



クラウドサービスの利用は大丈夫？ IDaaSによるセキュリティ対策を実現

キヤノンマーケティングジャパン株式会社

セキュリティソリューション事業推進部

友納 源



想いと技術をつなぎ、想像を超える未来を切り拓く



キヤノンマーケティングジャパン株式会社
セキュリティソリューション事業推進部
セキュリティソリューション促進課

友納 源（とも の う げん）

活動内容

セキュリティ製品の販売促進を担当

セキュリティリスクを抱えるお客様の課題を解決

自己紹介



01

クラウドサービスの問題点

02

ID Entranceのご紹介

03

ID Entranceのデモ

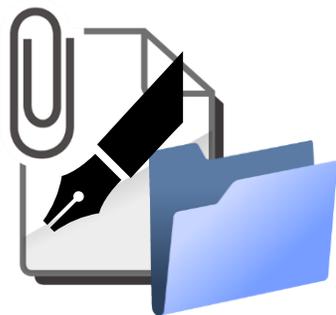
04

本日のまとめ

クラウドサービスの問題点



- クラウドサービスとは、インターネット経由で利用できるサービス全般を指す。
機器の購入やシステム構築が不要になり、
管理・運用の手間や時間の削減や業務効率化、コストダウンを実現
- 災害対策やBCP対策としても有効



契約後、スムーズに利用可能



どこでも、利用可能



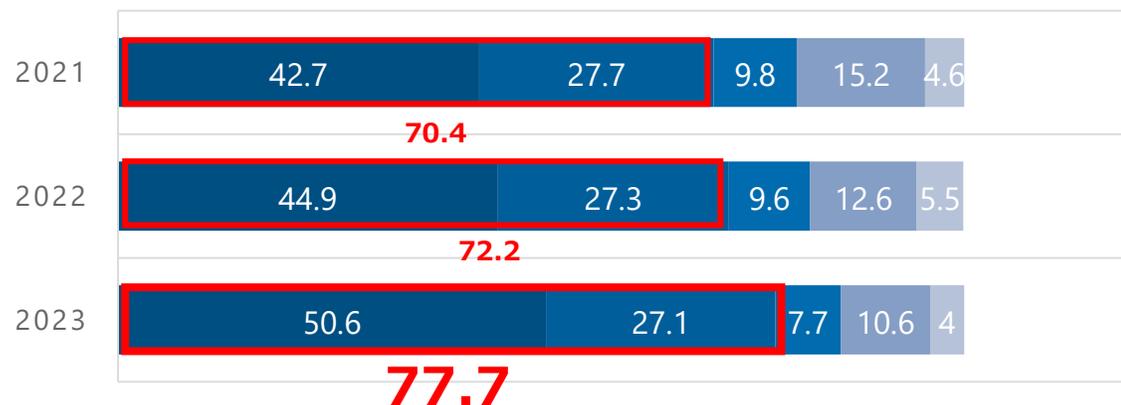
コストダウン

IT基幹システムの見直し時に注目されているのがクラウドサービス



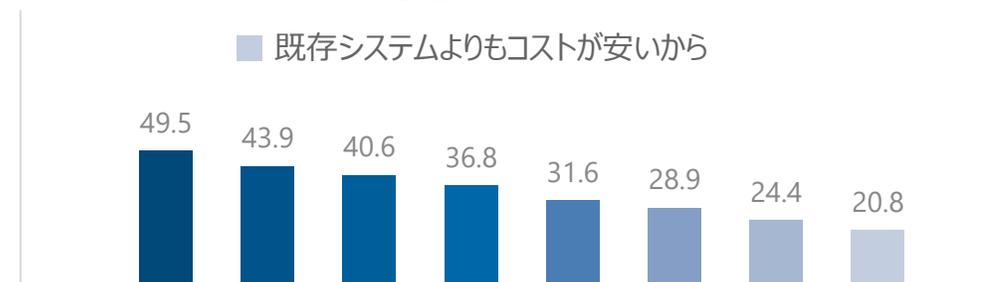
クラウドサービスの利用状況

- 全社的に利用している
- 一部の事業所または部門で利用している
- 今後利用する予定がある
- 利用していないし、今後も利用するつもりはない
- よくわからない



