F5 Networks
DNSSECへの取り組み

－ crypto chips搭載の強み －

vol1.0

NTTアドバンステクノロジ株式会社

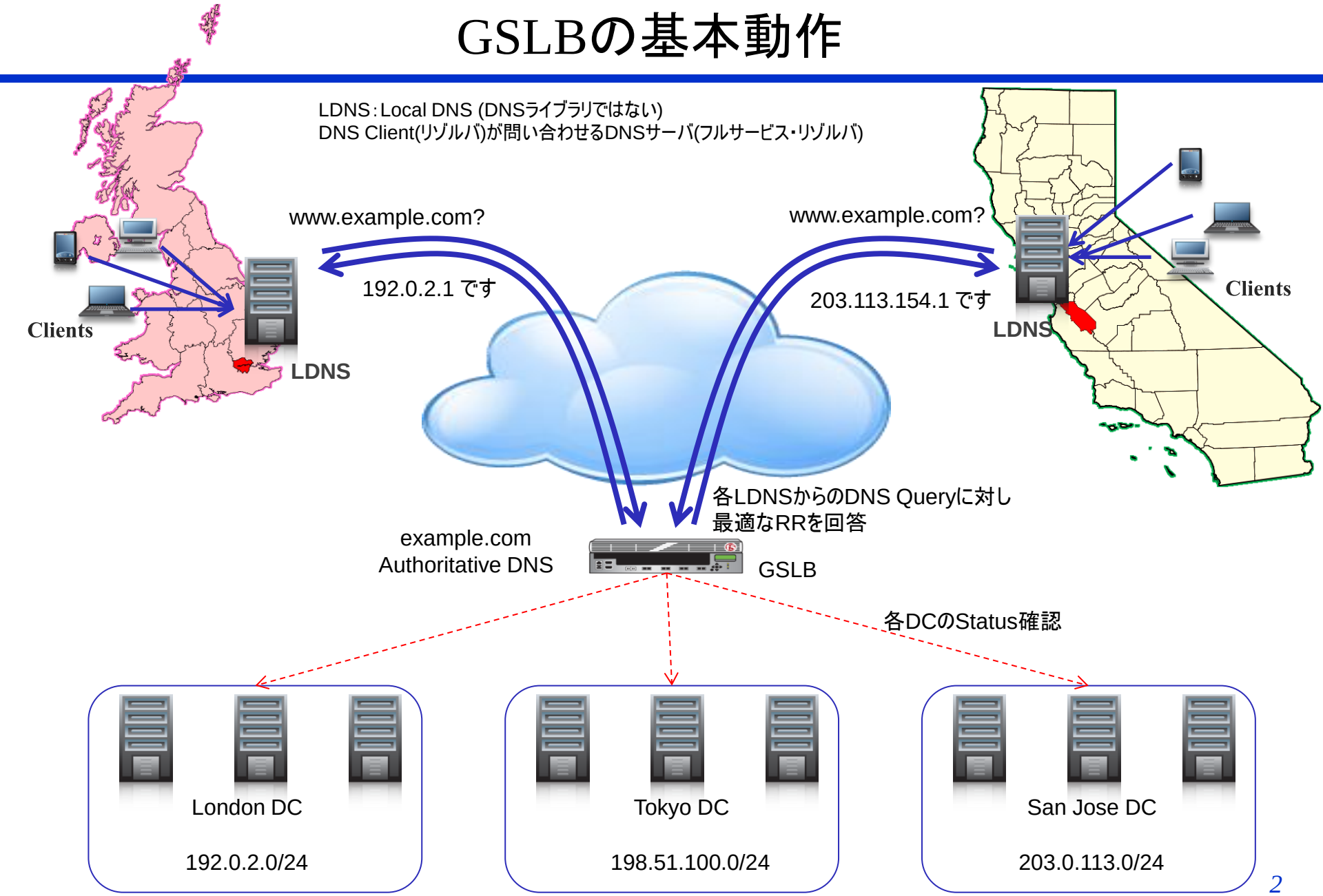
F5 NetworksってLBの会社でしょ？

- サーバロードバランサだけでなく、DNS、WAF、Firewall、SSL-VPN等のModule/製品があります

- DNSとしてトラフィックをコントロールするModule
  GTM：Global Traffic Manager
  - 一般的に GSLB (Global Server Load Balancing)と言われるModule
  - DNS Serverとして動作し、クライアントを最適なサイトに誘導
  - DRサイト構築で良く使われてます

