Security Issuesへの取り組みと対応
—「ちゃんと」「きちんと」伝えるためにできること—
～キャッシュポイズニングの手法を題材に～

2014年7月17日

JANOG34 Meeting

株式会社日本レジストリサービス（JPRS）

森下 泰宏（Yasuhiro Orange Morishita）

簡単な自己紹介

- 氏名: 森下 泰宏（もりした やすひろ）
  - 勤務先：株式会社日本レジストリサービス
  - 肩書: 技術広報担当
  - 別名：「重複をお許しくださいの人」
    - 決して正式名（CNAME）ではありません・・・
- ささやかな願いごと: 平穏無事な7月
  - 今年はどうなるでしょうか・・・

キャッシュポイズニングの「新手法」？

- 中京大学の鈴木常彦教授による解説
  - キャッシュポイズニングの開いたパンドラの箱 -1-
    <http://www.e-ontap.com/dns/endofdns.html>
  - キャッシュポイズニングの開いたパンドラの箱 -2-
    <http://www.e-ontap.com/dns/endofdns2.html>
- FACTA 2014年6月号 掲載記事
  - 「打つ手なし『jpドメイン』攻撃」

本件に関するわれわれの認識①

- 本件はDNSにおける「Security Issues」の一つ
  - 「Security Incident」になりうる事項
- 対象はJPドメイン名/JPRSのみにとどまらない
  - 他の多くのTLDやルートゾーンも同様の状況にある
  - 各組織におけるDNS運用にも影響を及ぼす
  - 逆引きDNSも同様の状況にある

本件に関するわれわれの認識②

- 本件の影響は、DNSのプロトコル・実装・運用のすべてに及ぶ
  - 問題の解決には各関係者との調整・働きかけ・協働と、プロトコル改善を含む中長期的な取り組みが必要になる
- 本件は新しい問題ではない
  - この問題は2008年に発表されたものであり、既に複数の対策・緩和策が提案・実装されている
  - ソースポートランダマイゼーションと攻撃の検知・対応を確実に実施することで、当面の危険を回避できる
  - 安全性を更に高めるための対策も提案・実装されている

われわれは「ちゃんと」「きちんと」対応できたのか

- 最初に本件について連絡を受けた2014年2月15日から、本日に至るまでのわれわれの取り組みについて、順を追ってご紹介します
- Security Issuesへの取り組み・対応例の一つとして、問題解決に向けた忌憚のないご意見・ご議論をいただければ幸いです

以降の内容

- 今回の攻撃手法の概要
- 今回の件に関するJPRSの対応
- 気になる「あのこと」
  - なぜ、攻撃手法の広報を控えてきたのか？
  - co.jpなどにTXTレコードを追加した理由は何か？
  - jpとdns.jpを別居した理由は何か？
- まとめと今後の議論に向けて

