

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

1.1.1.1. SSL 復号化除外対象の確認方法

SSL復号によって正常なWebアクセス通信ができない場合がある。

ファイアウォールポリシー、URL フィルタリングポリシー、脅威防御機能（脆弱性防御、アンチスパイウェア、アンチウイルス）によってブロックされていないにも関わらず、Web アクセス通信ができない場合、対象通信について SSL 復号化除外を行い事象が改善するかを確認する。

本手順は、SSL 復号化除外対象をログから特定する方法を記載する。

① 対象特定に必要な情報の確認

Web アクセス不可以以下の情報を確認する

- ・通信不可の発生日時（不明な場合は再度実施いただき日時を連絡いただく）
- ・接続元端末の IP アドレス
- ・接続できなかつた宛先 URL
- ・接続できなかつた宛先の概要（○○のアプリケーションサイトなど）
- ・接続できなかつたときの状況（可能であればブラウザの画面キャプチャを取得）

例)

- ブロック画面が表示された
- ブラウザの警告画面（信頼できない等）が表示された
- 読み込み中のまま進まない（タイムアウトして接続できなかつた等が表示）

② SSL 復号エラーから除外対象 URL を確認する

(ア) ログ管理サーバにログインし、「Monitor」タブ > 「トラフィック」を選択

(イ) 検索バーに以下内容を入力し、該当する通信がないかを確認する

フィルタ内容：

(session end reason eq decrypt-error) and (addr. src in 10.87.96.63)

※ 「addr. src in “①で確認した送信元 IP”」で入力してください

ここでは例として送信元 IP 「10.87.96.63」を指定しています。

(ウ) 検索の結果、ログが表示された場合は “①で確認した通信不可の発生日時”に近い時間のトラフィックログについて、詳細（ログエントリの最左にある「」）をクリック。

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 1 1 – 1 – 1 SSL 復号化除外対象の確認

(エ) 詳細ログビューにて、「送信元」、「URL」を確認する

図 1 1 – 1 – 2 SSL 復号化除外対象の確認

(オ) 確認した「URL」の FQDN を復号化除外用 URL に追加する

※追加手順は、「1 1. 1. 4 SSL 復号化除外用 URL の追加」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

③ 接続先 URL 情報から復号化除外対象 URL を確認する

「②SSL 復号エラーから除外対象 URL を確認する」で対象が確認できない、または除外対象を追加したが、Web アクセス通信ができない状況が改善しない場合、URL フィルタリングログから対象を特定する。

(ア) ログ管理サーバにログインし、「Monitor」タブ > 「URL フィルタリング」を選択

(イ) 検索バーに以下内容を入力し、該当する通信がないかを確認する

フィルタ内容：

(addr. src in 10.87.96.63)

※ 「addr. src in “①で確認した送信元 IP”」で入力してください

ここでは例として送信元 IP 「10.87.96.63」を指定しています。

発生日時	カテゴリ	操作	URL	対象ゾーン	状態	操作メニュー
09/13 09:48:21	WindowsUpdate	no	internetwork	WIT_G_Trust	10.87.96.63	... 10.192.2.202
09/13 09:48:12	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:48:14	WindowsUpdate	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:48:13	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:48:12	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:48:00	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:50	WindowsUpdate	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:55	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:49	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:40	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:36	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:30	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:24	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:13	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:11	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:09	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:47:02	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:57	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:56	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:50	WindowsUpdate	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:51	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:46	DefaultGroup_Allow	yes	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:40	DefaultGroup_Allow	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202
09/13 09:46:36	WindowsUpdate	no	internetwork	WIT_G_Trust	10.87.96.63	10.192.2.202

図 1-1-1-3 SSL 復号化除外対象の確認

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

(ウ)検索の結果から”①で確認した通信不可の発生日時”に近い時間の URL フィルタリングログについて、復号化の項目が“YES”であるログの「URL」を確認する。

※ 対象の URL について「①で確認した“接続できなかった宛先 URL”、“接続できなかった宛先の概要”」と明らかに無関係と思われる URL は除外すること

(エ)確認した「URL」の FQDN を復号化除外用 URL に追加する

※ 追加手順は、「1.1.1.4 SSL 復号化除外用 URL の追加」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

④ 接続先 IP 情報から復号化除外対象の宛先 IP を確認する

「③接続先 URL 情報から除外対象 URL を確認する」で対象が確認できない、または除外対象を追加したが、Web アクセス通信ができない状況が改善しない場合、トラフィックログの宛先 IP から対象を特定する。

※ 本手順についてはプロキシ経由の通信には適用できない。プロキシ経由の通信の場合は宛先 URL または送信元 IP アドレスでの除外指定となる

(ア) ログ管理サーバにログインし、「Monitor」タブ > 「トラフィック」を選択

(イ) 検索バーに以下内容を入力し、該当する通信がないかを確認する

フィルタ内容 :

(addr. src in 10.87.96.63)

※ 「addr. src in “①で確認した送信元 IP”」で入力してください

ここでは例として送信元 IP 「10.87.96.63」を指定しています。

送達したパケット数	受け取ったパケット数	発生日時	前回時間	タイプ	認可化	URL カテゴリ	送達先 IP アドレス	両者リンク	送信元ユーザー	送信元 IP アドレス	送信元 NAT ポート	送信元 HAT ポート	送信先 NAT ポート	送信先 HAT ポート	両方とも NAT ポート	両方とも HAT ポート
3	1	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43971	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	57177	0	0			8.8.8.8	
10	10	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	private-ip-address	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43973	0	0			10.192.2.202	
10	10	2023/09/22 09:50:23	2023/09/13 09:50:23	rnd	no	private-ip-address	internal_WEST	internal_SV_VIP	10.87.96.63	43971	0	0			10.192.201.114	
3	1	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	WindowsUpdate	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43970	0	0			10.192.2.202	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	58118	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	58118	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0	2023/09/22 09:50:23	2023/09/13 09:50:23	drop	no	any	WIT_G_Trust	WIT_G_Untrust	10.87.96.63	43969	0	0			8.8.8.8	
1	0															

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 接続元 IP 情報から復号化除外対象の送信元 IP を確認する

「④接続先 IP 情報から復号化除外対象の宛先 IP を確認する」で対象が確認できない、または除外対象を追加したが、Web アクセス通信ができない状況が改善しない場合、送信元 IP で除外を行う。

※ 送信元 IP で除外を行った場合、該当ホストからの通信は全て復号化除外となる。このため、実施時は必要性とリスクを確認の上で実施すること。

(ア) 「“①で確認した送信元 IP”」の IP アドレスを復号化除外用送信元アドレスに追加する

※ 追加手順は、「1.1.1.8 SSL 復号化除外用送信元アドレスの追加」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

2. URL を除外用の URL カテゴリグループに追加する。

- ① 統合 FW にログインし、「Objects」タブ > 「URL カテゴリ」から『NoDec_URL_List』を選択し、カスタム URL カテゴリ編集画面に遷移します。

※ 『NoDec_URL_List』は URL 除外専用カスタム URL カテゴリ

The screenshot shows the 'OBJECTS' tab selected in the top navigation bar. On the left, the 'URL カテゴリ' (Custom Categories) section is expanded, and the 'カスタム URL リスト' (Custom URL List) item is selected. A search bar at the top right contains the text 'NoDec'. The main pane displays a table titled 'URL リスト' with one entry: 'NoDec_URL_List'. The table columns are '名前' (Name), '場所' (Location), and 'タイプ' (Type). The '場所' column shows a path starting with 'w-neoco-groups.macsms.jp'. The 'タイプ' column shows '→ 路' (Path). Below the table, there is a list of URLs: 'west-kouki.jp', '*west-kouki.jp', '*fm777.co.jp', 'fm777.co.jp', 'blztn.bk.mutg.jp', and '*obc-service.biz'. A red box highlights the 'NoDec_URL_List' entry in the table.

図 1-1-1-6 SSL 復号化除外用カスタム URL カテゴリ

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 > 手順②で確認した URL を追加 > 「OK」をクリックします。

カスタム URL カテゴリ

名前 NoDec_URL_List
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	内容
.100777.co.jp	
fm777.co.jp	
biztn.bk.mufg.jp	
*.obc-service.biz	
obc-service.biz	
*.obc.jp	
obc.jp	

10 個の項目s → X

+ 追加 削除 インポート エクスポート

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 1 1 – 1 – 7 SSL 復号化除外対象の確認

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 1 1 - 1 - 8 設定変更のコミット

The screenshot shows a 'Commit' confirmation dialog. It displays a table with one row, indicating a commit scope of 'policy-and-objects' with a 'Policy and Objects' type. Below the table, there are tabs for '変更内容の確認', '変更サマリー', and 'コミットの検証'. 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。' At the bottom, there is a text input field labeled '内容' and two buttons: 'コミット' (highlighted with a red box) and 'キャンセル'.

図 1 1 - 1 - 9 コミット内容確認

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

11.1.2. SSL 復号化除外用 URL カテゴリの追加

※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。

① 「Policies」タブ > 「復号」> 対象除外用ポリシーの「名前」をクリックします。

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
37 WEST	none	Internet, WEST	10.0.0.0/8	any	any	Internet, SV,...	10.19.132.17/32	any	entertainment-and-arts	TCP_B
38 NoDec_Internet_WE...	none	Internet, WEST	Group, NDICOGroupALL	any	any	any	10.19.132.18/32	any	unknown	
39 NoDec_Internet_WE...	none	Internet, WEST	Group, Internet_SV_ALL	any	any	any	10.19.132.27/32	any		
40 NoDec_Internet_WE...	none	Internet, WEST	any	any	any	any	any	any	financial-services	any
41 NoDec_Internet_WE...	none	Internet, WEST	any	any	any	any	any	any	government	any
42 NoDec_Internet_WE...	none	Internet, WEST	Group, NDICOGrou...	any	any	any	any	any	health-and-medicine	any
43 NoDec_Internet_WEST...	none	Internet, WEST	any	any	any	any	any	any	NoDec_URL_List	
44 NoDec_Internet_DMZ...	none	Internet, DMZ	Group, DMZ_ALL	any	any	any	any	any	financial-services	any
45 NoDec_Internet_DMZ...	none	Internet, DMZ	Group, DMZ_ALL	any	any	any	Group, NDICOGrou...	any	government	any
46 NoDec_Internet_DMZ...	none	Internet, DMZ	Group, NDICOGrou...	any	any	any	any	any	health-and-medicine	any
47 Dec_Internet_DMZ...	none	Internet, DMZ	Group, DMZ_ALL	any	any	any	any	any	NoDec_URL_List	

図 11-1-10 SSL 復号化除外用 URL カテゴリの追加

② 「サービス/URL カテゴリ」タブ > 「URL カテゴリ」項目 > 「追加」をクリックします。

サービス	URL カテゴリ
any	金融・サービス 政府 医療・保健 NoDec_URL_List

図 11-1-11 SSL 復号化除外用 URL カテゴリの追加

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 「URL カテゴリ」を選択 > 「OK ボタン」をクリックします。

※ここは例として「ALL_Allow」を選択

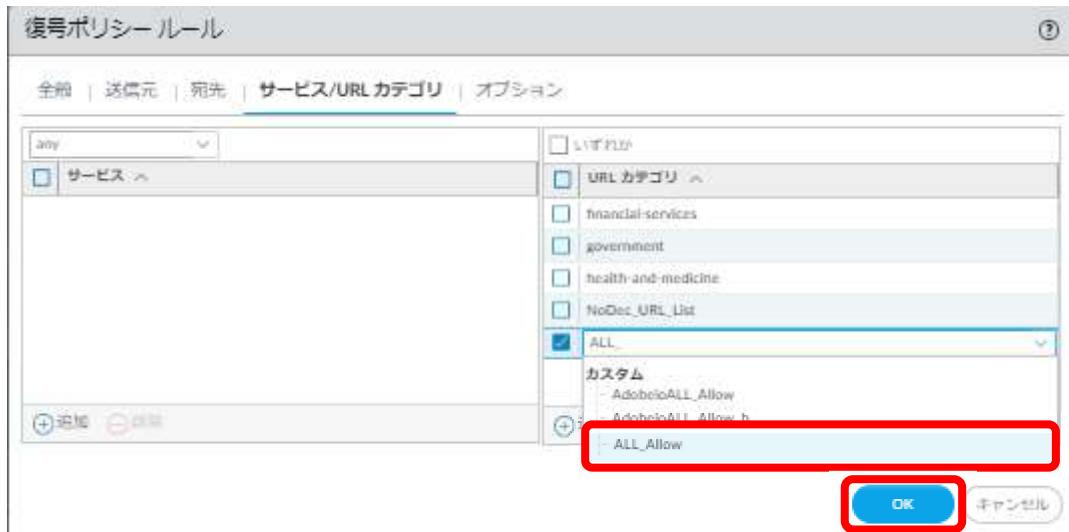


図 1 1 – 1 – 1 2 SSL 復号化除外用 URL カテゴリの追加

④ 対象ポリシーの URL カテゴリ項目内に追加した URL カテゴリが存在していること確認します。

図 1 1 – 1 – 1 3 SSL 復号化除外用 URL カテゴリの追加

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）

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 1 1 – 1 – 1 4 SSL 復号化除外用 URL カテゴリの追加

The screenshot shows a 'Commit' dialog box. At the top, it says 'コミット' and has a help icon and a close button. Below that, it says '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。' and shows two radio buttons: 'Commit すべての変更' (selected) and 'Commit 変更の実行者(1) admin'. The main table has four columns: 'コミットスコープ', '場所タイプ', 'オブジェクトタイプ', and 'エンティティ' (empty). A row is selected with the value 'policy-and-objects' under 'Policy and Objects'. At the bottom, there are three links: '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 '内容' input field. At the very bottom right, there are 'コミット' and 'キャンセル' buttons, with 'コミット' highlighted with a red box.

図 1 1 – 1 – 1 5 SSL 復号化除外用 URL カテゴリの追加

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

1.1.1.3. SSL 復号化除外用 URL カテゴリの削除

- ① 「Policies」タブ > 「復号」> 対象除外用ポリシーの「名前」をクリックします。

The screenshot shows the Palo Alto Networks PA-5450 interface. The top navigation bar has tabs: DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box), OBJECTS, NETWORK, and DEVICE. Below the navigation is a search bar and a toolbar with icons for Commit, Undo, Redo, and Refresh. The main area is titled 'セキュリティ' (Security) and contains sections for NAT, QoS, Firewall, Application Optimizer, and SD-WAN. Under 'セキュリティ', there's a '復号' (Decryption) section. A table lists various policies, with one row for 'ALL_Allow' highlighted by a red box. The table columns include: 名前 (Name), タグ (Tag), ゾーン (Zone), アドレス (Address), ユーザー (User), デバイス (Device), ゾーン (Zone), アドレス (Address), デバイス (Device), URL カテゴリ (URL Category), and サービス (Service). The 'ALL_Allow' policy is categorized under 'financial-services', 'government', 'health-and-medicine', and 'NoDec_URL_List'.

図 1.1-1-1-6 SSL 復号化除外用 URL カテゴリの削除

- ② 「サービス/URL カテゴリ」タブ > 「URL カテゴリ」項目 > 削除対象の「URL カテゴリ」を選択し、「削除ボタン」をクリックします。

The screenshot shows the 'Decryption Policy Rule' configuration screen. At the top, there are tabs: 全般 (General), 送信元 (Source), 宛先 (Destination), and サービス/URL カテゴリ (Services/URL Categories) (which is highlighted with a red box). On the left, there's a list of services. On the right, there's a list of URL categories. The 'ALL_Allow' category is selected and highlighted with a red box. At the bottom right of the list, there's a 'Delete' button (highlighted with a red box). Below the list, there are 'OK' and 'キャンセル' (Cancel) buttons, with 'OK' also highlighted with a red box.

図 1.1-1-1-7 SSL 復号化除外用 URL カテゴリの削除

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 対象ポリシーの URL カテゴリ項目内に削除したこと確認します。

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
37 WEST	none	Internet_WEST	10.0.0.0/8	any	any	Internet_SV...	10.19.132.17/32	any	entertainment-and-arts	TCP, S...
38 NoDec_Internet_WE...	none	Internet_WEST	Group_NIDCOGroupAll	any	any	any	any	any	unknown	any
39 NoDec_Internet_WE...	none	Internet_WEST	Group_Internet_SV_All	any	any	any	any	any	any	any
40 NoDec_Internet_WE...	none	Internet_WEST	any	any	any	any	any	any	any	any
41 NoDec_Internet_WE...	none	Internet_WEST	any	any	any	Group_NoDec_Dst	any	any	any	any
42 NoDec_Internet_WE...	none	Internet_WEST	Group_NoDec_Src	any	any	any	any	any	any	any
43 Dec_Internet_WEST...	none	Internet_WEST	any	any	any	any	any	any	any	any
44 NoDec_Internet_DMZ	none	Internet_DMZ	Group_DMZ_All	any	any	any	any	any	financial-services	any
45 NoDec_Internet_DMZ...	none	Internet_DMZ	Group_DMZ_All	any	any	any	Group_NoDec_Dst	any	any	any
46 NoDec_Internet_DMZ...	none	Internet_DMZ	Group_NoDec_Src	any	any	any	any	any	any	any
47 Dec_Internet_DMZ...	none	Internet_DMZ	Group_DMZ_All	any	any	any	any	any	any	any

図 11-1-18 SSL 復号化除外用 URL カテゴリの削除

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 11-1-19 SSL 復号化除外用 URL カテゴリの削除

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 11-1-20 SSL 復号化除外用 URL カテゴリの削除

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

1.1.1.4. SSL 復号化除外用 URL の追加

- ① 「Policies」タブ > 「復号」> 対象除外用ポリシーの URL カテゴリを確認します。

※ここでは例として「NoDec_URL_List」となります。

名前	タグ	ソース	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
WEST	none	Internet, WEST	10.0.0.8	any	any	Internal, SV...	10.19.132.17/32	any	entertainment-and-arts	TCP_B
38 NoDec_Internet_WEST...	none	Internet, WEST	Group_NDCCGroupALL	any	any	any	10.19.132.18/32	any	unknown	
39 NoDec_Internet_WEST...	none	Internet, WEST	Group_Internal_SV_ALL	any	any	any	10.19.132.27/32	any	any	
40 NoDec_Internet_WEST...	none	Internet, WEST	any	any	any	any	any	any	All_Access	any
41 NoDec_Internet_WEST...	none	Internet, WEST	any	any	any	any	any	any	financial-services	
42 NoDec_Internet_WEST...	none	Internet, WEST	Group_NoDec_Src	any	any	any	any	any	government	
43 Dec_Internet_WEST...	none	Internet, WEST	any	any	any	any	any	any	health-and-medicine	
44 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_DMZ_ALL	any	any	any	any	any	NoDec_URL_List	
45 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_DMZ_All	any	any	any	any	any	any	
46 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_NoDec_Src	any	any	any	any	any	any	

図 1.1.1.4. SSL 復号化除外用 URL の追加

- ② 「Objects」タブ > 「URL カテゴリ」> フィルタに「NoDec_URL_List」を入力して、右側の「→」ボタンをクリックし、検索します。

名前	場所	タイプ
NoDec_URL_List		URLリスト

図 1.1.1.4. SSL 復号化除外用 URL の追加

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 「NoDec_URL_List」 の名前をクリックします。

The screenshot shows the Palo Alto Networks PA-5450 interface. The left sidebar contains navigation links such as DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (which is selected), NETWORK, and DEVICE. The main pane displays a table titled 'NoDec_URL_List' with columns: 場所 (Location), タイプ (Type), and -R (Rule). There is one entry: 'w-nexco-group.mazero.jp'. A red box highlights the table header and the first row. The bottom status bar shows 'ログイン | 前回ログイン時間: 06/12/2023 16:05:29 | セッション有効期限: 07/12/2023 16:59:59'.

