

認証プラットフォーム HPE IceWallのご紹介

日本ヒューレット・パッカーード合同会社
Pointnext事業統括 IceWallビジネス推進部



認証基盤 IceWallとは

時代背景とITのニーズの変化に合わせて機能を拡充しています

複数ID・パスワードの統合

シングルサインオン

操作性の向上

PCログオンとの連携

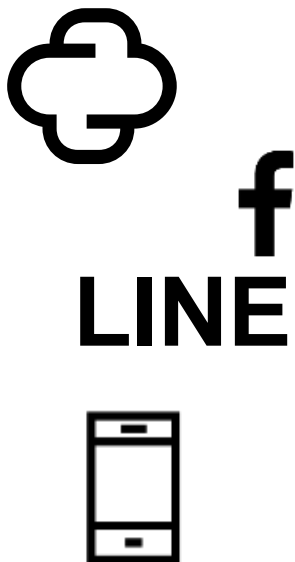
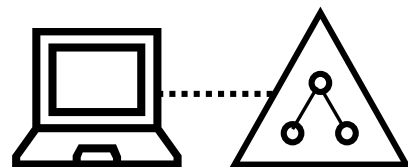
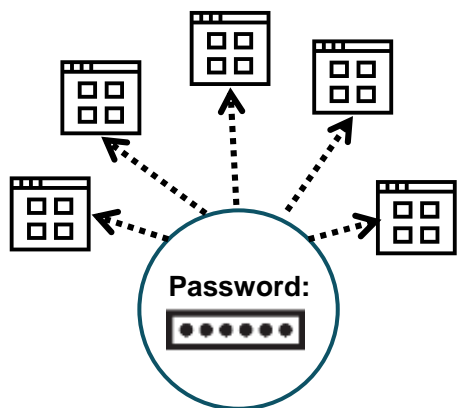
認証レベルの均一化

クラウド・SNS認証連携

パスワード運用の限界
認証強化
働き方の多様性

パスワードレス
多要素認証、生体認証

5G
IoT
ゼロトラスト



Agenda

- IceWall 3つの優位性
- IceWall概要
- 多要素認証基盤IceWall MFA
- クラウド認証連携 IceWall Federation
- 複数認証レポジトリへの対応
- 製品情報リソース



IceWall 3つの優位性

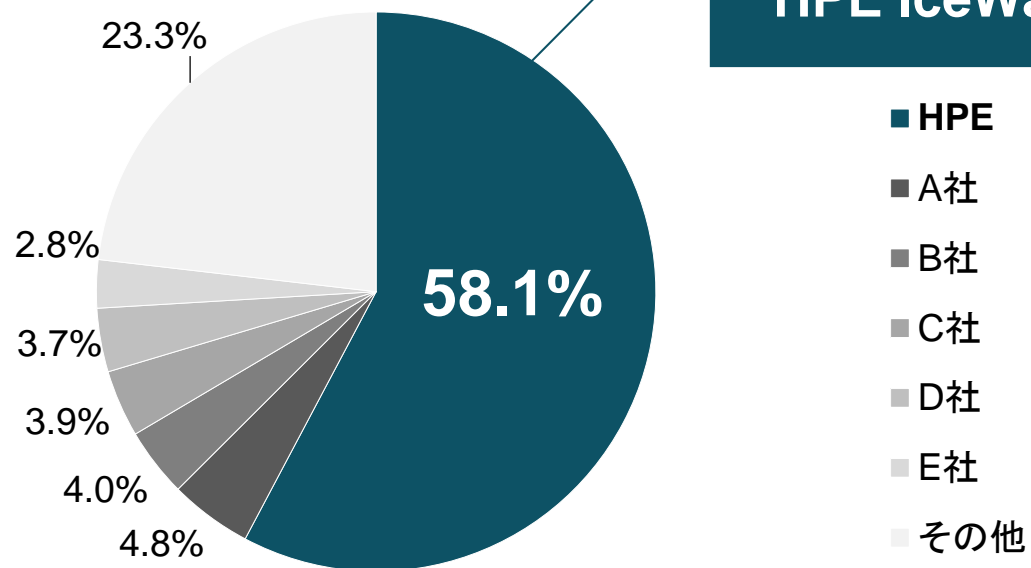


IceWall～圧倒的シェアの理由～

2019年度 国内Web SSO製品シェア*1

累計5,000万ユーザーライセンス
国内で15年以上にわたってトップシェア*2

HPE IceWall



1.豊富な実績に基づく安心と信頼
～数百万規模&ミッションクリティカルの実績～

2.実証済みの高品質と迅速・長期のサポート
～国内開発&国内サポート～

3.高性能・高可用性
～大規模やミッションクリティカルでも安心の仕組み～

*1 出典:デロイトトーマツ ミック経済研究所株式会社

「個人認証・アクセス管理型セキュリティソリューション市場の現状と将来展望 2021年版」(2021年3月刊)を基に日本ヒューレット・パカードが作成。

*2 デロイトトーマツ ミック経済研究所より2005年以降に発行された当該調査レポートに基づく。

1. 豊富な導入実績に基づく安心と信頼

ミッションクリティカル用途や
数百万ユーザー規模の実績多数

BtoC / GtoC システム

お客様名	ユーザー数	備考
第一生命保険	無制限	OIDC RP、オープンAPI連携
三菱UFJ銀行	数百万	インターネットバンキング
金融	数百万	スマホアプリでFIDO2(生体)
証券	10万～	リスクベース
全労済	数十万	マイページ
損保	10万～	OIDC RP、リスクベース
運輸	1千万	OIDC OP、スマホアプリ
NTTドコモ	数百万	

BtoB システム

お客様名	ユーザー数	備考
東京証券取引所	6万	情報提供サービス
三菱UFJインフォメーションテクノロジー	3万	マーケットプレイス
三菱UFJ銀行	数万	インターネットバンキング
NTTデータ	無制限	保険共同ゲートウェイ
日本ユニシス	数千	サポートサイト
損保	10万～	代理店システム、OTP
製造	数千	
通信	数十万	OpenID Connect、SAML
中央省庁	十数万	企業間認証連携

イントラネットシステム

お客様名	ユーザー数	備考
金融	25,000	IceWall MFA
金融	40万	
三菱商事	14,000～	OTP
住友商事	1.3万	
良品計画	5,000	
流通	20,000	ID探索(認証DB分散)
JFEスチール	6万	
伊藤忠テクノソリューションズ [®]	数万	
運輸	6万	
製造	5,000	FIDO2(生体認証)
製造	2万	FIDO2(生体認証)
ソニーネットワークコミュニケーションズ [®]	数千	
通信	6,000	顔認証+統合Windows認証
公共	数万	IceWall MFA(指静脈認証)
ユーティリティ	数万	
公共	60万	
明治大学	40,000	
佐賀県庁	4,000	

