Hosting-PRO セッション W1

動きだしたDNSSEC

株式会社ブロードバンドタワー
事業開発グループ
エキスパート
大本　貴

自己紹介

- 2000年　インターネット総合研究所(IRI)に入社
- 2001年　プロデュースオンデマンド(PoD)に出向
  - ストリーミング配信技術担当
- 2007年　インターネット総合研究所に復帰
  - 主に社内システムのサーバ運用、コンサルなど。
  - 2010年春からDNSSEC.jpに参加
- 2010年　ブロードバンドタワーに転籍

DNSSEC.jpでは、海外の動向調査とかを主に。
いろいろtaxiJPNというのでつぶやいてます・・・。

本日のAgenda

- DNSのおさらい
- DNSSECの技術概要
  - 権威DNSサーバ
  - リカーシブサーバ(リゾルバ・キャッシュサーバ)
- 海外・国内事業者などのDNSSECへの対応動向
- ホスティングとDNSSEC
- まとめ

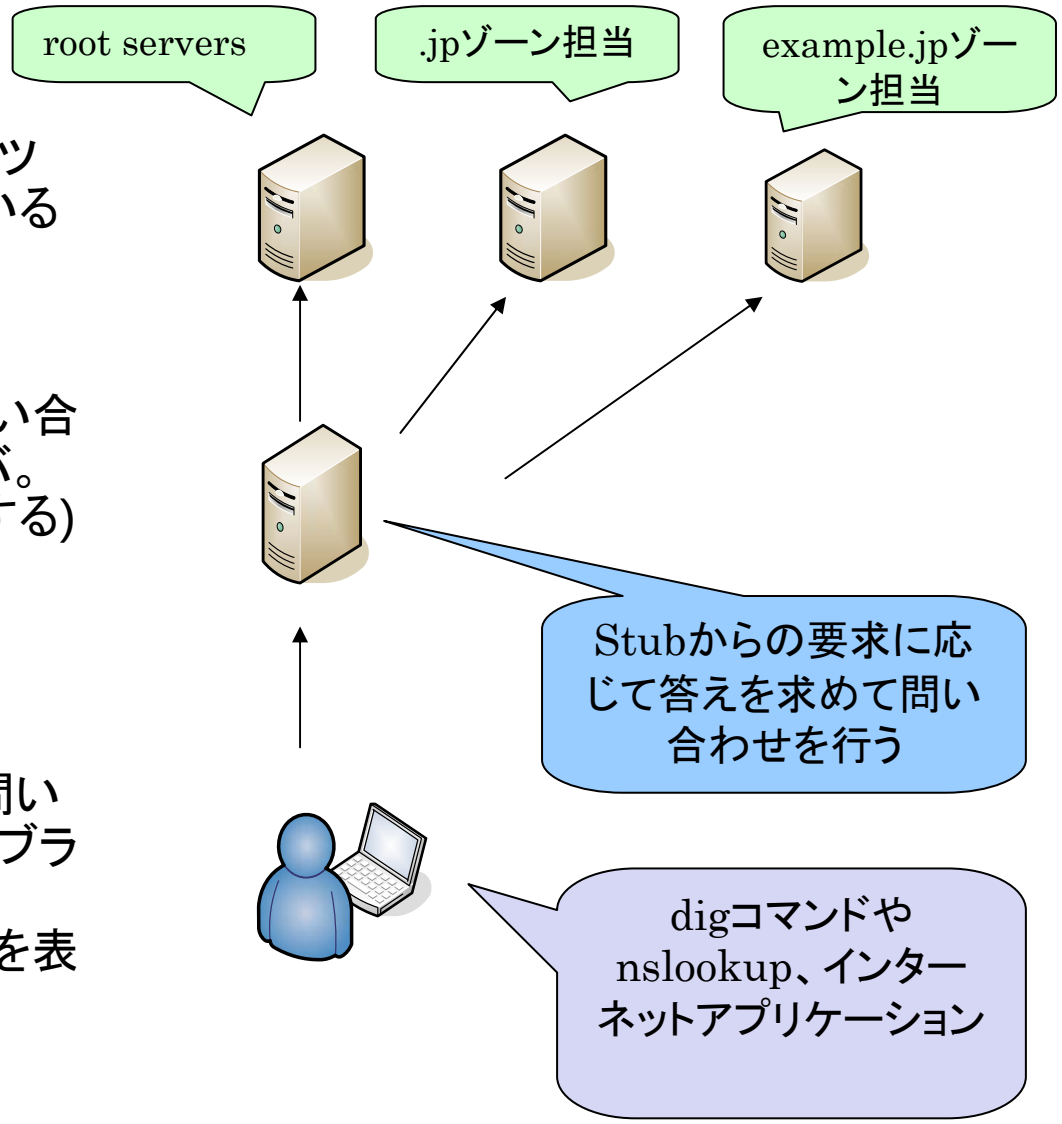
- DNSSEC、その前に。

DNS(Domain Name System)について簡潔な用語定義

- Zone ・・・ ゾーン。名前解決の対象となるデータの集まり。
- RR ・・・ リソースレコード。
  ゾーンファイルに登録されたデータ資源。
- Query ・・・ クエリ。owner(ホスト名やIP address)を
  keyにして RRを索くということ。
- Authority ・・・ 権威。コンテンツ(名前空間)について管理
- Delegation ・・・ 権限委譲。コンテンツ(名前空間)の
  一部の管理を下位サーバに委譲すること。
- Recursive query ・・・ 再帰検索。(後ほど説明)

DNSサーバ色々

- authoritative server
  - 権威DNSサーバ(コンテンツサーバ)。ゾーン管理している
- recursive server
  - リクエストに応じて再帰問い合わせを行うリゾルバサーバ。(キャッシュサーバも兼務する)
- stub resolver
  - リカーシブサーバに再帰問い合わせを行うリゾルバライブラリ。基本的にはリカーシブサーバから得た回答内容を表示するだけ。



- DNSSEC(DNS Security Extensions) の技術概要

そもそもなんでDNSSECが必要?

・毒入れアタック(ポイゾニング)

問い合わせ情報に対して第三者が偽装パケットにより偽のレコードをユーザに送りつける

→結果

ウィルス仕込み済みwebサイトへ誘導。
メールを正しい相手に送信できない。

(しかもエンドユーザは気が付きにくい。)

- インターネットの基盤であるDNSの信頼性が揺らいでいる。→何を信じればよいのか。

フィッシング(phishing)サイトかどうか見抜けますか?

- フィッシングサイトかどうかの判断手法の一つはURLを見ること

URLを見ると、正しくアクセス
しているように表示されていたら?

何が主たる原因か?

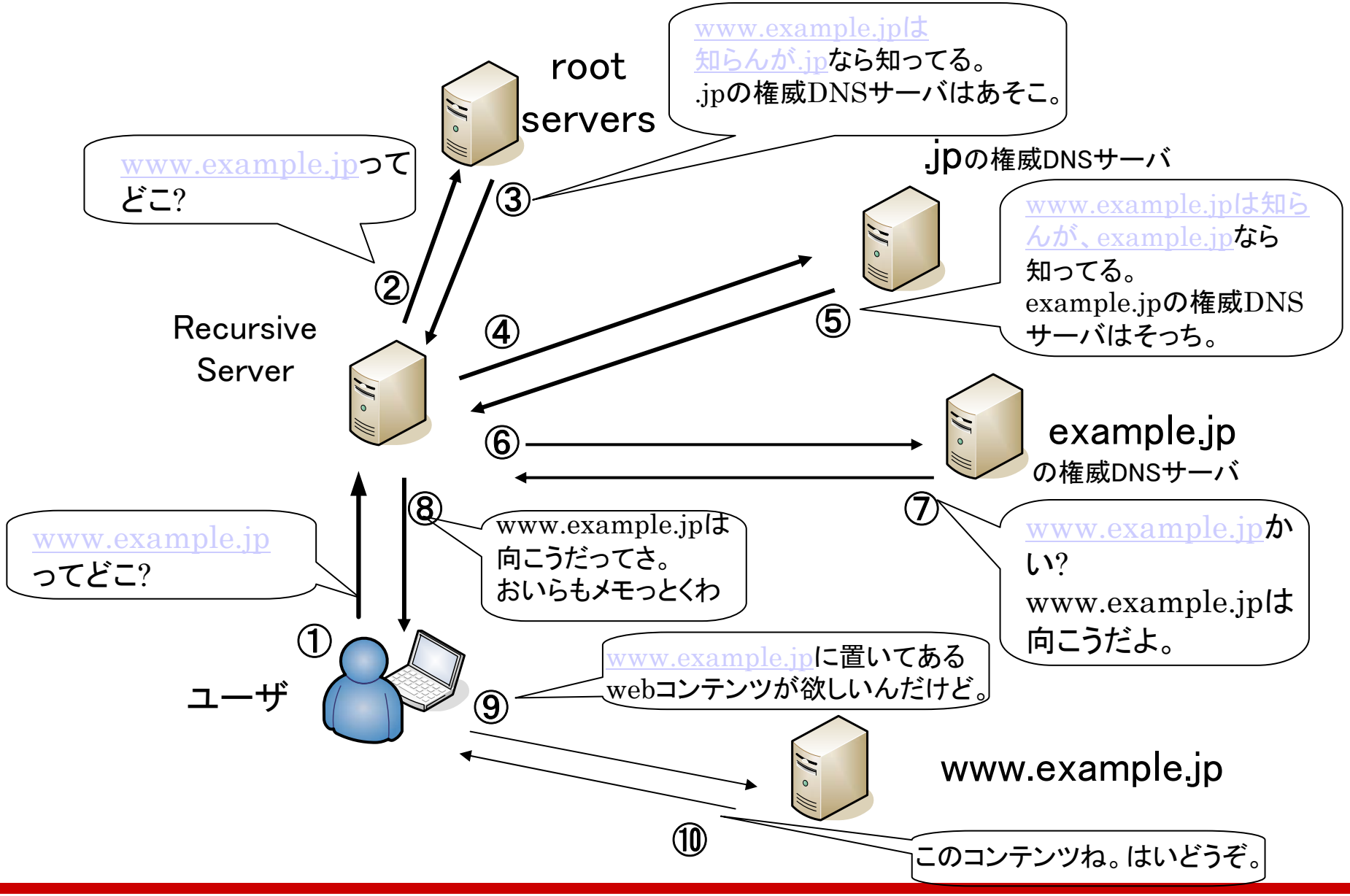
クエリの送受信をUDPでやりとりしているから。

→UDPでサイズ超過したらTCP fallbackで対応

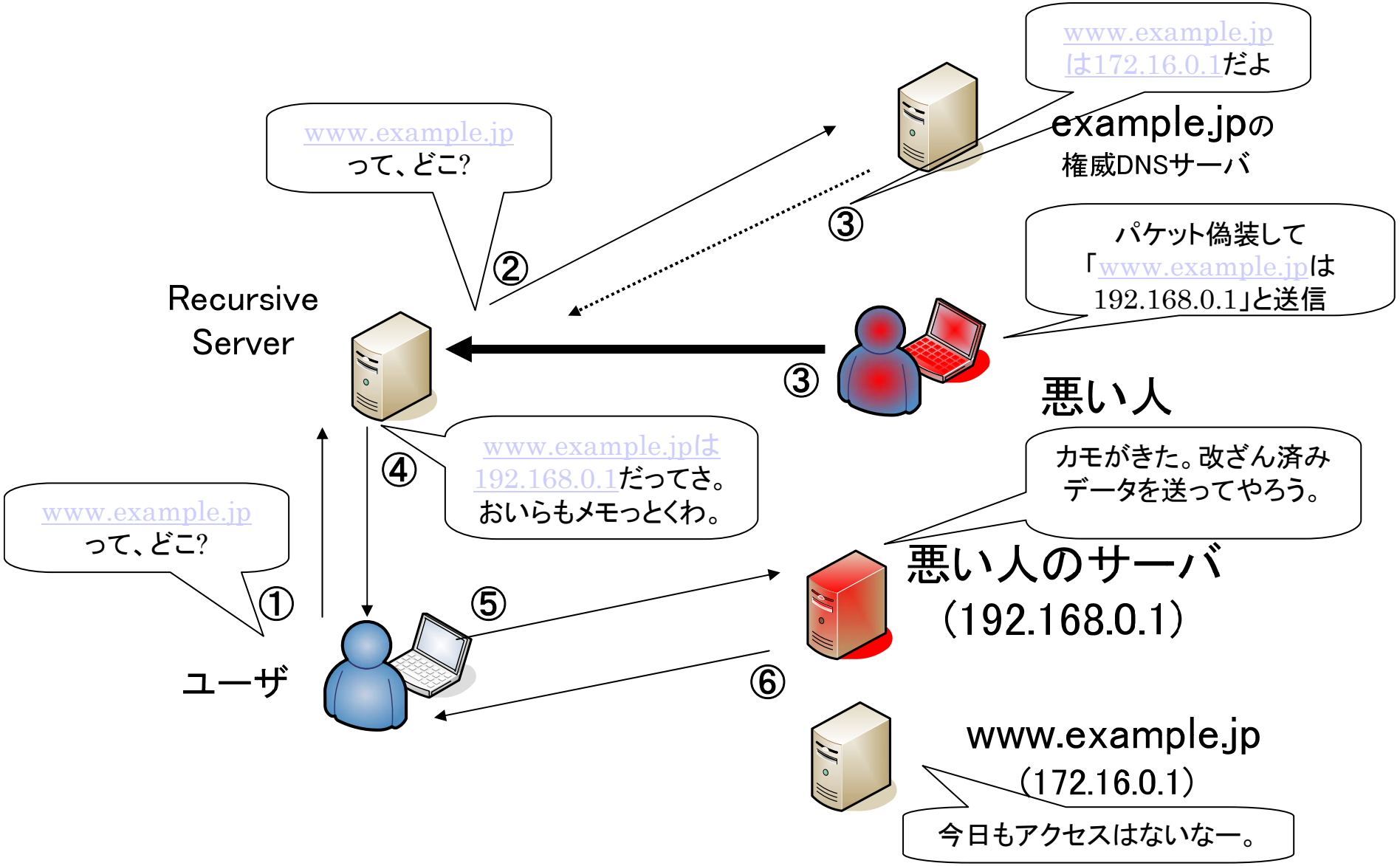
→そもそも最初からTCPで良いのでは?

