

【「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]

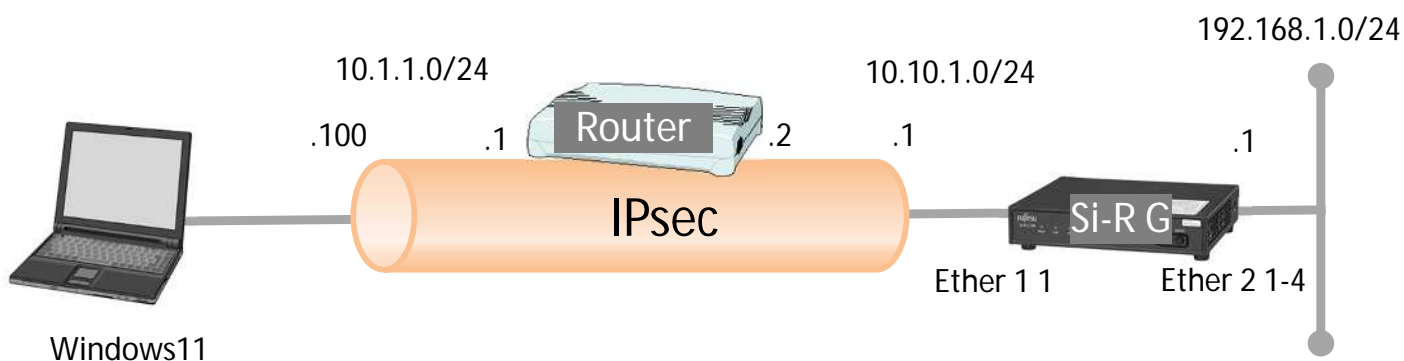
Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とします。
・LAN側に192.168.1.0/24を割り当てます。

・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
```

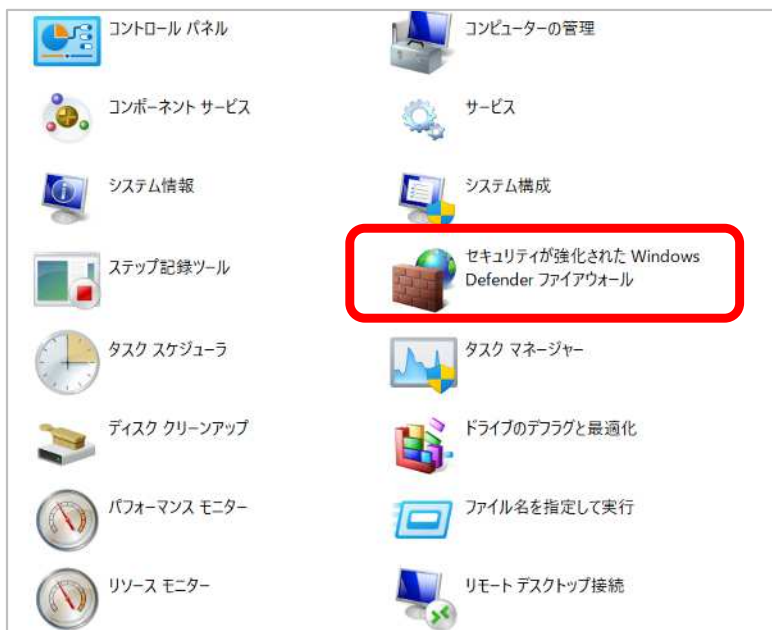
シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこのままで構いません。

