DNSSECをとりまく状況

2009年11月24日
DNS DAY @ Internet Week 2009

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
インターネット推進部　部長
前村　昌紀　　maem@nic.ad.jp

JPNIC 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

基本事項のおさらい

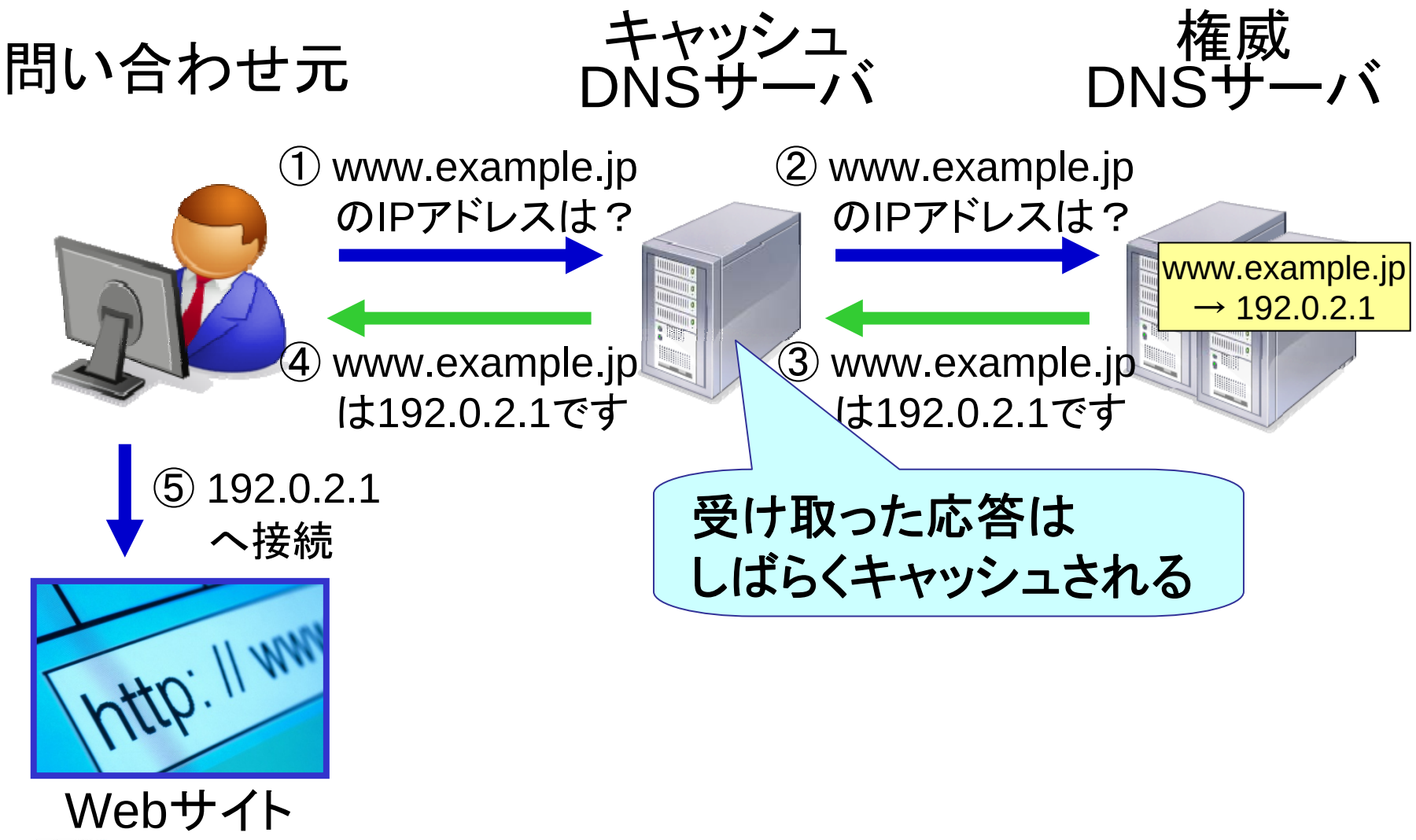
DNSSECをとりまく状況

DNS DAY @ Internet Week 2009

JPNIC前村

2009年11月24日

正常なアクセス（1回目）



正常なアクセス（2回目以降）

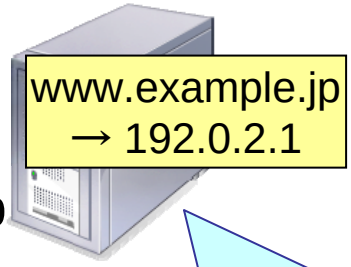
問い合わせ元

キャッシュDNSサーバ

