DNSキャッシュポイズニング脆弱性について

有限責任中間法人 JPCERTコーディネーションセンター

2008年10月3日

この資料について

2008年7月、DNS キャッシュポイズニングの脆弱性に対する攻撃方法の詳細が、海外のセキュリティ研究者により公開されました。遠隔の第三者によって DNS キャッシュサーバが偽の DNS 情報で汚染されることにより、ドメイン名が乗っ取られ本来の宛先への通信を横取りされるなど、深刻な問題が発生する可能性があります。

JPCERT/CCでは、引き起こされる被害を最小限に抑えるため、サーバ管理者の方を対象に、DNS の仕組みと本脆弱性の本質と対策手法を解説する勉強会を開催しております。

今回、多くのサーバ管理者の方々にご覧いただけるよう、勉強会の資料を公開しました。

注: この文書は、コンピュータセキュリティインシデントに対する一般的な情報提供を目的とするものであり、特定の個人や組織に対する、個別のコンサルティングを目的としたものではありません。また JPCERT/CC は、この文書に記載された情報の内容が正確であることに努めておりますが、正確性を含め一切の品質についてこれを保証するものではありません。この文書に記載された情報に基づいて、貴方あるいは貴組織がとられる行動 / あるいはとられなかった行動によって引き起こされる結果に対して、JPCERT/CC は何ら保障を与えるものではありません。

Copyright® 2008 JPCERT/CC All rights reserved.

アジェンダ

- DNSの仕組み
- キャッシュポイズニング攻撃
  - 従来の攻撃手法
  - 2008年7月に明らかになった攻撃手法
- 対策

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み - 概要

- DNS = Domain Name System

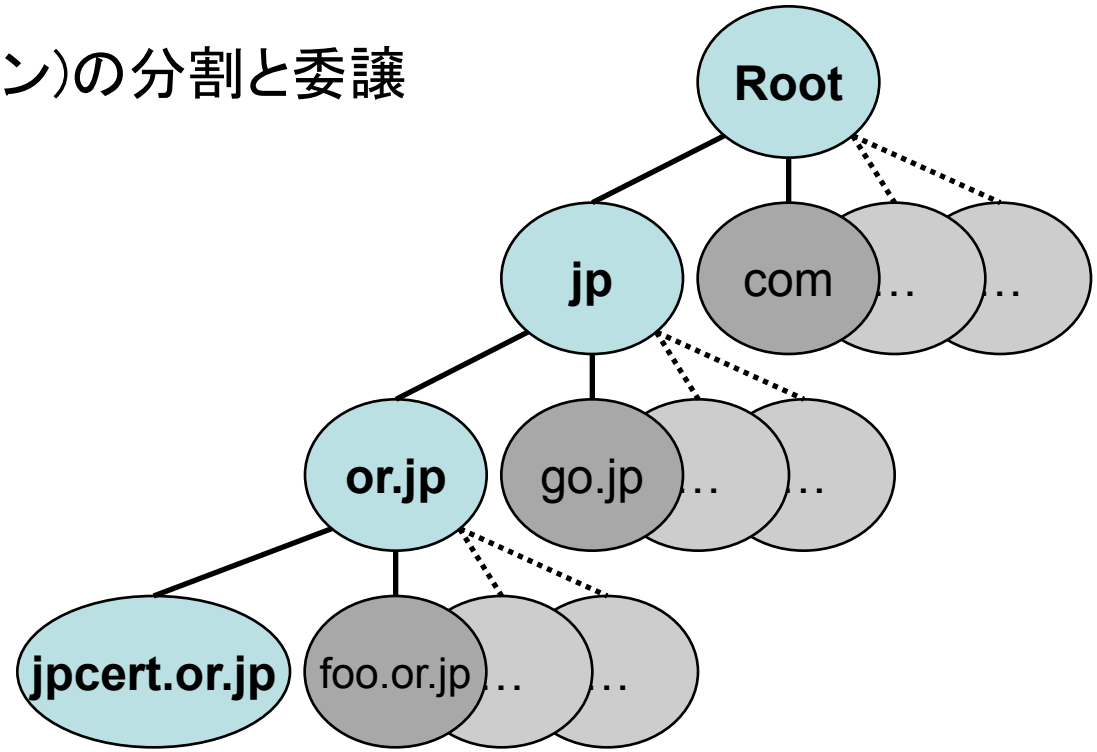
- 基本的な役割
  - インターネットにおける電話帳
    - ホスト名⇔IPアドレスを変換する(名前解決)
      - www3.example.com を 1.2.3.4へ
      - 1.2.3.4をwww3.example.comへ
    - 各ドメインのネームサーバがどれなのか教える
    - 各ドメインのメールサーバがどれなのか教える

- 位置づけ
  - インターネットにおける基本的なサービスの一つ
  - メールやWebなどの利用時に(通常意識せずに)使用
    - http://www.jpcert.or.jp/
    - To: foo@jpcert.or.jp, Cc: bar@jpcert.or.jp

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み – 階層化と分散化

- ルートネームサーバを頂点としたツリー構造
- 管理する範囲(ゾーン)の分割と委譲



Copyright® 2008 JPCERT/CC All rights reserved.

