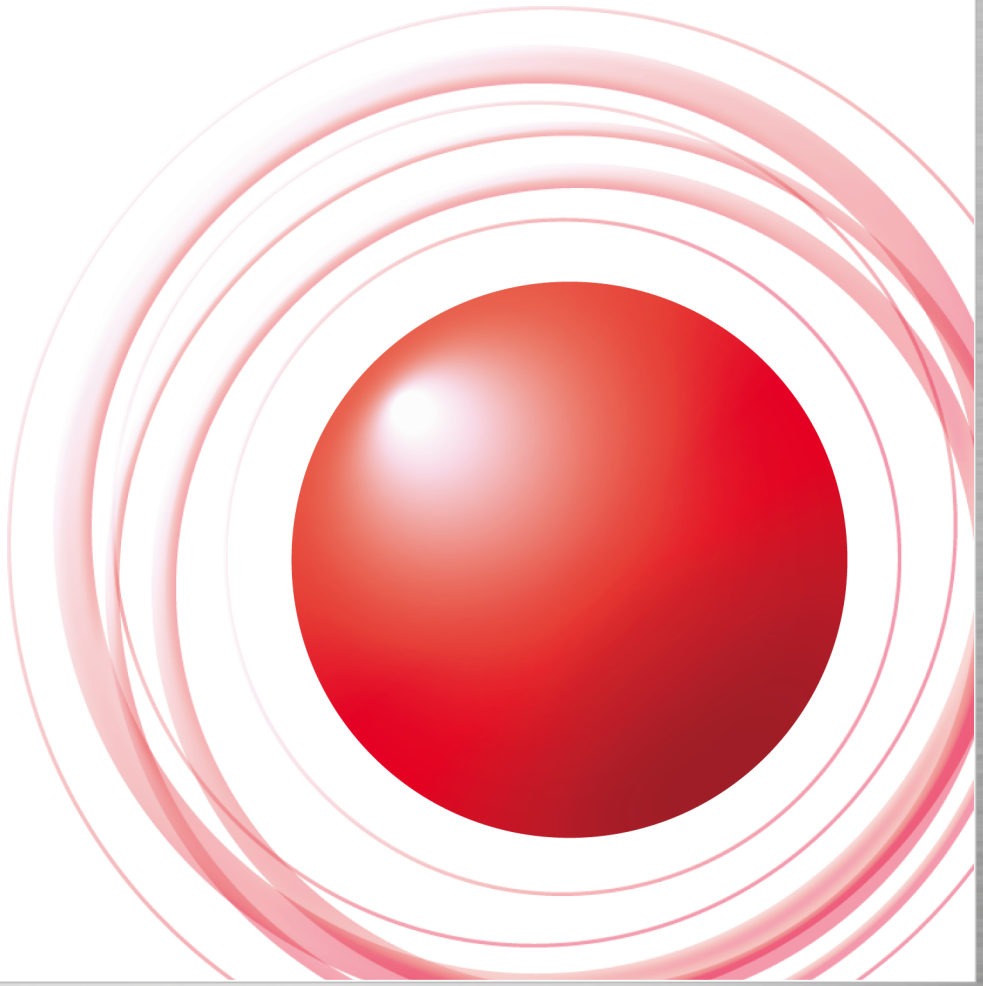
IP53Bの概要

IIJ
Internet Initiative Japan



InternetWeek 2014 DNS DAY
株式会社インターネットイニシアティブ
山口崇徳

Ongoing Innovation

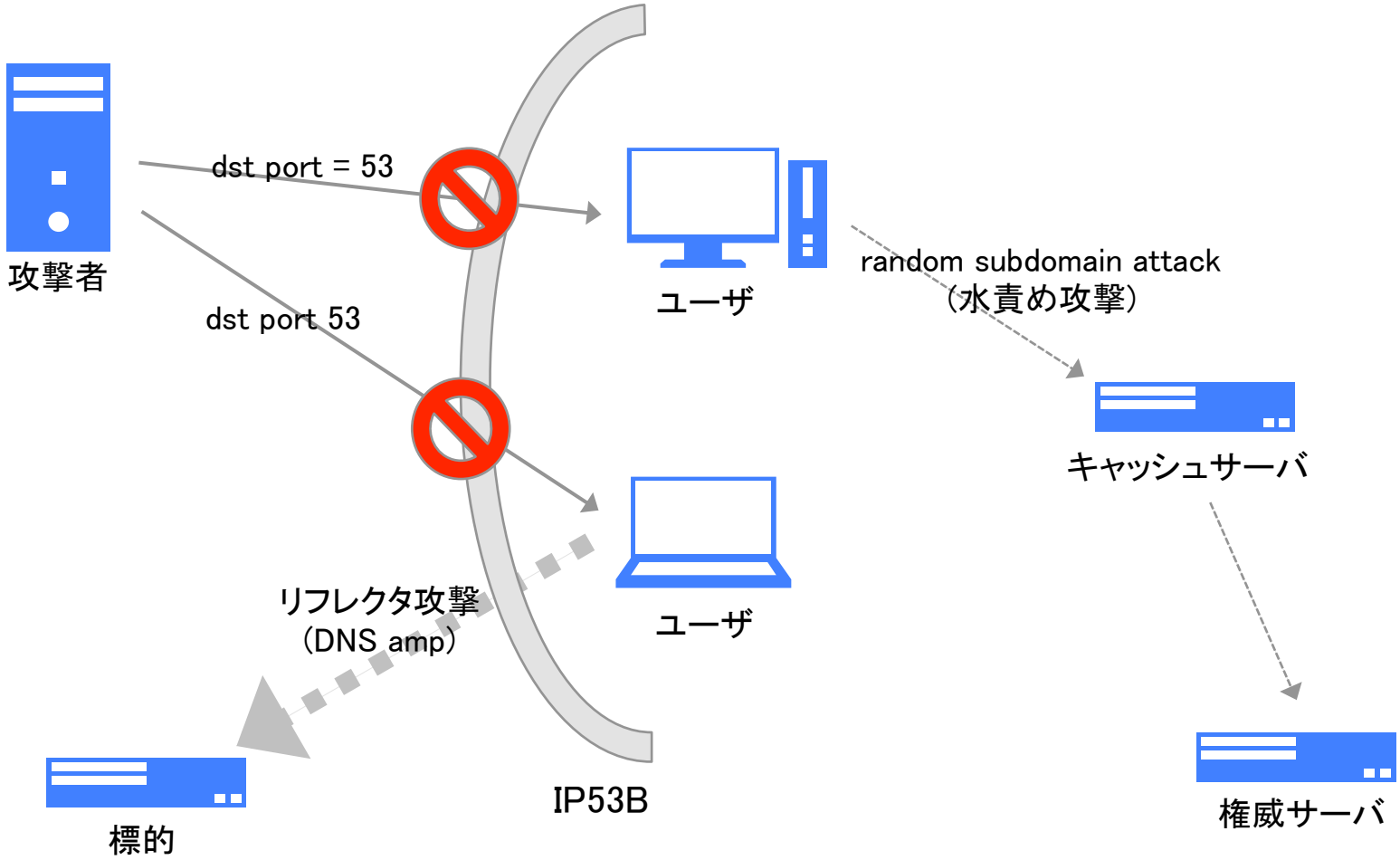
© 2013 Internet Initiative Japan Inc.

いま DNS になにが起きているのか

- **オープンリゾルバ/フォワーダを踏み台にした DDoS 攻撃**
  - DNS amp
  - random subdomain attack (DNS水責め攻撃)
    - ISP の設備に大きな負荷を与える
  - いずれもオープンリゾルバ/フォワーダとなっているエンドユーザはあくまで踏み台であって、攻撃対象そのものではない
- **対処方法**
  - 外からの DNS クエリを受けないようにする
  - 個人ユーザ宅内のホームルータなどを逐一設定変更していくのは現実的には困難
  - ISP で一括して止めてしまえば…?

© 2013 Internet Initiative Japan Inc.

Inbound Port 53 Blocking



© 2013 Internet Initiative Japan Inc.