```
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。

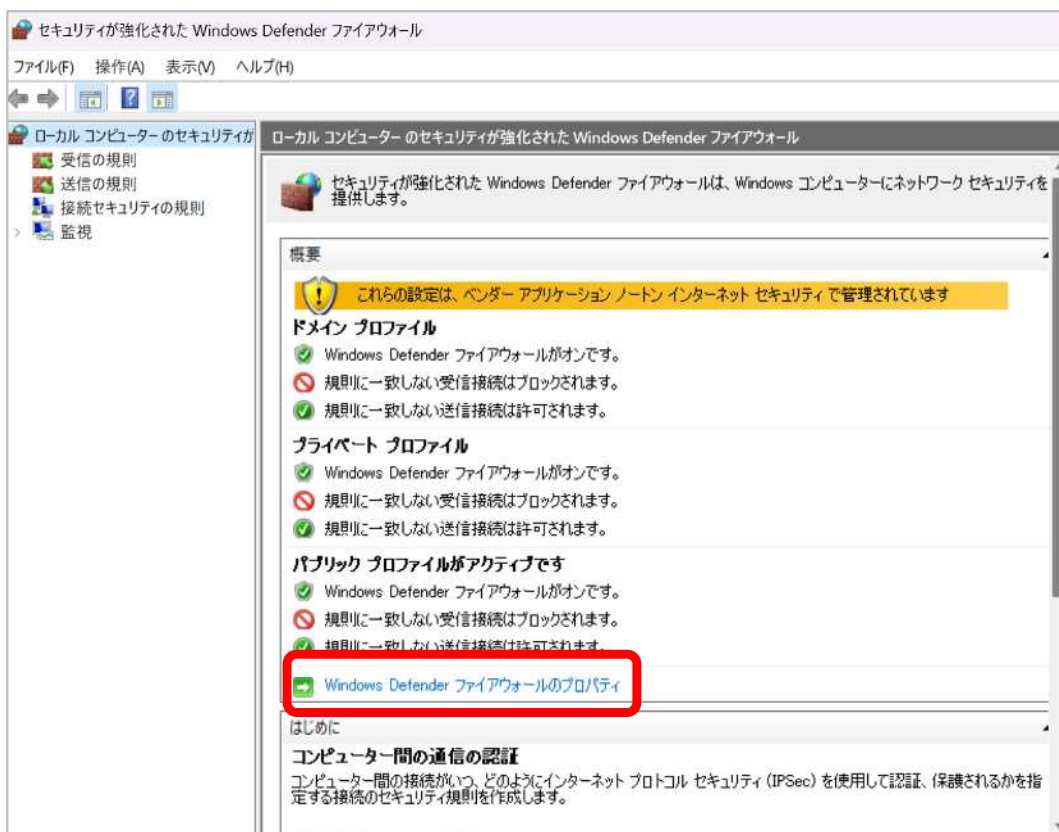
Windows11 設定例

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。

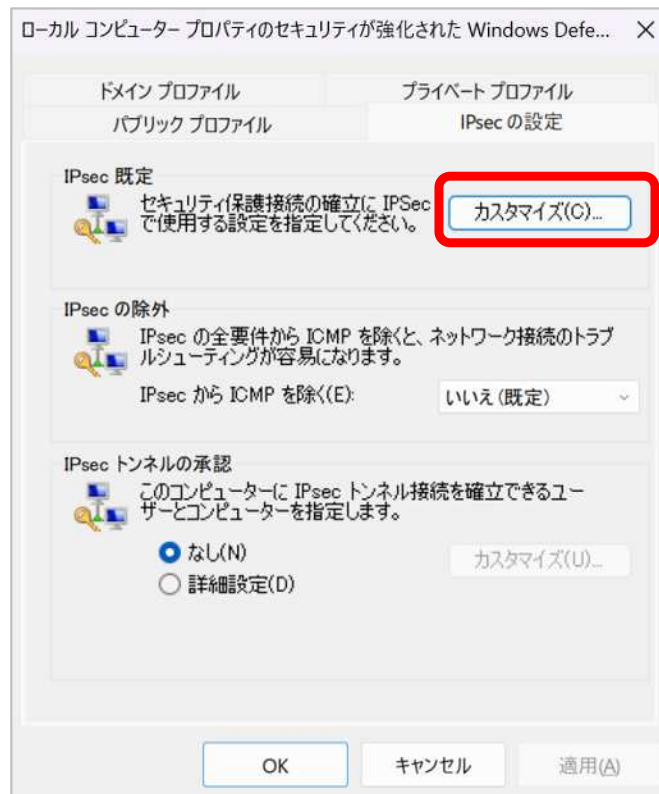


「セキュリティが強化されたWindowsファイアウォール」をダブルクリックします。

「Windowsファイアウォールのプロパティ」をクリックします。

