DNSSEC ツール調査報告

DNSSEC ジャパン技術検証ワーキンググループ

目次

本文書の目的

DNSSEC ジャパンでは DNSSEC に対応するツールやサービス、ライブラリの調査を行いました。本文書は各組織の円滑な DNSSEC 対応に資することを目的とし、その成果を公開するものです。

調査期間：2010 年 7 月～12 月

おことわり

本文書の内容には配慮していますが正確性については保証できません。免責事項については DNSSEC ジャパン Web(http://dnssec.jp)をご参照ください。重大な誤りに気づいた場合は下記事務局までご連絡いただけると幸いです。(修正をお約束するものではありません)

sec@dnssec.jp

ツールの分類と紹介

本文書では運用ツールを下記 5 つのカテゴリに分類し紹介します。

A. DNSSEC に対応する DNS サーバ
B. DNS サーバの前段に設置し DNSSEC 対応を行う DNSSEC プロキシ
C. 鍵や署名の管理といった DNSSEC 運用を支援するツール
D. DNSSEC の動作検証や監視をおこなうツールやサービス
E. DNSSEC 対応を行う開発者向けのライブラリやツールキット

※主にオペレータ向けの運用ツールを対象にしておりユーザ向けのツールは除外しています。

A. DNSSEC に対応する DNS サーバ

■ BIND

DNSSEC に対応する権威 DNS サーバ兼キャッシュ DNS サーバです。利用者の多い DNS サーバの一つで書籍や Web で情報を入手しやすいメリットがあります。日本語の情報も豊富です。鍵の生成から署名まで DNNSEC 運用に必要なツール群を備えており、BIND のみで DNSSEC 運用を完結することができます。運用を自動化する機能は組み込まれていないため運用に際しては工夫が必要です。

開発: Internet Systems Consortium
URL: http://www.isc.org

区分: オープンソースソフトウェア

■ NSD

DNSSEC に対応する権威 DNS サーバです。利用者の多い DNS サーバの一つですが日本語の情報は少ないです。鍵の生成や署名は後述の ldns に付属するツールを使う必要があります。運用を自動化する機能は組み込まれていないため運用に際しては工夫が必要です。同じ開発元から DNSSEC に対応するキャッシュ DNS サーバである Unbound が提供されています。

開発: NLnet Labs
URL: http://www.nlnetlabs.nl
日本語サイト: http://unbound.jp/nsd/
区分: オープンソースソフトウェア

■ Unbound

DNSSEC に対応するキャッシュ DNS サーバです。同じ開発元から DNSSEC に対応する権威 DNS サーバである NSD が提供されています。

開発: NLnet Labs
URL: http://www.nlnetlabs.nl
日本語サイト: http://unbound.jp/
区分: オープンソースソフトウェア

■ Infoblox

DNSSEC に対応する権威 DNS サーバ兼キャッシュ DNS サーバです。Infoblox 社が販売する BIND をベースとしたアプライアンス製品であり、GUI による運用支援機能があります。

開発: Infoblox
URL: http://www.infoblox.com
日本語サイト: http://www.infoblox.jp/
区分: 商用製品

■ Secure64 DNS Authority&Cache&Signer

DNSSEC に対応する権威 DNS サーバとキャッシュ DNS サーバです。Secure64 社が販売する NSD をベースとしたアプライアンス製品であり、GUI による運用支援機能があります。

開発: Secure64 Software Corporation
URL: http://www.secure64.com
区分: 商用製品

■ ANS&CNS

DNSSEC に対応する権威 DNS サーバです。Nominum 社が販売するアプライアンス製品で ANS は権威 DNS サーバ、CNS はキャッシュ DNS サーバです。GUI による運用支援機能があります。大量のゾーンを管理する大規模な事業者を対象としています。

開発: Nominum
URL: http://www.nominum.com
区分: 商用製品

■ DNSSHIM

DNSSEC に対応する権威 DNS サーバです。自動で DNSSEC の再署名を行う機能を有しています。実際にサービスを行わない隠されたマスターサーバとしての運用を想定しており、BIND のスレーブサーバ自動設定機能に対応しています。また、Java で開発されているため JRE が動作するあらゆる環境で動作します。

開発: Registro de Dominios para a Internet no Brasil
URL: http://registro.br/dnsshim/
区分: オープンソースソフトウェア

B. DNS サーバの前段に設置し DNSSEC 対応を行う DNSSEC プロキシ

■ F5 DNS SECURITY SOLUTIONS

権威 DNS サーバの前段に設置することで DNSSEC に対応させることができる製品です。ハードウェアモジュールを活用しリアルタイムに DNSEC の署名を行う機能を有しています。GUI による運用支援機能があります。

開発: F5 Networks
URL: http://www.f5.com
日本語サイト: http://www.f5networks.co.jp/
区分:商用製品

■ Phreebird Suite

権威 DNS サーバの前段に設置することで DNSSEC に対応させることができる製品です。レコードの不在証明(NSEC3)に意図的に偽ったレコードを返すなど、DNSSEC の仕様に正しく準拠していない点が多いため利用や導入にあたっては注意が必要です。(Ver.1.02 時点)

開発: Dan Kaminsky
URL: http://s3.amazonaws.com/dmk/phreebird_suite_1.02.tar.gz
区分: オープンソースソフトウェア

C. 鍵や署名の管理といった DNSSEC 運用を支援するツール

■ OpenDNSSEC

DNSSEC 運用の全過程を自動化することを目的として作られた運用支援ツールです。鍵の管理、ゾーンの再署名、鍵のロールオーバーをスケジューリングして実行します。署名されたゾーン情報の完全性を検証する機能も有しています。動作には HSM(Hardware Security Module)が必要ですが、HSM のソフトウェア実装である SoftHSM が同じ開発者から提供されています。

