



# 【Microsoft Azure】 VM不具合時の トラブルシューティング

2025年4月30日

# 改定履歴

版数	発行日	改訂内容
第1版	2025年4月30日	初版発行

資料の内容は2025/4/30 時点のものです。製品のアップデートにより変更となる場合がございます旨をご了承ください。

# Agenda

## 1. 前提情報

1. 前提条件
2. 本資料の目的とゴール
3. 用語集

## 2. トラブルシューティングの流れ

1. トラブルシューティングの流れ

## 3. 基盤障害の確認方法

1. Azure Service Healthについて
2. 基盤障害の確認方法

## 4. 事象別VM トラブルシューティング

1. VMへのRDP接続不可



# 1. 前提情報

## 1.1. 前提条件

- 本書に記載するサービス仕様、サービス名称などの各情報については、2025年4月時点でのサービス仕様に基づくものとしております。
- 本書は、Windows Server 2022のキャプチャを利用しております。
- ドメイン参加済みの Windows Server 2022 を使用することをお勧めします。Microsoft Entra Connect は Windows Server 2016 にデプロイできますが、Windows Server 2016 は延長サポートであるため、この構成に支援が必要な場合は有償サポート プログラムが必要になることがあります。

## 1.2. 本書の目的とゴール

### 目的

Azure仮想マシン（VM）で不具合が発生した際に、サポート担当者が迅速かつ的確に原因を特定し、適切な対応を行えるよう、標準的な切り分け手順を提供することを目的とする。

### ゴール

本資料を学ぶことで、以下の内容を理解し、顧客からの問い合わせに対してスムーズに切り分けし調査の依頼ができる状態を目指します

1. VMの不具合の問い合わせに対して、原因の切り分けが可能なスキルを習得する。
2. 切り分けの各ステップで活用できるAzureポータルやログ、診断ツールの使い方を理解する。
3. 初動対応に迷わず、切り分け手順の案内をスムーズに行えるようになる。

## 1.3. 用語集

本書で使用する用語及び略称を以下の通り定義します

No	用語	説明
1	NIC (ネットワークインターフェイス)	Azure 仮想マシン (以下VM) がネットワークと通信をするための窓口のような役割であり、VM)がインターネット、Azure、およびオンプレミスのリソースと通信できるようにするためにはNICが必要です。Azure ポータルで作成される VM には、既定の設定で 1 つの NIC があります。NICは仮想ネットワーク (以下Vnet) 内でVMが他のリソースやインターネットと通信するためのIPアドレスや設定情報を保持しています。
2	NSG (ネットワークセキュリティグループ)	ネットワークセキュリティグループは、Microsoft Azure上でVNet内のトラフィック (通信) を制御するセキュリティツールであり、VnetのサブネットおよびVMの仮想ネットワークインターフェイスで構成できる IP ファイアウォールです。NSGでは、外から内と内から外への送受信のセキュリティ規則を設定できます。



