FEITIAN
WE BUILD SECURITY

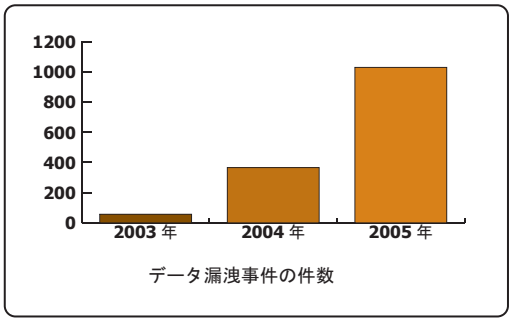
ePass USBトークンの必要性

Feitian

1. 電子証明書とは？

インターネットが一般化した現代では、企業間取引に電子メール、オンライン取引、ウェブなどの利用が一般的になっています。しかし、こうしたインターネットの普及が進むにつれ、インターネット上での犯罪、データ漏洩なども増加の一途をたどり、今や顧客や個人情報の保護に対する対策はインターネットを利用する企業では最重要課題にまでなっています。

現在、この個人情報保護に対する有効な手段として、「電子証明書」が広く利用されています。電子証明書とはインターネットの世界における身分証明書のようなもので、運転免許証などの様な役割をもち、インターネットという「匿名性」の高い世界において、身分を確認する重要な手段となっています。この電子証明書は誰でも発行することができますが、発行された電子証明書が本人のものであるという証明として認証局（CA）による認証が必要になります。



データ漏洩事件の件数

さらに、「なりすまし」や「データの改ざん」を防ぐ為に、電子証明書では「公開鍵暗号方式」という暗号化を用い、データの正確性を保護しています。この公開鍵暗号方式とは公開鍵と秘密鍵という 2 つの鍵（キーペア）を使いデータを暗号化する方法で、この暗号化方式は一方の鍵で暗号化した情報はもう一方の鍵を使わないと複合化できないという特長を持ち、非常に高いセキュリティを確保しています。また、この公開鍵暗号を用いた技術を PKI（Public Key Infrastructure：公開鍵暗号基盤）と呼びます。

2. 電子証明書や秘密鍵が盗まれたら？

電子証明書はインターネットにおいて個人の身分を特定するものとして大変便利なものですが、それだけに万が一盗難にあってしまうと、電子証明書に含まれる名前などの個人情報、秘密鍵、公開鍵などの様々な機密データが漏洩し、第 3 者が本人と偽る「なりすまし」をして大切な企業のデータや個人情報を盗み取ったり、「データの改ざん」などの被害にあう可能性が極めて高く、企業の信頼を失うことに繋がりかねません。その為、電子証明書を利用する際にはその保管場所についても慎重に考慮する必要があります。

情報漏えいが発生するケースの具体例

情報漏えい具体例 ケース1

電子証明書を利用していない場合

電子証明書を利用していない場合、取引をしている相手が「本人」だという証明はなく、また通信時のデータも暗号化されない為、第３者による「なりすまし」やデータの「盗聴」をされてしまう可能性があります。

ID とパスワードが盗まれてしまうと情報漏えい発生

情報漏えい具体例 ケース2

電子証明書を PC に保管している場合

電子証明書を格納している PC が紛失・盗難の被害に遭うと、PC 内部のデータ以外にも電子証明書を利用した「なりすまし」により、顧客情報などの機密情報も漏洩してしまう危険性があります。

PC が盗まれてしまうと情報漏えい発生

最も多い情報漏えいの発生原因としては「PC の盗難・紛失」が 1 番多く報告されています。セキュア通信の為に電子証明書を利用していても、それを保管している PC 自体が盗難にあってしまうと、せっかくの電子証明書の意味がなく、第 3 者による不正利用されてしまう危険性があります。また、盗難・紛失による被害は外出時のみではなく、社内に設置している PC に対しても報告されており、社内に設置している PC に対しても同様に対策を行う必要があります。

PCに保管する際の潜在的リスク

PC故障・ウィルス感染

PC のトラブルによる機密データ消失

普段利用しいる PC に電子証明書を格納している場合、ハードディスク故障、ウィルス感染によるデータの消失、その他 PC のトラブルにより、ある日突然機密情報を消失してしまう場合があります。

電子証明書などの機密情報はセキュリティの観点からもファイルサーバー上などにバックアップを保管するものではなく、一度消失してしまうと復旧が難しい為、PC 上に保管しておくのは潜在的リスクが非常に高いと言えます。

PC に保管するのはリスクが高い

3. USB トークンとは？


ePass2000

電子証明書を利用することにより、「なりすまし」、「盗聴」、「データの改ざん」など様々なリスクを回避する事ができますが、電子証明書そのものが盗まれてしまってはセキュリティ上問題があります。その為、電子証明書は PC 上などに保管するのではなく、安全な「保管庫」が必要になります。それが、「**USB トークン**」です。

USB トークンは USB フラッシュメモリーと形状が似ていますが、使用目的・機能は大きく異なり、USB メモリーは主にデータの持ち運びに利用されるのに対し、USB トークンは電子証明書、秘密鍵、認証情報を格納する事が主な利用目的の認証セキュリティデバイスです。

また、USB トークンには様々なタイプがあり、ePass2000（写真左上）の様に PIN（Personal Identification Number）番号と呼ばれる暗証番号を入力し、USB トークン内に格納した機密情報にアクセスするタイプと、PIN 番号の代わりに指紋などの生体認証を利用するタイプ（写真右下）があります。このようなハードウェアトークンと PIN 番号（または生体認証）を組み合わせる事で、今までの ID/ パスワードによる認証よりも高度な認証方式を実現しています。

