Panasonic
ideas for life

キャッシュDNSのDNSSEC対応

2012年11月21日

三洋ITソリューションズ株式会社
SANNET BU 技術運用チーム
其田　学

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSECに対応したキャッシュDNSとは

- 検証の仕組み

構築方法

- 構築前の確認事項
- ROOTゾーンのトラストアンカー
- キャッシュDNSサーバの設定

運用

- 監視・ログ項目
- トラブルシューティング

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSECに対応したキャッシュDNSとは

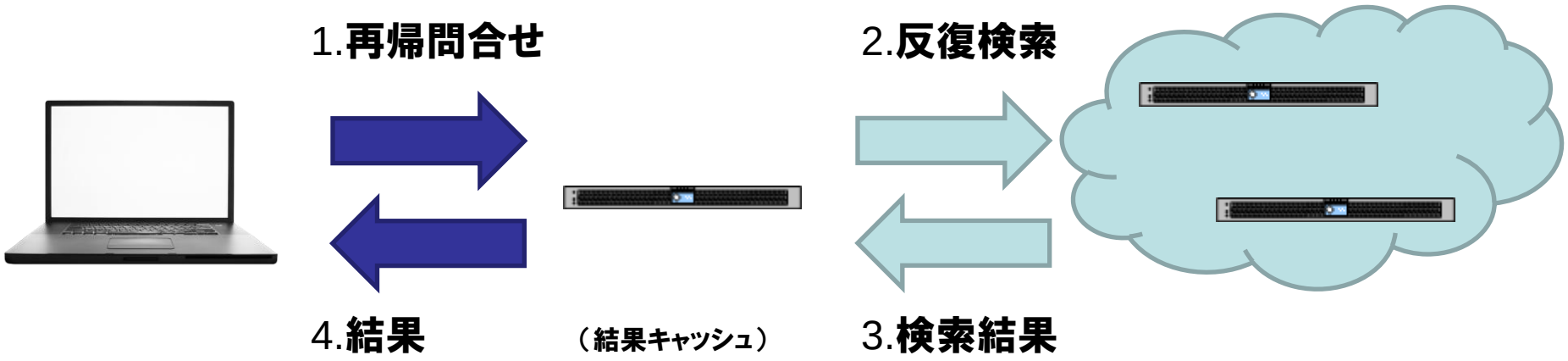
Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

通常のキャッシュDNSの機能に加え、
DNSSECの署名検証を行い、
RRsetの正当性を検証するキャッシュDNSサーバ。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSECに対応したキャッシュDNSとは

