アプライアンスによるDNSSEC対応

日本インターネットエクスチェンジ株式会社
技術部 吉武保

最初に

JPIXで行ったDNSアプライアンスを使った
DNSSEC対応について事例紹介したいと思います。

Agenda

- DNSアプライアンスについて
- DNSSEC対応の取り組み
- DNSSEC導入作業について
- DNSSEC運用について
- DNSSEC導入後の障害事例
- まとめ

DNSSEC導入に使用したアプライアンスについて

DNSアプライアンスについて

使用したDNSアプライアンス

- Infoblox社製 DNS&DHCPアプライアンス

  Infoblox-1050A(販売終了)

  → 現行製品Trinzic 1410相当

  - NIOS5.xからDNSSEC対応
  - 2台構成(Primary/Secondary)
  - GRID機能未使用
  - recursive兼用(validation disable)

Infoblox
CONTROL YOUR NETWORK

InfobloxのDNSSEC機能

- 簡単なクリック操作でDNSSEC
  - WebベースのGUIによる操作
  - 標準規格（NIST 800-81）推奨構成
  - NSEC3対応
- 暗号鍵や署名の管理（自動化）
  - ゾーン情報変更時の自動再署名
  - ZSKの自動ロールオーバー（再署名も自動）
  - KSKのGUIでのロールオーバー
  - HSM（鍵管理）を標準サポート
- DNSSEC バリデーション

詳しくはベンダーさんに問い合わせてください

質問

1. Infobloxを使って権威DNSサーバを運用されている方はどれくらいいらっしゃいますか?
2. InfobloxでDNSSEC署名されている方ってどれくらいいらっしゃいますか?

DNSアプライアンスでDNSSEC対応した理由

- たまたま検証中のInfobloxが手元にあった
  - 社内DNSサーバ集約用にInfobloxを購入済だった
  - 本番環境に投入する前だったので導入前の試験も容易だった
- 時間と稼働が無かった
  - OpenDNSSEC等を使って一から環境構築する時間が無かった..
- InfobloxのDNSSEC対応が機能的に申し分無かった

JPIXでのDNSSEC対応の取り組みについて

DNSSEC対応の取り組み

JPIXでのDNSSEC対応の取り組み

·2011年下期–	JPIX DNSサーバ更改準備
·2012年3月9日?	石田社長から署名依頼
·2012年3月15日	DNSSEC Readyロゴ&チェックリスト公開
·2012年3月21日	DNSサーバをInfobloxに入れ替え
·2012年3月27日	jpix.jpの署名
·2012年4月5日	jpix.co.jpの署名
·2012年4月12日	jpix.ad.jpの署名
·2012年4月18日	DNSSEC Readyロゴ利用登録
·2012年4月25日	DNSSEC 2012 Spring Forum
·2013年3月25日	jpix. jp KSKロールオーバ
·2013年4月1日	jpix.co.jp KSKロールオーバ
·2013年4月9日	jpix.ad.jp KSKロールオーバ
·2013年5月29日	DNSSEC 2013 Spring Forum

DNSアプライアンスを用いたDNSSEC導入作業について

導入作業

DNSSEC導入に必要な作業

1. DNSSECパラメータの決定
2. KSK作成
3. ZSK作成
4. ゾーン署名
5. DSをエクスポートして上位ゾーンに登録
6. 定期的なゾーン再署名
7. RR追加時の署名
8. 定期的なZSKロールオーバ
   - ZSKの更新と再署名
9. 定期的なKSKロールオーバ
   - KSKの更新と再署名
   - DSをエクスポートして上位ゾーンに再登録

DNSSEC導入に必要な作業(Infobloxの場合)

1. DNSSECパラメータの決定
2. KSK作成
3. ZSK作成

Infobloxが自動でやってくれる

4. ゾーン署名
5. DSをエクスポートして上位ゾーンに登録
6. 定期的なゾーン再署名
7. RR追加時の署名
8. 定期的なZSKロールオーバ
   - ZSKの更新と再署名

Infobloxが自動でやってくれる

9. 定期的なKSKロールオーバ
   - KSKの更新と再署名
   - DSをエクスポートして上位ゾーンに再登録

DNSSEC導入に必要な作業(Infobloxの場合)

