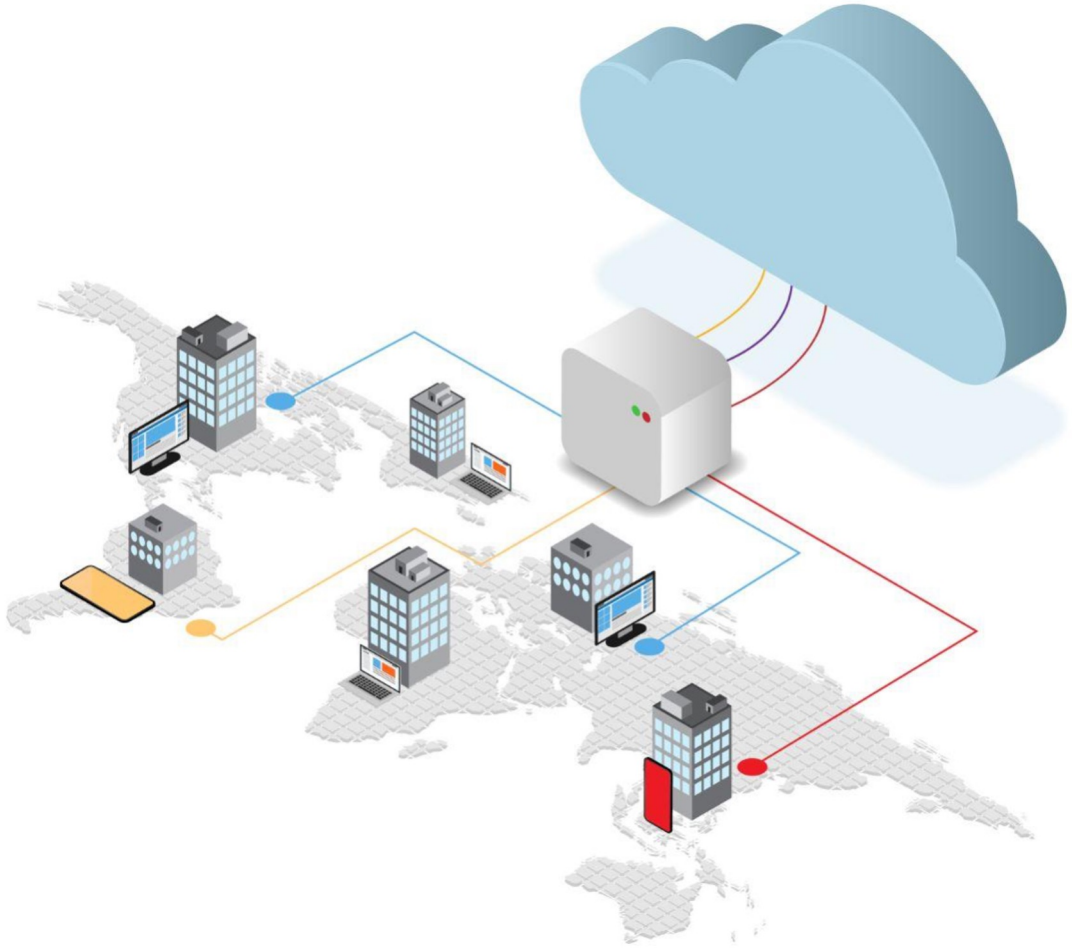


Session Report

進化を続けるネットワーキング サービス接続の
ベスト プラクティスを紹介

大解剖！ Google Cloud ネットワーキング サービス

Google Cloud
ソリューション＆テクノロジー部 カスタマー エンジニア
有賀 征爾

Google Cloud

Google Cloud

セッション レポート概要

Google Cloud のネットワーキング サービスはここ 1、2 年の間に大きく進化しており、それに伴ってベスト プラクティスも変わってきています。ネットワーキング サービスの進化と、スムーズにご利用いただくための最新情報をご提供します。

プレゼンター紹介

Google Cloud
ソリューション＆テクノロジー部 カスタマー エンジニア
有賀 征爾

Google Cloud でカスタマーエンジニア (ネットワーク プロダクト担当) として、日々お客様の技術的な課題の解決と、より良いアーキテクチャのご提案を目指しています。

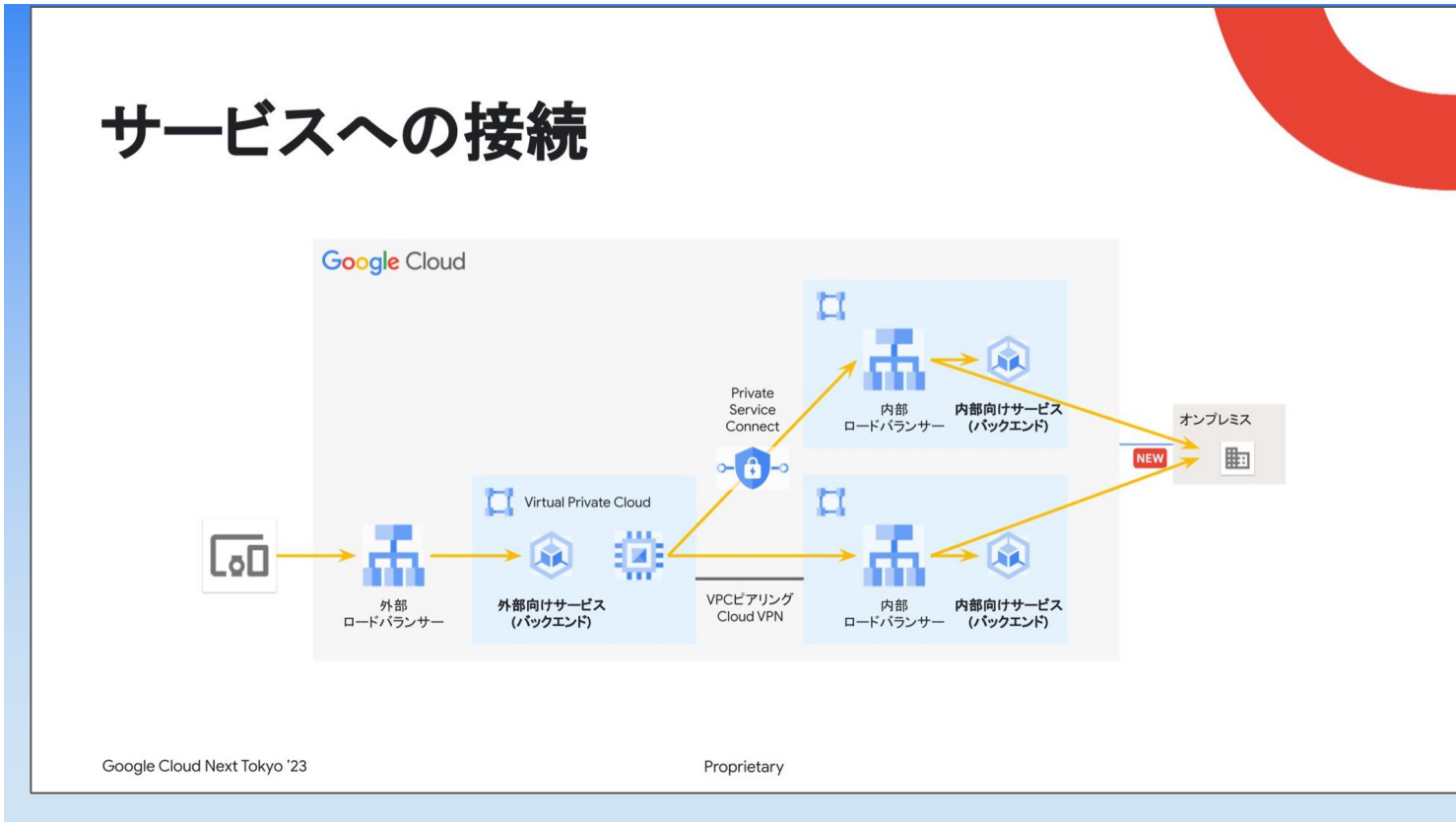
目次

Google Cloud とのネットワーク接続の概要

Google Cloud のサービスを接続する場合、まずはエンドユーザーのクライアントから、バックエンドを持つ外部のロード バランサーにつながります。その次に、外部向けサービスにつながります。

