技術情報：Si-R Gシリーズ設定例

[「Windows11」とのVPN（IPsec）-IPv4]

Windows11とSi-R GをIPv4でVPN接続する設定例です。

[対象機種と版数]

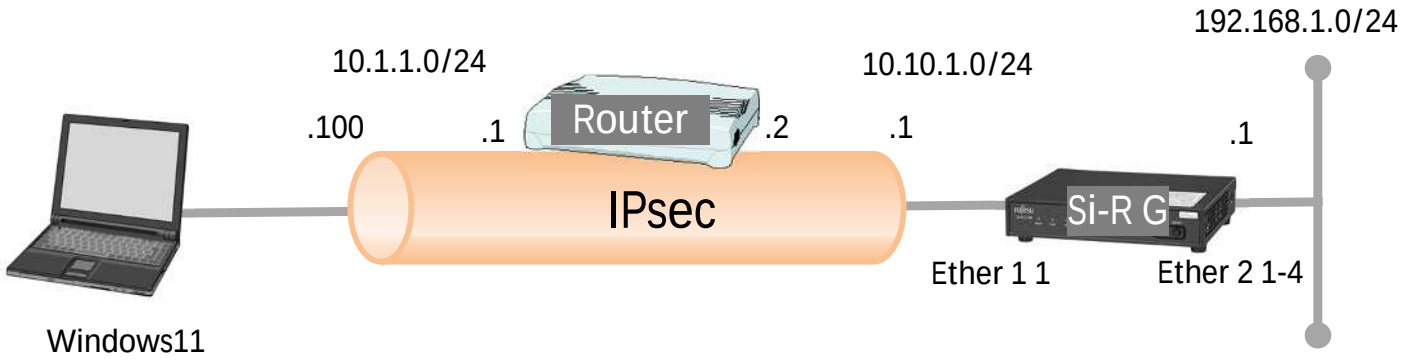
Si-R Gシリーズ V20.54以降

[設定内容]

Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とします。
・LAN側に192.168.1.0/24を割り当てます。

・IKEパラメータ条件
- キー交換モード　メインモード
- 暗号化アルゴリズム　AES-128
- 整合性アルゴリズム　SHA1
- DHグループ　1,024bit
- 事前共有鍵文字列　“test”
- キーの有効期限 480分

・IPsecパラメータ条件
- プロトコル ESP
- 暗号化アルゴリズム AES-128
- 整合性アルゴリズム SHA1
- キーの有効期限 60分/100,000Kbyte



[設定例]
・testにはIPsec鍵を設定してください。

Si-R G設定例

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 0 ip address 10.10.1.1/24 3
lan 0 ip route 0 10.1.1.0/24 10.10.1.2 1 1
lan 0 vlan 1
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 2
remote 0 name win11
remote 0 ap 0 name ipsec
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range 192.168.1.0/24 10.1.1.100/32
remote 0 ap 0 ipsec ike encrypt aes-cbc-128
remote 0 ap 0 ipsec ike auth hmac-sha1
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text test
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
remote 0 ap 0 ike proposal 0 hash hmac-sha1
remote 0 ap 0 ike proposal 0 pfs modp1024
remote 0 ap 0 tunnel local 10.10.1.1
remote 0 ap 0 tunnel remote 10.1.1.100
remote 1 name olap
remote 1 ap 0 name olap
remote 1 ap 0 datalink type overlap
remote 1 ap 0 multiroute pattern 0 use any 500 any 500 17 any
remote 1 ap 0 multiroute pattern 1 use any any any any 50 any
remote 1 ap 0 overlap to lan 0
remote 1 ap 0 overlap nexthop 10.10.1.2
remote 1 ap 1 name olap1
remote 1 ap 1 datalink type overlap
remote 1 ap 1 multiroute pattern 0 use any any any any any any
remote 1 ap 1 overlap to remote 0
remote 1 ip route 0 10.1.1.100/32 1 1
syslog facility 23
time zone 0900
resource system vlan 4089-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

[解説]

Si-R_G設定解説

ether 1 1 vlan untag 1
ether1 1ポートをTag なしVLAN1に設定します。

ether 2 1-4 vlan untag 2
ether2 1-4ポートをTag なしVLAN2に設定します。

lan 0 ip address 10.10.1.1/24 3
LAN0側IPアドレスを設定します。
　10.10.1.1/24 ： IPアドレス/マスクです。
　3 ： ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 0 ip route 0 10.1.1.0/24 10.10.1.2 1 1
スタティックルートを設定します。
　10.1.1.0/24 ： 宛先ネットワーク/マスクです。
　10.10.1.2 ： ネクストホップです。
　1 ： metric値です。通常はこのままで構いません。
　1 ： distance値です。通常はこのままで構いません。

lan 0 vlan 1
VLAN ID とlan 定義番号の関連付けを行います。
LAN0にTag なしVLAN1を設定します。

lan 1 ip address 192.168.1.1/24 3
LAN1側IPアドレスを設定します。
　192.168.1.1/24 ： IPアドレス/マスクです。
　3 ： ブロードキャストアドレスのタイプです。通常は3で構いません。

lan 1 vlan 2
VLAN IDとlan 定義番号の関連付けを行います。
LAN1にTag なしVLAN2を設定します。

remote 0 name win11
インタフェースの名前（任意）を設定します。

remote 0 ap 0 name ipsec
アクセスポイントの名前（任意）を設定します。

remote 0 ap 0 datalink type ipsec
パケット転送方法としてIPsecを設定します。

remote 0 ap 0 ipsec type ike
IPsec情報のタイプにIPsec自動鍵交換を設定します。

remote 0 ap 0 ipsec ike protocol esp
自動鍵交換用IPsec情報のセキュリティプロトコルにESP（暗号）を設定します。

remote 0 ap 0 ipsec ike range 192.168.1.0/24 10.1.1.100/32
自動鍵交換用IPsec 情報の対象範囲を設定します。
192.168.1.0/24 ： IPsec 対象となる送信元IP アドレス/マスクです。
10.1.1.100/32 ： IPsec 対象となる宛先IP アドレス/マスクです。

remote 0 ap 0 ipsec ike encrypt aes-cbc-128
自動鍵交換用IPsec情報の暗号情報にAES128ビットを設定します。

remote 0 ap 0 ipsec ike auth hmac-sha1
自動鍵交換用IPsec情報の認証情報にSHA1を設定します。

remote 0 ap 0 ike mode main
情報の交換モードを設定します。
main ： IKE 情報の交換モードとしてMain Mode を使用します。

