

ストレージアカウント

2023/6/20

ストレージアカウンとは

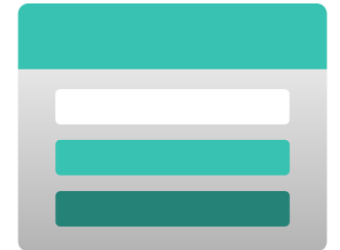
Blob / Files / Table / Queueの4サービスを利用可能

最大で2PB（米国・ヨーロッパのリージョン） / 500TB（その他リージョン、申請により2PBまで）までのデータを格納可能

Azureの基本的なストレージのサービス

- **Azure Blob Storage:** オブジェクトストレージ
 - 大量の非構造化データを安価に保存
 - HTTP/HTTPSでアクセス
- **Azure Files:** ファイル共有
 - 仮想マシンやオンプレミスのコンピュータからSMB・NFSでマウントして使用
 - ファイルサーバーのような使い方が可能
- **Azure Queue Storage:** キュー
- **Azure Table Storage:** テーブル (NoSQL)

「ストレージアカウント」リソースを作ると、その中で上記4つのサービスが利用できる。



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
- Storage Mover

データストレージ

- コンテナ
- 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
- Shared Access Signature
- 暗号化
- Microsoft Defender for Cloud

アップロード Explorer で開く

へ 要点

リソース グループ (移動)

場所

プライマリまたはセカンダリ ロケーション

サブスクリプション (移動)

サブスクリプション ID

ディスクの状態

タグ (編集) : タグを追加するにはここ

プロパティ 監視 機能 (7) 推奨事項

Blob service

Azure Queue Storage
(キュー、メッセージ)

Azure Table Storage
(テーブル、エンティティ)

Azure Blob Storage
(Blobコンテナ、Blob)

Azure Files
(ファイル共有、ファイル)

ストレージアカウントの作成

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 レビュー

Azure Storage は、高可用性、セキュリティ、耐久性、スケーラビリティ、冗長性を備えたクラウド ストレージを提供する Microsoft が管理するサービスです。Azure Storage には、Azure BLOB (オブジェクト)、Azure Data Lake Storage Gen2、Azure Files、Azure Queues、Azure Tables が含まれます。ストレージ アカウントのコストは、使用量と、下で選ぶオプションに応じて決まります。 [Azure ストレージ アカウントの詳細](#)

プロジェクトの詳細

新しいストレージ アカウントを作成するサブスクリプションを選択します。ストレージ アカウントを他のリソースと一緒に整理して管理するには、新規または既存のリソース グループを選択します。

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 *

testrg1



[新規作成](#)

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US

エッジゾーンにデプロイ

パフォーマンス ⓘ *

☒ **Standard:** ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)

☐ **Premium:** 低遅延が必要なシナリオにお勧めします。

冗長性 ⓘ *

geo 冗長ストレージ (GRS)

☒ リージョンが利用できなくなった場合に、データへの読み取りアクセスを行えるようにします。

冗長化オプション

「冗長性」で LRS / GRS / ZRS / GZRS を選択

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US

[エッジ ゾーンにデプロイ](#)

パフォーマンス ⓘ *

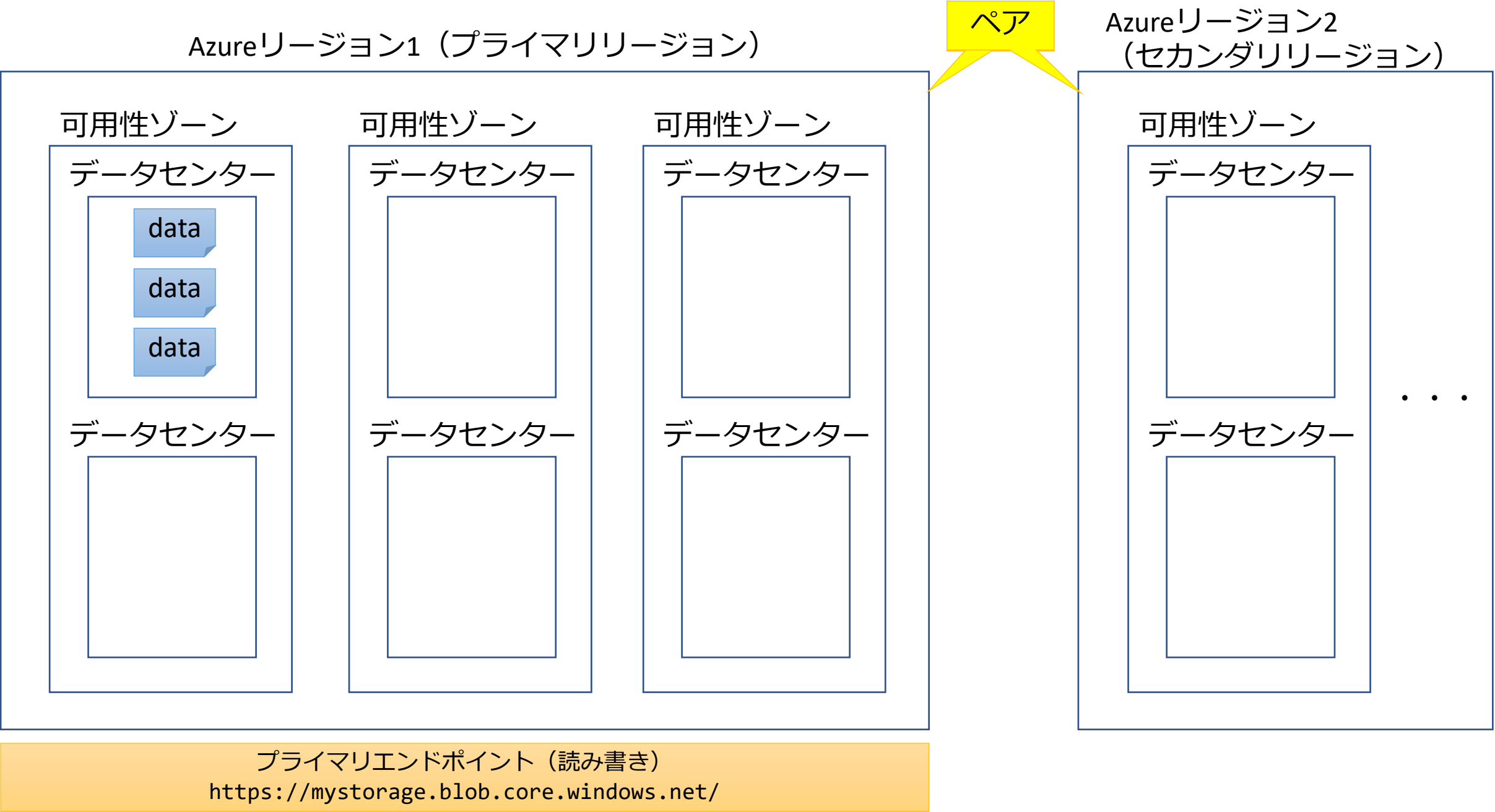
☒ **Standard:** ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)

☐ **Premium:** 低遅延が必要なシナリオにお勧めします。

冗長性 ⓘ *

ローカル冗長ストレージ (LRS)

LRS (Local Redundancy Storage): 1つのデータセンターを使用し、データを3重に複製



LRSについてのよくある質問

- データを1つ保存すると、それが（一覧表示などで）3つに表示されるということか？
 - いいえ。
 - ユーザーには、1つのデータは1つとして表示および操作されるため、内部の3重コピーを意識する必要はない
- 保存コストが3倍になるということか？
 - いいえ。
 - 料金は「LRSのストレージ料金」として表示されているものとなる。
 - 例: 東日本リージョンのLRSのストレージ料金: 0.02 USD / GB (2023/6現在)
- データが損傷した場合はどうなるのか？
 - 他の正常なデータから自動的にコピーが行われ、回復される（3重コピーが自動で維持される）
- データセンターは指定できるか？
 - いいえ。
 - データセンターはAzure側で決定される。
- RAIDのようなしくみを使用されているということか？
 - いいえ。
 - 「ストレージスケールユニット」と呼ばれるサーバーのグループを使用して冗長化されている

<https://learn.microsoft.com/ja-jp/azure/storage/common/storage-redundancy>

<https://learn.microsoft.com/ja-jp/azure/virtual-machines/page-blobs-backup-and-disaster-recovery>

参考: データセンターで火災・浸水などが発生する可能性は、0ではない。

■ 2021/3/11



フランスのクラウド「OVHcloud」でデータセンター火災、数百万サイトに影響か | 日経クロステック (xTECH)

表示

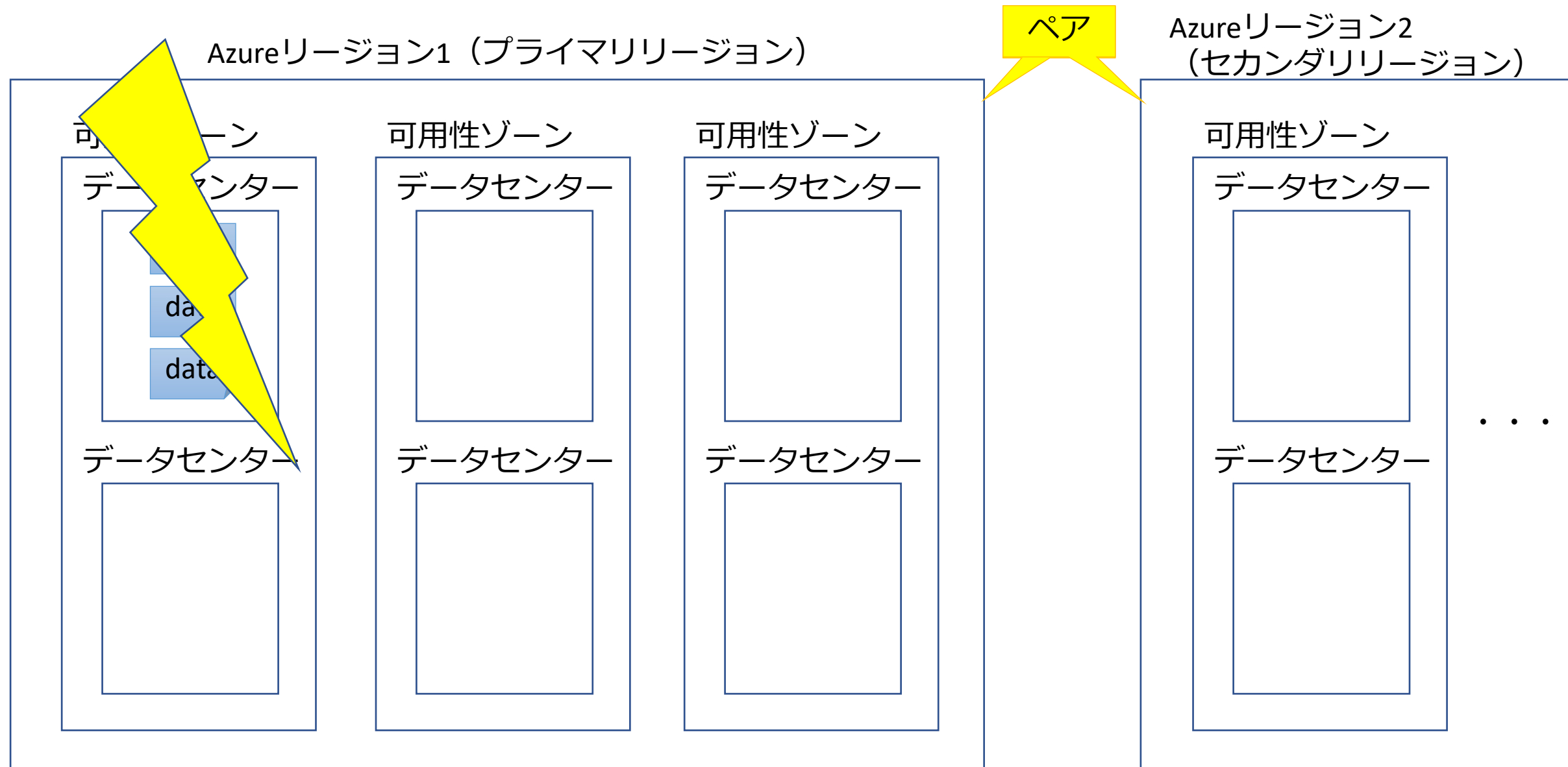
■ 2023/4/27

クラウドサービス「Google Cloud」のパリリージョン（europe-west9）で、4月26日午前11時ごろ（日本時間）から障害が発生している。**データセンターに水が浸入**したといい、一部のサービスを除いて27日午後3時41分時点で障害が続いている。障害は長引く見込みで「**現時点では、リージョンの運用が完全に回復する予定はない**」（米Google Cloud）としている。仮想マシンを立ち上げる「Google Compute Engine」（GCE）、ストレージサービス「Google Cloud Storage」（GCS）、音声認識サービス「Speech-to-Text」など複数のサービスが影響を受けた。このうちGCSなど4サービスはリージョン全体で復旧済み。GCEなど3サービスはリージョン内の一部ゾーンで復旧したという。

