



i-sprint
INNOVATIONS

HAS
High Availability Systems

AccessMatrix™ USO

non-intrusive single sign-on approach

人気の高いポータルとの連携、高度なセキュリティ確保のための
HSM とのインテグレーションが可能な
エンタープライズ・パスワード・マネージメントソリューション

AccessMatrix™ Universal Sign-On (USO) は、複数のアプリケーションやシステムのソースコードを変更することなく、容易にシングルサインオン機能を提供するユーザのパスワードマネージメントを行うセキュリティ製品です。現在、多くの組織では、ユーザはたくさんの ID/パスワードを覚える必要があり、しかも定期的にパスワードを変更したり、パスワードが増加する傾向にあります。USO を導入することにより、管理コストを削減するだけでなくスタッフの生産性とユーザ満足度を向上させることが可能です。

USO の動作原理

USO は AccessMatrix セキュリティ・サーバによりも基本的な機能を提供します。ユーザにとっての利点は管理機能、監査機能、アプリケーションレベルでの承認機能を後から追加することが可能なことです。USO は、クライアントの自動インストール、自動設定、セルフサービスが有効なので、各ユーザへの導入も簡単に行え、メンテナンスにかかる手間を最小限に行えるようになります。

USO は以下のコンポーネントにより構成されています。

USO トレーナー

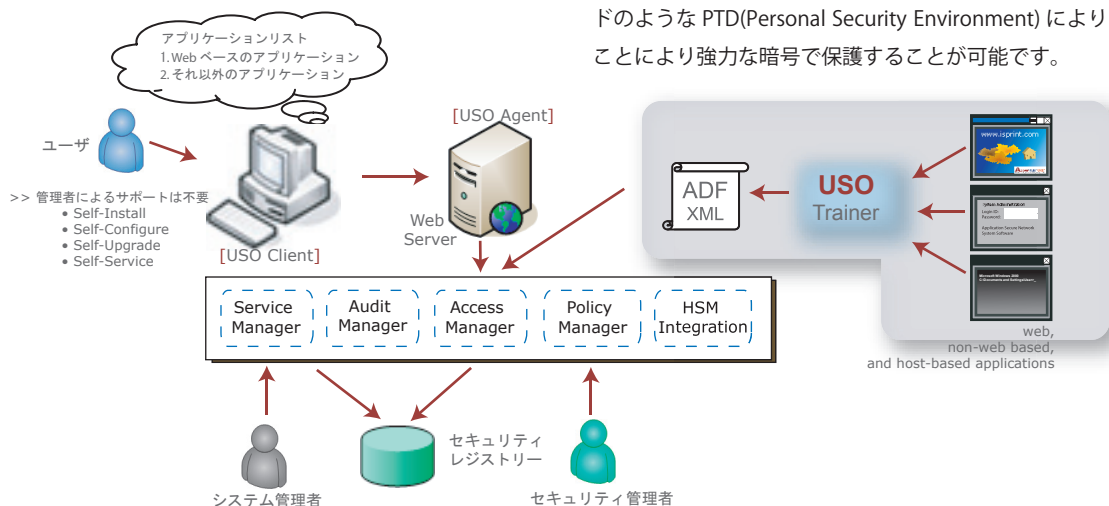
USO トレーナを利用して、ログインとパスワード変更の画面推移を対象となるアプリケーションに対して学習させます。トレーナは画面を特定する属性とセキュリティに関連するフィールドのマッピングを記憶し、ログインする時にアプリケーションに対して適切な情報を自動的に入力することを可能にします。その際にはログインやパスワード変更の自動入力の動作はアプリケーションのセキュリティ・ポリシーに添った形で行うことが可能です。トレーナーで学習する際にログインとパスワードの一連のキャプチャーされた動作を確認するためのテストを行うことも可能です。トレーナーで学習した内容はアプリケーション定義ファイル (ADF) としてエクスポートされます。管理者は ADF ファイルを AccessMatrix セキュリティ・サーバにインポートできます。

USO エージェント

USO エージェントは、セキュリティサーバへの認証時に USO クライアントとセキュリティサーバのゲートウェイのような役割を持っています。セキュリティサーバに対しての接続は暗号化され守られています。一度認証が終わると USO クライアントにユーザが使用できるアプリケーションが表示されます。

USO クライアント

USO クライアントは最初にログインしたときに自動的にダウンロードされインストールされます。USO クライアントはログイン画面を検知すると自動的にログインを行います。ユーザのログイン情報は PSE(Personal Security Environment) に保管することによりサーバと通信ができないオフライン状態のときも利用することが可能になります。PSEは 3DES や PKI 技術を利用したスマートカードのような PTD(Personal Security Environment) により暗号化することにより強力な暗号で保護することが可能です。



