DNSSECの現状

第15回 JPNICオープンポリシーミーティング
2008年11月27日
藤原和典 <fujiwara@jprs.co.jp>
株式会社日本レジストリサービス

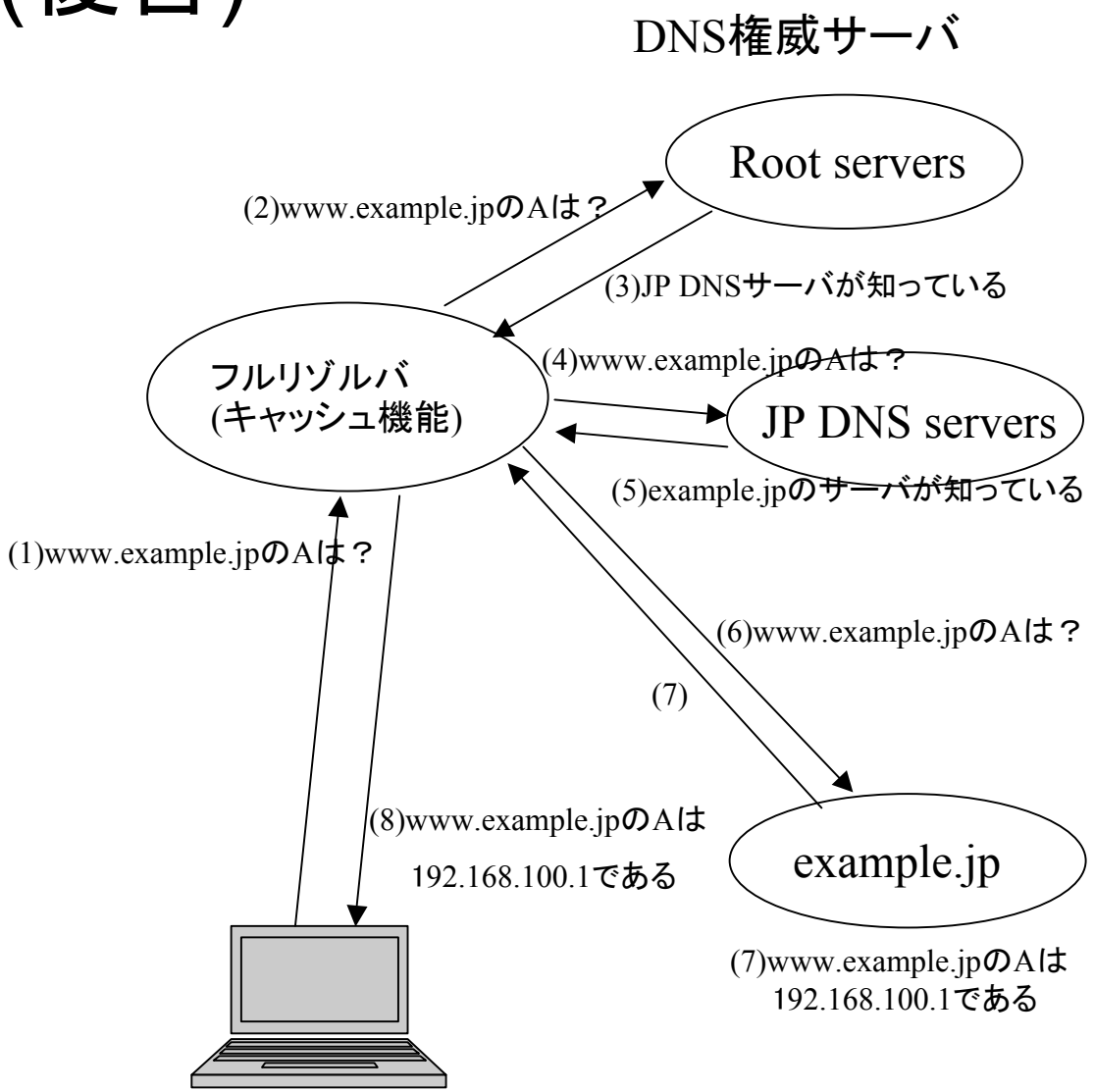
内容

- DNSへの攻撃
  - Kaminsky Attack
- DNSSECの概要
- DNSSECの動向
- DNSSECの運用
- まとめ

- DNSSECの検索例

DNSの動作(復習)

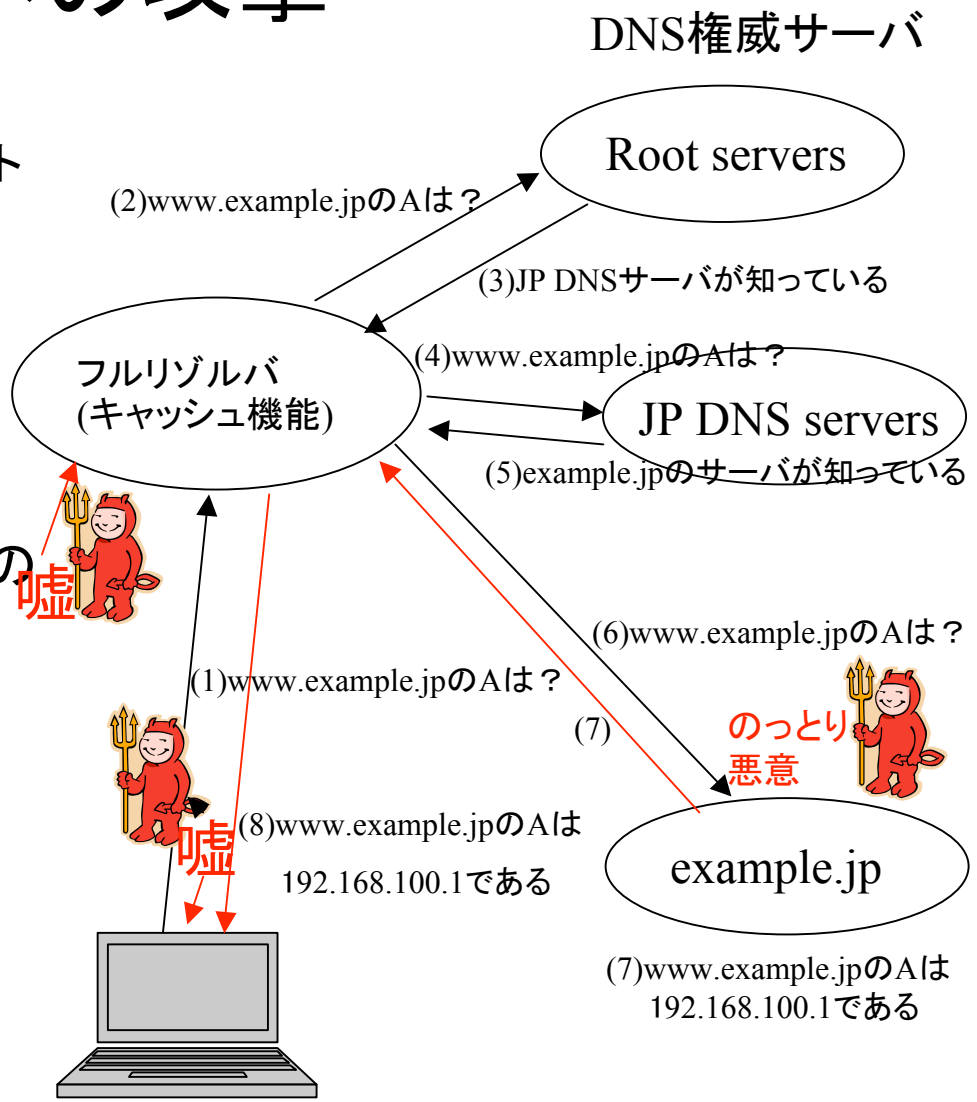
- ユーザのマシンはISPのフルリゾルバに問い合わせを行う(1)
- フルリゾルバはRootから順にたどり、アドレスを解決する(2～7)
- フルリゾルバはユーザのマシンに得られた結果を回答する(8)



よく知られたDNSへの攻撃

- Monkey-in-the-middle
  - 共有イーサネットや無線LANでパケットを盗聴し、嘘の応答を先に返す
  - (1)を見て(8)より前に嘘を返す
- キャッシュポイズニング
  - (3)や(5)、(7)を推定し、嘘を注入
  - バースデーアタック
  - Kaminsky Attack (後述)
- 嘘のglueを書いておき、フルリゾルバのキャッシュに注入
  - 他人の名前のAを返すなど(7で)
  - 多くの実装で無視するようになった
- DNSサーバそのものの乗っ取り

- RFC3833 Threat Analysis of the Domain Name System (DNS)にまとめられている



Kaminsky Attack

1. 概要
2. 危険度
3. 対策
   - Source Port Randomization
   - DNSSEC

Kaminsky Attackの概要

- Dan Kaminsky氏によって発見／報告された効率的なキャッシュポイズニング手法
  - US-CERT Vulnerability Note VU#800113
  - ¬ http://www.kb.cert.org/vuls/id/800113

- 基本的には昔からあった手法と同じで、問い合わせに対して本物の権威DNSサーバからの応答よりも先に偽の応答を到達させる手法

- これまでのキャッシュポイズニング
  - DNSのクエリーIDは16bitのIDであり1つの攻撃パケットによる攻撃成功率は65536分の1
  - フルリゾルバが外部の権威DNSサーバに問い合わせに行くのはキャッシュにその問い合わせの情報がない場合
  - したがって、キャッシュした情報の有効期限(TTL)が切れるまでは攻撃が繰り返せなかった

