

DNSSECジャパン DNSSEC 技術検証WG 活動報告

技術検証WG Chair

豊野 剛

toyono@mfeed.ad.jp

DNSSECジャパン

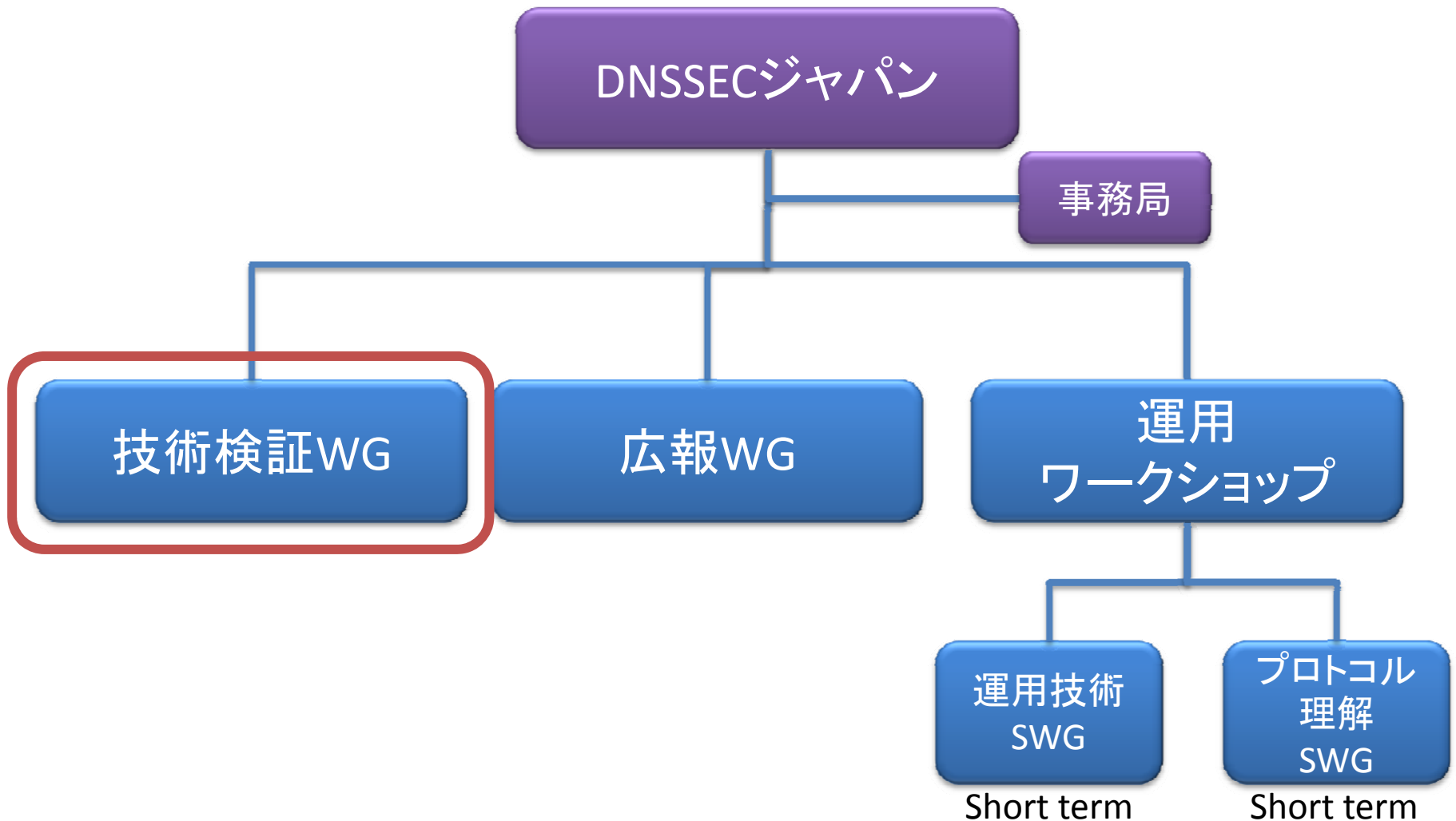
目的と活動内容

- 目的
 - DNSSECの導入・運用の課題の整理・検討
 - 参加者の技術力の向上, ノウハウの共有
 - 対外啓蒙活動
- 活動内容
 - DNSSECの導入・運用に関する
 - 課題の整理・共有
 - 技術検証の実施、ノウハウの蓄積
 - BCPの策定
 - 成果の対外的発信によるDNSSECの普及・啓発

技術検証WGの活動目的

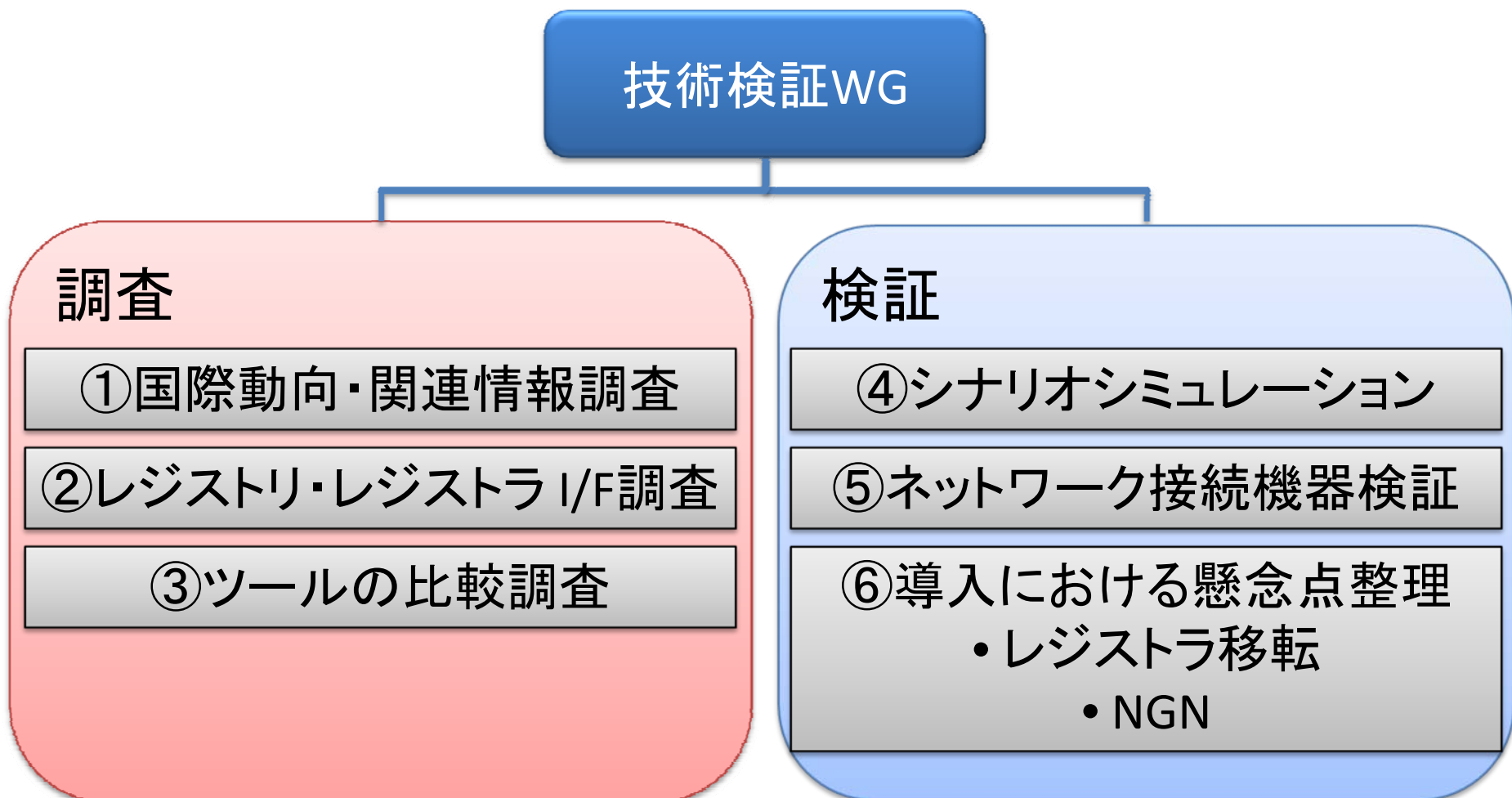
1. WGメンバが持つサービスやプロダクトにどのような影響が生じるかを調査，および実験環境の中で確認する
2. WGメンバが持つサービスやプロダクトのDNSSEC対応状況を確認し，運用ノウハウを共有・蓄積する
3. 蓄積したノウハウは必要であれば積極的にBCPやガイドラインとして公開する

