

JPドメイン名の概況と ドメイン名を取り巻く状況について

2009年5月28日(木)

株式会社日本レジストリサービス

目次

1. JPドメイン名の概況 (p.3)
2. 他TLDの状況 (p.11)
3. DNSSECに関する動向 (p.15)
4. 日本における「.日本」検討状況 (p.29)

1. JPドメイン名の概況

JPドメイン名の種類と登録数 (2009/5/1現在)

属性型・地域型JPドメイン名 (合計: 393,324)

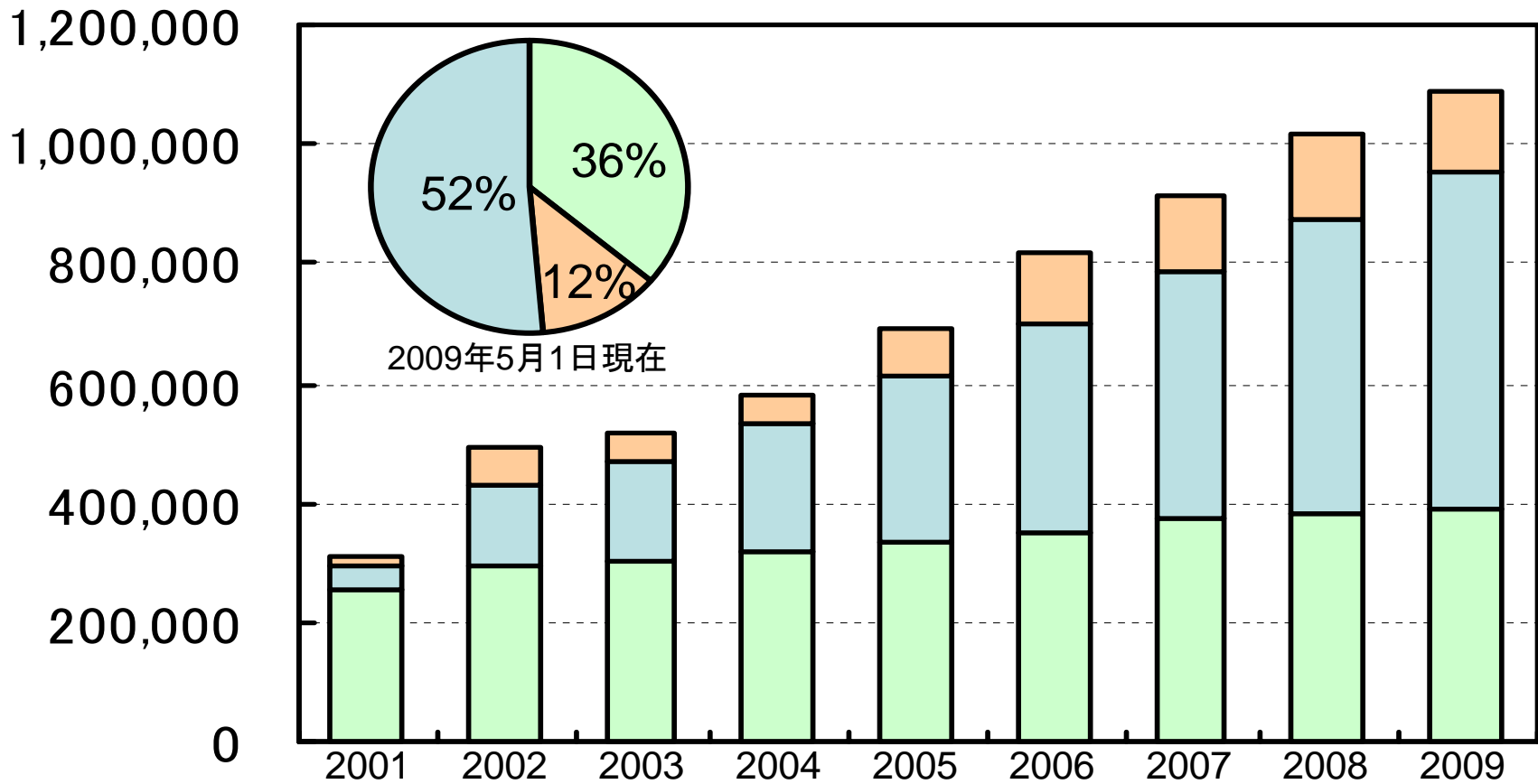
〇〇.AD.JP	JPNIC会員	271
〇〇.AC.JP	大学など高等教育機関	3,524
〇〇.CO.JP	企業	329,046
〇〇.GO.JP	政府機関	849
〇〇.OR.JP	企業以外の法人組織	24,904
〇〇.NE.JP	ネットワークサービス	17,207
〇〇.GR.JP	任意団体	8,086
〇〇.ED.JP	小中高校など初等中等教育機関	4,552
〇〇.LG.JP	地方公共団体	1,931
地域型	地方公共団体、個人等	2,954
汎用JPドメイン名 (合計: 697,152)		
〇〇.JP	組織・個人問わず誰でも(英数字によるもの)	561,571
□□.JP	組織・個人問わず誰でも(日本語の文字列を含むもの)	135,581

総計 **1,090,476**

JPドメイン名の登録数推移

登録数

■ 属性型・地域型 ■ 汎用(英数字) ■ 汎用(日本語)



