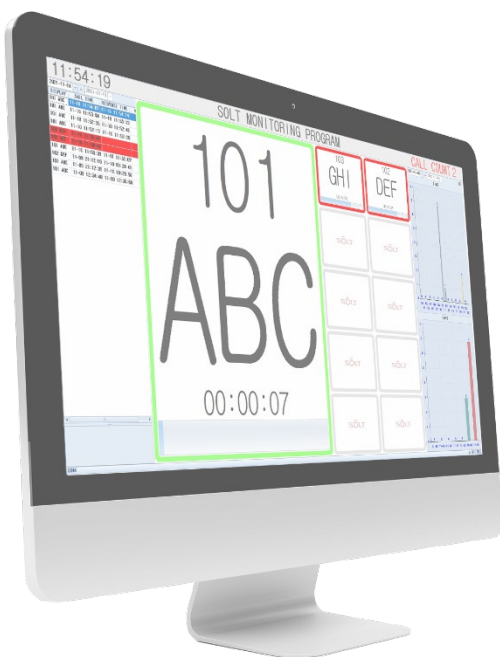




SOLTモニタリングプログラム Multi View ユーザーマニュアル

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。

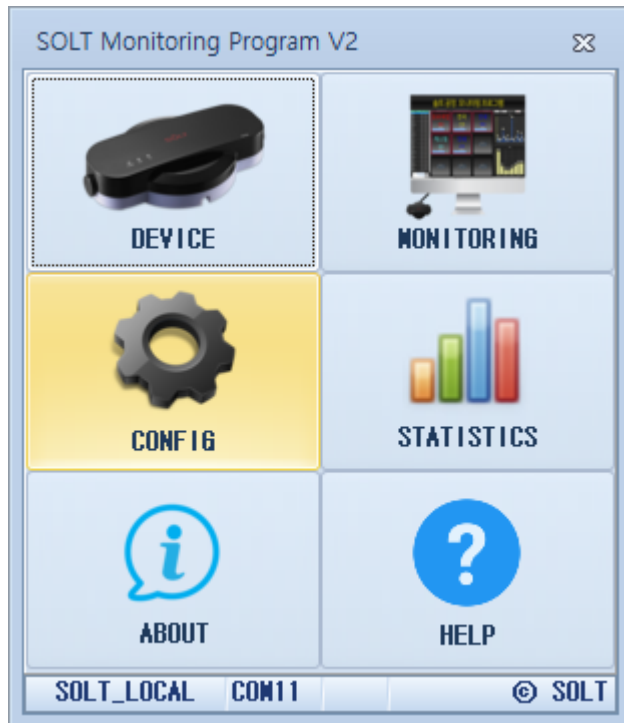
同じネットワーク上のコンピューターからプライベート IP で接続する方法

