

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

△△情報テクノロジー株式会社 御中

次期統合ファイアウォール構築業務

運用手順書（セキュリティ機器）

第 2.0 版

2023 年 11 月 7 日

KDDI 株式会社

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

改訂履歴

項番	改訂者	改訂日	版数	改訂内容
1	KDDI	2017/7/10	1.0	初版発行
2	KDDI	2018/3/9	1.1	<p>「図 2 – 1 – 2 . PA-5060 背面図」 (9) を追加 「3. 1. 2. SSH 接続方法 (PA-5060、M-500 共通)」接続先 IP アドレスについて文言修正 (管理インターフェースで統一) 「3. 2. 1. GUI による接続方法 (PA-5060)」接続先 IP アドレスについて文言修正 (管理インターフェースで統一) 「3. 2. 2. GUI による接続方法 (M-500)」接続先 IP アドレスについて文言修正 (管理インターフェースで統一) 「オペレーションモード」「コンフィグレーションモード」の用語集追加 「コンフィグレーションモードからオペレーションモードに戻るコマンド」を追記 「図 3 – 2 – 1 1 . Language 変更後」に本書では英文表記であることを追加 「3. 3. 1. PA-5060」起動時に電源ケーブルが接続されていれば、一度抜線することを追記 「3. 3. 1. M-500」起動時に電源ボタンを押下することを追記 「3. 5. 2. GUI による機器停止方法 (PA-5060)」③電源ケーブル抜線指示を追記 「3. 5. 3. GUI による機器停止方法 (M-500)」③電源ケーブル抜線指示を追記 「表 5 – 1 – 3 (7) Service/URL Category」の内容修正 「表 7 – 1 – 6 (3)」改行修正 「1 2. 2. Panorama 手動フェイルオーバー」大文字小文字修正 「1 3. 2. Panorama 手動フェイルバック」大文字小文字修正 「表 1 5 – 2 Traffic ログ」位置変更 「表 2 1 – 1 – 3 ポリシー設定」文言修正 「2 2. 2. パケットキャプチャの取</p>

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

				得手順」面一修正 誤字脱字、改行を修正 図の番号修正 表番号、図番号の統一 各章の表紙の下線長を修正 全角半角混在修正 「ください」で統一 「できます」を「します」に統一 句点修正 語尾「ですます」へ修正 「出力され」を「表示され」へ修正 「記載しております」を「記載しています」へ修正 「となります」を「です」へ修正 「例えば」「たとえば」を「例」に統一 「TeraTerm」に統一 「InterSafe」に統一
3	KDDI	2018/7/25	1.2	4. 2. 設定情報エクスポート Device_state ファイルのエクスポートを追加 6. 4. グループ会社向け NAT 設定例追加
4	KDDI	2019/5/20	1.3	以下の手順を追加 2 2. カスタムレポート作成 2 2. 1. カスタムレポート作成 2 2. 2. カスタムレポート作成例 2 2. 2. 1. 広島 DC からインターネット宛に通信した全てのトラフィックを抽出するレポート作成例 2 2. 2. 2. G 会社から吹田 DC(旧電算室)プロキシサーバ宛の URL フィルタログを抽出するレポート作成例
5	KDDI	2019/6/14	1.4	以下の手順を追加 2 3. サンドボックス (WildFire) の検査結果レポート 5. 1. 3 ポリシー設定にセキュリティプロファイルの説明を追加
6	KDDI	2019/7/18	1.5	9. ~ 1 1. SSL 復号化部分について全体的に加筆・修正
7	KDDI	2020/5/22	1.6	PAN-OS 7.1 から 8.1 へのバージョンアップに伴う全面改訂。 GUI 操作画面のキャプチャを 8.1 に変更。合わせて GUI 操作画面、メニューを日本語表記へ変更

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

8	KDDI	2021/1/25	1.7	25. スタティックルーティング追加/削除手順の追加。
9	KDDI	2023/11/7	2.0	次期統合 FW 構築に伴う修正。

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

目次

0.はじめに.....	12
0.1.本書について.....	13
0.2.本書の位置づけ.....	13
0.3.方針.....	13
0.4.用語集.....	14
0.5.VR のゾーン名一覧表.....	16
1.対応フロー.....	18
1.1.アクセス解除設定フロー.....	19
1.2.アクセスブロック設定フロー.....	20
1.3.カテゴリルール変更フロー.....	21
1.4.問い合わせ調査フロー(通信不具合).....	22
2.目次チェック.....	23
2.1.ランプ点検.....	24
2.1.1.PA-5450.....	24
2.1.2.PA-5450 前面図.....	24
2.1.3.PA-5450 背面図.....	24
2.1.4.LED 確認.....	24
2.1.5.ポート LED 確認.....	26
2.1.6.M-300 前面図.....	27
2.1.7.M-300 背面図.....	27
2.1.8.LED 確認.....	27
2.1.9.ポート LED 確認.....	28
2.2.ステータス確認.....	29
2.2.1.PA-5450.....	29
2.2.2.M-300.....	31
3.機器接続方法.....	33
3.1.CLI.....	34
3.1.1.コンソール接続方法.....	34
3.1.2.SSH 接続方法(PA-5450、M-300 共通).....	34
3.1.3.モード遷移.....	36
3.2.GUI.....	36
3.2.1.GUI による接続方法(PA-5450).....	36
3.2.2.GUI による接続方法(M-300).....	39
3.3.機器の起動.....	42

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. 3. 1. PA-5450	42
3. 3. 2. M-300	43
3. 4. 機器の再起動(リブート)	43
3. 4. 1. CLI による機器再起動方法 (PA-5450、M-300 共通)	43
3. 4. 2. GUI による再機器起動方法 (PA-5450)	44
3. 4. 3. GUI による再機器起動方法 (M-300)	45
3. 5. 機器の停止	46
3. 5. 1. CLI による機器停止方法 (PA-5450、M-300 共通)	46
3. 5. 2. GUI による機器停止方法 (PA-5450)	46
3. 5. 3. GUI による機器停止方法 (M-300)	47
4. 設定情報保存/復元	49
4. 1. 設定情報保存	50
4. 2. 設定情報エクスポート	51
4. 3. 設定情報インポート	53
4. 3. 1. 設定インポート	53
4. 3. 2. 設定ロード	54
4. 3. 3. 設定反映 (PA-5450)	55
4. 3. 4. 設定反映 (M-300)	56
5. ファイアウォールポリシー追加/修正/削除	60
5. 1. ファイアウォールポリシー追加	61
5. 1. 1. アドレス設定	61
5. 1. 2. サービス設定	62
5. 1. 3. ポリシー設定	64
5. 1. 4. ポリシー移動	70
5. 1. 5. 設定反映	70
5. 2. ファイアウォールポリシー修正	72
5. 3. ファイアウォールポリシー削除	74
6. NAT ポリシー追加/修正/削除	76
6. 1. NAT ポリシー追加	77
6. 1. 1. アドレス設定	77
6. 1. 2. ポリシー設定	78
6. 1. 3. ポリシー移動	83
6. 1. 4. 設定反映	83
6. 2. NAT ポリシー修正	84
6. 3. NAT ポリシー削除	86
6. 4. グループ会社向け NAT 設定例	88

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. 1. グループ会社セグメントの NAT 修正例.....	88
6. 4. 2. グループ会社/本体の公開サーバの NAT 追加、修正例	92
6. 4. 3. グループ会社参照プロキシサーバの変更方法.....	102
7. URL フィルタリングポリシー修正/追加/削除	105
7. 1. 1. URL フィルタリングログ確認方法.....	106
7. 1. 2. URL プロファイル修正.....	108
7. 1. 2. 1. 全社アクセス解除/全社ブロック(CLI 含む).....	108
7. 1. 2. 2. 本体アクセス解除/本体ブロック(CLI 含む).....	114
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).....	116
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).....	118
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).....	119
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).....	120
7. 1. 3. URL プロファイル追加.....	121
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).....	124
7. 1. 4. URL フィルタリングをポリシーに追加.....	125
7. 1. 5. URL プロファイル削除.....	137
7. 1. 6. カテゴリ修正.....	141
7. 1. 6. 1. 全社カテゴリ許可/全社カテゴリブロック.....	141
7. 1. 6. 2. 本体カテゴリ許可/本体カテゴリブロック.....	147
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.....	148
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.....	152
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.....	153
7. 1. 7. カスタムカテゴリ追加.....	154
7. 1. 8. カスタムカテゴリ削除.....	158
7. 2. URL フィルタリングポリシー修正.....	162
7. 2. 1. 全制限端末(NB 端末)のアクセス解除／端末追加・削除.....	165
7. 3. URL フィルタリングポリシー削除.....	168
8. URL フィルタリング機能 有効化/無効化	170
8. 1. URL フィルタリング機能有効化	171
8. 1. 1. URL フィルタリング 有効化設定	171
8. 1. 2. 設定反映	173
8. 2. URL フィルタリング機能無効化	174
8. 2. 1. URL フィルタリング 無効設定	174
8. 2. 2. 設定反映	176
9. SSL 復号化設定	177
9. 1 SSL 復号化ポリシー追加/変更/削除.....	179

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. 1. SSL 復号化ポリシー追加	179
9. 1. 2. ポリシー設定	179
9. 1. 3. ポリシー移動	184
9. 1. 4. 設定反映	185
9. 2 SSL 復号化ポリシー変更	186
9. 3 SSL 復号化ポリシー削除	188
10. 0. SSL 復号化ポリシー 有効化/無効化	190
10. 1. SSL 復号化ポリシー 有効化	191
10. 1. 1. SSL 復号化ポリシー 有効設定	191
10. 1. 2. 設定反映	193
10. 2. SSL 復号化ポリシー 無効化	194
10. 2. 1. SSL 復号化ポリシー 無効設定	194
10. 2. 2. 設定反映	196
10. 3. 設定例)G 会社の SSL 復号化ポリシー 有効化	197
10. 3. 1. G 会社の SSL 復号化ポリシー 有効設定	197
10. 3. 2. 設定反映	199
11. 1. SSL フォワードプロキシ除外設定	200
11. 1. 1. SSL 復号化除外対象の確認方法	201
11. 1. 2. SSL 復号化除外用 URL カテゴリの追加	210
11. 1. 3. SSL 復号化除外用 URL カテゴリの削除	213
11. 1. 4. SSL 復号化除外用 URL の追加	215
11. 1. 5. SSL 復号化除外用 URL の削除	219
11. 1. 6. SSL 復号化除外用宛先アドレスの追加	222
11. 1. 7. SSL 復号化除外用宛先アドレスの削除	225
11. 1. 8. SSL 復号化除外用送信元アドレスの追加	228
11. 1. 9. SSL 復号化除外用送信元アドレスの削除	232
11. 1. 10. SSL 復号化除外用サービスの追加	236
11. 1. 11. SSL 復号化除外用サービスの削除	239
12. 0. SSL インバウンドインスペクション設定	242
12. 1. 1. DMZ サーバの SSL 復号化ポリシー追加	243
12. 1. 2. DMZ サーバの SSL 復号化ポリシー削除	249
13. 0. 手動フェイルオーバー	251
13. 1. Palo Alto 手動フェイルオーバー	252
13. 2. Panorama 手動フェイルオーバー	256
14. 0. 手動フェイルバック	260
14. 1. Palo Alto 手動フェイルバック	261

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	265
15. ファイアウォール脅威ログ確認	269
15. 1. 脅威ログ確認	270
16. グループ会社の NAT 前アドレス確認	272
16. 1. グループ会社の NAT 前アドレス確認	273
17. シグネチャ更新確認	277
17. 1. UTM シグネチャ更新確認	278
17. 2. PAN-DB 更新確認	279
18. ログ管理	281
18. 1. 時刻同期確認	282
18. 2. ログ閲覧/検索	283
18. 3. ログの意味	286
18. 3. 1. はじめに	286
18. 3. 2. タイプ	286
18. 3. 3. 重要度	287
18. 3. 4. オブジェクト	288
18. 3. 5. イベント	288
18. 3. 6. 内容	288
18. 3. 7. システム単位の詳細イベント	289
18. 3. 8. アプリケーションフィールドの意味	324
18. 3. 9. セッション終了理由	324
18. 4. ログアーカイブ出力	326
18. 5. ログ閲覧画面カラム変更	329
18. 6. SSL 復号化対象通信のトラフィックログをフィルタする方法	331
18. 7. サーバ証明書の問題によりロックされている通信のトラフィックログをフィルタする方法	334
19. セキュリティゾーン追加	337
19. 1. セキュリティゾーン追加	338
20. 管理者アカウント作成	339
20. 1. 管理者アカウント追加	340
20. 1. 1. 管理者アカウント追加	340
20. 2. 管理者アカウント変更	343
20. 2. 1. 管理者アカウント変更	343
20. 2. 2. 設定反映	345
20. 3. 管理者アカウント削除	346
20. 3. 1. 管理者アカウント削除	346
20. 3. 2. 設定反映	347

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

2.1. SSL 証明書のインポート/エクスポート	348
21.1. SSL 証明書のエクスポート	349
21.2. 外部ルート認証局の証明書インポート	351
21.3. DMZ サーバの証明書インポート	355
2.2. ファイアウォールポリシーによる通信制御の設定例	357
22.1. インターネットへの全ての Web アクセス(プロキシを経由)を URL フィルタリングで拒否する方法	358
22.2. インターネットへの全ての通信(プロキシを経由しない)を拒否する方法	368
22.3. 特定のプロトコルのみを拒否する方法	375
2.3. カスタムレポート作成	382
23.1. カスタムレポート作成	383
23.2. カスタムレポート作成例	388
23.2.1. 広島 DC からインターネット宛に通信した全てのトラフィックを抽出するレポート作成例	388
23.2.2. G 会社から吹田 DC(旧電算室)プロキシサーバ宛の URL フィルタログを抽出するレポート作成例	394
2.4. 障害時に取得するログ情報について	399
24.1. トラブルシューティングに必要なログ	400
24.2. パケットキャプチャの取得手順	402
2.5. スタティックルーティング追加/削除	407
25.1. スタティックルーティング追加	408
25.1.1. スタティックルーティング追加(GUI)	408
25.1.2. スタティックルーティング追加(CLI)	411
25.2. スタティックルーティング削除	413
25.2.1. スタティックルーティング削除(GUI)	413
25.2.2. スタティックルーティング削除(CLI)	416
25.3. 仮想基盤 サイト切替え/切戻し時のスタティックルーティング追加/削除一覧	417
25.4. 仮想基盤 サイト切替え/切戻し時のスタティックルーティング追加/削除 CLI	420
25.4.1. 吹田→広島サイト切替え時の手動設定(CLI)	420
25.4.2. 広島→吹田サイト切替え(25.4.1の切り戻し)時の手動設定(CLI)	421
25.4.3. 広島→吹田サイト切替え時の手動設定(CLI)	421
25.4.4. 吹田→広島サイト切替え(24.4.3の切り戻し)時の手動設定(CLI)	427
25.5. 広島 DC と吹田 DC(旧電算室)のサイト切替えの留意点	432
2.6. アプリケーション識別機能	435
26.1. アプリケーション識別機能	436
2.7. URL フィルタリングログ転送カテゴリ追加/削除	437
27.1. ログ管理サーバで URL フィルタリングログの転送カテゴリ追加/削除を行う目的	438
27.2. URL フィルタリングログの転送カテゴリ追加	438

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

27. 3. URL フィルタリングログの転送カテゴリ削除.....	442
28. 基幹 L3SW でのフィルタリング追加/削除.....	446
28. 1. 基幹 L3SW でフィルタリングを行う目的	446
28. 2. 基幹 L3SW でのフィルタリングの考え方	447
28. 3. 基幹 L3SW でのフィルタリング追加が必要な条件	451
28. 4. 基幹 L3SW でのフィルタリング追加	452
28. 4. 1. 通信要件の整理	452
28. 4. 2. 現状の条件を確認する	452
28. 4. 3. コンフィグを事前作成する	453
28. 4. 4. コンフィグのバックアップ	454
28. 4. 5. フィルタリング追加 (CLI)	454
28. 5. 基幹 L3SW でのフィルタリング削除	457
28. 5. 1. 削除対象の条件のシーケンス番号を確認する	457
28. 5. 2. コンフィグのバックアップ	458
28. 5. 3. フィルタリング削除 (CLI)	458
付録 459	
付録1. CLI コマンドリスト	460

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. はじめに

この項では、本書の内容、本書の位置づけ、方針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

0. 1. 本書について

本書は、西日本高速道路株式会社

「広島 DC 構築に伴うネットワーク等の検証業務 業務仕様」における

「1. 2. 1 ネットワーク運用設計」を実施する為の「運用手順」です。

0. 2. 本書の位置づけ

本書では、基本設計書「ネットワーク構成検討・設計要件定義書兼基本設計書」を基に、

「広島 DC 構築に伴うネットワーク等の詳細設計業務 機器選定理由書」で選定し導入した
以下のセキュリティ機器について運用手順を記載します。

表 0-2-1 セキュリティ機器

メーカー	型番	導入バージョン	備考
Palo Alto Networks	PA-5450	PAN-OS 10.2.3-h2	新規導入
Palo Alto Networks	Panorama M-300	Panorama 10.2.3-h2	新規導入

0. 3. 方針

運用手順に関する方針は以下とします。

- ・TCP/IP ネットワークについての基本的な知識がある方を対象としています。
- ・簡易的な設定変更を実施する程度の操作を想定しています。
- ・お客様作業により発生した障害に対する責任は負いません。
- ・バックアップの取得、マニュアルやリリースノートの閲覧等、事前準備を行った上で、
作業を実施してください。
- ・本書に記載されている用語や操作、各種設定の詳細につきましては製品マニュアルを
ご参照ください。
- ・PA-5450 と M-300 の画面操作は同一です。
- ・M-300 は設定変更作業がない為、世代管理はしません。
- ・各機器に設定されている内容（パラメータ初期値）は、各電算室の Palo Alto 設定
シートをご参照ください。

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

0. 4. 用語集

表 0-4-1 用語集

No	用語	説明
1	アクセス解除	ファイアウォールでブロックされているサイトへの通信を許可します。 ※URL フィルタによりブロックされている場合も含みます。
2	アクセスブロック	ファイアウォールで許可されているサイトへの通信をブロックします。 ※URL フィルタにより許可されている場合も含みます。
3	全社	「△△」と「グループ会社」を合わせた呼び名の略称
4	本体	「△△」の略称
5	G 会社	「グループ会社」の略称
6	Panorama	パロアルトネットワークス社の統合管理製品の名称
7	シグネチャ	脆弱性、攻撃、ウイルスおよびマルウェアを検知・識別するための定義のこと。アンチウイルス機能、IPS/IDS 機能にて使用します。
8	ファイアウォールポリシー	通信のアクセスを制御するためのルール
9	Virtual System	仮想ファイアウォール機能、vsys と略して使用する場合があります。
10	NAT	Network Address Translation の略称 IP アドレスを変換する技術
11	StaticNAT	1 対 1 の IP アドレス変換技術
12	DynamicNAT	IP アドレスの変換範囲を指定しておくことで、通信が発生した時にその IP アドレスの範囲内の IP アドレスを 1 つ使用して変換する技術
13	URL フィルタリング	閲覧することが不適切なインターネット上の Web サイトをフィルタリングし、ユーザに見せなくすることを指します。
14	URL プロファイル	URL フィルタリングに関する情報を書き込んである、設定情報の集まり。
15	カテゴリ(URL)	URL フィルタリングにて使用する Web サイトを識別するための定義。ギャンブルサイト、オークションサイト、など。
16	カスタムカテゴリ(URL)	ユーザが自由に定義することができるカテゴリ 単に「カテゴリ」と記載している場合、パロアルトネットワークス社が定義しているカテゴリを示し、区別します。
17	SSL	インターネット上でデータを暗号化して送受信できるプロトコル
18	SSL 証明書	クライアントとサーバが SSL で通信するときに使用する電子証明書
19	ルート認証局	SSL 証明書を署名する認証局

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

20	PEM 形式	SSL 証明書のフォーマット 証明書のバイナリを Base64 でエンコードして表示された証明書情報は「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」で囲まれている。
21	フェイルオーバー	稼動系(Active)を待機系(Passive)に切り換える機能
22	フェイルバック	障害から復旧した後に、稼動系に切り戻す機能
23	HA	HA (High Availability) は可用性が高い事を示し、ペアのファイアウォールに障害が発生した場合に、代替ファイアウォールを使用できるようにすること。
24	UTM	UTM (Unified Threat Management) の略で、日本語で「統合脅威管理」と呼ばれている。 ファイアウォール機能のほか、IPS/IDS、アンチウイルス、アンチスパイウェア、URL フィルタリングなど複数のセキュリティ機能を一つに統合したもの
25	JSOC	Japan Security Operation Center の略称 LAC 社が所有するセキュリティ監視センターを指します
26	PAN-DB	パロアルネットワーク社自社製のデータベース
27	統合 FW	広島 DC、吹田 DC(旧電算室)に配置される、仮想ファイアウォール群の総称
28	基幹 SW	広島 DC、吹田 DC(旧電算室)に配置される、WAN 接続機器や統合 FW を接続するスイッチ 又は、主要拠点に設置される集約スイッチ
29	running-config	commit を実施し、設定を反映した config
30	candidate-config	commit 未実施の編集中の config
31	オペレーションナルモード	SSH もしくはコンソールケーブルから機器にログインした直後のモード。主に機器ステータスの確認、ログを取得するときに CLI から操作する。
32	コンフィグレーションモード	CLI から設定変更を行うときのモード。オペレーションナルモードから configure と入力するとコンフィグレーションモードに入る。