権威DNSサーバ

① www.example.jp のIPアドレスは？

② www.example.jp は192.0.2.1です

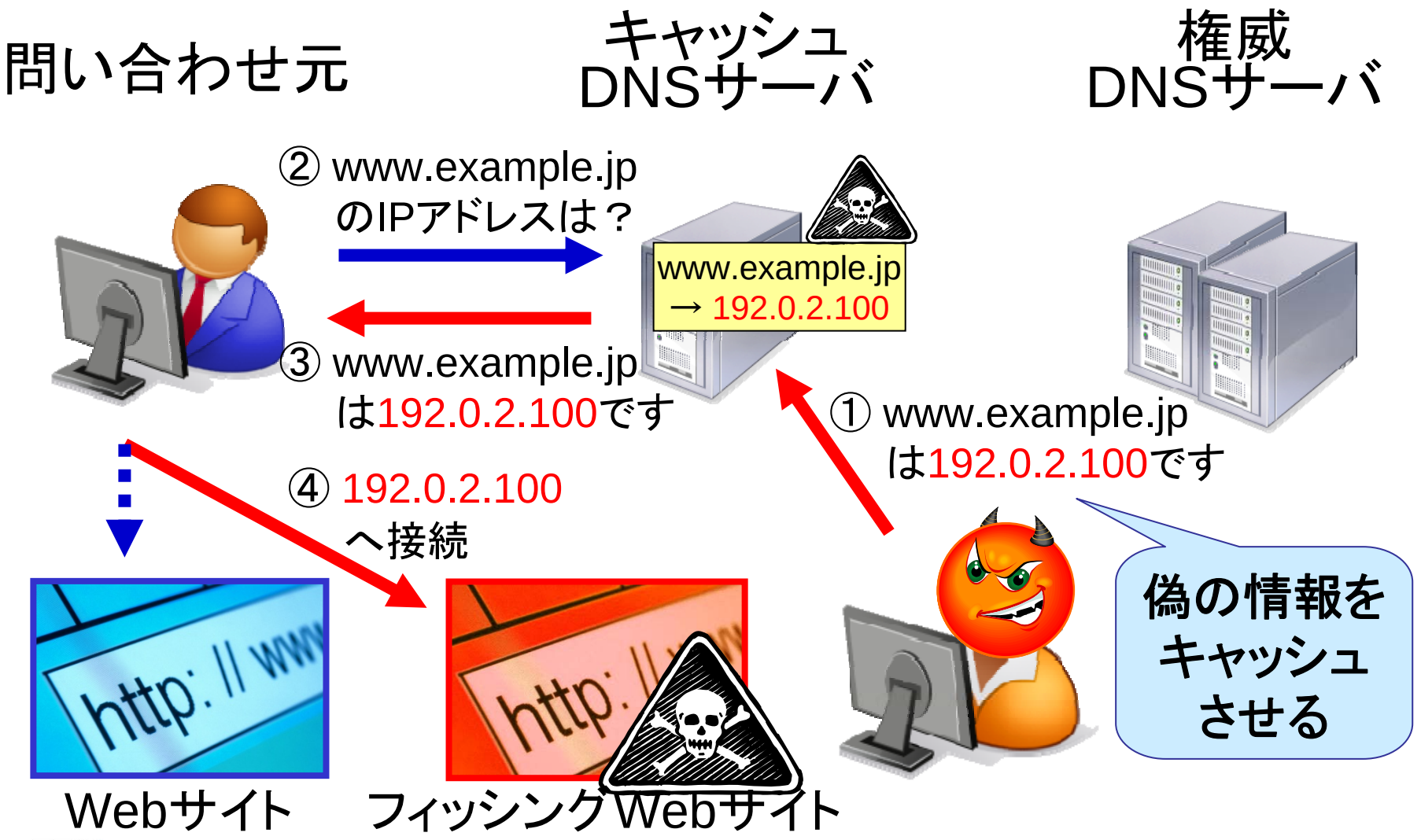


③ 192.0.2.1 へ接続

Webサイト

以前のアクセスと情報が一致していれば、キャッシュサーバで応答する

DNSへの毒入れ攻撃



DNS毒入れ攻撃

- ユーザが正常なアクセスを行っても、フィッシングサイトに誘導される
  - 攻撃されたことに気づきにくい
- 同じキャッシュサーバのユーザ全員が影響を受ける
  - ISPのキャッシュサーバが攻撃されると被害は甚大
- 攻撃そのものの検出が容易ではない
  - キャッシュへの毒入れは、見た目は通常のDNSパケットであるため、正常な応答と攻撃の区別が簡単ではない
- 危険性が高まった
  - 2008年夏に毒入れ攻撃の成功率を飛躍的に高める手法が公開された。

