A10

Always Secure. Always Available.

DNS Summary Day 2024
A10ネットワークス 最新DNSソリューションご紹介

A10ネットワークス株式会社
SP営業部 眞野 桐郎

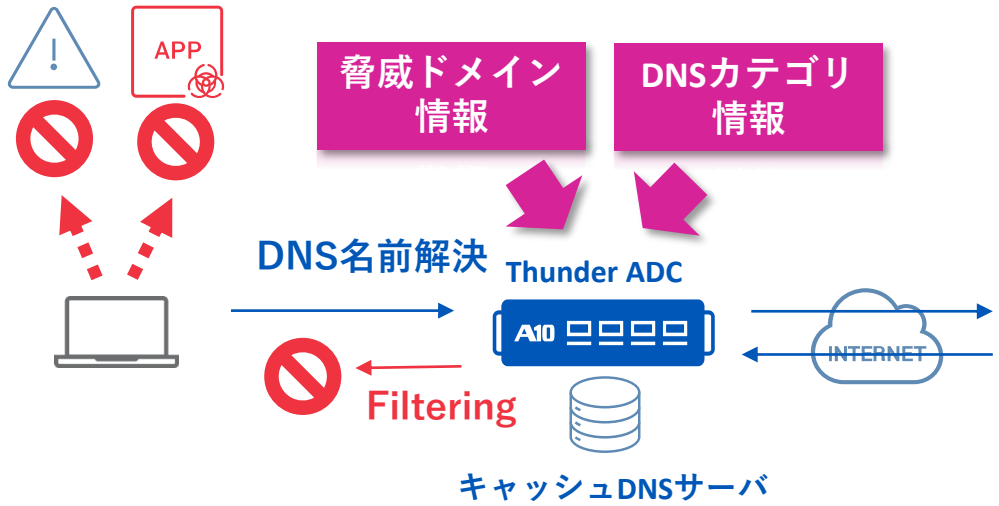
Agenda

本日ご紹介するA10 DNSソリューション

- A10ネットワークス会社紹介
- ①キャッシュDNSサーバ
- ②DNSフィルタリング
- ③Non-STOP DNS
- 本日のまとめ

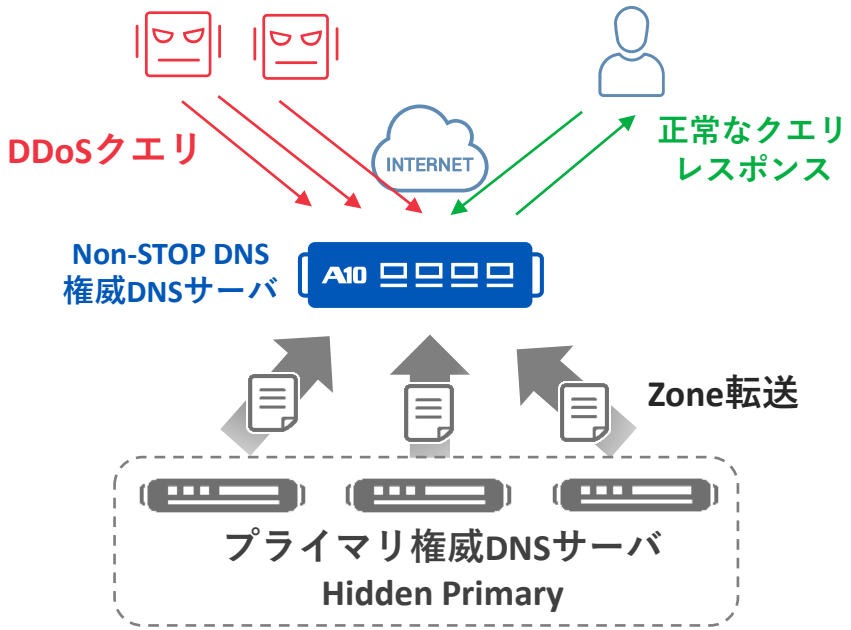
本日ご紹介するA10 DNSソリューション

① キャッシュDNSサーバ
② DNSフィルタリング



高性能＆セキュリティ キャッシュDNSサーバ

③ Non-STOP DNS



DDoSを超える性能 権威DNSサーバ

A10ネットワークス 会社紹介

A10ネットワークス

A10 Networks, Inc. (NYSE: ATEN)

- 設立　　：2004年9月
- 代表者　：Dhrupad Trivedi (CEO)
- 本社　　：米国カリフォルニア州サンノゼ
- 2014年 ニューヨーク証券取引所（NYSE）に上場

A10ネットワークス株式会社

- 設立　　：2009年4月
- 代表者　：川口 亨
  (日本法人代表兼社長 米国本社ヴァイスプレジデント兼務)
- 拠点：東京、大阪

シリコンバレー発
グローバル企業

拠点のある国

27

従業員数

700(日本: 50+)

