『SecureVisit』製品概要

～USBトークンを利用したWeb認証/リバースプロキシサーバ～

飛天ジャパン株式会社

目次

はじめに

現在主流のID/パスワードだけの認証では守れない脅威(ID/パスワードの不正流出などによるなりすまし)があります。

現状

- 企業が主に行っている対策
  - ユーザIDの管理
  - 社外からのアクセス制限
  - 定期的なパスワード変更

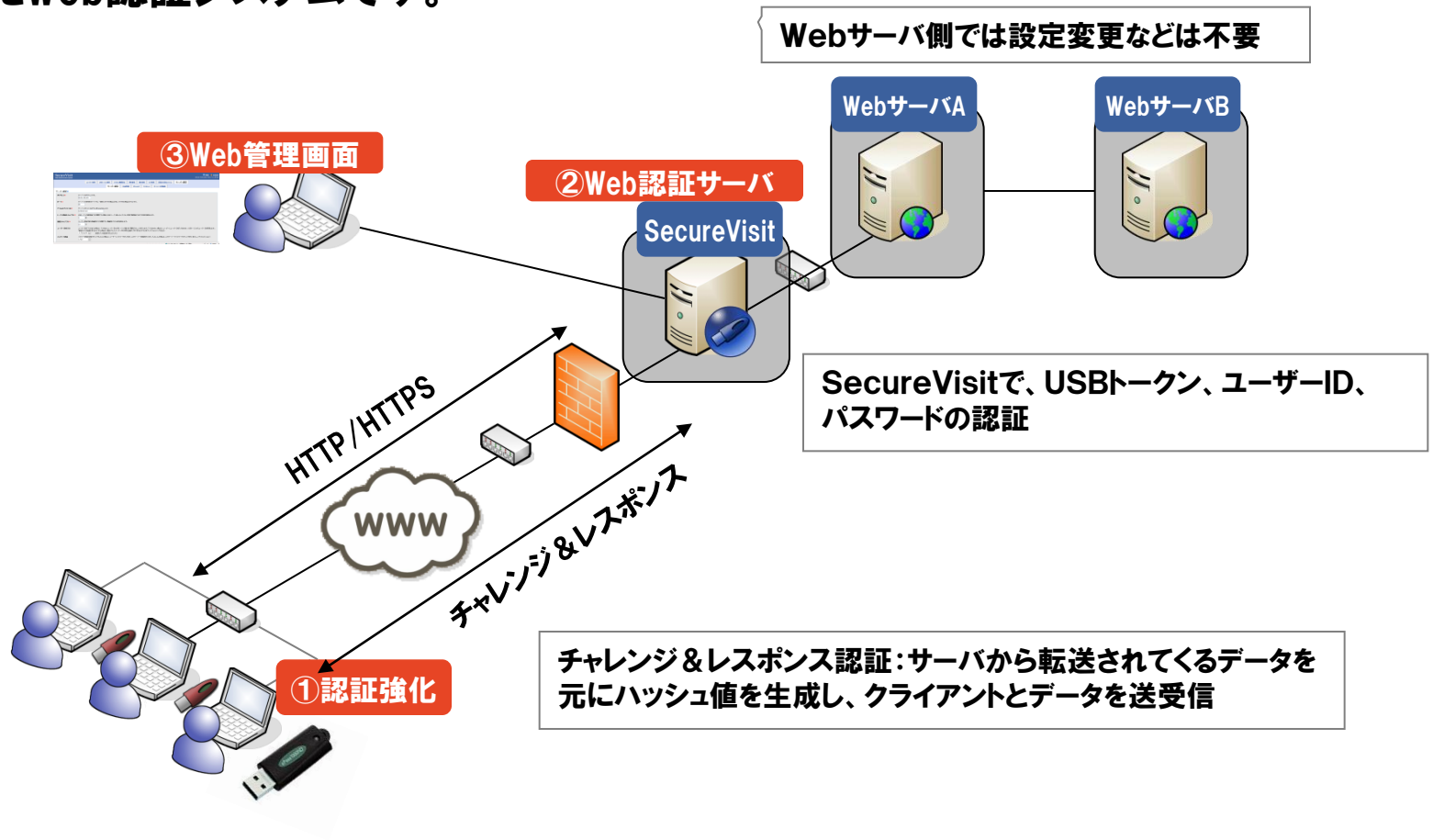
ご提案

- Webシステムへのログインは、ID/パスワードだけの認証に加え、2番目の認証を付加し、セキュリティの強化を実現します

SecureVisitは、USBトークンを利用することで2要素認証を実現します。

1. SecureVisitとは

USBトークン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したWeb認証システムです。



1-1. SecureVisitの基本機能

二要素認証、アクセスコントロールを容易に設定がおこなえる**リバースプロキシサーバ**です。

①二要認証

- ID、パスワードに加えてUSBトークンによるWeb認証システム
- チャレンジ＆レスポンス認証

（オプション：OTPトークンでスマートフォン/タブレットPC対応）

②Web認証サーバ

- リバースプロキシ機能
- IPアドレス/MACアドレスによる端末認証
- マルチドメイン登録、パラメータ転送機能

③Web管理画面

- IT管理者にとって操作性の良いGUIインターフェースです
  - ユーザの管理、トークンの管理、ログ情報の管理
  - アクセス制限の管理

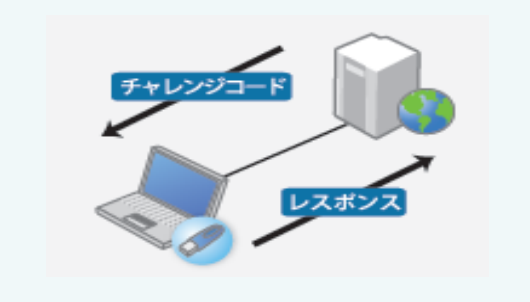
1-2. USBトークンの役割

クライアント側はUSBトークン(ePass1000ND/ePass1000)を使用します。クライアントプログラムは認証サーバからActiveXで提供され、SecureVisit初回アクセス時にダウンロードします。※ワンタイムパスワードc200トークンも使用できます。

ePass1000ND(※ドライバレスUSBトークン)

チャレンジ＆レスポンス認証を使用し、ユーザー識別することにより、固定パスワードより強固な二要素認証を実現します。

チャレンジ＆レスポンス認証(※)



※サーバから転送されてくるデータを元にハッシュ値を生成し、クライアントとデータの送受信を行う。

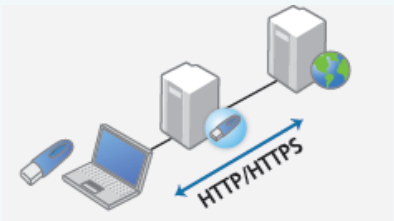
OTP c200(タイムベース型ワンタイムパスワードトークン)

60秒毎にパスワードを生成します。

1-3. SecureVisitの機能概要

SecureVisitは**リバースプロキシ、アクセスコントロール、チャレンジ＆レスポンス認証など**