    → Kaminsky型の攻撃手法

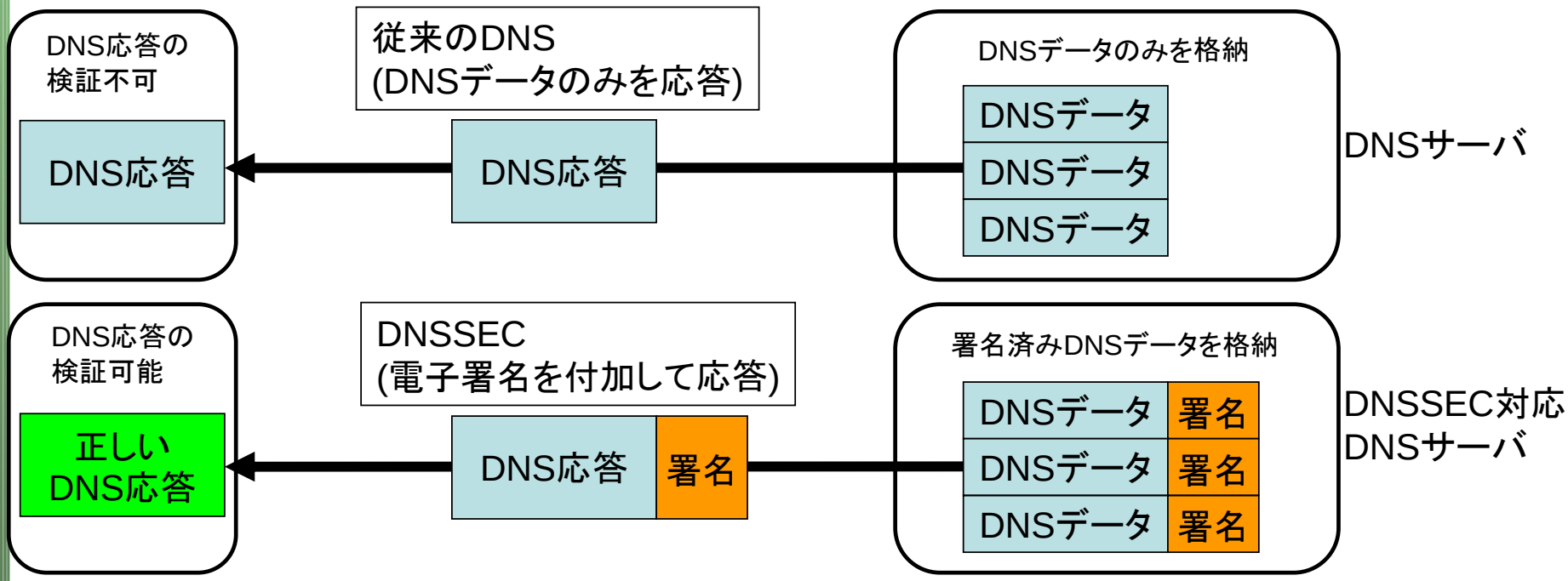
JPNIC

どう対応するか

- 毒入れはDNSプロトコルそのものが持つ脆弱性
  - UDPを使う、IDが16bitしかない、etc…
  - 特にKaminsky型の攻撃は、ブルートフォースアタックによる毒入れ攻撃手法で、未対策かつオープンリゾルバは極めて危険
- 完全対処にはDNSのセキュリティ面でのプロトコル拡張が必要
  ⇒ このための技術がDNSSEC

