NXNSAttackの概要

株式会社日本レジストリサービス

あはれん　よしたか

阿波連　良尚

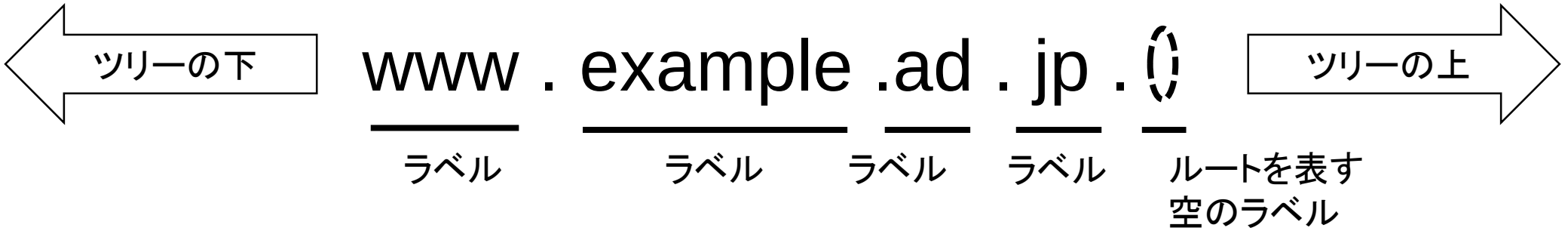
本セッションの内容

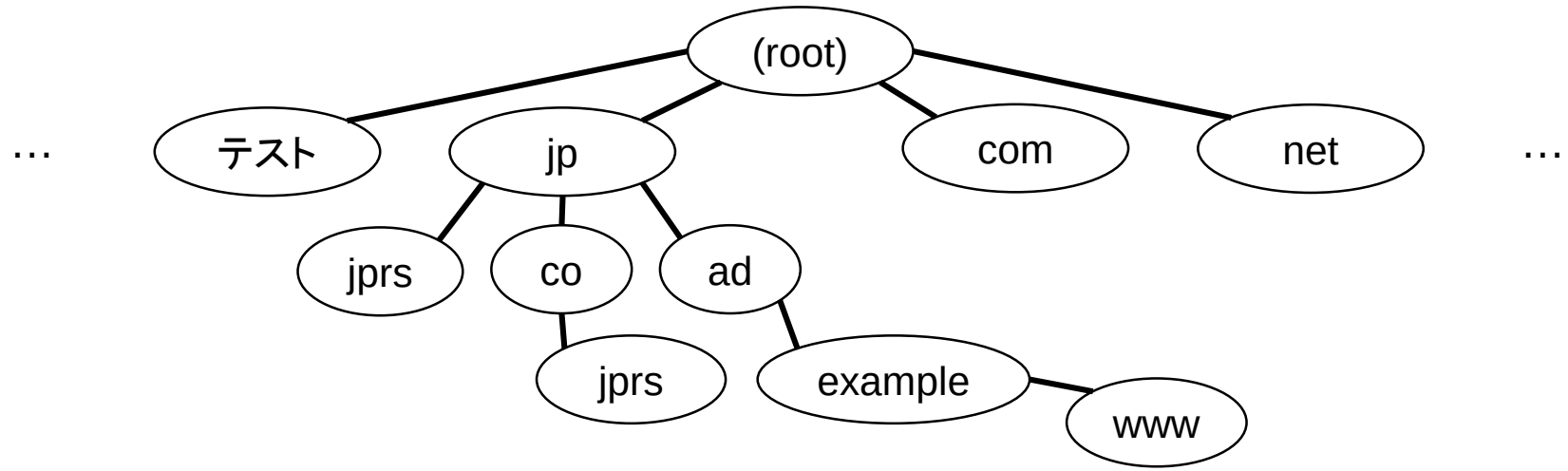
- 前提知識（ドメイン名空間と委任、referral応答）
- 水責め攻撃の概要
- NXNSAttackの概要
- 修正前の挙動（BIND 9・Unbound）
- 論文で提案された対策
- 修正後の挙動

