

FortiGate 操作ガイド

第 1.0 版 2022 年 6 月 10 日

NEC ネッツエスアイ株式会社

改版履歴

版数	日付	内容
1.0	2022/06/10	初版発行

本書は、FortiGate の GUI 操作方法を説明する資料です。

NEC ネッツエスアイ株式会社の許可なく、本書を転載・コピー・配布することを禁じます。

本書に記載されている内容は将来予告なしに変更することがあります。

copyright (c) NEC Networks & System Integration Corporation All Rights Reserved.

NEC ネッツエスアイ株式会社の許可なく複製・改変などを行うことはできません。

目次

1. はじめに	1
1.1. 本書の目的	1
1.2. 対象機種およびバージョン情報	1
2. FortiGate 操作	2
2.1. ログイン・ログアウト方法	2
2.1.1. ログイン方法	5
2.1.2. ログアウト方法	6
2.2. 電源 OFF/ON・再起動方法	7
2.2.1. 電源 OFF 方法	7
2.2.2. 電源 ON 方法	9
2.2.3. 再起動方法	10
2.3. 管理者パスワード変更	12
2.4. 設定のバックアップ・リストア方法	16
2.4.1. 設定のバックアップ方法	16
2.4.2. 設定のリストア方法	18
2.5. ログ閲覧方法	21
2.5.1. 転送トラフィックログ閲覧方法	21
2.5.2. システムイベントログ閲覧方法	21
2.5.3. Web フィルタログ閲覧方法	22
2.5.4. アプリケーションコントロールログ閲覧方法	23
2.6. セキュリティプロファイルの設定	24
2.6.1. アンチウィルスの設定	24
2.6.2. Web フィルタ設定	25
2.6.3. プリケーションコントロール設定	31
2.6.4. 侵入防止（IPS）設定	33
2.6.5. 新しいアプリケーションコントロールプロファイルの作成	36
2.7. ポリシー設定	38
2.7.1. ポリシー設定	39
2.7.1.1. セキュリティプロファイル	43
2.7.1.2. SSL インスペクション	43
2.7.2. アドレス設定	44
2.7.3. サービス設定	48
2.8. ルーティング設定	52
2.9. FortiClient ユーザの追加と削除設定	54

1. はじめに

1.1. 本書の目的

本書は、FortiGate の操作方法を簡易的にまとめた利用ガイドです。

詳細な操作方法については下記メーカーサイトから製品ガイドをダウンロードしてご参照ください。

- FortiGate

<http://docs.fortinet.com/fortigate/admin-guides>

1.2. 対象機種およびバージョン情報

本書において説明する FortiGate の機種/バージョン情報を以下に示します。

対象機種およびバージョン

項目	機種	バージョン
FortiGate	FortiGate 100F	v6.4.5, build1828, 210217 (GA)

2. FortiGate 操作

2.1. ログイン・ログアウト方法

FortiGateへのログインは、お客様端末のブラウザから別途通知されるログインID／パスワードを使用して接続していただきます。

接続先のIPアドレス（FortiGateのIPアドレス）は、パラメータシートをご確認願います。

ログイン環境

項目	説明
FortiGate接続アドレス	https://aaa.bbb.ccc.ddd/login (httpは接続できません。)
ログインID／パスワード	※パラメータシートをご確認願います。
FortiGate接続可能アドレス	パラメータシートをご確認願います。
利用可能ブラウザ	Firefox 85以上、Chrome 88以上、Edge 88以上 ※正常に表示されない場合は最新バージョンのブラウザを使用してください ※FortiGateの管理UIに接続するブラウザはFirefox、Chromeが推奨となります。 Internet Explorerはサポートしておりません。

本ガイドに掲載されている画像や手順は、Firefox、Chromeを使って作成しています。

(例) ログイン画面イメージ



※ブラウザで Web 管理画面への接続を行う時に、警告画面が表示される場合があります。

以下の手順に沿ってアクセス可能になります。

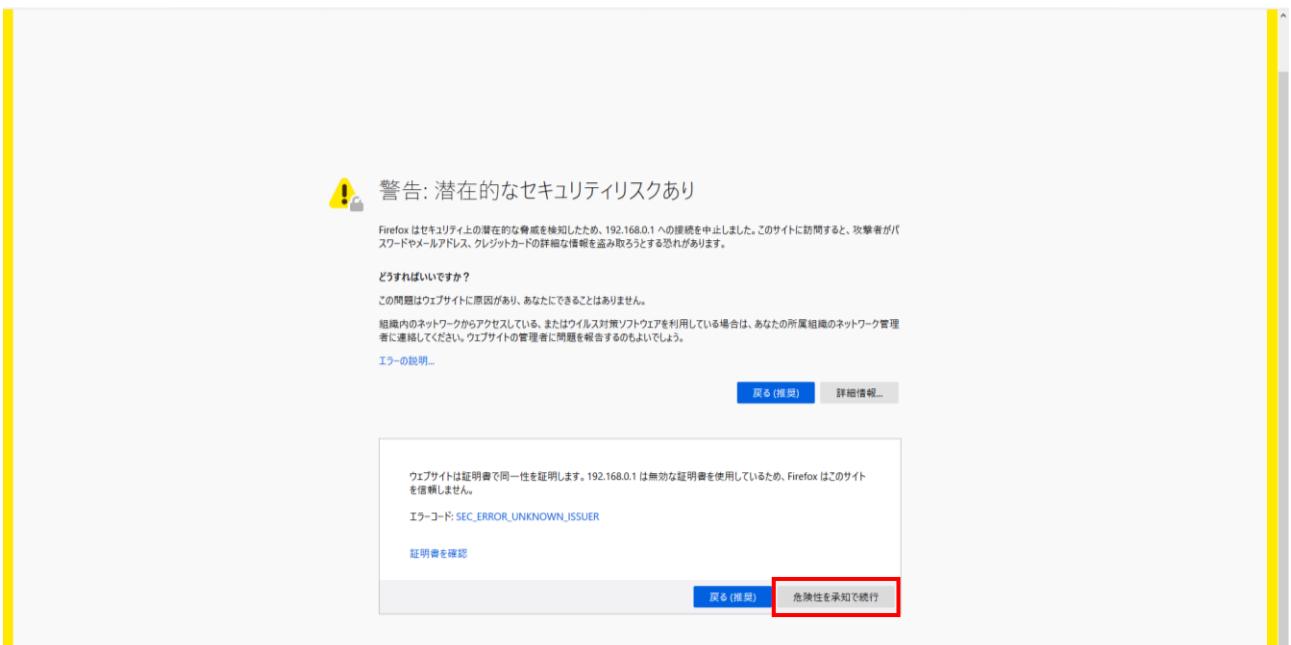
(参考 : Firefox におけるセキュリティ警告画面対処手順)

- ① Firefox を開き、FortiGate にアクセスすると下図のような画面が表示されます。

「詳細情報」をクリックします。



- ② 「詳細情報」クリック後下に展開される画面から「危険性を承知で続行」をクリックします。



- ③ 正常にログイン画面にアクセスできることが確認できます。



2.1.1. ログイン方法

ログイン画面からログインID／パスワードを入力し、「ログイン」をクリックします。



(ログイン後画面イメージ)

2.1.2. ログアウト方法

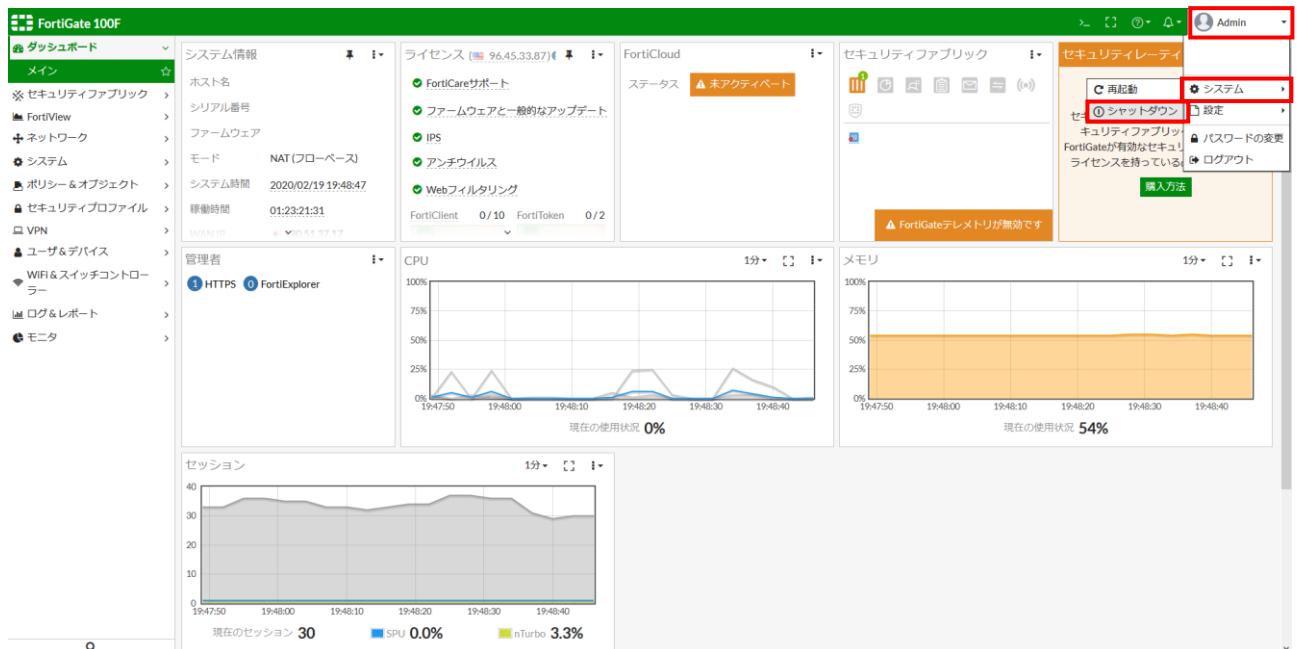
画面右上のログインユーザ名をクリックし、「ログアウト」をクリックします。

The screenshot shows the FortiGate 100F dashboard with various monitoring and configuration sections. In the top right corner, there is a user profile icon labeled 'Admin'. A red box highlights this area. Below it, a dropdown menu is open, also with a red box highlighting the 'Logout' option. Other options in the dropdown include 'System', 'Setting', 'Password Change', and 'Import Method'. The dashboard includes sections for System Information, Licenses, FortiCloud Status, Security Applications, and Performance Metrics (CPU, Memory, Sessions). A message at the bottom left states '⚠️ FortiGate metrics are invalid'.

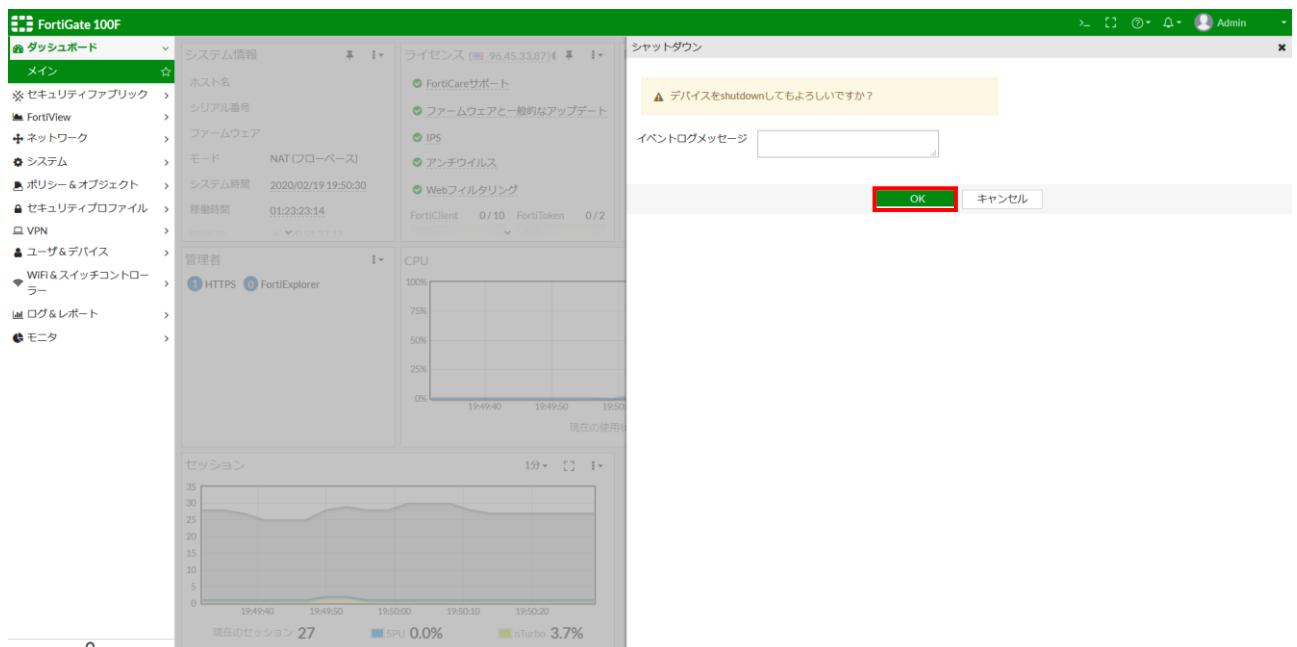
2.2. 電源 OFF/ON・再起動方法

2.2.1. 電源 OFF 方法

- ① 画面右上のログインユーザ名をクリックし、「システム」にカーソルを移動すると展開されるメニューから「シャットダウン」をクリックします。



- ② 任意でイベントログに記録するメッセージを入力し、「OK」をクリックします。

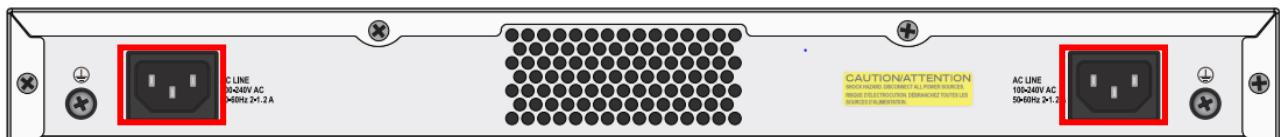


- ③ 下図のような画面が表示され機器がシャットダウンされます。



- ④ FortiGate-100F は機器背面にある AC 電源ケーブルを抜線することで OFF することが出来ます。

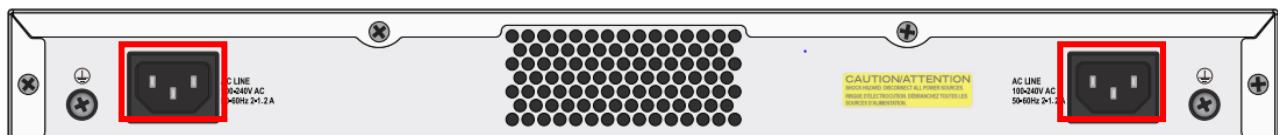
■ FortiGate-100F



2.2.2. 電源 ON 方法

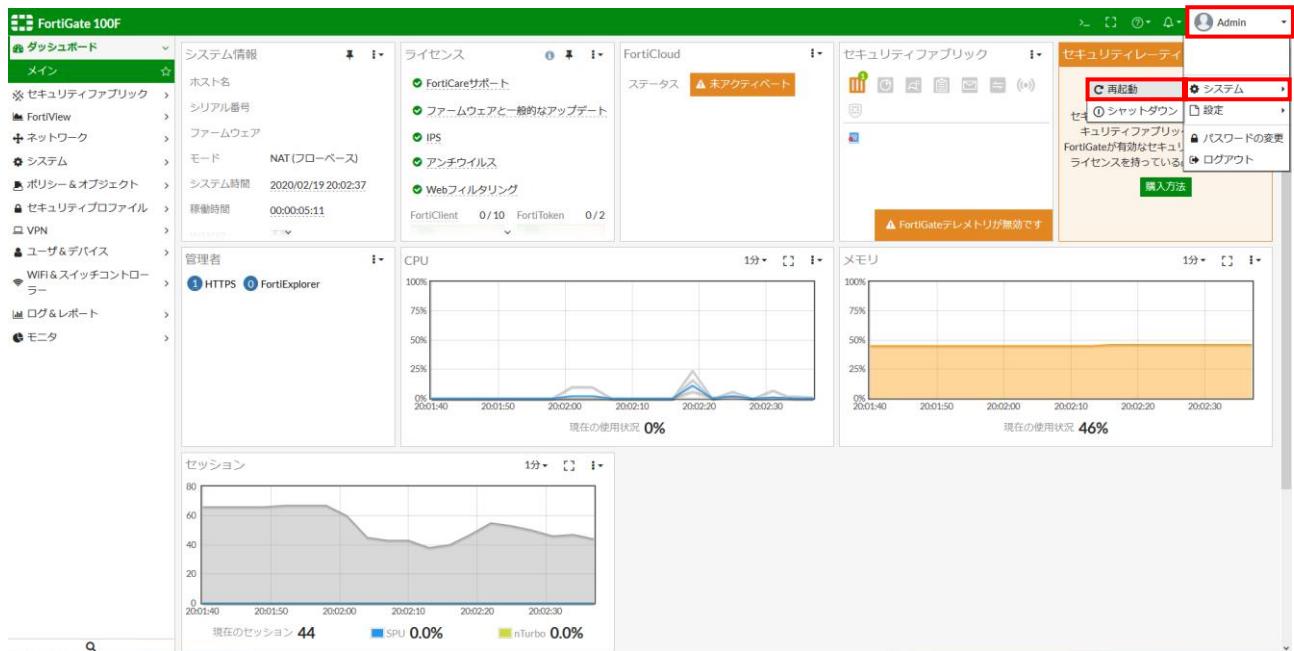
- ① FortiGate-100F は機器背面にある AC 電源ケーブルを結線することで ON にします。

