



# 民間認証業務の現状と課題

資料1

2006. 12. 27

日本認証サービス(株)

村松 晃

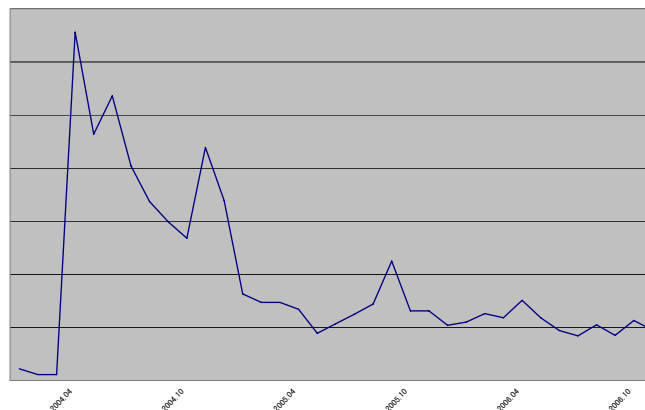


# 民間認証事業者の状況 1

## 特定認証事業者

### ■ 経営は苦しい

- 当社発行枚数の変遷 (右図)
- 証明書の主流が確定?
  - ▶ 電子政府は商業登記と公的個人
  - ▶ 電子自治体はJACIC



### ■ G向け証明書市場は魅力がない

- 従来業務をそのまま電子化→普及しない?
- 日本語(行政)とIT(電子化)のギャップ
  - ▶ 日本語をアルファベットにマッピングする完備な手段がない
    - ✦ ローマ字? 表記方式、長音、外国語
    - ✦ コード化? JISバージョン、コード化、非標準字形
  - ▶ JREのバージョン問題→一台で複数の電子申請は無理?
  - ▶ ブラウザやメーラにおける電子証明書の内容表示が難解
  - ▶ 証明書がPCの中でどのように扱われているか知らずに利用
- 認定取得コスト、一般認証における認定と別建ての認定



# 参考：社保庁の認める電子証明書

発行認証局等 申請者等	電子認証登 記所（商業 登 記 認 証 局）	日 本 認 証 サービ 株 式会社（基 本型）	公的個人認 証サービ ー	備 考
法人事業所（登記あり）	○	—	—	
法人事業所（登記なし）、官公庁等	—	—	—	現在、社会保険の手続にご利用いただける電子証明書はありません。
個人事業所	—	○※ 18,000円	○ 500円	※日本認証サービス株式会社の発行する電子証明書は（基本型）のみ利用可能です。



# 民間認証事業者の状況 2

## 一般認証事業者 (パブリックサービス)

### ■ 事業環境が良好で活況

#### ■ 大規模グローバル市場→アウトソーシング比率小

- ▶ 携帯端末のビジネスと似ている：日本のトップベンダもグローバルには存在していないに等しい

#### ■ 証明書単価が高い

- ▶ 50,000円～100,000円
- ▶ EVCは200,000円以上?

