第２回セキュアシステムシンポジウム
2014年3月13日

Man-in-the-Browserの脅威と根本的な解決策

独立行政法人産業技術総合研究所
セキュアシステム研究部門
セキュアサービス研究グループ
高木浩光，　渡辺創

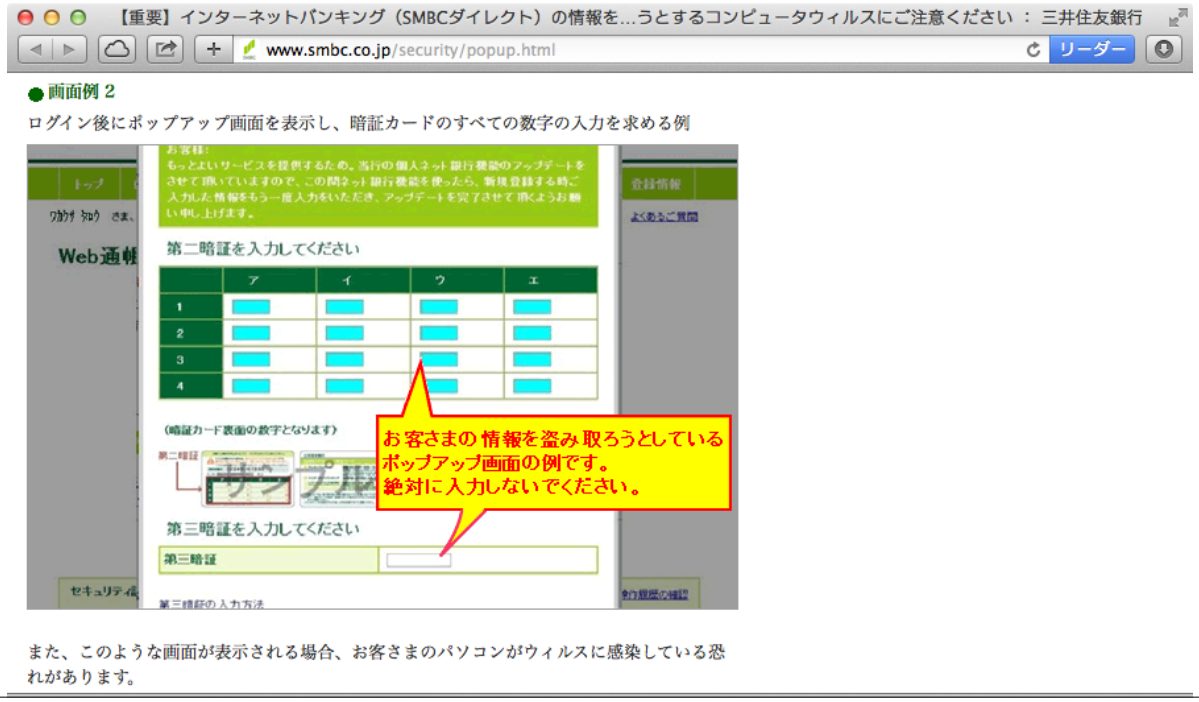
目次

- 銀行における不正送金被害
- Man-in-the-Browser攻撃とは
- いくつかの解決策
- シンガポールでの普及状況
- 解決策の様々な方式
- 産総研当グループでの研究開発
- 電子申請への応用
- 公的個人認証の在り方

AIST

銀行の被害状況

- マルウェア感染によるwebinject攻撃



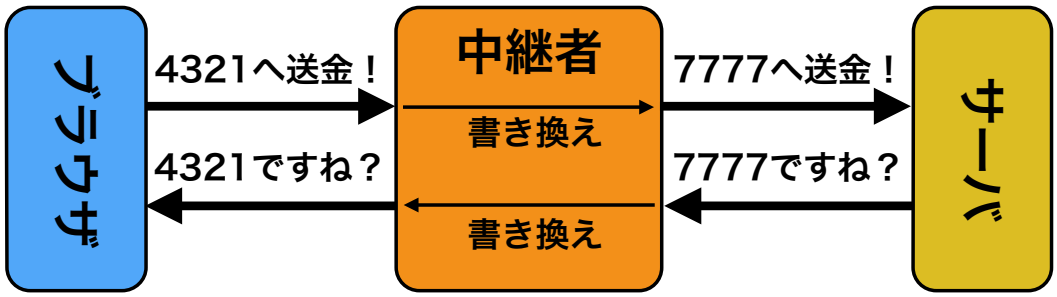
また、このような画面が表示される場合、お客さまのパソコンがウィルスに感染している恐れがあります。

AIST

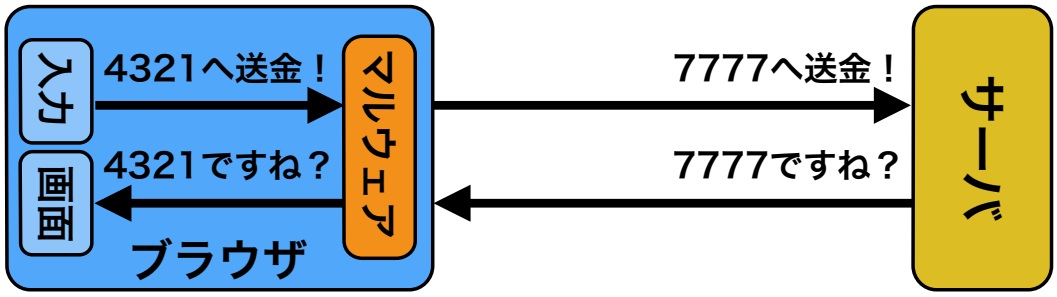
用語「Man-in-the-Browser」の混乱

- 濫用された意味
  - 前ページのような単なるwebinect攻撃全般を指して
    - 対策ソリューションベンダの売り文句において
- 本来の意味
  - 中間者攻撃（Man-in-the-Middle）と同じ原理で、中継サイトを要しないもの
  - マルウェアがブラウザ内で送受信データを改ざん
    - 見抜く方法が存在しないのが特徴である点に注意
    - 本人が銀行を利用している最中に、セッションを乗っ取ったり、振込先口座番号を差し替えるなどの攻撃が行われる
  - 通信の途中に割り込む中間者攻撃なら
    - SSLが異常を検知して警告画面が出る
  - 中継型のフィッシングサイトでの中間者攻撃なら
    - 警告画面は出ないが、アドレスバーで偽サイトであることを見抜ける

Man-in-the-Middle攻撃

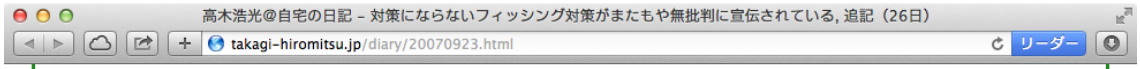


Man-in-the-Browser攻撃



歴史的経緯

- 中間者攻撃による送金先口座番号の差し替え攻撃



原理的にはこれと同様に、トロイに侵されていなくても、偽サイト上で同様に「ユーザーとともにオンラインバンキングを利用し口座の金を盗む」という中間者攻撃があり得るのであり、このことは研究者なら昔からわかり切っていたことだし、Bruce Schneierも2005年3月に次のように予言して警鐘を鳴らしていた。

- Bruce Schneier, Two-Factor Authentication: Too Little, Too Late, Communications of the ACM, vol.48, No.4, (2005).
- Schneier: 'Two-factor security is not our saviour'（Schneier曰く「二要素認証セキュリティは我々の救世主ではない」）, ComputerWeekly.com, 2005年3月21日
- Banks 'wasting millions' on two-factor authentication（銀行らは二要素認証で億単位の金をドブに捨てている）, The Register, 2005年3月15日
- More on Two-Factor Authentication, Crypto-Gram Newsletter, 2005年4月15日

そして2006年7月、米国のCitibankをターゲットとした中間者攻撃によるフィッシングが現れ、二要素認証が役に立たなかったということで騒動になった。

- Citibank Phish Spoofs 2-Factor Authentication, washingtonpost.com blog, Brian Krebs on Computer Security, 2006年7月10日
- Man-in-the-middle attacks Citi authentication system, Finextra Research, 2006年7月12日
- ワンタイム・パスワードでは防げない"中間者攻撃フィッシング"が出現, 日経IT Pro, 2006年7月13日
- Man-in-the-middle attack on Citibank users concerns experts, SC Magazine US, 2006年7月14日
- Phishers Beat Citi's Two-Factor Authentication, Bank Systems & Technology, 2006年7月18日
- Phishing and forward looking financial institutions, Financial Services Tecnology US edition, 日付不明

2007年1月には、中間者攻撃型フィッシングの構築キットが現れていると、RSA Securityが警告を出している。

報道例（英国, 2012年）

これまで・これから

- 十数年前：パスワード窃取対策
  - 2要素認証の導入（ワンタイムトークン、乱数表の併用）
  - 2要素認証を突破する中間者攻撃が実際に発生（2006年）
- これまで：フィッシング対策（偽サイト対策）
  - サーバ・クライアント間の相互認証で中間者攻撃の防止を提案
  - しかし、マルウェア感染には無力
  - 「Man-in-the-Browser攻撃」が現実に発生
- これから：マルウェア対策が必要
  - しかし、感染前提で全て防衛するのは原理的に無理
    - 例えば、盗み見されるのは防げない
  - 取引の処理だけは死守するという割り切り

解決策「ZTIC」

- ZTIC - IBM Zurich Research Laboratory（2008年）

IBM Research – Zurich | Computer Science | Security | IBM Zone Trusted Information Channel (ZTIC)

www.zurich.ibm.com/ztic/

Switzerland | Welcome [IBM Sign in / Register]

IBM | Industries & solutions | Services | Products | Support & downloads | My IBM | Search

← IBM Research

IBM Research - Zurich

COMPUTER SCIENCE

- Services research
- Systems management
- Distributed computing
- Business integration technologies
- Security
  - Secure ID solutions
  - Data storage security
  - Identity governance
  - BlueZ business computing
  - **Internet transaction security ZTIC**
    - Usage of ZTIC

IBM Zone Trusted Information Channel (ZTIC)

A banking server's display on your key chain

More and more attacks to online banking applications target the user's home PC, changing what is displayed to the user, while logging and altering key strokes. Therefore, third parties such as MELANI conclude that *"Two-factor authentication systems [...] do not afford protection against such attacks and must be viewed as insecure once the computer of the customer has been infected with malware".*

In a widely published real-world example of the Trojan "Silent banker", Symantec states that *"The ability of this Trojan to perform man-in-the-middle attacks on valid transactions is what is most worrying. The Trojan can intercept transactions that require two-factor authentication. It can then silently change the user-entered destination bank account details to the attacker's account details instead."*

In order to foil these threats, IBM has introduced the Zone Trusted Information Channel (ZTIC), a hardware device that can counter these attacks in an easy-to-use way. The ZTIC is a USB-attached device containing a display and minimal I/O capabilities that runs the full TLS/SSL protocol, thus entirely bypassing the PC's software for all security functionality.