2009年5月1日現在

※各年5月1日時点の登録数



汎用JPドメイン名(英数字)の概況

- 商品やサービスに対応するドメイン名登録
- 個人や小規模組織によるドメイン名登録
- インターネット利用形態の多様化(*)に伴うドメイン名利用の拡大

今後

- 企業市場でのブランディング用途でさらに普及
- 個人市場でさらに普及

(*) 例： - 携帯電話などでの利用に特化したインターネットサービス
- 簡易Webホスティングサービス

汎用JPドメイン名(日本語)の概況

- 商品名や氏名などをドメイン名として登録
- パソコン上のWebブラウザのほとんどで日本語JPドメイン名の利用が可能に

今後

- Webでの利用のための環境ができたため、
 - 活用事例が増え、認知向上や活用メリットの理解が進む
 - さらなる環境整備が進む
 - 携帯電話向けブラウザでの対応
 - インターネット検索サービスでの日本語JPドメイン名でのURL表示
 - 「国際化電子メールアドレス(EAI)」⇒@の左側も全部日本語で

属性型・地域型JPドメイン名の概況

- CO.JPドメイン名

- 属性型・地域型ドメイン名の84%を占める
- 汎用JPドメイン名サービス開始後も登録数増加
- 「日本の企業はCO.JP」というブランド(信頼)
- 申請手続即時処理サービス開始(2008年6月)により、CO.JP登録者の利便性が向上 (これまでは申請後利用開始までに日単位での時間を要した)

今後

- 信頼性の維持・向上
- 中小企業へのさらなる認知浸透
- 利便性向上による登録増

JPRSの最近1年間の主な活動 (1)

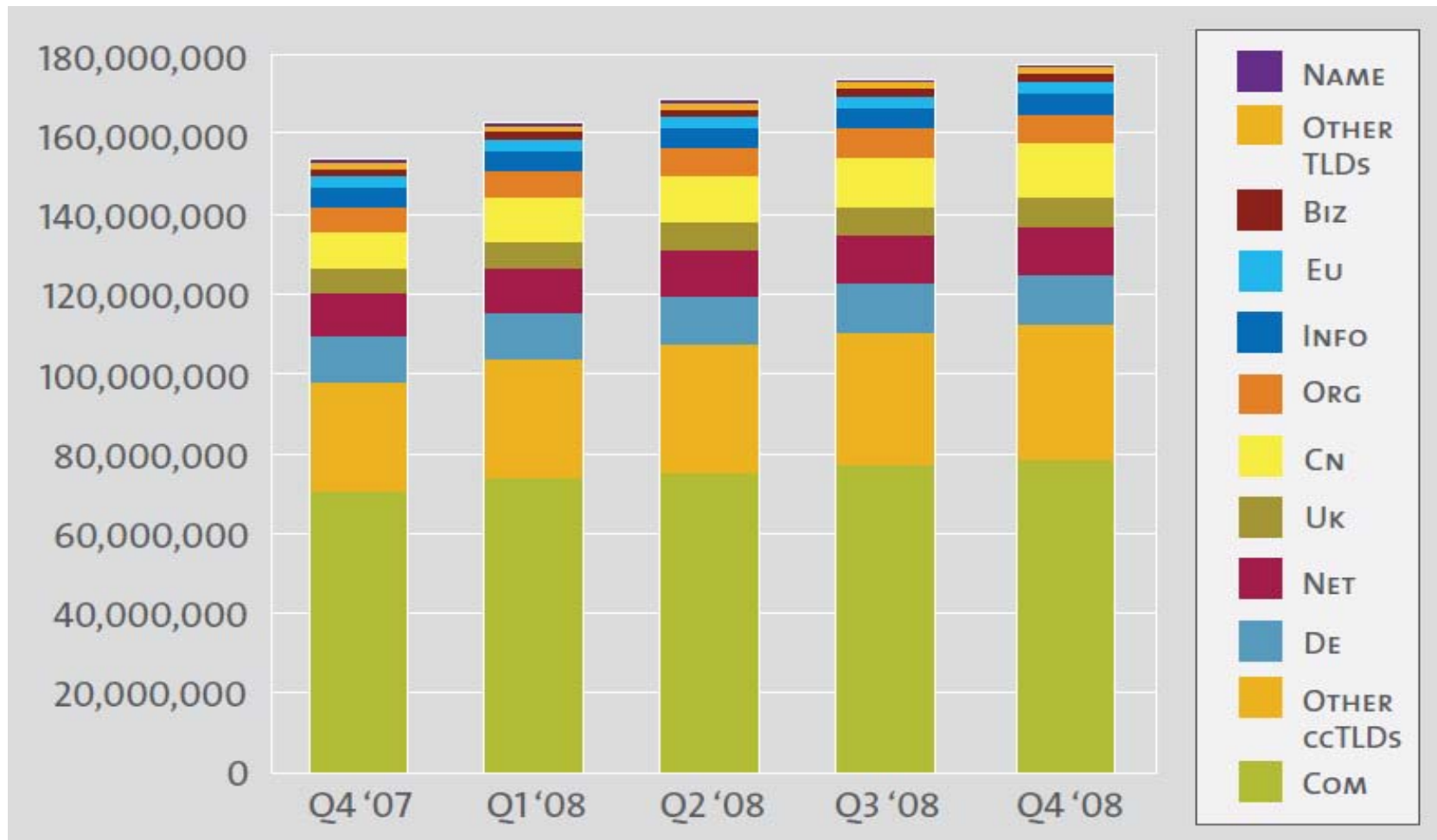
- 2008年6月
 - CO.JPDメイン名の申請手続即時処理サービス開始
 - 新たな申請方法が導入され、CO.JPDメイン名の即時登録・利用が可能に
- 2008年7月
 - DNSソフトウェアにおけるキャッシュポイズニングの脆弱性に関する注意喚起
 - DNSの応答を改ざんする攻撃(キャッシュポイズニング攻撃)の新たな手法が発見されたため、いち早く解説と対策をまとめ、ISPや企業等のDNSサーバ管理者へ注意喚起

JPRSの最近1年間の主な活動 (2)

