運用技術WG 活動報告

DNSSECジャパン
運用技術WG
大本　貴

運用技術WG

- WGの活動目的
  - .jpでのDNSSEC運用も開始し、サービスへ導入した事業者も出てきている中で、先達が解決してきた様々な技術的知見を集約し、DNSSECの運用を行っていくのにあたり技術情報をまとめ、活用してもらいたい
  - また、現在、DNSSECへ足踏みしている技術的課題、政治的課題について調査し、導入への障壁を明らかにしたい
- 活動状況
  - 2011年6月から2012年3月までに14回のWGを開催。
    - 11年6月14日より3週間に1度の開催
    - 活動時にはIIJさまに会議スペースのご提供いただきました。
    - メンバは親会から参加
  - 導入組織での失敗事例、HSM、DPSについての勉強会開催
  - アンケートの実施(DNSSEC導入への障壁は何かをヒアリング)
  - 成果はメンバ内で取りまとめ、資料公開をしました。

- 運用技術WGの公開資料

  http://dnssec.jp/?page_id=571

  - リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いるゾーンへのDNSSECの導入にあたっての注意喚起
  - DNSSEC運用失敗事例の研究と考察
  - DNSSEC ゾーン検証ツール調査報告
  - HSMを利用したDNSSECの運用に関する考察
  - ISP等のDNSSEC対応におけるDPS作成・公開の検討

運用技術WGの公開資料

- リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いるゾーンへのDNSSECの導入にあたっての注意喚起(2011/10月公開)
  - http://dnssec.jp/?page_id=570
  - セカンダリのbindが古い場合に起きる問題
  - DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、validation に失敗する
  - 当該ゾーンが不在証明の方式として NSEC3 を採用しているとき、DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、不在証明に失敗する
  - RHEL系で「yum install bind 」な人は是非ご一読を

リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いるゾーンへのDNSSECの導入にあたっての注意喚起

2012年4月25日

DNSSECジャパン

運用技術WG

この問題は…

- セカンダリの運用者が関知しないところでプライマリの運用者だけの手によって引き起こされ得る。
- セカンダリの運用者がDNSSECに対応しようとして何かアクションをとった結果ではなく、DNSSECに対応する意図がないときに起き得る。

この問題は…

- セカンダリの運用者がセキュリティホールへの対応を心がけ、OSのリリース元が提供するアップデートに迅速に追従していても、それとは無関係に起き得る。

背景事情

- この問題は、本質的には古いバージョンのBINDを使い続けていることが原因であり、Red Hat固有の問題ではない。しかし…
- RHEL 5(2017年3月31日に運用フェーズ終了)にはBIND 9.3.6-P1が搭載されている。
- RHEL 4(2012年2月29日に運用フェーズ終了)にはBIND 9.2.4が搭載されている。
  - 参考: https://access.redhat.com/support/policy/updates/errata/

背景事情

- だが、BINDの配布元であるISCでは、9.2は2007年9月に、9.3-P1は2009年1月にEnd of Lifeになっている。
- Red Hatでは、セキュリティfixは適用されていても機能追加のバックポートはされていない。
- 同じような状況のOSは他にもあるかもしれない。

何が起こる? [その0]

- BINDで今日のインターネットで使われている DNSSECがサポートされたのは9.3以降。
  - RFC 4033ファミリー、いわゆるDNSSEC bis
- したがってRHEL 4に搭載されているBIND 9.2は、かなり問題外。

何が起こる? [その1]

- シナリオ
  - プライマリが署名して上位ゾーンにDSを登録した。
  - セカンダリはoptions{dnssec-enable;}を明示的にyesにしていない。
    - BIND 9.3のデフォルトはno。9.4からyes。
- 結果
  - セカンダリからの応答を得たvalidatorは検証に失敗する。
- なぜなら上位ゾーンにはDSがあるのに、セカンダリはDNSKEY、RRSIGなどをサーブしないから。

何が起こる? [その2]

