DNSSEC導入に当たって

平成22年11月

DNSSECジャパン

はじめに

本資料はDNSSECの導入検討している事業者の方々に対して、導入までに検討しておくべき項目を挙げたものです。

本資料は一例にすぎませんが、これを参考として
DNSSEC導入を検討していただければと思います。

アジェンダ

はじめに

1. DNSSECについて知る
2. DNSに関連するサービス・影響範囲を洗い出す
3. DNSSEC導入までのTODO
    1. 技術検証
    2. 設備検証
    3. 運用体制構築
4. コストの算出
    1. 導入前のコスト
    2. 導入のためのコスト
    3. 導入後の運用コスト
5. リスクの算出
6. 総合評価により導入サービスを決定する

おわりに

１．DNSSECについて知る

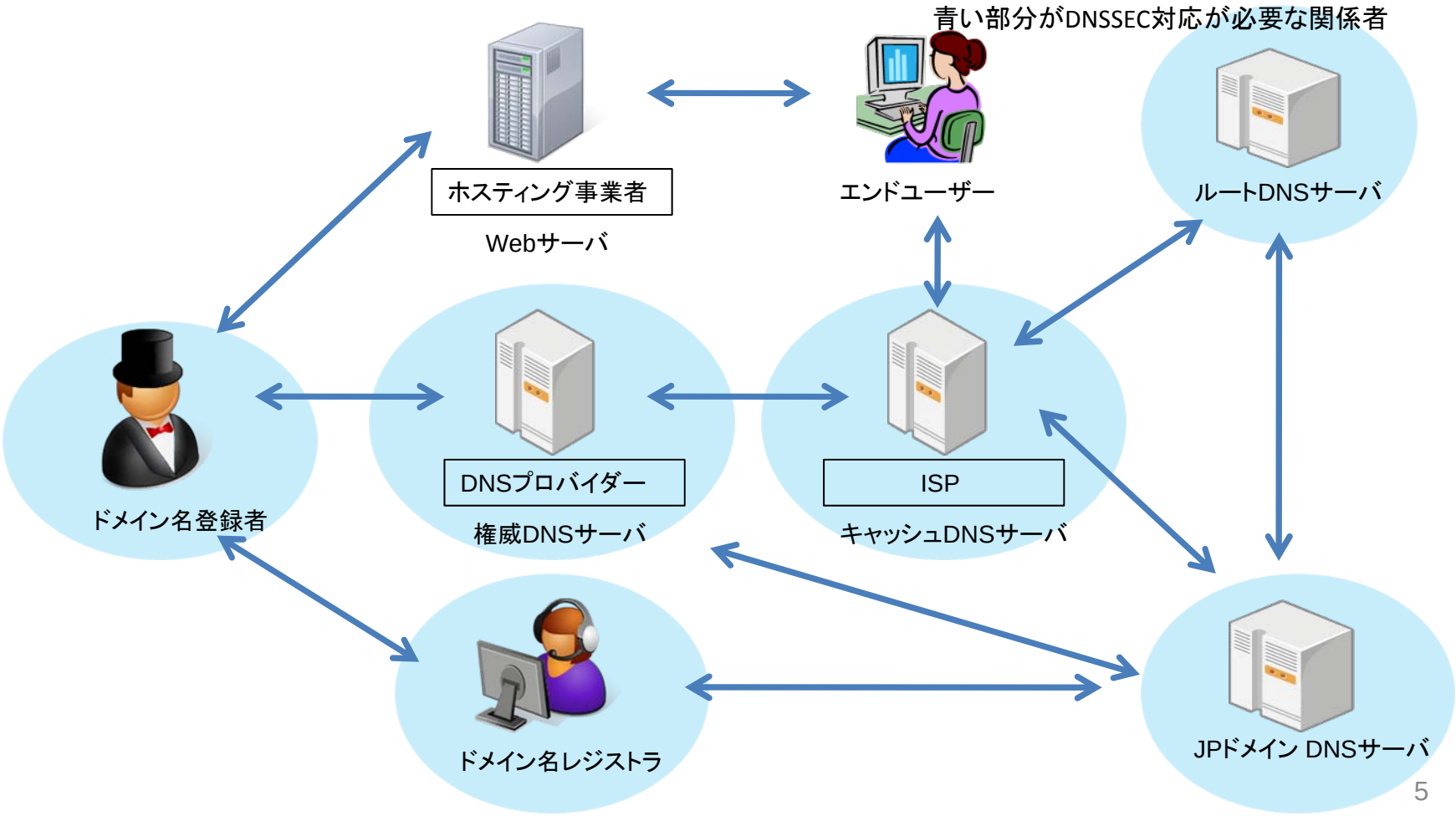
- DNSSECはDNSのキャッシュポイズニング攻撃に対応するために、導入が進められている技術です。

