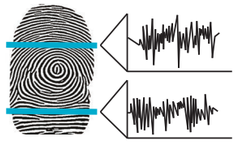
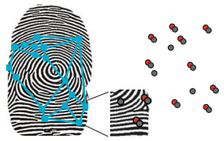
ハイブリッド指紋認証方式に対応

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●

	EVEMAサーバー	EVEMAクライアント・管理端末クライアント
ハードウェア	・CPU：3GHz 以上推奨 ・HDD：プログラム 30MB + データサイズ (ユーザー数や設定により変動。※1000ユーザーで最大100MB程度) (イベントログは別途見積もりが必要) ・RAM：8GB 以上推奨 ・LAN：1000BASE-TX 以上推奨	・CPU：3GHz 以上推奨 ・HDD：プログラム 150MB ・RAM：4GB 以上推奨 ・LAN：100BASE-TX 以上推奨 ・USB：1 ポート以上
OS	・Microsoft Windows Server 2016 Standard Edition(x64) ・Microsoft Windows Server 2019 Standard Edition(x64) ・Microsoft Windows Server 2022 Standard Edition(x64) 上記の日本語版	・Microsoft Windows 10 Pro/Enterprise Edition(x86/x64) ・Microsoft Windows 11 Pro/Enterprise Edition(x64) ・Microsoft Windows Server 2016 Standard Edition(x64) ・Microsoft Windows Server 2019 Standard Edition(x64) ・Microsoft Windows Server 2022 Standard Edition(x64) 上記の日本語版

※動作環境の詳細、対応する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。顔認証Nextプラグインをご利用の際は別途お問合せください。

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-Pocket, UBF-Tri
静脈認証	手のひら静脈：富士通フロンテック製 PalmSecure-F Pro センサー、PalmSecure V2 センサー 指静脈：モフィリア社製　FVA-U3SX
顔認証	VGA以上のPC内蔵カメラまたは外付けカメラ
ICカード認証	ICカードリーダー：ソニー製 PaSoRi RC-S300/S、RC-S300/S1、RC-S380/S ICカード：FeliCa, MIFARE Standard 1K/Standard 4K/Ultralight/Ultralight C, マイナンバーカード

※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。　※マイナンバーカードの利用をご希望の場合は、ご購入前に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。EVEMA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

202402_D181880_18

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

Multi Authentication
EVEMA

多要素認証基盤

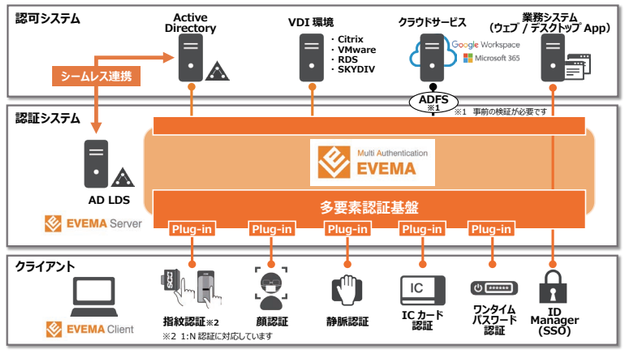
DDS

指紋認証をはじめ、ICカードなど企業で利用されるあらゆる認証デバイスの統合的な運用管理を実現

EVEMAで煩雑なパスワード管理から解放。
ADと連携した高い柔軟性。ニーズにあったセキュリティを実現。

EVEMAの特徴

EVEMAは必要に応じた規模から始められるプラグインアーキテクチャを採用し、エンタープライズシステムにおいて自在な認証設定を可能にします。
生体認証、ICカード認証、パスワード認証など様々な方式による認証をWindowsログオンからアプリケーション認証まで幅広いシステムに適用可能です。



Active Directoryとのシームレスな連携

◆ユーザー管理を容易に実現

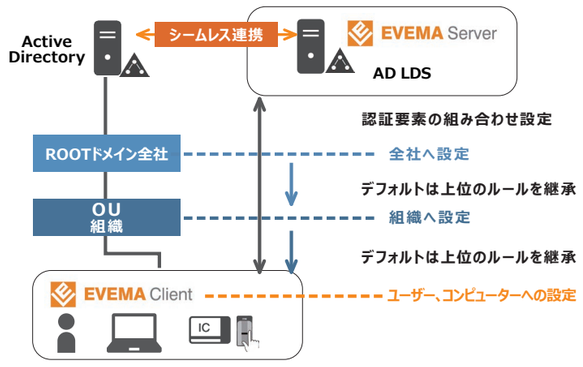
EVEMAの管理は「Active Directory ユーザーとコンピューター」を利用します。使い慣れたツールでユーザー管理が可能です。

◆信頼性の高いDB（AD LDS）が無償で利用可能

Windows標準のAD LDS（ Active Directoryライトウェイト ディレクトリ サービス）を採用することにより、無償で信頼性の高いDBが利用できます。Active Directoryと同様のDB冗長化が低コストで実現可能です。