AccessMatrix™ Universal Sign-On (USO) の機能と特長

USO は AccessMatrix フレームワークを利用しています。USO 独自の機能に加え AccessMatrix の主要な機能を利用できます。

以下に主な USO の特長をまとめています。

簡単な導入

・シングルサインオンを実現するためにアプリケーションのログインやパスワード変更画面を学習します。アプリケーション側のソースコードを変更する必要はありません。この手法により大変簡単に USO システムへアプリケーションを統合することが可能になります。

金融レベルのセキュリティ

・主だった HSM(Hardware Security Modules) ベンダーの HSM による暗号鍵を保護します。

既存のポータルとの連携

・組織で使用されているポータルと簡単にインテグレーションが行え、USO によりシングルサインオン環境を提供します。

自動的なクライアントのインストール

・煩雑な作業無しにユーザの PC にインストールを行います。

強力な認証・簡単な管理

・USO は、メジャーなトークン・ベンダーの様々な二要素認証デバイスをサポートしています。

簡単に利用が可能

・ユーザが USO 対象のアプリケーションに最初にアクセスするときに、ユーザが USO クライアントにユーザ ID とパスワードを登録することが可能です。

安全な通信

・USO コンポーネント間の全通信は SSL を使用することにより暗号化されています。

パスワード変更を含む管理

・パスワード変更画面が表示されたときに、管理者はそれぞれのアプリケーションに対して定義されたポリシーにあうパスワードを生成させる自動パスワード変更オプションを選択できます。マニュアルパスワード変更の場合は、ユーザにパスワードを入力させることにより対応します。対象となるアプリケーションと USO のデータベースでパスワードの同期が取れていない場合はユーザが登録されているパスワードをリセットすることが可能です。

モビリティ

・USO の PSE (Personal Security Environment) 機能やハードウェアトークンによりユーザのログイン情報やアプリケーション属性を保管することが可能です。この機能によりユーザが USO サーバに接続していなくても、シングルサインオン機能を利用することが可能です。

セキュリティ機能のアップグレード

・より統合され、高度なアクセスコントロールを実現したい場合 UAM と組み合わせることが可能です。AccessMatrix セキュリティサーバに UAM を組み込むことで管理の一元化を実現しています。

AccessMatrix™ について

AccessMatrix™ は i-Sprint 社の特許である階層モデルテクノロジー (Hierarchy Model technology (PCT/SG02/00027)) をベースにしています。USO は共通フレームワークである AccessMatrix 上で動作します。USO は AccessMatrix セキュリティ・サーバにある基本的な機能を利用し、さらに他の製品と組み合わせることも可能です。AccessMatrix はユーザが web やアプリケーションサーバなどの複数のイーコマースや企業内システムに対して集中的に認証、承認、監査サービスを提供します。管理者が簡単にしかも効率的にアプリケーションへのアクセス許可、ユーザ権限、セキュリティポリシーを組織全体にたいして管理するために、一元的かつ包括的なポリシー管理サービスを提供します。

簡単なユーザ管理

AccessMatrix の階層モデルにより、組織のレベルごとに管理者を分担させることが可能です。管理者の役割を分担させることで、セキュリティをより高め、セキュリティ管理者を分散させ、高いレベルでのアカウントバリティ (説明責任) を実現します。たとえば社内だけでなくビジネスパートナーがもつユーザの ID や権限を、ビジネスパートナー自身が管理するといったことも可能です。ユーザ情報は、既存のレジストリー例えば LDAP や Microsoft Active Directory を利用することが可能です。

大規模組織における簡略化した

セキュリティポリシーの拡張

全社的なセキュリティポリシーを実際の組織構造にあわせて階層的に定義し、管理することが可能です。組織全体のセキュリティポリシーの実施を一元的に行うことが可能です。

グローバルバンクでも必要な「ベストなセキュリティを 実践」するための管理機能をサポート

AccessMatrix はデュアルコントロールにより、各管理者の権限を最小限にし、責任範囲を明確にします。このような機能は金融業界をはじめその他の業種においても重要です。セキュリティ管理者の組織内の役割に適切な権限にあわせてきめ細かく管理者権限を割り当てることができません。設定者一確認者またはデュアルコントロールにより、ある一人の管理者が設定変更をした場合、他の管理者によって確認と承認を得た後でないと変更が有効にならないようになっています。さらに AccessMatrix は同一アプリケーション権限についてはユーザは複数のロールを設定することができません。これは設定の複雑さによるミスを防ぐためのものです。アプリケーションごとにアプリケーションに適切なロールを定義することが可能です。

JAVA 実装により、拡張性とプラットフォームに依存しない コストパフォーマンスが高いソリューション

AccessMatrix セキュリティサーバは Java テクノロジーと標準規格を使用しているため、Java Run-time 環境が動作するプラットフォームで利用することが可能です。

株式会社ハイ・アベイラビリティ・システムズ
ソリューション&コンサルティング事業部



〒108-0023
東京都港区芝浦4-13-23 MS芝浦ビル2F
TEL 03-5730-8870 FAX 03-5730-8619
email inquiry@ha-sys.co.jp
URL http://www.ha-sys.co.jp