<https://xtech.nikkei.com/atcl/nxt/news/18/09847/>

<https://www.itmedia.co.jp/news/articles/2304/27/news162.html>

データセンターが被災した場合（火災・洪水など）、LRSのデータは失われる可能性がある



プライマリエンドポイント（読み書き）
<https://mystorage.blob.core.windows.net/>

LRS以外の冗長化

- データセンター内で火災や洪水などの災害が発生した場合、LRS を使用しているストレージ アカウントの**すべてのレプリカ（データのコピー）**が失われたり、回復不能になる可能性がある。
- このリスクを軽減するために、Microsoft ではゾーン冗長ストレージ (ZRS)、geo 冗長ストレージ (GRS)、または geo ゾーン冗長ストレージ (GZRS) を使用することを推奨している。

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US



[エッジゾーンにデプロイ](#)

パフォーマンス ⓘ *



Standard: ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)



Premium: 低遅延が必要なシナリオにお勧めします。

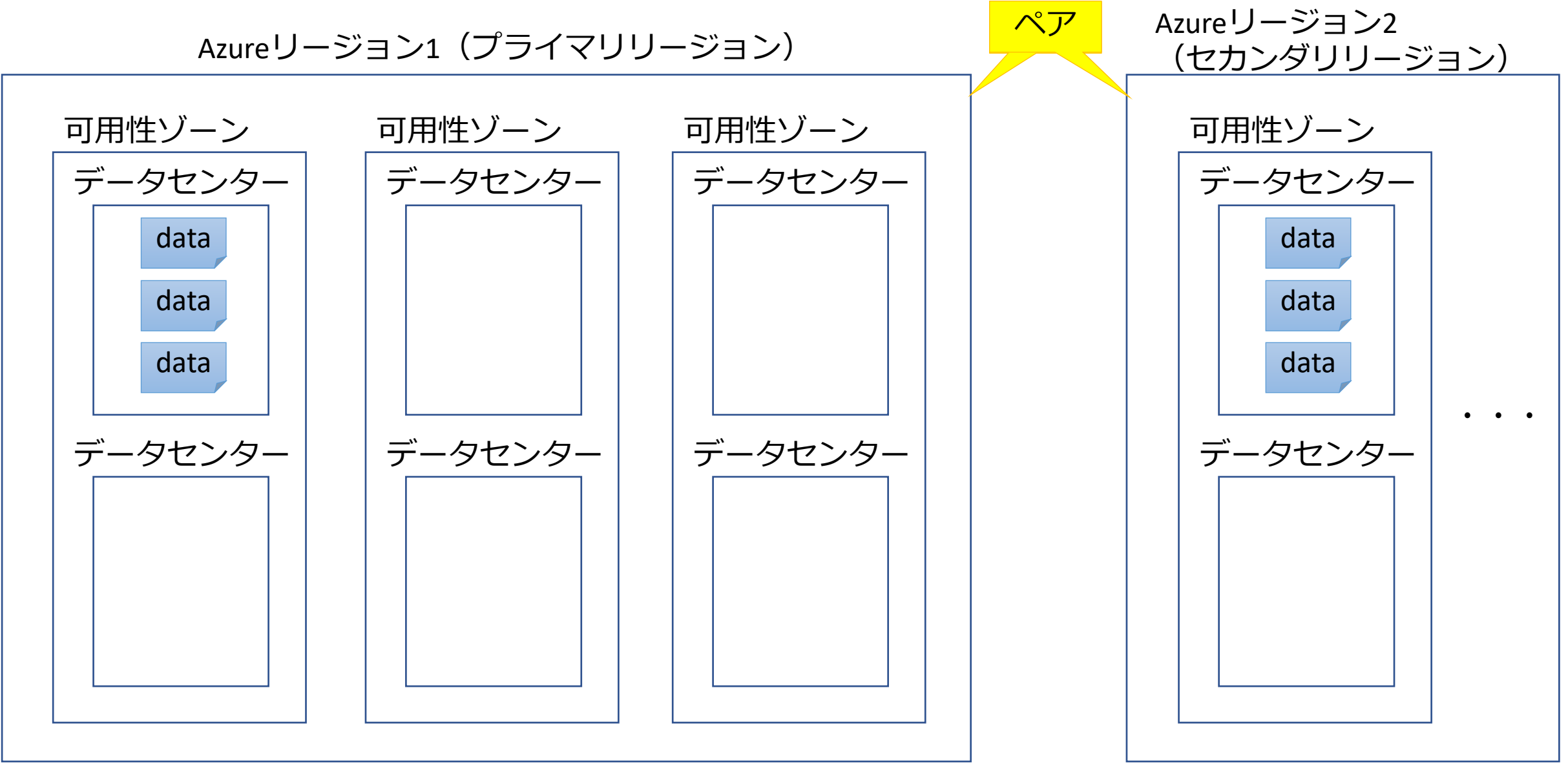
冗長性 ⓘ *

geo 冗長ストレージ (GRS)



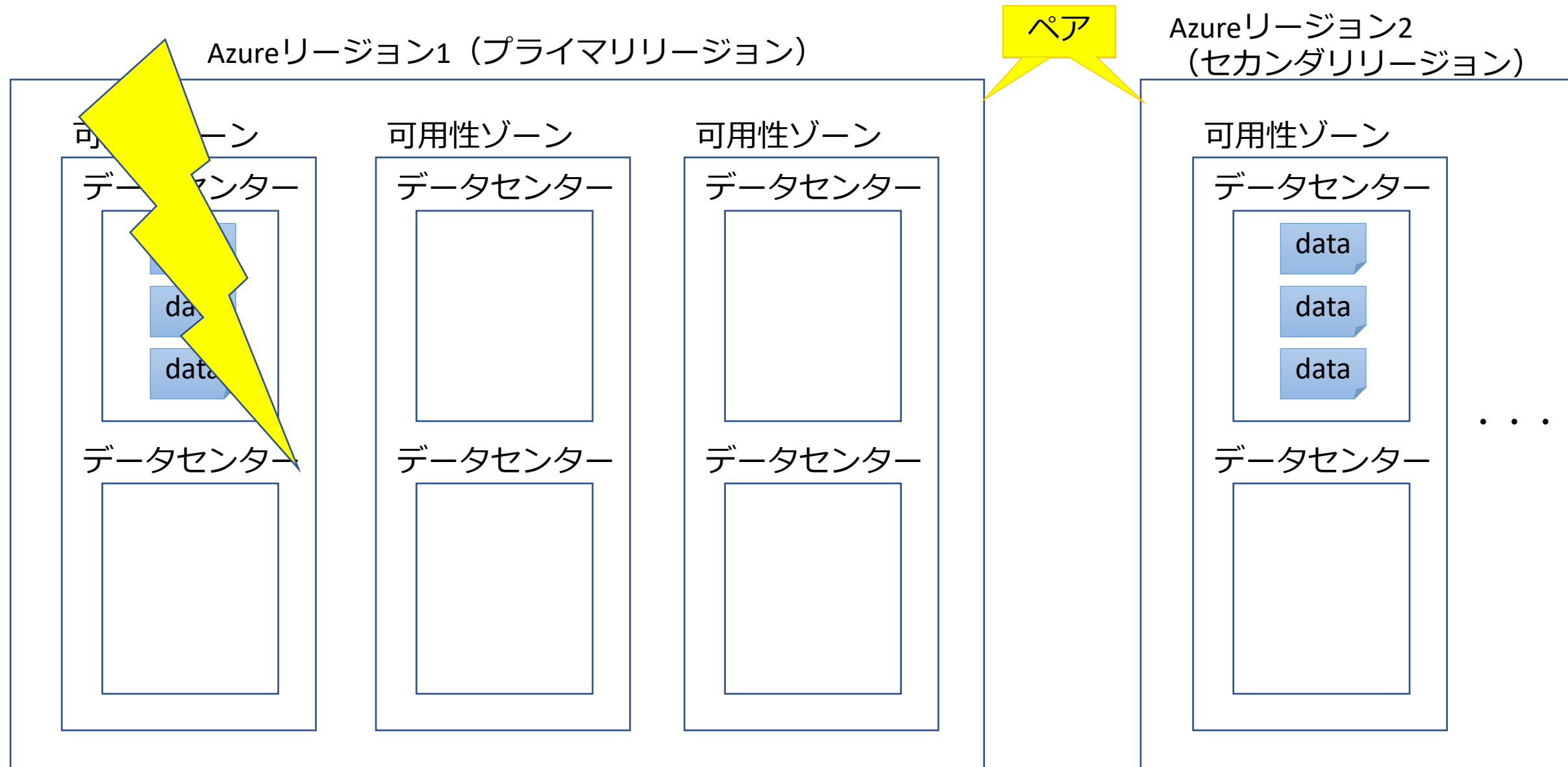
リージョンが利用できなくなった場合に、データへの読み取りアクセスを行えるようにします。

GRS (Geo Redundancy Storage): プライマリでLRS、セカンダリでLRSを使用し、データを6重に複製



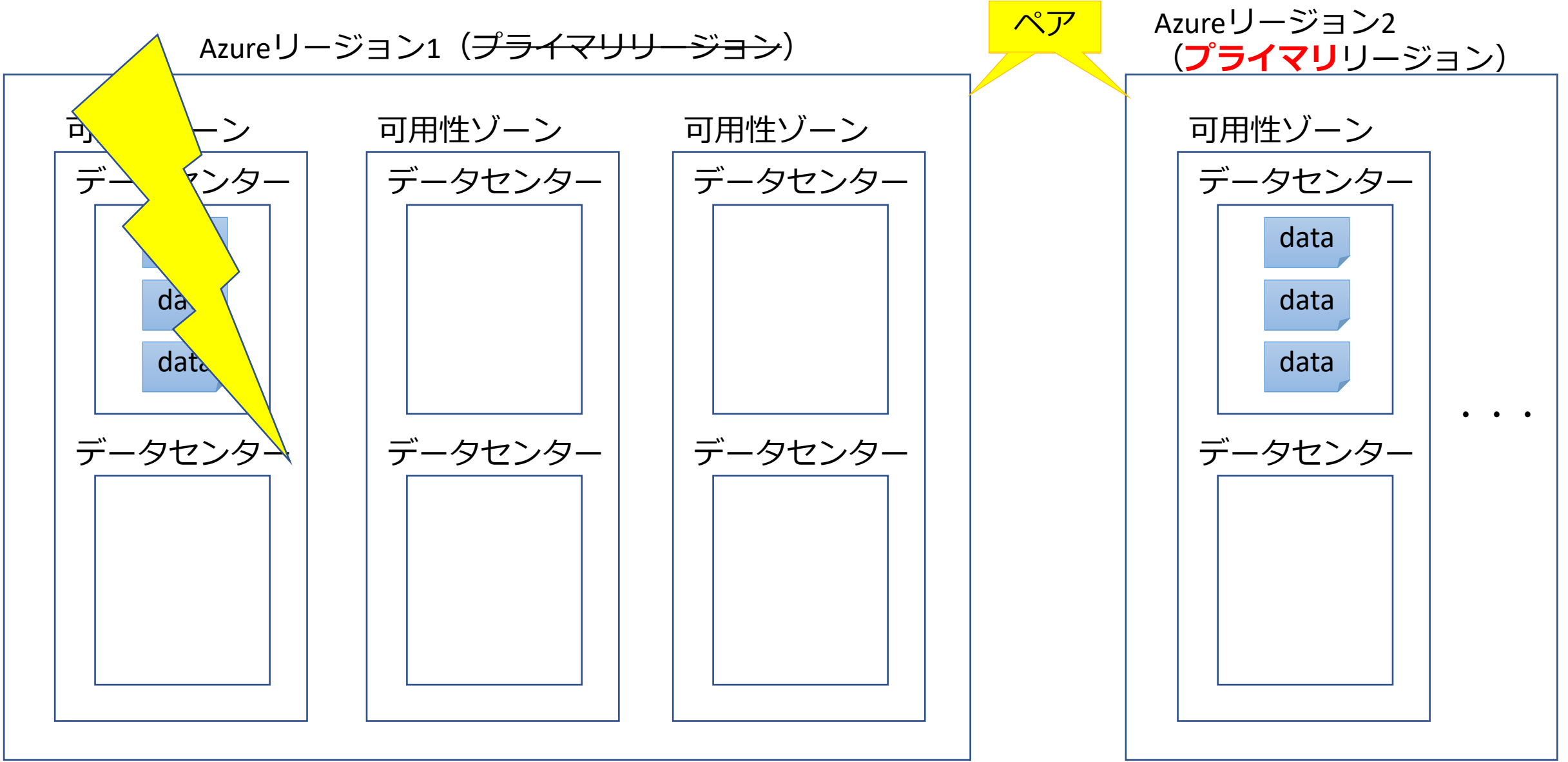
プライマリエンドポイント (読み書き)
<https://mystorage.blob.core.windows.net/>

