RFC 4033

DNSSEC.jp プロトコル理解SWG

1.Introduction

- DNSSECの導入。
- RFC 4033/4034/4035が1組。
- RFC 2535以前で定義されたセキュリティ拡張を更新/再定義/洗練。
- 拡張は新しいtypeのRRの導入と、既存のプロトコルの改変で実現。
  - 具体的なことは、関連RFCで。

- Section 3,4では、セキュリティ拡張の能力と限界
- Section 5では、ドキュメント群(=4033/4034 /4035)のスコープ
- Section 6～9ではレゾルバ、スタブレゾルバ、ゾーン、ネームサーバに与える影響について論じる。
- DNSSECはoriginの認証とデータの完全性、公開鍵配布の機能がある。
- 秘匿性は提供しない。

2. Definitions of Important DNSSEC Terms

2. Definitions of Important DNSSEC Terms

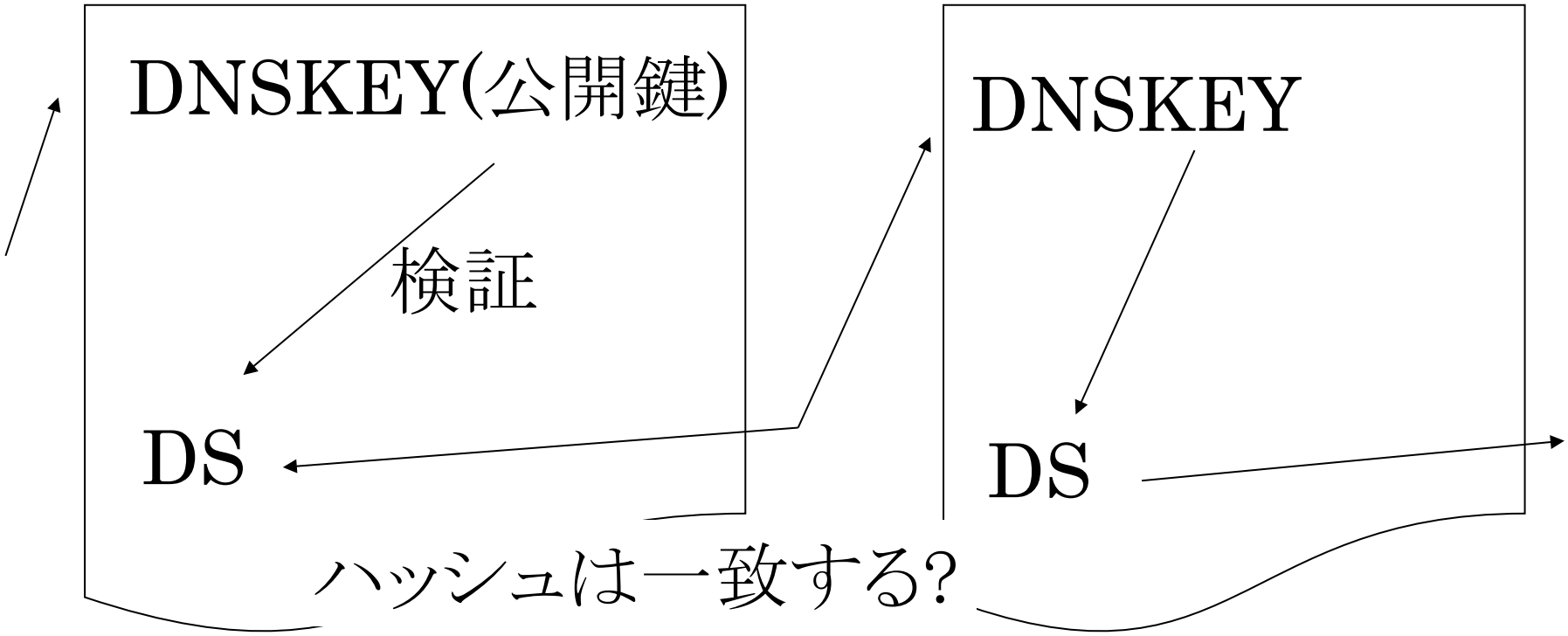
- Authentication Chain
- Authentication Key
- Authoritative RRset
- Delegation Point
- Island of Security
- Key Signing Key(KSK)
- Non-Validating Security-Aware Stub Resolver
- Non-Validating Stub Resolver
- Security-Aware Name Server
- Security-Aware Recursive Name Server
- Security-Aware Resolver
- Security-Aware Stub Resolver

2. Definitions of Important DNSSEC Terms

- Security-Oblivious <anything>
- Signed Zone
- Trust Anchor
- Unsigned Zone
- Validating Security-Aware Stub Resolver
- Validating Stub Resolver
- Zone Apex
- Zone Signing Key (ZSK)

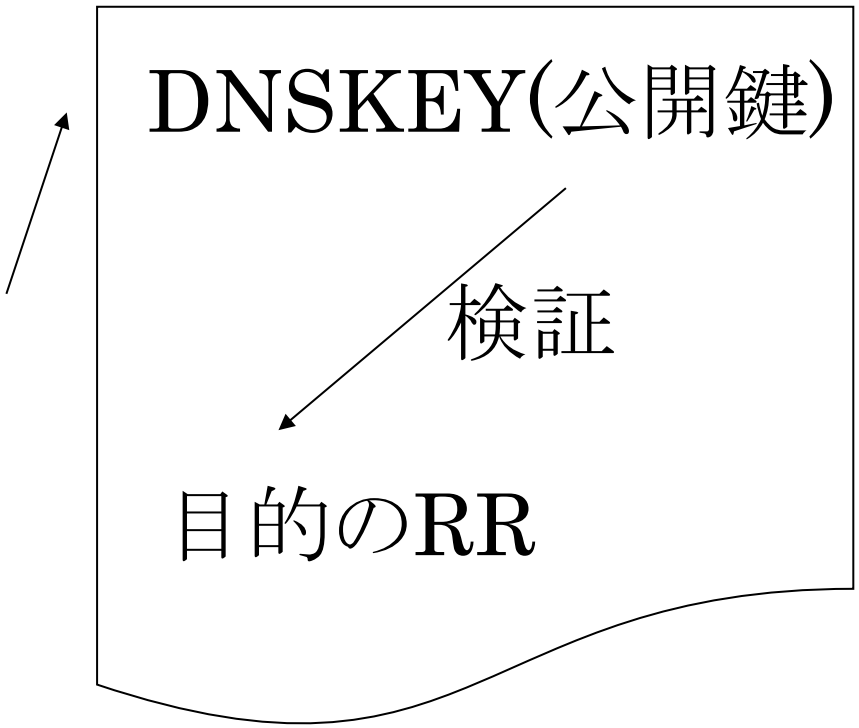
2. Definitions of Important DNSSEC Terms

- Authentication Chain



2. Definitions of Important DNSSEC Terms

- Authentication Chain



- DNSKEYは、RRの署名に使った秘密鍵と対応する公開鍵。
- DSは子供のDNSKEYのハッシュ。
  - DNSKEYのハッシュをとって、親が提示しているDSと一致するかを確認。