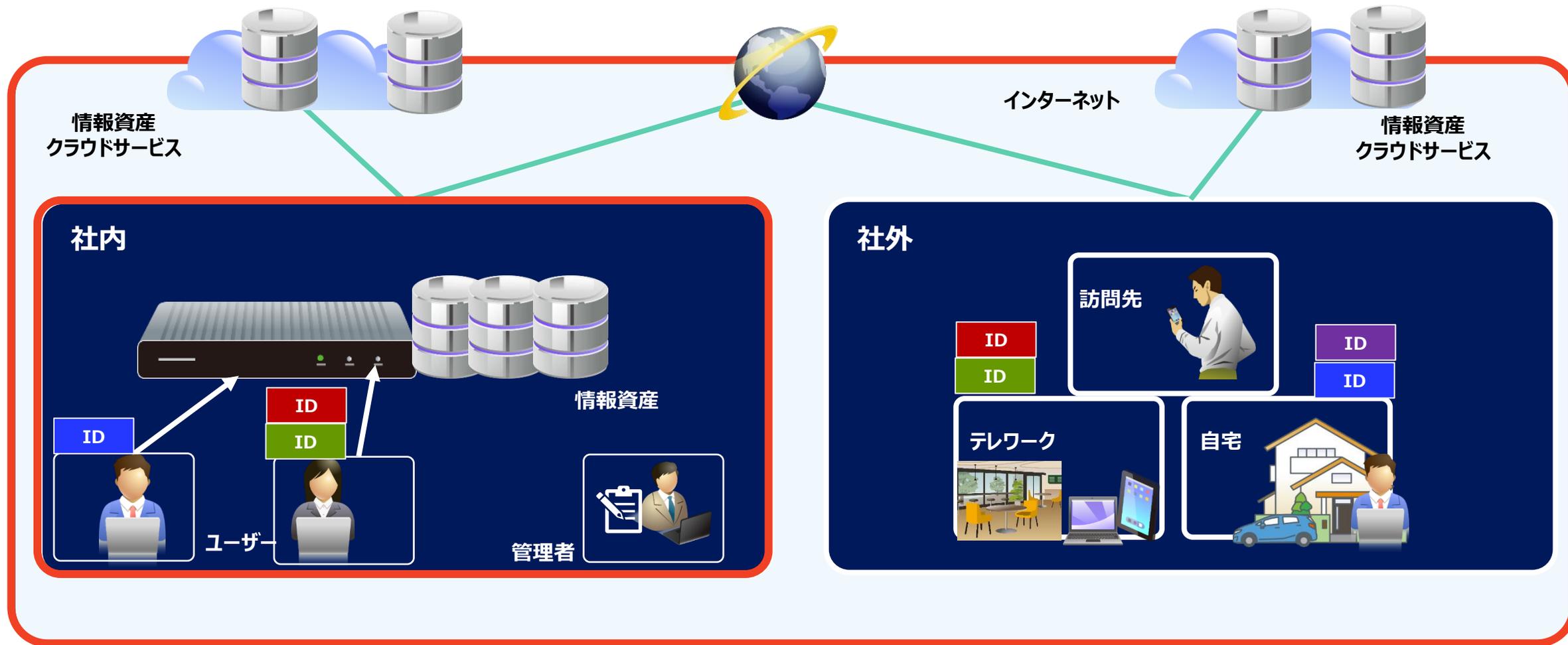
クラウドサービスを利用している理由

- 場所、機器を選ばずに利用できるから
- 資産、保守体制を社内に持つ必要が無いから
- 安定運用、可用性が高くなるから
- 災害時のバックアップとして利用できるから
- サービスの信頼性が高いから
- システムの容量の変更などに迅速に対応できるから
- システムの拡張性が高いから
- 既存システムよりもコストが安いから



出典：総務省「令和5年 通信利用動向調査」

クラウドサービス利用企業は7割超、場所・機器を選ばずに利用可能な点が評価されている

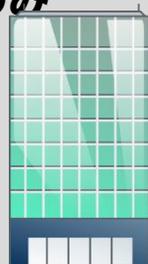


ネットワークのアクセス経路は「社内から社内」だけでなく、多様化



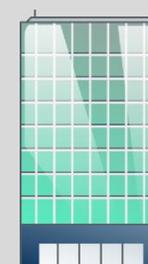
ID管理

ID管理は社内のみ



ID管理

ID管理は社内と社外



セキュリティ対策

情報資産は社内がメイン



セキュリティ対策

情報資産は
社内とクラウドサービス

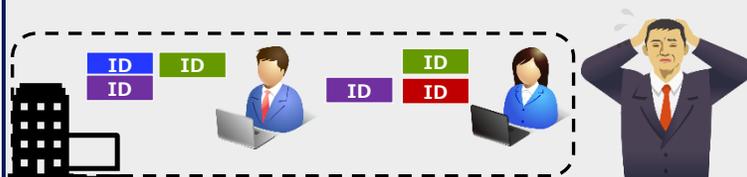
ネットワーク環境の変化により、ID管理とセキュリティ対策の見直しが必要



ID管理（管理者側）の問題点

管理が煩雑化・負担増加

- 1ユーザーごと、**複数のIDを管理**
- **IDの制御・管理が大変**
- 従業員のパスワード変更依頼の増加



ID管理（ユーザー側）の問題点

ユーザーの非効率な業務対応

- クラウドサービスごと**多数のID/パスワードを覚えられない**
- クラウドサービスごとにログインが必要



セキュリティ上の問題点

不正利用・不正アクセスのリスク

- 情報資産はクラウドサービスごとに保管され、バラバラにある
- 各ユーザーの**アクセス権が制御できていない**

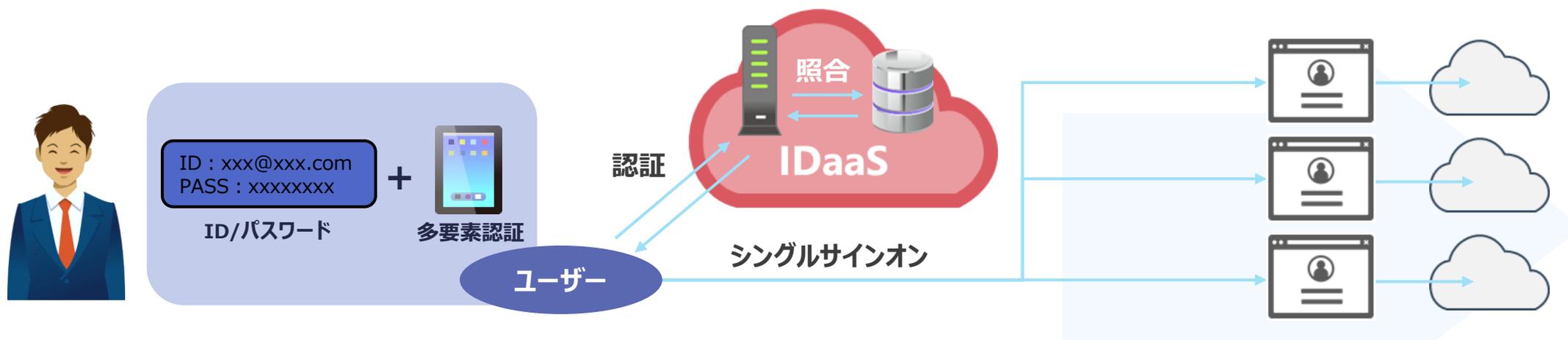


管理の煩雑化や不正利用・不正アクセスの大きな問題点が存在

ID Entranceのご紹介



- IDaaSとは、“**Identity as a Service**”の略称であり、**SaaS型のID管理サービス**です。
- ID情報を一括管理し、クラウドサービスへ連携することで効率的な認証が可能
- ログイン時の多要素認証やクライアント証明書の利用などを行い、セキュリティ対策



