権威DNSサーバーを狙った攻撃の影響範囲と可用性を高めるためのポイント

～ランダムサブドメイン攻撃を題材として～

2023年6月14～16日

Interop Tokyo 2023

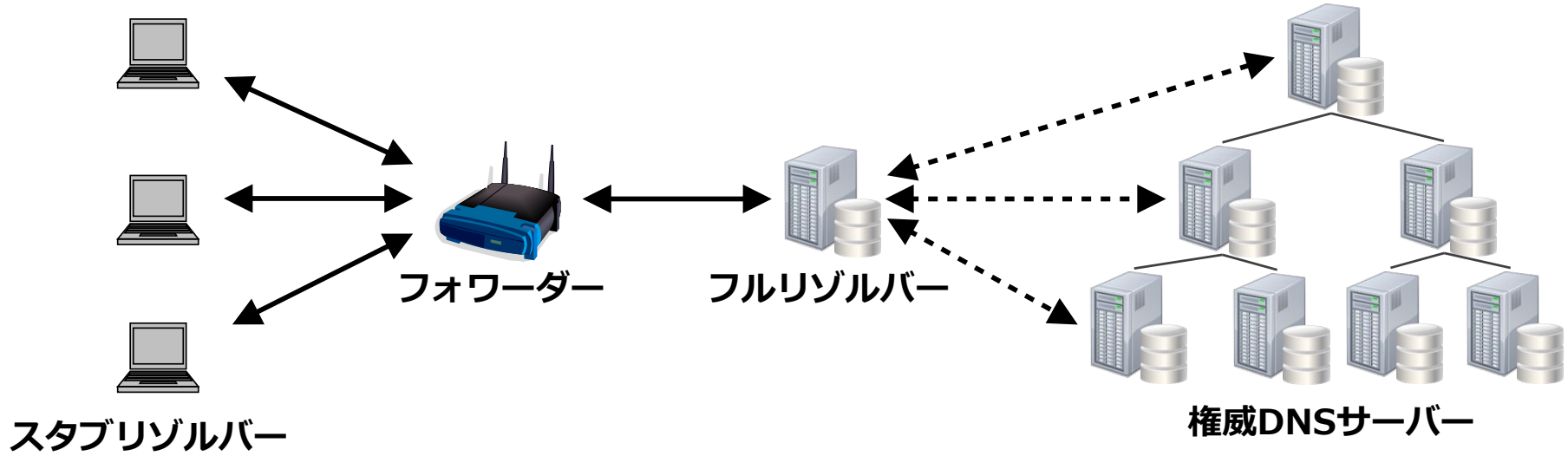
本セミナーの内容

- 権威DNSサーバーを狙った攻撃の影響範囲
- ランダムサブドメイン攻撃の概要
- 権威DNSサーバーの可用性を高めるためのポイント
- 運用担当者・責任者のみなさまへ

