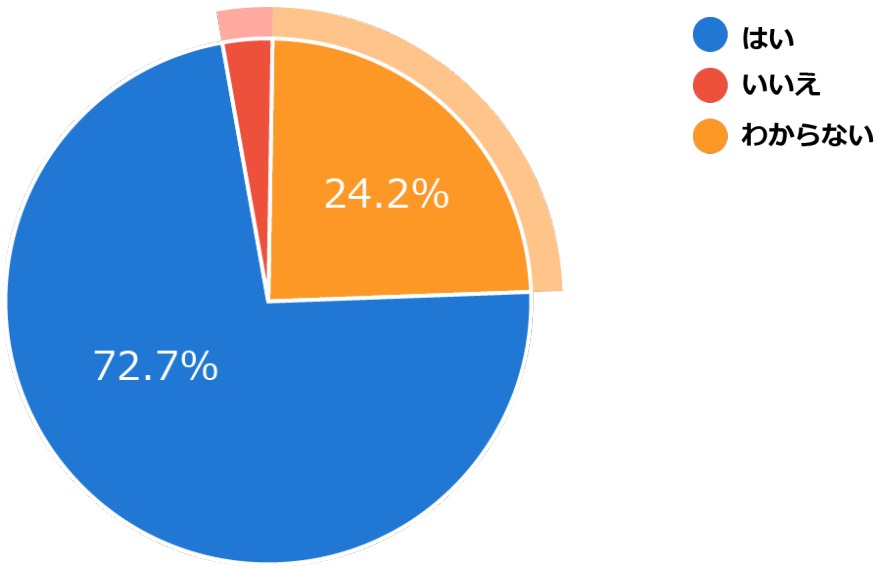

ユーザーに対して十分なセキュリティ機能を提供できていると思いますか。



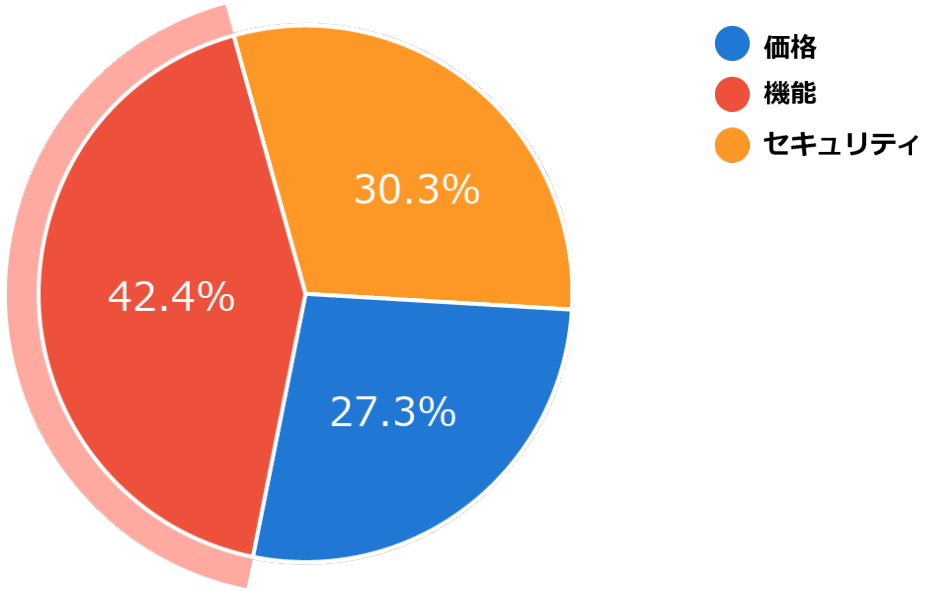
# SaaS セキュリティ実態調査（SaaS 利用者）

SaaS 利用者の約25%が利用SaaSのセキュリティ機能について意識しておらず、SaaS 選定ポイントとしても機能が重視されがちと言えます。

あなたの企業で利用している SaaS/IT ソフトウェアは、ユーザーに対してセキュリティ機能がありますか。



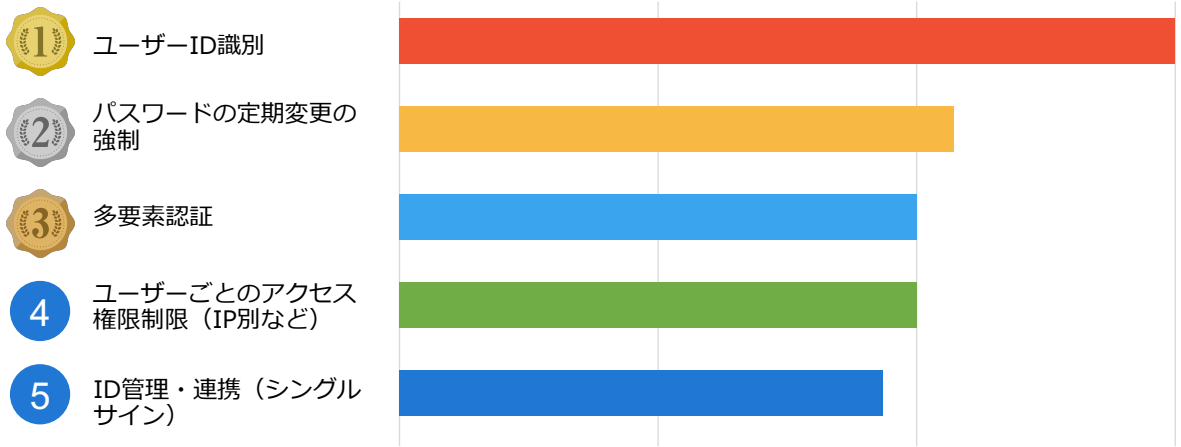

SaaS/IT ソフトウェアを選ぶ際の選定ポイントを教えてください。



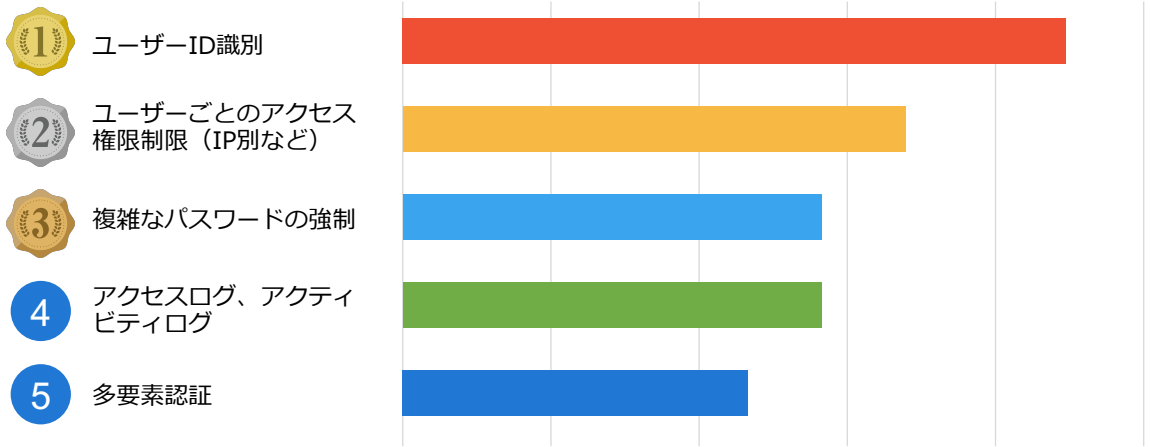
# SaaS セキュリティ実態調査（具体的なセキュリティ機能）

SaaS のセキュリティ機能について、提供機能に対してユーザーの利用割合は低く、SaaS 利用者のセキュリティに対する意識の低さが見て取れます。

具体的なセキュリティ機能を教えて下さい
（※複数回答可）




具体的なセキュリティ機能で使っているものを
教えて下さい（※複数回答可）



# SaaS の安全利用に向けて注意するべきポイント

## クラウドサービスを利用する前に確認しましょう！

- ☑ インターネット経由でのアクセスのため、いつでもどこからでもサービスを利用できることがクラウドサービスの大きなメリットです。

- ☑ 情報セキュリティ対策について、情報システムを所有する場合には、自社が対応すればよいのですが、”利用するだけ“のクラウドサービスではサービスを提供する事業者に委ねる部分が発生します。