Kaminsky Attackの危険度

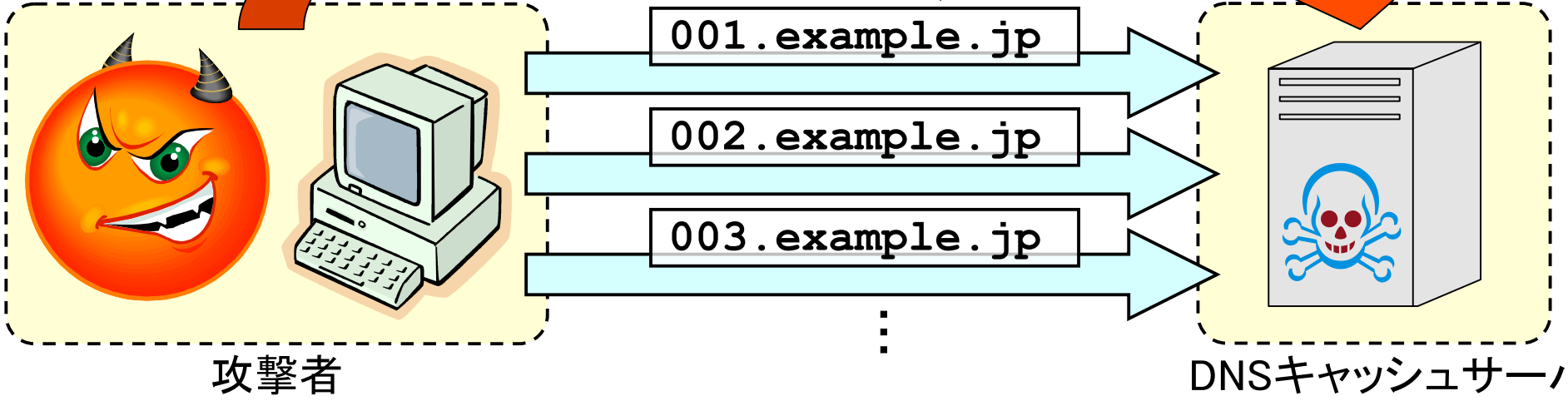
- 今回の手法の要点は、
  - 「同一ドメイン名の存在しない名前」を利用し
  - 連続的に攻撃が繰り返せる点
  - 秒数万パケット送ることで、数秒で汚染可能

- 攻撃者はフルリゾルバに対してDNSクエリを送ることができる必要がある
  - オープンリゾルバは危険
  - ただし、ISPの正規利用者なら楽に攻撃可能
  - 受動的攻撃(リンクを踏ませる)、メールを送る等も可能

②IPアドレスを詐称し、NSとAをセットにした偽の応答を送り続ける

①キャッシュが効かないように、ホスト名を変えながら問合せを繰り返す

```
example.jp        NS  www.example.jp
www.example.jp    A   192.0.2.1
```



カミンスキー・アタックが従来の攻撃方法と異なる点

1. 攻撃目標となる名前に対し連続・繰り返し攻撃が可能
2. 一部実装では既存のキャッシュが無効化される
   （上記の例ではwww.example.jpが既にキャッシュされていても上書きされる）

http://jpinfo.jp/topics-column/009.pdfより引用

Kaminsky Attackへの対策

- Source Port Randomization
  - 問い合わせ時のソースポート番号をランダム化
    - 7/8(US時)パッチ、CERT VU#800113の情報公開
    - その一ヶ月後に開催されるBlackHatで詳細な手法の公開の予定となっていたが、実際には、7/21に情報が漏えいしてしまったため対応の緊急度があがった
  - 当初のパッチは性能の大きな劣化があったためISPなどでは採用が難しかった
    - このため、しばらくは危険なまま運用されていたところもあった
  - 攻撃の成功確率を下げるための対策手法
- DNSSEC
  - DNS応答の正統性を検証できる仕組み
- その他
  - クエリーIDが正規のものではない応答がたくさんくる攻撃の特徴を検知
  - 攻撃を検知した場合、TCPで再度クエリ

DNSSECの概要

DNSSECとは

- DNSセキュリティ拡張(DNS Security Extensions)
- DNS利用者が受け取ったDNS応答の正統性を検証できる仕組み
  - 正統とは、DNSゾーン管理者が作成・公開したデータであること
- DNSゾーン管理者が自ゾーンに電子署名を追加
  - JPゾーンにはJPレジストリが電子署名を追加
  - example.jpゾーンにはexample.jp管理者が電子署名を追加
- 署名に使用した鍵情報を上位ゾーンに登録
  - example.jp管理者はexample.jpの電子署名に使用した鍵の公開鍵情報をJPレジストリに登録
- DNS利用者は電子署名が追加されたDNS応答の正統性を検証
  - ルートからの信頼の連鎖をもとにルートから末端まで検証

公開鍵暗号

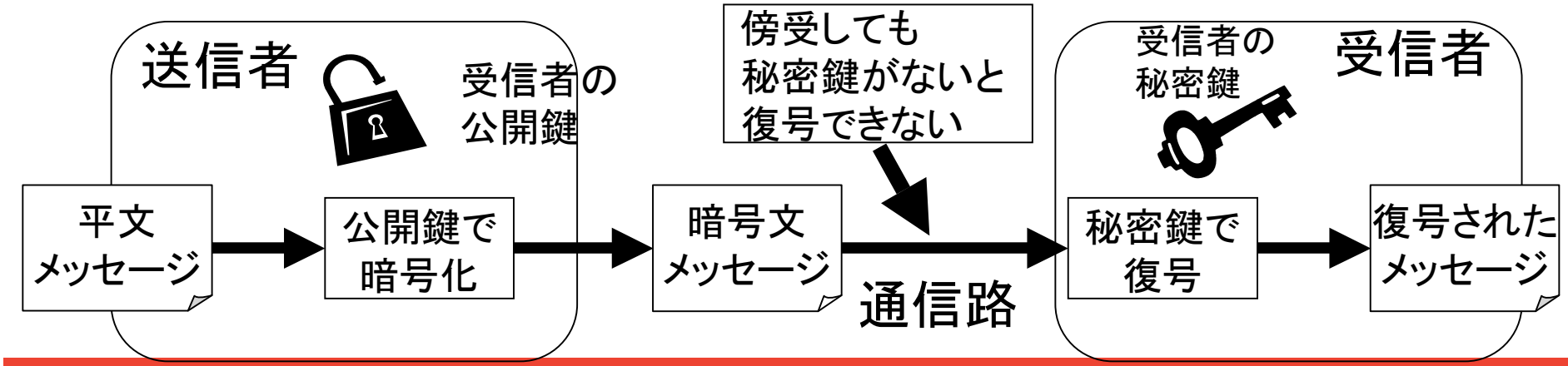
暗号化・復号に異なる鍵(秘密鍵と公開鍵)を用いる暗号方式

- 受信者の公開鍵で暗号化したものを、受信者の秘密鍵で復号(暗号通信)
- 送信者の秘密鍵で暗号化したものを、送信者の公開鍵で復号(電子署名)
- 代表的な公開鍵暗号方式: RSA暗号

秘密鍵

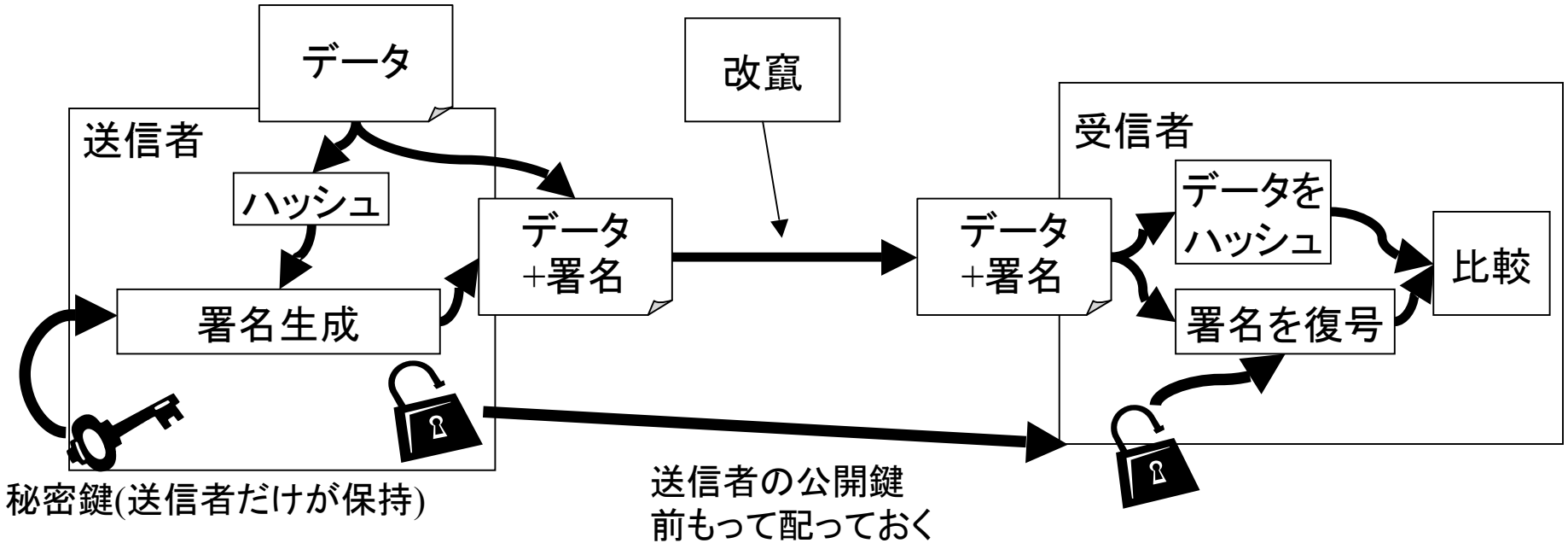
公開鍵
広く配布

- 暗号通信
  1. 受信者はあらかじめ公開鍵を広く公開
  2. 送信者は受信者の公開鍵で暗号化
  3. 受信者は本人の秘密鍵で復元
  - 秘密鍵は受信者のみが秘密に管理、秘密鍵を持つ受信者のみが復号可能
  - 秘密鍵を他人に伝える必要がない



