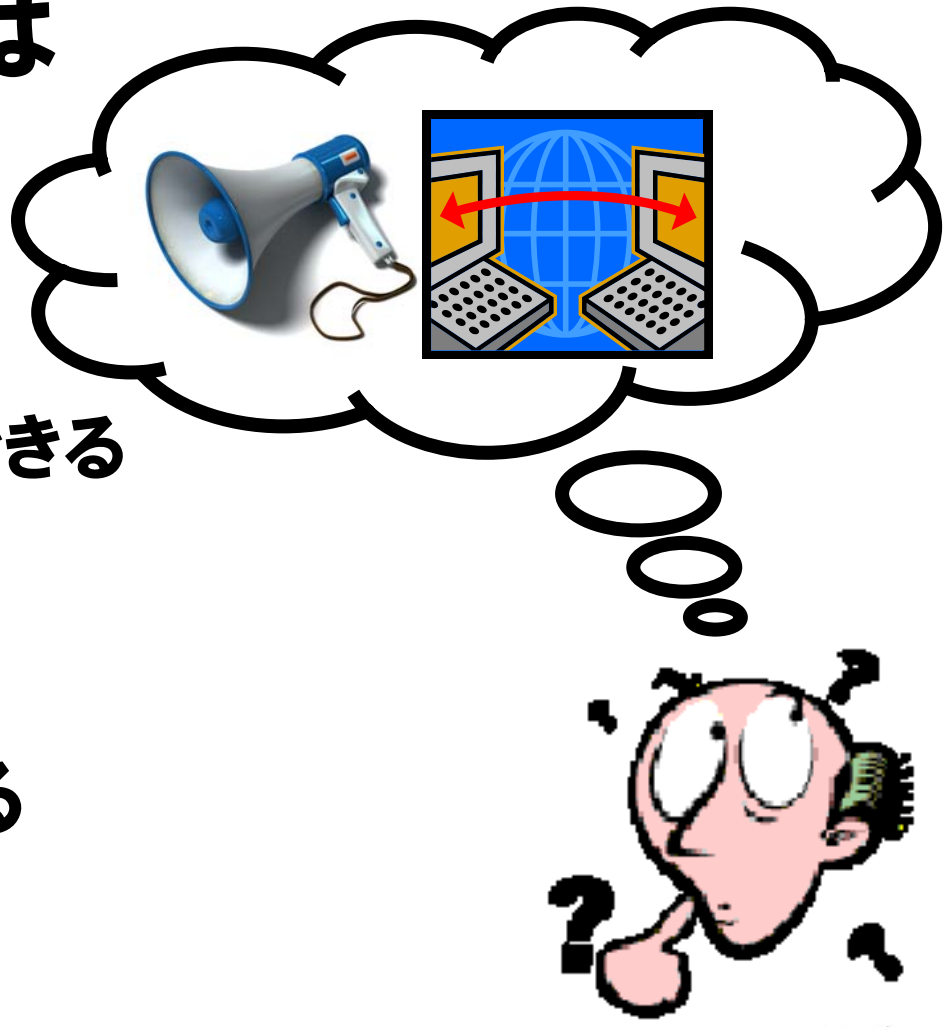
DDoSにあなたのDNSが使われる
～DNS Ampの脅威と対策～

INTEROP 2007

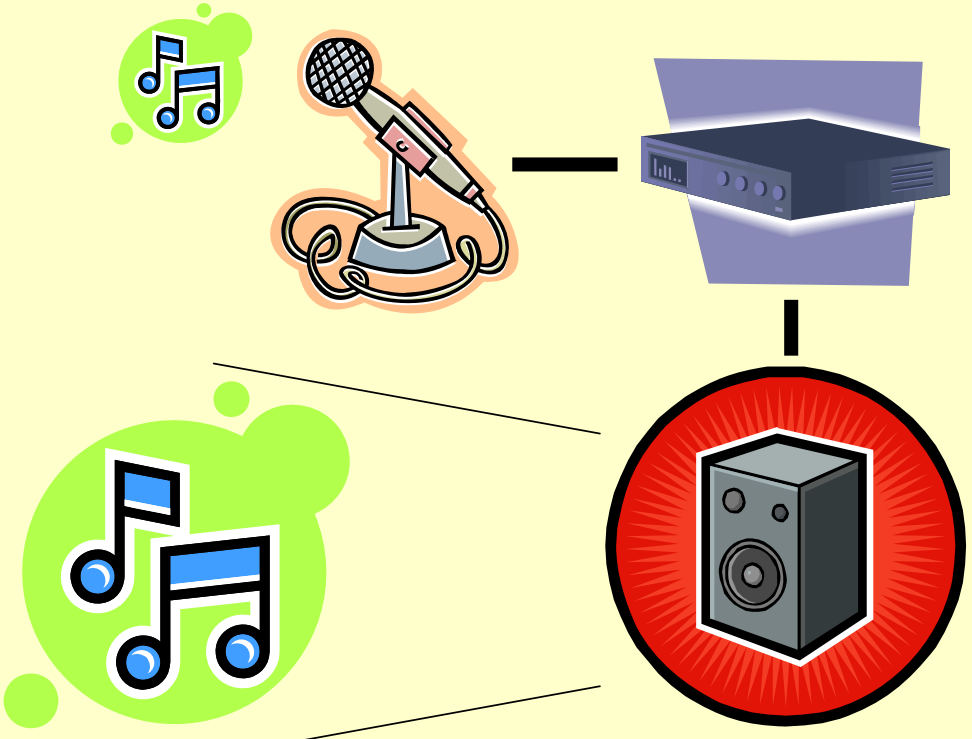
「DNS Amp攻撃」とは

- DDoS攻撃の一種
- DNSキャッシュサーバを悪用
  - より少ない資源で効果的に攻撃できる
- 攻撃力が強い
  - 分散型、数Gbps～数100Gbps
- 著名なサイトが被害を受けている
  - VeriSignやNetwork Solutionsなど

