SSLサーバ証明書における RSA公開鍵の安全性について

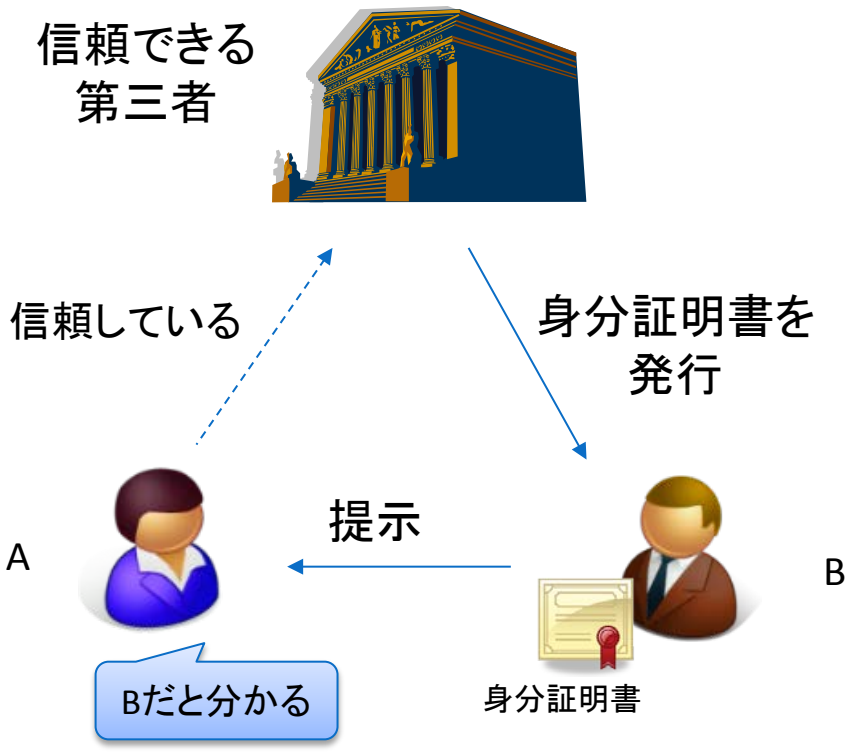
NICT ネットワークセキュリティ研究所
セキュリティ基盤研究室
盛合　志帆

目次

- はじめに
- RSA公開鍵への新たな脅威
- 公開鍵検証・可視化システム XPIA

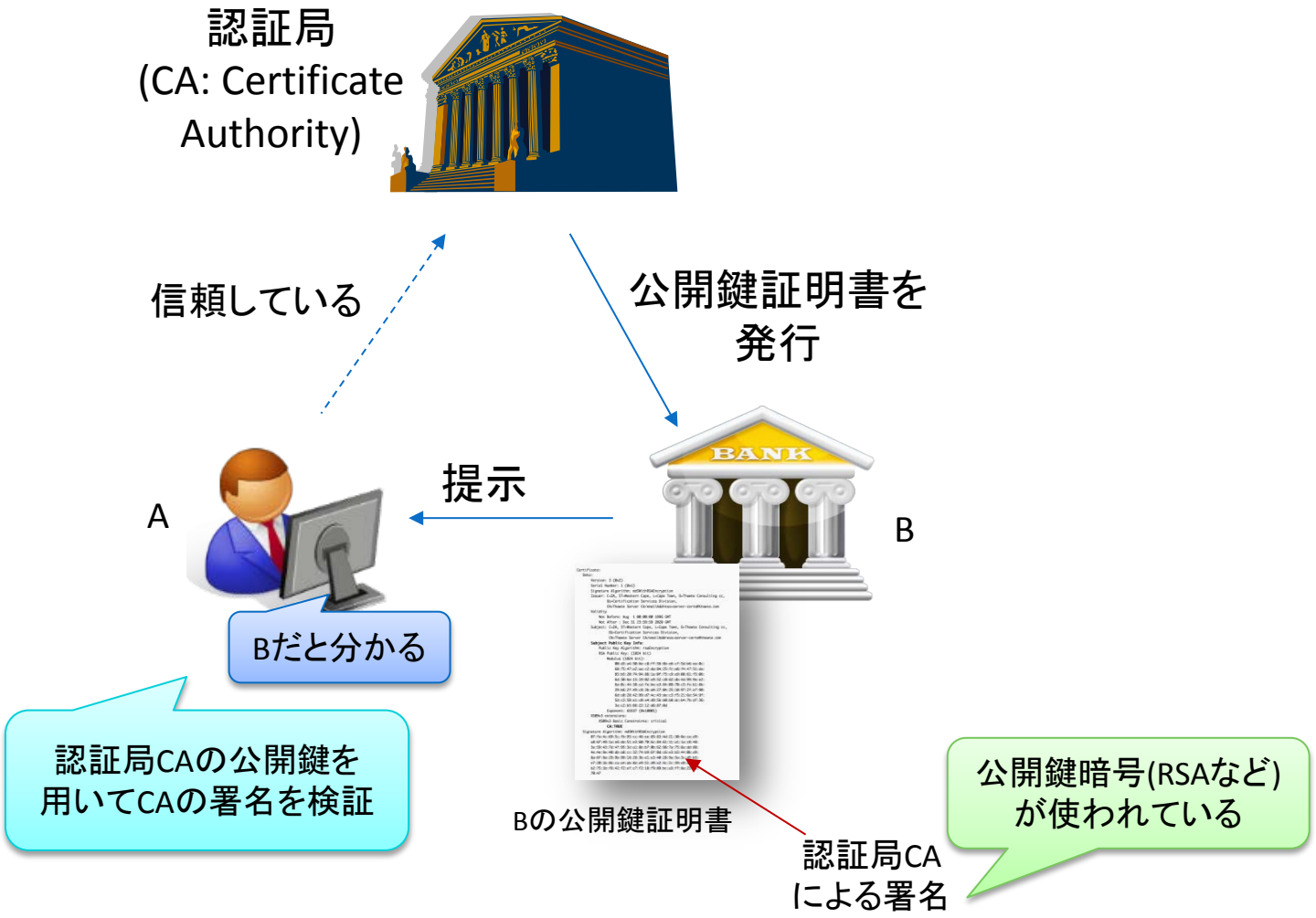
はじめに

実社会で
相手を認証するしくみ

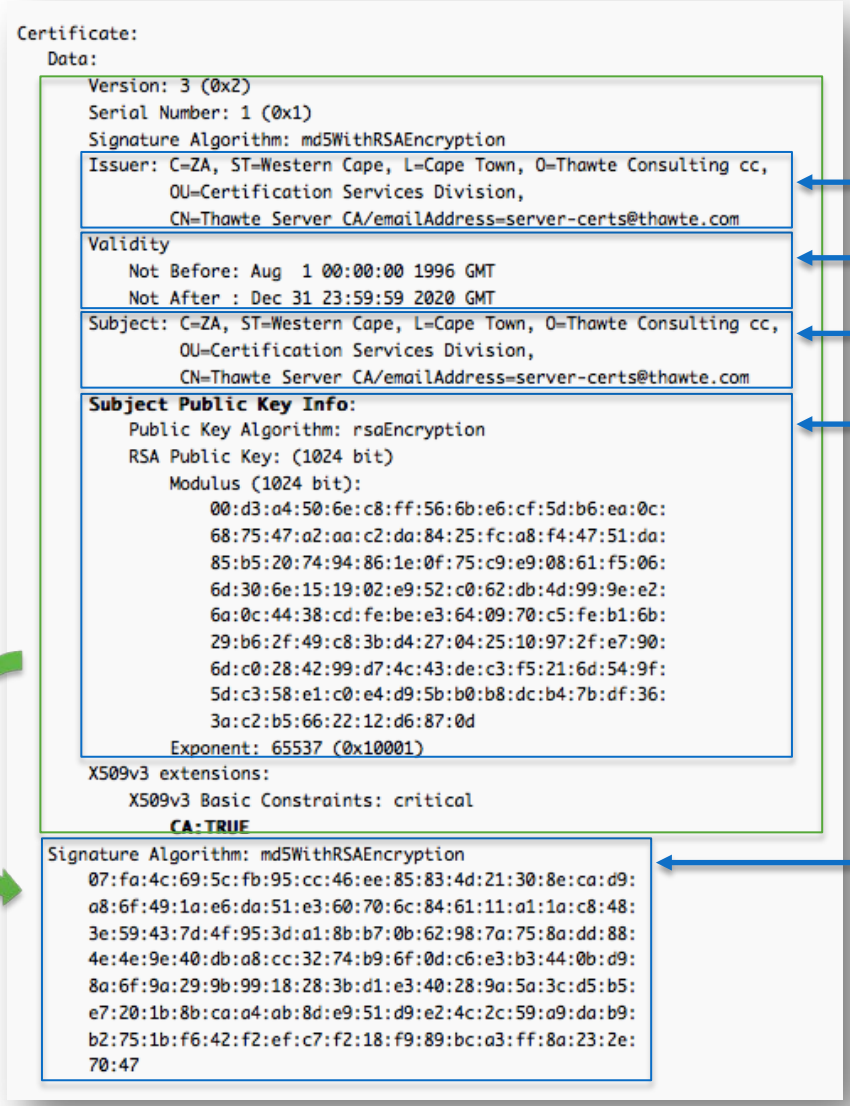


ネットワーク上で通信相手を認証するしくみ
公開鍵認証基盤(PKI)

PKI: Public Key Infrastructure



