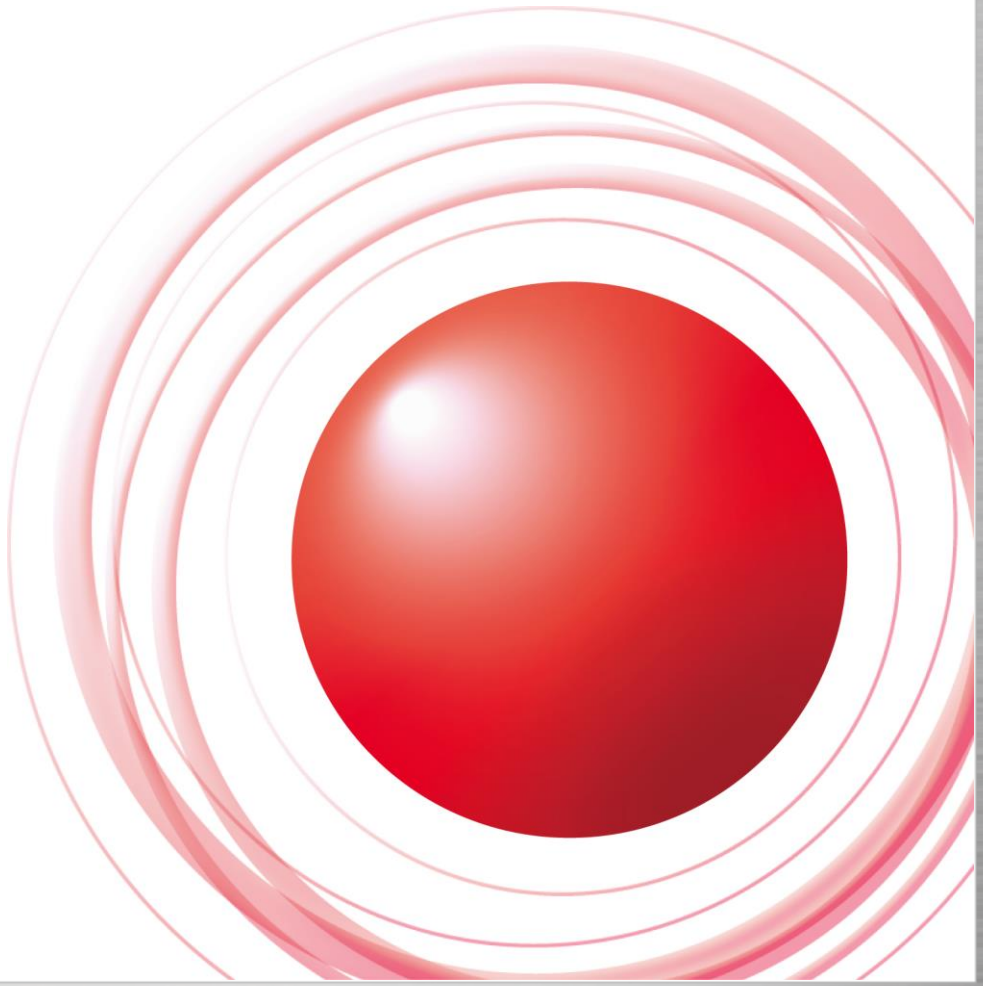
DNSにまつわるセキュリティのあれこれ

IIJ
Internet Initiative Japan



株式会社
インターネットイニシアティブ
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

© 2016 Internet Initiative Japan Inc.

自己紹介

- 島村 充 (しまむら みつる)
- 2006年IIJ入社
- 入社以来、普段はメールサービスの設計・開発・構築・運用業務に従事

- 2010年頃から回線サービス向け参照用DNSサーバの設計・開発・構築・運用業務
- 2015年からDNSアウトソースサービス(権威DNSサービス)の運用業務

© 2016 Internet Initiative Japan Inc.

過去の発表

- キャッシュDNSサーバとフィルタリングの実例
  (Internet Week 2011)
- 法人向けメールサービスにおける
  Submission踏み台問題の状況とその対策
  (IAjapan 第11回 迷惑メール対策カンファレンス)
- キャッシュDNSサーバー DNSSECトラブル
  シューティング (Internet Week 2015)
- 顧客向け参照用DNS管理者の憂鬱 ～無償だと
  思っていたDNSBLが有償だったら～
  (DNSOPS.JP BoF 2015)
- BINDからの卒業, Unboundの紹介とその運用,
  BIND辞められない理由Q&A
  (DNS Summer Day 2016)

© 2016 Internet Initiative Japan Inc.

Agenda

- DNSが止まると？
- DNSを使った攻撃
- DNSに対する攻撃
- 巻添えを喰らわないために
- IIJのDNSサービスの内側
- DNSソフトウェアの脆弱性

© 2016 Internet Initiative Japan Inc.

DNSが止まると？

© 2016 Internet Initiative Japan Inc.

DNSが止まると！

- DNSが止まるとどうなる？

↓

「インターネットが使えません!!」

- 雑なので、もう少し詳しく…
  - 権威DNSサーバ

    その権威DNSサーバが管理してるゾーン配下の、すべてのサービスが利用できない(メール, Web, etc...)
  - キャッシュDNSサーバ

    利用者「インターネットが使えません!!」

© 2016 Internet Initiative Japan Inc.

DNSは空気と同じ

- 普段は意識することはない
- 無くなったら(止まったら)大変

⋮

⋮

⋮

- しっかり運用していても、普段は頑張りを認められづらい
- 障害を起こすと大変怒られる
  - 理不尽です…。

    (インフラってそういうものですが。)

© 2016 Internet Initiative Japan Inc.

DNSを使った攻撃

© 2016 Internet Initiative Japan Inc.

DNS amp攻撃

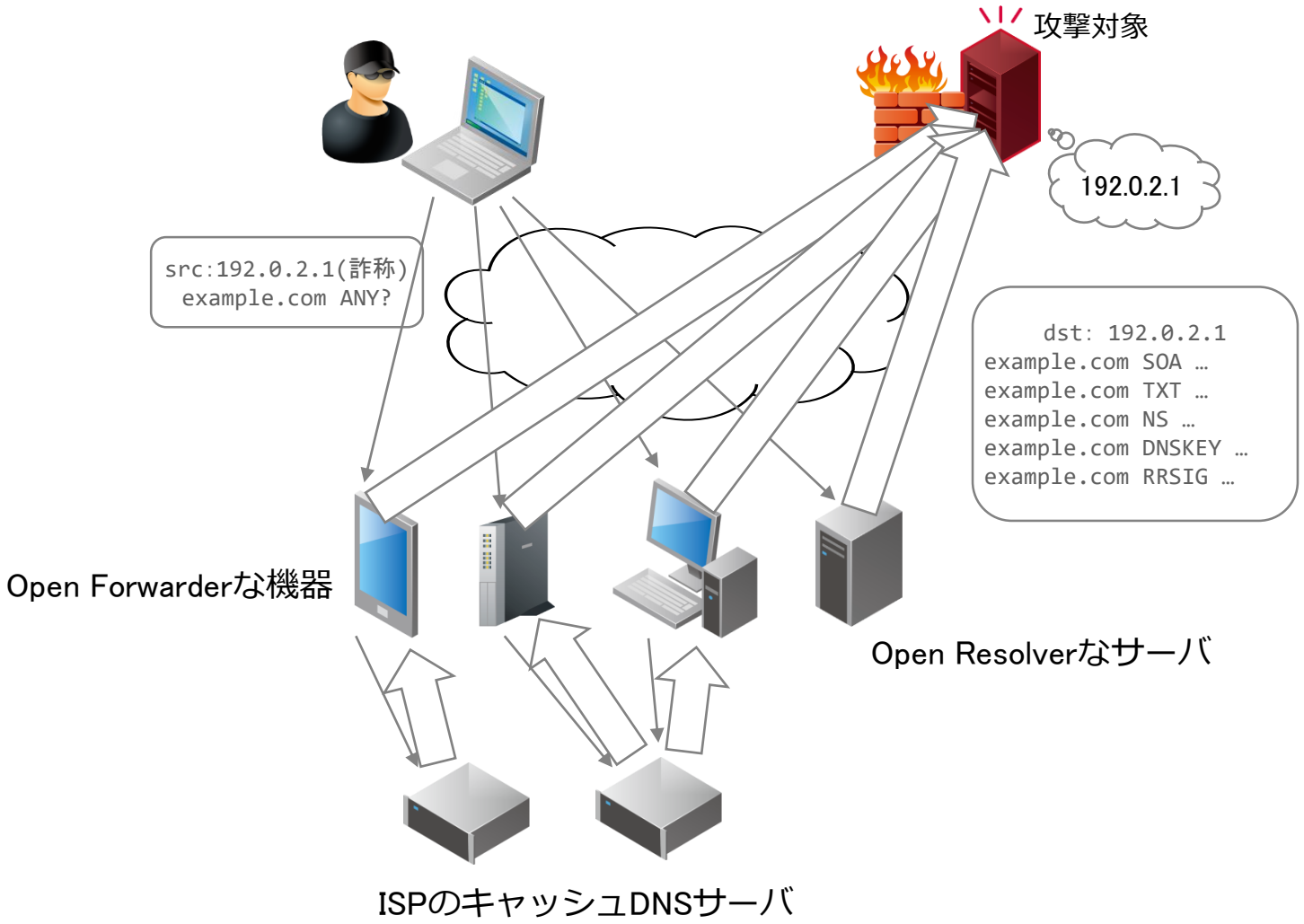
- Open Resolver(※)を踏み台(隠れ蓑)にして、攻撃対象の回線を輻輳(飽和)させるDDoS攻撃