- 2008年10月
 - CO.JPDメイン名の利用促進活動
 - CO.JPDメイン名のメリットを解説したWebやパンフレットを制作し、ドメイン名の効果的な使い方を提案
- 2008年10月～11月
 - JP DNSサーバの追加 (10月)
 - JP DNSサーバのIPv6対応 (11月)
 - JP DNSサーバの安定性・信頼性の向上、IPv6の環境整備
 - DNS拠点数を倍増させ、世界20拠点以上にDNSサーバを配置
- 2008年12月
 - OR.JPDメイン名の利用促進活動
 - 一般社団法人及び一般財団法人に関する法律の施行に合わせ、「OR.JP」の理解と効果的なドメイン名の使い方に関する情報を提供するサイトを開設

2. 他TLDの状況

世界のドメイン名数



出典：“The VeriSign Domain Name Industry Brief”
<http://www.verisign.com/static/044518.pdf>

他レジストリの状況 (1)

- ccTLDの動向
 - 制限の緩和
 - 1登録者が複数ドメイン名を登録可能に
 - 海外登録者への開放
 - 移転(ドメイン名売買)の自由化
 - 1文字ドメイン名や数字ドメイン名の登録開始
 - IDN ccTLD(例:「.日本」) Fast Trackによる導入プロセス検討
 - 2009年3月にICANN理事会が公表したスケジュール
 - 2009年第4四半期: 募集開始
 - 2010年第1四半期: 創設開始
 - DNSセキュリティ拡張(DNSSEC)のサービスを開始するレジストリが出現

他レジストリの状況 (2)

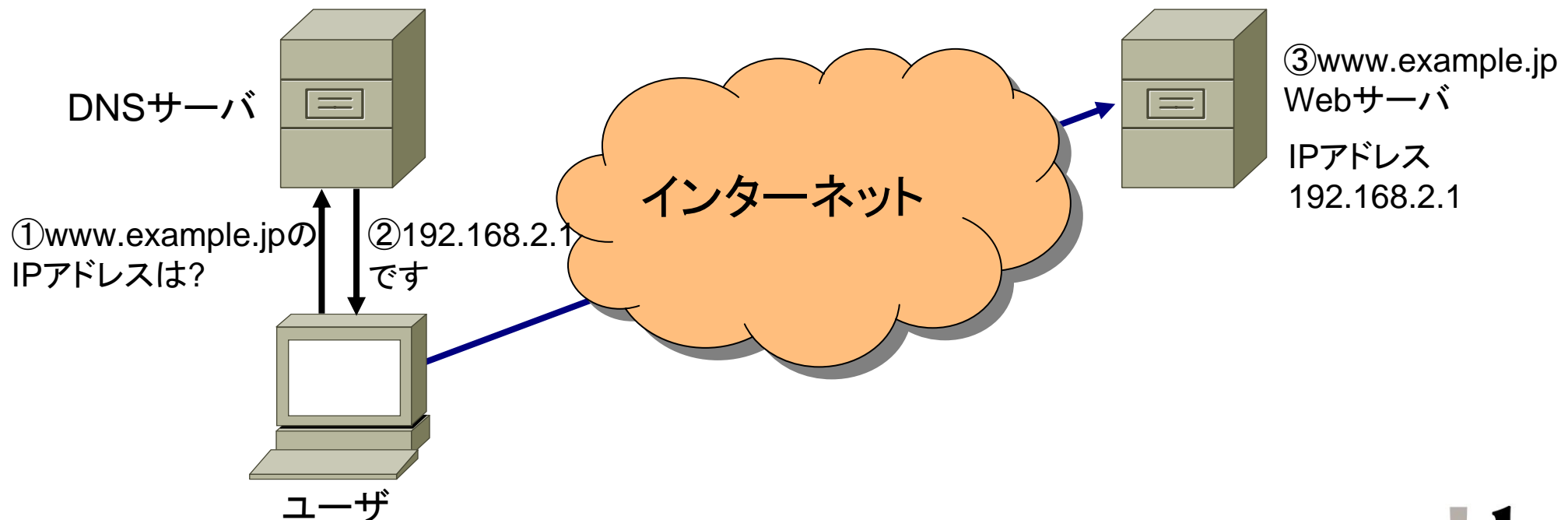
- gTLDの動向
 - 累計登録数の拡大
 - インターネット利用が拡大してきた国々(BRICs、開発途上国)でのドメイン名登録急増
 - 「自らのWebサイトや電子メールアドレス」以外の利用方法(*)の拡大
 - IDN TLDを含む新gTLD導入プロセス検討
 - 創設するgTLDの数にあらかじめ制限は設けず
 - 2009年3月にICANN理事会が公表したスケジュール
 - 2009年第4四半期：募集開始
 - 2010年第1四半期：創設開始