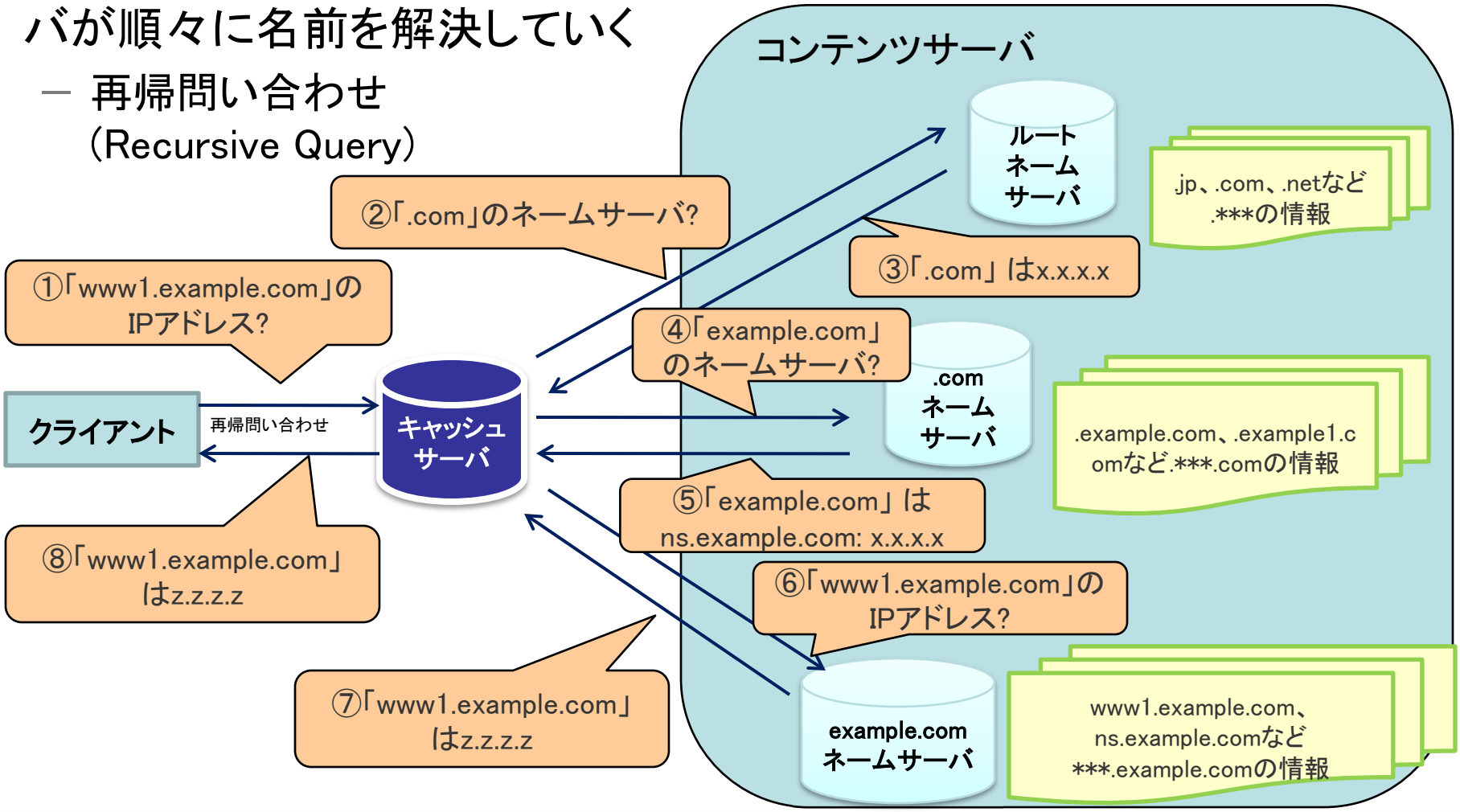
DNSの仕組み – 構成要素

- サーバ(DNSサーバ)
  - コンテンツサーバ
    - 当該ドメインのゾーンのIPアドレス、ホスト名の対応を管理
    - 当該ドメインの情報だけを返答
  - キャッシュサーバ
    - クライアントからの問い合わせに返答
    - クライアントの代わりにコンテンツサーバに問い合わせ
    - 結果の保存(キャッシュ)
- クライアント(リゾルバ)
  - キャッシュサーバへの問い合わせ

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み – 名前解決

- クライアントはキャッシュサーバに問い合わせをし、キャッシュサーバが順々に名前を解決していく
  - 再帰問い合わせ (Recursive Query)



Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み – 問い合わせ/返答の例

JPCERT CC®

- 問い合わせに対して、関連する情報も付加して返答

例:　% dig www.jpcert.or.jp

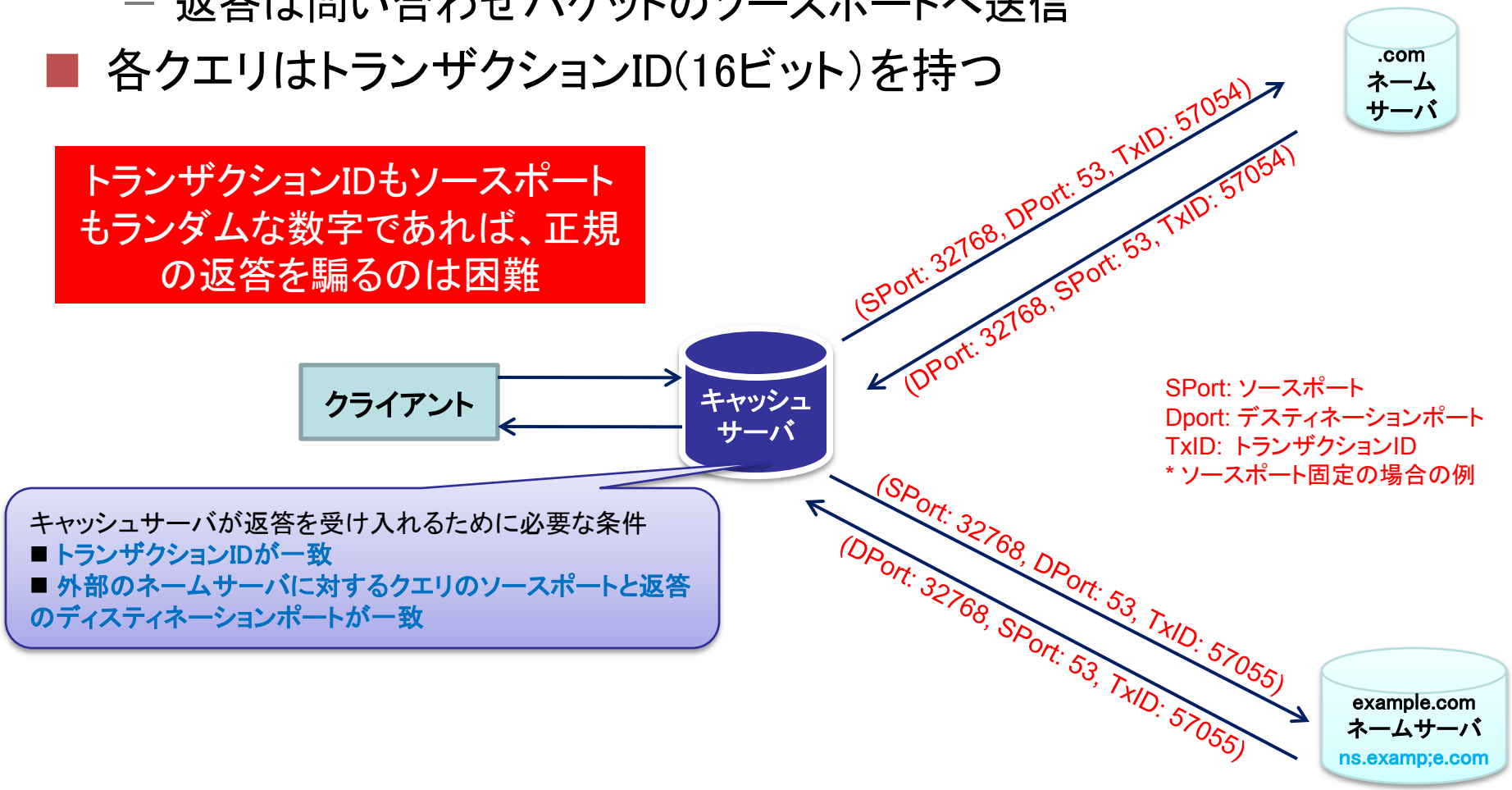
```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43922
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.jpcert.or.jp.              IN      A

;; ANSWER SECTION:
www.jpcert.or.jp.    86400     IN      A     210.148.223.7

;; AUTHORITY SECTION:
jpcert.or.jp.        65330     IN      NS    dns-a.iij.ad.jp.
jpcert.or.jp.        65330     IN      NS    ns.jpcert.or.jp.

;; ADDITIONAL SECTION:
ns.jpcert.or.jp.     65330     IN      A     210.148.223.4
dns-a.iij.ad.jp.     65330     IN      A     210.130.1.45
```

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み
– 問い合わせの識別：トランザクションIDとソースポート

- 問い合わせにはUDPプロトコルが使用される
  - 返答は問い合わせパケットのソースポートへ送信
- 各クエリはトランザクションID(16ビット)を持つ

トランザクションIDもソースポートもランダムな数字であれば、正規の返答を騙るのは困難

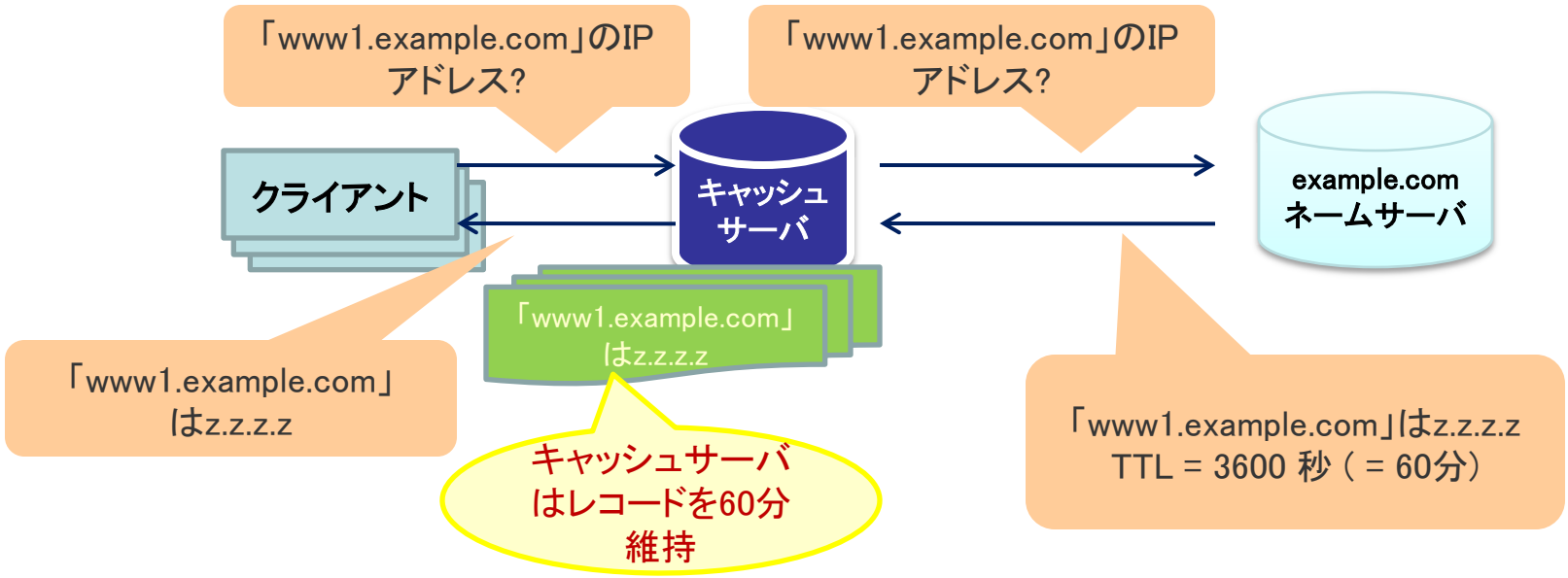


キャッシュサーバが返答を受け入れるために必要な条件
- トランザクションIDが一致
- 外部のネームサーバに対するクエリのソースポートと返答のディスティネーションポートが一致

Copyright® 2008 JPCERT/CC All rights reserved.

