

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。
※偽造検知機能は次期バージョンで対応予定です。



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

●動作環境●

OS	ブラウザ
Windows 10 / 11 (x32/x64/ARM)	IDaaS認証アプリ内のブラウザ、Edge 99以降、Chrome 98以降
macOS 11以降 (x64/apple silicon)	Safari 14以降、Chrome 98以降
iOS 14以降 iPadOS 16以降	Safari 15.3.1以降、Chrome 98以降
ChromeOS 116以降	Chrome
Android 12以降	Androidブラウザ、Chrome 98以降

※動作環境の詳細は、別途お問合せください。

●サービス内容●

機能		基本パック※1	GIGAスクールパック※2 アカデミックパック※3	メディカルパック※4
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マネージャーオプション※5	○	○
OSログオン	Windows OSログオン	Windows OSログオン認証 オプション※6	○	○
	ChromeOSログオン	○	○	○
多要素認証	顔認証（サーバー認証）	○	○	○
	指紋認証（サーバー認証）	オプション※7	オプション※7	オプション※7
	FIDO認証（WebAuthn）	○	○	○
	ワンタイムパスワード認証	○	○	○
	ICカード認証	オプション	オプション	オプション
	QRコード認証	○	○	○
	クライアント証明書認証	○	○	○
	パスワード認証	○	○	○
ユーザーメンテナンス (ID連携)	PIN認証	○	○	○
	Active Directory連携	○	○	○
	Microsoft Entra ID連携	○	○	○
	CSV	○	○	○

※1 最小利用 ID 数は 30 ID、契約単位は 1 年間です。価格は 200円（税別）ID / 月額 です。オプションは別途お問い合わせください。

※2 最小利用 ID 数は 100 ID、契約単位は 5 年間です。詳細はお問い合わせください。文部科学省認可の小学校・中学校・高等学校・高等専門学校・特別支援学校・養護学校・盲学校・聾学校を対象とします。

※3 最小利用 ID 数は 1000 ID、契約単位は 4 年間（大学の場合）、3 年間（短期大学）等対象の教育課程に準じます。詳細はお問い合わせください。文部科学大臣認可の私立大学及び私立高等専門学校を設置する学校法人、都道府県知事認可の専門学校、文部科学省認可の国立および公立の大学法人を対象とします。

※4 最小利用 ID 数は 30 ID、契約単位は 1 年間です。詳細はお問い合わせください。医療機関・介護施設・関連サービス事業者を対象とします。

※5 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。

※6 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。

※7 DDS製指紋認証ユニットUBF-Touchシリーズでの使用に限りです。

※8 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2025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。

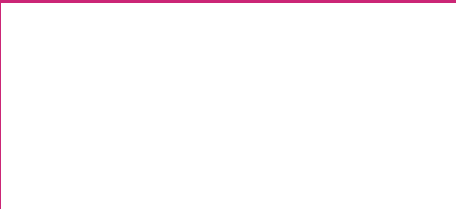
株式会社 ディー・ディー・エス
www.dds.co.jp/ja/

本 社：〒450-0002 愛知県名古屋市中村区名駅三丁目9番6号
アルティメイト名駅2nd 8F

TEL：052-955-6600（代表） FAX：052-583-7800
東京支社：〒108-0075 東京都港区港南二丁目16番1号 品川イーストワンタワー7F
TEL：03-6894-4098（代表） FAX：03-6894-4099



