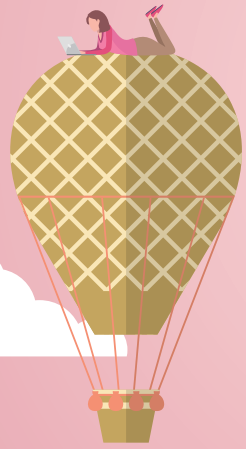
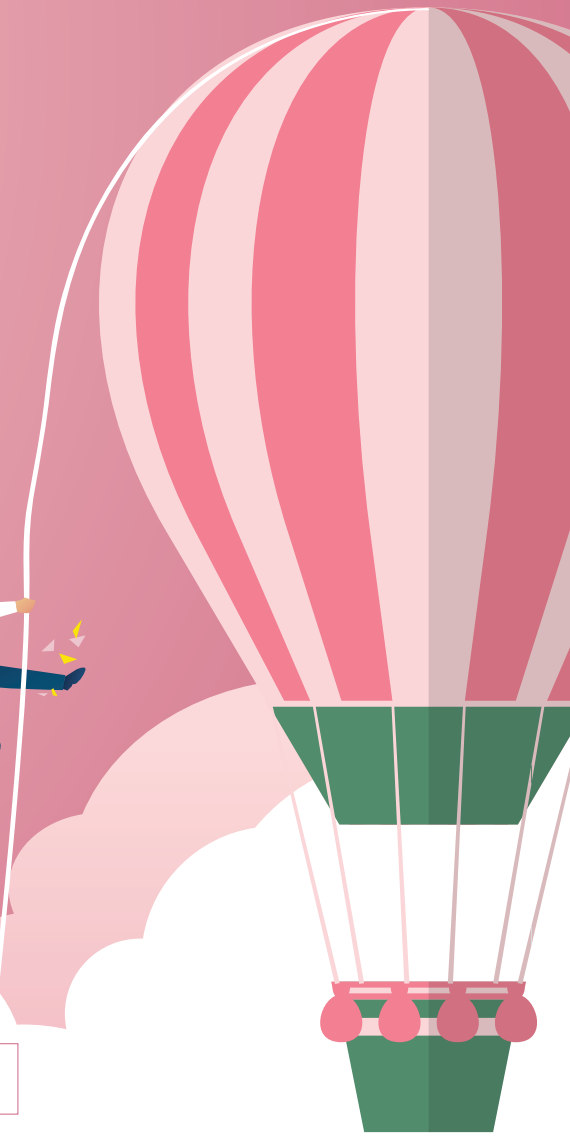
NTT Communications
Transform. Transcend.



AWS、Azure、GCP を徹底比較

3大クラウドの ネットワーク新常識

NTTコム ソリューションズ　小泉 信也（こいずみ しんや）　NTTコミュニケーションズ　飯塚 淳史（いいづか あつし）



「日経NETWORK」2019年6月号、「日経 xTECH」2019年6月3日掲載記事

AI
Artificial Intelligenceの略。
IoT
Internet of Thingsの略。

POINT 1

パブリッククラウドに移行する企業が増えている

企業がパブリッククラウド上でデータを活用する際、ネットワークへの考慮は極めて重要だ。例えば、オンプレミスとクラウドを組み合わせたハイブリッドクラウドの場合、クラウド上のデータベースとオンプレミスの間にネットワーク遅延があると、想定よりスループットが出なかったり、リアルタイム処理ができなかったりする事象が発生する。こうしたことを防ぐには、ネットワークの観点から各クラウドを比較することが不可欠だ。そこで本特集では、パブリッククラウドを導入する際のポイントをネットワークの視点から解説する。

1番目のポイントは、検証環境やバックアップシステム、重要システムなどをパブリッククラウドに移行する企業が増えていることだ。調査会社のIDC Japanは、国内のパブリッククラウドサービスの市場規模は、2018年の6688億円から2023年には2.5倍の1兆6940億円になると予測している(図1)。

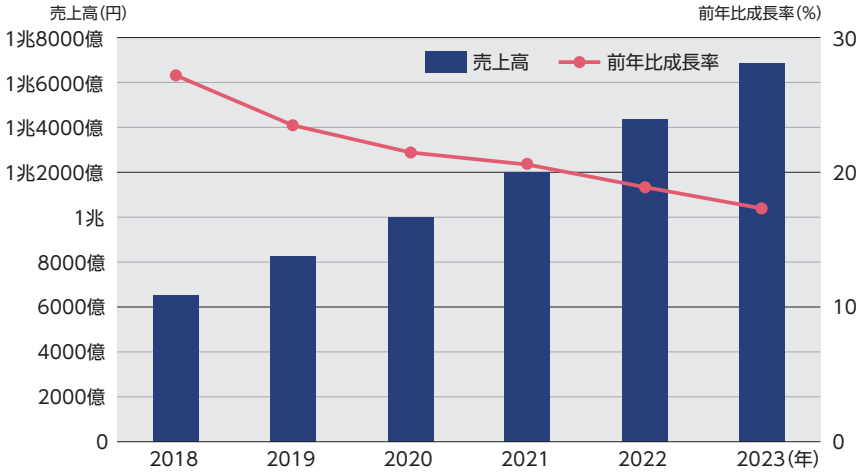
パブリッククラウドの活用が進む理由は、従来のオンプレミス利用と比較して、物理的なインフラストラクチャーの構築・管理・運用の手間から解放されることと、柔軟性・拡張性・冗長性の観点でメリットが得られることだ。

