DNSSECの仕組みと現状

平成22年11月

DNSSECジャパン

アジェンダ

1. DNSとは
2. DNSの動作
3. DNSSECとは
4. DNSSECの動作
5. DNSSECの現状
6. 参考URL
7. DNSSEC関連RFC

DNSとは

- DNS(Domain Name System)とは、ホスト（ドメイン）名をIPアドレスに。 IPアドレスをホスト（ドメイン）名に変換する仕組み。

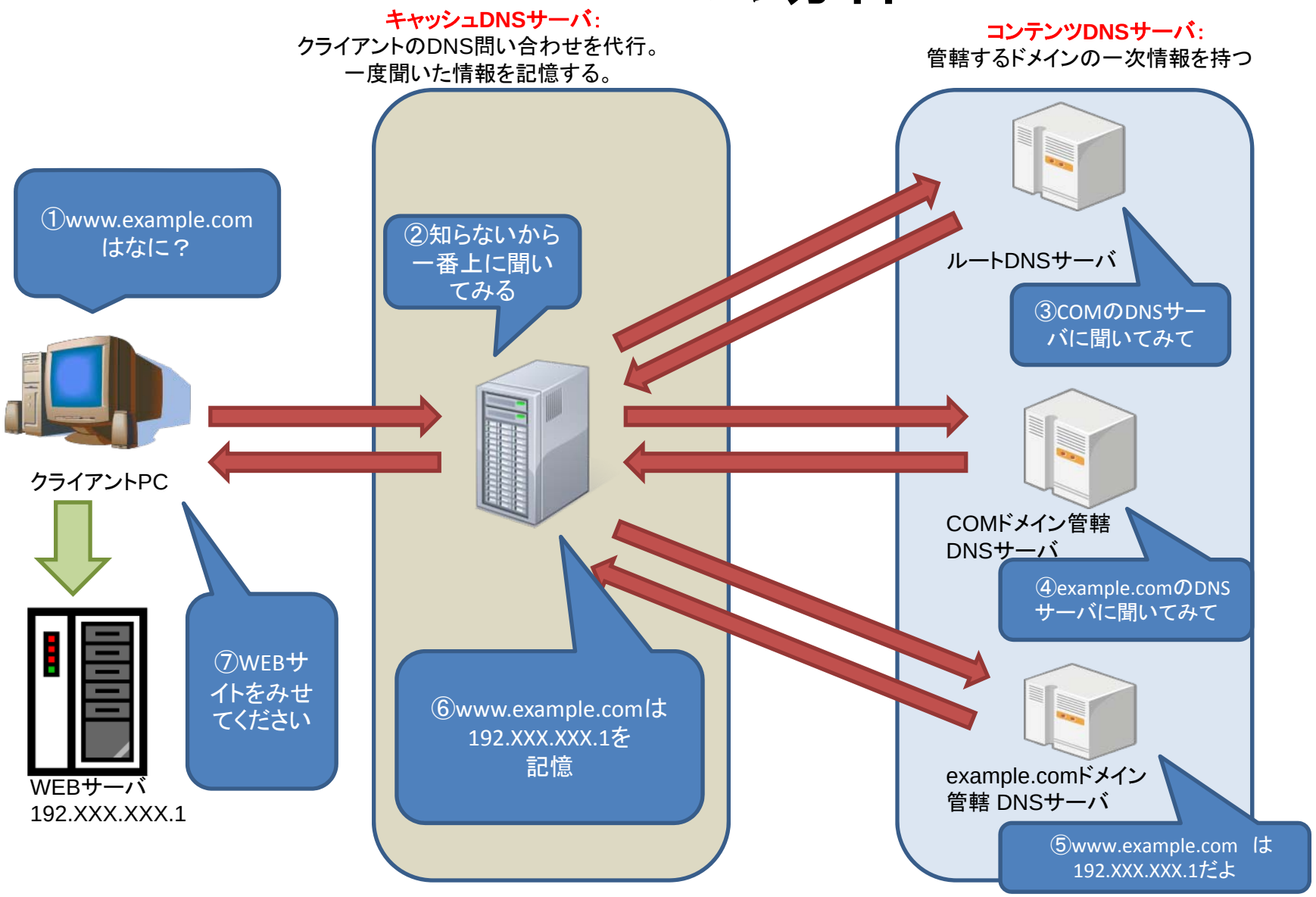
- www.example.comのWebサイトが見たい場合はブラウザのURL欄にwww.example.comと入力する。
するとそのWebサイトにたどり着けますが、実はその裏でDNSが動作し、IPアドレスを取得しているのです。