- 世界中で対応が始まっており、2010年7月にはルートゾーンが対応。
  日本でも.jpが2011年1月にサービス開始予定。

- 詳細については、別紙「DNSSECについて」を参照

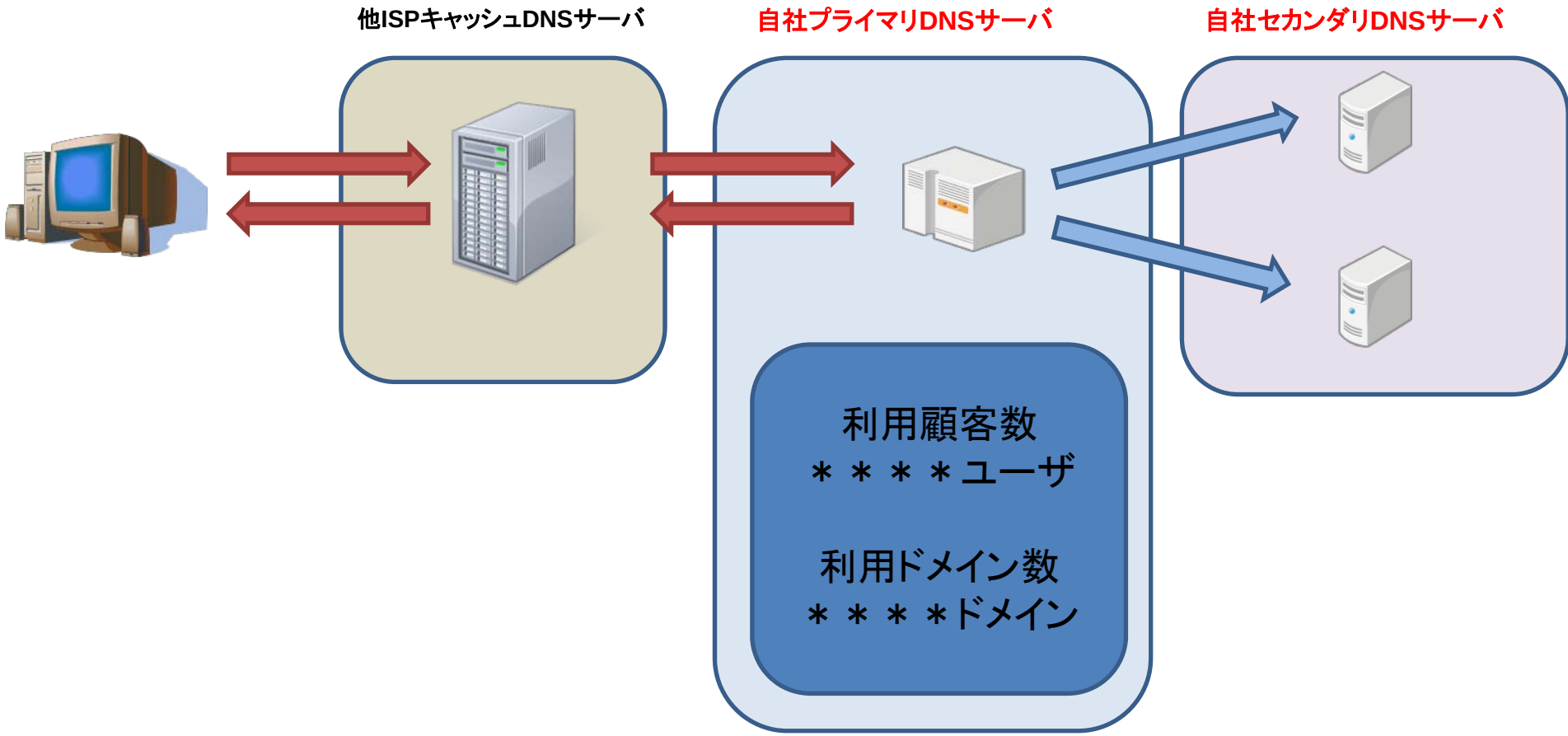
2. DNSに関連するサービス・影響範囲を洗い出す

- DNSSECに関連する関係者は多岐にわたります。
- 自社がどこに当てはまり、どのサービスをしているのかを洗い出す。
- 自社のサービスがどの程度のものなのか、影響範囲を割り出す。