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

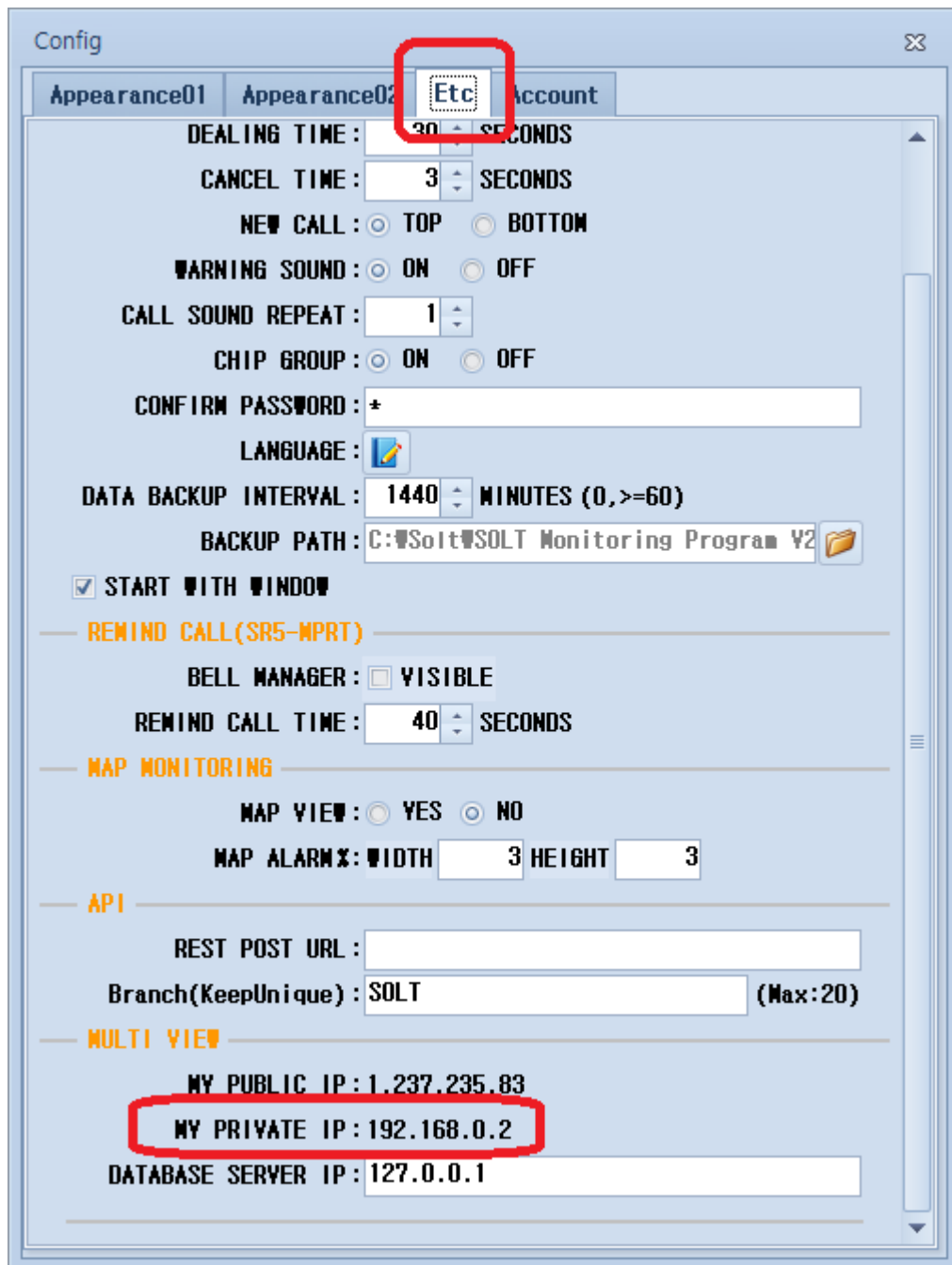
1.1 MPR が接続されているコンピューターにインストールされているプログラムを実行し、**CONFIG** 設定を入力します。



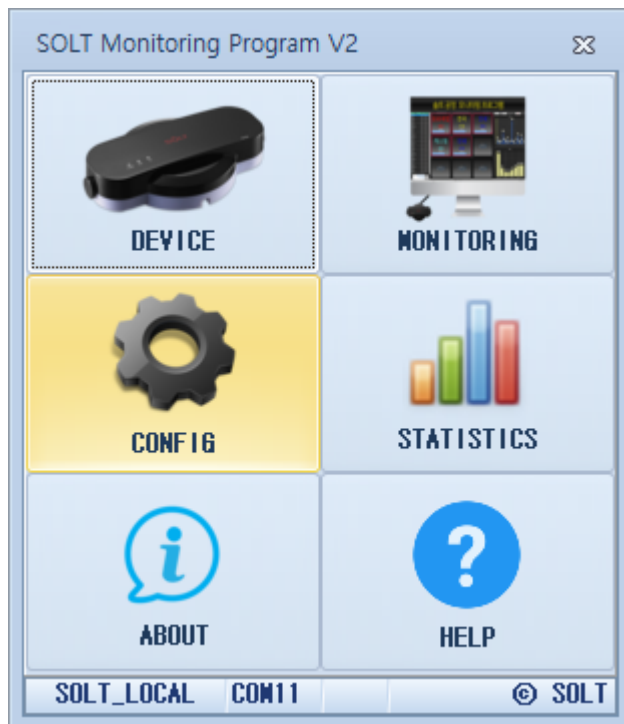
1.2 Etc タブに入り、スクロールして MULTI VIEW セクションの MY PRIVATE IP を確認します。

