

本章では、Windows XPに標準搭載されているVPNクライアント機能の設定方法について、順番に説明 します。

作業の流れ(→6ページ)	Windows XPにおけるVPN設定の作業の流れを
	フロー図で説明します。
WIndows XPの設定(→7ページ)	VPN構築に必要なセキュリティポリシーの設定
	方法について説明します。
動作確認(→19ページ)	セキュリティポリシーを設定したWindows XP
	の動作確認について説明します。

# 作業の流れ

Windows XPのVPNクライアント機能を使用してリモートアクセスVPN環境を構築する場合は、図のような流れで作業を行います。



# Windows XPの設定

リモートアクセスVPN環境を構築するためには、Windows XP(SG 01)側でセキュリティポリシーを設 定しておく必要があります。

## セキュリティポリシーの設定

Windows XPにおけるセキュリティポリシーの設定方法について説明します。

### ローカルセキュリティ設定の起動

ローカルセキュリティ設定を起動します。

[スタート]メニューから[コントロールパネル]→[管理ツール]を選択する。
 管理ツール画面が表示されます。



コントロールパネル画面が「カテゴリの表示」の場合、[パフォーマンスとメンテナンス] →[管理ツール]を選択します。

 「ローカルセキュリティポリシー」をダ ブルクリックする。
 ローカルセキュリティ設定が起動します。



### セキュリティポリシーの作成

セキュリティポリシーを新規に作成します。

「ローカルコンピュータのIPセキュリティポリシー」を選択し、操作メニューから[IPセキュリティポリシーの作成]を選択する。
 IPセキュリティポリシーウイザードが起動します。



2

VPNクライアントの設 定

[次へ]をクリックする。
 IPセキュリティポリシー名画面が表示されます。

P セキュリティ ポリシー ウィザード	?×
	IP セキュリティ ポリシー ウィザードの開始
	このウィザードでは、IP セキュリティポリシーを作成します。特定のコンピュー なたはコンピュータブループ(サブネット)との通信、および特定の種類の IP トラフィックにおける認識信で使用するセキュリティのレベルを指定します。
	統行するには、[次へ]をクリックしてください。
	< 戻る(B) (次へ似)> (キャンセル)

 名前の項目に、管理しやすいよう分かり やすい名前を、また、必要に応じて、説 明の項目にコメントを入力し、[次へ]をク リックする。 セキュリティで保護された通信の要求画

面が表示されます。

(右記の例では名前は「新しいIPセキュリ

ティポリシー」、説明は空白となっています。)

 「既定の応答規則をアクティブにする」 のチェックを外し、[次へ]をクリックする。 IPセキュリティポリシーウィザードの完 了画面が表示されます。

IP セキュリティ ポリシー ウィザード		?×
IP セキュリティ ポリシー名 この IP セキュリティ ポリシーの名前を付け、簡潔な	識明時に追加してください。	
名前( <u>M</u> ):		
新しい IP セキュリティ ポリシー		
見明( <u>D</u> ):		
		<u>^</u>
		<u> </u>
	〈戻る(B) (次へ(N))	キャンセル
- \		



 「プロパティを編集する」のチェックボ ックスのチェックがついているのを確認 し、[完了]をクリックする。 新しいIPセキュリティーポリシーのプロ パティ画面が起動します。



### セキュリティ規則の作成

セキュリティ規則を作成します。

 [規則]タブをクリックし、[追加]をクリッ クする。
 セキュリティの規則ウィザードが起動し、
 IPセキュリティの規則のウィザードの開 始画面が表示されます。

 新しい IP セキュリティ ポリシーのクロバティ
 ア

 規則 全般
 (まかのコンピュータとの通信に適用されるセキュリティの規則)

 IP セキュリティの規則の:
 [IP フィルター覧] フィルタ操作

 IP フィルター覧
 フィルタ操作

 (まかの):
 既定の応答

 Kerberos
 なし

 通知(D):
 編集(E):

 前序:
 (E) 通知ウィザードを使用(W)