クラウドサービスと連携し、ID管理とセキュリティ対策を実現



クラウド型統合ID管理サービス

ID Entrance

クラウド型認証・認可サービス

+

サポートセンターサービス

シングルサインオン

ユーザー管理

認証認可ポリシー

多要素認証

クライアント証明書(オプション)

AD連携:ID情報同期機能(オプション)

お問合せ対応

設定支援/設定代行

ポータルサイト運営

障害対応

クラウドサービス連携支援

ライセンス価格にサポートサービスが含まれた親切設計

ID Entranceはクラウド型認証・認可サービスとサポートセンターサービスのセットで充実

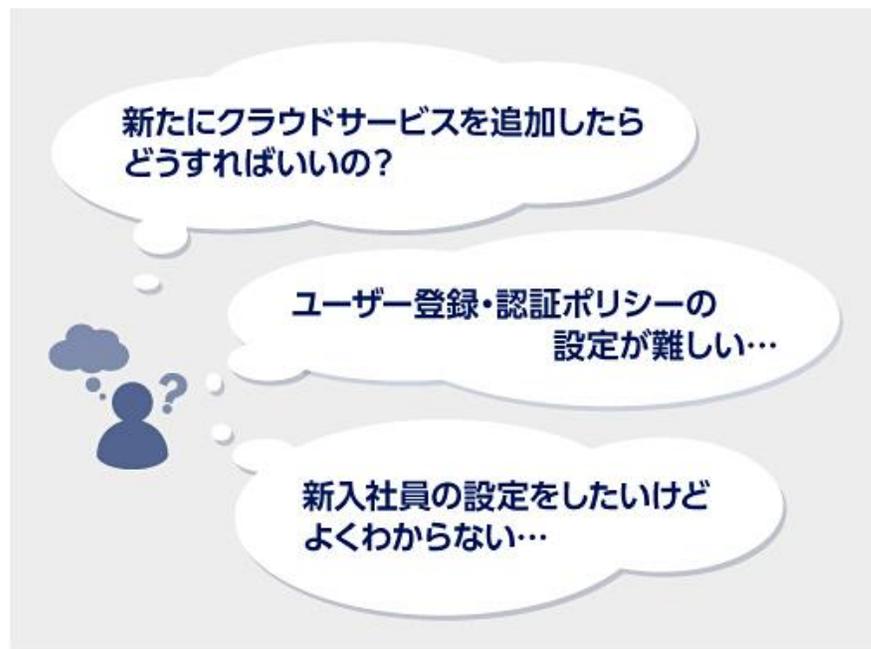


No	機能名	概要
1	アカウント情報管理	本サービスを利用するアカウントとパスワードを作成します。 アカウントは1件ごと、またはCSVファイル（最大100件まで）による一括編集が可能です。
2	グループ情報管理	複数のアカウントを束ねるグループを作成します。 グループは1件ごと、またはCSVファイル（最大100件まで）による一括編集が可能です。
3	デバイス情報管理	アカウントに紐づくデバイス情報を登録可能です。主にクライアント証明書発行に利用します。 デバイスは1件ごと、またはCSVファイル（最大100件まで）による一括編集が可能です。
4	クライアント証明書管理	※オプション機能 1アカウントあたり最大5デバイス分のクライアント証明書発行が発行可能です。MACアドレスやIMEIなどのデバイス固有情報に紐付けて発行可能なため、管理者が許可したデバイスだけに証明書を導入したアカウント認証が可能です。
5	AD連携：ID情報同期機能	※オプション機能 お客さまのActive Directory環境のユーザー情報をID Entranceに連携することができます。 ID Entranceのアカウントを既存のドメインコントローラーで管理できるため、2重での管理が不要になります。
6	クラウドサービス連携	SAML/OIDCに対応するクラウドサービスと連携し、シングルサインオンを実施します。
7	アカウント認証	アカウント情報とパスワードによる認証に加え、ワンタイムパスワードやクライアント証明書を使用した認証を実施します。
8	シングルサインオン	本サービスに登録したアカウント情報をもとに、お客さまが本サービスと連携済みのクラウドサービスへ、SP-initiatedおよびIdP-initiated（クラウドサービスが対応の場合）によるシングルサインオンを可能にします。
9	認証認可ポリシー	アカウント認証に際しての多要素認証、クライアント証明書認証、IPアドレスアクセス制限などの認証ポリシーを、アカウントおよびグループごとに設定、管理できます。
10	ファイル授受	アカウントやクラウドサービス連携の設定代行の際に用いる、お客さま記入のファイルのセキュアなやり取りを行います。



No	機能名	概要
1	問い合わせ対応	各種QAを対応いたします。受付時間 平日：9時-17時 電話・メール対応
2	設定支援/設定代行	本サービスと他社クラウドサービスとの連携設定サポート、および本サービス側(Idp)の設定の代行を提供
3	ポータル運営	契約ユーザー様向け各種情報を提供いたします。

サービス利用時によくあるお困りごと



サポートセンター

受付時間：平日9時～17時

受付体制：電話・メール

- 設定支援/設定代行でおまかせ!
- お客様のアカウント登録作業を代行!