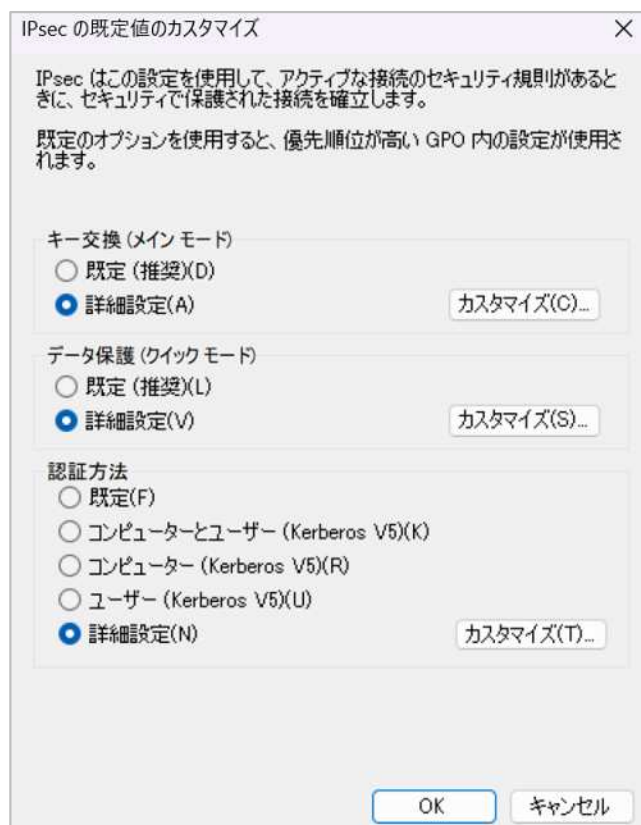


「IPsecの設定」カスタマイズをクリックします。



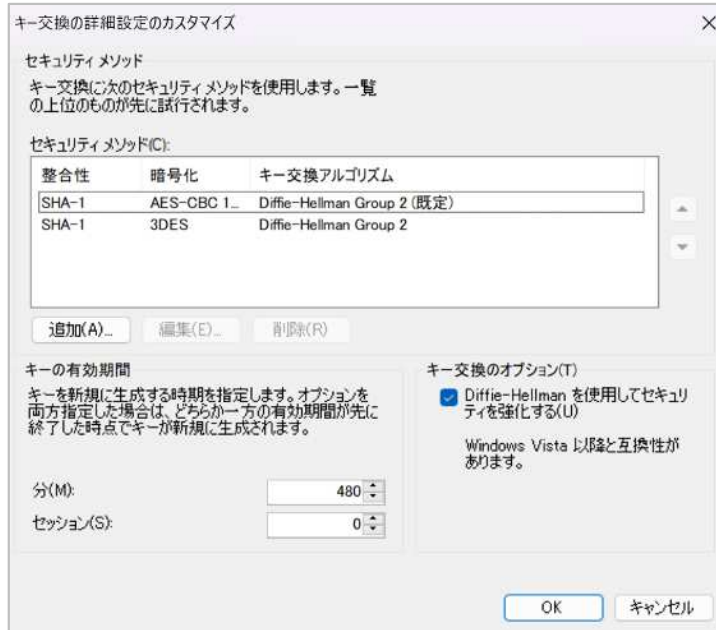
各項目を設定します。

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。



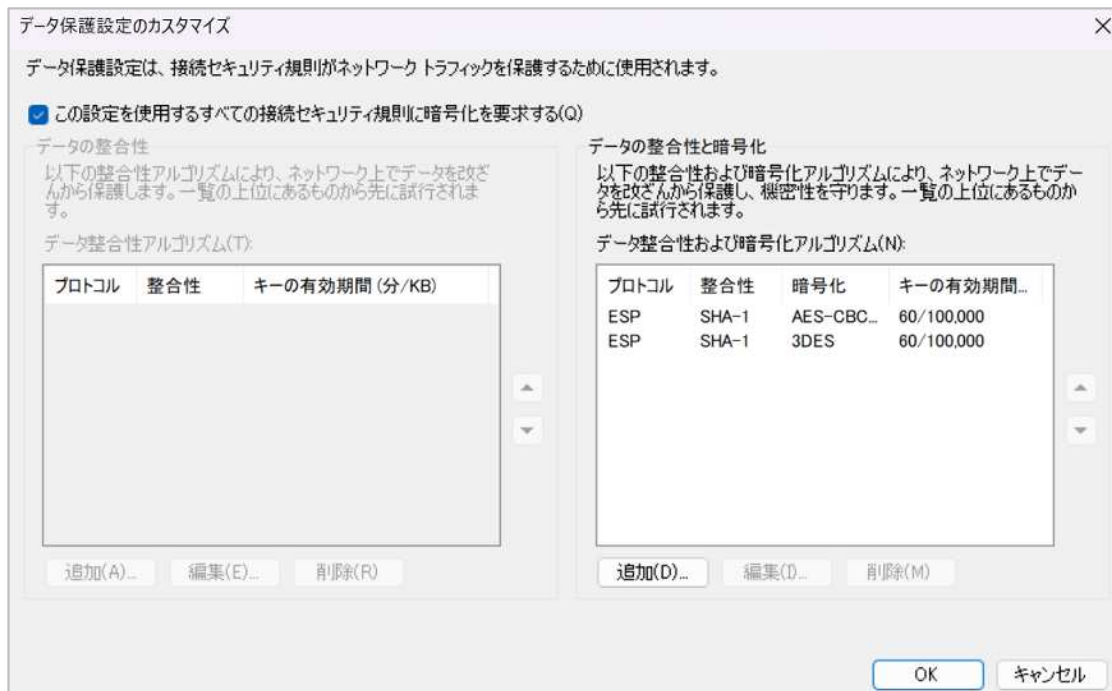
1. キー交換（詳細）

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)