企業がパブリッククラウドの導入を検討する際、まず候補に挙がるのは米アマゾン・ドット・コムの Amazon Web Services(AWS)、米マイクロソフトの Microsoft Azure(アジュール)、米グーグルの GoogleCloud Platform (GCP)。いわゆる 3 大クラウドだ。

各クラウドでは、コンピューティングやストレージなどの機能や料金は類似のものが提供されており、AIやIoTといった先端技術で独自性を出している(表1)。

図1 国内のパブリッククラウド市場の予測

IDC Japanが2019年3月27日に発表した国内パブリッククラウドサービス市場規模の予測。2018年は、前年比27.2%増の6688億円となった。2018～2023年の年間平均成長率は20.4%で推移し、2023年の市場規模は2018年比2.5倍の1兆6940億円になるとしている。



出所：IDC Japan

表1 3大クラウドの主なマネージドサービス

Amazon Web Services(AWS)、Microsoft Azure(以下、Azure)、Google Cloud Platform(GCP)の主なマネージドサービスを挙げた。

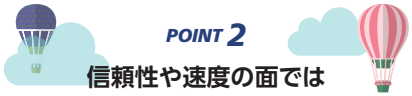
サービス	種別	AWS	Azure	GCP
ストレージ	非構造データ	Amazon S3	Azure Storage(BLOB)	Google Cloud Storage
	アーカイブ	Amazon S3 Glacier	Azure Archive Storage	Google Cloud Storage(Coldline)
	ファイル	Amazon EFS	Azure Files	Cloud Filestore
データベース	RDBMS	Amazon RDS (MySQL、PostgreSQL、SQL Server、Oracle Database、MariaDB、Amazon Aurora)	Azure Database for MySQL、Azure Database for PostgreSQL、SQL Database	Cloud SQL (MySQL、PostgreSQL、Microsoft SQL Server)、Cloud Spanner
	NoSQL	Amazon SimpleDB、Amazon DynamoDB	Azure Table Storage、Azure Cosmos DB	Cloud Datastore、Cloud Firestore、Cloud Bigtable
データウエアハウス	——	Amazon Redshift	SQL Data Warehouse	BigQuery

IPsec
Security Architecture for Internet Protocolの略。

VPN
Virtual Private Networkの略。

IaaS
Infrastructure as a Serviceの略。

ISP
Internet Service Providerの略。インターネットサービス事業者。単にプロバイダーと呼ぶこともある。



POINT 2
信頼性や速度の面では閉域接続が優れている

ハイブリッドクラウド環境においてオンプレミスとクラウドの接続方法は、大きく2パターンがある。1つは、インターネットを経由し、通信自体をIPsec（アイピーセック）などで暗号化するインターネットVPN接続。もう1つは、インターネットを経由せず、通信事業者の閉域網だけで通信する閉域接続である。

主にIaaSを利用する場合について、インターネットVPN接続と閉域接続を比較した（表2）。インターネットVPN接続は安価で、暗号化により十分なセキュリティーが保たれている。だが、複数のISPで構成されるインターネットを経由するため、遅延や通信の揺らぎがあり、帯域が保証されない。これに対し、閉域接続は信頼性や速度の安定性で優れる。また、通信が閉域網に閉じているので、インターネットVPN接続より安全といえる。

POINT 3
AWSやGCPは拠点数が多いと高価に

オンプレミスとパブリッククラウド（仮想ネットワーク）をインターネットVPN接続でつなぐ構成を示す（図2）。各要素の名称は異なるが、基本的な構成は各社で共通している。

クラウド上には、ユーザー企業ごとに仮想的なゲートウエイリソース（仮想ゲートウエイ）が作成される。オンプレミス環境にある物理的なルーターと仮想ゲートウエイはIPsecなどの暗号化トンネルで結ばれる。これを通して、オンプレミスにある機器とクラウド上の仮想ネットワークが通信する。

各社の仮想ゲートウエイを比較した（次ページの表3）。帯域や接続数の上限、料金などが異なる。

コストは、通信量に応じた課金とリソースに応じた課金の2つの合算なのは3社ともに同じである。ただし、課金の仕方に各社の特徴がある。AWSとGCPは、時間当たりのVPNトンネル数（VPN接続時間）に対して課金される。これに対しAzureは、時間当たりのVPNトンネル数に課金されるのではなく、実際に利用しているVPNトンネルの有無にかかわらず、仮想ゲートウエイのリソースが作成されてからの経過時間に対して課金される。つまり、AWSやGCPは実際に通信していなくてもVPNトンネル数に応じて課金が加算されるため、拠点数が多いような場合は高価になっていくので注意が必要である。

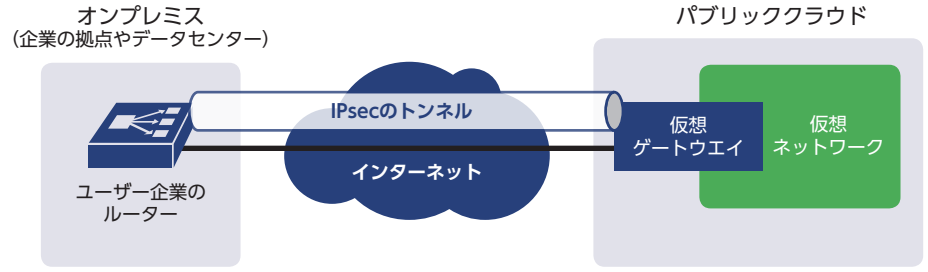
1本のVPNトンネル1本当たりの料金を比較すると、AWSはこれまで頻繁に料金を下げており、比較的安価にインターネットVPN接続を利用で