  ※) 適切なACLのかかっていない、世界中どこからの名前解決も処理してしまうサーバ・機器

- 回線を飽和させるので標的はなんでも良い
- 通信相手とハンドシェイクしないUDPサービス+src IPアドレス spoofingを組み合わせればDNS以外のプロトコルでも可能(NTP, snmp, chargen…)
  - 攻撃者が、攻撃に利用するレコードを用意することができ、増幅率を上げることが容易
  - Open Resolverが世界中にとても沢山あったため、同時に攻撃を行う際の上限が高い＆身バレしづらい

© 2016 Internet Initiative Japan Inc.

DNS amp攻撃の概略



© 2016 Internet Initiative Japan Inc.

DNS amp攻撃の歴史

- 古くは1999年頃から

  AusCERT Denial of Service (DoS) attacks using the Domain Name System (DNS)

- 2006年頃から国内でも問題視

  JANOG 18 DNS amplification attacks

- 2013年初頭 世界的に流行。大問題に

  過去最大300Gbps超のDDoS攻撃に悪用されたDNSの「オープンリゾルバー」とは - INTERNET Watch

  - この頃 Open Resolver Project 発足
  - 日本でもJPCERT/CCが openresolver.jp 立ち上げ
  - Open Resolver撲滅・BCP38(Source Address Validation(source IPアドレス詐称禁止))導入の機運が高まる

© 2016 Internet Initiative Japan Inc.

DNS amp攻撃の歴史

- 2016年9月頭、再び話題に

  DDoS攻撃と見られる大量のトラフィックによりスラドを含む国内の複数サイトがダウン | スラド セキュリティ

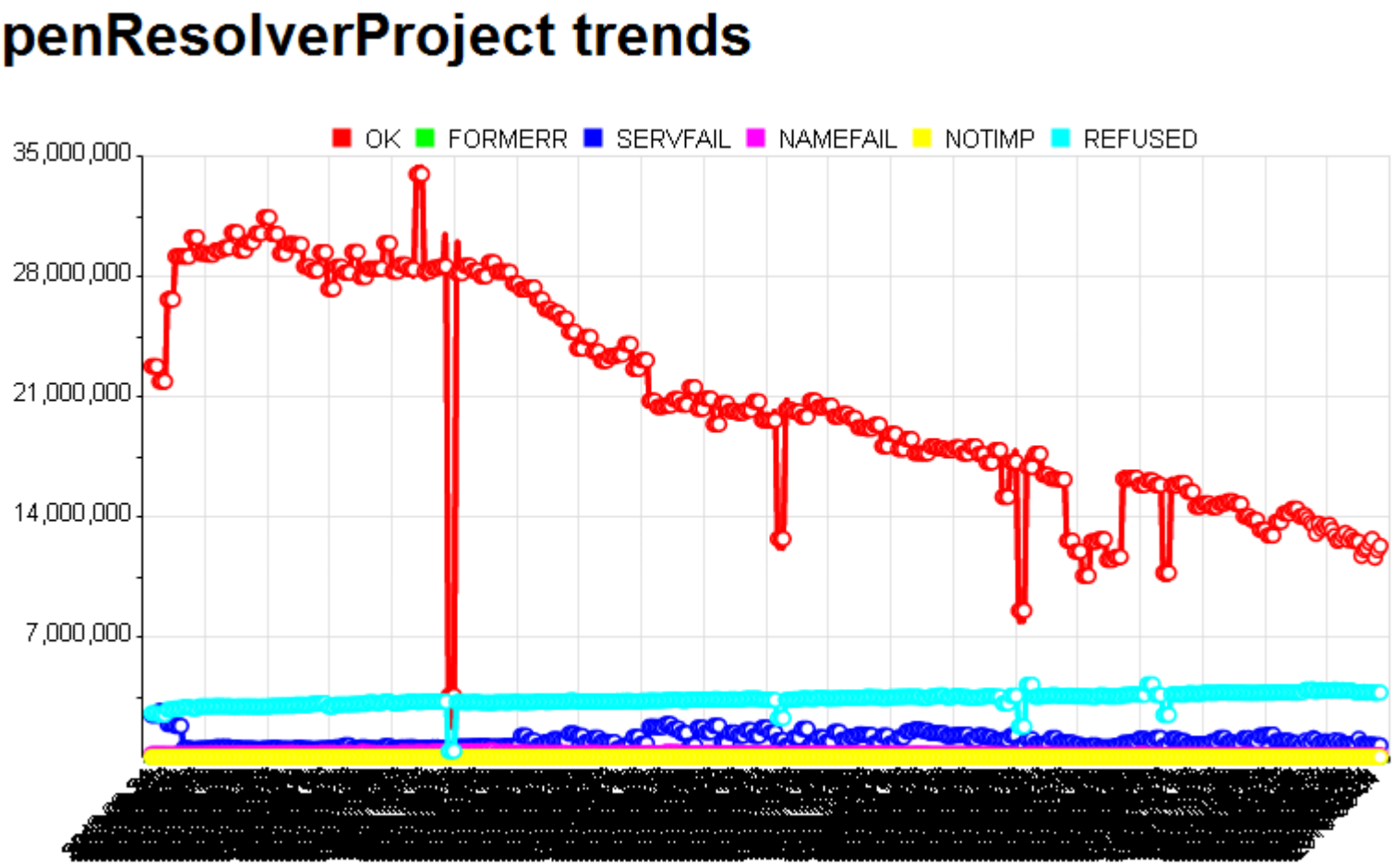
…なったと思ったが、主役交代…？

- IoT機器を悪用したBotnetからの直接攻撃 (Mirai) (後ほど解説)

© 2016 Internet Initiative Japan Inc.