万が一、データセンターが被災し、**データが回復できなくなった**場合・・・



プライマリエンドポイント (読み書き)
<https://mystorage.blob.core.windows.net/>

フェールオーバーを実行。セカンダリリージョンを新たなプライマリリージョンとして、LRS構成となる。

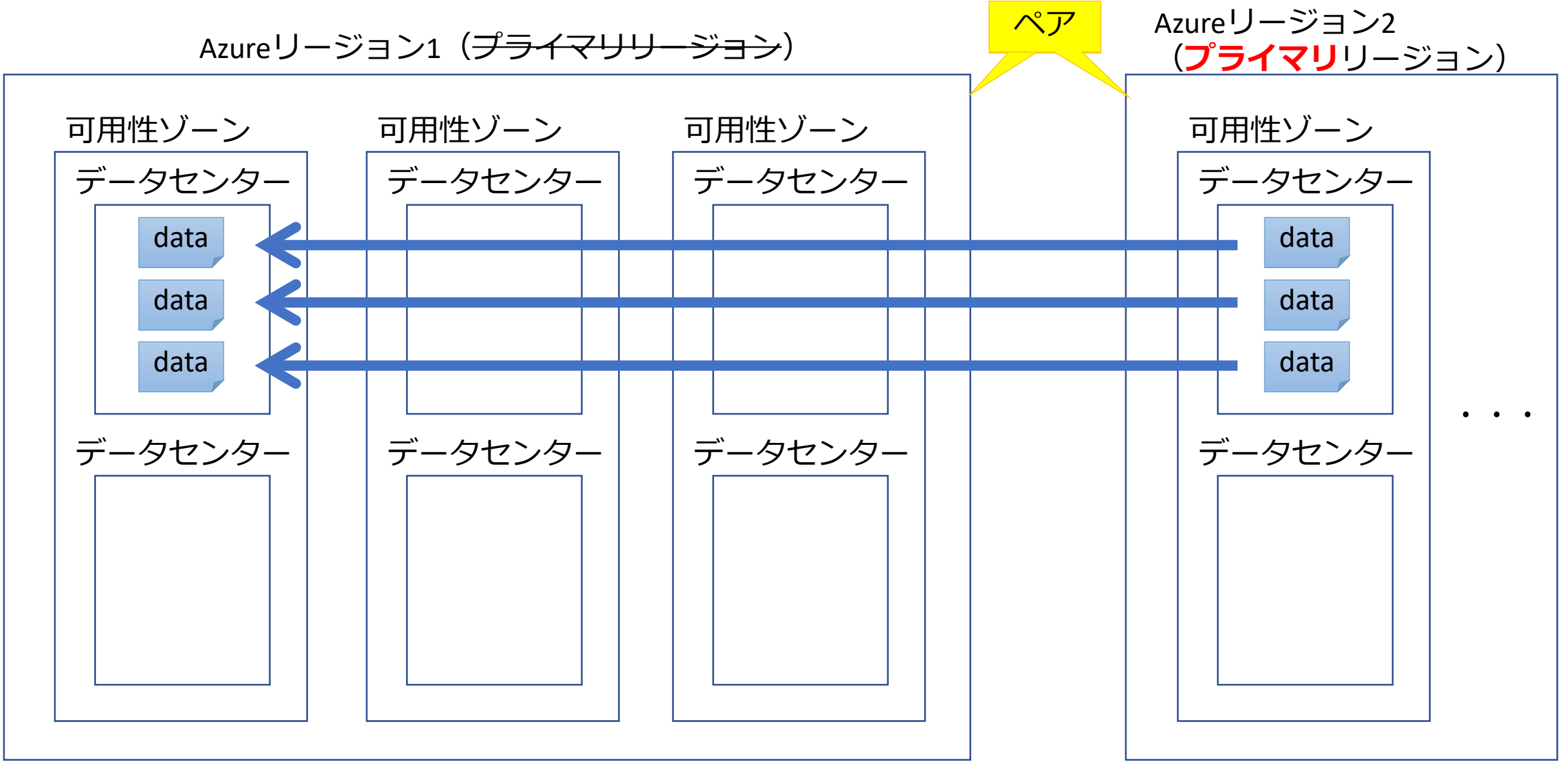


プライマリエンドポイント (読み書き)
<https://mystorage.blob.core.windows.net/>

フェールオーバーについてのよくある質問

- フェールオーバーは誰がいつ実行するのか？
 - ユーザーが、Azure portal、コマンド、REST APIなどから手動で実行する
 - 大きな災害のためにリージョンが失われるような極端な状況では、Microsoft がフェールオーバーを開始する場合がある
- フェールオーバーにはどのくらい時間がかかるのか？
 - フェールオーバーには、通常、約 1 時間かかる
- フェールオーバー後、アプリやシステム側でエンドポイントの書き換えは必要か？
 - 不要。DNS エントリが更新されて、要求が新しいプライマリ エンドポイントに送られるようになるため、プライマリエンドポイントのアドレスは変わらない。
- フェールオーバー後の冗長化構成はどうなる？
 - いったんLRSとなる
- フェールオーバー後、元の構成に戻すには？
 - **フェールバック**を実行する。
- **フェールバック**は自動で実行されるのか？
 - いいえ。

フェールバックの準備: ジオ冗長を再構成 (元のリージョンヘデータをコピー)



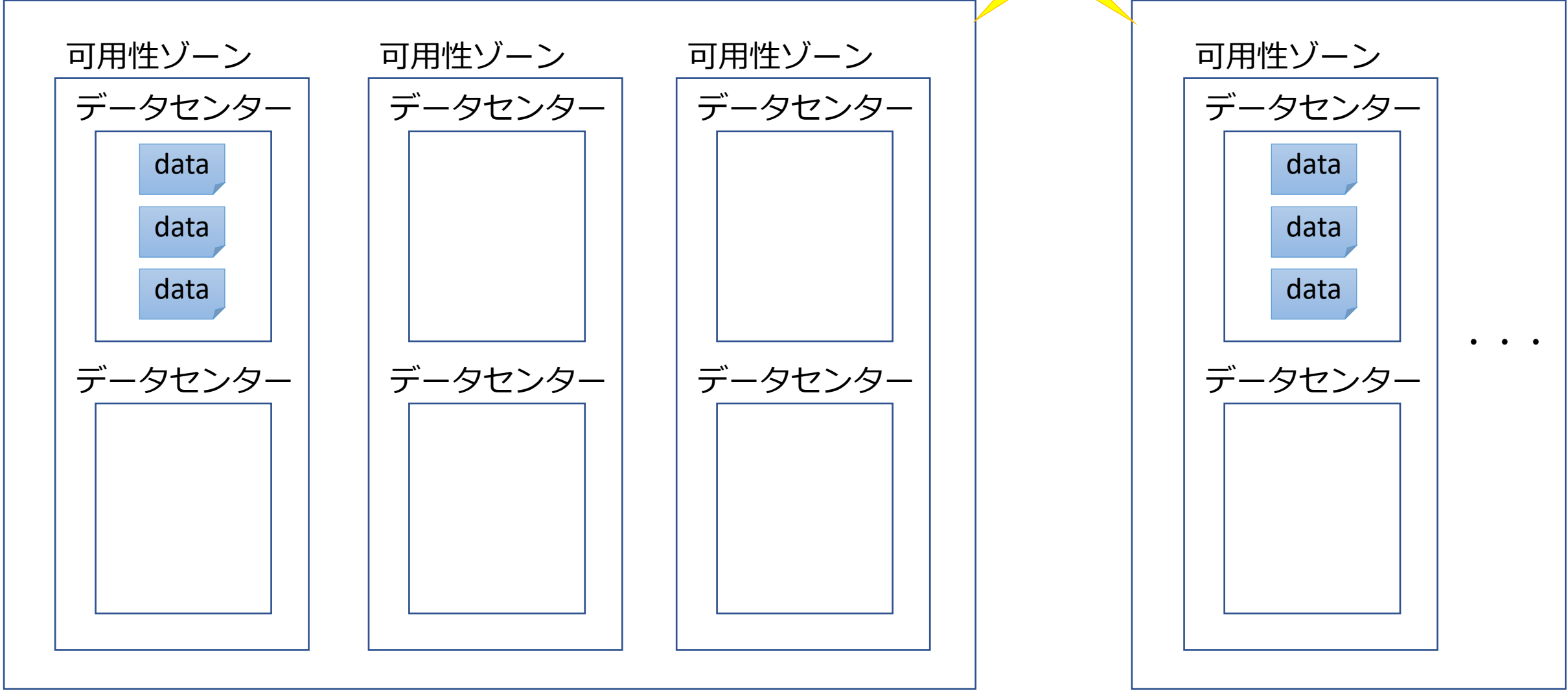
プライマリエンドポイント (読み書き)
<https://mystorage.blob.core.windows.net/>

フェールバックを実行。元のGRS構成に戻る。

Azureリージョン1（プライマリリージョン）

ペア

Azureリージョン2
（セカンダリリージョン）



プライマリエンドポイント（読み書き）
<https://mystorage.blob.core.windows.net/>

セカンダリリージョンについてのよくある質問

- データがセカンダリリージョンにレプリケーションされるまで、どのくらい時間がかかるのか？
 - 通常、プライマリリージョンにデータが書き込まれてから、**15分未満**で、セカンダリリージョンにデータが複製され、読み取りできるようになる

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US

[エッジ ゾーンにデプロイ](#)

パフォーマンス ⓘ *

☒ **Standard:** ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)

☐ **Premium:** 低遅延が必要なシナリオにお勧めします。

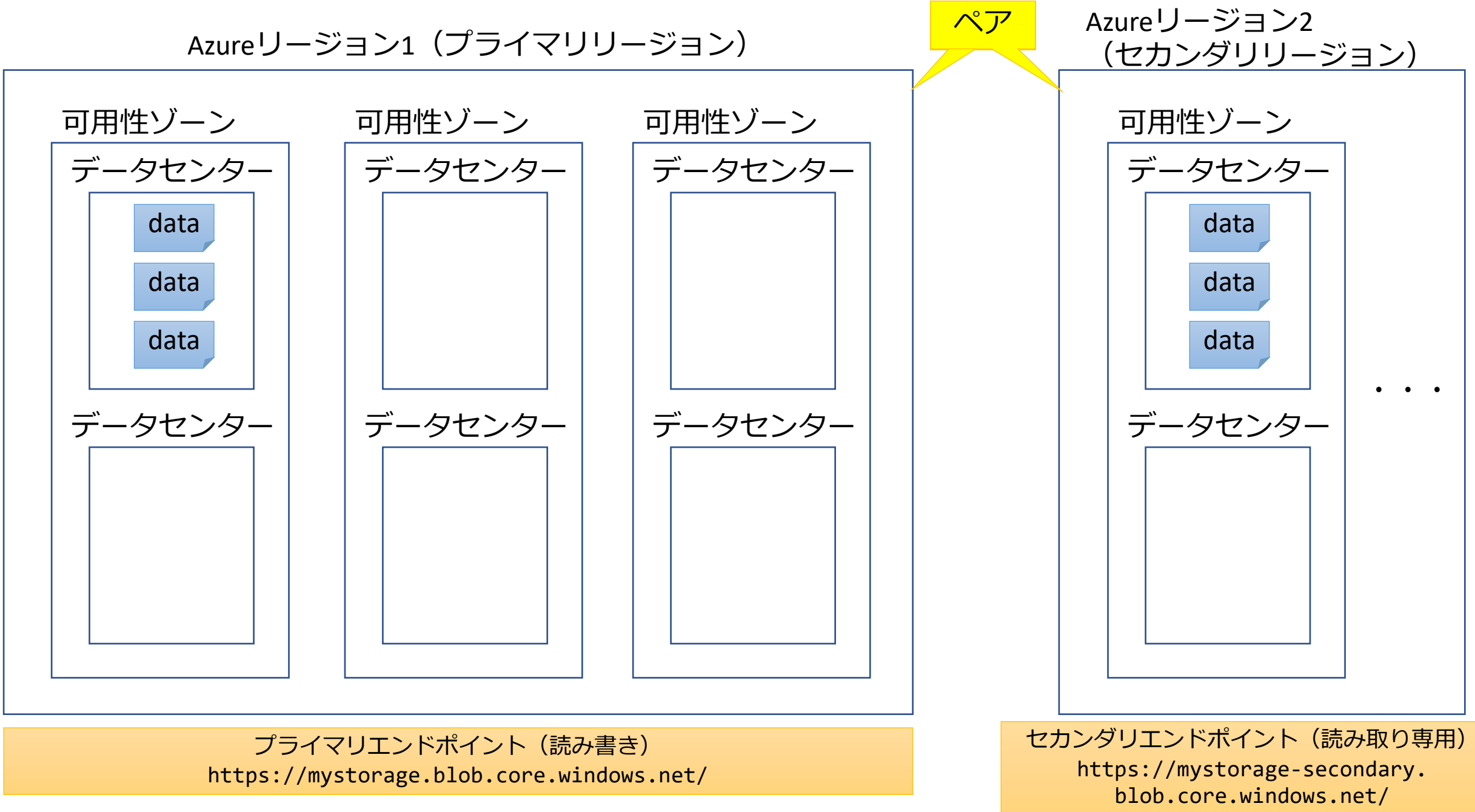
冗長性 ⓘ *

geo 冗長ストレージ (GRS)