外部向けサービスからクライアントにコンテンツを返すこともありますが、さらに内部ロード バランサーにつながり、内部向けサービスでコンテンツを作成してからクライアントに返すこともあります。

外部ロード バランサーと同様にバックエンドを持つ内部ロード バランサーから、内部向けサービスを経由し、オンプレミスやほかのクラウド サービスにつながるシステムを構築することも、簡単にできるようになりました。

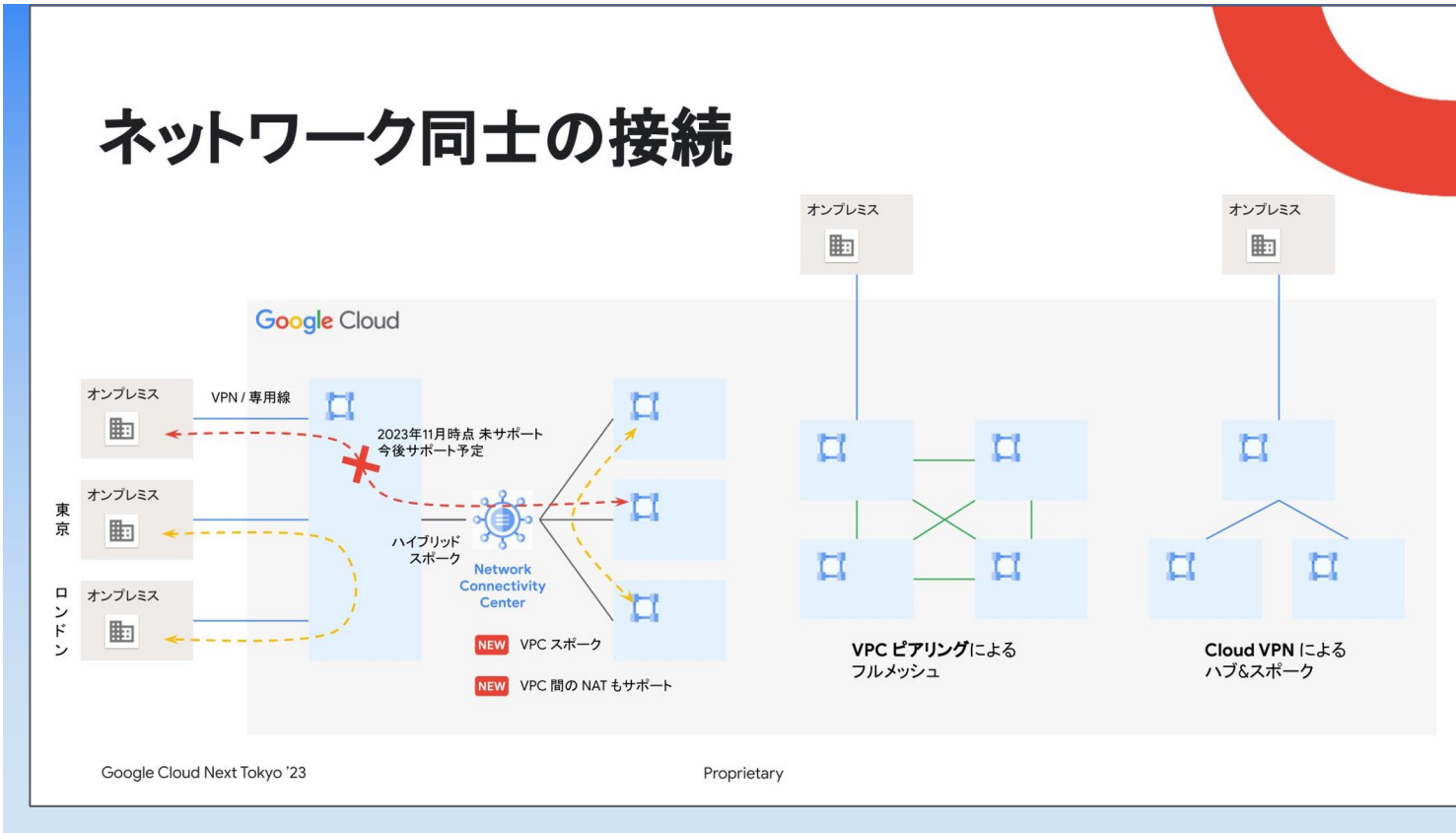


外部も内部もロード バランサーからサービスにつながる構成が基本

Google Cloud 内のネットワーク設計

Google Cloud へのサービス接続を構築するとき、ネットワークをどのように設計すればよいでしょうか。最もよくあるモデルは、Virtual Private Cloud（VPC）同士を VPC ピアリングのフルメッシュでつなぎ、そのうち 1 つの VPC を拠点にしてオンプレミスやほかのクラウド サービスと接続するというものです。また VPC を Cloud VPN でつなぎ、オンプレミスや他のクラウド サービスにつなぐ「ハブ アンド スポーク」というモデルも一般的です。

最近では、「Network Connectivity Center（NCC）」というサービスを利用するモデルが新しく登場しました。このモデルには大きく分けて 2 つの機能があります。1 つ目が、お客様の拠点間を Google Cloud のバックボーンを経由して接続する機能。2 つ目が、VPC 同士をフルメッシュでつなぐことなく、NCC をハブにして接続する機能です。「Cloud NAT」と併用することで、VPC のアドレスが重複していても接続できるのが特長です。残念ながら、この機能は 2023 年 11 月時点では未サポートで、今後サポートされる予定です。



Network Connectivity Center（NCC）を利用するモデルが新たに登場

他のクラウド サービスと接続する時のネットワーク設計

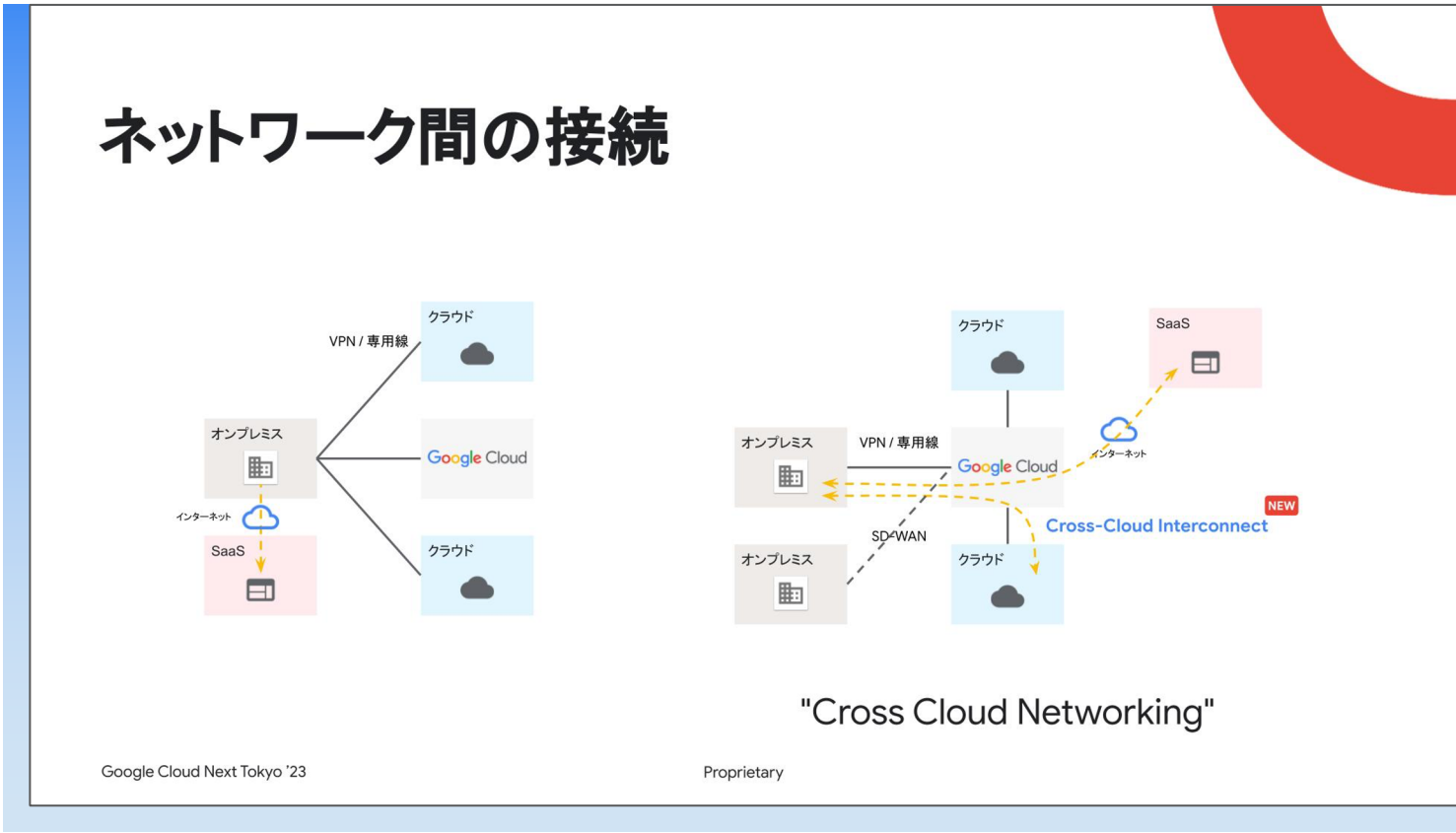
Google Cloud と他のクラウド サービスはどのようにつなげばよいでしょうか。

