

ITKeeper ゲートウェイセキュリティパック Lite
マネージドベーシックプラン



ユーザーマニュアル Ver1.0



目次

1	はじめに	1
2	おことわり	2
3	FortiGate の基本操作	3
3-①	FortiGate ダッシュボード（機器管理画面）へのログイン	3
3-②	FortiGate ダッシュボード（機器管理画面）からのログアウト	7
3-③	ログインパスワードの変更	8
3-④	設定のバックアップ	10
3-⑤	FortiGate の電源を入れる方法	11
3-⑥	FortiGate の電源を落とす方法	12
4	こんなときはどうする（トラブルシューティング）	14
4-①	Web ページを閲覧できない	14
4-①-①	FortiGuard カテゴリーによるブロックの解除方法	15
4-①-②	スタティック URL フィルタによるブロックの解除方法	18
4-②	HTTPS の Web ページにて警告が出力され、閲覧できない	22
4-②-①	FortiGate ローカル CA 証明書のダウンロード	23
4-②-②	ローカル CA 証明書の PC へのインポート	25
4-②-③	ローカル CA 証明書の FireFox へのインポート	30
4-②-④	SSL インスペクション機能の無効化	34
4-③	Web ページの閲覧をブロックしたい	37
4-③-①	FortiGuard カテゴリーによるブロックの設定方法	38
4-③-②	URL フィルタによる特定 URL のみ除外(ブロック解除)する 設定方法	43
4-④	受信したメールをスパム判定させたい	46
4-⑤	受信したメールをスパム判定させたくない	49
4-⑥	特定アプリケーションの動作をブロックしたい	52
4-⑦	特定アプリケーションの動作ブロックを解除したい	56
4-⑧	特定カテゴリのアプリケーションの動作をブロックしたい	58
4-⑨	特定カテゴリのアプリケーションのブロックを解除したい	60
4-⑩	アプリケーションのカテゴリを調べたい	62
5	FortiGate 上で FortiCloud レポートを参照する方法	64
5-①	FortiGate 上で FortiCloud レポートを参照する場合	64
5-②	FortiGate 上で FortiCloud レポートをダウンロードする場合	65
6	FortiGate 上でログを参照する方法	74
6-①	FortiGate 上で FortiView のログを参照する場合	74
6-②	FortiGate 上でログ&レポートのログを参照する場合	74

1 はじめに

表示	説明
 や赤字	本機器を取り扱う上で実施してならない事項です。 機器が正常起動しなくなったり、故障の原因に繋がります。
	本機器を取り扱う上で特に注意する事項です。 提供サービスやセキュリティ機能の一部が損なわれる可能性があります。
★ワンポイント★	本機器をより便利に取り扱う上でのワンポイントです。
本文中の青文字+下線	ハイパーリンク（ページ誘導）です。

- 管理者様はご使用前に本書を最後までよくご確認の上でご利用ください。
- 設定変更が必要になった際にすぐにご利用できるように本書は適切に保管ください。
- 弊社が提供するゲートウェイセキュリティパック Lite 専用機器（FortiGate（フォーティゲート））の管理操作説明、注意事項、制約事項を記述しています。
- お客様データの消失による損害、その他本サービスおよび使用説明書の使用または使用不能により生じた損害については法令上賠償責任が認められる場合を除き、当社は一切その責任を負えませんので、あらかじめご了承ください。
- お客様が追加、修正した情報、パスワードの管理についてはお客様にてお願いいたします。
- お客様がご利用の ISP（インターネット サービス プロバイダー）や NTT 回線のトラブル及びメンテナンス時には本サービスをご利用いただけない場合があります。
- 本機器の機器管理画面を操作する際の Web ブラウザは Google Chrome もしくは FireFox の最新版をご利用ください。

2 おことわり

- 本資料のログインユーザー名の表示される場所についてはお客様セキュリティ保護の観点から表示させていません。

別途配布している「FortiGate のログインアカウント情報」をご参照ください。

- 本資料についてはそれぞれ以下のバージョンにて作成しています。
そのため、機種や PC にインストールされている OS のバージョンや Web ブラウザのバージョンによって表示される内容が変わる場合があります。
 - ・ 動作検証 PC OS : Windows 10
 - ・ 動作検証 Web ブラウザ : FireFox 59
 - ・ 動作検証機器 : FortiGate-40F
 - ・ 動作検証 Forti OS : v6.2.10
- 本マニュアルに掲載されている内容以外の設定変更は行わないでください。
変更することにより機器が正常に動作しなくなる場合があります。
- 本資料の内容の一部または全てを無断で複写することは禁止されております。
- 本資料の内容は事前の予告なく変更されることがあります。
- 変更した設定による影響については責任を負いかねますので、ご了承ください。

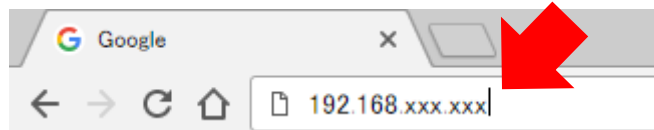
3 FortiGate の基本操作

FortiGate の基本操作方法を説明します。

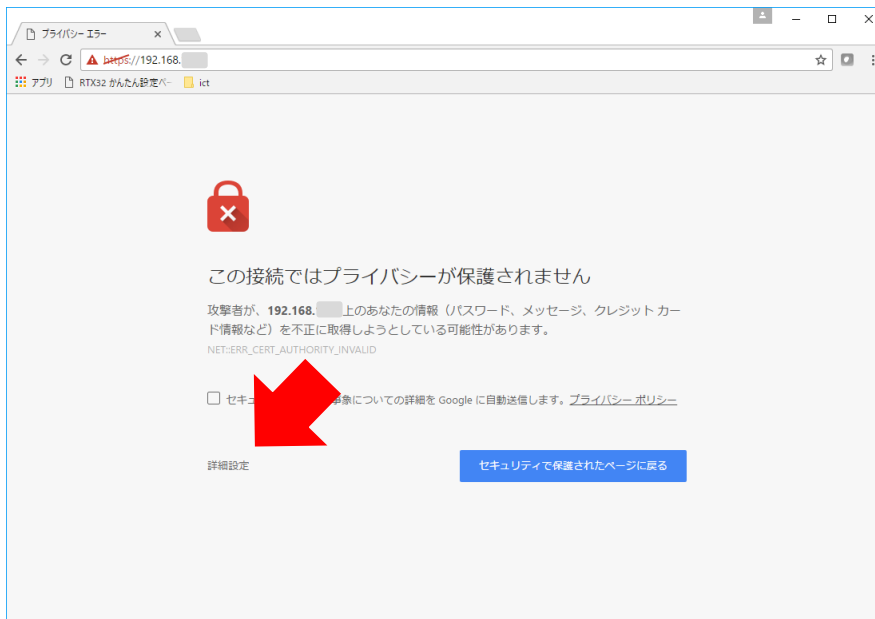
3-① FortiGate ダッシュボード（機器管理画面）へのログイン

機器の操作や設定の変更については本項の FortiGate の管理画面へログイン後に行います。

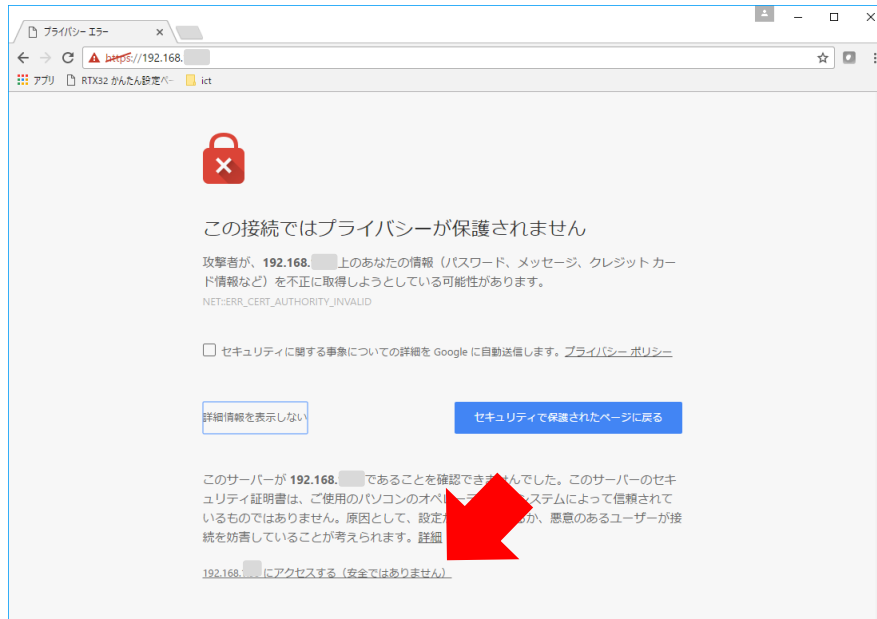
- Web ブラウザを起動し、アドレス入力欄にキーボードで IP アドレスを入力します。
IP アドレスは弊社エンジニアより導入作業時にお客様へお渡しした「導入準備シート」にて確認してください（下図は例）。



- アクセスすると以下のように「プライバシーエラー」や「安全ではない接続」の警告が出力される場合がありますが、使用する Web ブラウザごとに以下のように対処してください。
- Google Chrome のエラー画面例と対処法
- Google Chrome エラー画面左下の「詳細設定」にカーソルを合わせて左クリックします。

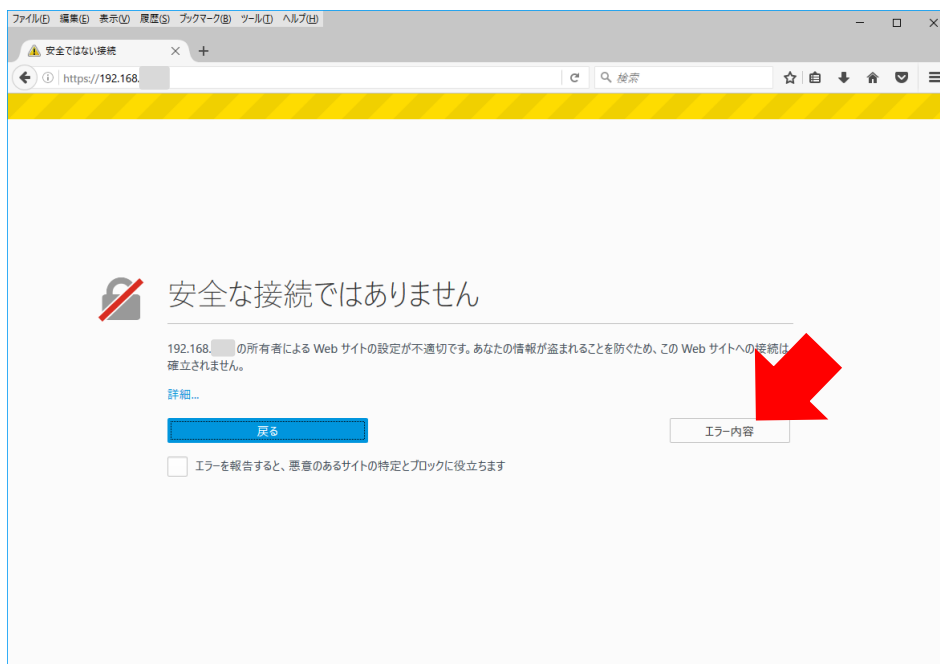


- 以下のように画面が展開されますので、画面下部の「192.168.xxx.xxx にアクセスする（安全ではありません）」にカーソルを合わせて左クリックします。



- Firefox のエラー画面例と対処法

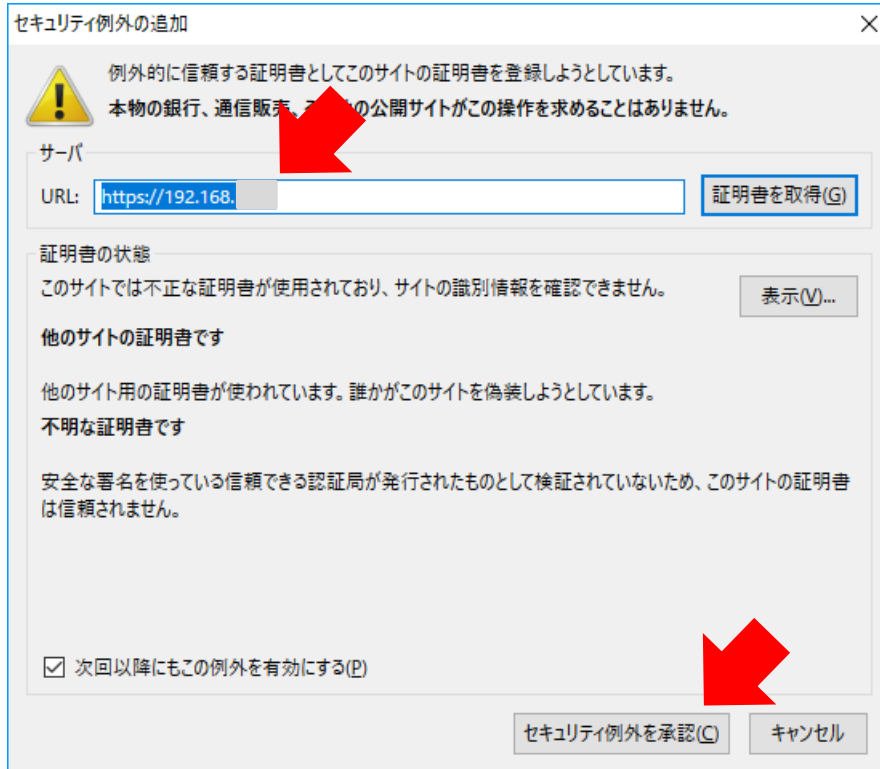
- Firefox エラー画面右側の「エラー内容」にカーソルを合わせて左クリックします。



- 以下のように画面が展開されますので、画面左下の「例外を追加」にカーソルを合わせて左クリックします。



- 以下の画面のように「セキュリティ例外の追加」が表示されますので、「URL:」の欄に FortiGate にアクセスした際の IP アドレス「https://192.168.xxx.xxx」が表示されていることを確認し、画面右下の「セキュリティの例外を承認」へカーソルを合わせて左クリックします。



RICOH

- 以下の認証画面表示がされたら、ユーザ名に別紙「FortiGateのログインアカウント情報」に記載されている「ログインユーザ名」、パスワードに同資料に記載されている「初期パスワード」を入力し、ログインを左クリックします（大文字、小文字は区別して入力してください）。

初期パスワードは [P8「3-③ ログインパスワードの変更」](#)にて変更することを推奨します。



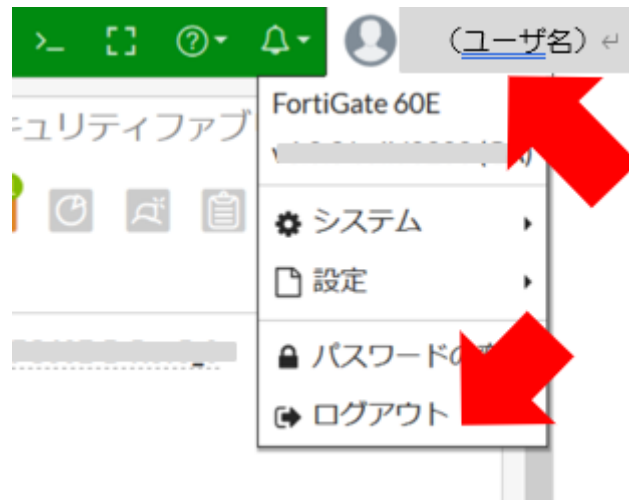
The image shows a login interface with a green header bar containing a white grid icon. Below the header, there are two white input fields with gray borders. The first field is labeled 'ユーザ名' (Username) and the second is labeled 'パスワード' (Password). At the bottom of the form is a green button with the text 'ログイン' (Login) in white.

RICOH

3-② FortiGate ダッシュボード（機器管理画面）からのログアウト

機器の操作や設定変更を終えたらセキュリティ保護の観点から機器からログアウトを行います。

- ダッシュボード画面右上に表示されているログインユーザー名にカーソルを合わせて左クリックし、「ログアウト」を左クリックします。
（下図ではお客様セキュリティ保護の観点からユーザー名については表示させていません。）

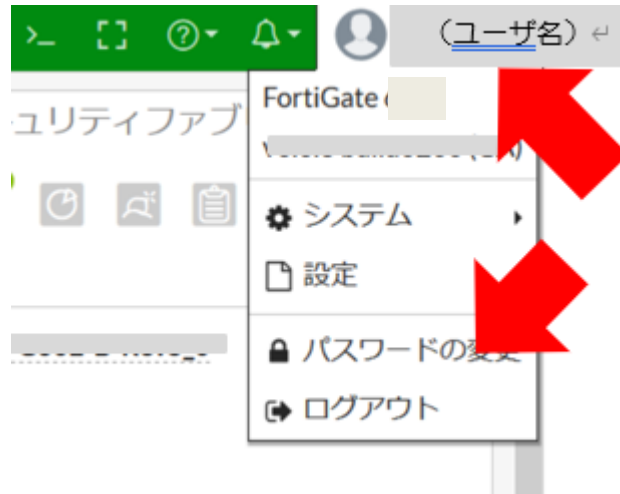


- ログアウトが完了するとログイン画面に戻ります。

A screenshot of the FortiGate login page. It features a green header bar with a white grid icon. Below the header, there are two input fields: 'ユーザー名' (Username) and 'パスワード' (Password). At the bottom, there is a green button labeled 'ログイン' (Login).

3-③ ログインパスワードの変更

- ダッシュボード画面右上に表示されているログインユーザー名にカーソルを合わせて左クリックするとメニューが表示されるので「パスワードの変更」を左クリックします。
(下図ではお客様セキュリティ保護の観点からユーザー名については表示させていません。)



- パスワード編集画面が出力されるので「旧パスワード」の欄に現在設定されているパスワードを入力します。
パスワード編集画面にて入力した文字は「●」にて表示され、平文では表示されません。
また、入力においてはアルファベットの大文字、小文字を識別します。

パスワードの編集

現在の管理者アカウントのパスワードを変更するには、再度ログインする必要があります。

ユーザー名

旧パスワード

新しいパスワード

パスワードの再入力

OK キャンセル

A screenshot of the 'パスワードの編集' (Edit Password) form. It contains a warning message, a 'ユーザー名' (Username) field, and three password fields: '旧パスワード' (Old Password), '新しいパスワード' (New Password), and 'パスワードの再入力' (Re-enter Password). A red arrow points to the '旧パスワード' field, which contains a series of dots representing masked text. At the bottom, there are 'OK' and 'キャンセル' (Cancel) buttons.

- 「新しいパスワード」の欄に新しく設定するパスワードを入力します。

パスワードの編集

現在の管理者アカウントのパスワードを変更するには、再度ログインする必要があります。

ユーザー名

旧パスワード

新しいパスワード

パスワードの再入力

必須フィールドです。

OK キャンセル

A screenshot of the 'パスワードの編集' (Edit Password) form, similar to the previous one. A red arrow points to the '新しいパスワード' (New Password) field, which also contains a series of dots. A red highlight is visible under the 'パスワードの再入力' (Re-enter Password) field. At the bottom, there are 'OK' and 'キャンセル' (Cancel) buttons.

