ePass1000ND

ドライバレス USBトークン

●ドライバのインストール作業が不要ですぐに利用可能
●SDK（開発キット）付属のプライベートAPIを利用する事で
　Web認証システムを容易に構築可能
●PIN番号（暗証番号）とUSBトークンによる
　二要素認証を実現

■ePass1000ND

ドライバレス | チャレンジレスポンス | Windows | EEPROM | 専用API
マルチ言語サポート | RoHS

PCに接続するだけで利用できるドライバレスUSBトークン

多くのインターネット環境ではIDとパスワードによる簡単な認証を行っていますが、ID/パスワードは簡単に共有でき、また、憶測も可能で、近年ではID/パスワードの不正利用による被害が多く報告されています。その為、ID/パスワード認証を強化するデバイスの必要性に迫られています。ePass1000NDはドライバのインストールが不要※でPCと接続するだけで利用可能なため、ユーザーにとって便利で使い易いセキュリティデバイスです。管理者・開発者は付属のSDK（開発キット）を利用する事で、様々なWeb認証システムのセキュリティを強化する事ができます。

※デバイスドライバのインストールは不要ですが、トークンを管理するプログラムはPC側に必要です。

ePass1000ND

ePass1000NDはASP/CGI/Delphi/Java/VB/VCなどの言語に幅広く対応し、チャレンジ＆レスポンス認証などのWeb認証ソリューションを構築する事ができます。また、ePass1000NDはOSの標準ドライバを利用するので、アプリケーションとの親和性が高いのも特徴です。認証方式は、USBトークンのみによる認証、USBトークン＋PIN番号、ID/パスワード＋USBトークンによる認証など様々な認証方式を実現できます。

ご利用方法と主な機能

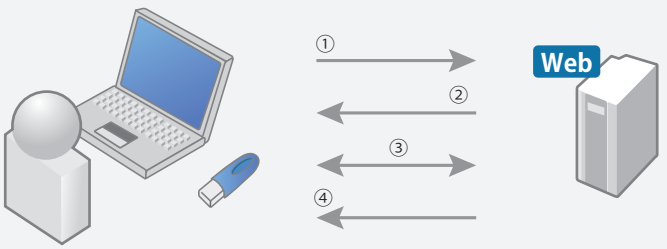
1. チャレンジ＆レスポンス認証

ePass1000NDはID/パスワードよりも強固なセキュリティを
実現するチャレンジ＆レスポンス認証を容易に実現できます。

新規でセキュアWebサイトを構築する際以外に、既にID/パスワード
を利用しているWebサイトからの移行も容易に行えます。

2. ドライバレス

ePass1000NDはドライバレスUSBトークンで、
PCに接続するだけですぐに利用できます。



チャレンジ＆レスポンス認証による接続方法

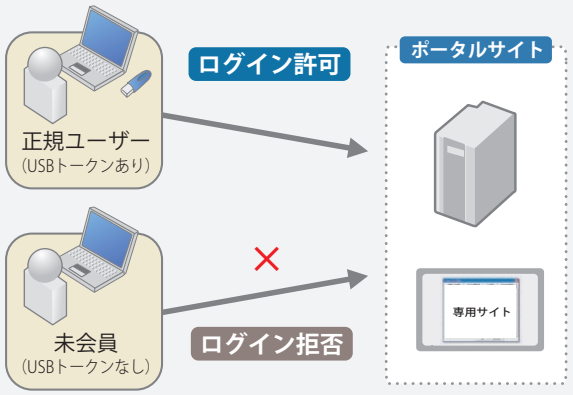
① Webサイトへログインの試行
② Webサーバーはクライアント PCにUSBトークンが接続されているか確認
③ USBトークンが接続されていれば、USBトークンとWebサーバー間でチャレンジ＆レスポンス認証を実行
④ 認証を行えたPCのみ接続を許可

