桃栗三年柿八年、DNSSECは何年？
「ランチのおともにDNS」は三年目

2009年11月24日
Internet Week 2009 ランチセミナー
株式会社日本レジストリサービス
森下泰宏（オレンジ）・民田雅人（みんみん）

本日のお題

- DNSSECがこれまでにたどってきた、「**長く曲がりくねった道のり**」の解説
  - プロローグ: 1983年—1990年
  - 第1章: 1990年—1995年
  - 第2章: 1995年—2000年
  - 第3章: 2000年—2005年
  - 第4章: 2005年—現在
- **ついにやってきた**DNSSEC
  - ルート・主なTLDにおける導入予定と今後の展望

プロローグ:1983年—1990年

- 1983年
  - DNSの最初のRFC（RFC 882/883）
  - 委譲による分散管理
- 1986年
  - BIND 4.3が4.3BSDに付属
- 1987年
  - DNSの現在のRFC（RFC 1034/1035）
- 1990年
  - BIND 4.8.3が4.3BSD-Renoに付属
  - sendmailにMXレコードでメールを配送するためのコードが入り、DNSが広く使われ始める
- 日本に商用のインターネットサービスはおろか、JPNICの前身であるJNICもまだなく、JPドメイン名の総数が数百だったあの頃・・・その道のりは始まった。

第1章
1990年—1995年

それは一つの論文から始まった

発表されなかった論文

DNSSEC標準化の開始

それは一つの論文から始まった

- 1990年
  - AT&Tベル研究所のSteven M. Bellovin氏が、“Using the Domain Name System for System Break-ins”という論文を書いた
  - 日本語訳:「システム侵入のためのドメインネームシステムの使用」
- 論文中で「DNSキャッシュポイズニング」の手法について、世界で初めて記述
- Bellovin氏は論文中で「DNSをあきらめるべきか（Should the DNS be Abandoned）?」と問いかけ
- しかしBellovin氏は自らそれに対し、否定的な結論を記述
  - （論文を書いた1990年の段階で）既にドメイン名空間は巨大であり、他の方法で安定運用をするのは困難である、と結論

発表されなかった論文

- インターネットに対する影響の大きさを考慮し、Bellovin氏はこの論文を数年間発表しなかった（1995年に発表）
- その間にこの脆弱性は一部の研究者・専門家などの間で伝えられ、1993～1995年頃には複数の研究者の間で既に知られていた
- その間にWorld Wide Webが実用化、商用インターネットサービスが開始され、Windows 95の発売とともに、世界的なインターネットの爆発的普及が起こり始めていた

DNSSEC標準化の開始

- このような状況から、DNSにセキュリティ機能を付加することの重要性が認識され、技術者の努力が開始された
- 1993年
  - 第28回IETFにおいて最初の「DNSSEC BOF」が開催
- 1994年
  - 第29回IETFにおいて「DNS Security Working Group」が組織、DNSSECの標準化活動を開始
- 1995年
  - USENIXにおいてBellovin氏、Paul Vixie氏らが、DNSセキュリティに関する論文を発表

第2章: 1995年—2000年

最初の標準: RFC 2065

「セキュリティ」と「機能」の間に流れる河

仕様の改良と実装: RFC 2535とBIND 9

最初の標準: RFC 2065

- DNSSEC WGではDNSへのセキュリティ機能の付加を目標に、電子署名の技術を用いたDNS拡張機能であるDNSSECの標準化作業をすすめていった
- 1997年
  - DNSSECの最初のRFC（**RFC 2065**）発行
- これで問題は解決するはず・・・ **ところが。**

「セキュリティ」と「機能」の間に流れる河

- 一方、発展し続けるインターネットの要求に対応すべく、DNSへの機能追加を議論するためのWGがIETFで組織され、活動を開始していた
- 1996年
  - 第37回IETFにおいてDNSIND WGが組織、活動を開始
  - DNS **I**XFR, **N**otification, and **D**ynamic Update
- 1996年
  - IXFR（RFC 1995）、DNS NOTIFY（RFC 1996）発行
- 1997年
  - Dynamic Update（RFC 2136）発行

「セキュリティ」と「機能」の間に流れる河

- 当時のDNSSECは「DNSエキスパート」よりもむしろ「セキュリティスペシャリスト」により、仕様の開発がすすめられていた傾向があった
- そのため、DNSプロトコルとの親和性やDNSへの新しい機能追加への対応には、あまり注意が払われていなかった
- 結果として、当時DNSIND WGで並行して進められていた、DNSへの機能拡張に対し十分な対応がなされなかった
  - 例えばRFC 2065では、Dynamic Update（RFC 2136）の機能は部分的にしかサポートされない