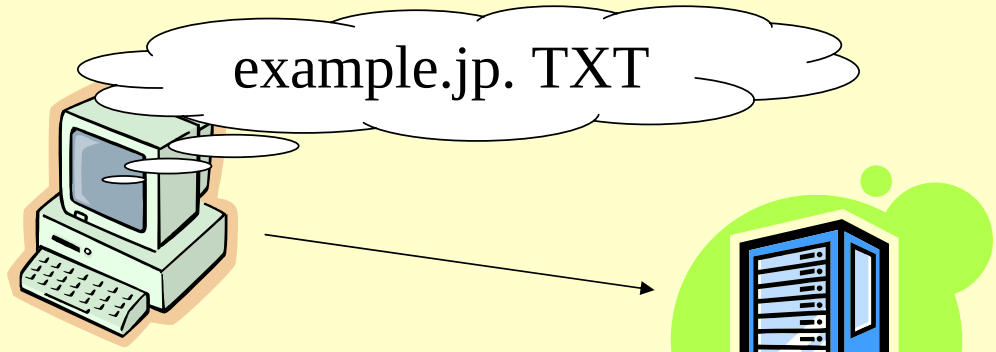


DNSがアンプ（増幅器）になる？

小さな音が大きくなる

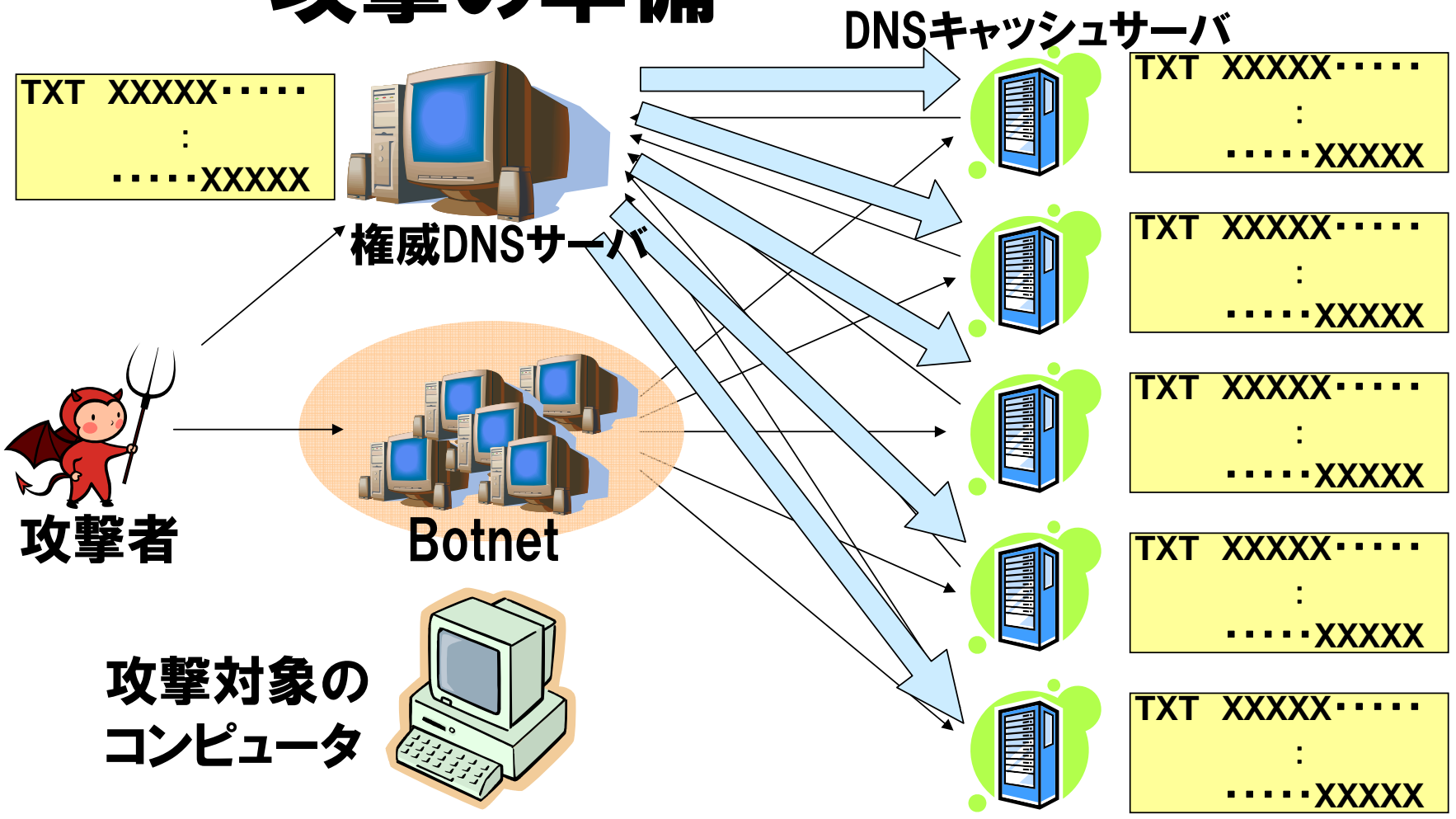


小さなパケットが大きくなる



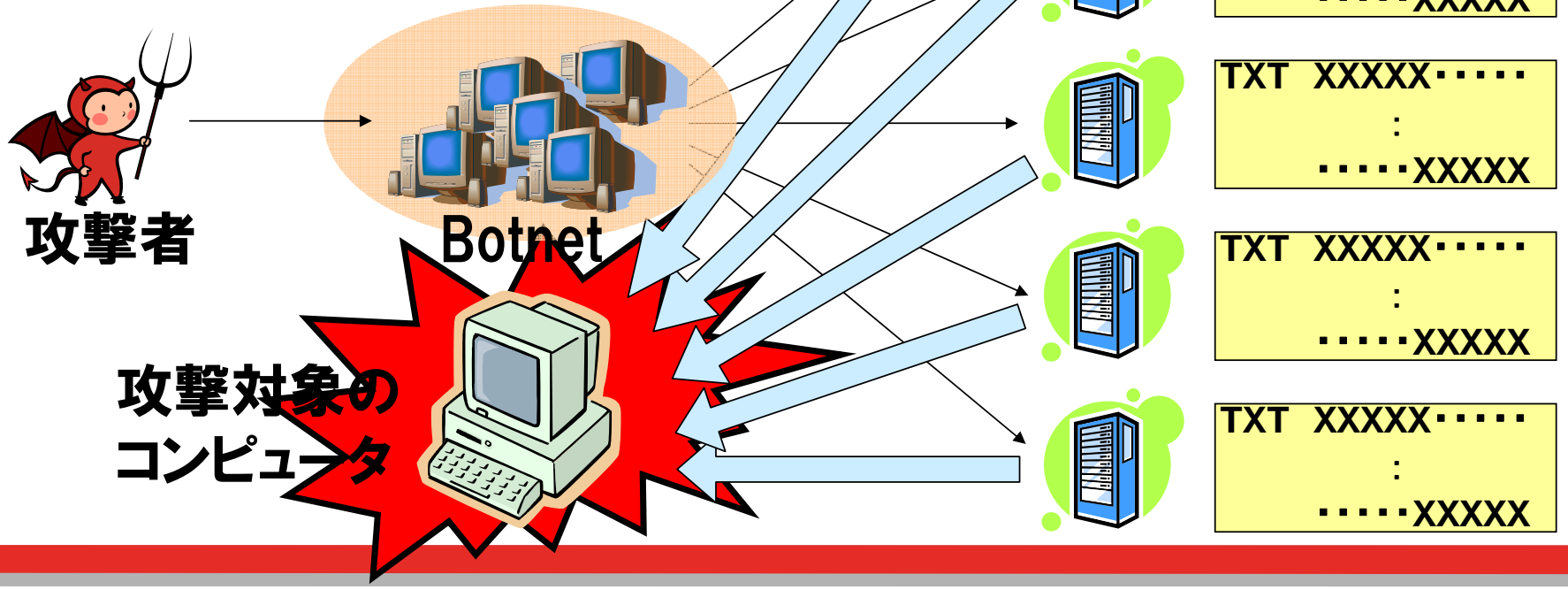

```
$ORIGIN example.jp.
@ IN TXT XXXXXXXXXXXX
        XXXXXXXXXXXX
        XXXXXXXXXXXX
        XXXXXXXXXXXX
        XXXXXXXXXXXX
        XXXXXXXXXXXX
```

