GMO INTERNET

権威サーバに対する攻撃と対策

Internet Week 2017
2017/11/30
GMOインターネット株式会社
永井祐弥

GMO INTERNET

目次

- 自己紹介
- 権威DNSサーバへの攻撃の種類
- 権威DNSサーバへの攻撃の状況
- 対策を考える
- まとめ

自己紹介

■ 名前

永井　祐弥（ながい　ゆうや）

■ 所属

GMOインターネット株式会社
システム本部 インフラサービス開発部

■ 担当

2012年にGMOインターネット株式会社へ入社。
お名前.com、ConoHa、Z.comのDNSや、
GMOインターネットグループ会社でレジストリシステムのDNSなど、
DNS関連サービスの開発、運用を担当

権威DNSサーバへの攻撃の種類

攻撃の分類 (1/3)

本日お話する内容

- DoS(サービス拒否)、DDoS(分散サービス拒否)攻撃
  - 攻撃者が権威DNSサーバに対して直接的、又は間接的にサービスを機能停止させる攻撃手法
  - 最終的にエンドユーザの名前解決が失敗すればこの攻撃は成立する
  - DoS/DDoS攻撃にはいくつかの攻撃手法が存在する
    - ボリューム型攻撃
      - 主にネットワーク層（L3）を狙い、パケットを大量に送信し帯域幅を圧迫させる攻撃
    - 状態枯渇攻撃
      - 主にトランスポート層（L4）を狙い、パケットを大量に送信しシステムリソースを枯渇させる攻撃
    - アプリケーション層攻撃
      - 主にアプリケーション層（L7）を狙い、ソフトウェアの脆弱性を利用しサービスを機能停止させたり、プロトコルの欠陥を利用してレスポンスデータを反射させるなど様々な攻撃手法が存在する

攻撃の分類 (2/3)

- スプーフィング(なりすまし)攻撃
  - 攻撃者がリゾルバに対して直接的に名前解決を偽装する攻撃手法
  - エンドユーザが偽装された応答を受け取ると様々な影響を受ける
    - 不正なサーバへの誘導（Web、メールなど）
    - 誘導先サーバでの情報奪取（セッションデータ、個人情報など）
  - スプーフィング攻撃にはいくつかの攻撃手法が存在する
    - 正常、又は異常なパケットを大量に送信し偽造データを挿入させる
    - プロトコルの脆弱性を利用し偽造データを挿入させる
    - ソフトウェアの脆弱性を利用し偽造データを挿入させる

攻撃の分類 (3/3)

- ドメイン名ハイジャック(乗っ取り)
  - 攻撃者がDNSホスティングサービスや、レジストリ、或いはレジストラに対して不正なアクセスを行いDNSレコードを改ざんする攻撃手法
    - 不正利用を目的として期限切れドメイン名を登録する行為や、同一サービス上のサブドメイン名を登録する行為もドメイン名ハイジャックに含まれる
  - スプーフィング攻撃と同様にエンドユーザが影響を受けるほか、ドメイン名登録者も深刻な影響を受ける恐れがある
  - ドメイン名ハイジャックにはいくつかの攻撃手法が存在する
    - ドメイン名登録者になりすまして申請を行い不正データを登録させる
    - サービスの脆弱性を利用し不正データを登録させる
    - サーバやネットワークに不正侵入し、データの改ざんなどの不正行為を行う

代表的な攻撃の種類 (1/2)

- DNS水責め攻撃
  - ボットネットを利用し、キャッシュDNSサーバに対して攻撃対象ドメイン名のランダムなサブドメイン名を大量に名前解決させるDDoS攻撃
  - 権威DNSサーバ、キャッシュDNSサーバ共にシステムリソースを枯渇させられたり、帯域幅が圧迫される恐れがあり、非常に厄介
- DNSリフレクター攻撃（DNSアンプ攻撃）
  - スプーフィング攻撃を利用したDDoS攻撃
  - 送信元を攻撃対象となるIPアドレスになりすますことでDNSサーバからの応答がなりすましたIPアドレス宛に返る
  - DNSサーバがDDoS攻撃の踏み台となるため、未対策のオープンリゾルバでは非常に深刻な問題となっている

代表的な攻撃の種類 (2/2)

