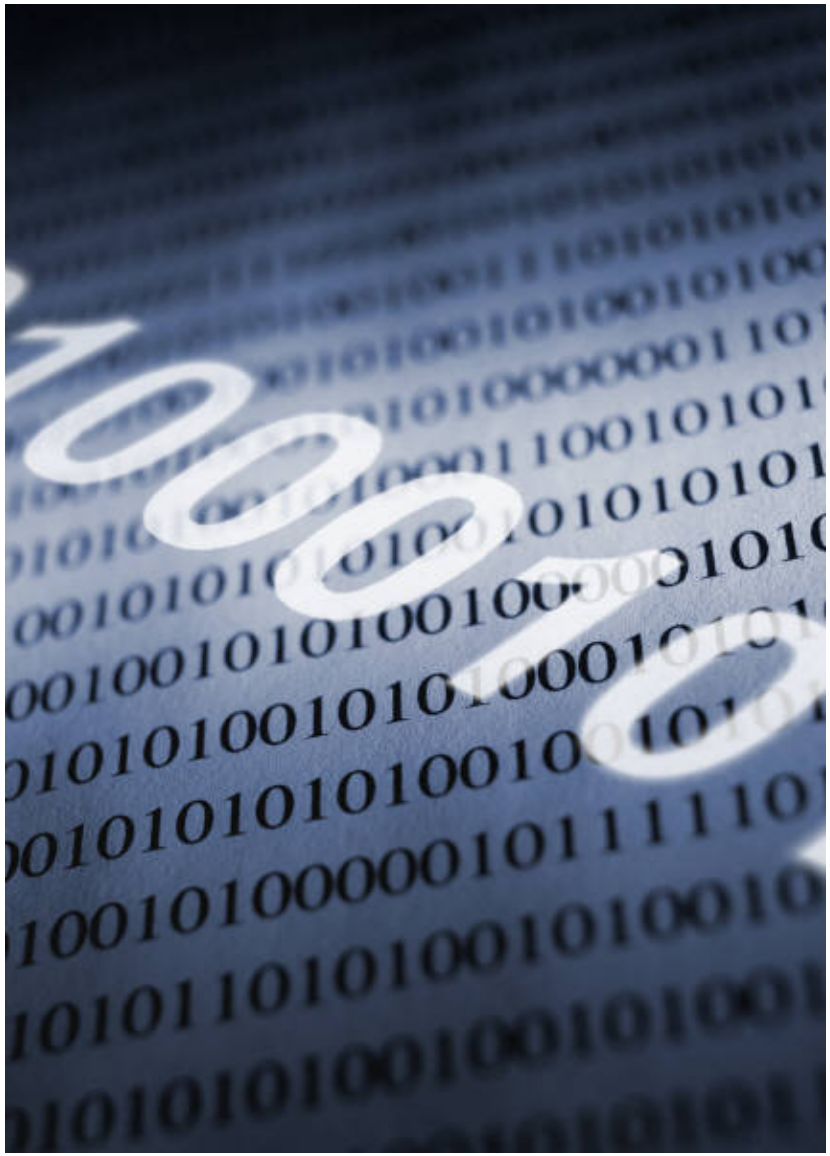


DNSのセキュリティ向上
DNSSEC

JAPAN REGISTRY SERVICES

Copyright © 2010 株式会社日本レジストリサービス

本日の内容

- DNSSECとは？
- 導入の背景
- DNSSECの仕組み
- DNSSECへの対応
- DNSSECの導入状況
- まとめ

Copyright © 2010 株式会社日本レジストリサービス

DNSSECとは？

Copyright © 2010 株式会社日本レジストリサービス

DNSSEC ～DNSのセキュリティ拡張～

Domain
Name
System

SECurity
Extensions

Copyright © 2010 株式会社日本レジストリサービス