DNSSECジャパン 技術検証WGの位置づけ



DNSSECジャパン

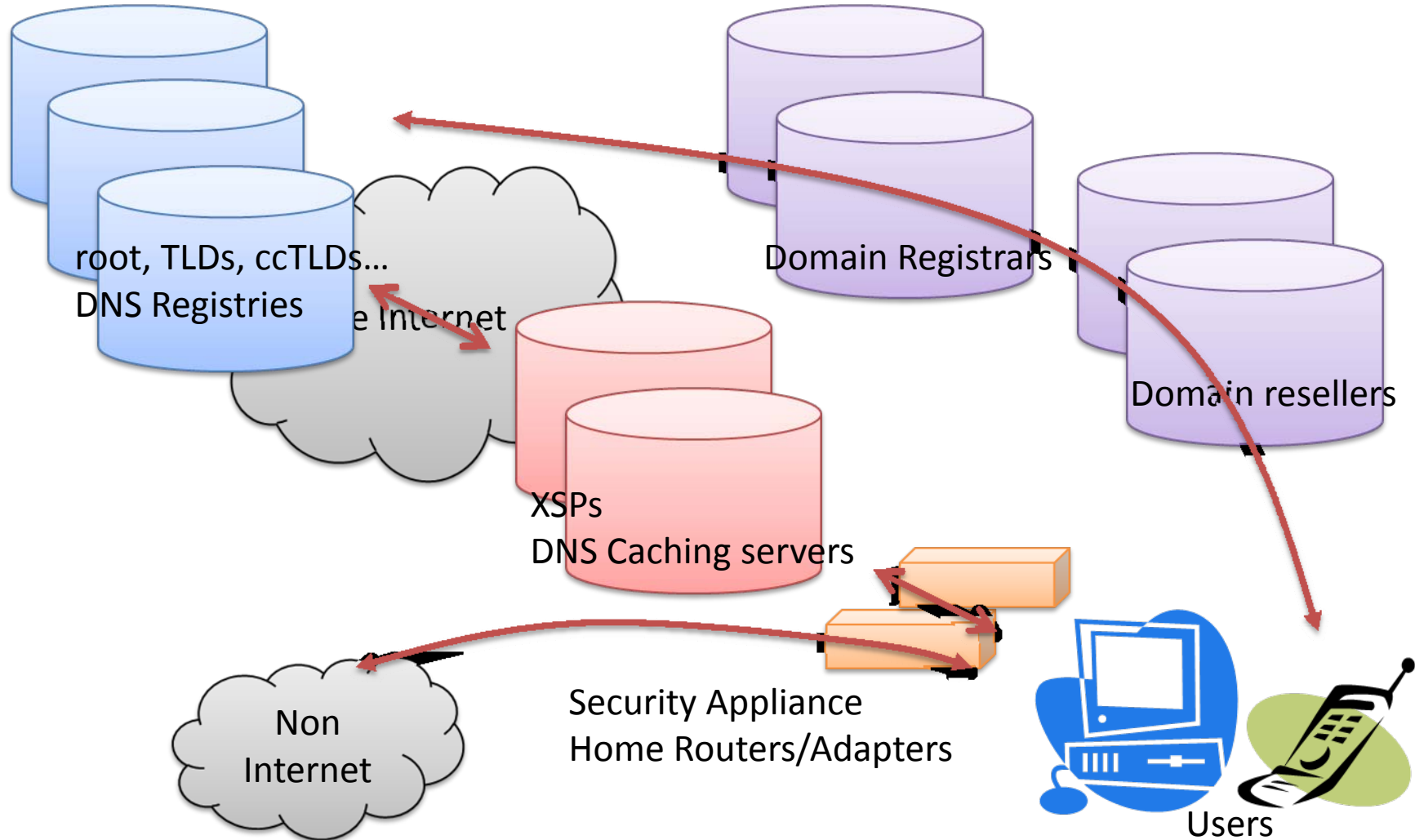
技術検証WGの主な活動内容



技術検証WGの活動

- メンバは親会の中から参加
- 主な活動はメーリングリスト
- 隔週程度の定例打ち合わせ
 - 必要に応じて各調査・検証項目ごとに個別打ち合わせ
- 成果はメンバにフィードバック
- 対外的なアクションに関しては親会および広報WGと連動

DNSSECに関わるプレイヤー



実際の運用現場

上層部

DNSSECってあるらしいけど、ウチはいつやるの？

別の上層部

リスクがある？ちゃんと検証しろ！

営業方面

安全なドメイン名とか言うお客様が...

設備・予算

DNSってタダでしょ？お金かかるの？

時期・稼働

いつだれがいくらで？え、継続？

サポートセンタ

インターネットに繋がりませんというお客様が...

DNSの運用に関わる人々

技術検証WGの目的（再）

- サービスやプロダクトの調査・実験環境で確認
→ 現場が困りそうなことは予め検討しておく。
- 運用ノウハウを共有
→ 現場でハマることがあったら皆で助け合う。
- BCPやガイドラインとして公開
→ 自分たちだけじゃどうしようもない。皆にも気づいて助けてもらう。

各調査・検証項目について 現在の活動状況

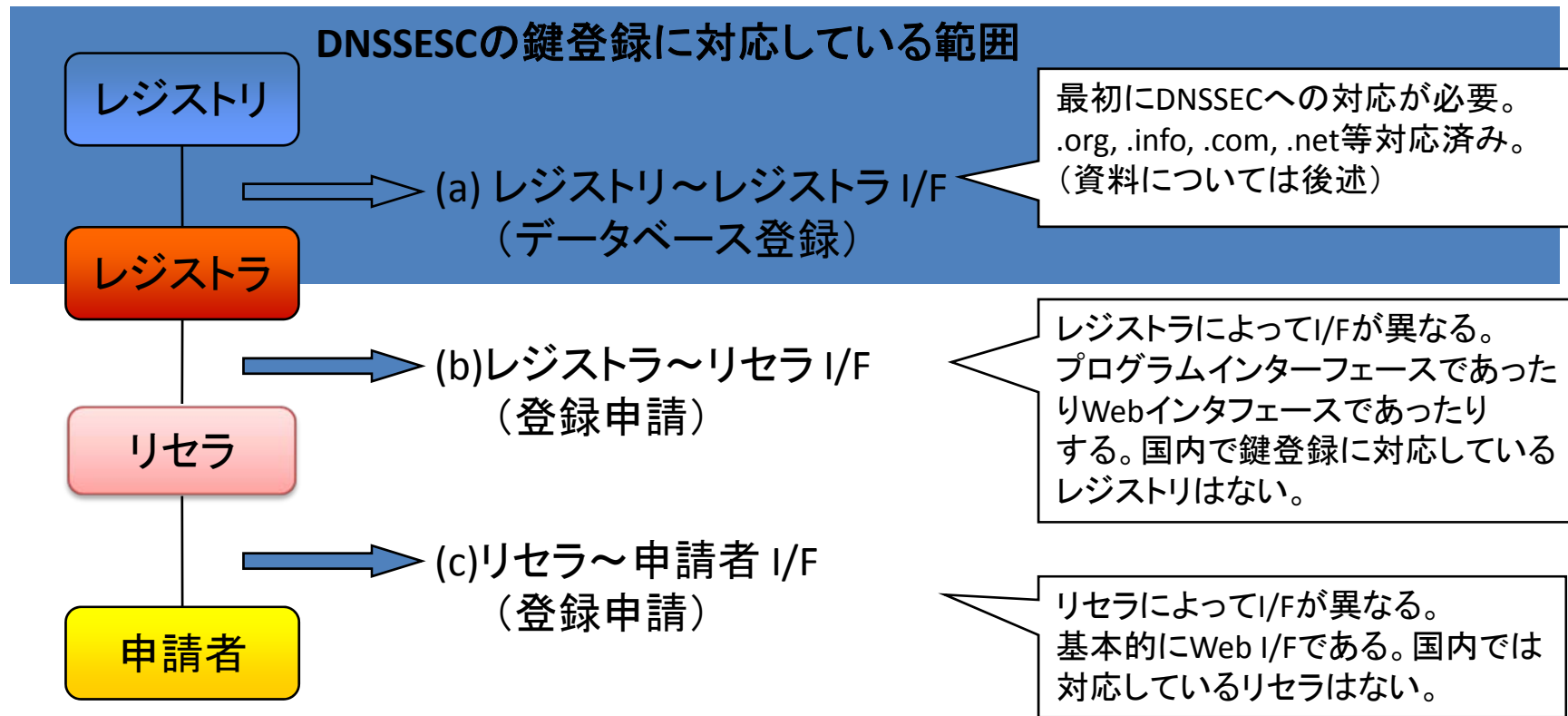
①国際動向・関連情報調査

- 調査の概要
 - 主に国外の最新のDNSSEC動向を調査し，日本語で短信として報告
 - 特に失敗談などは貴重なノウハウ
- 活動状況
 - 隔週開催の定例会内で報告中
 - 今後，要望があればレポート内容は広報WGと連携して公開も検討します

