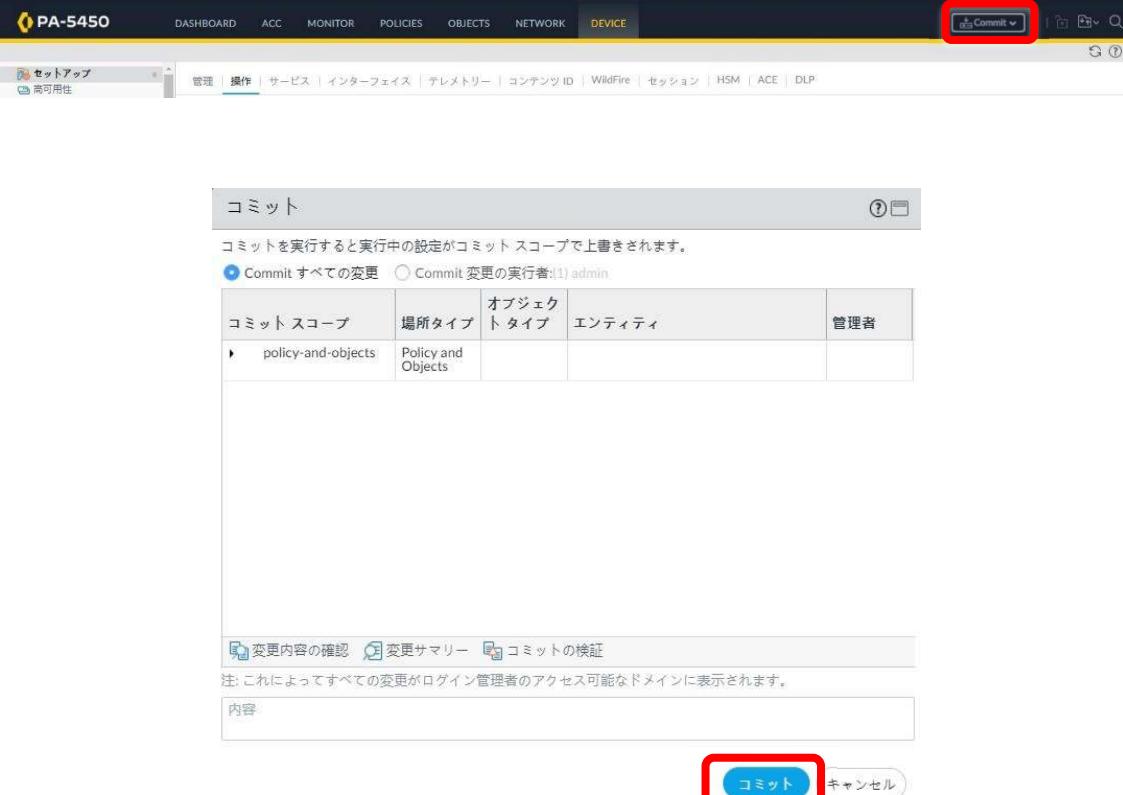


ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ④ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
 (設定が反映されるまで5分程度かかることがあります)



The screenshot shows the PA-5450 device management interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE. The DEVICE tab is selected. A red box highlights the 'Commit' button in the top right corner of the header.

The main content area is titled 'コミット' (Commit). It displays a table with one row of data:

コミット スコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

Below the table, there are three buttons: '変更内容の確認' (Review Change Content), '変更サマリー' (Change Summary), and 'コミットの検証' (Commit Verification). A note states: '注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。' (Note: This will display all changes in the domain accessible to the logged-in administrator.)

A large text input field labeled '内容' (Content) is present. At the bottom right, there are two buttons: a blue 'コミット' (Commit) button with a red box around it, and a 'キャンセル' (Cancel) button.

図 6－4－2 3 PA-5450 Security NAT Policies Add and Change

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

#### 6. 4. 3. グループ会社参照プロキシサーバの変更方法

G会社が参照しているプロキシを広島DCから吹田DC(旧電算室)のサーバに変更する手順を記載します。△△接続用ファイアウォールでNAT設定を行い、参照先のプロキシサーバを切り替えることが可能です。NAT後の実IPアドレスを広島から吹田に変更することで参照先が切り替わります。

※プロキシサーバにて障害が発生した場合など、NAT設定を変更することで切り替えることができます。

##### ① 「Objects」タブ > 「NAT」

名前	タグ	元のパケット					変換済みパケット	
		送信元ソース	宛先ソース	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換
1 test	none	Internal_W...	Internal_SV...	any	any	any	dynamic-ip-and-port	なし
2 test1	none	any	Internal_SV...	any	any	any	none	なし
3 SHD_G-Trust_SHD_G...	none	SHD_G-Trust	SHD_G-Un...	any	172.21.193...	any	static-ip 10.86.64.0_24 双方向: yes	なし
4 WEST_WEST_WEST_...	none	WEST_WE...	WEST_G-U...	any	10.19.36.1/32	any	static-ip 10.192.2.12/32 双方向: yes	なし
5 Proxy_NAT_Rule	none	WEST_WE...	WEST_G-U...	any	10.96.64.27/...	any	static-ip 10.192.2.202/32 双方向: yes	なし

図 6-4-24 PA-5450 Security NAT Policies Change

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② プロキシサーバの NAT ポリシーを選択します。

※プロキシサーバ用の NAT ポリシーは、NAT ポリシー名「Proxy\_NAT\_Rule」、

送信元変換「10.192.2.202」にて設定されています。

名前	タグ	元のパケット					変換済みパケット	
		送信元ゾーン	宛先ゾーン	宛先インターフェイス	送信元アドレス	宛先アドレス	サービス	送信元変換
test	none	Internal_W...	Internal_SV...	any	any	any	dynamic-ip-and-port	なし
test1	none	any	Internal_SV...	any	any	any	none	なし
SHD_G-Trust_SHD_G...	none	SHD_G-Trust	SHD_G-Untr...	any	172.21.193...	any	static-ip 10.86.64.0_24 双方向:yes	なし
WEST_WEST_WEST...	none	WEST_WE...	WEST_G-U...	any	10.19.36.1/32	any	static-ip 10.192.2.12/32 双方向:yes	なし
Proxy_NAT_Rule	none	WEST_WE...	WEST_G-U...	any	10.19.132.27/32	any	static-ip 10.192.2.202/32 双方向:yes	なし

図 6-4-25 PA-5450 Security NAT Policies Change

③ 送信元アドレスを直接編集し、アドレスを吹田 DC(旧電算室)（10.19.132.27）に変更します。

図 6-4-26 PA-5450 Security NAT Policies Change

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ④ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
 (設定が反映されるまで5分程度かかることがあります)

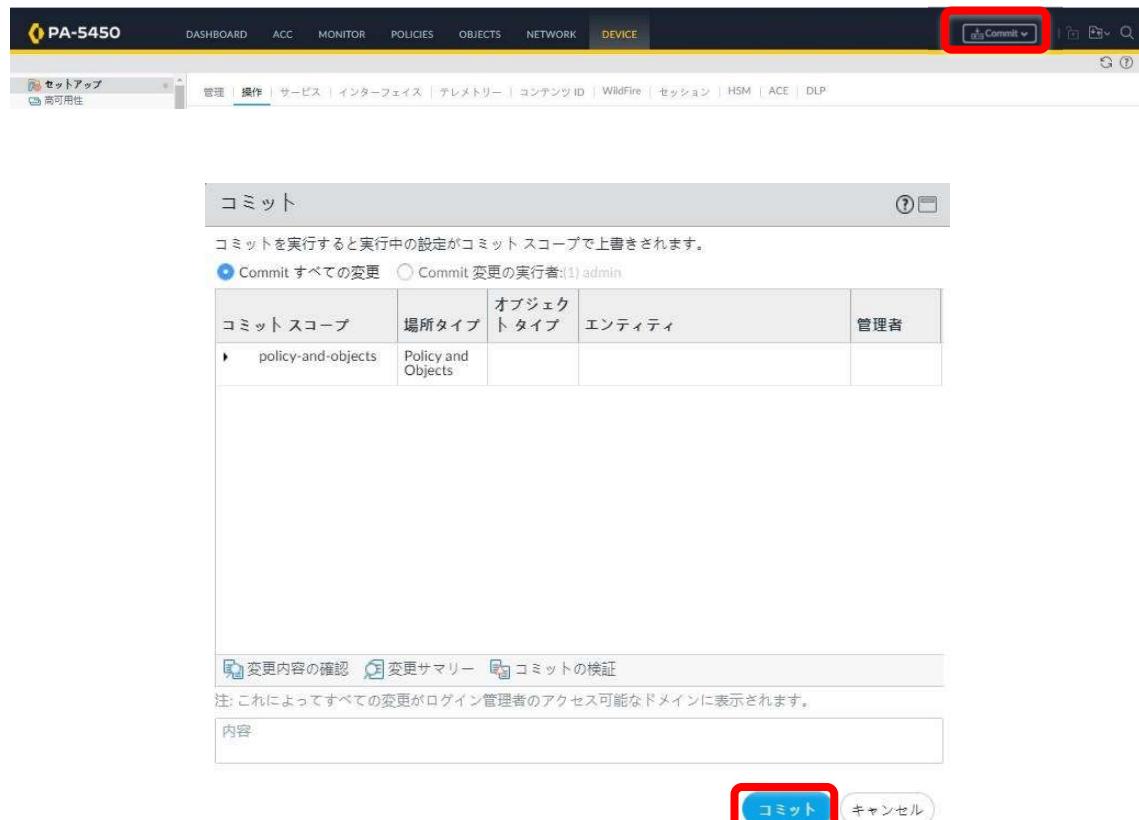


図 6-4-27 PA-5450 Security NAT Policies Change

コミットによる設定完了後、「1.7. 2. ログ閲覧/検索」の手順を参照し、トラフィックログからグループ会社のプロキシ通信が吹田 DC(旧電算室)を使用している事を確認します。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. URL フィルタリングポリシー修正/追加/削除

---

この項では、URL フィルタリングにおけるログの確認方法及び確認結果からパターン毎に URL フィルタリングを設定、適用する方法を記載しています。

記載されている URL プロファイル名は、適宜現在のものと置き換えてください。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメントID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 1. URL フィルタリングログ確認方法

① 通信不具合に関するユーザからの申告に基づき、以下の内容をヒアリングします。

- ・ 送信元 IP アドレス
- ・ アクセス先 URL
- ・ アクセスを試みたときの時刻

② 送信元 IP アドレス、アクセス先の URL 情報から該当通信のログをフィルタします。

表 7-1-1、表 7-1-2 のカラムを使用して、「ログビュー」にフィルタを記載します。複数のカラムを組み合わせる場合は、「and」で条件を接続します。

表 7-1-1 ログフィルタ

パターン	列	対象(例)	フィルタ
(1)	送信元	192.168.2.10	(addr.src in 192.168.2.10)
(2)	宛先	192.168.3.100	(addr.dst in 192.168.3.100)
(3)	URL	www.yahoo.co.jp www.yahoo.co.jp:443	<ul style="list-style-type: none"> <li>・ 対象 URL と一致する。 (url eq 'www.yahoo.co.jp/')</li> <li>(url eq 'www.yahoo.co.jp:443/')</li> <li>・ 対象 URL を含む。 (url contains 'www.yahoo.co.jp/')</li> <li>(url contains 'www.yahoo.co.jp:443/')</li> </ul>
(4)	受信日時	2017/12/01 12:00:00 ~ ~ 2017/12/01 13:00:00	(receive_time geq '2017/12/01 12:00:00') (receive_time leq '2017/12/01 13:00:00')
(5)	アクション	block-url	(action eq block-url)

表 7-1-2 ログフィルタ(複数組み合わせ)

パターン	Columns	対象(例)	フィルタ
(6)	送信元および 宛先	送信元:192.168.2.10 宛先 :192.168.3.100	(addr.src in 192.168.2.10) and (addr.dst in 192.168.3.100)
(7)	送信元および URL	送信元:192.168.2.10 URL: www.yahoo.co.jp	(addr.src in 192.168.2.10) and (url eq 'www.yahoo.co.jp/')
(8)	宛先および URL	宛先 : 192.168.3.100 URL:www.yahoo.co.jp:443	(addr.src in 192.168.3.100) and (url eq 'www.yahoo.co.jp:443/')
(9)	受信日時	受 信 日 時 : 2017/12/01 12:00:00 ~ 2017/12/01 13:00:00	(receive_time geq '2017/12/01 12:00:00') and (receive_time leq '2017/12/01 13:00:00')
(10)	アクション	送 信 元 :192.168.2.10 Action: block-url	(addr.src in 192.168.2.10) and (action eq block-url)

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 「Monitor」タブ > 「URL フィルタリング」>を選択し、ログフィルタ枠にフィルタ条件を入力します。

図 7-1-1 URL フィルタログ確認

- ④ 確認した結果、「Action」が「block-url」もしくは「alert」により、表 7-1-3 よりマッチするパターンを確認します。

- ⑤ 表 7-1-3 より、該当する変更対象 URL プロファイルもしくはカスタムカテゴリを選択します。

表 7-1-3 パターン別変更対象 URL プロファイル・カスタムカテゴリ

理由	対象	対象 URL プロファイル/カスタムカテゴリ
既存カテゴリ (social-networking など) でブロックされ ている、もしくは許可 されている。	(1) 全社(本体、G会社)アクセス解除	DefaultGroup_Allow
	(2) 全社(本体、G会社)ブロック	DefaultGroup_Block
	(3) 本体アクセス解除	w-nexco_allow
	(4) 本体ブロック	w-nexco_block
	(5) 本体拠点のアクセス解除	各拠点の URL プロファイル
	(6) 本体拠点のブロック	
	(7) 全 G 会社アクセス解除	Group_Allow
	(8) 全 G 会社ブロック	Group_Block
既存カテゴリ以外 (DefaultGroup_Block などのカスタムカテゴリ)	本体、G会社に紐づく 個別 URL プロファイル	個別 URL プロファイル ※本体個人は新規に URL プロファイルを作成する場合有

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 2. URL プロファイル修正

### 7. 1. 2. 1. 全社アクセス解除/全社ブロック（CLI 含む）

表 7-1-4 全社変更対象 URL プロファイル・変更カスタムカテゴリ

対象	変更 URL プロファイル/変更カスタムカテゴリ
(1) 全社(本体、G 会社)アクセス解除	全社（本体、G 会社）でアクセス解除を行う場合、「DefaultGroup_Allow」を変更します。ただし、アクセス解除する URL が「DefaultGroup_Block」などのカスタムカテゴリでブロックされている時は、各プロファイルに設定したカテゴリを変更します。  (1)-1 DefaultGroup_Allow(カスタムカテゴリ)  (1)-2 各 URL プロファイルに追加 本体および G 会社の URL プロファイルが変更対象です。
(2) 全社(本体、G 会社)ブロック	DefaultGroup_Block(カスタムカテゴリ)

#### (1) 全社(本体、G 会社)のアクセス解除

##### (1)-1. DefaultGroup\_Allow(カスタムカテゴリ)を利用

① GUI より、DefaultGroup\_Allow(カスタムカテゴリ)に URL を登録します。

「Objects」タブ > 「URL カテゴリ」 > 「DefaultGroup\_Allow」をクリックします。

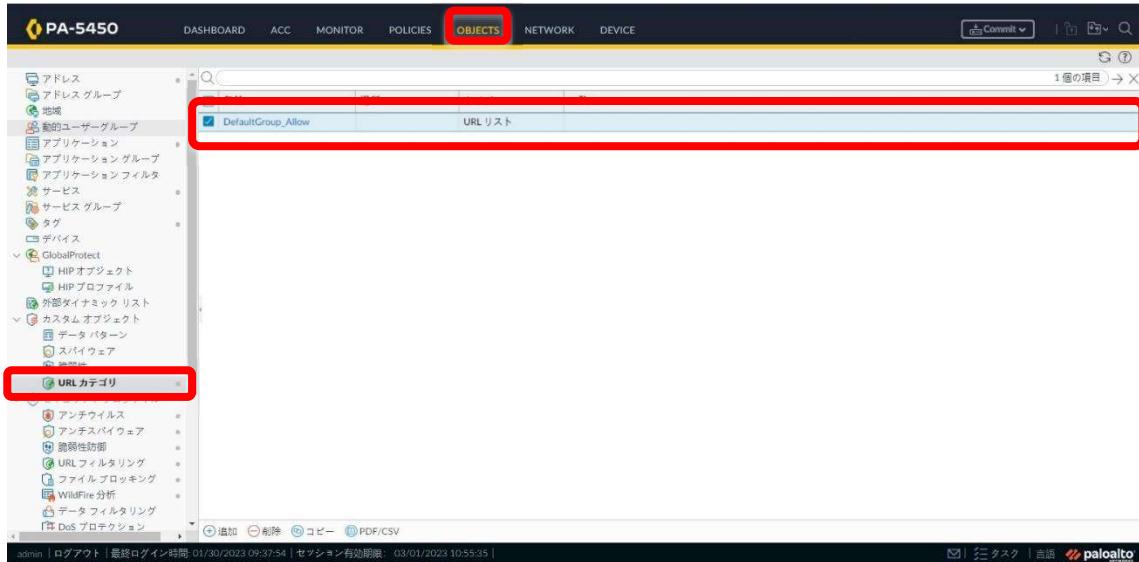


図 7-1-2 全社アクセス解除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 「追加」をクリックし、新規で登録する URL を入力します。