- ☑ 事業者に委ねる部分については、利用者が直接管理することはできないので、サービスの機能だけではなく、サービスに付随するセキュリティ対策についても、きちんと確認したうえで利用する必要があります。

- ☑ クラウドサービスのセキュリティ対策は、自社で所有する場合との共通点もありますが、次のスライドにあるようなポイントを考慮して検討します。

# SaaS の安全利用に向けて注意するべきポイント

## 利用者がやるべきことを知っておきましょう！

- クラウドサービスのセキュリティはサービスを提供する事業者と利用者との両者が、それぞれの役割・責任を分担し、必要とされる対策を実施することで維持・向上します。
- 複雑なパスワードだけでは攻撃からの防御は困難になっています。特に、SaaS はサービス間でのデータ連携も多いため、1つのサービスに不正ログインされた場合、連携するサービスのデータも露出してしまうことに注意する必要があります。
- 特に SaaS の場合、利用者が後付けのセキュリティ対策製品を導入しても万全の対応が困難なこともあり、SaaS に必要なセキュリティ機能が備わっている、または公式で他サービスと連携できていることが、機能およびコストの両面で重要になります。
- また、導入時には SaaS サービスがいかにセキュアに提供されているかを、SaaS 事業者の取得している認証や外部監査の報告書、ホワイトペーパーなどを通じて理解することが重要です。
- 次ページ以降では、SaaS 利用の上で特に重要な ID の保護の強化のために確認するべきポイントを紹介します。安全で安心な SaaS 利用につなげていきましょう。