DNSSECで何が変わる！？

これは本当にns.example.jpが回答したものか？

- **途中で回答が壊れてないか？**
- **偽者が回答したものではないか？**

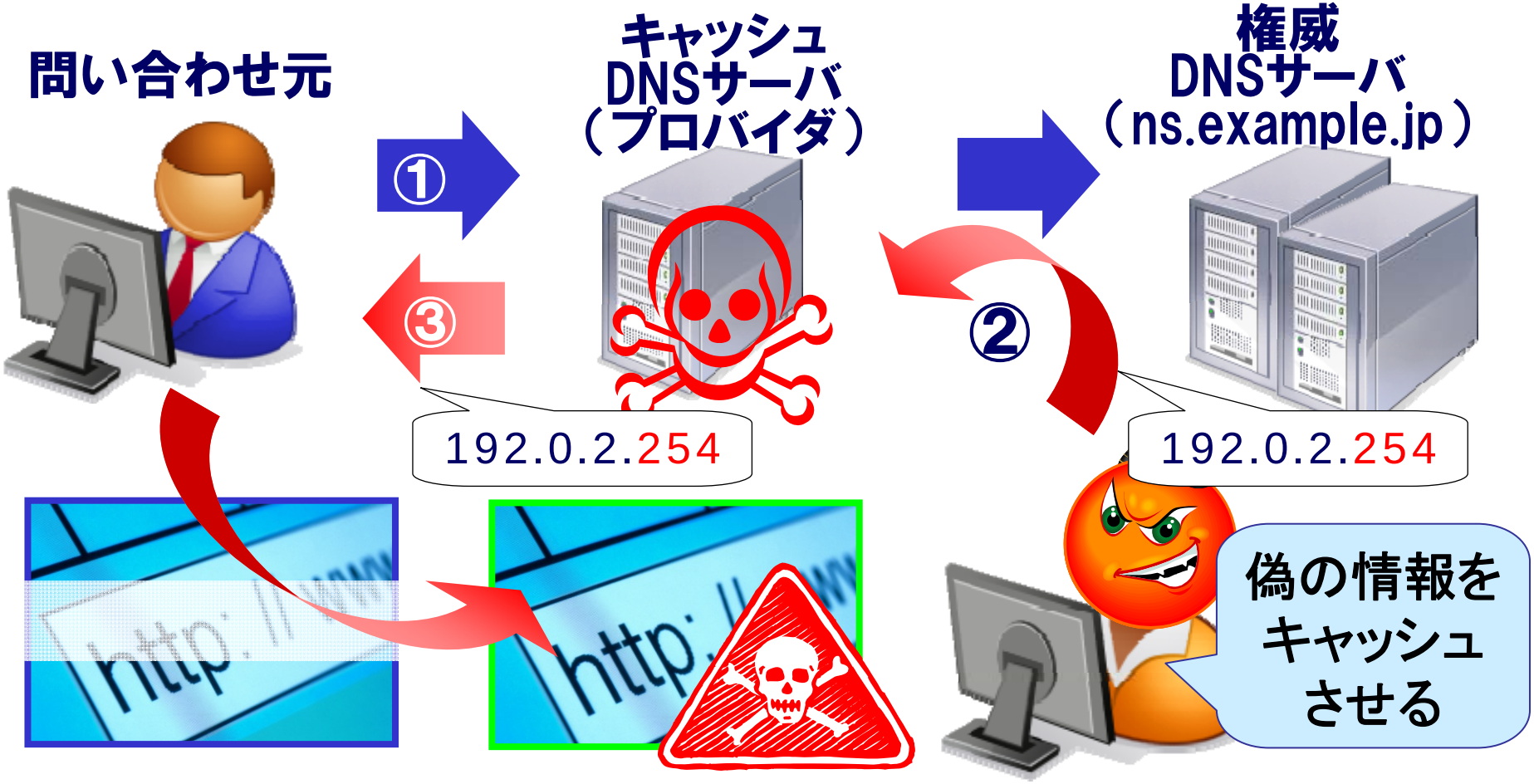
DNSSECでこれらを検知できる

Copyright © 2010 株式会社日本レジストリサービス

導入の背景

Copyright © 2010 株式会社日本レジストリサービス

DNSの脅威　～キャッシュポイズニング～



URLが本物のサイトと同じであるため、
見ただけでは判別できない。

Copyright © 2016 株式会社日本レジストリサービス

キャッシュポイズニング対策

① 攻撃が成功する確率を下げる

- ▶ 問い合わせポートのランダム化
- ▶ 権威DNSサーバの数を増やす
