キャッシュポイズニング攻撃対策：
権威DNSサーバー運用者向け―基本対策編

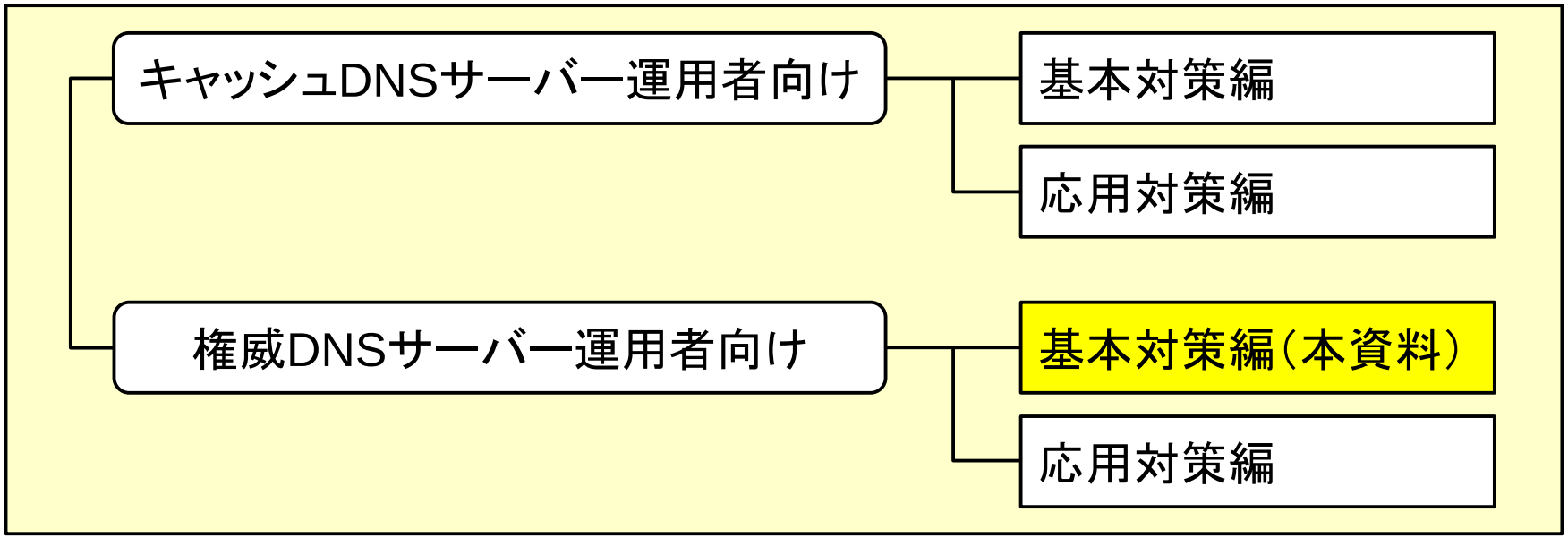
初版作成：2014年5月30日

最終更新：2014年5月30日

株式会社日本レジストリサービス（JPRS）

本資料の位置づけ

- 本資料は以下の四部構成の資料の一部
  - 対象者ごとに、キャッシュDNSサーバー運用者向けと権威DNSサーバー運用者向けに大別
  - それぞれを、基本対策編と応用対策編の二部で構成



