validator 3分間クッキング

株式会社ブロードバンドタワー
伊藤 高一

はじめに

- 対象
  - 今日のフォーラムに参加して、動作検証に手をつけてみようかな、という気分になってきたアナタ。
- 注意
  - 動作検証のとっかかりという前提で、かなり手を抜いています。
  - プロダクションサーバでは、先ほどのセッションで紹介のあったホワイトペーパなどを参考に、キッチリやって下さい。

用意する物

- おちゃらけてもいいサーバ
  - 動作検証の手始めなら、VMでも倉庫の片隅に眠っているサーバ機でもO.K.です。
- 9.6.2以降のBIND
  - じゃないと、(本当の)rootゾーンで使っているRSASHA256をサポートしてません。
  - プロダクションサーバではセキュリティ情報にも注意。
- インターネットへの接続性
  - NATの下流でO.K.です。

まずはvalidationしない recursiveサーバ

```
recns# cat named.conf
options {
        directory "/etc/namedb/
working";
};
```

まずはvalidationしない recursiveサーバ

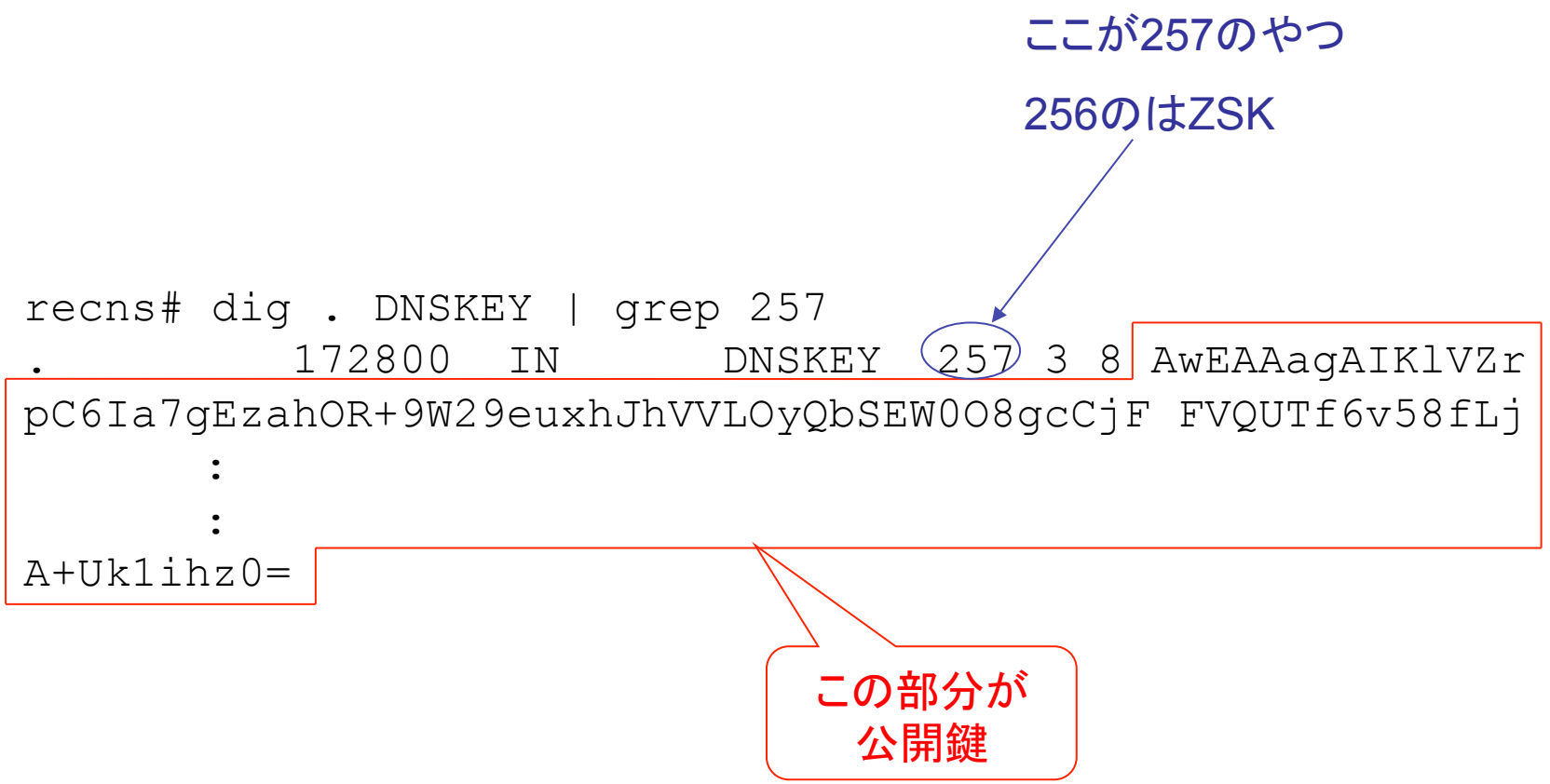
AD(Authenticated Data)は立っていない

```
recns# dig +dnssec dnssec.jp

; <<>> DiG 9.6.-ESV-R3 <<>> +dnssec dnssec.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
53631
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3,
ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec.jp.                          IN      A

;; ANSWER SECTION:
        :
```

trust anchorって?

- 「信頼の連鎖」の起点
- validatorにローカルに設定する。
- 普通はrootゾーンのKSKの公開鍵を使う。
  - 2010年7月15日以来

trust anchorを入手する



正しい手順

- プロダクションサーバでは、入手した公開鍵を「DNSSECを利用するリゾルバーのためのトラストアンカーの設定方法について」を参照して検証すること。
- 今日は思いっきり手抜き。

trust anchorを設定する

```
recns# cat named.conf
options {
        directory "/etc/namedb/
working";
};
trusted-keys {
        .  257 3 8
"AwEAAagAIKlVZrpC6Ia7
gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQ
      :
      :
```

追加

設定を反映させる

- BIND 9.6-ESV-R4では、trusted-keysを設定してrndc reconfigしただけでは反映されず、namedの再起動が必要だった。
- 他のバージョンは未調査。

これでvalidatorになった

AD(Authenticated Data)が立った

```
recns# dig +dnssec dnssec.jp

; <<>> DiG 9.6.-ESV-R3 <<>> +dnssec dnssec.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
51253
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY:
3, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;dnssec.jp.                          IN      A

;; ANSWER SECTION:
        :
```

応用編

- root以下、authoritativeサーバ群を適切に構築すると、インターネットとは独立した名前空間を作れる。
- recursiveサーバに、そっちのrootを指すroot hintと、そっちのrootのtrust anchorを設定すると、署名関係の検証も好き勝手にできる。

バリエーション

- BIND 9.7からはmanaged-keysが追加された。
  - RFC 5011方式の自動更新
- unboundは
  - trust-anchor-file: <filename>
  - trust-anchor: <"Resource Record">
  - trusted-keys-file: <filename>
  - auto-trust-anchor-file: <filename>