# パブリッククラウドの本格利用に伴うネットワークの課題と対策

豊田　太司
(株)中電シーティーアイ

【概要】
企業ネットワークが変革の時期を迎えている。
SaaS（Software as a Service）に代表されるパブリッククラウドサービスの利用拡大に伴い、イントラネット内で処理されていたトラフィックがインターネットへ流出している。このネットワークの変化がもたらす課題はいくつかあり、既存ネットワークに何も対策を行わない状態でパブリッククラウドの利用を始めると、基幹システムが長時間停止する、レスポンスが非常に悪くなる等の思わぬトラブルにつながることがある。
本論文では、インターネット上のパブリッククラウドを本格的に利用する際に、多数の企業が直面する課題について説明すると共に、その対応例について解説する。

キーワード（パブリッククラウド、インターネット、ADC、キャパシティ管理）

## １．はじめに

基幹システムをパブリッククラウドへ移行する企業が飛躍的に増えており、イントラネット内で処理されていたトラフィックがインターネットへ流出している。基幹システムをパブリッククラウドへ移行する場合、インターネットという外部ネットワークの集合体がシステムの通信経路の一部となるため、インターネットもシステムの一要素と捉えなければならない。その場合、対応しなければならないネットワークの課題が大きく分けて２つあり、何も対策を行わないまま既存ネットワーク上でパブリッククラウドを利用すると、基幹システムが長時間停止する、基幹システムのレスポンスが非常に悪くなり業務に支障をきたす等の想定外のトラブルにつながる可能性がある。

最初に考えなければならない課題としては、インターネット接続の可用性確保である。2017 年 8 月に起こった、米 Google 社の作業ミスによるインターネットの通信障害を始め、インターネット全体に及ぶネットワーク障害は定常的に発生している。インターネットは自社でのコントロールが不可能な箇所も多く、とりわけ万能なネットワークではない。それゆえに、自社で対応出来る範囲で可用性を高める対策をとらなければならない。

もう一つの課題として考えなければならないのは、インターネットへ流出する大量トラフィックへの対応である。この課題に対して何も対策を行わない状態で、パブリッククラウドの本格利用を開始すると、当該システムのみならず、他の業務システムへ影響を与えてしまう結果となる。こちらについても、現状のネットワークトポロジーにとらわれることなく、事前に対策を講じる必要がある。

本論文では、この２つの課題について、内容を説明するとともに、筆者が考える対応策について解説する。

## ２．インターネットを利用する際の課題

前章で触れたパブリッククラウドを利用する際に考慮が必要となる、「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」の２つの課題について、それぞれ内容を説明する。

### ２．１　インターネット接続の可用性確保

基幹システムの通信経路としてインターネットを利用する以上、インターネット接続の可用性確保は誰もが考える課題である。繰り返しとなるが、インターネットを始めとするネットワークは万能ではない。インターネットは ISP（インターネットサービスプロバイダー）が構築するネットワークの集合体であり、個々のネットワークは一企業が設計し、運営するネットワークシステムである以上、設計ミス、作業ミス等によるネットワークの停止は決してゼロにはならない。この状況を踏まえると、インターネットを通信経路の一部として利用する、ミッションクリティカルなシステムは、インターネット接続を担う ISP が長時間停止することを想定し、事前に対策を講じておく必要がある。

2017 年 8 月 25 日に、米 Google 社の作業ミスにより、インターネット全体を巻き込んだ通信障害が発生し、とりわけ日本国内の ISP は大きな影響を受けた。日本の大手プロバイダ（OCN、KDDI）でもネットワーク障害が発生し、JR 東日本、楽天証券などが影響を受けるなど、全国規模のネットワークトラブルとなった。（表 1 参照）[1]

**表１　2017 年 8 月 25 日に発生した主なトラブルの一覧**

| Web サイト | 発生時間 | 障害内容 |
|---|---|---|
| JR 東日本 | 12 時 30 分頃 | モバイル Suica、Web サイトにつながりにくい状態 |
| 楽天証券 | 12 時 30 分頃 | ログインしづらい状況 |
| 三重県 | 午後から | 入札サイトが利用しづらい状況 |
| 徳島市 | 12 時 30 分頃 | Web サイトが閲覧できない事象 |
| GMO クリック証券 | 12 時 30 分頃 | ログインしづらい状況 |
| SB 証券 | 不明 | 断続的にアクセスしづらい状況 |
| じぶん銀行 | 12 時 30 分頃 | ログインできない事象 |
| ジャパネット銀行 | 午後から | ログインしづらい状況 |