本資料の内容（基本対策編）

- 本資料では権威DNSサーバー運用者向けの基本対策編として、以下の項目について解説

  対策の基本的な考え方

  1. 各レコードにおけるTTL設定の見直し
  2. 権威DNSサーバーの安定運用・強化
  3. 権威DNSサーバーにおける攻撃の検知と対応

- キャッシュポイズニング攻撃の概要・攻撃対策の基本とその分類（三つの対策）については、「キャッシュDNSサーバー運用者向け―基本対策編」の内容を参照

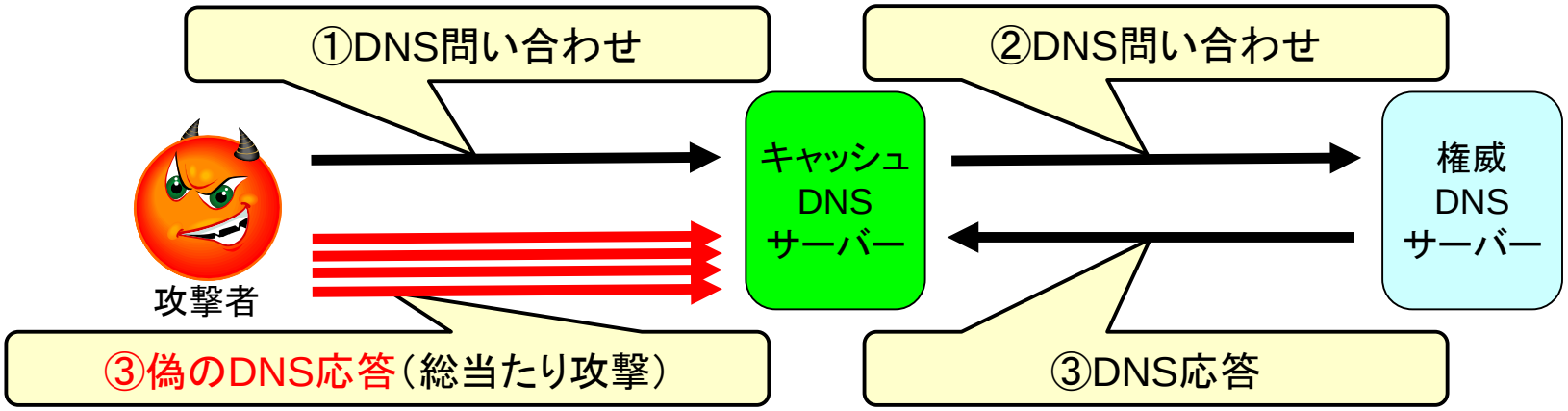
対策の基本的な考え方

おさらい：キャッシュポイズニング攻撃の流れ（偽の応答を本物よりも先に注入）

① 攻撃者がDNS問い合わせを送る
（あるいは、問い合わせを送るように仕向ける）