 OK
 キャンセル

[次へ]をクリックする。
 トンネル エンドポイント画面が表示されます。



 「この規則ではトンネルを指定しない」のラジオボタンを選択し、[次へ]を クリックする。
 ネットワークの種類画面が表示されます。  「すべてのネットワーク接続」のラジ オボタンを選択し、[次へ]をクリックす る。
 認証方法画面が表示されます。



定

2

 「次の文字列をキー交換(事前共有キ ー)の保護に使う」のラジオボタンを選 択し、SG側でVPNパスの設定時に指定 したパスワード(プリシェアードシーク レット)と同じ鍵の文字列を記し、[次へ] をクリックする。
 IPフィルター覧画面が表示されます。

セキュリティの規則ウィザード				?×
認証方法 複数の認証方法を追加するには、IP セキュリティの規 編集します。	観りウィザードを完了	した後にセキュ	リティの規則を	<u>[</u> ]
次のセキュリティの規則のための最初の認証方法を	設定します			
○ Active Directory 既定値 (Kerberos V5 ブロ)	(D) (אבי			
○ 次の証明機関 (CA) からの証明書を使う( <u>C</u> ):				
			参照( <u>R</u> )	
● 次の文字列をキー交換(事前共有キー)の保護	痩(c(使う( <u>S</u> ):			
password1			~	
	〈 戻る(旦)	(次へ(N))	***	ren 🛛

(右記の例では「password1」と記しています。)

■ ● 鍵の文字列は必ずSG300側でVPNパスの設定時に指定した鍵(パスワード) ■ と同じ文字列を記してください。

なお、パスワードは必ず英数字を組み合わせて、8文字以上500文字以内で入 カします。

#### ●IPフィルタの作成

IPフィルタを新規に作成します。

**13.** [追加]をクリックする。 IPフィルター覧が起動します。

セキュリティの規則ウィザード		?×
IP フィルター覧 このセキュリティの規則を適用する IP	トラフィックの種類で使用する IP フィルター覧を	
次の一覧に適切な IP フィルタがない IP フィルター覧の:	い場合は、 [追加] をクリックして新しい IP フィル!	9を作成してください。
名前	見明	這加(A)
O すべての IOMP トラフィック	このコンピュータとほかのコンピュータ間	
O すべての IP トラフィック	このコンピュータから、ブロードキャスト	編集(E) 育明除(B)
	_ < 戻る(但) ;太へ(t	0>

 14. 名前の項目に、管理しやすいよう分か りやすい名前を、また、必要に応じて、 説明の項目にコメントを入力し、[追加] をクリックする。

IPフィルタウィザードが起動し、新しい IPフィルタウィザードの開始画面が起動 します。

(右記の例では名前は「新しいIPフィル ター覧」、説明は空白となっています。)

IP フィルタ・	一覧	_			?×
	P フィルター覧は複数 ルルを1つの IP フィル!	のフィルタで構成されて() 対にまとめることができます	るので、複数のサブネッ 。	·K IP アドレフ	ヘ、 およびブロト
名前(N):					
新しい IP フ・	ィルター覧				
説明( <u>D</u> ):					近加(A)
				~	編集( <u>E</u> )_
				~	育川『余( <u>R</u> )
フィルタ(S):			I▼	1 追加ウィザ・	-ドを使用( <u>W</u> )
₹5 I	兑明	プロトコル	発信元ポート	宛先ポート	発信
<					>
			OK		キャンセル

15. [次へ]をクリックする。
 IPトラフィックの発信元画面が表示されます。

フィルタ ウィザード	?×
	新しい IP フィルタウィザードの開始 このウィザードで、IP トラフィックにフィルタをかけるのに必要な発信元、宛 先 およびトラフィックの種類に関する情報を提供します。 このウィザードで、著信 IP トラフィックなおよび発信 IP トラフィックの両方に 一致する、ミラービスたフィルタを取ります。 雑誌の発信を示われて読みの「アイン」、一次の IP パケット あるいけおやくの
	異なるとラインラが最後期のアンドメーまする。アンイパメー製を作成 するには、複数のフィルタを追加してください。 続行するにては、「たへ」をクリックしてください。
	< 戻る(日) (天ふ(日)) <b>**ンセル</b>