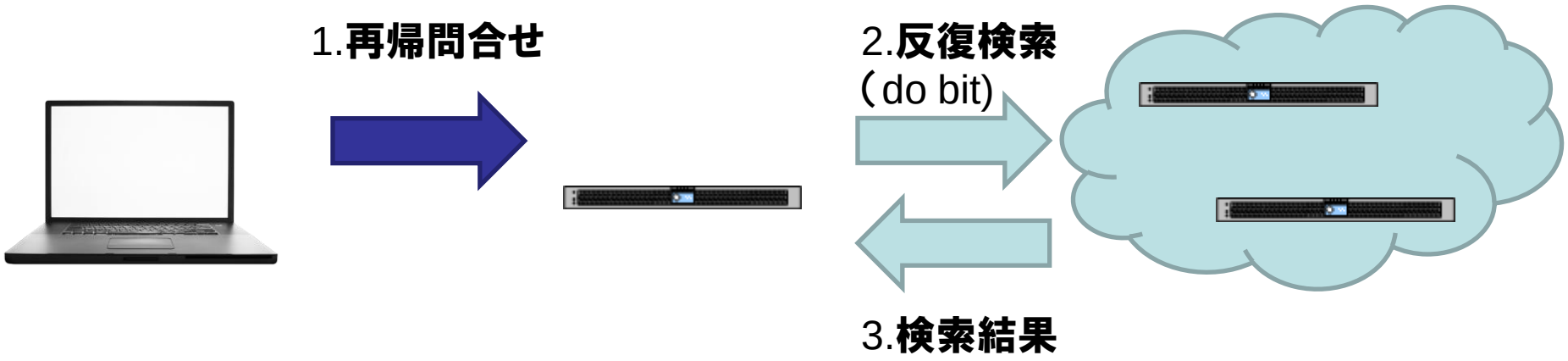
普通のキャッシュDNSサーバの動き



Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSECに対応したキャッシュDNSとは

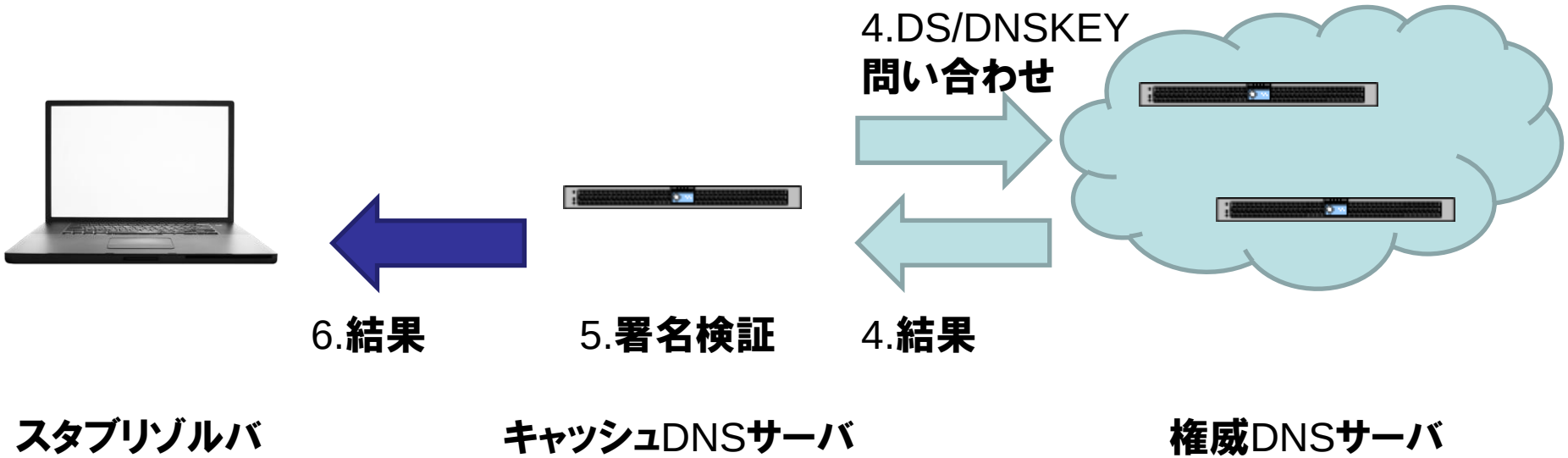
署名検証するキャッシュDNSサーバの動き



Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSECに対応したキャッシュDNSとは

署名検証するキャッシュDNSサーバの動き



Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

検証例:「jp. SOA」の検証

jp. SOAをdo bit付で問い合わせる

```
$ dig +dnssec +multiline +norec +noall ¥
+answer @a.dns.jp jp. SOA

jp.                 86400 IN SOA z.dns.jp. root.dns.jp. (
                          1352078102 ; serial
                          3600       ; refresh (1 hour)
                          900        ; retry (15 minutes)
                          1814400    ; expire (3 weeks)
                          900        ; minimum (15 minutes)
                          )
jp.                 86400 IN RRSIG SOA 8 1 86400 (
20121217174502 20121117174502 25848 jp.
OjWu/81==省略== )
```

署名者:jp.
鍵のID:25848
署名有効期間:2012年11月17日17時45分2秒(UTC)から
2012年12月17日17時45分2秒(UTC)まで

検証レコード
jp. SOA

RRSIG: jp. SOA
署名者: jp.
鍵のID:25848

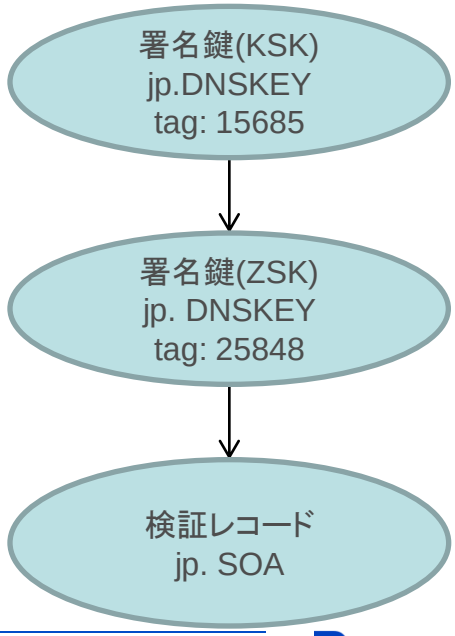
Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

検証例:「jp. SOA」の検証

jp. DNSKEYを問い合わせる

```
$ dig +dnssec +multiline +norec +noall ¥
+answer @a.dns.jp jp. dnskey
jp.                 86400 IN DNSKEY 256 3 8 (
AwEAAdY==省略==
) ; ZSK; alg = RSASHA256; key id = 25848

jp.                 86400 IN DNSKEY 256 3 8 (
AwEAAeW ==省略==
) ; ZSK; alg = RSASHA256; key id = 6831

jp.                 86400 IN DNSKEY 257 3 8 (
AwEAAdw ==省略==
) ; KSK; alg = RSASHA256; key id = 15685

jp.                 86400 IN RRSIG DNSKEY 8 1 86400 (
20130103184500 20121103184500 15685 jp.
Cc2iCOrJ==省略==
)
```

署名者:jp.
鍵のID:15685
署名有効期間:2012年11月3日18時45分0秒(UTC)から
2013年1月3日18時45分0秒(UTC)まで



RRSIG: jp. DNSKEY
署名者:jp.
鍵のID:15685

RRSIG: jp. SOA
署名者: jp.
鍵のID:25848

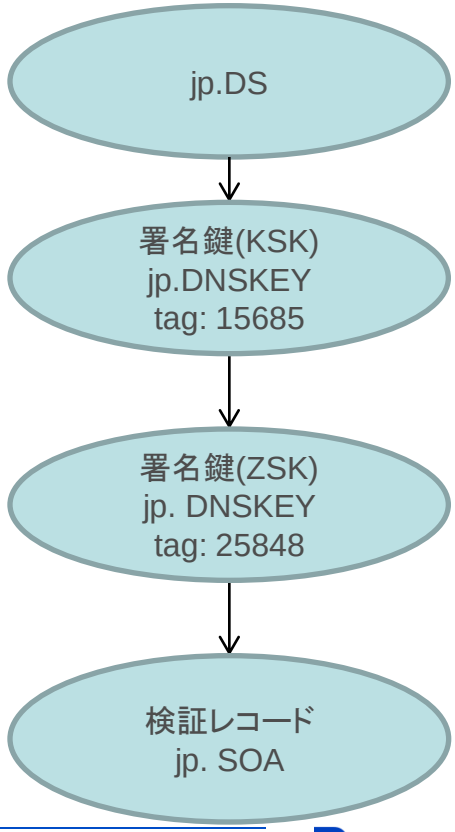
Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

