

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

				<reason>	失敗した理由。
general	informational	general	Failed to lock URL database update process! Maybe another instance is running.		URL フィルタリングデータベースのアップデートプロセスのロックが失敗しました。他のインスタンス(処理)が動作中と考えられます。
general	medium	general	Failed to upgrade Antivirus package to version <version>		バージョン <version>へのアンチウイルスパッケージのアップグレードが失敗しました。 <version> アップグレードしようとしたアンチウイルスパッケージバージョン。
general	medium	general	Failed to upgrade Application identification/Threat detection package to version <unknown version>/<unknown version>		Panorama 経由で行ったバージョン不明のApp-ID シグネチャとバージョン不明の脅威防御シグネチャへのアップグレードが失敗しました。
general	medium	general	Failed to upgrade Application identification/Threat detection package to version <version1>/<version2>		Panorama 経由で行ったバージョン <version1> の App-ID シグネチャとバージョン <version2> の脅威防御シグネチャへのアップグレードが失敗しました。 <version1> App-ID シグネチャのバージョン <version2> 脅威防御シグネチャのバージョン
general	critical	general	Fan #<fan_id> Speed: <speed> below low-limit 9500.00		ファンの回転数が最小閾値を下回りました。 <fan_id> ファンの番号 <speed> ファンの回転数（単位 rpm、小数点以下 2 術）
general	high	general	FIPS Mode Enabled Successfully		FIPS モードが正常に有効化されました。
general	medium	general	Generated shared policy and committed to device <device_name>		管理デバイス <device_name> にシェアードポリシーが生成されコミットされました。 本メッセージは Panorama の system log でのみ表示されます。
general	informational	general	HA control link statistics cleared by <admin_user>		管理ユーザ <admin_user> により HA コントロールリンクの統計情報がクリアされました。

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	informational	general	HA file sync performed by < admin_user >	管理ユーザにより HA のファイル同期が実施されました。< admin_user > ファイル同期を行った管理ユーザ名。CLI にて "request high-availability sync-to-remote disk-state" コマンドを実施すると本メッセージが表示されます。
general	medium	general	HA state set to functional by < admin_user >	管理ユーザ < admin_user > により HA 状態が functional に変更されました。
general	medium	general	HA state set to suspended by < admin_user >	管理ユーザ < admin_user > により HA 状態が suspend に変更されました。
general	informational	general	HA transition statistics cleared by < admin_user >	管理ユーザ < admin_user > により HA 状態遷移統計情報がクリアされました。
general	medium	general	Hostname changed to < hostname >	ホスト名が < hostname > に変更されました。 <hostname> 変更されたホスト名
general	critical	general	ID manager is reset	ID マネージャがリセットされました。
general	high	general	Install Anti-virus on < device_name > job failed	管理デバイス < device_name > へのアンチウイルスシグチャのインストール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	Install Anti-virus on < device_name > job succeeded	管理デバイス < device_name > へのアンチウイルスシグチャのインストール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	Install content on < device_name > job succeeded	管理デバイス < device_name > へのコンテンツシグチャのインストール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	Install content on < device_name > job succeeded	管理デバイス < device_name > へのコンテンツシグチャのインストール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	Install software on < <i>device_name</i> > job succeeded	管理デバイス< <i>device_name</i> >へのPANOS ソフトウェアのインストール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	Install software on < <i>device_name</i> > job succeeded	管理デバイス< <i>device_name</i> >へのPANOS ソフトウェアのインストール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	Install vpnclient on < <i>device_name</i> > job failed	管理デバイス< <i>device_name</i> >への SSL VPN クライアントソフトのインストール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	Install vpnclient on < <i>device_name</i> > job succeeded	管理デバイス< <i>device_name</i> >への SSL VPN クライアントソフトのインストール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	informational	general	Installed antivirus package: < <i>file_name</i> >	アンチウイルスパッケージをインストールしました。 < <i>file_name</i> >アンチウイルスパッケージ名。
general	informational	general	ldap cfg < <i>server_name</i> > connected to server < <i>ip_address</i> >:< <i>port_number</i> >	LDAP サーバ設定 < <i>server_name</i> > を使ってサーバ < <i>ip_address</i> > のポート < <i>port_number</i> > に接続しました。 < <i>server_name</i> > LDAP server 名 profile で設定した LDAP サーバ名 < <i>ip_address</i> > LDAP サーバの IP アドレス < <i>port_number</i> > LDAP サーバのポート番号
general	medium	general	ldap cfg < <i>server_name</i> > failed to connect to server < <i>ip_address</i> >:< <i>port_number</i> >: < <i>reason</i> >	LDAP サーバ設定 < <i>server_name</i> > を使ってサーバ < <i>ip_address</i> > のポート < <i>port_number</i> > に接続失敗しました。 失敗の理由は < <i>reason</i> > 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