X.509公開鍵証明書



署名対象データ

発行者

有効期間

主体者

主体者の公開鍵情報
- 公開鍵アルゴリズム
- 主体者の公開鍵

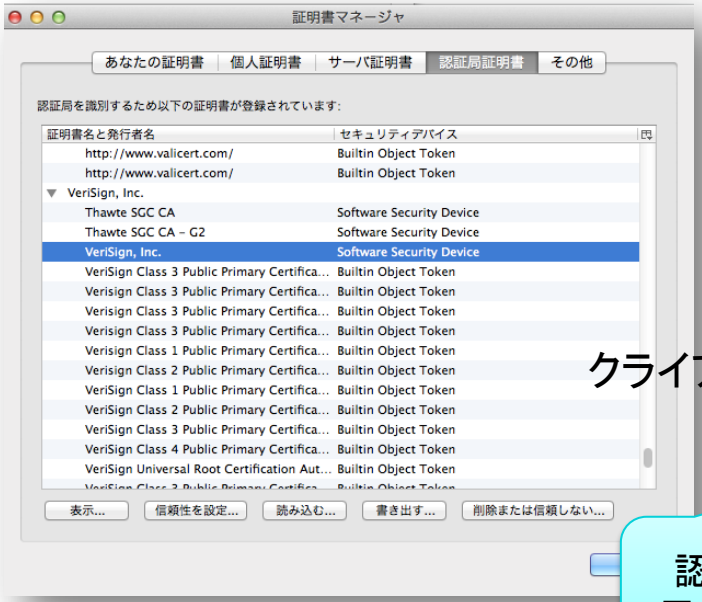
CAによる署名データ

TLS/SSLにおけるサーバ認証

認証局
(CA: Certificate Authority)

信頼している

公開鍵証明書を発行



主要な認証局の公開鍵証明書は
あらかじめブラウザに
組み込まれている

提示

クライアント

サーバ

サーバの身元
が確認できる

サーバの公開鍵証明書
(サーバ証明書)

認証局CAの公開鍵を
用いてCAの署名を検証

認証局CA
による署名

RSA公開鍵への新たな脅威

RSA


Rivest, Shamir, Adleman

- 1977年に発明され、最も利用されている公開鍵暗号
- 大きな合成数の素因数分解が困難であることを安全性の根拠としている
- 公開鍵(n, e)と秘密鍵 d の鍵ペアを作成し、公開鍵を公開

大きな2つの素数 p, q を生成
公開鍵: $n = p \times q$, e を選択 (65537 =2^{16}+1がよく使われる)
秘密鍵: $d = e^{-1} \pmod{(p-1)(q-1)}$

暗号化(平文m から暗号文c を作成): $c = m^e \pmod{n}$
復号(暗号文c からもとの平文m を得る): $m = c^d \pmod{n}$