今回の攻撃手法の概要

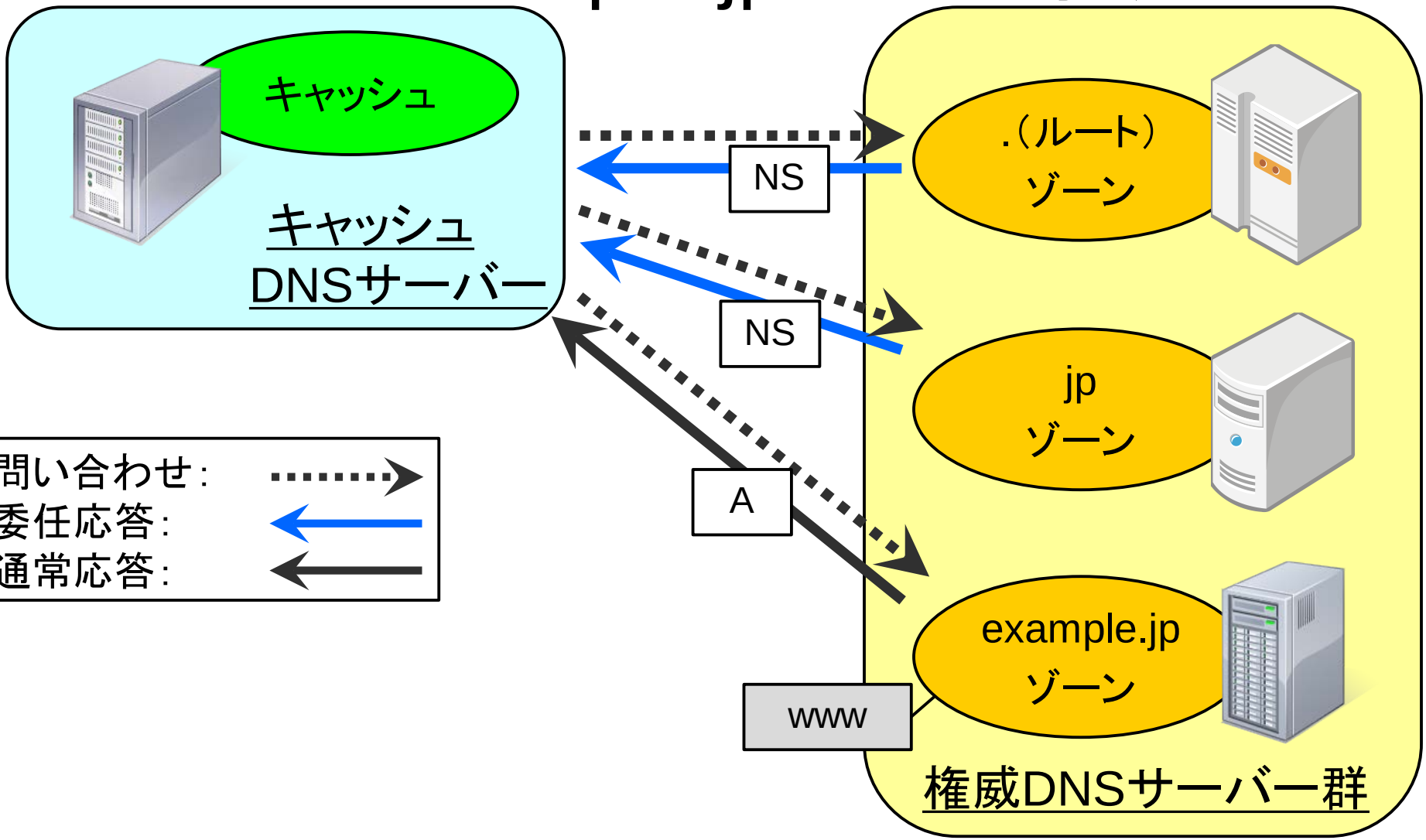
今回の攻撃手法

- 以下の二種類
  1. 「委任インジェクション攻撃」とJPRSが名づけたもの
  2. 「移転インジェクション攻撃」と中京大学の鈴木常彦教授（以下、鈴木先生）が名づけたもの
- 共通する特徴：注入対象がNSレコードである
  - ただし、攻撃成立の原理が異なっている

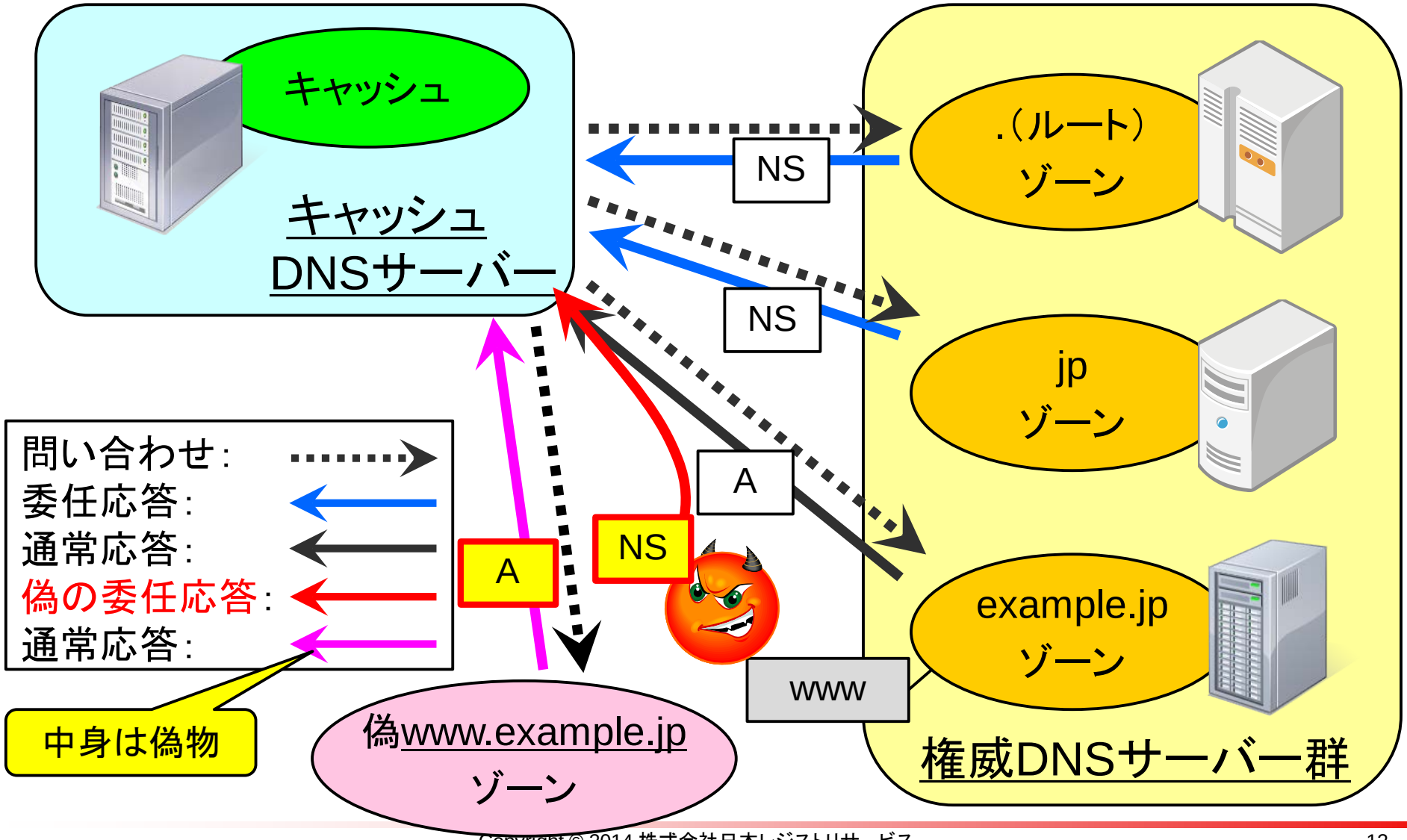
委任インジェクション攻撃（Delegation injection attacks）