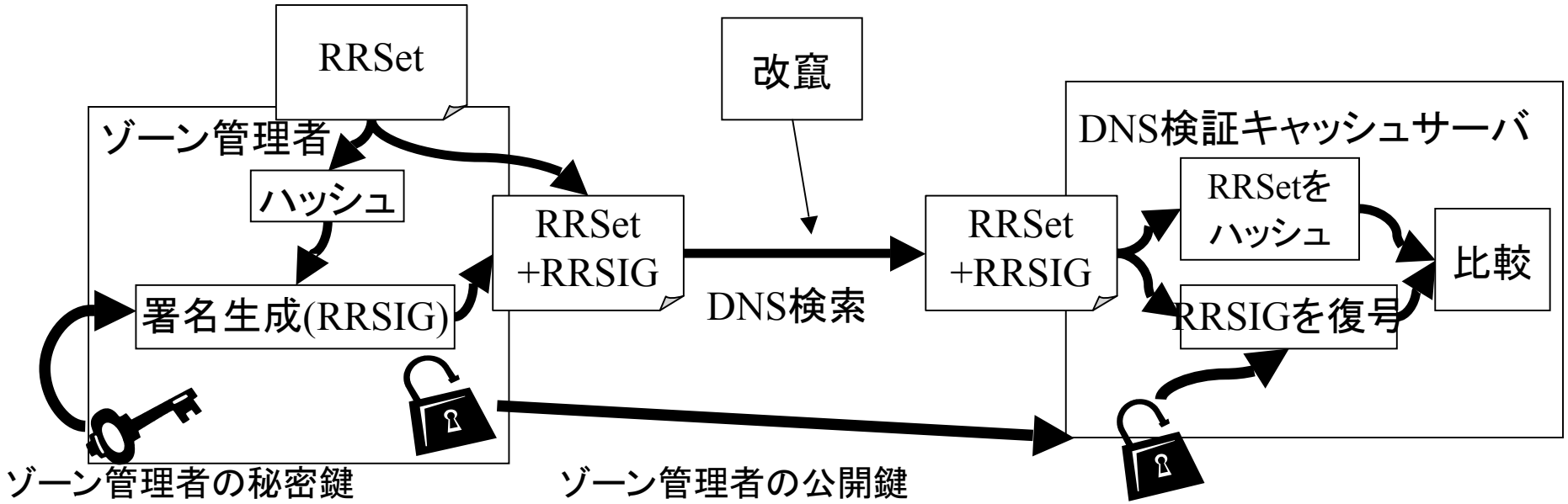
電子署名の概念

- 署名には、元データを圧縮した値(ハッシュ値)を用いる
- 送信者の秘密鍵でデータのハッシュ値を暗号化したものが署名
- 公開鍵で署名を復元するとハッシュ値が得られる
- 受信者は、データのハッシュ値と、復号したハッシュ値を比較、同じであれば、送信者が電子署名したデータであると判断できる
  - 送信者の秘密鍵は送信者しか持たないため



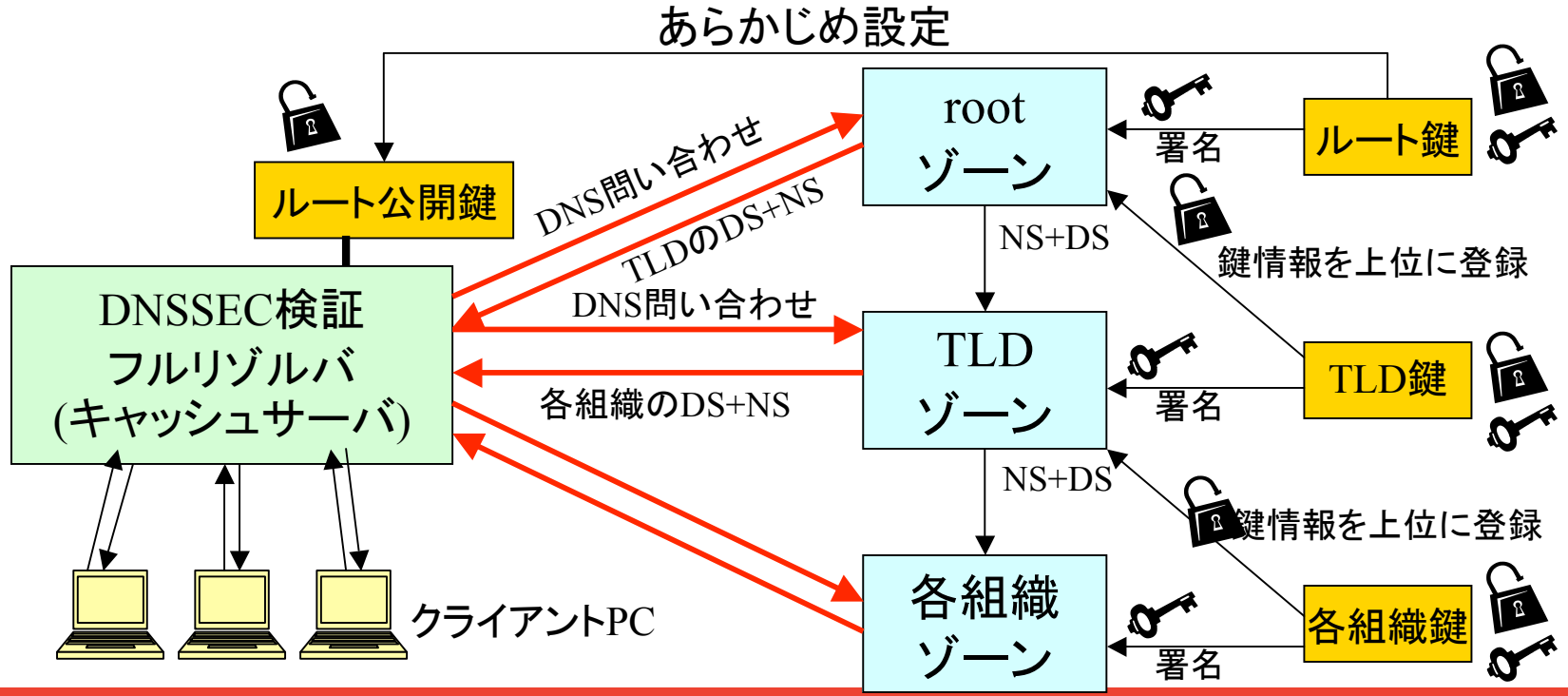
DNSへの応用 (DNSSEC)

- ゾーン管理者は、署名のための鍵対(秘密鍵、公開鍵)を作成する
- ゾーン内のリソースレコード(RRSet)を秘密鍵で署名する
  - www.example.jpのAや、AAAA
- DNSサーバはDNS応答に署名(RRSIG)を添付する
- ゾーンの公開鍵を知っていれば、RRSIG RRの署名を復号してゾーン情報と比較し、署名の検証が可能



信頼の連鎖

- 公開鍵の情報を上位レジストリに登録し、鍵による信頼の連鎖 を形成
  - 公開鍵をハッシュ化したもの(DS)を鍵情報として上位レジストリに登録
  - レジストリは、NSとグルーに追加して鍵情報をルート/TLDゾーンに記述
- ルート公開鍵をフルリゾルバ(DNSキャッシュサーバ)に登録するだけで、各組織までのデータを検証可能



DNSSECで追加されたリソースレコード

- DNSKEY
  - 公開鍵を保持
  - DNSKEY フラグ プロトコル アルゴリズム 公開鍵そのもの

- RRSIG
  - 電子署名を保持
  - RRSIG Type Algorithm Labels OriginalTTL 署名有効期限 署名有効開始時刻 鍵タグ 署名ドメイン名 署名そのもの
  - 署名対象のリソースレコードと同じパケット内に入る
  - 対象とするタイプ (A, AAAA, NS, DS, MX, SOAなど)
  - 署名有効期間
  - 署名に使われた鍵の情報 (署名ドメイン名、鍵タグ)

DNSSECで追加されたリソースレコード(2

- DS
  - DS 鍵タグ アルゴリズム DigestType DNSKEYのハッシュ
- 不存在証明のために用いられるRR
  - NSEC
  - NSEC3
  - NSEC3PARAM

DNSKEYの例

% dig @sec3.apnic.org 193.in-addr.arpa dnskey +dnssec

;; ANSWER SECTION:

193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAbTh+xrW1mbNvOyCEUcRS+BrfCHNgLXlyrb5t67m2uzJLR7W1qYx
lvT7juAwCu+1aue7IVPRBWX6WRtdsB0Xa9tTNcGAgV33TRuPPuaCnoX0
ZunxgqFon6LOratVCTNP2QoYA5oHybcTYwmP673AErGbKHbOEkmnO+Xd
3PeUrK5iYGg0vwV6nEkvQ6NlO2fFYc5H9kJtESiYE4LRnjUn8QbMfFhZ
TvHvT3JhCV+ikNy8SFjDxnggZBEpjP+z1PwhxfKUeri+gO9wH9Z01oBQ
D6OjLsuMeW+cqa1A0ofNKF/B+AOSmt91fUaVHB+IdCyP/hJW0Ov/TEhx ykxTJnzw0jM=

193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAdqNdfquJqmZ/fwt5zHqreU2qtomhLEPrsPTYruMmtzd514ZfAnR
RWH7qrO2eQTQ2mZMIVkq6JgHhjEAgP/PzDuHo9UaDrgGj1DYupKKLBy+
BGiT8Atv/JdbU7yIARenQsw7/7WG8Zx4SHcwfSPCs/BNKkeCR8RB4zJY
mUTnxsUf7CRYYBtNDeJK//h67a2TzIpuqwM/gstMNzRyx09ucHhY0ZAZ
vidxY7j2OOUHgw8ihkdJD7id7Qi8RQ+3oYyZkq1iR7KgnqXq5+EVQy5+
ESGGUpR1zx8cSbeEmuNmaas1g1vluzNk2SZcUoWWoTA8DGNv4eGuk8p2 4BxIpQ9ZAo8=