図 1-1-2-3 SSL 復号化除外用 URL の追加

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 「追加」をクリックし、除外したい「URL」を入力します。

※ここでは例として、「www.TEST.com」を入力します。

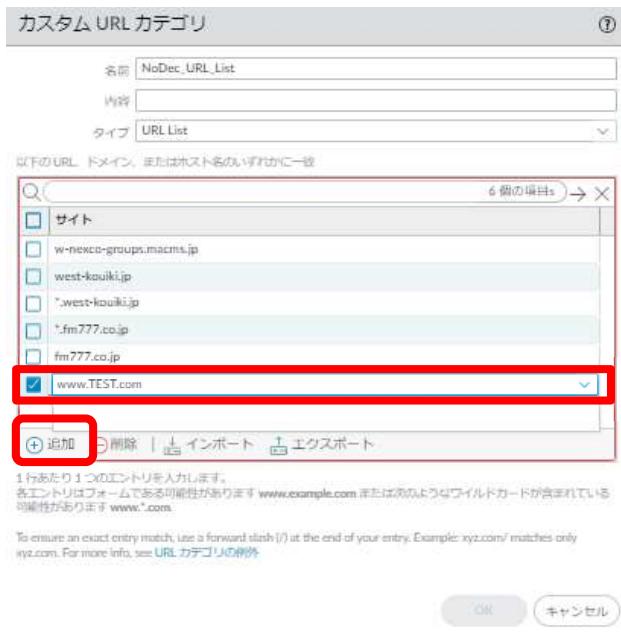


図 1 1 – 1 – 2 4 SSL 復号化除外用 URL の追加

※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

- ⑤ 「OK ボタン」をクリックします。



図 1 1 – 1 – 2 5 SSL 復号化除外用 URL の追加

- ⑥ 「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 1 1 – 1 – 2 6 SSL 復号化除外用 URL カテゴリの追加



図 1 1 – 1 – 2 7 SSL 復号化除外用 URL カテゴリの追加

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

1.1.1.5. SSL 復号化除外用 URL の削除

- ① 「Policies」タブ > 「復号」> 対象除外用ポリシーの URL カテゴリを確認します。

※ここでは例として「NoDec_URL_List」となります。

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
WEST	none	Internet, WEST	10.0.0.0/8	any	any	Internal, DV...	10.19.132.17/32	any	entertainment-and-arts	TCP_B
38 NoDec_Internet_WE...	none	Internet, WEST	Group_NDICOGroupALL	any	any	any	10.19.132.18/32	any	unknown	
39 NoDec_Internet_WE...	none	Internet, WEST	Group_Internal_SV_ALL	any	any	any	10.19.132.27/32	any	any	
40 NoDec_Internet_WE...	none	Internet, WEST	any	any	any	any	any	any	All_Access	any
41 NoDec_Internet_WE...	none	Internet, WEST	any	any	any	Group_NoDec_Del	any	any	NoDec_URL_List	
42 NoDec_Internet_WE...	none	Internet, WEST	Group_NoDec_Sec	any	any	any	any	any	any	
43 Dec_Internet_WEST...	none	Internet, WEST	any	any	any	any	any	any	any	
44 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_DMZ_ALL	any	any	any	any	any	financial-services	any
45 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_DMZ_ALL	any	any	any	Group_NoDec_Del	any	any	
46 NoDec_Internet_DMZ...	none	Internet, DMZ	Group_NoDec_Sec	any	any	any	any	any	any	

図 1.1-1-28 SSL 復号化除外用 URL の削除

- ② 「Objects」タブ > 「URL カテゴリ」> フィルタに「NoDec_URL_List」を入力して、右側の「→」ボタンをクリックし、検索します。

名前	種類	タイプ
NoDec_URL_List		URLリスト

図 1.1-1-29 SSL 復号化除外用 URL の削除

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 「NoDec_URL_List」 の名前をクリックします。

名前	場所	タイプ
NoDec_URL_List		URLリスト
w-nexco-group.mazars.jp		
west-kouki.jp		
west-kouki.jp		
*fn777.co.jp		
fn777.co.jp		

図 1 1 – 1 – 3 0 SSL 復号化除外用 URL の削除

④ フィルタに削除したい「URL」を入力し、右側の「→」ボタンをクリックします。

以下に URL、ドメイン、またはホスト名を記入してください
www.TEST.com
サイト
www.TEST.com

図 1 1 – 1 – 3 1 SSL 復号化除外用 URL の削除

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

⑤ 削除対象のサイトを選択し、「削除」をクリックし、「OK ボタン」をクリックします。



図 1 1 – 1 – 3 2 SSL 復号化除外用 URL の削除

⑥ 「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 1 1 – 1 – 3 3 SSL 復号化除外用 URL の削除



図 1 1 – 1 – 3 4 SSL 復号化除外用 URL の削除

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

11.1.6. SSL 復号化除外用宛先アドレスの追加

- ① 「Policies」タブ > 「復号」> 対象除外用ポリシーの宛先アドレスを確認します。
※SSL 復号化除外ポリシーは宛先アドレス除外専用のアドレスグループが「Group_NoDec_Dst」となります。

ID	名前	タグ	ソース	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
40	NoDec_Internet_WEST.any_000	Internet_VR	Internet_WEST	any	any	any	any	any	any	financial services	any
41	NoDec_Internet_WEST.any_004	Internet_VR	Internet_WEST	any	any	any	any	any	any	government	any
42	NoDec_Internet_WEST.any_005	Internet_VR	Internet_WEST	any	any	any	any	any	any	health-and-medicine	any
43	Dec_Internet_WEST.any_001	Internet_VR	Internet_WEST	any	any	any	any	any	any	NoDec_URL_List	any
44	NoDec_Internet_DMZ.any_001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	financial services	any
45	NoDec_Internet_DMZ.any_002	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	government	any
46	NoDec_Internet_DMZ.any_003	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	health-and-medicine	any
47	Dec_Internet_DMZ.any_001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	NoDec_URL_List	any
48	NoDec_Internet_WEST.any_002	Internal_VR	Internet_WEST	Group_NEXCOGroupALL	any	any	any	any	any	any	any
49	NoDec_Internet_WEST.any_003	Internal_VR	Internet_WEST	Group_DMZ_ALL	any	any	any	any	any	any	any
50	NoDec_Internet_WEST.any_004	Internal_VR	Internet_WEST	any	any	any	any	any	any	financial services	any
51	NoDec_Internet_WEST.any_004	Internal_VR	Internet_WEST	any	any	any	any	any	any	government	any
52	NoDec_Internet_WEST.any_005	Internal_VR	Internet_WEST	Group_NoDec_Src	any	any	any	any	any	health-and-medicine	any

図 11-1-35 SSL 復号化除外用宛先アドレスの追加

- ② 「Objects」タブ > 「アドレスグループ」> フィルタに「Group_NoDec_Dst」を入力して、右側の「→」ボタンをクリックし、検索します。

名前	メンバーカー	アドレス	タグ
Group_NoDec_Dst	1	Dummy_Address	

図 11-1-36 SSL 復号化除外用宛先アドレスの追加

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 「Group_NoDec_Dst」の名前をクリックします。

The screenshot shows the PA-5450 configuration interface. The left sidebar contains a tree view of objects: Addresses, Address Groups, Applications, Application Groups, Services, Service Groups, Tags, Policies, and GlobalProtect. Under 'Address Groups', 'Group_NoDec_Dst' is selected and highlighted with a red box. The main content area displays a table with one row for 'Group_NoDec_Dst'. The table columns are '名前' (Name), '場所' (Location), 'メンバー数' (Member count), 'アドレス' (Address), and 'タグ' (Tags). The entry shows 'Group_NoDec_Dst' in the 'Name' field, '1' in the 'Member count' field, and 'Dummy_Address' in the 'Address' field. A 'Commit' button is visible at the top right.

図 11-1-37 SSL 復号化除外用宛先アドレスの追加

④ 「追加」ボタンをクリックし、アドレスオブジェクトを選択し、「OK」ボタンをクリックします。

※アドレスオブジェクトが存在しない場合は、新規アドレスオブジェクトを作成が必要となります。（「章 5.1.1」に参照）、ここでは例として「TEST_1.1.1.1」を選択します。

The screenshot shows the 'Address Group' configuration dialog. It has fields for '名前' (Name) containing 'Group_NoDec_Dst', '内容' (Content), 'タイプ' (Type) set to 'スタティック', and an 'アドレス' (Address) section with 'TEST_1.1.1.1' selected. At the bottom, there are buttons for '参照' (Reference), '+追加' (Add), and '削除' (Delete). The 'OK' button is highlighted with a red box. Other buttons include 'キャンセル' (Cancel) and 'PDF/CSV'.

図 11-1-38 SSL 復号化除外用宛先アドレスの追加

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 「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 1 1 – 1 – 3 9 SSL 復号化除外用宛先アドレスの追加

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 1 1 – 1 – 4 0 SSL 復号化除外用宛先アドレスの追加

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

1.1.1.7. SSL 復号化除外用宛先アドレスの削除

① 「Policies」タブ > 「復号」 > 対象除外用ポリシーの宛先アドレスを確認します。

※SSL 復号化除外用ポリシーは宛先アドレス除外専用のアドレスグループが「Group_NoDec_Dst」となります。

名前	タグ	ソース	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
40_NaDec_Internet_WEST.any_000	Internet_VR	Internet_WEST	any	any	any	any	any	any	financial services	any
41_NaDec_Internet_WEST.any_004	Internet_VR	Internet_WEST	any	any	any	any	Group_NoDec_Dst	any	government	any
42_NaDec_Internet_WEST.any_005	Internet_VR	Internet_WEST	any	any	any	any	any	any	health-and-medicine	any
43_Doc_Internet_WEST.any_001	Internet_VR	Internet_WEST	any	any	any	any	any	any	NoDoc_URL_List	any
44_NaDec_Internet_DMZ.any_001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	financial services	any
45_NaDec_Internet_DMZ.any_002	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	Group_NoDec_Dst	any	government	any
46_NaDec_Internet_DMZ.any_003	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	health-and-medicine	any
47_Doc_Internet_DMZ.any_001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	NoDoc_URL_List	any
48_NaDec_Internet_WEST.any_002	Internal_VR	Internet_WEST	Group_DMZ_ALL	any	any	any	any	any	financial services	any
49_NaDec_Internet_WEST.any_003	Internal_VR	Internet_WEST	Group_DMZ_ALL	any	any	any	any	any	government	any
50_NaDec_Internet_WEST.any_004	Internal_VR	Internet_WEST	any	any	any	any	any	any	health-and-medicine	any
51_NaDec_Internet_WEST.any_004	Internal_VR	Internet_WEST	any	any	any	any	Group_NoDec_Dst	any	NoDoc_URL_List	any
52_NaDec_Internet_WEST.any_005	Internal_VR	Internet_WEST	Group_NoDec_Src	any	any	any	any	any	any	any

図 1.1.1.4.1 SSL 復号化除外用宛先アドレスの追加

② 「Objects」タブ > 「アドレスグループ」 > フィルタに「Group_NoDec_Dst」を入力して、右側の「→」ボタンをクリックし、検索します。

名前	場所	メンバーグ	アドレス	タグ
Group_NoDec_Dst		1	Dummy_Address	

図 1.1.1.4.2 SSL 復号化除外用宛先アドレスの削除

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 「Group_NoDec_Dst」 の名前をクリックします。

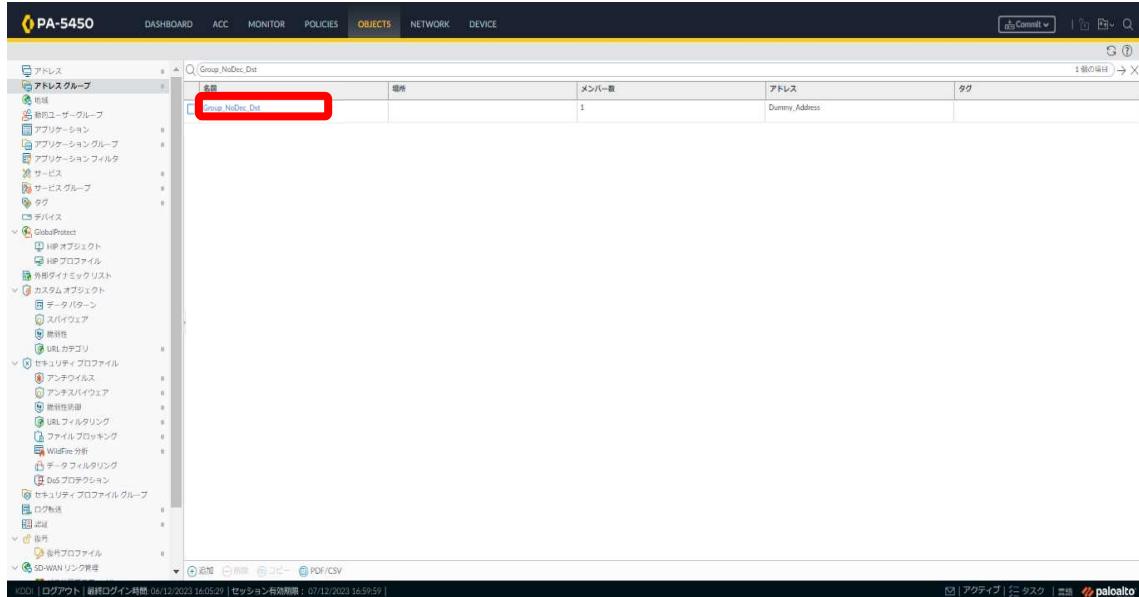


図 1 1 – 1 – 4 3 SSL 復号化除外用宛先アドレスの削除

④ 削除対象のアドレスを選択し、「削除」ボタンをクリックし、「OK」ボタンをクリックします。

※ここでは例として「TEST_1.1.1.1」を選択します。

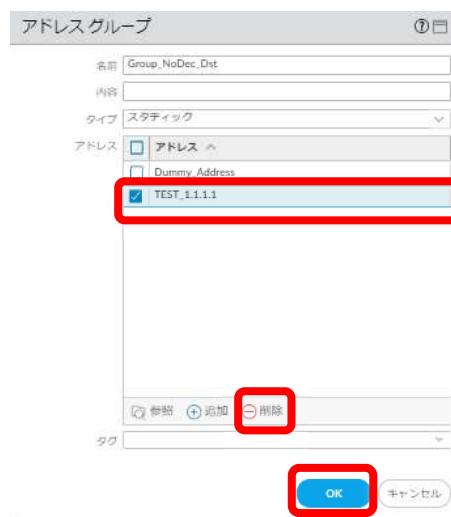


図 1 1 – 1 – 4 4 SSL 復号化除外用宛先アドレスの削除

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

- 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 1 1 – 1 – 4 5 SSL 復号化除外用宛先アドレスの削除

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 1 1 – 1 – 4 6 SSL 復号化除外用宛先アドレスの削除

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

11.1.8. SSL 復号化除外用送信元アドレスの追加

①「Policies」タブ > 「復号」 > 対象除外用ポリシーの送信元アドレスを確認します。

※SSL 復号化除外ポリシーは送信元アドレス除外専用のアドレスグループが「Group_NoDec_Src」となります。

各 G 会社の送信元アドレスの場合には、以下の要領にてアドレスグループを確認してください。

1. IP フラット化後のアドレス (10. ~) : 「Group_NoDec_Src」にアドレスを追加
2. IP フラット化前のアドレス (192.168. ~) : 「Group_NoDec_<G 会社>」にアドレスを追加

例 : SHD の場合は「Group_NoDec_SHD」

ソース	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
41 NuDoc_Internet_WEST_any_004	Internet_VR	Internet_WEST	any	any	any	any	any	any	financial services	any
42 NuDoc_Internet_WEST_any_003	Internet_VR	Internet_WEST	any	any	any	Group_NoDec_Src	any	any	government	any
43 Doc_Internet_WEST_any_001	Internet_VR	Internet_WEST	any	any	any	any	any	any	health-and-medicine	any
44 NuDoc_Hammet_DMZ_any_001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	NuDoc_URL_Ltd	any
45 NuDoc_Internet_DMZ_any_002	Internet_VR	Internet_DMZ	any	any	any	any	any	any	financial services	any
46 NuDoc_Internet_DMZ_any_003	Internet_VR	Internet_DMZ	Group_NoDec_Src	any	any	any	any	any	government	any
47 Doc_Internet_DMZ_any_001	Internet_VR	Internet_DMZ	any	any	any	any	any	any	health-and-medicine	any
48 NuDoc_Internet_WEST_any_001	Internal_VR	Internal_WEST	Group_NEKCGroupAll	any	any	any	any	any	NuDoc_URL_Ltd	any
49 NuDoc_Internet_WEST_any_002	Internal_VR	Internal_WEST	Group_DMZ_ALL	any	any	any	any	any	financial services	any
50 NuDoc_Internet_WEST_any_003	Internal_VR	Internal_WEST	any	any	any	any	any	any	government	any
51 NuDoc_Internet_WEST_any_004	Internal_VR	Internal_WEST	any	any	any	Group_NoDec_Src	any	any	health-and-medicine	any
52 NuDoc_Internet_WEST_any_005	Internal_VR	Internal_WEST	Group_NoDec_Src	any	any	any	any	any	NuDoc_URL_Ltd	any