マルチクラウドを使っているお客様でよく見られるモデルは、オンプレミスから複数のクラウド サービスにつなぐもので、SaaS を使うときにはインターネット経由で接続します。オンプレミスがハブになり、クラウド サービスがスポークになりますが、このモデルはオンプレミスの負担が大きくなるので Google Cloud をハブとして利用するモデルをご提案しています。

Google Cloud では、「Cross-Cloud Interconnect」という、ほかのクラウド サービスをマネージドにより専用線でつなぐサービスをご提供しています。Cross-Cloud Interconnect は、Google Cloud コンソールで簡単な設定をするだけで、Amazon Web Services（AWS）や Microsoft Azure、Oracle Cloud Infrastructure（OCI）などのクラウド サービスを広帯域幅の専用線で接続できます。

お客様が Google Cloud にさえ接続すれば、専用線を通して他のクラウド サービスにも接続できますし、内部のプロキシを通れば SaaS への接続を Google Cloud 経由で行えます。オンプレミスが VPN や専用線、SD-WAN でつながっている場合には、SD-WAN そのものを Google Cloud で終端することも可能です。

先ほどご紹介したハブ アンド スポーク モデルと同じように、Google Cloud をハブにしてほかのクラウド サービスや SaaS と接続する構成を、Google Cloud では Cross Cloud Networking というソリューション名で展開しています。

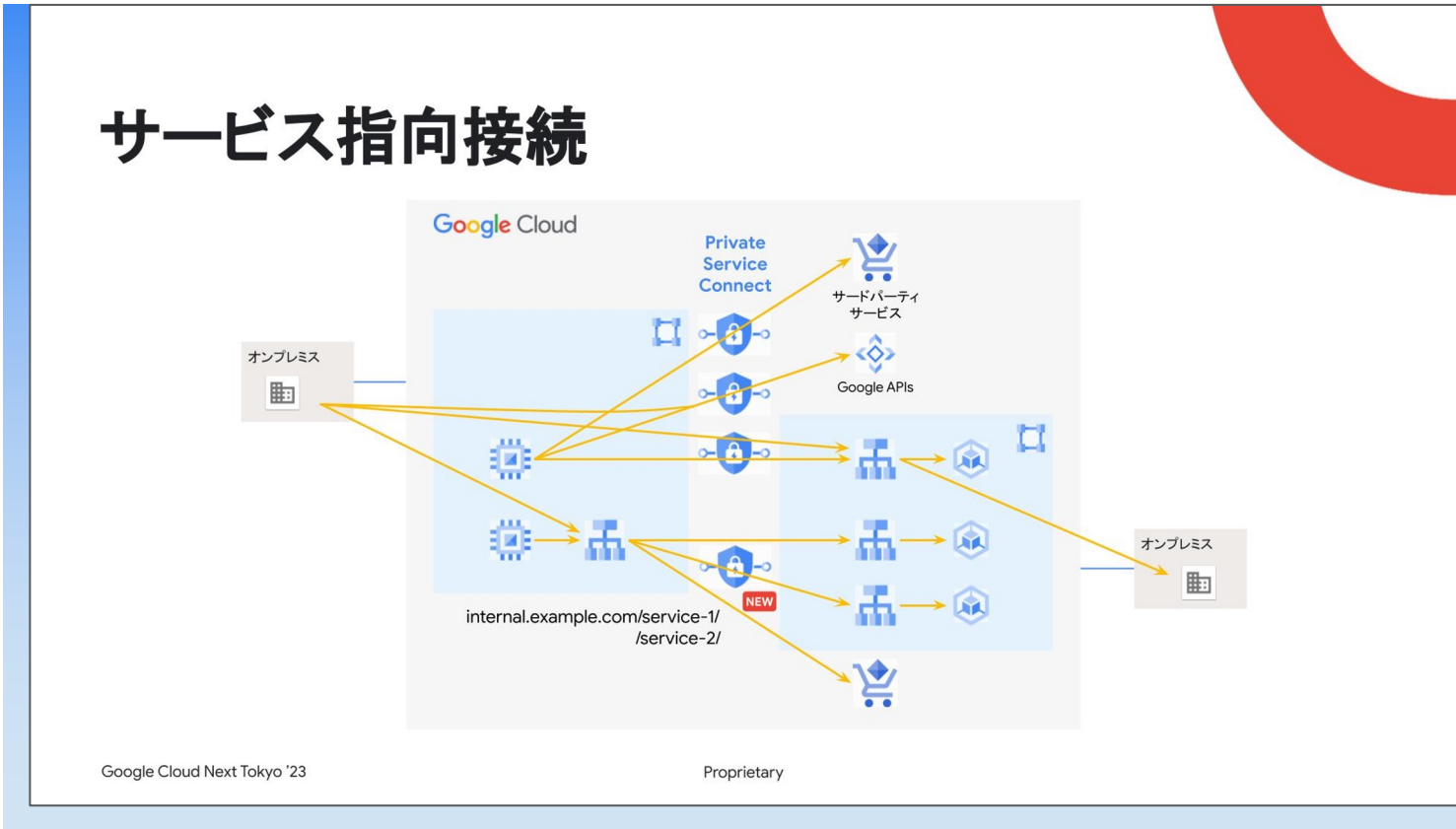


Google Cloud と他のクラウド サービスの接続方法

IP 接続を使わずに各サービスと接続する方法

また、IP 接続がなくても各サービスと接続できる「Private Service Connect」というサービスもあります。サービスを使う側にエンドポイントを作り、サービスを提供する側はアタッチメントを使うことで、ピアリングや VPN などの IP 上の接続がなくても Private Service Connect を通して仮想的に接続できます。

IP 接続がないので IP アドレスの重複を考える必要もなく、アクセス制限に関しても Private Service Connect 上で接続の許可/拒否を自動的に行えます。そのため、アクセス管理の負荷が大幅に軽減されます。



