クラウドのトラストを支える証明書とそのセキュリティ動向

セコム株式会社 IS研究所
島岡　政基

概要

- クラウドにおけるトラストとは?
- 証明書のトラスト
- 証明書のセキュリティトピック
  - パブリックルート認証局への攻撃
  - 鍵ペアにまつわるリスク

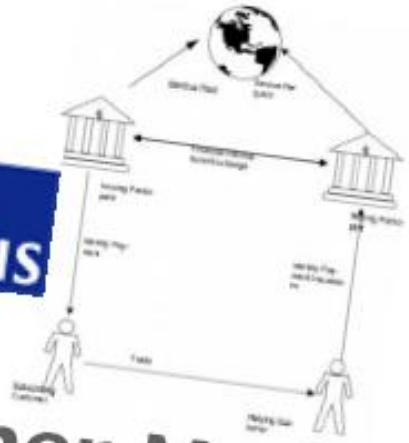
トラストフレームワークとは

- ネットワーク上のコミュニケーションにおいて、相手や情報の信頼性を確保する枠組み
  - 相手が誰なのか
  - その情報は信用できるのか

これまでの様々なトラストフレームワーク

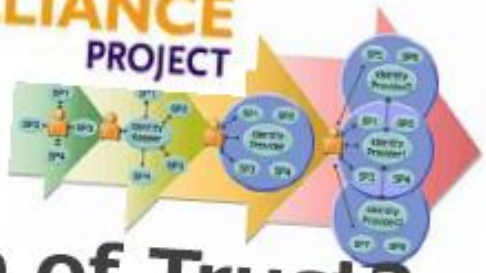
Bridge CA?

identrus



5-Corner Model?

LIBERTY ALLIANCE PROJECT



Circle of Trust?

WS-I WEB SERVICES INTEROPERABILITY ORGANIZATION

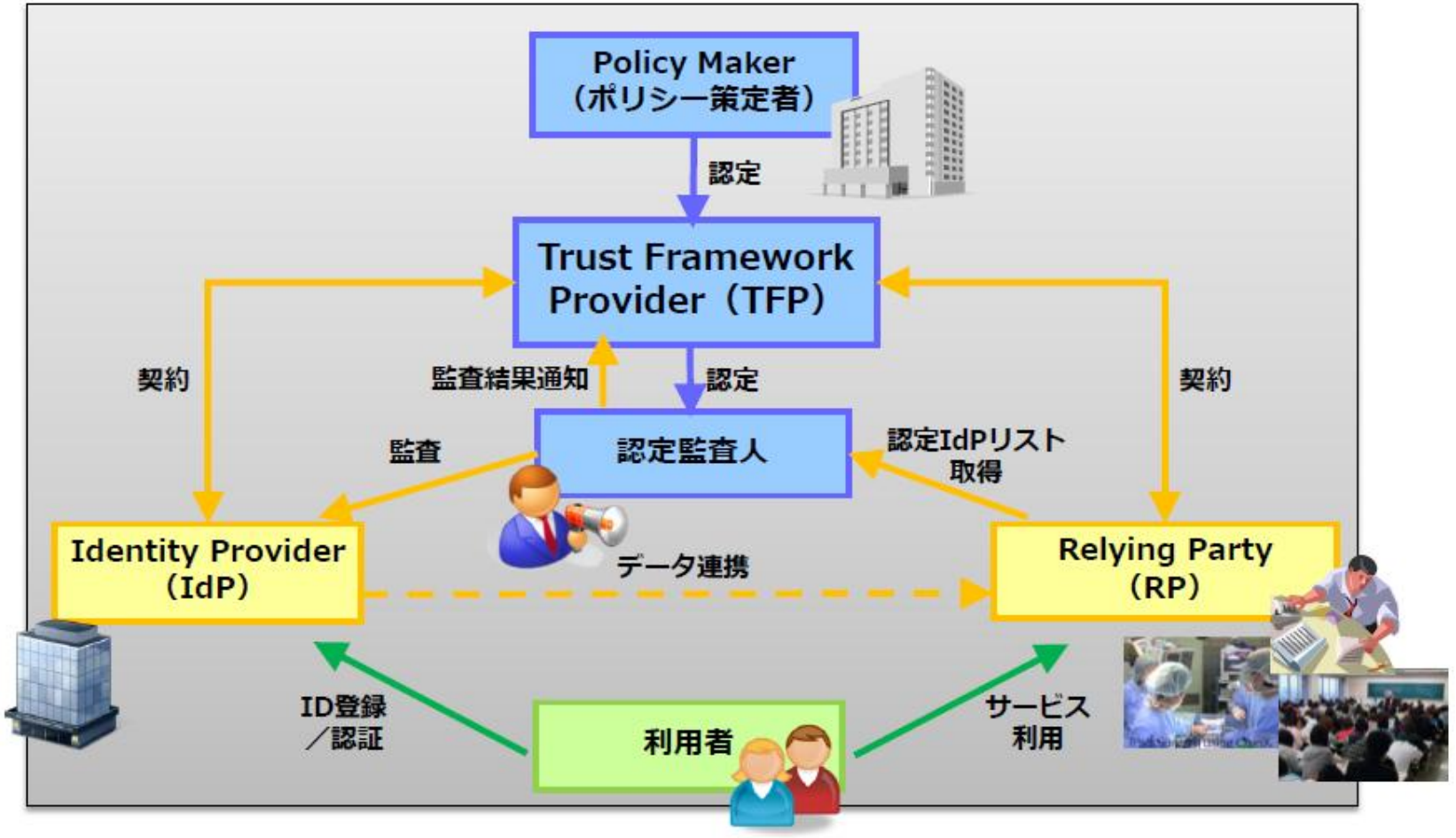
WS-Trust?