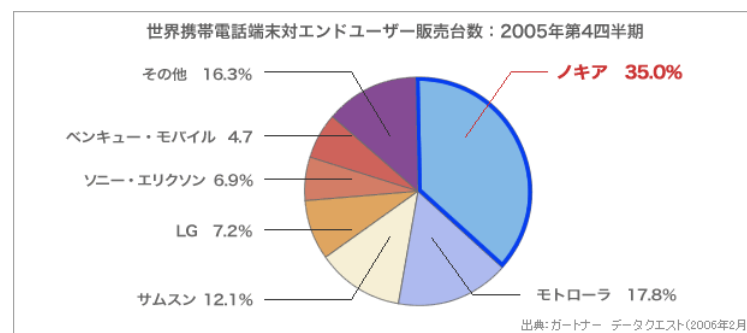
#### ■ 事業者の裁量余地大

#### ■ 未開拓市場で成長率大

- ▶ Web2.0で急成長のホスティング市場では95%はSSL未実装

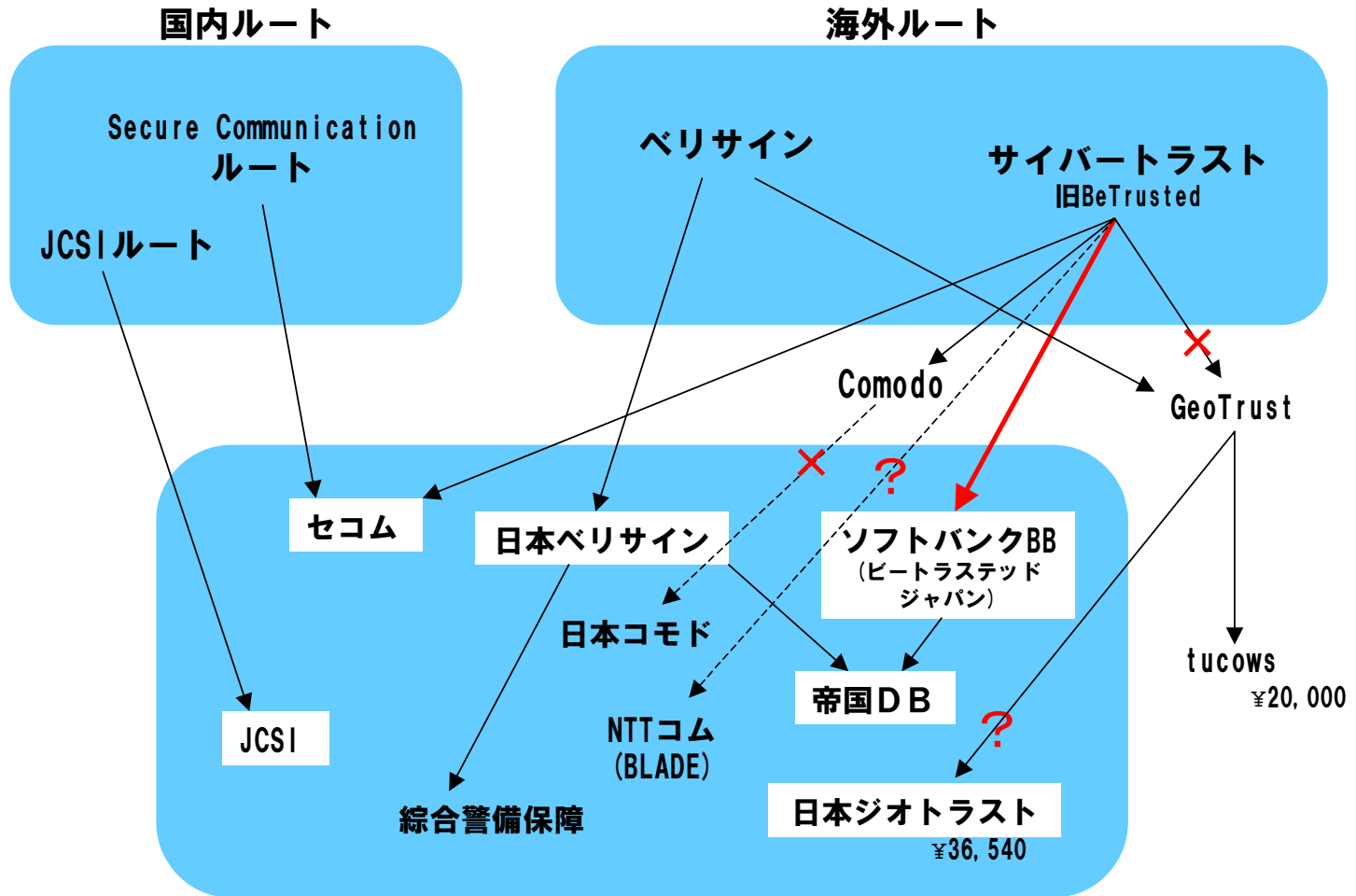
### ■ M&Aによるルート認証局のパイプライン問題

- 国内事業者の大半は海外ルート利用
- ソフトバンクによる買収の影響





# 最新認証局ルート相関図



## ■ 特定認証事業はB2Bへ展開

- 電子契約
- e文書化
- J-SOX

## ■ 一般認証事業は寡占化が進行?

- EVC (Extended Validation Certificate) の衝撃
  - ▶ 厳密な実在性審査に基き発行される“プラチナ証明書”
  - ▶ アドレスバーの変色機能により信頼性の指標と化す?
  - ▶ 法人の実在性証明から、個人の実在性証明、IP電話やIM(インスタントメッセージング)の相手認証、コード署名へ展開
  - ▶ EVCが発行できる財務体力のある事業者は世界で数社?
  - ▶ 日本は“蚊帳の外”
- 官製標準とグローバル・デファクト標準
  - ▶ Web2.0のブラウザ中心主義の世界はEVCが支配?
  - ▶ 日本電子認証協議会(2007.1予定): 当社は発起人のひとり

## ■ CA Brouser Forum(欧米の認証事業者とブラウザベンダにより本年2月に設立されたNPO)

- ▶ ベリサイン、サイバートラスト、エントラスト、コモド、ジオトラスト、RSAセキュリティーズ、Thawte、ウェルスファーゴ銀行等/マイクロソフト、オペラ、モジラ、KDE (4大監査法人はオブザーバー)

## ■ EV-SSLガイドライン(本年10月にドラフト)

- ▶ 厳格な実在性審査に基づいて発行されるEVCとその審査プロセスの要件を記載
  - ✦ 申請者の法的実在性、物理的実在性、事業活動の形跡、ドメイン名、申請者属性、署名または押印、申請の真正性、弁護士、ブラックリスト
