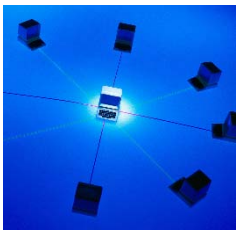
JPRS トピックス＆コラム



■DNSのさらなる信頼性向上のために
～IP Anycast技術とDNS～

ルートサーバーやTLDサーバーなど、特に重要な権威DNSサーバーを中心に導入されている「IP Anycast」技術について、その概要と特徴、DNSへの導入効果を解説します。

■インターネットにおける通信の仕組み

IP Anycast について解説する前に、インターネットにおける通信の仕組みについて、簡単におさらいしておきましょう。

インターネットでは通信相手をドメイン名で指定します。指定されたドメイン名は DNS によって対応する IP アドレスに変換され、実際の通信では IP アドレスにより、通信相手が指定されます（図1）。

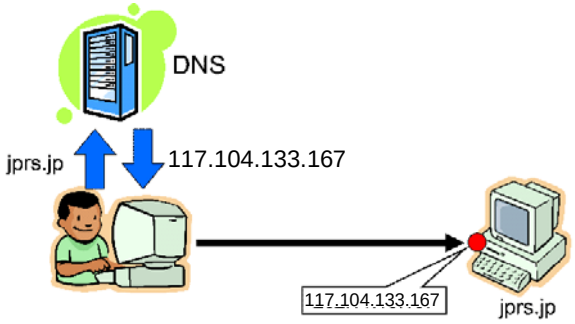


図1: ドメイン名から IP アドレスへの変換

インターネットに接続しているすべての機器には、それぞれ個別の IP アドレスが割り当てられます。そのため、通信相手の IP アドレスを送信先として指定することにより、その相手との間で一対一の通信を行うことができます（図2）。

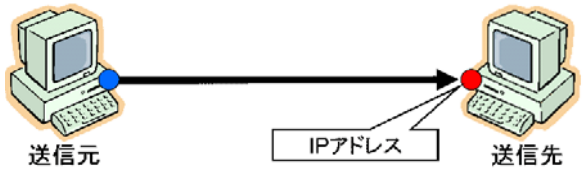


図2: IP アドレスを指定した一対一通信

このような通信方式はインターネットにおいて一般的なものであり、ユニキャスト（Unicast）と呼ばれています。ユニキャストの「ユニ」は「単一の」という意味の接頭辞で、ユニキャストでは送信元と送信先の機器は、常に一対一で対応付けられることになります。

■IP Anycast

これに対し IP Anycast では、一つの IP アドレスがインターネット上の複数の機器に同時に割り当てられ、共有されます。これらの機器は IP Anycast を構成するノード（node）と呼ばれ、送信元から送られたデータはそれぞれのノードのうちのいずれか一つ（any）に到達し、処理されます（図3）。

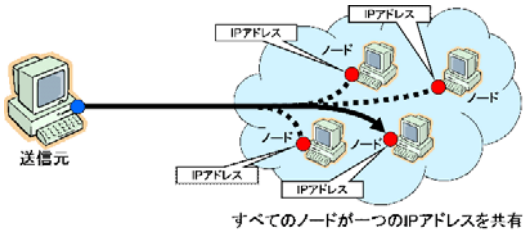


図3: IP Anycast による通信

IP Anycast を構成するノードには、それぞれの機器に個別に割り当てられる IP アドレスとは別に、IP Anycast で使用するための IP アドレス（共有アドレス）が追加で割り当てられます。そして、すべてのノードにおいて、当該の共有アドレスで同じサービスを動作させることにより、どのノードが処理をしても同じサービスが提供されるように設定されます。

■IP Anycast の特徴

IP Anycast では、同じ IP アドレスを持つ複数の機器（ノード）がインターネットに同時に接続された状態になります。そのため、通常の通信方式（ユニキャスト）にはない、次のような特徴を備えています。

①接続条件によりデータが到達する機器が異なる

ユニキャストでは送信元や送信先の接続条件、例えば利用しているプロバイダーや利用している地域などが異なっていても、データが到達する機器は常に一定です。しかし IP Anycast の場合、接続条件によりデータが到達するノードが異なってきます。

②送信元が同一であってもデータが到達する機器が異なる場合がある

インターネットにおける通信の状況は常に変化する可能性があるため、同じ発信元から送信されたデータであっても、状況の変化により別のノードに到達する場合があります。

■IP Anycast の制限

このように IP Anycast では、データが到達するノードが接続条件により異なり、また通信の状況の変化により、データが到達するノードが変化する可能性があります。このような変化は通信中であっても起こり得るため、IP Anycast を実際のインターネットに適用する場合、その特性をよく理解した上で導入を検討する必要があります。

例えば、インターネット上の通信で広く使われている TCP による通信では、事前に「スリーウェイ・ハンドシェイク」という手順により相手との間の接続を確立します。この手順では、送信元から送信先に二つのパケット（SYN と ACK）が送られますが、もしこの間に接続状況が変化してそれぞれのパケットが別のノードに到達してしまった場合、相手側との接続が確立できなくなってしまいます（図4）。

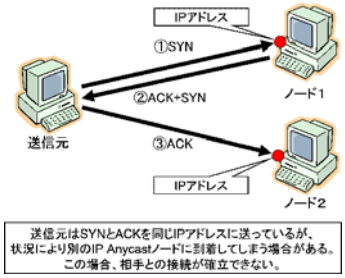


図4: スリーウェイ・ハンドシェイクの失敗

また、インターネット上の通信では送信元から送信先に送るデータサイズが大きい場合、経路の途中でデータが分割される場合があります。このような場合に分割された断片（フラグメント）が別のノードに到達してしまうと、相手側との通信が確立できなくなってしまいます。

■IP Anycast と DNS

DNS では主な通信プロトコルに UDP を使用しているため通信開始時の接続の確立が必要なく、基本的に一度のやり取りで通信が完結します。かつ、一般的な DNS の問い合わせパケットのサイズは 512 バイト以下であり、現在のインターネットでは経路途中におけるデータの分割は発生しません。

DNS はこれらの特徴により IP Anycast が適用可能なプロトコルの一つであると考えられ、2002 年 10 月に発生したルートサーバーへの大規模な DDoS 攻撃をきっかけとして、ルートサーバーや TLD サーバーなどの特に重要な DNS サーバーを中心に、IP Anycast の導入が行われてきました。

■IP Anycast により得られる効果

DNS サーバーに IP Anycast を導入することにより、以下に示す効果が期待できます。

①負荷分散・冗長化

複数のサーバーや複数の拠点にリクエストを分散させることにより、負荷分散や冗長化を実現できます。

②DNS 平均応答時間の短縮

ノードを地域ごとに分散配置することで、DNS サーバーの平均応答時間を短縮させることができます。

③DoS 攻撃の局所化

1カ所からの DoS 攻撃はネットワーク的に一番近いノードに局所化され、他のノードは被害を受けません。

④DDoS 攻撃の効果抑制

DDoS 攻撃は複数のノードに分割されるため、効果を抑制することができます。

このように、IP Anycast を DNS に導入することで DNS サーバーの性能や耐障害性を向上させ、結果として DNS 全体の信頼性を向上させることができます。

■IP Anycast 導入の現状

IP Anycast は 13 系列あるルートサーバーのうち、B-Root を除く 12 系列に導入されており、合計 450 以上のノードが世界中で稼動しています。

JP DNS では 7 系列あるサーバーのうち a.dns.jp、c.dns.jp、d.dns.jp、e.dns.jp の 4 系列に IP Anycast を導入し、信頼性の向上を図っています。