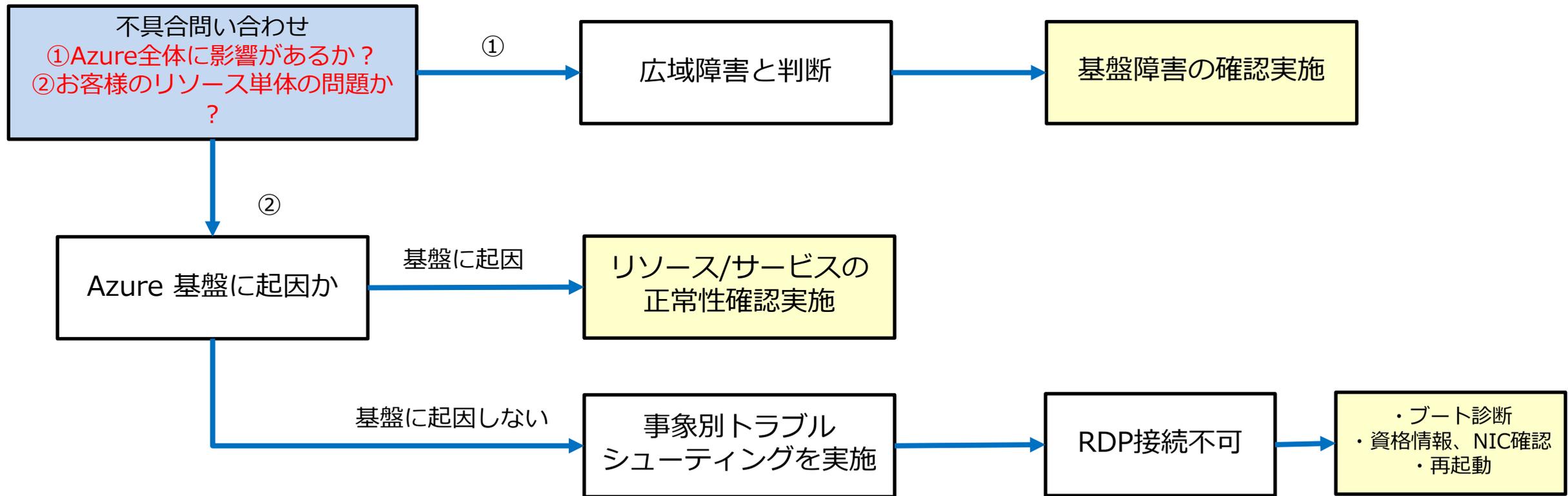
## 2. トラブルシューティングの流れ

## 2.1. トラブルシューティングの流れ

一般的な調査の流れの考え方について以下に記載しています。

「Azure全体」 = 「広域障害かどうか」の確認には Azure Service Health の活用が重要です。

「Azure基盤に起因するかどうか」の判断には Resource Health の確認が有効です。



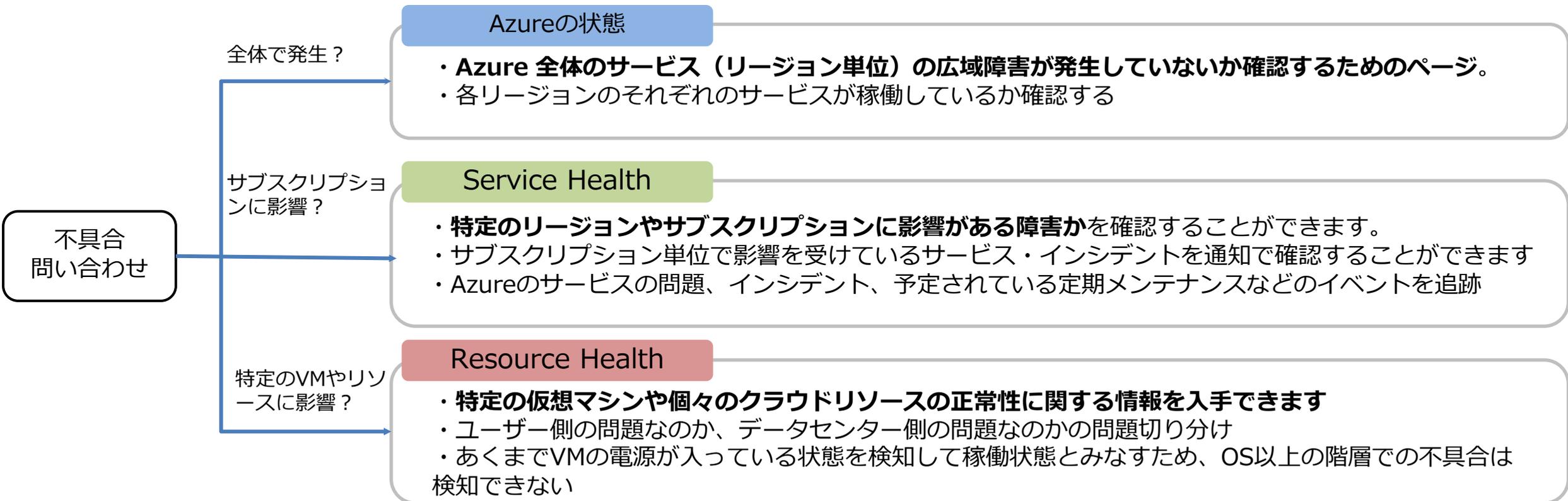


### 3. 基盤障害の確認方法

# 3.1. Azure Service Healthについて

## ■ Azure Service Health

Azureの障害や計画的メンテナンス、可用性に影響する可能性のある変更などを把握するためのサービスです。  
Azure Service Health は次の3つのサービスがあり、それぞれの特徴と確認ポイントは以下となります。



## 3.2. 基盤障害の確認方法

### Azureの状態

主にサービス機能全体に与える障害やリージョンに対する障害が発生しているか確認時に有効です。

一方で個別の障害に対してどのような問題が発生しているかを知るには不向きとなります。

The screenshot shows the Azure Status page. The 'Asia-Pacific' region is selected, and the 'East Japan' and 'West Japan' sub-regions are highlighted with a red box. The table below shows the status of various services in these regions.

