DDS の認証ソリューションのラインナップ

認証システム「EVE」シリーズと、独自アルゴリズムを採用した自社開発の指紋認証ユニット「UBF」シリーズを提供。

▶認証ソリューション（ソフトウェア）

Multi Authentication
EVE MA
イヴ エムエー

- ●指紋、静脈、顔、IC カード、OTP などの多要素認証ソリューション
- ●Active Directory と完全連携

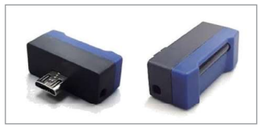
▶指紋認証ユニット（ハードウェア）

UBF-neo
デスクトップ型 PC の利用に最適なケーブルタイプ。
ラフな入力にも対応。

UBF-Tri
モバイル PC に直差しで利用可能な携帯に優れたユニット

UBF-cube
2in1 タブレット / ノート PC 用フルサイズ USB 版ユニット。
「Windows Hello」に対応。

UBF-Hello
Surface 専用ユニット。
「Windows Hello」に対応。



UBF-micro
2in1 タブレット / ノート PC 用 microUSB 版ユニット。
「Windows Hello」に対応。

UBF-Touch
ノート PC に最適なタッチ型指紋センサユニット。

EVE シリーズでサポートする認証方式

単一認証から多要素認証まで、自由にいくつでも組合せてご利用頂けます。

認証方式		対応デバイス
生体認証	指紋	ハイブリット指紋認証（UBF シリーズ）
	静脈	モフィリア（FVA-U3SX）、富士通（Palm Secure-F Pro）
	顔	VGA（640×480）の解像度を持つカメラ
IC カード認証		PaSoRi RC-S380/S（FeliCa、Mifare に対応）
ワンタイムパスワード認証		ハードウェアトークン、Google Authenticator
パスワード認証		独自パスワード

指紋認証をメインでご利用いただくなら、より手軽に導入！

Finger Authentication
EVE FA
イヴ エフエー

- ●指紋認証をメインとした二要素認証ソリューション
- ●SQL Server による ユーザー管理

Finger Authentication
EVE FA
Standalone Edition

- ●サーバー不要で 1 名から指紋認証を利用可能なスタンドアロン製品

（LS00003）

東芝デジタルエンジニアリング株式会社

E-mail: TDEN-sales@ml.toshiba.co.jp
https://www.toshiba-tden.co.jp/

TOSHIBA

商品情報 2021-12

情報漏えい対策ソリューション

多要素認証プラットフォーム

サービスの概要

煩雑なパスワード管理の負担を軽減し、利便性の向上とセキュリティ強化を両立

- ●ID 管理の運用コスト、データベース導入のコストを削減
- ●指紋認証、静脈認証、顔認証、OTP* 認証などに柔軟に対応
- ●Web サイトや業務アプリケーションをパスワードレスで
- ●複数の認証要素を組み合わせることでセキュリティを強化
- ●Active Directory をベースとして高信頼で低コストな運用
- ●拡張性が高いため、必要に応じた規模から運用開始が可能
- ●なりすましを防止し不正アクセスによる情報漏えいを防止

＊OTP：One Time Password

企業の課題

- ●地方自治体の情報セキュリティ対策の強化の最重要課題である「自治体情報システム強靭性向上モデル」にあげられている「個人を特定可能な二要素認証」で重要情報を強固に守りたい。
- ●管理すべき ID とパスワードが多い上に、組織ごとの設定など複雑な管理にコストがかかる。
- ●共用端末をいつ、誰が利用したのかわからない。
- ●アプリケーションごとに異なるパスワードを定期的に変更しなければならず、管理負荷が高い。
- ●アカウント情報を盗まれたら、なりすましによる企業内部からの情報漏えいは防げない。

東芝デジタルエンジニアリング株式会社

情報漏えい対策ソリューション

多要素認証プラットフォーム

個人情報の流出事故！

日本年金機構の個人情報流出事件は、サイバー攻撃が巧妙化･複雑化している現実と、情報セキュリティの強化が待ったなしであることを強く印象づけました。

教育情報セキュリティポリシーに関するガイドライン

文部科学省は「教育情報セキュリティポリシーに関するガイドライン」における推奨事項として「パスワード以外に生体認証や物理認証等の二要素認証を併用しなければならない」としています。

機微な個人情報を含む医療情報の漏えいの対策ガイドライン

厚生労働省も「医療情報システムの安全管理に関するガイドライン」において「本人の識別・認証に用いられる情報は本人しか知り得ない、または持ち得ない状態を保つ必要がある」としています。

