

# ネットワーク通信異常時 の情報採取について

2022 年 12 月 08 日（第 1.0 版）

富士通クラウドテクノロジーズ株式会社

## 目次

1. はじめに .....	3
2. 通信異常の詳細な内容 .....	4
3. ネットワーク構成図 .....	4
4. 問題の切り分けのために行った作業内容 .....	4
5. 実施していただきたい切り分けの例 .....	5
6. パケットキャプチャの取得場所 .....	6
7. 参考情報 .....	7
8. 改訂履歴 .....	8

## 1. はじめに

本資料では、ネットワーク通信不安定・通信断が発生した際に、被疑箇所を特定するために行う適切な切り分け作業やサポート窓口へお問い合わせいただく時の情報採取など、問題の早期解決に役立つポイントをまとめております。具体例も掲載していますのでぜひご参照ください。

- 本資料は、「トラブルの早期解決が期待できるお問い合わせ方法」の補足資料となります。

公式サイト【トラブルの早期解決が期待できるお問い合わせ方法】

[https://pfs.nifcloud.com/inquiry/best\\_practice.htm](https://pfs.nifcloud.com/inquiry/best_practice.htm)

- 下記 FAQ も合わせてご参照ください。

ニフクラ FAQ 「ネットワーク疎通ができません。」

<https://faq.support.nifcloud.com/faq/show/372>

ニフクラ FAQ 「ネットワーク通信異常関連」の FAQ 一覧

<https://faq.support.nifcloud.com/category/show/129>

## 2. 通信異常の詳細な内容

認識齟齬が生じた場合は問題解決の遅延に繋がるため、発生事象を正確に伝える必要があります。  
下記項目が含有される様に整理いただき、ご連絡ください。

- ① 通信の概要  
利用しているプロトコル・ポート番号、etc
- ② 事象の概要  
応答がない、パケット不達、etc
- ③ 事象が発生した時間、頻度
- ④ 事象発生直前に実施した作業  
サーバーやルーターなどのネットワーク設定変更、サーバーの再起動、etc
- ⑤ 事象のステータス  
一時的か、継続中か

## 3. ネットワーク構成図

下記情報が確認できるネットワーク構成図をご準備ください。

- ① NIFCLOUD 環境の構成
- ② 送信元、宛先サーバーの所属するネットワーク
- ③ 途中経路上に存在する機器  
ルーター、ファイアウォール、ロードバランサー、etc
- ④ 事象に関連するインスタンスの IP アドレス

抜粋などは必要なく、既存物で構いません

※ただし、情報が細かすぎると構成確認に時間を要するので、適度な粒度の物をお願い致します。

## 4. 問題の切り分けのために行った作業内容

お客様が問題の切り分けのために行った作業（事象発生直前に行っていた作業があれば、その作業内容も含む）を詳細にご記載ください。以下の様なレベル感でまとめていただけると助かります。

- ① 切り分け作業の内容  
(例 1) A・B サーバーから C サーバーに対して ping コマンドを実行  
(例 2) 送信元・宛先サーバーでパケットキャプチャを実行、etc
- ② 切り分け作業の結果  
(例 1) A サーバーから C サーバーに対しての ping は応答あり、B サーバーから C サーバーに対しての ping は応答なし  
(例 2) 送信元サーバーからパケットを送信していることが確認できたが、宛先サーバーにパケットが届いていない。

## 5. 実施していただきたい切り分けの例

下記図では、通信元サーバーと宛先サーバー、及び切り分けていただきたいポイントを示しています。



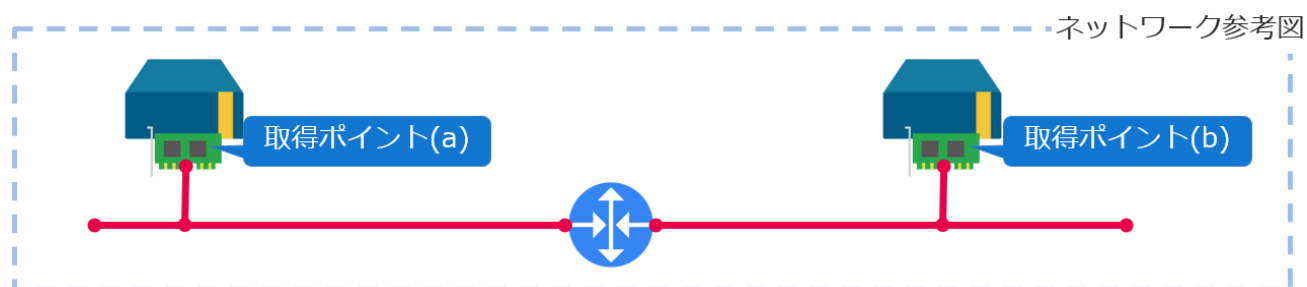
上記図の1～10番で実施いただきたい切り分けの具体的なコマンド例と、その目的を下記表に示します。

