ルートゾーンのKSKロールオーバーについて
(ISPから見た事前確認・準備のポイント)

2017年6月1日

Internet Week ショーケース @名古屋

九州通信ネットワーク株式会社 (QTNet)
技術本部　サービスオペレーションセンター

末松慶文 (yo_suematsu at qtnet.co.jp)

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

自己紹介

- 末松慶文(すえまつ よしぶみ)
  - DNSを含むサーバ関連の構築と保守などを9年ちょっとくらい。
- 九州通信ネットワーク(QTNet)
  - いわゆる電力系ISP　なんでもやっています！
  - DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)

    JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html

    QTNet: JPRSとの共同研究について　http://www.qtnet.co.jp/massmedia/2015/20150713_2.html
  - [janog38 LT] 大規模災害時のインターネットの継続提供への取り組み

    https://www.janog.gr.jp/meeting/janog38/lt-vt
  - [janog38] EDNS-client-subnetってどうよ? 改めRFC7871ってどうよ

    http://www.janog.gr.jp/meeting/janog38/program/edns
  - [APRICOT 2017] TLD Anycast DNS servers to ISPs

    https://www.slideshare.net/apnic/tld-anycast-dns-servers-to-isps

    https://2017.apricot.net/program/schedule/#/day/9/network-operations-2

どのような局面においても名前解決を継続的に提供し続けたい！

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

本発表の内容

- ルートゾーンKSKロールオーバーについて
  - ・IPフラグメントについて
  - ・トラストアンカーの更新について　※手動での更新については触れません
  - ・その他

ルートゾーンにおけるDNSSEC運用開始後、KSK ROは初の実施

※DNS及びDNSSECの基本的な部分については触れません

・[参考] IW2015 今日から始めるDNSSECバリデーション
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/t5/

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

IPフラグメントについて

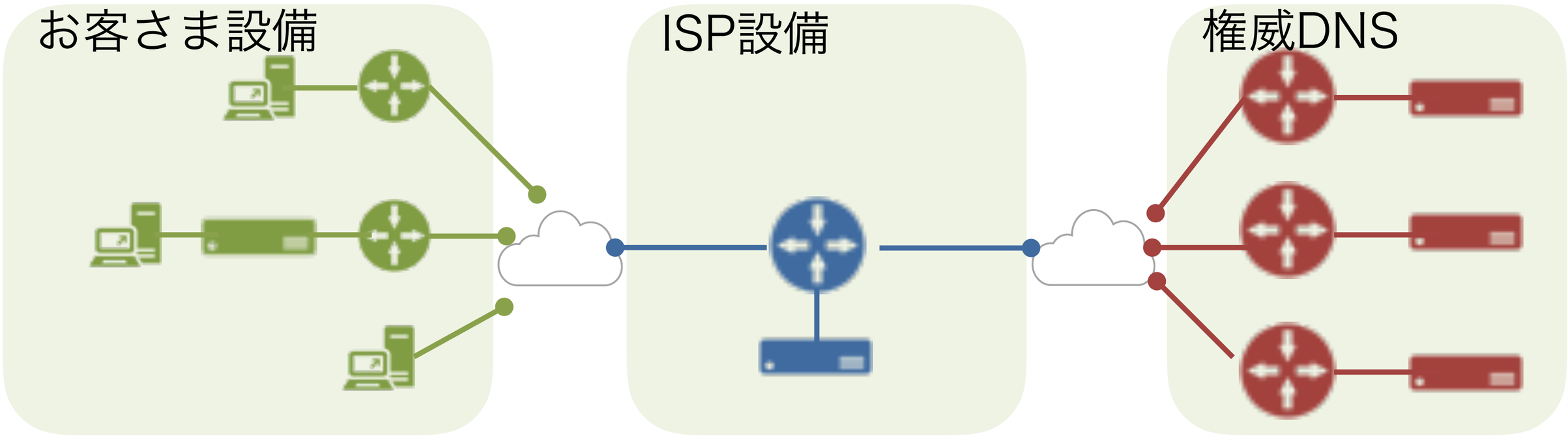
- 影響を受ける対象者と影響内容 ※検証の有効・無効に関係なくDNSKEYを取得する場合があるため
  - ・フルリゾルバー運用者(DNSSEC検証の**有効・無効**に関係なく影響する可能性)
  - ・名前解決に失敗する可能性
- 事前確認と準備のポイント
  - ・大きなUDPパケットを扱えるか
    - 512バイト以上のUDPパケットを扱えるか(edns0に対応しているか)
      - IPフラグメントしたUDPパケットを扱えるか(到着順序入れ替りも問題ないか)
  - ・TCPパケットについても扱えるか
- 確認方法
  - ・WEBから　http://keysizetest.verisignlabs.com/
  - ・コマンドラインから　dig +bufsize=4096 rs.dns-oarc.net txt +short

DNSのパケットが通る通信経路上の全ての機器で仕様の確認と検証をすることが重要

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

IPフラグメントについて

- IPフラグメントで名前解決が失敗した場合について



重要日付で問題が発生しても複数の要素が関連しており問題の切り分けが困難..