- 「パスワードの再入力」の欄に「新しいパスワード」にて入力した新しく設定するパスワードと同じ文字列を再度入力します。

パスワードの編集

▲ 現在の管理者アカウントのパスワードを変更するには、再度ログインする必要があります。

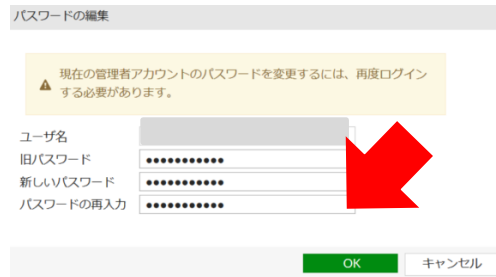
ユーザ名

旧パスワード

新しいパスワード

パスワードの再入力

OK キャンセル



- 「OK」にカーソルを合わせて左クリックし、変更したパスワードの設定を適用します。

パスワードの編集

▲ 現在の管理者アカウントのパスワードを変更するには、再度ログインする必要があります。

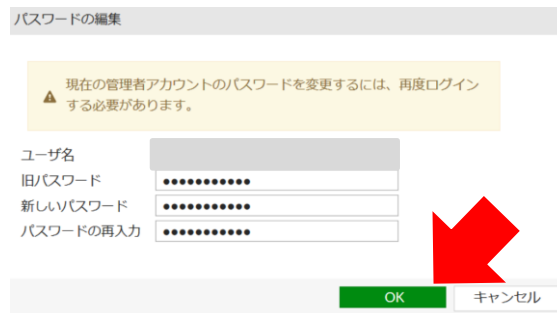
ユーザ名

旧パスワード

新しいパスワード

パスワードの再入力

OK キャンセル



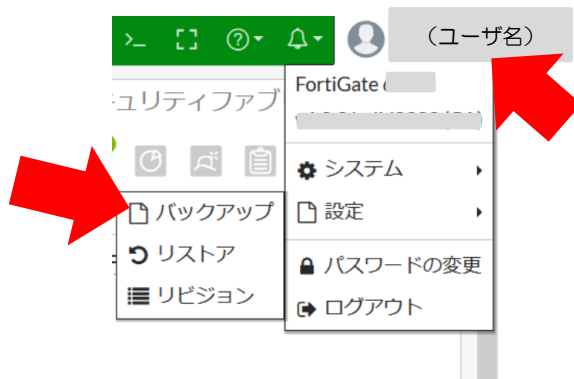
- 設定が完了したら、[P10「3-④ 設定のバックアップ」](#)にて設定をバックアップいただき、別紙「FortiGate のログインアカウント情報」に変更したパスワードを記載してください。

3-④ 設定のバックアップ

適用した設定のバックアップを取得します。

設定変更後は必ず設定のバックアップを取得してください。

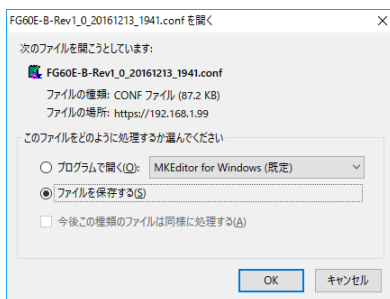
- 機器管理画面右上のログインユーザー名にカーソルを合わせて左クリックすると以下のようにメニューが展開されるので、「設定をバックアップ」にカーソルを合わせて左クリックします。
(下図ではお客様セキュリティ保護の観点からユーザー名については表示させていません。)



- 設定のバックアップ先を指定します。
本資料ではローカル PC に保存する手順について説明します。
バックアップの項目が「ローカル PC」となっていることを確認し、「OK」にカーソルを合わせて左クリックします。



- PC の任意のフォルダを指定し、「OK」を左クリックしてローカル PC の任意のフォルダに保存します。使用する Web ブラウザの設定によっては、ブラウザのダウンロード設定の場所に自動的に保管される場合があります。(FireFox の場合の例)



- ファイルが保存されたフォルダを開いて「機器ホスト名_日付_時間.conf」のファイルが保存されていることを確認します。

RICOH

3-⑤ FortiGate の電源を入れる方法

機器の電源を入れる際には以下の手順にて実施します。

- 機器の AC アダプタの先にある AC ケーブルのプラグをコンセントタップへ挿入します。
機器の起動中は機器本体前面の「STATUS」の LED ランプが緑色に点滅します。
- ⊗ **このときには AC ケーブルのプラグを抜くなどの電源を落とすような行為は行わないでください。
機器が正常起動しなくなる恐れがあります。**




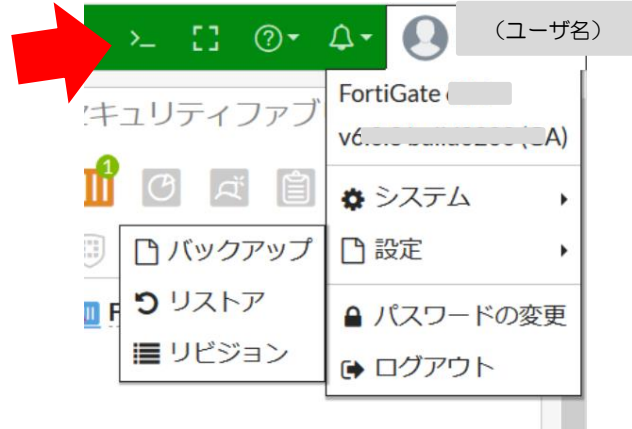
- 電源を入れてから 5 分程度で機器本体前面の「STATUS」の LED ランプが緑色に点灯し、正常起動完了となります。



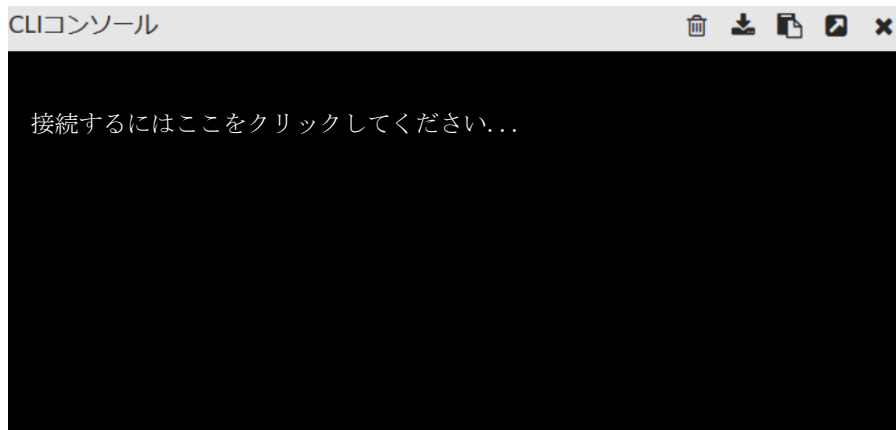
3-⑥ FortiGate の電源を落とす方法

機器の電源を落とす際には以下の手順にて実施します。

- FortiGate 機器管理画面右上の  アイコンをクリックし、CLI コンソールを左クリックします。



- 以下のように黒い画面が出力されるので、黒い画面にカーソルを合わせて左クリック後に Enter キーを押下します。(この画面が出ずに次画面が表示される場合もあります)



- Enter を押下すると以下のように出力されます。

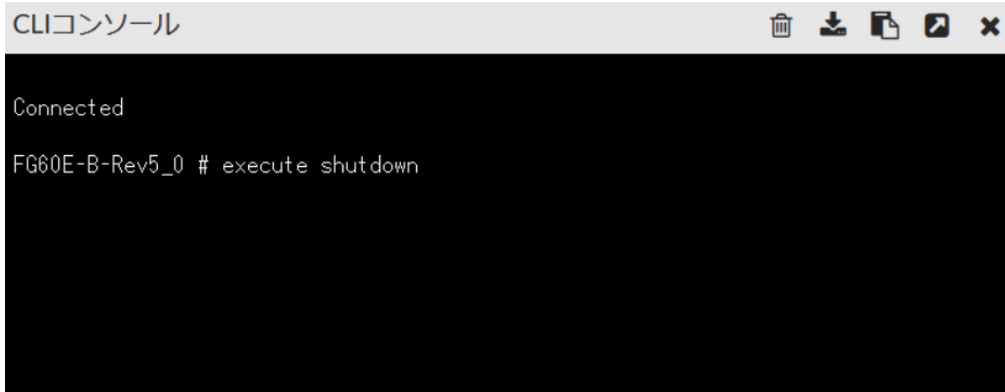


RICOH

- 黒い画面にて以下の文字列を全てアルファベット小文字で入力後にキーボードの「Enter」キーを押下します。

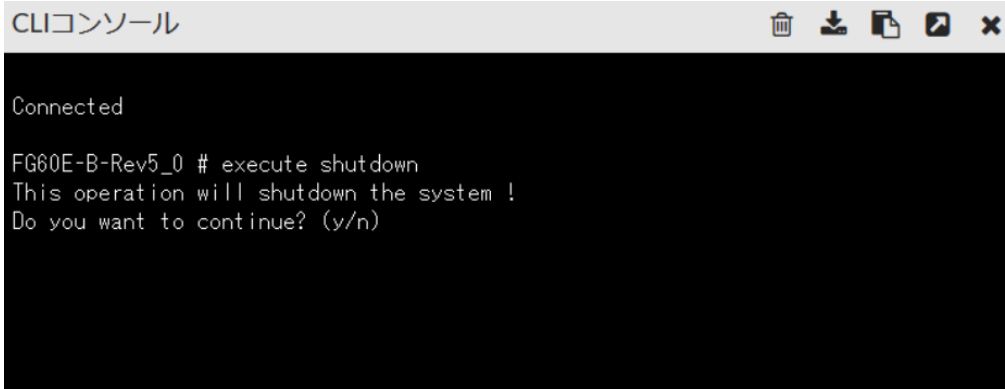
execute shutdown

(イー、エックス、イー、シー、ユー、ティー、イー、スペース、エス、エイチ、ユー、ティー、ディー、オー、ダブリュー、エヌ)



```
CLIコンソール
Connected
FG60E-B-Rev5_0 # execute shutdown
```

- 「Enter」キーを押下すると以下のように機器の電源を落とすことを続行するか英語で尋ねられますので、続行する場合にはキーボードの「Y」キーを押下します。逆に電源を落とさない場合はキーボードの「N」キーを押下します。



```
CLIコンソール
Connected
FG60E-B-Rev5_0 # execute shutdown
This operation will shutdown the system !
Do you want to continue? (y/n)
```

- 上記の操作後 30 秒～1 分程度で機器本体前面の「STATUS」の LED が消灯します。消灯したら、機器の AC アダプタの先にある AC ケーブルのプラグをコンセントタップより引き抜いてください。



4 こんなときはどうする（トラブルシューティング）

本商品を使用する上での各機能の利用方法及びよくあるトラブル事例の解決方法です。

4-① Web ページを閲覧できない

FortiGate にて Web ページをブロックすると Web ブラウザでは以下のような表示がされます。以下の表示の場合には閲覧しようとしている Web ページが Web フィルタリング機能で閲覧を許可していない可能性があります。



上記の状態を解決する場合には以下の 2 パターンの解決方法があります。

● 解決方法 1

Web ページが属するカテゴリごと閲覧ブロックを解除する

上記の方法では例として「ソーシャル・ネットワーキング」のカテゴリに属する Twitter、Facebook、Instagram などの SNS サービスの Web ページ全ての閲覧をしたい場合に使用します。

本方法でブロックを解除する場合は [P15「4-①-\(1\) FortiGuard カテゴリによるブロックの解除」](#)を参照します。

● 解決方法 2

Web ページが属するカテゴリのブロック設定は維持しつつ、特定 URL の Web ページのみ閲覧を許可する

上記の方法では例として「ソーシャル・ネットワーキング」のカテゴリに属する Web ページは基本的にブロックする設定を維持したい状態で、Twitter だけは閲覧したい場合などに使用します。

本方法でブロックを解除する場合は [P18「4-①-\(2\) スタティック URL フィルタによるブロックの解除」](#)を参照します。

4-①-(1) FortiGuard カテゴリーによるブロックの解除方法

Web ページのカテゴリによるブロックをカテゴリごとに「解除（許可）」する場合には以下の手順にて実施します。

- Web ブラウザのブロック画面の下部に表示されている「Category:」にてブロックされているカテゴリを確認します（以下の URL は例）。

```

URL: http://www.fortinet.co.jp/
Category: Information Technology
Client IP: 192.168.1.1
Server IP: 203.138.186.202
User name:
Group name:
  
```

- カテゴリについては大カテゴリにある小カテゴリが表示されるため、実際に FortiGate の画面のどの大カテゴリに含まれるかは「<http://www.fortiguards.com/webfilter/categories>」にて確認できます。

Web Filter Categories

FortiGuard URL Database Categories are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families. They also take into account customer requirements for Internet management. The categories are defined to be easily manageable and patterned to industry standards.

Each category contains websites or web pages that have been assigned based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized.

Descriptions of the categories are designed to assist the reader with category comprehension only; they are not meant to depict any form of symbolic representation of the individuals who own or surf these sites.

Adult / Mature Content

Category	Description	Tests
Abortion	Websites pertaining to abortion data, information, legal issues, and organizations.	Web Filter Full SSL Inspection SSL Certificate Inspection
Advocacy Organizations	This category caters to organizations that campaign or lobby for a cause by building public awareness, raising support, influencing public policy, etc.	Web Filter Full SSL Inspection SSL Certificate Inspection
Alcohol	Websites which legally promote or sell alcohol products and accessories.	Web Filter Full SSL Inspection SSL Certificate Inspection
Alternative Beliefs	Websites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings.	Web Filter Full SSL Inspection SSL Certificate Inspection
Dating	Websites that allow individuals to make contact and communicate with each other over the Internet, usually with the objective of developing a personal, romantic, or sexual	Web Filter Full SSL Inspection SSL Certificate Inspection

- 本サービスにて提供されている FortiGate では日本語でのサービス提供ですが、「FortiGuard Center」の Web ページでは英語にて表示されます。
以下の表は FortiGate の「FortiGuard カテゴリによるフィルタ」と「FortiGuard Center」の表示対比表となります。

FortiGate の「FortiGuard カテゴリによるフィルタ」での表示	FortiGuard Center Web ページでの表示
違法性・犯罪性の高いサイト	Potentially Liabile
成人/アダルトコンテンツ	Adult/Mature Content
帯域を消費しやすいサイト	Bandwidth Consuming
セキュリティ上問題のあるサイト	Security Risk
一般的な趣味・関心 - 個人	General Interest - Personal
一般的な趣味・関心 - ビジネス	General Interest - Business

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の管理画面にログインします。
- 管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせてクリックするとメニューが展開されるので「Web フィルタ」を左クリックします。



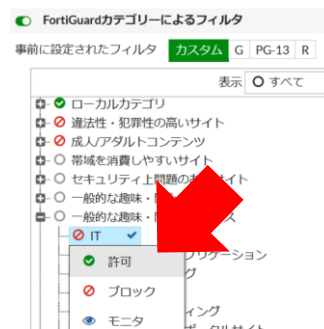
※以下画面が表示された場合は「default」の行をダブルクリックします。

名前	コメント	
WEB default	ITKeeper	1
WEB monitor-all	Monitor and log all visited URLs, proxy-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

- 右側ペインにある「FortiGuard カテゴリーによるフィルタ」にて事前に確認した対象のカテゴリを大カテゴリの中より探し、一番左の右向き三角を左クリックして大カテゴリの詳細を展開します。



- 対象となるカテゴリにて右クリックし、メニューが出力されるので「許可」を左クリックします。



- 設定が完了したら、右側ペインの下部にある「適用」にカーソルを合わせて左クリックします。



- 設定を適用後、該当するカテゴリの Web ページが閲覧できることを確認してください。
- Web ページが閲覧できることを確認したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得して下さい。

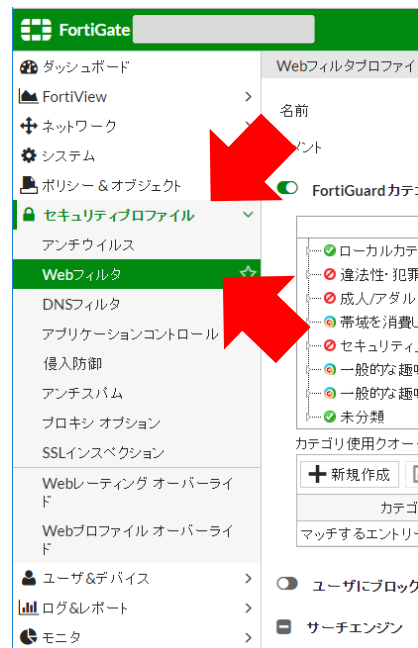
4-①-(2) スタティック URL フィルタによるブロックの解除方法

Web フィルタリング機能のカテゴリによるブロックを維持した状態で

特定 URL の Web ページの閲覧を許可する際に以下の手順にて実施します。

⚠ 本設定では設定した URL の通信はアンチウイルス機能が適用されなくなるので注意してください。

- Web ブラウザのブロック画面の下部に表示されている「Category」にてブロックされているカテゴリを確認します。
- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせて左クリックすると「セキュリティプロファイル」メニューが展開されるので「Web フィルタ」を左クリックします。



※以下画面が表示された場合は「default」の行をダブルクリックします。

+ 新規作成 編集 クローン 削除 検索			
名前		コメント	
WEB	default	ITKeeper	1
WEB	monitor-all	Monitor and log all visited URLs, proxy-based.	0
WEB	wifi-default	Default configuration for offloading WiFi traffic.	1

RICOH

- 右側ペインを中段までスクロールしたところに「スタティックURL フィルタ」にて「新規作成」へカーソルを合わせて左クリックします。



- 以下のように「URL フィルタ作成」のウィンドウが出現するため、「URL」の入力ボックスにブロックさせたくないURLを入力します。



★ワンポイント★

上記のような URL ブロックについては Yahoo! Japan の「news.yahoo.co.jp (Yahoo!ニュース)」や「mail.yahoo.co.jp (Yahoo!メール)」のような関連 URL のブロック解除はできません。こういった URL については以下の「*yahoo.co.jp」のように URL ドメインの前にアスタリスクを付与することで Yahoo! Japan の関連ページをブロック解除することができます。



RICOH

- 「タイプ」にて「ワイルドカード」にカーソルを合わせて左クリックします。

URLフィルタ作成

URL

タイプ シンプル 正規表現 **ワイルドカード**

アクション **除外(exempt)** ブロック 許可 モニタ

ステータス

OK キャンセル

- 「アクション」にて「除外 (exempt)」にカーソルを合わせて左クリックします。

URLフィルタ作成

URL

タイプ シンプル 正規表現 ワイルドカード

アクション **除外(exempt)** ブロック 許可 モニタ

ステータス

OK キャンセル

- 「OK」にカーソルを合わせて左クリックします。

URLフィルタ作成

URL

タイプ シンプル 正規表現 ワイルドカード

アクション **除外(exempt)** ブロック 許可 モニタ

ステータス

OK キャンセル

- 右側ペイン下部の適用にカーソルを合わせて左クリックします。

Webフィルタプロファイルの編集

すべての検査キーワードをログ

■ スタティックURLフィルタ

不正なURLをブロック

URLフィルタ

URL	タイプ	アクション	ステータス
www.netricoh.com	シンプル	<input checked="" type="checkbox"/> ブロック	<input checked="" type="checkbox"/> 無効
.update\microsoft\.com.	正規表現	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効
.download\windowsupdate\.com.	正規表現	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効
\.microsoft\.com.	正規表現	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効
login.live.com	シンプル	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効
\.windowsupdate\.com.	正規表現	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効
www.fortinet.co.jp	ワイルドカード	<input type="checkbox"/> 除外(exempt)	<input checked="" type="checkbox"/> 有効