☒ リージョンが利用できなくなった場合に、データへの読み取りアクセスを行えるようにします。

実際には「プライマリリージョンの利用可否状態にかかわらず、セカンダリエンドポイントを使用して、データの読み取りアクセスを行えるようにします」というのが正しい

RA-GRS (Read Access - Geo Redundancy Storage): GRSと同様だが、セカンダリエンドポイントも利用可能

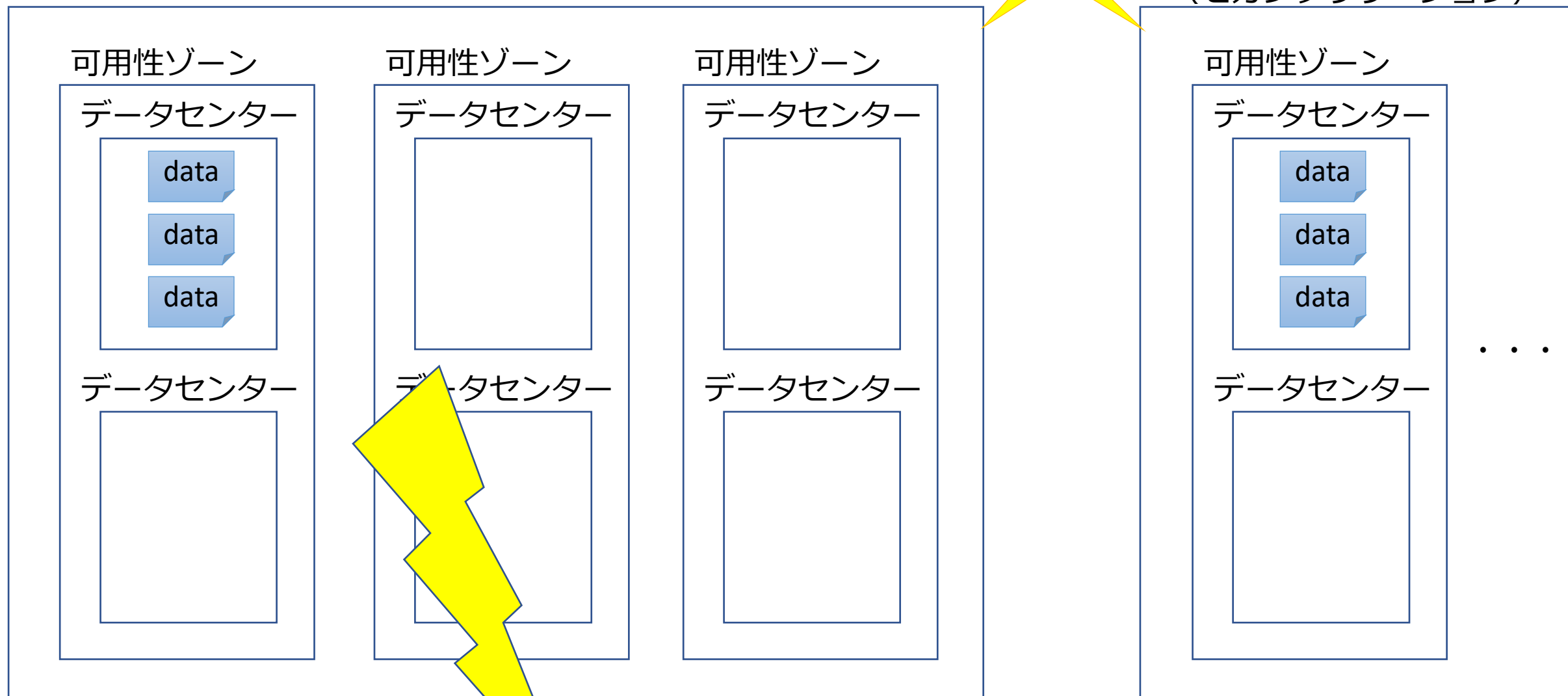


プライマリリージョンで一時的な障害が発生している間でも、クライアントはセカンダリエンドポイントを使用してデータを**読み取り**できる（いわゆる**縮退運転**が可能）

Azureリージョン1（プライマリリージョン）

ペア

Azureリージョン2
（セカンダリリージョン）



プライマリエンドポイント（読み書き）
<https://mystorage.blob.core.windows.net/>

セカンダリエンドポイント（読み取り専用）
<https://mystorage-secondary.blob.core.windows.net/>

セカンダリエンドポイントについてよくある質問

- セカンダリエンドポイントを使用してデータを書き込みできるか？
 - いいえ。
 - セカンダリエンドポイントでは、セカンダリリージョンに複製されたデータの**読み取りだけ**を実行できる
- アプリやシステムでは、各エンドポイントをどのように使うのか？
 - プライマリエンドポイント：平常時、データの読み書きのために使う
 - セカンダリエンドポイント：プライマリにアクセスできない際に、データの読み取りのために使う。いわば予備のエンドポイント。
- プライマリエンドポイントにアクセスできない際に、セカンダリエンドポイントに自動的に切り替えが行われるのか？
 - いいえ。
 - プライマリエンドポイントによる読み書きができないことを**アプリやシステム側で検出**したり、縮退運転（データの保存はできないが、セカンダリエンドポイントを使用してデータの検索や表示をするモードでの運用）をしたりするように、**アプリやシステムを設計する**必要がある

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US



[エッジ ゾーンにデプロイ](#)

パフォーマンス ⓘ *



Standard: ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)



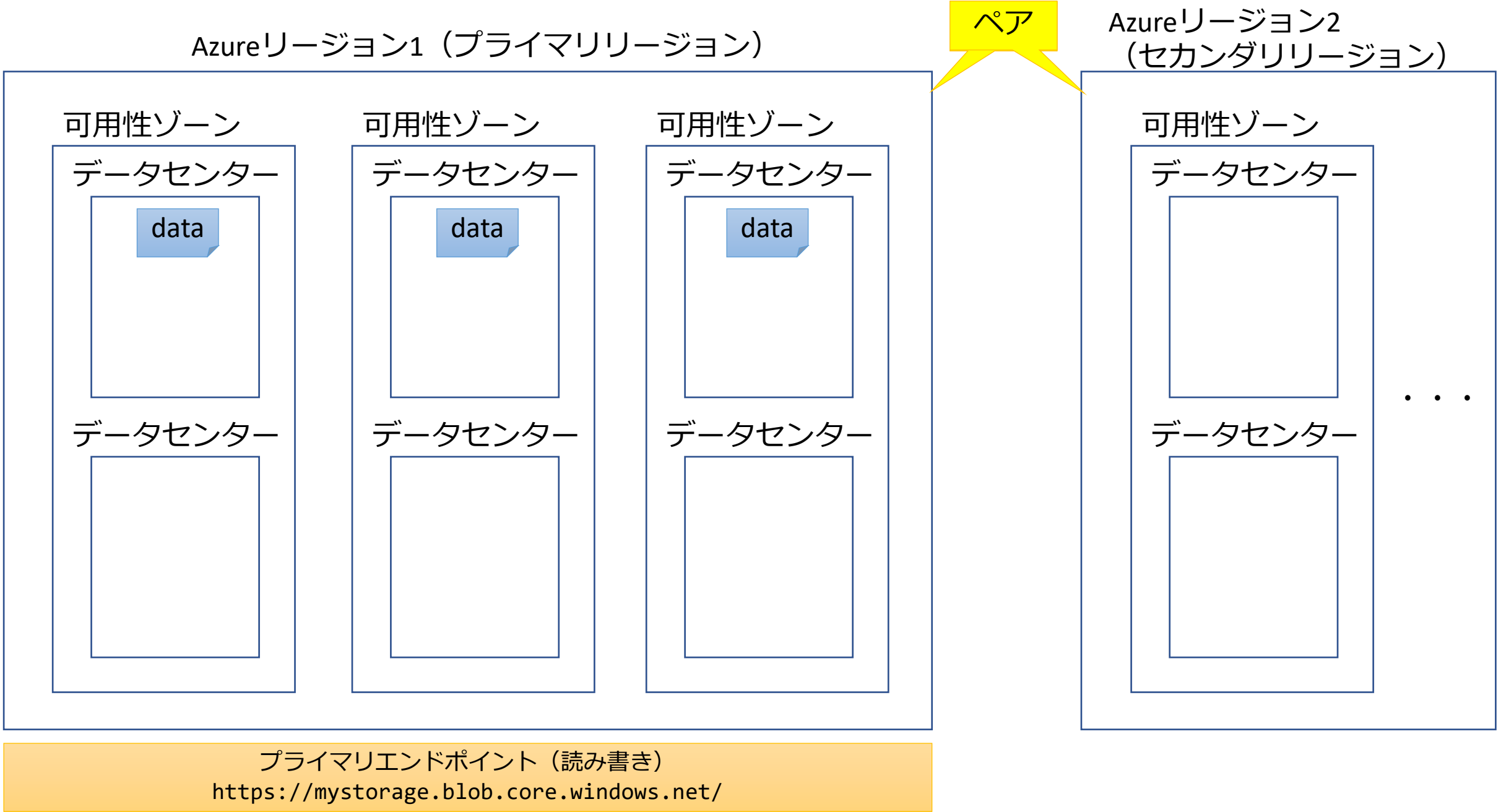
Premium: 低遅延が必要なシナリオにお勧めします。

冗長性 ⓘ *

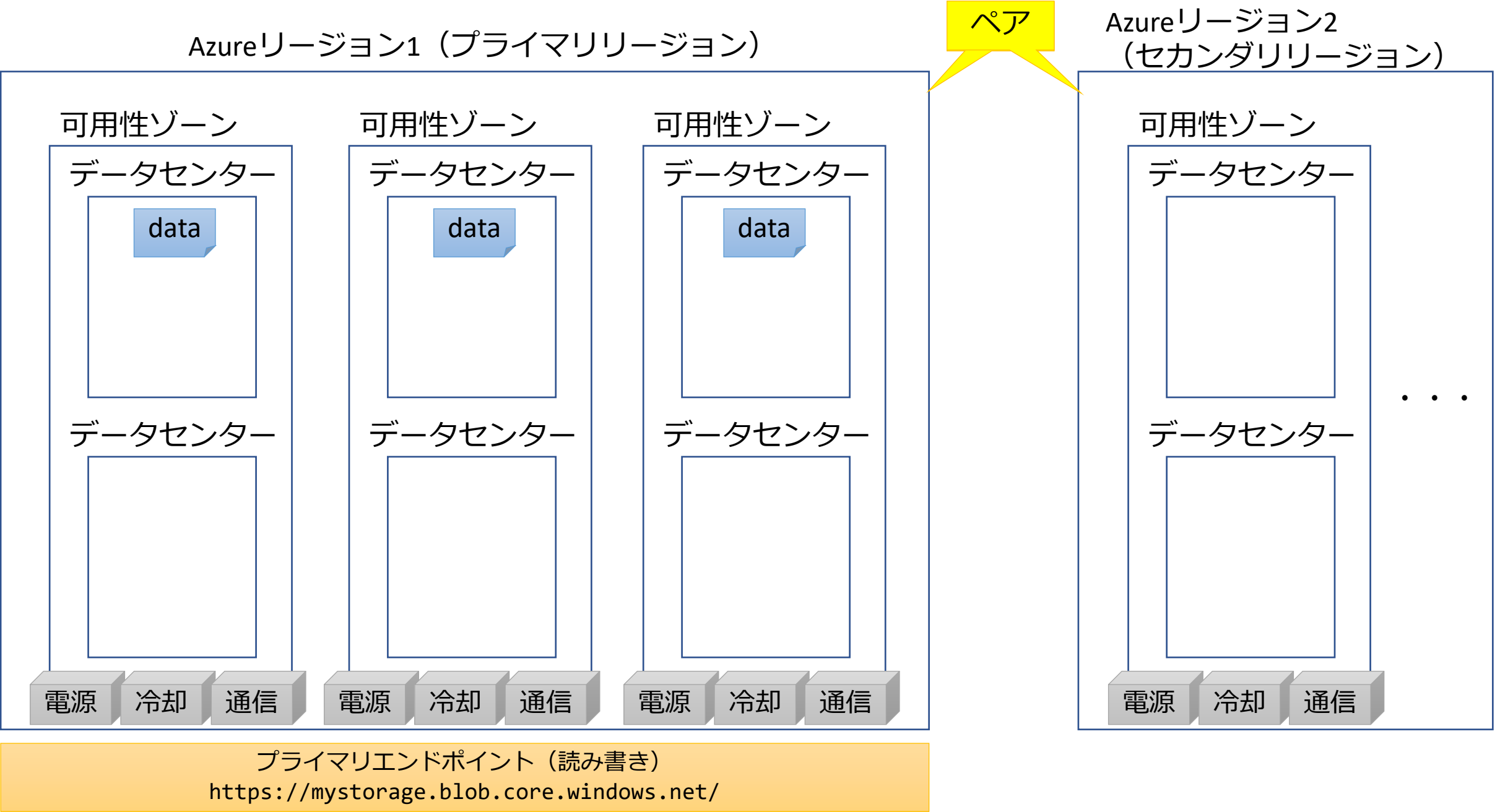
ゾーン冗長ストレージ (ZRS)



