NRIセキュアテクノロジーズ

DNSSEC スプリングフォーラム2013

PKIの事故から学ぶDNSSECの必要性
～DNSスプーフィング攻撃の考察～

2013年5月29日

NRIセキュアテクノロジーズ株式会社
テクニカルコンサルティング部
セキュリティコンサルタント

中島　智広

〒105-7113
東京都港区東新橋1-5-2 汐留シティセンター

はじめに

- DNSSECの必要性はキャッシュ汚染攻撃のメカニズムそのものや遠方の事例で語られることが多く実感を得にくかったと考えています。

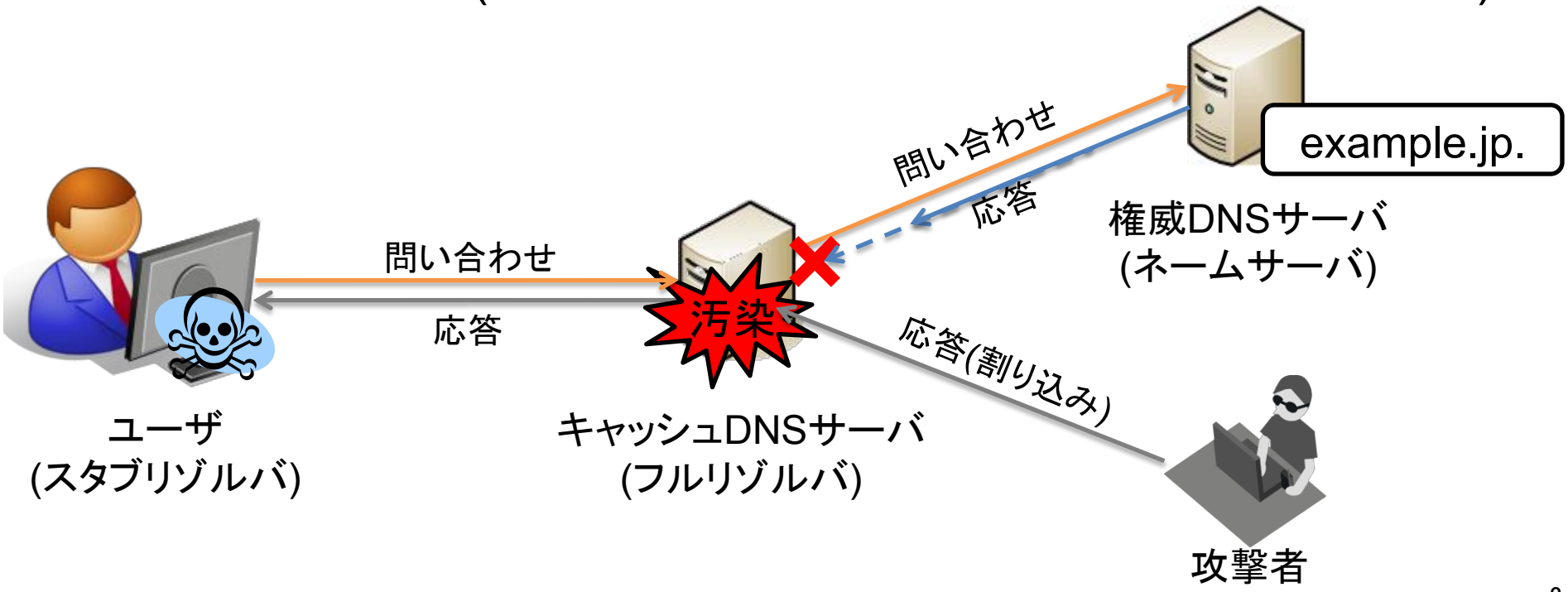
- 今回はDigiNotar事件や昨今の身近なセキュリティ侵害事例を踏まえ、インターネットセキュリティを構成する要素として必要性を再整理します。

