

# 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。



## 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)
<p>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。</p> <p>〈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</p>	<p>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の特徴情報としてとらえる。</p> <p>〈長所〉 ●粗い入力 (指回転や先端のみ入力) でも認証しやすい</p>

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 MAサーバー	EVE MAクライアント・管理端末クライアント
ハードウェア	<ul style="list-style-type: none"> <li>・CPU : 3GHz 以上推奨</li> <li>・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)</li> <li>・RAM : 8GB 以上推奨</li> <li>・LAN : 1000BASE-TX 以上推奨</li> </ul>	<ul style="list-style-type: none"> <li>・CPU : 3GHz 以上推奨</li> <li>・HDD : プログラム 150MB</li> <li>・RAM : 4GB 以上推奨</li> <li>・LAN : 100BASE-TX 以上推奨</li> <li>・USB : 1ポート以上</li> </ul>
OS	<ul style="list-style-type: none"> <li>・Windows Server 2008 Standard / Enterprise Edition SP2 (x86/x64)</li> <li>・Windows Server 2008 R2 Standard / Enterprise Edition SP1 (x64)</li> <li>・Windows Server 2012 Standard Edition (x64)</li> <li>・Windows Server 2012 R2 Standard Edition (x64)</li> <li>・Windows Server 2016 Standard Edition (x64) (Ver.1607)</li> <li>・Windows Server 2019 Standard Edition (x64) (Ver.1809)</li> <li>上記の日本語版</li> </ul>	<ul style="list-style-type: none"> <li>・Windows 7 Professional/Enterprise/Ultimate Edition SP1 (x86/x64)</li> <li>・Windows 8.1 Pro/Enterprise Edition (x86/x64)</li> <li>・Windows 10 Enterprise Edition (x64) (Ver.1709)</li> <li>・Windows 10 Pro/Enterprise Edition (x86/x64) (Ver.1803/1809/1903)</li> <li>・Windows Server 2012 Standard Edition (x64)</li> <li>・Windows Server 2012 R2 Standard Edition (x64)</li> <li>・Windows Server 2016 Standard Edition (x64) (Ver.1607)</li> <li>・Windows Server 2019 Standard Edition (x64) (Ver.1809)</li> <li>上記の日本語版</li> </ul>

※1 動作環境の詳細、対応仮想環境については弊社ウェブサイトをご参照ください。

## 主な対応認証デバイス ※2

指紋認証	DDS製 UBF-neo, UBF-Tri, UBF-cube, UBF-Hello, UBF-Pocket, UBF-Touch
指静脈認証	モフィア製 FVA-U3SX
手のひら静脈認証	富士通フロンテック製 Palm Secure V2 センサー、PalmSecure-F Pro センサー
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 : FeliCa, MIFARE Standard 1K/Standard 4K/Ultralight, マイナンバーカード

※2 他にも対応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 MAは、強化された法規制に基づき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	<ul style="list-style-type: none"> <li>生体特徴情報 (個人識別符号) の書き出し制御</li> <li>個人情報となる認証情報の復元および二次利用不可</li> <li>生体特徴情報の削除</li> </ul>
個人情報の取得に関する義務	<ul style="list-style-type: none"> <li>生体特徴情報登録時の利用目的の通知および確認</li> </ul>
確認・記録義務	<ul style="list-style-type: none"> <li>上記利用目的通知と本人同意確認および、その記録</li> </ul>

※記載の内容は2020年4月のものです。記載内容は、予告なく変更する場合があります。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。 202004 D181880\_04