参考にした論文:
Afek, Y., Bremler-Barr, A., & Shafir, L.
NXNSAttack:Recursive DNS Inefficiencies and Vulnerabilities.
http://www.nxnsattack.com/

ドメイン名空間と委任（1）

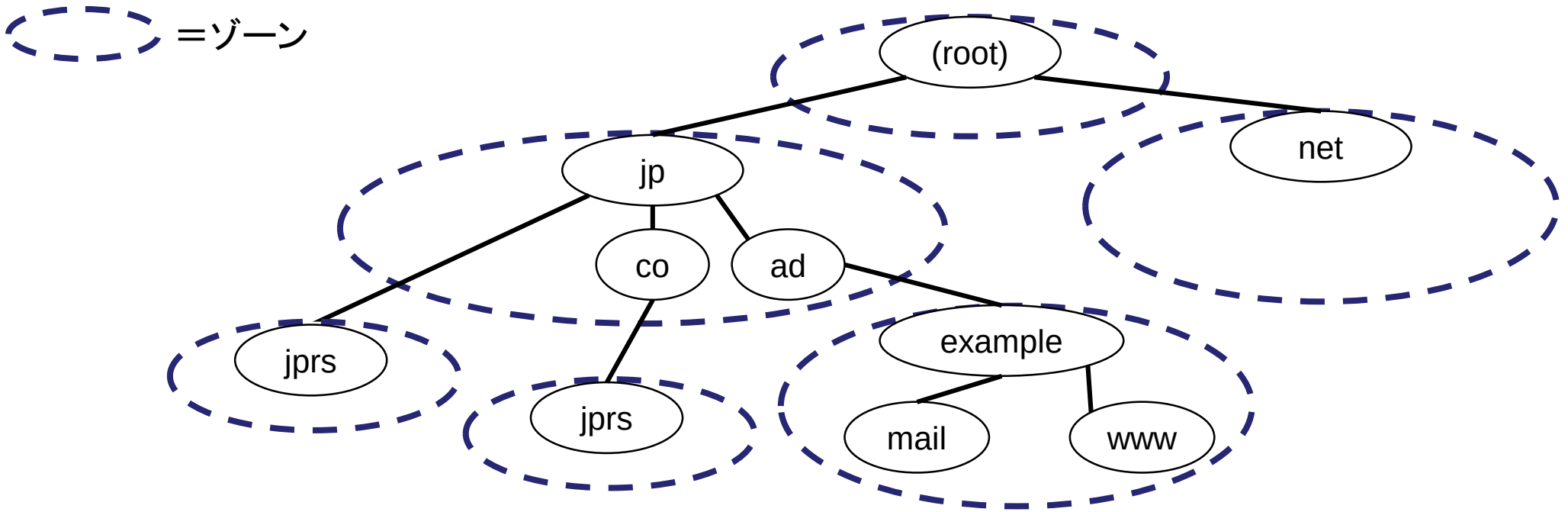
- ドメイン名はツリー構造
  - インターネット内で1つのドメイン名空間を構成する
    （インターネットの中でjprs.co.jpは一意）





ドメイン名空間と委任（2）

- サブツリーを別のゾーンとして切り出せる（委任）
  - ただし、「.」の区切りで必ず委任されているとは限らない
    - ➢例: jp → jprs.co.jp　　（co.jpゾーンは存在しない）
      fr → impots.gouv.fr　（gouv.frゾーンは存在しない）



referral応答（1）

- 権威DNSサーバーから、委任に関する情報を伝える
  - ゾーンの階層構造をたどる（反復検索）過程で現れる

問い合わせ:

フルリゾルバー（www.example.ad.jpを解決中）→ a.dns.jp

```
Header Flags:
Question:
  www.example.ad.jp.          IN   AAAA
```