を含め主に9つの機能を持っています。

①リバースプロキシ

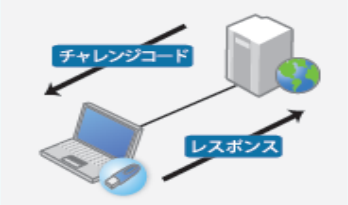


SecureVisit は既存のWebアプリケーションやシステムを変更せずに、USBトークンによる認証を追加できることを目的としたたシステムです。認証サーバは保護するWebサーバの前に置かれ、Webサーバの代りに利用者からのアクセスを受け、認証したうえで保護するWebサーバにそのアクセスをパスします。その結果、保護するWebサーバは認証サーバからのアクセスのみを受けます。SecureVisit は HTTP/HTTPSプロトコルをサポートします。

②アクセスコントロール

SecureVisit認証サーバには、「ユーザ」、「アクセスグループ」という概念があります。
「ユーザ」:SecureVisit Web認証システムにおける利用者のことです。「ユーザ」は「ユーザID」で識別します。
「アクセスグループ」:はアクセス権限を制御するための「ユーザ」グループのことです。「ユーザ」は最低一つの「アクセスグループ」に所属します。Webサーバのコンテンツ毎にアクセスできるアクセスグループを設定できます。

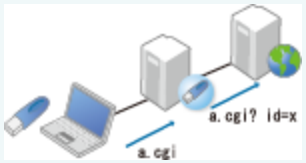
③チャレンジ＆レスポンス認証



SecureVisitが採用している認証方式です。USBトークンと認証サーバ間でセキュアな認証を行います。
認証サーバから送られてくるデータ(チャレンジ)を元にクライアントが持っているシークレットを組み合わせて演算し、ハッシュ値を認証サーバーに「レスポンス」として返すことにより認証を行う方式です。
チャレンジ:認証サーバが乱数から作り出したデータで認証時にクライアントへ送信します。
レスポンス:クライアントがシークレットとチャレンジを組み合わせ、ハッシュ値としてサーバへ返すデータです。ハッシュ値:ハッシュ関数により生成される値で、計算結果から元のデータへ戻すことができない不可逆な値です。

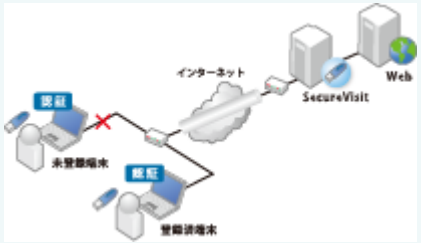
1-3. SecureVisitの機能概要(続)

④パラメータ転送



パラメータ転送機能は、指定されたURLにアクセスし認証後、バックエンドWebサーバに転送する際、HTTP(S)リクエストに指定された情報を付加して転送する機能です。
パラメータ情報は、認証サーバにおけるユーザIDやパスワード情報以外に、管理者によって任意に定義することができます。ユーザ毎に識別する情報に紐ついた異なる情報も付加することができます。
ユーザID/パスワードの入力フォームを持つ既存のWebシステムにSecureVisitを導入し、個の機能を用いるとトークン認証後にユーザID/パスワードの入力を省略することも可能です。