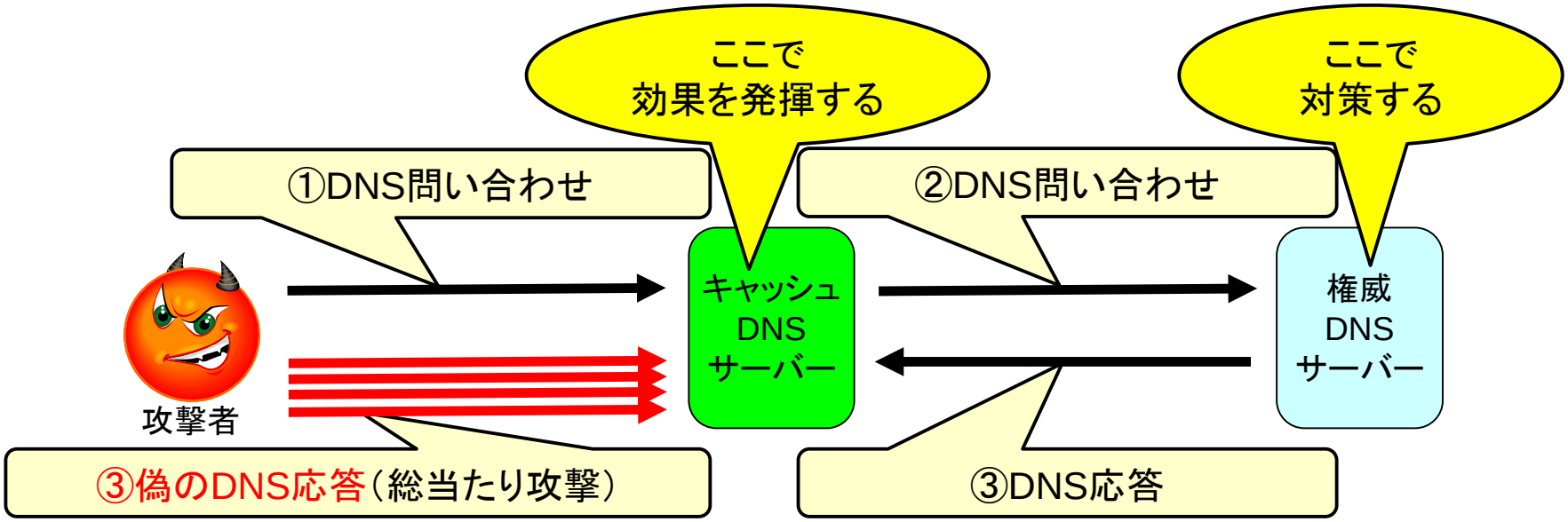
② キャッシュDNSサーバーが権威DNSサーバーにDNS問い合わせを送る

③ 攻撃者が②に対する偽の応答の注入を試みる



権威DNSサーバーにおける対策

- 自分が管理するドメイン名が被害に遭わないようにするための対策
- 通信相手のキャッシュDNSサーバーに対する**間接的な対策**が中心になる



攻撃対策の基本（三つの対策）

- 攻撃対策の基本（三つの対策）

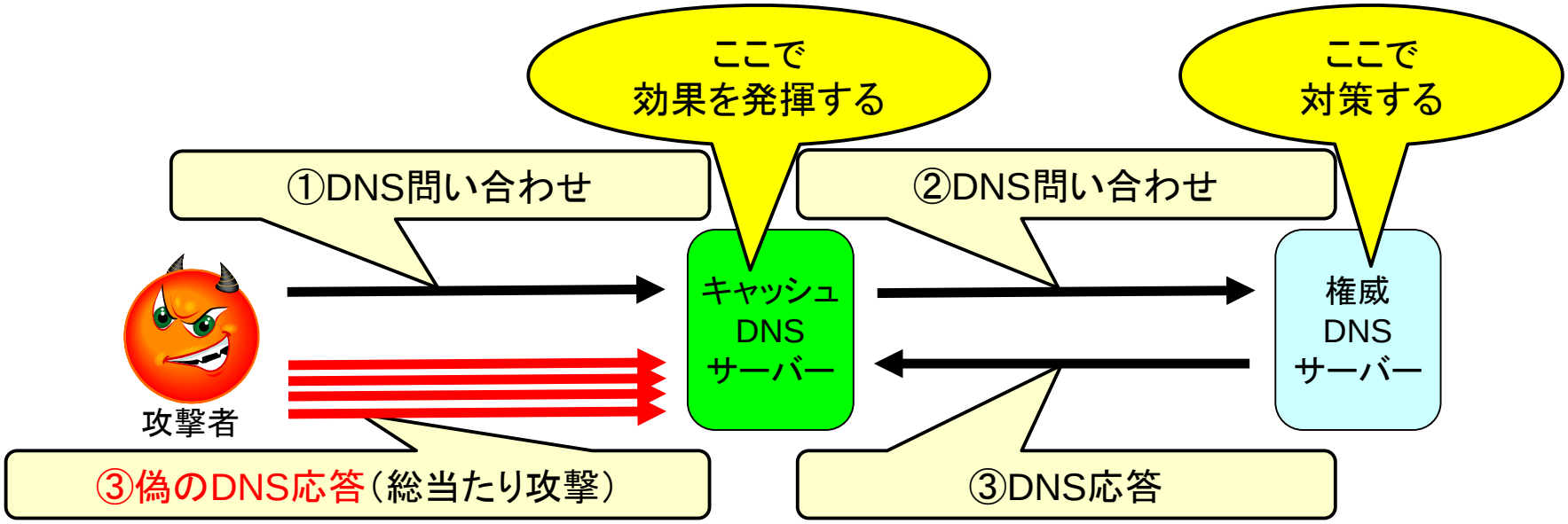
  ① 偽の応答を注入されない（されにくくなる）ようにする
  ② 受け取った応答のチェックを厳重にする
  ③ 攻撃を検知して対応する

