

リモートアクセス認証

USBトークン認証ソリューション for F5 FirePass



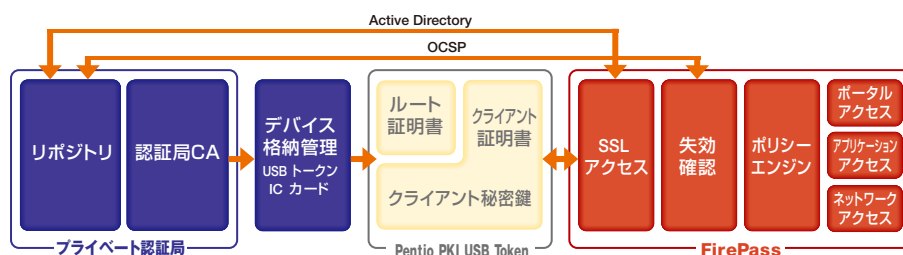
SSL-VPNアプライアンス F5ネットワークスジャパン株式会社 FirePass[®]シリーズとペンティオ株式会社のUSBトークンが連携。FirePass[®]が提供するクライアント端末のセキュリティ・チェックと暗号化通信に加え、FirePass[®]が発行する証明書によってクライアント認証の強化が可能になります。クライアント証明書は可搬性の高いPentio PKI USB Token[™]に格納すれば、外出先でノートPCからターゲットサーバへのセキュアなリモートアクセスを実現できます。

F5ネットワークスのSSL-VPNアプライアンス FirePass[®]は、インターネットにアクセスできる環境とWebブラウザを搭載するPC・PDA・携帯電話さえあれば、IPSecのような専用クライアントソフト無しで組織内LANへのリモートアクセスを可能にします。FirePassによるクライアントPCのセキュリティチェックに加え、Pentio PKI USB Token[™]によるPKI認証を行えば、ユーザ本人の認証を強化したリモートアクセス環境を実現できます。

FirePass[®]のユーザ認証

デフォルトでは、パスワードを使ってFirePass[®]の内部データベースと照合し、ユーザ認証が行われるようになっていきます。しかし、簡単な設定によって、RADIUS、Active Directory、RSA 2-Factor、LDAPの各種認証方式、フォームベースのベーシックなHTTP認証、アイデンティティ管理サーバ（Netegrityなど）、およびWindowsドメインサーバと連携させることもできます。Active Directoryによって、ユーザは現在のパスワードの期限切れのパスワードを変更することができ、またパスワードの期限が切れた時点で警告を受け取ることもできます。Active Directoryのネスト構造がサポートされていることで、より複雑な階層型のディレクトリ構造を利用することができます。

➤ Pentio PKI USB Token[™] + FirePass[®] 構成図



あくまでも概念構成図になります。

FirePass[®]のデジタル証明書/ PKIのサポート

管理者は、FirePass[®]のコントローラへのアクセスに使用したデバイスに基づいて、アクセスを制限または許可することができます。FirePass[®]は、ユーザのログイン中にクライアント側のデジタル証明書を確認できるためです。デジタル証明書があると、FirePass[®]はアプリケーションのアクセス範囲をより広くサポートできます。また、FirePass[®]は、クライアント側の証明書を2ファクタ認証の1つとしても使用できるため、有効なクライアント側の証明書がない場合、すべてのネットワークアクセスを禁止することもできます。

エンドユーザのGUIの日本語化

FirePassでは、機能名(Webアプリケーションなど)を始めとするエンドユーザWebページのすべてのフィールドをローカライズすることができます。これによって企業は、ユーザのお気に入りだけでなくエンドユーザのGUIもあわせてローカライズすることができ、ビジネス価値の向上とTCOの削減につながります。

➤ FirePass[®]の特長

安全なSSL通信と強力なエンドポイント・セキュリティ機能を備え、ユーザはWebブラウザさえあればデバイスや場所を選ぶことなく、ビジネスデータへセキュアにアクセスできるため、生産性を大幅に向上できます。

アプリケーションを選びません

IPSecのようなVPNクライアントソフトなしで、どんなアプリケーションにも対応するネットワークアクセス機能を標準搭載しています。

デバイスを選びません

Webブラウザを搭載するPCだけでなくPDAや携帯電話でもメールを読んだり共有ファイルにアクセスできます。

場所を選びません

インターネットに接続できる環境さえあれば、社内ネットワークへ安全にアクセスできます。

➤ FirePass[®]の主な機能

標準Webブラウザを使って

アプリケーションに接続
SSLに対応したWebブラウザを使うデバイス環境があれば、どこからでも社内イントラネットやメール、共有ファイルへのセキュアなアクセスが可能です。

モバイルアクセス

Webアプリケーション、モバイルe-mail、Windowsファイルに対応。ログイン画面からポータル画面までのコンテンツを自動変換。

ビジュアルポリシーエディタ

ポリシーチェックの基準となるアクセスポリシーを視覚的に分かりやすい方法で設定できるツールビジュアルポリシーエディタを標準搭載。フローチャートを描く要領で簡単にポリシーを定義できます。

クライアントセキュリティ機能

ログイン前とログイン後の2段階でポリシーチェックを実行し、ログイン自体と、ログイン後のリソースアクセスの許可を別々のポリシーで制御できます。これにより、ログインを許可したクライアントに対してより厳密なチェックを実行し、安全性に応じてアクセス可能なリソースを制御できます。