本書で使用している「」（カッコ）には、GUI に表示される項目、クリック可能なボタン項目を記載しています。

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

0. 5. VR のゾーン名一覧表

表 0-5-1 インターネット接続用 VR のゾーン区分表

No	VR 名	ゾーン俗称名	ゾーンの説明	ゾーン名
1	インターネット接続用 VR	インターネット接続ゾーン	インターネットを接続するためのゾーン。	Internet_Untrust
		DMZ ゾーン	インターネット上への公開サーバが接続されるゾーン。	Internet_DMZ
		内部ゾーン	△△の自社拠点が接続されるゾーン。	Internet_WEST

表 0-5-2 内部接続用 VR のゾーン区分表

No	VR 名	ゾーン俗称名	ゾーンの説明	ゾーン名
2	内部接続用 VR	△△重要サーバゾーン	【重要セグメント】△△社内もしくはグループ会社向けの業務系サーバや管理系サーバなどが接続されるゾーン。	Internal_SV_Critical
		△△通常サーバゾーン	【通常セグメント】△△社内もしくはグループ会社向けの業務系サーバや管理系サーバなどが接続されるゾーン。	Internal_SV_Medium
		△△管理サーバゾーン	【管理系セグメント】△△社内もしくはグループ会社向けの業務系サーバや管理系サーバなどが接続されるゾーン。	Internal_SV_Maintenance
		内部ゾーン	△△の自社拠点が接続されるゾーン。	Internal_WEST

表 0-5-3 △△接続用 VR のゾーン区分表

No	VR 名	ゾーン俗称名	ゾーンの説明	ゾーン名
3	△△接続用 VR	内部ゾーン	△△の自社拠点が接続されるゾーン。	WEST_WEST
		G 会社共通ゾーン	各グループ会社と△△自社拠点との境界ネットワークが属するゾーン。	WEST_G-Untrust

表 0-5-4 グループ会社接続用 VR のゾーン区分表

(例. SHD)

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

No	VR 名	ゾーン俗称名	ゾーンの説明	ゾーン名
4	グループ会社接続用 VR	G 会社ゾーン	グループ会社の自社拠点が接続されるゾーン。	SHD_G-Trust
		G 会社共通ゾーン	各グループ会社と△△自社拠点との境界ネットワークが属するゾーン。	SHD_G-Untrust
		サーバゾーン	グループ会社のサーバが接続されるゾーン。	SHD_G-SV

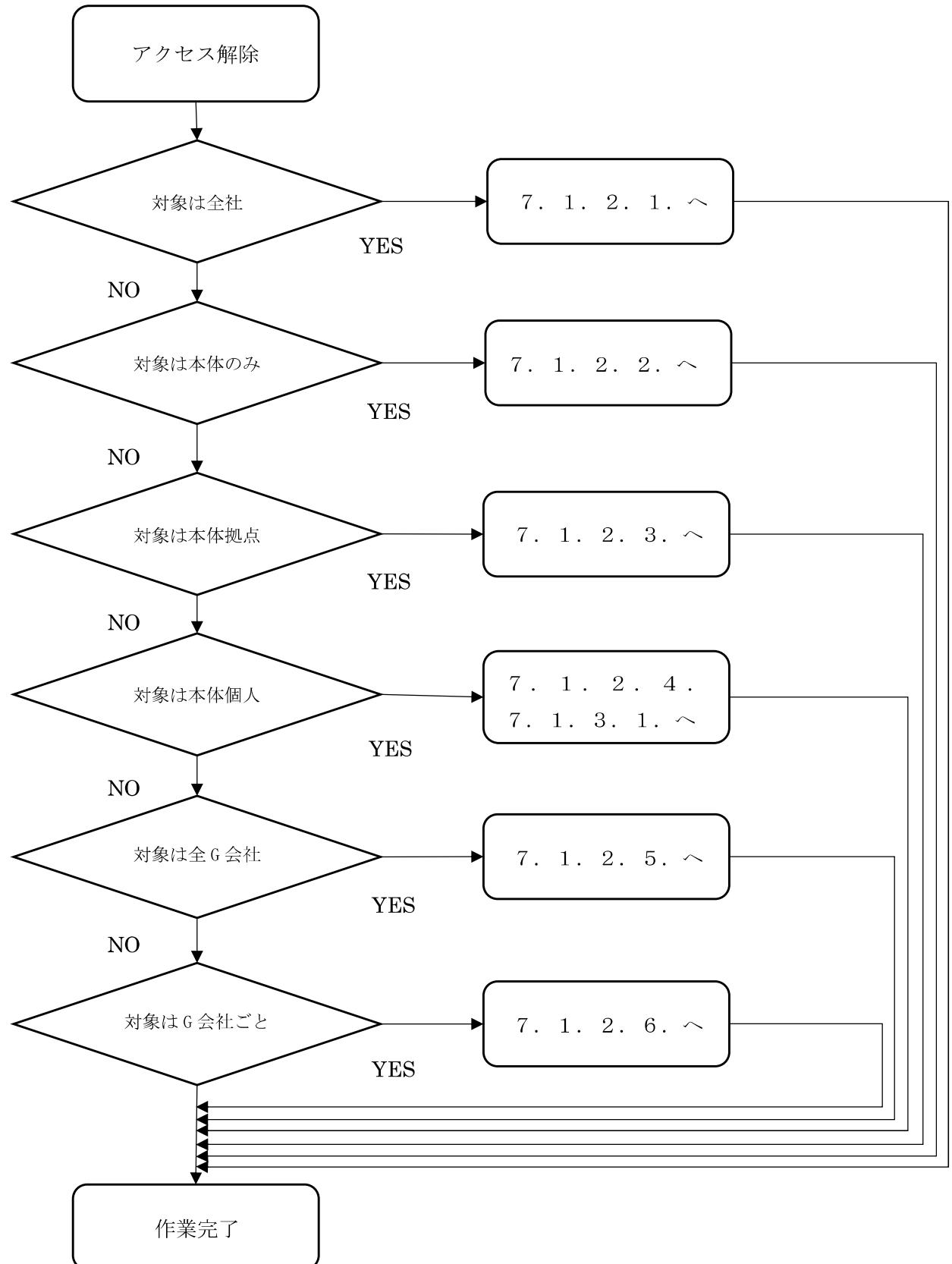
ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

1. 対応フロー

この項では各問い合わせに対する対応フローを記載しています。

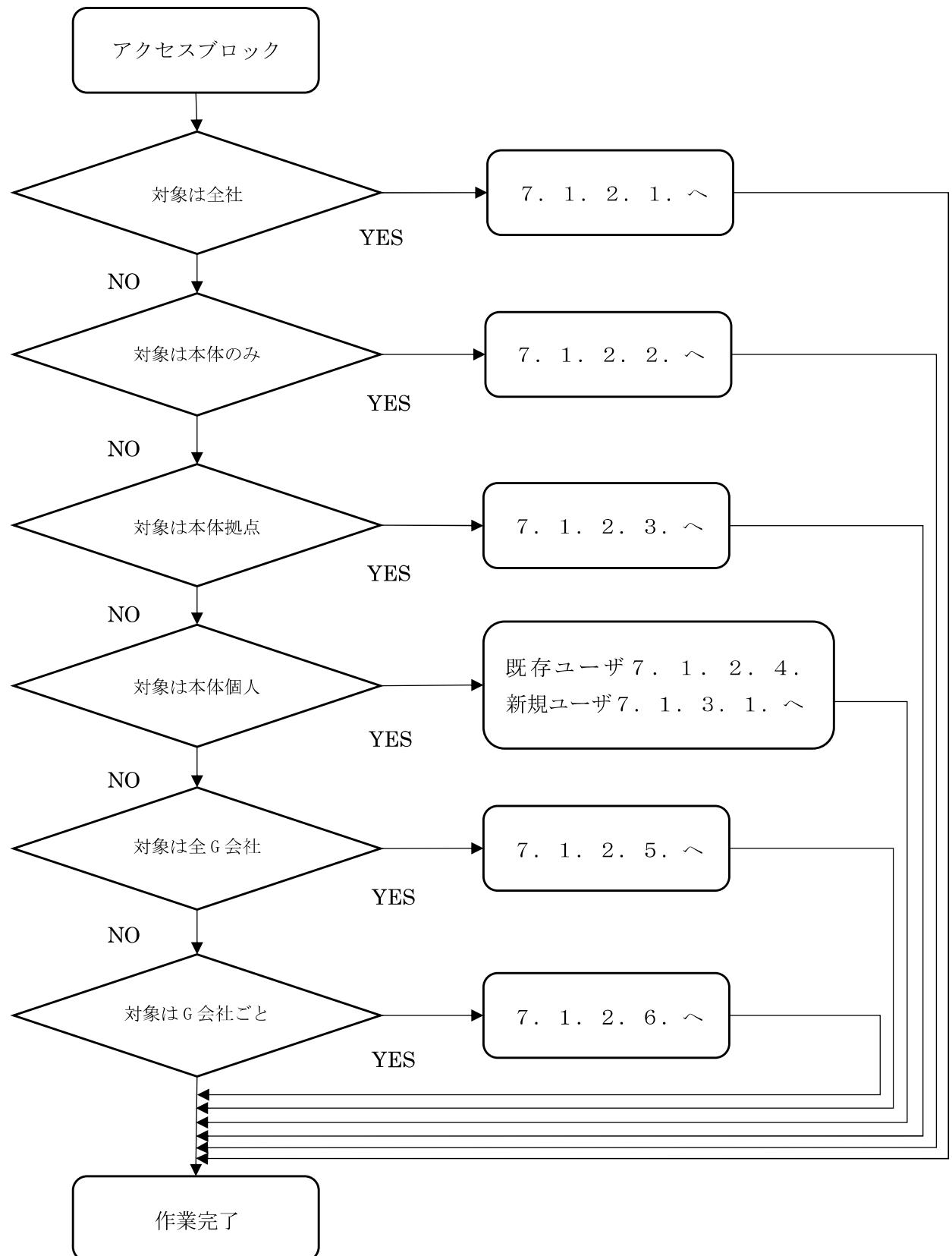
ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

1. 1. アクセス解除設定フロー



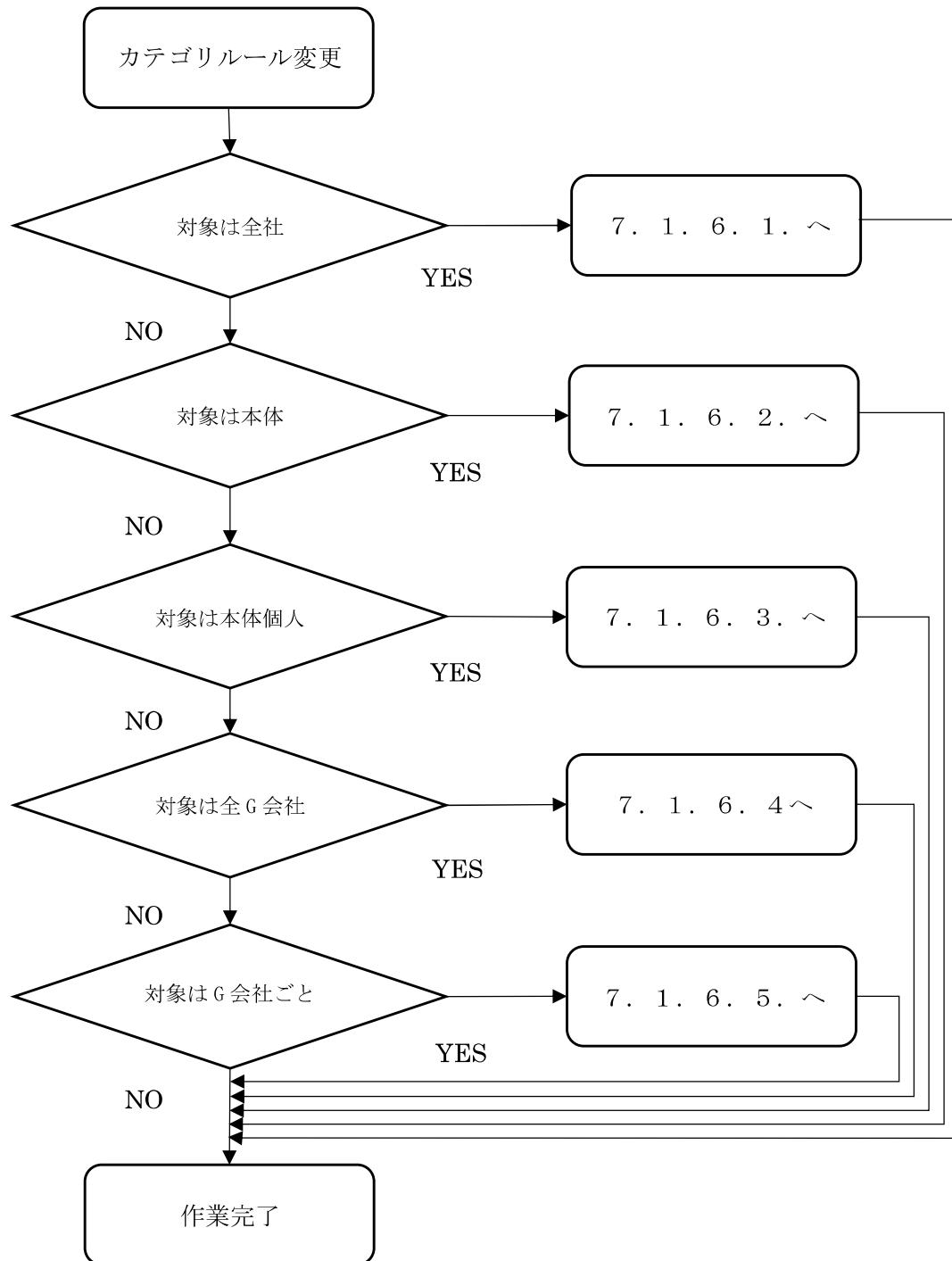
ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメントID		バージョン	2.0	2023/08/17	KDDI

1. 2. アクセスブロック設定フロー



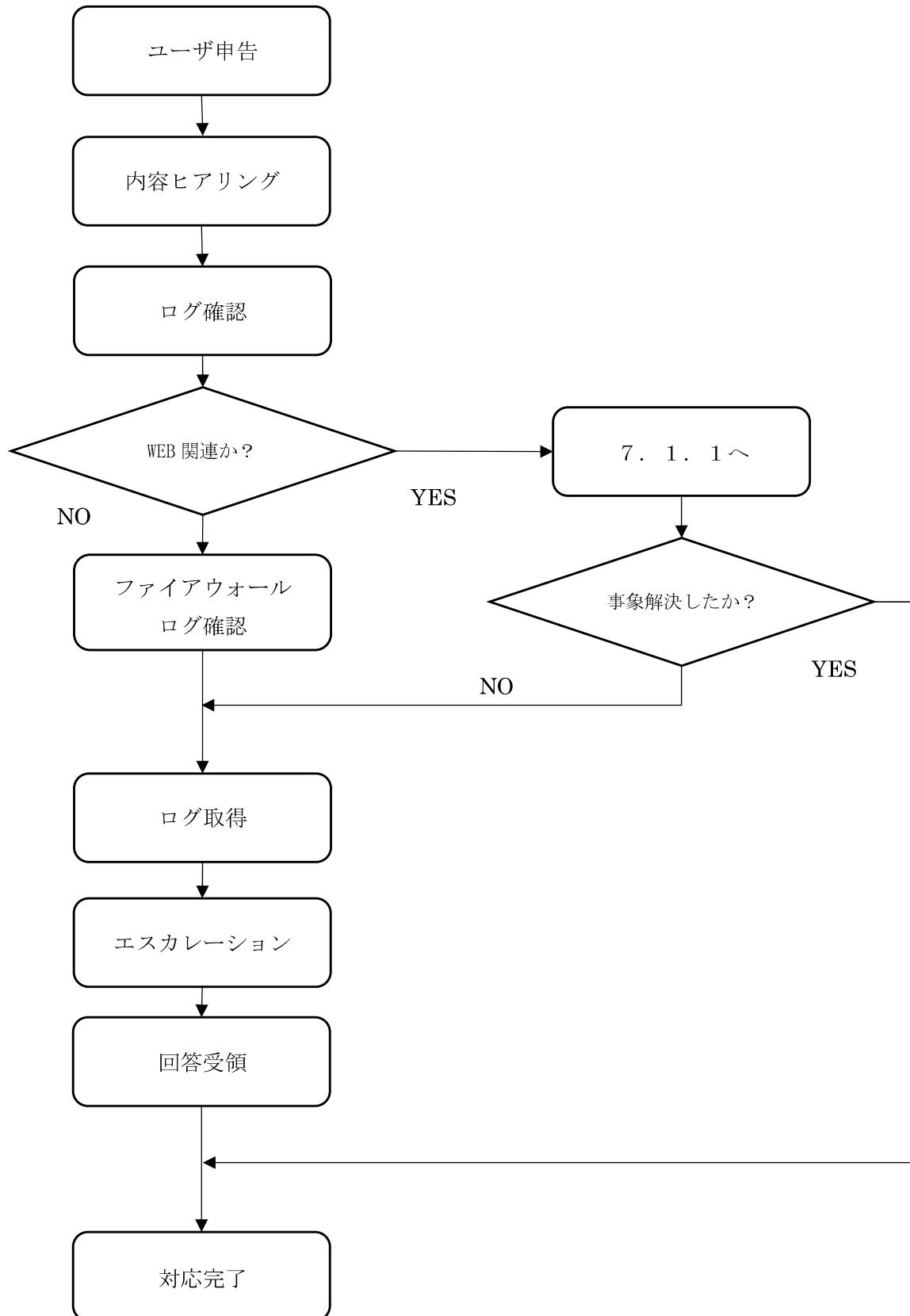
ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	最終更新者
ドキュメント ID		バージョン	2.0	2023/08/17	KDDI

1. 3. カテゴリルール変更フロー



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. 問い合わせ調査フロー（通信不具合）



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

2. 日次チェック

この項では、日時チェックで確認すべき項目、正常時の状態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

2. 1. ランプ点検

2. 1. 1. PA-5450

2. 1. 2. PA-5450 前面図

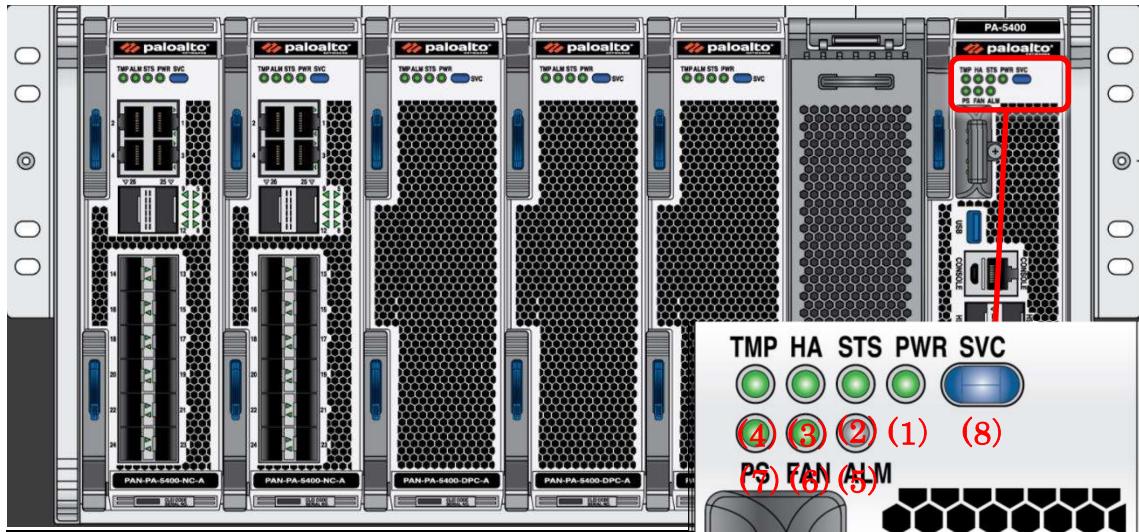


図 2－1－1 PA-5450 前面図

2. 1. 3. PA-5450 背面図

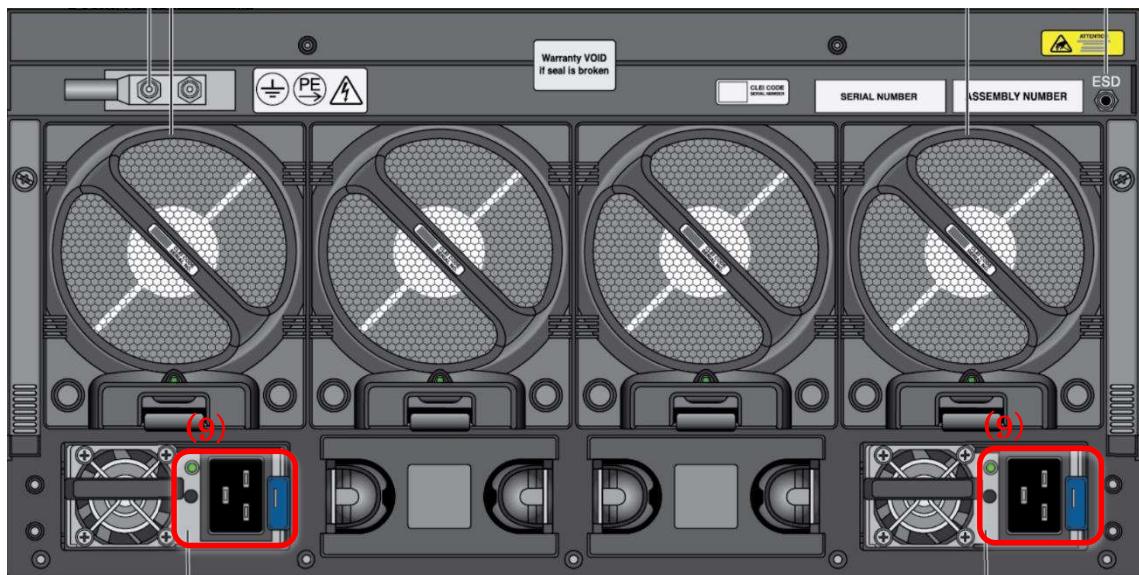


図 2－1－2 PA-5450 背面図

2. 1. 4. LED 確認

筐体前面および背面にある LED のステータスから、機器の状態を確認します。

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

(図2-1-1、図2-1-2、表2-1-1参照)

