FUJITSU Security Solution アイソレーションゲ ートウェイサービス ルーターパックの導入・運用

第3版

2021年8月

古河電気工業株式会社

目次

1	はし	じめに	3
2	FU	JJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックとは	3
3	サー	ービスにおける FITELnet の役割	3
4	FI	TELnet 構成例とコンフィグ	4
5	FI	TELnet へのクライアント PC の接続	6
6	ГĄ	分離・無害化サービス」を通したインターネットアクセス	7
7	PA	C ファイル管理機能	10
7	.1	PAC ファイル管理ページへのアクセス	10
7	.2	パスワード変更	11
7	.3	初期 PAC ファイル	12
7	.4	「分離・無害化サービス」を経由しないドメイン/IP アドレスの追加・削除	13
7	.5	適用	19
7	.6	バックアップ	21
7	.7	リストア	23
7	.8	削除	27
7	.9	送信先プロキシ変更	28
7	.10	サポートブラウザ	31
8	注意	意事項	31
付銀	łА	LAN 側ネットワークをお客様環境に合わせて変更する方法	32
付銀	B	Windows10に CA 証明書をインストールする方法	34
付錄	кC	リモートアクセス機能	38
С	-1	ルータ設定	38
С	-2	クライアント PC 設定	40

商標について

- ・Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- ・本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。
- ・本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- ・本書は、改善のために予告なしに変更することがあります。
- ・本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその 責を負いません。

©2021 Furukawa Electric Co., Ltd

1 はじめに

本書では、FITELnet F70M/F71M/F220M/F221M(以下、FITELnet)を利用した、「FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックの導入・運用」について記載します。

2 FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックと は

本サービスは、WEB アイソレーション技術(Menlo Security)とルータ製品(FITELnet)を組み合わせてブラ ウザ経由のマルウェア感染を防ぐ、安心・手軽・安価にお使いいただけるサービスです。 全ての Web サイトのコンテンツを、マルウェアの有無に関わらず仮想環境上でクリーンな情報に変換するた め、安心安全な Web アクセスが可能です。

3 サービスにおけるFITELnetの役割

図1に FITELnet を使ったサービスイメージを示します。クライアント PC を FITELnet に接続すると、 クライアント PC は、FITELnet から DHCP で配布されるアドレス情報をもとに FITELnet に置かれている プロキシ設定情報 (PAC ファイル)を取得します。このプロキシ設定情報に「分離・無害化サービス」の宛先 情報が記載されており、その情報から、クライアント PC はインターネットアクセスをする際に「分離・無害 化サービス」を通してアクセスします。



図 1 FITELnet を使ったサービスイメージ図

4 FITELnet構成例とコンフィグ

FITELnet を使った構成例を図 2 に示します。インターネット回線には Giga2/1 ポート(100.1.1.2)を通して 接続され、社内ネットワーク(192.168.1.0/24)には Giga1/1 ポートを通して接続されています。本サービスは コンテナ機能を使用しており、プロキシ設定情報はコンテナ環境に置かれています。コンテナには 192.168.1.254 のアドレスが設定されており、Giga1/1 ポートを通してアクセスします。FITELnet の DHCP サーバ機能により、クライアント PC に IP アドレス等の払い出しが行われます。このタイミングでプロキシ 設定情報のロケーション情報(URL)も一緒に通知されるため、クライアント PC はそのロケーション情報をも とにプロキシ設定情報を取得することが可能となります。Giga2/1 では NAT 変換を行い、パケットの送信元 アドレス (LAN のアドレス)を Giga2/1 のインタフェースのアドレスに変換しています。

※Giga1/1(192.168.1.1)とコンテナアドレス(192.168.1.254)は工場出荷時にデフォルトで設定されています。 Giga2/1 は工場出荷時には設定されておらず、お客様の環境に合わせて設定していただく必要があります。 工場出荷時にデフォルトで設定された LAN 側アドレスをお客様環境に合わせて変更したい場合には、文 末の付録 A を参照下さい。



図2 構成図

上記ネットワーク構成に合わせた FITELnet のコンフィグを以下に示します。

container enable	←コンテナのサービスを有効にする設定
container device disk /mnt/pac_mainte drive uid 101 gid	101
!	
container configuration	←コンテナの設定
!	
interface 1	コンテナのinterface1をルータの
bridge-group 1	←bridge-group1(giga1/1)に紐づける設定
ip address 192.168.1.254 255.255.255.0	←コンテナアドレスの設定
ip gateway 192.168.1.1	←コンテナのgetewayを設定
exit	

! exit I ←学習フィルタ設定 access-list 111 deny ip any any access-list 121 spi ip any any ←学習フィルタ設定 ←コンテナアドレスにホスト名 ip host fiteInet-container.fnsc.co.jp 192.168.1.254 (fiteInet-container.fnsc.co.jp)登録 ip route 0.0.0.0 0.0.0.0 100.1.1.1 ←デフォルトルートを設定 ip name-server 127.0.0.1 ip dhcp server-profile DHCP SERVER PROF ←DHCPサーバ機能のプロファイル address 192.168.1.2 192.168.1.101 ←DHCP払い出しアドレスレンジ lease-time 3600 ←払い出し情報のリース時間(秒) dns 192.168.1.1 gateway 192,168,1,1 option 252 ascii http://fiteInet-container.fnsc.co.jp/pac/web_security.pac ↑ PACファイル置き場情報 exit ip nat list 1 192.168.1.0 0.0.0.255 ←192.168.1.0/24 を list 1 と定義 hostname FITELnet interface GigaEthernet 1/1 vlan-id 1 bridge-group 1 channel-group 1 container-use exit interface GigaEthernet 2/1 vlan-id 21 bridge-group 21 channel-group 21 ip access-group 111 in ←WAN側からのアタックを防ぐための 学習フィルタ設定 ip access-group 121 out exit interface Port-channel 1 ←giga1/1にDHCPサーバ機能を設定 ip dhcp service server ip dhcp server-profile DHCP_SERVER_PROF ←DHCPサーバ機能のプロファイル名を指定 ip address 192.168.1.1 255.255.255.0 link-state always-up exit interface Port-channel 21 ip address 100.1.1.2 255.255.255.0 ←list 1に含まれる送信元アドレスを ip nat inside source list 1 interface exit インタフェースのアドレスにNAT変換する dns-server ip enable L ←お客様環境に合わせてDNSサーバを指定 proxydns domain 1 any * any static x.x.x.x して下さい(x.x.x.x の部分) end

5 FITELnetへのクライアントPCの接続

※本手順実施前に、「分離・無害化サービス」のアカウントの取得と本サービスから提供される CA 証明書の インストールを行ってください。CA 証明書のインストール方法については、文末の付録 B を参照下さい。