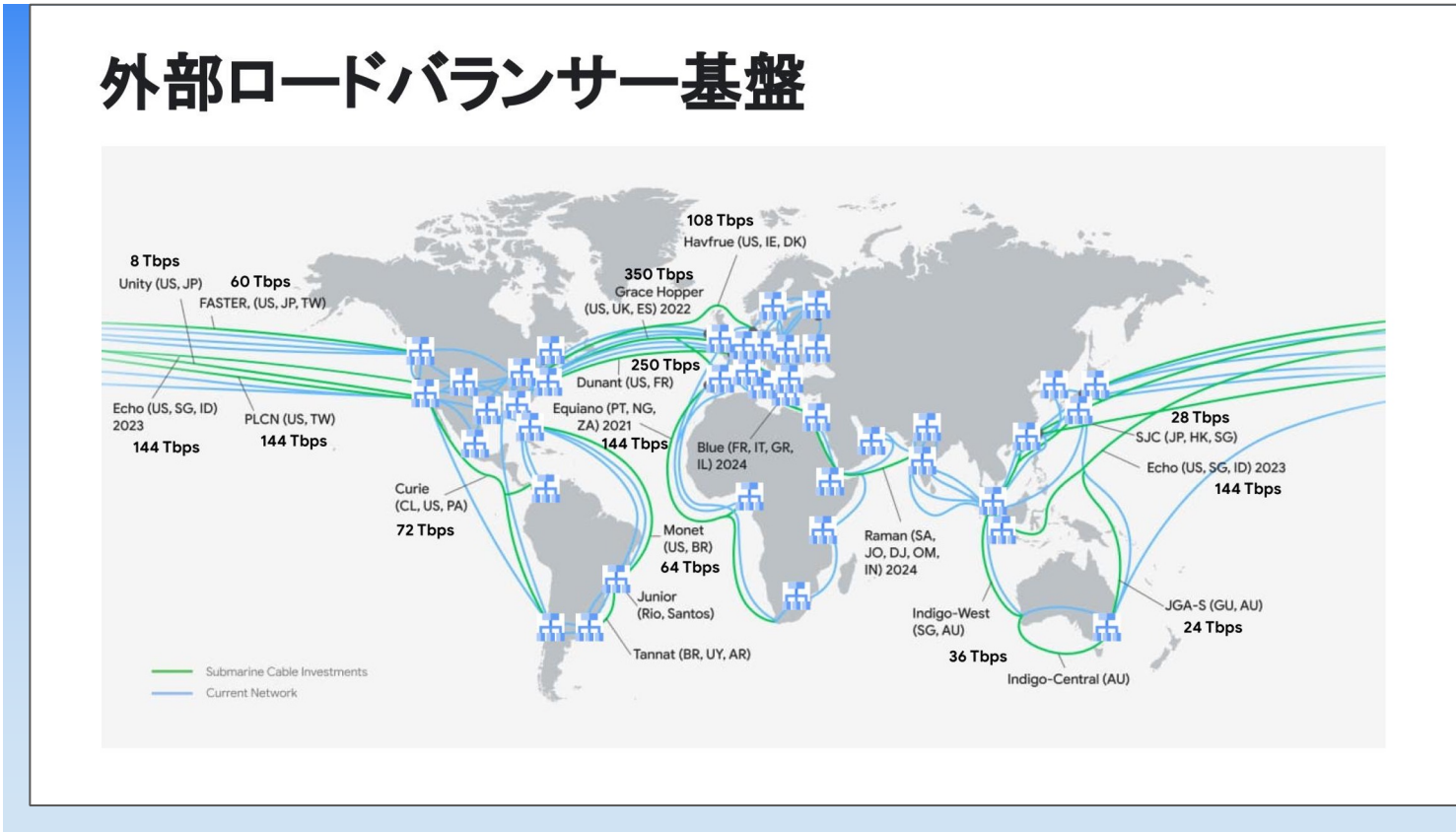
サービス指向接続でアクセス管理の負荷が大幅に軽減される

サービスを外部に公開する時の接続方法

次に、サービスを外部に公開する時の接続方法を解説します。

サービスを外部に公開する場合、Google Cloud 上にバックエンドを作り、これを外部に公開することで、エンドユーザーはインターネットからアクセスできるようになります。外部ロード バランサーは、エッジ ロケーションに実体があり、エッジ ロケーション上のサーバーで外部ロード バランサーの機能が動いています。

Google のグローバル ネットワークのエッジ ロケーションは、Google Cloud と全世界の ISP がつながっているポイントです。光ファイバーにより、Google Cloud のルータから 1 ホップで物理的に全世界の ISP と接続されます。エッジ ロケーションは海底ケーブルなどのバックボーンで接続されており、最大の帯域幅は 350Tbps です。

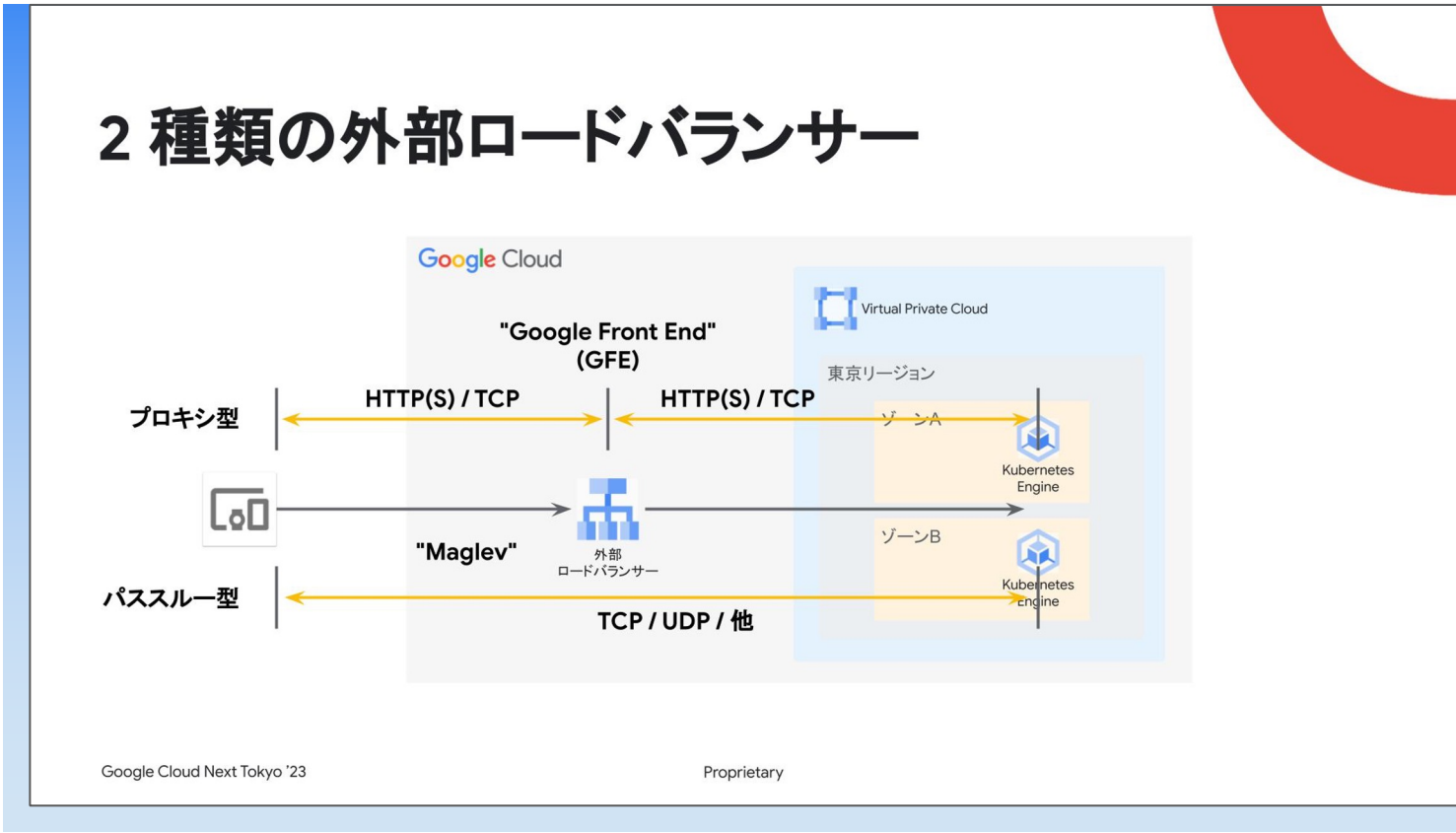


広帯域幅ネットワークを利用できるのが Google Cloud のメリット

2 種類の外部ロード バランサー

外部ロード バランサーには、プロキシ型とパススルー型の 2 種類があります。

プロキシ型は、クライアントからの接続を一度 Google Cloud のフロントエンドで終端します。これがエッジ ロケーションにあるサーバーで、「Google Front End（GFE）」と呼ばれます。一方、パススルー型は、エッジ ロケーションにある「Maglev」と呼ばれるロード バランサーによって、終端されることなくバックエンドまで送信されます。



