リスク軽減と過剰防衛

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

攻撃とか侵入とか踏み台とか

- 何か対策やってくれと言われる
  - 影響軽減
  - パケットフィルタ
  - 怪しい制御装置

ネットワークと利用者

- 一体であれば管理はとっても簡単
  - サービスのポリシ＝ネットワークのポリシ
  - CDNとか家庭とか
- 管理者が別な場合はめんどくさい
  - ISPなんてのは顕著な例
  - 関連する利用者間の調整が必要かもしれない
    - そんなもんだよねっていう共通認識

多様な利用者がいるかも

- 利用者
  - 法人、個人
- 用途
  - サービス、交流、遊び
  - 購買、検索、検証
  - いろいろ

緊急対応と予防対応

- 緊急対応
  - サービスの維持に支障があるなど、緊急の状態
  - 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2版
    - http://www.jaipa.or.jp/other/mtcs/info_110325.html
- 予防対応
  - 実際の対策が悩ましい
  - 正当業務行為だったら大丈夫
    - 無茶しちゃいけない

予防措置

- 現状、素敵な手段が無い
  - ポート毎のパケットフィルタ
  - Rate Limit
- オレ　パケットフィルタ　キライ
  - イケてない
  - 適切な通信権限を渡せてない
  - もっと良い方法があれば嬉しい
  - できるだけ影響範囲を最小限にしたい

サーバ側

- 通信制御を外に出ししたい
  - ネットワークでざっくりした制御
    - 通信許可する範囲とか
  - 細かい制御は手元でやっても良い
- ポリシが増えていく
  - 用途の違うサーバ群

- 利用者（サーバ）の要望によるフィルタリング

攻撃の全体像

- ルータは、パケットの記録は苦手
  - 攻撃は防げてるかもしれないけど
  - 手段としてはNetFlowで別途記録するぐらい

  → フィルタしていると見えなくなるかも
- 至る所にCGNが導入されてくる
  - 不用意にフィルタすると、同じIPアドレスを利用している利用者が一緒にフィルタされちゃうかも