The ZTIC achieves this by registering itself as a USB Mass Storage Device (thus requiring no driver installation) and starting a "pass-through" proxy configured to connect with pre-configured

Figure 1. Information flow of the ZTIC. The secure channel is opened between the (bank's) server and the ZTIC. The user communicates as usual with

当時の報道（2008年）

世界のセキュリティ・ラボから – Webブラウザを狙う中間者攻撃の対抗手段「ZTIC」：ITpro

itpro.nikkeibp.co.jp/article/COLUMN/20081117/319336/

ビッグデータ | 中国・アジア | ITpro まとめ

- CMO（Chief Marketing Officer）
- 医療IT

執筆者 一覧

記事カテゴリ

- ITpro全記事一覧
- 特集
- ニュース
- 連載
- インタビュー
- 事例
- キーワード
- イベント
- 週末スペシャル
- CIO
- Computerworld

イベントINFO -PR-

RSS | メルマガ

特番/イベント

テクノインパクト

世界のセキュリティ・ラボから　日経コミュニケーション

Webブラウザを狙う中間者攻撃の対抗手段「ZTIC」

2008/11/19

記事一覧へ >> | シェア | いいね！ 0 | ツイート 0 | +1 0 | B! 26

FREQUENCY X

STRAIGHT DOPE ON THE VULNERABILITY DU JOUR FROM **IBM Internet Security Systems**

「Beating the Man-in-the-browser with a ZTIC」より
October 29、2008 Posted by Gunter Ollmann

Webブラウザを狙う中間者攻撃についてご存知ない方のために まず説明しておこう。昔からあるMan-in-the-Middle（中間者）攻撃を、ずる賢くもWebブラウザ向けに特化させ、攻撃用コード（一般的にスクリプト対応プロキシ技術が使われる）をWebブラウザに仕掛ける攻撃手法が存在する。この攻撃を受けたWebブラウザは、最終的に中核機能を掌握され、送受信するデータが攻撃者に筒抜けとなり、好きなようにデータを操作されてしまう。

この種の手口は「Man-in-the-Browser（Webブラウザを狙う中間者）攻撃」と呼ばれ、2年前に初めて登場して以来、銀行を狙ったトロイの木馬で使われる例が増えてきている。

- チェックしておきたい脆弱性情報 <2014.03.12>
- Bitcoin事件のポイントを読み解く、あなたは何に用心すべきか
- 「Intel Security」になっても戦略は変わらない、マカフィー社長

CIO | COMPUTERWORLD

セキュリティ　いま読まれている記事

1. 【ニュース】IEのゼロデイ脆弱性を修正するパッチが公開、すぐに適用を
2. 【ニュース】「商品が破損していた！」クレームに見せかけたウイルスメールに注意
3. 【西本逸郎のIT社会サバイバル術】Bitcoin事件のポイントを読み解く、あなたは何に用心すべきか
4. 【ニュース】ANAマイレージクラブへの不正ログインで112万マイルが詐取、住所なども閲覧可能に
5. 【世界のセキュリティ・ラボから】偽Skype通知で攻撃ツールに誘導する手口が増加中