※MD5によるハッシュ計算のデータのみネットワーク上で送受信されるのでパスワードなどの盗聴を防ぎます。

ePass1000NDの製品特徴

- OS標準ドライバを利用するのでアプリケーションとの高い親和性を実現
- PIN番号/ID+パスワード/ハードウェアIDなどによる様々な認証方式をサポート
- オンボードで暗号化計算(MD5ハッシュ計算)を実行可能
- ASP/CGI/Delphi/Java/VB/VCなどの言語に幅広く対応
- ID/パスワードを利用しているWebサイトから容易に移行可能

●導入例



ePass1000NDを利用すれば会員制Webサイトなどで二要素認証(PIN番号+USBトークン)を容易に実現する事ができます。また、ePass1000NDはドライバレスなのでPCに接続するだけで利用でき、利便性を損なわずにセキュリティを大幅に強化する事ができます。

●製品仕様

	ePass1000ND
サポートOS (※1)	Windows 2000(32bit) Windows XP, Vista, 7, 8/8.1,10, Server2003/R2, 2008/R2 Server 2012/R2(64bit) Linux
対応標準	PKCS#11, MS CAPI, X.509 v3 Certificate Storage, SSL, IPSec / IKE
内蔵暗号化アルゴリズム	HMAC-MD5,TEA
API	Microsoft Crypto API (CAPI) PKCS#11
内蔵プロセッサー	8bit CPU チップ
内蔵メモリ	32KB (EEPROM)
書き換え寿命	100,000回以上
メモリデータの保存期間	10年以上
コネクタ	USB 1.1 / 2.0, Connector type A
インターフェイス	HID
消費電力	250mW 以下
動作温度	0℃～70℃
保存温度	-20℃～85℃
保存湿度	0～100% (結露なきこと)
認定	RoHS/WEEE, CE, FCC

(※1) 対応OSのバージョンについては、お問い合わせ下さい。

詳しくは、WEBサイトでもご覧頂けます。http://www.ftsafe.co.jp/

ePass2001

コストパフォーマンスに優れた高機能USBトークン

●2048bit RSA対応でセキュリティレベル向上
●電子証明書/秘密鍵のセキュリティを低コストで向上
●高速スマートカードチップを搭載し、
　高機能・高セキュリティを実現
●PIN番号（暗証番号）とUSBトークンによる二要素認証を実現

