2009年12月11日
第30回JPドメイン名諮問委員会
参考資料2

# 国内外でのDNSSECに関する検討状況

2009年12月11日（金）

株式会社日本レジストリサービス

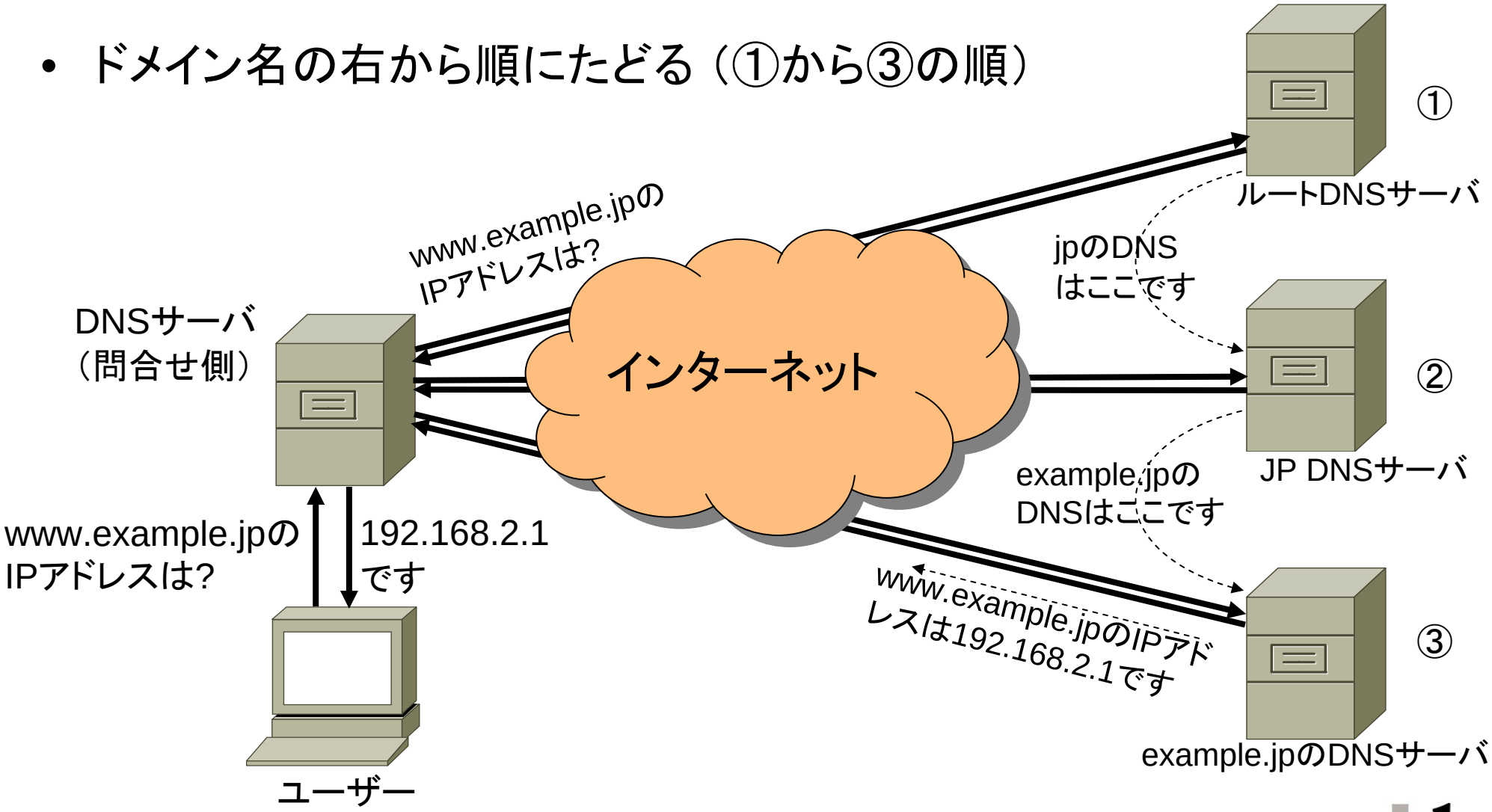
# 目次

1. DNSSECとは（振り返り）
2. 国外の状況
   - 各TLDにおけるDNSSEC対応状況
   - ルートDNSサーバのDNSSEC対応予定
3. 日本国内の状況
   - JPRSの活動状況
   - DNSSECジャパン（DNSSEC.jp）の設立