remote 0 ap 0 ike shared key text test
IKEセッション確立時の共有鍵（Pre-shared key）を設定します。

remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
IKEセッション用暗号情報の暗号アルゴリズムにAES128ビットを設定します。

remote 0 ap 0 ike proposal 0 hash hmac-sha1
IKE セッション用認証（ハッシュ）情報にSHA1を設定します。

remote 0 ap 0 ike proposal 0 pfs modp1024
IKE セッション用DH（Diffie-Hellman）グループにmodp1024を設定します。

remote 0 ap 0 tunnel local 10.10.1.1
IPsecトンネルの送信元アドレスの設定をします。

remote 0 ap 0 tunnel remote 10.1.1.100
IPsecトンネルの送信先アドレスの設定をします。

remote 1 name olap
インターフェースの名前（任意）を設定します。

remote 1 ap 0 name olap
アクセスポイント0の名前（任意）を設定します。

remote 1 ap 0 datalink type overlap
パケット転送方法にoverlapを設定します。

remote 1 ap 0 multiroute pattern 0 use any 500 any 500 17 any
remote 1 ap 0 multiroute pattern 1 use any any any any 50 any
remote 1 ap 0 overlap to lan 0
remote 1 ap 0 overlap nexthop 10.10.1.2
IKE,ESPパケットをlan 0から10.1.1.2に転送します。

remote 1 ap 1 name olap1
アクセスポイント1の名前（任意）を設定します。

remote 1 ap 1 datalink type overlap
パケット転送方法にoverlapを設定します。

remote 1 ap 1 multiroute pattern 0 use any any any any any any
remote 1 ap 1 overlap to remote 0
IKE,ESP以外の全てのパケットをremote 0から送出します。

remote 1 ip route 0 10.1.1.100/32 1 1
スタティックルートを設定します。
10.1.1.100/32 ：宛先ネットワーク/マスクです。
1 ： metric値です。通常は1で構いません。
1 ： distance値です。通常は1で構いません。

syslog facility 23
システムログ情報の出力情報／出力対象ファシリティの設定をします。通常はこのままで構いません。

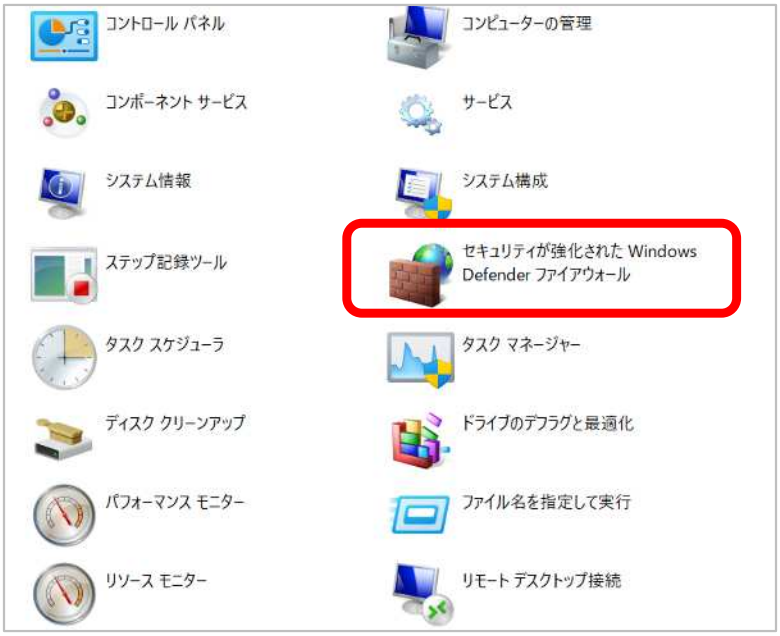
time zone 0900
タイムゾーンを設定します。通常はこのままで構いません。

consoleinfo autologout 8h
telnetinfo autologout 5m
シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこのままで構いません。