general	informational	general	ldap daemon become active	LDAP デーモンがアクティブになりました。
general	informational	general	ldap daemon become passive	LDAP デーモンがパッシブになりました。
general	critical	general	License for feature threat will expire on <date>	脅威防御ライセンスが <date> の日付で有効期限切れです。本メッセージは期限切れとなる 30 日前から毎日表示されます。 <date> ライセンス期間満了日
general	critical	general	License for feature url-filtering will expire on <date>	URL フィルタリングライセンスが <date> の日付で有効期限切れです。本メッセージは期限切れとなる 30 日前から表示されます。 <date> ライセンス満了日
general	informational	general	License information refreshed	ライセンス情報がリフレッシュされました。
general	informational	general	localhost.localdomain connected	localhost.localdomain に接続しました。
general	informational	general	localhost.localdomain disconnected	localhost.localdomain から切断しました。
general	informational	general	localhost.localdomainha connected	localhost.localdomainha に接続しました。
general	informational	general	localhost.localdomainha disconnected	localhost.localdomainha から切断しました。
general	informational	general	LOGIN ON ttys0 BY <admin_user>	管理ユーザ <admin_user> が ttys0 (TTY 回線) にログインしました。
general	informational	general	Management server shutting down	管理サーバをシャットダウンしています。
general	informational	general	Management server started. Running version <version>	管理サーバが開始されました。 <version> PANOS バージョン
general	critical	general	Marvell QuadPHY 2 (C): <temp>C above high-threshold 95.00C	CPU の温度が上限 (95°C) を超えました。 <temp> CPU の温度度 (単位 : °C、小数点以下2桁)
general	informational	general	Multi-vsyst mode set to False	複数vsys利用モードが設定されなくなりました。
general	informational	general	Multi-vsyst mode set to True	複数vsys利用モードが設定されました。

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	New web certificate installed by < <i>admin_user</i> >	管理ユーザ< <i>admin_user</i> >により新しいWeb証明書がインストールされました。
general	critical	general	No URL database! Please download one from 'dynamic update page'	URL フィルタリングデータベースが存在しません。 dynamic update ページからデータベースをダウンロードしてください。
general	informational	general	Non-qualified SFP detected on port < <i>number</i> >; vendor '< <i>vendor_name</i> >; part '< <i>part_name</i> >'	サポートしない SFP トランシーバがポート< <i>number</i> >番で検知されました。 < <i>vendor</i> > 検知された SFP のベンダ名 < <i>part_name</i> > 検知された SFP のパート番号
general	informational	general	Pan-Agent connected: IP < <i>ip_address</i> > port < <i>port_number</i> >	IP アドレス< <i>ip_address</i> >上の Pan-Agent にポート番号< <i>port_number</i> >で接続しました。
general	critical	general	Pan-Agent get config error: < <i>ip_address</i> > < <i>number</i> > time(s)	IP アドレス< <i>ip_address</i> >の Pan-Agent でコンフィグの読み込みエラーが< <i>number</i> >回起きました。 < <i>ip_address</i> >Pan-Agent の IP アドレス < <i>number</i> > エラーが起きた回数
general	critical	general	Pan-Agent get domain error: < <i>ip_address</i> >, please check Pan-Agent, log file for actual incorrect DC IP address(es)	IP アドレス< <i>ip_address</i> >の Pan-Agent でドメインエラーが起きました。Pan-Agent のログファイルをチェックし、いずれかのドメインコントローラの IP アドレスが間違っていないか確認してください。
general	critical	general	Pan-Agent get groups error: < <i>ip_address</i> > < <i>number</i> > time(s)	IP アドレス< <i>ip_address</i> >の Pan-Agent でグループの読み込みエラーが< <i>number</i> >回起きました。 < <i>ip_address</i> >Pan-Agent の IP アドレス < <i>number</i> >エラーが起きた回数
general	critical	general	Pan-Agent get users error: < <i>ip_address</i> > < <i>number</i> > time(s)	IP アドレス< <i>ip_address</i> >の Pan-Agent でユーザの読み込みエラーが< <i>number</i> >回起きました。 < <i>ip_address</i> >Pan-Agent の IP アドレス < <i>number</i> >エラーが起きた回数