前述のコンフィグが設定された FITELnet にクライアント PC を接続するにあたって、クライアント PC の 接続ポートのネットワーク設定を"自動(DHCP)"に設定します。Windows10 を例に取ると、下図のインター ネットプロトコル設定において、"IP アドレスを自動的に取得する"と"DNS サーバーのアドレスを自動的に 取得する"を選択した状態になります。

インターネット プロトコル バージョン 4 (TCP/IPv4)	のプロパティ	×
全般(代替の構成		
ネットワークでこの機能がサポートされている場 きます。サポートされていない場合は、ネットワ・ ください。	合は、IP 設定を自動的に取得することが - ク管理者に適切な IP 設定を問い合わせ	е tt
● IP アドレスを自動的に取得する(O)		
○ 次の IP アドレスを使う(S):		
IP アドレス(I):	· · · · ·	
サプネット マスク(U):		
デフォルト ゲートウェイ(D):		
● DNS サーバーのアドレスを自動的に取得	きする(B)	
──○ 次の DNS サーバーのアドレスを使う(E):		
優先 DNS サーバー(P):		
代替 DNS サーバー(A):		
○終了時に設定を検証する(L)	詳細設定(V)	
	OK ++>>t	JV -

また、プロキシ設定において、"設定を自動的に検出する"をオンにして下さい。

← 設定	- 🗆	\times
命 ホーム	プロキシ	
設定の検索の	自動プロキシ セットアップ	
ネットワークとインターネット	イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。	
⊕ 状態	設定を自動的に検出する	
記 1-サネット	オン セットアップ スクリプトを使う	
ิติ 9้าาขาว	● ^{オフ}	
% VPN	スクリプトのアドレス	
◎ データ使用状況	12.77	
⊕ プロキシ	µK 17	
	手動プロキシ セットアップ	
	イーサネットまたは Wi-Fi 接続にプロキシ サーバーを使います。これらの設定は、VPN 接続には適用されません。	

上記設定の後、クライアント PC を FITELnet の giga1/1 ポートのネットワークに接続します。

6 「分離・無害化サービス」を通したインターネットアクセス

次に、接続したクライアント PC から「分離・無害化サービス」を通してインターネットへアクセスします。 クライアント PC 上でウェブブラウザ(例では Google Chrome を使用)を立ち上げます。URL に試し に"www.furukawa.co.jp"を入力して古河電工のサイトへアクセスしようとすると、下記のような「分離・無 害化サービス」の認証画面が表示されます。Serial No.に契約番号、Email に受信可能なメールアドレスを 入力し、『Login』ボタンを押します。

Fujitsu App by Menlo Security ×	+		•	- 🗆 ×
← → C 🌲 fujitsu.menlosecurit	ty.com/login		\$	🗞 🗰 🔁 🗄
FUĴĨTSU				
	Login			
	Serial No.	Serial Number		
		Fujitsu device serial number		
	Email	Email Address		
		Corporate or business email address		
		◆〕 Login		
		© 2020 Menlo Security, Inc.		

6桁のコードを入力する画面が表示されます。

Fujitsu App by Menlo Security ×	+	0	—		×
\leftarrow \rightarrow C \bullet fujitsu.menlosecur	ity.com/login	☆	@ <u>.</u>	* 0	:
FUĴĨTSU					
	Verification Code				
	We've sent an email to with a verification code. Please enter that below.				
	6-Digit 000000 2 Code				
	✓ Confirm				
	© 2020 Menlo Security, Inc.				

記入したメールアドレス宛にメーカより 6 桁の数字が送付されます。メールアドレスに記載されている 6 桁の数字を前述のコード入力画面に入力し、『Confirm』ボタンを押します。



認証が完了しホームページが表示されます。URL 横の鍵マークをクリックします。次に、表示された情報の中で"証明書"を選択しクリックします。



下記のような証明書情報が表示され、発行者が"Menlo Security Intermediate CA"になっていることが確認 でき、「分離・無害化サービス」を通して表示されていることがわかります。

🔲 証	E明書			Х
全彤	设 詳細 証明(カパス		
	証明書の情	報		
	この証明書の目的:			
	 リモート コンビ 	ユーターの ID を保証する		
	 リモートコンビ 	ューターに ID を証明する		
	発行先:	*.furukawa.co.jp		
	発行者:	Menlo Security Intermedia	te CA	
	有効 期間 20	20/05/ 07 から 2021/06/10		
			発行者のステートメント(S)	
			ОК	

7 PACファイル管理機能

「分離・無害化サービス」を経由させないサイトへのアクセスがある場合は、FITELnet 上の PAC ファイルを編集して、特定のホスト・IP アドレス宛に対して「分離・無害化サービス」を経由させず直接通信させることが可能です。

PAC ファイルの編集は、クライアント PC から FITELnet の PAC ファイル管理ページへアクセスして行います。

以降、PAC ファイル管理機能の利用方法についてご説明します。

7.1 PACファイル管理ページへのアクセス

PAC ファイル管理ページにアクセスするために、クライアント PC 上でブラウザを開き、URL に" http://fitelnet-container.fnsc.co.jp/cgi-bin/pac_mainte/index.cgi"を入力します。

下記のようなログイン画面が表示されるので、ユーザー名とパスワードに"admin"を入力し『ログイン』ボ タンを押してログインします。

S fiteInet-container.fnsc.co.jp/cgi-b	× +	• - • ×
\leftrightarrow \rightarrow C (i) fiteInet-conta	iner.fnsc.co.jp/cgi-bin/pac_mainte/index.cgi	☆ 🖰 :
	ログイン http://fiteInet-container.fnsc.co.jp このサイトへの接続ではプライバシーが保護されません ユーザー名 パスワード ログイン キャンセル	

次のような PAC ファイル管理メインページが表示されます。

PACファイル管理ページ				
PACファイルを選択してください(更新順) menlo.pac イ				
編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。			
削除	選択したPACファイルを削除します。			
適用	選択したPACファイルを適用します。 適用中のPACファイル:menlo.pac			
バックアップ リストア	選択したPACファイルをバックアップ/リストアします。			
パスワード変更	ログインパスワードを変更します。 パスワードの変更をおすすめします。			

7.2 パスワード変更

初期パスワードを変更する場合は、『パスワード変更』ボタンを押し、新しいパスワードを設定して下さい。 パスワードは 8~12 文字の英数記号になります。

PACファイル管理ページ	
パスワ-	-ド設定
新しいパスワード [8 新しいパスワード(確認) [3~12文字の英数記号
設定	戻る

7.3 初期PACファイル

PAC ファイル管理メインページにおいて、上方のウインドウで編集する PAC ファイルを選択します。右端の \ をクリックすると初期の PAC ファイルがプルダウン表示されます。



