

写真による偽造対策が可能な軽快顔認証

一般的なPC内蔵カメラやウェブカメラを利用しつつ、DDSの顔認証エンジンにより、紙に印刷した顔やタブレット端末などディスプレイに表示した顔（写真や動画）を検知して、偽造による認証を防止します。

- ※ 偽造検知機能は、写真やディスプレイなど平面に映し出された顔を検知します。マスク着用時は本機能は利用できませんので、偽造検知機能を利用する場合は、マスクを外して利用ください。
- ※ 偽造を完全に防ぐものではありません。また、照明条件などによっては、本物を偽物と誤認することもありますので、事前に検証することをお勧めします。



クラウドビジネス部にて認証取得



クラウド認証プラットフォーム「EVECLOUD」のサービス提供と本サービス提供に係るAWSの利用において認証取得



IDentity As A Service

EVECLOUD クラウド認証サービス

●システム要件●

クライアントアプリケーション（Windowsログオン、IDマネージャー）

OS	ブラウザ
Windows 11（x64）	Edge 99以降、Chrome 98以降

WEBアプリケーション（SAML、管理ツール、ポータル）

OS	ブラウザ
Windows 10 / 11（x32/x64）	Edge 99以降、Chrome 98以降
macOS 11以降（x64/Apple silicon）	Safari 14以降、Chrome 98以降、Edge 99以降
ChromeOS 116以降	Chrome 98以降
iOS 14以降 iPadOS 16以降	Safari 15.3.1以降、Chrome 98以降
Android 12以降	Androidブラウザ、Chrome 98以降

●サービス内容

※動作環境の詳細は、別途お問合せください。

機能		バック内容
シングルサインオン	フェデレーション方式（SAML2.0）	○
	代行入力方式（IDマネージャー）	IDマネージャー オプション※2
OSログオン	Windows OS ログオン	Windows OSログオン認証 オプション※3
	ChromeOS ログイン	○
多要素認証（生体認証）	顔認証（サーバー認証）	○
	指紋認証（サーバー認証）	オプション※4
	FIDO2認証（WebAuthn/パスキー）	○
多要素認証（所持認証）	ワンタイムパスワード認証（TOTP）	○
	ICカード認証	オプション※5
	QRコード認証	○
多要素認証（知識認証）	パスワード認証	○
	PIN認証	○
	一時パスワード認証	○
その他の認証	メール認証	○
	デバイス認証（クライアント証明書/IPアドレス制限）	○
	リスクベース認証	○
	アウトオブバウンド認証	○
	代理認証	○
ユーザー情報管理	Active Directory連携	○
	Microsoft Entra ID連携	○
	CSV	○

※1 最小利用 ID 数は 30 ID、価格は ID / 月額 で、契約単位は 1 年間です。オプションは別途お問い合わせください。
※2 SAML非対応のアプリケーション（レガシーアプリ、Windowsアプリ、Webアプリ 等）への 多要素認証（FIDO認証除く）が利用いただけます。
※3 Windowsログオン時の認証に標準機能で備わる多要素認証（FIDO認証除く）が利用いただけます。
※4 DDS製指紋認証ユニットUBF-Touchシリーズでの使用に限ります。
※5 IC カードとカードリーダーの規格は以下の通りです。
・ICカード：FeliCa、MIFARE Standard 1K / MIFARE Standard 4K / MIFARE Ultralight
・カードリーダー：ソニー株式会社製カードリーダー PaSoRi (RC-S300/S、RC-S300/S1、RC-S380/S)
※6 サポートはメールでの対応となります。詳細は弊社ウェブサイトを参照ください。

※記載の内容は2026年3月現在のものです。記載内容は、予告なく変更する場合があります。
※EVECLOUDは株式会社ディー・ディー・エスの登録商標です。QRコードは株式会社デンソーウェーブの登録商標です。その他 記載の社名およびロゴ、製品名は、各社の商標または登録商標です。

株式会社ディー・ディー・エス www.dds.co.jp/ja/

本社：〒108-0075
東京都新宿区西新宿6-12-1 パークウエストビル 8F
TEL：03-6821-1630（代表） FAX：03-5321-5566
名古屋支社：〒450-0002
愛知県名古屋市中村区名駅3-9-6 アルティメイト名駅2nd 8F
TEL：052-955-6600（代表） FAX：052-583-7800