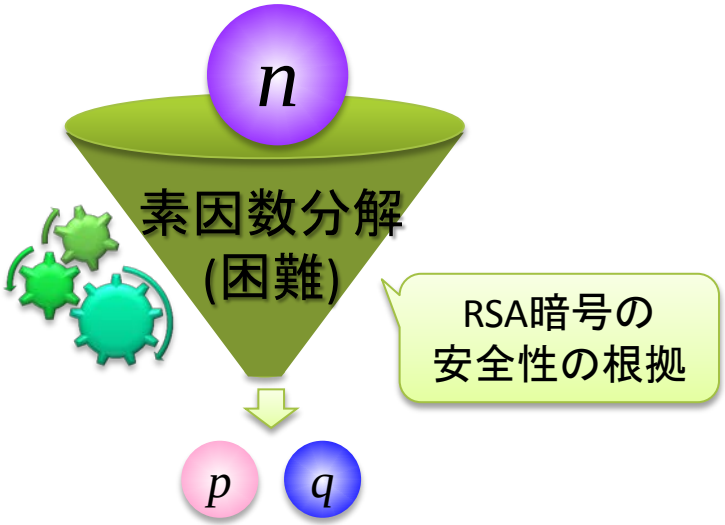
RSA公開鍵への新たな脅威

- 同じ素数を因子として含む公開鍵が多数生成され、公開鍵証明書等に組み込まれて利用されていることが明らかに.
  - Heninger et.al., “Mining your Ps and Qs: Detection of widespread weak keys in network devices”, Usenix Security 2012.
    - TLS scan (約585万, 2011/10)
    - SSH scan (約661万, 2012/2-4)
  - Lenstra et.al., “Public Keys”, CRYPTO 2012.
    - The Electronic Frontier Foundation (EFF) SSL Observatory (約619万, 2011/11)
      - https://www.eff.org/observatory

同じ素因子を含むと、何が起きるのか

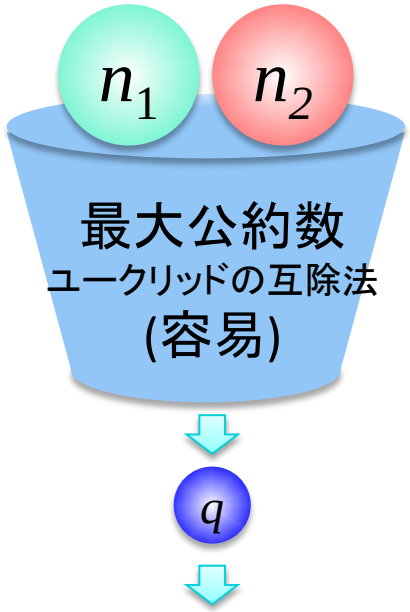
2つの大きな素数: p, q

RSAの公開鍵: $n = p \times q$



2つの公開鍵: n_1, n_2

$n_1 (= p_1 \times q)$ $n_2 = (p_2 \times q)$



2つの公開鍵 n_1, n_2が
容易に素因数分解できてしまう

$n_1 \Rightarrow p_1 \times q$ $n_2 \Rightarrow p_2 \times q$

p_1 q p_2 q

RSA公開鍵への新たな脅威

- RSAの安全性は大きな数の素因数分解が難しいことで支えられている.

  ⇒これまで長い鍵長(2048ビット等)のRSAを使っていれば安全とされてきた.