権威DNSサーバーを狙った攻撃の影響範囲

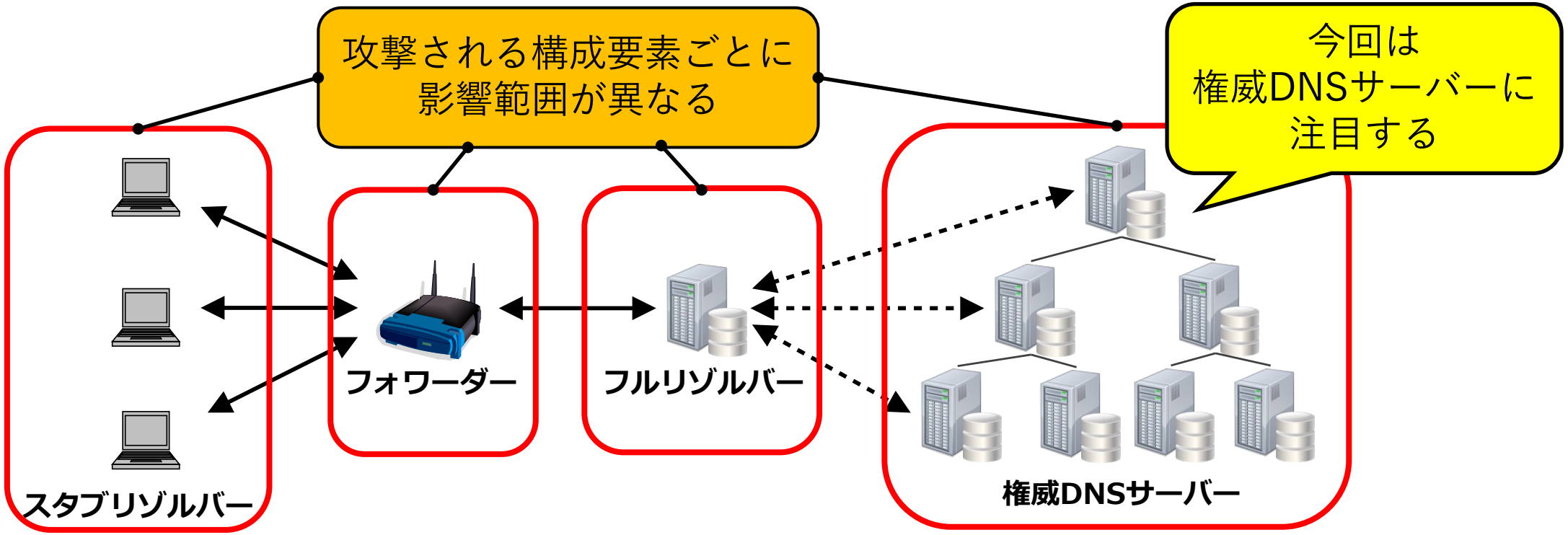
DNSの構成要素

- DNSは、4種類の構成要素で形作られている
  - スタブリゾルバー・フォワーダー・フルリゾルバー・権威DNSサーバー
  - フォワーダーが存在しない場合もある



