

# DNSSEC

Masakazu Asama @ NISOC

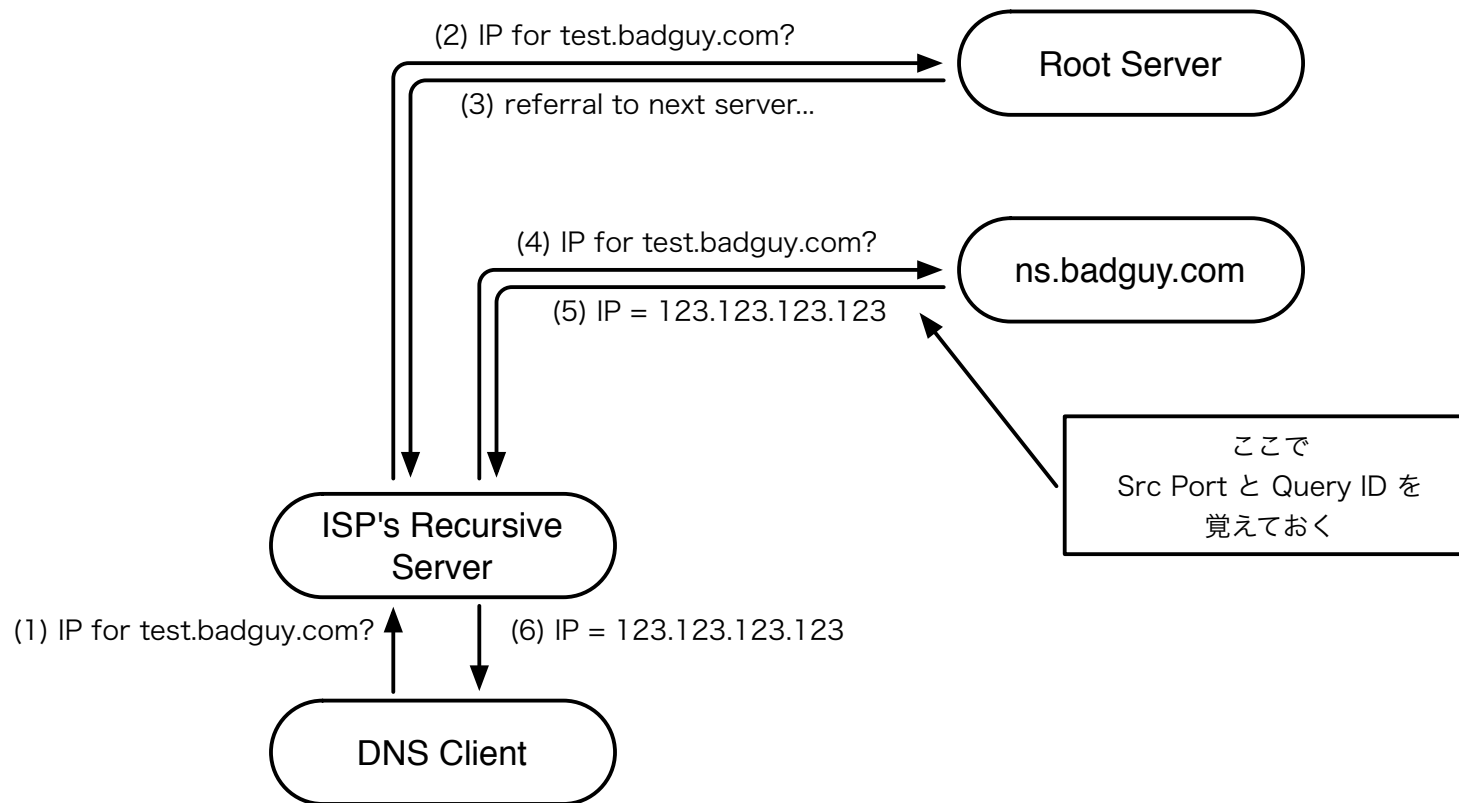
# What?

