WebARENA

JAIPA 情報セキュリティ部会 勉強会
DNSSEC: 技術と運用

2010/11/10 15:00-17:00

(株)NTTPCコミュニケーションズ
高田美紀 @mikiT_T

©2010 NTTPC Communications, Inc.

agenda

- キャッシュサーバ
- 権威サーバ
- 動作確認
- トラブルシューティング
- Q&A

©2010 NTTPC Communications, Inc.

想定環境

- CentOS 5
- OpenSSLのバージョン番号が古い
  - CentOSの脆弱性対応ポリシー
    - バージョンは上げず、穴を塞ぐ
  - あまり古いと新しい暗号アルゴリズムに対応していない
- #はroot作業、$は一般ユーザ作業

©2010 NTTPC Communications, Inc.

DNSSEC対応ソフトウェア

- BIND
  - 9.6-ESV以降、9.7がおすすめ
    - トラストアンカー自動更新
    - Smart Signing
  - 権威/キャッシュサーバ両方の機能
  - http://www.isc.org/software/bind/

©2010 NTTPC Communications, Inc.

Internet Systems Consortium

login

search GO

DOWNLOADS

DOWNLOADS (software) solutions services community store about ISC support us

(BIND) DHCP AFTR BIND 10 other software projects security advisories software forums

BIND

BIND is by far the most widely used DNS software on the Internet. It provides a robust and stable platform on top of which organizations can build distributed computing systems with the knowledge that those systems are fully compliant with published DNS standards.

BIND 9.7.2-P2

Released on 28 Sep 2010

BIND 9.7.2-P2 is a current production release.

Source Download **Windows Download** Release notes

BIND 9.6-ESV-R2

Released on 23 Sep 2010

BIND 9.6-ESV-R2 is a current Extended Support Version of BIND.

Source Download **Windows Download** Release notes

BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet. It is a reference implementation of those protocols, but it is also production-grade software, suitable for use in high-volume and high-reliability applications. BIND is available for free download under the terms of the ISC License, a BSD style license.

- Documentation and external links
- Vendor products based on ISC BIND

ISC developed and maintains BIND 9, the current version. Our ability to maintain this

ISC developed and maintains BIND 9, the current version. Our ability to maintain this
software and be actively involved in furthering core Internet protocols is directly

BIND

- What is BIND, History of BIND
- FAQ
- New features and capabilities
- BIND news, mailing lists and bug reporting
- Security advisories
- Professional services - Support contracts, Training
- Download BIND by specific version
- Current status of versions
- DNSSEC and BIND
- BIND 10

visit our store

It's like a bake sale, but for programming.

BINDインストール

```
# yum -y install gcc openssl-devel

$ wget http://ftp.isc.org/isc/bind9/9.7.2-P2/
bind-9.7.2-P2.tar.gz

$ tar zxf bind-9.7.2-P2.tar.gz

$ cd bind-9.7.2-P2/

$ ./configure --with-openssl --disable-
openssl-version-check --prefix=/usr/local/

$ make

# make install
```


©2010 NTTPC Communications, Inc.

configureオプション

- --with-openssl
  - OpenSSLライブラリを利用する
- --disable-openssl-version-check
  - openssslのバージョンによる脆弱性チェック回避
- --prefix=/usr/local/
  - インストールは /usr/local/ へ

©2010 NTTPC Communications, Inc.

キャッシュサーバ

- クライアントからのクエリに応じて再帰問い合わせを行い、答えを戻す
- 問い合わせ内容をキャッシュする
- DNSSECの署名検証を行う
- BIND
- Unbound (Appendix参照)

©2010 NTTPC Communications, Inc.

キャッシュサーバ設定(1)

- named.conf の options {}; に設定追加
  - dnssec-enable yes;
    - デフォルトでyesなので実際には不要
  - dnssec-validation yes;
    - 署名検証を行う

©2010 NTTPC Communications, Inc.

キャッシュサーバ設定(2)

- . (root) のトラストアンカーを managed-keys {}; に設定
  - RFC5011的に自動更新される(はず)

```
managed-keys {
  "." initial-key 257 3 8 "
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=";
};
```


©2010 NTTPC Communications, Inc.

rootトラストアンカー設定

- dig . dnskey | grep -w 257

```
.           84482    IN   DNSKEY   257 3 8
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS Qageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=
```

- managed-keys {}; 設定

```
        "." initial-key 257 3 8

"AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efuc p2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sG IcGOYl7OyQdXfZ57relS Qageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0=";
```


©2010 NTTPC Communications, Inc.

rootトラストアンカー検証1

```
$ wget --quiet https://data.iana.org/root-anchors/icann.pgp
$ gpg --import --quiet icann.pgp
$ gpg --list-keys --fingerprint dnssec@iana.org
pub   1024D/0F6C91D2 2007-12-01 DNSSEC Manager <dnssec@iana.org>
               指紋 = 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2
sub   2048g/1975679E 2007-12-01
```

公開PGPサーバにて指紋確認

http://pgp.nic.ad.jp/pks/lookup?op=vindex&search=dnssec%40iana.org&fingerprint=on

同じ？

Public Key Server -- Verbose Index
``dnssec@iana.org ''

```
Type bits /keyID    Date       User ID
pub  1024D/0F6C91D2 2007/12/01 DNSSEC Manager <dnssec@iana.org>
     Key fingerprint = 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C
sig         76092287             Olaf M. Kolkman <olaf@dacht.net>
sig         C9B42848             Kim Davies <kim@iana.org>
sig         0F6C91D2             DNSSEC Manager <dnssec@iana.org>
```


©2010 NTTPC Communications, Inc.

rootトラストアンカー検証2

```
$ wget --quiet https://data.iana.org/root-anchors/root-anchors.xml
$ cat root-anchors.xml
<?xml version="1.0" encoding="UTF-8"?>
<TrustAnchor id="AD42165F-3B1A-4778-8F42-D34A1D41FD93" source="http://data.iana.org/root-anchors/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>49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5</Digest>
</KeyDigest>
</TrustAnchor>
$ wget --quiet https://data.iana.org/root-anchors/root-anchors.asc
$ 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>"
gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 2FBB 91BC AAEE 0ABE 1F80  31C7 D1AF BCE0 0F6C 91D2
$ dig . dnskey | grep -w 257 >root-ta.key
$ /usr/local/sbin/dnssec-dsfromkey root-ta.key|grep -w 2
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32 F24E8FB5
```

同じ？

©2010 NTTPC Communications, Inc.

キャッシュサーバ設定(3)

- トラストアンカー更新ファイル自動生成
  - namedユーザの書き込み権が必要
  - drwxr-x--- root:named /var/named
  - そのまま起動するとエラー発生

```
managed-keys.bind.jnl: create: permission denied

managed-keys-zone ./IN: keyfetch_done:dns_journal_open
-> unexpected error
```

  - managed-keys-directory { “/var/named/keys/”; }; など書き込める設定

©2010 NTTPC Communications, Inc.

BIND 起動前の準備

- 起動スクリプトの準備
  - /usr/ から /usr/local/ へ
- その他TIPS
  - $PATH に気をつける
  - -4 オプション
    - IPv6接続性がないのに IPv6アドレスがインタフェースについている場合

©2010 NTTPC Communications, Inc.

BIND 起動

```
# service named start
$ ps axww|grep named
 5572 ?        Ss     0:00 /usr/local/sbin/
named -u named
 9855 pts/0    S+     0:00 grep named
$ tail /var/log/messages
Sep 22 14:21:47 baguette named[5572]: starting
BIND 9.7.2-P2 -u named
Sep 22 14:21:47 baguette named[5572]: built
with '--with-openssl' '--disable-openssl-
version-check' '--prefix=/usr/local/'
                    :                  :
Sep 22 14:21:47 baguette named[5572]: running
```


©2010 NTTPC Communications, Inc.

キャッシュサーバ確認

```
$ dig . ns +dnssec @127.0.0.1
; <<>> DiG 9.7.2-P2 <<>> . ns +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12049
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 14, AUTHORITY: 0,
ADDITIONAL: 4

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

;; ANSWER SECTION:
.                 498176 IN    NS    d.root-servers.net.
(略)
.                 498176 IN    NS    b.root-servers.net.
.                 498176 IN    RRSIG NS 8 0 518400 20100928000000 20100920230000 41248 .
gOG4vxTajV51RXajibiPsRmKE8VB9Yj7VgTA54T/r47v1Yki1rZvS9BI 0O6Ht0hfv+eBAIv+oQ5F5mjzPuY72ngIVolOzqISgAUhF
+O8uO4bc0Ss jykeZk76TS4CwPmsabyL43UjIaQSNIH5tliRE+ETr9NAzQzIl+uhz7gq sEY=

;; ADDITIONAL SECTION:
e.root-servers.net.    604744 IN    A     192.203.230.10
m.root-servers.net.    604698 IN    A     202.12.27.33
m.root-servers.net.    604698 IN    AAAA  2001:dc3::35

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Sep 22 14:37:04 2010
;; MSG SIZE  rcvd: 457
```

署名検証ok!