外部ロード バランサーにはプロキシ型とパススルー型の 2 種類がある

プロキシ型のロード バランサーは、グローバル ロード バランサーとリージョナル ロード バランサーというように、さらに 2 種類に分けられます。グローバル ロード バランサーは、一般的に使われているロード バランサーであり、一方のリージョナル ロード バランサーは、例を挙げると東京リージョンでのみ利用できるロード バランサーです。

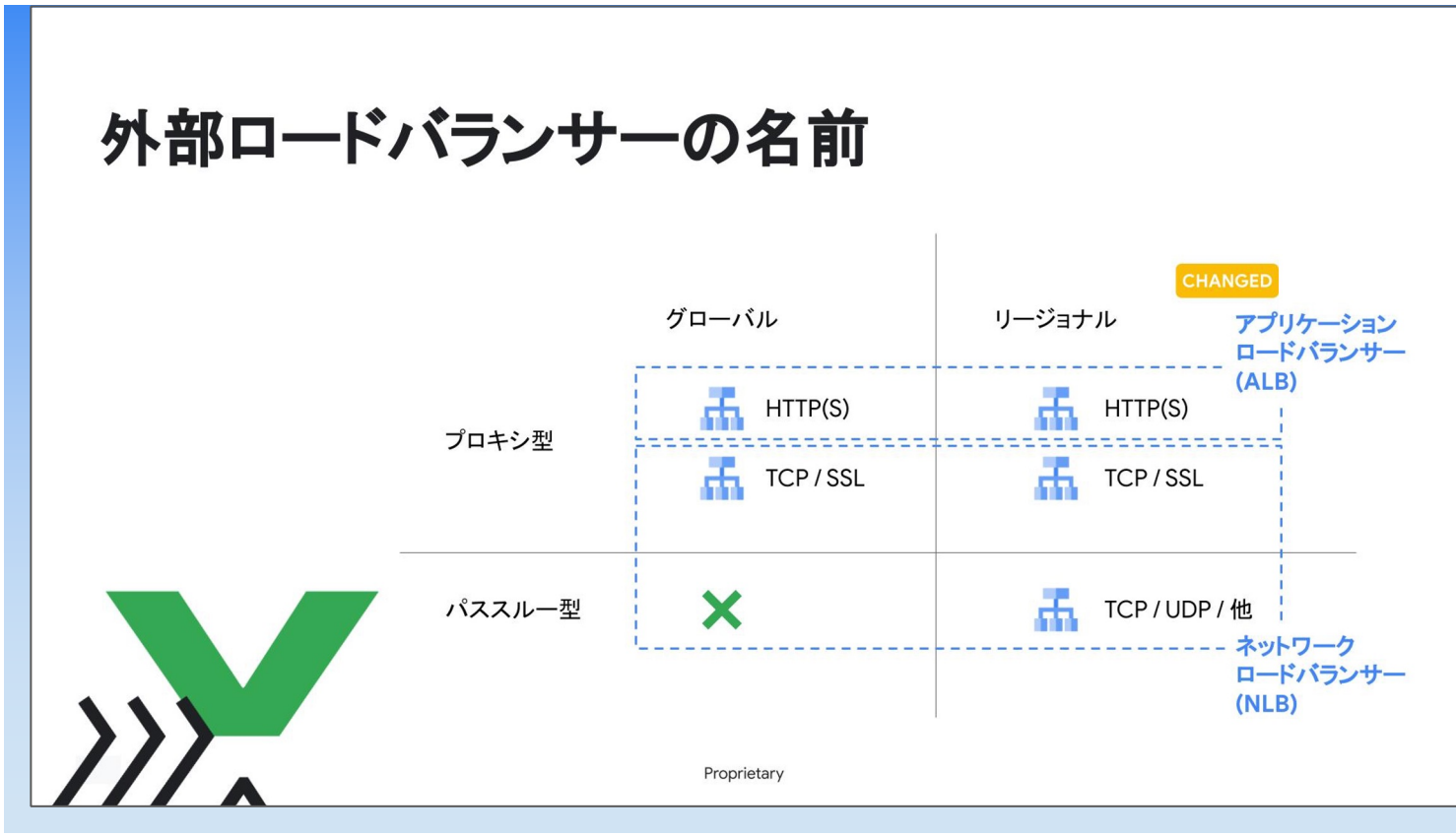
リージョナル ロード バランサーを使うのは、グローバル ロード バランサーを利用して東京リージョンだけにバックエンドを作るのと同じだと思うかもしれません。最大の違いはリージョナル ロード バランサーは実体がリージョンにあることです。

コンプライアンス上、リージョンが日本国内にあることが不可欠なお客様はリージョナル ロード バランサーの利用が適しています。それ以外はグローバル ロード バランサーの利用で問題ありません。

プロキシ型の外部ロード バランサーの名称は、以前は「HTTPS 負荷分散」でした。最近では、HTTP（S）を扱うロード バランサーを「アプリケーション ロード バランサー（ALB）」、TCP/UDP を使う外部ロード バランサーを「ネットワーク ロード バランサー（NLB）」という名称で呼びます。NLB にはプロキシ型とパススルー型の 2 つがあります。

注意が必要なのは、グローバル ロード バランサーは、あくまでエンドユーザーに最も近い場所で終端し、そこからどこかのリージョンのバックエンドにつながることです。パススルー型には「いったん終端する」という概念がないので、グローバルなパススルー型のロード バランサーはありません。