## SaaS 利用時に考慮するべきセキュリティのポイント

**不正なログインへの対策**

► 複雑なパスワードだけでは攻撃からの防御は困難になっています。また NIST（米国国立標準技術研究所）のガイドライン（NIST 800-63-3）においてもパスワードの定期変更は推奨事項ではなくなっています。特に、SaaS はサービス間でのデータ連携も多いため、1つのサービスに不正ログインされた場合、連携するサービスのデータも露出してしまうことに注意する必要があります。

**不正なログインの検知および対応**

► 攻撃の手段も日々進化しており、利用者も侵入されることを想定した対応が求められます。不正なログインを検知した後、パスワードリセットなどいかに初動の対応を速やかに行えるかが必要になります。

**クラウド事業者のセキュリティ体制のチェック**

► 安全とうたわれているクラウドサービスでも、実際にどのような対策が行われているかを確実に理解する必要があります。

# SaaS を安心に利用するためのチェックポイント

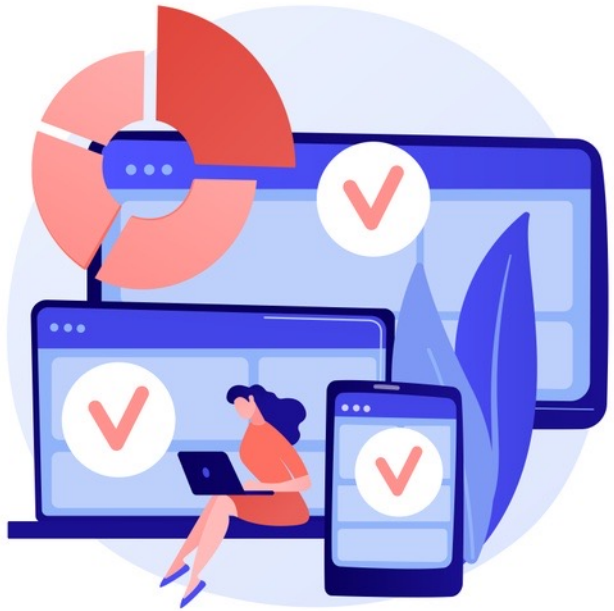
| No. | 項目 | 概要 | 技術 | チェックポイント |
|---|---|---|---|---|
| 1 | **認証強化** | 自社の ID 基盤との連携が実現できるアプリか | SSO 連携 | SAML2.0 や OIDC のような、業界標準技術の実装がされているか |
| | | 最新の認証技術が適用できるアプリか | 多要素認証の適用<br>パスワードレス認証の適用 | SSO 連携ができれば自社 ID 基盤で使う認証の仕組みをアプリにも適用できます。自社の IDaaS の機能をチェックしてみましょう |
| 2 | **データ連携** | 自社のユーザー更新情報を自動的にアプリケーションへ反映することができるか | プロビジョニング連携 | SCIM 連携が実装されており、ユーザー情報の同期が行えるアプリケーションか |
| 3 | **権限管理** | アクセスコントロールを行うことができるアプリか | 条件付きアクセスの適用 | SSO 連携ができれば自社 ID 基盤で使う権限管理の仕組みをアプリにも適用できます。自社の IDaaS の機能をチェックしてみましょう |
| 4 | **端末管理** | 悪意のあるユーザーやウイルスの攻撃による不正なログインを検知できるか<br>また、不正なログインに対する迅速な対応が可能か | 不正ログイン検知<br>セルフパスワードリセット | SSO 連携がされている自社の ID 基盤でパスワードをユーザー自身でリセットできるか<br>不正ログインがあった際に検知することができるか |
| 5 | **公式連携** | IT 運用・管理者が簡単にアプリの連携や管理を実現できるか | Azure AD Application gallery<br>公式登録アプリケーション | Azure AD Application Galleryに公式に登録されているか |

● ユーザーで対応可能　● SaaS ベンダーで対応

# 1-1. SSO 連携を利用したセキュリティ対策の余地があるか

## SSO が標準機能として提供が実現されているか

自社 ID 基盤とアプリケーションの SSO 連携がオプションとしての機能ではなく、標準機能としてアプリケーションに備わっているかどうかを確認しましょう。SaaS 利用が進む中で SSO 連携は悪意のある攻撃から守る手段の第一歩となります。必要なタイミングで迅速に SSO 連携を対応するためにも、標準機能で SSO 機能は実装されているアプリケーションが好ましいです。



