ISPにおけるDoS/DDoS攻撃の検知・対策技術

InternetWeek 2013 S2:DDoS攻撃の実態と対策
2013/11/26 (火) 13:00-15:30

NTTコミュニケーションズ株式会社 高田美紀

自己紹介

- 1993～ 株式会社NTTPCコミュニケーションズ
  - ISP (InfoSphere) サーバの運用
  - ホスティング (WebARENA) 立ち上げ～開発～運用
  - 主にDNS、メールシステム担当
- 2013/4～ NTTコミュニケーションズ株式会社
  - 先端IPアーキテクチャセンタ
    - ✓ R&D部門
    - ✓ DDoS対策技術、DNSまわりでの事業部サポート、対外活動
- 対外活動
  - dnsops.jp 幹事
  - ときどき JANOG meeting スタッフ、などなど
- エンジニア＋母親業の両輪で活動中

Agenda

- DNS amp 攻撃の仕組み
- 対策
- 世の中の動き
- ツール紹介
- まとめ
- 参考資料

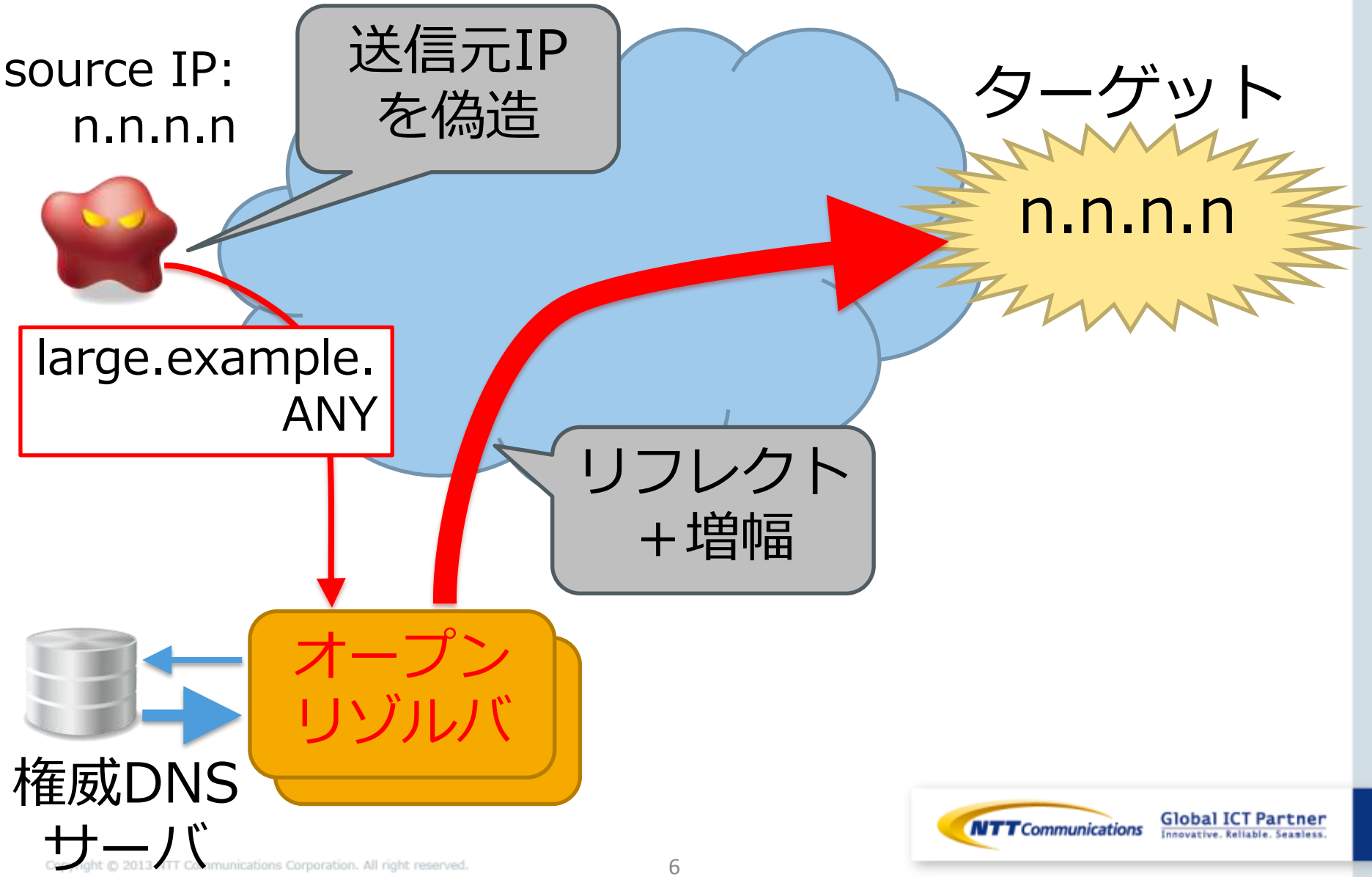
DNS amp 攻撃の仕組み

DNS amp 攻撃とは

- 送信もとを偽装したDNS問い合わせによる攻撃
  - ターゲットのアクセス回線帯域を溢れさせる目的
  - 送信もとを偽装
  - 多くは反射板 (リフレクター: オープンリゾルバ) を利用
  - リフレクターでパケットサイズを増幅
    - ✓ 応答 / 問い合わせ 倍率は数十倍