外部ロード バランサーの種類と名前をまとめると、以下の図のとおりです。



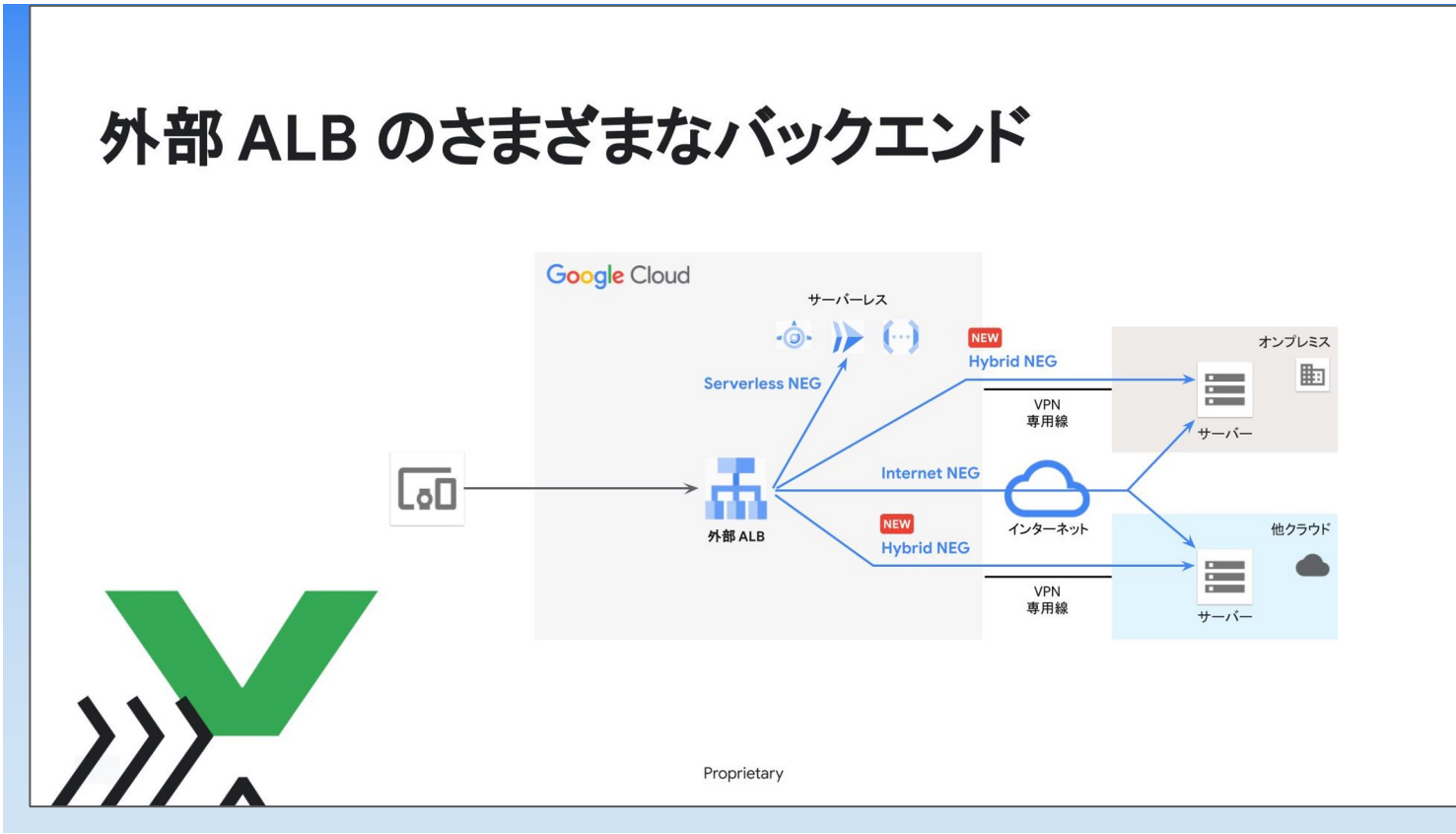
外部ロード バランサーの種類と名前

外部 ALB はさまざまなバックエンドに接続

外部 ALB のバックエンドの特長として、オンプレミスや他のクラウド サービスはもちろん、「App Engine」、「Cloud Run」、「Cloud Functions」などのサーバーレス サービスも接続できます。単に VM やコンテナでバックエンドを作るだけでなく、Cloud Functions を使って簡単な機能を 1 つのドメインの中で実現することもできます。

また「Internet NEG」や「Hybrid NEG」を利用して、インターネットや閉域網を越えてオンプレミスやクラウド サービスにつなぐことも可能です。バックエンドはそのままに、フロントエンドだけグローバル ロードバランサーを使いたい場合は、Google Cloud を利用することで、専用線を通してオンプレミスや他のクラウドサービスに接続できます。

さらに Cross-Cloud Interconnect を利用することで、簡単な設定で他のクラウド サービスへ接続可能です。これにより、オンプレミスから Google Cloud へのリフトを容易にコントロールできます。例えば既存のバックエンドをオンプレミスから Cloud Run に移行する場合、トラフィック管理機能を利用して、まずは 1% のトラフィックを Cloud Run に流して動作確認を行い、問題がなければ 100% のトラフィックを Cloud Run に切り替えるといったことが可能です。



外部 ALB のさまざまなバックエンド

なお、外部 ALB には、歴史的な理由によりバージョン 2（GFE2）とバージョン 3（GFE3）があり、GFE2 は「クラシック」と呼ばれています。少し前までは、GFE2 と GFE3 で機能が異なっていたので使い分けが必要でした。

現在は機能的な差はないので、特別な理由がない限り GFE3 を利用して問題はありません。GFE2 を使っているからといって GFE3 に移行する必要はありません。ちなみに GFE3 は、オープンソースのロード バランサーである Envoy をベースにしています。

キャッシュ インフラの 2 つの機能

外部向けにサービスを提供する時は、キャッシュが必要です。そのためのサービスが「Cloud CDN」です。以前 Cloud CDN にはチェック ボックスが 1 つしかなく、基本的にはキャッシュの TTL（Time To Live）を設定するだけで CDN の機能を利用できました。現在は、ネガティブ キャッシュや古いデータの提供など、新たな機能が追加されています。

Cloud CDN はロード バランサーと一緒に設定可能

キャッシュ インフラは、ロード バランサーと同じロケーションにあり、Cloud CDN と Media CDN という機能があります。Media CDN のキャッシュ インフラは、Google Cloud のインフラではなく、接続されている ISP 内にあります。Media CDN を ISP 内に置くことで、よりエンドユーザーに近いところでコンテンツの配信ができるので、パフォーマンスの向上とコストの削減が期待できます。

Media CDN は、ライブ配信や WebAssembly（Wasm）を使ったリクエストの調整もできるので、ぜひ試してほしい機能です。利用には事前に申し込みが必要なので、ビデオ配信、大規模ファイル ダウンロード、ライブ配信、サービス拡張が必要な場合、Google Cloud の担当者に問い合わせてください。