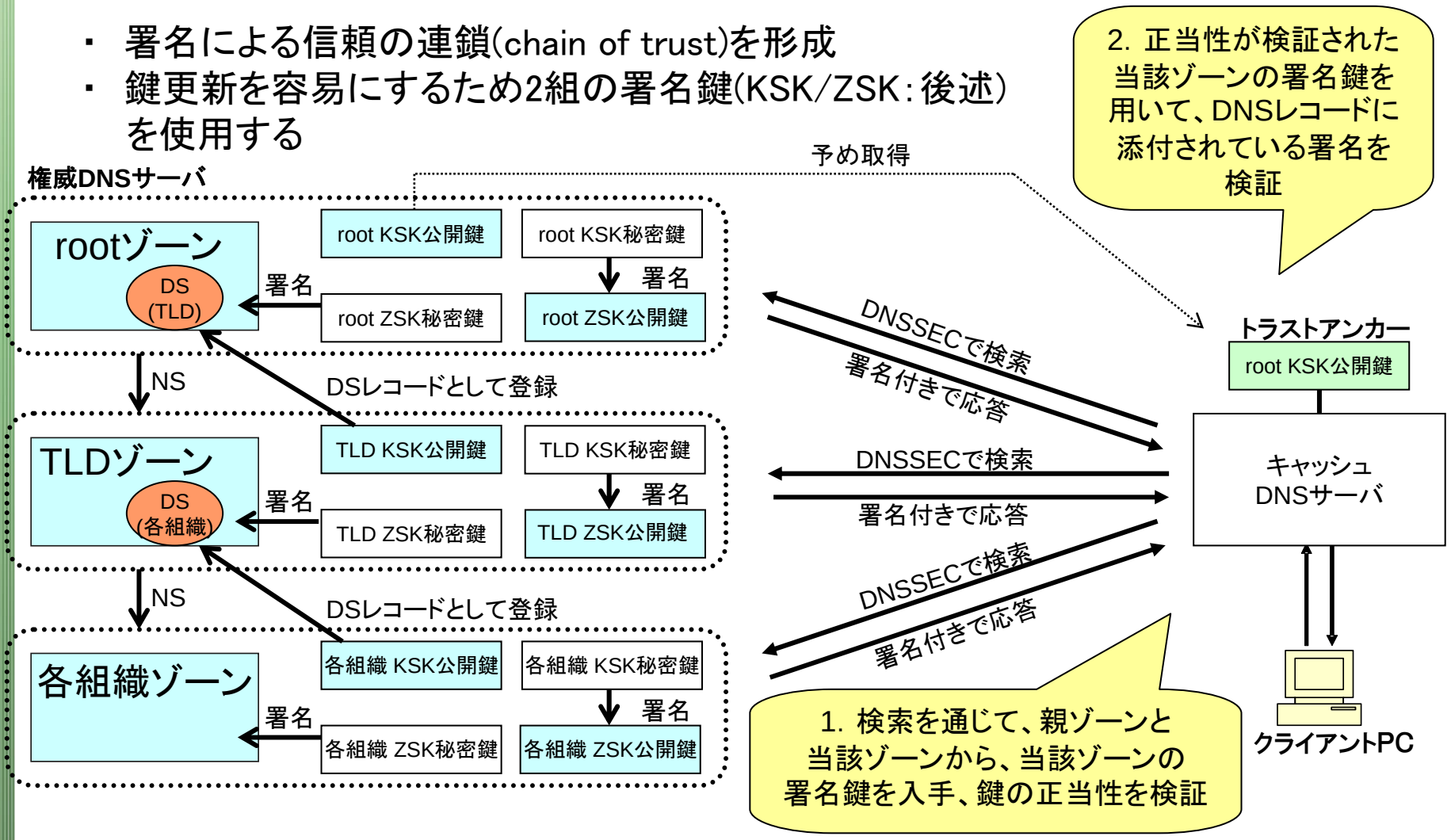
DNSSECとは

- DNSのセキュリティ機能拡張（DNS Security Extensions）
- DNSサーバは、応答に電子署名を付加し、出自を保証
- 利用者側で、DNS応答の改ざん有無を検出できる



DNSSECの信頼の連鎖

- 署名による信頼の連鎖(chain of trust)を形成
- 鍵更新を容易にするため2組の署名鍵(KSK/ZSK：後述)を使用する



世界的な動向

DNSSECをとりまく状況

DNS DAY @ Internet Week 2009

JPNIC前村

2009年11月24日

TLDにおけるDNSSEC対応状況

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
		.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
	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

TLDにおけるDNSSEC導入予定

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
		.ch（スイス）	・2009年9月実地検証開始、2010年2月サービスイン予定
		.cn（中国）	・2010年末までに導入予定
		.de（ドイツ）	・2009年5月にテストベッドを開始
		.gr（ギリシャ）	
		.jp（日本）	・2010年中を目処に導入予定
		.kr（韓国）	・2010年6月に導入し、2011年1月に全空間で対応予定
		.li（リヒテンシュタイン）	・2009年9月実地検証開始、2010年2月サービスイン予定
		.my（マレーシア）	・2010年第4四半期に導入予定
		.ru（ロシア）	
		.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

JPNIC

TLDにおけるDNSSEC導入予定

状況	種別	TLD名	特記事項
導入を表明 （非公式含む）	gTLD	.biz	
		.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月末に署名予定
		.info	
		.net	・2010年末までに時期に導入予定

RIRs(逆引き)におけるDNSSEC導入予定

状況 種別	RIR名	特記事項
導入済み	RIPE NCC	2005年にサービス開始済み
	ARIN	2009年7月1日ゾーン署名完了。2010年サービス開始予定
未導入	APNIC	調査・準備中。具体的な導入計画はなし
	AfriNIC	
	LACNIC	

