2011年 1 月 24 日

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

DNSSEC ジャパン 技術検証ワーキンググループ

■1. 概要

このドキュメントは、DNSSEC を利用する DNS キャッシュサーバ（またはリゾルバー）のために、現段階でよいと考えられる、トラストアンカーのデータを入手し確認する方法を説明したものです。

■2. 注意事項

このドキュメントで述べている方法が、必ずしも最善であるとは限りません。またこのドキュメントの内容は保証されたものではありません。改善点を見つけられた場合には、「■10. このドキュメントに関するご連絡先」に記載されているご連絡先までお知らせ頂ければ幸いです。

なお、このドキュメントに書かれた設定の実行環境は、以下を想定しております。

想定される実行環境
- UNIX　（ドキュメント作成には FreeBSD 7.2-RELEASE および FreeBSD 8.1 を使用）
- GnuPG　（ドキュメント作成には GnuPG 2.0.14 を使用）
- BIND 9.6 以降 （ドキュメント作成には BIND 9.7.2-P2 を使用）

■3. トラストアンカーとは何か

DNSSEC のトラストアンカーとは、リゾルバーにおける署名検証の基点です。トラストアンカーはリゾルバー毎に決められ設定されるもので、予め特定の公開鍵がトラストアンカーに選ばれるべきであると決まっているわけではありません。

一般的に、DNS は DNS ルートゾーンから、もしくは DNS ルートゾーンへ辿っていきますのでこのドキュメントでは、DNS ルートゾーンの公開鍵をトラストアンカーとするものとして説明します。

DNSSEC の署名検証を行うには、リゾルバーにトラストアンカーを適切に設定する必要があります。ここでいう適切さは以下の 2 点を指します。

a. 配布元の正しさ
　配布元が意図通りの組織（例：ICANN）であること[1]

b. 入手したものが配布されているものと同一あること
　配布されているデータと、入手したものが同一であること

[1] 執筆段階では、ルートゾーンのKSKに対する署名に使われているOpenPGPの鍵やS/MIMEの証明書がICANNのものであることを確認できず、厳密に配布元を確認する手段がありません。このドキュメントでは、この点を除いた確認方法を示します。

トラストアンカーはゾーンの KSK 公開鍵またはそのハッシュ値で表されます[1]。

■4. Web で入手したトラストアンカーの配布元の確認

入手したトラストアンカーのデータの配布元が正しいことを確認します。DNSSEC のトラストアンカーの配布は、ICANN の IANA function の一環として行われています。配布元が正しいことを確認できるようにするため、トラストアンカーを含むファイルは DNSSEC Manager <dnssec@iana.org>によって OpenPGP の署名が行われています。

以下に、この署名を確認する手順を示します。

(1) 鍵サーバや IANA の Web サーバから鍵を入手します。

(参照:■8. dnssec@iana.org の OpenPGP 公開鍵の入手元)

```
$ gpg --search-keys --keyserver <鍵サーバ> dnssec@iana.org
gpg: searching for "dnssec@iana.org" from hkp server pgp.mit.edu
(1)        DNSSEC Manager <dnssec@iana.org>
             1024 bit DSA key 0F6C91D2, created: 2007-12-01
Keys 1-1 of 1 for "dnssec@iana.org".    Enter number(s), N)ext, or Q)uit > 1
gpg: requesting key 0F6C91D2 from hkp server pgp.mit.edu
gpg: key 0F6C91D2: "DNSSEC Manager <dnssec@iana.org>" 7 new signatures
gpg: no ultimately trusted keys found
gpg: Total number processed: 1
gpg:              new signatures: 7
$
```

(2)IANA の Web サーバから最新のハッシュ値を含む xml ファイルを入手します。

```
$ fetch http://data.iana.org/root-anchors/root-anchors.xml
$
```

(3)IANA の Web サーバから OpenPGP の署名データを入手します。

```
$ fetch http://data.iana.org/root-anchors/root-anchors.asc
$
```

(4)署名を検証します。

```
$ gpg --verify root-anchors.asc root-anchors.xml
gpg: Signature made Wed Jul  7 07:49:10 2010 JST using DSA key ID 0F6C91D2
gpg: Good signature from "DNSSEC Manager <dnssec@iana.org>"
Primary key fingerprint: 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C
  91D2
$
```

署名検証に成功すれば、root-anchors.xml の配布元が IANA であると考えることができます。
確認できなかった場合、「■7. トラストアンカーの DNSKEY の正しさを確認できないときには」をご覧下さい。