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

general	informational	general	Pan-Agent no allow list: ⟨ip_address⟩	IP アドレス⟨ip_address⟩の Pan-Agent に Allow List の 設定がありません。Allow List の設定は必須です。
general	informational	general	Pan-Agent read log error: ⟨ip_address⟩ ⟨number⟩ time(s)	IP アドレス⟨ip_address⟩の Pan-Agent がドメインコントローラからセキュリティログを⟨number⟩回読み込みませ んでした。ドメインコントローラとの接続性がないか、読み込权限がないと思われます。 ⟨ip_address⟩Pan-Agent の IP アドレス ⟨number⟩ エラーが起きた回数
general	informational	general	Port ⟨number⟩: Down ⟨duplex⟩ duplex	ポート⟨number⟩番が⟨duplex⟩ の速度、デュプレックスでリンクダウンしました。 ⟨number⟩インターフェース番号 ⟨duplex⟩"10Mb/s-half", "10Mb/s full", "100Mb/s half", "100Mb/s-full", "1Gb/s-full"のいずれか
general	informational	general	running configuration synchronized with HA peer by ⟨admin_user⟩	管理ユーザ ⟨admin_user⟩ に よって running 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 ィグを渡しました。 "request high- availability sync-to-remote running- config"コマンドを実施する と 表示されます。
general	informational	general	Session for user ⟨admin_user⟩ via CLI from ⟨ip_address⟩ timed out	管理ユーザ ⟨admin_user⟩ のCLIセッションがタイムアウトしました。 ⟨ip_address⟩管理ユーザのホストの IP アドレス 不明な場合"unknown host"と 表示される。
general	informational	general	Session for user ⟨admin_user⟩ via Web from ⟨ip_address⟩ timed out	管理ユーザ ⟨admin_user⟩ のWebUI セッションがタイ ムアウトしました。 ⟨ip_address⟩管理ユーザのホストの IP アドレス。不明な 場合"unknown host"と表示 される。

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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	Software restart requested by < <i>admin_user</i> >	管理ユーザによりソフトウェアのリスタートが要求されました。 < <i>admin_user</i> >リスタート要求した管理ユーザ名 CLIコマンド "request restart software" を実施すると本メッセージが表示されます。
general	informational	general	SSL connect error(< <i>ip_address</i> >): < <i>reason</i> >	IP アドレス < <i>ip_address</i> > 上の Pan-Agent と SSL 接続エラーが発生しました。 < <i>reason</i> > エラーの理由
general	informational	general	SSL decryption certificate does not exist remember to install one to activate ssl-decryption policy	SSL 復号化ポリシーが設定されましたが、SSL decryption certificate(SSL 復号化用の証明書)が生成されていないか、インポートされていません。 SSL復号化ポリシーを有効にするには、"Device > Certificates > SSL Forward Proxy Certificate"にて self-signed certificate(自己署名証明書)を生成するか、有効な証明書をインポートしてください。
general	informational	general	State-synchronization started by < <i>admin_user</i> >	管理ユーザにより HA のステート同期が開始されました。 < <i>admin_user</i> > ステート同期を行った管理ユーザ名 CLI にて "request high-availability sync-to-remote runtime-state" コマンドを実施すると本メッセージが表示されます。
general	informational	general	synchronized running configuration from HA peer and local candidate configuration	HA ピアの running configuration が、ローカルデバイスの candidate configuration に同期されました。 本メッセージはコンフィグを受け取った側のデバイスでのみ表示されます。 コンフィグを渡す側のデバイスでは "configuration sync'd with HA peer" メッ

