DNSOPS.jp
DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECの現状と普及に向けた課題

日本インターネットエクスチェンジ株式会社
DNSOPS.JP代表幹事
DNSSECジャパン会長
石田慶樹

内容

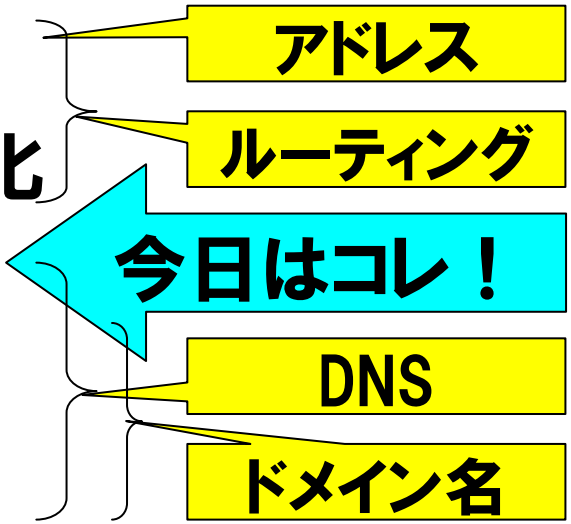
- DNSSECの基礎
- DNSSECの現状
- DNSSECの普及に向けた課題

はじめに

- 今回の講演内容は、各所の資料を参考にしつつ自分の理解に基づき、独自にまとめた部分も多くあります。
- 参考にした資料はURLを示しておりますので、内容の正確性については原資料をご確認ください。

はじめに

- 2011年（来年）はインターネット激動の年
  - IPv4アドレスの枯渇
  - 4 Octet AS番号の常態化
  - DNSSECの導入
  - IDN ccTLDの誕生
  - gTLDの増加