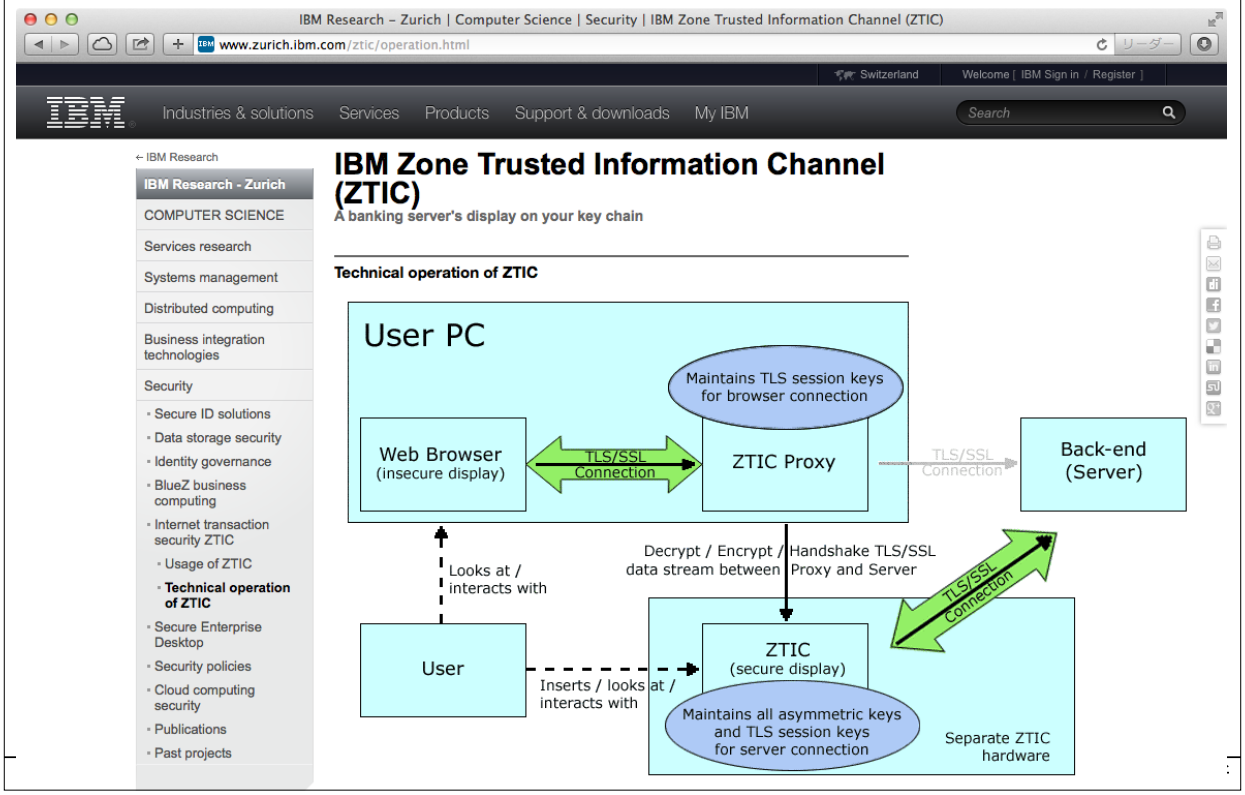
Facebookもチェック

ITpro | いいね！

18,181人がITproについて「いいね！」と言っています。

解決策「ZTIC」

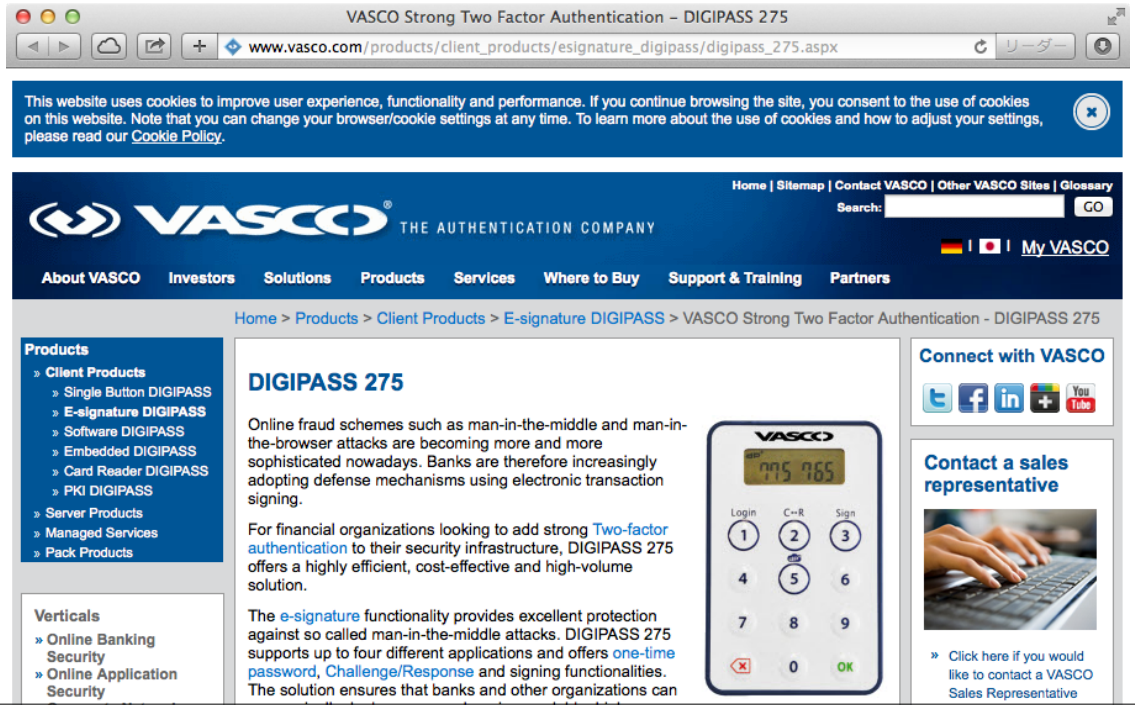
解決策「ZTIC」



AIST

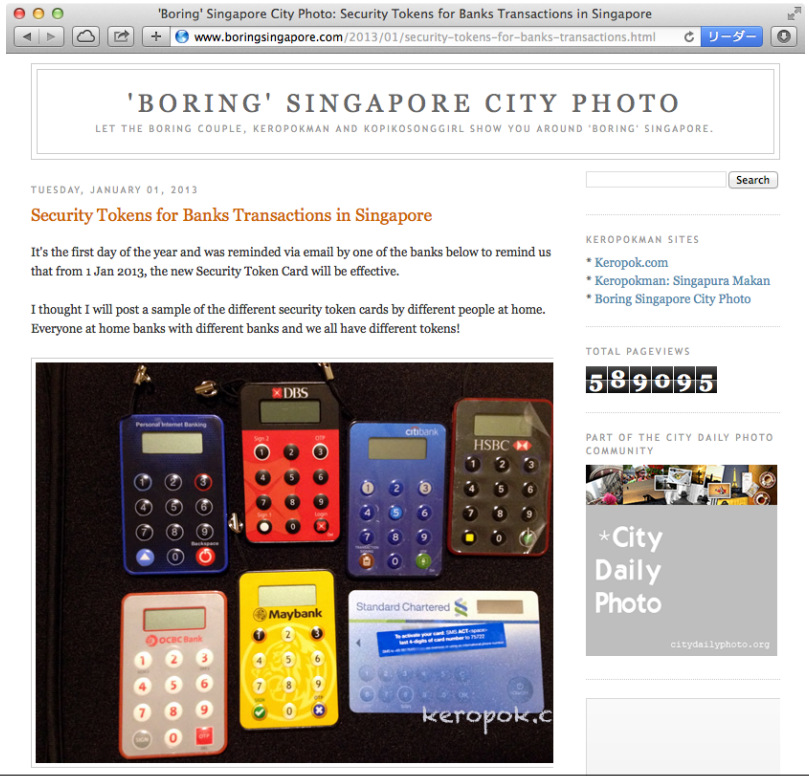
解決策「DIGIPASS」

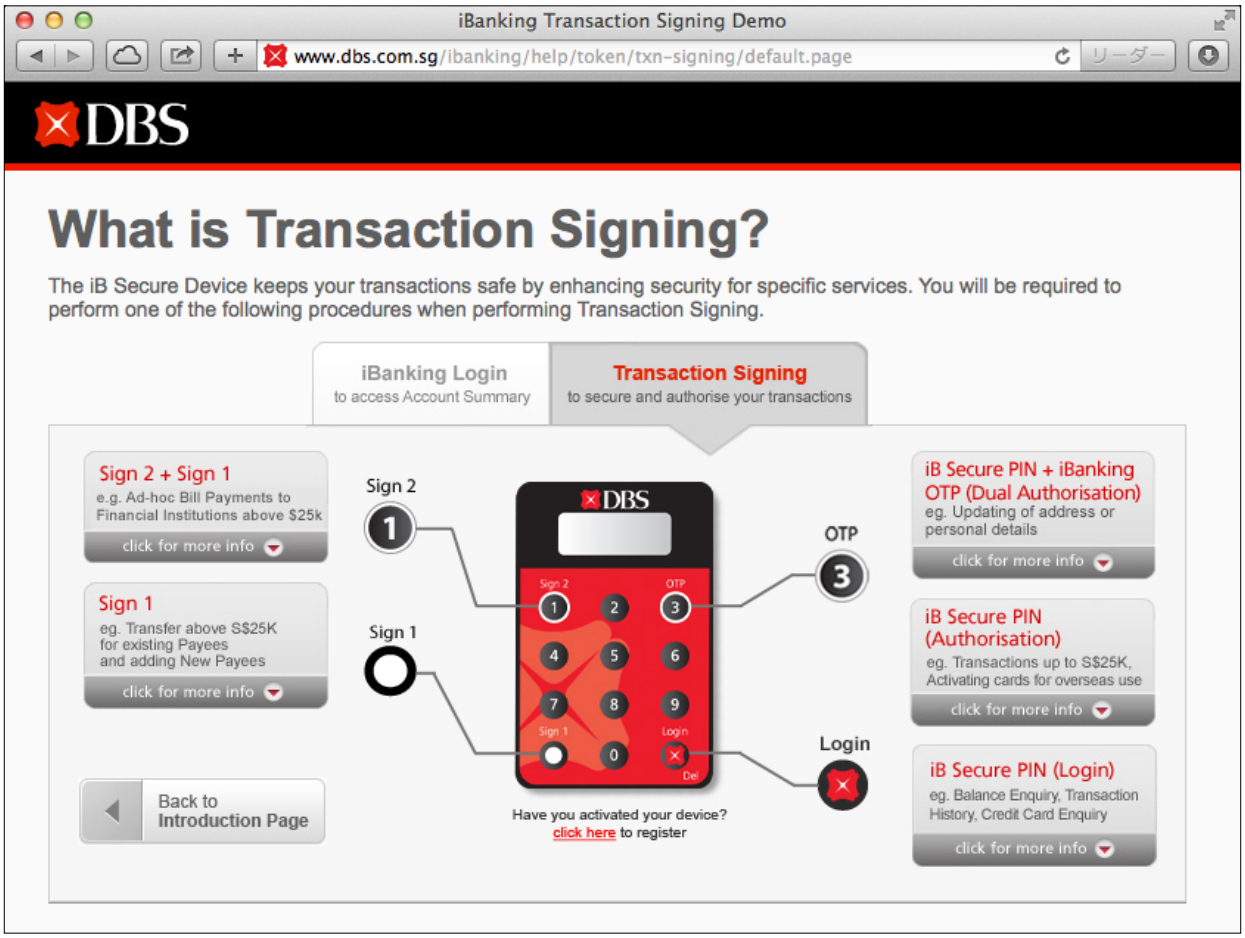
- DIGIPASS 270/275/320 - VASCO Data Security（2011年）

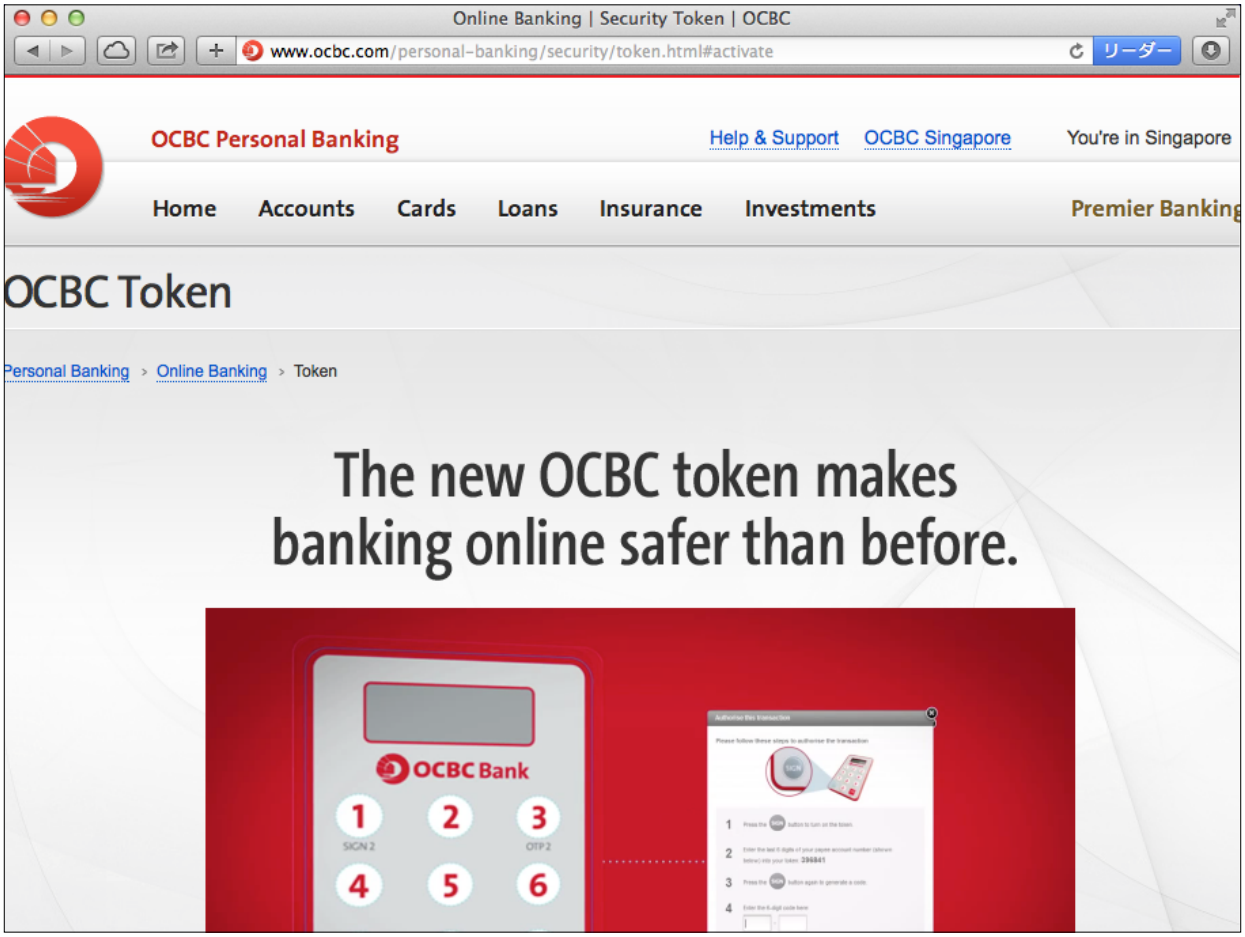


AIST

シンガポールでの普及状況

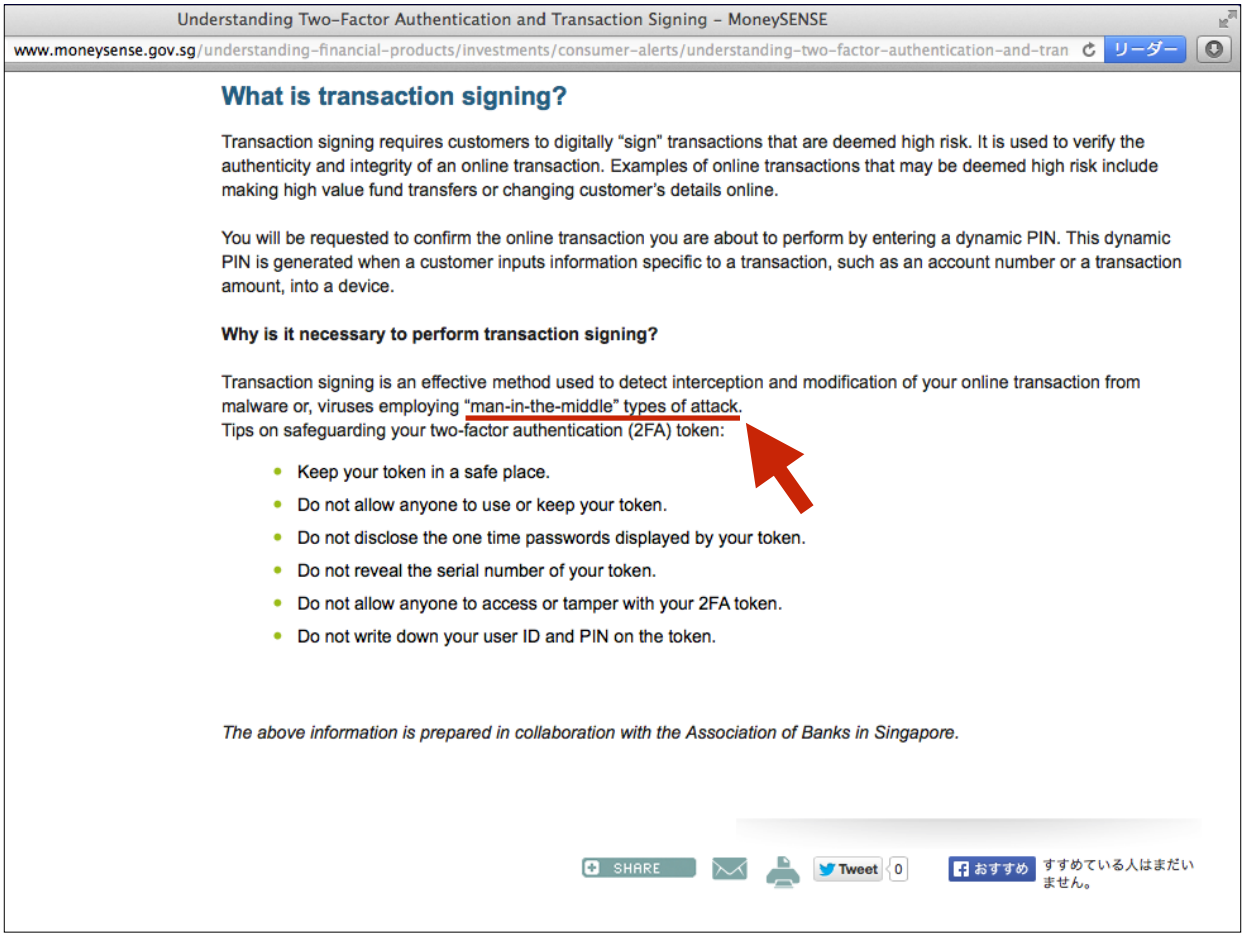



iBanking Transaction Signing Demo
www.dbs.com.sg/ibanking/help/token/txn-signing/default.page
DBS
What is Transaction Signing?
The iB Secure Device keeps your transactions safe by enhancing security for specific services. You will be required to perform one of the following procedures when performing Transaction Signing.
iBanking Login
to access Account Summary
Transaction Signing
to secure and authorise your transactions
Sign 2 + Sign 1
e.g. Ad-hoc Bill Payments to Financial Institutions above $25k
click for more info
Sign 1
eg. Transfer above S$25K for existing Payees and adding New Payees
click for more info
Back to Introduction Page
Sign 2
Sign 1
OTP
Login
Have you activated your device?
click here to register
iB Secure PIN + iBanking OTP (Dual Authorisation)
eg. Updating of address or personal details
click for more info
iB Secure PIN (Authorisation)
eg. Transactions up to S$25K, Activating cards for overseas use
click for more info
iB Secure PIN (Login)
eg. Balance Enquiry, Transaction History, Credit Card Enquiry
click for more info