- ▶ 適切なアクセス設定を行う　　….など

⇒上記は現在すでに実施されている対策だが、
根本解決ではない

② DNS応答が本物か受信側で確認可能にする

⇒DNSSECの導入が有効！

Copyright © 2010 株式会社日本レジストリサービス

DNSSECの仕組み

Copyright © 2010 株式会社日本レジストリサービス

DNSSECでは何が保証されるのか？

1. **出自の保証**
   - ➔ 正当な発信者からの応答であること

2. **完全性の保証**
   - ➔ DNS応答が改ざんされていないこと

~~3. **通信内容の暗号化**~~
   - ~~➔ 通信内容を暗号化し、問い合わせ内容を秘密にすること~~

Copyright © 2010 株式会社日本レジストリサービス

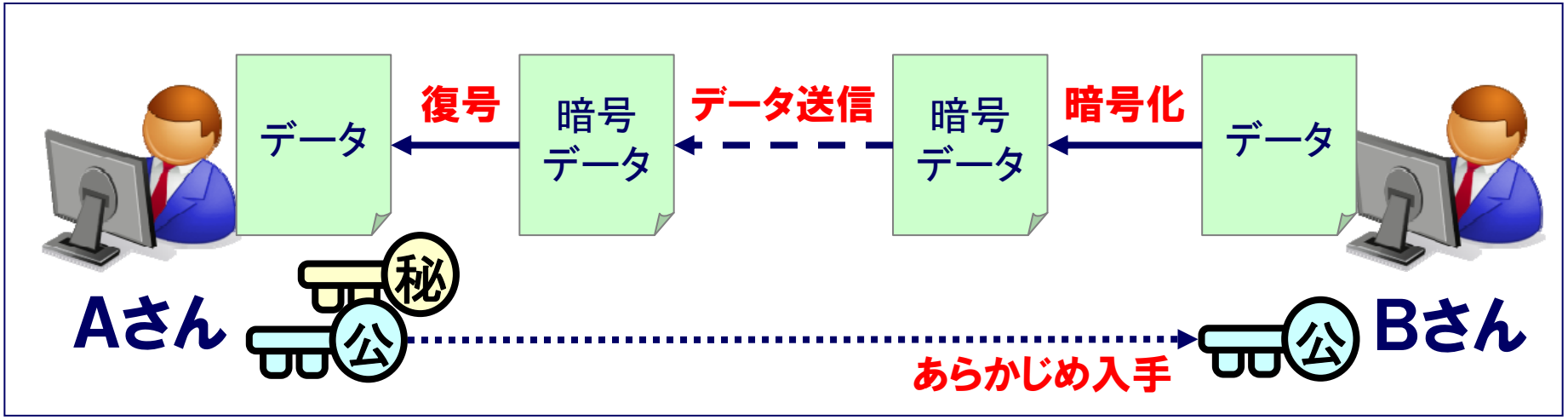
キーワード①　公開鍵暗号方式

■ ペアになっている2つの鍵（秘密鍵と公開鍵）を用いる

►秘密鍵・・・他人に見せない自分だけの鍵

►公開鍵・・・他人に見せてもいい鍵

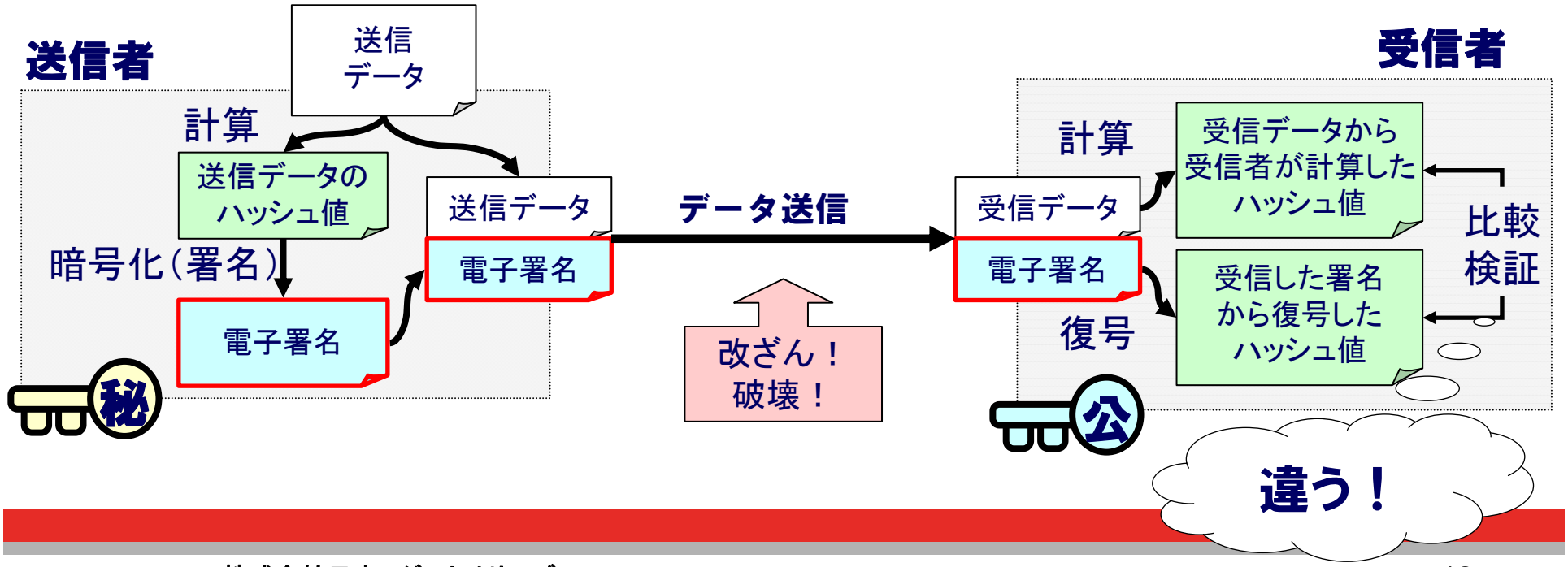
■ 一方の鍵で暗号化したデータは他方の鍵でのみ復号可能



Copyright © 2010 株式会社日本レジストリサービス

キーワード②　電子署名

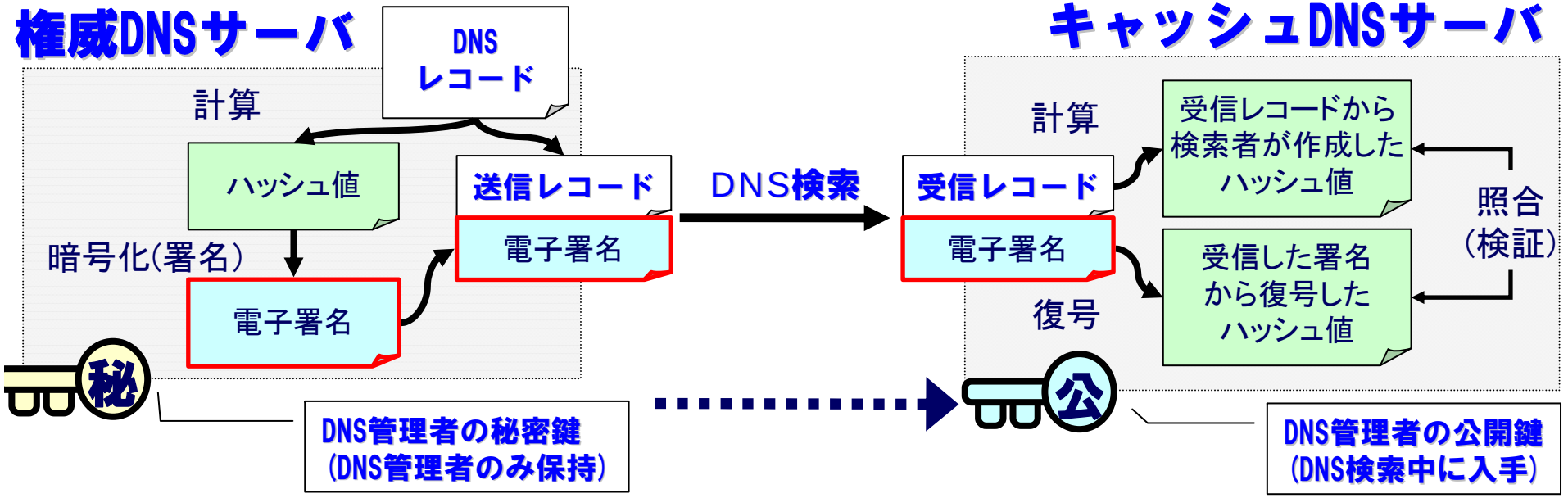
- 送信者は送信データからハッシュ値を計算し、秘密鍵で暗号化して送信データと一緒に送信
- 受信者は受信データからハッシュ値を計算し、署名を復号して得られたハッシュ値と比較検証