- 2008年8月にBernhard Müller氏が公開した「Node re-delegation（ノード再委任）」が初出
  - Improved DNS spoofing using node re-delegation
    <https://www.sec-consult.com/fxdata/seccons/prod/downloads/whitepaper-dns-node-redelegation.pdf>
  - カミンスキー型攻撃手法が公開された翌月
- 英語版Wikipediaでも紹介
  - DNS spoofing
    <http://en.wikipedia.org/wiki/DNS_spoofing#Redirect_the_NS_record_to_another_target_domain>

おさらい：名前解決の流れ（www.example.jpの名前解決）

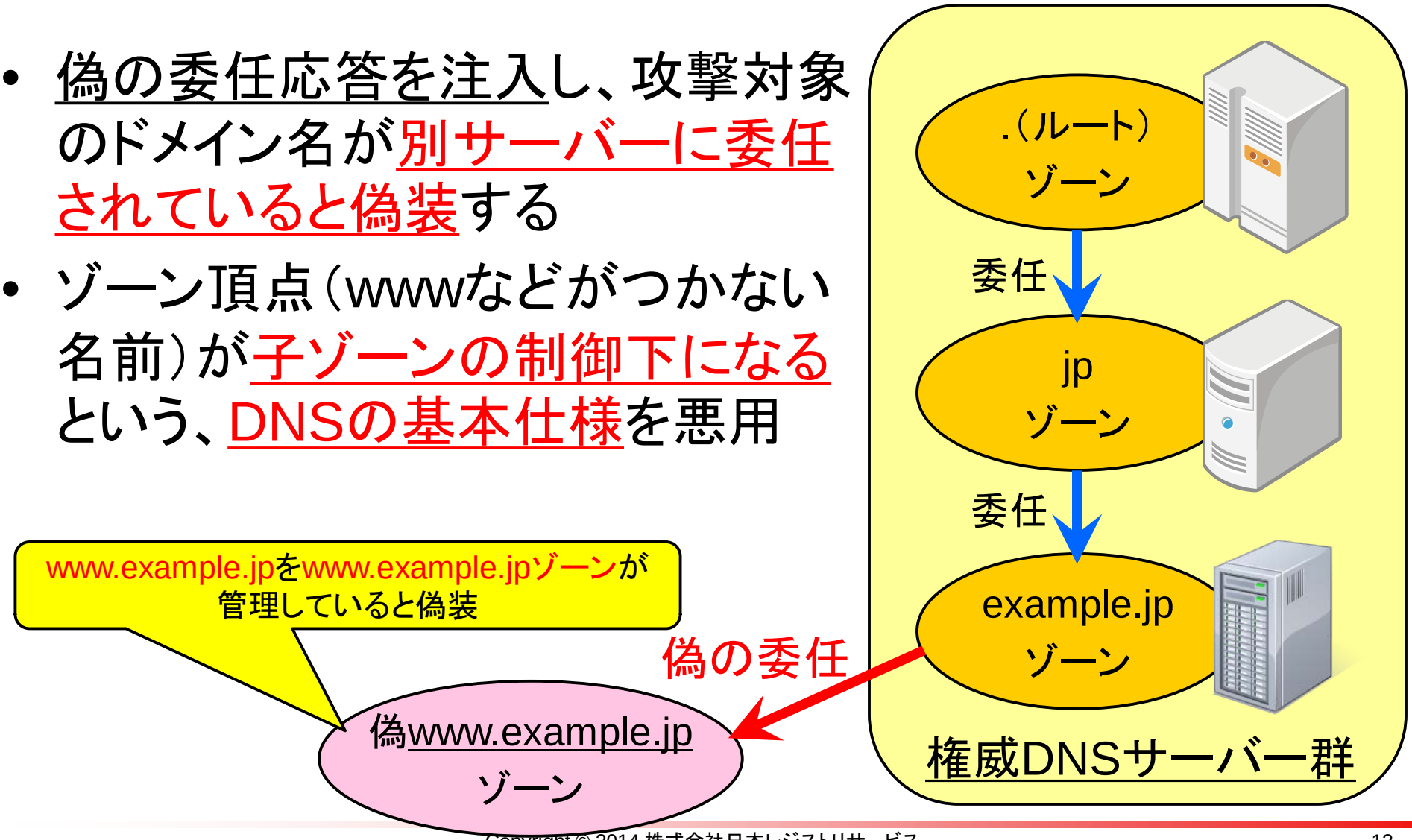


委任インジェクション攻撃の原理



委任インジェクション攻撃のしくみ

- 偽の委任応答を注入し、攻撃対象のドメイン名が別サーバーに委任されていると偽装する
- ゾーン頂点（wwwなどがつかない名前）が子ゾーンの制御下になるという、DNSの基本仕様を悪用