DNSの仕組み – キャッシュとTTL

- キャッシュサーバは一度名前解決した情報を一定期間保存する
- 保存する期間のことを「TTL（Time To Live）」という
- TTLはコンテンツサーバで設定されている



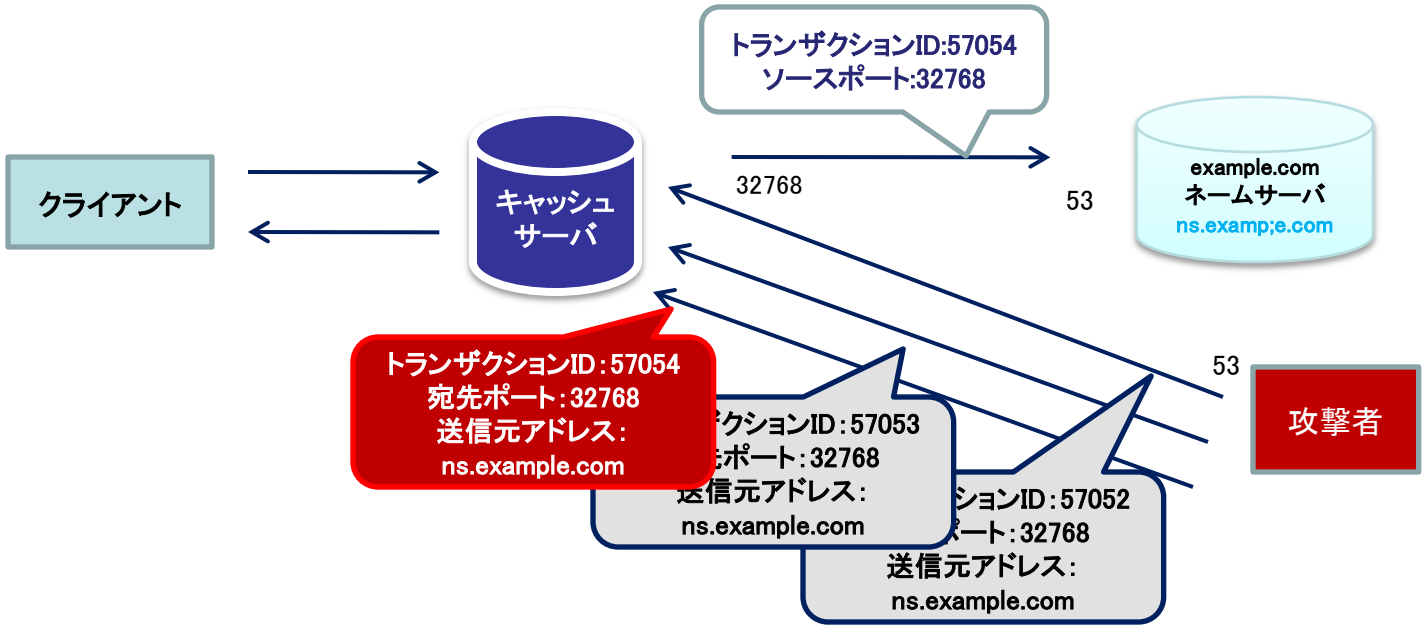
Copyright® 2008 JPCERT/CC All rights reserved.

キャッシュポイズニング攻撃
～従来の攻撃手法～

Copyright® 2008 JPCERT/CC All rights reserved.

DNSキャッシュポイズニングに関わる問題

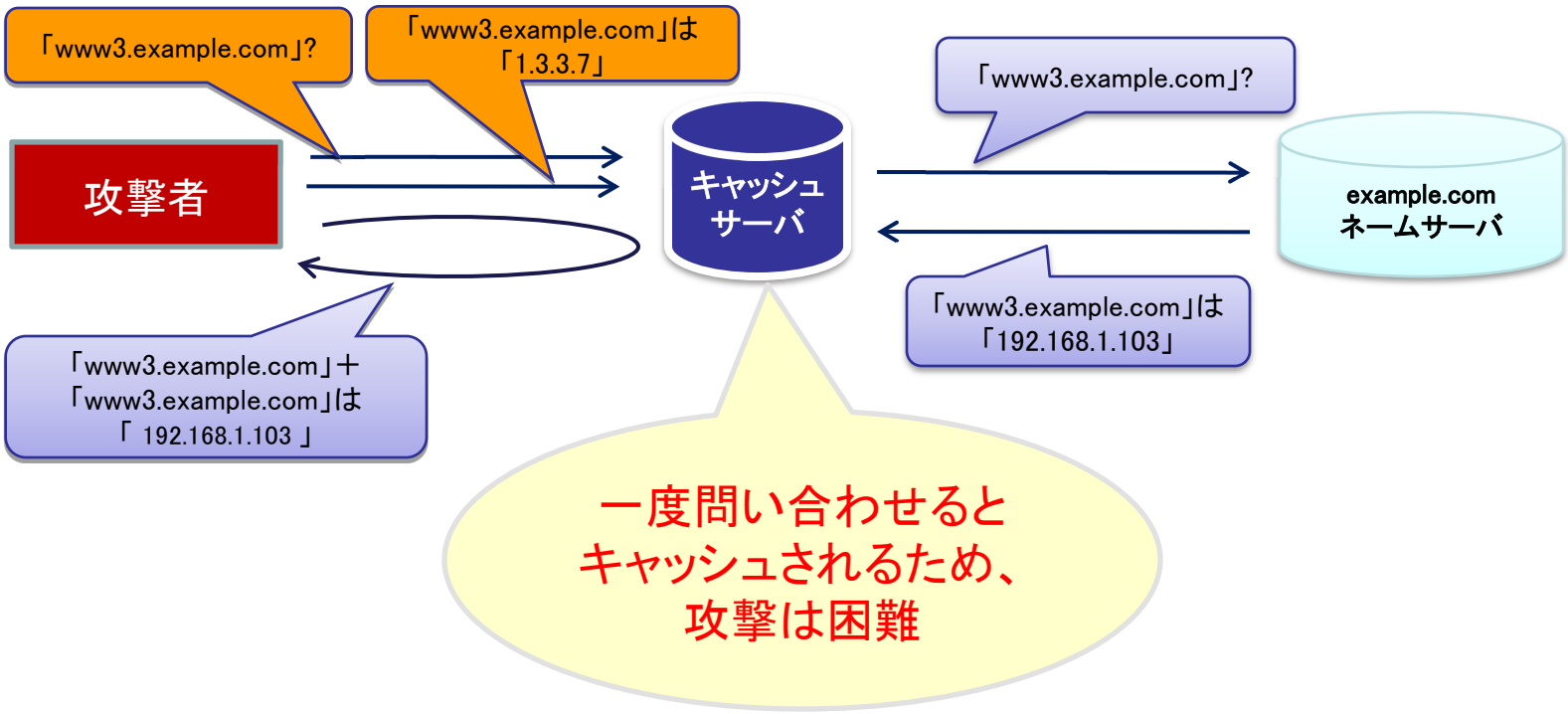
- 正規の返答を騙るには、トランザクションIDとソースポートが推測できればよい。
- 攻撃者はトランザクションIDとソースポートを推測して偽のパケットを送出する
  - 多くのDNSサーバではソースポートが固定（2008年8月の対策パッチ以前）
  - 攻撃者はトランザクションID(16ビット)のみ推測すれば良い
    - 1パケット送出すれば1/65,536の確率で一致
    - 数多く攻撃パケットを送出すれば一致する可能性が増加