仕様の改良と実装:RFC 2535とBIND 9

- この問題を解決し、よりDNSの機能に親和性の高いプロトコル仕様にDNSSECを改良するための作業が開始された
- 1999年
  - RFC 2065の改良版である**RFC 2535**が発行
  - RFC 2535を実装することを主目的の一つに掲げた「BIND 9プロジェクト」がISCにおいて開始された
- 2000年
  - DNSSECの実装を進めるべく、DNSSEC WGとDNSIND WGが合流し、DNSEXT WGとなった
  - DNSEXT:DNS Extensions

第3章:2000年—2005年

立ちはだかる「運用の壁」
運用の壁に立ち向かう
さらなる仕様の改良:DNSSECbis

立ちはだかる「運用の壁」

- RFC 2535に従い、example.jpがDNSSECを「とりあえず動かす」ためにはどうすればよいか

1. example.jp用の鍵対（公開鍵と秘密鍵）を作成する
2. example.jpを自身の秘密鍵で署名する
3. jpにexample.jpの公開鍵を送る
4. jpは自身の秘密鍵でexample.jpの公開鍵に署名する
5. jpは署名済み公開鍵をexample.jpに**送り返し**、example.jpは署名済み公開鍵を**自ゾーンで公開**する
   - これにより「example.jpの鍵はjpが承認したものである」と証明できる（**信頼の連鎖**）

立ちはだかる「運用の壁」

- これを実際に**運用し続ける**ためには・・・
- jpはexample.jpに、署名済みの鍵を送り返さなければならない
- example.jpは鍵を受け取り、その鍵をDNSで公開しなければならない
- そしてこの「送り返し」と「公開」を、
  - DNSSECに対応した子ドメイン名の数だけ
  - 子ドメイン名の鍵が更新される毎に毎回、定期的・不定期的に

  繰り返さなければならない
- また、もしjpが鍵を更新する場合、
  - ルート(.)に公開鍵を送り、ルートから署名済みの鍵を受け取り、その鍵をDNSで公開しなければならない
  - 親は全部の子に対し、自身の新しい秘密鍵で署名された相手の鍵を送り直し、子は鍵を受け取り、その鍵をDNSで公開しなければならない
- 果たしてこれを、インターネットで実際に運用できるのか？

運用の壁に立ち向かう

- 2つの「運用の壁」
  1. 鍵を取り替える時、毎回親に送り直さなければならない
  2. 親に送った鍵は、必ず親から送り返してもらわなければならない
- 1.の解決: **鍵を2つに分ける**
  - 署名鍵を「ゾーン署名鍵（ZSK）」と親に登録する「鍵署名鍵（KSK）」の2つに分け、セキュリティ向上を図るためにZSKを取り替えても、親にその鍵を送らなくてもいいようにする
  - ZSKだけを親と独立に取り替えられるようになる
- 2.の解決: **鍵を送り返してもらう必要をなくす**
  - 暗号論的に鍵と同じ意味を持つ、「Delegation Signer（DS）」という新しい概念を導入
  - 子は自身のKSKから作った「DS」を親に送る
  - 親は子から送られてきたDSを、従来のNSと同様の形で自身のゾーンに設定することにより「信頼の連鎖」を構築できる
  - DSは親から送り返してもらう必要がない

さらなる仕様の改良:DNSSECbis

- 2005年
  - DNSSECbis（**RFC 4033、4034、4035**）発行
  - DSの導入とZSK、KSKの分離
- この仕様改良により、RFC 2535とは互換性がなくなった
- そのため、関係するリソースレコードの名前を変更し、番号を新たに割り当て直した
  - SIG（24）→RRSIG（46）
  - KEY（25）→DNSKEY（48）
  - NXT（30）→NSEC（47）
- これでいよいよ、運用の問題も解決か・・・ **ところが。**

第4章:2005年—現在

「今のままじゃやりたくても導入できない」
「不存在の存在証明」という宿命
「芋づる式ゾーンウォーキング」と「いきなり8倍」
導入の壁に立ち向かう
更なるプロトコルの改良:NSEC3とOptOut

「今のままじゃやりたくても導入できない」

- DNSSECbisの完成後、.seなどいくつかのTLDがDNSSECの導入に踏み切った
- しかし、特に大規模TLDオペレータを中心に、タイトルにある声が多く上がった
- DNSSECにはまだ越えるべき「導入の壁」が存在していた
  - ゾーンウォーキング
  - 大規模ゾーンにおけるゾーン情報の急増