2011年　インターネット5重苦

「.日本」の選定基準については現在パブコメ募集中となります。是非一度、確認いただきますようお願いいたします。 http://jidnc.jp/?p=369

DNSSECの基礎

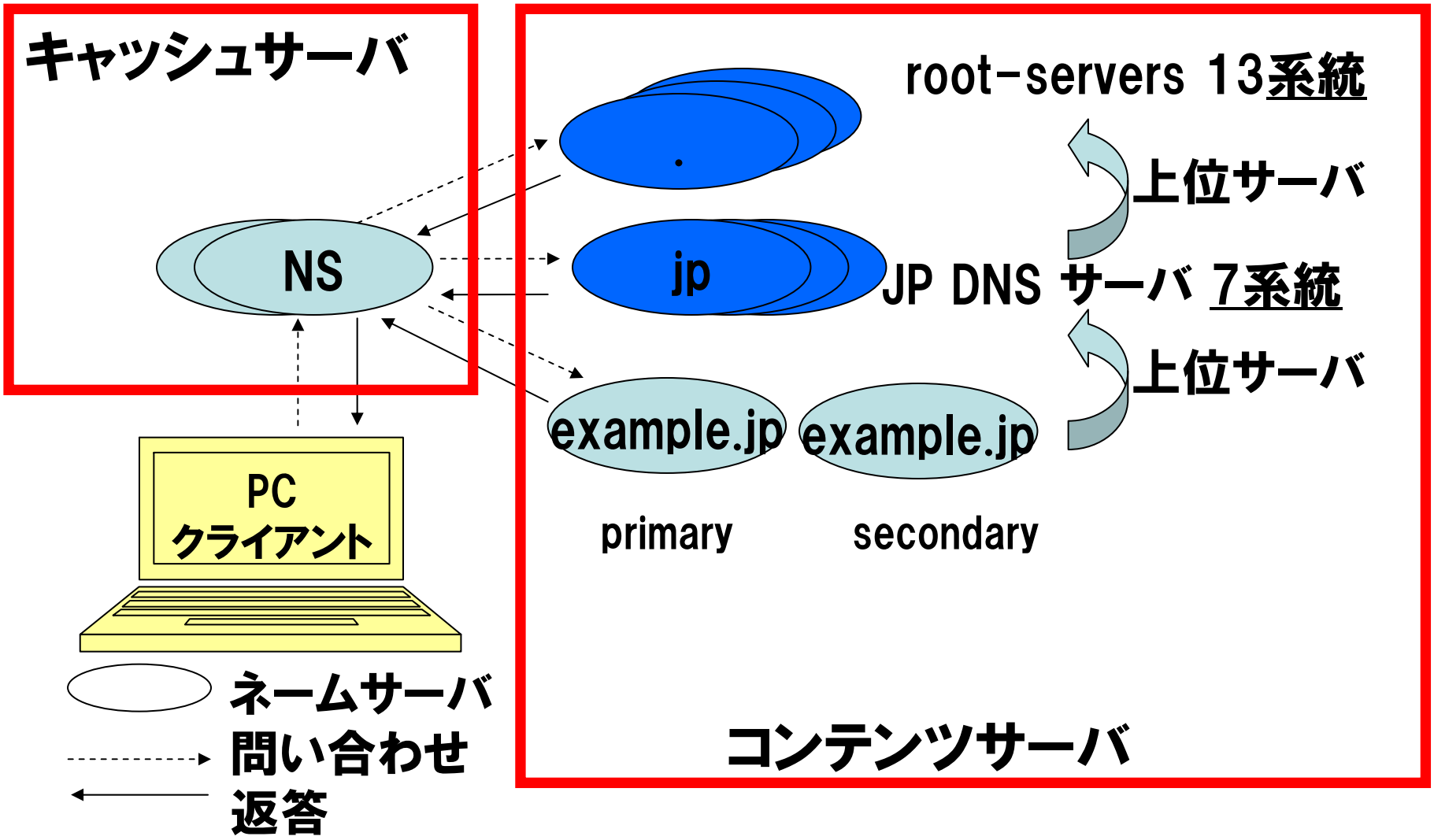
DNSとは

- Domain Name System/ドメインネームシステム
- ホスト名とIPアドレスの対応付けを行うためのメカニズム(の一つ)
- 数字の羅列ではなく人間にとって覚えやすい意味のある文字列を利用するため
- 世界規模の(唯一成功した)分散管理データベース

DNSサーバ

- DNSコンテンツサーバ
  - DNSのドメインに関するデータを保持するサーバ
  - DNS権威サーバ(権威DNSサーバ)とも呼ばれる
- DNSキャッシュサーバ
  - クライアント端末(PC)からのDNSの問い合わせに対してルートから順に再帰的に問い合わせをすることにより解決しクライアントに答えるサーバ
  - データを一時的に保持(キャッシュ)することが多いためDNSキャッシュサーバと呼ばれる