→ルートゾーンなどで膨大なリクエストを短時間で処理するためにはUDPで処理を軽くしていく必要がある。

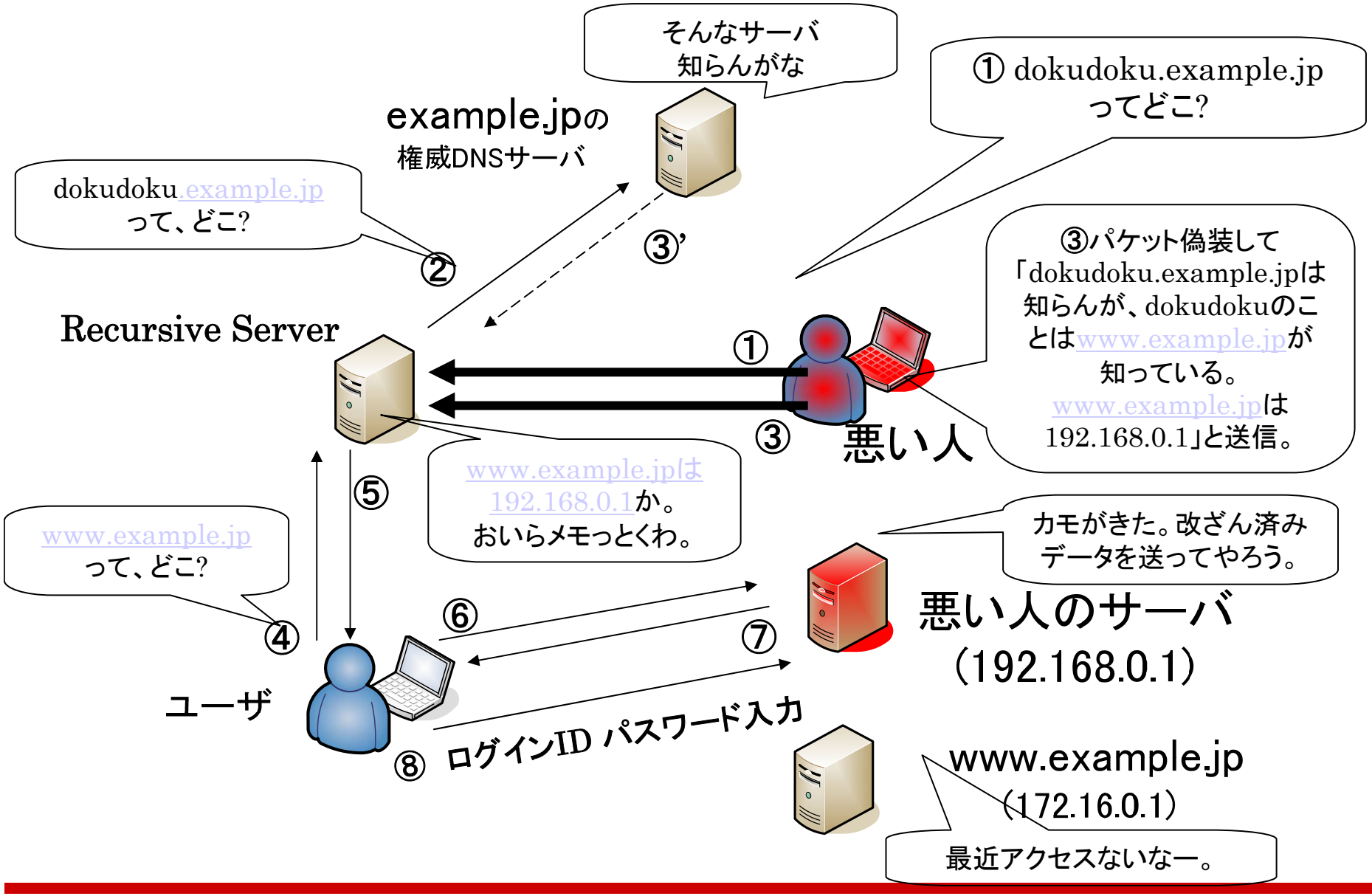
DNSの名前解決の流れ



キャッシュポイゾニングの概要



カミンスキーアタックの概要



DNSSEC、簡単にするとこんなイメージ?

DNSSEC なし

DNSSEC あり

・DNSSEC、誰に負担があるの？

- ドメイン名登録者(独自ドメイン取得している・したい人)
  - DNSSEC化への判断。
    (自分の管理しているドメインの信頼性。
    上位ゾーンが対応していないならDLV使うか)

- DNSサーバ管理者(ISP、ホスティング事業者 etc.)
  - 権威DNSサーバ
    - 管理しているゾーンのDNSSEC対応、
      鍵の定期的なロールオーバなどが業務に追加。
  - リカーシブサーバ(キャッシュDNSサーバ)
    - リカーシブサーバへトラストアンカーの導入。

- レジストラ
  - 鍵を上位ゾーンへ登録する仲介処理。
  - ドメイン契約の移転処理

- レジストリ
  - 下位ゾーンからの登録申請に対してDS登録処理。
    DS申請を受け付けるシステムの構築。

- ユーザサポート担当者
  - 障害時の切り分けのためのノウハウ習得。

DNSSEC、導入するとどうなるの?

- 勝ち得るもの

DNSの信頼性を高めることができる。真正性を担保できる。

- 試練

めんどくさい。(作業が増える)

- 鍵のロールオーバーとか鍵の管理とか再署名とか。
- 信頼の連鎖を形成するための第三者との連携。

管理コストの増加

- 作業自体の単純増加、チェックするポイントの増加。
  ゾーンが多いと署名処理も時間がかかる。

ハイスペックなハードの必要性(特にキャッシュサーバの)

- 署名の検証処理が加わることで必要スペックも増加。

SERVFAILによるトラブルへの懸念(運用リスク)

- 設定ミスなどで、検証に失敗する状況になると、
  該当ドメインの名前解決しない→障害に繋がる (実際に.ukとか.frとか・・・。)

顧客へのサポートに分岐が発生。(ISPなど)

- 問題がDNSSECかDNSなのかの切り分けが生じる。
- WindowsのnslookupではdigのようにSERVFAIL判定を判断できない。
  →Windows用のdigプログラム導入してもらうことに?

DNSSECに対応できる環境にするには？

- DNSSEC対応DNSサーバ
  - BINDのバージョン9.3以降 (権威DNSサーバ・リカーシブサーバ)
    - DNSSECだけではなくDNSのバグもあるので 9.7.3以降推奨。
    - 9.7からはSmart SigningというDNSSEC用の仕組みが機能追加。
  - NSD 2.x以降(権威DNSサーバ)
  - Unbound 1.x以降(リカーシブサーバ)
  - PowerDNS 3.0以降対応表明 (権威DNSサーバ まだpre版のみ公開)
  - Windows2008serverはまだ実装不十分。(R2でNSEC3未実装)
    - 2008 R2 sp1はNSEC3対応できるのかまだ未確認。
  - この資料内の例ではBIND9.7.xを設定事例として紹介します。

- EDNS0対応とTCP fallbackへの対応
  - キャッシュサーバが対応してても・・・

    qmail(と、netqmail)は、512byte 問題が存在。

    qmailはChristopher K. Davis氏が作成したpatch1.03
    (oversize DNS packets patch)を導入することが必須。

    http://www.ckdhr.com/ckd/qmail-103.patch

    ※IPv6で既に問題が顕在化しているので対応済みかも。

    netqmailは1.06に同梱されているnetqmail-dns-packetsz.patch

DNSSECのために新規に定義されたレコード

- DNSKEY ・・・・ DNSSECの公開鍵情報レコード
  - ZSK(Zone Signing Key)
    ・・・ RR(Resource Records)Setを署名する鍵
  - KSK(Key Signing Key)
    ・・・ TYPEがDNSKEYのRRSetを署名する鍵

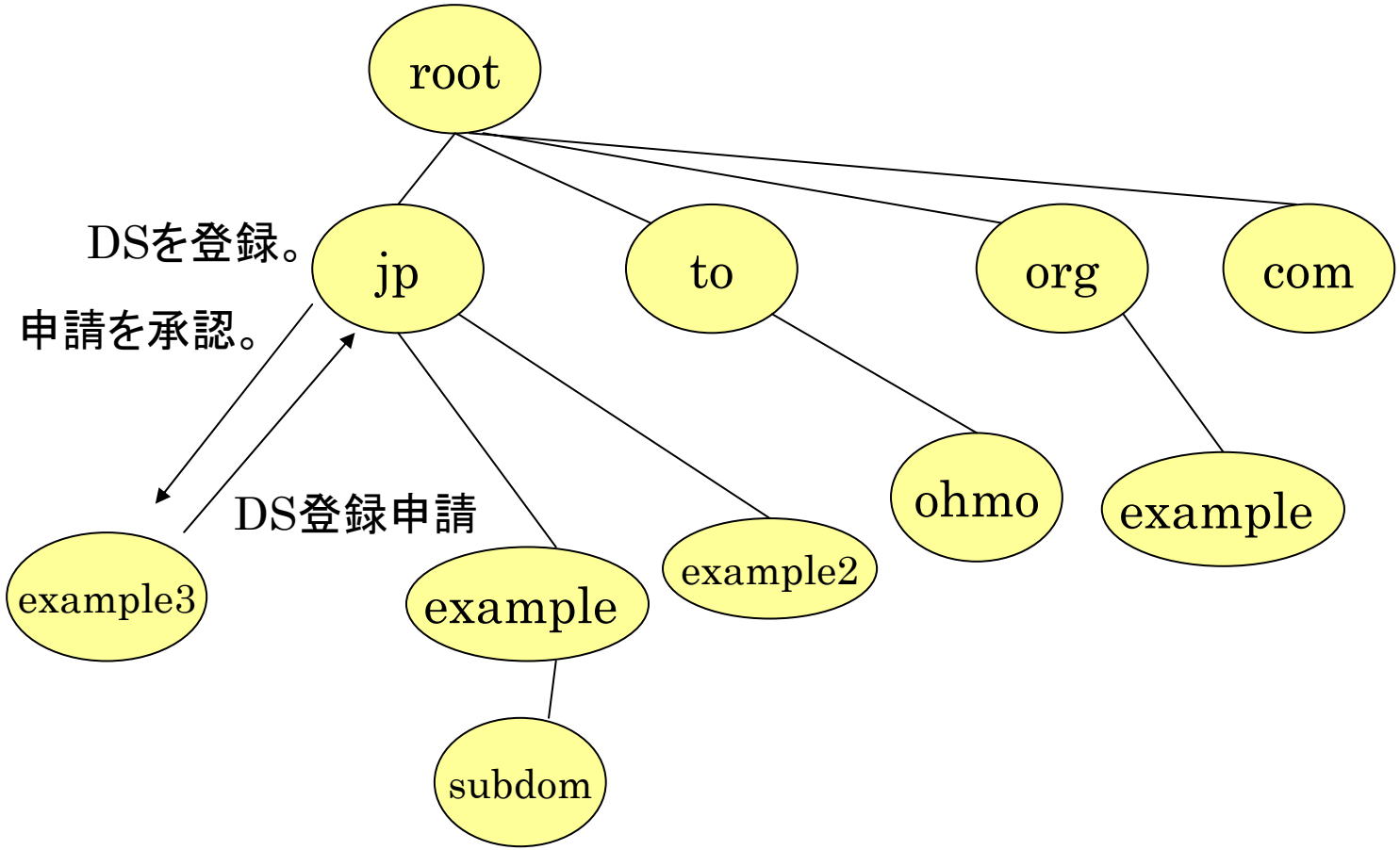
- RRSIG(Resource Record Signature) ・・・・・
  ゾーンファイル内の各レコードの署名を表現する
  レコード。(RRSIG自身には署名しない。)