- 恐怖を煽ってDNSSEC導入を焚き付ける意図はありません。必要性を見定めることを目標としています。

DNSスプーフィング

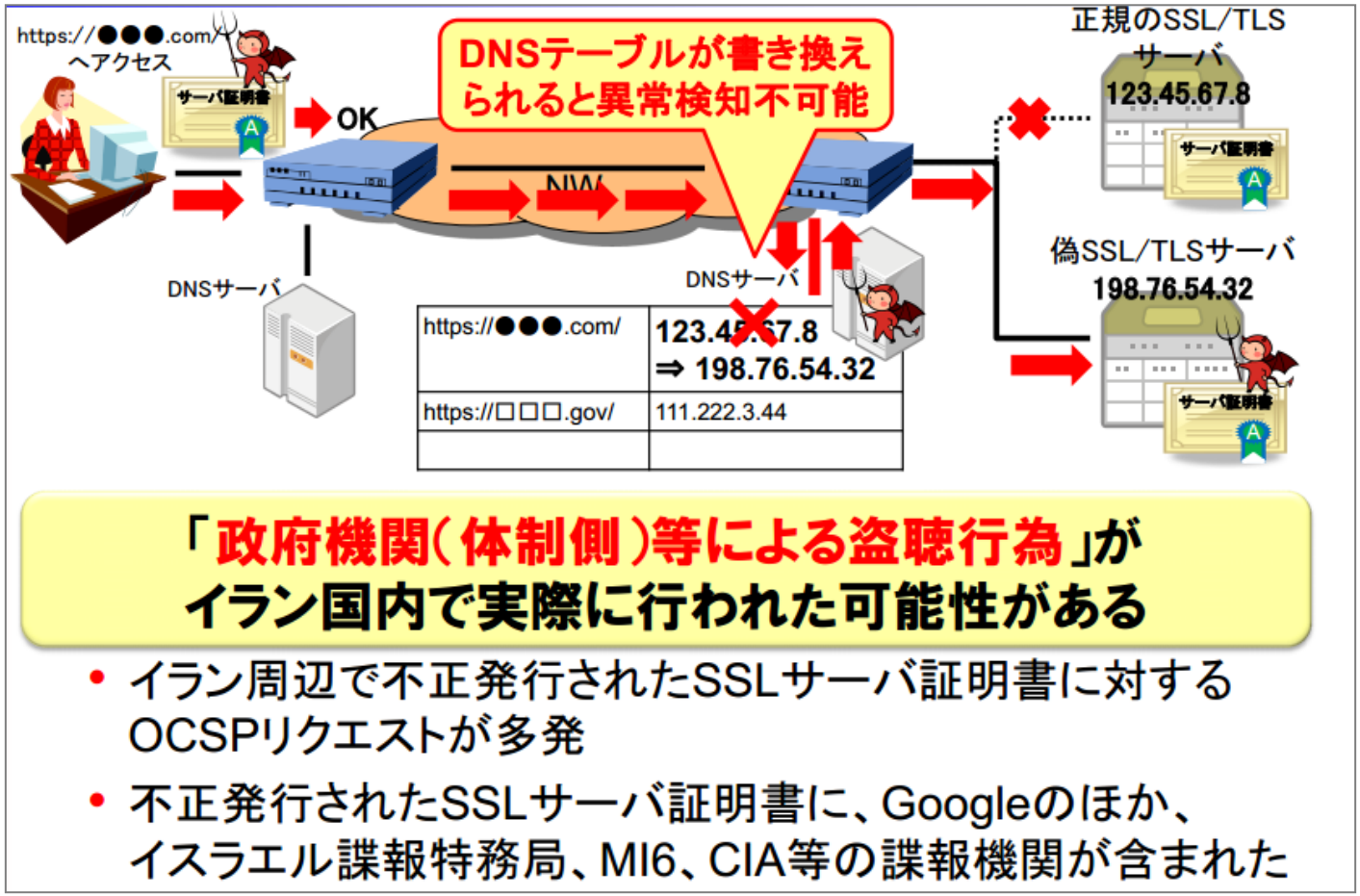
■DNSの問い合わせに対し偽の応答を送り込む技法の総称

DNSスプーフィングの例(応答への割り込みによるキャッシュ汚染攻撃)