DNSの構成

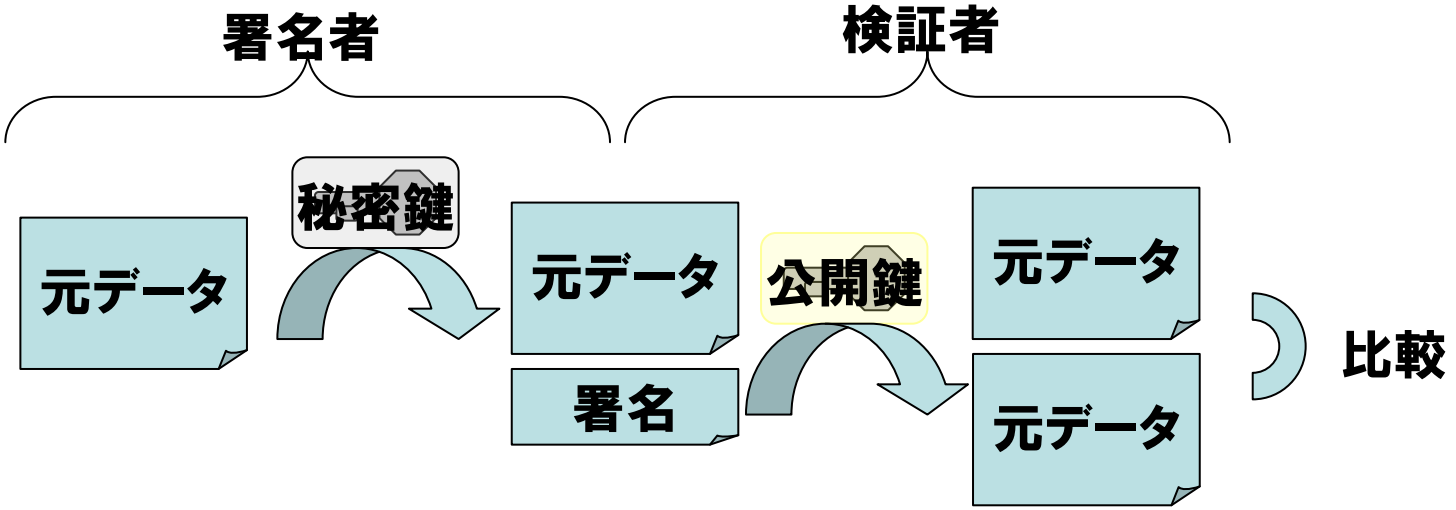

キャッシュサーバ
NS
PC
クライアント
root-servers 13系統
.
上位サーバ
jp
JP DNS サーバ 7系統
上位サーバ
example.jp
example.jp
primary
secondary
コンテンツサーバ
ネームサーバ
問い合わせ
返答

DNSSECとは

- DNSSEC: DNS SECurity extensionの略
- RFC4033, RFC4044, RFC4045
- 電子署名によりデータの内容を保証
- DNSコンテンツサーバのコンテンツ(内容)を署名鍵(秘密鍵)で署名することによりDNSキャッシュサーバ側でそのコンテンツが正当であるかの判定ができる
- DNSのツリー構造の中に署名鍵情報(公開鍵)を登録することによりDNSの中に閉じて解決が可能
- 但しルートの署名鍵情報についてだけは別途正当性の確認が必要

電子署名

- 公開鍵方式を利用して電子的に署名を行うこと
- 署名者は秘密鍵を用いて署名を行う
- 検証者は署名者の公開鍵を用いることで署名の検証が可能になる



DNSSECの必要性

- Kaminsky氏による脆弱性発見
  - 2008年7月に情報公開（脆弱性の発見は2008年2月ごろ）
  - キャッシュサーバへの毒入れ（偽のデータを信じ込ませること）が力技で可能となることを指摘
  - 存在しないドメイン名への問い合わせを繰り返す
  - それに対する偽の回答を返すことでそのデータをキャッシュさせる
- 脆弱性の原因
  - UDPであること（パケットの一方的送付が可能）
  - Source Address Spoofingが容易な環境
  - DNSの問い合わせの識別子（ID）が16bitしかなく問い合わせに対する返答が推測可能
  - とりあえずの回避方法としては乱雑さを増やすことによる（ポート番号を固定ではなくランダムにする）

