

Dynamic Enterprise AI Solution

<AIRead White Paper> AIRead WinRM 使用手順書

2024年2月
(AWP-003-11)



AIとローコード開発を活用し
世の中をより良い世界に

1. はじめに
2. 前提条件
3. 設定手順
4. 注意点

- 本書はAIReadを「WinRM」で実行させるための利用手順書を記載した文書です。
- 「WinRM」とは、Windows Server の Windows PowerShell を遠隔から操作する機能です
Windowsサーバのコマンドラインを外部から呼び出し、WindowsサーバにインストールされたAIReadの起動を行うことができます。
- 本機能はオンプレミス・サーバ版のAIReadでのみ利用が可能です。
- AIReadは、Ver. 4.0.0 以降のバージョンが前提となります。

■ サーバ

- Windows Server 2012 以降
- PowerShell バージョン2 以降
- Windows リモート管理 (WinRM) を有効
※Active Directoryでグループポリシーを構成している場合、対象サーバのWinRMを有効

■ クライアント

- Windows 10 以降
- 「Administrators」 又は 「Remote Management Users」 グループに所属するOSユーザ

■ ネットワーク

- サーバマシンは以下のポートをリッスン
 - WinRM(HTTPで構成(デフォルト))の場合 : 5985
 - WinRM(HTTPSで構成)の場合 : 5986※リッスンポートは変更可能
- サーバのリッスンポートに対して、クライアントからTCPで通信可能
 - WinRMのリッスンポートへの通信を受信できるよう、サーバのWindowsファイアウォールを構成
- クライアントとサーバが別セグメントの場合、通信経路中のファイアウォールに通信許可できること

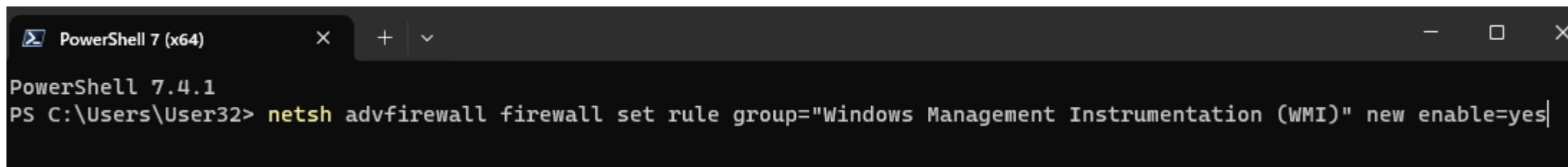
3. 設定手順(サーバ作業)

Confidential

- ファイアウォールでグループ化

WindowsPowerShellを起動し下記コマンドを実行します。

```
netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
```



```
PowerShell 7 (x64)
PowerShell 7.4.1
PS C:\Users\User32> netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes|
```