- DS(Delegation Signer) ・・・・
  子ゾーンのKSKを元に生成されたハッシュ。
  上位DNS権威サーバ(親)のゾーンに登録してもらい、
  親ゾーンのZSKにより署名してもらう。

- NSEC & NSEC3& NSEC3PARAM
  不在証明レコード。後ほど説明

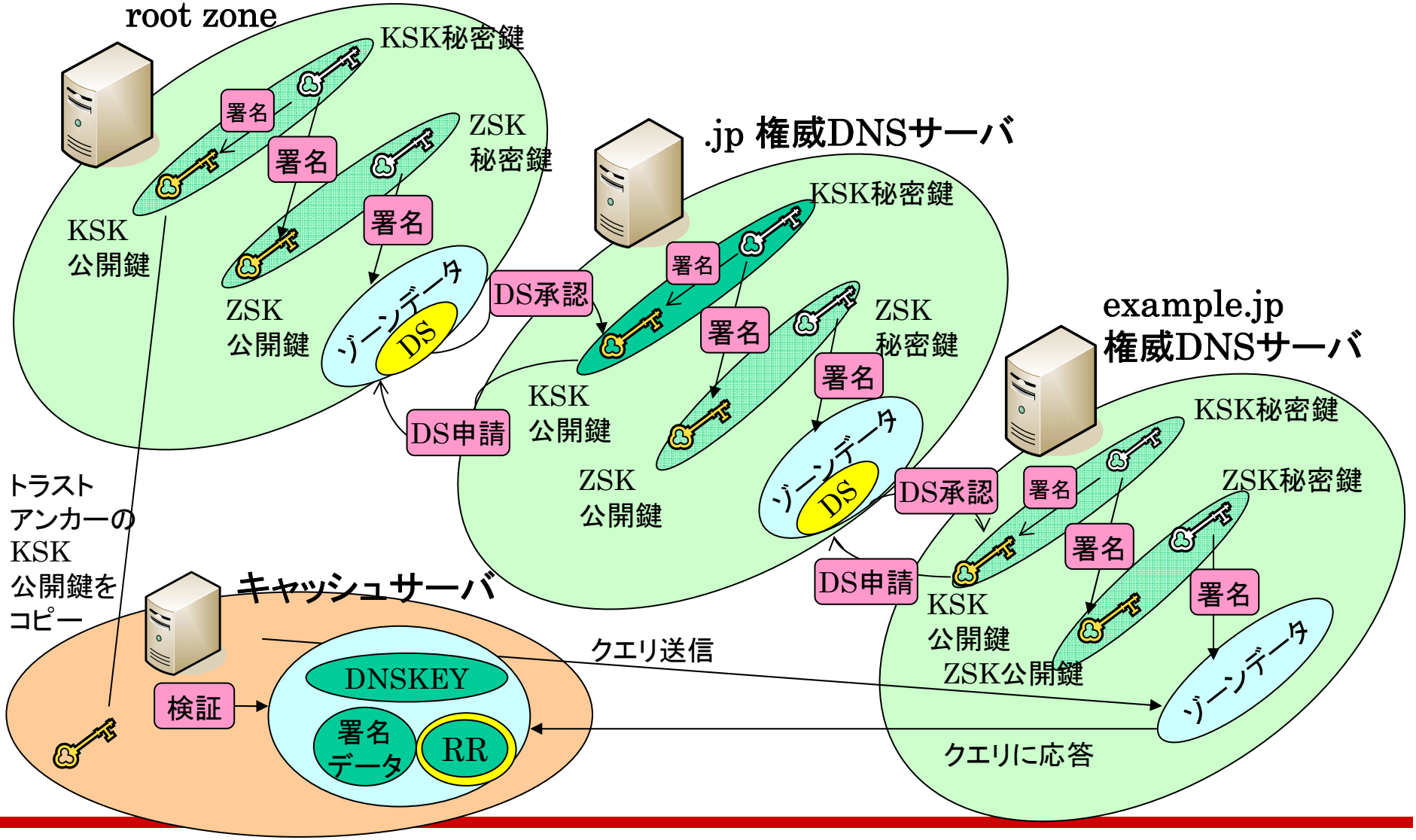
DNSツリーとDNSSEC

- DSを上位ゾーンに署名してもらうことで信頼の連鎖を形成させる。



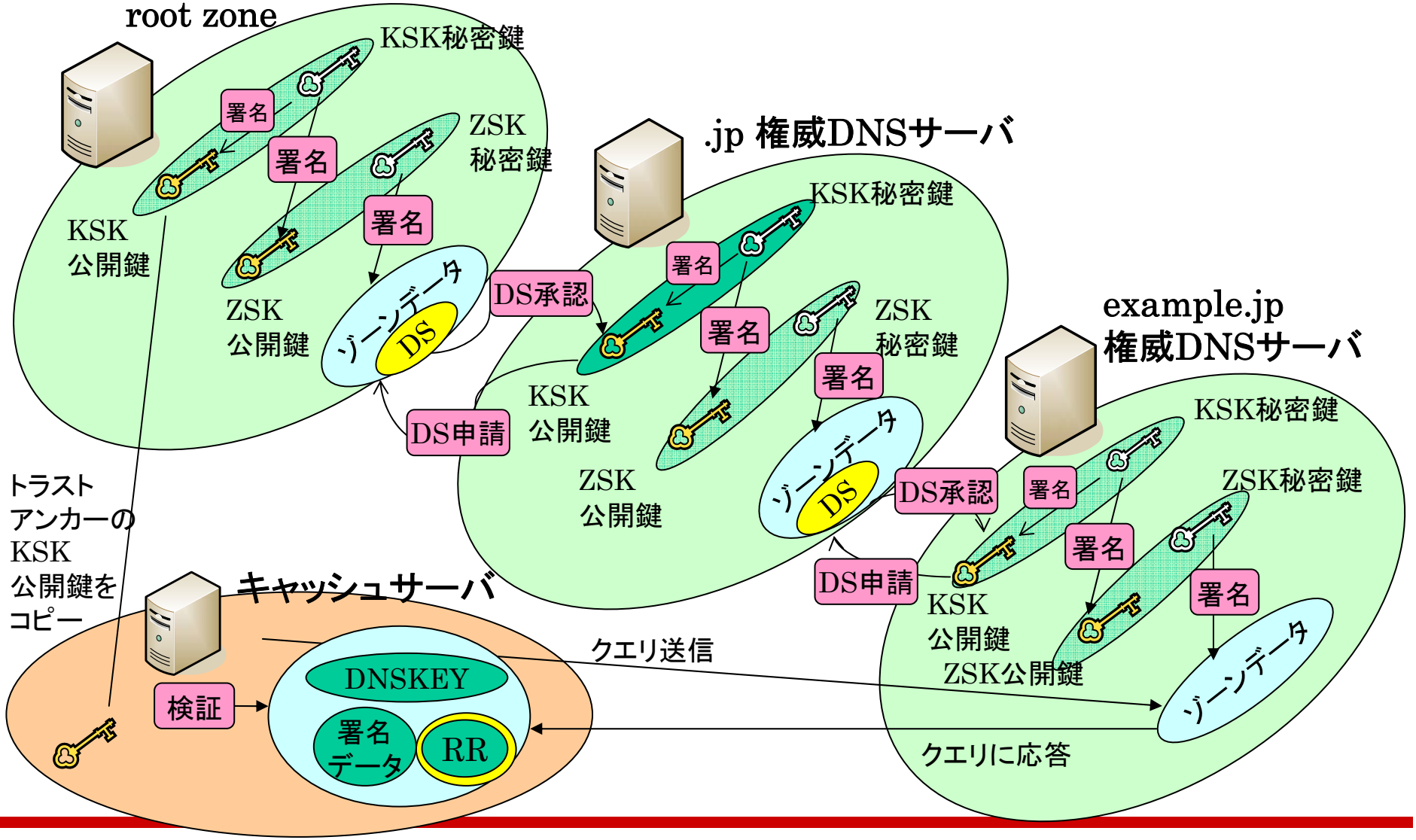
DNSSECの真正性担保の仕組み(俯瞰)

- 「信頼の連鎖」により、レコードの信頼性を担保



DNSSECの真正性担保の仕組み

- 「信頼の連鎖」により、レコードの信頼性を担保



Agenda

- DNSのおさらい
- DNSSECの技術概要
  - **権威DNSサーバ**
  - リカーシブサーバ(リゾルバ・キャッシュサーバ)
- 海外・国内事業者などのDNSSECへの対応動向
- ホスティングとDNSSEC
- まとめ

権威DNSサーバの運用

- DNSSEC対応した権威DNSサーバを運用するためにすること
  - 鍵生成
  - ゾーンへの署名
  - 上位ゾーンへのDS登録申請

定常業務

ゾーンの管理(これまでと同様+RR変更の都度署名処理)

鍵の管理(保管方法の確立とロールオーバー)

ゾーン署名有効期限の把握(再署名処理)

不定期業務

契約移転ユーザのDNSゾーンの授受と管理(委託されている場合)

(DNSSEC対応で留意事項が増える)

鍵の危殆化対応など。

鍵生成

- なんで鍵は二種類あるの?
  - 鍵をZSKとKSKを分けて管理することによって、鍵サイズや暗号強度を、役割に合わせたパラメータで運用できるメリットがある。
  - KSKは親ゾーンとの連携が必須になるため、鍵交換する頻度は少なくしたい。

- 鍵の諸パラメータは、ふつう どーする?
  - 鍵の暗号化アルゴリズムはRFC4641的にはRSA/SHA-256が推奨されている。
  - 鍵サイズは1024bit以上を推奨。(KSK・ZSK)
    (ルートゾーンのKSKでは2048bitが適用されている)
    ZSKはKSKよりも暗号強度が弱くとも良いが更新頻度でカバーしていく。

鍵生成の実際

ZSK…. dnssec-keygen -a RSASHA256 -b 1024 ゾーン名
KSK…. dnssec-keygen -a RSASHA256 -b 2048 -f ksk ゾーン名