本質的な解決はDNSSECによる

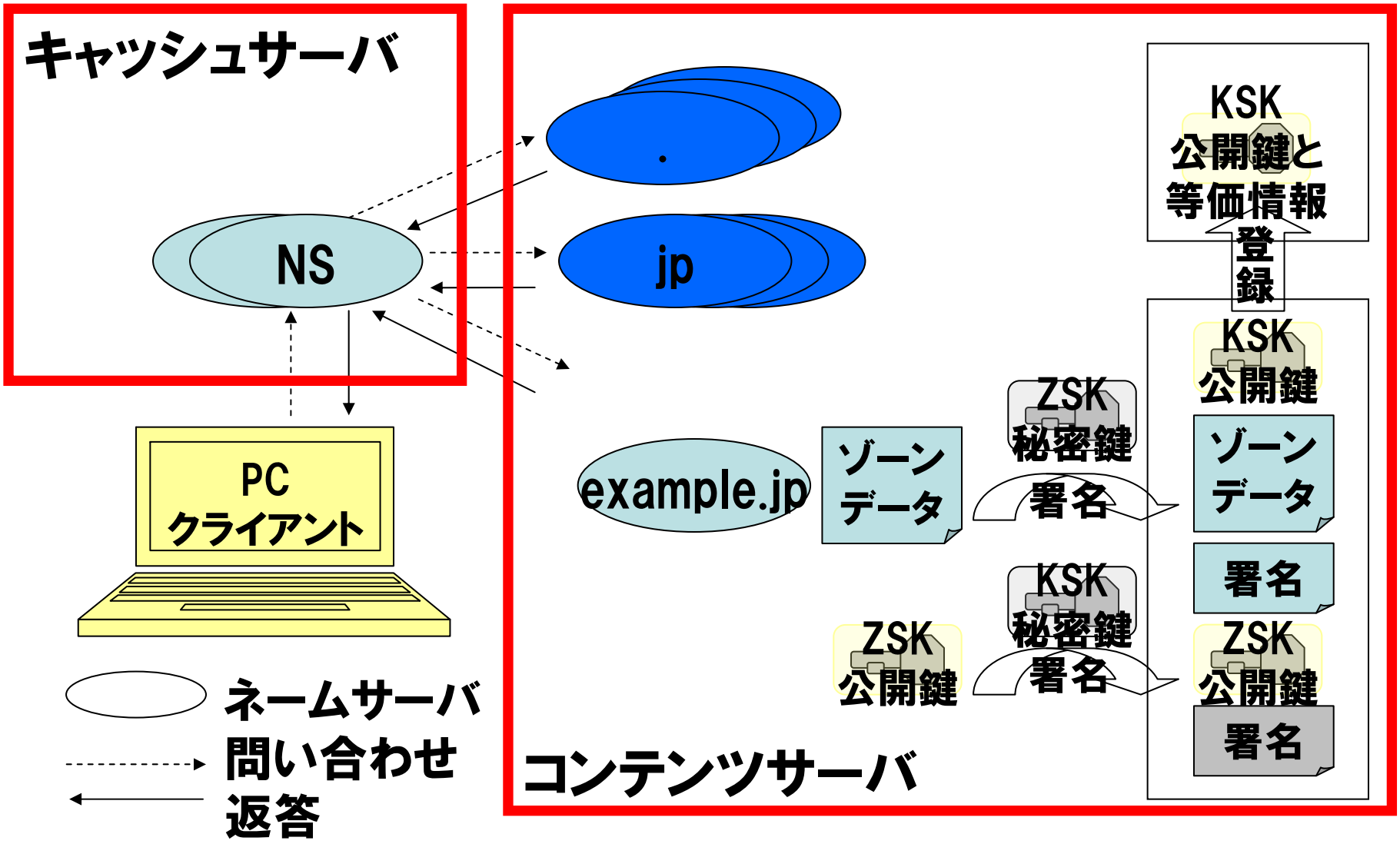
DNSSECの2つの鍵

- 2つの鍵対(4つの鍵)を用意
  - ZSK対(秘密鍵と公開鍵)
    - Zone Signing Key
    - DNSのゾーンに署名／署名検証をするための鍵対
    - 秘密鍵:DNSのゾーンに署名する
    - 公開鍵:DNSの自ゾーンに登録
  - KSK対(秘密鍵と公開鍵)
    - Key Signing Key
    - ZSKに署名／署名検証するための鍵対
    - 秘密鍵:ZSKに署名する
    - 公開鍵:DNSの自ゾーンに登録するとともに等価な情報を上位ゾーンに登録する

ZSKとKSK

- 2つの鍵対が必要な理由
  - 条件
    - 鍵には賞味期限がある
    - 賞味期限が長い鍵は利用のコストが大きい
    - 上位ゾーンに鍵を登録してもらわないといけない
  - 鍵を2つに分けることにより鍵の管理を容易に
    - 上位に登録する鍵は賞味期限が長い鍵が望ましい
      ⇒KSK（長い鍵長、更新頻度低）
    - データ（ゾーン）の署名にはコストが小さい鍵が望ましい
      ⇒ZSK（短い鍵長、更新頻度高）

DNSSECの構造


キャッシュサーバ
NS
PC
クライアント
.
jp
example.jp
ゾーン
データ
ZSK
秘密鍵
署名
KSK
公開鍵と
等価情報
登録
KSK
公開鍵
ゾーン
データ
署名
KSK
秘密鍵
署名
ZSK
公開鍵
ZSK
公開鍵
署名
コンテンツサーバ
ネームサーバ
問い合わせ
返答

DNSSECの構造

- 信頼の連鎖
  - 上位ゾーンにはKSKの公開鍵と等価な情報（ハッシュ値）を登録
  - 当該ゾーンには以下を登録
    - ゾーンのデータ
    - KSKとZSKの公開鍵
    - KSKの秘密鍵によって署名したZSKの公開鍵情報
    - 各データをZSKによって署名した情報
- 署名の検証
  - ルートのKSKの公開鍵はDNSSECの検証者が持つ
  - 検証者のことをバリデータ（Validator）と呼ぶ
  - バリデータは通常キャッシュサーバが行う

