

# SecureVisit

## USBトークン／OTPトークンを利用したWeb認証強化ソリューション

- リバースプロキシ/チャレンジ&レスポンス認証による強力なセキュリティ
- 既存のWeb環境を変更する事なくUSBトークンによる認証を実現
- OTPトークンを利用することによりスマートフォン/タブレットPCへの対応も可能



### USBトークンを利用したWeb認証／リバースプロキシサーバー

SecureVisitはUSBトークン「ePass1000ND」を利用した強力なチャレンジ&レスポンス認証・リバースプロキシ機能を搭載するWeb認証システムです。既存のWeb環境を変更せずに、USBトークンによる認証機能を実現します。

#### 製品特長

### SecureVisitを利用する3つのメリット

#### 高い安全性

USBトークンと認証サーバー間はチャレンジ&レスポンス認証方式を採用し、ID/パスワード認証より強力なセキュリティを実現しています。また、SSLもサポートし、暗号化通信も可能です。

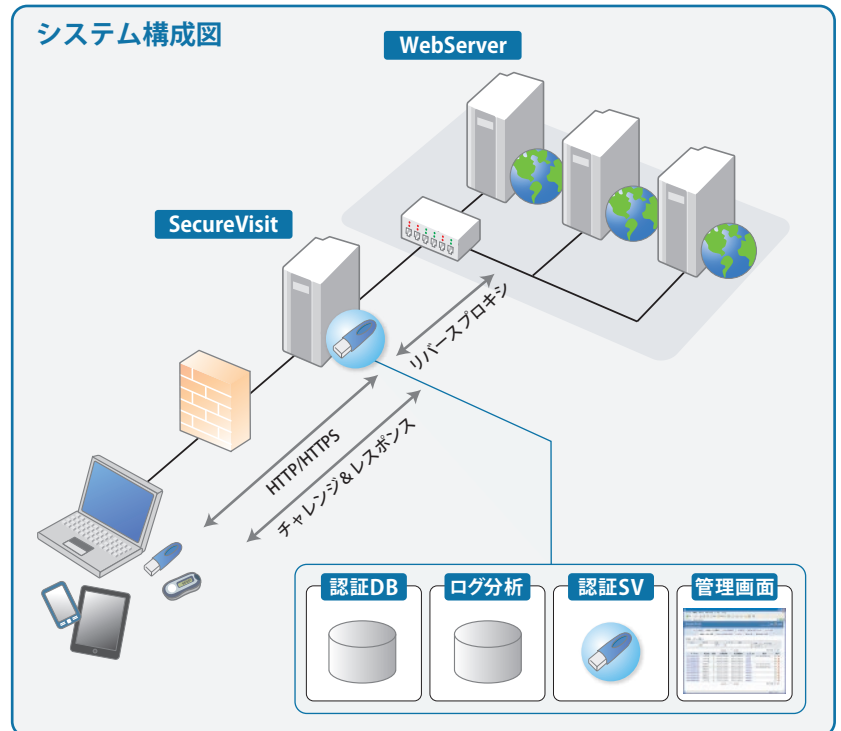
#### 低価格

SecureVisit認証サーバーおよびUSBトークンは、低価格でコストパフォーマンスに優れています。小規模はもとより、大規模ユーザー拠点でも安心して導入できます。

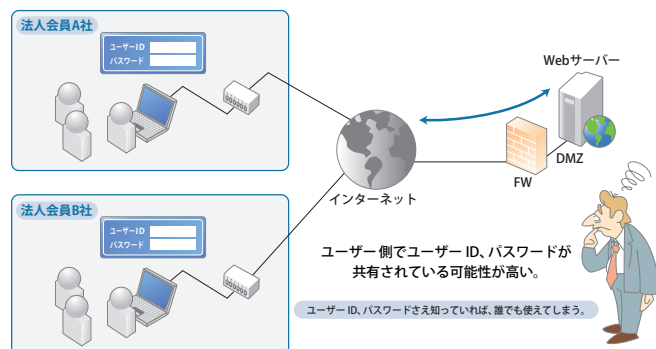
#### 高い利便性

USBトークンePass1000NDを利用すると、クライアント側では初回アクセス時にActiveXをダウンロードすることで利用できるようになります。既存システムに対し容易にUSBトークン認証を付加できます。