DNSとは

- DNSは階層化されており、最上位のルートDNSサーバから順番に下位DNSに問い合わせると、存在するドメインは必ず返答が返ってきます。（次ページ参照）

- しかし、毎回DNSサーバに問い合わせると負荷がかかる為、キャッシュサーバと呼ばれるサーバが一度問い合わせたドメインを記憶しています。
（次ページ参照）

DNSの動作

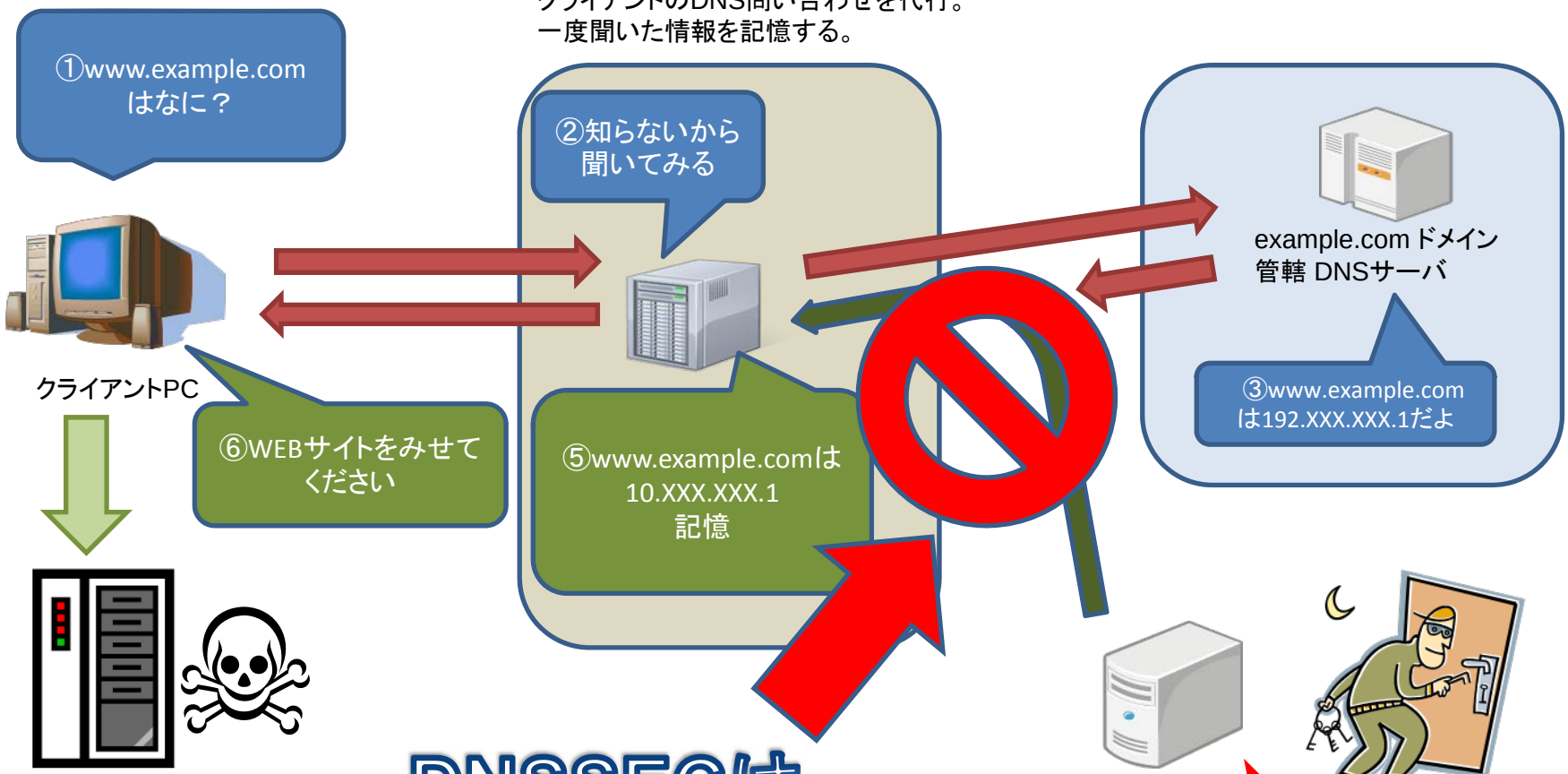

キャッシュDNSサーバ:
クライアントのDNS問い合わせを代行。
一度聞いた情報を記憶する。
コンテンツDNSサーバ:
管轄するドメインの一次情報を持つ
①www.example.com
はなに？
②知らないから
一番上に聞い
てみる
ルートDNSサーバ
③COMのDNSサー
バに聞いてみて
クライアントPC
COMドメイン管轄
DNSサーバ
④example.comのDNS
サーバに聞いてみて
⑦WEBサ
イトをみせ
てください
⑥www.example.comは
192.XXX.XXX.1を
記憶
example.comドメイン
管轄 DNSサーバ
⑤www.example.com は
192.XXX.XXX.1だよ
WEBサーバ
192.XXX.XXX.1

DNSSECとは

- DNSSEC（DNS Security Extensions)とはDNSへの毒入れ攻撃（キャッシュポイズニング）に対処するための技術です。
  - キャッシュポイズニングとは、キャッシュサーバに偽の応答をキャッシュさせることで、ユーザを本来意図していたWebサイトとは別のWebサイトなどに誘導する攻撃のことをいいます。
  - 誘導先のサイトで個人情報などを略取される可能性があります。
  - さらに同じキャッシュサーバを利用しているすべてのユーザが影響を受けるので、被害は甚大になります。