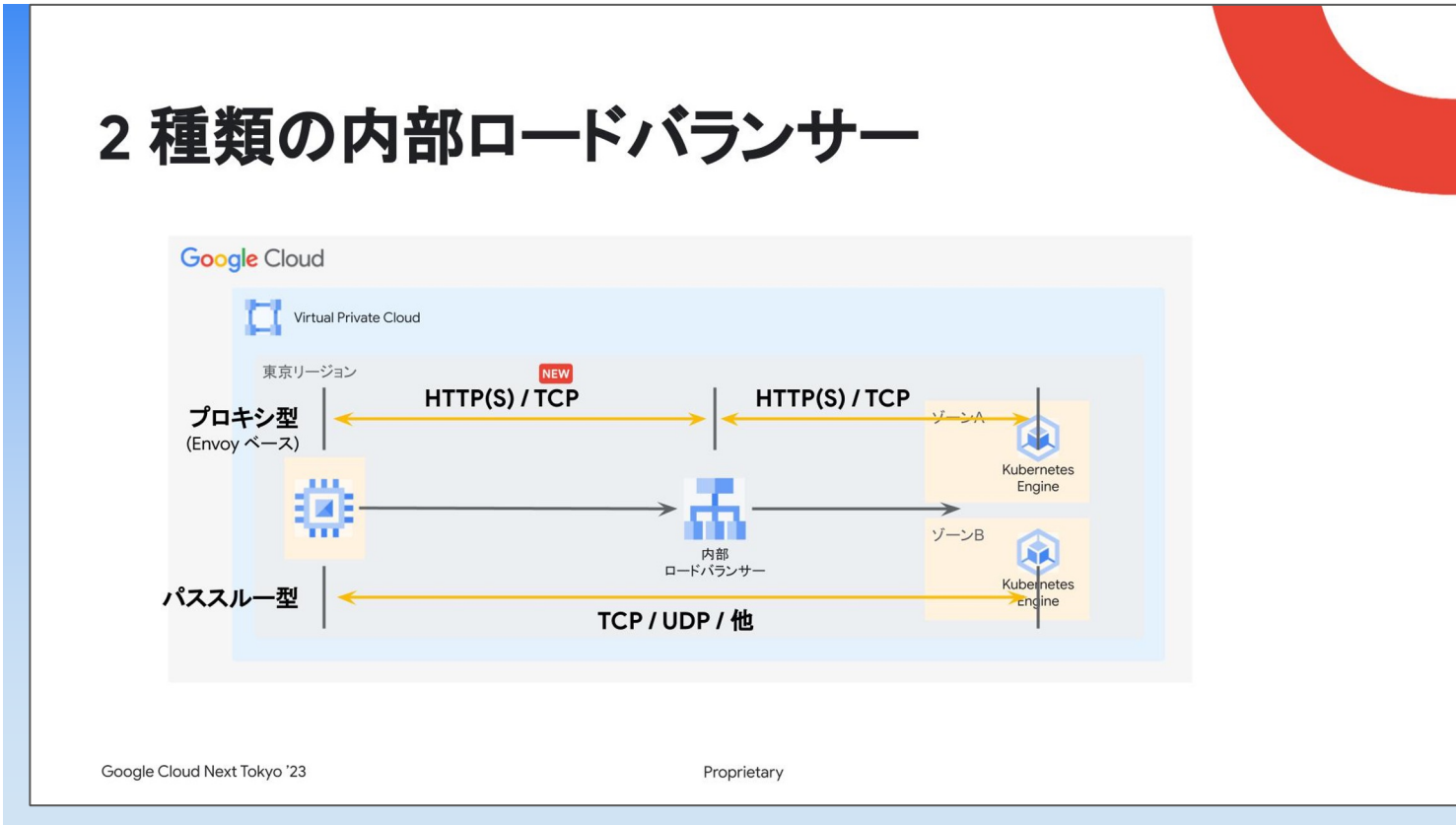
バックエンドを内部に公開する時の接続方法

バックエンドを内部に公開する場合の接続方法は、外部向けと大きく違いはありません。内部ロード バランサーは、外部ロード バランサーとは違い VPC 内の各リージョンにあり、プロキシ型とパススルー型の 2 種類の内部ロード バランサーで構成されます。

内部ロード バランサーと外部ロード バランサーの構成はほとんど同じですが、実装の観点では大きく異なります。外部ロード バランサーは全世界のロード バランサー基盤に分散されていますが、内部ロード バランサーは特にプロキシ型の場合、ロード バランサーの機能がお客様の VPC 内に構成されます。

プロキシ型の内部ロード バランサーは、バックエンドとして複数のリージョンを管理できる「クロス リージョン ロード バランサー」と 1 つのリージョンしか管理できない「リージョナル ロード バランサー」の 2 種類に分かれます。通常はクロス リージョン ロード バランサーを利用します。

一方、パススルー型はさらに特殊で、ロード バランサーの実体もありません。ロード バランサーを通して、クライアントがバックエンドにアクセスするときに、クライアントがどのバックエンドにアクセスするかを自分で決めます。Kubernetes のクラスタ内のロード バランサーと同じような仕組みです。



プロキシ型とパススルー型の違い

外部ロード バランサーには全世界にインフラがあるので、1つが停止しても問題ありません。しかし、内部ロード バランサーの場合は、リージョンが停止すると問題です。この事態を解決できるのが、「Cloud DNS」です。

Cloud DNS は、ヘルスチェック機能で内部ロード バランサーに対してヘルスチェックを行います。その結果停止していれば、別のリージョンのロード バランサーにフェイル オーバーします。内部 ALB のバックエンドに関しては、外部ロード バランサーとほぼ同じですが、現状ではサーバーレスのサービスとして Cloud Run しか使えない点には注意が必要です。

外部ロード バランサーも内部 ALB も共有 VPC により、ロード バランサーの責任分担が、よりフレキシブルにできるようになりました。これまでは、サービス プロジェクトがロード バランサーを管理しなければならず、アプリ開発チームがロード バランサーも管理する必要がありました。

またホスト プロジェクトがロード バランサーを管理できるようになったことで、ロードバランサーの実体はインフラチームが管理し、バックエンドだけを各アプリ開発チームで管理できます。そのため、アプリ開発チームはアプリケーション開発に集中できます。

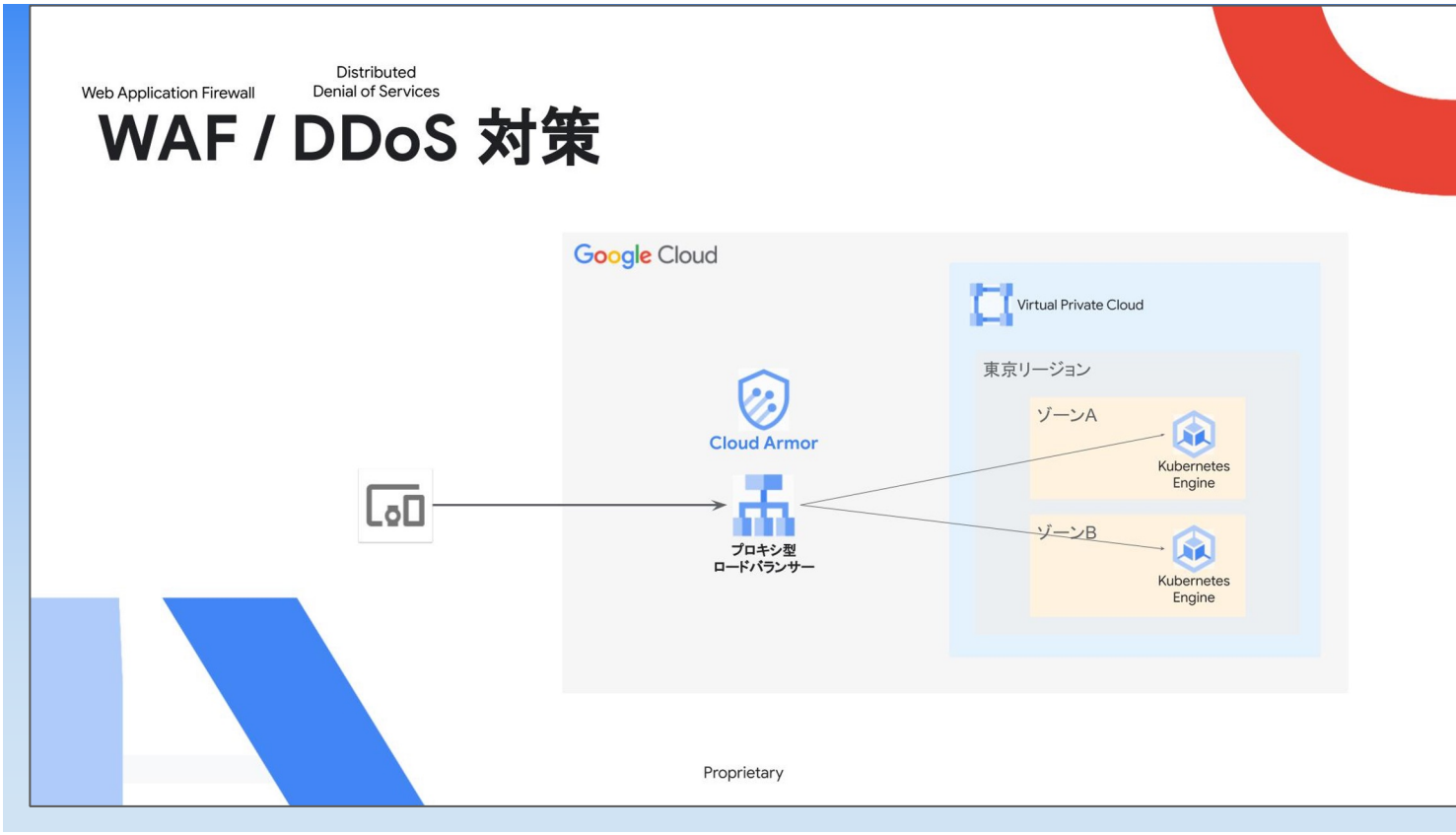
外部ロード バランサー、内部 ALB には多くの種類があるので、「ロード バランサーの選択」を参照してください。またロード バランサーの種類ごとの機能の差異は、「ロード バランサーの機能比較」を参照してください。

ロード バランサーの選択や機能比較は Google Cloud のドキュメントを参照。

WAF/DDoS 対策機能

WAF/DDoS 対策としては、「Cloud Armor」を展開しています。Cloud Armor は、ロード バランサーと同じエッジ ロケーションで動いています。

