DNS運用の「見抜く」を探る
～インシデント事例の紹介と必要な要素・項目～
ランチのおともにDNS

2016年12月1日

Internet Week 2016 ランチセミナー

株式会社日本レジストリサービス（JPRS）
森下 泰宏・尾崎 勝義

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 日本レジストリサービス（JPRS） 広報宣伝室
  - 主な業務内容：技術広報担当として、ドメイン名・DNSに関する技術情報の広報全般を担当
  - 一言：ランチセミナーは今年で10年目を迎えました！
- 尾崎 勝義（おざき かつよし）
  - 日本レジストリサービス（JPRS） システム部
  - 主な業務内容：ドメイン名登録システムの開発・運用、JPRSサーバー証明書発行サービスの運用・保守全般を担当
  - 一言：X.509のフォーマットについて勉強中です！

本日の内容

1. 運用における二つの「見抜く」
   – DNSにおける運用の重要性
   – 運用における二つの視点～「これまで」と「これから」
2. 2016年中に発生したDNS関連のインシデント事例から
   – APNICの逆引きDNSゾーンにおけるDNSSEC障害
   – DNSのQNAMEを通信手段として利用するマルウェア
   – 権威DNSサーバーを標的としたDDoS攻撃
3. 二つの「見抜く」のために必要なこと

本日は1.と3.を森下が、2.を尾崎が担当します

1. 運用における二つの「見抜く」

DNSにおける運用の重要性

- 1987年に標準化された仕様を、改良を加えながら現在も継続使用
  - インターネットサービスとしては電子メールと並び、最古のものの一つ
  - 仕様・実装を「運用でカバー」する状況が多い
- 運用できないものは、決してデプロイ（普及）しない
  - 多くの運用者は、大きな変化を望まない
  - 既存のサービスを止めずに、新しい技術を導入・運用する必要がある
    - DNSSECの導入には20年かかった
- そして、一度デプロイしたものは大きな影響力を持つ
  - みんながそれに頼るようになり、簡単には捨てられなくなる
  - サービスを安定、かつ安全に動かし続ける必要性が高まる

DNSでは、安定運用の継続が特に重要

運用における二つの視点 ～「これまで」と「これから」～

- Internet Week 2016全体のテーマ：見抜く力を！

> 今年のテーマは｢見抜く力を！｣です。課題が発生した時に、その課題の本質を的確に捉え、どういう対応が適切なのかを判断できる土壌をIWが提供していきたい、という気持ちを込めています。

<https://internetweek.jp/greeting.html> より引用

- 「見抜く力」のための二つの視点
  - 過去の問題の本質を捉え、適切に判断・対応することに生かす
  - 現在起こりつつある・将来起こりうる変化の状況・予兆を捉え、適切に判断・対応する

⇒「これまで」と「これから」

よりよい運用の実現のためには、これら双方が共に重要

以降の内容について

- 2016年中に発生したDNS関連のインシデント事例から
  - 2016年中に発生したいくつかのDNS関連のインシデント事例を振り返り、以下の点に注目する形で「見抜く」ポイントを探っていく
    - 何がまずかったのか、何をどうすべきだったのか
    - 今後、何をどうすべきなのか
- 二つの「見抜く」のために必要なこと
  - 紹介したインシデント事例や現在のインターネットの状況を踏まえつつ、よりよいDNS運用のために必要な要素・項目を探っていく
    - 「これまで」を踏まえた「これから」に必要なこと