## SSO 連携のための技術がパスワード代理入力方式ではなく、業界標準認証技術である SAML2.0 や OIDC が利用されているか

シングルサインオンと一言で言っても、この機能を実現する方法はいくつかあります。アプリケーションを検討する際には、このシングルサインオンが業界標準技術である SAML2.0 もしくは OIDC の技術で実現されているかどうかを確認しましょう。中には、パスワードベースシングルサインオン（パスワード代理入力方式）という技術でのシングルサインオン機能を目にすることもありますが、この技術を用いる場合は ID プロバイダーがアプリケーション向けのパスワードをどこかに保存していて、ユーザーの代わりに代理入力してくれるというものなので、業界標準技術の SAML2.0 や OIDC を用いたフェデレーション（ID 連携）とは別物になります。システム間で認証情報を交換するための規格としての標準技術である SAML2.0 や認証・認可の連携を実現する OIDC を用いたシングルサインオン機能が実装されているかどうかをアプリケーションの選定の際には確認しましょう。

# 1-2. SSO 連携を利用したセキュリティ対策の余地があるか

## SSO 連携後、自社 ID 管理基盤の多要素認証を適用しましょう

近年パスワードとユーザー ID を利用したサインインは危険だと警鐘がならされています。ユーザー側のセキュリティの技術が向上する一方で、悪意のある脅威の攻撃手法も複雑に、また高度になってきています。

これまでは、複雑なパスワードを用いることで、悪意のある脅威からの不正なサインインを防ぐことが有効な手段と伝えられてきましたが、近年は AI の技術なども用いて複雑なパスワードをいとも簡単に解かれ、企業のデータやアプリに不正にサインインをされてしまうという、パスワード漏れのセキュリティ事故が毎年ニュースに取り上げられます。

そこで、現在はパスワードはリスクを持っているという認識を持ち、パスワードに加えた別の要素を使った認証を推奨しています。それが、多要素認証です。多要素認証では、パスワードの入力に加えて、メールや電話、生体認証やアプリ認証で本人の確認を行ってからデータやアプリへのサインインをするような仕組みを提供します。

近年では、パスワード入力をせずに、生体・アプリケーション・FIDO キー のいずれかを利用したパスワードレス認証という技術も出てきています。パスワード自体はリスクを持つもの、パスワード入力以外の方法での認証を取り入れ、使っているアプリケーションはしっかり強固な認証方法が適用できるような運用を検討しましょう！

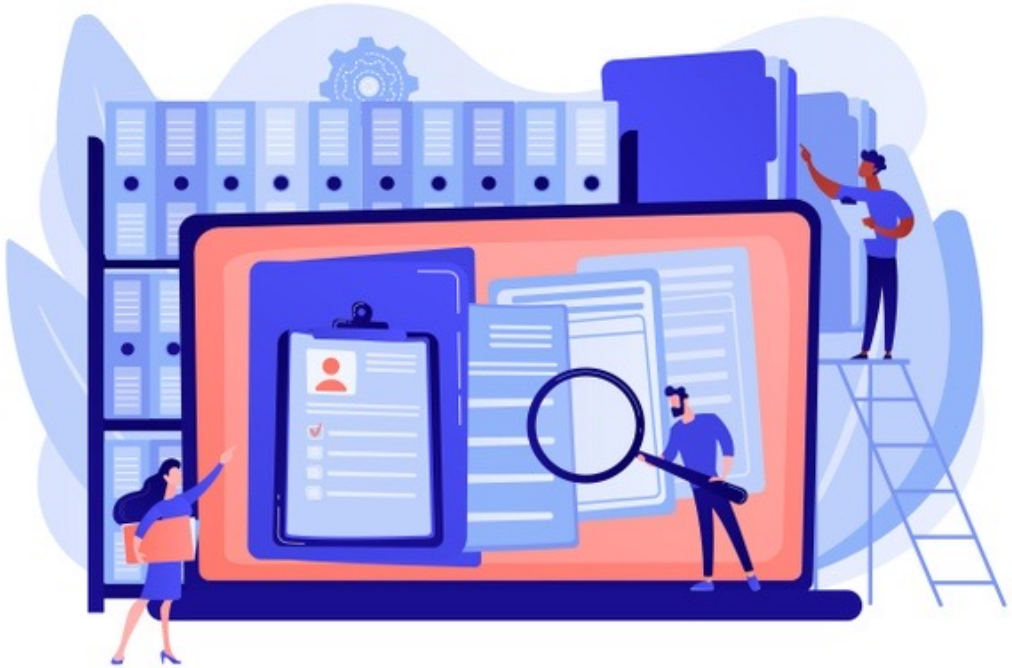
# 2．自社組織情報と連携できるか

## SCIM の実装によるユーザーの更新情報の自動同期の実現可否

ユーザーの更新情報を自動同期化することにより、日ごろ手入力などでユーザー情報の更新対応などを各アプリケーションに行っていたものを、自動的に自社で管理をしている ID 基盤上のユーザー情報更新をアプリ側にも反映することが可能になります。