次に、root-anchors.xml に含まれるハッシュ値を確認します。

■5. DNS で入手したトラストアンカーのハッシュ値との比較

以下に比較手順を示します。

(1)DNS でルートゾーンの DNSKEY を入手し、ハッシュ値を出力します。

```
$ dig . dnskey | grep 257 > rootzone-dnskey
$ dnssec-dsfromkey -2 -f rootzone-dnskey .
. IN DS 19036 8 2
49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32 F24E8FB5
$
```

(2) root-anchors.xml に含まれるハッシュ値を出力します。

```
$ cat root-anchors.xml
<Zone>.</Zone>
<KeyDigest id="Kjqmt7v" validFrom="2010-07-15T00:00:00+00:00">
<KeyTag>19036</KeyTag>
<Algorithm>8</Algorithm>
<DigestType>2</DigestType>
<Digest>49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F2
4E8FB5</Digest>
</KeyDigest>
</TrustAnchor>
$
```

(3) (1)のハッシュ値と(2)のハッシュ値を比較します。
同一であれば最新の DNSKEY のハッシュ値であることがわかります。

確認できなかった場合は、■7 をご覧下さい。

■6. トラストアンカーがきちんと使えていることを確認するには

リゾルバーにトラストアンカーを設定し、DNSSEC の署名検証を行う問い合わせを行います。

ネームサーバにおけるトラストアンカーの設定方法については、各プログラムのマニュアル等をご参照下さい。

(1)DNSSEC オプションを有効にして問い合わせを行います。

```
$ dig . ns +dnssec
:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54256
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1
:
:
$
```

応答ヘッダーの flags に ad があれば、そのリゾルバーで署名検証できていることがわかります。

■7. トラストアンカーの DNSKEY の正しさを確認できないときには

root-anchors.xml の署名の有効性が確認できなかった場合は、そこに含まれるハッシュ値を使用しないようにします。また Root DNSSEC の Web ページ（下記）をご覧になり、最新の情報を得ることをお勧めします。お問い合わせ先は「Feedback」に記載されています。

Root DNSSEC
http://www.root-dnssec.org/

もし root-anchors.xml に含まれるハッシュ値と DNS で問い合わせたハッシュ値が異なる場合には、いずれのハッシュ値も使用しないようにします。最新の root-anchors.xml は以下の URL から入手できますので、最新かどうかの確認を行うことをお勧めします。

root-anchors.xml の入手元
http://data.iana.org/root-anchors/

■8. dnssec@iana.org の OpenPGP 公開鍵の入手元

dnssec@iana.orgのOpenPGP公開鍵が入手できたPGPキーサーバー覧[2]

- pgp.mit.edu
- pool.sks-keyservers.net
- subkeys.pgp.net

この他に https://data.iana.org/root-anchors/icann.pgp からも入手できます。ただしこのサーバは、root-anchores.xml 等のファイルが置いてある、同一のサーバです。改ざんを検知するためには、OpenPGP の署名を確認するなどを行う必要があります。

[2] サーバによっては有効期限が切れている公開鍵を入手してしまうことがあります。複数のサーバを確認することをお勧めします。

■9. 日常的な運用のために

DNSルートゾーンに関する最新情報は、https://www.iana.org/dnssec に掲載されているアナウンス専用のメーリングリストを通じてアナウンスされることになっています[3]。

DNS ルートゾーンの KSK が更新された場合、リゾルバーにトラストアンカーとして設定されている KSK 公開鍵またはそのハッシュ値を設定しなおす必要があるかも知れません。メーリングリストに加入するなど、IANA のアナウンスを入手できるようにしておくことをお勧めします。

現在のアナウンス用メーリングリスト root-dnssec-announce
https://mm.icann.org/mailman/listinfo/root-dnssec-announce

■10. このドキュメントに関するご連絡先

DNSSEC ジャパン事務局 <sec@dnssec.jp>

■参考文献

[1] DNSSEC Trust Anchor Configuration and Maintenance
http://www.ietf.org/id/draft-ietf-dnsop-dnssec-trust-anchor-04.txt
[2] DNSSEC Trust Anchor Publication for the Root Zone
http://www.ietf.org/id/draft-jabley-dnssec-trust-anchor-01.txt
[3] NetAgent Official Blog：最近の DNSSEC の動向
http://www.netagent-blog.jp/archives/51489071.html

以上

[3] “DNSSEC Practice Statement for the Root Zone KSK Operator”, Root DNSSEC Design Team, https://www.iana.org/dnssec/icann-dps.txt