DigiNotar事件におけるDNSスプーフィング

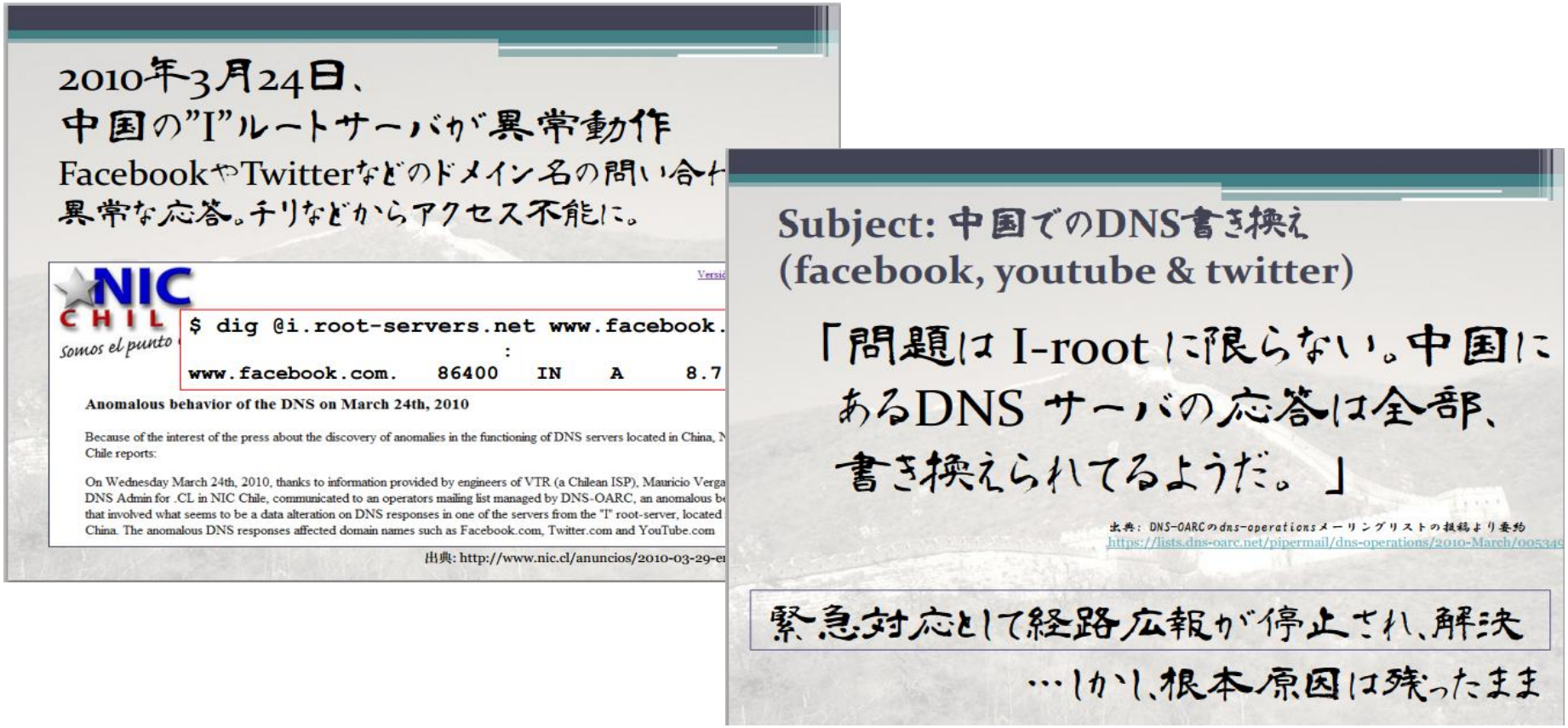
■国家規模のDNSスプーフィング



原典:PKI Day 2012 神田雅透氏「 サイバー攻撃ツールとしての公開鍵証明書の役割」

既視感

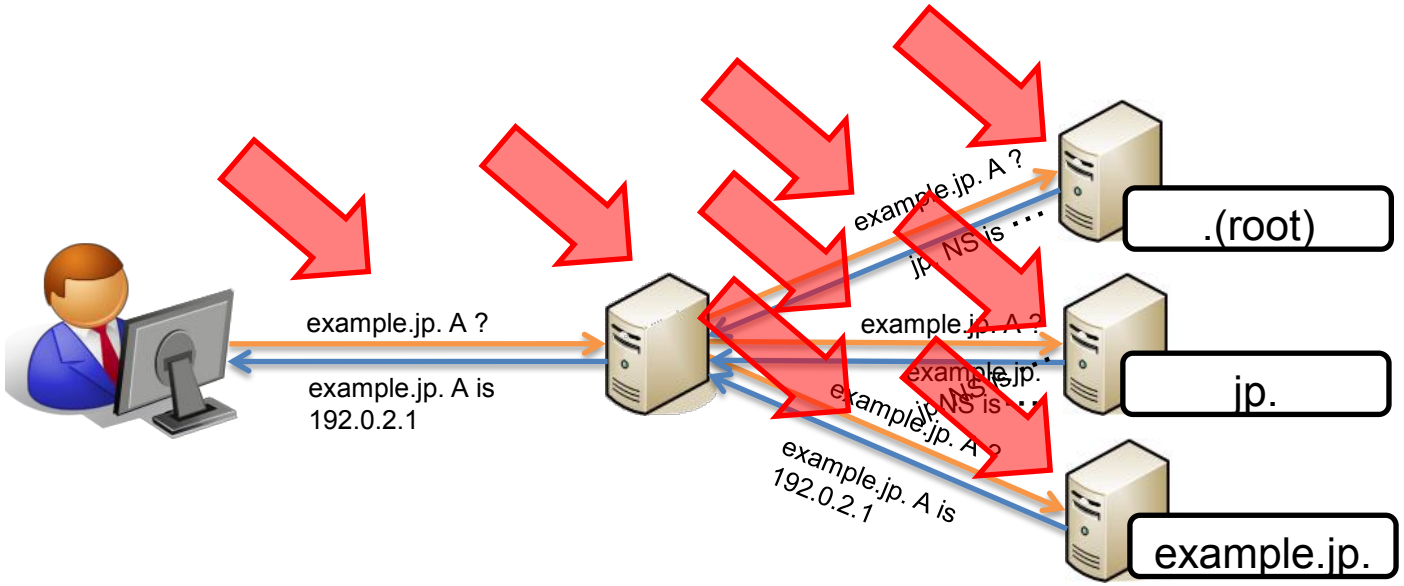
■国家規模のDNSスプーフィングは初めてではない



原典：JANOG27 戸山純一氏「特定の条件下で発生する通信エラーに関する考察」

改めてDNSスプーフィング考察

- DNSは全世界のサーバが協調して動作する分散型データベースと言えば聞こえはいいが、どこにでも悪意の入る余地のある脆弱な仕組み



想定される脅威

悪意ある第三者

■攻撃手法

- DNS応答への割り込みによるキャッシュ汚染攻撃
- サーバの脆弱性を突くなど何らかの手法によるDNSサーバを乗っ取ったDNS応答の改ざん

■対策手法

- 改ざんを検知する仕組みの導入
- 攻撃を検知・防御する仕組みの導入

国家規模の何か

■攻撃手法

- 通信経路ハイジャック、DNSサーバへの介入などによるDNS応答そのものの改ざん

■対策手法

- 改ざんを検知する仕組みの導入

素のDNSでこれらを防ぐことは困難

セーフティネットの不存在

■これが覆ったのがDigiNotar事件、
もはやPKIはDNSスプーフィングに対するセーフティネットたり得ない

DNSスプーフィングの現状

- DNSスプーフィングの影響が絶大なことは知る人ぞ知る状況
  効果的に使われた攻撃事例も世の中に広く知られる

- 応答への割り込みによるキャッシュ汚染の効率性も知る人ぞ知る状況
  様々な条件で変わるが気長にやれば有効な攻撃となり得る