  → 攻撃者と普通のトラヒックが見分け辛くなるかも

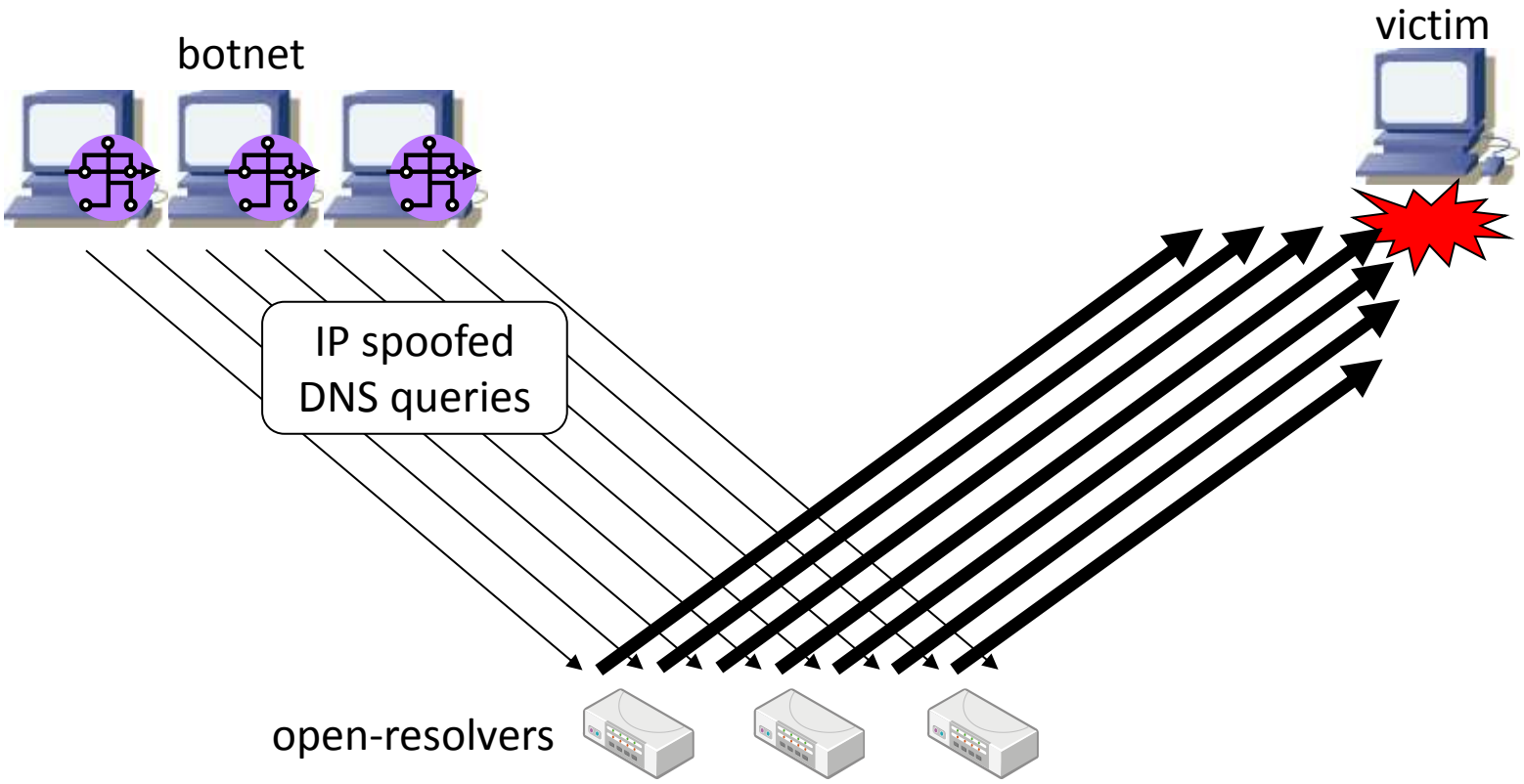
BCP162 - Logging Recommendations

- It is RECOMMENDED as best current practice that Internet-facing servers logging incoming IP addresses from inbound IP traffic also log:
  - The source port number.
  - A timestamp, RECOMMENDED in UTC, accurate to the second, from a traceable time source (e.g., NTP [RFC5905]).
  - The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports.