(*) 売買や他社広告を集めたWeb運用などを目的とした利用

3. DNSSECに関する動向

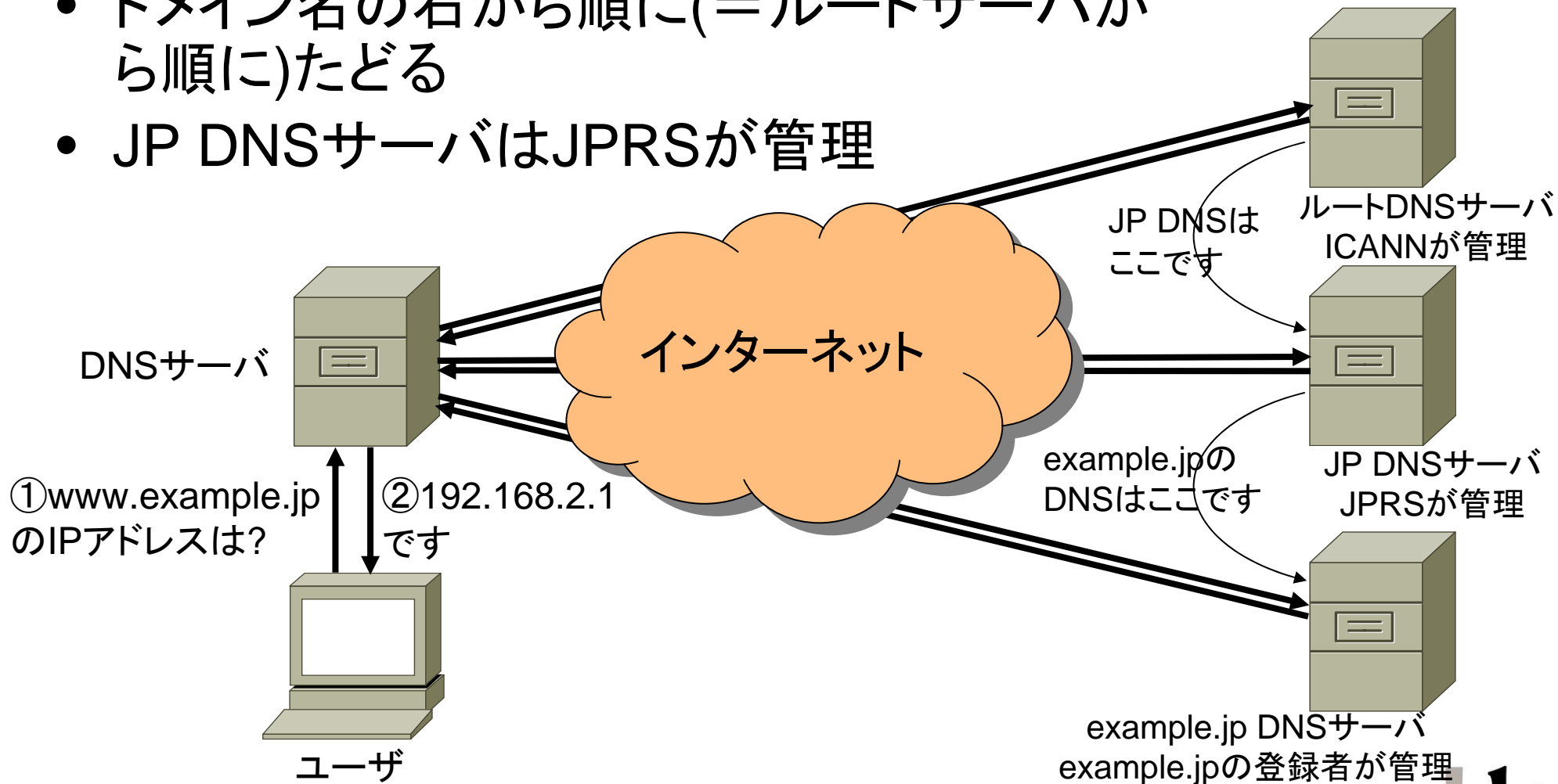
DNSの役割

- 「ドメイン名」と「IPアドレス」を対応づける
- ユーザはDNSサーバから得られたIPアドレスで、インターネットにアクセスする



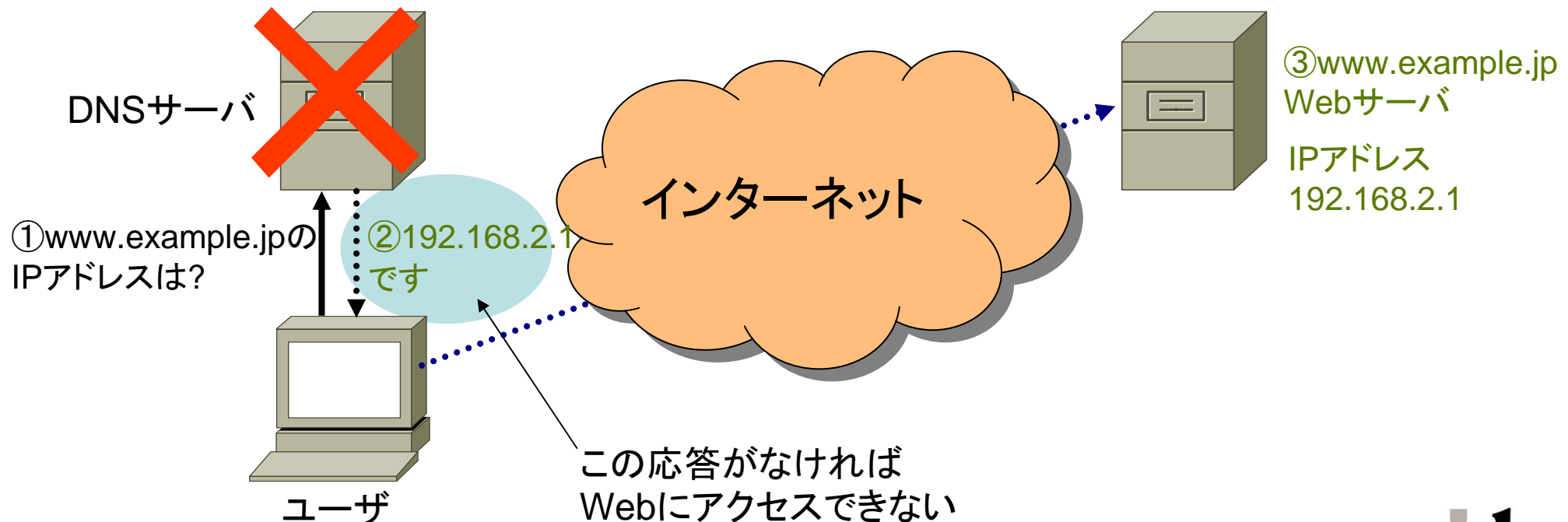
DNSのしくみ

- ドメイン名の右から順に(=ルートサーバから順に)たどる
- JP DNSサーバはJPRSが管理