表2　クラウドとの接続形態の比較
クラウドとの接続形態は、インターネットVPNを使う方法と閉域網を使う方法がある。それぞれの特徴を挙げた。

接続形態	インターネットVPN接続		閉域接続	
セキュリティー	暗号化技術により実現	○	インターネットを経由しない	◎
信頼性	アクセス回線やISP網の信頼性に依存	△	閉域網で直接接続するため、比較的信頼性は高い	◎
品質	●遅延や揺らぎがある ●帯域は保証されていない	○	●遅延や揺らぎが少ない ●パケット損失が少ない ●帯域が安定している	◎
コスト	安価	◎	比較的高価であるが、従量制など課金方法の選択肢が多い	△

ISP：Internet Service Provider

図2　インターネットVPN接続によるネットワーク構成
基本的な構成は各社で共通しているが、仮想ゲートウエイの名称などが異なる。



IPsec：Security Architecture for the Internet Protocol
VPN：Virtual Private Network

VPC
Virtual Private Cloudの略。
VGW
Virtual Private Gatewayの略。
IKEv2/IKEv1
IKEはInternet Key Exchange protocolの略。IPsecでコネクションを確立する際に安全に情報を交換するためのプロトコル。IKEv1はRFC 2409、IKEv2はRFC 4306で規定されている。
ピアリング
ルーティングプロトコルの一種であるBGPで、経路情報をやりとりするためのTCPコネクションを確立すること。
不要である
このほか、Cloud Routerによりオンプレミスへの経路広告をカスタマイズできる。他クラウドは仮想ネットワークの経路情報しか広告できないが、GCPでは自由に広告する経路情報を変更できる。例えばデフォルトルート(0.0.0.0/0)を広告することも可能で、柔軟なネットワーク設計ができる。

きる。また、GCPはVPNトンネル1本当たりの帯域の上限が高く、トンネルの接続数の上限も多いため、大規模な運用にも堪えられることが分かる。

運用を楽にする各社の工夫

各クラウドでは、運用の手間を省ける新しいサービスを提供している。

AWSは、2018年に開催された同社の年次イベント「re:Invent(リインベント)」において、「Transit Gateway(TGW)」を発表した。従来、オンプレミスのルーターを仮想ネットワーク(VPC)に接続する際、それぞれの仮想ゲートウエイ(VGW)にVPNを接続する必要があった。このため、新たにVPCを立ち上げるたびにルーターでのVPN設定の追加が必要になり、手間がかかっていた。これに対し、TGWを使うとVPNのトンネルは1本だけで済むため、構成がシンプルになるだけでなく、オンプレミス側での運用負荷の低減が可能となる(次ページの図3)。

Azureでは「Virtual WAN」というサービスが提供されている。Virtual WANはクラウド上の仮想ネットワークと企業の拠点などのサイトをつなぐハブとして機能する。大規模なサイト間接続を実現するのに有用なサービスである。現状、サイト間、ポイント対サイト(プレビュー版)、ExpressRoute(プレビュー版)が利用できる。

各拠点に置くVPN装置として、「Virtual WANパートナー」と呼ばれる推奨ベンダーの製品を使えば、VPN接続を自動化できる。VirtualWANパートナーとしては、米パロアルトネットワークスや米シトリックスなどがある。

Virtual WANパートナーの製品では、Virtual WAN設定時に作成されるデバイス設定ファイルを利用し、VPN接続を自動化する仕組み(ツールキットなど)が用意されている。ただし、AzureのIKEv2/IKEv1　IPsecサポートのための要件に準拠していれば、推奨ベンダー以外の製品でも接続が可能である。

新サービスではないが、GCPは仮想ネットワークの考え方が特徴的で、運用の手間を軽減するメリットがある。GCPの仮想ネットワーク(VPC)は、特定のリージョンにのみ存在するのではなく、標準機能としてグローバルなリージョンで利用できる。このため、異なるリージョンにアクセスする際、仮想ネットワーク間をピアリングする作業は不要である。

表3　3大クラウドの仮想ゲートウエイの比較
インターネットVPN接続で利用する仮想ゲートウエイを比較した。すべて東京リージョンでの利用を前提にしており、2019年4月時点の情報に基づいている。

	AWS	Azure	GCP
名称	Virtual Private Gateway	VPN Gateway	Cloud VPN(VLANアタッチメント、Cloud Router)
帯域上限	1.25Gbps/Virtual Private Gateway*1	Basic　：100Mbps VpnGw1：650Mbps VpnGw2：1Gbps VpnGw3：1.25Gbps	1.5Gbps/トンネル*2
接続数上限	10/Virtual Private Gateway 50/リージョン	Basic　：10/VPN Gateway VpnGw1：30/VPN Gateway VpnGw2：30/VPN Gateway VpnGw3：30/VPN Gateway	64/Cloud Router
クラウドへの経路広報数の上限*3	100	4000	100
通信量*4に応じた月額料金	最初の1GBまで　：0ドル 1G～10TB　：0.114ドル/GB 10T～50TB　：0.089ドル/GB 50T～150TB　：0.086ドル/GB 150T～500TB　：0.084ドル/GB	最初の5GBまで　：0ドル/GB 5G～10TB　：0.12ドル/GB 10T～50TB　：0.085ドル/GB 50T～150TB　：0.082ドル/GB 150T～500TB　：0.08ドル/GB	0～1TB　：0.14ドル/GB 1～10TB　：0.14ドル/GB 10TB～　：0.12ドル/GB
リソースに応じた料金	0.048ドル/時間*5	Basic　：0.04ドル/時間 VpnGw1：0.19ドル/時間 VpnGw2：0.49ドル/時間 VpnGw3：1.25ドル/時間	0.075ドル/時間/トンネル*6