NSEC

- 存在する名前の検証は署名により可能
- 存在しない名前を検証することは？
  - 存在しない名前（例えばwww1.example.jp）が存在しないことを検証できなければ不十分
- 存在しないことを検証する手段がNSEC
  - ゾーンのデータをある規則でならべて次のデータへのリスト構造を持つことにより次のデータが異なれば存在しないことがわかる：
    www.example.jp
    www0.example.jp
    www2.example.jp
    となっていればwww1.example.jpがないことがわかる

NSEC3

- NSECの大きな問題
  - リスト構造をたどればドメインを芋づるしきにたどることができる
  - そのドメインの構造がわかってしまう
  - セキュリティ上の問題
- NSECの問題を解決するために考えだされたのがNSEC3
  - リスト構造を構築する前にデータをある方法により元の名前が推測できないようにする
  - 一方向性ハッシュ関数を用いて変換する
- 今後TLDにおいてはNSEC3が主流となる見込み

DNSSEC

- ソフトウェアの実装
  - NSEC対応の実装
    - BIND 9.3.0 以降
      - コンテンツサーバとキャッシュサーバ
    - NSD 2.0.0 以降
      - コンテンツサーバのみ
    - Unbound
      - キャッシュサーバのみ
  - NSEC3対応の実装
    - BIND 9.6.0 以降
    - NSD 3.0 以降
    - Unbound

DNSSECを支えるツール

- DNSSECの運用は非常に複雑
  - 二つの鍵の管理
  - ゾーンデータへの署名と更新
  - 特に標準的なソフトウェアだけでの運用は困難
- DNSSECの運用を支援するツールが提供されている
  - OpenDNSSEC http://www.opendnssec.org/

DNSSECの現状

ルートゾーンの対応

- インクリメンタル・ロールアウト http://www.root-dnssec.org/
  - 段階的かつ慎重な導入
  1. 2009年12月: 内部的な署名と検証開始
     ICANNとVerisignによりルートゾーンのレジストリシステム内部において内部検証のために署名
  2. 2010年1月27日: L-rootにのみダミーの署名データ(DURZ)※を導入
     影響がないことを確認
  3. 2010年1月～2010年5月: 他のルートサーバにダミーの署名を順次導入
     2010年2月10日 A-root
     2010年3月　3日 M-root、I-root
     今後の予定
     2010年3月24日 D-root、K-root、E-root
     2010年4月14日 B-root、H-root、C-root、G-root、F-root
     2010年5月　5日 J-root
  4. 2010年5月～6月:ダミーの署名の影響を評価し最終的に判断
  5. 2010年7月1日: DURZを正規の署名データに差し換え

(※) DURZ:Deliberately-Unvalidatable Root Zone

TLDにおける状況

- すでに署名済みのTLD：25-35
  - .seがDNSSECに最も積極的に取り組む
- .org は2009年に署名
  - 現状では最も大規模な署名済みTLD
- .com (最大のTLD) は2011年に署名予定
- .arpaの署名は2010年3月15日～17日

TLDにおける状況

jPRS JAPAN REGISTRY SERVICES

TLDにおけるDNSSEC対応状況（導入済）

（2010年3月1日現在）

状況	種別	TLD名	特記事項
導入済	ccTLD	SE（スウェーデン）	・2005年9月に導入開始、世界で最初にDNSSEC対応したTLD ・2009年1月から料金を無料化 ・これまでに多くのノウハウを外部に発信
		PR（プエルトリコ）	・2006年8月に導入開始
		BG（ブルガリア）	・2007年1月に導入開始
		BR（ブラジル）	・2007年6月に導入開始、2009年1月に全属性で対応 ・最新方式（NSEC3）を採用した最初のTLD
		CZ（チェコ）	・2008年9月に導入開始
		TH（タイ）	・2009年3月に導入開始、アジアで最初にDNSSEC対応したccTLD
		TM（トルクメニスタン）	・2009年10月に導入開始
		US（アメリカ）	・2009年12月に導入開始
		PT（ポルトガル）	・2010年1月に導入開始
		CH（スイス）	・2010年2月に導入開始
		LI（リヒテンシュタイン）	・2010年2月に導入開始
		UK（イギリス）	・プロトコル策定・IANAとの共同実験など積極的に活動 ・2010年3月に導入開始
	gTLD	MUSEUM	・2008年9月に導入開始
		GOV（米国政府）	・2009年2月に導入開始、2009年末に全組織が対応予定
		ORG	・2009年6月に導入開始、2010年に本サービス化予定