FortiSandboxにより検知された悪意のあるURLをブロック

Webコンテンツフィルタ


■ レーティングオプション

レーティングエラー発生時にWebサイトを許可

ドメインまたはIPアドレスでURLをレーティング

URLでイメージを評価

適用



- 設定した URL の Web ページ閲覧ができることを確認してください。
- Web ページが閲覧できることを確認したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

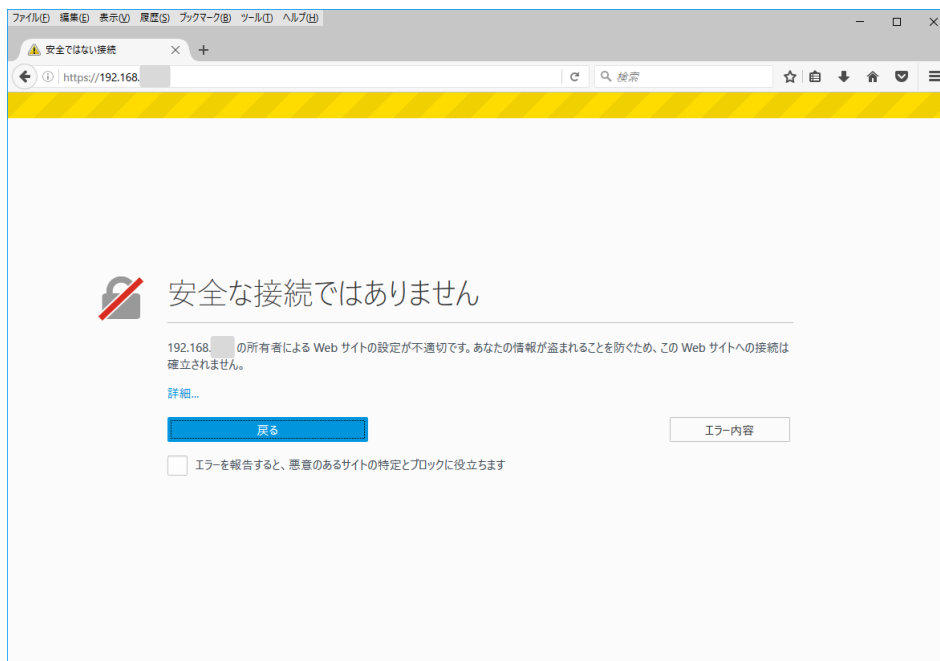
4-② HTTPS の Web ページにて警告が出力され、閲覧できない

HTTPS の Web ページにアクセスする際に FortiGate のローカル CA 証明書が PC にインストールされていない場合、以下のように Web ブラウザに以下のような警告画面が出力される場合があります。

- Google Chrome でのエラー画面例



- Firefox でのエラー画面例



4-②-(1) FortiGate ローカル CA 証明書のダウンロード

FortiGate よりローカル CA 証明書をダウンロードします。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面ログインしたら、左側ペインの「システム」にカーソルを合わせて左クリックすると、「システム」のメニューが展開されるので「証明書」にカーソルを合わせて左クリックします。



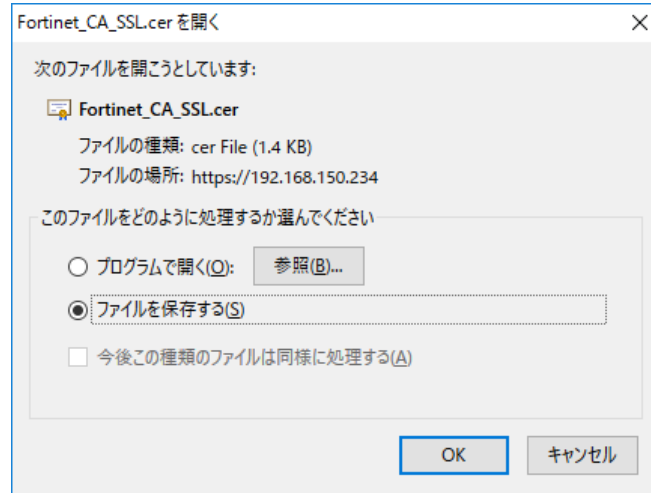
- 右側ペインの「ローカル CA 証明書」の項目にある「Fortinet_CA_SSL」にカーソルを合わせて左クリック後、右側ペイン上部の「ダウンロード」にカーソルを合わせて左クリックします。

The screenshot shows the 'Certificates' list in the FortiGate management interface. The list has columns for 'Name' and 'Subject'. The 'Fortinet_CA_SSL' entry is highlighted in yellow. A red arrow points to the 'Download' button in the top right corner of the list. Another red arrow points to the 'Fortinet_CA_SSL' entry in the list.

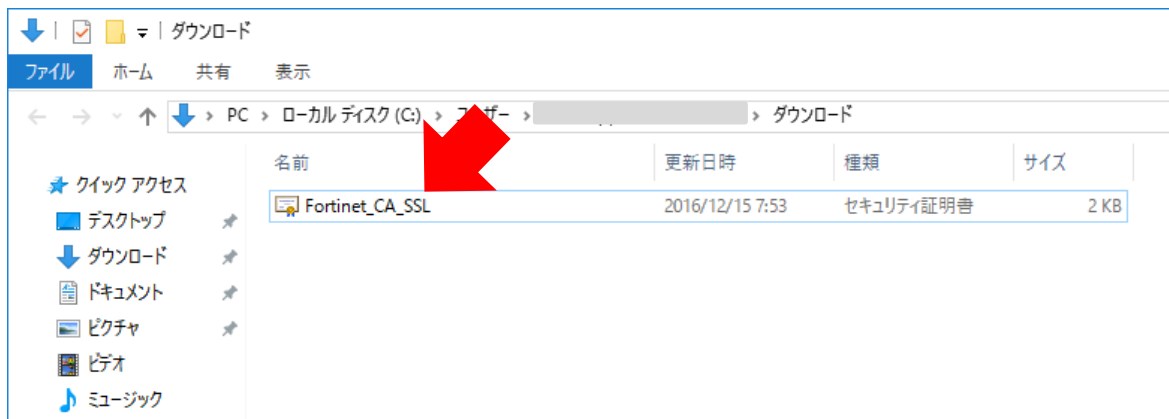
名前	サブジェクト
証明書 (9)	
Fortinet_Factory	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_DSA1024	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_DSA2048	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_ECDSA256	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_ECDSA384	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_RSA1024	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_SSL_RSA2048	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = F
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, Inc., ST = California, OU = FortiWifi
ローカル CA 証明書 (2)	
Fortinet_CA_SSL	C = US, CN = FGT60E4Q16004681, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = C
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = C

RICOH

- PC の任意のフォルダを指定し、OK をクリックしてローカル PC の任意のフォルダに保存します。使用する Web ブラウザの設定によっては、Web ブラウザのダウンロード設定の場所に自動的に保管される場合があります。
- ・ FireFox の場合の例