②レジストリ・レジストラ I/F調査

- 調査の概要
 - 国内でDNSSECを利用できるようにするには、レジストリ、レジストラ、リセラー等におけるDNSSECのための鍵登録に対応する必要がある
- 活動状況
 - 国内の対応状況を調査
 - レジストラにおける今後の対応のための情報源を収集，整理

ドメイン名登録I/Fにおける 鍵登録への対応状況



日本国内で鍵登録I/Fに対応しているレジストラがない。(2010年7月現在)

そこで、レジストラ向けの情報を収集すると共に、リセラーに鍵登録I/Fに関する要望をヒアリングした。

レジストリによる レジストラ向けの情報

- PIR (.ORG)
- <http://www.pir.org/dnssec>
 - DNSSECの解説記事の他にブロードバンドルーターへの影響や, ISPにおけるDNSSEC対応のためのチェックリストなどを公開
 - レジストラ向けの鍵登録I/FについてはWebExやデータシートを提供。
- VeriSign (.COM, .NETなど)
- <http://www.verisign.com/domain-name-services/index.html>
 - レジストラに関する情報を公開している。
 - 鍵登録I/Fに関する情報はレジストラのメンバーページにて提供。
- Affilias (.INFO, .MOBI, .ASIA, .AERO, ccTLDs)
- <http://www.afilias.info/dnssec>
 - 鍵登録I/Fについてのマニュアルはレジストラメンバサイト内で提供。
 - 「DNSSEC overview」(DNSSECの概要)や「Securing a Domain SSL vs DNSSEC」(ドメインのセキュリティに対するSSLとDNSSECの違い)といった記事も。

internet myf リセラへの鍵登録I/Fに関するヒアリング

- 複数のリセラーに共通した要望事項
 - 顧客向けWebではDSの登録を受け付けられることが望ましい
 - DNSサーバは顧客が管理していることがあるため
 - リダイレクトできるようことが望ましい
 - ドメイン名の設置当初はリダイレクトサービス（転送サービス）が必要.
 - 鍵の有効期限切れを知らせてくれることが望ましい
 - ドメイン名の移転と同時にDNSSECもできるようにすることが望ましい

③ツールの比較調査

- 調査の概要

- DNSSECの導入にあたっては、鍵や署名の管理・更新と言ったこれまでにない運用が必要
- 人力による運用には限界があり、ツールのサポートが必要となる



- DNSSECの導入・運用に有用なプロダクトの情報を、オープンソースやベンダー製品を問わず調査・公開

- 活動状況

- ツールの分類整理中。実証検証しているものも有り。
- 結果は整理後、公開予定。

分類項目

- DNSSEC対応DNSサーバ
→DNSSECに対応したDNSサーバ製品を分類
- 開発ツール/ライブラリ
→DNSSEC導入のために開発者が開発を行うために必要なツール/ライブラリを分類
- 運用サポートツール
→DNSSECの鍵の生成・管理や運用の自動化を行う運用サポートツールを分類
- 動作検証・活用ツール
→DNSSECの動作検証や実際にDNSSECを活用するためのツールセットを分類

調査対象分類

- DNSSEC対応DNSサーバ

- ISC BIND
- NLnetLabs NSD
- NLnetLabs Unbound
- Infoblox
- Nominum ANS & ANSP
- Secure64 DNS Server
- F5 DNS SECURITY SOLUTIONS
- DNSSHIM

- 開発ツール/ライブラリ

- libbind
- Idns
- libepp-nicbr
- Net::DNS::SEC
- Net::DNS::ZoneFile::Fast
- DNSRuby
- DNSJava
- DNSPython

- 運用サポートツール

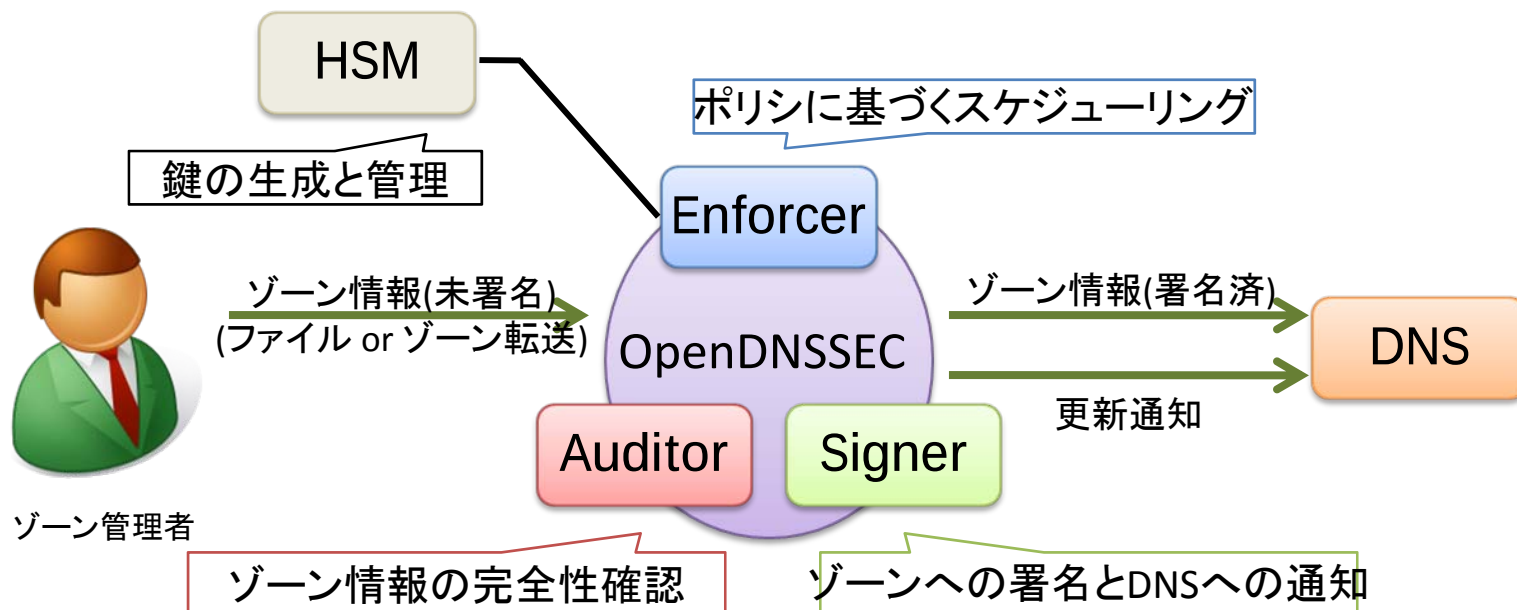
- OpenDNSSEC + SoftHSM
- DNSSEC Zone Key Tool
- DNSSEC Smartcard Utility
- DNSSEC Key Management Tool
- Vanteges
- AutoTrust

- 動作検証・活用ツール

- DNS Check
- DLV Test
- Sec Spider
- DNSSEC Reply Size Test
- DNSSEC Tools
- DNSSEC Toolkit
- Drill Extension for Firefox

例) OpenDNSSEC + SoftHSM

- DNSSEC運用の全課程を自動化することを目的として作られた運用支援ツール
- 鍵の管理、ゾーンの再署名、鍵のロールオーバーをスケジューリングして自動実行
- PKCS#11に準拠したHSMの利用を前提とし、代替となるSoftHSMも併せて提供