  - ✦ CA従業員の身元確認、教育
- ▶ サーバ証明書 (EV-SSL) から開始、引き続きSSLクライアント証明書、S/MIME、コード署名、タイムスタンプ、VOIP、IM、Webサービス等へ拡大
- ▶ EVC発行資格
  - ✦ Webtrust Program for CAとWebtrust EV Programの認定取得
  - ✦ 保険加入 (Commercial General Liabilityに対し最大200万ドル、Errors & Omissionsに対し最大500万ドル)

# JCSI 新ブラウザの動作

## ■ アドレスバーが変色

- EV-SSL証明書→アドレスバーが(緑)に変色し、企業名が表示
- 通常のトラストされている証明書→従来どおり(白)
- 疑わしいサイトに掲載の証明書→(黄)
- ブラックリストに掲載の証明書→アドレスバーが(赤)に変色し「フィッシングサイト」と表示される

## ■ Windows VISTA / IE7の例

Fig 2, IE7 address bar for a site with an EV SSL certificate (showing the identity of the site from the SSL certificate)

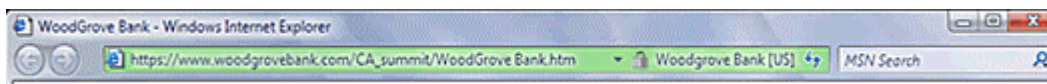
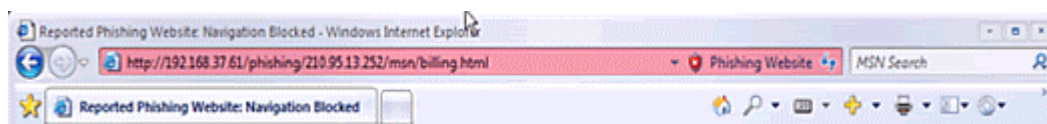


Fig 1, IE7 address bar for a known phishing website detected by the Phishing Filter





## ■ 個人情報の問題

- 基本4情報が署名検証者に渡ることの周知徹底が必要
- 基本的には検証者は行政と特定認証事業者に限るべき

## ■ 特定認証事業者の選択

- 公的個人による各種証明書のオンライン発行
  - ▶ 当社は技術的準備をほぼ完了
- EVC発行申請のための基本情報としてCA/Bフォーラムで認知してもらう