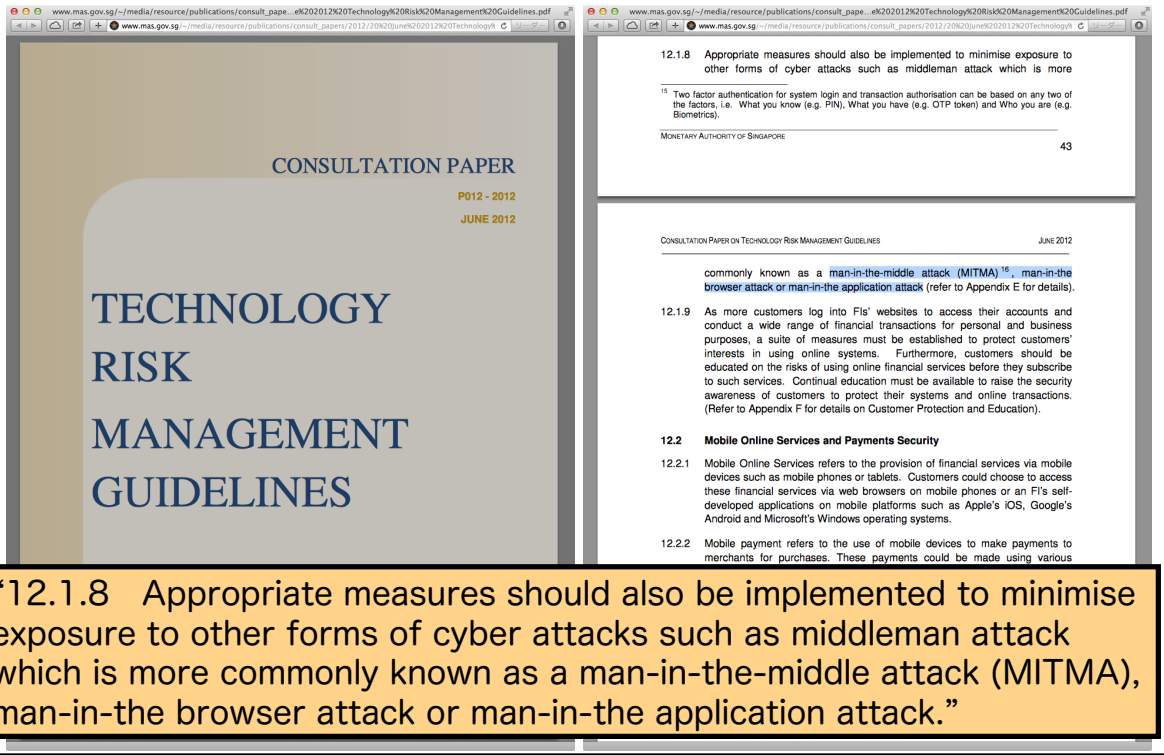

Online Banking | Security Token | OCBC
www.ocbc.com/personal-banking/security/token.html#activate
OCBC Personal Banking
Help & Support
OCBC Singapore
You're in Singapore
Home
Accounts
Cards
Loans
Insurance
Investments
Premier Banking
OCBC Token
Personal Banking › Online Banking › Token
The new OCBC token makes banking online safer than before.
OCBC Bank

シンガポール政府の教育プログラム

- シンガポール金融管理局



シンガポール金融管理局のガイドライン



CONSULTATION PAPER

P012 - 2012

JUNE 2012

TECHNOLOGY RISK MANAGEMENT GUIDELINES

12.1.8 Appropriate measures should also be implemented to minimise exposure to other forms of cyber attacks such as middleman attack which is more commonly known as a man-in-the-middle attack (MITMA)[15], man-in-the browser attack or man-in-the application attack (refer to Appendix E for details).

[15] Two factor authentication for system login and transaction authorisation can be based on any two of the factors, i.e. What you know (e.g. PIN), What you have (e.g. OTP token) and Who you are (e.g. Biometrics).

MONETARY AUTHORITY OF SINGAPORE 43

CONSULTATION PAPER ON TECHNOLOGY RISK MANAGEMENT GUIDELINES JUNE 2012

commonly known as a man-in-the-middle attack (MITMA)[16], man-in-the browser attack or man-in-the application attack (refer to Appendix E for details).

12.1.9 As more customers log into FIs' websites to access their accounts and conduct a wide range of financial transactions for personal and business purposes, a suite of measures must be established to protect customers' interests in using online systems. Furthermore, customers should be educated on the risks of using online financial services before they subscribe to such services. Continual education must be available to raise the security awareness of customers to protect their systems and online transactions. (Refer to Appendix F for details on Customer Protection and Education).

12.2 Mobile Online Services and Payments Security

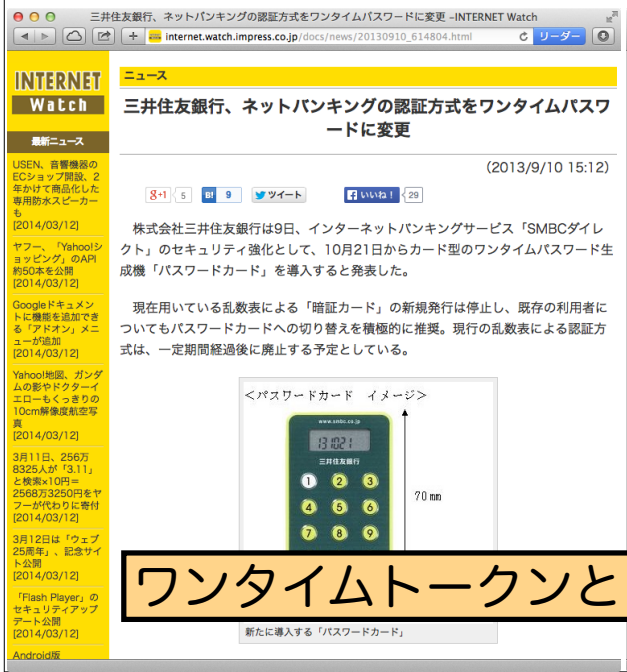
12.2.1 Mobile Online Services refers to the provision of financial services via mobile devices such as mobile phones or tablets. Customers could choose to access these financial services via web browsers on mobile phones or an FI's self-developed applications on mobile platforms such as Apple's iOS, Google's Android and Microsoft's Windows operating systems.

12.2.2 Mobile payment refers to the use of mobile devices to make payments to merchants for purchases. These payments could be made using various

"12.1.8 Appropriate measures should also be implemented to minimise exposure to other forms of cyber attacks such as middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack."

三井住友銀行が採用したもの

- 昨年9月の報道



三井住友銀行、ネットバンキングの認証方式をワンタイムパスワードに変更 -INTERNET Watch

internet.watch.impress.co.jp/docs/news/20130910_614804.html

INTERNET Watch

ニュース

三井住友銀行、ネットバンキングの認証方式をワンタイムパスワードに変更

(2013/9/10 15:12)

株式会社三井住友銀行は9日、インターネットバンキングサービス「SMBCダイレクト」のセキュリティ強化として、10月21日からカード型のワンタイムパスワード生成機「パスワードカード」を導入すると発表した。

現在用いている乱数表による「暗証カード」の新規発行は停止し、既存の利用者についてもパスワードカードへの切り替えを積極的に推奨。現行の乱数表による認証方式は、一定期間経過後に廃止する予定としている。

<パスワードカード イメージ>

70 mm

新たに導入する「パスワードカード」

三井住友銀行がネットバンキングでワンタイムパスワード…入へ | スラッシュドット・ジャパン セキュリティ

security.slashdot.jp/story/13/09/10/0439205/

Slashdot

三井住友銀行がネットバンキングでワンタイムパスワードを導入へ

ストーリー by hylom 2013年09月11日 6時00分
ネットゲーマーにはおなじみのアレ 部門より

三井住友銀行が、ネットバンキングにおいてワンタイムパスワードの導入を行うとのこと（MSN産経ニュース）。ワンタイムパスワードはオンラインゲームのログイン認証などでは広く普及しているが、国内の銀行で本格的に導入されるのは初めてという。

新規契約者だけでなく、既存の契約者も対象。パスワードを生成するデバイスはカード型電卓のような形状をしており、60秒ごとに使い捨てのパスワードを生成するもの。顧客に対し無料で配布されるという。近年ネットバンキングを狙った攻撃が増えていることからの導入のようだ。

66コメント

security セキュリティ

関連リンク

ワンタイムパスワード生成機能付きクレジットカード
Google のトークン認証システム、オープンソースで公開中
FF11などでワンタイムパスワード認証が利用可能に
ワンタイムパスワード生成カードが登場
システム化される銀行の「反社会的勢力」対策
タレコミ：三井住友銀行がネットバンキングでワンタイムパスワードを導入へ、ジャパンネット銀行以来の

ワンタイムトークンとしてしか話題にならず

ニュースリリース ： 三井住友銀行

www.smbc.co.jp/news/j600777_01.html

今般、更なる強化策として、カード型ワンタイムパスワード生成機「パスワードカード」を導入します。『ＳＭＢＣダイレクト』を新規に契約される全てのお客さま、及び既存のご契約者で切り替えを希望されるお客さまには「パスワードカード」を無料で提供し、「パスワードカード」をご利用のお客さまについては、振込等の重要取引等を実施する際の本人認証をワンタイムパスワードのみとします。今回導入する「パスワードカード」は、従来のパスワード生成機よりも携行性に優れ、将来的な不正取引対策への拡張性（*4）も兼ね備えています。本対策によりお客さまの利便性に配慮しつつ、更なるセキュリティの強化を図ります。

なお、暗証カードの新規発行は停止し、既存ご契約中のお客さまにつきましても「パスワードカード」への切り替えを積極的に推奨し、現行の認証方式は一定期間経過後に廃止する予定です。

	現行		変更後
名称	暗証カード	パスワード生成機	パスワードカード
利用対象者	契約者全員	希望者のみ	契約者全員
認証方式	乱数表	ワンタイムパスワード	ワンタイムパスワード
実物イメージ		 ※暗証カードと併用が必要	

次のページ

Man-in-the-Browser対策との説明はない

ジの先頭へ戻る

サイトのご利用にあたって | アクセシビリティ | プライバシーポリシー | セキュリティ

三井住友フィナンシャルグループ　三井住友銀行

21

Citibank | トークン型ワンタイムパスワードサービス | シティバンク銀行

Citibank Japan Ltd. www.citibank.co.jp/banking/services/cap/otp/index.html?tab=citibank