表2-1-1 LED

図中番号	LED名称	色及び状態	意味
(1)	PWR		電力供給中
			電源 OFF
(2)	STS		電力供給中
			エラーまたは障害が発生中
(3)	HA		アクティブ機器
			パッシブ機器
			High availability(HA)が有効でない
(4)	TMP		システムの全ての温度センサーが許容範囲内
			システムの1つ以上の温度センサーが許容範囲外
(5)	ALM		障害発生中
			正常に稼動している
(6)	FAN		全てのファンが動作している
			1つ以上のファンが故障している
(7)	PS		すべての電源装置は正常に動作しています。
			電源装置に障害が発生しました。
(8)	SVC		全てのカードは正常に稼働している
			障害が発生している ※show system service-led status コマンドで確認
(9)	Power Supply		正常に稼動している
			電源供給されていない



は正常な状態を示す

【正常確認内容】

- ・ PWR が緑色点灯であること
- ・ STS が緑色点灯であること
- ・ HA が緑色もしくは黄色点灯であること
- ・ TMP が緑色点灯であること
- ・ ALM が消灯であること
- ・ FAN が緑色点灯であること
- ・ PS が緑色点灯であること
- ・ SVC が緑色点灯であること
- ・ Power Supply LED が緑色点灯であること

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. 1. 5. ポート LED 確認

筐体前面にある LED のステータスから、ポート状態を確認します。

(図 2-1-3、表 2-1-2、表 2-1-3 参照)

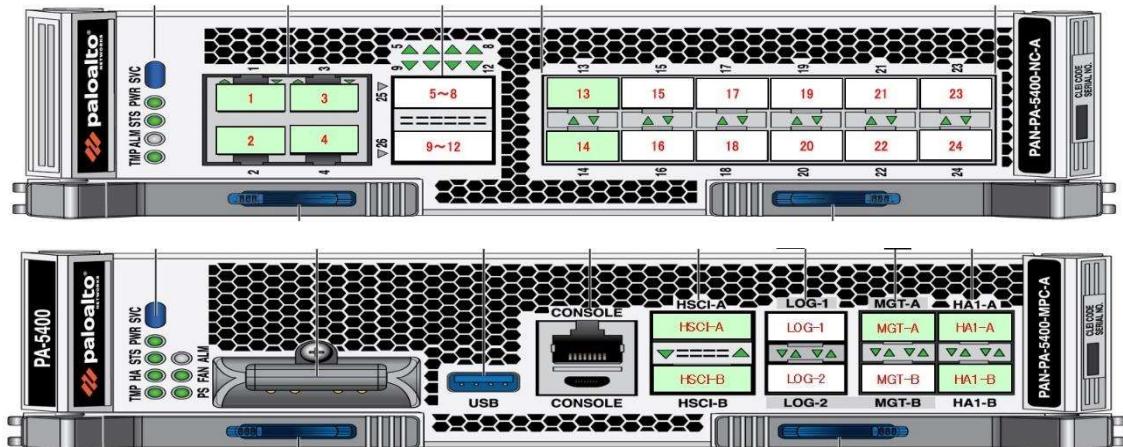


図 2-1-3 PA-5450 前面図（ポート表）

表 2-1-2 インターフェース

図中番号	インターフェース名	利用用途
1	Eth1/1	インターネット接続機器接続
2	Eth1/2	インターネット接続機器接続
3	Eth1/3	DMZ スイッチ接続
4	Eth1/4	DMZ スイッチ接続
1 3	Eth1/13	基幹 SW 接続
1 4	Eth1/14	基幹 SW 接続
HSCI-A	Eth1/2	統合 FW 接続
HSCI-B	Eth1/2	統合 FW 接続
HA1-A	Eth1/2	統合 FW 接続
HA1-B	Eth1/2	統合 FW 接続
MGT-A	Eth1/2	基幹 SW 接続

表 2-1-3 ポート LED

LED 名称	色及び状態	意味
Link	緑色で点灯	イーサネットケーブルが存在し、対向側とのリンクが確立している。
	緑色で点滅	データの送信中または受信中
	消灯	リンクなし、使用不可

※ は点滅する箇所です。

は正常な状態を示す

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

【確認内容】

- 利用しているポート LED が緑色であること

2. 1. 6. M-300 前面図

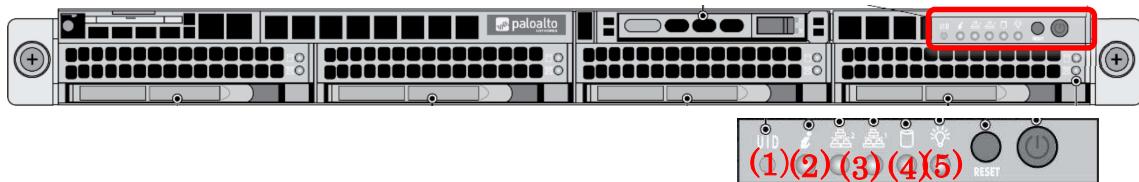


図 2-1-4 M-300 前面図

2. 1. 7. M-300 背面図

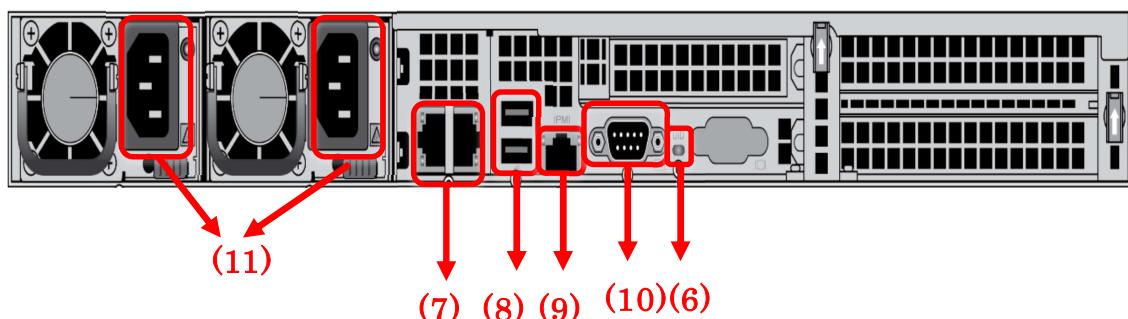


図 2-1-5 M-300 背面図

2. 1. 8. LED 確認

筐体前面にある LED のステータスから、機器の状態を確認します。

(表 2-1-4 参照)

表 2-1-4 LED

図中番号	LED 名称	色及び状態	意味
(1)	UID LED	青色で点灯	前面にある UID ボタンを押すと、背面の UID LED と前面パネルの LED が青く点灯再度ボタンを押すと、これらの LED が無効になります。
(2)	System information	赤色で点灯	過熱障害発生中
		赤色で 1 秒間隔 1 回点滅	ファンの障害が発生している
		赤色で 4 秒間隔 1 回点滅	二つの電源装置の一つが障害発生しているか、電源が接続されていない
		青色で点灯	正常に稼働している
(3)	Network activity LEDs	緑色で点滅	ネットワーク アクティビティを示します。
(4)	HDD LED	黄色で点灯	IDE チャネルアクティビティを示します。
(5)	Power LED	緑色で点灯	電力供給中
		赤色で点灯	障害発生中
		消灯	電源 OFF

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

※  は点滅する箇所です。

 は正常な状態を示す

【確認内容】

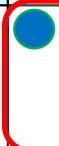
- ・(1) が青色点灯であること
- ・(2) が青色点灯であること
- ・(3) が緑色点滅していること
- ・(4) が黄色点灯していること
- ・(5) が緑色点灯であること

2. 1. 9. ポート LED 確認

筐体背面にある LED のステータスから、ポート状態を確認します。

(表 2-1-5、表 2-1-6)

表 2-1-5 LED

図中番号	LED 名称	色及び状態	意味
(6)	UID LED		前面にある UID ボタンを押すと、背面の UID LED と前面パネルの LED が青く点灯 再度ボタンを押すと、これらの LED が無効になります。

 は正常な状態を示す

【確認内容】

- ・(6) が青色点灯であること

表 2-1-6 インターフェース

図中番号	インターフェース名	利用用途
(7)	イーサネット ポート	2 つの RJ-45 100Mbps/1Gbps/10Gbps イーサネット ポート 左：アプライアンスの管理とデータ トライフィックに使用される 管理 (MGT) ポート。 右：イーサネット 1/1
(8)	USB ポート	使用されていない
(9)	IPMI ポート	使用されていない
(10)	コンソールポート	9 ピンのシリアル ケーブルと端末エミュレーション ソフトウェアを使用して管理コンピュータをアプライアンスに接続する
(11)	電源ポート	AC 電源入力を使用して、電源をアプライアンスに接続します。 2 番目の電源装置は冗長用です。

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

2. 2. ステータス確認

2. 2. 1. PA-5450

Active 機側

【確認内容】

高可用性のウィジェットが以下である事を確認する。

- ・Local が「Active」で緑
- ・ピアが「Passive」でアンバー
- ・実行コンフィグが「Synchronized」で緑
- ・アプリケーションバージョンが「Match」で緑
- ・脅威バージョンが「Match」で緑
- ・アンチウィルスバージョンが「Match」で緑
- ・PAN-OS バージョンが「Match」で緑
- ・GlobalProtect バージョンが「Match」で緑
- ・HA1 が「UP」で緑
- ・HA1 バックアップが「UP」で緑
- ・HA2 が「UP」で緑
- ・HA2 バックアップが「UP」で緑

The screenshot shows the PA-5450 dashboard with the 'High Availability' section circled in red. This section displays the status of various components:

モード	状態
Local	Active
ピア (10.19.132.4)	Passive
実行コンフィグ	Synchronized
アプリケーションバージョン	Match
脅威バージョン	Match
アンチウィルスバージョン	Match
PAN-OS バージョン	Match
GlobalProtect バージョン	Match
HA1	Up
HA1 バックアップ	Up
HA2	Up
プラグイン dip	Match

Below this, there are several status cards:

- ログインしている管理者**: 显示了三个登录会话，状态均为正常。
- 設定ログ**: 显示了“使用可能なデータなし。”
- ロック**: 显示了“ロック解除”。
- ACC リスク フラクタ(過去 60 分)**: 显示了风险分数为 2.6。
- データログ**: 显示了“使用可能なデータなし。”
- システムログ**: 显示了系统活动的日志条目。

図 2-2-1 PA-5450 Status

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

Passive 機側

【確認内容】

高可用性のウィジェットが以下である事を確認する。

- Local が「Passive」でアンバー
- ピアが「Active」で緑
- 実行コンフィグが「Synchronized」で緑
- アプリケーションバージョンが「Match」で緑
- 脅威バージョンが「Match」で緑
- アンチウィルスバージョンが「Match」で緑
- PAN-OS バージョンが「Match」で緑
- GlobalProtect バージョンが「Match」で緑
- HA1 が「UP」で緑
- HA1 バックアップが「UP」で緑
- HA2 が「UP」で緑
- HA2 バックアップが「UP」で緑

The screenshot shows the PA-5450 Status interface. The main window displays the 'High Availability' status, which includes a table of components and their modes (Local, Peers, Executable Config, Application Versions, PAN-OS Versions, GlobalProtect Versions, HA1, HA2, and Plugins) with color-coded status indicators (yellow for Local, green for others). Below this is a 'Logs' section containing four tabs: 'Login Log' (with no data), 'Data Log' (with no data), 'System Log' (listing user logins and sync events), and 'Setting Log' (listing configuration changes). At the bottom, there's a footer with navigation links and the Palo Alto Networks logo.

図 2-2-2 PA-5450 Status

※CPU 使用率、メモリ使用率は SNMP にて情報を取得し、

定量的に 75% を超過していない事を確認します。

※定量的に 75% を超過している状況がみられる場合は、調査が必要な為、

「24. 1. トラブルシューティングに必要なログ」を取得の上、

問い合わせを実施します。

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

2. 2. 2. M-300

Active 機側

【確認内容】

高可用性のウィジェットが以下である事を確認する。

- Local が「primary-active」で緑
- ピアが「secondary-passive」でアンバー
- 実行コンフィグが「Synchronized」で緑
- アプリケーションバージョンが「Match」で緑
- アンチウィルスバージョンが「Match」で緑
- Panorama バージョンが「Match」で緑
- HA1 が「UP」で緑

状態	説明
primary-active	Local
secondary-passive	ピア (10.19.132.2)
Synchronized	実行コンフィグ
Match	アプリケーションバージョン
Match	アンチウィルスバージョン
Match	Panorama バージョン
Up	HA1

図 2-2-3 M-300 Status

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

Passive 機側

【確認内容】

高可用性のウィジェットが以下である事を確認する。

- Local が「secondary-passive」でアンバー
- ピアが「primary-active」で緑
- 実行コンフィグが「Synchronized」で緑
- アプリケーションバージョンが「Match」で緑
- アンチウィルスバージョンが「Match」で緑
- Panorama バージョンが「Match」で緑
- HA1 が「UP」で緑

The screenshot shows the PANORAMA dashboard with the following status indicators:

- High Availability:**
 - Local: secondary-passive (Yellow)
 - Peers (10.9.6.4, 2): Primary-active (Green)
 - Config Sync: Synchronized (Green)
 - Application Version: Match (Green)
 - Anti-virus Version: Match (Green)
 - Panorama Version: Match (Green)
 - HA1: Up (Green)
- General Information:**
 - MGT IP Address: 10.19.132.2
 - MGT Network Mask: 255.255.255.240
 - MGT Default Gateway: 10.19.132.14
 - MGT IPv6 Address: unknown
 - MGT IPv6 Link Layer Address: fe80::dec:eff%eth0/64
 - MGT IPv6 Default Gateway: M-300
 - MGT MAC Address: 3:ace:fc:f5:60
 - Model: M-300
 - Serial Number: 02101000653
 - System Model: panorama
 - Software Version: 10.2.4
 - Application Version: 8704-8621 (05/03/23)
 - Device Dictionary Version: 80-401 (06/02/23)
 - Date: Fri Jun 9 18:21:41 2023
- Logs:**
 - Login Log:**

管理者	通常名	クライアント	セッション開始	アイドル時間
KDDI	10.19.132.13	Web	06/09 18:21:30	00:00:00s
panorama	Console	Panorama	06/01 17:36:56	23:19:32s
 - Data Log:** 使用可逆データなし.
 - System Log:**

内 容	時 間
User KDDI logged in via Web from 10.19.132.13 using https authenticated for user KDDI. From: 10.19.132.13.	06/09 18:21:30
Panorama has lost connection to its peer, no log will be forwarded.	06/09 18:21:21
lcs agent on 0119901002798 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13
lcs agent on 0119901002799 log-collection connected	06/09 18:21:13

図 2-2-4 M-300 Status

※CPU 使用率、メモリ使用率は SNMP にて情報を取得し、

定量的に 75%を超過していない事を確認します。

※定量的に 75%を超過している状況がみられる場合は、調査が必要な為、

「24. 1. トラブルシューティングに必要なログを取得」の上、

問い合わせを実施します。

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

3. 機器接続方法

この項では、機器への接続方法(CLI、GUI)、機器の起動、再起動方法(CLI、GUI)及び、機器の停止方法(CLI、GUI)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

3. 1. CLI

3. 1. 1. コンソール接続方法

各コンソールポート（図3-1-1赤枠参照）と管理端末を USB to RS-232 変換アダプターを使用して、コンソールケーブルにて接続します。

機器へのログインはターミナルソフト（TeraTerm）を利用します。

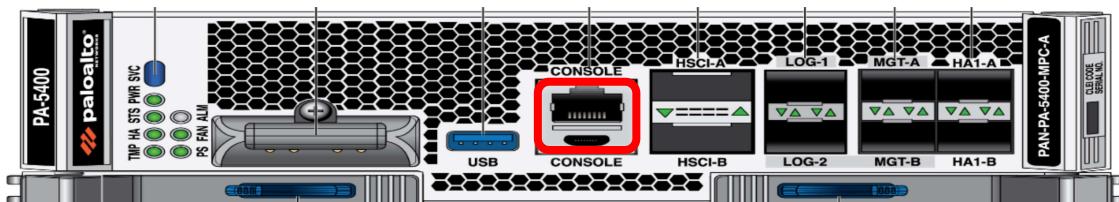


図3-1-1 コンソール接続箇所(PA-5450 前面)

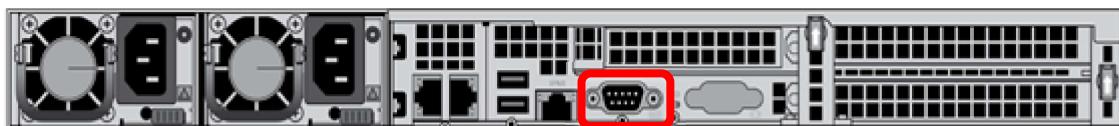


図3-1-2 コンソール接続箇所(M-300 背面)

表3-1-1 シリアルポート設定

設定項目	利用用途
Baud Rate	9600
Data	8bit
Parity	None
Stop	1bit
Flow Control	None

3. 1. 2. SSH 接続方法 (PA-5450、M-300 共通)

TeraTerm 等のターミナルソフトを使用し、各機器の管理用インターフェース（Management ポート）の IP アドレスに対して SSH にて接続します。

※(管理用インターフェースの IP アドレスはパラメータシート参照)

- ① ホストに対象機器の管理用インターフェースの IP アドレスを入力し、サービスは「SSH」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

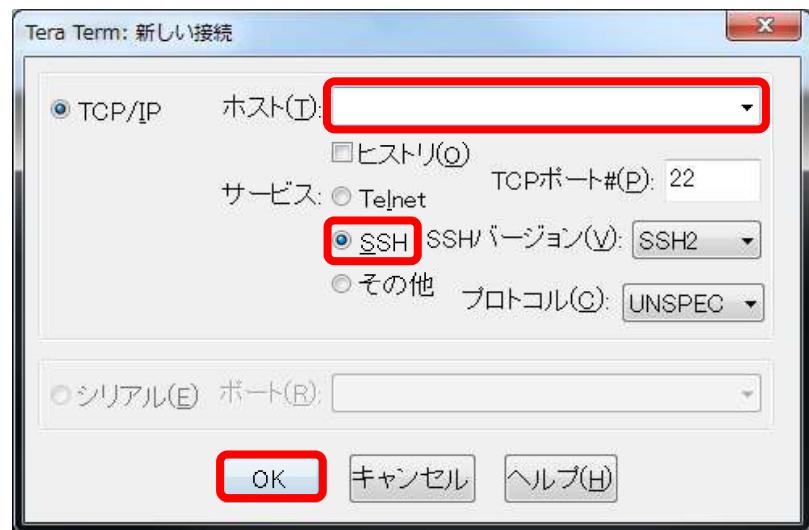


図 3-1-3 SSH 接続

- ② ユーザ名とパスワードを入力します。
 （※パスワードは「アカウント管理台帳（別紙）を参照」）

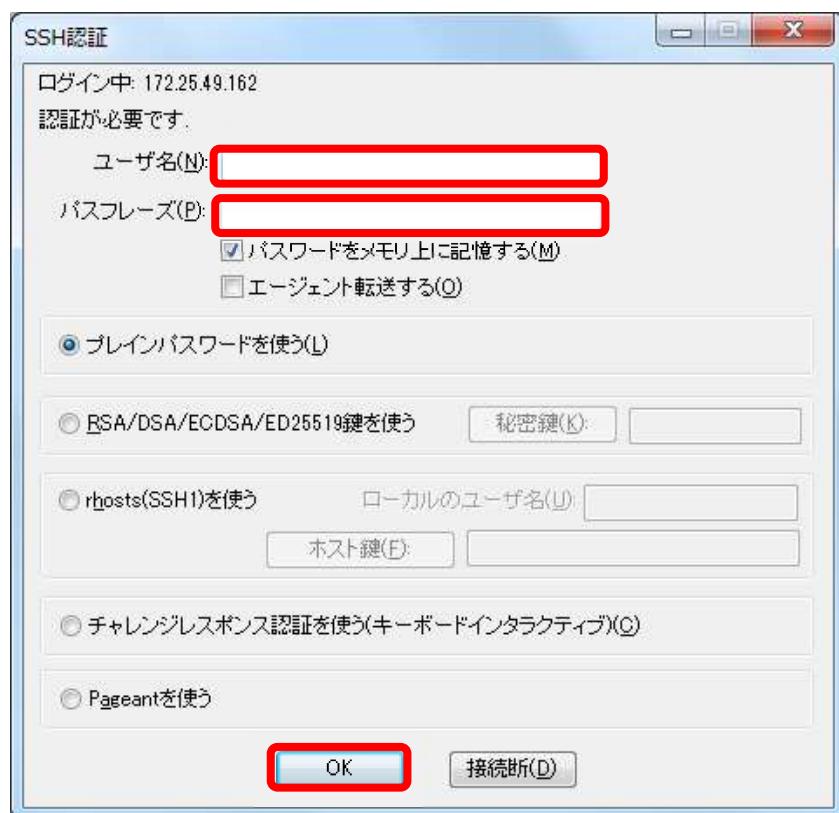


図 3-1-4 SSH ユーザ名とパスワード入力

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

3. 1. 3. モード遷移

CLI (コンソールもしくは SSH)によるログイン後のモードについて記載します。

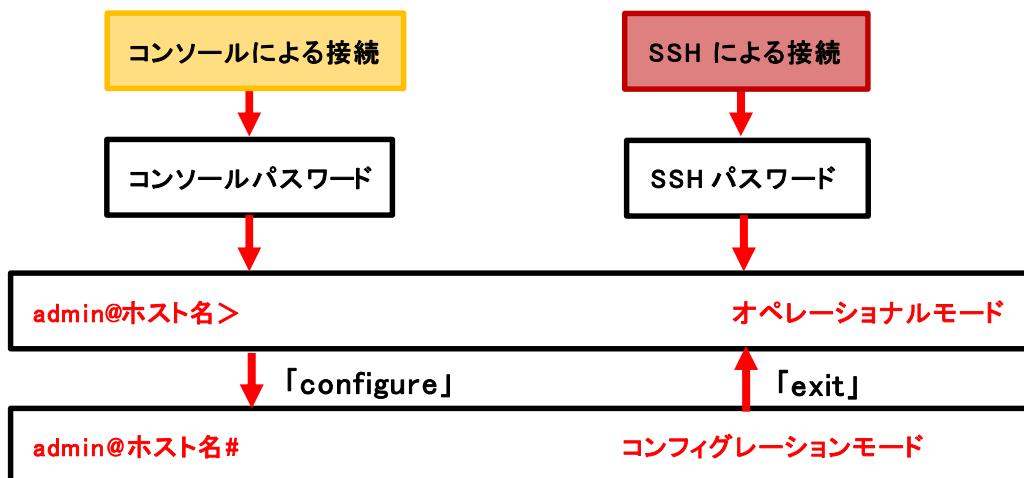


図 3-1-5 モード遷移

3. 2. GUI

3. 2. 1. GUI による接続方法 (PA-5450)

