

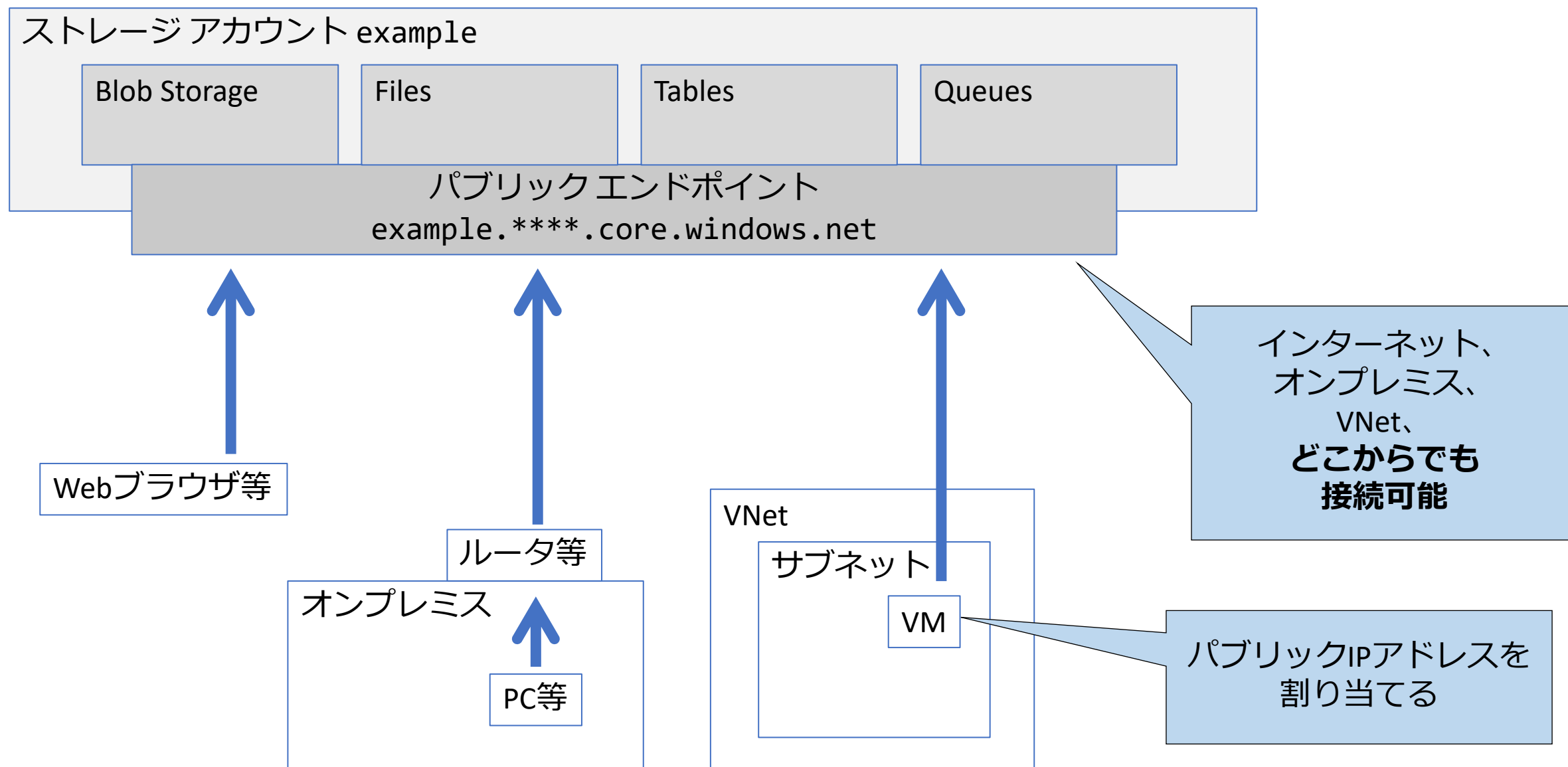
サービス エンドポイント
と
プライベート エンドポイント

	サービスエンドポイント	Private Link (プライベートエンドポイント)
概要	重要な Azure サービス リソースへのアクセスを仮想ネットワークのみに限定することができます。	仮想ネットワーク内のプライベートエンドポイント経由で Azure PaaS サービス (Azure Storage、SQL Database など) にアクセスできます。
サービスへのパブリックアクセスからの遮断	リソースへのパブリック インターネット アクセスを完全に排除し、仮想ネットワークからのトラフィックのみを許可することにより、セキュリティが強化されます。	パブリック インターネット にサービスを公開する必要はありません。
パブリック IP	VNet 内のプライベート IP アドレスは、VNet 上のパブリック IP アドレスを必要とせずに、Azure サービスのエンドポイントに接続できます。	接続元または接続先にパブリック IP アドレスを使用せずに、Azure 内のサービスに仮想ネットワークを接続できます。
トラフィックの経路	Azure のバックボーン ネットワーク上で最適化されたルートを介して、Azure サービスに安全に直接接続できます。	仮想ネットワークとサービスの間のトラフィックは、Microsoft のバックボーン ネットワークを通ります。
名前解決	Azure サービスの DNS エントリは変わらず、引き続き Azure サービスに割り当てられているパブリック IP アドレスに解決されます。	完全修飾ドメイン名 (FQDN) を使用してプライベート リンク リソースに接続する場合は、割り当てられたプライベート IP アドレスに解決されるように DNS 設定を正しく構成することが重要です。ホストファイル/プライベート DNS ゾーン/DNS フォワーダーを使用して設定します。
ルーティング	エンドポイントは常に、ご利用の仮想ネットワークから Microsoft Azure のバックボーン ネットワーク上のサービスへのサービス トラフィックを直接受け取ります。	(システム ルートの「仮想ネットワーク」に該当)

[Azure 仮想ネットワーク サービス エンドポイント | Microsoft Docs](#)

[Azure Private Link とは | Microsoft Docs](#)