初期の PAC ファイルは、下記の2種類存在します。

PAC ファイル名	説明
	「分離・無害化サービス」を使用するためにデフォ
menio.pac	ルトで用意された PAC ファイル
	「分離・無害化サービス」を使用しない設定の PAC
diment we a	ファイル
direct.pac	※全てのサイトに、「分離・無害化サービス」を経
	由せず直接アクセスする場合にご使用ください。

7.4 「分離・無害化サービス」を経由しないドメイン/IPアドレスの追加・削除

「分離・無害化サービス」を経由せず直接通信させるドメイン、IPアドレスを追加します。 PACファイル管理メインページにおいて"menlo.pac"を選択し、『編集』ボタンを押します。 ※"direct.pac"への追加・削除の操作は行うことができません。



『ドメイン/IPアドレス追加・削除』ボタンを押して先へ進みます。

PACファイル管理ページ				
編集内容を選択してください。 ここをクリックします	1			
ドメイン/IPアドレス 追加・削除 任意のドメイン/IPアドレスを追加・削除します。				
送信先プロキシ変更 送信先プロキシを変更します。				
戻る				

ドメインを追加する場合は、『ドメイン』を選択します。

PACファイル	管理ページ
	ドメイン/IPアドレスを追加・削除してください。
	ドメイン IPアドレス
	ドメイン 追加
	ドメイン
	次へ 戻る

下のウインドウに追加したいドメインを記入(例では"example.com"を記入)し『追加』ボタンを押します。

PACファイル管理ページ			
	ドメイン/IPアドレスを	5追加・削除してください。	
	ドメイン	IPアドレス	
	example.com	追加	
	ドメイン		
	次へ	戻る	

追加したドメインが表示されます。※右端の『削除』ボタンを押すことで削除することができます。

PACファイル管理ページ				
ドメイン/IPアドレスを減	〕加・削除してください。			
ドメイン	IPアドレス			
example.com	追加			
ドメイン				
example.com	削除			
次へ	庆合			

IP アドレスを追加したい場合は、『IP アドレス』を選択します。

PACファイ	イル管理ページ
	ドメイン/IPアドレスを追加・削除してください。
	ドメイン IPアドレス
	IPアドレス サブネットマスク 追加
	IPアドレス サブネットマスク
	次へ 戻る

下のウインドウに追加したい IP アドレスとサブネットマスクを入力(例では"192.0.2.0/255.255.255.0"を入 力)し『追加』ボタンを押します。

PACファイ	ル管理ページ	
	ドメイン/IPアドレスを	追加・削除してください。
	ドメイン	IPアドレス
	192.0.2.0	5.255.0 追加
	IPアドレス サブネ	ネットマスク
	次へ	戻る

追加した IP アドレスが表示されます。※右端の『削除』ボタンを押すことで削除することができます。

PACフ ァ	アイル管理ページ		
	ドメイン/IPア	ドレスを追加・削除してください。	
	ドメイン	IPアドレス	
	192.0.2.0	255.255.255.0 追加	
	IPアドレス	サブネットマスク	
	192.0.2.0	255.255.255.0 削除	
		欠へ 戻る	

ドメインおよび IP アドレスの追加が完了したら、追加した情報を保存するために、下の『次へ』ボタンを 押します。

PACファイル	を理ページ		
	ドメイン	/IPアドレスを追加・削除	휷してください。
	ドメイン		IPアドレス
1!	92.0.2.0	255.255.255.0	追加
	IPアドレス	サブネットマスク	7
	192.0.2.0	255.255.255.0	削除
		ここを 定る	クリックします 3

追加した情報が書き込まれた PAC ファイルが表示されます。右端のスクロールバーを一番下に持っていく と、"F220-M user defined domains"の下に追加したドメイン(<u>example.com</u>)、"F220-M user defined hosts" の下に追加した IP アドレス(192.0.2.0/255.255.255.0)が menlo.pac に追加されていることが確認できます。 ※修正したい場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。

return 'DIRECT';		^
/* F220-M user defined domains */ if (shExpMatch(host, "example.com"))	*	
return 'DIRECT'; }		
/* F22U-M user defined hosts */ if (isInNet(host, "192.0.2.0", "255.25	5 .255.0″))	
return DiktUl; } (6 (und substation(0, 2) === '''''''''		
return 'PROXY proxy0-d55b4568a5febb	aa8e98f626937b5ca.menlosecurity.com:3129; PROXY proxy1-	
00004006a0Tebb0aa6e96T62093/b0Ca.menlosect	rity.com:3128; Diweon ;	スクロールバー
if (url.substring(0, 5) === 'http:')		
return 'PRUXY proxyU-d5bb45b8a5tebb5 d55b4568a5febb5aa8e98f626937b5ca.menlosecu }	saabe98t62693765ca.menlosecurity.com:3129; PRUXY proxyl− urity.com:3129; DIRECT`;	
return 'DIRECT';		*
保存する	PACファイルの名前を入力してください。 	
	PACファイル名 .pac	

*全ての機種で「F220-M」と表示されます。お使いの機種に読み替えてご使用ください。

保存する PAC ファイル名を記入(例では"test"を記入)して下の『保存』ボタンを押します。

※PAC ファイル管理メインページのプルダウンで表示された既存のファイル名では保存できませんのでご 注意下さい。

PACファイル管理ページ
PACファイルの内容を確認してください。
<pre> return 'DIRECT'; /* F220-M user defined domains */ if (shExxMatch(host, "example.com")) { return 'DIRECT'; } /* F220-M user defined hosts */ if (islnNet(host, "182.0.2.0", "255.255.255.0")) { return 'DIRECT'; } /* F220-M user defined hosts */ if (url.substring(0, 6) === 'https:') return 'PROXY proxyD-d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e89f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b4568a5febb5aa8e98f628937b5ca.menlosecurity.com:3129; PROXY proxy1- d55b456837b5ca.menlosecurity.com:3129; DIRECT'; return 'DIRECT'; return 'DIRECT'; } } </pre>
」 保存するPACファイルの名前を入力してください。 testpac 保存 修正

"test.pac"で保存が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。

PACファイル管理ページ	
福	集したPACファイルを保存しました。 test.pac
	戻る HOME

保存したファイルは、PAC ファイル管理メインページのプルダウンで確認ができます。

※管理可能なファイル数は menlo.pac, direct.pac を含めて 10 ファイルまでです。11 ファイル以上のファ イルを作成しようとした場合、エラーとなり作成できません。必要に応じて不要なファイルを削除してく ださい。削除については、7.8 項でご説明します。