2. 2016年中に発生した DNS関連のインシデント事例から

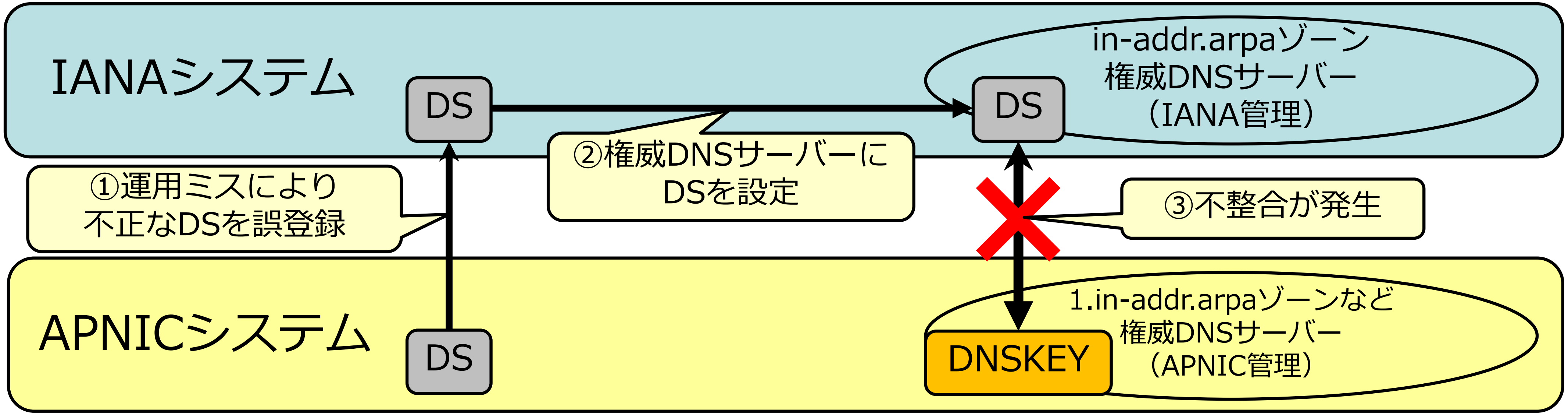
事例1：APNICにおける逆引きDNSSECエラー

- 2016年3月15日から16日にかけ、APNICが管理する以下のDNS逆引きゾーンにおいて、DNSSEC検証エラーが発生
  - すべてのIPv4逆引きゾーン（49ゾーン）
  - IPv6逆引きゾーン（0.4.2.ip6.arpa）
- APNICがインシデントレポートを3月17日に公開

Service announcement: 15 March 2016 | APNIC
<https://www.apnic.net/about-APNIC/service-updates/2016/service-announcement-15-march-2016>

障害の状況

- 運用ミスにより、APNICが不正なDSレコードをIANAに誤登録
  - IANAが管理するin-addr.arpa / ip6.arpaゾーンのDSレコードと、APNICが管理するDNS逆引きゾーンのDNSKEYレコード（KSK）との間に不整合が発生
- 本来のDSレコードに切り戻し、DSのTTL値（1日）経過後に復旧



本件のポイント

- インシデントレポートより引用

> Our monitoring system currently checks the DNSSEC validation from our DNS distribution servers. This check runs every 15 minutes, and APNIC can verify that the monitoring system was running for the duration of this outage. Unfortunately, the check did not report any failure due to the fact that the resolver used cached responses.

  - 15分ごとにDNSSEC検証チェックの監視を実施していた
  - しかし、キャッシュされた応答をチェックしていたため、障害として検知されなかった
    - 外部のMLへの障害報告により障害を認識

検証方法のレビューが不適切であったため、不具合を見抜けなかった

APNICで実施された再発防止策

- APNICにおける運用体制の改善
  - 更新時における内部プロセスの改善とレビュー体制の強化
  - 監視システムの改修
  - システムに対する外部監査の実施
- DPS（DNSSEC Practice Statement）の公開（2016年6月）

APNIC DNSSEC Policy and Practice Statement
<https://www.apnic.net/manage-ip/apnic-services/dnssec/DNSSEC_DPS_210616v1.pdf>

  - DPS：DNSSECの運用者が、自身が運用するサービスの安全性や運用の考え方、方式、関連する操作手順などについて記述した文書

事例2：DNSのQNAMEを通信手段として利用するマルウェア

- 従来の手法：DNSのデータ（RDATA）を通信に利用
  - DNSトンネリング（DNS tunneling）と呼ばれている
- 最近、DNSクエリのQNAMEを通信に利用するマルウェアが、相次いで報告された
  - QNAME：問い合わせの名前情報（ドメイン名）
- 本日紹介する事例（注意喚起2件）