世界のリーディング企業で採用

製品・サポート提供先の国

117+

導入社数

7,000+

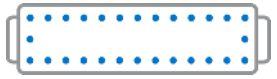
ハイパフォーマンスなネットワークアプライアンス製品により
セキュリティ・アプリケーション配信機能等を提供

共通OSをマルチプラットフォームで提供

仮想インスタンス

高いモビリティ
最大100Gbps

KVM
vmware vSphere
Microsoft Hyper-V



ベアメタル

ハードウェアの共通化
最大60Gbps

あらゆるIAサーバ

コンテナ

クラウドネイティブ
最大100Gbps

kubernetes

クラウドインスタンス

時間・月額サブスク
BYOL
最大10Gbps

Azure
aws
ORACLE CLOUD
Google Cloud

ハードウェアアプライアンス

ハイパフォーマンス
高いポート密度
最大370Gbps

マルチクラウドに対応したあらゆる提供形態

CLI とGUIによる高い操作性と運用性

使いやすいコマンドライン

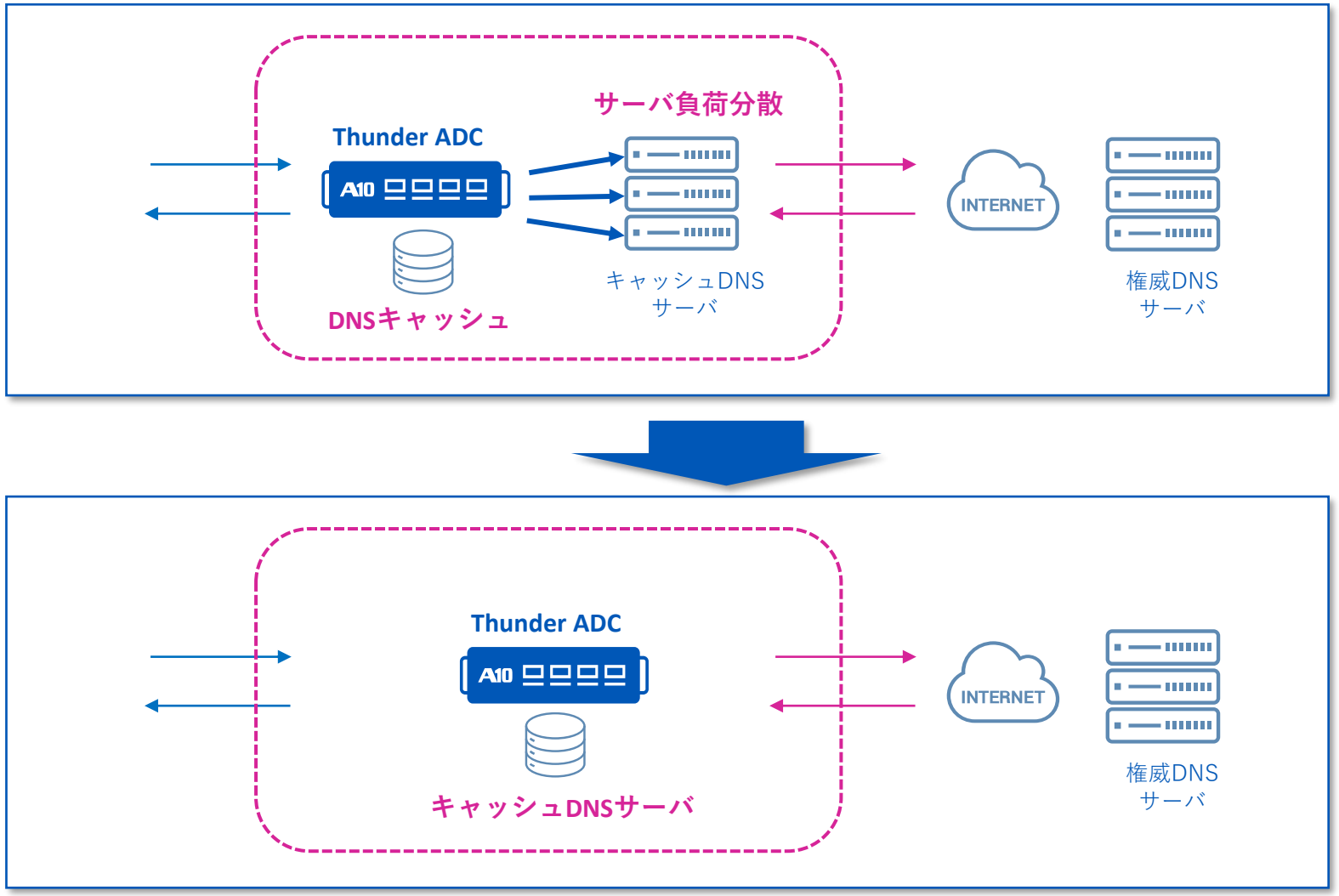
```
Password:
Last login: Mon Mar  5 00:40:34 2018 from …

System is ready now.

[type ? for help]

vThunder>en
Password:
vThunder#
vThunder#show version
Thunder Series Unified Application Service Gateway vThunder
```

