DNSSEC ゾーン検証ツール調査報告

平成 24 年 4 月

DNSSEC ジャパン 運用技術 WG

目次

1. はじめに

1.1. 背景

DNSSEC は正しく鍵を管理して正しい手順で正しく署名していれば、基本的に署名の有効期間内は検証に失敗することはないはずである。しかし、鍵と署名の管理は煩雑であり、慣れていないと間違いが発生しやすい。また、過去には正しい手順で署名したにもかかわらず、署名プログラムのバグにより検証できないゾーンを公開してしまった ccTLD の事例もあり、署名後のゾーンが正しく検証できるかどうかを公開前に事前テストすることは運用上有用だと考えられる。しかし、DNSSEC 署名は人間が目視でチェックできるようなものではないため、検証には正当性を機械的に判断できる手段が必要になる。DNSSEC ジャパン運用技術 WG では今回そのようなツールについて調査をおこなったので、その成果を報告する。

なお、インターネット上に公開されているゾーンに対して、署名を正しく検証できるかどうかをテストするネットワーク上のサービスもいくつか存在しているが、公開前にチェックをおこなうという観点からこの報告では取り上げない。そのようなサービスについては技術検証 WG より報告されている「DNSSEC ツール調査報告」の分類 D の項を参照されたい。

http://dnssec.jp/?p=489

1.2. 注意事項

- 免責事項

  本ドキュメントは保証されたものではない。下記 Web サイトの免責事項を確認のうえ、本ドキュメントを使用して頂きたい。

  http://dnssec.jp/?page_id=16

- 問合せ先

  本ドキュメントに関する改善点などのコメントは下記事務局まで連絡いただきたい。

  DNSSEC ジャパン事務局 <sec@dnssec.jp>

2. ゾーン検証ツールの紹介

2.1. BIND

ISC BIND に付属するユーティリティにはゾーンファイルの検証に有用なものが含まれている。

2.1.1. named-checkzone

文法チェックをおこなうツール。DNSSEC に特化したものではなく、検証できない署名があったとしても、文法的に間違っていなければ有効期間外の署名レコードなどごく一部の例外を除いて警告を出したりはしないため、DNSSEC のテストという意味では力不足である。しかし、署名前のゾーンファイルに対するチェックは強力なので、まず署名前のゾーンファイルに対して named-checkzone でテストし、これで問題なければ署名をおこない、さらに後述する

ような検証ツールでテストしてからゾーンを反映させるという手順を踏むとよいだろう。

2.1.2. dnssec-signzone

DNSSEC 署名をおこなうツールだが、実行時の引数に-a を加えると署名後にそれが正しいかどうかの検証をおこなう。ただし、署名と検証を同じプログラムでおこなうので、両者でコードを共有している部分に万が一バグが存在していると見逃す可能性もありうる点は注意が必要である。

2.2. OpenDNSSEC

OpenDNSSEC project による BSD ライセンスの DNSSEC 運用ツール。

http://www.opendnssec.org/

署名されたゾーンが正しく検証できるか内部的にチェックして、検証に成功したゾーンだけを DNS サーバにロードさせるような仕組みを備えている。ただし、近日リリースが予定されている OpenDNSSEC 1.4 からはこの検証機能が廃止されることになっているので注意が必要である。

その他、OpenDNSSEC 以外の DNSSEC 運用ツールにも、同様にゾーンの検証機能が具備されているものが多い。利用しようとするツールの機能を調べておくとよいだろう。

2.3. ldns-verify-zone

権威 DNS サーバ NSD や参照 DNS サーバ Unbound などで知られる NLNet Labs は DNS 関連のプログラムを C で開発する際に有用なライブラリ ldns も提供している。

http://nlnetlabs.nl/projects/ldns/

このライブラリにはサンプルプログラム扱いながら DNS/DNSSEC 運用に役立つユーティリティがいくつか含まれており、その中の ldns-verify-zone がゾーンファイル内にある署名レコード(RRSIG)が DNSKEY レコードに記述されている公開鍵で正しく検証できるかどうか、不在証明(NSEC/NSEC3)が適切かどうかといったチェックをおこなう。

実行例:

```
> ldns-verify-zone example.jp.signed
Checking: example.jp.
Checking: ns1.example.jp.
Checking: ns2.example.jp.
Checking: mx.example.jp.
Checking: www.example.jp.
Zone is verified and complete
```

2.4. YAZVS (Yet Another Zone Validation Script)

Verisign Labs による DNSSEC 署名されたゾーンファイルの検証ツール。GPLv2 ライセンスの perl スクリプトで、ルートゾーンや arpa ゾーンは公開前に実際にこのスクリプトを使って検証されているという。

http://yazvs.verisignlabs.com/

DNSKEY と RRSIG の対応が正しいかどうかといったゾーン内部で完結する署名検証だけではなく、トラストアンカーとして上位 NS に登録されている DS レコードを指定することで、KSK と DS レコードが正しく対応しているかも確認することができる。

