Money Forward Admina

SMPと周辺領域

— CASB、IdP/IDaaS、ISMS完全版 —

はじめに

近年、業務の効率化や柔軟な働き方の実現を目的に、SaaSを導入する企業が急増しています。SaaSは社内ネットワークに依存せず、インターネット環境さえあれば利用できるため、リモートワークやBYODなどの普及を後押し、多様な働き方を支えています。

一方で、SaaSの導入が進むにつれ、「誰が・どのサービスを・どのように使っているのか」を把握することが難しくなり、ライセンス管理やアカウントの棚卸、セキュリティ対策、コンプライアンス対応など、運用・管理面での課題が複雑化しています。

こうした背景を受けて注目されているのが、**SMP（SaaS管理プラットフォーム）です。**
SMPは、SaaSの利用状況やライフサイクルを一元的に管理することで、企業のIT運用を効率化し、セキュリティと統制の両立を実現します。

本ホワイトペーパーでは、SMPを軸に、CASB（Cloud Access Security Broker）、IdP（Identity Provider）/IDaaS（identity as a service）、ISMS（情報セキュリティマネジメントシステム）など、SMPと関係の深い周辺領域との関連性について整理し、それぞれの役割や違いをわかりやすく解説します。

SMPとは

SMP(SaaS管理プラットフォーム)とは

SMP（SaaS Management Platform）とは
企業が利用するSaaSを一元管理および効率的な運用を可能にするソフトウェアのことです

▽ ガートナー社が提唱するSMPの主な3つの機能

1

SaaSの検出

SaaSの情報を追跡

▽以下のソースを使用

- **SaaS API**
- **ネットワーク機器**
- **ブラウザ拡張機能**

また、SaaSを利用するユーザーの
アクティビティに関する情報も集計

2

SaaSの管理

SaaSの管理業務を一元化

▽以下のITタスクがシンプルに

- **アカウント発行**
- **ユーザーの入退職時の処理**
- **ライセンス管理**
- **部署のグルーピング**

3

セキュリティ

SaaSのコントロールセンター

▽以下のセキュリティ設定を一元化

- **アカウントに付与された権限情報**
- **データの保護**
- **アクセスのコントロール**

CASBとSMP

CASB(キャスビー)とは

CASB（Cloud Access Security Broker）とは
従業員のクラウドサービスの利用を可視化し、適切なセキュリティ対策を行うソリューションのことです

CASBは、2012年にアメリカのITアドバイザリー企業ガートナー社によって提唱された、情報セキュリティのコンセプトに基づいたソリューションです。
クラウドサービスを利用するユーザーとクラウドサービスプロバイダー（ベンダー）の間に配置され、オンプレミスやクラウドベースのセキュリティポリシーを制御するポイントとして機能します。
これにより、クラウドリソースへのアクセス時に企業のセキュリティポリシーが適用され、安全な利用が可能になります。

[具体的なセキュリティポリシー]
認証、認可、SSO、認証情報のマッピング、デバイスのプロファイリング、暗号化、トークン化、ロギング、アラート、マルウェアの検出・防止など

CASBの4つの機能

CASBは大きく分けて4つの機能を提供しています

可視化

どのユーザーがどのクラウドサービスにアクセスしているか可視化します。
ストレージサービスへのアップロード・ダウンロードを監視。
不審な動きや禁止ポリシー違反を検知し、リスクを可視化します。

データセキュリティ

クラウド上の機密情報を暗号化・監視し、情報漏洩や改ざんのリスクを検知。
アクセス権限を管理し、不正なデータ操作や持ち出しを防止します。

コンプライアンス

クラウドサービスの使い方が自社のセキュリティポリシーを満たしているか監査します。
自社の機密情報を定義し、認証強度、トランザクション量などを監視・制御。
クラウド利用の適正化を図ります。

脅威防御

クラウドサービスやウェブサイトのリスクを評価し、危険なクラウドサービスやマルウェア感染の恐れがあるサイトへのアクセスを制限。
企業のセキュリティリスクを最小限に抑えます。