検証例:「jp. SOA」の検証

jpのDSを取得する

```
$ dig +dnssec +multiline +norec +noall ¥
+answer @m.root-servers.net jp. DS
jp.                 86400 IN DS 15685 8 1 (

BB1FEA6AA10DBB52A7DF091DAE3AF22C28F65B4B )

jp.                 86400 IN DS 15685 8 2 (

170E77FF24DD8D8A1FDE99AEB4C93A85434C9376A3C1
                        98FBBFE12D0F807A14E9 )

jp.                 86400 IN RRSIG DS 8 1 86400 (
20121126000000 20121118230000 24220 .
7kz9NVJJhlI== 省略 ==)
```

署名者: . (root)
鍵のID: 24220
署名有効期間: 2012年11月18日23時0分0秒(UTC)から
2012年11月26日0時0分0秒(UTC)まで



RRSIG: jp. DS
署名者: .
鍵のID:24220

RRSIG: jp. DNSKEY
署名者:jp.
鍵のID:15685

RRSIG: jp. SOA
署名者: jp.
鍵のID:25848

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Panasonic ideas for life

検証例:「jp. SOA」の検証

. (root)のDNSKEYを取得する

```
$ dig +dnssec +multiline +norec +noall ¥
+answer @m.root-servers.net . DNSKEY
.                   172800 IN DNSKEY 257 3 8 (
AwEAAagAI0==省略==
) ; KSK; alg = RSASHA256; key id = 19036

.                   172800 IN DNSKEY 256 3 8 (
AwEAAfIcor==省略==
) ; ZSK; alg = RSASHA256; key id = 24220

.                   172800 IN RRSIG DNSKEY 8 0 172800 (
20121114235959 20121031000000 19036 .
prVRySVQ==省略==)
```

署名者: . (root)
鍵のID: 19036
署名有効期間:2012年10月31日0時0分0秒(UTC)から
2012年11月14日23時59分59秒(UTC)まで

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

検証例:「jp. SOA」の検証

検証

1. **トラストアンカーを使って、ルート**KSK
2. **ルート**KSK**を使ってルート**DNSKEY
3. **ルート**ZSK**を使って**JP DS
4. JP DS**を使って**JP KSK
5. JP KSK**を使って、**JP DNSKEY
6. JP ZSK**を使って、**JP SOA

という感じにトラストアンカーから検証していきます。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

検証結果による応答

DSが登録されていない

署名されていない(Indeterminate)

スタブリゾルバにはad無しで、RRsetを返します。

署名されている(Insecure)

スタブリゾルバにはad無しでRRESetを返します。

DSが登録されている

検証に成功した場合(Secure)

スタブリゾルバにはad bit付でRRsetを返します。

検証に失敗した場合(Bogus)

スタブリゾルバにはSERVFAILを返します。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

構築方法

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Panasonic ideas for life

今回のシナリオは、署名検証に対応していない、普通のキャッシュDNSサーバが構築されている環境に、署名検証対応の設定を入れることを想定しています。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

構築方法

構築前の確認事項

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

最重要

1. サーバの時刻・タイムゾーンを確認する。
   NTP Clientで自動補正できる場合は
   自動補正の設定を入れるのが望ましい。

理由

DNSSECの署名には有効期間があります。
キャッシュDNSサーバの時刻が署名の有効期間外の場合、検証に失敗します。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

最重要

サーバの時刻取得

```
$ date
Tue Nov  6 16:15:36 JST 2012
$ date -u
Tue Nov  6 07:14:46 UTC 2012
```

基準時刻の取得

- 117(時報)
- http://jjy.nict.go.jp/ NICTの日本標準時表示
- ntp (ex. ntp.nict.jp)

サーバ時刻と、基準時刻が1分以内であることを確認

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

2. DNSサーバソフトウェアのバージョンを確認する。
   Bind9の場合、9.7系以上の最新バージョン
   Unboundの場合は1.4系の最新バージョン

理由

1. 脆弱性の問題
2. 古いバージョンだと、NSEC3,RSASHA256に対応していないバージョンがあるため。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

3. 通信路がEDNS0/TCPに対応し、
   IPフラグメントを処理できるかを確認する

理由

1. キャッシュDNSサーバが対応していても、ネットワーク機器が対応していない可能性がある
2. FW・LBとかパケットの中身見る機械は特に注意

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNS Reply Size Test Serverを利用する確認方法

```
$ dig +short rs.dns-oarc.net txt

rst.x4091.rs.dns-oarc.net.
rst.x4049.x4091.rs.dns-oarc.net.
rst.x4055.x4049.x4091.rs.dns-oarc.net.
"2405:0:21:927::53:23 sent EDNS buffer size 4096"
"2405:0:21:927::53:23 DNS reply size limit is at least 4091"
"Tested at 2012-10-24 02:55:07 UTC"
```