193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAZ6b6cw/eUsDJrrL/z8Fu8pyHPSVM4UFlwWV3mfmW7fmpgCF7ZUZ
4/6tW77D7cBtr1mhv/LddaEj0546rti8IPvvZc2XJ7Ki+oETBhbR0gJz
YO6J1PuYF7kD3pIhuAqRX4f5Yu2hdD66a24Shvi5uCYcqUa1yJiUYENU
S+Vs/zJlKX6g+kP36YkQHV9YdI/ZubFndZKNzw==

193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAdTh0A7i2uE4iUQHmpDNwiwI5Eh9m5xJIHaO8XOk3nMqjOEhHtOi
0C5p55S/iNxqSnGnCEhyZCyVOp/phJcqDTCxJKKgqCwCOiSNbFgg2TOR
4gM0Y4FBSFqW7Y1HOWvsi0mfk1yxKhN3T6/RvI3VEHHwZyB8TgizQDXn
JatD7Ti9DYErGuQMkWbBcT9mJguFlMxtlVAQhQ==

RRSIG省略

PTR+署名の例

```
% dig @sec3.apnic.net 193.0.0.193.in-addr.arpa ptr
    +dnssec
;; ANSWER SECTION:
193.0.0.193.in-addr.arpa. 172800 IN     PTR     ns.ripe.net.
193.0.0.193.in-addr.arpa. 172800 IN     RRSIG   PTR 5 6
    172800 20081226062618 20081126062618 27381
    0.0.193.in-addr.arpa.
    gpP3wJt6VlFgm0bmZaGF2Oq/azHpBKksnq04O4Ah/dB
    hM8+gehmcyr3sFbjZsM35tPZO84bfhsj9AY8VxXOU+9FI
    Ucu94knjLYiVEnsMKp2ujhq0lMhAX8vZ+WLo/uuom0Be
    ePC+vPxZe0cUaUPT/FRJY6e2koL6MNcbvQIiGK8rd9o
    w87S2xd/tNnSKkbK4jl//hKli
```

署名者は0.0.193.in-addr.arpa

DSの例

```
% dig @ns.iana.org 193.0.0.193.in-addr.arpa ptr +dnssec
;; AUTHORITY SECTION:
193.in-addr.arpa.       86400   IN      NS      NS-EXT.ISC.ORG.
193.in-addr.arpa.       86400   IN      NS      SUNIC.SUNET.SE.
193.in-addr.arpa.       86400   IN      NS      NS3.NIC.FR.
193.in-addr.arpa.       86400   IN      NS      NS-PRI.RIPE.NET.
193.in-addr.arpa.       86400   IN      NS      SEC1.APNIC.NET.
193.in-addr.arpa.       86400   IN      NS      TINNIE.ARIN.NET.
193.in-addr.arpa.       86400   IN      NS      SEC3.APNIC.NET.
193.in-addr.arpa.       3600    IN      DS      48367 5 1
    2E2A517038612ED376F1CB498E294A80DDD5FF60
193.in-addr.arpa.       3600    IN      DS      38779 5 1
    F1BCC8E8193A855F867BB0D8C05333C278FD4563
193.in-addr.arpa.       3600    IN      RRSIG   DS 5 3 3600 20081201172521 20081125165521
    49170 in-addr.arpa.
    BDosTbhIlWoewN3QyJzPsYP0kcTwTO7lscKG2SLSA5+/jZnaauR9FMy0
    iT/8jQer5E9jimDeytmugdPOlhAh4NxG7zJQGrnlhTcmr2t2lmdSkSSL
    nyukj+OR612hCxRFJOfTPqGiKYcSft+2mwOMZ48zcc6IhPmSoVTDTkn3 X3g=
```

署名者はin-addr.arpa

DNSSECでの検証結果

- ルートからの検証が成功
- 信頼の連鎖が成立しない
  - DSが登録されていない → DNSSEC非対応
  - DSと公開鍵が一致しない → エラー
- 署名検証失敗 → エラー
  - 署名有効期間ではない
  - 署名と署名対象データが異なる

DNSSECが解決しないこと

- 改竄・騙りは発見できるが、正しいDNS検索結果は別途得る必要がある
  - キャッスポイズニングなどの攻撃で検証エラー
    - TCPで再検索？
  - そのままではアクセスできない
- DNS応答の正統性が保証されたとしても、その後の通信の安全を保証するわけではない
  - 通信路のハイジャック、盗聴はDNSでは防げない
  - TLS/SSLやIPsecなどと併用
- FAQ
  - DNSSECではDNS応答を暗号化するのか？
    - 暗号化しない

DNSSECの動向

各組織の動向

- IETF
  - プロトコルは既に策定済
  - 現在は、プロトコルの細かなバグ(ERRATA)の修正などを実施
- IANA
  - 2007/6からルートゾーンへの署名をテスト運用
  - https://ns.iana.org/dnssec/status.html
  - 鍵の管理方法が決まればすぐにでも開始できる準備をしている
- 米国　.GOV
  - 2009年に登録組織をふくめたDNSSEC対応を実施予定
  - 2008年11月14日に.GOVゾーンをDNSSEC対応(署名)実施
    - 現在はoff
- 米国商務省電気通信情報局
  - National Telecommunications and Information Administration (NTIA)
  - DNSSECに対するパブリックコメント募集 (2008/10/9 ～ 2008/11/24)
    - IANAからの提案やVeriSignからの提案も提示
    - ルートゾーンのDNSSEC対応方法の検討

各組織の動向 (TLD)

- DNSSECサービスを開始しているTLD
  - .SE　スウェーデン
  - .BR　ブラジル
  - .CZ　チェコ　2008/9?開始
  - .PR　プエルトリコ　2006/7
  - .BG　ブルガリア
  - .MUSEUM

- .SE　スウェーデンのサービスについて
  - 2007/2 DNSSEC商用サービス開始
  - 銀行や国内ISPと組み、フィッシング対策として実施
  - DNSSEC鍵登録は別料金
    - 年間120SEK (約2000円)　維持料とほぼ同じ
    - 無料化予定 (2009年)
  - 国内大手ISPが既に.SEの公開鍵をフルリゾルバ(DNSキャッシュサーバ)に設定

各組織の動向 (TLD)

- DNSSECのサービスを開始すると表明しているTLD
  - .GOV
  - .ORG
    - 2008/4 ICANNに対してDNSSEC実装を提案
    - 2010年までに段階的に導入予定 (2010年には登録者に広く提供)
  - .UK　(DNSSEC RFCの著者が所属)
  - .CA
- その他
  - VeriSign (.COM, .NET)
    - DNSSEC RFCの著者が所属
    - 2010年までのProject Titanで、new DNS security protocolを実装することを表明

各組織の動向(逆引き関連)

- RIPE NCC
  - 管理するゾーンのDNSSEC対応を実施済み
    - https://www.ripe.net/projects/disi//keys/
    - ゾーンへの署名
    - 登録者の鍵情報の登録
    - RIPE NCCが管理する逆引きゾーン
      - たとえば、193.in-addr.arpa
    - ENUMゾーン
      - e164.arpa
    - RIPE NCC自身の正引きゾーン
      - ripe.netなど

RIPE NCCでのDNSSEC鍵情報登録

- RIPE DBのDOMAIN objectに”ds-rdata:” attributeを追加
  - DSリソースレコードの値をそのまま記述
  - 例: ds-rdata: 64431 5 1 278BF194C29A812B33935BB2517E17D1486210FA
- DOMAIN object:

domain: [mandatory] [single] [primary/look-up key]
descr: [mandatory] [multiple] [ ]
admin-c: [mandatory] [multiple] [inverse key]
tech-c: [mandatory] [multiple] [inverse key]
zone-c: [mandatory] [multiple] [inverse key]
nserver: [optional] [multiple] [inverse key]
ds-rdata: [optional] [multiple] [inverse key]
以下略

http://www.ripe.net/rs/reverse/dnssec/registry-procedure.html

ソフトウェアの対応状況

- ISC BIND 9.3~9.5
  - .SEやRIPE NCC提供のものに対応可能
  - 署名機能、DNSSEC検証機能を含む
  - 差文署名実装済み(ドキュメントは不十分)
- ISC BIND 9.6
  - .ORGなどが使用を検討している方式に追加対応 (NSEC3: RFC 5155)
  - 定期的な自動再署名機能内蔵
  - ただしまだベータ版で、バグも確認されている
- NLNetlabs NSD 3、Unbound
  - NSEC3まで対応
  - 署名機能は実装していない
- dnssec-tools project
  - http://www.dnssec-tools.org/
  - DNSSEC検証ツール
  - DNSSEC対応アプリケーション
  - DNSSEC対応firefox-1.5

DNSSECの運用

権威DNSサーバでのDNSSEC署名手順(1)

1. BIND 9.3以降(9.6以降)を導入
2. 鍵対(秘密鍵、公開鍵)を作成
   - 例: dnssec-keygen -a RSASHA1 -b 2048 -n zone {ゾーン名}
   - 鍵ファイルが生成される
     - K{ゾーン名}+005+{数字}.private (秘密鍵)
     - K{ゾーン名}+005+{数字}.key (公開鍵、DNSKEY RR)
3. 鍵対の公開鍵情報(DNSKEY RR)をゾーンファイルに設定
   - 例: echo '$INCLUDE K{ゾーン名}+005+{数字}.key' >> example.jp
4. 秘密鍵を用いてゾーンに署名
   - 例: dnssec-signzone {ゾーン名} K{ゾーン名}+005+{数字}
     - 署名済みゾーンファイル {ゾーン名}.signed が生成
     - 署名されたファイルをゾーンファイルとしてnamed.confに指定する
   - 上位に登録する情報が生成
     - dsset-{ゾーン名}ファイル

権威DNSサーバでのDNSSEC署名手順(2)