これを実現することにより、迅速なアクセスコントロールの実現や情報更新の際の各アプリケーションへの適用の抜け漏れなどのリスクを防ぐことにつながります。

また、会社の異動時期などに情報更新にかけていた人件費や時間なども削減も実現できます。



# 3．権限管理の実現が可能かどうか

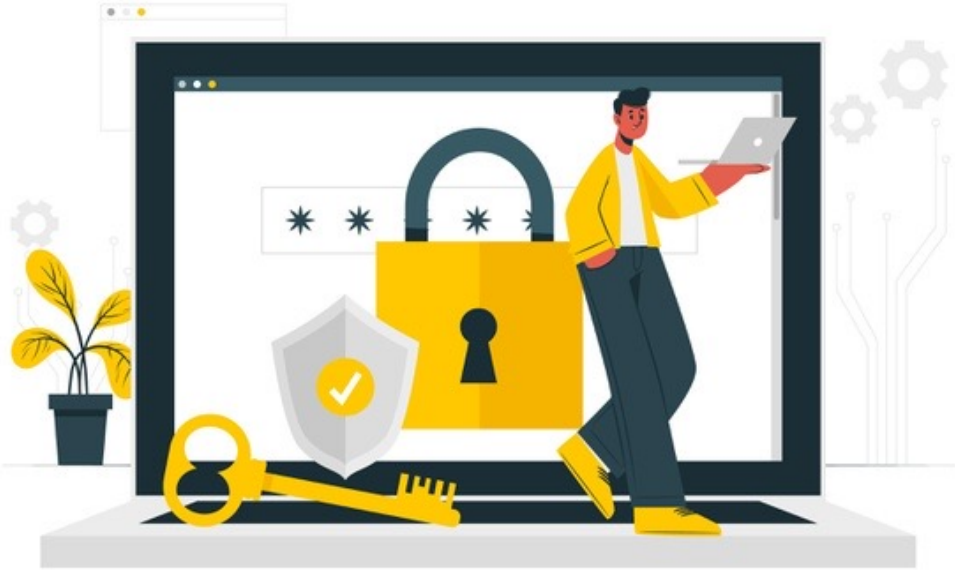
## SSO 連携後、権限管理対象アプリとして設定しましょう

SSO 連携されているアプリは、自社 ID 管理基盤の中で他のデータやインフラ同様に管理をすることができます。

1）誰が　2）どこから　3）どんな端末で　4）どのアプリに

という様々な要素を組み合わせて、アクセスのコントロールを連携しているアプリにも効かせることができます。

他の資産同様に、多々あるアクセスパターンをコントロールができるのは、SSO 連携したアプリへのメリットとなります。



こちらの権限管理の実現は SSO 連携が完了次第、設定を行いましょう。

# 4．端末管理を任せることができるか

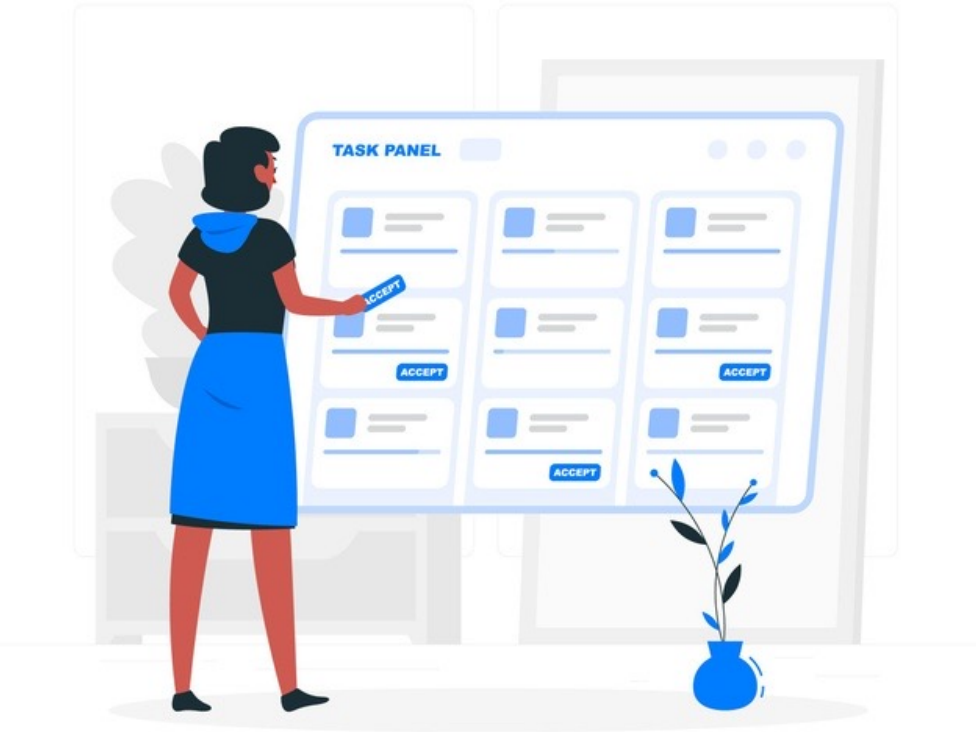
**対象アプリにて、不正ログインがあった場合の検知やその後の迅速な対応を自社 ID 基盤側で実施することができるか**