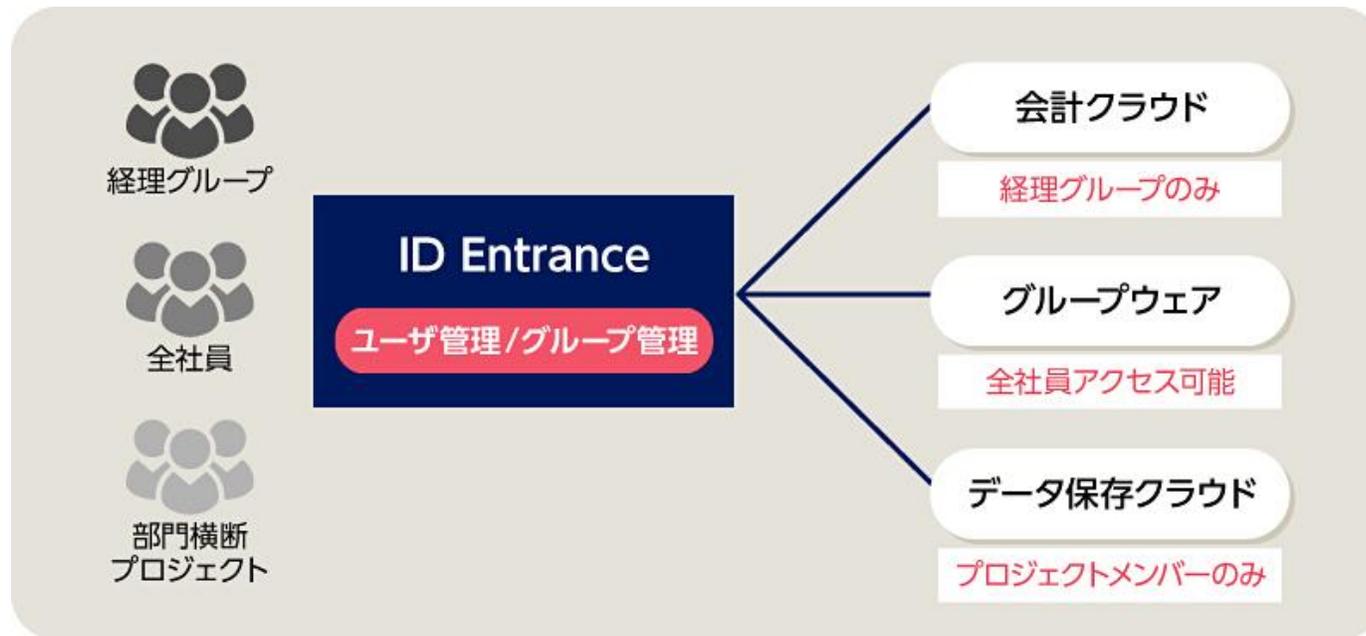


スムーズな導入・運用を実現!

**アカウント
登録・変更・削除**



例) グループ情報管理と認証認可ポリシーを使う場合



管理者の悩み

- ユーザーをグループに分けてアクセス制御をしたい



これで解決

- ユーザーが所属するグループごとにアクセスポリシーを制御
- グループ単位でIPアドレス制限やワンタイムパスワード認証、クライアント証明書認証を設定

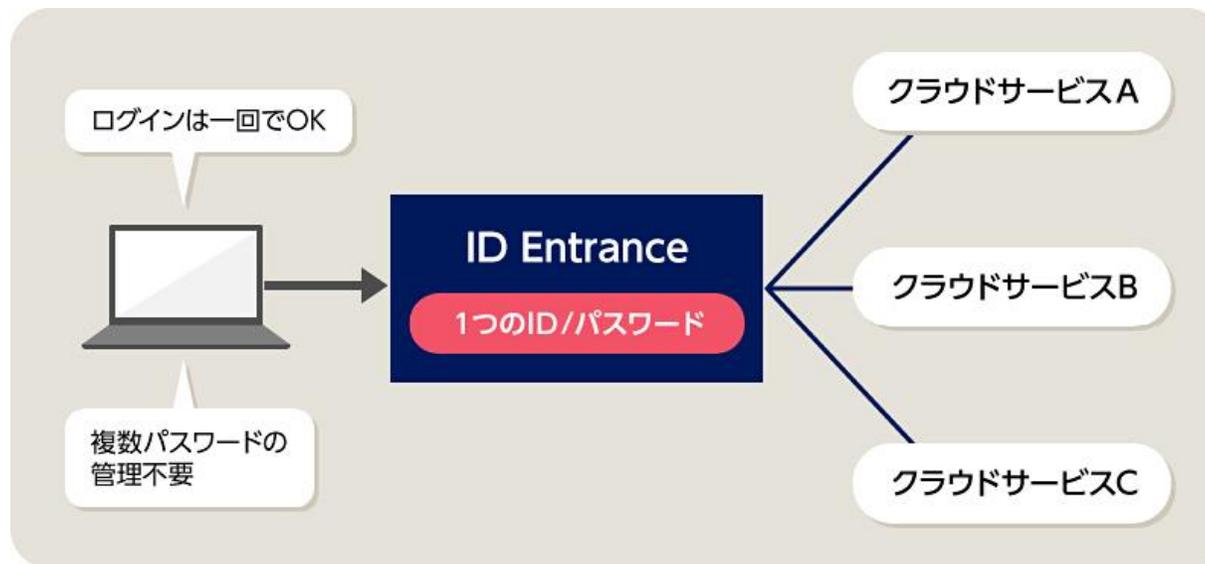
ID管理

セキュリティ強化





例) シングルサインオンを使う場合



利用者の悩み

- クラウドサービスごとにユーザーID/パスワードを入力するのが面倒
- セキュリティ上、問題があるとわかっているけど**同じパスワードを使いまわしてしまう**



管理者の悩み

- パスワードがひとつ破られてしまうと、他のクラウドサービスも**侵入されてしまう**リスクがある



これで解決

- ID EntranceでID/パスワードを一元管理
- クラウドサービスへのアクセス時にID Entranceがユーザ認証を実施
- 一度認証を行えば、その後の**パスワード入力は不要**に
- 複数クラウドに同じパスワードを使いまわして保存しないので**セキュリティ強化**