Copyright® 2008 JPCERT/CC All rights reserved.

従来の攻撃手法

- 従来のキャッシュポイズニング手法：ポイズニングしたいホスト名の問い合わせを送る



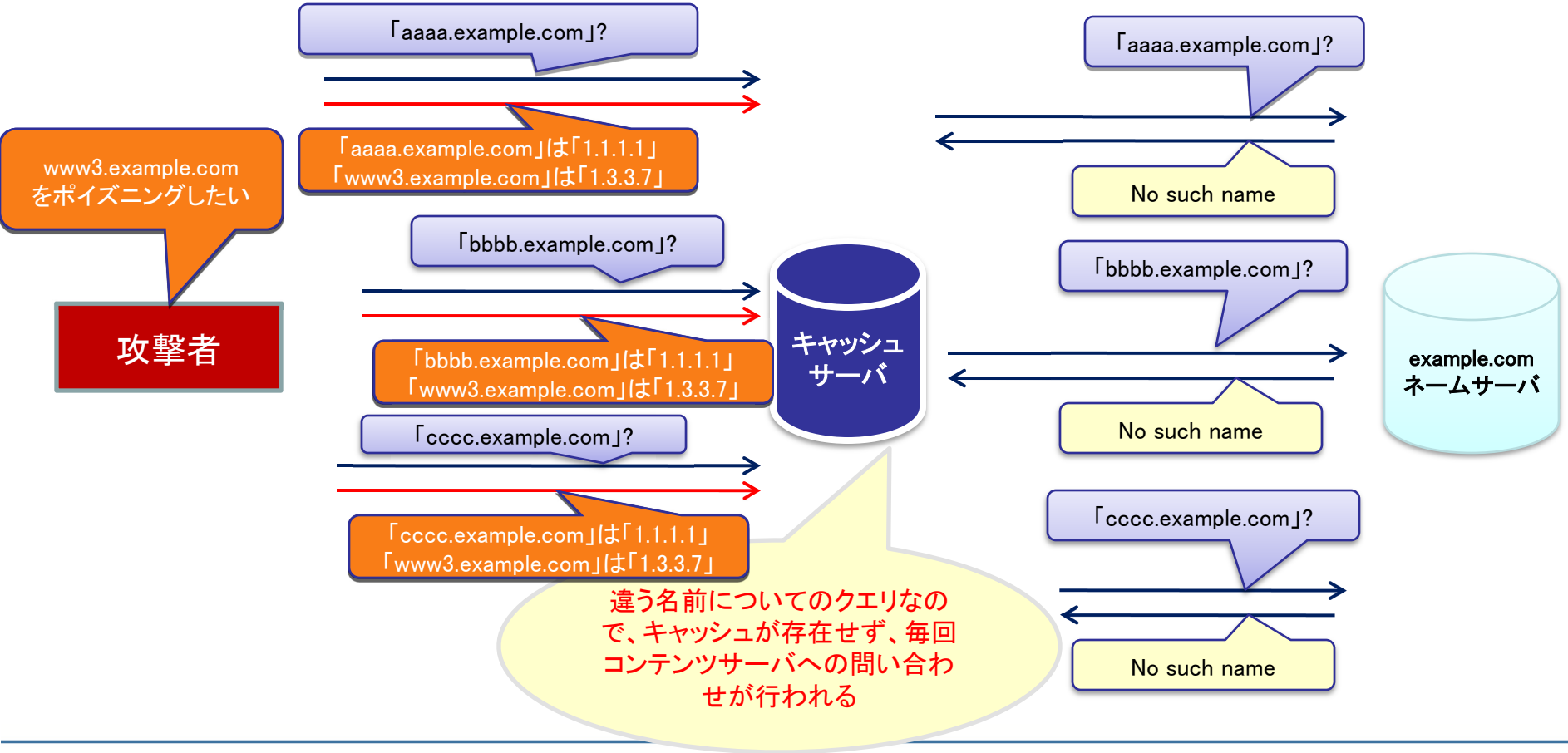
Copyright® 2008 JPCERT/CC All rights reserved.

キャッシュポイズニング攻撃
～2008年7月に明らかになった攻撃手法～

Copyright® 2008 JPCERT/CC All rights reserved.