「トラストフレームワークの国際動向」山中 進吾（OpenIDファウンデーション・ジャパン）
http://www.slideshare.net/shingoyamanaka/110728-trust-framework

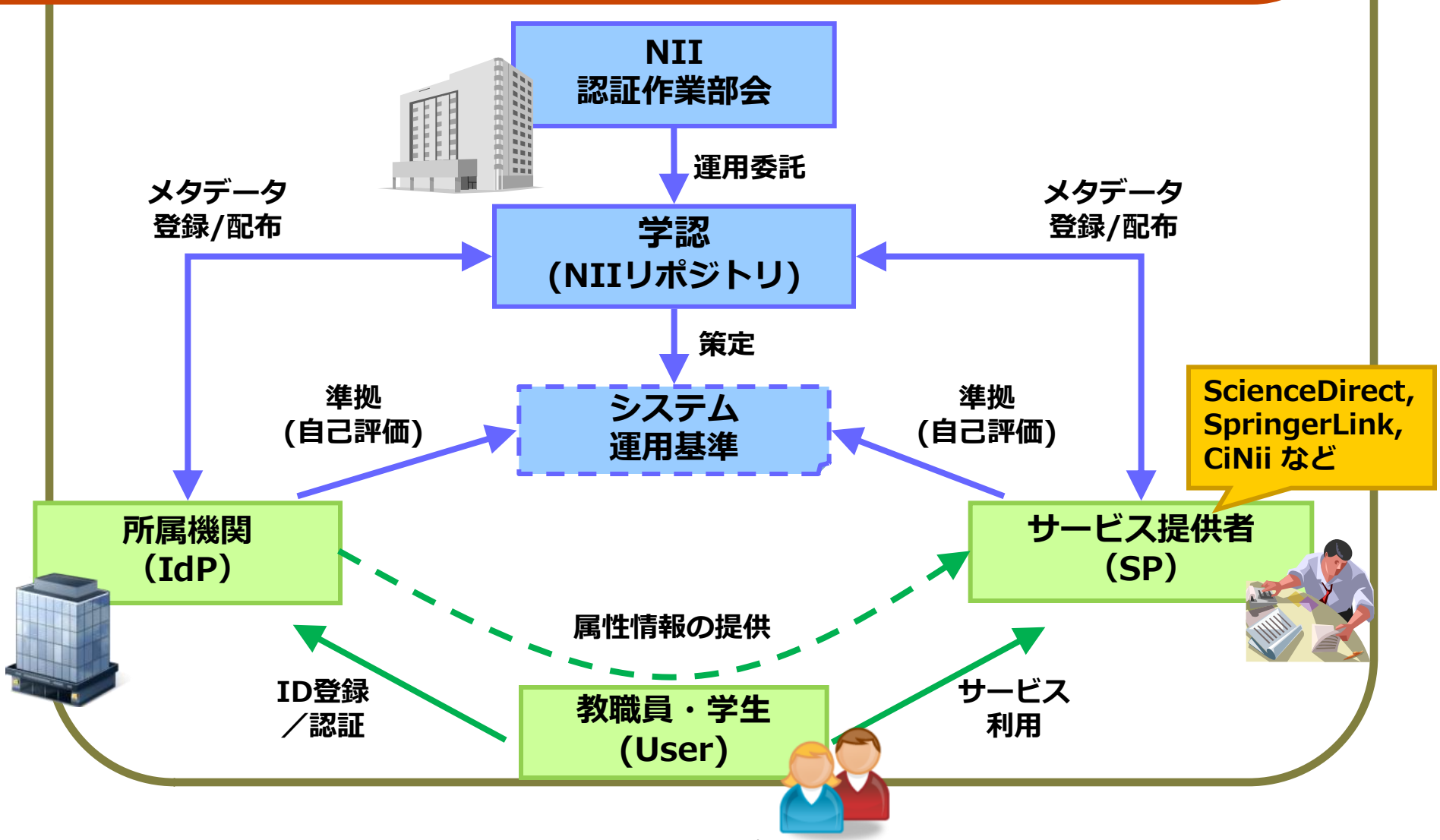
トラストフレームワークの本質

- ステークホルダーが遵守する基準
  - 技術基準、運用基準
  - 法制度
  - 基準の定期的な見直し
- 監査、認定、公表による透明性の確保
  - 基準にもとづく監査・認定
  - 各基準および認定事業者のリスティング

