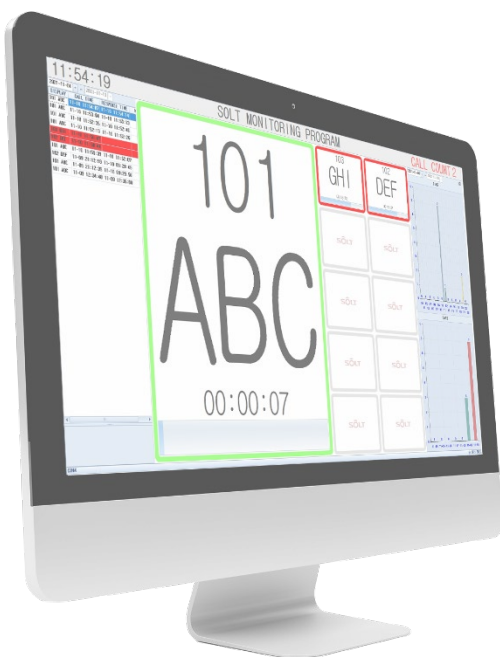




SOLTモニタリングプログラム Multi View ユーザーマニュアル

V2_2024.10.10



SOLT-JAPAN
株式会社メデタヤ・ネットワーク



概要

マルチビュー機能を使用すると、MPR(T)デバイスが接続されているコンピューターで行われた通信を、複数の異なるコンピューターとリアルタイムで共有することで監視できます。

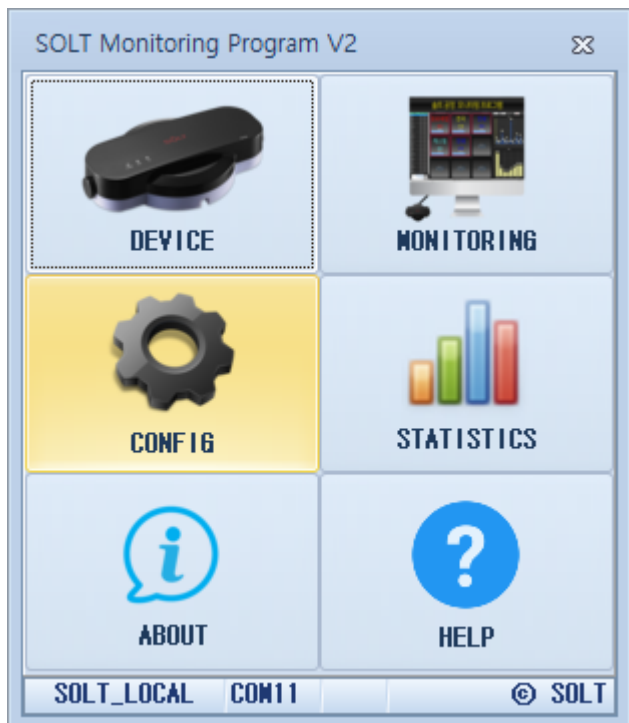
同じネットワーク上のコンピューターからプライベート IP で接続する方法

外部ネットワークからパブリック IP に接続する方法があります。

設定方法

一. プライベート IP で接続する

1.1 MPR が接続されているコンピューターにインストールされているプログラムを実行し、**CONFIG** 設定を入力します。



1.2 Etc タブに入り、スクロールして MULTI VIEW セクションの MY PRIVATE IP を確認します。

例)192.168.0.2

注意: MPR(T) デバイスが接続されているコンピュータ上のデータベース サーバ IP のデフォルト値は 127.0.0.1 である必要があります。

Config

Appearance01 Appearance02 **Etc** Account

DEALING TIME : 30 SECONDS

CANCEL TIME : 3 SECONDS

NEW CALL : TOP BOTTOM

WARNING SOUND : ON OFF

CALL SOUND REPEAT : 1

CHIP GROUP : ON OFF

CONFIRM PASSWORD : *

LANGUAGE : [icon]

DATA BACKUP INTERVAL : 1440 MINUTES (0, >=60)

BACKUP PATH : C:\Solt\SOLT Monitoring Program Y2 [icon]