terminal charset SJIS
ターミナルで使用する漢字コードをShift JISコードに設定します。

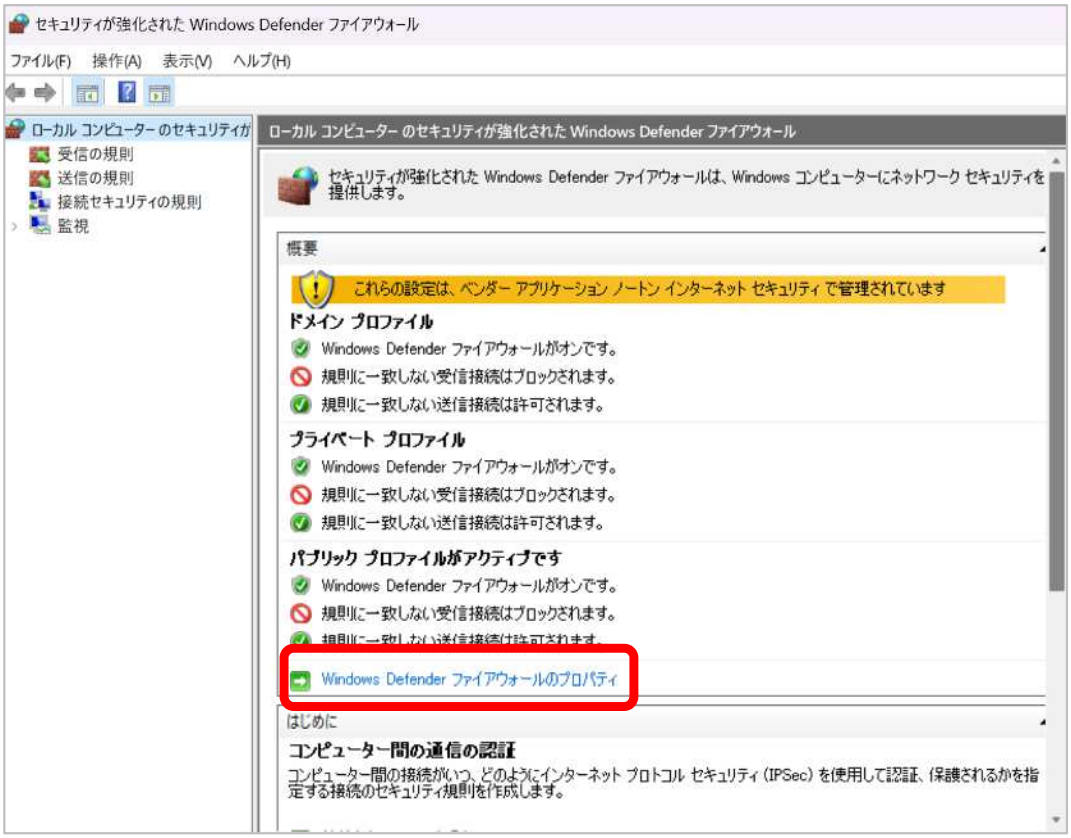
Windows11設定例

Windowsのメニュー→「Windowsツール」→「セキュリティが強化されたWindowsファイアーウォール」の順にクリックします。

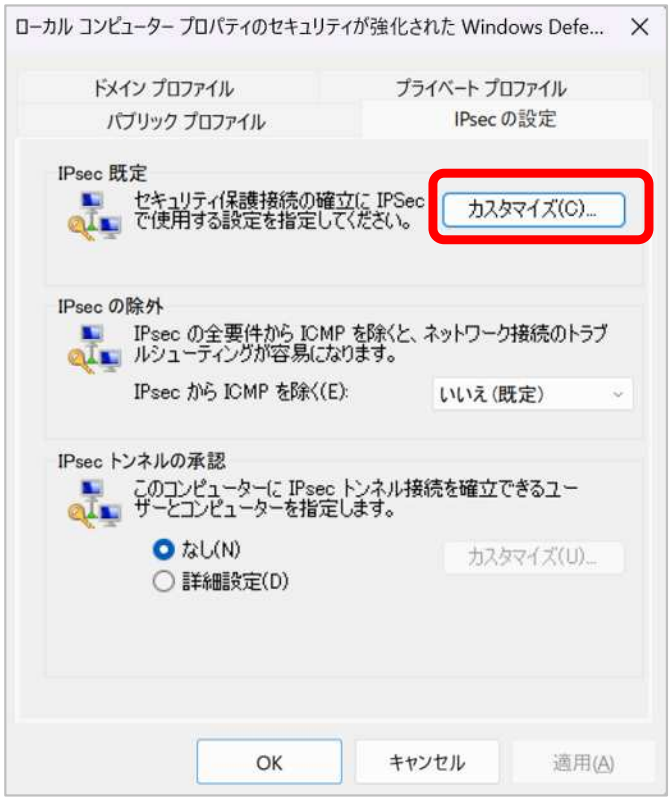


「セキュリティが強化されたWindowsファイアーウォール」をダブルクリックします。

「Windowsファイアーウォールのプロパティ」をクリックします。



「IPsecの設定」カスタマイズをクリックします。

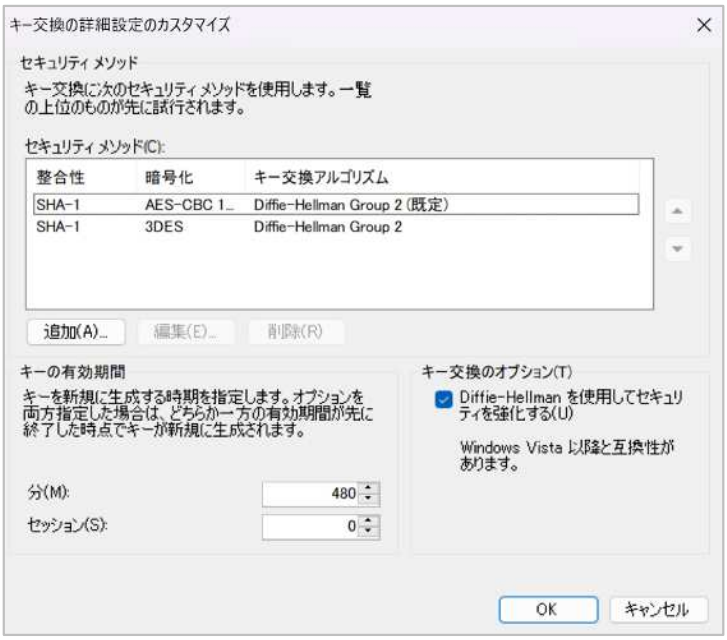


各項目を設定します。

1.「キー交換（メインモード）」詳細設定→カスタマイズをクリックします。
2.「データ保護（クイックモード）」詳細設定→カスタマイズをクリックします。
3.「認証方法」詳細設定→カスタマイズをクリックします。

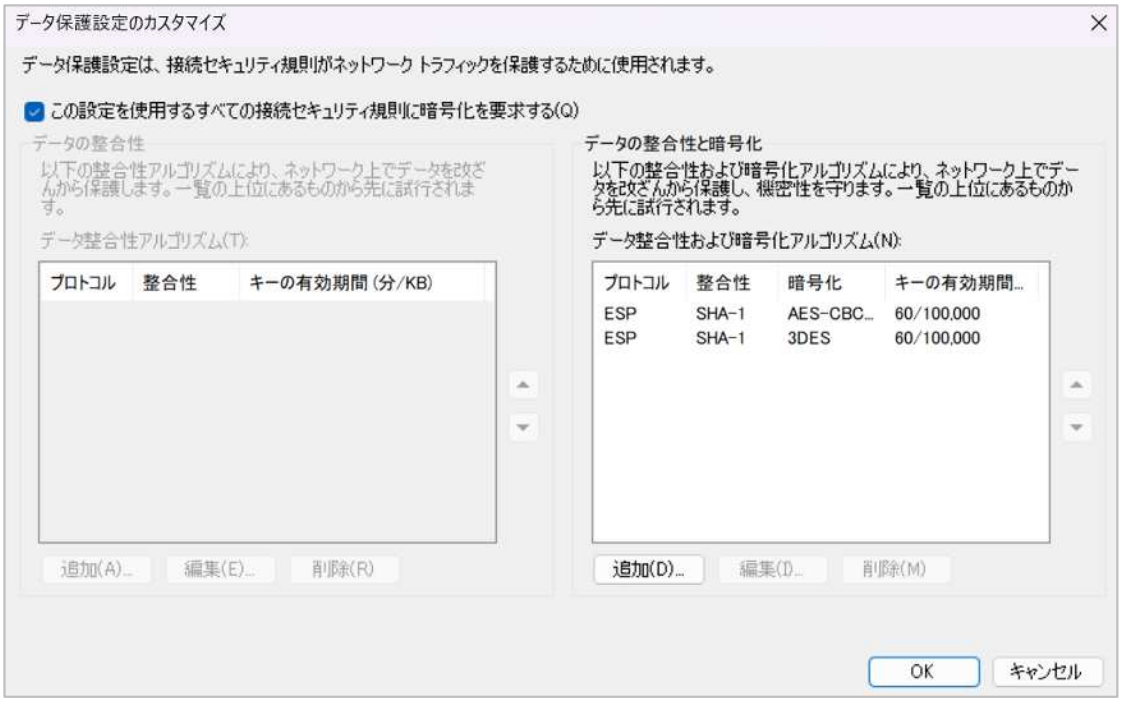
1. キー交換（詳細）

Si-Rとセキュリティメソッドとキー交換アルゴリズムを合わせます。
追加もしくは編集を行います。
キーの有効時間はデフォルトの設定で問題ありません。
（remote ap ike）