図 7－1－3 全社アクセス解除

③ 最下段に登録された URL を確認し、「OK」ボタンをクリックします。



図 7－1－4 全社アクセス解除

※URL の指定について、末尾のスラッシュ「/」を入力しない場合は、

ファイアウォールが自動的に追加してマッチングします。

エントリの一一致動作を明確にするため、末尾のスラッシュ「/」を手動で追加することが推奨されています。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

※URL が複数の場合には、「インポート」より予め用意しておいたテキストファイルを選択し、登録することも可能です。尚、「インポート」からの登録は登録済み URL への追加登録となり、上書きされません。テキストファイルには登録する URL を 1 行ずつ記載しておきます。

④ – 1 「インポート」をクリックします。



図 7 – 1 – 5 全社アクセス解除

③ – 2 「参照」をクリックし、ファイルを選択「OK」をクリックします。



図 7 – 1 – 6 全社アクセス解除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

「インポート」したファイルが登録されている事を確認し、「OK」をクリックします。



図 7－1－7 全社アクセス解除

- ④ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
(設定が反映されるまで 5 分程度かかることがあります)



図 7－1－8 全社アクセス解除／設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI



図 7－1－9 全社アクセス解除／設定反映

(1)－2. 各 URL プロファイルの「プロファイル名\_allow-list」（カスタムカテゴリ）URL を追加。

GUI から変更することも可能ですが、変更対象となる URL プロファイルが複数存在するため、CLI で変更する方法を記載します。

コンフィグレーションモードへ移行後、以下のコマンドを各 URL プロファイルに実施します。※モード遷移は図 3－1－5 を参照

表 7－1－5 URL プロファイルカテゴリ設定

名前	説明
name	「プロファイル名_allow-list」を入力 (例) URL_Profile_001 : 全社用プロファイル
URL	許可したい「URL」を入力

#### 構文

```
set profiles custom-url-category <name> list [ URL1 URL2 ]
```

#### 例

```
set profiles custom-url-category URL_Profile_001-allow-list list [ www.test.jp www.yahoo.jp ]
```

上記(例)のコンフィグは、Internal\_VR に設定されている URL\_Profile\_001 に許可カテゴリを追加する手順です。

※斜体は任意の文字列です。

※変更対象の URL プロファイルが複数存在し、流し込みで設定変更を実施する場合は、

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

「コピーと貼り付け」の「貼り付けの行間遅延(A)」を 350 ミリ秒にします。

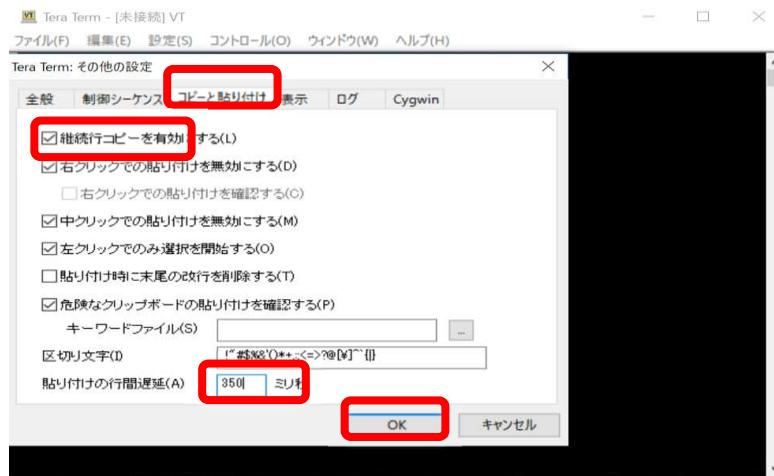


図 7-1-10 全社アクセス解除 CLI

① 設定を反映する為、「commit」を実施します。

(2) 全社(本体、G 会社)のアクセスブロック

**DefaultGroup\_Block(カスタムカテゴリ)を利用します。**

① GUI より、DefaultGroup\_Block(カスタムカテゴリ)にブロックする URL を登録します。

※以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック（1）－1」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 2. 2. 本体アクセス解除/本体ブロック (CLI 含む)

表 7-1-6 本体変更対象 URL プロファイル・変更カスタムカテゴリ

対象	変更 URL プロファイル/変更カスタムカテゴリ
(3) 本体アクセス解除	<p>本体のみのアクセス解除を行う場合、 「w-nexco_allow」を変更します。 ただし、アクセス解除する URL が 「DefaultGroup_Block」などのカスタムカテゴリでブ ロックされているときは、各プロファイルに設定した カテゴリを変更します。</p> <p>(3)-1 w-nexco_allow (カスタムカテゴリ) (3)-2 各 URL プロファイルに追加 「本体」の URL プロファイルが変更対象です。</p>
(4) 本体ブロック	w-nexco_block (カスタムカテゴリ)

### (3) 本体アクセス解除

(3)-1. w-nexco\_allow(カスタムカテゴリ)を利用します。

① GUI より、w-nexco\_allow(カスタムカテゴリ)に URL を登録します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1)-1」  
の手順と同様です。

(3)-2. 各 URL プロファイルの「プロファイル名\_allow-list」(カスタムカテゴリ)  
URL を利用します。

GUI から変更することも可能ですが、変更対象となる URL プロファイルが複数存在  
するため、CLI で変更します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1)-2」  
の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

(4) 本体ブロック

w-nexco\_block(カスタムカテゴリ)を利用します。

① GUI より、w-nexco\_block(カスタムカテゴリ)に URL を登録します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック（1）－1」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 2. 3. 本体拠点のアクセス解除/本体拠点のブロック (CLI 含む)

表 7-1-7 本体拠点の対象 URL プロファイル

対象	変更対象 URL プロファイル
(5) 本体拠点のアクセス解除 (例) 四国支社のアクセス解除を実施する場合	本体拠点のアクセス解除、ブロックを実施する場合、各拠点の URL プロファイルを変更します。
(6) 本体拠点のブロック (例) 四国支社のブロックを実施する場合	(5)、(6) 「本体各拠点」の URL プロファイルが変更対象です。

#### (5) 本体拠点のアクセス解除

各 URL プロファイルの「プロファイル名\_allow-list」（カスタムカテゴリ）URL を利用します。

GUI から変更することも可能ですが、変更対象となる URL プロファイルが複数存在するため、CLI で変更します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック（1）～2」の手順と同様です。

#### (6) 本体拠点のブロック

各 URL プロファイルの「プロファイル名\_block-list」（カスタムカテゴリ）URL を利用します。

GUI から変更することも可能ですが、変更対象となる URL プロファイルが複数存在するため、CLI で変更する方法を記載します。

- ① コンフィグレーションモードへ移行後、以下のコマンドを各 URL プロファイルに実施します。※モード遷移は図 3-1-5 を参照

表 7-1-8 URL プロファイルにカスタムカテゴリ設定

名前	説明
name	「プロファイル名_block-list」を入力 (例) URL_Profile_001：全社用プロファイル
URL	block したい「URL」を入力

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 構文

```
set profiles custom-url-category <name> list [ URL1 URL2 ]
```

### 例

```
set profiles custom-url-category URL_Profile_001_block-list list [ test.com yahoo.com ]
```

上記(例)のコンフィグは、Internal\_VR に設定されている URL\_Profile\_001  
にブロックカスタムカテゴリを追加する手順です。

※斜体は任意の文字列です。

※変更対象の URL プロファイルが複数存在し、流し込みで設定変更を実施する場合は、

「コピーと貼り付け」の「貼り付けの行間遅延(A)」を 350 ミリ秒にします。

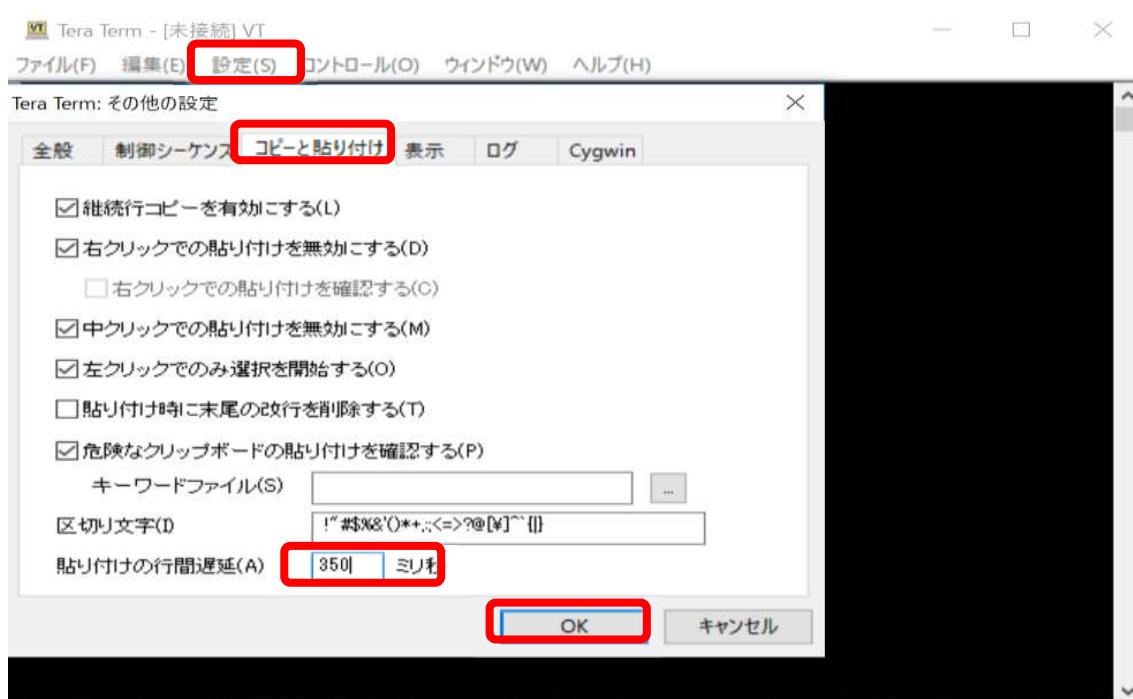


図 7－1－1 11 全社アクセスブロック CLI

② 設定を反映する為、「commit」を実施します。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

7. 1. 2. 4. 本体個人のアクセス解除/本体個人のブロック(既存 URL プロファイル有)

表 7-1-9 本体個人の対象 URL プロファイル(既存 URL プロファイル有)

対象	変更対象 URL プロファイル
(7) 本体個人のアクセス解除/本体個人のブロック 既存 URL プロファイルが存在する場合 (例) 役員用¥Allow_10.184.80.24	本体の個人向けのアクセス解除、 ブロックを行う場合、変更対象となる個人向けの URL プロファイルに対して変更を行います。  (7) 各 URL プロファイルの「プロファイル名 _allow-list/block-list」(カスタムカテゴリ) URL を追加します。 「本体個人」の URL プロファイルが 変更対象です。

- ③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
(設定が反映されるまで 5 分程度かかることがあります)



図 7-1-12 本体個人アクセス解除／設定反映

コミット

コミットを実行すると実行中の設定がコミットスコープで上書きされます。

Commit すべての変更  Commit 変更の実行者(1) admin

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

変更内容の確認 变更サマリー コミットの検証

注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容

**コミット** キャンセル

図 7-1-13 本体個人アクセス解除／設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 2. 5. 全G会社のアクセス解除/全G会社ブロック (CLI 含む)

表7-1-10 全G会社変更対象 URL プロファイル・カスタムカテゴリ

対象	変更 URL プロファイル/変更カスタムカテゴリ
(8) 全G会社のアクセス解除	<p>全G会社のアクセス解除を行う場合、Group_Allow を変更します。ただし、アクセス解除する URL が DefaultGroup_Block などのカスタムカテゴリでブロックされているときは、各プロファイルのカテゴリを変更します。</p> <p>(8)-1 Group_Allow(カスタムカテゴリ)</p> <p>(8)-2 各G会社 URL プロファイルのカテゴリに追加 各G会社の URL プロファイルが変更対象です。</p>
(9) 全G会社ブロック	Group_Block (カスタムカテゴリ)

### (8) 全G会社のアクセス解除

#### (8)-1. Group\_Allow(カスタムカテゴリ)

① GUI より、カスタムカテゴリ Group\_Allow に URL を登録します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1)-1」の手順と同様です。

#### (8)-2. 全G会社のアクセス解除

GUI から変更することも可能ですが、変更対象となる URL プロファイルが複数存在するため、CLI で変更します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1)-2」の手順と同様です。

### (9) 全G会社ブロック

① GUI より、カスタムブロック Group\_block に URL を登録します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1)-1」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 2. 6. G 会社ごとのアクセス解除/G 会社ごとのブロック (CLI 含む)

表 7-1-1-1 G 会社変更対象 URL プロファイル

対象	変更対象 URL プロファイル
(10) G 会社ごとのアクセス解除 (例)サービスホールディングスを変更する場合	G 会社ごとのアクセス解除、ブロックを行う場合、各 G 会社の URL プロファイルを変更します。
(11) G 会社ごとのアクセスブロック (例)サービスホールディングスを変更する場合	(10) 各 URL プロファイルのカテゴリに追加 URL_Profile_006 ※上記は2017年11月時点の該当プロファイルです。 (11) 各 URL プロファイルのカテゴリに追加各 G 会社の URL プロファイルが変更対象です。

(10) G 会社ごと(複数社)のアクセス解除

各 URL プロファイルのカテゴリに追加

- ① GUI より、変更対象 URL プロファイルのカテゴリに登録します。  
以降の手順は、「7. 1. 2. 4. 本体個人のアクセス解除/本体個人のブロック (7)」  
の手順と同様です。

変更対象となる G 会社が複数して CLI にて変更を実施する場合は、  
「7. 1. 2. 1. 全社アクセス解除/全社ブロック (1) - 2」の手順と同様です。

(11) G 会社ごと(複数社)のアクセスブロック

各 G 会社 URL プロファイルのカテゴリに追加

- ① GUI より、変更対象 URL プロファイルのカテゴリに登録します。  
以降の手順は、「7. 1. 2. 4. 本体個人のアクセス解除/本体個人のブロック (7)」  
の手順と同様です。

変更対象となる G 会社が複数して CLI にて変更を実施する場合は、

「7. 1. 2. 3. 本体拠点のブロック (6)」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 3. URL プロファイル追加

URL プロファイルを新規に作成する手順を記載します。

表 7-1-12 URL プロファイル設定

図中番号	タブ	名前	利用用途
(1)	-	Name	「URL プロファイル名」を入力 (※) 文字数制限は 31 字迄 また、英数字、スペース、ハイフン (「-」)、アンダースコア (「_」)、ピリオド (「.」) を名前に含めることが可能
(2)	カテゴリ	カテゴリ	URL カテゴリのリスト
(3)	URL フィルタリング設定	コンテナページのみロギング	有効 (default)
		セーフサーチを適用	無効 (default)
		ユーザーエージェント	無効 (default)
		Referer	無効 (default)
		X-Forwarded-For	無効 (default)
(4)	ユーザー証明書検出	ユーザー証明書検出	ユーザー証明書を利用しないため、「Disabled」で設定します。(default)
(5)	インライン分類	インライン分類	推奨： ローカルインライン分類を有効にする。 クラウドのインライン分類を有効にする

- ① 「Objects」タブ > 「URL フィルタリング」 > 「追加」をクリックします。



図 7-1-14 URL プロファイル追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 表 7-1-2 を参照し、各設定をします。

URL フィルタリング プロファイル

名前

内容 |

カテゴリ | URL フィルタリング設定 | ユーザー証明書検出 | HTTPヘッダー検査 | インライン分類

	サイト アクセス	ユーザー証明書送信
カテゴリ	allow	allow
カスタム URL カテゴリ	allow	allow
DefaultGroup_Allow*	allow	allow
test *	allow	allow
事前定義したカテゴリ	allow	allow
abortion	allow	allow
abused-drugs	allow	allow
adult	allow	allow

8 hex digits: 00000000 to FFFFFFFF  
URL カテゴリをチェック

OK キャンセル

図 7-1-15 URL プロファイル追加

③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。

（設定が反映されるまで 5 分程度かかることがあります）



図 7-1-16 URL プロファイル追加／設定反映

コミット

コミットを実行すると実行中の設定がコミット スコープで上書きされます。

Commit:すべての変更  Commit:変更の実行者:admin

コミット スコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

変更内容の確認 変更サマリー コミットの検証

注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容

コミット キャンセル

図 7-1-17 URL プロファイル追加／設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

一から URL プロファイルを作成する場合は、カテゴリを設定する必要があり時間を要するため、既存の URL プロファイルをコピーして作成します。コピー元になる URL プロファイルは、属性（本体、G 会社、本体拠点など）が同じになるものを選択します。