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

				セージがsystem log に表示されます。
general	informational	general	System clock synchronized with HA peer by < <i>admin_user</i> >	管理ユーザにより HA ピアとシステムクロックが同期されました。 < <i>admin_user</i> > クロック同期を行った管理ユーザ名 CLI にて "request high-availability sync-to-remote clock" 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	System restart requested by < <i>admin_user</i> >	管理ユーザによりシステム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 > Reboot Device" 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 system" コマンドを実施すると本メッセージが表示されます。
general	critical	general	The dataplane is restarting.	データプレーンがリスタートしました。 "Device > Restart Dataplane" をクリックしてデータプレーンをリスタートさせると本メッセージが表示されます。
general	medium	general	Threat detection package upgraded from version < <i>old_version</i> > to < <i>new_version</i> > by < <i>admin_user</i> >	脅威防御のシグネチャパッケージがアップグレードされました。 < <i>old_version</i> > 前回インストールされていた脅威防御シグネチャ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脅威防御シグネチャパッケージバージョン。 < <i>admin_user</i> > アップグレードを行った管理ユーザ名 自動アップデートの場合は "Auto update agent" と表示される
general	informational	general	Traffic and logging resumed Traffic and logging suspended due to unexported logs	トラフィックとログ取得が再開されました。 ログのエクスポートがされず、トラフィックとログ取得が中断されました。

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	critical	general	Unable to send dataplane-down to HA_agent.	データプレーンから HA エージェントへの送信ができませんでした。
general	medium	general	Unauthorized attempt to change password for user < <i>admin_user</i> > < <i>reason</i> >	管理ユーザがパスワードを変更しようとしましたが、その権限がありませんでした。 < <i>admin_user</i> > パスワード変更しようとした管理者名 < <i>reason</i> > 失敗した理由（オプションで、表示されない場合もある）
general	informational	general	URL filtering database is restored from archive.	URL フィルタリングデータベースがアーカイブからリストアされました。
general	informational	general	URL filtering database version < <i>current_version</i> > is already the latest version	PANOS が最新のURL フィルタリングデータベースを "request url-filtering upgrade" CLI コマンドによりリクエストしましたが、現在インストールされているバージョンが最新のものであるため、アップグレードは実施されませんでした。 < <i>current_version</i> > 現在インストールされているURLフィルタリングデータベースのバージョン。
general	informational	general	URL filtering database was reverted from version < <i>previous_version</i> > to version < <i>current_version</i> >	URL フィルタリングデータベースが以前のバージョンに戻りました。 < <i>previous_version</i> >前回インストールされていた新しいバージョンのURLフィルタリングデータベース。 < <i>current_version</i> >現在インストールされている URL フィルタリングデータベース < <i>current_version</i> >のほうが < <i>previous_version</i> >より古い。
general	informational	general	URL filtering database was upgraded from version < <i>old_version</i> > to version < <i>new_version</i> > by the auto-update agent	URLフィルタリングデータベースがアップグレードされました。データベースは不定期に更新され、"Dynamic Update > URL Filtering" の schedule にて none以外の設定にすると毎日または毎週アップデートが無いか確認し、あればデータベースがアップデートされて本メッセージが表示されます。 < <i>old_version</i> >前回インストールされていたURLフィルタリングデータベースのバージ

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

				ヨン。 最新のバージョンであり、 < <i>old_version</i> >よりも新しい (数値の大きい)。 注) 管理者が URL フィルタ リングデータベースのアッ プグレードを CLI の "request url-filtering upgrade"コマンドで実施し た場合も、ログ上では "by the auto-update agent"と 表示される。
general	informational	general	URL filtering license does not exist or expired! Database is not updated updated.	URLフィルタリングライセンス が存在しないか、有効期限 切れのため、URLフィルタリ ングデータベースのアップ デートが行えませんでした。 PAN デバイスに有効なURLフ ィルタリングライセンスが インストールされているか 確認してください。 "Device > Licenses" に "URL Filtering" 項がある 場合：項内の"Date Expires"を確認し、現在の 日付より古くないか確認しま す。古くない場合、ライセン スのリニューアルが必要で す。販売代理店へお問い合わせ ください。 "Device > Licenses" に "URL Filtering" 項がない場 合：ライセンス購入後、初 期化を行ってURL-Filtering のライセンス項が消えた場 合、"License Management" にて "Retrieve license keys from license server" をクリックしてライセンス情 報をライセンス管理サーバか らインターネット経由で取 得します。 このとき、PAN デバイスの管 理ポートはインターネットに 接続できなければなりませ ん。 それ以外の場合はお買い求め の販売代理店に合わせてく ださい。
general	informational	general	User < <i>admin_user</i> > logged in via CLI from Console	管理ユーザがシリアルコンソ ール経由で CLI にログイン しました。 < <i>admin_user</i> >管理ユーザ名
general	informational	general	User < <i>admin_user</i> >	管理ユーザがSSH または