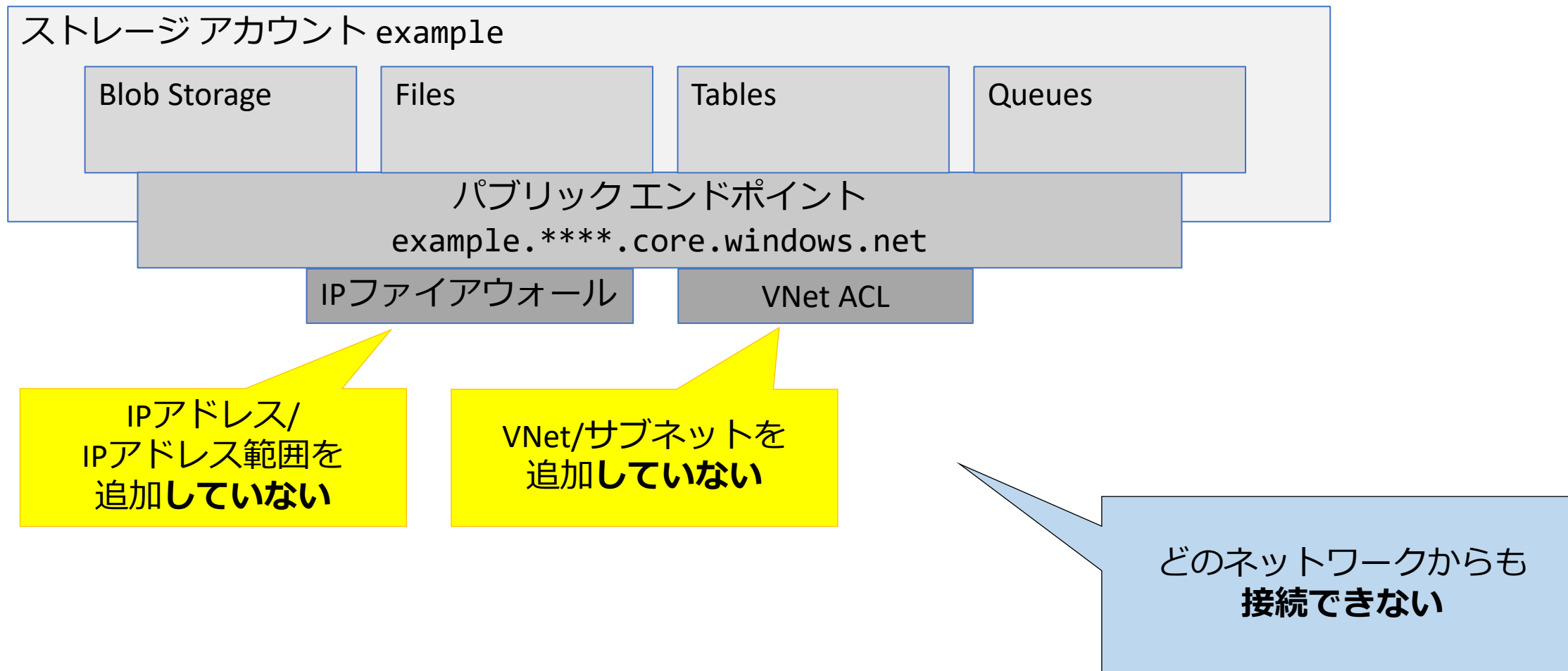
ストレージアカウントの設定＞許可するアクセス元：「すべてのネットワーク」



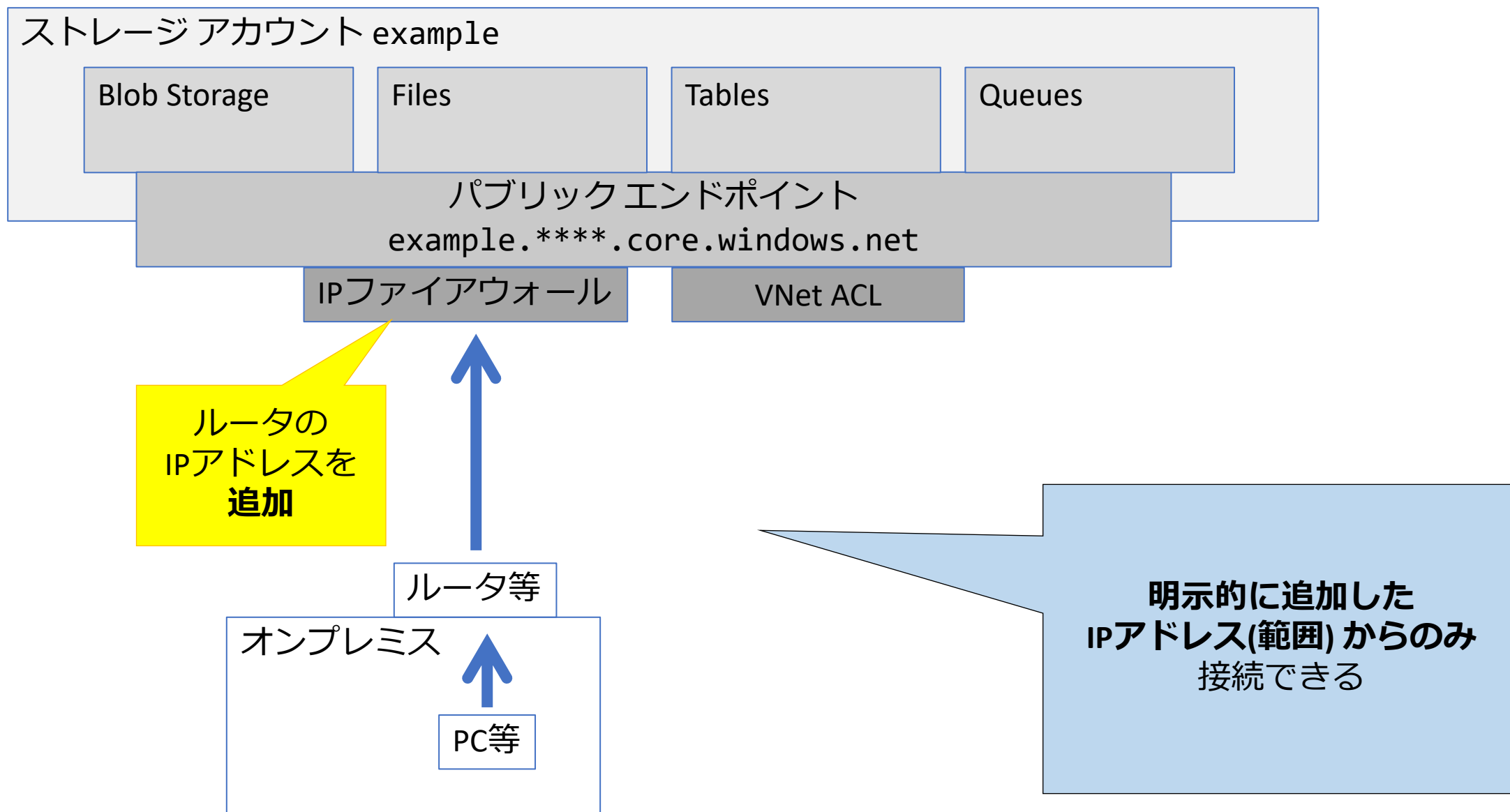
※正確には、パブリックエンドポイントは Blob や Files などのサービスごとに存在する