図 11-1-47 SSL 復号化除外用送信元アドレスの追加

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 > 「アドレスグループ」 > フィルタに「Group_NoDec_Src」を入力して、右側の「→」ボタンをクリックし、検索します。

名前	場所	メンバー数	アドレス	タグ
Group_NoDec_Src		2	Dummy_Address proxy.wuta.west.local	

図 1 1 – 1 – 4 8 SSL 復号化除外用送信元アドレスの追加

- ③ 「Group_NoDec_Src」の名前をクリックします。

名前	場所	メンバー数	アドレス	タグ
Group_NoDec_Src		2	Dummy_Address proxy.wuta.west.local	

図 1 1 – 1 – 4 9 SSL 復号化除外用送信元アドレスの追加

- ④ 「追加」ボタンをクリックし、アドレスオブジェクトを選択し、「OK」ボタンをクリックします。

※アドレスオブジェクトが存在しない場合は、新規アドレスオブジェクトを作成が必要となります。（「章 5. 1. 1」に参照）、ここでは例として「TEST_1.1.1.1」を選択します。

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

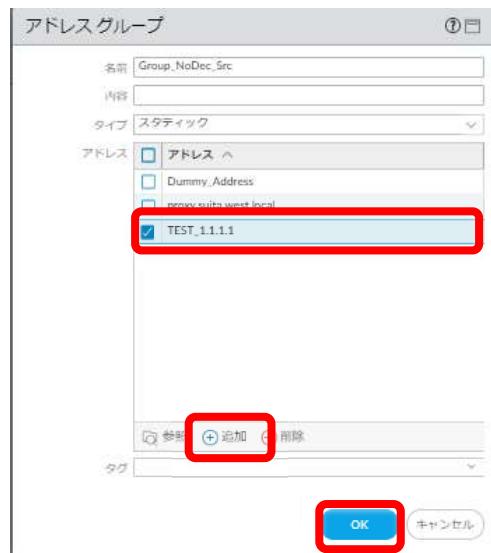
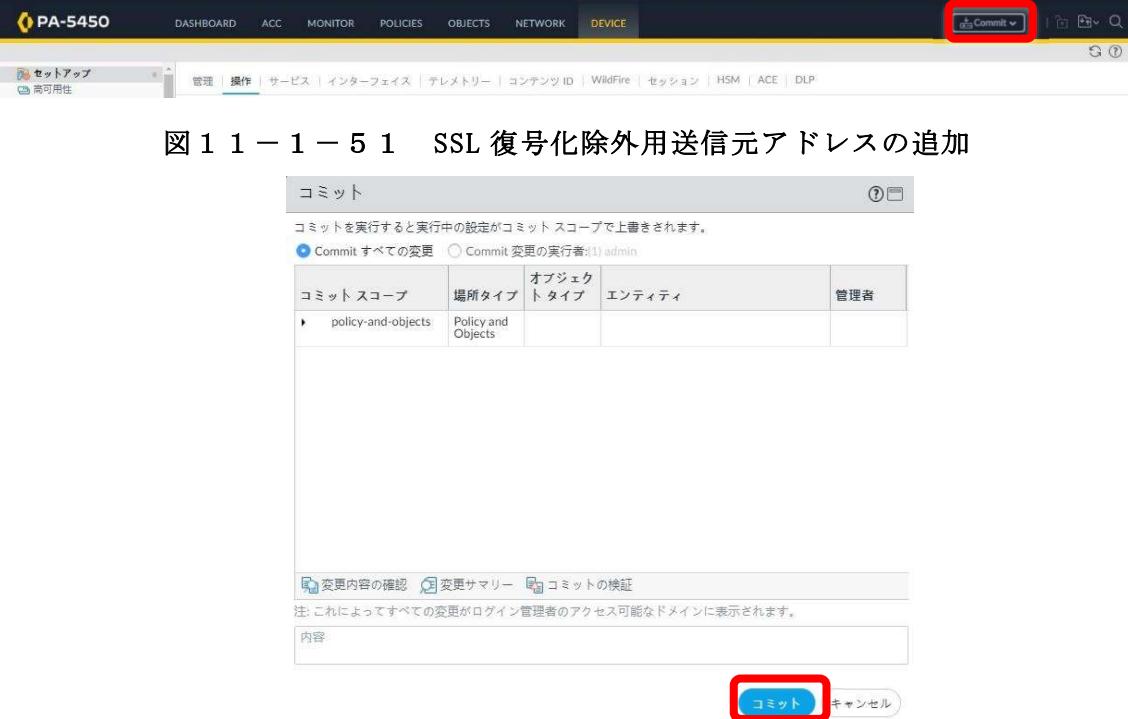


図 11-1-50 SSL 復号化除外用送信元アドレスの追加

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 「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 configuration 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 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。' (Executing a commit will overwrite the current settings in the commit scope.) Below this are two radio buttons: 'Commit すべての変更' (Commit all changes) and 'Commit 変更の実行者(1) admin' (Commit author of changes (1) admin). A table below shows the commit scope and location type:

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			

At the bottom, 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' (Validation of commit). 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.) Below these are '内容' (Content) and 'コメント' (Comment) input fields. The 'コミット' (Commit) button at the bottom right is highlighted with a red box.

図 11-1-5-2 SSL 復号化除外用送信元アドレスの追加

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

1.1.1.9. SSL 復号化除外用送信元アドレスの削除

①「Policies」タブ > 「復号」 > 対象除外用ポリシーの宛先アドレスを確認します。

※SSL 復号化除外用ポリシーは宛先アドレス除外専用のアドレスグループが「Group_NoDec_Src」となります。

各 G 会社の送信元アドレスの場合には、以下の要領にてアドレスグループを確認してください。

1. IP フラット化後のアドレス (10. ~) : 「Group_NoDec_Src」からアドレスを削除
2. IP フラット化前のアドレス (192.168. ~) : 「Group_NoDec_<G 会社>」からアドレスを削除

例：SHD の場合は「Group_NoDec_SHD」

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
NoDec_Internet_WEST.any.003	Internet_VR	Internet_WEST	any	any	any	any	any	any	financial services	any
NoDec_Internet_WEST.any.004	Internet_VR	Internet_WEST	any	any	any	any	any	any	government	any
NoDec_Internet_WEST.any.005	Internet_VR	Internet_WEST	Group_NoDec_Src	any	any	any	any	any	health-and-medicine	any
Dec_Internet_WEST.any.001	Internet_VR	Internet_WEST	any	any	any	any	any	any	NoDec_URL_List	any
NoDec_Internet_DMZ.any.001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	financial services	any
NoDec_Internet_DMZ.any.002	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	government	any
NoDec_Internet_DMZ.any.003	Internet_VR	Internet_DMZ	Group_NoDec_Src	any	any	any	any	any	health-and-medicine	any
Dec_Internet_DMZ.any.001	Internet_VR	Internet_DMZ	Group_DMZ_ALL	any	any	any	any	any	NoDec_URL_List	any
NoDec_Internet_DMZ.any.004	Internal_VR	Internal_DMZ	any	any	any	any	any	any	any	any
NoDec_Internet_DMZ.any.005	Internal_VR	Internal_DMZ	Group_NoDec_Src	any	any	any	any	any	any	any
NoDec_Internet_WEST.any.001	Internal_VR	Internal_WEST	any	any	any	any	any	any	financial services	any
NoDec_Internet_WEST.any.002	Internal_VR	Internal_WEST	Group_NEXCO_GroupALL	any	any	any	any	any	government	any
NoDec_Internet_WEST.any.003	Internal_VR	Internal_WEST	Group_DMZ_ALL	any	any	any	any	any	health-and-medicine	any
NoDec_Internet_WEST.any.004	Internal_VR	Internal_WEST	any	any	any	any	any	any	NoDec_URL_List	any
NoDec_Internet_WEST.any.005	Internal_VR	Internal_WEST	Group_NoDec_Src	any	any	any	any	any	any	any

図 1.1.1.5.3 SSL 復号化除外用送信元アドレスの削除

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 「Objects」タブ > 「アドレスグループ」 > フィルタに「Group_NoDec_Src」を入力して、右側の「→」ボタンをクリックし、検索します。

The screenshot shows the PA-5450 configuration interface. The 'OBJECTS' tab is selected. In the left sidebar, 'アドレスグループ' (Address Groups) is highlighted with a red box. A search bar at the top contains the text 'Group_NoDec_Src'. Below the search bar, a table lists a single entry: 'Group_NoDec_Src' with a member count of 2, address 'Dummy_Address', and tag 'group.suita.west.local'. A red box highlights the 'Group_NoDec_Src' entry in the table. A red circle with a right-pointing arrow is placed over the '→' button in the top right corner of the search results area.

図 1 1 – 1 – 5 4 SSL 復号化除外用送信元アドレスの削除

- ④ 「Group_NoDec_Src」の名前をクリックします。

This screenshot is identical to the previous one, showing the search results for 'Group_NoDec_Src'. However, the entry 'Group_NoDec_Src' in the table is now highlighted with a red box, indicating it has been selected for modification.

図 1 1 – 1 – 5 5 SSL 復号化除外用送信元アドレスの削除

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 削除対象のアドレスを選択し、「削除」ボタンをクリックし、「OK」ボタンをクリックします。

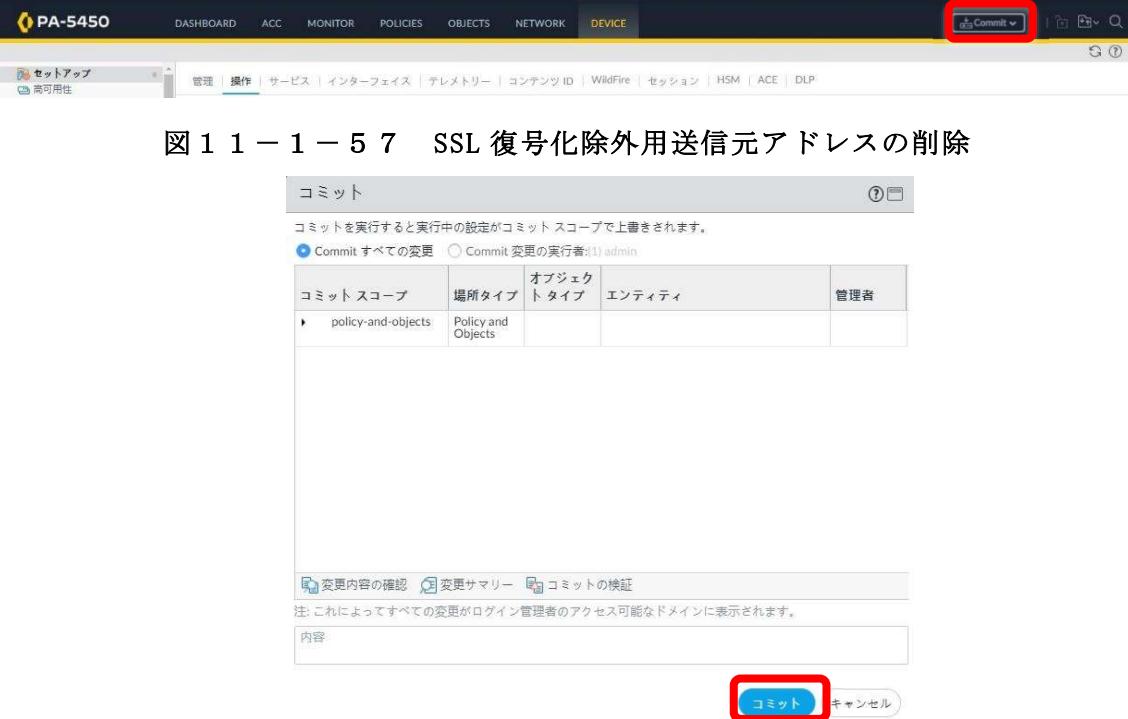
※ここでは例として「TEST_1.1.1.1」を選択します。



図 11-1-56 SSL 復号化除外用送信元アドレスの削除

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

- 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)



The screenshot shows the PA-5450 device configuration interface. The top navigation bar has tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, and DEVICE, with DEVICE 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 confirmation 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。' (Executing a commit will overwrite the current settings in the commit scope.) Below this, there are two radio buttons: 'Commit すべての変更' (Commit all changes) and 'Commit 変更の実行者(1) admin' (Commit author of changes (1) admin). A table below shows the commit scope and type:

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			

At the bottom, 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' (Validation of commit). 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.) Below these buttons is a text input field labeled '内容' (Content). The bottom right of the screen shows the 'コミット' (Commit) button, which is also highlighted with a red box, and a 'キャンセル' (Cancel) button.

図 11-1-5-8 SSL 復号化除外用送信元アドレスの削除

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

1.1.1.10. SSL 復号化除外用サービスの追加

- ① 「Objects」タブ > 「サービスグループ」 > フィルタに「Group_NoDec_Service」を入力して、右側の「→」ボタンをクリックし、検索します。

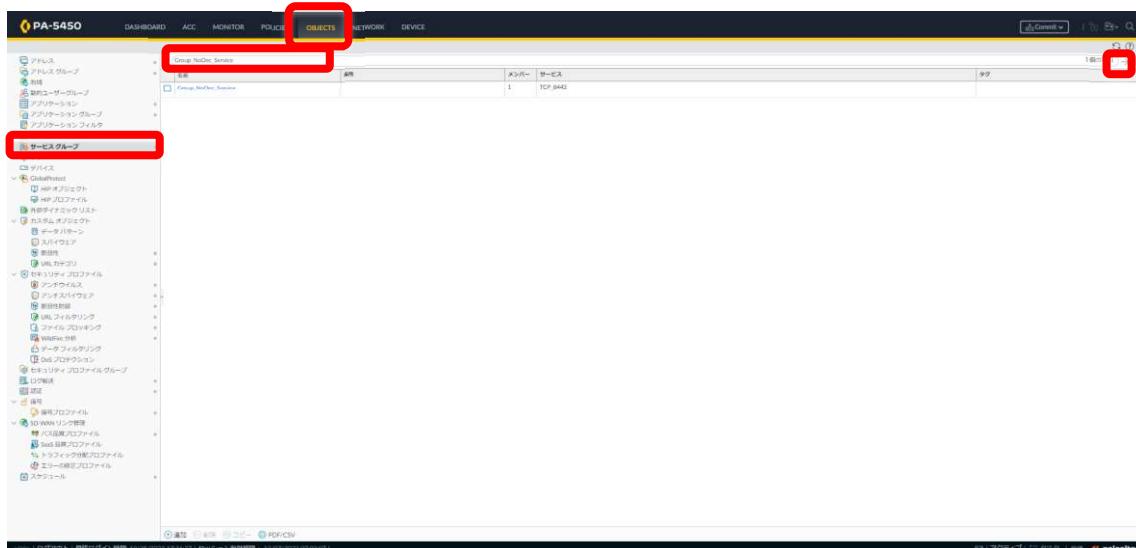


図 1.1-1-59 SSL 復号化除外用サービスの追加

- ② 「Group_NoDec_Service」の名前をクリックします。

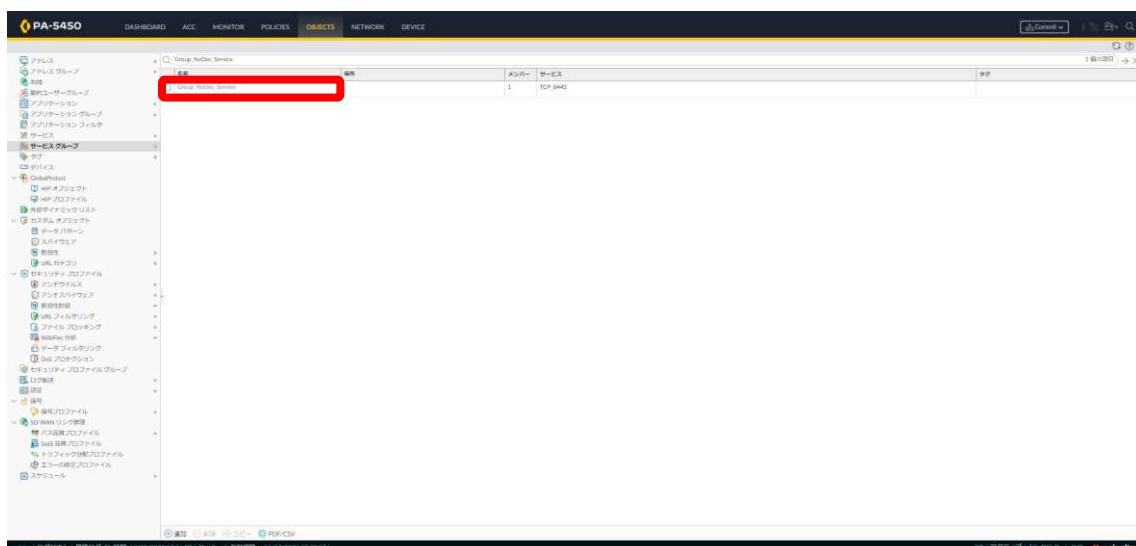


図 1.1-1-60 SSL 復号化除外用サービスの追加

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 「追加」ボタンをクリックし、サービスオブジェクトを選択し、「OK」ボタンをクリックします。

※サービスオブジェクトが存在しない場合は、新規サービスオブジェクトを作成が必要となります。、ここでは例として「TCP_21」を選択します。



図 1-1-6-1 SSL 復号化除外用サービスの追加

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 「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 configuration 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 'SSL 復号化除外用サービスの追加' (Add SSL Decryption Exemption Service). It displays a 'Commit' dialog box with the following details:

- Commit scope: policy-and-objects
- Location type: Policy and Objects
- Object type: None
- Entity type: None
- Manager: None

Below the dialog, 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' (Validation of Commit). A note states: '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。' (All changes will be displayed in the domain accessible to the logged-in administrator).

