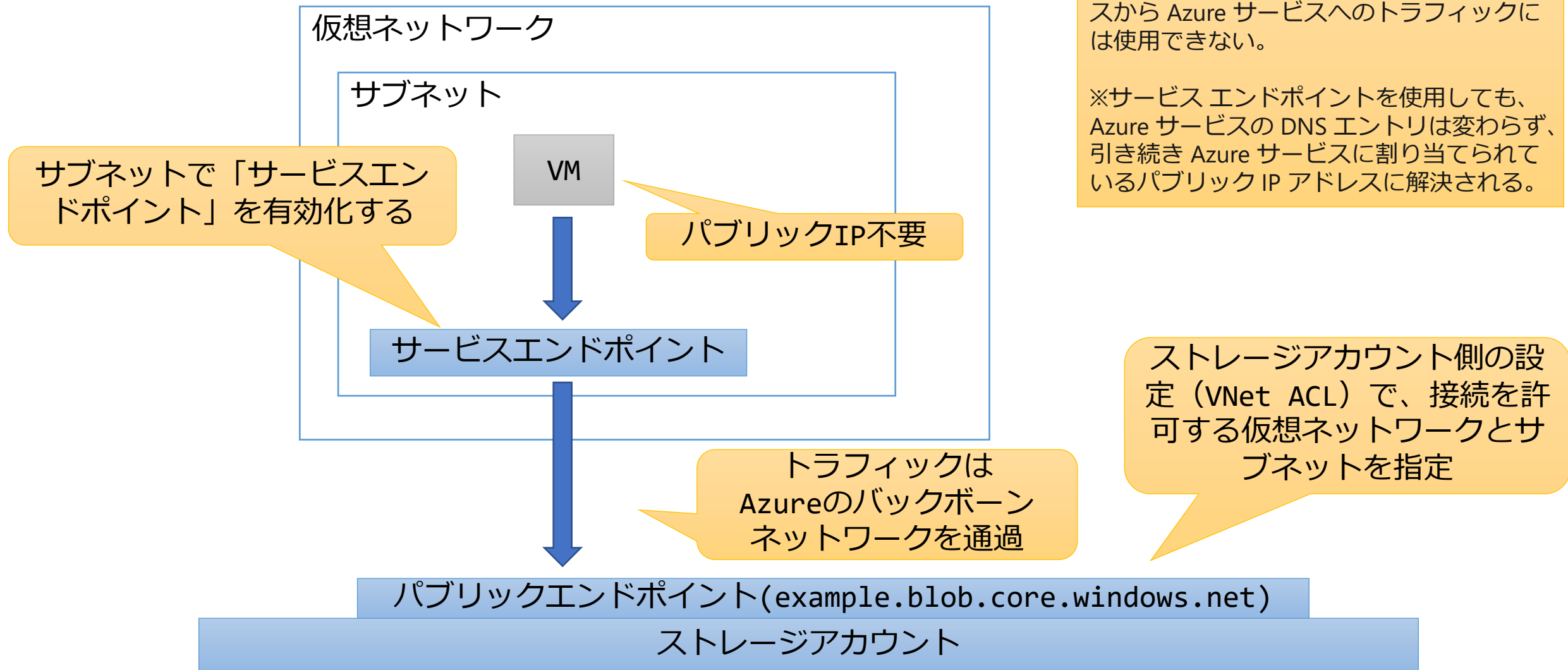


サービスエンドポイント

■ サービスエンドポイントの概要（ストレージアカウントへ接続する例）



<https://learn.microsoft.com/ja-jp/azure/virtual-network/virtual-networks-faq#virtual-network-service-endpoints>

<https://learn.microsoft.com/ja-jp/azure/virtual-network/virtual-network-service-endpoints-overview#secure-azure-services-to-virtual-networks>

■ストレージアカウントの作成画面＞ネットワーク (デフォルトでは「すべてのネットワークからのパブリックアクセスを有効にする」が選択されている)

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > ストレージ アカウント >

ストレージ アカウントを作成する ...