万が一悪意のある脅威により不正にアプリケーションへのサインインがあった場合、迅速に対応をする必要があります。

そのためにも大切なことは、このような不正ログインをすぐに検知できる状態にするということです。こちらも IDaaS の機能として備わっている場合は、連携したアプリケーションにおいても自社の資産同様に不正ログインを検知できる状態にしましょう。

また不正ログインを検知した際は初期対応の早さが重要です。

IDaaS にはユーザー自身でパスワードを変更するというパスワードリセットの機能も備わっているので、不正ログインの初期対応として、ユーザー自身でパスワードを変更することを推奨します。



# 5．Azure Active Directory の公式連携アプリケーションであるか

## Azure AD Application Gallery に登録されているアプリかを確認する

マイクロソフトの Azure Active Directory と公式に連携されているアプリケーションがどうかを確認しましょう。

Azure Active Directory  application gallery に登録されているアプリケーションはすべて公式に連携されているアプリケーションとなっています。ここに登録されているアプリケーションは簡単に SSO やプロビジョニング連携を実現することができ、連携のためのガイドラインもマイクロソフトが提供しているため、IT 管理者はガイドラインに沿って進めていただくことができます。

また連携後の管理も Azure portal 内にて行うことができ、運用者の運用者の手間を削減することができます。