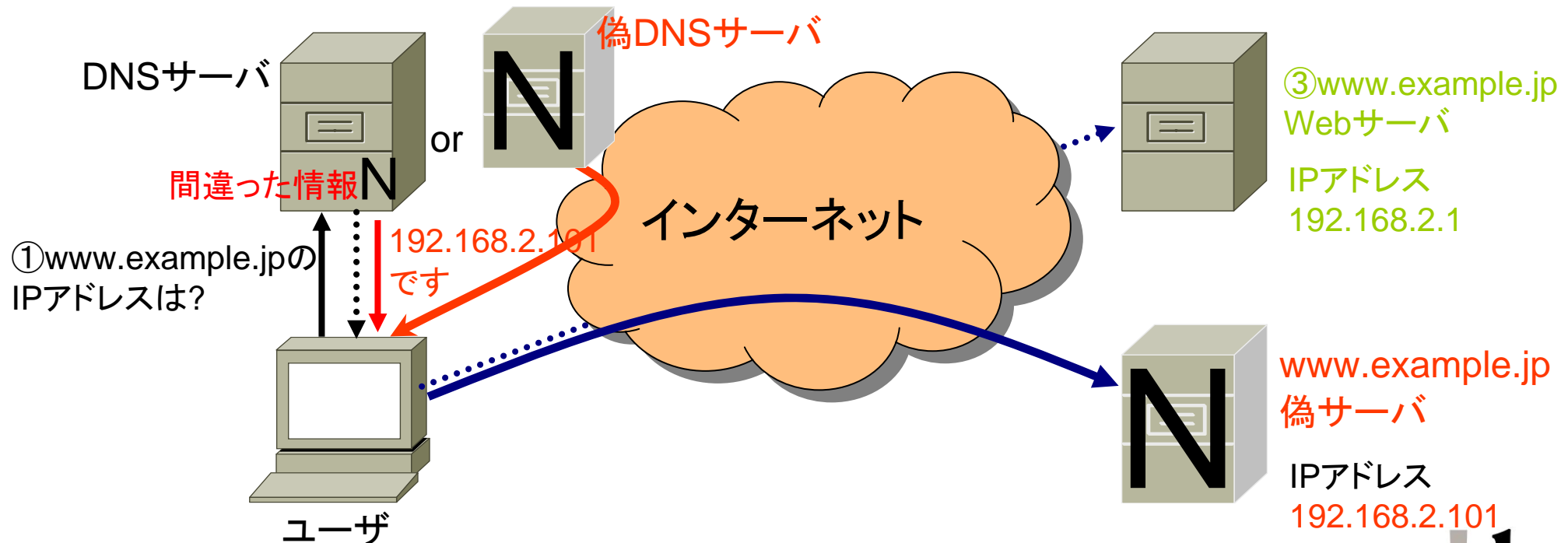
DNSの重要性(1)

- もしDNSが動かなかったら・・・
 - インターネットが使えない
 - Webが使えない
 - 電子メールも使えない



DNSの重要性(2)

- 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返事を信じてしまったら・・・
 - ユーザは大混乱
 - 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