Open Resolver数推移

- 全世界

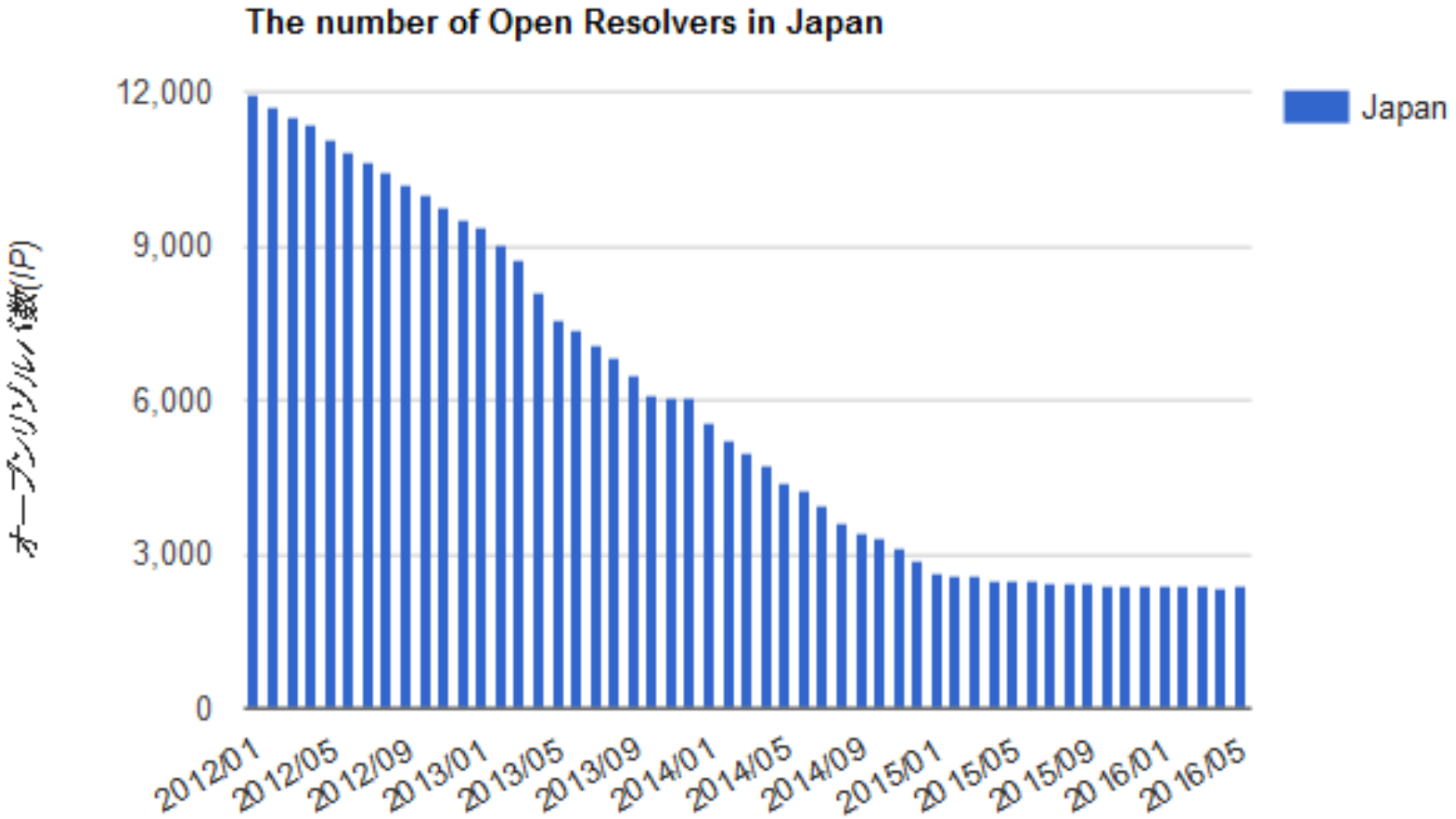


http://openresolverproject.org/graph-rcode.cgi

© 2016 Internet Initiative Japan Inc.

Open Resolver数推移

- 日本



http://www.openresolver.jp/

© 2016 Internet Initiative Japan Inc.

Miraiとは

- 史上最大規模のDDoS攻撃

  セキュリティニュースサイトに史上最大規模のDDoS攻撃、1Tbpsのトラフィックも - ITmedia エンタープライズ (9/26)

- Mirai
  - パスワードがザルなホームルータ、Webカメラ等に感染するマルウエア及び形成されたボットネットの名称
    - 工場出荷時のデフォルトや、よくあるパスワードでログインを試行しているだけ
  - github上でソースコード公開
    - 感染機器: 公開前21万台、公開後49万台

© 2016 Internet Initiative Japan Inc.

Miraiの攻撃手法

- いくつかの攻撃手法が実装されている
  - HTTP, DNS, UDP/SYN/ACK flood, GRE
- DNSはもはやオープンリゾルバを使わない
  - 「身バレしないんだから、そのまま攻撃すればいいじゃん」な発想？
  - 水責め攻撃(後述)が実装

© 2016 Internet Initiative Japan Inc.

Miraiが引き起こした世界的な障害

- Dyn(USの超大手DNSホスティング)の障害
  - 日本時間10/22未明から6時間ほど
- Dyn(だけ)を利用するサービスが軒並み障害

Affected services

Services affected by the attack include:

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[27]
- Vox Media[28]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[29]
- WWE Network[30]
- Xbox Live[31]
- Yammer[23]
- Yelp[13]
- Zillow[13]

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

© 2016 Internet Initiative Japan Inc.

DNSに対する攻撃

© 2016 Internet Initiative Japan Inc.

DNS「水責め(Water torture)攻撃」

"被験者を机や椅子に縛り付け、上部に備え付けられた桶から、常に一定間隔で額に水滴を落とし続ける。身体損傷よりはむしろ、終わることのない低刺激を繰り返すことにより精神苦痛と最終的な精神崩壊を誘発させる方法。西欧ではChinese water tortureとして広く知られている。"

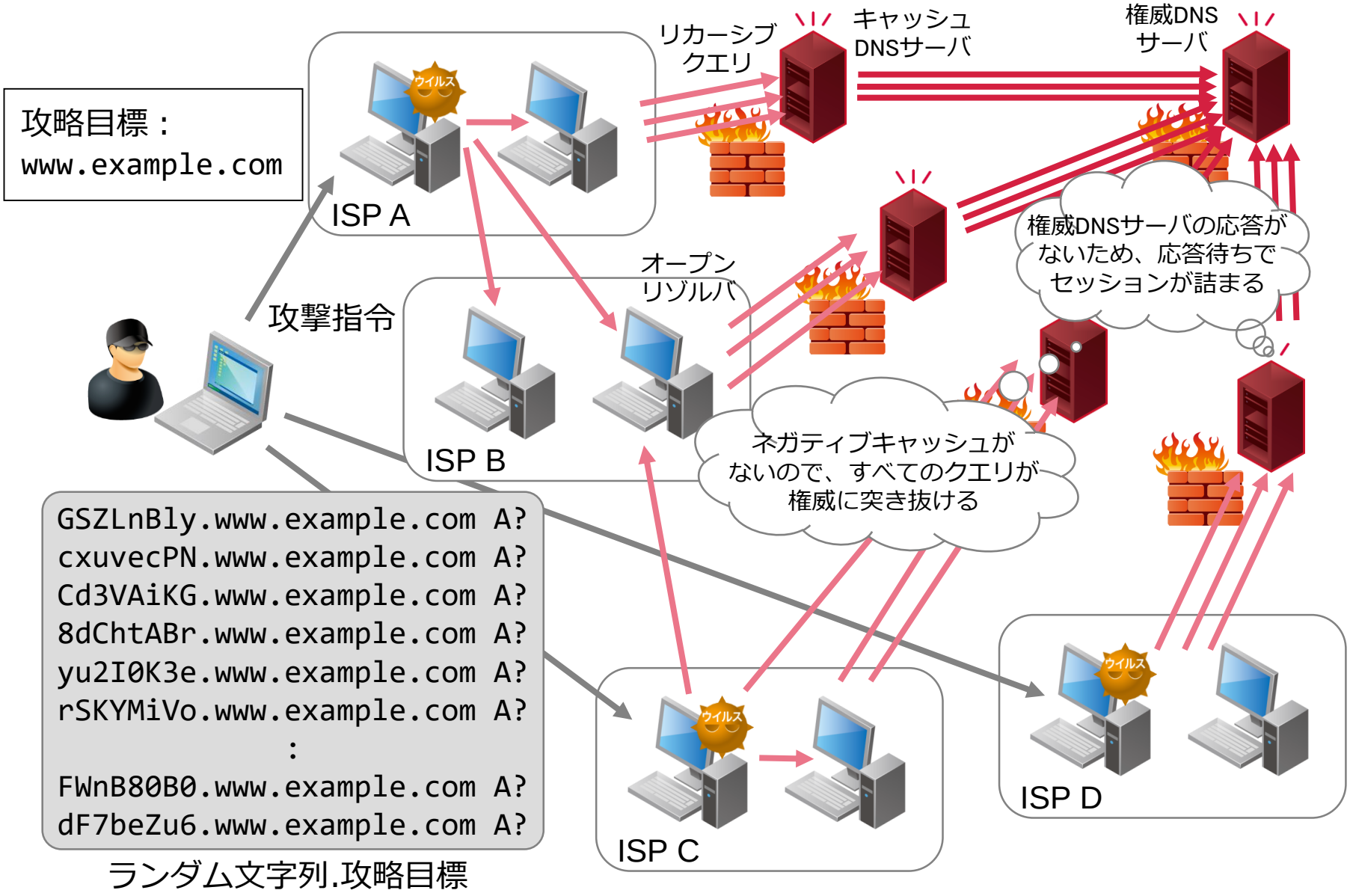
https://ja.wikipedia.org/wiki/水責め

別名:

- ランダムサブドメイン攻撃
- Slow drip攻撃

© 2016 Internet Initiative Japan Inc.