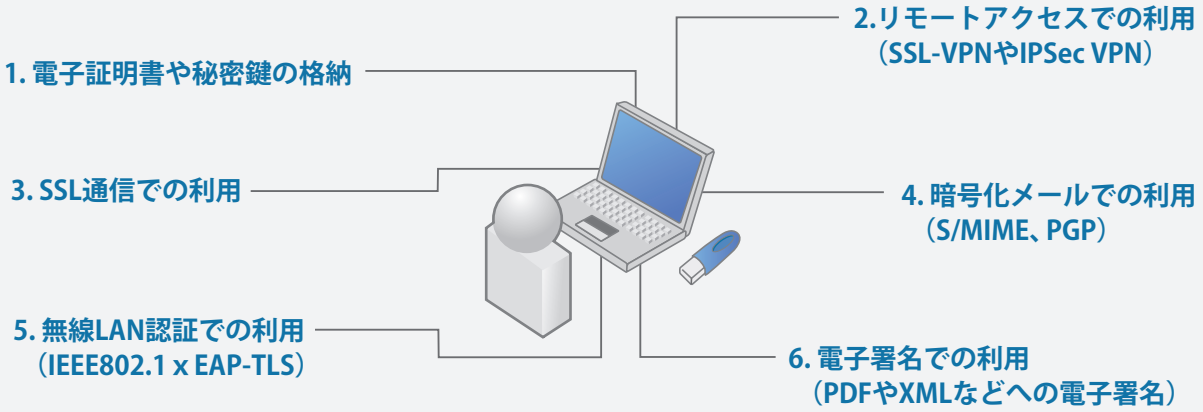
■ePass2001

電子証明書	リモートアクセス	暗号化メール	スマートカード・チップ搭載
Web認証	電子署名	無線LAN認証	RoHS

電子証明者をセキュアに格納するUSBトークン

ePass2001は、高速スマートカード・チップを搭載した製品で、通常スマートカードとカードリーダーのセットで実現される機能を本体一つで実現することができます。また、スマートカード・チップの技術により複製が困難なため、安心して携帯頂くことができます。VeriSign、Entrust、Betrustedなどの主要な認証局の電子証明書をはじめ、CheckPoint VPN-1、Cisco VPN3000、NetScreenなどの様々な製品をご利用される際の電子証明書や秘密鍵の格納に対応しています。さらに、秘密鍵をUSBトークン内で生成することができます。弊社が提供しているSDKを利用して、既存のセキュリティ・アプリケーションへの統合や、新規開発が容易に行えます。

ePass2001適用例



ePass2001の製品特徴

- PKI秘密キー生成の高速化（当社従来製品対比2.6倍）
- PKCS#11、MS CAPI、ISO7816-3 and 4 compliant等、各種標準に準拠
- スマートカードチップを搭載し、オンボートでPKI処理（電子署名/暗号計算）を実現
- 複数の秘密鍵・公開鍵の格納に加えて、ルート証明書や中間証明書をそれぞれ格納する事が可能

■ 容易な証明書管理

ePass2001USBトークンに証明書を格納するには、ブラウザから直接行う方法と、PCに保存された証明書ファイル（PFX、P12、P7B、CERなど）を付属の管理ツールを利用してインポートをする方法があります。

■ 証明書を管理ツールから直接インポート

ePass2001USB管理ツール（下図）では、証明書のインポート以外に、証明書の管理、PIN番号の変更、USBトークン名の変更、ロックの解除、USBトークンの初期化などを行う事ができます。

■ ブラウザー経由の直接インポート

ブラウザー経由で証明書を発行した場合、直接ePass2001USBトークンに格納する事ができます。

■ 付属ツール類は日本語対応

付属する管理ツールなどは日本語に対応しております。

●製品仕様

	ePass2001
サポートOS（※1）	Windows 2000（32bit） Windows XP, Vista, 7, 8/8.1,10, Server2003/R2, 2008/R2（32/64bit） Server 2012/R2（64bit） Linux Mac OS X
対応標準	PKCS#11, MS CAPI, X.509 v3 Certificate Storage, SSL, IPSec/IKE, ISO/IEC 7816, PC/SC
内蔵暗号化アルゴリズム	RSA 1024/2048bit DES, 3DES, AES, SHA-1, SHA256, SHA384, SHA512
API	Microsoft Crypto API（CAPI） PKCS#11
内蔵プロセッサー	8bit スマートカードチップ
内蔵メモリ	32KB
書き換え寿命	100,000回以上
メモリデータの保存期間	10年以上
コネクタ	USB 1.1/2.0, Connector type A
インターフェイス	HID
消費電力	320mW 以下
動作温度	0℃～70℃
保存温度	-20℃～85℃
保存湿度	0～100%（結露なきこと）
認定	RoHS/WEEE, CE, FCC

（※1）対応OSのバージョンについては、お問い合わせ下さい。

詳しくは、WEBサイトでもご覧頂けます。http://www.ftsafe.co.jp/

ePass2003

接続するだけで使える、
次世代アルゴリズム搭載のUSBトークン

- オンボードでRSA2048bit、AES256bit、SHA-256の暗号化を実現しセキュリティレベル強化
- Windows7/8/10では接続するだけで利用可能
- FIPS 140-2 Level3, Common Criteria EAL5＋モジュール搭載で高い信頼性を実現
- スマートカードログオン対応でリモートデスクトップ接続、シンクライアントへの利用が可能
- 64KBユーザメモリ(2048bit鍵長証明書が最大9枚格納可能)
- Microsoft Minidriver/OpenSCに対応
- Linux、Mac OS Xに対応
- A1通常パッケージに加えE5小型パッケージを追加