表 7－1－1－3 新規個別 URL プロファイル設定

コピー元	新規 URL プロファイル
URL_Profile_002(役員用)	端末が役員の場合
URL_Profile_029(本社)	端末が本社配下に作成する場合
URL_Profile_030(関西支社)	端末が関西支社に作成する場合
URL_Profile_031(中国支社)	端末が中国支社に作成する場合
URL_Profile_032(四国支社)	端末が四国支社に作成する場合
URL_Profile_033(九州支社)	端末が九州支社配下に作成する場合
URL_Profile_102(全制限)	カテゴリルールが全て「block」を作成する場合

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック(新規 URL プロファイル作成)

表 7-1-1-4 本体個人の対象 URL プロファイル(新規 URL プロファイル作成)

対象	変更対象 URL プロファイル
(12) 本体個人のアクセス解除/本体個人のブロック	<p>本体の個人向けのアクセス解除、ブロックを行う場合、変更対象となる個人向けの URL プロファイルに対して変更を行います。変更対象の個人向けプロファイルが存在しない場合、新規に作成します。</p> <p>(12) 各 URL プロファイルのカテゴリに追加</p>

個人向けの URL プロファイルが存在していないため、最初に URL プロファイルを新規に作成します。

作成した後に、URL プロファイルを適用したファイアウォールポリシーを作成します。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

#### 7. 1. 4. URL フィルタリングをポリシーに追加

URL フィルタ用ファイアウォールポリシーを作成する手順を記載します。

**VSYS 機能を利用しないと伴い、**

グループ会社のポリシーを追加/修正/削除する場合は、作成したポリシーの

送信元/宛先ゾーンは各グループ会社 VR に所属しているゾーンを指定します。

URL フィルタリング設定も通信一番手前の VR にあるポリシーに適用します。

詳細は本書の『0.5. VR のゾーン名一覧表』を参照してください。

※ここでは例として本社からの通信で、「Internal\_VR」に所属しているゾーン

「Internal\_WEST」から「Internal\_SV\_Critical」までのポリシーを下に作成されます。

**※作成時にポリシーを選択していた場合には選択していたポリシーの下に作成されます。**

最初にアドレス、サービスを作成後、ポリシーを追加します。

表 7-1-15 アドレス設定

図中番号	名前	利用用途
(1)	名前	「アドレス名」を入力 (※) 文字数制限は 63 字迄 また、英数字、スペース、ハイフン (「-」)、アンダースコア (「_」)、ピリオド (「.」) を名前に含めることが可能
(2)	タイプ	プルダウンから以下を選択 「IP ネットマスク」：「IP アドレス/サブネットマスク」を選択する場合 「IP 範囲」：「範囲指定アドレス」を選択する場合 「FQDN」：「FQDN」を選択する場合
(3)	アドレス	「ネットワークアドレス」、「範囲指定アドレス又は FQDN」を入力

表 7-1-16 サービス設定

図中番号	名前	利用用途
(1)	名前	「サービス名」を入力 (※) 文字数制限は 63 字迄 また、英数字、スペース、ハイフン (「-」)、アンダースコア (「_」)、ピリオド (「.」) を名前に含めることが可能

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

(2)	プロトコル	「TCP」：「TCP」プロトコルを使用する場合 「UDP」：「UDP」プロトコルを使用する場合
(3)	宛先ポート	「宛先ポート番号範囲」を入力

表 7-1-17 URL フィルタリングポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「セキュリティポリシー名」を入力 (※) 文字数制限は 31 字迄 また、英数字、スペース、ハイフン ([-])、アンダースコア (_)、ピリオド ( [. ]) を名前に含めることができます
(2)	送信元	送信元ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「送信元ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(3)	送信元	送信元アドレス	「送信元アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(4)	宛先	宛先ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(5)	宛先	宛先アドレス	「宛先アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(6)	アプリケーション	アプリケーション	デフォルトのまま
(7)	サービス/URL カテゴリ	サービス/URL カテゴリ	「サービス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(8)	アクション	アクション	プルダウンより以下を選択 Action が「許可」の場合：「Allow」を選択 Action が「拒否」の場合：「Deny」を選択
(9)	アクション	プロファイルタイプ	プルダウンより以下を選択 「プロファイル」 プルダウンより以下を選択 (手順 7-1-3 で作成した) 「URL プロファイル」
(10)	アクション	ログ設定	以下を選択 セッション終了後にロギング：セッション終了時にログ Panorama へ通信ログを送付する場合は、「ログ転送」のプルダウンより「Profile_Log_Forwarding」を選択。

- ① 「Objects」タブ > 「アドレス」> 「追加」ボタンをクリックします。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

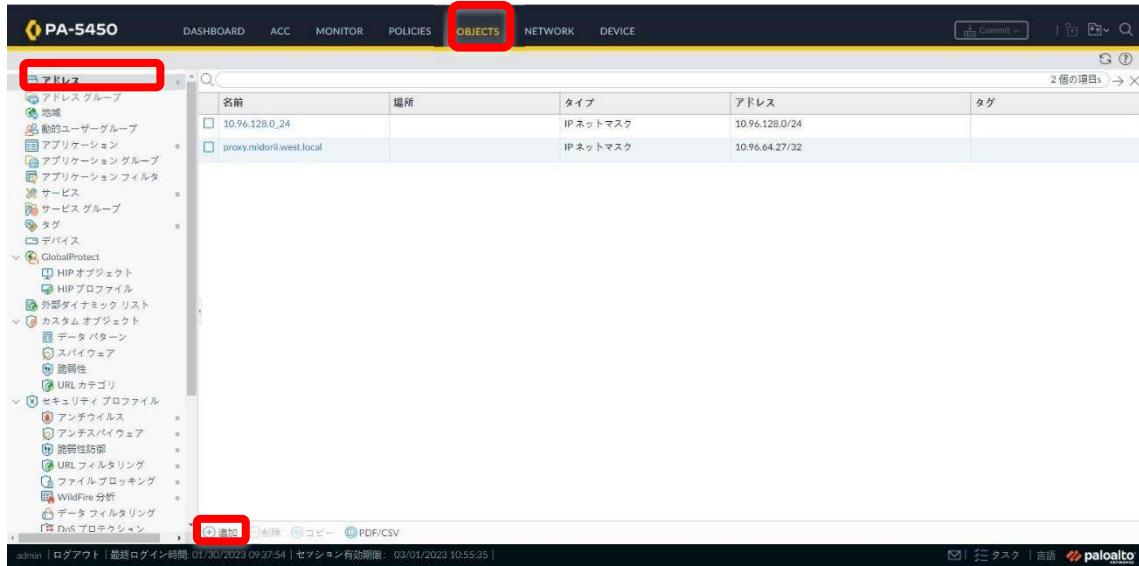


図 7-1-18 URL フィルタリングポリシー追加

② 以下 (1) ~ (3) を設定（「表 7-1-15」を参照）し、「OK」ボタンをクリックします。

図 7-1-19 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

③ 「Objects」タブ > 「サービス」> 「追加」ボタンをクリックします。

名前	場所	プロトコル	宛先ポート	タグ
service-https	事前定義名	TCP	443	

図 7-1-20 URL フィルタリングポリシー追加

④ 以下 (4) ~ (6) を設定（「表 7-1-16」を参照）し、「OK」ボタンをクリックします。

サービス

名前  (4)

内容

プロトコル  TCP  UDP (5)

宛先ポート  (6)

送信元ポート

セッションタイム  アプリケーションから継承  オーバーライド

アウト

タグ

OK キャンセル

図 7-1-21 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

⑤ 「Policies」 > 「セキュリティ」 > 「追加」 ボタンをクリックします。

The screenshot shows the PA-5450 configuration interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES (highlighted with a red box), OBJECTS, NETWORK, and DEVICE. Below the navigation is a search bar and a commit button. The main area is titled 'セキュリティ' (Security) and contains a table of existing policies:

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
interzone-default	none	interzone	any	any	any	any	any	any

A sidebar on the left lists security-related options like QoS, Policy-Based Forwarding, Tunnel Inspection, Application Overlay, and SD-WAN. At the bottom, there's a toolbar with buttons for adding, deleting, copying, and saving, along with PDF/CSV export and a help icon.

図 7-1-22 URL フィルタリングポリシー追加

⑥ 以下 (7) ~ (14) を設定（「表 7-1-17」を参照）し、「OK」ボタンをクリックします。

The dialog box is titled 'セキュリティ ポリシールール' (Security Policy Rule). It has tabs for General, Source, Destination, Application, Service/URL Category, and Actions. The General tab is active, showing fields for 'Name' (name) and 'ゾーン' (Zone) (selected as 'universal (default)'). A large red box highlights the 'Name' field. Other tabs show 'タグ' (Tag) set to 'None', '監査コメント' (Audit Comment) field, and audit comment archive link. At the bottom right are 'OK' and 'キャンセル' (Cancel) buttons, with a red box highlighting the 'OK' button.

図 7-1-23 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

⑦ 作成したポリシーを選択し、「移動」にて任意の位置へ移動します。

※新規で作成したポリシーは「intrazone-default」の上に作成されます。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any
test1	none	universal	internal_WEST	10.90.128.0_24	any	any	internal_Sv_Critical	any
intrazone-default	none	intrazone	any	any	any	any	[intrazone]	any

図 7-1-24 URL フィルタリングポリシー追加

⑧ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。

（設定が反映されるまで 5 分程度かかることがあります）

図 7-1-25 URL フィルタリングポリシー追加／設定反映

コミット スコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

図 7-1-26 URL フィルタリングポリシー追加／設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### URL フィルタリングポリシーの作成例

以下 URL フィルタリングポリシー追加の設定例として、

「7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック（新規作成）」にて作成した URL プロファイルをポリシーに適用する手順を記載します。

※一からポリシーを作成する場合、ポリシーの順序を検討する必要があるため、既存のポリシーをコピーし、その下に作成する手順を記載しています。

ここで追加するポリシーの前提条件として、個人向けのプロファイルを適用するポリシーであるため、SourceIP アドレスはホストの場合のみとしています。

その他、SourceIP アドレスがセグメント単位(/24 など)、アドレスレンジの場合、追加するポリシーの順序を検討して配置する必要があります。

※本項最後に記載している「補足：ファイアウォールポリシーの順序」を合わせてご参照ください。

設定例) 7. 1. 3. 1. で作成した URL プロファイルを新規作成したポリシーに適用する。

① 既存ポリシーをコピーし、新規ポリシーを作成する。

「Policies」>「セキュリティ」>ポリシー「test1」を選択>「コピー」をクリックします。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any
2 test1	none	universal	Internal_WEST	10.96.128.0_24	any	any	Internal_SV_Critical	any
interzone-default	none	interzone	any	any	any	any	(Unassigned)	any
4 interzone-default	none	interzone	any	any	any	any	any	any

図 7-1-27 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ② 「ルール順序」が「事後ルール」「test1」になっている事を確認し、「OK」をクリックします。

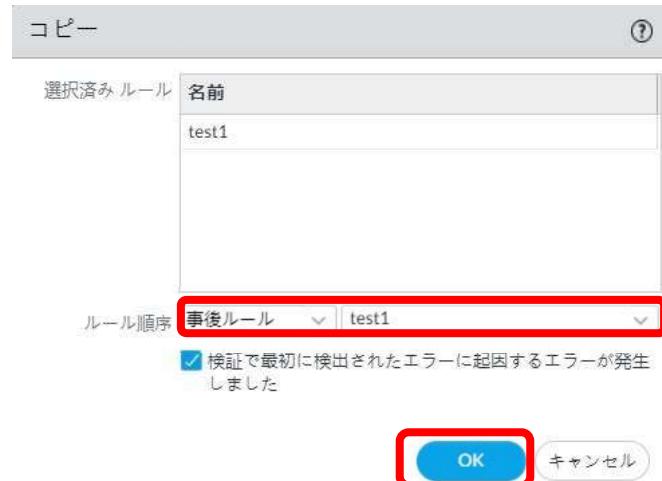


図 7-1-28 URL フィルタリングポリシー追加

- ③ 「test1」の下に「test1-1」で、  
新しいポリシーが作成されていることを確認します。

図 7-1-29 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ④ 新しく作成されたポリシー「test1-1」をクリックし、  
ポリシー名を変更します。

※ここでは(例)として変更後のポリシー名を「test2」としています。

図 7-1-30 URL フィルタリングポリシー追加

- ⑤ 「送信元」を選択し、「追加」ボタンを押下。空欄に入力したアドレスを選択します。

図 7-1-31 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ⑥ 空欄に入力したアドレスが存在しない場合、「アドレス」を押下し、アドレスを新規作成します。（作成方法は、7-1-5②を参照）

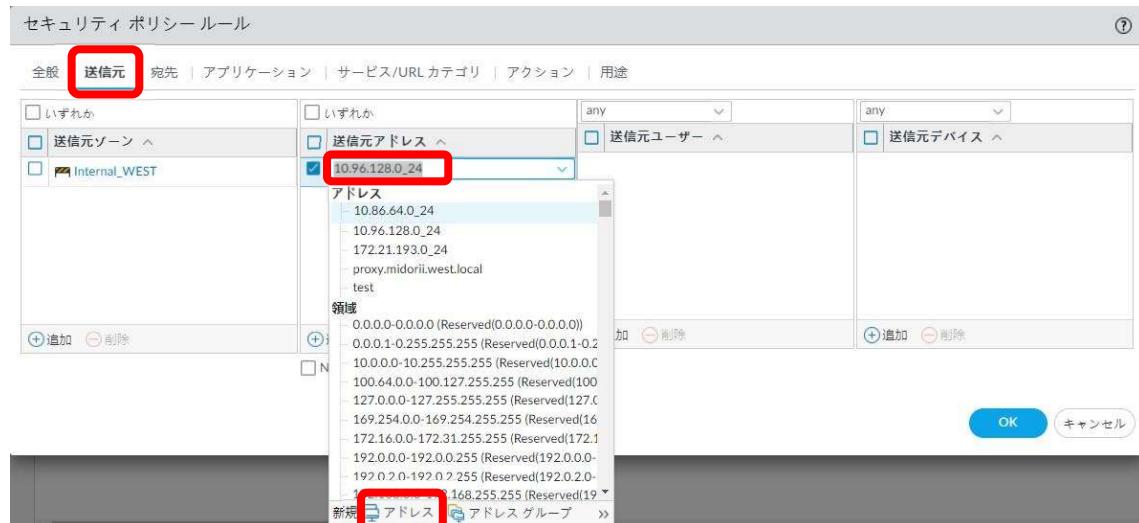


図 7-1-3-2 URL フィルタリングポリシー追加



図 7-1-3-3 URL フィルタリングポリシー追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

⑦ 作成した URL\_Profile を選択し、OK ボタンを押下します。

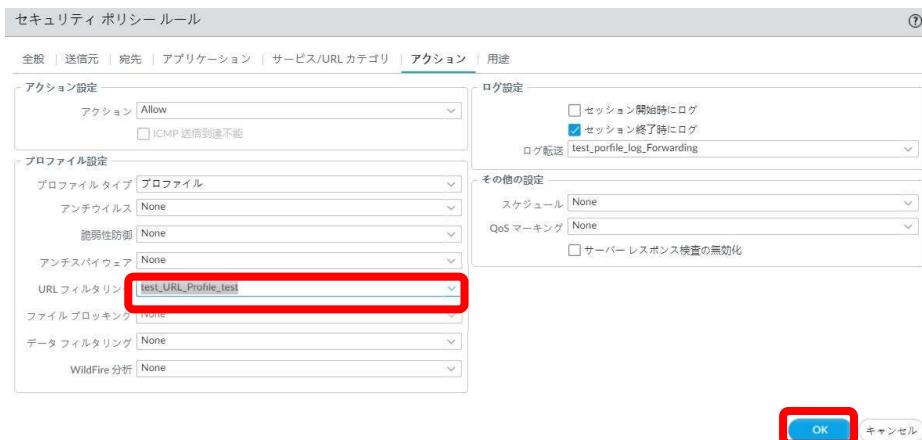


図 7-1-34 URL フィルタリングポリシー追加

⑧ ポリシーが作成されていることを確認します。

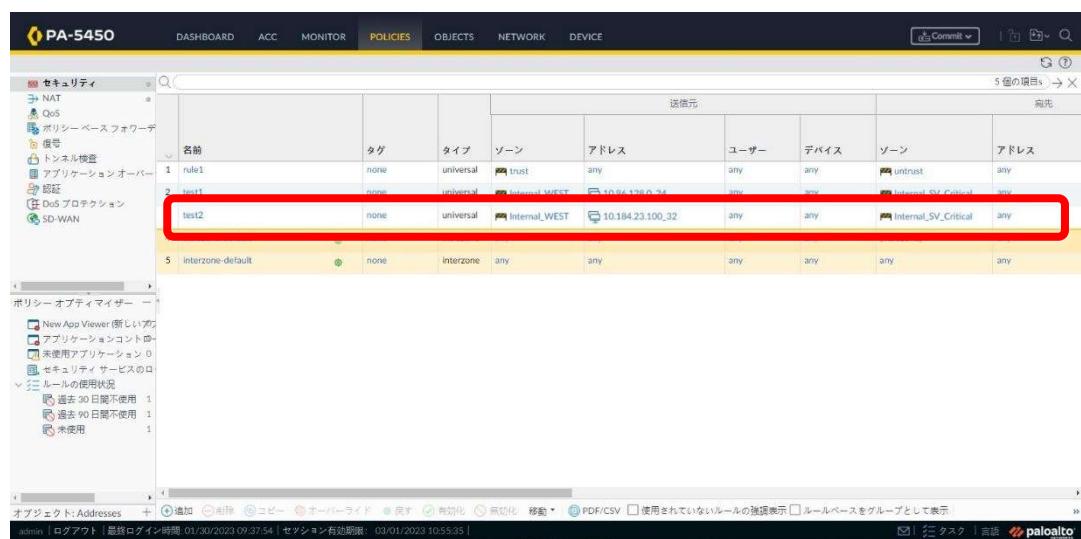


図 7-1-35 URL フィルタリングポリシー追加

#### 補足：ファイアウォールポリシーの順序

ポリシーは上から順番にチェックし、一致した時点でそれ以降のポリシーはチェックしません。そのため、IP アドレスの範囲が狭いものを上に、IP アドレスの範囲が広いものを下に記載します。