国内外でのDNSSECに関する検討状況
http://jprs.jp/advisory/material/31/a3.pdf より引用

TLDにおける状況

JPRS JAPAN REGISTRY SERVICES

TLDにおけるDNSSEC対応状況（導入予定）

（2010年3月1日現在）

状況	種別	TLD名	特記事項
導入を表明（非公式含む）	ccTLD	CA（カナダ）	・2009年10月にテストベッドを開始
		CL（チリ）	・2010年中に導入予定
		CN（中国）	・2010年末までに導入予定
		DE（ドイツ）	・2010年1月にテストベッドを開始
		GR（ギリシャ）	
		JP（日本）	・2010年を目処に導入予定
		KR（韓国）	・2010年6月に導入し、2011年1月に全空間で対応予定
		MY（マレーシア）	・2010年第4四半期に導入予定
		NL（オランダ）	・2010年8月に導入予定
		RU（ロシア）	
	gTLD	BIZ	・2010年第1四半期に導入予定
		CAT	・2009年中に導入予定
		COM	・2011年の早い時期に導入予定
		EDU	・2010年3月末に導入予定
		INFO	・2010年中に導入予定
		NET	・2010年末までに導入予定

国内外でのDNSSECに関する検討状況
http://jprs.jp/advisory/material/31/a3.pdf より引用

.JPの対応

- 「JPドメイン名サービスへのDNSSECの導入予定について」
  2009年7月9日公開
  「JPRSでは、DNSのセキュリティ拡張方式であるDNSSECを、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」
- 導入・普及に向けた活動
  - 権威DNSサーバ運用者
    - ルートDNS運用者
    - 他のTLDレジストリ
    - 日本国内のそれぞれのドメイン名のDNSサーバ運用者
  - キャッシュDNSサーバ運用者
  - JPドメイン名指定事業者
  - インターネット利用者

http://jprs.jp/info/notice/20090709-dnssec.htmlより引用

日本におけるDNSSECの普及

- DNSSECの普及にはDNSの運用面だけではなく、多くの関係者の協力が必要
  - レジストリ
  - レジストラ
  - ドメイン名登録者
  - DNSオペレータ(コンテンツサーバ・キャッシュサーバ)
  - ネットワークオペレータ
  - 各種機器ベンダー/HGW開発者
- さまざまなアプローチによる普及活動か必要
  - JPRSによる普及活動
  - DNSSECジャパンによる普及活動

JPRSによる普及活動

- JPRS単独での検証(～2009年11月)
  - DNSSECの基本機能確認
  - DNSSEC導入時のDNSサーバへの影響検証
- 他組織(IIJ, JPNIC, WIDE, NII)が運用するJP DNSサーバでの検証(2009年11月～)
  - 海外拠点など遠隔地への転送検証、高負荷時の機能検証
  - DNSサーバの応答内容検証、転送検証の追加実施(予定)
- 各種プレイヤーと連携した検証(2010年1月～)
  - 複数の大手ISPと、DNSサーバ(問合せ側)への影響検証等の実施(継続)
  - 機器ベンダー数社と、ネットワーク機器に対するDNSSEC対応検証の実施(継続)
  - 指定事業者と、DNSSECサービス導入への機能検証等の実施(予定)
  - 関連団体へのDNSSEC導入の啓発と技術検証への参加の働きかけ
  - DNSSEC導入者向けの、DNSSEC機能確認手順書の作成、公開(予定)

国内外でのDNSSECに関する検討状況
http://jprs.jp/advisory/material/31/a3.pdf より引用

DNSOPS.jp
DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECジャパン

- 2009年11月24日設立
- 設立趣意
  DNSのセキュリティを向上させるDNSSECについて、その導入ならびに普及のために、ドメイン名登録管理事業者、ドメイン名取扱事業者、ドメイン名登録者、DNS運用者、ネットワーク運用者などの関係者が集う場として「DNSSECジャパン（DNSSEC.jp）」を設立する。 DNSSEC.jpは参加者による相互扶助の活動を原則とする。
- 目的
  DNSSECの導入・運用に関する課題の整理と検討を行い、参加者の技術力の向上、ノウハウの共有を促進するとともに、ツールの提供や普及のための技術解説などの対外活動も行う。
- URL: http://dnssec.jp/
- **参加組織は随時募集中**