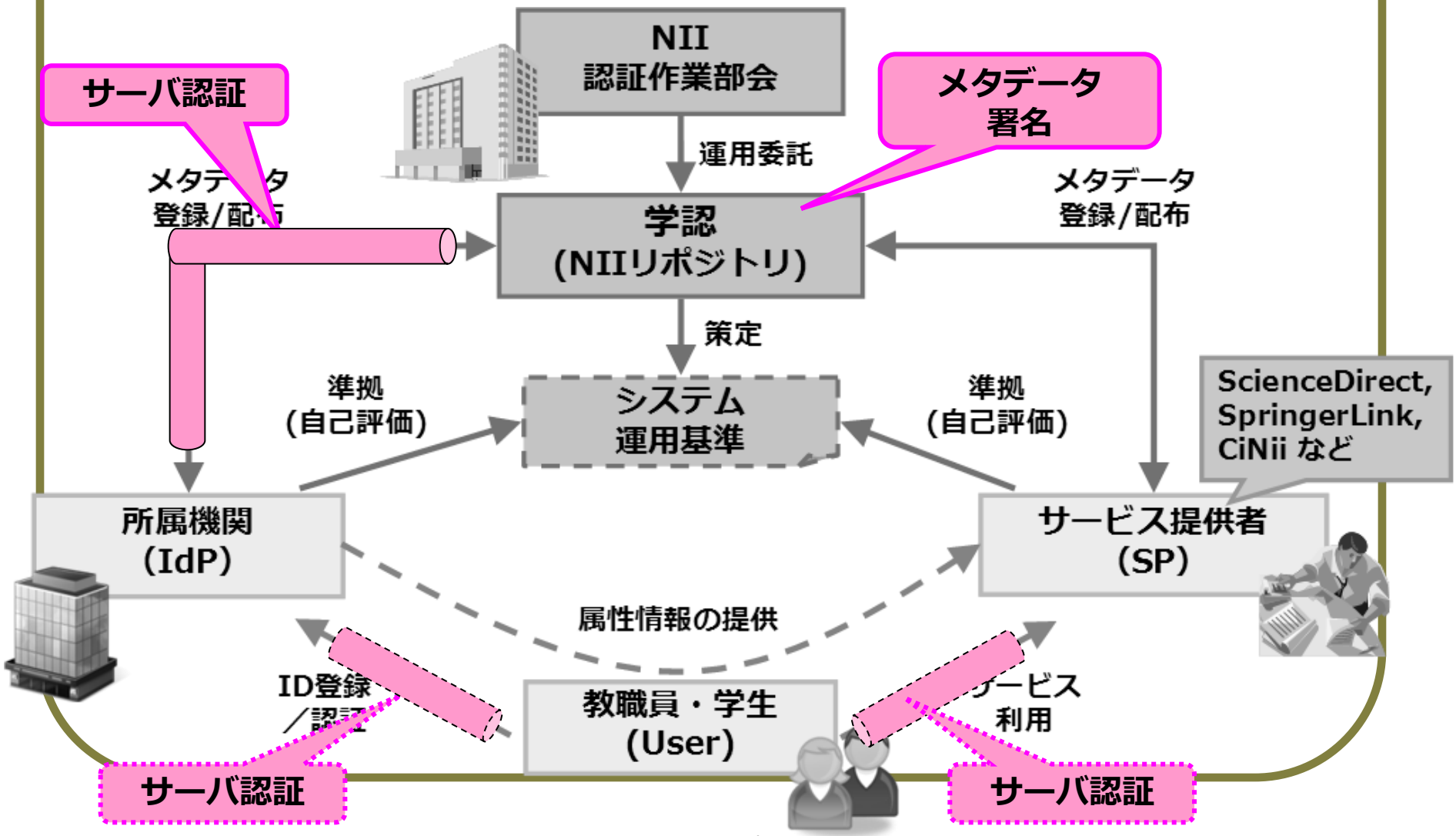
Open Identity Trust Framework



学認のトラストフレームワーク



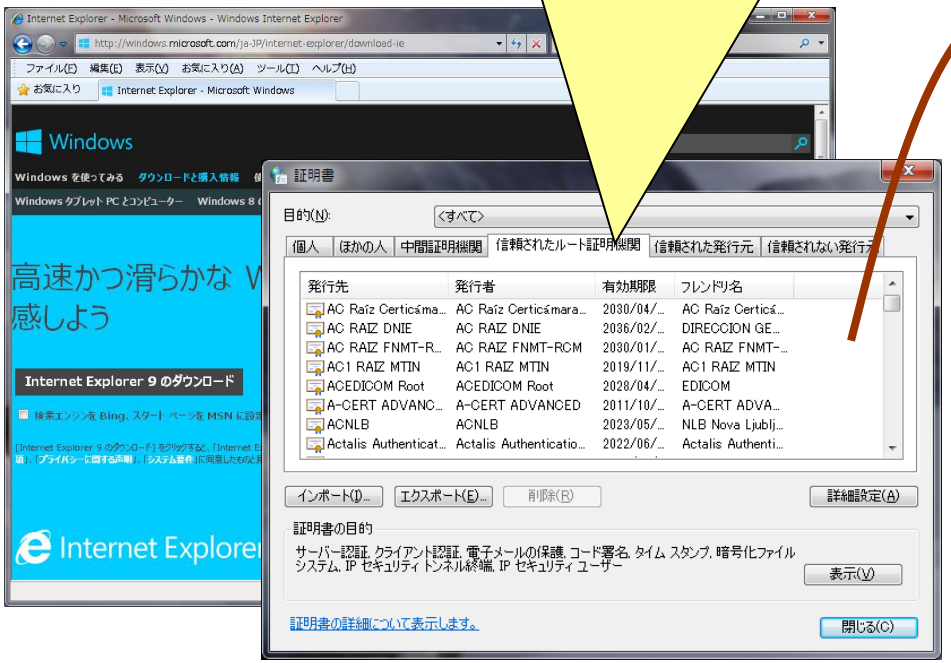
学認で使われている証明書

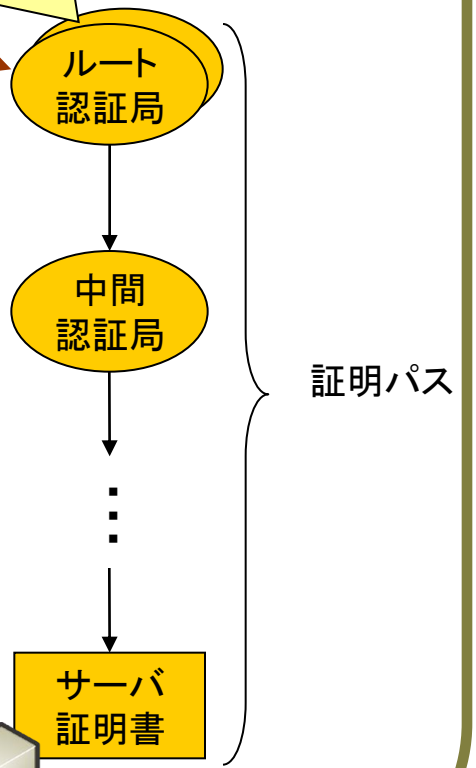


証明書のトラスト

パブリックルート認証局
デフォルトのトラストアンカ
OSやブラウザなどに標準で搭載されている認証局

トラストアンカ
証明パスの起点となる認証局





SSL/TLSサーバ認証

パブリックルート認証局の概要

- 膨大な数の認証局
  - IE7で300件超、Firefoxでも180件弱
  - ブラウザの登録手続きの明確化、各国の認定制度整備により爆発的に増加
- 国際規準への準拠(必須要件)
  - WebTrust for CA、ETSI TS 101 456または同 102 042、ISO 21188:2006のいずれか
  - 1年毎の外部監査
- ブラウザ毎に異なるルート認証局登録手続き
  - IE(PC), IE(WP7), Firefox, Safari, Opera, etc.
  - 準拠したら自動的に登録されるわけではない

Windows Root Certificate Program - Members List (All CAs) - TechNet Articles - United States (English) - TechNet Wiki
http://social.technet.microsoft.com/wiki/contents/articles/2592.windows-root-certificate-program-members-list-all-cas.aspx