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

			logged in via CLI from < <i>ip_address</i> >	Telnet 経由で CLI にログインしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）の IP アドレス
general	informational	general	User < <i>admin_user</i> > logged in via Panorama from < <i>ip_address</i> > using https	管理ユーザがPanorama経由で PANOSのWebUIへログインしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス
general	informational	general	User < <i>admin_user</i> > logged in via Web from < <i>ip_address</i> > using ttp	管理ユーザがHTTP経由で PANOSのWebUIへログインしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス 注) デフォルトではHTTP経由になりません。“Device > Setup > MGT Interface Services” でHTTPを enableにする必要があります。
general	informational	general	User < <i>admin_user</i> > logged in via Web from < <i>ip_address</i> > using https	管理ユーザが HTTPS 経由で PANOSのWebUIへログインしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス
general	informational	general	User < <i>admin_user</i> > logged out via CLI from Console	管理ユーザがシリアルコンソール経由のCLIからログアウトしました。 < <i>admin_user</i> >管理ユーザ名
general	informational	general	User < <i>admin_user</i> > logged out via CLI from < <i>ip_address</i> >	管理ユーザがSSHまたは Telnet経由のCLIからログアウトしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス
general	informational	general	User < <i>admin_user</i> > logged out via Panorama from < <i>ip_address</i> > using https	管理ユーザがPanorama経由の WebUIからログアウトしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス

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

general	informational	general	User < <i>admin_user</i> > logged out via Web from < <i>ip_address</i> > using http	管理ユーザがPANOSの HTTP経由WebUIからログアウトしました。 < <i>admin_user</i> >管理ユーザ名 < <i>ip_address</i> >クライアント（管理ユーザの PC）のIPアドレス
general	informational	general	User < <i>admin_user</i> > visits Monitor tab	管理ユーザがWebUIの Monitor タブを参照しました。 < <i>admin_user</i> >管理ユーザ名
general	informational	general	User information refreshed	パロアルトデバイスのユーザ情報が更新されました。
general	critical	general	UserID failed to connect to agent < <i>user_agent_name</i> >(< <i>ip_address</i> >):< <i>reason</i> >	PANOSのUserIDプロセスがユーザ識別エージェントと接続できませんでした。 < <i>user_agent_name</i> >PANOSに設定されたユーザ識別エージェント (UIA) 名 < <i>ip_address</i> >UIAのIP アドレス< <i>reason</i> >接続できない理由
general	high	general	websrvr: exiting because service missed too many heartbeats	サービスが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、Webサーバプロセスを終了しました。（バグが考えられる）
general	informational	general	Disk pair < <i>process_name</i> >is degraded and missing a device.	ディスクペアが検出できません。< <i>process_name</i> > プロセス名
general	informational	general	New Disk Pair < <i>process_name</i> > detected.	新たなディスクペアを検出しました。< <i>process_name</i> > プロセス名
general	high	systemshutdown	The system is shutting down.	システムはシャットダウンします
general	high	System start	The system is starting up.	システムは開始します。
general	informational	general	Auto update agent found no new Antivirus updates	オートアップデートエージェントは、Anti-Virusシグネチャの新しいアップデートを見つけられませんでした。

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

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

表 18-3-4 HA

タイプ	重要度	イベント	内容	意味
ha	critical	config-failure	HA Group <ha_id>: running configuration not synchronized after <number> retries	running configuration が <number> 回リトライしましたが同期されませんでした。 <ha_id>デバイスに設定されたHA ID
ha	critical	config-not-sync	HA Group <ha_id>: commit on [local peer] device with running configuration not synchronized; versions not compatible	ピア/ローカルでコミットされた running configuration が同期されませんでした。バージョン互換性がありません。 <ha_id>デバイスに設定されたHA ID
ha	critical	config-not-sync	HA Group <ha_id>: commit on [local peer] device with running configuration not synchronized; synchronize manually	ピア/ローカルでコミットされた running configuration が同期されません。手動で同期してください。 <ha_id>デバイスに設定されたHA ID
ha	critical	config-not-sync	HA Group <ha_id>: commit on local device disconnected from peer, running configuration not synchronized	ローカルデバイスで commit しましたがピアと切断されているため running configuration は同期されませんでした。 <ha_id>デバイスに設定されたHA ID
ha	high	config-not-sync	HA Group <ha_id>: <content> on HA peer devices do not match; configuration synchronization between peers is not allowed	ピアデバイス上の<content>が致しません。ピア間の同期が許可されません。 <ha_id>デバイスに設定されたHA ID。 <content>コンテンツ種別 ("Application Content", "Threat Content", "URL Database", "Build Release", "Anti-Virus", "VPN Client Software")
ha	critical	connect-change	HA Group <ha_id>: All HA1 connections down	すべての HA1 コネクションがダウンしました。 <ha_id>デバイスに設定されたHA ID
ha	informational	connect-change	HA Group <ha_id>: Control link running on HA1 connection	HA1コネクション上で control link が動作しています。 <ha_id>デバイスに設定されたHA ID