- ポートの開放

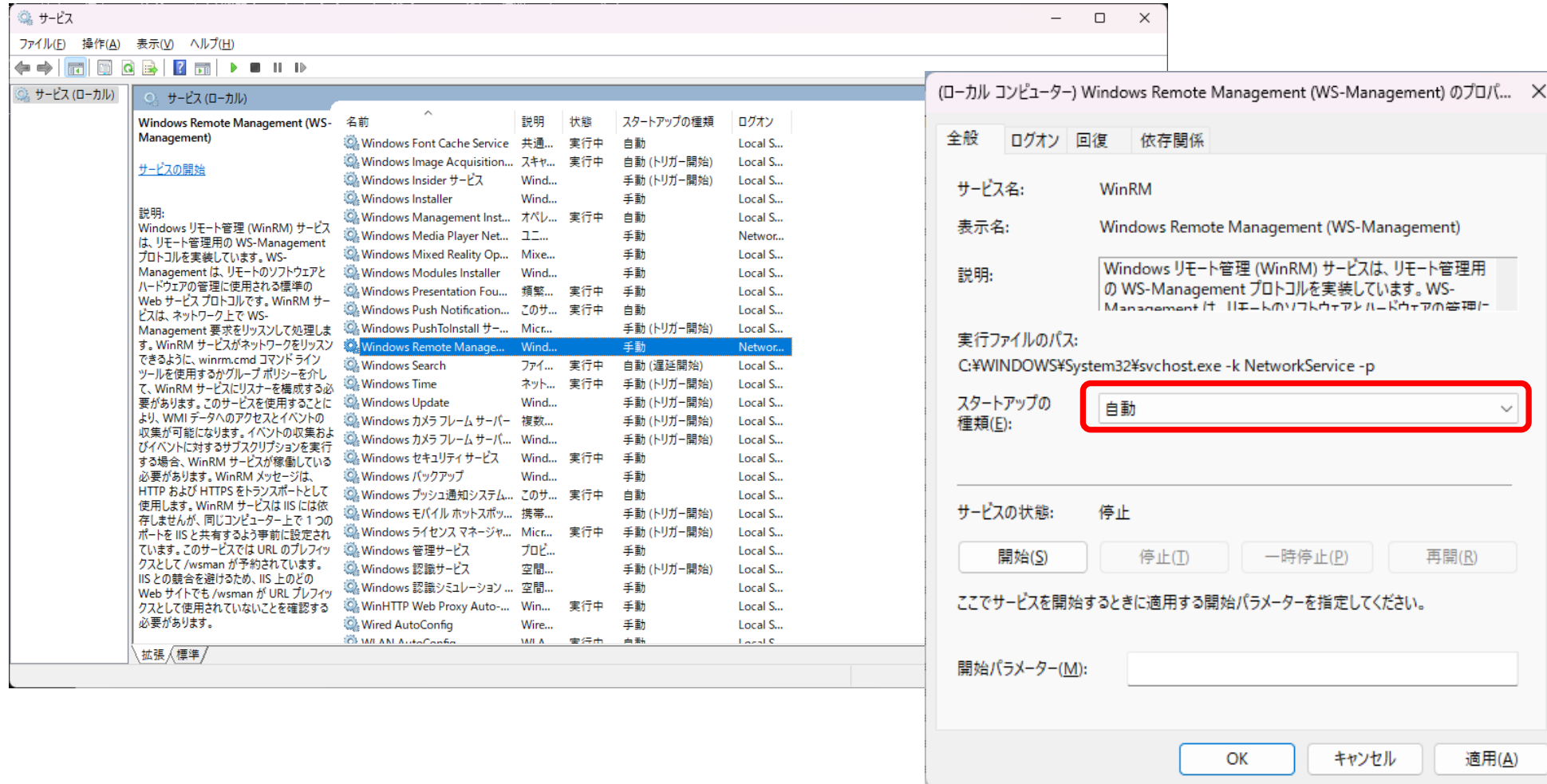
5985ポートを開放します(クライアントPCからの限定接続用)

「3. 設定手順(ポート開放):P11」 参照

3. 設定手順(サーバ作業)