1. DNSSECパラメータの決定
2. KSK作成
3. ZSK作成
4. ゾーン署名

ボタン押すだけ

5. DSをエクスポートして上位ゾーンに登録
6. 定期的なゾーン再署名
7. RR追加時の署名
8. 定期的なZSKロールオーバ
   - ZSKの更新と再署名
9. 定期的なKSKロールオーバ

ボタン押すだけ

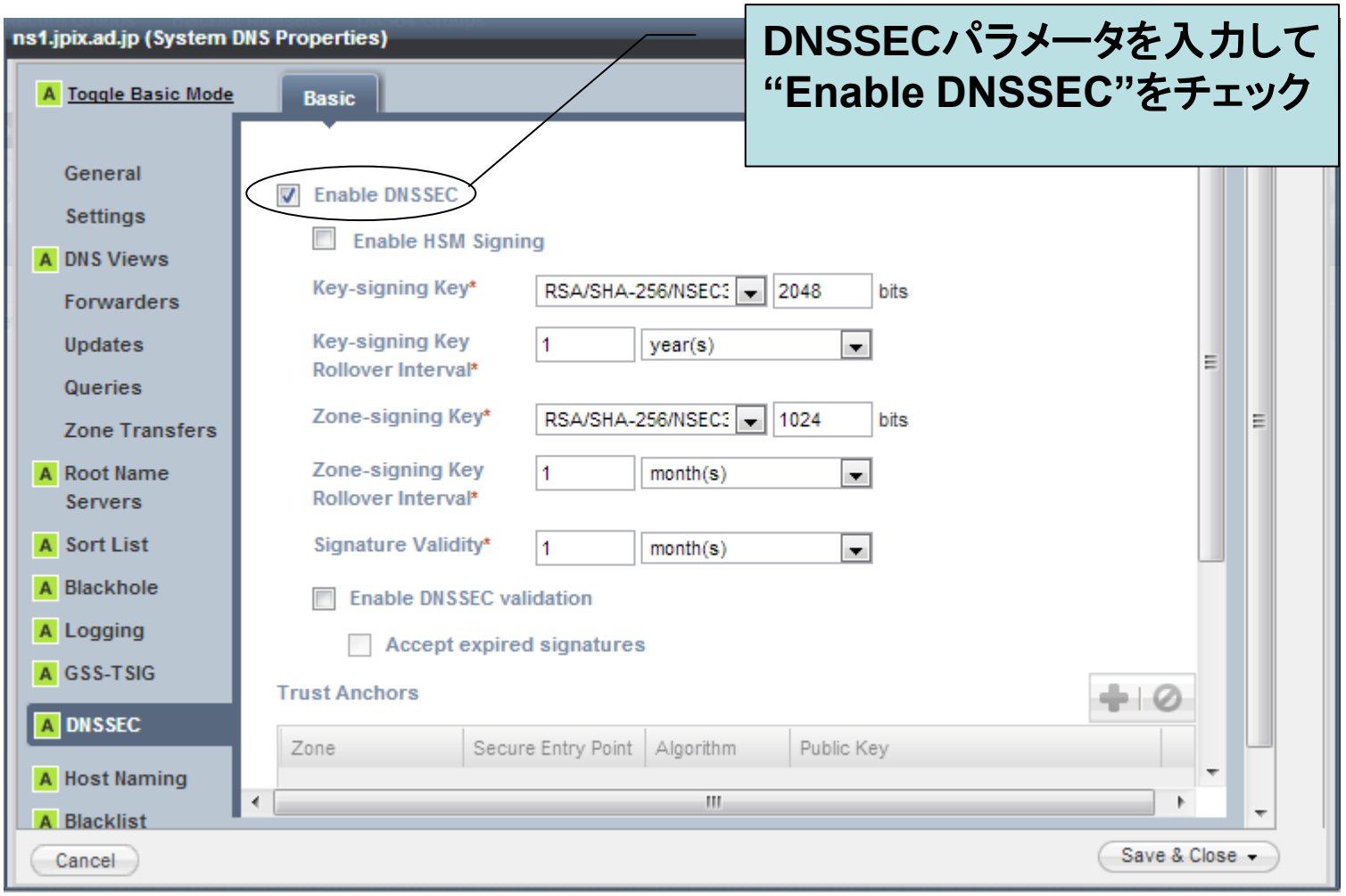
   - KSKの更新と再署名
   - DSをエクスポートして上位ゾーンに再登録