④シナリオシミュレーション

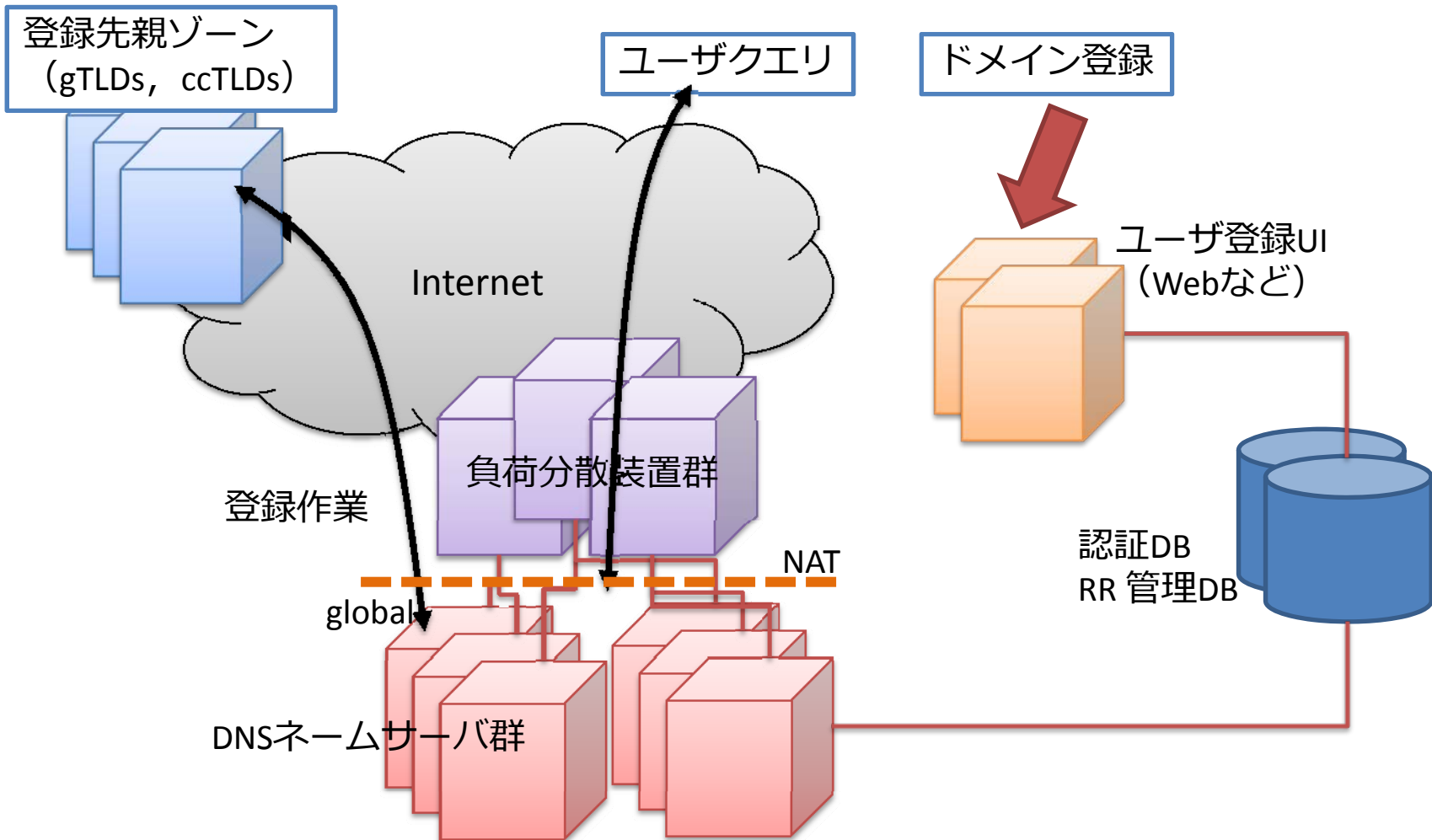
- 検証の概要

- DNSSEC導入検討事例を具体的な実手順により検討し，新たな課題や検討漏れがないかを参加メンバーで再確認・共有
- 導入事例としては以下の2つを想定
 - ネームサーバ運用者（レジストラ・リセラー）
 - キャッシュサーバ運用者（ISP）