■ サービス : WinRMの設定

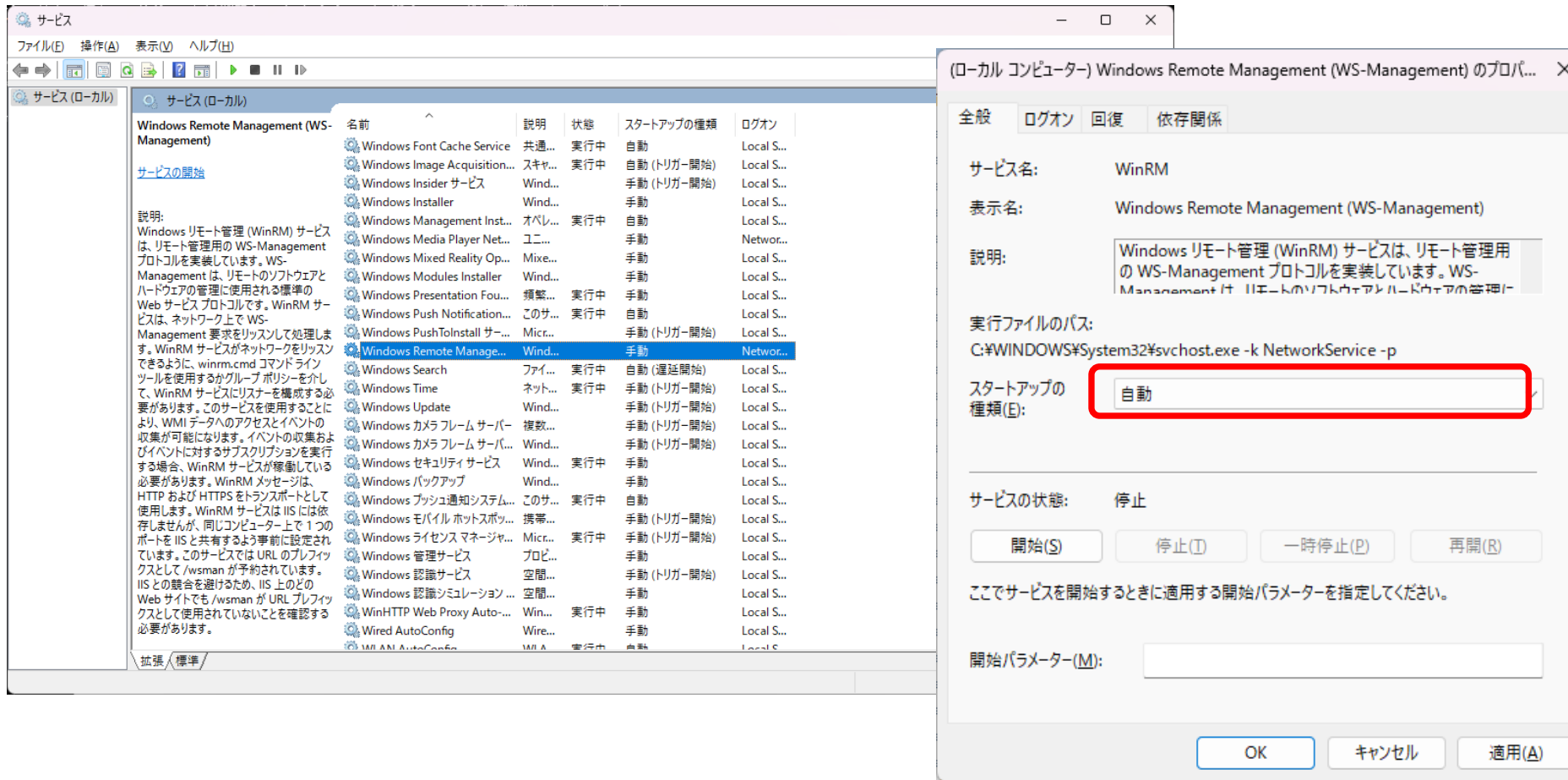
Windows Remote Management(WinRM) を自動起動で設定します。



3. 設定手順(クライアント作業)

■ サービス : WinRMの設定

Windows Remote Management(WinRM) を自動起動で設定します。



3. 設定手順(クライアント作業)

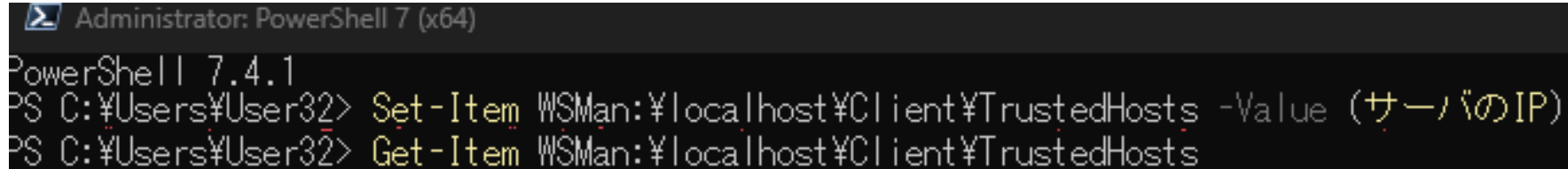
- TrustedHostsを追加

powershellを管理者権限で起動し、下記コマンドを実行します。

<https://docs.microsoft.com/ja-jp/powershell/scripting/learn/remoting/winrmsecurity?view=powershell-7.2>

Set-Item WSMan:¥localhost¥Client¥TrustedHosts -Value (サーバのIP)

Get-Item WSMan:¥localhost¥Client¥TrustedHosts



```
Administrator: PowerShell 7 (x64)
PowerShell 7.4.1
PS C:¥Users¥User32> Set-Item WSMan:¥localhost¥Client¥TrustedHosts -Value (サーバのIP)
PS C:¥Users¥User32> Get-Item WSMan:¥localhost¥Client¥TrustedHosts
```

3. 設定手順(batファイル:クライアントで作成)