⑤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。端末認証機能を導入する前は、USBトークンを利用すれば、どの端末からも認証することができます。端末認証機能導入の際には、管理者が、ユーザに端末登録許可情報を送り、ユーザが端末登録をSecureVisitに対して行うことで端末制限の認証を実現します。また、管理者はWeb管理画面によっていつでも端末認証機能を変更することが可能です。

⑥マルチドメイン

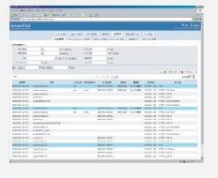
1つのSecureVisitシステムに複数のドメインを登録することができます。また、SecureVisitは1つのシステム環境で複数のシステムを共同で利用できるマルチテナントにも対応しています。

1-3. SecureVisitの機能概要(続)

⑦Web管理画面

Web認証システムではほとんどの管理作業をWeb管理画面から行う事ができます。管理者はWeb管理画面へアクセスする事で、ユーザーの登録/削除、USBトークンの登録/削除およびログ管理などを行う事ができます。
Web管理画面から実行できる主な機能:ユーザー管理、USBトークン管理、アクセス権限設定、属性管理、ログ管理、認証DB・設定ファイル管理

⑧ログ&レポート



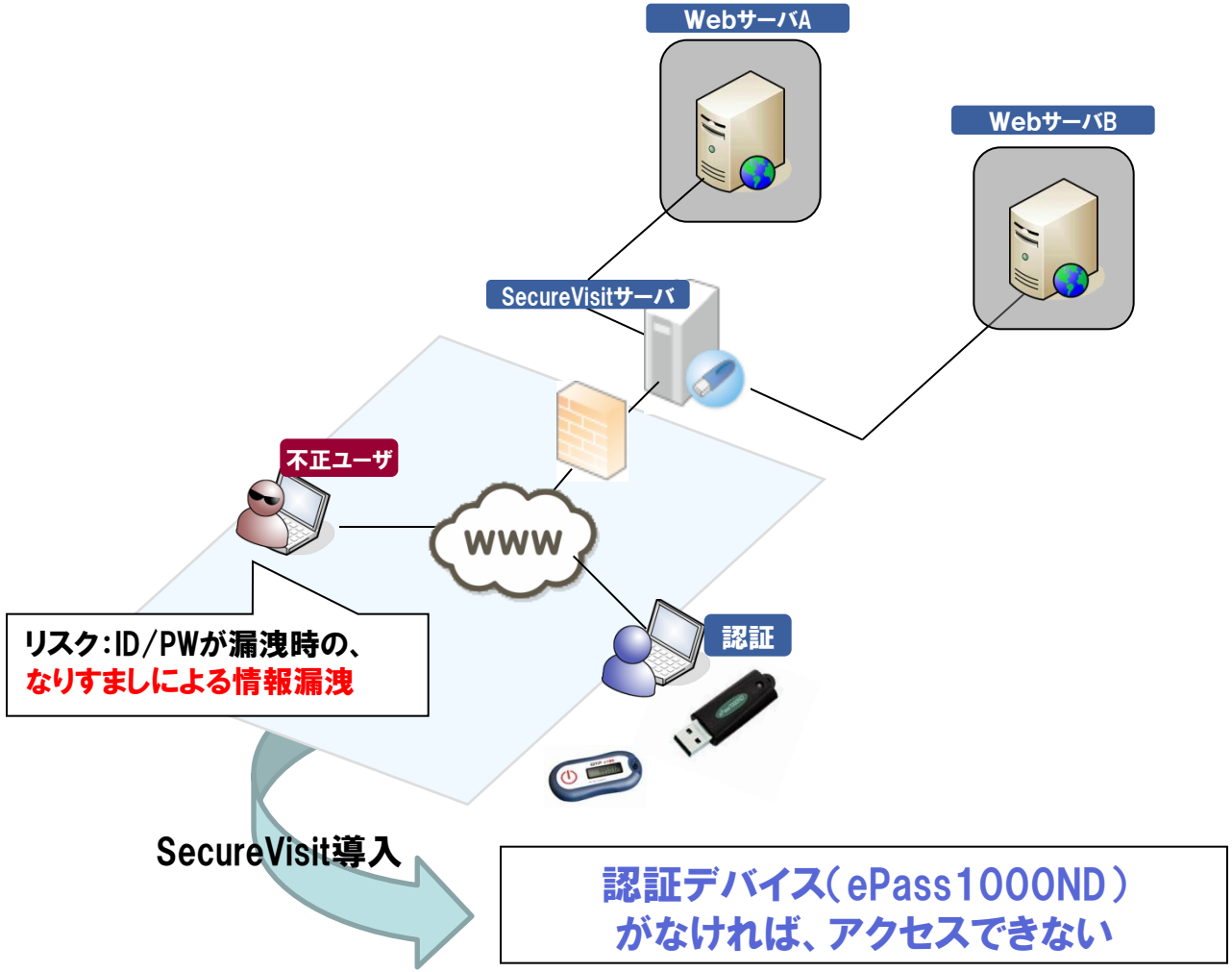
ログ管理ではSecureVisit が記録したログの内容を検索・表示する事ができます。ログの検索は、日付、URL、アクセスグループ、ユーザーID、トークンID などさまざまな条件から検索が行えます。また、検索結果をCSV ファイルとしてエクスポートする事もできます。