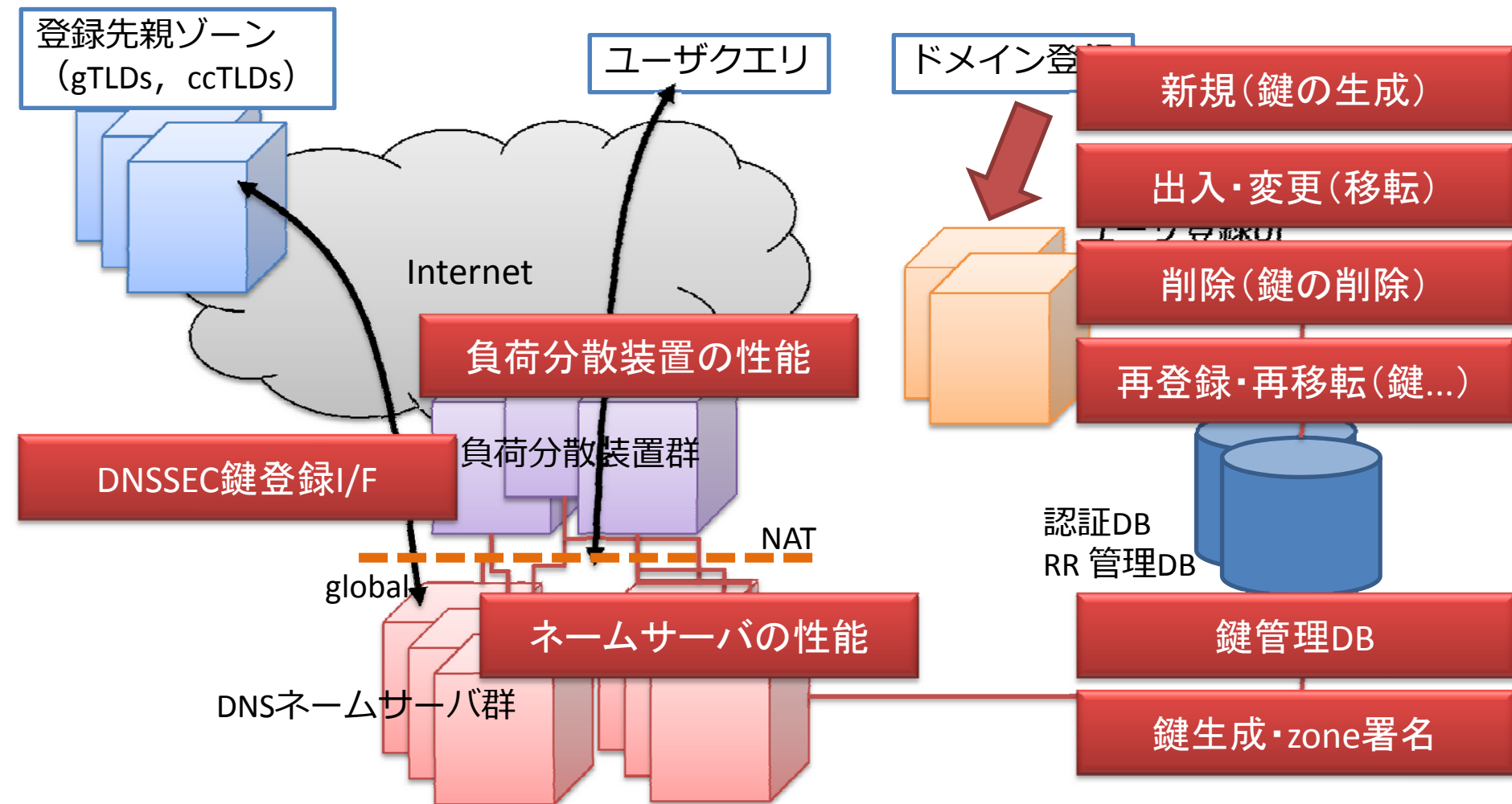
- 活動状況

- ネームサーバ運用の移行モデルについては検討済
 - 参加メンバーの1社を実例に，専門部会を開いて皆で議論

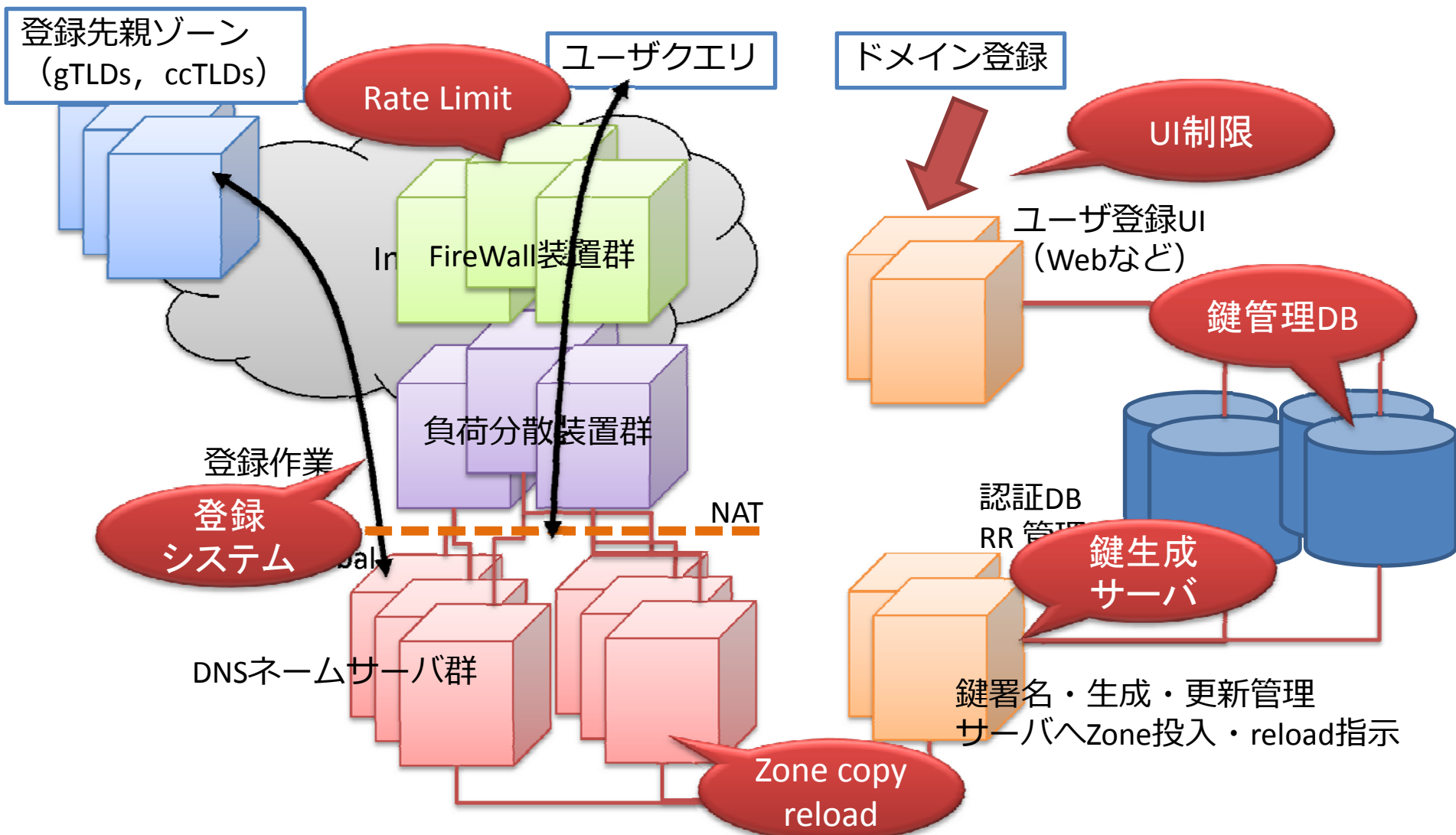
移行モデル (ドメインリセラの一例)



移行モデル (ドメインリセラの一例)



移行モデル (ドメインリセラの一例)



モデル検討により判明したことなど

- 思ったより機能変更が多い
 - 鍵生成・鍵管理・zone署名・実機へのzone情報反映
 - 持っているTLDの数だけ鍵登録システムの変更が必要
- UIを考えないと危険
 - DNSSEC署名・署名解除とか
 - 削除・再登録とか
- 設定も改めて見直しが必要か
 - 負荷分散装置の設定
 - Amp攻撃・DDoS攻撃等に対してのRate Limit
 - TCP port53 Filtering

⑤ ネットワーク接続機器検証

- 検証の概要
 - DNSSEC導入に当たって、オペレータは各種NW装置を含めた総合的な疎通性を評価する必要がある
 - チェックポイントは何か、の項目作りも重要
- 活動状況
 - NW装置の有無によるDNSSEC疎通確認、性能評価
 - 端末装置の有無によるDNSSEC疎通確認、性能評価（検討中）

NW装置のチェックポイント(例)

- **想定装置**

- 負荷分散装置

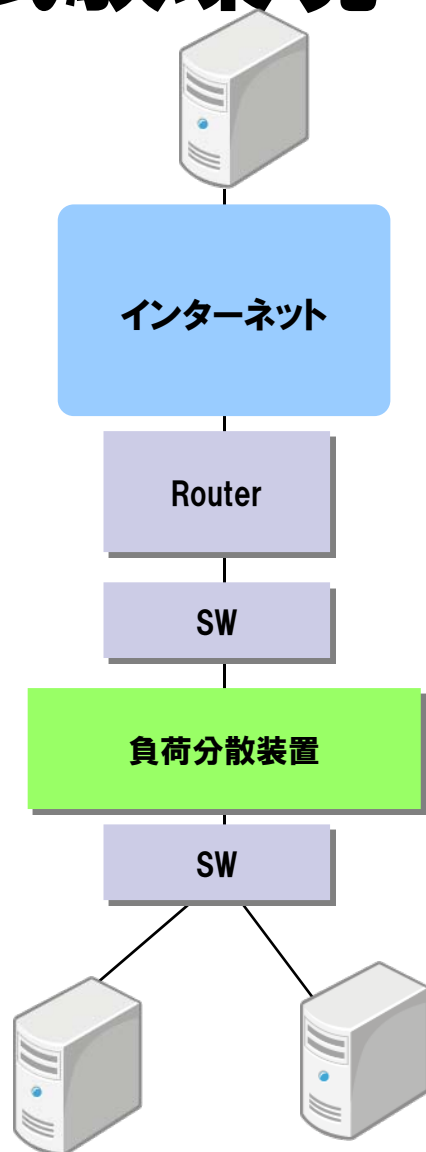
- **目的**

- (1) NW装置の構成が有り/無しで、DNSSECの通信に影響を測定する
 - (2) NW装置の構成が有り/無しで、キャッシュサーバ側の性能影響を測定する

- **負荷分散装置のチェックポイント**

- ①大きなUDPパケットを通せるか
 - ②UDP Fragment
 - ③TCPフォールバック
 - ④NATではなくGlobalのReachability
 - ⑤UDPのセッション数

一次試験環境



権威サーバ

インターネット

Router

SW

負荷分散装置

SW

キャッシュサーバ

L2SW, 負荷分散装置, Router
を経由した実証的な環境で負荷
試験を想定

その他のDNSSEC 中継装置と チェックポイントなど

- 想定される装置とチェックポイントはまだ洗い出しが必要
 - 想定される中継装置など
 - ブロードバンドルータ・VoIPアダプタ・ターミナルボックス
 - 無線機器
 - FireWall装置（宅内, エンタープライズ, NW）
 - 負荷分散装置
 - 想定されるチェックポイントなど
 - EDNS0対応およびUDPパケットサイズの取り扱い
 - UDP Fragment
 - TCP Fallback, TCP port 53 Filtering
 - UDP Stateの扱い（特に負荷分散装置, NAT装置など）
 - DNSキャッシュ機能, DNS Proxy機能

⑥ 導入における懸念点整理

- 検証の概要

- DNSSEC導入に伴い問題が発生しそうな事象に関しては、BCPやガイドラインを公開し啓蒙活動に努める
- 導入における懸念点に関するBCPの作成

- 活動状況

- (6-1) レジストラ移転手順検証
 - RFC4841bisは本当に動くのか？
- (6-2) NGN対応検討
 - DNSSEC + NGN対応でXSPのすべきことは？