A1タイプ


E5タイプ

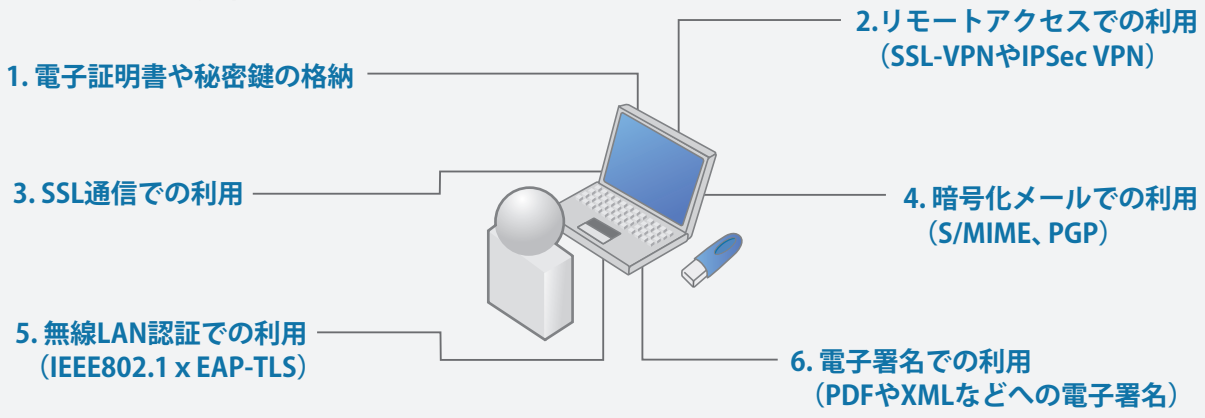
■ePass2003

電子証明書	リモートアクセス	暗号化メール	Mac OS Linux	スマートカード・チップ搭載	CCID	Microsoft Minidriver
Web認証	電子署名	無線LAN認証		RoHS	FIPS	

電子証明書をセキュアに格納するUSBトークン

ePass2003は、高速スマートカード・チップを搭載した製品で、通常スマートカードとカードリーダーのセットで実現される機能を本体一つで実現することができます。また、スマートカード・チップの技術により複製が困難なため、安心して携帯頂くことができます。VeriSign、Entrust、Betrustedなどの主要な認証局の電子証明書をはじめ、CheckPoint VPN-1、Cisco VPN3000、NetScreenなどの様々な製品をご利用される際の電子証明書や秘密鍵の格納に対応しています。さらに、秘密鍵をUSBトークン内でオンボートで生成することができます。弊社が提供しているSDKを利用して、既存のセキュリティ・アプリケーションへの統合や、新規開発が容易に行えます。

ePass2003適用例



ePass2003の製品特徴

- 公開鍵暗号RSA2048bit、共通鍵暗号AES256bit、ハッシュ関数SHA-256のオンボード処理を実現
- CCIDデバイス／Microsoft Minidriverに対応、Windows7/8/10環境では接続するだけで利用可能
- 内蔵チップは、米国連邦標準規格であるFIPS（Federal Information ProcessingStandards）140-2のレベル3に認定
- PKI秘密鍵の生成を高速化（当社従来製品対比2.6倍）
- PKCS#11、MS CAPI、ISO7816等、各種規格に準拠
- スマートカード・チップを搭載し、オンボードでPKI処理（電子署名／暗号計算）を実現
- OpenSCをサポートしていることにより、Linux、Mac OSにも対応

■ 容易な証明書管理

ePass2003に証明書を格納するには、ブラウザーから直接行う方法と、PCに保存された証明書ファイル（PFX、P12、P7B、CERなど）を付属の管理ツールを利用してインポートを行う方法があります。

■ ブラウザー経由の直接インポート

ブラウザー経由で証明書を発行した場合、直接ePass2003USBトークンに格納する事ができます。

■ 証明書を管理ツールから直接インポート

ePass2003管理者用管理ツール（下図）では、証明書のインポート以外に、証明書の管理、PIN番号の変更、USBトークン名の変更、ロックの解除、USBトークンの初期化などを行う事ができます。