遠隔操作ウイルスの制御にDNSプロトコルを使用する事案への注意喚起
（株式会社ラック、2016年2月1日）
<http://www.lac.co.jp/security/alert/2016/02/01_alert_01.html>

MULTIGRAIN – Point of Sale Attackers Make an Unhealthy Addition to the Pantry
（米国FireEye社、2016年4月19日）
<https://www.fireeye.com/blog/threat-research/2016/04/multigrain_pointo.html>

①Botと指令サーバー間の通信

- 株式会社ラックの注意喚起より引用

> サブドメイン名（abcde）は標的を特定する文字列か作戦名を表していると推察され、当社にて解析したマルウェアが使用しているドメインには、他に4つのサブドメインが存在することが確認されています。したがって、同じマルウェアは、複数の他の組織にも使用されている可能性があります。
> （中略）
> 実際のDNSリクエストでは、10秒程度の短い時間の間に、指令サーバとの通信と考えられるDNSクエリを送信しています。FQDNのホスト名部分には、暗号化されていると考えられる30文字以上の文字列が埋め込まれています。

- DNSクエリのQNAMEを、Botと指令サーバー間の通信に利用

<30文字以上の文字列>.<5種類のサブドメイン>.example.jp

指令サーバーとの通信データ？

標的名 or 作戦名？

攻撃者の制御下にあるドメイン名

②クレジットカード情報の抜き取り

- MULTIGRAIN：WindowsベースのPOS端末に感染、DNSクエリでクレジットカード情報の抜き取りを図るマルウェア
  - POS端末を狙うマルウェア「NewPosThings」の変種
- DNSクエリのQNAMEを、カード情報の抜き取りに利用
  - POS端末への感染（侵入成功）も、DNSクエリで攻撃者に伝達

侵入成功：install.<Base32エンコードされた文字列>.example.jp

POS端末の名前・MACアドレスなどから生成したID

攻撃者の制御下にあるドメイン名

抜き取り：log.<Base32エンコードされた文字列>.example.jp

カード番号・有効期限・セキュリティコードを
1024bit RSA公開鍵で暗号化した後、Base32エンコード

攻撃者の制御下にあるドメイン名

QNAMEが通信に利用される背景

- 攻撃者にとってメリットがある
  - DNSクエリログが取られていないことが多い
  - 外部に対するDNSクエリがフィルターされていないことが多い
  - 使うドメイン名を頻繁に変更して、フィルターの回避を図れる
  - 標的にインターネット到達性がなくても、情報を抜き取れる
    - MULTIGRAINの場合はPOS端末
    - フルリゾルバー（キャッシュDNSサーバー）が外部に名前解決した時点で情報が漏えいする
- 対策なしでは、感染や機密情報の抜き取りを検出できない

それらを「見抜く」ための材料集めと仕組み作りが必要

提案されている対策

- DNSクエリログの取得と保存・内容の調査
  - ログを取らないと、被害に遭ったことをそもそも知ることができない
  - 何かあった際、さかのぼって調査できるように備えておくためにも重要
  - 不審なQNAMEの例
    - ランダムな文字列のラベルを含むQNAME、長いラベルを含むQNAMEなど
- エンタープライズネットワークにおけるOP53Bの適用
  - 組織が提供しているリゾルバー以外の利用を制限
  - US-CERTが推奨：

Alert (TA15-240A) Controlling Outbound DNS Access
<https://www.us-cert.gov/ncas/alerts/TA15-240A>

- いわゆるDNSファイアーウォールの導入検討
  - いくつかのベンダーからソリューションが発表・提供されている

事例3：権威DNSサーバーを標的としたDDoS攻撃

- 最近の状況
  - ルートサーバーに対するDDoS攻撃（2016年6月）
    - 古典的なSYN flood攻撃が用いられた
  - 国内組織・サービスに対するDDoS攻撃（2016年8～9月）
    - Webサーバーに加え、権威DNSサーバーも攻撃対象となった
  - 米国Dyn社のサービスインフラに対するDDoS攻撃（2016年10月）
    - マネージドDNSサービスに対する大規模な攻撃
    - 大量のIoTデバイスが悪用された（Miraiを用いたBotnetによる攻撃）