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

ha	critical	connect-change	HA Group <ha_id>: Control link running on HA1-Backup connection	HA1 バックアップコネクション上でのコネクションリピングが動作しています。 <ha_id>デバイスに設定されたHA ID
ha	critical	connect-change	HA Group <ha_id>: HA heartbeat backup connection down	管理ポートを使ったハートビートリンクがダウンしました。 <ha_id>デバイスに設定されたHA ID
ha	high	connect-change	HA Group <ha_id>: HA heartbeat backup connection up	管理ポートを使ったハートビートリンクがアップしました。 <ha_id>デバイスに設定されたHA ID
ha	critical	connect-change	HA Group <ha_id>: HA heartbeat backup is being used to avoid split-brain; the HA functionality is in a degraded state pending the recovery of HA1	スプリットブレインを回避するためHAハートビートバックアップが利用されています。HA1 が回復するまでHA機能は制限状態です。 (コンフィグ同期ができないなど。) <ha_id>デバイスに設定されたHA ID
ha	critical	connect-change	HA Group <ha_id>: HA1 connection down	HA1 コネクションがダウンしました。 <ha_id>デバイスに設定されたHA ID
ha	informational	connect-change	HA Group <ha_id>: HA1 connection up	HA1 コネクションがアップしました。 <ha_id>デバイスに設定されたHA ID
ha	high	connect-change	HA Group <ha_id>: HA1-Backup connection down	HA1 バックアップコネクションがダウンしました。 <ha_id>デバイスに設定されたHA ID
ha	informational	connect-change	HA Group <ha_id>: HA1-Backup connection up	HA1 バックアップコネクションがアップされました。 <ha_id>デバイスに設定されたHA ID
ha	critical	dataplane down	HA Group <ha_id>: dataplane is down	データブレーンがダウンしました。本メモセクションはHA構成のタスクを行ふと表示されます。
ha	critical	hal-link-change	HA1 link down	HA1 リンクがダウンしました。

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

ha	informational	hal-link-change	HA1 link up	HA1リンクがアップしました。
ha	high	hal-link-change	HA1 peer link down	HA1ピアのリンクがダウンしました。
ha	informational	hal-link-change	HA1 peer link up	HA1ピアのリンクがアップしました。
ha	high	hal-link-change	HA1-Backup peer link down	HA1バックアップのピアリンクがダウンしました。
ha	informational	hal-link-change	HA1-Backup peer link up	HA1バックアップのピアリンクがアップしました。
ha	critical	ha2-link-change	All HA2 link paths down	すべてのHA2リンクパスがダウンしました。
ha	critical	ha2-link-change	HA2 link down	HA2リンクがダウンしました。
ha	informational	ha2-link-change	HA2 link up	HA2リンクがアップしました。
ha	critical	ha2-link-change	HA2 peer link down	HA2ピアリンクがダウンしました。
ha	informational	ha2-link-change	HA2 peer link up	HA2ピアリンクがアップしました。
ha	critical	ha2-link-change	HA2-Backup peer link down	HA2バックアップのピアリンクがダウンしました。
ha	informational	ha2-link-change	HA2-Backup peer link up	HA2バックアップのピアリンクがアップしました。
ha	critical	ha3-link-change	HA3 link down	HA3リンクがダウンしました。
ha	informational	ha3-link-change	HA3 link up	HA3リンクがアップしました。
ha	critical	ha3-link-change	HA3 peer link down	HA3ピアリンクがダウンしました。
ha	informational	ha3-link-change	HA3 peer link up	HA3ピアリンクがアップしました。
ha	critical	link-monitor-down	HA Group <ha_id>: link group <link_group> failure; all links are down	Link Monitoringで設定されたリンクがダウンしました

