2009年9月7日
第29回JPドメイン名諮問委員会
資料5

DNSSECを利用するには

2009年9月7日

株式会社日本レジストリサービス

DNSの役割

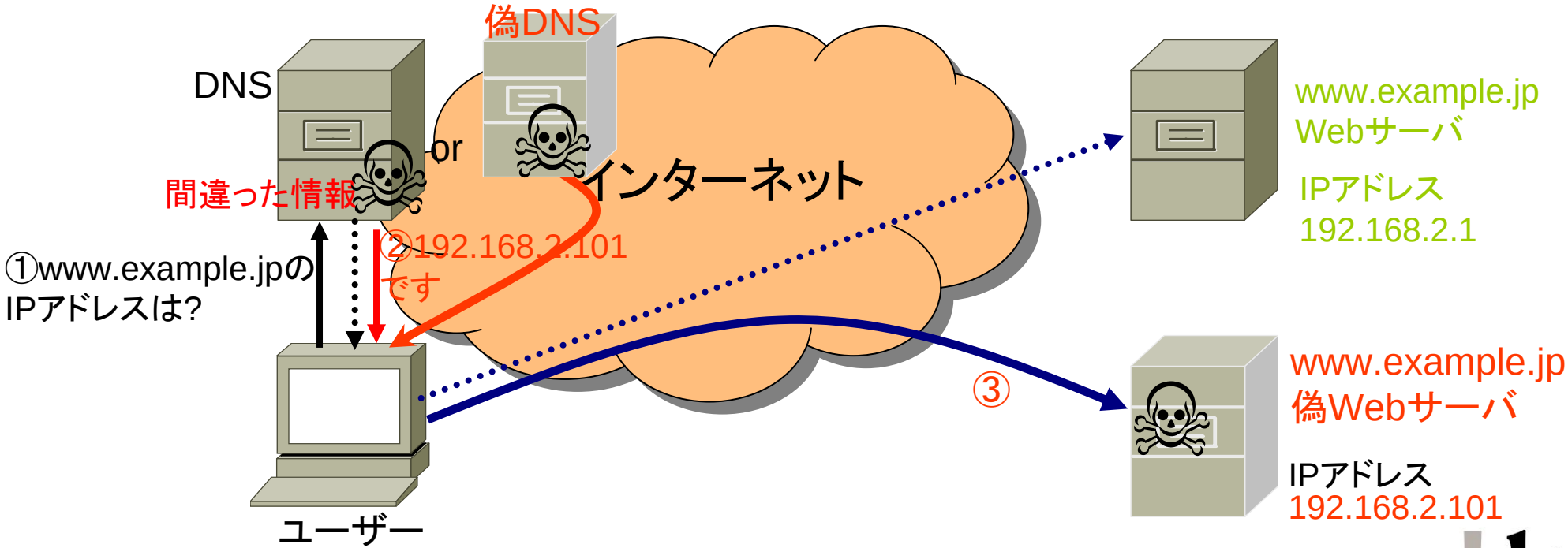
- 「ドメイン名」と「IPアドレス」を対応づける
- ユーザは、まず、DNSからIPアドレスを獲得し、そのIPアドレスを使ってWebサーバやメールサーバにアクセスする

DNSの応答が偽造されたら

- もし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の応答偽造の事例

- AlterNICによるInterNICのWebサーバ乗っ取り（1997年）
  - DNSサーバのセキュリティの穴を利用し、偽のDNS情報を注入
- ドメイン名登録者になりすますドメイン名ハイジャック
  - 登録情報の不正な書き換え
  - 偽のDNS情報の注入
- 嘘の参照先情報を使わせるコンピュータウイルス
  - フィッシングサイトへの誘導
  - システム自動更新の妨害