製品およびサービス	オーストラリア東部	オーストラリア中部	オーストラリア西部	インド中部	インド南部	東日本	西日本	韓国中部	韓国南部	ニュージーランド
コンピューティング										
Azure VMware Solution	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
CloudSimple による Azure VMware ソリューション	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
Batch	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常

正常 情報 警告 重大 -- 該当なし

### ■手順

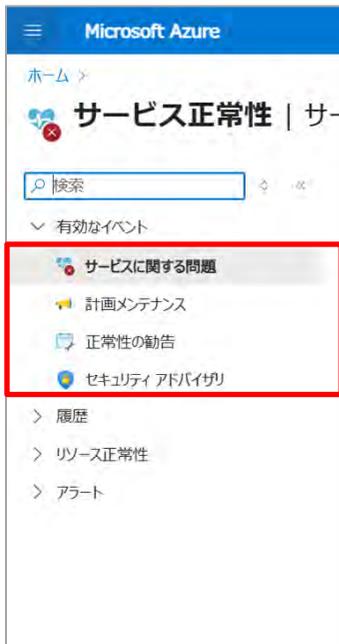
1. 以下のページにアクセスします  
<https://azure.status.microsoft.com/ja-jp/status>
2. 「アジア太平洋」タブの、[東日本]、[西日本]の該当製品、サービスのステータスを確認します。  
正常な場合は「正常」と表示されます。

## 3.2. 基盤障害の確認方法

### Service Health

リージョン規模の障害や自分のサブスクリプションなど大規模な障害があった場合に利用者がダッシュボードから確認したり、サービス正常性アラートとしてルールを登録しておくことで問題が発生した時などに通知を受け取ることができます。

Service Healthは障害だけでなく、次の4つに分類されたイベントを確認・追跡することができます。



No	イベントの種類	説明	確認できること
1	サービスに関する問題	現在発生中の障害など、利用に影響を与える情報を表示	<ul style="list-style-type: none"><li>発生している障害の概要</li><li>影響を受けているリージョンやサービス名</li><li>Microsoft社の対処状況 等</li></ul>
2	計画メンテナンス	可用性に影響する可能性がある、事前に予定されているメンテナンス作業の情報を表示	<ul style="list-style-type: none"><li>影響の有無</li><li>対象のリージョン/サービス</li><li>事前の通知の内容とスケジュール 等</li></ul>
3	正常性の勧告	Azureの機能の変更点。パフォーマンスやセキュリティに関する注意喚起などの表示	<ul style="list-style-type: none"><li>非推奨な設定の利用、古いバージョンの利用に関する警告</li><li>セキュリティ上の推奨されるアクション</li></ul>
4	セキュリティアドバイザリ	可用性に影響する可能性があるセキュリティ関連の通知や違反。セキュリティ脆弱性情報やその対策を表示	<ul style="list-style-type: none"><li>影響を受けるサービスリージョン</li><li>脆弱性の概要とリスクレベル 等</li></ul>

## 3.2. 基盤障害の確認方法

### Resource Health

Resource Health は、さまざまな Azure サービスからの信号を基に、リソースが正常であるかどうかを評価します。

リソースの正常性に関するパーソナライズされたダッシュボードを提供し、仮想マシンなどリソース単位で状態を確認したり、過去に発生した障害を確認することができます。

リソースが正常でない場合、Resource Health は追加の情報を分析して問題の原因を特定します。

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar with the text 'リソース、サービス、ドキュメントの検索 (G+/)', and the Copilot logo. The main content area is titled 'サービス正常性 | リソース正常性'. On the left, there is a navigation pane with a search bar and several menu items: '有効なイベント', 'サービスに関する問題', '計画メンテナンス', '正常性の勧告', 'セキュリティアドバイザー', '履歴', 'リソース正常性', and 'アラート'. The 'リソース正常性' item is highlighted with a red box. In the main content area, there are two dropdown menus: 'サブスクリプション' (Subscription) and 'リソースの種類' (Resource type). The 'サブスクリプション' dropdown is set to 'Azure subscription 1' and is highlighted with a red box. The 'リソースの種類' dropdown is set to '仮想マシン' (Virtual Machine) and is also highlighted with a red box. Below these dropdowns, there is a table with columns for 'リソース名' (Resource name) and '種類' (Type). The table is currently empty, with a note below it: 'ド롭ダウンからリソース タイプを選択します。' (Select resource type from the dropdown).