©2010 NTTPC Communications, Inc.

権威サーバ

- DNSのデータを保持するコンテンツサーバ
- BIND
- NSD (Appendix参照)

©2010 NTTPC Communications, Inc.

権威サーバでのDNSSEC対応

- 鍵の作成
- ゾーンへの署名
- 上位へDSレコードを登録(依頼をする)

©2010 NTTPC Communications, Inc.

鍵の作成

- ZSKの作成

鍵アルゴリズム　鍵長　ゾーン名

```
# dnssec-keygen -a RSASHA256 -b 1024 skrd.org
Generating key pair.........................+++++
+ .............++++++
Kskrd.org.+008+07623
```

- KSKの作成

鍵アルゴリズム　鍵長　KSK　ゾーン名

```
# dnssec-keygen -a RSASHA256 -b 2048 -f ksk skrd.org
Generating key pair............++
+
.....................................................
.....................................+++
Kskrd.org.+008+27841
```


©2010 NTTPC Communications, Inc.

鍵ファイルの中身(ZSK)

```
# cat Kskrd.org.+008+07623.key
; This is a zone-signing key, keyid 7623, for skrd.org.
; Created: 20100923020356 (Thu Sep 23 11:03:56 2010)
; Publish: 20100923020356 (Thu Sep 23 11:03:56 2010)
; Activate: 20100923020356 (Thu Sep 23 11:03:56 2010)
skrd.org. IN DNSKEY 256 3 8 AwEAAdb81Gi8EkBRQ61qP/JbXeaLkRCCberyqZqHJDsety6ZYXGFbmVy
m6pQfz232NexZVwj8BM6MuUlAWGF1X0V+520DDLAozYbG6HZ8PM/CPXl
Ab6O38l8fYtjFhAoiiyxf2oHr6xxiYCf0MQn4JxYeuItms59+2uKuBEJ ojLp4M2d
# cat Kskrd.org.+008+07623.private
Private-key-format: v1.3
Algorithm: 8 (RSASHA256)
Modulus: 1vzUaLwSQFFDrWo/8ltd5ouREIJt6vKpmockOx63LplhcYVuZXKbqlB/
PbfY17FlXCPwEzoy5SUBYYXVfRX7nbQMMsCjNhsbodnw8z8I9eUBvo7fyXx9i2MWECiKLLF/agevrHGJgJ/
QxCfgnFh64i2azn37a4q4EQmiMungzZ0=
PublicExponent: AQAB
PrivateExponent: Df6DLRYg8gLYLu+dnf8Ii7tGBBcZZJPLKn3lg9up/OSLDUKsPvpI27tFrRTMjq3DdU35kKbXLUdNYbW
+gdfueuTd2EB151F/Z7m7q1xNN4IUtwjQgVSgvv7gRrmGIbhy4RbPsx5SNxikUscsHSdKPgm1pUy5cCFiSosB8YNYH9k=
Prime1: /TnWsUg7+D3quZl6k3EFiAkS/8G3ptRECFt7E35/2HJ//et1fm11GbqA2yW6g0JdnSaHzTwcqyIXZVpBaLz7ow==
Prime2: 2VfA239530CJkifg2Sp+RHliIsSloTVc+v9ghqbnn0kSQ1QAVwFQ19rEtdAbHhvA78SgzWMz0eDfCiXTqZulvw==
Exponent1: PMpGzRZvNx/+GoJK19x5HHg5NGbX5NfuYSc8+6gRnu+V5GpDMY
+rXfrU9kcvaFVlTdWzIkT9CORNQ4qQS0mbCw==
Exponent2: 0bBNXDgP3+nHEKCy2TKbIfsuSDcLSY5Ph8XtXdwXqeD44sZfkZGuaqMhl/wQvaqvKWS
+c4nbTAk1hvfZz1Bgxw==
Coefficient:
+QvvH0GECljH8SaZq6eZpLB8QTEFb3uZxevZ6ygZa0PXn26Zm12ucNWkmSkSPtzjY58bXSsYrH4GnQQEe5yAfQ==
Created: 20100923020356
Publish: 20100923020356
Activate: 20100923020356
```


©2010 NTTPC Communications, Inc.

鍵ファイルの中身(KSK)

```
# cat Kskrd.org.+008+27841.key
; This is a key-signing key, keyid 27841, for skrd.org.
; Created: 20100923020410 (Thu Sep 23 11:04:10 2010)
; Publish: 20100923020410 (Thu Sep 23 11:04:10 2010)
; Activate: 20100923020410 (Thu Sep 23 11:04:10 2010)
skrd.org. IN DNSKEY 257 3 8 AwEAAcmreXb4nc7dhs1j8RMm7E70YDCwjohsEVIgkw2kCAi5ze3S/4kH
gSUe2zaQ9zKUS1usssHssgVCcXuwqjbZDW+ZyOXQ+uia7+4/3m3aDa0F hLvJF7N5WGny7z194NAsuvKrt6xurMhFlnkIH8w4/kqDUvbl07jhV7fG
RO3b0MBzeFASlCIDU2mNOQs8Rk5TpVLhXx4OGcmbwoyKwI3IfBL0FBEt 2lYHqvNrOzo56PeBThvt6a9miYpd6VGmILfPKeJ/RXadwXb7cupn7npy
vVLz7Z0l+7mlGfkLC1e7bLLpNPWvpsb6YOXstO0kkeBqZGjcAH5jkUAJ SYoduDSzyh8=
# cat Kskrd.org.+008+27841.private
Private-key-format: v1.3
Algorithm: 8 (RSASHA256)
Modulus: yat5dvidzt2GzWPxEybsTvRgMLCOiGwRUiCTDaQICLnN7dL/iQeBJR7bNpD3MpRLW6yyweyyBUJxe7CqNtkNb5nI5dD66Jrv7j/
ebdoNrQWEu8kXs3lYafLvPX3g0Cy68qu3rG6syEWWeQgfzDj
+SoNS9uXTuOFXt8ZE7dvQwHN4UBKUIgNTaY05CzxGTlOlUuFfHg4ZyZvCjIrAjch8EvQUES3aVgeq82s7Ojno94FOG
+3pr2aJil3pUaYgt88p4n9Fdp3Bdvty6mfuenK9UvPtnSX7uaUZ+QsLV7tssuk09a+mxvpg5ey07SSR4GpkaNwAfmORQAlJih24NLPKHw==
PublicExponent: AQAB
PrivateExponent: WC4SPmMXHYzflI9OqgEq8psINEH/EMewCykTI7PFj4su7/6CnXgakBCd6Y4ZiJQvHza0Mvc8H/
CdjmgBBVqC9XlYzqRCEdMtdg+XQpFFyZHQKAwVwPQeJLWExm50DpKAa/uJpGwAQNGsqd9TiAijqBEkBbEYko51vHWFTjv/
WyZbhiPOAXPbpBaFsQM8SupvRqE6LLH1012StKb08Vb3MZzBy5koOS57GHYKz/
g81bRuYEboHzAufvg2KknzMfNfQKdqEE9QK6z3cSbaBifnqzy5lv0TDcvRg2k5oFGLFKgHxy0qdAEvd7JOG3vuXqYsjt1hM7n2DCesJmbO30ACAQ=
=
Prime1: 5/WS565JkDMqqAQAt0nPGlRD0b6xSQxYE9/LmVhQZ5Z99vMfYiMlWH+AT9JlhZa4Bm6fJgU3N/A
+F7Oh0hzDlA21yR56TnQUY9VoFn47ovfyZy0epQrLEc2SX5BuA+HNbZGyrCb1qSY91Sw99sE4iAmRCuyRDFqlwY1TeTYuwZE=
Prime2: 3pJAB5lNKA4Ot9b7sJ/Ufx8OwEbP22l5FiQn1xcPX7y/
aPE4LEdDn7g7OImtrkueypCsUB4IUVLhvQMSevPkshjD9VfE0hvxLfkkVfB6KOgwOO7BER5aQKMDfT0gI7kRO7+RDA2MDEm+i5VbuebWR/
VuQ5pxF36jNPVUtG8p+K8=
Exponent1: VkWhAOhy1d4h9GGgvosGKz3CB6XMHGYp8CJhgEQ3i3+OlCWyu3Zk8nhhic6wEbKP
+Vx1dtejxPtmrLwT6KjoGQ3MWeQrCzjjSIpb71m95owfrT470pikFJgH4+E8+dam6CSzdpH69pGRl9KfrUIKO5aLSqvX+udQFR/yNvfvBfE=
Exponent2: GphRLFdGH+4mFhOLOZyvkI0Ofy028xnUTS/+zrXDsYXlPU3tj2TokLI76VKSPUxt6fiFjoE4Lzd/
H825LJXuEtXgvHVDYHPUStEFZXt5rV+pO3RT/46n7CdOaG2gZIRdqc0HMPCBdoptSVKMhlct7aVHCq7uqocIS3CxMWpDEqM=
Coefficient: ySkzg8SLXoBnFxk8VYzPQraIT3QJIttbCDRh5ITr/
IQgRXOHKR387+i9Ku5oHOYOMiI8uslfJ2ZM2lweWTr6f6HCETqnQkMCuJI2sfkdu0yB4EZvg38iaDtg4twQ0Ic4xrLEUyJnmDNQGOQWaPn75MhzEK
MiEZvSaAiYdIlggew=
Created: 20100923020410
Publish: 20100923020410
Activate: 20100923020410
```


©2010 NTTPC Communications, Inc.