- “DNS SECurity extensions” の略らしい。
- DNS Resource Record(RR) に対し公開鍵暗号方式による電子署名を施し, 新たな RR として公開する. 検証者(Validator)は RR と公開鍵から署名を検証する。
- ある RR が存在しないことも証明可能。

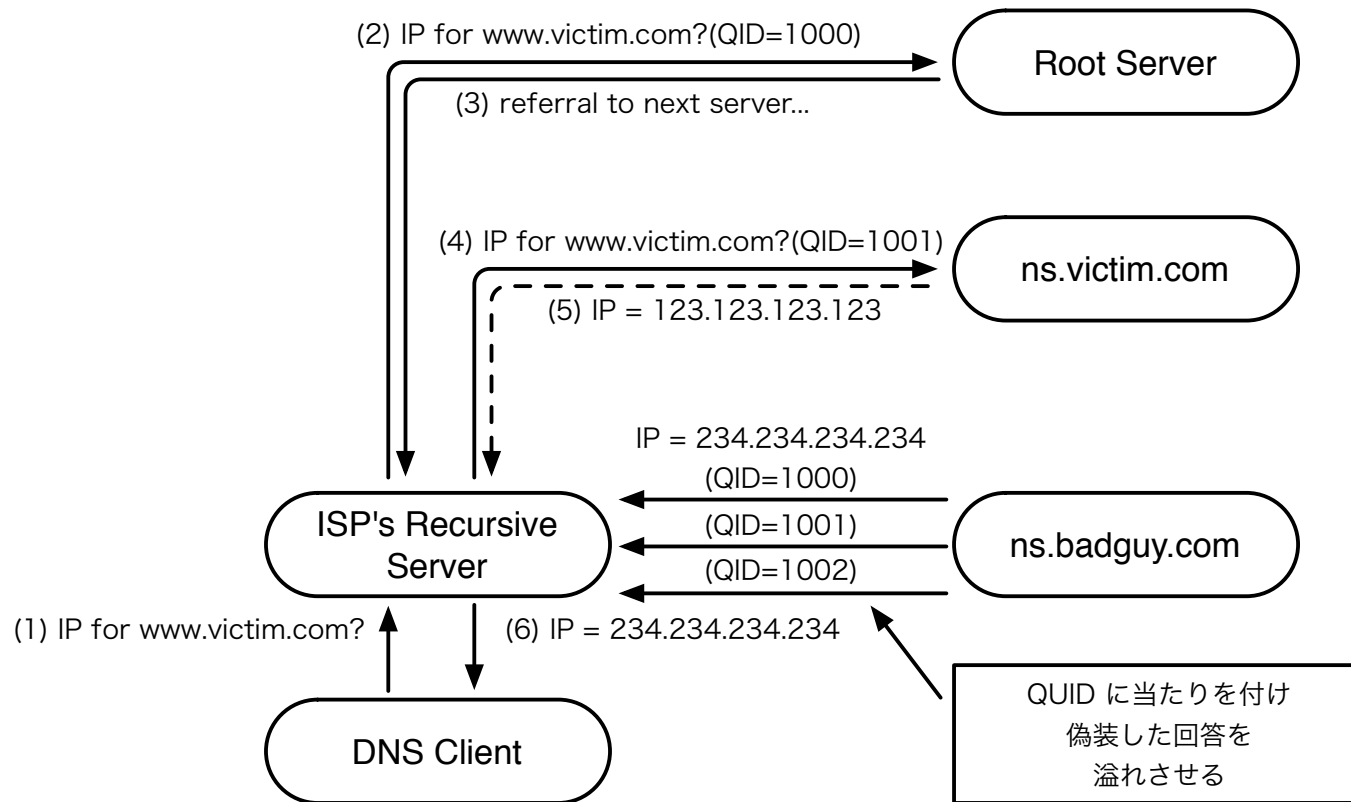
# Why?

- Thread Analysis of the Domain Name System(RFC3833):
  - ✓ Packet Interception
  - ✓ ID Guessing and Query Prediction
  - ✓ Name Chaining
  - ✓ Betrayal By Trusted Server
  - Denial of Service
  - ✓ Authenticated Denial of Domain Name
  - ✓ Wildcards

# The Kaminsky DNS Vulnerability (I)



# The Kaminsky DNS Vulnerability (2)



# 4 New RRs

- DNSKEY: 公開鍵を公開するための RR.
- RRSIG: 電子署名を公開するための RR.
- NSEC: 現在のオーナー名がもつ資源タイプの一覧と次に来るオーナー名を公開するための RR.
- DS: 親ゾーンが署名を委譲するための RR.

# DNSKEY

example.org. DNSKEY 256 3 5 AwEAAZbg..n7psoP8=

- The Flags Field: 8bit 目(256) が Zone Key かどうかのフラグ. 16bit 目(1) が Secure Entry Point(SEP) フラグ(後述). それ以外は現時点では 0.
- The Protocol Field: 常に 3.
- The Algorithm Field: 1=RSA/MD5, 2=Diffie-Helman, 3=DSA/SHA-1, 4=Elliptic Curve, 5=RSA/SHA-1(MANDATORY).
- The Public Key Field: 公開鍵を Base64 でエンコードしたもの.