2. Definitions of Important DNSSEC Terms

- Authentication Key
  - security-aware resolverが既に検証済みで、データの認証に使うことができる公開鍵。
  - 入手には3つの方法
    - security-aware resolverには、一般に少なくとも1つの公開鍵が設定されている。
      - 公開鍵そのもの
      - DS RRと同様のハッシュ
    - ある公開鍵でDSを検証し、そのDSが指し示すDNSKEY。
    - ある公開鍵の署名が、既検証の別の公開鍵と対応する秘密鍵で署名されているかどうか。
  - ある公開鍵を認証するかどうかは、ローカルポリシにしたがうこと。

2. Definitions of Important DNSSEC Terms

- Authoritative RRset
  - あるRRsetがauthoritativeであるとは、if&only if
    - ownerの名前がzone apex自体かその下位
    - もし独立した子ゾーンがあるなら、それよりは上位
  - 例外を除き、zone apexのRRsetは、親側ではなく子側がauthoritative。
  - 例外はDS、そのDSを指すNSEC、それらの署名のRRSIG。これらは親側がauthoritative。

2. Definitions of Important DNSSEC Terms

```
jp. IN SOA ... (
                ...)
          :
example.jp.   NS   ns.example.jp.
              RRSIG ...
              DS   ...
              RRSIG ...
              NSEC ...
              RRSIG ...
```

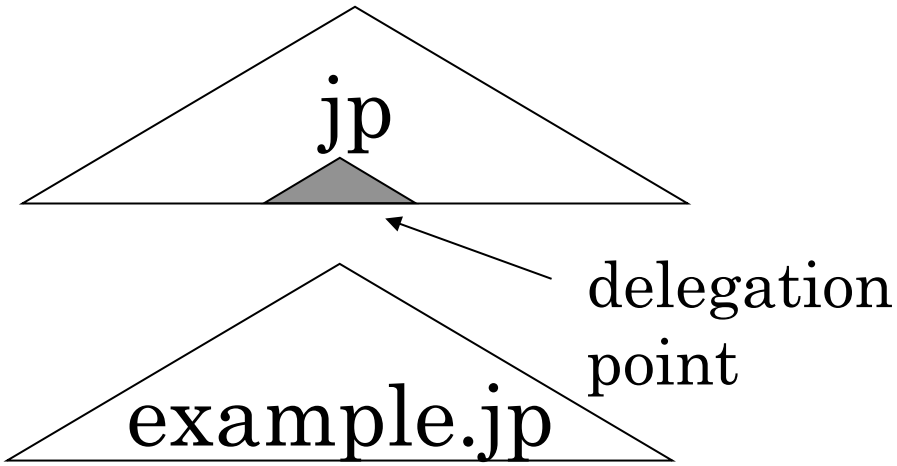
ゾーン外データ

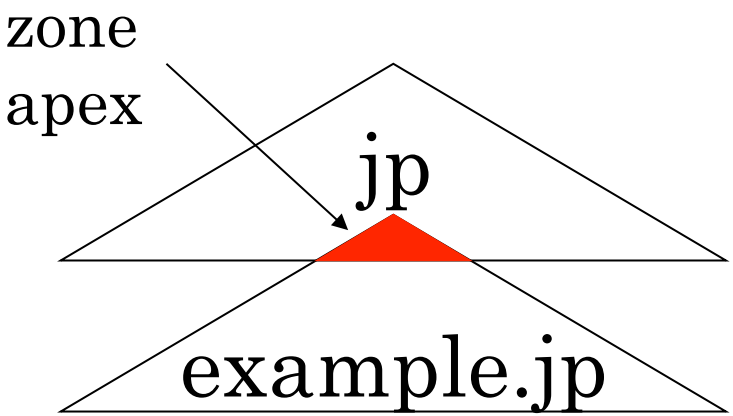
訂正:このNSはゾーン外だからRRSIGはない

authoritative

2. Definitions of Important DNSSEC Terms

- Delegation Point
  - zone cutの親側。
  - zone apexの逆側。





2. Definitions of Important DNSSEC Terms

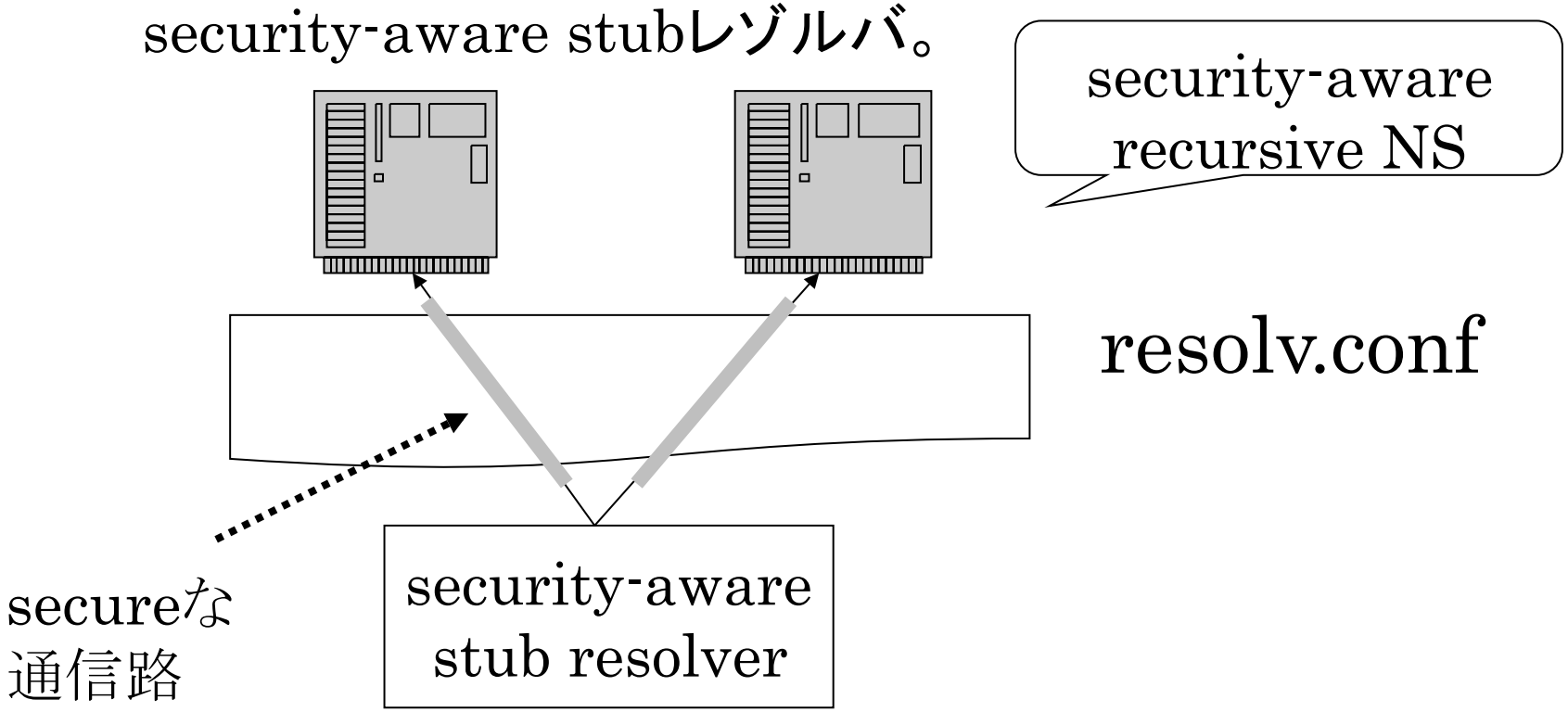
- Island of Security
  - 署名されたゾーン。
  - 親からauthorityの委任を受けている。
  - 親からauthentication chainはつながっていない。
  - DNS以外の方法でauthentication keyを手に入れないと、island of securityが返してきたデータは認証できない。