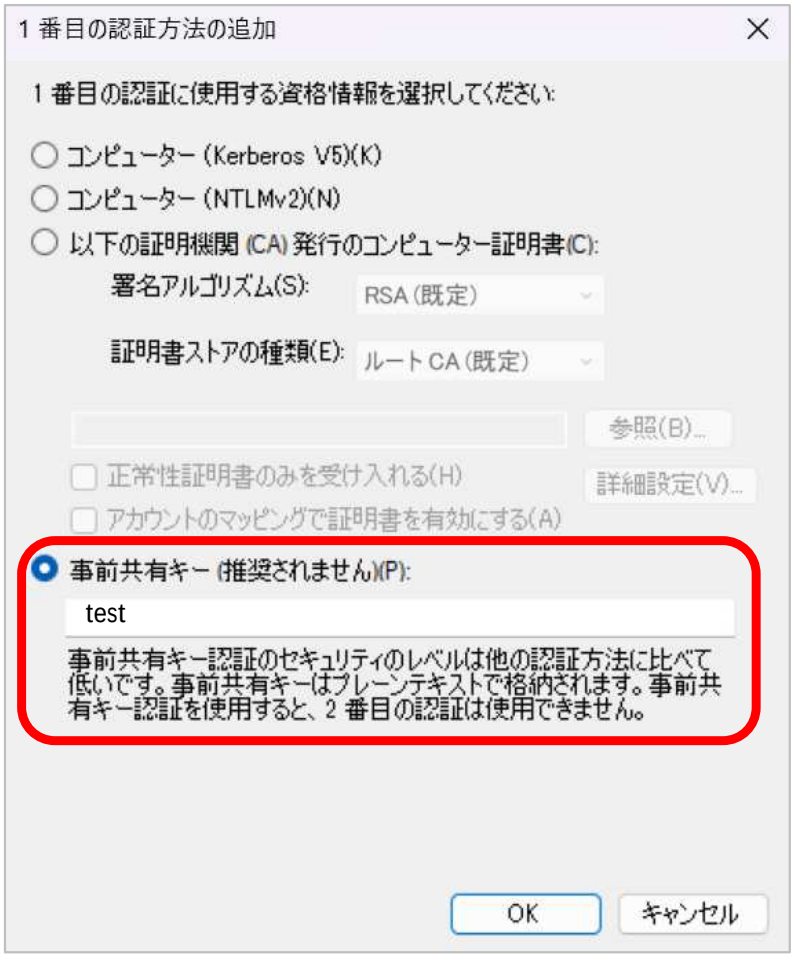
2. データ保護（詳細）

データの整合性と暗号化でSi-Rとアルゴリズムを合わせます。
追加もしくは編集を行います。
（remote ap ispec ike）



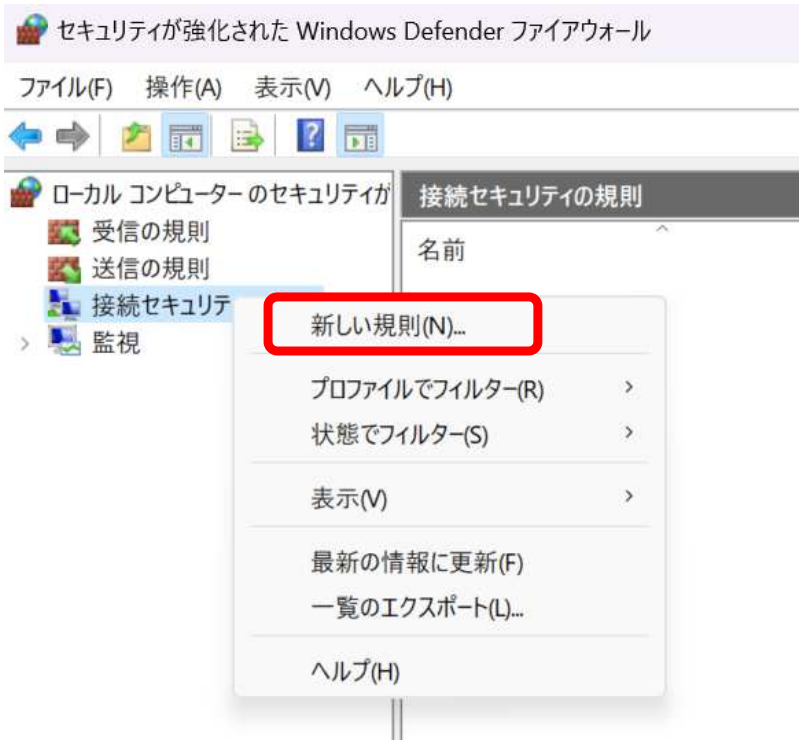
3. 認証

1番目の認証で事前共有キーを設定します。



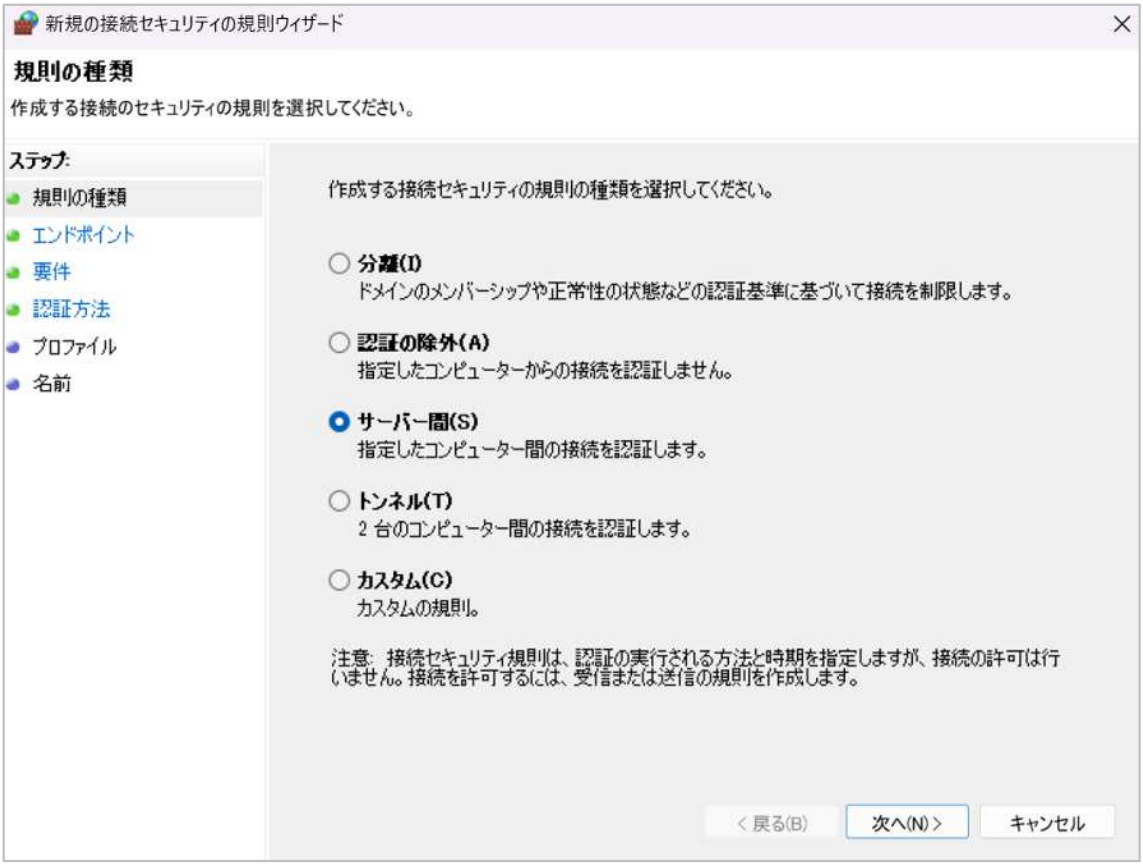
「接続セキュリティの規則」を設定します。