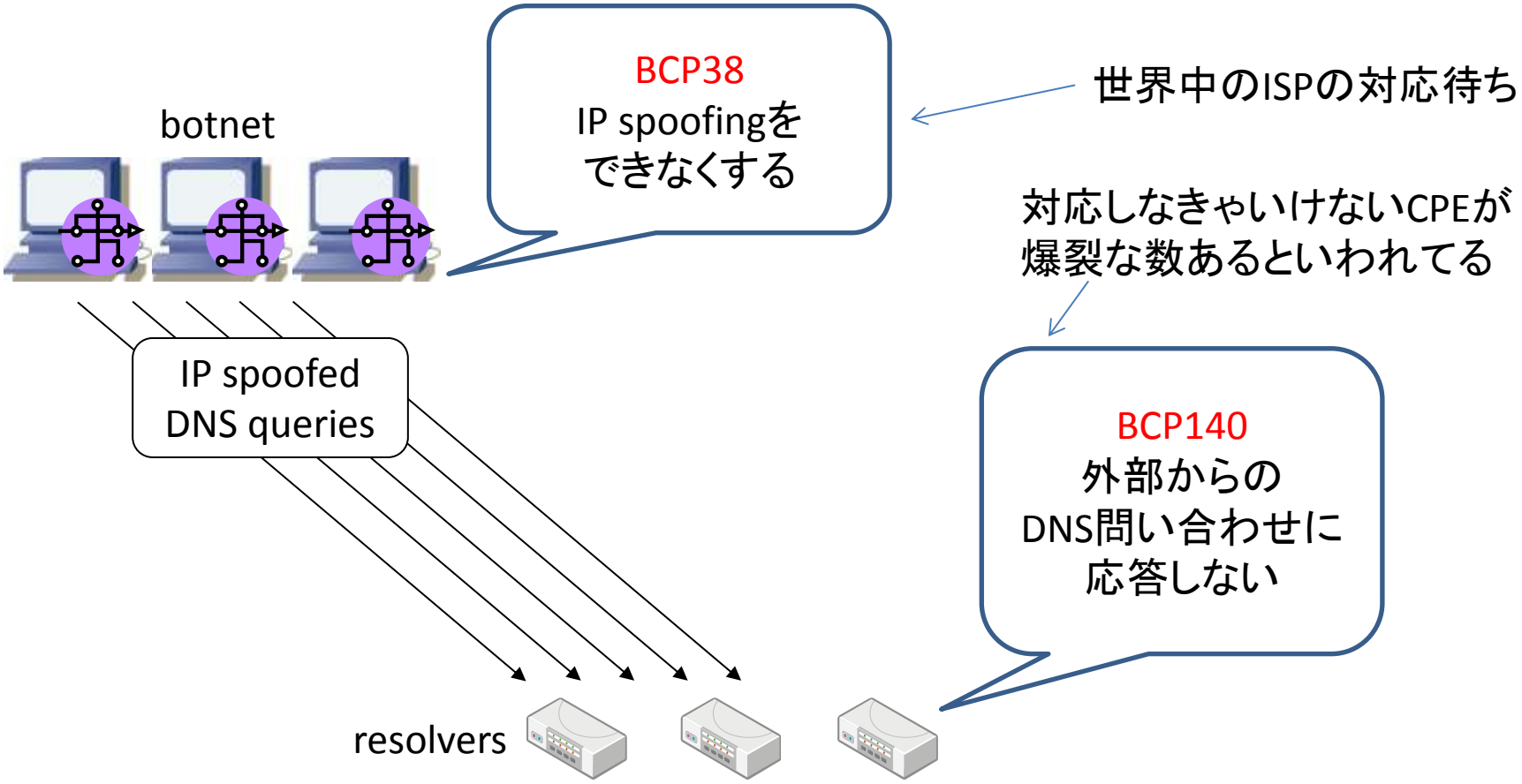
コンシューマ側

- 利用者が何やってるか分からない
  - これからどんな通信が流行るか分からない
    - IPSEC?UDP?新しいプロトコル?
- でも脆弱性が放置される傾向
  - 端末とか
  - CPE

