# VACMAN Controller

## アプリケーションの認証強化を実現

**VACMAN Controllerは、VASCO社製トークンのバックエンドとして動作する最新のAPIベースの認証プラットフォームです。自動的にログイン要求を処理し、正しく認証されたユーザのみオンラインアプリケーションやネットワークにアクセスすることができます。また、VACMAN Controllerには、マンインザミドル攻撃からインターネット上の取引を保護するためのトランザクション署名(改ざん検知)機能やフィッシング対策などサーバ認証機能も統合されています。ユニークなデザイン、無制限のスケーラビリティと柔軟性によって、インターネットバンキング/電子商取引/オンラインゲーム/Webポータルなどの顧客の様々なアプリケーションにおいて、大規模な実装を完全にサポートします。**

### ネイティブな統合

VACMAN Controllerは、OS/データモデル/アーキテクチャに関わらず既存アプリケーションにカスタマイズ・統合が可能となります。このAPIベースのソリューションの多用性は、二要素認証の実装の容易性と効果的なROIを実現します。また、既存インフラと運用面において、アプリケーションへの影響や運用負荷を最小限に抑えます。

### 拡張性

VACMAN Controllerは、バックエンドのインフラを再構築する必要なく、既存システムへの認証機能の追加を容易に実現します。追加サーバやバックアップサーバの開発と保守を必要としません。

### 高可用性

VACMAN ControllerのAPIは、サーバのダウンタイムとサービス停止を心配する必要はありません。その高い信頼性は、認証が必要な時はいつでも、ユーザに対してシステムへの安全なアクセスを保証します。

### 効果的なROI(Return On Investment)を実現

VACMAN Controllerは、将来にわたりVASCO製品の認証とトランザクション署名のテクノロジ及び様々なデバイスに対応していけるように設計されています。これは、新たな規格や、任意のオペレーティングシステムまたはプラットフォーム用のアプリケーション、更にネットワークセキュリティの最新動向などに対応可能な柔軟性を実現していることを意味します。

VACMAN Controllerは、企業のIT投資を活用し、個別の認証サーバやデータベースの追加要件なしに一元的なプラットフォームを提供し、費用対効果の高いソリューションです。サーバファームや専用の災害復旧システムは必要ありません。

### 高い安全性

VACMAN Controllerは、お客様のセキュリティポリシーに合わせて、安全な鍵管理及鍵配布を実現するシングルプラットフォームです。

- VASCOの製造サイトからお客様までエンドツーエンドのセキュリティチェーンで配送
  - 物理的及び論理的なハイレベルなセキュリティを兼ね備えたセキュリティールーム内での初期化
  - オプションとして、お客様のセキュリティ担当者とのキーセレモニーで、セキュアに暗号化された経路によりDIGIPASSのキーファイル(DPX)をデリバリすることが可能
- オプションとしてハードウェアセキュリティモジュール準拠のソリューションを提供
  - ハードウェアによりDPXファイルの暗号化を提供
  - ワンタイムパスワードとトランザクション署名の検証をHSM内にて動作
  - 機密情報はHSM内で保護
  - FIPS規格に準拠

### 戦略的なパートナー製品に統合

VACMAN Controllerは、現在までにポータル/シングルサインオン/金融機関等の100以上のアプリケーションに統合されています。ネイティブな統合により、実装コストを大幅に削減し、管理運用を簡素化することができます。

VASCO
THE AUTHENTICATION COMPANY

VACMAN

## 複数の技術要素のサポート

VACMAN Controllerは、多様な認証デバイスとメカニズムをサポートしたマルチプラットフォーム対応テクノロジーです。VASCO社製トークンと同様にOATH準拠デバイス及びEMV CAPスマートカードにも対応可能です。VASCO社製トークンと組み合わせることで、エンドツーエンドの安全なオンラインプロビジョニングとトークンの管理機能を提供します。

以下のVASCO社製DIGIPASSシリーズをサポートしております。

- ワンボタン式のハードウェアトークン
- PINパッド付きハードウェアトークン
- マトリックスカード
- ソフトウェアトークン
  - DIGIPASS for Web/DIGIPASS for Mobile/DIGIPASS SDK
- Virtual DIGIPASS
  - SMSゲートウェイまたはSMTPとの連携が必須
- USBトークン
- スマートカード(ICカード)

## 複数の認証要素をサポート

VACMAN Controllerは、以下の通り様々な認証方式をサポートしています。

- 時刻ベースまたは回数ベースのワンタイムパスワード認証
- 時刻ベースまたは回数ベースのチャレンジレスポンス認証
- 時刻ベースまたは回数ベースのトランザクション署名
- トランザクション署名用のホストコード認証
- サーバPINの検証
- ワンタイムパスワード認証を使用したCHAP及びマイクロソフトのレスポンス認証
- 記憶ベース認証(秘密の質問及び回答方法)

## 他の機能

- 時刻ベースまたは回数ベースの同期メカニズム
- DES/3DES/AESの標準的な暗号方式のサポート
- ソフトウェアトークン用の管理機能
- アクティベーション情報などのプロビジョニング機能
- SMSベースの認証要求に対するOTP生成機能の一元管理
- マルチスレッド及びマルチタスクでの実装
- アカウントロックされたユーザへの安全なロック解除機能
- その他様々な機能別サンプルプログラムを装備

## 技術的な仕様

| | | | |
|---|---|---|---|
| ほとんど大部分のプロセッサとプラットフォームをサポート | • Windows XP/2003/2008/Vista/7 (32ビット、64ビット)<br>• Linux (32ビット、64ビット)<br>• Sun Solaris Sparc / Intel (32ビット、64ビット)<br>• HP/UX (32ビット、64ビット)<br>• AIX (32ビット、64ビット)<br>• FreeBSD (32ビット)<br>• AS/400<br>• OS/390<br>• Z/OS (32ビット、64ビット) | | |
| 標準化 | • EMV CAP (2004, 2007)<br>• EMV CAP E (2008)<br>• OATH (時刻ベースとカウンタベース) | | |
| 互換性 | • Safenet Protect server Orange/Gold/External,<br>• nCipher netHSM (ARM & Power PC アーキテクチャ)<br>• Safenet Luna SA, Thales WebSentry, IBM ICSF | | |
| 言語 | Windows:<br>• C / C++<br>• Java<br>• C# (.NET) | Unix/Linux:<br>• C / C++<br>• Java | メインフレーム:<br>• C / C++<br>• Java<br>• COBOL<br>• PL1<br>• アセンブラ |

## VASCOについて

VASCOは強力な認証や電子署名のソリューションおよびサービスのナンバーワンサプライヤです。国際金融機関をはじめ、全世界の大企業を顧客に持つ、インターネット上の安全を守る、世界のリーディングソフトウエアカンパニーです。VASCO製品は、金融機関/エンタープライズセキュリティ/政府機関/教育機関等で活用されています。

お問い合わせ先

www.vasco.co.jp phone: 03.3507.5750 email: info-japan@vasco.com