DNS Security Update 2015

2016年1月31日
SECCON 2015 カンファレンス
株式会社日本レジストリサービス（JPRS）
森下 泰宏

講師自己紹介

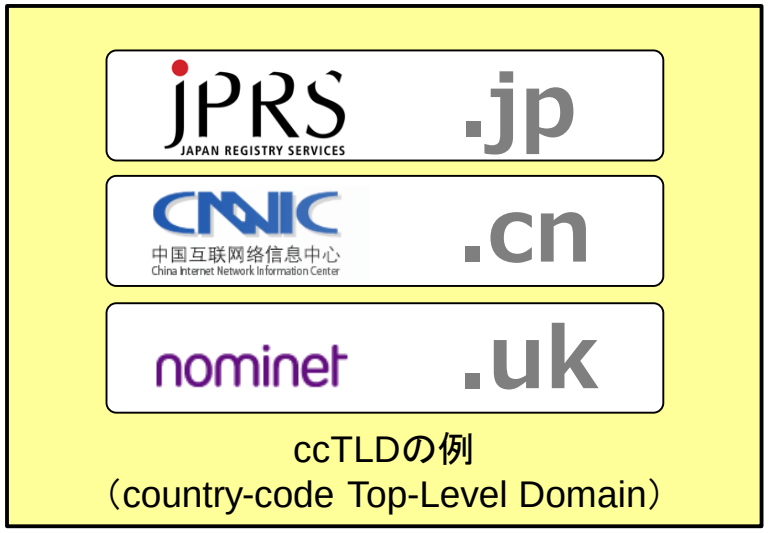
- 名前：森下 泰宏（もりした やすひろ）
  - 所属：株式会社日本レジストリサービス（JPRS）
  - 肩書：技術広報担当
- 主な業務内容：ドメイン名・DNSに関する技術情報をわかりやすく伝える
  - 技術情報の発信
  - 脆弱性に関する注意喚起の作成・公開など

JPRSとは？

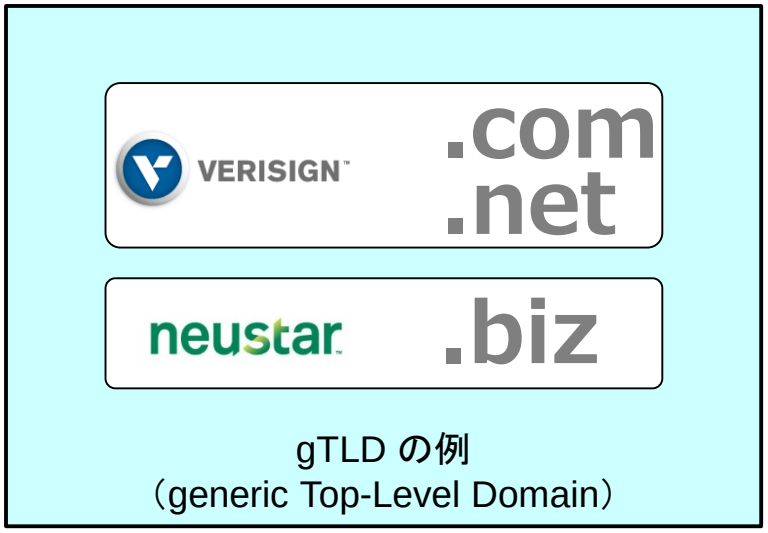
- 正式名：株式会社日本レジストリサービス
  - 英文名称：Japan Registry Services Co. Ltd.
  - 略称：JPRS（ジェーピーアールエス）
- 「日本」に割り当てられているccTLD「.jp」を管理
  - ccTLD：country-code Top-Level Domain
    - 国・地域ごとに割り当てられるトップレベルドメイン
  - 例：seccon.jp, jprs.co.jp, dendai.ac.jp, ...
- 「ドメイン名レジストリ」という組織の一つ
  - ドメイン名業界では単に「レジストリ」と呼ばれている

ドメイン名レジストリの役割

- あるTLD（.jp、.comなど）に対し、一つ存在
- 二つの重要な役割を持つ
  - ドメイン名登録の受け付けと登録情報の管理
  - TLDの権威DNSサーバーの管理運用



ccTLDの例
（country-code Top-Level Domain）



gTLD の例
（generic Top-Level Domain）

本日の内容

1. 2015年のDNSセキュリティの状況
2. 2015年のDNSセキュリティ関連トピックス
3. DNSとセキュリティに共通するもの

本資料は、SECCON公式Webで公開いただく予定です

1. 2015年の
DNSセキュリティの状況

全般的な状況

- 2014年からの状況が継続
  - DNS水責め攻撃
  - 登録情報の不正書き換えによるドメイン名ハイジャック
  - ホームルーターの脆弱性の悪用
- BINDの脆弱性を狙った攻撃による被害が、日本国内の複数のISPで発生