ゾーンへの署名

NSEC3のsalt
16進文字列で適宜指定

SOAのシリアル更新

ゾーン名

```
# dnssec-signzone -3 ec1067 -N unixtime -S skrd.org
Fetching KSK 27841/RSASHA256 from key repository.
Fetching ZSK 7623/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
skrd.org.signed
```

署名済ゾーンのファイル

©2010 NTTPC Communications, Inc.

署名済ゾーンファイルの中身

```
; File written on Thu Sep 23 15:35:03 2010
; dnssec_signzone version 9.7.2-P2
skrd.org.               3600    IN SOA  cherry.skrd.org. root.cherry.skrd.org. (
                                        1285223703 ; serial
                                        3600       ; refresh (1 hour)
                                        900        ; retry (15 minutes)
                                        2419200    ; expire (4 weeks)
                                        300        ; minimum (5 minutes)
                                        )
                        3600    RRSIG   SOA 8 2 3600 20101023053503 (
                                        20100923053503 7623 skrd.org.
                                        YER624kn+Nxr3iBUxhUpO56uOIpzlKvRQMNq
                                        TPQeiu2CGeAs7ozhLeNPavsJi6O4sQSNroVx
                                        MS6hB6cmNVsKZ7lHkilaLnEf69vmiEstGoHx
                                        CtTxBDgGsWiF80XqLm4pi7ganaGEQv3YMb1x
                                        5JG6eVRXAm5NtykZ/vRcXAWYJ5U= )
                        3600    NS      cherry.skrd.org.
                        3600    NS      currant.skrd.org.
                        3600    RRSIG   NS 8 2 3600 20101023053503 (
                                        20100923053503 7623 skrd.org.
                                        bVYOUcnXII/rlYr2INPVWP6B+SWxd7O5qZtj
                                        4Sij8bT2PpYpkgVQVxM0sQhpgMYTw1kkUBhC
                                        EF0A8BoEDDp/aTuWVtt90TiimEADdcqrBks4
                                        zCy4V8paT1B2AjP0JimO0Y+MY7uk4JzHbMpi
                                        K+yYHfmvvX7Wa7aEBQWnVOBfU5Y= )
                        3600    A       59.106.173.70
                        3600    RRSIG   A 8 2 3600 20101023053503 (
                                        20100923053503 7623 skrd.org.
                                        hSj0IkVbWQqP9nku9PQYMbEss/uz0JjrXmja
                                        Y1cgxmpZhKkMBfw2Sjs2glhhKZudAoTflrkm
                                        zIZFT+SMRd+NqufBqCRlvQ6HWPup/bvYH8h7
                                        fs6JtY1GfAAhc+v1+eRfE9KFj74r8rf/eqGE
                                        Kwy8nnPBZyxI6svEskY5U9q+rW0= )
```


©2010 NTTPC Communications, Inc.

named.conf編集、リロード

```
zone "skrd.org" IN {
        type master;
        file "skrd.org.signed";
};

# rndc reload
server reload successful
```

署名済ゾーンファイルに書き換え

ログ確認

```
zone skrd.org/IN: (master) removed
reloading configuration succeeded
zone skrd.org/IN: loaded serial 1285223703 (DNSSEC signed)
managed-keys-zone ./IN: loaded serial 0
reloading zones succeeded
zone skrd.org/IN: sending notifies (serial 1285223703)
client 202.212.225.201#33884: transfer of 'skrd.org/IN': AXFR-style IXFR started
client 202.212.225.201#33884: transfer of 'skrd.org/IN': AXFR-style IXFR ended
```


©2010 NTTPC Communications, Inc.

自サーバにて確認

```
$ dig skrd.org dnskey @127.0.0.1

; <<>> DiG 9.7.2-P2 <<>> skrd.org dnskey @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48401
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;skrd.org.              IN    DNSKEY

;; ANSWER SECTION:
skrd.org.       3600 IN    DNSKEY    257 3 8
AwEAAcmreXb4nc7dhs1j8RMm7E70YDCwjohsEVIgkw2kCAi5ze3S/4kH gSUe2zaQ9zKUS1usssHssgVCcXuwqjbZDW
+ZyOXQ+uia7+4/3m3aDa0F hLvJF7N5WGny7z194NAsuvKrt6xurMhFlnkIH8w4/kqDUvbl07jhV7fG
RO3b0MBzeFASlCIDU2mNOQs8Rk5TpVLhXx4OGcmbwoyKwI3IfBL0FBEt
2lYHqvNrOzo56PeBThvt6a9miYpd6VGmILfPKeJ/RXadwXb7cupn7npy vVLz7Z0l
+7mlGfkLC1e7bLLpNPWvpsb6YOXstO0kkeBqZGjcAH5jkUAJ SYoduDSzyh8=
skrd.org.       3600 IN    DNSKEY    256 3 8 AwEAAdb81Gi8EkBRQ61qP/
JbXeaLkRCCberyqZqHJDsety6ZYXGFbmVy m6pQfz232NexZVwj8BM6MuUlAWGF1X0V+520DDLAozYbG6HZ8PM/CPXl
Ab6O38l8fYtjFhAoiiyxf2oHr6xxiYCf0MQn4JxYeuItms59+2uKuBEJ ojLp4M2d

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Sep 23 15:38:05 2010
;; MSG SIZE  rcvd: 450
```


©2010 NTTPC Communications, Inc.

上位へDSレコードを登録

- dsset-ゾーン名.というファイルが自動生成
  - DSレコードが格納されている

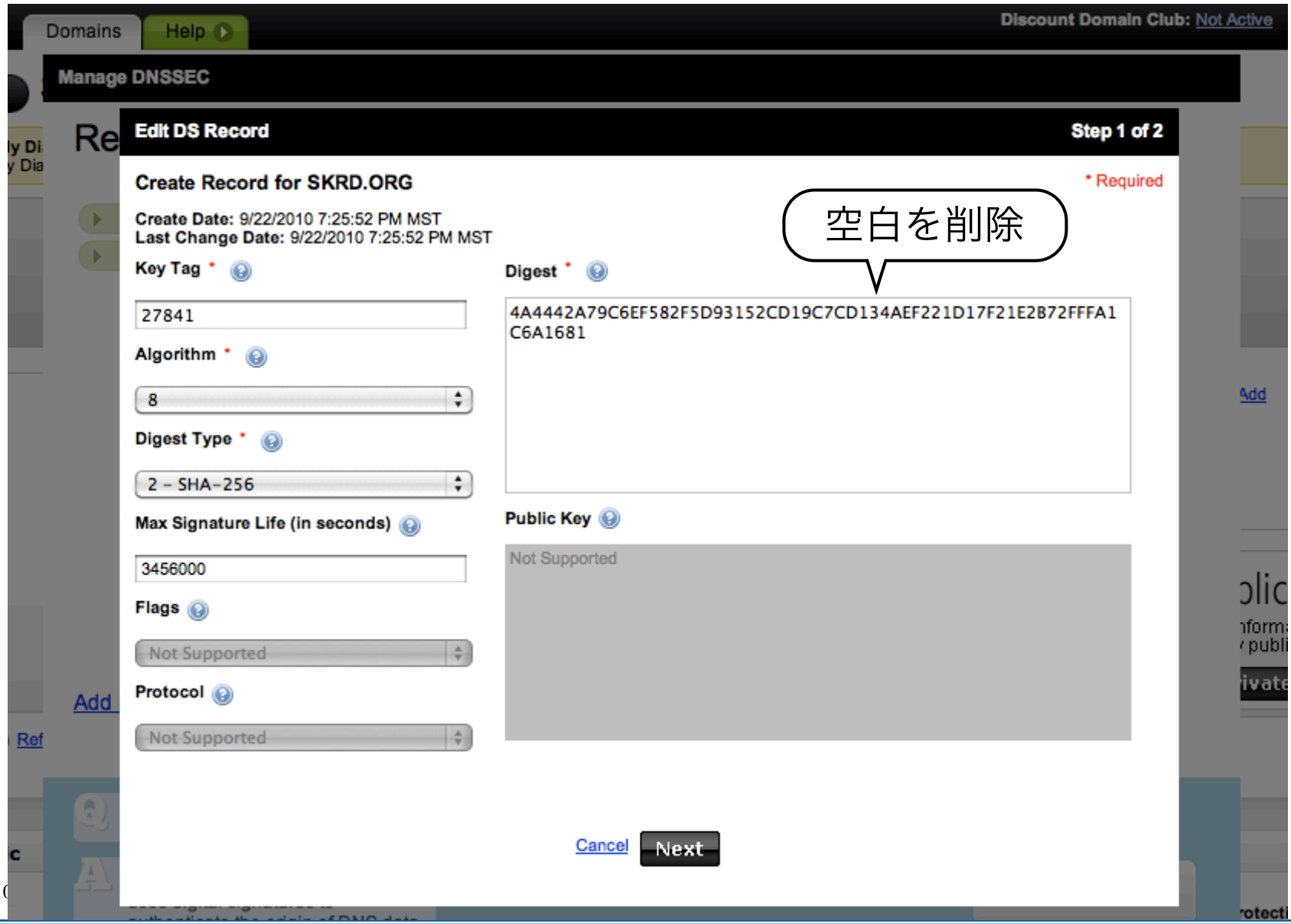
```
$ cat dsset-skrd.org.

skrd.org.    IN DS 27841 8 1
54953D271219D69316928729E6A1DA276A95F44

skrd.org.    IN DS 27841 8 2
4A4442A79C6EF582F5D93152CD19C7CD134AEF221D17F2
1E2B72FFFA 1C6A1681
```