  「キャッシュDNSサーバー運用者向け―基本対策編」から引用

- 権威DNSサーバーにおいてとりうる対策：
  - 上記のうちの①と③

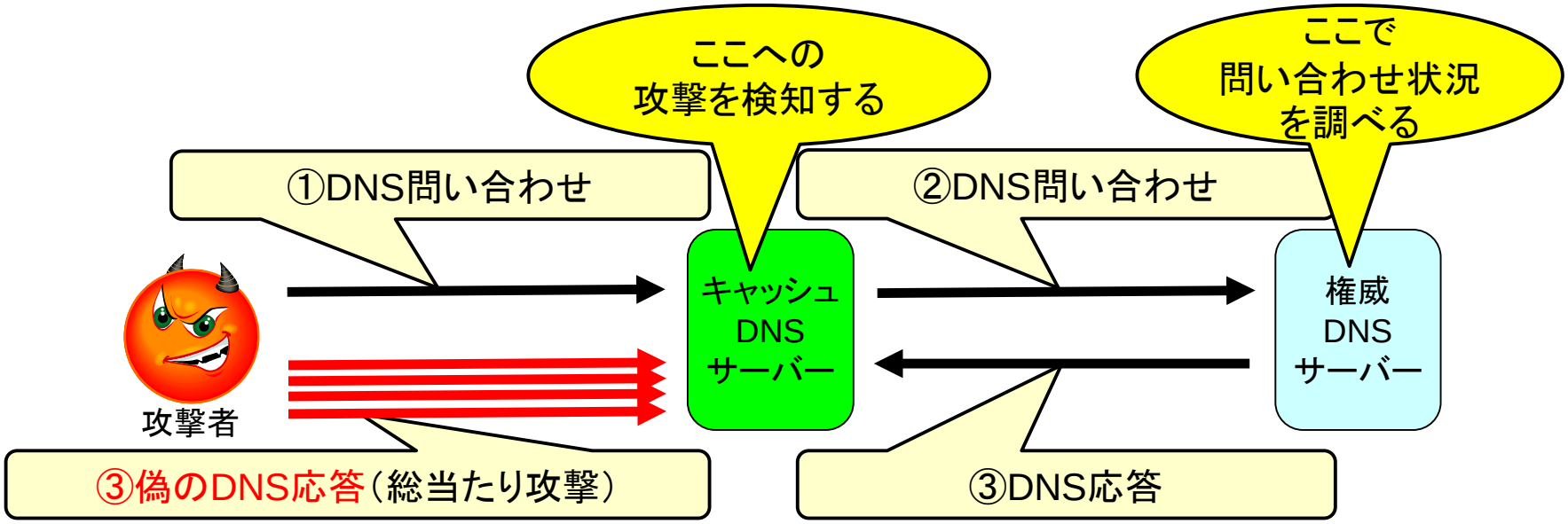
偽の応答を注入されない（されにくくなる）ようにする

- 考え方：
  - 通信相手のキャッシュDNSサーバーに、
    自分が管理するドメイン名の偽の応答を注入されない（されにくくなる）ようにする



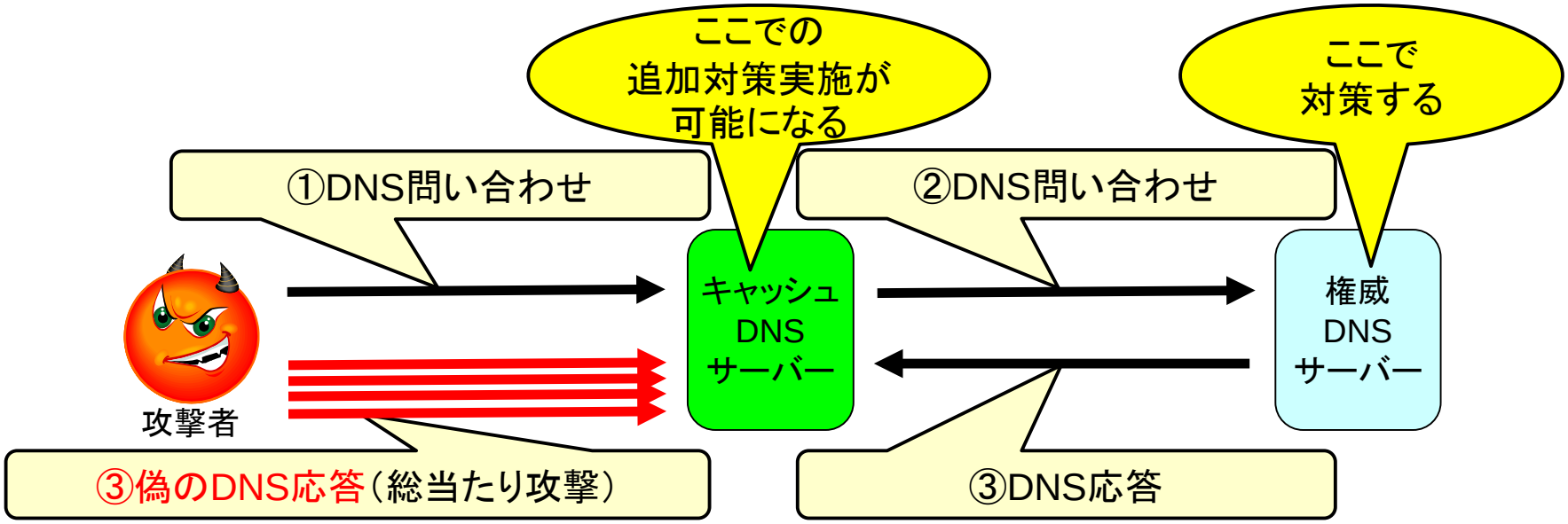
攻撃を検知して対応する(1)

- 考え方:
  - 通信相手のキャッシュDNSサーバーで、
    自分が管理するドメイン名が攻撃を受けている
    ことを検知する



攻撃を検知して対応する(2)

- 考え方:
  - 通信相手のキャッシュDNSサーバーに、
    自分が管理するドメイン名への攻撃検知(追加対策)
    の手段を提供する



本資料で解説する対策例：基本対策編で解説

- 偽の応答を注入されない（されにくくなる）ようにする
  1. TTL設定値の見直し
  2. 権威DNSサーバーにおける安定運用・強化
- 攻撃を検知して対応する（1）
  3. 権威DNSサーバーにおける攻撃の検知と対応

応用対策編で解説

- 偽の応答を注入されない（されにくくなる）ようにする
  - ドメイン名の管理構造における配慮
- 攻撃を検知して対応する（2）
  - DNSSECの導入
  - DNS cookiesの導入

1. TTL設定値の見直し

① 偽の応答を注入されない（されにくくなる）ようにする対策の一つ

TTLと攻撃に対するリスク

- キャッシュポイズニング攻撃対策における基本
  - カミンスキー型攻撃手法の出現後も、TTLによる保護は依然として有効
- 短すぎるTTLは、キャッシュポイズニング攻撃に対する潜在的なリスクを高める
  - 参考：これでいいのかTTL―短いDNS TTLのリスクを考える
    <http://www.janog.gr.jp/meeting/janog19/files/DNS_Minda.pdf>