実行例:

```
> yazvs.pl -a dsset-example.jp. example.jp.signed
Crypto Validation of example.jp 1330625701
------------------------------------------------------------------------
OK: Parsed 32 RRs from example.jp.signed
OK: 1 trusted KSKs found
OK: Apex DNSKEY RRset validated
OK: 0 expiring RRSIGs found
OK: 0 bad RRSIGs found
OK: 15 good RRSIGs found

Comparison to current zone
------------------------------------------------------------------------
OK: Received 32 RRs from 192.168.0.1
OK: Current serial 1330625701
DIFF: KSK 0 added, 0 removed, 1 unchanged
DIFF: ZSK 0 added, 0 removed, 1 unchanged
DIFF: RRSIG 0 added, 0 removed, 15 unchanged
DIFF: DS 0 added, 0 removed, 1 unchanged

Validation for example.jp 1330625701 PASSED, 0 problems
```

2.5. validns

Anton Berezin 氏による BSD ライセンスのゾーンファイル検証ツール。

http://www.validns.net/

前述の YAZVS や ldns-verify-zone は DNSSEC の検証に特化したものだが、この validns は未署名ゾーンの文法チェックもおこなうことも可能である。named-checkzone に DNSSEC 検証の機能を追加したものと考えるといいだろう。

開発が始まってからまだ日が浅く、当 WG の調査では検証に一部問題があることも確認されたが、バグレポート後の対応も早く、将来的には有望なツールになると思われる。

実行例:

```
> validns -s example.jp.signed
records found:          32
skipped dups:           0
record sets found:      26
unique names found:     11
delegations found:      0
    nsec3 records:      5
not authoritative names, not counting delegation points:
                        0
validation errors:              0
signatures verified:            15
time taken:             0.011s
```

2.6. donuts

SPARTA, Inc が提供している BSD ライセンスの DNSSEC 運用ツール群 DNSSEC-Tools に含まれるゾーン検証ツールで、単体での利用も可能である。

https://www.dnssec-tools.org/wiki/index.php/Donuts

検証ルールはプラグイン方式になっていて、どんなルールを用いて検証するかを自由に選択できる。大半は DNSSEC 関連のルールだが、DNSSEC 以外の検証項目もいくつか含まれている。ドメインの委譲関係を調べて正しく親子間の連携が取れているかチェックすることもできる。また、コマンドラインだけでなく GUI による利用も可能である。

実行例:

```
> donuts -v example.jp.signed example.jp
--- loading rule file rules/check_nameservers.txt
    rules: MEMORIZE_NS_ADDRS DNS_SERVERS_MATCH_DATA
--- loading rule file rules/dns.errors.txt
    rules: DNS_SOA_REQUIRED MEMORIZE_NS_CNAME_RECORDS DNS_NS_NO_CNAME
--- loading rule file rules/dnssec.rules.txt
    rules: DNSSEC_RRSIG_TTL_MATCH_ORGTTL DNSSEC_MEMORIZE_NS_RECORDS
DNSSEC_CHECK_IF_NSEC3 DNSSEC_MISSING_NSEC_RECORD
DNSSEC_MISSING_RRSIG_RECORD DNSSEC_RRSIG_NOT_SIGNING_RRSIG
DNSSEC_RRSIG_FOR_NS_GLUE_RECORD DNSSEC_NSEC_FOR_NS_GLUE_RECORD
DNSSEC_RRSIG_SIGEXP DNSSEC_NSEC_TTL DNSSEC_NSEC3_TTL
DNSSEC_DNSKEY_MUST_HAVE_SAME_NAME DNSSEC_DNSKEY_PROTOCOL_MUST_BE_3
DNSSEC_BOGUS_NS_MEMORIZE DNSSEC_MISSING_RRSIG_RECORD
DNSSEC_RRSIG_TTL_MUST_MATCH_RECORD DNSSEC_MISSING_NSEC_RECORD
DNSSEC_RRSIG_SIGNER_NAME_MATCHES DNSSEC_NSEC_RRSEC_MUST_NOT_BE_ALONE
DNSSEC_MEMORIZE_KEYS DNSSEC_RRSIGS_VERIFY DNSSEC_TWO_ZSKS
DNSSEC_OPENSSL_KEY_ISSUES
--- loading rule file rules/nsec_check.rules.txt
    rules: DNSSEC_NSEC_MEMORIZE DNSSEC_NSEC3_MEMORIZE
DNSSEC_NSEC3_CHECK DNSSEC_NSEC_CHECK
--- loading rule file rules/parent_child.rules.txt
    rules: DNS_MULTIPLE_NS DNSSEC_SUB_NOT_SECURE
DNSSEC_DNSKEY_PARENT_HAS_VALID_DS DNSSEC_DS_CHILD_HAS_MATCHING_DNSKEY
--- loading rule file rules/recommendations.rules.txt
    rules: DNS_REASONABLE_TTLS DNS_NO_DOMAIN_MX_RECORDS
--- Analyzing individual records in example.jp.signed
--- Analyzing records for each name in example.jp.signed results on
testing example.jp:
  rules considered:     38
  rules tested:         25
  records analyzed:     32
  names analyzed:       10
  errors found:         0
```

2.7. dig / drill

dig や drill などの DNS 問い合わせをおこなうツールを使って、ゾーン全体ではなくレコード単位での DNSSEC 検証が可能である。

ただし、この方法で一般に公開する前にチェックするには、隠れマスター(hidden master; NS レコードに指定されない DNS サーバ)に署名済みゾーンを置いてテストする必要があり、サーバ構成についても十分に検討しておかなければならない。

以上