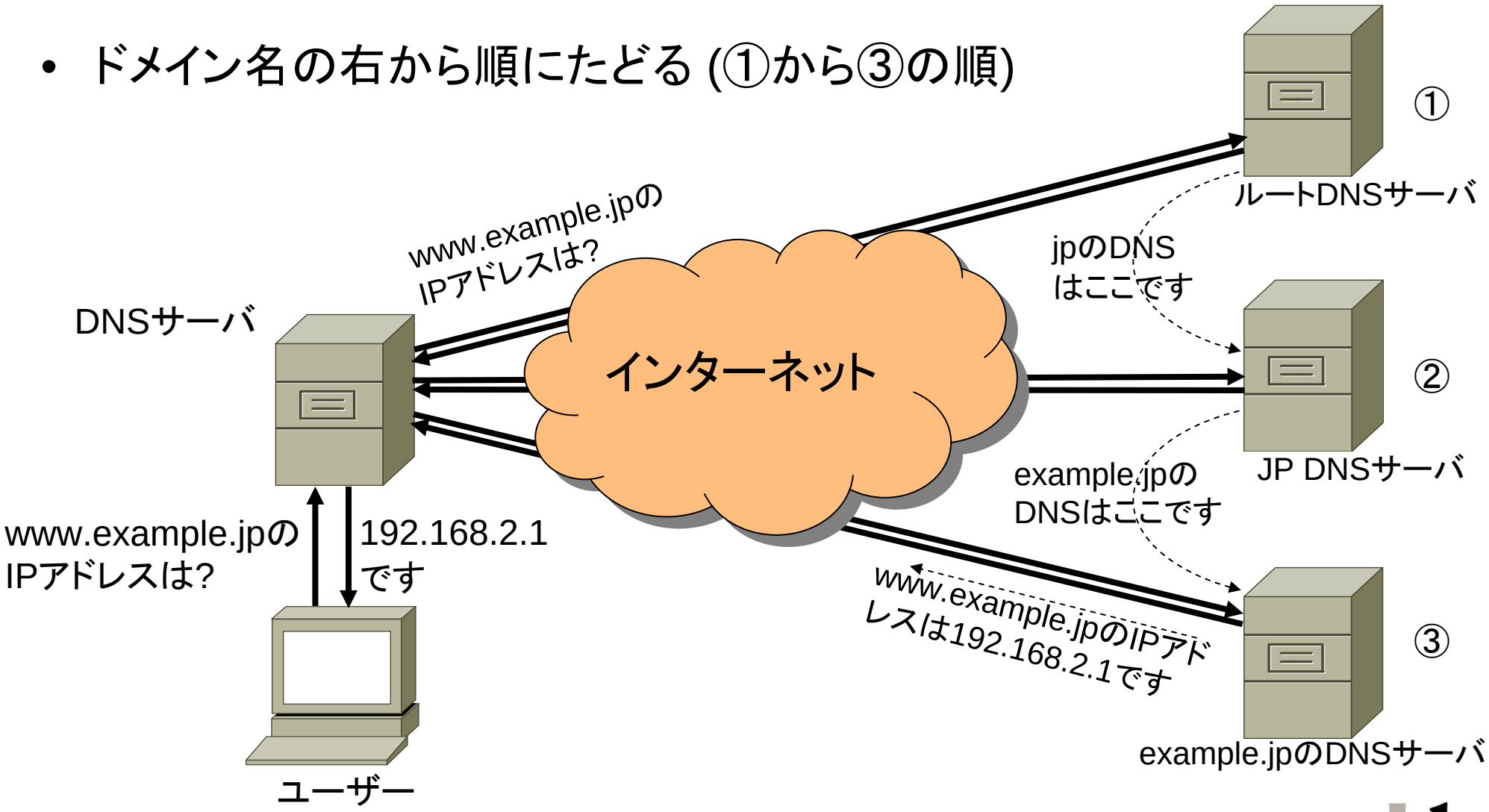
IPAからの注意喚起
(http://www.ipa.go.jp/security/vuln/20050627_dns.html)

DNSの応答偽造に対するJPRSのこれまでの活動

- レジストリデータベース更新の際のアクセス者認証の導入（2002年）
- 不適切なDNS設定によるフィッシング等の危険性解消のための措置（2005年）
- 著名人ブログに対するDNSキャッシュ汚染攻撃の分析と対策をISPと共同で実施（2006年）
- 新たに発見された、DNS情報を改ざんする攻撃手法に対する解説と対策を整理し、DNSサーバ管理者へ注意喚起を実施（2008年）
- インターネットコミュニティへの継続的な情報提供
  - JPRS TechWeb(Webサイト)、JANOG会合/ML、DNSOPS.JP会合/MLなど
- TAO・NICTの委託研究を通じたDNSSECの実用化研究(2001～2007年)

