DATA SHEET

FortiTrust Identity

提供形態：

クラウド

アイデンティティ / アクセス管理ソリューション

IAM（アイデンティティ / アクセス管理）ソリューションのセキュリティ、エンドユーザーエクスペリエンス、総コストに関する懸念が、WFA（Work From Anywhere：場所に縛られない働き方）を始めとするデジタルビジネスの採用により高まっています。FortiTrust Identity は、既存のネットワークインフラストラクチャを活用しつつ、最新の認証テクノロジーを使用して、クラウドやオンプレミスのアプリケーションやサービスへのユーザーアクセスの保護を可能にする、クラウドから提供する IAM ソリューションです。

主な機能と特長

FortiTrust Identity は、フォーティネット セキュリティ ファブリック、サイロ化されたアイデンティティストア、IT ハイブリッド環境のシステムと統合することにより、以下を可能にします。

- アイデンティティとアクセスの一元管理によるユーザー認証
- アダプティブ認証やパスワードレス（FIDO2）方式を含む多要素認証（MFA）
- アイデンティティプロバイダーのプロキシ機能などの SSO（シングルサインオン）
- 証明書の管理

特長と利点

- サブスクリプションサービス、設備投資が不要
- ユーザーのアイデンティティ情報の管理を簡素化および一元化することで、企業のセキュリティを強化し、IT 運用の複雑さを軽減
- スケーラブルなアーキテクチャと Admin ポータルにより、容易な運用、管理、保守を実現
- クラウドベースのブローカー / プロキシ機能で複数のプロトコルをサポートしているため、複数の IdP（アイデンティティプロバイダー）戦略によるゼロトラストアクセスにも対応（図 1 の課題、図 2 のブローカー / プロキシ機能によるソリューションを参照）
- OTP や FIDO2（パスワードレス）方式などのさまざまな多要素認証をサポートしているため、アイデンティティ認証の確実な導入が可能
- アダプティブ認証と SSO（シングルサインオン）により、エンドユーザーのデジタルエクスペリエンスを簡素化し、一貫性を提供
- フォーティネット セキュリティ ファブリックとのネイティブ統合により、多くのセキュリティ制御を IT に提供
- REST API による統合が可能