 発信元アドレスのプルダウンメニュ ーから「このコンピュータのIPアドレス」
 を選択し、[次へ]をクリックする。
 IPトラフィックの宛先画面が表示されます。

フィルタ ワィサード		?×
IP トラフィックの発信元 IP トラフィックの発信元アドレスを指定します。		E.
発信元アドレス( <u>S</u> ):		
このコンピュータの IP アドレス		
	〈 戻る(目) (次へ(N) 〉	キャンセル
フィルタ ウィザード		?×

- 17. 宛先アドレスのプルダウンメニュー から「特定のIPアドレス」を選択し、IP アドレスには、ファイアウォールのIPア ドレスを入力し、[次へ]をクリックする。 IPプロトコルの種類画面が表示されます。 (右記の例では、IPアドレスは 「202.247.5.136」となっています。)
- プロトコルの種類の選択のプルダウ ンメニューから「任意」を選択し、[次へ] をクリックする。
   IPフィルタウィザードの完了画面が表示 されます。

フィルタ ウィザード IP トラフィックの宛先 IP トラフィックの宛先アドレスを指	定します。				?×?
<b>宛先アドレス(型)</b>  特定の IP アドレス IP アドレス(B): サブネット マスク(Q):	202	. 247 . 255	. 5 . 255	• 136 • 255	
			< 戻る(B)	<u> </u>	



 「プロパティを編集する」のチェック ボックスのチェックが外れているのを確 認し、[完了]をクリックする。
 IPフィルター覧画面に戻ります。

ルタ ウィザード	?×
A.	IP フィルタウィザードの完了 IP フィルタウィザードを正しく完了しました。
	すぐに IP フィルタを編集するには、「プロパティを編集する] チェック ボックス をオンにしてから 「完了] をグックしてください。
-7	□ プロパティを編集する(空)
	ウィザードを閉じるには、「完了]をクリックしてください。
	< 戻る(B) 完了 キャンセル

フィルタが追加されていることを確認し、[OK]をクリックする。
 これでIPフィルタが作成されました。
 セキュリティの規則ウィザードに戻ります。

🔲 IP フィル	ター覧				?×
	IP フィルター覧( コルを1つの IP	は複数のフィルタで構成さ フィルタにまとめることがで	られているので、複数のサ ごきます。	ブネット、IP アドレ	ス、およびプロト
名前(N):					
新しい IP	フィルター覧				
説明( <u>D</u> ):				C	追加(A)
				~	編集( <u>E</u> )
				~	削除( <u>R</u> )
フィルタ(S)				☞ 追加ウィザ	ードを使用( <u>W</u> )
35	説明	プロトコル	発信元ポート	宛先ポート	発信
はい		任意	任意	任意	<20
<					>
				ОК	キャンセル

●フィルタ操作の設定 作成したフィルタの操作を設定します。

- 21. 先に作成したフィルタのラジオボタン を選択し、[次へ]をクリックする。 フィルタ操作画面が表示されます。 (右記の例では名前は「新しいIPフィルタ 一覧」となっています。14で入力した名 称が記されています。)
- 22. [追加]をクリックする。
   フィルタ操作ウィザードが起動し、IPセキ ュリティのフィルタ操作ウィザードの開 始画面が起動します。



セキュリティの規則ウィザード	?×
<b>フィルタ抹作</b> このセキュリティ規則のフィルタ操作を選択	lity E
次の一覧に適切なフィル対衆作がない場 い。ウィザードを使ってフィル対衆作を作成 フィル対象作(C):	合は、「追加」をグックして新しいフィル対象作を作成してくださ するには「追加ウィザードを使用」を選んでください。 ▽ 追加ウィザードを使用 \20
名前	IV88
<ul> <li>○ 世キュリティが必要</li> <li>○ 世キュリティを要求(高略可能)</li> <li>○ 許可</li> </ul>	セキュリティで保護されていない通信。 セキュリティで保護されていない通信。 セキュリティで保護されていない IP パ 単原本(2)
	< 戻る(Q) 次へ(Q) キャンセル