©2010 NTTPC Communications, Inc.

GoDaddyの場合



©2010 NTTPC Communications, Inc.

再署名

- 署名には有効期限がある
  - RRSIGレコード右辺5つめのフィールド

    3600 RRSIG SOA 8 2 3600 20101023031030
  - それまでに再署名を行う必要がある
  - ゾーンへの署名と同様の作業
- 自動的実行等スケジューリング

©2010 NTTPC Communications, Inc.

鍵のロールオーバー

- ZSK
  - Double signatures (二重署名方式)
  - Pre-publication (事前公開方式)
- KSK
  - Double signatures (二重署名方式)
  - Double-DS(二重DS方式)
  - Double-RRSet (二重RRSet方式)

©2010 NTTPC Communications, Inc.

ZSKの更新(事前公開方式)

公開(publish)は今すぐ

(例)使用開始は2週間後

```
# dnssec-keygen -a RSASHA256 -b 1024 -P now -A now+2w skrd.org
Generating key pair.....................................++++++
Kskrd.org.+008+41178
# dnssec-signzone -3 ec1069 -N unixtime -S skrd.org
Fetching KSK 27841/RSASHA256 from key repository.
Fetching ZSK 7623/RSASHA256 from key repository.
Fetching ZSK 41178/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 1 stand-by, 0 revoked
skrd.org.signed
```

新ZSK

適宜変更

rndc reload を忘れないように!

©2010 NTTPC Communications, Inc.

ZSKの入れ替え

- -Aで指定した期間が経過した後ならいつでも可能

```
# mv Kskrd.org.+008+07623.* bak/
# dnssec-signzone -3 ec1070 -N unixtime -S skrd.org
Fetching KSK 27841/RSASHA256 from key repository.
Fetching ZSK 41178/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked

skrd.org.signed
```

別ディレクトリへ

rndc reload を忘れないように!

©2010 NTTPC Communications, Inc.

KSKの更新(二重署名方式)

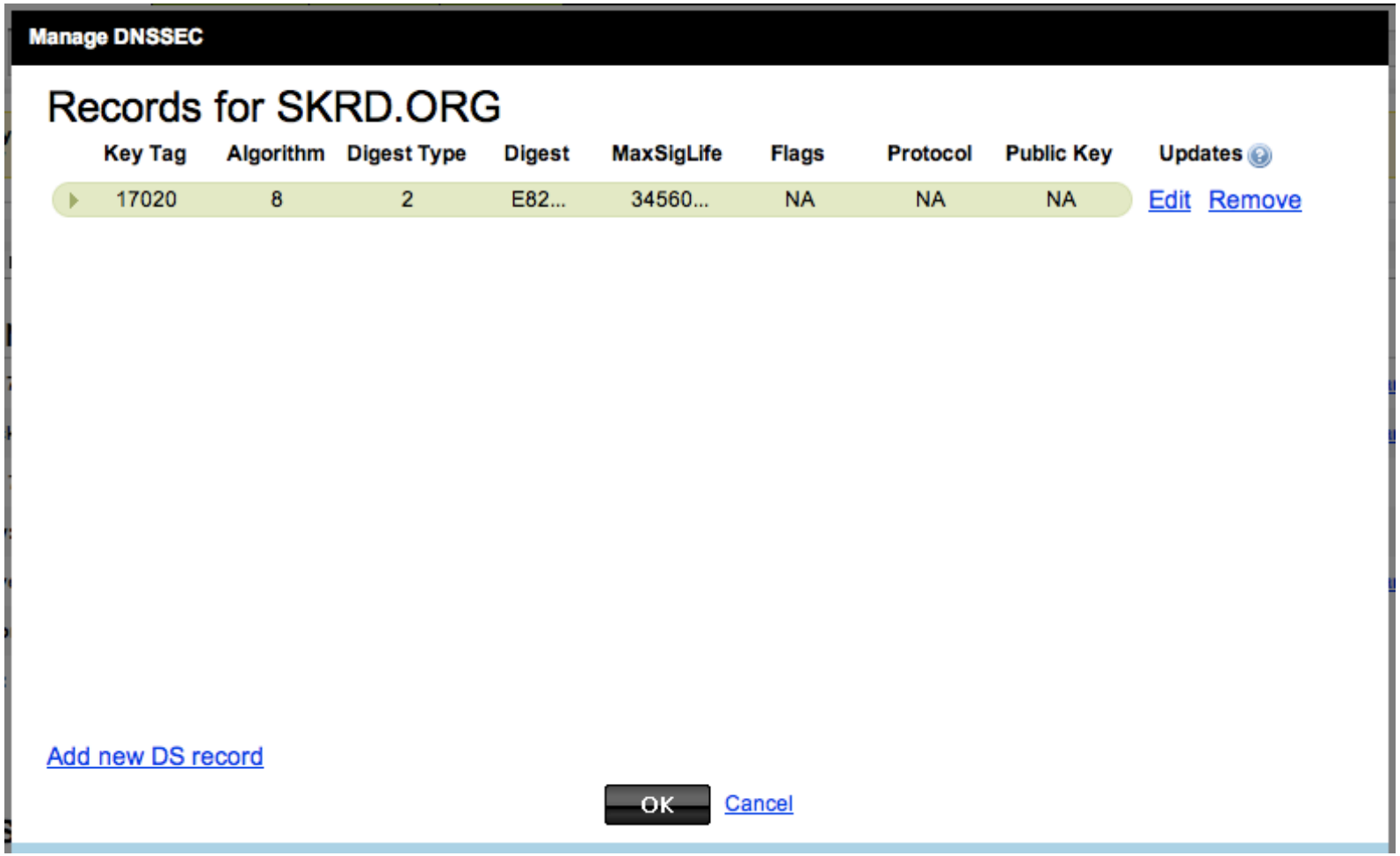
```
# dnssec-keygen -a RSASHA256 -b 2048 -f ksk skrd.org
Generating key pair.....................+++ ......................+++
Kskrd.org.+008+17020
# dnssec-signzone -3 ec1071 -N unixtime -S skrd.org
Fetching KSK 17020/RSASHA256 from key repository.
Fetching KSK 27841/RSASHA256 from key repository.
Fetching ZSK 41178/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 2 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
skrd.org.signed
# cat dsset-skrd.org.
skrd.org.         IN DS 17020 8 1 52F9E6AE3D4D90D61CC8F04935B5F45829C76BA1
skrd.org.         IN DS 17020 8 2
E82664DBBC7C24826C1D29AA70F7708BB34FDFE29D52387B0D354554 F6A1E1A6
skrd.org.         IN DS 27841 8 1 54953D271219D693165928729E6A1DA276A95F44
skrd.org.         IN DS 27841 8 2
4A4442A79C6EF582F5D93152CD19C7CD134AEF221D17F21E2B72FFFA 1C6A1681
```

新KSK

rndc reload を忘れないように!

©2010 NTTPC Communications, Inc.