- DNSを用いたDDoS攻撃手法の一つ
  - 古くからある: JANOG18/2006 でも話題に
    - ✓ DNS amplification attacks 松崎 吉伸（株式会社インターネットイニシアティブ）
    - ✓ http://www.janog.gr.jp/meeting/janog18/program-abstract.html#P8
  - 当時との違い
    - ✓ DNSSEC等の普及で応答パケットの大きいドメインが増えた

DNS amp: 基本的な仕組み



ところで。。用語の混乱

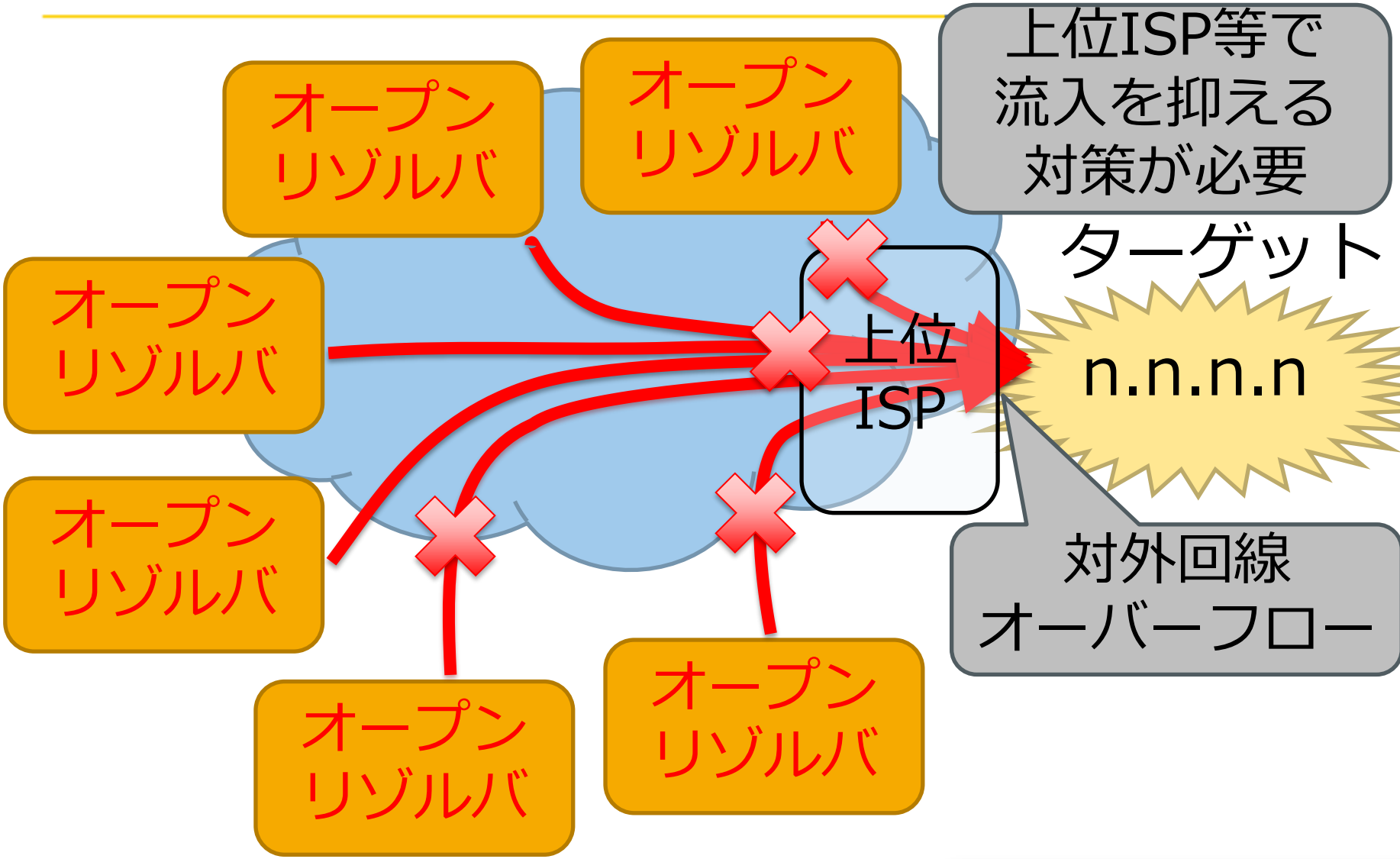
- 正式(?)な用語
  - RFC 5358/BCP 140によると Reflector Attacks
    - ✓ http://tools.ietf.org/html/rfc5358
  - 技術解説：「DNS Reflector Attacks（DNSリフレクター攻撃）」について
    - ✓ http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html
- 検索結果では DNS amp が圧倒的
  - 今回は DNS amp を使います
    - ✓ 厳密な用語の定義が目的ではないので