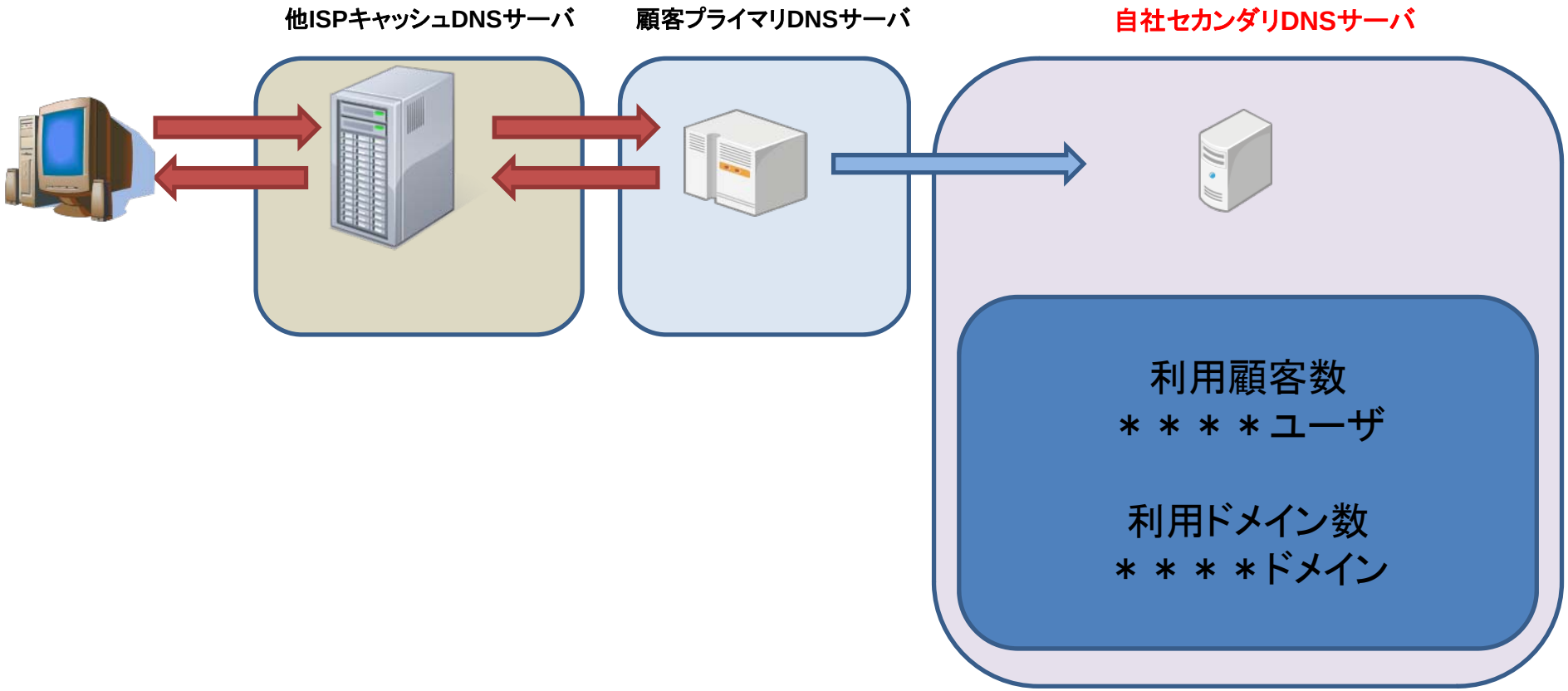
プライマリDNSサービス

- プライマリDNSサービス
  - 顧客に対して、プライマリDNSを提供



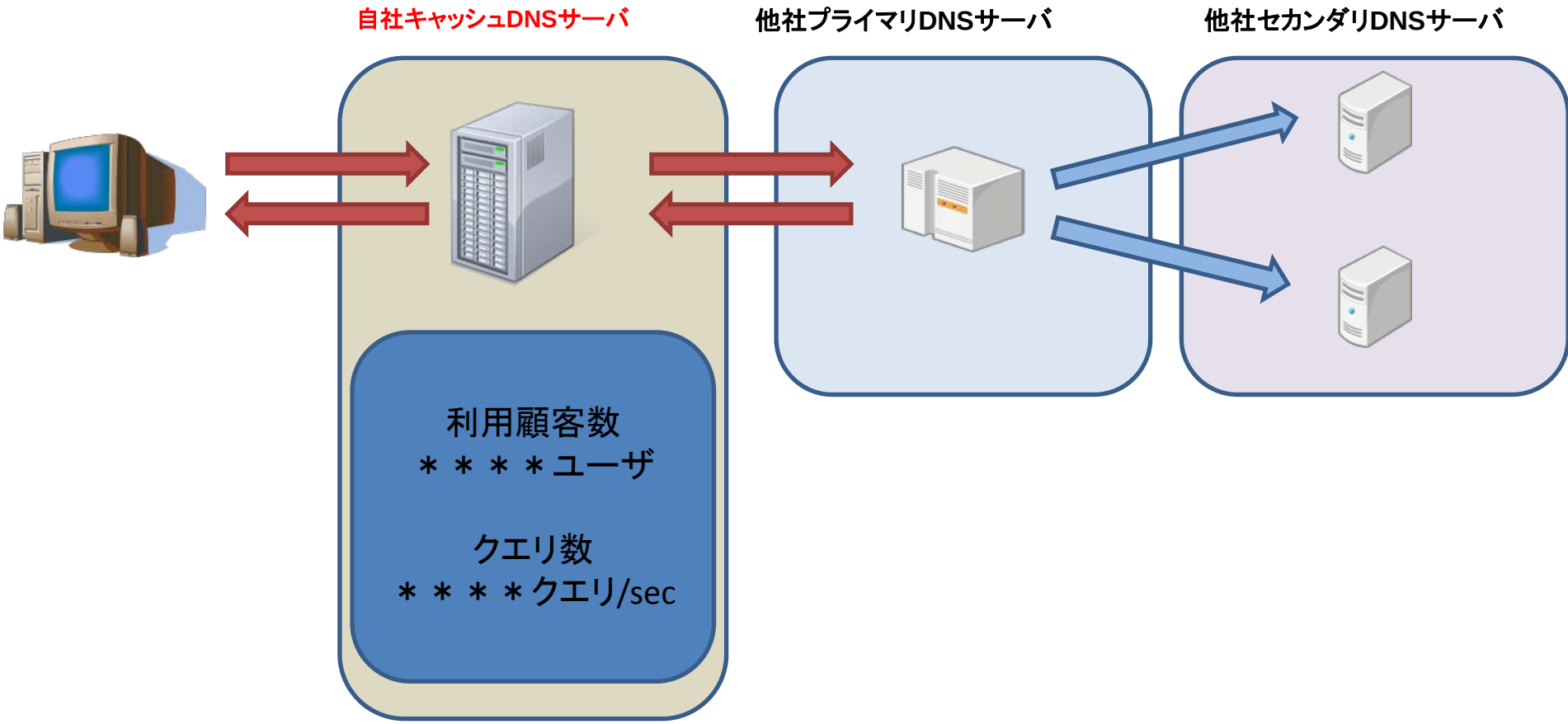
セカンダリDNSサービス

- セカンダリDNSサービス
  - 顧客に対して、セカンダリDNSを提供



キャッシュDNSサービス

- キャッシュDNSサービス
  - 顧客に対して、キャッシュDNSを提供



ドメイン維持管理サービス

- ドメイン維持管理サービス