- DNSキャッシュポイズニング（毒入れ）攻撃
  - リゾルバのキャッシュ汚染を目的としたスプーフィング攻撃
  - 2008年にカミンスキー氏やミューラー氏が
    キャッシュポイズニングの効率的な手法を発表
  - 2014年にはNSレコードを対象とした委任/移転通知インジェクションについて国内でも熱い議論がありました☺
- DNSトンネリング
  - 不正通信経路にDNSを利用するもの（DNSの攻撃ではない）
  - 最終的にエンドユーザへの直接の影響はない
  - 遠隔操作ウイルスや、マルウェアなど悪意あるプログラムが不正通信にDNSを利用するため、検知、ブロックしにくい傾向がある

権威DNSサーバへの攻撃の状況

最近の出来事

- DNSへの攻撃
  - 2017年
    - 3月 Godaddyの権威DNSサーバにDDoS攻撃があり6時間のサービス停止
  - 2016年
    - 10月 Dynの権威DNSサーバに620GbpsのDDoS攻撃が発生
    - 8月 さくらインターネットの権威DNSサーバにDDoS攻撃が発生
- DNS以外でもDoS/DDoS攻撃は日常的に発生している
  - 数十Gbps規模のDDoS攻撃はもはや当たり前
  - 闇市場ではDDoS攻撃の代行サービスが流行中
  - 攻撃者の目的は様々

GMOインターネットの状況

- ホスティングサービス（共有サーバ/VPS）へのDDoS攻撃
  - 直近だとほぼ毎週ペース
  - 共有サーバの場合、攻撃対象となるWebサイトを
    権威DNSサーバのクエリログから特定することが難しい
- 仮想通貨サービスへのDDoS攻撃予告
  - 攻撃対象は対象Webサイトのネットワーク全て
  - 他サービスへの影響を考慮し、DNSを含め事前対策の強化
- 権威DNSサーバを狙った攻撃は今年は未観測
  - 昨年のIW2016で発表した調査系のバーストクエリは継続

DDoS攻撃全般

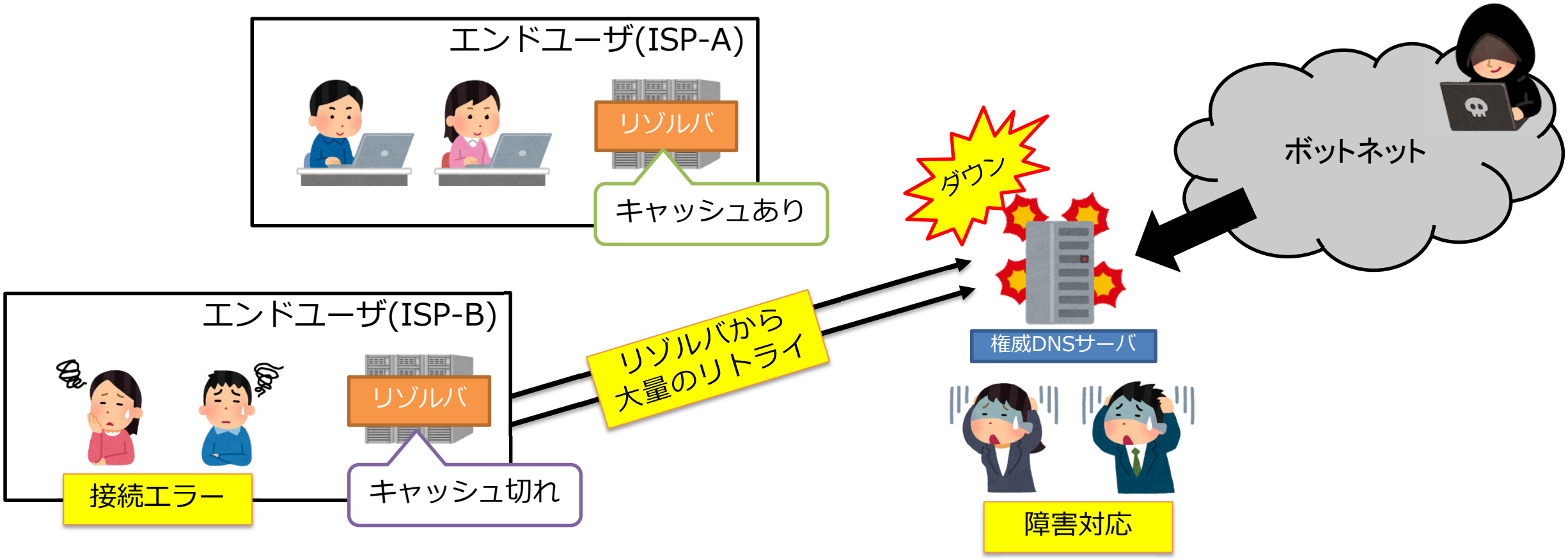
- 妨害を目的としたDDoS攻撃
  - 特定の人物・イベント・Webサイトなどを狙い、Webサイトへのアクセスを妨害する目的としたDDoS攻撃
  - DDoS攻撃は数時間から数日の間継続
- 金銭要求を目的としたDDoS攻撃
  - 短時間のDDoS攻撃と脅迫文が届く
  - 金銭の要求と、支払わない場合は大規模にDDoS攻撃するという内容
- DDoS攻撃の矛先
  - 攻撃者は狙いやすいところから攻撃する
  - 権威DNSサーバに向いた場合の影響を考える

