DNS水責め（Water Torture）攻撃について

2014年9月27日 最終更新：2014年10月2日

SECCON 2014 長野大会 DNS Security Challenge

株式会社日本レジストリサービス（JPRS）
森下 泰宏（Yasuhiro Orange Morishita）

どんな攻撃なのか？

- 2014年1～2月頃から世界的に観測され始めた、DNSサーバーに対するDDoS攻撃の手法
  - 攻撃は現在も続いている模様
- 2014年6～7月にかけて国内の複数のISPで発生した「DDoS攻撃によるDNS障害」の原因の多くは、この攻撃によるものであったと考えられる
  - 複数の状況証拠
  - 複数のISP関係者からの伝聞

攻撃の特徴(1/2)

- 第三者のオープンリゾルバーやホームルーターを、攻撃の踏み台として悪用している
- しかし、DNS応答を攻撃に使っておらず、いわゆるDNSリフレクター(DNS Amp)攻撃ではない
  - この攻撃では送信元IPアドレスの詐称は必須ではない
- 攻撃に使われる問い合わせのパターンが、カミンスキー型攻撃手法のものと同じである

「カミンスキー型攻撃手法の問い合わせパターン」とは？

攻撃の特徴(2/2)

- カミンスキー型攻撃手法の問い合わせパターン
  - 攻撃対象のランダムなサブドメインへの問い合わせ
    - 例:asdykuadknce.www.example.jpのAレコード

ランダムな文字列(サブドメイン)

攻撃対象のドメイン名

- しかし、カミンスキー型攻撃手法において検出されるはずの、この問い合わせに対応する偽の応答が検出されない
- そのため、当初は攻撃の目的が判然としなかった

当初言われたこと:一体誰が何のためにこんなことを?

攻撃の目的(と考えられていること)

- 攻撃対象ドメイン名の権威DNSサーバーが、真の攻撃対象であったと考えられている
  - 攻撃対象ドメイン名の権威DNSサーバーを過負荷にし、そのドメイン名をアクセス不能の状態に陥らせる
  - 有力な状況証拠:攻撃対象になった数百のドメイン名の多くが、中国・台湾・香港関係のECサイトやカジノサイトなどの「中華系の金が動くサイト」であった
  - Botからの直接攻撃に比べ、フィルターしにくい
    - 正規のキャッシュDNSサーバーからのアクセスであるため

だとすると、国内ISPは攻撃者の真の攻撃目標ではなかった？

- 前述した国内ISPにおける「DDoS攻撃によるDNSの障害」の原因は、この攻撃の巻き添えによるものであったのではないかと言われている
  - 巻き添えの仕組みについては後述

事後資料で更新：水攻めではなく水責めが正しい旨の記述を追加

なぜ「水責め」と呼ばれるのか？

- 2014年2月にこの攻撃を報告した米国Secure64 Softwareが、公式ブログで命名
  - Water Torture: A Slow Drip DNS DDoS Attack
    <https://blog.secure64.com/?p=377>
- Slow Drip攻撃、ランダムDNSクエリー攻撃、ランダムサブドメイン攻撃などとも呼ばれている
- dns-operations MLでの関係者の発言・Secure64の技術者の発言から「水責め拷問」、特に「中国式水責め拷問」に由来している模様

注意：torture=拷問なので、「水攻め」ではなく「水責め」が正しい

「中国式水責め拷問」

- Wikipedia英語版：Chinese water torture
  <http://en.wikipedia.org/wiki/Chinese_water_torture>

> “Chinese water torture is a process in which water is slowly dripped onto a person's forehead, allegedly driving the restrained victim insane.”

（椅子に拷問相手を縛り付け、額にゆっくりと水滴を滴下する）

- 今回の攻撃形態や、攻撃により各DNSサーバーが徐々に追い込まれていくさまが、<u>この拷問を彷彿（ほうふつ）とさせる</u>
  - 多数のBot（送信元IPアドレス）を用いた低頻度の攻撃