# 1. DNSSECとは（振り返り）

# DNSの仕組み

- ドメイン名の右から順にたどる（①から③の順）

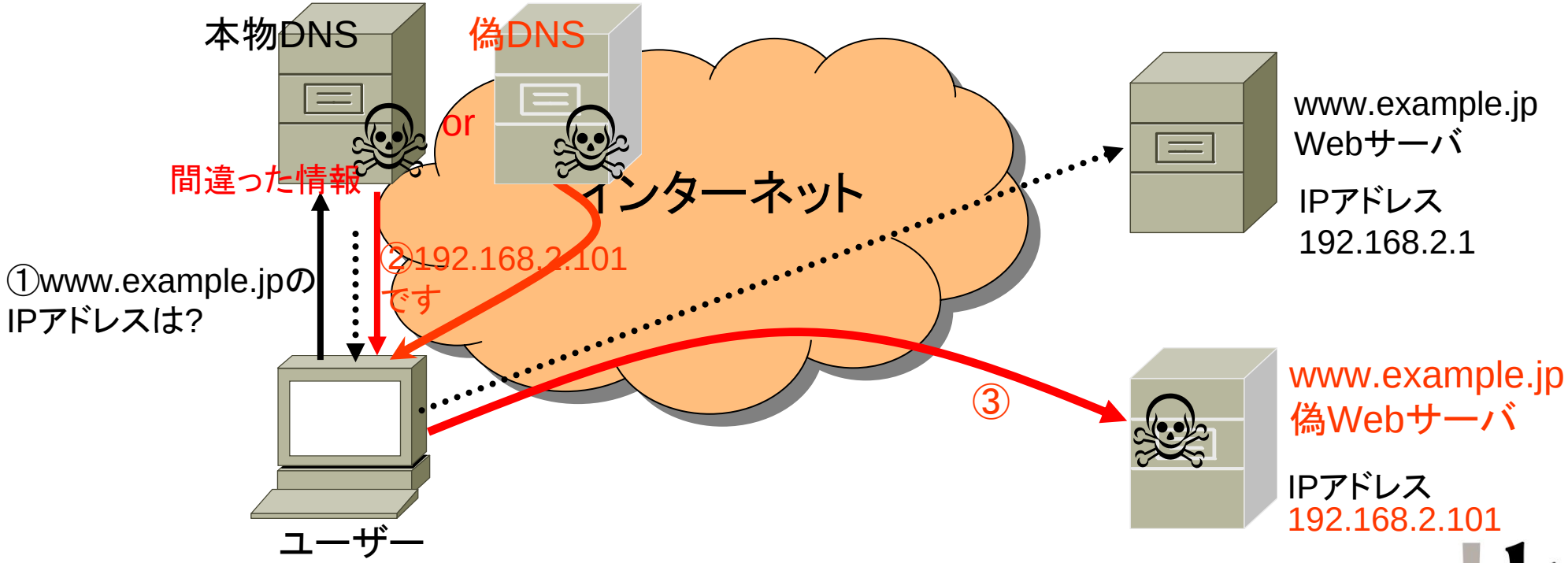


# DNSの応答が偽造されたら

