

## パネル討論: 金融業務と情報セキュリティ技術 この10年の経験と今後の展望

独立行政法人産業技術総合研究所  
情報セキュリティ研究センター

高木 浩光

<http://staff.aist.go.jp/takagi.hiromitsu/>

1

## 今は昔

- 専用ソフト方式
  - SET (Secure Electronic Transaction) 専用プロトコル (1996)
  - SECE (Secure Electronic Commerce Environment )  
日本版SET (1997)
- 「ブラウザバンキング」(1998)
  - 専用の電話番号にダイヤルアップ接続して、IP接続を確立して、Webブラウザで利用する(インターネット経由ではない)
  - 電話中は専用端末状態になる
    - インターネットの他のサイトを同時に閲覧することはない
- 専用ソフトや専用電話回線方式は、セキュリティ脆弱性の問題が生じにくい
  - スパイウェアに対して耐性があるわけではないが

2

## 10年前の将来展望

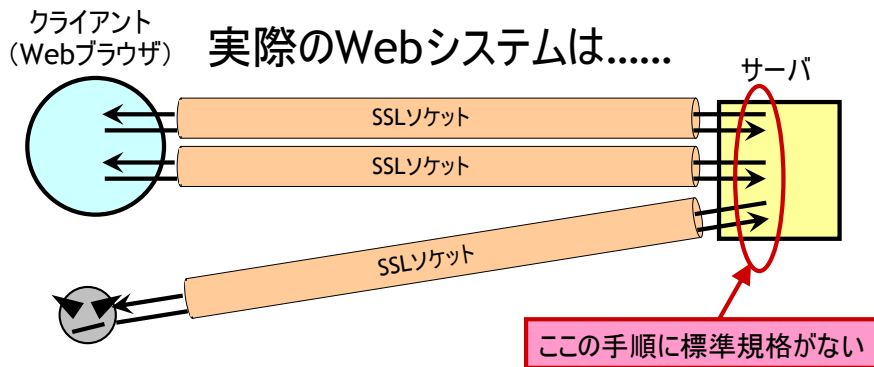
- EDI推進協議会 Newsletter No.32より
  - 平成9年度 産業情報化シンポジウム  
講演「新ネットワーク社会における金融機関の役割」  
(株)さくら銀行 専務取締役 吉田千之輔氏  
(中略) 当行では、ブラウザ技術を用いる「ブラウザバンキング」、単なるエレクトロニックバンキングとしての「ダイレクトバンキング」、さらにインターネットを利用する「インターネットバンキング」、特定の法人顧客の社内LANのなかで利用できる「イントラネットバンキング」、といった幾つかの枠組みを考えている。ここで、128bit暗号技術の輸出規制が解除されたことでインターネットバンキングの普及が促進されるのではないかという見通しをもっている。今後、セキュリティでは標準化が進み、加入手続きではブラウザ技術により簡便なインストールが可能となり、さらにオフラインのICカードとの併用が進むことで、インターネットバンキングの利用が進むことも予想される。

3

## インターネットバンキング

- プロトコルは「SSL」でよいという判断(があった?)
  - しかし、SSLは1本の通信路をsecureにするものでしかない
- Webアプリケーションは、
  - 複数のHTTP接続を同時に又は何度も接続して動作するもの
  - HTTP接続間の連携方法に関するセキュリティを、SSLが保障してくれるわけではない
- Webアプリケーションは脆弱性が生じ易い
  - Cookieを用いたセッション管理方式における脆弱性の発生
  - 入力ページから <https://> でなければならぬ等、規格化されていない画面設計上の注意点がある
- Phishingの脅威
  - あらゆるサイトが横並びで同時につながっているのが「Web」

4



5

## 脆弱性情報の流通

- 事例: 2002年2月、ある都市銀行
  - 「予測できてしまうセッションID」という脆弱性の存在を確認
  - 古いWebアプリケーションサーバの既知の脆弱性がパッチ対応されていなかった
    - 2001年9月にBUGTRAQで、ドイツの銀行(おそらく)に存在した問題として報告され、国際的に広く知られていた
    - 2001年5月にベンダーから修正パッチが出ていた
    - 9か月間対処されていなかったのは、脆弱性情報が行き渡らない状況だったためと推察
- 脆弱性情報等の届出と流通の枠組み
  - 2004年7月より IPA, JPCERT/CC

6

## 予測できてしまうセッションID

- 連続して繰り返しログインしたときに発行されたセッションID

```
0001EGEAPVIAAA21QCXZAFITWSI
0001EGGBTOQAAA2VACXZAFJ4JSQ
0001EGG1NIYAAA2VCCXZAFJ4JSQ
0001EGGTY4QAAA2VECXZAFJ4JSQ
0001EGHQJQAAA2VGCXZAFJ4JSQ
```

