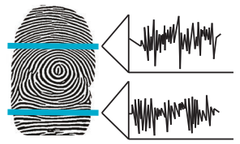
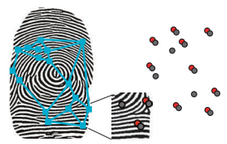
ハイブリッド指紋認証方式に対応

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●

	Themisサーバー（オンプレミス構築の場合）	Themis DBサーバー（オンプレミス構築の場合）	Themisクライアント		
			Windows OS	Chrome OS	iPadOS
ハードウェア	・CPU：2GHz以上、8コア以上推奨 ・RAM：16GB以上推奨 ・HDD：100GB以上（OSシステム領域、Themisサーバー基本領域） ・LAN：1000BASE-TX以上	・CPU：2GHz以上、8コア以上推奨 ・RAM：16GB以上推奨 ・HDD：100GB以上（OSシステム領域、ThemisサーバーDB領域） ・LAN：1000BASE-TX以上	・RAM：8GB以上推奨 ・LAN：1000BASE-TX以上 ・USB：1ポート以上（認証デバイス利用時） ※顔認証Next利用時のCPU：Intel Core i5 / Intel Core i7 / Intel Xeon Scalableで動作確認済	―	
OS	・Ubuntu Server 22.04 LTS	・Ubuntu Server 22.04 LTS	・Microsoft Windows 10,11 ・Windows Server 2019, 2022 ※ Windows OS ログオン、IDマネージャー、Web認証連携（SAML）に対応 ※ 顔認証Nextはx64にのみ対応	・Chrome OS（顔認証Next、パスワード認証、QRコード認証、OTP認証） ※ Chrome OS ログイン認証、Web認証連携（SAML）に対応	・iPadOS（顔認証Next、パスワード認証、QRコード認証、OTP認証） ※ Web認証連携（SAML）に対応
ネットワーク	・IPv4プロトコル	・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	―	

※別途、Ansibleサーバー（構築作業用ホスト）が必要です。詳細はお問い合わせください。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	
指紋認証	DDS製 UBF-neo, UBF-Touch®, UBF-Touch® Type-C, UBF-cube, UBF-Hello, UBF-micro, 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
顔認証およびQRコード認証装置	VGA（640×480）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：ソニー社製PaSoRi RC-S380/S、PaSoRi RC-S300/S ICカード：FeliCa、MIFARE Standard 1K/Standard 4K/Ultralight、マイナンバーカード

※ 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

202402_D181760_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

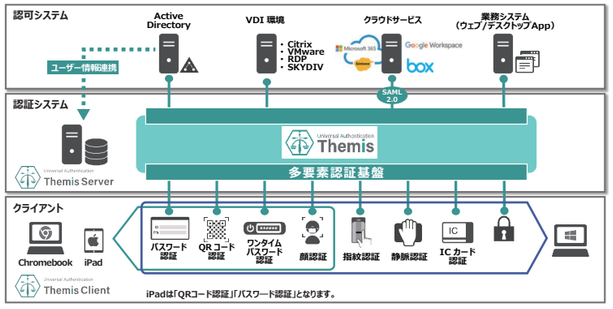
Universal Authentication
Themis
万能認証基盤

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

認証方法とログイン対象を自由に組み合わせ、システムが要求する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

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。

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

◆マルチテナント構成に対応

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。
Themisは、マルチテナント構成に対応しており、
複数のADやワークグループ端末が混在していても運用可能です。

◆ウェブ管理ツールを用いたユーザー管理

ユーザーおよびグループの管理、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、認証に必要な設定をウェブ管理ツールで行います。一般ユーザー向けには、個人用ポータルを用意しており、ログインユーザーの生体情報の登録などが行えます。

◆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/ログインをご利用いただけます。

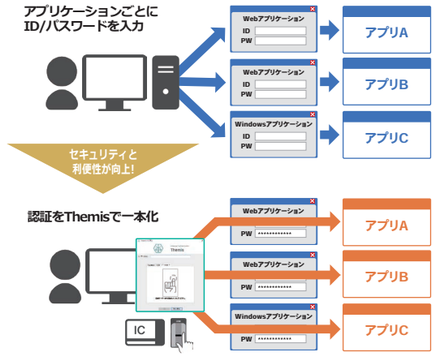
マスク・メガネ着用時でも認証可能

※Windows 10 / Windows 11 (x64)

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。　※2024年春頃を対応予定

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インなど、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としてログインできます。

◆個人IDの特定

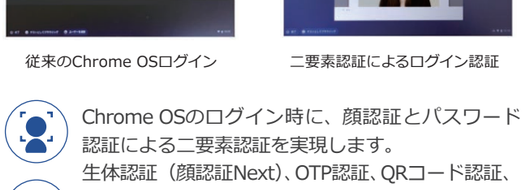
管理者は共通IDとしてログインした「個人」を特定できるため、セキュリティが確保できます。

■共用端末での課題

個人IDで利用する場合、ユーザーが替わる度にログオフ必要。
また、ログイン中のユーザーしかロック解除できない。

■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。



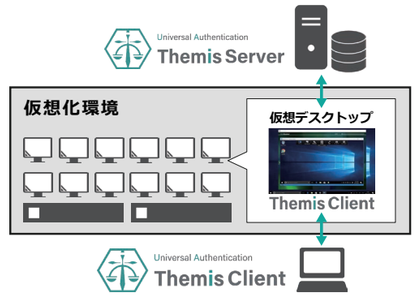
仮想化環境対応

◆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

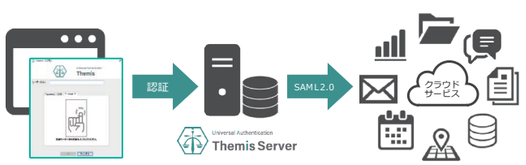
各種利用端末にも対応
- FATクライアント
- シンクライアント、ゼロクライアント



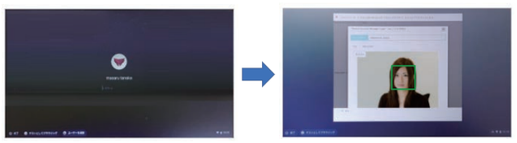
認証連携

認証連携によるSSO

SAML2.0を利用したフェデレーション連携により、ウェブベースのクラウドサービスのログイン認証を多要素認証に置き換えます。
ThemisサーバーがIdPとなりSAML連携が可能なウェブサービス（SP）に対してID連携による認証を提供します。



Chrome OSログイン対応



従来のChrome OSログイン　　二要素認証によるログイン認証

Chrome OSのログイン時に、顔認証とパスワード認証による二要素認証を実現します。
生体認証（顔認証Next）、OTP認証、QRコード認証、パスワード認証がご利用いただけます。