DNSSECとは

キャッシュDNSサーバ:
クライアントのDNS問い合わせを代行。
一度聞いた情報を記憶する。



DNSSECは
キャッシュポイズニング
攻撃を阻止！

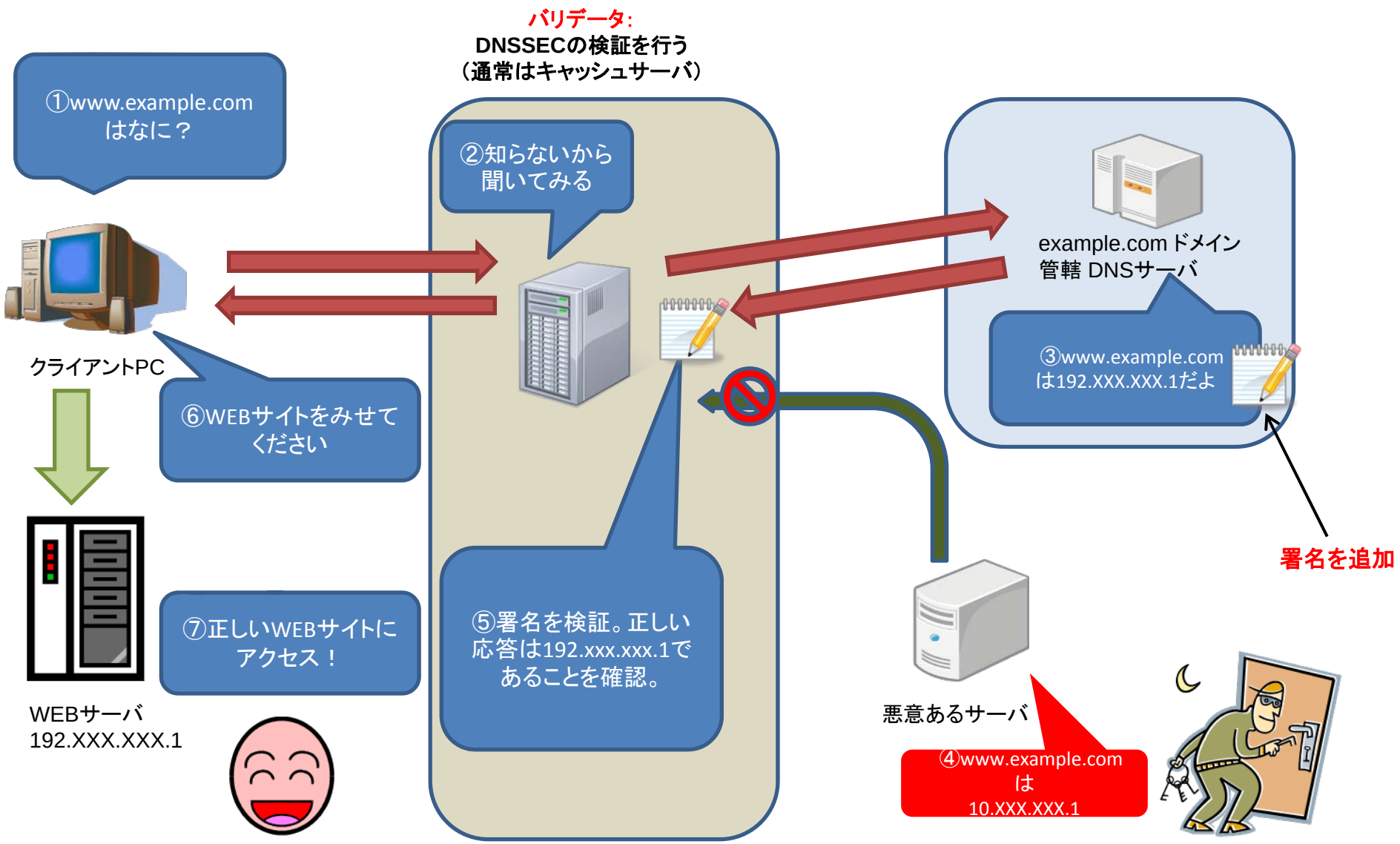
DNSSECの動作

- DNSSECは公開鍵暗号方式と呼ばれる暗号方式と電子署名技術を利用しています。応答を送信するDNSサーバーが秘密鍵を使って応答に署名し、受信する側が公開鍵で検証します。

- 秘密鍵を持っていないと正しく署名を付けられないので、署名の検証によって偽の応答を検知できます。

- 署名の検証は従来のキャッシュDNSサーバに検証（バリデーション）機能を持たせることによって、キャッシュDNSサーバが受け取った情報の出自と完全性を証明します。

DNSSECの動作


バリデータ:
DNSSECの検証を行う
（通常はキャッシュサーバ）
①www.example.com
はなに？
②知らないから
聞いてみる
example.com ドメイン
管轄 DNSサーバ
③www.example.com
は192.XXX.XXX.1だよ
クライアントPC
⑥WEBサイトをみせて
ください
署名を追加
⑤署名を検証。正しい
応答は192.xxx.xxx.1で
あることを確認。
⑦正しいWEBサイトに
アクセス！
WEBサーバ
192.XXX.XXX.1
悪意あるサーバ
④www.example.com
は
10.XXX.XXX.1

DNSSECの現状

- **ルートゾーン対応状況**
  - 2010年7月に導入済
- **gTLD対応状況（2010年10月現在)**
  - .biz .cat .edu .info .museum .org
  - その他も2010年後半～2011年前半で対応予定
- **ccTLD対応状況(2010年10月現在)**
  - .se .be .fi .bg .pr .cz .br .th .na .eu .tm .us .pt .li .ch .uk .lk .hk .nu .kg .pm .md .pn .nl .fr .dk
  - その他約20カ国が2010年後半～2011年前半で対応予定
  - .jpは2010/10/17にJPゾーンへの署名を開始
    2011/1/16にJPドメイン名サービスへの導入を開始予定
- DNSSEC対応状況の最新情報は下記を参照
  - ICANN http://stats.research.icann.org/dns/tld_report/

- 世界中で次々と署名が開始されています。