※実際にデータにアクセスできるかどうかは 認証などの設定の状況による

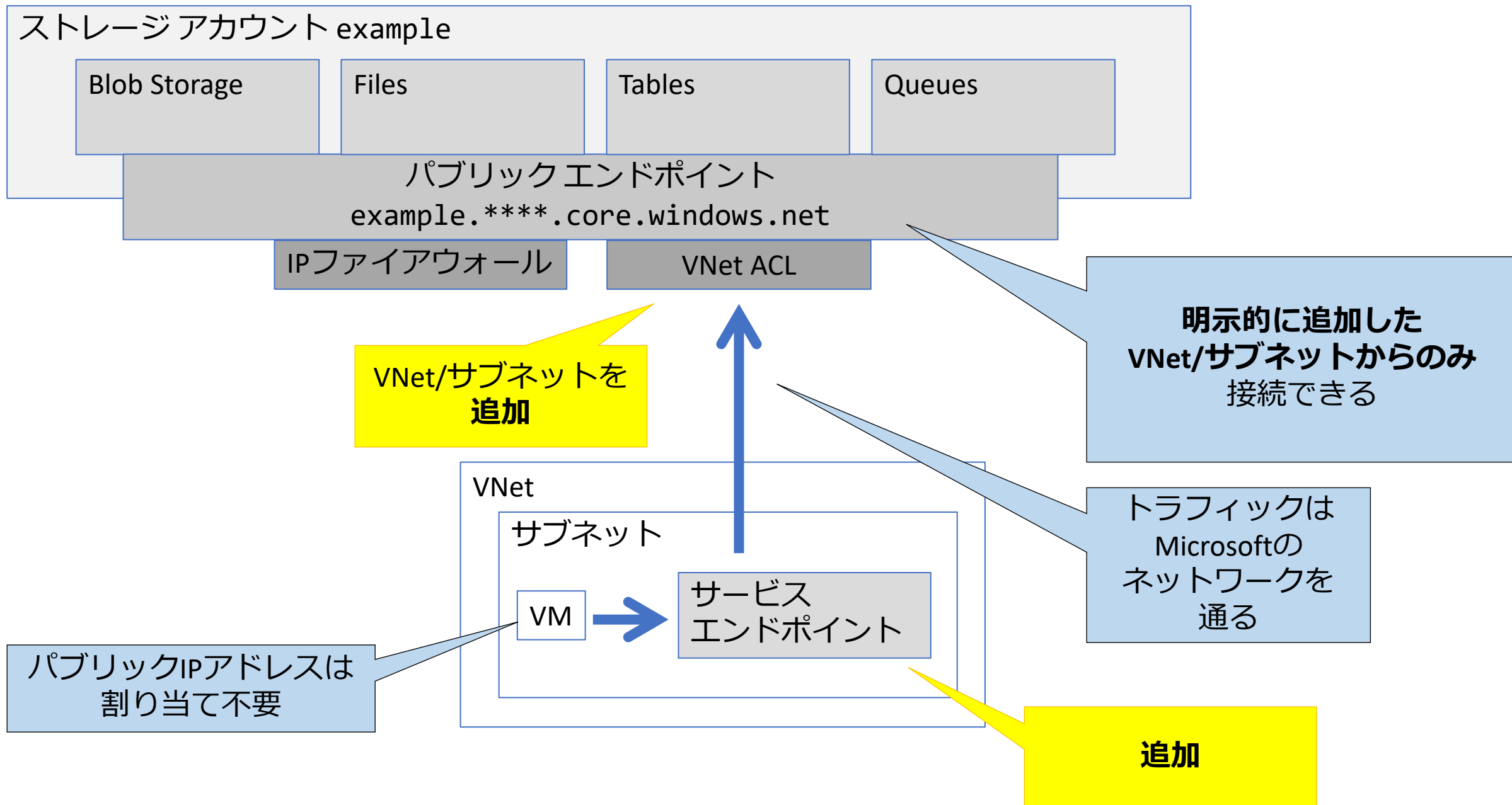
ストレージアカウントの設定> 許可するアクセス元：「**選択されたネットワーク**」