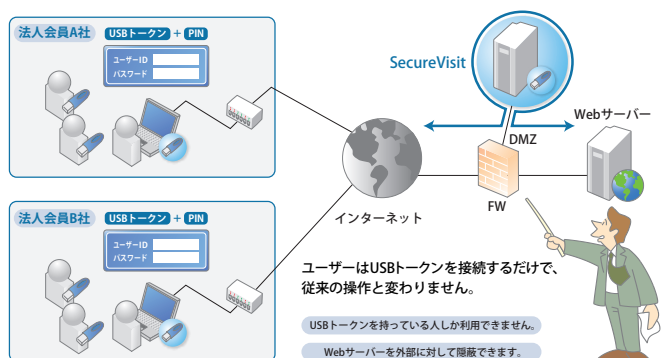
#### システム構成図



このようなお客様に最適です。 法人会員向けWebサービスをユーザーID、パスワードのみで管理している

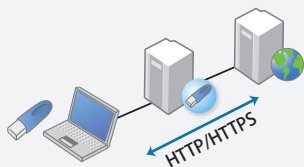


SecureVisit 導入後 従来の運用形態を変えず、USBトークン認証を付加できます



## SecureVisitの機能

### リバースプロキシ



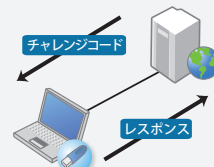
SecureVisitサーバーはリバースプロキシサーバーとして動作し、すべてのリクエストを中継するので既存Webサーバーの設定、コンテンツを変更する必要がなく、既存の認証方式から容易にUSBトークンを利用した認証方式に移行できます。また、クライアント側からみると透過的で、ユーザーはSecureVisitを意識する必要がありません。

### アクセスコントロール



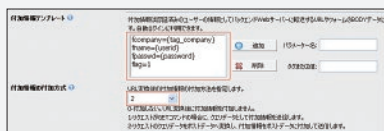
SecureVisitでは転送先URLへのアクセス拒否/許可をユーザーグループ毎に制御する事が可能です。また、許可リスト/拒否リストで特定のIPアドレスからのアクセスの許可/拒否も制御できます。転送先に指定するWebサーバーは複数のサーバーを指定できます。

### チャレンジ&レスポンス認証



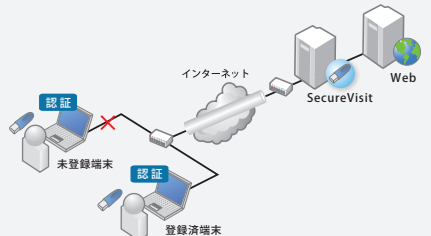
SecureVisitではサーバーから送られてくるデータを元にハッシュ値を生成し、送信する「チャレンジ&レスポンス認証」を採用しています。

### パラメータ転送機能



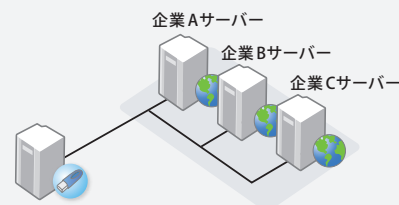
SecureVisitの付加情報転送機能は、クライアントからのHTTP(S)リクエストに認証情報を付加してバックエンドのWebサーバーに転送する機能です。パラメータ転送機能を利用すればID、パスワード等の入力を省略することも可能です。

### 端末認証



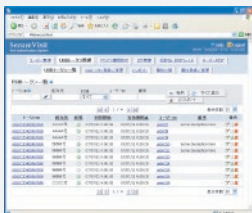
SecureVisit 端末認証機能は、既存のUSBトークン認証の上で、端末のMACアドレスによる認証を付加します。

### マルチドメイン



1つのSecureVisitシステムに複数のドメインを登録することができます。また、SecureVisitは1つのシステム環境で複数のシステムを共同で利用できるマルチテナントにも対応しています。

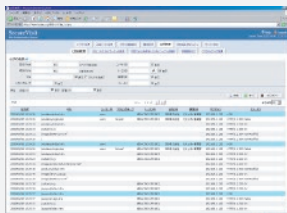
### Web 管理画面



■ SecureVisitのWeb管理画面

管理画面では、ユーザーの登録/削除、USBトークンの発行/削除、USBトークンとユーザーの関連付けから各コンテンツに対してアクセスコントロールの設定を行います。また、ログ内容の確認/検索や各種設定情報のバックアップなども行えます。

### ログ&レポート



認証サーバー経由で行ったリクエストの様々なログを記録しています。保存されているログは管理画面から検索でき、レポート機能を利用することでグラフ表示でアクセスログの検索、分析ができます。

### ePass1000ND/OTP



クライアント側はePass1000ND/OTPを使用します。クライアントプログラムはActiveXで提供され、SecureVisit初回アクセス時に自動的にダウンロードします。

## 製品仕様

### ■ サーバー動作環境

サポートOS (※1)	Red Hat Enterprise Linux ES5, ES6 CentOS 5, 6
CPU	Celeron 1.7GHz以上 (2GHz以上推奨)
メモリ	1GB以上
ハードディスク	50GB以上
ネットワーク	Ethernet

### ■ クライアントおよび管理コンソール動作環境

サポートOS (※1)	Windows 2000 Professional SP4 Windows Vista, XP, 7, 8/8.1, 10 (32/64bit)
ブラウザ	Internet Explorer 6.0以上 (ActiveX/JavaScript/Cookieが有効であること) また、Microsoft Edge、Chrome等他のブラウザには対応しておりません。
その他	USB 1.1 / 2.0 空きポート1つ以上

### ■ 製品仕様/対応機器

認証	チャレンジ&レスポンス (MD5:128bit)
セキュリティ強度	SSL Ver.3.0 (128bit) HTTPS使用時
対応デバイス	ePass1000ND USBトークン / OTPトークン

●「SecureVisit」は飛天ジャパン株式会社の登録商標です。

(※1) 対応OSのバージョンについては、お問い合わせ下さい。