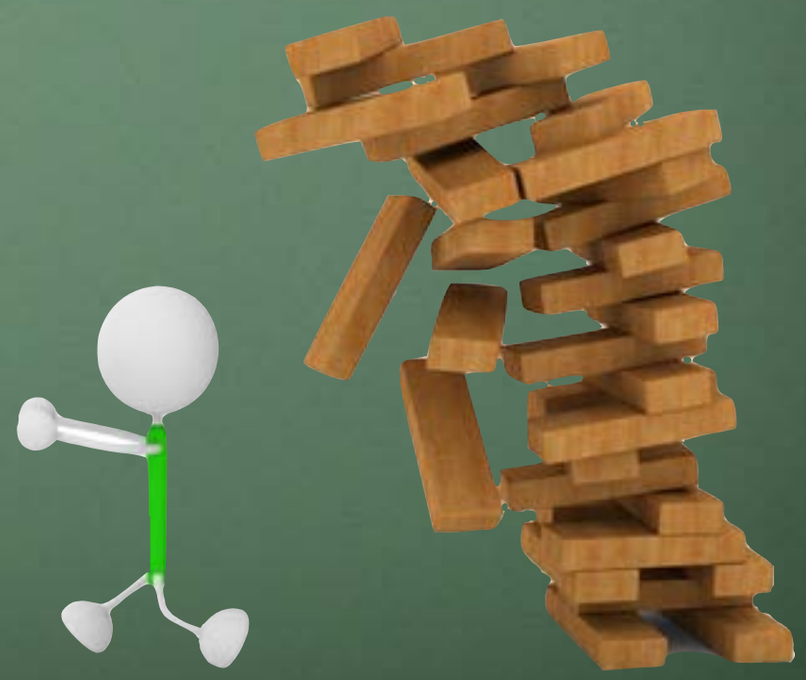
加速する
インターノット崩壊

2015.1.29　ESD21

鈴木常彦　@tss_ontap
中京大学工学部
インターノット崩壊研究室
/ (株)リフレクション

本日のおはなし

- 次々見つかる重大な脆弱性
- 放置される脆弱性
- 放置される古いOS
- 放置される設定不良
- 増加するサービス不能攻撃
- 根幹的な問題
- 未熟すぎる技術の濫用



次々見つかる重大な脆弱性

- 2014.4.7　HeartBleed
暗号化通信基盤ライブラリの深刻な欠陥

- 2014.4.15 Pandora Poisoning
名前解決基盤 DNS の根本的な欠陥

- 2014.9.24 ShellShock
Unix系OSの基盤ツールの深刻な欠陥

- 2014.10.14 POODLE
暗号化通信基盤ライブラリの深刻な欠陥

放置される脆弱性

- アップデートされない家庭用ルータ
- Google が Android 4.4より前の脆弱性は対策しないと発言
  - 9億台が放置?
  - 2年縛りをかけながら、セキュリティアップデートは続かない
- ZeuS 感染 パソコン 国内20万台
- 対策困難な基盤技術の脆弱性
- 今後は IoT が問題に?

IoT に対する危惧

東工大 松岡聡教授 のツイート

http://twitter.com/ProfMatsuoka/status/559730228268781569

放置される設定・運用不良

- なぜか暗号化(HTTPS)が外された銀行とか
- 毒入れ危険性の非常に高いDNSサーバ 10%
- 乗っ取りの危険性が放置されたままの
  レンタルDNSサービス 多数(?)
- 設定不良のない DNS サーバは稀
  - 内閣サイバーセキュリティセンター
    2台のうち1台が何ヶ月(?)も停止