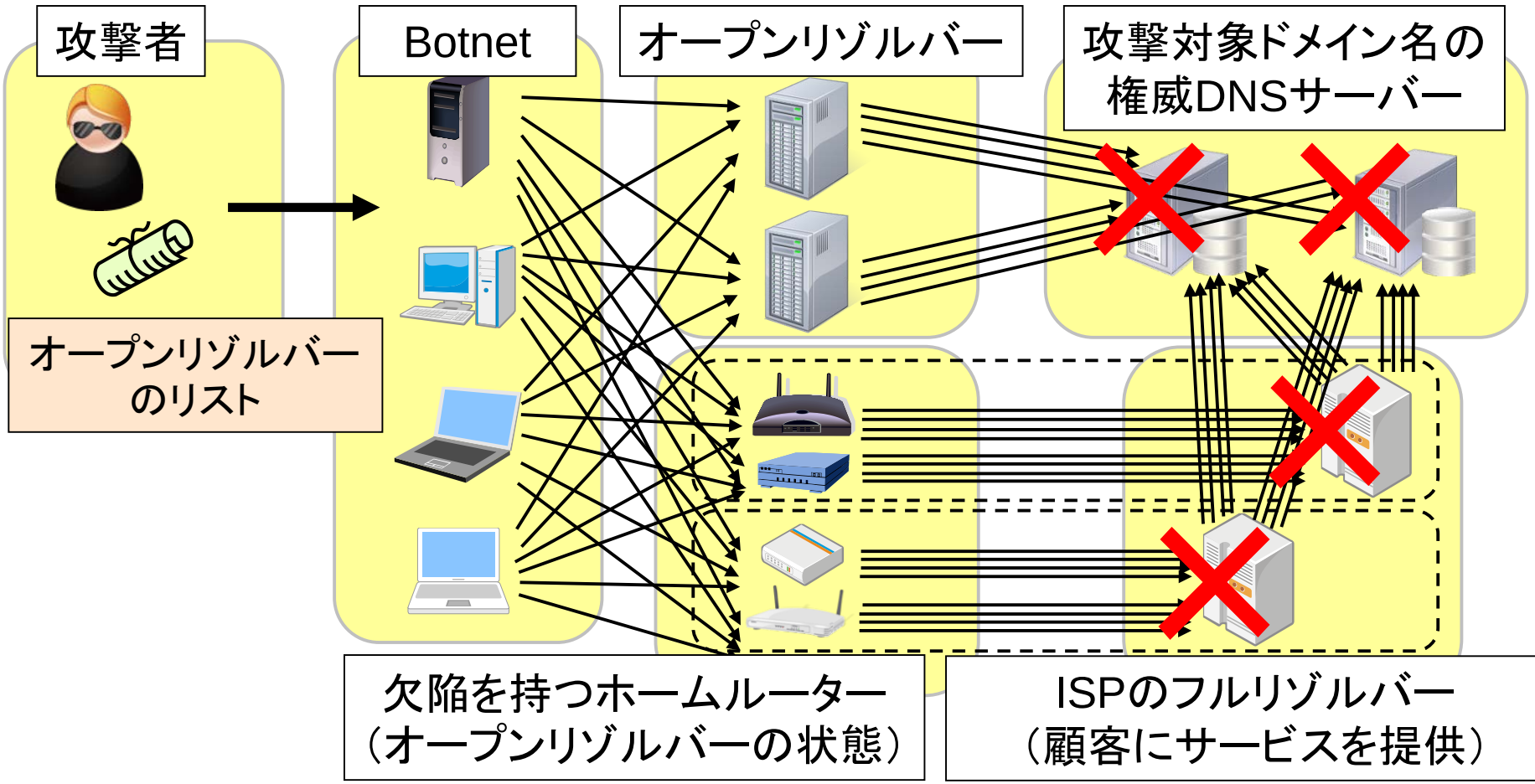
DNS水責め攻撃（攻撃事例）

- JPドメイン名が標的となった攻撃事例が発生（2015年2月）
  - 警察庁@police – インターネット観測事例等（平成27年2月期）
    <https://www.npa.go.jp/cyberpolice/topics/?seq=15932>
  - JPCERT/CC – インターネット定点観測レポート（2015年 1～3月）
    <https://www.jpcert.or.jp/tsubame/report/report201501-03.html>
- 国内のDNSサービスにおいて、巻き添えの被害が発生

今回のDNS水責め攻撃の対象となった国内ドメインは、国内のドメイン登録代行事業者が運用する権威DNSサーバに登録されていました。この権威DNSサーバは、国内でも利用者数の多い複数のサイトのドメインを管理していました(以下、複数ドメインを管理する権威DNSサーバを「共有DNSサーバ」という。)。このため攻撃により国内の共有DNSサーバに過剰な負荷が上がることで、**対象となった国内ドメインだけではなく、同一の共有DNSサーバで管理されていた複数のドメイン(クラウドを使用したサービスを提供している事業者やオンラインゲームなど)も名前の解決ができなくなり、Webサイトが閲覧できない、メールが受け取れないなどの問題が発生していた**と推測されます。