PACファイル管理ページ				
	PACファイルを選択してください(更新順)			
		menlo.pa	c 🗸	
г		menlo.pa	c	
	編集	test.pac direct.pac		
	削除		選択したPACファイルを削除します。	
	適用		選択したPACファイルを適用します。 適用中のPACファイル:menlo.pac	
	バックアッ リストア	ップ ,	選択したPACファイルをバックアップ/リストアします。	
	パスワード	変更	ログインパスワードを変更します。 パスワードの変更をおすすめします。	

7.5 適用

作成した PAC ファイルを適用します。

PAC ファイル管理メインページで適用するファイル名を選択(例では"test.pac"を選択)して、『適用』ボタン を押します。※初期状態では"menlo.pac"が適用されています。

PACファイル管理ページ		
test	PACファイルを選択してください(更新順) .pac イ	
編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。	
削除	選択したPACファイルを削除します。	
適用	ここをクリックします 選択したPACファイルを適用します。 適用中のPACファイル: menlo.pac	
バックアップ リストア	選択したPACファイルをバックアップ/リストアします。	
パスワード変更	ログインパスワードを変更します。 パスワードの変更をおすすめします。	

確認画面で適用する PAC ファイルが表示されます。下の『適用』ボタンを押して適用します。

PACファイル管理ページ
このPACファイルを適用しますか? test.pac
<pre>function FindProxyForURL(url, host) { /* Normalize the URL for pattern matching */ url = url.tolowerCase(); host = host.toLowerCase(); uar hostDrDomainIs = function(host, val) { return (host === val) dnBomainIs(host, '.' + val); }; var hostIs = function(host, val) { return (host === val); /* Don't proxy local hostnames */ if (isPlainNostName(host)) /* tori view local hostnames */ if (isPlainNostName(host)) /* Don't or hock IPV6 addresses */ if (isPlainNostName(host)) /* Don't hock IPV6 addresses */ if (isPlainNostName(host)) /* Don't or hock IPV6 addresses */ if (isPlainNostName(host)) /* Don't proxy non-routable addresses (RFC 3330) */ /* Don't proxy non-routable addresses (RFC 3330)</pre>
適用 戻る

"test.pac"の適用が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。

PACファイル管理ページ	
	PACファイルを適用しました。 test.pac
	戻る HOME

PAC ファイル管理メインページに戻ると適用中のファイル名が"test.pac"になっています。

※"test.pac"がクライアント PC に反映されるのは、クライアント PC の DHCP リース更新時です(ブラウ ザによっては、ブラウザ起動時に PAC ファイル取得/反映します)。

PACファイル管理ページ		
	PAC test.pac	Cファイルを選択してください(更新順) ✓
	編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。
	削除	選択したPACファイルを削除します。
	適用	選択したPACファイルを適用します。 適用中のPACファイル:test.pac
	バックアップ リストア	選択したPACファイルをバックアップ/リストアします。
	バスワード変更	ログインパスワードを変更します。 パスワードの変更をおすすめします。

7.6 バックアップ

作成した PAC ファイルのバックアップデータを抽出することができます。

PAC ファイル管理メインページで抽出するファイル名を選択して(例では"test.pac"を選択)して『バックア ップ リストア』ボタンを押します。

PACファイル管理ページ		
	PAC test.pac	ファイルを選択してください(更新順)
	編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。
	削除	選択したPACファイルを削除します。
	適用	選択したPACファイルを適用します。 適用中のPACファイル:test.pac
	バックアップ リストア	ここをクリックします 選択したPACファイルをバックアップ/リストアします。
	パスワード変更	ログインパスワードを変更します。 パスワードの変更をおすすめします。

バックアップデータの表示画面に遷移して、"test.pac"のバックアップデータが表示されます。ここで表示 される情報は"menlo.pac"に対してお客様が追加したドメイン・IPアドレスのみとなります。

下記の例では 7.4 項で追加したドメイン(example.com)と IP アドレス(192.0.2.0/255.255.255.0)が、それぞ れバックアップデータの"user_domains"と"user_ipaddrs"の下に表示されています。

バックアップデータは、コピー&ペーストしてテキストファイル形式で保存して下さい。次のリストアコマンドで、保存したバックアップデータを使って PAC ファイルの復元が可能になります。

『戻る』ボタンで PAC ファイル管理メインページへ戻ります。

PACフ	アイル管理ページ		
	PACファイルのバックアッフ	プ/リストアを行います。	
	バックアップ	リストア	
	バックアップデータをテキス test,	〜として保存してください。 pac	
	<pre>{</pre>		
	戻る	5	

7.7 リストア

7.6 項のバックアップデータを使って、PAC ファイルを復元します。

PAC ファイル管理メインページで menlo.pac を選択して『バックアップ リストア』ボタンを押します。



バックアップが選択された状態で確認ページに遷移するので、リストアを選択します。

PACファイ	イル管理ページ
	PACファイルのバックアップ/リストアを行います。
	パックアップリストア
	バックアップデータをテキストとして保存してください。 menio.pac
	このPACファイルはバックアップできません。
	戻る

7.6 項で保存したバックアップデータをコピー&ペーストで下記のウインドウに貼り付けます。 PAC ファイルを復元するために下の『次へ』ボタンを押します。

PACフ:	アイル管理ページ		
	PACファイルのバックアッ	プ/リストアを行います。	
	バックアップ	リストア	
	PACファイルのリン バックアップデータ	ストアを行います。 を入力してください。	
	<pre>{</pre>	ここに貼り付けます	
	次へ	戻る	

復元した PAC ファイルが表示されます。右端のスクロールバーを一番下に持っていくと、"F220-M user defined domains"の下に追加したドメイン(example.com)、"F220-M user defined hosts"の下に追加した IP アドレス(192.0.2.0/255.255.255.0)が確認できます。

※修正する場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。

PACファイル管理ページ	
PACファイルの内容を確認してください。	
i return 'DIRECT'; i f (220-H user defined dowains */) * i f (220-H user defined dowains */) * i f (220-H user defined dowains */) * i f (220-H user defined hosts */) * i f (200-H user defined hosts */) * i f (200-H user defined hosts */) * i f (200-H user defined hosts */) * i f (url.substring(0, 8) === 'https:') * i f (url.substring(0, 5) === 'https:') * i f (url.substring(0, 5) === 'http:') * i return 'PRXY proxy0-d55b4568a5feb5ca.sen[osecurity.com:3129; PRXY proxy1- d55b4668a5feb5case048feb268937b5ca.sen[osecurity.com:3129; PRXY proxy1- d55b4668a5feb5case048feb268937b5ca.sen[osecurity.com:3129; PRXY proxy1- i return 'DIRECT'; return 'DIRECT'; return 'DIRECT': R存するPACファイルの名前を入力してください。 PACファイル名 pac R存存 修正	ーを下に移動