攻撃のシナリオ：登場人物

攻撃者

オープンリゾルバーのリスト

Botnet

オープンリゾルバー

攻撃対象ドメイン名の権威DNSサーバー

ns1

ns2

ISP A

ISP B

欠陥を持つホームルーター（オープンリゾルバーの状態）

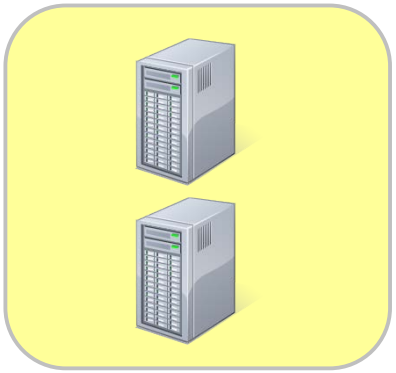
ISPのキャッシュDNSサーバー（ISPの顧客にサービスを提供）

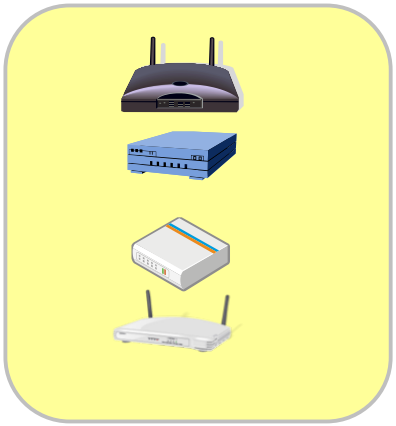
登場人物は大きく分けて6種類

登場人物紹介（1/3）

- 攻撃者
  - オープンリゾルバーのリストを持っている
  - Botnetを遠隔操作できる
- Botnet
  - 数多くのPCにより構成
  - 攻撃者により遠隔操作される

登場人物紹介(2/3)

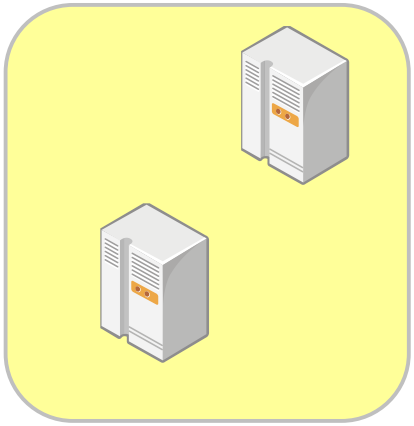


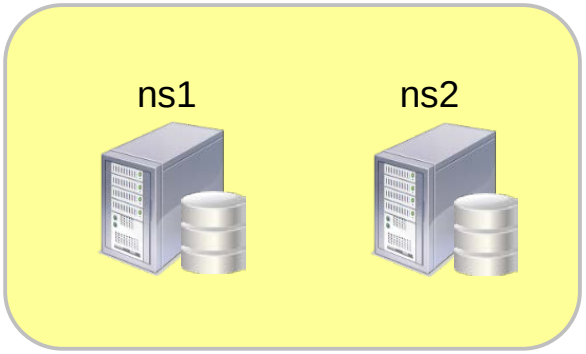


- オープンリゾルバー
  - 本来必要なアクセス制限がされておらず、外部から不正使用可能なDNSサーバー
- 欠陥を持つホームルーター
  - 本来受け付けてはならないWAN側からのDNS問い合わせを受け付け、正しく処理してしまう
  - 外部から見た場合、オープンリゾルバーの状態

攻撃者が持つオープンリゾルバーのリストには、
上記の双方が掲載されている模様(区別されていない)

