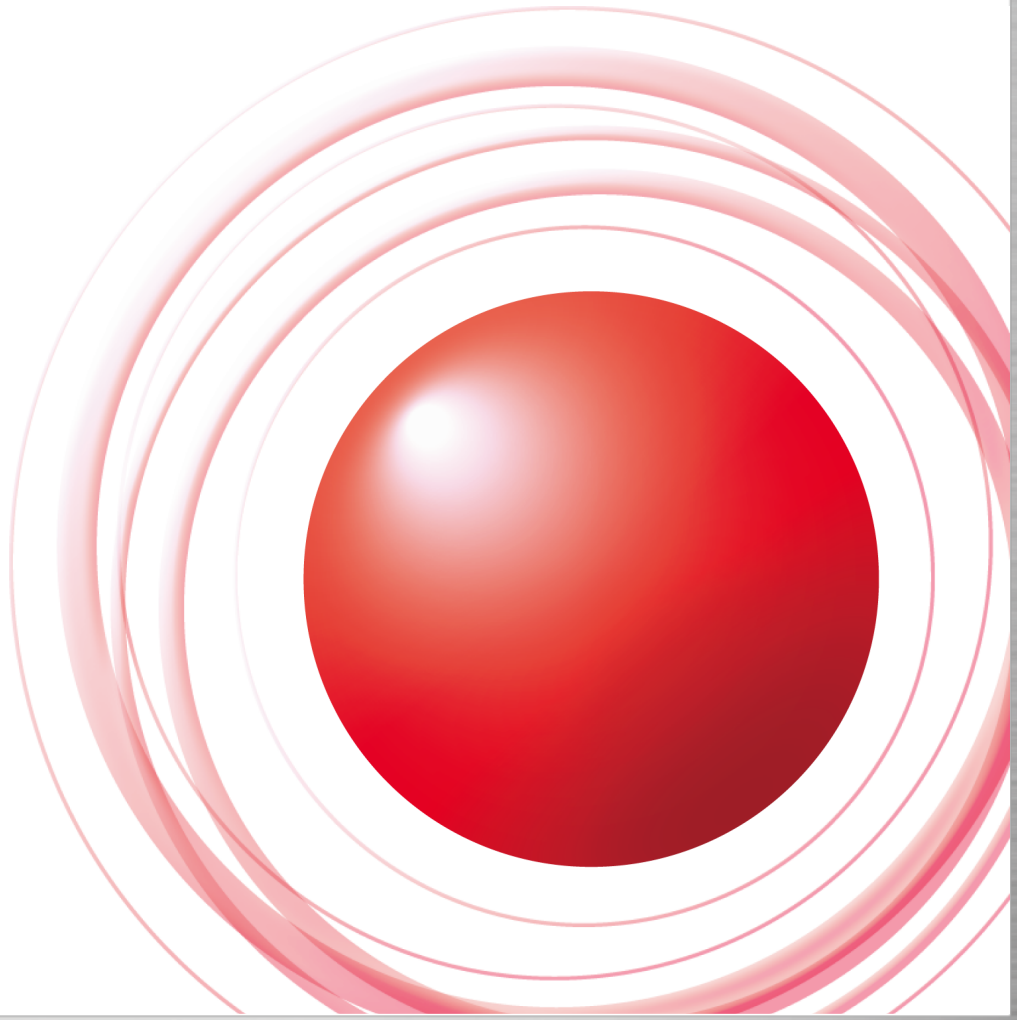
IIJ Technical Week

DNSSECの現状とIIJでの導入事例

IIJ Internet Initiative Japan



2011/11/11

株式会社インターネットイニシアティブ
サービス本部　アプリケーションサービス部
山本 功司

Ongoing Innovation

DNSSECの現状

DNSSECとは

- DNS Security Extension
  - RFC4033,4034,4035（他）
- Extension = 拡張
  - なくても動く
  - 実装されても、今までの実装も問題なく動く
- 公開鍵暗号の技術を使い、DNSのゾーンに対して署名を行う