DNSSEC導入後のルートゾーン管理における ICANN, NTIA, VeriSignの役割と関係

ICANN
IANA Functions Operator

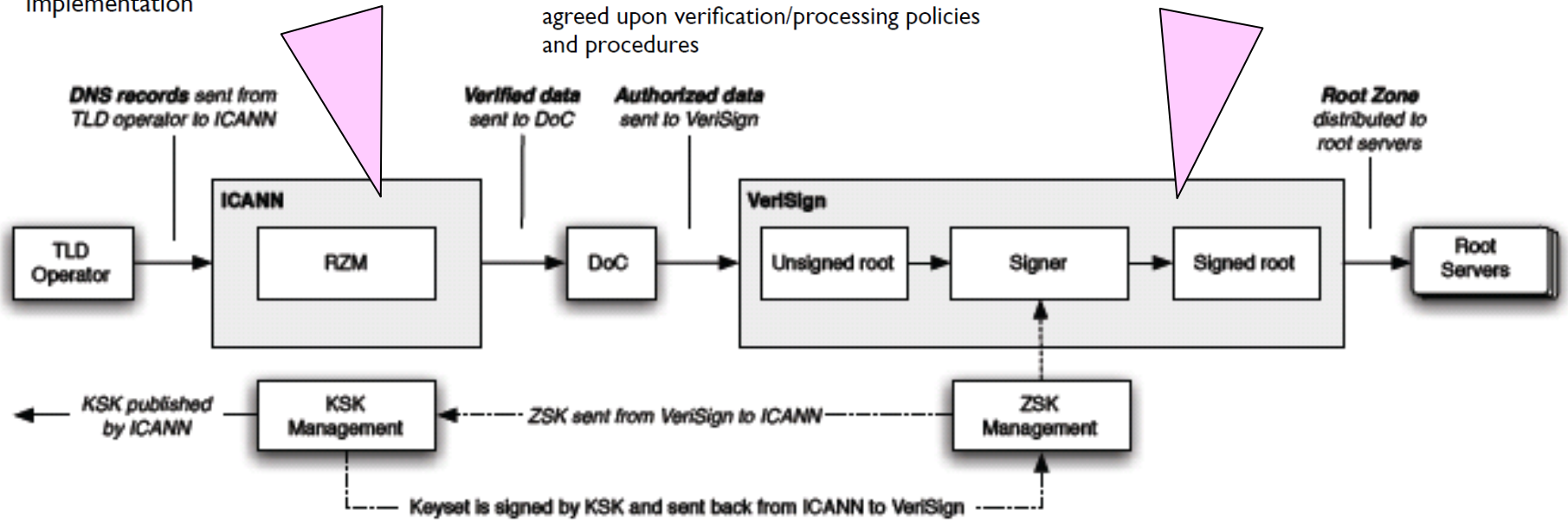
- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC for authorization and to VeriSign for implementation

DoC NTIA
U.S. Department of Commerce
National Telecommunications and Information Administration

- Authorizes changes to the root zone
  - DS records
  - Key Signing Keys
  - DNSSEC update requests follow the same process as other changes
- Checks that ICANN has followed their agreed upon verification/processing policies and procedures

VeriSign
Root Zone Maintainer

- Manages the Zone Signing Key (ZSK)
- Incorporates NTIA-authorized changes
- Signs the root zone with the ZSK
- Distributes the signed zone to the root server operators

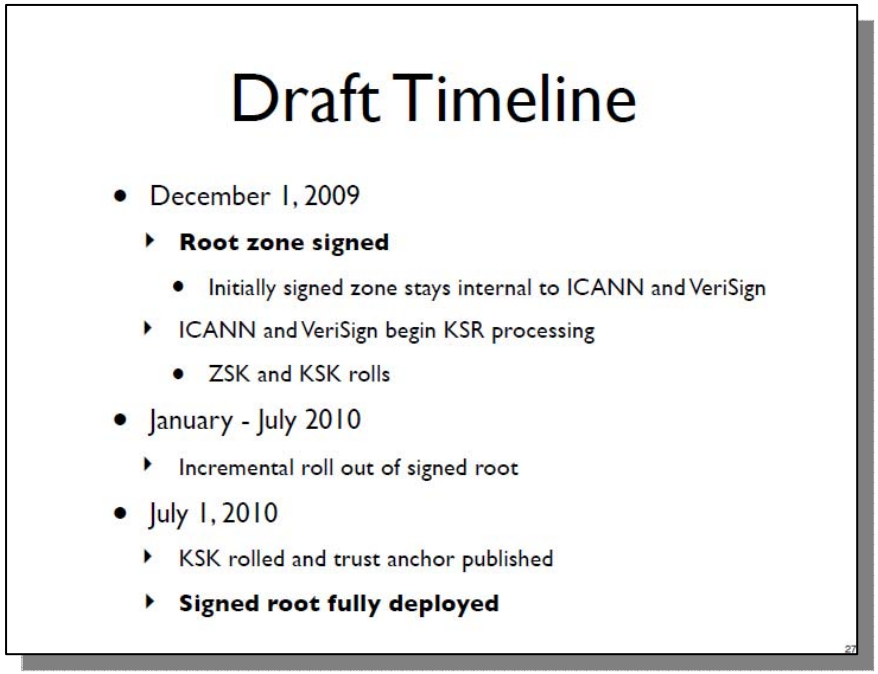


http://sel.icann.org/meetings/seoul2009/presentation-dnssec-workshop-lamb-28oct09-en.pdf