At the bottom of the page, there is a text input field labeled '内容' (Content) and two buttons: 'コミット' (Commit) and 'キャンセル' (Cancel). A red box highlights the 'Commit' button.

図 1 1 – 1 – 6 3 SSL 復号化除外用サービスの追加

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

1.1.1.1.11. SSL 復号化除外用サービスの削除

- ① 「Objects」タブ > 「サービスグループ」 > フィルタに「Group_NoDec_Service」を入力して、右側の「→」ボタンをクリックし、検索します。

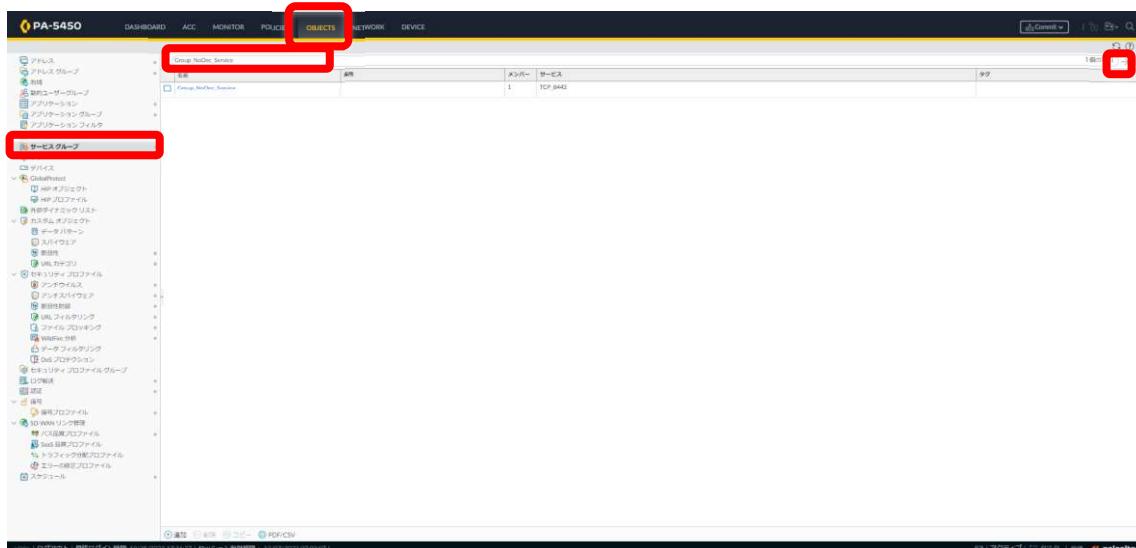


図 1.1.1.1.11. SSL 復号化除外用サービスの削除

- ② 「Group_NoDec_Service」の名前をクリックします。

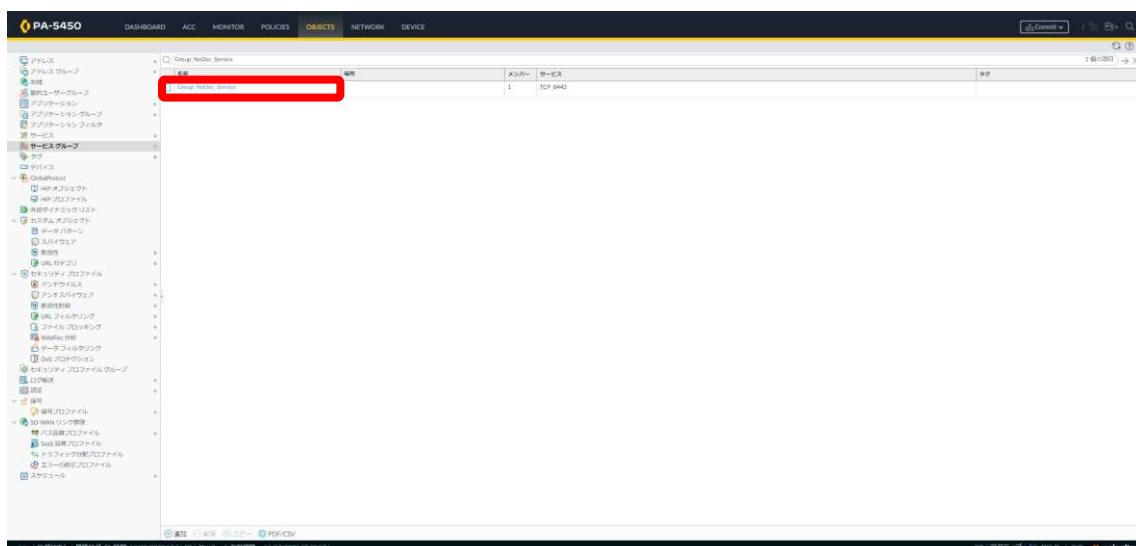


図 1.1.1.1.11. SSL 復号化除外用サービスの削除

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 削除対象のアドレスを選択し、「削除」ボタンをクリックし、「OK」ボタンをクリックします。

※ここでは例として「TCP_21」を選択します。



図 1 1 – 1 – 6 6 SSL 復号化除外用サービスの削除

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

- 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 11-1-67 SSL 復号化除外用送信元アドレスの削除

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 11-1-68 SSL 復号化除外用送信元アドレスの削除

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

12. SSL インバウンドインスペクション設定

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。

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

1.2.1.1. DMZ サーバの SSL 復号化ポリシー追加

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

図 1.2-1-1 DMZ サーバの SSL 復号化ポリシー追加

- ② 以下(1)～(10)を設定（「表 9-1-1」を参照）し、「OK」ボタンをクリックします。※ここでは例として「DMZ_TEST」を作成します。

(1)

(10)