- もし本物のDNSが間違った情報を返したら・・・　または、
- 本物のDNSサーバ以外から来た応答を信じてしまったら・・・

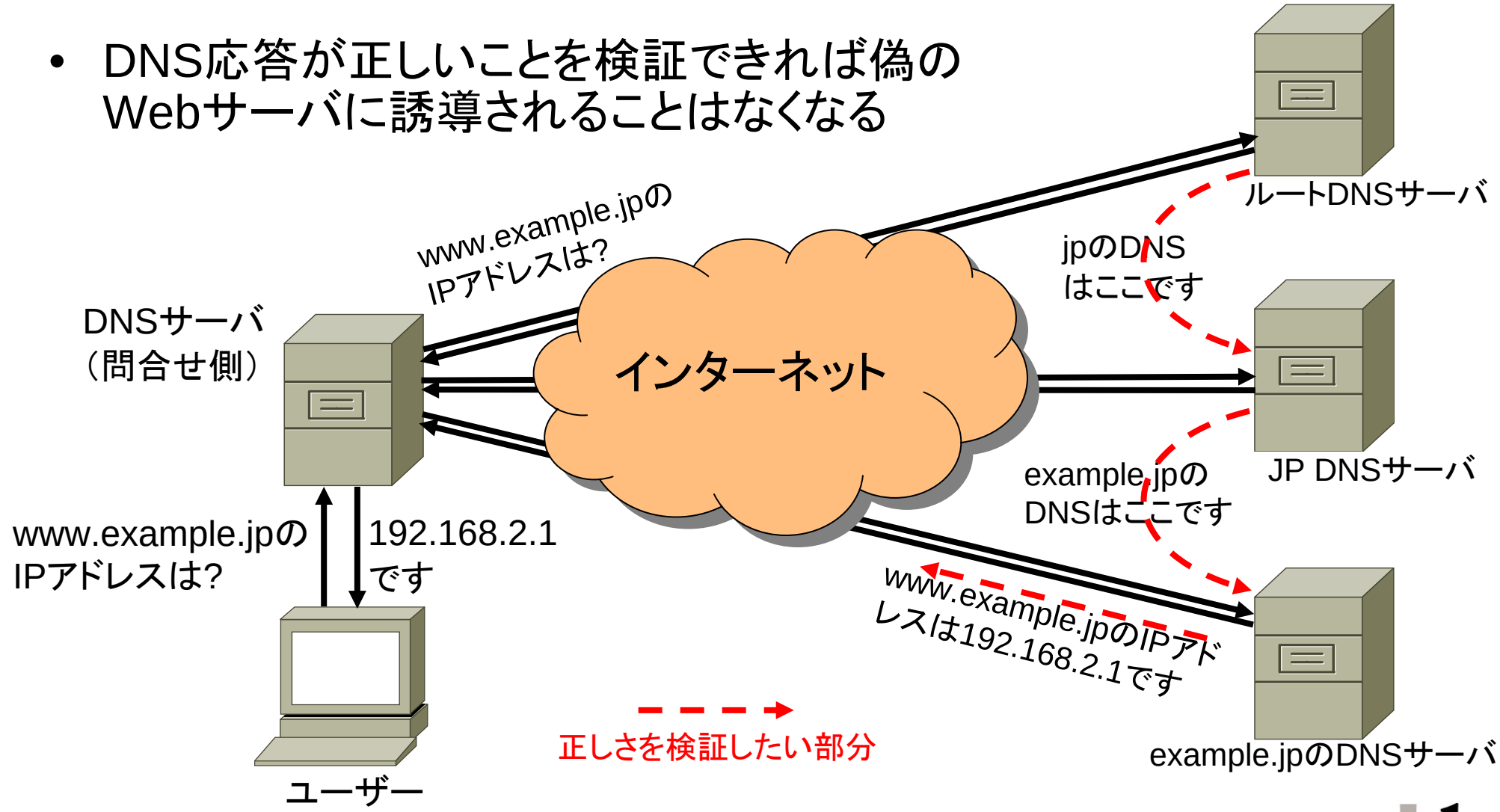
→ユーザーは大混乱

- 間違ったWebサイトにアクセスしてしまう
