PKIの事故から学ぶ DNSSECの必要性

セコム(株) IS研究所

島岡　政基

DigiNotar事件
知ってる人は挙手！

おそ1/3

- ✓ 認証局への不正侵入
- ✓ 証明書の不正発行
- ✓ DNSハイジャック
- ✓ SSL通信の盗聴

ここまで把握してた人は1/6程度でした

IPA神田さん資料@PKI Day2012にて DigiNotar事件を概説

http://www.jnsa.org/seminar/pki-day/2012/

スライド完全版、ストリーミングアーカイブが公開されています。

この後のパネル

- DNSハイジャックは当たり前のインシデントになるのか?(NRIセキュア中島さん)
  - これまでは抜かずの刀だったはずだが…
  - インターネットガバナンスの危機
  - (最終的にドメインの信頼性にまで議論が及ぶ??)
- 証明書の偽造は今後も起こり得るのか?(NTTソフト菅野さん)
  - WebPKIの信頼性崩壊
  - DNSの名前空間との関係についての考察

問題提起

- 証明書の不正発行・偽造問題
- DNSハイジャック

- いずれも対処にはDNSSECが不可欠
- しかしドメインの真正性そのものはレジストラに依存している
  - 標的型攻撃やフィッシング詐欺などメール主導の攻撃手法からDNS主導の攻撃手法へ変わる可能性はあるだろうか?
  - 移行障壁はそれほど高くはない