DSの入れ替え



©2010 NTTPC Communications, Inc.

KSKの入れ替え

```
# mv Kskrd.org.+008+27841.* bak/
# dnssec-signzone -3 ec1072 -N unixtime -S skrd.org
Fetching KSK 17020/RSASHA256 from key repository.
Fetching ZSK 41178/RSASHA256 from key repository.
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
skrd.org.signed
```

rndc reload を忘れないように!

©2010 NTTPC Communications, Inc.

whois

```
Domain ID:D159715153-LROR
Domain Name:SKRD.ORG
Created On:22-Jul-2010 08:06:11 UTC
Last Updated On:23-Sep-2010 13:32:19 UTC
Expiration Date:22-Jul-2011 08:06:11 UTC
Sponsoring Registrar:GoDaddy.com, Inc. (R91-LROR)
(略)

Name Server:CURRANT.SKRD.ORG
Name Server:CHERRY.SKRD.ORG
(略)

DNSSEC:Signed
DS Created 1:23-Sep-2010 13:32:18 UTC
DS Maximum Signature Life 1:3456000 seconds
DS Key Tag 1:17020
Algorithm 1:8
Digest Type 1:2
Digest
1:E82664DBBC7C24826C1D29AA70F7708BB34FDFE29D52387B0D354554F6A1E1A6
```


©2010 NTTPC Communications, Inc.

トラブル実例

```
$ dig fail.skrd.org ns

; <<>> DiG 9.7.2-P2 <<>> fail.skrd.org ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 36998
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fail.skrd.org.                 IN     NS

;; Query time: 5 msec
;; SERVER: 124.146.194.76#53(124.146.194.76)
;; WHEN: Fri Sep 24 00:32:41 2010
;; MSG SIZE  rcvd: 31

$ dig fail.skrd.org ns +cd

; <<>> DiG 9.7.2-P2 <<>> fail.skrd.org ns +cd
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13357
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;fail.skrd.org.                 IN     NS

;; ANSWER SECTION:
fail.skrd.org.            3572   IN     NS     cherry.skrd.org.

;; ADDITIONAL SECTION:
cherry.skrd.org.    3572   IN     A      59.106.173.70
cherry.skrd.org.    3572   IN     AAAA   2002:3b6a:ad46::1

;; Query time: 24 msec
;; SERVER: 124.146.194.76#53(124.146.194.76)
;; WHEN: Fri Sep 24 00:32:46 2010
;; MSG SIZE  rcvd: 96
```

checking disabled

返答あり

©2010 NTTPC Communications, Inc.

トラブルシューティング例

```
$ dig fail.skrd.org rrsig +cd
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.2-P2 <<>> fail.skrd.org rrsig +cd
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19051
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 4, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;fail.skrd.org.                 IN      RRSIG

;; ANSWER SECTION:
fail.skrd.org.          3600    IN      RRSIG   NS 8 3 3600 20100923151356 20100923141056 2895
fail.skrd.org. djqAzjF09KTRQJa5N31HJCLAWrFW7hSlFVXbI1FZjP4ZSy2E106cAJYo HuYcRLoEALvKMbdM/
WIGOoMXqmQ1YBiMSNf1nXxjJZDM2nr06DeRGksY BO4v5t+3JIuKZIYnQ+XpfXThjDgJaKZPe8mjV9UaFuy5zEZMIKlfAQra
exc=

fail.skrd.org.          3581    IN      RRSIG   DNSKEY 8 3 3600 20100923151356 20100923141056 2895
fail.skrd.org. UFEaIqSzfpkUyfI+lwmhtWjZGW4ZbMeEUWHK+HB0cK/edqK2tkwscXaQ
kbOtA0fjC9YJAuHWVyDtjhfIMbxBNLHIN3dhahmqTxaRs+8wZfgmYL84
DY8HpSo9KLw9Q3GiiaiRyXVfBjKXfHaZMyxOTFjd4tRv9+qHC4h0qOx8 5V0=

fail.skrd.org.          3581    IN      RRSIG   DNSKEY 8 3 3600 20100923151356 20100923141056 64294
fail.skrd.org. OQgyVMYRDzDV8uRLX8bJrRr/9fBZiu1oZ8OrSTGMOYrn6kxLBNthUZRg
ozBXEDNUTtqqKVpr6RyCRfLhwcPjRGuy3AhQQmoG08NJakfRCdMDVjQW
P7VCqRgQAKNT3HWyeveToIFPu2voFt3QpMjkml4CY4cxXuq5LiYeiaxq
yLj3WsWxH8THHJx9gaTi2mQcSVGjJvUcpThYJlfdA0nxW7/dscVICmtM
qRB0yrmgtGylnFPUAYUn0ky07exFGXQvyFBgWfKtXZLqj//+YTkDXA3w GhN/0XFxkMRfb+N3htUFbcdOpQeIkIQYn
+f2DUa3IyoIWUN8QHuQ9B7Y Imyaqw==
fail.skrd.org.          3578    IN      RRSIG   DS 8 3 3600 20101023140723 20100923140723 41178 skrd.org.
OxRW/zwh1beUBTFa8VMgEPiXyfF3lrA4nRGxxOdu1YFtA55yS4NZPaet Qj7sWU0q3ZrdE/nKXHR2J/Nh8iUTa/+X
+xRWNaH1xgwDhQcuhi/Ymn2/ SUEfmGBPcaTeMCHZd/SIfNtgPh1rysaHdqb7gs/7ZKi4X1SUTXQSm38l ARI=
```

署名の有効期限切れ

©2010 NTTPC Communications, Inc.

チェックツール

- 設定内容のチェック
- 自組織内
  - dig example.jp. soa +dnssec など
- 他組織からはどう見えているか?
- 信頼の連鎖が保たれているかどうか?

©2010 NTTPC Communications, Inc.

DNS-OARC ODVR

- The DNS Operations, Analysis, and Research Center の Open DNSSEC Validator Resolver
- 自組織外からの検証に利用できる
- resolv.conf に設定するやり方が紹介されているが、dig で @ 指定しても ok
- https://www.dns-oarc.net/oarc/services/odvr

©2010 NTTPC Communications, Inc.

DNS-OARC

Domain Name System Operations Analysis and Research Center

Hot News

Introduction to DNS-OARC PDF

Joining and Participating in DNS-OARC

DNS-OARC Workshop and AGM: October 13-14 in Denver, Colorado

DNS-OARC Public Comment on ICANN's DNS-CERT Business Case

Meeting Calendar

Most Recent Posts

Root Zone Archive

Reply Size Test

Content Navigation

- Services
  - ODVR
  - Porttest
  - TLDmon
  - Reply Size

OARC's Open DNSSEC Validating Resolver

OARC is pleased to offer open DNSSEC-validating resolvers ("ODVR") that anyone can use to experiment with DNSSEC. The IP addresses for ODVR nameservers are:

Instance	IPv4	IPv6
BIND 9	149.20.64.20	2001:4f8:3:2bc:1::64:20
Unbound	149.20.64.21	2001:4f8:3:2bc:1::64:21
~~IANA testbed~~	~~149.20.64.22~~	~~2001:4f8:3:2bc:1::64:22~~

UPDATE: On September 3, 2010 ICANN decommissioned the IANA DNSSEC testbed *(announcement here)*. **Consequently we will no longer offer DNS resolution via this mechanism. We *will* continue to offer the BIND and Unbound open DNSSEC-validating resolvers.**

How To Use ODVR

You might like to manually query the ODVR nameservers with a tool such as *dig*. Be sure to add the *+dnssec* option:

```
$ dig +dnssec iis.se | less
```

The AD bit in the response flags tells you that the reply data has been validated:

```
;; flags: qr rd ra ad; ...
```

Another way to use ODVR is to place the following lines in your Unix

OARC Members

Platinum
ISC

Gold
Afilias
Google
ICANN
Nominet
RIPE NCC
VeriSign

Silver
AFNIC
Cisco
Comcast
DENIC
McAfee
Microsoft
UltraDNS

Bronze
.SE
CIRA
CNNIC
Community DNS
CZ.NIC
Damballa
Detica
DK Hostmaster
eNom

digでの確認 via ODVR

```
$ dig skrd.org ns +dnssec @149.20.64.20

; <<>> DiG 9.7.2-P2 <<>> skrd.org ns +dnssec @149.20.64.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 470
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;skrd.org.              IN    NS

;; ANSWER SECTION:
skrd.org.         3600  IN    NS    currant.skrd.org.
skrd.org.         3600  IN    NS    cherry.skrd.org.
skrd.org.         3600  IN    RRSIG NS 8 2 3600 20101023123033 20100923123033 41178 skrd.org. (略)

;; ADDITIONAL SECTION:
cherry.skrd.org. 3600  IN    A     59.106.173.70
cherry.skrd.org. 3600  IN    AAAA  2002:3b6a:ad46::1
currant.skrd.org.      3600  IN    A     202.212.225.201
cherry.skrd.org. 3600  IN    RRSIG A 8 3 3600 20101023123033 20100923123033 41178 skrd.org. (略)
cherry.skrd.org. 3600  IN    RRSIG AAAA 8 3 3600 20101023123033 20100923123033 41178 skrd.org. (略)
currant.skrd.org.      3600  IN    RRSIG A 8 3 3600 20101023123033 20100923123033 41178 skrd.org. (略)

;; Query time: 1243 msec
;; SERVER: 149.20.64.20#53(149.20.64.20)
;; WHEN: Thu Sep 23 23:05:31 2010
;; MSG SIZE  rcvd: 812
```


©2010 NTTPC Communications, Inc.