基本 詳細設定 **ネットワーク** データ保護 暗号化 タグ 確認および作成

ネットワーク接続

ストレージ アカウントには、パブリック IP アドレスまたはサービス エンドポイント経由で公的に接続することも、プライベート エンドポイントを使用してプライベートに接続することもできます。

ネットワーク アクセス *

- ☒ すべてのネットワークからのパブリック アクセスを有効にする
- ☐ 選択した仮想ネットワークと IP アドレスからのパブリック アクセスを有効にする
- ☐ パブリック アクセスを無効にし、プライベート アクセスを使用する

i すべてのネットワークからパブリック アクセスを有効にすると、このリソースがパブリックで利用可能になる場合があります。パブリック アクセスが必要な場合を除き、より制限されたアクセスの種類を使用することをお勧めします。 [詳細情報](#)

- 「選択した仮想ネットワークとIPアドレスからのパブリックアドレスを有効にする」を選ぶ。
- 接続を許可する仮想ネットワークとサブネットを選択する。

ネットワーク アクセス *

- ☐ すべてのネットワークからのパブリック アクセスを有効にする
- ☒ 選択した仮想ネットワークと IP アドレスからのパブリック アクセスを有効にする
- ☐ パブリック アクセスを無効にし、プライベート アクセスを使用する

2番目（選択した仮想ネットワークとIPアドレスからのパブリック アクセスを有効にする）を選択

仮想ネットワーク

このストレージ アカウントにアクセスできるのは、選択したネットワークのみです。 [詳細情報](#)

仮想ネットワークのサブスクリプション



Azure Pass - スポンサー プラン



接続を許可する
仮想ネットワークと
サブネットを選択

仮想ネットワーク ⓘ

rg1-vnet



[仮想ネットワークの作成](#)

[選択した仮想ネットワークの管理](#)

サブネット ⓘ *

default (10.0.0.0/24) ('Microsoft.Storage' エンドポイントが追加されます)



i 選択した 1 つ以上のサブネットでは 'Microsoft.Storage' エンドポイントを追加する必要があります。エンドポイントの追加中、これらのサブネットを利用するサービストラフィックが一時的に中断される可能性があります。 [詳細情報](#)

■ストレージアカウントの「ネットワーク」の設定の確認

st234253423 | ネットワーク ...

ストレージ アカウント

検索

概要

アクティビティ ログ

タグ

問題の診断と解決

アクセス制御 (IAM)

データ移行

イベント

ストレージ ブラウザー (プレビュー)

データ ストレージ

コンテナー

ファイル共有

キュー

テーブル

セキュリティとネットワーク

ネットワーク

Azure CDN

マウント

ファイアウォールと仮想ネットワーク プライベート エンドポイント接続 カスタム ドメイン

保存 破棄 最新の情報に更新

パブリック ネットワーク アクセス

☒ 選択した仮想ネットワークと IP アドレスから有効

☐ すべてのネットワークから有効

☐ 無効

ストレージ アカウントのネットワーク セキュリティを構成します。 [詳細情報](#)

仮想ネットワーク

既存の仮想ネットワークを追加する

新しい仮想ネットワークを追加する

Virtual Network	サブネット	アドレス範囲	エンドポイントの状態	リソース グループ
▼ rg1-vnet	1			rg1
	default	10.0.0.0/24	✓ 有効	rg1

ファイアウォール

インターネットまたはオンプレミスのネットワークからのアクセスを許可するための IP 範囲を追加します。 [詳細。](#)

☐ クライアント IP アドレス () の追加 ⓘ

アドレス範囲

IP アドレスまたは CIDR

2番目（選択した仮想ネットワークとIP
アドレスから有効）が選択されている選択した仮想ネットワークと
サブネットが追加されている。アクセスを許可するIP範囲
(オンプレミス側の固定IP等) を
追加で指定可 ※オプション