2008年7月に明らかになった攻撃手法

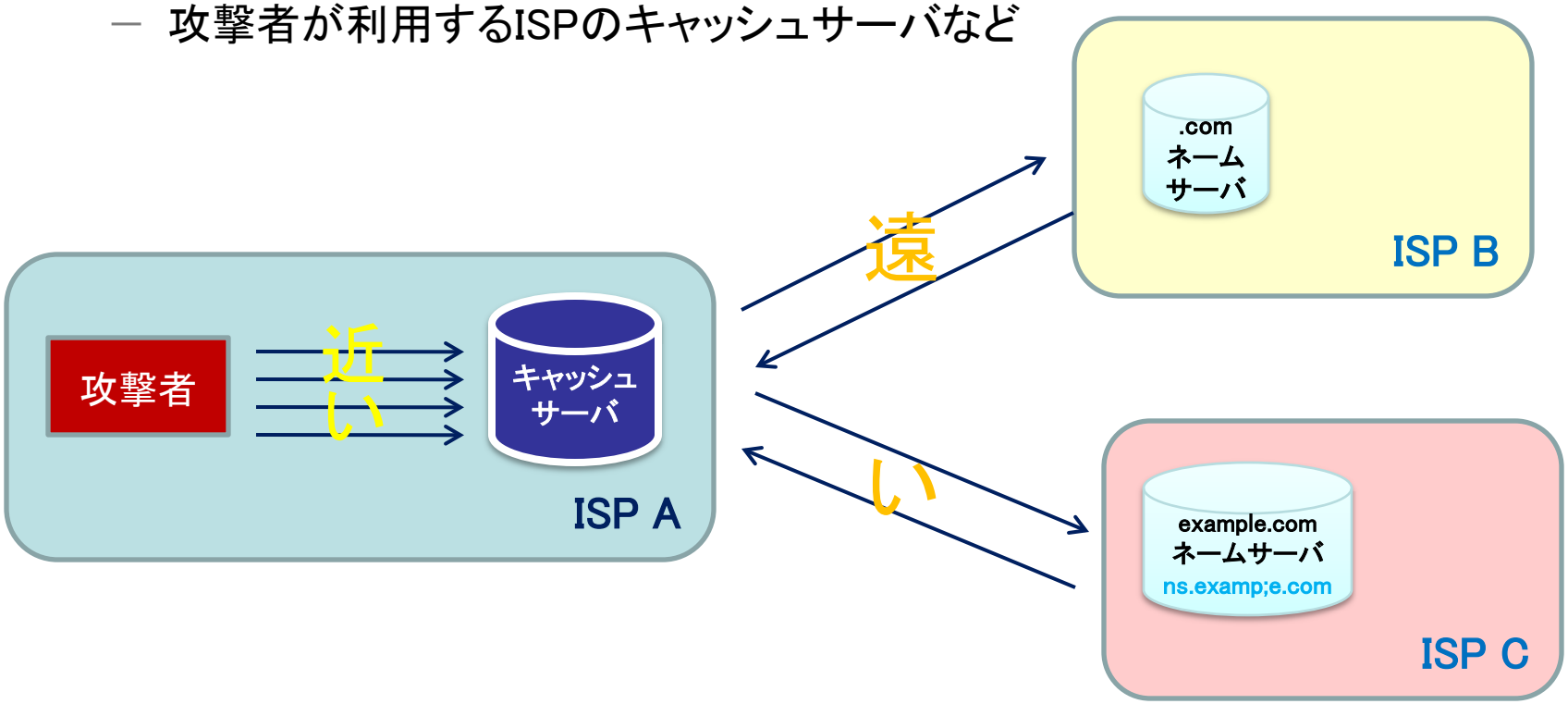
- 今回発表された手法：「[ランダムな文字列].[ドメイン名]」という毎回違う名前のクエリを送信し、「Additional Record」にポイズニングしたいホスト名の情報を入れる



Copyright® 2008 JPCERT/CC All rights reserved.

攻撃の成功率が上がる要因 その1

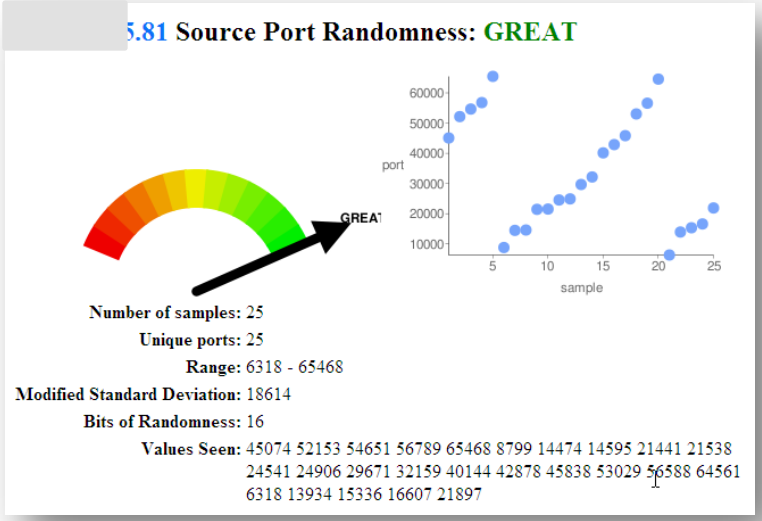
- 正規のネームサーバの返答よりも攻撃者が送信する偽の返答が早くキャッシュサーバに到達する場合
  - 攻撃者が利用するISPのキャッシュサーバなど



Copyright® 2008 JPCERT/CC All rights reserved.