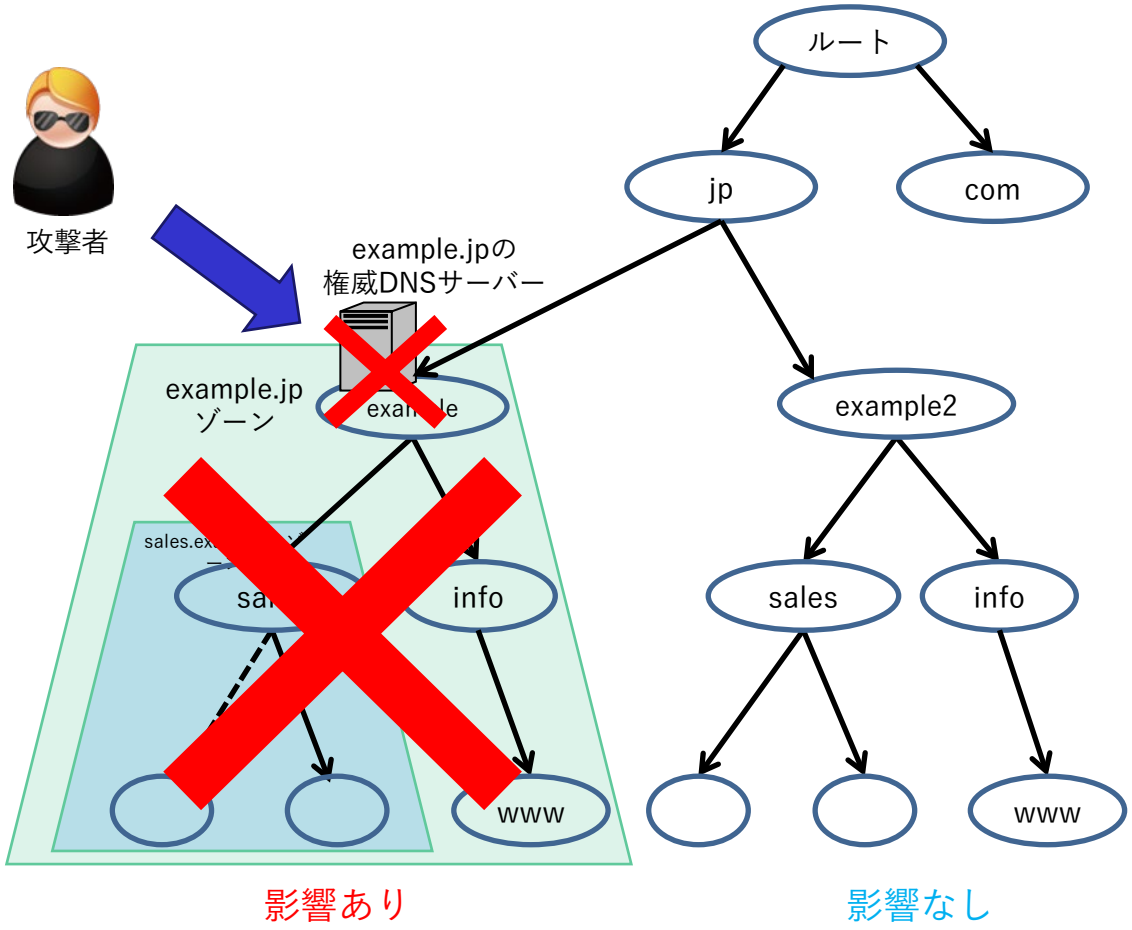
攻撃を受けた場合の影響範囲

- DNSが攻撃されてサービスに影響が及んだ場合、攻撃される構成要素ごとに、その範囲が異なる



権威DNSサーバーの影響範囲（1/2）

- 権威DNSサーバーが攻撃されてサービスに影響が及んだ場合、その権威DNSサーバーが管理するすべてのゾーンに影響が及ぶ
- かつ、そのゾーンから委任されているすべてのゾーンにも影響が及ぶ



権威DNSサーバーの影響範囲（2/2）

- かつ、権威DNSサーバーの影響は、対象となるゾーンのすべての利用者に及ぶ

構成要素	攻撃を受けた場合の影響範囲
スタブリゾルバー	その機器の利用者
フォワーダー	そのフォワーダーを使っているローカルネットワークの利用者
フルリゾルバー	そのフルリゾルバーを使っている組織・ISPの利用者
権威DNSサーバー	その権威DNSサーバーが管理するゾーンと、 そのゾーンから委任されているゾーンを使っているすべての利用者