# RRSIG

```
www.example.org. RRSIG A 5 3 86400 20091027075323 (
    20090927075323 7083 example.org. ifSp..yg== )
```

- The Type Covered Field: この RRSIG がどの資源タイプに対する署名か.
- The Algorithm Number Field: DNSKEY の Algorithm Number Field と一緒.
- The Labels Field: ラベルの数(この場合 www, example, org の 3 つなので 3).
- Original TTL Field: 署名対象 RR の TTL.
- Signature Expiration and Inception Fields: 署名有効期限と署名日.
- The Key Tag Field: 鍵の指紋.
- The Signer's Name Field: 署名するゾーンの名前.
- The Signature Field: 電子署名を Base64 でエンコードしたもの.

# NSEC

```
example.org.  NSEC      mail.example.org. (
                NS SOA MX RRSIG NSEC DNSKEY )
```

- The Next Domain Name Field: このオーナー名(上記例では example.org.)の次にくるオーナー名(上記例では mail.example.org.). このオーナー名が最後のときは一番最初のオーナー名とする.
- The Type Bit Maps Field: このオーナー名がもつ資源タイプの一覧.

# DS

```
example.org.      IN DS 18124 5 1 C9A8675E..E4A283F9
```

- The Key Tag Field: 鍵の指紋.
- The Algorithm Field: DNSKEY の Algorithm Number Field と一緒.
- The Digest Type Field: 0=Reserved, 1=SHA-1(MANDATORY), 2-255=Unassigned.
- The Digest Field: DNSKEY のオーナー名と DNSKEY の RDATA を結合しハッシュ化したもの.

```

example.org. IN SOA ns1.example.org. info.example.org. (
                2009072901 ; serial
                28800      ; refresh (8 hours)
                7200       ; retry (2 hours)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
                )
                RRSIG SOA 5 2 86400 20091027075323 20090927075323 7083 example.org. XNck..dQ==
                NS ns1.example.org.
                NS ns2.example.org.
                RRSIG NS 5 2 86400 20091027075323 20090927075323 7083 example.org. MRQp..oJ==
                MX 10 mail.example.org.
                RRSIG MX 5 2 86400 20091027075323 20090927075323 7083 example.org. TDvE..9w==
                NSEC mail.example.org. NS SOA MX RRSIG NSEC DNSKEY
                RRSIG NSEC 5 2 86400 20091027075323 20090927075323 7083 example.org. ggbs..Sg==
                DNSKEY 256 3 5 AwEAAZbg..n7psop8= ; key id = 7083
                DNSKEY 257 3 5 AwEAAAdMd..ZaDMP40= ; key id = 18124
                RRSIG DNSKEY 5 2 86400 20091027075323 20090927075323 7083 example.org. YckV..Lw==
                RRSIG DNSKEY 5 2 86400 20091027075323 20090927075323 18124 example.org. HE+Q..jg==
mail.example.org. IN A 192.168.4.1
                RRSIG A 5 3 86400 20091027075323 20090927075323 7083 example.org. ifSp..yg==
                NSEC ns1.example.org. A RRSIG NSEC
                RRSIG NSEC 5 3 86400 20091027075323 20090927075323 7083 example.org. DPOP..+A==
ns1.example.org. IN A 192.168.1.1
                RRSIG A 5 3 86400 20091027075323 20090927075323 7083 example.org. MoXm..jQ==
                NSEC ns2.example.org. A RRSIG NSEC
                RRSIG NSEC 5 3 86400 20091027075323 20090927075323 7083 example.org. WPGK..Yw==
ns2.example.org. IN A 192.168.2.1
                RRSIG A 5 3 86400 20091027075323 20090927075323 7083 example.org. TS7A..Eg==
                NSEC www.example.org. A RRSIG NSEC
                RRSIG NSEC 5 3 86400 20091027075323 20090927075323 7083 example.org. DgM5..0g==
www.example.org. IN A 192.168.3.1
                RRSIG A 5 3 86400 20091027075323 20090927075323 7083 example.org. OTme..kQ==
                NSEC example.org. A RRSIG NSEC
                RRSIG NSEC 5 3 86400 20091027075323 20090927075323 7083 example.org. LUDU..GA==

```

Key Tag = 7083 の  
秘密鍵で署名

Key Tag = 7083 の  
秘密鍵で署名

以下同様に署名...