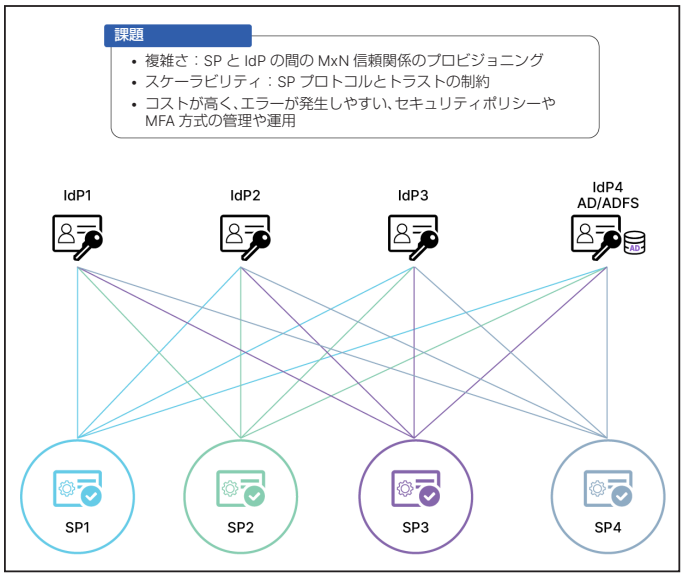

図 1：複数の IdP を使用する組織

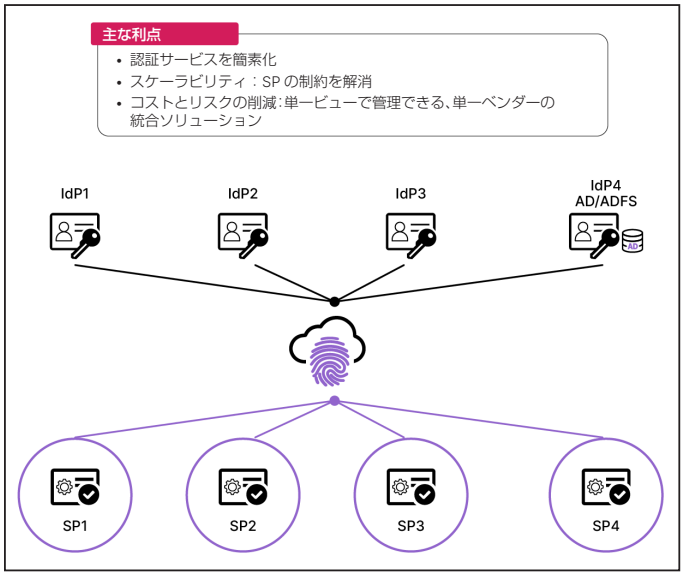

図 2：複数の外部 IdP を使用する IdP ブローカー / プロキシ

機能

高可用性 IDaaS（Identity-as-a-Service）

- フォーティネットのデータセンターでホスティング
- 24 時間 365 日体制の監視

認証サービス

FortiTrust Identity に組み込まれた認証サービスが、フォーティネットのアクセスアイデンティティ / 検証方式による従業員、パートナー、請負業者の認証を可能にし、外部の IdP とシームレスに連携する IdP ブローカー / プロキシなどの機能も提供します。FortiTrust Identity を使用することで、複数の方式を 1 つのエクスペリエンスに統合し、単一ビューでアイデンティティを管理できるようになります。FortiTrust Identity は、認証と承認の次のような業界標準をサポートしています。

- クラウド / Web タイプ：SAML、OAuth2、OIDC
- 多要素認証または強力な認証：さまざまなハードウェアフォームファクターやモバイルアプリの OTP、E メール、SMS（OTP）、FIDO2 セキュリティ。自社の環境に最適な1つ以上のファクターを選択できます。iOS と Android のデバイスでモバイルアプリケーションを使用して、クロスプラットフォームのトークン転送を保護することができます。
- アダプティブ認証は、ログイン試行時に収集した情報を使用して、そのログイン試行の状況的リスクを評価します。時間帯、位置情報、過去の使用パターンなどの情報が収集され、そのリスクが所定のしきい値を超えた場合にのみ、2 つ目の認証要素が要求されます。状況的リスクが高い場合にログイン試行をブロックすることもできます。

SSO

- SSO は、エンドユーザーエクスペリエンスを簡素化し、認証の繰り返しを少なくして、エンタープライズアプリケーションやサービスへの安全なアクセスを可能にします。

相互運用性

- FortiTrust Identity は、複数の外部 IdP でアイデンティティを管理する組織に対し、設定を必要とすることなく、IdP ブローカー / プロキシ機能を提供します。これにより、外部 IdP の認証サービスが一元化され、外部 IdP に依存することなく、ポリシーや多要素認証方式を統一できます。

統合

- フォーティネット セキュリティ ファブリック、すなわち FortiGate とのネイティブ統合により、認証サービスが拡張され、オンプレミスのリソースへの安全なユーザーアクセスが可能になります。追加のゲートウェイやソフトウェアエージェントを購入、インストール、メンテナンスする必要はありません。

証明書の管理

- 証明書の管理が効率化されることで、証明書の迅速な導入とコスト効果の向上が実現します。

技術仕様：標準サポート

- アイデンティティフェデレーション：SAML2.0、OAuth2、OIDC
- 多要素認証：OTP（ワンタイムパスワード）トークン、E メール、SMS（OTP）、FIDO2（ローミング認証器、FIDO サーバー）
- その他：証明書失効（RFC3280）、PKCS#12 証明書インポート、PKCS#10 CSR インポート（RFC2986）、オンライン証明書ステータスプロトコル（RFC2560）、SCEP（Simple Certificate Enrollment Protocol）

技術仕様：アイデンティティ

	アイデンティティ
多要素認証	
モバイルプッシュによるモバイルトークン	✓
E メール / SMS OTP、ハードウェアトークン	✓
SMS クレジット	✓
FIDO2 認証 / 登録サーバー	✓
サードパーティアプリケーションの統合	✓
アダプティブ認証	
動的ポリシーやファブリックコネクターとの統合	✓
認証されたネットワークに基づく適用	✓
ユーザーの位置情報に基づく適用	✓
時間帯 / 曜日に基づく適用	✓
デバイス態勢に基づくデバイス信頼ポリシーの適用 *	✓
クラウドでホスティングされるアイデンティティコントローラー	
セキュアアプリケーションアクセス	✓
FSSO（Fortinet Single Sign On）	✓
アイデンティティベースおよびロールベースのセキュリティポリシー	✓
ユーザーアイデンティティの集中管理	✓
証明書の管理 - VPN	✓
SAML サービスプロバイダー / アイデンティティプロバイダー Web SSO	✓
OpenID Connect の SSO	✓
その他の情報	
FortiCare プレミアムサポート	✓

* FortiClient EMS が必要

オーダー情報

USER LICENSES	SKU	Description
100-499	FC2-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 100-499 Users
500-1999	FC3-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 500-1999 Users
2000-9999	FC4-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 2000-9999 Users
10 000+	FC5-10-ACCLD-511-02-DD	Cloud-managed Identity User Subscription including 24×7 FortiCare and SMS credits for 10 000+ Users

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