シャドーIT検知におけるCASBとSMPの相違点

CASBとSMPは「シャドーITが検知できる」という点で共通しています
しかし、シャドーIT検知の目的とテクノロジー構造が異なります

	CASBのシャドーIT検知 セキュリティコントロール	SMPのシャドーIT検知 クラウドマネジメント
目的	■許可したクラウドのみ利用 ■社内ポリシーを徹底 ■セキュリティリスクから保護	■余分なクラウドを発見し、統合または削除 ■ライセンス、アカウントライフサイクルの適正化 ■未使用ライセンスの最適化
検知方法	リバースプロキシ、フォワードプロキシ、ネットワークログ、エージェント、API ベースなどのアプローチを組み合わる	SaaS API、IdPやMDMのAPI、OAuthの可視化、Browser拡張機能の一括配布などを活用した軽量なアプローチ
ネットワーク依存度	既存ネットワークを考慮した導入が一般的	既存ネットワークを考慮せず導入できる
検知の仕組み	新たにネットワークに介在	既存のクラウド環境や企業のアセットを活用

CASB？or SMP？

CASBとSMPのメリット/デメリット

	CASB セキュリティコントロール	SMP クラウドマネジメント
メリット	■より多くのユーザ通信を検知可能 ■様々なセキュリティアクションが可能 （リスク評価や通信の制御など）	■導入が簡単で低価格 ■セキュリティ以外の運用が可能 （アカウント管理、コスト削減など）
デメリット	■ハイエンドサービスのため高めの価格設定 ■既存のネットワークに介在するため、導入や運用に多くの工数が発生する	■セキュリティ統制などの要件が厳密な場合、CASBの方がより広範囲に細かい精度で検知可能

IdP/IDaaSとSMP

IdP(Identity Provider)/IDaaS(Identity-as-a-Service)とは

IdP/IDaaSとは、社内システムやクラウドサービスに対して、
ID認証、IDパスワード管理、シングルサインオン (SSO)、アクセス制御などを提供するサービスのことです

具体的には、認証情報を一元管理し、パスワードの管理を簡素化。
SAMLなどを用いたSSOにより、ユーザーのSaaSアクセスを円滑にするだけでなく、多様なアクセス条件を組み合わせることで、セキュリティレベルを向上させるサービスです。