- bat、powershellの作成

リモート実行を行うためにbatファイルとpowershellの実行ファイルを作成します。

※batファイルからpowershellのファイルを実行

batファイルの記載内容：例

ファイル名:AIRead.bat

```
rem @echo off

rem 管理者権限付与
cd /d %~dp0
for /f "tokens=3 delims=% " %%i in ('whoami /groups^|find "Mandatory"') do set LEVEL=%%i
if NOT "%LEVEL%"=="High" (
powershell.exe -NoProfile -ExecutionPolicy RemoteSigned -Command "Start-Process %~f0 -Verb runas"
exit
)

rem powershellのファイルを置いている場所に移動する
cd C:¥Users¥ユーザ名¥Desktop

rem セキュリティ解除
powershell set-ExecutionPolicy Unrestricted
rem psファイルの実行:実行するpsファイルを指定
powershell "psファイルの格納フォルダ:フルパス指定/psファイル名"
rem セキュリティ再設定
powershell set-ExecutionPolicy Restricted
```

3. 設定手順(psファイル：クライアントで作成)

- bat、powershellの作成

powerShellファイルの記載内容：例

ファイル名:AIRead_server.ps1

```
$scriptPath = Split-Path -Parent $MyInvocation.MyCommand.Path  
cd $scriptPath
```

```
$ID="サーバユーザ名"  
$PlainPassword="パスワード"  
$AIReadIP="サーバIPアドレス"
```

```
$SecurePassword = ConvertTo-SecureString -String $PlainPassword -AsPlainText -Force  
$Credential = New-Object System.Management.Automation.PSCredential($ID, $SecurePassword)
```

```
Invoke-Command -ComputerName $AIReadIP -Credential $Credential {CMD /C "サーバのAIRead処理実行ファイルのパス¥実行ファイル名"}
```

AIReadの処理起動についてはShortcutCreatorで作成したarexファイルの指定でも可
{CMD /C ・ ・ }で指定するパスはサーバ側の実行ファイルの格納場所を指定

3. 設定手順(ポート開放)