23. [次へ]をクリックする。

フィルタ操作名画面が表示されます。

ィルタ操作ウィザード	?×
	IP セキュリティのフィル対象作ウィザードの開始
161	このウィザードでは、新しいフィルタ操作のブロパティを指定できます。
	フィル好衆作でデータを転送するときのセキュリティ要求を設定します。セ キュリティ要求は、フィル対衆作の中のセキュリティ メソッドの一覧で指定 されています。
	コンピュータが同じセキュリティ メソッドを使用している場合のみ、データを 転送できます。雑飯のセキュリティメソッドを使うと、2 つのコンピュータが 同じメソッドを使う可能性が高くなります。
	統行するには、D太へ」をグリックしてください。
	〈戻る(B) (法への) キャンセル

24. 名前の項目に、管理しやすいよう分か りやすい名前を、また、必要に応じて、 説明の項目にコメントを入力し、[次へ] をクリックする。 フィルタ操作の全般オプション画面が表 示されます。 (右記の例では名前は「新しいフィルタ

操作」となっています。)

- 25. 「セキュリティのネゴシエート」のラ ジオボタンを選択し、[次へ]をクリックす る。 IPSecをサポートしないコンピュータと 通信中画面が表示されます。
- 26. 「IPSecをサポートしないコンピュー タとは通信しない」のラジオボタンを選 択し、[次へ]をクリックする。 IPトラフィックセキュリティ画面が表示 されます。





フィルタ操作



2

 27.「暗号化と整合性」のラジオボタンを 選択し、[次へ]をクリックする。
 IPセキュリティフィルタ操作ウィザードの完了画面が表示されます。



IPトラフィックセキュリティ画面では、実際に通信する際に使用する暗号アルゴリズム

 「プロパティを編集する」のチェック ボックスのチェックが外れているのを確 認し、[完了]をクリックする。 セキュリティの規則ウィザードに戻りま す。

マルタ操作ウィザード	?×
11 <del>6</del> 3	IP セキュリティ フィル対象作ウィザードの完了 IP セキュリティ ポリシー ウィザードを正しく完了しました。
	すぐにフィル対象作を編集するには、[プロパティを編集する] チェック ボック スをオンにしてから「売了] をクリックしてください。
	□ プロパティを編集する(2)
	ウィザードを閉じるには、「完了」をクリックしてください。
	< 戻る(B) 完了 キャンセル

- ●セキュリティ規則の作成完了 セキュリティ規則の作成を完了します。
- 29. 先ほど設定したフィルタ操作(24で設定した名前のフィルタ操作)のラジオボタンを選択し、[次へ]をクリックする。新しい規則ウィザードの完了画面が表示されます。 (右記の例では名前が「新しいフィルタ

操作」のラジオボタンを選択します。)

 「プロパティを編集する」のチェック ボックスのチェックを外し、[完了]をクリ ックする。
 新しいIPセキュリティポリシーのプロパ ティに戻ります。





鍵交換の設定

SG300とWindows XP間で行われる鍵交換の際に必要となる項目を設定します。

 Pセキュリティの規則のIPフィルター 覧から先ほど設定したフィルタのチェッ クボックスをチェックし、[編集]をクリッ クする。
 規則の編集のプロパティが起動します。
 (右記の例では「新しいIPフィルター覧」 をチェックします。)

 新しい IP セキュリティ ポリシーのプロバティ
 ? ×

 規則
 金岐

 (ほかのコンピュータとの通信に適用されるセキュリティの規則)

 IP セキュリティの規則(Φ):