5. named.confのoptionsにdnssec-enable yes; を追加
   - 9.5ではデフォルトで設定されている

6. 生成されたdssetを上位ゾーン・レジストリに送り設定してもらう
   - RIPE NCCならばds-rdata項目

7. 署名有効期間に注意し、定期的にシリアルを進めて再署名し、ゾーンファイルを更新
   - 署名有効期間は一ヶ月程度、終了よりもTTL前には更新する必要あり

フルリゾルバ・検証サーバ (キャッシュDNSサーバ)

1. BIND 9.3以降または9.6以降を導入
2. 信頼ツリーの最上位の公開鍵情報を取得する
   - 信頼ツリーが複数存在する場合は、その分だけ必要
   - 定期的に変更される
3. 取得した公開鍵情報をtrusted-keysとしてnamed.confに設定する
   - IANAのテストベッドに対応する場合

```
trusted-keys {
    "." 257 3 5 "AwEAAff8EiNa/S3wovNzPUmuBqe1pSjnNoen
      cXDNMpmjTgngGMPct+8KDKxM6FwvPSRx15gN
      RyRQfzSPU0WshDNkBV2TMtVpzqn/dsurbmTo
      ixRzLyLK2Kd2adg5o5yS/gaTgCo0HVBmIruS
      N3FVI2ugCWJBFLkFGHLvMJ0BTSYVqWGwQIzp
      EPKCbKN+L9nrLcvJRCWG59Yq6BUsSEKlzSK3
      jMhYQs6y5IiCGAVol+3VyjN93/lXkeUG6u7d lQsyiY9fxfeUvmn004y0TjAgjZqdwKZB0K9M
      A7qcALG3Tw2TXEdQsn9aY3DzNii3YEBidzER mY7n4hIUri1r59MnuNJq2x0=";
   "." 257 3 5 "AwEAAbWMiPoQlFp+snq84lbEPx2kPgessP91
      ieS+jeablsxi9tE9MCbEeCrRqPtKT1p50l+C 0cvapYFAsg8VhyDIM1Tpyw8KHTgh267GciKf
      VkxRRZy68ndKRHC/bq8zqD4cYxVdJofTblAm bxdX8OdYwtJ7ZFS7B14aSSQ/1y/8stX+l3oA
      PgSbclhjCMKzHOloR9npD6gGJpUud5zoyG1+
      GkVvuD7XPQpzmqO8KAyMz7/Nh2MmJHzfWp4L
      glqT4cdCT/S8YTdE46I9+vDGlhknHlyEyI5m
      P9kZWXZa58wWbv9ZBTzN0PNPWQHfPWp045wU AqrRagTbRs7sWw/fpKgC5I0=";
};
```

4. named.confのoptionsにdnssec-enable yes; を追加
   - 9.5ではデフォルトで設定されている

DNSSECの課題 (1)

- DNS応答パケットが大きくなる
  - DNSKEYやRRSIGが大きい (最大256バイト)
  - 全体で1000から4000バイトのパケット
- ブロードバンドルータの問題
  - DNS Proxyの実装に不具合がある例が報告されている
- アプリケーションから違いがみえない
  - アプリケーションのDNSSEC対応を考える必要あり
  - ブラウザの鍵マークのようなもの

DNSSECの課題 (2)

- 容易な運用方法がまだない
  - 定期的な鍵更新・鍵の取り扱い
  - 定期的な再署名
  - ルート鍵の配布・更新
  - 自動ツールやDNS運用サービスがないと運用困難
- フルリゾルバ(キャッシュサーバ)の更新が必須
  - ISPのフルリゾルバ
  - DNSSEC検証に必要なCPUパワーの検討が必要
- 自組織以外に、上位ドメイン(ルート、TLD、RIR、LIR)でのDNSSEC対応が必要

まとめ

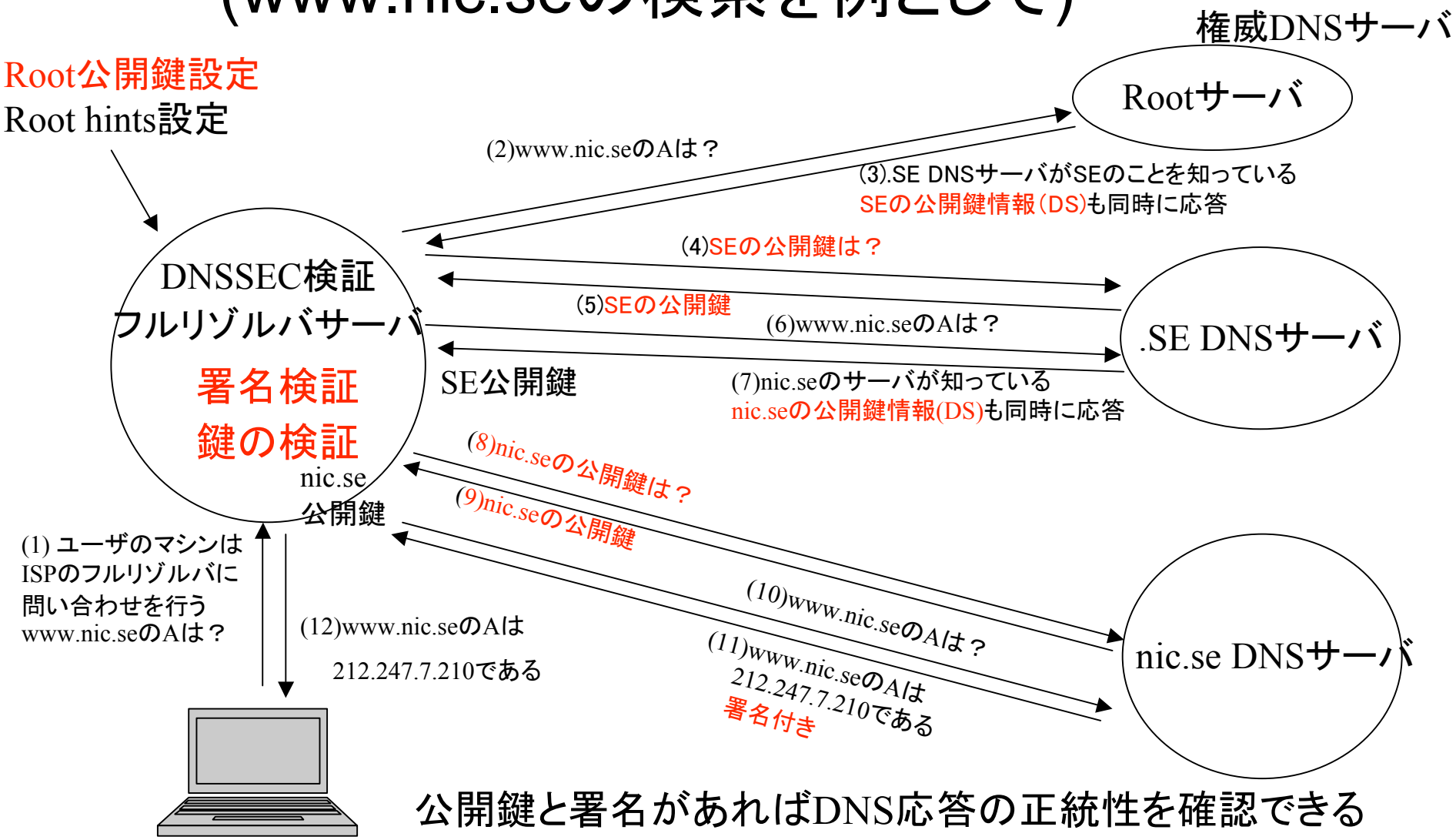
- 従来のDNSには改竄などを確認する手段がない
  - 攻撃可能
- DNSSECはDNS応答の正統性を確認できるようにする拡張
- プロトコルは決まり、ソフトウェアも開発されてきた
- 一部のTLDやRIRでDNSSECのサービスを開始
- 運用コストは増加
  - 定期的な署名•鍵更新
  - パケット長　→　回線の太さ
  - 検証に必要なCPUパワー
- DNSSEC対応の準備が必要

Questions?

DNSSECの動作概要と動作例

- IANAのルートサーバテストベッド
- .SE
- RIPE NCCの逆引き

DNSSECの動作概要 (www.nic.seの検索を例として)



公開鍵と署名があればDNS応答の正統性を確認できる

IANAテスト環境ルートサーバへ www.nic.seのA問い合わせ

```
% dig @ns.iana.org www.nic.se +dnssec
;; AUTHORITY SECTION:
se.             172800  IN      NS      B.NS.se.
se.             172800  IN      NS      D.NS.se.
se.             172800  IN      NS      I.NS.se.
se.             172800  IN      NS      F.NS.se.
se.             172800  IN      NS      H.NS.se.
se.             172800  IN      NS      J.NS.se.
se.             172800  IN      NS      G.NS.se.
se.             172800  IN      NS      C.NS.se.
se.             172800  IN      NS      A.NS.se.
se.             172800  IN      NS      E.NS.se.
se.             3600    IN      DS      6166 5 1
    CE2B007F6D000B064B4A82E8840C19D3D09B8F8E
se.             3600    IN      DS      49678 5 1
    6672948B37E6B7B3EFE87FB711849EF17786C8E3
se.             3600    IN      RRSIG   DS 5 1 3600 20081202001433 20081125234433 10386 .
    mB0MrC5vjP52l/XrYkUTE6B5/cZXWJopCwB+zGtS4XaD6nhIJVWcDxv0
    s4l+9kim8c8DzObjdejy5MTQmZjEMSRIjZGEnBh+PD/aDcCjJ55rXHBC
    zD4nfscpEqvx5rTV5yW9OyvhAhsWNNit0hXxYl5yEthSPXO/gyvlLw5H uio=
```