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。



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

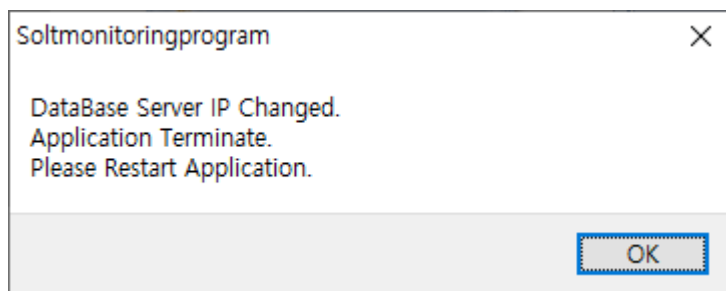
IP]フィールドに入力します。

「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: 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**



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

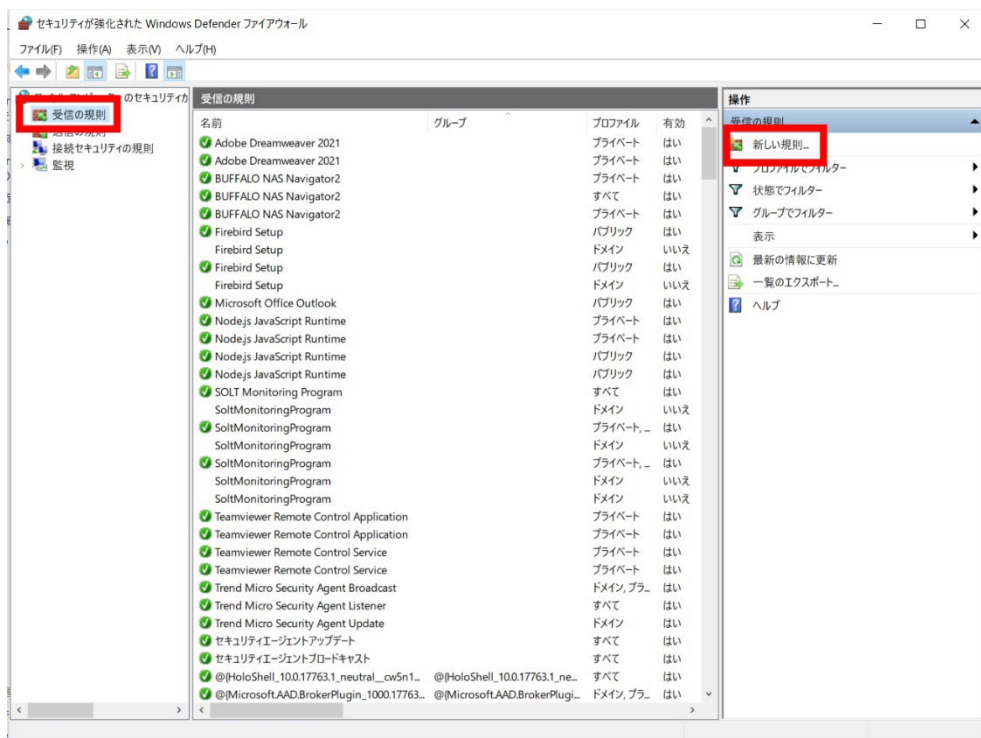