＊1　1つのVirtual Private Gatewayで複数のVPNトンネルが接続されている場合、累積で1.25Gbpsが上限になる
＊2　VPNトンネルを複数利用することで、トータルの帯域をさらに増やせる　＊3　オンプレミスからパブリッククラウドへの経路広告数の上限
＊4　クラウドからオンプレミスへの通信量を指す。オンプレミスからクラウドへの通信については無料
＊5　VPN接続がアクティブな時間に対して課金される　＊6　ready状態のVPNトンネルのみが課金対象

bps:ビット/秒
VLAN:Virtual LAN(Local Area Network)

POINT 4

物理接続型サービスでは GCPが高速でAWSが安価

閉域網や専用線を使ってオンプレミスとパブリッククラウドをつなぐ閉域接続には、「物理接続型」と「論理接続型」の2種類の構成がある(図4)。

物理接続型では、オンプレミスにあるユーザー企業のルーターとパブリッククラウドを光ファイバーケーブルで物理的に接続する。これに対し、論理接続型ではパブリッククラウドの設備と直接つながるのは通信事業者などの接続パートナーだ。

接続パートナーはユーザー企業に対して、パブリッククラウドの物理的な帯域を分けて提供す

図3 AWSの「Transit Gateway」を使った構成

Transit Gatewayは2018年の「AWS re:Invent 2018」で発表された。これを利用すると構成がシンプルになる。またユーザー企業側でトンネルを構築する負荷を減らせる。

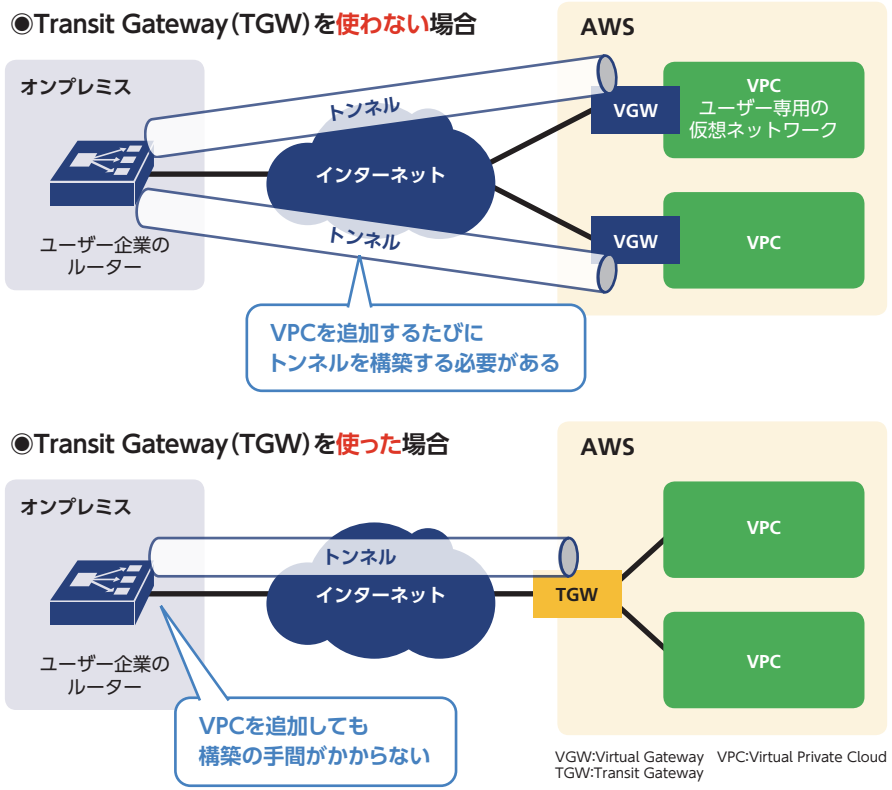


図4 物理接続型と論理接続型の違い

オンプレミスとパブリッククラウドを閉域接続でつなぐ方法として、物理接続型と論理接続型の2種類がある。物理接続型はユーザー企業の設備とパブリッククラウドを直接光ファイバーケーブルでつなぐ。論理接続型は接続パートナー経由でつなぐことになる。