InfobloxによるDNSSEC導入作業

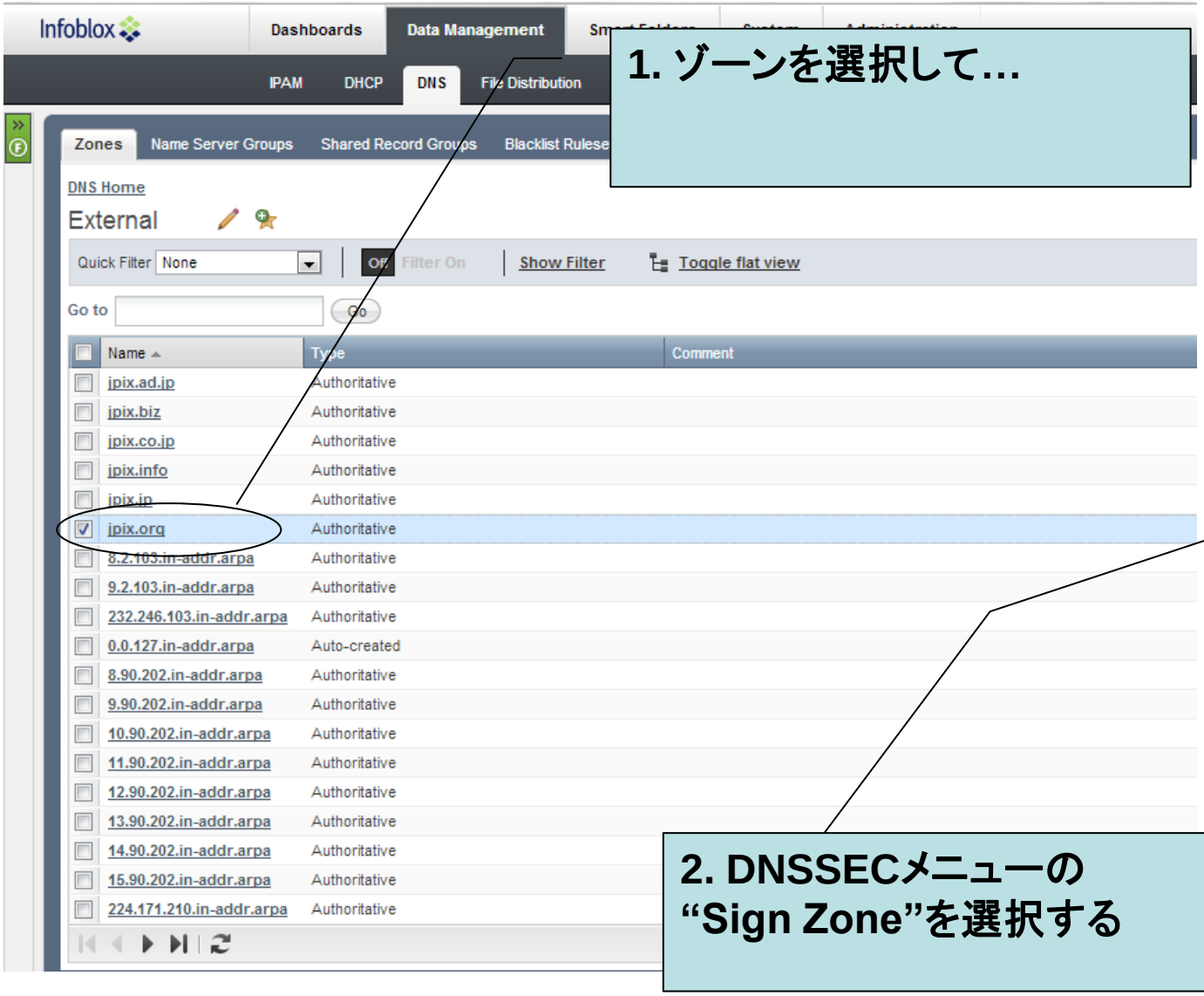
1. DNSSECパラメータの決定
4. ゾーン署名
5. DSをエクスポートして上位ゾーンに登録
9. 定期的なKSKロールオーバ
   - KSKの更新と再署名
   - DSをエクスポートして上位ゾーンに再登録