dns amp攻撃



dns amp攻撃対策

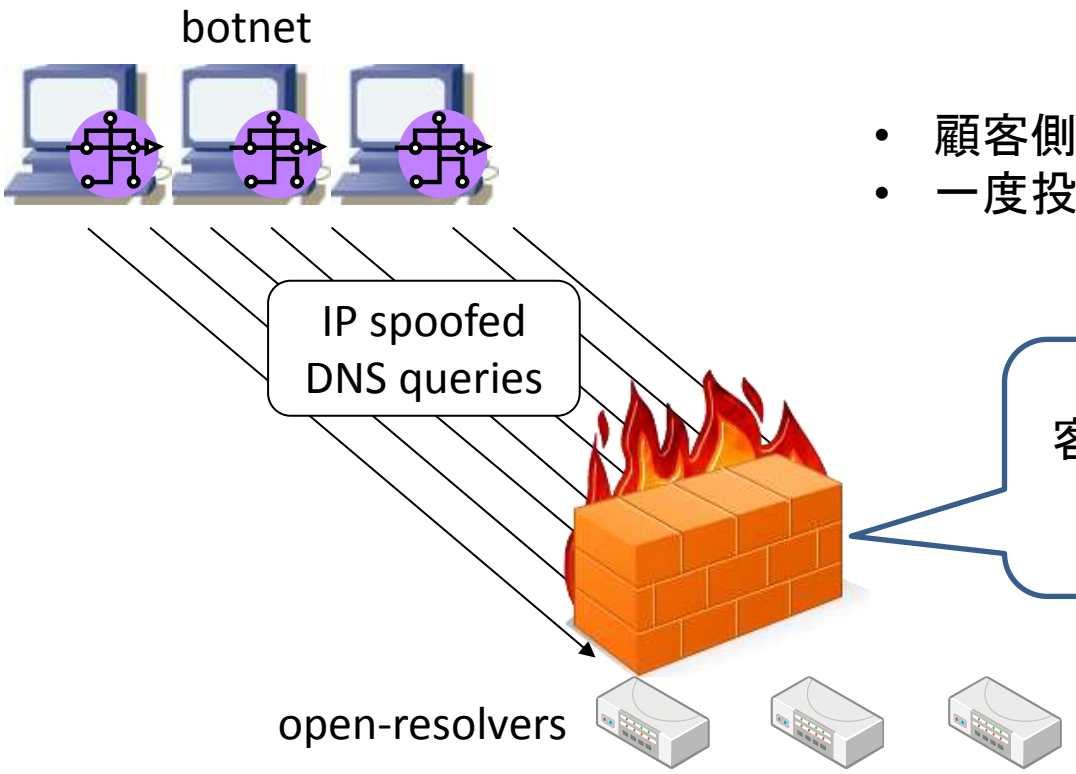

BCP38
IP spoofingを
できなくする
世界中のISPの対応待ち
botnet
対応しなきゃいけないCPEが
爆裂な数あるといわれてる
IP spoofed
DNS queries
BCP140
外部からの
DNS問い合わせに
応答しない
resolvers


Telecom-ISAC Japan
https://www.telecom-isac.jp/news/news20130617.html
Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan
Telecom-ISAC Japan 2013/06/17
ネットワークデバイスの脆弱性保有状況調査について
情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ通信協会テレコム・アイザック推進会議(所在地:東京都港区、会長:飯塚久夫(NECビッグローブ株式会社)、以下、Telecom-ISAC Japan)は、国内主要通信事業者、ISP(インターネットサービスプロバイダ)の業界団体として、インターネットの安定運用に関わる事象の検出および対処に取り組んでおります。
I. 背景・概要
Telecom-ISAC Japanでは数年前より、ルータなどのネットワークデバイスの脆弱性問題について議論を重ね、対策検討を行ってまいりました。
本年2月にはUPnPの脆弱性が国内外で指摘され、3月にはDNSのOpen Resolverを踏み台とした大規模なDoS攻撃が発生するなど、ネットワークデバイスの脆弱性を利用したサイバー攻撃の脅威が高まっております。
さらに、ネットワークデバイスの脆弱性を悪用されるとサイバー攻撃の踏み台に利用されるだけでなく、ネットワーク内への不正侵入やデバイス内保存情報の不正取得などの被害に及ぶ場合もあります。
Telecom-ISAC Japanでは、このような攻撃被害の最小化を図っていくために、日本国内のネットワークに接続するデバイスの脆弱性保有について、実態把握を目的とした調査を6月以降順次行ってまいります。

議論

- サーバとネットワークの棲み分け
  - ISP側で常時パケットフィルタしたい？
  - あるいは融合の流れ？
- CPEのopen resolver対策
  - 顧客連絡？
  - 台数で対応が違う？
  - 将来、脆弱性が出たらどうする？