■ 5985ポートを開放

5985ポートは通常閉じているため、開放する必要があります。

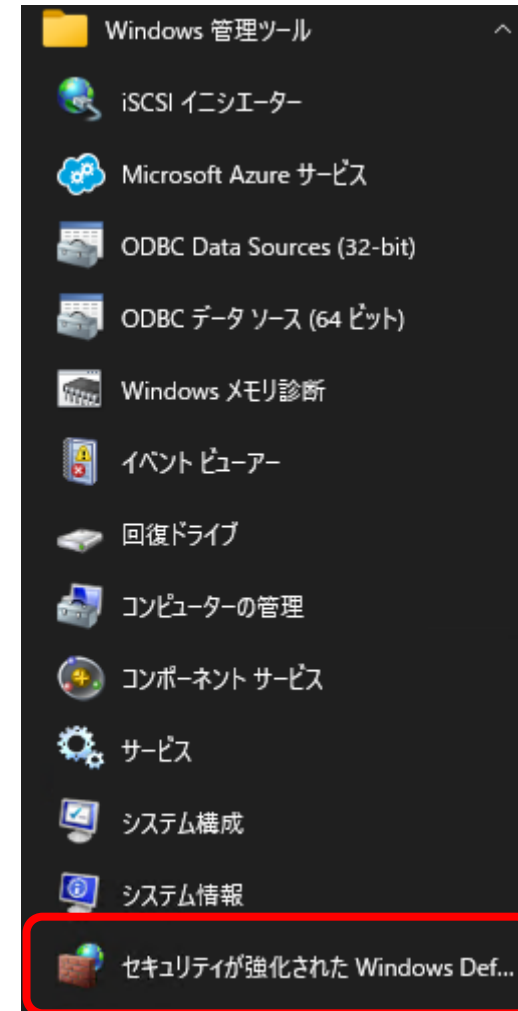
開放する手順は下記の通りです。

1. セキュリティが強化された

Windows Defender ファイアウォールを開く

Windowsメニュー→Windows管理ツール

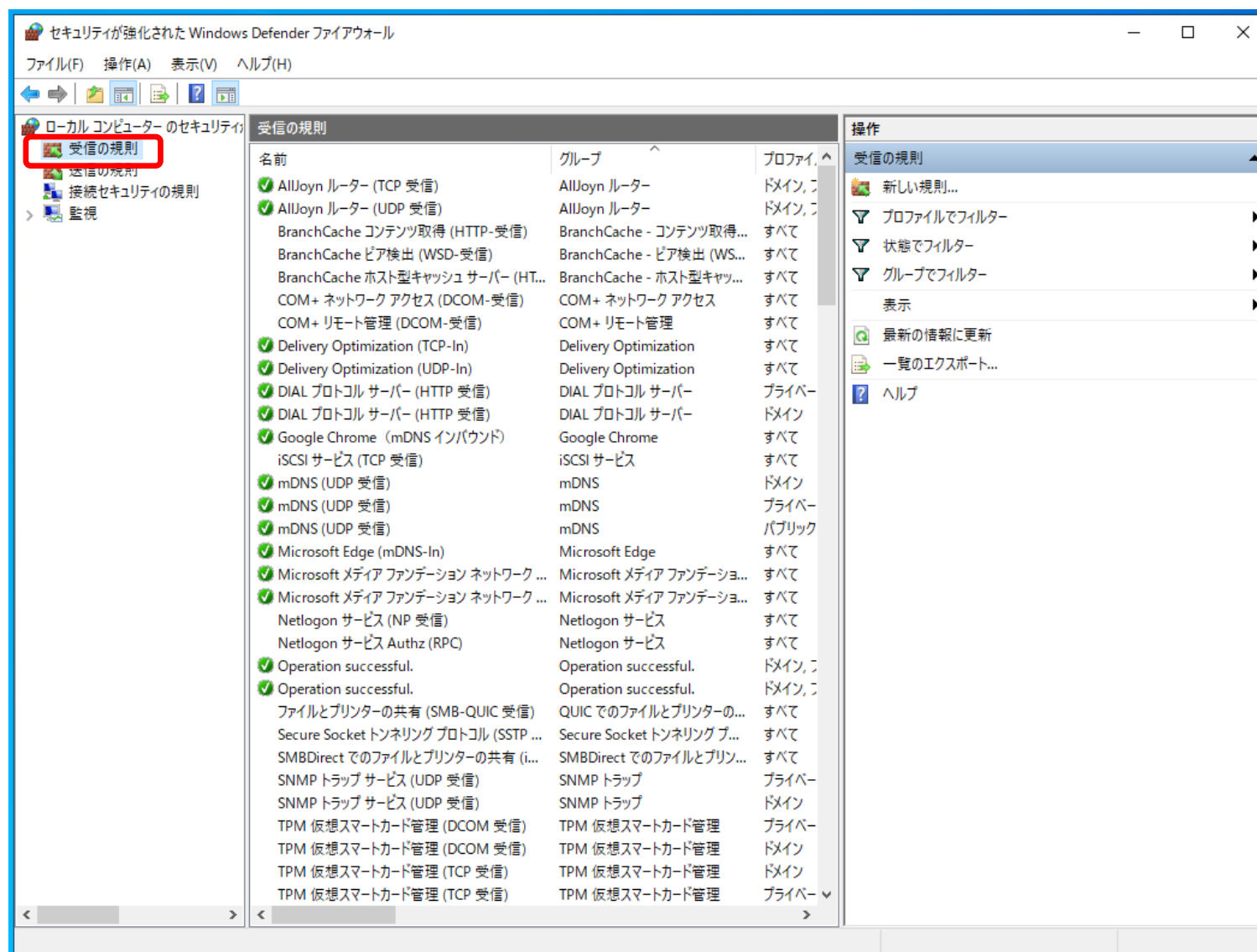
→セキュリティが強化されたWindows Defender ファイアウォールを開く



3. 設定手順(ポート開放)