DNS reply sizeが4000超えていればOK

DNS Reply Size Test Server
https://www.dns-oarc.net/oarc/services/replysizetest

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

構築方法

ROOTゾーンのトラストアンカー

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

rootのゾーントラストアンカーとは？

ルート（．）のDNSKEY（KSK）を信頼する為の基点
通常はルートのDNSKEYのKSK（またはDS）を登録し、
名前解決したKSKと比較して等しければ、
このKSKを信頼できる鍵とします。

ルートのトラストアンカーを登録すれば、ルートから信頼の連鎖が繋がっているドメインは全て検証可能になります。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

1. DNSソフトウェアに付属しているものを使う

2. ROOTサーバからDNSKEY取得する

```
$ dig +norec +multi @a.root-servers.net . DNSKEY
```

検証方法は

IANA Root Zone Management

https://www.iana.org/domains/root

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

rootのKSKは5年ごとにロールオーバー(鍵の交換)が発生します。
その為、5年毎にトラストアンカーの更新が必要です。

=>大変なのでRFC5011により、トラストアンカーの自動更新が規定されてます。

実際の設定に関しては、自動更新を使用する設定を説明します。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

構築方法

キャッシュDNSサーバの設定

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Panasonic ideas for life

パターン1　トラストアンカーを設定する場合

named.conf

```
managed-keys {
"." initial-key 257 3 8
        "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
        FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
        bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
        X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
        W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYI7OyQdXfZ57relS
        Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
        QxA+Uk1ihz0=";
};
```

ルート以外のゾーンのトラストアンカーを設定したい時にも使用します。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

パターン2　BINDに付属する、トラストアンカーを使用する場合

named.conf

```
options {
        dnssec-validation auto;
        以下略

};
```

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Step1. トラストアンカーファイルの作成

◆unbound-anchorを使用する場合

```
$ unbound-anchor –a “トラストアンカーファイルパス”
```

◆unbound-anchorを使用しない場合は下記のようなルートゾーンのKSKのRRSetを1行で記載したファイルを作成する。

トラストアンカーファイル

```
.       172800  IN      DNSKEY  257 3 8 AwEAAagAIKl==省略=
```

Step2. トラストアンカーファイルの指定

◆unbound.confのauto-trust-anchor-fileにトラストアンカーファイルを設定する

unbound.conf

```
server:
        auto-trust-anchor-file: “トラストアンカーファイルパス"
```

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

確認方法

```
$ dig @キャッシュDNSサーバIP +dnssec www.iana.org
; <<>> DiG 9.9.1-P3 <<>> +dnssec www.iana.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24834
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.iana.org.                  IN      A
```

```
$ drill -D www.iana.org @キャッシュDNSサーバIP  SOA IN
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 56876
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 0
;; QUESTION SECTION:
;; www.iana.org.        IN      SOA
```

ad bitが立っていれば検証成功

http://test.dnssec-or-not.org/を見に行こう

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

運用

監視・ログ項目

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

監視項目

統計関係

監視項目	BIND	Unbound
署名検証失敗数	DNSSEC validation failed	num.answer.bogus
SERVFAIL数	queries resulted in SERVFAIL	num.answer.rcode.SERVFAIL

※Unboundはextended-statistics: yesが必要

これらの値が急増している場合は、何らかのトラブルが考えられる。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

ログ項目

ログ関係

BIND　DNSSEC関係のログを出力

```
logging {
        category dnssec { dnssec_log; };
        channel dnssec_log { file ….. };
};
```

Unbound　検証失敗時にログを出力

```
Server:
        val-log-level: 1
```

ログを出すことで、どのドメインの検証に失敗しているのかわかるので、切り分けが楽になる。

**複数台構成の場合は、全部ログを有効にするとパフォーマンスの問題が生じるので、
何台かログを有効にするだけでも、十分傾向はつかめる。**

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

運用

トラブルシューティング

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

運用中起こりうるDNSSEC対応のDNSキャッシュサーバ固有の問題

問題

検証エラー(Bogus)時はスタブリゾルバからの応答にSERVFAILを返します。
よって、権威DNSサーバ側で署名更新、鍵更新に失敗すると、
DNSSEC対応のキャッシュサーバのみ名前解決に失敗します。

インパクト

◆DNSSECに対応しているドメインは少ないのは事実
◆しかしルートやTLDの普及率はかなり高いため、ここで問題が発生すると、
多くのドメインが影響を受ける。
- ルートに問題が生じると、完全に名前解決ができなくなります。
- TLDに問題が生じると、そのTLDのドメインは名前解決できなくなります。
- NSが外部名設定の場合は、影響を受けることもあります。

ルート、TLD、大規模サイト等の影響が大きいゾーンがFailした場合に備えて、
切り分け方法と対応方法を考えることが大切です。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

あるドメインの名前解決ができなくなった理由がDNSSEC検証かどうか調べたい場合

```
$ dig @[キャッシュサーバのIP] fail.sannet.jp SOA
; <<>> DiG 9.9.1-P3 <<>> fail.sannet.jp SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 59329
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fail.sannet.jp.                IN      SOA
```

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

cdビット（check disable）をつけて問い合わせてみる

*$ dig +cd @[**キャッシュサーバの**IP] fail.sannet.jp SOA*

```
; <<>> DiG 9.9.1-P3 <<>> +cd @202.216.0.53 fail.sannet.jp SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17619
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fail.sannet.jp.                 IN      SOA

;; ANSWER SECTION:
fail.sannet.jp.         3570    IN      SOA     dns.sannet.ne.jp. postmaster.sannet.jp.
2012110501 10800 1800 604800 3600
```