権威DNSサーバーを標的としたDDoS攻撃事例の報告が相次いでいる

最近のDDoS攻撃の特徴（1/2）

- 送信元IPアドレスを偽装した攻撃
  - 従来はこれが主流であった（現在も主流）
    - 各種リフレクター攻撃（DNS、NTP、SNMP、SSDPなど）
    - DNS水責め（ランダムサブドメイン）攻撃
      - 偽装の必要はないが、送信元IPアドレスを偽装する事例が多い
    - SYN flood攻撃（古典的な攻撃手法だが根本的対策は困難）
- 送信元IPアドレスを偽装しない攻撃
  - 最近（再び）、見られるようになってきた
    - Miraiを用いたBotnetによる攻撃
      - 複数の攻撃手法を組み合わせて利用
  - 直接攻撃で十分 & 踏み台だから足がついてもいいという割り切り？

最近のDDoS攻撃の特徴（2/2）

- 攻撃規模の飛躍的な増大
  - Dynに対するDDoS攻撃では、最大1.2Tbpsを観測したと言われている
- 攻撃手法の「巧妙化」
  - 「複数の手法を組み合わせた、複雑かつ高度な攻撃」が恒常化
    - Dynの分析レポート（2016年10月26日公開）

> The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.

Dyn Analysis Summary Of Friday October 21 Attack
<https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/> より引用

  - 2016年8～9月の国内のDDoS攻撃でも、複数の手法の使用が報告されている
- 攻撃ツールの進化と利用の容易さから、手軽な攻撃が流行
  - 他人のツールを利用するだけで「複雑かつ高度な攻撃」が可能な時代に

できることはあるのか？

- 「1.2Tbps」をまともに食らったら非常に厳しい
  - 最後は「物量（資源投入）作戦」になりがち
    - 例：IP Anycastやサーバーの分散化などによる、大規模なスケールアウト
    - さまざまなサービスプロバイダーがソリューションを発表・提供している
- しかし、それ以前にできることは色々ある
  - 起こりうることを見抜き、備える
    - 攻撃の効果軽減
    - 情報提供用チャンネルの確保（特にサービス提供者）
  - 起こりつつあることを見抜き、早期に対策する
    - 攻撃の検知・緩和

対策：攻撃の効果軽減

- サービスダウンした際の被害を最小限に留めるための備え
- 対策1：複数のDNSプロバイダーを利用する（サービスの冗長化）
  - データの管理において注意が必要（下記資料のp.29～36に詳細な解説あり）

> 参考：DNSにまつわるセキュリティのあれこれ（IIJ 島村充氏）
> <http://www.iij.ad.jp/company/development/tech/techweek/pdf/161111_04.pdf>

- 対策2：TTL値を無用に短くするのを避ける
  - 特に、NSやネームサーバーホスト名のA/AAAAのTTL値に注意
    - ゾーンファイルの$TTLの設定値が本来短くすべきではない、NSレコードやネームサーバーホスト名のA/AAAAレコードにも設定されることに注意
    - NSやネームサーバーホスト名のA/AAAAには、長い（1日以上）TTL値を別途設定すべき
  - 参考：Dynの障害後、twitter.com/AのTTL値が300→1800に変更された

対策：情報提供用チャンネルの確保

- サービスやWebサイトがダウンしている間も利用可能な、情報提供用のチャンネルを別途確保する
  - 顧客や組織内外の関係者に、障害状況や対応状況を伝達
    - 自身の障害のため、アナウンスを読んでもらえない状況を回避する
- 運用事例
  - Dynではサービス状況提供用サイト「dynstatus.com」を、自社のインフラに依存しない形で以前から運用
    - 10月の障害の際に、Webと電子メールによる緊急の情報提供を実施
  - Twitterなど、外部のサービスの利用
    - 2016年8～9月の障害の際、さくらインターネットや技術評論社が実施

対策：攻撃の検知・緩和

- 攻撃の検知
  - 権威DNSサーバーにおけるトリガーの例
    - 未見かつ複数のIPアドレスから、多数のDNSクエリが到達する
    - 同一IPアドレスから、同内容のDNSクエリが頻繁に到達する
      - かつ、リソースレコードのTTL値よりも明らかに短い