攻撃の準備



攻撃！！！

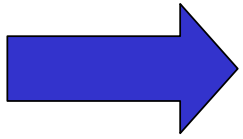
攻撃対象のコンピュータの
IPアドレスを騙って
一斉にDNS問い合わせを行う



何が問題なのか

DNSの仕組み・特徴

UDPなので処理が軽い
小さな問い合わせに大きな応答
インターネットの根幹機能の一つ
キャッシュ機能の存在



DNS Amp攻撃の特徴

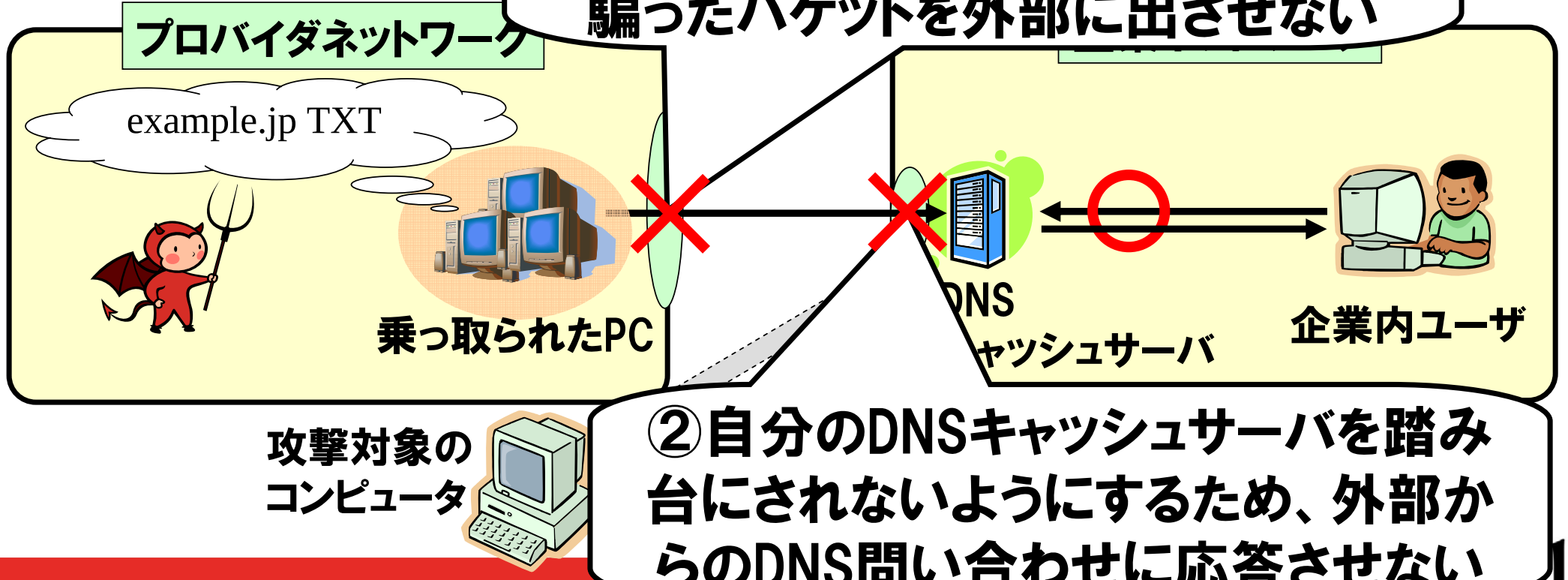
UDPなので送信元の詐称が容易
容易に大きなデータを作成可能
インターネット中に踏み台が存在
踏み台の被害に気づきにくい