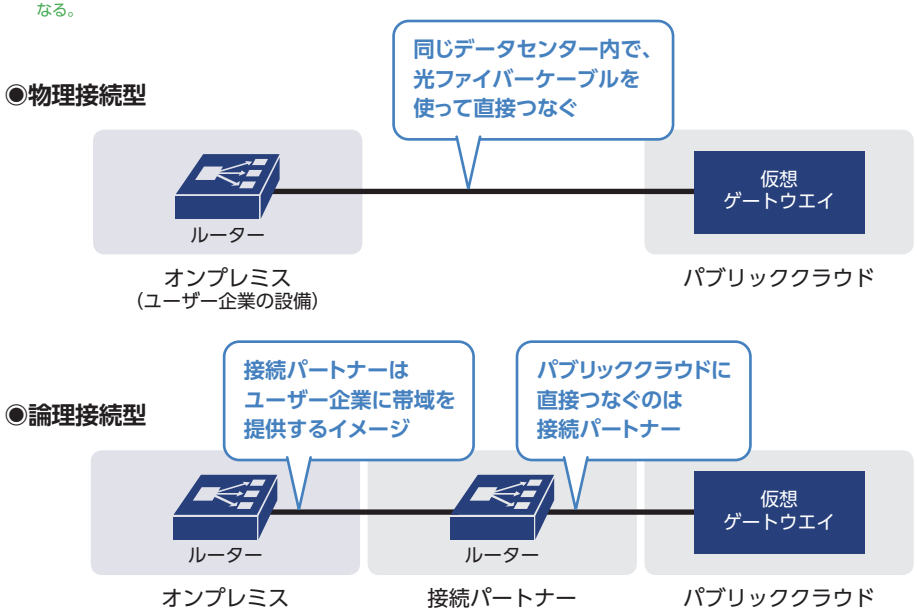


表4 AWSとGCPにおける物理接続型サービスの比較

AWSとGCPの物理接続型を比較した。Azureは物理接続型を提供していない。2019年4月時点の情報に基づいている。

	AWS	GCP
サービス名	Direct Connect(専用接続)	Dedicated Interconnect
接続用途	private接続、public接続	VPC接続
接続帯域	1Gbps、10Gbps	10Gbps、100Gbps(ベータ版)
クラウドへの経路広報上限	100(private接続)、1000(public接続)	100
接続ロケーション*1	Equinix TY2(東京)、アット東京CC1(東京)、Equinix OS1(大阪)など	ComSpace I(東京)、Equinix TY2(東京)、アット東京(東京)、Equinix OS1(大阪)、NTTテレパーク堂島ビル2(大阪)など
料金	● ポート料金 1G:0.285ドル/時間 10G:2.142ドル/時間 ● データ転送料金*3: 0.041ドル/GB	● 相互接続*2(10Gbps):1700ドル/月 ● VLANアタッチメント費用*2:72ドル/月 ● データ転送料金:0.042ドル/GB

＊1 AWSはアジアパシフィック(東京)リージョン、GCPはasia-northeast1(日本)
＊2 GCPの専用接続の場合、相互接続がポート料金に相当し、VLANアタッチメントを利用することでオンプレミスとクラウドの間でBGPセッションを確立できる。
＊3 接続元リージョンや接続ロケーションに応じて費用が異なる。ここでは接続元が東京リージョン、Equinix TY2経由のデータ転送料を記載している。

るイメージとなる。AWSとGCPは、物理接続型と論理接続型の両方を提供している。一方、Azureは物理接続型を提供しておらず、接続パートナー経由の論理接続型のみとなる。

まず物理接続型についてAWSとGCPを比較した(前ページの表4)。

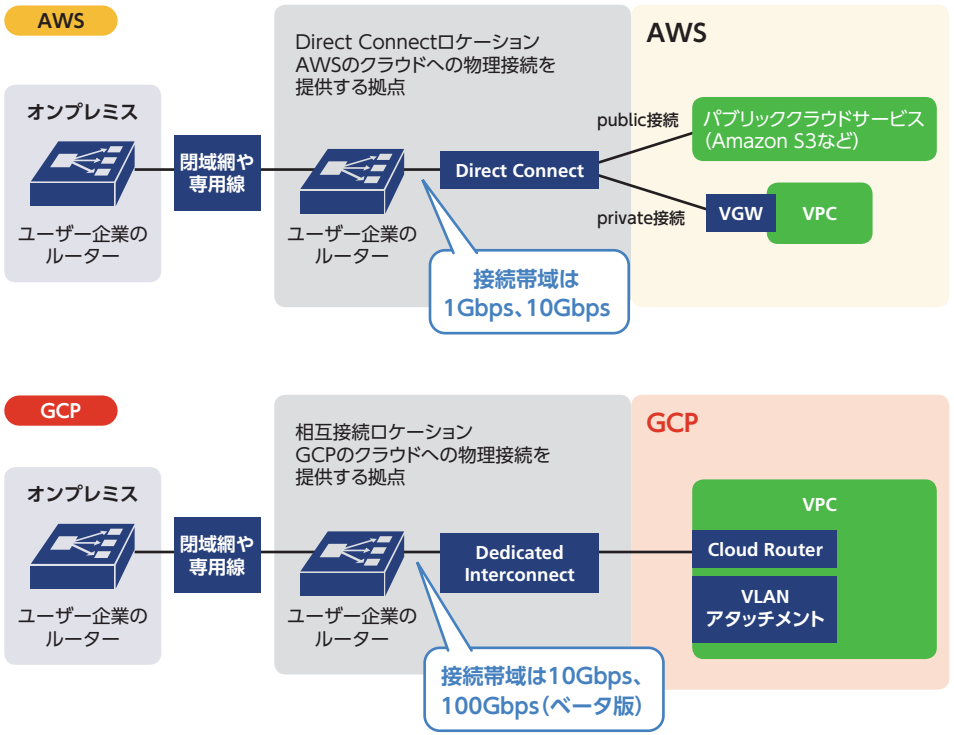
AWSは接続帯域のメニューとして1Gビット/秒と10Gビット/秒を提供している。対して、GCPは10Gビット/秒を基本とし、100Gビット/秒もベータ版としてリリースしている。AWSに比べGCPは、より広帯域での利用が可能となっている。