1は初期設定。4、5はゾーン署名時のみ。
9は定期的(年一回など)のみ。

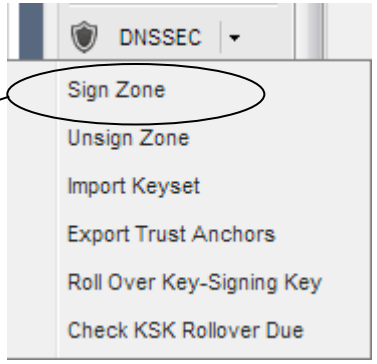
設定例）1. DNSSECパラメータの決定



設定例）4. ゾーン署名

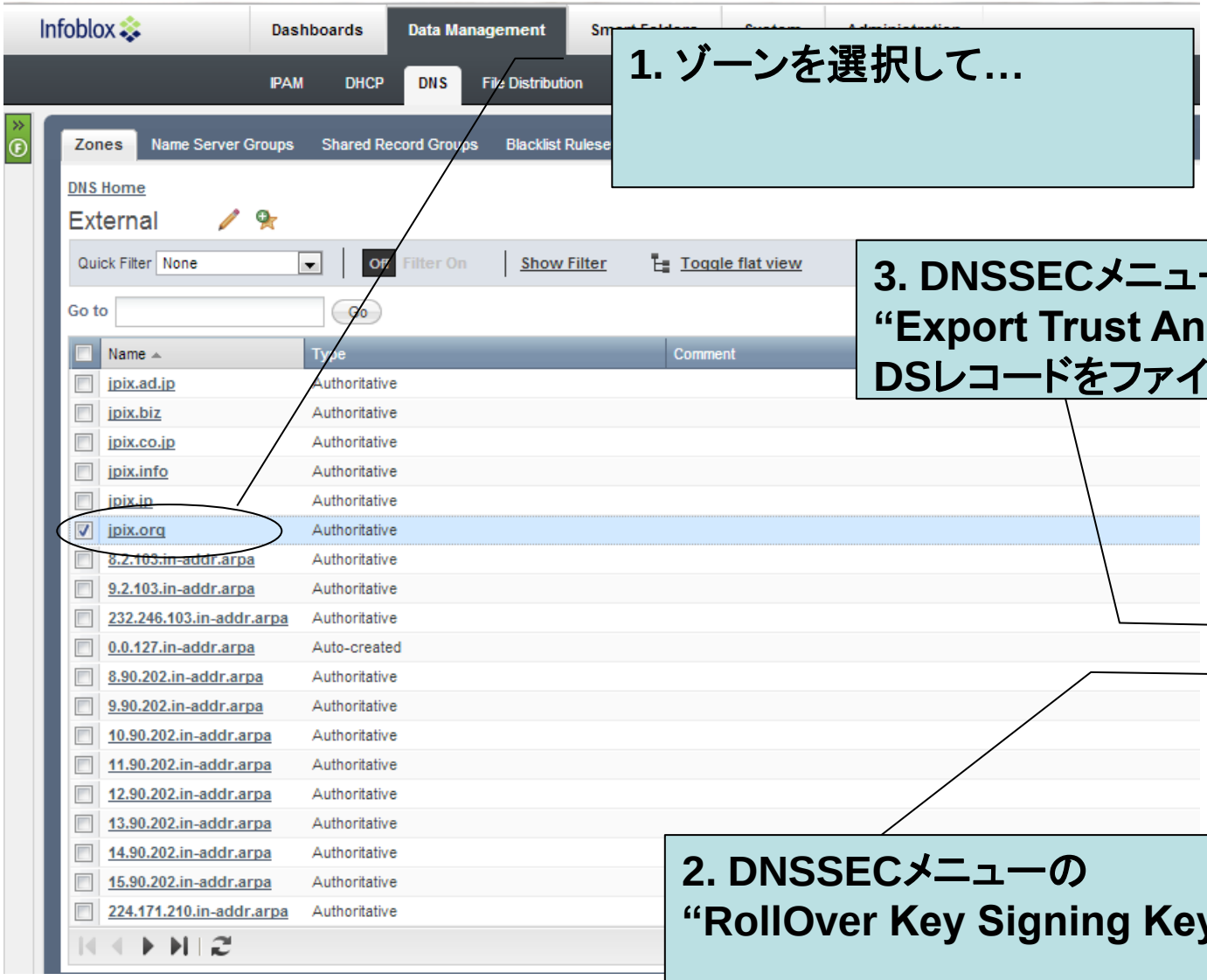


1. ゾーンを選択して…



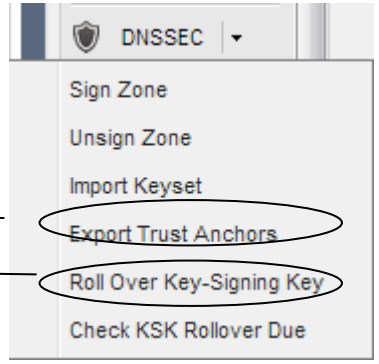
2. DNSSECメニューの
“Sign Zone”を選択する

設定例）9. KSKロールオーバ



1. ゾーンを選択して…

3. DNSSECメニューの