「不存在の存在証明」という宿命

- DNSSECでは情報が正しいことを、存在するレコードに対し電子署名することにより証明している
  - 存在する情報に対してはこれで問題なくうまくいく
- しかしDNSには「存在しない情報を、確かに存在しないと答える」という、もう一つの重要な役割がある
- DNSSECでは名前が存在しないことを、
  - 聞かれた名前の前後にはこれとこれが存在します
  - しかし、その間には何も存在しません

  を問い合わせ元に示すことで、つまり、
  「**不存在を存在で証明する**」ことにより証明している

芋づる式ゾーンウォーキング

- これを利用することにより、外部からのDNS問い合わせにより、芋づる式に名前情報を入手することが可能になってしまう
  - 「ゾーンウォーキング（zone walking）」と呼ばれている
- 通常の場合DNSに掲載される情報は公開情報とみなされるが、特にTLDではセキュリティやプライバシー上の理由により、ゾーン情報を非公開にしている場合が多い
- このようなTLDにおいてDNSSECを導入した場合、TLDに登録されているゾーン情報のコピーを、外部から自由に入手できることになってしまう

いきなり8倍

- DNSSECにおいてあるゾーンに署名した場合、ゾーンファイルの大きさは署名前の約8倍程度増加する
  - 増加度合いは鍵長などの条件に依存
- TLDのように、1つのゾーン内に数多くのDNSデータが存在している場合、DNSSECの導入によるゾーン情報の増加そのものが、DNSSECの導入に対する大きな障壁となりうる

導入の壁に立ち向かう

- 2つの「導入の壁」
  1. ゾーンウォーキング
  2. 導入によるゾーンサイズの急激な増加
- 1.の解決: ゾーンウォーキングを困難にする
  - 不存在証明に「NSEC3」を導入する
    - NXT→NSEC→NSEC3（3は「不存在証明バージョン3」）
  - 名前そのものではなく名前のハッシュにより不存在を示す
- 2.の解決: ゾーンサイズの増加を緩やかにする
  - 「NSEC3+OptOut」を導入する
  - DNSSEC情報を持たない子ゾーンの情報は、DNSSEC署名の対象外とする（DNSSEC的に存在しないとみなす）

更なるプロトコルの改良:NSEC3とOptOut

- 2008年
  - **RFC 5155**（NSEC3、NSEC3PARAM、OptOut）発行
- DNSSECbisにNSEC3による不存在証明と、「DNSSEC未署名の子ゾーン」の除外（OptOut）機能を追加
- 名前情報を公開してもよいゾーンに対しては、従来のNSECによる不存在証明も継続して使用可能
- これによりTLDにとっての導入障壁は小さくなった

- そして、ついに・・・ **ついに。**

ついにやってきたDNSSEC

ついにやってきたDNSSEC

- 主要なTLDが続々と、2010年から2011年にかけてのDNSSECの導入を表明
  - ルート(.) 2010年7月1日までに段階的な導入を完了
  - .org 試験導入済み、2010年に本格導入予定
  - **.jp 2010年中**
  - .info 2010年中
  - .net 2010年第四四半期
  - .com 2011年第一四半期
  - .arpa / .in-addr.arpa
- BIND 9.7の開発テーマ: “DNSSEC for Humans”
- Bellovin氏の論文執筆から来年で20周年
  - 我々は今「**長く曲がりくねった道のり**」のどのあたりにいるのか・・・

付録:参考情報

- The IETF standards process & DNSSEC
  - Olaf Kolkman – IAB chair, 2007
  - http://www.menog.net/meetings/menog2/presentations/keynote-olaf-kolkman-ietf.pdf
- Using the Domain Name System for System Break-ins
  - Steven M. Bellovin, 1995 (written in 1990)
  - http://usenix.org/publications/library/proceedings/security95/bellovin.html
- IETF Meeting Proceedings
  - http://www.ietf.org/meeting/proceedings.html

最後にちょっと宣伝がてら、息抜きを・・・

- ドメイン名を使って楽しく遊びましょう。

総統の夢。jp
（ここに入力。
全角のままでおk）

日本語ドメイン名も
DNSSECで署名される
日が来るんだな・・・

(´ー`)

まとめ

- 桃栗三年柿八年、DNSSECは・・・

なんと、20年

- ・・・「ランチのおともにDNS」は三年目