Windows Defender ファイアウォールによる PC の保護

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。

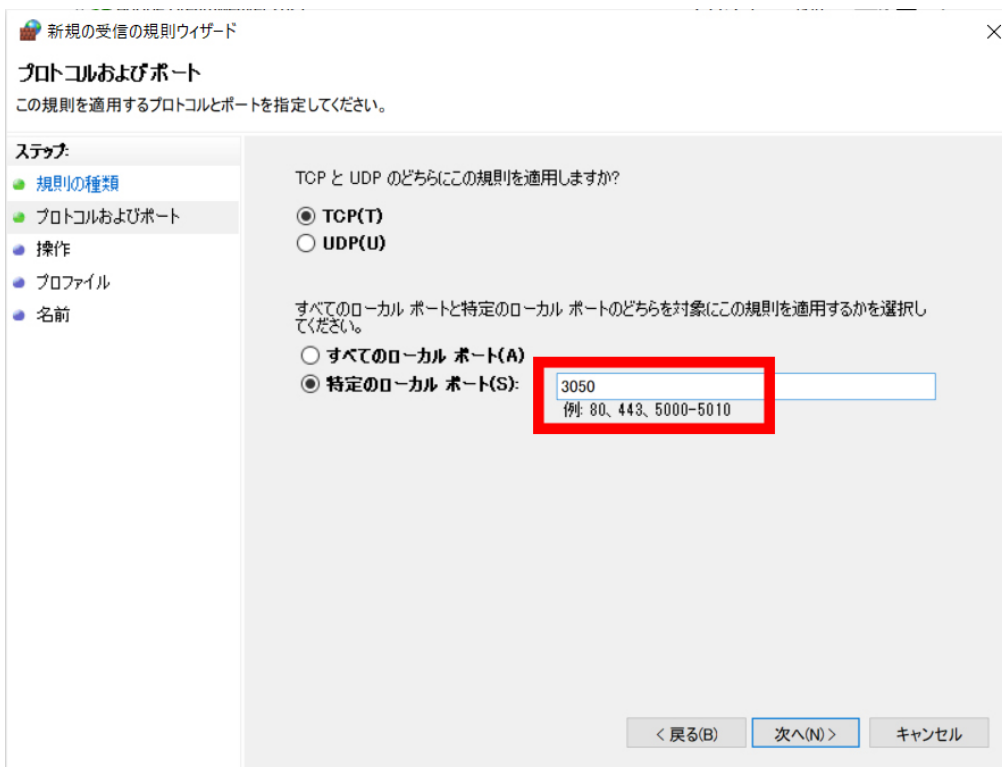
🟢 プライベート ネットワーク(R) 接続済み	
ネットワーク上のユーザーとデバイスを認識および信頼している、ホームまたは社内ネットワーク	
Windows Defender ファイアウォールの状態:	有効
着信接続:	許可されたアプリの一覧にないアプリへのすべての接続をブロックする
アクティブなプライベート ネットワーク:	
通知の状態:	Windows Defender ファイアウォールが新しいアプリをブロックしたときに通知を受け取る