（JPCERT/CC「インターネット定点観測レポート（2015年1～3月）」より引用）

DNS水責め攻撃の仕組み



問い合わせが集中する攻撃対象ドメイン名の権威DNSサーバーや
ISPのフルリゾルバーが過負荷になり、サービス不能状態に陥る

DNS水責め攻撃（対応状況）

- 関係者の努力と対策により、影響（被害）の規模は2014年に比べ抑え込まれた
  - ISPにおける攻撃の早期検知・対応
  - 負荷分散、サーバー・ネットワークインフラの強化
  - オープンリゾルバーを減らすための地道な努力
  - ISP顧客向けアクセス網へのIP53B（*）の導入（後述）

（*）Inbound Port 53 Blockingの略称。
顧客側の53/udp（DNSのポート番号）へのアクセスをISP側でブロックすること。

DNS水責め攻撃（対応状況）

- 攻撃対策として、IP53Bを導入するISPが増加
  - ソフトバンク（2015年5月11日）
    - DNSアンプ攻撃対策実施のご案内
      <http://www.softbank.jp/mobile/info/personal/news/support/20150511a/>
  - BIGLOBE（2015年8月6日）
    - 一部ポートの通信規制によるセキュリティ強化について
      <http://support.biglobe.ne.jp/news/news470.html>
  - 朝日ネット（2015年12月14日）
    - 【第2報】障害に関するお詫びとご報告
      <http://asahi-net.jp/support/news/20151214_02_ja.pdf>

固定IPアドレスの顧客にも導入
（申請によるOpt-Out方式）

通信の秘密の保護の観点から、導入には慎重な検討が必要

登録情報の不正書き換えによるドメイン名ハイジャック（攻撃事例）

- 最近の主な攻撃事例（2014年1月～）

年月	対象TLDレジストリ、レジストラ
2014年1月	.me（モンテネグロ）
2014年2月	MarkMonitor（facebook.comなど、登録情報には被害なし）、.uk（英国）
2014年9月～10月	Network Solutions（nikkei.com）、eNom（st-hatena.com）
2014年10月	.id（インドネシア）、.qa（カタール）
2014年11月	Network Solutions（craigslist.org）、GoDaddy（gigya.com）
2014年12月	.ca（カナダ）

年月	対象TLDレジストリ、レジストラ
2015年1月	WebNIC（malaysiaairlines.com）
2015年2月	.vn（ベトナム）、WebNIC（lenovo.com）
2015年4月	.my（マレーシア）、Network Solutions（teslamotors.com）
2015年7月	.ma（モロッコ）、.pn（ピトケアン諸島）

注：JPRSにおいて把握しているもののみ

攻撃の概要・仕組みについてはSECCON 2014カンファレンスの発表資料を参照

DNSセキュリティ最新動向 ～対策の基本と最近の攻撃手法～
<http://2014.seccon.jp/conference/20150207-dnssecurity.pdf>

事例：malaysiaairlines.com、lenovo.comなど（2015年1月～2月）

- レジストラWebサイトに対するコマンドインジェクション攻撃により、rootkitをアップロードされた旨の報告あり
  - Lenovo.com hijack reportedly pulled off by hack on upstream registrar

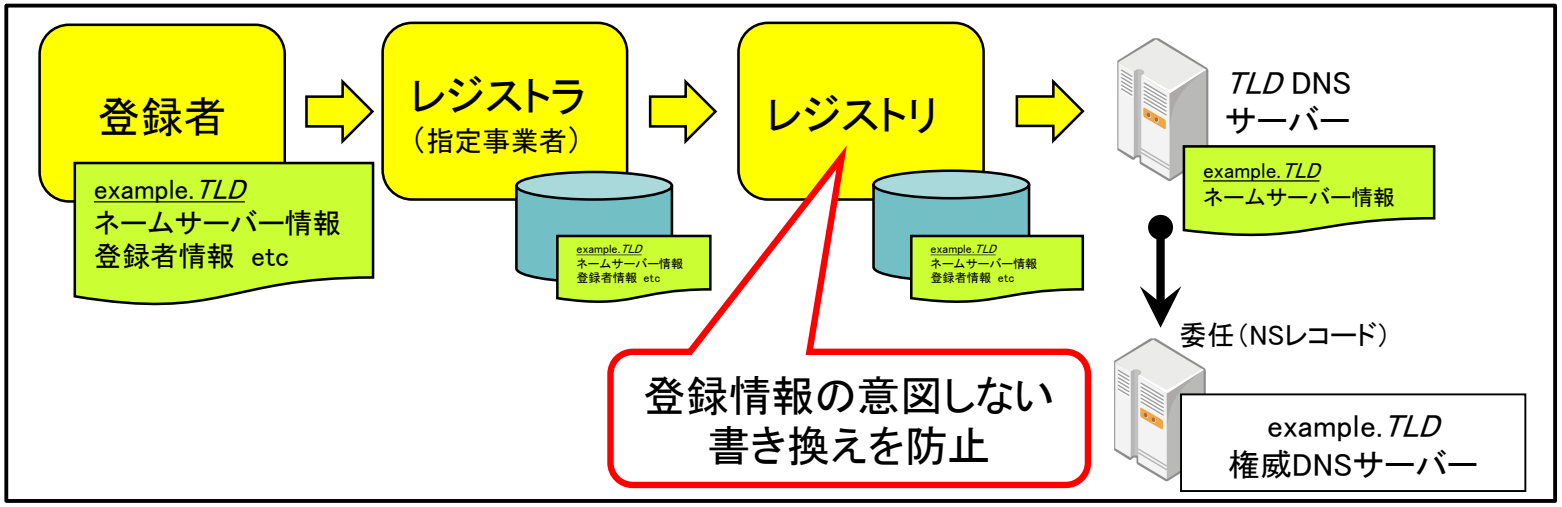
    <http://arstechnica.com/security/2015/02/lenovo-com-hijack-reportedly-pulled-off-by-hack-on-upstream-registrar/>
- この攻撃により、当該レジストラは数日間にわたり業務停止の状態に陥った