権威DNSサーバの影響

- 権威DNSサーバが機能停止するとどうなるのか？
  - 攻撃を受けた権威DNSサーバで運用されている全てのドメイン名が名前解決に失敗する
  - リゾルバにキャッシュが生存している間は名前解決が可能なため、全体で見ると徐々に失敗していくと考えられる
  - 名前解決の失敗によりエンドユーザは接続エラーが発生する
    - 対象となるドメイン名のWebサイトは表示不可、メールも送信不可
    - APIやオンラインゲームなどのシステムも対象ドメイン名を利用している場合は接続エラーにより通信できなくなる
  - リゾルバから権威DNSサーバに大量のリトライが届く
    - DDoS攻撃が停止した後でも、キャパシティに余裕がないとリトライクエリがDDoS攻撃になりうる

権威DNSサーバの影響

- 権威DNSサーバが機能停止するとどうなるのか？



権威DNSサーバの影響

- 事業的な観点
  - Webサイトが表示されない
    - 障害情報をWebページで告知できない
    - 決済システムやAPIなどをドメイン名で外部提供している場合は当然機能しない
  - メールの送受信が出来ない
    - 障害情報をメールで告知できない
    - お問い合わせメールが届かない
  - 事故の報告
    - 一定の要件を満たす事業者は官公庁に事故の報告が義務付けられている

対策を考える

基本対策その1 ～TTL値の見直し～

- TTL値は長すぎても短すぎても微妙

```
example.tokyo.    10    IN    A    192.0.2.123
```

	短いTTL値	長いTTL値
障害発生時	すぐに名前解決出来なくなる	徐々に名前解決出来なくなる
DNSレコードの更新	体感的に反映が早い	体感的に反映が遅い
権威DNSサーバへのクエリ数	多くなる	少なくなる

- 障害回復までのシナリオを検討すること
  - 名前解決が失敗してから、障害が回復するまでの時間
  - DNSレコードの更新に必要な本当の時間
  - CDNなどで短いTTL値を設定しているのはDNSレコードの更新を含めてシステムが自動化されているため