- 間違った相手に電子メールが送られてしまう



# DNS応答の正しさの検証

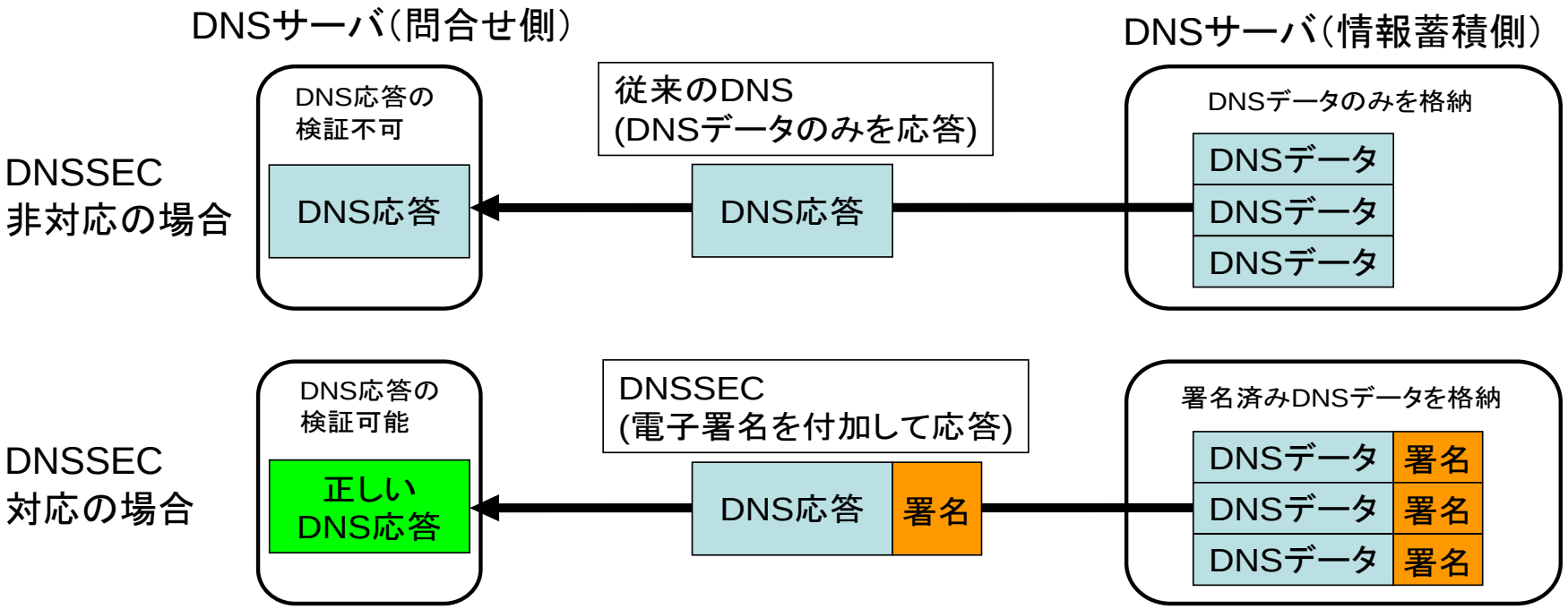
- DNS応答が正しいことを検証できれば偽のWebサーバに誘導されることはなくなる