*全ての機種で「F220-M」と表示されます。お使いの機種に読み替えてご使用ください。

保存する PAC ファイル名を記入(例では"test2"を記入)して下の『保存』ボタンを押します。 ※既存のファイル名では保存できませんのでご注意下さい。

PACファイル管理ページ
PACファイルの内容を確認してください。
<pre> return 'DIRECT'; /* F220-M user defined domains */ if (shExpMatch(host, "example.com"))</pre>
保存するPACファイルの名前を入力してください。 test2 .pac 保存

"test2.pac"というファイル名で復元が完了しました。『HOME』ボタンで PAC ファイル管理メインページ へ戻ります。

PACファイル管理ページ
編集したPACファイルを保存しました。 test2.pac
戻る HOME

7.8 削除

不要な PAC ファイルを削除する場合は、PAC ファイル管理メインページで削除するファイル名を選択して (例では"test.pac"を選択)して 『削除』ボタンを押します。

※適用中のファイルや"menlo.pac"、"direct.pac"はエラーとなり削除できませんのでご注意下さい。

PACファイル管理ページ		
PAC test.pac	ファイルを選択してください(更新順) ~	
編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。	
削除	<u>ここをクリックします</u> 選択したPACファイルを削除します。	
適用	選択したPACファイルを適用します。 適用中のPACファイル:menlo.pac	
バックアップ リストア	選択したPACファイルをバックアップ/リストアします。	
パスワード変更	ログインバスワードを変更します。 パスワードの変更をおすすめします。	

確認画面に削除する PAC ファイルが表示され、下の『削除』ボタンを押して削除します。

PACファイル管理ページ
このPACファイルを削除しますか? test.pac
<pre>function FindProxyForURL(url, host) { /* Wormalize the URL for pattern matching */ url = url.toLowerCase(); host = host.toLowerCase(); var host0rDomainIs = function(host, val) { return (host === val) dnsDomainIs(host, '.' + val); }; var host1s = function(host, val) { return (host === val) dnsDomainIs(host, '.' + val); }; var host1s = function(host, val) { return (host === val) dnsDomainIs(host, '.' + val); }; var host1s = function(host, val) { return (host === val) for some state is a st</pre>
削除 戻る

"test.pac"の削除が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。

PACファイル管理ページ	
	PACファイルを削除しました。 test.pac
	同日 FOME

7.9 送信先プロキシ変更

PAC ファイルの送信先プロキシ情報を変更することも可能です。

PAC ファイル管理メインページで変更するファイル名を選択して(例では"test.pac"を選択)して『編集』ボ タンを押します。※direct.pac はエラーとなり変更できませんのでご注意下さい。

PACファイル管理ページ		
	PACファイルを選択してください(更新順)	
test	pac ✓ ここをクリックします	
編集	選択したPACファイルを編集します。 編集したPACファイルは別名で保存します。	
削除	選択したPACファイルを削除します。	
適用	選択したPACファイルを適用します。 適用中のPACファイル:test.pac	
バックアップ リストア	選択したPACファイルをバックアップ/リストアします。	
パスワード変更	ログインバスワードを変更します。 パスワードの変更をおすすめします。	

FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックの導入・運用

『送信先プロキシ変更』ボタンを押します。

PACファイル管理ページ		
	編集内容を選択してください。	
	メイン/旧アドレス	
	追加・削除 任意のドメイン/IPアドレスを追加・削除します。 ▲ ここをクリックします	
送	生信先プロキシ変更 送信先プロキシを変更します。	
	戻る	

送信先プロキシは2つ設定されており、どちらも変更可能です。

PACファイル管理ページ				
		送信先プロキシを変更してください。		
	番号	送信先プロキシ	ポート	
	1	proxy0-d55b4568a5febb5aa8e98f626937b5ca.meniosecurity.com	3129	
	2	proxy1-d55b4568a5febb5aa8e98f626937b5ca.meniosecurity.com	3129	
		次へ 戻る		

変更する送信先プロキシを記入 (例では No1 を"proxy0-test.com: 5555"に変更)し『次へ』ボタンを押します。

PACファイル管理ページ				
		送信先プロキシを変更してください。		
	番号	送信先プロキシ	ポート	
	1	proxy0-test.com	5555	
	2	proxy1-d55b4568a5febb5aa8e98f626937b5ca.menlosecurity.com	3129	
		次へ 戻る		

変更した PAC ファイルが表示されます。右端のスクロールバーを移動すると、No.1 のドメインが"proxy0test.com: 5555"に変更されていることが確認できます。

※修正したい場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。

PACファイル管理ページ
PACファイルの内容を確認してください。
<pre> Isinet(idst, 132.175.36.0 ; 233.233.182.0)) return 'DIRECT'; if (hostOrDomain1s(host, "Lioketmaster.com")]] hostOrDomain1s(host, "tioketmaster.com")]] forturn 'DIRECT'; if (url.substring(0, 5) === 'http:') return 'PROXY proxy0-test.com:5555; PROXY proxy1-d55b4568a5febb5aa8e38f626937b5ca.menlosecurity.com:3123; lif(url.substring(0, 5) === 'http:') return 'PROXY proxy0-test.com:5555; PROXY proxy1-d55b4568a5febb5aa8e38f626937b5ca.menlosecurity.com:3123; lif(url.substring(0, 5) === 'http:') return 'DIRECT'; return 'DIRECT'; } </pre>
保存するPACファイルの名前を入力してください。 PACファイル名.pac
保存 修正

保存する PAC ファイル名を記入(例では"test3"を記入)して下の『保存』ボタンを押します。 ※既存のファイル名では保存できませんのでご注意下さい。

PACファイル管理ページ
PACファイルの内容を確認してください。
<pre>IsinMer(Nost, 192.173.36.0., 235.235.192.0.7) { return 'DIRECT'; } if (hostOrDomain1s(host, "Licketmaster.com") hostOrDomain1s(host, "ticketmaster.com") hostOrDomain1s(host, "ticketmaster.com") hostOrDomain1s(host, "ticketmaster.com") return 'DIRECT'; } if (url.substring(0, 5) === 'http:') return 'PROXY proxy0-test.com:5555; PROXY proxy1-d55b4568a5febb5aa8e38f626337b5ca.menlosecurity.com:3128; } DIRECT'; if (url.substring(0, 5) === 'http:') return 'DIRECT'; } return 'DIRECT'; } </pre>
様存9 SPACファイルの名削を入力してくたさい。 test3pac
保存 修正

test3.pac で保存が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。

PACファイル管理ページ	
編集したPACファイルを保存しました。 test3.pac	
戻る HOME	

7.10 サポートブラウザ

本機能は、以下のブラウザで動作確認しています。

- Google Chrome(83)
- Firefox(77)
- Microsoft Edge(44.18362.449.0)
- Internet Explorer(11.719.18362.0) (**)
- Safari(13.1)