■ FortiGate-100F

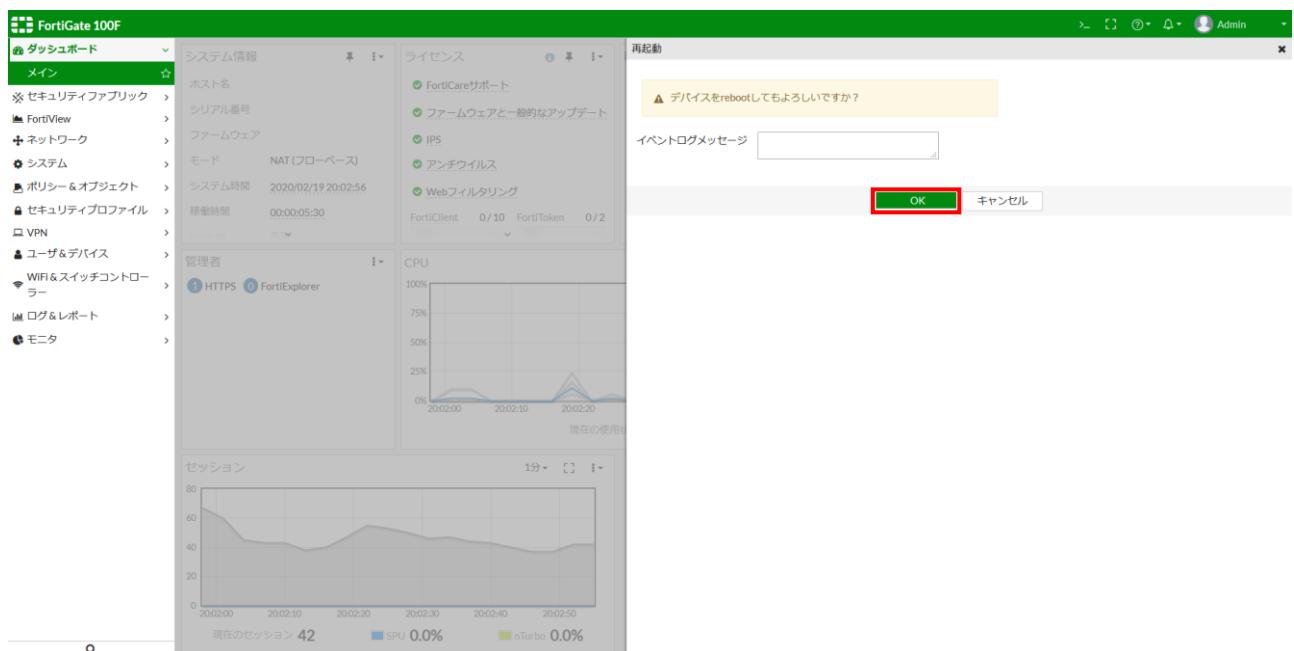


2.2.3. 再起動方法

- ① ログイン後、画面右上のログインユーザ名をクリックし、「システム」にカーソルを移動すると展開されるメニューから「再起動」をクリックします。



- ② 任意でイベントログに記録するメッセージを入力し、「OK」をクリックします。



- ③ 下図のような画面が表示され機器の再起動が始まります。
-



2.3. 管理者パスワード変更

Fortigate の管理者パスワードを変更します。

- ① ログイン後、画面左側のメニューから「システム」をクリックします。

The screenshot shows the Fortigate 100F dashboard. On the left, the navigation menu is open, and the 'System' option under 'Dashboard' is highlighted with a red box. The main content area displays various system status cards and performance graphs for CPU and memory usage.

- ② システムメニューが展開されるので「管理者」をクリックします。

The screenshot shows the 'Administrators' section of the Fortigate 100F system settings. The 'Administrators' option under the 'System' menu is highlighted with a red box. A table lists the current administrator accounts, showing one account named 'Admin' with the role 'super_admin' and type 'ローカル'.

名前	信頼されるホスト	プロファイル	タイプ	二要素認証
Admin		super_admin	ローカル	無効化済み

- ③ パスワード変更対象アカウントを右側の画面で選択して「編集」ボタンをクリック、もしくはアカウントをダブルクリックで編集画面を開きます。

名前	信頼されるホスト	プロファイル	タイプ	二要素認証
Admin		super_admin	ローカル	無効化済み

- ④ 「パスワード変更」をクリックします。

管理者の編集

ユーザ名: Admin

パスワードの変更

ローカルユーザー

リモートサーバグループの特定ユーザーにマッチ
リモートサーバグループのすべてのユーザーにマッチ
public key infrastructure (PKI) グループを利用

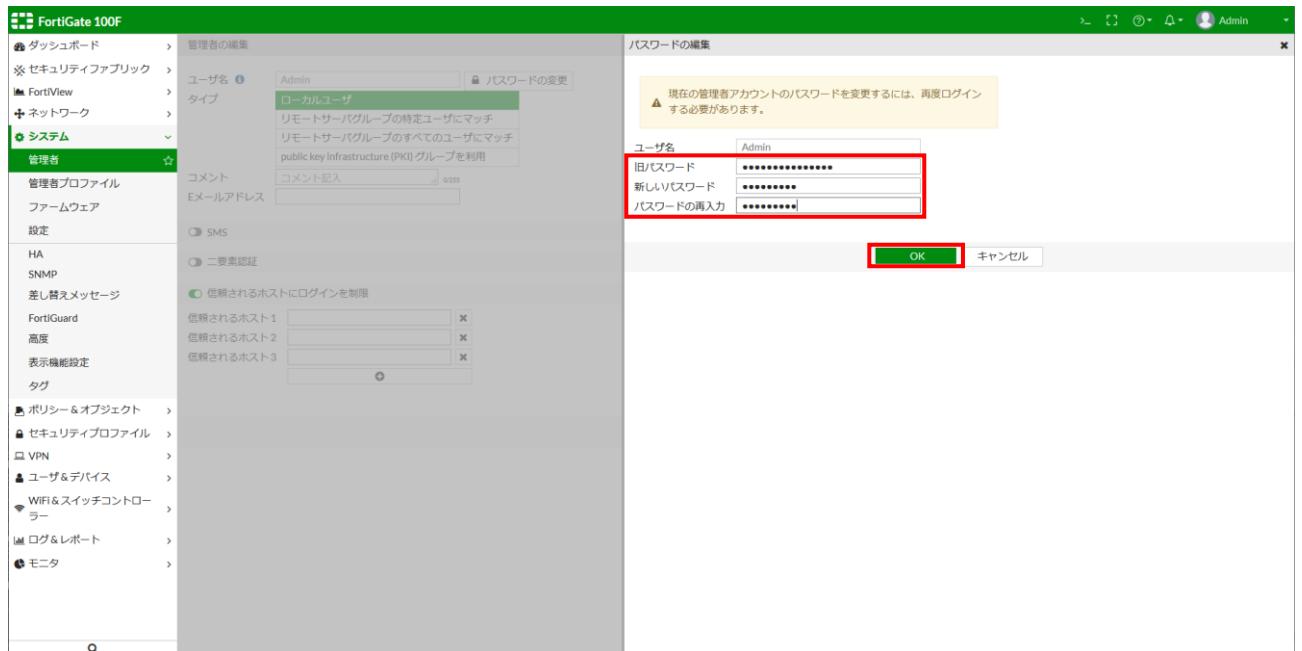
コメント: コメント記入 [6255]
Eメールアドレス:

SMS
二要素認証
信頼されるホストにログインを制限

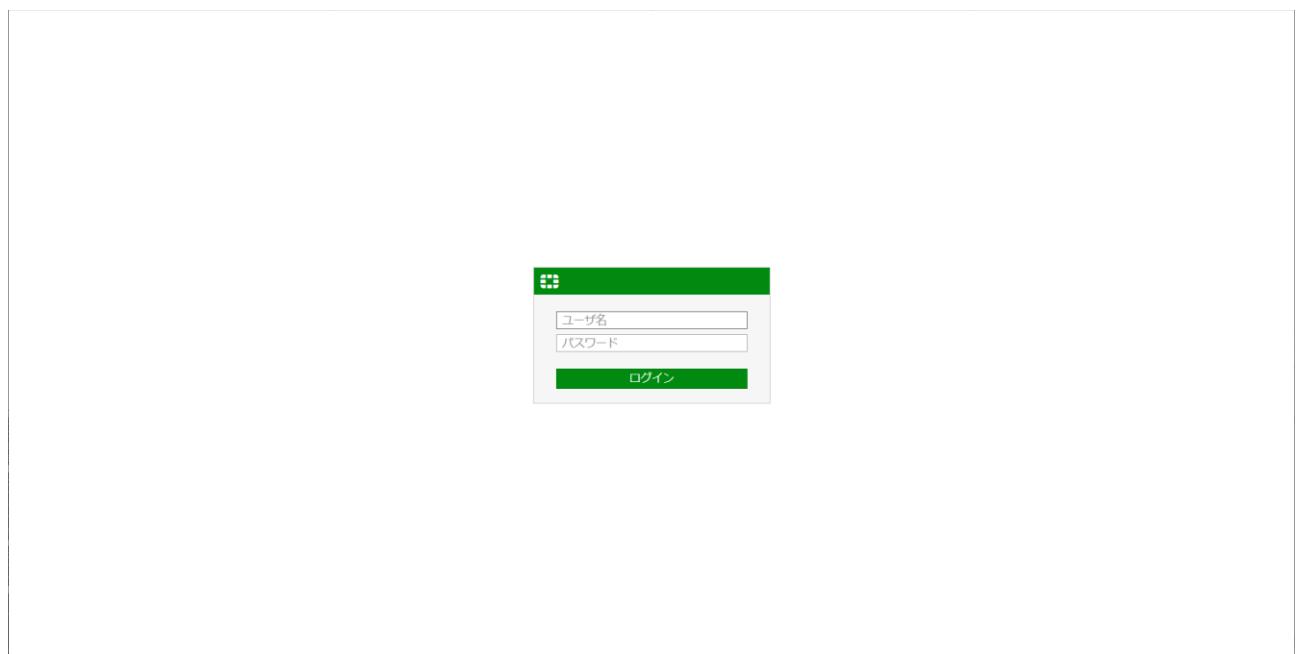
信頼されるホスト 1: []
信頼されるホスト 2: []
信頼されるホスト 3: []

OK キャンセル

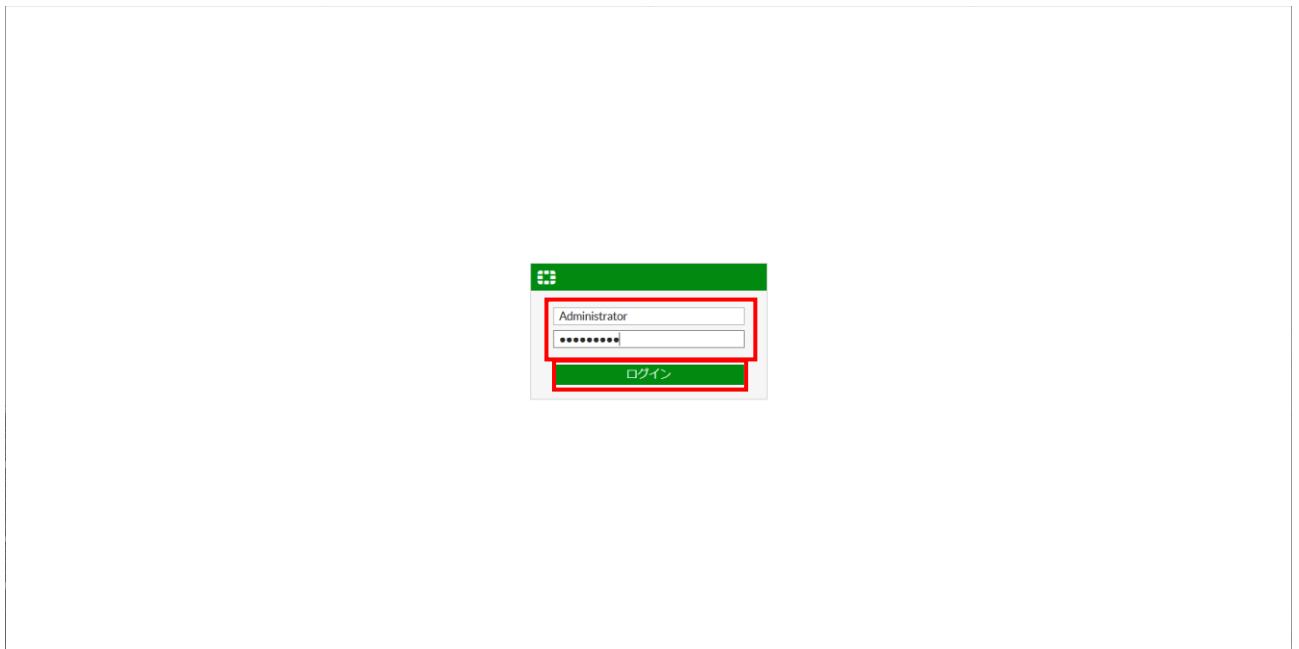
- ⑤ パスワード編集画面が展開されるので、「旧パスワード」には現在のパスワードを、「新しいパスワード」と「パスワードの再確認」に変更するパスワードを入力して「OK」をクリックします。