しかし、

不正アクセスや内部の悪意による情報漏えいには、ID・パスワードの管理だけでは不十分です。

こうした課題を解決するのが、

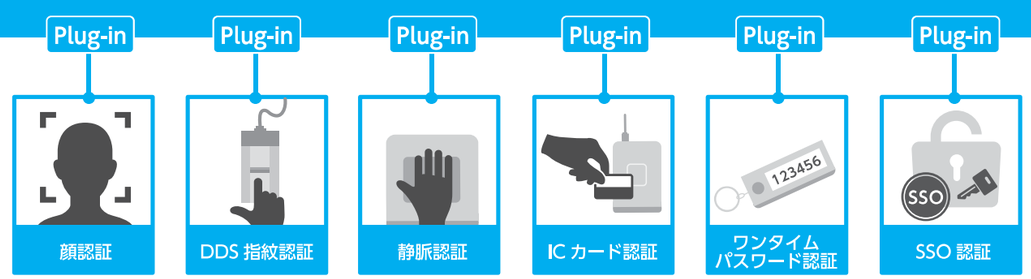
多要素認証統合プラットフォーム EVE MA

情報セキュリティの高度化、運用コストの低減、利便性の向上を同時に実現します。

EVE MA は拡張性が高いプラグインアーキテクチャを採用。必要に応じた規模から始められ、エンタープライズシステムにおいて自在な認証要素の設定が行えます。IC カード認証、指紋認証、静脈認証に加え、顔認証機能にも対応。多様な方式による認証を、Windows ログオンからネットワーク認証、アプリケーション認証など、幅広いシステムに適用できます。

複数の認証要素を自由に組み合わせて利用可能！

多要素対応プラグインプラットフォーム



顔認証

Windows ログオンやアプリケーションログインを顔認証に置き換えます。
カメラに顔を向けるだけのハンズフリー認証で手間なくログオン。
常時監視による離席時の画面ロックで、第三者のなりすましによる不正利用も防ぎます。

認証時の顔向き判定

カメラの前で顔を左右に動かして認証するように設定できるので、本人が確実にカメラの前にいることが確認でき、**写真によるなりすましを防止**します。

離席ロック

ログオン後も本人の利用を常時監視。本人を検出できない場合や認証したユーザー以外を検出した場合は画面をロック。**本人以外の利用を防止**します。

指紋認証

マニューシャ方式と周波数解析方式、2 つの認証方式を融合させたハイブリッド認証方式。

マニューシャ方式（一般的な方式）

指紋模様の盛り上がった部分の端点や分岐点の位置関係を特徴としてとらえます。

メリット
- 粗い入力（指か移転や先端のみ入力）でも認証しやすい。

デメリット
- 経時変化非対応。
- 登録ができない人がいる。(2~5%)

周波数解析方式（DDS 独自）

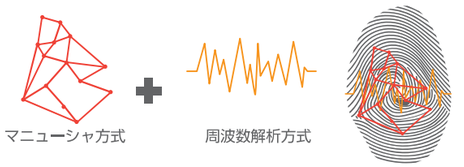
指紋模様パターンをスライスした箇所を、波形として特徴情報をとらえる。

メリット
- 経時変化に対応。
- 登録拒否がなく、誰でも利用可能。

デメリット
- 丁寧な入力が必要。

2 つのいいとこ取りで
『誰でも使える』『格段に使いやすい』を実現

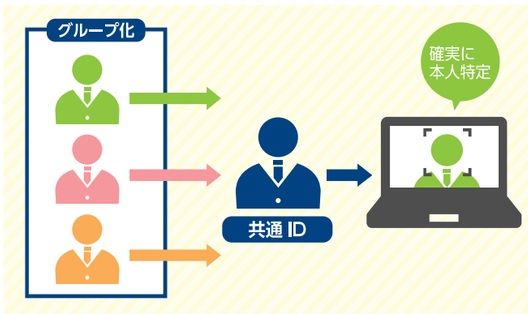
登録成功率100%



多様な利用シーン

共用端末での利用

窓口端末、店舗の共用端末など共通 ID を利用するシーンでも、確実に本人を特定。認証ログから共通 ID をどのユーザーが利用したかも特定可能。



仮想化環境での利用

仮想化環境でも二要素認証によるログオンが可能。
VMware Horizon、Citrix XenApp/XenDesktop、Windows RDP、Ericom Connect などの仮想デスクトップに対応。