Infoblox

DNSサーバメンテナンスあれやこれや

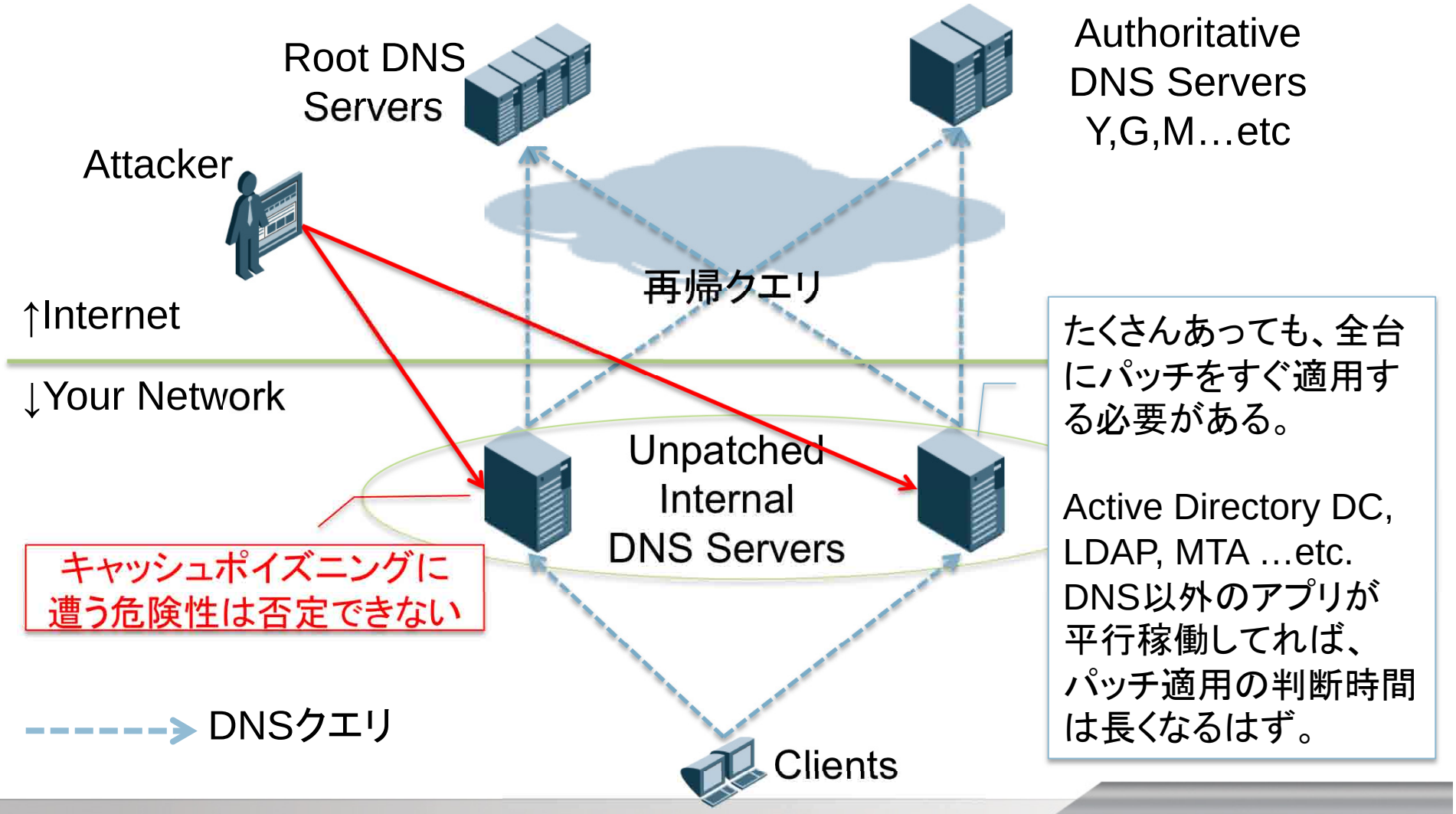
Infoblox K.K.
K. Fujikawa

前口上 ～Agendaに代えて～

Infoblox

- **DKAでインターネット終了？**
  - まだだ、まだ終わらんよ
    - 終わられたら(いろんな意味で)困る。
- **結局、どうすりゃいいのだ？何かできることはないのか？**
  - 安全なDNSサーバやら、IDS/IPSとかDNSに関するアプリケーションFirewallを見つけてくる
    - 予算の問題があったり、製品そのものを探すのが面倒だったり
  - DNS応答の複数回チェックとか、DNSSECとか、実装を見直す
    - 時間がかかりそう…その時間さえ惜しい。
  - ひたすらパッチを適用する
    - 今回のお話は、これを中心に。
- **ポイント**
  - パッチ適用作業をいかにシンプルにするか
  - パッチ適用作業中のサービス停止をいかに短くするか

Before (or Now)