IdP/IDaaSの機能 ①

ITアドバイザリー企業のガートナー社は、アカウント管理の領域において、
IdP/IDaaSのコア機能として以下を挙げています

統合的なID管理

内部・外部システム、ディレクトリ、同期ツールを含む、すべてのIDを一元的に管理

アカウントおよびプロファイル管理

管理者およびユーザーによるアカウント登録、パスワード管理、プロファイル設定、委任管理の提供

SSOとアプリケーションワークスペース

SSOの実施に加え、ユーザーが業務をスムーズに遂行できるアプリケーションワークスペースを提供

モダンなIDプロトコルと適応型アクセス

OAuth 2.0などの最新プロトコルに対応し、適応型アクセス（Adaptive Access）を活用したユーザー認証を提供

アクセス制御と通信管理

ユーザーアクセスに関する通信を管理し、不正アクセスのリスクを軽減

多要素認証(MFA)とSSOの統合

セキュリティ強化のため、MFAとSSOを組み合わせた認証機能を提供

IdP/IDaaSの機能 ②

ITアドバイザリー企業のガートナー社は、アカウント管理の領域において、
IdP/IDaaSのコア機能として以下を挙げています

BYOI(Bring Your Own Identity)の対応

従業員のID管理に加え、個人所有のIDを業務で使用するBYOI対応により、ソーシャルメディアアカウントなどのパブリックIDを統合することで、柔軟な認証手段を実現

APIアクセスの制御と認証・認可

APIを用いたアプリケーションの動作を管理し、安全な認証・認可を実施

最新のIDプロトコル対応

SAMLやOpenID Connectを活用し、SaaSや標準ベースのWebアプリケーションに対する迅速なアクセス、SSO、MFAを可能にする機能を提供

非標準アプリケーションの有効化

標準SSOプロトコルに対応していないレガシーWebアプリケーションへのアクセスをサポートし、SSOやMFAの適用を実現

監査・分析機能

アクセスイベントの履歴、ログ、ID分析情報を提供し、管理および実行時の可視性を向上

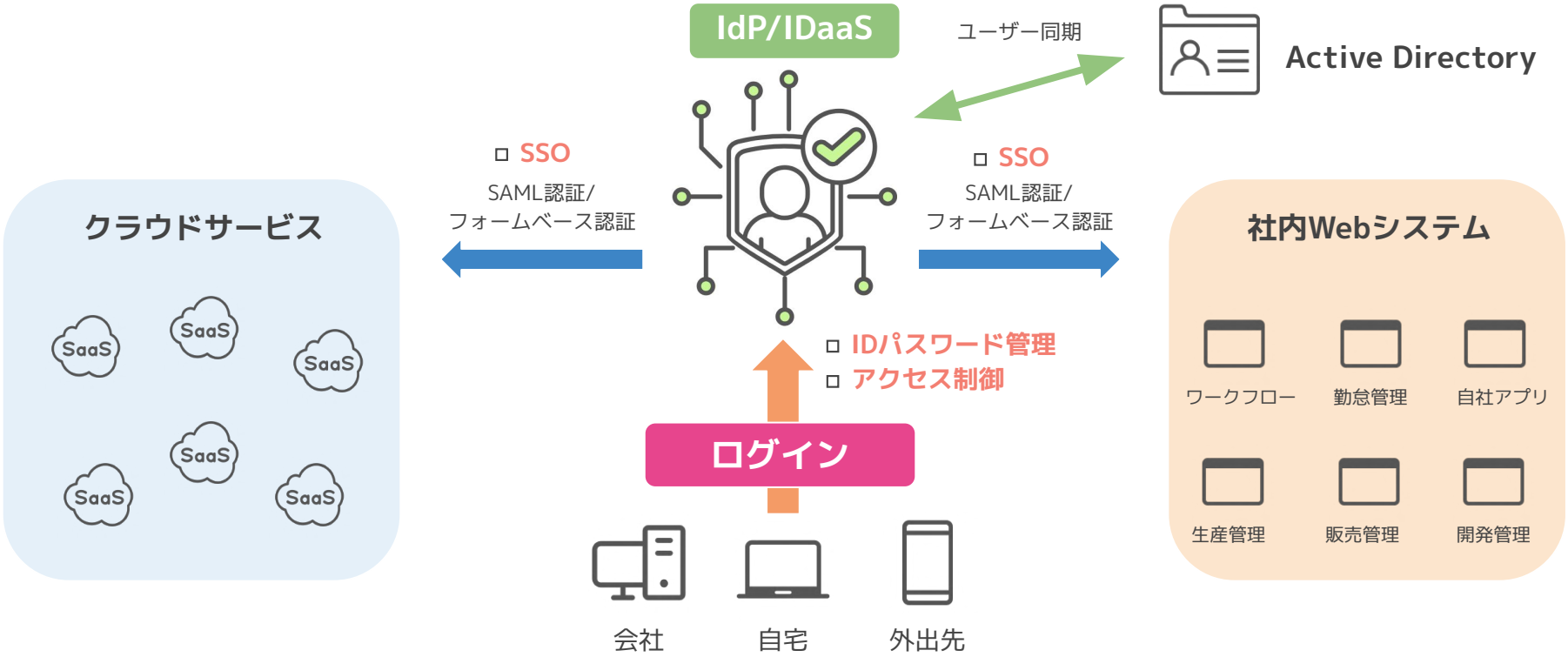
IdP/IDaaSとSMPの共通点

IdP/IDaaSとSMPは異なるアプローチを取るものの、以下のような共通点があります

IdP/IDaaS		SMP
ユーザー認証やアクセス管理を一元化し、IT部門の管理負担を軽減	組織のIT管理を効率化	SaaSの利用状況を可視化し、アカウントやコストの管理を効率化
SSOやMFAを提供し、不正アクセスを防ぐ	セキュリティを強化	シャドーITを可視化し、管理外のセキュリティリスクを低減
SAMLやOpenID Connectなどの標準プロトコルを通じてSaaSや社内システムと統合可能	他のシステムと統合が可能	API連携やディレクトリサービスとの統合によって、より包括的なSaaS管理が可能
アクセスログの管理や、ガバナンスの強化に貢献	内部統制を推進	SaaSの利用状況を把握し、ライセンス管理や規制対応をサポート