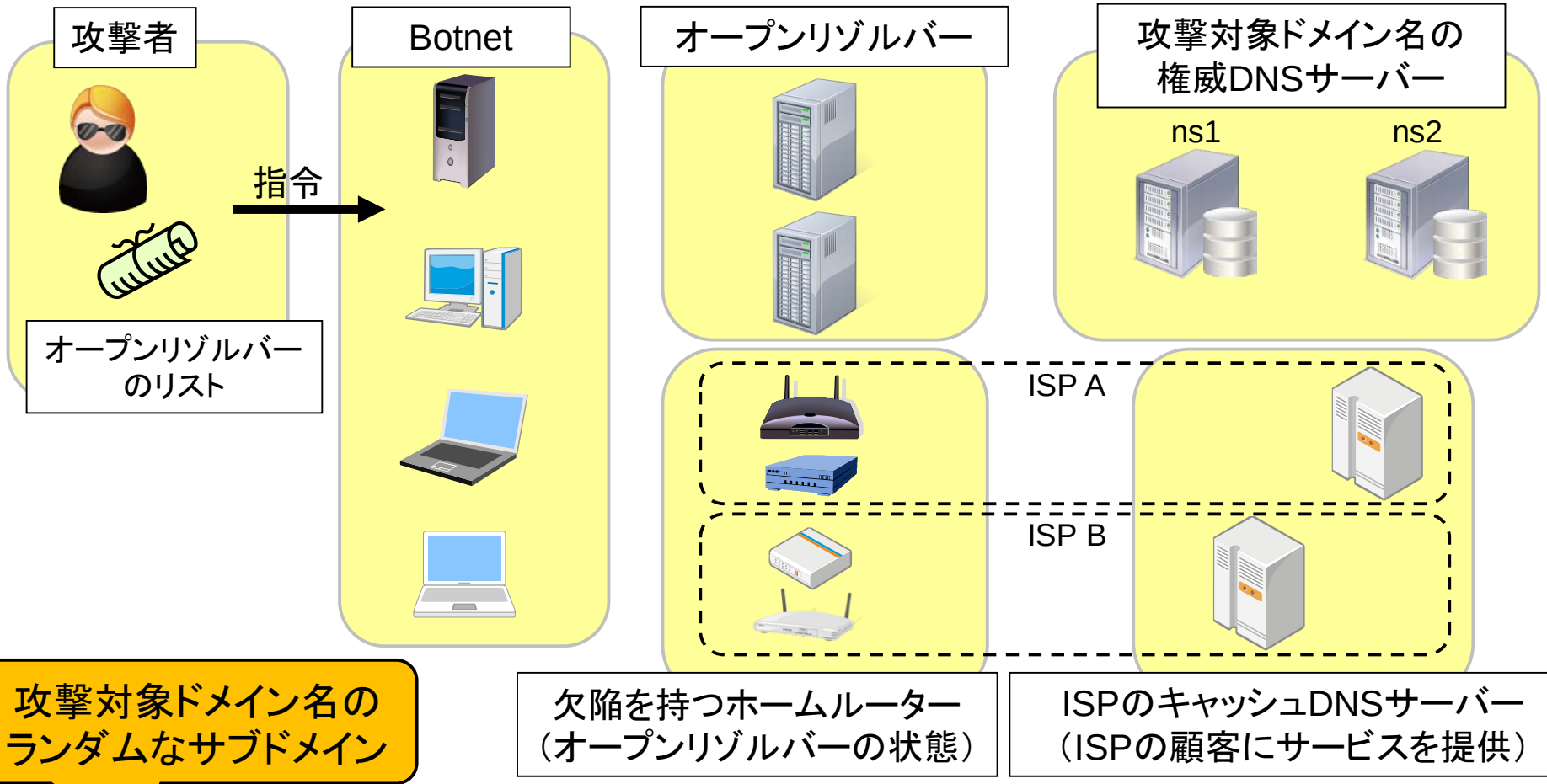
登場人物紹介(3/3)