(敬称略)、OIDC=OpenID Connect

2. 高品質 & 迅速なサポート

●高いシェアを背景とした圧倒的な高品質

- ✓ 金融などでのミッションクリティカル事例
- ✓ 豊富なハードウェア & 人的リソースを使った徹底的な製品テスト

●100%国内開発で日本のお客様ニーズにフィット

- ✓ 国内のニーズを柔軟・迅速に製品に反映
- ✓ アプリ対応やカスタマイズ等の日本語ドキュメントも充実

●国内サポート

- ✓ 迅速なサポート体制
- ✓ サポートサイトで、パッチ情報などを日本語で配信

●長期サポートによる投資保護

- ✓ IceWall MFA 4.0は 2029年5月末までサポート

●広範囲なモバイル端末の動作確認

- ✓ 動作確認済みブラウザの一覧

<https://www.hpe.com/jp/ja/software/icewall/requirements.html#smartphone>

- [最初にお読みください 1812](#)
(Rev.190925A / 2019-09-27改訂)
(PDF / 421,608Bytes / MD5 = 1cb67e9181de70701f6fd96df1ba4d0c)
- [リリースノート 1812](#)
(Rev.181212A / 2018-12-21改訂)
(PDF / 456,023Bytes / MD5 = 38c602e4802b942cc47df7ea4272cd5b)
- [ライセンスガイド](#)
(Rev.190220A / 2019-04-12改訂)
(PDF / 446,915Bytes / MD5 = a65cab36a4aa496738bdfdf8fc6d2b075)
- [MFA モジュール 導入ガイド](#)
(Rev.170123A)
(PDF / 209,332Bytes / MD5 = 828b4ced5b5cace034c9569cdb4d5e6c)
- [MFA プロキシモジュール 導入ガイド](#)
(Rev.171110A / 2017-11-24改訂)
(PDF / 168,011Bytes / MD5 = d44308197e31dbd044789094f7d827b0)
- [導入ガイド for U2F オプション](#)
U2F オプションの機能は Hello オプションに統合しました。
それに伴いマニュアルの公開を終了しました。
- [導入ガイド for 統合 Windows 認証オプション](#)
(Rev.180927A / 2018-11-16改訂)
(PDF / 434,852Bytes / MD5 = abcf9192bc01caaf7e72ead1e050bf03)
- [MFA モジュール リファレンスマニュアル](#)
(Rev.180927A / 2018-11-16改訂)
(PDF / 974,008Bytes / MD5 = 217616dc16bae76967d1776adb4b3e4a)
- [MFA プロキシモジュール リファレンスマニュアル](#)
(Rev.190409A / 2019-07-05改訂)
(PDF / 1,995,884Bytes / MD5 = 7c638fe9c59b40323819ca9814899e67)
- [Web Application 開発者マニュアル](#)
(Rev.190411A / 2019-07-05改訂)
(PDF / 700,232Bytes / MD5 = f852e9c4316d4ccd36fe84f690d9add6)
- [自動フォーム認証設定マニュアル](#)
(Rev.170121A)
(PDF / 325,266Bytes / MD5 = 2892a51ec5062f08854fae190811bf25)
- [ユーザーズマニュアル](#)
(Rev.190411A / 2019-07-05改訂)
(PDF / 3,484,868Bytes / MD5 = 429b0d3ab53cebfe18ba2f6dd131c0bb)
- [サンプル設定ガイド](#)
(Rev.190109A / 2019-01-25改訂)
(PDF / 570,734Bytes / MD5 = 6e022c1eeaf174a7df6848c4715ea7de)
- [標準 HTML テンプレートカスタマイズガイド](#)
(Rev.180927A / 2018-11-16改訂)
(PDF / 8,631,850Bytes / MD5 = 29de7fc282fbc28da999778f6371e4c5)

サポートサイトで提供している日本語ドキュメントの一部

3. 高性能・高可用性 大規模やミッションクリティカルでも安心のアーキテクチャ

● 高性能: リバースプロキシだけで数百万ユーザー規模の実績

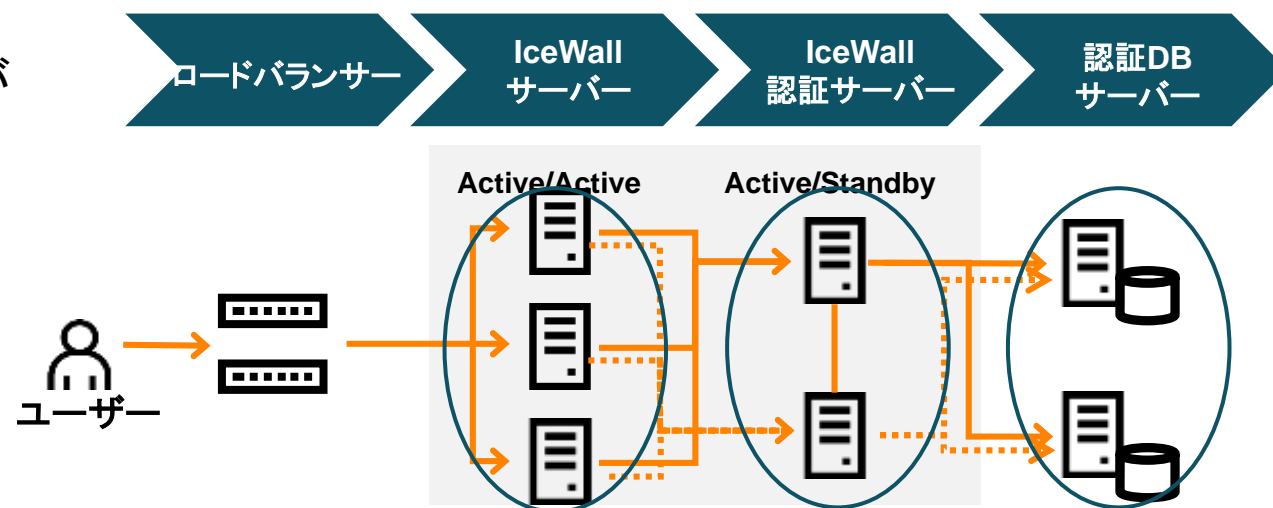
- ✓ 数千ヒット/秒、数百ログイン/秒という高い処理性能
- ✓ 数百万ユーザー規模でアクセスが集中しても、性能は落ちずユーザービリティに影響を与えない

● 高可用性: 全てのモジュールで完全な二重化構成

- ✓ どのモジュールがダウンしてもシステムが止まらないだけでなく、ログインセッションも維持 ~ユーザーは再ログイン不要で、モジュールダウンに気がつかない

リバースプロキシ型SSOは全てのトラフィックが集中し、性能ボトルネックや単一障害点になりがちだが...

IceWall なら心配不要！
多くの事例で実証済みの
高性能・高可用性



IceWall 概要



IceWall MFA と IceWall SSOの違い

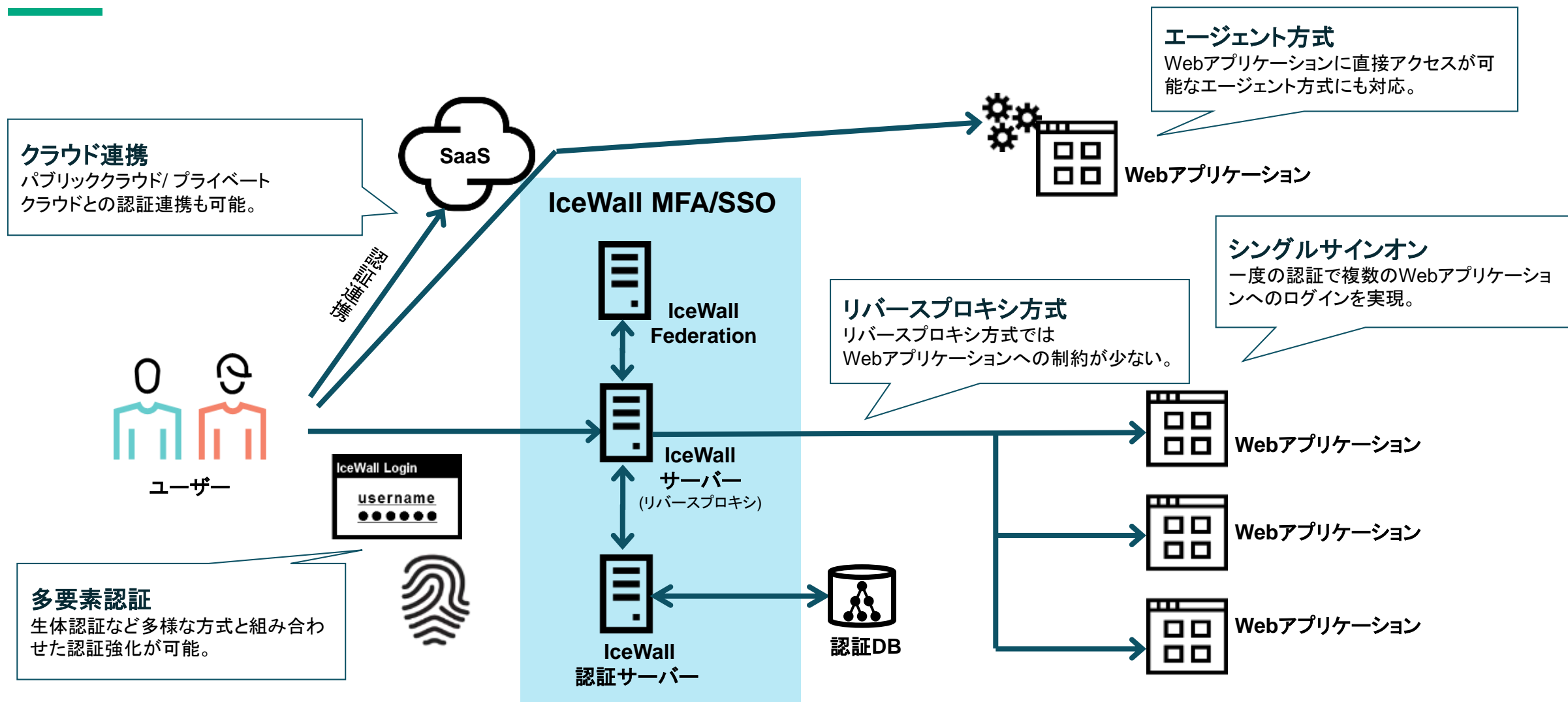
IceWall MFA

- ・最新の多要素認証に対応 (3rd Party製の認証デバイスとの組み合わせも可能)
- ・ポリシーベースの認証設定 (Webアプリ毎の認証方式・再認証・追加認証etc)
- ・高速リバースプロキシ