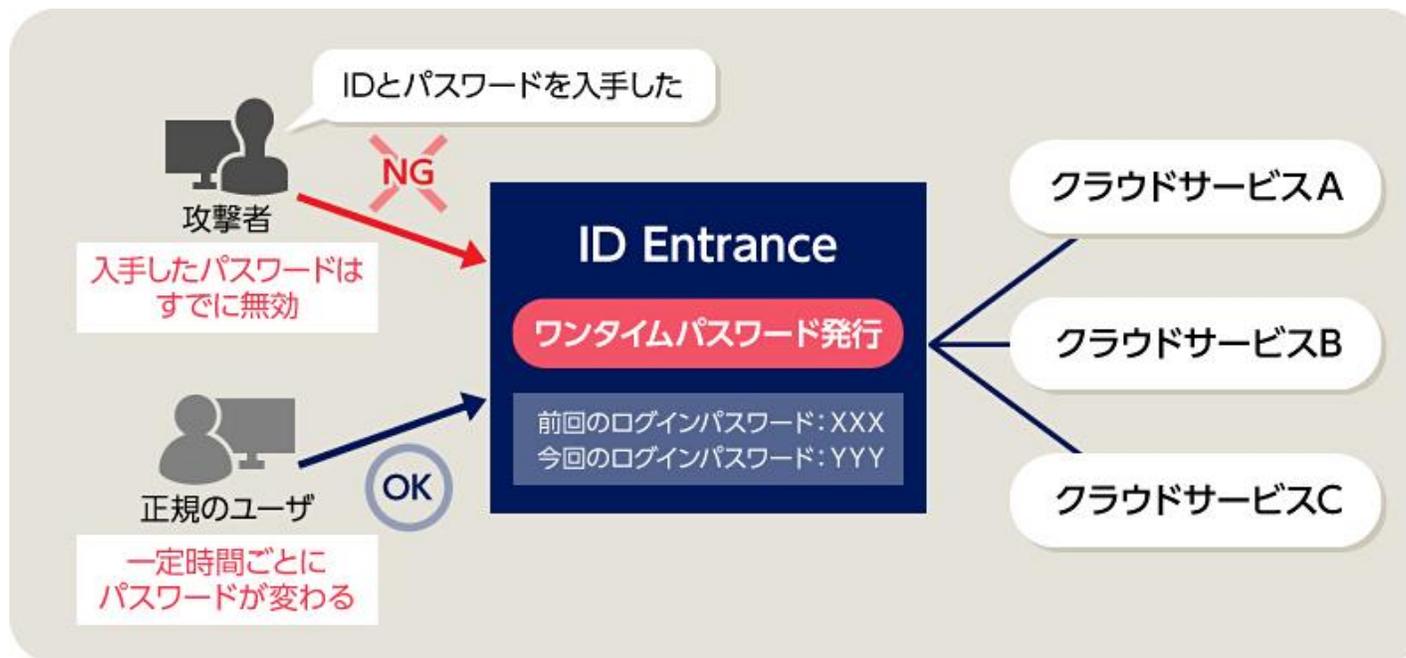
利便性向上

セキュリティ強化





例) アカウント認証 (ワンタイムパスワード) を使う場合 (別途オプション)



管理者の悩み

- パスワードがもれて不正侵入をされてしまうと情報が漏洩してしまう
- パスワード管理は最終的に各個人に委ねられるためリスクが残る



これで解決

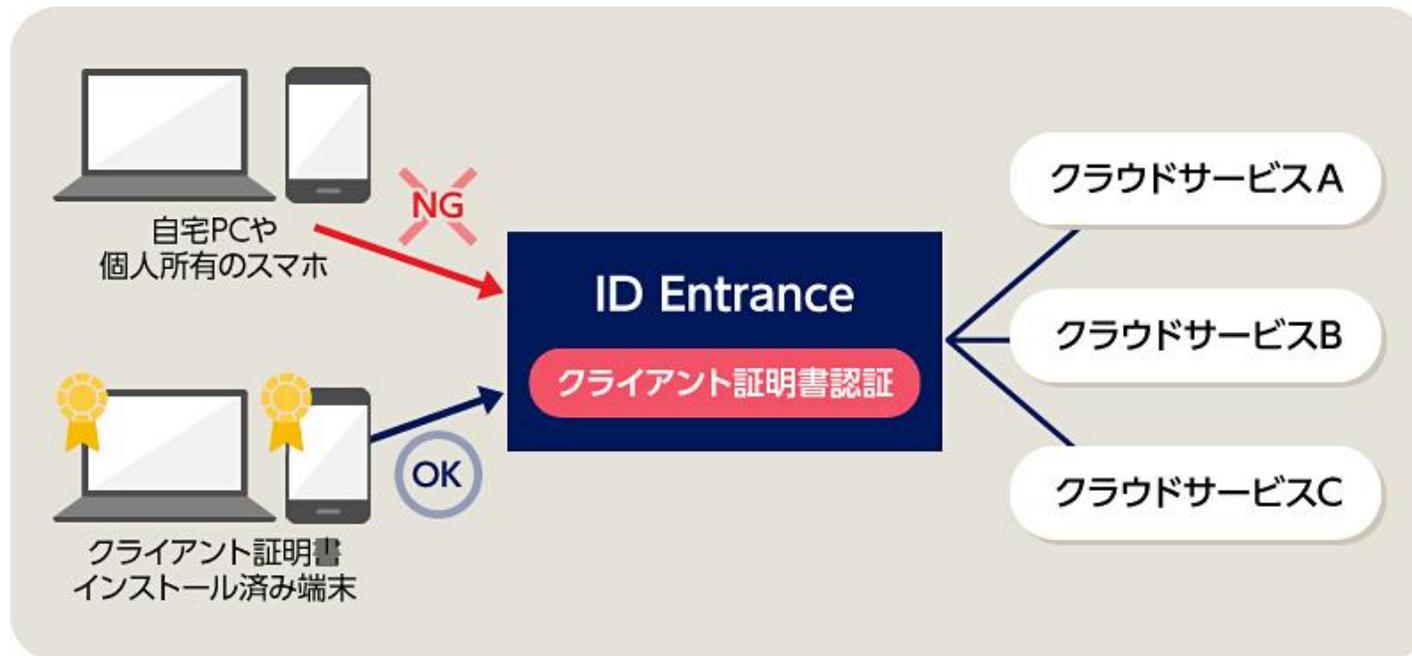
- ワンタイムパスワード機能を利用して認証の都度有効なパスワードを発行、パスワードが漏れても**第三者のログインを防止**