(2013/11/4 時点)

word ¥ engine	google	bing	goo
DNS reflection attack	388,000	58,100	14,200
DNS reflector attack	102,000	54,400	4,310
DNS amplification attack	158,000	61,100	9,660
DNS amp attack	316,000	68,300	13,800
DNS amp	2,080,000	776,000	142,000

対策

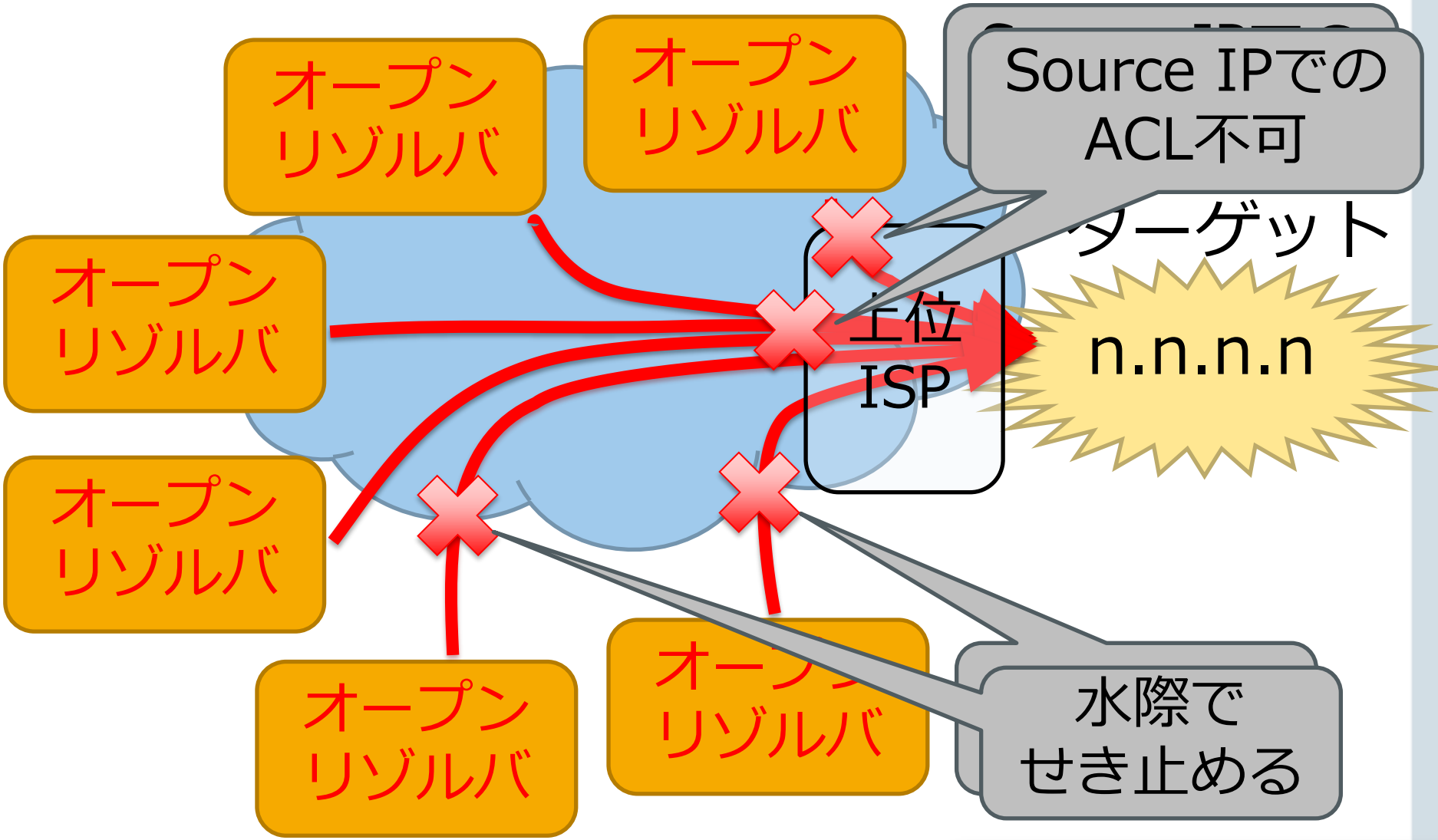
DDoS対策の難しさ



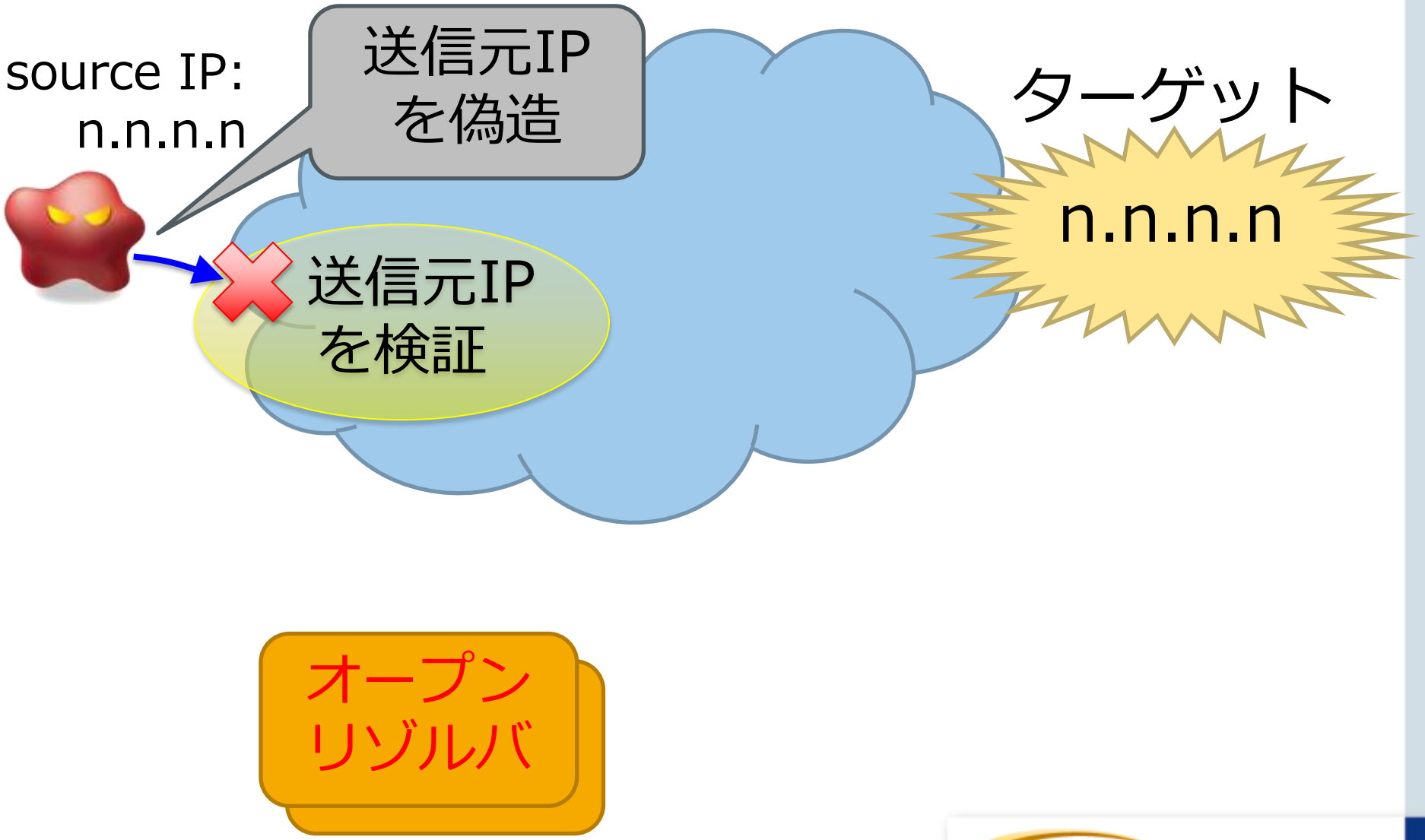
二面性

- 対策には二面
  - DDoSの被害を受けない (軽減する) ため
    - ✓ ターゲットとなってしまった場合
    - ✓ 自ネットワークでの対策には限界がある
  - DDoSの攻撃者とならないため
    - ✓ そうと知らずに誰かを攻撃するための道具に使われているかも
      - ✓ 自設備を守るため
      - ✓ お客さまを守るため
      - ✓ ターゲットからの訴訟リスクもあるかも。。?
    - ✓ 自らのネットワーク帯域を使い切ってしまう事例も
      - ✓ お客さまからISPへクレームが上がり気づく例
- 対策の必要性
  - 理由もなく「うちは大丈夫!」と思ってませんか?
  - 普段からネットワークの健康状態を確認できてますか?
  - 西塚さんにバトンタッチ