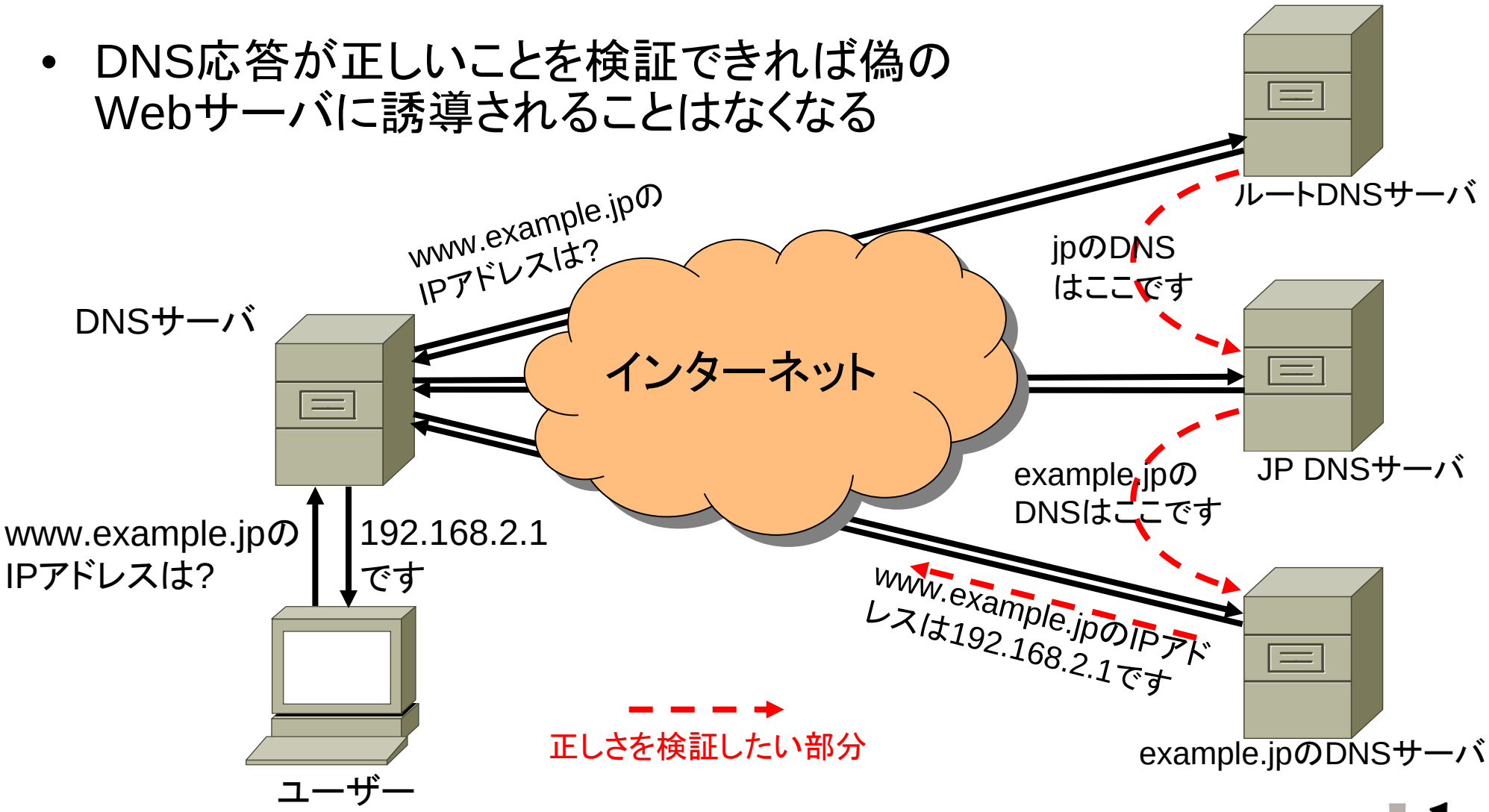
DNSの仕組み

- 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