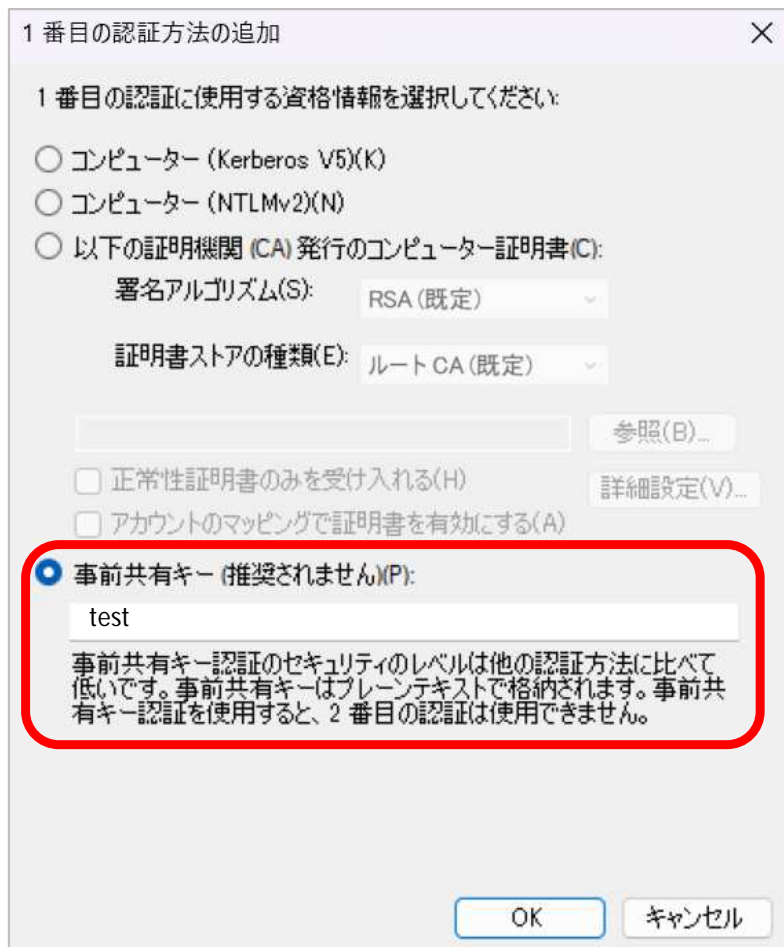
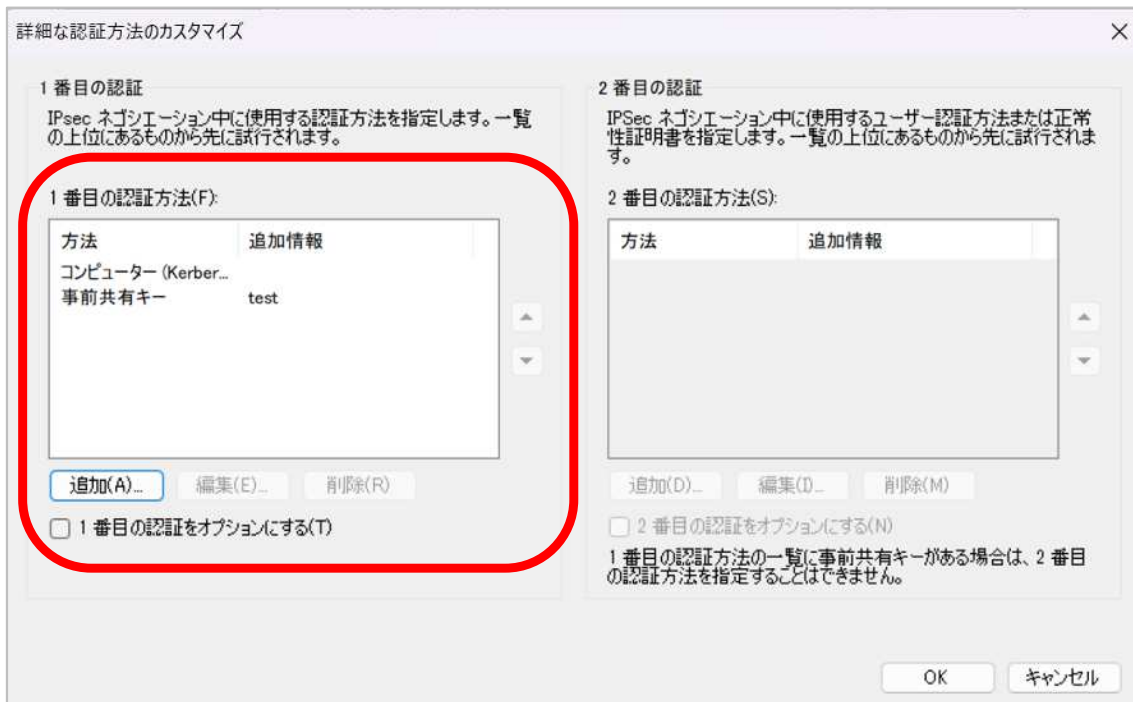
2. データ保護（詳細）

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)