応答:

a.dns.jp → フルリゾルバー（www.example.ad.jpを解決中）

```
Header Flags: qr
Question section:
  www.example.ad.jp.          IN   AAAA
Answer section: （空）
Authority section:
  example.ad.jp.       3600   IN   NS   ns1.dns-provider.example.
  example.ad.jp.       3600   IN   NS   ns2.dns-provider.example.
```

Authority sectionに
委任先の権威DNSサーバーの
ドメイン名が含まれる

referral応答（2）

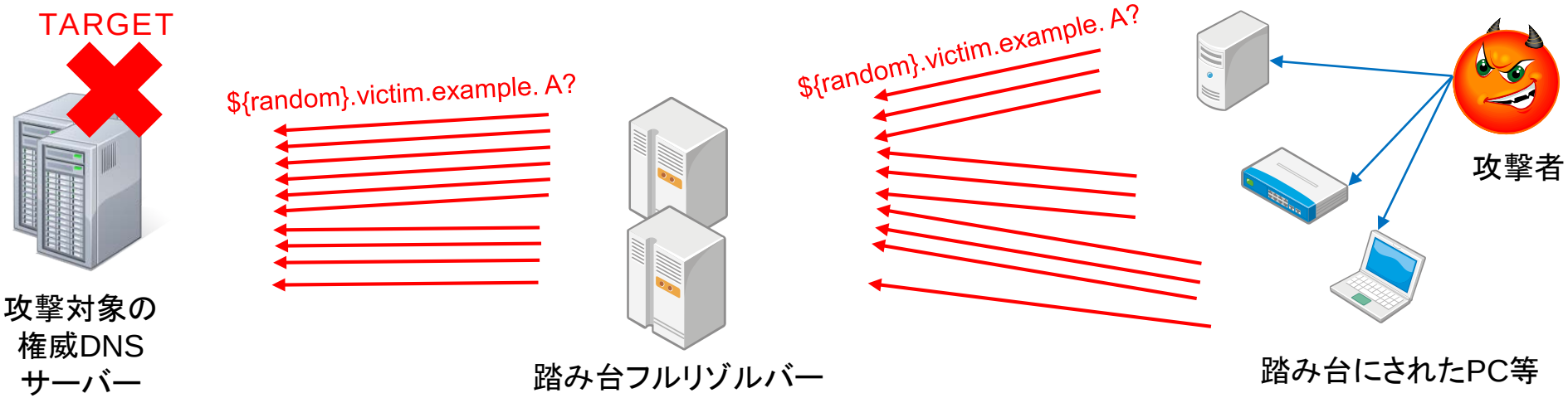
a.dns.jp → フルリゾルバー（www.example.ad.jpを解決中）

```
Header Flags: qr                                【委任先が内部名ではない例】
Question section:
  www.example.ad.jp.          IN   AAAA
Answer section: （空）
Authority section:
  example.ad.jp.        3600  IN   NS   ns1.dns-provider.example.
  example.ad.jp.        3600  IN   NS   ns2.dns-provider.example.
```

- 応答に含まれるNSレコードは権威DNSサーバーのドメイン名を指す
  - 内部名であればAdditional sectionにIPアドレス情報が含まれるので、それを使って委任先の権威DNSサーバーに問い合わせる
  - 内部名ではない場合、**権威DNSサーバーのドメイン名を改めて名前解決**してIPアドレスを得る必要がある

水責め攻撃の概要

- フルリゾルバーに、攻撃対象ドメイン名の権威DNSサーバーへ大量クエリを送るよう仕向ける
  - ランダムなラベルを攻撃対象ドメイン名の左側に付けたクエリを送ることで、キャッシュにヒットしない（必ず権威DNSサーバーに問い合わせる）ようにする
  - 対象ドメイン名の権威DNSサーバーのネットワークや処理能力が飽和する
  - フルリゾルバーもネットワークやシステムリソースを消費する