■ 仮想ネットワークのサブネットの「サービスエンドポイント」設定の確認

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

20+

test2022-1114@outlook...
既定のディレクトリ

ホーム > 仮想ネットワーク > rg1-vnet

rg1-vnet | サブネット

仮想ネットワーク

検索

概要
アクティビティ ログ
アクセス制御 (IAM)
タグ
問題の診断と解決

設定

アドレス空間
接続デバイス
サブネット
Bastion
DDoS 保護
ファイアウォール
Microsoft Defender for Cloud
ネットワーク マネージャー
DNS サーバー
ピアリング
サービス エンドポイント
プライベート エンドポイント
プロパティ
ロック

監視

警告

サブネット

サブネットの検索

名前 ↑↓	IPv4
default	10.0.0.0/24

default

rg1-vnet

名前

default

サブネット アドレス範囲 *

10.0.0.0/24

10.0.0.0 - 10.0.0.255 (251 + 5 個の Azure 予約アドレス)

IPv6 アドレス空間の追加

NAT ゲートウェイ

なし

ネットワーク セキュリティ グループ

なし

ルート テーブル

なし

サービス エンドポイント

仮想ネットワークからサービス エンドポイントを介して特定の Azure リソースへのトラフィックを許可する、サービス エンドポイントのポリシーを作成します。[詳細情報](#)

