

働き方改革を支えるインターネット環境の選定において重視すべきポイント

株式会社矢野経済研究所 ICT・金融ユニット

Sponsored by アルテリア・ネットワークス株式会社

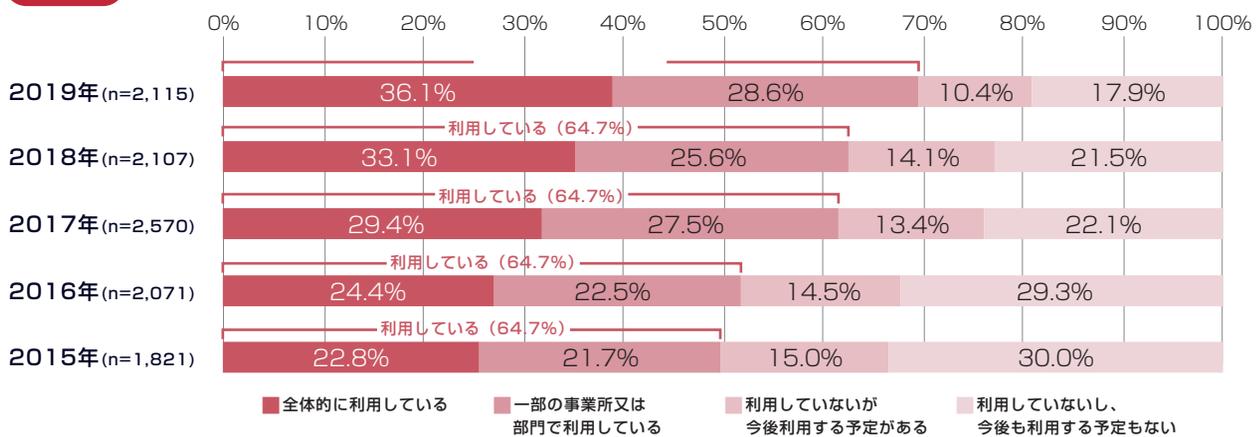
01 働き方改革などを背景に、クラウドの利用率が初めて6割超えとなる一方、新たな課題も

近年、業界を問わずに多くの企業が働き方改革の一環として、働く場所の制約を取り払うべく、Web 会議システムやグループウェア、ファイル共有サービスなどのクラウドサービスを積極的に活用している。

総務省が毎年実施している「通信利用動向調査」によると、2019年12月の調査において利用率が初めて6割を超える結果となった。毎年上昇傾向が続いているうえ、利用の効果も「非常に効果があった」「ある程度効果があった」との回答が利用企業の8割超と、クラウドサービスの導入効果を実感している状況にある。

グローバルでも、クラウドサービスの市場規模は二桁成長を続けており、国内のクラウドサービスの利用状況は引き続き堅調に伸びていくことが期待されている。

図表1 クラウドサービスの利用状況



急速に普及しているクラウドサービスだが、導入企業では次のような課題が発生している。

図表2 クラウドサービス導入後の課題

	課題	被害例
課題①	トラフィック量の増大によるレスポンスの遅延	メールやグループウェア、ファイルサーバーをクラウドに変えたら、レスポンスに数倍の時間が掛かるようになった
課題②	不安定な通信	クラウド化した基幹システムのネットワークが途切れてしまい、ビジネス上において大きなダメージを受けた。
課題③	マルウェア等の攻撃による被害の発生	マルウェアに感染し、個人情報などの機密情報が流出してしまったため、損害賠償を支払うことになり、会社の信頼も失った。

このようなユーザー企業が抱えるクラウドサービスに関わる課題を解決し、クラウドサービスが持つメリットを享受するためには、インフラとなるインターネット接続回線の選定が重要になる。

具体的には、課題①に対しては「通信速度の速い回線」、課題②に対しては「可用性が担保された安定性の高い回線」、課題③に対しては「安全性の高い回線」を利用することがそれぞれ重要である。