Key Tag = 7083 の  
公開鍵

Key Tag = 18124 の  
公開鍵

# 信頼の連鎖

- そもそも RRSIG って信用していいの？
  - ❖ 親ゾーンがきちんと子ゾーンの DNSKEY と DS を検証し、公開することで署名が信頼できることを担保する。
- でも root ゾーンや jp ゾーンはまだ DNSSEC 対応してないよね？
  - ❖ 最終的には root ゾーンが DNSSEC 対応し、root ゾーンの DNSKEY をリゾルバが事前に知っているような世界になる。
  - ❖ 現時点では対応しているゾーンの部分木の根の DNSKEY をリゾルバに直接登録する(Trust Anchor)ことで署名の検証を行うしかない(Island of Security)。

# NSEC による RR 不在証明

- 該当するオーナー名の RR が存在しない場合:
  - ❖ 例えば example.org. の例で foo.example.org. の A RR を問い合わせると example.org. NSEC mail.example.org. ... が返される. NSEC 整列ルールでは foo.example.org. が仮に存在したとしたら example.org. と mail.example.org. の間に入るが example.org. の次は mail.example.org. ということなので存在しないと判断できる.
- 該当するオーナー名の資源タイプの RR が存在しない場合:
  - ❖ 例えば www.example.org. の CNAME RR を問い合わせると www.example.org. NSEC example.org.A RRSIG NSEC なので CNAME は存在しないと判断できる.

# 鍵署名鍵とゾーン署名鍵

- ゾーンの情報的大量に署名していると秘密鍵が割れてしまう危険性が高くなる.かといって鍵長を長くすると署名と検証に時間がかかって大変.かといって鍵を頻繁に交換して親ゾーンに DS を更新してもらうのは面倒.
- 鍵署名鍵(KSK):
  - ❖ 割と鍵長が長め.
  - ❖ Secure Entry Point(SEP) フラグ On.
  - ❖ こっちのみ親ゾーンに登録.ゾーン署名鍵の署名にしか使わない.
- ゾーン署名鍵(ZSK):
  - ❖ 割と鍵長が短め.
  - ❖ Secure Entry Point(SEP) フラグ Off.
  - ❖ ゾーンの署名にはこっちを使う.鍵署名鍵よりは簡単に更新できる.

# DO, AD and CD

- DNSSEC に対応した問い合わせのために以下の 3 つのオプション・フラグが定義されている。
  - ❖ DO: DNSSEC OK. 問い合わせ側が DNSSEC に対応していることを示し, 応答メッセージに DNSSEC 関連の RR を含めることを要求するためのもの.
  - ❖ AD: Authenticated Data. 承認済みデータの意味. DNSSEC をサポートするネームサーバからの応答はこのフラグがセットされる.
  - ❖ CD: Checking Disabled. ネームサーバに対してリゾルバ側で検証ができるので DNSSEC の検証についてかまわないでほしいと伝えるためのもの.

# How?

- Step 1) 権威サーバで KSK/ZSK の鍵ペアを生成.
- Step 2) 生成した秘密鍵でゾーンを署名.
- Step 3) 署名時に生成された KSK の DS RR を親ゾーンに登録してもらう.
- Step 4) 適当なタイミングで ZSK を更新し, 新しい ZSK でゾーンを再署名する.

# When?

- root
  - ❖ ...on the goal of an operationally Signed Root Zone as soon as feasible in 2009.
  - ❖ ICANN to Work with United States Government and VeriSign on Interim Solution to Core Internet Security Issue
    - <http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm>
- jp
  - ❖ ...2010年中を目処にJPドメイン名サービスへ導入する予定で準備を進めています。
  - ❖ JPドメイン名サービスへのDNSSECの導入予定について
    - <http://jprs.jp/info/notice/20090709-dnssec.html>

# References

- DNS Security Introduction and Requirements  
- <http://tools.ietf.org/html/rfc4033>
- Resource Records for the DNS Security Extensions  
- <http://tools.ietf.org/html/rfc4034>
- Protocol Modifications for the DNS Security Extensions  
- <http://tools.ietf.org/html/rfc4035>
- Threat Analysis of the Domain Name System (DNS)  
- <http://tools.ietf.org/html/rfc3833>
- An Illustrated Guide to the Kaminsky DNS Vulnerability  
- <http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>