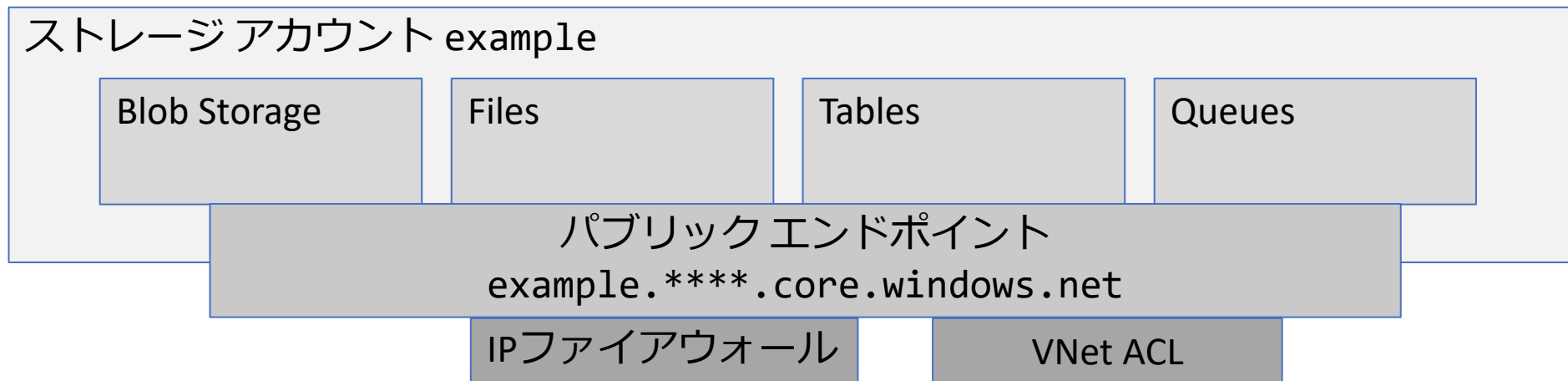
ストレージアカウントの設定> 許可するアクセス元：「選択されたネットワーク」



サービスエンドポイント



ストレージアカウントの設定＞許可するアクセス元：「**選択されたネットワーク**」

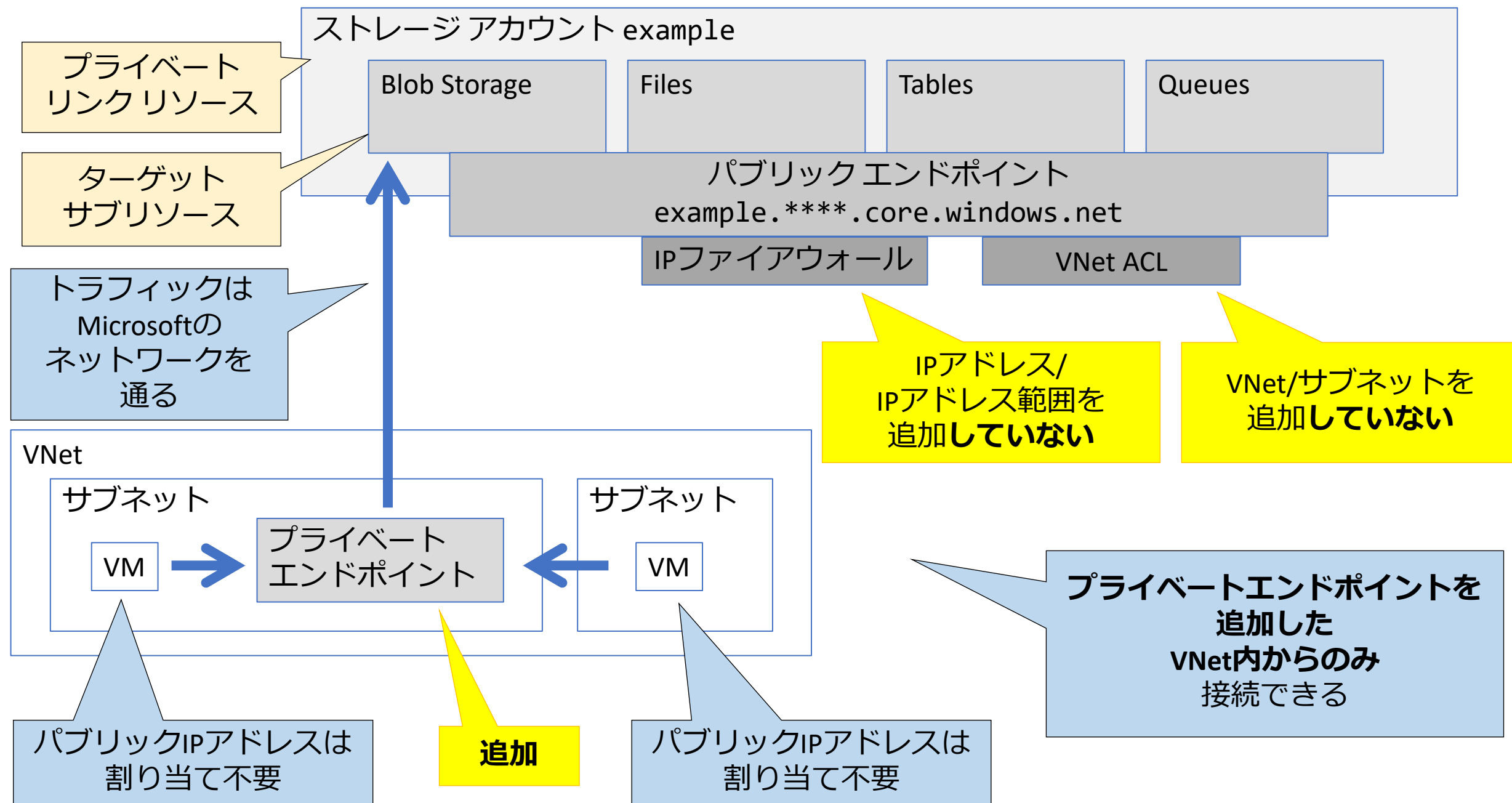