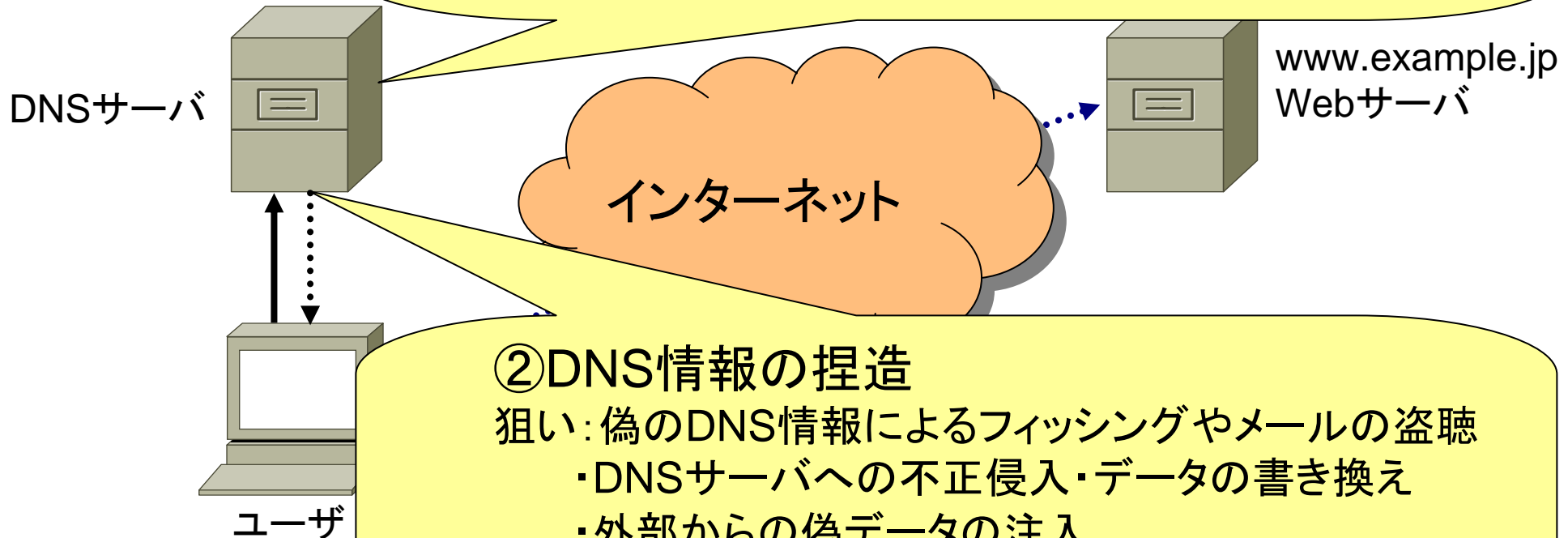


DNSに対する2種の脅威

①DNSの機能停止

狙い: DNSの機能停止によるインターネット利用妨害

- ・DNSサーバそのものに対する攻撃
- ・接続ネットワークに対する攻撃、など



②DNS情報の捏造

狙い: 偽のDNS情報によるフィッシングやメールの盗聴

- ・DNSサーバへの不正侵入・データの書き換え
- ・外部からの偽データの注入
- ・DNS登録用データの不正な書き換え
- ・偽のDNSサーバへの誘導、など

DNSトラブル事例①—DNSの機能停止

- 米Network Solutions社のオペレーションミスによるDNSデータ破損(1996年)
 - 数百万件のcom/net/orgドメイン名が到達不能に
- ルートサーバに対するDDoS攻撃(2002年、2007年)
 - 2002年の攻撃
 - 13台中7台のルートサーバに大きな影響
 - インターネット全体への影響は免れた
 - 2007年の攻撃
 - IP Anycast等の施策が奏功、影響はほぼなし

News: ルートサーバに一斉DoS攻撃 - Windows Internet Explorer

http://www.itmedia.co.jp/news/0210/23/njbt_01.ht

News: ルートサーバに一斉DoS攻撃

News: ニュース速報 2002年10月23日 03:05 PM 更新

ルートサーバに一斉DoS攻撃

10月21日午後5時ごろ(米国東部時間)、世界13のルートサーバに一斉にDoS(サービス拒否)攻撃が仕掛けられた

米国メディアの報道によると、10月21日午後5時ごろ(米国東部時間)、世界13のルートサーバに一斉にDoS(サービス拒否)攻撃が仕掛けられた。

Weekly Traffic to/from JPIX

東京に置かれたルートサーバ「M」のトラフィック。日本時間の22日早朝に増大している

攻撃は米国当局が防御策を講じるまで約1時間にわたって続けられたという。急激なトラフィック増加を受け、米国内と東京、ストックホルムなどの7台に大きな影響が出たが、一般ユーザーのネット利用に問題は生じなかったという。13台のルートサーバすべてに一斉攻撃が仕掛けられたまれなケースだと報じられている。攻撃者は分かっておらず、米国連邦捜査局(FBI)が捜査に乗り出した。

ルートサーバは、ドメイン名とIPアドレスを対応させるDNSの最上位に位置するインターネットの根幹。WIDEプロジェクトが管理する東京の1台を含む合計13台が稼働している。

関連記事

ページが表示されました インターネット 100%

2002年のルートサーバに対するDDoS攻撃(ITmedia)

DNSトラブル事例②—DNS情報の捏造

- AlterNICによるInterNICのWebサーバ乗っ取り(1997年)
 - BINDの脆弱性を利用し、偽のDNS情報を注入
- ドメイン名ハイジャック
 - 登録情報の不正な書き換え
 - 不適切な登録情報の放置
 - 偽のDNS情報の注入
- 嘘の名前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の脅威に対するJPRSのこれまでの活動

①DNSの機能停止に対する施策

- JP DNSの地理的分散化(2003年)
- JP DNSへのIP Anycast技術の導入(2004年)
- オペレーションセンターの導入による障害検知・対応の迅速化(2006年)
- JP DNSをさらに地理的分散化(2008年)

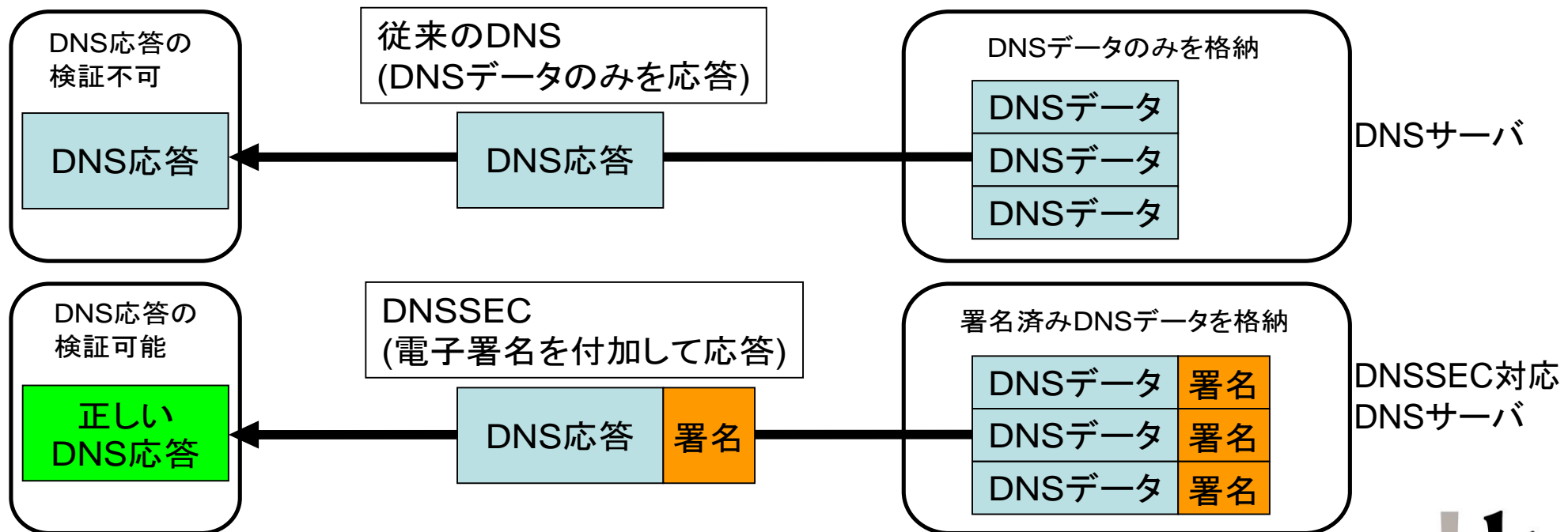
②DNS情報の捏造に対する施策

- 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の応答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
- 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)