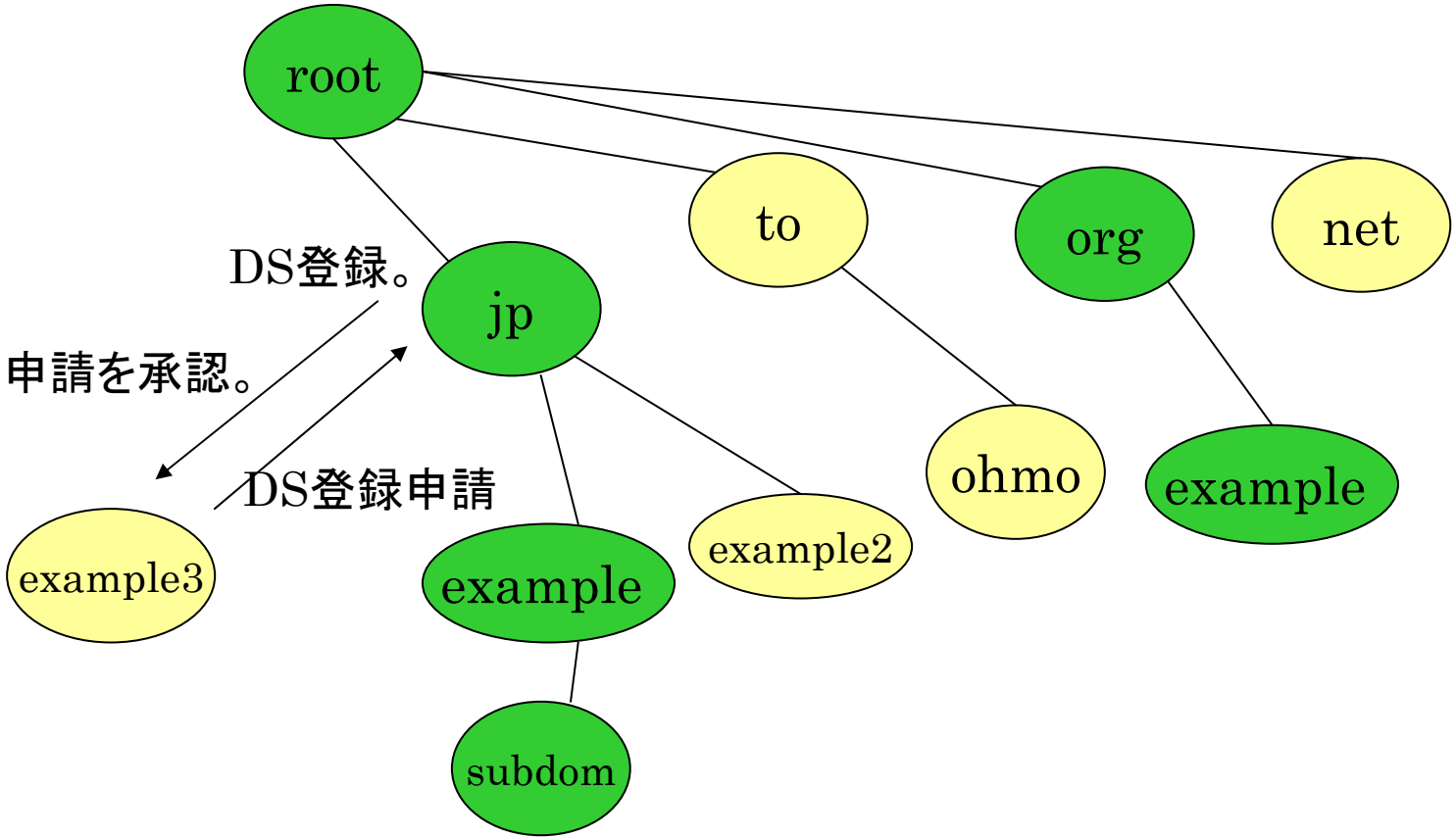
```
# cat Kohmo.to.+008+60799.key
; This is a key-signing key, keyid 60799, for ohmo.to.
; Created: 20100913141843 (Mon Sep 13 23:18:43 2010)
; Publish: 20100913141843 (Mon Sep 13 23:18:43 2010)
; Activate: 20100913141843 (Mon Sep 13 23:18:43 2010)
ohmo.to. IN DNSKEY 257 3 8 AwEAAdLEIOzWiWrHtOEdc60BH4v4Qh6O8JHCO6cNwi5LsF
nLTJAsc4AV CFV5YG131CIHPAfM1hGnBe4qRnjGj+uA7hIDPD/CsKOd9zaFk8LFYiLb…
```

```
#cat Kohmo.to.+008+48543.key
; This is a zone-signing key, keyid 48543, for ohmo.to.
; Created: 20100913141801 (Mon Sep 13 23:18:01 2010)
; Publish: 20100913141801 (Mon Sep 13 23:18:01 2010)
; Activate: 20100913141801 (Mon Sep 13 23:18:01 2010)
ohmo.to. IN DNSKEY 256 3 8 AwEAAcPn4Oj7xRAYMRZ2IkFQmRi5S9wNy7lNkDxMijyB2f
d3aNzw5i1G l3YsG3FHBpgCvbmj3pMkpCIyVi/l74xt2MLF5jAeQKtYdvP2HUjwIsEl….
```

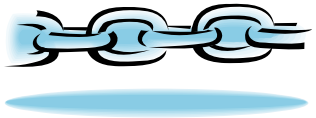
```
#cat Kohmo.to.+008+48543.private
Private-key-format: v1.3
Algorithm: 8 (RSASHA256)
Modulus:
w+fg6PvFEBgxFnYiQVCZGLlL3A3LuU2QPEyKPIHZ93do3PDmLUaXdiwbcUcGmAK……
```

上位ゾーンへのDSレコード登録

- KSKを上位ゾーンに署名してもらうことで信頼の連鎖を形成させる。



署名と「信頼の連鎖」構築の実際



- DSゾーン申請前提
  - named.confに署名したいゾーンが設定されていること。
  - KSKの鍵生成とZSKの鍵を生成済み。

- 署名してみる。

dnssec-signzone –S example3.jp. (←対象ゾーン名)

  - 処理が正常終了すると、dsset-example3.jp.(対象ゾーン名)というDSSetファイルと、署名済みゾーンファイル「example3.jp.signed(対象ゾーン名+.signed)」が生成される。DSSetファイル内に記載された2行のうち、いずれかを上位ゾーンに登録申請する。

example3.jp.　IN DS 60799 8 1 D736F20FB259279A4A5FFCEB45536C5CAD33EC78
example3.jp.　IN DS 60799 8 2
EBC75A18FAEDA255DCD9148418BFCDCF95D6BD6E367EB469EA7BA83A 713CF50F

1=SHA1
2=SHA256

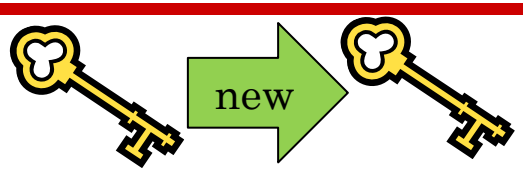
署名の運用 (有効期限)

- 署名には有効期限が設けられている。
  - 有効期限が切れると署名が有効ではない→名前の検証に失敗する→SERVFAILの反応→名前解決できない。→メールは届けられない。webも見れない。

- かといって有効期限を長くしすぎていると期間内に鍵がクラックされる可能性も・・・。
- 有効期限が決められているからサーバ内の時計がずれていると・・・。(.kgが2月22日にUTC+6時間で署名しちゃった)

- KSKの有効期限は長く、鍵の暗号強度を高く、
  ZSKの有効期限は短く、暗号強度は多少緩め、
  というのが推奨されている。
  - RFC4641的にはKSKは13ヶ月に1度のタイミングでの交換を提案している。
  - ZSKは1ヶ月に1度程度を目安(dnssec-signzoneはオプションなしだと30日で設定される。)

鍵のロールオーバー



ロールオーバ手法としては下記の手法がある。

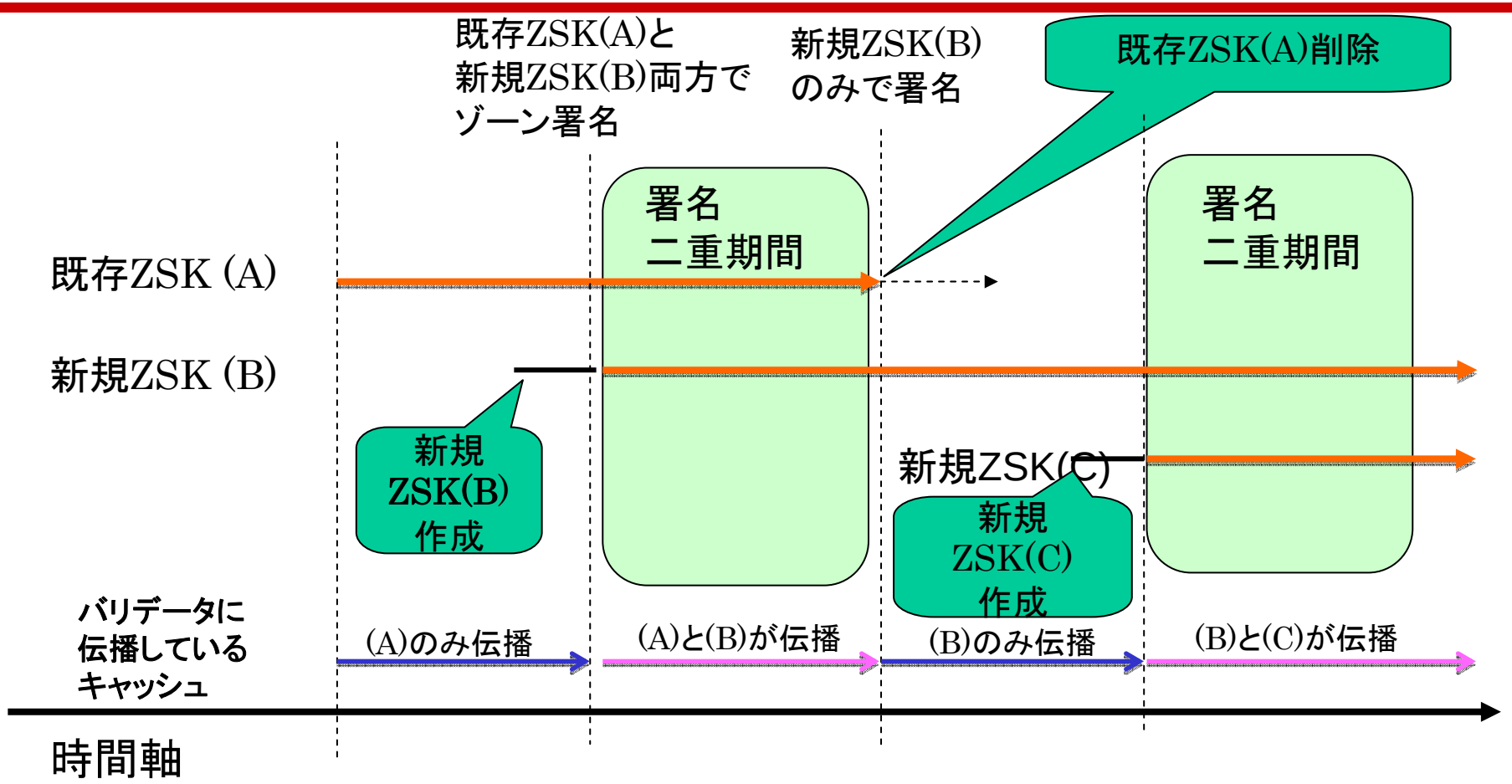
ZSK

- 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)