IPアドレス/
IPアドレス範囲を
追加していない

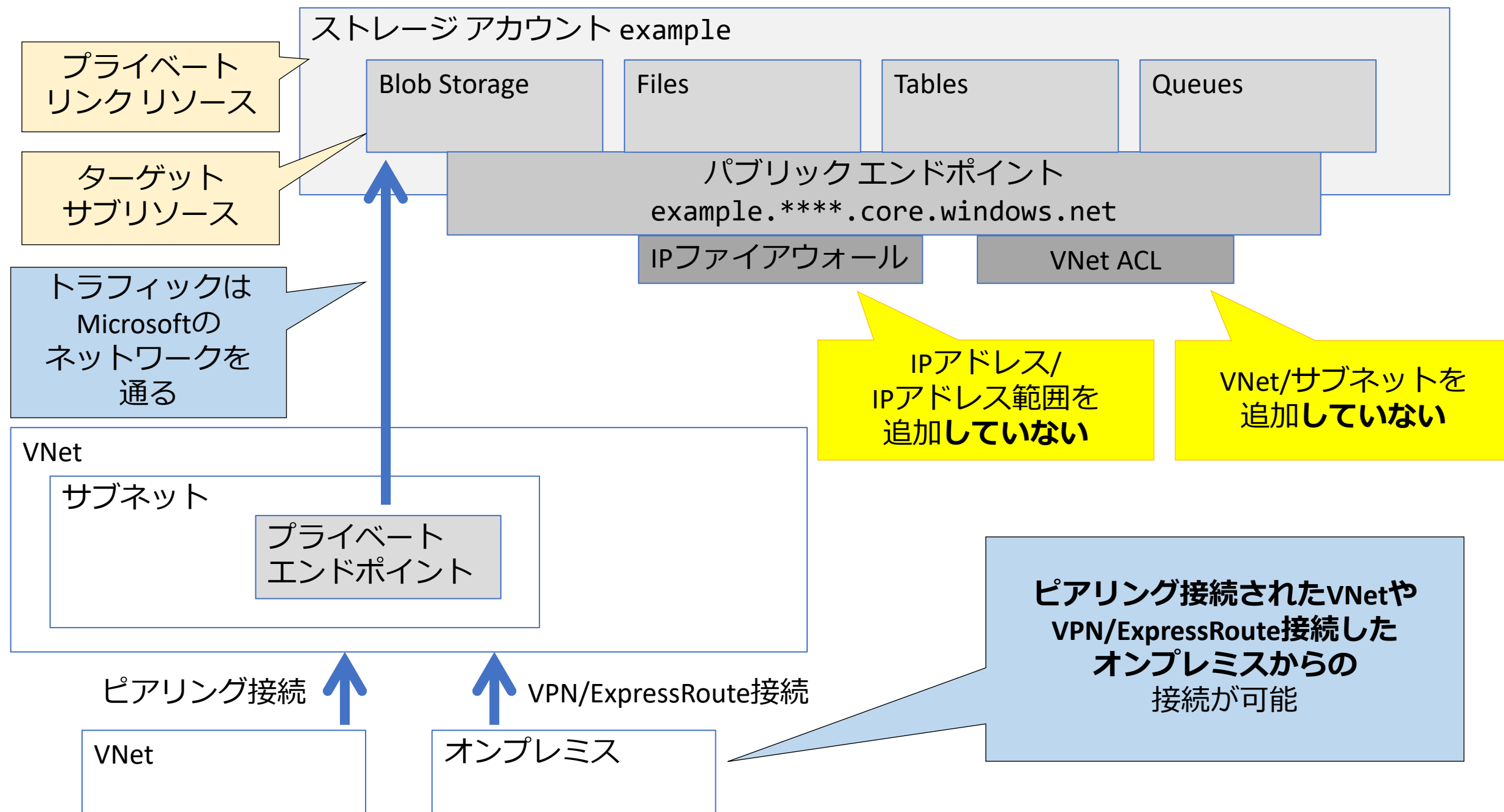
VNet/サブネットを
追加していない

どのネットワークからも
接続できない

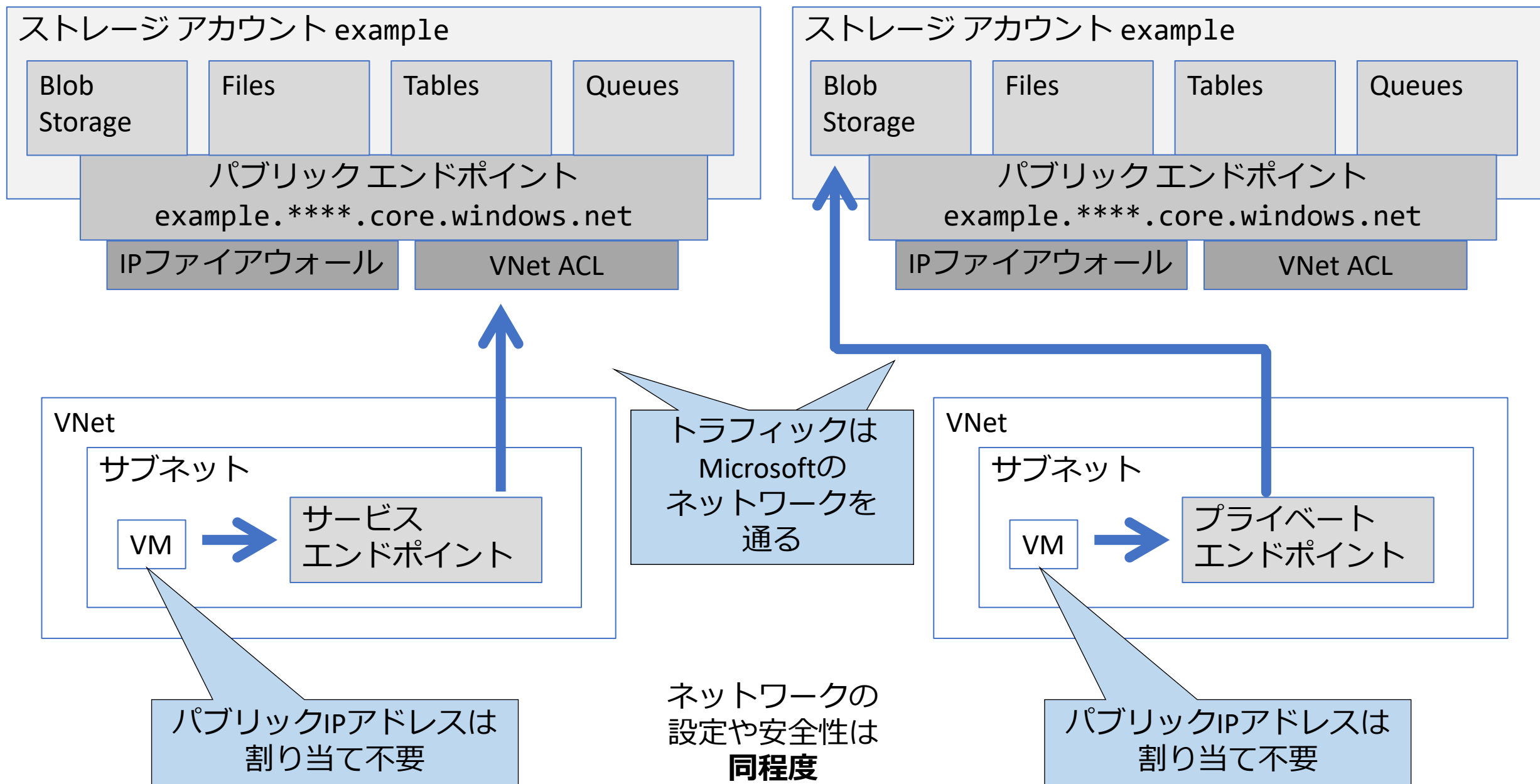