最初は何も設定が無いので追加して下さい。



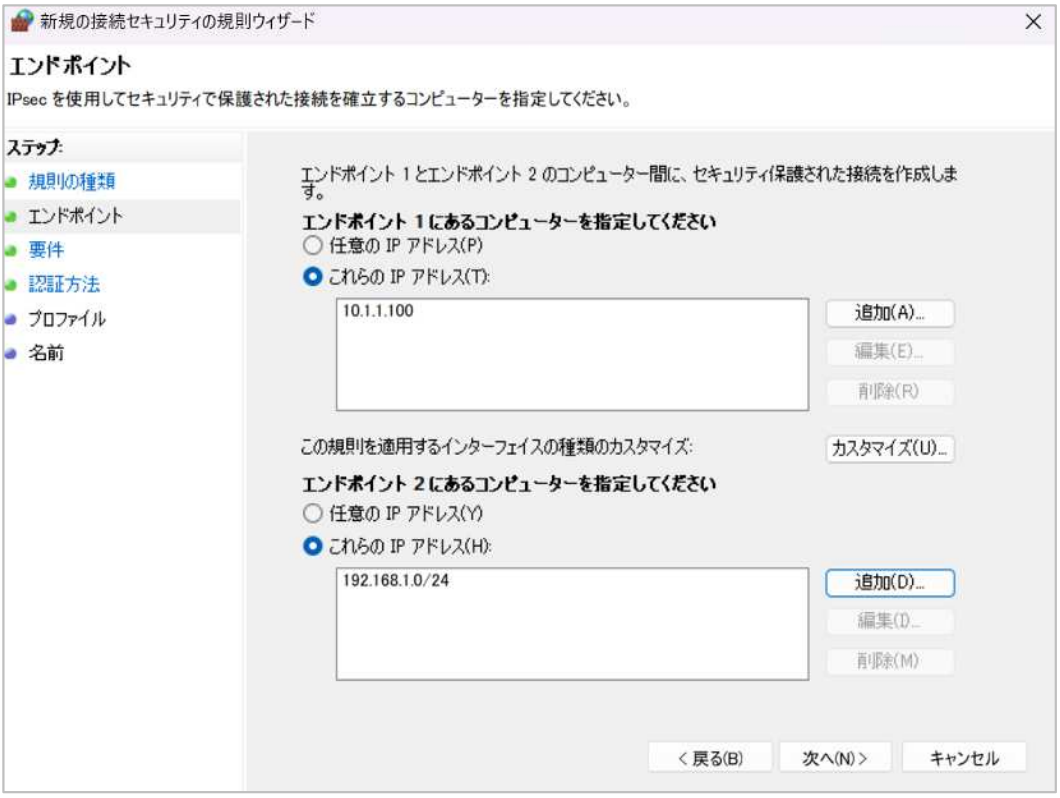
「規則の種類」

規則の種類で「サーバ間」を選択します。



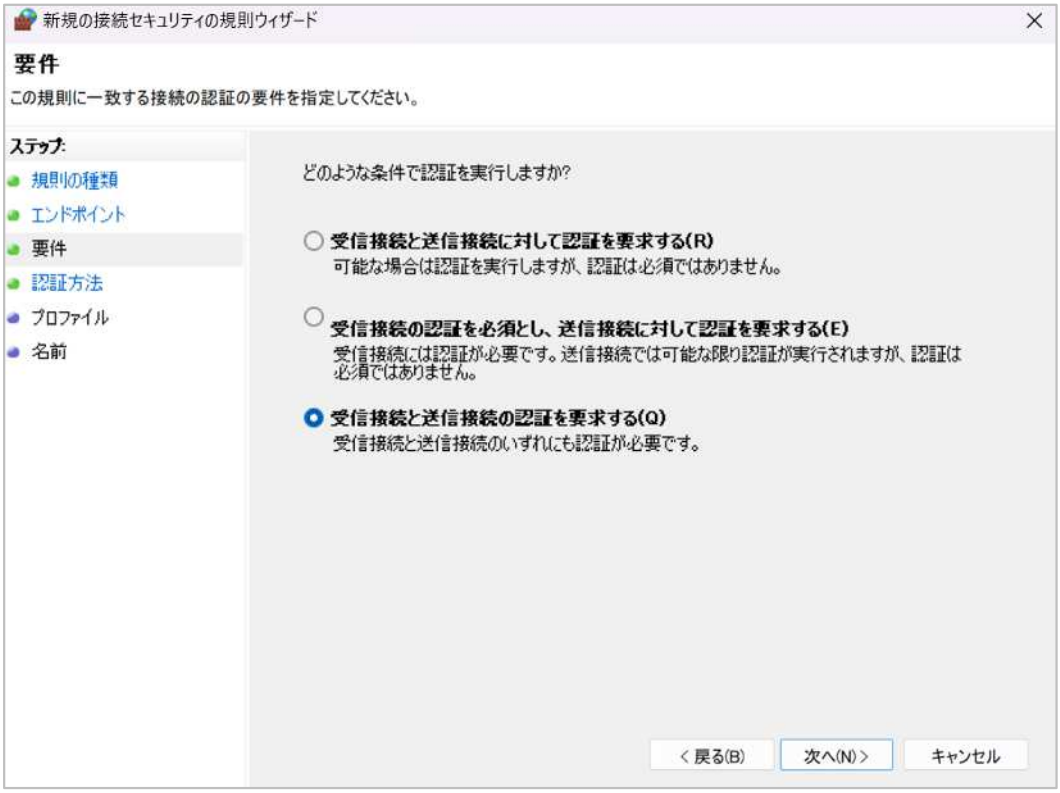
「エンドポイント」

エンドポイント1はwindows11側のIPsec暗号化対象パケットの範囲です。
エンドポイント2はSi-R側のIPsec暗号化対象パケットの範囲です。
（remote ap ipsec ike range）