Citibank Japan

閉じる

citi

※イメージ

重要なお知らせ

ワンタイムパスワード（OTP）サービスは、
「eメール型」から「トークン型」に
変わりました。

ワンタイムパスワード（OTP）サービス

ワンタイムパスワード（OTP）は、シティバンク オンラインで、事前に振込先登録をしていない口座へのお振込み（都度振込）、キャッシュカードの暗証番号変更、ご登録情報の変更等、各種お手続きを行う際にご入力いただく使い捨てパスワードです。セキュリティの高い6桁の数字で組合わされており、インターネットバンキング（シティバンク オンライン）にて第三者に不正利用されるリスクを抑えることができます。

シティバンクでは、お客様により安全にシティバンク オンラインをご利用いただくために、従来の「eメール型OTPサービス」を終了し、「トークン型OTPサービス」を開始いたしました。

22


Citibank | トークン型ワンタイムパスワードサービス | シティバンク銀行
Citibank Japan Ltd.
www.citibank.co.jp/banking/services/cap/otp/index.html?tab=citibank
1 トークンとは？
2 トークンのお申込み方法
3 よくある質問
4 ご注意
3 よくある質問
なぜ、トークン型のワンタイムパスワード（OTP）サービスを導入したのですか？
当行では、eメール型のOTPサービスを提供しておりましたが、お客様にさらにセキュリティの高いお取引をご提供するため、トークン型OTPサービスを導入いたしました。
インターネットバンキングのID・パスワード等を盗み取るウィルスを使用するなどして、インターネットバンキングに不正にアクセスして送金を行うなど、金融犯罪の手口が高度化していることから、警察庁はこのような手口による不正送金を防止する手段として、トークンによるOTPの利用を呼びかけています。
なぜ、eメール型のワンタイムパスワード（OTP）サービスを終了したのですか？
お客様が、シティバンク オンラインでお取引をされる際に必要なOTPを確実にお届けし、かつより安全な方法でのお取引をご提供するために、eメール型OTPサービスについては、トークン型OTPサービスの導入をもって終了させていただきました。
Man-in-the-Browser対策との説明はない

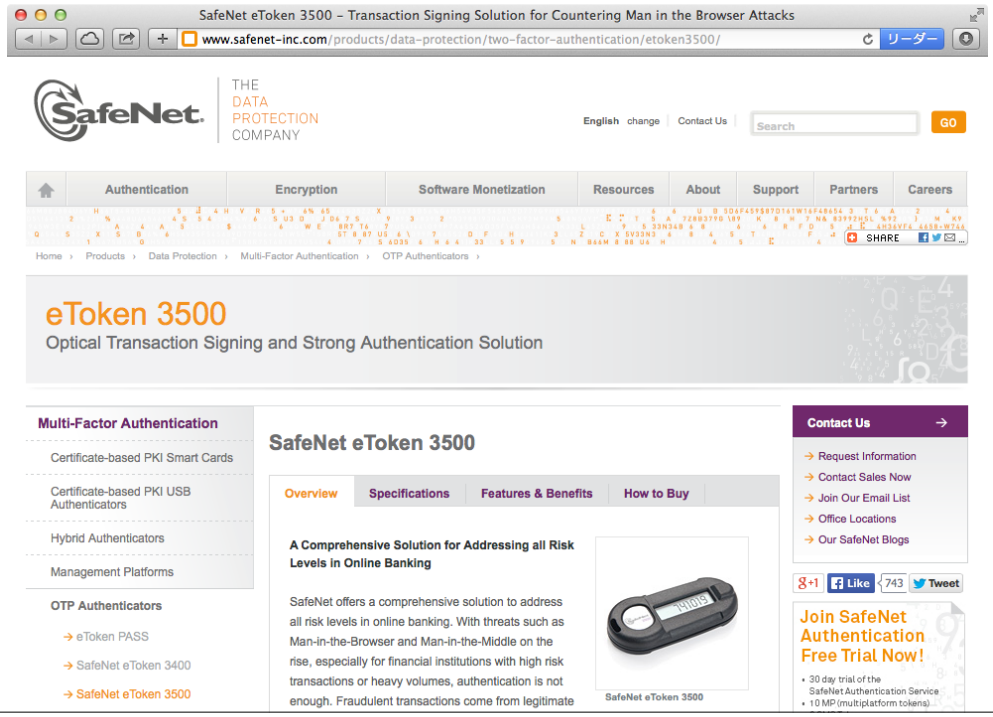

Sumitomo Mitsui Banking Corporation (SMBC) is one of the largest banks in the world. More than 22,000 employees guard the bank's mission: providing valuable services that help its customers to build their own prosperity, to create sustainable value for its shareholders founded on growth in their business, and provide a challenging and professional rewarding working environment for its dedicated employees.
SMBC
A GROWING NUMBER OF FRAUD CASES
The number of criminalities, fraud cases and incidents on the Internet, such as phishing and man-in-the-middle attacks, is growing very fast, also in Japan. In the last few years, not only financial institutions but also many other organizations have been targeted. In this environment, SMBC realized it had to consider a more sophisticated security measurement to protect its Internet banking services. The bank called in a consultancy company, so that an independent third party could evaluate a range of different security solutions, such as static passwords, table of random digits (TAN), one-time passwords, risk-based authentication and browser/malware detecting solutions.
The most imperative points for the bank were the ease of understanding and user-friendliness, the possibility to share the security model with its affiliate financial companies and the implementation of a future-proof solution that could withstand future advanced attacks. In the end, VASCO's DIGIPASS technology proofed to be the solution that met all requirements.
EASY, CONVENIENT AND INTUITIVE
The most adjusted solution to meet the above requirements was VASCO's DIGIPASS 275. "We concluded that a risk-based solution or a browser/malware detection solution would be too cumbersome for our users," said Hirohito Yokoyama, Group Head of Retail Banking department of SMBC. "With the customer in mind, we looked for a more intuitive and portable solution. Of course, it needed to be a proven solution able to protect our users from advanced fraud schemes, such as man-in-the-browser attacks."
the DIGIPASS
device can su
VASCO社資料より
KEEP AN EYE ON THE BUDGET
"Of course, there were also some non-technical requirements. The cost and the time-to-market in short terms were also indispensable points to select the right vendor," explains Yuji Konishi, Manager of Retail banking department of SMBC. "The internal coordination of the departments was a very challenging project, because this has been the biggest innovation since we started the direct Internet banking service ten years ago."
SMBC plans to replace its existing authentication service, TAN lists, to VASCO's DIGIPASS 275. Their customers can get a DIGIPASS in their numerous branches, free of charge.
Yuji Konishi, Manager of Retail banking department of SMBC, has faith in the solution: "We are very happy with DIGIPASS 275: it is portable in our wallets, design-oriented and a functionally high-evaluated product. Moreover, VASCO's proven records in global rollouts for the financial industry is also a plus-point. We highly evaluate VASCO's solutions, so we trust it when unknown attacks in the future arise."
www.smbc.co.jp
三井住友銀行

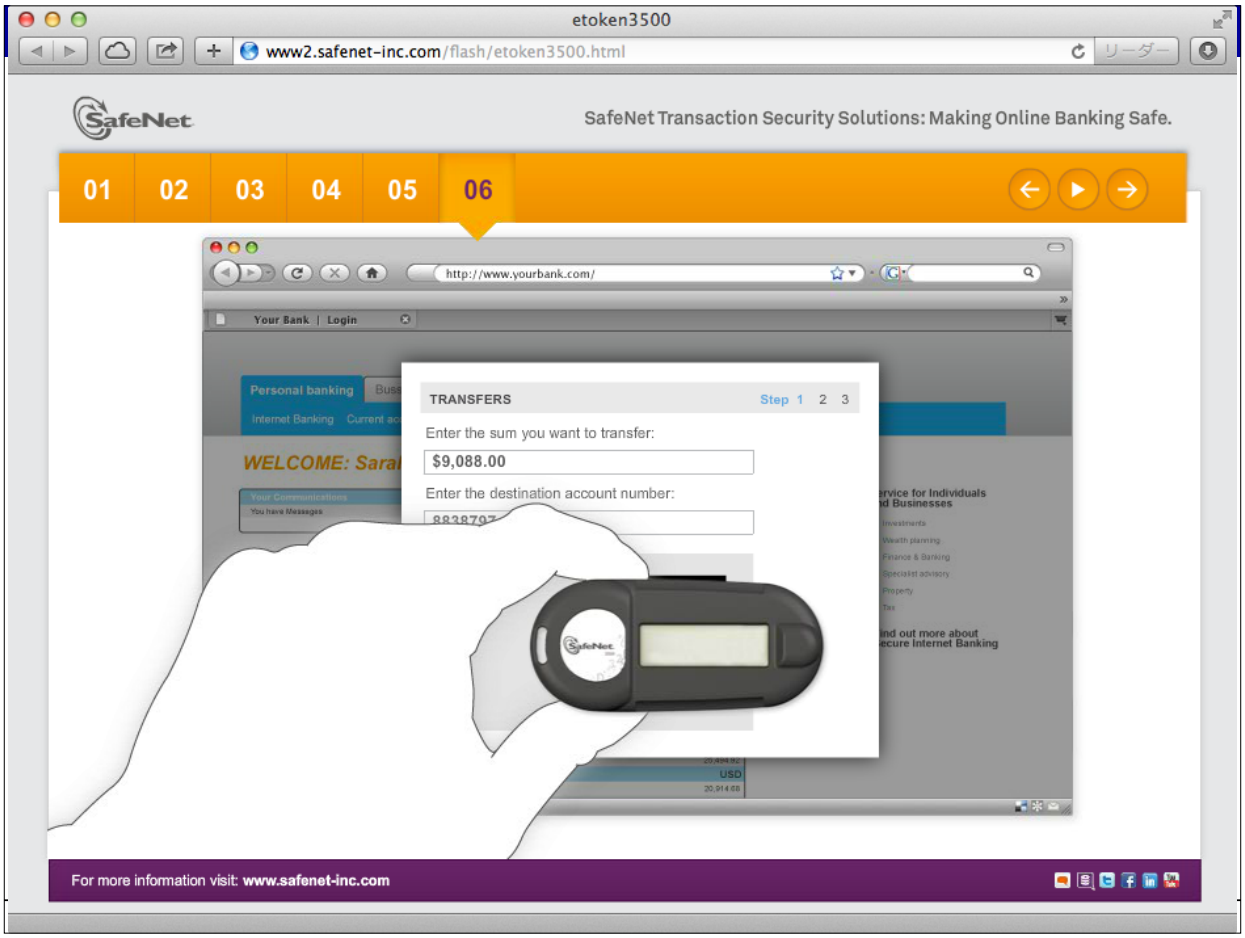
今後導入される可能性

- 現状
  - 被害の大半がwebinjectによる偽画面生成
    - パスワードと乱数表の値を盗まれている
  - 真のMan-in-the-Browser攻撃はあまり来ていない
  - まずは送金時のワンタイムパスワード認証で防げる
- 今後
  - 真のMan-in-the-Browser攻撃が流行し始めると
  - 送金時のワンタイムパスワード認証では防げない
    - 送金先を差し替えられてしまうので
  - 配布済みトークン（カード）の機能を使う
  - ウェブアプリ側での機能対応が必要
    - 送金の操作に手順が追加される