※IP アドレス範囲が広いものを上に記載した場合には、そのポリシーに一致した時点でそれ以降のポリシーを見ない為、意図した制御ができなくなります。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

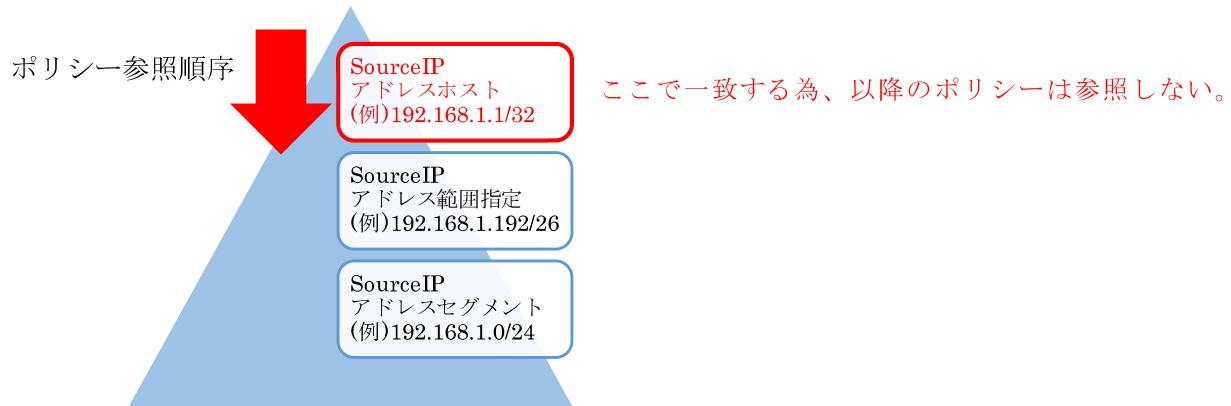


図 7－1－5 3 ポリシー参照順序

上記のポリシー順序の場合、192.168.1.1/32 で通信してきた際、一番上に記載したポリシーに一致する為、意図した制御が可能です。



図 7－1－5 4 ポリシー参照順序

上記のポリシー順序の場合、192.168.1.1/32 で通信してきた際、一番上に記載されたポリシーに一致し、それ以降を参照しない為、意図した制御が出来ません。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 5. URL プロファイル削除

不要になった URL プロファイルを削除する手順を記載します。

URL プロファイルはファイアウォールポリシーに適用されている場合、削除することができません。削除する前にファイアウォールポリシーから削除します。

表 7-1-18 URL プロファイル削除

URL プロファイル	削除方法
(1) ポリシーに適用されていない	直接 URL プロファイルの削除実施
(2) ポリシーに適用されている	該当のポリシーから未適用状態にし、URL プロファイルの削除を実施

#### (1) ポリシーに適用されていない URL フィルタの削除

- ① 「Objects」 > 「URL フィルタリング」 > 削除対象の URL プロファイル名にチェックします。「削除」をクリックします。

名前	場所	サイト アクセス	ユーザー証明書送信	HTTP ヘッダー検査
default	事前定義済み	Allow Categories (59) Alert Categories (5) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (75) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_001		Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1)	
test_URL_Profile_003		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_test		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	

図 7-1-36 URL プロファイル削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 「はい」をクリックし、削除します。



図 7-1-3-7 URL プロファイル削除

③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
(設定が反映されるまで 5 分程度かかることがあります)



図 7-1-3-8 URL プロファイル削除

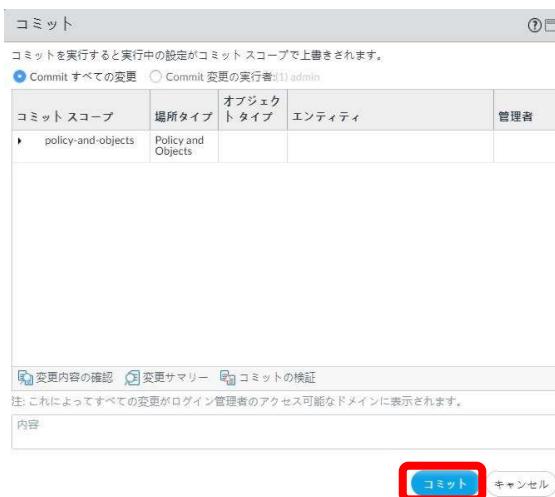


図 7-1-3-9 URL プロファイル削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

(2) ポリシーに適用されている URL フィルタの削除

- ① 「Objects」 > 「URL フィルタリング」 > 削除対象の URL プロファイル名にチェックします。「削除」をクリックします。

名前	場所	サイトアクセス	ユーザー証明書送信	HTTPヘッダー検査
default	事前定義済み	Allow Categories (59) Alert Categories (5) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (75) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_001		Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1)	
test_URL_Profile_003		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_test		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	

図 7-1-40 URL プロファイル削除

- ② 「はい」をクリックし、削除します。



図 7-1-41 URL プロファイル削除

- ③ ポリシーに適用されている為、エラーメッセージが表示されます。



図 7-1-42 URL プロファイル削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ④ 「Policies」 > 「セキュリティ」 > エラーメッセージで表示されたポリシー名で検索します。ポリシー名「test2」をクリックします。  
※ここでは(例)として「test2」としています。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	Trust	any	any	any	untrust	any
test1	none	universal	Internal_WEST	10.96.128.0-24	any	any	Internal_SV_Critical	any
test2	none	universal	Internal_WEST	10.184.23.100-32	any	any	Internal_SV_Critical	any
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
Interzone-default	none	interzone	any	any	any	any	any	any

図 7-1-4-3 URL プロファイル削除

- ⑤ 「アクション」 > 「URL フィルタリング」を選択し、「None」に変更します。

図 7-1-4-4 URL プロファイル削除

以上でファイアウォールポリシーから削除対象の URL プロファイルが外されました。次に URL プロファイルを削除します。削除の手順は、「(1) ポリシーに適用されていない URL フィルタの削除」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 6. カテゴリ修正

カテゴリによる許可、ブロックする動作を変更する手順を記載します。

全社、本体、本体個人、全 G 会社、G 会社ごとのそれぞれの手順を記載します。

### 7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック

表 7-1-19 全社カテゴリ

対象	変更対象 URL プロファイル
(13) 全社（本体、G 会社）のカテゴリ許可に変更 (例) 「Insufficient-content」を「alert」に変更 (1 3) - 1 GUI 変更方法記載 (1 3) - 2 CLI 変更方法記載	本体、G 会社の URL フィルタプロファイルから変更します。 (13)、(14) 本体、G 会社の URL プロファイルが変更対象です（全制限端末以外の全てのプロファイルが変更対象）。
(14) 全社（本体、G 会社）のカテゴリブロックに変更 (例) 「Insufficient-content」を「block」に変更 (1 4) - 1 GUI 変更方法記載 (1 4) - 2 CLI 変更方法記載	

(13) 全社（本体、G 会社）のカテゴリ許可に変更

#### (13)-1 各 URL プロファイルを GUI にて変更

- ① 「Objects」 > 「URL フィルタリング」 > 変更対象の URL プロファイル名をクリックします。

図 7-1-45 全社（本体、G 会社）のカテゴリ許可に変更

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② カテゴリ「Insufficient-content」（例）を選択します。

※「Insufficient-content」を入力すると、「Insufficient-content」のみ表示されます。

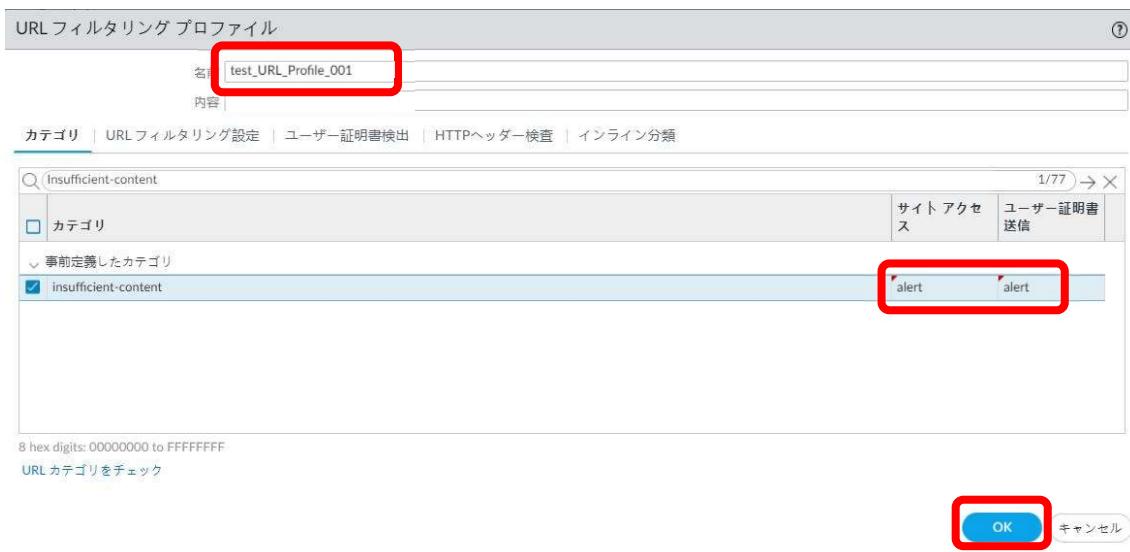


図 7-1-4-6 全社(本体、G 会社)のカテゴリ許可に変更

③ カテゴリ「Insufficient-content」のサイトアクセスを「block」から「alert」に、ユーザ証明書送信を「block」から「allow」に変更します。

※カテゴリをブロックに変更する場合はサイトアクセスを「alert」から「block」に変更します。（ユーザ証明書送信は自動で block へ変更されます）

図 7-1-4-7 全社(本体、G 会社)のカテゴリ許可に変更



ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ④ カテゴリ「Insufficient-content」のサイトアクセスが「alert」、ユーザ証明書送信が「allow」になっている事を確認し、「OK」をクリックします。

※アクションを「block」に変更した場合は、「block」になっている事を確認します。

- ⑤ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
(設定が反映されるまで5分程度かかることがあります)



図 7-1-48 全社(本体、G会社)のカテゴリ許可に変更／設定反映

コミット

コミットを実行すると実行中の設定がコミットスコープで上書きされます。

Commit すべての変更  Commit 変更の実行者:(1) admin

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

変更内容の確認 变更サマリー コミットの検証  
注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容

**コミット** キャンセル

図 7-1-49 全社(本体、G会社)のカテゴリ許可に変更／設定反映

### (13)-2 各 URL プロファイルを CLI にて変更

- ① コンフィグレーションモードへ移行後、以下のコマンドを各 URL プロファイルに実施します。※モード遷移は図 3-1-5 を参照

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

表 7-1-20 URL プロファイルカテゴリルール変更（ブロック→許可）

名前	説明
url-filtering	「URL プロファイル名」を入力 （※）User_Profile_001：全社用プロファイル
Category	ブロックからアラートに変更したい「カテゴリルール」を入力

#### 構文

```
delete profiles url-filtering <name> block <Category>
```

```
set profiles url-filtering <name> alert <Category>
```

#### 例

```
delete profiles url-filtering URL_Profile_001 block insufficient-content
```

```
set profiles url-filtering URL_Profile_001 alert insufficient-content
```

上記(例)のコンフィグは、vsys2Internal\_VR に設定されている URL\_Profile\_001 のカテゴリルールです。

「Insufficient-content」を「block」から「alert」に変更する手順です。

1 行目の delete で block を削除し、2 行目の set で alert を設定しています。

※斜体は任意の文字列です。

※変更対象の URL プロファイルが複数存在し、流し込みで設定変更を実施する場合は、

「コピーと貼り付け」の「貼り付けの行間遅延(A)」を 350 ミリ秒にします。

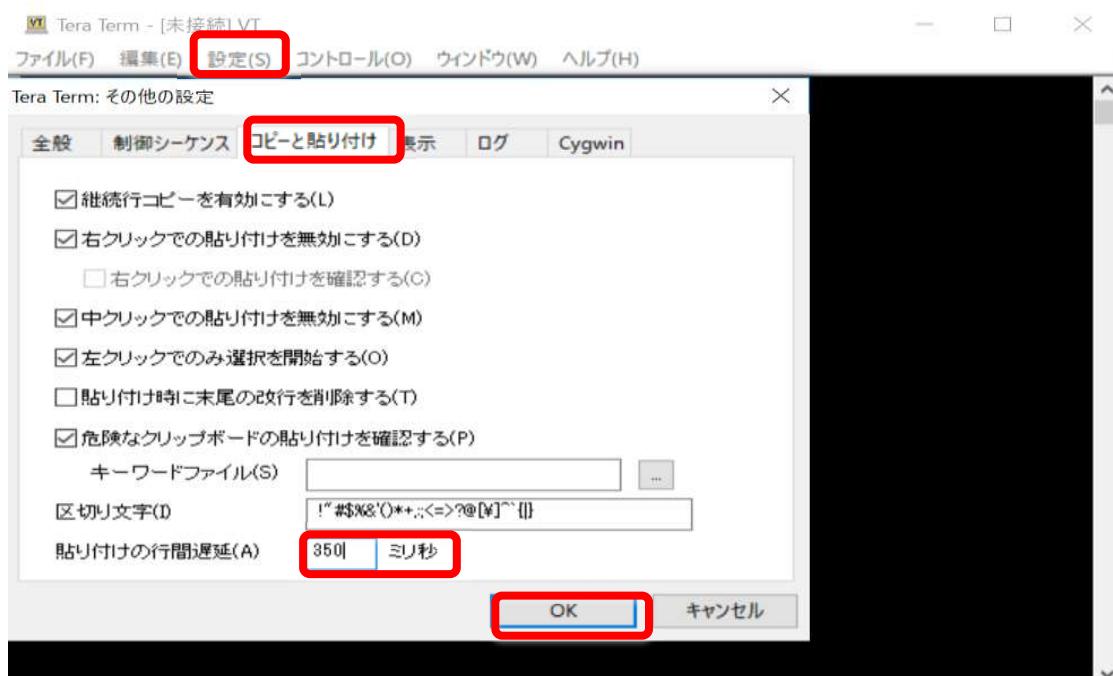


図 7-1-50 全社(本体、G 会社)のカテゴリ許可に変更 CLI

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 設定を反映する為、「commit」を実施します。

(14) 全社(本体、G 会社)のカテゴリブロックに変更

#### (14) – 1 各 URL プロファイルを GUI にて変更

① 各 URL プロファイルを GUI にて変更します。

カテゴリ「Insufficient-content」のアクションを「alert」から「block」に変更します。

以降の手順は「7. 1. 6. 1 (13) – 1」の手順と同様です。

#### (14) – 2 各 URL プロファイルを CLI にて変更

① コンフィグレーションモードへ移行後、以下のコマンドを各 URL プロファイルにて実施します。※モード遷移は図 3 – 1 – 5 を参照

表 7 – 1 – 2 1 URL プロファイルカテゴリルール変更（許可→ブロック）

名前	説明
url-filtering	「URL プロファイル名」を入力 （※）User_Profile_001：全社用プロファイル
Category	アラートからブロックに変更したい「カテゴリルール」を入力

#### 構文

```
delete profiles url-filtering <name> alert <Category>
```

```
set profiles url-filtering <name> block <Category>
```