Confidential

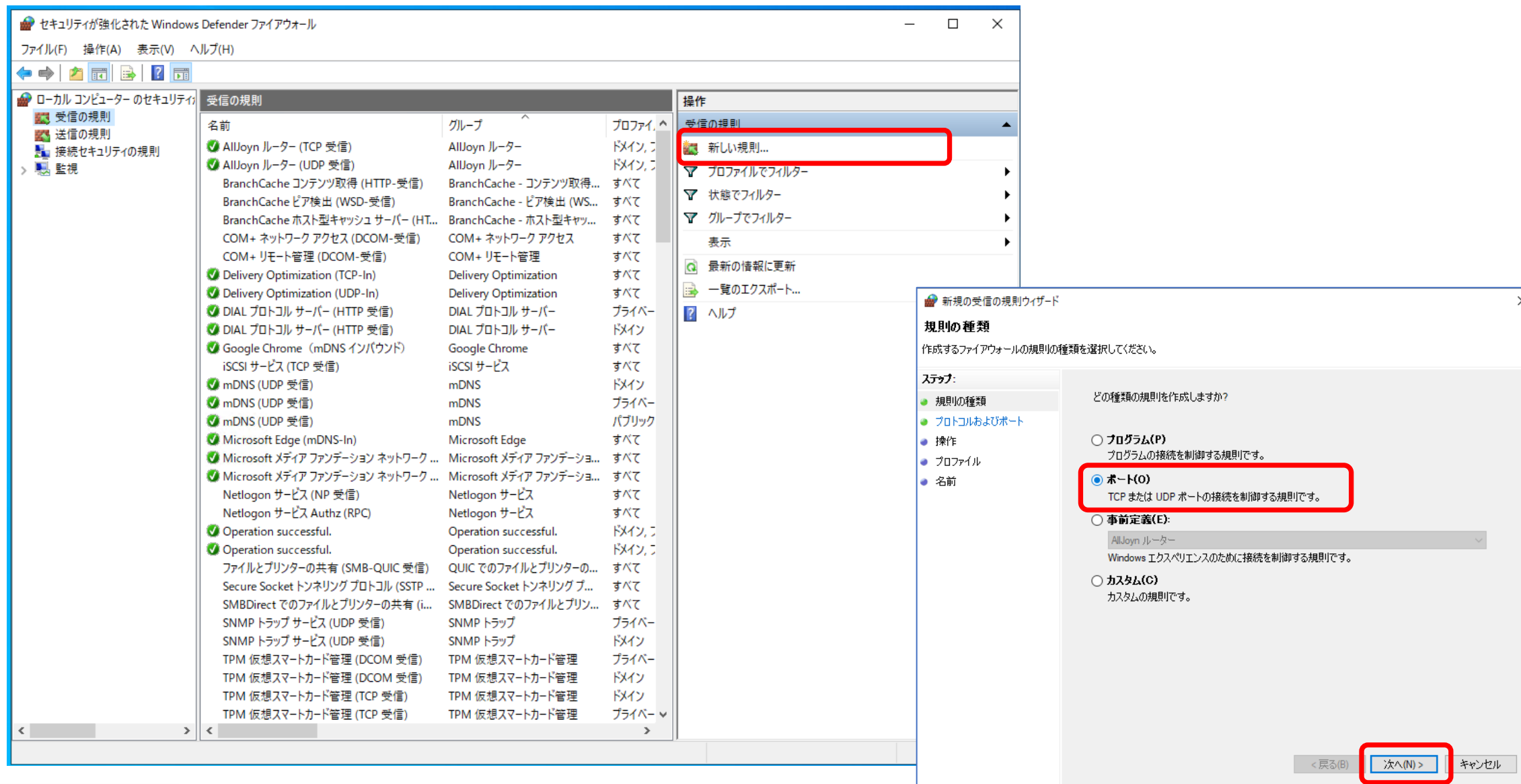
2. 受信の規制 > 「新しい規制」をクリックする



3. 設定手順(ポート開放)

Confidential

3. 新規の受信の規制ウィザードが開き、ポートを選択して「次へ」ボタンをクリックする



3. 設定手順(ポート開放)

Confidential

4. TCPプロトコル、特定のローカルポートに通信を許可したいポート番号(5985)を入力して
「次へ」ボタンをクリックする

新規の受信の規則ウィザード

プロトコルおよびポート

この規則を適用するプロトコルとポートを指定してください。

ステップ:

- 規則の種類
- プロトコルおよびポート
- 操作
- プロファイル
- 名前

TCP と UDP のどちらにこの規則を適用しますか?

☒ TCP(T)

☐ UDP(U)

すべてのローカルポートと特定のローカルポートのどちらを対象にこの規則を適用するかを選択してください。

☐ すべてのローカルポート(A)

☒ 特定のローカルポート(S):

例: 80, 443, 5000-5010

< 戻る(B) 次へ(N) > キャンセル

3. 設定手順(ポート開放)

Confidential

5. 「接続を許可する」を選択して次へボタンをクリックする

新規の受信の規則ウィザード

操作

規則で指定された条件を接続が満たす場合に、実行される操作を指定します。

ステップ:

- 規則の種類
- プロトコルおよびポート
- 操作
- プロファイル
- 名前

接続が指定の条件に一致した場合に、どの操作を実行しますか？

☒ **接続を許可する(A)**
IPsec を使用して保護された接続と保護されていない接続の両方を含みます。

☐ **セキュリティで保護されている場合のみ接続を許可する(C)**
IPsec を使用して認証された接続のみを含みます。接続は、IPsec プロパティ内の設定と接続セキュリティ規則ノード内の規則を使用して、セキュリティ保護されます。