基本対策その2 ～バックアップを用意～

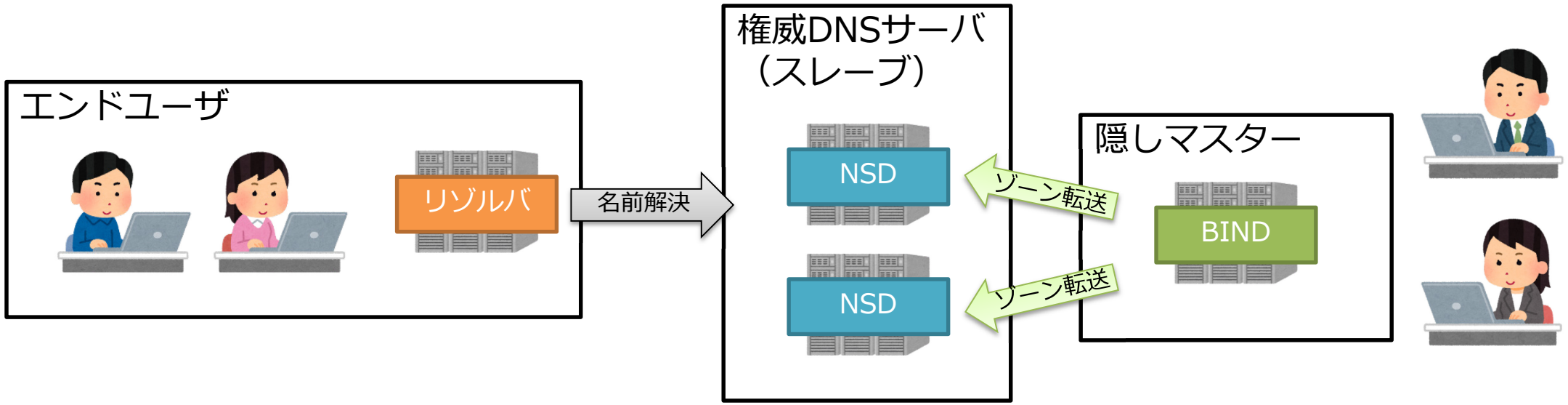
- ゾーンファイルのバックアップは必ず用意する
  - 緊急時にゾーンファイルが無くて何も出来ないのは避ける
  - 緊急時でもアクセス可能な場所に保管する（稼働中のサーバはNG）
- マスター/スレーブ構成の場合はマスターのサーバを隠避する
  - 隠しマスター（Hidden Master）はスレーブへのゾーン転送のみ行い、外部には公開しない
- 緊急時の手順書を用意する
  - DNSレコードの変更方法
  - 権威DNSサーバの変更方法

高負荷対策その1 ～パフォーマンスの強化～

- OS、アプリケーションの設定をチューニングする
  - デフォルト値は低く設定されていることが多いので見直しが必要
    - システムリソースを浪費しすぎないための制限
  - 見るべき箇所（詳細を列挙すると時間が不足するため割愛...）
    - ソケットのバッファサイズ
    - セッションのテーブルサイズ（数）
    - ファイルディスクリプタの制限
    - マルチスレッドの各種設定値
    - ゾーンファイルチェックの無効化（他のチェック方法を検討する）
    - クエリログの無効化（統計情報を使用するなど他の方法を検討する）
    - RRL（Response Rate Limiting）の導入

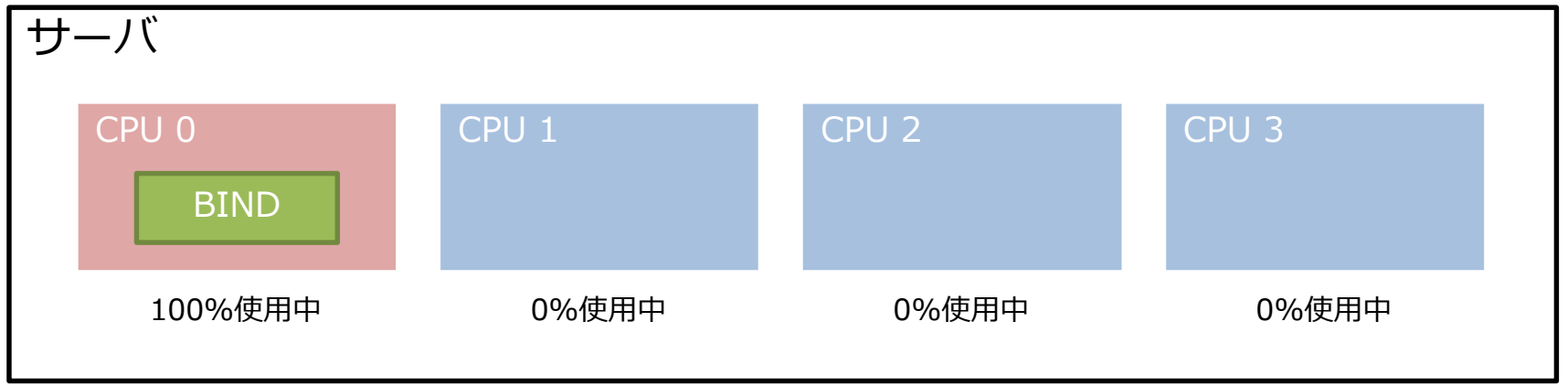
高負荷対策その2 ～パフォーマンスの強化～

- アプリケーションの構成変更を検討する
  - BINDやPowerDNS、djbdnsはパフォーマンスが低い
  - NSDやKnotDNSはパフォーマンスが高い
  - 隠しマスター/スレーブの構成で、スレーブをパフォーマンスが高い NSD/KnotDNSといったアプリケーションで住み分けをすると良い