ZRS (Zone Redundancy Storage): 3つの**可用性ゾーン**を使用し、データを3重に複製



各**可用性ゾーン**には、それぞれ電源・冷却・通信設備が設置されている

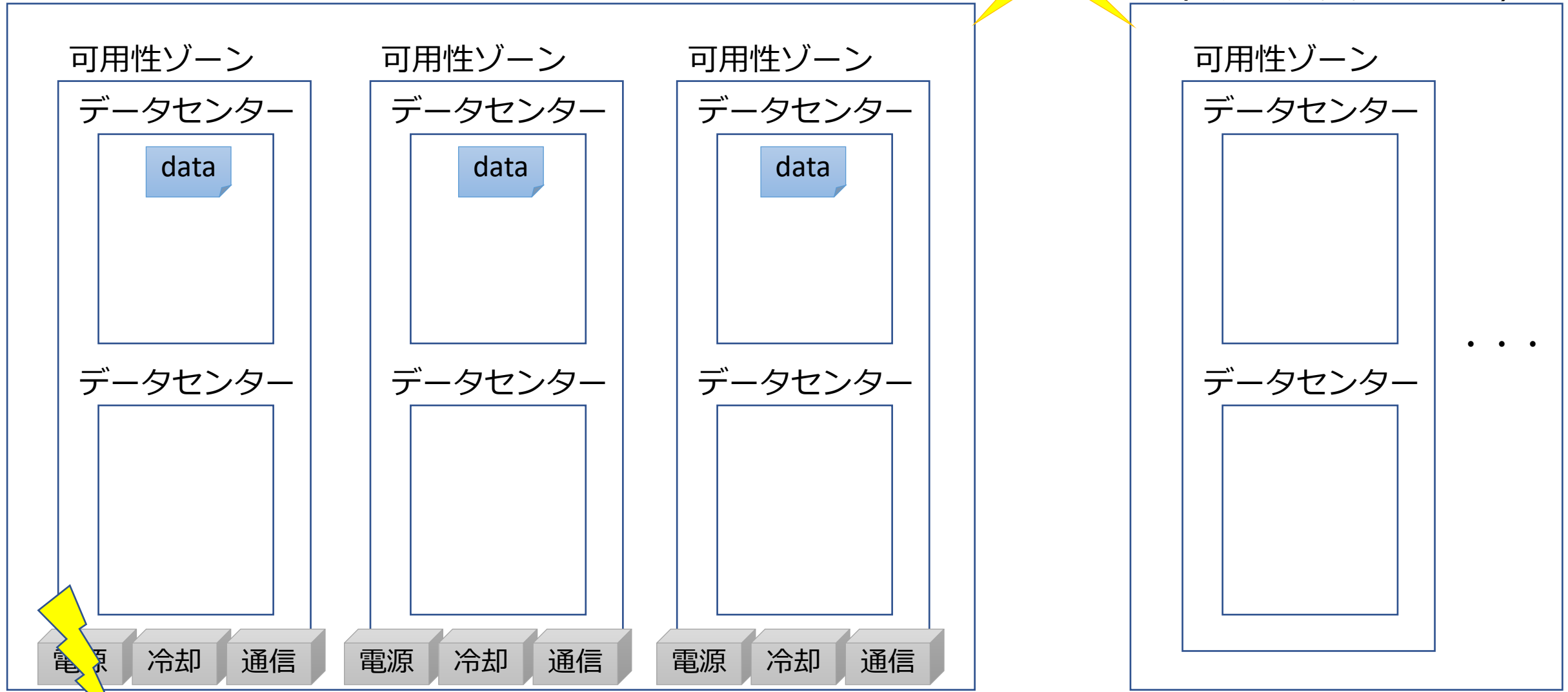


1つの可用性ゾーンで設備の一時的な障害が発生しても、別の可用性ゾーンを使用して、サービスの運用を読み書きを継続できる。したがって**可用性が高い**。

Azureリージョン1（プライマリリージョン）

ペア

Azureリージョン2
（セカンダリリージョン）



プライマリエンドポイント（読み書き）

<https://mystorage.blob.core.windows.net/>

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US

[エッジゾーンにデプロイ](#)

パフォーマンス ⓘ *

☒ **Standard:** ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)

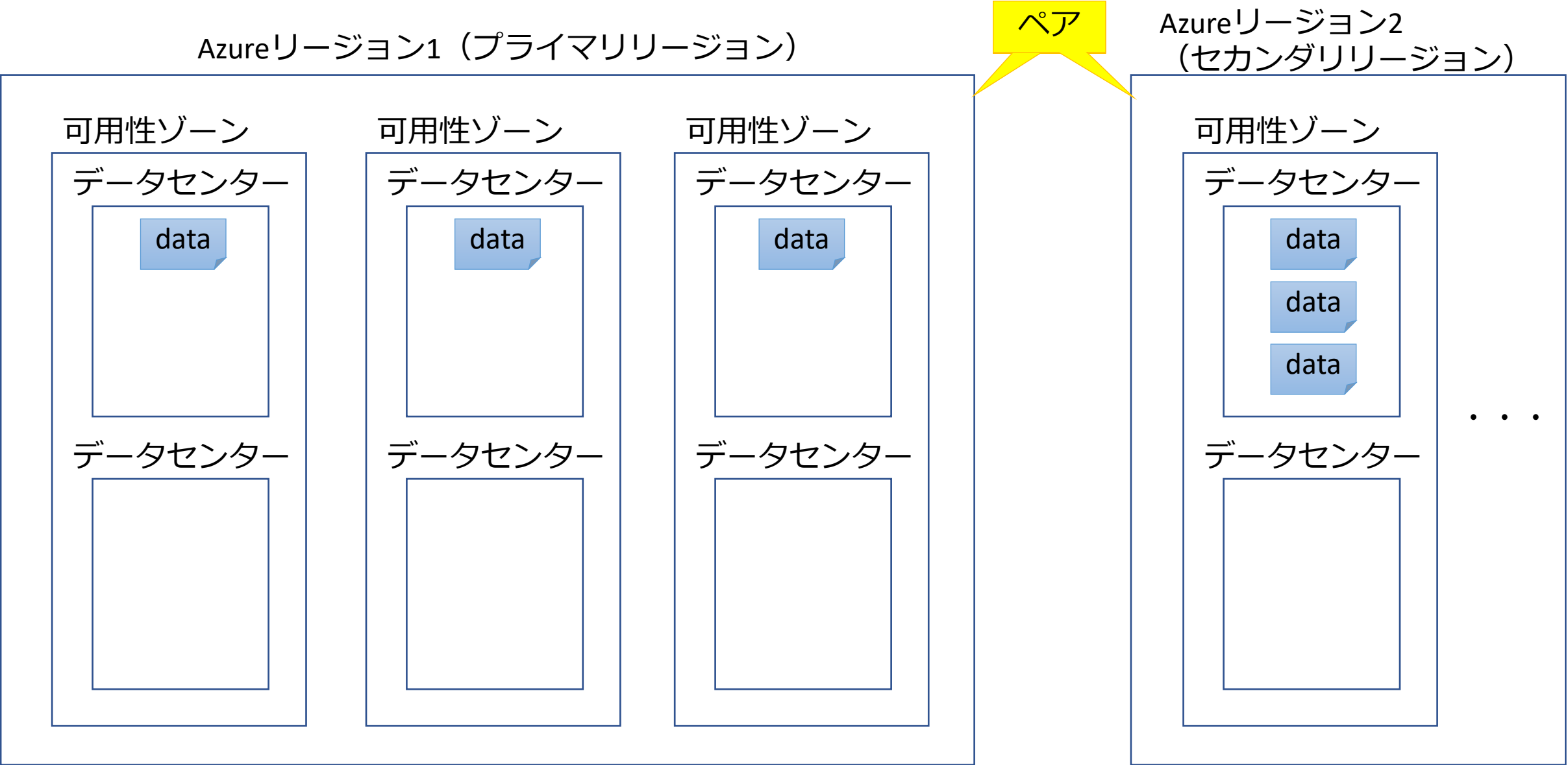
☐ **Premium:** 低遅延が必要なシナリオにお勧めします。

冗長性 ⓘ *

geo ゾーン冗長ストレージ (GZRS)

☐ リージョンが利用できなくなった場合に、データへの読み取りアクセスを行えるようにします。

ZGRS (Geo Zone Redundancy Storage): プライマリでZRS、セカンダリでLRSを使用し、データを6重に複製



プライマリエンドポイント (読み書き)
<https://mystorage.blob.core.windows.net/>

インスタンスの詳細

ストレージ アカウント名 ⓘ *

st9238742

地域 ⓘ *

(US) East US



[エッジゾーンにデプロイ](#)

パフォーマンス ⓘ *



Standard: ほとんどのシナリオに対して推奨される (汎用 v2 アカウント)



Premium: 低遅延が必要なシナリオにお勧めします。

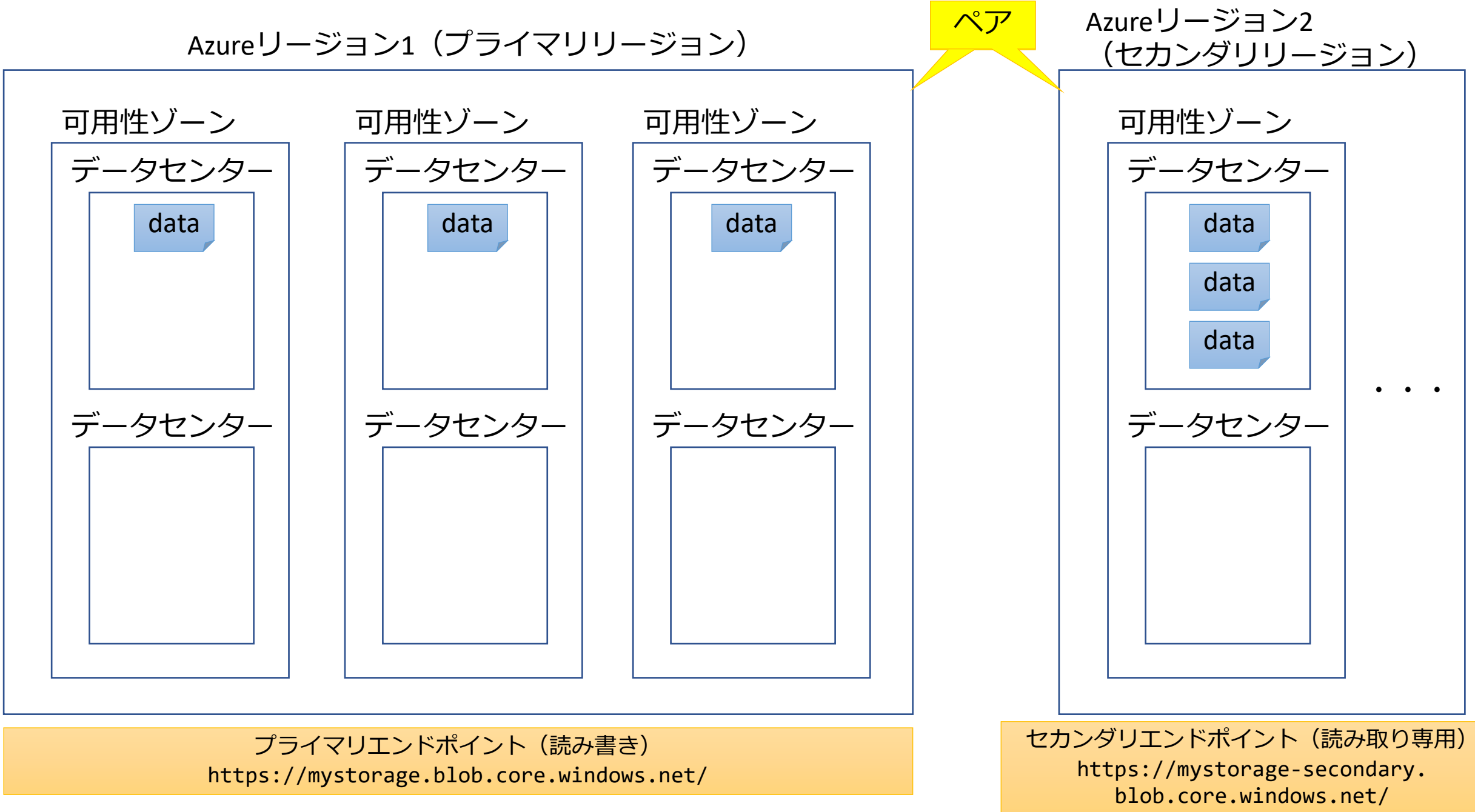
冗長性 ⓘ *

geo ゾーン冗長ストレージ (GZRS)