START WITH WINDOW

REMINO CALL(SR5-MPRT)

BELL MANAGER : VISIBLE

REMINO CALL TIME : 40 SECONDS

MAP MONITORING

MAP VIEW : YES NO

MAP ALARM X : WIDTH 3 HEIGHT 3

API

REST POST URL : [input]

Branch(KeepUnique) : SOLT (Max:20)

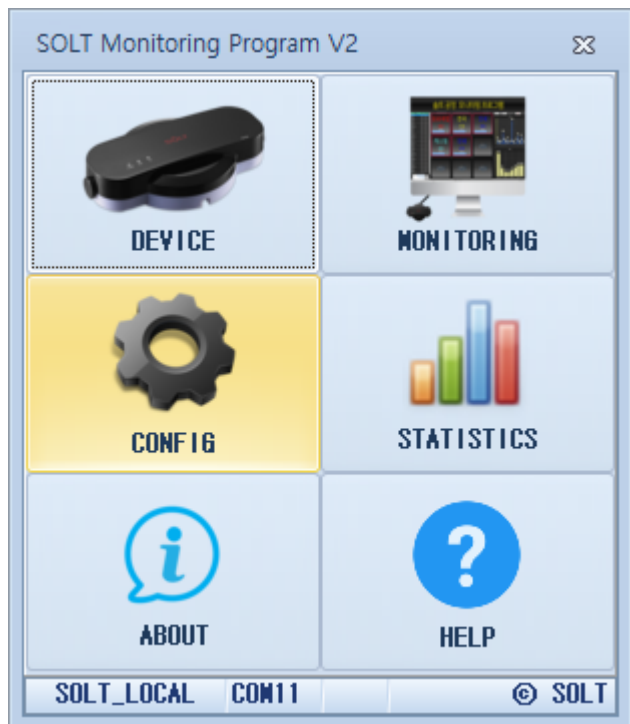
MULTI VIEW

MY PUBLIC IP : 1.237.235.83

MY PRIVATE IP : 192.168.0.2

DATABASE SERVER IP : 127.0.0.1

1.3 **Multi View** 機能を使用するコンピューターにインストールされているプログラムを実行し、**CONFIG** 設定画面を開きます。



1.4 [ETC]タブに入り、スクロールして[MULTI VIEW]項目の[DATABASE SERVER

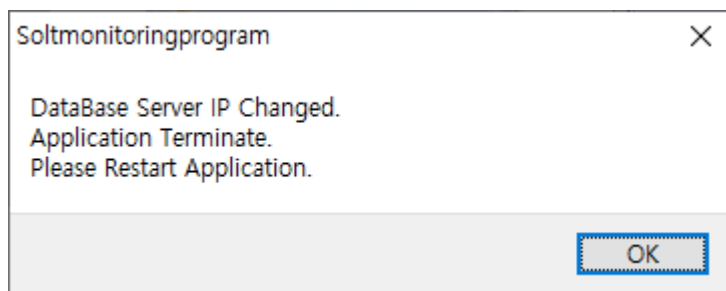
IP]フィールドに入力します。

「PRIVATE IP 例) 192.168.0.2」と入力して Enter キーを押すと、プログラムは終了し、プログラムを再起動するように求められます。

プログラムを再起動すると、MPR は接続されたコンピューターで行われた通信をリアルタイムで共有および監視できるようになります

The screenshot shows the 'Config' window with the following settings:

- Appearance01** | **Appearance02** | **Etc** | **Account**
- DEALING TIME: 30 SECONDS
- CANCEL TIME: 3 SECONDS
- NEW CALL: TOP BOTTOM
- WARNING SOUND: ON OFF
- CALL SOUND REPEAT: 1
- CHIP GROUP: ON OFF
- CONFIRM PASSWORD: *
- LANGUAGE: [Icon]
- DATA BACKUP INTERVAL: 1440 MINUTES (0, >=60)
- BACKUP PATH: C:\Solt\SOLT Monitoring Program Y2
- START WITH WINDOW
- REMINO CALL(SR5-MPRT)**
- BELL MANAGER: VISIBLE
- REMINO CALL TIME: 40 SECONDS
- MAP MONITORING**
- MAP VIEW: YES NO
- MAP ALARM X: WIDTH 3 HEIGHT 3
- API**
- REST POST URL: [Empty]
- Branch(KeepUnique): SOLT (Max:20)
- MULTI VIEW**
- MY PUBLIC IP: 1.237.235.83
- MY PRIVATE IP: [Empty]
- DATABASE SERVER IP: 192.168.0.2**