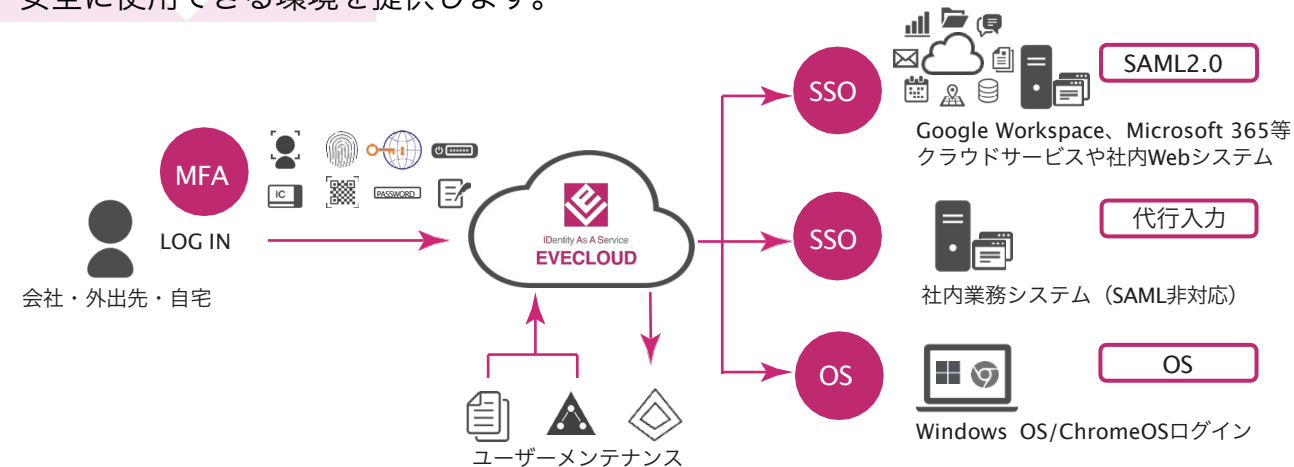


ID管理とクラウドサービス利用時の認証強化、シングルサインオンによる利便性を実現するクラウド認証サービス

ID管理とクラウドサービスへのシングルサインオン による利便性を実現するクラウド認証サービス

EVECLOUDの特徴

EVECLOUDは、ID管理とクラウドサービス利用時の認証強化、およびシングルサインオンによる利便性を実現するクラウド認証サービスです。シングルサインオン（SSO）機能により、業務で利用するGoogle WorkspaceやMicrosoft 365などのサービスを、クラウド上で安全に使用できる環境を提供します。

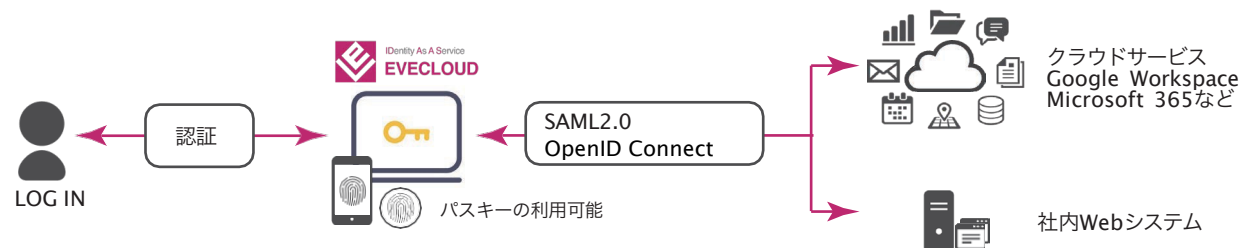


シングルサインオン（SSO）

クライアント証明書や顔認証による多要素認証（MFA）とフェデレーション方式のシングルサインオン（SSO）に加え、Windowsログオンやレガシーアプリ、Windowsアプリ、Webアプリへの代行入力方式のシングルサインオンに対応します。

◆ フェデレーション方式

EVECLOUDがIdentity Provider（IdP）となり、フェデレーション（SAML2.0）による連携が可能なウェブサービス（Service Provider（SP））に対して、ID連携による認証を提供します。さまざまなクラウドサービスやウェブシステム、SAML2.0に対応していればオンプレミスのアプリケーションに対してもSSOが行えます。
※次期バージョンでは OpenID Connect に対応予定



◆ 代行入力方式

SAML2.0 に対応していない業務アプリやWebアプリに対しては、EVECLOUDのIDマネージャーを利用し代行入力方式（ログイン情報を代行で入力する方式）でシングルサインオンが利用いただけます。

緊急時でも安心

◆ 一時パスワード認証

パスワードはEVECLOUD管理ツールで発行され、有効期限内であれば何度でも利用できる8桁のパスワードで認証が可能です。有効期限は最小で1日、最大で185日の設定が可能です。

