PSB Computer Protection Windows でのファイヤーウォールコントロール-firewall

弊社 Computer Protection にはファイヤーウォールは搭載されておりませんが、Windows ファイヤーウォールをコントロールする機能が搭載されております。 当記事ではこの機能を利用して Windows ファイヤーウォールにルールを追加する手法を解説いたします。

当シナリオでは、「暗黙の Deny」(″許可条件に合致しない通信は全ブロック″)を Windows ファイヤーウォールに担当させ、PSB ポータルから許可ルールのみ登録する手法を採用しております。

［Windows ファイヤーウォールの特徴］

Windows ファイアウォールは、設定されたルールの順序を考慮せず、全てのルールをチェックします。通信に対して複数のルールが一致した場合、**拒否が優先**されます。その為、ルール最下部の「全ての通信を拒否」(暗黙の deny)がある場合、RDP 通信施行は失敗します。また、Windows ファイヤーウォールに既存の拒否ルールが存在している場合も RDP 通信施行は失敗します。当手順では、そういった Windows ファイヤーウォール既存ルールついて無効化を行います。

［既存 Window ファイヤーウォールルール無効化手順］

1.PSB ポータルにログインし、コントロールしたいデバイスに適用中の「プロフィール」を開きます。

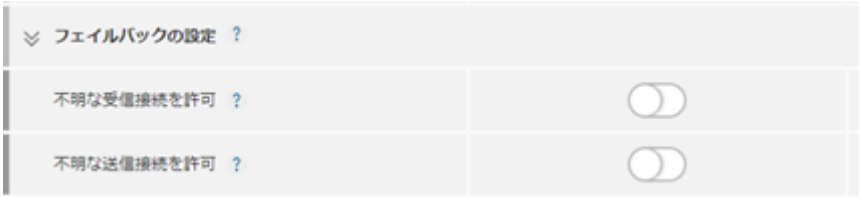
2.Windows ファイヤーウォールを Computer Protection でコントロールする設定にします。