IceWall SSO

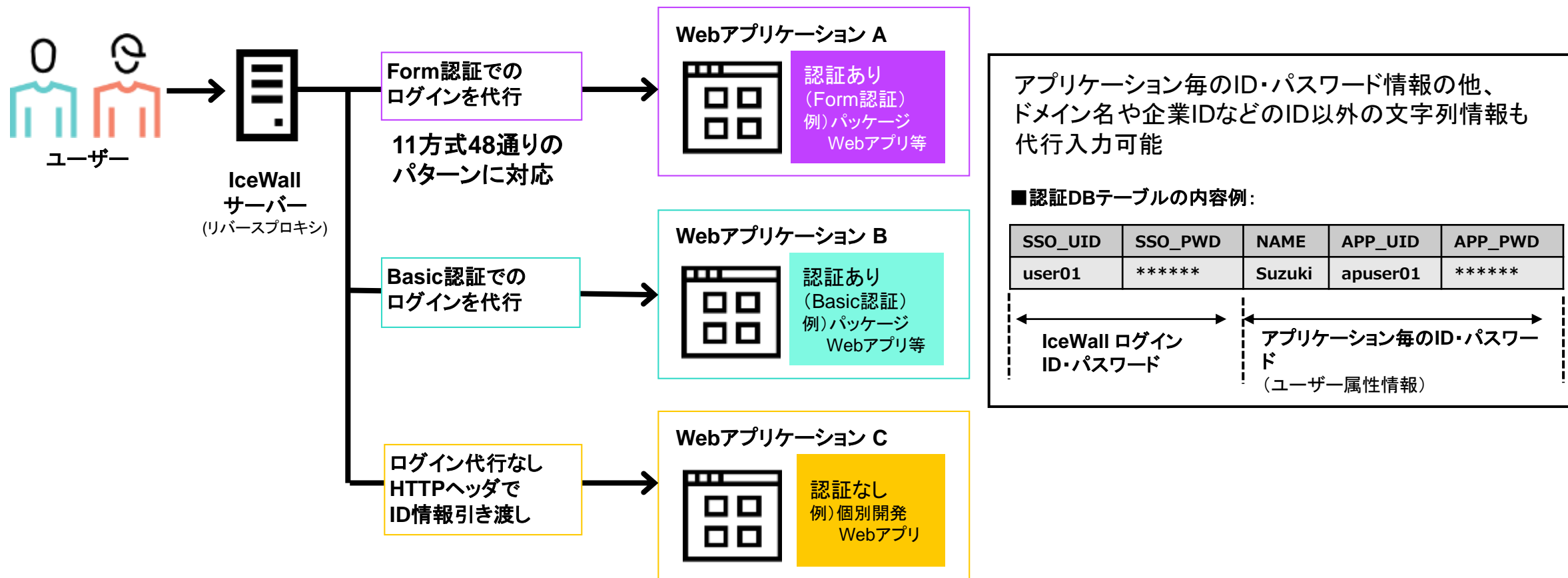
- ・ID/Passwordによる認証
- ・統合Windows認証
- ・従来の多要素認証 (クライアント証明書等)
- ・WebアプリケーションのSSO (リバースプロキシ方式、エージェント方式)
- ・クラウドサービスとの認証連携 (Federation)
- ・ポリシーベースのアクセス制御設定

IceWallの基本機能



幅広いWebアプリケーションへの対応

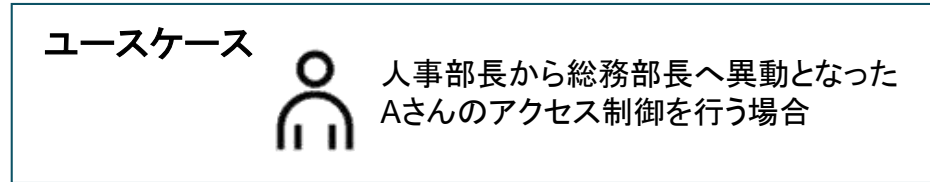
Webアプリケーションへの制限が少なく、
ほとんどの環境に代行入力でSSOが適用可能(カスタマイズレス)※OS・Webサーバ依存がない



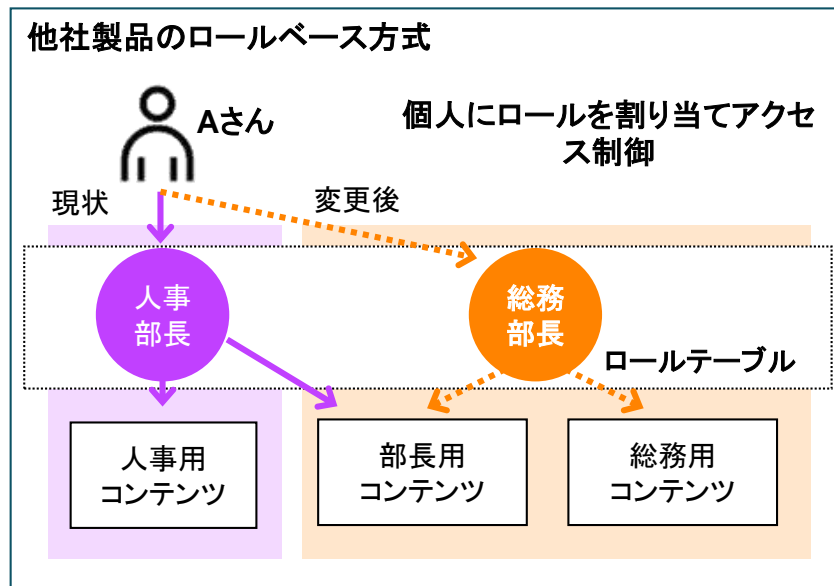
ポリシーベースの効率的なアクセス制御

「ポリシーベース」のアクセス制御により、効率的なアクセス制御が可能

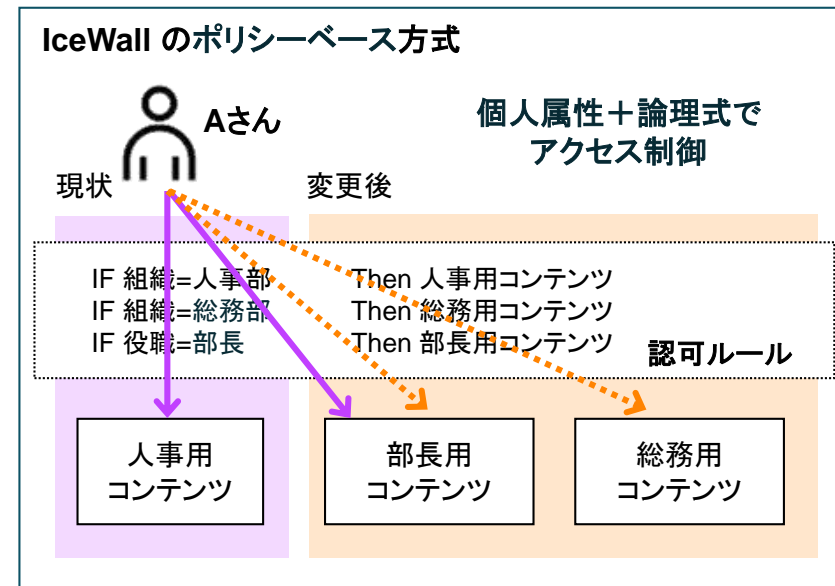
「ロールベース」アクセス制御では、個人の属性変更の都度に権限変更が必要で、運用管理の負担大



△ 個人のロールを新たに割り当てる必要があり、都度、時間と費用がかかる



◎ 個人属性が変われば自動的に変更処理されるため、人事異動の多い企業でも安心!!