接続ロケーションは、GCPは比較的選択肢が多い。料金についてはほぼ変わらないが、データ転送料金はAWSが若干安価である。

AWSおよびGCPの物理接続型の構成を示す(図5)。基本的な構成は似ている。ユーザー企業がルーターを接続ロケーションに持ち込み、クラウド事業者が用意したルーターに光ファイバーケーブルでつなぐ。

図5 AWSおよびGCPの物理接続型サービスの構成

ユーザー企業が接続ロケーションに自社ルーターを持ち込み、光ファイバーケーブルで直接接続する。接続帯域はAWSが1Gビット/秒と10Gビット/秒なのに対し、GCPは10Gビット/秒が基本で、ベータ版だが100Gビット/秒のメニューも用意している。



POINT 5

論理接続型サービスは柔軟な帯域選択が可能

次に論理接続型サービスを見ていこう。Azureを例に構成を示した(図6)。基本的な構成は物理接続型と似ているが、前述のように、クラウド事業者のルーターに直接つなぐのは接続パートナー(ExpressRouteパートナー)が持ち込んだルーターだ。

3大クラウドが提供している論理接続型サービスを比較した(次ページの表5)。各クラウドとも、豊富な接続帯域メニューが用意されており、物理接続型に比べて、より柔軟な帯域選択が可能である。注意したいのは、500Mビット/秒以下の帯域については、AzureはAWSやGCPよりメニューが少ない点だ。300Mビット/秒や400Mビット/秒が用意されておらず、200Mビット/秒を少し超えると500Mビット/秒を選択する必要がある。

AWSとGCPについては接続帯域の種類や価格体系が似ている。広帯域になるとGCPがAWSよりも低コストとなる。

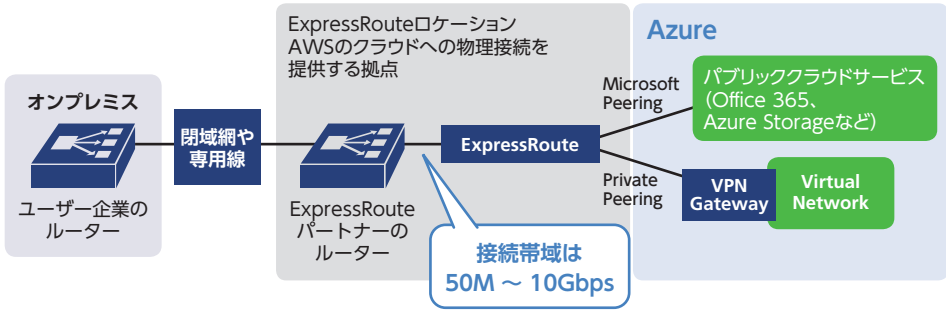
Azureは、データ転送料金が他社に比べ安価だが、データ転送量のほかに、ExpressRouteを接続するためのゲートウエイに費用が発生する(表5のERゲートウエイ費用)。

また、データ転送量に応じた料金は、インターネットVPN接続に比べ、各社とも比較的安価に設定している点は注目すべきだろう。閉域接続にする分、専用線や閉域網にかかる料金が必要になるが、インターネットVPN接続に比べ料金が安価に設定されている項目もある。コストは利用状況に応じて、注意深く計算すべきである。

注意したいのは、表に示したパブリッククラウドの料金のほか、接続パートナーにネットワーク利用料など支払う場合があることだ。また、各クラウドで料金体系が異なっているので分かりづらいところもある。このため詳細は接続パートナーに確認する必要がある。

図6 Azureの論理接続型サービスの構成

各ExpressRouteパートナーごとに帯域の種別が異なるので注意が必要だ。ここではAzureを例に挙げたが、AWSやGCPも基本構成は似ている。



「private接続」を使う
public接続がないとパブリッククラウドに閉域で接続できないわけではない。
例えば、private接続のみの環境において、EC2上でプロキシーサーバーを立ち上げれば、それを経由してパブリッククラウドに接続できる。

VLAN ID
VLANを識別するためのIDで、12ビット長の値で定義される。
VLANはVirtual LAN(Local Area Network)の略。

パブリッククラウドとの接続方法

物理接続型と論理接続型のいずれも、各パブリッククラウドに閉域で接続できる。

AWSでは、「public接続」を使うことで、パブリックサービスであるAmazon S3などと直接のデータ送受信が可能となる。AmazonEC2などの仮想マシン(VM)との接続には「private接続」を使う。

Azureの場合、「Private Peering」がAWSのprivate接続に、「Microsoft Peering」がpublic接続に相当する。GCPでは「PartnerInterconnect」がAWSのprivate接続に相当する。グーグルのパブリッククラウドへの閉域接続は、「ダイレクトピアリング」や「キャリアピアリング」という接続サービスを利用することで可能となる。

表5 3大クラウドの論理接続型サービスの比較

1カ月の使用時間を744時間(24時間×31日)とし、冗長化のための2接続という条件で料金を計算した。AzureのExpressRouteについては、従量課金プランと無制限データプランが存在し、それぞれStandardプランとPremiumプランが選択できる。ここでは従量課金プラン／Standardプランの例を挙げた。2019年4月時点の情報に基づいている。