※Internet Explorer を使用される場合には、ブラウザの[設定](右上歯車マーク) > [互換表示設定]にて「イントラネットサイトを互換表示で表示する」のチェックを外してご使用下さい。

8 注意事項

"reset clear コマンドによる初期化"や"装置起動時の初期化(RESET スイッチを押しながら装置を起動)" を実施された場合、本機能が全てクリアされ使用できなくなりますのでご注意下さい。

付録 A LAN 側ネットワークをお客様環境に合わせて変更する方法

F F220M は工場出荷時に giga1/1 ポートは 192.168.1.1 (192.168.1.0/24 のネットワーク) に、コンテナ アドレスは 192.168.1.254 に設定してあります。これらのアドレスをお客様環境に合わせて変更する場合の 変更箇所についてご説明します。

冒頭でご説明した F220M のコンフィグにおいて、下記赤枠で囲まれた部分の設定を、お客様ネットワークに合わせて変更をして下さい。

```
container enable
container device disk /mnt/pac_mainte drive uid 101 gid 101
container configuration
L
interface 1
 bridge-group 1
 ip address 192.168.1.254 255.255.255.0
                                     ←お客様のネットワークに合わせてコンテナアドレスを
 ip gateway 192.168.1.1
                                      変更して下さい
                   ↑変更後のgiga1/1のアドレスを設定して下さい
exit
!
exit
L
access-list 111 deny ip any any
access-list 121 spi ip any any
ip host fiteInet-container.fnsc.co.jp 192.168.1.254
                                      ↑お客様のネットワークに合わせてコンテナアドレスを
ip route 0.0.0.0 0.0.0.0 100.1.1.1
                                      変更して下さい
ip name-server 127.0.0.1
ip dhcp server-profile DHCP_SERVER_PROF
address 192.168.1.2 192.168.1.101
                                     ←お客様のネットワークに合わせてDHCP払い出し
lease-time 3600
                                       アドレスレンジを変更して下さい
dns 192.168.1.1
                                     ←変更後のgiga1/1のアドレスを設定して下さい
gateway 192.168.1.1
                                     ←変更後のgiga1/1のアドレスを設定して下さい
option 252 ascii http://fitelnet-container.fnsc.co.jp/pac/web_security.pac
exit
ip nat list 1 192.168.1.0 0.0.0.255
                                     ←お客様のネットワークに合わせて変更して下さい
hostname FITELnet
interface GigaEthernet 1/1
vlan-id 1
bridge-group 1
channel-group 1
container-use
exit
L
```

```
interface GigaEthernet 2/1
vlan-id 21
bridge-group 21
channel-group 21
ip access-group 111 in
ip access-group 121 out
exit
I.
interface Port-channel 1
ip dhcp service server
ip dhcp server-profile DHCP_SERVER_PROF
                                          ←お客様のネットワークに合わせてgiga1/1のアドレス
ip address <u>192.168.1.1 255.255.255.0</u>
                                             を変更して下さい
link-state always-up
exit
I
interface Port-channel 21
ip address 100.1.1.2 255.255.255.0
ip nat inside source list 1 interface
exit
1
dns-server ip enable
I.
proxydns domain 1 any * any static x.x.x.x
L
end
```

付録 B Windows10 に CA 証明書をインストールする方法

入手した CA 証明書(例: MenloSecurityCACert2020.cer)をインストールするクライアント PC のデス クトップ上に置きダブルクリックします。



次の証明書ダイアログが表示されたら、『証明書のインストール』をクリックします。



次の画面が表示されたら、保存場所『ローカルコンピュータ』を選択して『次へ』をクリックします。

	×
← 😼 証明書のインポート ウィザード	
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
保存場所	
○現在のユーザー(C)	
・ ローカル コンピューター(L)	
続行するには、[次へ] をクリックしてください。	
クリック	
	1411
◆次八(N) 1 千秒.	12IV

次の画面が表示されたら、『証明書をすべて次のストアに配置する』を選択して『参照』をクリックしま す。

←	☞ 証明書のインポート ウイザード
	証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。
	Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U) ④ 証明書をすべて次のストアに配置する(P) ① 証明書ストア: ② 証明書ストア: ③ 証明書ストア:
	次へ(N) キャンセル

次の画面が表示されたら、『信頼されたルート証明機関』を選択して『OK』をクリックします。

証明書ストアの選択	\times
使用する証明書ストアを選択してください(C)	
篇 個人	^
…──── 信頼されたルート証明機関	
エンタープライズの信頼	
信頼された発行元	
🧰 信頼されていない証明書	
ジャード パーティルート証明機関	~
□ 物理ストアを表示する(S) クリック	
OK キャンセノ	L

次の表示が確認できたら『次へ』をクリックします。

- 4	🖗 証明書のインポート ウィザード
	証明書ストア
_	証明書ストアは、証明書が保管されるシステム上の領域です。
	Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。
	○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
	● 証明書をすべて次のストアに配置する(P)
	証明書ストア:
	信頼されたルート証明機関 参照(R)
	クリック

次の表示が確認できたら『完了』をクリックします。

	×
証明書のインポート ウィザード	
証明書のインポートウィザードの完了	
[完了]をクリックすると、証明書がインポートされます。	
次の設定が指定されました:	
ユーザーが選択した証明書ストア 信頼されたルート証明 5000 5000 5000 5000	機関
이상 때까만	
	クリック
	完了(F) キャンセル
	 ・証明書のインポートウィザードの完了

『正しくインポートされました。』のメッセージが表示されれば完了です。



付録 C リモートアクセス機能

リモート環境から F220M ヘアクセスし、分離・無害化サービスを利用する場合の設定方法についてご説明 します。構成例を図3に示します。

クライアント PC と F220M は L2TP/IPsec でトンネル接続を行います。この時、クライアント PC には 192.168.1.102~192.168.1.200 の範囲のアドレスが払い出されます。トンネル接続後、ルータは PPP により クライアント PC に DNS サーバアドレス (ルータ) 情報を通知し、クライアント PC はプロキシ自動検出動 作によりプロキシ設定情報である wpad.dat ファイル(PAC ファイルと同一)をコンテナから取得します。取得 したプロキシ設定をもとに分離・無害化サービスを通したインターネットアクセスが可能になります。