サービス

Microsoft.Storage

サービス	状態
Microsoft.Storage	成功

サービス エンドポイント ポリシー

0 項目が選択されました

サブネットの委任

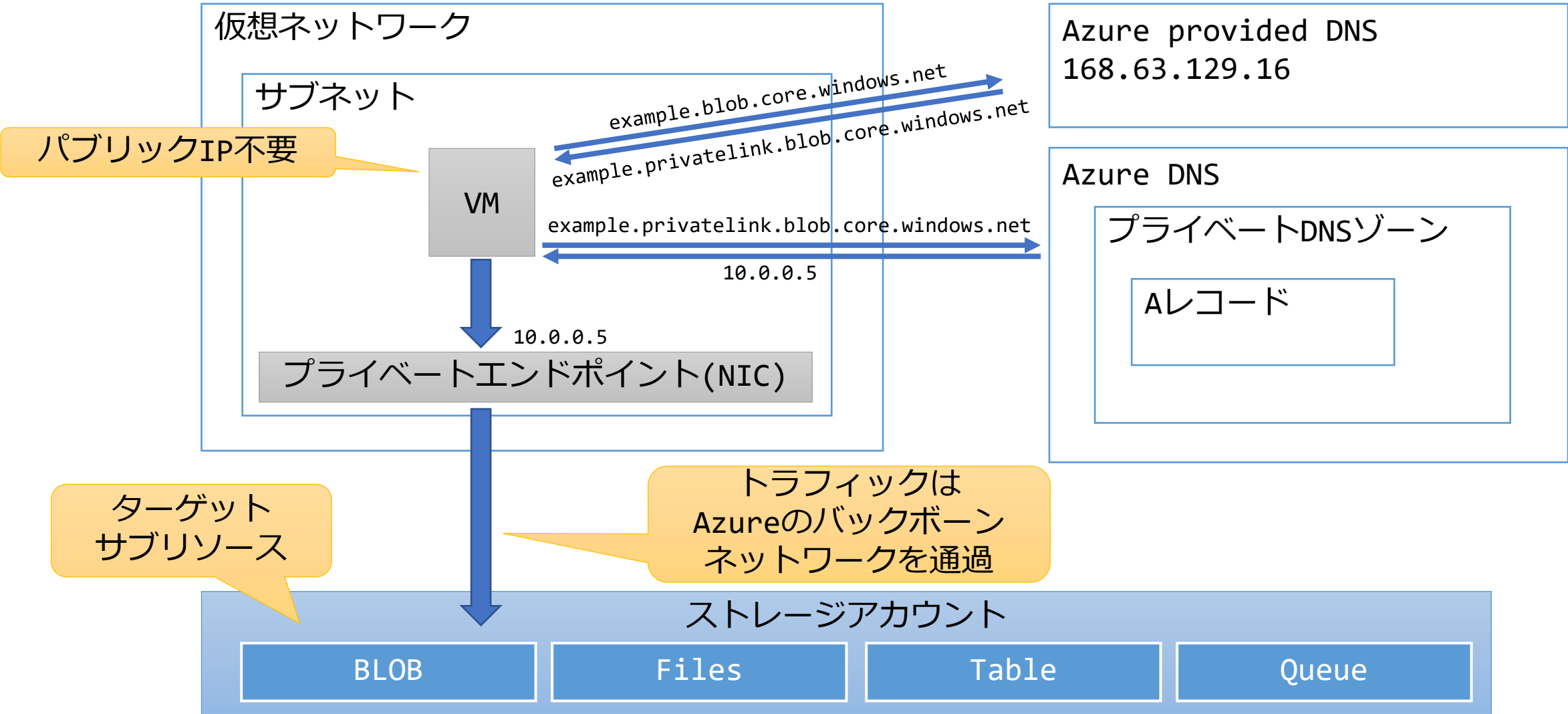
保存

キャンセル

サービスエンドポイントとして「Microsoft.Storage」が追加されている。

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の概要（ストレージアカウントへ接続する例）



<https://learn.microsoft.com/ja-jp/azure/private-link/private-endpoint-overview>

<https://learn.microsoft.com/ja-jp/azure/private-link/private-endpoint-dns>

■ ストレージアカウントの作成画面 > ネットワーク

(デフォルトでは「すべてのネットワークからのパブリックアクセスを有効にする」が選択されている)

The screenshot shows the 'Microsoft Azure' portal interface. At the top, there's a navigation bar with the Azure logo, a search bar containing 'リソース、サービス、ドキュメントの検索 (G+/)', and several utility icons. Below the navigation bar, the breadcrumb 'ホーム > ストレージ アカウント >' is visible. The main heading 'ストレージ アカウントを作成する ...' is highlighted with a red box. Below this, a series of tabs are shown: '基本', '詳細設定', 'ネットワーク' (which is selected and highlighted with a red box), 'データ保護', '暗号化', 'タグ', and '確認および作成'. The 'ネットワーク接続' section contains a paragraph explaining that storage accounts can be accessed via public IP addresses or service endpoints. Below this, the 'ネットワーク アクセス *' section features three radio button options. The first option, 'すべてのネットワークからのパブリック アクセスを有効にする', is selected and highlighted with a red box. The second option is '選択した仮想ネットワークと IP アドレスからのパブリック アクセスを有効にする'. The third option is 'パブリック アクセスを無効にし、プライベート アクセスを使用する'. Below the third option is an information icon (i) followed by a paragraph explaining that enabling public access from all networks makes the resource publicly accessible, which may not be desired in all cases, and recommends using restricted access types. A link labeled '詳細情報' is provided at the end of this paragraph.

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > ストレージ アカウント >

ストレージ アカウントを作成する ...

基本 詳細設定 **ネットワーク** データ保護 暗号化 タグ 確認および作成

ネットワーク接続

ストレージ アカウントには、パブリック IP アドレスまたはサービス エンドポイント経由で公的に接続することも、プライベート エンドポイントを使用してプライベートに接続することもできます。

ネットワーク アクセス *

☒ すべてのネットワークからのパブリック アクセスを有効にする

☐ 選択した仮想ネットワークと IP アドレスからのパブリック アクセスを有効にする

☐ パブリック アクセスを無効にし、プライベート アクセスを使用する

i すべてのネットワークからパブリック アクセスを有効にすると、このリソースがパブリックで利用可能になる場合があります。パブリック アクセスが必要な場合を除き、より制限されたアクセスの種類を使用することをお勧めします。 [詳細情報](#)

- 「パブリックアクセスを無効にし、プライベートアクセスを使用する」を選択
- 「+プライベートエンドポイントの追加」をクリック

ストレージ アカウントを作成する

×

基本 詳細設定 ネットワーク データ保護 暗号化 タグ 確認および作成

ネットワーク接続

ストレージ アカウントには、パブリック IP アドレスまたはサービス エンドポイント経由で公的に接続することも、プライベート エンドポイントを使用してプライベートに接続することもできます。