多要素認証基盤 IceWall MFA

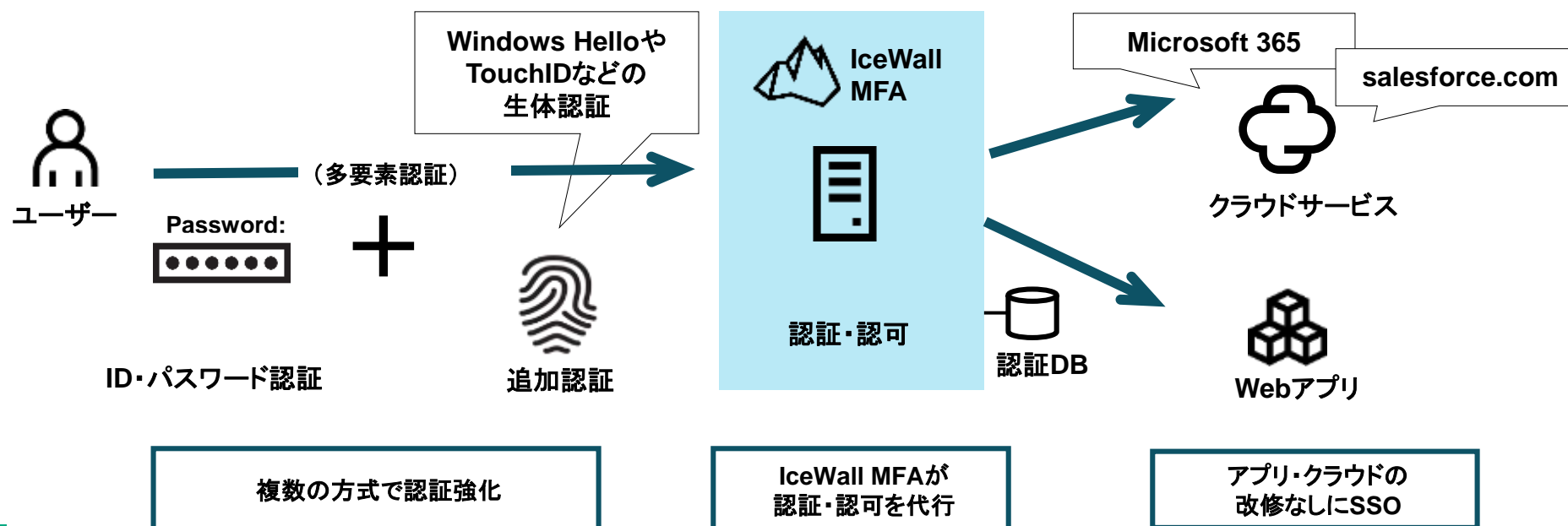


IceWall MFAとは

アプリケーションを改修せずに、多要素認証 (Multi Factor Authentication) で認証を強化

IceWall MFAの特長

標準化された認証方式に対応	FIDO準拠の認証デバイス/OATH準拠のワンタイムパスワード/ブラウザトークン/ 統合Windows認証/その他、認証プラグインモジュールの追加で各種認証方式に対応可能
アプリの改修なしに Webシステムを容易に認証強化	IceWall MFAがWebアプリやクラウドサービスへのログインを代行します。Webアプリやクラウドサービスの改修は不要なので、広い範囲のWebアプリやクラウドサービスを容易に多要素認証化することが可能
各システムの用途に応じて 認証ポリシーを調整可能	各アプリの認証要件に応じて複数の認証方法の組合せを選択可能



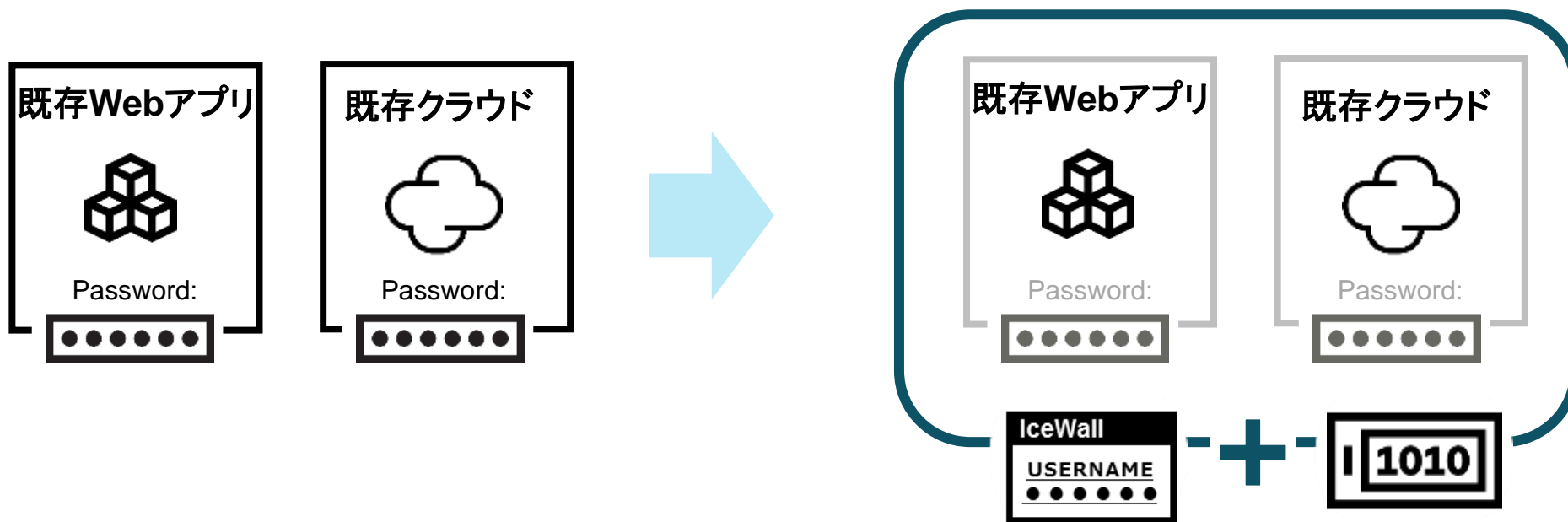
特長: Webアプリ・クラウドサービスの改修不要

IceWall MFAがWebアプリやクラウドサービスへのログインを代行します。
Webアプリやクラウドサービスの改修は不要なので、
広い範囲のWebアプリやクラウドサービスを容易に多要素認証化することができます。

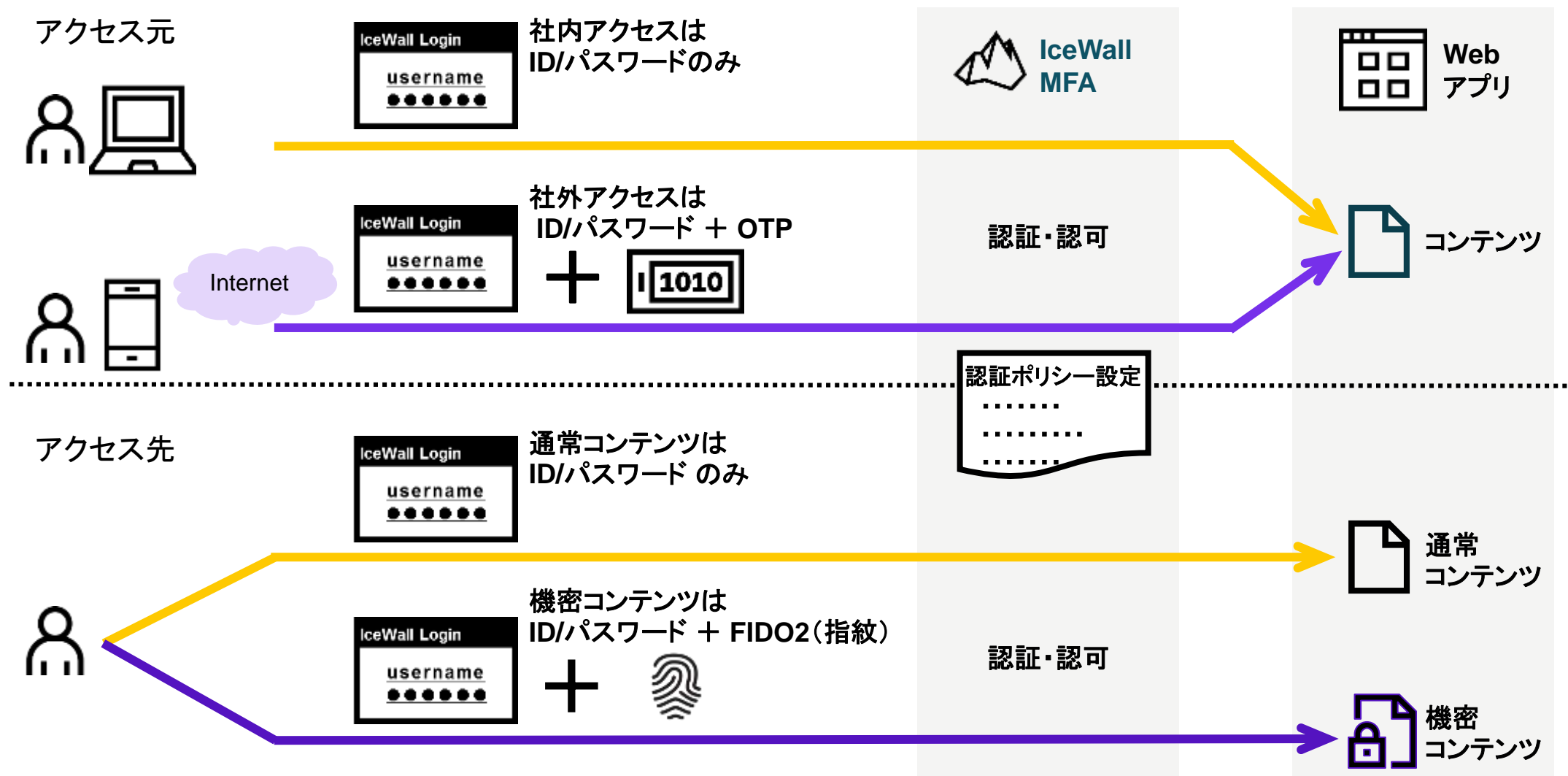
今お使いのWebアプリや
クラウドサービスが...