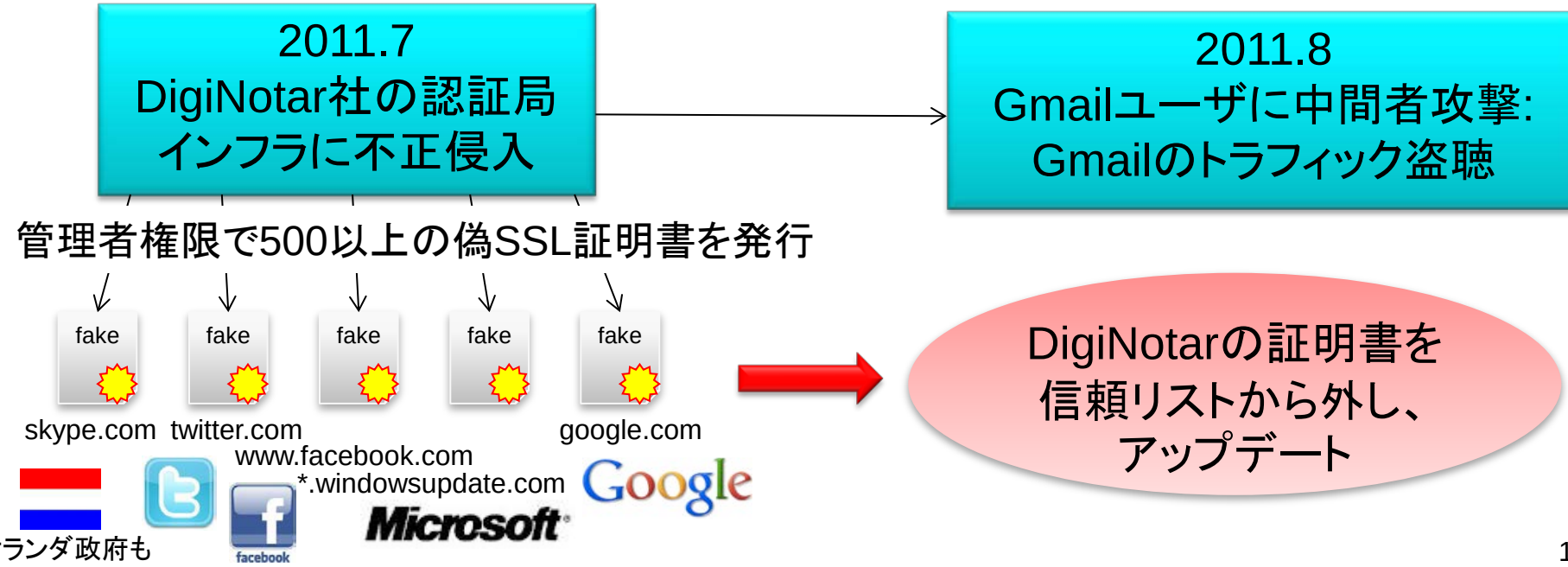
- 大きな数の素因数分解は難しいが、2つの大きな数の最大公約数を求めることは容易
- もし、2つのRSAの公開鍵に同じ素数が含まれていた場合、最大公約数を求めることで簡単にその素数が分かり、素因数分解でき秘密鍵が暴かれてしまう.

脅威の原因

- RSA鍵生成時に同じ素数が生成されている
  - 素数生成時の乱数生成のseedがランダムでない
    - 特にルーター、ファイアウォールや組み込みデバイス等（物理乱数源を取得する手段が乏しい）
  - RSAの鍵生成時の疑似乱数生成モジュールに脆弱性
  - そもそも9個の素数しか生成しないモジュールも
  - 出荷時のデフォルト鍵がそのまま利用されている

RSA秘密鍵が暴かれると？

- 認証局の秘密鍵が暴かれた場合、認証局になりすまして署名が可能になり、不正SSL証明書などが発行できる →偽サイトへの誘導など
- [参考事例] DigiNotarの不正証明書問題 (2011年)



課題

- この新たな脅威の実態が把握されていない
  - 発表されたのは過去のある時点での統計情報
    → 現在の状況は不明、個々の実態も不明
  - 日本国内の実態は?
  - 多くのユーザが利用しているサイトは安全なのか

XPIA構築の目的:実態の把握

公開鍵検証・可視化システム
XPIA (エクスピア)