※エラーが出る場合は次ページからのファイアウォールの設定を行ってください。

1.5 ファイアウォールのポート 3050 での受信接続を許可する

1.5.1 ファイアウォールの設定画面から「詳細設定」をクリック。

Windows Defender ファイアウォール

← → ↓ ↑ > コントロール パネル > すべてのコントロール パネル項目 > Windows Defender ファイアウォール

コントロール パネル ホーム

Windows Defender ファイアウォールを介したアプリまたは機能を許可

- 通知設定の変更
- Windows Defender ファイアウォールの有効化または無効化
- 既定値に戻す
- 詳細設定**
- ネットワークのトラブルシューティング

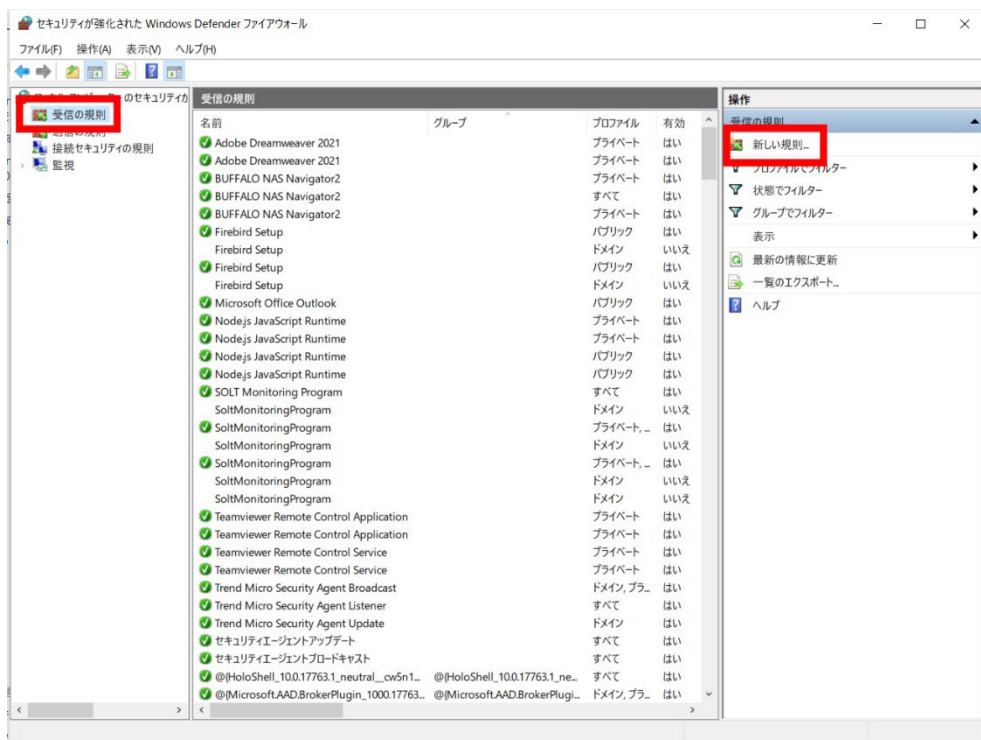
Windows Defender ファイアウォールによる PC の保護

Windows Defender ファイアウォールによって、ハッカーまたは悪意のあるソフトウェアによるインターネットまたはネットワークを経由したアクセスを防止できるようになります。