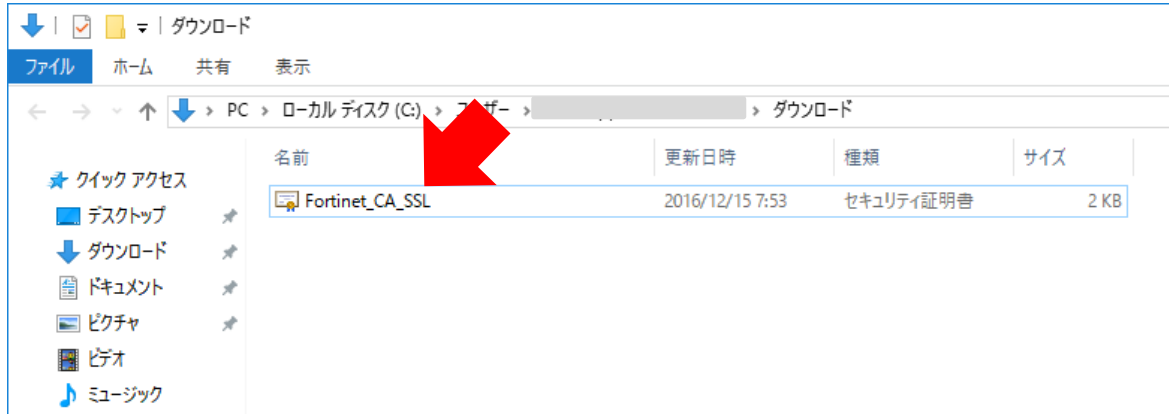


- ファイルが保存されたフォルダを開いて「Fortinet_CA_SSL.cer」のファイルが保存されていることを確認します。

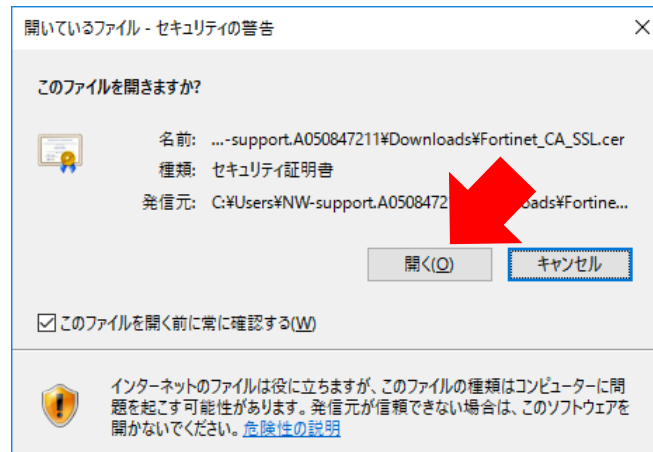


4-②-(2) ローカル CA 証明書の PC へのインポート

- ダウンロードした「Fortinet_CA_SSL.cer」をダブルクリックしてファイルを開きます。

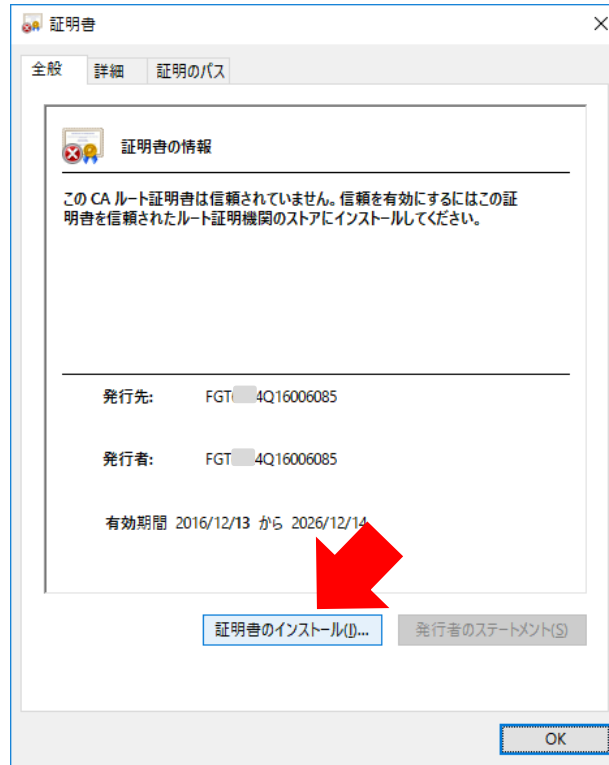


- ダブルクリックすると以下のように「セキュリティの警告」が表示される場合がありますが、「開く」にカーソルを合わせて左クリックします。

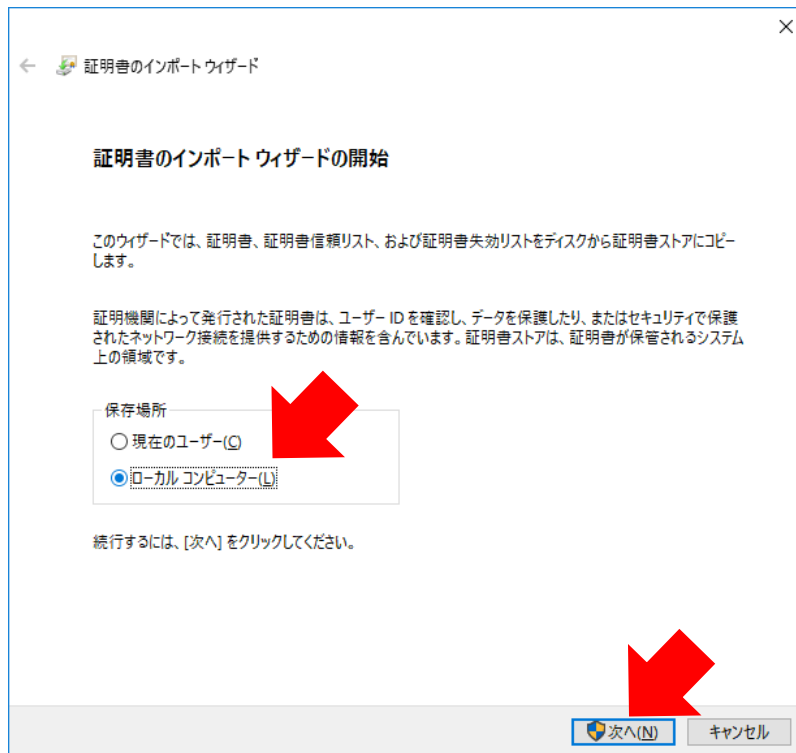


RICOH

- 開いた「証明書」のウィンドウが出力されるので、「証明書のインストール」にカーソルを合わせて左クリックします。



- 「証明書のインポートウィザード」のウィンドウが出力されるので、「ローカルコンピューター」を左クリックし、「次へ」にカーソルを合わせて左クリックします。

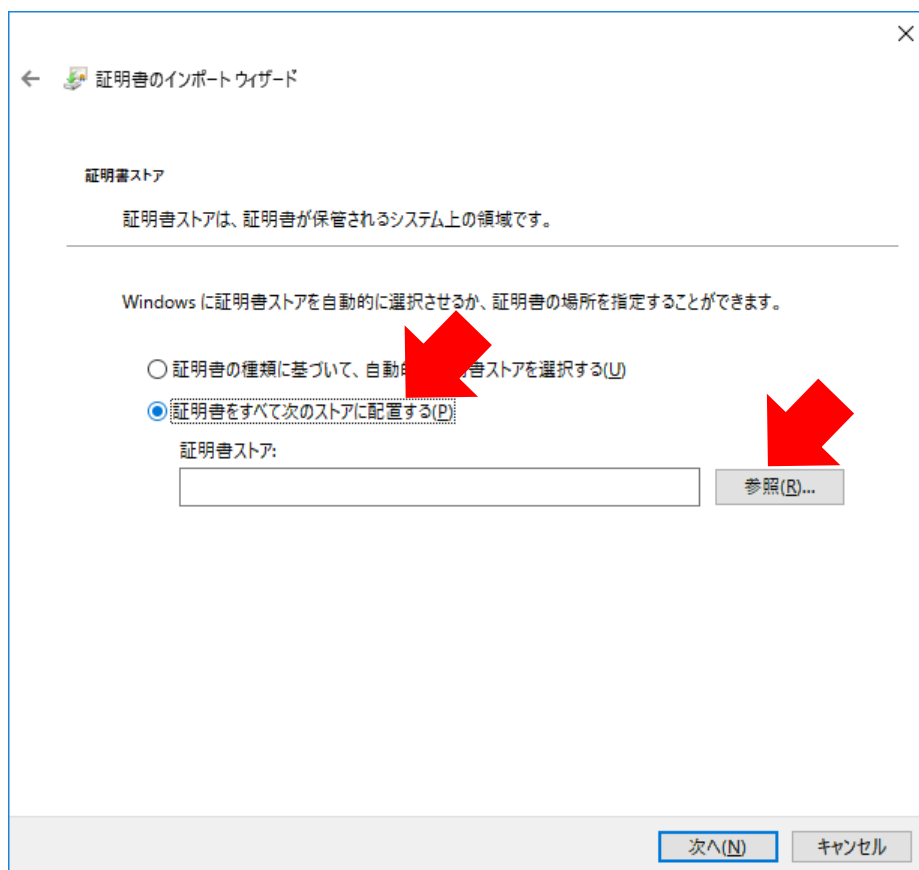


RICOH

- 以下のように「ユーザーアカウント制御」画面が出力される場合は「はい」へカーソルを合わせて左クリックします。

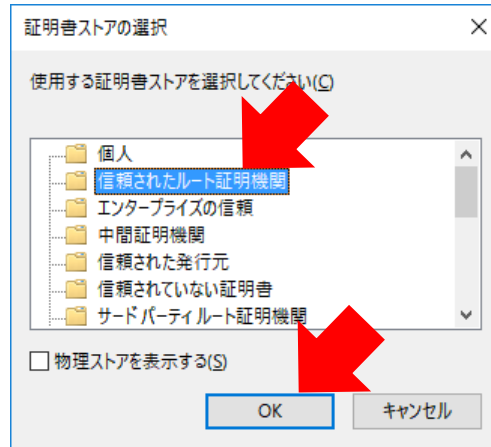


- 「証明書をすべての次のストアに配置する」を左クリックし、「参照」にカーソルを合わせて左クリックします。

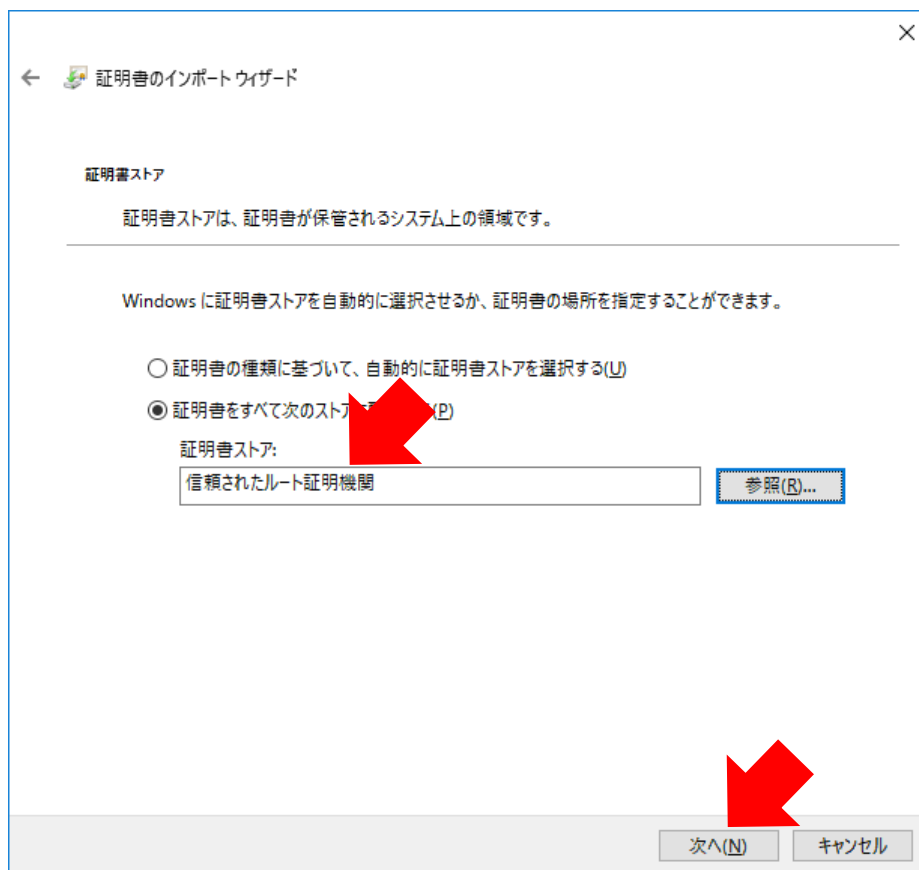


RICOH

- 「証明書ストアの選択」の画面が出力されるので「信頼されたルート証明書」にカーソルを合わせて左クリック後、「OK」にカーソルを合わせて左クリックします。

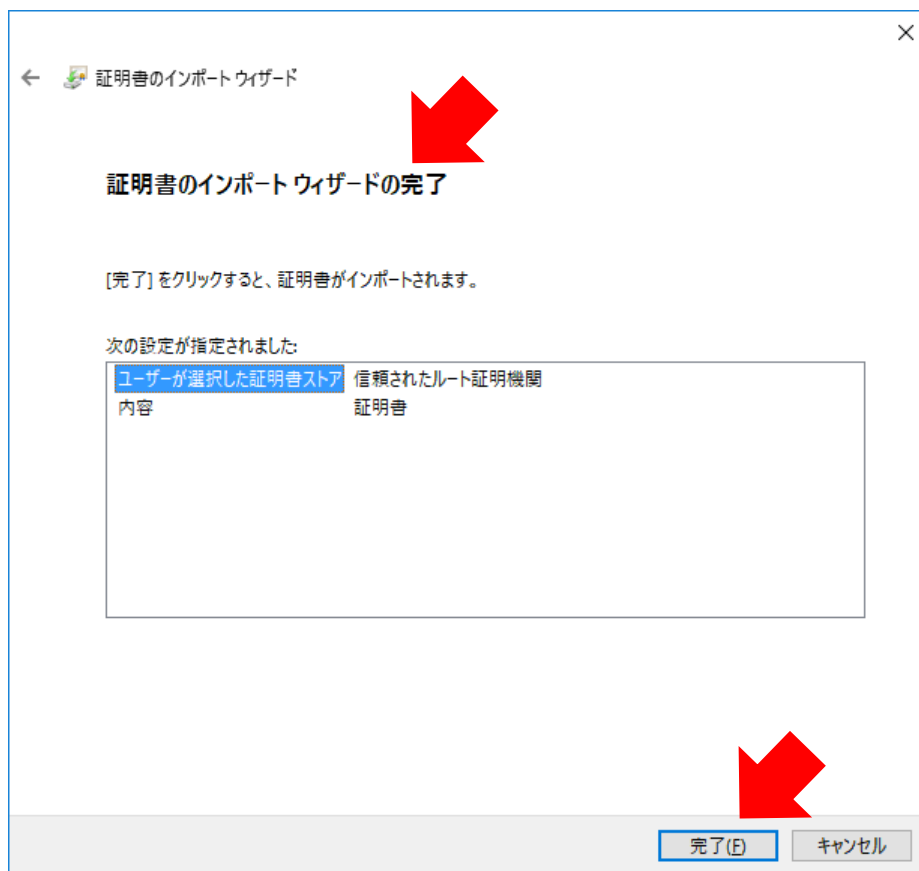


- 「証明書のインポートウィザード」の「証明書ストア」の項目に「信頼されたルート証明機関」が入力されたことを確認したら、「次へ」にカーソルを合わせて左クリックします。

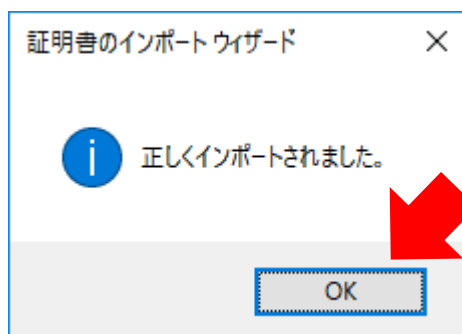


RICOH

- 「証明書のインポートウィザード」のウィンドウにて「証明書のインポートウィザードの完了」と表示されるので「完了」にカーソルを合わせて左クリックします。



- CA 証明書が正しくインポートされると以下のように完了画面が出力されるので「OK」にカーソルを合わせて左クリックします。



- インポートが完了したら、Web ブラウザ（FireFox 以外）で [P22 「4-② HTTPS の Web ページにて警告が出力され、閲覧できない」](#) のような警告が表示されないことを確認してください。

RICOH

4-②-(3) ローカル CA 証明書の Firefox へのインポート

Firefox にて https の Web サイトを閲覧する場合については Firefox 自体で証明書管理機能を持っているため、Firefox 自体に CA 証明書のインポートが必要です。

Firefox にて https ページを閲覧する場合にのみ本作業が必要になります。

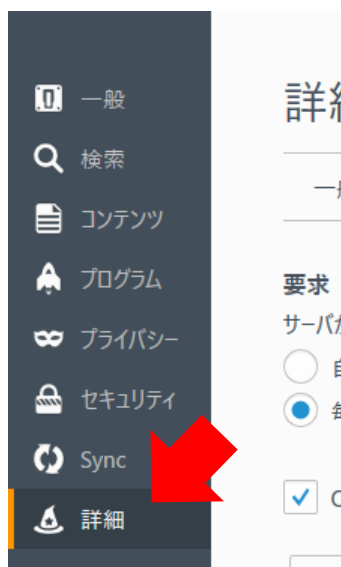
それ以外の Web ブラウザにて Web ページを閲覧する場合には本作業は必要ありません。

- Firefox の右上にあるメニューにカーソルを合わせて左クリックし、「オプション」にカーソルを合わせて左クリックします。



RICOH

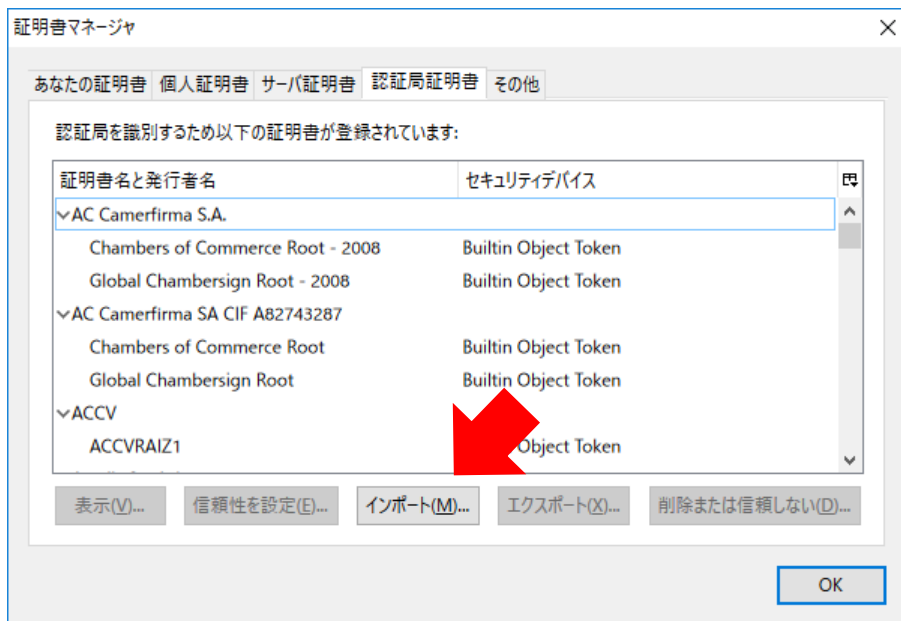
- オプションメニューが開かれたら、左側ペインにて「詳細」にカーソルを合わせて左クリックします。



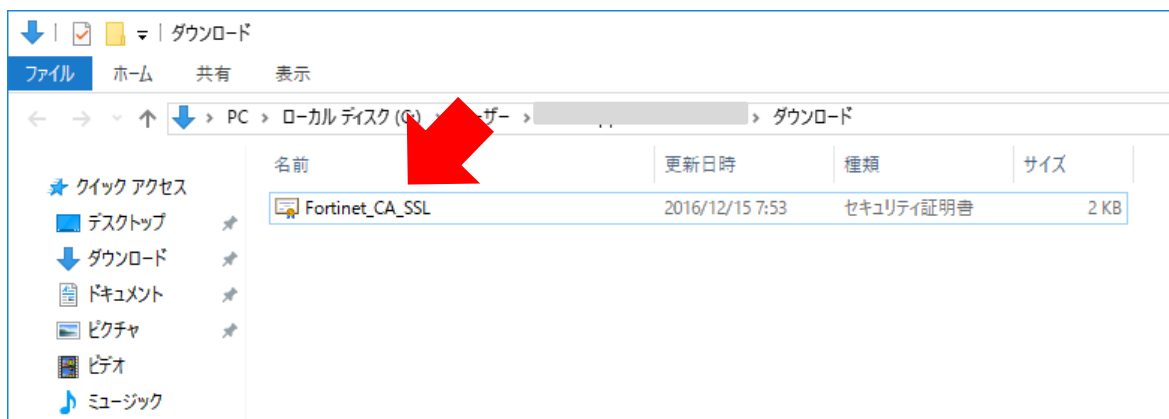
- 右側ペインに移り、「証明書」にカーソルを合わせて左クリックし、「証明書を表示」にカーソルを合わせて左クリックします。



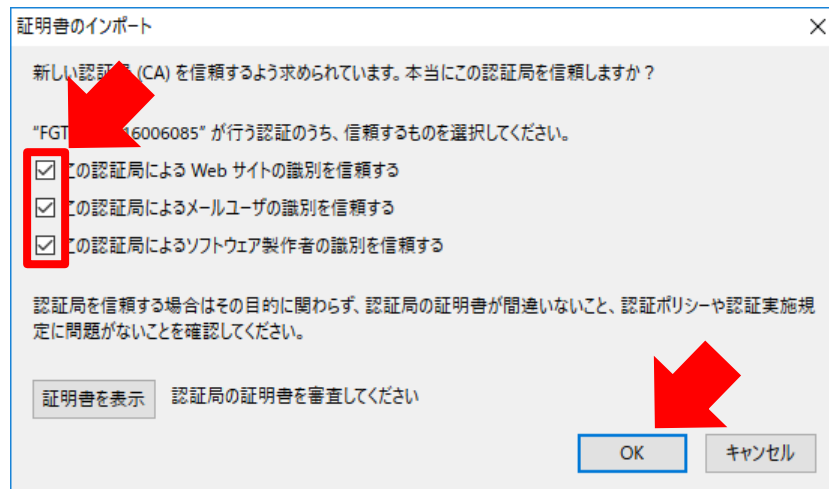
- 「証明書マネージャ」が表示されたら、「インポート」へカーソルを合わせて左クリックします。



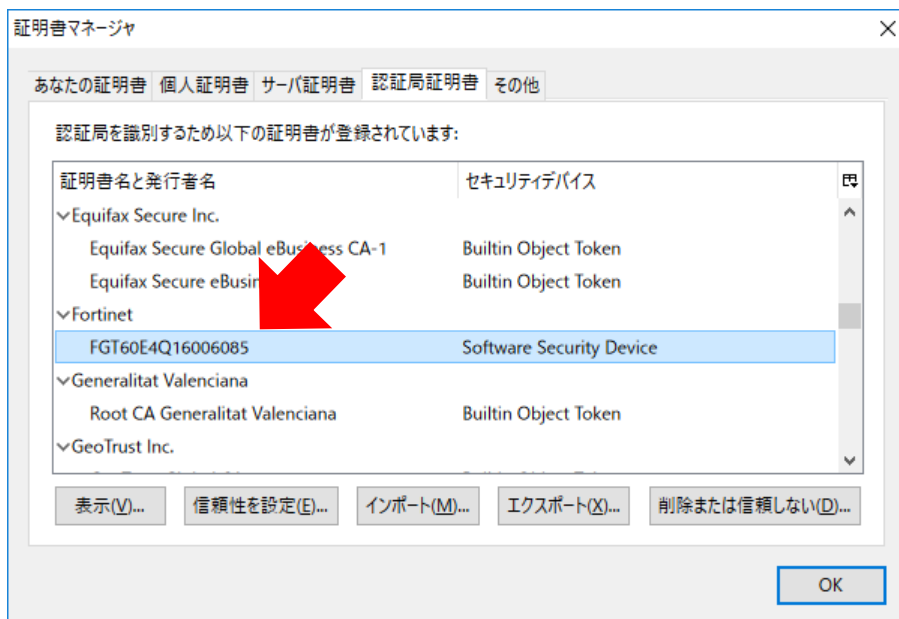
- 「インポート」をクリックすると Windows エクスプローラが開かれるので、[P23「4-②-\(1\) FortiGate ローカル CA 証明書のダウンロード」](#)にてダウンロード・保存した「Fortinet_CA_SSL.cer」をダブルクリックします。



- 「証明書のインポート」のウィンドウが表示されるので、以下の図のように全てのチェックボックスをクリックしてチェックし、「OK」を左クリックします。



- 「証明書マネージャ」の画面に戻るので、画面をスクロールして Fortinet 以下のような表示で証明書がインポートされていることを確認したら、「OK」にカーソルを合わせて左クリックし、インポート完了になります。



- インポートが完了したら、FireFox にて [P22 「4-② HTTPS の Web ページにて警告が出力され、閲覧できない」](#) のような警告が表示されないことを確認してください。

4-②-(4) SSL インспекション機能の無効化

https 等の SSL 通信の安全性を検査する SSL インспекション機能を無効化します。

⚠ 本機能を無効化すると、SSL 通信の安全性を確保する UTM 機能が無効になるので注意してください。

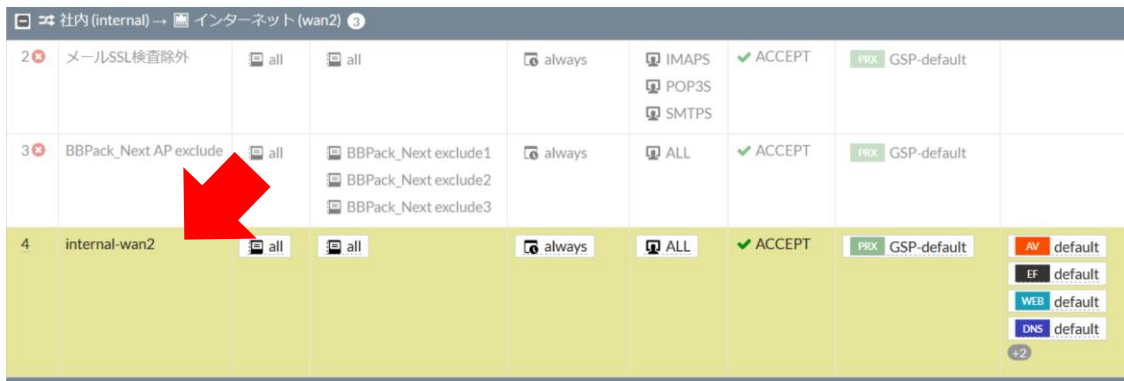
- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 左側ペインの「ポリシー&オブジェクト」へカーソルを合わせて左クリックし、展開されたメニューの「IPv4 ポリシー」へカーソルを合わせて左クリックします。



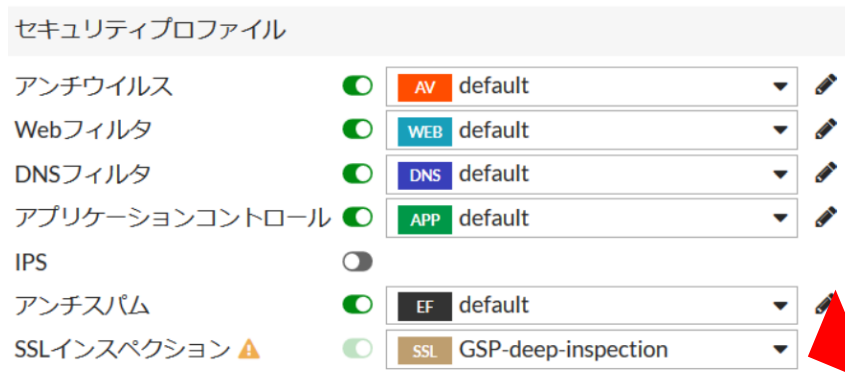
- 右側ペインに移り、「社内（Internal） - インターネット（WAN2）（2-3）」にカーソルを合わせて左クリックします。



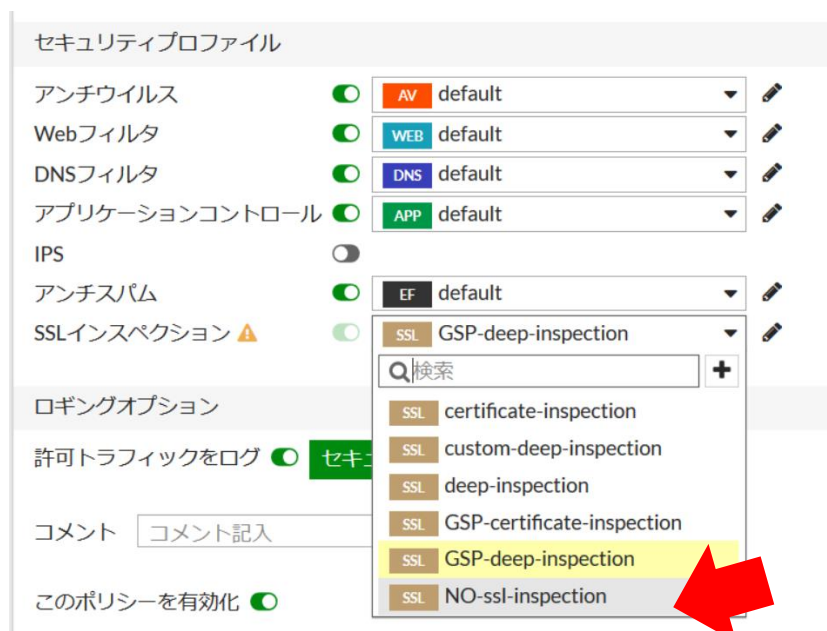
- 右側ペインの「社内 (Internal) - インターネット (WAN2) (2-3)」が展開されるので、「internal-wan2」の項目をダブルクリックします。



- 右側ペインの画面が切り替わり、中段の「セキュリティプロファイル」の項目にあるリストボタンにカーソルを合わせて左クリックします。



- 複数の選択リストが出てきますので「NO-SSL-inspection」を選択します。



- クリック後、スイッチマークが黒くなるので右側ペイン下部の「OK」を左クリックします。

セキュリティプロファイル

アンチウイルス AV default

Webフィルタ WEB default

DNSフィルタ DNS default

アプリケーションコントロール APP default

IPS

アンチスパム EF default

SSLインスペクション SSL NO-ssl-inspection

ロギングオプション

許可トラフィックをログ セキュリティイベント すべてのセッション

コメント 0/1023

このポリシーを有効化

OK キャンセル

- 設定が完了したら、Web ブラウザで [P22 「4-② HTTPS の Web ページにて警告が出力され、閲覧できない」](#) のような警告が表示されないことを確認してください。
- Web ページが閲覧できることを確認したら、[P10 「3-④ 設定のバックアップ」](#) にて変更した設定のバックアップを取得してください。

4-③ Web ページの閲覧をブロックしたい

FortiGate にて特定のカテゴリの Web ページや特定 URL の Web ページの閲覧をブロックする場合には以下の方法で設定します。

- 解決方法 1

Web ページが属するカテゴリごと閲覧をブロックする

上記の方法では例として「ソーシャル・ネットワーキング」のカテゴリに属する Twitter、Facebook、Instagram などの SNS サービスの Web ページ全ての閲覧をブロックしたい場合に使用します。

本方法でカテゴリごと閲覧をブロックする場合は [38 「4-③-\(1\) FortiGuard カテゴリーによるブロックの設定方法」](#)を参照します。

- 解決方法 2

Web ページが属するカテゴリの閲覧設定は維持しつつ、特定 URL の Web ページのみ閲覧をブロックする

上記の方法では例として「ソーシャル・ネットワーキング」のカテゴリに属する Web ページは基本的に閲覧を許可する設定を維持したい状態で、Twitter だけの閲覧をブロックしたい場合などに使用します。