#### 例

```
delete profiles url-filtering URL_Profile_001 alert insufficient-content
```

```
set profiles url-filtering URL_Profile_001 block insufficient-content
```

上記(例)のコンフィグは、Internal\_VR に設定されている URL\_Profile\_001 のカテゴリルールです。

「Insufficient-content」を「alert」から「block」に変更する手順です。

1 行目の delete で alert を削除し、2 行目の set で block を設定しています。

※斜体は任意の文字列です。

※変更対象の URL プロファイルが複数存在し、流し込みで設定変更を実施する場合は、

「コピーと貼り付け」の「貼り付けの行間遅延(A)」を 350 ミリ秒にします。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

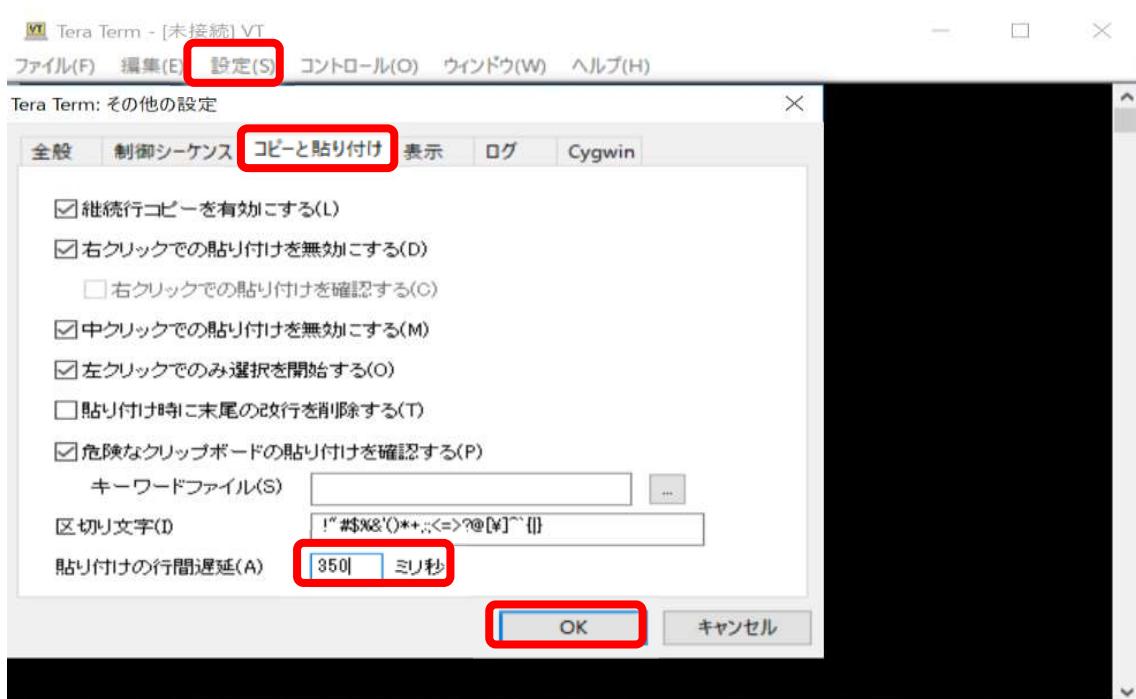


図 7－1－5 1 全社(本体、G 会社)のカテゴリブロックに変更 CLI

② 設定を反映する為、「commit」を実施します。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 6. 2. 本体カテゴリ許可/本体カテゴリブロック

表 7-1-22 本体カテゴリ許可／本体カテゴリブロック

対象	変更対象 URL プロファイル
(15) 本体カテゴリ許可に変更 (例) 「Insufficient-content」を「alert」に変更 (15)-1 GUI 変更方法 (15)-2 CLI 変更方法	(15)、(16) 本体の URL プロファイルが変更対象です。
(16) 本体カテゴリブロックに変更 (例) 「Insufficient-content」を「block」に変更 (16)-1 GUI 変更方法 (16)-2 CLI 変更方法	

(15) 本体カテゴリ許可に変更

### (15)-1 各 URL プロファイルを GUI にて変更

- ① カテゴリ「Insufficient-content」のアクションを「block」から「alert」に変更します。

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック (13)-1」の手順と同様です。

### (15)-2 各 URL プロファイルを CLI にて変更

- ① カテゴリ「Insufficient-content」のアクションを「block」から「alert」に変更します。

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック (13)-2」の手順と同様です。

(16) 本体カテゴリブロックに変更

### (16)-1 各 URL プロファイルを GUI にて変更

- ① カテゴリ「Insufficient-content」のアクションを「alert」から「block」に変更します。

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック (13)-1」

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

の手順と同様です。

#### (16) – 2 各 URL プロファイルを CLI にて変更

- ① カテゴリ「Insufficient-content」のアクションを「alert」から「block」に変更します。

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（14）– 2」の手順と同様です。

7. 1. 6. 3. 本体個人のカテゴリ許可/本体個人のカテゴリブロック

表 7 – 1 – 2 3 本体個人のカテゴリ許可／本体個人のカテゴリブロック

対象	変更対象 URL プロファイル
<p>(17) 本体個人のカテゴリ許可に変更 (例) 「Insufficient-content」を「alert」に変更</p> <p><b>(17) – 1 GUI 変更方法</b>            (17) – 1 – 1 既存 URL プロファイルが存在する場合 (例) 役員用 ¥Allow_10.184.80.24            (17) – 1 – 2 新規 URL プロファイルを作成する場合 (例) 四国支社配下に個別 URL プロファイルを作成する。</p> <p><b>(17) – 2 CLI 変更方法</b>            (17) – 2 – 1 既存 URL プロファイルが存在する場合 (例) 役員用 ¥Allow_10.184.80.24            (17) – 2 – 2 新規 URL プロファイルを作成する場合 (例) 四国支社配下に個別 URL プロファイルを作成する。</p>	本体個人の URL プロファイルが変更対象です。
<p>(18) 本体個人のカテゴリブロックに変更 (例) 「Insufficient-content」を「block」に変更</p> <p><b>(18) – 1 GUI 変更方法</b>            (18) – 1 – 1 既存 URL プロファイルが存在する場合 (例) 役員用 ¥Allow_10.184.80.24            (18) – 1 – 2 新規 URL プロファイルを作成する場合 (例) 四国支社配下に個別 URL プロファイルを作成する。</p> <p><b>(18) – 2 CLI 変更方法</b>            (18) – 2 – 1 既存 URL プロファイルが存在する場合 (例) 役員用 ¥Allow_10.184.80.24            (18) – 2 – 2 新規 URL プロファイルを作成する場合 (例) 四国支社配下に個別 URL プロファイルを作成する。</p>	本体個人の URL プロファイルが変更対象です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

(17) 本体個人のカテゴリ許可に変更

#### (17)-1 URL プロファイルを GUI にて変更

設定変更対象の個人プロファイルが「存在する」「存在しない」により手順が異なります。

##### (17)-1-1 既存 URL プロファイルが存在する場合

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-1」の手順と同様です。

##### (17)-1-2 新規 URL プロファイルを作成する場合

① 「7. 1. 3.」および「7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック（新規 URL プロファイル作成）」の手順を参照し、個別 URL プロファイルを新規に作成します。

② 「7. 1. 5. URL フィルタリングポリシー追加」の手順を参照し、ポリシーを作成します。

③ 以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-1」の手順と同様です。

#### (17)-2 URL プロファイルを CLI にて変更

設定変更対象の個人プロファイルが「存在する」「存在しない」により手順が異なります。

##### (17)-2-1 既存 URL プロファイルが存在する場合

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-2」の手順と同様です。

##### (17)-2-2 新規 URL プロファイルを作成する場合

① 「7. 1. 3.」および「7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック（新規 URL プロファイル作成）」の手順を参照し、個別 URL プロファイルを作成します。

② 「7. 1. 5. URL フィルタリングポリシー追加」の手順を参照し、ポリシーを作成します。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

③ 以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－2」の手順と同様です。

(18) 本体個人のカテゴリブロックに変更

(18)－1 URL プロファイルを GUI 変更方法

設定変更対象の個人プロファイルが「存在する」「存在しない」により手順が異なります。

(18)－1－1 既存 URL プロファイルが存在する場合

以降の手順は「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－1」の手順と同様です。

(18)－1－2 新規 URL プロファイルを作成する場合

- ① 「7. 1. 3.」および「7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック(新規 URL プロファイル作成)」の手順を参照し、個別 URL プロファイルを作成します。
- ② 「7. 1. 5. URL フィルタリングポリシー追加」の手順を参照し、ポリシーを作成します。
- ③ 以降の手順は、「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－2」の手順と同様です。

(18)－2 URL プロファイルを CLI 変更方法

設定変更対象の個人プロファイルが「存在する」、「存在しない」により手順が異なります。

(18)－2－1 既存 URL プロファイルが存在する場合

以降の手順は、「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（14）－2」の手順と同様です。

(18)－2－2 新規 URL プロファイルを作成する場合

- ① 「7. 1. 3.」および「7. 1. 3. 1. 本体個人のアクセス解除/本体個人のブロック(新規 URL プロファイル作成)」の手順を参照し、個別 URL プロファイルを作成します。
- ② 「7. 1. 5. URL フィルタリングポリシー追加」の手順を参照し、ポリシーを

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

作成します。

- ③ 以降の手順は、「7. 1. 7. 1. 全社カテゴリ許可/全社カテゴリロック（1  
3）－2」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 6. 4. 全G会社のカテゴリ許可/全G会社カテゴリブロック

表7-1-24 全G会社のカテゴリ許可／全G会社のカテゴリブロック

対象	変更対象 URL プロファイル
(19) G会社全てのカテゴリ許可 (例)「Insufficient-content」を「alert」に変更  (19)-1 GUI 変更方法 (19)-2 CLI 変更方法	全G会社の URL プロファイルが変更対象です。
(20) G会社全てのカテゴリブロック (例)「Insufficient-content」を「block」に変更  (20)-1 GUI 変更方法 (20)-2 CLI 変更方法	

(19) 全G会社のカテゴリ許可

(19)-1 GUI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-1」の手順と同様です。

(19)-2 CLI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-2」の手順と同様です。

(20) 全G会社のカテゴリブロック

(20)-1 GUI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）-1」の手順と同様です。

(20)-2 CLI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（14）-2」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 1. 6. 5. G 会社ごとのカテゴリ許可/G 会社ごとのカテゴリブロック

表 7－1－25 全 G 会社ごとのカテゴリ許可／全 G 会社ごとのカテゴリブロック

対象	変更対象 URL プロファイル
(21) G 会社全てのカテゴリルール変更 (例) 「Insufficient-content」を「alert」に変更 (21)－1 GUI 変更方法 (21)－2 CLI 変更方法	G 会社ごとの URL プロファイルが変更対象です。
(22) G 会社全てのカテゴリルール変更 (例) 「Insufficient-content」を「block」に変更 (22)－1 GUI 変更方法 (22)－2 CLI 変更方法	

(21) G 会社全てのカテゴリルール変更

(21)－1 GUI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－1」の手順と同様です。

(21)－2 CLI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－2」の手順と同様です。

(22) G 会社全てのカテゴリルール変更

(22)－1 GUI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（13）－1」手順と同様です。

(22)－2 CLI 変更方法

以降の手順は、

「7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック（14）－2」の手順と同様です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 7. カスタムカテゴリ追加

カスタムカテゴリを新規に追加するときの手順を記載します。

- ① 「Objects」タブ > 「URL カテゴリ」 > 「追加」をクリックします。

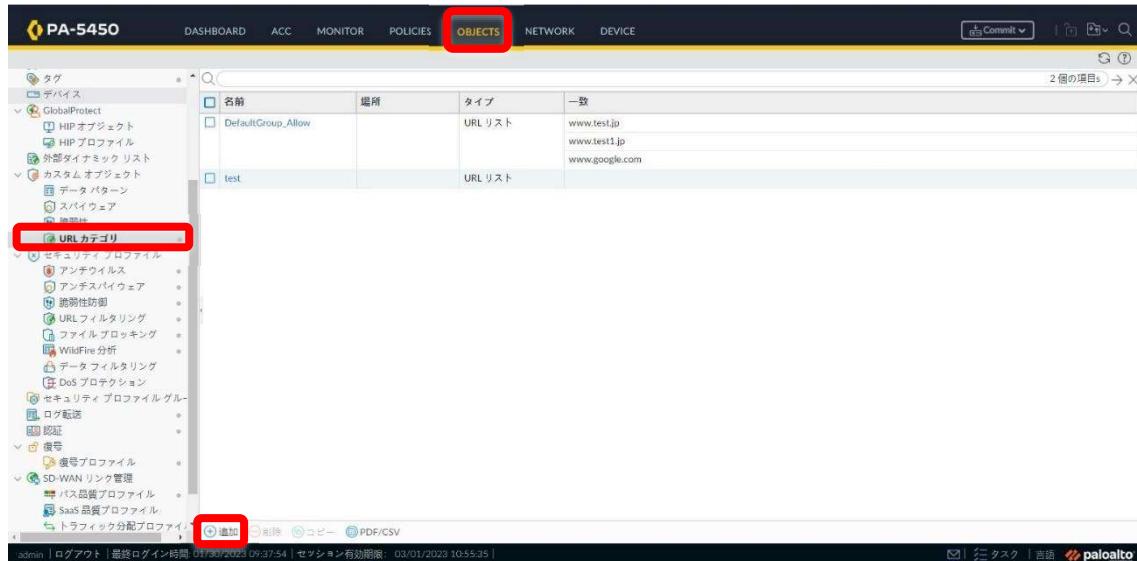


図 7-1-5-2 カスタムカテゴリ追加

- ② カスタムカテゴリ名を入力し、「OK」をクリックします。

名前	test_category
内容	
タイプ	URL List

以下の URL、ドメイン、またはホスト名のいずれかに一致

サイト
-----

1行あたり1つのエントリを入力します。  
各エントリはフォームである可能性があります www.example.com または次のようなワイルドカードが含まれている可能性があります www.\*.com.

To ensure an exact entry match, use a forward slash (/) at the end of your entry. Example: xyz.com/ matches only xyz.com. For more info, see URL カテゴリの例外

OK

キャンセル

図 7-1-5-3 カスタムカテゴリ追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 最下段に登録されている事を確認します。

名前	場所	タイプ	一覧
DefaultGroup_Allow		URL リスト	www.testjp www.test1.jp www.google.com
test_category		URL リスト	

図 7-1-5-4 カスタムカテゴリ追加

- ④ 新しく作成したカスタムカテゴリに URL を登録します。

※URL の登録手順は、

「7. 1. 2. 1. 全社アクセス解除/全社ブロック」の登録手順と同様

- ⑤ 新しく作成したカスタムカテゴリを URL プロファイルに適用します。

名前	場所	サイト アクセス	ユーザー証明書送信	HTTP ヘッダー検査
default	事前定義済み	Allow Categories (59) Alert Categories (5) Continue Categories (0) Block Categories (11) Override Categories (0)	Allow Categories (75) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_001		Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (1)	
test_URL_Profile_003		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	
test_URL_Profile_test		Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (0)	

図 7-1-5-5 カスタムカテゴリ追加

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ⑥ サイトアクセスを「none」から「allow」へ、ユーザ証明書送信を「none」から「allow」へ変更します。

※カスタムカテゴリを新規に追加すると、既に設定済みの全URLプロファイルに対して、Actionが「none」の状態で追加されます。

カタゴリ	サイト アクセス	ユーザー証明書
DefaultGroup_Allow *	allow	allow
test *	allow	allow
test_category *	none	none
abortion	allow	allow
abused-drugs	allow	allow

図 7－1－5 6 カスタムカテゴリ追加

- ⑦ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。

(設定が反映されるまで5分程度かかることがあります)

図 7－1－5 7 カスタムカテゴリ追加/設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

コミット

コミットを実行すると実行中の設定がコミット スコープで上書きされます。

Commit すべての変更  Commit 変更の実行者(1) admin

コミット スコープ	場所タイプ	オブジェクト タイプ	エンティティ	管理者
▶ policy-and-objects	Policy and Objects			

変更内容の確認 変更サマリー コミットの検証

注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容

**コミット** キャンセル

図 7-1-58 カスタムカテゴリ追加/設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 1. 8. カスタムカテゴリ削除

カスタムカテゴリを削除するときの手順を記載します。削除するカスタムカテゴリの「Action が「none」以外の URL プロファイルが存在する場合」、そのカテゴリは使用されていると判断されて削除することができません。削除する前に Action を「none」に変更する必要があります。

- ① 「Objects」タブ > 「URL カテゴリ」 > 「test\_category」を選択し、削除対象のカスタムカテゴリ名にチェックし、「削除」をクリックします。