- 「Windows ファイヤーウォールにプロフィールを追加」を有効
- 「F-Secure ファイアウォール プロフィールを追加」を有効

3.PSB ポータルファイヤーウォールプロフィールで許可されている通信以外は、拒否する設定にします。

・「不明な受信接続を許可」を無効

・「不明な送信接続を許可」を無効



4.既存 Windows ファイヤーウォールルールをすべて無効化する設定にします。

・「他のルールを許可する」を無効

※Active Directory/GPO や監査ソフト等で強制的に設定されているルールは無効化できません。

［PSB プロフィールへのファイヤーウォールルール追加手順］

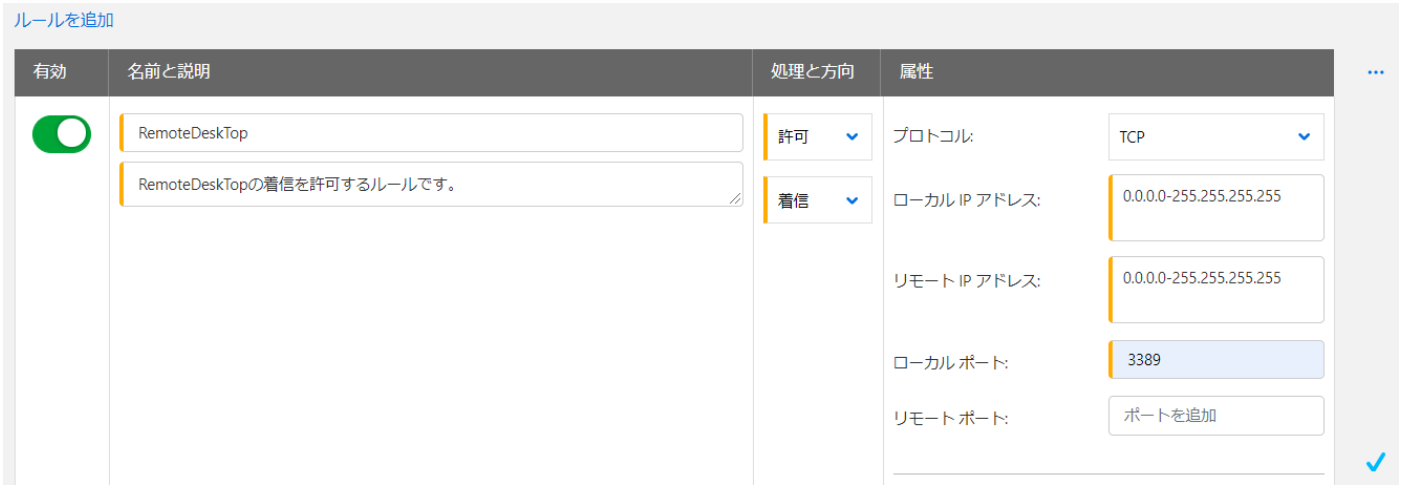
1.変更するプロフィールを選択します。

※ここでは Normal Workstaion を選択します。

2.「ルールを追加」からルールを追加します。

3.ルールに必要な項目を入力します。

※当記事では RemoteDesktop(TCP: 3389)許可ルールを追加します。



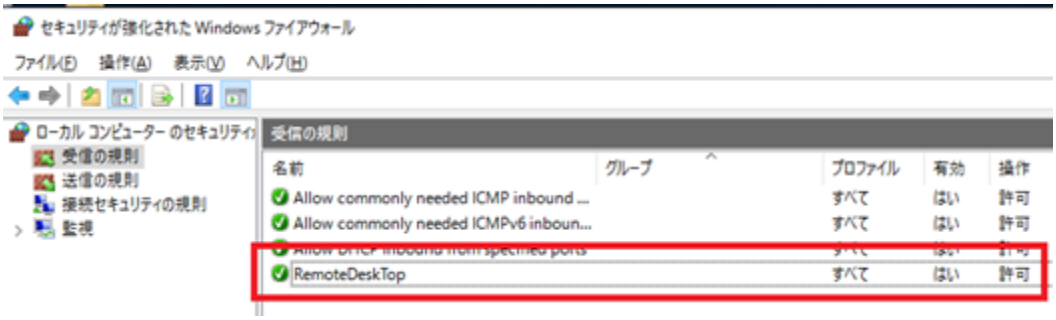
※**ルール追加** をクリックして必要な情報を入力します。

- プロフィールを追加　:プロフィール名を**入力します**
- **説明を追加**　:**説明を入力します**
- **処理**　:**許可**
- **方向**　:**着信**
- **プロトコル**　:TCP
- **ローカル IP アドレス**　: 0.0.0.0-255.255.255.255
- **リモート IP アドレス**　: 0.0.0.0-255.255.255.255
- **ローカルポート**　:3389
- **リモートポート**　:指定なし

4.入力後は右側のチェックをクリックし、ルールの設定を確定します。

5.「保存して発行」をクリックし、プロフィールを確定します。

6.Computer Protection クライアントの「コントロールパネル」→「Windows ファイアウォール」→「詳細設定」→「受信の規則」にルールが追加された事を確認します。



［補足情報］

当手法を行うことで既存の Windows ファイヤーウォールルールを上書きし、既存のアプリケーション通信に影響を与える可能性があります。あらかじめお使いのコンピュータに必要な通信(IP アドレス/ポート番号/etc)を把握した上で当手法をお試しください。

Windows ファイヤーウォールはポリシーのインポート/エクスポート、既定のポリシーの復元機能を備えております。Computer Protection での設定変更前のポリシーをエクスポートしておく事で設定ミスが発生した場合でも設定復元が可能です。
※手順 4 で無効化した既存のルールは、同手順の「他のルールを許可する」を有効化する事で復元できます。


セキュリティが強化された Windows ファイアウォール
ファイル(F)
操作(A)
表示(V)
ヘルプ(H)
ローカル コンピューター のセキュリティ
送信の規則
接続セキュリティの規則
監視
ローカル コンピューター のセキュリティが強化された Windows ファイアウォール
セキュリティが強化された Windows ファイアウォールは、Windows コンピューターにネットワーク セキュリティを提供します。
概要
ドメイン プロファイル
Windows ファイアウォールは有効です。
プライベート プロファイル
Windows ファイアウォールは有効です。
パブリック プロファイルがアクティブです
Windows ファイアウォールは有効です。
Windows ファイアウォールのプロパティ
操作
ローカル コンピューター のセキュリ...
ポリシーのインポート...
既定のポリシーの復元
診断と修復
表示
最新の情報に更新
プロパティ
ヘルプ