#### ■ 手順

1. 「サービス正常性」 > 「リソース正常性」をクリックします
2. [サブスクリプション]を選択し、[リソースの種類]から「仮想マシン」を選択します

## 3.2. 基盤障害の確認方法

リソース名	種類	場所	サブスクリプション
 AzureVM	仮想マシン	japaneast	Azure subscription 1

ホーム > サービス正常性 | リソース正常性 >

### リソース正常性

AzureVM

+ リソース正常性アラートの追加 [問題の診断と解決](#)

リソース正常性ではリソースが監視されるので、正しく動作しているかどうか分かります。 [詳細情報](#)

 **利用できません**

許可されているユーザーまたはプロセスからの要求によって、この仮想マシンは停止および割り当て解除されました。

実行できる操作

1. 問題が発生している場合は、[トラブルシューティング ツール](#) を使用して、推奨される解決策をご確認ください。

正常性の履歴

日付	説明
> 04/24/2025	 1 正常性イベント

- 対象のサブスクリプションの仮想マシンが表示されるので、クリックして詳細を表示します。
- [利用可能],[利用できません]と表示されます。(左の例は[利用できません]と表示)
- 正常性の履歴から、最大30日間の履歴を確認することが可能です。



## 4. 事象別トラブルシューティング

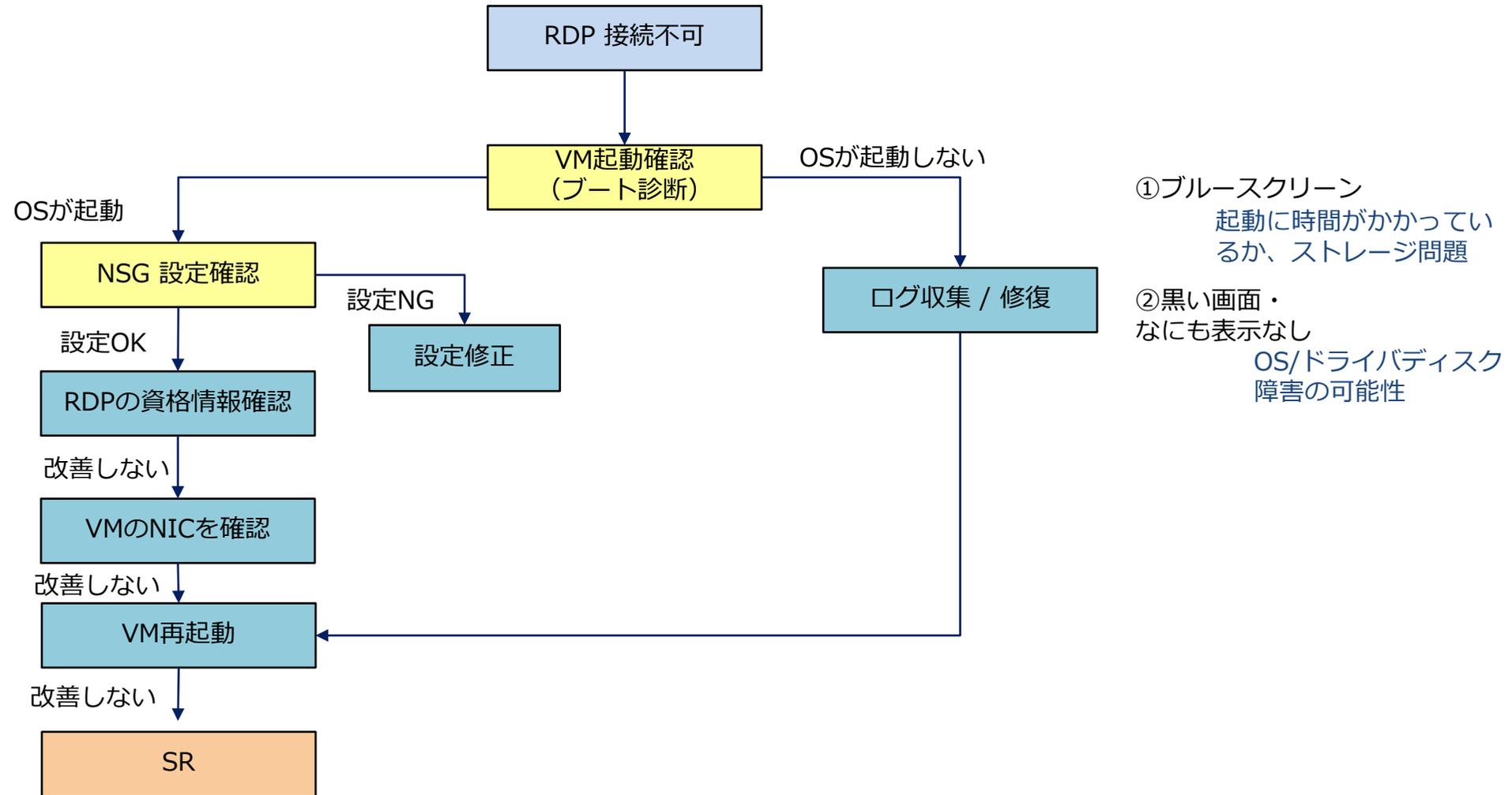


## 4.1. VMへのRDP接続不可

## 4.1.1. 切り分け手順

以下のフローに沿って切り分けを行っていきます。

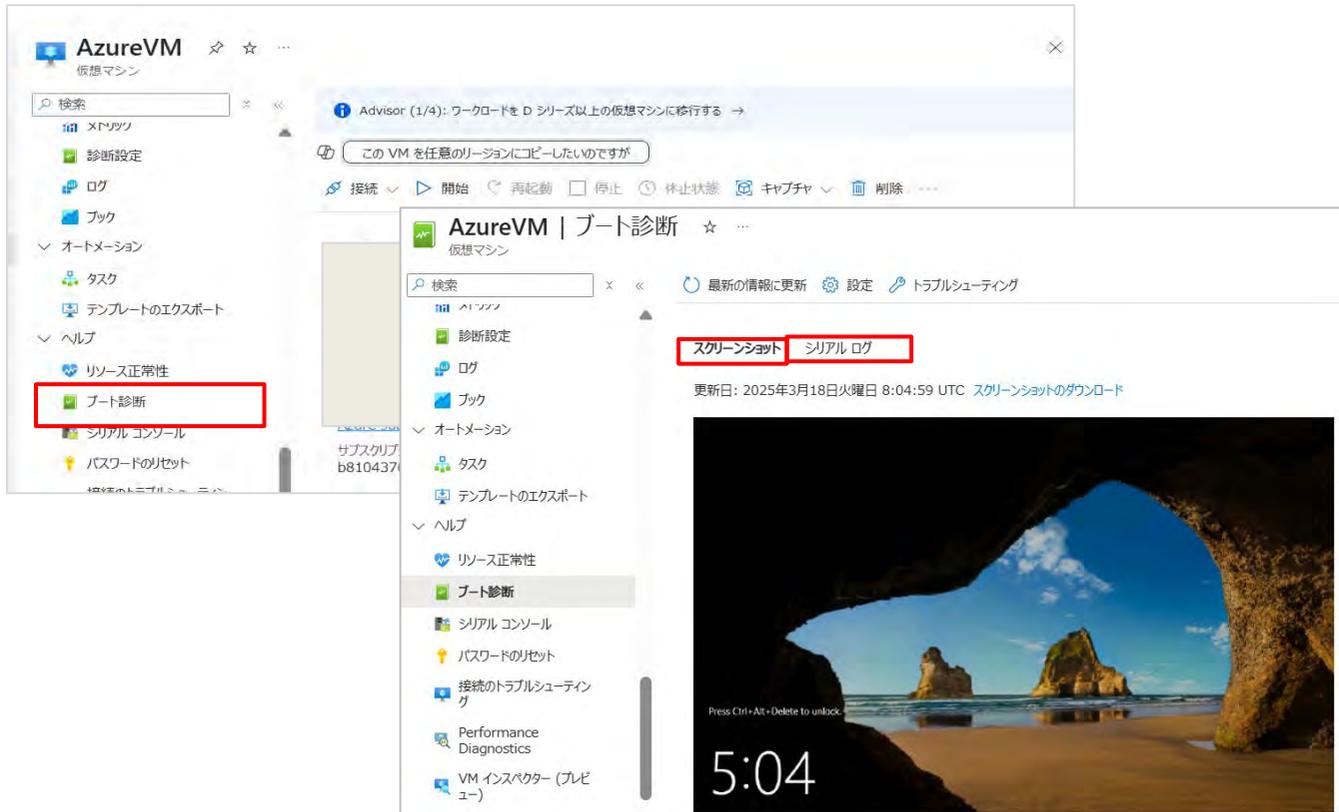
VM再起動を実施しても事象が改善しない場合は、詳細な調査を行うべくSRを投げるフローとしています。



# 4.1.2 VMの起動確認

## 概要

起動確認方法としてブート診断機能を利用します。(VM作成時に、ブート診断は既定で有効になっています。)  
ブート診断は、VMブートエラーの診断を可能にする、VMのデバッグ機能です。  
ブート診断を有効化することで、**Azureポータル上からOSの画面ショットとシリアルログ情報を収集し、起動中のVMの状態を確認することができます。** OSレベルで正常に起動しているか否かを判断するのに役立つ機能となります。