- ① 管理用端末をネットワークに接続します。
- ② ウェブブラウザで管理用インターフェース (Management ポート) の IP アドレスに HTTPS でアクセスします。
- ③ https://管理用インターフェース (Management ポート) の IP アドレス
※(管理用インターフェースの IP アドレスはパラメータシート参照)
- ④ 接続時にセキュリティ警告が表示された場合は、継続するオプションを選択します。



図 3-2-1 ブラウザ警告 (PA-5450)

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 3-2-1 サポートブラウザ (PA-5450)

サポートブラウザ
Internet Explorer 11 以降
Firefox 3.6 以降
Safari 5 以降
Chrome 11 以降

- ⑤ ログイン画面が表示されますので、ユーザ名、パスワードを入力して「ログイン」をクリックします。（※パスワードは「アカウント管理台帳（別紙）」を参照）

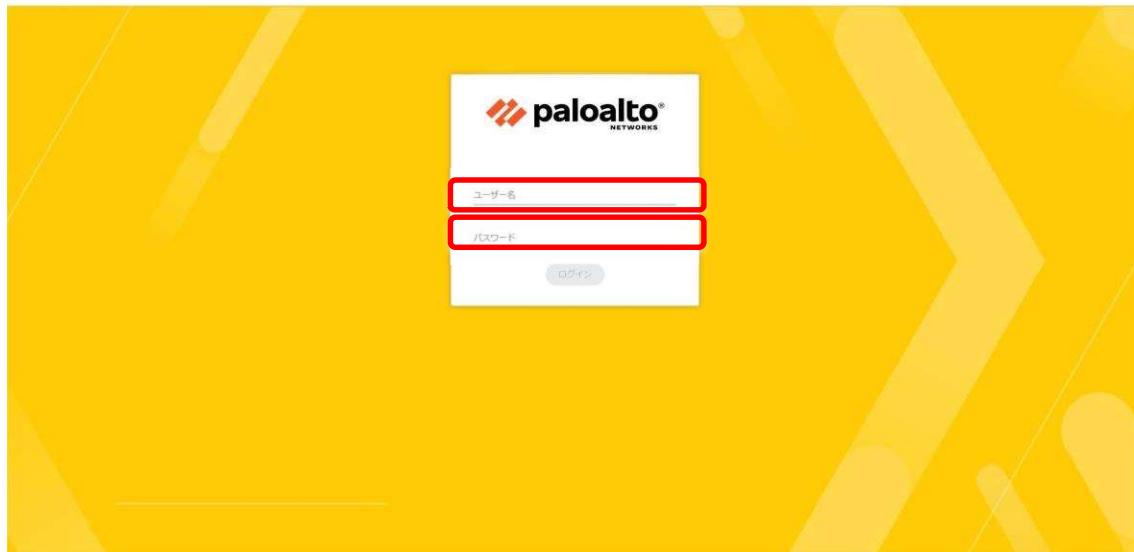


図 3-2-2 ログイン

- ⑥ ログインに成功すると以下の画面が表示されます。

管理者	接続元	クライアント	セッション開始	アイドル状態
admin	192.168.1.10.254	Web	01/30 10:55:35	00:00:00s

使用可能データなし。	
------------	--

内容	時間
User admin logged in via Web from 192.168.1.10.254 using https	10:55:25
authenticated for user 'admin' From: 192.168.1.10.254.	10:55:25
User admin logged out via Web from 192.168.1.10.254	10:55:35
Connection to Update server: updates.paloaltonetworks.com completed successfully. Initiated by 192.168.1.10.254	10:55:43
Connection to Update server: updates.paloaltonetworks.com completed successfully. Initiated by 192.168.1.10.254	10:48:28
Session for user test via Web from 192.168.1.10.254 timed out	10:50
Connection to Update server: updates.paloaltonetworks.com completed successfully. Initiated by 192.168.1.10.254	10:50:46
Session for user admin via Web from 192.168.1.10.254 timed out	10:50:46
Session for user admin via Web from 192.168.1.10.254 timed out	10:50:46
Connection to Update server: updates.paloaltonetworks.com completed successfully. Initiated by 192.168.1.10.254	10:50:46
Session for user admin via CLI from unknown host timed out	10:50:46

スロット 1 は NC CPU	0%	Up
スロット 2 は CA でない	0%	Up
スロット 3 は NC でない	0%	Up
5400-DIM-CPU	0%	Up

図 3-2-3 ログイン成功

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 「言語」（英語表示になっている場合「Language」）をクリックすると、表示言語の変更が可能です。

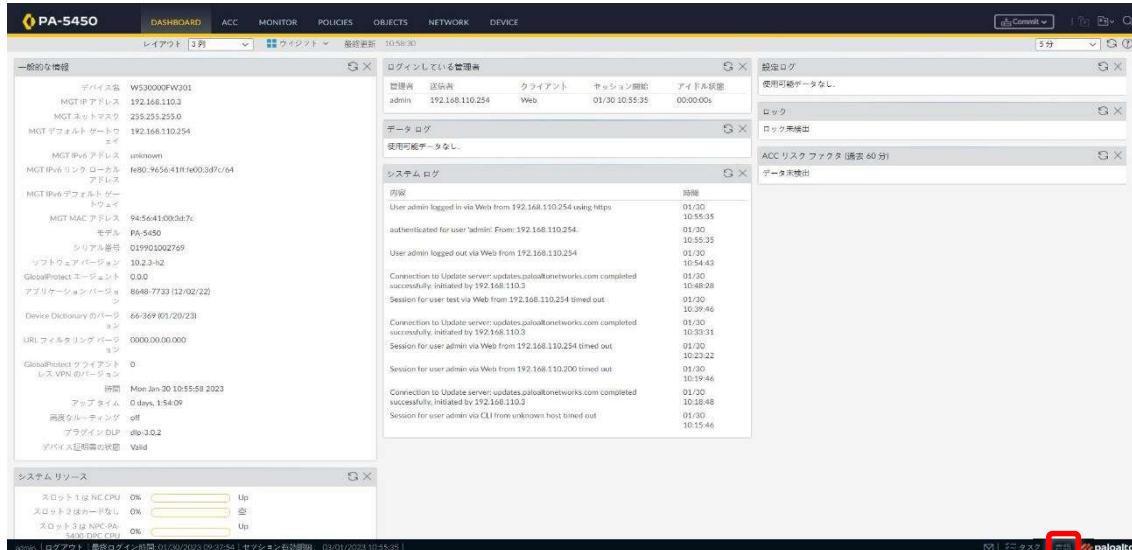


図 3-2-4 Language 変更

- ⑧ 表示言語を日本語に変更した場合は以下です。

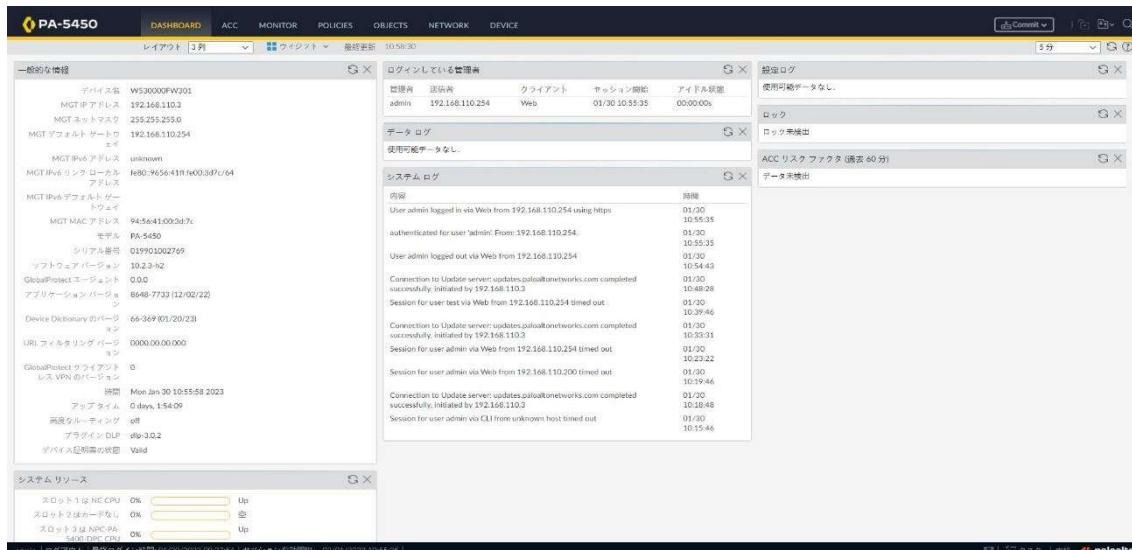


図 3-2-5 Language 変更後

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 以下の「ログアウト」をクリックするとログアウトします。

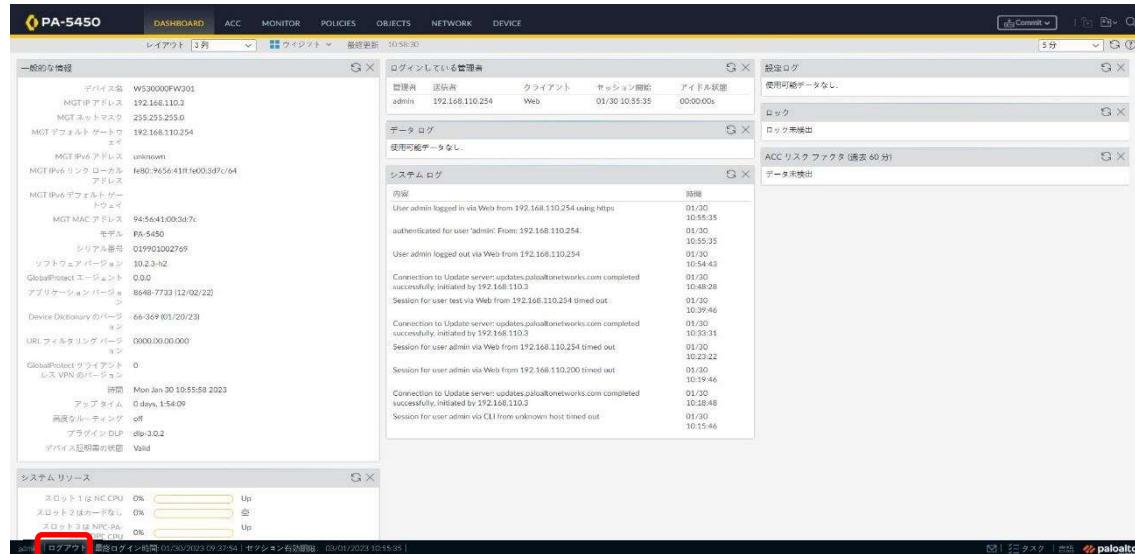


図 3-2-6 Logout

3. 2. 2. GUI による接続方法 (M-300)

- ① 管理用端末をネットワークに接続します。
- ② ウェブブラウザで管理用インターフェース(Management ポート)の IP アドレスに HTTPS でアクセスします。
- ③ https:// 管理用インターフェース(Management ポート)の IP アドレス
※(管理用インターフェースの IP アドレスはパラメータシート参照)
- ④ 接続時にセキュリティ警告が表示された場合は、継続するオプションを選択します。



図 3-2-7 ブラウザ警告 (M-300)

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 3-2-2 サポートブラウザ (M-300)

サポートブラウザ
Internet Explorer 7 以降
Firefox 3.6 以降
Safari 5 以降
Chrome 11 以降

- ⑤ ログイン画面が表示されますので、ユーザ名、パスワードを入力して「ログイン」をクリックします。（※パスワードは「アカウント管理台帳（別紙）」を参照）

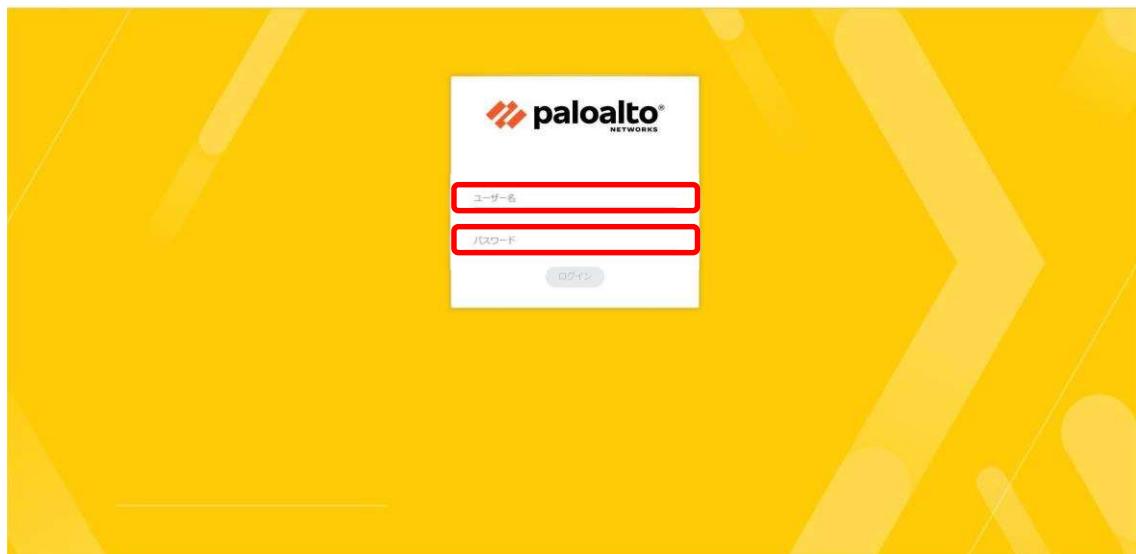


図 3-2-8 ログイン

- ⑥ ログインに成功すると以下の画面が表示されます。

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

図 3-2-9 ログイン成功

⑦ 「言語」（英語表示の場合は「Language」）をクリックすると、表示言語の変更が可能です。

The screenshot shows the PANORAMA web interface. At the top, there is a navigation bar with tabs: PANORAMA, DASHBOARD, ACC, MONITOR, and PANORAMA. Below the navigation bar, there is a search bar and a dropdown menu labeled "ログインしている管理者". This dropdown menu lists the current user "admin" with IP address "192.168.110.254" and session start time "01/30 11:04:48". To the right of this dropdown, there is a "Language" dropdown menu with options: English (selected), Japanese, and Chinese. The main content area displays various system logs and management information. The URL in the browser's address bar is "https://192.168.110.254:443".

図 3-2-10 Language 変更

⑧ 表示言語を日本語に変更した場合は以下です。

This screenshot is identical to the one above, but the "Language" dropdown menu is now set to "Japanese". The Japanese characters "日本語" are visible next to the English option. The rest of the interface, including the logs and management sections, remains the same.

図 3-2-11 Language 変更後

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 以下の「ログアウト」をクリックするとログアウトします。

The screenshot shows the PANORAMA web interface with multiple tabs and panels. In the bottom left corner, there is a red rectangular box highlighting the 'Logout' button. The interface includes sections for general information, device groups, accounts, monitoring, and panoramic views. On the right side, there are several log and status windows.

図 3-2-12 Logout

3. 3. 機器の起動

3. 3. 1. PA-5450

PA-5450 の機器起動方法について記載します。

① 電源モジュールに電源ケーブル(図中 (1))を接続します。

※起動時に電源ケーブルが接続されていれば、一度抜線する。

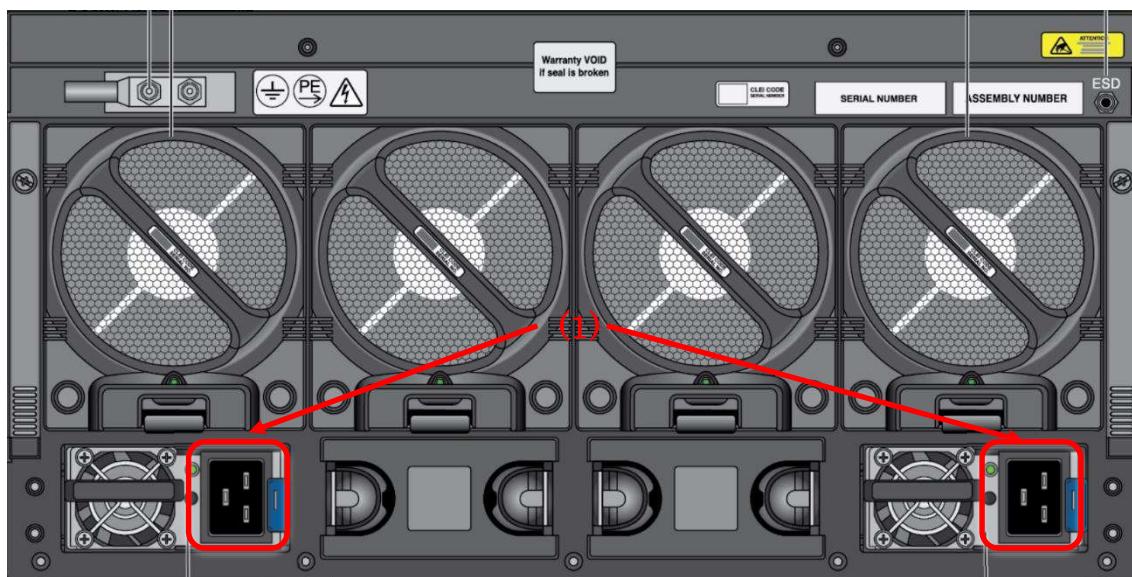


図 3-3-1 PA-5450 背面図

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. 3. 2. M-300

M-300 の機器起動方法について記載します。

- ① 電源ケーブルが抜けている場合は、電源モジュールに電源ケーブル(図中 (1))を接続します。

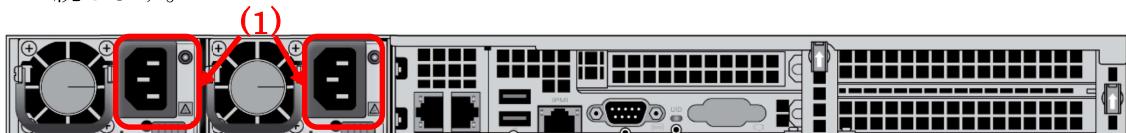


図 3-3-2 M-300 背面図

- ② 機器前面の電源ボタンを押下します。(図中 (2))

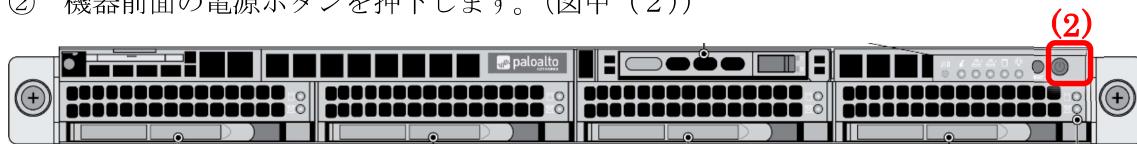


図 3-3-3 M-300 前面図

3. 4. 機器の再起動（リブート）

3. 4. 1. CLI による機器再起動方法(PA-5450、M-300 共通)

対象機器において「request restart system」コマンドを入力し、機器の再起動を実施します。

```
admin@ホスト名> request restart system
Executing this command will disconnect the current session. Do you want to continue? (y or n) y
Broadcast message from root (pts/0) (Thu Jun 29 22:03:07 2017):
The system is going down for reboot NOW!
~省略~.
```

図 3-4-1 CLI 再起動

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. 4. 2. GUI による再機器起動方法 (PA-5450)