VeriSign Labs DNSSEC Debugger

- VeriSign Labs の DNSSECデバッグ用ツール
- http://dnssec-debugger.verisignlabs.com/

©2010 NTTPC Communications, Inc.

VeriSign | Labs

Domain Name: skrd.org Detail: more(+) / less(-) Time: 2010-09-23 14:08:28 UTC, NTP stratum 3

Debugging DNSSEC problems for skrd.org

TA	Locally configured Trust Anchor
.	Found 3 DNSKEY records for . DS=19036/SHA1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset . refers to org for skrd.org Found 2 DS records for org in the referral Found 1 RRSIGs over DS RRset RRSIG=41248 and DNSKEY=41248 verifies the DS RRset
org	Found 4 DNSKEY records for org DS=21366/SHA1 verifies DNSKEY=21366/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=21366 and DNSKEY=21366/SEP verifies the DNSKEY RRset org refers to skrd.org for skrd.org Found 1 DS records for skrd.org in the referral Found 1 RRSIGs over DS RRset RRSIG=37812 and DNSKEY=37812 verifies the DS RRset
skrd.org	Found 2 DNSKEY records for skrd.org DS=17020/SHA256 verifies DNSKEY=17020/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=17020 and DNSKEY=17020/SEP verifies the DNSKEY RRset skrd.org A RR has value 59.106.173.70 Found 1 RRSIGs over A RRset RRSIG=41178 and DNSKEY=41178 verifies the A RRset

Move your mouse over any or symbols for remediation hints.

DNSViz

- A DNS visualization tool
  - ゾーンを視覚化するツール
- 米国エネルギー省サンディア国立研究所
- http://dnsviz.net/

©2010 NTTPC Communications, Inc.

Sandia National Laboratories

DNSViz Home » skrd.org

DNSViz

Go to domain name... Go »

A DNS visualization tool

skrd.org

Last updated: **2010-09-23 10:37:35 UTC** (Update now) *Current time: 2010-09-23 14:30:12 UTC*

DNSSEC | Servers | Analyze

DNSSEC options (show)

Notices

RRset status

Secure (3)

DNSKEY/DS/NSEC status

Secure (7)

Delegation status

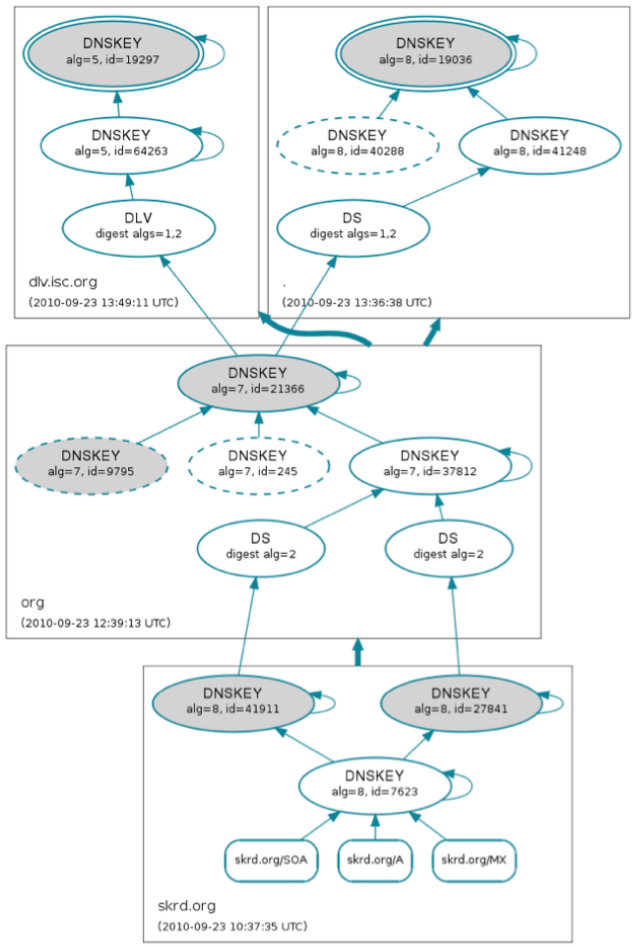
Secure (3)

DNSKEY legend

- Published only
- SEP bit set
- Revoke bit set
- Trust anchor

DNSSEC authentication chain

Download as png

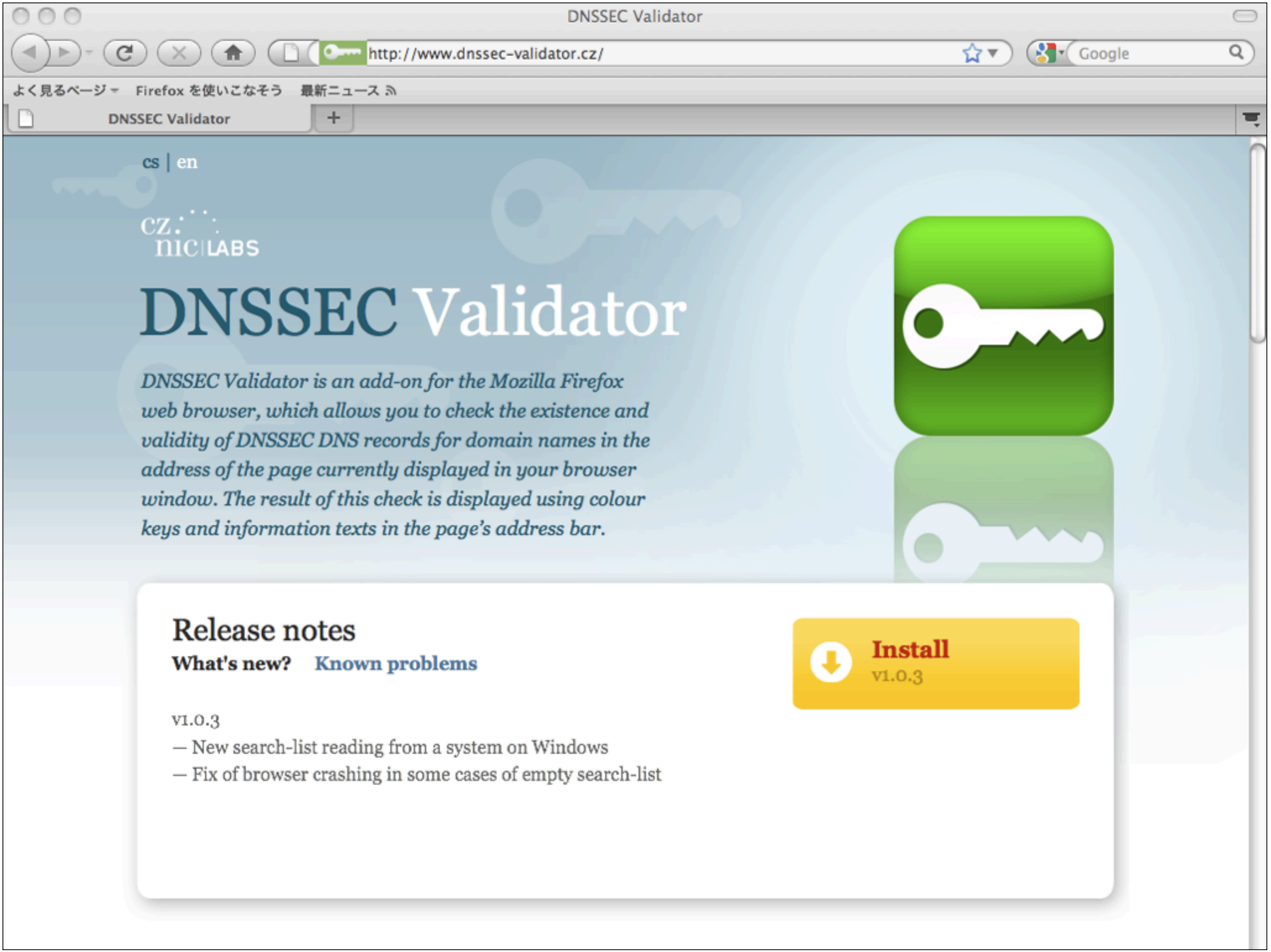


Copyright © 2010 Sandia Corporation | Questions and Comments | Privacy and Security | Sandia Corporate Website

DNSSEC Validator

- CZ (チェコ) NIC LABS 製
- FireFoxのアドオン
  - リゾルバ(DNSSEC検証サーバ)を指定
- 接続先のドメイン名のDNSSEC検証結果を鍵マークで表示
- http://www.dnssec-validator.cz/

©2010 NTTPC Communications, Inc.