本方法でブロックを解除する場合は [P43 「4-③-\(2\) URL フィルタによる特定 URL のみ除外\(ブロック解除\)する 設定方法」](#)を参照します。

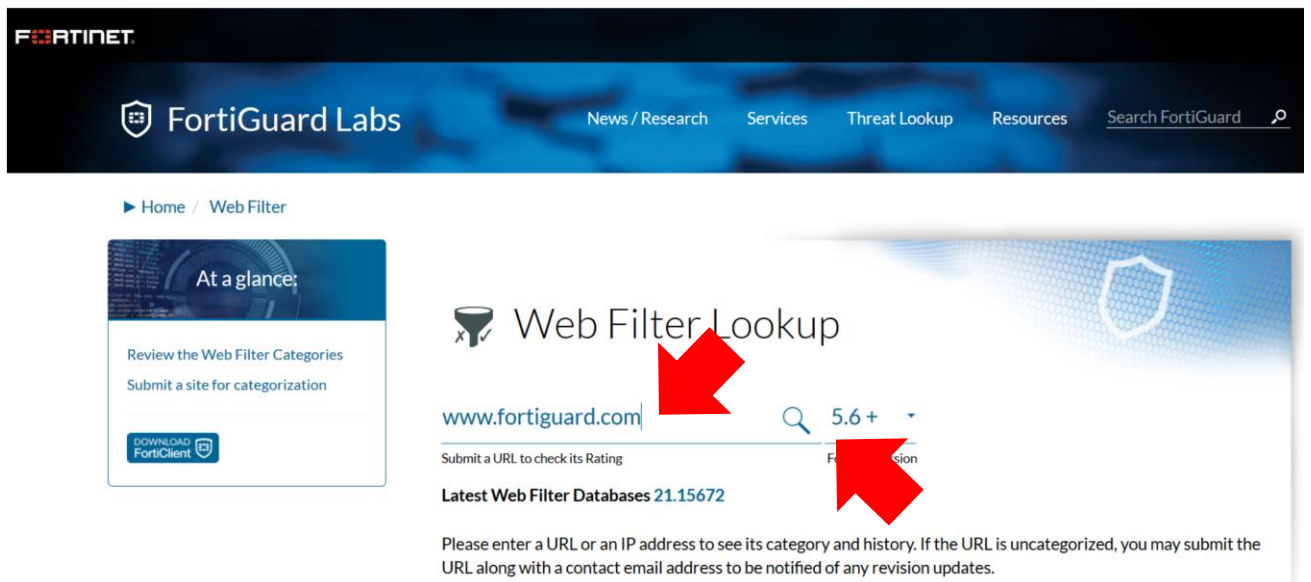
4-③-(1) FortiGuard カテゴリによるブロックの設定方法

Web ページのカテゴリによるブロックをカテゴリごとブロックする場合には以下の手順にて実施します。

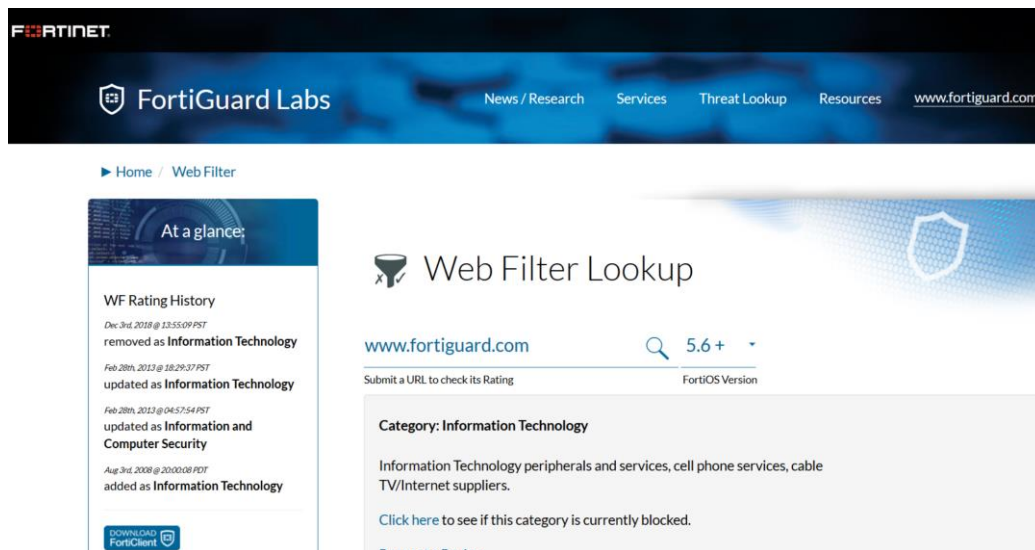
- インターネットに接続されている PC の Web ブラウザにて以下の URL へアクセスします。
(英語サイトのみ提供)

<http://www.fortiguards.com/webfilter>

- FortiGuard Center にアクセスできたら、画面中央にある「Search URL」の項目の検索ボックスにブロックしたい対象の URL を入力し、「虫眼鏡」にカーソルを合わせてクリックします (下記の URL は例)。



- 検索結果が表示されるので、「Category:」の項目に表示されているカテゴリを確認します。
(以下の出力については例)



- カテゴリについては大カテゴリにある小カテゴリが表示されるため、実際に FortiGate の画面のどの大カテゴリに含まれるかは「<http://fortiguard.com/webfilter/categories>」にて確認できます。

Web Filter Categories

FortiGuard URL Database Categories are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families. They also take into account customer requirements for Internet management. The categories are defined to be easily manageable and patterned to industry standards.

Each category contains websites or web pages that have been assigned based on their dominant Web content. A website or webpage is categorized into a specific category that is likely to be blocked according to its content. When a website contains elements in different categories, web pages on the site are separately categorized.

Descriptions of the categories are designed to assist the reader with category comprehension only; they are not meant to depict any form of symbolic representation of the individuals who own or surf these sites.

Adult / Mature Content

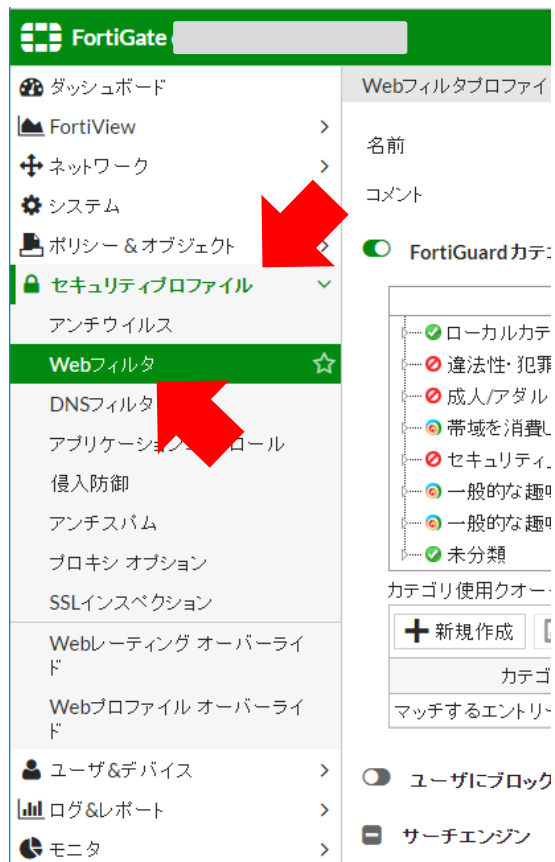
Category	Description	
Abortion	Websites pertaining to abortion data, information, legal issues, and organizations.	Test
Advocacy Organizations	This category caters to organizations that campaign or lobby for a cause by building public awareness, raising support, influencing public policy, etc.	Test
Alcohol	Websites which legally promote or sell alcohol products and accessories.	Test
Alternative Beliefs	Websites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings.	Test
Dating	Websites that allow individuals to make contact and communicate with each other over the Internet, usually with the objective of developing a personal,	Test

- 本サービスにて提供されている FortiGate では日本語でのサービス提供のため、「FortiGuard Center」の Web ページにて表示されます。

各大カテゴリは FortiGate の「FortiGuard カテゴリによるフィルタ」では以下のように表示されます。

FortiGate の「FortiGuard カテゴリによるフィルタ」での表示	FortiGuard Center Web ページでの表示
違法性・犯罪性の高いサイト	Potentially Liabile
成人/アダルトコンテンツ	Adult/Mature Content
帯域を消費しやすいサイト	Bandwidth Consuming
セキュリティ上問題のあるサイト	Security Risk
一般的な趣味・関心 - 個人	General Interest - Personal
一般的な趣味・関心 - ビジネス	General Interest - Business

- ブロックしたい対象の Web ページのカテゴリを確認したら、[P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の管理画面にログインします。
- 管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせてクリックするとメニューが展開されるので「Web フィルタ」をクリックします。



RICOH

- 右側ペインにある「FortiGuard カテゴリーによるフィルタ」にて事前に確認した対象のカテゴリを大カテゴリの中より探し、一番左の + を左クリックして大カテゴリの詳細を展開します。

FortiGuard カテゴリーによるフィルタ

事前に設定されたフィルタ **カスタム** G PG-13 R

表示 すべて

- ローカルカテゴリ
- 違法性・犯罪性の高いサイト
- 成人/アダルトコンテンツ
- 帯域を消費しやすいサイト
- セキュリティ上問題のあるサイト
- 一般的な趣味・関心-個人
- 一般的な趣味・関心-ビジネス
- 未分類

カテゴリ使用クォータ ⓘ

+ 新規作成 編集 削除

カテゴリ	クォータ
マッチするエントリーはありません。	

- 右側ペインにある「FortiGuard カテゴリーによるフィルタ」にて事前に確認した対象のカテゴリをマウスの右クリックを押下すると、メニューが出力されるので「ブロック」を左クリックで選択します。

FortiGuard カテゴリーによるフィルタ

事前に設定されたフィルタ **カスタム** G PG-13 R

表示 すべて

- ローカルカテゴリ
- 違法性・犯罪性の高いサイト
- 成人/アダルトコンテンツ
- 帯域を消費しやすいサイト
- セキュリティ上問題のあるサイト
- 一般的な趣味・関心-個人
- 一般的な趣味・関心-ビジネス

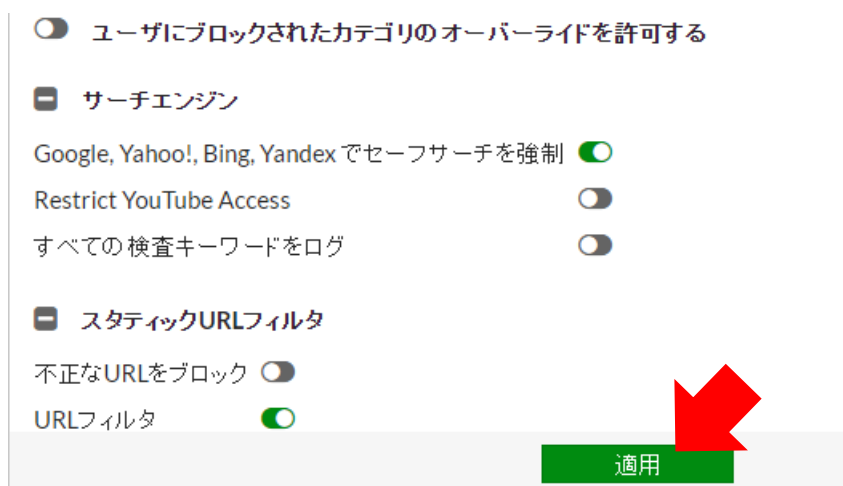
- IT
 - 許可
 - 許可
 - ブロック
 - モニタリング
 - モニタリング
 - 警告
 - 警告
 - 認証

カテゴリ

+ 新規作成 編集 削除

RICOH

- 設定が完了したら、右側ペインの下部にある「適用」にカーソルを合わせて左クリックします。



- 設定を適用後、該当するカテゴリの Web ページが閲覧できないことを確認してください。
- Web ページが閲覧できないことを確認したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-③-(2) URL フィルタによる特定 URL のみ除外(ブロック解除)する 設定方法

Web フィルタリング機能の “カテゴリによる閲覧ブロック” は維持した状態で特定 URL の Web ページ閲覧を許可する際に以下の手順にて実施します。

⚠ 本設定では設定した URL の通信に関してはアンチウイルス機能が適用されなくなるので注意してください。

- [P3「3-① FortiGate ダッシュボード \(機器管理画面\) へのログイン」](#)の章を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせて左クリックすると「セキュリティプロファイル」メニューが展開されるので「Web フィルタ」をクリックします。



RICOH

- 右側ペインを中段までスクロールしたところに「スタティックURLフィルタ」にて「新規作成」へカーソルを合わせて左クリックします。



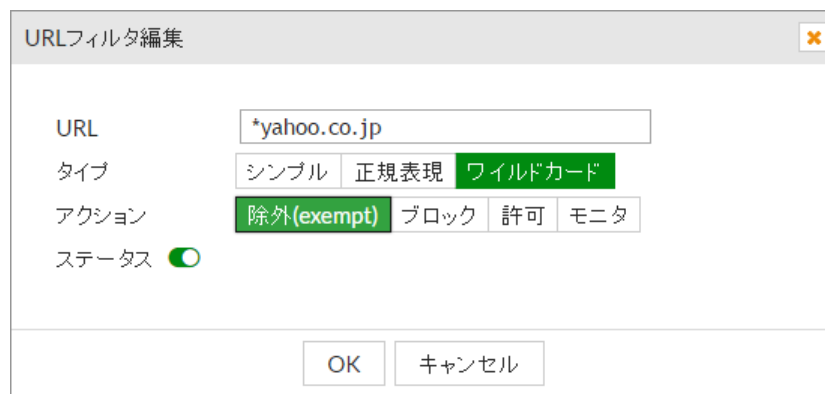
- 以下のように「URL フィルタ作成」のウィンドウが出現するため、「URL」の入力ボックスにWEB 閲覧を可能としたい URL を入力します。



★ワンポイント★

URL ブロックにて Yahoo Japan のような ” www.yahoo.co.jp ” ” news.yahoo.co.jp ” ” mail.yahoo.co.jp ” のように関連する URL が ” 多岐に渡る場合、「*yahoo.co.jp」のように URL ドメインの前にアスタリスクを付与することでYahoo! Japan の関連する全てのページを除外することができます。

(*yahoo.co.jp = www.yahoo.co.jp や news.yahoo.co.jp や mail.yahoo.co.jp も含む)



- 最後に右側ペイン下部の「適用」をクリックします。

■ スタティックURLフィルタ

不正なURLをブロック

URLフィルタ

URL	タイプ	アクション	ステータス
www.netricoh.com	シンプル	🚫 ブロック	❌ 無効
.*update\.microsoft\.com.*	正規表現	⊖ 除外(exempt)	✅ 有効
.*download\.windowsupdate\.com.*	正規表現	⊖ 除外(exempt)	✅ 有効
\.microsoft\.com.	正規表現	⊖ 除外(exempt)	✅ 有効
login.live.com	シンプル	⊖ 除外(exempt)	✅ 有効
\.windowsupdate\.com.	正規表現	⊖ 除外(exempt)	✅ 有効
www.fortinet.co.jp	シンプル	⊖ 除外(exempt)	✅ 有効

FortiSandboxにより検知された悪意のあるURLをブロック

Webコンテンツフィルタ


■ レーティングオプション

レーティングエラー発生時にWebサイトを許可

ドメインまたはIPアドレスでURLをレーティング

URLでイメージを評価

適用

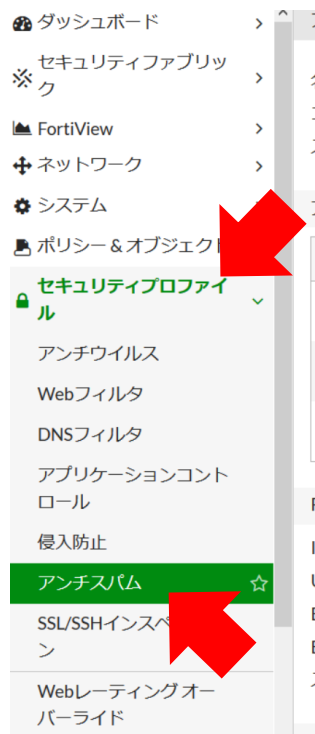


- 設定した URL の Web ページ閲覧が閲覧出来る事を確認してください。
- Web ページが閲覧できることを確認したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-④ 受信したメールをスパム判定させたい

PC の E-mail クライアントにて受信したメールをスパム判定させたい場合、以下の手順にてスパム判定させる設定を行います。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アンチスパム」を左クリックします。



- 右側ペイン「ローカルスパムフィルタリング」にある「ブラック/ホワイトリスト」にチェックがついていることを確認します。チェックが付いていない場合は左クリックします。

ローカルスパムフィルタリング

- HELO DNSルックアップ
- リターンEメールDNSチェック
- ブラック/ホワイトリスト

- 以下のように新しくスパムフィルタリングのルール設定が作成できるようになります。
「タイプ」の選択ボックスは「Email ワイルドカード」を左クリックします。
「パターン」の入力ボックスにスパム判定させたい任意の E-mail アドレスを入力します。
「アクション」の選択ボックスは「スパムとしてマーク」を左クリックします。
最後に「OK」ボタンを左クリックします。(以下は例)

アンチスパムのブラックリスト・ホワイトリストエントリの作成

タイプ	<input type="text" value="IP/ネットマスク"/> <input type="text" value="IPv6/ネットマスク"/> <input type="text" value="Eメール正規表現"/> <input type="text" value="Eメールワイルドカード"/>
パターン	<input type="text" value="abc@example.com"/>
アクション	<input type="text" value="拒否としてマーク"/> <input type="text" value="スパムとしてマーク"/> <input type="text" value="してマーク"/>
ステータス	<input checked="" type="radio"/>

★ワンポイント★

ドメイン単位でブロックしたい場合には「パターン」の入力ボックスに以下のように @ (アットマーク) の前に「* (アスタリスク)」を入力後、任意の E-mail アドレスの@以降を入力することにより、ドメイン単位でのスパム判定ができます。
(以下の E-mail アドレスは例)

アンチスパムのブラックリスト・ホワイトリストエントリの作成

タイプ	<input type="text" value="IP/ネットマスク"/> <input type="text" value="IPv6/ネットマスク"/> <input type="text" value="Eメール正規表現"/> <input type="text" value="Eメールワイルドカード"/>
パターン	<input type="text" value="*@example.com"/>
アクション	<input type="text" value="拒否としてマーク"/> <input type="text" value="スパムとしてマーク"/> <input type="text" value="クリアとしてマーク"/>
ステータス	<input checked="" type="radio"/>