「上流で止める」難しさ



基本的な対策: Source Address Validation



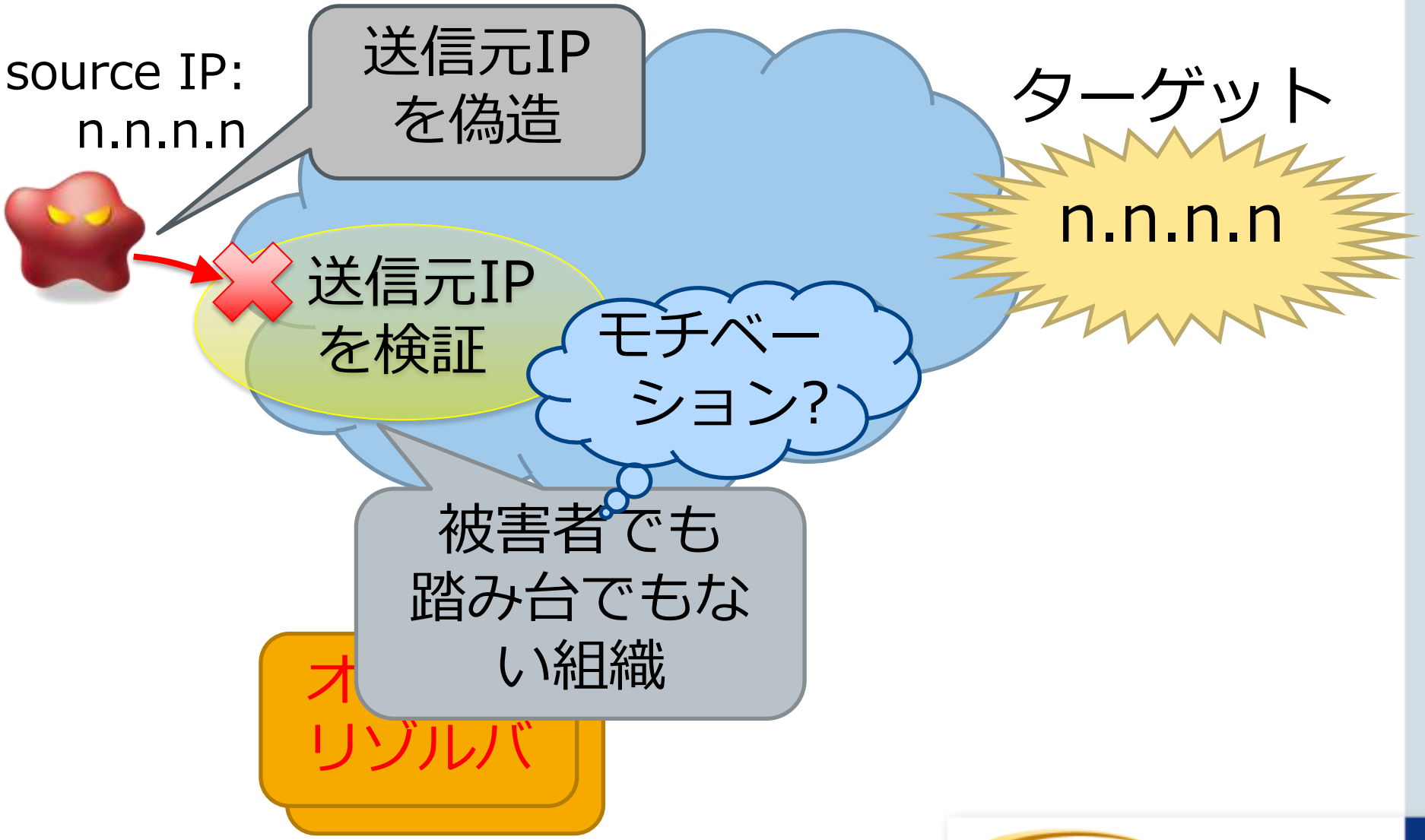
Source Address Validation

- 送信元アドレスを偽装したパケットの流入を拒否する対策
  - 攻撃のトリガーとなるパケットをブロック

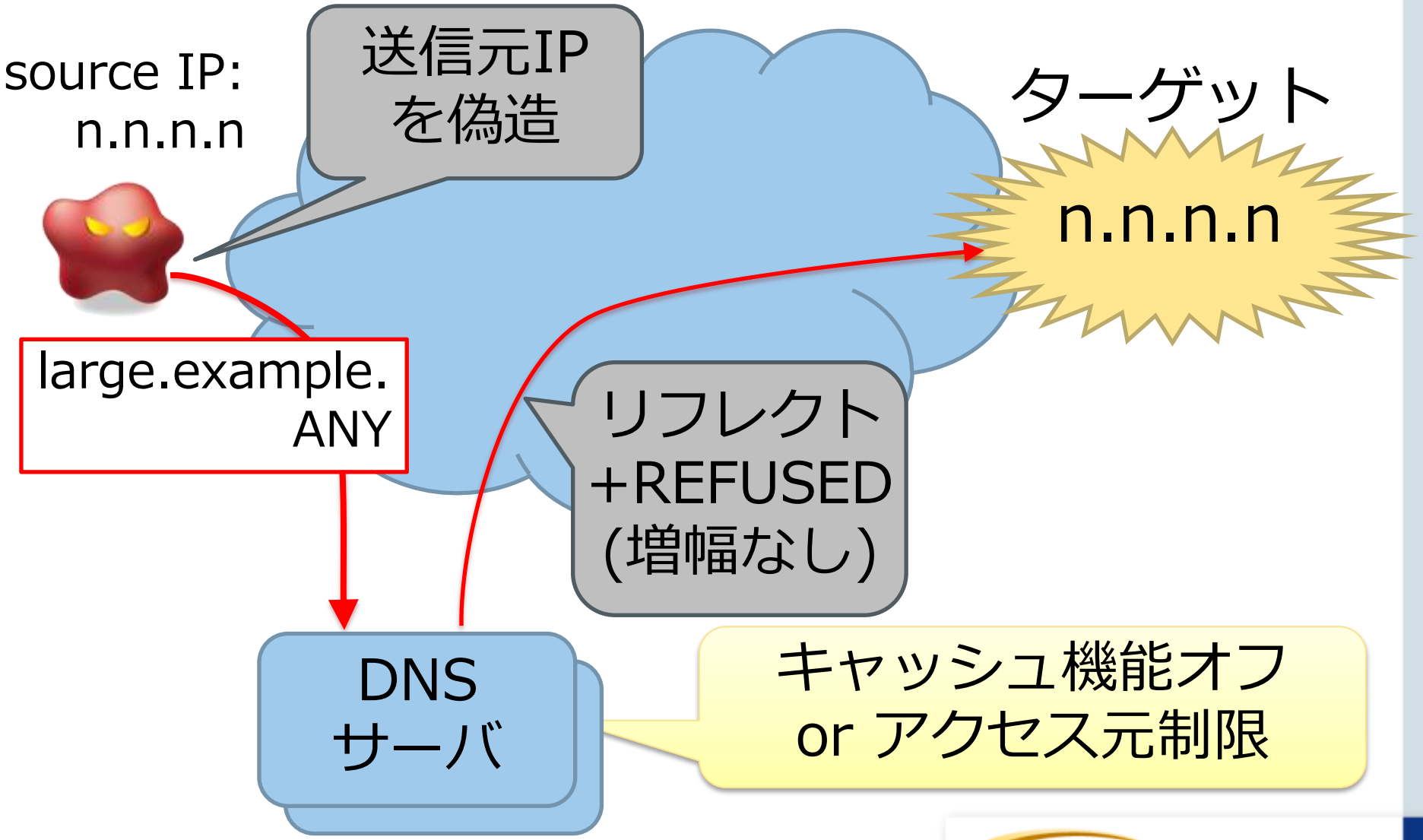
- ISP
  - 国内では導入している事業者は少ない模様
  - 非対称ルーティング、マルチホーム顧客への対応の難しさ
- ホスティング/クラウド
  - サービス内でのなりすまし防止のため必要
  - 顧客サーバが送信するパケットのソースIPアドレスは一定
    - ✓ 導入障壁は (ISPに比べ) 低い
    - ✓ AWS的なやりかたの事業者だと技術的にspoofパケットを出せない