もう一つの攻撃手法：移転インジェクション攻撃

- 偽の委任応答ではなく、通常応答を注入
- 通常応答に付随するNSレコードにより、キャッシュ済みNSレコードの無効化（上書き）を図る
- 二つの疑問：
  - なぜ、通常応答でNSレコードの注入が可能なのか？
  - 「キャッシュ済みNSレコードの上書き」とは何か？

通常応答に付随するNSレコード

- DNSでは、問い合わせに対する応答（A/AAAAなど）と共に、NSレコードも返される（下記参照）
  - 意味：自分のゾーンの権威DNSサーバーの一覧

```
$ dig +norec +noedns www.example.jp a @ns1.example.jp
…
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; ANSWER SECTION:
www.example.jp.         86400   IN      A       192.0.2.100
;; AUTHORITY SECTION:
example.jp.             86400   IN      NS      ns1.example.jp.
example.jp.             86400   IN      NS      ns2.example.jp.
;; ADDITIONAL SECTION:
ns1.example.jp.         86400   IN      A       192.0.2.1
ns2.example.jp.         86400   IN      A       192.0.2.10
```

このNSレコードの意味（実社会における例え）

- 例：まんじゅう屋さんでお買い物

まんじゅう屋さんがまんじゅうと一緒に、同じまんじゅうを売っている支店の一覧が書かれた紙も渡してくれた

ということに相当し、

- 現在のDNSの仕様では、

まんじゅう屋さん自身からもらった紙の内容が、まんじゅう屋さんの場所を教えてくれた人からもらった紙の内容よりも優先される

と定められている

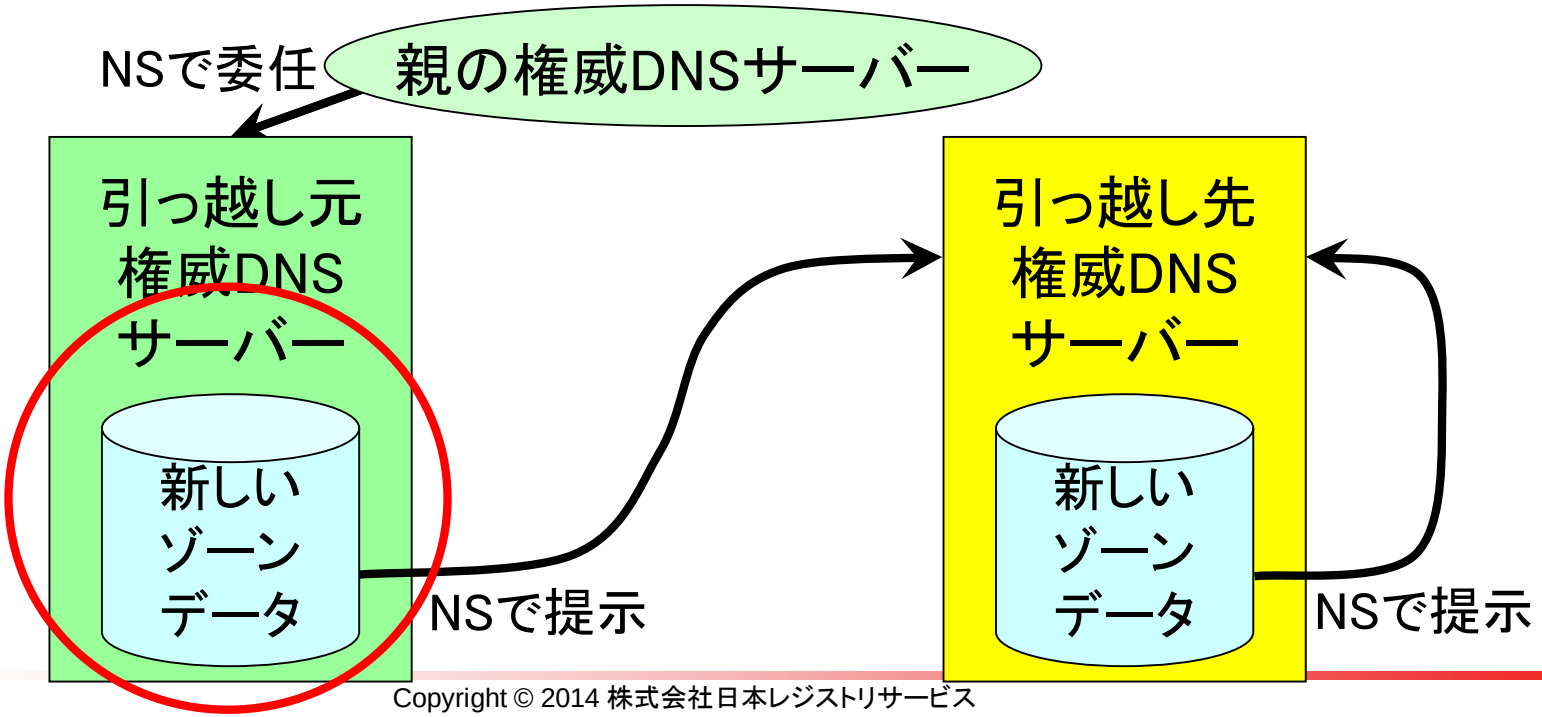
新規開店して支店が増えてるかもしれないし、
閉店して減ってるかもしれないし・・・