ZSK / Double signatures （二重署名方式）

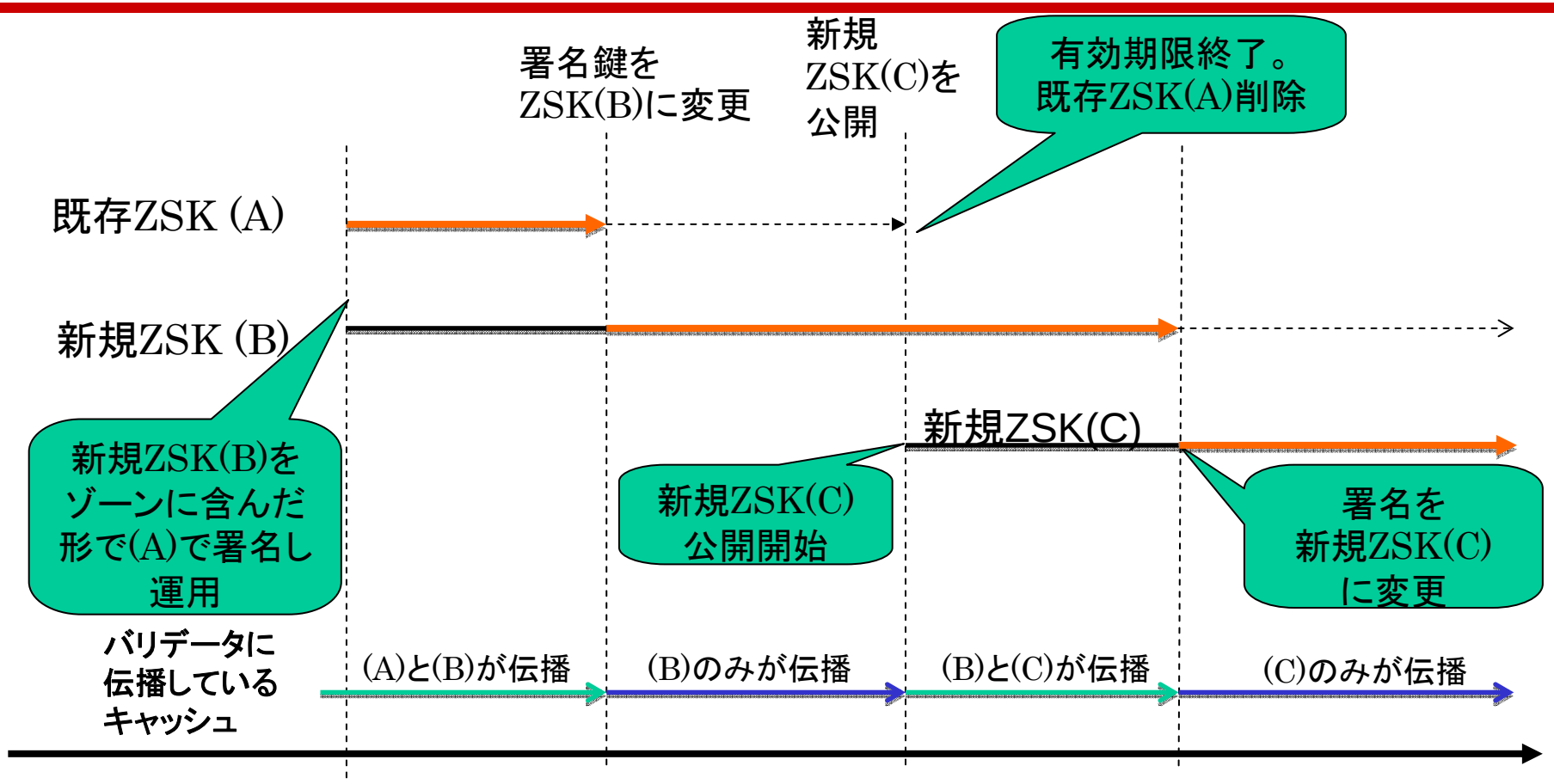


active

rolled

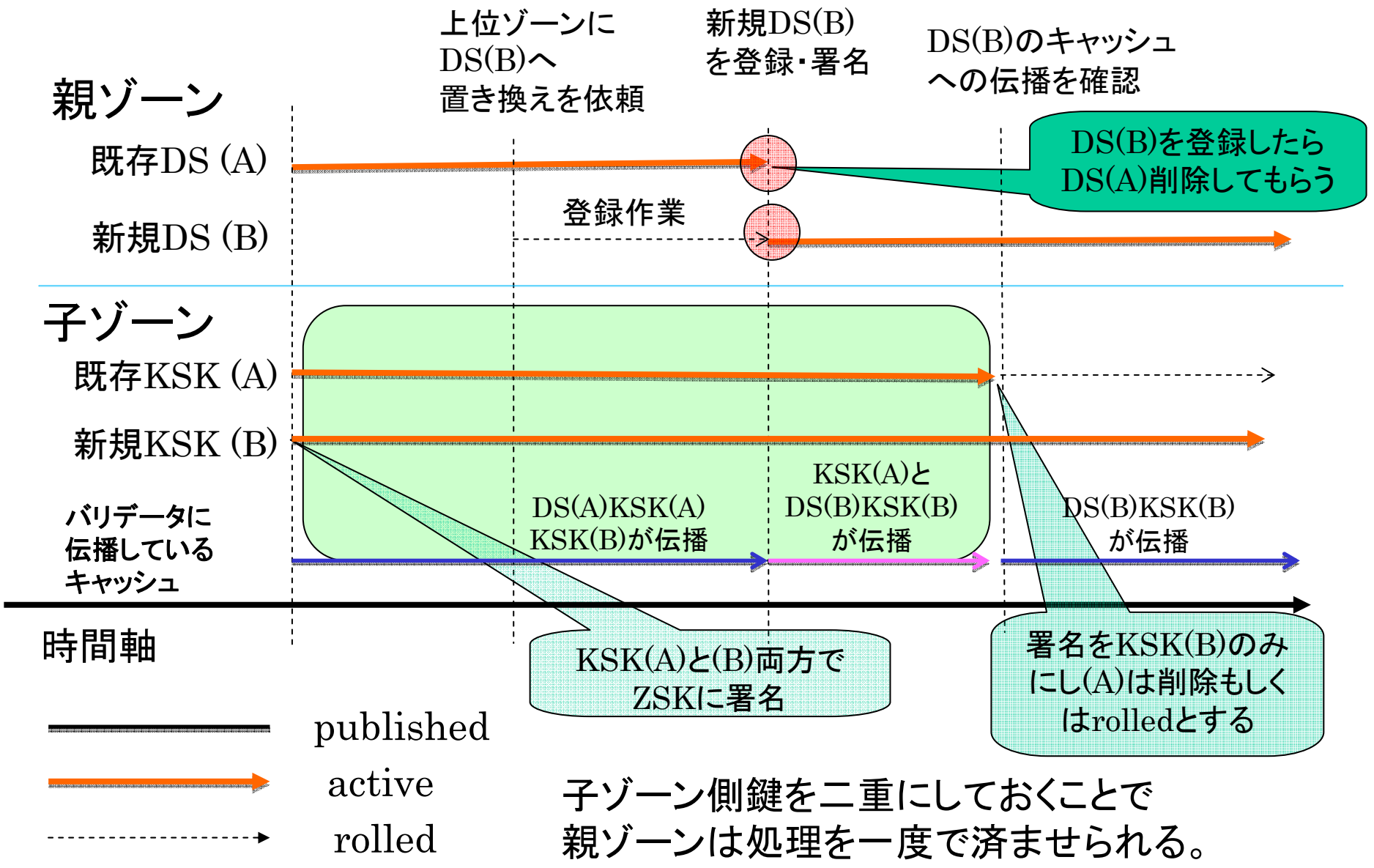
既存と次期両方のDNSKEYで署名し、バリデータへの伝播を待つ。充分に伝播が行き渡っているならば、DNSKEYをいつ切り替えても問題が出ないように考慮した方式。

ZSK / Pre-publication(事前公開方式)



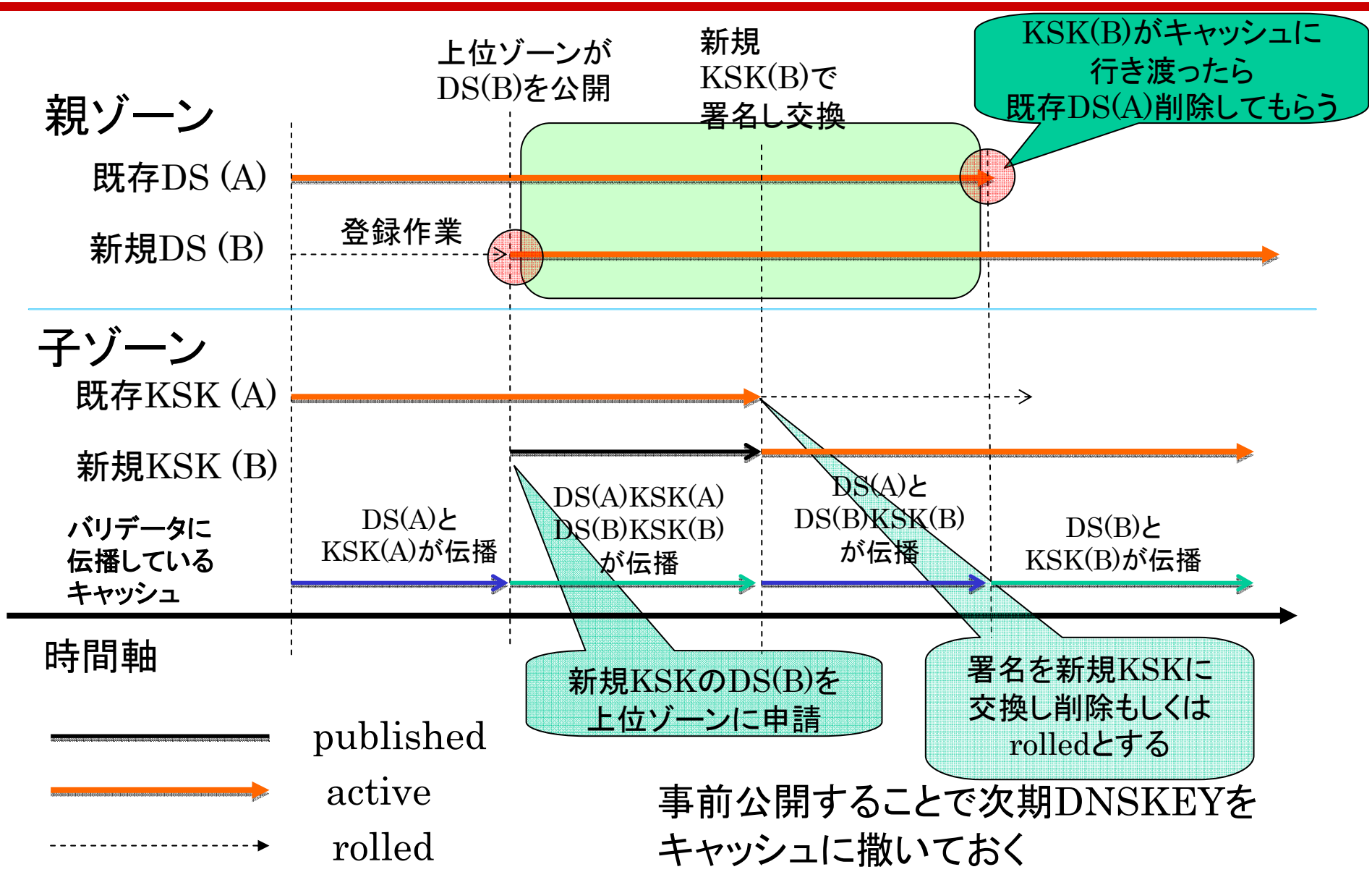
事前公開することで次期DNSKEYを
キャッシュに撒いておける。
これにより署名を切り替えても問題ない
よう考慮した方式

KSK / Double signatures(二重署名方式)



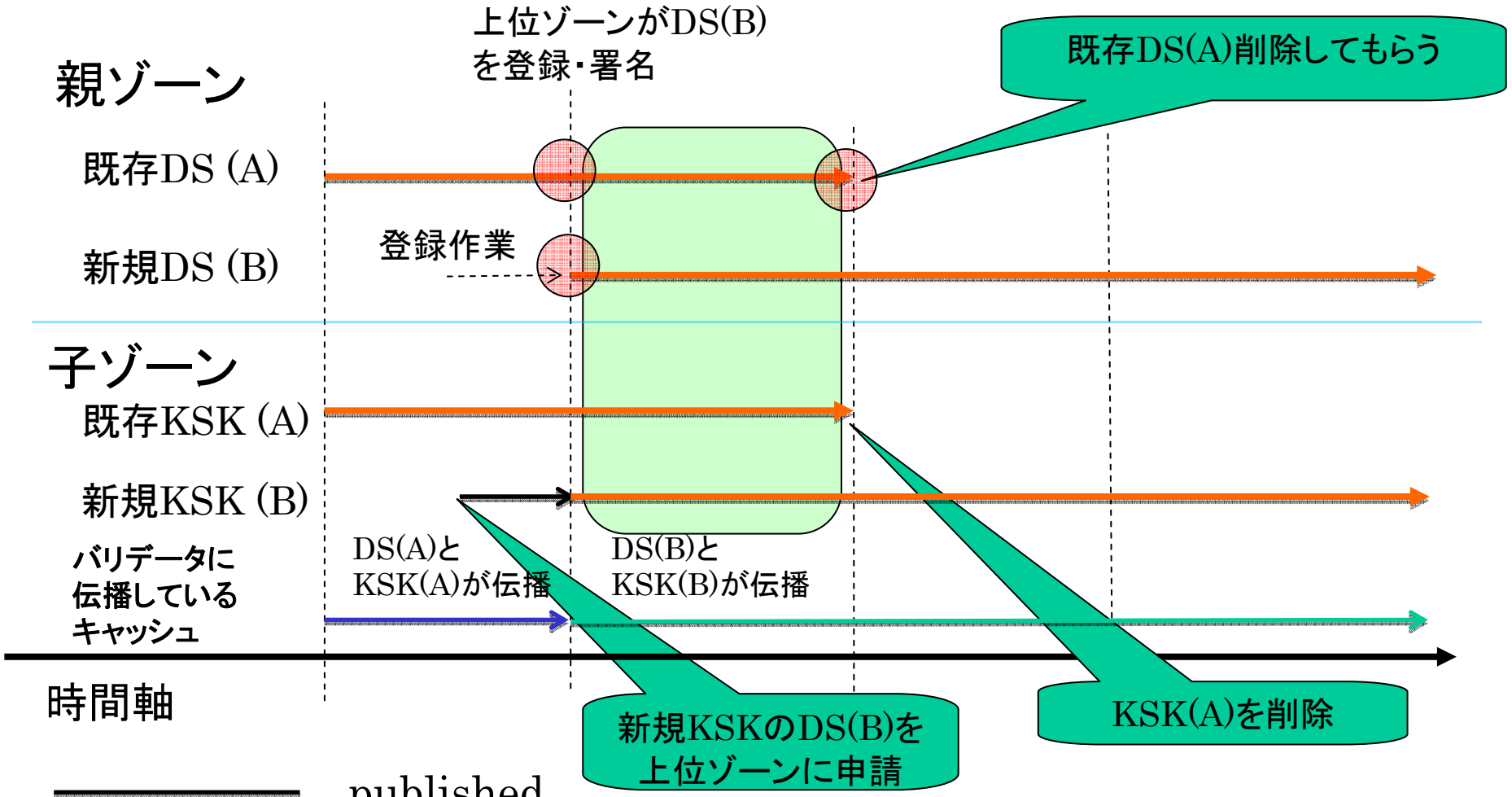
子ゾーン側鍵を二重にしておくことで
親ゾーンは処理を一度で済ませられる。

KSK / Double-DS(二重DS方式)