$$0.5 \leq 1 - (1 - \frac{Rr \times W}{N \times 65536 \times 65536})^{t \times Rq}$$

Source:JANOG19 "これでいいのかTTL"民田さん@JPRSを改変

Rr:応答攻撃のレート
Rq問い合わせ攻撃のレート
W:正規応答が返ってくるまでの時間
N:ネームサーバの数
t:時間

- 応答への割り込みによるキャッシュ汚染だけがDNSスプーフィングの
  攻撃手法ではない

攻撃手法のパラダイムシフト

- 最も弱い鎖の輪(WeakestLink)が狙われる
- 流行した攻撃手法は対策が進むため、
  次の最も弱い鎖の輪(WeakestLink)を狙う攻撃にシフトしていく
- 攻撃者は常に心の隙を狙う「成功する確率は低いだろう」
- 攻撃手法の有効性が広く認知されることで流行する

DNSスプーフィングの狙われやすさはどのくらい？

[参考事例] アカウント推測によるアカウントハッキングの流行

大量のユーザのID/パスワードの組み合わせを用い
ログイン試行を行うことでアカウントを乗っ取る攻撃手法
総当たり型、辞書型、リバース型、リスト型などのバリエーション有

■流行の背景
- 他の効率的な攻撃手法への対策が進んだ
- 試行すれば当たること、攻撃による旨味(マネタイズ手法)が認知された
- 広帯域回線、ボットの活用、リストの流通など試行の効率性を高める手法が確立

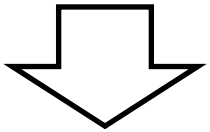
■サービス提供者の直面する課題
- 被害が拡大することでユーザのID/パスワード管理の責任と言い切れなくなり、強固な認証オプションや監視といった対策を求められる
- 実際にセキュリティ侵害が発生すると想像以上のコストが必要