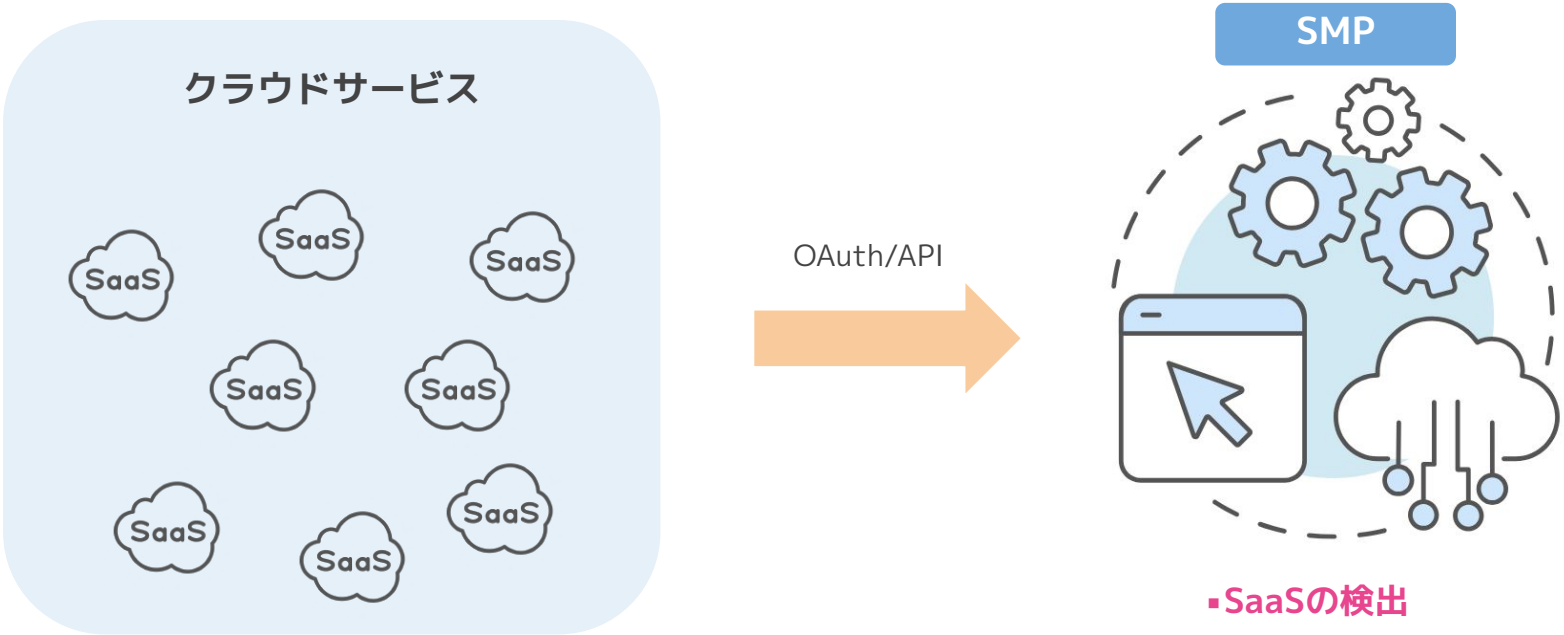
IdP/IDaaSの構成

IdP/IDaaSは、利用する社内システムやSaaSに対して、
ID認証、IDパスワード管理、SSO、アクセス制御などを提供



SMPの構成

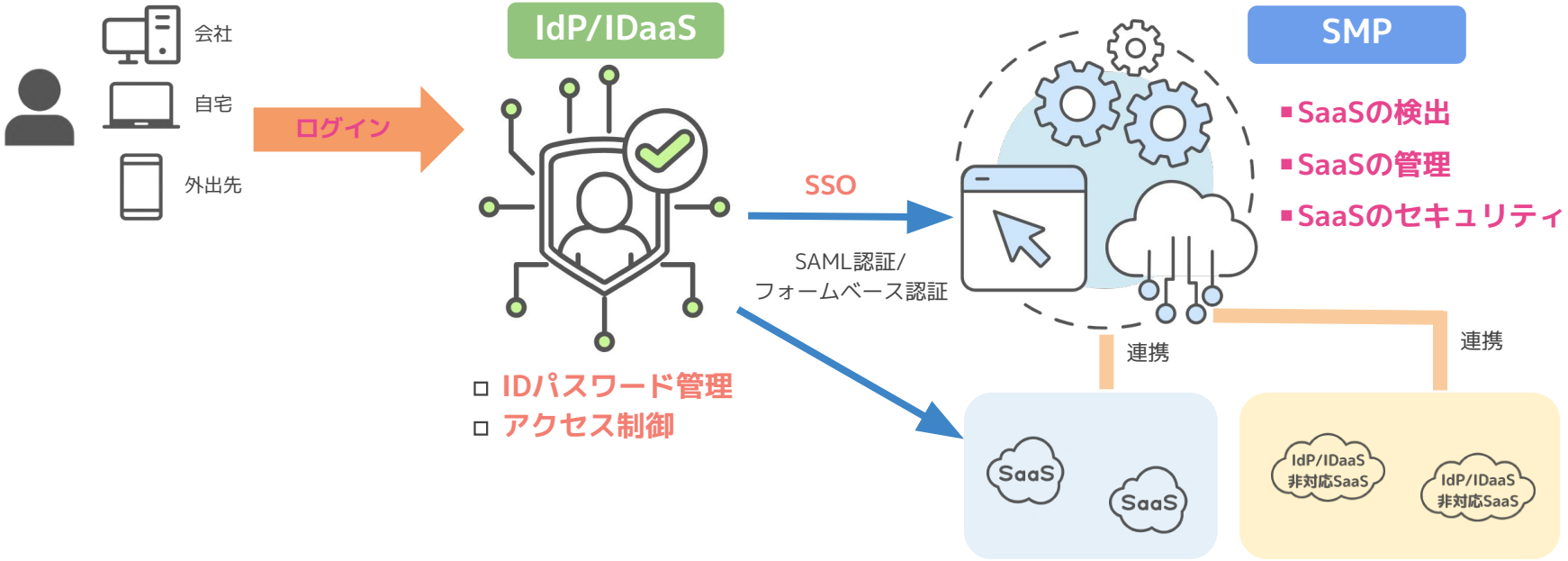
SMPは、利用するSaaSに対して、検出、管理、セキュリティ機能を提供
SaaSとの連携方法はOAuth、APIが用いられます



- **SaaSの検出**
- **SaaSの管理**
- **SaaSのセキュリティ**

IdP/IDaaSとSMPを併用した、効率的で統制の取れた構成

IdP/IDaaSとSMPを併用することで以下が可能になり、SaaSを効率的に一元管理できます
・IdPのSSO機能で、SMP管理コンソールに効率的にアクセス
・SMPを通じて、IdPが対応していないSaaSを管理



IdP/IDaaSとSMPを併用した導入がおすすめ

IdP/IDaaSは「IDベース」で認証を管理し、SMPは「SaaSベース」でSaaSを管理します
これら異なるアプローチは相互補完的であり、併用することで高度なID管理とSaaS管理を実現できます

導入時の考慮ポイント

要件とリソースを考慮してツールを選定しましょう。

IdP/IDaaSは認証管理に優れたサービスですが、既存システムとのID同期やIDの整理が必要となり、対象が全従業員に及ぶため、導入には大きなリソースが求められます。
また、全社的に利用される認証基盤は、クラウドサービスであっても短期間でのリプレースが難しく、慎重な選定が必要です。