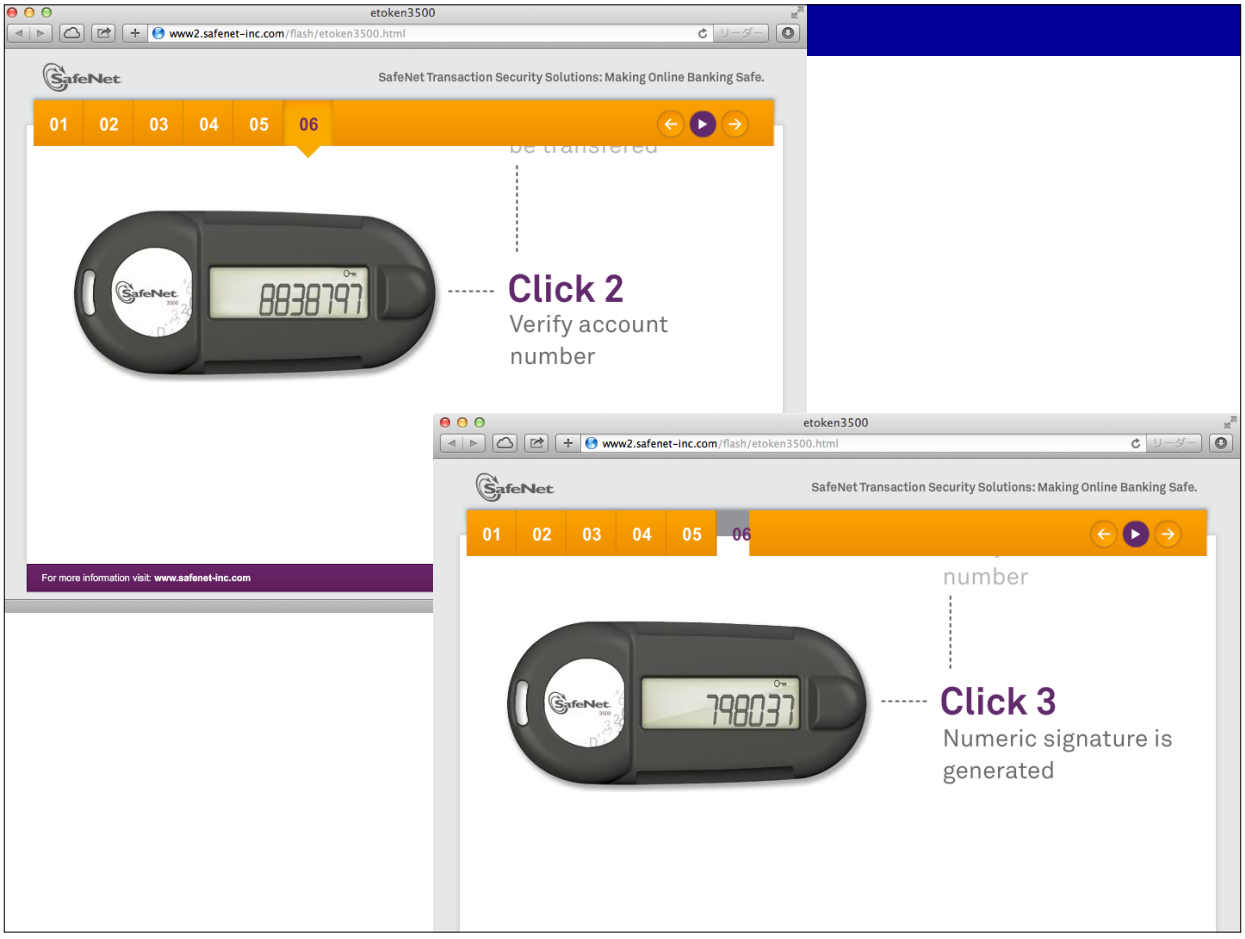
解決策「eToken 3500」

- eToken 3500 - SafeNet（2011年）




etoken3500
www2.safenet-inc.com/flash/etoken3500.html
SafeNet Transaction Security Solutions: Making Online Banking Safe.
01 02 03 04 05 06
http://www.yourbank.com/
Your Bank | Login
Personal banking
TRANSFERS
Step 1 2 3
Enter the sum you want to transfer:
$9,088.00
Enter the destination account number:
For more information visit: www.safenet-inc.com

27


etoken3500
www2.safenet-inc.com/flash/etoken3500.html
SafeNet Transaction Security Solutions: Making Online Banking Safe.
01 02 03 04 05 06
8838797
Click 2
Verify account number
For more information visit: www.safenet-inc.com
etoken3500
www2.safenet-inc.com/flash/etoken3500.html
SafeNet Transaction Security Solutions: Making Online Banking Safe.
01 02 03 04 05 06
number
798037
Click 3
Numeric signature is generated

28

セーフネット、光学センサーで独自の電子署名を生成するトークン - クラウド Watch

cloud.watch.impress.co.jp/docs/news/20120209_510846.html

クラウド Watch

記事検索

検索

2014年3月12日

インタビュー Salesforce 1で進化するService Cloudの現状～米salesforce.com バードSVPに聞く [2014/03/12]

MSが3月の月例パッチ公開、IEのゼロデイ脆弱性の修正など計5件 [2014/03/12]

サイボウズのクラウドサービス無料相談窓口「導入相談Cafe」がオープン [2014/03/12]

クラウドの運用手順書から運用フローを自動生成、富士通研が新技術 [2014/03/12]

ウイングアーク、PDF帳票保管ツール「SVF PDF Archiver」にWeb APIを追加 [2014/03/12]

セーフネット、光学センサーで独自の電子署名を生成するトークン

不正な金融取引を防止

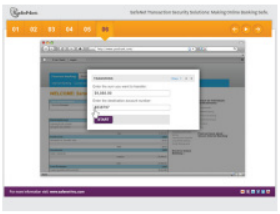
2012年2月

日本セーフネット株式会社は9日、ID保護・トランザクション保護を実現する光学署名デバイス「SafeNet eToken 3500」を発表した。国内では14日より販売する。

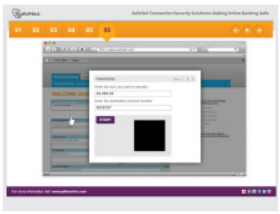
SafeNet eToken 3500は、Webで金融取引を行う際に、光学センサーを利用して独自の電子署名を生成する製品。トークンに表示されるワンタイムパスワード（OTP）で金融Webサイトにアクセスし、例えば、送金を行おうとすると、画面上に点滅するボックス画面が表示される。SafeNet eToken 3500を画面に向けてかざすと光学センサーが暗号化された金融取引の詳細を読み込み、独自の電子署名を生成。それをWebブラウザに入力することで、取引が有効であることが確認される。

SafeNet eToken 3500

OTPでユーザーを認証し、電子署名で各トランザクションが認証されるため、これら組み合わせによって、ユーザーの不正ななりすましや取引中にハッカーが送金先を変更する「Man-in-the-Browser（MinB）攻撃」などの脅威が減少される。また、デバイスの光学機能が取引データを自動スキャンするため、手動による入力は必要なく、入力ミスと手間を削減できるという。



OTPでログイン後、送金額とユーザーアカウントを入力



光学センサーで読み取るためのボックス（点滅）が表示される

AIST

方式の比較

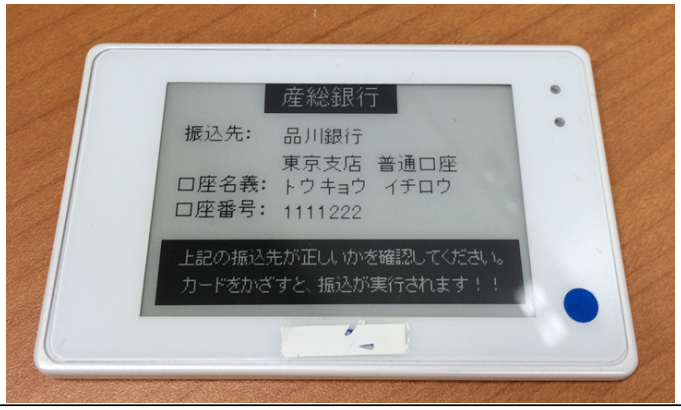
- 回線割り込み方式（IBM ZTIC）
  - 中継する口座番号を目視確認し、OKボタンで許可
- 手入力MAC表示方式（VASCO DIGIPASS）
  - 口座番号等を手入力し、メッセージ認証コードを計算、結果をWebに手入力
- 目視確認MAC表示方式（SafeNet eToken）
  - 自動転送される口座番号を目視確認し、OKボタンを押して、メッセージ認証コードを計算、結果をWebに手入力
- 目視確認MAC転送方式（？）
  - 自動転送される口座番号を目視確認し、OKボタンを押して、メッセージ認証コードを計算、結果を転送

残る問題

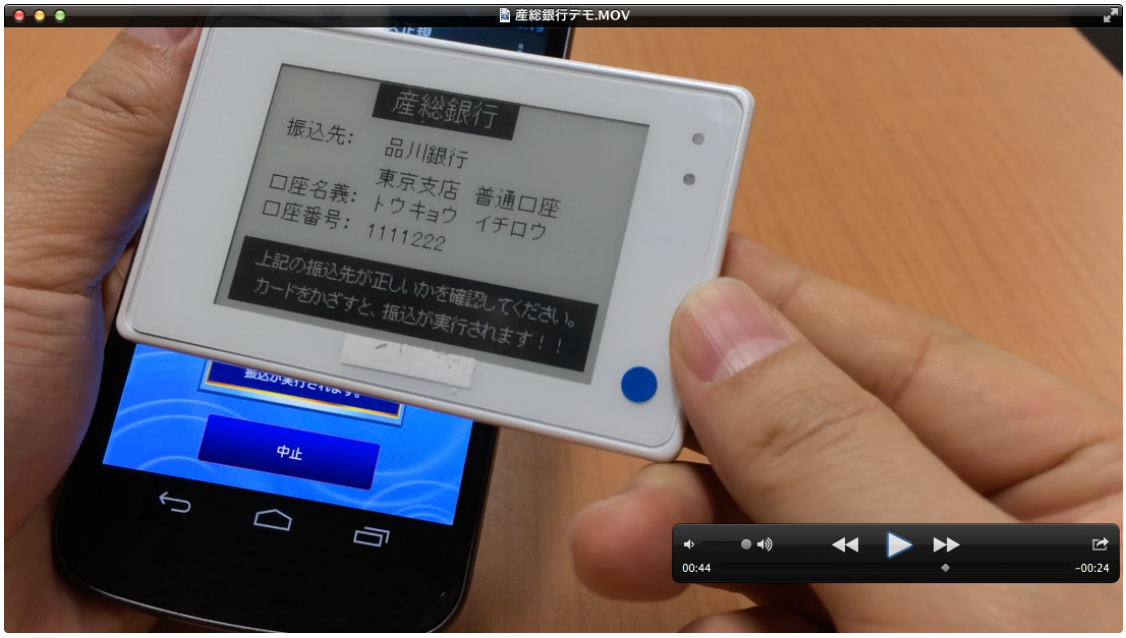
- 住所変更をどうするか
  - 本人が住所変更の操作中に、Man-in-the-Browser攻撃され、変更先住所を差し替えられる脅威
  - 不正に変更された住所にトークンが送付されてしまう
- 解決策
  - 変更先の住所も目視確認できるようにする？
    - どうやって表示する？
  - 数字だけを入力してMAC生成する？
    - 郵便番号と番地の保証だけで安全？
  - 連絡先電話番号を用いて何かする？
    - 電話番号の変更を同様の方法で安全に行い、
    - そこに電話をかけて住所変更を安全に行う？