 IP フィルター覧

 フィルター覧

 フィルター覧

 ブイルター覧

 ブイルター覧

 ブイルクスポイ

 新しい IP フィルター覧

 フィルター覧

 マルター覧

 ブイルクスポインジャンクシー

 第し、アノルターを

 「新しい IP フィルター 覧

 フィルターを

 「新しい IP フィルター 覧

 「新しい IP フィルター 覧

 「新しい IP フィルター 覧

 「新しい IP フィルター 覧

 「新しい IP フィルター 読んのに

 「新しい IP フィルター 覧

 「新しい IP フィルター 覧

 「「新しい IP フィルター 覧

 「「新しい IP フィルター 覧

 「「新しい IP フィルター 覧

 「「新しい IP フィルター 覧

 「「「「」」」

 「「」」

 「「」」

 「「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

 「」」

32. [フィルタ操作]タブをクリックする。

規則の編集のフロパティ	?×				
IP フィルター覧 フィルタ操作 認証方法	トンネルの設定 接続の種類				
選択した IP フィルター覧は、この規則で影響を受けるネットワークトラフィ					
→ ックを指定します。					
2前	1988				
O すべての ICMP トラフィック	このコンピュータとほかのコンピュータ間の				
○ すべての IP トラフィック	このコンピュータから、ブロードキャスト、マ				
●新しい IP フィルター覧					
追加( <u>D</u> ) 編集( <u>E</u> )	削除( <u>R</u> )				
01	K キャンセル 適用(品)				

33. 先ほど設定したフィルタ操作(24で設定した名称のフィルタ操作)のラジオボタンを選択し、[編集]をクリックする。新しいフィルタ操作のプロパティが起動します。

(右記の例では「新しいフィルタ操作」 となっています。)

規則の編集のフロパティ	?×
IP フィルター覧 フィルタ操作 認証方法	トンネルの設定 接続の種類
選択したフィルタ操作は、こ トラフィックに対してネゴシュー がセキュリティで「保護される」	の規則でセキュリティで保護されたネットワーク トできるかどうか、およびどのようにトラフィック かを指定します。
フィルタ操作( <u>F</u> ):	
名前	説明
○セキュリティが必要	セキュリティで保護されていない通信を
○ セキュリティを要求(省略可能)	セキュリティで保護されていない通信を
〇許可	セキュリティで保護されていない IP パケ
⊙新しいフィルタ操作	
追加( <u>D</u> ) 編集(E)	削除(2) 🔽 追加ウィザードを使用(₩)
0	K キャンセル 道用(A)

34. [セキュリティメソッド]タブの「セッションキーのPFS (Perfect Forward Secrecy)」のチェックボックスをチェックし、[OK]をクリックする。 規則の編集のプロパティに戻ります。

新しいフィルタ掛	ホ作のプロパテ	1		?×
セキュリティ メン:	)ド 全般			
○ 許可(M) ○ ブロック(L) ○ セキュリティ	のネゴシェート()	D:		
セキュリティ メン 種類 A	ッドの優先順位 H 整合性	ī( <u>S</u> ): ESP 機密性	ESP 整合性	追加(0)
暗号化 <	なし>	3DES	SHA1	編集( <u>E</u> )
				肖明余( <u>R</u> )
				上へ移動(U)
<			>	下八移動(Q)
<ul> <li>マ セキュリティ</li> <li>□ IPSec に対</li> <li>マ セッション キ</li> </ul>	で保護されてい。 I応していないコ 〒一の PFS (Per	ない通信を受け付け ンピュータとセキュリテ fect Forward Secr	るが、常に IPSec ፣ ィで保護されていな ecy)( <u>P)</u>	を使って応答型 い通信を許可( <u>W</u> )
		OK	*+>>t	2ル 適用(A)

35. [閉じる]をクリックする。
 新しいIPセキュリティポリシーのプロパティに戻ります。

規則の編集のフロパティ	?×
IP フィルター覧 フィルタ操作 認証方法	トンネルの設定 接続の種類
選択したフィル対象作は、ここ 、 ドラフィックに対してネゴシエー がセキュリティで保護されるが	の規則でセキュリティで保護されたネットワーク トできるかどうか、およびどのようにトラフィック かを指定します。
フィルタ操作( <u>E</u> ):	
名前	説明
O セキュリティが必要	セキュリティで保護されていない通信を
○ セキュリティを要求(省略可能)	セキュリティで保護されていない通信を
O 許可	セキュリティで保護されていない IP パケ
⊙ 新しいフィルタ操作	
追加(D)	削除(円) ▼ 追加ウィザードを使用(W)
	る キャンセル 適用(点)