NXNSAttackの概要（1）

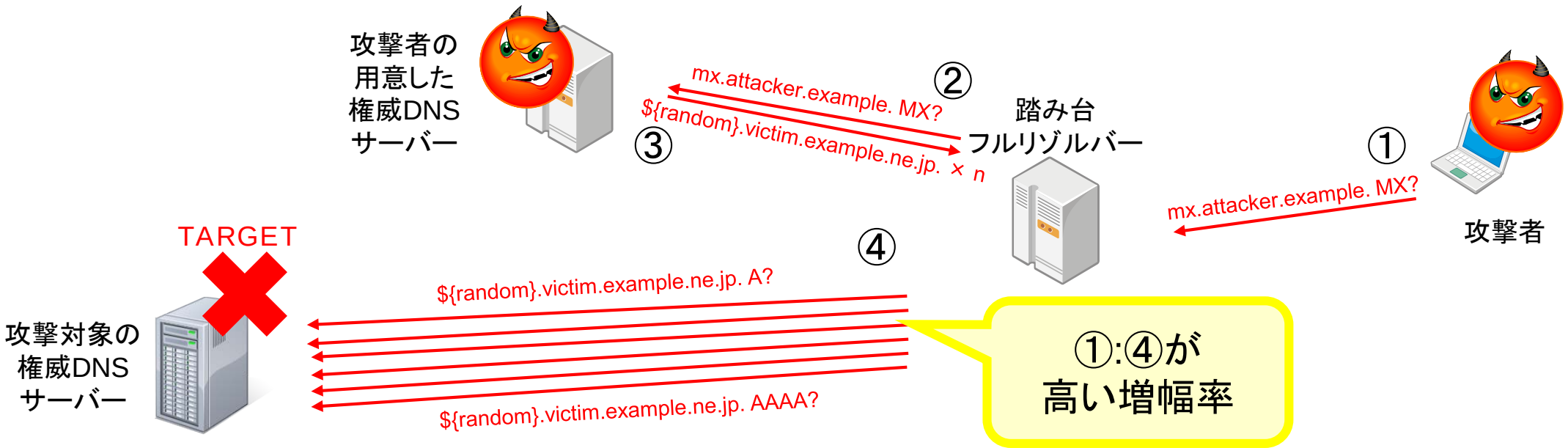
- 前準備として、攻撃用のドメイン名を用意する
  - ドメイン名を登録し、権威DNSサーバーを設定して名前解決できる状態にする
  - ゾーンの頂点以外のドメイン名として、攻撃対象ドメイン名に委任する NSレコード（攻撃用ドメイン名から見て内部名ではない）を多数（37個）作る

```
$TTL 86400
$ORIGIN attacker.example.
@       IN  SOA    ns1 johndoe 1592990141 3600 900 604800 900
        IN  NS     ns1
ns1     IN  A      192.0.2.53
        IN  AAAA   2001:db8:feed::53
mx      IN  NS     9o7z.victim.example.ne.jp.
        IN  NS     kyzf.victim.example.ne.jp.
        IN  NS     kcn7.victim.example.ne.jp.
        IN  NS     lvlq.victim.example.ne.jp.
        […]
```

存在しない名前にするため
左にラベルを付けた
攻撃対象ドメイン名を
委任先として多数指定

NXNSAttackの概要(2)

- 前スライドで用意したドメイン名を、踏み台に名前解決させる
  - 途中の委任先が外部名の権威DNSサーバーなので、フルリゾルバーの内部処理として別途名前解決が必要になる
  - 委任先として指定されている権威DNSサーバーのドメイン名に対して、踏み台となるフルリゾルバーから大量に問い合わせが送られる(次スライドで説明)