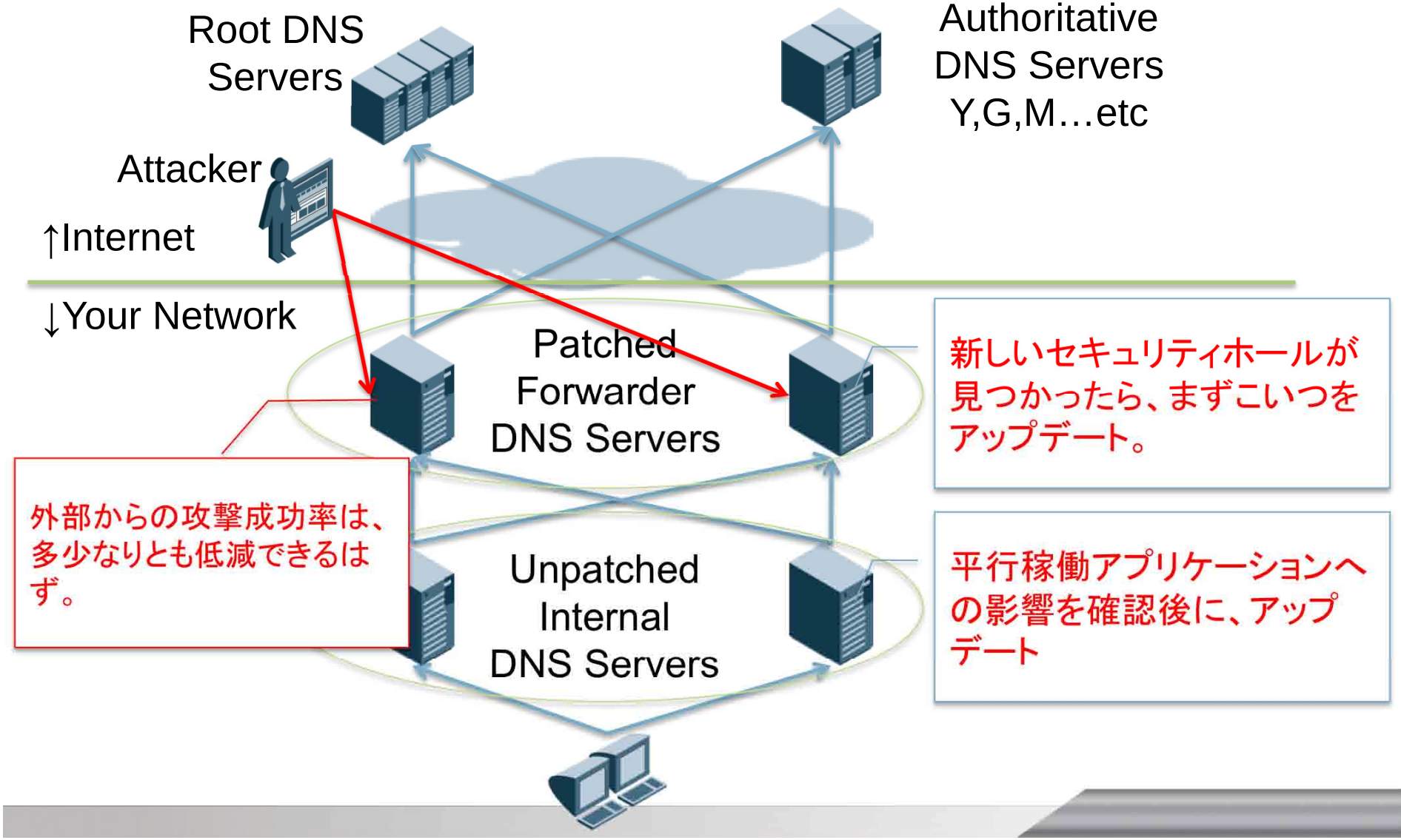
パッチ適用のタイミングを遅らせるもの

Infoblox

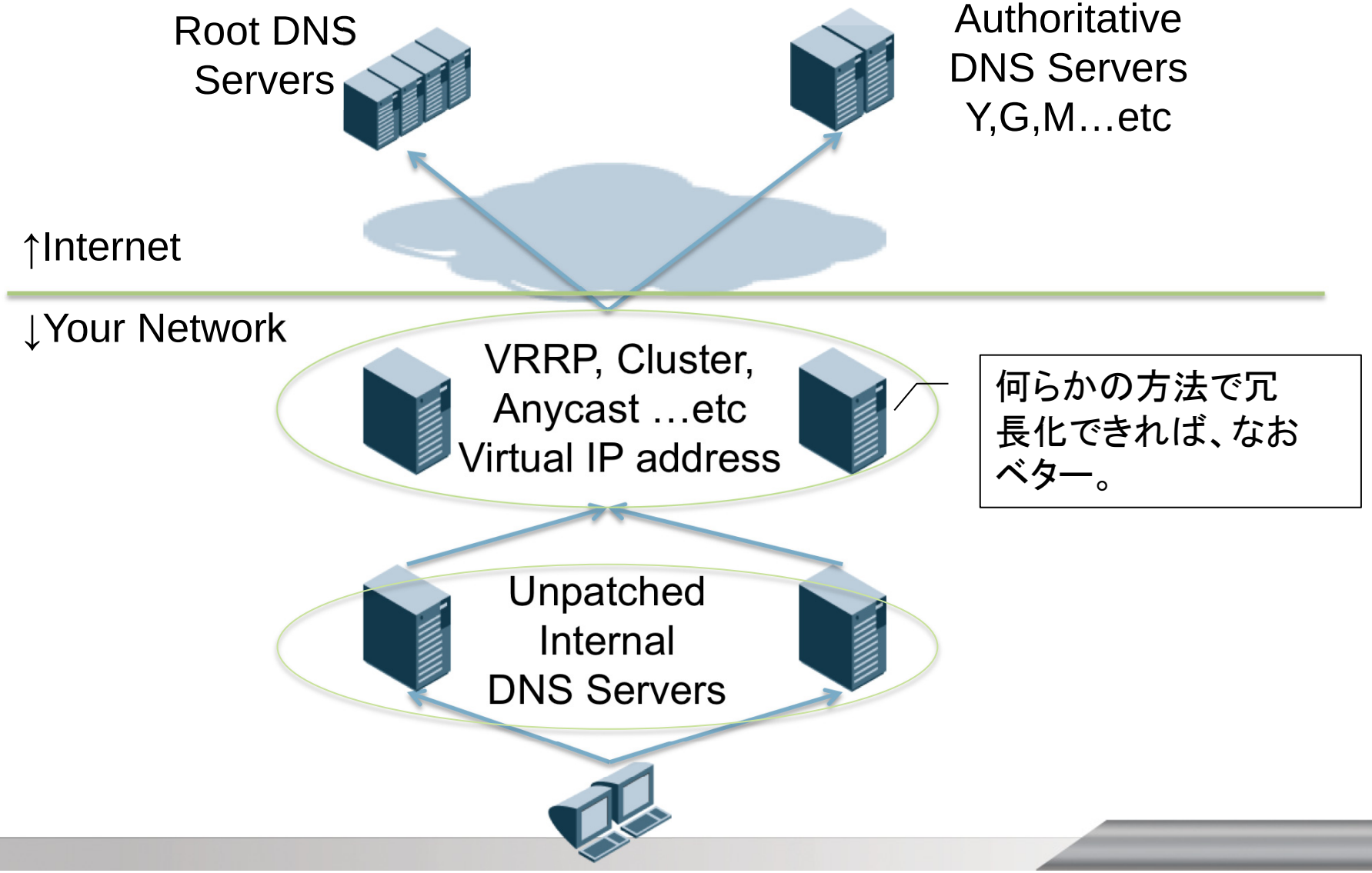
- **パッチ適用すべきかどうかの判断時間**
  - 自分の環境で対応が必要なのか？
  - 必要だとしたら、どのタイミングでやる？
- **他のアプリケーションへの影響調査/ドキュメントの確認時間**
  - 人的な二次被害を防ぐためには、必要な時間
- **パッチ適用環境の動作確認に必要な時間**
  - パフォーマンスに影響はない？とか