# DNSSECとは

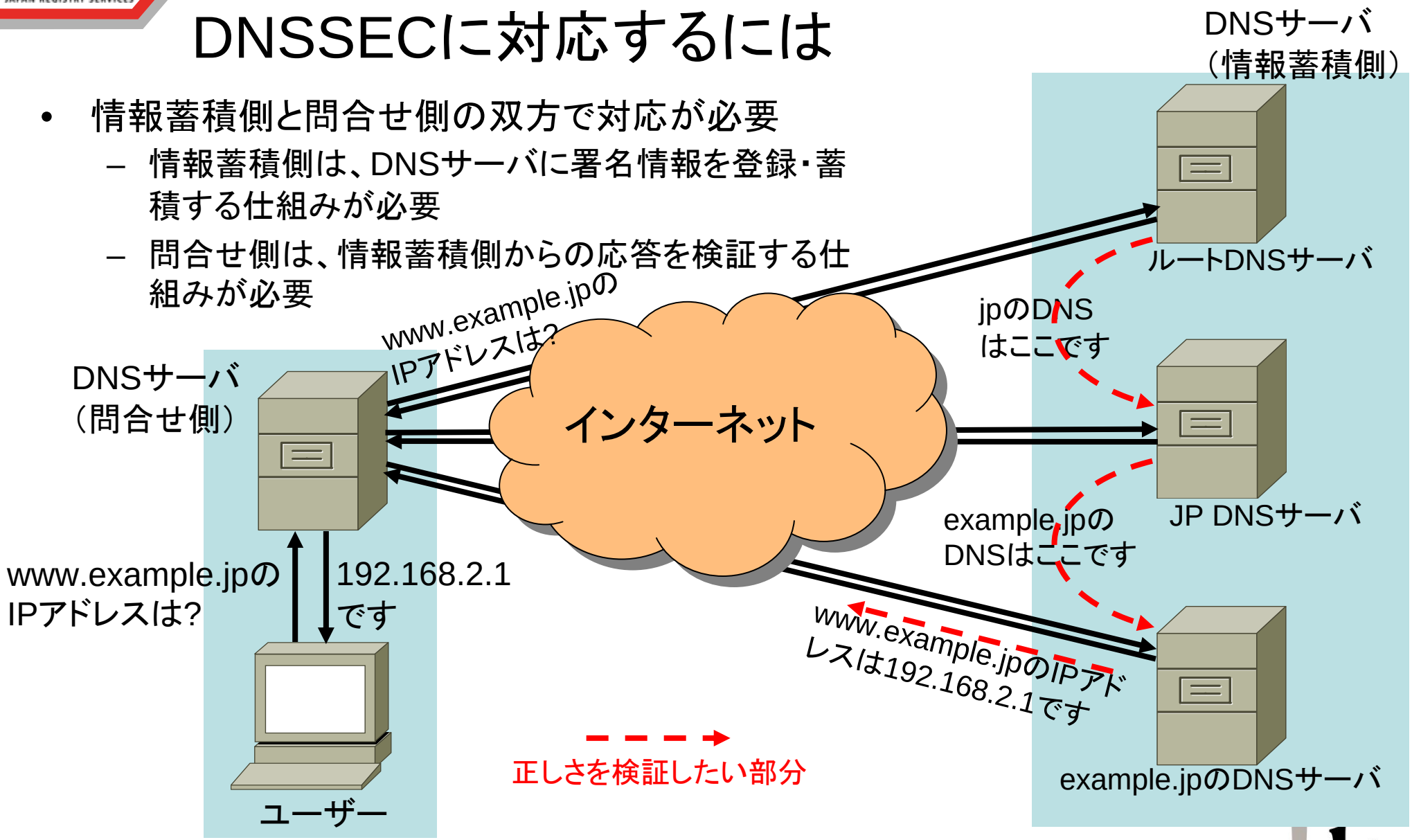
- DNSのセキュリティ機能拡張（DNS Security Extensions）
- DNSサーバで、応答に公開鍵暗号による署名(*)を付加し、出自を保証
- ユーザー側で、DNS応答を検証（偽造有無を自動的に検出）