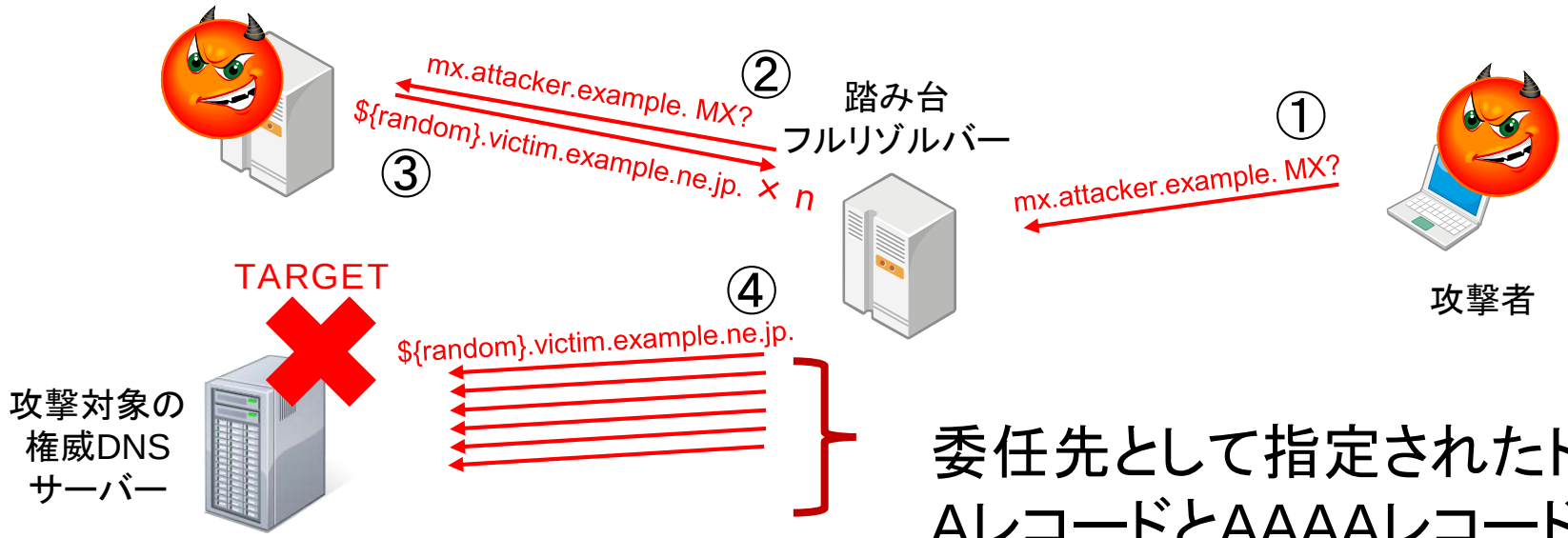
NXNSAttackの概要(3)

```
Header Flags: qr
Question section:
  mx.attacker.example.          IN  MX
Answer section: (空)
Authority section:
  mx.attacker.example.  3600    IN  NS  9o7z.victim.example.ne.jp.
  mx.attacker.example.  3600    IN  NS  kyzf.victim.example.ne.jp.
  mx.attacker.example.  3600    IN  NS  02vu.victim.example.ne.jp.
  mx.attacker.example.  3600    IN  NS  wrpl.victim.example.ne.jp.
  […]
```

これらのドメイン名について、
Aレコード・AAAAレコードを
並列に問い合わせしてしまう

- 多くの実装で、委任先である権威DNSサーバーの名前解決を並列に、かつ回数の上限が緩い設定で行っていた
  - 結果、フルリゾルバーが高倍率の増幅器として作用してしまった
- 応答パケットに詰められるだけ`${prefix}.victim.example.ne.jp`を詰めると、74倍～1602倍程度の増幅率を得られる