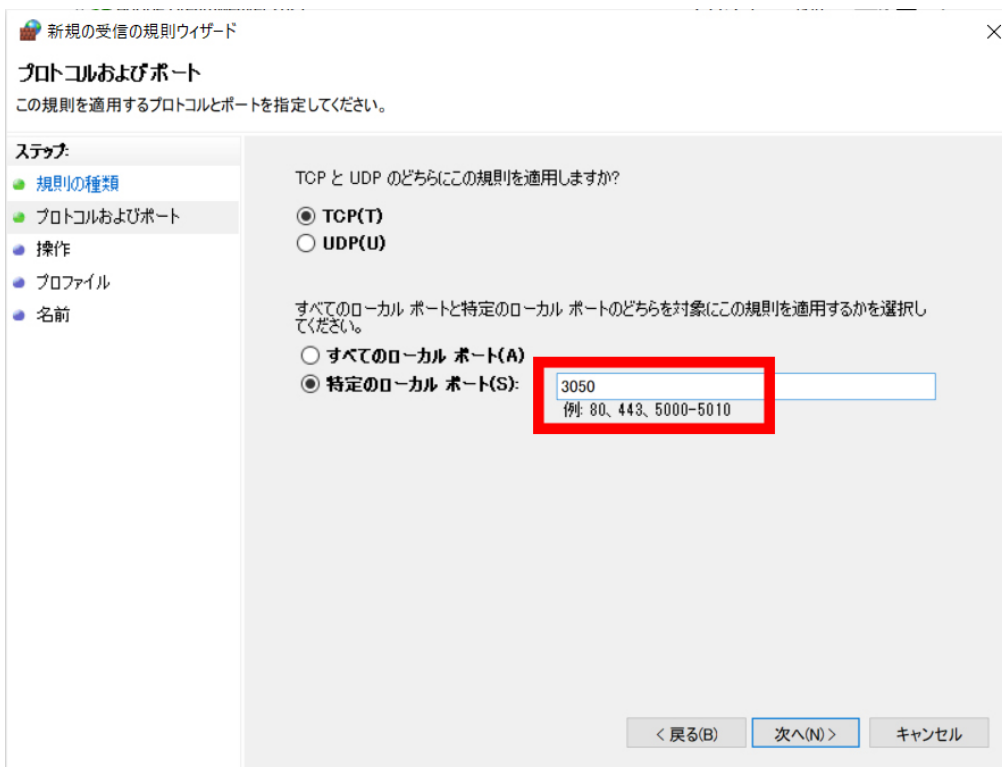
🟢 プライベート ネットワーク(R) 接続済み	
ネットワーク上のユーザーとデバイスを認識および信頼している、ホームまたは社内ネットワーク	
Windows Defender ファイアウォールの状態:	有効
着信接続:	許可されたアプリの一覧にないアプリへのすべての接続をブロックする
アクティブなプライベート ネットワーク:	
通知の状態:	Windows Defender ファイアウォールが新しいアプリをブロックしたときに通知を受け取る

🟢 ゲストまたはパブリック ネットワーク(P) 接続されていません	
--	--

1.5.2 左部分の「受信の規則」をクリックし、右の「新しい規則」をクリック。



1.5.3 以下のように、ファイアウォールの受信ルールにポート 3050 を追加します。



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。

カスタマイズ(Z)...

接続をブロックする(K)

< 戻る(B) **次へ(N) >** キャンセル

新規の受信の規則ウィザード

プロファイル

この規則が適用されるプロファイ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
- プロファイル
- 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