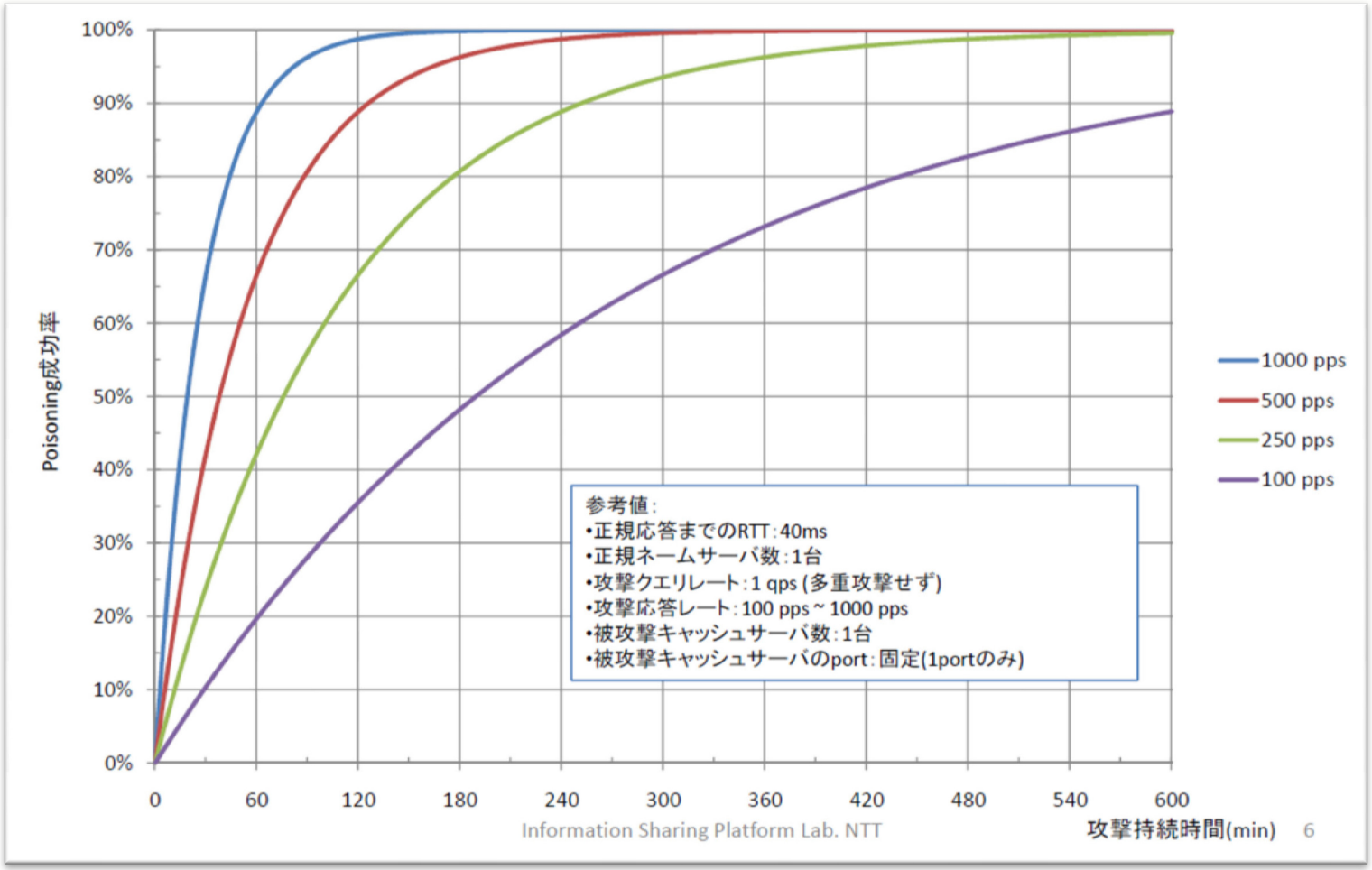
攻撃の成功率が上がる要因 その2

- 他の問題と組み合わせる
  - 乱数生成ロジックの脆弱性を利用すれば、トランザクションIDやソースポート番号の推測が容易になる
  - Debianの古いbind9パッケージでは、ソースポートが53番に固定されている
    - http://www.debian.or.jp/blog/dns_cache_poisoning.html



Copyright® 2008 JPCERT/CC All rights reserved.

攻撃の成功率(理論値)



出典: “DNS Cache Poisoningの概要と対処” NTT情報流通プラットフォーム研究所 豊野剛

正規応答が40msという環境で1000ppsの攻撃を行えば60分以内に攻撃成功する確率は約90%と推定される

Copyright® 2008 JPCERT/CC All rights reserved.