  - お客様のドメインを維持管理する
  - JPRSへの変更、登録などの取次ぎ
  - レジストラ移転などの対応

管理ドメイン数
＊＊＊＊ドメイン

新規登録顧客数
＊＊＊＊ユーザ/月

ドメイン移行ユーザ
＊＊＊＊ユーザ/月
etc.etc

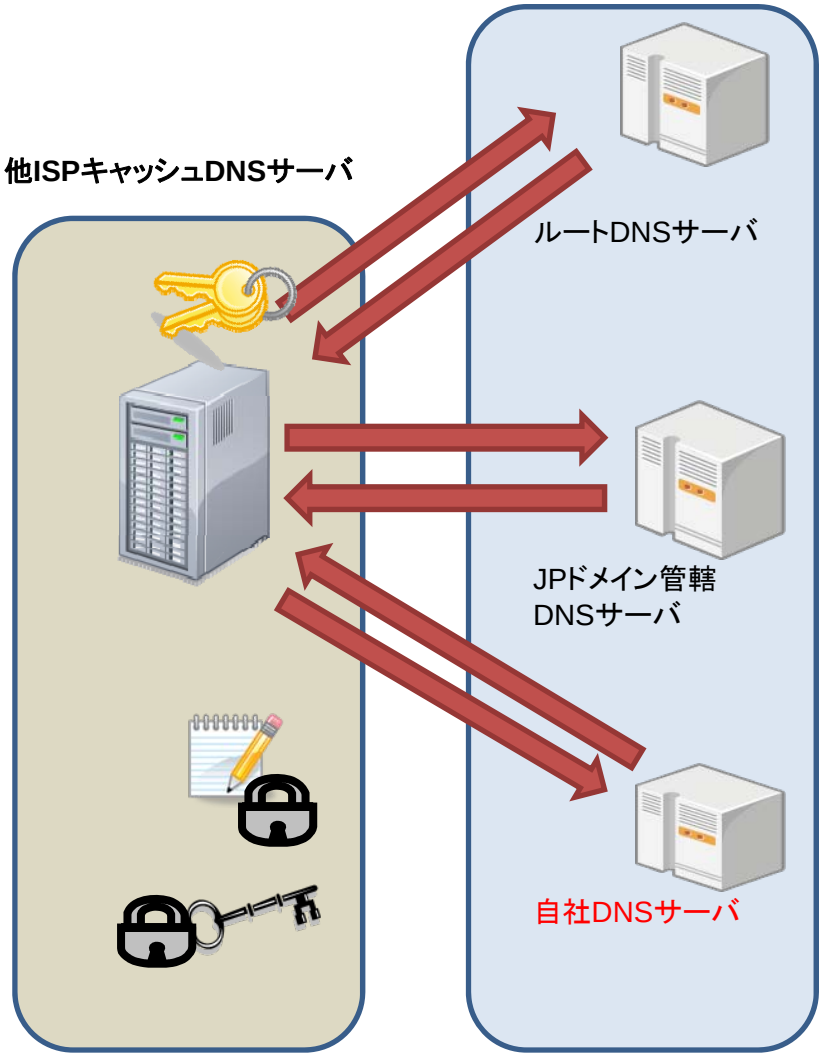
自社の業務利用ドメイン

- 自社のDNS
  - 社内システムとしてのDNS
    - 自社ドメインのプライマリやセカンダリ
    - 社内サーバやPCのためのキャッシュ
    - 自社ドメインの維持管理