・ソフトウェア、ハードウェアの両面から仕様確認、構成の確認が必要

事前に(**今すぐにでも！**)

機器ベンダやSIerと協力して

KSKロールオーバーの際に問題が生じないことを確認することが重要！

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

トラストアンカーの更新について

- ルートゾーンのKSK定期更新について
  - ・鍵長、鍵アルゴリズムの**変更無し、実績無し** (初の実施)

- 影響を受ける可能性のある対象者と影響内容
  - ・フルリゾルバー運用者(DNSSEC検証が**有効**である場合)
  - ・更新に失敗した場合、DNSSEC検証失敗となり名前解決不可

- 更新の方法
  - ・手動更新 ※手動でのKSK更新については触れません
  - ・自動更新 (RFC5011) 例) BIND9、Unbound
  - ・自動更新 (dnssec-validation auto) 例) BIND9に含まれる鍵を用いる

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

トラストアンカーの更新について

- 事前確認と準備のポイント

[既存設定の確認(BIND)]

```
options { ...
        dnssec-enable yes_or_no;
        dnssec-validation yes_or_no | auto;
};
```

DNSSEC対応にするかどうか

DNSSEC署名検証を行うか

・dnssec-validation yes;

- trusted-keysやmanaged-keysを指定して**いる**場合、指定された物を使う
- trusted-keysやmanaged-keysを指定して**いない**場合、BIND built-inを使う

・dnssec-validation auto;

- BIND built-inを使う

予期せず、DNSSEC検証が
有効になっていませんか

※BIND 9.9.8では両方ともyesがdefault　現在どのような設定になっているか**要確認**

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

トラストアンカーの更新について

- 事前確認と準備のポイント

[鍵の更新について]

・BIND ”dnssec-validation auto;” による更新について

設定例

```
options { ...
        dnssec-enable yes;
        dnssec-validation auto;
        bindkeys-file “/etc/bind.keys”
};
```

新しいルートゾーンのトラストアンカーが含まれているか要確認

・BIND 9.9.9-P8, 9.10.4-P8, 9.11.0-P5からは更新版bind.keysが同梱

・bind.keysのみ入手することも可能

[参考]BIND 9.8.x and higher bind.keys file https://ftp.isc.org/isc/bind9/keys/9.11/

[参考]Current Root Trust Anchors (bind.keys) https://www.isc.org/downloads/bind/bind-keys/

[参考]BIND 9.11 Administration Reference Manual https://ftp.isc.org/isc/bind9/keys/9.11/