事例：teslamotors.com（2015年4月）

- レジストラのアカウントリカバリ機能の不備を悪用
  - Tesla、ウェブとTwitterアカウントを同時に乗っ取られる（復旧済み）
    - <http://jp.techcrunch.com/2015/04/27/20150425teslas-site-and-twitter-account-hacked/>
- 攻撃者はドメイン名に加え、同社のTwitter公式アカウントの乗っ取りにも成功
  - Twitterのパスワードリセット機能を悪用
  - ドメイン名を乗っ取った後、Twitter公式アカウントのパスワードを故意にリセットしてteslamotors.com宛の電子メールを送信させ、そのメールを盗難

登録情報の不正書き換えによるドメイン名ハイジャック（対応状況）

- レジストリロックの導入が進行
  - 登録情報の意図しない書き換えを防止する仕組み
  - 一部TLDにおいて、オプションサービスとして提供
- レジストリロックに対応しているTLD（JPRS調べ）
  - gTLD：.biz、.com、.name、.net、.org
  - ccTLD：.at、.be、.ca、.ch、.cc、.eu、.fr、.is、.jp、.li、.nl、.se、.tv、.uk、.us

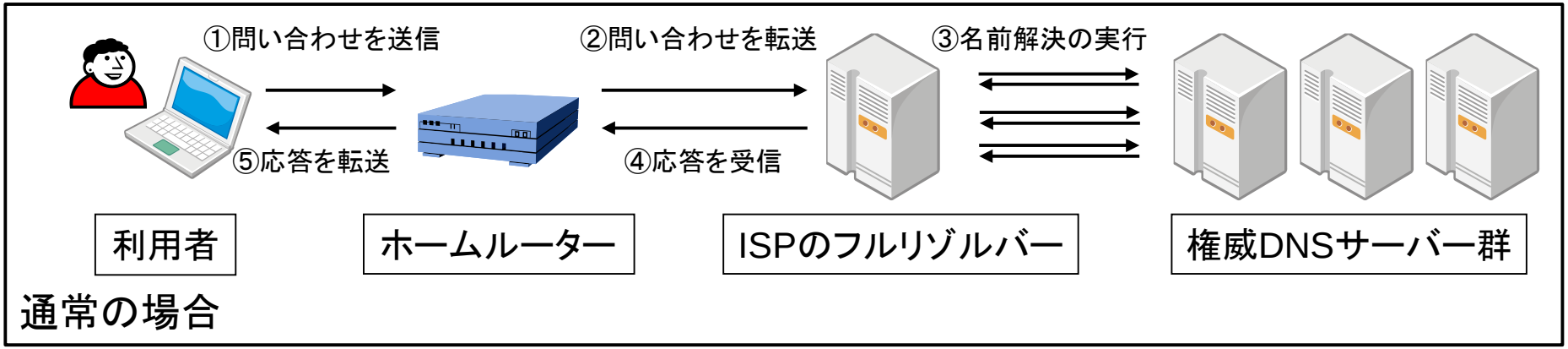


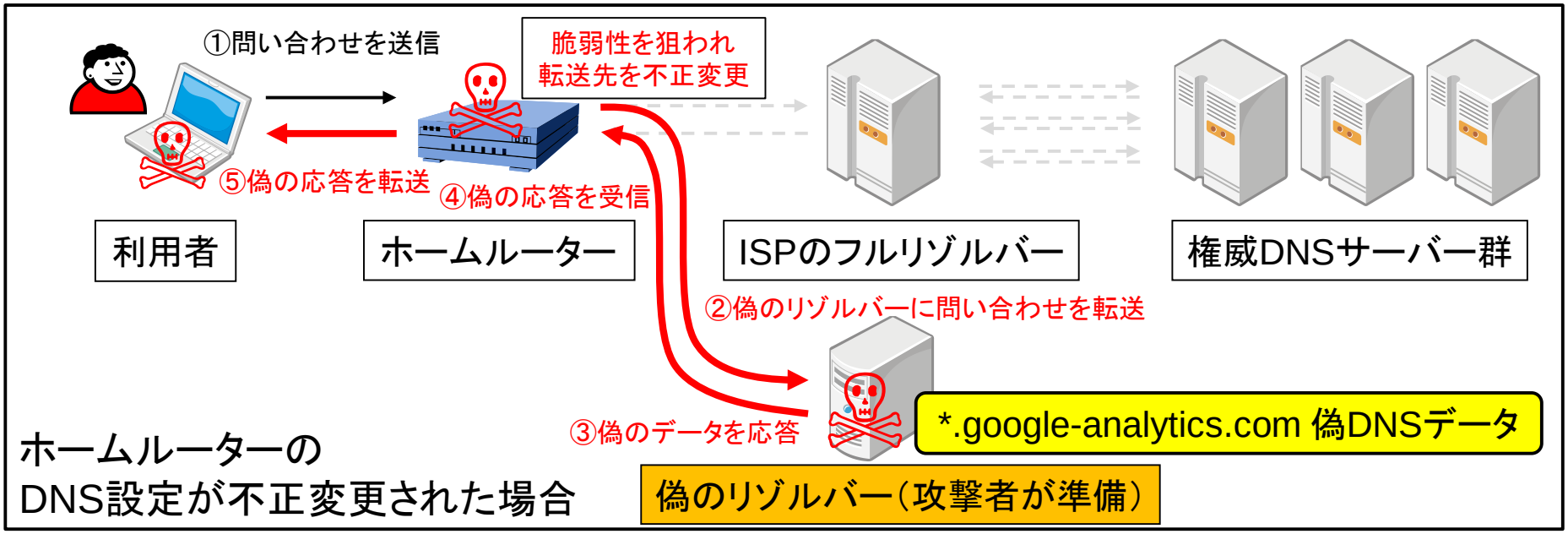
ホームルーターの脆弱性悪用（攻撃事例）

- 不適切な広告の挿入を図った事例（2015年3月）
  - Ad-Fraud Malware Hijacks Router DNS – Injects Ads Via Google Analytics

    <https://sentrant.com/2015/03/25/ad-fraud-malware-hijacks-router-dns-injects-ads-via-google-analytics/>
  - 特定のホームルーターに存在する既知の脆弱性を悪用、攻撃者が準備した偽のリゾルバーにDNS問い合わせを誘導
    - *.google-analytics.comのIPアドレスを偽物に差し替えてWebアクセスを偽サーバーに誘導、不適切な広告を挿入