ネットワーク アクセス *

☐ すべてのネットワークからのパブリック アクセスを有効にする

☐ 選択した仮想ネットワークと IP アドレスからのパブリック アクセスを有効にする

☒ パブリック アクセスを無効にし、プライベート アクセスを使用する

プライベート エンドポイント

このリソースへのプライベート接続を許可するには、プライベート エンドポイントを作成します。追加のプライベート エンドポイント接続は、ストレージ アカウントまたはプライベート リンク センターで作成できます。

+ プライベート エンドポイントの追加

名前	サブスクリ...	リソース ...	リージョン	ターゲット...	サブネット	プライバー...	プライバー...
[追加] をクリックしてプライベート エンドポイントを作成します							

Review

< 前へ

次へ: データ保護 >

■プライベートエンドポイントの作成画面

プライベート エンドポイントの作成

サブスクリプション *

Azure Pass - スポンサー プラン

リソース グループ *

rg1

新規作成

場所 *

Japan East

名前 *

privateendpoint1

ストレージのサブリソース *

blob

ネットワーク

プライベート エンドポイントを展開するには、仮想ネットワーク サブネットを選択します。[プライベート エンドポイント ネットワークの詳細](#)

仮想ネットワーク *

rg1-vnet (rg1)

サブネット *

default

上記のサブネットで有効なネットワーク セキュリティ グループ (NSG) がある場合、それはこのサブネットのプライベート エンドポイントに対してのみ無効になります。このサブネット上の他のリソースには引き続き NSG が強制されます。

プライベート DNS 統合

プライベート エンドポイントとプライベートに接続するには、DNS レコードが必要です。プライベート エンドポイントプライベート DNS ゾーンと統合することをお勧めします。また、独自の DNS サーバーを利用したり、仮想マシン上のホスト ファイルを使用して DNS レコードを作成したりすることもできます。[プライベート DNS 統合の詳細](#)

プライベート DNS ゾーンと統合する

はい

いいえ

プライベート DNS ゾーン *

(新規) privatelink.blob.core.windows.net

OK

破棄

プライベートエンドポイントの名前

プライベートエンドポイントの
接続先リソース

プライベートエンドポイントを
設置するVNet/サブネット

「プライベートDNSゾーン」が
作成される。

※ゾーンの名前は
「privatelink.blob.core.windows.net」
で決まっている。

■ストレージアカウント>ネットワーク>「プライベートエンドポイント接続」の確認

ホーム > ストレージ アカウント > st2324536242

st2324536242 | ネットワーク ...

ストレージ アカウント

検索

概要
アクティビティ ログ
タグ
問題の診断と解決
アクセス制御 (IAM)
データ移行
イベント
ストレージ ブラウザー (プレビュー)

データ ストレージ
コンテナー
ファイル共有
キュー
テーブル

セキュリティとネットワーク
ネットワーク
Azure CDN
アクセス キー

ファイアウォールと仮想ネットワーク プライベート エンドポイント接続 カスタム ドメイン

+ プライベート エンドポイント ✓ 承認 ✕ 拒否 🗑 削除 ↺ 最新の情報に更新

名前でフィルター... すべての接続の状態

<input type="checkbox"/>	接続名	接続の状態	プライベート エンドポイン...	説明
<input type="checkbox"/>	st2324536242.84a90...	承認済み	privateendpoint1	Auto-Approved

st2324536242.84a909ba-32fa-4459-9279-0be123b41936

接続名
(ストレージアカウント
の名前.GUID)

クリックすると
プライベートエンドポイントの画面へ移動

■プライベートエンドポイントの確認

ホーム > ストレージ アカウント > st2324536242 | ネットワーク >

 **privateendpoint1** ☆ ...
プライベート エンドポイント

検索 << 削除 最新の情報に更新

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

設定

アプリケーション セキュリティ グループ

DNS の構成

プロパティ

ロック

監視

分析情報

警告

メトリック

オートメーション

タスク (プレビュー)