NSレコードは子のものが優先

- DNSの仕様により、子の通常応答経由で受け取ったNSレコードは、親の委任応答経由で受け取ったNSレコードよりも優先される
  - DNSの仕様では、子のNSレコードのみが権威を持つ
- かつ、BIND 9では親から受け取ったNSレコードのキャッシュが、子から受け取ったNSレコードにより上書きされる
  - 上書きされるのはBIND 9に固有の事項（実装の問題）
    - RFC 2181 5.4.1では「additional information」の上書きのみが記述されている

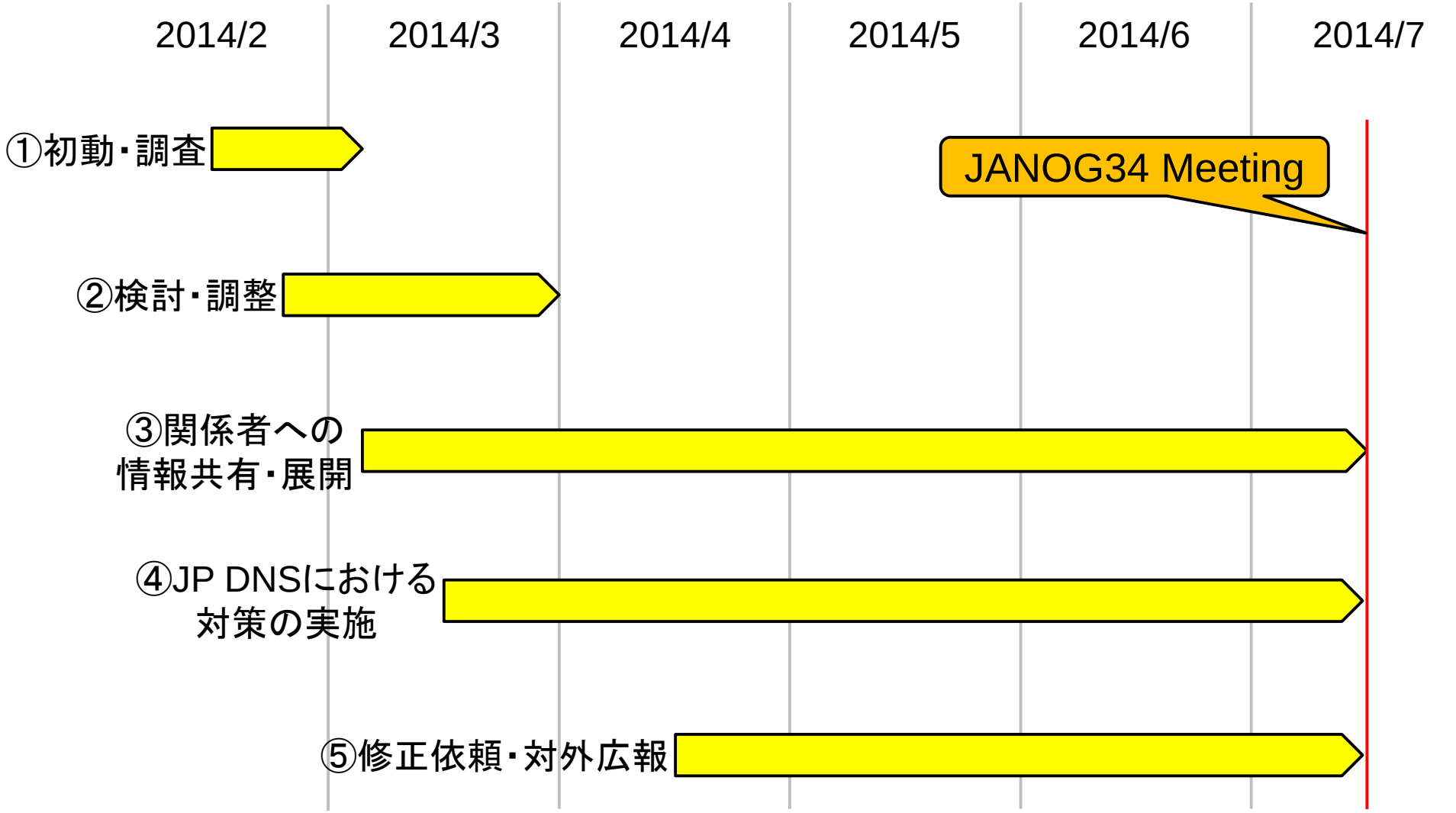
「移転インジェクション」という名前の由来について

- 権威DNSサーバーの引っ越し作業の途中において現れるDNS応答と同様であるため、と推測
- だとしたら、「移転通知インジェクション」の方が、名称としてより適切な気がします



