DNSの可用性と完全性について考える

2015/1/15

JANOG35@静岡

IIJ 其田　学

本セッションの目的

1. キャッシュポイズニング（完全性へのリスク）についての認識の共有

2. 完全性へのリスクを低減する手段としてのDNSSECが与える可用性への影響の共有。

3. そして、皆さんがどうリスク判断するのか、どうして行きたいのか議論

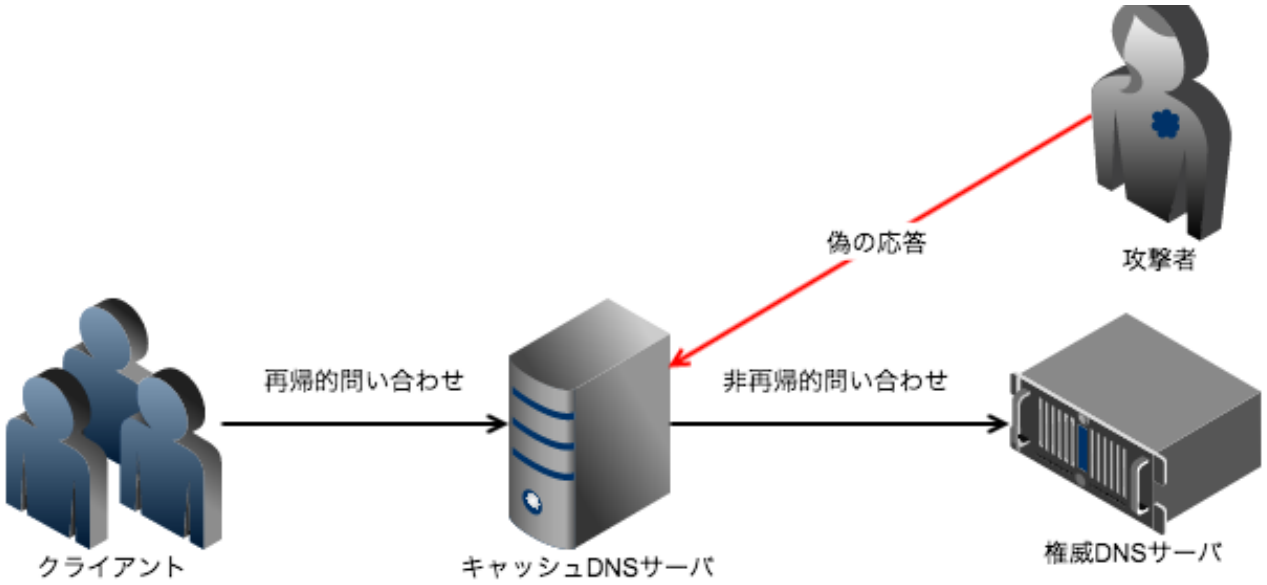
アジェンダ

- キャッシュポイズニングついての認識の共有
- DNSSEC導入の効用、反作用の共有
- 実運用している側からの知見
  - 検証に対応したキャッシュDNS運用から
    - 九州通信ネットワーク株式会社　末松さん
  - 権威DNSサーバのDNSSEC対応から
    - 株式会社インターネットイニシアティブ 山口

キャッシュポイズニングのおさらい

キャッシュポイズニングとは

- 定義
  - キャッシュDNSサーバに偽の情報をキャッシュさせること。



キャッシュポイズニングの問題点

キャッシュDNSサーバを利用している
全てのユーザに偽の応答を返してしまう。

ポイズニングされたドメインへのサービス不能
攻撃、盗聴が可能。

キャッシュポイズニング攻撃の3つの型

1. 偽装したパケットを投げつける。
   - カミンスキー型攻撃
     - DNSプロトコルの脆弱性をついた攻撃
2. IPフラグメントを利用した攻撃
   - 第一フラグメント便乗攻撃
     - IPv6プロトコルの実装バグをついた攻撃
3. 権威DNSサーバのIPを経路ハイジャックする。
   - 不正な経路をBGPで広報して権威DNSサーバを乗っ取る。

キャッシュポイズニング攻撃が出来る理由

- データの完全性を保証していない。
  - 正しいデータか間違ったデータか判別できない
  - そもそもキャッシュポイズニングされてるかどうかすら、分からない状態です。
  - DNSってそういうプロトコルです