接続形態	AWS	Azure	GCP
サービス名	Direct Connect (ホスト型接続)	ExpressRoute (standard、premium)	Partner Interconnect
接続用途	private接続、public接続	Private Peering、 Microsoft Peering	VPC接続
クラウドへの経路広報数の上限	100(private接続)、 1000(public接続)	4000(Standard)、 10000(Premium)	100
接続料金	50M　：43.152ドル/月 100M　：84.816ドル/月 200M　：113.088ドル/月 300M　：169.632ドル/月 400M　：226.176ドル/月 500M　：282.72ドル/月 1G　：467.232：ドル/月 2G　：932.976ドル/月 5G　：2333.184ドル/月 10G　：3513.168ドル/月	50M　：55ドル/月 100M　：100ドル/月 200M　：145ドル/月 500M　：290ドル/月 1G　：436ドル/月 2G　：872ドル/月 5G　：2180ドル/月 10G　：3400ドル/月	50M　：78ドル/月 100M　：90ドル/月 200M　：120ドル/月 300M　：160ドル/月 400M　：200ドル/月 500M　：250ドル/月 1G　：400ドル/月 2G　：820ドル/月 5G　：1800ドル/月 10G　：3400ドル/月
データ転送量に応じた料金	データ転送料金*1： 0.041ドル/GB	データ転送料金 (従量課金プラン):0.025ドル/GB ※別途ERゲートウエイ費用がかかる	データ転送料金： 0.042ドル/GB
必要なリソースなど	仮想インターフェース、 仮想Virtual Private Gateway（無料）	ERゲートウエイ費用 Standard ER：0.19ドル/時間 高性能ER：0.49ドル/時間 超高性能ER：1.87ドル/時間	Cloud Router（無料）

＊1　接続元リージョン、接続ロケーションに応じて費用が異なる。今回は、東京リージョンが接続元で、Equinix TY2経由でのデータ転送量を記載している。

ER:ExpressRoute

柔軟さと大容量に対応

ここまで基本的な閉域接続サービスについて取り上げた。3大クラウド事業者は、閉域接続をより柔軟に、より大容量にする方向でサービス開発を進めてきた。そのうち、2つを紹介したい。

まずAWSの「Direct Connect Gateway」である。Direct Connectで仮想ネットワーク(VPC)やパブリッククラウドサービス(Amazon S3など)を接続する際、必ず「仮想インターフェース（VIF)」と呼ぶものを設定する。これはVLAN(ブイラン) IDによって識別される仮想的な回線だ。従来、1個のVIFは1個の仮想ゲートウエイ（VGW）にしか接続できなかった。Direct Connect Gatewayを利用することで、VIFを複数のVPCに接続することが可能となった。

もう1つはAzureの「Express Route Direct」というサービス。これはマイクロソフトのグローバルネットワークに100Gビット/秒で直接接続できるサービスである。例えばAzureのクラウドストレージサービス(Azure Storage)に対し、大容量通信が必要な場面などで活用できる。

POINT 6

ペタバイト級のデータは物理的な移行サービスを使う

これまで取り上げてきたインターネットVPN接続や閉域接続は、ネットワークを使った通信でデータをやりとりする。だがケースによって、この方法はクラウドへの移行の際に問題になる場合がある。

オンプレミスにペタバイト級のデータがある場合、移行時にはオンラインでパブリッククラウドに送信する必要がある。しかし、この方法では、高速な回線がないと移行に膨大な時間を要してしまう。加えて、一時的にしか利用しない移行時の大容量通信のために、高価な閉域回線などを利用するのはコストパフォーマンスに優れない。

そこで各クラウド事業者は、オンラインではなく物理的にデータを移行するサービスを提供し

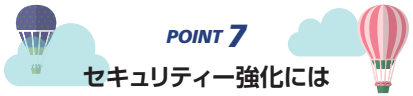
表6 **物理的なデータ移行サービスの比較**

オンプレミスに巨大なデータがあり、それをクラウドに転送する場合、ネットワークを使うと時間がかかるだけでなく、コストが高くついてしまう。そこでクラウド各社は、物理ディスクを使ってデータを移行するサービスを用意している。2019年4月時点の情報に基づいている。

	AWS	Azure	GCP
サービス名	Snowball	Azure Import/Export	Transfer Appliance
ディスク容量	50TB、80TB	ディスク当たり8TB、 1注文当たり最大40TB (Azure Databox Diskの場合) ※自身でディスクを用意する場合は指定なし	100TB、480TB
料金	● 利用料(配送料は別) 50TB:200ドル 80TB:250ドル ● アプライアンス利用超過料金 15ドル/日(10日間無料)	● 利用料(配送料は別) 取り扱ったストレージディスクごとに80 ドルの固定費	● 利用料(配送料は別) 100TB:300ドル 480TB:1800ドル ● アプライアンス利用超過料金 100TB:30ドル/日(10日間無料) 480TB:90ドル/日(25日間無料)

ている(表6)。各社ともに、物理的なストレージアプライアンスを利用することで、数日程度でパブリッククラウドのストレージサービスにデータを格納できる。

コストとしては、ストレージ移行用ディスクは利用日数に応じて課金される(10日程度の無料期間あり)。ただし、ストレージからクラウドサービスへのデータ転送は無料である。コストパフォーマンスに優れたデータ移行が実現可能となるため、うまく活用したい。



POINT 7

セキュリティー強化にはプライベート接続を活用

パブリッククラウドでデータを活用する際に、特に留意すべきなのがセキュリティーである。

各クラウド事業者は、仮想ネットワークに対するセキュリティー機能を提供している。具体的には、一種の仮想ファイアウオールを使って、IPアドレスやプロトコル、ポート番号などを用いて通信を制御する。

ストレージなどのパブリッククラウドサービスの場合は別の仕組みが使われる。例えば、データをパブリッククラウドのストレージにアップロードして、クラウド内のVMやオンプレミスから利用することを考えてみよう。一般的には、ストレージの操作権限を企業ユーザーの管理者に付与して、アクセス制御する(RBAC)。