☐ **接続をブロックする(K)**

< 戻る(B) **次へ(N) >** キャンセル

3. 設定手順(ポート開放)

Confidential

6. ドメイン、プライベートにチェックして「次へ」ボタンをクリックする

新規の受信の規則ウィザード

プロフィール

この規則が適用されるプロフィールを指定してください。

ステップ:

- 規則の種類
- プロトコルおよびポート
- 操作
- プロフィール
- 名前

この規則はいつ適用しますか?

- ☒ **ドメイン(D)**
コンピューターがその企業ドメインに接続しているときに適用されます。
- ☒ **プライベート(P)**
コンピューターが自宅や職場などのプライベート ネットワークに接続しているときに適用されます。
- ☐ **パブリック(U)**
コンピューターがパブリック ネットワークに接続しているときに適用されます。

< 戻る(B) **次へ(N) >** キャンセル

3. 設定手順(ポート開放)

Confidential

7. 名称、説明を任意で入力して「完了」ボタンをクリックする

新規の受信の規則ウィザード

名前

この規則の名前と説明を指定してください。

ステップ:

- 規則の種類
- プロトコルおよびポート
- 操作
- プロファイル
- 名前

名前(N):

AIRead_5985

説明 (オプション)(D):

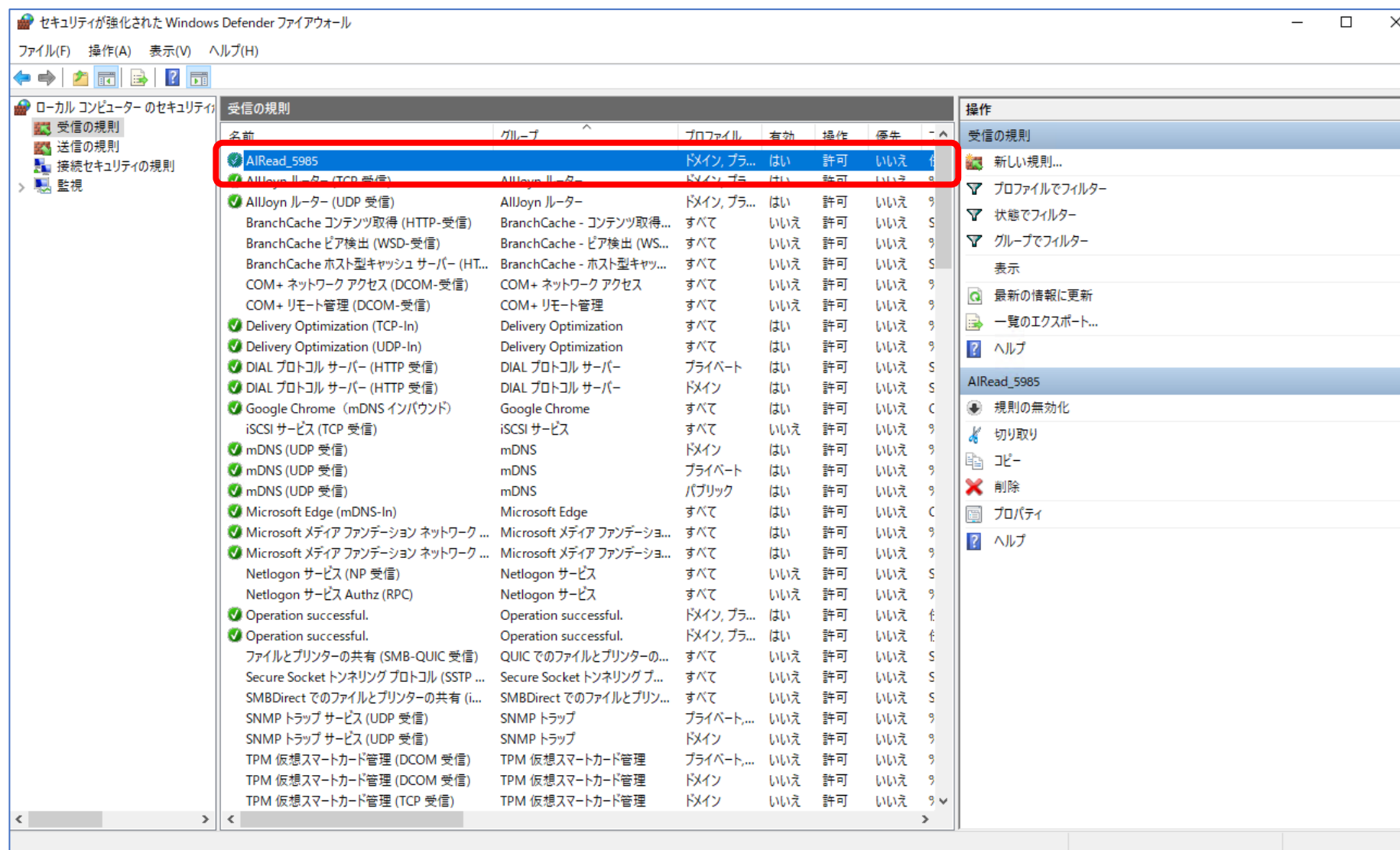
AIRead接続用ポート

< 戻る(B) 完了(F) キャンセル

3. 設定手順(ポート開放)

Confidential

8. ポートが追加され、設定完了です。



3. 設定手順(疎通確認)

- 5985ポートの疎通確認の実施

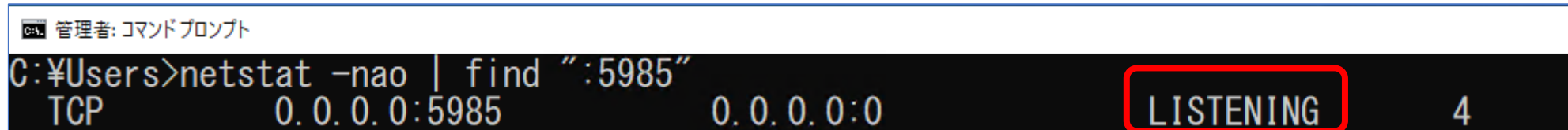
クライアントPCよりサーバの5985ポートへ疎通できるか確認を行います。

※疎通できなかった場合はポートが解放されていないのでサーバの5985ポートを開放する。

- ポート開放確認方法(サーバ)

コマンドプロンプトより下記コマンド実行します。

`netstat -nao | find ":5985"`



```
管理: コマンドプロンプト
C:\Users>netstat -nao | find ":5985"
TCP        0.0.0.0:5985      0.0.0.0:0      LISTENING      4
```

上記の様に表示され、LISTENINGになっていればOK。

3. 設定手順(疎通確認)

■ 疎通確認方法(クライアント)