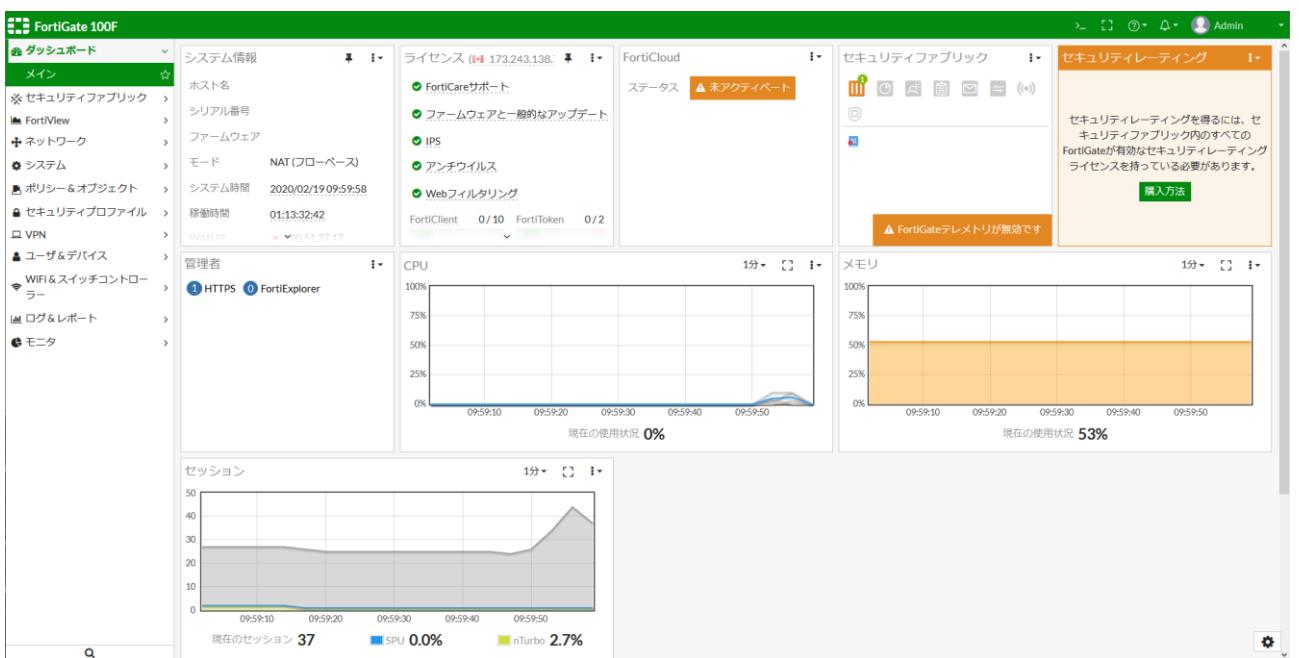
- ⑥ 自動的にログアウトされ、ログイン画面が表示されます。



⑦ 変更したパスワードを入力してログインします。



⑧ 正常にログインできることを確認します。

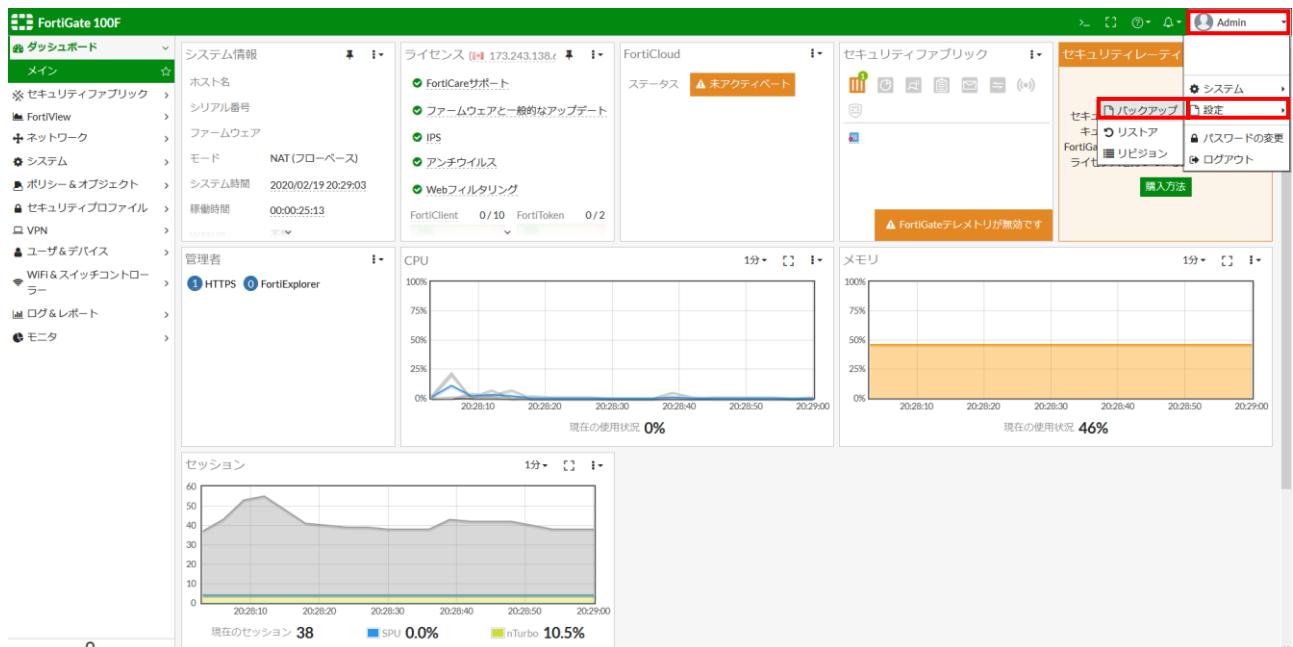


2.4. 設定のバックアップ・リストア方法

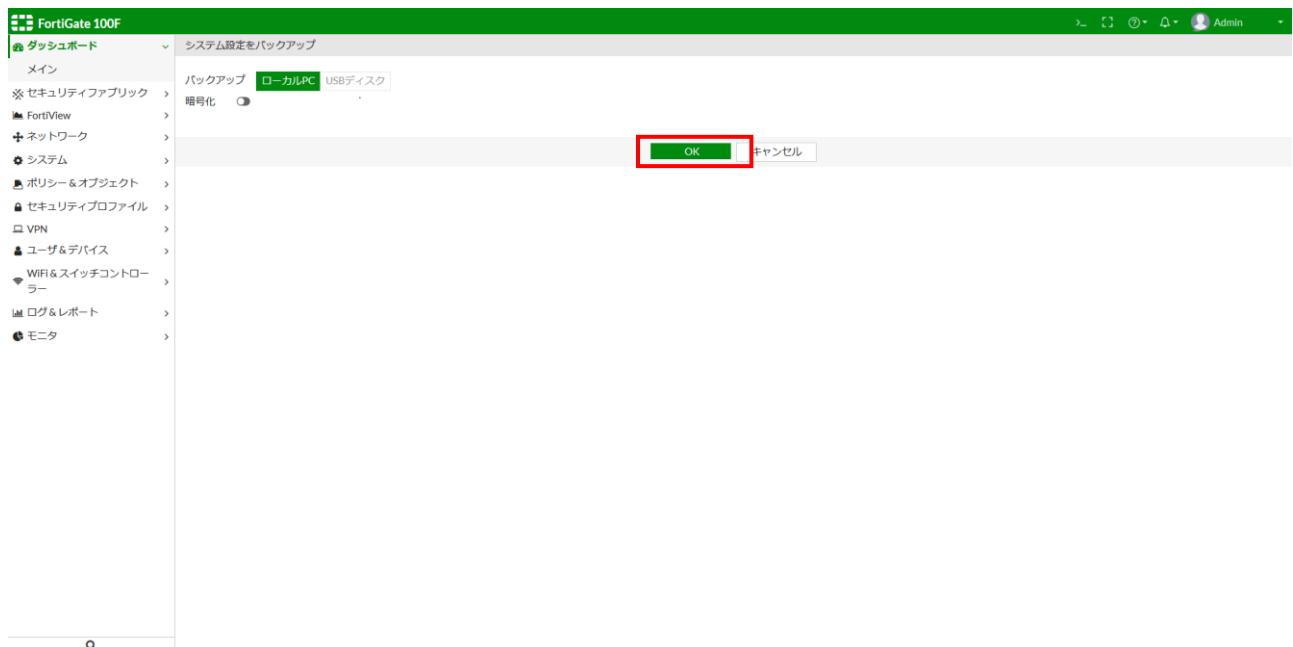
2.4.1. 設定のバックアップ方法

FortiGate の設定情報を端末に保存します。

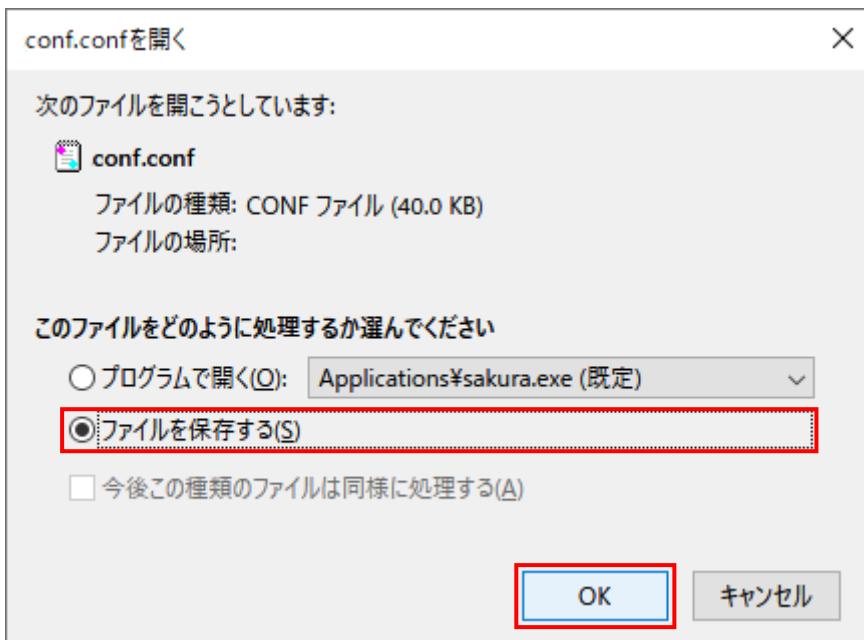
- ① ログイン後、画面右上のログインユーザ名をクリックし、「設定」にカーソルを移動すると展開されるメニューから「バックアップ」をクリックします。



- ② 「システム設定をバックアップ」画面に遷移しますので「OK」をクリックします。



- ③ ファイル保存のポップアップが表示されますので「ファイルを保存する」を選択し、「OK」をクリックします。



※ファイル保存場所やファイル名を指定して保存したい場合はブラウザの設定を変更してください。

(Firefox の場合)

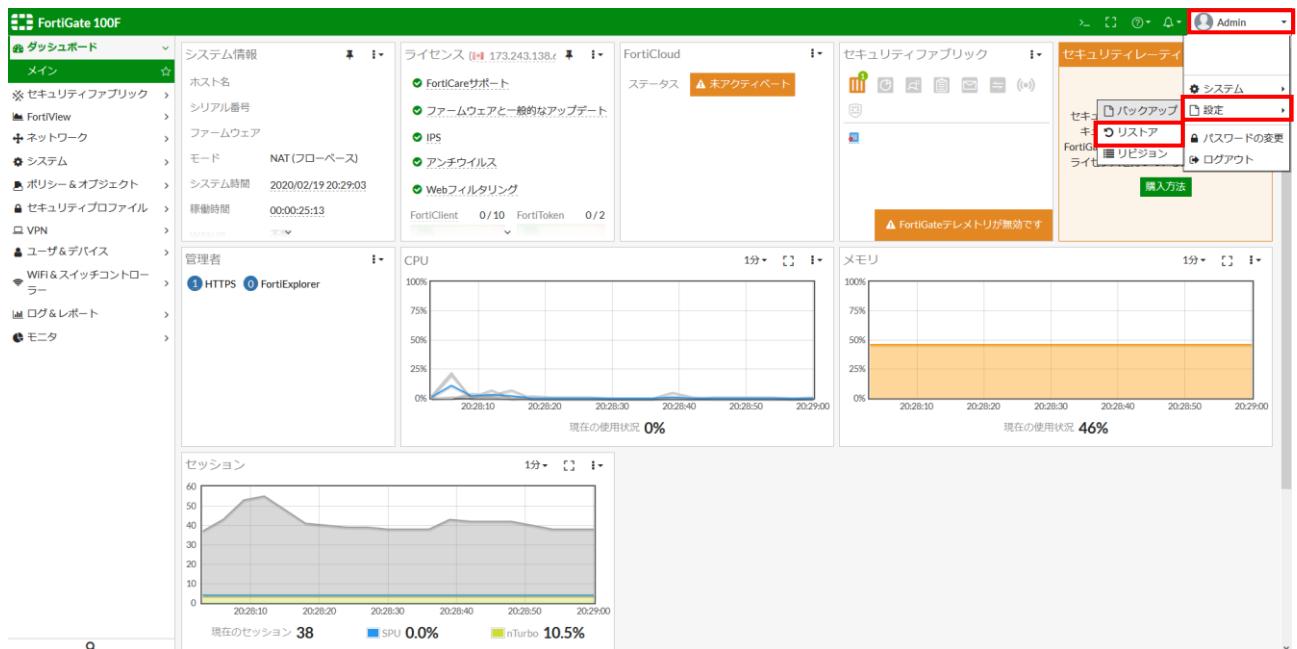
オプションのダウンロード設定から「ファイルごとに保存先を指定する」を選択します。



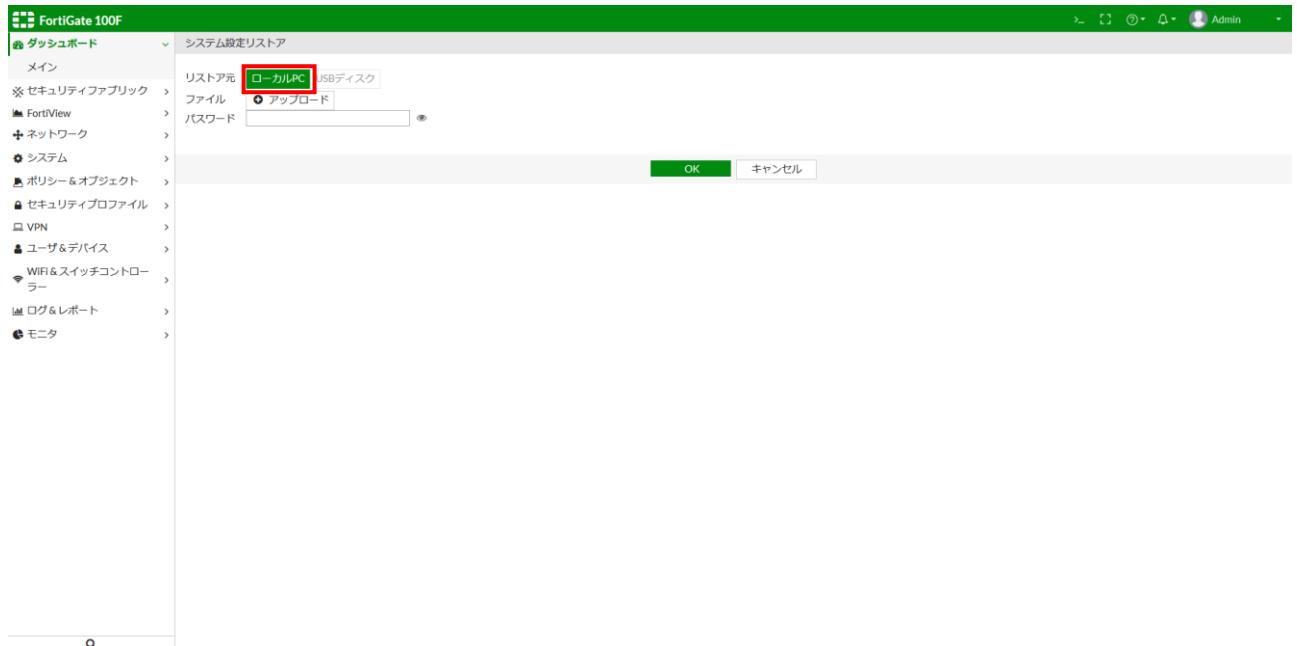
2.4.2. 設定のリストア方法

FortiGate のバックアップファイルをリストアします。

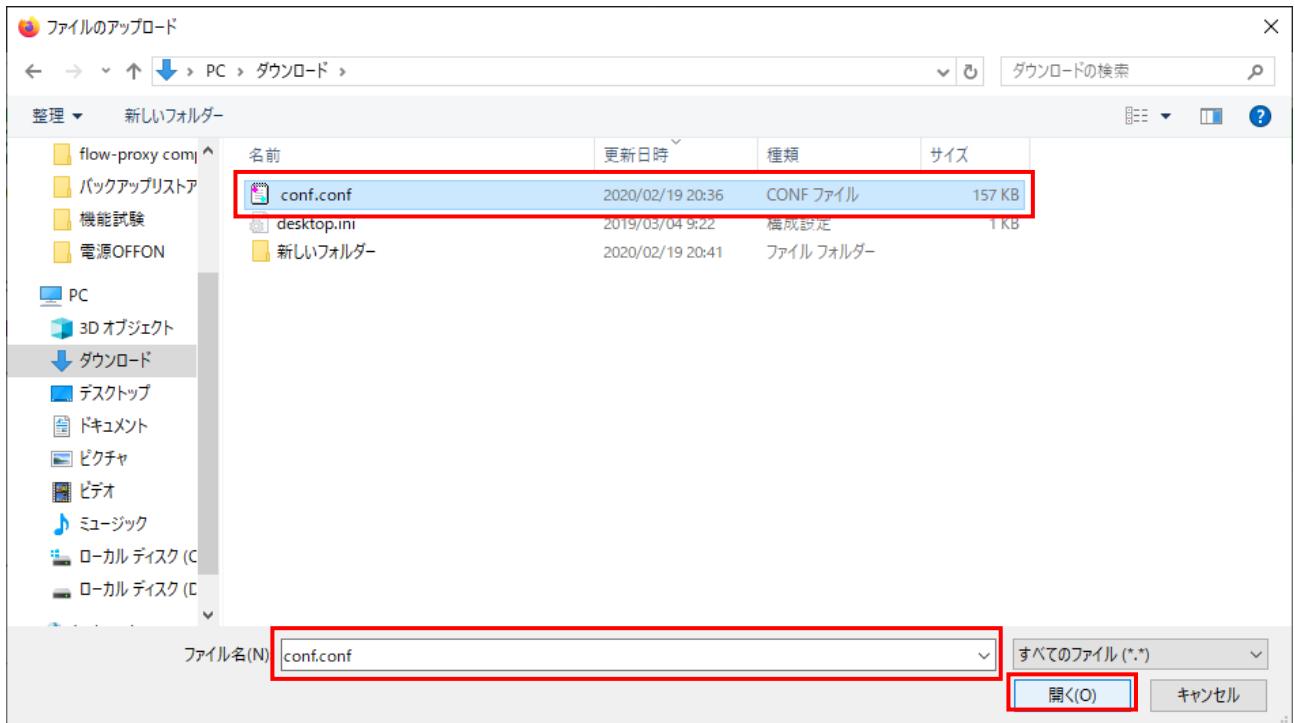
- ① ログイン後、画面右上のログインユーザ名をクリックし、「設定」にカーソルを移動すると展開されるメニューから「リストア」をクリックします。



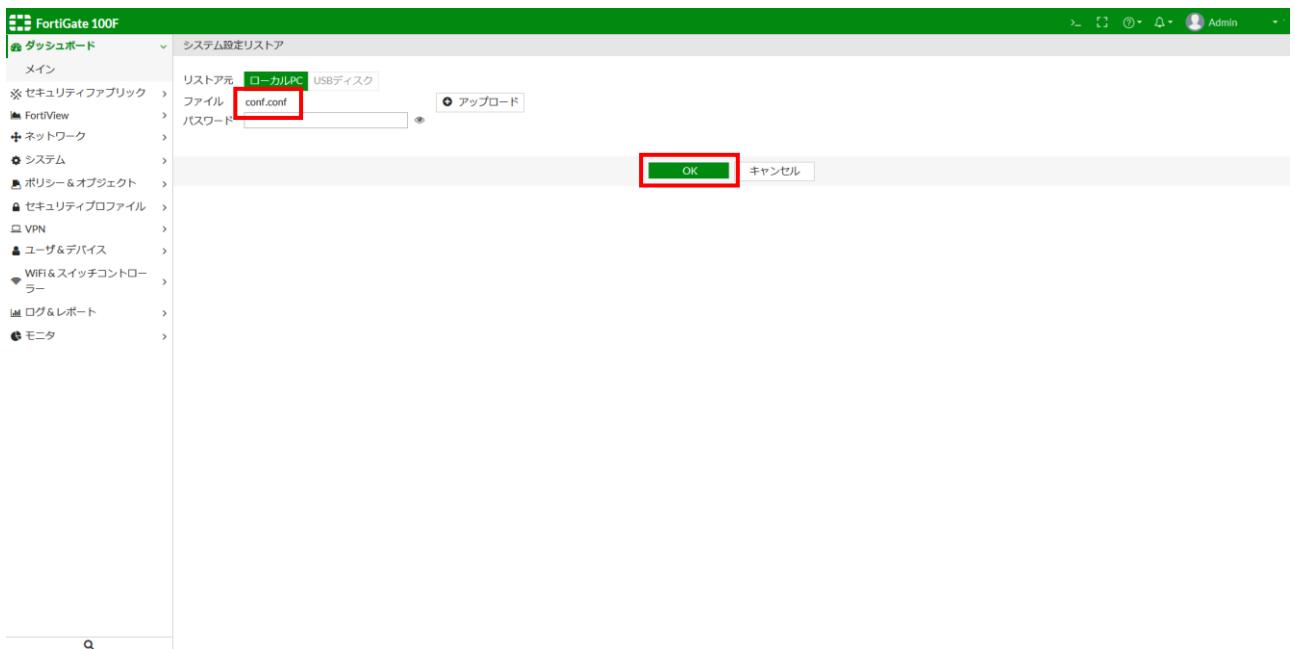
- ② 「システム設定リストア」画面に遷移しますので「アップロード」をクリックします。