プライベートエンドポイント



プライベートエンドポイント



サービスエンドポイント vs プライベートエンドポイント



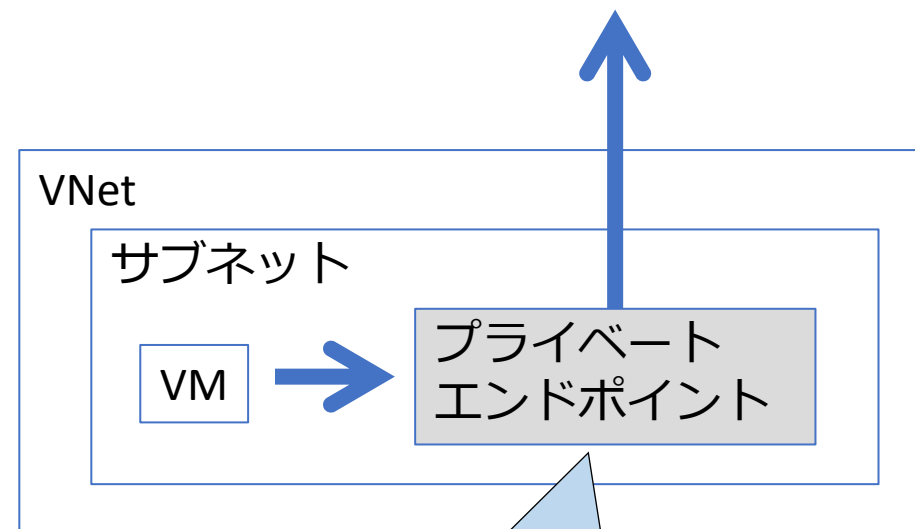
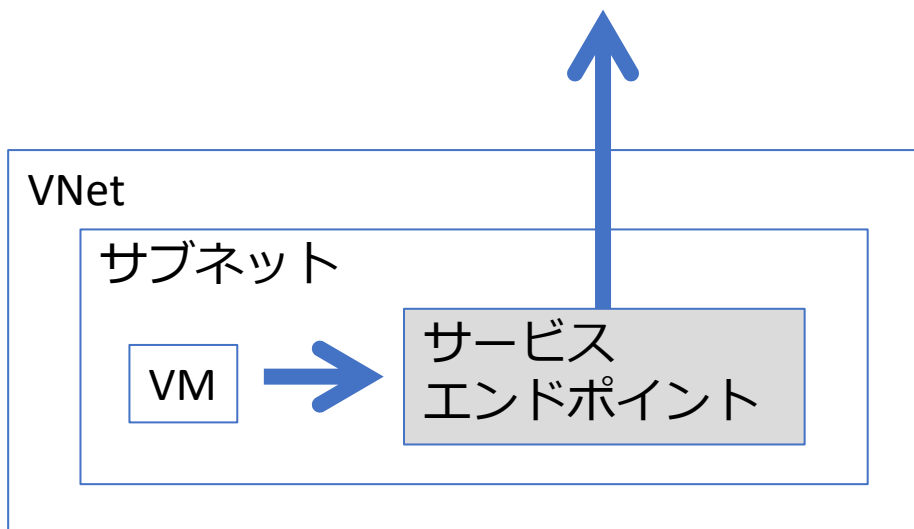
サービスエンドポイント vs プライベートエンドポイント