⑨USB/OTPトークン認証

クライアント側はUSBトークン ePass1000NDを使用します。クラインとプログラムはActivX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。また、飛天OTP認証システム(FOAS)との連携でワンタイムパスワードトークンを使用しての認証も可能になります。

2. 導入イメージ

SecureVisitを導入する事により、既存Webシステムの変更なしに、セキュリティに関する懸念事項を解決できます。



3. 特徴

SecureVisitが持つ特徴により多くのユーザ様にご利用されております。

- 特徴
  1. 既存システムに改造を加えず二要素認証強化が容易に実現可能
  2. システム管理者にとって導入、運用しやすいシステム構成
  3. 端末制御も可能なため登録端末からしかアクセスさせない事も可能
  4. 利用者の従来の運用形態を踏襲しつつUSBトークン認証を行うことが可能
  5. 電子証明書を使用しない為、初期導入費用、ランニングコストの節約

- 実績
  1. 大手空港情報関連企業、大手教育関連企業、建設関連企業、データセンター、ASPサービス企業様など幅広く導入

4. 定価

FEITIAN WE BUILD SECURITY

お見積りに関しては、小ロット(25～)も含め柔軟に対応させていただきます。

100ライセンスの概算

必要製品群	製品名	数量	定価金額(税抜)
認証サーバクライアントライセンス(ソフトウェア)	SecureVisit	1セット	756,000円
USBトークン(ドライバレス)	ePass1000ND USBトークン	100個	310,000円
保守費用	年間保守費用	1式	120,000円
		合計	1,186,000円
※SecureVisit用サーバのハードウェアはユーザ様ご用意(既存Webサーバとの共存も可能)			

※価格は導入条件やロット数などで変わってきますので詳細はお問い合わせください

・SecureVisit認証サーバのインストレーションは飛天ジャパンで無償でおこないます。
・他システムとの連携についても柔軟に対応します。(要相談)

参考資料

A-1. 他社比較

FEITIAN WE BUILD SECURITY

飛天ジャパンのSecureVisitは2要素認証を含め他社にないアクセス制御機能や柔軟な販売価格でご提供します。

SecureVisitと他社認証システムとの比較

企業名 製品名	認証 デバイス	認証技術	SSO対応	端末毎のアクセス制限	IPアドレスによるアクセス制限	価格
飛天ジャパン 『SecureVisit』	USBトークン OTPトークン	チャレンジ＆ レスポンス方式	SAML対応	○	○	33万/25ライセンス
A社 認証システム	USBトークン	-	×	×	×	200万/ライセンス無制限
B社 認証システム	なし	チャレンジ＆ レスポンス方式	SAML対応	×	×	200万～