Inbound Port 53 Blocking

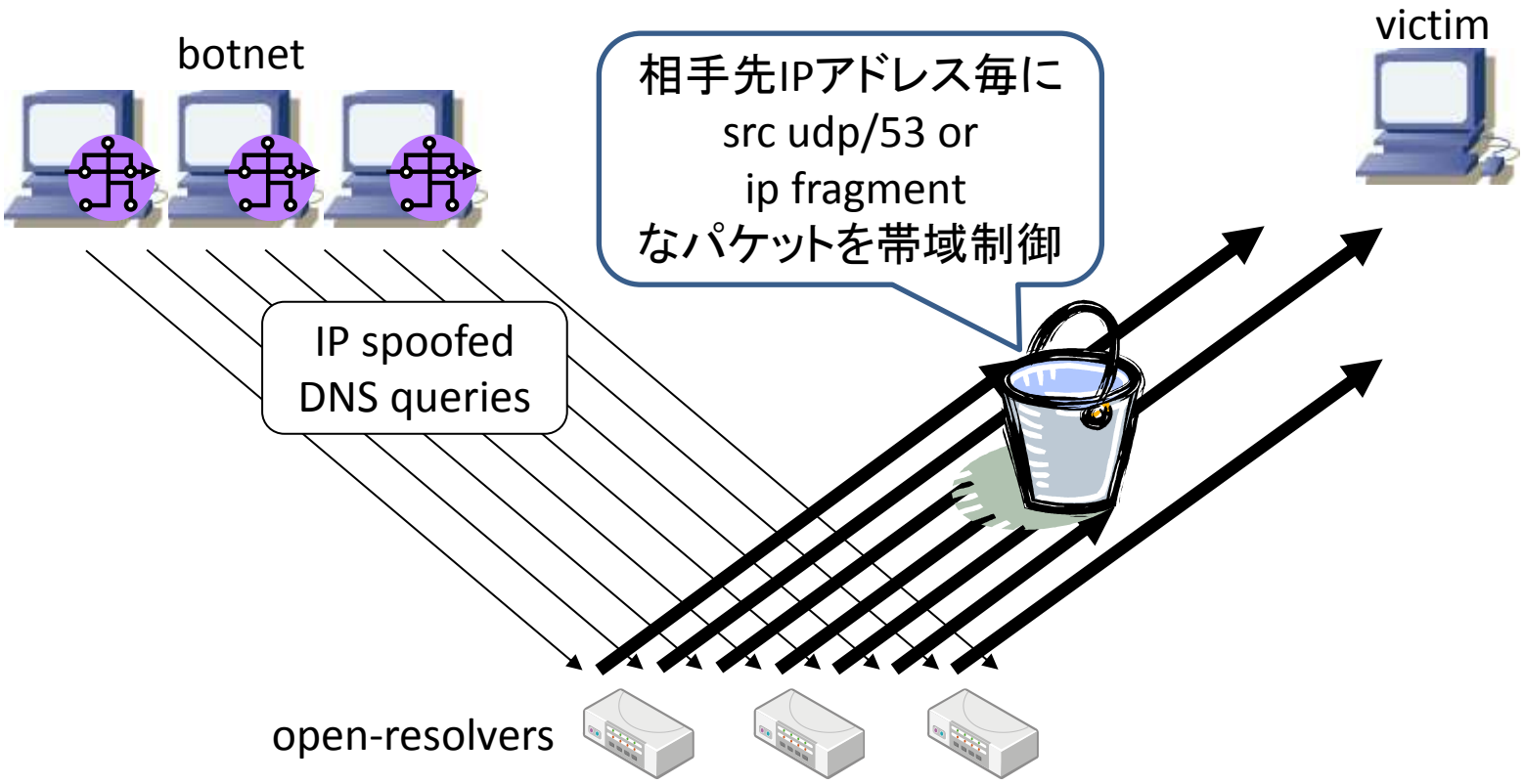


- 顧客側でDNS立ててたら利用不可に
- 一度投入しちゃうと、外すのは難しい

客向け dst udp/53 な
パケットをフィルタ

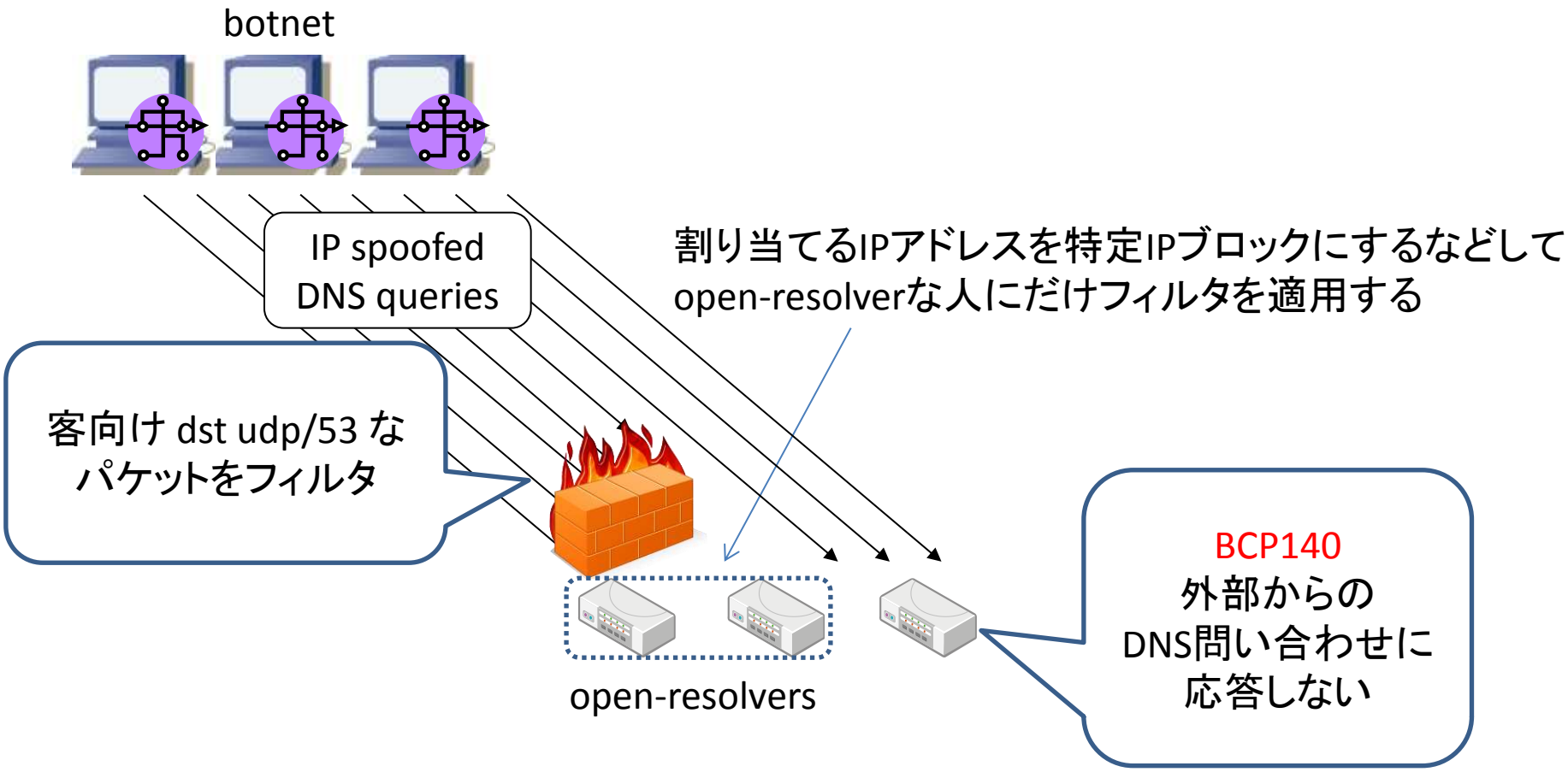
ちょっと粒度が荒すぎる

Outbound dns amp Rate Limiting



もしかしたら動くかも

Segmented IP53B



最近の端末環境

事業者によってポリシが違うよね

まとめ

- パケットフィルタは時に有用だけど、乱暴者
  - ご利用は計画的に
  - 押し付けで設定されるフィルタは共通認識があった方が良いよね
- 過剰防衛にならないように
  - 将来の利用を阻害しない様に
  - 「これで安全ですよ」とか甘い言葉に騙されないように

おわり