ルートゾーンのDNSSEC対応状況

- 2009年10月現在のタイムライン案:

- 2009年12月
  - ルートゾーンを署名
- 2010年1月—7月
  - A—Mに対して順次展開
- 2010年7月
  - 展開完了
  - トラストアンカーを公開



http://sel.icann.org/meetings/seoul2009/presentation-dnssec-workshop-lamb-28oct09-en.pdf

ルートゾーンのスケーラビリティ問題(1/2)

- DNSSECは、新TLDs，IDN TLDs，IPv6とともに、ルートゾーンのスケーラビリティに対する脅威要素
- RRやゾーンファイルのサイズより、ゾーンの更新頻度のほうがスケーラビリティに対する影響大

Effects of Root Zone Changes

	New TLDs	DNSSEC	IDNs	IPv6 addresses
Increases number of TLD entries in the root zone	X		X	
Increases size of the root zone file	X	X	X	X
Increases amount of data per TLD		X	X	X
Increases number of variables per TLD		X		X
Increases number of changes per TLD per year		X		X

20

Types of Stress

- Zone size
  - In itself not much of a problem ...
  - ... but a bigger zone leads to ...
- Zone volatility
  - Affects the volume of data per unit of time that needs to be transferred from the distribution masters to the individual root servers.

13

http://sel.icann.org/meetings/seoul2009/presentation-scaling-the-root-summary-findings-28oct09-en.pdf

ルートゾーンのスケーラビリティ問題(2/2)

- プロビジョニング(ゾーンファイル生成)サイド:ヒューマンプロセスが大きく影響
- 公開(ゾーンファイル転送)サイド:ネットワーク環境が大きく影響
  - 但し、定量的な考察はまだまだ足らない

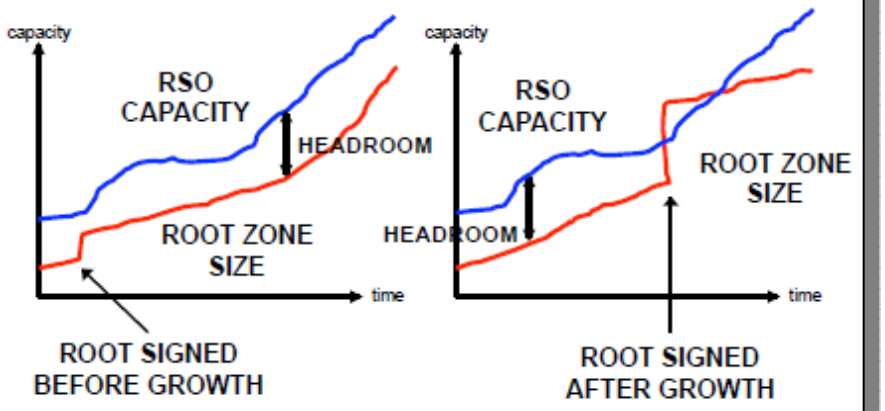
Findings

- On the **provisioning side**, the ability to scale the root is completely dominated by the steps that involve **human intervention**.
- On the **publication side**, scaling the root primarily **affects poorly-connected** Internet locations.
- The risks associated addition of a **few hundred TLDs can be managed** without changing any actor's current arrangement.
- The risks associated with an **annual increase in the size of the root zone** on the order of thousands of new entries can be managed **only with changes to the current arrangements** of one or more actors.