■ 付属ツール類は日本語対応

付属する管理ツールなどは日本語に対応しております。

● 製品仕様

	ePass2003
サポートOS（※1）	Windows Vista, XP SP3, 7, 8/8.1,10, Server2003/R2, 2008/R2（32/64bit） Server 2012/R2（64bit） Linux Mac OS X
ミドルウェア	Microsoft Windows MiniDriver Windows middleware for Windows CSP Direct-called library for PKCS#11 under Windows, Linux & Mac
対応標準	X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID
内蔵暗号化アルゴリズム	RSA 512/1024/2048 bit ECDSA 192/256 bit DES/3DES AES 128/192/256 bit SHA-1 / SHA-256
暗号化API	Microsoft Crypto API（CAPI） Cryptography API：Next Generation（CNG） Microsoft Smart Card MiniDriver PKCS#11 PC/SC
内蔵プロセッサー	16 bit スマートカードチップ
内蔵メモリ	64KB（EEPROM）
書き換え寿命	500,000回以上
メモリデータの保存期間	10年以上
コネクタ	USB 2.0 full speed, Connector type A
インターフェイス	ISO 7816, CCID
消費電力	250mW 以下

	ePass2003
動作温度	0℃～70℃
保存温度	-20℃～85℃
保存湿度	0～100%（結露なきこと）
防水性能	IPX8
認定	Microsoft WHQL Linux PCSC-Lite / Lib CCID RoHS/WEEE, CE, FCC

（※1）対応OSのバージョンについては、お問い合わせ下さい。

詳しくは、WEBサイトでもご覧頂けます。http://www.ftsafe.co.jp/

ePass3003/ePass3003Auto

32bitスマートカードチップ搭載
高性能USBトークン

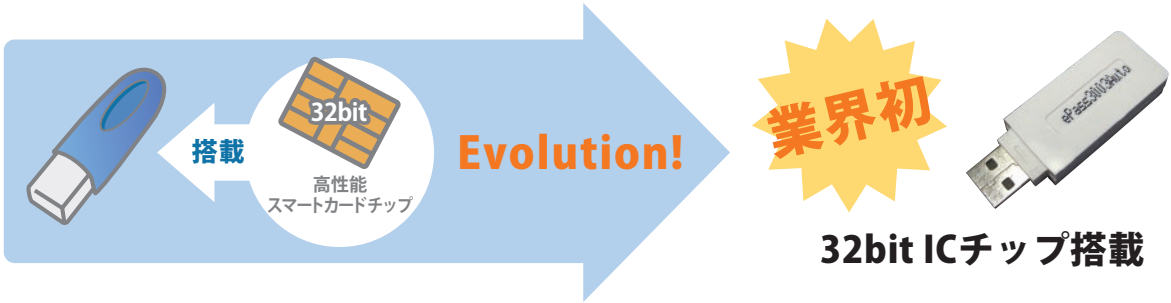
●2048bit RSA対応でセキュリティレベル向上
●高速性 認証、署名処理を32bitスマートカードでオンボード処理
●PKI対応、デジタル署名、暗号化、VPN、SSL認証など
●ドライバレス対応で高いユーザビリティを実現