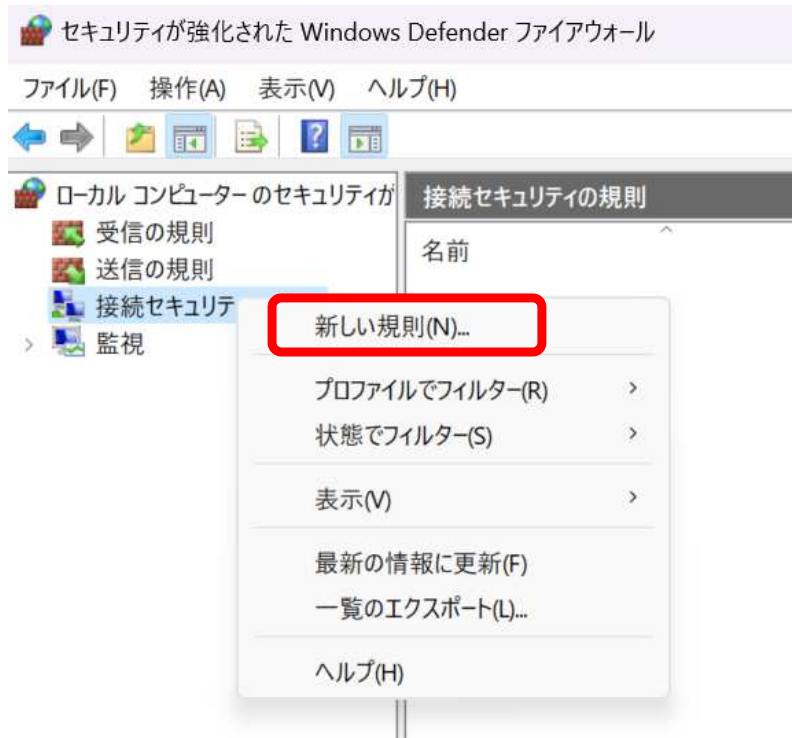
3. 認証

1番目の認証で事前共有キーを設定します。



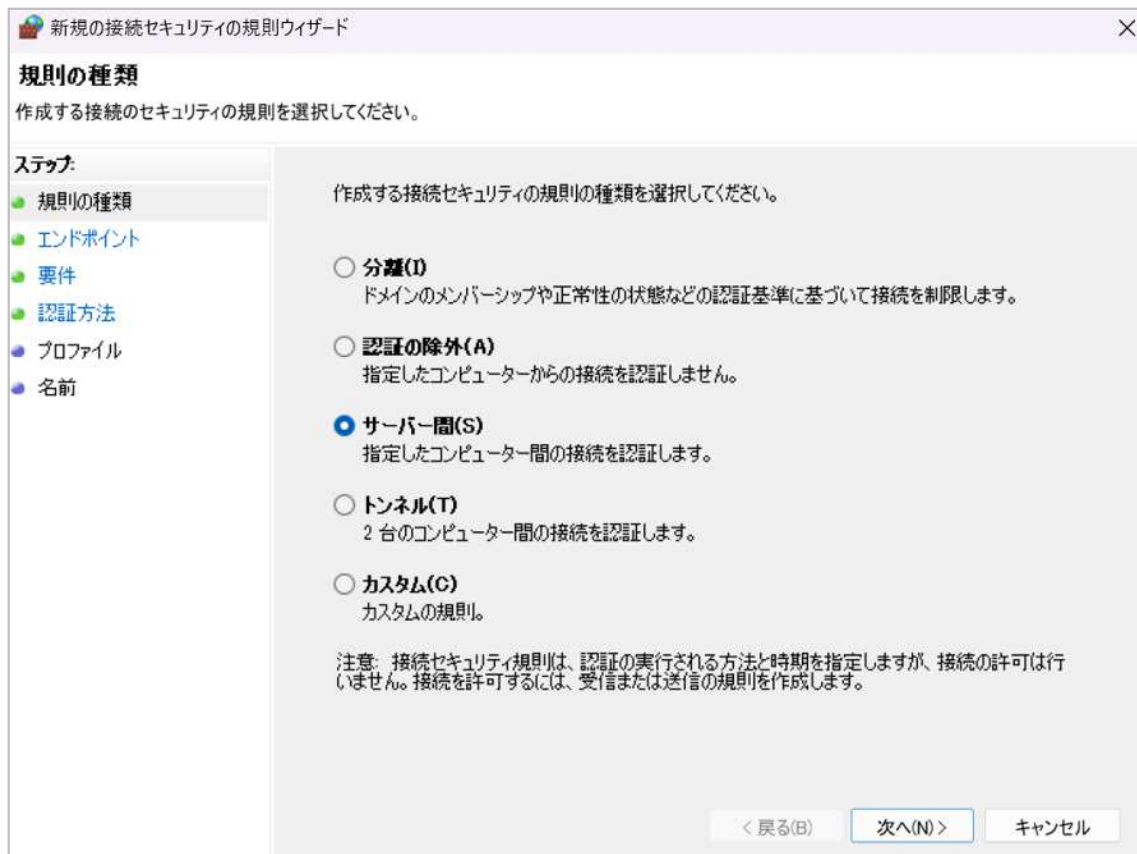
「接続セキュリティの規則」を設定します。

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)