    - コンテンツ書き換えが広告のみ ⇒ 不正が露見しづらい

攻撃の仕組み（DNS転送先の不正変更）





BINDの脆弱性（2015年の状況）

- 7件の脆弱性が公開

ISCにおける文書公開日	CVE-ID	Severity（深刻度）
2015年2月18日	CVE-2015-1349	High（高）
2015年7月7日	CVE-2015-4620	Critical（重大）
2015年7月28日	CVE-2015-5477	Critical（重大）
2015年9月2日	CVE-2015-5986	Critical（重大）
2015年9月2日	CVE-2015-5722	Critical（重大）
2015年12月15日	CVE-2015-8000	Critical（重大）
2015年12月15日	CVE-2015-8461	Medium（中）

- 国内の複数のISPにおいて、CVE-2015-5477による攻撃の被害が発生（2015年7月）

CVE-2015-5477（2015年7月）

- （緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2015年7月31日更新）
  <http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html>
- TKEYリソースレコードの取り扱いの不具合
- PoCが出回り、国内の複数ISPにおいて被害が発生
- 特徴：

① リモートからのDNS問い合わせ一発でnamedを落とせる
② 多くのバージョンのBINDが対象となる
③ 権威DNSサーバー・フルリゾルバーの双方が対象となる
④ namedの設定やオプションでは回避できない

速やかなパッチの適用を！

2. 2015年のDNSセキュリティ関連トピックス

本日解説する事件・出来事（1/2）

- Rubyのgem installにおける名前衝突
- megaupload.comのNS更新忘れ
- QRコードのアクセス先がポルノサイトに
- .onionが特殊用途ドメイン名として予約
- 「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」の改定