(*)電子データに署名者のみが作れる情報を付加する技術。
紙文書での印・サインにあたる。



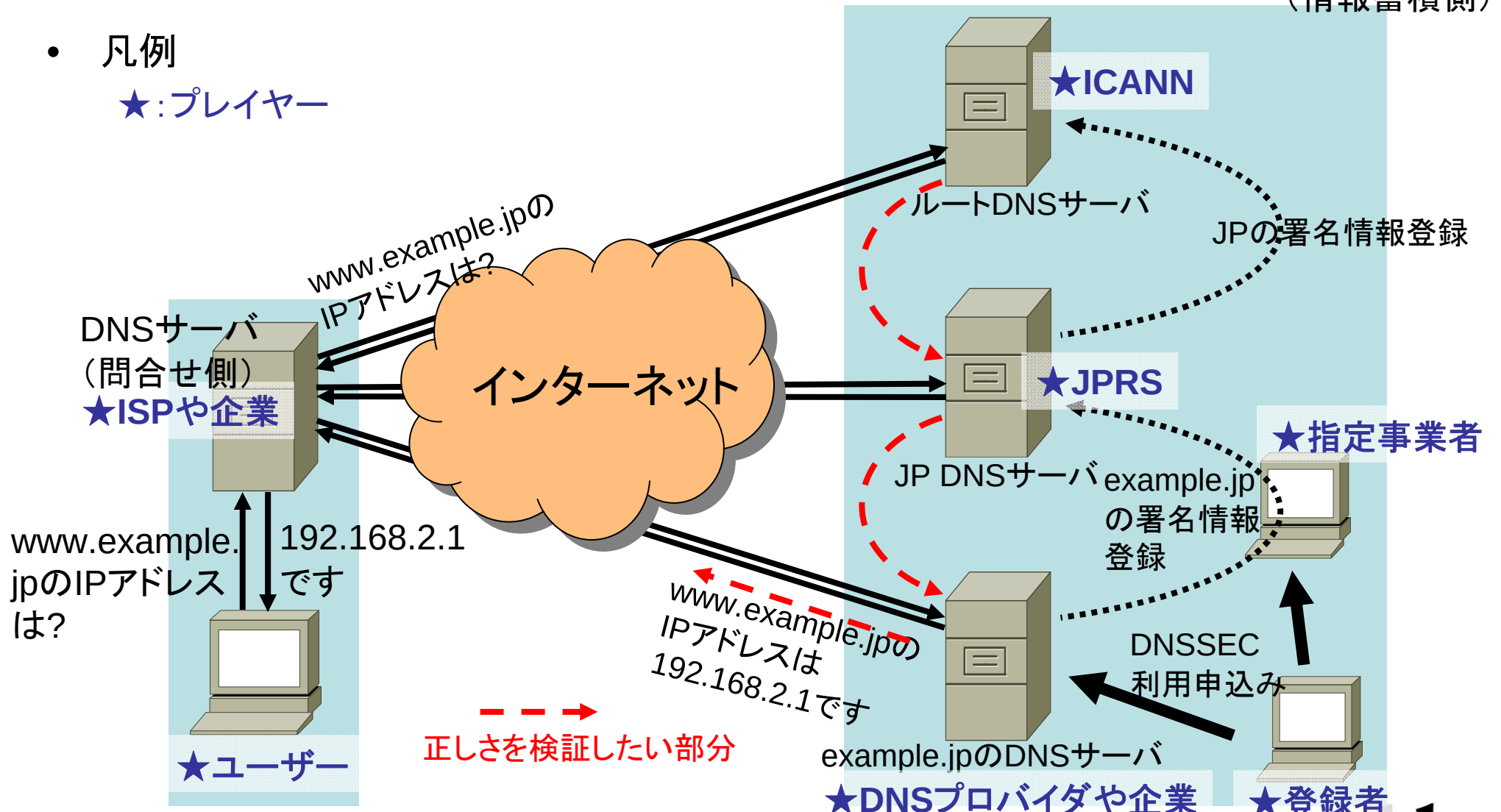
# DNSSECに対応するには

- 情報蓄積側と問合せ側の双方で対応が必要
  - 情報蓄積側は、DNSサーバに署名情報を登録・蓄積する仕組みが必要
  - 問合せ側は、情報蓄積側からの応答を検証する仕組みが必要