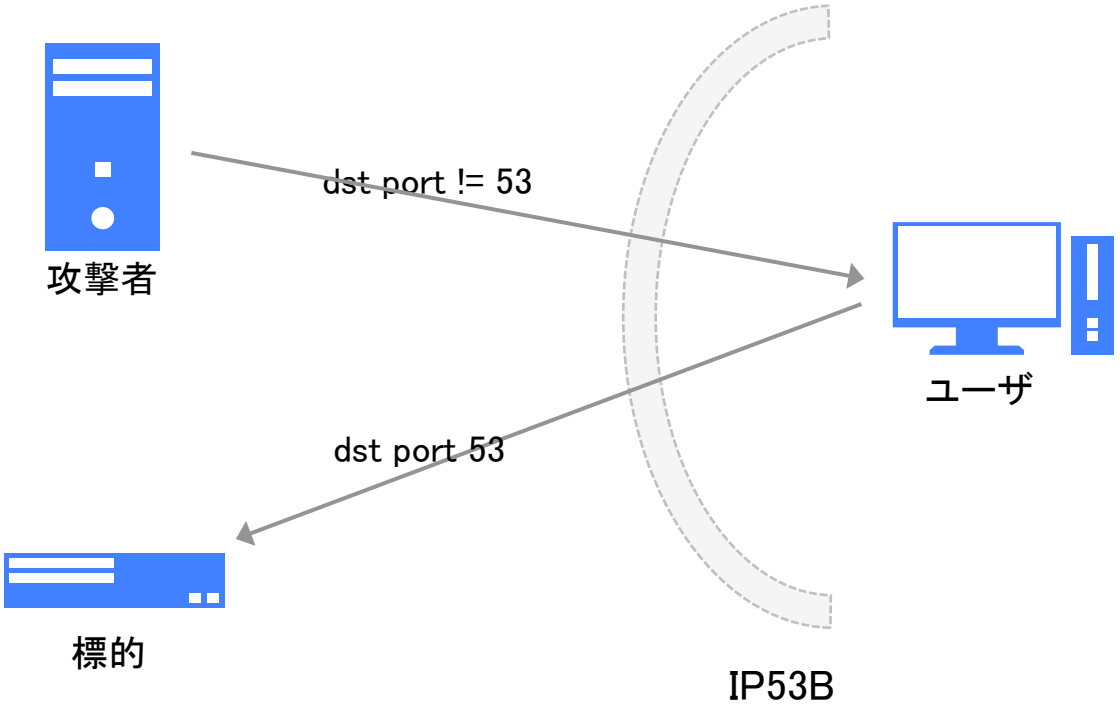
IP53B で制限される通信

- **ユーザの IP アドレスに届く dst port 53 のパケット**
- **使えなくなる例**
  - 外部からアクセスされる DNS サーバ
    - 動的割り当ての IP アドレスでは権威/キャッシュともほぼ実用にならない
    - 固定 IP での実施は困難か
  - src port 53 固定のキャッシュ DNS サーバ
    - 権威サーバからの応答が dst port 53 になる
    - この場合は、内部利用限定でもひっかかる
  - DNS 以外の用途での port 53 の利用
    - ファイアウォールの制限回避などの目的で、sshd その他のアプリケーションを port 53 で動かしている例が稀に存在する模様
- **通常の使い方であれば、動的割り当ての IP アドレスにこのようなパケットは届かない**
  - dynamic DNS で自宅サーバを運用してもひっかからない
  - ユーザに与える影響はないはず

© 2013 Internet Initiative Japan Inc.

IP53B で制限できない通信

- **ユーザの PC をマルウェアに感染させ、そこから攻撃目的の DNS パケットを送出させるような行為**
  - 感染 PC に届くのは DNS とは異なるプロトコルによる攻撃指令
    - 攻撃指令は攻撃者が push するのではなく、感染者が pull することも



© 2013 Internet Initiative Japan Inc.

OP53B

- **エンドユーザが dst port 53 のパケットを送れないよう、ISP 側でフィルタしちゃおう**
  - ISP で用意したキャッシュサーバにはアクセスできるようにしておく
- **攻撃の踏み台に使われてしまっても、外部の攻撃対象にパケットが届かずフィルタされる**
  - が、ISP のサーバへのフォワードは可能なので、踏み台防止の効果は薄い
  - google public dns その他、外部のキャッシュサーバを使おうとしても使えない
- **IP53B よりスジが悪い**
- **しかし、マルウェア感染 PC からの DNS への攻撃を防げる**
  - OP53B の適用例外(ISP のキャッシュサーバ)への攻撃は防げない

© 2013 Internet Initiative Japan Inc.