事前公開することで次期DNSKEYを
キャッシュに撒いておく

KSK / Double RRSet (二重RRSet方式)



作業タイミングを親子で合わせることで
作業工数を減らして交換できる。

鍵のロールオーバーポリシー

- 危殆化して初めて交換するのか定期的に交換するのかの考え方が二種類ある
- 特にKSKの場合は親ゾーン管理者との連携作業になるのでロールオーバーのポリシーは良く考えなくてはならない。

- 危殆化して初めての場合
  - 定期的作業の頻度軽減
  - 作業フローを手が忘れてしまう。 →リスク増大とのトレードオフ

- 定期的に交換する場合
  - 人的作業コストの増加
  - KSKの場合、親ゾーン管理者と都度やりとりする必要が出てくる。(親ゾーン管理者の作業タイミングの調整や待ち時間等も発生。)
  - 定期的に行うので作業をルーチン化できる

Agenda

- DNSのおさらい
- DNSSECの技術概要
  - 権威DNSサーバ
  - **リカーシブサーバ(リゾルバ・キャッシュサーバ)**
- 海外・国内事業者などのDNSSECへの対応動向
- ホスティングとDNSSEC
- まとめ

リカーシブサーバの運用

- DNSSEC対応したバリデーター(検証サーバ)を運用するためにすること。
  - named.confへのmanaged-keys設定

定常業務

ユーザサポートでの切り分け作業 (DNSSECに起因するかの切り分け)

※dig オプションで+cd (check disable)など利用するなど

不定期業務

trusted-keys設定ならroot-serverの鍵交換に応じて変更

トラストアンカー[Secure Entry Point(SEP)]の設定

- バリデート(検証を行う)サーバに、トラストアンカーとなっているKSKの公開鍵をコピーしてきて設定する。
  KSK公開鍵はDNSSECに対応しているゾーンは公開している。
- # dig *ドメイン名* DNSKEY +norec @対象DNS権威サーバで表示される。
  (実際はdig . DNSKEY +norec @m.root-servers.net など。)

```
.          172800    IN    DNSKEY  257 3 8
                           AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
                                   FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL……
.          172800    IN    DNSKEY  256 3 8
                           AwEAAb5gVAzK59YHDxf/DnswfO1RmbRZ6W16JfhFecfI+EUHRXPWlXDi
                                   47t2FHaKyMMEROapL5SZ8HiCzl05lORZGGdN37WY7fkv55r……..
```

- named.confに以下を設定すると、トラストアンカーと対応するゾーン以下については検証を行う。

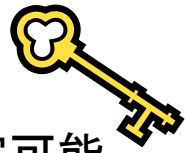
  # trusted-keys { };でトラストアンカーとなるKSKを登録。
  (bind9.7からRFC5011に準拠したmanaged-keysステートメントが実装された。9.7.3でbug解消済み)

```
managed-keys{
        "." initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEz……(略)";
                };

options{
        dnssec-enable yes;          # bind9.5以降ではdefaultでyesなので必要ない
        dnssec-validation yes;    #バリデータとして動作させるか
        }
```

トラストアンカーの注意点

1. Validator(バリデータ) は誰がやるの?
   - リゾルバ(キャッシュ)サーバ
   - 仕様としてはエンドのクライアント側でもバリデータとして設定可能
     - ただし、現段階ではエンド側で対応できるのはこれからというところ。



2. **トラストアンカーとなるKSKをコピーしてくる手法の信頼性**
   - 前頁で紹介した方法だとKSKのキャッシュがすでに汚染していたら・・・。
     - 取得したKSKからDSレコードを生成し(dnssec-dsfromkey) 、一方でHTTPSで取得したWEB上のDSレコードをPGP鍵を利用して真正性を検証、2つを突き合わせてみる。
       https://data.iana.org/root-anchors/root-anchors.xml
     - 詳しい手法はDNSSEC.jpのwebサイトに記載されていますので要確認。
       http://dnssec.jp/wp-content/uploads/2011/02/20110124-techwg-dnssec-trustanchor-install-howto-2.pdf

3. トラストアンカー設定上での注意点
   - BINDではtrusted-keysにDSを設定するのは×　DNSKEYじゃないとだめ。
   - unboundではDSでもDNSKEYでも両方OK

NSEC & NSEC3

- NSECってなに?
  - 登録していないホスト名についての不在証明レコード
    - 検証した際に「そのホスト名のレコードは存在しない」ということを証明する。

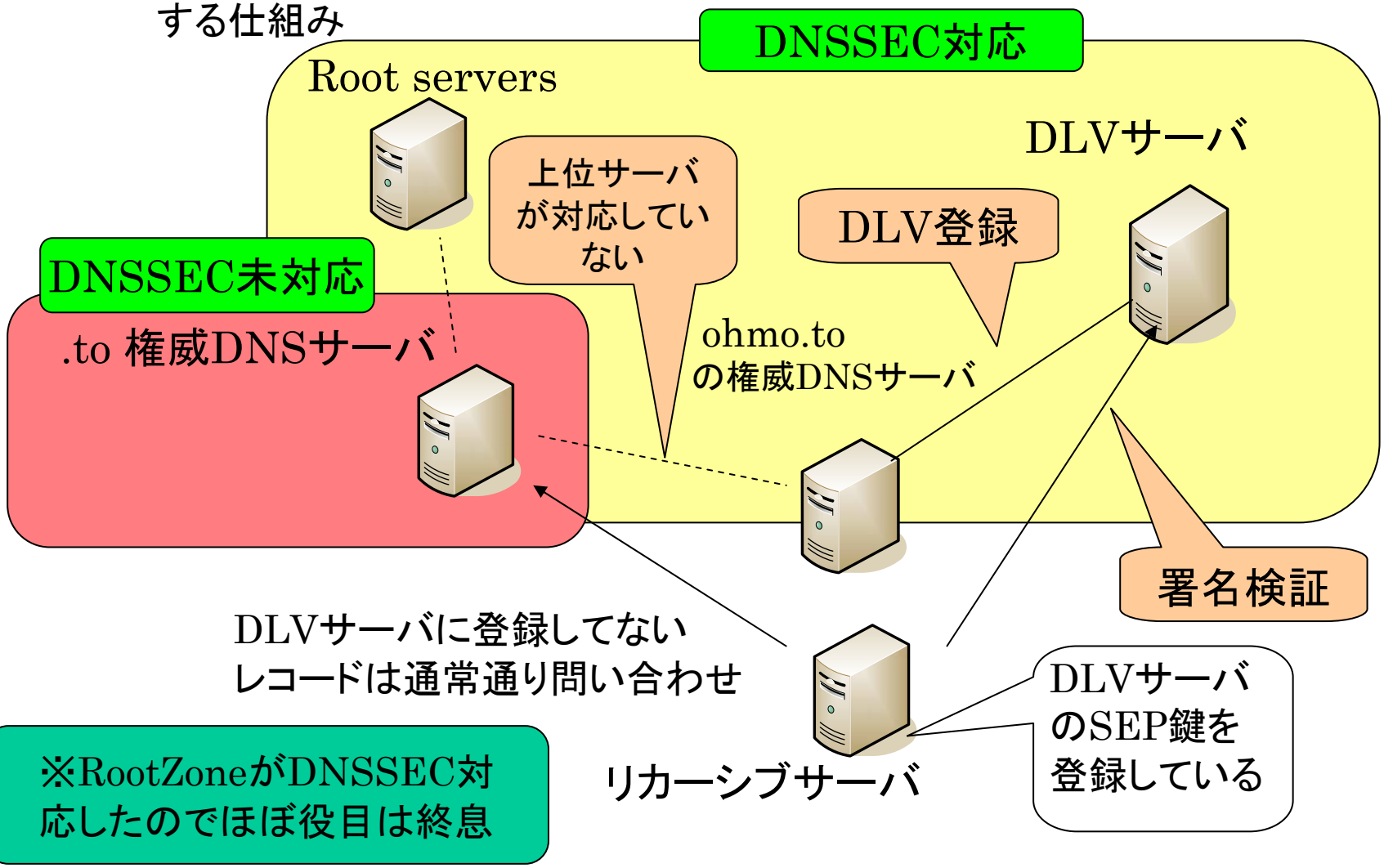
- zonewalkによる露出の危険性(NSEC)
  - NSECの場合、zonewalkをすることで登録しているホスト名が意図せずに露出してしまう。
    - そのゾーンで管理しているホスト名を問い合わせた際に、アルファベット順に次に登録されているレコードが表示される。
    - ohmori.example.jpの次の登録レコードはohmoto.example.jpと表示
      - それってohmo(ri～toの)間には登録ホストがない事の証明でもある。
        (というか、それが本来の目的なのですが。)
- →zonewalk対策となるNSEC3が登場

- NSEC3では、FQDNを一方向にハッシュ化して、
  ハッシュ値をてがかりに不在証明。
  - →ただし、NSECに較べても、キャッシュサーバの処理に結構な負荷がかかる
    Janog26 民田さん@JPRSの報告参照
    http://www.janog.gr.jp/meeting/janog26/doc/post-dnssec-min.pdf

- NSEC3PARAMはNSEC3のハッシュ化するにあたって利用するソルト値などを含むパラメータを格納しているレコード

DLV(DNSSEC Lookaside Validation)(参考)

- 通常のドメインツリーとは別にDNSSEC専用の問い合わせ先を用意し、~~root zoneや~~上位TLDが対応していなくとも署名の検証を可能とする仕組み



OpenDNSSECその他ツール(参考)

- DNSSECは覚えることも多くて運用するにもかなりの慣れが必要そう・・・

- 海外のレポートでもDNSSECに対しての知識がまだエンジニアに浸透していない(対応できるエンジニアが少ない)のが悩みの一つとされている。http://www.afilias.info/webfm_send/119
  - 実際に.uk .frといった、TLDレベルでもDNSSECに起因する障害が発生している。

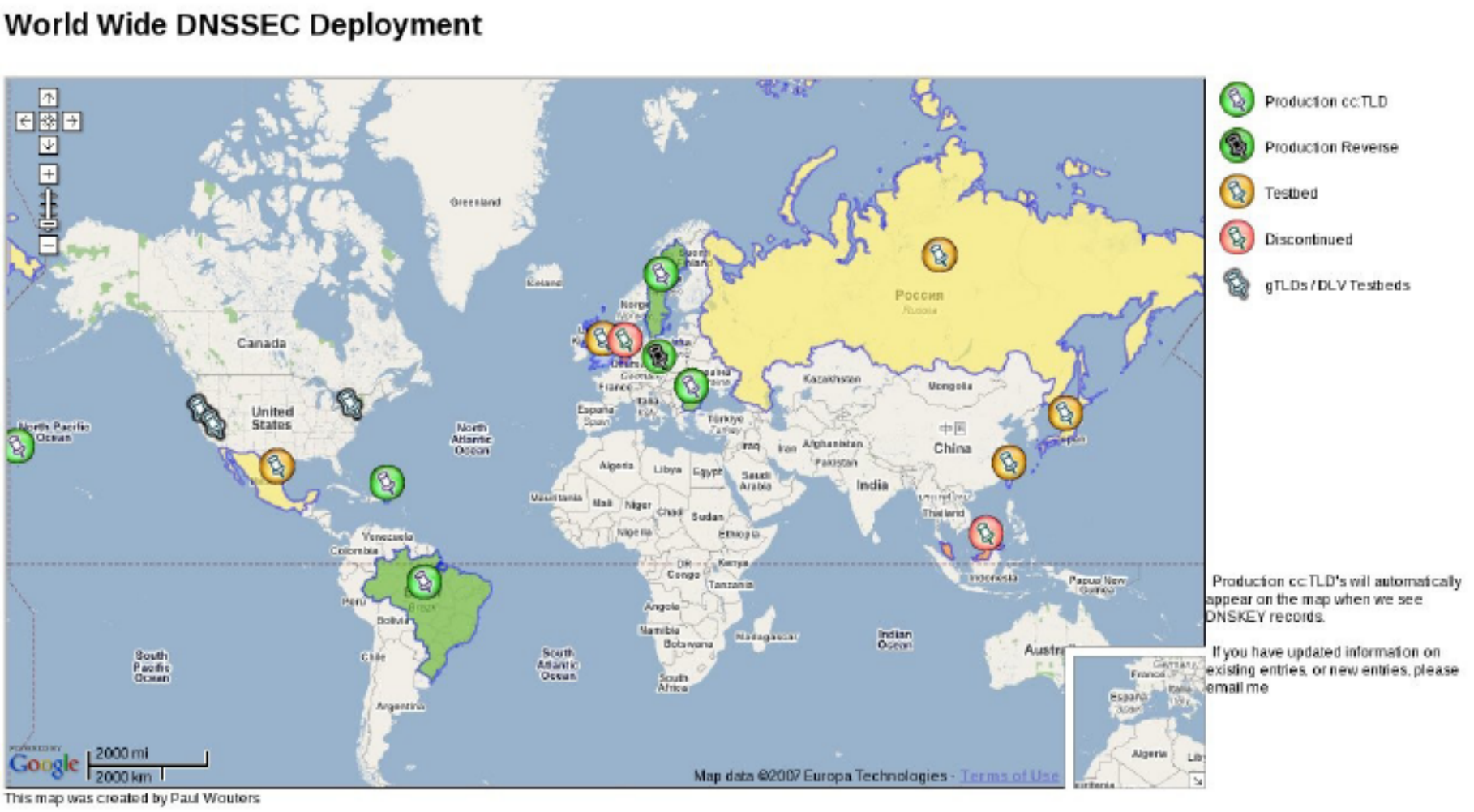
- ということで、代表的なツールとして、OpenDNSSECというツールが公開されています。
  http://www.opendnssec.org/ (2010年2月現在ver1.20が公開中)
  - 鍵更新とゾーン署名の自動化や、ゾーンの完全性チェック、ソフトウェアHSMも含んだツール