“Export Trust Anchor”を選択して
DSレコードをファイルに出力



2. DNSSECメニューの
“RollOver Key Signing Key”を選択する

DNSアプライアンスによるDNSSEC導入後の運用について

運用

DNSSEC導入後の運用について

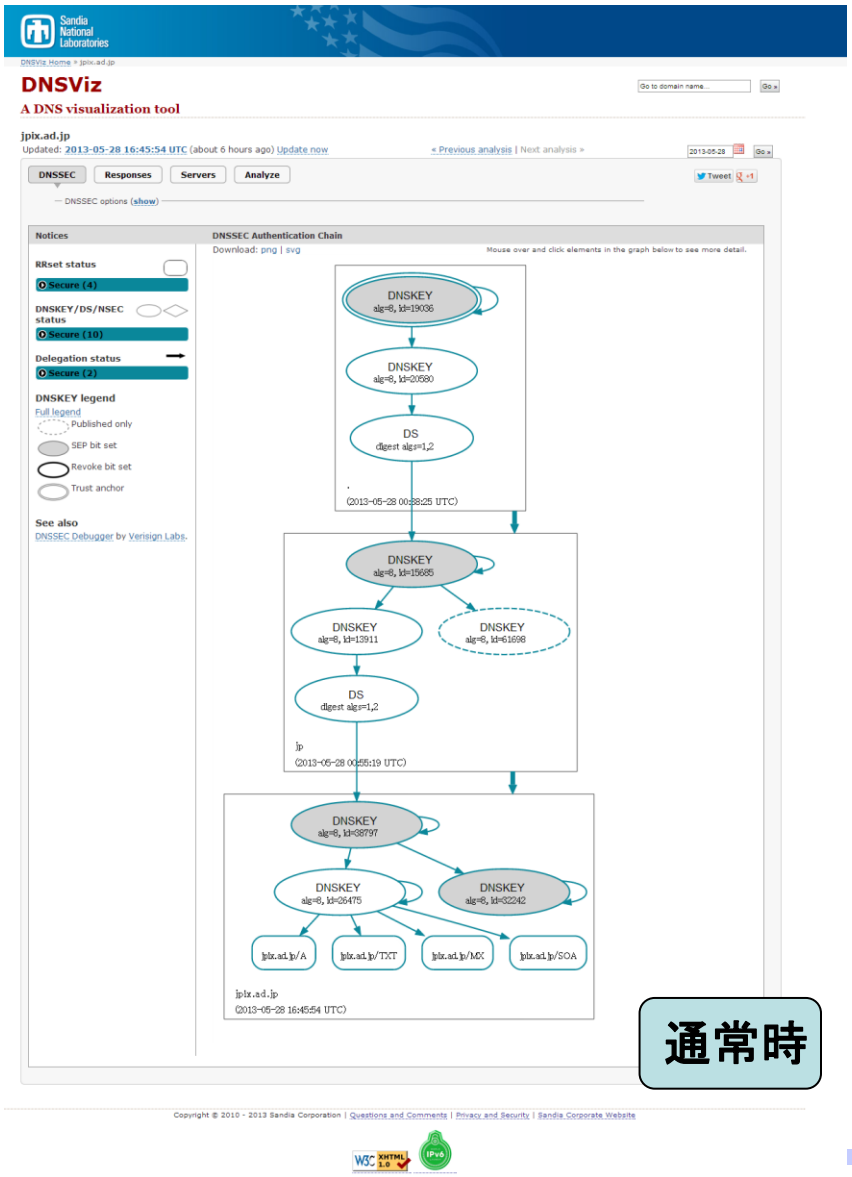
- DNSSEC署名前と基本的に変わらない
- RR追加/削除時の作業手順もDNSSEC未署名ゾーンと全く同じ
- 署名済ゾーンは年に一回KSKロールオーバを忘れずに実施するだけ
- KSKのロールオーバタイミングはWeb GUIで通知