- シナリオ
  - プライマリはNSEC3を使って署名した。
  - セカンダリはdnssec-enable yes;に設定している。
- 結果
  - セカンダリからの応答を得たvalidatorは不在証明に失敗する。
  - ない名前がNXDOMAINになるかSERVFAILになるかの違いなので、[その1]ほど大問題ではない。
- BINDがNSEC3をサポートしたのは9.6から。

守りな回避策

- 該当するOSのセカンダリでbindというRPMパッケージを使うなら…
- セカンダリでdnssec-enable yes;に設定しないのであれば、プライマリの運用者にDNSSECを有効にしないよう周知する必要がある。
- セカンダリでdnssec-enable yes;に設定するのであれば、プライマリの運用者にNSEC3を使わないように周知する必要がある。

攻めな回避策

- RHEL 5.6からは、bind(BIND 9.3.6)とは別にbind97というRPMパッケージが提供されている。
- RHEL 6はbindというRPMパッケージはBIND 9.7になった。
- これらにアップグレードすれば、ここで注意を喚起した問題は回避できる。

プライマリを運用するアナタへ

- もしプライマリは自営、セカンダリはSPに委託で運用しているなら、署名する前にセカンダリの状況を把握しましょう。
- セカンダリも自営でも、implementation diversityで該当OSを使っていませんか?

おまけ: 未知のアルゴリズム

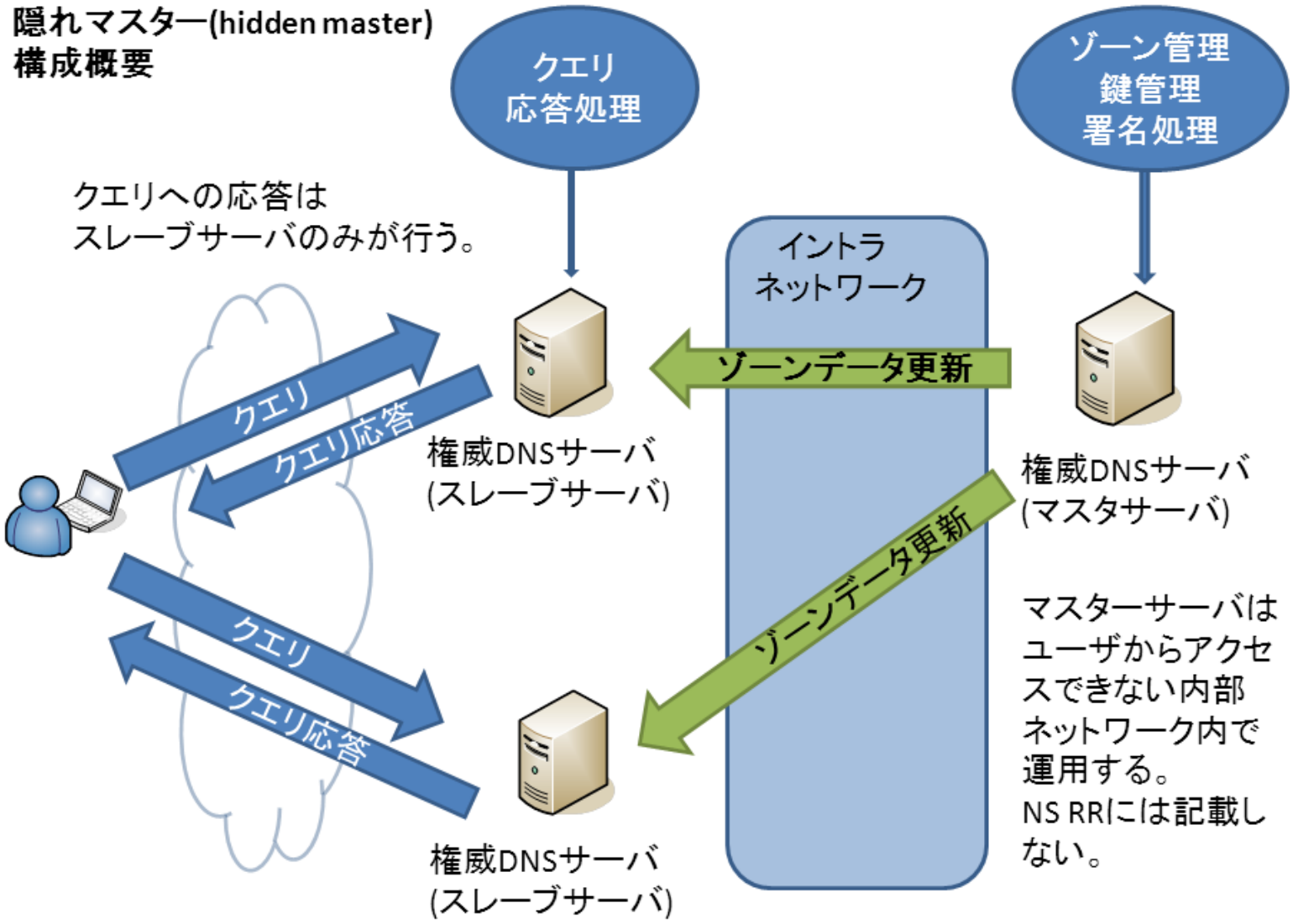
- BINDがRSASHA256をサポートしたのは9.7から。
  - 9.6へは9.6.2でバックポートされた。
- シナリオ
  - プライマリでRSASHA256を使って署名した。
  - 9.3.6-P1のセカンダリでdnssec-enable yes;
- 結果
  - セカンダリもDNSKEYやRRSIGをちゃんとサーブした。