翌日（2017 年 8 月 26 日）、米 Google 社が作業ミスを認めて謝罪を行ったが、作業ミスの詳細な内容については公表されていない。このように、一企業の作業ミスが、日本全国規模のネットワーク障害につながってしまうこともある。また、世界規模で見ても、インターネット上においてこのような通信障害が発生している頻度は決して少なくない。[2]

このような状況のインターネットに対して、インターネット接続の可用性を高める対策を取ることは必須であり、自社で対応できる範囲で対策することが重要である。

## ２．２　インターネット向け大量トラフィックへの対応

もう一つの課題であるインターネット向け大量トラフィックへの対応は、パブリッククラウドを本格的に利用することで新たに発生する課題であり、対応できている企業は少ないと思われる。

これまでの一般的なインターネット接続の形態は、インターネットとの接続ポイントを１カ所に集中させる形が主流である。この形態を取ることでインターネット向けトラフィックの管理が容易になる。また、ファイアウォール、プロキシサーバ、その他情報漏洩対策等のセキュリティ機器といった、インターネット接続時に経由する機器を１カ所に集約することで、初期導入コスト、および運用コストの削減にもつながる。この従来の１極集中型のインターネット接続構成を変えない状態で大量のトラフィックがインターネットへ流出した場合、想定外の問題が発生する恐れがある。

真っ先に考えられる問題としては、トラフィック量の増加に伴うレスポンスの悪化である。この問題の原因は、インターネット接続時に経由する機器（プロキシサーバ、ファイアウォールなど)、もしくはインターネット接続回線のいずれかが性能限界となっていることが多く、既存システムも含めて影響を受けてしまう。(図１参照)

他に考えられる問題として、インターネット向けセッション数の増加が、同じ経路を利用している既存システムへ悪影響を及ぼすことがある。こちらは、セッション数が増えるにつれて、徐々に業務システムのレスポンスが悪化していき、利用者からの苦情によって気づくといったケースが多い。また、対処が必要となった場合、TCP/IP 関連のパラメータの一部に原因が潜んでいるなど、調査および対応に時間がかかることも多い。