## 手順

1. Azureポータルから対象VMを選択します
2. 左メニューから「ブート診断」をクリックします
3. 表示されるスクリーンショットが表示によって以下のことが考えられます。

- 左の図のようにデスクトップが映っている場合  
→OSの問題はない（ネットワーク被疑の可能性あり）
- ブルースクリーンや画面が黒い場合などはOSがクラッシュしている可能性が考えられます。確認・対処方法は次のページにて説明します。

## 4.1.2 VMの起動確認

### ブルースクリーン・黒い画面の際の対処方法

ブルースクリーンや画面が黒く表示され（何も表示されない）場合は、OS起動に時間がかかっている場合や、ストレージに問題がある可能性がございます。

ブート診断を実行しエラーコード確認後、エラーコードに対して調査、又は適切な対応を実施します。対応方法はエラーコードにより異なる為、Microsoftの公式ページを参考に対応を進めます。

以下は、代表的なエラーコード一覧となります。

（※下記エラーコードをクリックしますと、それぞれのエラーコードのページに遷移いたします。）

- [0xC000000E](#)
- [0xC000000F](#)
- [0xC0000011](#)
- [0xC0000034](#)
- [0xC0000098](#)
- [0xC00000BA](#)
- [0xC000014C](#)
- [0xC0000221](#)
- [0xC0000225](#)
- [0xC0000359](#)
- [0xC0000605](#)

# 4.1.3. NSGの設定確認

## 概要

ネットワークセキュリティグループ (NSG) の規則を確認し、RDPポート (TCP3389) が正しく許可されているか、適切な規則が設定されているかを確認します。

The screenshot shows the Azure portal interface for an Azure VM. The left sidebar contains navigation options like '概要', 'アクティビティ ログ', 'アクセス制御 (IAM)', and 'ネットワーク'. The main content area shows 'ネットワーク設定' (Network settings) for the VM 'azurevm42 (プライマリ) / ipconfig1 (プライマリ)'. A red box highlights the 'ネットワーク インターフェイス / IP の構成' section. Below this, the '受信セキュリティ規則' (Inbound security rules) table is displayed with a red box around the '3389,22' port value in the first rule.

優先度 ↑	名前 ↑↓	ポート ↑↓	プロトコル ↑↓	ソース ↑↓
100	AllowCidrBlockInbound	3389,22	TCP	10.0.1.0/26
65000	AllowVnetInBound	任意	任意	VirtualNetwork
65001	AllowAzureLoadBalanc...	任意	任意	AzureLoadBalancer
65500	DenyAllInBound	任意	任意	任意

## 手順

1. Azureポータルから仮想マシンを選択します。
2. ネットワーク設定 > ネットワークインターフェイスをクリックします
3. インターフェイスに適用されているNSGを確認します
4. 「受信規則」をクリックします
5. ポート [ 3389 ] が適切な優先順位 (数値が低い程優先されます) で設定され、登録されていることを確認します

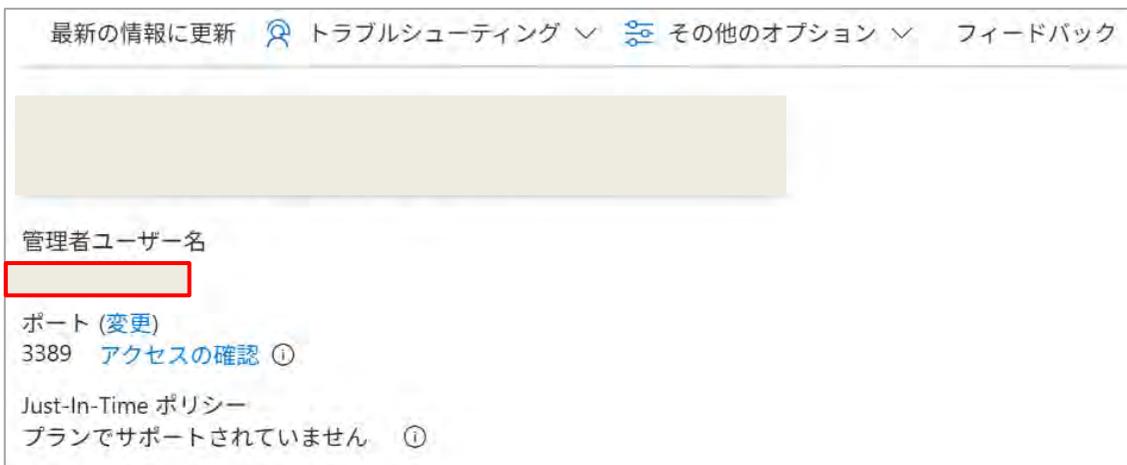
## 4.1.4. RDPの資格情報確認

### 概要

ヒューマンエラーにより資格情報に誤りがありRDP接続が出来ない場合、下記の手順に沿って対応致します。  
※RDP資格情報の確認またはリセットを行う際の手順を記載いたします。