- 他にもhttp://www.dnssec.net/softwareにDNSSECに関連する便利なツールがまとめられています。

Agenda

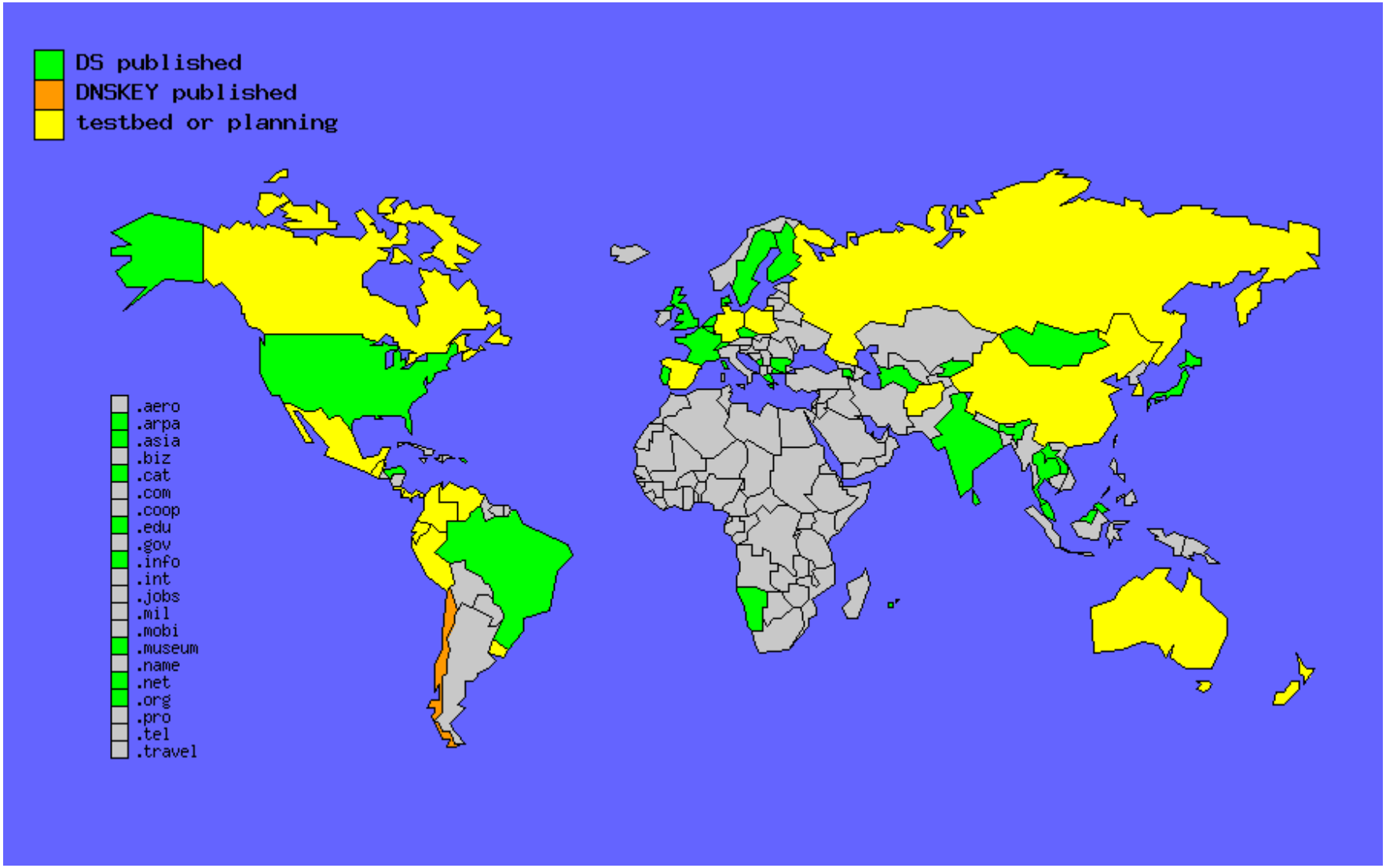
- DNSのおさらい
- DNSSECの技術概要
  - 権威DNSサーバ
  - リカーシブサーバ(リゾルバ・キャッシュサーバ)
- **海外・国内事業者などのDNSSECへの対応動向**
- ホスティングとDNSSEC
- まとめ

各TLDの対応状況@2007年



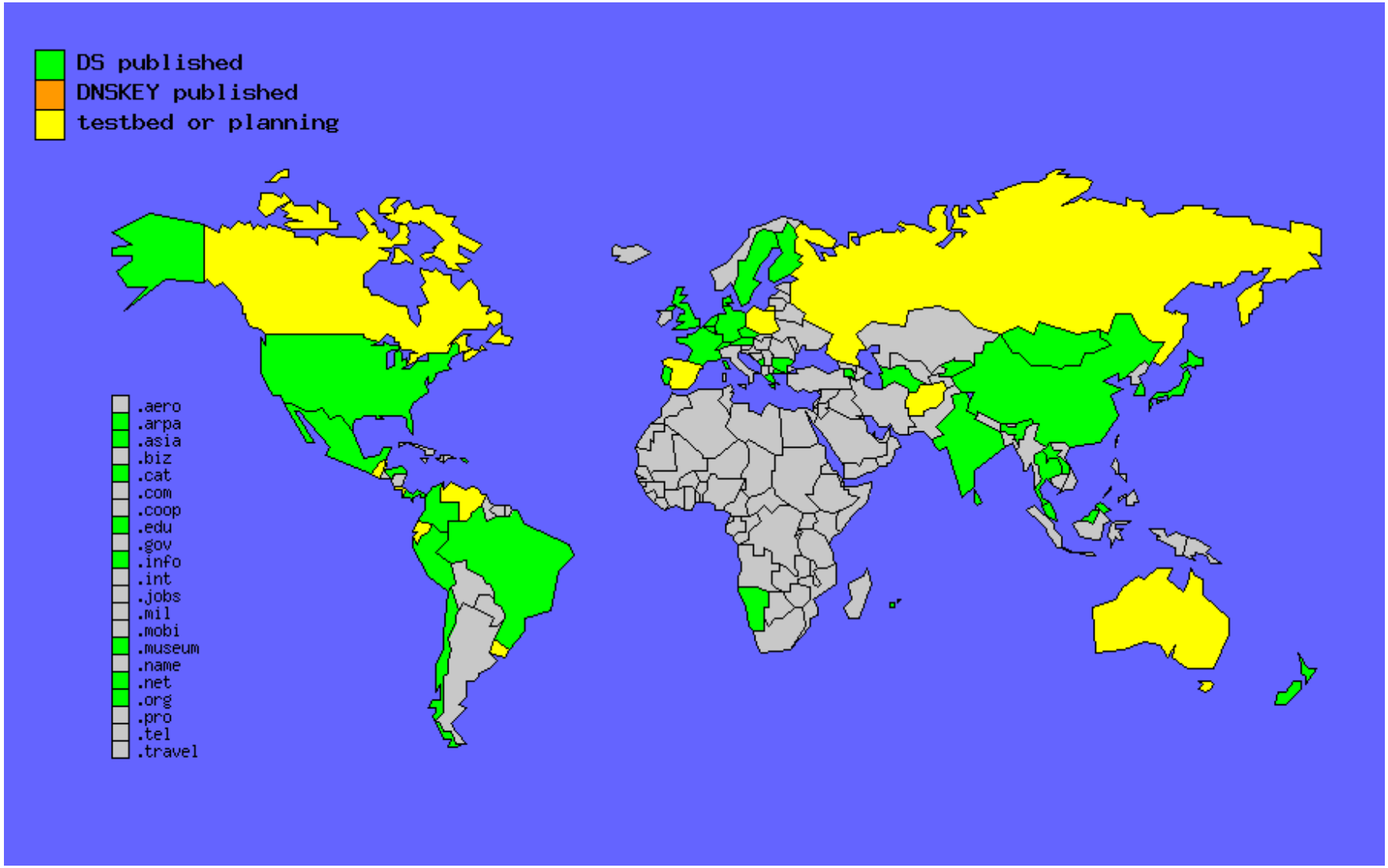
Paul Wouters氏資料 http://www.xelerance.com/talks/sector/Sector2007DNSSEC.pdf より

急速に広がったDNSSEC @2011年2月



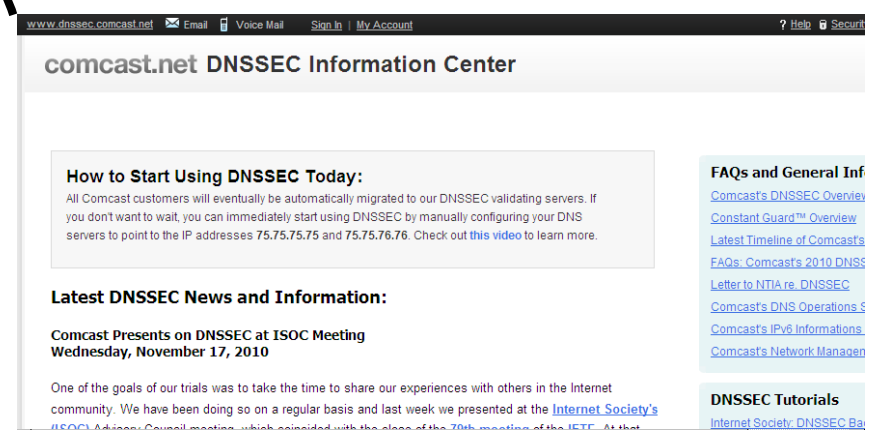
- http://www.ohmo.to/dnssec/maps/

各アナウンスからの2011年末の対応状況予想



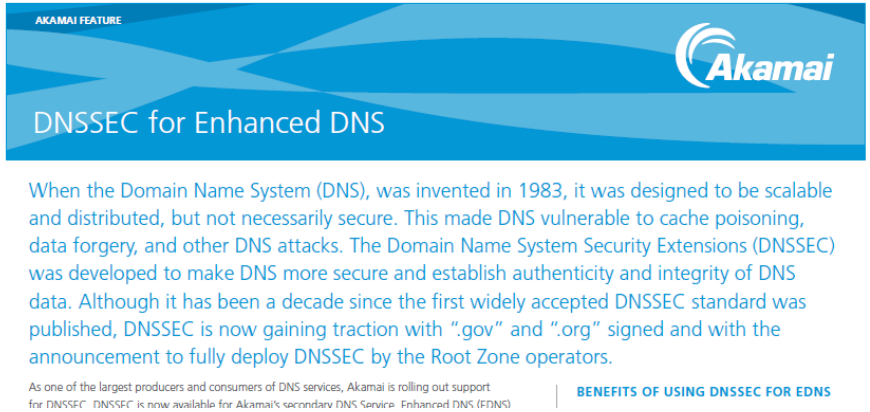
海外の事業者の動き

- Comcast(USのCATV ISP)は、顧客向けrecursiveサーバ(複数台)で順次署名の検証を有効にしている模様。(5000ドメイン管理)