運用技術WGの公開資料

- DNSSEC運用失敗事例の研究と考察
  - 公開は後日
  - WGの会合内でDNSSEC運用中組織における障害の原因・対処について情報確認し議論および考察を行った。
  - WG会合内で議論した内容を公開することで、すでに想定可能な運用上のトラブルの回避あるいは対処するための検討の一助としていただきたい。
  - 内容
    - 失敗事例のサマリー
    - WG会合における総括

- **失敗への対応**
  - (1) ゾーンデータの公開前の検証
    こちらは別資料で検証ツールを紹介
  - (2) 署名／鍵管理システムと対外公開権威サーバ(NSレコードとして指定するサーバ)の分離
    (隠れマスター[hidden master]構成。次スライドで。)
  - (3) 失敗時の対応の明文化
    - 失敗は絶対に0%にはならない。失敗した時の対応タスクを整理しておく。
    - また、DNSに依存しない連絡手段を考慮すべし。

隠れマスタ(hidden master構成例)



運用技術WGの公開資料

- DNSSEC ゾーン検証ツール調査報告
  http://dnssec.jp/?page_id=771
  - 署名の有効期間切れなどによるServfailの確認の他、そもそも公開予定のゾーンファイルの正常性を事前に確認できる手段が必要。
  - ゾーンファイル検証が可能なツールをリストアップした。
  - 昨年技術検証WGが公開したツール資料と併せてご活用ください。

運用技術WGの公開資料

- **ISP等のDNSSEC対応におけるDPS作成・公開の検討**
  - http://dnssec.jp/?page_id=837
  - DPS(DNSSEC Practice Statement)に対する日本語の公開資料は少ないことも一因だが、そもそもDPSに関しての認知度自体が低い。
  - ISPがDNSSECを導入するにあたってDPSを作成する場合のメリットと、公開するにあたっての課題をそれぞれ検討した。