2. Definitions of Important DNSSEC Terms

- Key Signing Key(KSK)
  - そのゾーン中の、他のauthentication keyに署名するのに使った秘密鍵と対応するauthentication key。
  - 典型的には、対応する秘密鍵でzone signing key (ZSK)に署名する。
  - ZSKは頻繁に交換したいが、そのゾーンのSEPは安定させたいので、KSKは長期間有効にしたい。
  - あるauthentication keyをKSKにするのはオプショナル。
    - 検証のときはKSKと他のauthentication keyを区別しない。
    - 1つの鍵をKSK兼ZSKに使ってもいい。

2. Definitions of Important DNSSEC Terms

- Non-Validating Security Aware Stub Resolver=Non-Validating Stub Resolver
  - security-aware recursive name serverを信頼する security-aware stubレゾルバ。



2. Definitions of Important DNSSEC Terms

- Security-Aware Name Server
  - RFC 4033/4034/4035で定義しているDNSSECを理解するネームサーバ。
  - EDNS0のメッセージサイズ拡張とDO(DNSSEC OK)bitをサポート。
  - DNSSEC関連のRR typeとヘッダのフラグをサポート。
- Security-Aware Recursive Name Server
  - security-aware name serverであり、かつsecurity-aware resolverである物。

2. Definitions of Important DNSSEC Terms

- Security-Aware Resolver
  - RFC 4033/4034/4035で定義するDNSSECを理解する(RFC 1034の意味での)レゾルバ。
    - full resolverかstub resolverかは問わない。
  - EDNS0のメッセージサイズ拡張とDO bit、DNSSECに関するRR typeとヘッダのフラグをサポートする。

2. Definitions of Important DNSSEC Terms

- Security-Aware Stub Resolver
  - RFC 1034のsection 5.3.1で定義されているstubレゾルバ。
  - security-oblivious stubレゾルバにはできないDNSSECのサービスができる。
  - 署名を検証するか否かによってvalidatingかnon-validatingかになる。
  - validatingは、自力で検証するか、security-aware name serverを信頼する。

2. Definitions of Important DNSSEC Terms

- Security-Obliviousほげ
  - security-awareではない、ほげ。
- Signed Zone
  - RRsetに署名され
  - DNSKEYとRRSIG、NSECとオプションでDS RRが正しく構成されているゾーン。

2. Definitions of Important DNSSEC Terms

- Trust Anchor
  - validating security-aware resolverに設定されているDNSKEYかRR、つまりDNSKEYのハッシュ。
  - 署名されているDNSの応答に対してauthentication chainを構築するためのスタート地点として使う。
  - セキュアな、あるいは信頼できる経路で入手しなければならない。
  - trust anchorが設定されていたら、そのゾーンには署名されていると期待すべき。

2. Definitions of Important DNSSEC Terms

- Unsigned Zone
  - 署名されていないゾーン。
- Validating Security-Aware Stub Resolver =Validating Stub Resolver
  - recursiveモードのqueryを出し、
  - 上流のsecurity-aware recursive name serverを無条件に信頼するのではなく、自身で署名を検証する
  - security-aware resolver。

2. Definitions of Important DNSSEC Terms

- Zone Apex
  - zone cutの子供側。
- Zone Signing Key(ZSK)
  - ゾーンに署名するのに使った秘密鍵と対応するauthentication key。
  - 典型的には、そのDNSKEY RRset自体に署名するのに使った秘密鍵と対応するKSKと一緒のDNSKEY RRsetに属する。
  - 用途だけでなく寿命などの点でもKSKとは違う。
  - KSKとZSKを分けるのはオプション。KSKと同じ議論。

3. Service Provided by DNS Security

3. Service Provided by DNS Security

- DNSSECが提供するもの
  - originの認証
  - DNSのデータの完全性の保証
  - 非存在性の認証を伴った提示
- DNSプロトコルの改変が必要
  - RRのtypeを4つ追加
    - RRSIG: Resource Record Signature
    - DNSKEY: DNS Public Key
    - DS: Delegation Signer
    - NSEC: Next Secure

3. Service Provided by DNS Security

- ヘッダのフラグを2bit追加
  - CD: Checking Disable
  - AD: Authenticated Data
- 大きなデータをやりとりするのでEDNS0のサイズ拡張が必須
- EDNSのDO(DNSSEC OK)bitのサポート
  - security-aware resolverがDNSSECのRRを要求するときに、リクエストでそのことを提示するため。

- DNSSECで、RFC 3833で論じられている脅威の大半が防御できる。

3.1. Data Origin Authentication and Data Integrity

- DNSSECは、暗号技術で生成されたディジタル署名とDNSのRRsetとを組み合わせることで認証機能を提供する。
  - RRSIG
- 典型的には、あるゾーンのデータには1つの秘密鍵で署名するが、複数もあり得る。
  - 複数の署名アルゴリズムを使って、それぞれで署名。
- あるゾーンの信頼できる公開鍵があれば、security-aware resolverは、そのゾーンの、署名を施されたデータを認証することができる。

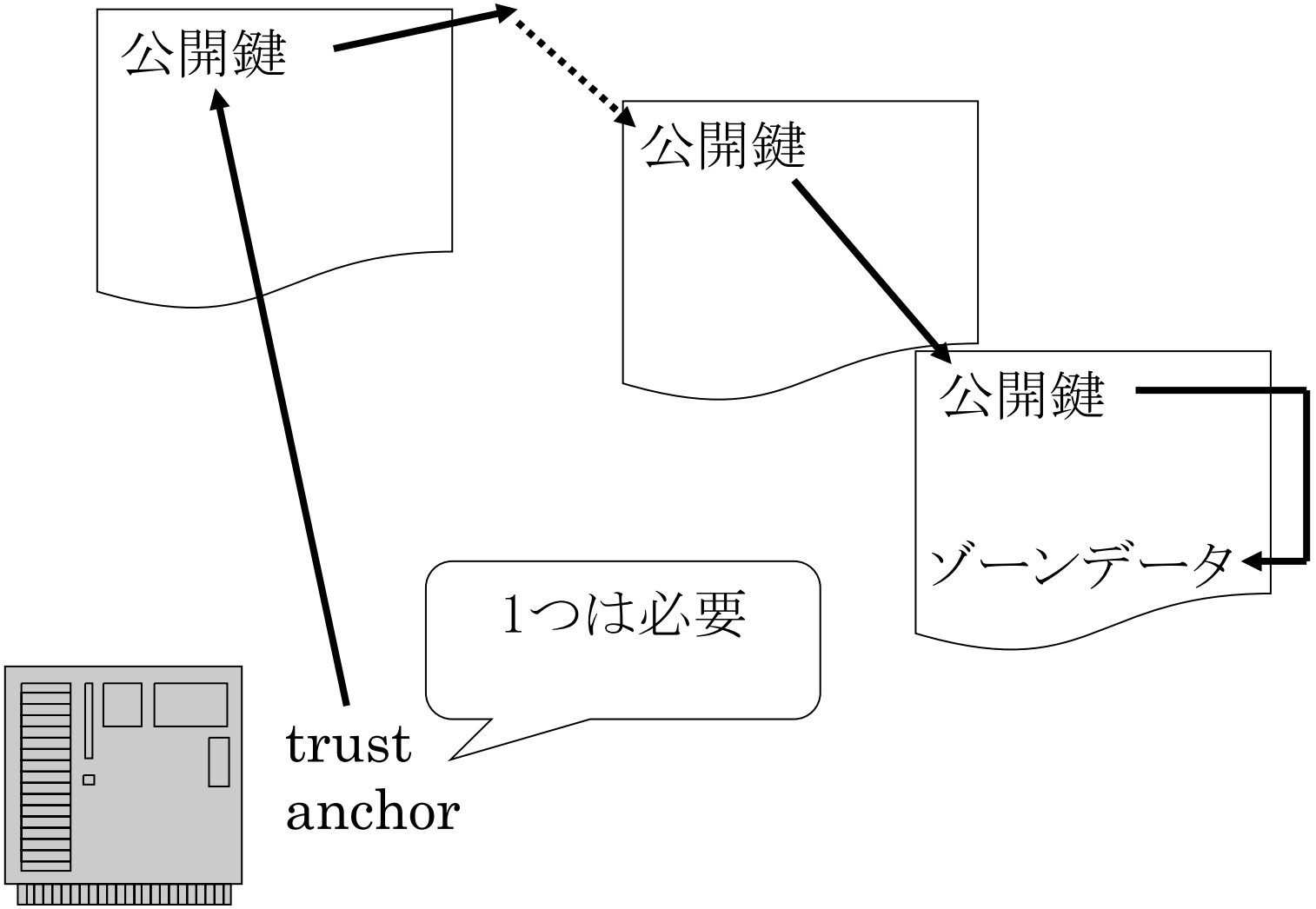
3.1. Data Origin Authentication and Data Integrity

- DNSSECの重要なコンセプトは、ゾーンのデータを署名するのに使った鍵は、そのゾーンを認証するのであって、authoritativeサーバを認証するのではない、という点。
- RFC 2931(SIG(0))で論じられている、トランザクションの認証と混同しないこと。

3.1. Data Origin Authentication and Data Integrity

- security-aware resolverが、あるゾーンの公開鍵を入手する方法。
  - 設定情報の中にあるtrust anchor
  - 通常の名前解決
- 後者を実現するために、公開鍵はDNSKEY RRに保持される。
- 秘密鍵は、ちゃんとヒミツにすること。
- 公開鍵を名前解決により信頼できる手段で入手するには、レゾルバに設定されているauthentication keyか、既に認証済みの、別の鍵で署名されていなければならない。

3.1. Data Origin Authentication and Data Integrity



3.1. Data Origin Authentication and Data Integrity

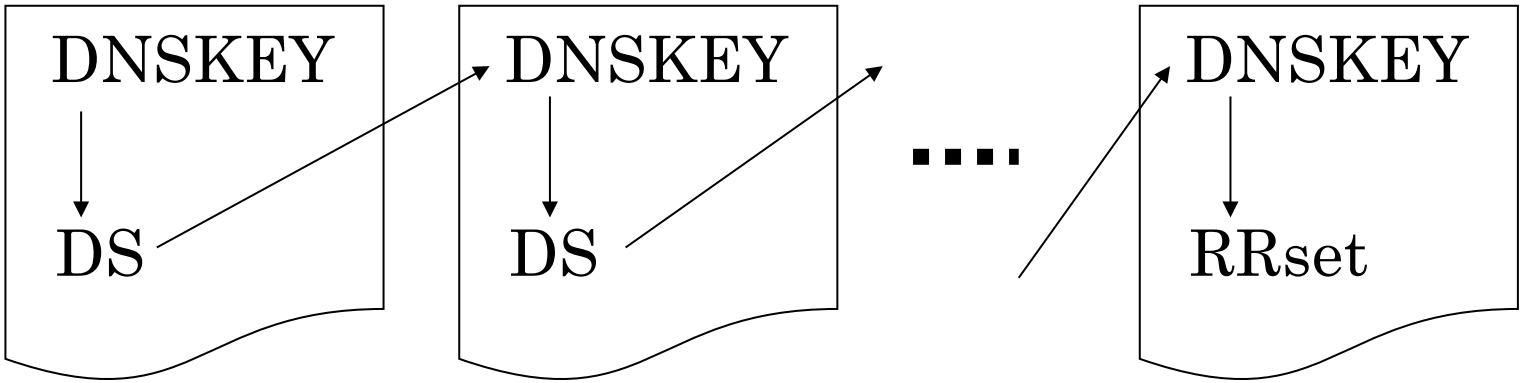
- trust anchor
  - ZSKなら、そのままゾーンデータを認証する。
  - KSKなら、ZSKを認証する。
  - ハッシュなら
    - DNS queryで鍵を入手
    - hash(その鍵)
    - trust anchorと突合せ
- security-aware name serverは、そのゾーンの公開鍵を認証するために必要な署名も鍵自体と一緒に送る。
  - メッセージの大きさに余裕があれば。
  - security-aware resolverがauthentication chainを形成するのを助けるため。

3.1. Data Origin Authentication and Data Integrity

- DS
  - 組織間の委任に対する署名にまつわる管理作業を簡略化する。
  - 親側のdelegation pointに置く。
  - 子側のzone apexにあるDNSKEYに署名するのに使った秘密鍵と対応する公開鍵を指し示す。
    - 発表者注: 一般にはKSKのこと
  - 子側のゾーンの管理者は、ゾーンのデータに署名するのに、このDNSKEYに含まれる公開鍵と対応する秘密鍵を使う。
    - 発表者注: 一般にはZSKのこと
    - DNSKEY RRsetだから、KSKもZSKも含まれている。