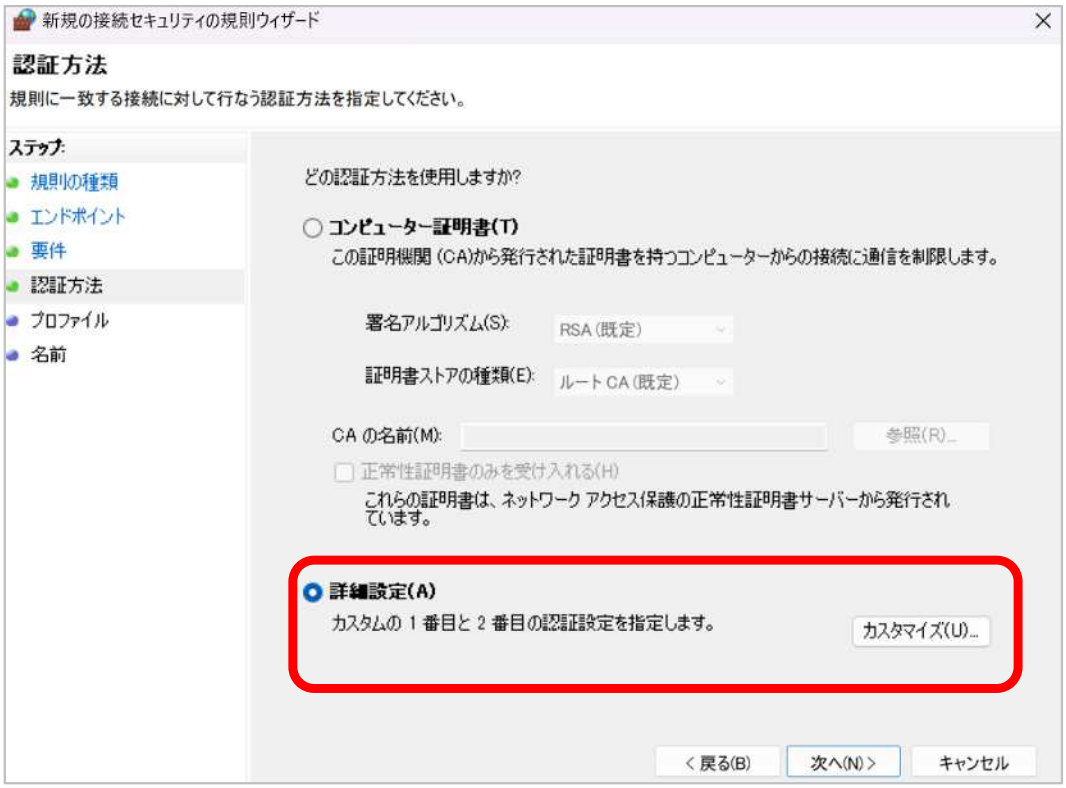
「要件」

要件で「受信接続と送信接続の認証を要求する」を選択します。

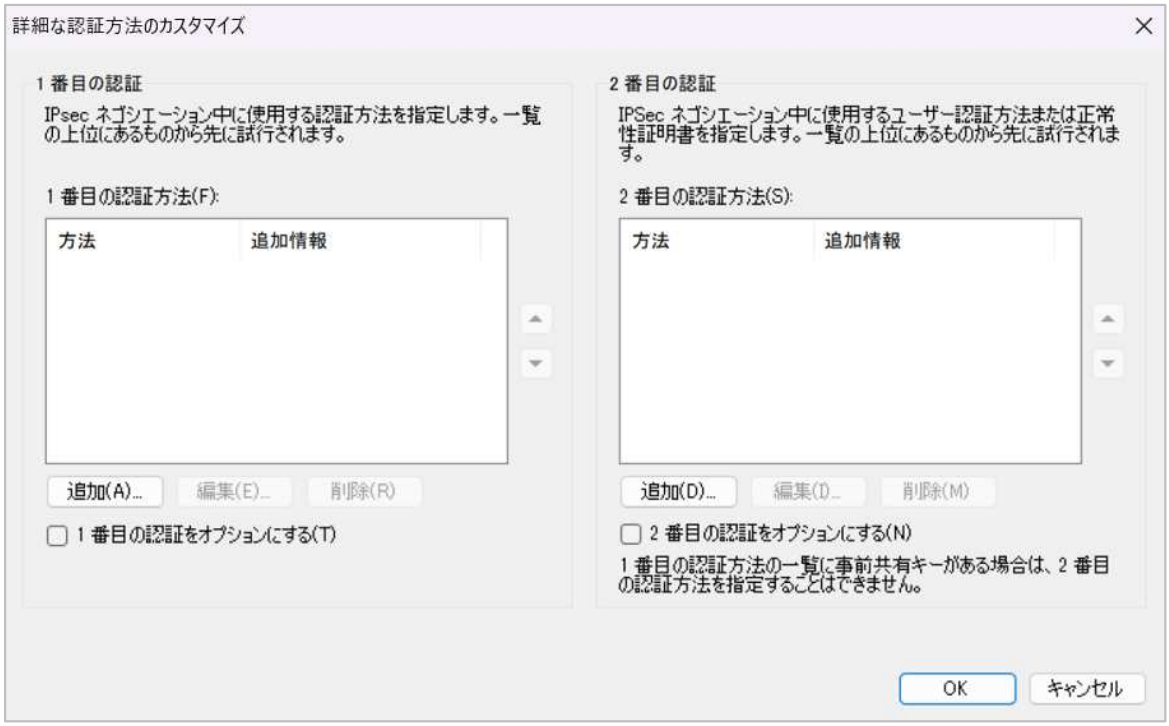


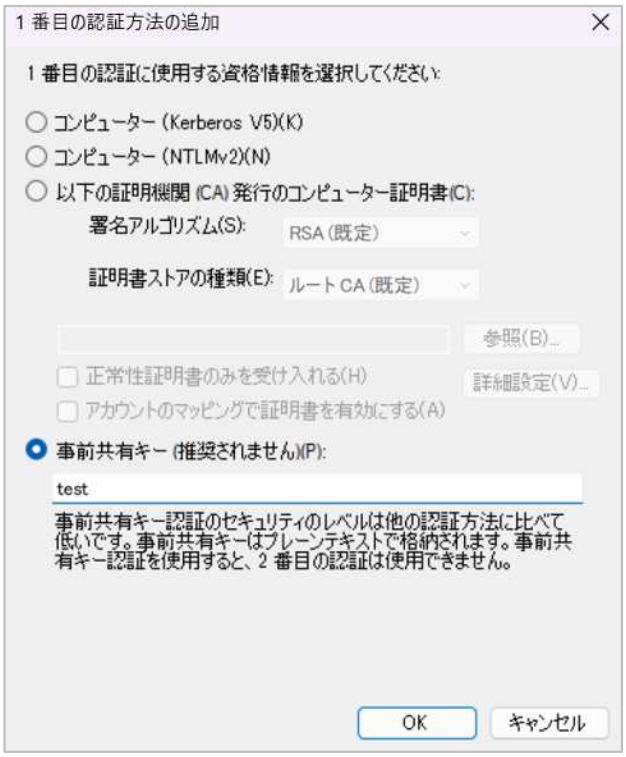
「認証方式」

詳細設定でカスタマイズを選択します。