セキュリティ強化



例) アカウント認証 (クライアント証明書) を使う場合 (別途オプション)



管理者の悩み

- ❑ 会社配布の端末以外からもクラウドサービスにアクセスできてしまう
- ❑ アカウントを共有しているのですでに退職した元社員もログインできてしまう
- ❑ 認証セキュリティを破られたら情報が漏洩してしまう



これで解決

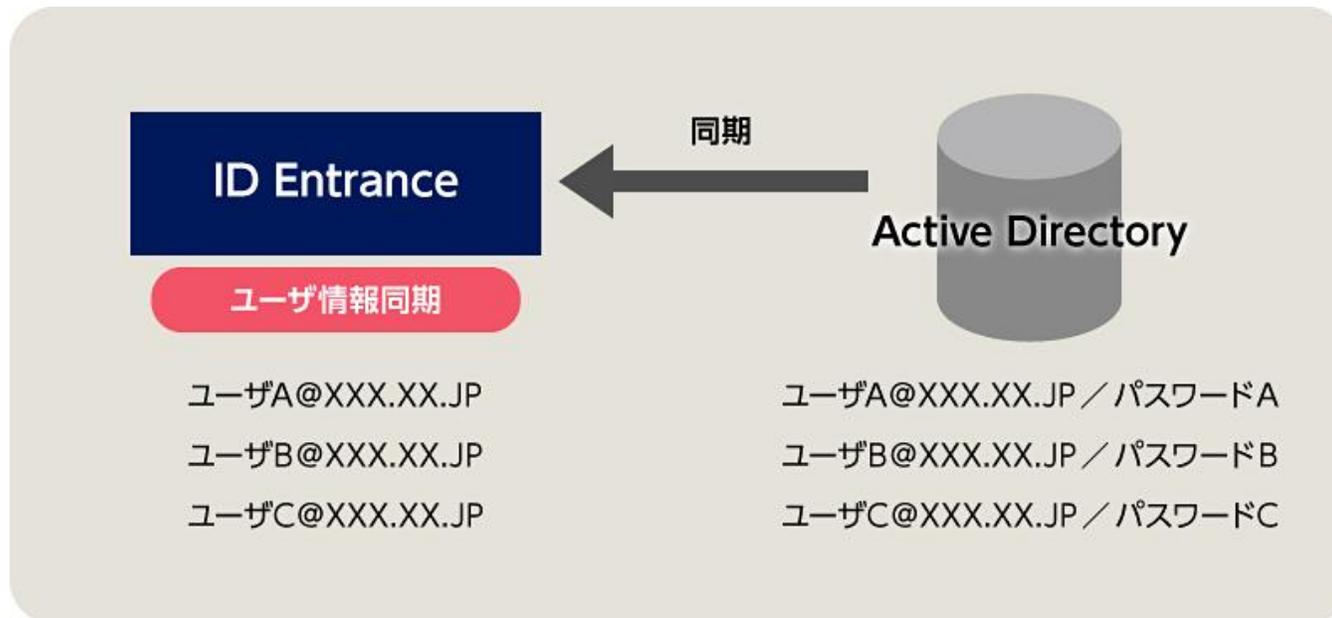
- ❑ クライアント証明書インストール済みの端末のみアクセス許可
→セキュリティに不安がある管理外端末からはアクセスできない
→ID/パスワードを知っていても退職者はアクセスできない



セキュリティ強化



例) AD連携：ID情報同期機能（別途オプション）を使う場合



管理者の悩み

- 社員のID情報をクラウドサービスとActive Directoryで別々に管理するのが面倒



これで解決

- 「AD連携：ID情報同期機能オプション」により、社内のActive DirectoryからID Entranceにユーザ情報が同期され、ID Entrance内のユーザ管理が不要に
- ユーザの追加/削除が発生しても差分同期されるので、ユーザ情報のメンテナンス不要