しかしながら、パスワードが漏洩した場合などは、データの流出リスクが発生する。そこで各クラウド事業者は、パブリッククラウドへのアクセスに対し、接続元のIPアドレスや仮想ネットワークを制限する機能を提供している(表7)。詳細な仕様や利用方法は、各クラウド事業者のサイトなどで確認してほしい。

ストレージやデータベースなどパブリッククラウドサービスへのアクセスはインターネット経由を前提にしていた。オンプレミスから仮想ネットワークまでは閉じているが、そこからパブリッククラウドサービスにアクセスするにはインターネットを経由する必要があった。

そこで各クラウド事業者は、仮想ネットワークからパブリッククラウドサービスにアクセスする際、インターネット経由せずに、クラウド内で直接接続できる「エンドポイント」と呼ばれる機能を追加している。これにより、通信経路をよりセキュアにできる(次ページの表8、次ページの図7)。

また、オンプレミスからパブリックサービスを利用する場合、閉域接続であっても、グローバルIPアドレスが必要だったり、ユーザー企業のネットワーク内にグローバルIPアドレスの経路情報が流入したりするなどの問題があった。

RBAC
Role Based Access Controlの略。
ロールベースアクセス制御。ユーザーやグループに対し、アクセスや操作の権限を制御する方法。

表7 **ストレージサービスへのネットワーク接続制限に関する比較**

クラウド上のストレージにあるデータをオンプレミスなどから利用する場合、ユーザー企業に操作権限を付与することになる。ただし、パスワードの漏洩などでデータ流出のリスクがある。そこでストレージに対して様々なアクセス制御を実施する機能が用意されている。

	AWS	Azure	GCP
制限内容	● 「S3バケットポリシー」により、接続元VPC/IPの制限が可能	● 「仮想ネットワーク(vNet)サービスエンドポイント」を利用することで、接続元VPCの制限が可能 ● ストレージアカウントのIPネットワークルールを利用することで、接続元IPの制限が可能	● 「VPC Service Control」を利用することで、接続元VPCの制限が可能 ● 併せて「Access Context Manager」を利用することで、細かな条件(IPレベルなど)での制限も実装可能

そこで、ハイブリッドクライド環境でオンプレミスからパブリッククラウドサービスに直接アクセスできる機能拡充も進んでいる。

GCPは、「Private Google Access for onpremis hosts（ベータ版）」の提供を始めた。これにより、オンプレミスや仮想ネットワークからGoogle Cloud Storage、BigQueryなどのパブリッククラウドサービスに直接アクセス可能となる。

ただ、このようなサービスは、現時点では限定的であるため、最新の情報を調査した上で利用してほしい。

これで見てきた通り、各クラウドのネットワーク関連項目では、名称は類似していても考え方や上限値が異なる部分も多い。またクラウドの頻繁なアップデートに追従するのに日々の情報収集は欠かせない。このため、クラウドのネットワークに詳しい接続パートナーを活用をするのは、現実的な選択肢だろう。

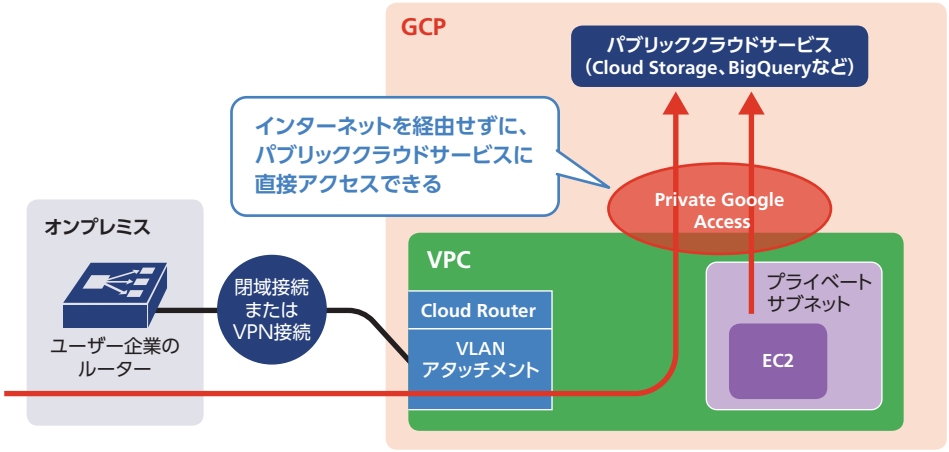
表8 パブリックサービスに直接接続できるエンドポイントサービス

パブリッククラウドサービスへの接続はインターネット経由が基本だが、最近はセキュリティー強化のため、オンプレミスや仮想ネットワークからパブリッククラウドサービスに直接接続するサービスが提供されている。

接続内容	AWS	Azure	GCP
仮想ネットワークからパブリックサービスにプライベート接続	VPCエンドポイントサービス（gateway型）	vNetエンドポイント	Private Google Access
オンプレミスからパブリックサービスにプライベート接続	VPCエンドポイントサービス（interface型）	――	Private Google Access for on-premis hosts（ベータ版）

図7 プライベートなVPCからパブリッククラウドに直接つなぐサービス

GCPの「Private Google Access」を例として示した。AWSやAzureにも同様のサービスがある。



「日経NETWORK」2019年6月号、「日経 xTECH」2019年6月3日掲載記事
株式会社日経BPより記事利用の許諾を得て、制作・発行しています。