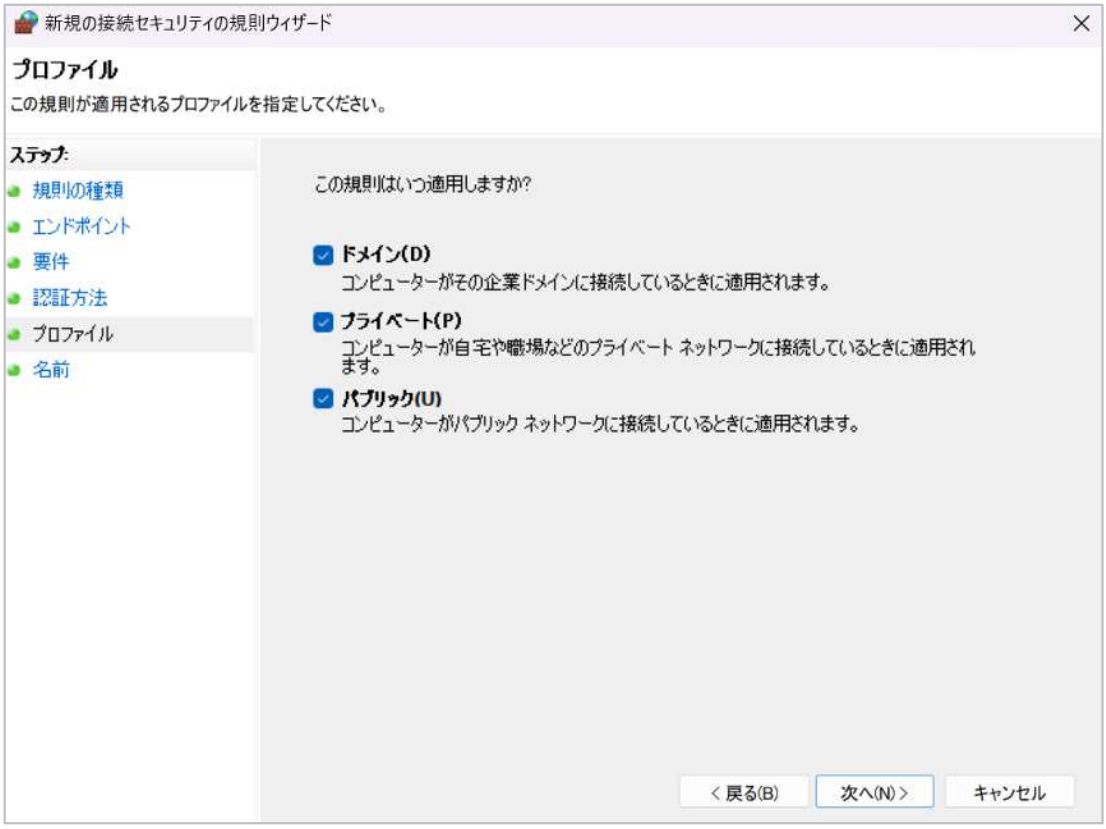
1番目の認証方法に事前共有キーを追加します。





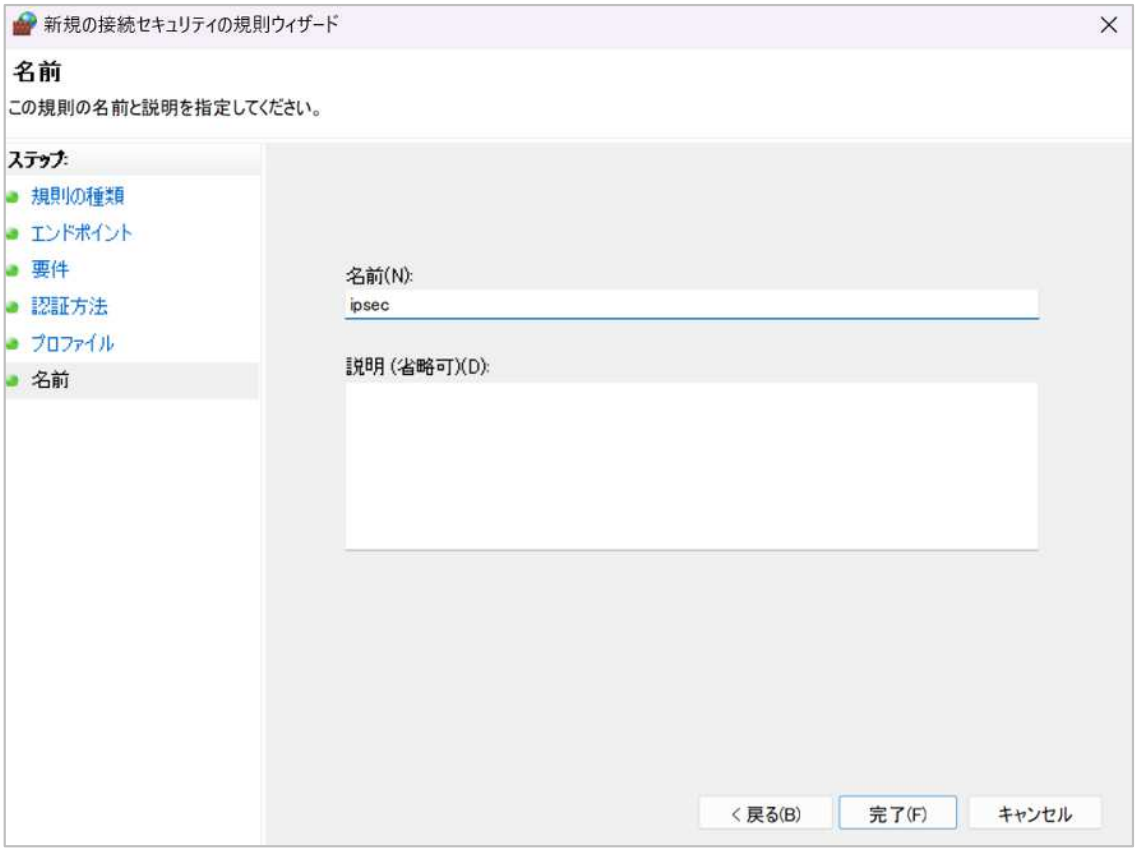
「プロファイル」

ドメイン、プライベート、パブリックにチェックがついている事を確認します。

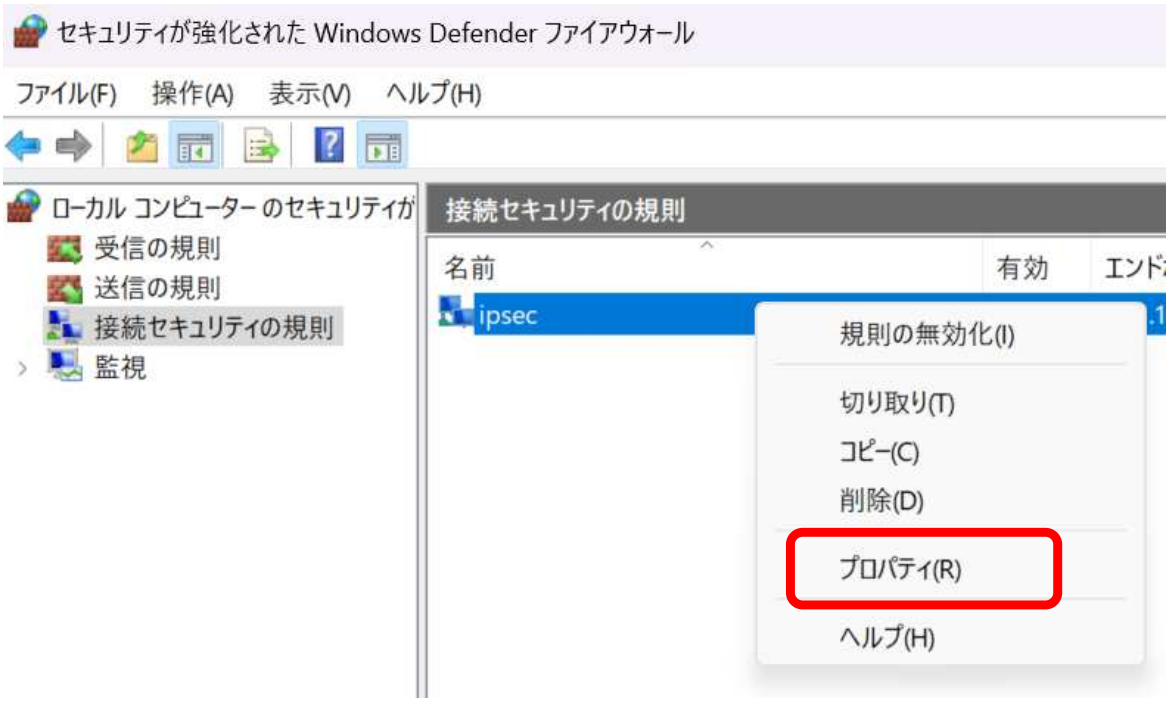


「名前」

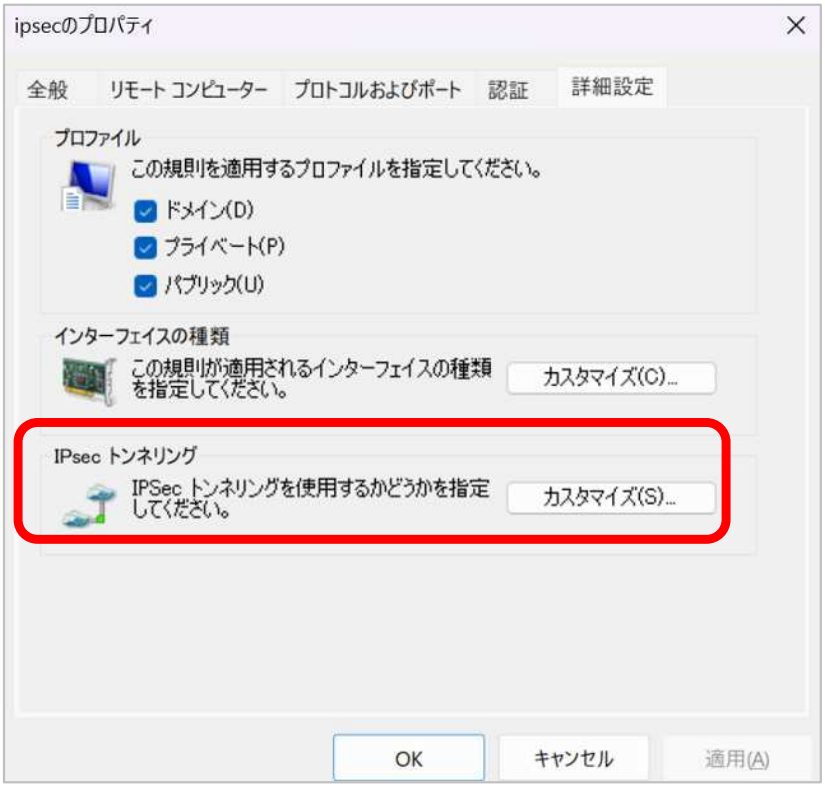
ipsecという名前でセキュリティ規則を追加します。



先ほど追加したセキュリティ規則のプロパティを開きます。



詳細設定タブのIPsecトンネリングのカスタマイズをクリックします。



IPsecトンネリングを使用するをチェックします。

ローカルはwindows11側、IPsecトンネルの起点アドレスです。

リモートはSi-R側、IPsecトンネルの起点アドレスです。