DNS水責め攻撃の概略



© 2016 Internet Initiative Japan Inc.

DNS水責め攻撃の標的

- 攻撃者の狙いは権威DNS(ドメイン)であると思われる
  - 中華系ショッピングやゲームサイト等
- ISPのキャッシュDNSサーバは巻添えを食らう
  - キャッシュDNSサーバの利用者にBot PCやオープンリゾルバなエンドユーザーが多いほど被害は拡大する
  - FirewallやLoadBalancerのセッションが埋まって、一番に倒れることが多い

© 2016 Internet Initiative Japan Inc.

DNS水責め攻撃の履歴

- 一時期、かなり猛威を奮い、日本のドメインはほとんど標的にされなかったことから、ISPのキャッシュDNSサーバの障害が目立つ形になった
- 2014年1月頃から観測され始める
- 4, 5月～ 日本のISP各社で被害拡大
- 2016年5月末、パッタリ止む
  - その後、散発的に発生

© 2016 Internet Initiative Japan Inc.

DNS水責め攻撃への対策

- 権威DNS側
  - 物量(サーバー台数)で耐える
  - 攻撃クエリを送ってきているネットワークレンジを遮断(巻き添え)
  - Response Rate Limit (RRL)

    あるセグメントからのクエリに対して、一定時間に規定回数回までしか答えない

あまり、出来る対策がない…

© 2016 Internet Initiative Japan Inc.

DNS水責め攻撃への対策

- キャッシュDNS側
  - 組織内(エンドユーザ)のOpen Resolver, Bot PCの撲滅
  - BCP38(Source Address Validation)の徹底
  - 攻略対象のドメインを遮断 (DoS成立)
  - hashlimit (iptables)
  - BIND: fetch-per-zone, fetch-per-server
  - unbound: ratelimit-for-domain, ratelimit
  - (どうにもならない場合)IP53B

    自網のエンドユーザーセグメント宛のdst port 53遮断

© 2016 Internet Initiative Japan Inc.

攻撃者に(本気で)狙われたら？

- 物量(サーバーを増やす)で耐える
- DDoS対策サービスやCDNをかませる
  - そのDDoS対策サービスのuplinkが埋まったら…？
  - ISPの対外接続が埋まったら…？
  - CDN業者から追い出されたら…？
- (金銭要求があるなら)お金を払う？
- 嵐が過ぎ去るのを祈りながら待つ？

割りとどうしようもない

© 2016 Internet Initiative Japan Inc.

Miraiが引き起こした世界的な障害

- Dyn(USの超大手DNSホスティング)の障害
  - 日本時間10/22未明から6時間ほど
- Dyn(だけ)を利用するサービスが軒並み障害

Affected services

Services affected by the attack include:

- Airbnb[11]
- Amazon.com[8]
- Ancestry.com[12][13]
- *The A.V. Club*[14]
- BBC[13]
- *The Boston Globe*[11]
- Box[15]
- *Business Insider*[13]
- CNN[13]
- Comcast[16]
- CrunchBase[13]
- DirecTV[13]
- *The Elder Scrolls Online*[13][17]
- Electronic Arts[16]
- Etsy[11][18]
- FiveThirtyEight[13]
- Fox News[19]
- *The Guardian*[19]
- GitHub[11][16]
- Grubhub[20]
- HBO[13]
- Heroku[21]
- HostGator[13]
- iHeartRadio[12][22]
- Imgur[23]
- Indiegogo[12]
- Mashable[24]
- National Hockey League[13]
- Netflix[13][19]
- *The New York Times*[11][16]
- Overstock.com[13]
- PayPal[18]
- Pinterest[16][18]
- Pixlr[13]
- PlayStation Network[16]
- Qualtrics[12]
- Quora[13]
- Reddit[12][16][18]
- Roblox[25]
- Ruby Lane[13]
- *RuneScape*[12]
- SaneBox[21]
- Seamless[23]
- *Second Life*[26]
- Shopify[11]
- Slack[23]
- SoundCloud[11][18]
- Squarespace[13]
- Spotify[12][16][18]
- Starbucks[12][22]
- Storify[15]
- Tumblr[12][16]
- Twilio[12][13]
- Twitter[11][12][16][18]
- Verizon Communications[16]
- Visa[27]
- Vox Media[28]
- Walgreens[13]
- *The Wall Street Journal*[19]
- Wikia[12]
- *Wired*[15]
- Wix.com[29]
- WWE Network[30]
- Xbox Live[31]
- Yammer[23]
- Yelp[13]
- Zillow[13]

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

© 2016 Internet Initiative Japan Inc.

他者の巻添えを喰らわないために

- Dynへの攻撃理由
  - NANOGでの対Botnet対策の発表への報復？(Dyn自体への攻撃)
  - EAの新作ゲームへの攻撃？
    - ◆誰を狙ったのか(現状)不明…。
- 狙われていないドメインも巻添えでダウン

巻添えを喰らわないためには大手・マイナーを取り混ぜた複数事業者と自社運用を組み合わせましょう

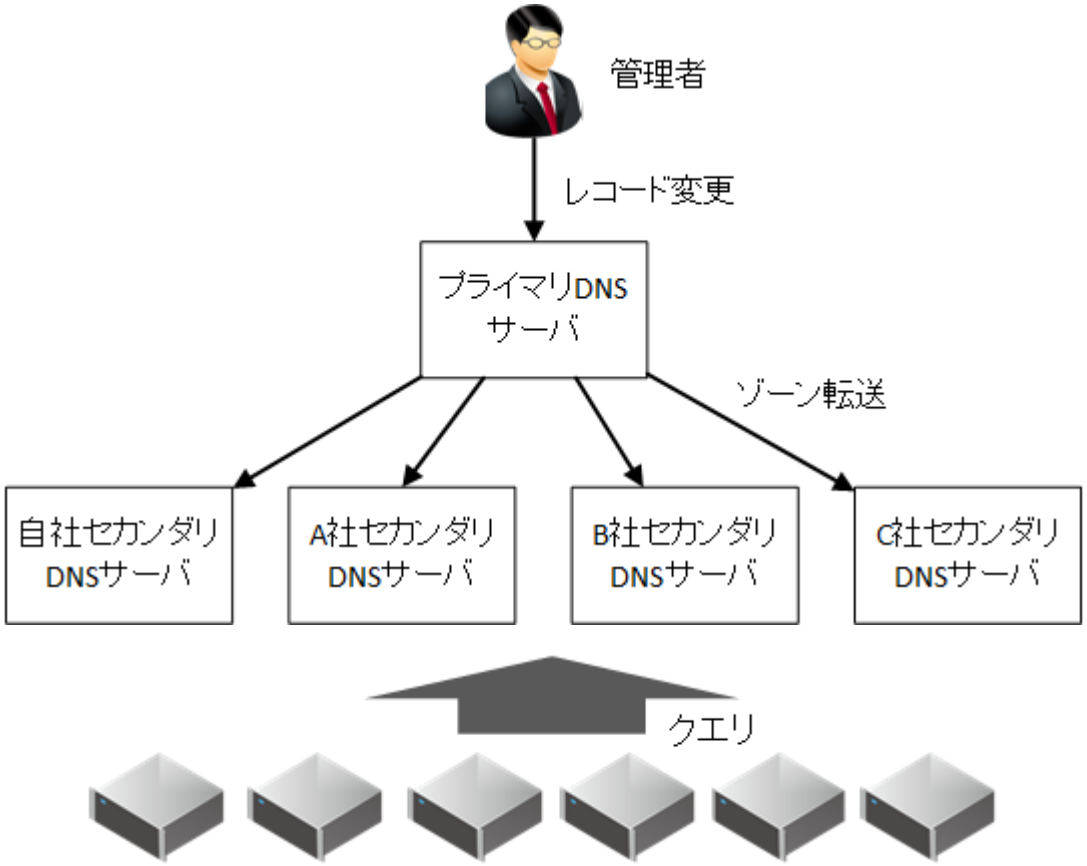
© 2016 Internet Initiative Japan Inc.