RICOH

- 「ローカルスパムフィルタリング」のリストに設定した内容が登録されていることを確認します。

ローカルスパムフィルタリング

HELO DNSルックアップ

リターンEメールDNSチェック

ブラック/ホワイトリスト

+ 新規作成				✎ 編集	🗑 削除
タイプ	パターン	アクション	ステータス		
Eメール..	abc@exam...	スパムとし...	✔ 有効		

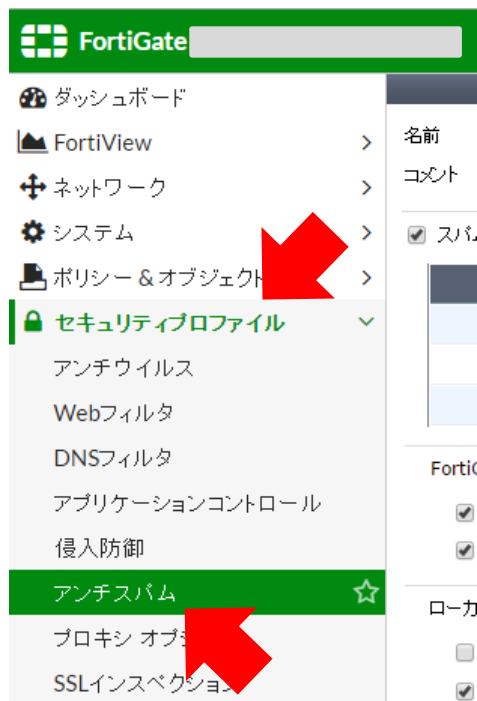
適用

- 対象となる E-mail アドレスのからのメールがスパム判定されることを確認します。
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-⑤ 受信したメールをスパム判定させたくない

PC の E-mail クライアントにて受信したメールがスパムメールではないにも関わらず、スパム判定されてしまう場合は以下の手順にてスパム判定より除外する設定を行います。FortiGate のアンチスパム機能にて E-mail がスパム判定された場合は E-mail の件名に [spam] の文字列が付与されます。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アンチスパム」を左クリックします。



- 右側ペイン「ローカルスパムフィルタリング」にある「ブラック/ホホワイトリスト」にチェックがついていることを確認します。チェックが付いていない場合は左クリックします。



RICOH

- 「以下のように新しくスパムフィルタリングのルール設定が作成できるようになります。
「タイプ」の選択ボックスは「Email ワイルドカード」を左クリックします。
「パターン」の入力ボックスにスパム判定させたくない任意の E-mail アドレスを入力します。
「アクション」の選択ボックスは「クリアとしてマーク」を左クリックします。
最後に「OK」ボタンを左クリックします。(以下は例)

アンチスパムのブラックリスト・ホワイトリストエントリの作成

タイプ	IP/ネットマスク
	IPv6/ネットマスク
	Eメール正規表現
	Eメールワイルドカード
パターン	abc@example.com
アクション	拒否としてマーク
	スパムとしてマーク
	クリアとしてマーク
ステータス	<input checked="" type="radio"/>

OK キャンセル

★ワンポイント★

ドメイン単位でスパム判定させたくない場合には「パターン」の入力ボックスに以下のように @ (あっとマーク) の前に「* (アスタリスク)」を入力後、任意の E-mail アドレスの@以降を入力することでドメイン単位でのスパム判定を解除できます。

(以下の E-mail アドレスは例)

アンチスパムのブラックリスト・ホワイトリストエントリの作成

タイプ	IP/ネットマスク
	IPv6/ネットマスク
	Eメール正規表現
	Eメールワイルドカード
パターン	* @example.com
アクション	拒否としてマーク
	スパムとしてマーク
	クリアとしてマーク
ステータス	<input checked="" type="radio"/>

OK キャンセル

RICOH

- 「ローカルスパムフィルタリング」のリストに設定した内容が登録されていることを確認します。

ローカルスパムフィルタリング

HELO DNSロックアップ

リターンEメールDNSチェック

ブラック/ホホワイトリスト

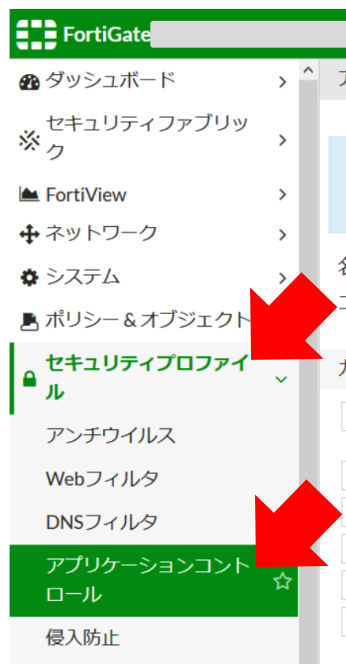
タイプ	パターン	アクション	ステータス
Eメール	abc@exam...	クリアとし...	有効

- 対象となる E-mail アドレスのからのメールがスパム判定されないことを確認します。
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-⑥ 特定アプリケーションの動作をブロックしたい

特定のアプリケーションの使用をブロックしたい場合には以下のように設定します。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アプリケーションコントロール」にカーソルを合わせて左クリックします。



- 右側ペインにて「アプリケーションオーバーライド」の項目にある「シグネチャ追加」にカーソルを合わせて左クリックします。

アプリケーションオーバーライド

アプリケーションシグネチャ	カテゴリ	
<input type="checkbox"/> Share	P2P	<input type="checkbox"/> ブロック ▼
<input type="checkbox"/> Winny	P2P	<input type="checkbox"/> ブロック ▼

- シグネチャリストが出てくるので、「フィルタを追加」にカーソルを合わせて左クリックします。

シグネチャ追加

すべてを選択 フィルタ追加 All Cloud 選択済み: 0/21

名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■■
2ch	Social.Media	Browser-Based	★★★★☆	■■■■■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■■
3PC	Network.Service	Network-Protocol	★★★★☆	■■■■■

- 「フィルタを追加」を選択すると、どの検索フィルタにてアプリケーションを検索するか選ぶことができるので、ここでは「名前」を例にカーソルを合わせて左クリックします。

シグネチャ追加

すべてを選択 All Cloud 選択済み: 0/21

名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■■
2ch	Social.Media	Browser-Based	★★★★☆	■■■■■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■■
3PC	Network.Service	Network-Protocol	★★★★☆	■■■■■
4shared	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
4shared_File.Down	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
4shared_File.Uplo	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
5ch	Social.Media	Browser-Based	★★★★☆	■■■■■

- 検索ボックスにブロック対象としたいアプリケーションの名前を検索ボックスに入力し、Enter キーを押下します（下記の検索については例です。）。

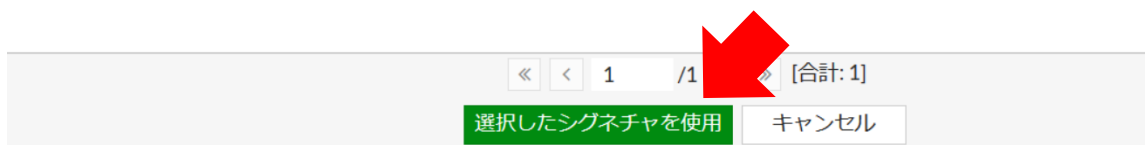
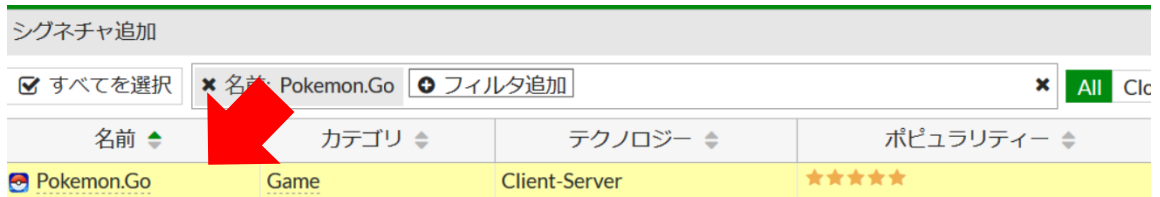
シグネチャ追加

すべてを選択 名前: pokemon All Cloud 選択済み: 0/21

名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■■
2ch	Social.Media	Browser-Based	★★★★☆	■■■■■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■■
3PC	Network Service	Network-Protocol	★★★★☆	■■■■■

RICOH

- 検索結果が表示されるので、対象のアプリケーションであればアプリケーション名にカーソルを合わせて左クリック後、右側ペイン下部の「選択したシグネチャを使用」をにカーソルを合わせてクリックします。



RICOH

- 対象となるアプリケーションが「アプリケーションオーバーライド」項目のリストに登録されたことを確認したら、右側ペイン下部の「適用」にカーソルを合わせて左クリックします。

アプリケーションセンサーの編集

カテゴリ

すべてのカテゴリ

<input type="checkbox"/> Business (144, ☰ 6)	<input type="checkbox"/> Cloud.IT (43)	<input type="checkbox"/> Collaboration (268, ☰ 10)	<input type="checkbox"/>
<input type="checkbox"/> Game (87)	<input type="checkbox"/> General.Interest (231, ☰ 7)	<input type="checkbox"/> Mobile (3)	<input type="checkbox"/>
<input type="checkbox"/> P2P (63)	<input type="checkbox"/> Proxy (167)	<input type="checkbox"/> Remote.Access (84)	<input type="checkbox"/>
<input type="checkbox"/> Storage.Backup (173, ☰ 17)	<input type="checkbox"/> Update (50)	<input type="checkbox"/> Video/Audio (160, ☰ 14)	<input type="checkbox"/>
<input type="checkbox"/> Web.Client (23)	<input type="checkbox"/> 不明なアプリケーション		

アプリケーションオーバーライド

アプリケーションシグネチャ	カテゴリ	
Pokemon.Go	Game	<input type="checkbox"/> ブロック
Share	P2P	<input type="checkbox"/> ブロック
Winny	P2P	<input type="checkbox"/> ブロック

フィルタオーバーライド

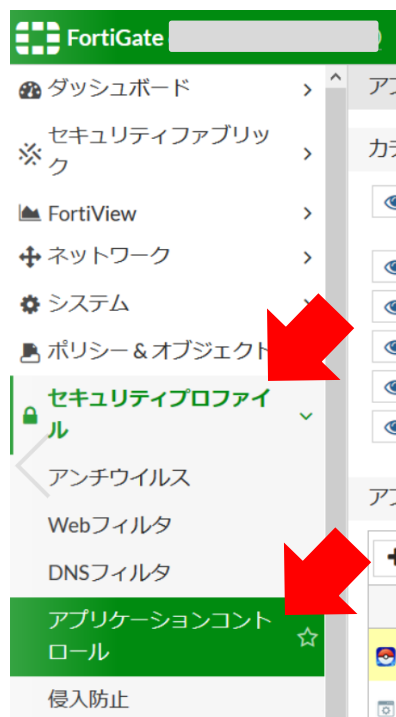
フィルタ詳細	<input type="button" value="適用"/>	アク
--------	-----------------------------------	----

- 適用後、ブロック設定したアプリケーションが正しく動作しないことを確認してください。（動作についてはアプリケーション毎に異なります。）
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-⑦ 特定アプリケーションの動作ブロックを解除したい



設定されている特定アプリケーションの動作ブロックを解除する場合は以下のように設定します。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アプリケーションコントロール」にカーソルを合わせて左クリックします。



- 右側ペインの「アプリケーションオーバーライド」のリストにあるブロック設定を解除したいアプリケーションにカーソルを合わせて左クリックします。

アプリケーションオーバーライド

+ シグネチャ追加 ✎ パラメータ編集 🗑️ 削除		
	アプリケーションシグネチャ	カテゴリ
	Pokemon.Go	Game
<input type="checkbox"/>	Share	P2P
	Winny	P2P

RICOH

- ブロック設定を解除したいアプリケーションを左クリックにて選択したら、「削除」にカーソルを合わせて左クリックします。

アプリケーション オーバーライド

+ シグネチャ追加		パラメータ編集	削除
アプリケーションシグネチャ		カテゴリ	
Pokemon.Go		Game	
Share		P2P	
Winny		P2P	

- 削除が完了したら、画面下部の「適用」にカーソルを合わせて左クリックします。

アプリケーションセンサーの編集 default + 🗑️ ☰ [アプリケーションシグネチャを表示]

名前

コメント 8/255

カテゴリ

<input checked="" type="checkbox"/> Botnet	<input type="checkbox"/> Game	<input type="checkbox"/> Proxy	<input type="checkbox"/> Video/Audio
<input type="checkbox"/> Business	<input type="checkbox"/> General.Interest	<input type="checkbox"/> Remote.Access	<input type="checkbox"/> VoIP
<input type="checkbox"/> Cloud.IT	<input type="checkbox"/> Mobile	<input type="checkbox"/> Social.Media	<input type="checkbox"/> Web.Client
<input type="checkbox"/> Collaboration	<input type="checkbox"/> Network.Service	<input type="checkbox"/> Storage.Backup	<input type="checkbox"/> 不明なアプリケーション
<input type="checkbox"/> Email	<input checked="" type="checkbox"/> P2P	<input type="checkbox"/> Update	

アプリケーション オーバーライド

+ シグネチャ追加			パラメータ編集	削除
アプリケーションシグネチャ		カテゴリ	アクション	
<input type="checkbox"/> Share		P2P	<input checked="" type="checkbox"/> ブロック	
Winny		P2P	<input checked="" type="checkbox"/> ブロック	

オーバーライドでフィルタ

+ フィルタ追加		編集	削除
詳細でフィルタ		アクション	
マッチするエントリーはありません。			

オプション

DNSトラフィックの許可とログ

HTTPベースアプリケーションの差し替えメッセージ

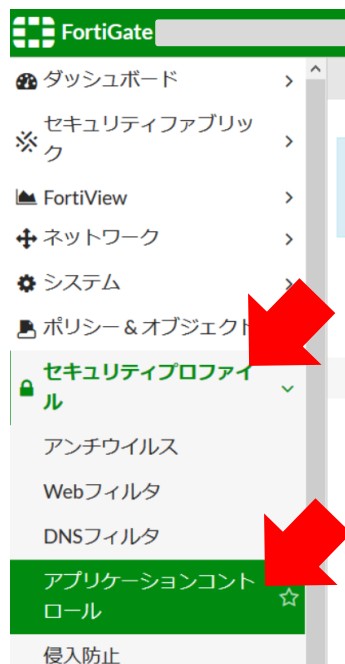
適用

- 適用後、ブロックの解除設定したアプリケーションが正しく動作することを確認してください。（動作についてはアプリケーション毎に異なります。）
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

4-⑧ 特定カテゴリのアプリケーションの動作をブロックしたい

特定カテゴリのアプリケーションの使用をブロックしたい場合には以下のように設定します。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アプリケーションコントロール」にカーソルを合わせて左クリックします。



- 右側ペインにアプリケーションセンサーの編集画面が表示されるので、ブロックしたいカテゴリの名前横のアイコンにカーソルを合わせて左クリックします。
ここでは「Game」のカテゴリをブロックする例にて説明します。



RICOH

- アイコンをクリックすると、以下のように動作メニューが出てくるので「ブロック」にカーソルを合わせて左クリックします。
設定が完了したら、画面下部の「適用」にカーソルを合わせて左クリックします。

The screenshot shows the 'カテゴリ' (Category) selection screen. A dropdown menu is open for the 'Game (87)' category, with 'ブロック' (Block) selected. A red arrow points to this menu. Below the categories, there is a table of application signatures with their categories and actions. A red arrow points to the '適用' (Apply) button at the bottom.

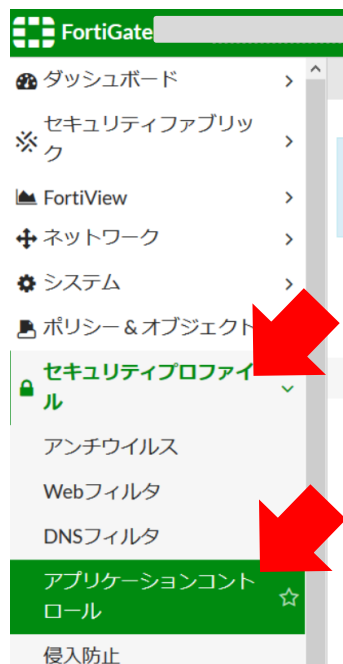
アプリケーションシグネチャ	カテゴリ	アクション
Share	P2P	ブロック
Winny	P2P	ブロック

- 適用後、ブロック設定したアプリケーションが正しく動作しないことを確認してください。
(動作についてはアプリケーション毎に異なります。)
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得して下さい。

4-⑨ 特定カテゴリのアプリケーションのブロックを解除したい

特定カテゴリのアプリケーションのブロックを解除したい場合には以下のように設定します。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アプリケーションコントロール」にカーソルを合わせて左クリックします。



- 右側ペインにアプリケーションセンサーの編集画面が表示されるので、ブロックを解除したいカテゴリの名前横のアイコンにカーソルを合わせて左クリックします。
ここでは「Game」のカテゴリを解除する例にて説明します。



RICOH

- アイコンをクリックすると、以下のように動作メニューが出てくるので「モニタ」にカーソルを合わせて左クリックします。
設定が完了したら、画面下部の「適用」にカーソルを合わせて左クリックします。

カテゴリ

すべてのカテゴリ

- Business (144, 17)
- Game (87)
- モニタ
- 許可
- ブロック
- 隔離
- サインネチャを表示(87)

- Cloud.IT (43)
- General.Interest (231, 7)
- Proxy (167)
- Update (50)
- 不明なアプリケーション

- Collaboration (268, 10)
- Mobile (3)
- Remote.Access (84)
- Video/Audio (160, 14)

- Email (80, 12)
- Network.Service (329)
- Social.Media (121, 31)
- VoIP (24)

アプリケーションサインネチャ

アプリケーションサインネチャ	カテゴリ	アクション
Share	P2P	ブロック
Winny	P2P	ブロック

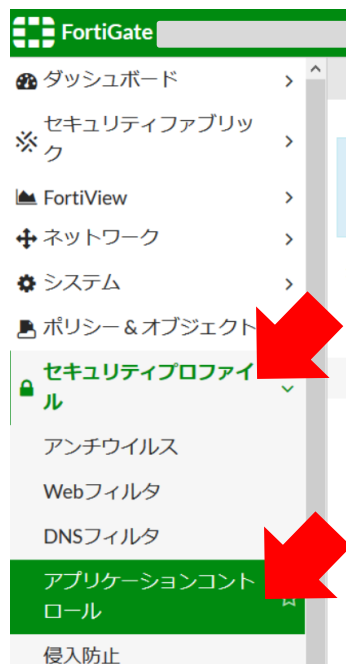
適用

- 適用後、カテゴリブロックの解除設定したアプリケーションが動作することを確認してください。
(動作についてはアプリケーション毎に異なります。)
- 動作確認が完了したら、[P10「3-④ 設定のバックアップ」](#)にて変更した設定のバックアップを取得してください。

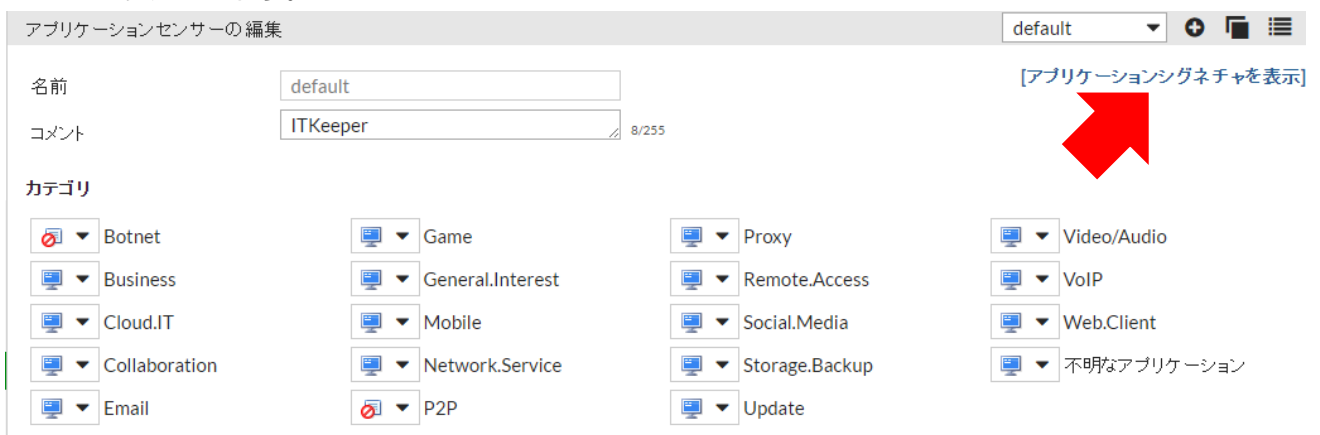
4-⑩ アプリケーションのカテゴリを調べたい

特定アプリケーションのカテゴリを調べる場合には以下を参考に実施します。

- [P3「3-① FortiGate ダッシュボード（機器管理画面）へのログイン」](#)を参考に FortiGate の機器管理画面にログインします。
- 機器管理画面にログイン後、左側ペインにて「セキュリティプロファイル」にカーソルを合わせ、左クリックすると「セキュリティプロファイル」メニューが展開されるので、「アプリケーションコントロール」にカーソルを合わせて左クリックします。

