

二要素認証デバイス

ハードウェアトークン



ePass トークン OTP トークン



ePass トークン



ユーザ情報をセキュアに格納し、なりすましによる不正を防止することが可能です。

ePassトークンは高度な暗号化アルゴリズムを搭載し、大切な個人認証情報（電子証明書、秘密鍵、ユーザID/パスワード）をセキュアに格納することで、なりすましによるデータの漏洩や改ざんなどの脅威から堅牢に保護します。

PKIに準拠した様々な認証ソリューションとの連携が可能です。

※ePass2000/3000シリーズはICカードチップを搭載し、ICカードと同等の強固なセキュリティを実現しております。

ワンタイムパスワード(OTP)トークン



一度限りの使い捨てパスワードを利用し、パスワードの漏洩やなりすましによる不正を防止することが可能です。

OTPトークンで発行されたワンタイムパスワードは、一度利用すると次回は利用できなくなります。

万が一、フィッシングなどでワンタイムパスワードが盗まれたとしても、そのパスワードは再利用ができないため、不正アクセスなどの被害を未然に防ぐことができます。

また、端末に接続しないため、OSやハードウェアに依存せず、タブレットやスマートフォンでも二要素認証を可能にします。

提供元

飛天ジャパン株式会社

使えるセキュリティをお客様へ

お問い合わせ・評価キットのお申し込みはこちらまで

飛天ジャパン 営業部

☎ 03-3668-6668

✉ sales@ftsafeco.jp

〒103-0016 東京都中央区日本橋小網町 9-3 CANAL TOWER 4F
<http://www.ftsafeco.jp/>

USBトークン ePass シリーズ ワンタイムパスワードトークン OTP c100 / c200

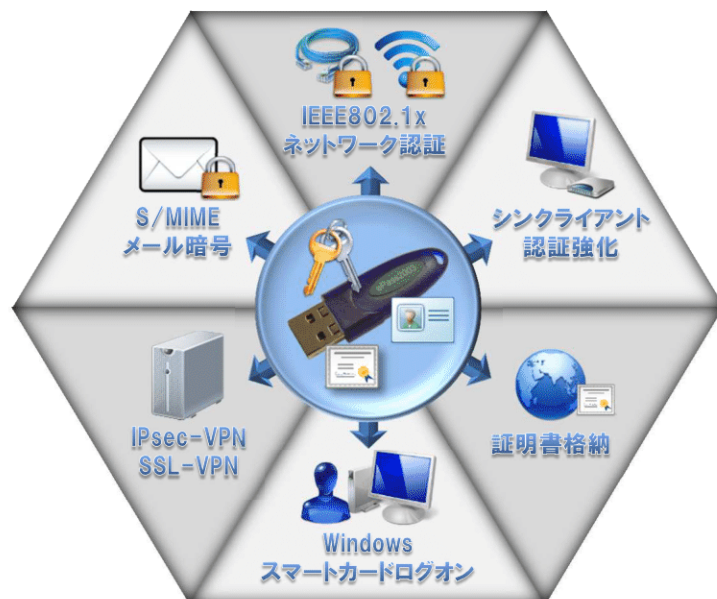
ePass

認証強化で不正を防止

ePassトークンは、コンパクトな設計で携帯性にも優れたUSBトークンで、トークンとPIN番号(個人識別番号)を組み合わせることで、ID/パスワードの認証より強固な二要素認証方式を実現できます。

Microsoft CAPIやPKCS #11に準拠したPKIソリューション(S/MIME, デジタル署名, セキュア認証, VPN接続, SSLウェブサイト)と容易に連携できます。
また、Cisco, CheckPoint, NetScreen などのネットワーク機器との連携にも幅広く対応しています。

- **マルチアクセスのサポート**
ePassトークンは同時に複数のアプリケーションをサポートする事ができます。
- **二要素認証**
PIN番号(個人識別番号)とUSBトークンの組合せでユーザを識別する二要素認証を実現します。
- **容易なインテグレーション**
SDK(開発キット)を利用すれば容易にチャレンジ&レスポンス方式を利用する事ができます。
- **利用用途に合わせた豊富な製品ラインナップ**
用途やセキュリティレベルに合わせて最適なトークンを選択できます。



ワンタイムパスワード

モバイルバンキングからオンラインゲームまで、幅広い用途で認証強化を実現

- **高セキュリティ**
発行されたワンタイムパスワードは1回限りの使い捨てのパスワードとして、従来の固定パスワードより強固な認証を実現できます。
サーバとの同期方式は、時刻を同期するタイムベース型(c200)と、発行回数カウンタにより同期を取るイベントベース型(c100)を選択できます。
- **利便性**
端末に接続しないため、クライアント端末へのアプリケーションのインストールは不要で、タブレットやスマートフォンでも使用が可能です。
持ち運びやすいキーホルダーデザインを採用しています。
- **幅広い用途で使用可能**
OATH規格に準拠し、様々なOATH規格準拠サーバーと簡単に連携できます。(※)
- **柔軟な対応**
1年～5年の保証期間プランを提供します。
トークンのケース色、会社ロゴ、フェイスプレートなどをカスタマイズすることが可能です。

パスワード同期の仕組み (タイムベース型)



oath
Initiative for open authentication

※「OATH(Initiative for Open AuTHentication)規格
OATHは認証に関連する業界をまたいだコラボレーションを推進
する組織として米VeriSignの呼び掛けにより設立されました。