そのため、本レポートでは、次項から各々の選定ポイントについて述べる。

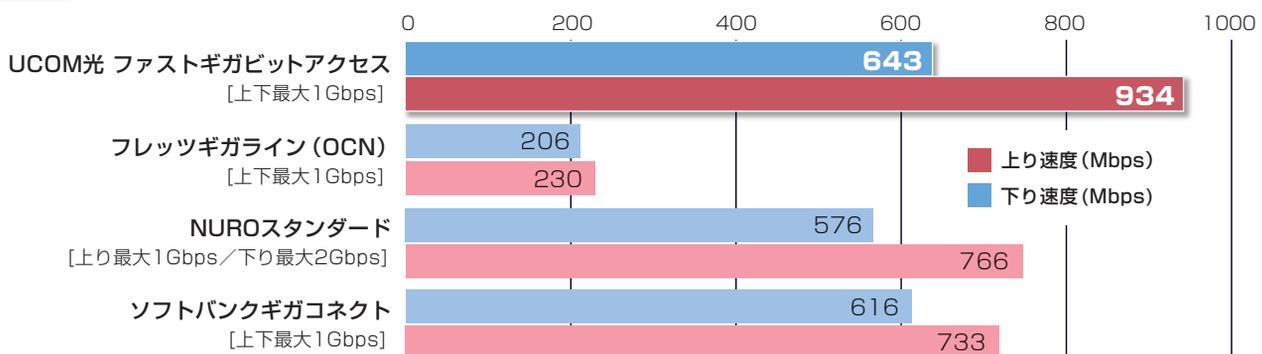
02 課題①：トラフィック量の増大によるレスポンスの遅延 「通信速度の速い回線」の選定ポイント

クラウド上でのトラフィック量が増大した結果、業務ソフトなどを利用する際に、操作が重くなり、レスポンスの遅延が生じることがある。そのような課題に対するインフラの基本能力を比較するために、インターネット接続回線の3つの指標に関する比較結果を見てみたい。

この調査では、クラウドアプリケーション利用時のスループットをみるために「①通信速度」を比較対象としている。また、往復の遅延時間（RTT）が短くなるほど、高いスループットが期待できるため「②RTTの測定」を行っている。そして大容量のファイルを受け渡す際に、ファイル転送がストレスなく使えるかを比較するために「③容量1GBのファイル転送時間」を比較している。それぞれの結果について、最適な数値に色が付いている。

この結果を見てわかる通り、クラウドサービスの応答速度はインターネット接続回線によって大きく異なる。クラウドサービスの活用の際には、クラウド上でトラフィック量が増大した際にも応答速度が維持できる回線を選定することが重要であることがわかる。

図表3 速度測定サイトによるスループット比較



図表4 pingコマンド実行によるRTTの測定比較

	UCOM光 ファストギガビットアクセス [上下最大1Gbps]	フレッツギガライン (OCN) [上下最大1Gbps]	NUROスタンダード [上り最大1Gbps/下り最大2Gbps]	ソフトバンクギガコネク ト [上下最大1Gbps]
AWS	3.6	11.7	3.7	6.7
Azure	36	45.2	33.9	40.6
Microsoft 365	1.2	24.9	1.7	4.6
G suite	1.0	15.6	1.0	4.1
サイボウズ	1.0	4.2	1.7	4.1

※各クラウドサービス（AWS、Azure、Microsoft 365、Google Workspace、サイボウズ）に ping コマンドを実行し、RTT を 3 回測定した結果の平均値