NTT AT

GSLBの基本動作



NTT AT

It's DNSSEC Not DNSSUX

by Lori MacVittie
F5 Networks, Inc

NTT AT

DNSSUXと言わる理由

- DNSSECも例外なく、鍵、証明書、PKIを利用したセキュリティソリューションのアーキテクチャは複雑になりやすい

- 複雑さや難しさ負荷への懸念がDNSSEC導入の遅れを引き起こしている

- ベリサインは全てのTLDのDNSSEC実装に2年要すると述べている。

参考：http://www.networkworld.com/news/2009/022409-verisign-dns-security.html

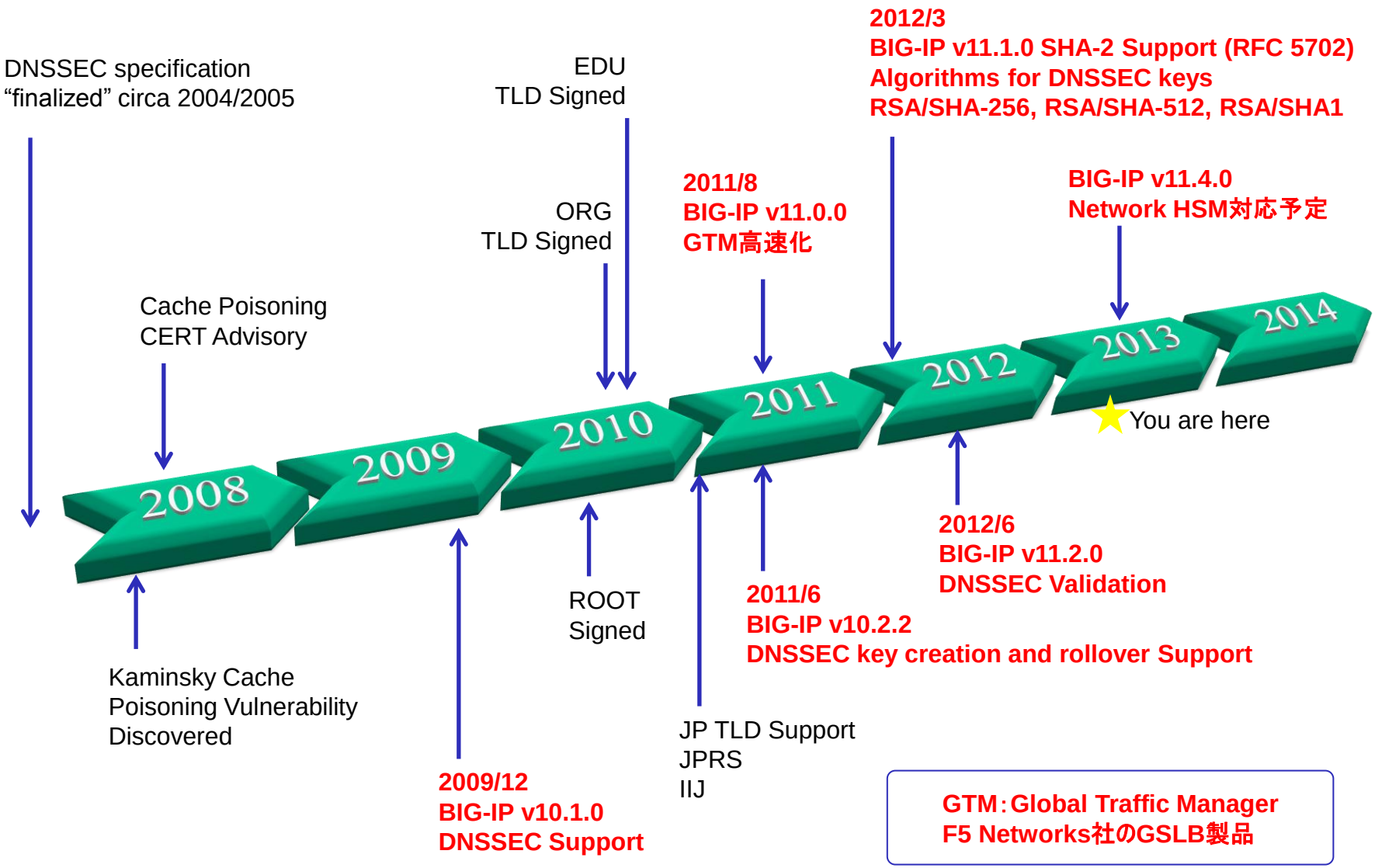
DNSSUXと言われないように

- HTTPSの処理はWEBサーバではなくSSLアクセラレータで処理させる方法が一般化している。
- HTTPS(SSL)の管理は集中する事が最良の答え
- F5 Networks社はDNSSECにHTTPSと同じロジックを適用

DNSSEC doesn’t have to be DNSSUX.