権威DNSサーバーは他の構成要素と比べて影響範囲が広いため、
より高い可用性が必要になる

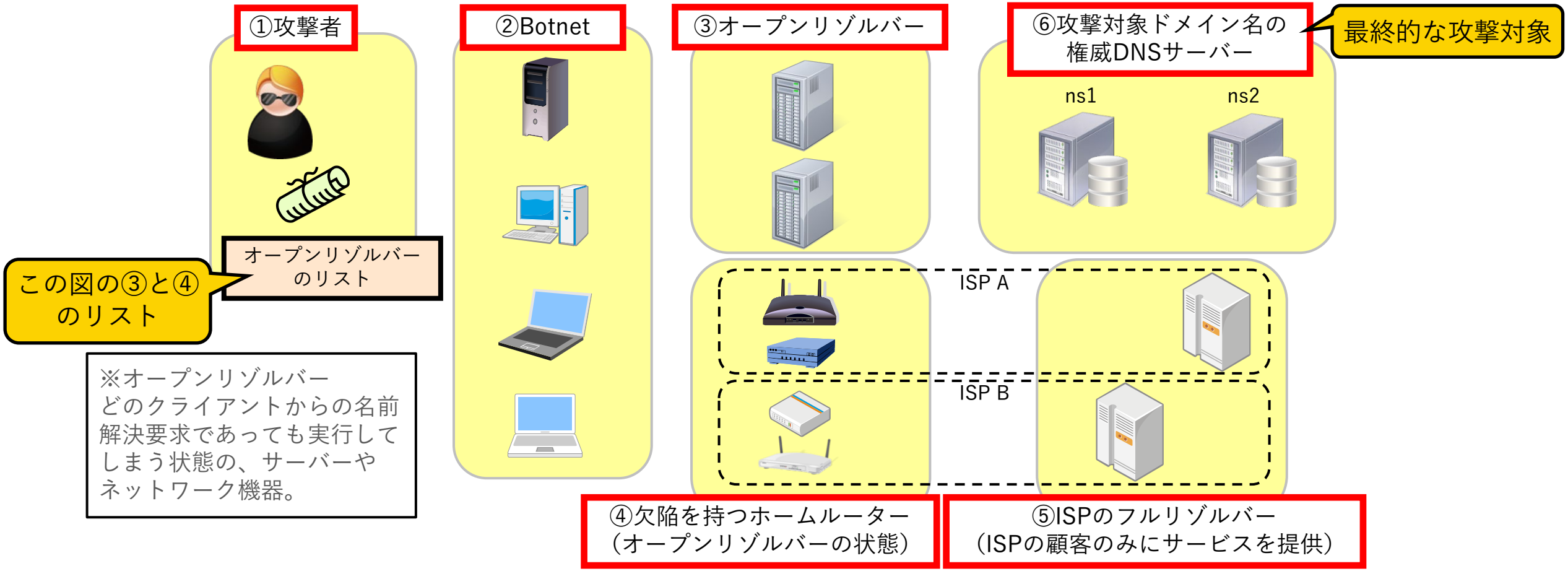
※可用性：システムが継続して稼働できる能力。

ランダムサブドメイン攻撃の概要

ランダムサブドメイン攻撃とは？

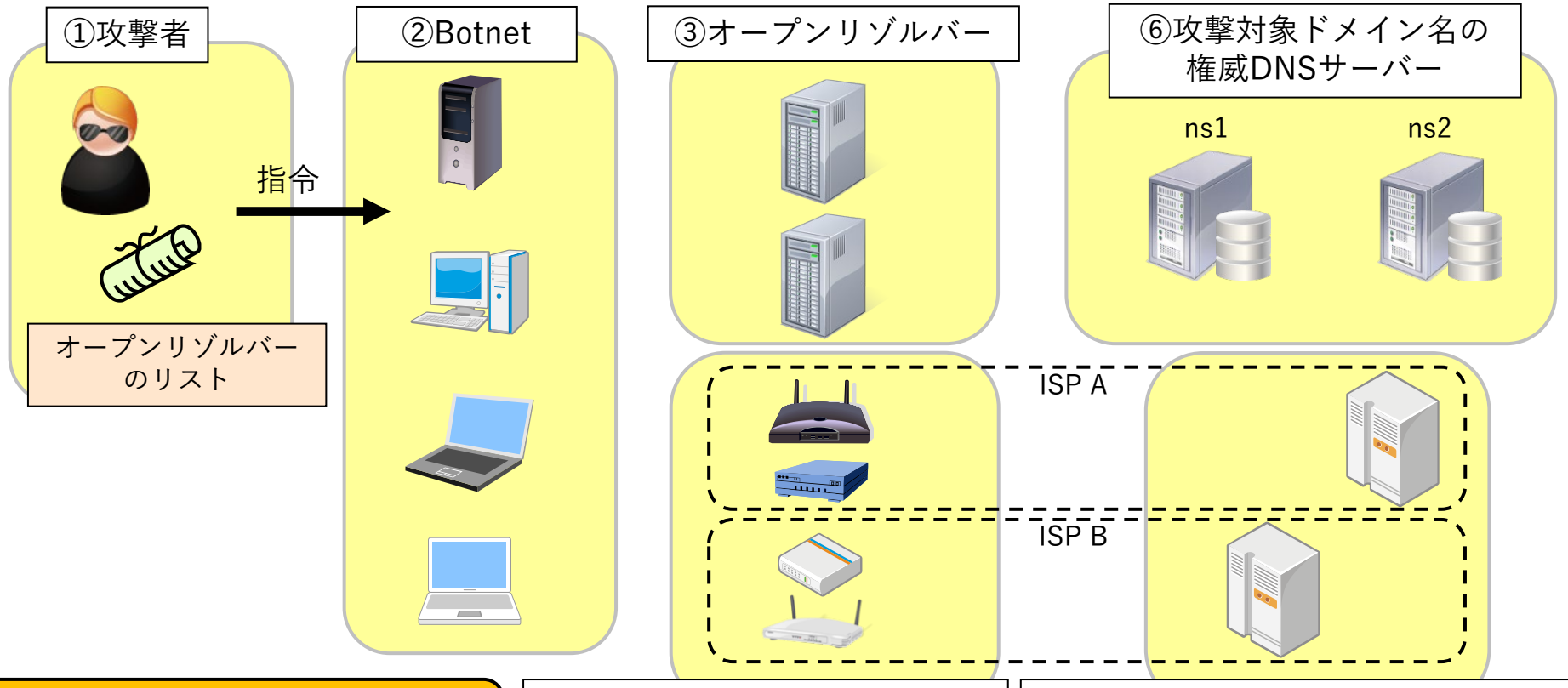
- 攻撃対象のドメイン名の権威DNSサーバーを過負荷にしてサービス不能にする、DDoS攻撃の手法
  - 攻撃の特徴から、DNS水責め攻撃とも呼ばれる
- DNSの問い合わせを使って攻撃する（以降で説明）
- 攻撃の規模はさまざま（数千～数十万qps程度）
  - 100万qpsを超えた事例も報告されている