図 3 F220M リモートアクセス 構成図

次にリモートアクセス機能を実現するための F220M とクライアント PC の設定についてご説明します。

C-1 ルータ設定

F220M のコンフィグを以下に示します。前述(4項)のコンフィグに赤字部分の設定が追加されています。

```
←コンテナのサービスを有効にする設定
container enable
container device disk /mnt/pac mainte drive uid 101 gid 101
container configuration
interface 1
 bridge-group 1
 ip address 192.168.1.254 255.255.255.0
 ip gateway 192.168.1.1
exit
ļ
exit
ŗ
access-list 100 permit udp any host 100.1.1.2 eq 500 ←フィルタ設定(ISAKMPパケット許可)
access-list 100 permit udp any host 100.1.1.2 eq 4500 ←フィルタ設定(ISAKMPパケット許可)
access-list 100 permit 50 any any
                                                ←フィルタ設定(ESPパケット許可)
```

```
←学習フィルタ設定
access-list 111 deny ip any any
                                                 ←学習フィルタ設定
access-list 121 spi ip any any
                                                 ←コンテナアドレスにホスト名
ip host fiteInet-container.fnsc.co.jp 192.168.1.254
ip host wpad.example.com 192.168.1.254
                                                 (fiteInet-container.fnsc.co.jp)登録
ip route 0.0.0.0 0.0.0.0 100.1.1.1
                                                 ←デフォルトルートを設定
ip name-server 127.0.0.1
                                                 ←L2TP/PPPにより通知するアドレス範囲
ip local pool POOL1 192.168.1.102 192.168.1.200
                                                  の確定
                                                 ←DHCPサーバ機能のプロファイル
ip dhcp server-profile DHCP SERVER PROF
address 192,168,1,2 192,168,1,101
                                                 ←DHCP払い出しアドレスレンジ
lease-time 3600
                                                 ←払い出し情報のリース時間(秒)
dns 192.168.1.1
gateway 192.168.1.1
option 252 ascii http://fitelnet-container.fnsc.co.jp/pac/web_security.pac
                                                 ↑ PACファイル置き場情報
exit
                                                 ←192.168.1.0/24 を list 1 と定義
ip nat list 1 192.168.1.0 0.0.0.255
aaa authentication ppp LOCAL_AUTH local-group LOCAL_GROUP
                                                 ↑ PPPoEセッションの認定方式を設定
L
aaa local group LOCAL_GROUP
                                                 ←クライアントデータベース設定モード
username user1 password secret1
                                                 ←接続を許可するユーザ名/パスワード設定
exit
hostname FITELnet
                                                ←IPsecポリシー設定(Phase2)
crypto ipsec policy IPSECPOL_1
mode transport
set security-association lifetime seconds 86400
set security-association transform-keysize aes 128 256 256
set ip df-bit 0
set ip fragment post
set udp-encapsulation nat-t keepalive interval 30 always-send
exit
L
                                                 ←DPD設定
crypto isakmp keepalive always-send
crypto isakmp log sa detail
crypto isakmp log session detail
crypto isakmp log negotiation-fail detail
L
                                                 ←ISAKMPポリシー設定(Phase1)
crypto isakmp policy ISAPOL_1
authentication pre-share
encryption aes
encryption-keysize aes 256 256 256
group 1 2 5 14 15
lifetime 86400
hash sha
initiate-mode main
exit
```

```
I.
                                               ←ISAKMPプロファイル設定
crypto isakmp profile ISAPROF_001
                                               ←ISAKMPポリシーを指定
set isakmp-policy ISAPOL_1
                                               ←IPsecポリシーを指定
set ipsec-policy IPSECPOL 1
                                               ←IKEバージョンを指定
ike-version 1
local-key secret
                                               ←Pre-shared Keyを指定
exit
L
crypto map MAP_001 ipsec-isakmp dynamic
                                               ←crypto MAP設定
set isakmp-profile ISAPROF_001
                                               ←セレクタを指定
exit
L
interface GigaEthernet 1/1
vlan-id 1
bridge-group 1
channel-group 1
container-use
exit
L
interface GigaEthernet 2/1
vlan-id 21
bridge-group 21
channel-group 21
                                               ←ISAKMP、ESPを通す設定
ip access-group 100 in
ip access-group 111 in
                                               ←WAN側からのアタックを防ぐための
                                                学習フィルタ設定
ip access-group 121 out
exit
interface Port-channel 1
                                               ←giga1/1にDHCPサーバ機能を設定
ip dhcp service server
                                               ←DHCPサーバ機能のプロファイル名を指定
ip dhcp server-profile DHCP_SERVER_PROF
ip address 192.168.1.1 255.255.255.0
ip proxy-arp
                                               ←proxy-arp動作を行う設定
link-state always-up
exit
L
interface Port-channel 21
ip address 100.1.1.2 255.255.255.0
ip nat inside source list 1 interface
                                               ←list 1に含まれる送信元アドレスを
                                                インタフェースのアドレスにNAT変換する
exit
L
dns-server ip enable
L
                                               ←お客様環境に合わせてDNSサーバを指定
proxydns domain 1 any * any static x.x.x.x
                                                して下さい(x.x.x.x の部分)
end
```

C-2 クライアント PC 設定

クライアント PC の設定手順は次のようになります。 ※windows10 を例にご説明します。

手順	設定内容	画面	面表示
1	①Windows10左下のスタートボタンをクリックします。 ②「設定」を選択します。	 □ ドキュメント □ ピクチャ ◎ 設定 ② ① 電源 □ ○ □ 	
2	「設定」のメニュー画面が表示されたら、「ネットワークとインターネット」 を選択して、次を実行します。 ①左側のメニューで「VPN」を選択します。 ②右のような画面が表示されたら「VPN接続を追加する」をクリックしま す。	 ← 設定 ☆ ホーム 設定の検索 > オットワークとインターネット ⑦ 状態 印 イーサネット 奈 ダイヤルアップ ⑦ VPN ① ① プロキシ 	VPN
3	右の画面が表示されますので、以下の5つの情報を入力もしくは確認します。 1) VPNプロバイダー: 「Windows(ビルトイン)」と表示されていることを確認します。 2) 接続名:任意の名前を入力します。 3) サーバ名またはアドレス:お使いの環境に合わせて接続先のサーバー名もしくはアドレスを入力します。本設定例ではFITELnet装置の WAN側アドレス(100.1.1.2)となります。 4) VPNの種類: 「事前共有キーを使ったL2TP/IPsec」を選択します。 5) 事前共有キー:事前共有キー(Pre-shared Key)の文字列を入力します。 よ記5つの情報を入力したら、右下の「保存」をクリックしてください。	 ◆ PE ◆ PPN接続を追加 ▼PN74/4- Windows (ビルトイク) #読を L2TP-connection ワーパーキまたはアドレス 100.1.12 マレハの確實 単前共有手-を使った L2TP/IPsec 単前共有手 単のしていたい サインイン/情報の確頻 ユーザー名とパズワード 	- □ × - □ × - □ × - □ ×
4	手順2の画面が再び表示されますので、手順3で追加した接続名が表示されることを確認します。	 ← 設定 ☆ ホーム 設定の検索 > オットワークとインターネット プリ・ワークとインターネット ⑦ 状態 ? イーサネット ⑦ ダイヤルアップ ? ダイヤルアップ ? シートン 	 VPN 接続を追加する VPN 接続を追加する レンド・レンド・レンド・レンド・レンド・レンド・レンド・レンド・レンド・レンド・