# DNSSECに関わるプレイヤー

- 凡例
  - ★:プレイヤー



# 2. 国外の状況

# TLDにおけるDNSSEC対応状況（導入済）

| 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<br>・2009年1月から料金を無料化<br>・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<br>・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 |
| | 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対応状況（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月に実地検証開始、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月に実地検証開始、2010年2月サービスイン予定 |
| | | MY（マレーシア） | ・2010年第四四半期に導入予定 |
| | | NL(オランダ) | ・2010年8月に導入予定 |
| | | RU（ロシア） | |
| | | 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 |
| | gTLD | BIZ | ・2010年第一四半期に導入予定 |
| | | 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 |

# ルートDNSサーバのDNSSEC対応予定

- ICANNとVeriSignを中心に導入プランを検討
  - ICANN　：ルートDNS情報の内容責任者
  - VeriSign：ルートDNS情報の編集責任者
- 導入スケジュール発表（2009年10月）
- 発表されたスケジュール
  - 2009年12月1日　　ルートDNS情報への署名開始
  - 2010年1月～7月　　署名を付加したDNS応答を返す
    ルートDNSサーバの数を段階的に増やす
    （署名の検証はできないようにしておく）
  - 2010年7月1日　　全てのルートDNSサーバが、署名を付加したDNS応答を返し、署名の検証が可能な状態にする

# 3. 日本国内の状況

# JPRSの活動状況（技術検証）

- 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*が運用するJP DNSサーバでの検証（2009年11月～）

  * IIJ、JPNIC、NII、WIDE
  - 海外拠点など遠隔地への転送検証、高負荷時の機能検証
- 各種プレイヤーと連携した検証（2009年12月～（予定））
  - 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
  - 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
  - 指定事業者と、DNSSECサービス導入への機能検証等の実施
  - 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ジャパン（後述）を舞台にした連携（2009年11月～）
  - 一般参加型の技術検証実施に向けた協力

# JPRSの活動状況（サービス開発）

- DNSSECサービス仕様検討
  - JP DNSデータの署名、および、登録者の署名情報をJP DNSに登録するサービス
  - DNSSECサービス導入による主な変更点
    - 指定事業者向け申請インターフェースの追加（登録者の署名情報登録）
    - JP DNSデータに署名を付加するための改造
    - Whois、データエスクロー等の周辺機能の改造
- 指定事業者向けサービス仕様説明
  - 2010年1月、指定事業者向けに公開予定
    - サービスの手続き説明資料
    - 申請インターフェースの仕様

# JPRSの活動状況（対外活動）

- DNSSECの導入・普及を促進するための国内コミュニティの形成
  - DNSSECジャパン（後述）の設立支援と参加（11月）
- 指定事業者向け情報提供
  - JPパートナーズミーティングでの解説（12月）
- 教育・啓発活動
  - DNSOPS.JP BoF*　　* DNS運用者の有志会合
    「いますぐDNSSECで遊ぶには」「DNSSECの導入に向けて」（9月）
  - JAIPA 地域ISPの集い in 群馬 「これだけは知っておきたいDNSSEC」（9月）
  - インフラエンジニア勉強会 hbstudy #4 「今こそDNSSEC!」（10月）
  - Internet Week 2009でのDNSSECチュートリアル（11月）
  - DNSOPS.JP BoF
    「DNSSECの拡張とBIND 9.7の新機能、小規模なDNSSEC遊びその後」（11月）
  - 日本UNIXユーザ会 「DNSSECの動向と運用」（12月）
- 国際的な議論・情報交換
  - ICANNソウル会合にて「DNSSEC in .JP」発表（10月）
  - IETF広島会議前後における他レジストリとの情報交換（11月）

# DNSSECジャパン（DNSSEC.jp）の設立

- 2009年11月24日設立
- 活動目的
  - 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。
- 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・運用に関するガイドラインの策定
  - 成果の対外的発信によるDNSSECの普及・啓発
- 会員（2009年12月10日現在）
  - ISP、ホスティングプロバイダ、レジストリ、インターネットエクスチェンジ等、全17会員
- http://dnssec.jp/