The screenshot shows the 'New Connection Security Rule Wizard' dialog box, specifically the 'Endpoints' step. The title bar reads '新規の接続セキュリティの規則ウィザード'. The main heading is 'エンドポイント' (Endpoints). Below the heading, it says 'IPsec を使用してセキュリティで保護された接続を確立するコンピューターを指定してください。' (Specify computers to establish a security-protected connection using IPsec). On the left, a 'ステップ' (Steps) pane lists: 規則の種類 (Rule type), エンドポイント (Endpoints), 要件 (Requirements), 認証方法 (Authentication method), プロファイル (Profile), and 名前 (Name). The 'エンドポイント' step is currently selected. The main area contains the following text: 'エンドポイント 1 とエンドポイント 2 のコンピューター間に、セキュリティ保護された接続を作成します。' (Create a security-protected connection between the computers of Endpoint 1 and Endpoint 2). Under 'エンドポイント 1 にあるコンピューターを指定してください' (Specify computers at Endpoint 1), there are two radio buttons: '任意の IP アドレス(P)' (Any IP address) and 'これらの IP アドレス(T):' (These IP addresses), with the latter selected. A text box contains '10.1.1.100'. To the right are buttons: '追加(A)...' (Add), '編集(E)...' (Edit), and '削除(R)' (Remove). Below this, it says 'この規則を適用するインターフェイスの種類のカスタマイズ:' (Customize the type of interface to which this rule is applied), with a 'カスタマイズ(U)...' (Customize) button. Under 'エンドポイント 2 にあるコンピューターを指定してください' (Specify computers at Endpoint 2), there are two radio buttons: '任意の IP アドレス(Y)' (Any IP address) and 'これらの IP アドレス(H):' (These IP addresses), with the latter selected. A text box contains '192.168.1.0/24'. To the right are buttons: '追加(D)...' (Add), '編集(I)...' (Edit), and '削除(M)' (Remove). At the bottom are buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).

「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。

The screenshot shows the 'New Connection Security Rule Wizard' dialog box, specifically the 'Requirements' step. The title bar reads '新規の接続セキュリティの規則ウィザード'. The main heading is '要件' (Requirements). Below the heading, it says 'この規則に一致する接続の認証の要件を指定してください。' (Specify the requirements for authentication of connections that match this rule). On the left, a 'ステップ' (Steps) pane lists: 規則の種類 (Rule type), エンドポイント (Endpoints), 要件 (Requirements), 認証方法 (Authentication method), プロファイル (Profile), and 名前 (Name). The '要件' step is currently selected. The main area contains the following text: 'どのような条件で認証を実行しますか?' (Under what conditions do you want to perform authentication?). There are three radio buttons: '受信接続と送信接続に対して認証を要求する(R)' (Require authentication for both incoming and outgoing connections), '受信接続の認証を必須とし、送信接続に対して認証を要求する(E)' (Require authentication for incoming connections and require authentication for outgoing connections), and '受信接続と送信接続の認証を要求する(Q)' (Require authentication for both incoming and outgoing connections), with the latter selected. Below the radio buttons are explanatory text blocks: '可能な場合は認証を実行しますが、認証は必須ではありません。' (Perform authentication where possible, but authentication is not required.), '受信接続には認証が必要です。送信接続では可能な限り認証が実行されますが、認証は必須ではありません。' (Authentication is required for incoming connections. Authentication is performed where possible for outgoing connections, but authentication is not required.), and '受信接続と送信接続のいずれにも認証が必要です。' (Authentication is required for both incoming and outgoing connections.). At the bottom are buttons: '< 戻る(B)' (Back), '次へ(N) >' (Next), and 'キャンセル' (Cancel).

「認証方式」

詳細設定でカスタマイズを選択します。

新規の接続セキュリティの規則ウィザード

認証方法

規則に一致する接続に対して行なう認証方法を指定してください。

ステップ:

- 規則の種類
- エンドポイント
- 要件
- 認証方法
- プロファイル
- 名前

どの認証方法を使用しますか?

コンピューター証明書(T)
この証明機関 (CA)から発行された証明書を持つコンピューターからの接続(通信)を制限します。

署名アルゴリズム(S): RSA (既定)

証明書ストアの種類(E): ルート CA (既定)

CA の名前(M): 参照(R)...

正常性証明書のみを受け入れる(H)
これらの証明書は、ネットワーク アクセス保護の正常性証明書サーバーから発行されています。

詳細設定(A)
カスタムの 1 番目と 2 番目の認証設定を指定します。

1番目の認証方法に事前共有キーを追加します。

詳細な認証方法のカスタマイズ

1 番目の認証
IPsec ネゴシエーション中に使用する認証方法を指定します。一覧の上位にあるものから先に試行されます。

1 番目の認証方法(F):

方法	追加情報
----	------

追加(A)... 編集(E)... 削除(R)

1 番目の認証をオプションにする(T)

2 番目の認証
IPsec ネゴシエーション中に使用するユーザー認証方法または正常性証明書を指定します。一覧の上位にあるものから先に試行されます。

2 番目の認証方法(S):

方法	追加情報
----	------

追加(D)... 編集(D)... 削除(M)

2 番目の認証をオプションにする(N)

1 番目の認証方法の一覧に事前共有キーがある場合は、2 番目の認証方法を指定することはできません。

OK キャンセル

1 番目の認証方法の追加

1 番目の認証に使用する資格情報を選択してください:

コンピューター (Kerberos V5)(K)

コンピューター (NTLMv2)(N)

以下の証明機関 (CA) 発行のコンピューター証明書(C):

署名アルゴリズム(S): RSA (既定)

証明書ストアの種類(E): ルート CA (既定)

参照(B)...