図 1.2-1-2 DMZ サーバの SSL 復号化ポリシー追加

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

表9—1—1 (2) / (3) 送信元ゾーン/送信元アドレスは「Internet_Untrust」 / 「いずれか」を選択します。

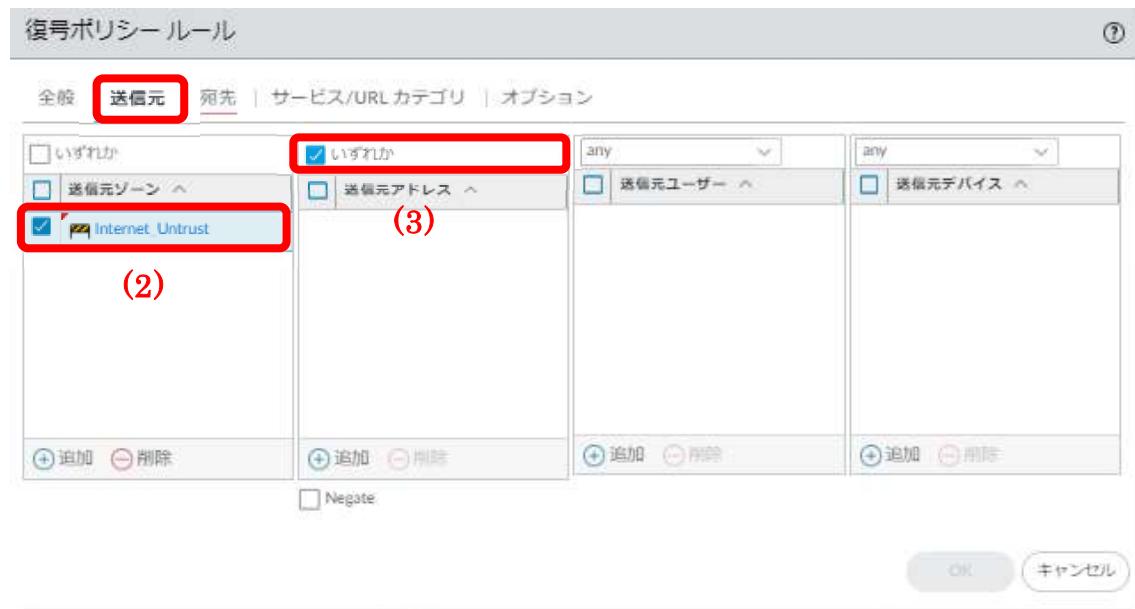


図12—1—3 DMZ サーバの SSL 復号化ポリシー追加

表9—1—1 (4) 宛先ゾーンは「Internet_DMZ」を選択します。

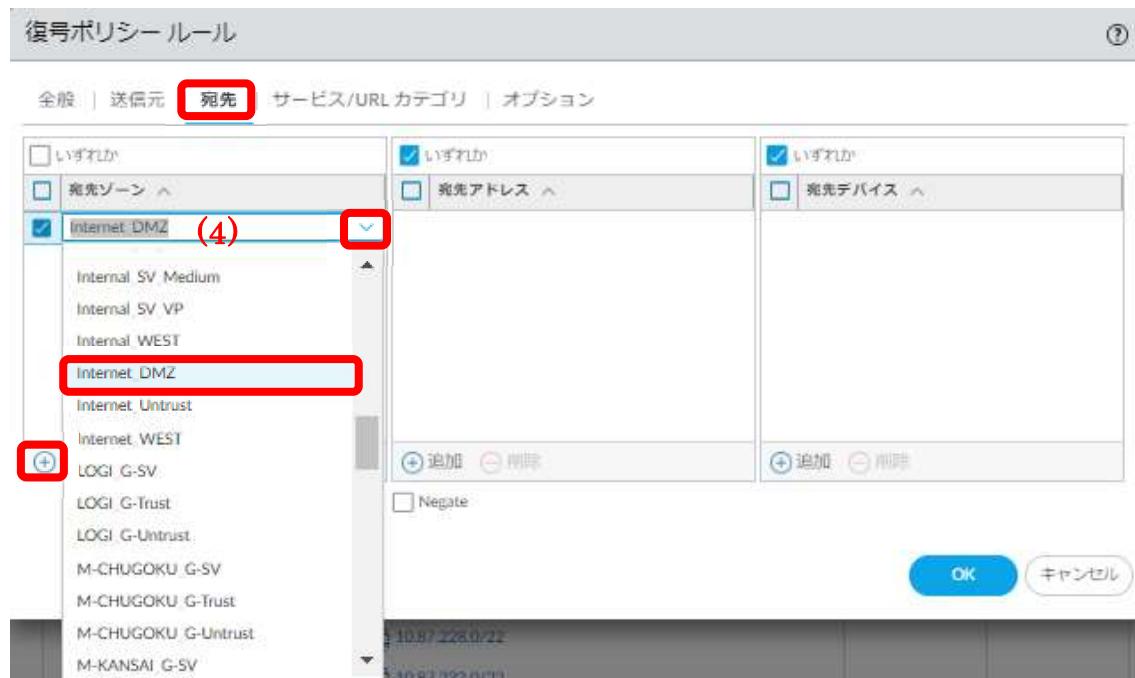


図12—1—4 DMZ サーバの SSL 復号化ポリシー追加

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

表9—1—1 (5)宛先アドレスを追加し、「DMZ サーバのグローバル IP」を選択します。

※アドレスオブジェクトが存在しない場合は、新規アドレスオブジェクトを作成が必要となります。（「章5.1.1」に参照）。



図12—1—5 DMZ サーバの SSL 復号化ポリシー追加

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。

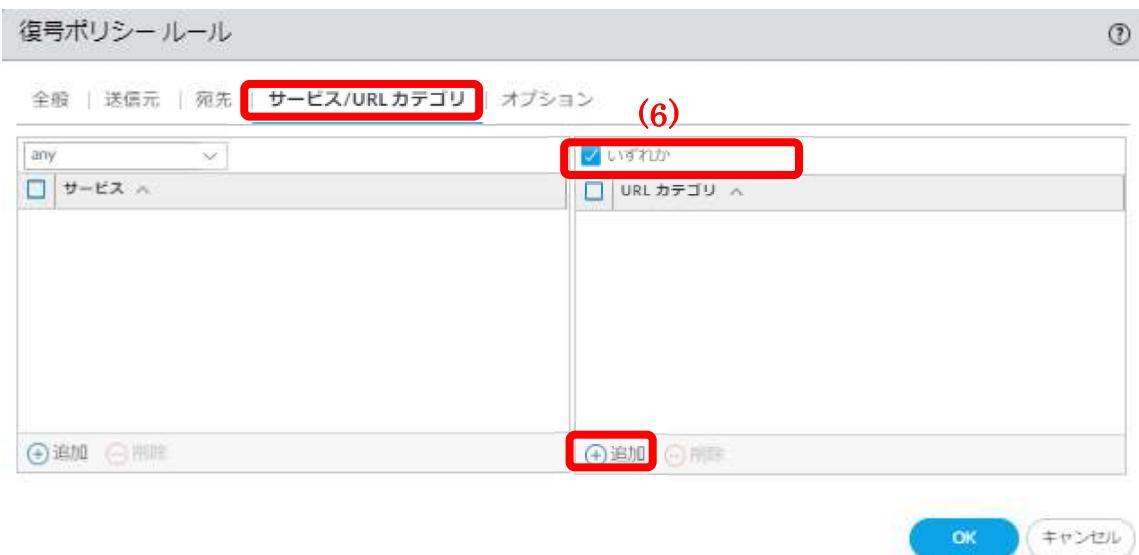


図12—1—6 DMZ サーバの SSL 復号化ポリシー追加

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

表9—1—1 (7) アクションは「復号」をチェックが入れます。

表9—1—1 (8) タイプを入力します。

ここは「SSL インバウンドインスペクション」を選択します

表9—1—1 (9) 復号プロファイルを入力します。ここは「None」を選択します。

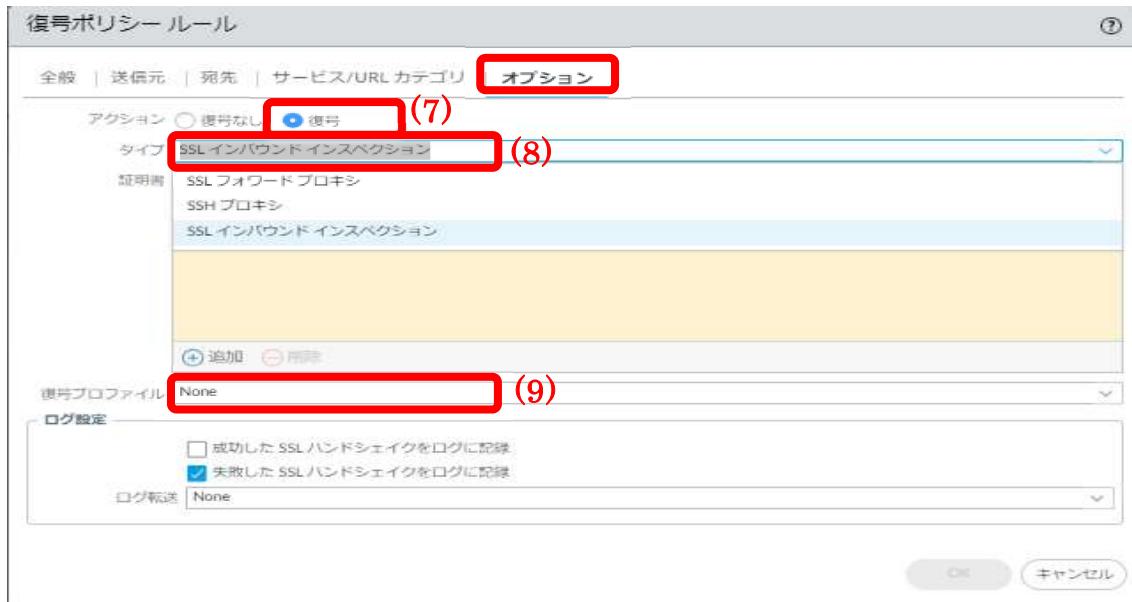


図12—1—7 DMZ サーバの SSL 復号化ポリシー追加

表9—1—1 (11) SSL 証明書を追加します。

※証明書は事前に作成が必要となります。

※証明書作成は（章21.3. DMZ サーバの証明書インポート）を参照

ここは例として、仮証明書「TEST_DMZ」を選択します。

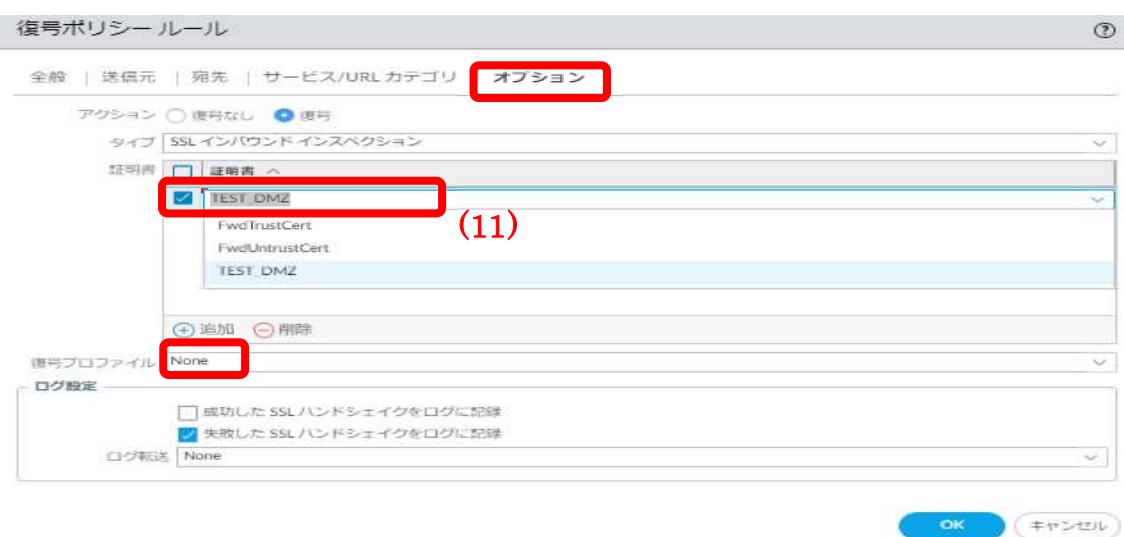


図12—1—8 DMZ サーバの SSL 復号化ポリシー追加

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「OK」ボタンをクリックします。

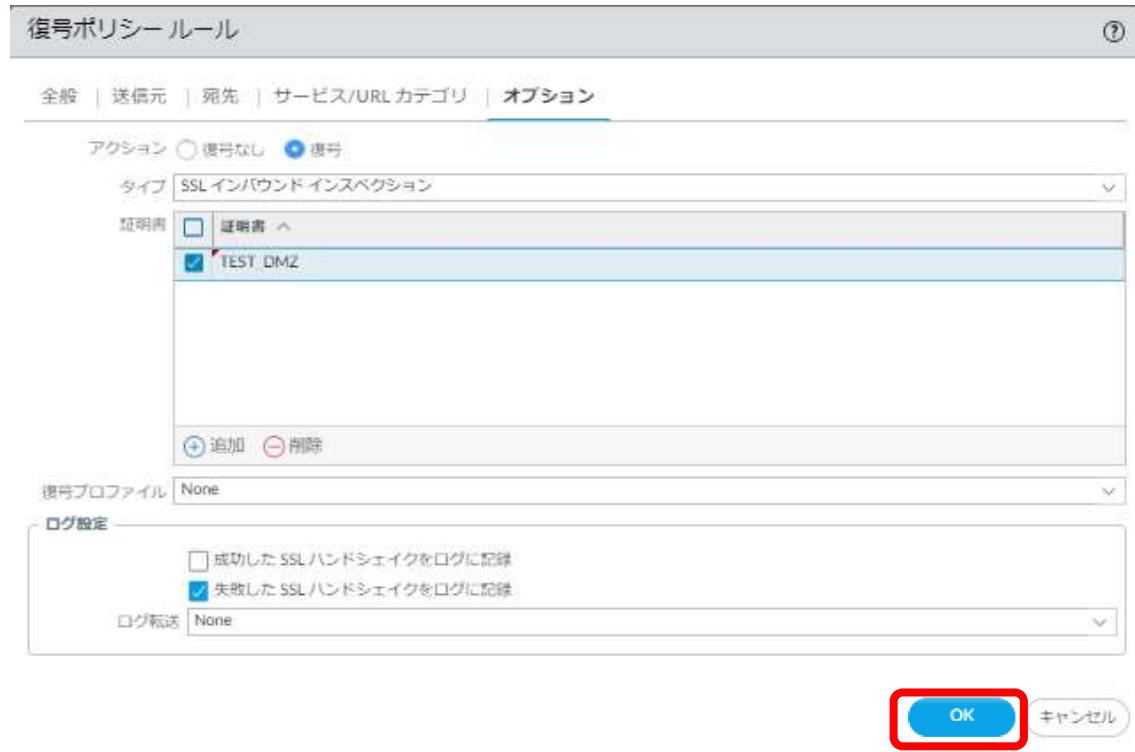


図 12-1-9 DMZ サーバの SSL 復号化ポリシー追加

④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。

※既存の復号化ポリシーより上位に配置するように移動します。

図 12-1-10 DMZ サーバの SSL 復号化ポリシー追加

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 「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 12-1-1-1 DMZ サーバの SSL 復号化ポリシー追加

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			

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

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 12-1-1-1-2 DMZ サーバの SSL 復号化ポリシー追加

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

1.2.1.2. DMZ サーバの SSL 復号化ポリシー削除

- ① 「Policies」タブ > 「復号」> 削除対象のポリシーを選択 > 「削除」ボタンをクリックします。

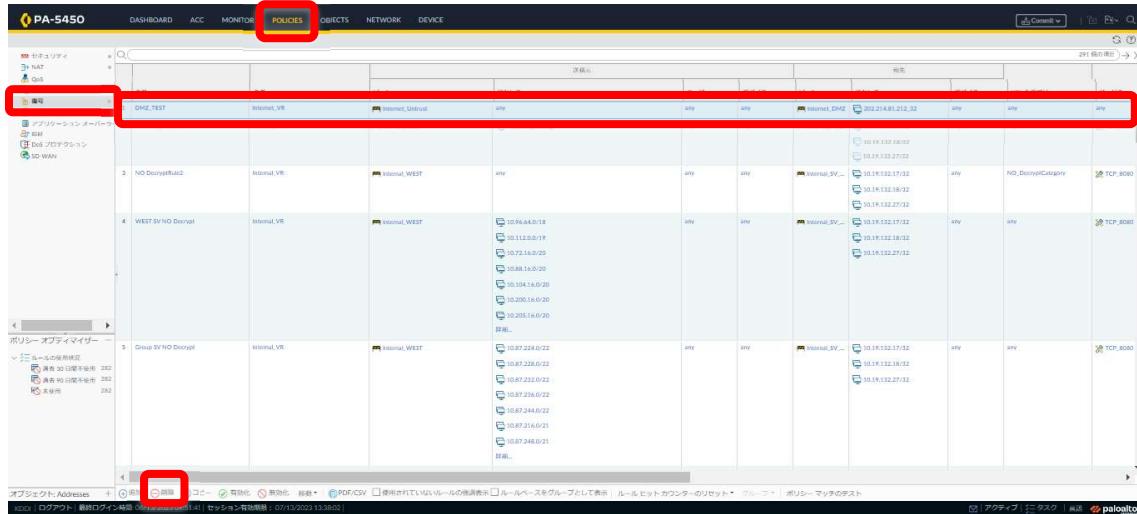


図 1.2-1-1-3 DMZ サーバの SSL 復号化ポリシー削除

- ② 「はい」をクリックします。



図 1.2-1-1-4 DMZ サーバの SSL 復号化ポリシー削除

- 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 1.2-1-1-5 DMZ サーバの SSL 復号化ポリシー追加

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

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 1-2-1-1-16 DMZ サーバの SSL 復号化ポリシー追加

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

1 3 . 手動フェイルオーバー

この項では、オペレーションによる切り替え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

1.3.1. Palo Alto 手動フェイルオーバー

Active 機側のステータスを Suspend に変更して系統を切替る手順を記載します。

※本手順は現 Active 機側にて実施する手順です。

(HA の「ステータス」については、「表 1.3-1-1」を参照)。

- ① 「Device」タブ > 「高可用性」 > 「操作コマンド」タブ > 「Suspend local デバイス for high availability」をクリック後、「OK」ボタンをクリックします。



図 1.3-1-1 PA-5450 HA FailOver



図 1.3-1-2 PA-5450 HA FailOver

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 「Dashboard」タブ > 「高可用性」タブにて、「local」ステータスが「Suspended User requested」、「ピア」ステータスが「Active」であることを確認します。

管理者	送信者	クライアント	セッション開始	アイドル状態
KDDI	10.19.132.13	Web	06/12 14:34:15	00:14:50s
admin	10.88.0.1	Web	06/12 14:41:31	00:00:00s
panorama	Console	Panorama	06/02 19:16:28	00:00:01s
KDDI	10.19.132.13	CLI	06/12 14:30:07	00:19:03s
KDDI	10.19.132.13	CLI	06/12 14:32:56	00:15:3s

図 13-1-3 PA-5450 HA FailOver

- ① HA 対向機器で、「Dashboard」> 「高可用性」にて、「Local」ステータスが「Active」、「ピア」ステータスが「Suspended User requested」になっていることを確認します。

管理者	送信者	クライアント	セッション開始	アイドル状態
panorama	Console	Panorama	06/02 20:00:12	00:00:13s
KDDI	10.19.132.13	Web	06/12 14:30:38	00:19:14s
admin	10.88.0.1	Web	06/12 14:53:05	00:00:00s

図 13-1-4 PA-5450 HA FailOver

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 旧 Active 機 (Suspend を実行した機器) の「Device」タブ > 「高可用性」タブ > 「操作コマンド」タブ > 「Make local デバイス functional for high availability」をクリックします。



図 1 3 – 1 – 5 PA-5450 HA FailOver

- ③ 「Dashboard」 > 「高可用性」にて、「Local」ステータスが「Passive」、「ピア」ステータスが「Active」であることを確認します。

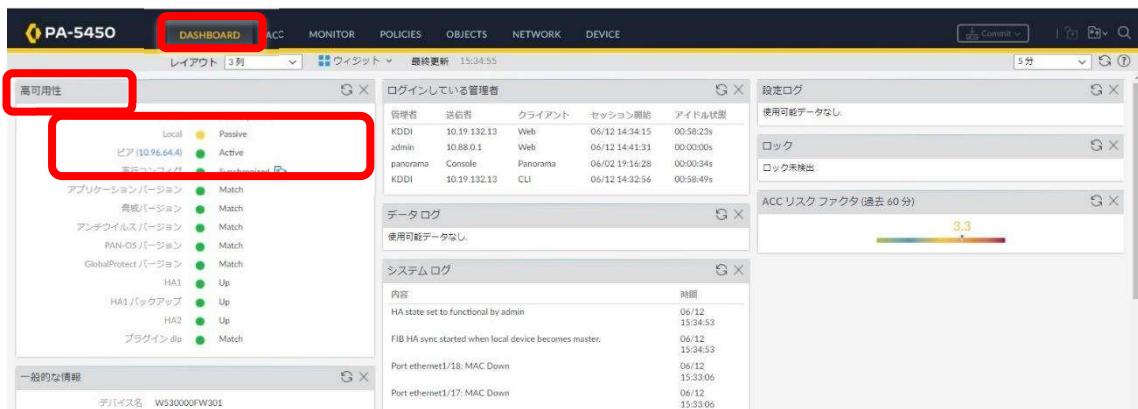


図 1 3 – 1 – 6 PA-5450 HA FailOver

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 HA 対向機器で、「Dashboard」 > 「高可用性」にて、「Local」ステータスが「Active」、「ピア」ステータスが「Passive」であることを確認します。



図 13-1-7 PA-5450 HA FailOver

表 13-1-1 HA ステート

名前	利用用途
Initial	HA 情報構成機器の「初期状態」
Active	HA 変換構成機器において、トラフィック処理を行う「ステータス」
Passive	HA 変換構成機器において、トラフィック処理を行う「Active」機器側と「セッション同期」を行う「バックアップ機」の「ステータス」
Non-functional	Active 機/Passive 機で「Link Failure」、「Path Failure」、「Data-Plane Failure」が検出された場合に、この「ステータス」となる。
Suspended	HA 変換構成において、管理上「無効」にされた「ステータス」

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

1.3.2. Panorama 手動フェイルオーバー

「Primary-active」機側のステータスを Suspended に変更して系統を切替る手順を記載します。(HA の「ステータス」については、「表 1.3-2-1」を参照)

- ① 「Panorama」タブ > 「高可用性」 > 「操作コマンド」の「Suspended local

Panorama for high availability」をクリックし、「OK」ボタンをクリックします。

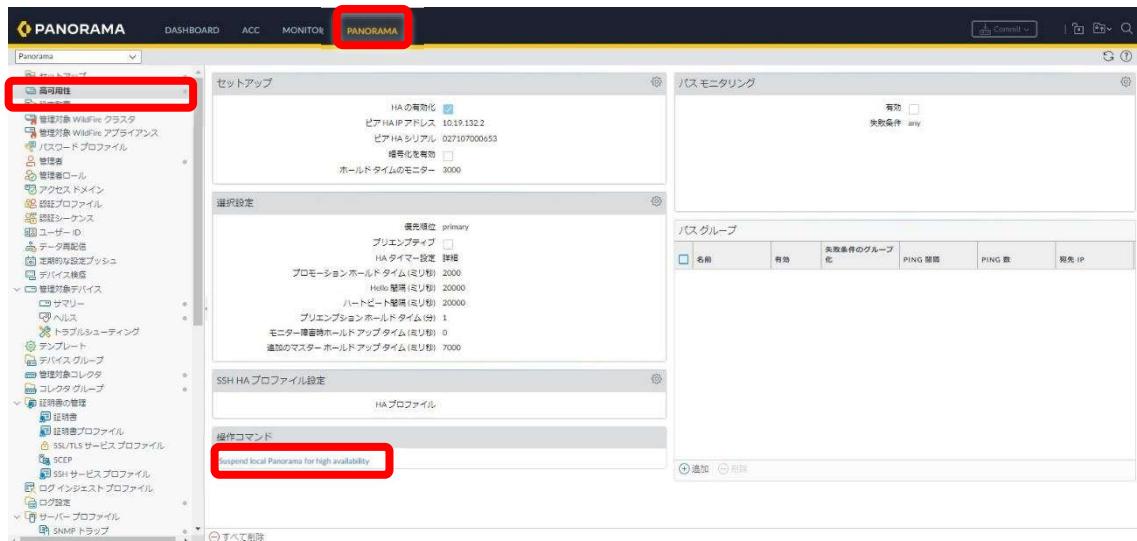


図 1.3-2-1 Panorama M-300 HA FailOver



図 1.3-2-2 Panorama M-300 HA FailOver

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 「Dashboard」タブ > 「高可用性」の「Local」ステータスが「primary-suspended(User requested)」に、「ピア」ステータスが「Secondary-active」になっていることを確認します。

状態	説明
Local	primary-suspended (User requested)
ピア (10.19.132.2)	Secondary-active

図 13-2-3 Panorama M-300 HA FailOver

- ③ HA 対向機器で、「Dashboard」タブ > 「高可用性」の「Local」ステータスが「secondary-active」に、「ピア」ステータスが「Primary-suspended(User requested)」になっていることを確認します。

状態	説明
Local	secondary-active
ピア (10.96.64.2)	Primary-suspended (User requested)

図 13-2-4 Panorama M-300 HA FailOver

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 旧 Active 機 (Suspend を実行した機器) の「Panorama」タブ > 「高可用性」タブ > 「操作コマンド」の「Make local Panorama functional for high availability」をクリックします。

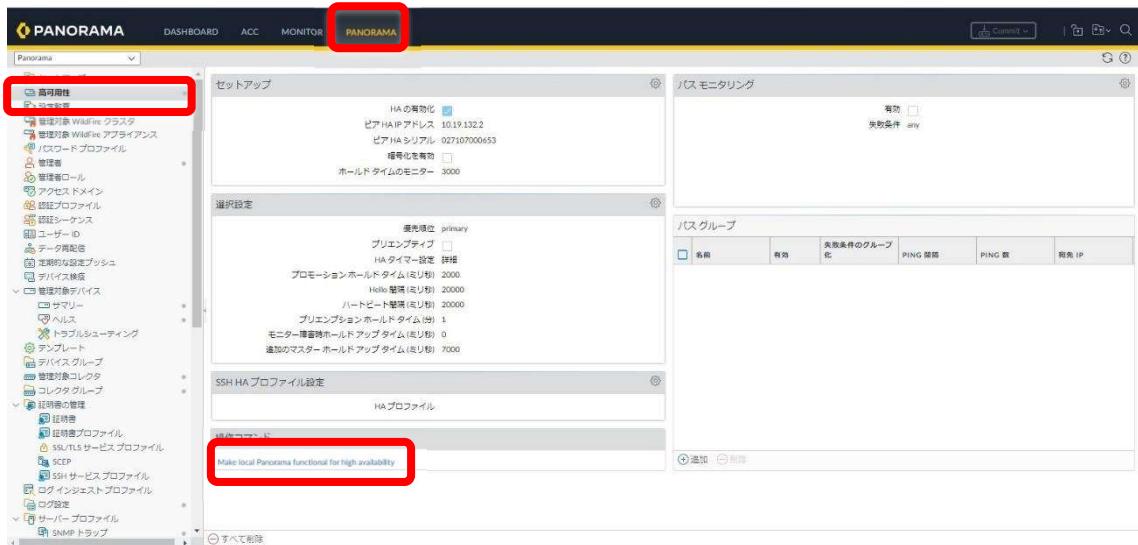


図 13-2-5 Panorama M-300 HA FailOver

- ⑤ 「Dashboard」タブ > 「高可用性」にて、「Local」ステータスが「primary-passive」に、「ピア」ステータスが「Secondary-active」であることを確認します。

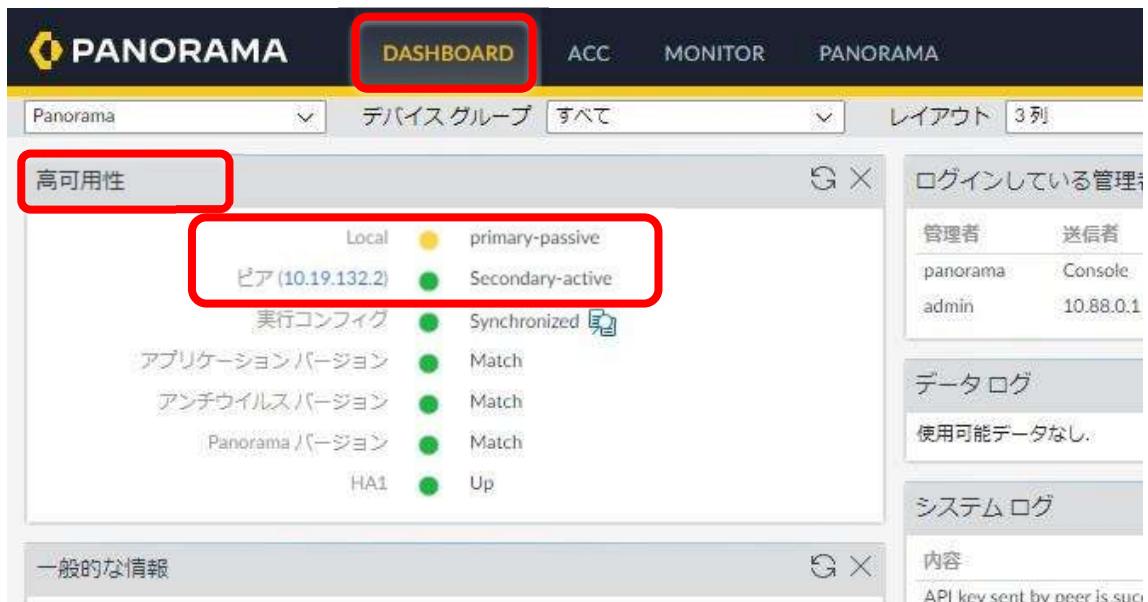


図 13-2-6 Panorama M-300 HA FailOver

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 HA 対向機器で、「Dashboard」 > 「高可用性」にて、「Local」ステータスが「secondary-active」に、「ピア」ステータスが「Primary-passive」であることを確認します。