対応サービス

14種類

対応サービス

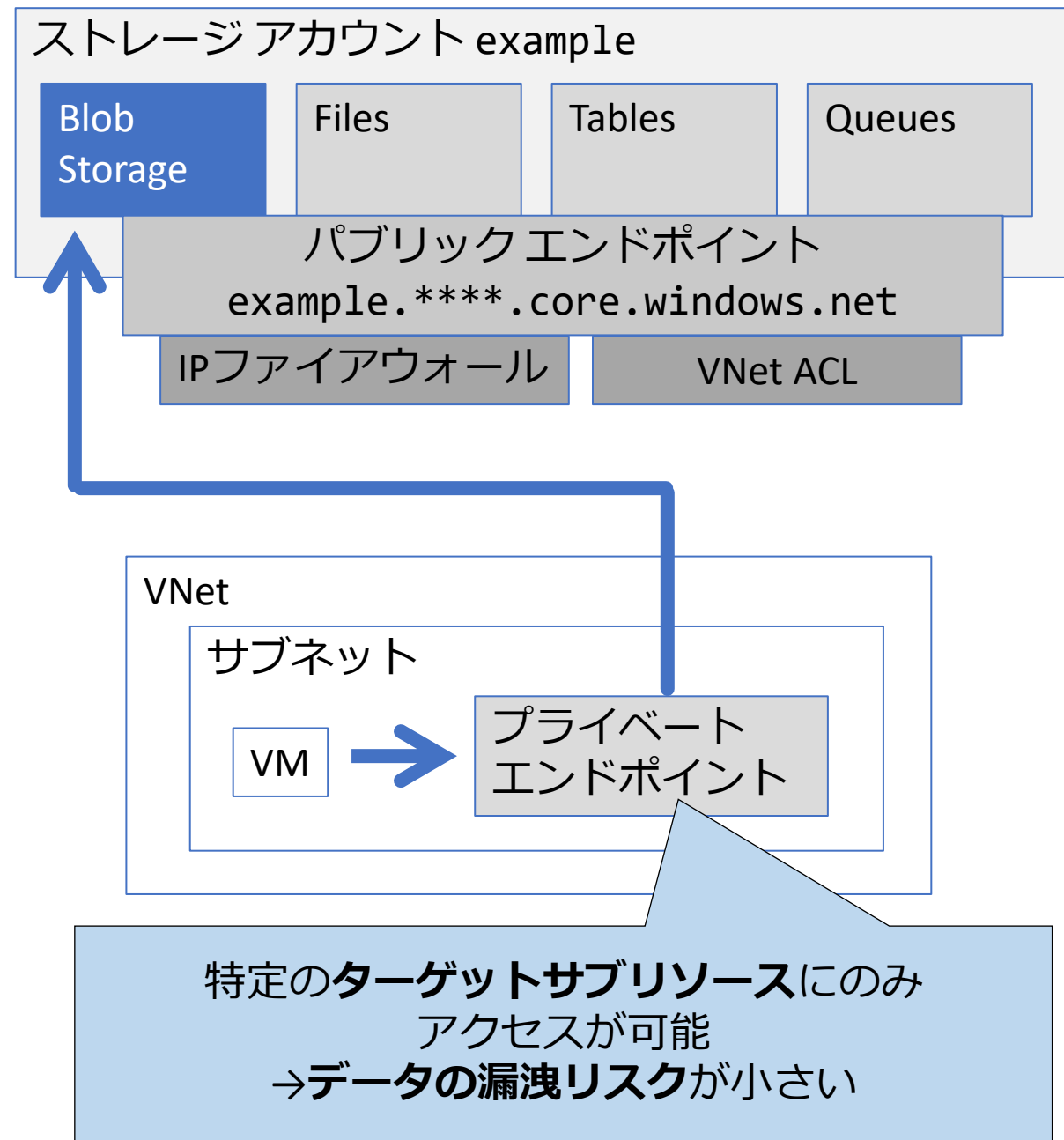
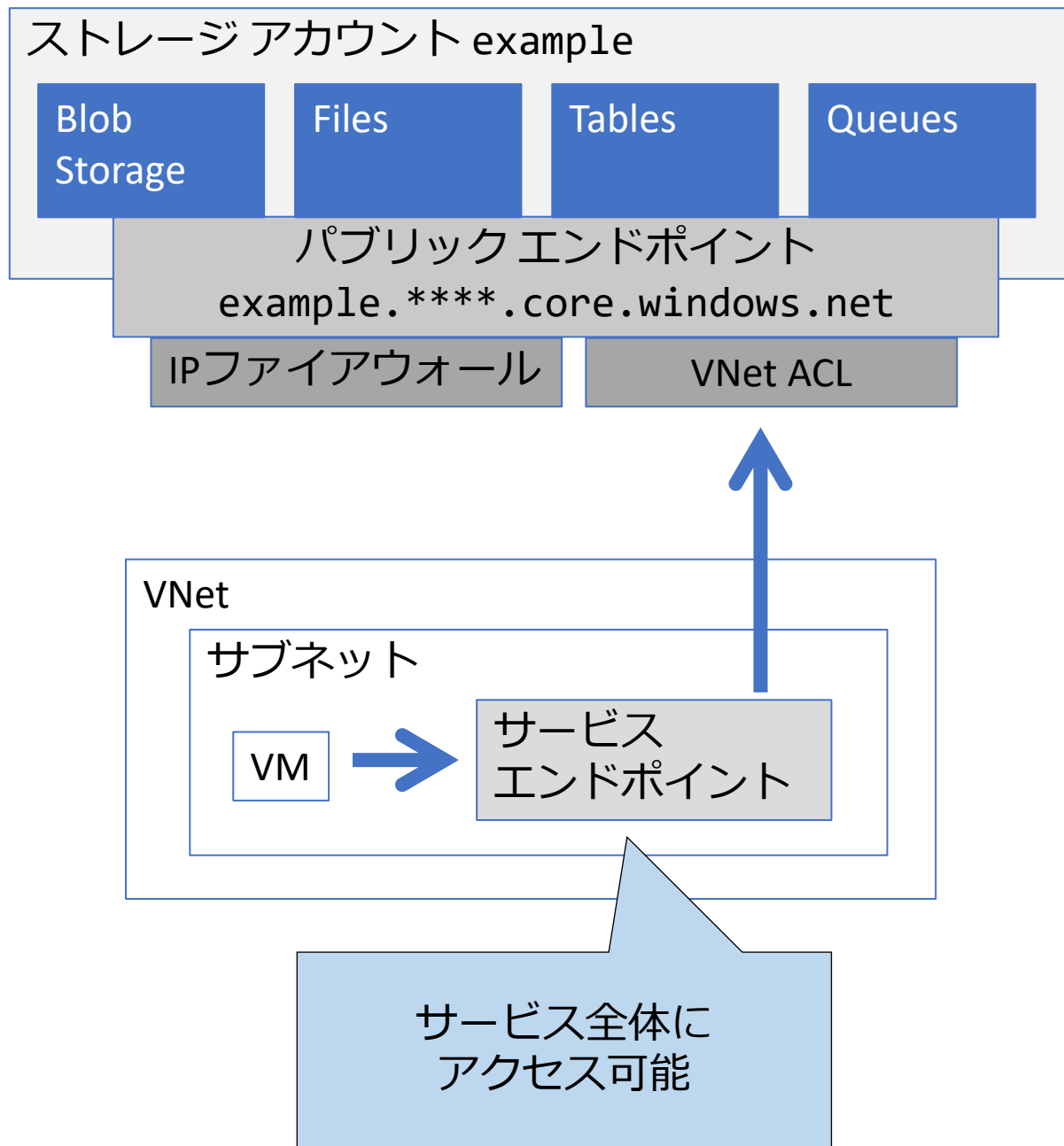
30種類