レコードの種別とTTLの考察

- 利用者が直接検索するレコード（通常のホスト名のA/AAAA）と、名前解決を制御するためのレコード（NS/ネームサーバーホスト名のA/AAAA）のTTLは、本来区別して考えるべき
- CDNサービスの普及により、通常のホスト名のA/AAAAレコードのTTLは短くなる傾向にある
  - 短いTTLのリスクを把握した上で運用する必要がある
- NSレコードのTTLが短すぎるのは、DNS運用上無意味かつ危険
  - 通常のDNS運用において、NSレコードに短いTTLを設定する必要性はほとんどない

各レコードにおけるTTLの推奨値は？

- 現時点において標準化されていない
- 参考：IETFの過去の議論（I-D）ではDNS運用の可用性向上のため、NS/ネームサーバーホスト名のA/AAAAのTTLとして「より長い値」「日単位」を推奨
  - Improving DNS Service Availability by Using Long TTL Values
    <http://tools.ietf.org/html/draft-pappas-dnsop-long-ttl-04>

> “More specifically we propose that Infra-RRs SHOULD have longer TTL values than those observed (12 or less hours), and we recommend that their TTL value SHOULD be in the order of days.”

2. 権威DNSサーバーの安定運用・強化

① 偽の応答を注入されない（されにくくなる）ようにする対策の一つ

期待される効果とリスク

- 権威DNSサーバーを安定運用することで、キャッシュDNSサーバーにおける偽の応答注入成功の確率を相対的に減少させる
- 権威DNSサーバーが適切に運用されていないと、キャッシュポイズニング攻撃成功の確率が上がる
  - 無応答や応答の遅延
    - 攻撃可能な時間（ウィンドウ）が増える
  - Lame delegation
    - 攻撃の機会が増える
      （権威DNSサーバーへの問い合わせが毎回実行される）

とりうる手法例(1)

- DoS攻撃耐性の強化
  - サーバーやネットワークの強化など

DoS攻撃により無応答や応答の遅延が発生すると、
キャッシュポイズニング攻撃成功の確率が上がる(前ページ参照)

- 権威DNSサーバーの健全な運用
  - サーバーソフトウェアの脆弱性対応
  - 親子間のネームサーバーホスト情報の整合
  - 適切な運用状況監視の実施(攻撃の検知にも有効)

とりうる手法例(2)

- 複数の権威DNSサーバーの公開
  - セカンダリサーバーの追加
  - 信頼できるDNS運用サービスの導入検討
- IP Anycastの導入検討
  - 応答遅延時間の減少やDoS攻撃耐性の強化に有効