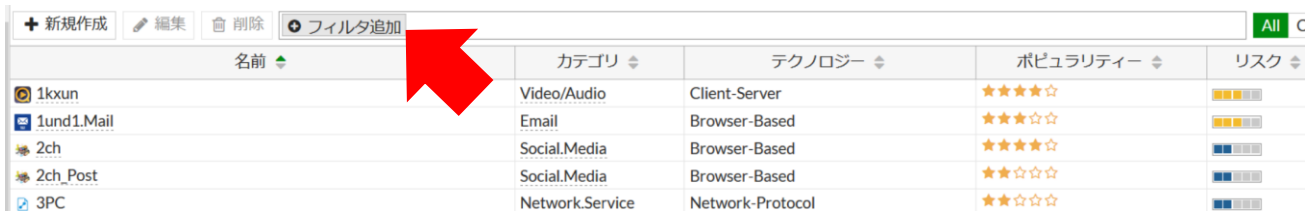


- 右側ペインにて画面右部にある「アプリケーションシグネチャを表示」にカーソルを合わせて左クリックします。



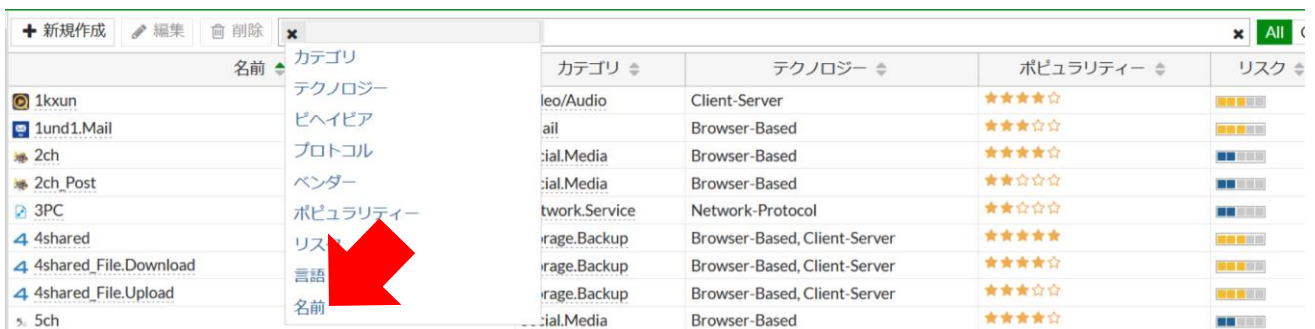
RICOH

- アプリケーションの一覧が表示されるので、「フィルタ追加」にカーソルを合わせて左クリックします。



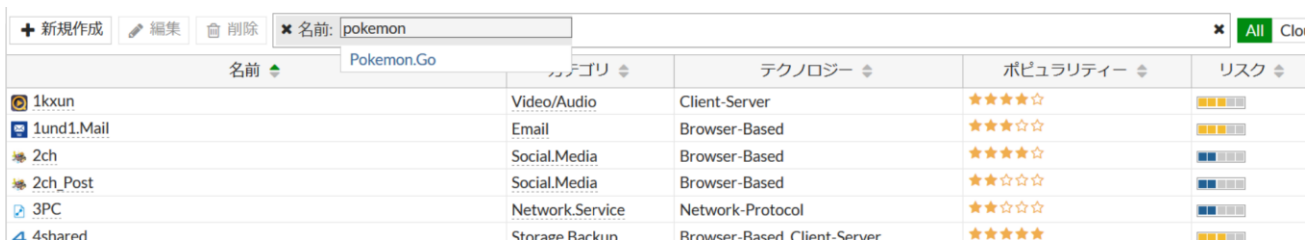
名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■■
2ch	Social.Media	Browser-Based	★★★★☆	■■■■■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■■
3PC	Network.Service	Network-Protocol	★★★★☆	■■■■■

- どの検索フィルタにてアプリケーションを検索するか選ぶことができるので、ここでは「名前」を例にカーソルを合わせて左クリックします。



名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
1kxun	Video/Audio	Client-Server	★★★★☆	■■■■■
1und1.Mail	Email	Browser-Based	★★★★☆	■■■■■
2ch	Social.Media	Browser-Based	★★★★☆	■■■■■
2ch_Post	Social.Media	Browser-Based	★★★★☆	■■■■■
3PC	Network.Service	Network-Protocol	★★★★☆	■■■■■
4shared	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
4shared_File.Download	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
4shared_File.Upload	Storage.Backup	Browser-Based, Client-Server	★★★★☆	■■■■■
5ch	Social.Media	Browser-Based	★★★★☆	■■■■■

- 検索ボックスに検索するアプリケーション名を入力後、Enter キーを押下します。



名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
Pokemon.Go	Game	Client-Server	★★★★☆	■■■■■

- 以下のようにアプリケーションの Fortinet 社での評価が表示されます。
カテゴリの項目に「Game」とあるので「Game」のカテゴリであることが確認できます。



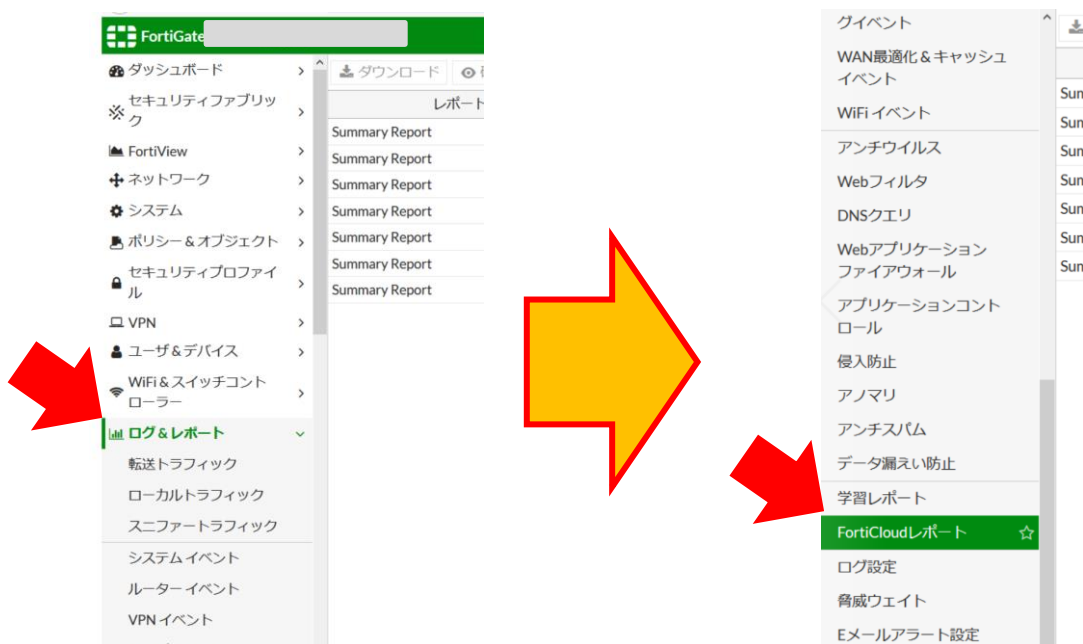
名前	カテゴリ	テクノロジー	ポピュラリティー	リスク
Pokemon.Go	Game	Client-Server	★★★★☆	■■■■■

5 FortiGate 上で FortiCloud レポートを参照する方法

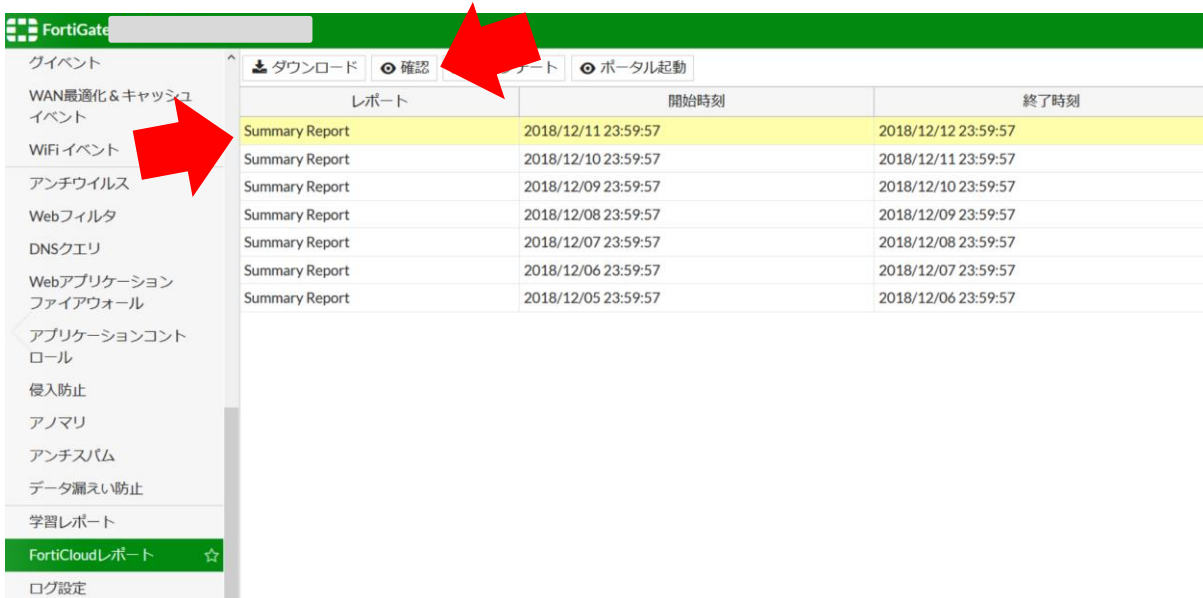
FortiGate から FortiCloud レポートを参照する方法を説明します。

5-① FortiGate 上で FortiCloud レポートを参照する場合

- 機器管理画面にログイン後、左側ペインにて「ログ&レポート」にカーソルを合わせ、左クリックすると「ログ&レポート」メニューが展開されるので、「FortiCloud レポート」にカーソルを合わせて左クリックします。



- 表示されたレポート一覧から参照したいレポートを左クリックで選択し、「確認」を左クリックします。例：Summary Report（デフォルトの daily レポート）



- レポートが表示されますので参照ください。

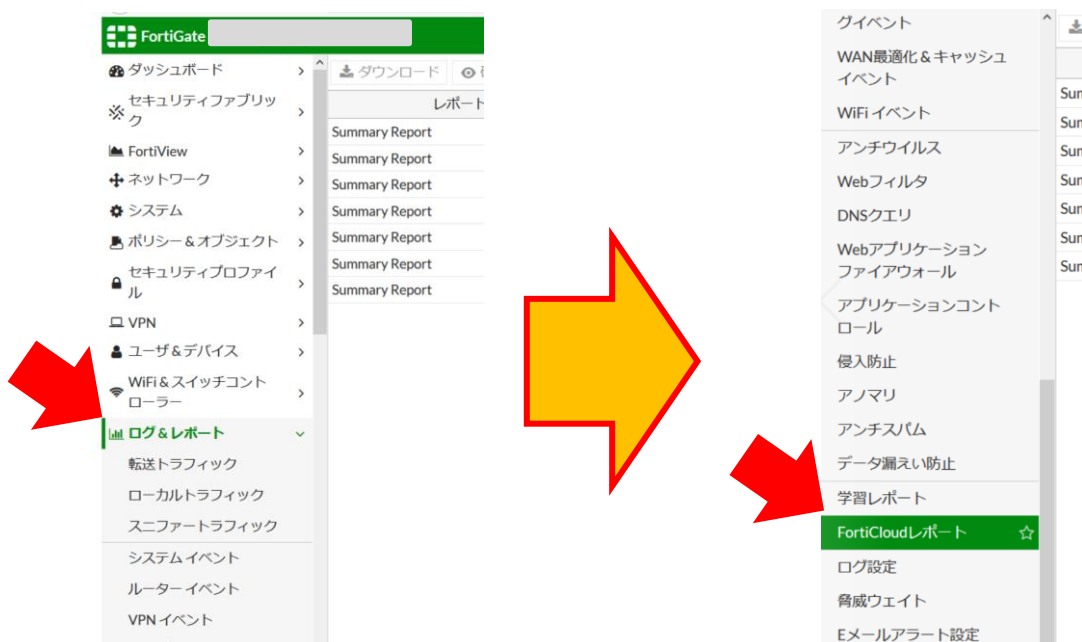
デバイス: FG
2018-12-12 13:50 - 2018-12-13 13:50

Summary Report

Threat Analysis				
Top Threats				
Threat	Category	Level	Score	%
tg.socdm.com		High	210	16.7%
s.eximg.jp		High	180	14.3%
cr-p3.ladsp.jp		High	150	12.0%
sync.im-apps.net		High	120	9.6%
wfurltest.fortiguard.com		High	60	4.8%
wfurltest.fortiguard.com		High	60	4.8%
EICAR_TEST_FILE		Critical	50	4.0%
EICAR_TEST_FILE		Critical	50	4.0%
wfurltest.fortiguard.com		High	40	3.2%
wfurltest.fortiguard.com		High	40	3.2%
rt.gsspat.jp		High	30	2.4%
match.basebanner.com		High	30	2.4%
2016.eicar.org		High	30	2.4%
cr-p10.ladsp.jp		High	30	2.4%
jp.cinarra.com		High	30	2.4%
ws2.rqtrk.eu		High	30	2.4%
prod.bidr.io		High	30	2.4%
wfurltest.fortiguard.com		High	30	2.4%

5-② FortiGate 上で FortiCloud レポートをダウンロードする場合

- 機器管理画面にログイン後、左側ペインにて「ログ&レポート」にカーソルを合わせ、左クリックすると「ログ&レポート」メニューが展開されるので、「FortiCloud レポート」にカーソルを合わせて左クリックします。



RICOH

- 表示されたレポート一覧から参照したいレポートを左クリックで選択し、「ダウンロード」を左クリック後に画面の指示に従ってダウンロードします。

例：Summary Report（デフォルトの daily レポート）

The screenshot shows the FortiGate management console. On the left is a navigation menu with categories like 'WAN最適化 & キャッシュイベント', 'WiFi イベント', 'アンチウイルス', etc. The main area displays a table of reports:

レポート	開始時刻	終了時刻	スケジュール
Summary Report	2018/12/11 23:59:57	2018/12/12 23:59:57	毎日
Summary Report	2018/12/10 23:59:57	2018/12/11 23:59:57	毎日
Summary Report	2018/12/09 23:59:57	2018/12/10 23:59:57	毎日
Summary Report	2018/12/08 23:59:57	2018/12/09 23:59:57	毎日
Summary Report	2018/12/07 23:59:57	2018/12/08 23:59:57	毎日
Summary Report	2018/12/06 23:59:57	2018/12/07 23:59:57	毎日
Summary Report	2018/12/05 23:59:57	2018/12/06 23:59:57	毎日

Below the table, a dialog box titled 'FortiCloudReport9.pdf を開く' is shown. It contains the following information:

- 次のファイルを開こうとしています:
- FortiCloudReport9.pdf
- ファイルの種類: PDF ファイル (36.1 KB)
- ファイルの場所: https://192.168.250.7
- このファイルをどのように処理するか選んでください
- プログラムで開く(O): TWINUI (既定)
- ファイルを保存する(S)
- 今後この種類のファイルは同様に処理する(A)
- Buttons: OK, キャンセル

- ダウンロードしたレポートを参照ください。
※レポート表示形式は FortiCloud のバージョン（バージョン Up は Fortinet 社で実施）によって変更される可能性がありますので、ご了承ください。

<Threat Analysis（攻撃の分析）>

Top Threats				
Threat	Category	Level	Score	%
Failed Connection Attempt	Firewall Control	Low	5035	70.6%
clients1.google.com	Search Engines and Portals	High	630	8.8%
219.96.76.18	Unrated	High	360	5.0%
Blocked Connection Attempts	Firewall Control	High	180	2.5%
google.co.jp	Search Engines and Portals	High	120	1.7%
apis.google.com	Search Engines and Portals	High	90	1.3%
yahoo.co.jp	Search Engines and Portals	High	90	1.3%
wfbs-svc-nabu-aal.trendmicro.com	Information Technology	High	90	1.3%
fortiguard.com	Information Technology	High	60	0.8%
www.abcd.com	Malicious Websites	High	60	0.8%
metric.gstatic.com	Search Engines and Portals	High	60	0.8%
HTTP.URI.SQL.Injection	Attack	High	60	0.8%
Blocked Connection Attempts	Firewall Control	High	60	0.8%
virus_test	Malware	Critical	50	0.7%
Unscanned or uncertain	Malware	Critical	50	0.7%
tcp_syn_flood	Anomaly	Critical	50	0.7%
www.xyz.com	Information Technology	High	30	0.4%
NetworkActiv.Web.Server.XSS	Attack	High	30	0.4%
bittorrent	p2p	Low	5	0.1%
			トータル:	7130

↑ 検知したマルウェア（Malware）・攻撃（Attack）

Top Viruses		
Virus	Incidents	%
virus_test	1	100.0%
		トータル: 1

↑FortiGateで検知したマルウェア

Top Virus Victims		
Source	Incidents	%
1.1.1.1-user	1	100.0%
		トータル: 1

↑マルウェアの標的にされた端末

Top Attacks		
Attack ID	Incidents	%
HTTP.URI.SQL.Injection	2	40.0%
NetworkActiv.Web.Server.XSS	2	40.0%
	1	20.0%
		トータル: 5

↑IPSで検知した攻撃

Top Attack Victims		
Destination	Incidents	%
172.25.9.212	4	80.0%
2.2.2.2-user	1	20.0%
		トータル: 5

↑IPSで検知した攻撃の標的にされた端末

Top Spam by Source IP		
Source	Incidents	%
1.1.1.1-user	2	100.0%
		トータル: 2

↑スパムを検知した通信の送信元（端末）

※Threat Analysis のデータを取得する為には、以下の条件が必要です。

- アンチウイルス、IPS、アンチスパムにてログを取得できるアクション（ブロック、モニタ等）であること。
- ポリシーでセキュリティログまたはすべてのセッションのログを許可すること。

※基本的には Source（送信元）となるのはセッションを開始した端末（多くの場合、社内の端末）となります。

Threat Analysis (Viruses)