エッジ ロケーションでは、ロード バランサー、キャッシュ、WAF/DDoS 対策が提供されています。WAF の機能はバックエンドにあるイメージですが、Cloud Armorではエンドユーザーに一番近いエッジ ロケーションで攻撃を防御しているため、リクエストがバックエンドまで来ることはありません。



Google Cloud では WAF/DDoS 対策として Cloud Armor を提供

Cloud Armor の機能は、以下のとおりです。

- **WAF ルール**
- **DDoS 防御**
- **アクセス制御（IP、地域、AS 番号）**
- **ボット管理（reCAPTCHA 連携）**
- **レートリミット**
- **適応型 DDoS 防御（機械学習ベース）**
- **高度なレイヤ 3/レイヤ 4 DDoS 防御**
- **脅威情報にもとづく防御**

ここで特に言及したいのは「レートリミット」と「脅威情報にもとづく防御」です。

レートリミットは、例えば「1 クライアント、1 秒あたり 10 リクエストまでしか受け付けないようにする」などの制限を設ける機能です。これによって、パスワード リスト攻撃などを防ぐことができます。脅威情報に基づく防御は、IP アドレスのカテゴリ情報を利用して、過去の情報に基づいて攻撃をブロック可能です。

これまではプロキシ型のロード バランサーでの利用を想定していましたが、新しく搭載された高度なレイヤ 3/レイヤ 4 DDoS 防御により、パススルー型のロード バランサーでも防御できるようになりました。Cloud Armor には、今後も新しい機能を追加していく計画です。

証明書サービスである「Certificate Manager」については、コンソールからの設定はできませんが、gcloud コマンドで簡単に設定が可能です。これまでのロード バランサーの証明書は、ワイルドカードが使えない、設定できる件数が少ないなどの課題がありましたが、Certificate Manager は、DNS の認証も、ワイルドカードも容易に設定できます。

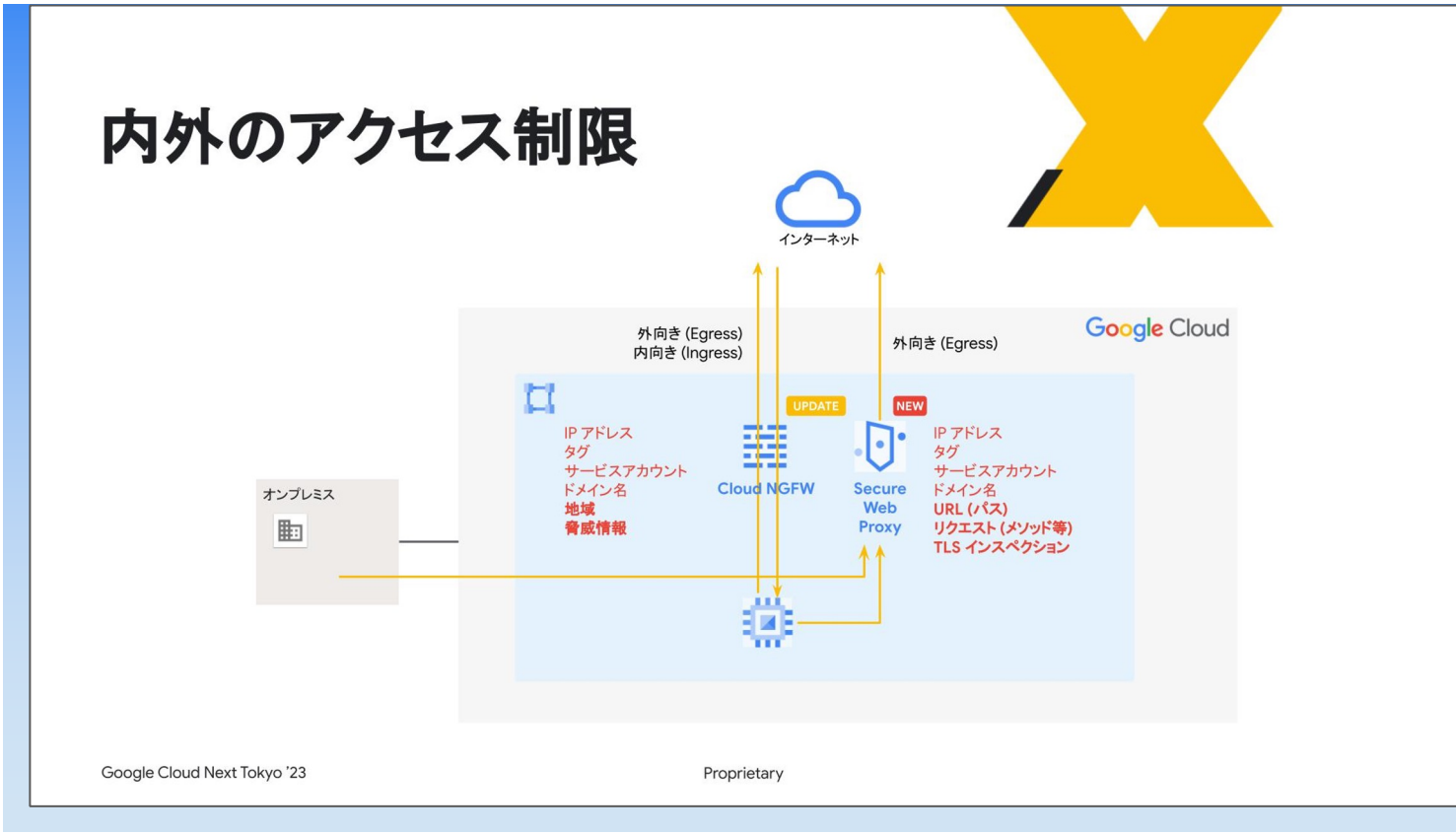
また、これまで内外のアクセス制限は「Cloud Firewall」が使われていましたが、現在は「Cloud NGFW」にアップグレードされています。Cloud NGFW はドメイン名や地域、IP アドレスの脅威情報などを使ったフィルタリングが可能です。

Cloud NGFW の機能は、以下のとおりです。

- **グローバル/リージョナル ファイアウォール ポリシー**
- **「タグ」との統合**
- **ステートフル インスペクション**
- **アドレス グループ**
- **脅威情報にもとづく防御**
- **ドメイン(FQDN)ベース フィルタリング**
- **地域情報ベース フィルタリング**
- **IPS（Intrusion Prevention System）**

IP アドレスやドメイン名だけでなく、HTTP（S）のパスなど、より細かい制限をしたい場合、Secure Web Proxy を使えば、フルプロキシの機能により URL などを確認しながらコントロールできます。この場合、オンプレミスで運用していた出口となるプロキシを、Secure Web Proxy でクラウド側に移すことでプロキシの運用管理の負荷を軽減できます。

侵入検知のサービスとしては、「Cloud IDS」を提供していましたが、Cloud IDS だけでは検知はできても防御まではできないことが課題でした。今回、Cloud NGFW に IPS（Intrusion Prevention System）の機能が実装されたことで、ネットワーク構成はそのままに、侵入検知だけでなく、防御の機能を追加できるようになりました。



Cloud NGFW はパロアルト ネットワークスのエンジンを採用しており高い精度を実現

ここまで、ネットワーク サービスの変遷や発展についてお話してきました。ネットワークの設計をする人の「何ができるようにするか」、「どれくらい簡単にするか」、「どれだけ自動化するか」という構想を支援する機能が、Private Service Connect にはどんどん増えています。ロード バランサーにもさまざまな機能が追加されており、外部のサービスとの接続や種類がそろってきたので、アプリケーション開発やデプロイメントと併せてご検討ください。

参照リンク

1. Google Cloud ネットワーキング プロダクトの概要
2. 大解剖！Google Cloud ネットワーキング サービス アーカイブ動画視聴ページ

製品、サービスに関するお問い合わせ

goo.gl/CCZL78

Google Cloud の詳細については、上記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。

Google Cloud