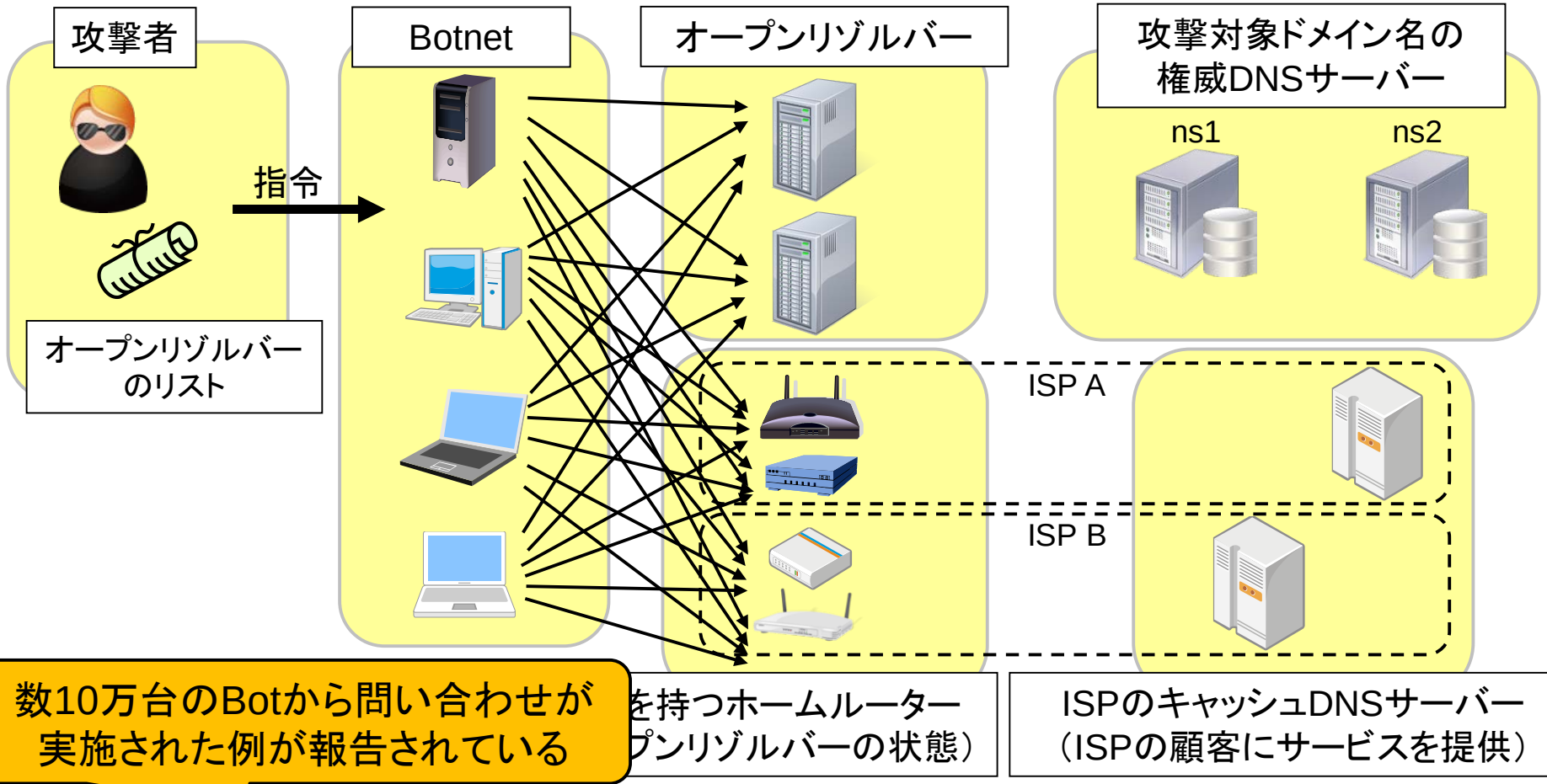
- ISPのキャッシュDNSサーバー
  - ISPの顧客にサービスを提供
  - オープンリゾルバーではない場合にも、攻撃の被害を受けうる
- 攻撃対象ドメイン名の権威DNSサーバー
  - 攻撃対象ドメイン名(ゾーン)を管理する権威DNSサーバー
  - 攻撃者の(真の)攻撃対象と考えられている