7

## 製品の脆弱性とWebの脆弱性

- ソフトウェア製品の脆弱性は、情報が流通するようになった
- その一方、Webアプリの脆弱性は、サイト固有であるため流通しない
- SETには標準規格があった
  - これに従って実装していればよかった
- Webでは、SSLだけが標準規格
  - ブラウザバンキング以降、Webアプリケーションという、**標準規格が存在しない**技法でシステムが構築されてきた
- 責任はサイト運営者にある
  - ベンダーと責任の分担を明確に

8

## 今後の方向性

- 専用ソフトに戻るのも一興かと
  - phishing被害を防げる
  - CD-ROMで配る
    - ただし、二セCD-ROM問題を解決する必要あり
  - 今や、インストールの手間が本当に障害となるのか疑問
- Webアプリケーション構成法の標準規格を作りそれに従う
  - ご参考：経済産業省の取り組み「ウェブアプリケーションのセキュリティガイドライン策定に関する調査研究」
  - FISCの安全対策基準は？

9

## 安全設計・実装のガイドライン

- 設計段階で生じる脆弱性の排除
  - 設計上のセキュリティ要件をすべて列挙
    - SSL使用時のhttps://とすべき画面の指定
    - ドメイン名の使用方法の指定
    - アドレスバー、フレーム、ウィンドウについての指定
    - CSRF対策が必要な画面の設計時からの特定
    - セッション追跡実現手法の指定
    - 使用する乱数生成系、暗号の指定
    - パスワードに関する設計
- 実装段階で生じる脆弱性の排除
  - クロスサイトスクリプティング、SQLインジェクション等
  - 実装方法として安全なものを指定してしまう
    - SQL文の組み立てをPrepared Statementで行うことを必須に
    - SQL文の組み立てを一か所に集中させることを必須に
    - HTML出力をテンプレートで行うことを必須に

10

## 期待される効果

- 発注時のセキュリティ要件として示す
  - (新規開発案件を前提)
- 検査コストを低価格化できる
  - 従来: コード監査でインジェクション系脆弱性の疑いのあるコーディングがされた部分が見つかって、本当に脆弱かどうかは、データフローを追いかけて調べなくてはならず、手間がかかる
  - 解決: 指定された実装方法にしたがっていないことを調べるだけで、発注要件を満たしていないと診断できる
- 開発ベンダの責任の明確化(と適正な料金積み上げ)
  - 要件を満たしていない部分は、開発ベンダの瑕疵として扱える
- 開発ベンダと検査事業者の力量の評価
  - ガイドライン準拠の開発実績、評価実績による判断

11

## 既存のガイドライン等

- 内閣官房(政府機関向け)
  - 「ソフトウェア開発における情報セキュリティ対策実施規定」
    - 技術的セキュリティ要件を挙げることを試みているが、Webアプリについては、脆弱性を排除するための具体的な記述はない
    - 「検証と妥当性確認」についても規定されているが、検査基準に具体性がない
- 経済産業省(民間向け)
  - 「情報システムの信頼性向上のための取引慣行・契約に関する研究会 報告書」
    - システム開発発注における契約の観点の記述が充実しており、別紙として「セキュリティ要求仕様書サンプル」が例示されており、「6. 開発に係るセキュリティ対策」の節があるが、具体性に欠け、「ITセキュリティ評価・認証制度による認証取得製品の活用を検討すること」と、非現実的な要件を挙げることしかできていない

12

- クレジットカード業界
  - 「PCIデータセキュリティ基準」(PCIDSS)  
[https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)
    - 6.5項にWebアプリについて記述があるが、抽象的で網羅性に乏しい
      - 「Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following: ... (OWASP Top 10 の列挙)」
- FISC
  - 「金融機関等コンピュータシステムの安全対策基準」
    - 関連項目: 技7, 技8, 技9, 技10, 技11, 技12, 技26, 技27, 技28, 技29, 技30, 技31, 技35, 技36, 運106
    - Webアプリについての具体的な基準に関する記述はない
    - 技10: 「主にWebシステム構築時のセキュリティ...セキュアプログラミング技法がある。Webシステムについては、セキュアプログラミングを考慮してシステムを構築することが望ましい。」
      - 「セキュアプログラミング技法」などというものがあるわけではないのだが.....

13

## ドメイン名とサーバ証明書の要件

- ドメイン名に関する要件
  - システムが使用するURLのすべてにおいて、ドメイン名は1つとする
    - 例外1: インライン画像等を除く
    - 例外2: 他のサイトを呼び出す必要がある(決済機能を他社サービスに依存する場合)場合には、以下を利用者に説明する画面を表示する。この画面は https:// とする(SSLを使用しないサイトを除く)。
      - ジャンプ先URLのドメイン名
      - ジャンプ先のサービスの名称、運営者名
  - **ドメイン名保有者とサイト運営者を一致させること**
    - 例外: 業務委託しているために一致させられない場合、以下を利用者に説明しているならば認める。
      - 業務委託先の名称
      - 業務委託先のドメイン名
- 地方銀行の多くがこの要件を満たさない
  - NTTデータ「anser.or.jp」、日立「ib-center.gr.jp」、「finemax.net」、IBM「cyber-biz.ne.jp」、「chance.co.jp」

14

## Phishing対策

- 全銀協の方からうかがった話
  - フィッシングからの自衛策を解説する資料を作ったが、「証明書の内容を確認しよう」と書きたくても、現実に地方銀行らが、「NTTDATA」や「日立製作所」となっていて、アドバイスできず困っている。
- そろそろ安全対策基準に入れないといけないのでは.....