応答が返ってくる場合は、DNSSECの検証に失敗しています。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

drillを使っての調査

$ drill -T -D -Q -k ~/.root.key fail.sannet.jp SOA
;; Number of trusted keys: 1
;; Domain: .
[T] . 172800 IN DNSKEY 256 3 8 ;{id = 24220 (zsk), size = 1024b}
. 172800 IN DNSKEY 257 3 8 ;{id = 19036 (ksk), size = 2048b}
[T] jp. 86400 IN DS 15685 8 2 170e77ff24dd8d8a1fde99aeb4c93a85434c9376a3c198fbbfe12d0f807a14e9
jp. 86400 IN DS 15685 8 1 bb1fea6aa10dbb52a7df091dae3af22c28f65b4b
;; Domain: jp.
[T] jp. 86400 IN DNSKEY 256 3 8 ;{id = 6831 (zsk), size = 1024b}
jp. 86400 IN DNSKEY 256 3 8 ;{id = 25848 (zsk), size = 1024b}
jp. 86400 IN DNSKEY 257 3 8 ;{id = 15685 (ksk), size = 2048b}
[T] sannet.jp. 86400 IN DS 64024 8 2 0cefe2e6dde3fdd2348aefab2e711f50018f456fb9074dd5e0b813a495604700
;; Domain: sannet.jp.
[T] sannet.jp. 3600 IN DNSKEY 256 3 8 ;{id = 17061 (zsk), size = 1024b}
sannet.jp. 3600 IN DNSKEY 257 3 8 ;{id = 64024 (ksk), size = 2048b}
sannet.jp. 3600 IN DNSKEY 256 3 8 ;{id = 33444 (zsk), size = 1024b}
sannet.jp. 3600 IN DNSKEY 257 3 8 ;{id = 31819 (ksk), size = 2048b}
[T] fail.sannet.jp. 3600 IN DS 42292 8 2 0be8aa52b8329023c644bedd2be2b84a559766631ad5016e1f717467aec3500d
fail.sannet.jp. 3600 IN DS 42292 8 1 36e10f413f6b55c317545083cc2dd94ed7ef7cf4
;; Domain: fail.sannet.jp.
[B] fail.sannet.jp. 3600 IN DNSKEY 257 3 8 ;{id = 42292 (ksk), size = 2048b}
fail.sannet.jp. 3600 IN DNSKEY 256 3 8 ;{id = 14196 (zsk), size = 1024b}
[B] fail.sannet.jp. 3600 IN SOA dns.sannet.ne.jp. postmaster.sannet.jp. 2012110501 10800 1800 604800 3600
;; Error: No keys with the keytag and algorithm from the RRSIG found
;;[S] self sig OK; [B] bogus; [T] trusted

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

□DNSの設定チェック

http://dnscheck.jp/

DNSのチェックも行ってくれる

□DNSViz

http://dnsviz.net/

信頼の連鎖を視覚的に見たい時に有効

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

対応方法

検証を一時的に止める

ルートやTLD等の影響が大きいゾーンがFailした場合で、キャッシュDNSサーバへの攻撃ではなく、権威DNSサーバ側の問題と確認できた場合、検証を一時停止する。

BINDの場合

rndc validation disableで停止できます。(enableで再開)

unboundの場合、特定のドメインのみ、検証を停止することができます。

domain-insecure: "example.com"

相手が復旧させるのを待つ

基本的にはこちらが多いです。
場合によってはキャッシュクリアして、復旧を早めることもできます。

基本的に、相手側の事故なので、対応することは難しいです。
どのような対応をするかは運用者のポリシーになると思います。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

DNSSEC対応のキャッシュサーバとは

- **DNSSECの署名検証を行い、正当性を検証するキャッシュDNSサーバ**

構築するには

- **検証に必要なトラストアンカーを設定する**

運用

- **切り分け方法をマスターしておく**
- **ルートやTLD等の影響が大きいゾーンが失敗した場合の対応策をあらかじめ考えておく**

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Panasonic

ideas for life

参考情報

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考情報：お勧めツールの紹介

- **CLI系**
  - dig
    - ISC BINDに付属
    - ここにきている人であれば普通に使ってる筈
  - drill
    - nlnetlabs ldnsに付属
    - -T -D オプションが非常に強力
- WEB系
  - DNSの設定チェック（JPRS)
    - http://dnscheck.jp/
    - DNSSECのチェックだけではなく、DNSのチェックも行われます。
  - DNSSEC Analyzer
    - http://dnssec-debugger.verisignlabs.com/
  - DNSViz
    - http://dnsviz.net/
    - 信頼の連鎖を視覚的に見たい時に有効

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考情報：お勧めツールの紹介

- **ライブラリ系**
  - ldns
    - nlnet Labs**が作成しているライブラリ**
    - Unbound,NSD**で使用されている。**
  - Net::DNS::SEC
    - CPAN**のライブラリ**
  - Dnsruby
    - Ruby**の**DNS**ライブラリ**
    - **弊社の**DNS**テストプログラムで使用中してます。**