今回の件に関するJPRSの対応

全体のタイムライン



①初動・調査（2/15～3/4）

- 前野年紀氏（以下、前野氏）から連絡を受け取る（2/15）
- 社内展開開始（2/18～）
  - 技術検証により再現性を確認
  - 問題認識を社内共有
    - プロトコル・実装・運用のすべてに影響を及ぼすこと
    - 世界的な調整・対策が必要になること
  - 重要課題として全社的に取り組むことを決定（2/21）
- 影響範囲の調査（2/21～）
  - 他TLDの設定状況調査
  - 考えうる対策の調査
- 関係者の洗い出し・コンタクトリストの作成（～3/4）

インターネットの発展にご協力いただき、
改めてありがとうございました

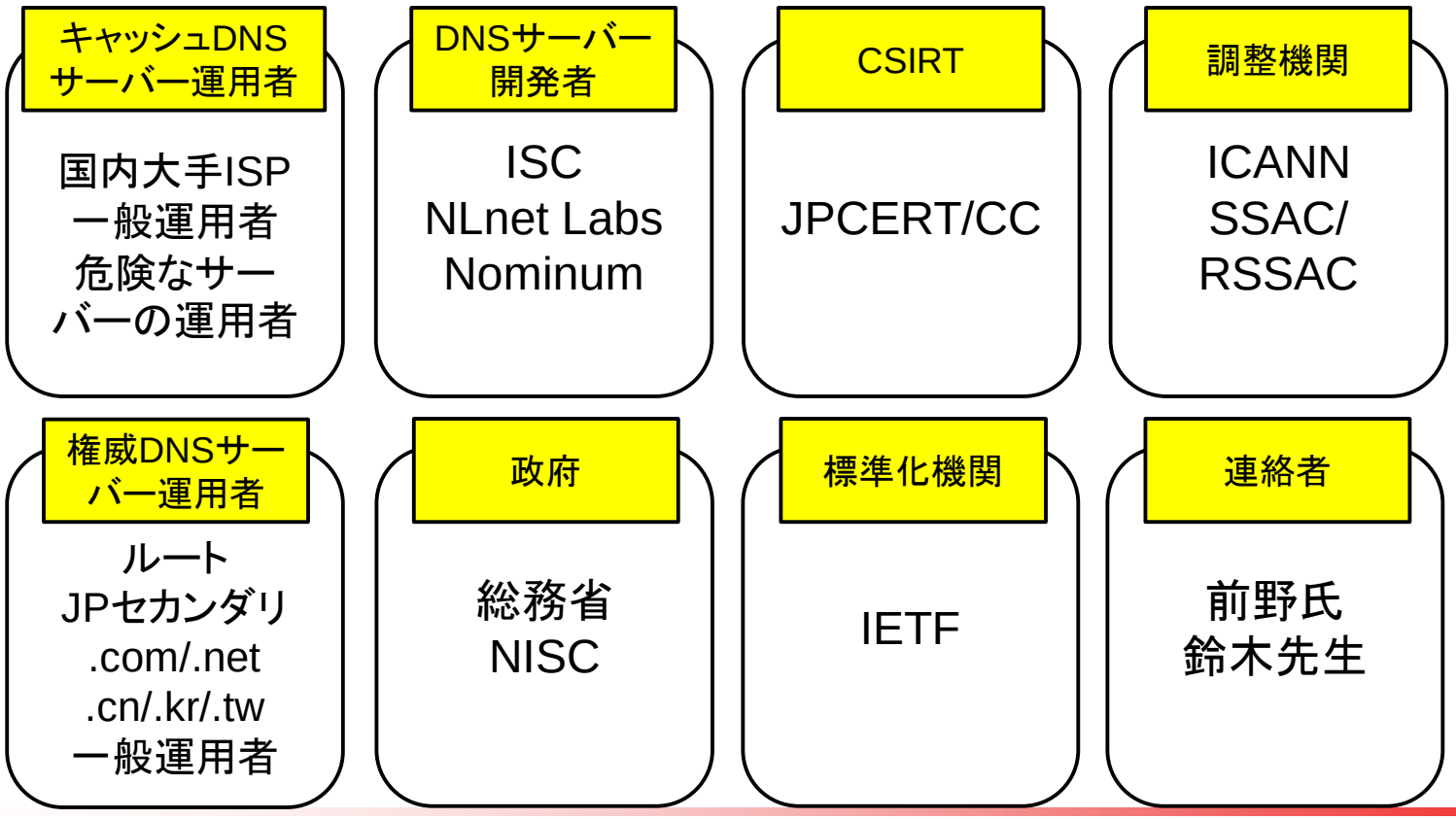
②検討・調整（2/25～3/31）

- 注意喚起経路・対象の検討（対象・内容）
- 標準化活動検討（プロトコルの問題点の洗い出し）
- 連絡をいただいた前野氏、鈴木先生に対し、問題解決に向けた協力を要請
- JP DNSサーバーにおける対策内容の検討
- 影響範囲の検討と情報の取り扱いの決定