# Microsoft が推奨するモダンな SaaS の特徴

セキュリティ対応に加えて、より便利に、柔軟に SaaS を活用するためのポイントをお伝えします。

## 1 SSO 連携による十分なセキュリティ対策の余地がある

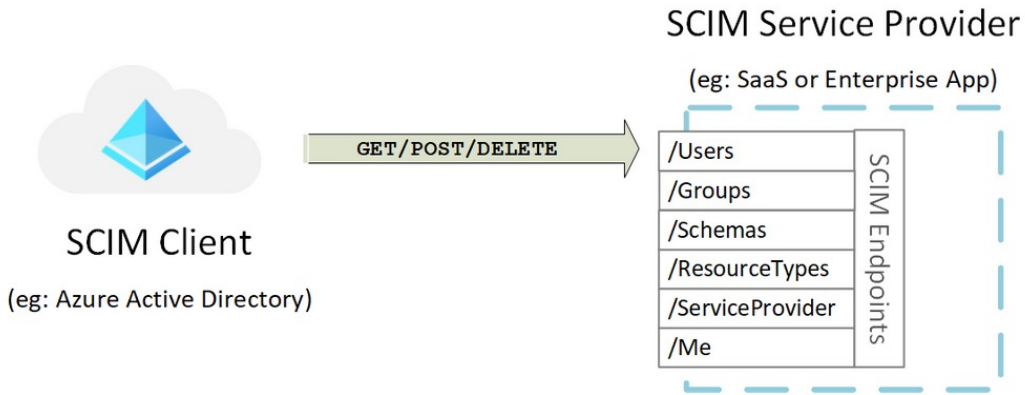
モダンプロトコル（SAML2.0や OIDC）への対応

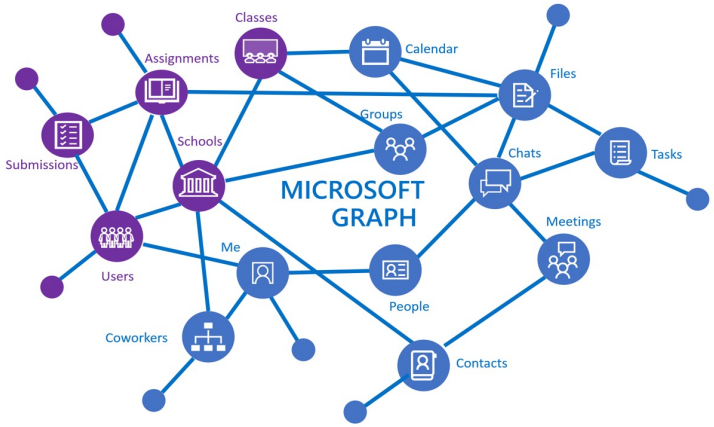
## 2 IT 運用管理者が便利に使える

Azure Active Directory Application Gallery に登録済

## 3 自社の組織情報とデータ連携できる

例：SCIM 連携の対応（プロビジョニング連携）
Microsoft Graph API を利用している



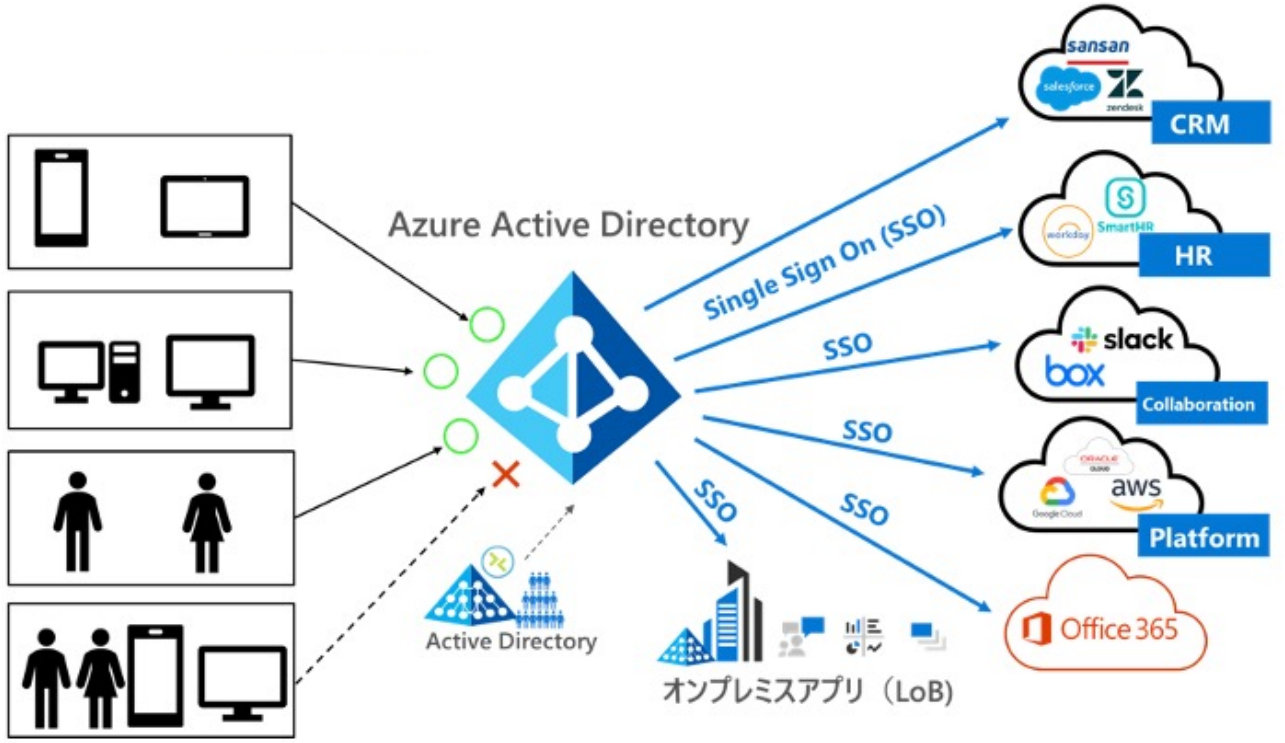



# Microsoft Azure Active Directory

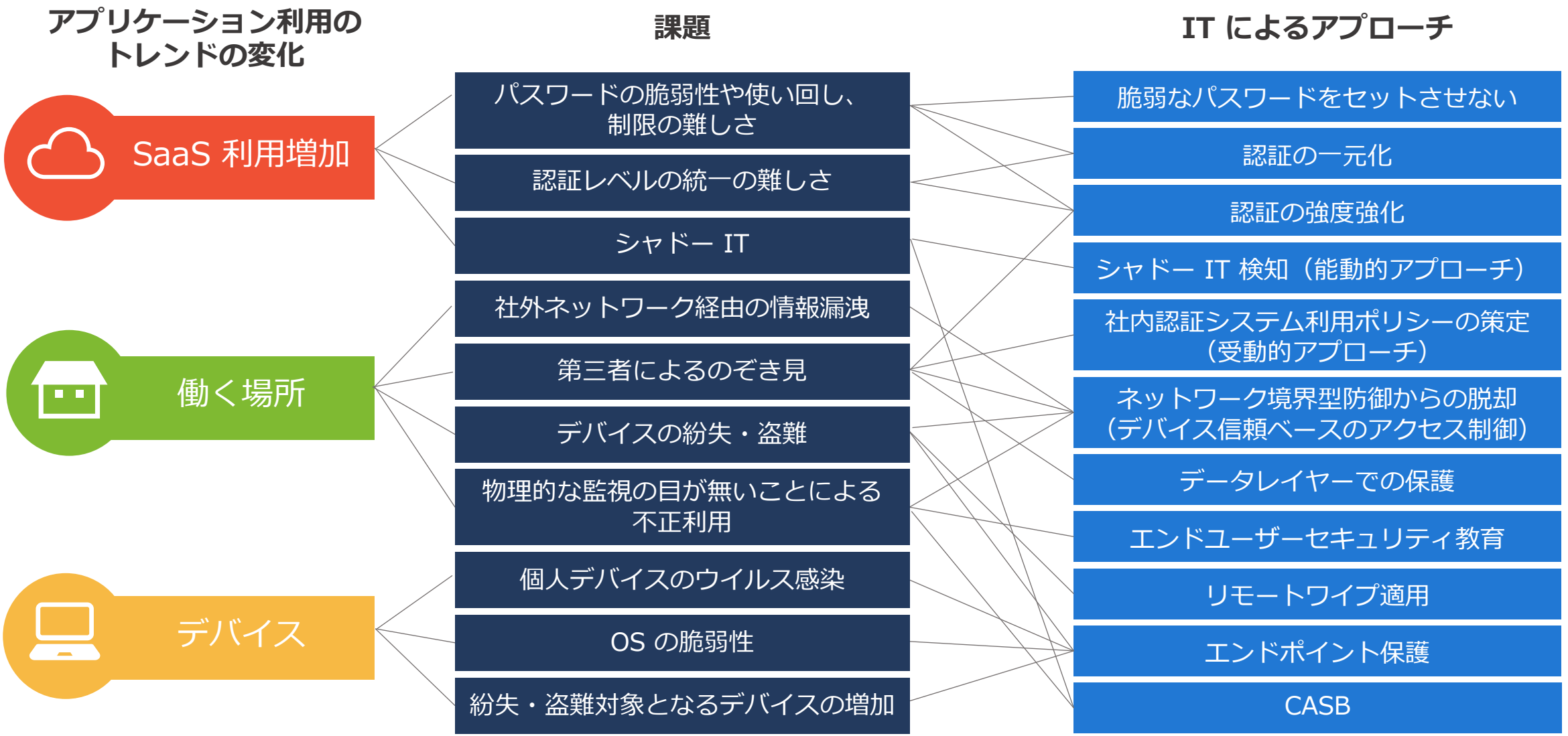
Office 365の認証基盤としてつかわれている、Azure Active Directory を ID 基盤として、SaaS アプリや自社のオンプレカスタムアプリなど、様々なアプリケーションを一元管理下に置くことが可能です。Azure Active Directory と SSO 連携いただくことで認証やアクセスコントロール以外にも、ガバナンスの自動化や、監査といった多様なシナリオを適用いただき、シンプルな ID 管理を実現することができます。