正常性証明書のみを受け入れる(H) 詳細設定(V)...

アカウントのマッピングで証明書を有効にする(A)

事前共有キー (推奨されません)(P):

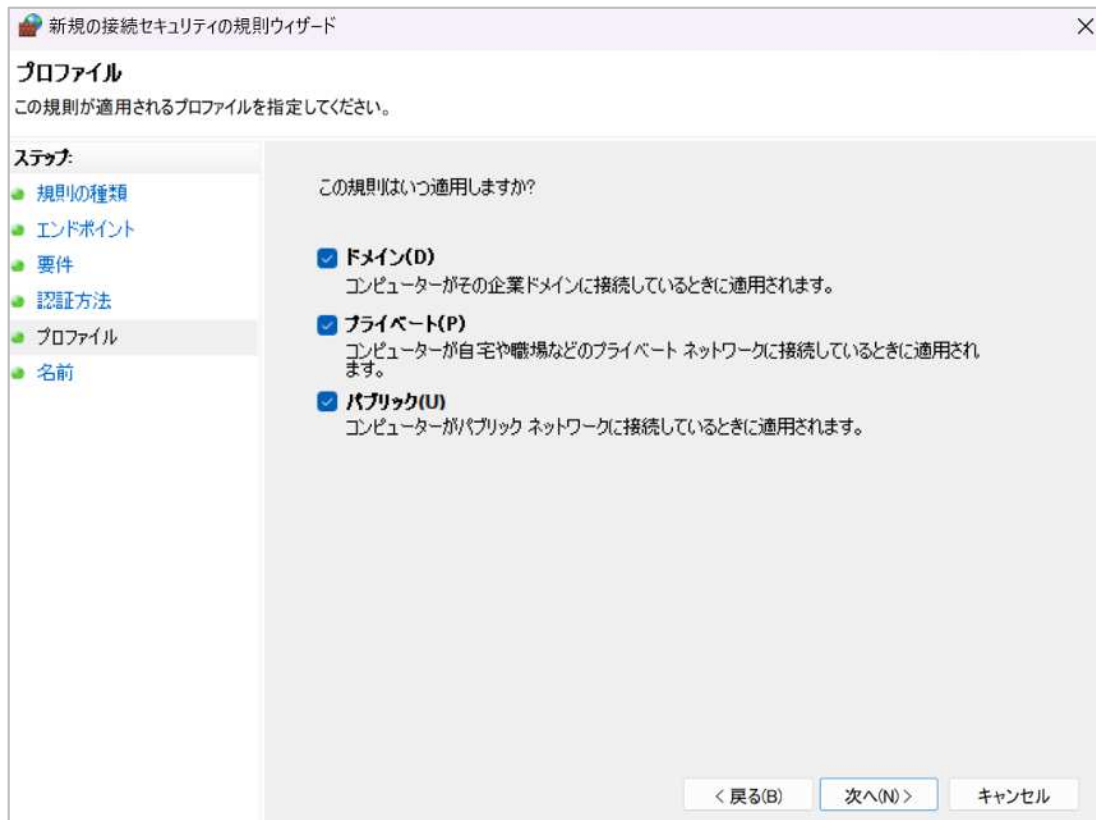
test

事前共有キー認証のセキュリティのレベルは他の認証方法に比べて低いです。事前共有キーはプレーンテキストで格納されます。事前共有キー認証を使用すると、2 番目の認証は使用できません。