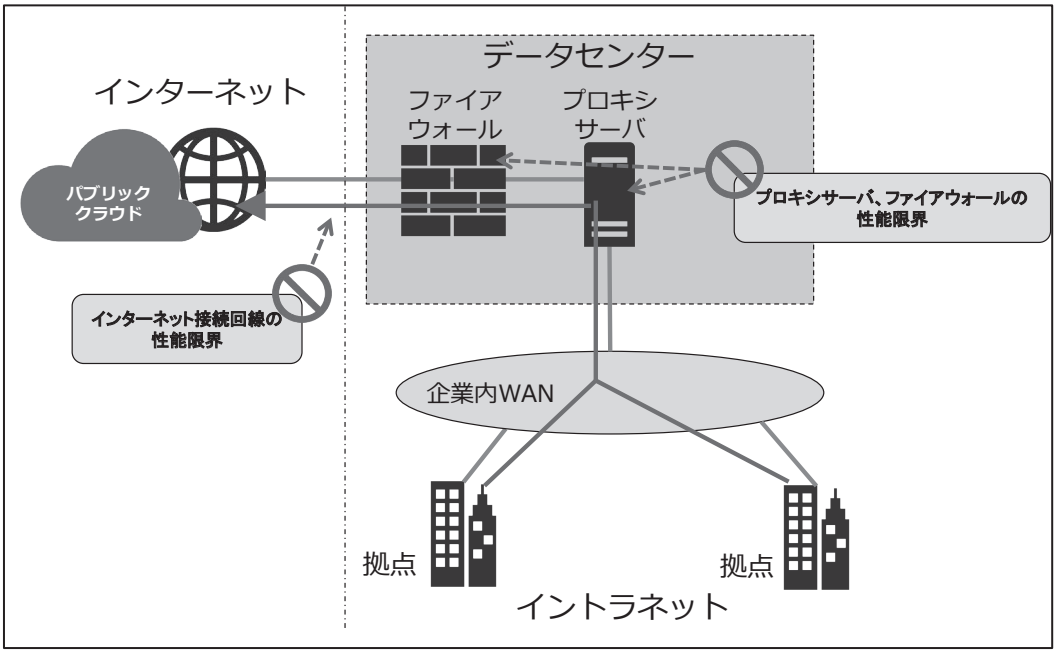


**図１　従来の１極集中型のインターネット接続**

これらの問題を放置したまま、パブリッククラウドの本格利用を進めてしまうと、遅かれ早かれ、前述した問題に直面し、右往左往することになる。そのような事態になる前に、増加するトラフィック量、セッション数の試算を行った上で、対策を講じる必要がある。

## ３．課題への対応方法

前章で述べた「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」の２つの課題に対する対応方法について表にまとめる。（表 2 参照）

どちらの課題についても対応の流れとしては、「インターネット回線の冗長化」、「アプリケーションごとの経路制御」、「インターネット接続回線のキャパシティ管理」という順序で対応を行うことになる。

これらの３つの対応方法について、事項から順に説明する。

**表 2　対応方法と課題に対する効果**

| No | 対応方法 | 課題に対する効果 | | 具体的な対策 |
|---|---|---|---|---|
| | | インターネット接続の可用性確保 | インターネット向け大量トラフィックへの対応 | |
| 1 | インターネット接続回線の冗長化 | インターネット接続の可用性向上 | 負荷分散によるボトルネックの緩和 | 信頼できる複数の ISP へ接続する |
| 2 | アプリケーションごとの経路制御 | トラブル発生時の影響範囲を局所化 | トラフィックの分散によるボトルネック箇所のコントロール | ADC 等の機器を用いて、アプリケーションごとに経由機器、接続回線をコントロールする |
| 3 | インターネット接続回線のキャパシティ管理 | プロアクティブな対応による障害の未然防止 | 性能データに基づく適切な機器増強判断 | アプリケーションごとのトラフィック量、セッション数を定期的に取得・分析する |

### ３．１　インターネット接続回線の冗長化

対応済みの企業が多い対策となるが、インターネット回線を複数準備し、回線の冗長化を行うことが必要となる。こうすることで、トラフィックの負荷分散が可能となり、1 カ所にトラフィックが集中することを回避できる。インターネット回線を選択する際は、接続する ISP や接続する地域を分けることで、さらに効果が大きくなる。ただし、インターネット回線の冗長化を行うためには、何らかの手段でインターネット接続回線の振り分けを行う必要があり、ネットワーク設計が複雑になる。それが起因して別のトラブルにつながるといったデメリットもあるため、できるだけ設計をシンプルにすることも重要になる。

また、接続する ISP を決める際の判断材料の一つとしては、２．１項で述べた通信障害のような、想定外の事象を考慮した機器構成となっているかを、ISP の担当へ確認すればよい。具体的には、「インターネット全体を巻き込んだ通信障害の発生に備え、御社ではどのような対策を行っていますか？」という質問を ISP の担当へ投げかけ、その回答の納得度を判断材料にするという方法も考えられる。

### ３．２　アプリケーションごとの経路制御

アプリケーションごとに経由させる機器、およびインターネット接続回線を分ける対策を行うことも重要になる。この対策を行うためには、トラフィックの可視化、すなわちアプリケーションごとにトラフィックの流れを把握する作業を行った上で、ADC（Application Delivery Controller）等の機器を用いて、アプリケーション層のデータによって、通信経路を決定するといった対応が必要となる。トラフィック種別ごとにインターネット接続経路をコントロールすることで、インターネット向けに大量トラフィックを発生させる通信については、通常の通信が経由する機器をバイパスさせ、インターネット接続時にボトルネックとなるポイントを減らすと共に、トラフィックの集中によるレスポンス低下が発生しない構成とする。（図 2 参照）