監視について

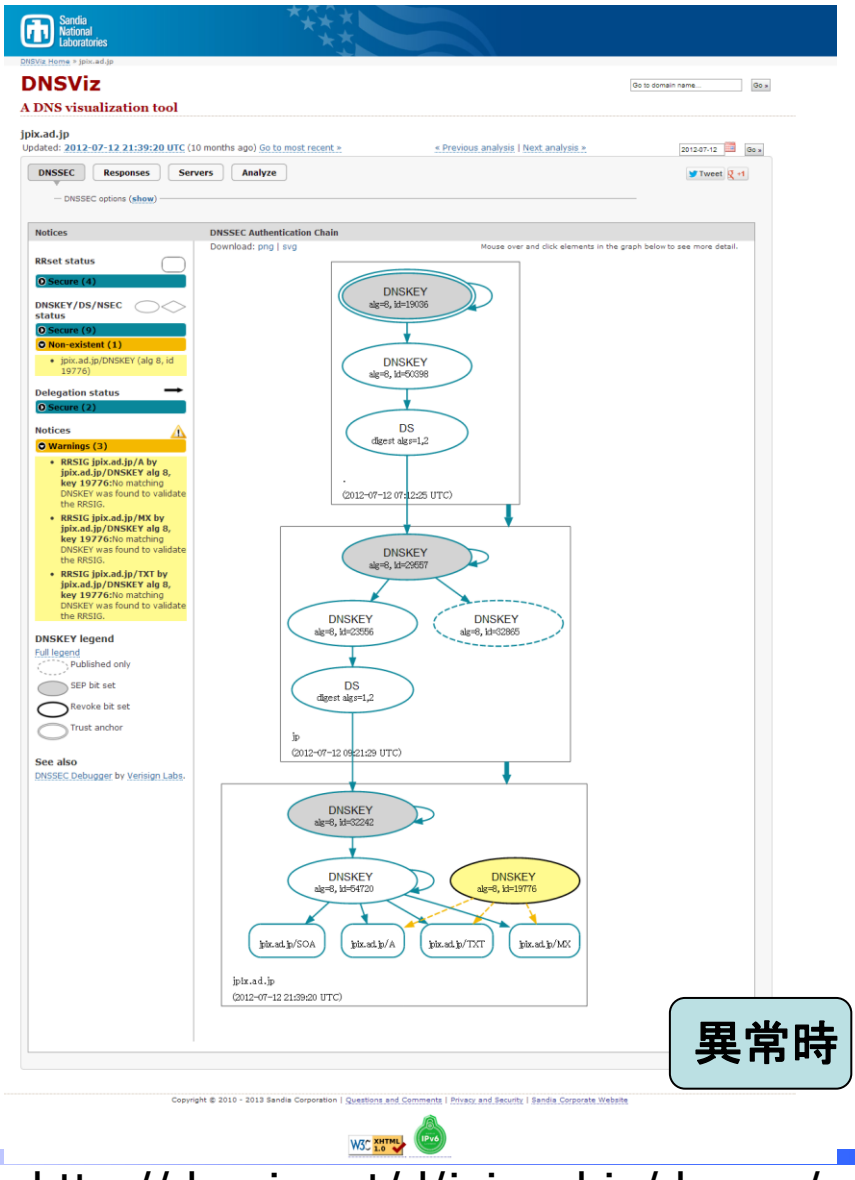
- DNSSECの常時監視は未実施
  - Nagios用のValidationプラグインを調査中
  - 何か良い監視ツールありません?
- ゾーンの変更履歴をGitで管理
  - Stealth SlaveのLinuxサーバを立ててゾーン転送したファイルの変更履歴をGit+Gitwebで管理
- 外部サイトのWebサービスを利用
  - http://dnsviz.net/がすごく便利
  - http://dnssec-debugger.verisignlabs.com/などと併用