- ① 「Device」タブ > 「操作」タブ > 「デバイスの操作」の「デバイスの再起動」をクリックします。

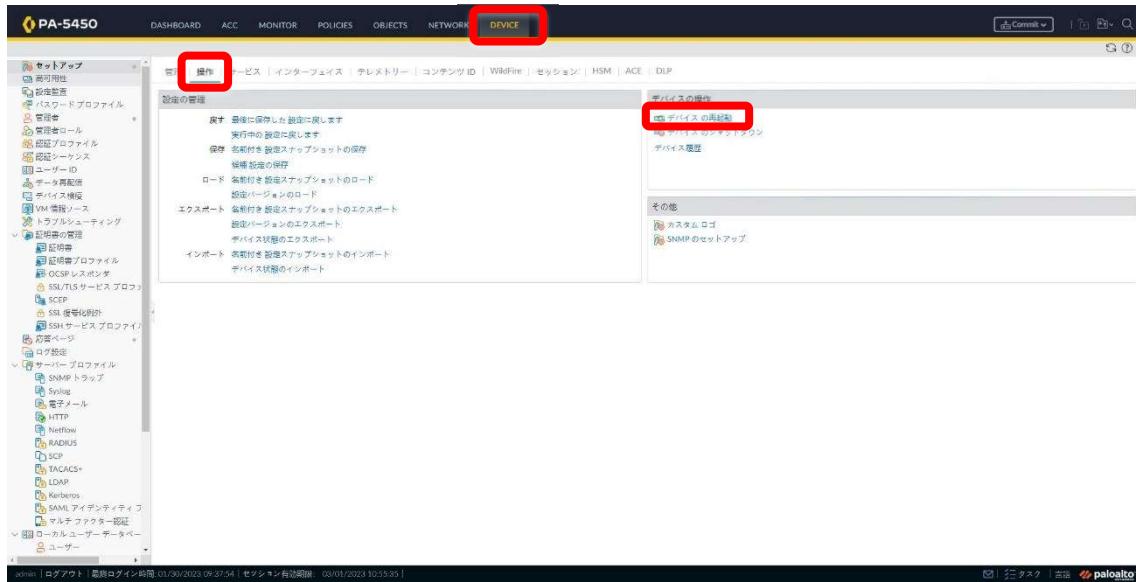


図 3-4-2 GUI 再起動 (PA-5450)

- ② 以下のメッセージが表示されるので、「はい」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 3－4－3 GUI 再起動確認

3. 4. 3. GUI による再機器起動方法 (M-300)

- ① 「Panorama」タブ > 「操作」タブ > 「デバイスの操作」の「Panorama の再起動」をクリックします。

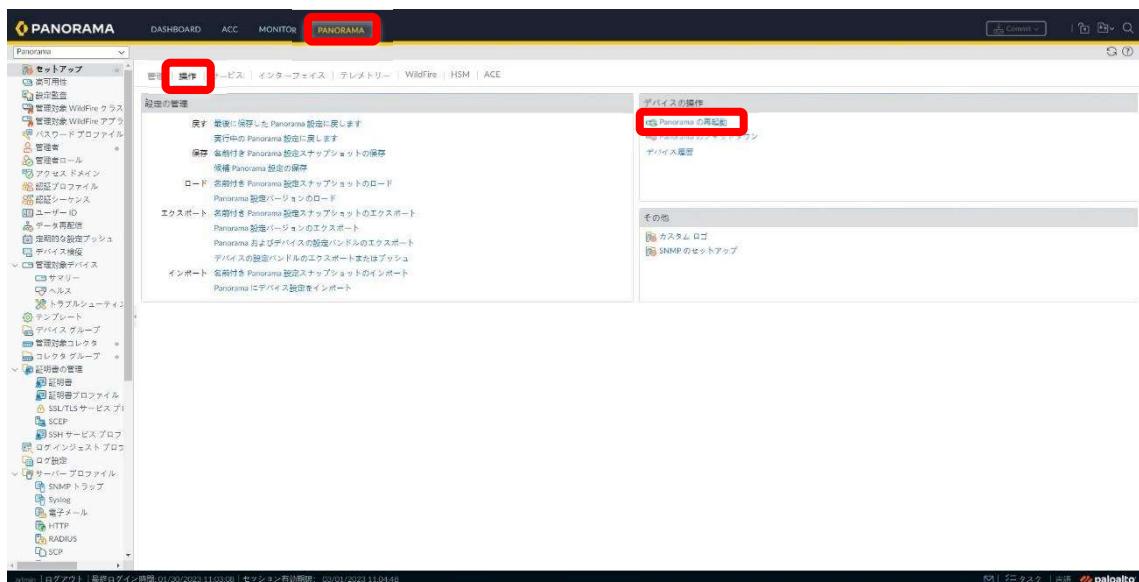


図 3－4－4 GUI 再起動 (M-300)

- ② 以下のメッセージが表示されるので、「はい」をクリックします。



図 3－4－5 GUI 再起動確認 (M-300)

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. 5. 機器の停止

3. 5. 1. CLI による機器停止方法 (PA-5450、M-300 共通)

- ① request shutdown system コマンドを実行します。
- ② 「Power down.」が表示されたら電源ケーブルを抜きます。

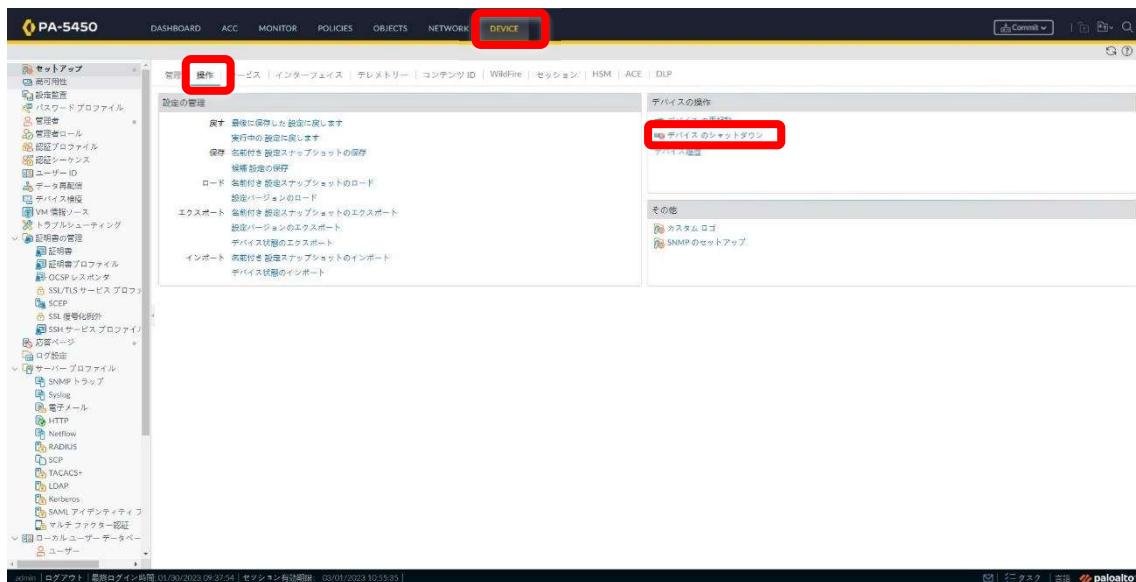
```
admin@ホスト名> request shutdown system
Warning: executing this command will leave the system in a shutdown state. Power must be removed and reapplied for the system to restart. Do you want to continue? (y or n) y
Broadcast message from root (ttyS0) (Wed Apr 12 10:19:38 2017):
~省略~

Halting system...
sd 0:0:0:0: [sda] Synchronizing SCSI cache
sd 0:0:0:0: [sda] Stopping disk
Disabling non-boot CPUs ...
Broke affinity for irq 19
Broke affinity for irq 4
Power down.
```

図 3－5－1 CLI 機器停止

3. 5. 2. GUI による機器停止方法 (PA-5450)

- ① 「Device」タブ > 「操作」タブ > 「デバイスの操作」の「デバイスのシャットダウン」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 3－5－2 GUI 停止 (PA-5450)

② 以下のメッセージが表示されるので、「はい」をクリックします。

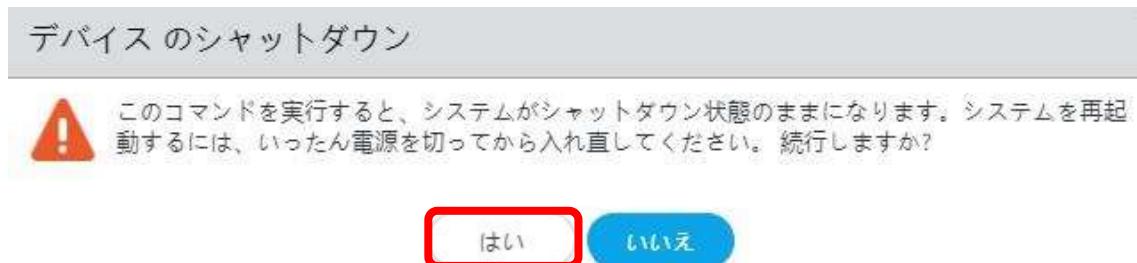


図 3－5－3 GUI 停止確認 (PA-5450)

③ 電源ケーブルを抜線します。

3. 5. 3. GUI による機器停止方法 (M-300)

① 「Panorama」タブ > 「操作」タブ > 「デバイスの操作」の「Panorama のシャットダウン」をクリックします。

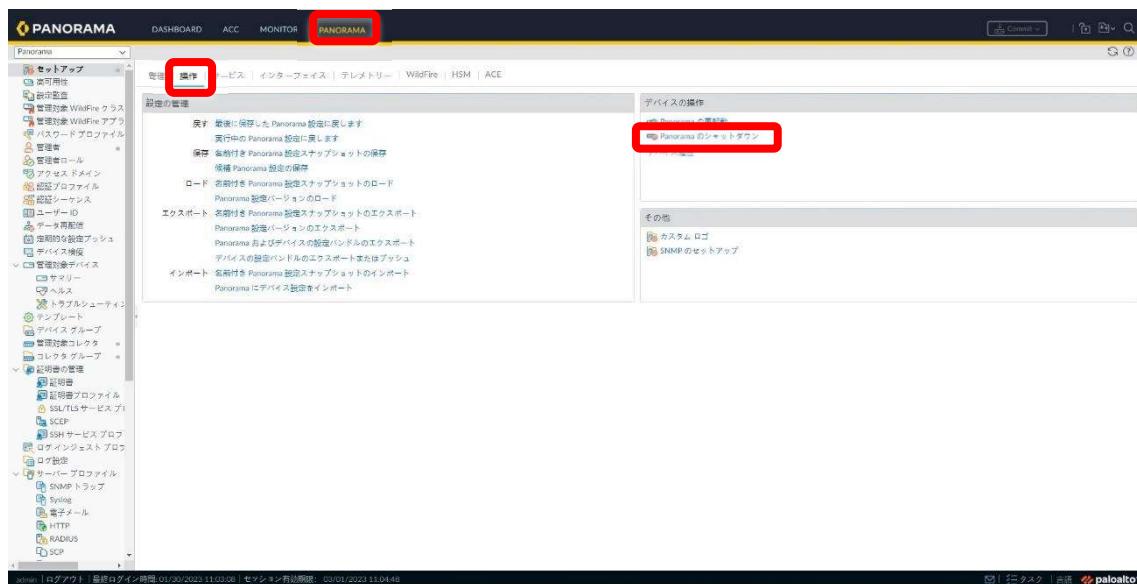


図 3－5－4 GUI 停止 (M-300)

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 以下のメッセージが表示されるので、「はい」をクリックします。



図 3－5－5 GUI 停止確認 (M-300)

- ③ 電源ケーブルを抜線します。

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

4. 設定情報保存/復元

この項では、設定情報の保存方法及び、復元方法、設定反映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

4. 1. 設定情報保存

設定情報を保存する手順を記載します。

- ① 「Device」タブ > 「セットアップ」 > 「操作」タブ > 「保存」 > 「名前付き設定スナップショットの保存」を選択します。

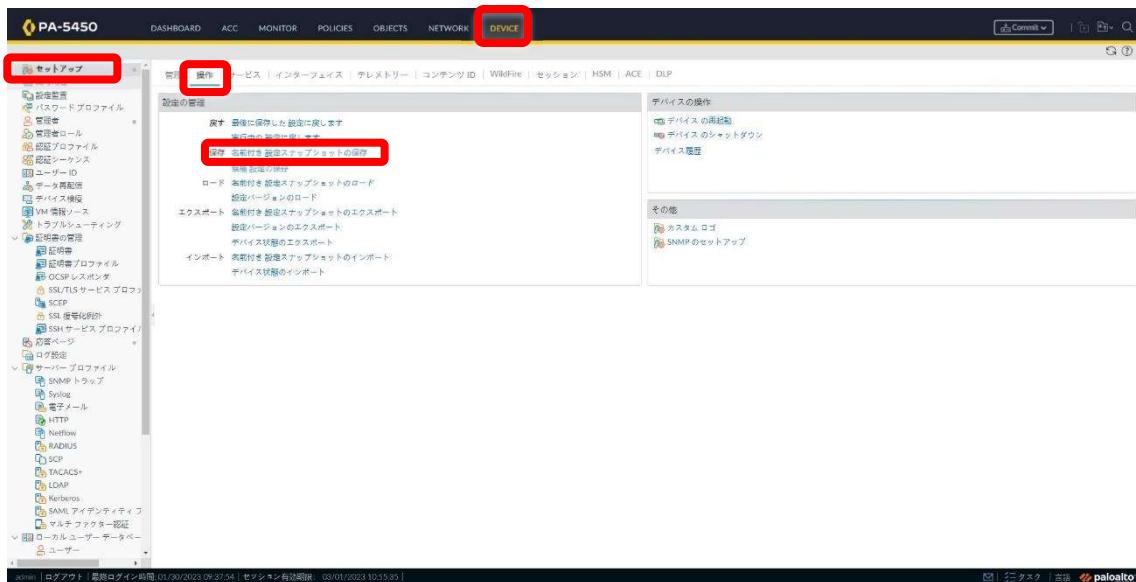


図 4－1－1 PA-5450 Device Save

- ② 「名前」タブをクリックし、「保存」対象のコンフィグファイル名を入力し、「OK」ボタンをクリックします。



図 4－1－2 PA-5450 Device Save

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 Save 完了ダイアログ表示後、「閉じる」をクリックします。



図 4－1－3 PA-5450 Device Save

4. 2. 設定情報エクスポート

設定情報をエクスポートする手順を記載します。

- ① 「Device」タブ > 「セットアップ」 > 「操作」タブ > 「エクスポート」 > 「名前付き設定スナップショットのエクスポート」を選択します。

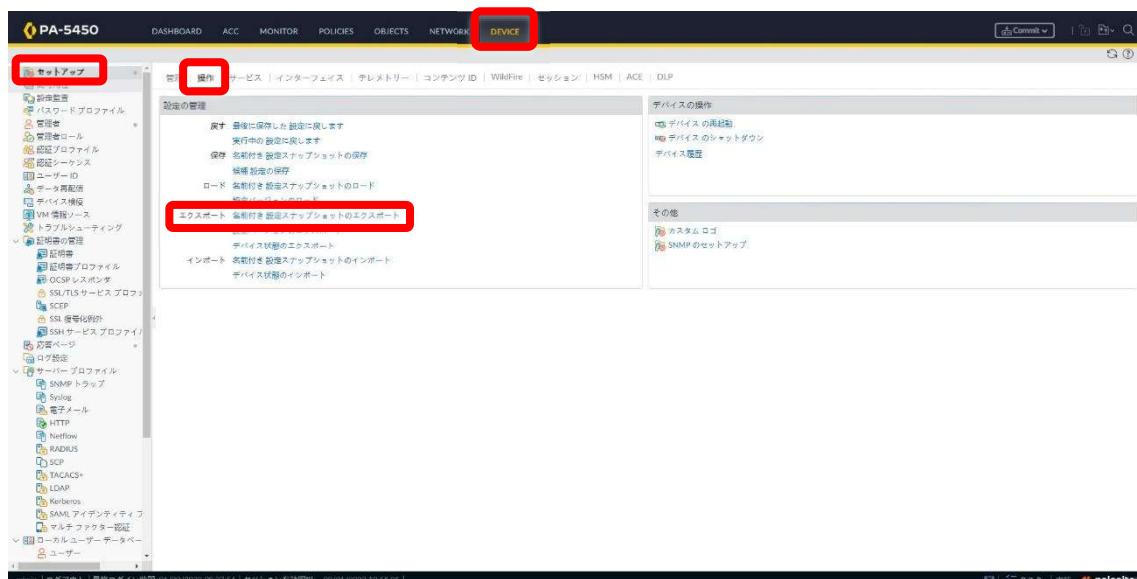


図 4－2－1 PA-5450 Device Export

- ② 「名前」を選択し、「OK」ボタンを押下します。



図 4－2－2 PA-5450 Device Export

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 「Device」タブ > 「セットアップ」> 「操作」タブ > 「エクスポート」> 「デバイス状態のエクスポート」を選択します。

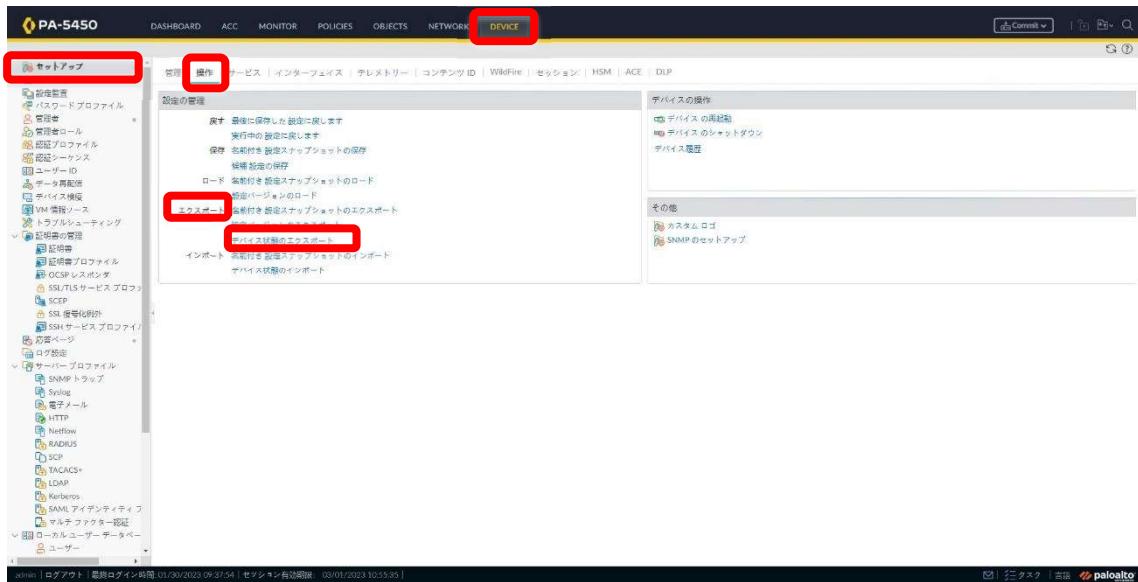


図 4－2－3 PA-5450 Device Export

自動的にダウンロードが開始されます

※ファイル名は固定値となります「device_state_cfg.tgz」

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. 3. 設定情報インポート

設定情報をインポートする手順を記載します。

4. 3. 1. 設定インポート

- ① 「Device」タブ > 「セットアップ」> 「操作」タブ > 「インポート」> 「名前付き設定スナップショットのインポート」を選択します。

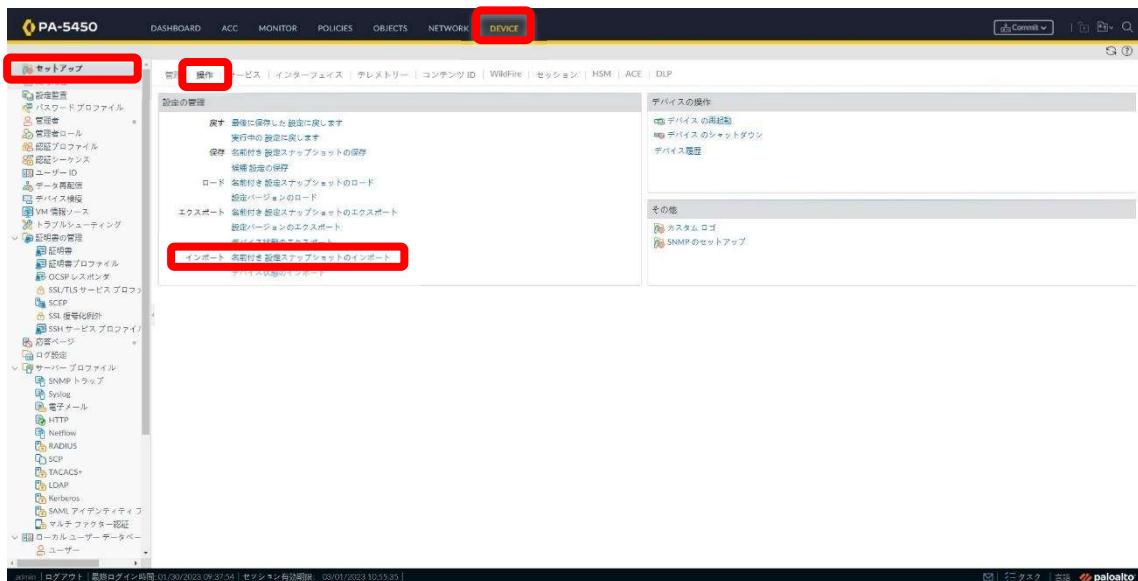


図 4 – 3 – 1 PA-5450 Device Import

- ② 「参照..」を押下し、「Import file」を選択後、「OK」ボタンをクリックします。



図 4 – 3 – 2 PA-5450 Device Import



図 4 – 3 – 3 PA-5450 Device Import

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. 3. 2. 設定ロード

- ① 「Device」タブ > 「セットアップ」 > 「操作」タブ > 「ロード」 > 「名前付き設定スナップショットのロード」を選択します。

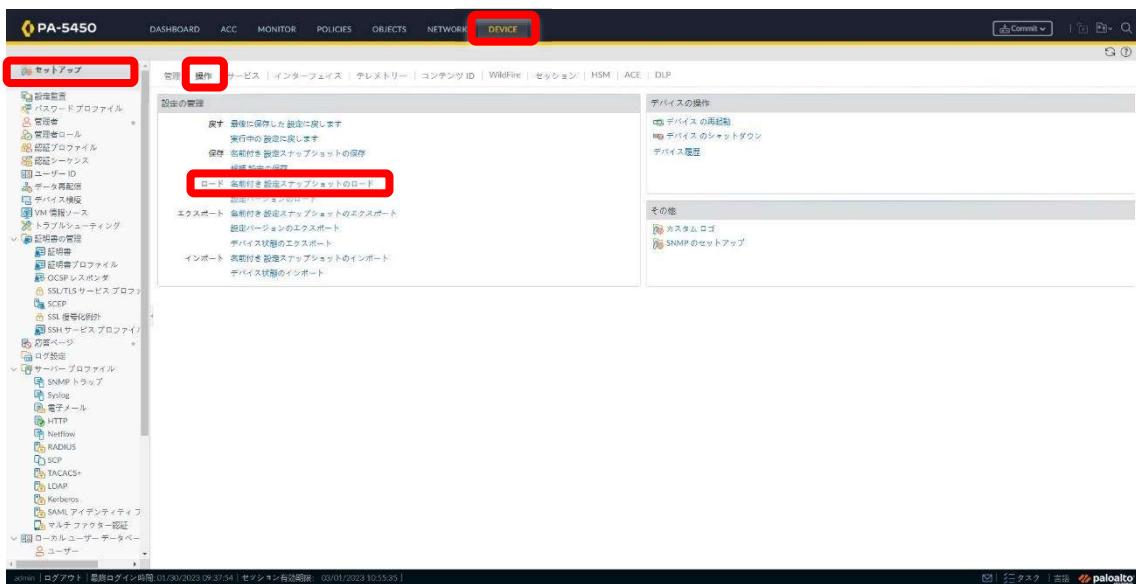


図 4－3－4 PA-5450 Device Load

- ② 「名前」タブをクリックし、「ロード」対象のコンフィグファイルを選択し、「OK」ボタンをクリックし、Load 完了ダイアログ表示後、「Close」をクリックします。



図 4－3－5 PA-5450 Device Load



図 4－3－6 PA-5450 Device Load

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. 3. 3. 設定反映 (PA-5450)

- 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入力後、「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 left sidebar contains a tree view of configuration categories like 'セッティング' (Settings), '設定監査' (Audit), '認証プロファイル' (Authentication Profiles), etc. The main panel shows a '設定の管理' (Management) section with various options like '実行' (Run), '保存' (Save), 'ロード' (Load), and 'エクスポート' (Export). A red box highlights the 'Commit' button at the top right of the panel.