先行事例: OP25B

- **Outbound Port 25 Blocking**
- **悪意あるユーザや、マルウェアに感染した PC から大量の spam メールを送信されるのを防止するための対策**
  - ISP が用意したメールサーバ以外にメールを送る場合には、port 25 の通常のユーザ認証なし SMTP ではなく、587 (submission) や 465 (smtps) などの認証あり別ポートの利用を強制する
  - 2006年ごろから ISP 各社で導入
- **発想としては OP53B と同じ**
  - 順番はこっちが先ですが
  - 入ってくるメールではなく、出ていくメールの対処が焦点なので、IP25B では対策にならない

© 2013 Internet Initiative Japan Inc.

先行事例: SQL Slammer

- **2003/01/25 に爆発的に増殖し、世界中でネットワーク障害を起こしたワーム**
  - MS SQL Serverの脆弱性を狙う
  - 1434/udp 宛に大量のパケットを撒き散らす
- **一部に IP1434B なフィルタを入れた ISP や組織があったらしい**
  - [janog:04421] SQL SlammerのフィルタとDNSについて
  - ワームによるパケットが増大して、放置すれば他の通信も阻害されるおそれがあった
  - 自社設備に対してだけ適用したのか、顧客宛通信にもフィルタを入れたのかは不明(おそらく後者)

© 2013 Internet Initiative Japan Inc.

法的問題

- ISP が顧客宛通信の中身を見て、dst port 53 だったら顧客に届けずパケットを捨てる
- 通信の秘密を侵害する
- 違法性を阻却する事由として妥当か否か?

- 詳しくは戸取さんのお話を

© 2013 Internet Initiative Japan Inc.

実際の運用

- そもそも、IP53B をやらなきゃいけないぐらい切羽詰まってるの?
- 具体的にどうやってるの?
- 適用後の状況は?

- 詳しくは鵜野さんのお話を

© 2013 Internet Initiative Japan Inc.

DNS 以外のプロトコルは?

- **amp に使われやすいのは、DNS だからというより、UDP だからというのが本質**
- **同様に amp 攻撃の踏み台に利用されやすい UDP 上のプロトコルがいくつかある**
  - NTP、SNMP、CharGEN、SSDP など
  - https://www.us-cert.gov/ncas/alerts/TA14-017A
- **IP53B と同じように、該当ポート番号をフィルタすることで対応は可能**
  - が、実際に適用するかどうかは個別に検討すべき

© 2013 Internet Initiative Japan Inc.

NTP (IP123B)

- **NTP amp の対策に有効……か?**
- **多くの NTP クライアントの実装は src port 123 固定**
  - NTP サーバからの応答が dst port 123 になる
  - OpenNTPD (OpenBSD)、Chrony (RHEL7) などの比較的新しい実装はポート固定しないが、現時点では少数派
  - 安易に IP123B を実施すると、PC の時計合わせがうまくいかなくなる
- **でも KDDI さんは断行したんだよなぁ**
  - http://www.au.kddi.com/information/notice_internet/service/20140825-01.html

© 2013 Internet Initiative Japan Inc.

SSDP (IP1900B)

- **UPnP で利用されるプロトコル**
  - ホームルータなどの機器で多く使われる
- **amp 攻撃の増幅率およそ30倍**
- **リモートからコード実行の脆弱性のある実装が複数存在**
  - https://community.rapid7.com/docs/DOC-2150
  - 機器のファームウェア更新が必要
- **全世界に1800万台の open SSDP server が存在**
  - https://ssdpscan.shadowserver.org/
- **すでに実際に amp 攻撃が観測されはじめている**
  - http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf
- **1900 は WinXP など一部の古い OS でエフェメラルポートとして使われる範囲に含まれる**
  - ごく稀に、SSDP とは無関係の通常の通信がひっかかる可能性

© 2013 Internet Initiative Japan Inc.

まとめ

- **IP53B = Inbound Port 53 Blocking**
- **オープンリゾルバ/フォワーダになっているホームルータなどの機器が攻撃の踏み台として悪用される対策に有効**
  - 動的アドレスならユーザへの悪影響はないはず
  - 積極的に実施すべきなのかどうかは議論の余地あり
    - が、少なくともサービス提供が困難になる前には実施した方がよい
- **DNS 以外にも amp 攻撃が可能なプロトコルがいくつか存在する**
  - IPxxB がどんどん拡大する?
  - 実際の導入は個別に検討を

© 2013 Internet Initiative Japan Inc.