直観的で分かりやすい
日本語GUI対応

※英語/日本語/中国語に対応

① キャッシュDNSサーバ

ADCを拡張しキャッシュDNSサーバ機能を実装



～ACOS 4.x

DNSサーバ負荷分散
DNSレスポンスキャッシュ

2020年～（現在最新はACOS 6.x）

ACOS 5.x～

キャッシュDNSサーバ
（フルサービスリゾルバ）
＋DNSサーバ負荷分散

豊富なキャッシュDNSサーバ機能

フルサービスリゾルバ	DNSSec
HA構成	EDNS(0) Client Subnet
キャッシュのストレージ保存（再起動時のキャッシュ保持） ネガティブキャッシュ **HA間のDNSキャッシュエントリ同期**	DoH/DoT ハードウェアオフロード可能
aFlexによるDNSパケットのエンジニアリング	**DNS DDoS防御機能** **DNSクエリ/レスポンスベースRate-limiting**
DNS LBの併用可能	ACL
DNSクエリロギング	DNSキャッシュポイゾニング対策 Source Port Randomization
マルチテナント構成	不正DNSクエリのフィルタ (Malformed Query Drop) DNS Firewall
IPv6対応	RPZ (Response Query Zone)
DNS64対応	DNS Flag Day 2020 準拠
DNSアプリケーショントラフィックの可視化	**独自コード実装でBind等OSSの脆弱性に該当しない**

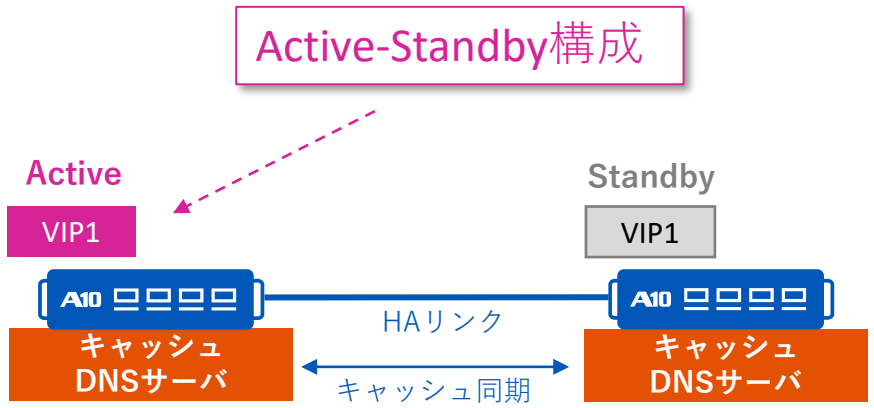
高いキャッシュDNSサーバ性能

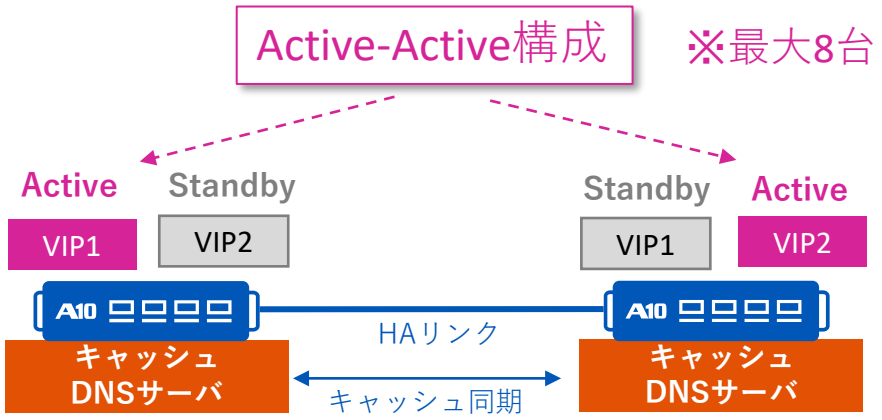
ミドルレンジモデルの Thunder 3350S ADCで1台あたり100万QPS超の性能

会場のみ

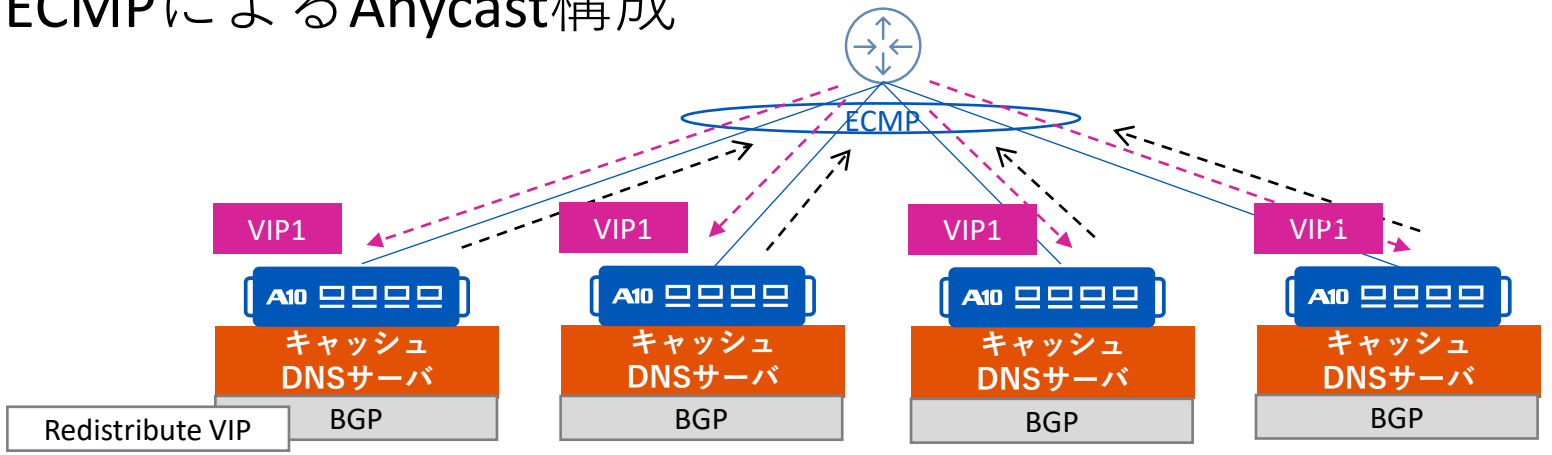
冗長化/拡張構成

- VRRP-A（HA）構成





- ECMPによるAnycast構成



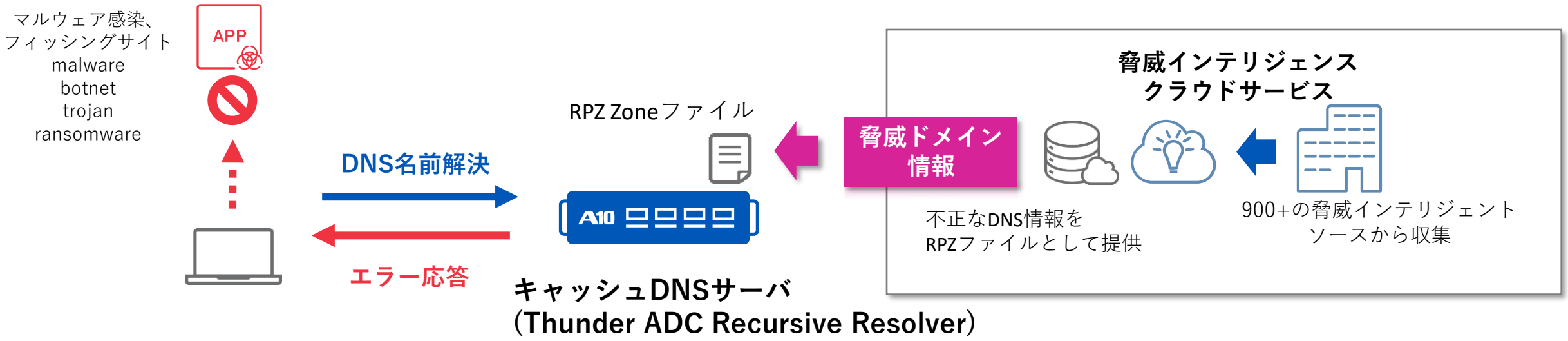
BGP, OSPF, IS-ISサポート
BFDサポート
CLOSデザイン対応
　BGP Unnumbered, RFC 5549サポート

② DNSフィルタリング

DNSフィルタリング（1）脅威対策

- マルウェア感染、フィッシングサイトなどセキュリティ上の脅威が含まれるURL/ドメインの名前解決を、キャッシュDNSサーバであるThunder ADCでフィルタリング
- 脅威インテリジェンスのクラウドサービスから脅威ドメイン情報をRPZ Zoneファイルとして Thunder ADCにインポート

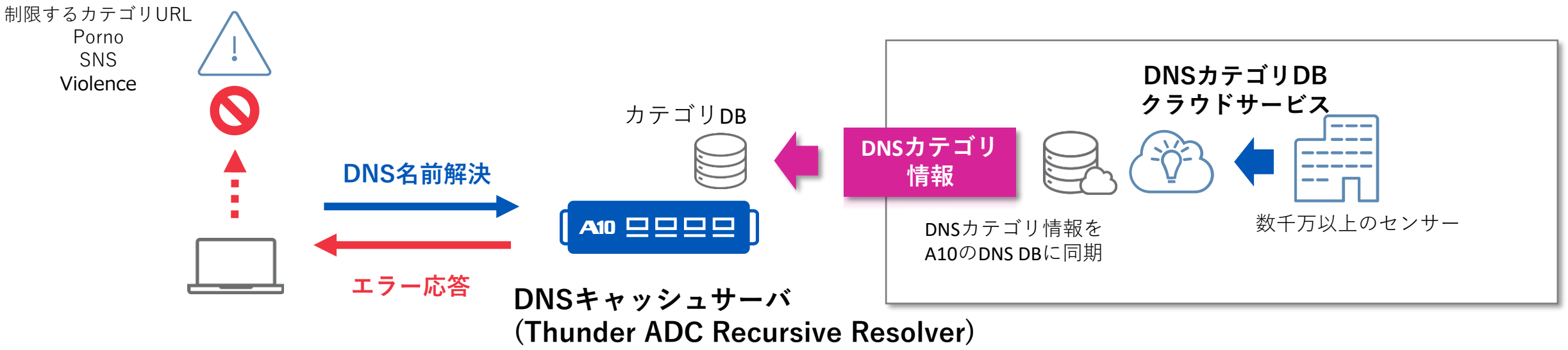
DNSによる脅威防御に最適



DNSフィルタリング（2）アクセス制御

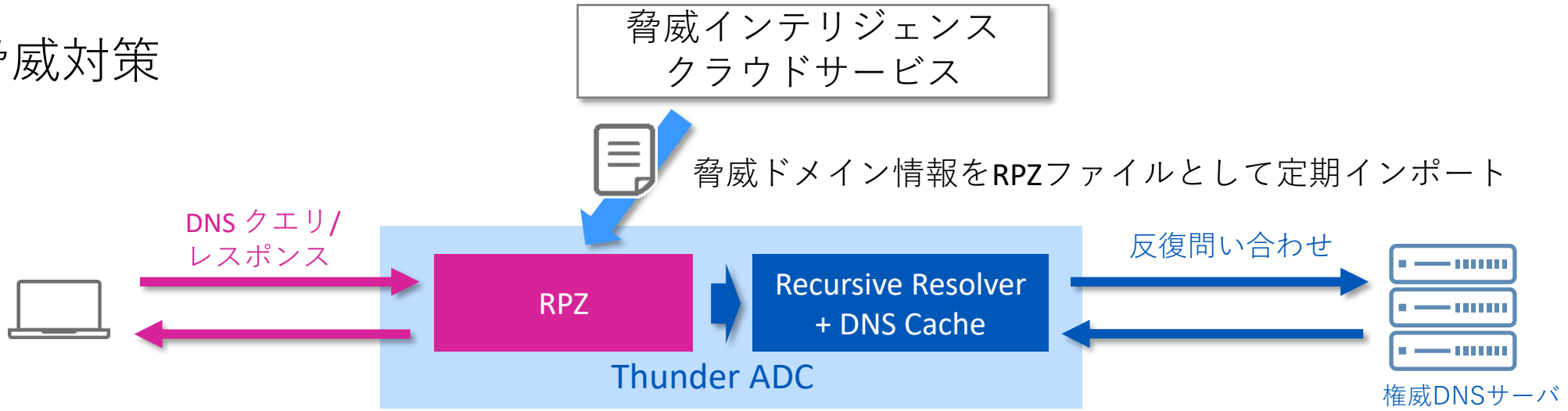
- Web通信のHTTPS暗号化が進んだことで、プロキシ型URLフィルタでFQDN以上のアクセス制御が困難。キャッシュDNSサーバによるFQDNベースのアクセス制御がその代用として利用可能。URLフィルタ比べ導入、構成がより容易。
- DNSカテゴリDBのクラウドサービスからカテゴリ情報をThunder ADCのDBに同期

DNSによるアクセス制御に最適

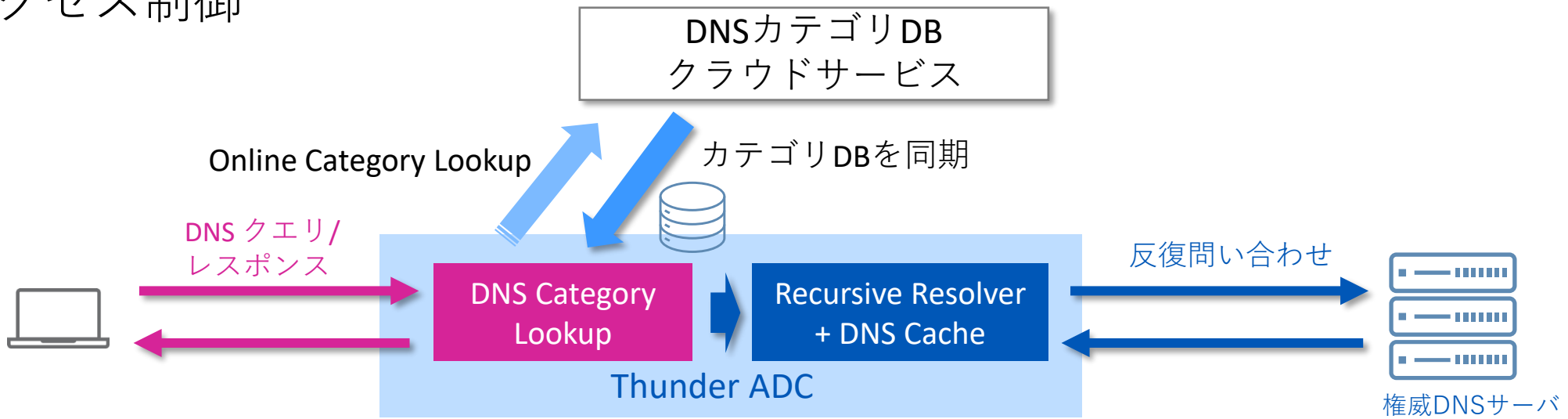


動作フロー図

（1）脅威対策



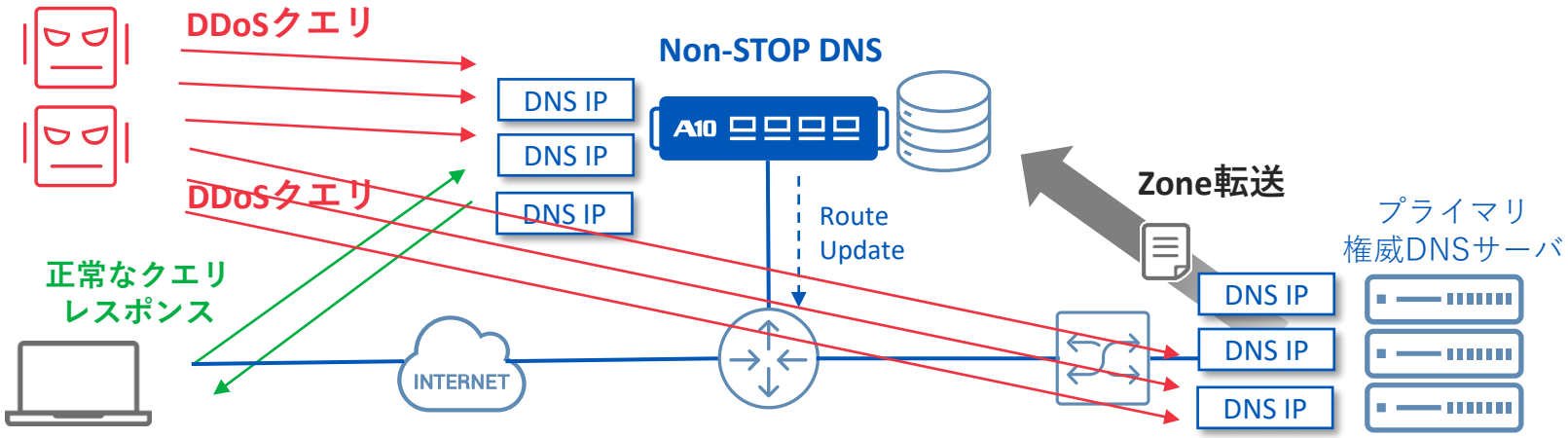
（2）アクセス制御



③ Non-STOP DNS

Non-STOP DNS（権威DNSサーバ）

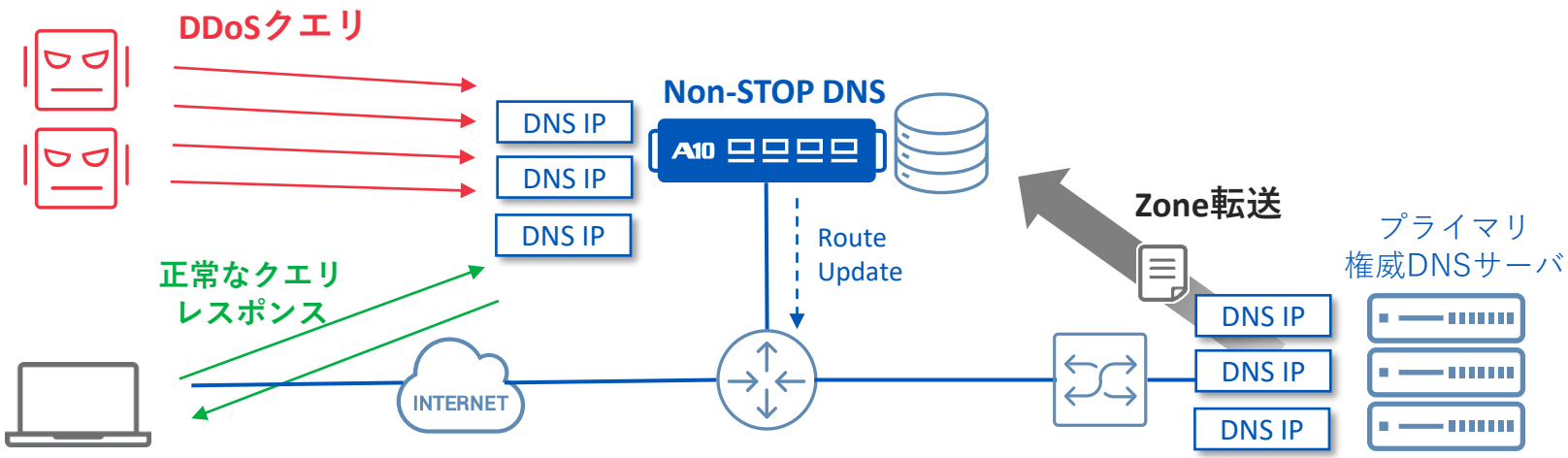
- **セカンダリ権威DNSサーバとして構成**（Hidden Primary）
- 既存権威DNSサーバのIPをそのまま利用可能（アドレス重複OK。Routing Updateで権威DNS宛のトラフィックを引き込む）
- DDoS含めた全てのDNSクエリを圧倒的な性能で処理（多数の権威DNSサーバ、ドメインを1台に収容可能）



Non-STOP DNS（権威DNSサーバ）

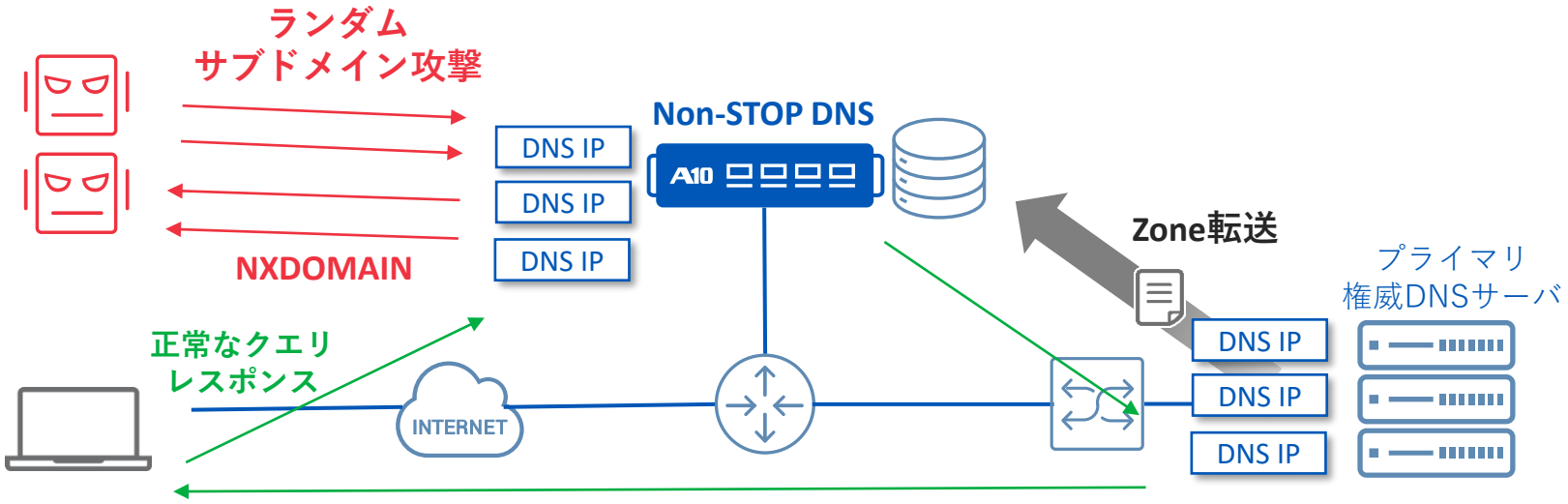
- **圧倒的な性能でDDoS攻撃が無効化**
- DDoS専用機ではフィルタが難しいランダムサブドメイン攻撃にも対応
- DDoSクエリ/正常なクエリ関係なく全て応答（ランダムサブドメイン攻撃にはNXDOMAINで応答）

最大3,500万 DNS QPS 処理可能（Thunder 7445 TPS/6655S TPS）
DDoS防御はフィルタでなく圧倒的な性能で全て応答する



Non-STOP DNS（権威DNSサーバ）

- **正常なDNSクエリのみプライマリ権威DNSサーバへ転送可能**
- DDoSに対するエラー（ランダムサブドメイン攻撃に対するNXDOMAINなど）はNon-STOP DNSが直接応答
- 正常なDNSクエリのみプライマリ権威DNSサーバに転送し、プライマリ権威DNSサーバからはNon-STOP DNSを経由せず直接応答可能



DNS DDoS Mitigationの限界と Non-STOP DNSによる回答

- **DDoS Mitigatorによるランダムサブドメイン攻撃防御は難しい**

複数要素を組み合わせ動的に攻撃を特定、検知
- QPS
- 送信元IPアドレス
- ドメイン名
- FQDN
- 宛先IPアドレス
- DNS DDoS Botアドレスを収集

それでも正確な検知は難しく
誤検知の可能性高い
・DDoSの検知漏れ
・正常通信までDrop

A10はDNSクエリの中のDDoSのみフィルタするのでなく、DDoSまで含めた全てのDNSクエリを処理できる性能で対応します

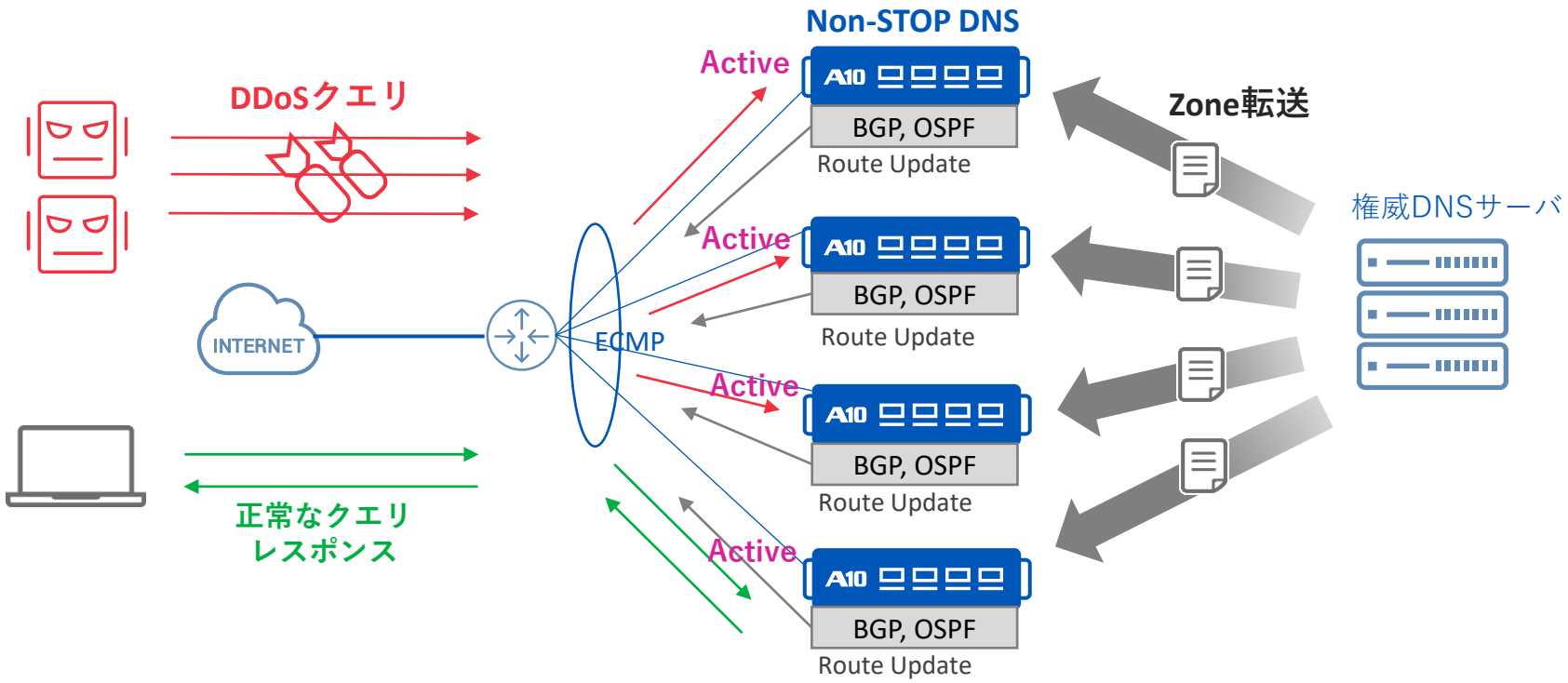
Non-STOP DNSの圧倒的DNS QPS性能

- 圧倒的なDNS QPS性能とDNS Zone収容キャパシティ
- DDoS含めた全てのDNSクエリ処理する圧倒的な性能

Non-STOP DNS 対応モデル	Thunder 5845 TPS	Thunder 7445 TPS	Thunder 6655S TPS
最大QPS性能	18M QPS	35M QPS	35M QPS
最大ドメイン数	256K	2M（2百万）	4M（4百万）
最大FQDN数	25M	40M（4千万）	400M（4億）

冗長化/拡張構成

- ECMPによる負荷分散構成可能
  - StandaloneのNon-STOP DNSからRoute Updateを行い、ECMPによりDNSクエリを分散
  - Non-STOP DNS障害時、障害検知やECMPからの切り離しはBFD、Neighbor切断で実現



本日のまとめ

①キャッシュDNSサーバ
②DNS Filtering

- ADC由来のDNS機能（DNS LB、キャッシュ同期、DNS64 etc.）
- 高性能DNSアプライアンス（1M QPS超）
- 豊富なネットワーク機能（HA、eBGP etc.）
- DNSフィルタリングによる脅威防御/アクセス制御
- 独自コードのためOSSの脆弱性に影響を受けない

③Non-STOP DNS

- 圧倒的なDNSレスポンス性能
- DDoS攻撃、ランダムサブドメイン攻撃にも対応
- 既存DNS構成に追加するだけで実装可能
- 権威DNSサーバを集約可能
- 独自コードのためOSSの脆弱性の影響なし


A10
Always Secure. Always Available.
The A10 Advantage