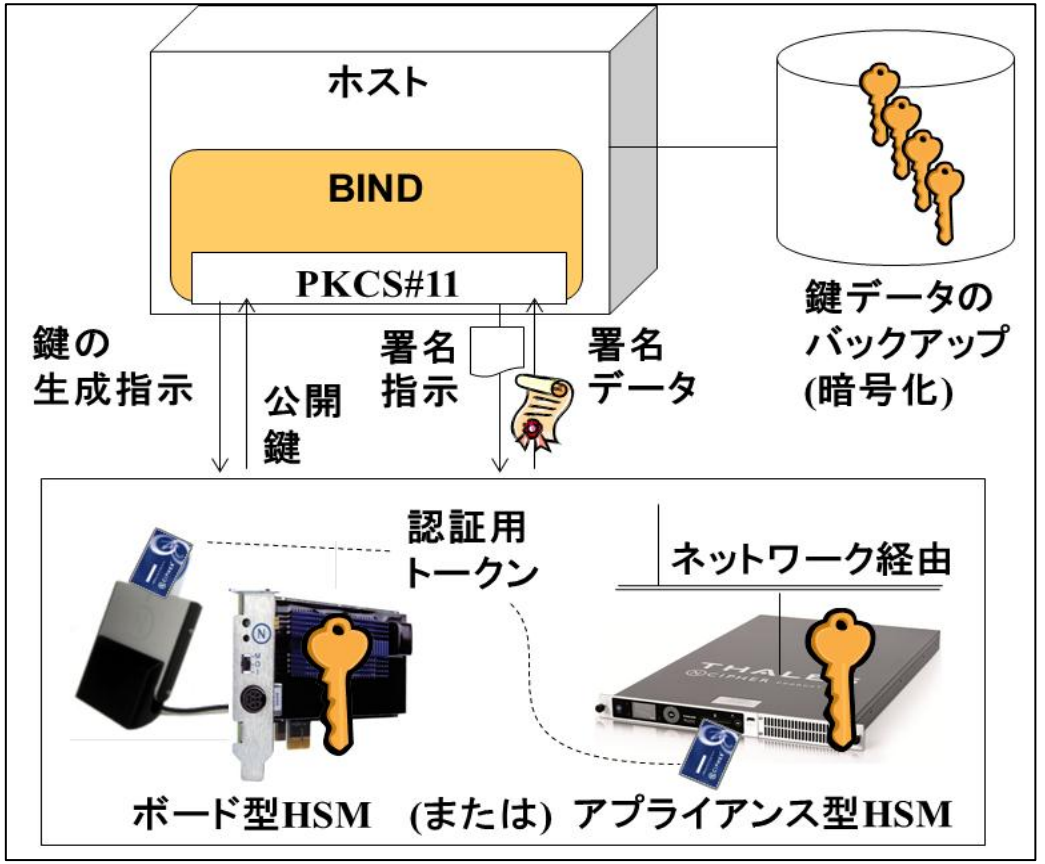
- (参考) 2012/03/22、FCC(Federal Communications Commission・アメリカの連邦通信委員会)が「DNSSEC Implementation Practice for ISP 」を公開。
  - http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf
  - ISPがDNSSECを導入するにあたって確認すべきポイントなどが提言されています。

運用技術WGの公開資料

- HSMを利用したDNSSECの運用に関する考察
  - http://dnssec.jp/?page_id=792
  - DNSSECにおける鍵管理ツールとしてのHSM(Hardware Security Module)に関する情報が日本内外含めて乏しい。
  - WG内で議論したHSMに関する情報をまとめて公開することで、導入要否の判断材料を提供したい。
  - 内容
    - HSMとは　　(HSMの概要等)
    - DNSSECとHSM　　(HSM導入によるメリット等の考察)
    - HSM導入の注意点　(運用上・セキュリティ上の注意点)
    - 導入事例

HSMの概要とメリット

- HSMには現在2タイプ
  - ・ボード型
  - ・アプライアンス型
- 認証用トークンを挿すことで動作する。



- HSMを入れるメリット
  - (1) 暗号鍵の保護
  - (2) 安全な鍵のバックアップ
  - (3) 運用ポリシーの確実かつ迅速な実装
  - (4) アカウンタビリティ

ご清聴ありがとうございました。