本日解説する事件・出来事（2/2）

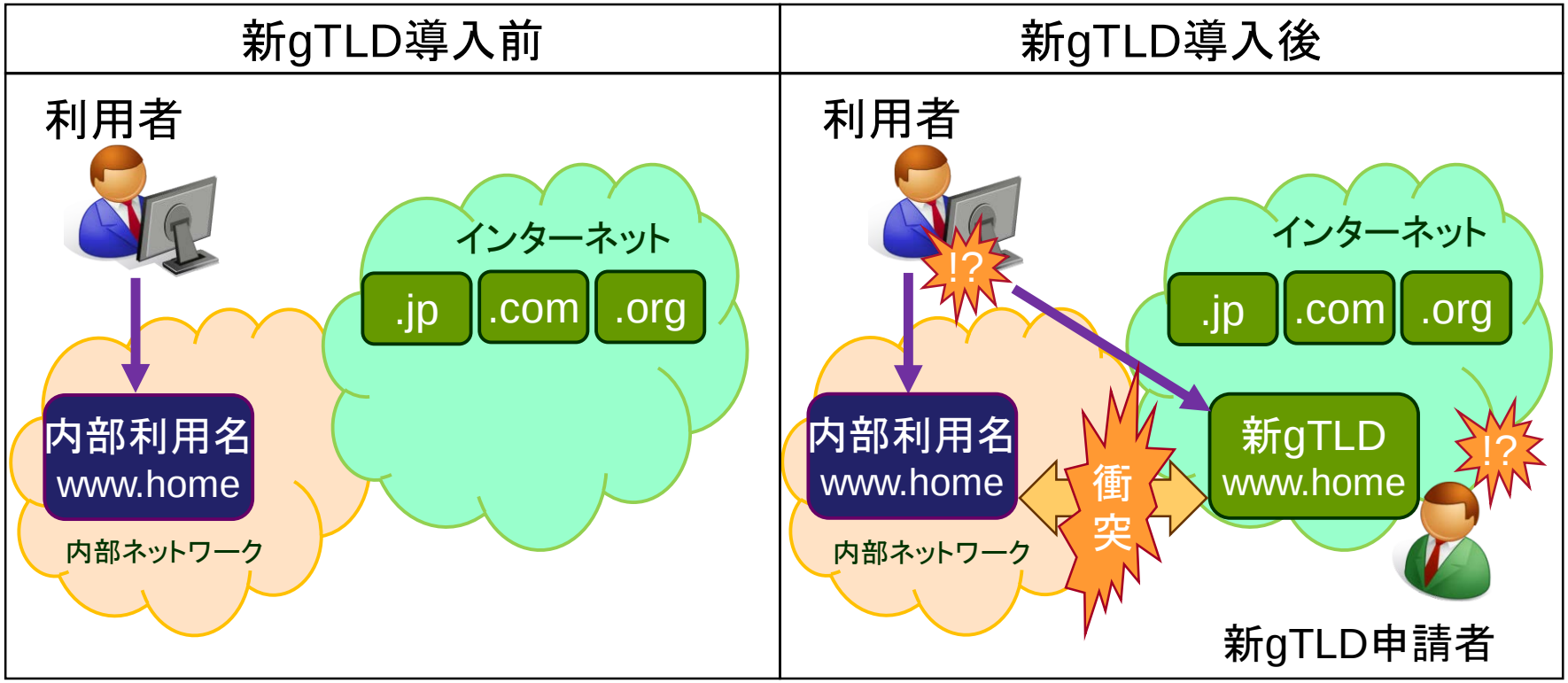
- ルートサーバーへの大量問い合わせ
- ソースポートランダマイゼーションが不十分なホームルーターが複数報告される
- ゾーン転送の設定不備に関する注意喚起

Rubyのgem installにおける名前衝突（2015年1月）

- RubyGems（Ruby言語用のパッケージ管理システム）において、名前衝突による障害が発生
  - .dev で終わる hostname のとき gem install が（ある条件で）失敗するようになった
    <http://uasi.hatenablog.com/entry/2015/01/07/225351>
  - .devは2014年12月18日にルートゾーンから委任
- 一部コミュニティにおいて、開発環境に.devで終わるホスト名（内部利用名）を付ける慣習があった
  - powやinvokerなどにもあるとのこと（伝聞）

参考：名前衝突とは

- 内部利用目的で使われている名前（内部利用名）が、インターネットのドメイン名と衝突すること
  - 新gTLDの導入により問題が顕在化



megaupload.comのNS更新忘れ（2015年5月）

- megaupload.comがドメイン名ハイジャックされ、ポルノ・マルウェア・詐欺サイトへのリンクが表示される状態になっていた
  - Porn and adware found on former FBI web domains
    <http://www.bbc.com/news/technology-32929309>
- megaupload.comは2012年にFBIが押収
- 原因：NSに指定していたcirfu.netの更新忘れ

megaupload.com.	IN	NS	ns6.cirfu.net.
megaupload.com.	IN	NS	ns5.cirfu.net.

当時の設定内容（現在は変更済み）

QRコードのアクセス先がポルノサイトに（2015年6月）

- ドイツのハインツのケチャップに印刷されていたQRコードのドメイン名が期限切れとなっており、ポルノサイトに変わっていた
  - Heinz QR porn code too saucy for ketchup customer
    <http://www.bbc.com/news/technology-33200142>
  - 購入者からのクレームを受け、ハインツ社が謝罪
- ドメイン名は「sagsmitheinz.de」
  - 英語で「Say it with Heinz」の意味
  - キャンペーン用サイトだったとのこと
    - キャンペーン期間は2012～2014年
  - 現在は売り出し中である旨のページが表示

.onionが特殊用途ドメイン名として予約（2015年9月）

- 特殊用途ドメイン名とは？
  - RFC 6761: Special-Use Domain Names
    <https://www.ietf.org/rfc/rfc6761.txt>
  - プライベートアドレスの逆引き（10.in-addr.arpaなど）、例示用ドメイン名（example.{com,net,org}）、.localなど、特殊な用途のドメイン名をIANAが予約
- 一覧をIANA Webで公開
  - Special-Use Domain Names
    <https://www.iana.org/assignments/special-use-domain-names/special-use-domain-names.xhtml>

.onionが特殊用途ドメイン名として予約（2015年9月）

- RFC 7686: The ".onion" Special-Use Domain Name
  <https://www.ietf.org/rfc/rfc7686.txt>
- .onionのTor以外での使用・登録・設定を禁止
  - 名前解決API・ライブラリ・リゾルバーは.onionを特別扱いし、Torの処理を行うこと（MUST）
    - Torを使っていなければエラーとし、名前解決をしないこと
    - OSの名前解決ライブラリなどに影響あり
  - フルリゾルバー（キャッシュDNSサーバー）では.onionの名前解決をしないこと（SHOULD）
    - ルートサーバーやネットワークに情報が漏洩することを防止
    - プライベートアドレスの逆引きなどと同様、空のゾーンを設定する必要あり