リージョンが利用できなくなった場合に、データへの読み取りアクセスを行えるようにします。

RA-ZGRS (Read Access Geo Zone Redundancy Storage): GZRSと同様だが、セカンダリエンドポイントも利用可能



ネットワーク構成

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 レビュー

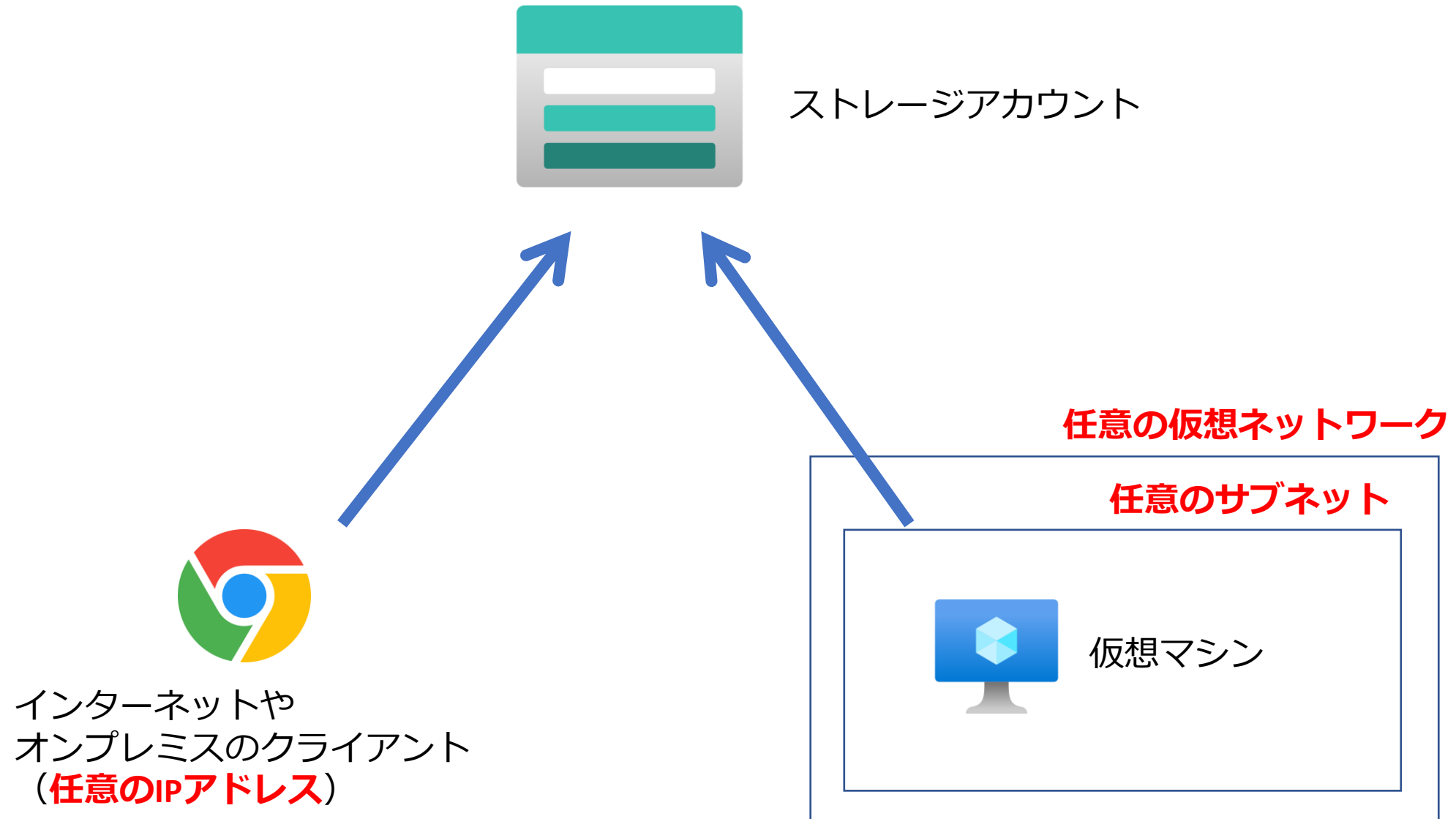
ネットワーク接続

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](#)

デフォルトの設定（「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」）の場合、ネットワーク的には特に制限がかかっておらず、**どのネットワークからでもアクセスが可能**である。
※実際にサービスを利用するには、ネットワークアクセスが可能であることに加え、**認証と承認**も必要。



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 レビュー

ネットワーク接続

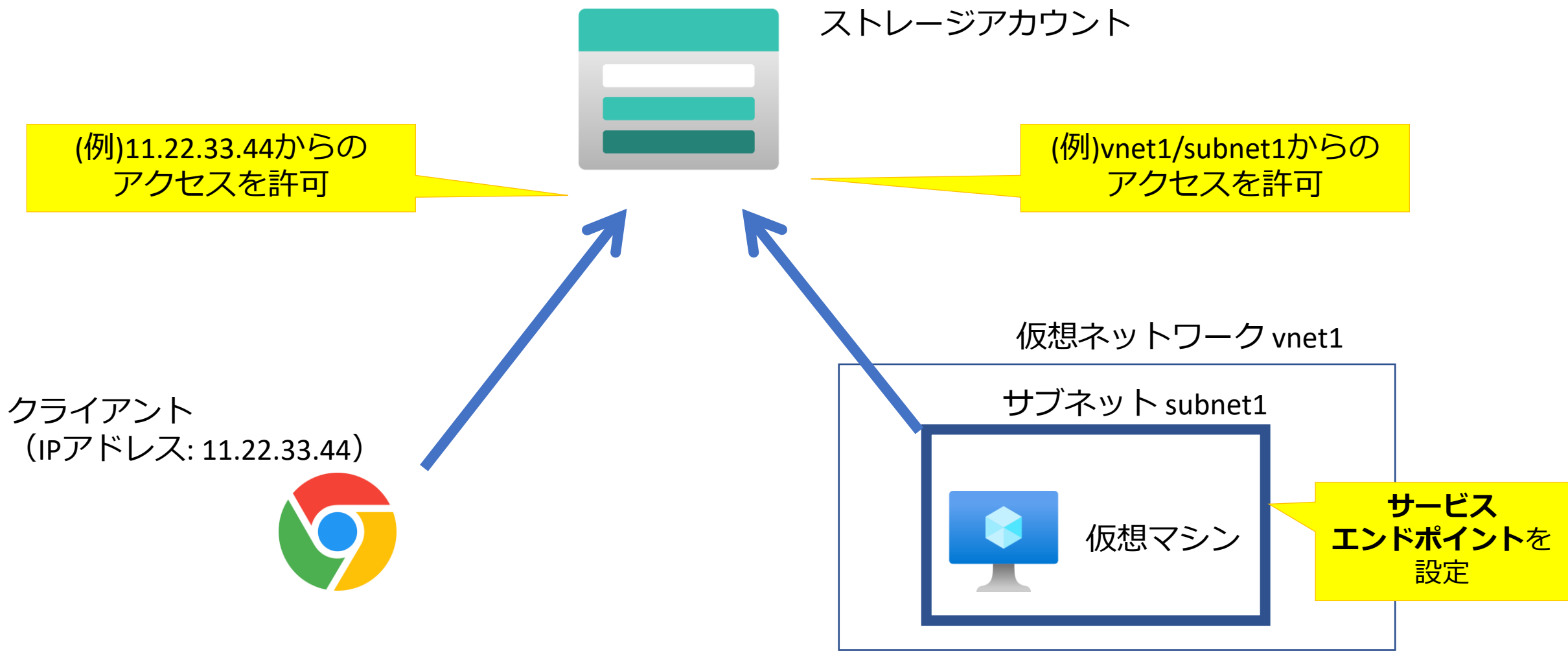
ストレージ アカウントには、パブリック IP アドレスまたはサービス エンドポイント経由で公的に接続することも、プライベート エンドポイントを使用してプライベートに接続することもできます。

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](#)

明示的に指定した**特定のIPアドレス**や、**特定のサブネット**からのアクセスのみを許可し、
その他の場所からのアクセスを禁止できる。



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 レビュー

ネットワーク接続

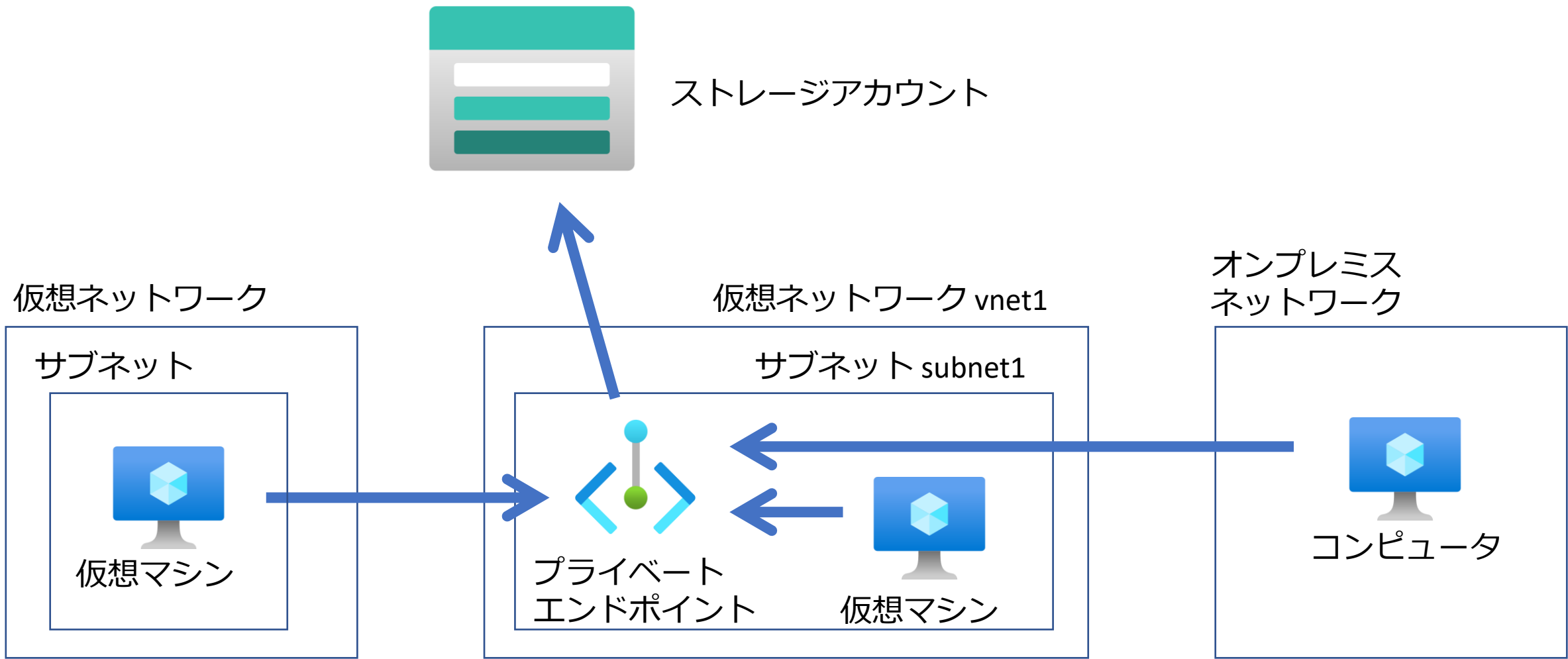
ストレージ アカウントには、パブリック IP アドレスまたはサービス エンドポイント経由で公的に接続することも、プライベート エンドポイントを使用してプライベートに接続することもできます。

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](#)

仮想ネットワークのサブネットの中に**プライベートエンドポイント**を作成し、その**プライベートエンドポイント**からのアクセスのみを許可し、その他の場所からのアクセスを禁止できる。