- RFC 2827 BCP 38 / RFC 3074 BCP 84

基本的な対策: Source Address Validation



基本的な対策: キャッシュ機能オフ or アクセス元制限



基本的な対策: キャッシュ機能オフ or アクセス元制限

- オープンリゾルバでなくする対策

- キャッシュ機能をオフ
  - 再帰検索機能が必要なければオフ
  - DNS機能の必要がない場合は、それ自体オフにする
- アクセス元制限
  - 機能は必要な場合
  - サービスする対象をはっきりさせ、そこ限定でサービス

- リフレクトはするが、パケットサイズの増幅は起こらない

世の中の動き
Good News & Bad News

各社の取り組み

- 歴史的経緯のオープンリゾルバを停止する取り組み
  - さくらインターネット株式会社
    - ✓ 2013/8/5 DNSキャッシュサーバ仕様変更のお知らせ
      - ✓ http://www.sakura.ad.jp/news/sakurainfo/newsentry.php?id=776
  - 株式会社インターネットイニシアティブ
    - ✓ 2013/8/12 DNSサーバ仕様変更のお知らせ
      - ✓ https://www.iij4u.or.jp/info/iij/20130812-1.html
    - ✓ 「昔IIJを使っていた人」にお願いです – オープンリゾルバ対策
      - ✓ http://techlog.iij.ad.jp/archives/718
  - NTTコミュニケーションズ株式会社
    - ✓ 2013/9/30 DNSサーバーのセキュリティ制限実施のお知らせ
      - ✓ http://www.ocn.ne.jp/business/info/130930.html
  - 株式会社IDCフロンティア
    - ✓ 2013/10/18 【重要】DNSサーバ仕様変更のお知らせ
      - ✓ http://portal.idc.jp/news/20131018_01_SC20131018_0205.html

