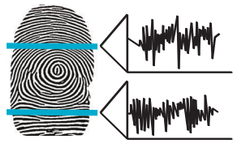
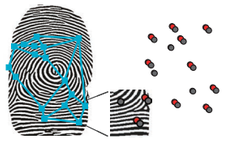
ハイブリッド指紋認証方式に対応

ハイブリッド指紋認証方式では、DDS独自の周波数解析法を用いた指紋認証アルゴリズムとマニューシャアルゴリズムの2種類の指紋認証アルゴリズムを同時に使用し、複合的なハイブリッド特徴量により登録・照合します。これにより2つのアルゴリズム優位性を兼ね備えた高性能な指紋認証性能を実現します。

※ DDS独自の方式で元の指紋画像には復元できない特徴量データを登録しています。

※ 指紋認証ユニットの種類により、使用する指紋認証アルゴリズムは異なります。UBF-Touch®シリーズは、従来の数十倍の情報量を利用した詳細な認証処理によりスイープ型指紋センサーと同等の認証精度を確保し、PAD（Presentation Attack Detection：提示型攻撃検知）の対策として、LBP（Local Binary Pattern）などに代表される複数の画像認識技術をベースとしたDDS独自の攻撃耐性や偽造指対策をした高い認証精度と安全性を実現した新アルゴリズムを使用しています。

ハイブリッド指紋認証方式では２つのアルゴリズムの長所を融合

周波数解析法（DDS社独自方式）	マニューシャ法（一般的な方式）
	
指紋模様パターンをスライスした個所を、波形として特徴情報をとらえる。 〈長所〉 ●登録拒否がなく、すべての人が利用可能 ●指紋模様の特徴情報の作成が早い	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情報としてとらえる。 〈長所〉 ●粗い入力（指回転や先端のみ入力）でも認証しやすい

特許番号（米国）7,079,672 7,310,433 8,369,583　特許番号（日本）4,221,220 4,730,502 4,897,470

●動作環境●

	EVE FAサーバー	EVE FAクライアント・管理端末クライアント
ハードウェア	・CPU：2GHz 以上 ・HDD：プログラム 80MB + データサイズ（設定や運用により変動。100 ユーザーでログを 365 日保存の場合、約 3GB 程度） ・RAM：3GB 以上 ・LAN：100BASE-TX 以上推奨	・CPU：1GHz 以上 ・HDD：プログラム 160MB ・RAM：1GB 以上 ・LAN：100BASE-TX 以上推奨 ・USB：1 ポート以上
OS	・Microsoft Windows Server 2016 Standard Edition ・Microsoft Windows Server 2019 Standard Edition ・Microsoft Windows Server 2022 Standard Edition ・Microsoft Windows Server 2025 Standard Edition 上記の日本語版	・Microsoft Windows 10 Pro/Enterprise Edition(x86/x64) ・Microsoft Windows 11 Pro/Enterprise Edition ・Microsoft Windows Server 2016 Standard Edition ・Microsoft Windows Server 2019 Standard Edition ・Microsoft Windows Server 2022 Standard Edition ・Microsoft Windows Server 2025 Standard Edition 上記の日本語版
データベース	・Microsoft SQL Server 2016 Express/Standard/Enterprise Edition SP1 ・Microsoft SQL Server 2017 Express/Standard/Enterprise Edition ・Microsoft SQL Server 2019 Express/Standard/Enterprise Edition ・Microsoft SQL Server 2022 Express/Standard/Enterprise Edition ・Oracle Database 19c Standard Edition 2/Enterprise Edition 上記の日本語版	—
ネットワーク	IPv4プロトコル	IPv4プロトコル
ディスプレイ解像度	—	800×600以上

	主な対応認証デバイス
指紋認証	DDS製 UBF-neo, UBF-Touch®, UBF-Touch® Type-C, UBF-cube, UBF-Hello, UBF-micro
ICカード認証	ICカードリーダー：ソニー社製 PaSoRi RC-S380/S, PaSoRi RC-S300/S,PaSoRi RC-S300/S1 ICカード：FeliCa, MIFARE