- JPドメインのDNSSECサービス開始に伴い、国内でも準備をする必要があります。

参考となるURL

- DNSSECジャパン(DNSSEC.jp)
  - http://dnssec.jp/
- JPRS(DNSSEC関連情報）
  - http://jprs.jp/dnssec/
- JPNIC（DNSSEC)
  - http://www.nic.ad.jp/ja/newsletter/No43/0800.html

DNSSEC関連RFC(主要なもの)

- RFC 4033 - DNS Security Introduction and Requirements.
- RFC 4034 - Resource Records for the DNS Security Extensions.
- RFC 4035 - Protocol Modifications for the DNS Security Extensions.
- RFC 4431 - The DNSSEC Lookaside Validation (DLV) DNS Resource Record.
- RFC 4509 - Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs).
- RFC 4641 - DNSSEC Operational Practices.
- RFC 4986 - Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover.
- RFC 5011 - Automated Updates of DNS Security (DNSSEC) Trust Anchors.
- RFC 5074 - DNSSEC Lookaside Validation (DLV).
- RFC 5702 - Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource.
- RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence.
- Internet-Draft - DNSSEC Operational Practices, Version 2.
  (draft-ietf-dnsop-rfc4641bis-02)
- Internet-Draft - DNSSEC Key Timing Considerations.
  (draft-ietf-dnsop-dnssec-key-timing-00)

- DNSSECジャパンRFC資料参照
  - http://dnssec.jp/?page_id=124