サーバー追加における注意点

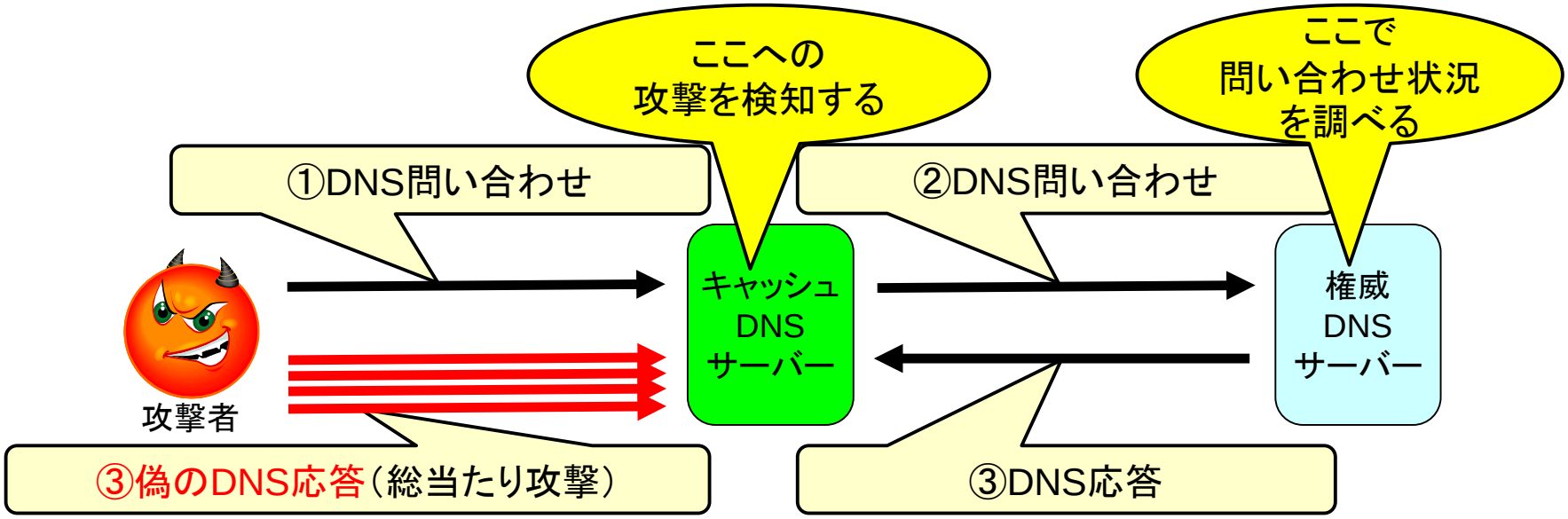
- サーバー数が多いほど良いわけではない
  - DNSプロトコルにおける制限に注意
  - 系全体としての安定性確保が重要
    - 不安定なサーバーがあると、かえってリスクが増す
- 設置するネットワーク環境も重要
- どのサーバーが選択されるかは、キャッシュDNSサーバー側の選択アルゴリズムに依存
  - 権威DNSサーバー側では制御不可

3. 権威DNSサーバーにおける攻撃の検知と対応

③ 攻撃を検知して対応する対策の一つ

権威DNSサーバーにおいて実施可能な対策

- 自分が管理するドメイン名に対する攻撃検知
  - 自分が管理するドメイン名が攻撃を受けていることを検知する



攻撃の検知（DNS問い合わせの内容）

- カミンスキー型攻撃手法の場合、到達する問い合わせパケットの内容が特徴的
  - $(random).ドメイン名に対する大量の問い合わせ
    - 攻撃対象ドメイン名にランダム文字列を加えたサブドメイン
- 典型的な攻撃パターン
  - 問い合わせパケットの数が急増している
  - そのパケットが同一・あるいは少数のIPアドレスから集中的に到達している
  - DNS問い合わせの内容が上記に該当する

検知可能な内容

- 以下の二点を権威DNSサーバー側で検知可能
  - あるキャッシュDNSサーバーにおいて、
    自分が管理するドメイン名が攻撃を受けていること
  - そのキャッシュDNSサーバーのIPアドレス
    - サービス用のIPアドレスと異なる場合もあることに注意
      （例：Google Public DNS）

検知の手法例

- 権威DNSサーバーにおける検知
  - サーバーにおけるトラフィック監視
  - ネームサーバーホストにおけるログ取得の実施、など
- 接続ネットワークにおける検知
  - 問い合わせ・応答パケットのキャプチャリング
  - ルーター・スイッチにおけるトラフィック監視、など

検知後の対応例

- JPCERT/CCへの報告
- サイトの利用者への告知
- DNSSEC導入の検討、など

参考リンク

- （緊急）キャッシュポイズニング攻撃の危険性増加に伴う
  DNSサーバーの設定再確認について（2014年4月15日公開）
  <http://jprs.jp/tech/security/2014-04-15-portrandomization.html>
- JPRS トピックス&コラム No.005
  DNSのさらなる信頼性向上のために
  ～IP Anycast技術とDNS～
  <http://jprs.jp/related-info/guide/005.pdf>
- JPRS トピックス&コラム No.020
  DNSの安全性・安定性向上のためのキホン
  ～お使いのDNSサーバーは大丈夫ですか？～
  <http://jprs.jp/related-info/guide/020.pdf>

更新履歴

- 2014年5月30日　　初版作成