SHIELD ID

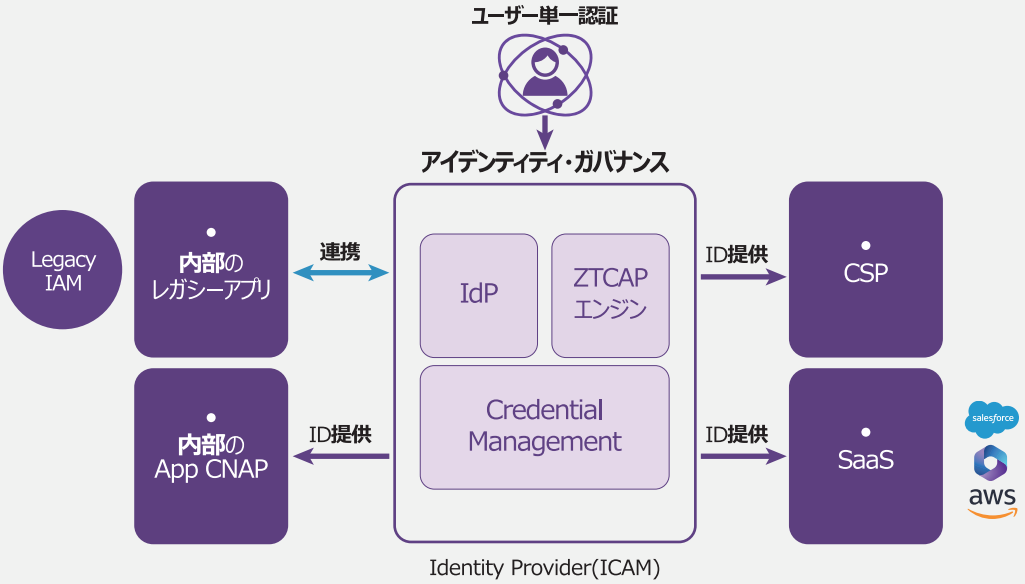
ゼロトラストベース
クラウド環境におけるアカウント管理サービス

物理的な境界がないクラウドIT環境では、いつでもどこでも認証さえ通ればアカウントの利用が可能になるため、ユーザー認証が重要な課題として浮上しています。

SHIELD IDは、ゼロトラストに基づいたユーザーの身元およびアクセス権限の管理を行い、セキュリティを維持する機能を提供します。また、Webアプリケーションに対する**SSO (Single Sign-On)**や**MFA(多要素認証)** などの認証サービスも提供します。

条件や状況に応じてユーザーの身元確認を継続して検証し、その結果に応じてアクセス権限を変更することで、認証および身元確認を中心とした**ゼロトラストのエコシステムを構築します。**

ICAM、IDPを同時に提供するゼロトラスト基盤のクラウド環境向けアカウント管理サービスです。



*IdP=Identity Provider

*ZTCAP(Zero Trust Conditional Adaptive Policy)=
すべてのアクセス行動に対して認証と権限をゼロトラストの原則に基づいて継続的に検証するポリシー

ゼロトラスト基盤の資格証明管理

多様なユーザー業務環境に応じたオンプレミス型サービスを支援し、
ユーザー／デバイス／接続位置などの検証を通じて
SaaSアクセスを安全に制御し、
条件付きアクセス制御や多要素認証などの機能をサポートします。

RBAC (ロールベースアクセス制御)に基づくユーザープロビジョニング

役割ベースのプロビジョニングにより、ユーザーのアカウントを
連携されたシステムと連動させ、新しいユーザーが登録されると、
連携されたシステムに自動でアカウントを生成します。
単なるユーザーアカウントだけでなく、システムアクセスに必要なアクセス権限まで、アカウント作成と同時に自動配布をサポートします。

SHIELD ID

IDフェデレーション (Identity Federation)に対応

ユーザーがWindows PCにログインするとクラウドサービスへも
アクセスできるように*IdPを通じたIDフェデレーションにより、
標準規約ベースのMicrosoft 365など様々なサービスと連携し
セキュリティを向上

国際標準プロトコル対応 (OAuth2、SAMLなど)

インターネットユーザーがあるサービスの資格情報を使って
他のサービスにログインできるようにするOAuth2や、
異なるドメイン間での認証や権限付与が可能なSAMLを
サポートすることで国際標準プロトコルに対応

SHIELD IDの主な特長

01 ICAMおよびIDPの同時提供

単なる認証情報（クレデンシャル）管理を超え、
先進的な認証フレームワークであるICAMと、クラウド環境における
統合認証管理を実現するIdP機能を一体的に提供します。

*ICAM = Identity Credential Access Managementによりユーザー認証管理を強化
*IdP = Identity Provider

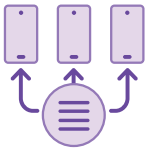
02 *SSO＆ゼロトラスト

複数のクラウドサービスへ一回のログインでアクセスできる*SSOを提供
標準規約に基づくフェデレーション（Federation）認証を通じて様々なサービスとの
連携およびセキュリティ向上、企業内のオンプレ型およびクラウドサービスに対応

*SSO(Single Sign-On) = 一回のユーザー認証で複数のアプリケーションやウェブサイトへの
ログインを許可する認証ソリューション

03 RBAC に基づくユーザープロビジョニング

社内のLDAP、AD、人事DBなどの人事情報と連携し、
役割ベースのアクセス制御（RBAC）によって、クラウドサービス利用時に
ユーザーアカウント、権限、ライセンスを自動的にプロビジョニングおよび管理します。



04 Pairwise ID 管理

ユーザーは各サービスプロバイダーから異なる固有識別子（Pairwise ID）を付与され、
個別サービス内ではユーザー識別が可能ですが、サービス間では相互連携や追跡が
不可能な方式により、ユーザーアカウントを管理します。