PPTP利用の際のF-Secureの設定

リモートアクセスでPPTPを利用する場合、接続時にエラー721が表示されることがあります。 その場合、F-SecureのGREのポートを解放する必要があります。

① タスクバーにあるF-Secureのアイコンをクリックし、管理画面を開きます。



② 左メニューのインターネット防御をクリックします。

F-Secure PSB	Workstation Security	171	
F-Secure F	TOTECTION SERVICE		
💮 т-2	インターネット防御	オフィス	変更
111222181	🗳 ファイアウォール	オフィス	<u>変更</u>
17月2日 ひェア時間	🥝 アプリケーション制御	プロンプトを表示 / プロン	ヴト <u>変更</u>
(2) インターネット	📙 🔮 侵入防止	ブロックしてログ	変更
P 5184	🕝 ダイヤルアップ制御	有効	無効にする
() スパム 制御	 登録アプリ数 [許可/拒否] 	0	<u>変更</u>
	 最近の警告一覧 	14:26 から:1件	表示
自動更新	▶ 最近の警告	16:19	言羊糸田
			ポートを開く
			∎¥śm
-sicuri			armann
V	日本エフ・セキュアホームページ	最新ウィルス情報 製品さ	サポートページ
NUTH			閉じる

③ ファイアーウォールをクリックします。

7 詳細設定			
F-Secure Prote	ection Service		-
 ■ ウィルスとスパイウェア防御 ■ インターネット防御 ■ ファイアウォール 	インターネット防御 ステータス インターネット防御	<i>オフィ</i> ス	
アプリケーション制御 侵入防止 ダイヤルアップ制御	○ 詳細	有如	無効にする
ーロギング	アプリケーション制御	有効	無効にする
国 スパム制御	侵入防止:	有効	無効にする
国目動更新	ダイヤルアップ制御	有効	無効にする

④ ルールタブの下部にある追加をクリックします。

 ● ウィルスとスパイウェア防御 ● インターネット防御 ● ファイアウォール ● アプリケーション制御 ● 侵入防止 ● ダイヤルアップ制御 	(ファイアウ) (ファイアウ)	ォール ールを有効にする(F)			
	ルール	サービス	設定	アクティ	1274
	有効	名前		タイプ	ሀモート ホスト
 □-ロギング ③ スパム制御 ● 自動更新 ④ その他 		Outbound TCP and L Commonly needed IC pptp ルールはここに近知た Deny inbound compu Block remote access Deny rest	IDP traffic MP messages れます ter browsing and fil. to vulnerable local.	× × ×	0000/0 0000/0 0000/0 0000/0 0000/0
	1 Strong	<u> </u>		2570(名)	AUP#(B)

⑤ 名前には、使用目的が分かる名称を入力し、タイプが"許可"が選択されていることを確認し、 次へをクリックします。

ルールを使用し	て、ネットワーク トラフィックを許可また	は拒否できます。
名前:	PPTP_starTAINS	
オプ:	●許可(A)	
	○拒否回	
- 8760	→*#2/50-5/-のひり、りま/ま円400	

⑥ デフォルトのまま、次へをクリックします。



⑦ GRE / Cisco Generic Routing Encapsulation Tunnelを選択します。(MS PPTPと同じPort47を利用しているため)



⑧ 端末のアイコンと地球のアイコンの間の?を押下すると双方向の矢印が表示されるので その状態で次へをクリックします。

i 規ルール(ールのサービスを	の追加 ここで、 選択してください。	ステップ 3/
サービスの方向	を変更するには [方向] をクリックします。	
方向	サービス 🔺	~
	ESP / Encapsulation Security Payload protoco F-Secure updates F-Secure VPN+ default web output port Finger FTP / File Transfer Protocol, active mode FTP / File Transfer Protocol, only in passive r GIBE - Trojan GirlFriend - Trojan	ol mode
	GRE / Cisco Generic Routing Encapsulation Tr Hack a tack - Trojan(TCP)	unnel 💌

⑨ デフォルトのまま次へをクリックします。

警告の表示とログ 示されます。	方法を設定します。[警告のテキスト] はログおよびポップアップに表
警告のタイプ:	 ● 警告なし(A) ○ ログ(L) ○ ログとボッブアップ(G)
警告のテキスト:	PPTP_starTAINS

1 設定が下図のようになっていることを確認し完了をクリックします。

「規ルールの追 規ルールの内容を確認	1 70 2してください。	ステップ 5/5
名前: タイプ:	PPTP_starTAINS 許可(A)	
リモートアドレス:	0.0.0.0/0	
サービス:	サービス 🛋	方向
	GRE / Cisco Generic Rou	tin 両方
警告:	警告なし(A)	

① 最初に入力した名前のルールができていることを確認しOKをクリックします。

F-Secure Protect	ion Serv (ファイアウ	ice ォール			15
 インターネット防御 ファイアウォール 	☑ ファイアウォ	ールを有効にする(E)			
アプリケーション制御	ルール	サービス	設定	アクティ	パディ
 - 侵入防止 - ダイヤルアップ制御 - ロギング ■ スパム制御 ● 自動更新 ● その他 	有効	名前		タイプ	リモート ホスト
		Active F1P Outbound TCP and UD Commonly needed ICM PPTP_starTAINS ルールはここに追加され Deny inbound compute Block remote access t Deny rest	P traffic P messages 3 J r browsing and fil o vulnerable local	> > > > × × ×	0.000/0 0.000/0 0.000/0 0.000/0 0.000/0 0.000/0
	I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			<u>追加(A)</u>	. 肖·滕余(B)

以上で、F-Secureの設定は完了です。