Copyright © 2010 株式会社日本レジストリサービス

電子署名のDNSへの応用

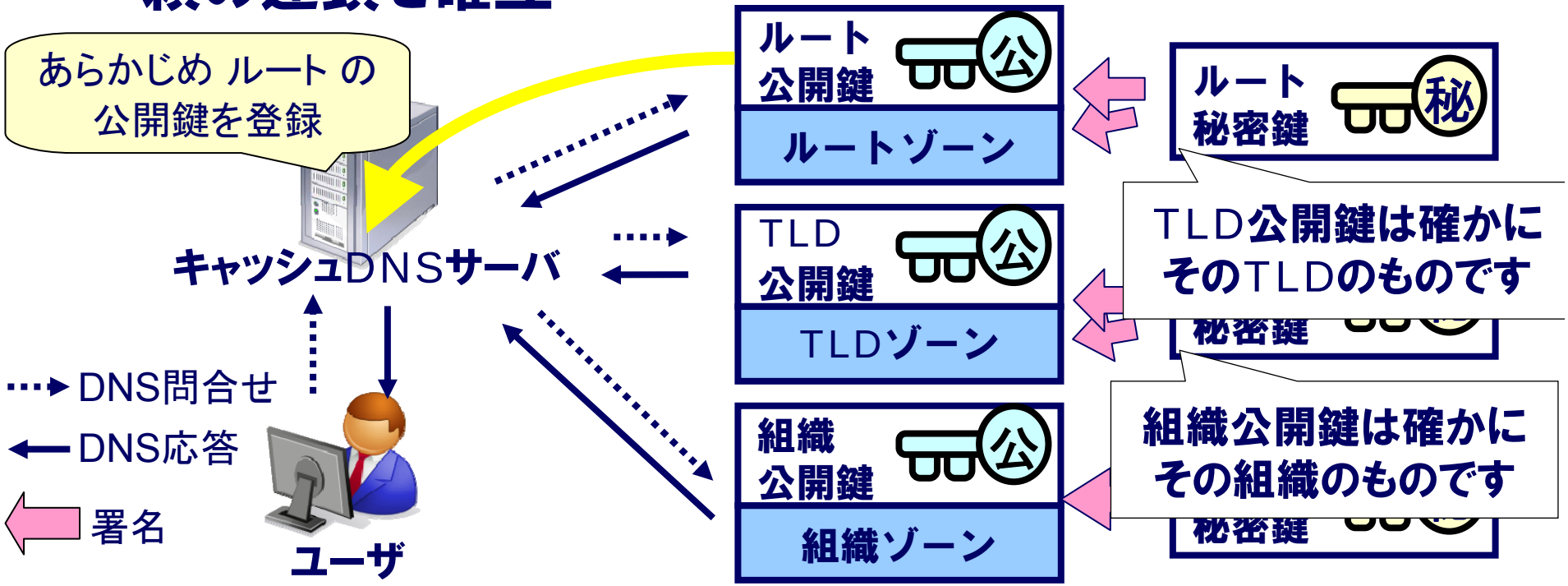
■ キャッシュDNSサーバはDNS管理者の公開鍵で署名を復号し、受信レコードから計算したハッシュ値と照合して検証を行う



Copyright © 2010 株式会社日本レジストリサービス

信頼の連鎖

- 秘密鍵で、自ゾーンと下位ゾーンの公開鍵に署名
- 最上位(ルート)の公開鍵をキャッシュDNSサーバに登録することでルートゾーンから組織ゾーンまでの信頼の連鎖を確立

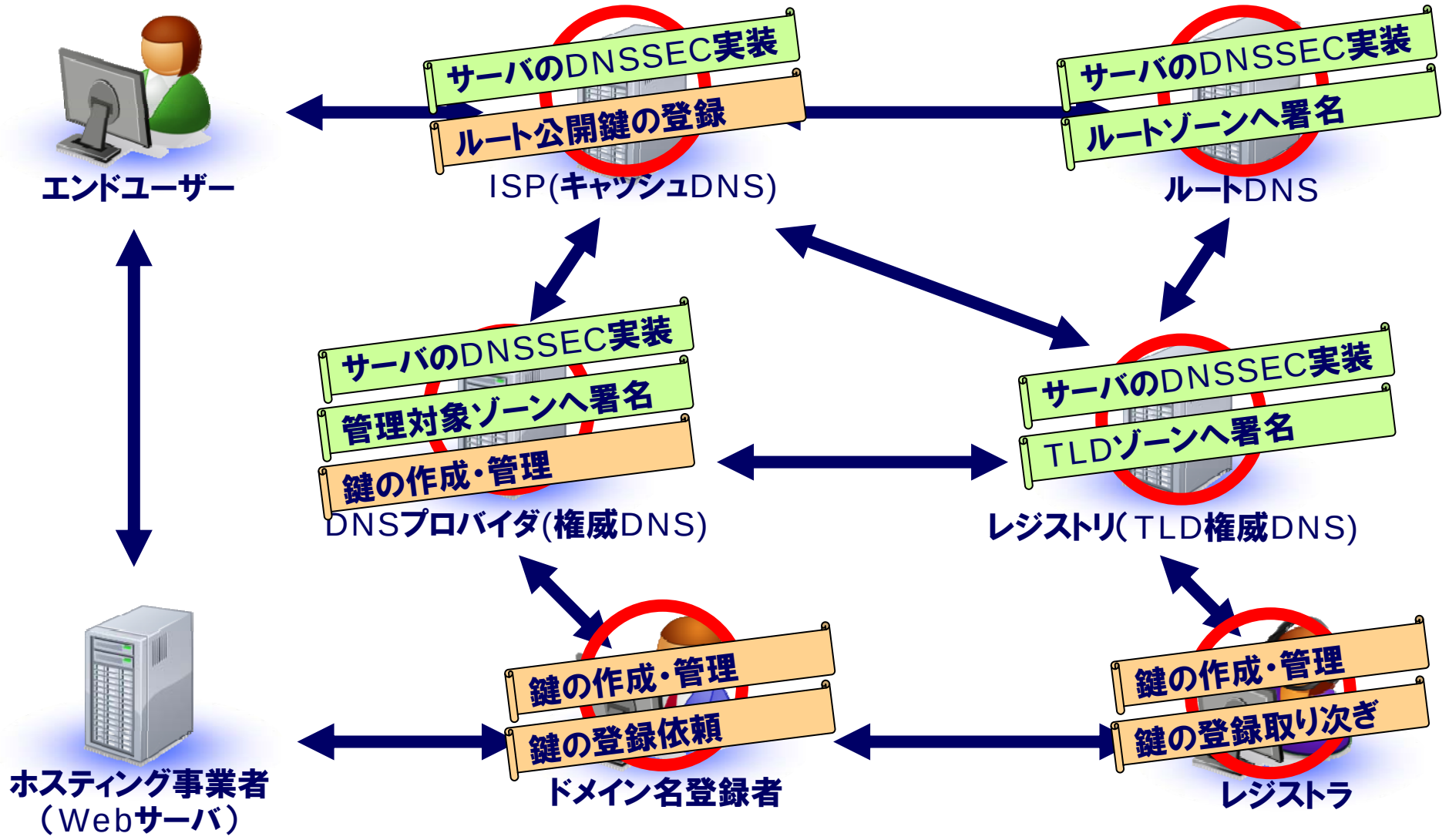


Copyright © 2010 株式会社日本レジストリサービス

DNSSECへの対応

Copyright © 2010 株式会社日本レジストリサービス

DNSSECで対応が必要な関係者



Copyright © 2010 株式会社日本レジストリサービス

DNSSECの導入状況

Copyright © 2010 株式会社日本レジストリサービス

各TLDの導入状況

ccTLD

►**導入済みの主な**ccTLD（**※試験的な導入も含む**）
.se(**スウェーデン**) .bg(**ブルガリア**) .br(**ブラジル**) .us(**アメリカ合衆国**) **など**

►**今後導入を予定している主な**ccTLD
.ca(**カナダ**) .ch(**スイス**) .cn(**中国**) .de(**ドイツ**) .jp(**日本**) .kr(**韓国**) **など**