暗号化


Storage Service Encryption (SSE) とも


暗号化 暗号化スコープ

Storage Service Encryption では、保存データを保護します。Azure Storage では、ユーザーのデータを Microsoft のデータセンターに書き込む時点で暗号化し、ユーザーがアクセスした時点で自動的に暗号化を解除します。

Storage Service Encryption を有効にした後、新しいデータのみが暗号化され、このストレージ アカウントの既存のファイルはすべて、バックグラウンドの暗号化プロセスで遡及的に暗号化されます。[Azure Storage 暗号化に関する詳細情報](#) 

暗号化の選択

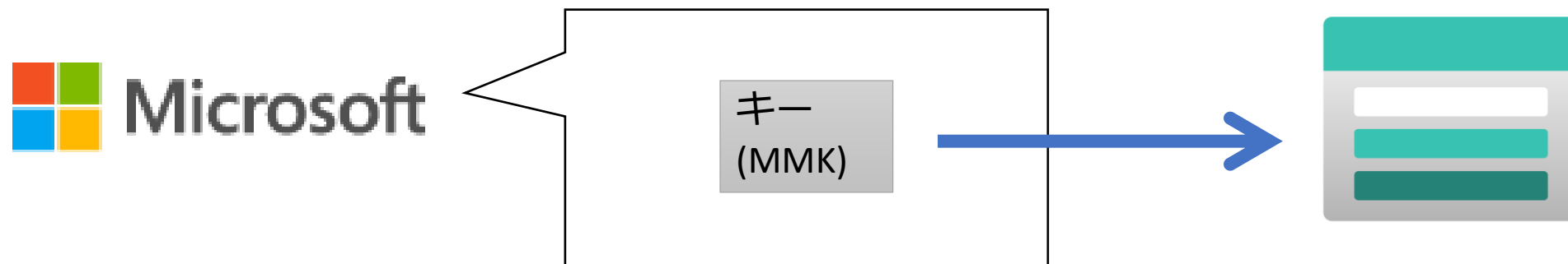
カスタマー マネージド キーのサポートを有効にする  BLOB とファイルのみ

インフラストラクチャ暗号化  無効

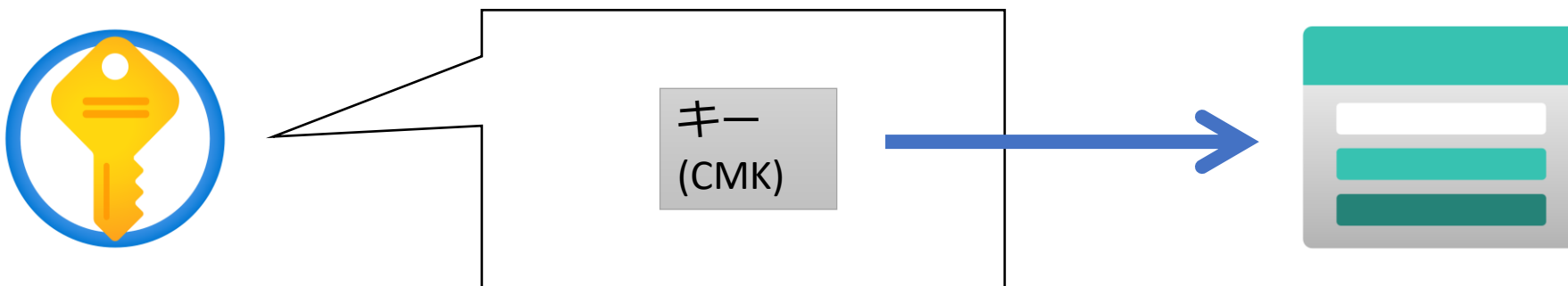
暗号化の種類

- ☒ Microsoft マネージド キー
- ☐ カスタマー マネージド キー

デフォルトでは、ストレージアカウントのすべてのデータは、**Microsoftが管理するキー（Microsoft-managed keys, MMK）**を使用して暗号化・復号が行われる。



キーの運用をユーザーが管理したい場合、**顧客が管理するキー（Customer-managed keys, CMK）**を使用して暗号化・復号を行うように設定できる。**Azure Key Vault**というリソースを準備し、その中に**キー**を作成し、ストレージアカウントでその**キー**を使用するように設定する。



<https://learn.microsoft.com/ja-jp/azure/storage/common/storage-encryption-key-model-get?tabs=portal>

<https://learn.microsoft.com/ja-jp/azure/key-vault/keys/about-keys>

暗号化についてのよくある質問

- そもそもなぜ暗号化を行っているのか？
 - 不正アクセスやデータの持ち出しなどに対する防衛策のひとつ。
- 暗号化するとデータの読み書きに時間がかかるのでは？
 - 原理的にはそうですが、ストレージアカウントのデータの暗号化は常に有効であり、それによって読み書きが特段に遅いということはありません。
- 暗号化は有料？
 - MMKを使用する場合は特に料金はかからない
 - CMKを使用する場合はAzure Key Vaultの料金がかかる
- キーの運用を顧客が行う（CMKを使用する）場合のメリットは？
 - PCI DSSやHIPAAなどの規制に従ってデータ保護やキーローテーションなどを行うことが可能となる
 - キーへのアクセス制御や暗号化設定などを行うことでセキュリティレベルを高めることができる。
 - 例えばRBACやポリシーなどで特定のユーザーやロールだけにキーへの操作権限を付与したり、AES256やRSA2048など強力な暗号化方式やアルゴリズムを選択したりすることができる。

ツール

Azure Storage Explorer: クロスプラットフォームのGUIツール。開発環境やオンプレミスPC上からストレージアカウントの操作が可能。

EXPLORER

Search for resources

Refresh All

Collapse All

Local & Attached

Storage Accounts

Storage Explorer (microsoft.com)

Storage Accounts

asadgulmantest1

asamonaftest

actbizztestab6703

azcodelemetry

Blob Containers

Slogs

abc

lotsofiles

File Shares

Queues

Tables

azuretoolsuxtesting (Classic)

blobversionbugbashja

blobversionbugbashja2

blobversioncentraleuap

blobversioncentraleuap2

blobversioncentraleuap3

blobversioneastuap

blobblobtestchu (Premium)

chetttest

chipchipstest

conftosocsample

coolstorageencrypted (Blob)

Actions

Properties

File Endpoint

Queue Endpoint

Table Endpoint

Web Endpoint

Primary Key

Secondary Key

Primary Connection String

Secondary Connection String

HNS Enabled

https://azcodelemetryfile.com

https://azcodelemetryqueue.

https://azcodelemetrytable.c

https://azcodelemetry.z22.w

.....

.....

.....

.....

false

lotsofiles

Upload

Download

Open

New Folder

Select All

Copy

Paste

Clone

Delete

Undo

Manage History

Folder Statistics

Refresh

Active blobs (default)

lotsofiles > Level-0-Branch-0

Show Filter Panel

Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Type	Size	Status	Remaining Days	Deleted Time
Level-1-Branch-0 Folder									
File-0.txt	Hot	6/23/2020, 10:37:19 AM	11/18/2019, 5:35:42 PM	Block Blob	text/plain; charset=utf-8	836.2 KB	Active		
File-1.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:53 PM	Block Blob	text/plain; charset=utf-8	915.7 KB	Active		
File-101.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:50 PM	Block Blob	text/plain; charset=utf-8	368.5 KB	Active		
File-102.txt	Hot	6/23/2020, 10:37:19 AM	11/18/2019, 5:36:30 PM	Block Blob	text/plain; charset=utf-8	486.3 KB	Active		
File-105.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:08 PM	Block Blob	text/plain; charset=utf-8	826.6 KB	Active		
File-106.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:40 PM	Block Blob	text/plain; charset=utf-8	37.0 KB	Active		
File-107.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:30 PM	Block Blob	text/plain; charset=utf-8	864.9 KB	Active		
File-108.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:50 PM	Block Blob	text/plain; charset=utf-8	302.0 KB	Active		
File-109.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:44 PM	Block Blob	text/plain; charset=utf-8	92.0 KB	Active		
File-11.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:59 PM	Block Blob	text/plain; charset=utf-8	280.1 KB	Active		
File-110.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:33 PM	Block Blob	text/plain; charset=utf-8	63.1 KB	Active		
File-111.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:57 PM	Block Blob	text/plain; charset=utf-8	865.4 KB	Active		
File-112.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:20 PM	Block Blob	text/plain; charset=utf-8	996.9 KB	Active		
File-113.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:36 PM	Block Blob	text/plain; charset=utf-8	227.7 KB	Active		
File-114.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:33 PM	Block Blob	text/plain; charset=utf-8	704.8 KB	Active		
File-115.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:03 PM	Block Blob	text/plain; charset=utf-8	636.5 KB	Active		
File-118.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:05 PM	Block Blob	text/plain; charset=utf-8	770.2 KB	Active		
File-119.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:10 PM	Block Blob	text/plain; charset=utf-8	658.5 KB	Active		
File-120.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:34 PM	Block Blob	text/plain; charset=utf-8	948.4 KB	Active		
File-121.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:50 PM	Block Blob	text/plain; charset=utf-8	650.5 KB	Active		
File-124.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:45 PM	Block Blob	text/plain; charset=utf-8	816.2 KB	Active		
File-125.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:50 PM	Block Blob	text/plain; charset=utf-8	186.2 KB	Active		
File-126.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:58 PM	Block Blob	text/plain; charset=utf-8	687.9 KB	Active		
File-128.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:57 PM	Block Blob	text/plain; charset=utf-8	278.7 KB	Active		
File-13.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:05 PM	Block Blob	text/plain; charset=utf-8	817.1 KB	Active		
File-130.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:38 PM	Block Blob	text/plain; charset=utf-8	531.0 KB	Active		
File-131.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:41 PM	Block Blob	text/plain; charset=utf-8	108.7 KB	Active		
File-132.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:59 PM	Block Blob	text/plain; charset=utf-8	247.7 KB	Active		
File-133.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:30 PM	Block Blob	text/plain; charset=utf-8	791.3 KB	Active		
File-134.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:46 PM	Block Blob	text/plain; charset=utf-8	125.4 KB	Active		
File-135.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:36:16 PM	Block Blob	text/plain; charset=utf-8	14.7 KB	Active		
File-137.txt	Hot	6/23/2020, 10:37:20 AM	11/18/2019, 5:35:53 PM	Block Blob	text/plain; charset=utf-8	393.3 KB	Active		

Showing 1 to 100 of 365 cached items

<< < 1 2 3 4

Activities

Azure portalの「ストレージブラウザー」: 基本的な操作を提供するツール。

st2038482 | ストレージブラウザー

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

Storage Mover

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

st2038482

お気に入り

最近表示した項目

BLOB コンテナー

\$logs

images

すべて表示

ファイル共有

st323

すべて表示

キュー

テーブル

ディレクトリの追加

アップロード

アクセスレベルを変更します

BLOB コンテナー > images

認証方法: アクセス キー (Azure AD のユーザー アカウントに切り替える)

フィルターを追加する

プレフィックスによる BLOB の検索 (大文字と...