一方、SMPは認証管理に適したサービスではありませんが、導入が容易であり、SaaSの可視化を迅速に実現できます。
そのため、**IdPの導入前におけるセキュリティリスク管理の手段の一つとしても活用可能**です。

ISMSとSMP

ISMS(情報セキュリティマネジメントシステム)とは

ISMS（情報セキュリティマネジメントシステム）とは
情報の機密性・完全性・可用性を維持し、絶えず改善を行うための仕組みのことです

社内の情報を守るためには、社員一人ひとりが心がけるだけでは足りません。
また、一部の専門家だけが理解している状態でも意味がありません。
組織として情報を適切に管理できる体制を構築する必要があり、そのための仕組みがISMSです。

情報セキュリティの3要素の確保と維持

情報セキュリティを徹底し、
組織がもつ情報の外部流出を防ぐとともに、利用しやすい状態で情報を保護することが重要です

▽ ISMSでは、情報セキュリティの要素として以下の3つを定義

1

機密性

情報資産を利用してはいけない
人が利用できない状態

2

完全性

情報資産が改ざんや
削除をされない状態

3

可用性

情報資産を利用すべき人が
速やかに利用できる状態

機密性と完全性は、第三者による不正利用や、削除・改ざんを防ぐための重要なセキュリティ要素です。
しかし、機密性と完全性を求めるあまりセキュリティが強固になり、利用者が必要なときに必要な情報にアクセスできない状態に陥るのは問題です。
そこで重要な観点が可用性です。ISMSでは上記3つの要素をバランスよく維持することが求められます。