gTLD

►**導入済みの主な**gTLD（**※試験的な導入も含む**）
.museum .gov .org

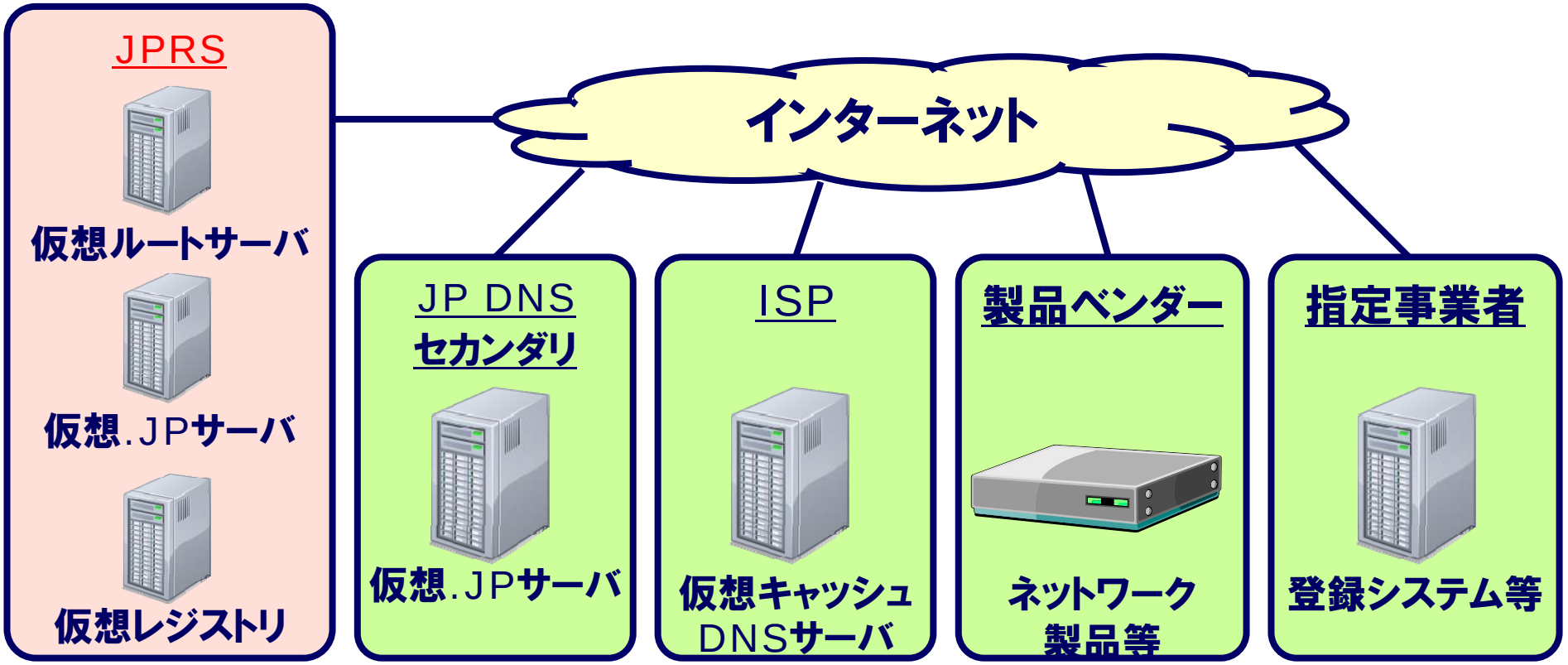
►**今後導入を予定している主な**gTLD
.biz .cat .com .edu .info .net

Copyright © 2010 株式会社日本レジストリサービス

.JPにおける取り組み

■ 段階を踏んだ技術検証を実施中

► JP DNSセカンダリ、ISP、製品ベンダー、指定事業者と協力し、実験環境を構築



Copyright © 2010 株式会社日本レジストリサービス

ルートサーバのDNSSEC導入状況

■ 2009年12月 DNSSEC導入のための実作業を開始

►インパクトが大きいため、段階的に導入

►検証できない署名データを追加したルートゾーン(DURZ※)を用意

■ 2010年5月 全ルートサーバでDURZの導入が完了

■ 2010年7月 正式運用開始

►ルートゾーンの公開鍵データを公開

►正規の署名データによるDNSSECの運用開始

※Deliberately Unvalidatable Root Zone

Copyright © 2010 株式会社日本レジストリサービス

まとめ

- DNSSECは、DNS応答の出自と完全性を保証する
- DNSSECの導入により、偽のDNS応答を受信側で検知する
- DNSSECでは、電子署名を応用することでデータを検証する
- DNSSECの普及には、各関係者の協力が必要不可欠
- ルートゾーンのDNSSECは、2010年7月から正式運用開始

Copyright © 2010 株式会社日本レジストリサービス

Copyright © 2010 株式会社日本レジストリサービス