項目	状態
Local	secondary-active
ピア (10.96.64.2)	Primary-passive
実行コンフィグ	Synchronized
アプリケーションバージョン	Match
アンチウイルスバージョン	Match
Panorama バージョン	Match
HA1	Up

図 13-2-7 Panorama M-300 HA FailOver

表 13-2-1 HA ステータス

名前	利用用途
primary (secondary)-active	HA冗長構成機器において、主系機器の「ステータス」
primary (secondary)-passive	HA冗長構成機器において、副系機器の「ステータス」
primary (secondary)-suspended	HA冗長構成において、管理上「無効」にされた「ステータス」

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

14. 手動フェイルバック

この項では、オペレーションによる切り戻し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

1.4. 1. Palo Alto 手動フェイルバック

Active 機側のステータスを「Suspend」に変更して系統を切り戻す手順を記載します。
通常時は「Active」として稼動している 1 号機が障害復旧し、1 号機側のステータスが「Passive」、2 号機側のステータスが「Active」の状態から系統を切り戻す手順を記載します。(HA の「ステータス」については、「表 1.4-1-1」を参照)

- ① 2 号機側で、「Device」タブ > 「高可用性」 > 「操作コマンド」 > 「Suspend local デバイス for high availability」をクリック後「OK」ボタンをクリックします。



図 1.4-1-1 PA-5450 HA FailBack

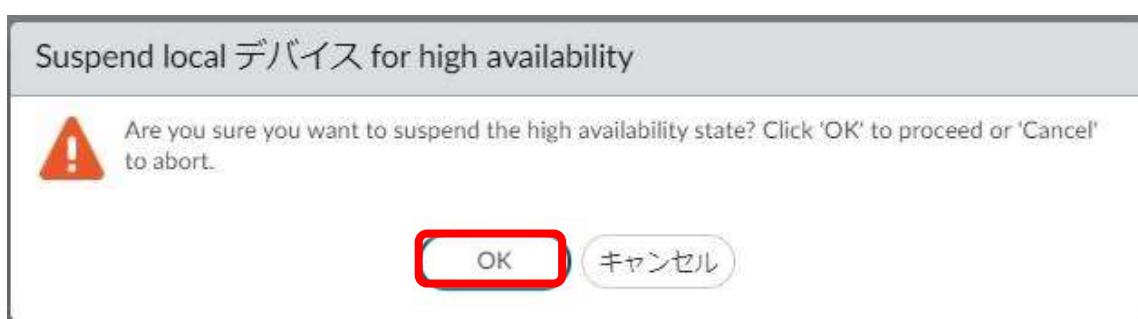


図 1.4-1-2 PA-5450 HA FailBack

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 2号機側で、「Dashboard」タブ > 「高可用性」をクリックし、「Local」ステータスが「Suspend(User requested)」、「ピア」ステータスが「Active」であることを確認します。

モード	状態
Local	Suspended (User requested)
ピア (10.96.64.4)	Active

図 1 4 – 1 – 3 PA-5450 HA FailBack

- ③ 1号機側で、「Dashboard」タブ > 「高可用性」をクリックし、「Local」ステータスが「Active」、「ピア」ステータスが「Suspended(User requested)」であることを確認します。

モード	状態
Local	Active
ピア (10.96.64.3)	Suspended (User requested)

図 1 4 – 1 – 4 PA-5450 HA FailBack

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 2号機側で、「Device」タブ > 「高可用性」 > 「操作コマンド」タブをクリックし、「Make local デバイス functional for high availability」をクリックします。



図 1 4 – 1 – 5 PA-5450 HA FailBack

- ⑤ 2号機側で、「Dashboard」>「高可用性」をクリックし、「Local」ステータスが「Passive」、「ピア」ステータスが「Active」であることを確認します。

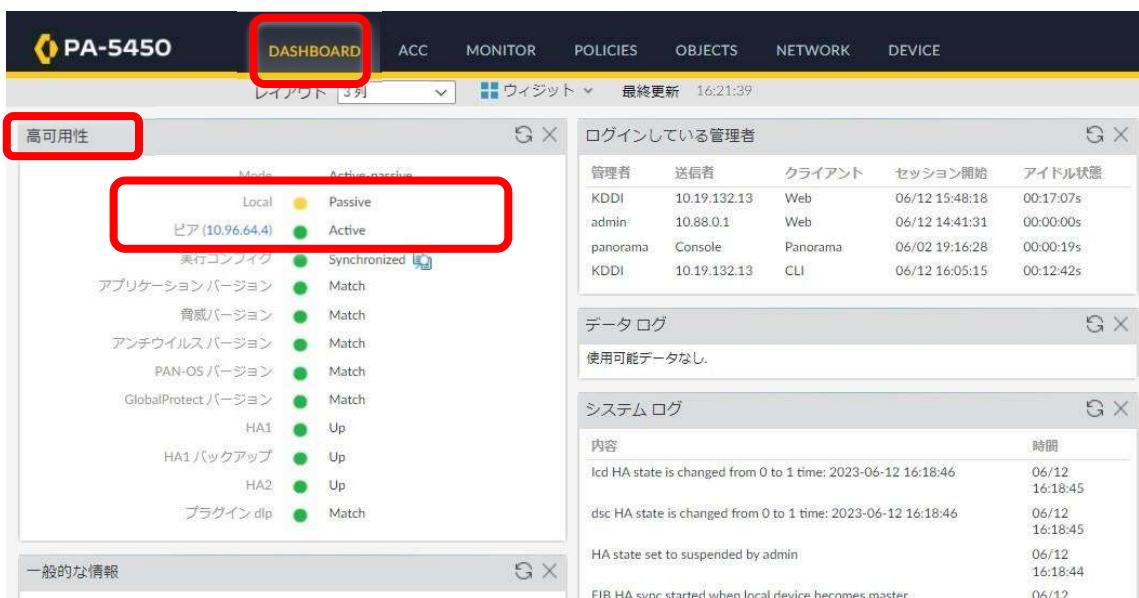


図 1 4 – 1 – 6 PA-5450 HA FailOver

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 1号機側で、「Dashboard」>「高可用性」をクリックし、「Local」ステータスが「Active」、「ピア」ステータスが「Passive」であることを確認します。

管理者	送信者	クライアント	セッション開始	アイドル状態
panorama	Console	Panorama	06/02 20:00:12	00:00:16s
KDDI	10.19.132.13	Web	06/12 14:30:38	00:32:44s
admin	10.88.0.1	Web	06/12 14:53:05	00:00:00s

データログ
使用可能データなし。

内容	時間
KEYMGR sync all IPSec SA to HA peer exit.	06/12 16:21:42
FIB HA sync started when peer device becomes passive.	06/12 16:21:42
KEYMGR sync all IPSec SA to HA peer started.	06/12 16:21:42
SATD daemon sync all gateway infos to HA peer started.	06/12 16:21:42

図 14-1-7 PA-5450 HA FailOver

表 14-1-1 HA ステート

名前	利用用途
Initial	HA 情報構成機器の「初期状態」
Active	HA 変換構成機器において、トラフィック処理を行う「ステータス」
Passive	HA 変換構成機器において、トラフィック処理を行う「Active」機器側と「セッション同期」を行う「バックアップ機」の「ステータス」
Non-functional	Active 機/Passive 機で「Link Failure」、「Path Failure」、「Data-Plane Failure」が検出された場合に、この「ステータス」となる。
Suspended	HA 変換構成において、管理上「無効」にされた「ステータス」

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

14.2. Panorama 手動フェイルバック

Active 機側のステータスを「Primary(Secondary)-Suspended」に変更して系統を切り戻す手順を記載します。主系が障害復旧し 1 号機側のステータスが「Primary-passive」、2 号機側のステータスが「Secondary-active」の状態から系統を切り戻す手順を記載します。

(HA の「ステータス」については、「表 14-2-1」を参照)

- 2 号機で、「Panorama」タブ > 「高可用性」> 「操作コマンド」の「Suspend Local Panorama for high availability」をクリックし、「OK」ボタンをクリックします。

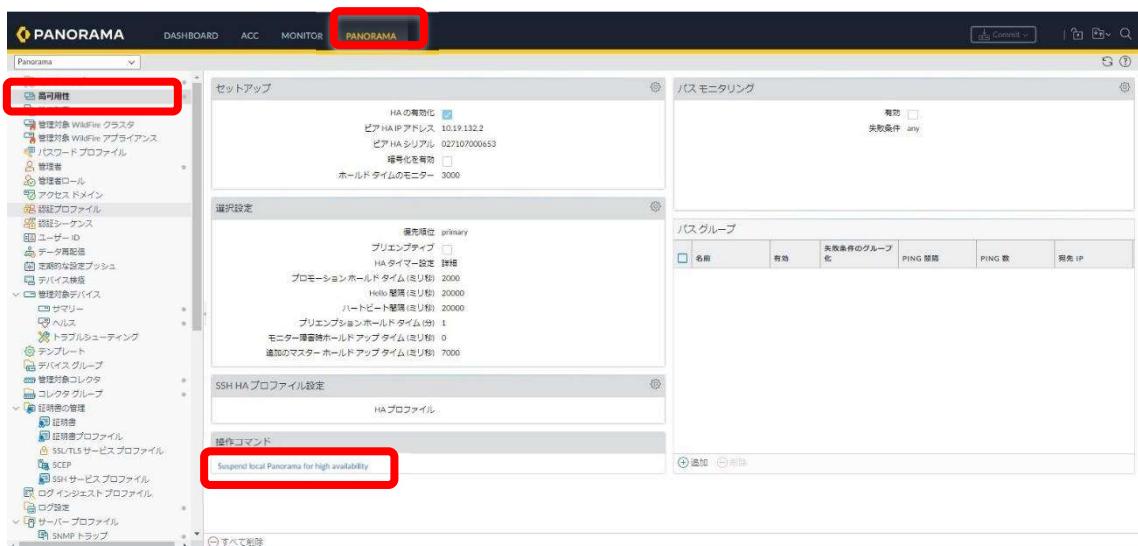


図 14-2-1 Panorama M-300 HA FailBack



図 14-2-2 Panorama M-300 HA FailBack

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 2号機側で、「Dashboard」タブ > 「高可用性」をクリックし、「local」ステータスが「secondary-suspended(User requested)」に、「ピア」ステータスが「Primary-active」なっていることを確認します。

The screenshot shows the Panorama M-300 interface. The 'DASHBOARD' tab is selected. In the 'High Availability' section, the 'Local' status is shown as 'secondary-suspended (User requested)' and the 'Peer' (IP 10.96.64.2) status is 'Primary-active'. Other sections like 'Synchronization', 'Application Version', 'AntiVirus Version', 'Panorama Version', and 'HA1' show 'Match' or 'Up' status. On the right, there are log panels for 'Login Log', 'Data Log', and 'System Log'.

図 14-2-3 Panorama M-300 HA FailBack

- ③ 1号機側で、「Dashboard」タブ > 「高可用性」をクリックし、「Local」ステータスが「primary-active」に、「ピア」ステータスが「Secondary-suspended」になっていることを確認します。

This screenshot is identical to Figure 14-2-3, showing the Panorama M-300 interface with the 'DASHBOARD' tab selected. The 'High Availability' section shows the 'Local' status as 'primary-active' and the 'Peer' (IP 10.96.64.2) status as 'Secondary-suspended (User requested)'. The other status indicators remain the same. The right side displays the same log panels.

図 14-2-4 Panorama M-300 HA FailBack

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 2号機側で、「Panorama」タブ > 「高可用性」> 「操作コマンド」> 「Make local Panorama functional for high availability」をクリックします。

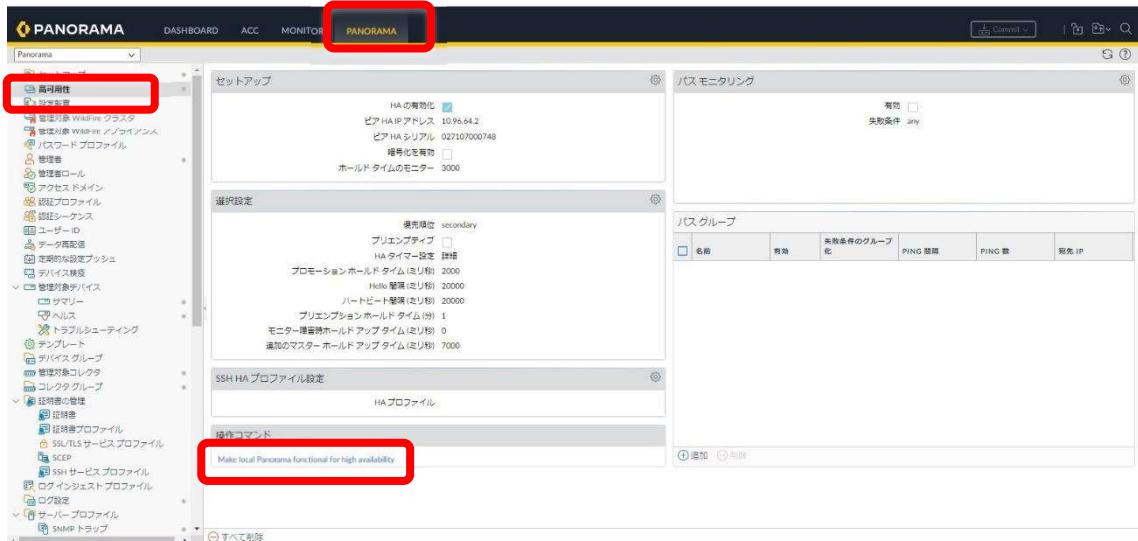


図 14-2-5 Panorama M-300 HA FailBack

- ⑤ 2号機側で、「Dashboard」タブ > 「高可用性」にて、「Local」ステータスが「secondary-passive」に、「ピア」ステータスが「Primary-active」であることを確認します。

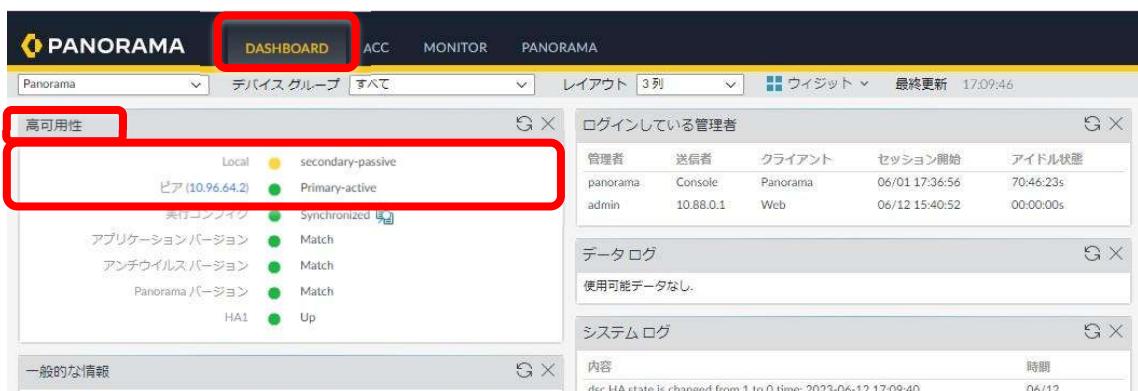


図 14-2-6 Panorama M-300 HA FailBack

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 1号機側で、「Dashboard」タブ > 「高可用性」にて、「Local」ステータスが「primary-active」に、「ピア」ステータスが「Secondary-passive」であることを確認します。

図 14-2-7 Panorama M-300 HA FailBack

表 14-2-1 HA ステート

名前	利用用途
primary(seconday)-active	HA冗長構成機器において、主系機器の「ステータス」
primary(seconday)-passive	HA冗長構成機器において、副系機器の「ステータス」
primary(seconday)-suspended	HA冗長構成において、管理上「無効」にされた「ステータス」

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

15. ファイアウォール脅威ログ確認

この項では脅威ログの確認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

15. 1. 脅威ログ確認

脅威ログを確認する方法を記載します。（PA-5450、M-300 共通）

- ① 「Monitor」タブ > 「ログ」> 「脅威」をクリックします。

図 15-1 M-300 Threat Log

- ② (A)の部分は記録されている各ログを選択する部分となり、ログリストの「閲覧（虫眼鏡マーク）」をクリックすると詳細項目が表示されます。

図 15-2 M-300 Threat Log

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 15-1 Threat ログ

図中番号	名前	利用用途
(1)	ルール	「ポリシー名」
(2)	IP プロトコル	「サービス」
(3)	生成日時	ログが生成された日時
(4)	送信元	「送信元アドレス」
(5)	ポート	「送信元ポート」
(6)	ゾーン	「送信元ゾーン」
(7)	脅威タイプ 脅威名	「脅威タイプ」 「脅威名」
(8)	重大度	「ログ」の重要度
(9)	宛先	「宛先アドレス」
(10)	ポート	「宛先ポート」
(11)	ゾーン	「宛先ゾーン」

③ 脅威ログの詳細項目が表示されます。

図 15-3 M-300 Threat Log

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

16. グループ会社の NAT 前アドレス確認

この項では、グループ会社の NAT 前アドレスの確認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

16. 1. グループ会社の NAT 前アドレス確認

トラフィックログからグループ会社の NAT 前アドレスを確認する手順を記載します。

(PA-5450、M-300 共通)

- 「Monitor」タブ > 「ログ」> 「トラフィック」をクリックします。

図 16-1 M-300 Traffic Log

- 「+」ボタンをクリックします。

(「+」ボタンにカーソルを合わせると「フィルタの追加」と表示されます。)