巻添えを喰らわないために

© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

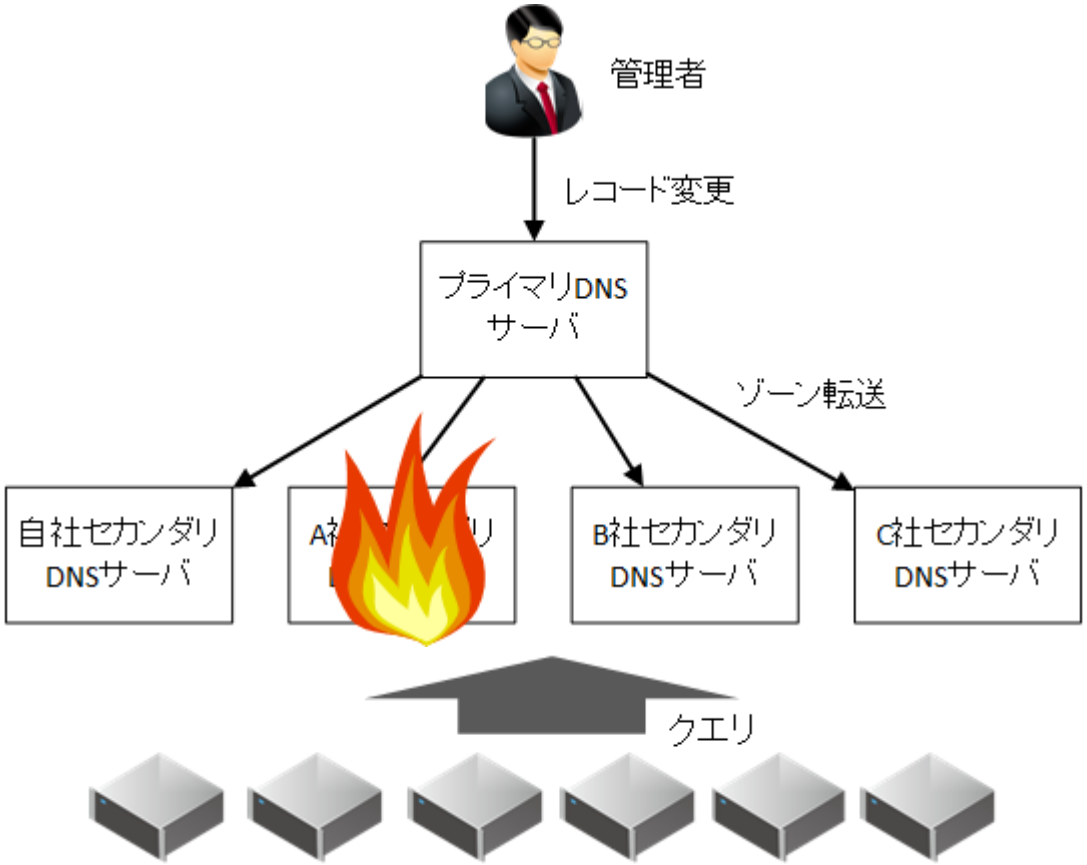
- 例1: 自社プライマリ＋セカンダリサービス



© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

- 例1: 自社プライマリ＋セカンダリサービス



© 2016 Internet Initiative Japan Inc.

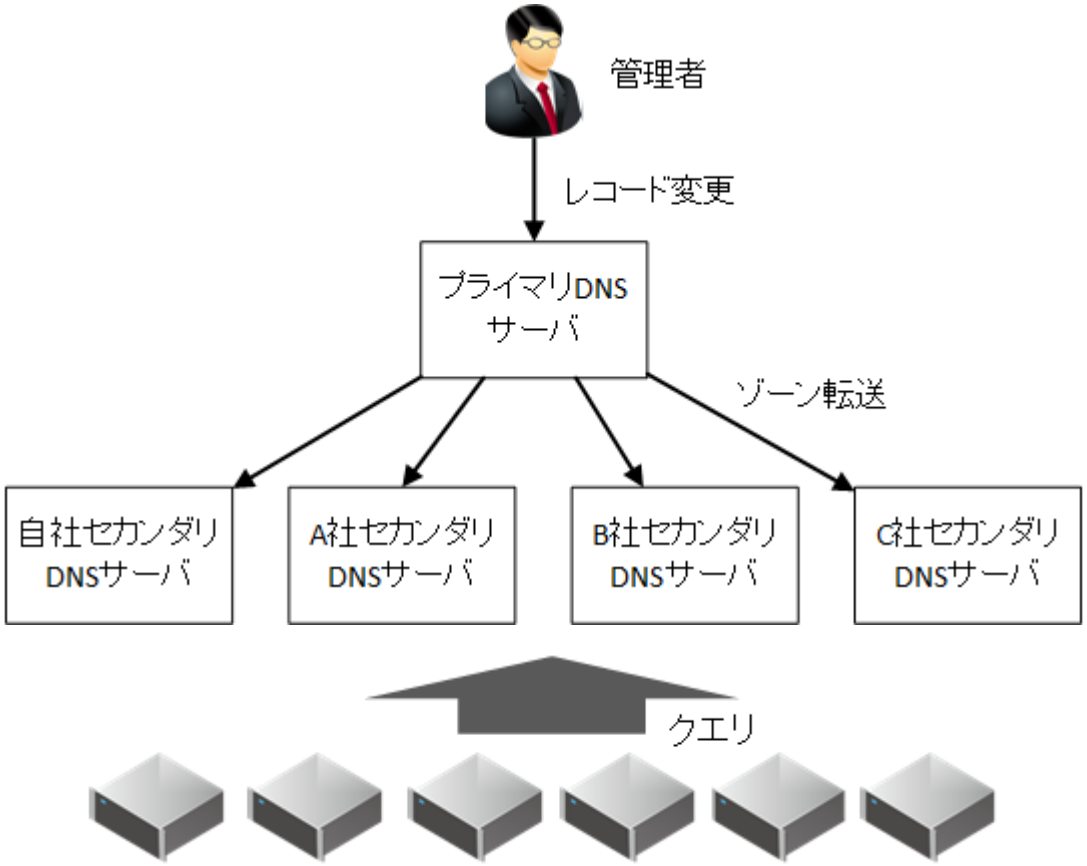
DNSサービスの組合せ例

- 例1: 自社プライマリ＋セカンダリサービス
  - 利点: DNSレコードの変更が、自社管理以外のサービスへもゾーン転送の仕組みで、反映される(別途の作り込みが不要)
  - 欠点: セカンダリサービスをやっているところが少ない

© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

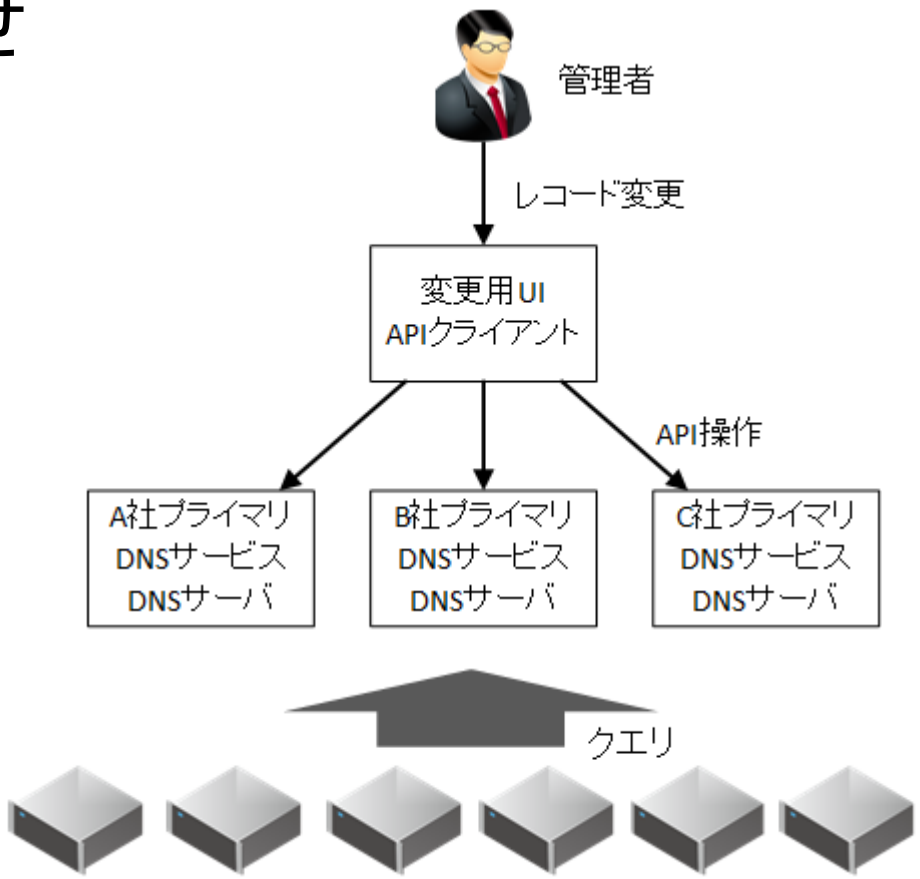
- 例1: 自社プライマリ＋セカンダリサービス



© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

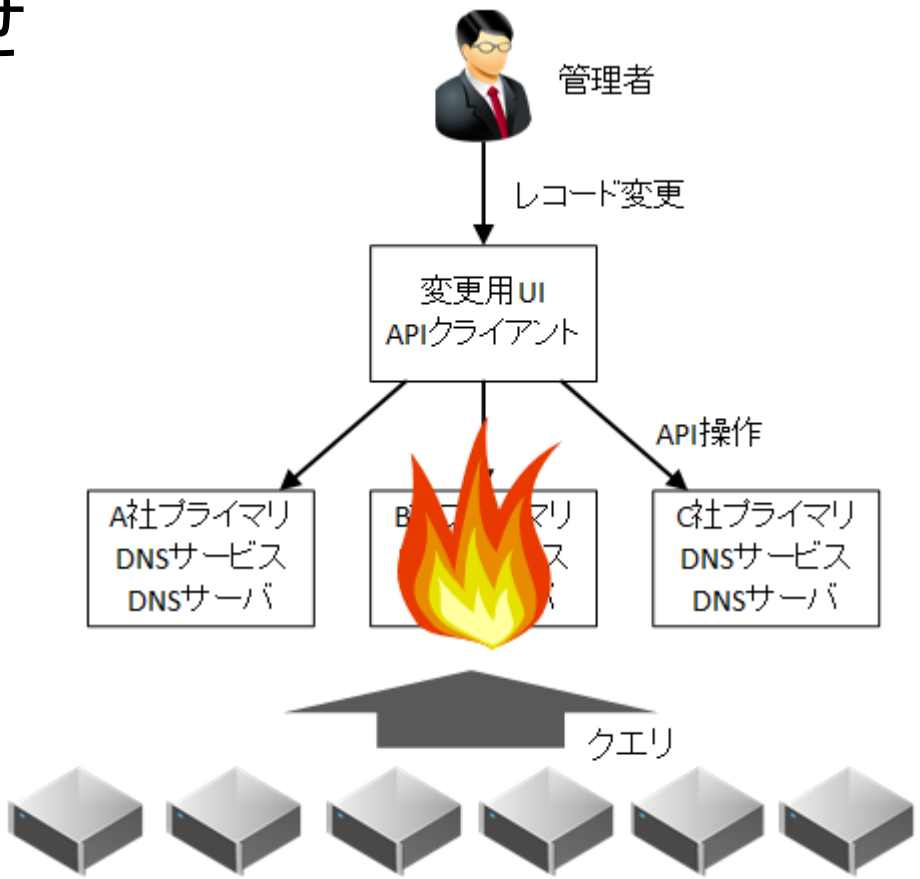
- 例2: プライマリDNSサービスを複数
  - 自社運用、Route53、IIJサービス等を組合せ



© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

- 例2: プライマリDNSサービスを複数
  - 自社運用、Route53、IIJサービス等を組合せ



© 2016 Internet Initiative Japan Inc.

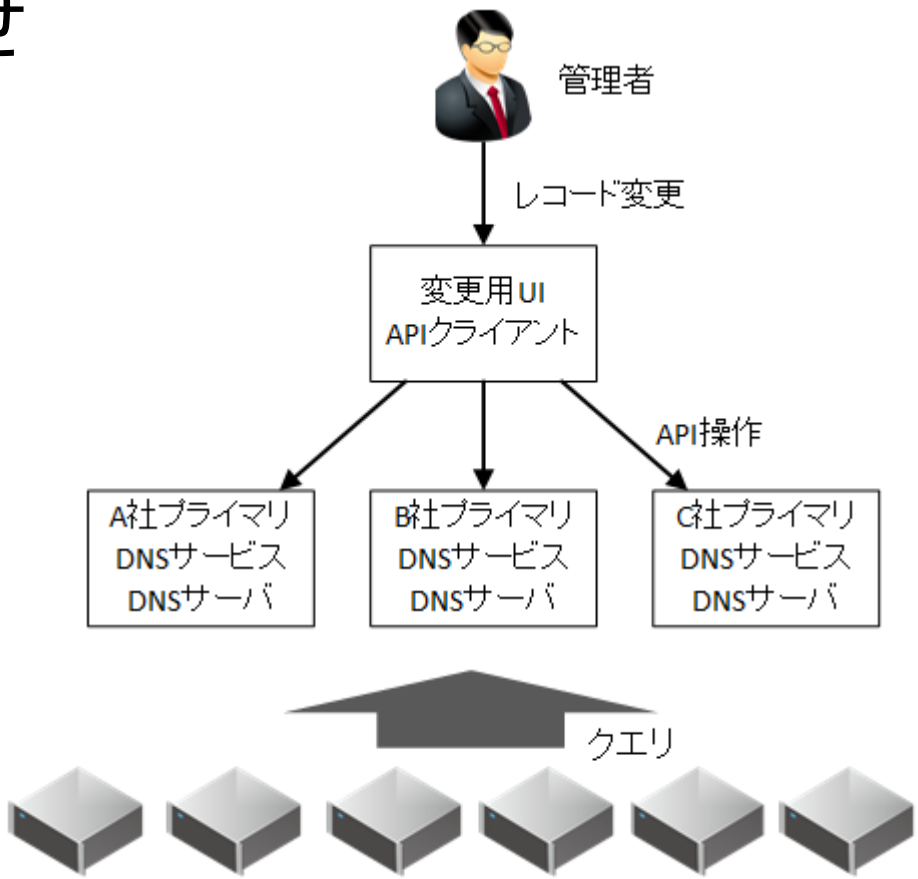
DNSサービスの組合せ例

- 例2: プライマリDNSサービスを複数
  - 利点: サービスの選択肢が豊富
  - 欠点: DNSレコードの変更をゾーン転送以外の何らかの手段ですべてのサービスに行き渡らせなければならない
    - ×人手でポチポチ…？
    - ◎APIで一括変更
      - ◆APIに対応しているサービス以外は利用できなくなる
        - API対応しているサービスは少ない？
      - ◆APIクライアントを作り込む必要あり

© 2016 Internet Initiative Japan Inc.

DNSサービスの組合せ例

- 例2: プライマリDNSサービスを複数
  - 自社運用、Route53、IIJサービス等を組合せ



© 2016 Internet Initiative Japan Inc.

IIJのDNSサービスの内側

© 2016 Internet Initiative Japan Inc.