高負荷対策その3 ～パフォーマンスの強化～

- サーバのスペックを増強する
  - 権威DNSサーバのクエリ処理量はほぼCPUのクロック数に依存する
    - コア数を増やしても、アプリケーション次第では処理量が向上しない場合がある
    - プロセスを2つ起動した方が処理量が向上することもある



高負荷対策その4 ～パフォーマンスの強化～

- ロードバランサを導入する
  - OS、アプリケーションのチューニング同様にデフォルト値には注意する
    - セッションのテーブルサイズ
    - ヘルスチェック
  - クエリ処理量とレスポンスの帯域幅を考慮する
    - クエリ処理量と帯域幅には余裕を持たせる
    - 1リクエストが32バイト、1レスポンスが128バイトで秒間10万クエリの場合
      - 32 byte × 8 bit × 100,000 qps = 24Mbps
      - 128 byte × 8 bit × 100,000 qps = 98Mbps

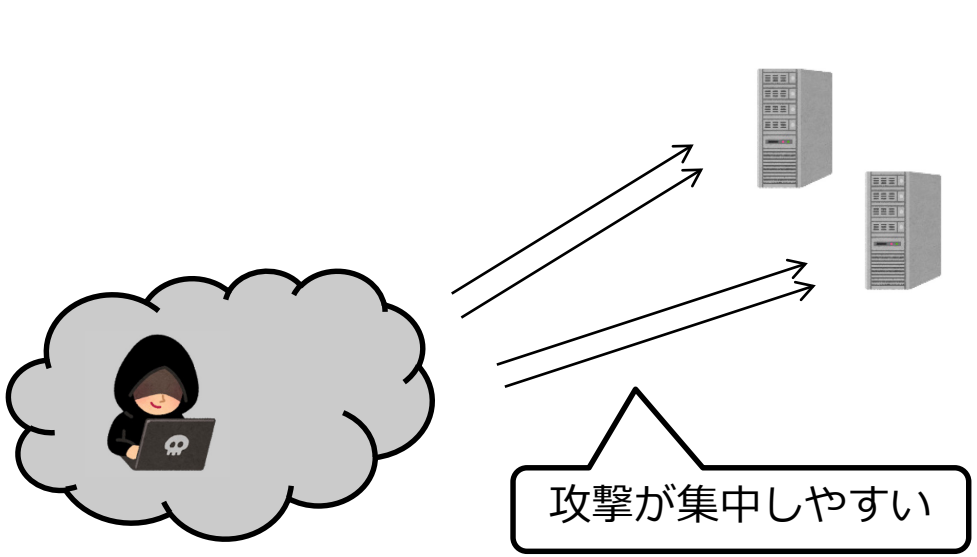
高負荷対策その5 ～パフォーマンスの強化～

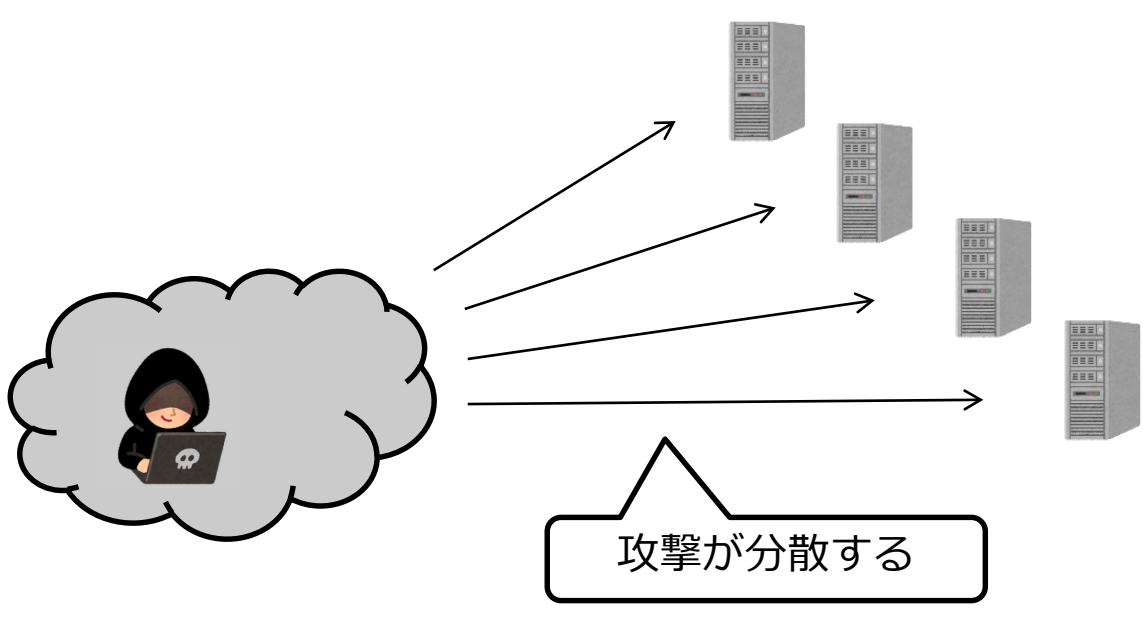
- 帯域幅を増強する
  - DDoS攻撃の場合トラフィックが10Gbpsを超えることが多い
  - 100Mbpsでは小さなDoS/DDoS攻撃でも一発KOしてしまうため最低でも1Gbpsは必須、可能であれば10Gbps以上あるとよい

