社員証ICカードで実現する エンタープライズ・シングル・サインオン

基盤第２ソリューション部　第５ソリューション室
シニアITスペシャリスト　平田　義和

1. エンタープライズ・シングル・サインオンの必要性

1.1. ユーザID・パスワード管理に関する悩み

IDとパスワードの管理において、コスト面、セキュリティ面、法令面での問題が顕在化しており、これら問題を解決するためにSSO（Single Sign-On）ソリューションが再び脚光を浴びている。

アプリは、通常、ユーザを識別、認証するために、個別にIDとパスワードを管理し、個別にユーザの認証を行っている。SSOは、このユーザの識別・認証を一元化し、IDとパスワードを１度入力するだけで、各アプリを利用できるようにする機能である。

1.2. エンタープライズSSOの登場

SSOソリューションは、WebアプリへのSSOに特化したリバースプロキシ型のものが一般的であるが、最近では、エンタープライズSSOという新しいタイプのSSOソリューションが登場している。

エンタープライズSSOは、PCにクライアントモジュールを導入し、利用者に代わって認証画面に IDとパスワードを自動的に代行入力する仕組みである。利用者がSSO対象のアプリを起動すると、SSOシステムが認証画面を検知して事前に設定されたアプリ認証情報（ID、パスワードなど）を認証画面に入力し、アプリへのログオンを行う。

エンタープライズSSOには、リバースプロキシ型SSOに比べ以下のようなメリットがある。

- Webアプリ、Windows®アプリ、Java®アプリなど、広範なアプリをサポートする。
- ICカードなど高度認証との親和性が高く、より一層のセキュリティ強化ができる。
- アクセス履歴の集中管理とレポート化により、ユーザアクセスの可視化ができる。

2. TAM E-SSOの紹介

TAM E-SSO（Tivoli® Access Manager for Enterprise Single Sign-On）は、パスワードを一元管理するエンタープライズSSOソリューションを提供する。TAM E-SSOは、アプリケーションプロファイル（ログオン画面の検知と自動ログオンを実行するための定義）を作成するための環境が充実しており、広範囲のアプリを効率的にSSO化できる。また、PCの共用使用において、複数人が使用することで生じるセキュリティ上の問題を、現行運用に大きな影響を与えることなく解決する。ユーザ認証時の監査ログだけでなく、ユーザ追加、パスワードリセット等の管理業務の監査ログを取得する機能も備える。

TAM E-SSOは、クライアントPCで稼働する「AccessAgent」、各種設定情報を管理する「TAM E-SSOサーバ」、アプリケーションプロファイルを作成する「AccessStudio」の３つのコンポーネントで構成される（図１）。

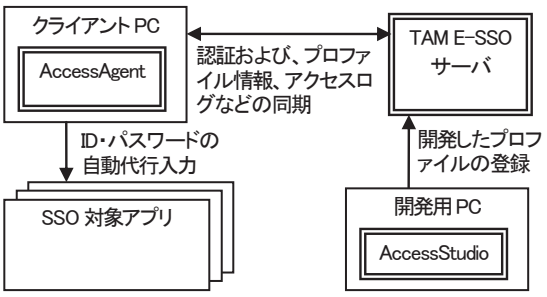

図１　TAM E-SSOの構成

3. エクサのソリューション

3.1. 社員証ICカードによるエンタープライズSSOソリューション

TAM E-SSOの環境では、クライアントPCの起動後にTAM E-SSOサーバへID、パスワードによるログオンを行えば、その後はWindowsログオンを含め対象アプリのログオン操作は全て自動化される。このため、TAM E-SSOサーバの認証強度は重要である。

TAM E-SSOは、ID、パスワードによる認証に加え、ICカードやUSBトークンなどの高強度認証デバイスをサポートする。モノと秘密情報による２要素認証を実現することで、よりセキュリティレベルの高い認証を実現可能とする。

エクサでは、社員証で広く普及しているFeliCaカードと、TAM E-SSOの認証を連携し、高強度認証と利便性向上を実現するソリューションを開発中である（2010年9月時点）。

このソリューションでは、TAM E-SSOとFeliCaカードドライバの間で稼働するミドルウェア（ICカード認証モジュール）を提供予定である。

利用者がPCに接続されたカードリーダに社員証ICカードをかざす(タップする)と、AccessAgentは、このミドルウェアを介して、カードからユーザ情報を取り出し、PCのログオン画面にユーザIDを自動入力する。利用者は、TAM E-SSOのパスワードのみを入力してPCにログオンする（図２）。

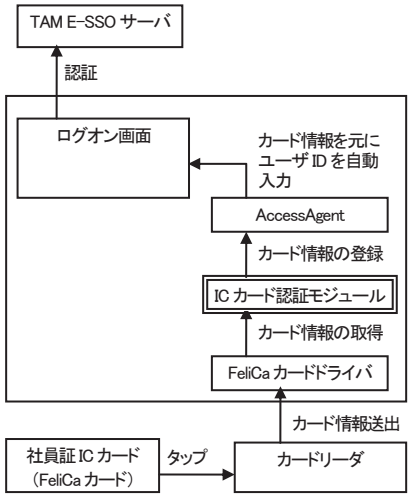

図２　社員証ICカードによる認証の仕組み

3.2. TAM E-SSO導入サービスパッケージ

TAM E-SSO導入サービスパッケージ(表１)は、予め設計済みの標準的な機能仕様でTAM E-SSOシステムを導入するサービスである。短期間・低コストでエンタープライズSSOを実現する。

事前に接続対象を調査(簡易ヒアリング)して、導入パッケージの適用可否を判断した後、約３ヶ月間でTAM E-SSOシステムを構築する。お客様は、このTAM E-SSOシステムに対し、順次接続対象アプリを拡大していくことが可能である。

表１　TAM E-SSO導入サービスパッケージの内容

項目	パッケージ内容
ユーザ認証	ID・パスワード認証のみ(ICカード認証等はオプション)
TAM E-SSO サーバ構成	1台構成（複数台の構成はオプション）
E-SSO対象数	1000台程度のクライアントPC。接続対象は３アプリまで。画面数は６画面
端末形態	共有端末または個人端末のどちらか1つを選択
Active Directory 連携	Active Directoryとの連携はオプション
監査ログ	TAM E-SSOおよび対象アプリへのログオンのログを取得
ユーザ一括登録	ユーザ情報を一括登録するバッチプログラムはオプション
ランダムパスワード自動入力	対象アプリに対し、TAM E-SSOがランダムパスワードを生成して代行入力する機能はオプション

※パッケージの仕様外の要件は、別途見積で対応可能。

4. おわりに

昨今のセキュリティ規制やテクノロジーの進化により、社員証ICカードによる入退出管理などの物理セキュリティは広く普及してきている。一方、エンタープライズSSOはこれからの新しいソリューションであり、注目度が高い。

エクサの提供するICカードによるE-SSOソリューションとTAM E-SSO導入パッケージの組み合わせは、利便性、コストを兼ね備えながらセキュリティを向上する優れたソリューションであると確信している。