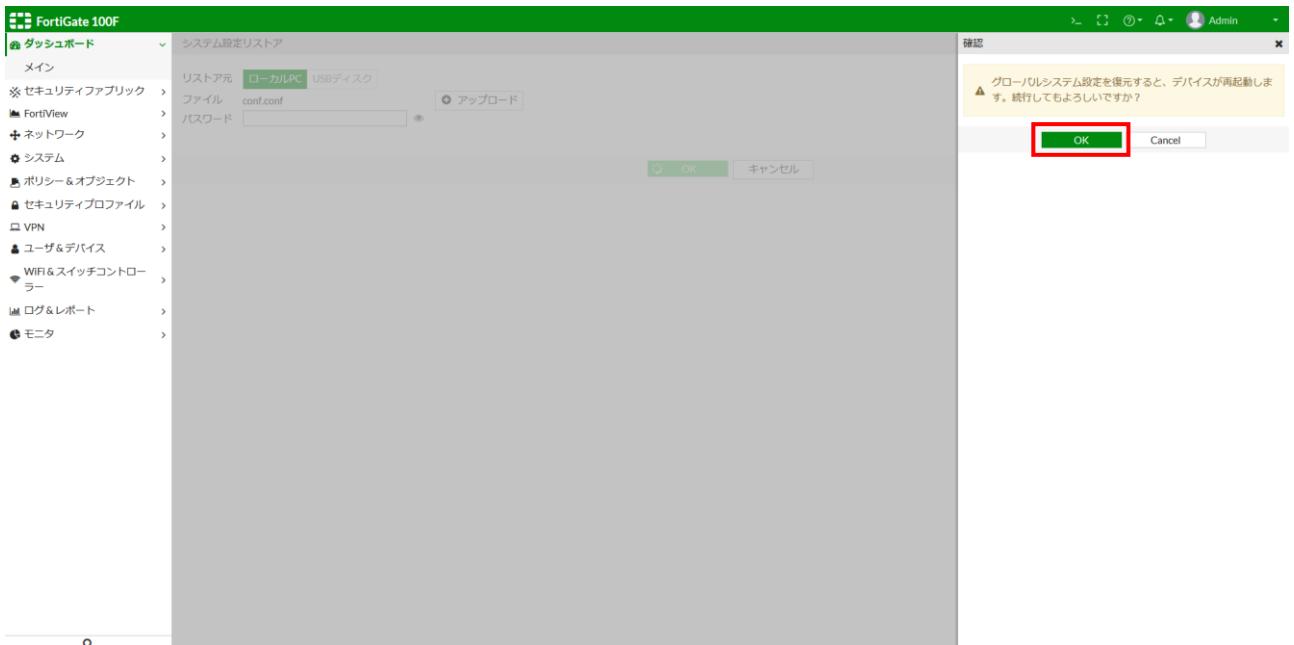
- ③ ファイルのアップロードのポップアップが表示されますので
リストアするバックアップファイルを選択し、「開く」をクリックします。



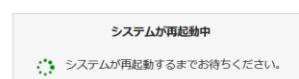
- ④ 「システム設定リストア」画面の「File」欄に選択したバックアップファイル名が
表示されていることを確認し、「OK」をクリックします。



- ⑤ 下図のような確認画面が表示されるので「OK」をクリックします。



- ⑥ 設定がリストアされ再起動が開始されます。



2.5. ログ閲覧方法

2.5.1. 転送トラフィックログ観覧方法

「ログ&レポート」→「転送トラフィック」の順に選択して転送トラフィックログを確認します。

The screenshot shows the FortiGate 100F dashboard with the 'Forward Traffic' log list highlighted. The left sidebar shows various log categories like Security Applications, Network, System, and more. The main area displays a table of logs with columns: #, 日/時 (Date/TIME), 送信元 (Source),宛先 (Destination), アプリケーション名 (Application Name), セキュリティイベント (Security Event), and ログ詳細 (Log Detail). A red box highlights the log table. A tooltip in the top right corner says '詳細を表示するには、ログエントリを選択します。' (Select the log entry to view details).

2.5.2. システムイベントログ観覧方法

「ログ&レポート」→「システムイベント」の順に選択してシステムイベントログを確認します。

The screenshot shows the FortiGate 100F dashboard with the 'System Event' log list highlighted. The left sidebar shows various log categories like Security Applications, Network, System, and more. The main area displays a table of logs with columns: #, 日/時 (Date/TIME), レベル (Level), ユーザ (User), and メッセージ (Message). A red box highlights the log table. A tooltip in the top right corner says '詳細を表示するには、ログエントリを選択します。' (Select the log entry to view details).

2.5.3. Web フィルタログ閲覧方法

「ログ&レポート」→「Web フィルタ」の順に選択して Web フィルタログを確認します。

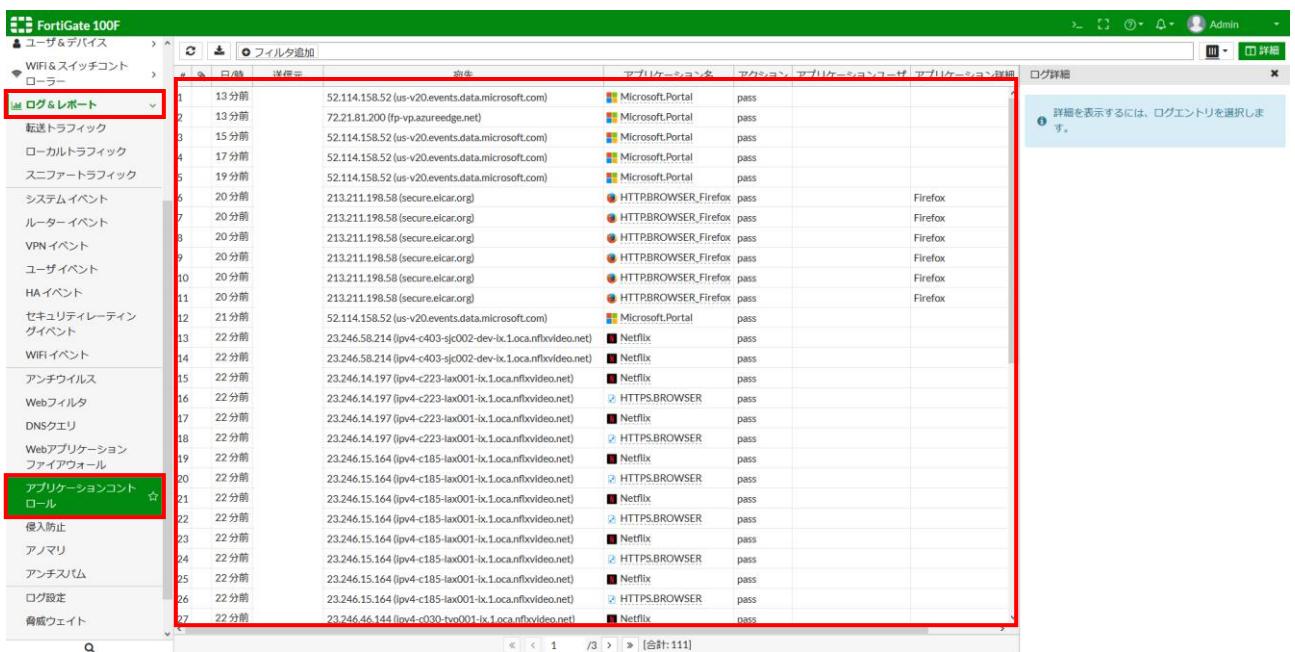
The screenshot shows the FortiGate 100F web interface. The left sidebar has a tree view with categories like 'ユーザ & デバイス', 'WiFi & スイッチコント', 'ローラー', and 'ログ&レポート'. Under 'ログ&レポート', 'Web フィルタ' is selected and highlighted with a red box. The main content area displays a table of log entries with columns: #, 日時, コード, 送信元, URL, カテゴリ, 説明, 送信/受信, and ログ詳細. A red box highlights the entire content area. A tooltip in the top right corner says '詳細を表示するには、ログエントリを選択します。' (To view details, select a log entry.).

#	日時	コード	送信元	URL	カテゴリ	説明	送信/受信	ログ詳細
1	2時間前	192.168.0.210	blocked	www.jra.go.jp/	ギャンブル		377 B / 0 B	
2	2時間前	192.168.0.210	blocked	www.asahibeer.co.jp/	アルコール		517 B / 0 B	
3	2時間前	192.168.0.210	blocked	ero-nuki.net/	ボルノ		517 B / 0 B	
4	2時間前	192.168.0.210	blocked	www.jra.go.jp/favicon.ico	ギャンブル		264 B / 0 B	
5	2時間前	192.168.0.210	blocked	www.jra.go.jp/	ギャンブル		343 B / 0 B	

2.5.4. アプリケーションコントロールログ観覧方法

「ログ&レポート」→「アプリケーションコントロール」の順に選択して、

アプリケーションコントロールログを確認します。



順位	日付	詳細元	アクション	ア�플리케ーション名	ア�플리케ーションポート	ア�플리케ーション状態
1	13 分前	52.114.158.52 (us-v20.events.data.microsoft.com)	Microsoft.Portal	pass		
2	13 分前	72.21.81.200 (fp-vp.azureedge.net)	Microsoft.Portal	pass		
3	15 分前	52.114.158.52 (us-v20.events.data.microsoft.com)	Microsoft.Portal	pass		
4	17 分前	52.114.158.52 (us-v20.events.data.microsoft.com)	Microsoft.Portal	pass		
5	19 分前	52.114.158.52 (us-v20.events.data.microsoft.com)	Microsoft.Portal	pass		
6	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
7	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
8	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
9	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
10	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
11	20 分前	213.211.198.58 (secure.elcar.org)	HTTPBROWSER_Firefox	pass	Firefox	
12	21 分前	52.114.158.52 (us-v20.events.data.microsoft.com)	Microsoft.Portal	pass		
13	22 分前	23.246.58.214 (ipv4-c403-sjC002-dev-ix.1.oca.nfxfvideo.net)	Netflix	pass		
14	22 分前	23.246.58.214 (ipv4-c403-sjC002-dev-ix.1.oca.nfxfvideo.net)	Netflix	pass		
15	22 分前	23.246.14.197 (ipv4-c223-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
16	22 分前	23.246.14.197 (ipv4-c223-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
17	22 分前	23.246.14.197 (ipv4-c223-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
18	22 分前	23.246.14.197 (ipv4-c223-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
19	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
20	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
21	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
22	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
23	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
24	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
25	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	Netflix	pass		
26	22 分前	23.246.15.164 (ipv4-c185-lax001-ix.1.oca.nfxfvideo.net)	HTTPS.BROWSER	pass		
27	22 分前	23.246.46.144 (ipv4-c030-tvp001-ix.1.oca.nfxfvideo.net)	Netflix	pass		

2.6. セキュリティプロファイルの設定

2.6.1. アンチウィルスの設定

[アンチウィルスプロファイルにて特定シグネチャの除外ルールを設定する方法]

アンチウィルスのセキュリティプロファイルでは除外ルールを設定する機能はございません。アンチウィルスのログ情報でブロックされたファイルの宛先 IP アドレスおよびポート情報をポリシーに登録して許可する方法で実現します。

- ① 下図のブロックされている除外設定対象ファイルの詳細情報をダブルクリックで確認します。
宛先 IP アドレスおよびポート番号を控えてください。

The screenshot shows the FortiGate 100F web interface under the 'Logs & Reports' section. A single log entry is selected, showing a blocked file named 'sample.zip' from host 'host'. The detailed view on the right side highlights the 'Destination' section, which includes the IP address '192.168.100.231' and port '80'. Other details like session ID, user, and URL are also visible.

- ② ①で控えた IP アドレス情報を用いて、手順「2.7.2 アドレス設定」を参考し宛先 IP アドレスオブジェクトを作成します。
- ③ ①で控えたポート番号を用いて、手順「2.7.3 サービス設定」を参考しサービスオブジェクトを作成します。作成する際、プロトコルは TCP/UDP の両方とも指定します。
- ④ ②と③で生成したアドレスオブジェクトとサービスオブジェクトを用いて、「手順 2.7.1 ポリシー設定」を参考し例外ポリシーを作成します。
【注意】作成したポリシーは必ずアンチウィルスフィルタ適用中の既存のポリシーの上に配置する必要があります。

2.6.2. Web フィルタ設定

Web フィルタ設定では、URL フィルタと FortiGuard カテゴリによるフィルタにて Web 閲覧を制御します。

お客様環境では FortiGuard カテゴリによるフィルタと個別 URL のフィルタを利用しています。

A) 特定カテゴリの許可/ブロック

(例) P2P ファイル共有カテゴリの許可

- ① 「セキュリティプロファイル」→「Web フィルタ」→「Web フィルタプロファイル」→「Web フィルタプロファイル名」を選択し、「編集」ボタンを押下します。

The screenshot shows the FortiGate 1100E configuration interface under the 'セキュリティプロファイル' (Security Profiles) section. The left sidebar highlights the 'セキュリティプロファイル' section, and the main area shows the 'Web フィルタ' (Web Filtering) profile list. A red box highlights the 'WF' icon next to the 'wf-prof_HD' profile, which is selected and highlighted in yellow. Another red box highlights the '編集' (Edit) button at the top of the list.

名前	コメント	参照
WEB default	Default web filtering.	0
WEB wf-prof_HD		2
WEB wf-prof_IEMS		8
WEB wf-prof_Lab		3
WEB wif-default	Default configuration for offloading WiFi traffic.	1

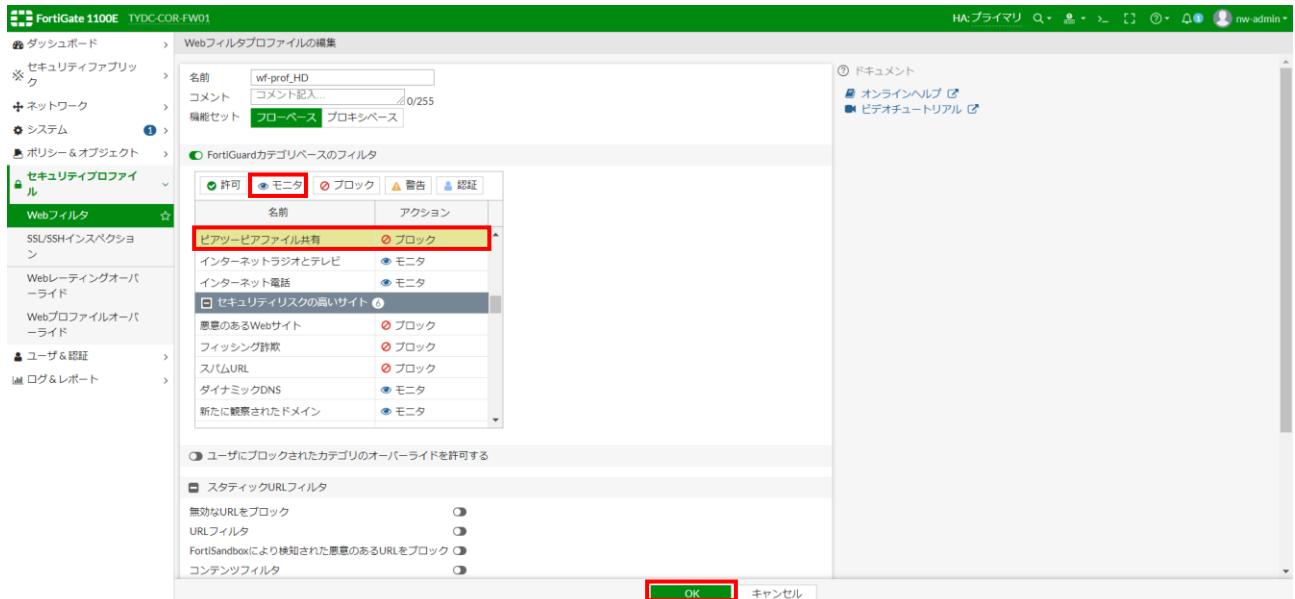
- ② 「FortiGuard カテゴリベースのフィルタ」→「特定カテゴリ」を選択し、アクションを選択します。

アクションは以下の 2 パターンからお選びください。

許可する場合：モニタ

ブロックする場合：ブロック

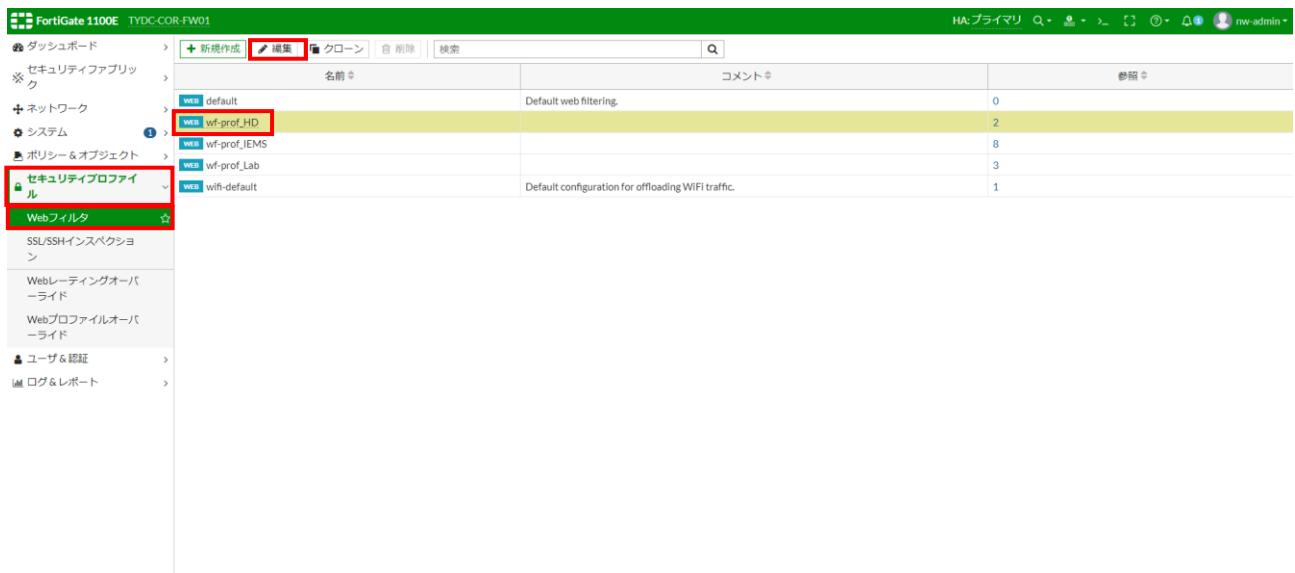
アクションを選択後、「OK」ボタンを押下します。



B) 特定サイトの許可/ブロック

(例 2) URL フィルタに閲覧許可サイトを追加

- ① 「セキュリティプロファイル」→「Web フィルタ」→「Web フィルタプロファイル」→「Web フィルタプロファイル名」を選択し、「編集」ボタンを押下します。



- ① URL フィルタの「On/Off ボタン」をクリックして有効化します。

The screenshot shows the FortiGate 100F configuration interface under the 'Webフィルタ' tab. In the 'URLフィルタ' section, the '不正なURLをブロック' (Block Malicious URLs) checkbox is checked, and the 'URLフィルタ' (URL Filter) switch is turned on. The '適用' (Apply) button is visible at the bottom right.