DNSの仕組み・特徴そのものを悪用している

DNS Amp攻撃への対策

- 2つの対策

①自分のネットワークが攻撃元とならないようにするため、IPアドレスを騙ったパケットを外部に出させない



②自分のDNSキャッシュサーバを踏み台にされないようにするため、外部からのDNS問い合わせに応答させない

DNS Amp攻撃への対策

①IPアドレスを騙ったパケットを外部に出させない

⇒ Source Address Validation（送信元検証）の導入

- Ingress Filter（BCP 38 / RFC 2827）
- バックボーン側通信機器で送信元IPアドレスの正当性を確認
- 偽装された送信元IPアドレスを利用した通信を遮断

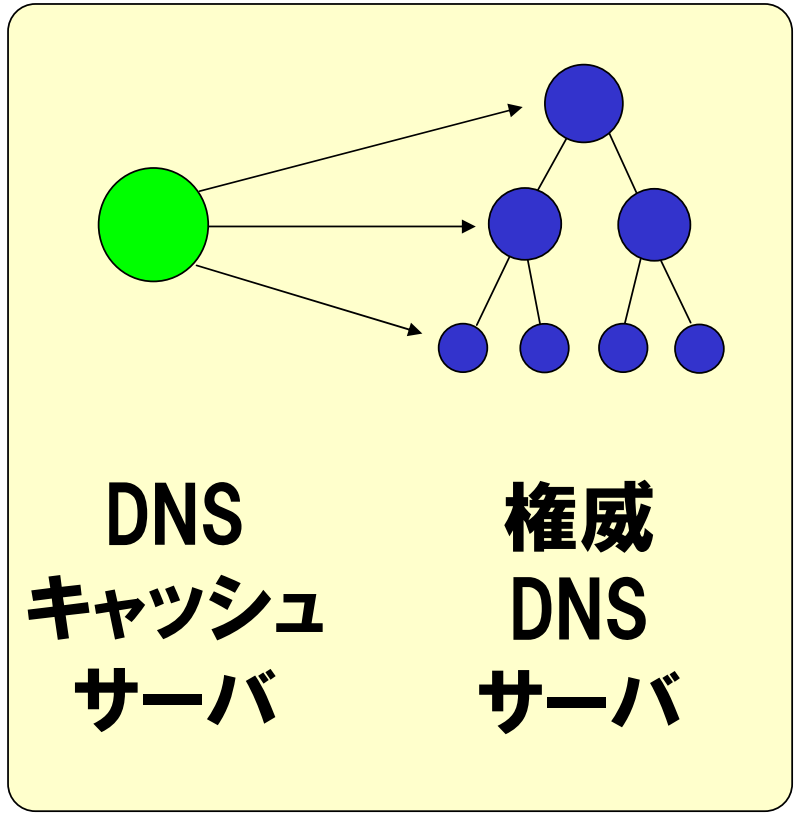
・ プロバイダやiDC単位での導入が望ましい

DNS Amp攻撃への対策

②外部からのDNS問い合わせに応答させない

Open Resolverって何?

- どこからのDNS問い合わせにも応答する状態のDNSサーバ
- ここで素直な疑問「DNSサーバってインターネット上のどこからの問い合わせでも応答しなきゃいけないんじゃないの?」
- DNSサーバには機能の異なる2種類のサーバが存在する
  - 「DNSキャッシュサーバ」と「権威DNSサーバ」



DNSキャッシュサーバと権威DNSサーバ

DNSキャッシュサーバ

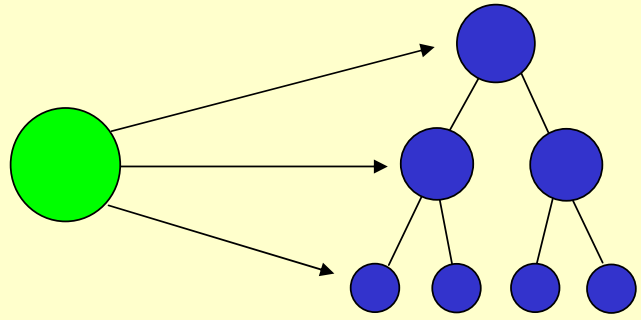
- ユーザが参照
- ゾーンデータを管理しない
- 反復検索を行う
- データをキャッシュする