手順	設定内容	画面表示	
5	「ネットワークとインターネット」のメニューで「イーサネット」を選択しま す。「アダプターのオプションを変更する」をクリックします。	 ● 設定 ☆ ホーム ☆ ホーム ☆ ホーム ☆ ホーム → ホーム オットワークとインターネット ● 状態 ● オペ地 ● ダイヤルアップ ● ダイヤルアップ ● グロキシ (1) (1) ※ VPN ◆ プロキシ ● プロキシ 	
6	手順3で追加したVPN接続名を右クリックして、プロパティをクリックしま す。	 マーロX マーロX	
7	プロパティのセキュリティタブを開き、以下を選択して、OKをクリックしま す。 1)VPNの種類: IPsecを利用したレイヤー2トンネリングプロトコル(L2TP/IPsec) 2)データの暗号化:暗号化が必要 3)認証:次のプロトコルを許可する チャレンジハンドシェイク認証プロトコル(CHAP)	L2TP-connectionのプロ/(ティ 全般 オブション ゼキョリティ ネットワーク 共有 VPN の種類(T): Prese を利用したレイヤー 2 トンネリングプロトコル (L2TP/Psec) データの信号化(D): 理号化が必要 (サーバーが拒否する場合は切形します) ジロ 登証 ○ 妊娠認証プロトコル (EAP) を使う(E) 「 一 二 一 一 二 一 二 一 二 一 二 一 二 一 二 一 二 一 二	
8	プロパティのネットワークタブを開き、「インターネットプロトコルバージョ ン4」をチェックして、プロパティをクリックします。	L2TP-connectionのプロパティ × 登録 オブション セキュリティ (ネットワーク 共有 この接続は次の項目を使用します(O): ローム・クシーク コーン バーンヨン バーンヨン キ (オロリーン・) ローム・クシーク コーン バーンヨン パーンヨン キ (オロリーン・) ローム・クシーク コーン アンパンスーール(ロ) ローム・クシーク コーン コーン コーン コーン ルマ・・ ローム・ハーク コーン コーン ローム・ ローム・	

手順	設定内容	画面表示
9	詳細設定をクリックします。	となる テレー 中、レー 中、
10	「リモートネットワークでデフォルトゲートウェイを使う」のチェックを外し て、DNSタブを開きます。	TCP/IP 詳細設定 X IP 設定 [NIS] WINS このチェックボックスは、Dーカル・ヤットク・クとダイヤルアップ ネットワークに開発に 課題しているとこのみ運用されます。オンになっている場合、ローカル ネットワーク で注信できないデータはダイヤルアップ ネットワークに転送されます。 [1] ジモート ネットワークでデフスルト ゲートウェムを使う(い) [2] ウラス ペースのルートの追加を無効にする 〇 自動メトリック(A) インターフェイス メドリック(N):
11	「この接続のDNSサフィックス」のところに「example.com」と入力して、 OKをクリックします。	TCP/IP 詳細設定 × IP 設定 DNS WINS DNS サー/(- アドレス (使用頃)(N): 1 ・ ・ ・<
12	インターネットプロトコルバージョン4のプロパティに戻りましたら、OKを クリックします。 VPN接続名のプロパティに戻りましたら、OKをクリックします。	パソワーキャトプロトンドパージョン4 (100/IP+480/JD/IF)イ × タントワーケアに30時度が1が1-1-14/11/31時まは、Ph2F151時かに内容すた (2017)を見ます、ガポーや1711/31時まは、Ph2F151時かに内容な (2018)を見たいたされい、 * ● アドレスを自動的に応用す 20(0)

手順	設定内容	画面表示
13	コマンドプロンプトにてPowershellを実行して、右の画面のようにVPN接 続先の経路情報を登録します。本設定例では、FITELnet装置のLAN側 のホストと通信するために、192.168.1.0/24を登録します。	■ コマゾガロンガト-Powershell – □ × C:¥Users> C:¥Users> C:¥Users> C:¥Users>Powershell ←「Powershell」と入力 Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. 新しいクロスブラットフォームの PowerShell をお試しください https://aka.ms/ pscore6 PS C:¥Users> Add-VpnConnectionRoute ←「Add-VpnConnectionRoute」と入力 コマンド バイブライン位置 1 のコマンドレット Add-VpnConnectionRoute」と入力 コマンド バイブライン位置 1 のコマンドレット Add-VpnConnectionRoute」と入力 コマンド バイブライン位置 1 のコマンドレット Add-VpnConnectionRoute 次のパラメーターに値を指定してください: ConnectionName: L2TP-connection ← VPN接続名を入力 DestinationPrefix: 192.168.1.0/24 ← VpN経路を入力 PS C:¥Users> PS C:¥Users> PS C:¥Users> PS C:¥Users> PS C:¥Users>
14	設定>ネットワークとインターネット のメニューでVPN接続を選択して、 手順3で追加したVPN接続名を選択して、「接続」をクリックします。	 ◆ 設定 ◆ ホーム ◇ ホーム ◇ サーム ◇ シント <l< th=""></l<>
15	VPNアカウントとパスワードを入力して、OKをクリックします。	Windows セキュリティ × サインイン user1 ← VPNアカウントを入力(本設定例では「user1」) ●●●●●●● ←パスワードを入力(本設定例では「secret1」) ドメイン: コーザー名またはパスワードが正しくありません。 0к
16	「接続済み」の表示が確認されたら、接続完了です。	 ← 設定 ー □ × ☆ ホム ジアワンクンインターネット クリヤワークンインターネット ウ 状態 ロ イーサネット ウ イヤリルアップ ジアト ジロキック ジアト ジェローク シェローク ジェローク シェローク ショング 中の VPN を許可 ・ シェローク シェローク ショローク シェローク シェローク シェローク ショローク

上記設定後、L2TPトンネル接続した状態で、前述6項の手順を行うことで分離・無害化サービスを通した インターネットアクセスが可能となります。

以上