お問い合わせ

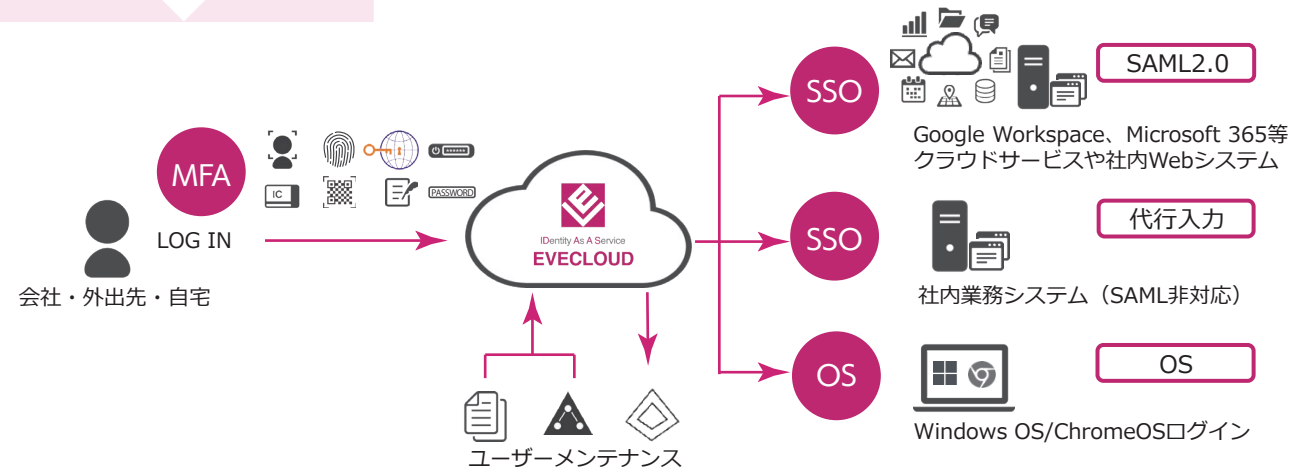


ID管理とクラウドサービス利用時の認証強化、シングルサインオンによる利便性を実現するクラウド認証サービス

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。



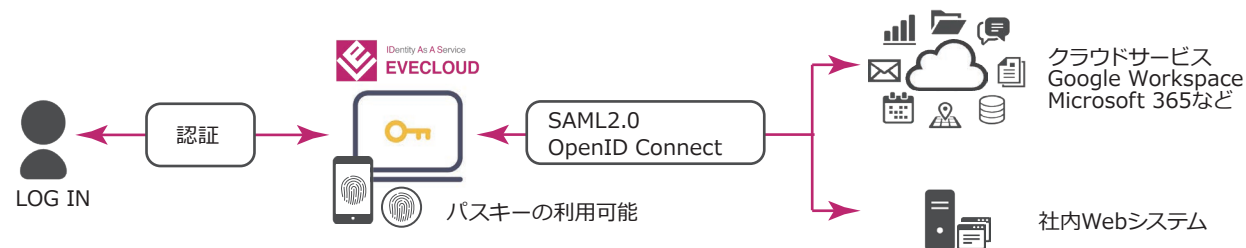
シングルサインオン（SSO）

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」「クライアント証明書認証」「パスワード認証」「PIN認証」から利用するシーンや職務の権限に沿って認証方式の選択ができ、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）に対応

端末内蔵のセンサーやセキュリティキーを使用したブラウザ機能による認証（FIDO2）に対応しています。FIDO パスキーも利用できます。

◆クライアント証明書

端末にインストールする電子証明書です。認証要素の一つとして設定することができます。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。

ユーザーメンテナンス（ID連携）

◆CSVファイルによるメンテナンス

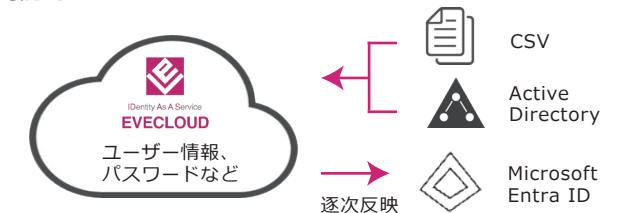
管理者用GUIによる個別メンテナンスに加えて、CSVファイルを用いたユーザー情報等の一括メンテナンスが可能です。

◆Active Directory 連携によるメンテナンス

Windows Server の 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

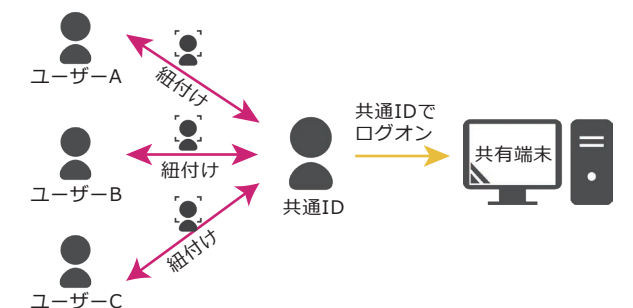
EVECLOUD ユーザーの同期先のドメインとグループを設定することで、EVECLOUD グループ1つに対し、Entra ID のドメインと複数グループを紐づけることができます。EVECLOUD ユーザー追加時のEntra ID アカウントの新規作成、更新時のEntra ID アカウントのプロパティ更新のほか、パスワード変更も可能です。



代理認証機能

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

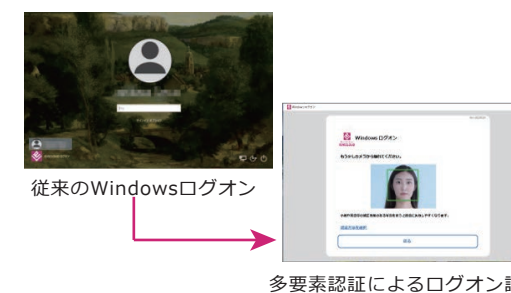
共有端末を利用するシーンでは、共通IDと個人IDを紐付ける代理認証機能が有効です。ユーザーは個人IDで認証すると共通IDとしてログオンできます。画面ロックした場合、別ユーザーはWindowsをログオフせずに画面ロックを解除し、継続利用ができます。



OSログイン

◆Windows OSログオン

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。（WORKGROUPでの利用、Microsoftアカウント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。