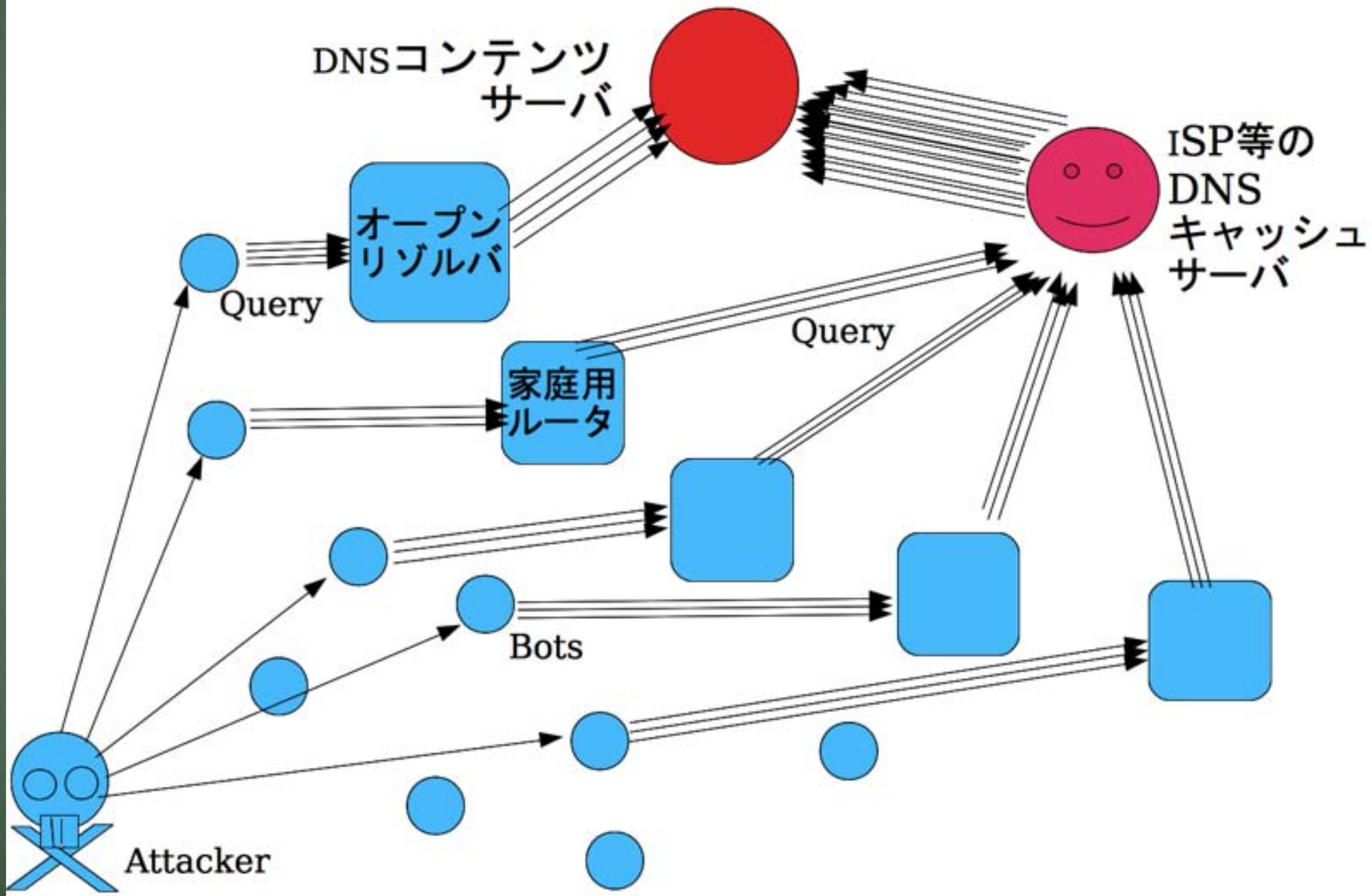
増加するサービス不能攻撃

- 事例
  - Sony Playstation Network
  - プロバイダ各社
  - 国内初検挙は高校一年生
- 手法
  - DNSリフレクション(反射)攻撃
  - NTPリフレクション攻撃
  - DNS水攻め攻撃

DNS水責め攻撃

- 2014年8月2日 読売新聞要約
  - 家庭用ルーターを悪用する新たな攻撃が
  - 少なくとも４８０万世帯が通信障害
  - 脆弱なルーター等
- サイバー攻撃に詳しい中京大の鈴木常彦教授は「攻撃者が弱点のあるルーターを一斉に攻撃すると、日本中のネットをダウンさせることも可能だ。深刻な脅威で、ほかの利用者に迷惑をかける恐れがあり、利用者は早急に更新すべきだ」と指摘している。

DNS 水責め攻撃


DNSコンテンツ
サーバ
ISP等の
DNS
キャッシュ
サーバ
オープン
リゾルバ
Query
Query
家庭用
ルータ
Bots
Attacker

根幹的な問題

- 基盤技術は30年以上前の実験ネットのまま
- 経路制御は騙せる、壊せる
  (偽ネットワークへの誘導)
- DNS は騙せる、壊せる
  (偽サーバへの誘導)
- 電子メールは風前の灯火
- 基盤技術者が絶滅中

未熟すぎる技術の濫用

某銀行サイトの図

監視社会の到来

米オバマ大統領曰く
「政府が暗号化されたコミュニケーションに阻まれることがあってはならない」

ところで裁判は?

残念ながら東京高裁で不当判決→最高裁も不受理

報告会を兼ねたフォーラムを開きます

http://www.can.initiative.jp/forum.html