Included Certificate List
http://www.mozilla.org/projects/security/certs/included/

パブリックルート認証局のセキュリティ

- 【技術】Hardware Security Moduleによる鍵ペア管理
  - FIPS 140-2 Level 3 または CC EAL4以上
- 【運用】複数名による相互牽制、要員教育
- 【設備】災害対策、電波漏洩対策など

Symantec's Certificate Authority 'Vault': $11M Worth Of James Bond-Like Security
http://www.crn.com/news/security/240005644/symantecs-certificate-authority-vault-11m-worth-of-james-bond-like-security.htm
【和訳記事】シマンテックの認証局「Vault」、1100 万ドルをかけたジェームズ・ボンド並みのセキュリティ
https://www.verisign.co.jp/ssl/first/pdf/11m_worth_of_JamesBond-like_security.pdf

証明書のセキュリティトピック

- パブリックルート認証局への攻撃
- 鍵ペアにまつわるリスク

↓元ネタはこちらから、、、

NPO日本ネットワークセキュリティ協会 PKI相互運用技術WG主催セミナー
PKI Day 2012 (2012年12月13日開催)
【午後の部】「PKIへの攻撃とその対応」
【講演】「サイバー攻撃ツールとしての公開鍵証明書の役割
～信頼の起点にカモフラージュされた攻撃の起点～」(IPA神田雅透氏)
【講演】「公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題
～いつのまにか他人と秘密鍵を共有してませんか？～」(IIJ須賀祐治氏)

下記URLより講演資料ダウンロード、Ustreamアーカイブ視聴可能です。
http://www.jnsa.org/seminar/pki-day/2012/

パブリックルート認証局への攻撃

- ComodoHacker事件
  - 2011年3月、Comodo社の委託登録局(RA)のアカウントハッキングによる証明書の不正発行
  - Gmailなど著名なドメインに対するMITM攻撃
- DigiNotar認証局事件
  - 2011年8月、DigiNotar社自体への不正侵入による大量の証明書不正発行
  - 本事件の影響により同社は翌9月に倒産
- Flame事件
  - 2012年5月、Microsoftの認証局に対するMD5選択平文攻撃による証明書の不正発行
  - 高度な暗号解読技術

鍵ペアにまつわるリスク

- 公開鍵使いまわし問題
  - 2012年8月、ほぼ同時期にHeningerら、Lenstraらが指摘
  - インターネット上でデフォルトの鍵ペアまたは既知の脆弱な鍵ペアを使っているHTTPSサーバが少なくとも5.57%以上存在する
- GitHub私有鍵露出問題
  - 2013年1月23日、GitHubがリポジトリの検索機能をリリース
  - 検索機能によってユーザの.ssh/id_rsaなどが検索可能になった

⇒ 1月25日に復旧済

ディスカッション