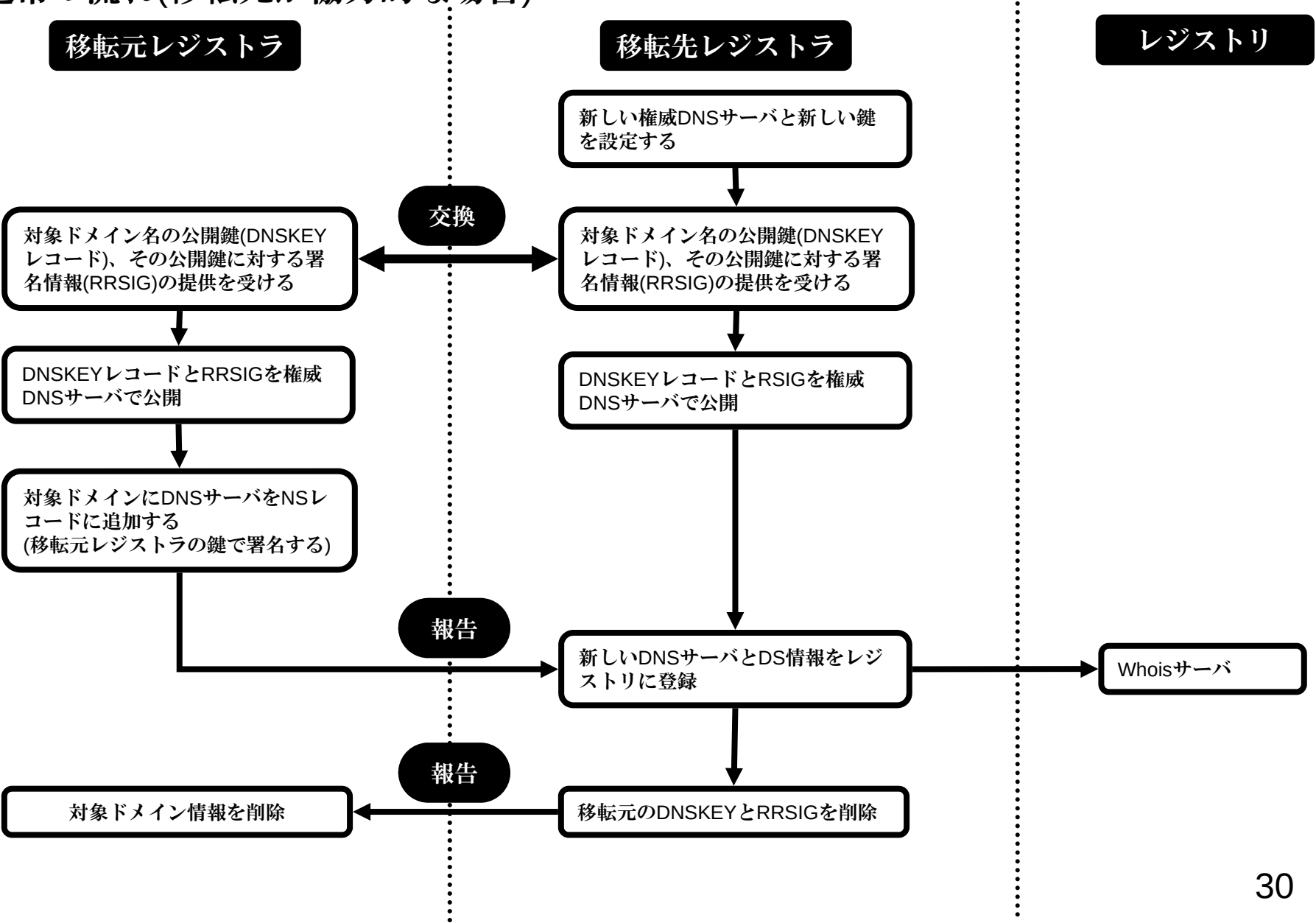
⑥ 導入における懸念点整理

(6-1) レジストラ移転手順検証

- 運用する上で考えておかなければならないこと
 - 対応方針をあらかじめ決めておく必要がある（お客様希望の有無も）
 - 移転入の場合，移転元レジストラへ鍵交換の要求を行うか
 - 移転出の場合，鍵の交換に応じるかどうか
 - レジストラ同志の連絡先DB？
- 新旧のレジストラ同士でDNSKEYとRRSIGの交換が必要
 - 相手レジストラが協力的か，非協力的か
 - NSと同様にDSも引き継ぐ？（上位NSに設定）
 - 鍵の授受？
- レジストリへの要求事項もあるかもしれない？
 - ドメイン移転時にもNS設定と同様DSも引き継がれる仕様にする
 - その場合移転後のレジストラが設定されているDSを取得できる

DNSSEC移転の考えられる流れ確認(RFC4641bisベース)

通常の流れ(移転元が協力的な場合)



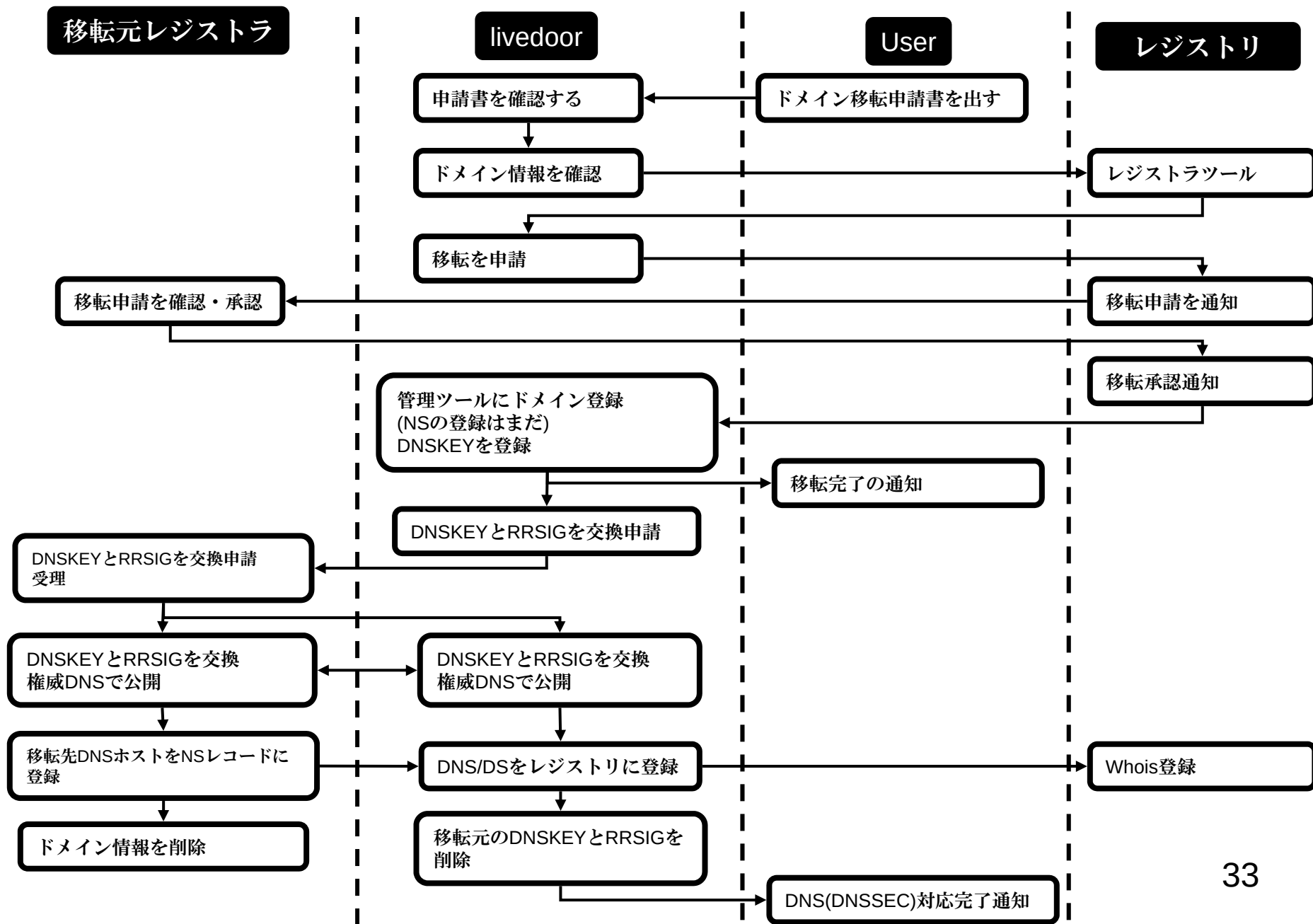
Transfer IN

1. ドメインを移転 NSも変更(移転先のNSを使う)
2. ドメインを移転 NSは自前で持っている
3. NSを元レジストラのままドメインを移転
4. 移転元レジストラが非協力的な場合(DNSKEYとRRSIGの交換に応じてくれない等)