名前	場所	タイプ
DefaultGroup_Allow		URL リスト
test		URL リスト
test_category		URL リスト

図 7-1-59 カスタムカテゴリ削除

- ② 「はい」をクリックし、削除します。



図 7-1-60 カスタムカテゴリ削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

③ URL プロファイルで適用されている為、エラーメッセージが表示されます。

削除中にエラーが発生しました カスタム URL カテゴリ

Number of failed record(s): 1

1- Failed to delete custom URL category - test\_category.  
◦ test\_category cannot be deleted because of references from:  
◦ profiles -> url-filtering -> test\_URL\_Profile\_test -> block.  
◦ profiles -> url-filtering -> test\_URL\_Profile\_test -> credential-enforcement -> block

閉じる

図 7－1－6 1 カスタムカテゴリ削除

④ 「Objects」タブ > 「URL フィルタリング」 > エラーメッセージで表示された URL プロファイル名で検索します。

URL プロファイル名「test\_URL\_Profile\_test」をクリックします。

※ここでは(例)として「test\_URL\_Profile\_test」としています。

PA-5450

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

1/4 → X

名前	サイト アクセス	ユーザー証明書送信	HTTP ヘッダー検査
test_URL_Profile_test	Allow Categories (77) Alert Categories (0) Continue Categories (0) Block Categories (1) Override Categories (0)	Allow Categories (77) Alert Categories (0) Continue Categories (0)	

admin | ログアウト | 最終ログイン時間: 01/30/2023 09:37:54 | セッション有効期限: 03/01/2023 10:55:35 | License required for URL Filtering to function. (\* カスタム URL カテゴリを示す。外部ダイナミックリストを指定)

図 7－1－6 2 カスタムカテゴリ削除

⑤ 削除対象のカスタムカテゴリのサイトアクセス及びユーザ証明書送信を「none」に変更し、「OK」をクリックします。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI



図 7-1-63 カスタムカテゴリ削除

- ⑥ 「Objects」タブ > 「URL カテゴリ」 > 削除対象のカスタムカテゴリ名にチェックし、「削除」をクリックします。

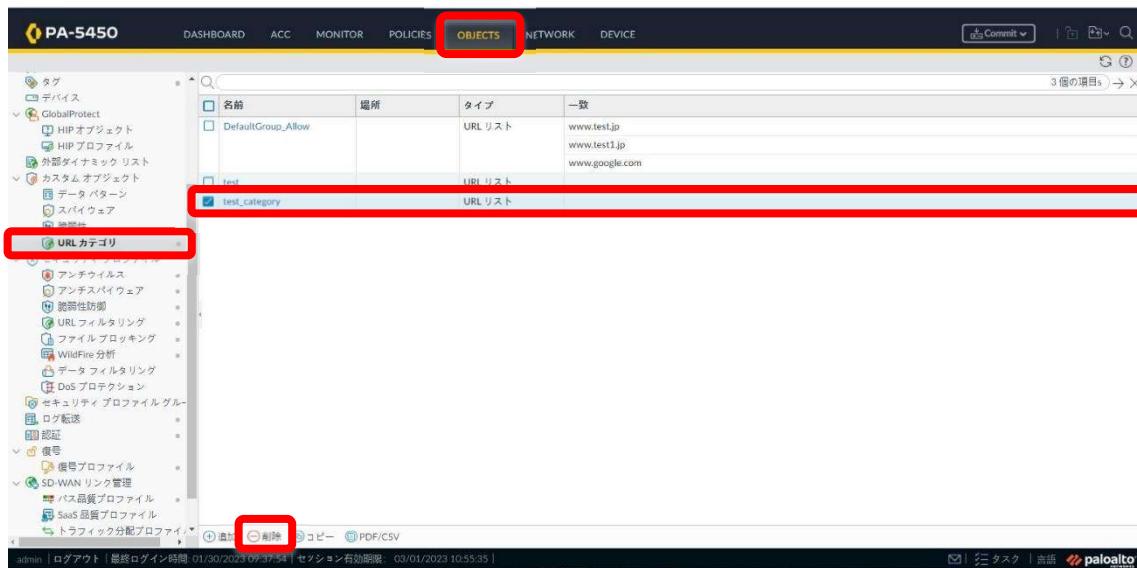


図 7-1-64 カスタムカテゴリ削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ⑦ 「はい」をクリックし、削除します。

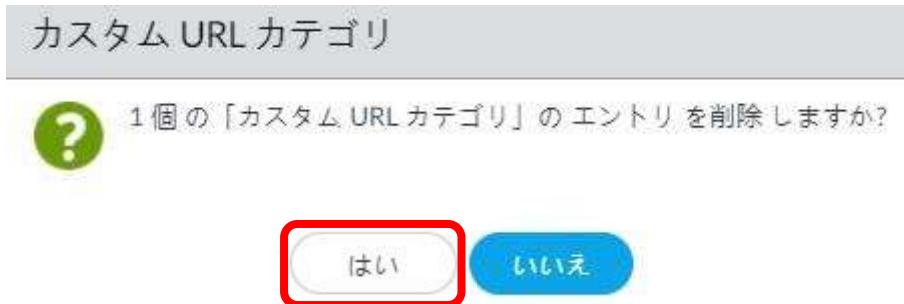


図 7-1-6-5 カスタムカテゴリ削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 2. URL フィルタリングポリシー修正

URL フィルタリングポリシーの修正手順を記載します。

表 7-2-1 URL フィルタリングポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「セキュリティポリシー名」を入力 (※) 文字数制限は 31 字迄 また、英数字、スペース、ハイフン (「-」)、アンダースコア (「_」)、ピリオド (「.」) を名前に含めることが可能
(2)	送信元	送信元ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「送信元ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(3)	送信元	送信元アドレス	「送信元アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(4)	宛先	宛先ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(5)	宛先	宛先アドレス	「宛先アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(6)	アプリケーション	アプリケーション	デフォルトのまま
(7)	サービス/URL カテゴリ	サービス/URL カテゴリ	「サービス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(8)	アクション	アクション	プルダウンより以下を選択 Action が「許可」の場合：「Allow」を選択 Action が「拒否」の場合：「Deny」を選択
(9)	アクション	プロファイルタイプ	プルダウンより以下を選択 「プロファイル」 プルダウンより以下を選択 (手順 7-1-3 で作成した) 「URL プロファイル」
(10)	アクション	ログ設定	以下を選択 セッション終了後にロギング：セッション終了時にログ Panorama へ通信ログを送付する場合は、「ログ転送」のプルダウンより「Profile_Log_Forwarding」を選択。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ① 「Policies」タブ > 「セキュリティ」 > 修正対象のポリシー名（名前欄）のリンクをクリックします。

名前	タグ	タイプ	送信元		宛先			
			ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	untrust	any	
test1	none	universal	Internal_WEST	10.96.128.0_24	any	any	Internal_SV_Critical	any
test2	none	universal	Internal_WEST	10.184.23.100_32	any	any	Internal_SV_Critical	any
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
interzone-default	none	interzone	any	any	any	any	any	any

図 7-2-1 URL フィルタリングポリシー修正

- ② 修正対象のタブをクリックし、修正後（手順は「7. 1. 3」、「7. 1. 4」を参照）、「OK」ボタンをクリックします。

図 7-2-2 URL フィルタリングポリシー修正

- ③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
(設定が反映されるまで 5 分程度かかることがあります)

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI



図 7-2-3 URL フィルタリングポリシー修正／設定反映

The screenshot shows a 'Commit' dialog box. It has a title bar 'コミット' with a close button. Below it, there's a message: 'コミットを実行すると実行中の設定がコミットスコープで上書きされます。' followed by two radio buttons: 'Commit すべての変更' (selected) and 'Commit 変更の実行者:(1) admin'. A table below shows the commit scope: 'policy-and-objects' (オブジェクトタイプ: Policy and Objects). At the bottom, there are three buttons: '変更内容の確認', '変更サマリー', and 'コミットの検証'. A note says '注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。' Below that is a text input field labeled '内容'. At the very bottom right, there are 'コミット' and 'キャンセル' buttons, with 'コミット' also highlighted with a red box.

図 7-2-4 URL フィルタリングポリシー修正／設定反映

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 7. 2. 1. 全制限端末（NB 端末）のアクセス解除／端末追加・削除

表 7-2-2 全制限端末（NB 端末）のアクセス解除／端末追加・削除

対象	対象 URL プロファイル
(23) 全制限端末（NB 端末）のアクセス解除 GUI による URL プロファイルカテゴリ登録方法記載	NB_PC
(24) 全制限端末（NB 端末）の端末追加・削除	NB_PC

### （23）全制限端末（NB 端末）のアクセス解除

#### GUI によるカスタムカテゴリ登録方法

① GUI より URL カテゴリ NB\_PC\_allow-list を選択し、URL を登録します。

以降の手順は、「7. 1. 2. 1. 全社アクセス解除/全社ブロック（1）－1」の手順と同様です。

### （24）GUI による端末追加（IP アドレス追加）方法

① 「Objects」 > 「アドレスグループ」 > NB\_PC をクリックします。

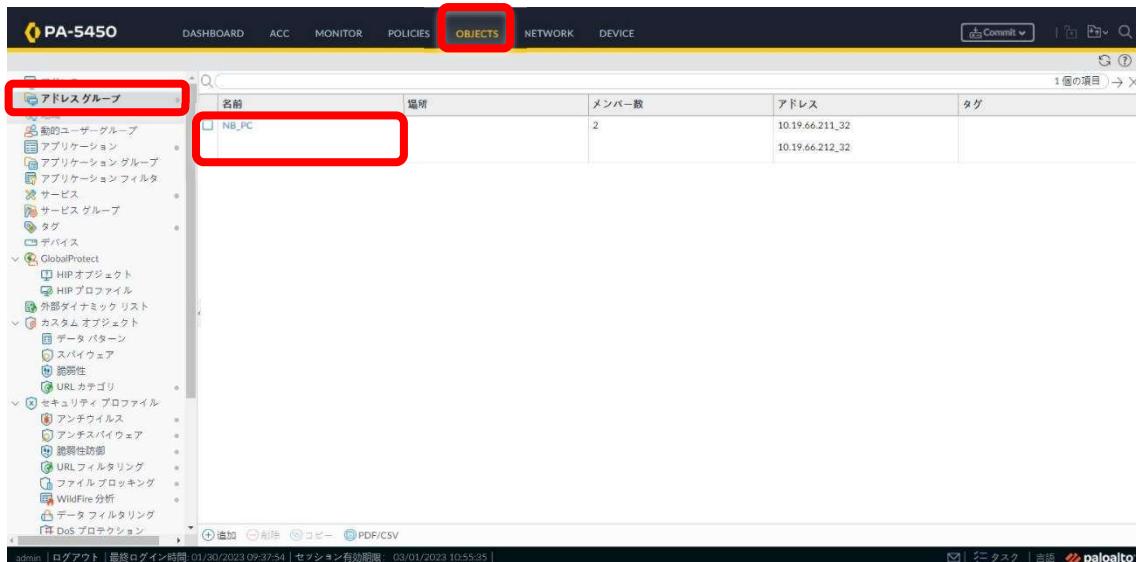


図 7-2-11 GUI による端末追加（IP アドレス追加）方法

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 「追加」 > 「アドレス」を選択します。

アドレスを作成（手順は7-1-5②を参照）

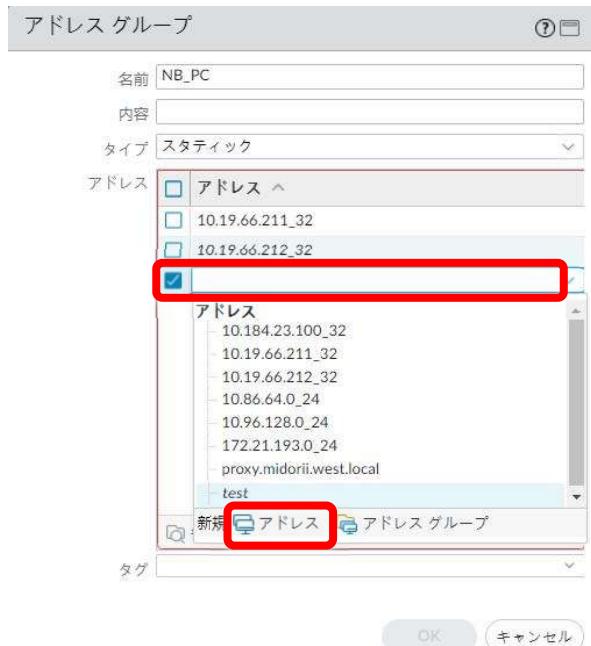


図 7-2-1-2 GUIによる端末追加（IPアドレス追加）方法



図 7-2-1-3 GUIによる端末追加（IPアドレス追加）方法

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

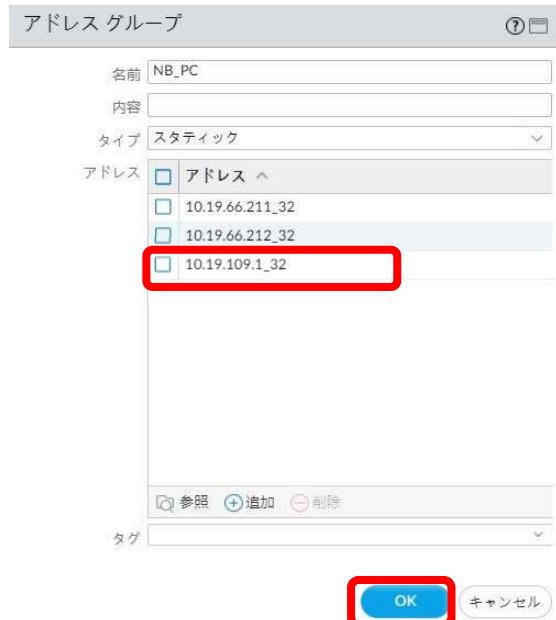


図 7－2－14 GUI による端末追加（IP アドレス追加）方法

※全制限端末として設定している「Web-Seigen」、「Intra-mart」の URL プロファイルの端末変更（IP アドレス追加/IP アドレス削除）も同様の手順です。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 7. 3. URL フィルタリングポリシー削除

URL フィルタリングポリシーの削除手順を記載します。

- 「Policies」タブ > 「セキュリティ」 > 対象のポリシーを選択後、「削除」ボタンをクリックします。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any
test1	none	universal	Internal_WEST	10.96.128.0-24	any	any	Internal_SV_Critical	any
test2	none	universal	Internal_WEST	10.184.23.100-32	any	any	Internal_SV_Critical	any
intrazone-default	none	intrazone	any	any	any	(Intrazone)	any	any
interzone-default	none	interzone	any	any	any	any	any	any

図 7-3-1 URL フィルタリングポリシー削除

- 「はい」ボタンをクリックします。



図 7-3-2 URL フィルタリングポリシー削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載  
 後、「コミット」ボタンをクリックします。（設定が反映されるまで5分程度かかることがあります）



図 7-3-3 URL フィルタリングポリシー削除

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

変更内容の確認 变更サマリー コミットの検証

注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容

**コミット** キャンセル

図 7-3-4 URL フィルタリングポリシー削除

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 8. URL フィルタリング機能 有効化/無効化

---

この項では、URL フィルタリング機能を有効化、無効化する手順を記載しています。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 8. 1. URL フィルタリング機能有効化

既存のセキュリティポリシーにて、URL フィルタリング機能を有効化する手順を記載します。

### 8. 1. 1. URL フィルタリング 有効化設定

- ① 「Policies」タブ > 「セキュリティ」 > 修正対象のポリシー名（名前欄）のリンクをクリックします。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any
test	none	universal	any	any	any	any	internal_WEST	any
test_URLFilter_ALL_Allow	none	universal	any	any	any	any	any	any
intrazone-default	none	intrazone	any	any	any	any	intrazone	any
interzone-default	none	interzone	any	any	any	any	any	any

図 8-1-1 PA-5450 URLfilter Policies Enable

表 8-1-1 URL フィルタリング有効化設定

図中番号	名前	利用用途
(1)	プロファイルタイプ	プルダウンより以下を選択 「Profiles」
	URL フィルタリング	プルダウンより「URL フィルタリング URL プロファイル」を選択

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 以下(1)を設定（「表 8-1-1」を参照）し、「OK ボタン」をクリックします。

セキュリティポリシールール

全般 | 送信元 | 宛先 | アプリケーション | サービス/URLカテゴリ | **アクション** | 用途

アクション設定

アクション Allow  
□ ICMP 送信到達不能

プロファイル設定

プロファイルタイプ **プロファイル (1)**  
アンチウイルス None  
脆弱性防御 None  
アンチスパイウェア None  
URL フィルタリング **test\_ALL\_Allow (1)**  
ファイルブロッキング None  
データフィルタリング None  
WildFire 分析 None

ログ設定

ログ転送 None  
□ セッション開始時にログ  
**□ セッション終了時にログ**  
ログ転送 None

その他の設定

スケジュール None  
QoS マーキング None  
□ サーバーレスポンス検査の無効化

OK キャンセル

図 8-1-2 PA-5450 URLfilter Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 8. 1. 2. 設定反映

- ① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。（設定が反映されるまで5分程度かかることがあります）



図 8-1-3 PA-5450 URLfilter Policies Enable

 This is a continuation of the previous screenshot, showing the 'Commit to Panorama' dialog. The 'Commit' button at the bottom right is highlighted with a red box. The rest of the interface, including the table and other buttons, remains the same.