DNSSEC Validator
http://www.dnssec-validator.cz/
Google
よく見るページ
Firefox を使いこなそう
最新ニュース
DNSSEC Validator
cs | en
CZ NIC LABS
DNSSEC Validator
DNSSEC Validator is an add-on for the Mozilla Firefox web browser, which allows you to check the existence and validity of DNSSEC DNS records for domain names in the address of the page currently displayed in your browser window. The result of this check is displayed using colour keys and information texts in the page's address bar.
Release notes
What's new?
Known problems
Install
v1.0.3
v1.0.3
— New search-list reading from a system on Windows
— Fix of browser crashing in some cases of empty search-list

.jpの対応

- JPRSの発表より
  - JPゾーンにおけるDNSSEC署名開始の日付を2010年10月17日に、JPドメイン名サービスへのDNSSEC導入の日付を2011年1月16日に決定しました。
  - http://jprs.jp/info/notice/20090709-dnssec.html
- あと2か月です

©2010 NTTPC Communications, Inc.

jpのDNSKEY

```
$ dig jp. dnskey
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.1-P2 <<>> jp. dnskey
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54132
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;jp.                    IN    DNSKEY

;; ANSWER SECTION:
jp.               32967 IN    DNSKEY      256 3 8 AwEAAbYhrQMQH9ItfsO/SFNAFVwpV669OF9+FGtEe5IOTuajY871KONN
qqyojToAiyQSTmhibS7q1zaNNx4cZlQwl/PvF4yVwYU51OYPs5SsMntZ lWTkebDpTbfyVzPkKZ2brrS/+6QOmxB5IpqzdbdLc/
mjH6UWVWOgrG+C BSmD9PoX
jp.               32967 IN    DNSKEY      256 3 8 AwEAAcxWIhw/wv6vwbOKO+umDTP+cPMkoRykho4kLyccg6MB8XkXMThB
Nd1GXEolvzuyd/RAjGJqo2mdzxLyq3T54NTE9iIezmFhM00LWNLFH8rS zhx0PyIid3GJT/
SQnH4wqdaYZ3gVEzGfriWFWP3u2LqntGjdTr9+rdAf 0V+ekrEj
jp.               32967 IN    DNSKEY      256 3 8 AwEAAfR82Pggt5LKS2i52o9erUXPjDEZ71OorqVyhvTbuIlfEuBQ/A9j
xGkI89gIsId2CadVfcBeUzz8RyowQPhnjGW6Zcap7s5fWq7+H6dECtEq h8Jgbe6sPlC27+
+yMHBBYcLtLOTVxRvQyDwds4rnfsVOzHYMkUu1wmOw GPkokqGz
jp.               32967 IN    DNSKEY      257 3 8 AwEAAbPUX+Fy7ONuMs8+HY77DX/qaI2ZCaGUNJRKDxdvk2XiecvXNu8u
pgjg9B9UH6fP6TRxE3NQ6iP3DeHkNSQCFeWa7ItBxY0gQyPZPJATzIc/ lWPcjWAwMOYUI/
Un0KSq93suzUhS5sDjW6O7FWfURLYeAhg4zvDHEksC G0wULldI7qQENO/zKhtz1MpNDHjZrMdSbfPgCseodrfsgOlD+Br5Nz97
mSXg5RbYYhEJ9+yWcUA9YT/sYMNr7JRRzd71UIIIbvo5Th+YM+f34s+O
0JTqwOyvNmehlRElvyTyicvk6db80PLTslWLHSNrUkI06Yo9JyHuitcQ KumIGnA8tO8=

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Nov 10 16:05:32 2010
;; MSG SIZE  rcvd: 740
```


©2010 NTTPC Communications, Inc.

日本での取り組み

- DNSSECジャパン
- 2009/11/24設立
- DNSSECの導入と普及のため
- DNSSECに関わるプレイヤーの集う場
  - 相互扶助
- ISP、IXP、ホスティング、ドメイン事業者、ベンダ、各種団体など31組織
- 活動は2011/3までの予定
- http://dnssec.jp/

©2010 NTTPC Communications, Inc.

カテゴリー

- RFC (3)
- イベント (4)
- プロトコル理解SWG (3)
- 技術情報 (4)

関連情報[ML]

- dns-operations [dns-oarc.net]
- dnsop Discussion [ietf.org]
- dnsops [dnsops.jp]
- The DNSSEC-Deployment Working Group [dnssec-deployment.org]

関連情報[TOOL]

- bind [isc.org]
- DNSCheck [iis.se]
- DNSSEC Validator [nic.cz]
- NSD [nlnetlabs.nl]
- OpenDNSSEC
- Unbound [nlnetlabs.nl]
- Unbound ユーザ会

RFC資料掲載、その3

BY DNSSECJP, ON 8月 31ST, 2010

DNSSECジャパン プロトコル理解SWGにて、各組織で作成いただいた解説資料を 資料 - RFC のページに順次掲載しています。 先週、先々週に引き続き、2つの解説文書を追加しましたので、お知らせします。 RFC443 [...] . . . → Read More: RFC資料掲載、その3

COMMENTS ARE CLOSED　RFC, プロトコル理解SWG, 技術情報

RFC資料掲載、その2

BY DNSSECJP, ON 8月 24TH, 2010

DNSSECジャパン プロトコル理解SWGにて、各組織で作成いただいた解説資料を 資料 - RFC のページに順次掲載しています。 先週に引き続き、4つの解説文書を追加しましたので、お知らせします。 RFC5155 DN [...] . . . → Read More: RFC資料掲載、その2

COMMENTS ARE CLOSED　RFC, プロトコル理解SWG, 技術情報

RFC資料掲載

BY DNSSECJP, ON 8月 18TH, 2010

TWITTER

DNSSEC.JP
dnssec_jp

本日の技術検証WGのレ
ストラ移転検討会は終了
ました。宿題の読み合わ
せ、移転のパターンを検
証、最後に宿題の分担を
いました。13時半から長
時間お疲れさまでした!
#dnssec_jp
10 days ago

本日の技術検証WGは終了
しました。ドメイン事業
移転のさまざまなパター
について議論を行いまし
が、収束せず宿題を残し
引き続き検討を行うこと
なりました。みなさまお
れさまでした! #dnssec_
17 days ago

第6回技術検証WGなう。

twitter
Join the convers

アーカイブ

- 2010年8月

活動内容

- ハンズオンセミナー
- RFC輪講
  - Appendixの関連RFC資料掲載
- 技術検証
  - 主に運用における課題整理
  - ノウハウ蓄積
- 成果を公開
- 参加組織募集中

©2010 NTTPC Communications, Inc.

イベント予定

- Internet Week 2010
  - 2010/11/24(水)～26(金)
    - 11/25(木)はDNS DAY
  - 富士ソフトアキバプラザ
  - http://internetweek.jp/
- SecurityDay 2010
  - 2010/12/22(水) 13:00～
  - http://securityday.jp/

©2010 NTTPC Communications, Inc.

まとめ

- .jpの対応まで、あと2か月
- 運用への落とし込みはこれから
  - TTL等の細かなパラメータ
  - 鍵の危殆化、 ドメイン移転
  - トラブルシューティング手法
- 事業者間の連携が必須

©2010 NTTPC Communications, Inc.

Q&A

- ご清聴ありがとうございました。
- any questions ?

©2010 NTTPC Communications, Inc.

Appendix

- 関連RFC一覧
- Unbound
- NSD

©2010 NTTPC Communications, Inc.