３．DNSSEC導入までのTODO

- それぞれのサービスに対して、DNSSECを導入するに当たり、必要な対応を検討する

プライマリDNSのDNSSEC対応



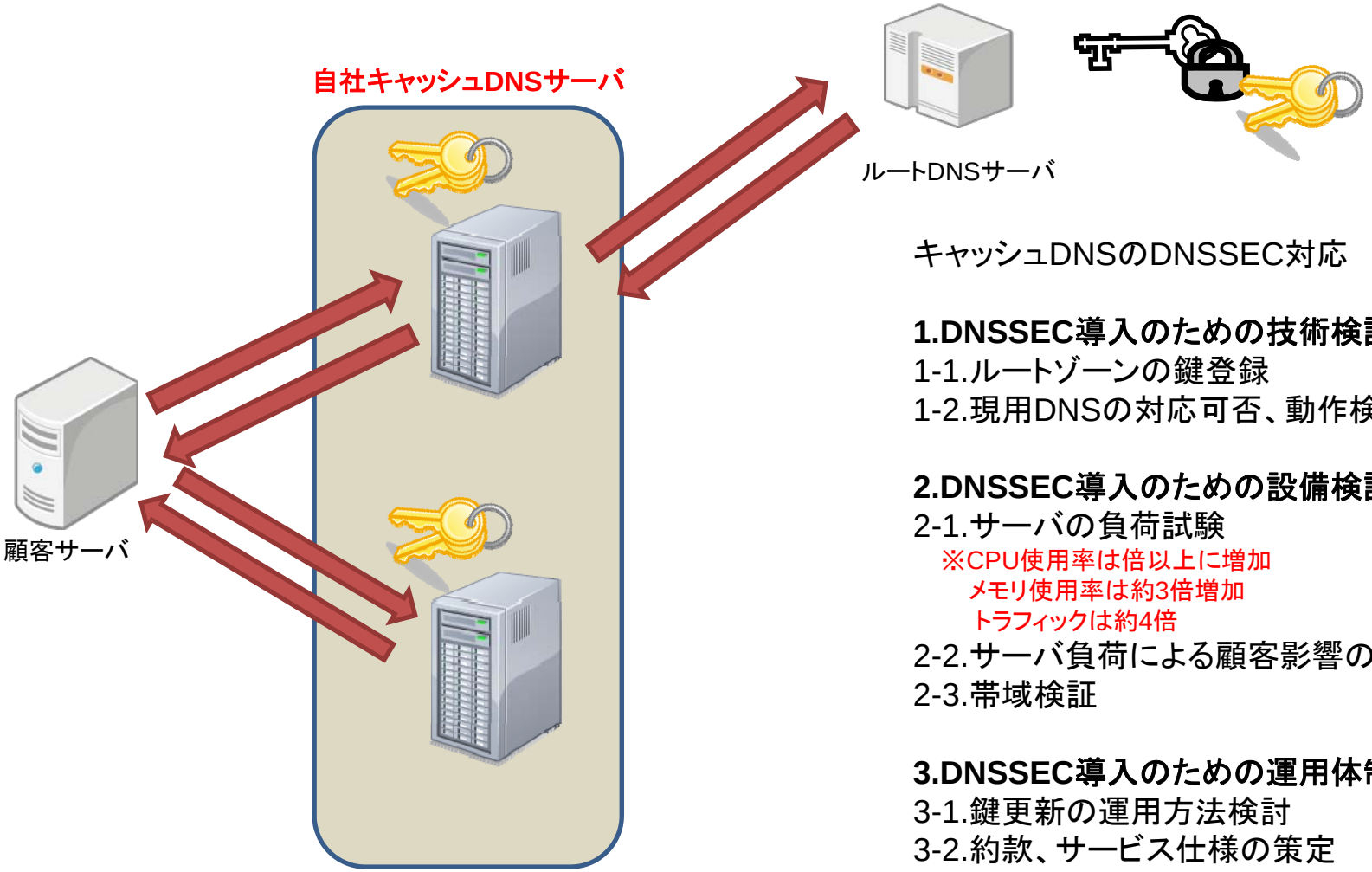
プライマリDNSのDNSSEC対応

1.DNSSEC導入のための技術検証
1-1.署名に使用するツール検証
1-2.鍵作成から署名までの検証
（鍵作成・署名とDNSサーバ分離など)
1-3.鍵更新の検証
1-4.顧客用のI/F開発・検証
1-5.他NW機器やFWのDNSSEC対応検証
（UDPフラグメント、EDNS0など）
1-6.DB利用の場合は、登録項目の検証

2.DNSSEC導入のための設備検証
2-1.サーバの負荷試験（処理速度・帯域）
※存在応答で10-20%処理能力低下
不在応答で50%以上処理能力低下

3.DNSSEC導入のための運用体制構築
3-1.鍵や署名の管理方法検討
3-2.鍵長や署名の有効期限などのポリシー策定
3-3.約款、サービス仕様の策定
3-4.運用のための手順やフローの作成