参考までですが、以下のようなポイントを確認することができます。

- マルウェアが検知されたか。
悪意のあるファイルのダウンロードやボットネットの検出があった場合に記録されます。
マルウェアのダウンロードの場合、FortiGateの導入によりセキュリティを高めることができます。
ボットネットの検出があった場合、既に感染している可能性があります。
FortiGateでは悪意のあるファイルのダウンロードやボットネット通信をブロックすることができます。

マルウェアの詳細は下記を参照してください。

- <http://fortiguard.com/encyclopedia>
- 例) Virus: JS/FakejQuery.16Fltr (<http://fortiguard.com/encyclopedia/virus/7176618>)
(意識)
該当のウイルスはユーザに隠れ下記の動作を行います。
リモートアクセスの確立、キーボードの入力キャプチャ、ファイルのダウンロード/アップロード、他のマルウェアのダウンロード、(クライアントを踏み台にした)Dos攻撃、クライアントのプロセスの終了。

Threat Analysis (Attack, Spam)

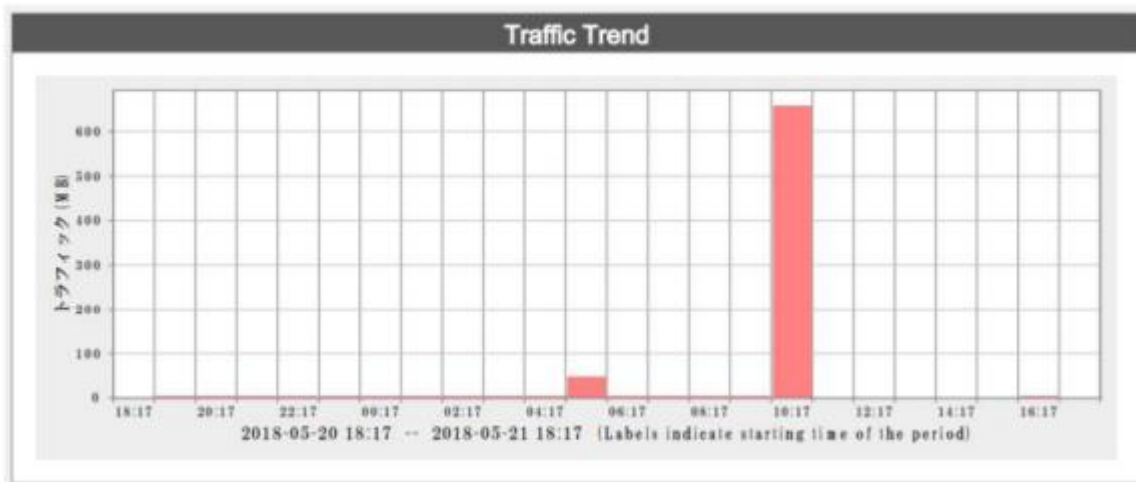
参考までですが、以下のようなポイントを確認することができます。

- IPSによる攻撃が検知されたか。
外部からの攻撃が発生していた場合に記録されます。
サーバをDMZで公開している場合には、攻撃を受けている可能性があります。
FortiGateのIPSによってこれらの攻撃を防ぎます。
- スパムメールを受信していないか。
メールは標的型攻撃の初期潜入やランサムウェアの配布等で使用されます。
スパムメールが記録されている場合、これらの攻撃の標的となっている可能性があります。

攻撃の詳細は下記を参照してください。

- <http://fortiguard.com/encyclopedia>

<Traffic Analysis (通信の分析)>

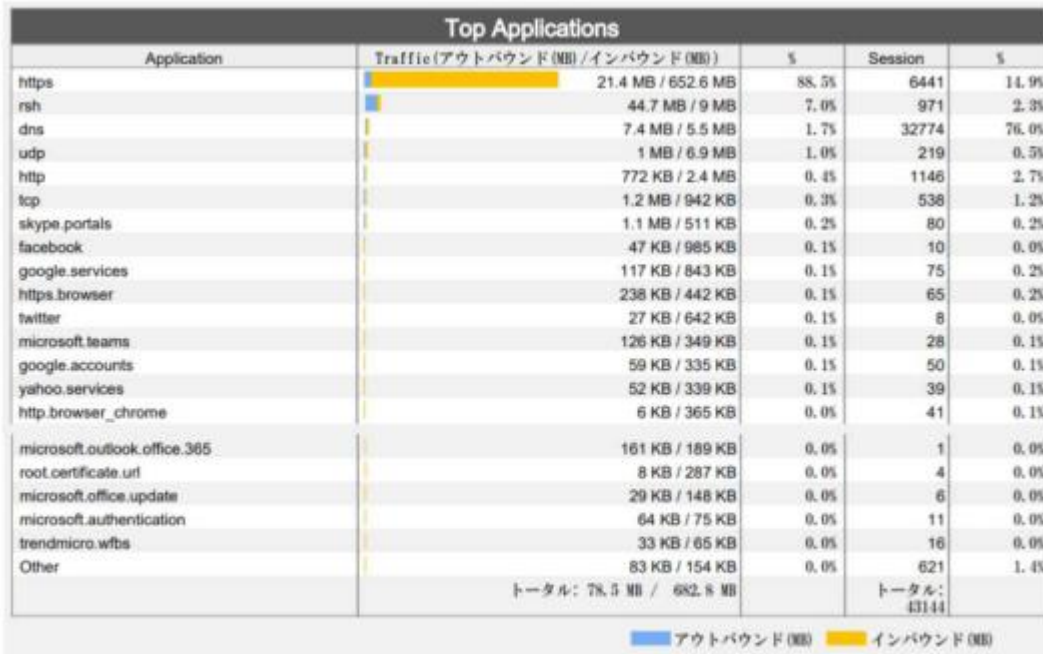


↑回線の時間当たりの利用量

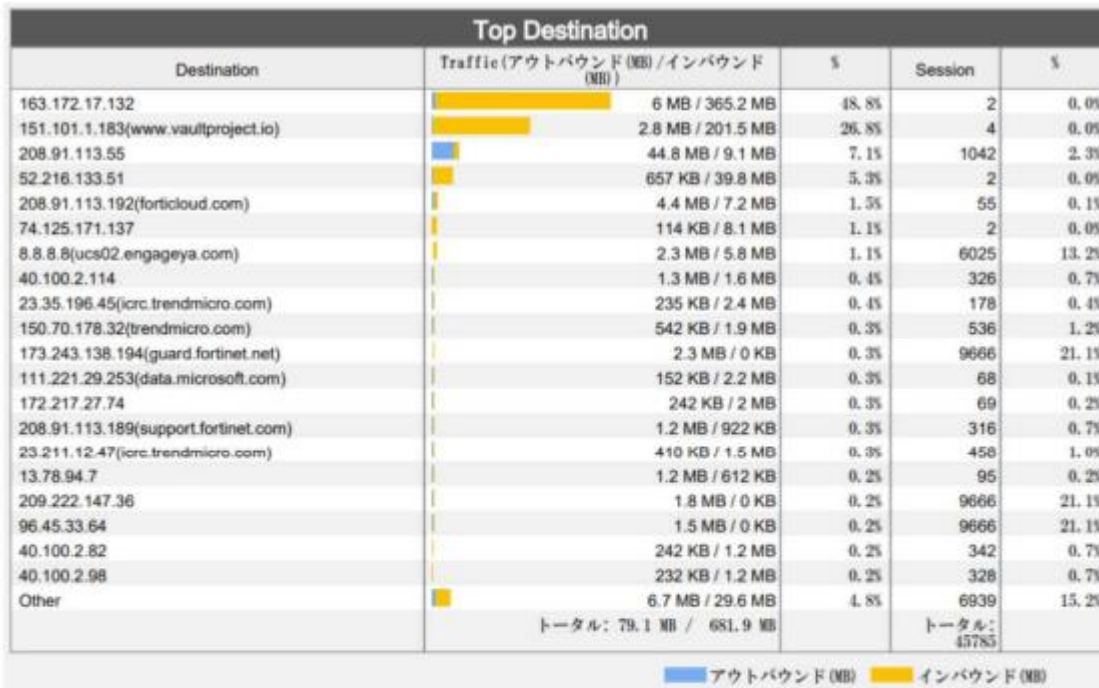
Top Source					
Source	Traffic(アウトバウンド(MB)/インバウンド(MB))	%	Session	%	
192.168.1.1	22.4 MB / 656.2 MB	89.1%	11593	26.9%	
192.168.1.99	53.1 MB / 15.3 MB	9.0%	29016	67.3%	
192.168.1.110	937 KB / 5.7 MB	0.9%	1503	3.5%	
192.168.1.2	1.9 MB / 2.7 MB	0.6%	602	1.4%	
192.168.1.210	231 KB / 2.9 MB	0.4%	399	0.9%	
1.1.1.1	21 KB / 10 KB	0.0%	11	0.0%	
10.1.1.1	3 KB / 1 KB	0.0%	2	0.0%	
9.1.1.1	3 KB / 1 KB	0.0%	2	0.0%	
172.16.78.32-test user	1 KB / 2 KB	0.0%	6	0.0%	
4.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
7.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
2.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
5.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
8.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
3.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
6.1.1.1	1 KB / 0 KB	0.0%	1	0.0%	
101:101:0:0:0:0:0	1 KB / 0 KB	0.0%	1	0.0%	
172.16.78.88-test user	0 KB / 1 KB	0.0%	2	0.0%	
トータル: 78.6 MB / 682.8 MB			トータル:	43144	

■ アウトバウンド (MB) ■ インバウンド (MB)

↑データ使用量の多い端末とそのセッション数



↑データ使用量の多いアプリケーションとそのセッション数



↑データ使用量の多い通信の宛先とそのセッション数

- ※ Traffic Analysisのデータを取得する為には、以下の条件が必要です。
- ・アプリケーションコントロールにてログを取得できるアクション（ブロック、モニタ等）であること。
 - ・ポリシーで全てのセッションのログを許可すること。

<参考情報>

Traffic Analysis

参考までですが、以下のようなポイントを確認することができます。

- P2Pやファイル共有アプリケーションを使用していないか。
使用していた場合、許可されていない不正なデータ通信が発生している可能性があります。
FortiGateではこのようなアプリケーションを禁止することができます。
- 帯域を消費するアプリケーションを使用していないか。
使用していた場合、他のアプリケーションを圧迫している可能性があります。
必要に応じてFortiGateでこのようなアプリケーションを禁止することができます。

FortiGateで制御できるアプリケーションは下記を参照してください。

- <http://fortiguard.com/appcontrol>

<Web Activities (Web サイトの利用状況) >

Most Visited Websites					
Web Site	Visits	%	Estimated Browsing Time	%	
clients1.google.com	21	36.8%	00h 02m 43s	52.6%	
219.96.76.18	12	21.1%	00h 01m 42s	32.9%	
google.co.jp	4	7.0%	00h 00m 00s	0.0%	
apis.google.com	3	5.3%	00h 00m 00s	0.0%	
wfbs-svc-nabu-aal.trendmicro.com	3	5.3%	00h 00m 40s	12.9%	
yahoo.co.jp	3	5.3%	00h 00m 05s	1.6%	
fortiguard.com	2	3.5%	00h 00m 00s	0.0%	
metric.gstatic.com	2	3.5%	00h 00m 00s	0.0%	
mki.co.jp	1	1.8%	00h 00m 00s	0.0%	
ssl.gstatic.com	1	1.8%	00h 00m 00s	0.0%	
www.abcd.com	1	1.8%	00h 00m 00s	0.0%	
www.googleapis.com	1	1.8%	00h 00m 00s	0.0%	
www.xyz.com	1	1.8%	00h 00m 00s	0.0%	
safebrowsing.googleapis.com	1	1.8%	00h 00m 00s	0.0%	
update.googleapis.com	1	1.8%	00h 00m 00s	0.0%	
	トータル: 57		トータル: 00h 05m 10s		

↑ 接続されたWEBサイト

Most Visited Web Sites by Most Active Users				
User	%	Web Site	%	訪問
	96.5%	clients1.google.com	38.2%	21
		219.96.76.18	21.8%	12
		google.co.jp	7.3%	4
		apis.google.com	5.5%	3
user	3.5%	wfbs-svc-nabu-aal.trendmicro.com	5.5%	3
		Other	21.8%	12
		www.abcd.com	50.0%	1
		www.xyz.com	50.0%	1
			トータル: 57	

■ 訪問

↑ ユーザごとのWEB利用時間と訪問先WEBサイトの内訳

Threat Analysis

Top Threats				
Threat	Category	Level	Score	%
Failed Connection Attempt	Firewall Control	Low	5035	70.6%
clients1.google.com	Search Engines and Portals	High	630	8.8%
219.96.76.18	Unrated	High	360	5.0%
Blocked Connection Attempts	Firewall Control	High	180	2.5%
google.co.jp	Search Engines and Portals	High	120	1.7%
apis.google.com	Search Engines and Portals	High	90	1.3%
yahoo.co.jp	Search Engines and Portals	High	90	1.3%
wfbs-svc-nabu-aal.trendmicro.com	Information Technology	High	90	1.3%
fortiguard.com	Information Technology	High	60	0.8%
www.abcd.com	Malicious Websites	High	60	0.8%
metric.gstatic.com	Search Engines and Portals	High	60	0.8%
HTTP.URI.SQL.Injection	Attack	High	60	0.8%
Blocked Connection Attempts	Firewall Control	High	60	0.8%
virus_test	Malware	Critical	50	0.7%
Unscanned or uncertain	Malware	Critical	50	0.7%
tcp_syn_flood	Anomaly	Critical	50	0.7%
www.xyz.com	Information Technology	High	30	0.4%
	Attack	High	30	0.4%
NetworkActiv.Web.Server.XSS	Attack	Medium	20	0.3%
bittorrent	p2p	Low	5	0.1%
			トータル:	7130

↑ブロックしたWEBサイトとそのカテゴリ

- ※ Web Activitiesのデータを取得する為には、以下の条件が必要です。
 - ・ Webフィルタにてログを取得できるアクション（ブロック、モニタ等）であること。
 - ・ ポリシーでセキュリティログまたは全てのセッションのログを許可すること。
- ※ ブロックしたWebサイトはTreat AnalysisのTop Threatsに表示されます。

Web Activities

参考までですが、以下のようなポイントを確認することができます。

- 危険なWEBサイトや禁止されたWEBサイトへのアクセスが発生していないか。
「Malicious Websites」、「Phishing」、「Spam URLs」へのアクセスや、業務と無関係なWEBサイトへのアクセスが発生していた場合、セキュリティ上のリスクが発生します。

各WEBサイトがFortiGateでどのカテゴリに分類されたかは下記を参照してください。

- <http://fortiguard.com/webfilter>

6 FortiGate 上でログを参照する方法

FortiGate からログを参照する方法を説明します。

6-① FortiGate 上で FortiView のログを参照する場合

機器管理画面にログイン後、左側ペインにて「FortiView」にカーソルを合わせ、左クリックすると「FortiView」メニューが展開されるので、確認したい項目「(例) アプリケーション」にカーソルを合わせて左クリックします。※該当ログを選択して、ダブルクリックすることで詳細情報が確認できます。

(例) アプリケーション



6-② FortiGate 上でログ&レポートのログを参照する場合

機器管理画面にログイン後、左側ペインにて「ログ&レポート」にカーソルを合わせ、左クリックすると「ログ&レポート」メニューが展開されるので、確認したい項目「(例) ローカルトラフィック」にカーソルを合わせて左クリックします。※該当ログを選択して、ダブルクリックすることで詳細情報が確認できます。

(例) ローカルトラフィック

#	日/時	送信元	デバイス	宛先	アプリケーション名	送信 / 受信
1	秒前				Web Management(HTTPS)	20.41 kB / 105.50 kB
2	秒前				Web Management(HTTPS)	725 B / 313 B
3	秒前				Web Management(HTTPS)	24.29 kB / 39.59 kB
4	秒前				Web Management(HTTPS)	24.70 kB / 33.80 kB
5	秒前				Web Management(HTTPS)	725 B / 313 B
6	秒前				Web Management(HTTPS)	725 B / 313 B
7	秒前				Web Management(HTTPS)	729 B / 393 B
8	秒前				Web Management(HTTPS)	689 B / 353 B
9	秒前	100.107.100.107		200.17.0.220	Web Management(HTTPS)	3.00 kB / 2.62 kB

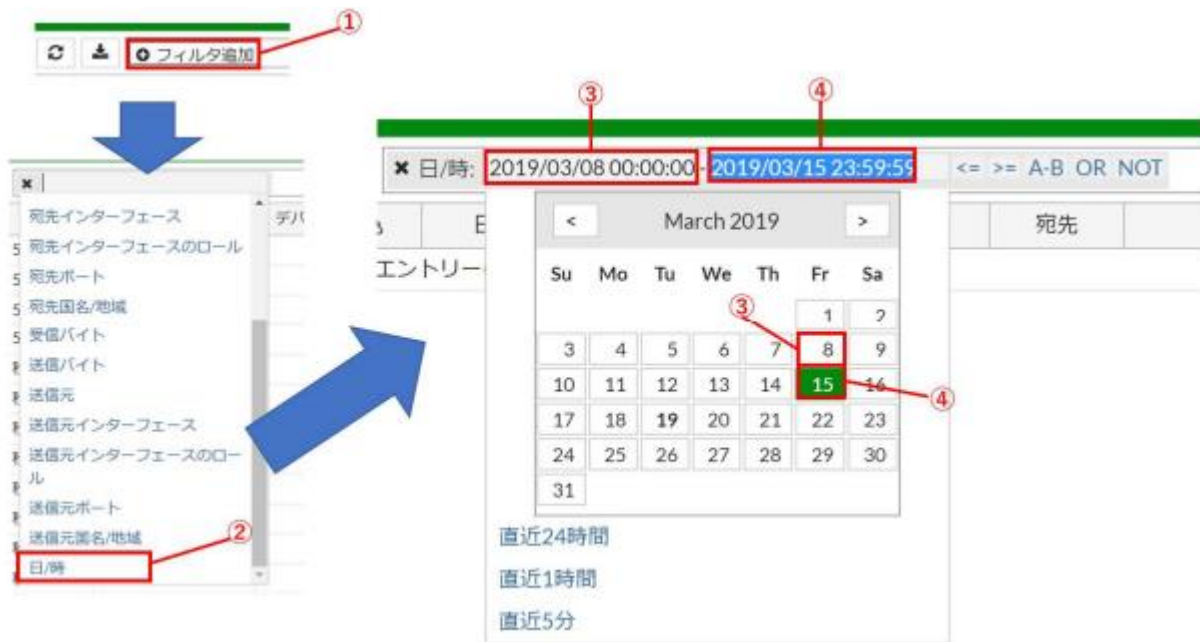
RICOH

<補足>

尚、ログは「フィルタ追加」(赤枠箇所) から日時を設定することで確認したい日時分のログを確認することが可能です。

①「フィルタ追加」を左クリックし、リストから②「日/時」を選択し、開始日時を③カレンダー日付選択、もしくは手動入力で指定し、終了日時を同様に④カレンダー日付選択、もしくは手動入力で指定することで指定した間の日時分のログが確認できます。

注：終了日時はカーソルで選択した状態でカレンダー日付選択しないと開始日時も変更になってしまいます。



RICOH

Fortinet®, FortiGate®, FortiCare®, FortiCloud、および FortiGuard® は Fortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です

Google および Google Chrome™ ブラウザは Google Inc.の商標です。

Mac OS は、米国および他の国々で登録された Apple Inc.の商標です。

Firefox、Thunderbird は Mozilla Foundation の商標です。

Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Microsoft、Windows、Windows 10、Internet Explorer、Windows Live、Excel および Outlook Express は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。
その他の製品名、名称は各社の商標または登録商標です。