危険なキャッシュDNSサーバーの利用者の保護を図るため、
十分な周知の実施と対策の効果の確認まで、
攻撃手法の広報を控えることを決定

③関係者への情報共有・展開（3/4～）

- 作成したコンタクトリストをベースに、JPRSが直接コンタクト可能な関係者への情報共有・展開を開始



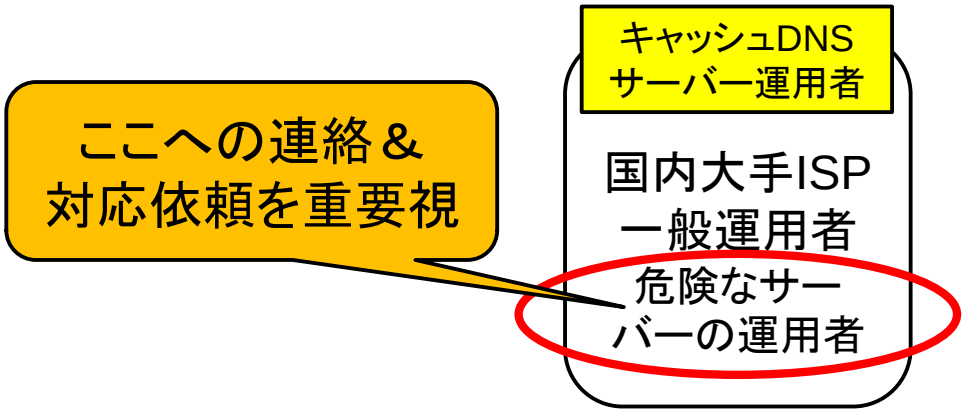
④JP DNSにおける対策の実施（3/16～）

- 現状のJP DNSの安定運用に影響を及ぼさない範囲で、実施・適用可能な対策について検討
- 検討結果を受け、以下の二つを決定・実施
  1. co.jpなどへのTXTレコードの追加（3/16）
  2. jpとdns.jpゾーンの別居（6/9～24）

それぞれの目的と効果については後述

⑤修正依頼・対外広報（4/15～）

- 一般向け注意喚起の実施（4/15）
  - JPRSとして、本件に関する最初の一般向け広報
- 注意喚起の実施に合わせ、対策未実施の危険なキャッシュDNSサーバーの管理責任者への連絡＆対応依頼を実施
  - 指定事業者経由
  - JPCERT/CC経由
  - 国内大手ISP経由
  - NII経由（大学関係）
  - CNNIC（.cn）/KISA（.kr）/TWNIC（.tw）経由（各国分）



⑤修正依頼・対外広報（続き）

- 技術文書の公開
  - 「キャッシュポイズニング対策」
    - キャッシュDNSサーバー運用者向け：基本対策編（4/30）
    - 権威DNSサーバー運用者向け：基本対策編（5/30）
- セミナー・プレゼンテーションなど
  - Interop 2014 Tokyo：ミニセミナー（6/11～13）
  - DNS Summer Days 2014（6/27）
  - 指定事業者向け技術セミナー（7/7、7/11）
  - JANOG 34本会議におけるセッション（7/17）