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

				に。 ⟨ha_id⟩リンクダウン が起きたHA グループの HA ID ⟨link_group⟩ デバイ スに設定されたリンク グループ名
ha	critical	link-monitor-down	HA Group ⟨ha_id⟩: link group or ⟨link_group⟩ failure; one or more links are down	Link Monitoring で 設定されたリンクグ ループが1つ以上の リンクがダウンしま した。 ⟨ha_id⟩リンクダウン が起きたHA グループの HA ID ⟨link_group⟩ デバイ スに設定されたリンク グループ名
ha	critical	link-monitor-down	HA Group ⟨ha_id⟩: link group , ⟨link_group⟩ link ⟨interface_name⟩ is down	Link Monitoring で 設定されたリンクグ ループが1つ以上の リンクがダウンしま した。 ⟨link_name⟩ がダウン しました。 ⟨ha_id⟩リンクダウン が起きたHA グループの HA ID ⟨link_group⟩ デバイ スに設定されたリンク グループ名 ⟨interface_name⟩ インターフェース名
ha	critical	non-functional-loop	HA Group ⟨ha_id⟩: going to suspended state due to detection of a non-functional loop after ⟨count⟩ loops allowed	non-functional のル ープが ⟨count⟩ 回発生したの でsuspended 状態に遷 移しました。 ⟨ha_id⟩デバイスに 設定されたHA ID ⟨count⟩ non- functional が発生した回数
ha	critical	path-monitor-down	HA Group ⟨ha_id⟩: path group IP ⟨path_group⟩ destination IP ⟨ip_address⟩ is down	Path Monitoring で 設定されたパスグル ープ内のが宛先IP ⟨ip_address⟩がダウ ンしました。 パス障害は200ms毎に echo request を宛先 IP へ送信し、応答が10 回連続で返ってこない 場合にダウンとみなさ れます。 ⟨ha_id⟩ デバイスに設 定されたHA ID ⟨path_group⟩パスグル ープ名 ⟨ip_address⟩ダウンが 検知された宛先IPアド レス

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

ha	critical	path-monitor-down	HA Group <ha_id>: path group <path_group> failure; all destination IPs are down	Path Monitoringで設定されたパスグループの宛先IPがダウンしました。 <ha_id>デバイスに設定されたHA ID <path_group>パスグループ名
ha	critical	path-monitor-down	HA Group <ha_id>: path group <path_group> failure; one or more destination IPs are down	Path Monitoringで設定されたパスグループの1つ以上の宛先IPがダウンしました。 <ha_id>デバイスに設定されたHA ID。1～254の値が入る。 <path_group>パスグループ名。
ha	critical	peer-error	HA Group <ha_id>: received peer error: <reason>	ピア（もう1台のHA構成）を受信しました。 <ha_id>デバイスに設定されたHA ID。 <reason> 受信したエラーの詳細
ha	critical	peer-split-brain	HA Group <ha_id>: split-brain detection on peer	ピアにおいてスプリットブレインを検知しました。デバイスの状態が異なっている場合、相手の状態が表示されます。 <ha_id> デバイスに設定されたHA ID
ha	critical	peer-split-brain	HA Group <ha_id>: Staying in Active state after splitbrain recovery: <time>s	スプリットブレインから回復し、Active状態を保持しています。 <ha_id> デバイスに設定されたHA ID <time>スプリットブレイン期間、秒単位
ha	critical	peer-sync-failure	HA Group <ha_id>: can't synchronize control plane data; some state may be lost on switchover	コントロールプレーンのデータ同期が失敗しました。切り替わった際のデータが失われる可能性があります。 <ha_id> デバイスに設定されたHA ID
ha	high	peer-version-match	HA Group <ha_id>: Build Release version does not match	HAグループ内のピア間で現在動作しているPANOSバージョンが一致しません。
ha	high	peer-version-match	HA Group <ha_id>: Threat Content version does not match	HAグループ内のピア間で現在いる脅威防御シングルバージョンが一致しません。