攻撃のシナリオ（1/4）



1. 攻撃者がBotnetに対し、リストにあるオープンリゾルバーに対し、(random).www.example.jpをDNS問い合わせするように指令を出す

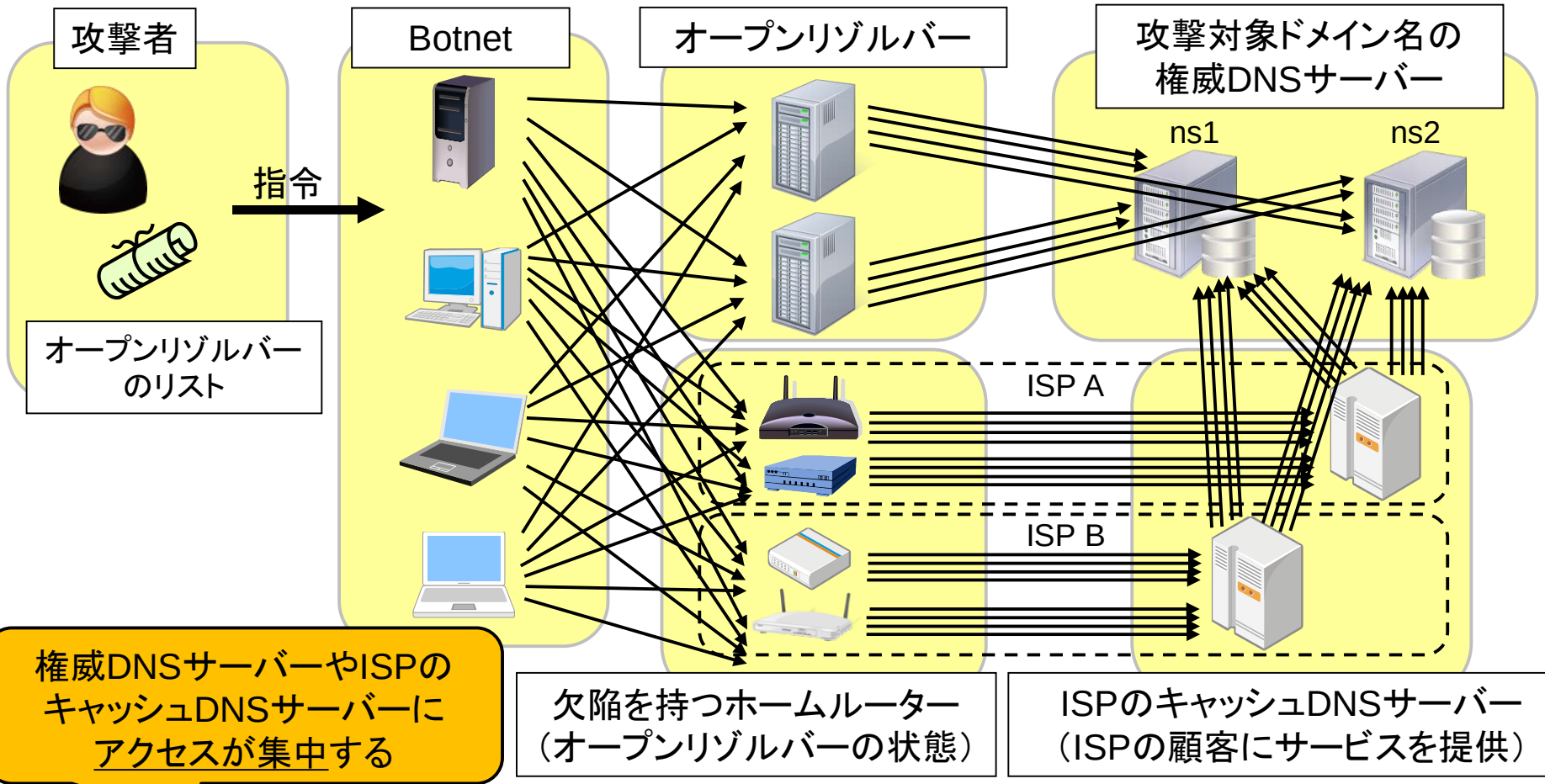
攻撃のシナリオ（2/4）



数10万台のBotから問い合わせが実施された例が報告されている

2. Botnetを構成する各PC（Bot）が、リストに掲載されたIPアドレスに問い合わせを送る
規制回避のため、数多くのBotから「広く薄く」問い合わせが送られる（Slow Drip）

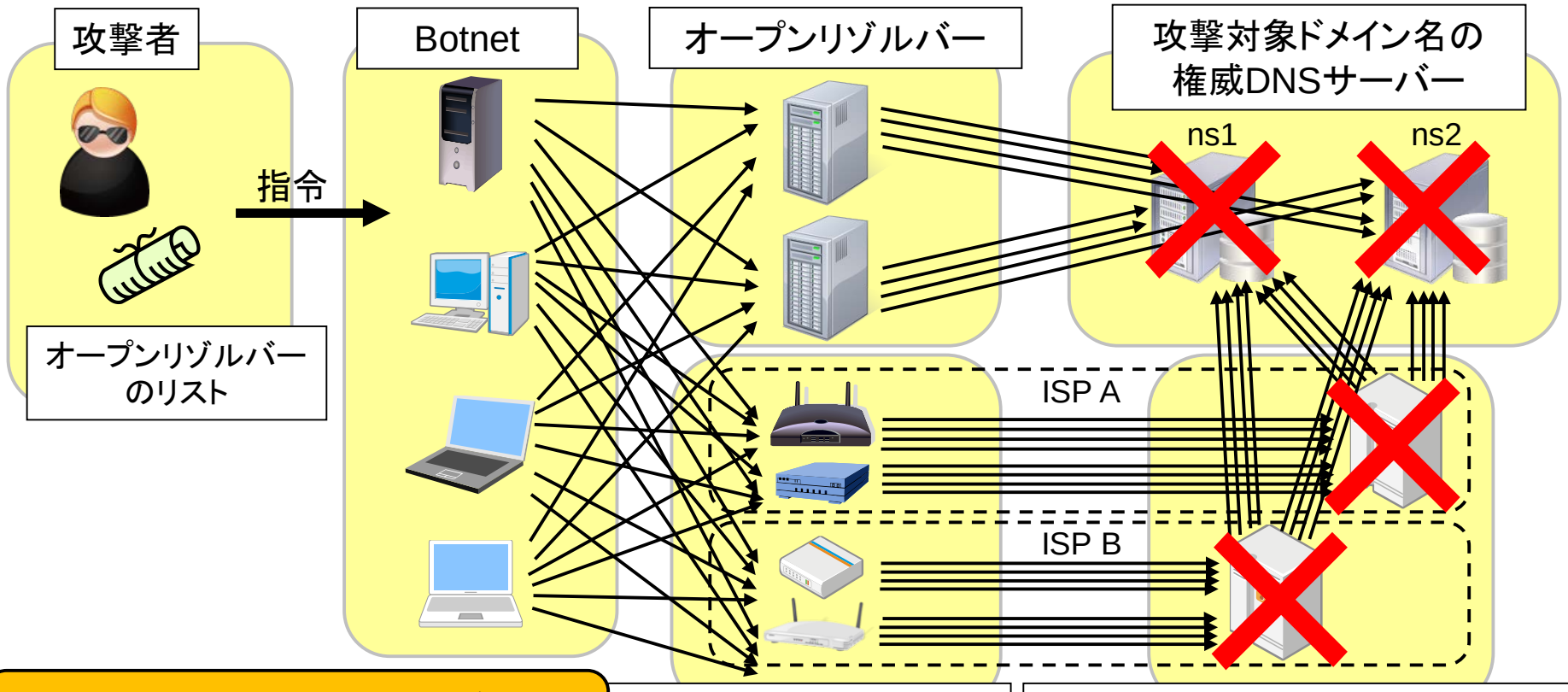
攻撃のシナリオ（3/4）



権威DNSサーバーやISPのキャッシュDNSサーバーにアクセスが集中する

3. キャッシュに存在しないため、権威DNSサーバーに問い合わせが毎回発生
（ホームルーターではISPのキャッシュDNSサーバーに問い合わせが毎回転送）

攻撃のシナリオ（4/4）



ISPのキャッシュDNSサーバーは、顧客側から攻撃されることになる

4. 問い合わせが集中する攻撃対象ドメイン名の権威DNSサーバーや
ISPのキャッシュDNSサーバーが過負荷になり、サービス不能状態に陥る

攻撃成立の理由

- 存在しない・キャッシュされていない名前の検索処理は、コストが高い
  - 権威・キャッシュのいずれにとっても（特にキャッシュ）
- 権威DNSサーバーの過負荷（応答遅延・無応答）が、キャッシュDNSサーバーにも悪影響を及ぼす
  - タイムアウトを待ったり、再送したり、別サーバーへの問い合わせを実施したりしなければならない
    - 処理中のセッションが溜まっていく
  - キャッシュDNSサーバーが並列処理可能なセッションの数には限度がある
    - 限度を超えると、問い合わせを受け付けなくなる実装が存在