18

Root Server Operator Headroom

Impact as factor of zone size

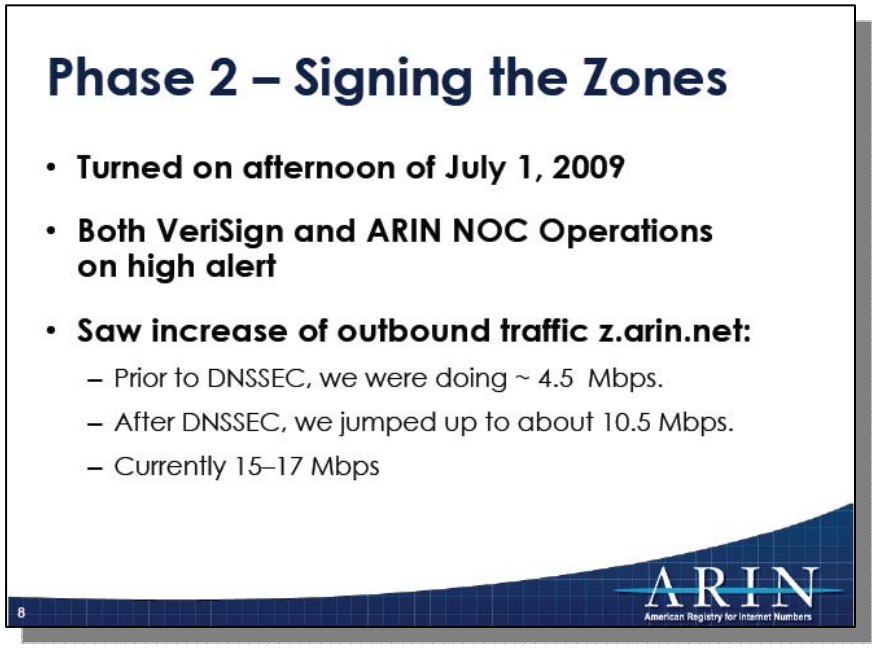


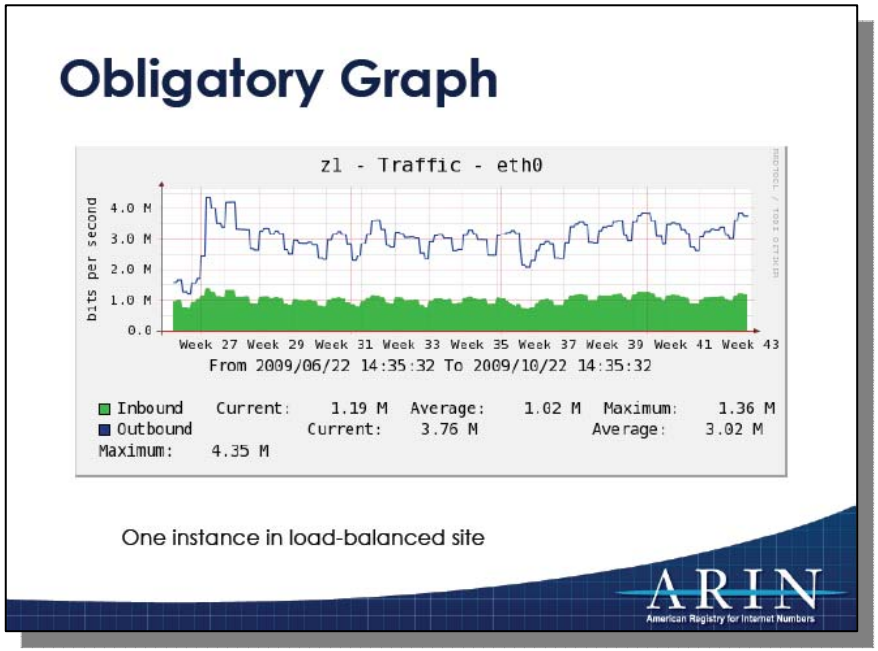
19

http://sel.icann.org/meetings/seoul2009/presentation-scaling-the-root-summary-findings-28oct09-en.pdf

ゾーン署名によるトラフィックの変化

- ARINの例
  - 2—3倍が観測されている





http://sel.icann.org/meetings/seoul2009/presentation-dnssec-workshop-kosters-28oct09-en.pdf

ありがとうございました。

DNSSECをとりまく状況

DNS DAY @ Internet Week 2009

JPNIC前村

2009年11月24日