36. [全般]タブをクリックし、「次の設定 を使用してキー交換を行う」の[詳細設定] をクリックする。 キー交換の設定が起動します。

新しい IP セキュリティ ポリシーのフロパティ	?×
規則全般	
○ IP セキュリティ ポリシーの全般プロパティ	
名前(1):	
新しい IP セキュリティ ポリシー	
[覚8月( <u>D</u> ):	
ポリシーの変更を確認する間隔(©): 180 分 次の設定を使用してキー交換を行う: 詳編設定( <u>V</u> )	
開じる	キャンセル

**37.** 「マスタキーのPFS (Perfect

Forward Secrecy)」のチェックボック スをチェックし、「IDの保護に用いるセ キュリティメソッド」の[メソッド]をクリ ックする。 キー交換のセキュリティメソッドが起動

します。

キー交換の設定	?×
▼ マスタキーの 新しいキーを認証	PFS (Perfect Forward Secrecy)( <u>P)</u> して生成する間隔( <u>A</u> ):
480	分
新しいキーを認証	して生成する間隔(凹):
1	セッション
ID の保護に用いる	5セキュリティ メソッド:
メソッド( <u>M</u> )	
Windows XP イン Jointly develope	ターネット キー交換(IKE) d by Microsoft and Cisco Systems, Inc.
	0K 7777/

認証のときに ID を保護するセキュリティ メソッドを指定します。

Diffie-He

中(2) 中(2) 低(1) 低(1)

>

OK

PFSは、鍵を更新する際、以前の鍵から新しい鍵を推測できないようにする機能です。 ヒント

è

種類

IKE IKE IKE IKE

<

キー交換のセキュリティ メソッド

セキュリティ メソッドの優先順位(M):

暗号化 整合性 3DES SHA1 3DES MD5 DES SHA1 DES MD5

38. 下記のように設定されていることを確 認し、[OK]をクリックする。

種類	暗号化	整合性	Diffie-	
			Hellman	
IKE	3DES	SHA1	中 (2)	
IKE	3DES	MD5	中 (2)	
IKE	DES	SHA1	低(1)	
IKE	DES	MD5	低(1)	

新しいIPセキュリティポリシーのプロパ

**39.** [OK]をクリックする。

ティに戻ります。

キー交換の設定画面に戻ります。

▼ マスタキーの PI 新しいキーを認証し	-S (Perfect For て生成する間隔	ward Secrecy) (A):	( <u>P</u> )	
480	分	-		
。 新しいキーを認証し	て生成する間隔			
1	セッション			
ID の保護に用いる・	セキュリティ メソッ	r:		
<u></u>				

 $\mathbf{2X}$ 

追加(<u>D</u>)...

編集(E)..

削除(<u>R</u>) 上へ移動(し 下へ移動(⊙)

キャンセル

480	分	_		
所しいキーを読	騙して生成する	5間隔(山):		
1	セッション			
D の保護に用	いるセキュリティ	メソッド		
🗇 እንምዚመን				

## セキュリティポリシーの設定完了

セキュリティポリシーの設定を完了します。

- 40. [閉じる]をクリックする。
- **41.** 以上で、WindowsXPにおけるセキュ リティポリシーの設定は完了しました。

新しい IP セキュリティ ポリシーのプロパティ	?×
規則全般	
● IP セキュリティ ポリシーの全般プロパティ	
名前(N):	
新しい IP セキュリティ ポリシー	
説明( <u>D</u> ):	
	~
ポリシーの変更を確認する間隔(©): 180 分	
次の設定を使用してキー交換を行う:	
開じる	キャンセル