◆ アカウントリカバリ機能

パスワードを忘れた、またはアカウントロックしたユーザーが自身で復旧できるようにする機能です。あらかじめ登録したメールアドレスに送信されたメールのURLをクリックすることで、パスワードを発行します。

多要素認証で本人認証強化

「顔認証」「指紋認証」「FIDO認証（WebAuthn）」「ワンタイムパスワード認証」「ICカード認証」「QRコード認証」「パスワード認証」「デバイス認証」などから自由に選択ができます。他にも「デバイス認証」「リスクベース認証」「メール認証」などもあり、利用するシーンや職務の権限に沿って本人確認を強化することができます。今後も認証方式を追加してご提供します。



◆ FIDO2（WebAuthn/パスキー）に対応

端末内蔵の認証器（顔、指紋）やセキュリティキーを使用したFIDO2（WebAuthn/パスキー）に対応しています。

◆ デバイス認証

端末にインストールする電子証明書（クライアント証明書）または許可した「IPアドレス」を用いた認証方法です。証明書がインストールされた端末でなければ認証できないため、不正なアクセスを防止することができます。

ユーザー情報管理（ID連携）

◆ Active Directory 連携によるメンテナンス

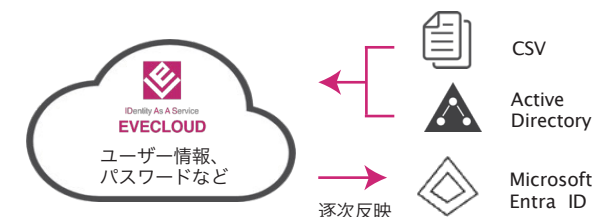
Active Directoryと連携を行い、ユーザー情報（ユーザーID、パスワード）を同期する機能です。EVECLOUDへユーザーを追加したり、退職時に削除させたりする手間を省略できます。

◆ Entra ID 連携によるメンテナンス

EVECLOUDユーザーの同期先のドメインとグループを設定することで、EVECLOUDグループ1つに対し、Entra IDのドメインと複数グループを紐づけることができます。EVECLOUDユーザー追加時のEntra IDアカウントの新規作成、更新時のEntra IDアカウントのプロパティ更新のほか、パスワード変更も可能です。

◆ CSVファイルによるメンテナンス

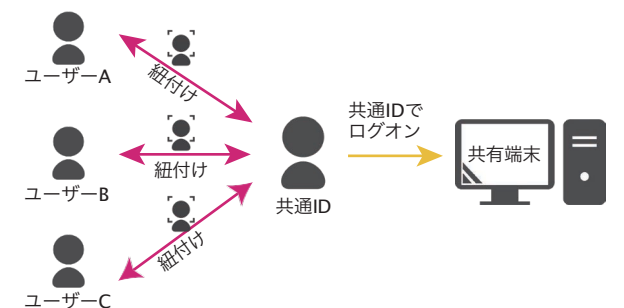
管理者用GUI による個別メンテナンスに加えて、CSVファイルを用いたユーザー情報等の一括メンテナンスが可能です。



代理認証機能

◆ Windows Helloでは不可能な共通IDの利用 個人ユーザーの紐付けを実現

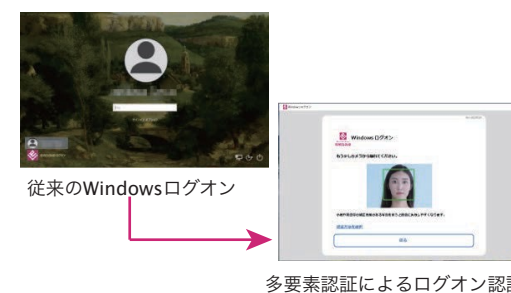
共有端末を利用するシーンでは、共通IDと個人IDを紐付ける代理認証機能が有効です。ユーザーは個人IDで認証すると共通IDとしてログオンできます。画面ロックした場合、別ユーザーはWindowsをログオフせずに画面ロックを解除し、継続利用ができます。



OSログイン

◆ Windows OSログイン

Active Directory とのユーザー情報同期を行うことで、Windowsログオン認証でも利用可能となります。ユーザーは多要素認証を利用してWindows にログオンすることができます。画面ロックした場合、別ユーザーはWindowsをログオフせずに画面ロックを解除し、継続利用ができます。
* WORKGROUPでの利用、Microsoftアカウントでの利用にも対応しています。



◆ ChromeOSログイン

Google Workspace との SAML連携 をすることで、ユーザーは ChromeOS（Chromebookなど）のログインに顔認証などを利用した多要素認証を利用することができます。