DNSSECの原理

- ゾーンの権威委譲の仕組みを使い、信頼の連鎖を築く
  - DSレコード
    - NSで委譲した先のゾーンの署名鍵（のハッシュ）
  - ゾーンの署名鍵（のハッシュ）と、その委譲元にあるDSレコードが一致していることを検証
- ルートから目的のドメインまで、すべての階層でDNSSEC対応（署名）がされていないと、信頼の連鎖が築けない
  - . (root)
  - jp
  - iij.ad.jp

DNSSEC対応状況

- 2010年7月 rootゾーンの署名、TLDのDSレコード受け入れ開始
- 2010年10月 jpゾーンの署名開始
- 2011年1月 jpゾーンでDSレコードの受け入れ開始
  - jp配下のゾーンで、DNSSECの信頼の連鎖が築ける状態に

DNSSEC対応状況

- 2011年3月 .comでの署名、DSレコードの受け入れ開始
- 各種TLDでの対応状況
  - ICANN Research TLD DNSSEC Report
    - http://stats.research.icann.org/dns/tld_report/
    - 2011年11月1日現在、73のTLDで署名＆rootへのDS公開
  - Status map of DNSSEC deployment in ccTLD and gTLD
    - http://www.ohmo.to/dnssec/maps/
    - ブロードバンドタワー大本氏による調査

DNSSEC普及への課題

- 事業者の対応
  - レジストラ
  - DNSホスティング事業者
  - ISPでのキャッシュサーバの対応
- 費用対効果
  - 「鶏卵問題」
  - 運用の複雑さ
  - トラブルシュートの難しさ
  - 技術者の育成

IIJサービスにおけるDNSSEC対応のご紹介

ドメイン管理サービス

- サービス内容
  - 独自ドメインの登録申請、維持管理
- DNSSEC対応
  - DSレコードの上位DNS（TLD）への登録取り次ぎ
- JPドメイン 2011/01/31サービス開始
  - 汎用JP型ドメイン管理サービス
  - 属性地域JP型ドメイン管理サービス
- gTLDドメイン 2011年8月より順次サービス開始
  - gTLD型ドメイン管理サービス
    - 旧来のサービス契約では、対応レジストラへ移行する必要あり

権威DNSサービス
DNSアウトソースサービス

- サービス内容
  - DNSサーバのホスティング
- DNSSEC対応
  - ゾーンの署名、鍵の管理
  - お客様はWeb画面からボタン一つで署名開始、メンテナンスフリー
- 2011/01/31サービス開始
- 制限事項
  - 上位へのDS登録自動化の都合上、ドメイン管理サービスとの併用に限る
  - サブドメインには未対応

権威DNSサービス
DNSセカンダリサービス

- サービス内容
  - セカンダリDNSサーバのホスティング
- DNSSEC対応
  - お客様側プライマリサーバが署名すればセカンダリも対応
  - NSEC3/RSASHA256等のパラメータに対応
- 2011/01/31サービス開始

サービス対応における基本方針

- DNSSECを有効にしたいお客様が利用できる環境を提供
  - IIJの顧客（大企業、官公庁、教育機関等）のニーズ
- お客様が利用を希望した場合のみ、オプションとして提供
  - 特に導入初期はトラブルを懸念して導入を希望しないお客様も存在する
- オプション利用料金は無料
  - 利用希望の有無はあれど、サービスとしては備えているべき基本機能という考え
  - 現状、有料としたところでその収入でコストを回収できるとは思えない