※SSO対応に関してはSecureVisit2.0より対応いたします。

A-2. 製品仕様

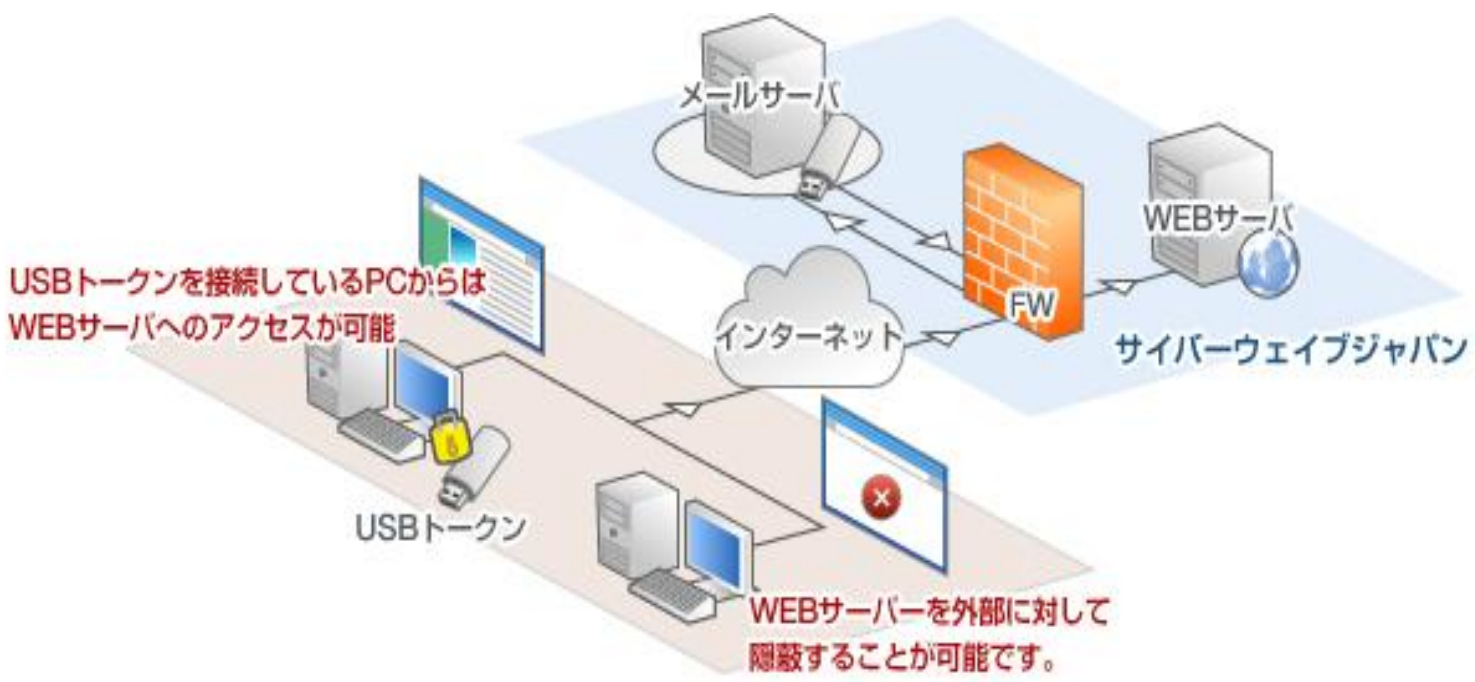
SecureVisitサーバ	
対応OS	RedHat Enterprize Linux ES4/ES5 CentOS4/5
CPU	Celeron 1.7GHz以上
メモリ	1GB以上
ハードディスク	50GB以上
ネットワーク	Ethernet

管理コンソール	
対応OS	Windows 7
	Windows Vista SP1/SP2
	Windows XP SP1/SP2
	Windows 2000 Professional SP4
ブラウザ	IE6以上（32bit)（ActiveXが実行できること）
その他	USB1.1/2.0 空きポート2つ以上

クライアント	
対応OS	Windows 7
	Windows Vista SP1/SP2
	Windows XP SP1/SP2
	Windows 2000 Professional SP4
ブラウザ	IE6以上（32bit)（ActiveXが実行できること）
その他	USB1.1/2.0 空きポート2つ以上

データセンターで運用しているWebサーバの接続の認証を強化するためにSecureVisitを導入した事例

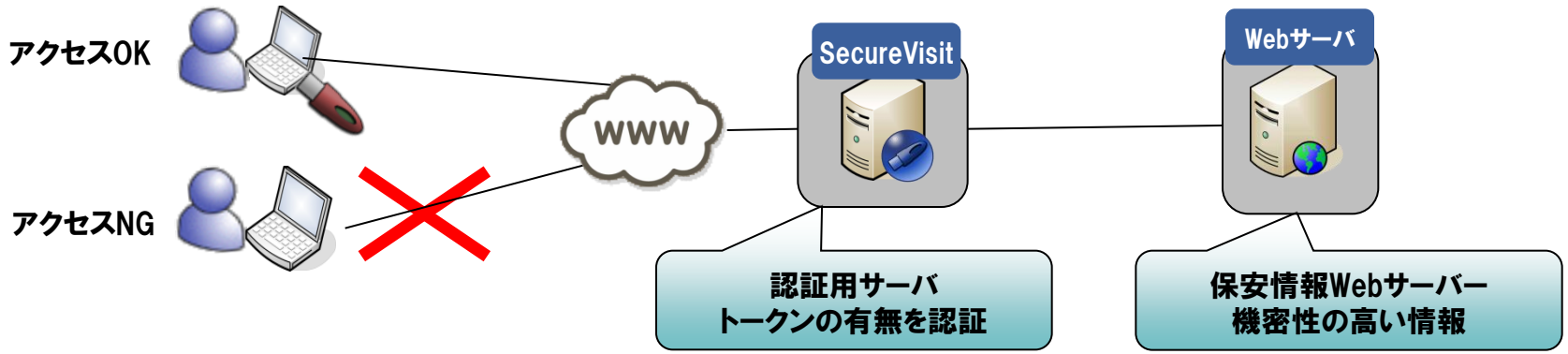
- データセンターで運用するグループウェアの認証を強化したいというエンドユーザ様のご要望にUSBトークンを用いて認証を強化する「SecureVisit」をご採用いただきました。



FEITIAN WE BUILD SECURITY

某保安センター様への導入事例

- 目的：
  1. 機密性の高い情報を扱うWebサイトを運営する際、会員にセキュアな通信を提供する。
- 課題：
  1. 非常に機密性の高い情報の為、外部への情報漏洩があってはならない。
- 導入効果：
  - セキュリティ向上により信頼性が向上した。
  - USBトークンの利用により、利用者の利便性が向上した。
  - 非常に管理しやすいシステムの為、管理コストの低減に繋がった。