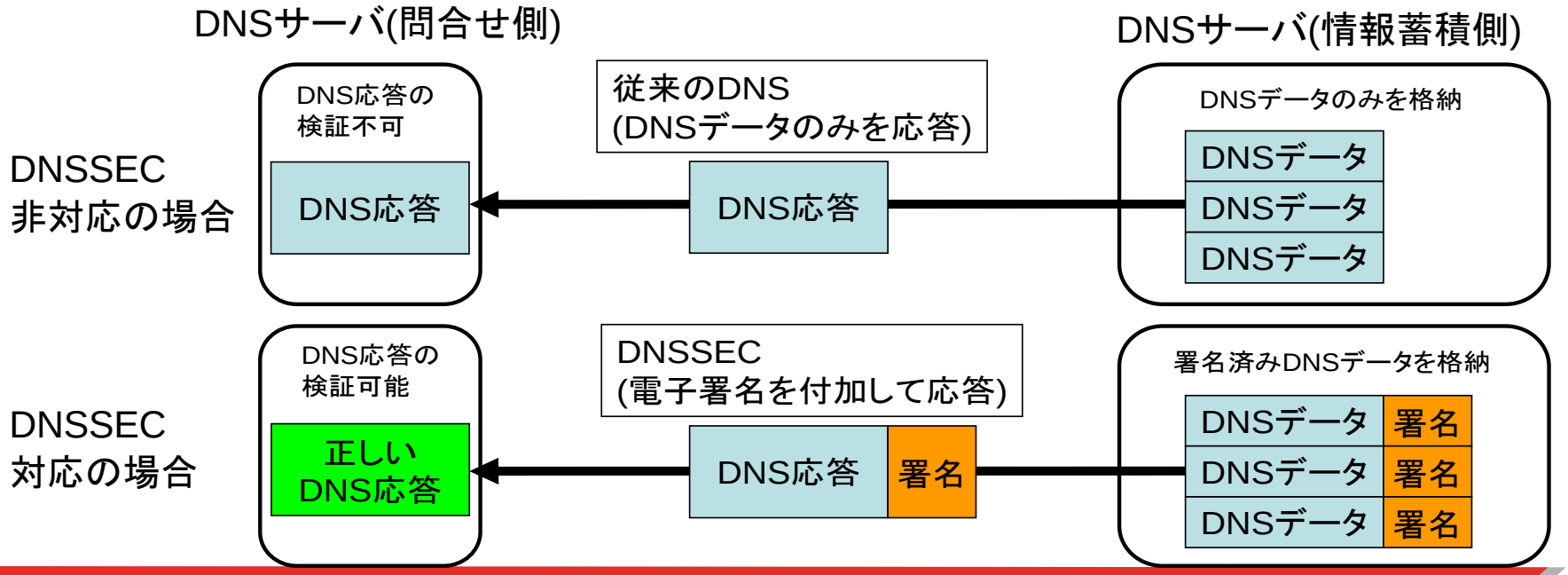
- DNS応答が正しいことを検証できれば偽のWebサーバに誘導されることはなくなる