OK キャンセル

「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。

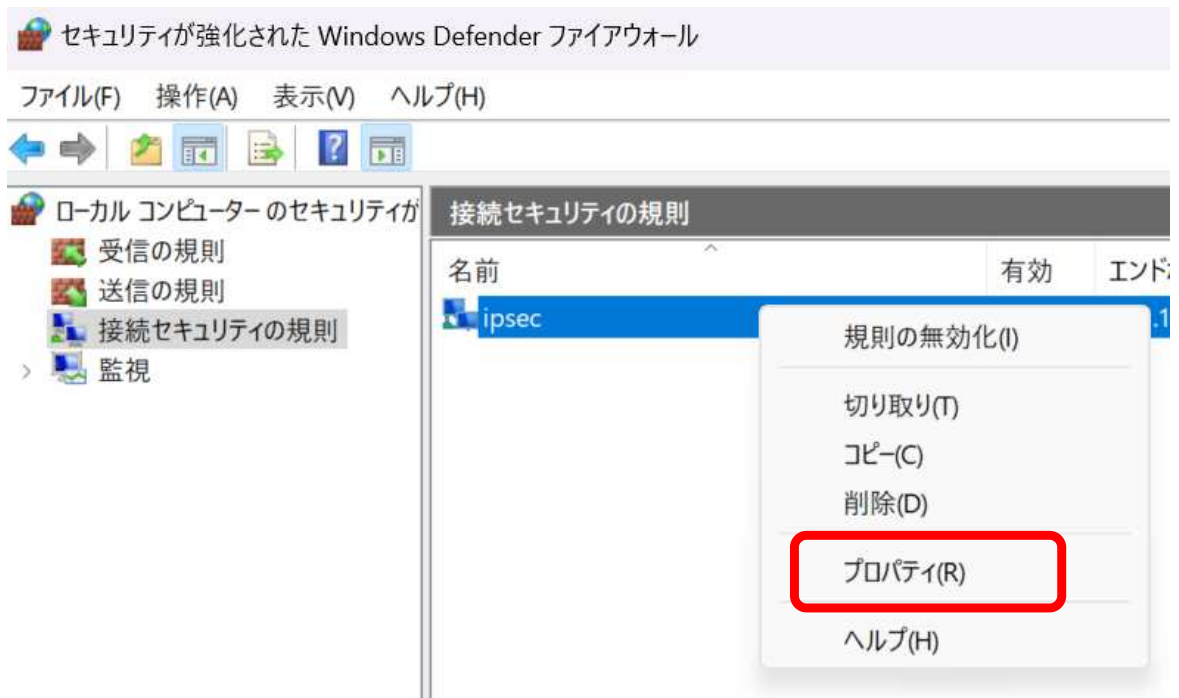


「名前」

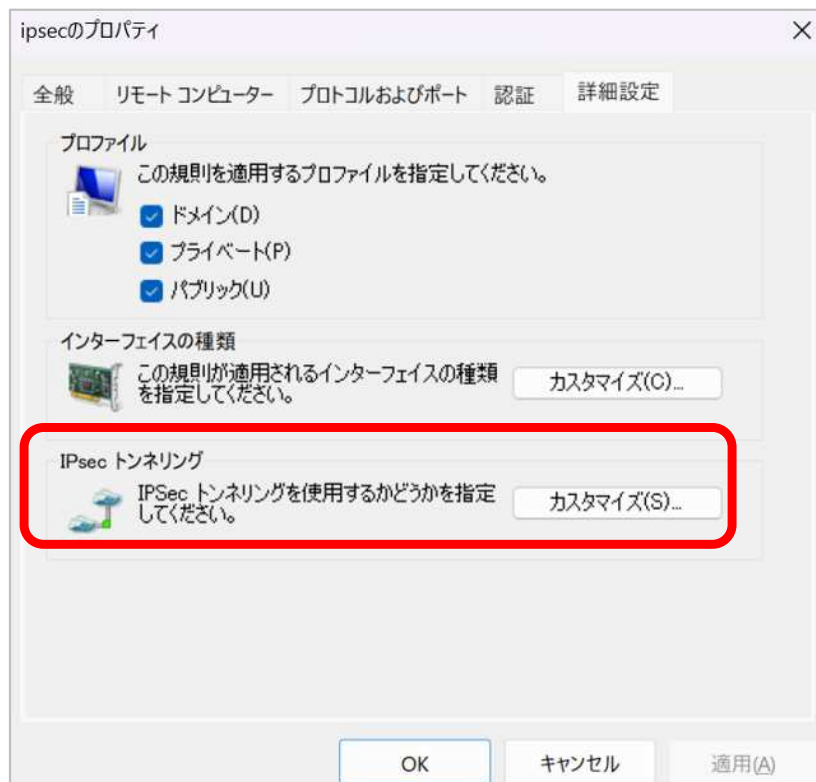
ipsecという名前でセキュリティ規則を追加します。



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。

IPsec トンネリング設定のカスタマイズ

エンドポイント 1 から 2 への間の接続は指定のトンネル エンドポイントを経由します。一般的にトンネル エンドポイントはゲートウェイ サーバーです。

注意: IPsec トンネリングを使用する場合は、認証モードを [受信および送信で必須] または [受信で必須、送信では不要] (ゲートウェイ デバイス用) に設定する必要があります。

IPsec トンネリングを使用する(U)

承認を適用する(A)

IPsec で保護されている接続を除外する(X)

ローカルトンネル エンドポイント (エンドポイント 1 に最も近い):

IPv4(I): 10.1.1.100 編集(E)...

IPv6(P):

リモートトンネル エンドポイント (エンドポイント 2 に最も近い):

IPv4(V): 10.10.1.1 編集(D)...

IPv6(6):

OK キャンセル