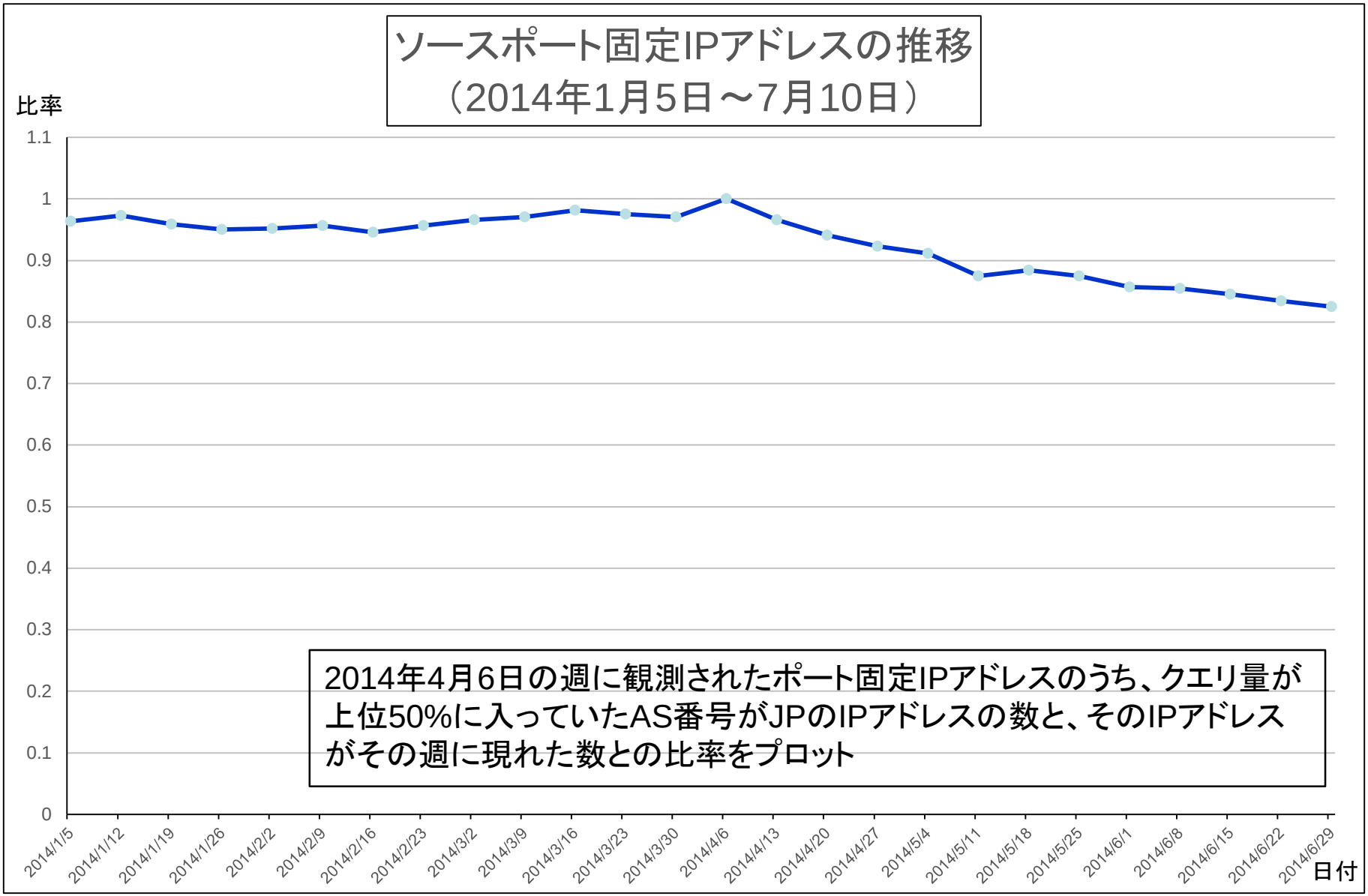
イマココ

気になる「あのこと」

なぜ、攻撃手法の広報を控えてきたのか？

- 理由：危険なキャッシュDNSサーバーの利用者の保護を図るため
- 各チャンネルからの個別連絡と対応要請により、ソースポートランダマイゼーションが未対策のキャッシュDNSサーバーは、4月以降確実に減少しつつある（次ページのグラフを参照）
  - しかし、減少のペースは早いとはいえない

ソースポート固定IPアドレスの推移
（2014年1月5日～7月10日）



2014年4月6日の週に観測されたポート固定IPアドレスのうち、クエリ量が上位50%に入っていたAS番号がJPのIPアドレスの数と、そのIPアドレスがその週に現れた数との比率をプロット

co.jpなどにTXTレコードを追加した理由は何か？

- 理由：DNSSEC検証においてEmpty non-terminal（*1）を確実に保護対象とするため
- 自分が管理するゾーンをNSEC3+Opt-OutでDNSSEC署名している場合以外は追加不要
  - NSEC3+Opt-Outの仕様では、署名済サブドメインが一つもない場合、empty non-terminalは必ずしも保護されない
  - そのため、サブドメインの状況に関わらずempty non-terminalを保護対象とするため、一律にTXTを追加した
  - 現在、co.jpには署名済サブドメインが一つ以上あるため、TXTレコードの有無による安全性の変化はなし

（*1）Empty non-terminal：リソースレコードが一つも設定されていないが、一つ以上のサブドメインが設定されているドメイン名（RFC 5155で定義）

jpとdns.jpを別居した理由は何か？

- 理由：委任インジェクション攻撃成功の確率を下げるため
- jpとdns.jpが同居している場合、dns.jpが委任インジェクション攻撃の対象となり得る
  - dns.jpへの攻撃が成功した場合、JPドメイン名がキャッシュポイズニングされる
- jpとdns.jpが別居であった場合、上記と同様の効果を得るためにはJP DNSサーバーのホスト名（a.dns.jp～g.dns.jp）すべてについて、委任インジェクション攻撃を成功させる必要がある

まとめと今後の議論に向けて

本件の対応で感じたこと

- 今回の取り組みと対応について、
  - ccTLD/gTLDの技術担当者への連絡・問題解決に向けた活動を進められるチャンネルの必要性
  - キャッシュDNSサーバーの管理者との情報共有や、対策を進められる場所の必要性
- 各機関との問題意識や優先度の共有の難しさ
- 情報のリーチ・アクションにつなげることの難しさ
- 情報開示による攻撃拡大と対応促進のジレンマ

今後の取り組み

- 本件に関する活動は今後も続けていく予定
  - 危険なキャッシュDNSサーバーを減らすための活動
  - 各関係者との調整、対策推進・推奨を含む活動
  - ぜひともご協力をお願いいたします
- 今後は攻撃手法と対策を併せた解説、プロトコルの改善や運用の改良なども織り交ぜた活動を、地道に継続していく予定
- プロトコルの改善や運用ガイドラインの改良を伴う項目については、今後IETFで進めていく予定

ご意見・ご議論いただきたい内容

- 今回の対応は適切だったのか？
  - 初動・調査から修正依頼・対外広報までの取り組み
  - 特に、情報開示による攻撃拡大と対応促進のジレンマという観点において

- この「ジレンマ」に、みんなでどう対座していくか？
  - ますます多種化・多様化するSecurity Issues/Incident
  - 攻撃手法を話せばよい、攻撃対策を話せばよいなどといった、個別・単純な対応だけではたぶん駄目

Thanks!