ランダムサブドメイン攻撃の仕組み①



登場人物は6種類

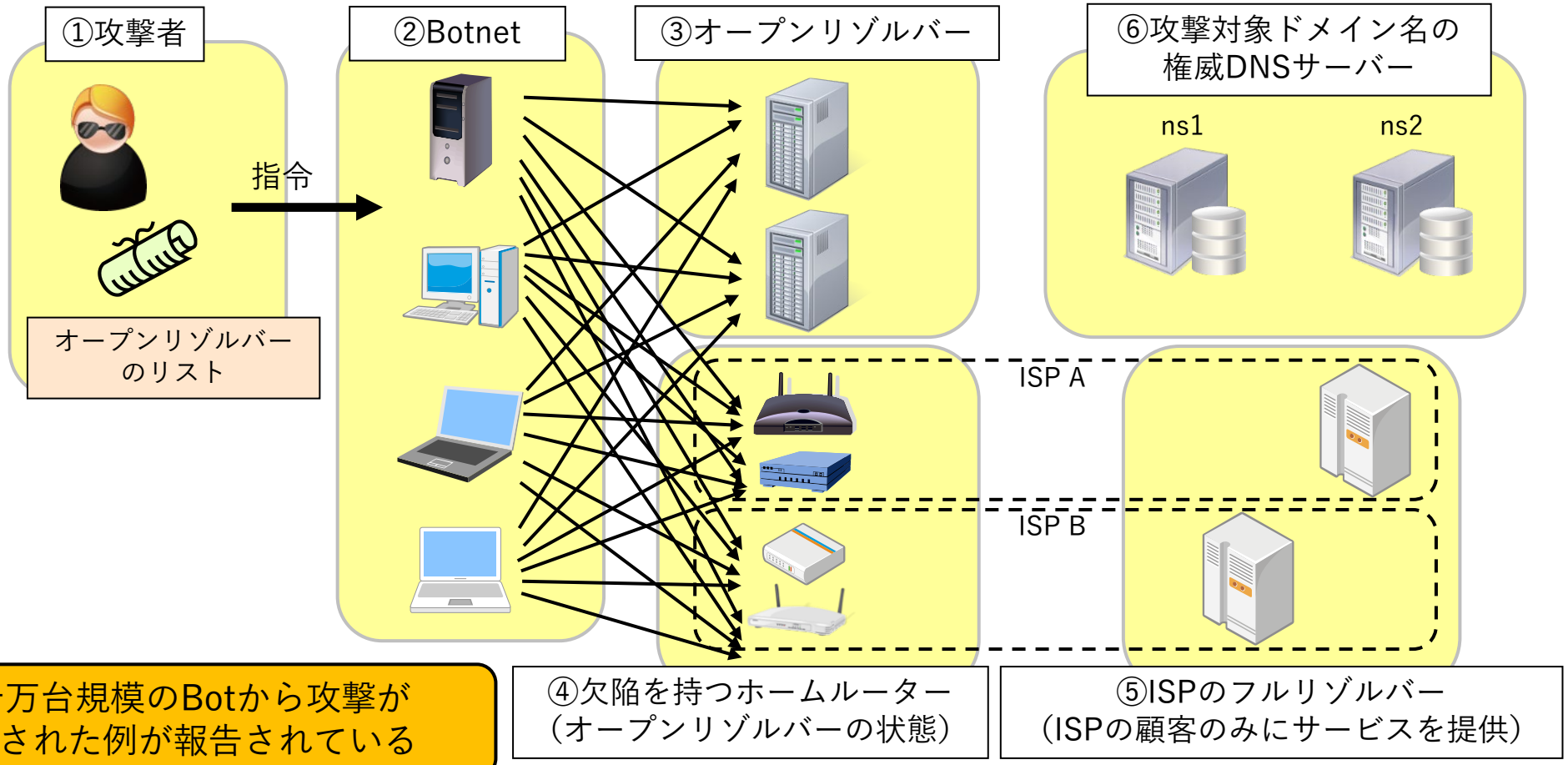
ランダムサブドメイン攻撃の仕組み②



攻撃対象がexample.jpである場合、
(random).example.jpを問い合わせ名に指定

攻撃者がBotnetに、リストにあるオープンリゾルバーに対して
(random).攻撃対象ドメイン名をDNS問い合わせするように指令を出す

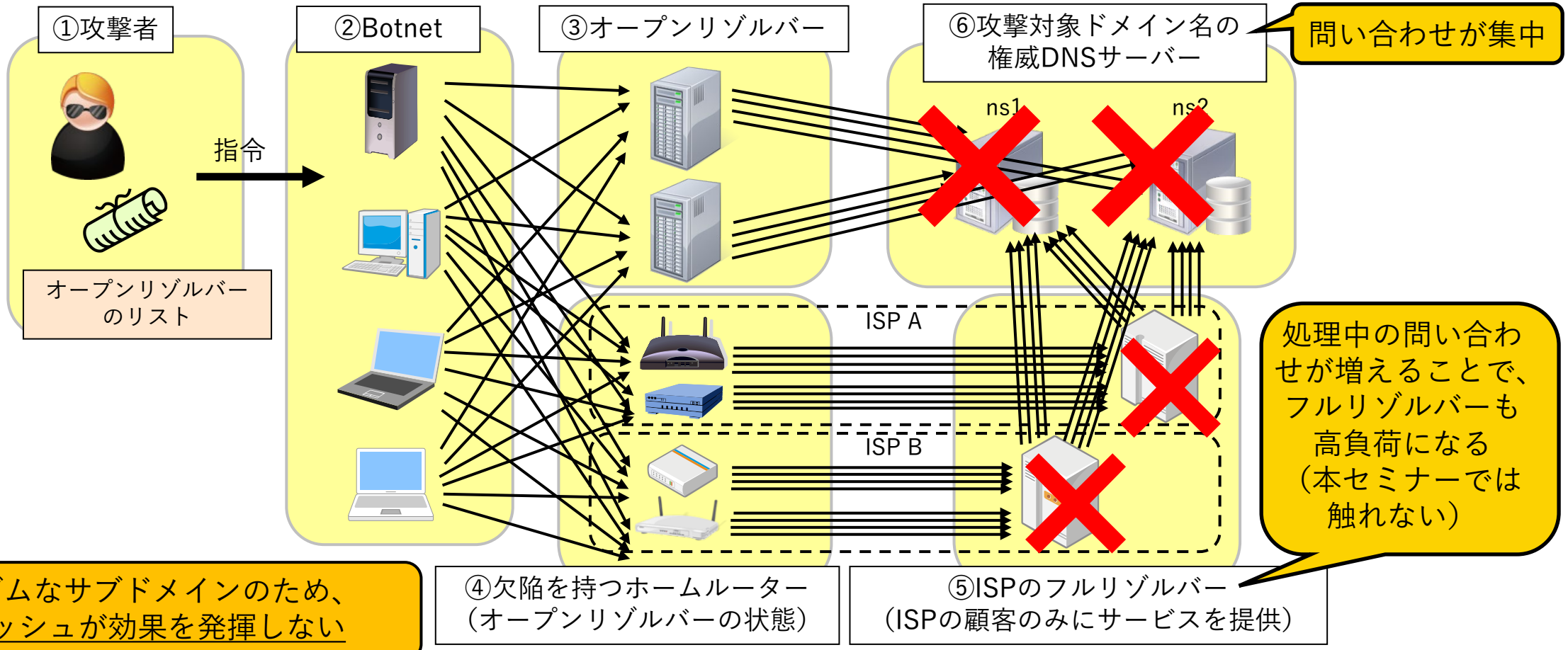
ランダムサブドメイン攻撃の仕組み③



数十万台規模のBotから攻撃が実施された例が報告されている

Botnetを構成する各機器（Bot）が、
リストに掲載されたオープンリゾルバーに問い合わせを送る

ランダムサブドメイン攻撃の仕組み④



ランダムなサブドメインのため、キャッシュが効果を発揮しない

問い合わせ名にランダムなサブドメインが付加されているため、攻撃対象の権威DNSサーバーに問い合わせが毎回送られ、過負荷になる

過去の流行と再活発化

- 2014年から2015年にかけ、世界的に流行
  - 当時の攻撃対象：中国語圏のECサイト・ニュースサイトなど
    - 香港の反政府デモを支持する報道機関が記事を掲載した直後、そのドメイン名が大規模なランダムサブドメイン攻撃を受けた事例が観測
- 2023年3月ごろから、国内外の研究者・専門家・サービス事業者などが、攻撃の再活発化を報告
  - 攻撃によるものと考えられる、複数の被害事例も報告

現在の状況

- 攻撃の目的は現時点で不明
  - 2014年から2015年の流行と異なり、攻撃対象となっているドメイン名の傾向が判然としない
- 本格的な攻撃の前準備や、攻撃の効果測定である可能性も指摘されている