- ② 展開された URL フィルタ入力欄の「新規作成」をクリックします。

The screenshot shows the FortiGate 100F configuration interface under the 'Webフィルタ' tab. The 'URLフィルタ' list table has a new row highlighted with a red border, and the '+ 新規作成' (New Rule Creation) button is visible above it. The '適用' (Apply) button is also present at the bottom right.

- ③ 「URL」を入力、「タイプ」「アクション」を選択し、「OK」を実行します。

・ URL に入力する情報

許可する URL パスを記入してください。「http://」や「https://」は不要です。

パスは完全一致で大小文字を区別します。例えば、「example.com」では「www.example.com」は制御できません。

ワイルドカード「*」の指定も可能です。

ドメイン全体を指定する際は「example.com」と「*.example.com」の両方を指定する必要があります。

・ タイプの選択

URL にワイルドカード「*」が含まれる場合は【ワイルドカード】を選択し、それ以外は【シンプル】を選択します。

・ アクションの選択

接続を許可する場合、【除外(exempt)】を選択します。

接続をブロックする場合、【ブロック】を選択します。



- ④ 「OK」を押下します。

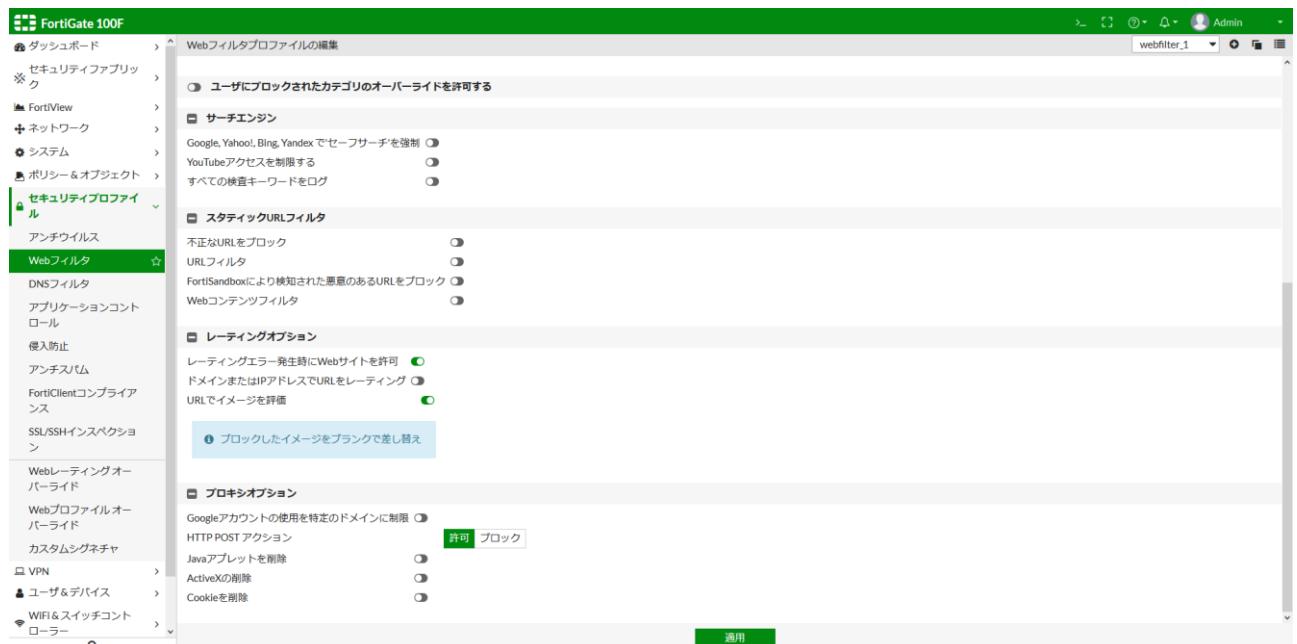
- ⑤ URL フィルタに登録された URL を削除する場合は、削除したい URL をクリックし、「削除」ボタンをクリックします。

The screenshot shows the 'Webフィルタプロファイルの編集' (Edit Web Filter Profile) screen. In the 'URLフィルタ' (URL Filter) section, there is a table with one row containing 'defense.gov'. The 'Actions' column for this row has a red box around the 'Delete' button. Below the table, there is a note: 'FortiSandboxにより検知された恶意のあるURLをブロック' (Block URLs detected by FortiSandbox as malicious). At the bottom right of the page, there is a green '適用' (Apply) button.

- ⑥ 削除後「適用」をクリックします。

The screenshot shows the same 'Webフィルタプロファイルの編集' screen after the URL 'defense.gov' has been deleted. The note 'マッチするエントリーはありません。' (No matching entries found.) is displayed. The green '適用' (Apply) button at the bottom right is highlighted with a red box.

- ⑦ 適用後削除結果が反映され、登録された URL フィルタの条件が一つもない場合、自動的に無効状態へ戻ります。



2.6.3. プリケーションコントロール設定

- ① 「セキュリティプロファイル」→「アプリケーションコントロール」→「アプリケーションセンター」バーの右奥「プロファイル名▼」→「app-prof_default」の順に選択します。

The screenshot shows the FortiGate 100F configuration interface. The left sidebar navigation includes: ダッシュボード, セキュリティプロファイル (highlighted with a red box), ネットワーク, システム, ポリシー & オブジェクト, アプリケーションコントロール (highlighted with a red box), 侵入防止, アンチスパム, FortiClientコンプライアンス, SSL/SSHインスペクション, Webレーティングオーバーライド, Webプロファイルオーバーライド, カスタムシグネチャ, VPN, ユーザ&デバイス, WiFi&スイッチコントローラー. The main panel title is 'アプリケーションセンサーの編集'. It shows a profile named 'default' with a comment 'Monitor all applications.' A note says '97個のクラウドアプリケーションはディープインスペクションが必要です。' Below it, there's a 'カテゴリ' section with various application categories like Business, Cloud.I.T, Collaboration, etc., each with a count. Under 'アプリケーションオーバーライド', there's a table for 'シグネチャ' (Signature) with columns 'アクション' (Action) and 'カテゴリ' (Category). The 'モニタ' (Monitor) action is selected. At the bottom right, there's a '適用' (Apply) button.

- ② アプリケーションのアクションアイコンをクリックし、変更したいアクションをクリックします。

This screenshot shows the same FortiGate 100F configuration interface as the previous one, but with a different profile selected. The profile 'block_P2P' is now highlighted with a red box. The 'モニタ' (Monitor) action is still selected in the 'シグネチャ' (Signature) table. The rest of the interface remains the same, including the sidebar navigation and the main configuration panel.

③ 「適用」をクリックして、右下に「変更が更新されました」と通知されることを確認します。

The screenshot shows the FortiGate 100F web interface for managing application signatures. The left sidebar contains navigation links like Dashboard, Security Policies, Network, System, and Application Context. The main content area is titled 'Application Signature Editor' and shows a list of signatures. A message at the top right says '97個のクラウドアプリケーションはディープインスペクションが必要です。 1個のポリシーがこのプロファイルを使用しています。'. Below this, there's a table for adding signatures, a filter table, and an options section with a 'Block' button. A red box highlights the green 'Apply' button at the bottom right. To its right, a red box highlights a green notification bar that says '設定が更新されました'.

2.6.4. 侵入防止（IPS）設定

- ① 「セキュリティプロファイル」→「侵入防止」→「IPS センサーの編集」バーの右奥「プロファイル名▼」→「ips-prof_default」の順に選択します。

有効	シグネチャ	しきい値	期間(秒)	トラック	アクション	ブロック時間(分)
○	Apache.OptionsBleed.Scanner	10	50	Any	● ブロック	None
○	Apache.Tomcat.HTTP2.DoS	50	2	Any	● ブロック	None
○	Apache.Tomcat.HTTP2.GOAWAY.Frame.DoS	30	1	Any	● ブロック	None
○	Apache.Traffic.Server.HTTTP2.Settings.Flood.DoS	39	1	Any	● ブロック	None
○	Cisco.Adaptive.Security.Appliance.SIP.Handling.DoS	100	1	Any	● ブロック	None
○	Digium.Asterisk.Chan.skinny.SCCP.Memory.Exhaustion.DoS	100	10	Any	● ブロック	None
○	Digium.Asterisk.RTP.Stack.Information.Disclosure	20	1	Any	● ブロック	None
○	DnsMasq.DNS.Handling.Out.Of.Memory.DoS	5	2	Any	● ブロック	None

- ② 展開された画面の「+シグネチャ追加」ボタンをクリックします。

有効	シグネチャ	しきい値	期間(秒)	トラック	アクション	ブロック時間(分)
○	Apache.OptionsBleed.Scanner	10	50	Any	● ブロック	None
○	Apache.Tomcat.HTTP2.DoS	50	2	Any	● ブロック	None
○	Apache.Tomcat.HTTP2.GOAWAY.Frame.DoS	30	1	Any	● ブロック	None
○	Apache.Traffic.Server.HTTTP2.Settings.Flood.DoS	39	1	Any	● ブロック	None
○	Cisco.Adaptive.Security.Appliance.SIP.Handling.DoS	100	1	Any	● ブロック	None
○	Digium.Asterisk.Chan.skinny.SCCP.Memory.Exhaustion.DoS	100	10	Any	● ブロック	None
○	Digium.Asterisk.RTP.Stack.Information.Disclosure	20	1	Any	● ブロック	None
○	DnsMasq.DNS.Handling.Out.Of.Memory.DoS	5	2	Any	● ブロック	None
○	critical_high_block				● ブロック	

③ 「+ フィルタ追加」ボタンをクリックします。

The screenshot shows the FortiGate 100F configuration interface. On the left, the navigation menu includes 'IPS Sensor' under 'IPS Signature'. In the center, there's a 'Signature Add' dialog with the 'Filter Add' tab selected. A red box highlights the 'Filter Add' button at the top left of the dialog.

④ 追加したいシグネチャの種類に合わせてフィルタ条件を選択します。

The screenshot shows the FortiGate 100F configuration interface. On the left, the navigation menu includes 'IPS Sensor' under 'IPS Signature'. In the center, there's a 'Signature Add' dialog with the 'Filter Add' tab selected. A red box highlights the 'Type' dropdown menu, which is open and showing options like OS, Action, Application, Target, Protocol, Severity, and Name.

- ⑤ 検索された「シグネチャ」の中で、指定したい項目を選択し、「選択したシグネチャを使用」ボタンをクリックします。

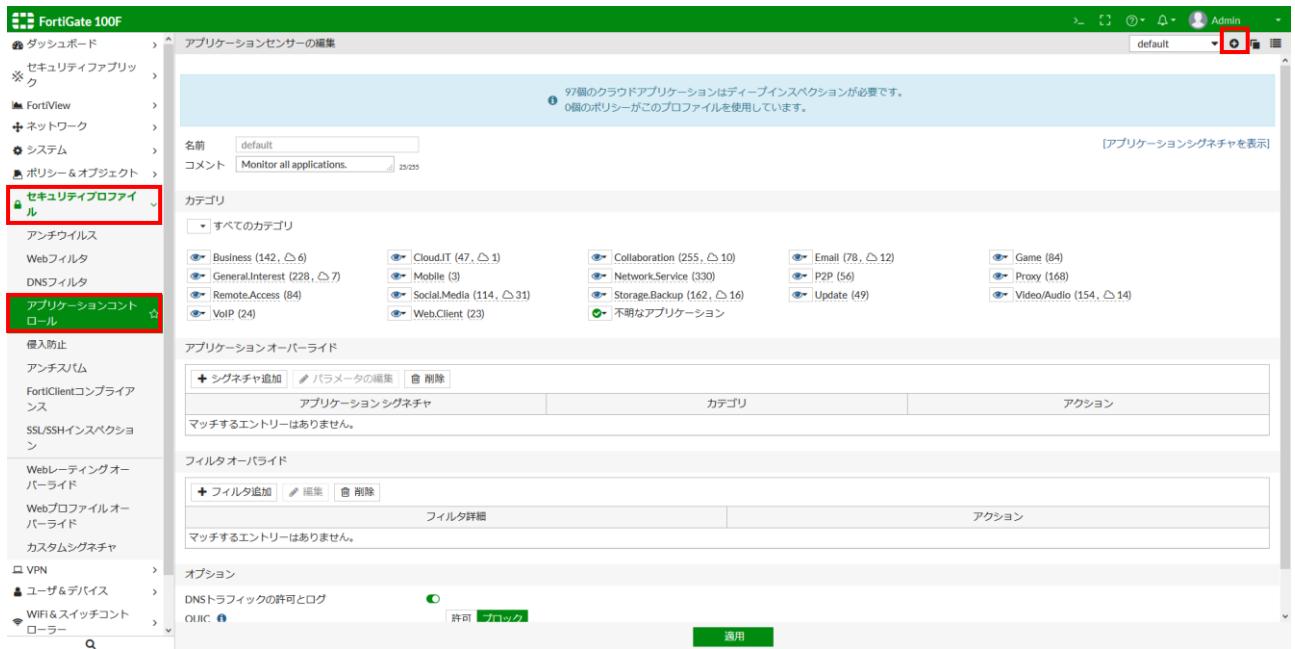
名前	除外IP	重大度	ターゲット	OS
3Com.3CDaemon.FTPServer.Buffer.Overflow		高	サーバ	Windows
3Com.Intelligent.Management.Center.Information.Disclosure		中	サーバ	Windows
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS		中	サーバ	Linux
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		中	サーバ	Linux
3Ivx.MPEG4.File.Processing.Buffer.Overflow		中	クライアント	Windows
7-Zip.RAR.Solid.Compression.Remote.Code.Execution		高	サーバ, クライアント	Windows
74CMS.Config.Controller.Remote.Code.Execution		高	サーバ	Windows, Linux, BSD, Solaris, Mac OS
427BB.CookieBased.Authentication.Bypass		中	サーバ	Other
A32S.Botnet		中	サーバ, クライアント	All
AAEH.Botnet		中	サーバ	All
AARC.Botnet		中	クライアント	All
Aardvark.Topsites.PHP.Remote.Command.Execution		中	サーバ	Windows, Linux, BSD, Solaris, Mac OS
ABBS.Audio.Media.Player.LST.Buffer.Overflow		中	サーバ, クライアント	Windows
ABNR.Botnet		中	サーバ	All
ACal.Calendar.Cookie.Based.Authentication.Bypass		中	サーバ	Windows, Linux, BSD, Solaris, Mac OS
Accellion.FTA.Cookie.Information.Disclosure		中	サーバ	Linux, BSD
Accellion.FTA.getStatus.verify_oauth_token.Command.Injection		高	サーバ	Linux, BSD
ACMEmini_httpd.Arbitrary.File.Read		中	サーバ	Linux
ActFax.RAW.Server.Buffer.Overflow		中	サーバ	Windows
ACTIASOC.Web.Configurator.Remote.Command.Execution		中	サーバ	Other
ActivePDF.Toolkit.Multiple.File.Memory.Corruption		高	サーバ, クライアント	Windows

- ⑥ 追加されたシグネチャを削除したい場合は、IPS シグネチャに追加されたシグネチャを選択し、「削除」ボタンをクリックします。

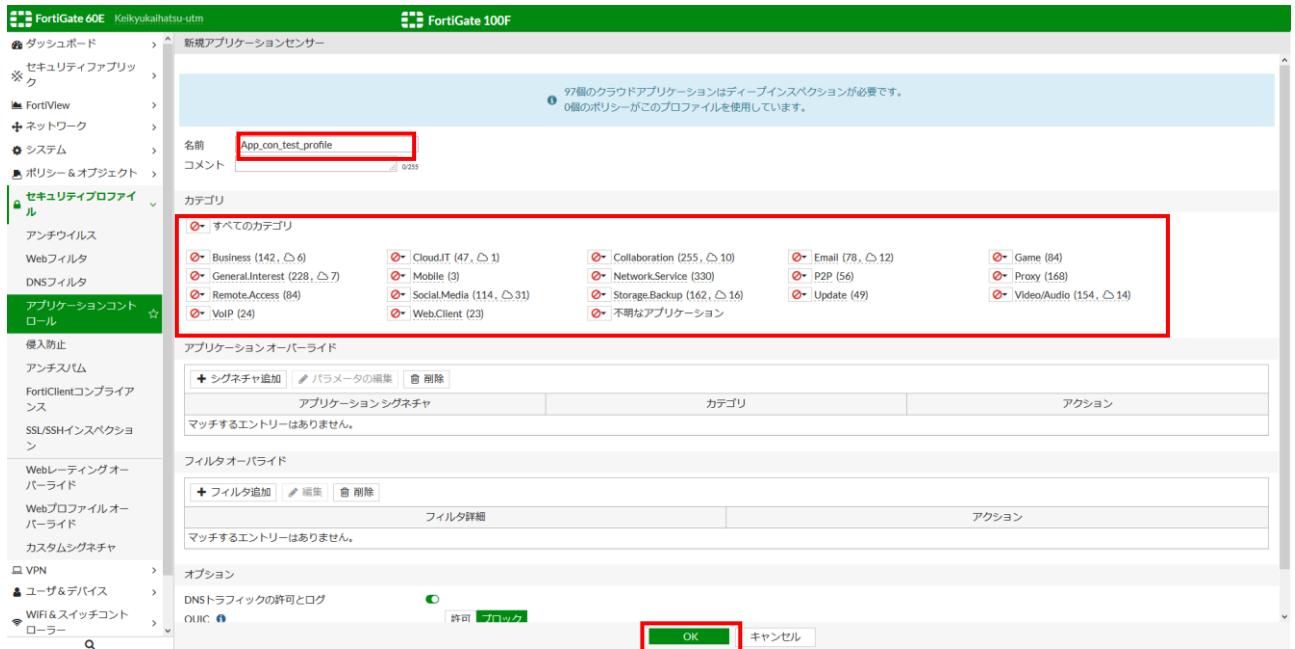
名前	除外IP	重大度	ターゲット	サービス	OS	アクション	パケットロギング
3Com.3CDaemon.FTPServer.Buffer.Overflow	0	高	サーバ	TCP, FTP	Windows	デフォルト	○