組織内ネットワークからの問い合わせにのみ応答すればよい

権威DNSサーバ

- DNSキャッシュサーバが参照
- ゾーンデータを管理する
- 反復検索を行わない
- データをキャッシュしない

インターネットからの全ての問い合わせに応答する必要あり



DNS キャッシュ サーバ

権威 DNS サーバ

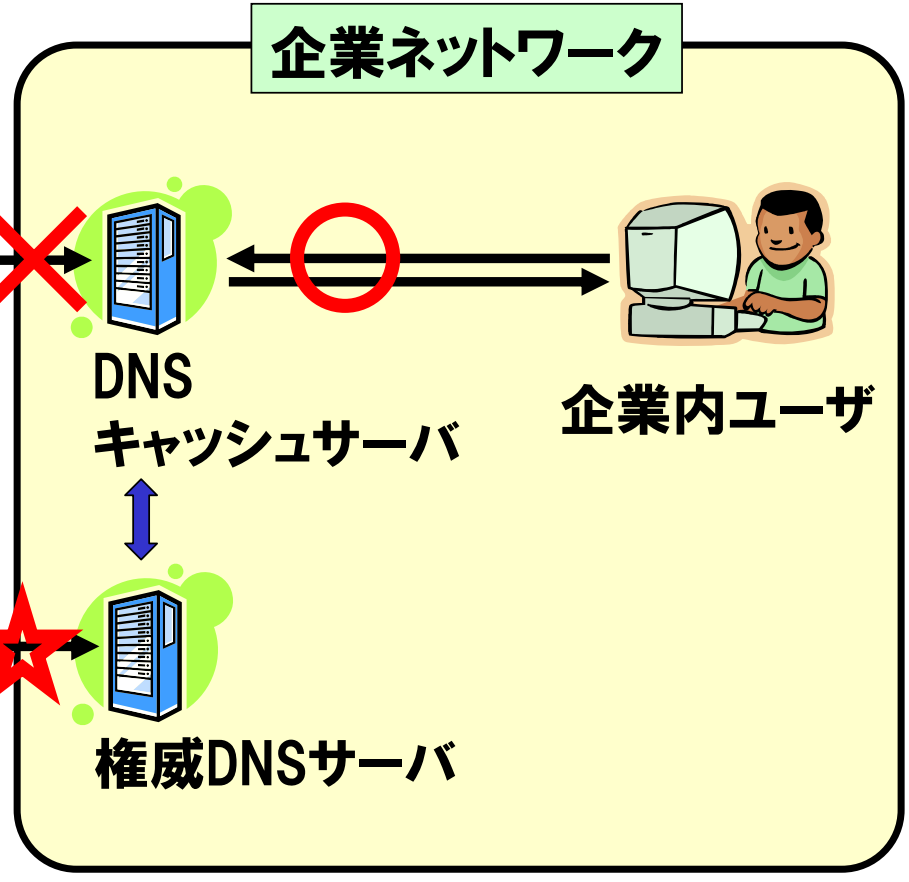
Open Resolverの撲滅のために

- 必要な3つの対策

① DNSキャッシュサーバと権威DNSサーバ(DNSコンテンツサーバ)の分割

② 権威DNSサーバでは不必要な反復検索機能を無効に設定

③ DNSキャッシュサーバでは外部からの問い合わせに応答しないようにアクセスコントロールを設定



まとめ – DNS Amp攻撃を撲滅するために

- 自分のネットワークが攻撃元とならないように
  - Source Address Validation（送信元検証）が有効です
- 自分のDNSサーバを踏み台にされないように
  - あなたのDNSサーバ、Open Resolverになっていませんか？
  - 3つの対策を実施しましょう
    - ① DNSキャッシュサーバと権威DNSサーバを分離
    - ② 権威DNSサーバでは反復検索機能を無効に
    - ③ DNSキャッシュサーバでは自分以外のネットワークからのアクセスを禁止

インターネット全体での取り組み

- 会議・イベント等における活動
  - INTEROP / Internet Week 等
  - APNIC / RIPE Meeting 等
- オペレータコミュニティ
  - JANOG / NANOG / OARC 等
  - DNSOPS.JP
    - BoF: 6月13日 (水) 18:30- (参加無料)