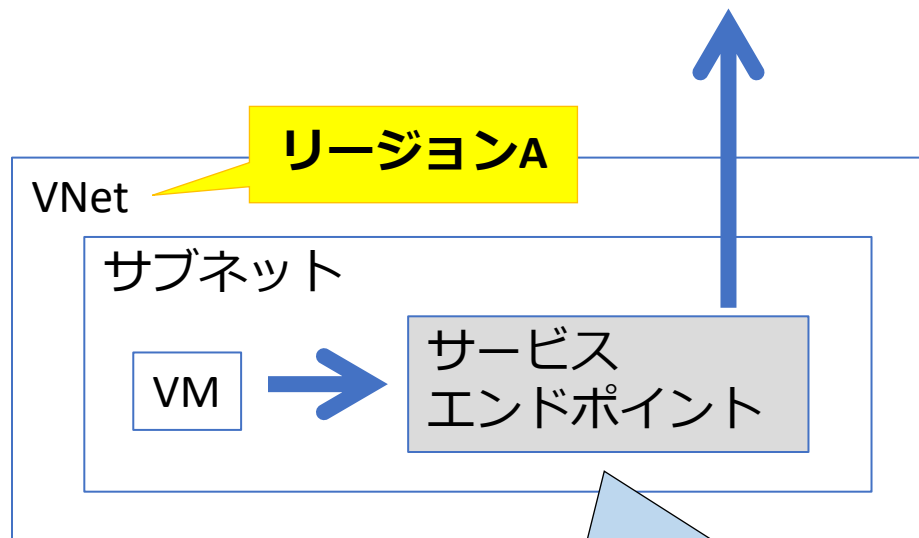
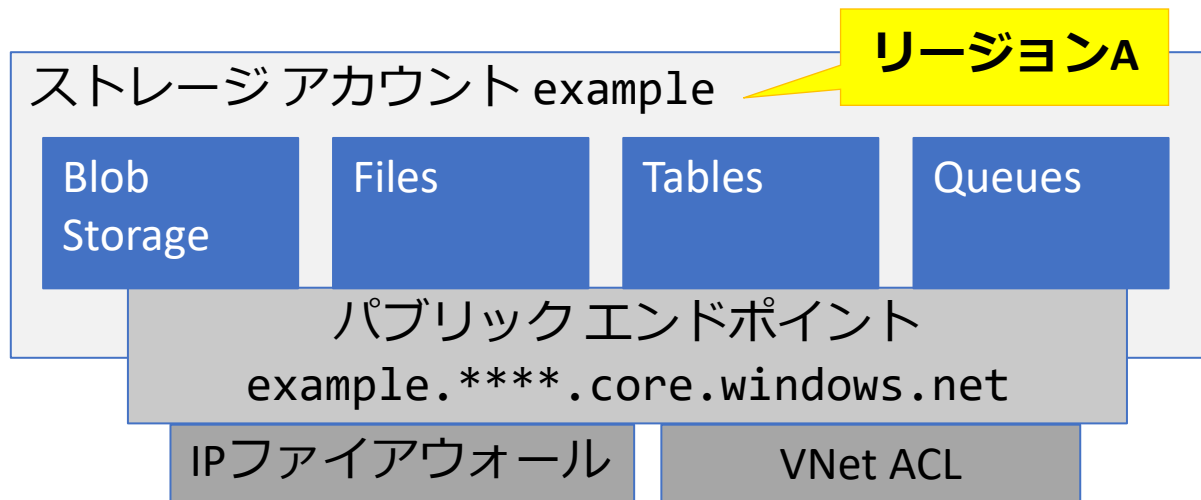
より多くの
サービスをサポート

※ 両方に対応しているサービス、
片方にだけしか対応していないサービスも一部存在

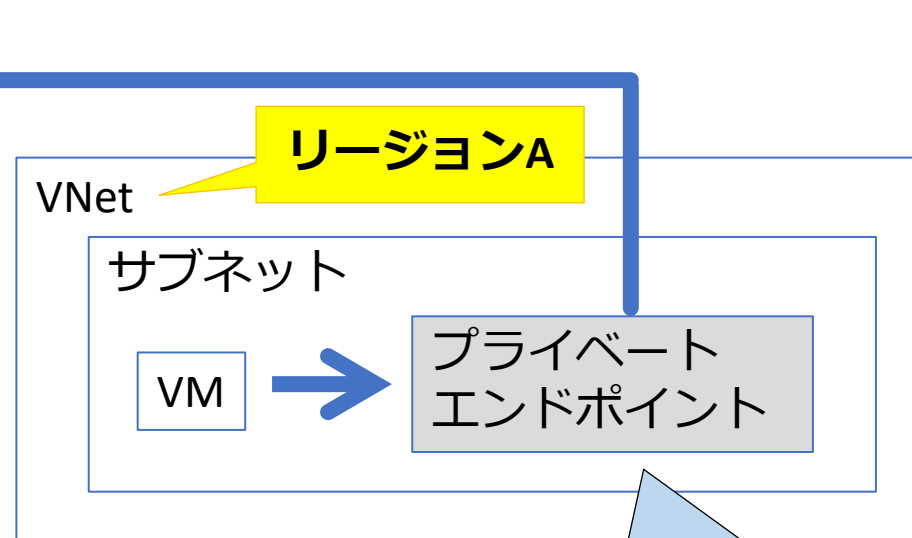
サービスエンドポイント vs プライベートエンドポイント



サービスエンドポイント vs プライベートエンドポイント



同一のリージョンでなければならない
※ストレージ、SQLの場合



異なるリージョンの
サービスに接続できる
→グローバル展開がしやすい

サービスエンドポイント vs プライベートエンドポイント

サービス エンドポイントの使用に
追加料金はかかりません。

プライベート エンドポイント	\$0.01 / 時間
受信データ処理量	\$0.01/GB
送信データ処理量	\$0.01/GB

* データ処理量の料金はトラフィックの方向に基づきます。たとえば、プライベート エンドポイント経由でストレージ アカウントに書き込んでいる場合、送信データ処理量に対して支払います。同じように、プライベート エンドポイント経由でストレージ アカウントから読み込んでいる場合、受信データ処理量に対して支払います。

** 上記の価格は Azure Private Link のプレミアム料金です。データ転送には引き続き、データ転送の料金が適用されます。

サービス
エンドポイント

プライベート
エンドポイント

有料

サービスエンドポイント vs プライベートエンドポイント