キャッシュサーバ

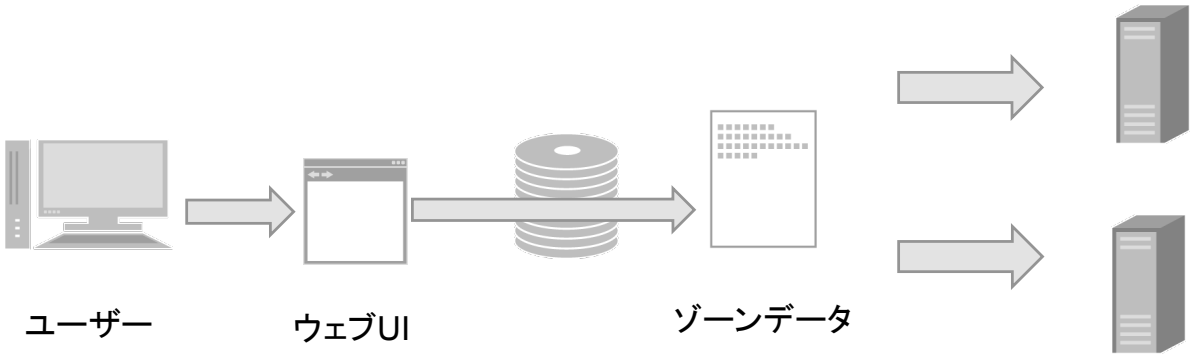
- 技術的な検証等、導入準備は完了
- 様子見中
  - TLDや逆引きゾーンでの障害
    - 鍵ロールオーバーの失敗
    - 署名有効期限切れ
- DNSに関連した各種イベント
  - 児童ポルノブロッキング（4/21～）
  - World IPv6 Day（6/8）
- 今年度下半期での導入を視野に

キャッシュサーバ

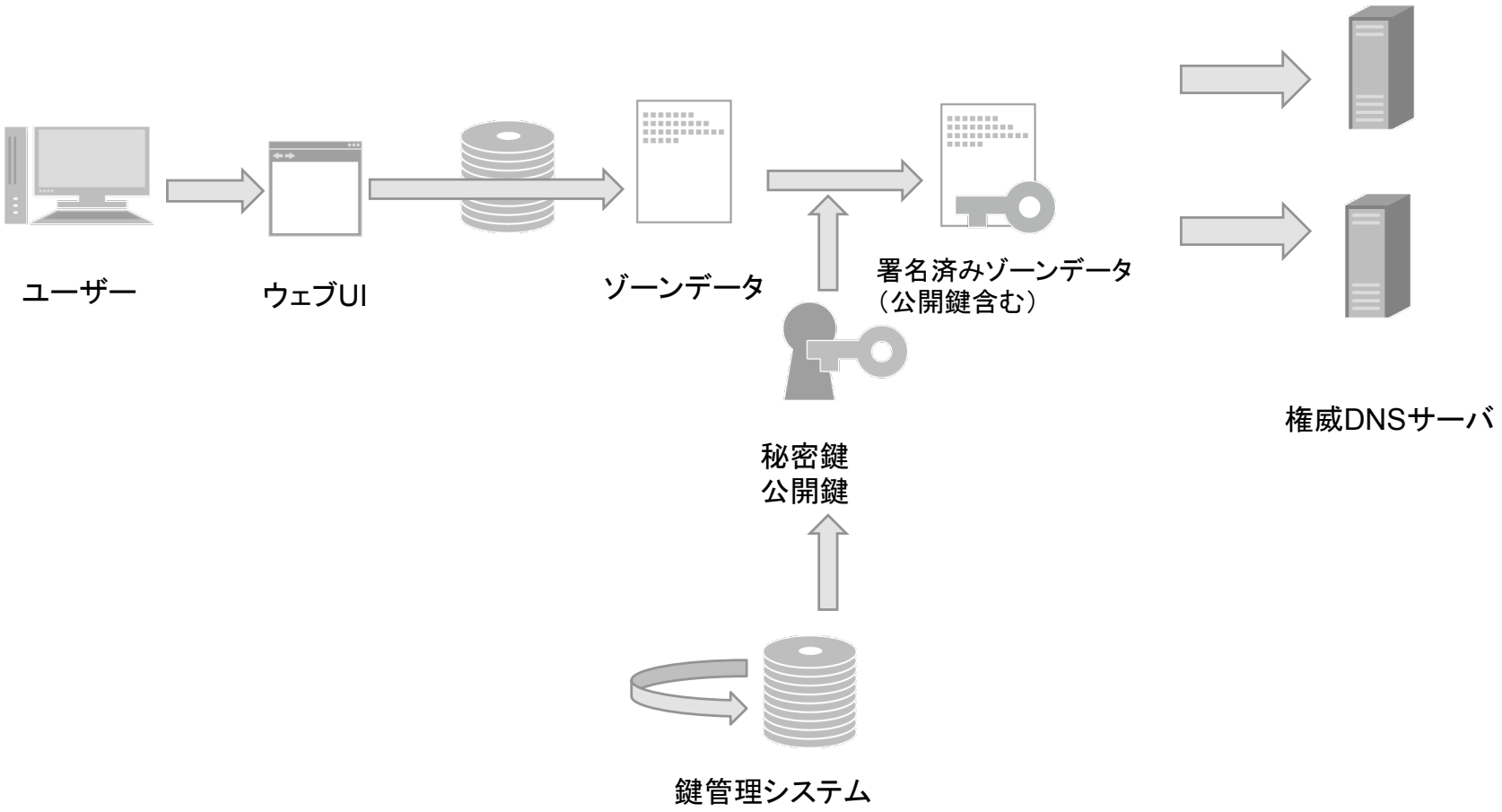
- 技術的困難はあまりない
  - CPU、メモリ等のマシンリソースに気をつける
- 他者要因でユーザーに影響が出てしまう
  - 自社が完璧な運用をしていても、TLDの運用ミスで特定TLD以下の全ドメインが引けなくなってしまう可能性
  - 現時点で積極的にキャッシュサーバでのバリデーションを求めているユーザーはごく一部