- Akamai (CDN事業者)

  DNSサービスで
  DNSSECサポート



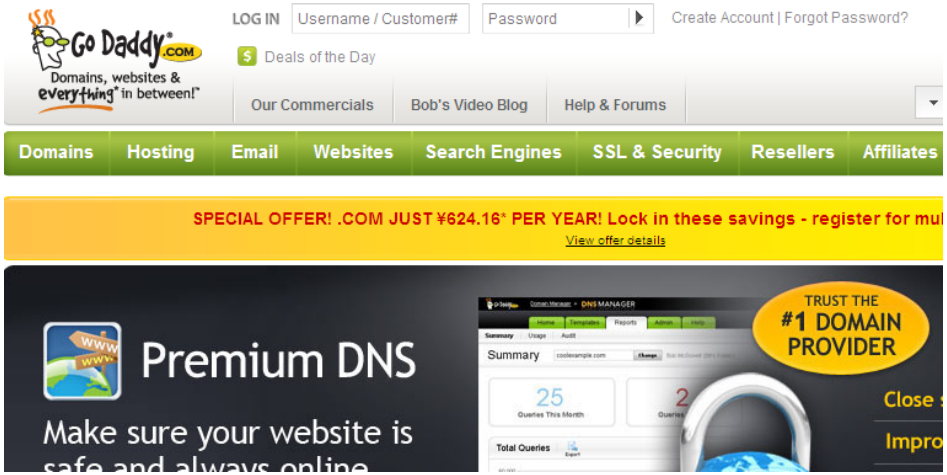
海外の事業者の動き

- Blue Cat Network

  DNSSEC対応の
  Virtual アプライアンス発売

- Go Daddy

  ¥300円弱/月で
  DNSSEC対応のASPサービス



日本の事業者の対応状況

- JPRSさんのドメイン名登録サービス一覧
  http://jpshop.jp/list/gjp_list/gjp_pl1_01.html

.Jp　会社案内　JP WHOIS　用語辞典

JPドメイン名について　JPドメイン名の登録と活用　関連ニュース　指定事業者

ホーム > JPドメイン名の登録と活用 > 指定事業者一覧 > 汎用 > ドメイン名登録サービス

- JPドメイン名の登録と活用
  - JPドメイン名を登録するには
  - 指定事業者一覧
    - 汎用
      - ドメイン名登録サービス
      - インターネット接続サービス
      - ホスティングサービス
      - 転送系サービス
      - 日本語ドメイン名サービス
    - 属性型・地域型
  - JPドメイン名の活用方法
  - 見つけた！JP
  - TOPICS
  - FAQ

名づけてねっと NTTPC

ドメイン名登録サービス

汎用JPドメイン名の登録サービス提供指定

登録サービスを提供している指定事業者を、その取り扱いメイン名登録数順となっています。(2011/02/15 現在)

登録・更新のみのサービス提	
○	ドメイン名の登録・更新のみのサービスを提供してい
×	接続・ホスティングなど、他のサービスと合わせたご利

IPv6	
○	ネームサーバホスト情報のIPアドレスとしてIPv6形式
×	ネームサーバホスト情報のIPアドレスとしてIPv6形式

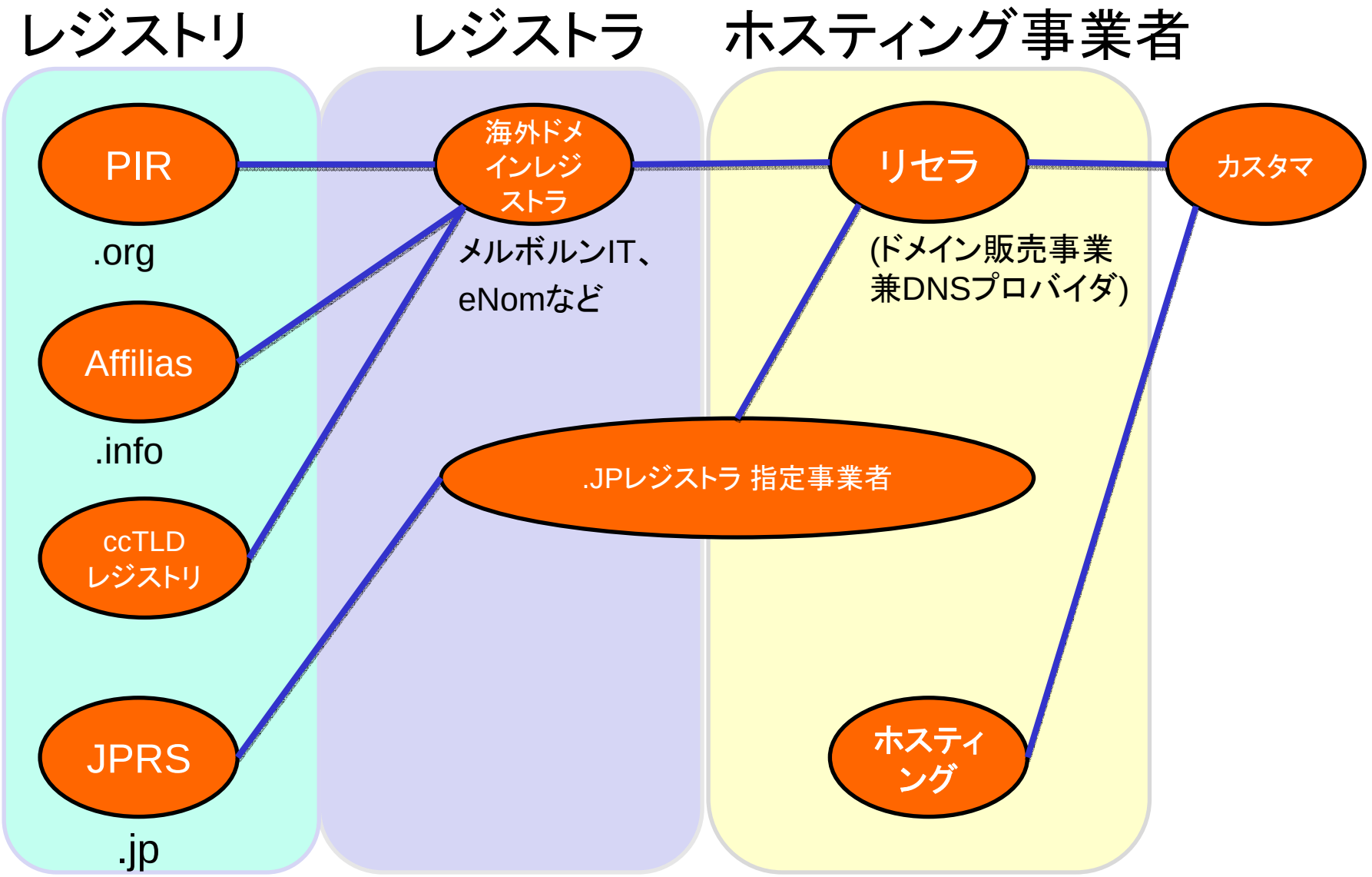
DNSSEC	
○	ドメイン名のDNSSEC署名鍵(DSレコード)の取次ぎサ
×	ドメイン名のDNSSEC署名鍵(DSレコード)の取次ぎサ

サービス名（指定事業者名）	汎用JP登録	登録・更新のみのサービス提供	IPv6	DNSSEC
お名前.com（GMOインターネット株式会社）	.Jp	○	×	×
ムームードメイン（株式会社paperboy&co.）	.Jp	○	×	×
バリュードメイン（株式会社デジロック）	.Jp	○	×	×
SAKURA Internet（さくらインターネット株式会社）	.Jp	○	×	×
OCN（エヌ・ティ・ティ・コミュニケーションズ株式会社）	.Jp	×	×	×
Doレジ（ファーストサーバ株式会社）	.Jp	○	×	×
NTTPC（株式会社エヌ・ティ・ティピー・シーコミュニケーションズ）	.Jp	○	×	○
アイル（GMOホスティング＆セキュリティ株式会社）	.Jp	○	×	×
21-Domain.com（株式会社アンネット）	.Jp	○	○	×
ドメインネーム・フォー・ユー（株式会社ヒューメイアレジストリ）	.Jp	○	○	○
αWeb	.Jp	×	×	×

Agenda

- DNSのおさらい
- DNSSECの技術概要
  - 権威DNSサーバ
  - リカーシブサーバ(リゾルバ・キャッシュサーバ)
- 海外・国内事業者などのDNSSECへの対応動向
- **ホスティングとDNSSEC**
- まとめ

ホスティング事業のモデル

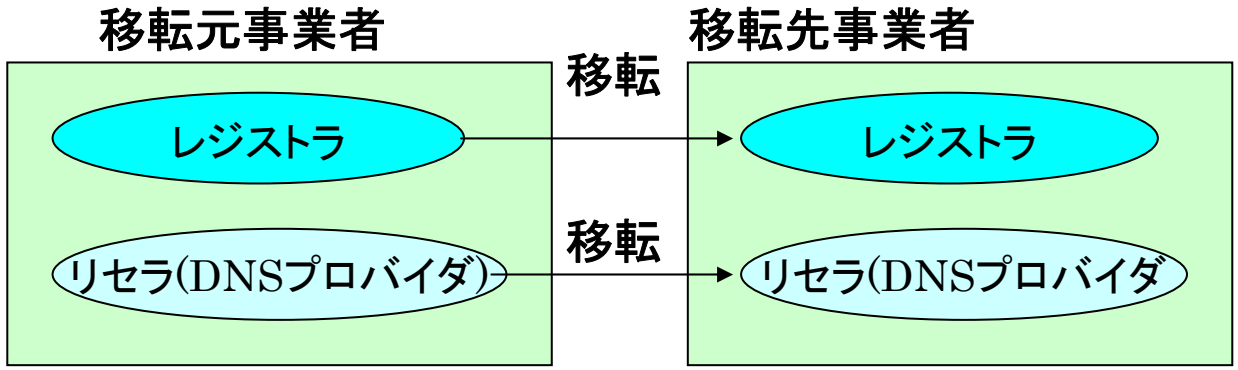


ホスティング事業とDNSSEC対応の留意点

- DS登録できるのか
  - レジストラのAPIがDNSSEC対応しているか
    - GoDaddyは対応、メルボルンITはまだ・・・とか。
- 鍵の管理はどうするのか?
  - 顧客のゾーンの秘密鍵の管理方法をどうするのか
    - HSM(Hardware Secure Module)使う?
- 検証(バリデート)
  - リカーシブサーバのサービス提供でDNSSEC対応するのか
- セカンダリサービスの提供
  - プライマリは自前で構築、セカンダリは事業者のサーバを利用するケースもある。セカンダリをDNSSEC対応するのか。
  - カスタマのプライマリが対応すると知らないうちに大きなゾーンデータがセカンダリに飛んでくる。

ドメイン事業者 移転対応業務

- 不定期業務



顧客の契約満了→別事業者へ移転するケース。

→事業者間でDNSサービスの移管が発生。

DNSSECが絡むことで現状よりも複雑になる。

- 一時的にDS登録を解除して引き渡す処理が入る。
- パターンも複雑化。
  - 移転元(DNSSEC対応・未対応)-移転先(DNSSEC対応・未対応)の組み合わせ)

DNSSEC.jpでは移転ガイドラインを公開しています。

http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-registrar-transfer-guideline.pdf

gTLDのレジストラ変更作業のまとめについては、現在鋭意制作中

- まとめ

・・・の前に

SCSEの精神とホスティングサービス

- SCSEって知ってますか?

  あるテーマパークの運営で徹底されている

  S(Safety 安全)

  C(Courtesy 礼儀)

  S(Show 演出・見栄え)

  E(Efficiency 効率)

  の順で行動を優先する運営・行動指針

  テーマパークとホスティングは違うけど、顧客にサービスを提供するという視点では同じじゃないかな?

  DNSの今の”効率”を優先させて、安全性に目をつぶるのか?

まとめ

- 今現在も危険性は潜在しており、国内外問わず、日々DNSSEC対応が進んでいる。
- 本格的なDNSSEC運用に向けて、負荷を軽減するために色々な機能が開発されてきているので運用への敷居は少しずつ低くなってきている。
- DNSSECの導入には負担や課題も多いが、インターネットの基盤を維持するため、まずは導入の検討をすべき。

ご清聴ありがとうございました。

オチ

まぁ、僕個人のドメインは
DNSSEC未対応の.toドメインなんで
DNSSECへの対応は・・・まだDLVのみ　orz
↓
taxi@ohmo.to