この対策に加えて、トラフィックの帯域制御を行うことも有効である。専用の機器が必要となるが、回線を流れるトラフィック種別、およびその必要帯域をあらかじめ把握していれば、最優先すべき業務トラフィックに必要帯域を割り当てることで、最も優先させる業務のトラフィックを保証するといった対応も取れる。

これらの対策は、継続的に機能していることが重要である。帯域制御の設定について言えば、対象のシステムに仕様変更が入り、必要帯域の増減があった場合は、変更内容に合わせた設定修正が必要になる。せっかく設定した帯域制御の設定も、システムが撤去されているにもかかわらず、帯域制御の設定が残っている場合などは、ただ無駄に帯域を確保しているだけの設定である。そのようなことにならないように、定期的な棚卸、設定の見直しが重要となる。

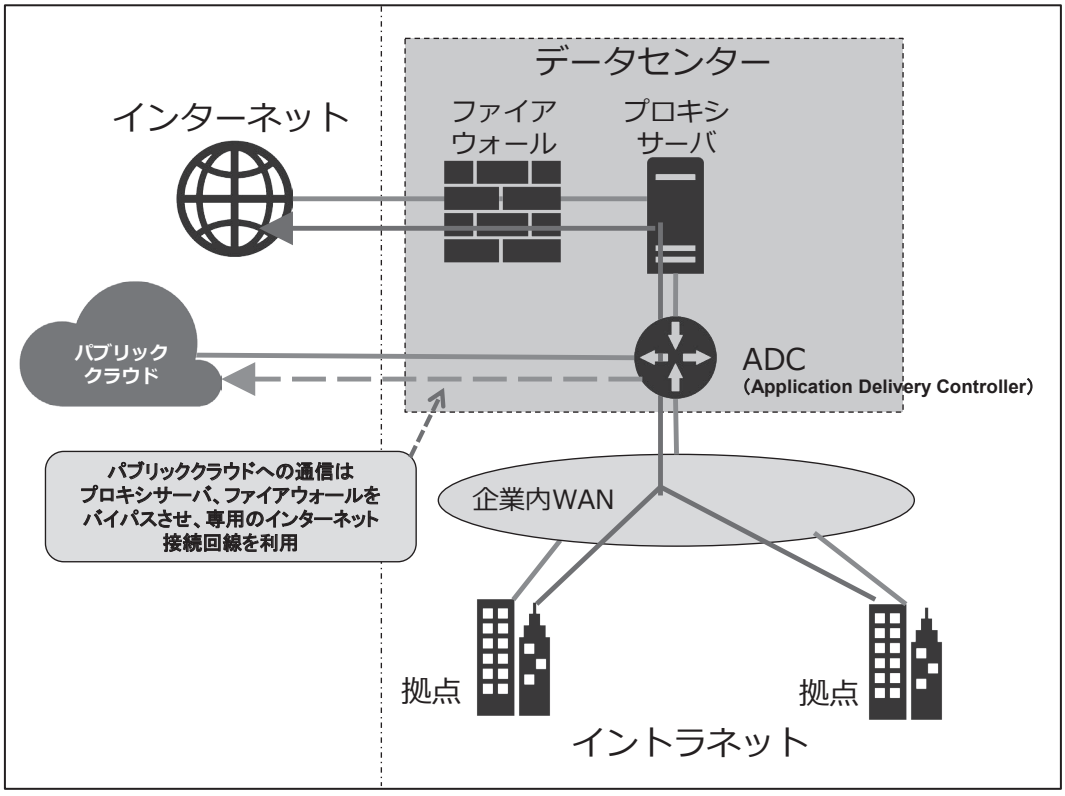


図 2　ADC を用いたトラフィックコントロール

### ３．３　インターネット接続回線のキャパシティ管理

ネットワーク性能データ（トラフィック量、セッション数など）を長期的に記録し、プロアクティブな対応を取ることによる障害の未然防止、およびネットワーク性能データに基づく適切な機器増強判断を行うことも重要である。

どのシステムが、どこの回線を、どの程度利用しているかを把握し、トラフィックを可視化することが最終的な目標となるが、そこまでの対応を短期間で行うことは困難である。最初のステップとしては、既存のネットワーク機器で取得できる MIB（Management Information Base）情報の範囲で、ネットワーク性能データを定期的に取得し、過去のデータを調査できるようにしておくことができれば十分である。