名前(オプション)指定後の仕上げ

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):
Solt Monitoring Program

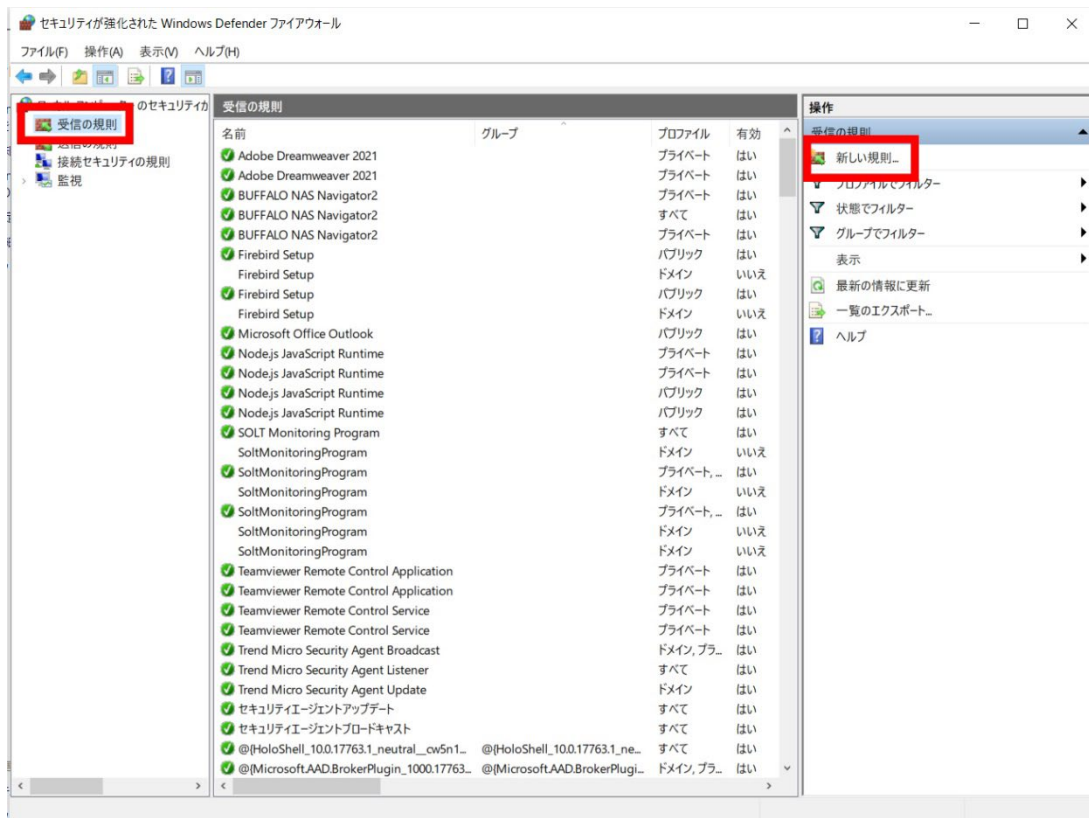
説明(オプション)(D):

< 戻る(B) **完了(F)** キャンセル

1.6 ファイアウォールの FireBird での受信接続を許可する

1.6.1 同じ手順で FireBird プログラムの受信規則を設定します。

Windows Defender ファイアウォール



プログラムを選択して次へ

新規の受信の規則ウィザード

×

規則の種類

作成するファイアウォールの規則の種類を選択してください。

ステップ:

- 規則の種類
- プログラム
- 操作
- プロファイル
- 名前

どの種類の規則を作成しますか?

プログラム(P)
プログラムの接続を制御する規則です。

ポート(O)
TCP または UDP ポートの接続を制御する規則です。

事前定義(E):
@FirewallAPI.dll-80200
Windows エクスプレィエンスのために接続を制御する規則です。

カスタム(C)
カスタムの規則です。

< 戻る(B) 次へ(N) > キャンセル

「このプログラムのパス」で「%ProgramFiles%(x86)%Firebird\Firebird_2_5\bin\Fbserver.exe」を参照

新規の受信の規則ウィザード

×

プログラム

この規則が一致するプログラムの完全なプログラムのパスと実行可能ファイル名を指定してください。

ステップ:

- 規則の種類
- プログラム
- 操作
- プロファイル
- 名前

すべてのプログラムと特定のプログラムのどちらにこの規則を適用しますか?