図表5 容量1GBのファイル転送時間における比較

	UCOM光 ファストギガビットアクセス [上下最大1Gbps]		フレッツギガライン+OCN [上下最大1Gbps]		NUROスタンダード [上り最大1Gbps/下り最大2Gbps]		ソフトバンクギガコネクト [上下最大1Gbps]	
	上り(秒)	下り(秒)	上り(秒)	下り(秒)	上り(秒)	下り(秒)	上り(秒)	下り(秒)
AWS	38.8	12.4	122.5	106.9	44.4	15.9	51.8	17.9
Azure	33.6	20.9	83.2	93.7	36.2	24.0	39.8	40.2
Microsoft 365	35.0	9.8	78.7	79.4	54.1	15.6	44.7	23.4
G suite	31.6	10.6	46.9	83.6	33.7	15.6	40.0	17.9
サイボウズ	33.7	9.2	136.3	60.3	37.2	13.6	40.0	17.9

※容量1GBのファイルを各々のクラウドサービスに3回アップロード/ダウンロードした場合における転送時間の平均値

※<図表3~5>の測定事業者：アルテリア・ネットワークス株式会社
 ※<図表3~5>測定条件：比較数値は、回線ごとに朝（9:00~11:00）、昼（13:00~14:00）夕（17:30~19:00）の時間帯に計測した平均値
 ※<図表3~5>調査時期：2021年2月5日~2021年2月15日
 ※<図表3~5>各回線サービス提供事業者 アルテリア・ネットワークス株式会社（UCOM光 ファストギガビットアクセス）、東日本電信電話株式会社、エヌ・ティ・ティ・コミュニケーションズ株式会社（フレッツ光ネクストファミリー・ギガラインタイプ）、ソニービズネットワークス株式会社（NUROアクセススタンダード）、ソフトバンク株式会社（イーサネットアクセス（S）Gigaコネクト）

03 課題②：安定な通信「可用性が担保された安定性の高い回線」の選定ポイント

クラウド化した基幹システムなどのネットワークが途切れたり、システムがダウンしたりしてしまうと、ビジネスに多大な影響を与えることになる。そこで本項では回線提供事業者が安定性の高い回線を提供するために取り組んでいる工夫について触れたい。まず「回線の提供方法」には、大きく分けて「専有型」と「共有型」がある。「専有型」は1社に1本を直収で敷設することや状態を常時監視していることなどから、複数ユーザーが回線をシェアする「共有型」と比較するとコスト面では若干割高となる。しかし、各社の利用状況に応じて、トラフィックのコントロールや増設を柔軟に行うなど、一定の品質を維持、提供することが可能であり、輻輳を回避することが可能となっている。

一方、「共有型」は、回線を分岐する分、コストを安く抑えられるものの、近年のトラフィック量の増加に対して許容量が追いつかず、速度低下が生じる可能性がある。

また、「輻輳の可能性」について、「共有型」の場合には、スプリッタの分配ポイントなどで輻輳が生じる可能性がある。一方、「専有型」は輻輳ポイントがなく安定した回線を提供できると考えられる。

このように安定性を重視するのであれば、「専有型」の回線を選定することが望ましいといえるだろう。

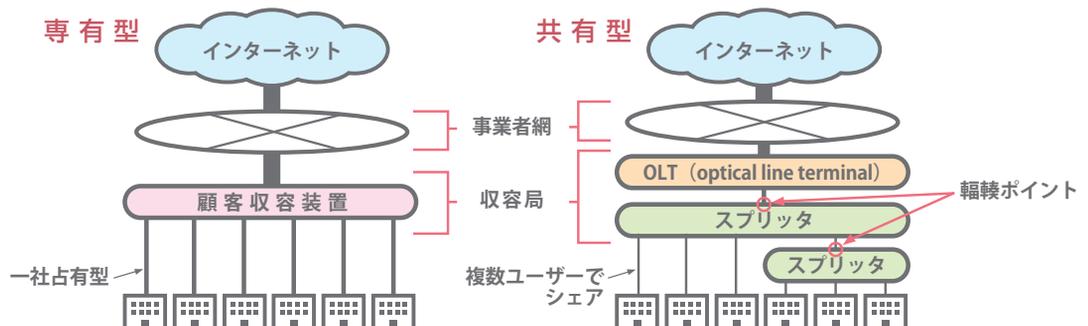
図表6

専有型/共有型

	専有型	共有型
概要	● 1社ごとに1本の回線を割り当てる	● 光ファイバー回線をスプリッタで分岐、複数ユーザーがシェアする
メリット	● 安定的かつ一定の品質を維持、提供が可能	● コストが割安な傾向
デメリット	● コストが若干割高な傾向	● 速度低下が生じる恐れ ● 輻輳が生じる恐れ
採用している事業者名	● アルテリア・ネットワークス ● ソフトバンク	● ソニービズネットワークス ● オプテージ ● NTT東日本 ● NTT西日本