- ベンチマークを計測する
  - これらの高負荷対策を行った上で、ベンチマークを計測すること
    - queryperf、dnsperf、dnstcpbenchなどのベンチマークツールを使用する
    - ベンチマークツールはローカルで実行する
      - 可能であれば、複数クライアントを想定してプライベートネットワーク内で計測すること
  - パラメータの確認や、事前検証、動作確認はしっかり行うこと
    - 本番環境で適用漏れが発生するケースも考えられる

DDoS攻撃対策その1 ～権威DNSサーバの分散～

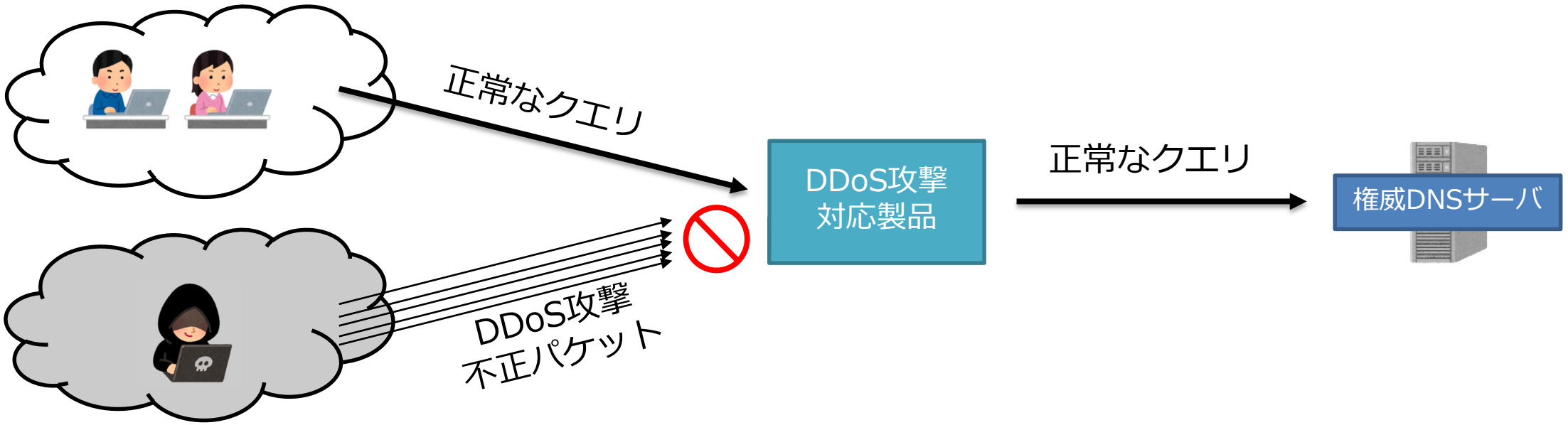
- 権威DNSサーバは複数用意する
  - 攻撃を分散させる事で生存率を高める
    - 分散先はそれぞれ異なるネットワークに設置することが望ましい
    - 複数のNSレコード、NSレコードに対する複数のA/AAAAレコード