ユーザ情報管理業務の負荷低減



管理者側の問題点

- 1ユーザーごと、**複数のIDを管理**
- **IDの制御・管理が大変**
- 従業員のパスワード変更依頼が頻発

ユーザー側の問題点

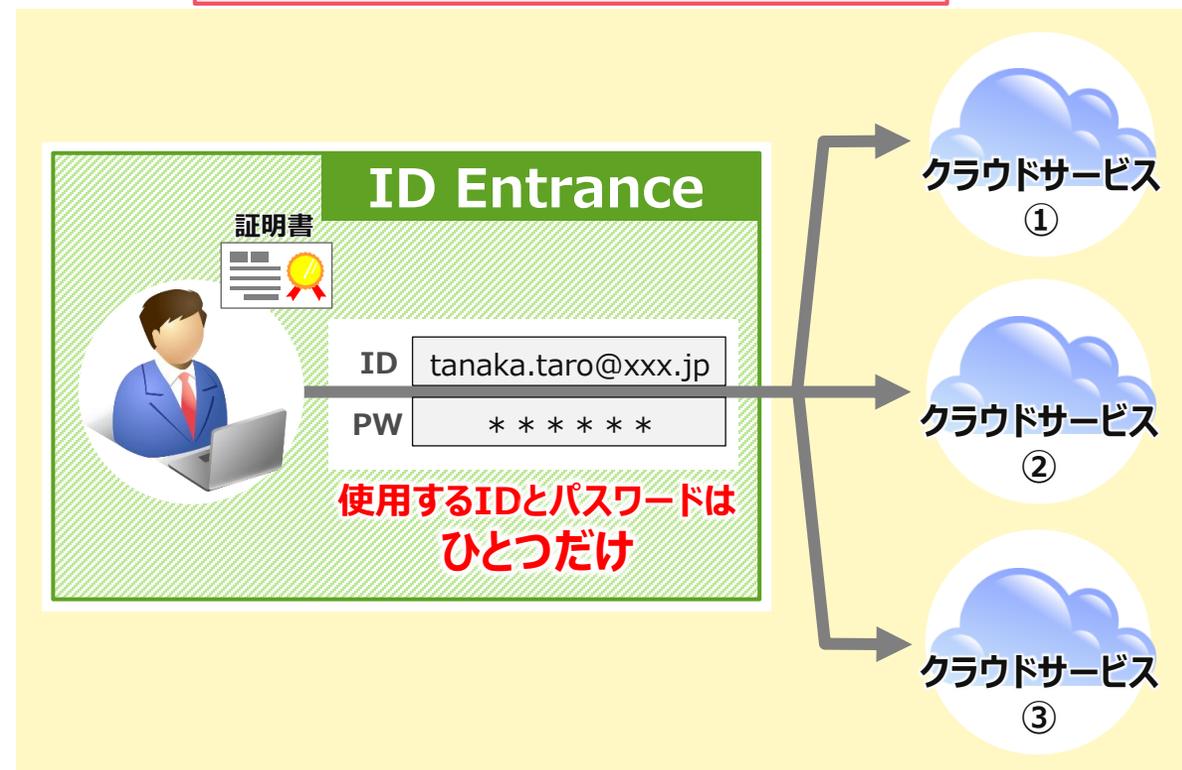
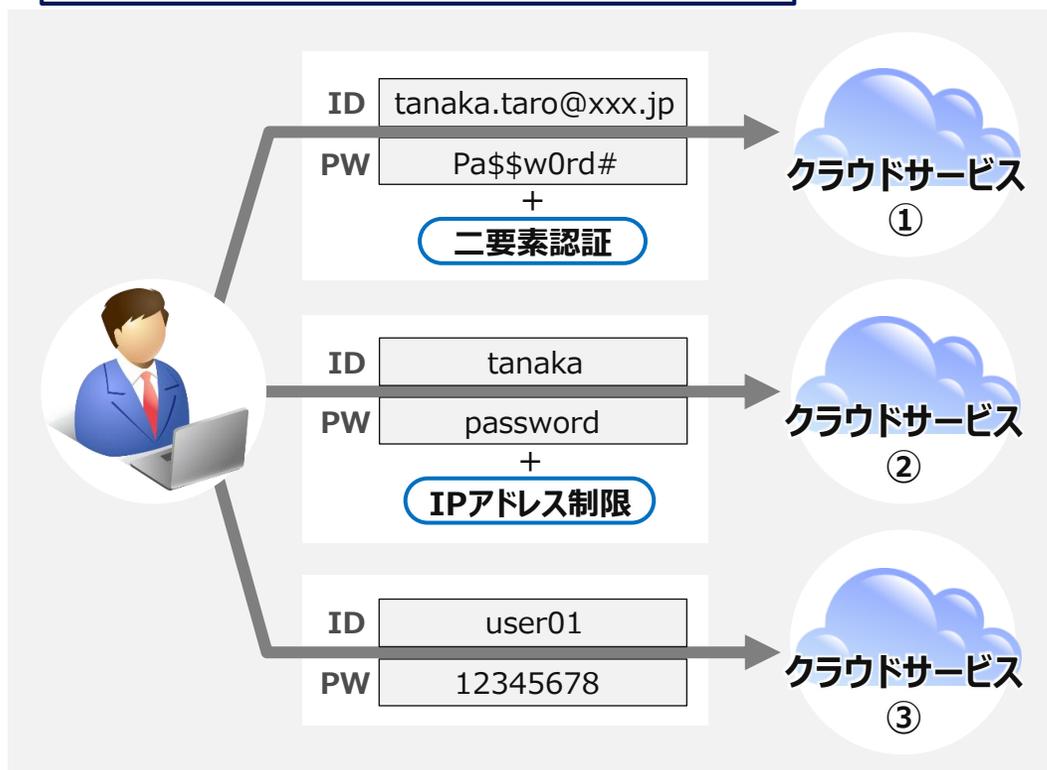
- クラウドサービスごとに異なる、
多数のID/パスワードを覚えられない
- クラウドサービスごとにログインが必要

管理者側のメリット

- 1ユーザー1IDで管理
- アカウント情報を一元管理
- Active Directoryからアカウント情報を同期

ユーザー側のメリット

- 1つのID・パスワードで複数サービスにログイン
- パスワード忘れが減少
- シングルサインオンにより、利便性向上





セキュリティ上の問題点

- 情報資産はクラウドサービスごとに保管され、バラバラにある
- 各ユーザーの**アクセス権が制御できていない**



セキュリティ上のメリット

- **アクセス権を制御し**、不正利用・不正アクセスを未然に防ぐ
- 各ユーザーに**適切な権限付与**

< ヒトで特定する >

ワンタイムパスワード (機能紹介③)



CHECK!