キャッシュDNSのDNSSEC対応



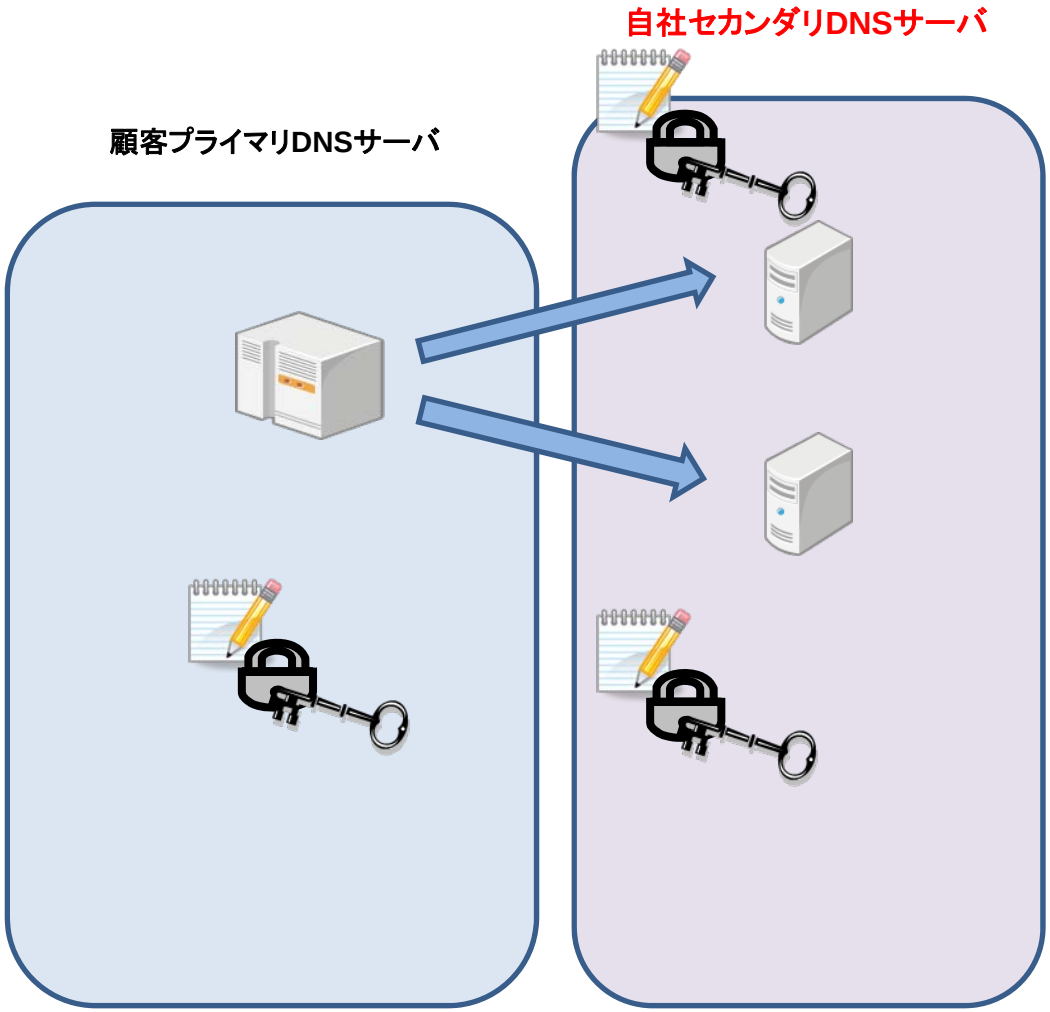
キャッシュDNSのDNSSEC対応

1.DNSSEC導入のための技術検証
1-1.ルートゾーンの鍵登録
1-2.現用DNSの対応可否、動作検証

2.DNSSEC導入のための設備検証
2-1.サーバの負荷試験
※CPU使用率は倍以上に増加
メモリ使用率は約3倍増加
トラフィックは約4倍
2-2.サーバ負荷による顧客影響の検証
2-3.帯域検証