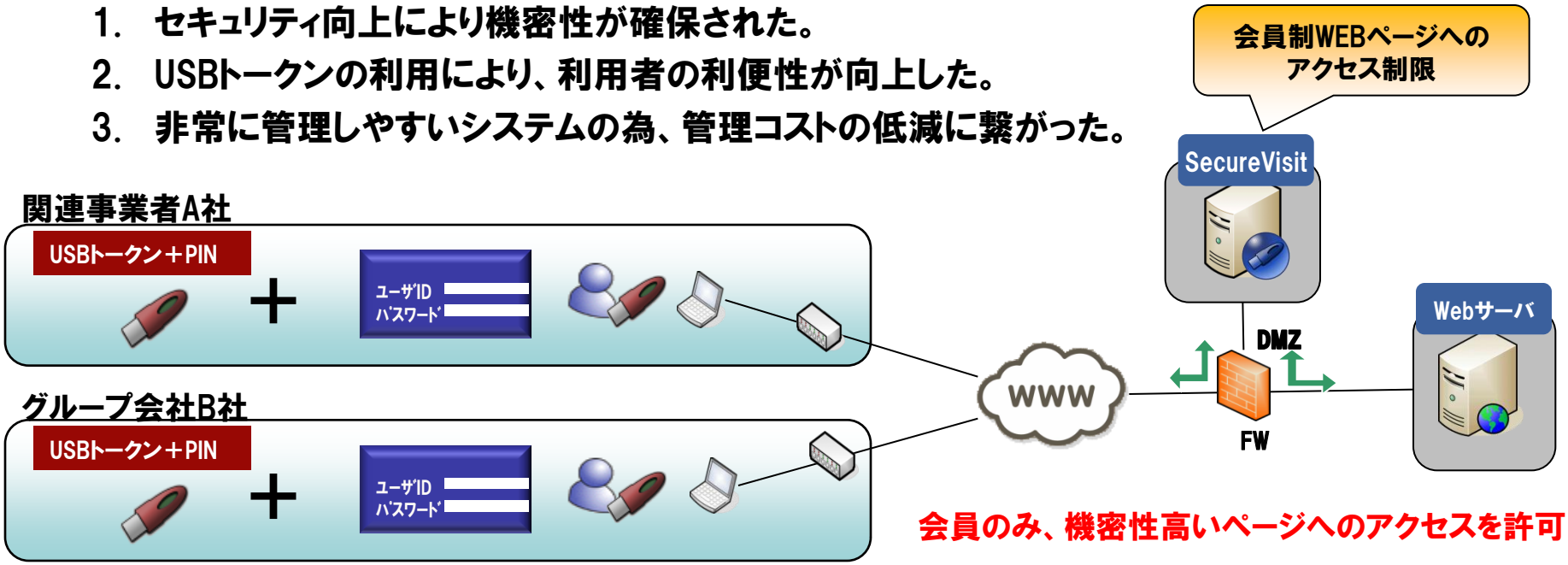


二要素認証にて、強固なセキュリティを実現

FEITIAN WE BUILD SECURITY

某大手衛生TV局様

- 目的：
  1. 関連事業者またはグループ会社と機密性の高い情報を共用する。
- 課題：
  1. 外部へ情報漏洩し、不正に利用されると企業機密漏洩、信用低下に繋がる。
- 導入効果：
  1. セキュリティ向上により機密性が確保された。
  2. USBトークンの利用により、利用者の利便性が向上した。
  3. 非常に管理しやすいシステムの為、管理コストの低減に繋がった。