MicrosoftのサイトよりPSToolを入手。解凍し、Cドライブ直下に配置します。

コマンドプロンプトより、PSToolのフォルダに移動し下記コマンド実行します。

C:¥PSTools>C:¥PSTools¥psping.exe サーバのIPアドレス:5985

```
C:\> 選択管理者: コマンド プロンプト
C:\>¥>cd PSTools
C:\PSTools>psping.exe サーバIPアドレス :5985
```

ポートへ接続できると下記のようなメッセージが返ってきます。

```
PsPing v2.12 - PsPing - ping, latency, bandwidth measurement utility
Copyright (C) 2012-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

TCP connect to サーバIPアドレス :5985:
5 iterations (warmup 1) ping test:
Connecting to サーバIPアドレス :5985 (warmup): from ローカルIPアドレス :63207: 8.20ms
Connecting to サーバIPアドレス :5985: from ローカルIPアドレス :63208: 8.44ms
Connecting to サーバIPアドレス :5985: from ローカルIPアドレス :63209: 8.45ms
```

※ポートが開放されていない場合「ネットワーク接続拒否」等メッセージが表示されます。

■ AIRead(サーバ)読取実行での注意点

下記フォルダ名に全角文字を使用しない。

半角英数でフォルダ名を設定します。

inputフォルダ ←読み取り実行するファイルを格納するフォルダ

outputフォルダ ←出力結果を格納するフォルダ

全角文字を使用したフォルダ名を設定した場合、読取実行すると

下記のようなメッセージが出力されます。

Not found image file or directory Please check input.



アライズイノベーション株式会社

東京都中央区勝どき3-13-1

Mail : airead_support@ariseinnovation.co.jp

AIRead Official : <https://airead.ai/>

AIRead Support : <https://support.airead.ai/>

AIRead Manual : <https://manual.airead.ai/>