3.1. Data Origin Authentication and Data Integrity

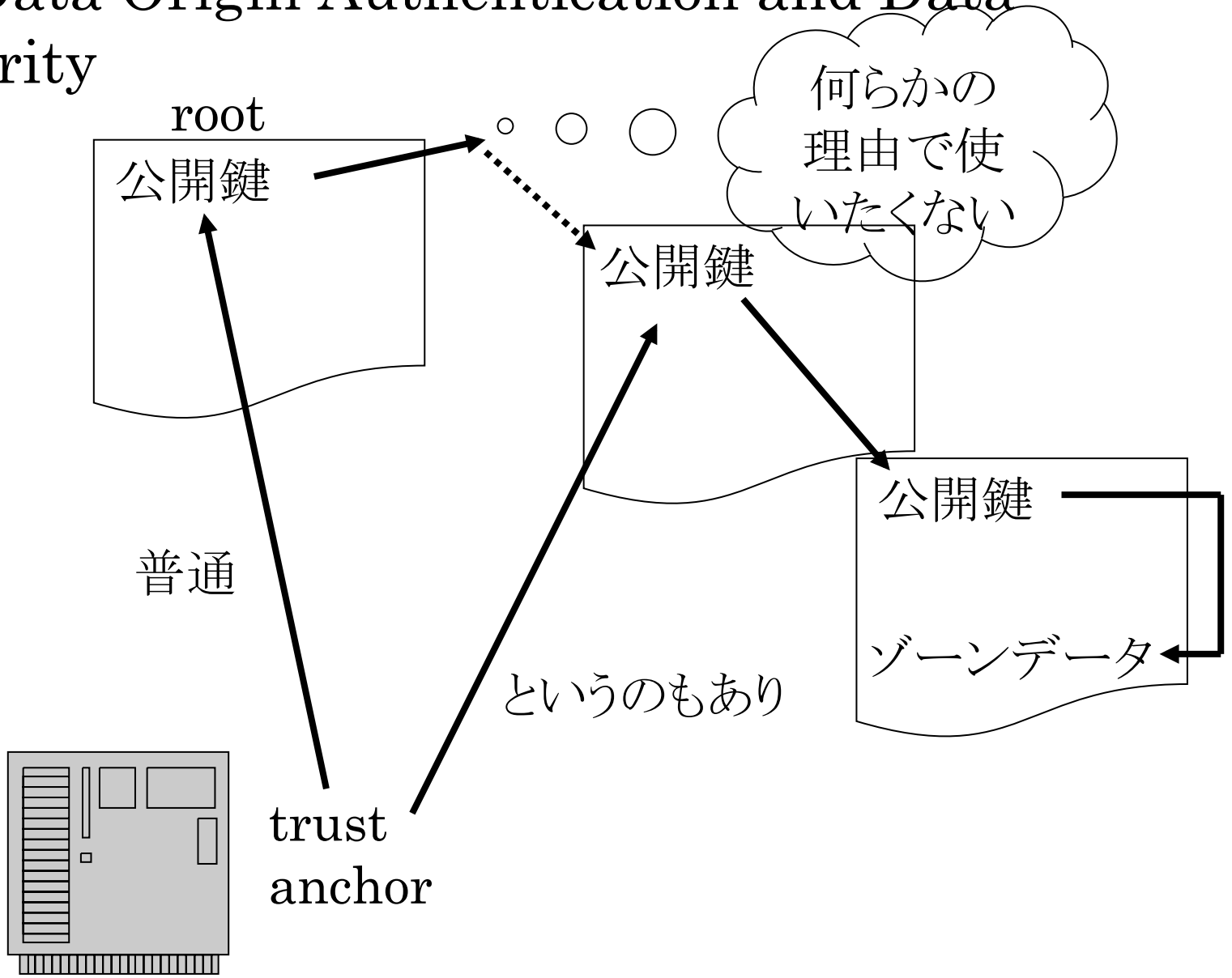
- 典型例



3.1. Data Origin Authentication and Data Integrity

- DNSSEC permits more complex authentication chains, such as additional layers of DNSKEY RRs signing other DNSKEY RRs within a zone.
  - よくわからん…。
  - KSKとZSKの関係のこと??
- 独立したゾーンではなくjpゾーンの中のco.jpというサブドメインに、jpとは別のDNSKEYを定義して…みたいなこと? という議論あり。

3.1. Data Origin Authentication and Data Integrity



3.1. Data Origin Authentication and Data Integrity

- DNSSECは、security-aware resolverが、RRsetに施されている署名がDNSSECの意味するところにおいて”valid”かどうかを判定するための機構を提供する。
- DNSの鍵もデータも、認証するのはローカルのポリシによる。
  - RFC 4033/4034/4035で定義するプロトコル拡張を拡大したり、それより優先されたりし得る。

3.2. Authentication Name and Type Non-Existance

- Section 3.1で説明したセキュリティの機構は、存在するRRsetに対して署名を施す方法でしかない。
- 同レベルの認証と完全性の否定応答を提供する、という課題は、新規に導入するNSECレコードで実現する。
- security-aware resolverは、NSECを使うと他のDNS応答を認証するのと同じ方法で、名前、typeのいずれについても否定応答を認証できる。

3.2. Authenticating Name and Type Non-Existance

- NSECレコードの連鎖
  - そのゾーンに属するドメイン名同士の間の隙間、言い換えれば「空き空間(empty space)」を明示的に表現する。
  - 存在する名前に対して定義されているRRsetのtypeのリストを表現する。
- 各NSECレコードは、Section 3.1で説明した方法で署名され、認証される。

4. Services Not Provided by DNS Security

4. Services Not Provided by DNS Security

- 元来、DNSは
  - 誰に訊かれても同じ答えを返す
  - DNSに載っているデータは全部見える

  ことを仮定して設計された。
- というわけで、DNSSECは
  - 秘匿性
  - access control listやその他問い合わせ毎に相違を持たせる

  機能を提供するようには設計されていない。

4. Services Not Provided by DNS Security

- DNSSECはDoSアタックに対する防御は提供しない。
- security-aware resolverとsecurity-aware name serverは、暗号化技術に起因する、新たな種類の攻撃に対して脆弱になるかもしれない。

4. Services Not Provided by DNS Security

- DNSSECはデータと、そのデータの出所の認証を提供する。
- ここまでで説明した機構は、ゾーン転送やダイナミックアップデートのような操作を保護するようには設計されていない。
- TSIG(RFC 2845)やSIG(0)(RFC 2931)が、それらを保護する。

5. Scope of DNSSEC Document Set and Last Hop Issue

5. Scope of the DNSSEC Document Set and Last Hop Issue

- RFC 4033/4043/4035は、バリデータがデータの状態を明確に判定できるようにするための、ゾーン署名者やsecurity-awareなネームサーバやレゾルバの挙動を規定している。
- validating resolverは
  - Secure
  - Insecure
  - Bogus
  - Indeterminate