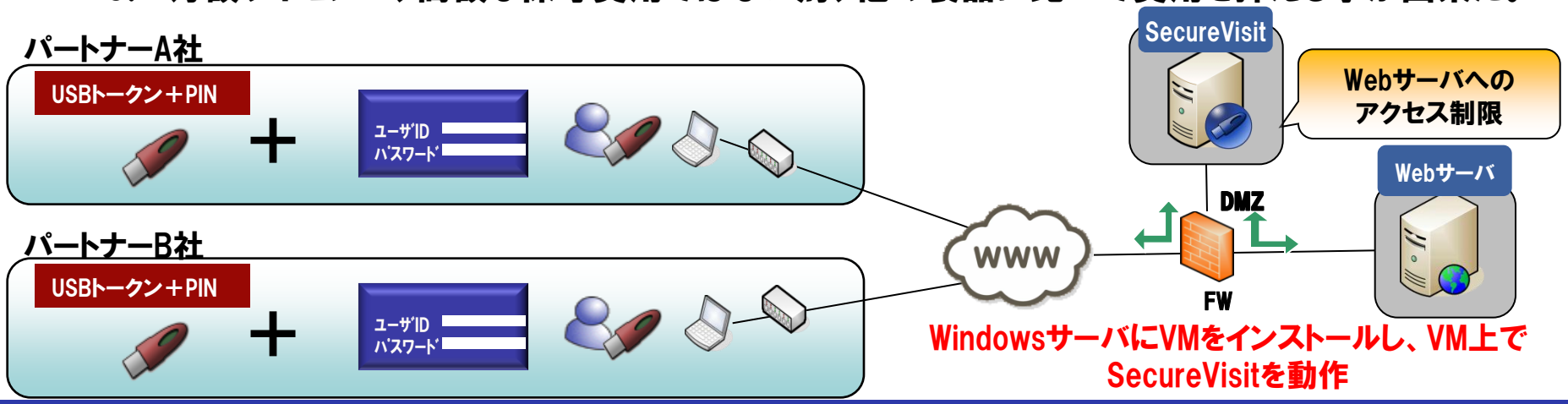


会員のみ、機密性高いページへのアクセスを許可

FEITIAN WE BUILD SECURITY

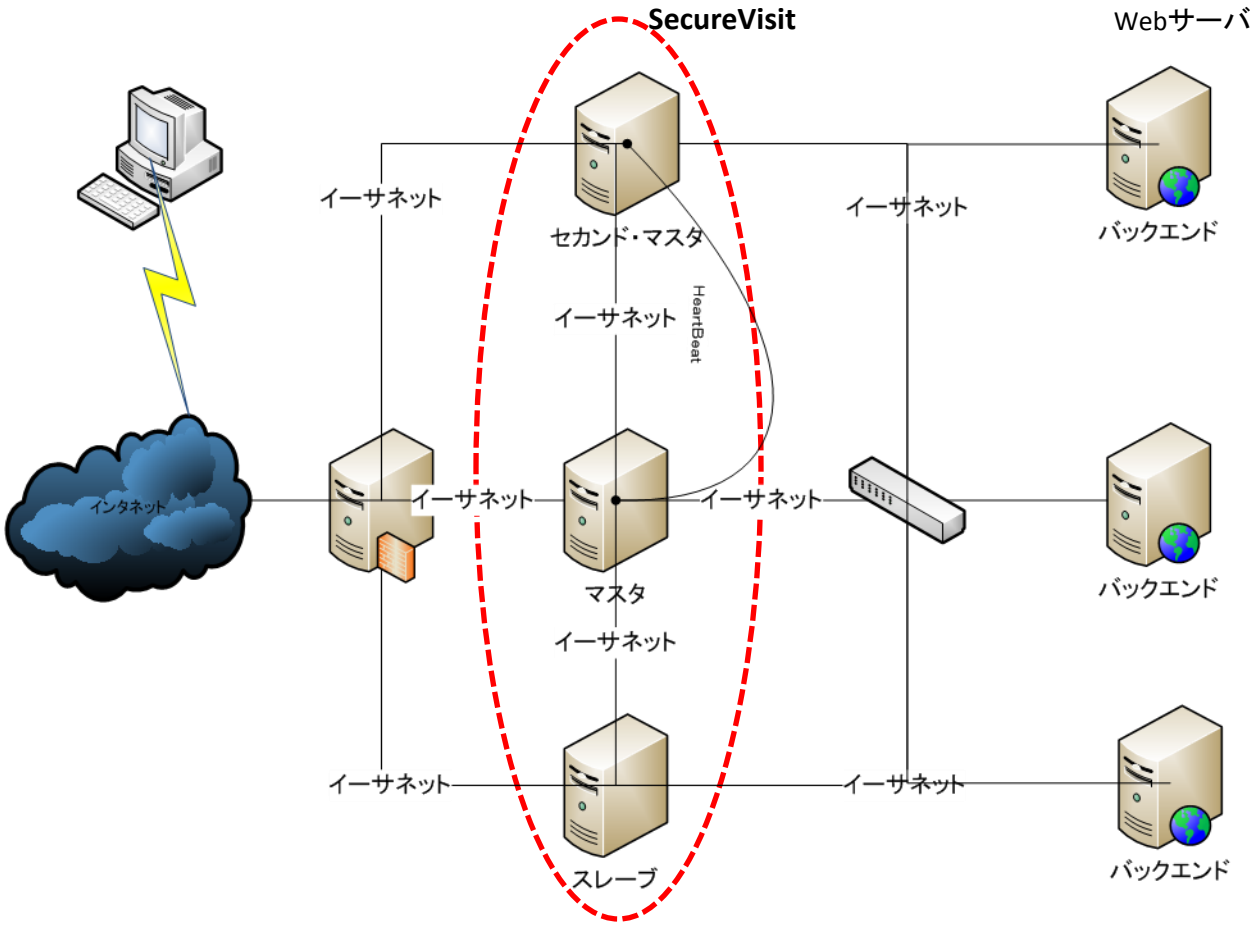
某建築系企業様

- 目的：
  1. 個人情報を取り扱う為パートナー企業との間で安全に情報共有を行う必要がある。
- 課題：
  1. パートナー企業では、知らない間に人事異動などが発生し、ID/パスワードを管理する事が困難である。ID/パスワードは漏洩しても気が付かない危険性がある。
- 導入効果：
  1. アクセス制御が物理的である為、紛失、漏洩などがすぐにわかるようになった。
  2. 誰にでも簡単に扱える為、使用法の説明が簡単で、管理コストの軽減に繋がった。
  3. 月額ライセンス、高額な保守費用ではない為、他の製品に比べて費用を抑える事が出来た。