企業が保有する情報資産

企業や組織が保有する
「顧客の個人情報」「従業員の人事情報」「会社の財務情報」のことを“情報資産”といいます

情報資産が悪意のある第三者に狙われると、個人情報の流出など深刻なリスクを招く可能性があります。
これら資産価値のある情報は適切な情報セキュリティによって保護することが不可欠です。

情報資産の例

情報資産には情報システムやソフトウェアも含まれ、ISMSでは保護すべき対象とされています

企業/組織が保有する情報資産の例

- 生産計画、製品技術情報（製品の設計図面・仕様書・部品表・作業手順など）
- 経営や事業計画、新製品情報、情報セキュリティなど戦略情報、企業間契約書類など
- 企業／組織の財務情報
- 顧客情報（顧客名や住所、電話番号、クレジットカード情報、注文履歴、仕入先・販売先など）
- 人事情報（従業員個人の携帯番号やメールアドレス、住所、採用時の応募情報、給与・昇給・勤怠情報、マイナンバーなど）
- 設備機械や施設、物理的資産（社用車など）
- **情報システム、ソフトウェア（SaaS）**、社内ネットワーク（サーバー／パソコン、通信機器等）、DB、IT技術ノウハウなど
- 無形資産（製品ブランドや企業イメージなど）

情報資産を保護するための3STEP

保有する情報資産のうち、対応が必要となる可能性のあるものを洗い出す

洗い出した情報資産の、保管方法、利用場所、利用者、管理状況を確認する

情報資産管理台帳を作成して適切に管理する

抽出された情報資産は
リスクアセスメント（リスク分析・評価）の対象となり、**機密性・完全性・可用性の観点**から対策の必要性を検討する

情報資産管理台帳の作成

情報資産管理台帳へ利用SaaSのアカウント、管理者も記載します

情報資産管理台帳の項目例

① 業務分類　　：人事・経理・営業・調達・共通など
② 情報資産名　　：**利用SaaS名**、給与システムデータ、請求書控え、メールデータ、社員名簿、受注契約書など
③ 利用範囲　　：部署名、処理担当名など
④ 管理部署／管理責任者：**部署名および管理責任者**
⑤ 媒体の種類　　：書類・電子データなど
⑥ 保存先　　：社内サーバー、外部記憶媒体、モバイル機器、クライアントＰＣなど
⑦ 個人情報の有無　　：有無
⑧ 評価値（機密性／完全性／可用性）
⑨ 保存期間　　：文章保管規定など企業・組織の社内規程参照
⑩ 登録日（更新日）

SaaS管理のファーストステップ

SaaS管理のファーストステップ

情報資産管理台帳作成において、
シャドーITやSaaSの利用状況を可視化し、素早く情報を反映できるかがポイントとなります

利用SaaS

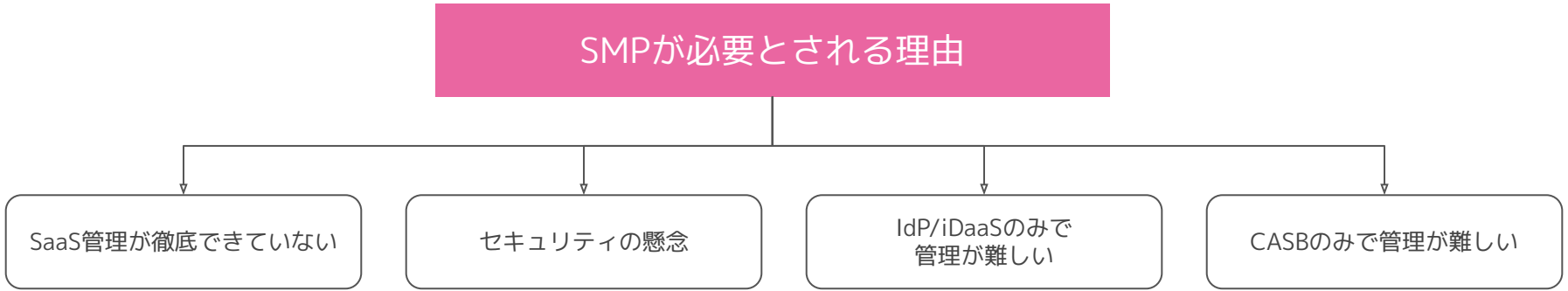
情シスが把握(承認)しているSaaS

- **情シスが主幹**となり、従業員に配布しているSaaS
- 部門利用の場合、ワークフローなどで**情シスの承認を得て利用**しているSaaS

情シスが把握していないところで現場が利用しているSaaS

- 情シスの承認を得ずに、現場判断で利用しているSaaS
- 外部企業の環境下で、招待を受けて利用しているSaaS
- トライアルなど、無課金で利用しているSaaS