今回の問題の重大性

想像以上に攻撃を成立させるのは容易

- 理論上は1時間の攻撃で90%の成功率

攻撃成立を検知することが困難

- キャッシュサーバ上のキャッシュの正当性を保障する仕組みが無い

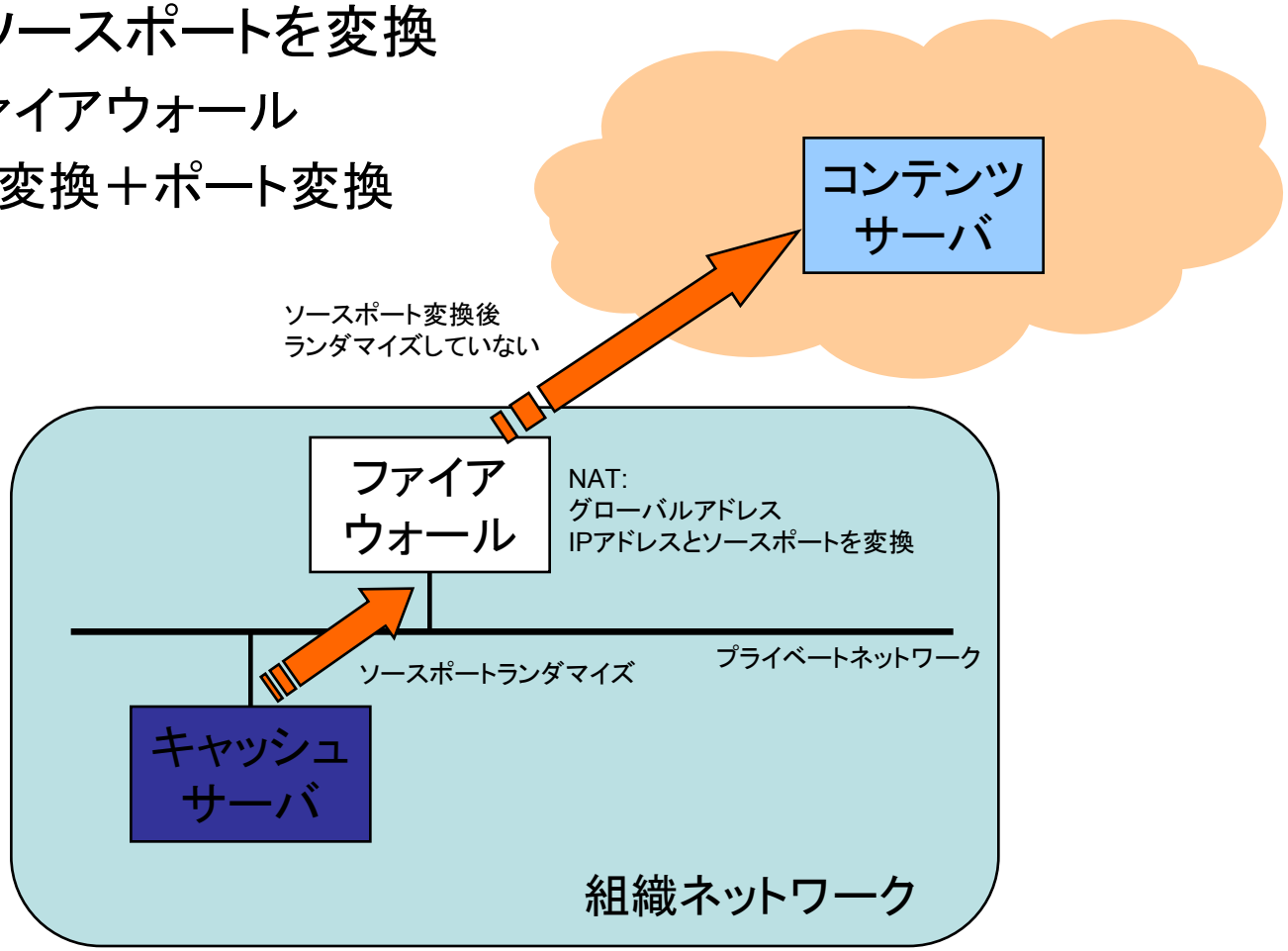
効率的な攻撃が可能

- 一台のキャッシュサーバへの攻撃で数万台のクライアントに影響
- さまざまなシナリオ
  - フィッシング
  - メール詐取
  - 標的型攻撃
  - etc.

Copyright® 2008 JPCERT/CC All rights reserved.

補足：NATの問題

- 組織内ネットワークのキャッシュサーバで問題
- NAT装置がソースポートを変換
  - 組織のファイアウォール
  - IPアドレス変換＋ポート変換



Copyright® 2008 JPCERT/CC All rights reserved.

対策

Copyright® 2008 JPCERT/CC All rights reserved.

対策1：本攻撃への対策（サーバ管理者向け）

JPCERT CC®

- パッチの適用
  - ソースポートランダマイゼーション
    - CERT VU#800113 DNS Cache Poisoning Issue
    - http://www.isc.org/sw/bind/forgery-resilience.php
    - マイクロソフト セキュリティ情報 MS08-037 - 重要：DNS の脆弱性により、なりすましが行われる（953230）
    - http://www.microsoft.com/japan/technet/security/bulletin/ms08-037.mspx
  - パッチが存在しない場合はバージョアップ（e.g. BIND 8）

Copyright® 2008 JPCERT/CC All rights reserved.

対策2：安全なDNSサーバ運用のために

JPCERT CC®

- 再帰問い合わせの制限
  - 組織内からの問い合わせのみに返答するように制限
  - コンテンツサーバは再帰問い合わせに返答する必要はない
- DNSサーバの動作の統計情報を確認
  - 短時間に大量のクエリー送信など攻撃に繋がる試みを検知する仕組み
- キャッシュサーバがNATの下にある場合はNAT装置の対策

Copyright® 2008 JPCERT/CC All rights reserved.

付録: 参考情報

- JPCERT/CC 注意喚起 JPCERT-AT-2008-0014
  [続報] 複数の DNS サーバ製品におけるキャッシュポイズニングの 脆弱性に関する注意喚起
  http://www.jpcert.or.jp/at/2008/at080014.txt

- Japan Vulnerability Notes JVNVU#800113
  複数の DNS 実装にキャッシュポイズニングの脆弱性
  http://jvn.jp/cert/JVNVU800113/index.html

- JVNTA08-190B
  複数の DNS 実装にキャッシュポイズニングの脆弱性
  http://jvn.jp/cert/JVNTA08-190B/index.html

- 独立行政法人 情報処理推進機構 セキュリティ センター
  DNSキャッシュポイズニングの脆弱性に関する注意喚起
  http://www.ipa.go.jp/security/vuln/documents/2008/200809_DNS.html

- 独立行政法人 情報処理推進機構 セキュリティ センター
  複数の DNS 製品の脆弱性について
  http://www.ipa.go.jp/security/ciadr/vul/20080724-dns.html

- JPRS DNS 関連技術情報
  複数のDNSソフトウェアにおけるキャッシュポイズニングの脆弱性について
  http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning.html

- JPRS DNS 関連技術情報
  (緊急)複数のDNSソフトウェアにおけるキャッシュポイズニングの脆弱性について(続報)
  http://jprs.jp/tech/security/multiple-dns-vuln-cache-poisoning-update.html

- JPRSドメイン名やDNSの解説コラム
  新たなるDNSキャッシュポイズニングの脅威～カミンスキー・アタックの出現～
  http://jpinfo.jp/topics-column/009.pdf

- US-CERT Vulnerability Note VU#800113
  Multiple DNS implementations vulnerable to cache poisoning
  http://www.kb.cert.org/vuls/id/800113

- NTT 情報流通基盤総合研究所 情報流通プラットフォーム研究所 IPネットワーク技術コアチーム
  DNS Cache Poisoningの概要と対処 (Dan KaminskyによるDNS脆弱性指摘に関して)
  http://www.nttv6.net/files/DKA-20080723.pdf

Copyright® 2008 JPCERT/CC All rights reserved.

JPCERT CC®

JPCERTコーディネーションセンター

- Email：office@jpcert.or.jp
- Tel：03-3518-4600
- http://www.jpcert.or.jp/

インシデント対応依頼/情報提供 窓口

- Email：info@jpcert.or.jp

  PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73　57 EE 3C 2B 13 F0 48 B8
- 報告様式

  http://www.jpcert.or.jp/form/