冗長構成対応

SecureVisitは冗長構成に対応しており、大規模システムへの対応も可能です



＊）冗長構成イメージ図

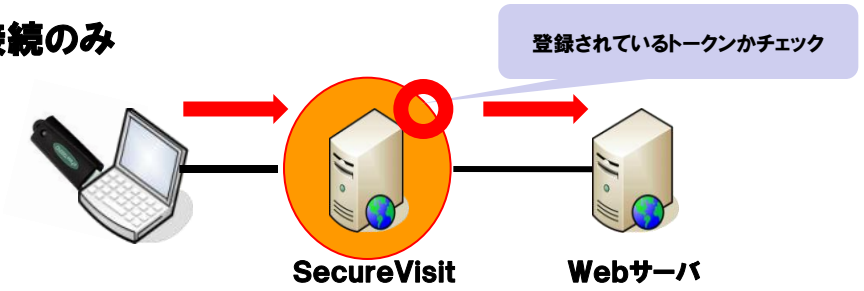
認証モード

FEITIAN WE BUILD SECURITY

・ユーザ側から見た認証モード

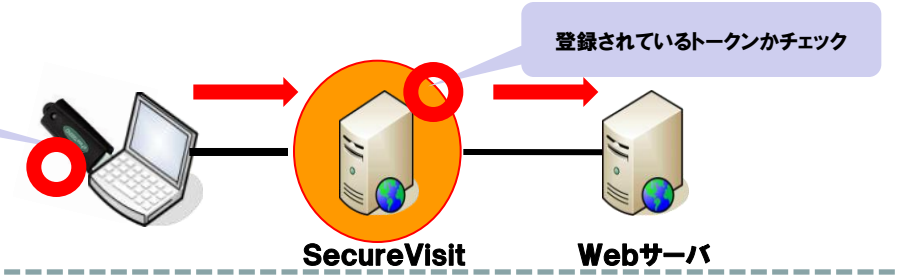
SecureVisitではお客様のセキュリティポリシーに応じて3段階の動作モードがあります。

Mode1　USBトークン接続のみ



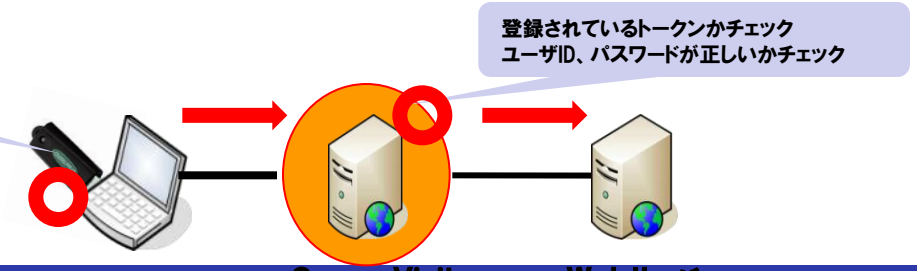
初期導入時にお薦めです。

Mode2　USBトークン＋　PIN入力（USBトークンにアクセスする為の暗証コード'を入力します）



トークンを盗難されてもPINが分からないと使えないので安心です。

Mode3　USBトークン　＋　PIN入力　＋「ユーザID、パスワード」



いずれのモードでもWebサーバがユーザID、パスワードを要求する場合は左記に加え、さらにWebサーバに対してユーザID、パスワードの入力をすることになります。

会社概要

FEITIAN
WE BUILD SECURITY

Feitian Technologies Co.,Ltd.

http://www.ftsafe.com.cn/

- 1998年設立　本社　中国　北京
- 主要拠点：中国国内5拠点、
- 現地法人：日本、マレーシア
- 従業員数：300名（2010年1月現在）
- 事業内容：
  セキュリティ認証デバイス製品の開発・製造・販売

2008年から：
中国国内USBトークン出荷量No.1連続達成

2010年現在：
51金融機関に導入済み

飛天ジャパン株式会社

http://www.ftsafe.co.jp/

- 2004年4月設立　東京
- Feitian Technologies社日本現地法人
- 従業員数 13名（2010年1月現在）
- 事業内容：
  - ・中国飛天製造セキュリティ製品の販売
  - ・中国飛天製造セキュリティ製品を利用したソフトウェアの開発・製造・販売
  - ・ﾃﾞﾊﾞｲｽﾄﾞﾗｲﾊﾞ、WindowsAPI、ICカードOSなどの受託オフショア開発
- 導入実績：400社以上の顧客2011年1月現在）

お問合せ先

飛天ジャパン株式会社
営業部

TEL:03-3668-6668（代）
E-mail : sales@ftsafe.co.jp
URL : http://www.ftsafe.co.jp/

FEITIAN
飛天ジャパン株式会社
WE BUILD SECURITY