.SEのDNSサーバへ SEのDNSKEY問い合わせ

```
% dig @a.ns.se SE. DNSKEY  +dnssec
;; AUTHORITY SECTION:
se.             3600    IN      DNSKEY  256 3 5
    AwEAAa1dxi4igz3Beqf8duqvUJBwl3ZFhexAlENmMyGS3LLytTXiNCer
    qojQxtScl4lQjbl/PMmL1UbOIx9jm9+7JIa1ISfghptRk+g9PltKVerQ+KSIHPRydxjTYDVpZtjdmCNw
    Wy5SCPwf7h83siagAO+uS1WeZ1pRDR0 J2miM+7r
se.             3600    IN      DNSKEY  256 3 5
    AwEAAcSG3TSr/HbjbQL1S9YC1mFnxwKfgyPOVcDgeVYJh5Q+7tjBAlbvXSPENbqNusxtPE9HB/
    h+5rwe7PFHuuFCiMRgQlMq+KUVFwc2N4g9w4ZlFtTEb3anr3CjaSuspNbbPJWfqCNMaX5HokY
    QmSkS/k7JiOyqJRnXOY7O eb6WeN07
se.             3600    IN      DNSKEY  257 3 5
    AwEAAb6xRZHEf+PyF5dxEvz0BHEHbziu6iZaiNW/yjSaZcmrmZiRMF8FPppD+XuKSau0rgu4eB
    wYdpkEoMVR4FhI8frkuPHIue2LP1ETo+2hCrdr60K1538yLvzbOhMxXt6knjPN+OlalMmCknadaof
    Kga5FLKOPQs2C3nw6AH4WUNGrchmDMVBwRwfZdQXYZTXesqULmGMK7mwjQGOxerRDQ
    WrFv8Nh NnVV31PihaYBdQ1TJjvfGS/FYZJwv/BddiELiLeUnNWu3AOsRAshgOcD
    BOAPUvKJNEq6RHELFmvXOOe2d8H2yzv02EMQik6GwUm16DrSdmX+SWfe lQs+9ELFN6k=
se.             3600    IN      DNSKEY  257 3 5
    AwEAAdKc1sGsbv5jjeJ141IxNSTdR+nbtFn+JKQpvFZETaY5iMutoyWHa+jCp0TBBAzB2trGHzdi
    7E55FFzbeG0r+G6SJbJ4DXYSpiiELPiu0i+jPp3C3kNwiqpPpQHWaYDS9MTQMu/QZHR/sFPbUn
    sK30fuQbKKkKgnADms0aXalYUuCgDyVMjdxRLz5yzLoaSO9m5ii5cI0dQNCjexvj9M4ec6woi6
    +N8v1pOmQAQ9at5Fd8A6tAxZI8tdlEUnXYgNwb8eVZEWsgXtBhoyAru7
    Tzw+F6ToYq6hmKhfsT+flhFXsYso7L4nYUqTnM4VOZgNhcTv+qVQkHfO OeJKUkNB8Qc=
se.             3600    IN      DNSKEY  256 3 5
    AwEAAZtfqzh+nTAox8jx3Kik+25bW8SgkJqZzZF+XlhjbhpdyHbKMTSQtMwbNsVMICCicw838PUk
    Vdell7wciCBX6+s0FUTK4XZvsIjypZsI6ih65s3oxpw2+oz1IGWLeK0EtU4sdsTO49P+BdhB2XWBx
    D+onTRiEZr/N2qO FFODEDed
RRSIG省略
```

.SEのDNSサーバへ www.nic.seのA検索

```
% dig @a.ns.se www.nic.se +dnssec

;; AUTHORITY SECTION:
nic.se.             86400   IN      NS      ns3.nic.se.
nic.se.             86400   IN      NS      ns.nic.se.
nic.se.             86400   IN      NS      ns2.nic.se.
nic.se.             3600    IN      DS      16696 5 1
    EF5D421412A5EAF1230071AFFD4F585E3B2B1A60
nic.se.             3600    IN      DS      16696 5 2
    40079DDF8D09E7F10BB248A69B6630478A28EF969DDE399F95BC3B39
    F8CBACD7
nic.se.             3600    IN      RRSIG   DS 5 2 3600 20081201014919 20081125121248
    56172 se. NUmo4Jwm63RBqMoiDIL1PlWS2BUZ5VNijof/Da41Eh6Xf2ZUFl5M6QHw
    81xZBMr9KPWvZl4g7gb2W3l5/jEHvezoVpTa+PjTJVKUfYjpOvwdRGFZ
    1aStfNtO/oFMcsSLKsmSxB7N+sScrh93c3x3eFHifbbp/tGaN3Aj/opA vMY=

;; ADDITIONAL SECTION:
ns.nic.se.          86400   IN      A       212.247.7.228
ns2.nic.se.         86400   IN      A       194.17.45.54
ns3.nic.se.         86400   IN      A       212.247.3.83
```

nic.seのDNSサーバへ nic.seのDNSKEY検索

% dig @ns.nic.se nic.se dnskey +dnssec

;; ANSWER SECTION:

nic.se. 3600 IN DNSKEY 256 3 5
AwEAAcLIeHMnCcD7J+m779vTxhk2mNUJXW/8MwOvu8FvQFRTM4AoIc/v
TkULkBWBqA8Gh/x7TrwE2NCQLg1oFJg9ykzG6FsLQt+B1iwa2wDvW4L4
GTrTjjqSqpRob5MXA40dWiW7t3FEI+z/R/ai/O0MY477zdTbob/IUBJU UJsAyhGx

nic.se. 3600 IN DNSKEY 256 3 5
AwEAAcL+VP4WMgpr9BoJyh8Hvpfh7wAcJLeG551774GynUBF8faMkXPL
VULFR8vcfYRyMrdYBZ8gZRJrFDqP15frIju3JXrP1tb3pb1QGHb6n4qQ
oM53nDwLaZFGDeAcs2iwwl04ic8020UmGhUcQzI4ClHdCkPO3s0/7Mv3 xaXUTXlB

nic.se. 3600 IN DNSKEY 257 3 5
AwEAAdhJAx197qFpGGXuQn8XH0tQpQSfjvLKMcreRvJyO+f3F3weIHR3
6E8DObolHFp+m1YkxsgnHYjUFN4E9sKa38ZXU0oHTSsB3adExJkINA/t
INDlKrzUDn4cIbyUCqHNGe0et+IHmjmfZdj62GJlHgVmxizYkoBd7Rg0
wxzEOo7CA3ZadaHuqmVJ2HvqRCoe+5NDsYpnDia7WggvLTe0vorV6kDc
u6d5N9AUPwBsR7YUkbetfXMtUebux71kHCGUJdmzp84MeDi9wXYIssjR
oTC5wUF2H3I2Mnj5GqdyBwQCdj5otFbRAx3jiMD+ROxXJxOFdFq7fWi1
yPqUf1jpJ+8=

RRSIG省略

nic.seのDNSサーバへ www.nic.seのA問い合わせ

```
;; ANSWER SECTION:
www.nic.se.          60     IN     A      212.247.7.210
www.nic.se.          60     IN     RRSIG  A 5 3 60
    20081202051001 20081122051001 54675 nic.se.
    fDiGr0+P5gR/05oEb82YTNqTz7xiTN4VUHT4kWePiip37
    n9F2yBgc4OO9rZotypaXWTR0PGHqqLaSvCKx88QjBlk
    3kMeI52z5MWisMhWUhysn1/WPP2HKra5tmpXWw7WI
    Y6PuGreWF9EuDD7TDgamjNF6j2f+wq9G7VXzAfa 67I=
;; AUTHORITY SECTION:
略
;; ADDITIONAL SECTION:
略
```

www.nic.se A検証

1. ルートの公開鍵は検証サーバに設定済
2. SEのDS + ルートによる署名
3. SEのDNSKEY(公開鍵)
4. NIC.SEのDS + SEによる署名
5. NIC.SEのDNSKEY(公開鍵)
6. www.nic.seのA + NIC.SEによる署名

- 結果としてwww.nic.seの署名検証可能

逆引きにおける動作例:
193.0.0.193.in-addr.arpa

ルートへの 193.0.0.193.in-addr.arpa PTR問い合わせ

```
% dig @ns.iana.org 193.0.0.193.in-addr.arpa ptr +dnssec

;; AUTHORITY SECTION:
193.in-addr.arpa.       86400   IN      NS      NS-EXT.ISC.ORG.
193.in-addr.arpa.       86400   IN      NS      SUNIC.SUNET.SE.
193.in-addr.arpa.       86400   IN      NS      NS3.NIC.FR.
193.in-addr.arpa.       86400   IN      NS      NS-PRI.RIPE.NET.
193.in-addr.arpa.       86400   IN      NS      SEC1.APNIC.NET.
193.in-addr.arpa.       86400   IN      NS      TINNIE.ARIN.NET.
193.in-addr.arpa.       86400   IN      NS      SEC3.APNIC.NET.
193.in-addr.arpa.       3600    IN      DS      48367 5 1 2E2A517038612ED376F1CB498E294A80DDD5FF60
193.in-addr.arpa.       3600    IN      DS      38779 5 1 F1BCC8E8193A855F867BB0D8C05333C278FD4563
193.in-addr.arpa.       3600    IN      RRSIG   DS 5 3 3600 20081201172521 20081125165521 49170 in-
    addr.arpa. BDosTbhIlWoewN3QyJzPsYP0kcTwTO7lscKG2SLSA5+/jZnaauR9FMy0
    iT/8jQer5E9jimDeytmugdPOlhAh4NxG7zJQGrnlhTcmr2t2lmdSkSSL
    nyukj+OR612hCxRFJOfTPqGiKYcSft+2mwOMZ48zcc6IhPmSoVTDTkn3 X3g=
```