- **トータルで、3日～2週間!?**
  - もう少し、できればもっと、短くしたい。

After


Root DNS Servers
Authoritative DNS Servers Y,G,M…etc
Attacker
↑Internet
↓Your Network
Patched Forwarder DNS Servers
Unpatched Internal DNS Servers
外部からの攻撃成功率は、多少なりとも低減できるはず。
新しいセキュリティホールが見つかったら、まずこいつをアップデート。
平行稼働アプリケーションへの影響を確認後に、アップデート

After


Root DNS
Servers
Authoritative
DNS Servers
Y,G,M…etc
↑Internet
↓Your Network
VRRP, Cluster,
Anycast …etc
Virtual IP address
何らかの方法で冗
長化できれば、なお
ベター。
Unpatched
Internal
DNS Servers

要するに

Infoblox

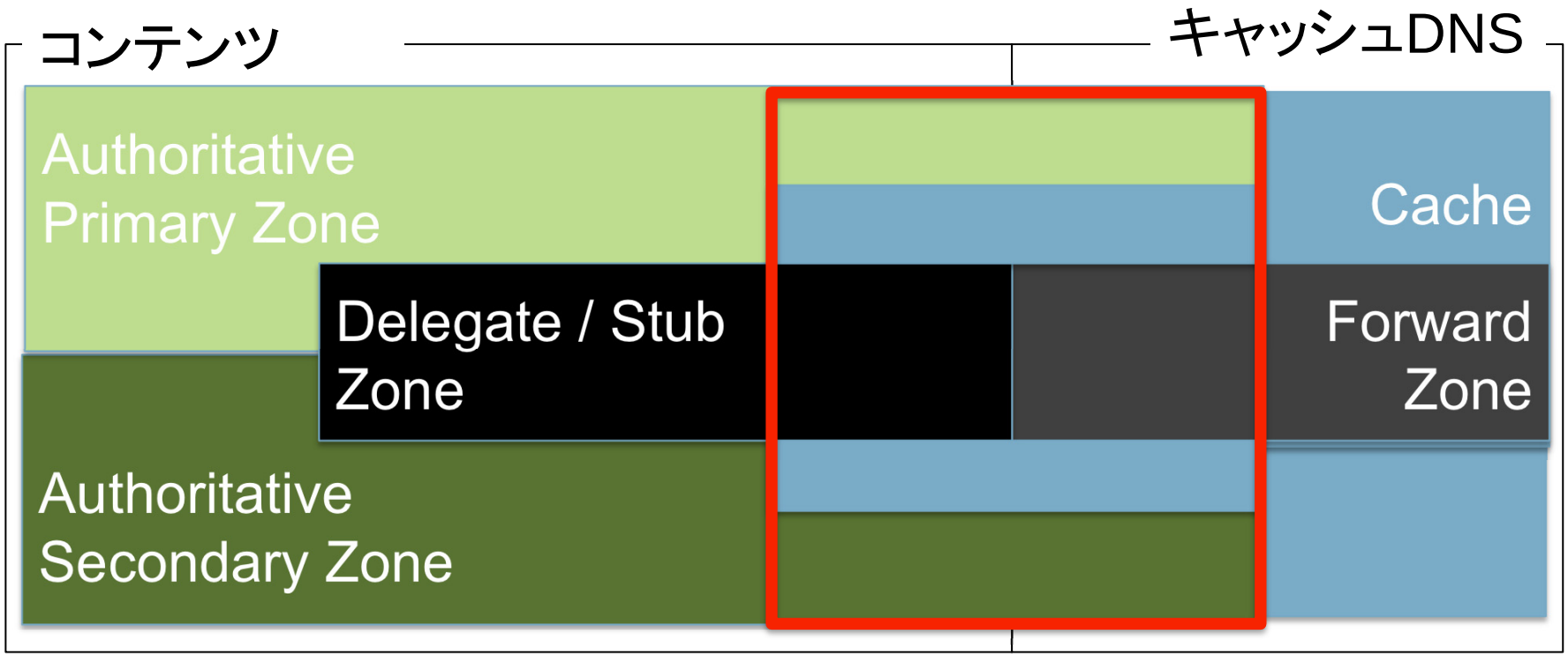
- **最新パッチを適用しやすい、DNSサービス専用のホストを用意するだけで、全然違う。**
  - 意外とDNSサービスと他のアプリケーションを併用している環境は多かったりする…
    - DHCPとか、MTAとか、ドメインコントローラとか。
    - ハードウェアが高性能かつ廉価になった弊害なのかな、と思ったり。
  - 将来的にそれなりのパフォーマンスを求められる可能性があるなら、それまでにさっさとサービス分離して用意しておきたい、という気持ちもある。
- **これを機に、コンテンツDNSサーバとキャッシュDNSサーバの分離が促進されると、みんな幸せになれそうな気がする。**
  - Viewで分離させても、オペミスでOpen Resolverになる可能性は否定できない…