我々の研究開発

- 前提
  - スマホ時代を想定
  - NFC（近距離無線通信）を利用する
- 特徴
  - 電子ペーパーを利用（NFC電源）
- 試作品



デモ「産総銀行アプリ」

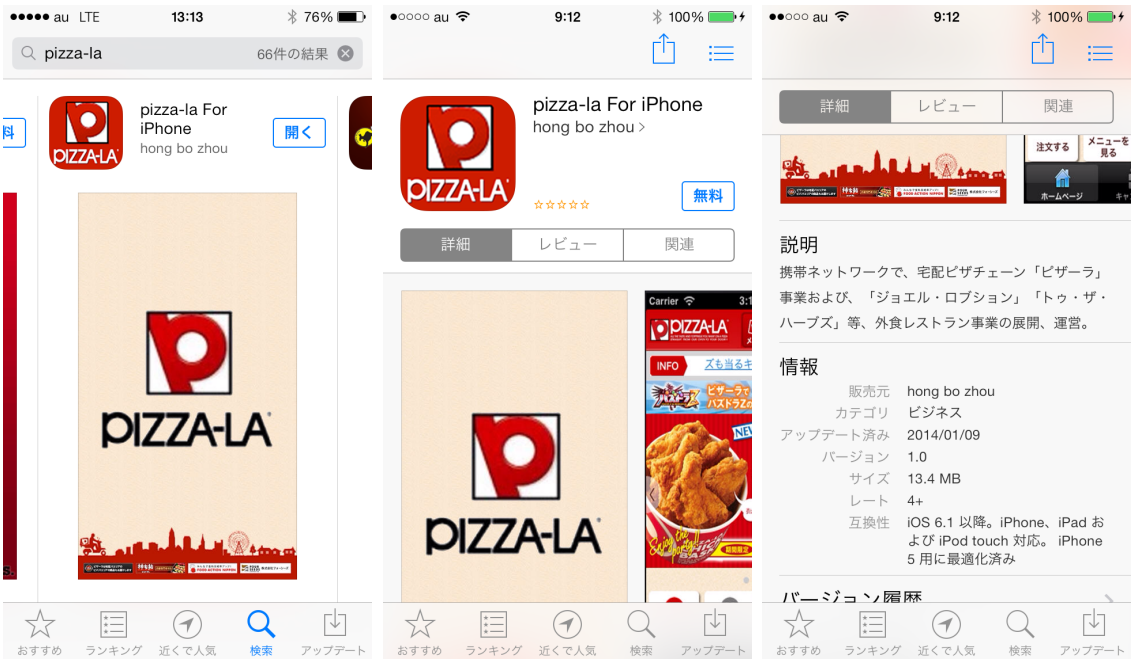


偽アプリの問題

- スマホにおける脅威
  - ウイルス感染？
    - アプリごとに隔離されているためPCほどの脅威ではない
      - OSの脆弱性を突かれない限り
  - 偽アプリの可能性
    - 偽アプリを確実に見分ける方法が存在しない
    - PhishingのようにURLのドメイン名で見分ける的な方法がない
- 偽アプリの脅威
  - 正規アプリの挙動そのままに送金先を差し替えるなど
    - Man-in-the-Browserと同等のことができてしまう