DNSSECとは

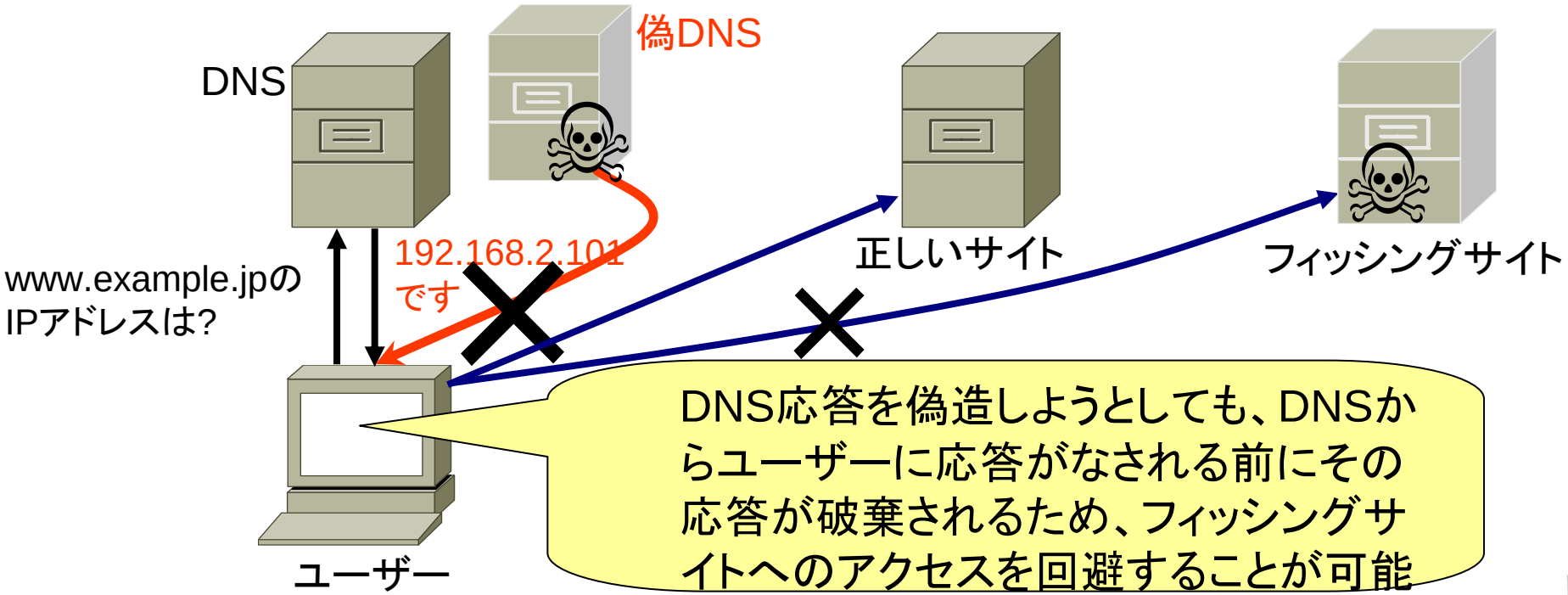
- DNSのセキュリティ機能拡張 (DNS Security Extensions)
- DNSサーバで、応答に公開鍵暗号による署名(*)を付加し、出自を保証
- ユーザー側で、DNS応答を検証(偽造有無を自動的に検出)

(*) 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。



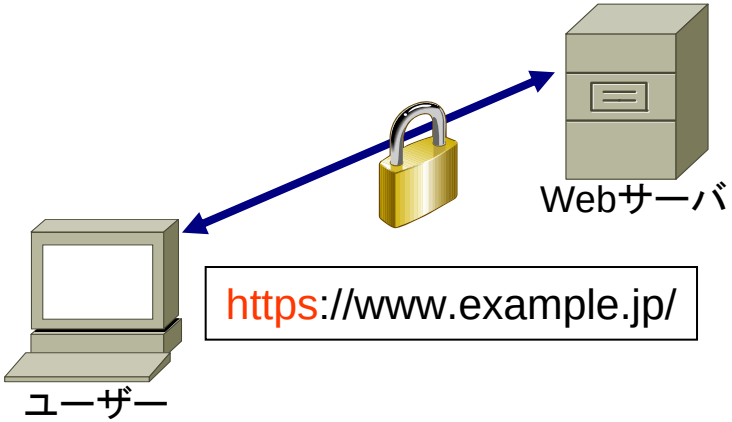
DNSSECでできること

- DNS応答の真偽の判別
  - 偽の応答や不完全な応答をユーザ側で判別可能
- DNS応答の捏造によるフィッシングや、電子メールの盗聴防止などに有効

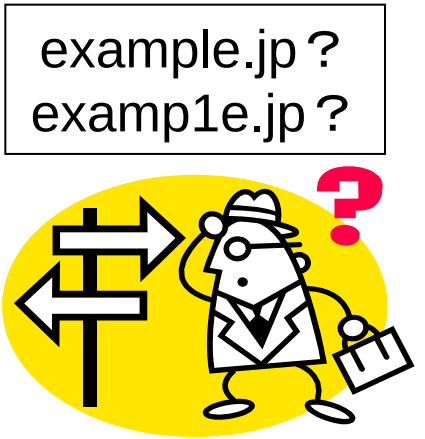


DNSSECではできないこと

- DNS応答の暗号化はしない
  - DNSSECは「登録者が登録したDNS情報を利用者に正しく伝える」ための技術
- インターネット上の通信そのものの安全は保証しない
  - 別の技術（SSL等）により実現
- ドメイン名の見間違いや思い違いを狙うタイプのフィッシングには対応できない