（参考）DNSVizはすごく便利

DNSSECの信頼の連鎖をVisual化してくれるWebサービス



通常時



異常時

http://dnsviz.net/d/jpix.ad.jp/dnssec/

DNSSEC導入後のトラブル事象について

障害事例

DNSSEC導入後のトラブル事象

1. メールの受信トラブル
2. ServFail発生
3. ZSK署名ロールオーババグ

DNSSEC導入後のトラブル事象(その1)

- 署名したドメインへのメール不達
  - エラーを返すMTAがqmailで、エラーの内容が”CNAME Lookup Failure”だった場合、送信側のqmailに512バイトUDPパッチが当たっていない
  - JPRSトピックス＆コラム No.16 ■DNSSECに関するよくある質問と回答（技術仕様編）のQ6参照 <http://jpinfo.jp/topics-column/016.pdf>
  - 2社ほど申告あり

参考: http://jprs.jp/tech/notice/2011-03-03-inappropriate-handling-for-long-dns-packet.html

DNSSEC導入後のトラブル事象(その2)

- www.jpix.ad.jpでServfailが返ると連絡
  - jpix.ad.jpドメインを署名したその日に連絡あり
  - 先方のキャッシュサーバはdnssec-validation yes;
  - 4台あるキャッシュサーバのうち2台で事象発生
    - キャッシュクリアで事象解消
    - 原因は不明。署名タイミング時に変な情報をキャッシュしてしまった?
- 外部からの連絡は一件だけ

DNSSEC導入後のトラブル事例(その3)

- ZSK署名ロールオーババグ
  - ロールオーバ時に本来削除されるべき古いRRSIGがゴミとして残る
  - バリデーション的には問題なし
  - ただし各種チェックツールで警告がでる
    - dnsviz.netはWarning表示
    - jprsからRRSIG validation errorの通知メールが届く
  - 修正ファームリリース予定

まとめ

まとめ

- InfobloxによるDNSSEC環境構築/運用の敷居は低い
  - 初期導入時は「DNSSECパラメータ決定」「ゾーン署名」「上位ゾーンにDSを登録」するだけ
  - 運用は定期的に「KSKのロールオーバ」のみ
  - ZSKの更新を意識しなくてよい
  - 署名作業を意識する必要が無い
  - 複雑なコマンドを覚える必要が無い
  - 障害対応はベンダーに丸投げ可能

まとめ

- アプライアンスだからといって良いことばかりではありません…
  - Web GUIによるゾーンの一覧性が非常に悪い
    - RRSIGでRR数が増えるのでなおさら…
  - アプライアンス独自の情報が少ない
  - ベンダのDNSSEC関係障害経験値が低い?
    - 他の問い合わせに比べて対応が遅い気がする
    - そもそもDNSSECの障害切り分け大変ですけど…
  - アプライアンス独自のバグだけでなくBIND/OSの脆弱性も…
    - BIND脆弱性祭りに参加可能(もちろんアプライアンス独自の対策も施されてます…
    - 昨年はntpのうるう秒で高負荷になるバグに遭遇..

ご清聴ありがとうございました