Multi Authentication  
**EVE MA**

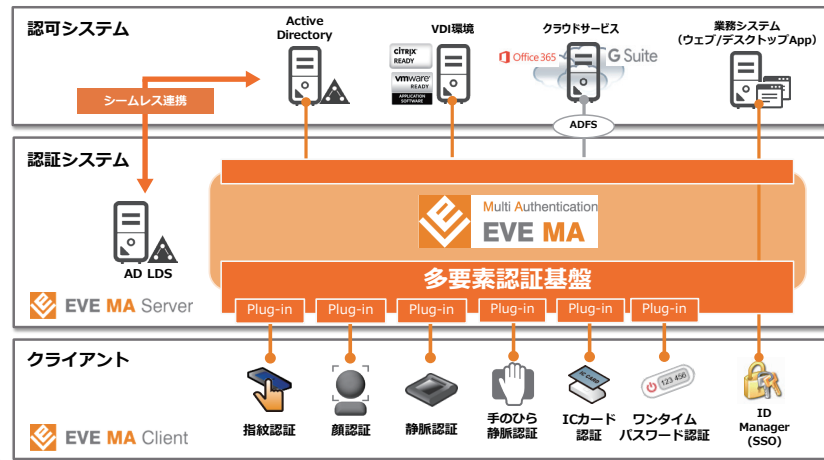
多要素認証基盤



# EVE MA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。

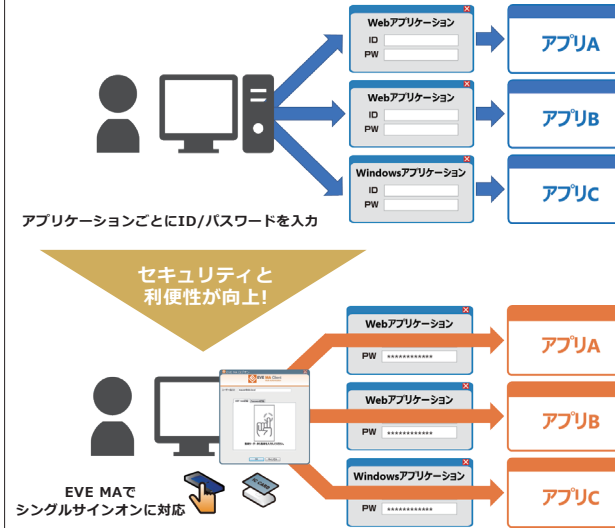
## EVE MAの特徴

EVE MA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。



## 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、EVE MA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。



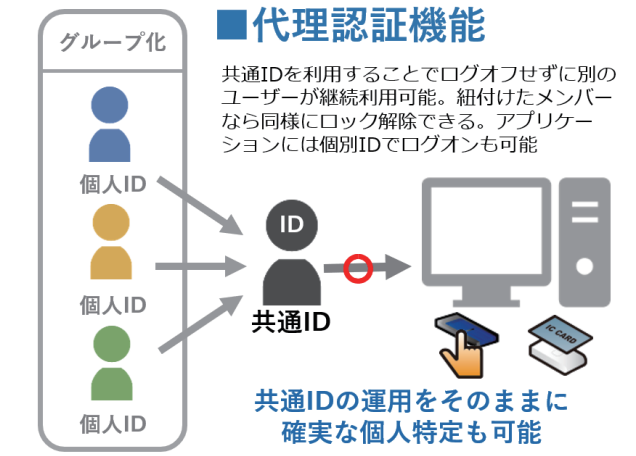
## 共通IDへの対応

### ◆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。



## Active Directoryとのシームレスな連携

### ◆ユーザー管理を容易に実現

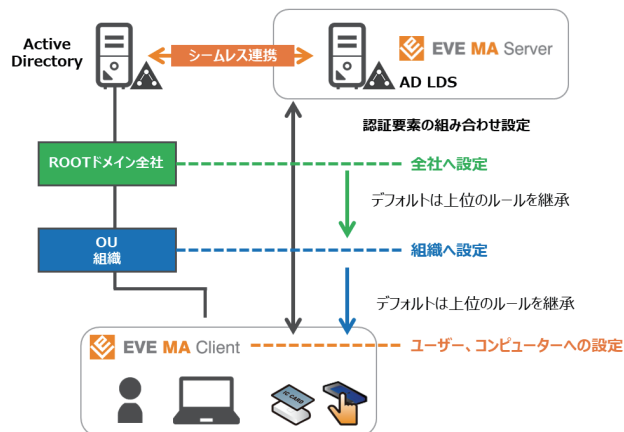
EVE MAの管理は「Active Directory ユーザーとコンピュータ」を利用します。使い慣れたツールでユーザー管理が可能です。

### ◆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EVE MAでは社員証や入退室のIC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。EVE MA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、より高いセキュリティを構築できます。

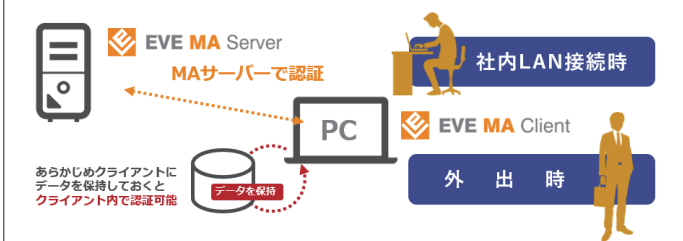
## ログの収集と確認でセキュリティ管理

ログビューアを利用して、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

EVE MA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

### ◆EVE MAは多くの企業・団体に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。