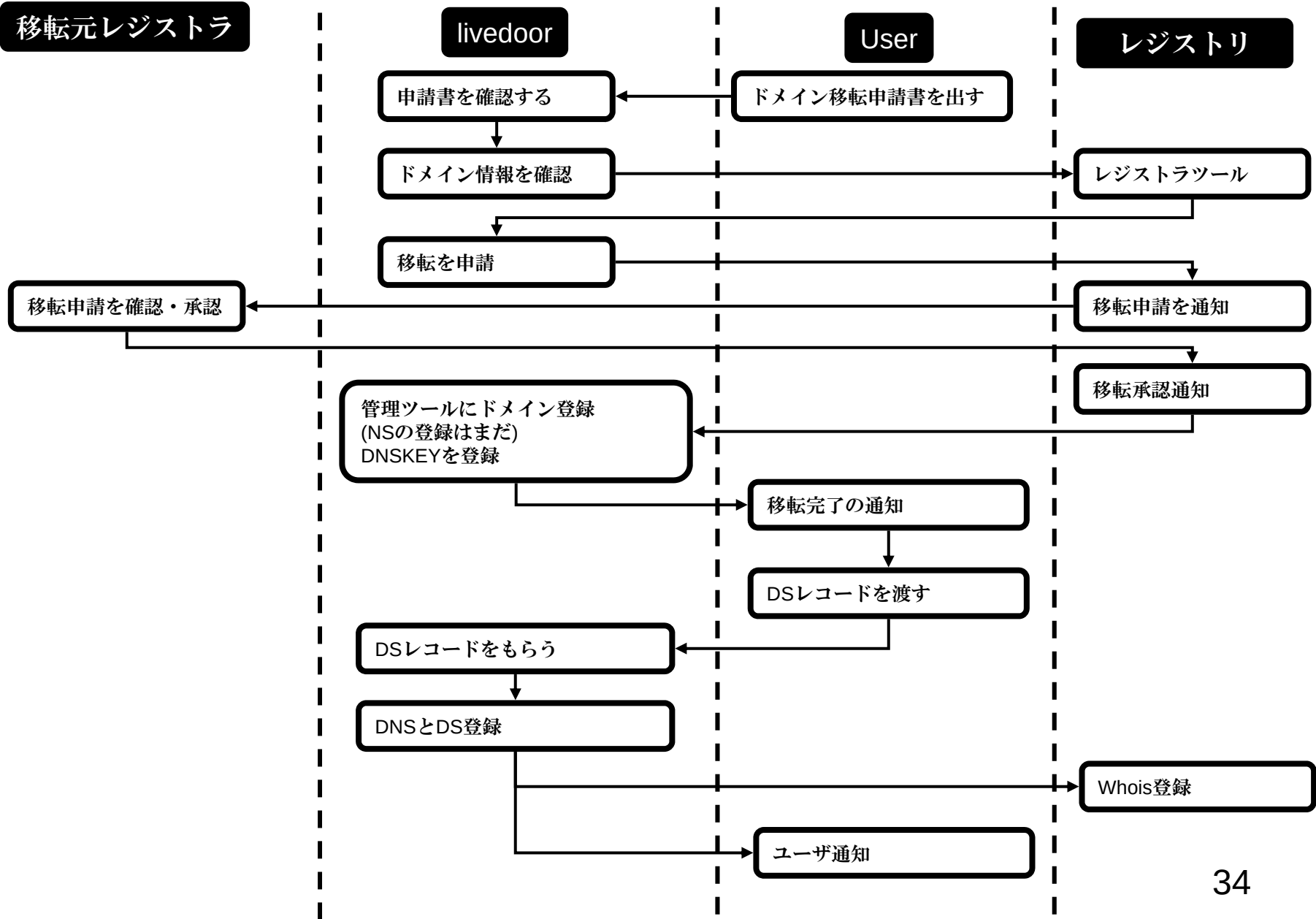
Transfer OUT

1. ドメインを移転 NSも変更
2. ドメインを移転 NSは自前で持っている
3. ドメインを移転するもNSだけ残していく
4. DNSKEYとRRSIGの交換に非協力的(レジストラ側)

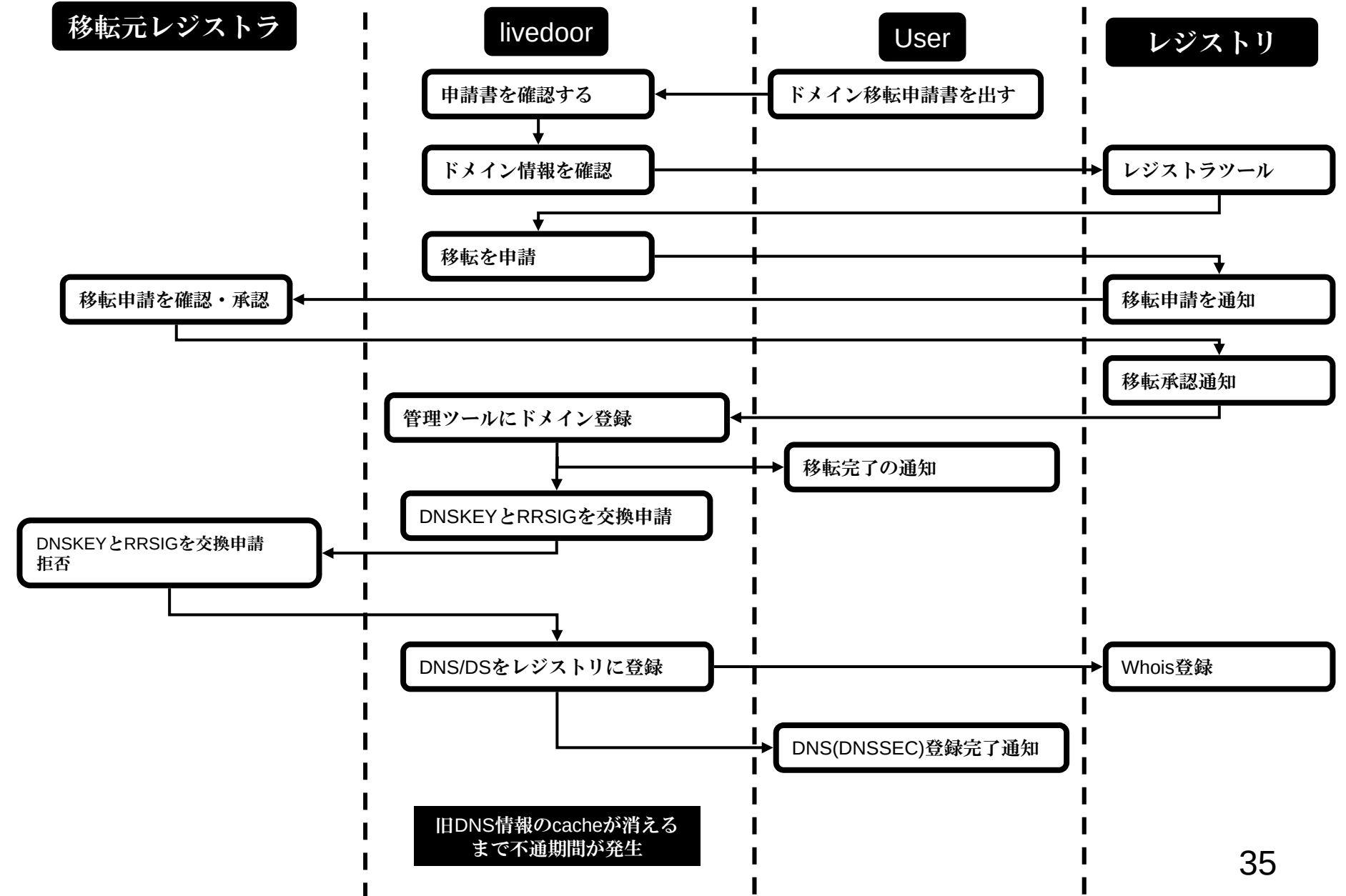
相手が協力的だった場合通常のパターン1 (例: JPドメイン) transfer IN



相手が協力的だった場合・NSを自前でもつ場合 パターン2&3(例:JPドメイン)

