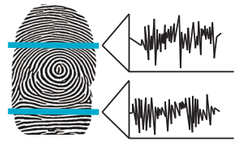
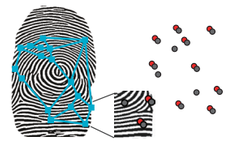
ハイブリッド指紋認証方式に対応

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つのアルゴリズムの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）
	
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●

	Themisサーバー（オンプレミス構築の場合）	Themis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：ユーザー数や設定により変動します ・RAM：4GB以上推奨 ・LAN：100BASE-TX以上	・HDD：プログラム150MB ・LAN：100BASE-TX以上 ・USB：1ポート以上 ・CPU：2GHz以上推奨 ・RAM：1GB以上推奨
OS	・CentOS 7.2 (amd64) ・RedHat Enterprise Linux 7.2 (amd64)	・Microsoft Windows 10 (x86/x64) ※顔認証はx64のみ
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

※1 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。

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
指静脈認証	モフィリア製　FVA-U3SX
手のひら静脈認証	富士通フロンテック製 PalmSecureセンサーV2
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

※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。Themis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

株式会社ディー・ディー・エス　www.dds.co.jp
【本社】〒460-0002 愛知県名古屋市中区丸の内三丁目6番41号 DDSビル7F
TEL:052-955-6600（代表）FAX:052-955-6610
【東京支社】〒103-0028　東京都中央区八重洲一丁目8番5号 新槇町ビル別館第二 2F
TEL:03-3272-7900（代表）FAX:03-3272-7901

Universal Authentication
Themis
万能認証基盤

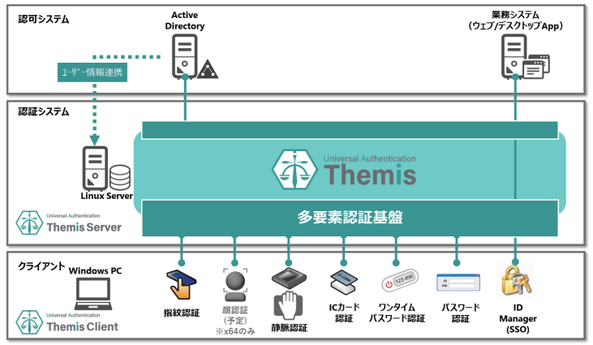
DDS

ICカード認証、指紋認証、パスワードをはじめとするさまざまな方法による認証を実現する万能認証基盤

**認証方法とログオン対象を自由に組み合わせて利用することで、
システムが要求したセキュリティレベルに応じた認証方法の活用が可能。
従来の認証と比較して高いセキュリティを保つことができます。**

Themisの特長

Themisでは、指紋認証をはじめとする生体認証やICカード認証など、様々な認証要素を組み合わせたユーザー認証がご利用いただけます。
複数の認証要素を組み合わせるAND認証
（例：指紋認証とICカード認証による二要素認証）
や、ひとつを選択して認証するOR認証
（例：指紋認証またはパスワード認証いずれかによる認証）
の設定も可能です。



利便性・作業性の向上　◆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。

かけたコストが無駄にならない　◆既存資産の活用

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

多様な働き方に対応する確実な本人認証　◆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。Themis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。
Themisなら、生体認証を社内・社外、テレワーク時のVDI環境にも柔軟に適応できます。

認証要素を自由に選べる　◆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。

Active Directoryとのユーザー情報連携と利便性を向上する各種対応機能

◆ADとのユーザー情報連携

Active Directory（AD）で管理するユーザーアカウントを、Themisのアカウント情報と同期してご利用いただけます。
ADのユーザーアカウントおよびパスワードを自動で反映するため、アカウントの新規作成、複雑なパスワードの設定や定期的な変更に柔軟に対応します。

◆ウェブ管理ツールを用いたユーザー管理

ユーザーの追加と削除、グループの追加と削除、
認証要素・認証セットの設定、アプリケーションの設定など
認証に必要なセットアップをウェブの管理ツールで行います。
Themisでは、管理者向けと一般ユーザー向けを用意、
一般ユーザーとしてログインすると、ログインしたユーザーの情報
を見たり、指紋やパスワードの登録などを行ったりすることができます。

◆内部統制につながるログ解析

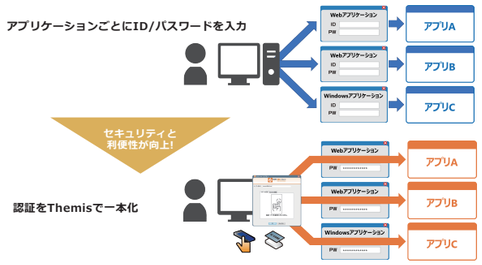
認証ログを確認することで内部統制に有用な情報を調査することができます。
ログ情報はCSV形式のファイル出力も可能です。

◆オフライン認証の対応

オフライン認証に対応しています。
オンライン時にあらかじめ認証に必要な情報を取得しておくことで、社外でのオフライン環境でもThemisによる認証/ログオンをご利用いただけます。

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、Themis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。



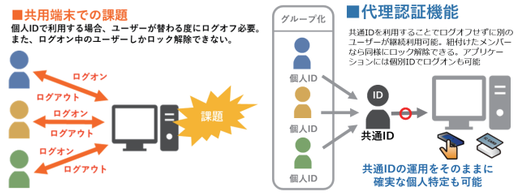
共通IDへの対応

◆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。



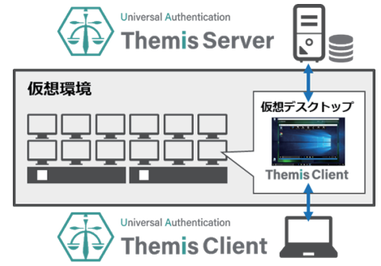
仮想化環境対応

◆Themis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 Terminal Service

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



NEW 連携認証

**フェデレーション対応により、SAMLを
利用したシームレスなSSOも実現します。**

NEW スマートデバイス利用

◆ スマートデバイスによる認証

スマートフォンに搭載されている生体認証を使用して認証を行う
FIDO OOB（Out Of Band）機能により、プッシュ通知による
認証開始、もしくはQRコードによる認証開始を設定することができます。

◆ スマートデバイスでのクラウドサービス認証

スマートデバイスで利用するウェブアプリケーション
（ブラウザ経由、 SAML連携が可能であること）の認証に
スマートフォンに搭載されている生体認証が使用できます。

※ FIDO OOBのご利用にはマガタマサービスとの連携が必要です。Themis単体でのご利用はできません。