「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」の改定（2015年11月）

- JAIPAなど5団体が公開するガイドライン
  - 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン（第4版）
    <https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf>
  - 2015年11月30日に第4版が公開
- ガイドラインの目的（第4版 第1条より引用）

本ガイドラインでは、遮断等を始めとするサイバー攻撃等や電気通信役務の不正享受への対処が、**通信の秘密の侵害に該当しうるのか否か、また、通信の秘密の侵害に該当したとしても、違法性が阻却されうるのか否かについて、基本的な考え方を整理する**と共に、該当する事例を挙げることにより、電気通信事業者におけるサイバー攻撃等や電気通信役務の不正享受への対処の参考に資するものである。（中略）また、**本ガイドラインに記述されているものであっても、個々の判断は実際の状況に応じて個別になされるべきものである**。

第4版における改正点（DNS関連）

- DNS水責め攻撃対策を想定した項目の追加

  DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、リストに基づいて、FQDNが一致する場合に当該名前解決要求に係る通信を遮断することについて追加しました。

- 欠陥を持つホームルーターを保有する顧客に対する注意喚起を想定した項目の追加

  リフレクション攻撃に悪用され得る脆弱性やPPPoE認証の情報を窃取され得る脆弱性を有するブロードバンドルータを、ネットワーク上で調査し、契約者の接続ログから、当該ブロードバンドルータを保有している契約者を特定し、契約者に対して注意喚起することについて追加しました。

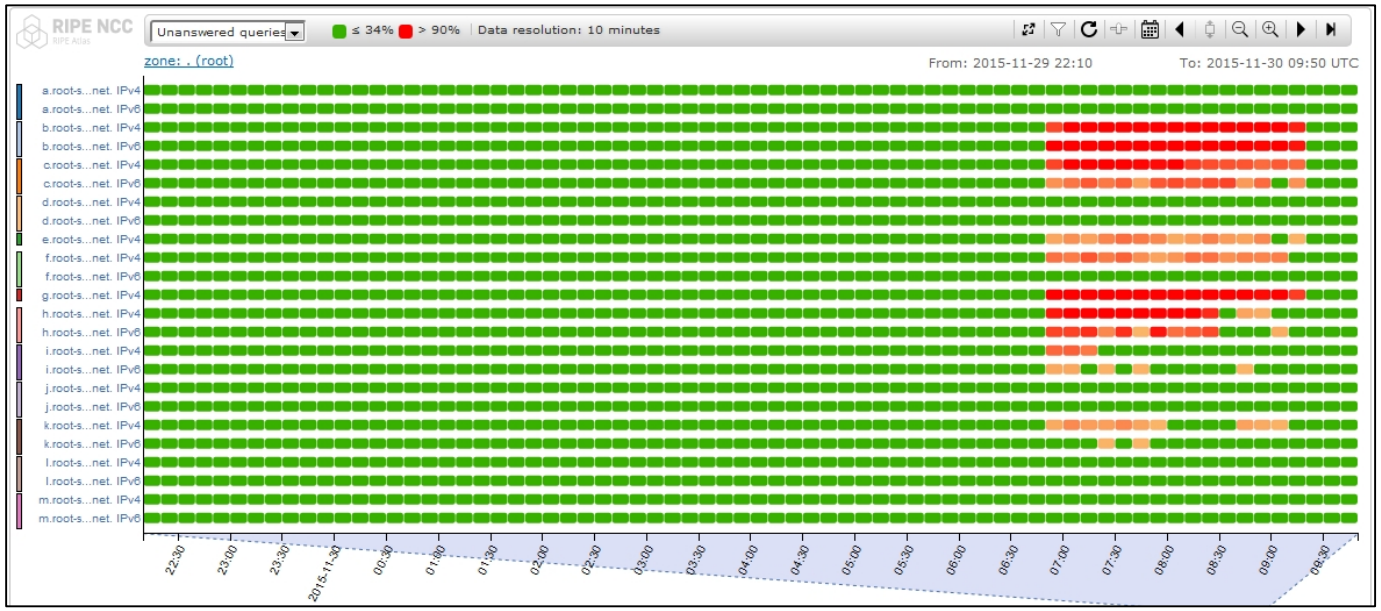
- マルウェアの制御用通信の遮断を想定した項目の追加

  C&Cサーバ等との通信の遮断における有効な同意として、個別の同意を取得していない場合であっても、契約約款等に基づく事前の包括同意として、マルウェア感染端末とC&Cサーバ等との通信をレピュテーションDBに基づいて遮断することについて追加しました。

電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインの改定について <https://www.jaipa.or.jp/topics/2015/11/post.php> より引用