図 8-1-4 PA-5450 URLfilter Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 8. 2. URL フィルタリング機能無効化

既存のセキュリティポリシーにて、URL フィルタリング機能を無効化する手順を記載します。

### 8. 2. 1. URL フィルタリング 無効設定

- ① 「Policies」タブ > 「セキュリティ」 > 修正対象のポリシー名（名前欄）のリンクをクリックします。

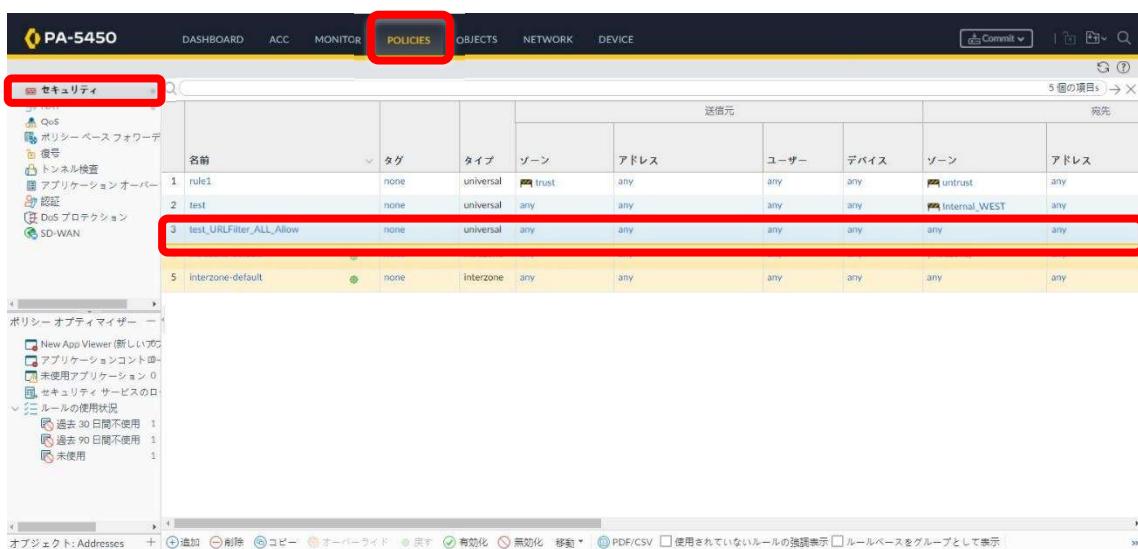


図 8-2-1 PA-5450 URLfilter Policies Disable

表 8-2-1 URL フィルタリング無効化設定

図中 番号	名前	利用用途
(1)	URL フィルタリング	プルダウンより以下を選択 「None」

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

② 以下(1)を設定（「表 8－2－1」を参照）し、「OK ボタン」をクリックします。

セキュリティポリシー ルール

全般 | 送信元 | 宛先 | アプリケーション | サービス/URL カテゴリ | **アクション**

アクション設定

アクション Allow  
□ ICMP 送信到達不能

プロファイル設定

プロファイルタイプ プロファイル  
アンチウイルス None  
脆弱性防御 None  
アンチスパイウェア None  
**URL フィルタリング None (1)**  
ファイルブロッキング None  
データフィルタリング None  
WildFire 分析 None

用途

ログ設定

□ セッション開始時にログ  
**✓ セッション終了時にログ**  
ログ転送 None

その他の設定

スケジュール None  
QoS マーキング None  
□ サーバレスポンス検査の無効化

**OK** キャンセル

図 8－2－2 PA-5450 URLfilter Policies Disable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 8. 2. 2. 設定反映

- ① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。

(設定が反映されるまで5分程度かかることがあります)



図 8－2－4 PA-5450 URLfilter Policies Disable

 A screenshot of a 'コミット' (Commit) dialog box. It contains a message: 'コミットを実行すると実行中の設定がコミットスコープで上書きされます。' followed by two radio buttons: 'Commit すべての変更' (selected) and 'Commit 変更の実行者: admin'. Below is a table with columns: 'コミットスコープ' (policy-and-objects), '場所タイプ' (Policy and Objects), 'オブジェクトタイプ' (Policy and Objects), 'エンティティ' (None), and '管理者' (None). At the bottom are buttons for '変更内容の確認' (Review changes), '変更サマリー' (Change summary), 'コミットの検証' (Commit verification), and '内容' (Content). A large red box highlights the 'コミット' (Commit) button at the bottom right.

図 8－2－5 PA-5450 URLfilter Policies Disable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 9. SSL 復号化設定

---

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

SSL 復号化のための復号化ポリシーの設定方式は以下の通りです。

### 1. SSL フォワードプロキシ方式

内部（サーバ、本社 NW、グループ会社 NW など）から外部（インターネット）方向の通信に適用します。

統合ファイアウォールはプロキシ（中間者）として SSL 通信を復号する動作となり、クライアントがウェブサイトに SSL ハンドシェイクをする際に、自己認証局もしくは他の認証局によって認証された証明書（鍵ペア）を利用します。

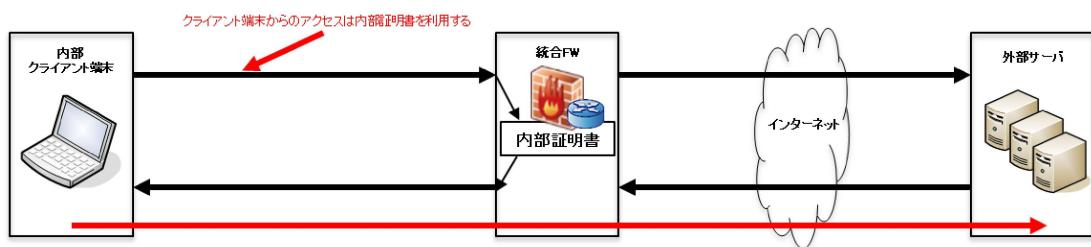


図 9-1 SSL 復号化フォワードプロキシ方式

### 2. SSL インバウンドインスペクション方式

外部（インターネット）から内部（DMZ サーバ）方向の通信に適用します。

SSL ハンドシェイクを密かに監視して SSL 通信を復号する動作となり、対象のサーバにて実際に利用している証明書（鍵ペア）を利用します。

この復号方式は、対象のサーバ証明書がコントロール配下で、統合ファイアウォールに証明書（鍵ペア）取り込むことができる前提で利用します。

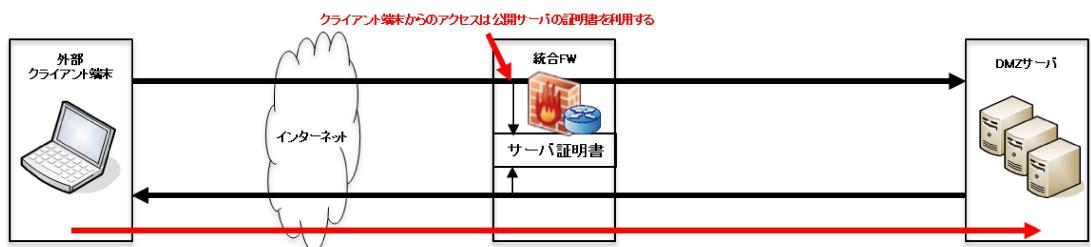


図 9-2 SSL 復号化インバウンドインスペクション方式

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 9. 1 SSL 復号化ポリシー追加/変更/削除

### 9. 1. 1. SSL 復号化ポリシー追加

ファイアウォールアドレスを作成後、SSL 復号化ポリシーを追加する手順を記載します。

※作成時にポリシーを選択していた場合には選択していたポリシーの下に作成されます。

※下記例として、G 会社の SSL 復号化ポリシーを作成します。

ポリシーの送信元/宛先ゾーンは各グループ会社 VR に所属しているゾーンを指定します。

詳細は本書の『0.5. VR のゾーン名一覧表』を参照してください。

### 9. 1. 2. ポリシー設定

① 「Policies」タブ > 「復号」> 「追加」ボタンをクリックします。

※ここではポリシー通信の一番手前の VR に SSL 復号化を行う。

名前	タグ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス	デバイス	URL カテゴリ	サービス	アクション
test1	none	any	any	any	any	any	any	any	any	any	no-decrypt
test_west-west	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any	no-decrypt
test2	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/32	any	test_category	any	no-decrypt

図 9 – 1 – 1 PA-5450 SSL Decryption Policies Add

表 9 – 1 – 1 SSL 復号化ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「SSL 復号化ポリシー名」を入力 (※) 文字数制限は 31 字迄 また、英数字、スペース、ハイフン (‘-’), アンダースコア (‘_’), ピリオド (‘.’) を名前に含めることができます
(2)	送信元	送信元ゾーン	「送信元ゾーン」を選択、登録したい対象を検索して、 プルダウンからその対象を選択

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

		※『0.5. VR のゾーン名一覧表』を参照	
(3)	送信元	送信元アドレス	登録したいアドレスを入力
(4)	宛先	宛先ゾーン ※『0.5. VR のゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択
(5)	宛先	宛先アドレス	登録したいアドレスを入力
(6)	サービス/ URL カテゴリ	URL カテゴリ	復号化対象となるカテゴリを選択
(7)	オプション	アクション	以下を選択 復号化あり：「復号」 復号化なし：「復号なし」
(8)	オプション	タイプ	プルダウンより以下を選択 「SSL フォワードプロキシ」 「SSL プロキシ」 「SSL インバウンドインスペクション」 ※クライアントが外部 Web サーバへアクセスするときの SSL 通信を復号化する場合は、「SSL フォワードプロキシ」を選択します。 ※外部 Web サーバから DMZ へアクセスする時の SSL 通信を復号化する場合は、「SSL インバウンドインスペクション」を選択します。
(9)	オプション	復号プロファイル	プルダウンより以下を選択 「Profile_Decryption」
(10)	全般	タグ	適用する VR 名を選択
(11)	オプション	証明書	SSL 証明書を選択

- ① 以下(1)～(8)を設定（「表 9－1－1」を参照）し、「OK」ボタンをクリックします。

復号ポリシールール

全般 | 送信元 | 宛先 | サービス/URL カテゴリ | オプション

名前	Dec_SHD_G_Trust_any_001
内容	(1)
タグ	
タグによるルール のグループ分け	None
監査コメント	
監査コメント アーカイブ	
OK キャンセル	

図 9－1－2 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

表 9—1—1 (2) 送信元ゾーンを入力します。



図 9—1—3 PA-5450 SSL Decryption Policies Add

表 9—1—1 (3) 送信元アドレスを入力します。

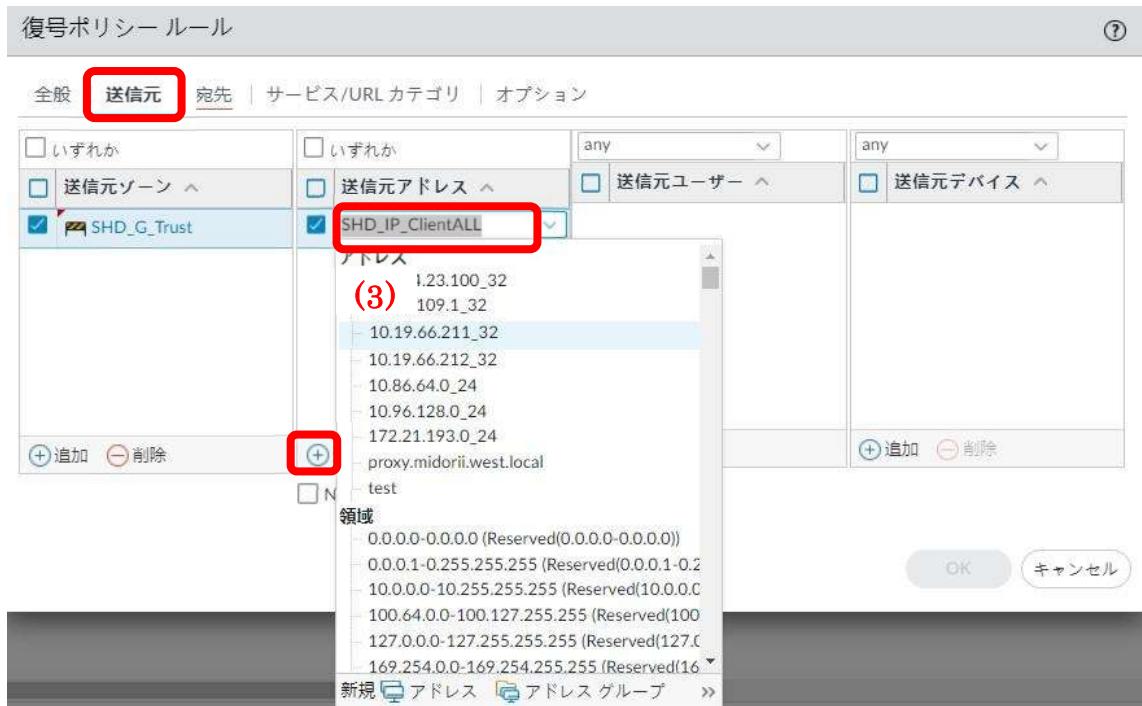


図 9—1—4 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

表 9—1—1 (4) 宛先ゾーンを入力します。

宛先ゾーンを指定する場合は「追加」をクリックします。

宛先ゾーンは any の場合は「いずれか」をクリックします。

※ここは「いずれか」をチェックが入れます。

復号ポリシー ルール

宛先

<input checked="" type="checkbox"/> いずれか	<input checked="" type="checkbox"/> いずれか	<input checked="" type="checkbox"/> いずれか	
<input type="checkbox"/> 宛先ゾーン ▾	<input type="checkbox"/> 宛先アドレス ▾	<input type="checkbox"/> 宛先デバイス ▾	
(4)			
<b>+ 追加</b>	<b>- 削除</b>	<b>+ 追加</b>	<b>- 削除</b>
<input type="checkbox"/> Negate			

OK キャンセル

図 9—1—5 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

表 9—1—1 (5)宛先アドレスを入力します。

宛先アドレスを指定する場合は「追加」をクリックします。

宛先アドレスはanyの場合は「いずれか」をクリックします。

※ここは「いずれか」をチェックが入れます。



図 9—1—6 PA-5450 SSL Decryption Policies Add

表 9—1—1 (6) URL カテゴリを入力します。

URL カテゴリを指定する場合は「追加」をクリックします。

URL カテゴリはanyの場合は「いずれか」をクリックします。

※ここは「いずれか」チェックが入れます。

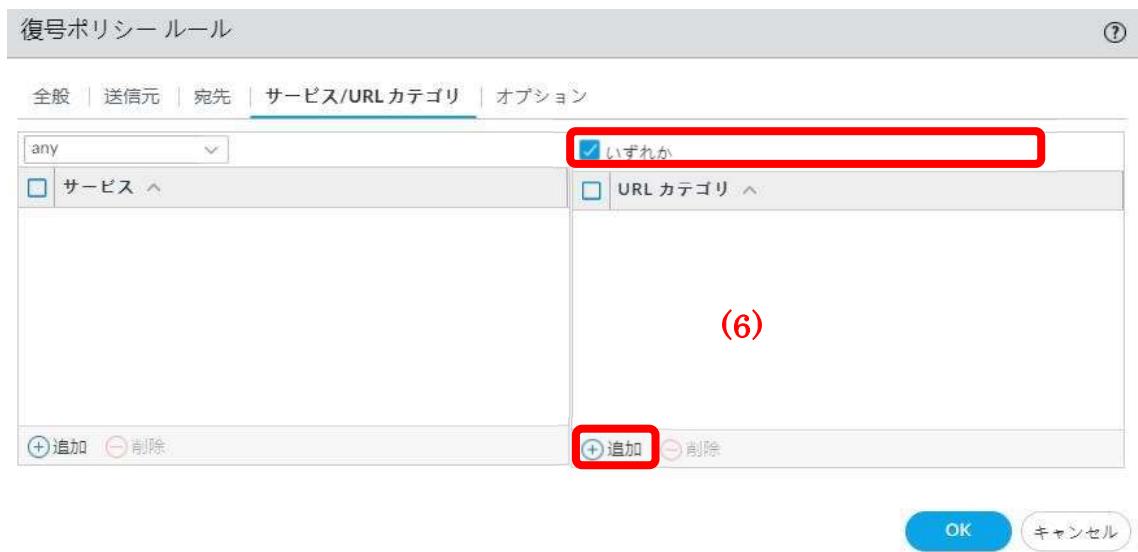


図 9—1—7 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

表9-1-1 (7) アクションを入力します。

表9-1-1 (8) タイプを入力します。

表9-1-1 (9) 復号プロファイルを入力します。

The screenshot shows the 'SSL Decryption Policies' configuration page. The 'Actions' dropdown is set to 'Decryption' (7), the 'Type' dropdown is set to 'SSL Forward Proxy' (8), and the 'Decryption Profile' dropdown is set to 'Profile\_Decryption' (9). The 'Logs' section contains two checkboxes: 'Successful SSL handshake logs to the log' (unchecked) and 'Failed SSL handshake logs to the log' (checked). The 'Log Transfer' dropdown is set to 'None'. At the bottom right are 'OK' and 'Cancel' buttons.