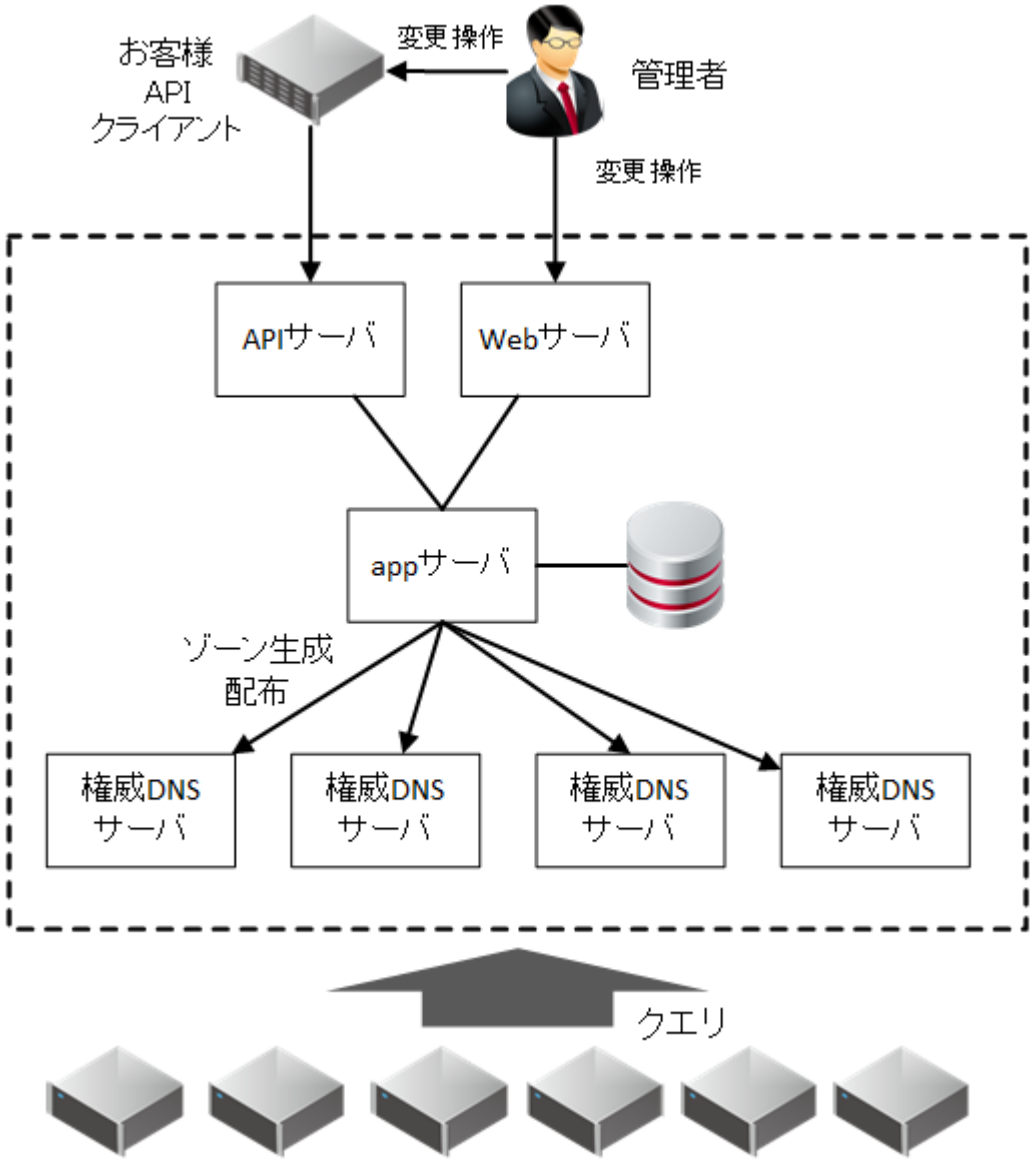
DNSサービスの種類

(ドメイン管理サービスは省略します)

- DNSアウトソースサービス
  - 権威DNSサーバをIIJですべて運用
  - WebUI(サービスオンライン)からの変更操作
  - REST APIでの操作
  - サイトフェイルオーバーオプション
    - ◆監視付き、ディザスタリカバリ用GSLB
- DNSセカンダリサービス
  - プライマリ権威DNSサーバはお客様運用の、セカンダリのみのサービス

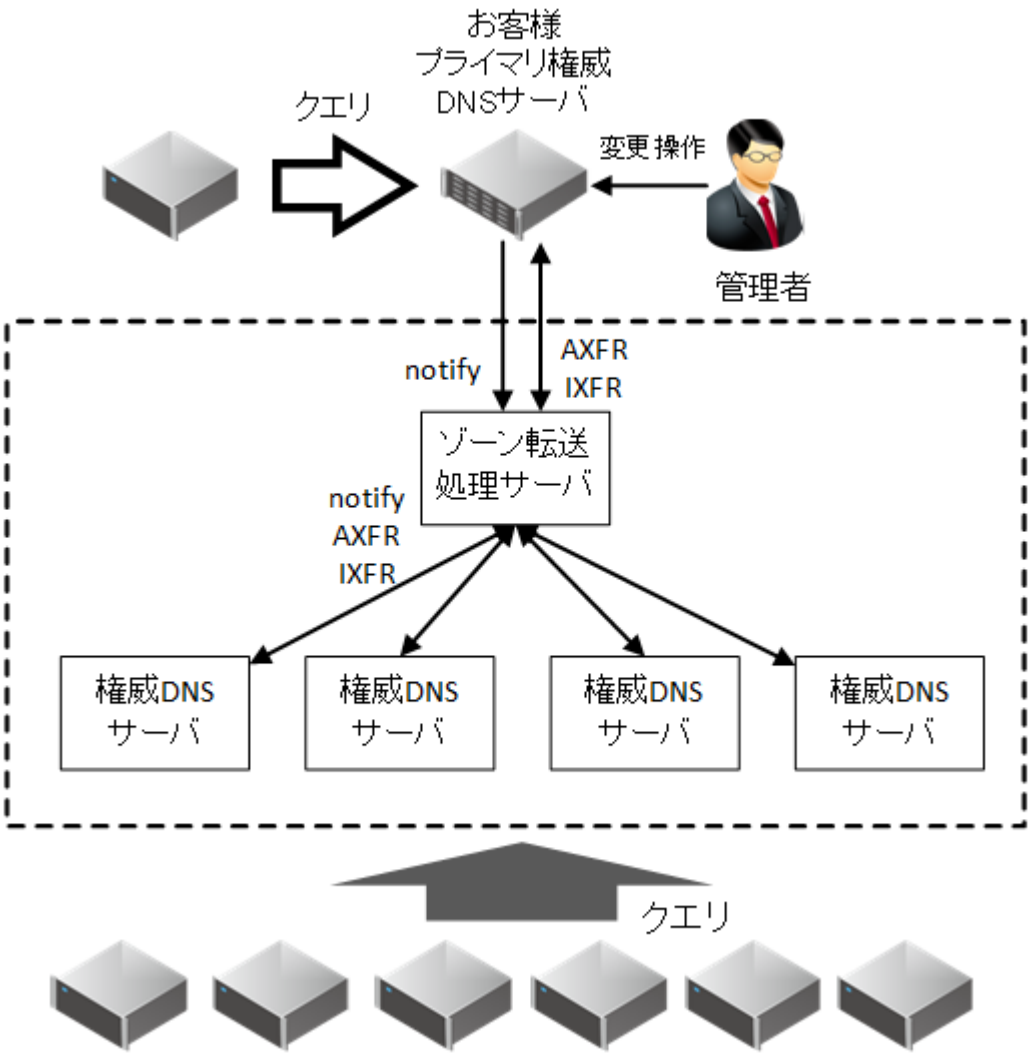
© 2016 Internet Initiative Japan Inc.

DNSアウトソースサービス概略図



© 2016 Internet Initiative Japan Inc.

DNSセカンダリサービス概略図



© 2016 Internet Initiative Japan Inc.