利用者が持っているスマートフォンなどでの認証を追加することで、利用者を特定

※アクセスできる端末自体を限定・制限することはできません

< デバイスで制限する >

クライアント証明書利用 (機能紹介④)



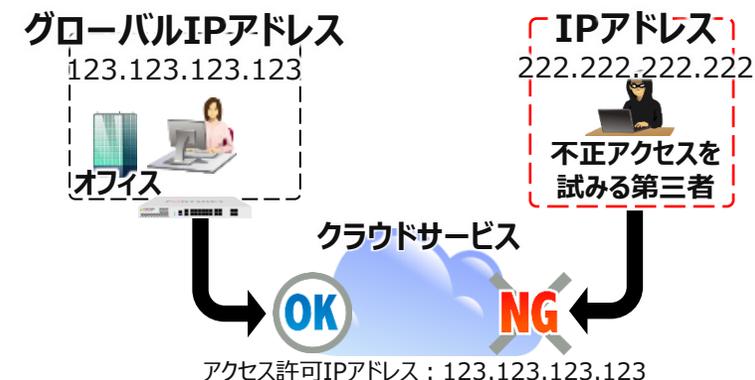
CHECK!

会社が許可している端末からの利用に制限し、プライベート端末からの利用を制限

※端末に電子証明書のインストールが必要

< 場所で制限する >

接続元 IPアドレス制限



CHECK!

オフィスなどの決められた特定の場所からの利用に制限

※固定のグローバルIPアドレスが必要

ID Entranceのデモ



- 以下のクラウドサービスに対応しています。（対応サービスの一部です。詳細はお問い合わせください。）
- 評価環境の発行も受け付けておりますので、ご利用を希望される場合は担当営業までご連絡ください。

キャノンMJ クラウドサービス	グループウェア	ERP/CRM/SFA	経費精算/勤怠管理	ストレージ	タスク管理/情報共有	コミュニケーション	その他
DigitalWork Accelerator 電子取引管理サービス	cybozu.com	楽楽明細 ／楽楽販売	楽楽精算	Box	Sansan	ChatLuck	Google Workspace
GUARDIANWALL Mail セキュリティ・クラウド プレミアム	desknet's NEO	Evernote Teams	勘定奉行クラウド	Dropbox	GEMBA Note Business 6	direct	Datadog
uniFLOW Online	kintone	クライゼル	ジョブカン	DirectCloud	gamba!	Slack	GROWI.cloud
VisualStage Pro powered by Arcules	Microsoft 365	MotionBoard Cloud	HRMOSシリーズ		Kibela		Phrase TMS
VisualStage Type-S/Safie	NI Collabo 360	Salesforce	MAJOR FLOW Z CLOUD		My Redmine		Zabbix
					Qiita Team		セキュリオ

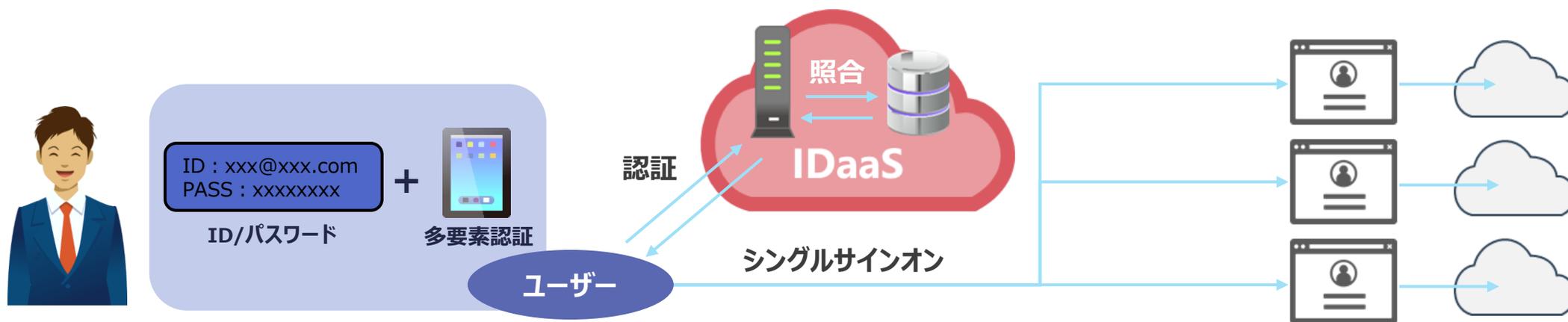


ID Entranceの標準価格表です。
ご利用を希望される場合は担当営業までご連絡ください。

No	製品名	標準価格（年額）	概要
1	ID Entrance 基本ライセンス	1,800円/ユーザー (月額換算:150円)	1ユーザーあたりの年額利用料です。 基本ライセンスをご購入いただくことで、ID Entranceの機能がご利用いただけます。 最低購入数は5ユーザーから5ユーザー単位で購入になります。 利用開始にあたっての初期費用はありません。
2	クライアント証明書 (オプション)	2,400円/デバイス (月額換算:200円)	購入は任意です。 1デバイスあたり1ライセンスの購入が必要になります。 最低購入数は1ライセンスになります。 利用開始にあたっての初期費用はありません。
2	AD連携：ID情報同期機能 (オプション)	1,200円/ユーザー (月額換算:100円)	購入は任意です。 ID Entrance基本ライセンスと同数の購入になります。 最低購入数は5ユーザーから5ユーザー単位で購入になります。 利用開始にあたっての初期費用はありません。



- クラウドサービスの問題点を整理
(管理の煩雑さ・ユーザーの非効率的な業務対応・不正利用不正アクセスのリスク)
- ID Entranceは、**ID管理×セキュリティ対策 + サポートが充実** を提供



クラウドサービス利用時の問題点を正しく理解し、自社内のセキュリティ対策を見直しましょう

Canon

キヤノンマーケティングジャパングループ