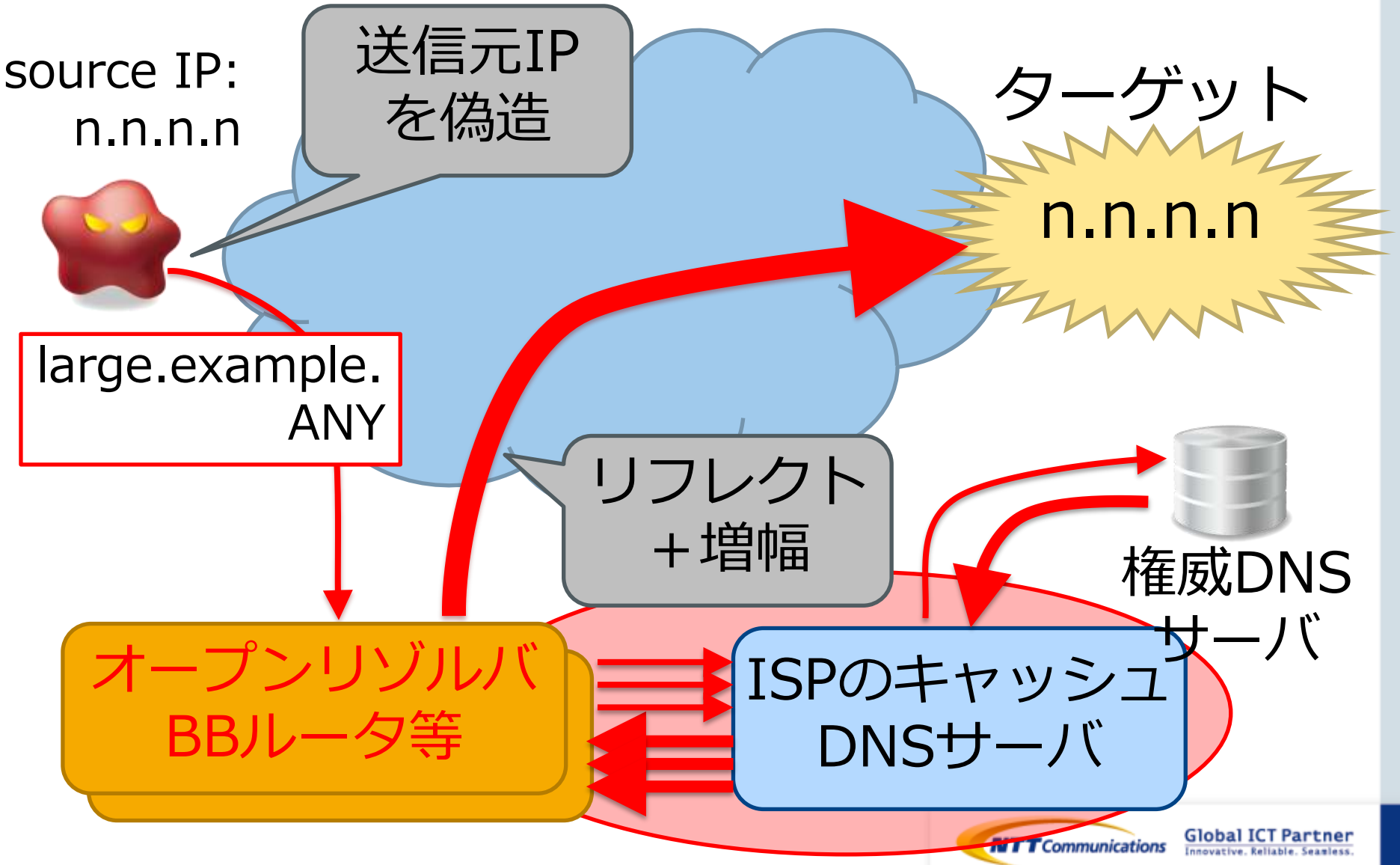
CPE問題の認知

- CPE 脆弱性
  - 2013/9/19 JVN#62507275
    - ✓ 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
      - ✓ http://jvn.jp/jp/JVN62507275/index.html
  - 2013/9/19 JVNDB-2013-000087
    - ✓ 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
      - ✓ http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-000087.html