IceWall MFA
を導入すると

Webアプリやクラウドサービスを
改修することなく
それらの認証をIceWall MFAが代行します

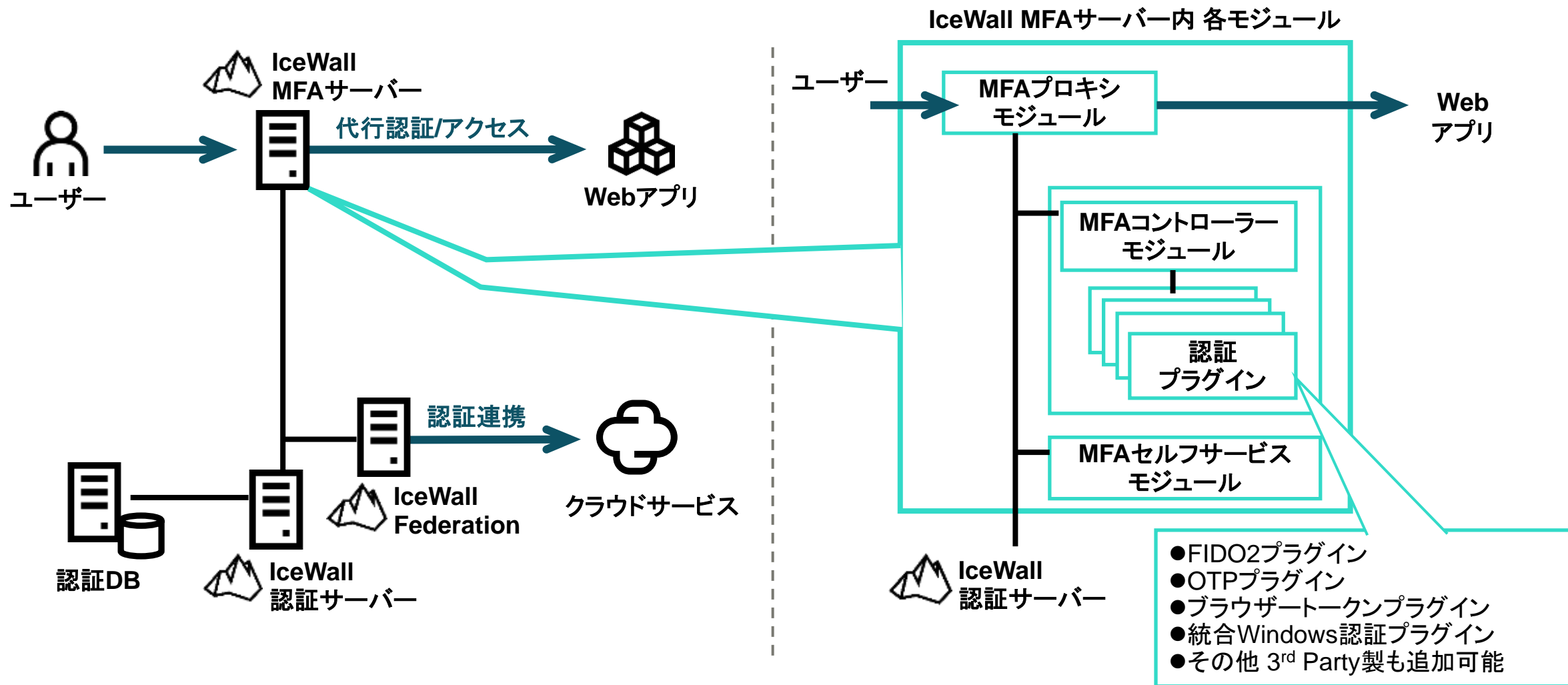


特長: アクセス元やアクセス先に応じて認証方式を決定



システム構成

IceWall MFAのシステムは、各サーバー/モジュールから構成されます。



IceWall MFAが対応する認証方式 (多様な方式に対応)

No	認証方式	IceWall MFA		3rd Party製品/ 外部サービスとの 組合せ
		ID識別認証	追加認証	
1	ID/パスワード	○	○	—
2	統合Windows認証	○	—	Active Directory
3	FIDO2(指紋、顔、セキュリティキー、PIN)	○	○	—
4	OTP(OATH準拠、ソフトウェアトークン)	—	○	—
5	メールOTP	—	○	Mailサーバ
6	SMS OTP	—	○	Twilio
7	クライアント証明書	○	○	MPKI
8	SAML認証(SAML SP)	○	○	IDaaS
9	マトリクス	—	○	PassLogic
10	指静脈	—	○	日立指静脈
11	拡張機能(カスタムプラグイン開発環境)	○	○	—

<セキュリティまたは利便性を高める付加機能>

セレクト
追加認証
再認証
ブラウザトークン

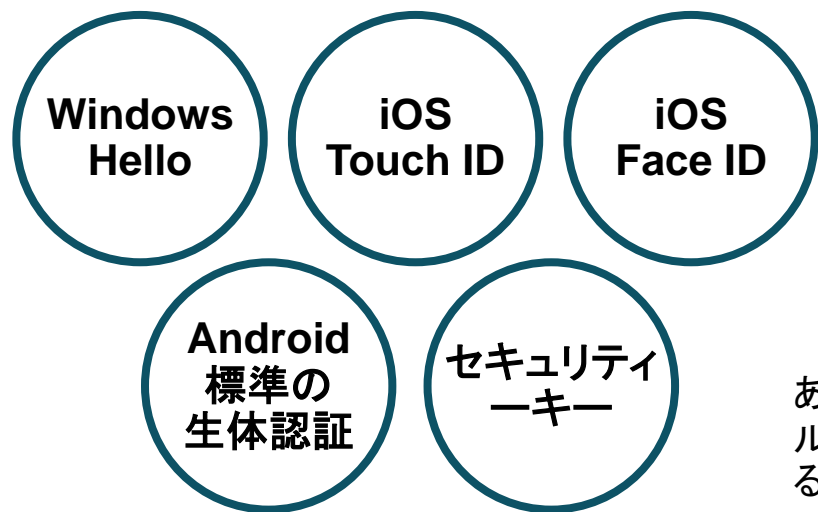
認証方式の選択メニュー
認証レベル状態やユーザ属性に応じた認証
認証済み状態での特定URLアクセス時
追加認証済み端末の登録と一定期間スキップ

ID識別認証：1段目又は2段目以降の認証に利用可能。
追加認証：2段目以降の認証に利用可能。

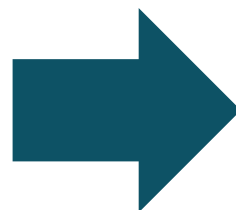
IceWall MFA FIDO2オプションとは

標準規格である「FIDO2」および「W3C Web Authentication」に対応した仕様を採用し、各種デバイス標準の生体認証と連携して、パスワードレス認証や多要素認証を実現。SaaSを含む幅広いアプリケーションの認証を強化します。