開発: .SE, Kirei, NLnet Labs, Nominet, SIDN, Sinodun Internet Technologies, SURFnet
URL: http://www.opendnssec.org
区分: オープンソースソフトウェア

■ DNSSEC Tools

DNSSEC の運用を容易にするための運用支援ツール集です。DNSSEC の署名を検証するバリデータや、自動で鍵のロールオーバーを行うデーモン、ゾーン情報の視覚化ツール、DNSSEC 関連ライブラリ、各種アプリケーション用の DNSSEC サポートパッチなどで構成されています。

URL: http://www.dnssec-tools.org
区分: オープンソースソフトウェア

■ Vantages

DNSSEC の運用を容易にするための運用支援ツールです。親ゾーンと子ゾーンの DS/DNSKEY を同期を監視し鍵交換の適切なタイミングを通知する機能や、DNSKEY のトラストアンカーを自動的に配布・検証する機能、権威 DNS サーバの最大 MTU サイズを調査する機能などを提供します。GUI による運用支援機能もあります。

開発: Colorado State University Network Security Group
URL: http://www.vantage-points.org
区分: オープンソースソフトウェア

■ DNSSEC Zone Key Tool

DNSSEC ゾーンの鍵と署名を管理するツールです。BIND で提供される DNSSEC 関連ツールと同程度の機能を有しています。少数の DNSSEC ゾーンのメンテナンス上の問題を解決する目的で設計されています。

開発: Holger Zuleger
URL: http://www.hznet.de/dns/zkt/
区分: オープンソースソフトウェア

■ DNSSEC Key Management Tool

DNSSEC の鍵と署名の管理を支援するツールです。BIND で提供されるツール群のフロントエンドとして動作します。データベースを用いて鍵や署名の管理を行います。

開発: RIPE NCC
URL: http://www.ripe.net/disi/dnssec_maint_tool/
区分: オープンソースソフトウェア

■ Thales (タレス) 社 nShield (エンシールド) シリーズ HSM

暗号化や電子署名の際に使われる暗号鍵を安全に運用するための HSM (ハードウェア・セキュリティ・モジュール)です。BIND9 等で DNSSEC の署名を付与する際の鍵の生成、保管、更新、廃棄などライフサイクルで必要となる管理作業を、漏洩や改竄の危険から防御する形で実施できます。安全度の目安として CC や FIPS など国際セキュリティ基準の認証を受けており、PCI DSS 対応などでも使われています。

開発: Thales e-Security
URL: http://iss.thalesgroup.com/
日本語サイト: http://iss.thalesgroup.com/ja-JP.aspx
区分: 商用製品

D. DNSSEC の動作検証や監視をおこなうツールやサービス

■ DNSSEC Debugger

Verisign が提供する DNSSEC 動作確認サービスです。対象ドメインの鍵や署名、ルートゾーンからの信用の連鎖に問題がないかを検証します。

提供: Verisign Labs
URL: http://dnssec-debugger.verisignlabs.com
日本語サイト: https://www.verisign.co.jp/ (DNSSEC Debugger は未掲載)
区分: サービス

■ DNSViz

DNS の視覚化サービスです。DNSSEC にも対応しており対象ドメインの鍵や署名、ルートゾーンからの信用の連鎖に問題がないかを検証し視覚化します。

提供: Sandia National Laboratories
URL: http://dnsviz.net
区分: サービス

■ DNS Check

.SE が提供する DNSSEC 動作確認サービスです。対象ドメインの鍵や署名、ルートゾーンからの信用の連鎖に問題がないかを検証します。RSA-SHA256 や RSA-SHA512 には対応していません。

開発: .SE
URL: http://dnscheck.iis.se
区分: サービス

■ DNS Reply Size Test

DNS が 512byte を超えるパケットを受け取ることができるかを確認するためのテストゾーン。応答の値によって EDNS0 への対応や途中経路での IP フラグメントフィルタの有無を検証できます。

開発: DNS-OARC
URL: https://www.dns-oarc.net/oarc/services/replysizetest
区分: サービス

E. DNSSEC 対応を行う開発者向けのライブラリやツールキット

■ libbind

BIND を開発する ISC から提供されている DNS 関連ライブラリです。DNSSEC に対応しています。

開発: Internet Systems Consortium
URL: http://www.isc.org
区分: オープンソースソフトウェア

■ ldns

NSD や Unbound を開発している NLnet Labs から提供される DNS 関連ライブラリです。DNSSEC に対応しています。サンプルコード扱いで署名や鍵生成などのツールが含まれています。

開発: NLnet Labs
URL: http://www.nlnetlabs.nl
区分: オープンソースソフトウェア

■ Net::DNS

Perl で実装された DNS 関連ライブラリです。DNSSEC に対応しています。

URL: http://www.net-dns.org
区分: オープンソースソフトウェア

■ DNSRuby

Ruby で実装された DNS 関連ライブラリです。DNSSEC に対応しています。

URL: http://dnsruby.rubyforge.org
区分: オープンソースソフトウェア

■ DNSJava

Java で実装された DNS 実装です。DNSSEC をサポートしています。

URL: http://www.dnsjava.org/
区分: オープンソースソフトウェア

■ DNSPython

Python で実装された DNS 関連ツールキットです。DNSSEC に対応しています。

URL: http://www.dnspython.org/

区分: オープンソースソフトウェア