  の4種類の状態を判定できる。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- Secure
  - validatorは
    - trust anchorを保持している。
    - 信頼の連鎖を持っている。
    - 応答に含まれているすべての署名が検証できた。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- Insecure
  - validatorは
    - trust anchorを保持している。
    - 信頼の連鎖を持っている。
    - どこかのdelegation pointにDSが存在しないことを署名付きで確認した。
  - このことは、ツリーのそれ以下の部分がinsecureかもしれないことを示している。
  - validating resolverは、ドメイン空間の一部がinsecureである、とするローカルポリシを持ってもよい。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- Bogus
  - validating resolverは
    - trust anchorを保持している。
    - 下位のデータに署名されていることを示すセキュアな委任がある。
    - 何らかの理由で応答の検証に失敗した。
      - 署名に誤りがある、とか
      - 署名の有効期限が切れている、とか
      - サポートしていないアルゴリズムで署名されている、とか
      - NSECによれば存在することになっているはずるデータがない、とか。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- Indeterminate
  - ツリーの中の目的の部分がセキュアであることを示すtrust anchorがない。
  - これがデフォルトの動作モード。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- この仕様では、データがbogusであることが判明したときに、security-aware name serverがnon-validating stub resolverに、そのことを通知するための方法だけを定義する。
  - RCODE=2, Server Failureによる。
- データがセキュアであることが判明したときに、security-aware name serverがsecurity-aware stub resolverに、そのことを通知するにはAD bitを使う。

5. Scope of the DNSSEC Document Set and Last Hop Issue

- この仕様では、bogusだったりinsecureだったときに、その理由を通知するフォーマットは規定していない。
- 現行の通知機構では、indeterminateとinsecureの区別はつかない。
  - 将来の課題
- でも、そこが足りないことは、ゾーンに対する署名や、bogusなデータの伝播を阻止するsecurity aware recursive name serverの普及を妨げるわけではない。

6. Resolver Considerations

6. Resolver Considerations

- security-aware resolverは、ディジタル署名を検証するために、少なくともmandatory-to-implementのアルゴリズムで暗号化できなければならない。
- security-awareレゾルバは、新たに得られたゾーンからauthentication keyへさかのぼるauthentication chainを形成できなければならない。

6. Resolver Considerations

- 途中で、必要なDNSKEY、DS、RRSIGを取得するために、中間のゾーンへのqueryが追加で発生するだろう。
- security-aware resolverには、authentication chainを形成するときの起点として、trust anchorを、少なくとも1つ設定しなければならない。

6. Resolver Considerations

- もし
  - security-aware resolverが、問い合わせ相手のauthoritativeサーバとは別。
  - 間にrecursiveサーバとか、何らかのDNS proxyが入っている。
  - その中間デバイスがsecurity-awareではない。

だと、security-aware resolverはセキュアモードでは動作できない。

6. Resolver Considerations

- 例えば
  - security-aware resolverがNAT経由でつながっている
  - NAT箱にsecurity-awareではないDNS proxyが　載っている
- security-aware resolverは署名されたDNSデータを得たり検証したりすることが困難だったり不可能だったりする。
- DSはzone cutでのownershipが普通と違うので、難しい。
  - これはNAT固有の問題ではないのに注意。

6. Resolver Considerations

- もし、security-aware resolverがunsigned zoneとかsecurity awareじゃないネームサーバに依存しなきゃならないと、レゾルバは応答を検証できない。
- 検証できていない応答を受け入れるかどうかのローカルポリシの策定が必要。

6. Resolver Considerations

- security-aware resolverは、署名の有効期限を越えてデータをキャッシュしてしまわないように、データをキャッシュするときのTTLを決めるときには署名の有効期限を考慮に入れるべきである。
- security-aware resolver自身の時計が狂っている可能性も考慮すべき。
- security-aware resolverの一部であるsecurity-aware recursiveサーバはchecking disable(CD) bitに注意を払わなければいけない。
  - 正当な署名が、このrecursiveサーバのクライアントであるsecurity-aware resolverに到達するのを妨げないため。

7. Stub Resolver Considerations

7. Stub Resolver Considerations

- ほとんどのDNS queryはstubレゾルバから出てくる。
  - プロトコル上の要請ではないが。
- stubレゾルバ
  - recursive queryモードを使って、処理の大部分をrecursive サーバに負担させる、最小限のレゾルバ。
- DNSSECのアーキテクチャにstubレゾルバは無視し得ない。
- セキュリティについての要請は、反復レゾルバに対する物とは異なる。

7. Stub Resolver Considerations

- security-awareなrecursiveサーバを使っていれば、security-obliviousなstubレゾルバでもDNSSECの恩恵に与ることはできる。
- stubレゾルバが、DNSSECが提供する信頼性を本当に享受するためには、問い合わせ相手のrecursiveサーバと、そことの間の通信路の両方が信頼できなければならない。

7. Stub Resolver Considerations

- ローカルポリシの問題
  - security-oblivious stub resolverは、自分では検証できないので、リカーシブサーバの配下となるしか選択肢はないことが要点。
- 通信路の問題
  - SIG(0)とかTSIGとかの、DNSトランザクションを認証する機構を正しく使う。
  - IPsec
  - OS依存のプロセス間通信、とか。
  - 秘匿性は不要。完全性とメッセージの認証は必要。

7. Stub Resolver Considerations

- security-aware stub resolver
  - recursiveサーバと、そこへの通信路が共に信頼できる。

  →応答のメッセージヘッダのAuthenticated Data(AD) bitを評価する選択肢が得られる。
    - recursiveサーバが、AnswerセクションとAuthorityセクションに含まれるすべてのデータが検証できたかどうかの手がかりとして使える。
  - 何らかの理由でrecursiveサーバが信頼できないなら、問い合わせのChecking Disable(CD) bitを立てて、検証は自分でやる方法もある。

8. Zone Considerations

8. Zone Considerations

- signed zoneとunsigned zoneの違い
  - セキュリティ関連のRRが含まれる
    - RRSIG/DNSKEY/DS/NSEC
  - RRSIGとNSECは、サービス投入前の署名工程で生成される。
  - RRSIGレコードには、署名とその署名が担保するデータについての検証の有効期間の始点と末尾の時刻が含まれている。