マルチデバイスで



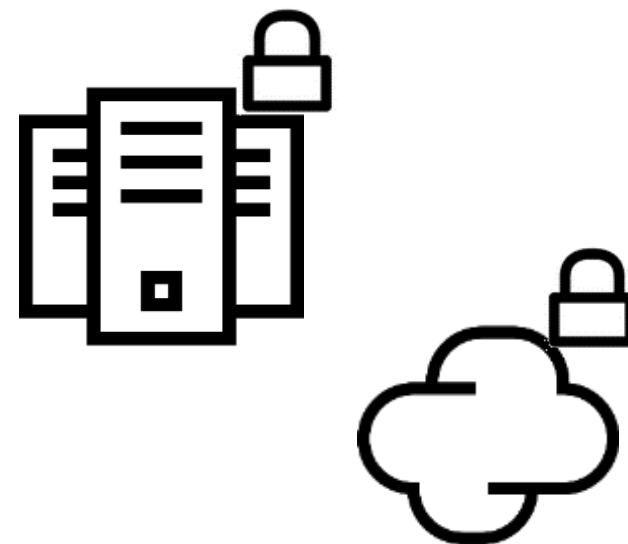
生体認証



多要素認証

あらかじめ暗号化されたキーがインストールされた端末からのアクセスのみ認証することで、ユーザーの利用端末を限定

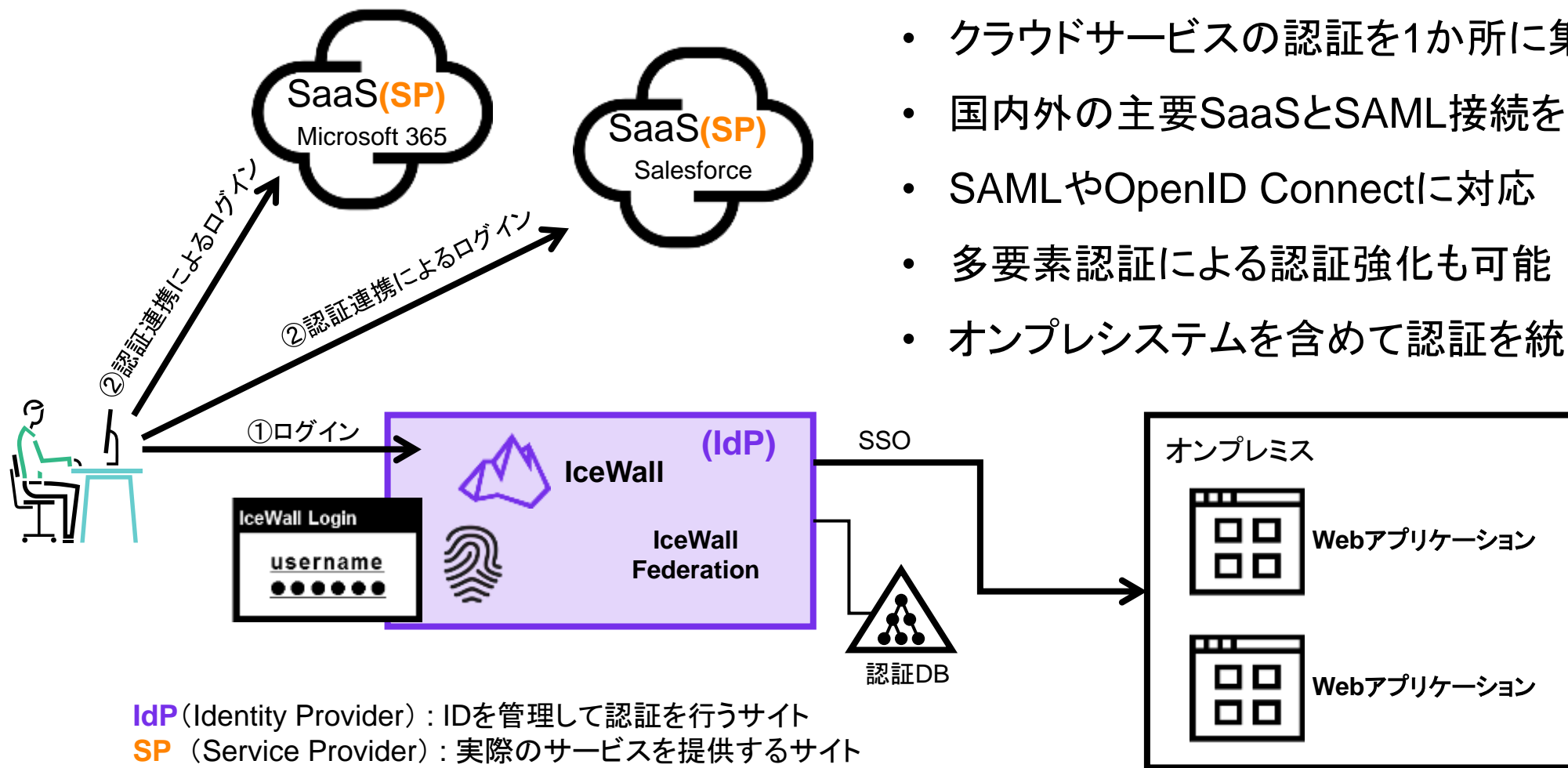
WebアプリケーションやSaaSへ



クラウド認証連携 IceWall Federation



IceWall Federation ~SaaSとのSSO~



- クラウドサービスの認証を1か所に集約
- 国内外の主要SaaSとSAML接続を検証済み
- SAMLやOpenID Connectに対応
- 多要素認証による認証強化も可能
- オンプレシステムを含めて認証を統合

IdP (Identity Provider) : IDを管理して認証を行うサイト
SP (Service Provider) : 実際のサービスを提供するサイト

各サービス/ソフトウェアとの認証連携を検証済み

- IceWall Federationは**実際の各サービスとの相互接続検証を行っており**、安心・迅速な導入が可能
- フェデレーション機能を提供する製品の多くは、SAML等の「標準仕様に準拠」を確認していても、各サービスとの相互接続確認/検証はユーザー任せ、という製品も少なくない
- **国内**のサービス/ソフトウェアも実績多数

一般的なフェデレーション機能提供製品

導入時: 特定の対象サービス(SP)のインターフェースに合わせて、SAML等、適用する標準仕様の詳細を理解し、自身で設定・接続検証をする必要あり

運用時: 万が一、本番運用において障害が発生した場合、個々の標準仕様におけるエラーは自身で解析してから各社製品窓口に問い合わせる必要あり



IceWall Federation

導入時: 適切な標準仕様を用い日本ヒューレット・パカードにて各サービス(SP)単位での接続検証をしているため、安心かつ迅速にサービス導入が可能

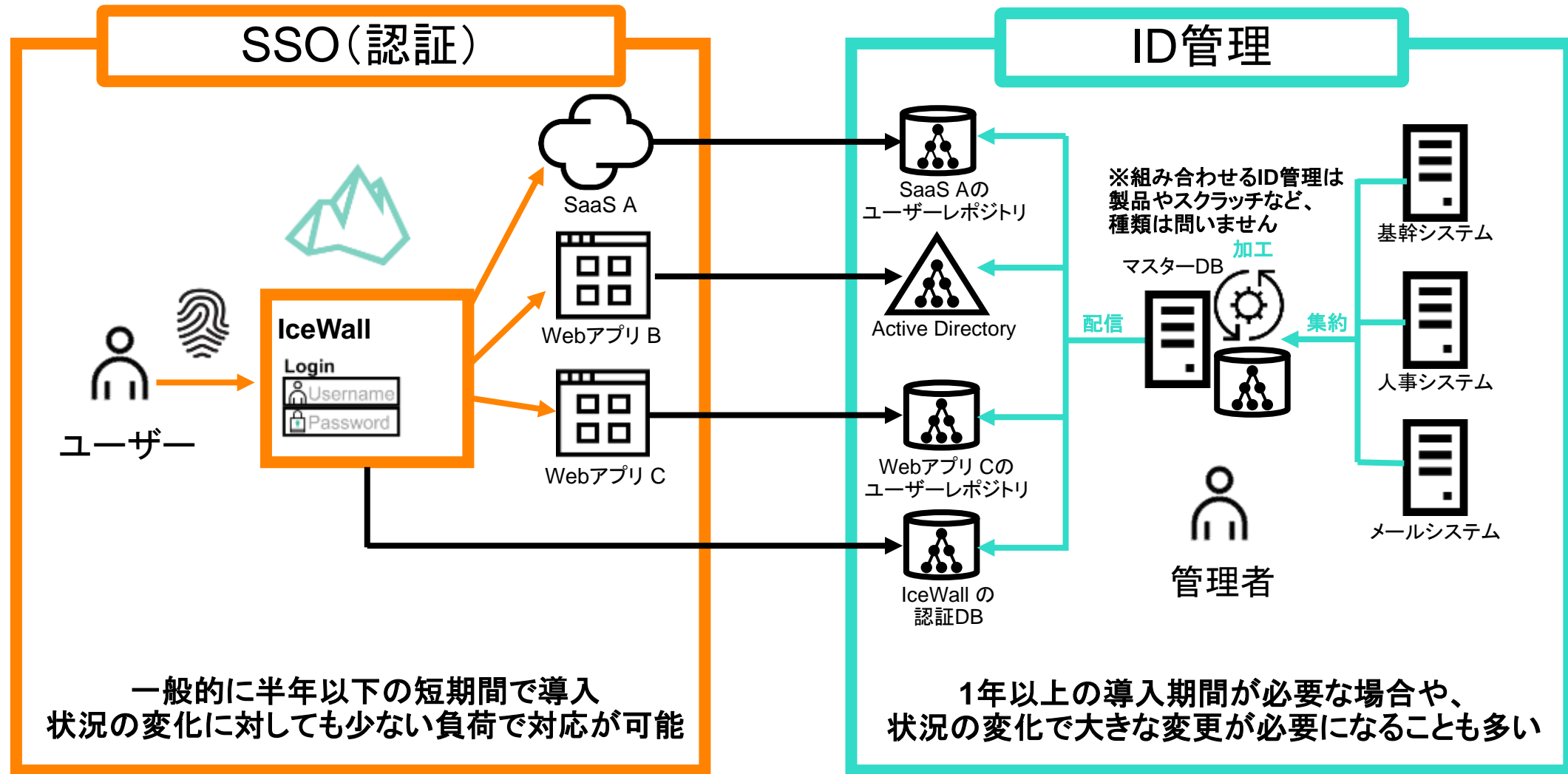
運用時: 接続検証された対象サービス(SP)との接続において障害が発生した場合、日本ヒューレット・パカードから問題解決のためのサポートを受けることができる