🟢 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。





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

2.1 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。

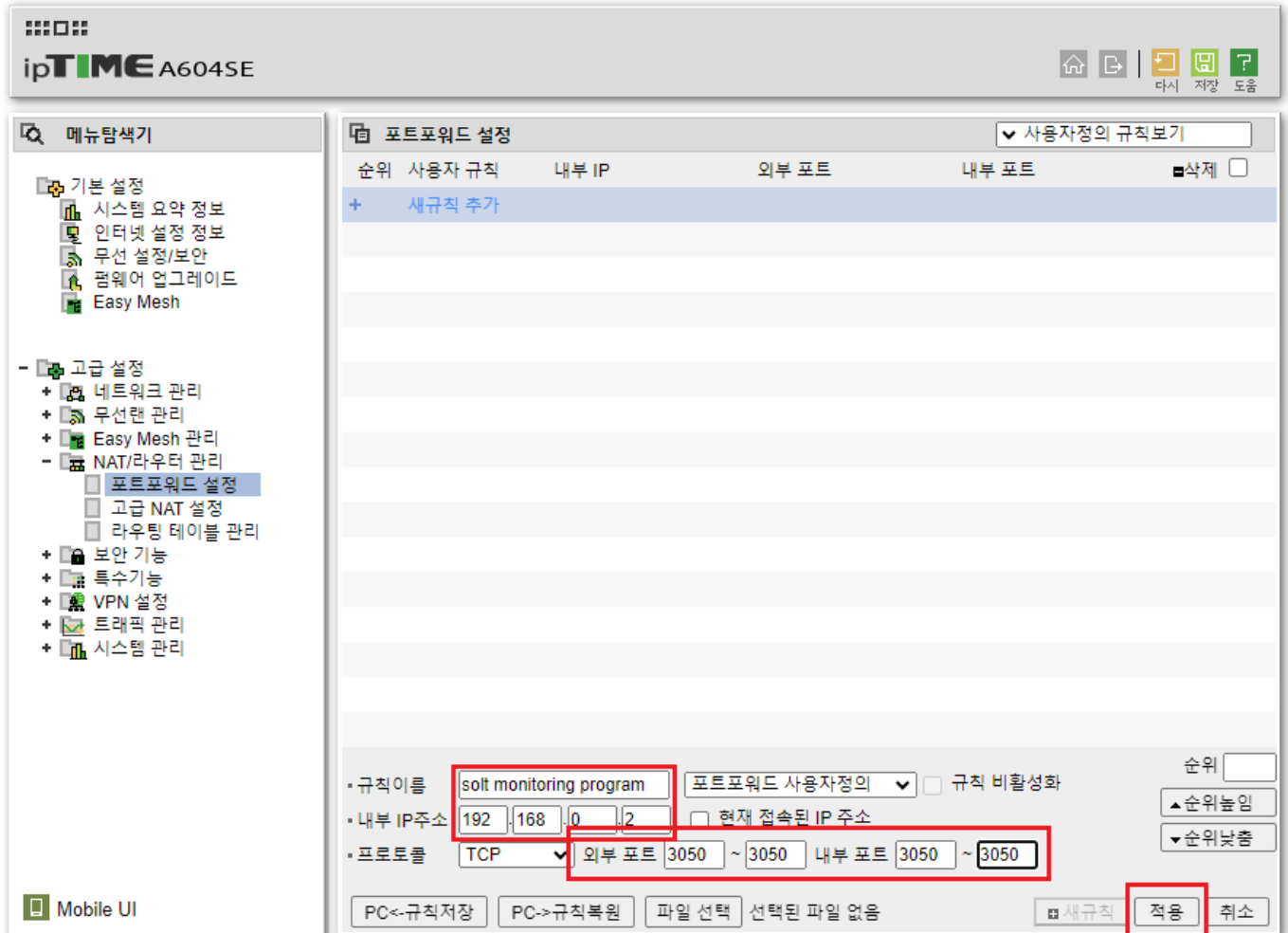


2.1.3 NAT/Portforward 設定を入力します。

The screenshot shows the web interface for ipTIME A604SE. On the left, the '메뉴탐색기' (Menu Search) sidebar has 'NAT/라우터 관리' expanded, with '포트포워드 설정' (Port Forward Setting) highlighted in red. The main content area is titled '포트포워드 설정' and features a table for managing port forwarding rules. The table has columns for '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 visible. Below the table, there are configuration fields: '규칙이름' (Rule Name), '포트포워드 사용자정의' (Port Forward User Defined) dropdown, '규칙 비활성화' (Disable Rule) checkbox, '내부 IP주소' (Internal IP Address) with input fields for 192, 168, 0, and '현재 접속된 IP 주소' (Current Connected IP Address) checkbox. The '프로토콜' (Protocol) is set to TCP, and there are fields for '외부 포트' (External Port) and '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), '선택된 파일 없음' (No file selected), '새규칙' (New Rule), '적용' (Apply), and '취소' (Cancel).