図 16-2 M-300 Traffic Log

- 「ログフィルタの追加」画面で、「結合子」、「属性」、「演算子」、「値」を選択し、「追加」及び「適用」ボタンをクリックします。（「属性」でグループ会社の「グループ会社送信元ゾーン」を指定します）

(フィルタ条件（属性）については「表 16-1」を参照)

図 16-3 M-300 Traffic Log

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

ログ フィルタの追加

フィルタビルダーを使ってフィルターを入力あるいは追加してください。

結合子	属性	演算子	値
and	送信元カテゴリ	equal	
or	送信元ゾーン	次の値と等しくない	
	送信元ダイナミック アドレス グループ		
	送信元プロファイル		
	送信元ホスト		
	送信元ポート		
<input type="checkbox"/> Negate			

追加 適用 閉じる

図 16-4 M-300 Traffic Log

ログ フィルタの追加

フィルタビルダーを使ってフィルターを入力あるいは追加してください。

結合子	属性	演算子	値
and	送信元カテゴリ	equal	
or	送信元ゾーン	次の値と等しくない	SHD_G_Trust
	送信元ダイナミック アドレス グループ		
	送信元プロファイル		
	送信元ホスト		
	送信元ポート		
<input type="checkbox"/> Negate			

追加 適用 閉じる

図 16-5 M-300 Traffic Log

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 16-1 Add Log Filter 「属性」例（抜粋）

番号	名前	利用用途
(1)	アクション	ログが表示された通信の「アクション」
(2)	送信元アドレス	ログが表示された通信の「送信元アドレス」
(3)	送信元ポート	ログが表示された通信の「送信元ポート」
(4)	送信元ゾーン	ログが表示された通信の「送信元ゾーン」
(5)	送信元インターフェース	ログが表示された通信の「送信元インターフェース」
(6)	宛先アドレス	ログが表示された通信の「宛先アドレス」
(7)	宛先ポート	ログが表示された通信の「宛先ポート」
(8)	宛先ゾーン	ログが表示された通信の「宛先ゾーン」
(9)	宛先インターフェース	ログが表示された通信の「宛先インターフェース」
(10)	ルール	ログが表示された通信を検知した「FWポリシーID」
(11)	セッション終了理由	ログが表示された通信の「セッション終了理由」

④ 「ログビュー」にフィルタが表示された後、「→」ボタンをクリックします。

（「→」ボタンにカーソルを合わせると、「フィルタの適用」と表示されます）

The screenshot shows the PANORAMA interface with the 'MONITOR' tab selected. In the search bar, the query '(zone.src eq SHD_G_Trust)' is entered. Below the search bar, there is a table with columns: 生成日時 (Timestamp), タイプ (Type), 送信元ゾーン (Source Zone), 宛先ゾーン (Destination Zone), 送信元 (Source), 送信元ユーザー (Source User), 送信元ダイナミックアドレスグループ (Dynamic Address Group), 宛先 (Recipient), 宛先ダイナミックアドレスグループ (Dynamic Address Group), 動的ユーザーグループ (Dynamic User Group), 宛先ポート (Recipient Port), アプリケーション (Application), and アクション (Action). A red box highlights the '→' button at the top right of the table.

図 16-6 M-300 Traffic Log

⑤ ログリストの「閲覧（虫眼鏡マーク）」をクリックします。

（※ログリストの「閲覧（虫眼鏡マーク）」をクリックすると、ログの詳細部分が表示されます）

The screenshot shows the PA-5450 interface with the 'MONITOR' tab selected. In the search bar, the query '(zone.src eq SHD_G_Trust)' is entered. Below the search bar, there is a detailed log table. One specific log entry is highlighted with a red box around its magnifying glass icon. The log table has columns: 生成日時 (Timestamp), タイプ (Type), 送信元ゾーン (Source Zone), 宛先ゾーン (Destination Zone), 送信元 (Source), 送信元ユーザー (Source User), 送信元ダイナミックアドレスグループ (Dynamic Address Group), 宛先 (Recipient), 送信元ユーザーグループ (Dynamic User Group), 宛先ポート (Recipient Port), アプリケーション (Application), and アクション (Action). The highlighted log entry shows a timestamp of '08/07/21 21:57' and a type of 'end'. The magnifying glass icon is located in the 'アクション' (Action) column of this row.

図 16-7 M-300 Traffic Log

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 16-2 Traffic ログ

図中番号	名前	利用用途
(1)	送信元	ログが表示された通信の「NAT 実施前の送信元アドレス」
(2)	NAT IP NAT ポート	ログが表示された通信の「NAT 実施後の送信元アドレス」 ログが表示された通信の「NAT 実施後の送信元ポート」

⑥ ログ詳細画面の「送信元」のアドレスを確認します。

PCAP	受信日時	タイプ	アプリケーション	アクション	ルール	ルール UUID	バイト	最大値	カテゴリ	URL カテゴリ	対応	URL	ファイル名
	2023/06/07 21:26:57	end	dns-base	allow	SHD_G_Trust,SHD_G_Untrust_0041	399bc256-4033-4749-b6b4-a447a777ad04	any						

図 16-8 M-300 Traffic Log

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. シグネチャ更新確認

この項では、シグネチャ更新の確認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

1.7. 1. UTM シグネチャ更新確認

UTM のシグネチャ更新状況や更新時期を確認する手順を記載します。

UTM の運用は JSOC にて実施しています。シグネチャの更新、チューニング（有効/無効化、適用シグネチャの変更など）が必要になった場合は、JSOC への依頼をお願いします。

※シグネチャの更新、チューニング時に通信への影響はありません。

表 17-1-1 UTM シグネチャ更新

図中番号	名前	利用用途
(1)	最終チェック	最後にシグネチャの更新有無を確認した時刻
(2)	スケジュール	シグネチャの自動更新確認の時期
(3)	現在インストール済み	現在インストールされているシグネチャ

① 「Device」タブ > 「ダイナミック更新」を選択します。

(各確認項目は「表 17-1-1」を参照)

図 17-1-1 PA-5450 UTM Signature

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

17.2. PAN-DB 更新確認

PAN-DB の更新状況や更新時期を確認する手順を記載します。

- ① 「Monitor」タブ > 「システム」をクリックします。
- ② 「ログビュー」に「 subtype eq url-filtering 」でフィルタを実施します。
(確認項目は「表 17-2-1」を参照)

表 17-2-1 PAN-DB 更新確認

図中番号	フィールド	詳細
(1)	受信時間	事象発生時間
(2)	タイプ	イベントの一般的分類
(3)	重大度	重要度
(4)	イベント	発生している特定イベント
(5)	内容	説明

受信日時	タイプ	重大度	イベント	オブジェクト	内容
01/31 13:03:36	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/31 09:03:36	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/31 05:03:35	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/31 01:03:34	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/30 21:03:33	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/30 17:03:32	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/30 13:03:31	url-filtering	informational	url-backup-seed-success	url-backup-seed-success	Backup of PAN-DB finished successfully.
01/30 09:14:49	url-filtering	informational	url-engine-starts		PAN-DB engine started.
01/30 09:14:49	url-filtering	informational	url-engine-starts		PAN-DB engine is starting..
01/30 09:14:49	url-filtering	informational	upgrade-url-database-success		PAN-DB was upgraded to version 0000.00.00.00.
01/30 09:14:49	url-filtering	informational	url-backup-seed-success		Backup of PAN-DB finished successfully.
01/30 09:14:49	url-filtering	informational	starts-from-backup-seed		Starting with backup seed.
01/29 16:36:57	url-filtering	informational	url-engine-starts		PAN-DB engine started.
01/29 16:36:57	url-filtering	informational	url-engine-starts		PAN-DB engine is starting..

図 17-2-1 PAN-DB Update Check

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

「Failed」となり、ダウンロードできない場合は、
以下「show url-cloud status」の表示結果と「2.4. 1. ブラウザによる問題のトラブルシューティングに必要なログ」を取得し、問い合わせをしてください。

```
admin@ホスト名> show url-cloud status
PAN-DB URL Filtering
License : valid
Current cloud server : s0500.urlcloud.paloaltonetworks.com
Cloud connection : connected
Cloud mode : public
URL database version - device : 20171219.40121
URL database version - cloud : 20171219.40121 (last update time 2017/12/20
19:07:00)
URL database status : good
URL protocol version - device : pan/0.0.2
URL protocol version - cloud : pan/0.0.2
Protocol compatibility status : compatible
```

図 17-2-2 CLI Normal

```
admin@ホスト名> show url-cloud status
PAN-DB URL Filtering
License : valid
Cloud connection : not connected
URL database version - device : 20171213.40036
URL protocol version - device : pan/0.0.2
```

図 17-2-3 CLI Failed

※Passive 機では「not connected」の表示ですが、正常な状態です。

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

18. ログ管理

この項では、ログの閲覧、検索方法、意味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

1.8. 1. 時刻同期確認

CLI による時刻同期確認方法(PA-5450、M-300 共通)

- ① show ntp コマンド実行します。
- ② status が synched と表示されていることを確認します。

```
admin@ホスト名> show ntp

NTP state:

  NTP synched to 10.96.0.62
    NTP server: 10.96.0.62
      status: synched
      reachable: yes
      authentication-type: none

  NTP server: 10.19.128.62
    status: available
    reachable: yes
    authentication-type: none
```

図 1.8-1-1 NTP Sync

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

18.2. ログ閲覧/検索

ログの閲覧する手順を記載します。（PA-5450、M-300 共通）

- ① 「Monitor」タブ > 「ログ」 > 「トラフィック」タブ をクリックします。

図 18-2-1 M-300 Traffic Log

- ② 「+」ボタンをクリックします。

（「+」ボタンにカーソルを合わせると「フィルタの追加」と表示されます）

図 18-2-2 M-300 Traffic Log

- ③ 「ログフィルタの追加」画面で、「結合子」、「属性」、「演算子」、「値」を選択し、「追加」及び「適用」ボタンをクリックします。

（フィルタ条件（属性）については「表 18-2-1」を参照）

結合子	属性	演算子	値
and	ヘッドレス	所有	PCAP
or	バイト		NAT
	パケット		SSL Proxy
	フラグ		キャプティブ ポータル
	ポッドのネームスペース		プロキシ トランザクション
Negate			

図 18-2-3 M-300 Traffic Log

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 18-2-4 M-300 Traffic Log



図 18-2-5 M-300 Traffic Log

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 18-2-1 ログフィルタの追加 「属性」例（抜粋）

番号	名前	利用用途
(1)	アクション	ログが表示された通信の「アクション」
(2)	送信元アドレス	ログが表示された通信の「送信元アドレス」
(3)	送信元ポート	ログが表示された通信の「送信元ポート」
(4)	送信元ゾーン	ログが表示された通信の「送信元ゾーン」
(5)	送信元インターフェース	ログが表示された通信の「送信元インターフェース」
(6)	宛先アドレス	ログが表示された通信の「宛先アドレス」
(7)	宛先ポート	ログが表示された通信の「宛先ポート」
(8)	宛先ゾーン	ログが表示された通信の「宛先ゾーン」
(9)	宛先インターフェース	ログが表示された通信の「宛先インターフェース」
(10)	ルール	ログが表示された通信を検知した「FWポリシーID」
(11)	仮想システム名	ログが表示された通信の「仮想システム名」
(12)	セッション終了理由	ログが表示された通信の「セッション終了理由」

- ④ 「ログビュー」にフィルタが表示された後、「→」ボタンをクリックします。
 （「→」ボタンにカーソルを合わせると、「フィルタの適用」と表示されます）



図 18-2-6 M-300 Traffic Log

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

18.3. ログの意味

18.3.1. はじめに

システム内のさまざまなモジュールにおいて、管理者の注意を喚起する必要のあるイベントが発生します。これは主にシステムログ機能を介して通知されます。

18.3.2. タイプ

タイプフィールドはイベントの一般的分類を与える目的があります。

通常、イベントに関連する機能が入ります（例：routing（ルーティング）、vpn（VPN）、ha（High Availability）、等）

表18-3-1 ログフィールド

タイプフィールド値	機能名	説明
dhcp	DHCP	DHCPに関するログ
dns proxy	DNS proxy	DNS Proxyに関するログ
general	General	一般的な機器管理のためのログ
globalprotect	GlobalProtect	GlobalProtectに関するログ
ha	High Availability	冗長構成(HA)に関するログ
ntp	NTP	NTPに関するログ
pbf	Policy Base Forwarding	PBFに関するログ
port	Port	物理インターフェースの UP/Down に関するログ
pppoe	PPPoE	PPPoEに関するログ
ras	Remote Access Server	SSL-VPN利用時のユーザ認証処理プロセスに関するログ
routing	Routing	ダイナミックルーティングに関するログ
Satellite daemon	Satellite daemon	サテライトデーモンに関するログ
SSL manager daemon	SSL manager daemon	SSLマネージャーデーモンに関するログ
sslvpn	SSL VPN	SSL-VPN接続に関するログ
url-filtering	URL Filtering	URLフィルタリングに関するログ
userid	User-ID	ユーザ識別に関するログ
vpn	IPsec VPN	IPSec-VPNに関するログ
crypto	Crypto	暗号に関するログ

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

18.3.3. 重要度

各イベントは重要度に関連付きます。重要度の目的は、管理者へ緊急性とイベントの影響を通知することです。以下に各重要度度レベルの意味を説明します。

表18-3-2 Severity（重要度）

Severity	意味
Critical	<ul style="list-style-type: none"> 障害および緊急の注意を要するシグナルを示します。 広範囲にデプロイされたソフトウェアのデフォルトインストールに影響するような深刻な脅威です。サーバの root が悪用され、弱点のあるコードが広範囲の攻撃者の手に渡ることになります。 攻撃者は通常、特殊な認証資格証明や個々の被害者に関する知識を必要としません。また、標的がなんらかの特殊な機能を実行するように操作する必要もありません。
High	<ul style="list-style-type: none"> 差し迫った障害や、システム運用またはセキュリティを害する状態を示します。 重大度が Critical に変わるべき可能性があるものの、軽減要因が存在する脅威です。例)悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害サーバ数が多くなかつたりする場合です。
Medium	<ul style="list-style-type: none"> より深刻な問題に発展する可能性のある状態を示します。 影響が最小限に抑えられる小さな脅威です。例)標的に侵入することのない DoS 攻撃や、攻撃者が被害サーバと同じ LAN 上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。
Low	<ul style="list-style-type: none"> 問題の可能性があるか、問題となりえることを示します。 組織のインフラストラクチャへの影響がわずかな警告レベルの脅威です。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーや DoS の問題、情報漏洩などが発生することがあります。データ フィルタリング プロファイルの一致は、「Low」としてログに記録されます。
Informational	<ul style="list-style-type: none"> 注意を要しない、通常のシステム運用に有用な情報を伝えます。 直ちに脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベント。URL フィルタリング ログエントリは Informational としてログに記録されます。

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

18.3.4. オブジェクト

オブジェクトフィールドの目的は、イベントに何かしら関係するコンフィグレーションを付与することです。

例) 特定の SSL-VPN ポータルに関するイベントが起きた場合、object フィールドにはそのオブジェクトが表され、そのポータルに関係するすべてのイベントを迅速にフィルタできるようにします。この情報としてはインターフェース名、デバイス名（Panorama の場合）、VR 名などがあります。

18.3.5. イベント

Event フィールドはイベントごとに一意で、発生している特定イベントを表示します。

詳細情報ですがイベントに関するオブジェクトや値は含みません。

例) sslvpn-auth-succ や sslvpn-auth-fail という SSL VPN 認証のイベントなどがあります。認証プロファイルやユーザに関する情報は object や description フィールドに出力されます。

18.3.6. 内容

イベントの説明には実際の事象に関連するすべての詳細が含まれます。認証されたユーザの送信元 IP アドレスやアップロードされたファイルのファイル名のような詳細情報が付与されます。簡単に理解できる文章の中に object や event フィールドの情報が再表示される場合もあります。Description フィールドは約 80 文字を超えないように作られています。これは厳格な制限ではありません。実際のフィールドサイズはさらに大きいですが、これより長いメッセージは値が追加された場合に限ります。

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

1.8.3.7. システム単位の詳細イベント

※斜体は任意の文字列です。

表 1.8-3-3 General

タイプ	重要度	イベント	内容	意味
general	informational	auth-fail	User' < <i>admin_user</i> > failed authentication. Reason: < <i>reason</i> >	管理ユーザが PAN デバイスへのログイン認証に失敗しました。 < <i>admin_user</i> > 管理ユーザ名 < <i>reason</i> > 失敗した理由
general	informational	authsuccess	User' < <i>admin_user</i> > authenticated.	管理ユーザが PAN デバイスへのログイン認証に成功しました。 < <i>admin_user</i> > 管理ユーザ名
general	informational	general	< <i>serial_number</i> > Connected	Panorama にシリアル番号が < <i>serial_number</i> > の管理デバイスが接続されました。 本メッセージは Panorama の system log でのみ表示されます。 Panorama と接続が確立した時、PAN デバイスには "Connected to Panorama Server:< <i>ip_address</i> > Port:< <i>port_number</i> >" というメッセージが表示されます。
general	critical	general	< <i>number</i> > of < <i>total_number</i> > dataplane processor cores failed verification.	データプレーンのプロセッサコア (< <i>total_number</i> > 個中の < <i>number</i> > 番) が識別に失敗しました。
general	high	general	< <i>serial_number</i> > Disconnected	シリアル番号 < <i>serial_number</i> > の管理デバイスが Panorama から切断されました。 本メッセージは Panorama の system log でのみ表示されます。
general	informational	general	< <i>value</i> > is not present	< <i>value</i> > が存在しません。