図 4 – 3 – 7 PA-5450 Device Load

This screenshot shows a confirmation dialog titled 'コミット' (Commit). It asks if the user wants to commit all changes. Below the question, it specifies 'Commitすべての変更' (Commit all changes) and 'Commit変更の実行者:(1) admin'. A table shows the commit scope: 'コミットスコープ' is 'policy-and-objects', '場所タイプ' is 'Policy and Objects', and 'オブジェクトタイプ' and 'エンティティ' are empty. The '管理者' column is also empty. At the bottom, there 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 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。' (Note: All changes will be displayed in the domain accessible to the logged-in administrator.) A large red box highlights the 'コミット' (Commit) button.

図 4 – 3 – 9 PA-5450 Device Load

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. 3. 4. 設定反映 (M-300)

- ① 「コミット」ボタンをクリックし、「Panoramaへのコミット」を選択します。
- ② 「コミット」をクリックします。

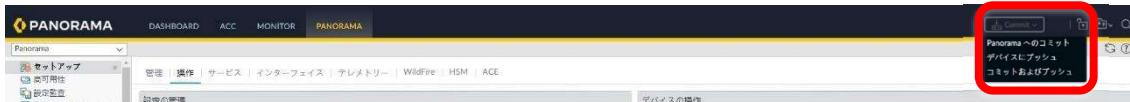


図 4-3-10 M-300 Device Load

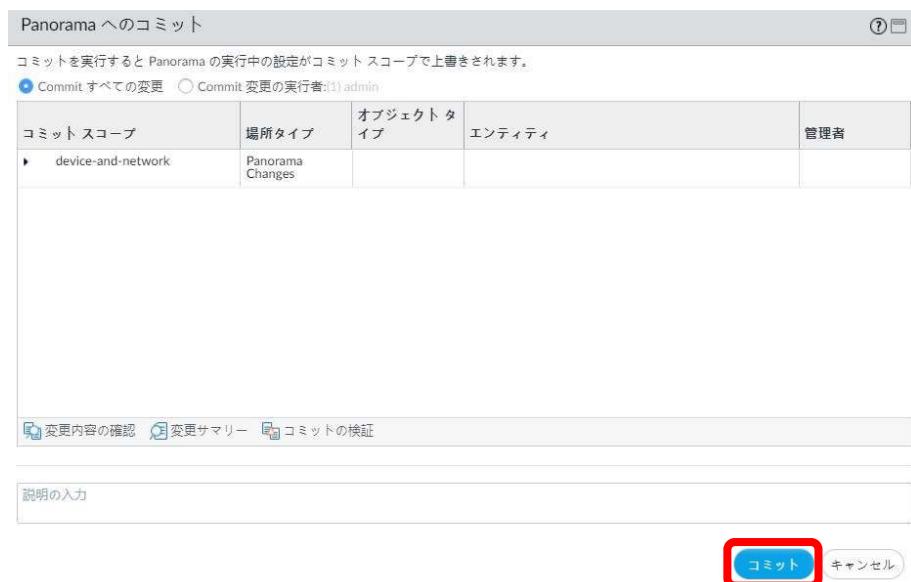


図 4-3-11 M-300 Device Load

設定完了後に Commit を行うことで稼働しているコンフィグに反映されます。「コミット」は「candidate config」を「running config」に設定反映と設定保存させるための実行コマンドです。

注意事項

シグネチャのアップデート、レポーティング情報の作成、ログデータのサマライズ関連の動作など、管理系内部プロセスの状態によって、設定の同期、もしくは「コミット」に失敗する場合があります。

同期に失敗した場合は、PA は自動で設定の同期をリトライしますが、少し時間をあけてから手動で「コミット」を実施してください。

補足 1：GUI から「candidate config」と「running config」の差分を確認する方法

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

- ① 「Device」タブ > 「設定監査」を選択し、「Local Running config」と「Local Candidate config」を選択後、「実行」ボタンを押します。
※Panoramaで差分を確認する場合は「Panorama」タブ>「設定監査」を選択します。

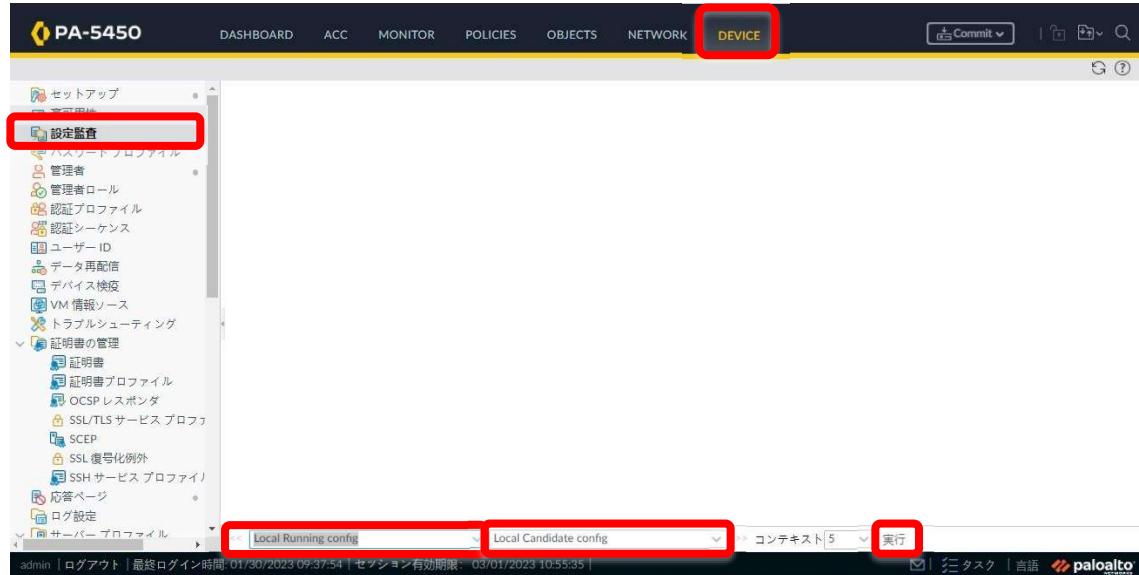


図 4-3-1-2 config difference

- ② 「candidate config」と「running config」の差分が表示されます。

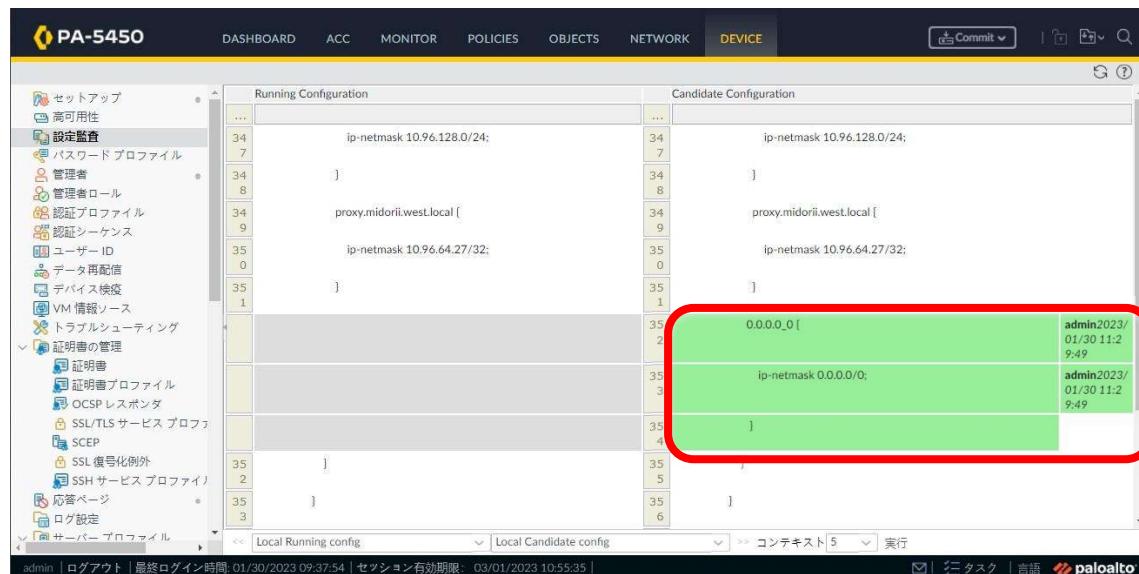


図 4-3-1-3 config difference

補足 2：設定変更前のコンフィグに戻す方法（直近のコミット状態に設定を戻す方法）

GUI および CLI から設定変更を実施し、コミットせずに設定変更を行う前の状態に戻す手順を記載します。CLI からの設定間違えなどで変更内容を破棄したいときに本手順を実施します。

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

- ① 「Device」タブ > 「セットアップ」> 「操作」と辿り、「戻す」> 「実行中の設定に戻します」を選択します。



図 4－3－1 4 revert to running-config

- ② 「実行中の設定に戻します。続行しますか？」と聞かれるので「はい」を押下します。



図 4－3－1 5 revert to running-config

- ③ 「閉じる」を押下します。



図 4－3－1 6 revert to running-config

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」ボタンがグレーアウト状態になっていることを確認します。



図 4－3－17 revert to running-config

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. ファイアウォールポリシー追加/修正/削除

この項では、ファイアウォールポリシーの設定方法について、アドレス設定、サービス設定、ポリシー設定に分けて記載しています。

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

5. 1. ファイアウォールポリシー追加

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

送信元/宛先ゾーンは同一の 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。

※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。

5. 1. 1. アドレス設定

表 5-1-1 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

- 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

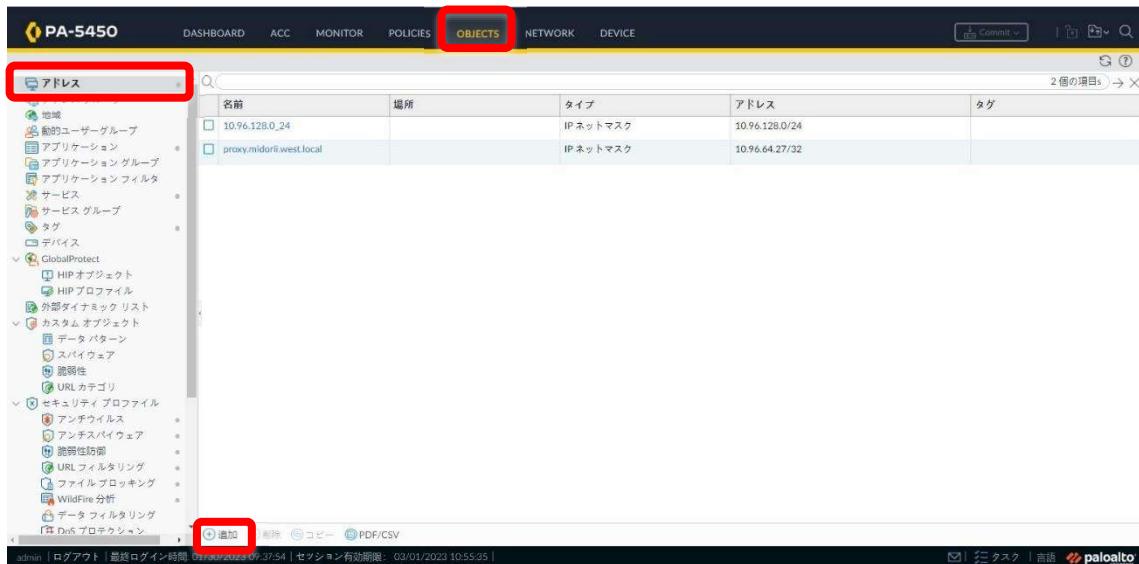


図 5－1－1 PA-5450 Security Policies Add

- ② 以下 (1) ~ (3) を設定（「表 5－1－1」を参照）し、「OK」ボタンをクリックします。

図 5－1－2 PA-5450 Security Policies Add

5. 1. 2. サービス設定

表 5－1－2 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
(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

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

The screenshot shows the PA-5450 interface. The top navigation bar has tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS (highlighted with a red box), NETWORK, and DEVICE. On the left, there's a sidebar with categories like Addresses, Services, Tags, and GlobalProtect. Under GlobalProtect, there are sub-options like IP Objects, Firewall Rules, and URL Filtering. The main area is titled 'Services' and contains a table with three rows: Service-http, Service-https, and TCP_8080. Below the table is a large red box highlighting the 'Add' button at the bottom left of the service configuration area.

図 5－1－3 PA-5450 Security Policies Add

② 以下 (1) ~ (3) を設定（「表 5－1－2」を参照）し、「OK」ボタンをクリックします。

This screenshot shows the 'Service' configuration dialog. It includes fields for Name (名前) containing 'test_TCP_50700-50799' (1), Protocol (プロトコル) with TCP selected (2), Destination Port (宛先ポート) set to '50700-50799' (3), and an OK button at the bottom right highlighted with a red box.

図 5－1－4 PA-5450 Security 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

5. 1. 3. ポリシー設定

表 5-1-3 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)	全般	タグ	「ポリシー適用先の VR 名」を入力 例：Internet_VR、SHD_VR(G 会社)
(3)	送信元	送信元ゾーン ※『0.5.VR のゾーン名一覧表』	「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)
(4)	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)
(5)	宛先	宛先ゾーン ※『0.5.VR のゾーン名一覧表』	「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)
(6)	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)
(7)	アプリケーション	アプリケーション	ping、icmp のプロトコルを許可する場合は、 本項目で「ping」、「icmp」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 ※「ping」、「icmp」以外は、デフォルトのまま
(8)	サービス/URL カテゴリ	サービス/URL カテゴリ	ping、icmp の場合：「application-default」を選択 any の場合：「any」を選択 指定する場合：「追加」ボタンをクリックし、指定のサービスを選択 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 ※複数指定する場合は、「追加」ボタンにて追加
(9)	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
(10)	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 ・「プロファイルタイプ」を指定する (UTM 機能を有効) 場合：「プロファイル」 ※各 UTM 機能を有効化する場合は、各プロファイルをプルダウンより指定 「アンチウイルス」：「JSOC」を指定 「脆弱性防御」：「JSOC」を指定 「アンチスパイウェア」：「JSOC」を指定 「URL フィルタリング」：プロキシサーバ宛のポリシーでのみ、手順「7-1-3」で作成した「URL プロファイル」を指定 ・「プロファイルタイプ」を指定しない (UTM 機能を無効) 場合：「None」
(11)	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」 > 「追加」ボタンをクリックします。

図 5－1－5 PA-5450 Security Policies Add

③ 以下 (1) ~ (11) を設定（「表 5－1－3」を参照）し、「OK」ボタンをクリックします。

名前	(1)
ルールタイプ	universal (default)
内容	
タグ	(2)
監査コメント	

図 5－1－6 PA-5450 Security 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



図 5－1－7 PA-5450 Security Policies Add

表 5－1－3 (4) 送信元アドレスを入力します。

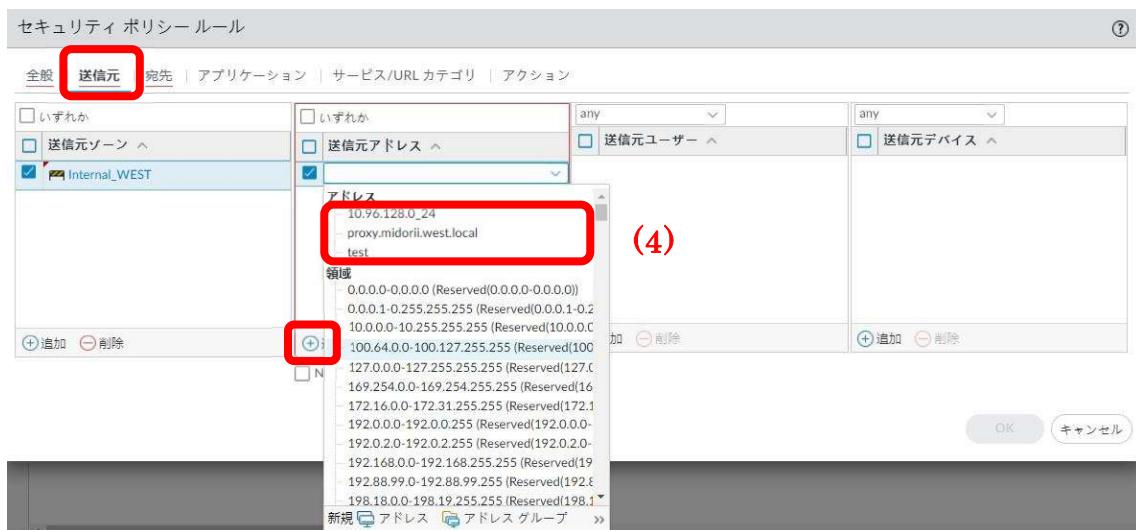


図 5－1－8 PA-5450 Security Policies Add

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 5-1-3 (5)宛先ゾーンを入力します。



図 5-1-9 PA-5450 Security Policies Add

表 5-1-3 (6)宛先アドレスを入力します。

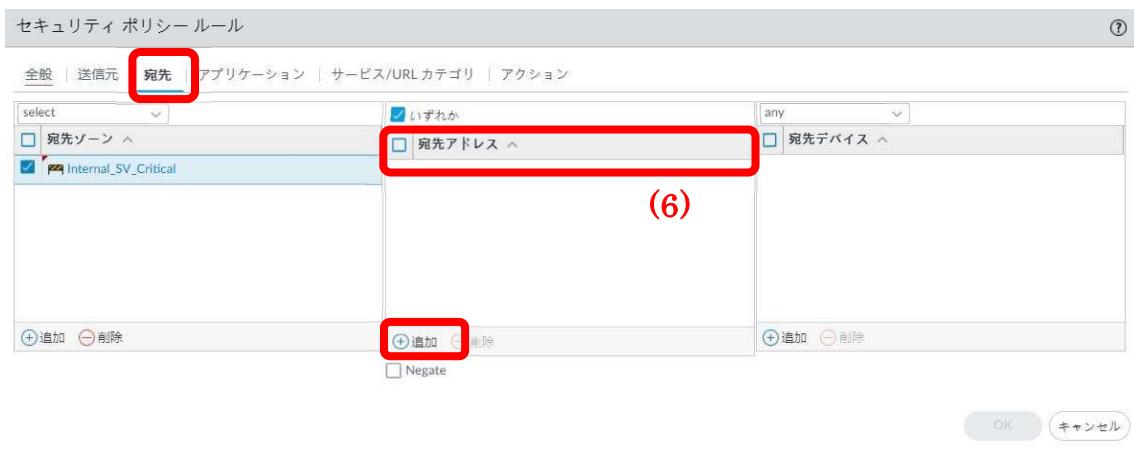


図 5-1-10 PA-5450 Security Policies Add

表 5-1-3 (7) アプリケーションを入力します。

※プロトコルで「ping」「icmp」を指定する場合は「アプリケーション」にて選択します。

「ping」「icmp」以外はデフォルトのままで変更しない。

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



図 5－1－1－1 PA-5450 Security Policies Add

表 5－1－3 (8) サービス/URL カテゴリ

※プロトコルで「ping」「icmp」を指定した場合は「application-default」を選択します。



図 5－1－1－2 PA-5450 Security Policies Add

※プロトコルで「ping」「icmp」以外の場合は、「Service」が「any」の場合は「any」を選択します。

指定する場合は「選択」を選択、「追加」を押下し、対象のサービスを選択します。



図 5－1－1－3 PA-5450 Security 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5－1－3（8）サービス/URL カテゴリを入力します。