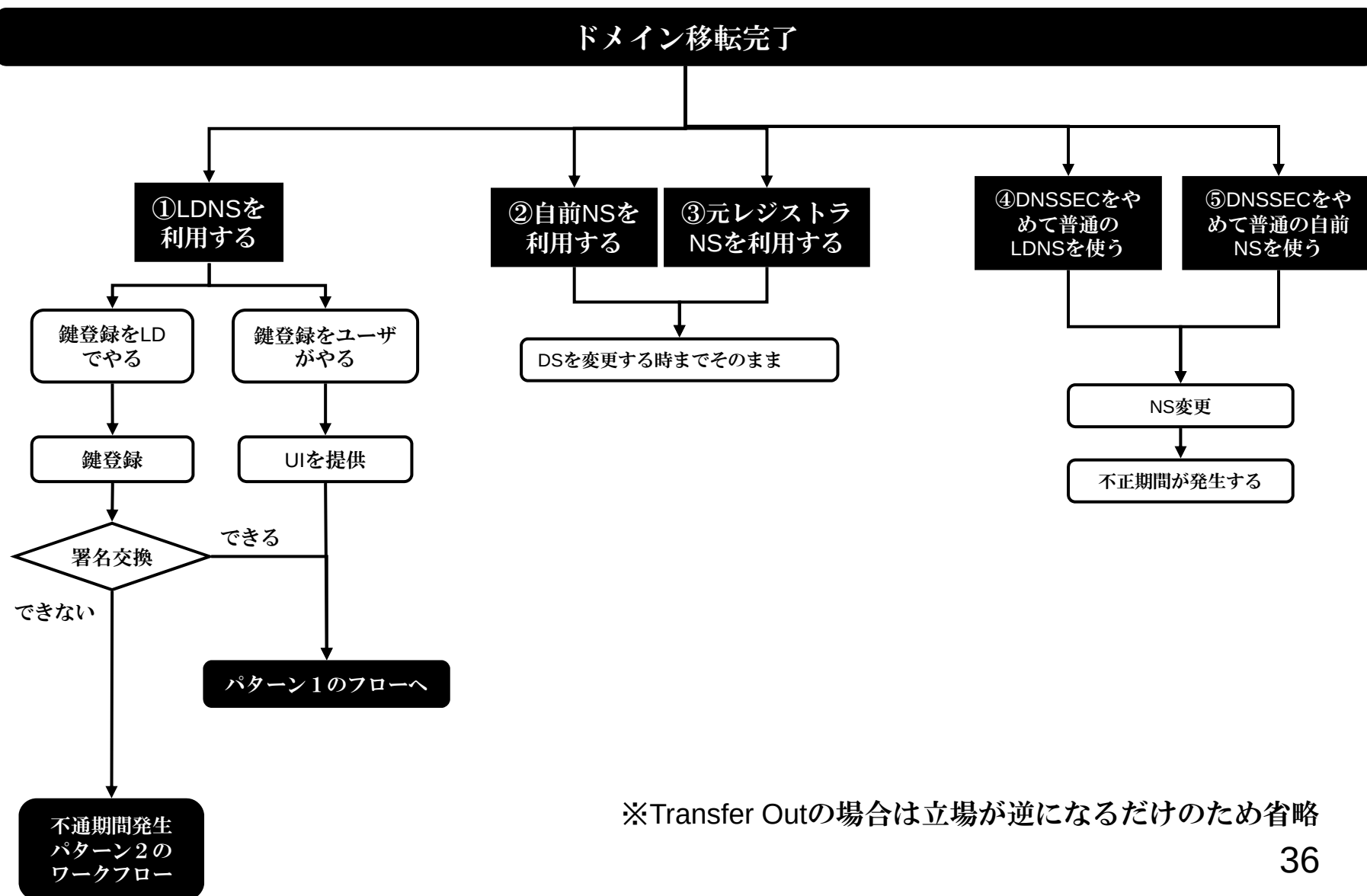


相手が非協力的だった場合パターン4(例:JPドメイン)



Transfer IN後の考えられるパターン

※パターン別のフローでわかるように、DNSSEC対応はドメイン自体が移転してから。
※ドメイン移転後考えられるパターン



考えられるCheck Point

※それぞれの選択や手段はサービスレベルや運用ポリシーなどに基づくことになる

Transfer IN

- ドメイン移転時のゾーン情報(有効期限など)の確認
- 鍵登録を誰がやるのか？
(レジストラ間ですることができるのか、ユーザがやるのか、できないのか、またはその手段)
- パターンによって不通期間が発生することを予め説明する(不正期間が発生すること約款等に盛り込むなど)

Transfer OUT

- 移転して出て行った後どの程度ドメイン情報を保持するのか
(移転後猶予期間を設けて削除する、または持たないなど)
- 移転後ドメイン情報を削除したあと、不通期間が生じる場合(猶予期間終了後は削除しますなど)、またはその可能性についての免責について約款に入れる
- 鍵交換に応じるのか(応じる場合こういった手段をとるのか)

⑥ 導入における懸念点整理 (6-2) NGN対応検討

- NTT NGNのISP IPv4/IPv6 接続環境
– 2011/4に開始が予定されている

- DNSSEC導入後に
いかを検討

現在のところ進捗なし。

- も
決
証V
- 8月から情報が出てくるのでその後検討予定
- DNSSEC.jp技術検
ひ関係者間で共有。

まとめとご案内



まとめ

- DNSSEC技術検証WGの紹介
- // 各活動のご案内
- 困ったことは現在進行形で議論
- 今後は広報WGと連携し，積極的な資料公開も検討していきます

技術検証WG ご参加のご案内

- 技術検証WGでは、~~一緒に悩む同志~~ メンバを募集しています
 - 導入にあたり検討したいことがある方
 - これからの実験検証で共にやりたいこと、やってほしいこと、がある方
- ご興味のある方はDNSSECジャパン事務局までご連絡をお願いいたします
 - 下部組織である技術検証WGのみへの単独加入は出来ません

技術検証環境について

- 技術検証WGはDNSSECに関連する技術検証の環境をJPRSと連携して準備します.
- 環境提供の目的
 - DNSSEC導入の際に想定される技術的な課題を検証し, 実環境への導入をスムーズにすること
- 環境提供期間
 - 2010年8月～2011年3月
- 環境条件
 - 環境へのアクセスは利用者に限定

利用条件など

- 利用条件

- ① 技術検証WGの活動に参加すること

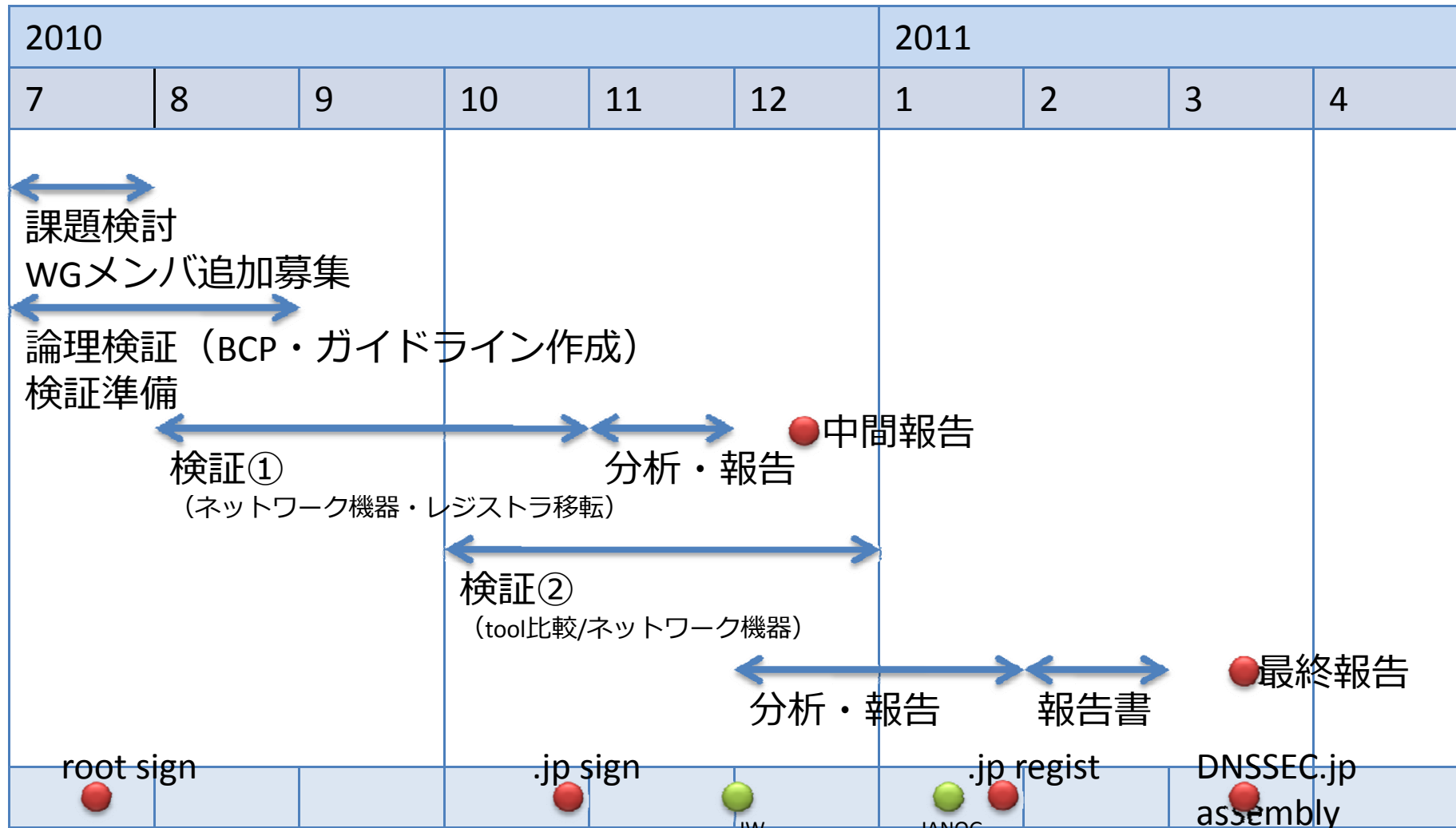
- 既存の検証項目（サブチーム）に参加するか、適切なサブチームがない場合は自らサブチームを作って参加.
 - 活動成果は原則的に参加者，または可能な範囲内でDNSSECジャパンとして公開予定.

- 付帯条件

- ① JPRSの実験環境を利用する場合

- JPRSが提供する実験環境を利用する場合は，JPRSが別途用意する実験参加申込書を提出して頂きます.

今後のスケジュール（予定）



以上