攻撃は現在も散発的に観測され続けており、注意が必要

権威DNSサーバーの
可用性を高めるためのポイント

警察庁とNISCの注意喚起

- 2023年5月1日付で、警察庁サイバー警察局と内閣サイバーセキュリティセンター（NISC）が連名で、DDoS攻撃に関する注意喚起を公開

DDoS攻撃への対策について（概要）
<https://www.npa.go.jp/bureau/cyber/pdf/20230501gaiyo.pdf>
<https://www.nisc.go.jp/pdf/press/20230501NISC_gaiyou.pdf>

DDoS攻撃への対策について
<https://www.npa.go.jp/bureau/cyber/pdf/20230501.pdf>
<https://www.nisc.go.jp/pdf/press/20230501NISC_press.pdf>

注意喚起の内容

- DDoS攻撃の状況とリスク軽減に向けた対策が解説されている
- 被害を想定した対策として、システムの重要度に基づいた、サービスの選別が挙げられている（以下に引用）

> **2　DDoS 攻撃による被害を想定した対策**
>
> **①　システムの重要度に基づく選別と分離**
>
> コストをかけてでも守る必要のあるサービスと、一定期間のダウンタイムを許容できるサービスを選別することで、それぞれの対応方針を策定するとともに、重要性に応じてシステムを分離することが可能か確認し、事業継続に重要なシステムは狙われやすいシステムとネットワークを分離することも検討する。

権威DNSサーバーの重要性

- 権威DNSサーバーは「コストをかけてでも守る必要のあるサービス」の一つであると言える
  - 権威DNSサーバーのサービス停止は、サービスの提供における致命的な機会損失につながる
    - 顧客や閲覧者がWebサイトを訪問できなくなる
- 可用性を高めるためのポイントは？

ポイント①：サーバーの強化・分散化

- サーバーの台数・拠点数の確保
  - サービスするIPアドレスを増やす（NS数を増やす）
  - 同じIPアドレスで複数のサーバーを動作させる
    - ロードバランサーや、BGPによるIP Anycastなどの導入
  - 必要に応じた、ネットワーク環境の強化
- 外部DNSサービスの利用
  - 高負荷に耐えるマネージドDNSサービスの導入
  - 複数のマネージドDNSサービスの併用

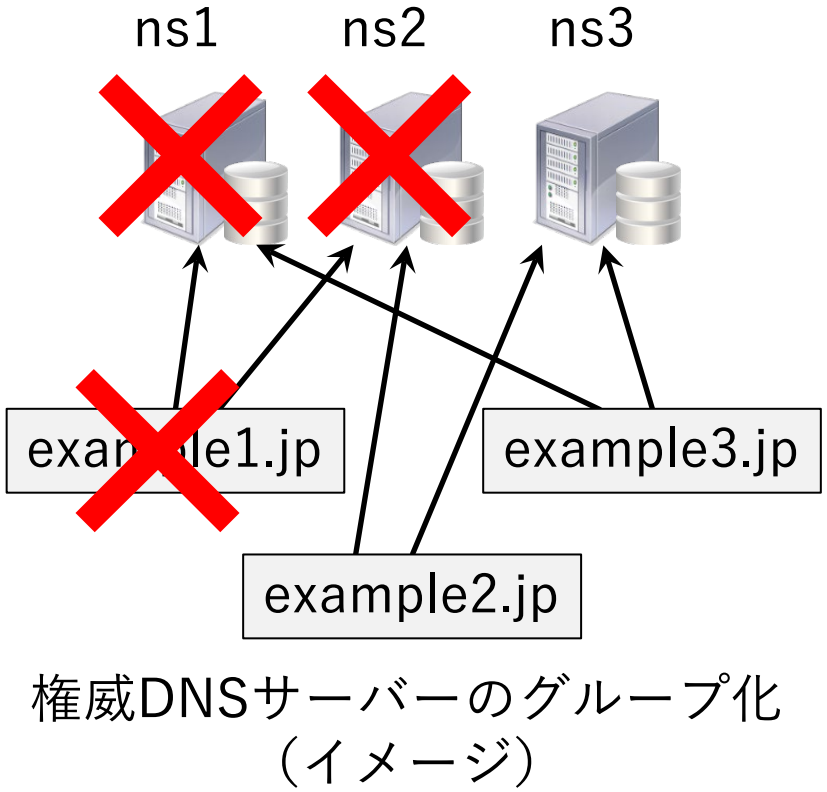
サーバーの強化・分散化とコストの関係

- サーバーの台数・拠点数の確保や外部サービスの利用には、一定のコストがかかる
  - 機材・工数・回線・外部DNSサービスの使用料など
- Webサービスなどと比べ、DNSにかかるコストは忘れられがちである
  - DNSは守る必要のあるサービスであり、コストをかけるべき
    - …ではあるが、無限にはコストをかけられない