参考：https://devcentral.f5.com/blogs/us/it-rsquos-dnssec-not-dnssux

DNSSECへのアプローチ



GTM：Global Traffic Manager
F5 Networks社のGSLB製品

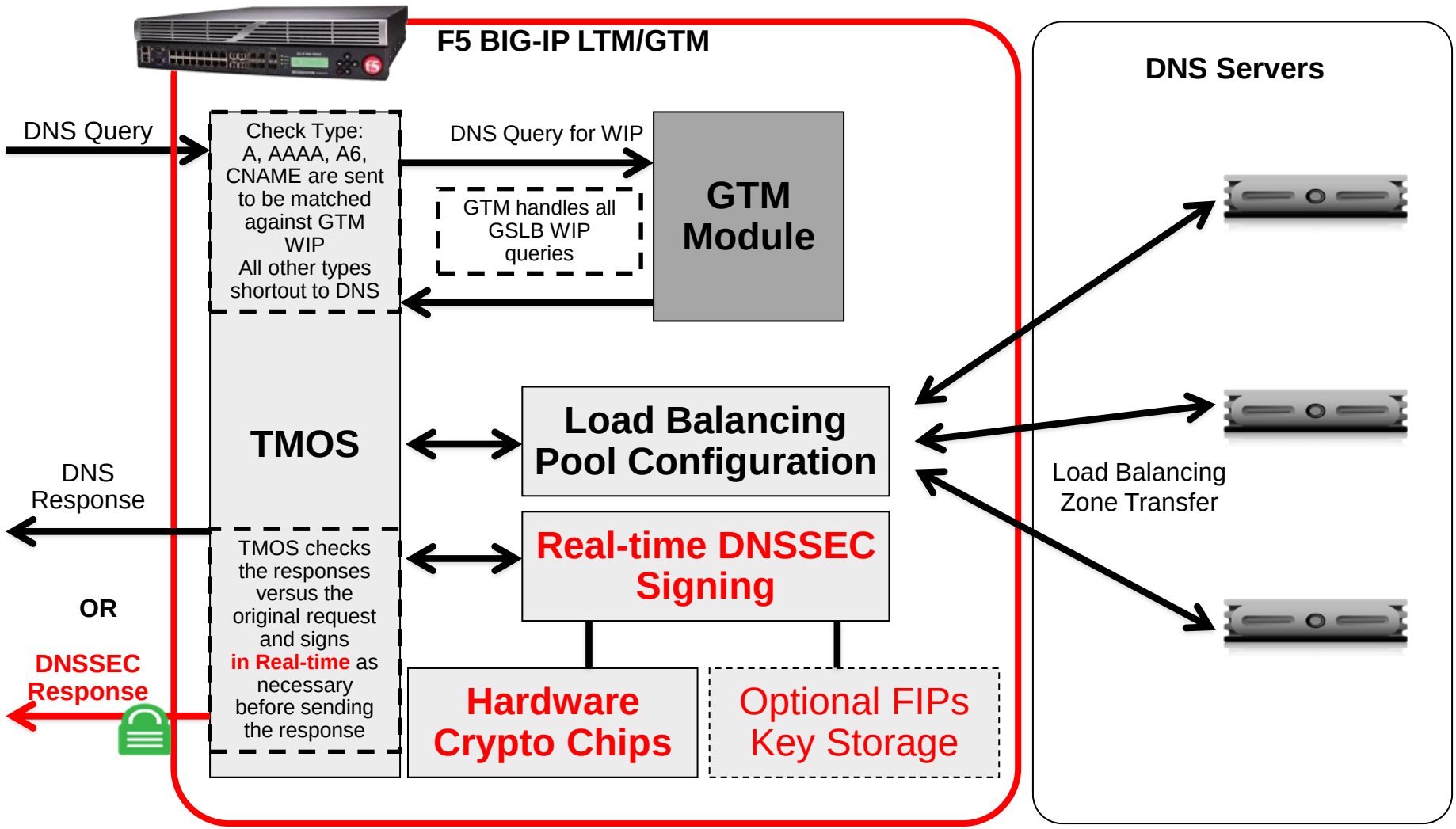
NTT AT

GTMによるDNSSEC対応

AUTHORITATIVE DNSサーバ

- GTMはLTM(Server Load Balancer)と同じHardwareを使用
- LBの得意とするSSLアクセラレーションのcrypto chipsを内臓
- DNSSECの署名でcrypto chipsを使わない手は無い

DNSSEC Architecture



リアルタイム署名

NTT AT

DNSSEC対応状況

Authoritative DNS Serverとして動作する際のサポート状況

DS Record Hash Algorithm	SHA-1, SHA-256 の何れか
NSEC3 Hash Algorithm	SHA-1, SHA-256

署名	
署名鍵のアルゴリズム	RSA/SHA1 RSA/SHA256 RSA/SHA512
鍵長	1026, 2048, 4096
Key Rollover	KSK, ZSK共に二重署名法

Latest Version : v11.3.0

NTT AT

DS Records

- DSの申請は手動で行う必要がある
- OpenDNSSECでも同様
- 保存場所
  - /config/gtm directory
    - dsset-<dnssec_domain_name>

<Sample>
cat /config/gtm/dsset-example.org
example.org. 86400 IN DS 56079 7 1
09f22e86b96725c2f41891bc260304b903c30448 ; xedez-durym-kuvyk-lunos-dituc-meger-sunib-fecar-nibos-fuceg-maxex {key = example.ksk, gen = 0}

DNSSEC対応

DNSキャッシュサーバ

DNSキャッシュサーバの懸念

- キャッシュするだけなら負荷は変わらない？
  - 署名の検証が求められる
  - パケットサイズ、数の増加

- DNSSECによるDNSキャッシュサーバへの影響
  - JANOG26で負荷試験結果が発表されていました
    - CPU、メモリ、帯域使用率の上昇
    - キャッシュDNSサーバの対応は早めが得策
      - DNSSEC普及初期は負荷の影響は少ない
      - DNSSEC普及後の対応では負荷の影響が大きく敷居が高い