大量の試行を必要とする攻撃も効果が認知されれば流行する

[仮説] DNSスプーフィング流行に至るパラダイムシフト

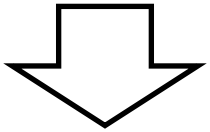
■前提

- 大量の試行を必要とする
  応答への割り込みによるキャッシュ汚染攻撃は効率が悪く好まれない
- DNSスプーフィングだけでは旨味がない



■条件

- 他の攻撃手法の対策が進む
- DNSスプーフィングの有効性が広く認知される
- 応答への割り込みによるキャッシュ汚染が試行すれば成功することが広く認知される

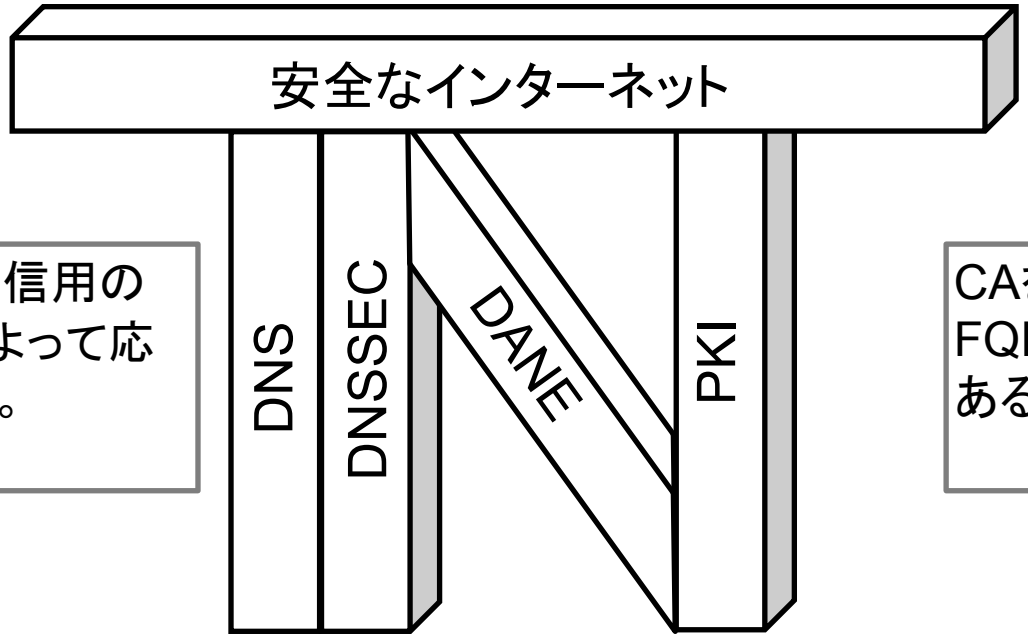


■結果

- 対策が遅れているDNSスプーフィングが流行する可能性
- サービス提供者にDNSスプーフィングへの対応責任が求められる可能性

DNSスプーフィングと一連の攻撃を防ぐアプローチ

■DANEは安全なインターネットを支えるDNSとPKIの柱をつなぐ筋交い
※仕様としてDNSSECが必須



.(root)を基点とした信用の連鎖、委譲関係によって応答の正当性を表す。

CAを基点とした信用の連鎖、FQDN管理者の実態をある一定の基準で証明する。

信用の基点の冗長化により攻撃に気づけることが肝要

DNSSEC導入が進まない日本

■DNSSEC.JP/DNSOPS.JPの功罪

- 功：日本国内におけるDNSSECの導入・運用ノウハウを蓄積・共有した
- 罪：DNSSECの導入・運用が高負荷・高コストであると印象づけてしまった

■文化

- 事なかれ主義
- 過剰な高品質要求、トラブルに敏感
- 黒船襲来にあたふた

DNSSEC導入が進まない間に脅威が増大している可能性

まとめ

- DNSスプーフィング事例は広く知られる状況、脅威は二つ
  - 悪意のある第三者
  - 国家規模の何か
- 攻撃手法のパラダイムシフト
  - 素のDNSはインターネットセキュリティにおける
    最も弱い鎖の輪(Weakest Link)の一つである可能性、流行は時間の問題？
  - DNSスプーフィングに対するセーフティネットは存在しない
- 脅威の増大と対応責任
  - DNSSEC導入が進まない間に脅威が増大している可能性
  - サービス提供者に求められる対応責任、侵害事故に支払うコストは膨大

改めてDANE/DNSSECは不要でしょうか？