→ 署名者はin-addr.arpaのため、in-addr.arpaの公開鍵が必要

193.in-addr.arpaの公開鍵を検証可能

ルートへのin-addr.arpa DS検索

```
% dig @ns.iana.org in-addr.arpa ds +dnssec

;; ANSWER SECTION:
in-addr.arpa.        3600    IN      DS      13771 5 2
        5933822A0219260F7B8BE3030CDA6171ACCDFA4A7D15FF571812E587 D50546CC
in-addr.arpa.        3600    IN      DS      51667 5 1
        288F3711631A2FABDBF405450372F410BA826EB8
in-addr.arpa.        3600    IN      DS      51667 5 2
        1F84AD17794909D4E22C79AF83F6D66F8ADF2FE2EEC593DE4E07F615 7AF76791
in-addr.arpa.        3600    IN      DS      13771 5 1
        D46CB35D7A1F48CAA75613759C087E1AF8996BF5
in-addr.arpa.        3600    IN      RRSIG   DS 5 2 3600 20081201172537 20081125165537 50007
        arpa. o6HheKzgC3UgCzBIr9htGNDcO0PJ5XNvjJ0IPTGn12WRMStmG2dD3dkG
        OQJ8LQZDUUY7qW04aEGZiwhHlXBJ86IX3yEwDV8C1kfMy5zFzf3g/K2z
        Tb2GkJ37luagYbYbBbRdJ7MSe04I0PU+6J0w5JlMEwxnfViae9iPBp0H 4Fk=
;; AUTHORITY SECTION:
arpa.                518400  IN      NS      pch-test.iana.org.
arpa.                518400  IN      NS      ns.iana.org.
arpa.                518400  IN      RRSIG   NS 5 1 518400 20081201172537 20081125165537 50007
        arpa. YXDBYo+Nlb997aEXYEOvGejyEEtI9eC6sU1Bpk9vbTYbgFY4YD9+RNJm
        fZvbWwgW9y/lwkxQyyr85Z7Ut8EUC0XWvsWFTsc7JckU+sdG/DBp8Zb1
        o54gMzjmBCZAtlaZbNneD2sHr5WOA/OTJ5mtlU3EW9iEwN47EeJH9lgN PB8=
```

→ 署名者はarpa.のため、arpaの公開鍵が必要

ルートへのarpa DS検索

```
% dig @ns.iana.org arpa ds +dnssec

;; ANSWER SECTION:
arpa.           3600    IN      DS      28808 5 1 734BB562A98364F21D4D47671E5BB6577FE9D849
arpa.           3600    IN      DS      28808 5 2
        47C0DF9C6AC7408CFBD59F4D66E21FB3314AEEBFCD4BA237DA05FF18 B1189626
arpa.           3600    IN      DS      53018 5 1
        535BB7466E21C7C21E0DC09957EF42AAA055C1DD
arpa.           3600    IN      DS      53018 5 2
        87B205F87E55D3E5CA82EA1514E3D846D0E2C1BFBBEFEE9B4D7EBE72 4F33C362
arpa.           3600    IN      RRSIG   DS 5 1 3600 20081202001433 20081125234433 10386 .
        WoB12xhLi1xPIPOe0zD1Pq2AwE8ifrmYuCC/Qi5Kwkm3aRB52bEmRdKo
        MZ75LaEscmuMri0frx3sf4GT5Xfl/PSMQ8+oXstapoCZP4AlvjDEMwBh
        yX6HEK2dt6hLBDQMzymcp9VTbQvyMN0OFL2Ls/jgTLrpnPqTCZ49J1M4 O1k=

;; AUTHORITY SECTION:
.               518400  IN      NS      ns.iana.org.
.               518400  IN      NS      pch-test.iana.org.
.               518400  IN      RRSIG   NS 5 0 518400 20081202001433 20081125234433 10386 .
        HoHvelCLEanFEriPViVt17MTqQmxTq9AZtxegJ/MDBhvT4NW6HOJ2xZU
        aUP7lJ3VwO/1yFNkKjlqM5FW3DwMtOw/Vbw2Nv/TYS3/loHfG7HN/1BF
        hMFobejdJ5mSNAsEBvsTm7OOvm9KZlmMVPlnEVqn6Jb5y3FQ3fasEiq/ MRc=
```

→ 署名者はルートなので検証可能

arpa zoneへのarpa DNSKEY検索

% dig @ns.iana.org arpa dnskey +dnssec

;; ANSWER SECTION:

arpa. 3600 IN DNSKEY 256 3 5
AwEAAb6YtLEOkcX8Hfz1Dxs6UPf/auOfuQVVJDHQP0qy8vuZ7t50PdoP
tiXoH5yj94iwrkdzZQdgNgCZ7UaUMm9SVd7j7qpmSKONJ8CANP2d2JYG
fmVd2b7NonS3B4w846YZCmL2A3gqh8s52no+E8ua/+JzNb0hQ4M52MM/ JTkZFb4N

arpa. 3600 IN DNSKEY 257 3 5
AwEAAav5jjkZHDaYmpuBSLRBUjrkA91uk9r7CpM0HB4weCoWO9btxJ9M
likcxh6oJVEsVXYfXu6COuppWmcs2lkaNCTuRGdvzbI/bSBMPY2D+uP0
I2FjWZ8nPJeYZNRqmllHQuno98lJ6tiQu//rExiDBYVekkp99p/KfKh1
a+X6DvXi3qfPTLBEM21JgQGRqVK1nPHowJsvoVr9T6LpuEBsACrA0Dhm
f23y3q3lGuaUR3I4Rf2f78BiOXVc1ywZ+cW+fr9NDfjkY2S6XIHU3SAa
pyTHP56pWpMHRj0ZMXyp2lYs6U+zI8OipdrloICz4XTVmeXGoLin0Gow Z8pBvQf3bLk=

arpa. 3600 IN DNSKEY 257 3 5
AwEAAcGe8bTqSxvwHvanBDyEoV0RClXSQBlzMPsPKUlkCzwMTkjMjNOy
J6hLPA9b94ltE8bVhBNHMiZTm7UBniHtglnknyx3Uy4LALrBCxYERVfM
28o+ij3kNoUAMlUZJYbcZ5E+frdmOoQ6lWxeYoXmqCOOl8lRbjT+gSy6
hoaNvphD/U/VMnUpjPzI7tgYtPVvqe7QLh62HEjmzhs9CGqddmrFCAhu
fg/I8tPSGw++tRT9kI5mYN/Y35plx3WcUQ5fFdRqP6tFneKGCDIDYCtm
fq6rjEmGBz5VHAVzJyzLtfAQBoEpAfvnQjOWqmoaMCFXF9E6yBEJaB7I NtP7oYSqS3E=

arpa. 3600 IN DNSKEY 256 3 5
AwEAAcdoTLpVE69wOUzSpJVTHd6eHeXh74hzIehCwZv9QBjAOueQkmZq
lWjfqRlnCBFgZApziQQmoTqMJyfxL1eeQ6uxekh1B4RSAwrjw8CKD0q7
Yv/f3Tq6XttbpZwq2PzPan3yjrKjQ5lAhUiuMmlyPf/2FfwnNaagesol PsHcQ+Ih

arpa. 3600 IN DNSKEY 256 3 5
AwEAAcCzsNAzdq39SD8qRtTSP5cwkjRijj48p28UX6YVbkInPBCKPPYN
FM0Kq4SnmyyVCur2+g4q1OO3EZzunFU/qqxVmekb0NYKLj5+TsqecstG
rDEVgeIy6umqy8odNVDXvji8YyOhiDIopWSvx+ajmviabb8LhTwSwKDy H5w9GLDb

RRSIG省略

in-addr.arpaゾーンへのin-addr.arpa DNSKEY検索

% dig @ns.iana.org in-addr.arpa dnskey +dnssec

;; ANSWER SECTION:

in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAdcwgXk+fVXKP4pjDRbxURHEg5xC/22kpoKPqd7kp6d0cUBNOFXz
lAzu0oL0lPkt9pG9aZnd+aIa9p9Pl5VaaHSkrYoZy4wswphTyzRzkGn3
Uk4an5lCFdEq80lFDgkh3WBEhnlKv7lVpM24bp2t53WDupFSOWEoSxy1
iQ49NLStAPswYQhTKhrz2fPCq7gXlRSD/W72LL3teS2cndCWq4Ui0m1v
MxFH8DJxOw2l8ARM0P2BeBpNBQgG2v6v4wN7YhlxDBI+VD7pa4VedMDx
cG2Bm2p2Mn/20s46HyUOjUbQWLrJ/3JfjKY30uprw9P+5NMFyibkOK/k AvN/iJfIrLU=

in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAfG9PZQvT9Fr8/QnRNQ9ZYVlWYCLgeOMw5uX4Kf/thPthfqteTDr
BMciJMl02xUyF2Z4UWgC8Pq449UKn3Psqby6X59P0/kQp6+Me6apaSVM
dBHnfNZCVKOL8V4F5AScLFBY6D+59fI2b76Bel+NNIRQcJRxqYBY8t/v ken1poAB

in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAe10kqEdoSgo8bnUhuuTMF0Tg0gmjlioQC/XeHoQd/bIa3h/6aQ8
qn+7SWLqsbpuJpn1VgoqXCNLn+oJGqOgcbLRXUFywwKVnfRmHm/L9bnE
rqdST/4shkKh/XHBThOoAxPzf4mx/AUmXkhEBxVN3GVLe93Cz+WFmqQq cXKdnrjp

in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAcdIBQJMuiyDXTO86cBsbPnqbon7OyWwW92rM+/vSeVJxHKcRkYW
dHK8n8pGjyO8bEM6ZPx4ogF9uafB+VsPtfkUw9BRR24yWcfm3Q8/cFtu
CqW28irVqCuas0lMdvw0hxjo/kpbir4FT5MVvde+ZlR1V9Pg+cWqvcM1 zY2WFqBx

in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAcNF+NK6ZTvr6JNptCBtDVB404U+AZ89E2r3tN1sStDTsgFZ7/9Z
ORS6NJ+68e56g5V2Tak7+KFTylXwQhj3w3o84iu/8V4YxDUcXfKd8H2d
K4ow5nJJcbYoaObKULCv0VjuZ/5UKXLh56rCpiNrTmS1ixJcnWV/TjCH
cTrPT5o/NbsulfhHKDCGwSoRho298f0IJsYFFNM8+5/QqDY07RmhxWLL
030W6ur/EeT8GfRzVORExYlmgSqvhDAXsvP5WbPzlmcfyrJgaMQDSI+N
0Jy+qRafCQbJubQRDpVXSvAj5LJLefttEkon1DQKJX5+oWKlGz7fOU5V UnV4axsLsmU=