15

アドレス(D) http://www.rcis.aist.go.jp/special/websafety2007/

RCIS 情報セキュリティ研究センター  
 RCIS (Research Center for Information Security)

Japanese | English  
 独立行政法人  
 産業技術総合研究所

### 安全なWebサイト利用の鉄則

産総研 > RCIS > 安全なWebサイト利用の鉄則

#### この解説について

目的: フィッシング被害を防止するWebサイト利用手順の確認

著名なブランド名や会社名を騙った偽のWebサイトを作り、人をそこに誘い込んでパスワードや個人情報を入力させてかすめ取る、「フィッシング」(phishing)と呼ばれる行為がインターネットの安全を脅かすつとあります。フィッシングの被害を防止するには、利用者ひとりひとりが本物サイトを正しく見分けることが肝心です。

しかしながら、どうやってWebサイトを安全に利用するか、その手順のことはあまり広く知られていないようです。技術者達の間では暗黙の了解となっていることですが、市販のパソコンの取扱説明書には書かれていませんし、学校の教科書にも書かれていません。最近では行政機関や企業からフィッシングに注意を呼びかける文書が発表されることがありますが、あまり正しく解説されていないのが現状です。

この解説は、Webサイトを安全に利用する簡潔な手順を示します。無用で余分な確認手順等は排除しています。必要な手順のみを示します。

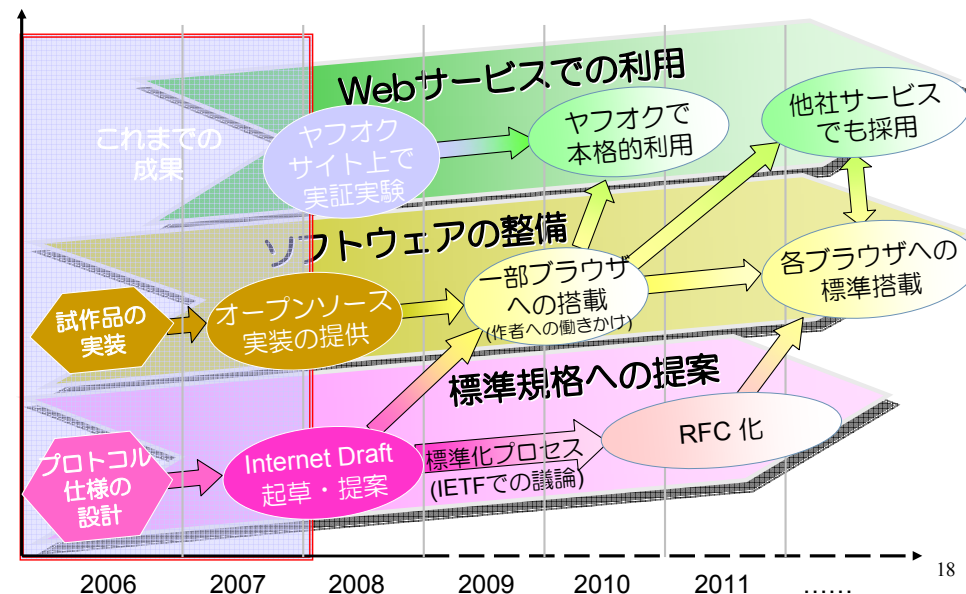
#### 想定する読者: 利用手順をユーザに説明する方、サイトを設計する方

## 金融庁監督指針

- 主要行等向けの総合的な監督指針(19年6月版)
  - 中小・地域金融機関向けの総合的な監督指針(19年8月版)
    - III-3-7 インターネットバンキング
      - III-3-7-2 主な着眼点
      - (2) セキュリティの確保
- インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、必要に応じて見直す体制を整えているか。特に、本人認証については、個々の認証方式の各種犯罪手口に対する強度を検証した上で、取引のリスクに見合った適切な認証方式を選択しているか。
- ホームページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。また、フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。

17

## Phishing対策 相互認証プロトコルの利用



18

## 「スパイウェア」の問題

- スパイウェアの問題は解決が困難
  - ワンタイムパスワード、ソフトウェアキーボードでは解決しない
- 特にWebは危なく、簡単に不正送金等ができてしまう
  - 専用ソフトなら攻撃を若干難しくできる(が不可能ではない)
- TPM (Trusted Platform Module)  
Trusted Computing による解決(?)
  - 耐タンパ性を持つセキュリティチップ
    - 近年の市販PCに内蔵されている
  - 応用の可能性
    - ユーザのPC端末と使用ソフトウェアがマルウェアに侵されていないことを確認したうえで、インターネットバンキングへのログインを認める方式

19