2.1.4 룰명(ランダム)을 지정し、送信 IP 地址を 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.

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"/>

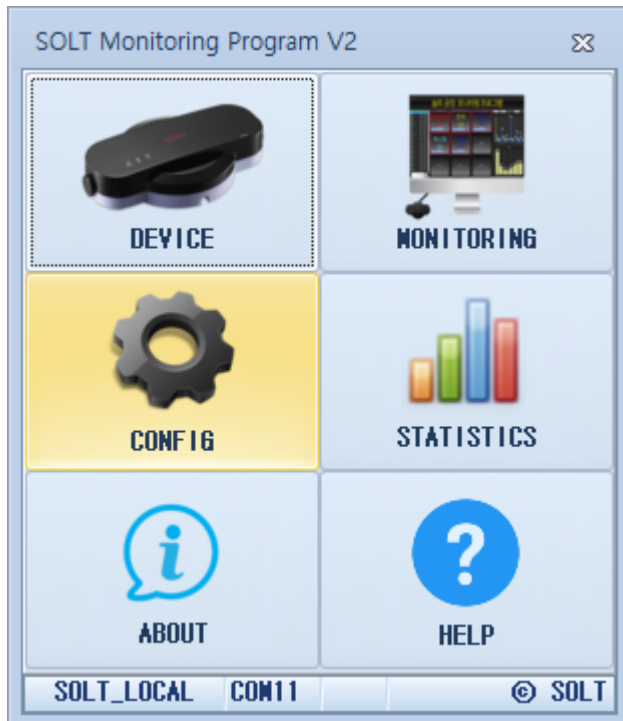
Configuration fields for the selected rule:

- 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

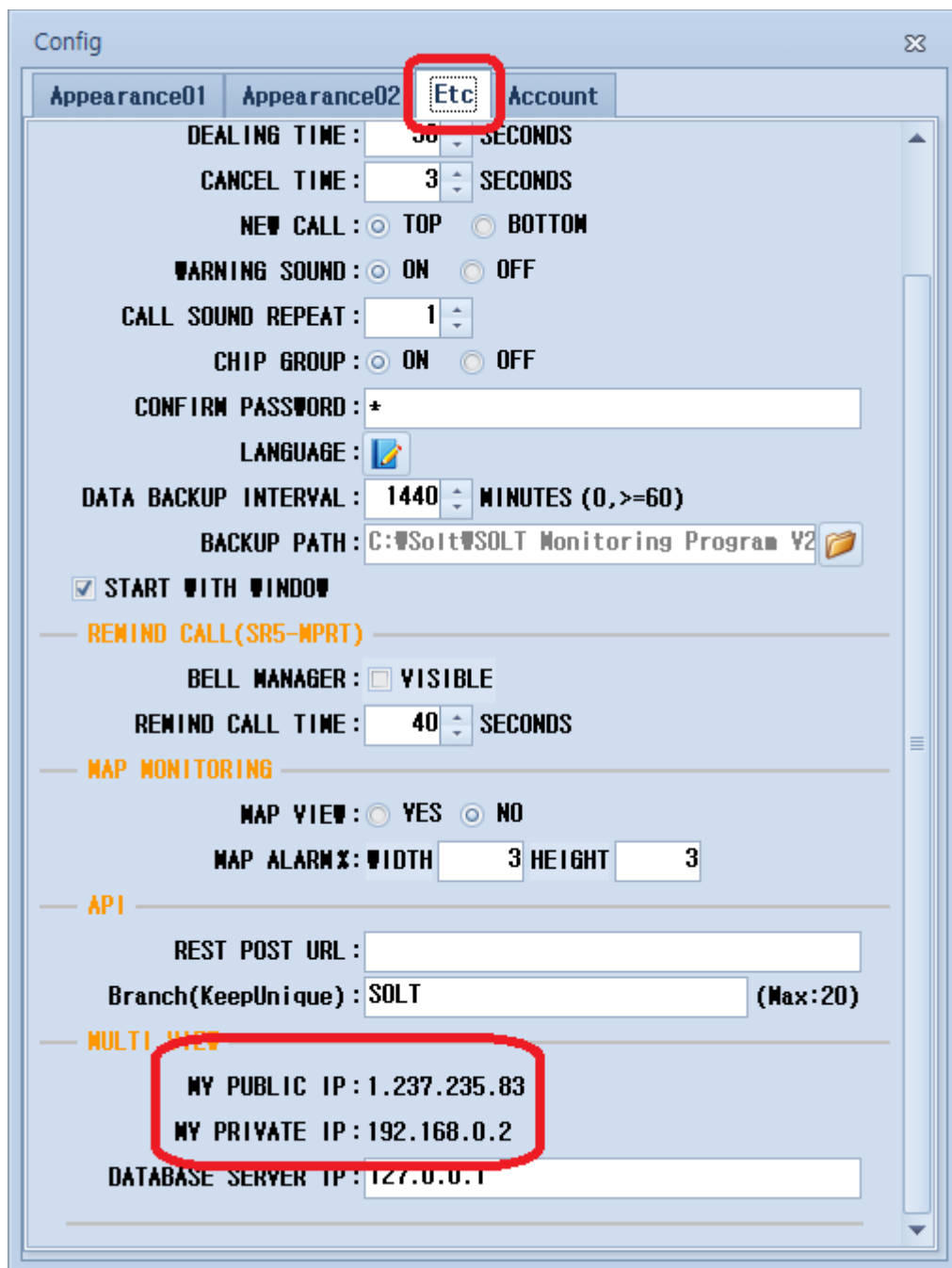
2.2 MPR が接続されているコンピューターにインストールされているプログラムを実行し、**CONFIG** 設定を入力します。



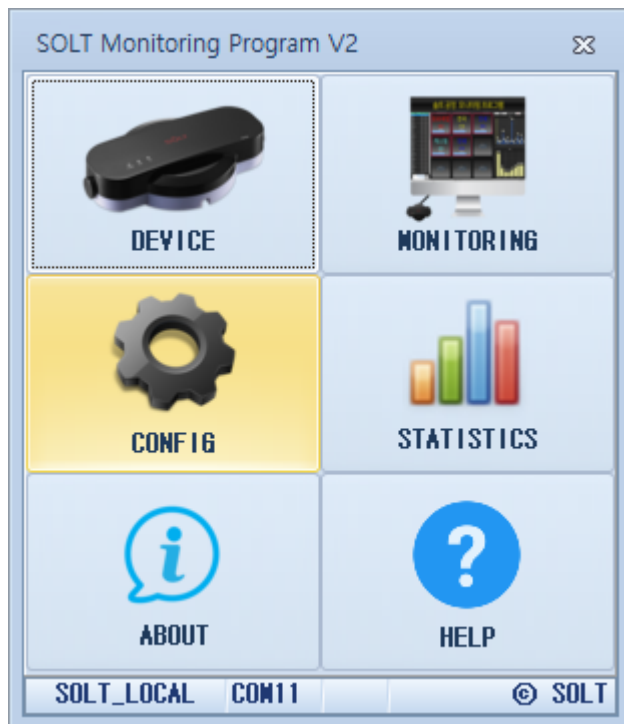
2.3 ETC タブに入り、スクロールして MULTI VIEW セクションの MY PUBLIC IP と MY PRIVATE IP の内容を確認します。

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: 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**