3.DNSSEC導入のための運用体制構築
3-1.鍵更新の運用方法検討
3-2.約款、サービス仕様の策定
3-3.運用のための手順やフローの作成

セカンダリDNSのDNSSEC対応



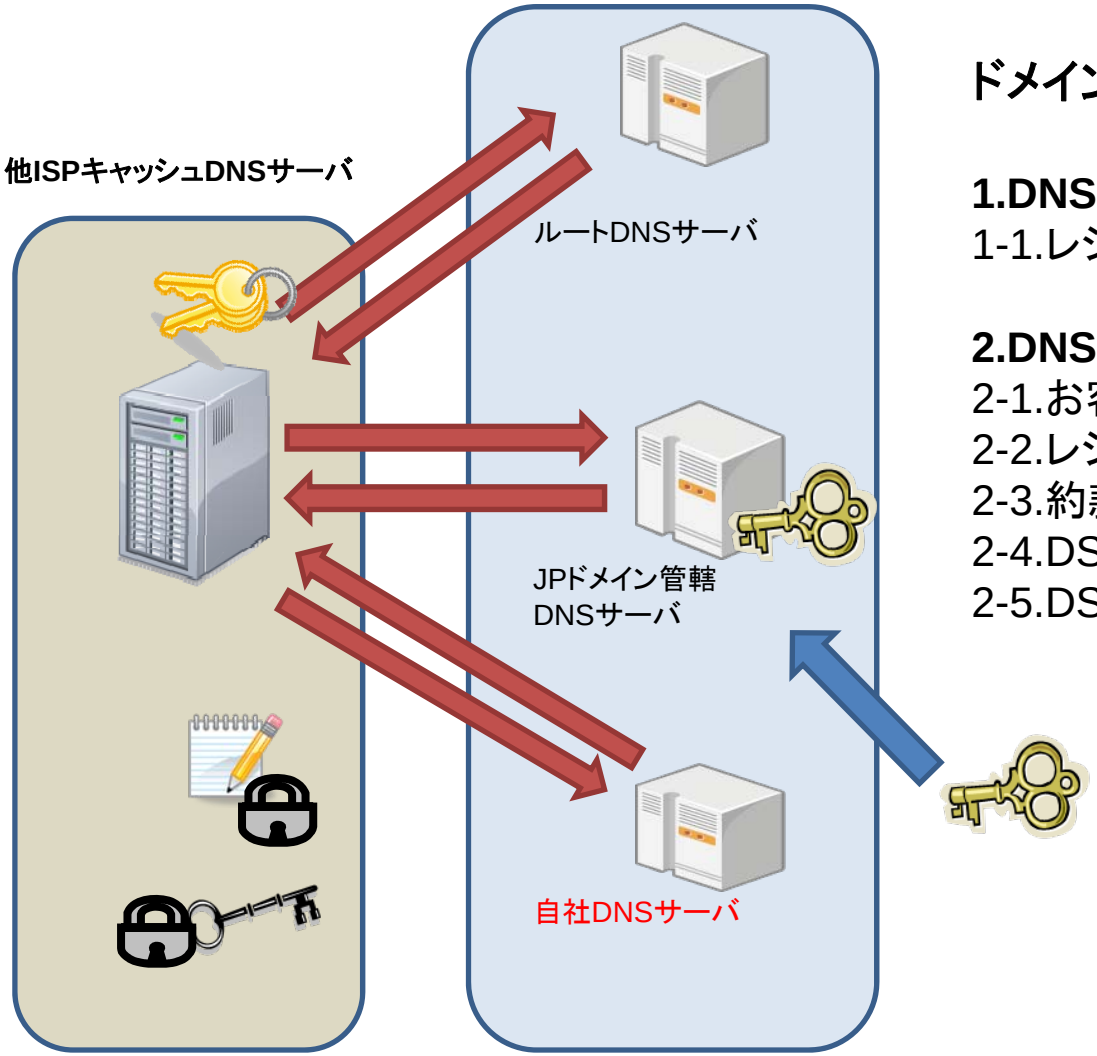
セカンダリDNSのDNSSEC対応

1.DNSSEC導入のための技術検証
1-1.ゾーン転送の正常性試験

2.DNSSEC導入のための設備検証
2-1.サーバの負荷試験

3.DNSSEC導入のための運用体制構築
3-1.約款、サービス仕様の策定
3-2.運用のための手順やフローの作成

ドメイン維持管理のDNSSEC対応



ドメイン維持管理のDNSSEC対応

1.DNSSEC導入のための技術検証
1-1.レジストリ/レジストラに対しての鍵登録検証

2.DNSSEC導入のための運用体制構築
2-1.お客様対応について
2-2.レジストラ移転時の運用方法確立
2-3.約款、サービス仕様の策定
2-4.DS情報のやりとりの手順、フローの作成
2-5.DS情報の保存や管理方法の確立

4. コストの算出

- DNSSEC導入前の運用コスト
  - 維持費、稼動費、etc
- DNSSEC導入のためのイニシャルコスト
  - 開発費、設備投資費、稼動費、etc
- DNSSEC導入後の運用コスト（主に下記のような稼動費）
  - 2週間に一度程度、署名の有効期限を切らさないよう、再署名
    - 全てのドメインに対して定期的かつ大規模な署名更新
    - 全ドメインの署名の有効期限が同じとは限らない
    - 全ドメインの有効期限管理と再署名が重要
  - 1カ月に一度程度、DNSデータ用(ZSK)の鍵を更新
    - 古い鍵との併用期間は必要
      - 古い鍵を削除して新しい鍵のみで署名すると、古い鍵を記憶しているキャッシュサーバがいた場合検証できなくなります
    - 新旧の鍵で全てのドメインに対して再署名
    - 古い鍵の削除
  - 1年に一度程度、鍵用の鍵(KSK)を更新