X.509 certificate Public-key Investigation and Analysis system

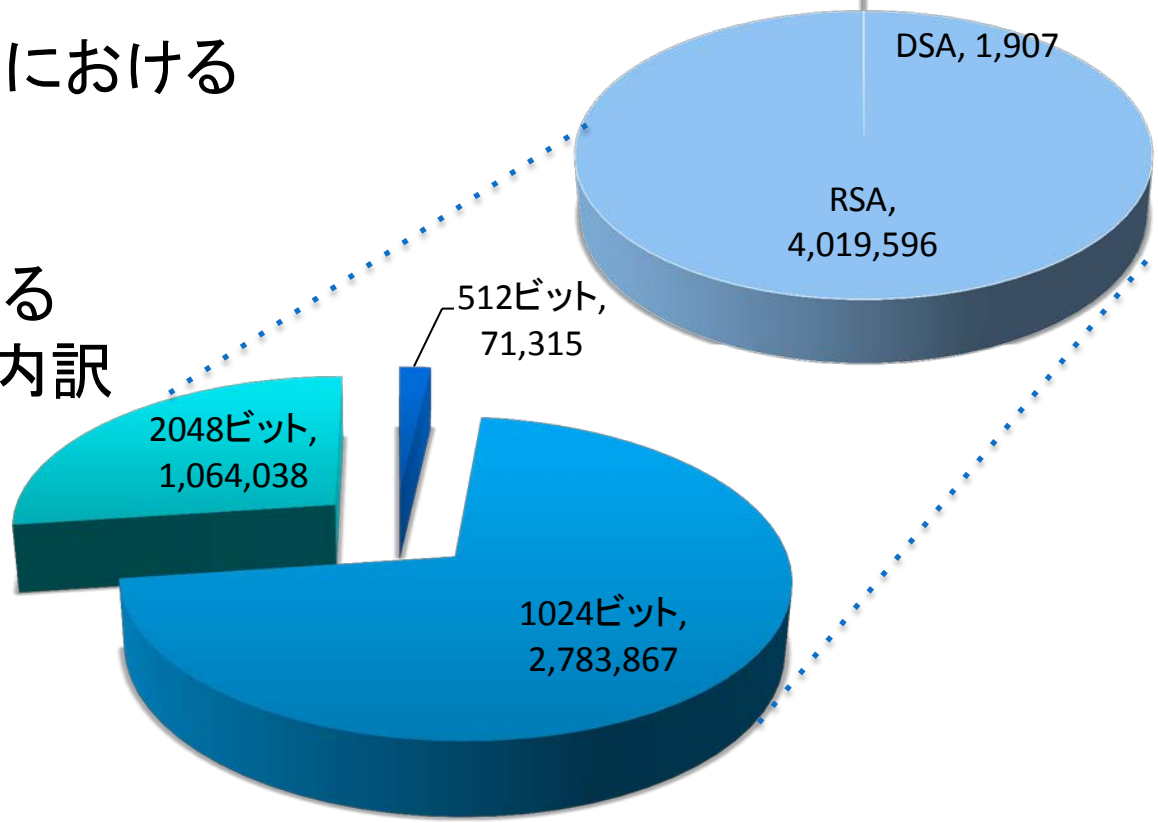
“Supercalifragilisticexpialidocious”（メリー・ポピンズ）
困難な状況に陥った際、唱える事で万事解決すると言われる呪文