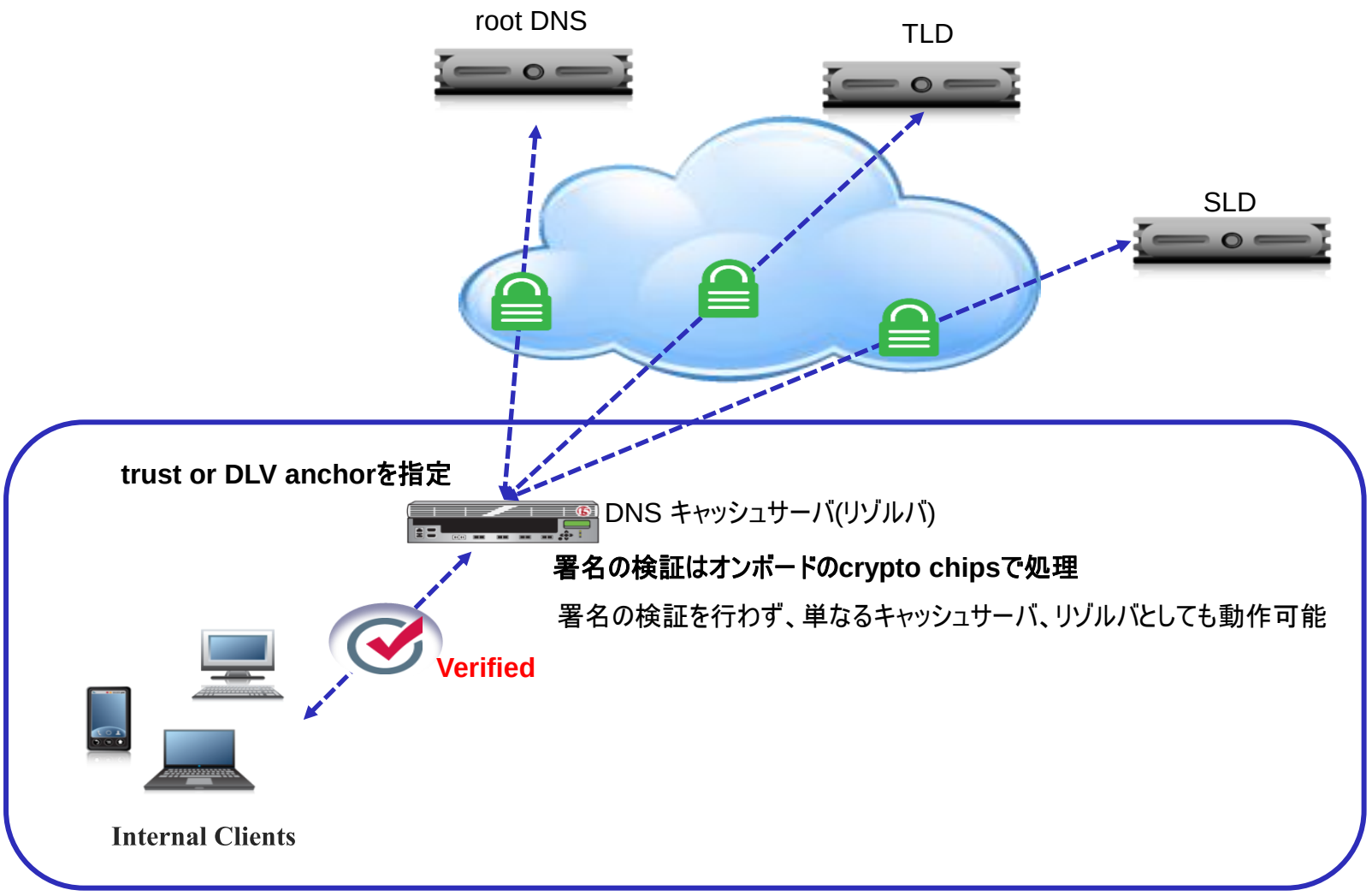
参考：http://internet.watch.impress.co.jp/docs/event/janog26/20100714_380523.html
http://www.atmarkit.co.jp/news/201007/20/janog26.html

DNSキャッシュサーバへの対応

- これまでBIG-IPはAuthoritative DNSや、DNSの負荷分散の対応だけでしたが、DNSSEC対応のリゾルバとして動作し、署名検証ができるDNSキャッシュ、リゾルバをサポートしました
  - ※ v11.2.0以降、GTM or LTM+DNS Moduleで対応

- Authoritative DNSとDNS Cacheとの位置づけ
  - 同居は注意
  - DNSSECの意味も考慮

DNSSEC対応のDNSキャッシュサーバ



NTT AT

BIG-IP GTM Performance

- BIG-IP 1600: ~ 252,000 qps (DNS Query per Second)
- BIG-IP 3900: ~ 694,000 qps
- BIG-IP 8900: ~ 1,789,000 qps
- 1000万 Query per Secondまでスケールアップ

注：DNSSECのPerformanceではありません。

DNSSECやIPv6の場合、TCPを使用する場合が多く、処理能力は環境によって変化します。

NTT AT

DNSSEC導入状況

- 海外では？
- 国内では？
- まだまだ、これから。
  - 最近F5社はDNS関連含めFirewall系の機能追加に注力してる。。。
  - 経験/Know Howは自力で検証して正確性を確認

DNSSUXと言われない為に

- DNSSECの導入は、まだ容易と言い切れない
- エンドユーザはFirewallほど、必要性を感じていない。認知度が低い。またはDNSSECの抵抗感、不安が強い
- DNSSECの普及には今抱える課題を解決し、発展させる事が必要
- ご興味があればご相談下さい

〒170-0013 東京都豊島区東池袋3-23-5 Daiwa東池袋ビル 4F
TEL 03-5956-9603
URL: http://www.ntt-at.co.jp/
f5-sales@ml.ntt-at.co.jp