2.6.5. 新しいアプリケーションコントロールプロファイルの作成

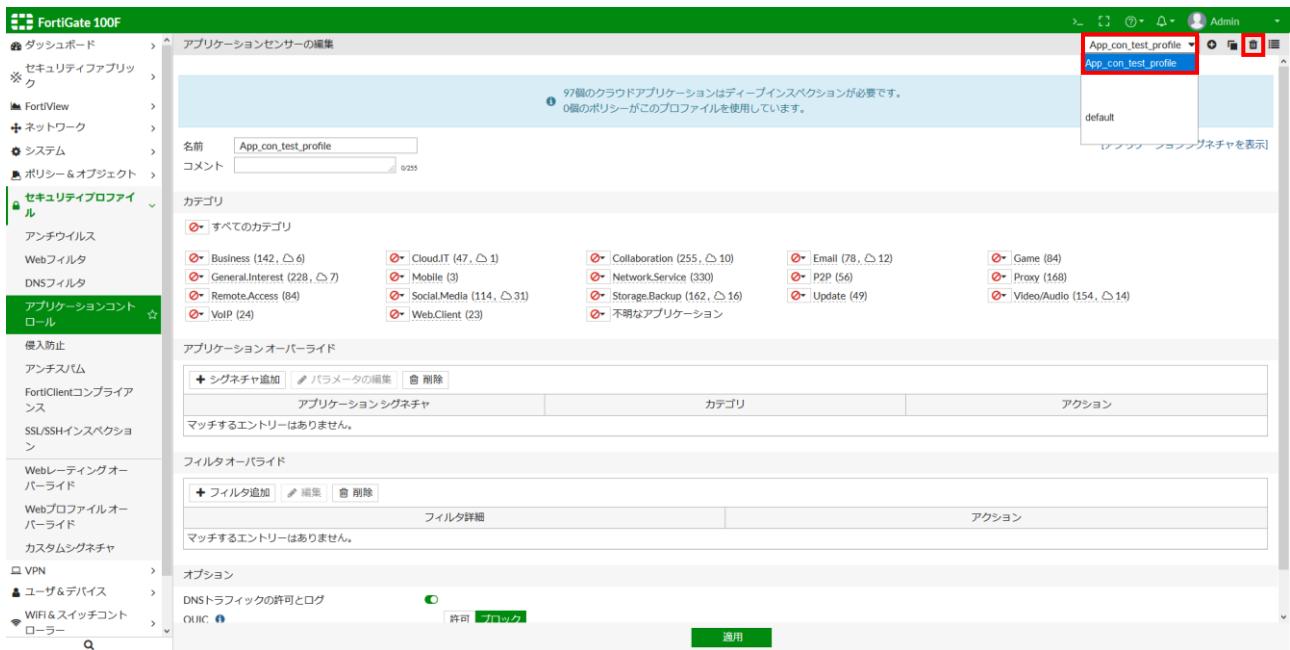
- ① 「セキュリティプロファイル」→「アプリケーションコントロール」→「アプリケーションセンターの編集」バーの右端のボタンのうち、「丸い+ボタン」をクリックします。



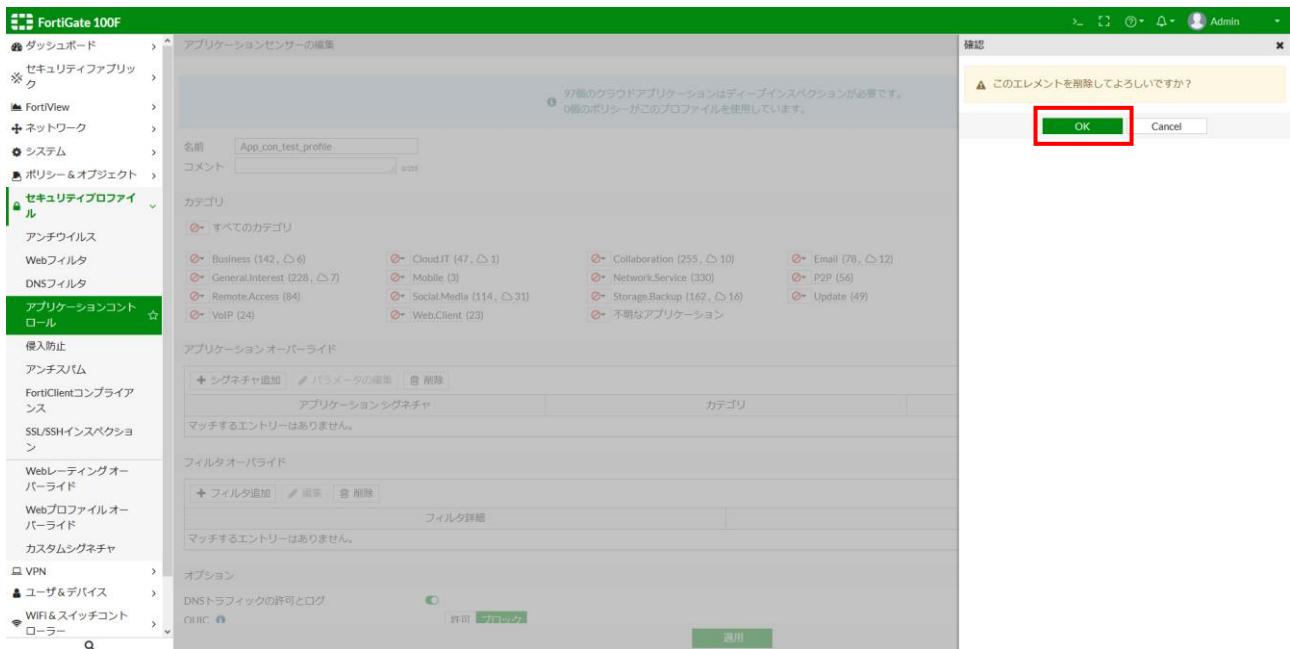
- ② 名前とカテゴリのアクションを指定して「OK」をクリックします。



- ③ 追加されたアプリケーションコントロールプロファイルを削除したい場合は、アプリケーションセンターの編集」バー右端の「プロファイル名▼」ボタンを押して、追加した名前のプロファイルを選択し画面右上の「ゴミ箱アイコン」をクリックします。



- ④ 「このエレメントを削除してよろしいですか？」が表示されたら、「OK」ボタンをクリックして削除します。



2.7. ポリシー設定

ポリシー設定では、各種オブジェクトを組み合わせることでより厳密な通信制御が可能です。

ポリシー設定追加時の作業手順は以下の通りです。

順番	設定項目	備考
1	ポリシー設定追加	2.7.1 章を参照
2	アドレス設定追加	2.7.2 章を参照
3	サービス設定追加	2.7.3 章を参照

2.7.1. ポリシー設定

FW を経由する通信において、許可または拒否したい通信をポリシーで指定します。ポリシーの最終行には「Implicit Deny」という全通信が拒否されるポリシーがあります。

また、ポリシーは上のルールから順番に評価され、通信内容に一致する最初のルールが使用されるとそれ以降のルールは評価されなくなります。

(例) ポリシーの追加(セキュリティプロファイル利用なし)

- ① 「ポリシー & オブジェクト」→「IPv4 ポリシー」→「新規作成」の順に選択します。

ID	名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト
2	net	192.168.0.0/24	all	always		DENY			無効化済み	1.09 kB
3	Internet	192.168.0.0/24	all	always	ALL	ACCEPT	有効化済み	default webfilter_1 block_P2P critical_high_block certificate-inspection	UTM	168.17 MB
1		all	all	always	ALL	ACCEPT	有効化済み		UTM	0 B

② ポリシー設定に必要な以下の情報を入力し、「OK」を実行します。

「入力インターフェース」「出力インターフェース」「送信元」「宛先アドレス」「サービス」を選択

「アクション」の ACCEPT を選択

「インスペクションモード」は「フローベース」を選択

「NAT」の ON/OFF を選択(アドレス変換が不要な場合は OFFにして下さい)

「プロトコルオプション」は「proto-prof_default」を選択

「許可トラフィックログ」の「すべてのセッション」を選択

新規ポリシー

ID	0
名前	policy20
着信インターフェース	internal1
発信インターフェース	wan1
送信元	all
送信元をネゲート	all
宛先	all
宛先をネゲート	always
サービス	HTTP
アクション	<input checked="" type="checkbox"/> 許可 <input type="checkbox"/> 拒否 <input type="checkbox"/> IPsec
インスペクションモード	フローベース

ファイアウォール/ネットワークオプション

NAT	ON
IPプール設定	発信インターフェースのアドレスを使用
送信元ポートの保持	OFF
プロトコルオプション	proto default

セキュリティプロファイル

アンチウイルス	OFF
Webフィルタ	OFF
DNSフィルタ	OFF
アプリケーションコントロール	OFF
IPS	OFF
ファイルフィルタ	OFF
Eメールフィルタ	OFF
VoIP	OFF
SSLインスペクション	SSL no-inspection

ロギングオプション

許可トラフィックをログ	ON
セキュリティイベント	すべてのセッション

高度な設定

WCCP	OFF
キャブティブポータルから除外	OFF
コメント	コメント記入... 0/1023

このポリシーを有効化

(例) ポリシーの追加(セキュリティプロファイルの Web フィルタ利用あり)

- ① 「ポリシー & オブジェクト」→「IPv4 ポリシー」→「新規作成」の順に選択します。

The screenshot shows the FortiGate 100F web interface under the 'Policy & Object' section. The left sidebar has 'Policy & Object' selected, with 'IPv4 Policy' highlighted. The main table displays three existing IPv4 policies:

ID	名前	送信元	宛先	スケジュール	サービス	アクション	NAT	セキュリティプロファイル	ログ	バイト
2	net	192.168.0.0/24	all	always		DENY			無効化済み	1.09 kB
3	Internet	192.168.0.0/24	all	always	ALL	ACCEPT	有効化済み	default webfilter_1 block_P2P critical_high_block certificate-inspection	UTM	168.17 MB
1		all	all	always	ALL	ACCEPT	有効化済み		UTM	0 B

A red box highlights the 'New Operation' button at the top left of the table area.

② ポリシー設定に必要な以下の情報を入力し、「OK」を実行します。

「入力インターフェース」「出力インターフェース」「送信元」「宛先アドレス」「サービス」を選択

「アクション」の ACCEPT を選択

「インスペクションモード」は「フローベース」を選択

「NAT」の ON/OFF を選択(アドレス変換が不要な場合は OFFにして下さい)

「プロトコルオプション」は「proto-prof_default」を選択

[セキュリティプロファイル]

「Web フィルタ」を選択し、プロファイル「wf-prof_default」を選択

「SSL インスペクション」は「2.7.1.2. SSL インスペクションについて」を参照し選択

[ロギングオプション]

「許可トラフィックログ」の「セキュリティイベント」を選択

The screenshot shows the 'New Policy' configuration window in Winbox. The configuration includes:

- ID:** 0
- 名前:** policy20
- 入力インターフェース:** internal1
- 出力インターフェース:** wan1
- 送信元:** all
- 宛先:** all
- アクション:** 許可 (selected)
- インスペクションモード:** フローベース (selected)
- セキュリティプロファイル:** Web フィルタ (selected)
- プロトコルオプション:** proto default
- ロギングオプション:** 許可トラフィックをログ (selected) - セキュリティイベント (selected)

At the bottom right, the 'OK' button is highlighted with a red border.

2.7.1.1. セキュリティプロファイル

設定するポリシーに適用するセキュリティプロファイルにより、オプション項目の設定が異なります。下表に設定パターンをまとめます。

	アンチウイルス	Web フィルタ	アプリケーション コントロール	IPS	E メール フィルタ
プロファイル名	av-prof_default	wf-prof_default	app-prof_default	ips-prof_default	ef-prof_default
インスペクション モード	プロキシベース	プロキシベース	プロキシベース	プロキシベース	プロキシベース

2.7.1.2. SSL インスペクション

セキュリティプロファイルを適用すると、SSL インスペクションプロファイルの指定が必須となります。下表に設定パターンをまとめます。

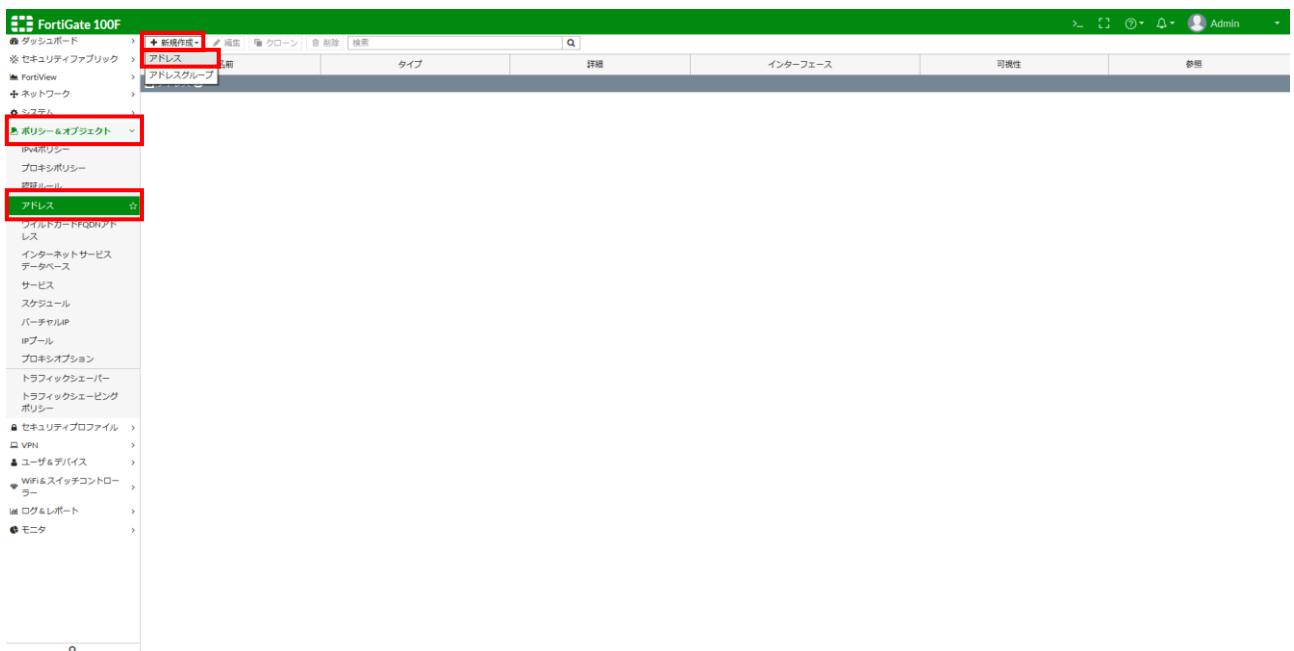
セキュリティ プロファイル指定	SSL 復号しての 検査必要有無	SSL/SSH インスペクション プロファイル	説明
なし	—	no-inspection	SSL 暗号通信内容の検査はしません。セキュリティプロファイルを指定しない単純な FW ポリシーの場合はこちらを指定してください。
あり	なし	custom-certificate-inspection	SSL 暗号通信が発生しない。または Web フィルタ機能のみの場合は、こちらを指定してください。 SSL ハンドシェイクから証明書情報を確認し、 COMMONNAME 情報を入手します。これにより Web フィルタ機能は SSL 通信であっても接続先 FQDN が取得できフィルタリングが機能します。 その他のセキュリティ機能については SSL 通信に対しては機能しません。
あり	あり	custom-deep-inspection	SSL 暗号通信を復号して、各種セキュリティプロファイルによる検査を行う場合は、こちらを指定してください。