図9-1-8 PA-5450 SSL Decryption Policies Add

### 9. 1. 3. ポリシー移動

① 作成したポリシーを選択し、「移動」にて任意の位置へ移動します。

**※新規で作成したポリシーは最下位に作成されます。**

The screenshot shows the 'SSL Decryption Policies' list page. A context menu is open over the fourth policy row, with options: '↑ 最上部へ', '↑ 上へ', '↓ 下へ', and '↓ 最下部へ'. The policy table lists four entries: test1, test\_west-west, test2, and Dec\_SHD\_G\_Trust\_any\_001. The left sidebar shows security policies like NAT, QoS, and Application Overlays. The bottom navigation bar includes buttons for adding, deleting, copying, and committing changes.

図9-1-9 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

#### 9. 1. 4. 設定反映

① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載

後、「コミット」ボタンをクリックします。

（設定が反映されるまで5分程度かかることがあります）

The screenshot shows the 'PA-5450' interface with the 'DEVICE' tab selected. Under the 'POLICIES' section, there is a sub-menu for 'SSL Decryption Policies'. A new policy is being added, as indicated by the 'Add' button. The main area is titled 'コミット' (Commit) and contains a table for defining the policy scope. The table has columns: 'コミットスコープ' (Commit Scope), '場所タイプ' (Location Type), 'オブジェクトタイプ' (Object Type), 'エンティティ' (Entity), and '管理者' (Administrator). A single row is present with the values: 'policy-and-objects', 'Policy and Objects', 'Policy and Objects', 'admin', and an empty field. Below the table, there are three buttons: '変更内容の確認' (Change Content Confirmation), '変更サマリー' (Change Summary), and 'コミットの検証' (Commit Verification). A note below states: '注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。' (Note: All changes will be displayed in the domain accessible to the logged-in administrator). At the bottom, there is a large text input field labeled '内容' (Content) and two buttons: 'コミット' (Commit) and 'キャンセル' (Cancel), with the 'Commit' button also highlighted with a red box.

図 9-1-10 PA-5450 SSL Decryption Policies Add

ドキュメント名	運用手順書（セキュリティ機器）				最終更新日	最終更新者
ドキュメント ID	バージョン				2.0	2023/08/17 KDDI

## 9. 2 SSL 復号化ポリシー変更

SSL 復号化ポリシーの変更手順を記載します。

- ① 「Policies」タブ > 「復号」> 変更対象のポリシー名（名前欄）のリンクをクリックします。

※ここではポリシー通信の一番手前の VR に SSL 復号化を行う。

名前	タグ	送信元ゾーン	送信元アドレス	送信元ユーザー	送信元デバイス	宛先ゾーン	宛先アドレス	宛先デバイス	URL カテゴリ	サービス
test1	none	any	any	any	any	any	any	any	any	any
test_west-west	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any
test2	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any
Dec_SHD_G_Trust_any_001	none	SHD_G-Trust	SHD_IP_Cle...	any	any	any	any	any	any	any

図 9-2-1 PA-5450 SSL Decryption Policies Modify

- ② 変更対象のタブを押下し、変更後（手順は「9-1-1」を参照）、「OK」ボタンをクリックします。

図 9-2-2 PA-5450 SSL Decryption Policies Modify

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
 (設定が反映されるまで5分程度かかることがあります)



図 9－2－3 PA-5450 SSL Decryption Policies Modify

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

図 9－2－4 PA-5450 SSL Decryption Policies Modify

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 9. 3 SSL 復号化ポリシー削除

SSL 復号化ポリシーの削除手順を記載します。

- 「Policies」タブ > 「復号」> 対象のポリシーを選択後、「削除」ボタンをクリックします。

※ここではポリシー通信の一番手前の VR に SSL 復号化を行う。

名前	タグ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス	デバイス	URL カテゴリ	サービス	アクション
1. test1	none	any	any	any	any	any	any	any	any	any	no-decrypt
2. test-west-west	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any	decrypt

図 9-3-1 PA-5450 SSL Decryption Policies Delete

- 「はい」ボタンをクリックします。



図 9-3-2 PA-5450 SSL Decryption Policies Delete

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。  
 (設定が反映されるまで5分程度かかることがあります)



図 9－3－3 PA-5450 SSL Decryption Policies Delete



図 9－3－4 PA-5450 SSL Decryption Policies Delete

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 10. SSL 復号化ポリシー 有効化/無効化

この項では、SSL 復号化ポリシーの有効化方法及び無効化の方法について記載しています。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 10.1. SSL 復号化ポリシー 有効化

既存の SSL 復号化ポリシー（アクションが復号なし設定状態）にて、SSL 復号化ポリシーを有効化する手順を記載します。

### 10.1.1. SSL 復号化ポリシー 有効設定

- ① 「Policies」タブ > 「復号」>修正対象のポリシーネーム（名前欄）のリンクをクリックします。

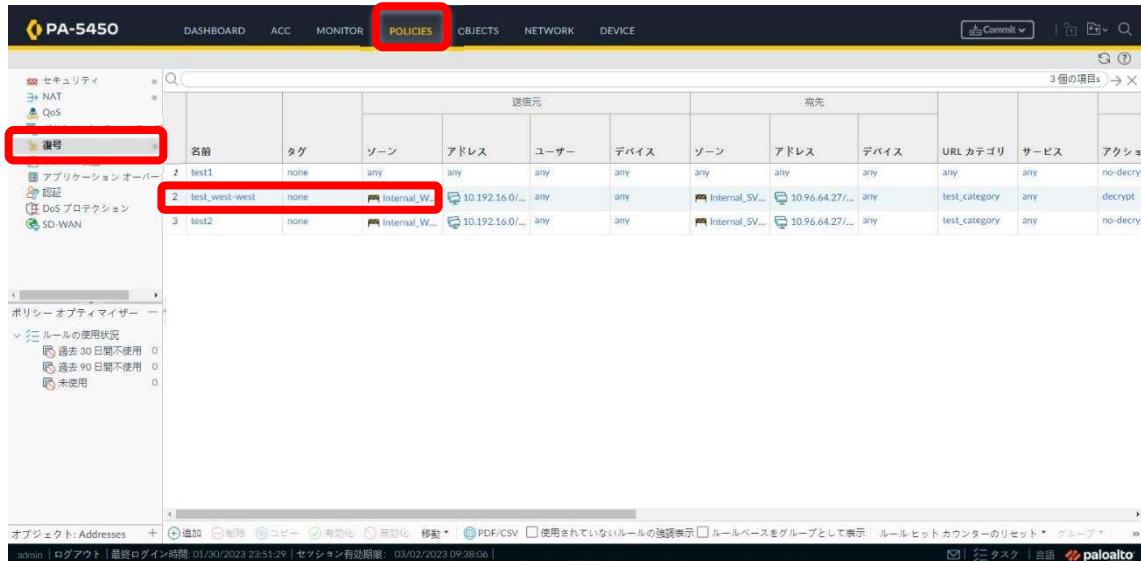


図 10-1-1 PA-5450 SSL Decryption Policies Enable

表 10-1-1 SSL 復号化ポリシー設定

図中番号	名前	利用用途
(1)	アクション	以下を選択 「復号しない」から「復号」へ変更
(2)	タイプ	プルダウンより以下を選択 「SSL フォワードプロキシ」 ※クライアントが外部 Web サーバへアクセスするときの SSL 通信を復号化するため、この方式を選択します。
(3)	復号プロファイル	プルダウンより以下を選択 「Profile_Decryption」

- ② 以下 (1) ~ (3) を設定（「表 10-1-1」を参照）し、「OK」ボタンをクリックします。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

復号ポリシールール

①

全般	送信元	宛先	サービス/URL カテゴリ	オプション
アクション	<input type="radio"/> 復号なし	<input checked="" type="radio"/> 復号	(1)	
タイプ	SSL フォワード プロキシ			(2)
復号プロファイル	Profile_Decryption			(3)
ログ設定	<input type="checkbox"/> 成功した SSL バンドシェイクをログに記録 <input checked="" type="checkbox"/> 失敗した SSL バンドシェイクをログに記録 ログ転送 <input type="button" value="None"/>			
	<input type="button" value="OK"/> <input type="button" value="キャンセル"/>			

図 10-1-2 PA-5450 SSL Decryption Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 10.1.2. 設定反映

- ① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載  
後、「コミット」ボタンをクリックします。  
(設定が反映されるまで5分程度かかることがあります)



図10-1-3 PA-5450 URLfilter Policies Enable

コミット

コミットを実行すると実行中の設定がコミットスコープで上書きされます。

Commit すべての変更  Commit 変更の実行者: admin

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

変更内容の確認 变更サマリー コミットの検証

注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。

内容:

**コミット** キャンセル

図10-1-4 PA-5450 URLfilter Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 10.2. SSL 復号化ポリシー 無効化

既存の SSL 復号化ポリシー（アクションが復号設定状態）にて、SSL 復号化ポリシーを無効化する手順を記載します。

### 10.2.1. SSL 復号化ポリシー 無効設定

- ① 「Policies」タブ > 「復号」 > 修正対象のポリシーネーム（名前欄）のリンクをクリックします。

名前	タグ	ソーン	アドレス	ユーザー	デバイス	ソーン	アドレス	デバイス	URL カテゴリ	サービス	アクション
1 test1	none	any	any	any	any	any	any	any	any	any	no-decrypt
2 test_west-west	none	Internal_W...	10.192.16.0/...	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any	decrypt

図 10-2-1 PA-5450 SSL Decryption Policies Enable

表 10-2-1 SSL 復号化ポリシー設定

図中番号	名前	利用用途
(1)	アクション	以下を選択 「復号」から「復号しない」へ変更
(2)	復号プロファイル	プルダウンより以下を選択 「None」

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

- ③ 以下(1)～(2)を設定（「表 10—2—1」を参照）し、「OK」ボタンをクリックします。

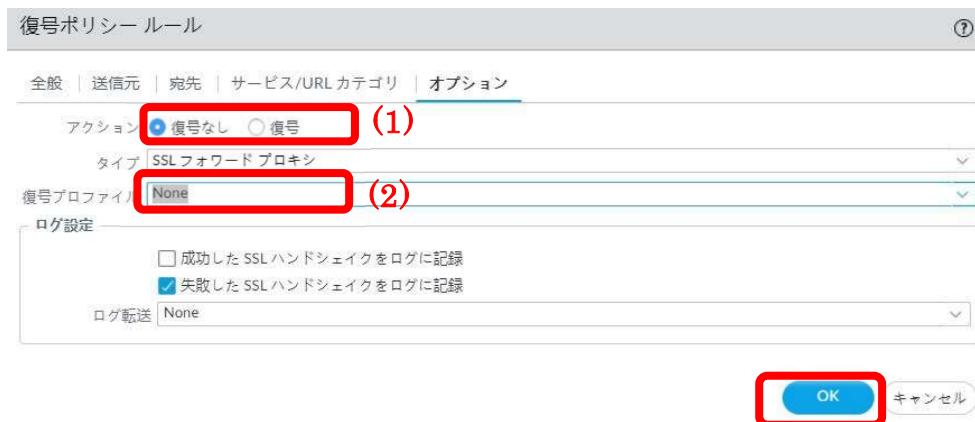


図 12—2—2 PA-5450 SSL Decryption Policies Disable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 10.2.2. 設定反映

- ① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載  
後、「コミット」ボタンをクリックします。（設定が反映されるまで5分程度かかることがあります）

The screenshot shows the PA-5450 configuration interface. The top navigation bar includes 'PA-5450', 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', 'DEVICE', and a 'Commit' button. Below the navigation is a breadcrumb trail: 'セットアップ' > '操作' > 'URLfilter Policies Enable'. The main area is titled 'コミット' (Commit) and contains a note: 'コミットを実行すると実行中の設定がコミットスコープで上書きされます。' (Executing commit will overwrite the current settings in the commit scope). It shows two radio buttons: 'Commitすべての変更' (Commit all changes) and 'Commit変更の実行者:(1) admin'. A table lists a single entry: 'policy-and-objects' with 'Policy and Objects' selected under 'オブジェクトタイプ'. At the bottom are buttons for '変更内容の確認' (Review changes), '変更サマリー' (Change summary), and 'コミットの検証' (Commit verification). A note states: '注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。' (Note: All changes will be displayed in the domain accessible to the logged-in administrator). A large text input field labeled '内容' (Content) is present. The 'Commit' button at the bottom right is highlighted with a red rectangle.

図10-2-3 PA-5450 URLfilter Policies Enable

This screenshot shows the same 'コミット' (Commit) screen as the previous one, but with a larger view of the content area. It includes the note about overwriting settings, the commit scope selection, the table with the single policy entry, and the bottom buttons for review, summary, and verification. The 'Commit' button at the bottom right is again highlighted with a red rectangle.

図10-2-4 PA-5450 URLfilter Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 10.3. 設定例) G 会社の SSL 復号化ポリシー 有効化

G 会社の SSL 復号化ポリシーにて、SSL 復号化ポリシーを有効化する手順を記載します。

#### 10.3.1. G 会社の SSL 復号化ポリシー 有効設定

- ① 「Policies」タブ > 「復号」 > 修正対象のポリシー名（名前欄）のリンクをクリックします。本体と G 会社の場合で修正対象のポリシーが異なります。

名前	タグ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス	デバイス	URL カテゴリ	サービス
test1	none	any	any	any	any	any	any	any	any	any
test_west-west	none	Internal_W...	10.192.16.0/21	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any
test2	none	Internal_W...	10.192.16.0/21	any	any	Internal_SV...	10.96.64.27/...	any	test_category	any
NoDec_SHD_G_Trust_any_001	none	SHD_G-True	SHD_IP_ClientALL	any	any	any	any	any	test_NoDec_U...	any
Dec_SHD_G_Trust_any_001	none	SHD_G-True	SHD_IP_ClientALL	any	any	any	any	any	any	any

図 10-3-1 PA-5450 SSL Decryption Policies Enable

表 10-3-1 SSL 復号化ポリシー設定

図中番号	名前	利用用途
(1)	アクション	以下を選択 「復号しない」から「復号」へ変更
(2)	タイプ	プルダウンより以下を選択 「SSL フォワードプロキシ」 ※クライアントが外部 Web サーバへアクセスするときの SSL 通信を復号化するため、この方式を選択します。
(3)	復号プロファイル	プルダウンより以下を選択 「Profile_Decryption」

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

④ 「オプション」タブを選択し図中（1）～（3）を設定します。



図 10-3-2 PA-5450 SSL Decryption Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

### 10.3.2. 設定反映

- ① 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載  
後、「コミット」ボタンをクリックします。  
(設定が反映されるまで5分程度かかることがあります)

コミットスコープ	場所タイプ	オブジェクトタイプ	エンティティ	管理者
policy-and-objects	Policy and Objects			

図10-3-3 PA-5450 URLfilter Policies Enable

コミット キャンセル

図10-3-4 PA-5450 URLfilter Policies Enable

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

## 1.1. SSL フォワードプロキシ除外設定

この項では、SSL 復号化ポリシーの有効化方法及び無効化の方法について記載しています。

SSL フォワードプロキシ（アウトバウンド SSL 復号）における、各通信方向に適用する SSL 復号ポリシーの設計は以下の通りです。  
SSL 復号化除外設定の追加は、以下の優先順序で検討します。

1. SSL 復号除外 URL カテゴリを指定して、SSL 復号から除外する。
2. カスタム URL カテゴリ（NoDec\_URL\_List）に復号除外する URL を登録し、SSL 復号から除外する。  
手順は「1.1. 1. 4」を参照。
- 3.宛先 IP アドレスグループ（Group\_NoDec\_Dst）に復号除外するアドレスを登録し、SSL 復号から除外する。  
手順は「1.1. 1. 6」を参照。
- 4.送信元 IP アドレスグループ（Group\_NoDec\_Src）に復号除外するアドレスを登録し、SSL 復号から除外する。  
手順は「1.1. 1. 8」を参照。
- 5.サービスグループ（Group\_NoDec\_Service）に復号除外するサービスを登録する。  
手順は「1.1. 1. 10」を参照。
6. 1～5以外の通信は全て復号化する。

※一番手前の VR にて SSL 復号化を行います。2～5 のカスタム URL カテゴリおよびアドレスグループ、サービスグループは全 VR で共通とします。