テンプレートのエクスポート

へ 基本

リソース グループ (移動)
[rg1](#)

場所
Japan East

サブスクリプション (移動)
[Azure Pass - スポンサー プラン](#)

サブスクリプション ID
c515cce0-db02-4093-ab0b-6f5f04de54f3

プロビジョニング状態
成功

タグ (編集)
[タグを追加するにはここをクリック](#)

JSON ビュー

仮想ネットワークまたはサブネット
[rg1-vnet/default](#)

ネットワーク インターフェイス
[privateendpoint1.nic.b397c6b9-1176-4050-84b9-1b2d6...](#)

プライベート リンク リソース
[st2324536242](#)

ターゲット サブリソース
blob

接続の状態
承認済み

要求または応答
Auto-Approved

プライベートエンドポイントが作成されたVNet/
サブネット

プライベートエンドポイントとして作成されたNIC

接続先のリソース（ストレージアカウント）

■プライベートDNSゾーンの確認

ホーム > プライベート DNS ゾーン >

DNS

privatelink.blob.core.windows.net

プライベート DNS ゾーン

検索

レコード セット

移動

ゾーンを削除する

最新の情報に更新

概要

アクティビティ ログ

アクセス制御 (IAM)

タグ

問題の診断と解決

設定

仮想ネットワーク リンク

プロパティ

ロック

監視

警告

メトリック

オートメーション

タスク (プレビュー)

テンプレートのエクスポート

ヘルプ

新しいサポート リクエスト

基本

JSON ビュー

リソース グループ (移動)

rg1

サブスクリプション (移動)

Azure Pass - スポンサー プラン

サブスクリプション ID

c515cce0-db02-4093-ab0b-6f5f04de54f3

タグ (編集)

タグを追加するにはここをクリック

このページに読み込まれたレコード セットを検索できます。探しているものが見つからない場合は、スクロールしてその他のレコード セットを読み込むことができます。

レコード セットの検索

名前	種類	TTL	値	自動登録済み
@	SOA	3600	電子メール: azureprivatedns-host.microsoft.com ホスト: azureprivatedns.net 更新: 3600 再試行: 300 有効期限: 2419200 最小 TTL: 10 シリアル番号: 1	False
st2324536242	A	3600	10.0.0.5	False

■プライベートDNSゾーンのレコードセットの確認

[ホーム](#) > [プライベート DNS ゾーン](#) > [privatelink.blob.core.windows.net](#) >

st2324536242 ...

privatelink.blob.core.windows.net

 保存  破棄  削除  アクセス制御 (IAM)  メタデータ

名前

st2324536242.privatelink.blob.core.windows.net.

種類

A

TTL *

1

TTL の単位

時間


IP アドレス

10.0.0.5

0.0.0.0


■仮想ネットワークの「接続デバイス」の確認

ホーム > 仮想ネットワーク > rg1-vnet

 **rg1-vnet | 接続デバイス** ☆ ...

仮想ネットワーク

🔍 検索

⏪  最新の情報に更新

- 🔗 概要
- 📅 アクティビティ ログ
- 👤 アクセス制御 (IAM)
- 🏷️ タグ
- 🔧 問題の診断と解決

設定

- 🔗 アドレス空間
- 🔗 接続デバイス**
- 🔗 サブネット
- 🔗 Bastion
- 🛡️ DDoS 保護
- 🔥 ファイアウォール
- 🛡️ Microsoft Defender for Cloud

🔍 接続デバイスの検索

デバイス ↑↓	種類 ↑↓	IP アドレス ↑↓	サブネット ↑↓
web1869	ネットワーク インターフェイス	10.0.0.4	default
privateendpoint1.nic.b397c6b9-1176-4050-84b9-1b2d64c3fe69	ネットワーク インターフェイス	10.0.0.5	default

プライベートエンドポイントとして
作成されたNIC

サブネットのプライベート
IPアドレスを1個使用する