    - 古い鍵との併用期間は必要
    - 新しい鍵で、DNSデータ用の鍵(ZSK)を署名
    - 上位DNSへ鍵を登録
  - 顧客の要望への対応
    - 新しい鍵を作成直後に変更してほしい、すぐに鍵を更新してほしいetc.etc
  - ドメイン事業者移転希望顧客への対応
  - 1年に一度程度、キャッシュサーバに登録しているルートゾーンの鍵を更新する

5. リスクの算出

- 前述の導入後運用が一つでも失敗した場合・・・
  - プライマリサーバ利用顧客:『ゾーン全体』の名前解決が不能になる
    ⇒インターネットから消滅する
  - キャッシュサーバ利用顧客:DNSSECを利用した名前解決が不能になる
    ⇒目的のサーバにアクセスできなくなる
- DNSSECを導入しなかった場合・・・
  - キャッシュポイズニングにより、お客様に被害がでる可能性がある
  - DNSSECが広まった後でこの被害が出た場合、自社の信用に影響する
- DNSSECを導入した場合、導入しなかった場合のリスクを算出する

６．総合評価により導入サービスを決定する

- 導入するメリット
  - キャッシュポイズニングによる攻撃の阻止
  - セキュリティを担保しているという信頼
  - 新しいものに常に挑戦する先進性
  - 堅牢なセキュリティを望む顧客の受注機会創出・・・など

- 導入するデメリット
  - 導入までのハードル
  - コストの増大
  - 運用稼動の増大
  - オペレーションミスによる障害・・・など

- 今まで検討してきた項目を総合的に評価し、導入するか否かを判断する

おわりに

以上が、DNSSEC導入に当たって必要な検討事項の概略になります。

このほかにも、事業者によっては検討事項の増減があるかと思いますが、基本的な流れは同じだと考えています。

もし、導入に当たっての詳細な情報が必要な方は、DNSSECジャパンの公式サイトを参照してください。

DNSSECジャパン
http://dnssec.jp/