XPIAのシステム概要

解析対象のSSL公開鍵証明書

SSL Observatory (2010) における
RSA と DSA の内訳

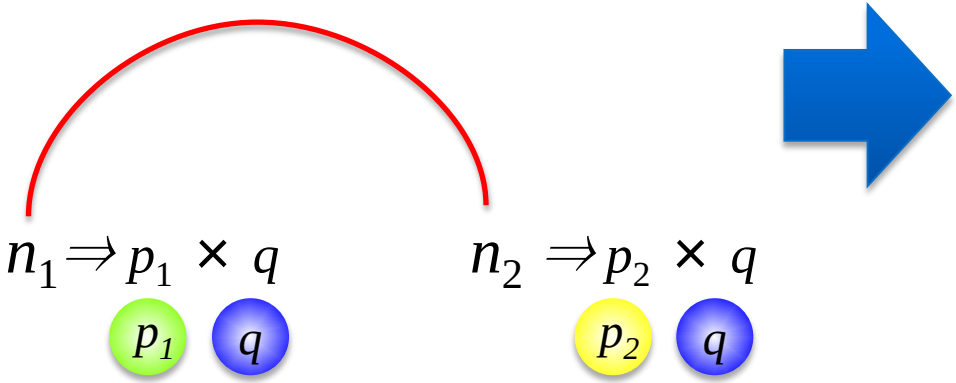
SSL Observatory における
RSA公開鍵のサイズ別内訳

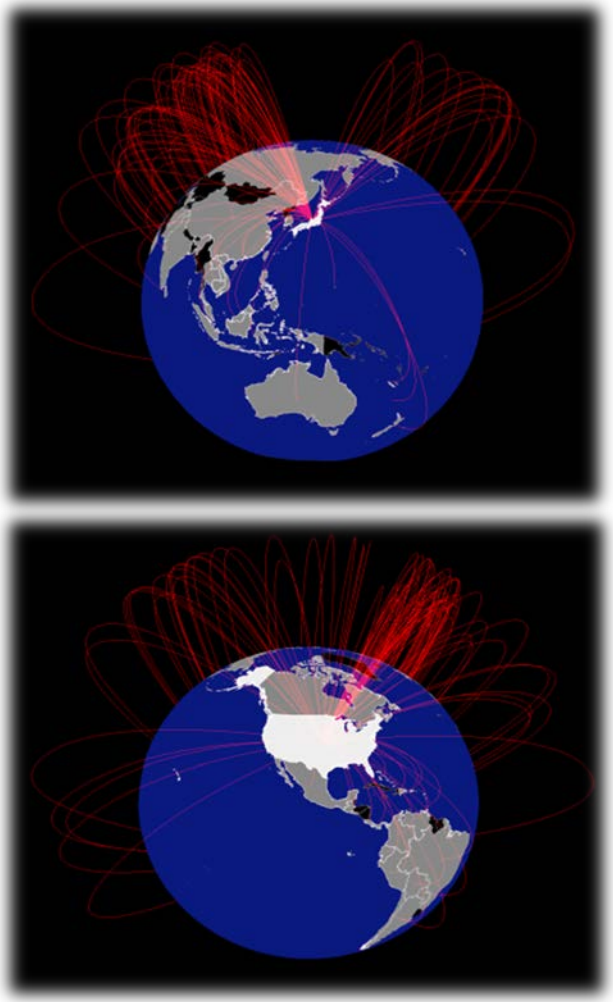


8,703個の異なるRSA公開鍵が素数を共有
⇒ 8,703台のSSLサーバが危険な状態

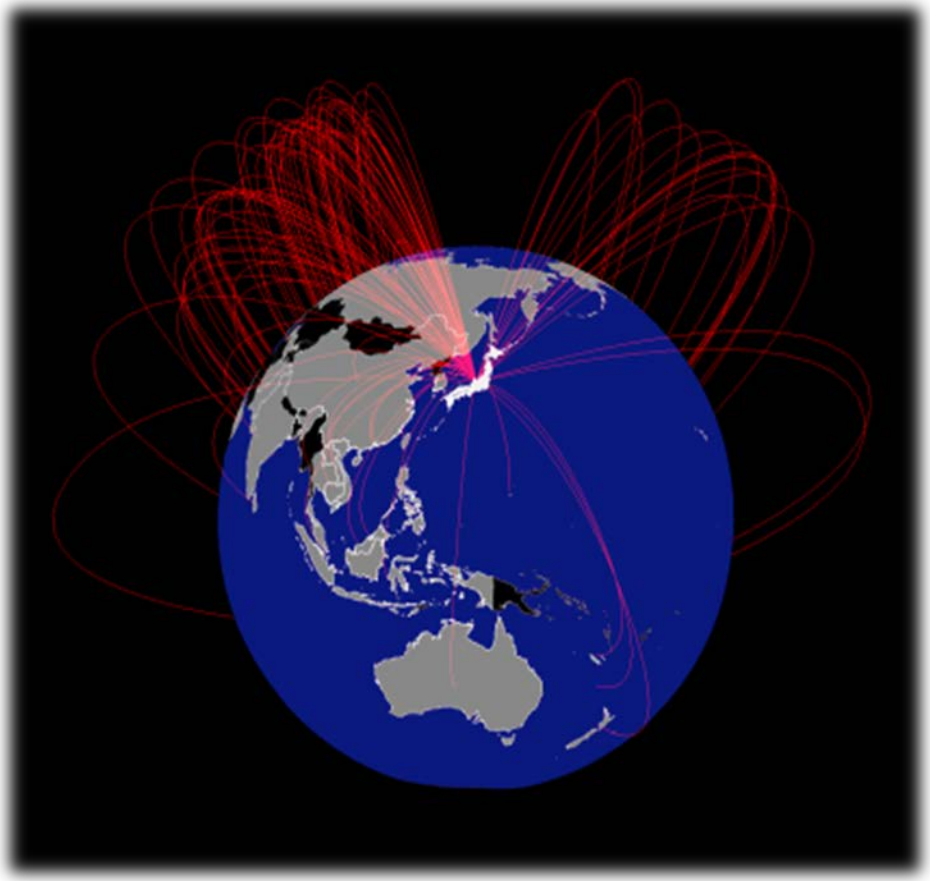
可視化

公開鍵証明書が素因子を共有している
2つのSSLサーバ間を赤い線で結ぶ
(サーバ位置情報は国情報のみ)