現在までにSPとして接続が確認できているサービス/ソフトウェア 例

- | | | | | | |
|-----------------------|-------------------|------------------------|-----------------|--------------------------|---|
| ✓ G Suite | ✓ 福利厚生倶楽部 | ✓ SharePoint | ✓ 出張なび | ✓ Confluence (RickCloud) | ✓ Adobe Creative Cloudエンタープライズ版、Adobe Document Cloudエンタープライズ版 |
| ✓ Salesforce Platform | ✓ Box | ✓ ADFS 2.0 | ✓ Bulas | ✓ Sansan | ✓ Phone Appli People (旧連絡とれるくん) |
| ✓ Microsoft 365 | ✓ SECURE DELIVER | ✓ cybozu.com | ✓ e-革新サービス | ✓ intra-mart | ✓ Citrix Virtual Apps and Desktops (旧XenDesktop) |
| ✓ LINE WORKS | ✓ GigaCC | ✓ KDDI | ✓ ShibbolethのSP | ✓ WebEx | ✓ VMware Horizon (VMware Identity Manager) |
| ✓ クリプト便 | ✓ Aruba ClearPass | KnowledgeSuite (GRIDY) | ✓ Windows Azure | ✓ 楽々精算 | 他、多数 |
| ✓ Fileforce | ✓ SharePoint | | ✓ GoodData | | |

接続確認ができていないサービスの最新状況は[弊社Webページ](#)をご確認ください

統合認証基盤に必要な要素・・・「SSO」と「ID管理」



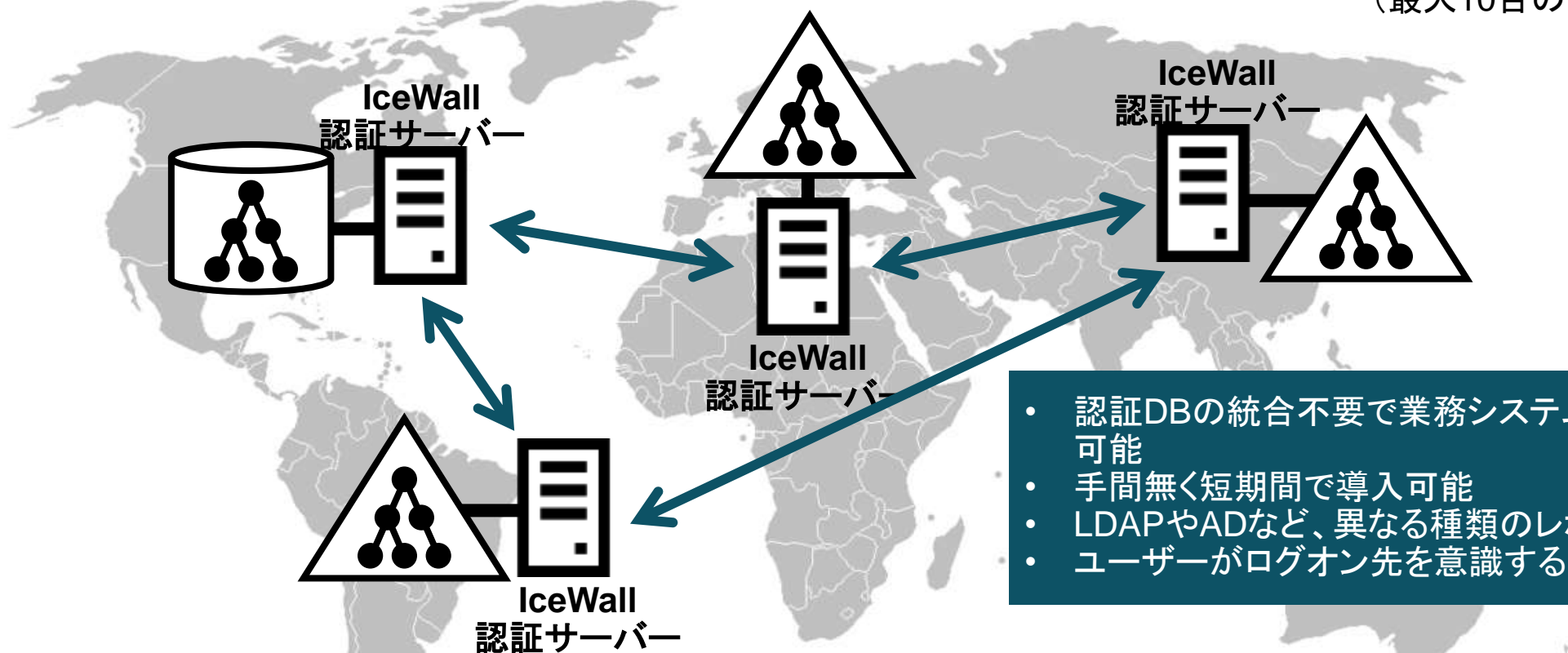
複数認証レポジトリへの対応



ID探索機能

- ADなどの認証DBが、独立して複数に分散している場合の課題を解決
- IceWall認証サーバー同士が通信し、複数の認証DBの中からID情報を探索し、どの認証DBのユーザーもSSOを利用可能

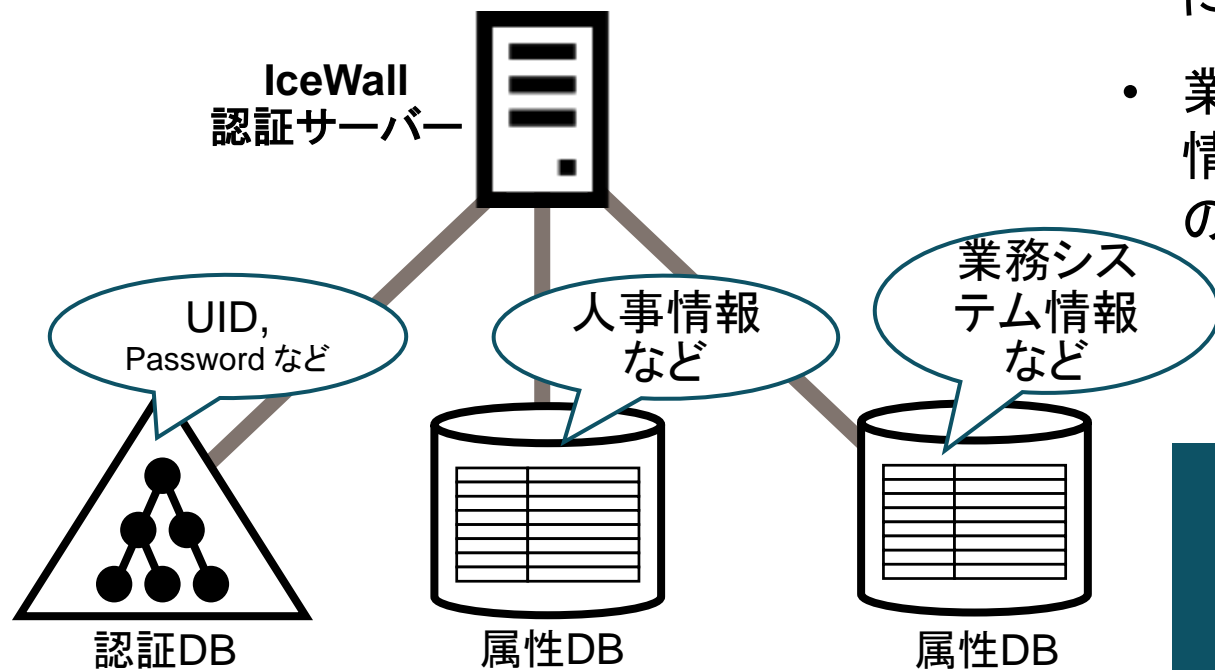
(最大10台のIceWall認証サーバー)