すべてのプログラム(A)
他の規則のプロパティに一致する、コンピューター上のすべての接続に規則を適用します。

このプログラムのパス(T):
%ProgramFiles%(x86)%Firebird\Firebird_2_5\bin\Fbserver.exe 参照(R) ...
例: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

< 戻る(B) 次へ(N) > キャンセル



名前を付けて完了

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):
Solt Monitoring Program

説明(オプション)(O):

< 戻る(B) **完了(F)** キャンセル

ポートフォワーディング

例)ipTime ルーター

2.1.1 ルーターの管理ページにログインします。



2.1.2 管理ツールに入ります。



2.1.3 NAT/Portforward 設定を入力します。

The screenshot shows the web interface for ipTIME A604SE. On the left, the '메뉴탐색기' (Menu Search) sidebar has '고급 설정' (Advanced Settings) expanded, and 'NAT/라우터 관리' (NAT/Router Management) is selected, with '포트포워드 설정' (Port Forward Setting) highlighted in red. The main content area is titled '포트포워드 설정' (Port Forward Setting) and shows a table for user-defined rules. The table has columns: '순위' (Priority), '사용자 규칙' (User Rule), '내부 IP' (Internal IP), '외부 포트' (External Port), and '내부 포트' (Internal Port). A '+ 새규칙 추가' (Add New Rule) button is at the top left of the table. Below the table, there are input fields for:

- 규칙이름 (Rule Name): []
- 내부 IP주소 (Internal IP Address): 192.168.0. []
- 프로토콜 (Protocol): TCP
- 외부 포트 (External Port): [] ~ []
- 내부 포트 (Internal Port): [] ~ []

 At the bottom, there are buttons for 'PC<-규칙저장' (Save Rule to PC), 'PC->규칙복원' (Restore Rule from PC), '파일 선택' (File Select), and '선택된 파일 없음' (No file selected). On the right side, there are buttons for '순위' (Priority), '순위높임' (Increase Priority), '순위낮춤' (Decrease Priority), '새규칙' (New Rule), '적용' (Apply), and '취소' (Cancel).

2.1.4 룰명(ランダム)을 지정し、送信 IP アドレスを 2.2 で識別した PRIVATE IP に設定します。

外部ポートと内部ポートの両方を 3050 (Firebird データベース エンジン サービス ポート) として指定し、適用します。



The screenshot shows the '포트포워드 설정' (Port Forwarding Settings) page in the ipTIME A604SE web interface. The left sidebar contains a navigation menu with categories like '기본 설정' (Basic Settings), '고급 설정' (Advanced Settings), and '보안 기능' (Security Features). The main content area displays a table of port forwarding rules. A red box highlights the first rule, which is selected. Below the table, there are configuration fields for the selected rule, including rule name, internal IP, protocol, and ports. At the bottom, there are buttons for saving, restoring, and deleting rules.

순위	사용자 규칙	내부 IP	외부 포트	내부 포트	삭제
1	solt monitoring...	192.168.0.2	TCP(3050~3050)	TCP(3050~3050)	<input type="checkbox"/>

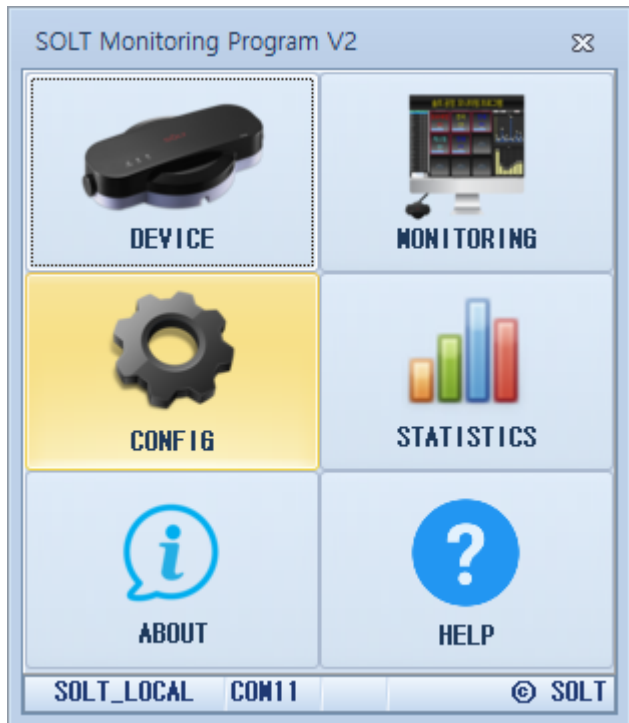
Configuration fields for the selected rule:

- 규칙이름: solt monitoring program
- 내부 IP 주소: 192.168.0.2
- 프로토콜: TCP
- 외부 포트: 3050 ~ 3050
- 내부 포트: 3050 ~ 3050

設定方法

二. パブリック IP との接続

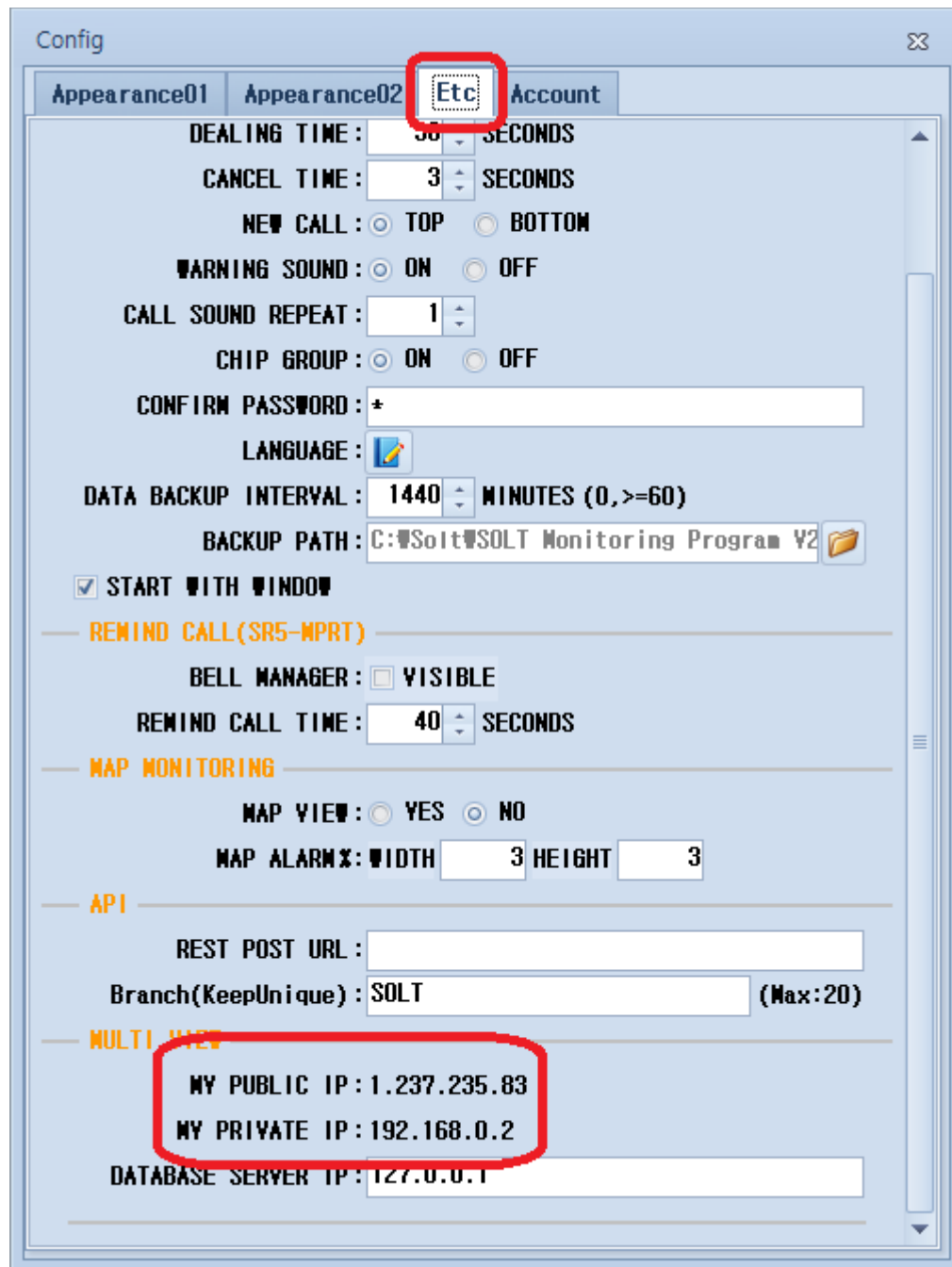
2.2 MPR が接続されているコンピューターにインストールされているプログラムを実行し、**CONFIG** 設定を入力します。