DNSOPS.jp
DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECジャパン

- 活動内容
  - DNSSECの導入・運用に関する課題の整理・共有
  - DNSSECの導入・運用に関する技術検証の実施、ノウハウの蓄積
  - DNSSECの導入・運用に関するBCPの策定
  - 成果の対外的発信によるDNSSECの普及・啓発
- 組織
  - 部会(WG)による活動が主体
    - 技術検証WG
    - 広報WG
    - DNSSEC運用ワークショップ
      - 運用技術SWG
      - プロトコル理解SWG
- 活動状況
  - DNSSECに関する理解を深めるためにDNSSEC運用ワークショップの活動開始
  - ワークショップの内容についてはTwitterやU-Streamによる中継の試み

DNSOPS.jp
DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECジャパン

組織名
GMOホスティング＆セキュリティ株式会社
一般社団法人JPCERTコーディネーションセンター
NECビッグローブ株式会社
NeuStar Inc. (www.neustar.biz, www.neustarregistry.biz)
NRIセキュアテクノロジーズ株式会社
株式会社NTTPCコミュニケーションズ
NTTコミュニケーションズ株式会社
株式会社ＳＴＮｅｔ
株式会社インターネットイニシアティブ
株式会社インターネット総合研究所
インターネットマルチフィード株式会社
株式会社エヌ・ティ・ティ・データ三洋システム
さくらインターネット株式会社
ソフトバンクBB株式会社
ソフトバンクテレコム株式会社
株式会社ディーネット
日本インターネットエクスチェンジ株式会社
日本DNSオペレーターズグループ
財団法人日本データ通信協会Telecom-ISAC Japan
社団法人日本ネットワークインフォメーションセンター
株式会社日本レジストリサービス
株式会社ライブドア

- 会員数:22

•『DNSSECの導入・普及へ、「DNSSECジャパン」設立』
http://internet.watch.impress.co.jp/docs/news/20091125_331241.html

DNSSECジャパンの今後の予定

2009/11/24 DNSSECジャパン
（DNSSEC.jp）設立総会
2010/上半期 ワークショップの開催
プロトコル理解、運用技術
広報体制の整備
実験計画策定・準備
2010/下半期 実験実施・運用ノウハウの共有
2011/3 総会

DNSOPS.jp
DNS Operators Group, Japan

jpix Japan Internet Exchange

DNSSECの普及に向けた課題

DNSSECの普及の困難性

- 自ドメイン内に閉じていない
  - 上位ゾーン(レジストリ／レジストラ)との署名鍵情報のやりとり
- BCPが不十分
  - 鍵長、鍵の期限、鍵の更新の仕組み
- クライアント側での対応が不十分
  - キャッシュサーバとエンドクライアントの役割分担
  - エンドクライアントのDNS問い合わせを守る手段
- 費用の問題
  - DNSSECの署名鍵情報の登録にともなう費用はどうなるか
  - レジストリ側、レジストラ側
- DNSを利用した広域負荷分散

⇒課題は山積ながらDNSSECに向け舵が切られている

DNSSEC普及に関する懸念事項

- EDNS0によるUDPパケット長の変化
  - フラグメントの問題
- DNSSECのための負荷の増大
  - コンテンツサーバにおける署名の負荷
  - キャッシュサーバにおける検証の負荷
  - 署名に関するデータ量の負荷
- 検証が失敗した場合にSERVFAILとなる
- キャッシュサーバ・エンドクライアント間のセキュリティ
- DNSの外の問題について
  - 署名鍵を誰がどのように管理するのか
- 費用と運用負荷

Hot Topics

- ComCastの対応
  - アメリカ最大のケーブルTV事業者がDNSSECへの対応を表明
- DNSSEC vs. DNSCurve
  - DJB氏がDNSCurveという別のアイデアを提示および実装
  - そもそもDNSSECと排他的かどうか
  - IETFやその周辺で議論がおきている