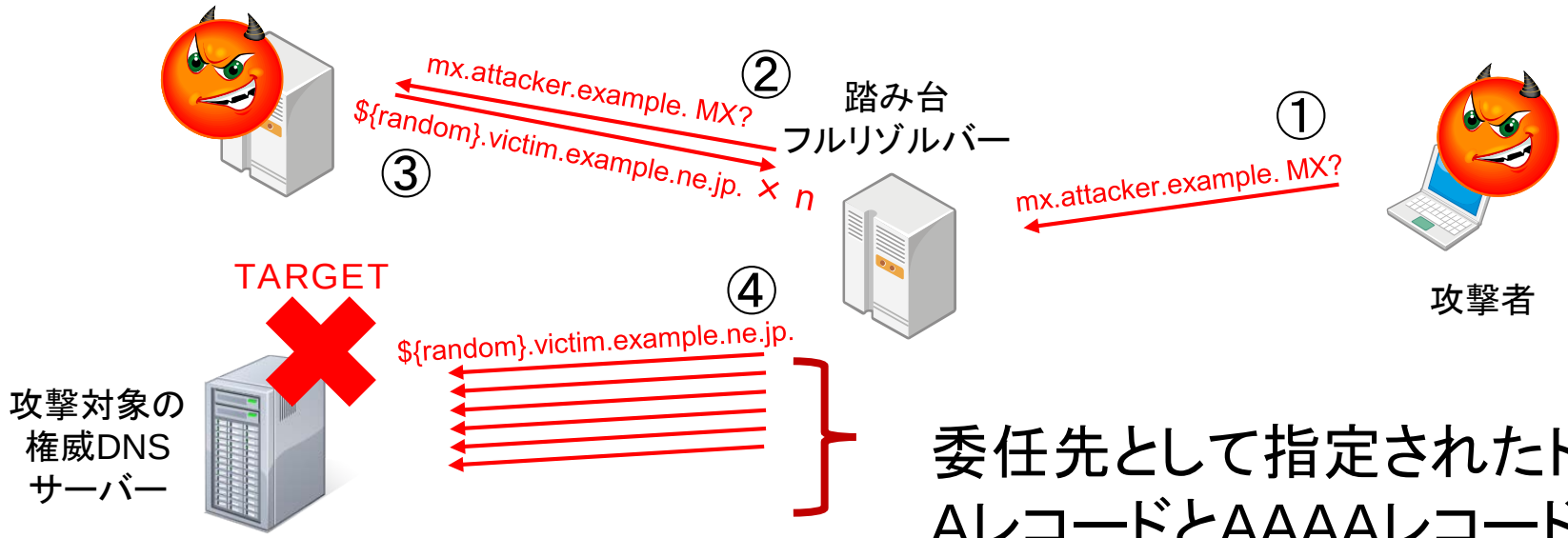
修正前の挙動: BIND 9



委任先として指定されたドメイン名の
AレコードとAAAAレコードを問い合わせ

- 委任先ドメイン名のIPアドレスを、応答を待たずに並列で問い合わせる
  - Aレコード・AAAAレコード両方を問い合わせるので2倍
  - 攻撃対象の権威DNSサーバーがIPv6通信可能な場合、さらに2倍
  - ただし、①から派生した追加の②・④等の問い合わせ総数の上限として、`max-recursion-queries` オプション（デフォルト: 75）で制限される