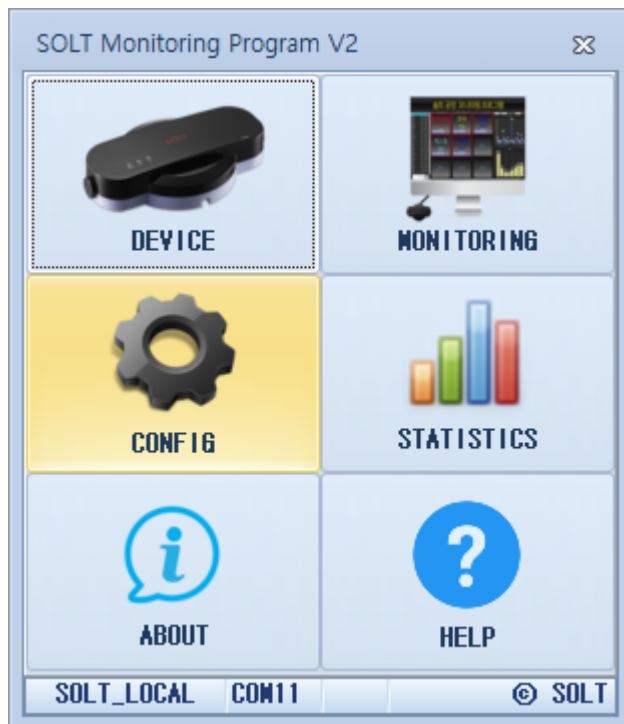
2.3 ETC タブに入り、スクロールして MULTI VIEW セクションの MY PUBLIC IP と MY PRIVATE IP の内容を確認します。

例) 1.237.235.83 と 192.168.0.2

注意: MPR(T) デバイスが接続されているコンピュータ上のデータベース サーバ IP のデフォルト値は 127.0.0.1 である必要があります。



2.4 **Multi View** 機能を使用するコンピューターにインストールされている監視プログラムを実行し、**CONFIG** 設定を入力します。



2.4 [ETC]タブに入り、スクロールして[MULTI VIEW]項目の[DATABASE SERVER

IP]フィールドに入力します。

PUBLIC IP Ex) を 2.2 1.27.235.83 で識別し、Enter キーを押すと、プログラムを終了し、プログラムを再実行するように求められます。

プログラムを再起動すると、MPR は接続されたコンピューターで行われた通信をリアルタイムで共有および監視できるようになります

The screenshot shows the 'Config' window with the following settings:

- Appearance01 | Appearance02 | **Etc** | Account
- DEALING TIME: 30 SECONDS
- CANCEL TIME: 3 SECONDS
- NEW CALL: TOP BOTTOM
- WARNING SOUND: ON OFF
- CALL SOUND REPEAT: 1
- CHIP GROUP: ON OFF
- CONFIRM PASSWORD: *
- LANGUAGE: [Icon]
- DATA BACKUP INTERVAL: 1440 MINUTES (0, >=60)
- BACKUP PATH: C:\Solt\SOLT Monitoring Program Y2
- START WITH WINDOW
- REMINO CALL(SR5-MPRT)
- BELL MANAGER: VISIBLE
- REMINO CALL TIME: 40 SECONDS
- MAP MONITORING
- MAP VIEW: YES NO
- MAP ALARM X: WIDTH 3 HEIGHT 3
- API
- REST POST URL: [Empty]
- Branch(KeepUnique): SOLT (Max:20)
- MULTI VIEW
- MY PUBLIC IP: [Empty]
- MY PRIVATE IP: 192.168.0.2
- DATABASE SERVER IP: 1.237.235.83**