■ePass3003/ePass3003Auto

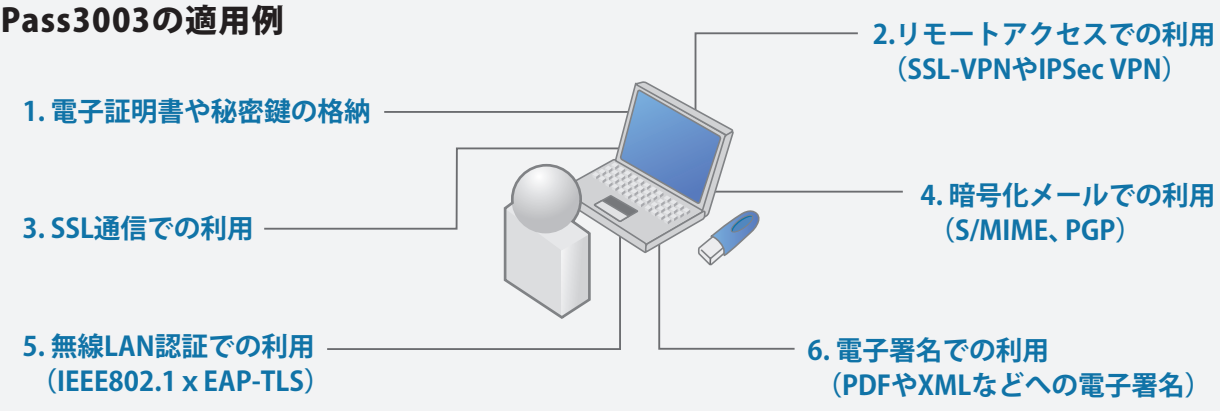
電子証明書	リモートアクセス	暗号化メール	Mac OS Linux	スマートカード・チップ搭載	32bitスマートカードチップ
Web認証	電子署名	無線LAN認証		RoHS	

32bit 高性能スマートカードチップ搭載USBトークン

ePass3000シリーズ製品は32bit高性能スマートカードチップを搭載した業界初のUSBトークン製品です。秘密鍵・公開鍵ペアの生成や、認証、署名処理を高速にオンボードで行い、最高レベルのセキュリティが確保できます。PKIアプリケーションに対応し、電子メールの暗号化、デジタル署名、VPN、SSLウェブサイト認証などにご利用いただけます。



ePass3003の適用例



ePass3003の製品特徴

- 32bit高性能スマートカードチップ搭載
- オンボード RSA,DES,3DES,MD5,SHA-1
- オンボード 1024/2048bit RSA キーペア生成
- オンボード電子署名
- オンボード乱数生成器
- ユニークな64bitハードウェアID
- 64Kバイトセキュアなユーザーメモリ領域
- USB1.1/2.0標準インターフェイス
- ドライバレス／ Plug-and-Playデバイス
- PKIアプリケーションへの全面的なサポート
  - ▶PKCS#11ライブラリ、CSPモジュール提供
  - ▶PKCS#11、MS CAPIインターフェイス提供
  - ▶X.509 v3電子証明書セキュアストレージ
  - ▶複数の電子証明書ストレージ

●製品仕様

	ePass3003	ePass3003Auto
サポートOS（※1）	Windows Vista, XP, 7, 8/8.1,10, Server2003/R2, 2008/R2(32/64bit) Server 2012/R2(64bit) Linux Mac OS X	Windows Vista, XP, 7, 8/8.1,10, Server2003/R2, 2008/R2(32/64bit) Server 2012/R2(64bit) Linux Mac OS X
ミドルウェア	Windows middleware for Windows CSP PKCS#11	Windows middleware for Windows CSP PKCS#11, 自動インストール
対応標準	X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816	
内蔵暗号化アルゴリズム	RSA 1024 / 2048 bit DES / 3DES AES 128 bit SHA-1 / SHA-256	
暗号化API	Microsoft Crypto API（CAPI） PKCS#11	
フラッシュメモリ	—	2MB
フラッシュ書き換え寿命	—	20,000回以上
内蔵プロセッサー	32 bit スマートカードチップ	
内蔵メモリ	64KB（EEPROM）	
書き換え寿命	500,000回以上	
メモリデータの保存期間	10年以上	
コネクタ	USB 2.0 full speed, Connector type A	
インターフェイス	ISO 7816	
消費電力	250mW 以下	
動作温度	0℃～70℃	
保存温度	-20℃～85℃	
保存湿度	0～100%（結露なきこと）	
防水性能	IPX8	
認定	Microsoft WHQL RoHS/WEEE, CE, FCC	

（※1）対応OSのバージョンについては、お問い合わせ下さい。