SMPが必要とされる背景



SaaS Management Platform
マネーフォワード Adminaとは

マネーフォワード Adminaとは

従業員が利用するSaaS/デバイスを一元管理するサービス

✔会社にあるIT資産情報を統合

✔3つの台帳を自動で作成

- 従業員軸のIT資産台帳
- SaaS軸の台帳
- デバイス軸の台帳

✔それぞれの台帳を更新する必要なし

マネーフォワード Adminaの概要

管理業務の効率化/セキュリティ強化/コスト削減を実現

管理業務の効率化	セキュリティの強化	コスト削減
✔従業員/SaaS/デバイス台帳を統合	✔退職アカウントを自動検知	✔未利用アカウントを自動検知
✔SaaS台帳の自動作成	✔シャドーIT検知	✔SaaSコストの可視化/自動レポート
✔SaaSアカウントの発行/削除	✔公開/外部共有ファイルを検知	✔契約台帳管理

コラボレーション型SaaS管理の実現

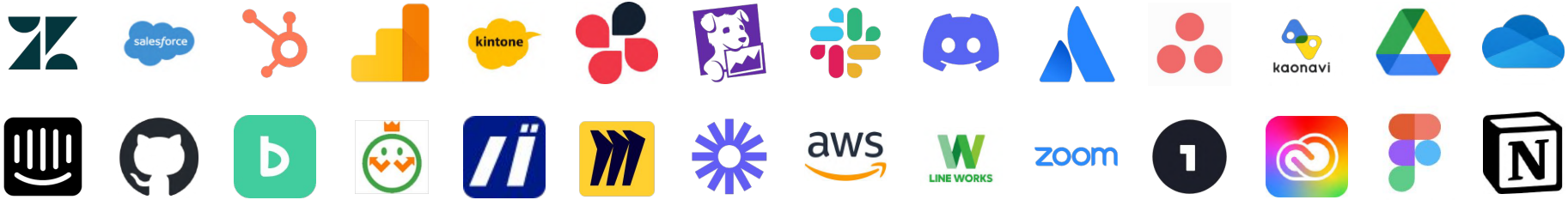
部門ごとのSaaS利用を促進し、企業成長のスピードを維持しながら
情シス部門による全体像の把握・セキュリティ対策・コスト最適化を実現

自部門のSaaSのみ把握・管理

それぞれの部門が管理しつつも、全体像を把握

リリースから4年で300以上のSaaSと連携

連携できるSaaSが多いからこそ、効率的かつ網羅的な管理が可能に



一部連携SaaS抜粋

< お客様の要望に対応してSaaSの連携開発も実行 >

Rentio

ご担当者 様

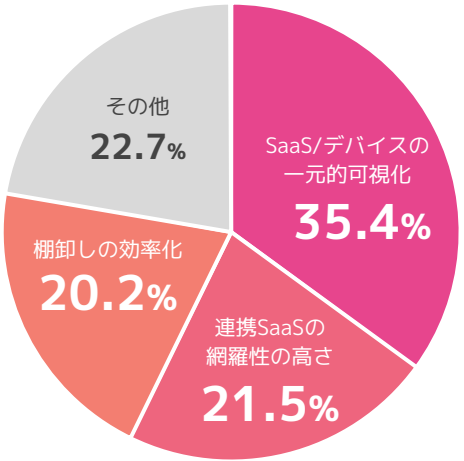
弊社では以前からKandji というMDM製品を運用しています。
これは主に欧米向けの製品なのですが、近頃複数の代理店で取り扱いがスタートしており、これから日本でも流行りそうな予感がしています。

▶ 1ヶ月で連携の実装！

マネーフォワード Adminaが選ばれる理由

おかげさまで多くのユーザー様にAdminaをご利用いただいております
Adminaをみなさまが選ばれた理由を一部ご紹介

課題解決に最も役に立った
Adminaの特徴



お客様の声
一部ご紹介

情報システムの視点から見ると、Adminaのようなツールの導入が、アカウント管理の効率化や上場企業に求められるIT統制に対応する手段となります。また、費用対効果の透明性向上も期待できます。Adminaを利用することで、企業の運用がより効率的になり、管理面での向上が見込まれます。