◆部門事情に応じた柔軟な設定が可能

社内のセキュリティ要件は部門によって異なることがほとんどです。Active Directory上のOU（組織）やグループを活用して、セキュリティを強化したい部門は生体認証、それ以外の部門はICカードを採用といった、柔軟な設定が可能です。



セキュリティの強化

◆パスワード管理からの解放

複雑なパスワード入力、定期的なパスワード変更が不要になります。パスワードは管理負荷が高い反面、セキュリティの維持が困難です。指紋認証やICカード認証を採用することにより、パスワード管理の問題から解放されます。

◆既存資産の活用

複数の認証要素をサポートしているEVEMAでは社員証や入退室のICカード、マイナンバーカードなども利用できます。

◆なりすましの防止

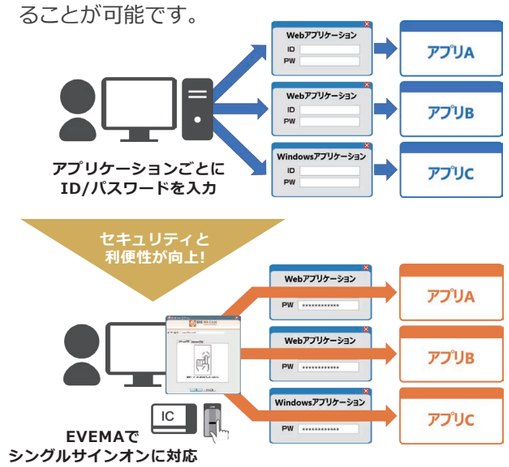
パスワード認証には、なりすましのリスクがあります。EVEMAは、指紋、静脈や顔などの生体認証によって、なりすましを防ぎます。
重要な情報にアクセスする部門、外部社員アクセスが必要な部門など、なりすましリスクを伴うシーンには「確実な」本人認証を提供します。

◆AND認証によりセキュリティ強化

指紋とICカード、ワンタイムパスワードトークンとパスワードなど、複数の認証を要求する「AND認証」に対応しています。
必要に応じて認証要素を組み合わせて、より高いセキュリティを構築できます。

認証を統合し利便性を向上

企業では、Windowsログオン、Webサイトの認証、業務システムのログオンなど、あらゆる場面でパスワードが求められます。
ID Manager機能を利用すると、従来は別々に管理していたパスワードを、EVEMAの認証システムに一本化できるためスマート且つ安全な運用が可能になります。また、セキュリティを統合的に一元管理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

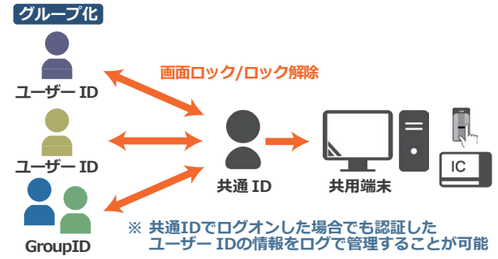
窓口端末などの共通IDを利用するシーンでは、個人IDと共通IDを紐づける、代理認証機能が有効です。普段と同じ個人IDの認証操作で、共通IDとしてログオンできます。

◆個人IDの特定

管理者は共通IDとしてログオンした「個人」を特定できるため、セキュリティが確保できます。

■代理認証機能

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でログインも可能。



ログの収集と確認でセキュリティ管理

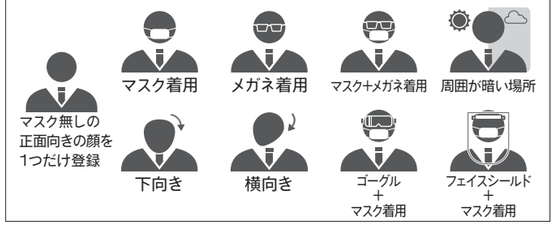
ログビューアーを利用して、アクセス時のログ詳細（日時、ユーザー、コンピューター、認証要素、認証結果など）を閲覧することができます。
取得したログをCSVに出力・保存することも可能です。

モバイル端末の認証

EVEMA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。

マスク・メガネ着用時でも認証可能

高速判定を実現するDDSの軽快顔認証とパナソニック コネクトの顔認証技術を採用した顔認証Nextをご用意しています。マスク着用時の認証が可能で、認証時の不安を軽減します。



仮想化環境への対応

◆EVEMA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、多要素認証を適用いただけます。また、ファットクライアント、シンクライアント（Windows 10 IoT等）の他、一部の認証要素でゼロクライアントでの利用に対応しています。

各種仮想化方式に対応
- Citrix Virtual Apps and Desktops
- VMware Horizon
- Windows Server RDS
- SKYDIV Desktop Client

各種利用端末にも対応
- FATクライアント
- シンクライアント、ゼロクライアント