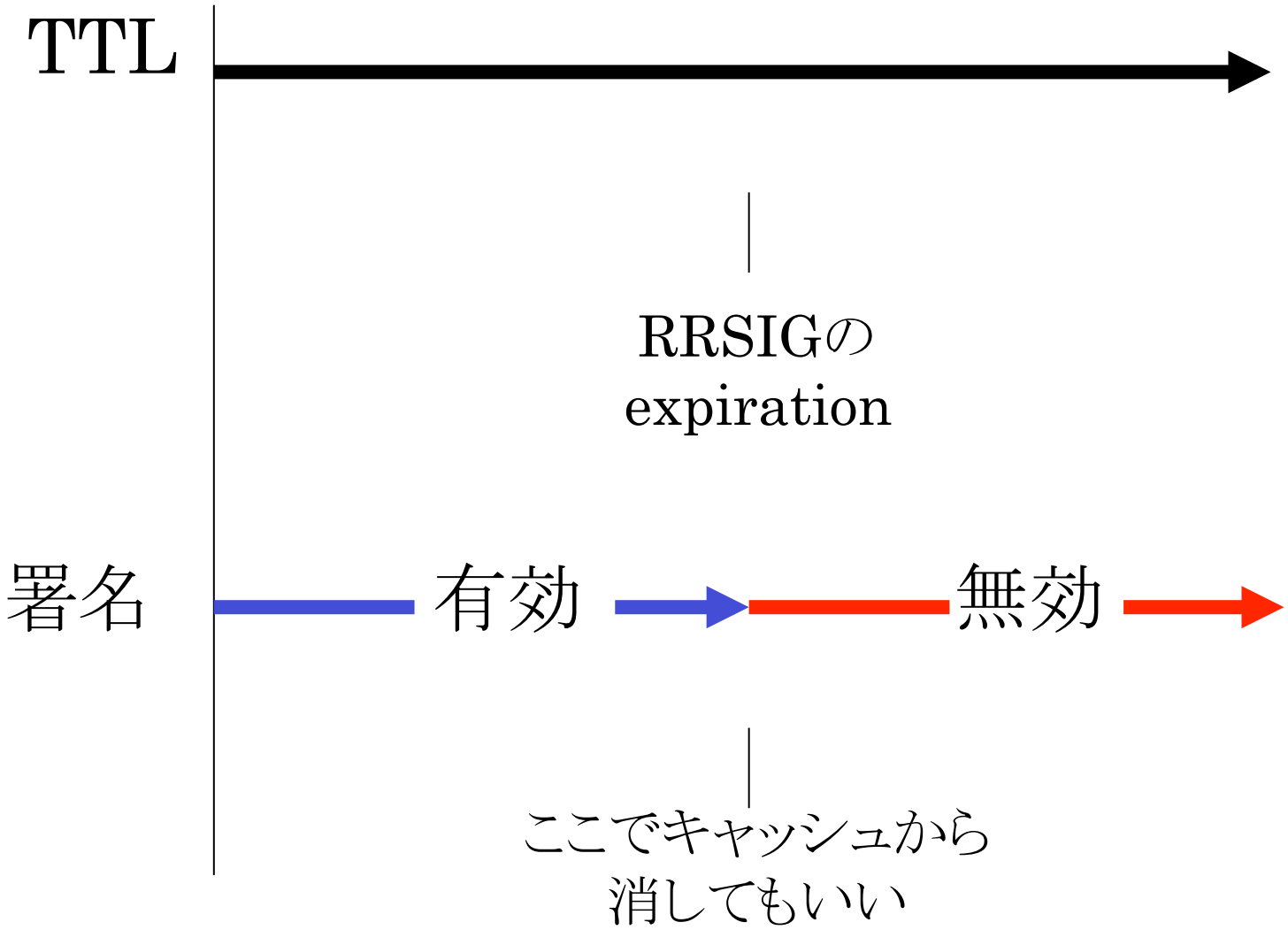
8.1. TTL Values vs. RRSIG Validity Period

- RRsetのTTLと、そのRRsetに対するRRSIGの署名の有効期限とを区別することが重要。
- DNSSECはTTLの意味を変えていない。
- キャッシュするレゾルバは、security-awareかどうかに関係なく、RRsetのTTLフィールドに指定されている期限までにキャッシュからRRsetを消さなければいけない。

8.1. TTL Values vs. RRSIG Validity Period

- RRSIGのinceptionとexpirationのフィールドは、対象のRRsetに対する署名の有効期間を示す。
- ゾーンデータに対する署名は、それらのフィールドに示されている期間だけ有効。
- TTLはレゾルバのキャッシュ上で署名されたRRsetの有効期間を延ばすことはできない。
- RRsetとそれへの署名の有効期間の末尾をTTLの上限にしてもよい。

8.1. TTL Values vs. RRSIG Validity Period



8.2. New Temporal Dependency Issues for Zones

- signed zoneに含まれる情報は、元来DNSプロトコルにはなかった依存関係がある。
- ゾーン中の各RRsetは、その時点で有効なRRSIGがあることを担保するため、定期的なメンテナンスが必要。
- RRSIGの有効期間は、それぞれの署名付きRRsetの有効期間であって、別のRRsetは別のタイミングでexpireする。

8.2. New Temporal Dependency Issues for Zone

・どれかのRRsetに再署名

→RRSIGに変化が生じる

→そのゾーンのSOAのserialを増やさなきゃいけない

- ゾーンデータが変化したことを示す
- SOA自体にも再署名が発生

→DNS NOTIFYメッセージを送出

→ゾーン転送が発生

9. Name Server Considerations

9. Name Server Considerations

- security-aware name serverは、DO bitを立てて要求を提示してきたレゾルバからの問い合わせに対しては、メッセージサイズが許す限り、すべての応答に適切なDNSSECのRRを含めるべき。
  - RRSIG, DNSKEY, DS, NSEC
- DNSSECのRRを応答に含めると、UDPではtruncationが簡単に起きてTCPにfallbackしてしまうので、security-aware name serverは、EDNSの”sender’s UDP payload”機構のサポートが必須である。

9. Name Server Considerations

- できることなら、秘密鍵はofflineでヒミツに保管すべきである。
- でも、dynamic updateを有効にしているゾーンについては、そうはできない。
- updateされたら、そのゾーンは再署名しなければいけないので、秘密鍵はonlineじゃなきゃいけない。
- これはZSKとKSKとを分離するのが役立つ例の1つ。
- KSKはofflineで大丈夫なので、ZSKより有効期間を長く設定できる。
  - （発表者注: updateされたとき再署名に必要なのはZSKだけ）

9. Name Server Considerations

- DNSSEC自体はゾーン転送の処理中のゾーンの完全性に対する保護は、十分ではない。
  - signed zoneであっても、子供のゾーンがあると、署名されていないnon authoritativeなデータが含まれる。
- ゾーンメンテナンス処理は、他の機構が必要。
  - ありがちなのは、TSIGとかSIG(0)とかIPsecとかのchannel security。

10. DNS Security Document Family

10. DNS Security Document Family

- The DNSSEC document setは、DNS base protocol documentsという大枠の中で、いくつかのグループに分類される。
  - DNSSEC protocol document set
  - Digital Signature Algorithm Specification
  - Transaction Authentication Protocol
  - New Security Uses

10. DNS Security Document Family

- DNSSECのコア部分
  - DNSセキュリティの導入と要求(RFC 4033)
  - DNSセキュリティ拡張のためのRR(RFC 4034)
  - DNSセキュリティ拡張のためのプロトコルの改変(RFC 4035)
  - DNSセキュリティ拡張に関して追加や変更するドキュメント
    - security-aware stub resolverと上流のsecurity-aware recursive name serverとの間の通信などの、将来の課題も含む。

10. DNS Security Document Family

- ディジタル署名アルゴリズムの仕様
  - ディジタル署名のアルゴリズムをDNSSECのRR フォーマットにどうやって実装するか。
  - それぞれのドキュメントは、個別のディジタル署名アルゴリズムを取り扱う。
  - RFC 4034の付録”DNSSEC Algorithm and Digest Types”参照

10. DNS Security Document Family

- Transaction Authentication Protocol
  - 秘密鍵の生成や検証など、DNSメッセージの認証について。
  - DNSSECの仕様の核心ではないが、DNSSECと関連している。

10. DNS Security Document Family

- New Security Uses
  - DNSSECを他のセキュリティ関連分野に適用するためのドキュメント
  - 証明書をDNSで保管/配布する提案であるRFC 2538 (Storing Certificates in the Domain Name System(DNS))など