以降で、強化・分散化とコストのバランスを図る運用方法の例を二つ紹介する

ポイント②：サーバーのグループ化

- 収容するドメイン名を分散して、権威DNSサーバーの全断を回避
  - 攻撃の巻き添えによるサービス停止リスクを低減



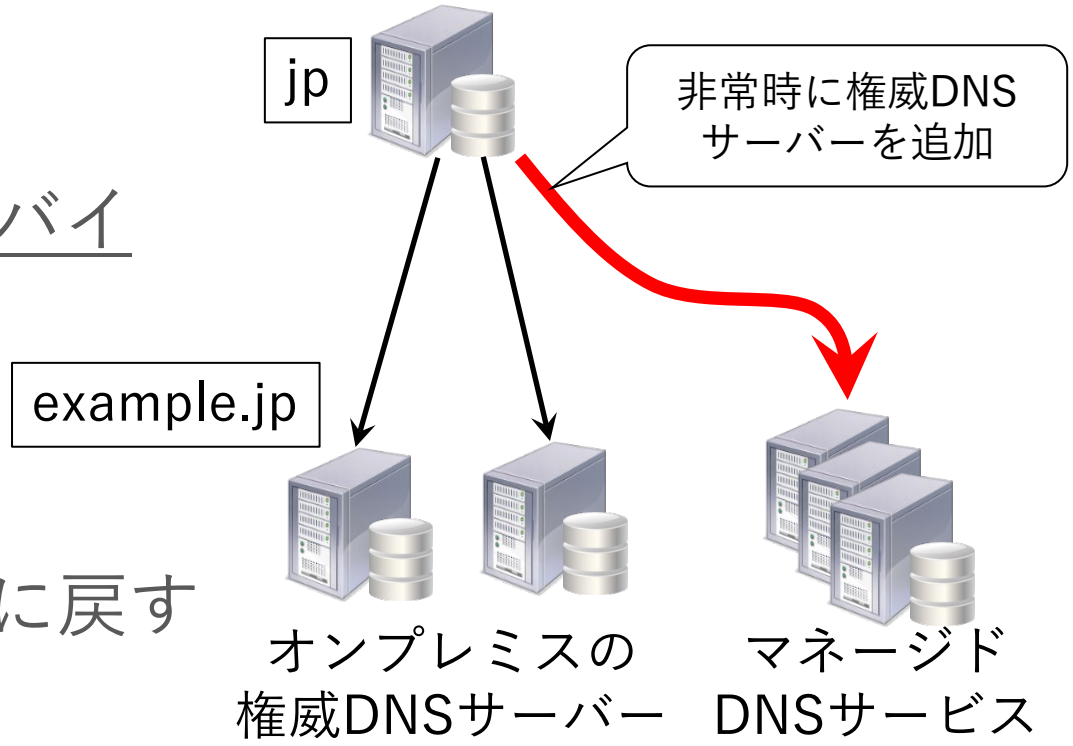
権威DNSサーバーのグループ化（イメージ）

グループ1：ns1+ns2
グループ2：ns2+ns3
グループ3：ns3+ns1

この例では、example1.jpが攻撃されて権威DNSサーバーが全断しても、example2.jpとexample3.jpはサービスを継続できる

ポイント③：状況に応じた柔軟な運用

- 状況に応じ、権威DNSサーバーを追加・削除
  - 平常時（低負荷時）
    - マネージドDNSサービスをスタンバイ
  - 非常時（高負荷時）
    - マネージドDNSサービスを追加
    - 平常に戻った時点で、スタンバイに戻す



従量課金のマネージドDNSサービスをフレキシブルに活用

運用担当者・責任者のみなさまへ

運用担当者・責任者のみなさまへ

- 権威DNSサーバーはコストをかけてでも守る必要のあるサービスの一つであり、より高い可用性が必要になる
- 権威DNSサーバーを適切に運用することで、可用性を高めることができる

常日頃から権威DNSサーバーに気を配り、守ることは、
サービスの安定運用のための必要条件である

権威DNSサーバーを守りましょう！