関連RFC一覧

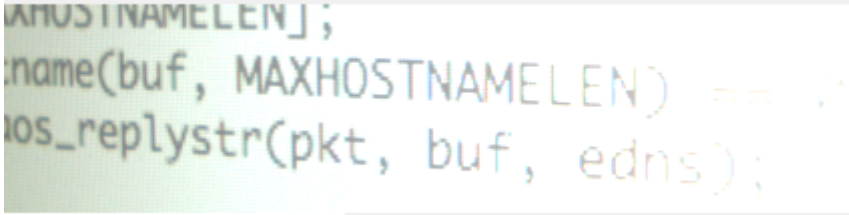
4033	DNS Security Introduction and Requirements.	DNSセキュリティ拡張の紹介とその要件
4034	Resource Records for the DNS Security Extensions.	DNSセキュリティ拡張で使用するリソースレコード
4035	Protocol Modifications for the DNS Security Extensions.	DNSセキュリティ拡張のためのプロトコル修正
5011	Automated Updates of DNS Security (DNSSEC) Trust Anchors.	DNSSECトラストアンカーの自動更新
5155	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.	ハッシュ化された認証による存在否定 (NSEC3)
4641	DNSSEC Operational Practices.	DNSSEC運用上の慣行
i-d	DNSSEC Operational Practices, Version 2.	DNSSEC運用上の慣行 バージョン2
4509	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).	DNSSECのDSリソースレコードにおけるSHA-256の利用
5702	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource.	DNSKEYとRRSIGにおけるSHA-2アルゴリズムの使用について
4431	The DNSSEC Lookaside Validation (DLV) DNS Resource Record.	DNSリソースレコード「DLV」
4986	Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover.	DNSSECトラストアンカーロールオーバーに関する要件
5074	DNSSEC Lookaside Validation (DLV).	DNSSEC Lookaside Validation (DLV).
i-d	DNSSEC Key Timing Considerations	DNSSEC鍵運用タイミングの考察

©2010 NTTPC Communications, Inc.

Unbound

- NLnet Labs他4組織で開発
  - BINDの代替、DNSサーバの多様性
  - 現在はNLnet Labsにて保守
- キャッシュサーバ
  - 権威サーバの機能もある
- http://www.unbound.net/
- http://unbound.jp/

©2010 NTTPC Communications, Inc.



Unbound

NLnet Labs

VeriSign

nominet

kirei

About Unbound

Unbound is a validating, recursive, and caching DNS resolver.

The C implementation of Unbound is developed and maintained by **NLnet Labs**. It is based on ideas and algorithms taken from a java prototype developed by **Verisign** labs, **Nominet**, **Kirei** and **ep.net**.

Unbound is designed as a set of modular components, so that also DNSSEC (secure DNS) validation and stub-resolvers (that do not run as a server, but are linked into an application) are easily possible.

The source code is under a **BSD License**.

Download

The latest source code tarball is available for **download**.

Bugs

Report bugs using bugzilla **here**.

Mailing List

You can subscribe to the unbound users mailing list **here**.

Browse the **archives** of unbound-users.

Maintenance and Support

Unbound is being maintained by **NLnet Labs**, a not for profit, public benefit foundation. Problems can be reported through the **bugzilla webinterface**. In the case we stop supporting the product we will announce such two years in advance.

Commercial support for Unbound is available from **several organizations**.

News

Release 1.4.6
Tue Aug 3 13:37:50 CEST 2010

Version 1.4.6 of unbound has been released.

more

Flavors of Unbound
Wed Jul 28 16:57:32 CEST 2010

Men and Mice have published an article on how to select between different flavors of Unbound compilation. This article will explain the technical di fferences of the possible flavors of Unbound and will give proposals under which type of DNS workload a specific flavor will perform best. The article will be kept upd ated when new versions of unbound are released.

more

Release 1.4.5
Tue Jun 15 09:15:50 CEST 2010

Version 1.4.5 of unbound has been released.

more

Release 1.4.4
Thu Apr 22 10:37:11 CEST 2010

Version 1.4.4 of unbound has been released.

more

日本Unboundユーザ会

Japan Unbound Users Group.

検索 Go

Home | Unboundとは | 日本語マニュアル | ガイド | ユーザ会概要 | ユーザーフォーラム

UnboundはDNSリゾルバ、キャッシュ、DNSSEC検証機能を持つDNSキャッシュサーバーです。次のような特徴を持ちます。

- DNSキャッシュ汚染に対する耐性が強い
- 設定が容易である（デフォルトで安全な設定ができる）
- 高性能
- IPv4、IPv6デュアルスタック
- DNSSEC対応

UnboundはBSDライセンスの元で公開されています。

Unboundの機能の概要については、DNSOPS.JP BoF発表資料「**Unboundの紹介(PDF)**」をご覧ください。

3月 10 2010

DNSSEC関連ドキュメントの翻訳を公開

DNSSEC関連ドキュメントの日本語翻訳を公開しました。また、古くなったインス

Entries RSS | Comments RSS

ページ

- Unboundとは
- 日本語マニュアル
  - unbound(8)
  - unbound-checkconf(8)
  - unbound-control(8)
  - unbound.conf(5)
  - unbound.conf(5) - 1.0.x
  - unbound-host(1)
- ガイド
  - DNSSECを有効にするには
  - IANA ITARを利用するには
  - インストール方法
- ユーザ会概要

ドキュメント

- ユーザーフォーラム

リンク

- Comparison of DNS server software (wikipedia)
- JPRS DNS関連技術情報
- NLnet Labs
- Unbound公式サイト
- 日本DNSオペレーターズグルー

Unbound: インストール

WebARENA

```
# yum -y install gcc openssl-devel
$ wget http://www.unbound.net/downloads/
unbound-1.4.6.tar.gz
$ tar zxf unbound-1.4.6.tar.gz
$ cd unbound-1.4.6/
$ ./configure --prefix=/usr/local/
$ make
# make install
# /sbin/ldconfig
# groupadd -r unbound
# useradd -r -g unbound -d /var/unbound -s /
sbin/nologin -c "unbound name daemon" unbound
```


©2010 NTTPC Communications, Inc.

Unbound: unbound-control

- BIND の rndc 的ツール
  - ネットワーク経由でUnboundサーバを
    コントロール可能
- 設定
  - /usr/local/sbin/unbound-control-setup
    実行で設定ファイル自動生成

©2010 NTTPC Communications, Inc.

Unbound: 設定

/usr/local/etc/unbound/unbound.conf に下記設定

```
server:
        interface: 192.0.2.5
        access-control: 192.0.2.5 allow

        auto-trust-anchor-file: "anchors/root"

remote-control:
        control-enable: yes
```

/usr/local/etc/unbound/anchors/root

```
. IN DS 19036 8 2 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32
F24E8FB5  (紙面の都合で開業されていますが一行で)
```


©2010 NTTPC Communications, Inc.

Unbound: 起動

WebARENA

```
# /usr/local/sbin/unbound-control-setup
# unbound-control start
# ps axww|grep unbound
 9752 ?        Ss     0:00 unbound -c /usr/
local/etc/unbound/unbound.conf
# tail /var/log/messages
Sep 22 13:15:46 baguette unbound: [9752:0]
notice: init module 0: validator
Sep 22 13:15:46 baguette unbound: [9752:0]
notice: init module 1: iterator
Sep 22 13:15:46 baguette unbound: [9752:0]
info: start of service (unbound 1.4.6).
```


©2010 NTTPC Communications, Inc.

NSD

- オランダのNLnet Labsで開発
- 権威サーバ機能に特化
- ゾーンファイルの書式はBIND同様
- 鍵生成ツール、署名ツールもBINDのものを利用可能
- http://nlnetlabs.nl/projects/nsd/

©2010 NTTPC Communications, Inc.

NSD: Name Server Daemon

NSD is an authoritative only, high performance, simple and open source name server. The latest current stable release is NSD 3.2.6. Download the latest version.

NSD is thoroughly tested, there is a regression tests report available: differences.pdf

For NSD 3.0, a memory usage estimation tool is provided.

NLnet Labs has a long term commitment for supporting **NSD**. There will be an advanced notice when our commitment ends. The latest **NSD** release will supported for at least two years after this notice. More details on the support program are found here.

Mailing lists

If you are using NSD, you might want to consider subscribing to nsd-users by going to this page.

Browse the archives of nsd-users.

SVN repository

The repository of NSD is available at /svn/nsd/.

The NSD 3.x.x development tree is located in `trunk/`.

Links

Releases

NSD 3.2.6

Aug 2, 2010

Features

- Expand command line option '-a' and config option 'ip-address:' with port number.

Bugfixes

- Bugfix #314: correctly print NSEC next field, escape spaces and fix label overflows.

Operational notes

NSD: インストール

```
# yum -y install gcc openssl-devel
$ wget http://nlnetlabs.nl/downloads/nsd/
nsd-3.2.6.tar.gz
$ tar zxf nsd-3.2.6.tar.gz
$ cd nsd-3.2.6/
$ ./configure --prefix=/usr/local/
$ make
# make install
```


©2010 NTTPC Communications, Inc.

NSD: 設定

/usr/local/etc/nsd/nsd.conf に下記設定

```
server:
        ip-address: 192.0.2.5
        username: named

zone:
        name: example.jp
        zonefile: example.jp.signed
        provide-xfr: 192.0.2.6 NOKEY
```


©2010 NTTPC Communications, Inc.