  ⇒ 適切な攻撃検知と、適切なフィルタリングの組み合わせが有効
    - 今日のDNS DAYの話題の一つ（データを見て対策を考える）
- 攻撃の緩和
  - ネットワーク・サーバーにおける緩和策の例
    - 上流ISPとの連携
    - 権威DNSサーバーの複数ネットワーク・サービスへの配置

3. 二つの「見抜く」のために必要なこと

①気付き

- 普段と何か違う、何か様子がおかしい、など
  - Webブラウザーの表示、システムの反応、DNSの応答、etc.
    - 何だか重い、という感覚が障害発見のきっかけになる場合が多い
- 「気付き」はシステムやネットワークの状況などに限らない
  - こんな気付きも…
    - 従来は頻繁に更新されていたWebサイトが、突然更新されなくなる
    - Twitterのタイムラインがざわついている
- 事例：2016年3月のAPNICの逆引きDNSSECエラー
  - 申請を受け付けたIANAが異常に気付くべきだったのかもしれない
    - 50ゾーン分のDS更新申請をいつもと違う時期に受け取った、はず

②状況把握

- 普段の状況を把握していないと、
  普段と違うということを把握できない
- 状況を適切に把握するためには、普段からの蓄積が重要
  - 知る（気付く）ための仕組み作り
    - トラフィックの異常な変化や異常なクエリの検出、アラートの伝達
    - 各種ログの取得・分析
    - 複数のコミュニティへの注意喚起（情報発信者における活動例）
  - 普段の積み重ねと有事に対する備え
    - 見抜くための感覚の向上
    - 有事を想定したシステム設計・設定の実施

③仕組み作り

- 知る（気付く）ための仕組み作り
  - インシデントによる被害を防げなかったとしても、被害を小さくできたり、再発を防止できたりする場合がある
  - 予防・早期発見・早期対応にもつなげる
- 適切、かつ機能する（見抜ける）仕組み作りが必要
  - 事例：2016年3月のAPNICの逆引きDNSSECエラー
    - 仕組みは稼動していたが、見る場所・方法が適切でなかった
  - 事例：DNSのQNAMEを通信に利用するマルウェア
    - 新たな攻撃手法に対応するための仕組み作り
      - DNSクエリログの取得と保存、OP53B、DNSファイアーウォール、etc.

④普段の積み重ねと備え

- 見抜くための感覚（直感）の向上を図る例
  - 毎日触る（サーバー、システム、ネットワーク、etc.）
  - 普段のトラフィックパターンや傾向の把握
  - 運用対象の技術仕様（仕組み）や動作の勉強
- 有事を想定したシステム設計・設定の例
  - 複数のDNSプロバイダーの利用
  - 短いTTL値の回避
  - 対外的なリレーションや連絡網の確保
- 参考事例：東日本大震災発生時の行動（p.5に当日の行動記録あり）

日本のインターネットは本当にロバストだったのか～国内編～（NTTコム 吉田友哉氏）
<https://www.janog.gr.jp/meeting/janog28/doc/janog28-robust-yoshida-after.pdf>

⑤周囲や社会の理解

- 日常の積み重ねや備えは、得てして適切に評価されない

「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」

（IIJ 島村充氏の発表資料（前出）より引用）

- こうした取り組みが、周囲や社会に理解されることが重要
  - 経営者・上司による、組織としての理解
  - 組織内・組織外に対する啓発活動
  - 技術者全体の社会的プレゼンスの向上

おわりに

- 本パートで取り上げた五つの項目
  ①気付き　②状況把握　③仕組み作り
  ④普段の積み重ねと備え　⑤周囲や社会の理解
- DNS運用の「見抜く」は、何気ない日常の中にある
  - サービスを安定、かつ安全に動かし続けるための継続的な活動
- そして、その取り組みが内外で正しく理解されることも重要
- というわけで日々の運用と「見抜く」の両立は大変だけど…

DNSをよりよく、楽しく支えていくため、
みんなで力を合わせてがんばっていきましょう

That’s it!