さらに、USB トークンに格納した電子証明書や認証情報は強力な暗号化により保護されるので、万が一 USB トークンを紛失または盗難の被害にあっても、データの解読はほぼ不可能で、データ漏洩のリスクを未然に回避する事ができます。また、IC カードチップ内蔵タイプ（ePass2000/BioPass3000）の場合はオンボードで秘密鍵の生成を行うこともでき、機密情報を外部に漏らすことがありません。

なお、USB トークンには電子証明書や秘密鍵の格納以外にも、業務で利用する Web アプリケーションなどの認証情報をトークン内に暗号化して格納する事もできるので、様々な認証システムに利用できます。


BioPass3000

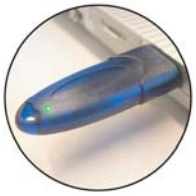
FEITIAN
WE BUILD SECURITY

ePass USBトークンの必要性

Feitian

4. 情報漏えいへの対策

ePass USBトークンを利用する事で 様々な情報漏えいのリスクを回避できます



情報漏えいケース1対策：
電子証明書を利用した暗号化通信でデータの安全を確保

情報漏えいケース2対策：
電子証明書を USB トークン内に保存することで漏洩を回避

電子証明書や秘密鍵を USB トークン内に暗号化して格納する事で、

- **第 3 者による「なりすまし」**
- **「データの盗聴・改ざん」**
- **PC の紛失・盗難による情報漏えい**
- **ハードディスク故障よる機密データの消失**
- **ウィルスによる機密データの漏洩**

などの脅威を未然に防ぐことができます。

5. ePass USB トークンのメリット

業界最高水準のセキュリティ
ePass2000 は IC カード内蔵（FIPS140-2 認定モジュール）、BioPass3000 は IC カード・32bitCPU を内蔵し、業界で最高のセキュリティを実現しています。

優れた携帯性
USB トークンはカードリーダ不要で、USB ポートがあれば何処でも利用できます。また、本体は軽量かつ耐タンパ機能があり、携帯も容易にできます。

豊富なバリエーション
独自プログラムが可能な ePass1000 から生体認証を利用する BioPass3000 まで、幅広いラインナップで様々なニーズにも柔軟に対応します。

優れたコストパフォーマンス
ePass/BioPass シリーズは高い品質・性能を実現しつつも低価格を実現しており、小規模から大規模導入まで幅広く対応し、大幅なコストダウンを可能にします。

PINによる不正利用防止
トークン内に格納した機密情報にアクセスするには PIN 番号（BioPass3000 は指紋認証）が必要となるので、第 3 者による不正利用を防ぎます。

複数の電子証明書の利用
電子証明書は 1 組だけではなく複数格納することができます。また、電子証明書以外にも、Web アプリケーションなどの認証情報なども安全に格納できます。

二因子認証（USBトークン＋PIN/ 指紋）

ePass1000/ePass2000
PIN 番号を入力しないと、格納したデータへのアクセスは不可能

BioPass3000
PIN 番号の代わりに指紋認証により格納したデータにアクセス

ePassシリーズ製品一覧

【ePass1000】
- 独自プログラム可能
- 優れたコストパフォーマンス

【ePass2000】
- FIPS140-2 認定モジュール搭載
- IC カードチップ搭載

【BioPass3000】
- 指紋認証 USB トークン
- 32bit CPU 搭載
- IC カードチップ搭載

6.「SecureCore」ならPCの保護まで可能

「SecureCore」は専門知識が無くても使える個人情報保護ソフトウェアです。ePass1000, ePass2000, BioPass3000 まで幅広く対応しており、USB トークンと組み合わせる事で、PC の紛失・盗難による情報漏えいは勿論、個人情報保護対策に対しての包括的なソリューションを提供します。

SecureCore の主な機能

セキュアログイン
USB トークンを「鍵」として Windows へログインします。USB トークンが挿入されていないと Windows にログインが出来ない為、PC の不正利用を防ぎます。

シングルサインオン
様々な Web サイト・アプリケーションの ID とパスワードを一元管理し、対象サイトへのログイン時に ID とパスワードを自動送出することでパスワード漏洩を防ぎます。

ファイル・フォルダ暗号化
ドラッグアンドドロップの直感的な操作で、ファイル・フォルダーを暗号化します。USB トークンが挿入されていないと複合化できない為、ファイルの不正コピーを防ぎます。

サーバーによる一元管理
SecureCore ではサーバーによる USB トークンの一元管理が可能で、管理負荷を大幅に低減しつつも、情報漏えい対策を行うことができます。

■評価版ePass USBトークン
- 無料貸出 -

ePass1000/ePass2000
Feitian PC Security

梱包物：
- USB トークン
- ソフトウェア CD-ROM
- 開発者ガイド

弊社評価キットは情報保護対策や認証システム構築時の検証に最適な評価版となっております。また、ご購入前に検証ができるので導入後のトラブルを軽減します。
※無料評価キットのお申し込みは弊社 Web サイトから行えます。

飛天ジャパン株式会社
〒101-0051
東京都千代田区神田神保町 1-42-4 鉄建神保町ビル 8 階
TEL:03-5281-0688 FAX:03-5281-0655
http://www.ftsafe.co.jp/ E-mail : sales@ftsafe.co.jp