RRSIG省略

sec3.apnic.net(193.in-addr.arpaゾーン)への 193.in-addr.arpa DNSKEY問い合わせ

% dig @sec3.apnic.org 193.in-addr.arpa dnskey +dnssec

;; ANSWER SECTION:

193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAbTh+xrW1mbNvOyCEUcRS+BrfCHNgLXlyrb5t67m2uzJLR7W1qYx
lvT7juAwCu+1aue7lVPRBWX6WRtdsB0Xa9tTNcGAgV33TRuPPuaCnoX0
ZunxgqFon6LOratVCTNP2QoYA5oHybcTYwmP673AErGbKHbOEkmnO+Xd
3PeUrK5iYGg0vwV6nEkvQ6NlO2fFYc5H9kJtESiYE4LRnjUn8QbMfFhZ
TvHvT3JhCV+ikNy8SFjDxnggZBEpjP+z1PwhxfKUeri+gO9wH9Z01oBQ
D6OjLsuMeW+cqa1A0ofNKF/B+AOSmt91fUaVHB+IdCyP/hJW0Ov/TEhx ykxTJnzw0jM=

193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAdqNdfquJqmZ/fwt5zHqreU2qtomhLEPrsPTYruMmtzd514ZfAnR
RWH7qrO2eQTQ2mZMIVkq6JgHhjEAgP/PzDuHo9UaDrgGj1DYupKKLBy+
BGiT8Atv/JdbU7yIARenQsw7/7WG8Zx4SHcwfSPCs/BNKkeCR8RB4zJY
mUTnxsUf7CRYYBtNDeJK//h67a2TzIpuqwM/gstMNzRyx09ucHhY0ZAZ
vidxY7j2OOUHgw8ihkdJD7id7Qi8RQ+3oYyZkq1iR7KgnqXq5+EVQy5+
ESGGUpR1zx8cSbeEmuNmaas1g1vluzNk2SZcUoWWoTA8DGNv4eGuk8p2 4BxIpQ9ZAo8=

193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAZ6b6cw/eUsDJrrL/z8Fu8pyHPSVM4UFlwWV3mfmW7fmpgCF7ZUZ
4/6tW77D7cBtr1mhv/LddaEj0546rti8IPvvZc2XJ7Ki+oETBhbR0gJz
YO6J1PuYF7kD3pIhuAqRX4f5Yu2hdD66a24Shvi5uCYcqUa1yJiUYENU
S+Vs/zJlKX6g+kP36YkQHV9YdI/ZubFndZKNzw==

193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAdTh0A7i2uE4iUQHmpDNwiwI5Eh9m5xJIHaO8XOk3nMqjOEhHtOi
0C5p55S/iNxqSnGnCEhyZCyVOp/phJcqDTCxJKKgqCwCOiSNbFgg2TOR
4gM0Y4FBSFqW7Y1HOWvsi0mfk1yxKhN3T6/RvI3VEHHwZyB8TgizQDXn
JatD7Ti9DYErGuQMkWbBcT9mJguFlMxtlVAQhQ==

RRSIG省略

sec3.apnic.netへの 193.0.0.193.in-addr.arpa PTR問い合わせ

% dig @sec3.apnic.net 193.0.0.193.in-addr.arpa ptr +dnssec

;; ANSWER SECTION:

193.0.0.193.in-addr.arpa. 172800 IN PTR ns.ripe.net.

193.0.0.193.in-addr.arpa. 172800 IN RRSIG PTR 5 6 172800 20081226062618 20081126062618 27381 0.0.193.in-addr.arpa. gpP3wJt6VlFgm0bmZaGF2Oq/azHpBKksnq04O4Ah/dB hM8+gehmcyr3sFbjZsM35tPZO84bfhsj9AY8VxXOU+9FI Ucu94knjLYiVEnsMKp2ujhq0lMhAX8vZ+WLo/uuom0Be ePC+vPxZe0cUaUPT/FRJY6e2koL6MNcbvQIiGK8rd9o w87S2xd/tNnSKkbK4jl//hKIi

→署名者は0.0.193.in-addr.arpaのため、0.0.193.in-addr.arpaの公開鍵が必要

sec3.apnic.netへの 0.0.193.in-addr.arpa DS問い合わせ

```
% dig @sec3.apnic.net 0.0.193.in-addr.arpa ds +dnssec

;; ANSWER SECTION:
0.0.193.in-addr.arpa.   172800  IN      DS      62161 5 1
    A22665A026E149743C9F63866DAB71054F994EDF
0.0.193.in-addr.arpa.   172800  IN      RRSIG   DS 5 5
    172800 20081226060503 20081126060503 19017
    193.in-addr.arpa.
    hB1z79efpJs+Km6o1IhDmxsc8N9WAnxcREfrwRR+hFy
    K30XuGs6RpLqWEm+J9bOF2QUtpQkNlk9gjK4LNDiJf3
    u24mI5ehUTnQNAJKTpDtNpL+zhI0shphfyooSjrIgvqMV
    mQCUaRhQTRwS9IlBoiypQh5niT77AYmDPxDwoi/VsPJ
    6EjsOJ1MXgiohU87ci6yVpWIAi
```

→193.in-addr.arpaの公開鍵で検証

sec3.apnic.netへの 0.0.193.in-addr.arpa DNSKEY問い合わせ

% dig @sec3.apnic.net 0.0.193.in-addr.arpa dnskey +dnssec

;; ANSWER SECTION:

0.0.193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAcZVDWNpWWxQKJNqvGuvQIv4A5XvSjGhINVbTkBqQtn1TyAlN4kg
d93B6V1AEkF5wQTnYYq/oa0xa8/ccSkC+liVtE8vuPCGCOJEi/SWHeaB
/8WOlT+G80MXJeP2or9WfO5Xr5ilmOsyDKuTPRrhRxYZ6VuwlbkFT5e2
GhzwQtl6e1gzCIQe2kTC8lGujPIYttaA8X0qdQ==

0.0.193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAd/xGA7JyJXzAfH+x3EMdMJlNuGerkVTO/zi33fJM0n6z8X6W9+GGZJh3/NrXYCnPLS1oV
FPQ5wQ9p/5k2cYcVziwCAnad31GlEF9b5aoT3EfyVTiSyD2A4BOWb2H+AUkqvstrzsGJQfxdk0T
Ep08UXK15z6w26ud1gtXBHnzSI3leykzG2I2HTPFbKdtCBu33D1O0DL3Y4KG7N9+/SVqeW2k89
9qx02aijijvuPG5q6SIySDjZWseq0pxaNgxnSRLugMrZdPxYAKS9hs+/GYyDSCZpWfmsSfhd34MC
vC/Y7KKUlRyL97j76sKzuazBeAFx7Cpc/qNSD MUfX7vyBxUU=

0.0.193.in-addr.arpa. 3600 IN DNSKEY 257 3 5
AwEAAeo8t5uEFRfCx/FULbfs/7Aiwx58/Yvf+cQmxSMZmD2n8eCr8d2qf26KKQjbCJjm2u4x2QZdz
CPBVz2oI4YI1jVpZCc+AqyBYU4/A5VXKx7tTxir2y2sfOvHEN8j8E9j6EEipvsaBM4HF0oWQbmFT
xcSwd1Y5Avpcipz/5AVd63ZJx+KUWP7JdG+HbptNdQ9girh7oZp4Ign9nlWppNUnBUr6FFmpTHT
PdhK8k0bDsgsBp4ftwT7EqheXAXs3AFxvf7n/ocJKlsgtYNyfY5ApuV6dKWmr0I/jPotp1vh5VqCyLY
5gQTE3j4EprsSxwTbTAn142LoKatm vtAH4wFHPL8=

0.0.193.in-addr.arpa. 3600 IN DNSKEY 256 3 5
AwEAAap67CwjbScyNAX2AMdLlHEzYzfXqV3Gb8JPWtv6vzE9NQ+FUBNu
ctt6gfr1C4MLRfW6efhXLVdk44HuIiiG6CZvVXrs+2HbjTBCgcOq+ovvdihKcHNdiTLYysj1yaAvWp2
En7Heq3r7/6Fn0YdiIFHyiJ/DZRR4VgjU TKH7rTELJ+6a6ZNIa7qAvFu4mP/k6CkkkKd8Kw==

RRSIG省略

193.0.0.193.in-addr.arpa PTR検証

1. ルートの公開鍵は設定済
2. arpaのDS + ルートによる署名
3. arpaのDNSKEY(公開鍵)
4. in-addr.arpaのDS + arpaによる署名
5. in-addr.arpaのDNSKEY(公開鍵)
6. 193.in-addr.arpaのDS + in-addr.arpaによる署名
7. 193.in-addr.arpaのDNSKEY(公開鍵)
8. 0.0.193.in-addr.arpaのDSと193.in-addr.arpaによる署名
9. 0.0.193.in-addr.arpaのDNSKEY(公開鍵)
10. 193.0.0.193.in-addr.arpaのPTRと、0.0.193.in-addr.arpaによる署名

結果として193.0.0.193.in-addr.arpaの検証が可能

逆引きの検証での注意点

- 同じサーバに親・子・孫ゾーンが存在する場合はすべてのDSとDNSKEYを取得する必要がある
  - 正引きではあまりみかけないが逆引きでは頻繁
  - 193.in-addr.arpaと0.0.193.in-addr.arpaが同じサーバ
  - ルートとarpa、in-addr.arpaが同じサーバ
  - アルゴリズムに従った実装が可能
- 外部名DNSサーバもDNSSECにより名前解決する
  - 今回の例ではsec3.apnic.net
  - しかしながらDNSSECではDNSサーバではなく、ゾーンの内容の署名であるので、DNSサーバ名が署名検証できなくても実害はない