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

弊社も検証しました！

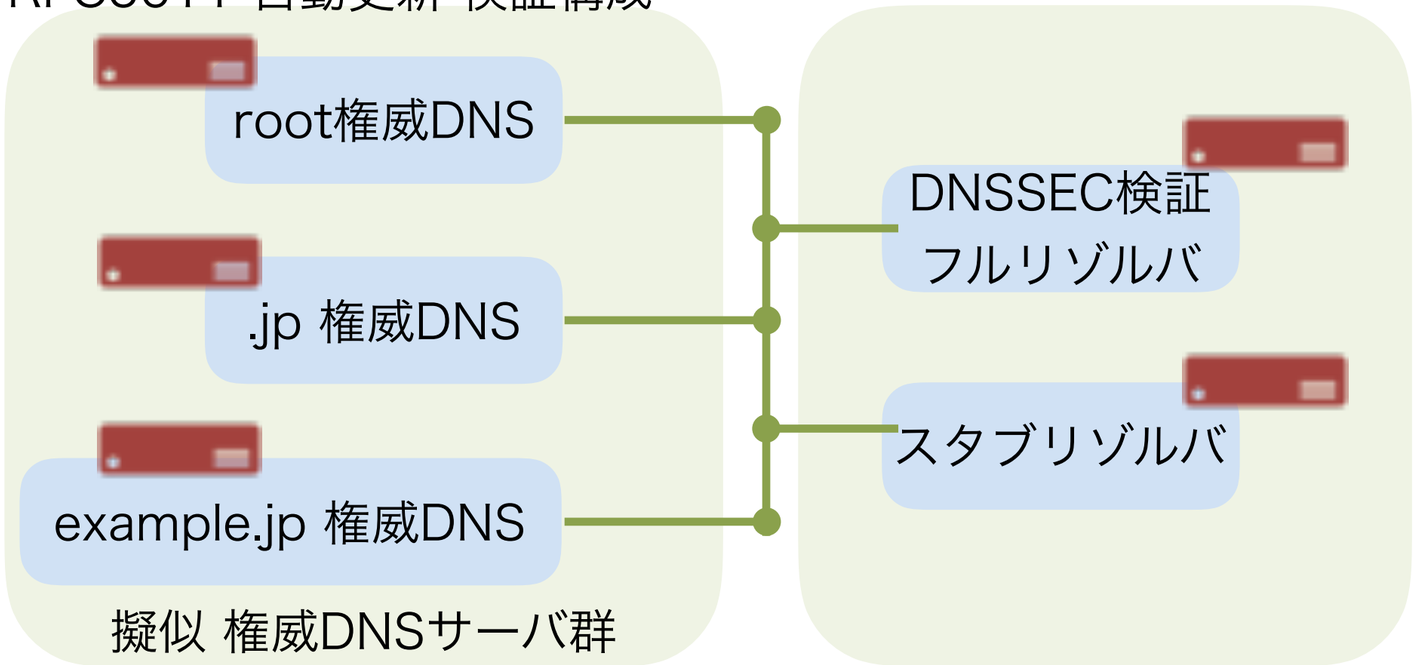
フルリゾルバのRFC5011への対応について

- 事前確認と準備のポイント

仕様と前述した設定などを確認

・ソフトウェアがRFC5011に対応しているか、自動更新が機能するか。

RFC5011 自動更新 検証構成



・検証前提

.(root)、.jp、example.jpはDNSSEC署名

hintsファイルは擬似root権威DNSを指定

- 検証の流れ

1. 新KSK生成、署名
   ・key stateが
   新KSK:add-pending, 旧KSK:validであること
   ・DNSSEC検証に失敗しないこと
2. 29日経過後
   ・1と同様の結果が得られること
3. 30日経過後
   ・新KSK:valid, 旧KSK:validであること
   ・DNSSEC検証に失敗しないこと
4. 旧KSKをREVOKEする
   ・DNSSEC検証に失敗しないこと
   ・新KSK:valid, 旧KSK:REVOKEDであること

[参考]ICANN Automated Trust Anchor Update Testbed
https://automated-ksk-test.research.icann.org/

key stateが**正しく遷移**すること、DNSSEC**検証が失敗しない**ことを確認

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

Negative Trust Anchor(NTA)について

- 事前確認と準備のポイント
  - 指定したドメイン名をDNSSEC検証を停止する機能
    - BIND9.9系, 9.10系　**未実装**
    - BIND9.11系, BIND9.9サブスクリプション版(有償)　**実装済**

      例）$ rndc nta dnssec.fail

      ※default 1時間、最大で一週間　永続化不可なので注意

ntaに指定したドメインに対して定期的にDNSSEC検証のチェックを行う
結果に問題がなければntaの設定を解除する。

※nta-recheckで間隔を指定可能(default 5分)

    - unbound1.6　**実装済**

      例）$ unbound-control insecure_add dnssec.fail

DNSSEC検証が有効な環境であればNTAの利用方法と仕様を要確認

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.

KSKロールオーバに関するその他の注意点

- DNSSEC検証が有効なフルリゾルバーについて
  - 統計情報からの監視
    - DNSSEC検証失敗数
    - 成功した検索要求
    - SERVFAIL数

平時から監視することでトレンドを把握することが重要

  - 正常性の監視
    - フルリゾルバーへルートゾーンのDNSKEYを問い合わせADbitが返ること

※失敗した場合は+cdをつけて確認

- 万が一に備えて、DNSSEC検証を停止する手順を整備しておくこと
- コールドスタンバイの場合、トラストアンカーが更新されないことに注意

・[参考] IW2015 Root KSK(鍵署名鍵)更新に対応する方法
https://www.nic.ad.jp/ja/materials/iw/2015/proceedings/t5/

重要な日付を迎える前に事前確認と準備を**確実**に行うことが重要！

Copyright © 2017 Kyushu Telecommunication Network Co., Inc. All rights reserved.