2.7.2. アドレス設定

ポリシー設定で使用するアドレス範囲をアドレスオブジェクトとして定義します。なお、複数のアドレスオブジェクトをグループ化（アドレスグループ）することも可能です。

(例) アドレスの追加

- ① 「ポリシー＆オブジェクト」→「アドレス」→「新規作成」→「アドレス」の順に選択します。



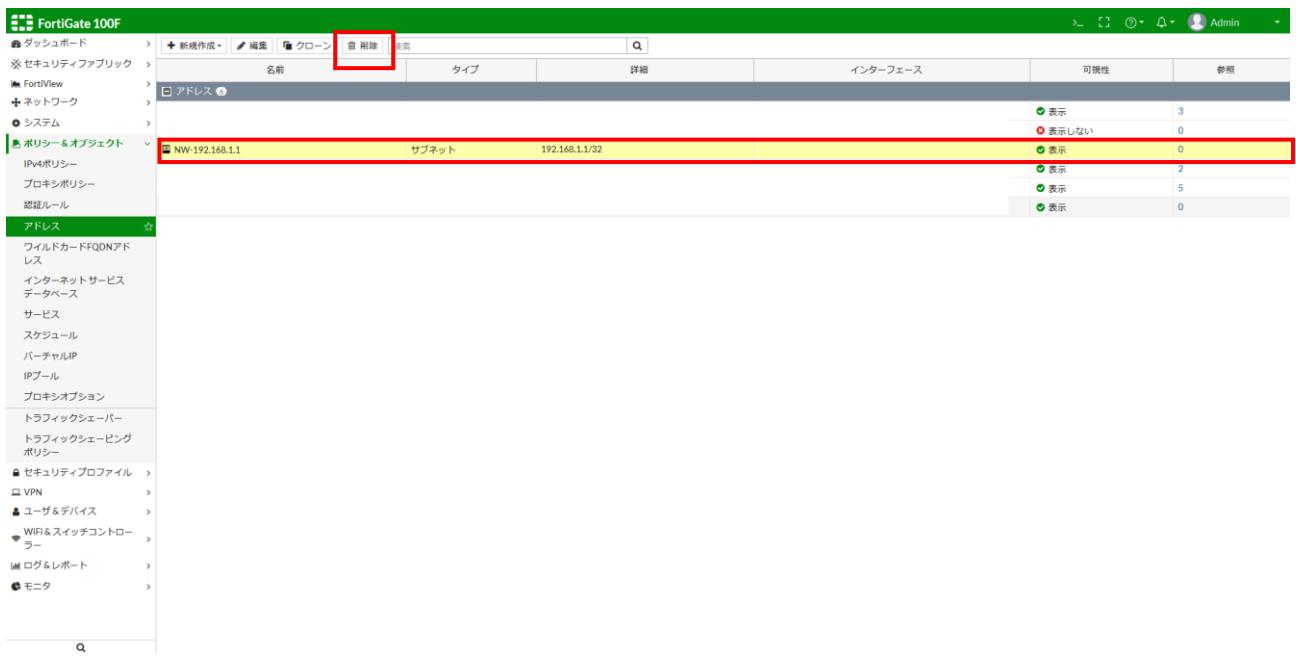
- ② 「名前」「サブネット / IP 範囲」を入力し、「OK」を実行します。

アドレスでは IP ネットマスク指定の他に FQDN、地域、IP 範囲で定義することも可能です。

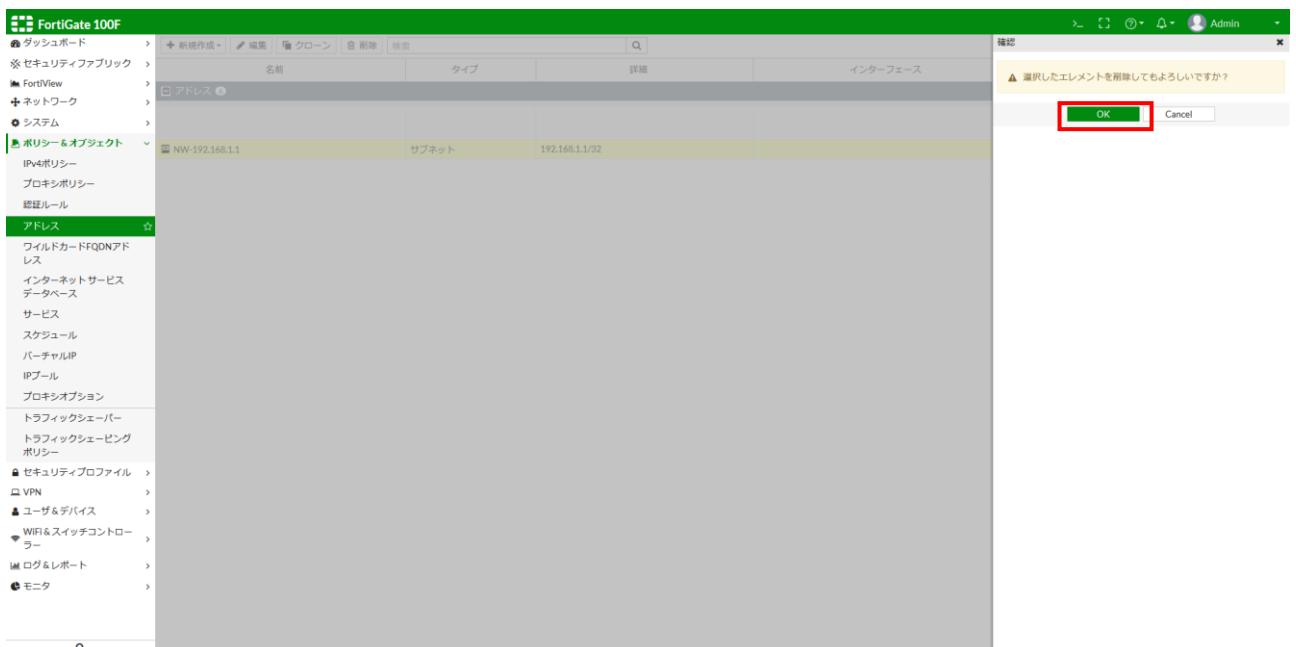
アドレス作成

カテゴリ	アドレス	プロキシアドレス
名前	NW-192.168.1.1	
カラー	<input type="button" value="変更"/>	
タイプ	サブネット	
サブネット / IP範囲	192.168.1.1/32	
インターフェース	<input type="button" value="any"/>	
アドレスリストに表示	<input checked="" type="radio"/>	<input type="radio"/>
スタティックルート設定	<input type="radio"/>	<input checked="" type="radio"/>
コメント	0/255	
タグ	<input type="button" value="タグカテゴリの追加"/>	
<input type="button" value="OK"/> <input type="button" value="キャンセル"/>		

③ 削除する場合、「アドレス」リストの削除対象アドレスをクリック後「削除」ボタンをクリックします。

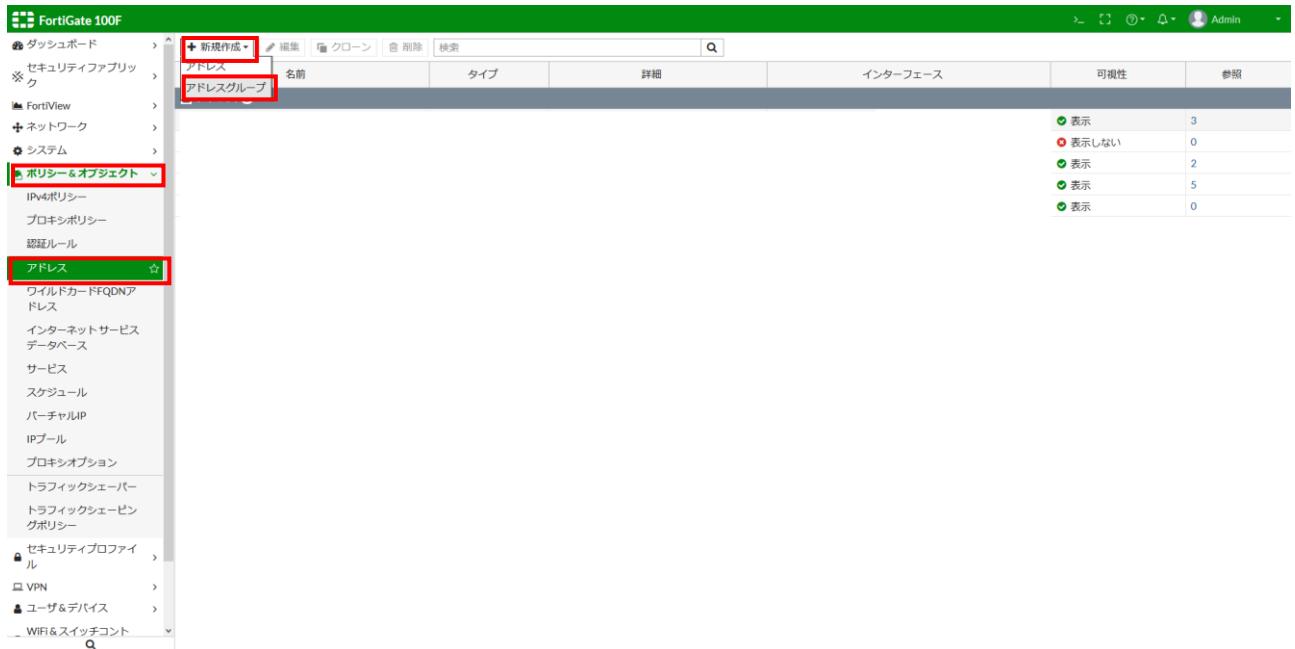


④ 「選択したエレメントを削除してもよろしいですか？」が表示されたら「OK」をクリックします。



(例) アドレスグループの追加

- ① 「ポリシー&オブジェクト」→「アドレス」→「新規作成」→「アドレスグループ」の順に選択します。



- ② 「グループ名」を入力、「メンバ」のエントリーを選択からグループ化したいアドレスを選択し、「OK」を実行します。

This is a screenshot of the 'Create Address Group' dialog box. The 'Group Name' field contains 'port1-addr-group'. The 'Members' field contains 'host-192.168.16.2'. The 'Display in Address List' checkbox is checked. The 'Static Route Setting' checkbox is unchecked. There is a comment input field with placeholder 'Comment entry' and a character count of '0/255'. At the bottom right are 'OK' and 'Cancel' buttons, with 'OK' being highlighted by a red box.

- ③ 削除する場合「アドレス」リストのアドレスグループに登録されている削除対象グループを選択後「削除」ボタンをクリックします。

The screenshot shows the FortiGate 100F configuration interface. On the left, there's a navigation tree with 'ポリシー & オブジェクト' selected. Under it, 'アドレス' is expanded, showing various address types like FQDNアドレス, インターネットサービスデータベース, and サービス. In the main content area, a table lists 'アドレス' and 'アドレスグループ'. A row for 'NW_addr_group' is selected and highlighted with a red box. At the top of the interface, there's a toolbar with several buttons, one of which is '削除' (Delete), also highlighted with a red box.

- ④ 「選択したエレメントを削除してもよろしいですか？」が表示されたら「OK」をクリックします。

This screenshot shows the same FortiGate interface as above, but with a confirmation dialog box overlaid. The dialog box contains the message '選択したエレメントを削除してもよろしいですか？' (Are you sure you want to delete the selected element?). It has two buttons at the bottom: 'OK' (highlighted with a red box) and 'Cancel'.

2.7.3. サービス設定

ポリシー設定で使用するサービスポート範囲（TCP・UDP・SCTP ポート番号）をサービスオブジェクトとして定義します。なお、複数のサービスオブジェクトをグループ化（サービスグループ）することも可能です。

(例) サービスの追加

- ① 「ポリシー&オブジェクト」→「サービス」→「新規作成」→「サービス」の順に選択します。



- ② 「名前」を入力、「カテゴリ」の Custom を選択、宛先ポート「TCP」「UDP」「SCTP」のいずれかを選択、ポート番号を入力し、「OK」を実行します。

「1-1024」のように範囲の指定や、宛先ポート横の「+」を押し複数のポートをまとめることも可能です。

The screenshot shows the 'Service Create' dialog box. The 'Name' field contains 'tcp/13389'. The 'Comment' field contains 'test_service'. The 'Service Type' dropdown is set to 'ファイアウォール' (Firewall). The 'Protocol Options' section shows 'Protocol Type' as 'TCP/UDP/SCTP'. The 'Destination Port' section shows 'IP Range' as '0.0.0.0' and 'Port' as 'TCP 13389 - High'. The 'OK' button is highlighted with a red box at the bottom right of the dialog.

- ③ 削除する場合、「サービス」リストから削除対象サービスを選択し、「削除」ボタンをクリックします。

サービス名	ポート	IP/FQDN	状態
tcp/13389	TCP/13389	0.0.0.0	表示
未分類			
ファイアウォールグループ			

- ④ 「選択したエレメントを削除してもよろしいですか？」が表示されたら「OK」をクリックします。

▲ 選択したエレメントを削除してもよろしいですか？

OK
Cancel

(例) サービスグループの追加

- ① 「ポリシー & オブジェクト」→「サービス」→「新規作成」→「サービスグループ」の順に選択します。



- ② 「グループ名」を入力、「メンバ」のエントリーを選択からグループ化したいサービスを選択し、「OK」を実行します。

The screenshot shows the 'Service Group Add' dialog box. The 'Group Name' field contains 'service_group'. The 'Members' field contains 'tcp/13389'. The 'Type' dropdown is set to 'Firewall'. The 'OK' button is highlighted with a red box. The 'Cancel' button is also visible.

グループ名	service_group
コメント	0/255
カラー	変更
タイプ	ファイアウォール
メンバ	tcp/13389

OK キャンセル

- ③ 削除する場合、「サービス」リストから削除対象サービスグループを選択し、「削除」ボタンをクリックします。

The screenshot shows the FortiGate 100F configuration interface. The left sidebar navigation includes 'ダッシュボード', 'セキュリティアブリック', 'FortView', 'ネットワーク', 'システム', 'ポリシー & オブジェクト' (selected), 'IPv4ポリシー', 'プロキシポリシー', '認証ルール', 'アドレス', 'ワイルドカードFQDNアドレス', 'インターネットサービスデータベース', 'サービス' (selected), 'スケジュール', 'パーキャルIP', 'IPプール', 'プロキシオプション', 'トラフィックシェーバー', 'トラフィックシェーピングポリシー', 'セキュリティプロファイル', 'VPN', 'ユーザ&デバイス', and 'WiFi&スイッチコントローラ'. The main content area displays a table for 'サービス名' (Service Name) with entries like 'Web Access', 'File Access', 'Email', etc., and a 'サービスグループ' (Service Group) entry for 'service_group' (tcp/13389). The top toolbar has buttons for '新規作成' (New), '編集' (Edit), 'クローン' (Clone), '削除' (Delete), 'カテゴリ設定' (Category Setting), and '検索' (Search). A red box highlights the 'Delete' button and the 'service_group' row.

- ④ 「選択したエレメントを削除してもよろしいですか？」が表示されたら「OK」をクリックします。

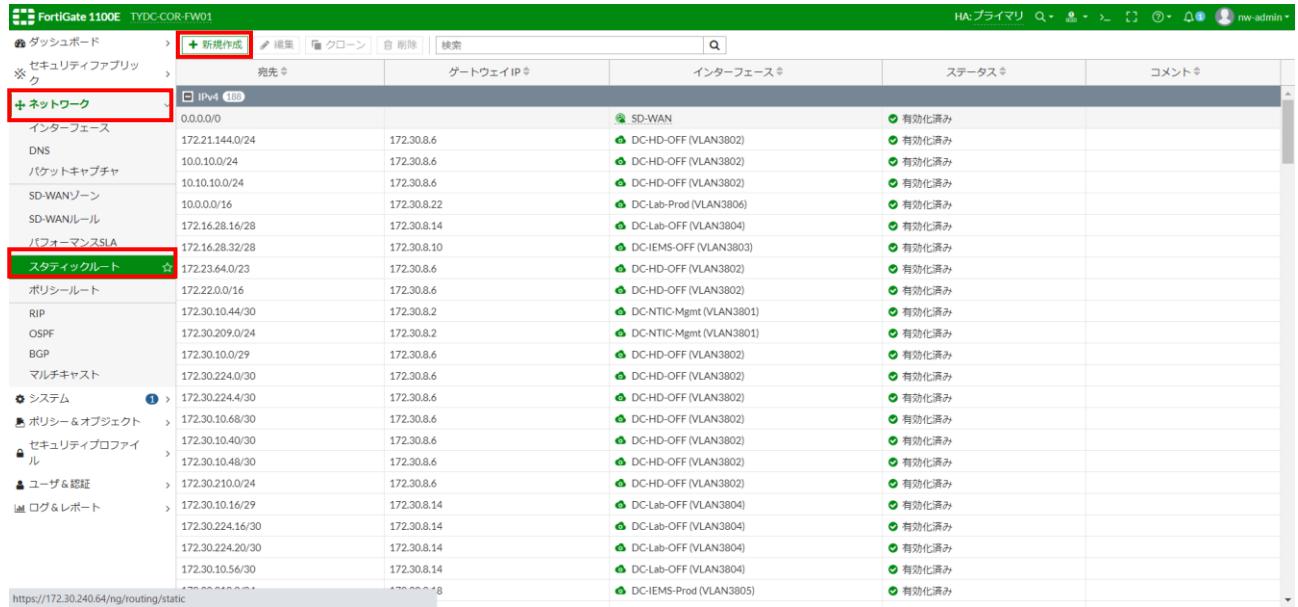
The screenshot shows the FortiGate 100F configuration interface with the same navigation and service group list as the previous screenshot. A confirmation dialog box titled '確認' (Confirmation) is overlaid on the screen, containing the message '△ 選択したエレメントを削除してもよろしいですか?' (Are you sure you want to delete the selected element?). The 'OK' button in the dialog box is highlighted with a red box.

2.8. ルーティング設定

ルーティングの設定方法を説明します。

(例)ルーティングの新規追加

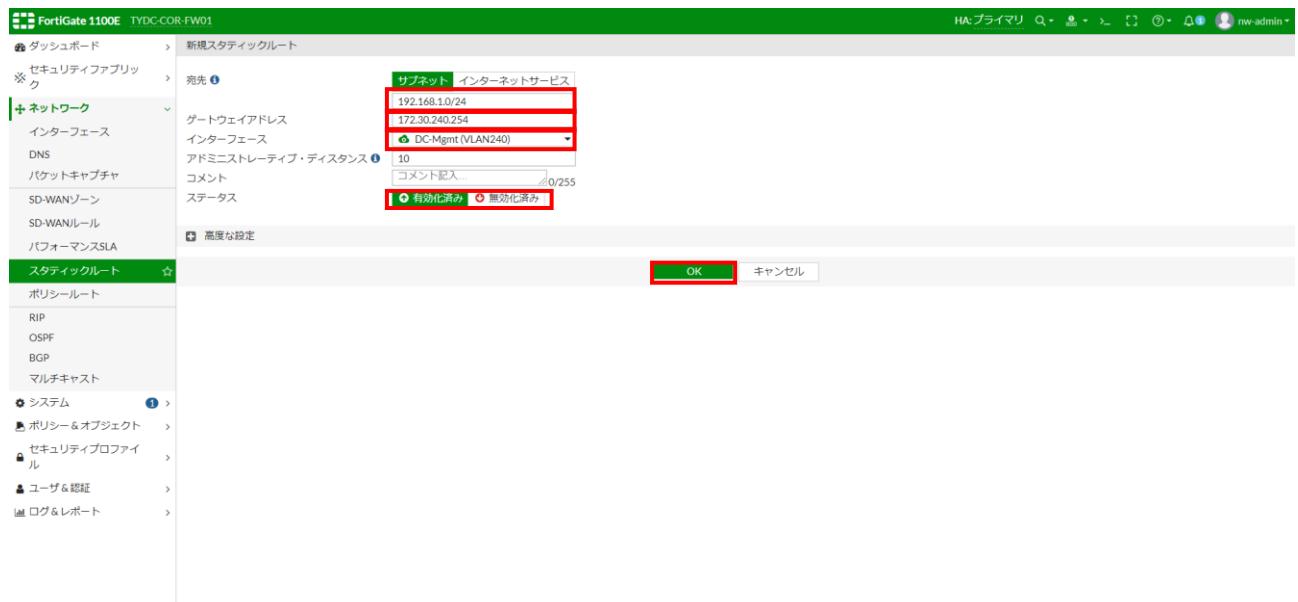
- ① 「ネットワーク」→「スタティックルート」を選択し、「新規作成」を押下します。



The screenshot shows the FortiGate 1100E configuration interface. The left sidebar has a tree view with 'ネットワーク' (Network) selected. In the main area, there is a table titled 'IPv4' with 160 entries. A red box highlights the '新規作成' (New) button at the top left of the table header. Another red box highlights the 'Static Routes' entry in the tree view.