アクティブな BLOB のみを表示する

すべての 0 項目の表示

名前	最終変更日	アクセス層	BLOB 0
項目が見つかりませんでした			

その他

- Azure CLI と Azure PowerShell
 - ストレージアカウントの管理、BlobやFilesなどの操作が可能
- AzCopy
 - ストレージアカウントのBlobやFilesの操作が可能なコマンドラインユーティリティ
 - データの転送などに便利な機能を持つ
 - ローカルのファイルシステム、Amazon S3、Google Cloud Storageと接続してデータを転送できる
- Azure Data Factory
 - 様々なデータサービス間でデータの転送が可能

<https://learn.microsoft.com/ja-jp/azure/storage/common/storage-use-azcopy-v10>

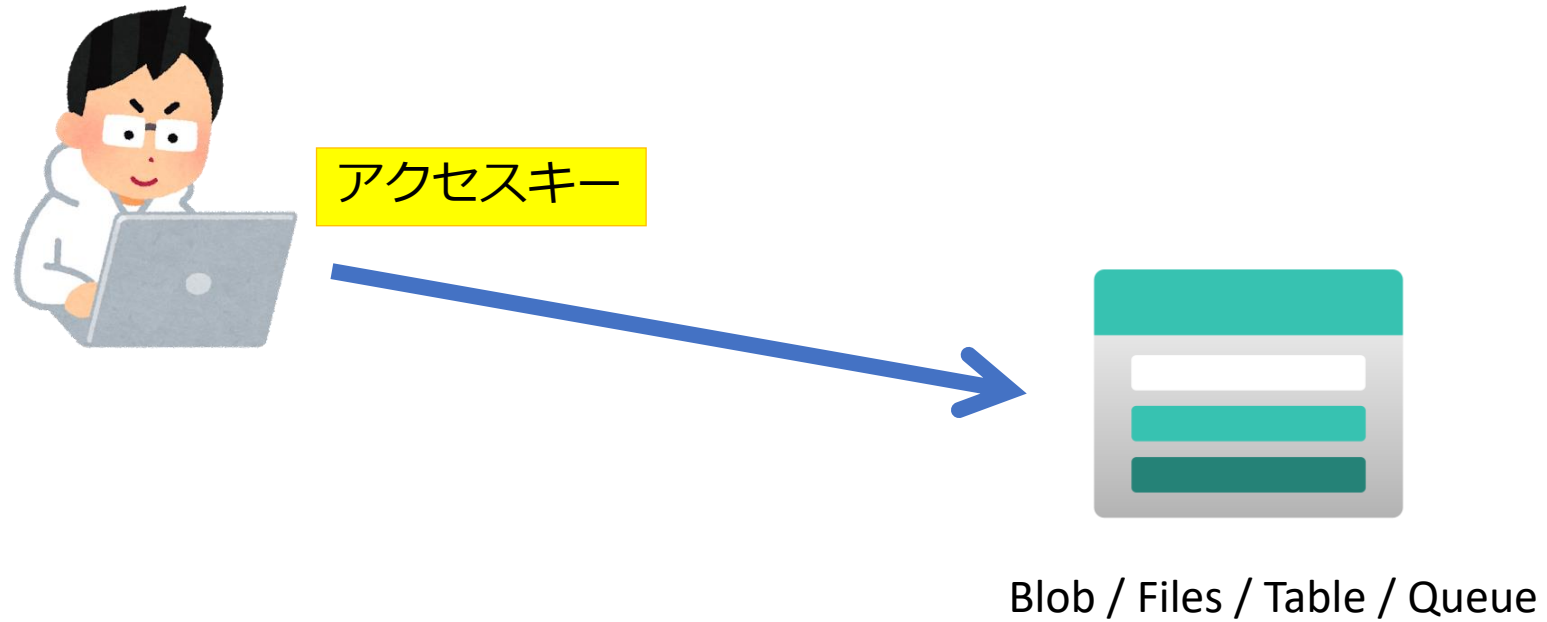
<https://learn.microsoft.com/ja-jp/azure/data-factory/connector-azure-blob-storage>

アクセス制御

アクセスキー、Azure AD認証とロール

表示

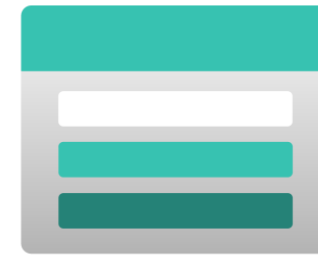
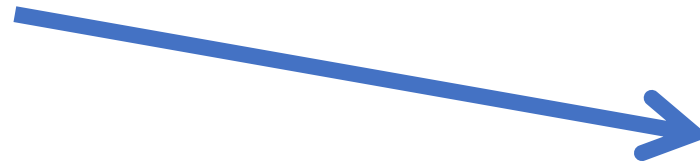
ストレージアカウントの「アクセスキー」を使用すると、そのストレージアカウントに対するフルアクセスが許可される。



もし「アクセスキー」が漏洩してしまうと・・・



アクセスキー



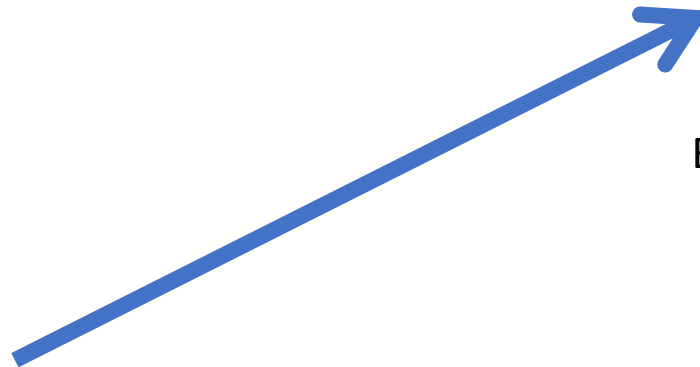
Blob / Files / Table / Queue

データ破壊・漏洩・改ざん

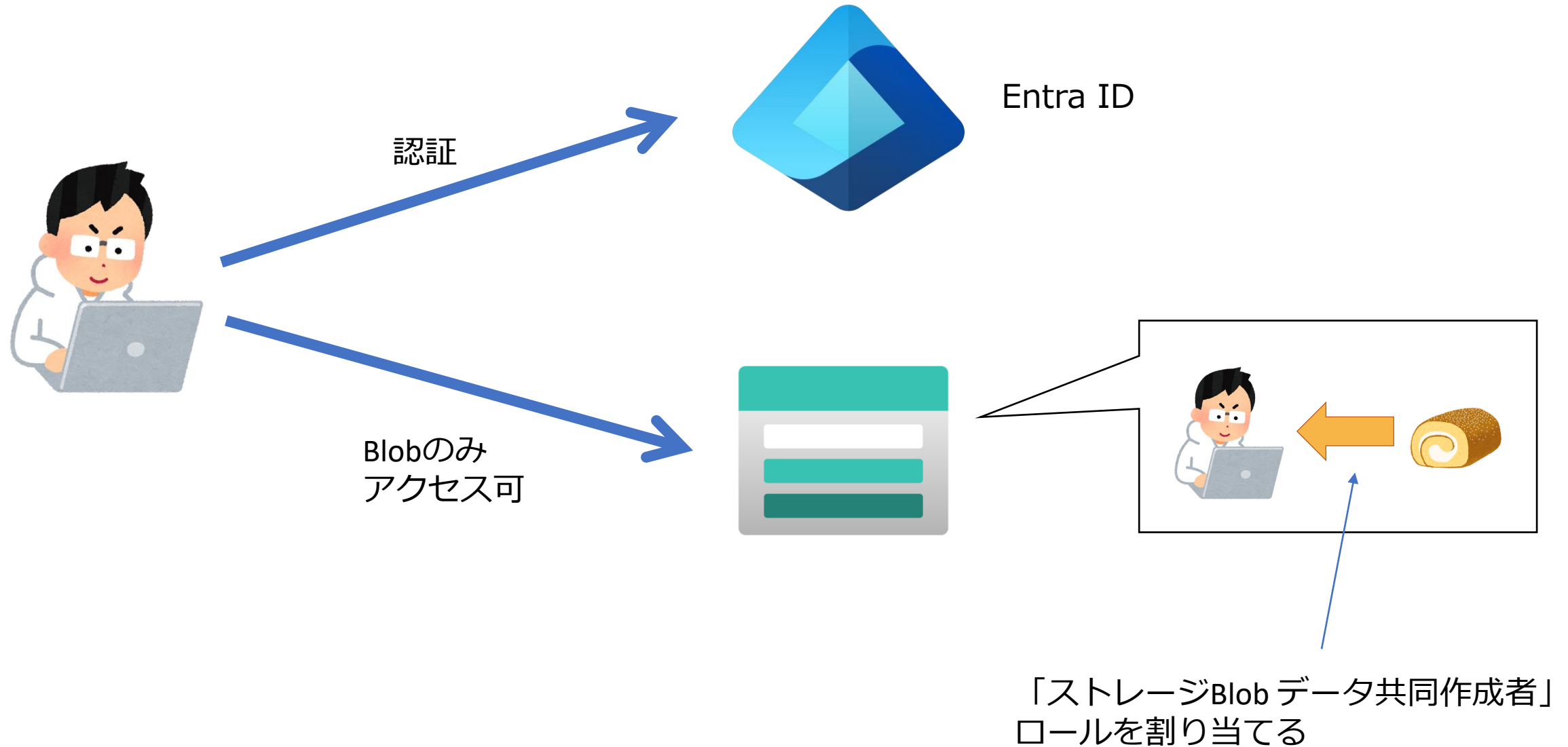


暗号化、身代金要求
(ランサムウェア)

アクセスキー



アクセスキーのような漏洩の危険がない「Entra ID認証」と「ロール」を使用しましょう。
ロールを使用することで、アクセスの許可も、より絞り込むことができます。





st2038482 | アクセス制御 (IAM)

ストレージ アカウント



検索



追加



ロール割り当てのダウンロード



列の編集



最新の情報に更新



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

Storage Mover

データ ストレージ

コンテナー

ファイル共有

キュー

ロールの割り当ての追加

共同管理者の追加

役割

拒否の割り当て

従来の管理者

ロールの割り当ての追加

マイ アクセス

このリソースへのアクセス レベルを表示します。

マイ アクセスの表示

アクセスの確認

ユーザー、グループ、サービス プリンシパル、マネージド ID がこのリソースに対して持つアクセス レベルを確認します。 [詳細情報を見る](#)

アクセスの確認


このリソースへのアクセス権の付与

ロールを割り当てることで、リソースへのアクセス権を付与します。

[詳細情報を見る](#)

ロールの割り当ての追加 ...

ロール メンバー 条件 (省略可能) レビューと割り当て

ロールの定義は、アクセス許可のコレクションです。組み込みロールを使用するか、カスタム ロールを作成することができます。 [詳細情報を見る](#) 

割り当ての種類

職務ロール 特権管理者ロール

仮想マシンを作成する権限など、職務に基づいた Azure リソースへのアクセス権を付与します。

 blob × 種類: すべて カテゴリ: すべて

名前 ↑↓

説明 ↑↓

Storage Blob デリゲータ

SAS トークンの署名に使用できるユーザーの委任キーの生成を許可します

ストレージ BLOB データ閲覧者

Azure Storage Blob コンテナおよびデータに対する読み取りアクセスを許可します

ストレージ BLOB データ共同作成者

Azure Storage Blob コンテナおよびデータに対する読み取りアクセス、書き込みアクセス、削除アクセスを許可します

ストレージ BLOB データ所有者

Azure Storage Blob コンテナとデータに対するフル アクセス (POSIX アクセスの制御の割り当てを含む) を許可します。

< 前へ

ページ

1

▼

/1

次へ >

ロールの割り当ての追加 ...

ロール

メンバー

条件 (省略可能)

レビューと割り当て

選択されたロール

ストレージ BLOB データ所有者

アクセスの割り当て先

☒ ユーザー、グループ、またはサービス プリンシパル

☐ マネージド ID

メンバー

+ メンバーを選択する

名前

オブジェクト ID

メンバーが選択されていません

レビューと割り当て

前へ

次へ

メンバーを選択する



選択 ⓘ

yamada



yamada

yamada@contoso1800.onmicrosoft.com

選択したメンバー:

メンバーが選択されていません。このロールに割り当てるメンバーを 1 人以上検索し、このリソースに対して追加してください。

[RBAC の詳細](#)

選択

閉じる

Blobコンテナーへのアクセス時にAzure AD認証とロールを利用するには

ホーム > ストレージ アカウント > st2038482 | コンテナ >

images

コンテナ

検索

概要

問題の診断と解決

アクセス制御 (IAM)

設定

共有アクセス トークン

アクセス ポリシー

プロパティ

メタデータ

アップロード

アクセス レベルを変更します

更新

削除

認証方法: アクセス キー

(Azure AD のユーザー アカウントに切り替える)

場所: images

プレフィックスによる BLOB の検索 (大文字と小文字を区別)

削除された Blob を表示

フィルターの追加

名前	変更日時	アクセス層	アーカイブ
BLOB が見つかりませんでした。			

Azure AD認証と
ロールを使用して
アクセスするモードに
切り替える

ストレージアカウントで、アクセスキーによるアクセスを無効化するには

ホーム > ストレージ アカウント > st2038482

 **st2038482 | 構成** ☆ ☆ ...

ストレージ アカウント

検索

Shared Access Signature

暗号化

Microsoft Defender for Cloud

データ管理

冗長性

データ保護

オブジェクト レプリケーション

BLOB インベントリ

静的な Web サイト

ライフサイクル管理

Azure Search

設定

 **構成**

Data Lake Gen2 のアップグレード

リソースの共有 (CORS)

保存 破棄 最新の情報に更新 フィードバックの送信

ストレージ アカウントのコストは、使用量と、下で選ぶオプションに応じて決まります。 [ストレージの価格に関する詳細](#)

アカウントの種類
StorageV2 (汎用 v2)

パフォーマンス ①
☒ Standard ☐ Premium

① ストレージ アカウントが作成された後にこの設定を変更することはできません。

安全な転送が必須 ①
☐ 無効 ☒ 有効

BLOB パブリック アクセスを許可する ①
☐ 無効 ☒ 有効

ストレージ アカウント キーへのアクセスを許可する ①
☐ 無効 ☒ 有効

Shared Access Signature (SAS) の有効期限間隔に対して推奨される上限を許可する ①
☒ 無効 ☐ 有効

Azure portal で Azure Active Directory の承認を既定にする ①
☒ 無効 ☐ 有効

TLS の最小バージョン ①