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

Panasonic ideas for life

参考情報：お勧めする資料

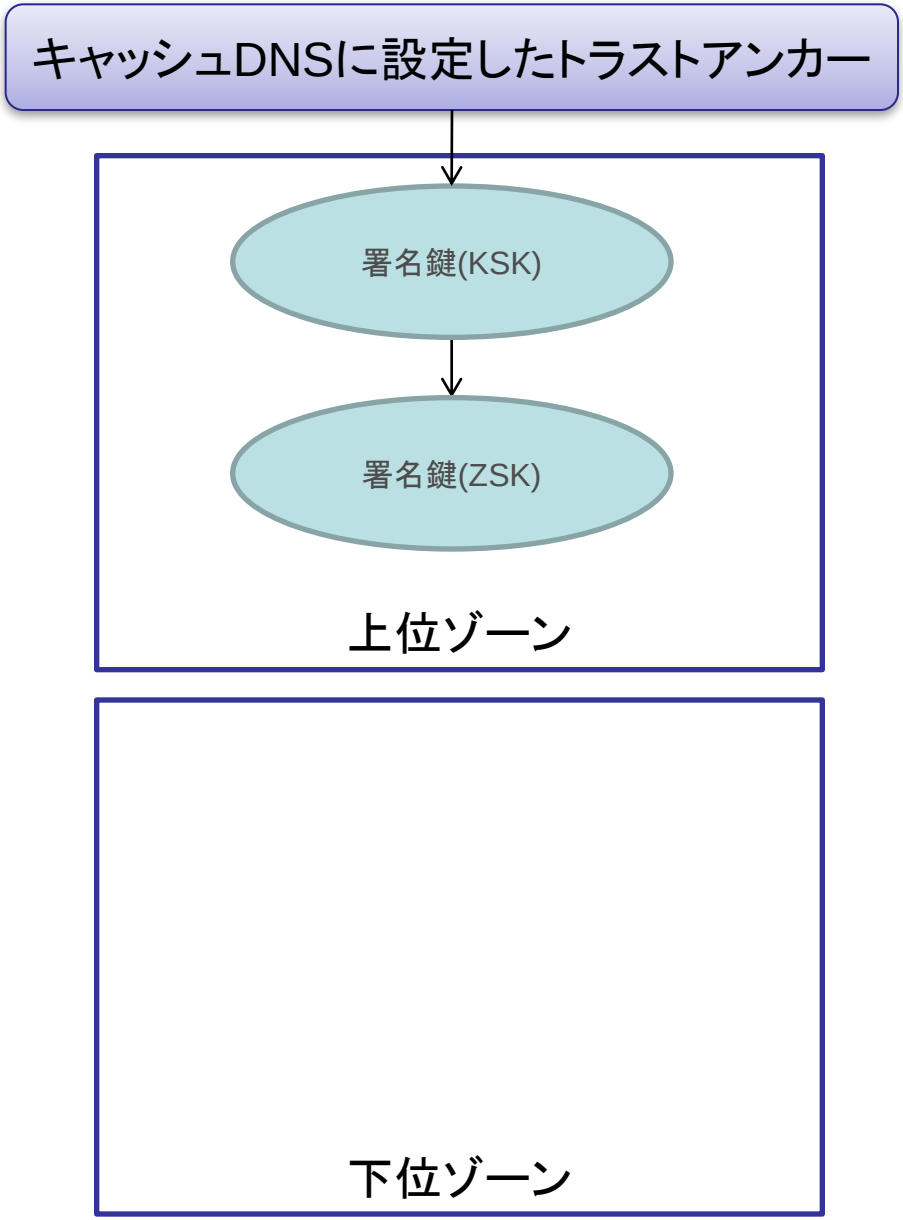
- DNSSECジャパン
  - DNSSEC Readyロゴ チェックリスト（カテゴリ：キャッシュDNSサーバ）
  - DNSSECを利用するリゾルバーのためのトラストアンカーの設定方法について 第2版
  - キャッシュDNSサーバDNSSEC導入ガイドライン
  - DNSサーバDNSSEC導入Load Balancer機能チェックリスト

- JPRS
  - 実践DNS　[ISBN 978-4-04-870073-3]
  - DNSSECチュートリアル http://jprs.jp/related-info/guide/#a01
  - トピックス＆コラム No18「運用者から見たDNSSECと従来のDNSの違い」