## Azure AD で実現できるシナリオ

| | | |
|---|---|---|
| 認証強化 | アクセス コントロール | アプリ 連携 |
| デバイス 管理 | 特権アカウント管理 | 監査 |
| アプリ開発 | ガバナンス 自動化 | 外部ユーザー 協業 |



# Microsoft の SaaS セキュリティリスクに対する解決アプローチ



# ランドリースタートアップ OKULAB の SaaS 活用法


## Laundry is More Fun!

ハイアールグループ「アクア」の元事業責任者と技術開発責任者が2016年に創業した OKULAB は、多くのランドリー店舗の開発や、併設するカフェなどの運営を行うスタートアップ。

事業の成長スピードや柔軟な体制変更を行うため、社内IT基盤に様々な SaaS を利用してきたが、さらなる次の成長を実現するため2020年の社内 SaaS の棚卸しを実施。Microsoft、Google、Salesforce、Slack、ChatWork と様々な SaaS の管理をしてきたが、現在は Azure AD と Office 365を中心としてインフラに徐々に集約・移行をすすめている

## OKULAB のポイント

1．内製で70名規模の会社の O365移行及び Azure AD 移行を完了
2．Azure AD への統合を実施することでコスト削減の実施
3．顧客サービス向上に自社でアプリ開発を可能にしている

# OKULAB 社 CIO に聞く、今後の SaaS 採用基準

企業が SaaS を採用する基準は、自社で作る！OKULAB 流、SaaS アセスメントのポイントをご紹介します。

## SaaS 事業者への評価

### – いまの OKULAB の運営にあっているか

✓ Microsoft 組織の ID と連携できるか
✓ Azure AD を利用して多要素認証が可能か
✓ Audit Log API があるか
✓ 利用規約・セキュリティポリシー

### – OKULABの成長を加速させる事業者か

✓ コストの柔軟性（長期コミットを前提としない）
✓ 運営する事業者が未来を見据えているか
✓ マイクロサービス、サーバーレス、API エコノミーの親和性

## 担当社員の SaaS リテラシー

### – 社員が十分な知識を備えているか

✓ ソフトウェアやアプリの仕組みの理解
✓ ユーザー端末やネットワークへの理解
✓ ビジネス価値の理解

### – 適切な認証・認可を設定できるか

### – モダンな IT 運用に向けた発想力

【例】
・権限の管理（プロビジョニング）
・セルフパスワードリセット
・パスワード付き ZIP を廃止している
・アクセスログからの脅威検知

# 日本マイクロソフト/スマートキャンプ企業情報

Microsoft

**セキュアリモート窓口**

(セキュア リモートワーク相談窓口 | Microsoft 法人向けサイト)

SMARTCAMP

**総合問い合わせ窓口**

(https://smartcamp.co.jp/contact)