ルートサーバーへの大量問い合わせ（2015年11～12月）

- 2015年11月30日と12月1日に、複数のルートサーバーで「高いレートの問い合わせ（a high rate of queries）」を受信
  - Events of 2015-11-30
    <http://www.root-servers.org/news/events-of-20151130.txt>
- 複数のルートサーバーノードのサービスに影響（数時間）



RIPE DNSMON <https://atlas.ripe.net/dnsmon/> による観測結果（2015年11月30日分）

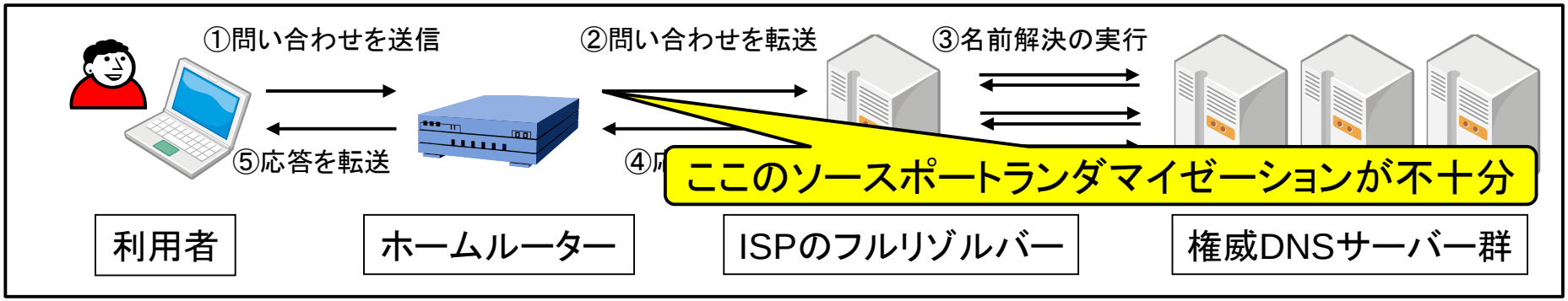
ルートサーバーへの大量問い合わせ（2015年11～12月）

- ルートサーバーオペレーターからの状況報告
  - K-root DNS Service Incident
    <https://www.ripe.net/support/service-announcements/k-root-dns-service-incident>
  - Verisign’s Perspective on Recent Root Server Attacks
    <http://blogs.verisign.com/blog/entry/verisign_s_perspective_on_recent>
- 問い合わせ元のIPアドレスが偽装されていた
  - BCP 38（*）を導入していたISPは送信元とならず、結果的にそのネットワークの利用者が使うルートサーバーのノードは生き残った旨の証言あり
    - [dns-operations] Storm on the DNS
      - <https://lists.dns-oarc.net/pipermail/dns-operations/2015-December/013933.html>

（*）送信元を偽装したIPパケットの送信を防ぐ手法の一つ。RFC 2827 (BCP 38)で定義。

ソースポートランダマイゼーションが不十分なホームルーターが複数報告される（2015年12月）

- 米国The CERT Divisionの研究者が報告
  - Buffalo AirStation Extreme N600 Router WZR-600DHP2 uses insufficiently random values for DNS queries
    <https://www.kb.cert.org/vuls/id/646008>
- 国内ベンダーのホームルーターを含む
  - DNS偽装の脆弱性
    <http://buffalo.jp/support_s/s20151211.html>
    - ファームウェアの更新を呼びかけ



ゾーン転送の設定不備に関する注意喚起（2016年1月）

2016年の話題

- JPCERT/CC、JPNIC、JPRSが注意喚起を公開（2006年1月12日）
  - DNS ゾーン転送の設定不備による情報流出の危険性に関する注意喚起
    <https://www.jpcert.or.jp/at/2016/at160002.html>
  - 権威DNSサーバにおけるゾーン転送の設定に関する注意喚起
    <https://www.nic.ad.jp/ja/topics/2016/20160112-01.html>
  - 権威DNSサーバーの設定不備による情報流出の危険性と設定の再確認について
    <http://jprs.jp/tech/security/2016-01-12-unauthorized-zone-transfer.html>
- JPRSでは設定ガイドも併せて公開
  - 設定ガイド：ゾーン転送要求への応答を制限するには【BIND編】
    <http://jprs.jp/tech/notice/2016-01-12-fixing-bind-zonetransfer.html>

BINDはデフォルトですべてのゾーン転送を許可することに注意

3. DNSとセキュリティに共通するもの（本日のまとめに替えて）

「DNS」と「セキュリティ」の共通点

- 関係者間の連携・協調が必要不可欠
  - DNSというプロトコルそのものが持つ特徴でもある
- さまざまな分野の知識・知見・経験が必要
  - 次世代への技術の伝承も重要なポイント
- 状況を良くするためには、
  すべての関係者の地道な努力が必要不可欠

たぶんわれわれはもっと強く、たくましくなる必要がある

自分にも言っています

参考リンク（JPRSからの技術情報発信）

- DNS関連技術情報
  <http://jprs.jp/tech/>
- メールマガジン「FROM JPRS」
  <http://jprs.jp/mail/>
- JPRSトピックス&コラム
  <http://jprs.jp/related-info/guide/>
- ドメイン名関連会議報告
  <http://jprs.jp/related-info/event/>

That’s it!