### 手順

1. Azureポータルから対象のVMを選択
2. 「接続」→[ 管理者ユーザ名] に記載されているものが必要な資格情報となります。RDP接続時に入力しているID情報と相違が無いかを確認いたします。



最新の情報に更新 [トラブルシューティング](#) [その他のオプション](#) フィードバック

管理者ユーザー名

ポート (変更)  
3389 [アクセスの確認](#)

Just-In-Time ポリシー  
プランでサポートされていません

## 4.1.4. RDPの資格情報確認

### 概要

ログインIDに問題がない場合、パスワードの再発行を実施し対応いたします。

※RDPに必要なID情報はAzure上で確認が行えますが、パスワードの確認が行えない為、再発行にて対応いたします。

### 手順

この場合、VMAccess 拡張機能を使用して、あらかじめ登録された Administrator アカウントとリモート デスクトップ サービス構成がリセットされます。VM にログイン後、対象ユーザーのパスワードをリセットする必要があります。

[詳細情報](#)

モード \* ①

パスワードのリセット

構成のみのリセット

ユーザー名 \* ②

パスワード \*

パスワードの確認 \*

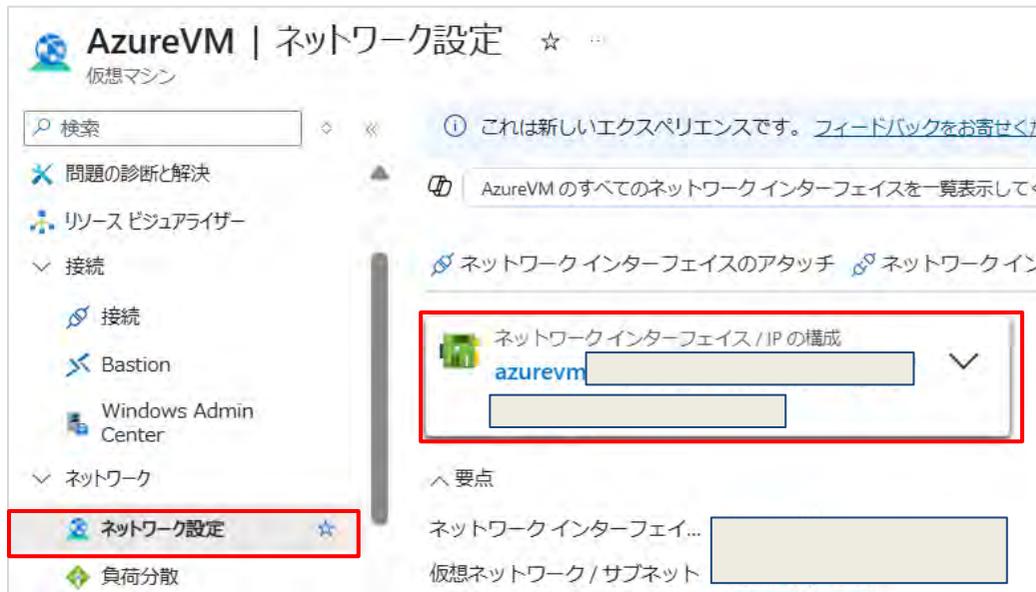
更新

1. Azureポータルから対象のVMを選択
2. 「ヘルプ」→「パスワードのリセット」こちらにチェックを入れパスワードの更新を行います。
3. 新しいパスワードを入力しRDP接続が行えるかを確認。

## 4.1.5. VMのNICの確認

### 概要

NICをリセットすることで、ネットワーク経路のソフト不整合、キャッシュのずれ等が原因かがわかります。



AzureVM | ネットワーク設定 ☆

仮想マシン

検索

問題の診断と解決

リソース ビジュアライザー

接続

接続

Bastion

Windows Admin Center

ネットワーク

ネットワーク設定 ☆

負荷分散

これは新しいエクスペリエンスです。フィードバックをお寄せください

AzureVM のすべてのネットワーク インターフェイスを一覧表示して

ネットワーク インターフェイスの アタッチ ネットワーク イン

ネットワーク インターフェイス / IP の構成

azurevm

要点

ネットワーク インターフェイ...