Merits & DEMERITS

Infoblox

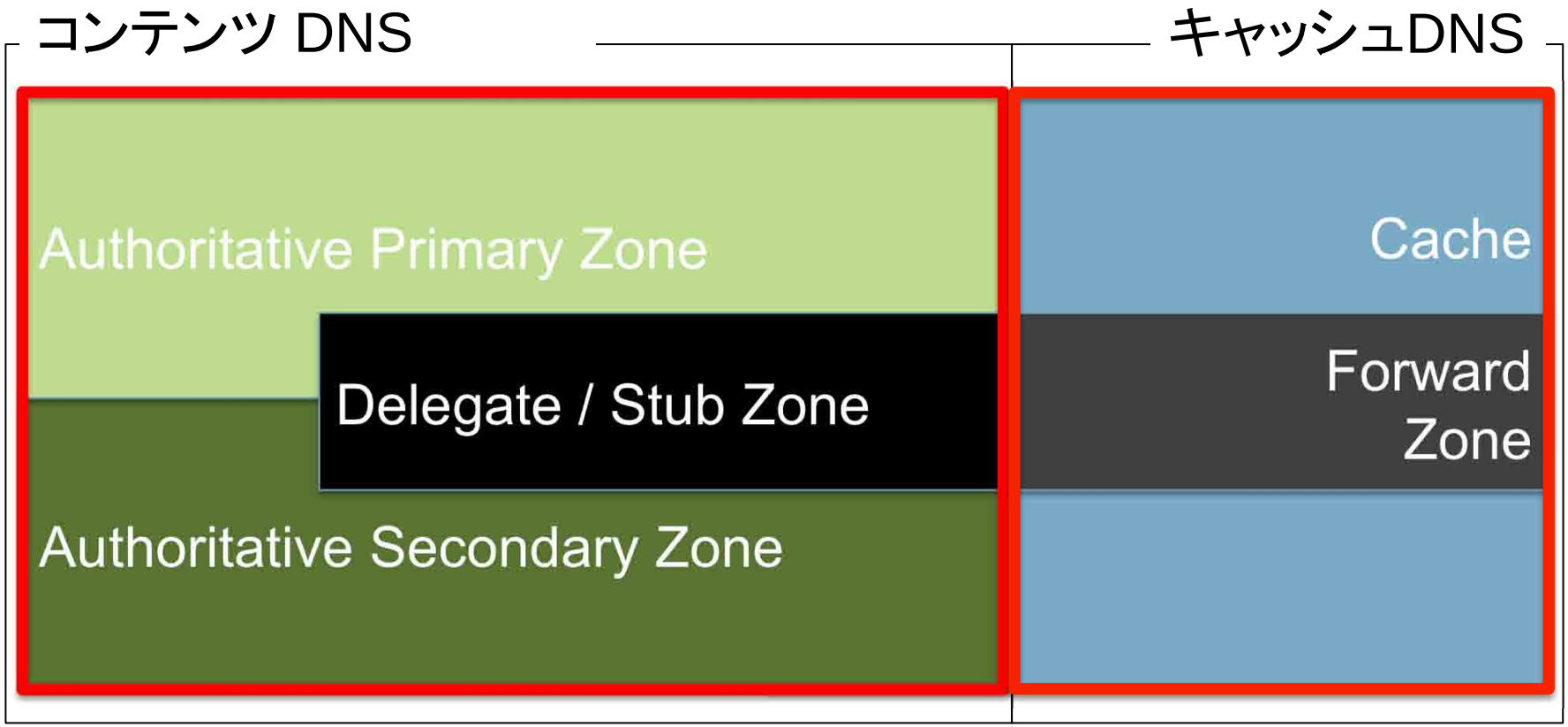
- **Merits**
  - メンテナンス性の確保
    - 内部用DNSサーバが他のアプリケーションを兼ねている環境であれば、トータルのメンテナンス性は向上するはず。
  - セキュリティ確保
    - キャッシュ専用DNSホストのサービスを常に最新に保てば、外部からの攻撃にはある程度耐えられる。
- **Demerits**
  - 内部用DNSがたくさんあると、最初のForwarders設定は大変
    - 一度変えてしまえば、後々楽になれるんですけど…
  - サーバ台数は増加する
    - ラックの温度や電源容量は大丈夫ですか？
  - クエリ処理にかかるレイテンシが大きくなる
    - キャッシュができてしまえば問題ないはず。
    - 一般的な企業環境であれば、問題にならないはず。

前提資料：DNSサーバの役割とゾーン種別



赤枠のように、1DNSサーバに異なる役割やゾーンが混在すると、メンテナンス性の悪さが目立つようになり、結果的に危険な状態になりかねない。

前提資料：DNSサーバの役割とゾーン種別



明確に機能を分けた設計になっていれば、かなりマトモなDNS環境になる。

余談ですが、Infobloxに関して。

- **アプライアンスなので、メンテナンス性は飛躍的に向上しています。**
  - 筐体二重化とか、複数デバイスの統合管理とか
- **詐称DNS応答の検知/通知/mitigate機能を実装**
  - SNMP Trap/E-mailで通知します

- **However：日本市場での特異点**
  - DHCPサーバとしての利用が圧倒的大多数
    - US/ヨーロッパでは、DNSサーバとしての利用が圧倒的
    - この逆転現象はいったい…なぜ？(´ρ`)

Infoblox

Thank you

ご質問等は、お気軽にどうぞ。