DNSSECとは

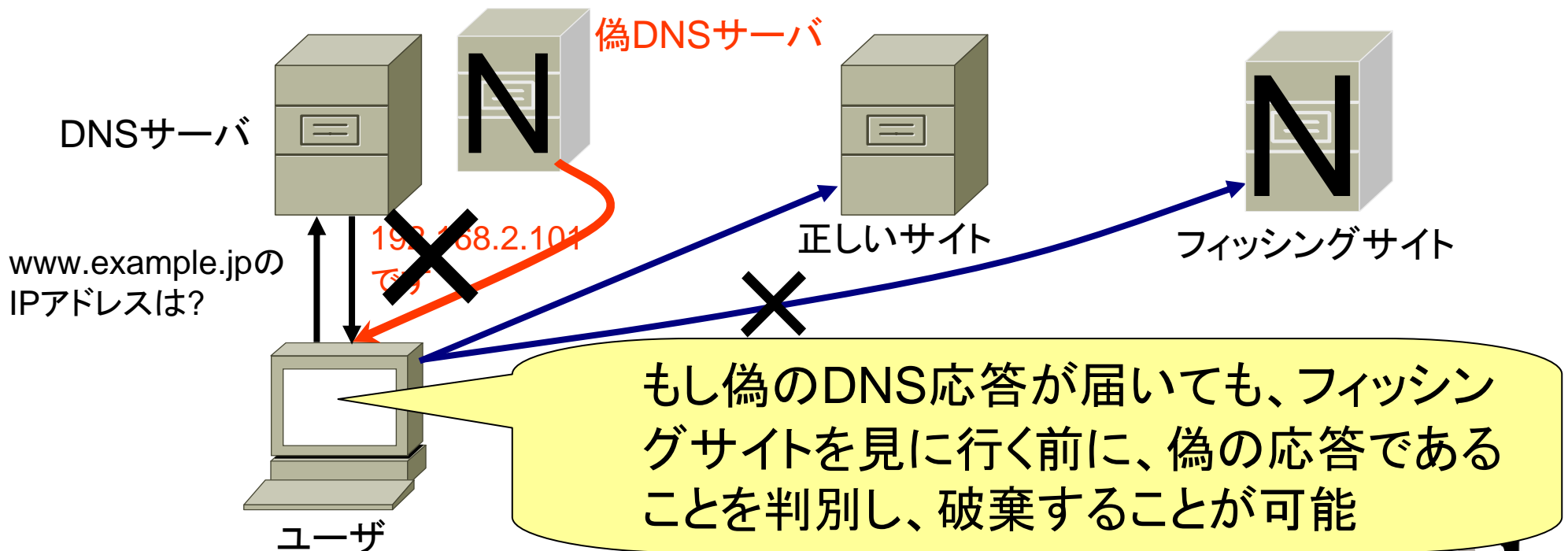
- DNSのセキュリティ機能拡張 (DNS Security Extensions)
- DNSサーバは、応答に電子署名(*)を付加し、出自を保証
- 利用者側で、DNS応答の改ざん有無を自動的に検出

(*)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。



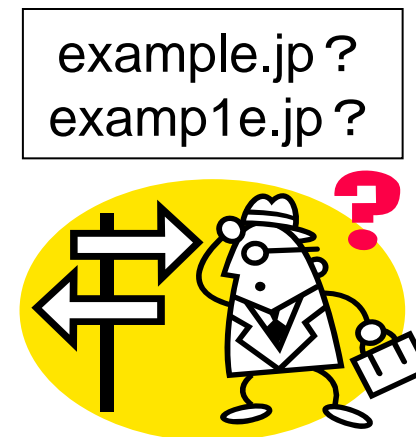
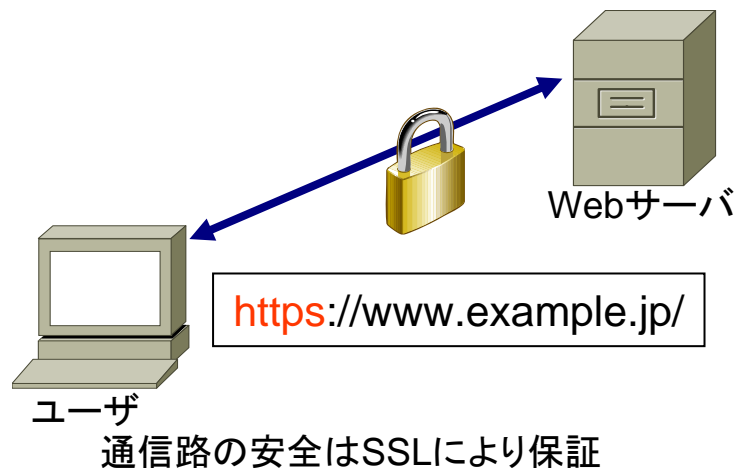
DNSSECでできること

- DNS応答の真偽の判別
 - 偽の応答や不完全な応答を受信側で判別可能
- 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路の安全は保証しない
 - 別の技術(SSL)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



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

- DNSSECの検証もドメイン名の右から順にたどる
(検証1から3の順)
- つまり、原則として、上位組織からDNSSECに対応しなければならない(①から③の順)
- DNSSECの有効化には、ISPにおける対応も必要