- 認証DBの統合不要で業務システムをグローバルに公開可能
- 手間無く短期間で導入可能
- LDAPやADなど、異なる種類のレポジトリでも対応可能
- ユーザーがログオン先を意識する必要なし

※サードパーティ認証製品と組み合わせる場合は、本機能が使えないケースがあります。

属性統合機能



(接続可能なDBは5セットまで)

- ID情報だけでなくユーザーの属性情報も複数のDBに分散している場合もある
- 業務システムが、複数の属性DBにまたがった属性情報を取得したい場合、DBの統合や、業務システムの改修が求められてしまう

属性統合機能を使えば、
IceWall認証サーバーが
複数の属性DBの情報を収集
より柔軟に属性情報の利用が可能

※サードパーティ認証製品と組み合わせる場合は、本機能が使えないケースがあります。

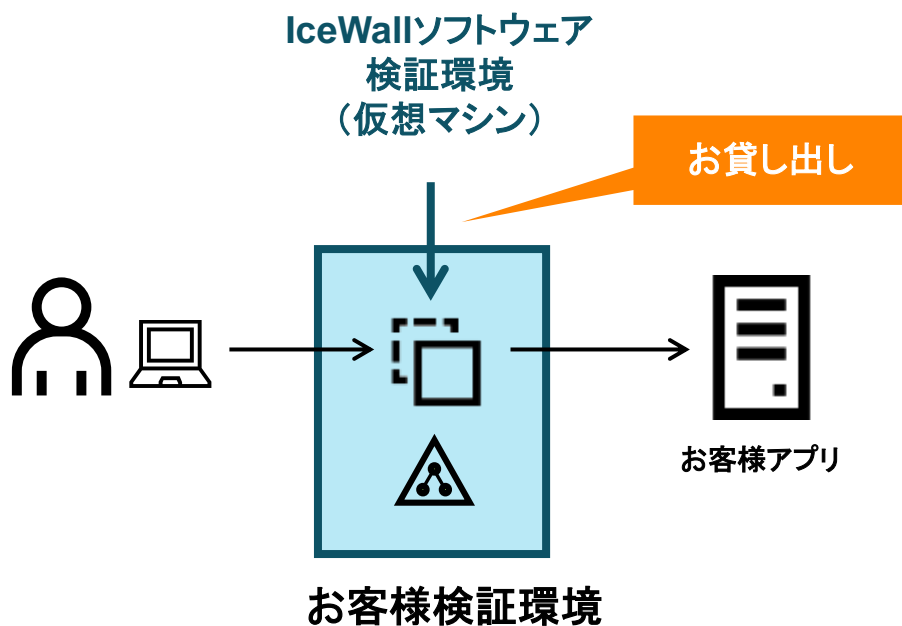
製品情報リソース



IceWallソフトウェア 検証環境 評価キットのご紹介

評価キット概要

標準的な構成のIceWallソフトウェアが導入されたVMware仮想マシンを、検証用としてディスクイメージファイルでお貸し出しいたします。仮想マシンをお客様の検証環境で稼働いただくことにより、実際のアプリケーションとIceWallソフトウェアを組み合わせた動作や操作方法、運用イメージの確認を、リアルな環境で実施いただけます。



お客様のメリット

- ✓ 仮想マシンを稼働させるだけで検証開始
- ✓ お客様環境で実際のアプリケーションを使用した動作確認が可能
- ✓ 運用イメージや、動作イメージを事前に把握し、本番導入後のスムーズな展開が可能

評価キット内容

以下よりご選択ください。

- ✓ 評価版の形態(複数可。製品マニュアルはどちらにも含まれています)
 - VMWare版 ~ IceWall製品がインストール済みのVMware仮想マシンイメージが含まれており、VMware Playerで実行可。*1)
 - 製品版(インストール版) ~ インストール作業が必要。
- ✓ 提供方法(いずれかを選択)
 - ダウンロード
 - メディアの送付

*1 VMware版は、VMware Workstation Player 12.0.以降(Windows版)用の仮想マシンイメージとなっております。ESXServer等でご利用いただく際は、VMware vCenter Converter等でコンバートいただく必要があります。

前提条件

- ✓ 原則として、メディアのお貸し出しは1か月間以内、検証期間は3か月間以内となります。
- ✓ 検証環境はお客様にてご用意いただきます。
- ✓ お客様の検証環境で稼働させるために必要な設定等については、お客様にて実施いただくことを想定しております。
- ✓ 事前にご利用目的を確認させていただきます。場合によってはご希望に添えない事がございますのであらかじめご了承ください。お貸し出しには所定の申請書への記入・捺印をお願い致します。

IceWallソフトウェア 検証環境 評価キットのご案内

含まれるソフトウェア

- IceWall MFA 4.0(メールOTPオプション、FIDO2オプション)
- HPE IceWall アプリ(IE用ActiveX)
- IceWall Gen11 認証モジュール
- IceWall Gen11 Dynamic Menu Portal
- IceWall Gen11 Agent Option
- IceWall SSO 11.0 フォワーダ
- IceWall Identity Manager 6.0
- IceWall MCRP 4.0
- IceWall Federation 4.0 SAML IdP
- IceWall Federation Agent 4.0
- IceWall Gen11 Password Reset Option
- OpenLDAP 2.4(OSにバンドル)
- IceWall Management Suite 6.0
(Setup Manager、Console for SSO、
Console for MFA、Console for Federation)

ご利用を希望の場合はお問い合わせください

ポータル画面イメージ



IceWall Dynamic Menu Portal
(リバースプロキシ方式)

エンドユーザ向けIceWall管理機能
(リバースプロキシ方式)

サンプルバックエンドサーバ
(リバースプロキシ方式)

サンプルCGI
(認証連携方式)

サンプルサイト
(エージェント方式)

IceWall Identity Manager
IceWall パスワードリセットオプション
(リバースプロキシ方式)

IceWall MFA
1) FIDO2パスワードレス認証
2) パスワード+メールOTP または
FIDO2追加認証

多要素認証機能



IceWall MFAトレーニング

多要素認証基盤「IceWall MFA」を実機での演習を交えて学習できるハンズオントレーニングを開催しております。

IceWall MFAトレーニングコース(1日)

コースコード: H0AC7S
価格: 70,000円(税抜き)
日数: 1日(10:00~18:00)

開催地: 日本ヒューレット・パカード本社(東京都江東区)
またはライブオンライン

※各回の開催地についてはお申し込みURLにてご確認ください

コースの目的

- ✓ IceWall MFAの機能を理解する。
- ✓ IceWall MFAの基本的な設定方法について理解する。
- ✓ IceWall MFAを使ったWebアプリケーションやクラウド利用の多要素認証化について理解する。

対象者

IceWall MFAの導入を予定されていて、機能や設定方法を習得したいお客様。

前提知識

基礎的なLinuxの知識とコマンド操作経験、およびWebに関する基礎知識が必要です。

コース内容

- IceWall MFAの概要
 - 機能、システム構成
 - リバースプロキシによるシングルサインオン
- 基本機能設定
 - 認証、認可、アクセスコントロール設定
- 多要素認証
 - FIDO対応機器を使用した生体認証
 - ワンタイムパスワード
 - 複数の認証方式の制御
- 自動フォーム認証
 - HTMLフォーム認証への対応
 - Basic認証への対応
- 冗長化
 - 冗長化構成の設定
- その他の機能
 - クラウドとの認証連携(フェデレーション)
 - 統合Windows認証との連携
 - エージェント構成でのシングルサインオン
 - URL変換機能

コーススケジュールとお申し込み: www.hpe.com/jp/iw-training

お問い合わせおよび周辺サービス

お電話でのお問い合わせ(日本ヒューレット・パカード カスタマー・インフォメーションセンター)

0120-268-186 / 03-6743-6370 (スマートフォン・携帯電話から)

受付時間：月曜日～金曜日 9:00-19:00

(土、日、祝祭日、年末年始および5月1日を除く)

Webフォームからのお問い合わせ www.hpe.com/jp/iw-contact

最新/詳細情報

- HPE IceWall 公式サイト
www.hpe.com/jp/icewall
- お客様事例
www.hpe.com/jp/iw-casestudy
- 技術レポート(新規レポート随時公開中)
www.hpe.com/jp/iw-report
- カタログ
www.hpe.com/jp/iw-catalog
- IceWallトレーニングコース
www.hpe.com/jp/iw-training

各種サービス

- 導入サービス
- コンサルティングサービス
- エンジニア様向け技術トレーニング
- 海外拠点への導入・コンサルティングサービス

THANK YOU