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

select

□ サービス ▲

TCP_8080

サービス

- service-http
- service-https
- TCP 8080
- test_TCP_50700-50799

新規 新規 サービス サービス グループ

(8)

(9)

(+) 追加 (⊖) 削除

(+) 追加 (⊖) 削除

OK キャンセル

図5－1－14 PA-5450 Security Policies Add

表5－1－3（9）アクションを入力します。

表5－1－3（10）プロファイルタイプを入力します。

※UTM機能を有効化するときに選択します。

表5－1－3（11）ログ設定を入力します。

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 (9)

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 (10)

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_URL_Profile_001

ファイル ブロックング None

データ フィルタリング None

WildFire 分析 None

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 (11)

ログ転送 test_profile_log_Forwarding

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5－1－15 PA-5450 Security 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

5. 1. 4. 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「intrazone-default」の上に作成されます。

図 5－1－16 PA-5450 Security Policies Add

CLI でポリシーを移行する手順は下記です。コマンドにて移動したあとにコミットします。

表 5－1－4 ポリシー移動

名前	説明
name1, name2 (rules)	name1: 「移動させたいポリシー」を入力 name2: 「移動先ポリシー」を入力

構文（先頭へ移動する）

```
move rulebase security rules <name1> top
```

例（Trsut2_DMZ_1 という名前のポリシーを先頭に移動する）

```
move rulebase security rules Trsut2_DMZ_1 top
```

構文（指定したポリシーの下に移動する）

```
move rulebase security rules <name1> after <name2>
```

例（「Trsut2_DMZ_1」という名前のポリシーを「Trust2_Untrust2_1」の下に移動する）

```
move rulebase security rules Trsut2_DMZ_1 after Trust2_Untrust2_1
```

5. 1. 5. 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。

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

(設定が反映されるまで 5 分程度かかることがあります。)

名前	タグ	タイプ	送信元		宛先		ゾーン	アドレス
			ゾーン	アドレス	ユーザー	デバイス		
test1	none	universal	Internal_WEST	10.96.128.0_24	any	any	Internal_SV_Critical	any
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

図 5－1－17 PA-5450 Security Policies Add

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 5－1－18 PA-5450 Security 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

5. 2. ファイアウォールポリシー修正

ファイアウォールポリシーの修正手順を記載します。

- ① 「Policies」タブ > 「セキュリティ」 > 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	タイプ	ゾーン	送信元	宛先
1 test1	none	universal	Internal_WEST	10.96.128.0_24	any
2 rule1	none	universal	trust	any	any
3 intrazone-default	none	intrazone	any	any	any
4 interzone-default	none	interzone	any	any	any

図 5－2－1 PA-5450 Security Policies Modify

- ② 修正対象のタブを押下し、修正後（手順は「5. 1. 3」を参照）、「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

名前: test1
ルール タイプ: universal (default)

内容:

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 5－2－2 PA-5450 Security 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)

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
test1	none	universal	Internal_WEST	10.96.128.0_24	any	any	Internal_SV_Critical	any
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

図 5－2－3 PA-5450 Security 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			

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 5－2－4 PA-5450 Security 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

5. 3. ファイアウォールポリシー削除

ファイアウォールポリシーの削除手順を記載します。

- ① 「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。

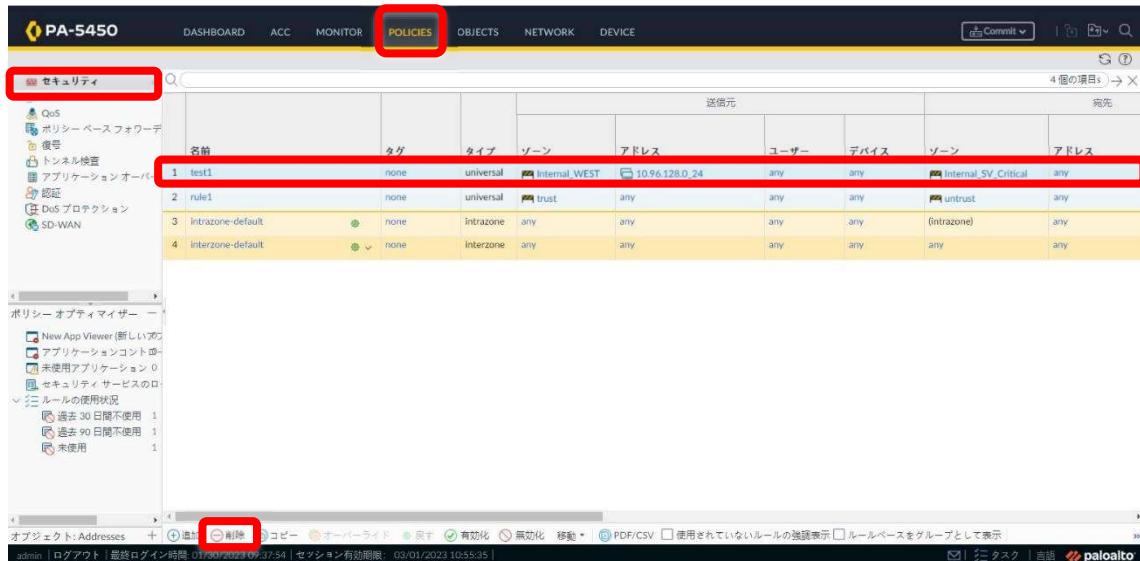


図 5－3－1 PA-5450 Security Policies Delete

- ② 「はい」ボタンをクリックします。



図 5－3－2 PA-5450 Security 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)



The screenshot shows the PA-5450 Security Policies Delete interface. At the top, there is a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (which is selected), and a search bar. Below the navigation bar, there is a breadcrumb trail: セットアップ > 管理 > 操作 > サービス > インターフェイス > テレメトリー > コンテンツ ID > WildFire > セッション > HSM > ACE > DLP.

The main area is titled "図 5 – 3 – 3 PA-5450 Security Policies Delete". It contains a "Commit" section with the following content:

- 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。"
- Two radio buttons: "Commit すべての変更" (selected) and "Commit 変更の実行者:(1) admin"
- A table with one row:

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			
- Buttons at the bottom: "変更内容の確認", "変更サマリー", and "コミットの検証".
- A note: "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。"
- A text input field labeled "内容" with placeholder text "内容".
- Buttons at the bottom right: "コミット" (highlighted with a red box) and "キャンセル".

図 5 – 3 – 4 PA-5450 Security 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

6. NAT ポリシー追加/修正/削除

この項では NAT を使用する為に必要な設定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

6. 1. NAT ポリシー追加

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

6. 1. 1. アドレス設定

表 6-1-1 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

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

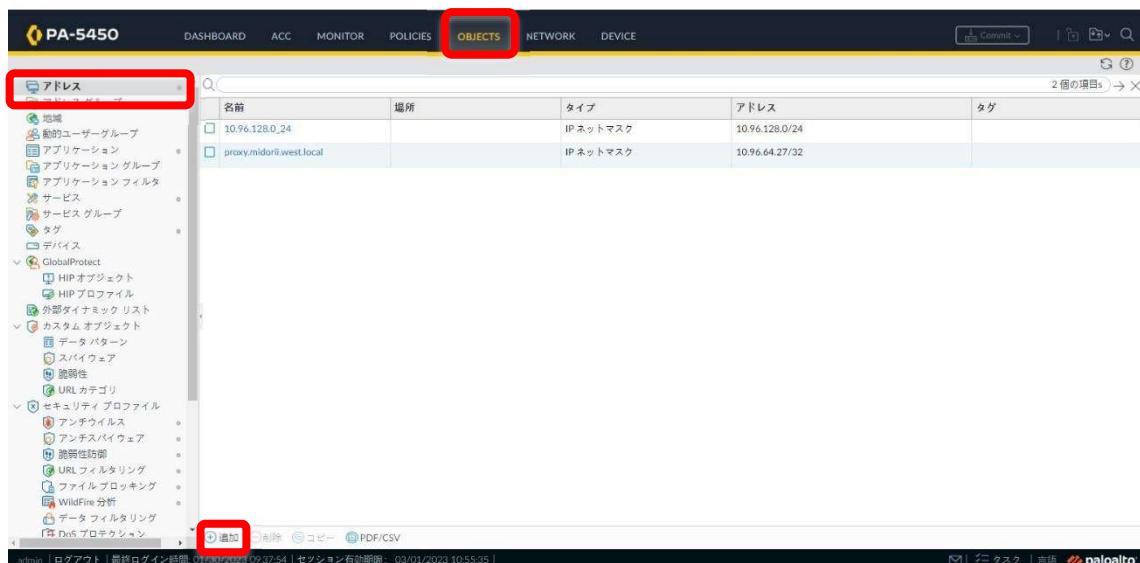


図 6-1-1 PA-5450 NAT Policies Add

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

- ② 以下(1)～(3)を設定（「表 6－1－1」を参照）し、「OK」ボタンをクリックします。



図 6－1－2 PA-5450 NAT Policies Add

6. 1. 2. ポリシー設定

表 6－1－2 NAT ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「NAT 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)	元のパケット	送信元ゾーン ※『0.5. VR のゾーン名一覧表』	「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)	元のパケット	宛先ゾーン ※『0.5. VR のゾーン名一覧表』	「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
(4)	元のパケット	送信元アドレス	StaticNAT の場合 : 「NAT 変換前の送信元アドレス」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 DynamicNAT の場合 : 未指定（「いずれか」にはチェックを入れたままでよい）
(5)	変換済みパケット	変換タイプ	StaticNAT の場合 : 「スタティック IP」を選択 DynamicNAT の場合 : 「ダイナミック IP およびポート」を選択
		変換タイプ	StaticNAT の場合 : 未指定 DynamicNAT の場合 : 「変換後アドレス」を選択
(6)	変換済みパケット	変換後アドレス	StaticNAT の場合 : 「NAT 変換後の送信元アドレス」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) DynamicNAT の場合 : 「NAT 変換後の送信元アドレス」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)

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)	変換済みパケット	双方向	双方向で StaticNAT を有効 する場合：「双方向」にチェック
-----	----------	-----	------------------------------------

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

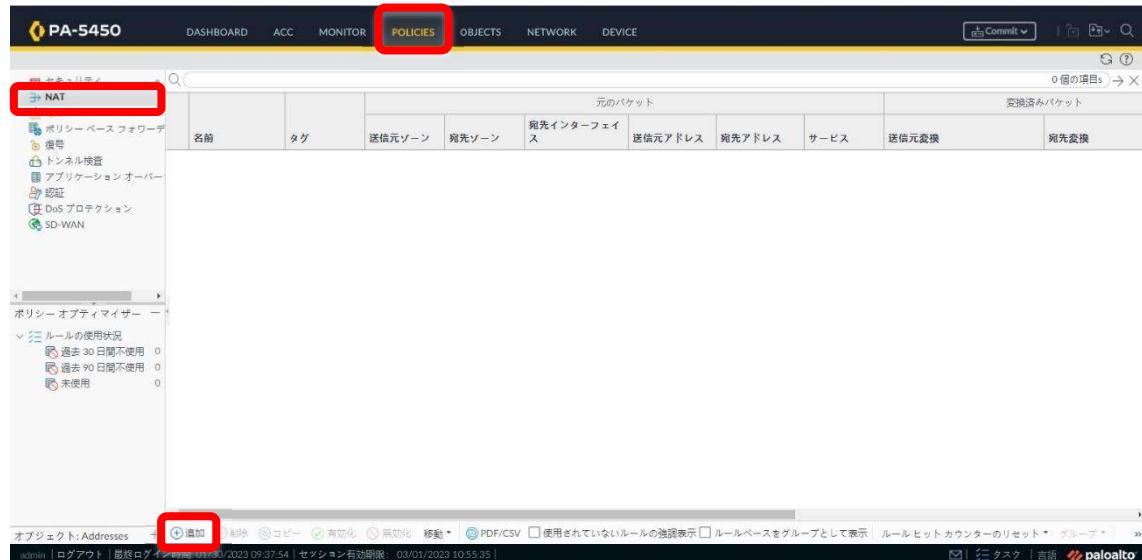


図 6-1-3 PA-5450 NAT Policies Add

- ① 以下 (1) ~ (6) を設定（「表 6-1-2」を参照）し、「OK ボタン」をクリックします。

名前	(1)
内容	
タグ	
タグによるルールのグループ分け	None
NAT タイプ	ipv4
監査コメント	
監査コメント アーカイブ	
OK キャンセル	

図 6-1-4 PA-5450 NAT 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 6－1－2 (2) 送信元ゾーンを入力します。

NAT ポリシールール

全般 元のパケット 変換済みパケット

<input type="checkbox"/> いずれか	<input checked="" type="checkbox"/> 送信元ゾーン	<input type="checkbox"/> Internal_SV_Critical	<input checked="" type="checkbox"/> いずれか	<input type="checkbox"/> 送信元アドレス	<input checked="" type="checkbox"/> 宛先アドレス
<input checked="" type="checkbox"/> Internal_WEST			<input checked="" type="checkbox"/> Internal_SV_Critical		
Internal_SV_Critical			Internal_WEST		
Internal_WEST			any		
trust					
untrust					
<input type="button" value="追加"/>	<input type="button" value="削除"/>		<input type="button" value="追加"/>	<input type="button" value="削除"/>	<input type="button" value="追加"/>

(2)

OK キャンセル

図 6－1－5 PA-5450 NAT Policies Add

表 6－1－2 (3) 宛先ゾーンを入力します。

NAT ポリシールール

全般 元のパケット 変換済みパケット

<input type="checkbox"/> いずれか	<input type="checkbox"/> 送信元ゾーン	<input type="checkbox"/> Internal_SV_Critical	<input checked="" type="checkbox"/> いずれか	<input type="checkbox"/> 送信元アドレス	<input checked="" type="checkbox"/> 宛先アドレス
<input checked="" type="checkbox"/> Internal_WEST		Internal_SV_Critical	<input checked="" type="checkbox"/> Internal_SV_Critical		
Internal_WEST			Internal_SV_Critical		
Internal_SV_Critical			any		
Internal_WEST					
trust					
untrust					
<input type="button" value="追加"/>	<input type="button" value="削除"/>		<input type="button" value="追加"/>	<input type="button" value="削除"/>	<input type="button" value="追加"/>

(3)

OK キャンセル

図 6－1－6 PA-5450 NAT 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 6-1-2 (4) 送信元アドレスを入力します。(StaticNAT の場合)

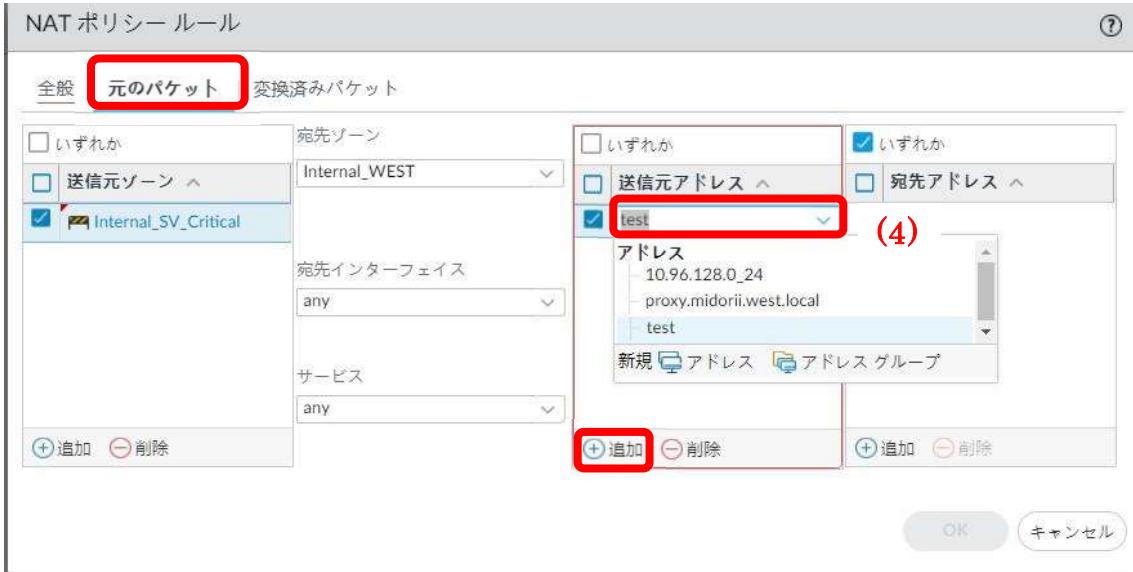


図 6-1-7 PA-5450 NAT Policies Add (StaticNAT の場合)

表 6-1-2 (4) 送信元アドレスを入力します。(DynamicNAT の場合)



図 6-1-8 PA-5450 NAT Policies Add (DynamicNAT の場合)

表 6-1-2 (5) 変換タイプを入力します。

表 6-1-2 (6) 変換後アドレス(例)を入力します。

表 6-1-2 (7) 双方向を入力します。

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 6－1－9 PA-5450 NAT Policies Add (StaticNAT の場合)

表 6－1－2 (5) 変換タイプ、アドレスタイプを入力します。

表 6－1－2 (6) 変換後アドレス(例) を入力します。



図 6－1－10 PA-5450 NAT Policies Add (DynamicNAT の場合)

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

6. 1. 3. ポリシー移動

- ① 作成したポリシーを選択し、「移動」にて任意の位置に移動します。

The screenshot shows the 'PA-5450' interface with the 'POLICIES' tab selected. Under the 'NAT' section, there is a table of policies. A policy named 'test1' is selected and highlighted with a red box. Below the table, a 'Move' button is highlighted with a red box. A dropdown menu next to the 'Move' button shows options: '最上部へ', '↑ 上へ', '↓ 下へ', and '↓ 最下部へ'. The bottom of the screen shows various navigation and status buttons.

図 6-1-1-1 PA-5450 NAT Policies Add

6. 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 'POLICIES' tab selected. Under the 'セキュリティ' section, there is a 'Commit' button highlighted with a red box. The bottom of the screen shows various navigation and status buttons.

図 6-1-1-2 PA-5450 Security Policies Add

The screenshot shows a 'Commit' dialog box. It contains a message about committing changes and two radio button options: '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: 'コミット スコープ' is set to 'policy-and-objects', '場所タイプ' is 'Policy and Objects', 'オブジェクトタイプ' is empty, 'エンティティ' is empty, and '管理者' is empty. At the bottom, there are buttons 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。' Below is a '内容' input field, and at the bottom right are 'コミット' and 'キャンセル' buttons, with 'コミット' highlighted with a red box.

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 6－1－1 3 PA-5450 Security Policies Add

6. 2. NAT ポリシー修正

NAT ポリシーの修正手順を記載します。

- ① 「Policies」タブ > 「NAT」> 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	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
1 test	none	Internal_SV...	Internal_W...	any	any	any	dynamic-ip-and-port 10.96.128.0_24
2 test1	none	any	Internal_SV...	any	any	any	none なし

図 6－2－1 PA-5450 NAT Policies Modify

- ② 修正対象のタブを押下し、修正後（手順は「6. 1. 2」を参照）、「OK」ボタンをクリックします。

名前	test1
内容	
タグ	
タグによるルールのグループ分け	None
NATタイプ	ipv4
監査コメント	
監査コメント アーカイブ	
<input type="button" value="OK"/> <input type="button" value="キャンセル"/>	

図 6－2－2 PA-5450 NAT 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 6－2－3 PA-5450 NAT Policies Modify

The screenshot shows a '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(1) admin'. A table below shows settings: 'コミットスコープ' is 'policy-and-objects', '場所タイプ' is 'Policy and Objects', 'オブジェクトタイプ' is empty, 'エンティティ' is empty, and '管理者' is empty. At the bottom, there are links for '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 is a '内容' (Content) input field. The 'Commit' button is highlighted with a red circle.