最近のネットワーク機器であれば、通信する TCP ポート番号ごとに、ネットワーク性能データを取得できる機器もあるため、該当するネットワーク機器の MIB 情報を調査し、既存の性能管理システムに登録することで、即座に対応することが可能である。

定常的にネットワーク性能データを収集することで、ベースラインとなる平常時の状態を数値で把握することができる。また、大量に増えるトラフィック量、セッション数を踏まえ、定期的なデータの確認を行い、必要であれば機器の増強などの対応を取ればよい。

本章では、「インターネット接続の可用性確保」、「インターネットへ流出する大量トラフィックへの対応」という２つ課題に対して、「インターネット接続回線の可用性確保」、「アプリケーションごとの経路制御」、「インターネット接続回線のキャパシティ管理」という３つの対策を順に説明してきた。これらの一連の対策は、一度対応したら終わりではなく、定期的に対策内容の評価、見直しを行うことも重要となる。

## ４．まとめ

本論文では、パブリッククラウドの本格利用を開始する際に考慮が必要となるネットワークの課題、およびその対応方法について解説を行ってきた。

パブリッククラウドの利用拡大に伴い、企業ネットワーク設計を根本から見直す時期に来ているが、対応出来ている企業は少ない。これは既存システムへ影響を与えないことを最優先に考え、10 年以上も前に設計したネットワークトポロジーをなるべく維持し、企業ネットワークの根本的な見直しを先延ばしにしてきた結果である。

しかし、トラフィックの流れが、大きく変わろうとしている今、企業ネットワークを根本的に見直す以外に、利用者全てが幸せになる選択肢は見つからない。ネットワークのトポロジーを見直すと、既存システムへ大きな影響を与える結果につながることがあるため、足踏み状態になりがちであるが、長期的なシステム導入計画を考慮した移行設計を行うことで、システム側への影響を最小限にすることはできる。この機会をチャンスと捉え、一歩を踏み出すことにより、利用者満足度の高いネットワーク環境の構築を目指すべきである。

これまでのネットワークエンジニアは、共通インフラのエンジニアとしてサポート役に徹し、表舞台に立つことは少なかったように思うが、現在のシステムはネットワークなしでは考えられず、システムの構築プロジェクトにおいて重要な役割を果たすことも少なくない。AI（人工知能）やビッグデータといった最新技術の活用についても、ネットワークの信頼性に依存するところが

大きいと思われ、ネットワークエンジニアの仕事は、ますます忙しくなっていくと予想される。

最後に、これからネットワークエンジニアが学ぶべきスキルについて考えてみた。SDN（Software Designed Network）や、API（Application Programming Interface）を利用したネットワーク機器の運用管理などの普及により、プログラミング技術が重要になることは誰もが想像する所であるが、トラフィックの流れが大きく変わり、インターネット上で論理的なイントラネットの構築が始まろうとしている今、一般企業においても、ISP 事業者のネットワークエンジニアが持っているような、インターネットルーティング等の知識の習得も重要になると考える。

このような時代のニーズを素早く読み取り、どの部門に、どのような知識を優先的に学ばせるかといった戦略についても、これからの IT 企業では必要になってくると思う。

以上

## 著者紹介

豊田　太司（CITP 認定番号：16006338）
株式会社中電シーティーアイ
情報システムの提案、開発、構築のプロジェクトに従事。現在は主に大規模なネットワークの構築案件を担当。
高度情報処理技術者（ネットワーク、セキュリティ、IT サービスマネージャ）

## 参考文献

[1]http://d.hatena.ne.jp/Kango/20170825/1503655538
[2] http://www.geekpage.jp/blog/?id=2017-9-13-1
[3] BGP によるドメイン間経路制御の現状と将来：障害事例と対策
[4] 平成 29 年 8 月に発生した大規模なインターネット接続障害に関する検証報告
[5] これまでの常識は捨てるべし！ クラウド時代の理想の企業ネットとは 2017/09/26 businessnetwork.jp
[6]CITP 制度を活用した高度 IT 人材の育成 ～超スマート社会を支える実践的技術者育成～
[7]ソフトバンク（IT 統括）の人財育成について