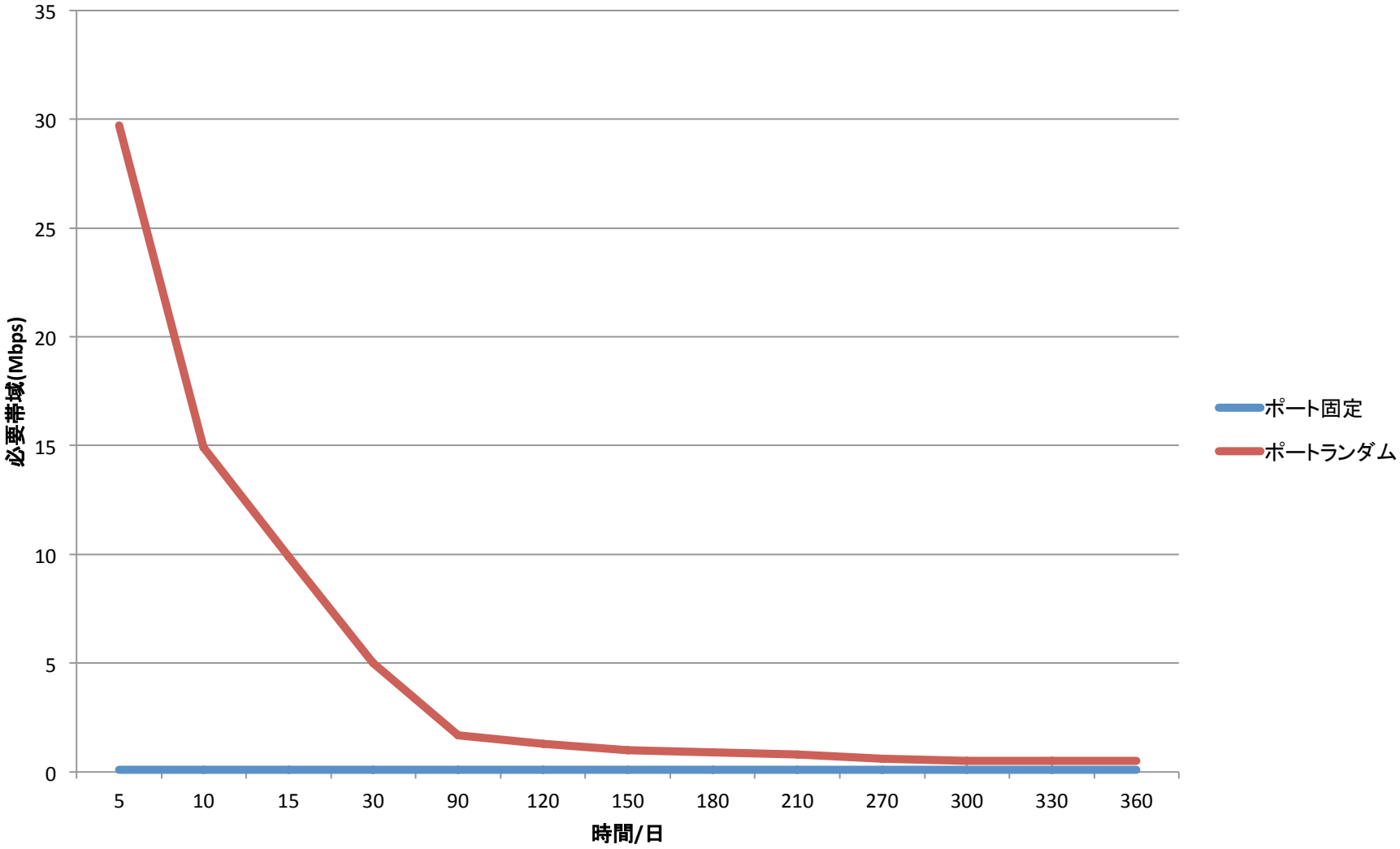
攻撃手法別のリスク

攻撃手法に必要なリソース

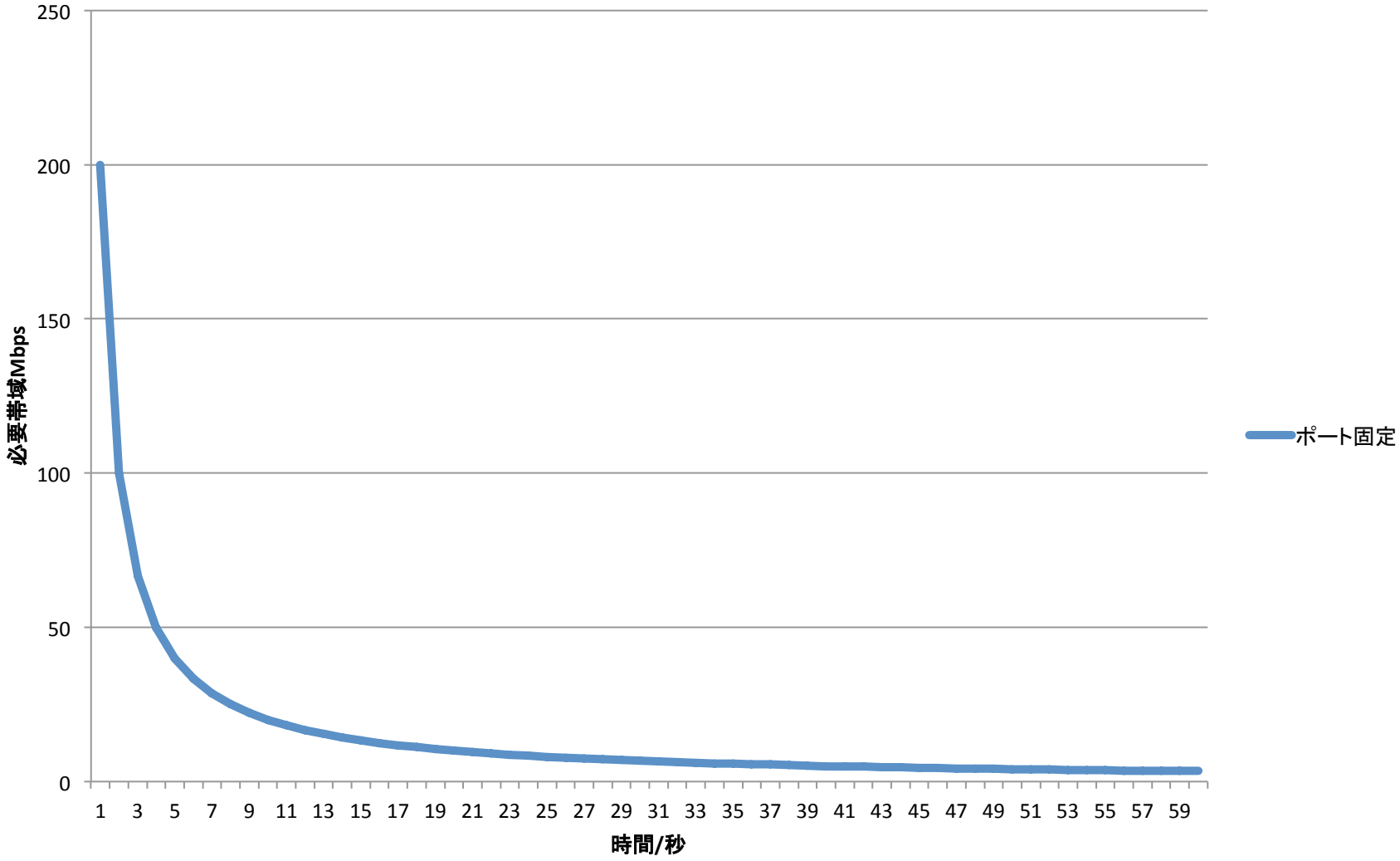
項目	カミンスキー型	第一フラグメント便乗	経路ハイジャック
誰でも実行可能？	YES	YES	No NW設備が必要
ターゲットは自由に選べる？	YES	NO （脆弱性のあるサーバ）	YES
攻撃時間	非常に長い （ポートランダマイズ実施時）	数分程度	一瞬
必要なデータ量	1.5TB~	25MB～	極小

なお、攻撃に必要なリソースはここ数年特に変化していません。

ソースポートランダム時の
カミンスキー型攻撃に対する耐性



第一フラグメント便乗攻撃に対する耐性



DNSSEC導入の効用、反作用の共有

DNSSECの役割

- ワクチンを作る
  ゾーンのDNSSEC対応
  ドメインごとにワクチンができていくイメージ

- ワクチンを打つ（全部のワクチンを打つ）
  キャッシュDNSでの署名検証
  全てのワクチンを一気に打つイメージ

  ワクチンを作るだけでは効果がない。
  ワクチンが無いと、ワクチンが打てない関係

DNSSEC導入による作用

- ドメイン所有者
  - 署名する事で、利用者、キャッシュDNSサーバが検証していれば、完全性を提供できる。

- 名前解決する利用者
  - 署名されているレコードに対して、ポイズニングされた場合、検証に失敗して、ポイズニングされているかどうか分かる。

DNSSEC導入による副作用

- ドメイン所有者
  - qmailを使っているドメインからのメールが届かなくなる事象が発生。（相手が検証していなくても発生）
- 権威DNSサーバ運用者
  - 運用負荷の増大
    - 定期的な電子署名、署名鍵の交換が必要
  - 安全に運用するには、システム構築が必要
    - 構築費用の発生

DNSSEC導入による副作用

- キャッシュDNSサーバ
  - 権威DNSサーバ側の運用ミスによる検証失敗が発生した場合、影響が子ゾーンにまで及ぶ。（主にTLD）
  - また、検証していない場合、問題が発生しない為、現在は検証していないサーバ多いため、キャッシュDNSサーバの障害だと思われる。
    - comcastのNASAの事例等

実運用している側からの知見

- 署名検証しているキャッシュDNS運用から
  - 九州通信ネットワーク株式会社　末松さん
- 権威DNSサーバのDNSSEC運用から
  - IIJ 山口さん（権威DNS運用者の立場で）