11. IANA Considerations

略

12. Security Considerations

12. Security Considerations

- このドキュメント(RFC 4033)は、DNSSECの導入であり、新たなセキュリティ関連のRRとDNSプロトコルへの改変に関するドキュメントについても言及している。
- この拡張は、RRsetにディジタル署名を適用することによって、データの出所の認証とデータの完全性を提供する。
- このセクションでは、これらの拡張の限界について論じる。

12. Security Considerations

- security-aware resolverがDNSの応答を検証できるためには
  - 信頼のスタート地点から目的の応答が含まれているゾーンまでの途中のゾーンが全部署名されていること
  - 名前解決に関与するすべてのネームサーバとレゾルバがsecurity-awareであること

  が必要。

12. Security Considerations

- security-aware resolverには
  - unsigned zoneの情報を根拠とする応答
  - security-aware name serverが提供していないゾーンが出所の応答
  - security-awareではないrecursiveサーバを経由してしか得られない、あらゆるデータ

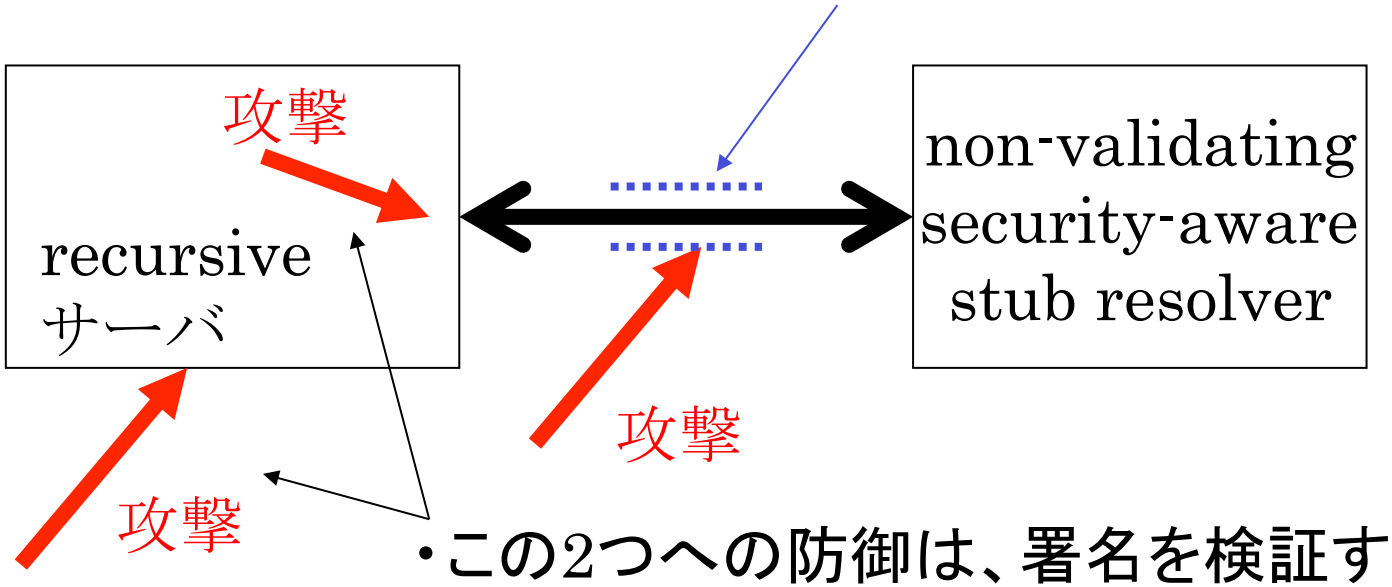
  を検証することはできない。
- 必要なauthentication keyが得られなかったり検証できなかったり、のような理由でauthentication chainに途切れがあると、security-aware resolverは、該当するデータを検証できない。

12. Security Considerations

- このドキュメントでは、IPsec、TSIG、SIG(0)などによりセキュアである通信路を使うなど、さらにセキュリティを向上させる方法についても論じたが、トランザクションのセキュリティは、DNSSECの範囲外である。

12. Security Considerations

- non-validating security-aware stub resolver
  - 署名は検証しない(っていう定義だから)
  - 下の攻撃に対して脆弱
  - 通信路はchannel securityで守るべき



・この2つへの防御は、署名を検証すること。
・定義と矛盾

12. Security Considerations

- DNSSECはDoSアタックへの保護にはならない。
- DNSSECは、security-aware resolverとsecurity-aware name serverに、暗号化技術に起因する新たな種類の脅威をもたらすかもしれない。
  - 例えば、DNSSECの機構を使って、被害者のリソースを使い果たさせる、とか。

12. Security Considerations

- その手の攻撃には、少なくとも2つの形態が想定される。
  - 応答に含まれるRRSIGを細工したり、無駄に複雑な署名の連鎖を含む応答をでっち上げたりして、security-aware resolverのリソースを使い果たさせる。
  - dynamic update対応のsecurity-aware name serverにupdateメッセージを連続して送りつけ、過剰な頻度の再署名を引き起こさせる。

12. Security Considerations

- 設計に際する選択として、DNSSECは秘匿性は提供しない。

12. Security Considerations

- DNSSECでは、NSECの連鎖をたどることによって、ゾーンに登場するすべての名前を列挙することができるようになってしまった。
  - （発表者注: NSEC3(RFC 5155)が、対策の提案）
- NSECは、ゾーンの中に存在する全部の名前を正規化した順序でリンクすることによって、そのゾーンの中に存在しない名前をあきらかにする。
- 攻撃者は、NSECを順に索いていくと、そのゾーンの中の全部の名前が手に入る。
  - （発表者注: RFC 5155では”zone enumeration”と呼んでいる）

12. Security Considerations

- それはDNS自体への攻撃ではないが、攻撃者がネットワーク上のホストやその他のリソースをmapできるようになってしまう。

- DNSSECはDNSに複雑さをもたらした。
  - 実装のバグやゾーンの設定不良が増えるだろう。
  - レゾルバで署名の検証を有効にすると、DNSSECがらみの設定ミスやバグで、正しいゾーンがまるごとunreachになることもあろう。

12. Security Considerations

- DNSSECはunsigned zoneのデータへの改ざんに対しては防御しない。
- zone cutにおけるnon-authoritativeデータは署名されない。
  - 親側ゾーンのglueとNS
  - authentication chainの検証には影響しない。
  - non-authoritativeデータその物は、ゾーン転送の処理中に、改ざんされ得る。

12. Security Considerations

- DNSSECはデータの出所の認証とRRsetの完全性は担保するが、ゾーンの完全性は担保しない。
  - ゾーン転送の処理を保護するためには、TSIG、SIG(0)、IPsecのような、他の機構を使わなければならない。

- さらなるsecurity considerationsについては、RFC 4034とRFC 4035を参照されたい。

13. Acknowledgements
14. References
Author's Addresses/Full Copyright Statement /Intellectual Property/ Acknowledgement

略