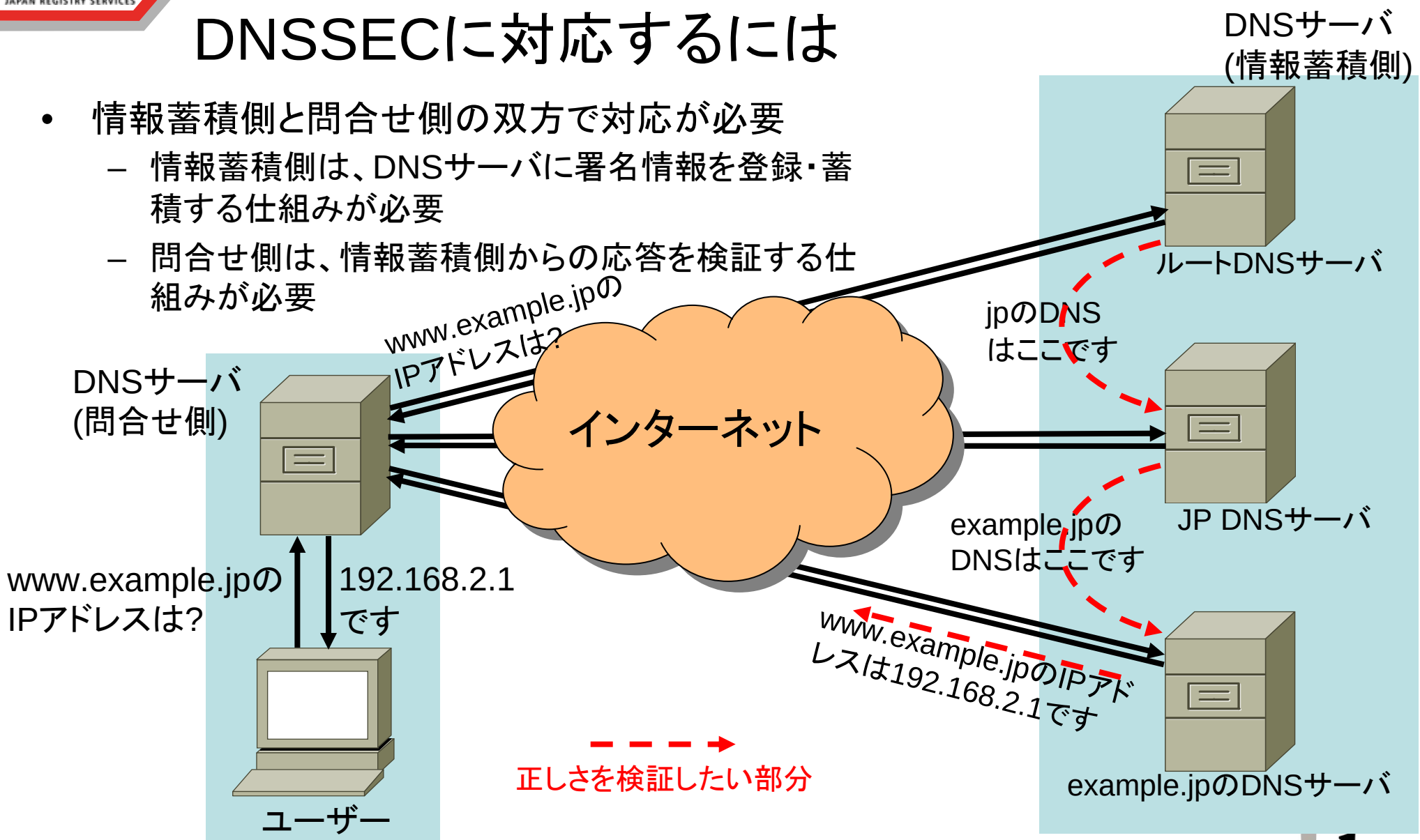
通信路の安全はSSLにより保証



見間違いを狙うフィッシングには対応不可

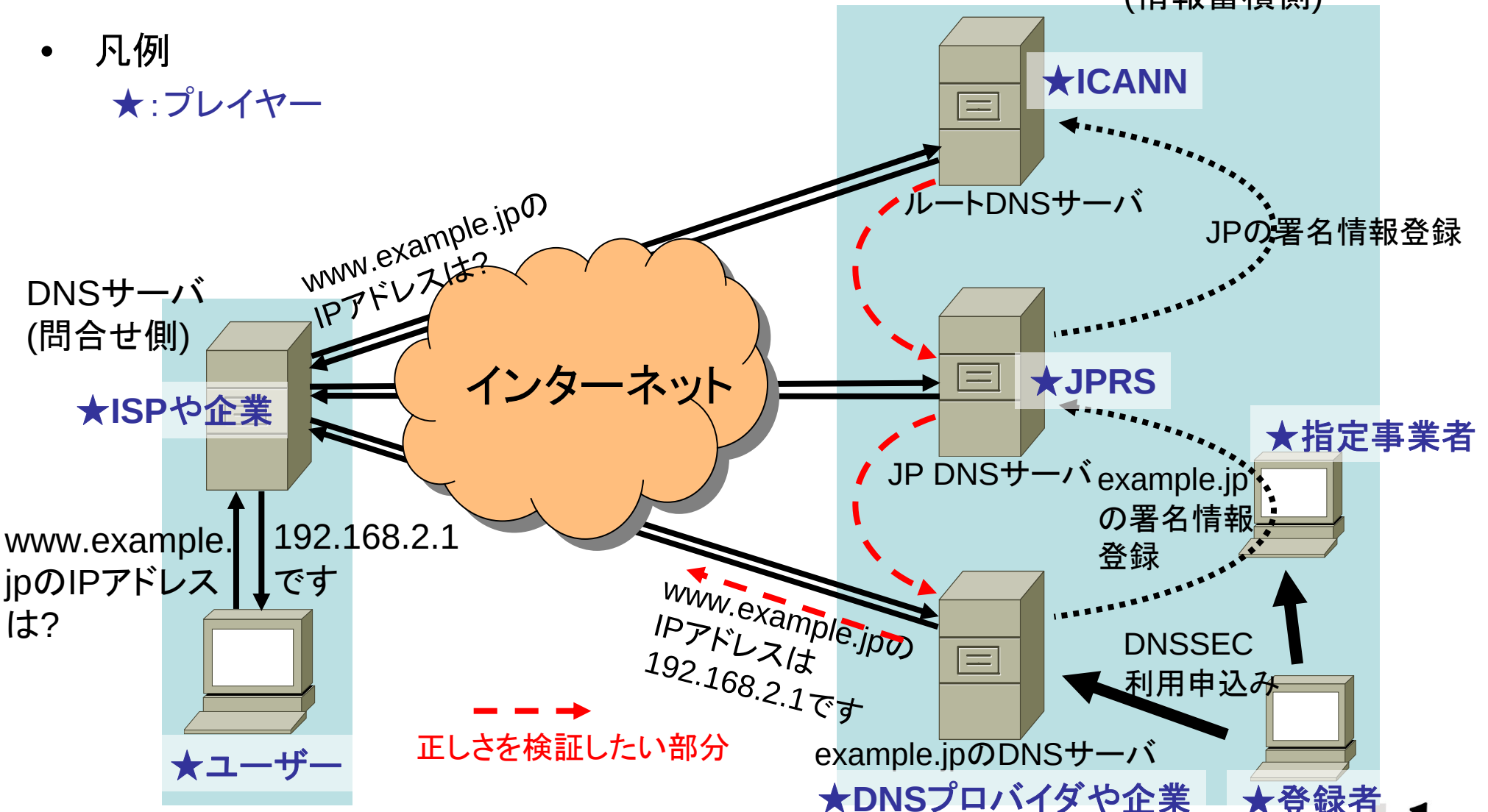
DNSSECに対応するには

- 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



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 ・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
	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）	
		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
		MY（マレーシア）	・2009年3月からテストベッド開始
		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	
		CAT	・2009年中に導入予定
		COM	・2011年の早い時期に導入予定
		INFO	
		NET	・2010年末までに導入予定