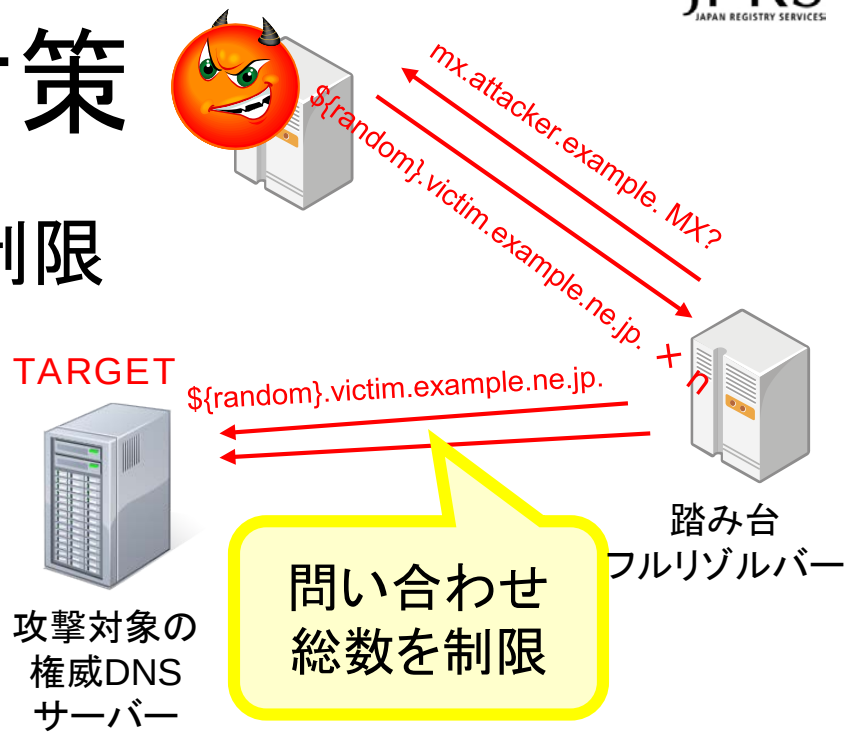
修正前の挙動: Unbound



委任先として指定されたドメイン名の
AレコードとAAAAレコードを問い合わせ

- 委任先ドメイン名のIPアドレスを、応答を待たずに並列で問い合わせる
  - BIND 9と比べると、応答がない時の並列度は控えめ
    （target-fetch-policy オプションで制限されると思われる）
  - 総数には上限がなく、委任先がいくつあっても全て問い合わせているようだ

論文で提案された対策



- MaxℓFetch: 派生した追加の問い合わせ数を制限
  - 権威DNSサーバーの名前解決が必要な場合、その回数に上限を設ける
  - 並列度は実装任せだが、問い合わせ総数を制限する形となる
- 対策として効果があり、副作用も軽微と主張
  - RTTへの影響はないそうだが……（IIJ島村さんのライトニングトークで☺）
- 論文では他にもいくつかの対策が提案されている
  - 多数の委任を含む応答を検知する
  - fetch-limit（ドメイン名単位・権威サーバー単位の問い合わせレートリミット）
- NSEC aggressive use（RFC 8198）もある程度対策になると思われる

修正後の挙動

- 派生した追加の問い合わせ総数が制限されるようになった
- BIND 9
  - 権威DNSサーバーの名前解決を試みた回数が4回を超えていて、委任先の権威DNSサーバーの数が5個を超えている場合に打ち切る
  - 定数（NS_FAIL_LIMIT: 4、NS_RR_LIMIT: 5）はハードコード
- Unbound
  - 権威DNSサーバーの名前解決を試みた回数が16回を超えたら打ち切る
  - 権威DNSサーバーの名前解決を試みた結果、NXDOMAINになった回数が5回を超えている場合にも打ち切る
  - 定数（MAX_DP_TARGET_COUNT: 16、MAX_TARGET_NX: 5）はハードコード

まとめ

- 名前解決中に、派生した別の名前解決をする必要がある
  - 委任先はドメイン名で指されるため、内部名ではない場合は追加で名前解決が必要になる
- 複数のフルリゾルバー実装で、「派生した別の名前解決」を行う際の問い合わせ総数の制限が不十分であった
  - 派生した問い合わせを高い倍率で発生させ、DoS攻撃の踏み台にさせる・フルリゾルバー自身のリソースを逼迫させることができた
- 各開発元が協調して、論文で提案された対策が実装された

影響を受ける製品は速やかにバージョンアップしてください