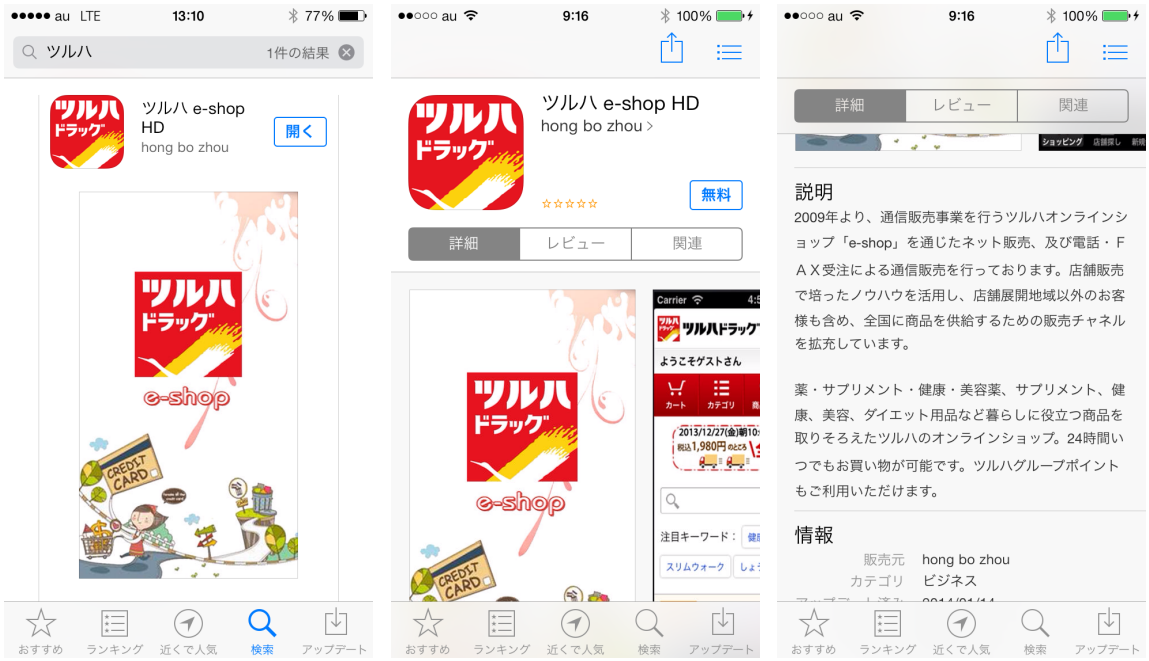
偽アプリの例

- 2014年1月に発覚

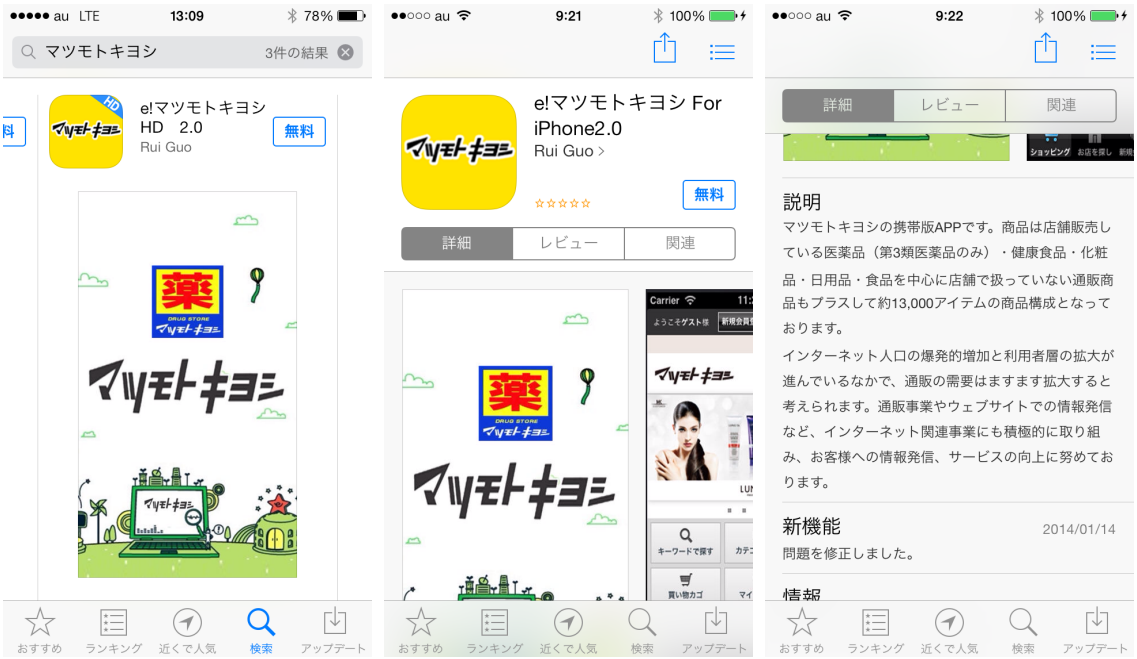


偽アプリの例

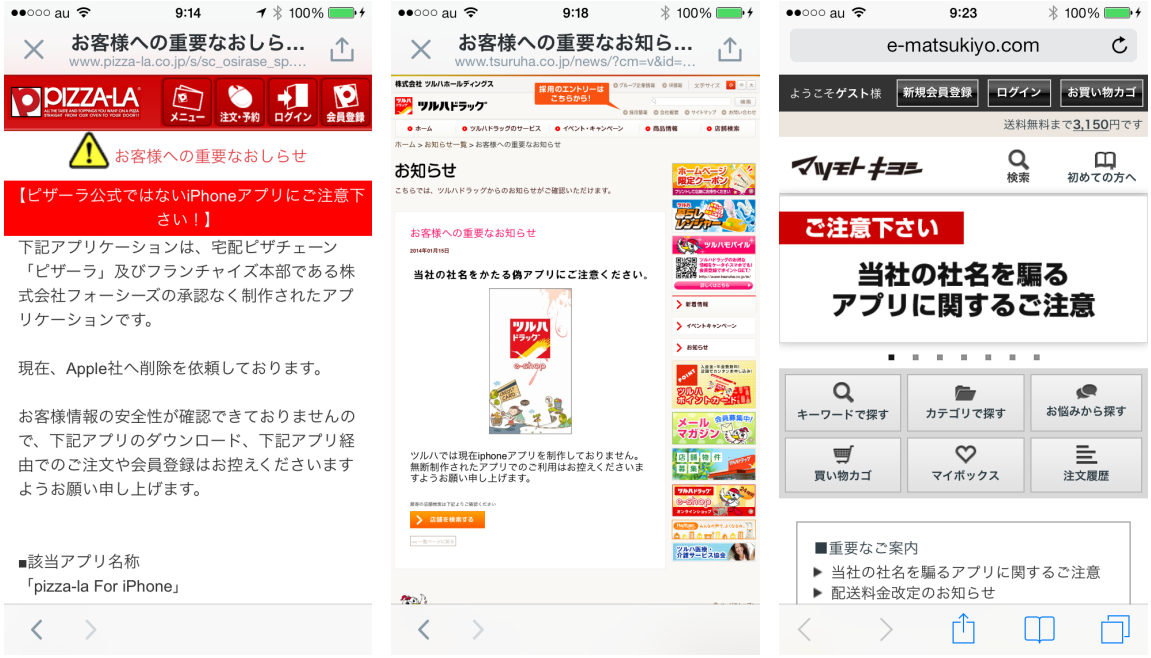
- 店名での検索結果に現れる



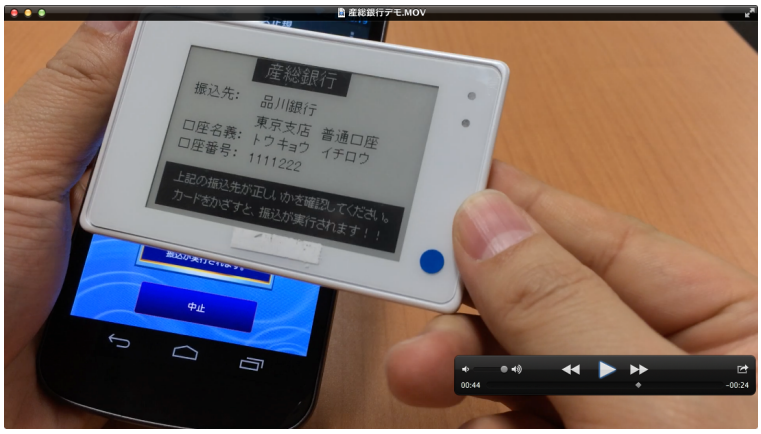
偽アプリの例


マツモトキヨシ
3件の結果
e!マツモトキヨシ HD 2.0
Rui Guo
無料
e!マツモトキヨシ For iPhone2.0
Rui Guo >
詳細
レビュー
関連
説明
マツモトキヨシの携帯版APPです。商品は店舗販売している医薬品（第3類医薬品のみ）・健康食品・化粧品・日用品・食品を中心に店舗で扱っていない通販商品もプラスして約13,000アイテムの商品構成となっております。
インターネット人口の爆発的増加と利用者層の拡大が進んでいるなかで、通販の需要はますます拡大すると考えられます。通販事業やウェブサイトでの情報発信など、インターネット関連事業にも積極的に取り組み、お客様への情報発信、サービスの向上に努めております。
新機能
2014/01/14
問題を修正しました。
おすすめ
ランキング
近くで人気
検索
アップデート

注意喚起


お客様への重要なおしらせ
www.pizza-la.co.jp/s/sc_osirase_sp....
PIZZA-LA
メニュー
注文・予約
ログイン
会員登録
お客様への重要なおしらせ
【ピザーラ公式ではないiPhoneアプリにご注意下さい！】
下記アプリケーションは、宅配ピザチェーン「ピザーラ」及びフランチャイズ本部である株式会社フォーシーズの承認なく制作されたアプリケーションです。
現在、Apple社へ削除を依頼しております。
お客様情報の安全性が確認できておりませんので、下記アプリのダウンロード、下記アプリ経由でのご注文や会員登録はお控えくださいますようお願い申し上げます。
■該当アプリ名称
「pizza-la For iPhone」
お客様への重要なお知らせ
www.tsuruha.co.jp/news/?cm=v&id=...
ツルハドラッグ
お知らせ
お客様への重要なお知らせ
当社の社名をかたる偽アプリにご注意ください。
ツルハでは現在iphoneアプリを制作しておりません。無断制作されたアプリでのご利用はお控えくださいますようお願い申し上げます。
e-matsukiyo.com
ようこそゲスト様
新規会員登録
ログイン
お買い物カゴ
送料無料まで3,150円です
マツモトキヨシ
検索
初めての方へ
ご注意下さい
当社の社名を騙るアプリに関するご注意
キーワードで探す
カテゴリで探す
お悩みから探す
買い物カゴ
マイボックス
注文履歴
■重要なご案内
▶ 当社の社名を騙るアプリに関するご注意
▶ 配送料金改定のお知らせ

外部デバイスによる確認



- 外部デバイスによる送金先確認で
  - 利用者はこれで確認さえすれば安心できる
  - アプリが偽であっても、他に何か未知の脅威があっても
- この外部デバイスが侵されないのが前提

電子申請への応用

- 行政機関や自治体への電子申請
  - 今のところさほど普及していないが
  - 今後広く普及すればマルウェアの攻撃対象となり得る
- 電子申請における脅威想定
  - e-Taxでの税申告で還付金の振込先口座を差し替えられる等
  - 自治体への申請で申請内容を差し替えられる
    - 住民票の写し交付申請を出したつもりが、付記転出届に差し替えられる等
- 公的個人認証に対するMan-in-the-Browser攻撃
  - 電子署名は強固な技術だがマルウェア感染には無力
  - 電子署名には否認防止の能力があるが、マルウェア感染の可能性があれば現実には否認防止は機能しない

群馬県前橋市｜公的個人認証サービス（電子証明書）について

www.city.maebashi.gunma.jp/kurashi/8/14/17/p001786.html

サイトマップ | 音声読み上げ | For foreigners | 文字サイズ 小 標準 大 | 文字色 標準 白黒 | 検索

前橋市 水と緑と詩のまち Maebashi City

ホーム 前橋市トップページ | 暮らしの情報 市民生活に役立つ情報 | 事業者の方へ ビジネス支援の情報など | 観光情報 市内のイベントや観光 | 施設・組織 施設や組織の一覧 | 市政情報 市の施策や財政、条例

ホム > 暮らしの情報 > 戸籍・住民異動・オンラインサービス > 住民基本台帳カード・公的個人認証サービス > 公的個人認証サービス > 公的個人認証サービス（電子証明書）について

公的個人認証サービス（電子証明書）について

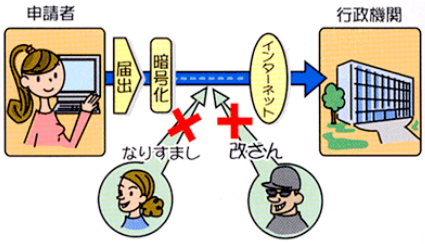
最終更新日：2013年2月12日(火) ページID：001786 印刷する

電子申告（e-Tax）・電子申請等に必要な手続きです。ご利用ください。

「住民基本台帳カード・公的個人認証サービス」のその他の分類
- 住民基本台帳ネットワーク
- 住民基本台帳カード
- 公的個人認証サービス

1 公的個人認証サービスとは

行政機関へのインターネットを利用した電子申請の際などに、申請者が間違いなく本人であることを確認するために、都道府県知事が電子証明書をICカードに格納して希望者に提供するものです。
この証明書が電子申請書に添付されることにより、別人によるなりすましや、通信途中での改ざんなどを防ぐことができます。



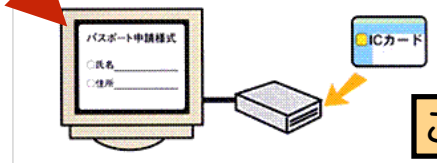
改ざん防止できるのは
通信回線のところだけ？

群馬県前橋市｜公的個人認証サービス（電子証明書）について

www.city.maebashi.gunma.jp/kurashi/8/14/17/p001786.html

Step4 ICカードをセットし、暗証番号を入力

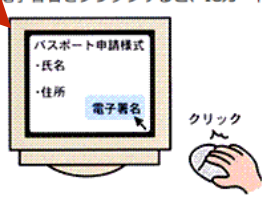
電子証明書が記録された住民基本台帳カード等のICカードをリーダライタにセットし、暗証番号を入力します。
電子証明書は、事前に市区町村役場で申請して、入手してください。（裏表紙参照）



このPCがマルウェアに感染していたら？

Step5 電子署名をクリック

電子署名をクリックすると、ICカードとパソコン間で情報がやり取りされます。



ここで申請内容を差し替えられ…

画面には正しい情報が出るのに…

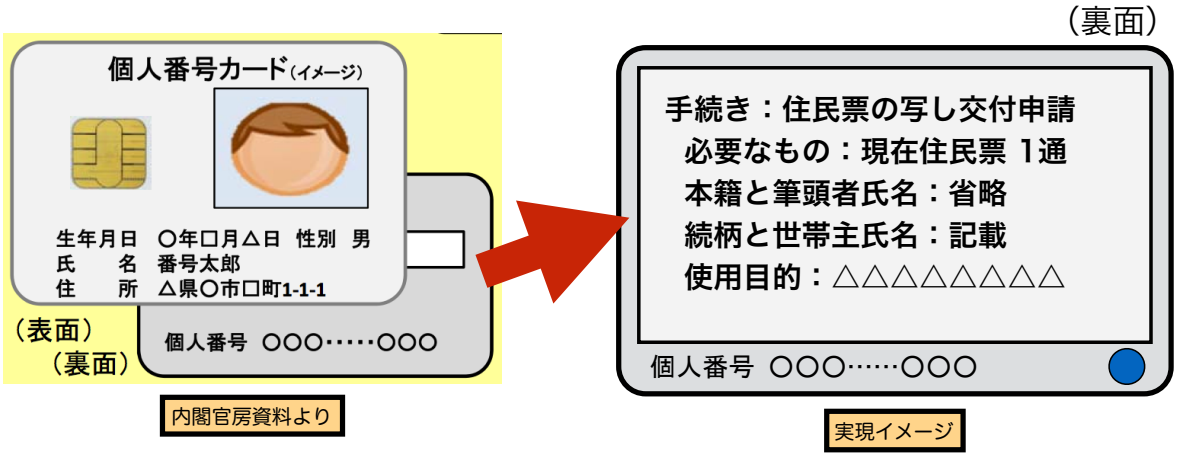
Step6 送信をクリック

送信をクリックすると、申請書、電子署名、電子証明書が暗号化され、行政機関に送られます。

差し替えられた申請書に電子署名したものを提出してしまう

提案：署名内容を表示し確認できるICカード

- ICカードに電子署名対象の情報を表示する機能
  - 個人番号カードの裏面に搭載してはどうか



内閣官房資料より

実現イメージ

- 認証だけいくら強化しても無駄！
  - これをやらなきゃ！

この脅威があまり想定されてこなかった

- 電子政府ユーザビリティガイドライン（2010年8月）
  - 「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」（各府省情報化統括責任者連絡会議決定）
- 中間者攻撃の脅威として想定はあるが、対策が……

表 A.4-2 署名等プロセスにおける脅威と対策の例

脅威	説明	脅威例	対策例
中間者攻撃	署名等プロセスに介入し、意図せぬ署名を生成させる。	・利用者が使用する機器やソフトウェアの脆弱性等を利用して、署名対象の改ざん、差し替え等を行い、利用者が意図しない対象に署名させる。	・利用者が、機器やソフトウェアの正当性を検証可能とする機能を搭載する。
アルゴリズム危殆化攻撃	危殆化した暗号アルゴリズムを用いるように誘導し、安全性の低い電子署名を行わせる。	・複数の暗号アルゴリズムを併用可能なシステムにて、危殆化した暗号アルゴリズムを用いるように	・ムに関する機能をシステムから削除し、安全な暗号アルゴリズムのみが動作するように

どうやって…？

数年後の未来への期待

- NFC対応スマホ・タブレットが普及
- アプリでe-Taxや電子申請
- 個人番号カードをNFC経由でアプリと連携
  - ログイン認証として
  - 公的個人認証を用いた電子署名機能として
- Man-in-the-App対策
  - 個人番号カード裏面の表示器で署名対象内容を確認
  - 事後否認の防止も実現可能に
- 別の鍵も使えるように
  - 公的個人認証以外の鍵が使えてもよい
  - インターネットバンキングの不正送金防止にも使える