※ 動作環境の詳細、対応仮想環境については弊社ウェブページをご参照ください。※ 他にも対応可能な認証デバイスがございます。別途 お問い合わせください。

改正個人情報保護法に対応

「個人情報保護法」の改正により、個人情報保有件数の定義が撤廃され、事実上すべての事業者が法規制の対象となりました。また、指紋、静脈、顔等の生体データが個人情報として明確に定義されました。EVE FAは、強化された法規制に基づくガイドラインの分類・機能に準拠した製品です。

分　類	機　能
個人データの管理に関する義務	生体特徴情報（個人識別符号）の書き出し制御
	個人情報となる認証情報の復元および二次利用不可
	生体特徴情報の削除
個人情報の取得に関する義務	生体特徴情報登録時の利用目的の通知および確認
確認・記録義務	上記利用目的通知と本人同意確認および、その記録

202503_D181890_13

株式会社 ディー・ディー・エス
www.dds.co.jp/ja/

本　　社：〒460-0002　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

Finger Authentication
EVEFA
二要素認証基盤

DDS　指紋認証やICカードなどで企業情報システムを情報漏えいから守る「二要素」本人認証ソリューション

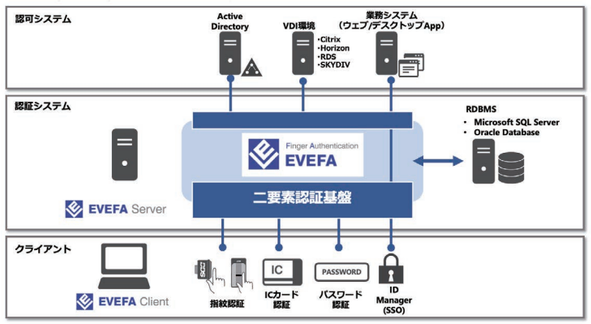
エンタープライズの強固なアクセスセキュリティを実現する大規模向け指紋認証ソリューション

EVEFAの特長

高いセキュリティレベルを実現するアーキテクチャ

◆高いセキュリティレベルとレスポンスを実現するサーバーサイド認証

- 指紋情報の照合、認証をサーバーサイドで実施。
- 認証プロセスの集中化による高いセキュリティレベルを実現。
- 高度なプロセスコントロールによるパフォーマンス向上を実現。



◆二要素認証によるセキュリティの強化

EVEFAでは、認証方式として、
単一認証から二要素認証まで設定が可能です。
マイナンバーを取り扱う自治体情報システムに求められるセキュリティの強化要件として重要視される「個人を特定可能な二要素認証」に対応します。

単一認証要素	指紋	ICカード	Windowsパスワード

二要素認証	ICカード+指紋	ICカード+Windowsパスワード	ICカード+FAコード	
	指紋+Windowsパスワード	指紋+FAコード	デバイス+Windowsパスワード	デバイス+FAコード

大規模運用を支えるスケーラビリティ

◆エンタープライズのアクセスセキュリティ環境を実現するスケーラビリティ

EVEFAでは、アプリケーション層であるFA Serverとデータ管理層の多層構造により、スケーラブルなシステム構成を可能にします。

◆各種負荷分散ソリューションへの対応

FA Serverでは、ロードバランサーなどの負荷分散装置を利用することで、DNSラウンドロビンなどの各種ロードバランシングを行うことが可能です。
また、FA Database ServerではRDBMSが備えるフェイルオーバークラスタリングなどの冗長機能構成を適用することができます。

高い管理運用性

◆充実した管理機能

管理者はFA管理ツールにより、ユーザー管理を一括で行うことが可能です。また、IDマネージャによるアプリケーションアクセス管理も一元的に設定可能です。さらに、ユーザーのアクセスログの保持機能も充実しており、リスク管理をサポートします。