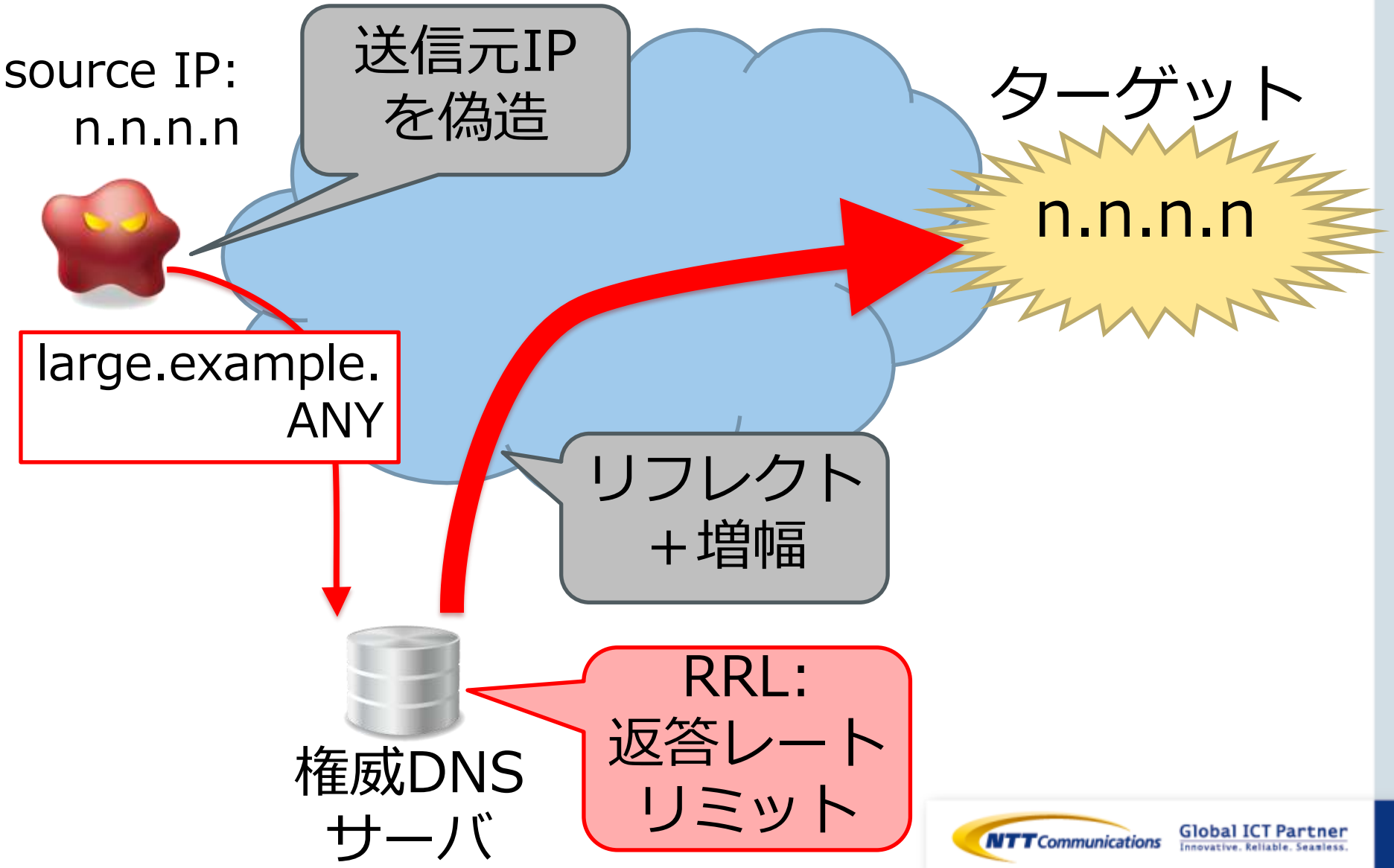
テレコム・アイザック推進会議

- 2013/6/17 ネットワークデバイスの脆弱性保有状況調査について
  - https://www.telecom-isac.jp/news/news20130617.html
- 調査内容、時期
  - 協力ISPのIPアドレス帯に対し、デバイスの状態を調査
    - ✓ 簡易なコマンド
  - 6月中旬～
- 調査結果
  - 統計データとして関係者内で今後の対策検討に活用

ISPのキャッシュサーバ負荷増大



権威DNSをリフレクターとした攻撃



攻撃者の視点

- オープンリゾルバ、Source Address Validation をしてない ISP/ホスティング等はインターネット上に多数存在している
  - オープンリゾルバのリストを作ることも難しくない

- 利点がいっぱい
  - 足がつきにくい
    - ✓ 到着したパケットから「攻撃しているのは誰なのか?」わからない
  - 手法は新しいものでなく、枯れていて確実
  - 攻撃コードは簡単
  - カジュアルに (やろうと思ってすぐに) 攻撃できる
  - コントローラブル
    - ✓ 任意の容量、任意の時刻、継続時間も任意に
  - (被害者側で) 防御しづらい
    - ✓ DDoS一般の特徴

DDoSビジネス

- 任意の宛先に対してDDoS攻撃を請け負う業者の存在
  - Cybercrime… for sale (I)
    - ✓ http://pandalabs.pandasecurity.com/cybercrime-for-sale-i/
      - ✓ 2007/4の記事
    - ✓ DDoS攻撃サービスの値段を紹介
      - ✓ 1時間: US$10-20 (販売者による)
      - ✓ 2時間: US$20-40
      - ✓ 1日: US$100
      - ✓ 1日増す毎に: US$200 (複雑さによる)
      - ✓ 10分間は無料。評価のため
    - ✓ その他、SPAM送信、FTPアカウント、オンラインショップアカウント等も商品として扱われている

DDoS対策と通信の秘密

- JAIPAほか4団体
  - 2011/3/25 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン
    - ✓ http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf
- JAIPA 行政法律部会長 木村さん資料より抜粋
  - 2012/9/12 インターネット上の情報セキュリティ関連ガイドラインの紹介
    - ✓ http://www.soumu.go.jp/main_content/000176006.pdf
      - ✓ 本ガイドラインは、大量通信等のネットワークに対する攻撃に対して、通信の秘密の保護に最大限配慮しながら電気通信サービスの円滑な提供の確保に資することを目的としています。
      - ✓ 電気通信事業者が大量通信等を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料として、本ガイドラインを策定しました。
- よくある事例に基づいて紹介されていてわかりやすい

ツール紹介

ツール

- 自身がオープンリゾルバとなってないかチェックするツール
  - http://www.openresolver.jp/
  - JPCERT/CC が 2013/10/31 開設
- 使い方:
  - ブラウザでアクセスし、ボタンを押すだけ
  - wget等コマンドラインでも確認できる
    - ✓ ホスティングサーバなどGUIのない場所でも
- チェック内容:
  - 使っているキャッシュDNSサーバの検査
  - 接続元IPアドレス(BBルータなど)の検査
- チェックして、ぜひ報告してください!!
  - 思ったより簡単に報告できます

まとめ

- DDoSは被害者側の対策だけでは防御/回避できない

- 協調
- 攻撃プラットホームの撲滅

- 被害者にも加害者にもなりうるリスク
- 自身の状態監視と適切な対策

Q & A

- ご清聴ありがとうございました。

参考資料

参考資料

- 最新の技術動向: 送信元検証「Source Address Validation」
  - http://www.iij.ad.jp/company/development/tech/activities/sav/
- 送信もとIPアドレス検証(Source Address Validation)実施について
  - http://dream.jp/support/techinfo/security/sav.html
- NSP-Security-JP update @JANOG17
  - http://www.janog.gr.jp/meeting/janog17/documents/13-1_nsp-sec-jp.pdf