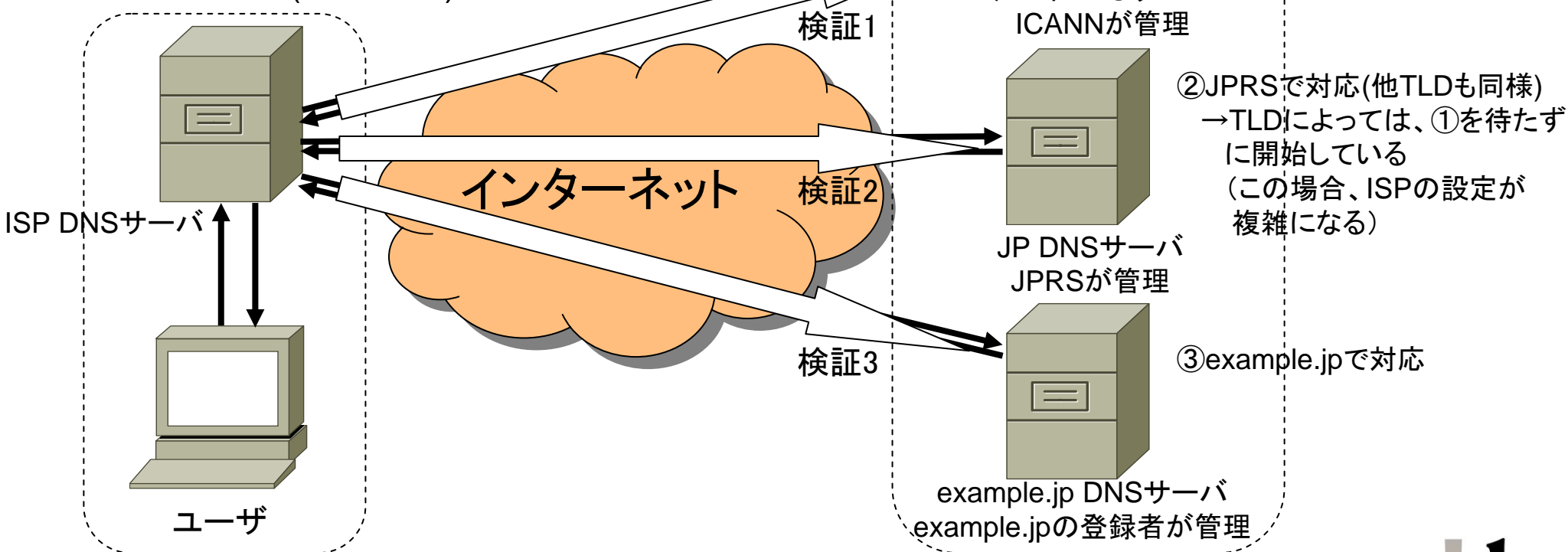
DNSSEC署名側(TLDなど)

①ルートで対応
→ICANN、DoC(米国商務省)
で対応方法を議論中

②JPRSで対応(他TLDも同様)
→TLDによっては、①を待たず
に開始している
(この場合、ISPの設定が
複雑になる)

③example.jpで対応

DNSSEC検証側(ユーザ側)



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)	<ul style="list-style-type: none"> ・2005年9月にサービスを開始し、世界で最初にDNSSEC対応したTLDとなった ・サービス開始当初は有料であったが、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(ペルトリコ)	・2006年8月にサービス開始
		BG(ブルガリア)	・2007年1月にサービス開始
		BR(ブラジル)	<ul style="list-style-type: none"> ・2007年6月にサービスを開始し、2009年1月に全空間(属性) に対応 ・NSEC3という最新の方式を採用した最初のTLD
		CZ(チェコ)	<ul style="list-style-type: none"> ・2008年9月に導入 ・内製開発を基本に、新技術を迅速・積極的に導入
		TH(タイ)	・2009年3月に導入し、アジアで最初にDNSSEC対応したccTLDとなった
	gTLD	MUSEUM	・2008年9月にサービス開始
		GOV(米国政府機関)	・2009年2月に導入し、2009年末に全組織が対応予定
導入を表明済 (非公式含む)	ccTLD	CA(カナダ)	・2008年10月に実装開始
		DE(ドイツ)	
		GR(ギリシャ)	
		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/NET	・インフラ強化計画「Project Titan」やマスコミ取材に対する回答から2010年末頃に導入すると予測
		ORG	・2008年7月に実装を始め、2009年中にパイロットサービスを開始し、2010年にサービス予定
		INFO	

4. 日本における「.日本」検討状況

インターネット基盤委員会

- 2008年11月、総務省が下記を決めるため、民間からなる委員会(インターネット基盤委員会)で検討開始
 1. TLD文字列
 2. レジストリの要件
 3. レジストリ選定の基準と手続き
- 委員会構成
 - 主査 村井純 慶應義塾 常任理事・慶應義塾大学教授
 - 委員
 - 有識者(技術、法律、社会、等)
 - 協会等(主に利用者)
 - メディア
 - オブザーバー
 - インターネット関連団体等 (JPRSを含む)
- 2009年後半に、RFP(提案募集)実施予定

検討状況

- 直近のスケジュール
 - 2009年4月28日 報告書案公開、パブリックコメント募集開始
 - 2009年6月3日までがパブリックコメント募集期間
- 報告書案の概要
 - TLD文字列は、「.日本」
 - 「.日本」と「.jp」の登録者を同一に限らない（「.日本」導入後一定期間は「.jp」登録者を優先登録）←ドメインの有効活用のため
 - 導入当初は登録者を日本の個人法人に限定 ←利用者保護のため
 - 管理運営事業者の選定方法
 - 民間協議会が「選定委員会」を設け、公正・中立・透明な比較審査を実施
 - 審査項目：技術的能力、経営基盤、事業計画、事業運営の公正性・透明性、コンプライアンス体制、利用者対応の体制、国際的役割の遂行、インターネット発展への貢献
 - 民間主導で選定し、国はその結果を原則尊重してICANNに推薦状を送付
 - 新規事業者が不利にならないよう配慮