DDoS攻撃対策その2 ～DDoS攻撃対応製品～

- DDoS攻撃対応製品、対応サービスを導入する
  - オンプレミス型、クラウドサービス型など、様々な製品が登場している
  - 攻撃を検知するとルータと連動して自動的にブロックすることが可能
  - 上流回線の帯域幅がパンクしない限りは攻撃を防ぐことが出来る

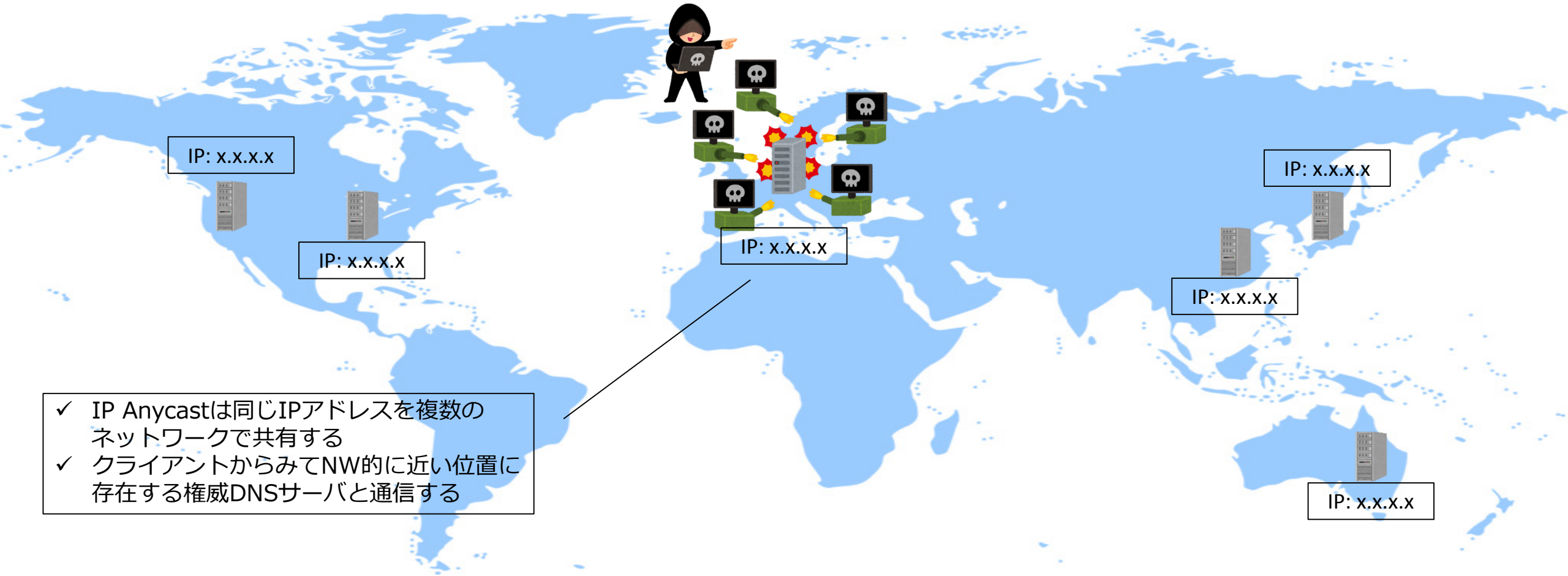


DDoS攻撃対策その3 ～IP Anycast～

- IP Anycastで地域分散化する
  - 同じIPアドレスを複数のネットワークで共有する技術
    - 多数の権威DNSサーバで同じIPアドレスを使用する
    - IP AnycastはRoot Serverを始め、多くのDNSサーバで使用されている
  - クライアント（攻撃者を含む）は自分自身からみてネットワーク的に最も近い位置に存在する権威DNSサーバと通信を行う
    - この特性を活かし、DDoS攻撃の影響範囲を狭めることが可能
    - IP Anycastのノードが多いほど、複数拠点からの攻撃が分散化される