# 動作確認

セキュリティポリシーを設定したWindows XPの動作確認方法について説明します。

- ●ユーザ認証
- ●セキュリティポリシーの有効化
- ●ブラウザによる接続確認

## ユーザ認証

ユーザ認証を行います。

- Internet Explorer等のブラウザを起動し、SG300側で設定した認証ページ (https://202.247.5.136)にアクセスする。 ユーザログイン画面が表示されます。
- SG300側で設定したユーザID (user\_tokyo)とパスワードを入力し、 [ログイン]をクリックする。 ログインに成功すると、グループルール で設定したポリシーが追加され、VPNパ スが有効になります。

🚰 ユーザログイ	ン - Micros	soft Interne	t Explorer				_0	×	
] ファイル(E)	編集(E)	表示⊙	お気に入り( <u>A</u> )	ツール①	ヘルプ(出	)   アドレ	2@ 🖉 💌 🖉		
ユーザロダイン									
ユーザログ・	í۷								
		ーザログイ				_			
	,	ユーサル イスワード							
			1912	バスワード	変更				
  創ページが表	示されました	:				白健化	ントラネット	<b>-</b> //	

 ユーザログイン絵果 - Microsoft Internet Explorer
 ニロメ

 ファイル(E) 編集(E) 表示(W) お気に入り(A) ツール(D) ヘルグ(H) アドレス(D) (A) マーマ
 アドレス(D) (A) マーマ

 ユーザログイン結果
 ニ

 ユーザログイン結果
 エ

 アビュニーザのログインにお助しました。
 利用できちサービスが追加されました。

 シーザログイン
 エーザロワイン

 ユーザログイン
 エーザログイン

 シーザログイン
 コーザログイン

 ユーザログイン
 ロッチョーレージ

 コーザログインに戻る
 エーザログインに戻る

 ビージが表示されました
 エージログインに戻る



さい。

SG300側の設定の詳細は、「リモートアクセスVPNの設定(サーバ編)」を参照してくだ

2

## セキュリティポリシーの有効化

設定したセキュリティポリシーを有効にします。

 ローカルセキュリティ設定を起動し、「セキュリティポリシーの設定」で設定したセキュリティポリシーを選択した後、[操作]メニューから[割り当て]を選択する。 (右記の例では「新しいIPセキュリティポリシー」となっています。)



 ポリシーの割り当ての項目に「はい」と 表示されます。選択したセキュリティポ リシーが、割り当てられたことを画面上 で、確認してください。

▶ ローカル セキュリティ読定				- BX							
ファイル(E) 操作(金) 表示(V) ヘルブ(E)											
←→ 白 ×27時 2 道士 1 1											
<ul> <li>● 1+3/7-64時度</li> <li>● 2+5/7-48/2</li> <li>● 2+5/7-48/2</li> <li>● 2+5/7-48/2</li> <li>● 3+7-7248/2</li> <li>● 3+7-7248/2</li> <li>● 3+7-7248/2</li> <li>● 3-76-724-5-80月 使生活分子(約5)</li> </ul>	名称 - (2015年3月1日) 2017/27-16年3月27日2日 2019年7月1日 2019年7月1日 2019年7月1日 2019年7月1日 2019年7日 2019 2019 2019 2019 2019 2019 2019 2019	1899 単次には 第4750 日 トラントウス & Ar. 第4750 日 トラントウス & Ar. 第4750 日 トラントウス & Ar.	2 <u>8</u> (00-50) 5(0) 5(0) 5(0) 5(0) 5(0)								

3. 以上で、登録したセキュリティポリシーが有効になりました。

## ブラウザによる接続確認

SG300とWindows XP間で、VPNによる接続が行えるかどうか確認します。

 Internet Explorer等のブラウザを起動し、SG300の内側のWebサーバ (http://202.247.5.136/)に接続可能かどうか確認してください。



接続ができなかった場合は、VPN通信が行われていません。再度、これまでの各設定を見 直してください。 設定を見直しても改善しない場合は、SG300側の設定が正しく行われているか、管理者に

確認してください。