考えうる攻撃対策：キャッシュDNSサーバーにおける対策例

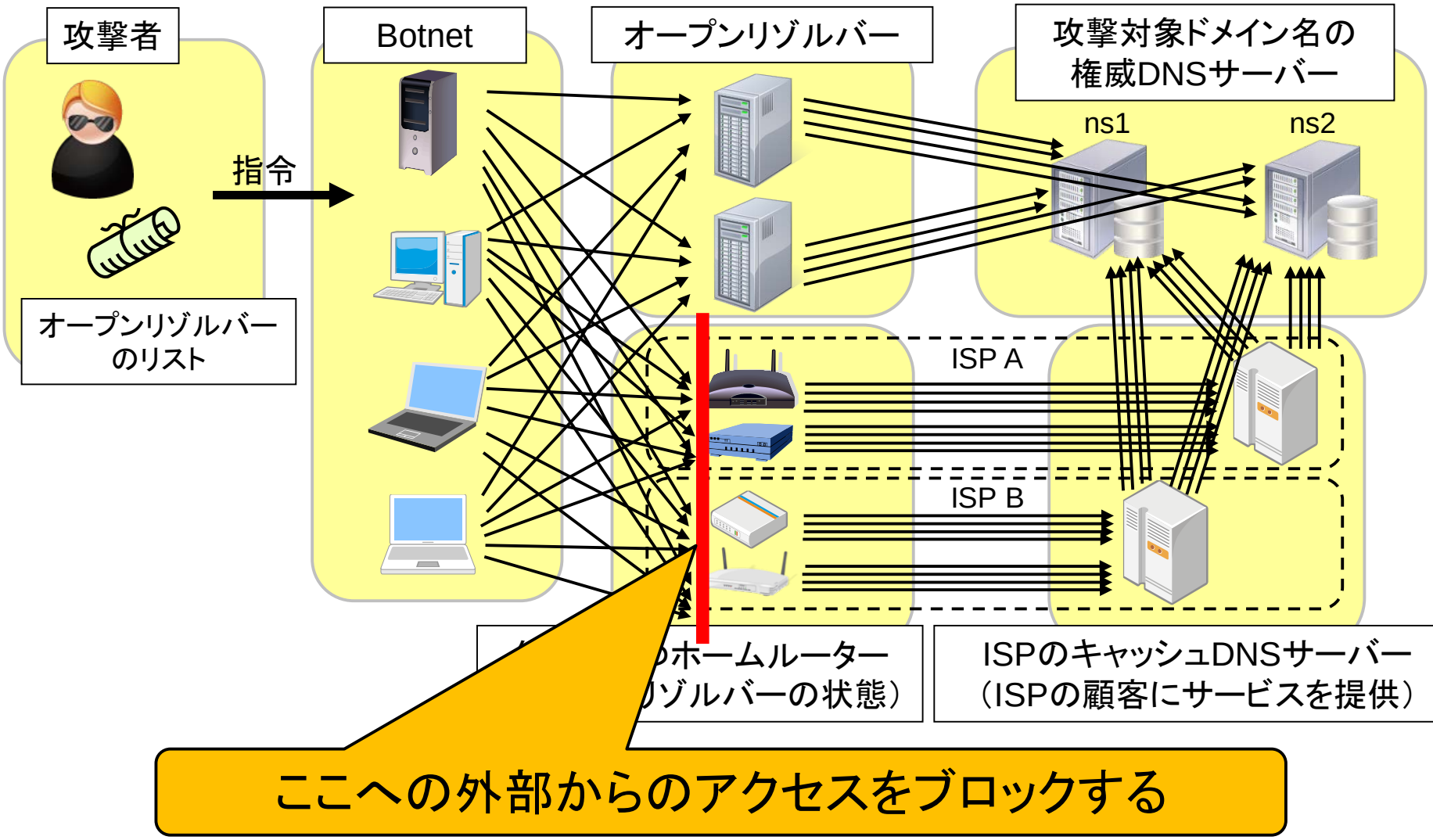
- 攻撃対象のゾーンをローカルに持たせる
  - 対象ドメイン名のDoSとしては成立していることに注意
  - 参考：とあるドメイン名の権威DNSサーバーへの攻撃とISP側の（間違った？）対応
    <https://yukar.in/note/ckFhbm>
    （2014年6月20～21日にかけてのtwitterでのやりとりのまとめ）
- BIND 9のRPZ（Response Policy Zone）機能を用い、「*.攻撃対象ドメイン名」の問い合わせに関する特別ルールを記述する
- iptables、あるいはそれに相当する機能でマッチングルールを書き、当該のDNS問い合わせを捨てる

決定打と考えられる対策はまだ存在しない

考えうる攻撃対策：ISPの網側における対策例

- IP53B（外部から53/udpへのアクセスをブロック）
  - ホームルーターの欠陥を外部から利用できなくする
  - リフレクター攻撃対策として、IP123B（NTP）と共に導入が進みつつある
- 「通信の秘密」との関係を考慮する必要あり
  - 詳細は後述

IP53Bの概要



事後資料で更新：「インターネットの安定的な運用に関する協議会」の記述を追加

IP53Bと通信の秘密との関係（1/2）

- 2014年7月22日にJAIPAなど5団体で組織される「インターネットの安定的な運用に関する協議会」のガイドラインが改定され、以下の事例について「正当業務行為として違法性が阻却されると考えられる」という記述が追加された