図 6－2－4 PA-5450 NAT 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

6. 3. NAT ポリシー削除

NAT ポリシーの削除手順を記載します。

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

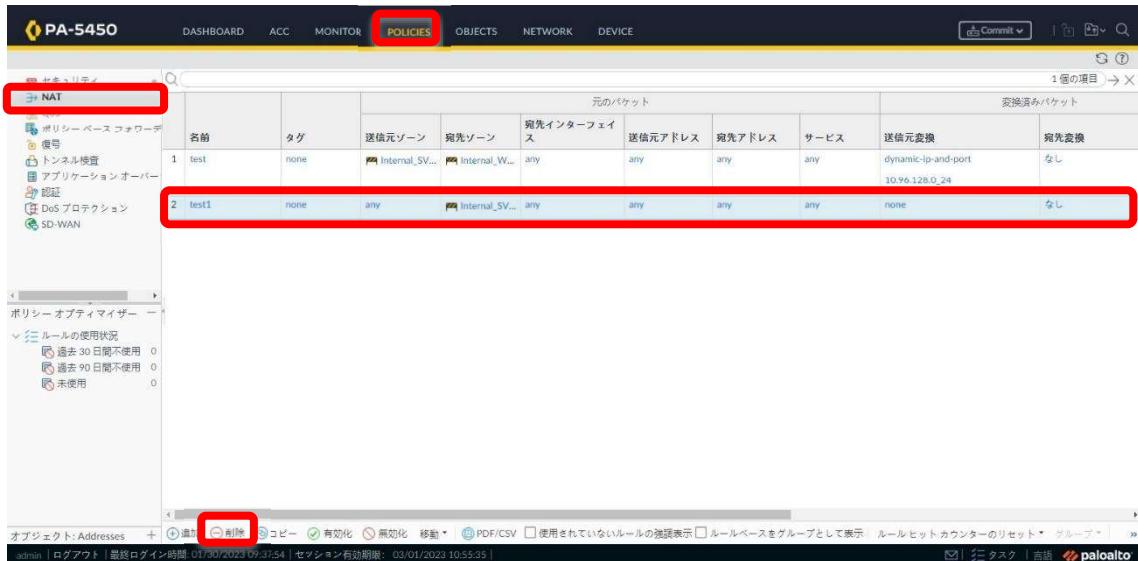


図 6－3－1 PA-5450 NAT Policies Delete

- 「はい」ボタンをクリックします。



図 6－3－2 PA-5450 NAT 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 6－3－3 PA-5450 Security Policies Delete

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 6－3－4 PA-5450 Security 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

6. 4. グループ会社向け NAT 設定例

6. 4. 1. グループ会社セグメントの NAT 修正例

G 会社の設定済み NAT アドレスを修正する時の設定変更手順を記載します。

具体例としてグループ会社「SHD」に設定済みの NAT 設定を修正する例になります。

※VSYS 機能を利用しないと伴い、

各グループ会社の NAT ポリシーの追加/修正/削除は各グループ会社 VR で行い、
NAT 設定時、送信元/宛先ゾーンはグループ会社 VR に所属しているゾーンを指定します。
本書の『0.5. VR のゾーン名一覧表』を参照してください。

(1) グループ会社側セグメントの IP（送信元アドレス）を変更する場合

- 「Policies」タブ > 「NAT」> 変更対象のポリシー名を選択し、クリックします。

※グループ会社「SHD_VR」に設定しているポリシーを選択します。

名前	タグ	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	宛先変換
test	none	Internal_W...	Internal_SV...	any	any	any	any	dynamic-ip-and-port	なし
test1	none	any	Internal_SV...	any	any	any	any	10.96.128.0_24	なし
SHD_G-Trust_SHD_G...	none	SHD_G-Trust	SHD_G-Un...	any	172.21.193...	10.86.64.0_24	any	none	なし

図 6-4-1 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 送信元アドレスを直接編集し、アドレスを変更します。

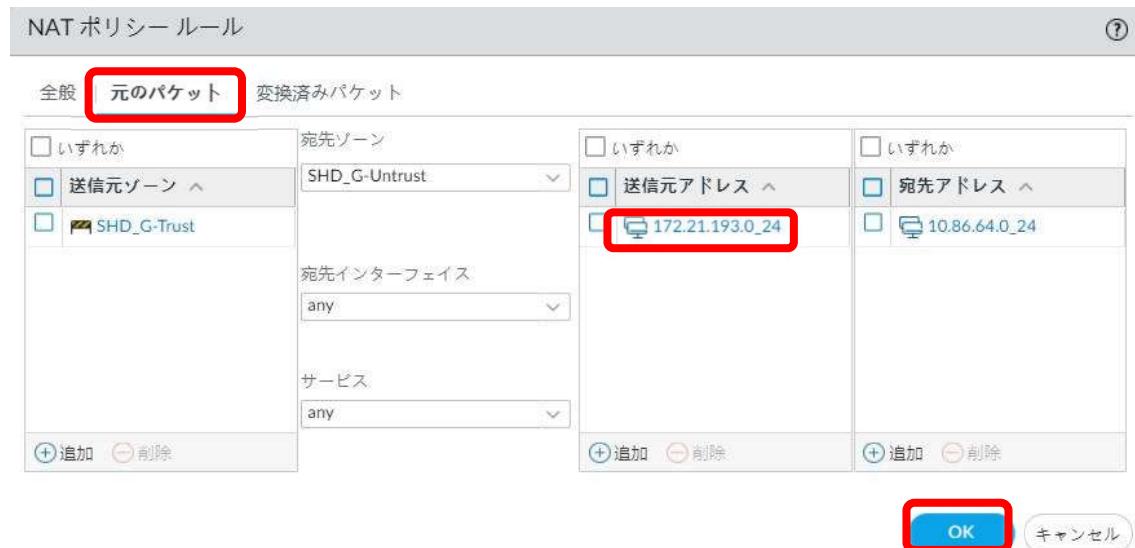


図 6－4－2 PA-5450 Security NAT Policies change

- 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)

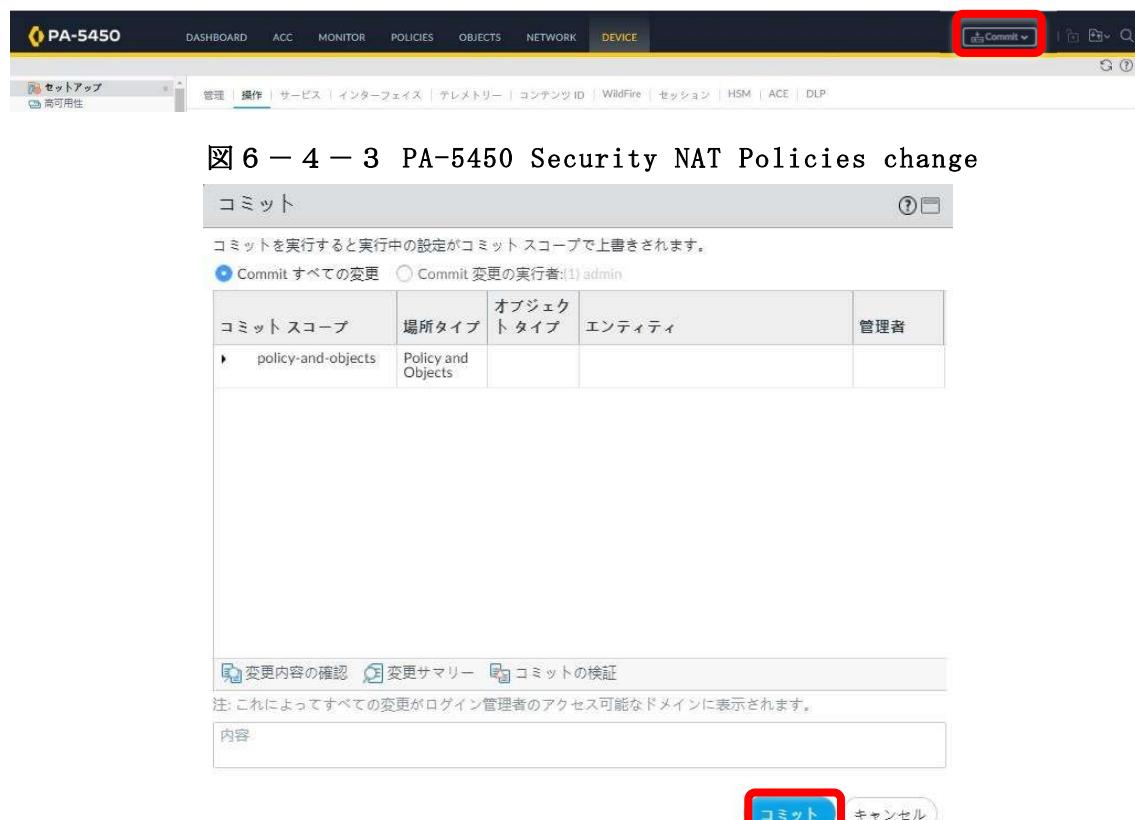


図 6－4－3 PA-5450 Security NAT Policies change

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) NAT 変換後のアドレスを変更する場合を記載します。

① 「Policies」タブ > 「NAT」> 変更対象のポリシー名を選択し、クリックします。

※グループ会社「SHD_VR」に設定しているポリシーを選択します。

図 6－4－4 PA-5450 Security NAT Policies change

② 変換後アドレスを直接編集し、アドレスを変更します。

図 6－4－5 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

- 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 6-4-6 PA-5450 Security NAT Policies change

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 6-4-7 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

6. 4. 2. グループ会社/本体の公開サーバの NAT 追加、修正例

本体もしくは G 会社が公開しているサーバの NAT アドレスを追加、修正する手順を記載します。

※VSYS 機能を利用しないと伴い、

各グループ会社の NAT ポリシーの追加/修正/削除は各グループ会社 VR で行い、

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

本書の『0.5. VR のゾーン名一覧表』を参照してください。

G 会社の公開サーバを追加もしくは変更する手順を記載します。

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

ここでは例として SHD に追加する手順を記載します。

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	10.96.128.0_24	なし
SHD_G-Trust_SHD_G...	none	SHD_G-Trust	SHD_G-Un...	any	172.21.193...	10.86.64.0_24	any	none

図 6-4-7 PA-5450 Security NAT Policies Add and Change

② 以下(1)～(7)を設定（「図中説明、表 6-4-1」を参照）し、「OK ボタン」をクリックします。

表 6-4-1 NAT ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「NAT 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)	元のパケット	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)	元のパケット	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）

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)	元のパケット	送信元アドレス	StaticNAT の場合：「NAT 変換前の送信元アドレス」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 DynamicNAT の場合：未指定（「いずれか」にはチェックを入れたままでよい）
(5)	変換済みパケット	変換タイプ	StaticNAT の場合：「静态 IP」を選択 DynamicNAT の場合：「ダイナミック IP およびポート」を選択
		変換タイプ	StaticNAT の場合：未指定 DynamicNAT の場合：「変換後アドレス」を選択
(6)	変換済みパケット	変換後アドレス	StaticNAT の場合：「NAT 変換後の送信元アドレス」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) DynamicNAT の場合：「NAT 変換後の送信元アドレス」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)
(7)	変換済みパケット	双方向	双方向で StaticNAT を有効する場合：「双方向」にチェック

表 6-4-2 (1) ポリシー名を入力します。

NAT ポリシー ルール

全般 元のパケット | 変換済みパケット

名前 (1)

内容

タグ

タグによるルールのグループ分け

NAT タイプ ipv4

監査コメント

監査コメント アーカイブ

OK キャンセル

図 6-4-8 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

表 6-4-1 (2) 送信元ゾーンを入力します。

新規セグメントを追加するグループ会社のゾーンを選択します。

ここでは（例）「SHD_G-Trust」ゾーンを選択します。



図 6-4-9 PA-5450 Security NAT Policies Add and Change

表 6-4-1 (3)宛先ゾーンを入力します。

ここでは（例）「SHD_G-Untrust」ゾーンを選択します。



図 6-4-10 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

表 6－4－1 (4) 送信元アドレスを入力します。

※送信元アドレスを直接入力します。

※送信元アドレスを変更する場合は直接編集し、変更します。

※アドレスオブジェクトは設定済みの場合は直接選択します。



図 6－4－1 1 PA-5450 Security NAT Policies Add and Change

表 6－4－1 (5) 変換タイプを入力します。

表 6－4－1 (6) 変換後アドレスを入力します。

表 6－4－1 (7) 双方向を入力します。

※NAT 変換後のアドレスを変更する場合は、(6) 変換後アドレスを直接編集し、アドレスを変更します。



図 6－4－1 2 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

- 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)

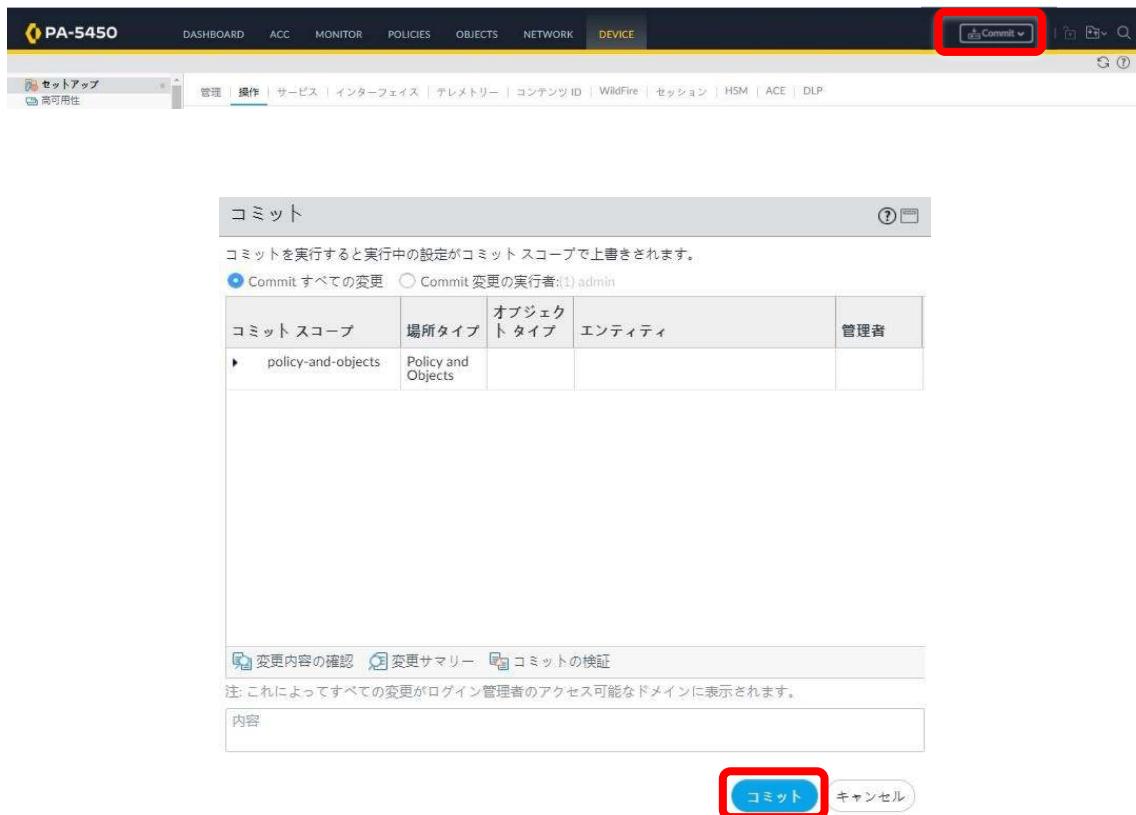


図 6－4－1 4 PA-5450 Security NAT Policies Add and Change

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

(2) 本体の公開サーバを追加もしくは変更する手順を記載します。

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

※WEST_VR(内部接続用VR)に適用するポリシー、

送信元/宛先ゾーンは WEST_VR に所属しているゾーンを指定します。

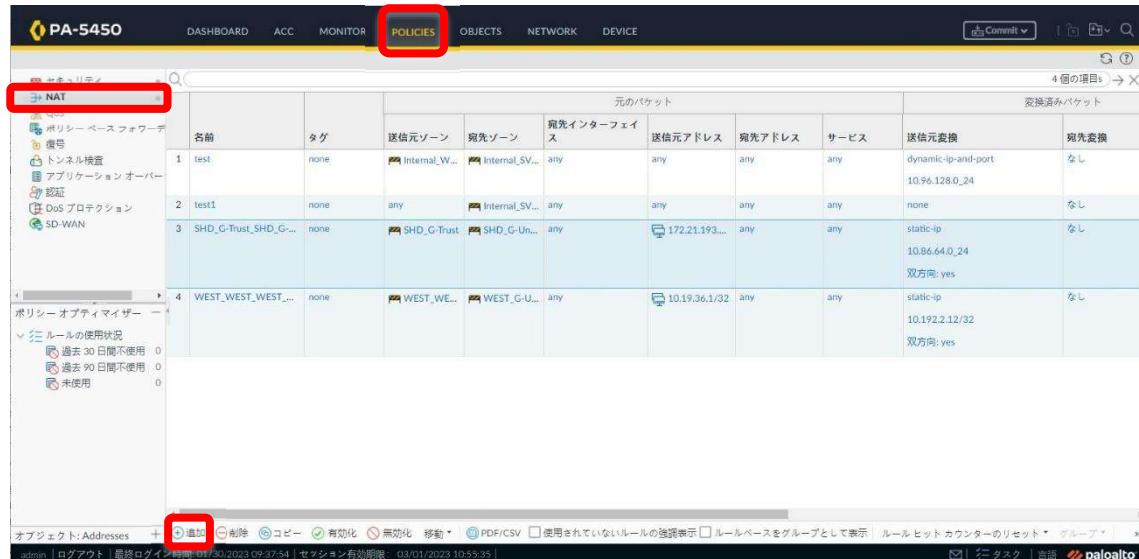


図 6-4-15 PA-5450 Security NAT Policies Add and Change

② 以下(1)～(7)を設定（「図中説明、表 6-4-2」を参照）し、「OK ボタン」をクリックします。

表 6-4-2 NAT ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	Name	「NAT 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)	元のパケット	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)	元のパケット	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）
(4)	元のパケット	送信元アドレス	StaticNAT の場合：「NAT 変換前の送信元アドレス」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 DynamicNAT の場合：未指定（「いずれか」にはチェックを入れたままでよい）
(5)	変換済みパケット	変換タイプ	StaticNAT の場合：「静态 IP」を選択 DynamicNAT の場合：「ダイナミック IP およびポート」を選択
		変換タイプ	StaticNAT の場合：未指定

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

			DynamicNAT の場合：「変換後アドレス」を選択 StaticNAT の場合：「NAT 変換後の送信元アドレス」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) DynamicNAT の場合：「NAT 変換後の送信元アドレス」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)
(6)	変換済みパケット	変換後アドレス	
(7)	変換済みパケット	双方向	双方向で StaticNAT を有効する場合：「双方向」にチェック

表 6-4-2 (1) ポリシー名を入力します。



図 6-4-16 PA-5450 Security NAT Policies Add and Change

表 6-4-2 (2) 送信元ゾーンを入力します。ゾーン「WEST_WEST」を選択します。



図 6-4-17 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

表 6-4-2 (3)宛先ゾーンを入力します。ゾーン「WEST_G-Untrust」を選択します。

NAT ポリシールール

元のパケット

□ いずれか	宛先ゾーン
□ 送信元ゾーン ▾	WEST_G-Untrust
<input checked="" type="checkbox"/> WEST_WEST	
<input type="button" value="+ 追加"/> <input type="button" value="○ 削除"/>	

□ いずれか	いずれか
□ 送信元アドレス ▾	10.19.36.1/32
<input checked="" type="checkbox"/> 宛先アドレス ▾	
<input type="button" value="+ 追加"/> <input type="button" value="○ 削除"/>	

(3)

OK キャンセル

図 6-4-18 PA-5450 Security NAT Policies Add and Change

表 6-4-2 (4) 送信元アドレスを入力します。

※送信元アドレスを直接入力します。

※送信元アドレスを変更する場合は直接編集し、変更します。

※アドレスオブジェクトは設定済みの場合は直接選択します。

NAT ポリシールール

元のパケット

□ いずれか	宛先ゾーン
□ 送信元ゾーン ▾	WEST_G-Untrust
<input checked="" type="checkbox"/> WEST_WEST	
<input type="button" value="+ 追加"/> <input type="button" value="○ 削除"/>	

□ いずれか	いずれか
□ 送信元アドレス ▾	10.19.36.1/32
<input checked="" type="checkbox"/> 宛先アドレス ▾	
<input type="button" value="+ 追加"/> <input type="button" value="○ 削除"/>	

(4)

OK キャンセル

図 6-4-19 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

表 6-4-2 (5) 変換タイプを入力します。

表 6-4-2 (6) 変換後アドレスを入力します。

表 6-4-2 (7) 双方向を入力します。

※NAT 変換後のアドレスを変更する場合は、変換後アドレスを直接編集し、アドレスを変更します。



図 6-4-2 1 PA-5450 Security NAT Policies Add and Change

③ ポリシー移動

作成したポリシーを選択し、「移動」にて、上に移動します。

※「StaticNAT」を「DynamicNAT」より優先して動作させる為移動します。

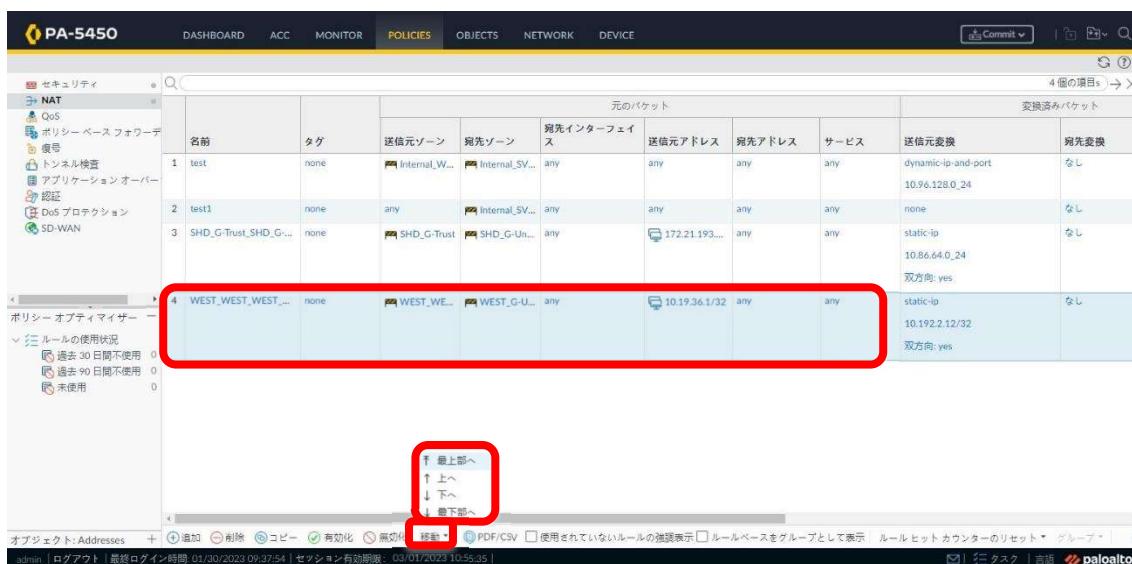


図 6-4-2 2 PA-5450 Security NAT Policies Add and Change