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

general	medium	general	< <i>admin_user</i> > failed to download content version < <i>version</i> > < <i>reason</i> >	管理ユーザが実施したコンテンツバージョン < <i>version</i> > のダウンロードが失敗しました。理由は< <i>reason</i> > です。 < <i>admin_user</i> > ダウンロードを行った管理ユーザ名 < <i>version</i> > コンテンツバージョン < <i>reason</i> >失敗した理由
general	informational	general	[CRL] Certificate < <i>certificate</i> > is revoked	CRL (Certificate Revocation List) 内の証明書 < <i>certificate</i> > は失効されました。
general	informational	general	[CRL] Certificate < <i>certificate</i> > has illegal URL: < <i>url</i> >	証明書 < <i>certificate</i> > を確認するCRL (Certificate Revocation List) の URL が不正でした。 < <i>url</i> >不正な CRL の URL
general	informational	general	[OCSP] Certificate < <i>certificate</i> > is revoked: depth:< <i>depth</i> >	OCSP (Online Certificate Status Protocol) によりチェックされた証明書 < <i>certificate</i> > は失効されました。 < <i>depth</i> > 証明書チェーンの階層
general	informational	general	[OCSP] Certificate < <i>certificate</i> > status is < <i>status</i> >;depth:< <i>depth</i> >	OCSP でチェックされる証明書 < <i>certificate</i> > の状態は < <i>status</i> > でした。 < <i>depth</i> > 証明書チェーンの階層
general	informational	general	[OCSP] Certificate < <i>certificate</i> > has illegal URL: < <i>url</i> >	証明書 < <i>certificate</i> > をチェックする OCSP サーバの URL が不正でした。 < <i>url</i> > 不正な OCSP サーバの URL
general	informational	general	Accepted keyboard-interactive/pam for < <i>admin_user</i> > from < <i>ip_address</i> > port < <i>port_number</i> > ssh2	PANOS が SSH 接続に対して keyboard-interactive/pam を管理ユーザに対して承認しました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >管理ホストの IPアドレス < <i>port_number</i> >SSH のポート番号

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

general	high	general	all_pktproc< <i>number</i> >: exiting because missed too many heartbeats	一定量の内部的なハートビートを処理できなかったため、パケット処理プロセスを終了しました。（バグが考えられる） < <i>number</i> >プロセス番号
general	medium	general	Anti virus package upgraded from version < <i>old_version</i> > to < <i>new_version</i> > by < <i>admin_user</i> >	管理ユーザ < <i>admin_user</i> > または Panorama によりアンチウイルスパッケージが < <i>old_version</i> > から < <i>new_version</i> > へアップグレードされました。 < <i>admin_user</i> > 管理ユーザ名 または "Panorama" < <i>old_version</i> > 前回インストールされていたアンチウイルスパッケージ < <i>new_version</i> > 現在インストールされているアンチウイルスパッケージ
general	informational	general	Anti-virus image < <i>file_name</i> > deleted by < <i>admin_user</i> >	管理ユーザ< <i>admin_user</i> >によりアンチウイルスイメージが削除されました< <i>file_name</i> >アンチウイルスイメージ。
general	medium	general	Antivirus installation could not be scheduled	アンチウイルスのインストールがスケジュールされていません。“Device > Dynamic Update >Anti-Virus” の Schedule が “Download but do not install” に設定されている場合に表示されます
general	medium	general	Antivirus package downloaded but installation could not be scheduled	アンチウイルスパッケージがダウンロードされましたがインストールがスケジュールされていません。
general	high	general	AntiVirus update job Failed	アンチウイルスアップデートジョブが失敗しました。
general	high	general	AntiVirus update job Succeeded	アンチウイルスアップデートジョブが成功しました。
general	high	general	AntiVirus update job succeeded for user < <i>admin_user</i> >	管理ユーザ< <i>admin_user</i> >が実施したアンチウイルスアップデートジョブが成功しました。 < <i>admin_user</i> >は表示されない場合もあります
general	informational	general	Antivirus version < <i>version</i> > downloaded by Auto update agent	アンチウイルスシグネチャのバージョン< <i>version</i> >が自動アップデートエージェントによりダウンロードされました。 < <i>version</i> > AV シグネチャのバージョン

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

general	medium	general	Anti-virus version <version> installed by <admin_user>	管理ユーザ<admin_user>によりアンチウイルスシグネチャのバージョン<version>がインストールされました。 <version> AV シグネチャのバージョン。
general	medium	general	Application Identification package upgraded from version <old_version> to <new_version> by <admin_user>	管理ユーザ <admin_user>により App-ID パッケージが <old_version>から <new_version>へアップグレードされました。 <old_version>前回インストールされていた App-ID パッケージ<new_version>今回インストールされたバージョンの新しいApp-ID パッケージ
general	high	general	Attempted to fix partition <partition>. If any problems are encountered it is advisable to update this partition	パーティション<partition>の修正を試みました。問題が起きるようであればパーティションをアップデートしてください。
general	medium	general	Authorization failed for user <admin_user> via Web from <ip_address> : <reason>	WebUI 経由で設定実施した管理ユーザの権限がありません。 <admin_user>管理ユーザ名 <ip_address>管理ユーザのアクセス元 IP アドレス <reason>
general	medium	general	Authorization failed for user <admin_user> via CLI from <ip_address> : <reason>	CLI 経由で設定実施した管理ユーザの権限がありません。 <admin_user>管理ユーザ名 <ip_address>管理ユーザのアクセス元 IP アドレス <reason>理由
general	high	general	Auto update agent failed to download content version <version>	Auto update agent が実施したコンテンツバージョン<version>のダウンロードが失敗しました。
general	high	general	Auto update agent failed to download new Content	Auto update agent が実施した新コンテンツパッケージのダウンロードが失敗しました。
general	informational	general	Auto update agent failed to fetch license information:	Auto update agent が実施したライセンス情報のフェッチが失敗しました。

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

			<i><information></i>	
general	high	general	Autocommit job failed	自動コミットジョブが失敗しました。
general	high	general	Autocommit job succeeded	自動コミットジョブが成功しました。 自動コミットジョブはブート時に実行されます。
general	high	general	Autocommit job succeeded for user <i><admin_user></i>	管理ユーザ <i><admin_user></i> が実施した自動コミットジョブが成功しました。 <i><admin_user></i> は表示されない場合もあります。
general	informational	general	Candidate configuration loaded from <i><file_name></i> by <i><admin_user></i>	<i><file_name></i> という名前のxmlファイルがcandidate configurationとして管理ユーザ <i><admin_user></i> によってロードされました。
general	informational	general	candidate configuration synchronized with HA peer by <i><admin_user></i>	管理ユーザ <i><admin_user></i> によってcandidate configurationがHA ピアと同期されました。 本メッセージが表示されたデバイスからHA ピアへコンフイグを転送しました。 CLI コマンド "request high-availability sync-to-remote candidate-config" を実施すると本メッセージが表示されます。
general	critical	general	Chassis Master Alarm: <i><alarm_name></i>	PANデバイス筐体の LEDアラームが点灯しました。 <i><alarm_name></i> LEDアラームの種類。"Power Supply"電源アラーム。"HA-event" HA イベントのアラーム。 HA 切替えが起きた場合に点灯。"Fans"ファンのアラーム。ファンの回転数が異常になった場合に点灯。

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

general	critical	general	Chassis Master Alarm: Cleared	PANデバイス筐体の LEDアラームがクリアされました。 どのアラームかは表示されないので、本メッセージ以前に表示された"Chassis Master Alarm: < <i>alarm_name</i> >" メッセージによりアラーム種別を特定してください。
general	high	general	Commit job failed	コミットジョブが失敗しました。
general	high	general	Commit job failed for user < <i>admin_user</i> >	管理ユーザ< <i>admin_user</i> > が実施したコミットジョブが失敗しました。
general	informational	general	Commit job succeeded	コミットジョブが成功しました。CLI コマンド"commit" (config モード) を入力するか、WebUI で"commit" をクリックするとコミットジョブが開始されます。
general	informational	general	Commit job succeeded for user < <i>admin_user</i> >	管理ユーザ< <i>admin_user</i> > が実施したコミットジョブが成功しました。
general	informational	unknown	Config installed	コンフィグレーションがインストールされました。
general	informational	general	configuration sync'd with HA peer	HA ピアとコンフィグが同期されました。
general	informational	general	Connected to Pan-Agent: IP< <i>ip_address</i> > port < <i>port_number</i> >vsys< <i>vsys_id</i> >	IP アドレス< <i>ip_address</i> > 上の PanAgent にポート番号< <i>port_number</i> > で接続しました。vsys は< <i>vsys_id</i> > です。
general	informational	general	Connected to Panorama Server: < <i>ip_address</i> > Port: < <i>port_number</i> >	IP アドレス < <i>ip_address</i> > のPanorama サーバにポート番号< <i>port_number</i> > で接続しました。 < <i>ip_address</i> >Panorama の IP アドレス < <i>port_number</i> >Panoramaのポート番号
general	high	general	Connection to CMS disabled by< <i>admin_user</i> >	CMS (Central Management Server; Panorama) へのコネクションが管理ユーザ< <i>admin_user</i> >により無効になりました。

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

general	high	general	Connection to CMS enabled by < <i>admin_user</i> >	CMS (Central Management Server; Panorama)へのコネクションが管理ユーザ < <i>admin_user</i> >により有効になりました。
general	informational	general	Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by < <i>ip_address</i> >	PAN デバイスの管理ポートアドレス < <i>ip_address</i> >から接続されたアップデートサーバへのコネクションが成功しました。
general	informational	general	Content image < <i>file_name</i> > deleted by < <i>admin_user</i> >	管理ユーザ < <i>admin_user</i> >によりコンテンツイメージが削除されました。 WebUI の "Device > Dynamic Update > Application and Threats" テーブルにてダウンロードまたはアップロード済みのコンテンツバージョンについて x マークをクリックして削除すると本メッセージが表示されます。 < <i>admin_user</i> >コンテンツイメージを削除した管理ユーザ名 < <i>file_name</i> >コンテンツイメージのファイル名
general	informational	general	Content image transferred from peer	HA 構成においてピアからコンテンツイメージが転送されました。
general	medium	general	Content package downgraded from version < <i>prev_version</i> > to < <i>new_version</i> > by < <i>admin_user</i> >	管理ユーザ < <i>admin_user</i> >により、コンテンツパッケージのバージョンが < <i>prev_version</i> >から < <i>new_version</i> >へダウングレードされました。 < <i>prev_version</i> >前回インストールされていたコンテンツパッケージバージョン < <i>new_version</i> >現在インストールされているコンテンツパッケージバージョン
general	medium	general	Content package downloaded but installation could not be scheduled	コンテンツパッケージがダウンロードされましたがインストールがスケジュールされていません。 "Device > Dynamic Updates > Application and Threats"

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”Schedule” が”Download but do not install”的場合に、スケジュールに従って新しいパッケージをダウンロードし、インストールは行いませんでした。
general	high	general	Content update job Failed	コンテンツアップデートジョブが失敗しました。
general	high	general	Content update job succeeded for user < <i>admin_user</i> >	管理ユーザ < <i>admin_user</i> > が実施したコンテンツアップデートジョブが成功しました。 < <i>admin_user</i> > コンテンツアップデートジョブを実施した管理ユーザ 表示されない場合もあります。
general	informational	general	Content version < <i>version</i> > downloaded by Auto update agent	コンテンツ (Application and Threat) のバージョン < <i>version</i> > が自動アップデートエージェントによりダウンロードされました。 < <i>version</i> > コンテンツパッケージのバージョン
general	medium	general	Content version < <i>version</i> > installed by < <i>admin_user</i> >	コンテンツバージョン < <i>version</i> > が管理ユーザ < <i>admin_user</i> > によってインストールされました。
general	high	general	Dataplane is now up	データプレーンがアップしました。
general	high	general	Dataplane restart requested by < <i>admin_user</i> >	管理ユーザによりデータプレーンのリスタートが要求されました。 < <i>admin_user</i> > リスタートを行った管理ユーザ名 ”Device > Restart Dataplane”をクリックしてデバイスをリブートさせるか、CLI コマンド “request restart dataplane” コマンドを実施すると本メッセージが表示されます。
general	high	general	Daily packet capture limit (directory threat/< <i>directorynumber</i> >) has been reached.	一日ごとのパケットキャプチャ制限値に達しました。 < <i>directory</i> > パケットキャプチャを格納しているディレクトリ名。 < <i>number</i> > パケットキャプチャ制限量

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

general	high	general	Deployment job download antivirus job failed	Panorama が実施したアンチウイルスシグネチャのダウンロードジョブが失敗しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job download antivirus job succeeded	Panorama が実施したアンチウイルスシグネチャのダウンロードジョブが成功しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job download content job failed	Panorama が実施したコンテンツ (Threat Prevention シグネチャ) のダウンロードジョブが失敗しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job download content job succeeded	Panorama が実施したコンテンツ (Threat Prevention シグネチャ) のダウンロードジョブが成功しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job download system software job failed	Panorama が実施したPANOS ソフトのダウンロードジョブが失敗しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job download system software job succeeded	Panorama が実施したPANOS ソフトのダウンロードジョブが成功しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job install <file_name> to <device_name> failed.	ファイル <file_name> を管理デバイス <device_name> へインストールするジョブが失敗しました。 本メッセージは Panorama のsystem log でのみ表示されます。
general	high	general	Deployment job install <file_name> to <device_name> succeeded.	ファイル <file_name> を管理デバイス <device_name> へインストールするジョブが成功しました。 本メッセージは Panorama のsystem log でのみ表示されます。

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

general	high	general	Deployment job update licenses for < <i>device_name</i> > failed.	Panorama が実施したデバイス名 < <i>device_name</i> >に対するライセンスアップデートのジョブが失敗しました。 本メッセージは Panorama の system log でのみ表示されます。 < <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job update licenses for < <i>device_name</i> >succeeded.	Panorama が実施したデバイス名 < <i>device_name</i> >に対するライセンスアップデートのジョブが成功しました。 本メッセージは Panorama の system log でのみ表示されます。 < <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job upload antivirus to < <i>device_name</i> > failed	Panorama が実施した管理デバイス < <i>device_name</i> >へのアンチウイルスシグネチャのアップロードジョブが失敗しました。 本メッセージは Panorama の system log でのみ表示されます。 < <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job upload antivirus to < <i>device_name</i> > succeeded	Panorama が実施した管理デバイス < <i>device_name</i> >へのアンチウイルスシグネチャのアップロードジョブが成功しました。 本メッセージは Panorama の system log でのみ表示されます。 < <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job upload content to < <i>device_name</i> > failed	Panorama が実施した管理デバイス < <i>device_name</i> >へのコンテンツ (Threat Prevention シグネチャ) のアップロードジョブが失敗しました。 本メッセージは Panorama の system log でのみ表示されます。 < <i>device_name</i> > Panorama で設定した管理デバイス名

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

general	high	general	Deployment job upload content to < <i>device_name</i> > Succeeded	Panorama が実施した管理デバイス< <i>device_name</i> >へのコンテンツ (Threat Prevention シグネチャ) のアップロードジョブが成功しました。本メッセージは Panorama の system log でのみ表示されます。< <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job upload software to < <i>device_name</i> > failed	Panorama が実施した管理デバイス< <i>device_name</i> >への PANOS ソフトのアップロードジョブが失敗しました。本メッセージは Panorama の system log でのみ表示されます。< <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment job upload system software to < <i>device_name</i> > Succeeded	Panorama が実施した管理デバイス< <i>device_name</i> >への PANOS ソフトのアップロードジョブが成功しました。本メッセージは Panorama の system log でのみ表示されます。< <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment manager failed to reboot device < <i>device_name</i> >	管理デバイス < <i>device_name</i> > を Panorama からリブートさせましたが失敗しました。本メッセージは Panorama の system log でのみ表示されます。< <i>device_name</i> > Panorama で設定した管理デバイス名
general	high	general	Deployment manager rebooted device < <i>device_name</i> >	管理デバイス < <i>device_name</i> > を Panorama からリブートさせました。本メッセージは Panorama の system log でのみ表示されます。< <i>device_name</i> > Panorama で設定した管理デバイス名
general	informational	general	Device requires protocol ver. < <i>version1</i> >, but < <i>ip_address</i> > supports only ver. < <i>version2</i> >	Pan-Agent のバージョン < <i>version1</i> > がデバイスで必要ですが、Pan-Agent はバージョン < <i>version2</i> > のみサポートしています。< <i>ip_address</i> > Pan-Agent がインストールされたホストの IP アドレス < <i>version1</i> > PAN デバイスが

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

				要求する Pan-Agent バージョン ⟨version2⟩現在 PAN デバイスと接続されている Pan-Agent のバージョン
general	informational	general	device-server HA queue is full	デバイスサーバの HA キューが一杯です。 HA 間通信の問題によりユーザ ID情報がパッシブ機に同期できません。
general	informational	general	Disconnected from Pan-Agent: IP ⟨ip_address⟩ port ⟨port_number⟩ vsys⟨vsys_id⟩	IP アドレス ⟨ip_address⟩ 上の Pan-Agent から切断しました。 ⟨ip_address⟩Pan-Agent の IPアドレス ⟨port_number⟩Pan-Agent のポート番号 ⟨vsys_id⟩ Pan-Agent を利用するvsys 番号
general	informational	general	Disconnected from Panorama Server: ⟨ip_address⟩	IP アドレス ⟨ip_address⟩ のPanorama サーバとの接続を切断しました。
general	high	general	Disconnecting due to possible replay attempt	リプレイ攻撃の可能性があるため切断しました。
general	high	general	Downloaded image cannot be authenticated	ダウンロードしたイメージが認証できませんでした。
general	informational	general	Failed to connect to Pan-Agent at⟨ip_address⟩	IP アドレス⟨ip_address⟩ 上のPan-Agent に接続できませんでした。
general	informational	general	Failed to connect to Panorama Server: ⟨ip_address⟩ Port: ⟨port_number⟩ Retry: ⟨retry_number⟩	IP アドレス⟨ip_address⟩の Panorama サーバへのポート番号 ⟨port_number⟩での接続が失敗しました。リトライ回数は ⟨retry_number⟩回です。
general	informational	general	Failed to connect to proxy server. Please check if proxy user name and password are correct.	プロキシサーバに接続失敗しました。プロキシユーザー名とパスワードが正しいか確認してください。
general	medium	general	Failed to downgrade content package to version ⟨version⟩ ⟨reason⟩	バージョン ⟨version⟩へのコンテンツパッケージのダウングレードが失敗しました。 ⟨version⟩ダウングレードしようとしたコンテンツパッケージのバージョン