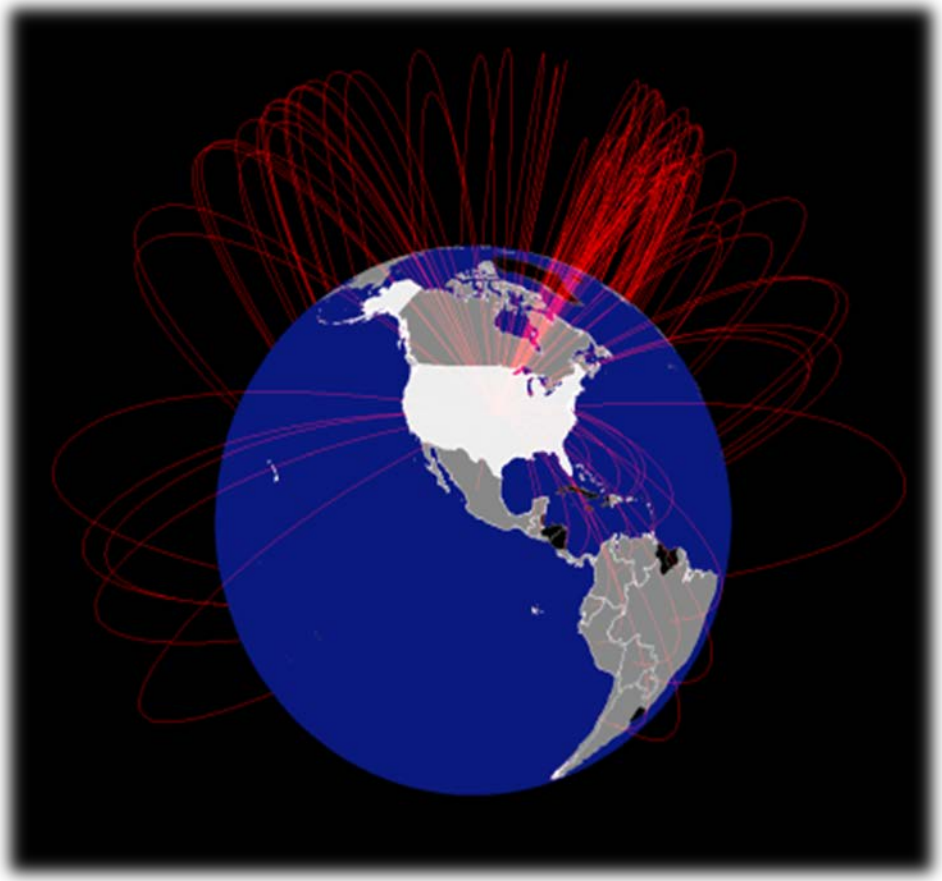


可視化（日本）



XPIAによる脆弱性分布の表示例

可視化（米国）



XPIAによる脆弱性分布の表示例

XPIAでの解析結果

8,703 (171) 個:SSL Observatory に含まれる
RSA 公開鍵で素因数分解できるもの

括弧内は日本

3,260 (104) 個：公開鍵を
ダウンロード可能

5,443 (67) 個：公開鍵を
ダウンロード不可能

ほとんどがタイムアウト

2,611 (90) 個：いまだに
脆弱な公開鍵を利用

649 (14) 個：異なる
公開鍵に更新

危険な状態にある2,611サイトを発見

XPIAの活用可能性

- 現在利用されている公開鍵証明書のRSA公開鍵の脆弱性の有無の把握
- 公開鍵証明書で利用されている公開鍵の種別・鍵長のリアルタイムでの把握
  - RSA/DSA/ECDSA等の利用分布
  - 世界的な傾向、国別、セクタ別の統計情報
  - RSA-2048への移行状況の把握
- 公開鍵証明書新規発行時の脆弱性チェック

おわりに

- 公開鍵検証・可視化システムXPIAを開発、SSLサーバ認証で最も利用されているRSA暗号に関する脆弱性の実態把握に成功
- 今後の展開
  - わが国の電子政府等において, 暗号技術を安全に利用するために活用
  - 本システムをSSLに対する他の攻撃(BEAST攻撃, RC4の統計的偏りを利用した攻撃) にも対応できるよう拡張