仮想ネットワーク / サブネット

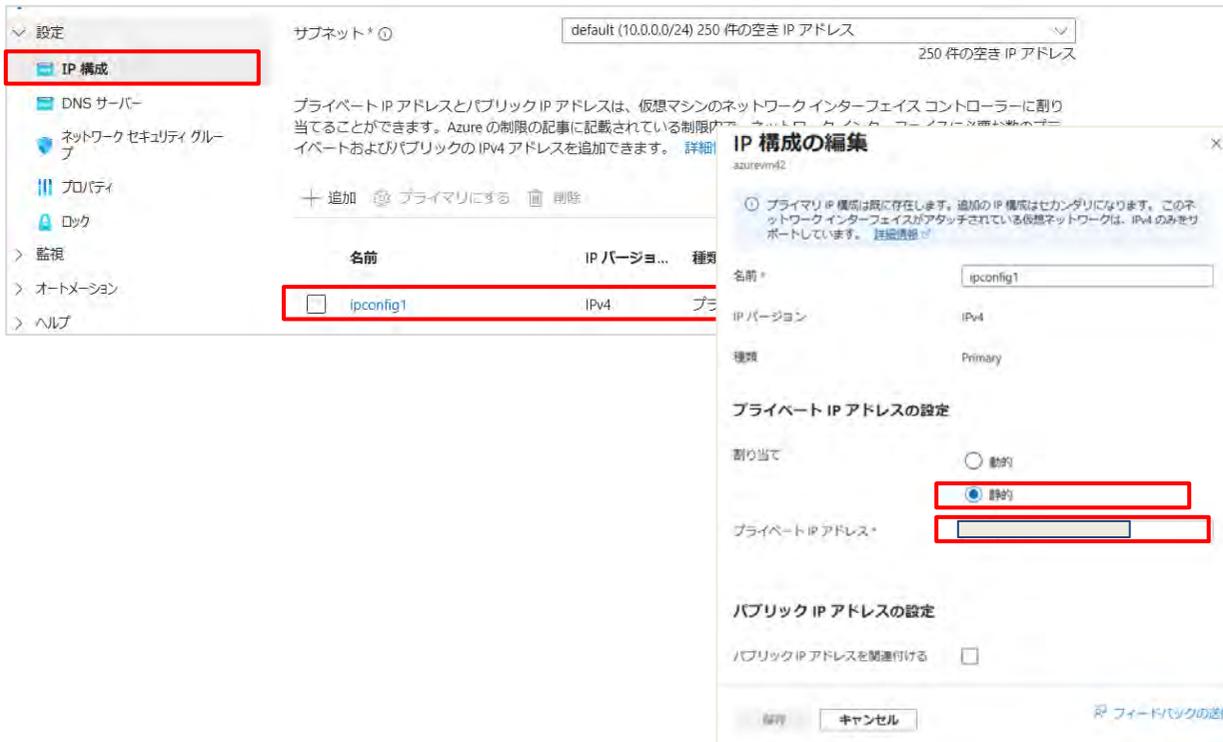
### 手順

#### Azure Portalを使用したNICリセット方法

※[ほかにAzure Power Shell ,Azure CLIを使用した方法もあります](#)

1. Azurポータルにアクセスします  
<https://portal.azure.com>
2. 影響を受ける仮想マシンを選択します
3. [ネットワーク設定] から、VMのネットワークインターフェイスを選択します。

## 4.1.5. VMのNICの確認



4. [IP構成]から、対象のIPを選択しクリックします
5. プライベートIPの割り当てが「静的 (Static) 」でない場合は「静的」に変更します
6. [IP アドレス] を、サブネットで使用できる別の IP アドレスに変更します。
7. 仮想マシンを再起動して、新しい NIC を確認します。
8. RDP を使用してマシンに接続を試みます。

接続確認後、必要に応じて元のプライベート IP アドレスに戻すことができます。あるいは、そのまま保持することもできます。

## 4.1.6. VMの再起動

### 概要

OS内部のサービスの原因やドライバ不具合が原因の場合、VMを再起動することで改善することがあります。

### 注意点

- ・ゲストOSがシャットダウン～ブートし直す間、数分～十数分オフラインとなります。  
バッチやユーザー接続に影響がでますので、実行時間を考慮するなどし実行する必要があります。

### 手順

1. Azurポータルにアクセスします  
<https://portal.azure.com>
2. 影響を受ける仮想マシンを選択します
3. 画面上部の「再起動」をクリックします
4. 確認画面が表示されるので、「はい」をクリックします
5. 再起動完了の画面が表示されましたら、再度接続が可能か確認します