項番	目的	通信元機器	宛先機器	確認方法
1	ファイアウォールの設定確認	通信元サーバー	-	Web GUI で IN/OUT を確認
2	ファイアウォールの設定確認	-	宛先サーバー	Web GUI で IN/OUT を確認
3	終端装置間での通信経路の確認	通信元サーバー	宛先サーバー	Ping
4	終端装置間での通信経路の確認	宛先サーバー	通信元サーバー	ping
5	ルーティングの確認	通信元サーバー	宛先サーバー	tracert/route -I/n
6	NIC 接続の確認	通信元サーバー	通信元サーバーと 同一 L2 の別サーバー	ping
7	通信経路の確認	通信元サーバー	直近のルーター (利用している場合)	ping
8	宛先側の NIC 接続確認	宛先サーバーと 同一 L2 の別サーバー	宛先サーバー	ping
9	宛先側のポート開放確認	宛先サーバーと 同一 L2 の別サーバー	宛先サーバー	telnet host port_no
10	ポート開放の確認	通信元サーバー	宛先サーバー	telnet host port_no

## 6. パケットキャプチャの取得場所

下記図にて取得ポイントを示していますが、パケットキャプチャを取得するには、必ず送信元・宛先サーバーでの取得、解析をお願い致します。

- ✓ 取得ポイント(a):送信元サーバー
- ✓ 取得ポイント(b):宛先サーバー



- ※ 時間は同期されている状況で取得、解析をお願い致します
- ※ 双方で、取得タイミングは合わせてください
- ※ 取得時に発生するサーバー負荷にはご注意ください

## 7. 参考情報

OS 毎にパケットキャプチャの参考手順を以下に記載します。情報採取時にご利用ください。

ツールについては導入済みであることを前提としています。

※Windows は OS 標準ツールでの方法をご紹介します。

### [ パケットキャプチャ(Linux の例) ]

#### ■ tcpdump の場合

```
# tcpdump -i [インターフェース名] -w [ファイル名]
```

※ 取得対象のインターフェースは事象が発生しているインターフェースをご指定ください

※ ファイルの保存先は、十分な空き容量があるパスをご指定ください

※ 取得パケットサイズはデフォルトで問題ありません（必要なのはヘッダ情報のため）

※ フィルタ条件は不要となります

### [ パケットキャプチャ(Windows の例) ]

#### ■ netsh trace の場合

```
# netsh trace show interfaces
```

イーサネット アダプター EthernetX:

説明: vmxnet3 Ethernet Adapter

インターフェイス GUID: {UUID}

インターフェイス インデックス: X

インターフェイス LUID: 0x0000000000000000

```
# netsh trace start capture=yes CaptureInterface={インターフェイス GUID} ¥  
traceFile=[保存パス]
```

```
# netsh trace stop
```

※ 取得対象のインタフェースは事象が発生しているインターフェースをご指定ください

※ ファイルの保存先は、十分な空き容量があるパスをご指定ください

※ フィルタ条件はインターフェース以外不要となります

#### ■ pktmon の場合

```
# pktmon list
```

ネットワーク アダプター:

ID	MAC アドレス	名前
----	----------	----

--	-----	--
----	-------	----

[ID]	XX-XX-XX-XX-XX-XX	vmxnet3 Ethernet Adapter
------	-------------------	--------------------------

```
# pktmon start --capture --comp [ID] -f [保存パス]
```

```
# pktmon stop
```

※ 取得対象のインタフェースは事象が発生しているインターフェースをご指定ください

※ ファイルの保存先は、十分な空き容量があるパスをご指定ください

※ フィルタ条件はインターフェース以外不要となります

## 8. 改訂履歴

版数	日付	変更内容
1.0	2022/12/08	初版