Adminaは、一言でいうと本当に使いやすいです！一元的な管理と退職アカウント、公開ファイルの管理はリスクマネジメントに直結します。コストと製品価値を考慮すると、Adminaは圧倒的な価値を提供します。また、今後のポートフォリオ拡充にも対応できる製品です。

アワード
バッジ

ITreview
SaaS管理で10期連続でLeader取得

BOXIL SaaS
Good Service 受賞

導入企業

SaaS

UZABASE　LayerX　RevComm　STORES　IOX　yappli　MIXTEND

弁護士ドットコム　smartround　mi-6　ABEJA　ULURU　SHANON Marketing is Science　トヨクモ

人材

dip　ONE CAREER　Wantedly

LAPRAS　LabBase　PIECE to PEACE

Webサービス

Makuake　モノタロウ　favy　FLN

レコチョク　note　SHIMAUMA PRINT

サービス

OPEN HOUSE GROUP　POLA ORBIS HOLDINGS

令和トラベル　山岡家

開発

Sun*　TECHORUS　Speee

SonicGarden　Serverworks

導入までの流れ

ご導入まで3つのステップ

STEP1	STEP2	STEP3
無料トライアル	サポート担当とMTG	ご契約
14日間フル機能を無料でトライアル可能	**トライアル時にフォローMTGが可能**	**トライアル環境をそのまま使える**
300を超えるSaaSと連携し、 社内のSaaS可視化や自動台帳化を ぜひお試しください	サポート担当から、設定方法や使い方、 メリットなどをオンラインミーティング にてレクチャー可能です	Adminaから簡単にお支払い登録可能。 トライアルで設定いただいた情報を そのまま引き継いで開始できます

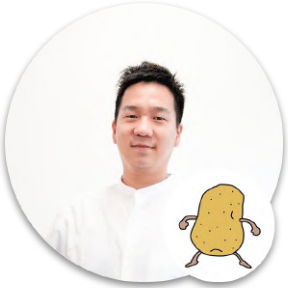
会社紹介

会社名	マネーフォワード i 株式会社
代表	今井 義人
創立年月	2021年2月
所在地	東京都港区芝浦3-1-21 msb Tamachi 田町ステーションタワーS 21F
株主	株式会社マネーフォワード(100%)
事業内容	情シス向けのSaaS/デバイス管理サービス マネーフォワードAdminaの開発・提供

役員紹介

CEO
今井 義人

2009年: Apple Japan
2012年: ミイル株式会社(プロダクトマネージャー)
2015年: 株式会社マネーフォワード
　　マネーフォワードクラウド経費 本部長就任
2021年: マネーフォワード i の代表取締役に就任



取締役/CPO
村上 勝俊

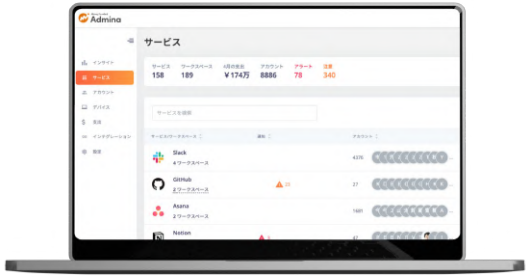
新卒からインフラ開発運用保守、PMを担当
社内開発プラットフ ォームの運用整備やクラウド導入
支援、クラウド利用ポリシーの整備を実施
2019年: 関西開発拠点長に就任し京都へ移住
2020年: 本事業を企画立案
2021年: 社内起業し、マネーフォワード i を創業

取締役
中出 匠哉

2001年: ジュピターショップチャンネル
注文管理・CRMシステムの開発・保守・運用を統括
2007年: シンプレクス株式会社
証券会社向け株式トレーディングシステムの開発・保守・運用に注力。FXディーリングシステムのアーキテクト兼プロダクトマネージャーとして開発を統括
2015年: 株式会社マネーフォワード
Financialシステムの開発に従事。
2016年: CTOに就任

お問い合わせ

Money Forward Admina



Money Forward i

サービス規約

サービスサイト

コミュニティうちの情シス

bizdev@i.moneyforward.com