- 各サーバソフトウェア関係
  - Unbound: Howto enable DNSSEC（日本語訳が日本Unboundユーザ会に有り）

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考資料：応答例 Indeterminate



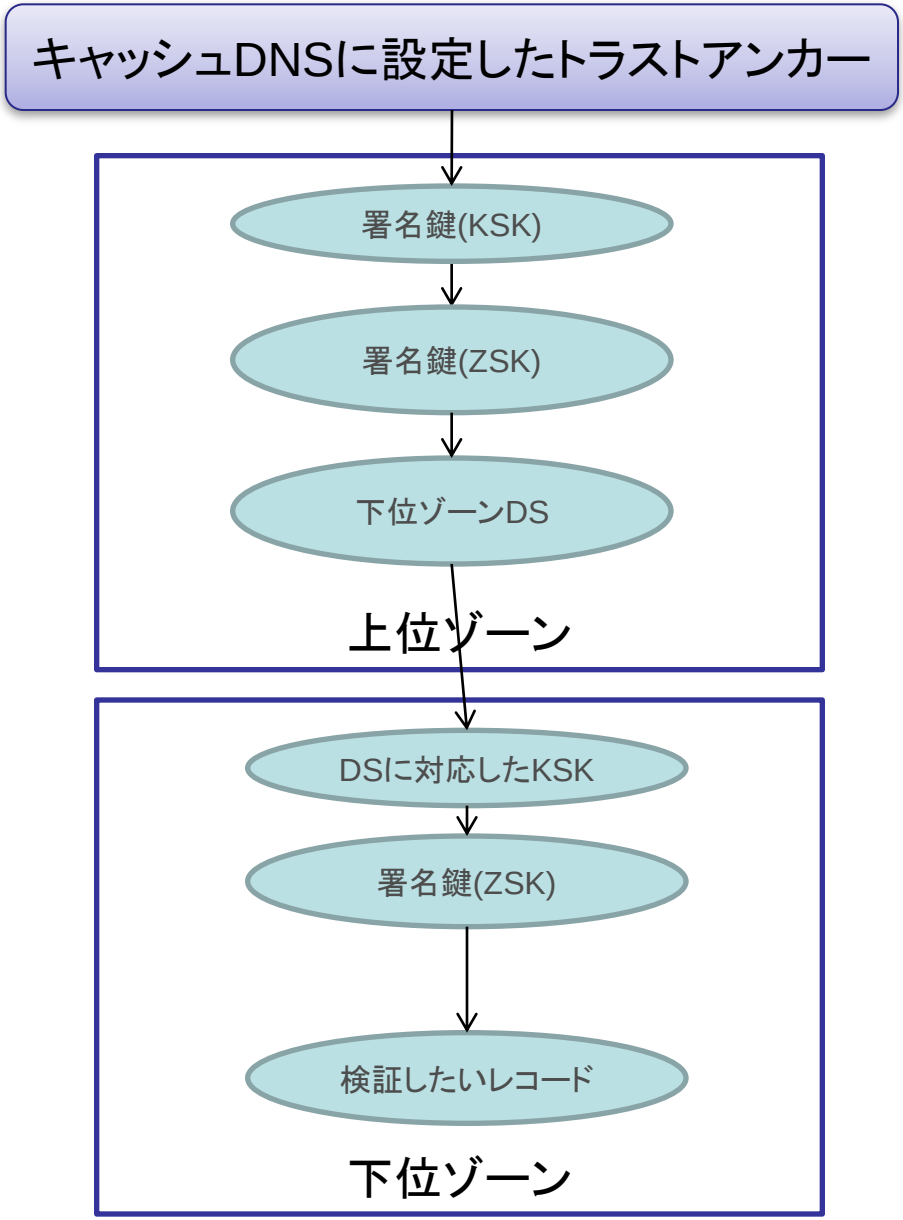
上位ゾーンに下位ゾーンのDSの登録なし

下位ゾーンにDNSKEY、RRSIG等なし

DNSSECに対応していないゾーン
普通のゾーンはこの状態

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考資料:応答例 Secure



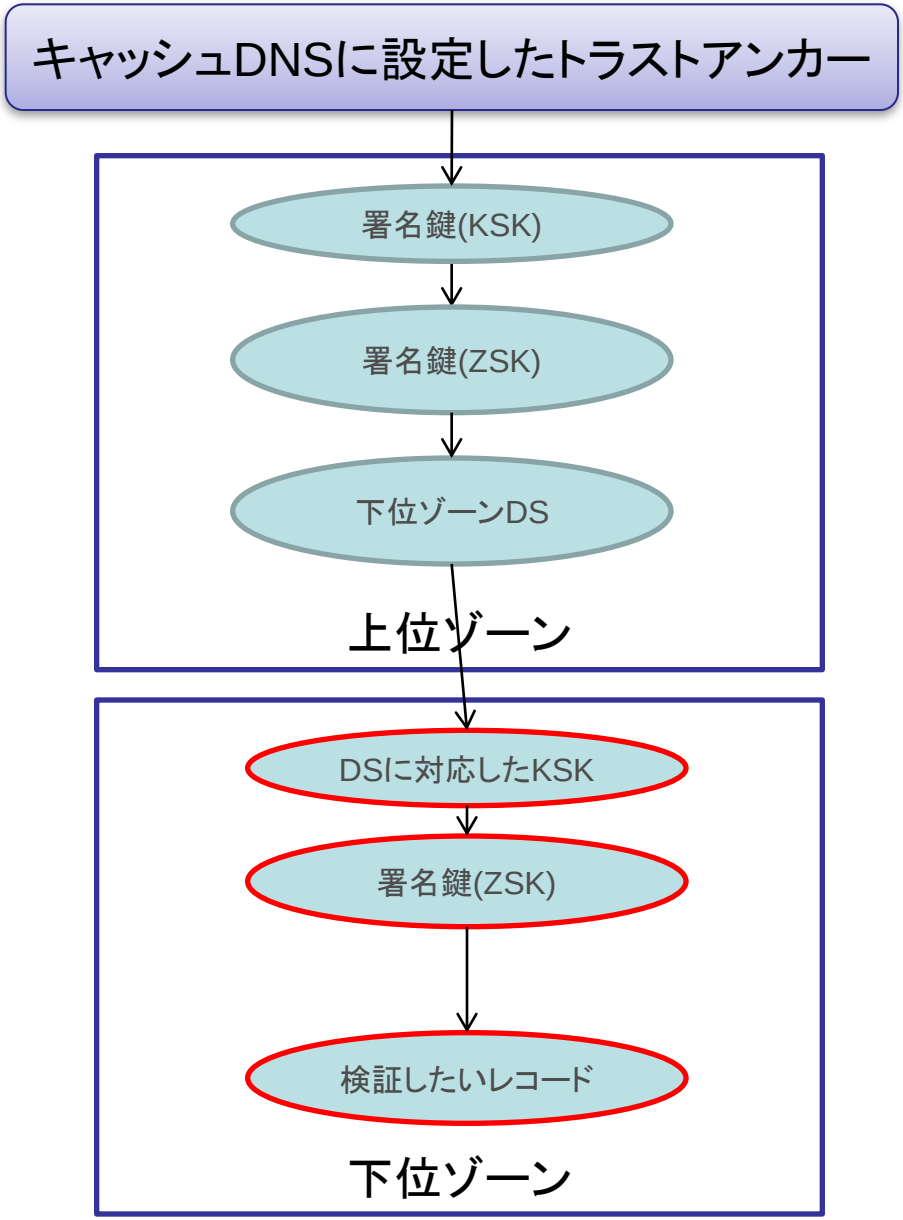
上位ゾーンに下位ゾーンのDSの登録あり

下位ゾーンにDNSKEY、RRSIGあり。
検証に成功

DNSSEC**にきちんと対応しているゾーン**

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考資料:応答例 Bogus



上位ゾーンに下位ゾーンのDSの登録あり

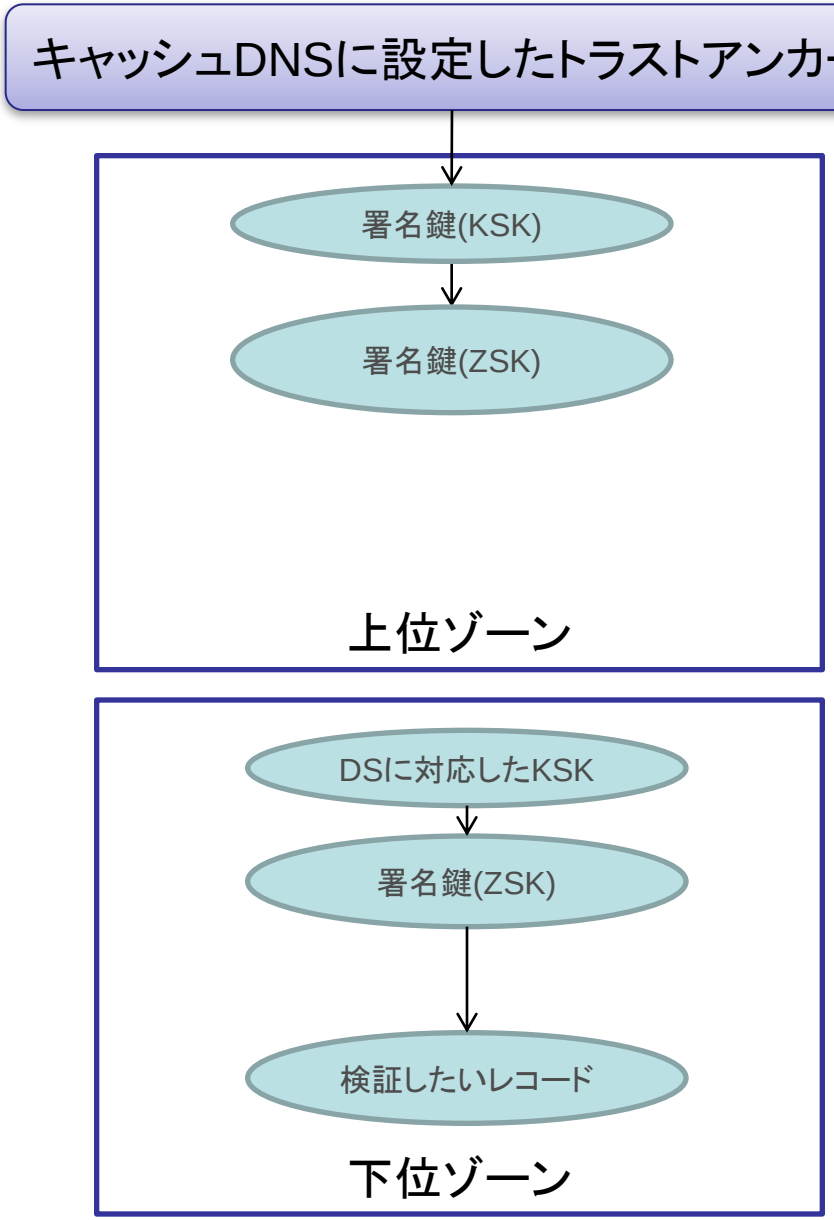
下記のいずれかの場合検証失敗

1. **上位ゾーンに登録のあるDSに対応するKSKがない場合**
1. DNSKEY**または検証レコードに対応する**
   RRSIG**がない**
   RRSIG**が有効期間外**
   RRSIG**に対応する鍵がない**
   RRSIG**と対応する鍵の署名検証に失敗**

DNSSEC**に対応しているが、署名、鍵が間違っている状態か、キャッシュ**DNS**が攻撃を受けて、**Bad Cache**をつかんでいる状態**

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.

参考資料：応答例 Insecure



上位ゾーンに下位ゾーンのDSの登録なし

下位ゾーンにDNSKEY、RRSIGあり。

トラストアンカーからの信頼の連鎖が構築できないので、検証不能

たとえ、子ゾーンの署名内容が間違っていても検証されないのでBogusにはならない

署名のみしていて、DSが登録されていないゾーンが該当。

Copyright© 2012 SANYO Information Technology Solutions Co., Ltd. All Rights Reserved.