◆Active Directoryとの連携

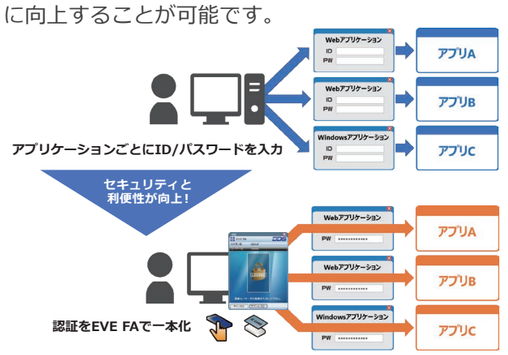
EVEFAは企業情報システムの中核となるActive Directoryとの親和性を実現しています。
これにより、従来のWindowsネットワーク内でのID/パスワードログオンを指紋認証に置き換えることを可能とします。

EVEFAは、Active Directoryをご利用でないお客様にも安心して二要素認証を導入いただけるソリューションです。

アプリケーションログオンへの対応

◆アプリケーションログオンにも指紋認証を容易に設定可能なIDマネージャを標準実装

IDマネージャ管理ツールからドラッグ&ドロップ操作でアプリケーションログオンに指紋認証を適用可能です。WEBアプリケーション、Windowsアプリケーションなどのさまざまなアプリケーションログオンにおけるユーザビリティとセキュリティを同時に向上することが可能です。



共通IDへの対応

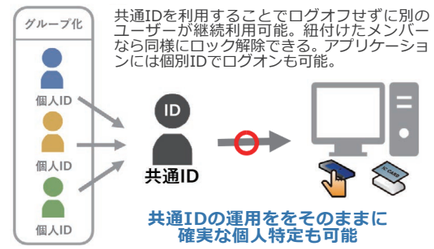
◆共通IDのセキュリティ

窓口端末など複数のユーザーを１つのユーザーIDでログオンさせたい場合、グループ認証機能を利用します。グループに登録されたユーザーはグループのIDでログオンできます。

◆個人IDの特定

管理者はグループ認証した「個人」を特定できるため、セキュリティが確保できます。

グループ認証機能

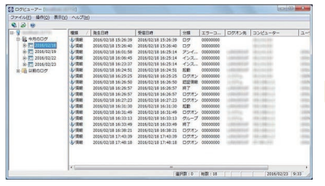


共通IDを利用することでログオフせずに別のユーザーが継続利用可能。紐付けたメンバーなら同様にロック解除できる。アプリケーションには個別IDでログオンも可能。

共通IDの運用ををそのままに確実な個人特定も可能

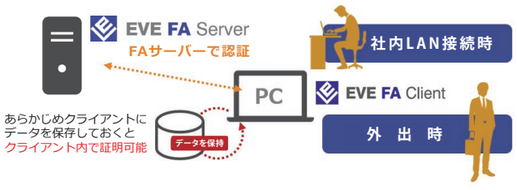
ログの収集と確認でセキュリティ管理

ログビューアーを利用して、アクセス時のログ詳細（日時、ユーザー、コンピューター、ログオン先など）を閲覧することができます。
取得したログをCSVに出力・保存することも可能です。



モバイル端末の認証

EVEFAは、ノートPCの社外持ち出し時の認証に対応しています。
社内LANから切断された環境下でも、セキュリティを確保できます。



仮想化環境への対応

◆EVEFAは多くの企業・団体で急速に導入が進んでいる仮想化環境に対応しています。

仮想化環境への接続用アプリケーションの認証や、仮想化環境内で動作するアプリケーションの認証に、二要素認証を適用いただけます。

各種仮想化方式に対応
- Citrix Virtual Apps and Desktops
- Horizon
- Remote Desktop Service
- SKYDIV Desktop Client

各種利用端末にも対応
- FATクライアント（Windows）
- シンクライアント（Windows 10 IoT等）