システム面でのDNSSEC対応の考え方と今後の可能性

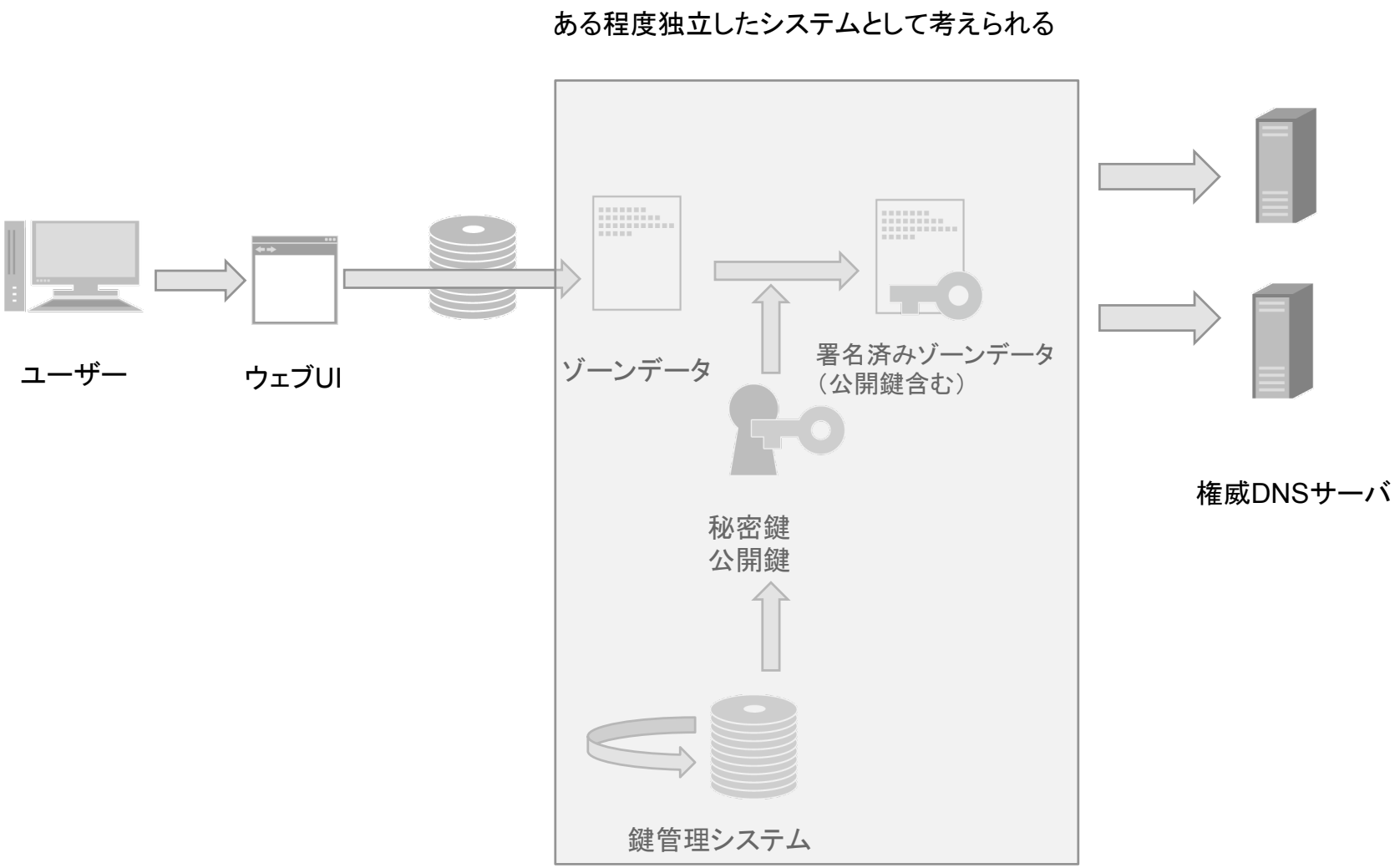
一般的なDNSホスティング



DNSSEC対応DNSホスティング



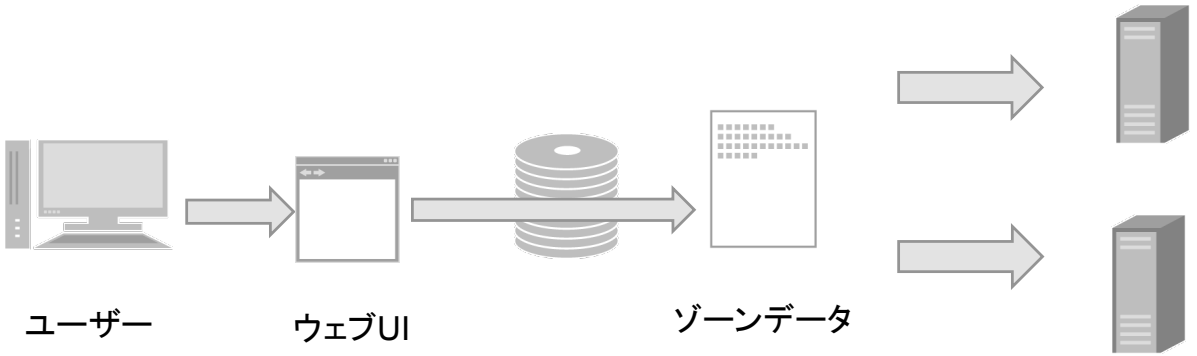
DNSSEC対応DNSホスティング



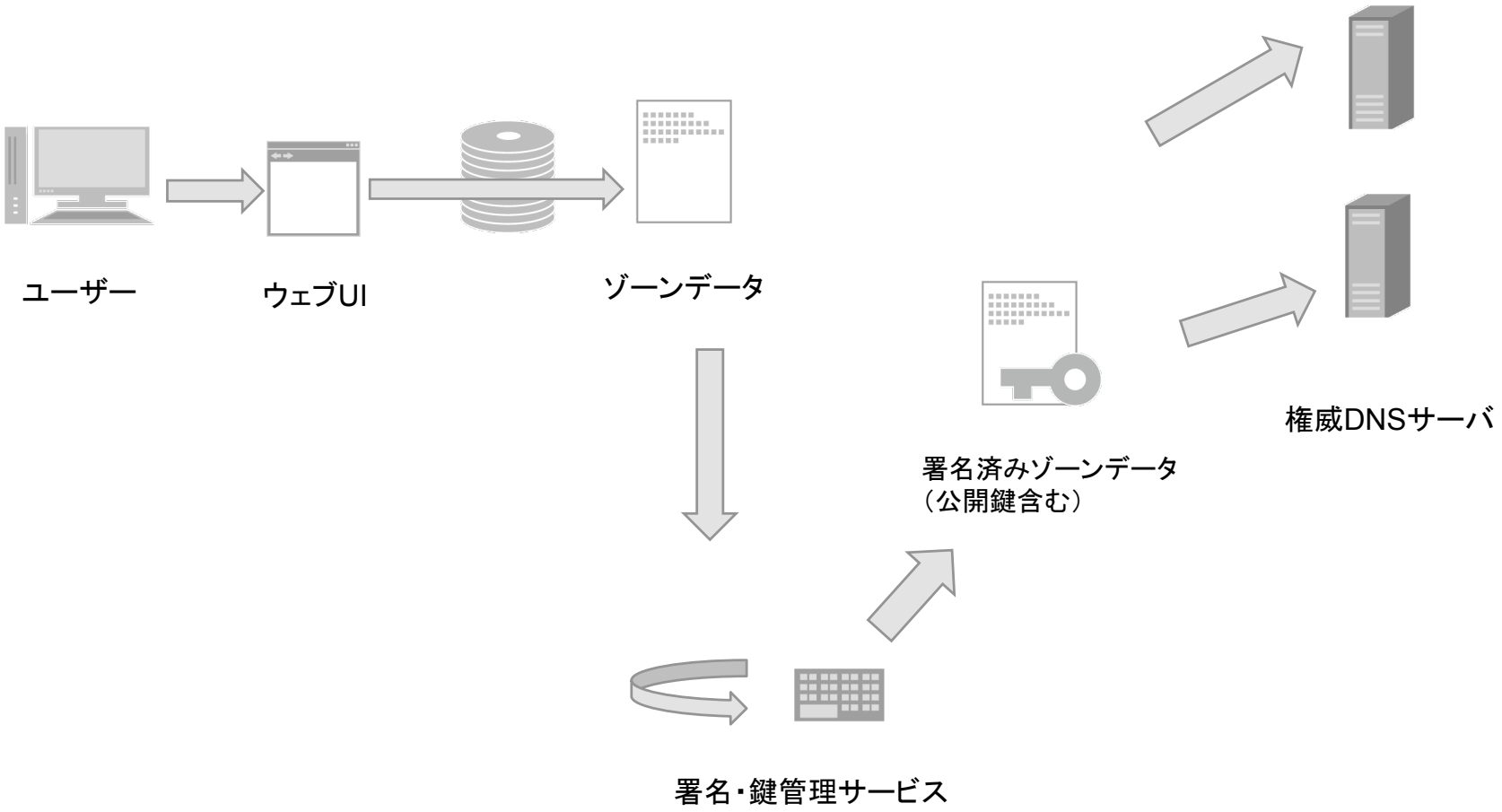
署名・鍵管理システム

- DNSSEC対応の肝
  - 鍵ペア、DSの生成
  - 鍵の更新タイミングの管理
  - 署名
  - 再署名タイミングの管理
  - 生成された署名済みゾーンの検証
- 既存の系からは独立したシステムとして扱える
  - その部分だけ切り出して提供？
  - 署名・鍵管理サービス？

一般的なDNSホスティング



DNSホスティング＋署名・鍵管理サービス？



DNSSEC zone signing service

- Verisign
  - gTLD（ICANN認定レジストラ向け）
  - ゾーン転送（AXFR/NOTIFY）とSOAP API
- Nominet
  - .uk向けにVerisignと同様のサービスを提供
- 以上はTLDレジストラでのサービス
  - DSの登録を考えると、レジストラがサービスするのが自然
  - それ以外でもCommunityDNSで同様のサービスをしている模様
  - 需要があるようであれば検討したい

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation