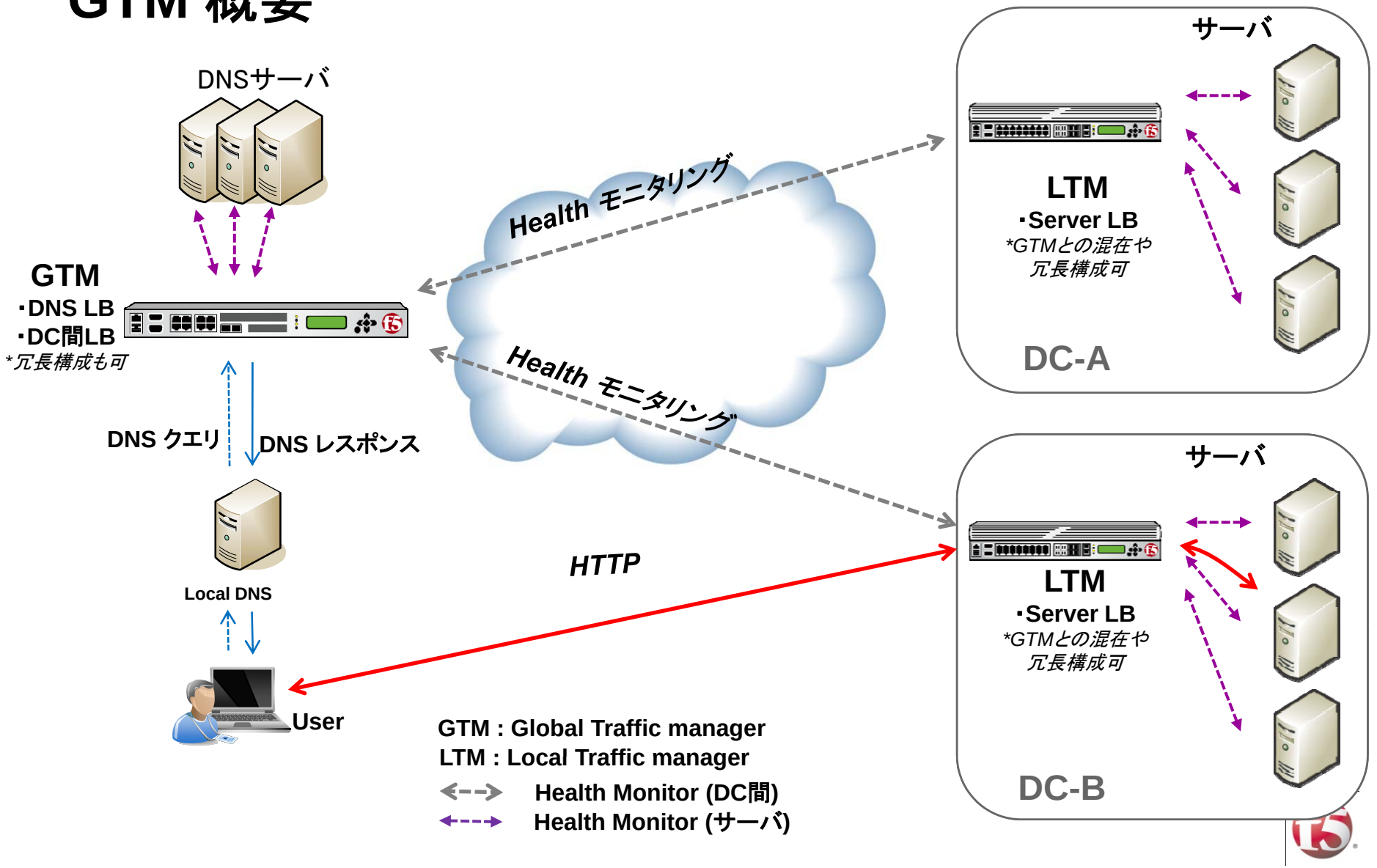
GTM (Global Traffic Manager) のご紹介

F5 Networks Japan Inc.

IT agility. Your way.

目次

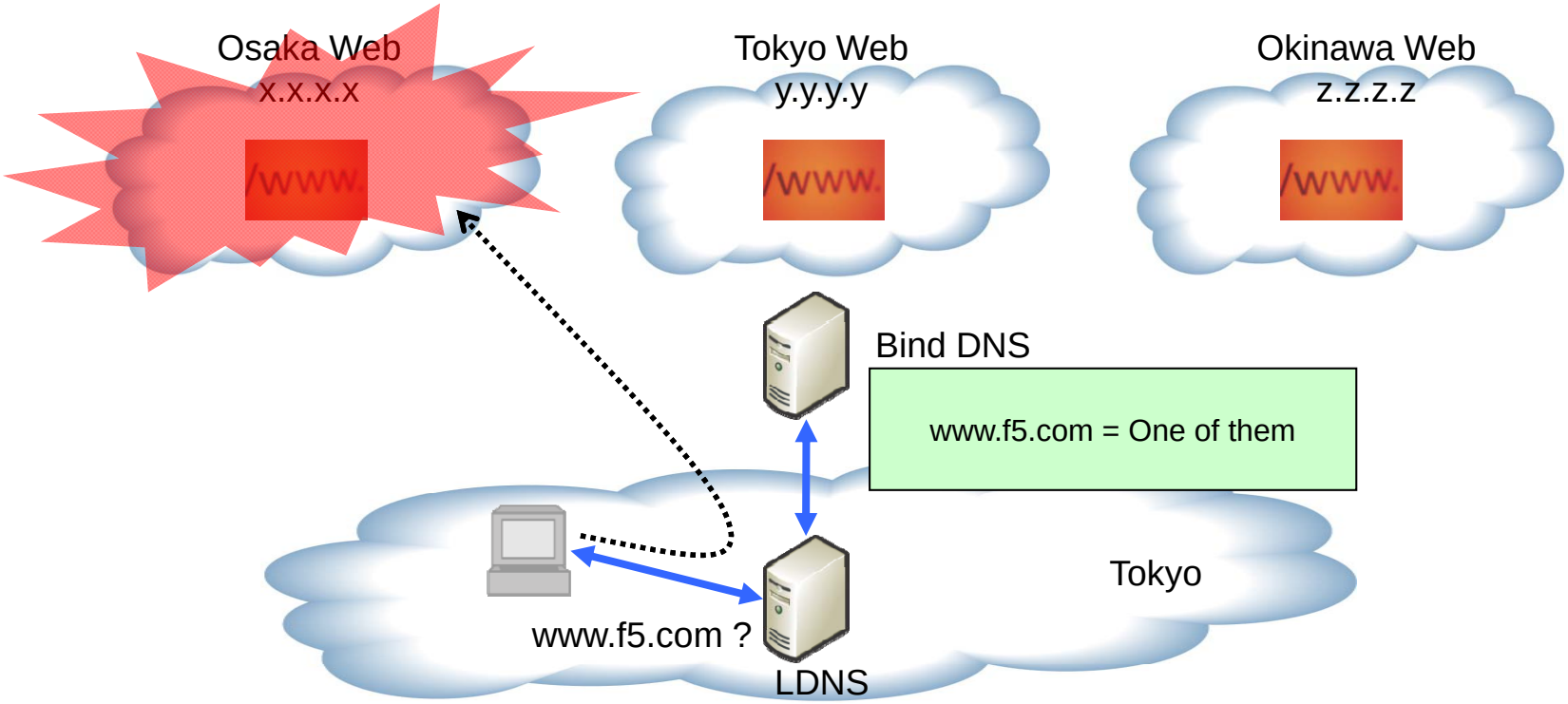
GTM 概要


DNSサーバ
GTM
・DNS LB
・DC間LB
*冗長構成も可
DNS クエリ
DNS レスポンス
Local DNS
User
Health モニタリング
Health モニタリング
HTTP
サーバ
LTM
・Server LB
*GTMとの混在や
冗長構成可
DC-A
サーバ
LTM
・Server LB
*GTMとの混在や
冗長構成可
DC-B
GTM : Global Traffic manager
LTM : Local Traffic manager
Health Monitor (DC間)
Health Monitor (サーバ)

BIG-IP GTMのベネフィット

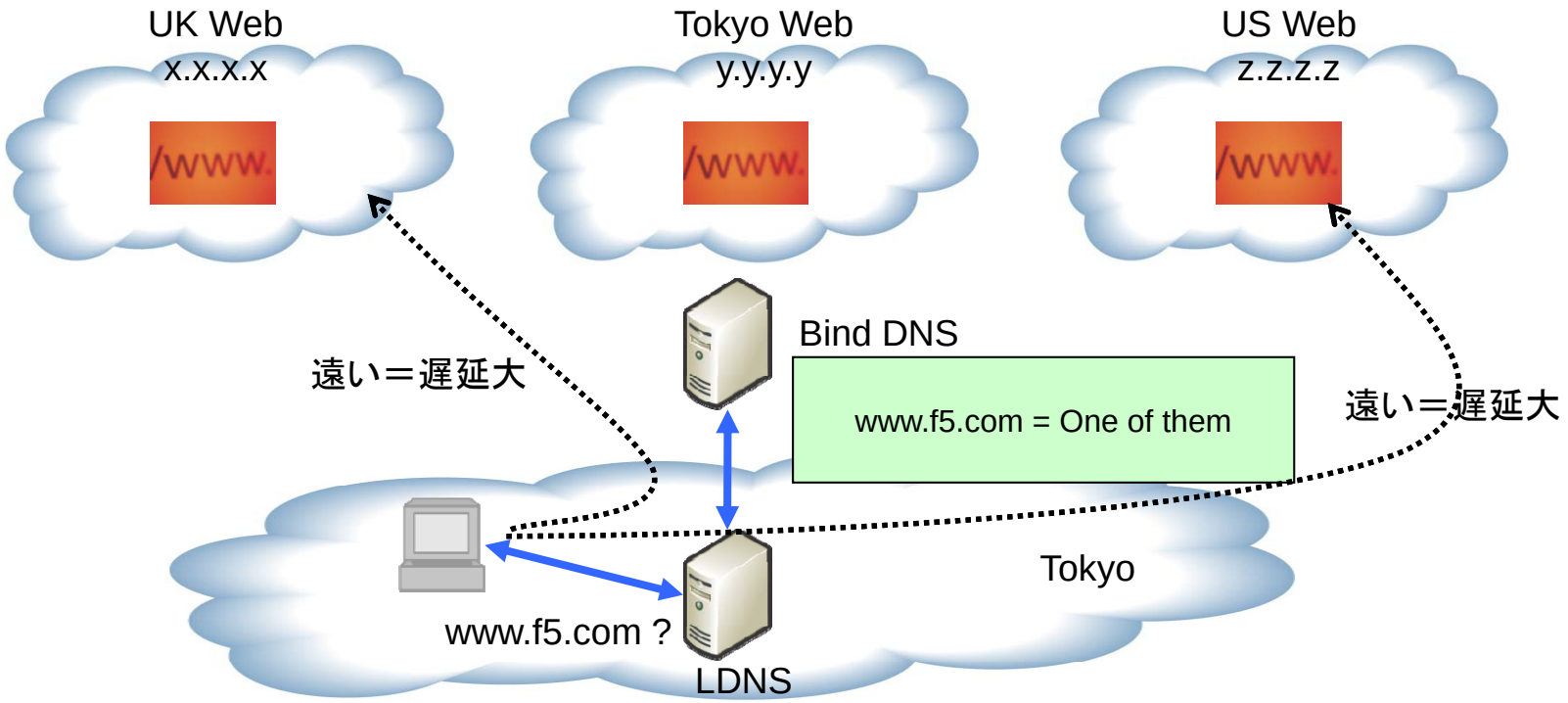
- サイトの可用性を最大限に引き出し、ダウンタイムを最小化
- 様々なアプリケーションに対応したモニターを実施して正常性を確認
- 他ベンダーのロードバランス機器に対応できる唯一のソリューション
- iRules を使ったきめ細かいポリシーを設定可能
- IPv6 AAAAレコード(クワッドAレコード)対応
- DNSSECへ対応

GTMが有効な例(1)
ディザスタリカバリ対策でウェブサーバを国内複数拠点に配置



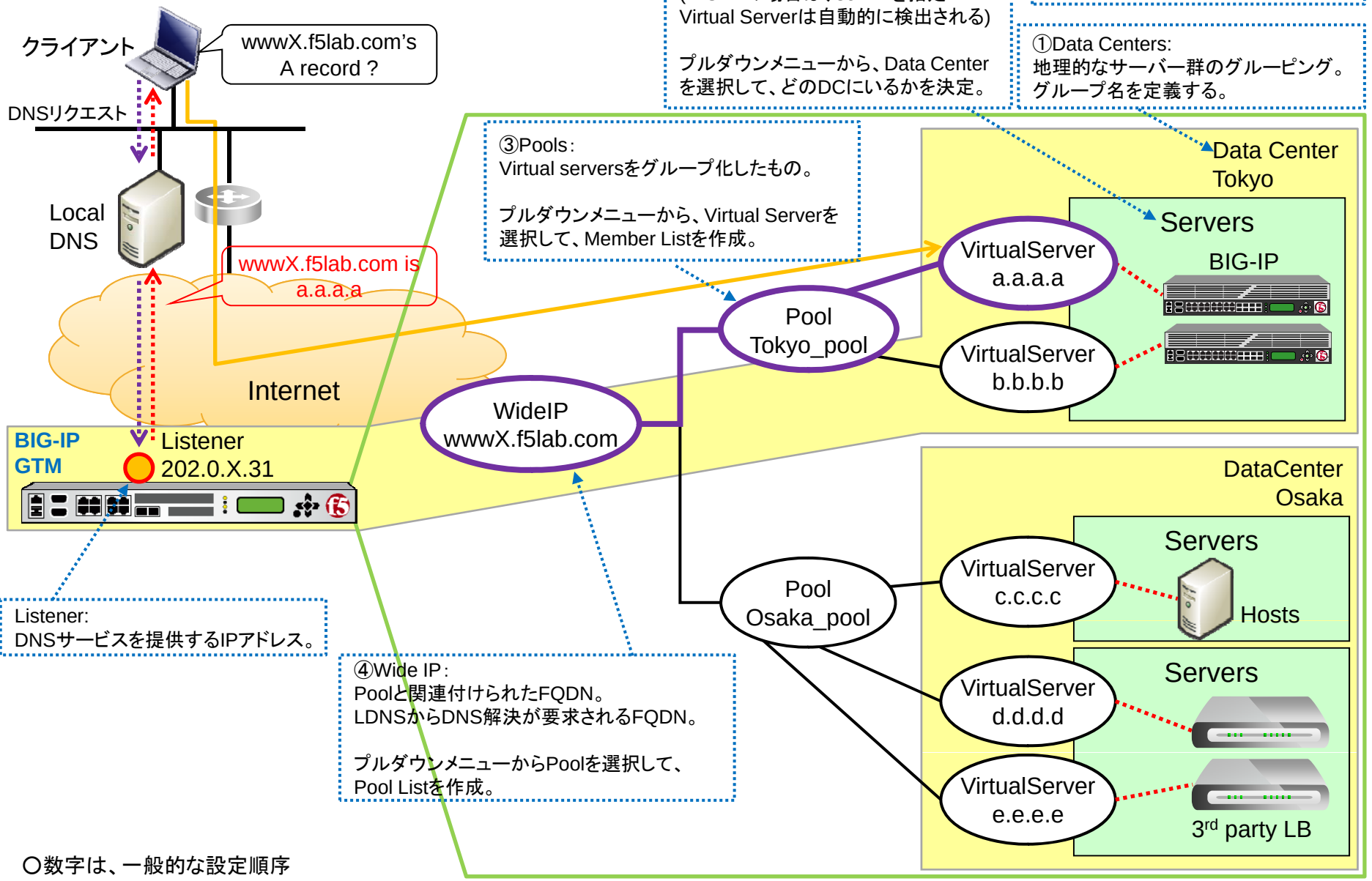
- 大阪DC全体がダウンしても、Bindによって大阪アドレスが返される場合があり、その場合、他拠点のサービスが稼動していた場合でもクライアントはサーバに接続できない

GTMが有効な例(2)
ディザスタリカバリ対策でウェブサーバを国外複数拠点に配置



- 東京のクライアントがUK/USのAレコードを受け取ってしまうと、ウェブサーバが近隣の東京に存在するにもかかわらず遠方のUK/USへ接続されてしまい効率が悪い
- 先の例のように1拠点がダウンした場合、クライアントの一部が接続不可能になる

GTMオブジェクトイメージ



○数字は、一般的な設定順序

GTMロードバランス

GTMロードバランス概要

- GTMがDNSリクエストを受け取ると、ベストなVirtual Serverを決定するために、ロードバランシングモードを使用する。
- Virtual Serverを決定したら、DNS応答を生成して、リクエストしてきたクライアントLDNSに返答する。

- ロードバランシングモードは、以下2つのカテゴリーに分かれる:

- スタティックロードバランシング
  - 事前に定義した方式によるバランシング

- ダイナミックロードバランシング
  - その時点のパフォーマンス集計情報に基づいてバランシング

階層ロードバランス

- 階層ロードバランスとは、クライアントLDNSからの問い合わせに対する名前解決プロセスの間に、複数のポイントで発生するロードバランシングシステムである。GTMの階層は以下の2つ。

- Wide-IPレベルロードバランシング
  - Wide-IPは2つ以上のプールを含んでいる状態において、GTMは、最初はプールに対してロードバランスし、そのあとで、選ばれたPoolのVirtual Serverにロードバランスする。

- Poolレベルロードバランシング
  - プールは、1つ以上のVirtual Serverを含んでいる状態で、GTMが、ベストなPoolを選ぶために、Wide-IPレベルロードバランシングを使った後で、そのPoolの中のVirtual Serverを選ぶために、Poolレベルロードバランシングを使う。
  - そのPoolの中の最初のVirtual Serverが利用できない場合、GTMは、そのプールにアサインされたロードバランシングモードに基づいて、次にベストなVirtual Serverを選択する。
  - このレベルには、3段階のロードバランシングメソッドを選択できる。

    ①Preferred　：最初に選ばれるロードバランシングモード

    ②Alternate　：①が何も返答しない場合に選択されるロードバランシングモード

    ③Fallback　：①及び②が何も返答しない場合に選択されるロードバランシングモード

スタティックロードバランシングモード

※
W：Wide-IP Level LB
①：Preferred
②：Alternate
③：Fallback

モード	概要	W	①	②	③
Round Robin	PoolのVirtual Serverの間を循環して、コネクションを分配する。 時間とともに、各Virtual Serverは等しい数のコネクションを受け取る。	○	○	○	○
Ratio	重み付けラウンドロビンとして、コネクションをVirtual ServerのPoolに分配する。 ユーザが各リソースに割当てたプライオリティレベルまたはウェイトをベースに、GTMがコネクション要求をローテーションさせる。	○	○	○	○
Static Persist	あるアルゴリズムを用いて、LDNSの送信元IPアドレスでPoolメンバー(Virtual Server)にパーシストする。 GTMがハッシュアルゴリズムを使ってリストのメンバーの順番を決定して、リストから選ぶ。 それぞれのLDNSは同じVirtual Serverの返答をもらうことになり、複数のLDNSからの要求により、全てのVirtual Serverへトラフィックを分配する。		○	○	○
Global Availability	Poolに順番にリストされているVirtual Serverを使う。各コネクション要求に対して、リストの最初の有効なVirtual Serverを送る。そのVirtual ServerがFull状態か、または利用できない時だけ、リストの中の次のVirtual Serverを返答する。 時間とともに、リストの中の最初のVirtual Serverが最多のコネクションを受け取り、最後のVirtual Serverは最少のコネクションを受け取る。	○	○	○	○
Topology	コンフィグレーションファイルのトポロジーステートメントに、トポロジーデータベースを追加することによって、トラフィックフローを制御または限定できる。 このモードによって、近隣へ誘導するロードバランスを展開できる。 例えば、特定地域のクライアントのリクエストは、同じ地域のデータセンターまたはサーバに向けさせることができる。	○	○	○	○

※それぞれのロードバランシングメソッドに利用できるものに「○」

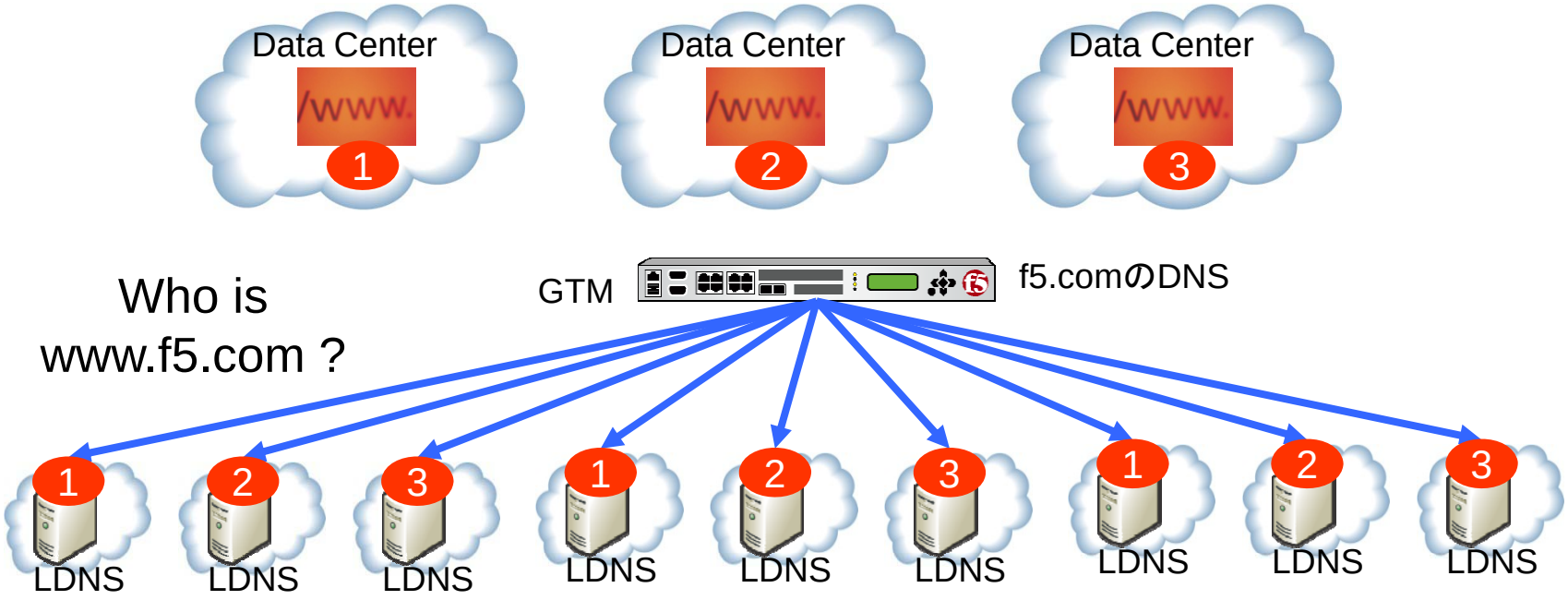
スタティックロードバランシングモード (Cont.)

※
W：Wide-IP Level LB
①：Preferred
②：Alternate
③：Fallback

モード	概要	W	①	②	③
Fallback IP	GTMは、クエリに対する応答として、Fallback IPとして、指定したIPアドレスを返す。 Fallback IPアドレスとしてIPv4とIPv6アドレスの両方を指定することができる。 指定したIPアドレスの有効性はモニターされない。Fallback IPモードを使う場合、どのロードバランシングモードも有効なVirtual Serverを返えさないときに、DRサイトのIPを指定することができる。 Fallbackメソッドのためにだけこのモードを使うように推奨。		○	○	○
None	現在のロードバランシングメソッドをスキップしたいときのスペシャルモード。 例えば、もし、AlternateメソッドをNoneに設定したとき、GTMは、Alternateメソッドをスキップして、Fallbackメソッドで指定したモードを使う。もし、FallbackメソッドがNoneに設定されていて、複数のPoolが存在していたら、GTMは、次の有効なPoolを使う。 もし、全てのPoolが利用不可であれば、GTMは、BINDによって、全てのPoolメンバーのIPアドレスをまとめて返答する。			○	○
Return to DNS	コネクション要求を即座に、他DNSに転送する、もうひとつのスペシャルモードである。 もし、一次的にサービスからPoolを取り除きたい場合等に、このモードは特に有益である。		○	○	○
Drop Packet	GTMはパケットによって何もせず、単に、要求を落とす。 FallbackにだけDropパケットロードバランシングモードを使うことを推奨。		○	○	○

※それぞれのロードバランシングメソッドに利用できるものに「○」

スタティックロードバランシングの例ーラウンドロビン



- GTMはLDNSからの問い合わせに対し、1，2，3，1，2，3と順番に応答

ダイナミックロードバランシングモード

※
W：Wide-IP Level LB
①：Preferred
②：Alternate
③：Fallback

big3dが測定

モード	概要	W	①	②	③
Round Trip Times(RTT)	クライアントLDNSとデータセンター間のラウンドトリップタイムが最も速いVirtual Serverを選択する。		○		○
Completion Rate	データセンターとクライアントLDNSの間のトランザクションで、パケットドロップ数または、タイムアウトしたパケット数が最少であるVirtual Serverを選択する。		○		○
Hops	Tracerouteユーティリティを使って、クライアントLDNSとそれぞれのデータセンター間の中間システム(ルータのホップ)数をトラックする。ホップ数が最も少ないVirtual Serverを選択する。		○		○
CPU	名前解決リクエストを処理するにあたって、CPU処理時間が最もアベイラブルなVirtual Serverを選択する。		○		○
Packet Rate	トラフィック量：Packets/Secの数が最も少ないVirtual Serverを選択する。		○	○	○
Kilobytes/Second	トラフィック量：KB/secの数が最も少ないVirtual Serverを選択する。		○		○
Least Connections	コネクション数の最も少ないLTM(及びSNMPが有効な他LBやホスト)上のVirtual Serverを選択する。		○		○

※それぞれのロードバランシングメソッドに利用できるものに「○」

ダイナミックロードバランシングモード (Cont.)

※
W：Wide-IP Level LB
①：Preferred
②：Alternate
③：Fallback

モード	概要	W	①	②	③
Quality of Service (QOS)	後述		○		○
VS Capacity	キャパシティによるウェイトをつけて、Virtual Serverのリストを生成し、そのリストから1つのVirtual Serverを選択する。 最もキャパシティを持つそのVirtual Serverがしばらく選択されるが、時間とともに、全てのVirtual Serverが選択される。 複数のVirtual Serverが同じキャパシティを持っていたら、GTMは、それらのVirtual Serverをラウンドロビンする。		○	○	○
Virtual Server Score	GTMが、ユーザ定義のランキングをベースに、コネクション要求をVirtual Serverに割当てる。 LTMのVirtual Server限定であり、LTM間でコネクションが管理されている場合にのみ有効。 ロードバランシング操作に影響を与える他の設定と違って、GTMを通して、Virtual Server Scoreをアサインすることはできない。 その代わりに、そのVirtual Serverが設定されたLTMを通して、この設定をアサインできる。		○	○	○

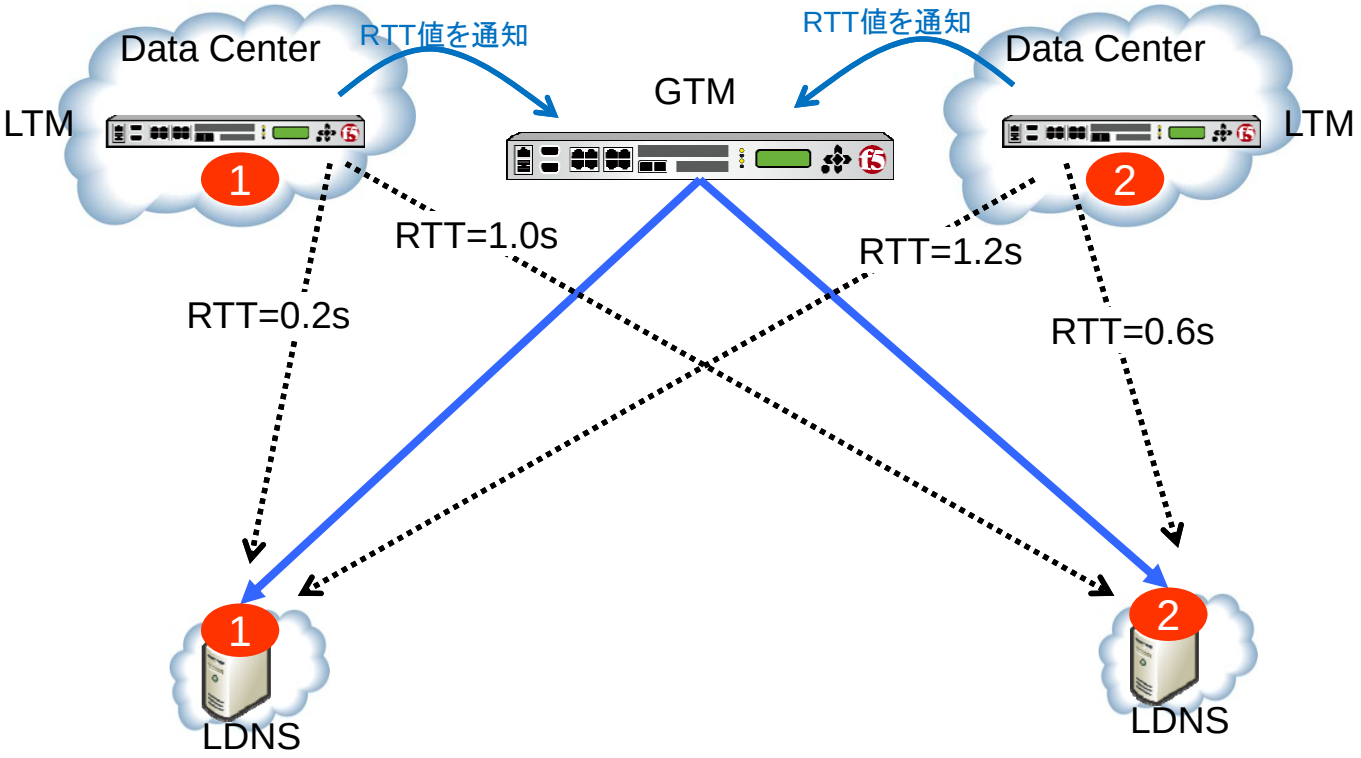
※それぞれのロードバランシングメソッドに利用できるものに「○」

ダイナミックロードバランシングモード (Cont.)

- Quality of Service
  - 下表の要素を含むロードバランシングモード。
  - これらのパフォーマンスファクタの算出値をベースにしており、全体スコアが最も良いサーバが選ばれる。
  - 以下の場合にはラウンドロビンが適用される。
    - リソースが同一のスコアを持っている場合
    - 何らかの理由でQoSスコアを決定することができない場合
  - 基本的に、この算出値を変更する必要はないが、個々のファクタに置くウェイトを変更することができる。

要素	どのように測定するか	Default値	上限値の例
Completion Rate	転送パケットの成功率(%)	5	100
Hops	中間システム数(ホップ数)	0	64
Kilobytes/second	スループット(Kbps)	3	15,000
Link Capacity	ターゲットの動的レシオをベースに	30	2,000,000
Packet Rate	Packets per Second(PPS)	1	700
Round Trip Time	Microsecond(ms)	50	2,000,000
Topology	LDNS IPアドレスとServerを比較して、ネットワークの近さを定義するスコア	0	100
Virtual Server Score	ユーザが定義したVirtual Serverのランキング	0	100
VS Capacity	ノードがUpしている数	0	20

ダイナミックロードバランシングの例-Round Trip Time



- クライアントは近隣のLDNSを参照することを前提
- LDNSからの最初のリクエストにはラウンドロビン等で応答する
- 各拠点のBIG-IPはLDNSまでのRTTを測定し、2度目以降のアクセスでは最もレスポンスの良い拠点のレコードを返す

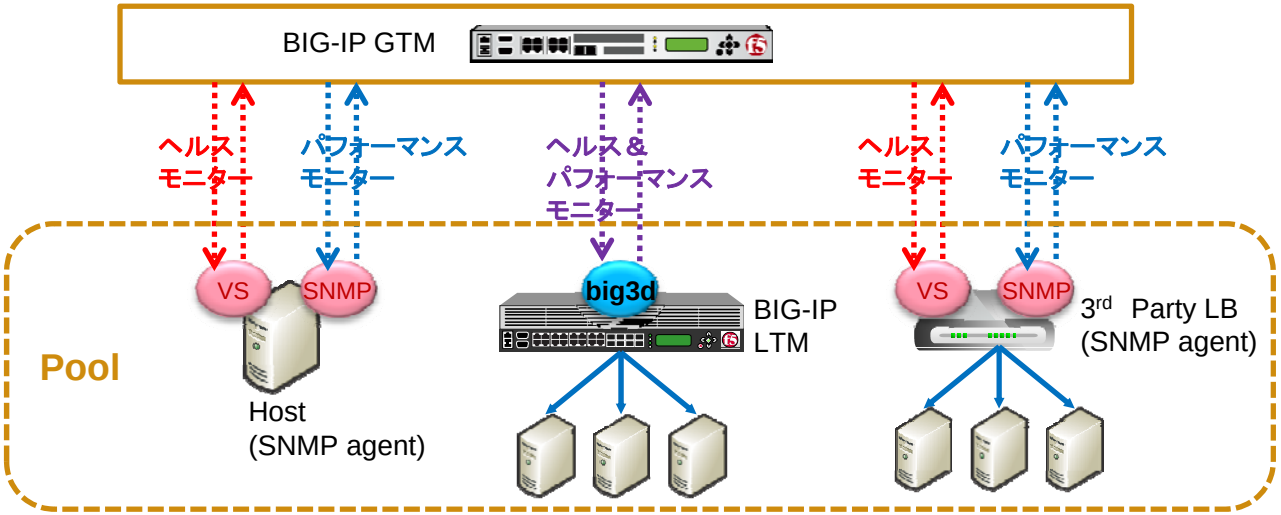
GTMによるモニター

モニター

- GTMの重要な機能の一つに、"モニター"と呼ばれる機能がある。
- モニター対象は、「Virtual Servers」または「Pools」上のコネクションである。
- モニターは、以下の2種類がある。

  ヘルスモニター
  - ある「Virtual Server」または「Pool」が、指定したタイムアウト時間内に反応があるかどうか

  パフォーマンスモニター
  - ある「Virtual Server」または「Pool」のステータスが、パフォーマンス劣化を示すかどうか
- モニターは、設定されたインターバルで、PoolまたはVirtual Serverのステータスをチェックする。
- モニターの結果により、GTMは、他のリソースにトラフィックをリダイレクトできる。



モニターのタイプ

- シンプルモニター
  - 指定したプロトコルのパケットをリソースに送り、レスポンスを待つことによって、ヘルスチェックを行う。
  - モニタがレスポンスを受けると、ヘルスチェックは成功(リソースはUpしている)と判断される。

- ECV (extended content verification)
  - 指定したプロトコルを使って、コンテンツをクエリとしてリソースに送り、コンテンツを受け取ることによって、ヘルスチェックを行う。
  - モニタが正しいコンテンツを受信すると、ヘルスチェックは成功(リソースはUpしている)と判断される。

- EAV (External Application Verification)
  - 指定したプロトコルのサービスチェッカープログラムを使って、アプリケーションにアクセスすることによってレスポンスを得る、ヘルスモニタまたはパフォーマンスモニタである。

シンプルモニター

- Gateway ICMP
  - ICMPを使用したシンプルなステータスチェック
  - GTMから見たServer(LTMのVirtual Serverや実サーバ)、またはLink監視として、ゲートウェイICMPモニターを使うことができる。
  - モニターがICMP_ECHOデータグラムへのReplyを受けると、チェックは成功。

- TCP Half Open
  - TCP SYNパケットを送ることによるステータスチェック
  - SYN-ACKパケットを受け取ると、サービスは起動していると判断し、3WAYハンドシェイクを完了させずに、RESETパケットをサービスに送る。

ECV (Extended Content Verification)

- HTTP
  - Webページから特定のコンテンツの受信を試みることで、HTTPサービスを確認
  - ユーザ名／パスワードも送信できる
  - 設定したレシーブストリング値と一致したら、成功と判断する
- HTTPS
  - SSLによってセキュリティーを確保されたWebページから特定のコンテンツの受信を試みることでHTTPSサービスを確認
  - ユーザ名／パスワードも送信できる
  - 設定したレシーブストリング値と一致したら、成功と判断する
- TCP
  - TCPで特定のコンテンツの受信を試みることで、TCPの正常性を確認
  - ユーザ名/パスワードは設定できない
  - 設定したレシーブストリング値と一致したら、成功と判断する

EAV (External Application Verification)

- BIG-IP
  - GTM配下にLTMが存在する場合、このモニターを設定することは必須。手動で設定しない場合は、GTMが自動的にこのモニターをLTMに割当てる。
  - LTMが行うリソース監視によって収集されたメトリックと統計の情報をGTMが得ることができる。(big3d / iQuery利用。後述。)
  - このモニターによって、BIG-IP配下のリソースを追跡する最も効率的な方法を提供。

- External
  - BashまたはPerlなどの様々なスクリプト言語を使って、ヘルスモニターを作成することができる。("/usr/bin/monitors"にスクリプトを作成)
  - グラフィックユーザーインターフェイス(GUI)のモニターセクションの中で、モニター名とスクリプト名を選ぶことによって、Externalモニターを定義する。

EAV (External Application Verification) (Cont.)

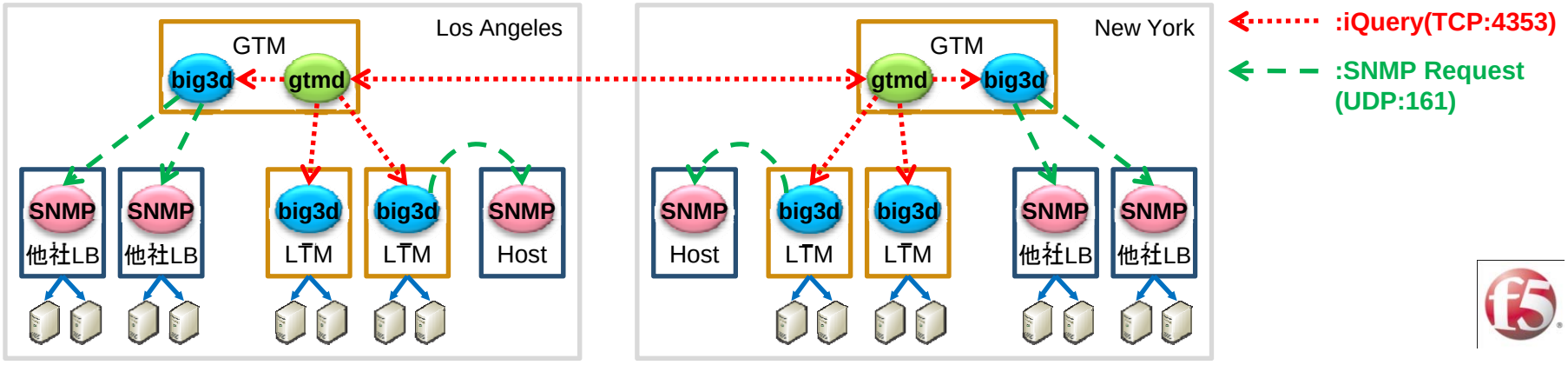
- FTP
  - 指定したファイルのダウンロードを試み、ファイルが取り出されるならば、チェックは成功。
  - ダウンロードされるファイルへのユーザーネーム、パスワード、およびフルパスを指定。
- IMAP
  - 指定したメールフォルダのオープンを試み、指定されたメールフォルダを開くことができるならば、チェックは成功。
  - ユーザーネームとパスワードを指定。
- その他
  - LDAP, MSSQL, NNTP, Oracle, POP3, RADIUS, Real Server, Scripted, SIP, SMTP, SNMP, SOAP, UDP, WAP, WMI, etc.

big3dによるパフォーマンスモニター

- BIG-IPモニタ
- SNMPモニタ

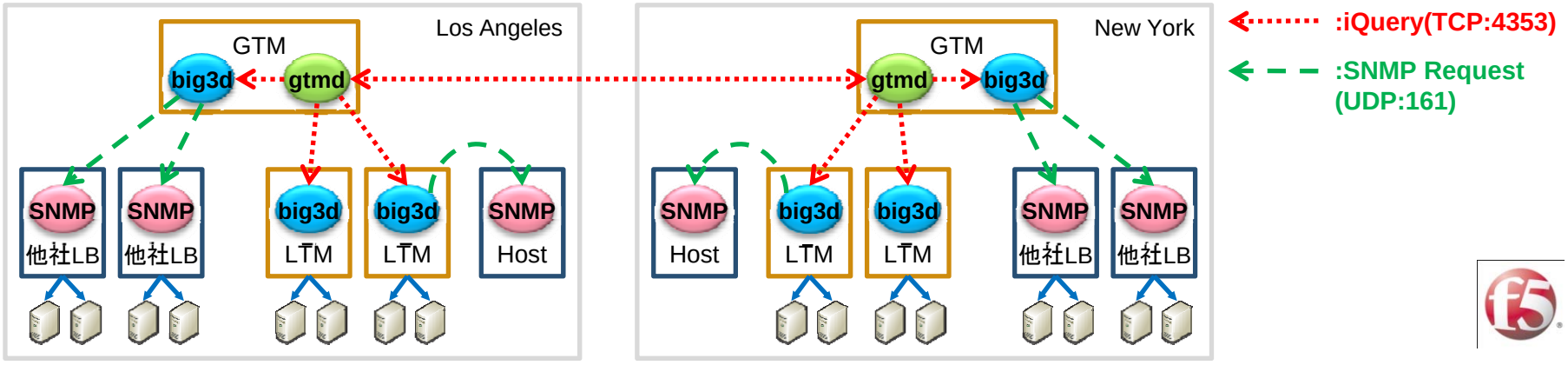
big3dの概要

- big3dエージェントは、全てのBIG-IPシステム上で動作する。
- big3dエージェントがGTMのためにパフォーマンス情報を収集し、GTMがロードバランスするServersのアベイラビリティを継続的にモニターする。
- big3dエージェントは、また、big3dエージェント自身と、接続してくるLocal DNS間のネットワークパスの完全性もモニターする。
- それぞれのbig3dエージェントは、その集めたデータを全てのGTMにブロードキャストし、GTMが最新情報を持って稼働できるようにする。
- big3dエージェントが、big3dを持たないServersに対して、SNMPによる情報収集を行う。
- gtmd~gtmd間及びgtmd~big3d間に使われる通信プロトコルが、iQueryである。



iQueryの概要

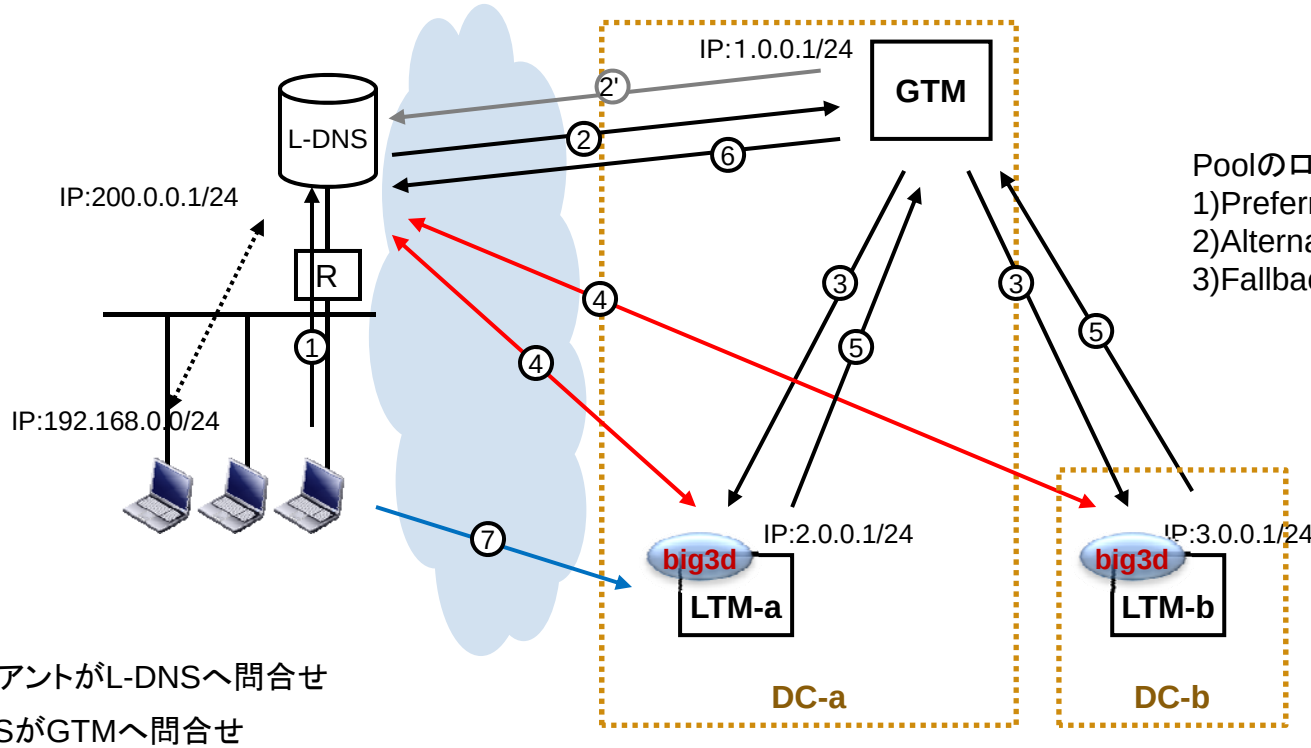
- iQueryプロトコルは、gzip圧縮とSSLを使って、各システム間で送られるXMLプロトコル。
- iQuery通信プロトコルによって、以下を行うことができる。
  - 同期グループ内にいる複数のGTMがコンフィグレーションを共有する
  - GTMが、プローブリクエストをbig3dエージェントに送り、ネットワークリソースのステータス情報を受け取る。
- BIG-IPシステム間でSSL証明書を交換しない場合、iQuery通信ができない。
- BIG-IPシステムは受信メッセージを受け取ったVLAN上にだけ、iQuery通信を送る。
- iQuery通信は、同じ同期グループ内だけで発生する。
- 各システム間でiQueryで送受信されたデータを見る場合には、iqdumpコマンドを使う。



big3dによる、パスデータの収集

- ネットワークパスのラウンドトリップタイム(RTT)
  - big3dエージェントが、「bid3dエージェントのデータセンター」と「DNSリクエストをしているクライアントLDNS」の間のネットワークパスのラウンドトリップタイムを計算する。
  - RTT or QoS ダイナミックロードバランシング時に利用
- ネットワークパスのパケットロス
  - big3dエージェントが、「bid3dエージェントのデータセンター」と「DNSリクエストをしているクライアントLDNS」の間ネットワークパスの非パケットロス(パケットコンプリーション)パーセンテージを計算する。
  - Completion or QoS ダイナミックロードバランシング時に利用
- ネットワークパスのルータホップ数
  - big3dエージェントが、「bid3dエージェントのデータセンター」と「DNSリクエストをしているクライアントLDNS」の間中間システム数(ルータホップ数)を計算する。
  - Hops or QoS ダイナミックロードバランシング時に利用

[参考]RTTによる近隣DCへの誘導イメージ

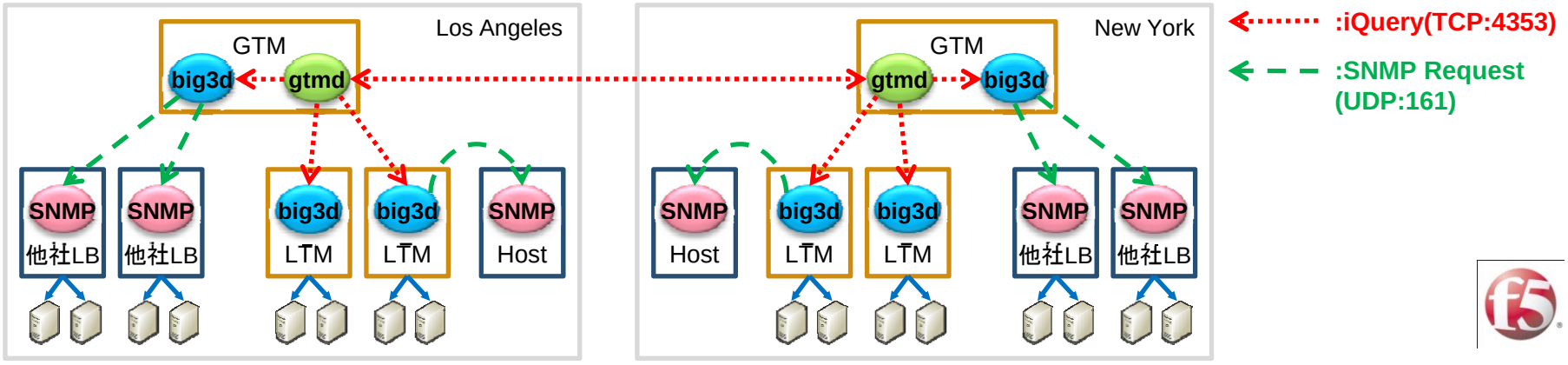


- (1)クライアントがL-DNSへ問合せ
- (2)L-DNSがGTMへ問合せ
- (2') 最初は、GTMのAlternateロードバランシングにて、DNSリプライ
- (3)GTMは、各DCのLTM(LTM-a,LTM-b)のbig3dエージェントへ、L-DNSのIPアドレス宛へのRTTを測定するよう指示
- (4)DCのLTM(LTM-a,LTM-b)のbig3dエージェントが、L-DNSへのRTTを測定
- (5)DCのLTM(LTM-a,LTM-b)のbig3dエージェントが、RTT値をGTMへ連絡
- (6)GTMは、LTM-aとLTM-bのRTT値を比較して、RTTの短いほうをIPリストのトップに書き換えて、L-DNSへ返答
  - ここでは、LTM-aのRTT値のほうが短いと仮定してLTM-aのVSを返答
- (7)Clientは、LTM-aのVIPへの通信を行う

big3dによる、サーバ性能値の収集

- サーバのパフォーマンス
  - big3dエージェントは、BIG-IPシステムやSNMPが有効なホストの、サーバメトリック値(Packets Rate等)を測定して、GTMに伝える。
  - Packet Rate / Kbps / Least Connections / QoSダイナミックロードバランシング時に利用

- Virtual Serverのアベイラビリティとパフォーマンス
  - big3dエージェントは、Virtual Serverがコネクションを受け取れるかどうかを確認するためにクエリし、ロードバランシングができるVirtual Serverだけを使う。
  - big3dエージェントは、BIG-IPシステムまたはSNMPが有効なホストに定義されたVirtual Serverへの現在のコネクション数を測定する。
  - Least Connections / VS Capacity ダイナミックロードバランシング時に利用



GTMのiRules

iRules

- WideIPに対して適用
  - LTMでVSに適用されるのと同じ
- Poolよりも優先して処理
  - LTMでもVSでpoolよりもiRuleが優先される
- iRule基本要素
  - Event宣言
  - オペレーター
  - コマンド

DNS Event Example

- WideIP名毎にPoolを選択する例

```
rule DNSPool {
  when DNS_REQUEST {
     if { [DNS::rrname] ends_with ".org" }
           { pool org_pool }
     elseif { [DNS::rrname] ends_with ".com" }
           { pool com_pool }
  }
}
```

IP ジオ・ロケーション

IP ジオロケーション・データベース

QUOVA

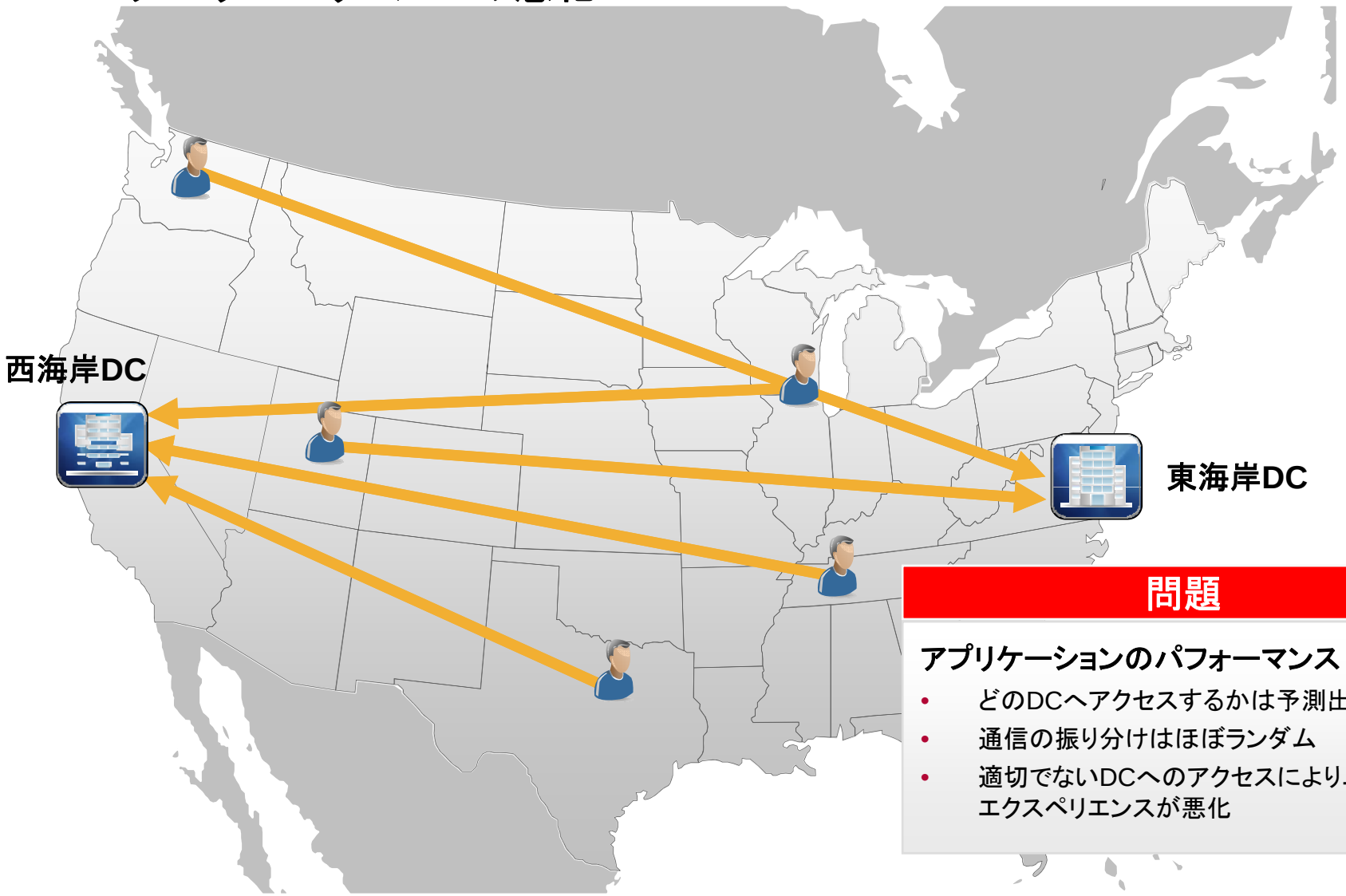
- バージョン10.1より組み込まれた、信頼度の高いIPロケーションデータ
- Quova社より提供される、地域情報データベース
- IPアドレスからクライアントの物理的な位置情報を判別

- より最適なDCサイトへリクエストをルーティング（GTM)
- iRulesによりユーザのアクセスをロケーションによりコントロール

- 使用例:
  - アクセスの最適化 ： ユーザを最適なDCへ誘導
  - ストリーミングメディアをコントロール
    - ー放送権、著作権などによる制限
  - 貿易制限の施行
  - 地域情報広告配信

ユーザを適切なサイトへ誘導

ユーザ エクスペリエンスの悪化



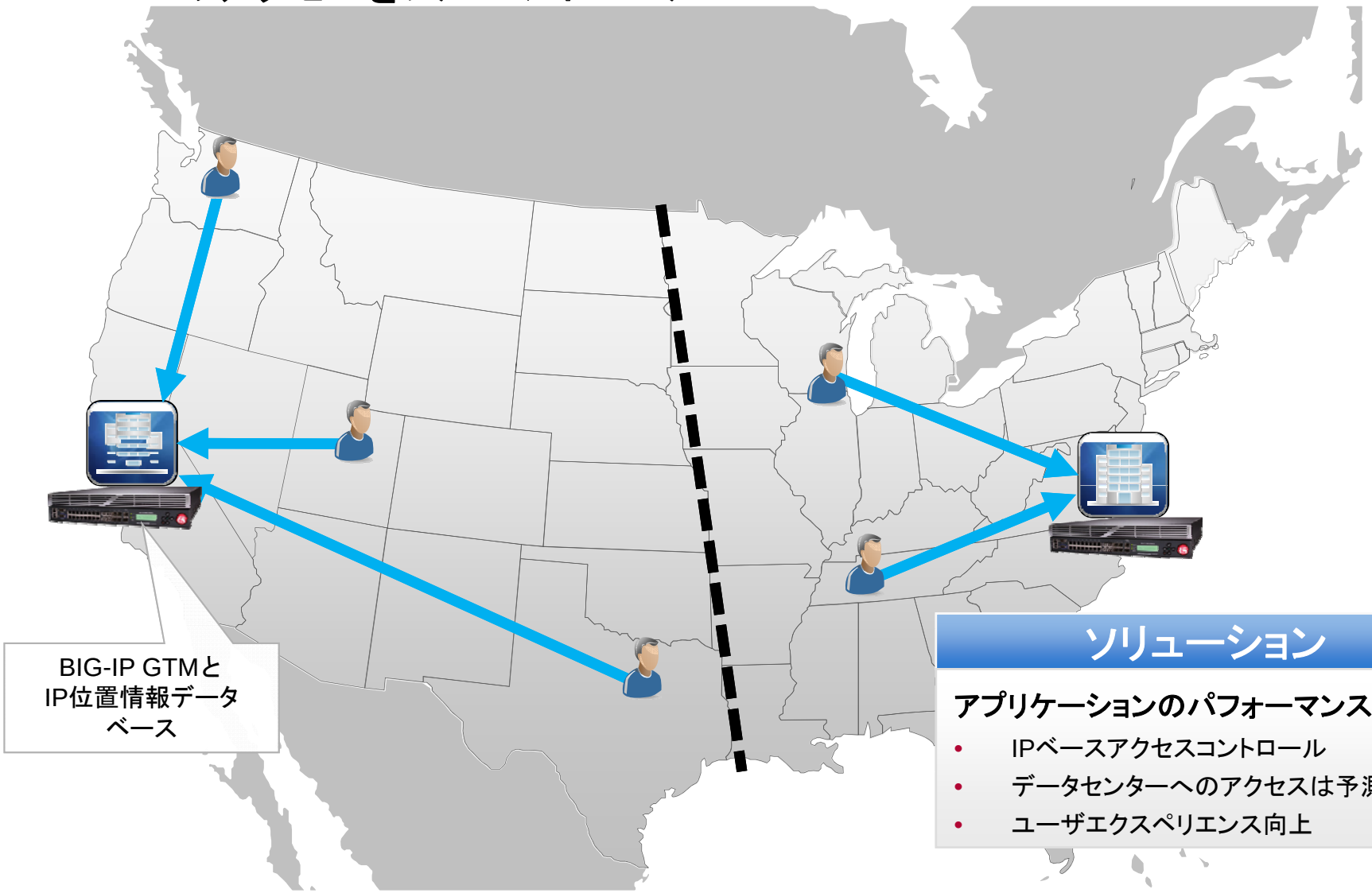
問題

アプリケーションのパフォーマンス

- どのDCへアクセスするかは予測出来ない
- 通信の振り分けはほぼランダム
- 適切でないDCへのアクセスによりユーザエクスペリエンスが悪化

ユーザを適切なサイトへ誘導

DCへのアクセスをフル コントロール



BIG-IP GTMと
IP位置情報データ
ベース

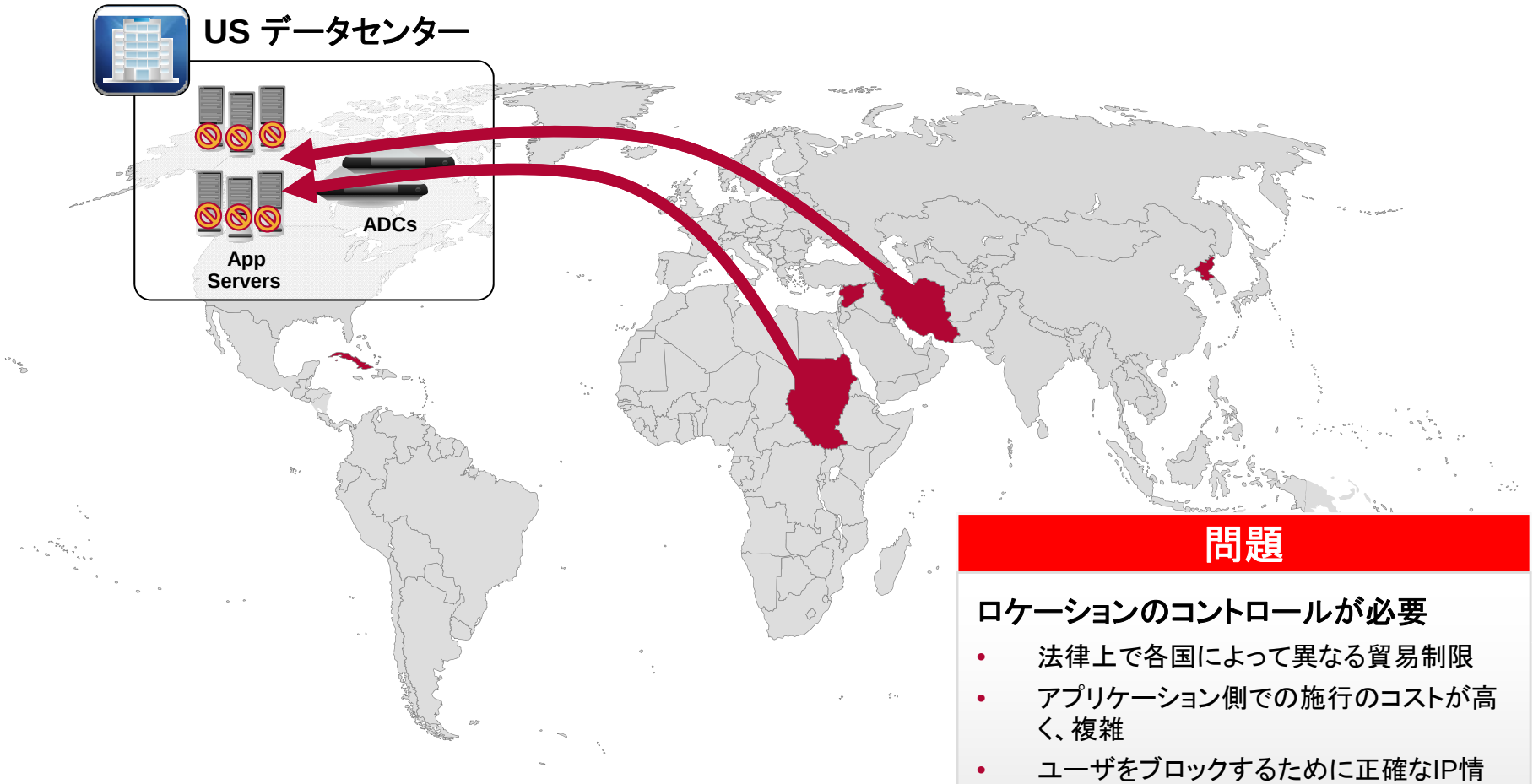
ソリューション

アプリケーションのパフォーマンス向上

- IPベースアクセスコントロール
- データセンターへのアクセスは予測可能
- ユーザエクスペリエンス向上

貿易制限の施行

アプリケーション側での施行は困難



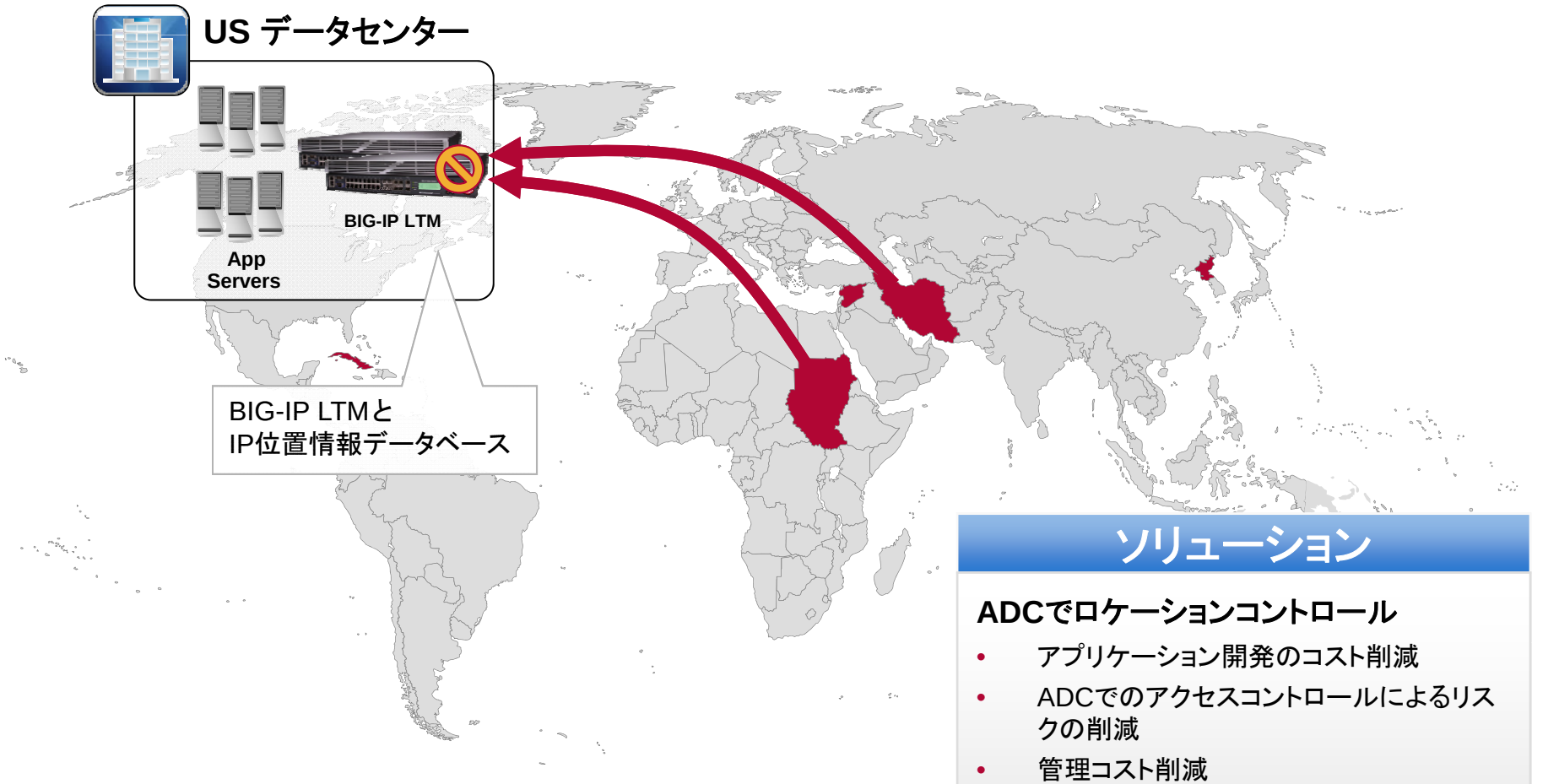
問題

ロケーションのコントロールが必要

- 法律上で各国によって異なる貿易制限
- アプリケーション側での施行のコストが高く、複雑
- ユーザをブロックするために正確なIP情報が必要

貿易制限の施行

シンプルで、正確なコントロール



ソリューション

ADCでロケーションコントロール

- アプリケーション開発のコスト削減
- ADCでのアクセスコントロールによるリスクの削減
- 管理コスト削減
- ネットワークの簡素化

DNSSEC

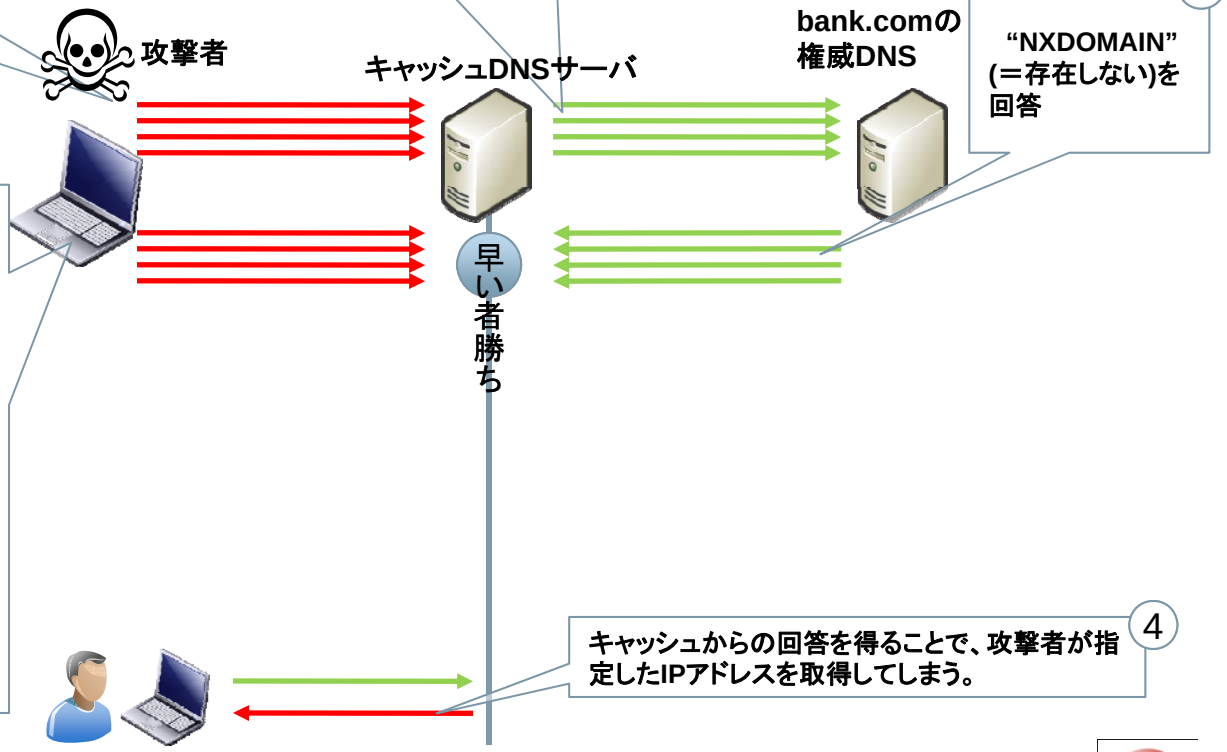
DNSキャッシュポイズニング攻撃
~カミンスキー攻撃~

※bank.comは存在するが、01.bank.comは存在しない前提

1
01.bank.com
02.bank.com
- - - -
0n.bank.com
実在しないFQDNを指定して、大量のクエリを生成する。

2
キャッシュサーバは、キャッシュにない情報なので、権威サーバにクエリを送信する。
このとき、クエリ毎に異なる、「トランザクションID(16bit:65536通り)」を付与する。

3
“NXDOMAIN”(＝存在しない)を回答



3’
bank.comの権威DNSのIPアドレスを詐称＆
「トランザクションID」をランダム生成し、
③のDNSリプライを偽装。 さらに、そのリプライに、
「ADDITIONAL SECTION」を含ませることができる。

例:
ANSWER SECTION
01.bank.com 123 IN A 誘導したいIPアドレス
AUTHORITY SECTION
権威DNS 123 IN NS 詐称ドメイン(1)
権威DNS 123 IN NS 詐称ドメイン(2)
:
ADDITIONAL SECTION
詐称ドメイン(1) 123 IN A 誘導したいIPアドレス
詐称ドメイン(2) 123 IN A 誘導したいIPアドレス
:

4
キャッシュからの回答を得ることで、攻撃者が指定したIPアドレスを取得してしまう。

DNSキャッシュポイズニング攻撃　(Cont.)
~カミンスキー攻撃~

- 正しいDNSリプライかどうかの判断
  - キャッシュDNSサーバは、DNSリプライの偽装を防止するために、16ビットのランダムなトランザクションIDを付与して、権威DNSに問合せる(DNSクエリ)。
    そして、以下2つを照合することで、正規の回答であることを確認する。
    - 送信したDNSクエリのトランザクションIDとDNSリプライのそれが一致すること
    - 送信したDNSクエリの送信元IPアドレス＆ポート宛への応答であること

- 攻撃方法
  - 攻撃者はこの穴をつく。権威DNSのIPアドレスを詐称し、想定できるDNSクエリのポート番号とトランザクションIDをランダムに生成。それらの値で、総当たり(ブルートフォース)で虚偽のDNSリプライを仕掛ける。
  - 図中①で行うDNSクエリに、”存在しないFQDN”を使うことで、総当たり攻撃試行チャンスをほぼ無限に増やし、成功確率を圧倒的に高くできる。
  - さらに、「ADDITIONAL SECTION」を含ませることで、任意のドメイン/FQDNの組合せをキャッシュさせることができる。
    「ADDITIONAL SECTION」は自由に設定することが可能であるため、さらに広範なドメイン/FQDNの詐称が可能となる。

DNSSECの動作概要

※DNSSEC対応

BIG-IP GTM

1
01.bank.com
02.bank.com
- - - -
0n.bank.com
実在しないFQDNを指定して、大量のクエリを生成する。

2
キャッシュサーバは、キャッシュにない情報なので、権威サーバにクエリを送信する。
このとき、クエリ毎に異なる、「トランザクションID(16bit:65536通り)」を付与する。

3 4 5
③ハッシュ関数で、DNSリプライのハッシュ値を計算

④そのハッシュ値を、権威DNSの秘密鍵で暗号化＝これが電子署名

⑤平文のDNSリプライに電子署名を添付して、キャッシュDNSサーバへ返答

攻撃者

キャッシュDNSサーバ

bank.comの権威DNS

DNS リプライ

3
ハッシュ値

bank.com 権威DNSの 秘密鍵

4
ハッシュ値

5
DNS リプライ

ハッシュ値

6 7 8 9
⑥ハッシュ関数で、DNSリプライのハッシュ値を計算

⑦電子署名を権威DNSの公開鍵で複合化

⑧これら2つのハッシュ値を比較

⑨比較の結果が同じならキャッシュ

ハッシュ値

bank.com 権威DNSの 公開鍵

7
ハッシュ値

DNS リプライ

6
ハッシュ値

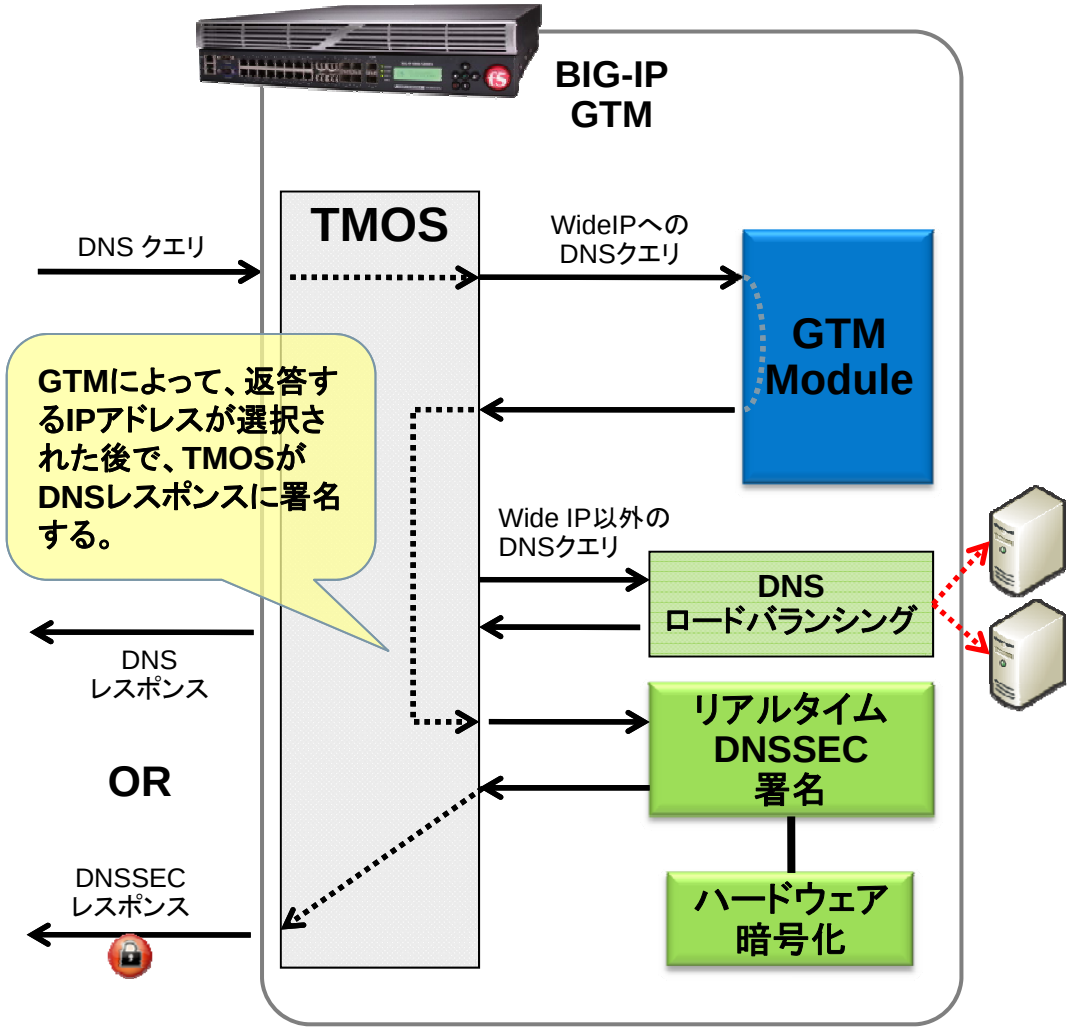
8
比較

9
キャッシュ

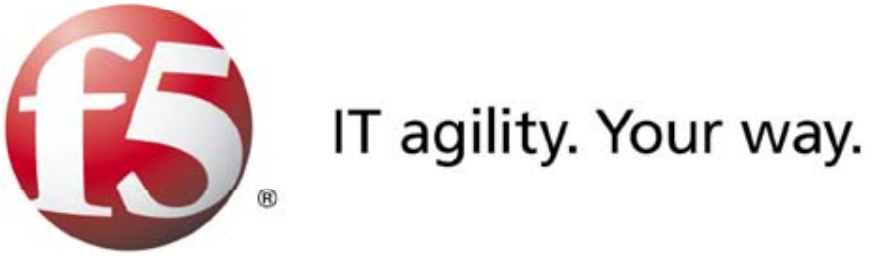
10

10 署名を持たないDNSリプライはキャッシュしない。

リアルタイムDNSSEC



- BIG-IP GTM DNSSEC機能は、DNSレスポンスにリアルタイムにサインして、既存環境に素早く、簡単にDNSSECを展開する方法を提供。
- リアルタイム署名は、ユーザが地球上の様々なロケーションからリクエストが発生する環境においては重要である。
- 静的DNSのDNSSECを提供することは、BINDを使えば、比較的簡単である。
- しかし、特にクラウド展開においては、GSLBタイプの、動的なDNSのDNSSECを提供することは、かなり難しい。
- F5は、GSLB環境で正しく機能する、真のDNSSECソリューションを持つ唯一のGSLBプロバイダーである。
- 他社は、考え得るDNSレスポンス全てに対して、事前に署名するシステムを提案するのに対して、F5は、これが実現可能なアプローチではないと判断した。



本資料に関するご意見、ご要望は、下記のメールアドレス(受信専用)にお願い致します。

F5J-Tech_Depot/atmark/f5.com

※迷惑メール防止のため、「@」を「/atmark/」 と表記しています。