IIJのDNSサービスの特徴

- 片方の権威DNSサーバのIPアドレスをanycastで世界中に分散
  - 東京、大阪、US、ヨーロッパ
- もう片方の権威DNSサーバのIPアドレスはDDoS対策装置で保護

© 2016 Internet Initiative Japan Inc.

anycast概念図

※あくまでイメージで、実際のルーティング状況とは異なりますし、
ルーティングは日々変化します。

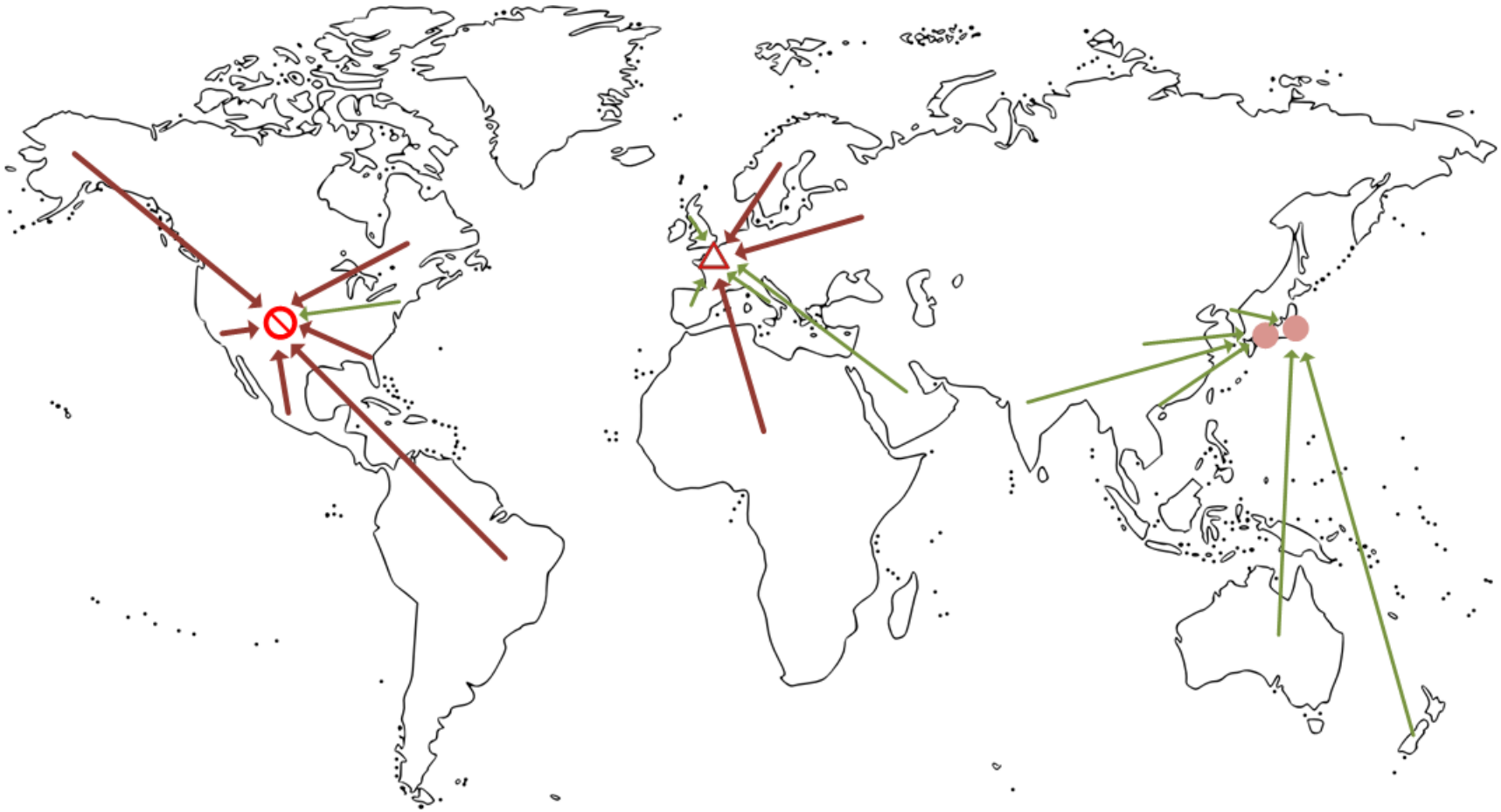
© 2016 Internet Initiative Japan Inc.

anycastの特徴

- anycastによる地理分散
  - ネットワーク的に近いノードにルーティングされる
    - RTTが改善する
    - DDoS攻撃を受けた際の、障害影響の局所化

© 2016 Internet Initiative Japan Inc.

anycastノードへのDDoS攻撃発生時



DDoS攻撃の発生源が国外に集中していた場合、
国内のノードには影響を与えず、サービス継続可能

© 2016 Internet Initiative Japan Inc.

DDoS対策装置による保護

- 不必要なProtocol, portを**バックボーン側で**(※)遮断
  - UDP/0, TCP/80など
- パケット数をカウントしてアノマリ検知
  → 防御発動
  - レート制限
  - トラフィックシェーピング
  - IPアドレスフィルタ

  ※)バックボーン側で対応できることが重要 (firewall・サーバの帯域を埋めない)

© 2016 Internet Initiative Japan Inc.

anycast OR DDoS対策装置？

- 世界中にDDoS対策装置があるわけではない
- 防御発動時の誤遮断の可能性が捨てきれない

→ anycastとDDoS対策装置による対策を別系統で実施

© 2016 Internet Initiative Japan Inc.

DNSソフトウェアの脆弱性

© 2016 Internet Initiative Japan Inc.

BINDの脆弱性

- BIND: DNSサーバソフトウェアのデファクトスタンダード
- DoS脆弱性が頻繁に出ることで有名
- 「パケット1つで即死」がそれなりにある

	1	2	3	4	5	6	7	8	9	10	11	12
2009							◎					
2010							◎					◎
2011		◎			○	◎	◎					◎/○
2012						◎	○		◎	◎		○
2013	○		◎			◎	◎					
2014	◎				◎	◎						○/◎
2015		◎					◎/◎		◎			◎
2016	◎		◎						◎		◎	

※ JPRSさん「DNS関連技術情報」にて“(重要)”→◎ 無印→○

© 2016 Internet Initiative Japan Inc.

BINDの脆弱性

- DNSサーバが落ちる

  →「インターネットが使えません！！」

- 脆弱性が公表されたら(遅くとも)2,3日以内に修正版を適用しなくてはいけない

  (実際、ここ2年で公表から1週間以内に落とされている国内の事業者さんが何件か…)

  → 運用コストがものすごく高い

© 2016 Internet Initiative Japan Inc.

BINDの脆弱性

- 自社でDNSサーバをBINDで運用されている方は、即刻他のソフトウェアに乗り換えるべき
  - 権威DNS: nsd
  - キャッシュDNS: unbound
- 詳細はDNS Summer Day 2016での拙発表資料を御覧ください
  - BINDからの卒業
  - BIND辞められない理由Q&A

© 2016 Internet Initiative Japan Inc.

まとめ

© 2016 Internet Initiative Japan Inc.

まとめ

- DNSはインターネットの根本を支える重要サービス。止まると阿鼻叫喚。
- DNSを用いたorDNSへの攻撃は昔からある
- Open Resolverを用いた攻撃は20年前から存在し、数年前に大問題となった
- しかし、直近ではIoT機器を利用した攻撃にシフトしつつある
  - DNSを用いた攻撃は引き続き継続

© 2016 Internet Initiative Japan Inc.

まとめ

- ここ2年程、DNS水責め攻撃が流行しISPのキャッシュDNSサーバがサービス停止するなど、話題になった
  - 緩和策は実装されているものの、決め手となる対策はなし
- 攻撃者に本気で狙われたら割とどうしようもない

© 2016 Internet Initiative Japan Inc.

まとめ

- 共用の権威DNSサービスを利用している場合、他の顧客が狙われた際に巻添えを食らう可能性があるため、複数のサービス・自社運用を組合せるべき
- BINDはDoS脆弱性が頻繁に出て、運用コストが大変高いため、即刻他のソフトウェアに移行するべき

© 2016 Internet Initiative Japan Inc.

おまけ

- 弊社blog(てくろぐ)でIIJのDNSサービスをもう少し詳しく解説しています

  (偶然にも本日公開。執筆者は同僚です)

- よろしくければご覧ください。

  http://techlog.iij.ad.jp/archives/2135

© 2016 Internet Initiative Japan Inc.

IIJ Internet Initiative Japan

Any Questions?

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、 複製・翻案・公衆送信等できません。 IIJ、Internet Initiative Japanは、 株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、 商標または登録商標です。本文中では™、®マークは表示しておりません。
©2016 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。