【事例】DNS及びNTPの仕組みを悪用したAmp攻撃が急増している状況を踏まえ、あるISPにおいて、当該攻撃によるインターネットアクセスやメールの遅延等の発生を未然に防止するため、自社のネットワーク網の入口又は出口を通過する全ての通信の宛先IPアドレス及びポート番号を常時確認し、自社の管理下の動的IPアドレス宛てであって、UDP53番ポート又はUDP123番ポートに対して送信された通信を割り出し、これを遮断した。

引用元：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（第3版）
<http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf>

IP53Bと通信の秘密との関係（2/2）

- この改定により、日本のISPは予防目的の正当業務行為として、IP53Bを事前実施可能になった
  - 予防目的：攻撃を受けていなくても実施可能
  - ただし、対象を「動的IPアドレス」の「UDP53番とUDP123番」のみに限定
- ある関係者によると前述のガイドラインは、「最小の記述で最大の効果を発揮させるようにする」ことをめざしたものであるとのこと

考えうる攻撃対策：プログラムの追加導入・機能追加

- いくつかの対策用プログラムが発表されている（注：私は試していません）
  - 「攻撃の検知」と「対応の自動化」を図るものが多い
    - dns_servfail_attack_mitigator <https://github.com/cejennings/dns_servfail_attack_mitigator>
    - unbound-reqmon <https://github.com/tarko/unbound-reqmon>
    - dnsbff <https://github.com/willt/dnsbff>
- BIND 9.11でExperimentalな実装が入る見込み
  - 9月のUKNOFの発表で案のいくつかが発表された（参考資料のリンク先を参照）

and what is worse…（1/2）

- この攻撃手法は単純かつ応用範囲が広い
  - DNSの仕組みそのものを攻撃に悪用している
  - キャッシュDNSサーバーへのDoSを目的にできうる
  - オープンリゾルバー経由やホームルーター経由でなくても成立しうる（クライアントPCのマルウェア経由など）
- 不用意な対策が悪影響を及ぼす場合がある
  - 例：キャッシュDNSサーバーにおける、不適切なローカルゾーンの記述（前述）

and what is worse…（2/2）

- DNS RRL（Response Rate Limiting）の導入が、この攻撃による影響を大きくする場合がある
  - DNS RRLによる応答廃棄やTCPでの再送依頼が、キャッシュDNSサーバーの負荷を高める
- キャッシュポイズニング攻撃と併用が可能である
  - 現在の状況は「木を隠すなら森」の状態かもしれない

※：DNS RRL：DNSリフレクター攻撃を防止する仕組みの一つとして、権威DNSサーバーに導入される技術の一つ

参考リンク（1/3）

- 米国Secure64 Softwareの公式ブログ
  - Water Torture: A Slow Drip DNS DDoS Attack
    <https://blog.secure64.com/?p=377>
- A10ネットワークスによる解説スライド
  - ランダムDNSクエリー攻撃（DNS Water Torture）対策について
    <http://www.a10networks.co.jp/files/140731/dns_water_torture.pdf>

参考リンク（2/3）

- 警察庁@policeによる注意喚起
  - 日本国内のオープン・リゾルバを踏み台としたDDoS攻撃発生に起因すると考えられるパケットの増加について
    <http://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf>
- JAIPAなど5団体によるガイドライン
  - 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（第3版）
    <http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf>
- JPRS藤原の解説スライド（第1回ISOC-JP勉強会）
  - DNSのタベ -セキュリティ・技術的動向に関して-
    <http://www.isoc.jp/wiki.cgi?page=1st%5FISOC%5FJP%5FWorkshop&file=20140729%2Disoc%2Epdf&action=ATTACH>

参考リンク（3/3）

- 2014年9月に英国で開催されたUKNOF29 & Internet Society ION Conferenceの発表資料
  - ① 米国Nominum社
  - – Latest Internet Plague: Random Subdomain Attacks
    <https://indico.uknof.org.uk/materialDisplay.py?contribId=15&materialId=slides&confId=31>
  - ② 米国ISC（BIND開発元：発表したのは英国在住の方）
  - – Tales of the unexpected - handling unusual DNS client behavior
    <https://indico.uknof.org.uk/materialDisplay.py?contribId=7&materialId=slides&confId=31>

Q & A