宛先	ゲートウェイ IP	インターフェース	ステータス	コメント
0.0.0.0		SD-WAN	有効化済み	
172.21.144.0/24	172.30.8.6	DC-HD-OFF (VLAN3802)	有効化済み	
10.0.10.0/24	172.30.8.6	DC-HD-OFF (VLAN3802)	有効化済み	
10.10.10.0/24	172.30.8.6	DC-HD-OFF (VLAN3802)	有効化済み	
SD-WANリーン	10.0.0.0/16	DC-Lab-Prod (VLAN3806)	有効化済み	
SD-WANルール	172.16.28.16/28	DC-Lab-OFF (VLAN3804)	有効化済み	
パフォーマンスSLA	172.16.28.32/28	DC-IEMS-OFF (VLAN3803)	有効化済み	
スタティックルート	172.23.64.0/23	DC-HD-OFF (VLAN3802)	有効化済み	
ポリシールート	172.22.0.0/16	DC-HD-OFF (VLAN3802)	有効化済み	
RIP	172.30.10.44/30	DC-NTIC-Mgmt (VLAN3801)	有効化済み	
OSPF	172.30.20.9/24	DC-NTIC-Mgmt (VLAN3801)	有効化済み	
BGP	172.30.10.0/29	DC-HD-OFF (VLAN3802)	有効化済み	
マルチキャスト	172.30.224.0/30	DC-HD-OFF (VLAN3802)	有効化済み	
システム	172.30.224.4/30	DC-HD-OFF (VLAN3802)	有効化済み	
ポリシー&オブジェクト	172.30.10.68/30	DC-HD-OFF (VLAN3802)	有効化済み	
セキュリティプロファイル	172.30.10.40/30	DC-HD-OFF (VLAN3802)	有効化済み	
ル	172.30.10.48/30	DC-HD-OFF (VLAN3802)	有効化済み	
ユーティリティ	172.30.210.0/24	DC-HD-OFF (VLAN3802)	有効化済み	
ログ&レポート	172.30.10.16/29	DC-Lab-OFF (VLAN3804)	有効化済み	
	172.30.224.16/30	DC-Lab-OFF (VLAN3804)	有効化済み	
	172.30.24.20/30	DC-Lab-OFF (VLAN3804)	有効化済み	
	172.30.10.56/30	DC-Lab-OFF (VLAN3804)	有効化済み	
		DC-IEMS-Prod (VLAN3805)	有効化済み	

② 各種情報を入力し、「OK」ボタンを押下します。



宛先：宛先のIPセグメントを入力します。

ゲートウェイアドレス：ゲートウェイアドレスを入力します。

インターフェース：ゲートウェイアドレスを入力することで自動的に選択されます。

ステータス：スタティックルートを有効化/無効化します。

2.9. FortiClient ユーザの追加と削除設定

FortiClient ユーザの追加と削除設定方法を説明します。

(例)ユーザの新規追加

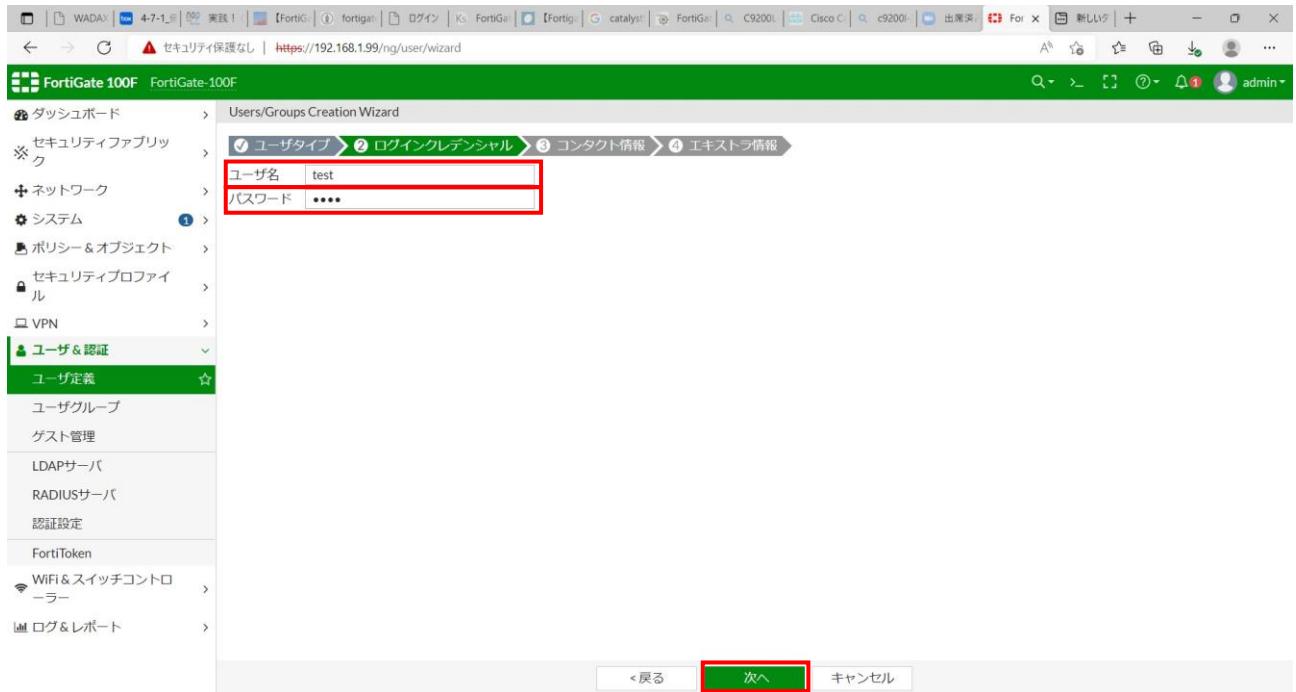
- ① 「ユーザ&認証」→「ユーザ定義」を選択し、「新規作成」を押下します。

The screenshot shows the FortiGate 100F web interface. On the left, the navigation menu is expanded to show 'ユーザ & 認証' (User & Authentication) and 'ユーザ定義' (User Definition). A red box highlights the '新規作成' (New Creation) button at the top of the main content area. The main table lists existing users: bobbytech, guest, info-service, kokuscorp, president, all belonging to 'SSLVPN-Group' and marked as '有効化済み' (Enabled). The table has columns for Name, Type, Two-factor authentication, Group, Status, and Reference.

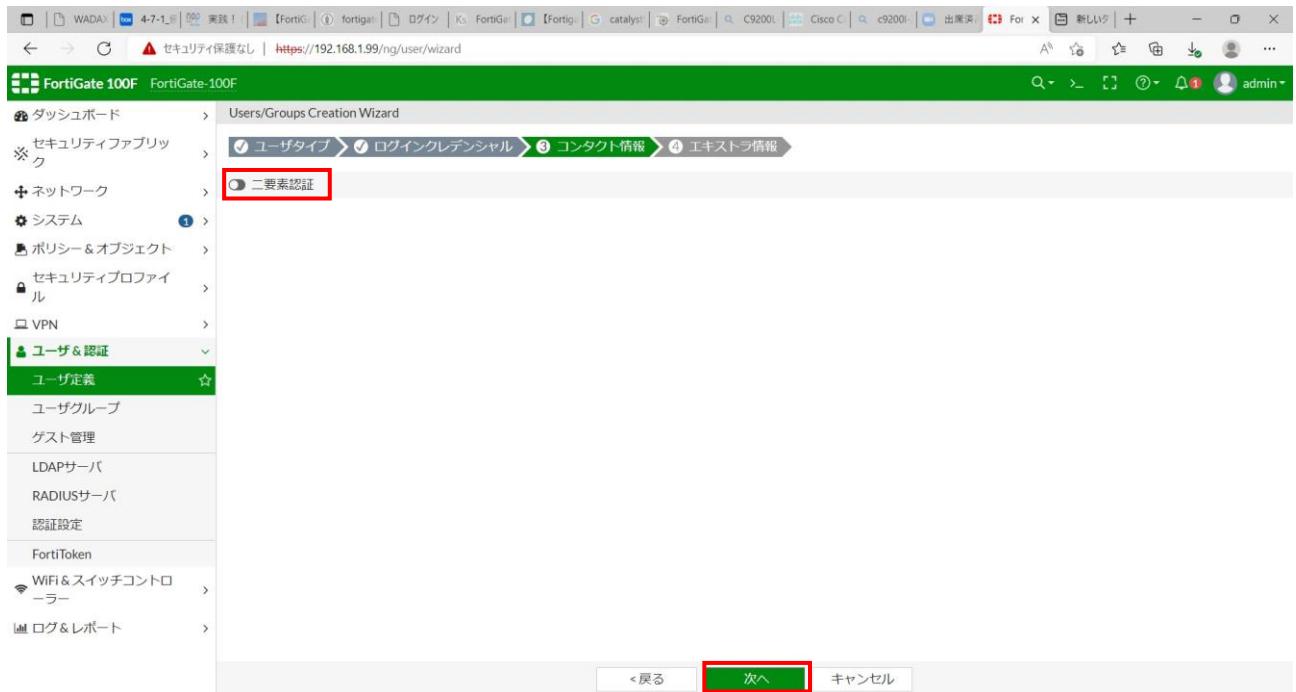
- ② 「ユーザタイプ」→「ローカルユーザ」を選択し、「次へ」を押下します。

The screenshot shows the 'Users/Groups Creation Wizard' step 1: 'ユーザタイプ' (User Type). A red box highlights the 'ローカルユーザ' (Local User) option. Below it are other options: 'リモートRADIUSユーザ' (Remote RADIUS User), 'リモートTACACS+ユーザ' (Remote TACACS+ User), 'リモートLDAPユーザ' (Remote LDAP User), 'FSSO', and 'FortiNACユーザ'. At the bottom of the wizard, the '次へ' (Next) button is highlighted with a red box.

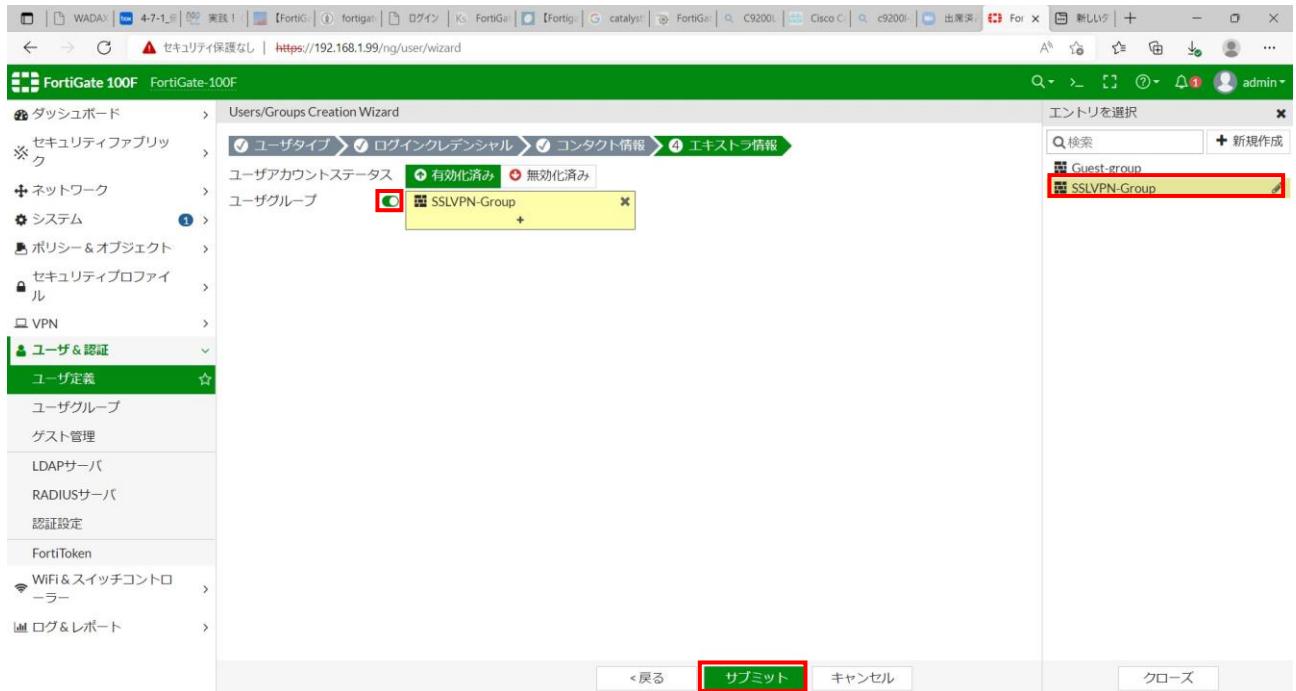
③ 「ログインクレデンシャル」のユーザ名とパスワードを入力し、「次へ」ボタンを押下します。



④ 「コンタクト情報」の二要素認証は OFF のまま、「次へ」ボタンを押下します。



- ⑤ 「エキストラ情報」の「ユーザグループ」を有効にして「+」を押下すると、右側に「SSLVPN-Group」が表示されるので選択して「サブミット」ボタンを押します。



- ⑥ 「ユーザ定義」の「名前」の列に新規ユーザが表示されれば完成です。

User Definition List					
+ 新規作成 編集 ■ クローン ■ 削除 検索 ■					
名前	タイプ	二要素認証	グループ	ステータス	参照
bobbytech	ローカル	×	SSLVPN-Group	有効化済み	1
guest	ローカル	×	Guest-group	有効化済み	1
info-service	ローカル	×	SSLVPN-Group	有効化済み	1
kokuscorp	ローカル	×	SSLVPN-Group	有効化済み	1
president	ローカル	×	SSLVPN-Group	有効化済み	1
test	ローカル	×	SSLVPN-Group	有効化済み	1

(例)ユーザの削除

- ① 「ユーザグループ」の「SSLVPN-Group」を押下します。

The screenshot shows the FortiGate 100F web interface under the 'User & Authentication' section. In the left sidebar, 'User Groups' is selected and highlighted with a green box. The main content area displays a table of user groups. One group, 'SSLVPN-Group', is selected and highlighted with a red box. The table columns include 'Group Name', 'Group Type', 'Members', and 'Reference'. The 'Members' column for 'SSLVPN-Group' lists five users: guest, bobbytech, info-service, kokuscorp, president, and test.

- ② 「ユーザグループの編集」の中の削除するユーザを「x」で選択し「OK」を押下します。

The screenshot shows the 'User Group Edit' dialog box. It contains fields for 'Name' (SSLVPN-Group), 'Type' (Firewall), and 'Members'. The 'Members' list includes six users: bobbytech, info-service, kokuscorp, president, and test. The 'test' user is selected and highlighted with a red box. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel', with 'OK' also highlighted with a red box.

③ 「ユーザグループ」の「SSLVPN-Group」のメンバーにユーザがいなくなったことを確認します。

グループ名	グループタイプ	メンバー	参照
Guest-group	ファイアウォール	guest	0
SSLVPN-Group	ファイアウォール	bobbytech info-service kokuscorp president	4
SSO_Guest_Users	Fortinetシングルサインオン(FSSO)		1

④ 「ユーザ定義」の削除するユーザを選択して、上の「削除」ボタンを押下します。

名前	タイプ	二要素認証	グループ	ステータス	参照
bobbytech	ローカル	×	SSLVPN-Group	有効化済み	1
guest	ローカル	×	Guest-group	有効化済み	1
info-service	ローカル	×	SSLVPN-Group	有効化済み	1
kokuscorp	ローカル	×	SSLVPN-Group	有効化済み	1
president	ローカル	×	SSLVPN-Group	有効化済み	1
test	ローカル	×		有効化済み	0

⑤ 「ユーザ定義」の「削除」ボタンを押下すると、右側に別画面が現れるので「OK」を押下します。

The screenshot shows the FortiGate 100F web interface. On the left, there's a sidebar with various configuration tabs. The 'User & Authentication' tab is selected, and its 'User Definition' sub-tab is also selected, highlighted with a green border. The main content area displays a table of user definitions:

名前	タイプ	二要素認証	グループ
bobbytech	ローカル	×	SSLVPN-Group
guest	ローカル	×	Guest-group
info-service	ローカル	×	SSLVPN-Group
kokuscorp	ローカル	×	SSLVPN-Group
president	ローカル	×	SSLVPN-Group
test	ローカル	×	SSLVPN-Group

A confirmation dialog box is overlaid on the screen, asking '選択した要素を削除してもよろしいですか?' (Are you sure you want to delete the selected elements?). It has 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a red box.

⑥ 「ユーザ定義」の中に削除したユーザがいなくなつたことを確認します。

The screenshot shows the same FortiGate 100F web interface after the user 'test' has been deleted. The 'User Definition' table now only lists the remaining users:

名前	タイプ	二要素認証	グループ	ステータス	参照
bobbytech	ローカル	×	SSLVPN-Group	有効化済み	1
guest	ローカル	×	Guest-group	有効化済み	1
info-service	ローカル	×	SSLVPN-Group	有効化済み	1
kokuscorp	ローカル	×	SSLVPN-Group	有効化済み	1
president	ローカル	×	SSLVPN-Group	有効化済み	1