DDoS攻撃対策その3 ～IP Anycast～

- IP Anycastで地域分散化する



- ✓ IP Anycastは同じIPアドレスを複数のネットワークで共有する
- ✓ クライアントからみてNW的に近い位置に存在する権威DNSサーバと通信する

GMOインターネットの対策

- DNS夏日の某日
- GMOインターネットに20Gbps程のDDoS攻撃が発生
  - DDoS攻撃対策製品により無事に防御
  - 前後にさらに数Tbpsの攻撃をほのめかす連絡が来る
- 攻撃シナリオ
  - 攻撃予告日は6日後、時間帯は記載が無く事前にDDoS攻撃を受けた前後の時間帯を想定
  - GMOインターネットのバックボーンのキャパシティを超える大規模攻撃を想定
- 対策状況
  - お名前.com（レンタルDNS）の権威DNSサーバと、
    自社利用の権威DNSサーバはIP Anycastで国内外に地域分散化している
  - 大規模DDoS攻撃が来た場合の対応方法を事前決定
    - 緊急度、重要度に基づき対応順序や対応方法について社内関係者の間で共有

GMOインターネットの対策

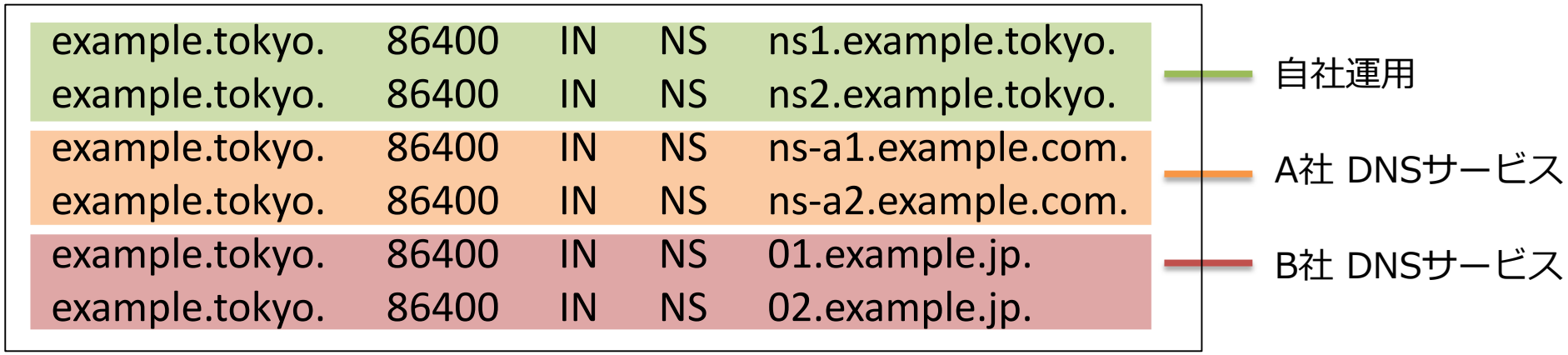
- 事前対策の強化
  - 対応期間が短く物理的な増設は難しい
  - その為、最重要ドメイン名についてはDNSホスティングサービスを契約し、自社運用＋DNSホスティングサービスの構成に変更
  - 隠しマスターについてもGMO以外のネットワークにスタンバイとして配置
    - 緊急時はスタンバイの隠しマスターからゾーンを更新する
- 結果
  - DDoS攻撃は来なかった（一安心）
  - 権威DNSサーバの事前対策はその後継続して利用中

DNSホスティングサービスのススメ

- DNSホスティングサービス
  - DNSホスティングサービス提供事業者が管理・運用する権威DNSサーバ
    - ドメイン名レジストラ、ホスティング事業者、ISPなどが提供
  - 国内外でIP Anycastを導入している所がベスト
    - 国内はレイテンシ重視
    - 海外はDDoS攻撃の吸い込み先
    - さらに、権威DNSサーバがIPv6に対応していることが望ましい
  - DDoS攻撃対応を謳っているDNSホスティングサービス
    - CDN事業者が提供している事が多い
    - お値段もそれなりにします

DNSホスティングサービスのススメ

- DNSホスティングサービスの多様性
  - DNSホスティングサービスの性質上、
    他ドメイン名への攻撃の巻き添えに遭う恐れがある
  - 複数のDNSホスティングサービスを利用することで、
    巻き添えを回避することが出来る



まとめ

- 権威DNSサーバに対する攻撃の種類
  - DoS/DDoS攻撃、スプーフィング攻撃、ドメイン名ハイジャック
- 権威DNSサーバに対する攻撃の状況
  - DDoS攻撃の脅威は年々増加
  - 権威DNSサーバが機能停止した場合の影響
- 対策を考える
  - 基本対策、高負荷対策、DDoS攻撃対策
  - DNSホスティングサービスのススメ

すべての人にインターネット