図表7

専有型/共有型の仕組みの違い



04 課題③：マルウェアなどによる攻撃による被害の発生 「安全性の高い回線」の選定ポイント

速度や安定性だけではなく、インターネット環境の選定においては、近年急激に増え続けているマルウェア対策についても考慮する必要がある。クラウドサービスやスマートフォンなどの急速な普及、ソーシャルメディアなどの利用の拡大に伴い、メールによるばらまき型攻撃やランサムウェア「WannaCry」をはじめ、さまざまな悪質なマルウェアが増加しており、多くの企業や政府機関において被害が発生している。

マルウェアに感染すると、個人情報などの機密情報の流出につながるほか、意図せずに加害者になることもあり、多大な損失につながってしまう恐れがある。

図表8 マルウェアによる被害事例

マルウェアの例	被害事例
ウイルス	感染したコンピュータ内にあるファイルを消去や改ざんされるほか、外部ネットワークに流出してしまう。
スパイウェア	社内のパソコンに相手に気づかれずに不正侵入し、Webサイトの閲覧履歴やID・パスワードなどの入力情報、コンピュータ内の保存情報を収集し、外部に送信、流出してしまう。
ボット	外部の指令サーバからの指示で、感染したコンピュータが内部のデータ流出や外部への攻撃を行う。また、DDoS攻撃に利用されたり、攻撃の踏み台にされたりする恐れもある。このため、感染すると意図せずに加害者になる可能性が大きい。

各種資料より矢野経済研究所作成

対策としてはここでも回線の選定が重要であり、マルウェアブロッキングを標準装備した回線を選定することが望ましいといえるだろう。

05 回線選定に際して意識したいポイント

働き方改革を背景に、クラウドサービスの活用が急速に進んでいる一方、クラウドサービスの導入企業においては「トラフィック量の増大によるレスポンスの遅延」、「不安定な通信」、「マルウェアなどによる攻撃による被害の発生」などの課題が発生している。そのような課題を見越し、適切なインターネット環境を整備していくためには、「通信速度の速い回線」、「可用性が担保された安定性の高い回線」、「安全性の高い回線」を選定することが重要となる。具体的には、クラウド上でのトラフィック増大時でも応答速度が速く、専有型で安定的な速さを持ち、マルウェア対策を標準装備している回線を選定することが望ましい。

こうしたポイントで比較した結果、アルテリア・ネットワークスのインターネット接続サービス「UCOM 光」は、専有型ならではの安定的な速さやSLAに裏付けられたバックボーンの高さに加え、マルウェア対策を標準装備している点でアドバンテージがあるといえる。

最後に昨今、SaaSを含めたクラウド化の急速な進展や、リモートアクセス需要の高まりによってトラフィックが急激に増大しており、特に本社や大規模拠点において回線の増強ニーズが出てきている状況にある。そうしたニーズに対応すべく、そうしたニーズに対応すべく、アルテリア・ネットワークスでは上下最大10Gbpsのインターネット接続回線「UCOM光 ファストギガビットアクセス」を東京・名古屋・大阪において提供している。また、10Gbpsに留まらず、2.5Gbpsや5Gbpsと幅広いラインアップを用意、トラフィックのひっ迫具合に応じた選択が可能となっている。

回線の選定に際しては、指摘した3つのポイントに加えて、トラフィックの増大に応じた回線の増強についても意識する必要がある。