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

ha	high	peer-version-match	HA Group < ha_id >: Application Content version does not match	HAグループ内のピアで現在インストールされているバージョンが一致しません。
ha	high	peer-version-match	HA Group < ha_id >: Anti-Virus version does not match	HAグループ内のピアで現在インストールされているアンチウイルスバージョンが一致しません。
ha	informational	peer-version-match	HA Group < ha_id >: Build Release version now matches	HAグループ内のピアでインストールしているPANOSのバージョンが一致しました。
ha	informational	peer-version-match	HA Group < ha_id >: Threat Content version now matches	HAグループ内のピアでインストールしている脅威防御システムが一致しました。
ha	informational	peer-version-match	HA Group < ha_id >: application Content version now matches	HAグループ内のピアでインストールされているアプリケーションバージョンが一致しました。
ha	informational	peer-version-match	HA Group < ha_id >: Anti-Virus version now matches	HAグループ内のピアでインストールされているアンチウイルスバージョンが一致しました。
ha	critical	pre-1.3	HA Group < ha_id >: peer device is running pre-1.3 code; incompatible version causes local device to stay in< state > state	ピアがPANOS バージョン 1.3 以前で動作しています。バージョンが一致しないためローカルデバイスは< state > 状態のままになっています。 < ha_id >デバイスに設定されたHA ID
ha	critical	pre-2.0	HA Group < ha_id >: peer device is running pre-2.0 code; going into partial compatibility mode	ピアがPANOS バージョン 2.0 以前で動作する場合、モードで動作します。 < ha_id >デバイスに設定されたHA ID
ha	critical	policy-push-fail	HA Group < ha_id >: policy push to dataplane failed	データプレーンへのポリシー書き込みが失敗しました。 < ha_id >デバイスに設定されたHA ID
ha	critical	preempt	HA Group < ha_id >: going to passive state due to preemption	プリエンプトのため、アクティブ状態に移行します。本マッチセレクションはPreemptiveの設定が有効なHAグループ内のデバイス優先度の低い（(大きい) Device Priority 値）がアクティベートされます。常にアクティベートされます。

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

				が障害状態から復旧したため、自デバイスはアクティブ状態へ遷移します。 〈ha_id〉デバイスに設定されたHA ID
ha	critical	preempt-loop	HA Group 〈ha_id〉: going to suspended state due to detection of a preemption loop after 〈count〉 loops	プリエンプトのループが〈count〉発生したのを、suspended状態に遷移しました。 〈ha_id〉デバイスに設定されたHA ID 〈count〉プリエンプトの回数が発生しました。
ha	critical	split-brain	HA Group 〈ha_id〉: going to Passive state due splitbrain detection	スプリットブレインを検知したためpassive状態に遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	informational	state-change	HA Group 〈ha_id〉: moved from state Active to state Passive	ActiveからPassiveへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	critical	state-change	HA Group 〈ha_id〉: moved from state Active to state Non-functional	ActiveからNon-functionalへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	informational	state-change	HA Group 〈ha_id〉: moved from state Active to state Suspended	ActiveからSuspendedへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	informational	state-change	HA Group 〈ha_id〉: moved from state Passive to state Active	PassiveからActiveへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	high	state-change	HA Group 〈ha_id〉: moved from state Passive to state Non-functional	PassiveからNon-functionalへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	info	state-change	HA Group 〈ha_id〉: moved from state Passive to state Suspended	PassiveからSuspendedへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	informational	state-change	HA Group 〈ha_id〉: moved from state Non-functional to state Active	Non-functionalからActiveへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	informational	state-change	HA Group 〈ha_id〉: moved from state Non-functional to state Passive	Non-functionalからPassiveへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID
ha	critical	state-change	HA Group 〈ha_id〉: moved from state Non-functional to state Suspended	Non-functionalからSuspendedへ状態が遷移しました。 〈ha_id〉デバイスに設定されたHA ID

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

ha	informational	state-change	HA Group < <i>ha_id</i> >: moved from state Initial to state Active	InitialからActiveへ状態が遷移しました。 < <i>ha_id</i> >デバイスに設定されたHA ID
ha	informational	state-change	HA Group < <i>ha_id</i> >: moved from state Initial to state Passive	InitialからPassiveへ状態が遷移しました。 < <i>ha_id</i> >デバイスに設定されたHA ID
ha	critical	state-change	HA Group < <i>ha_id</i> >: HA heartbeat backup information has been used for HA state-change	HA状態遷移に HAハートビート情報が利用されました。 < <i>ha_id</i> >デバイスに設定されたHA ID
ha	critical	peer-version-degraded	HA Group < <i>ha_id</i> >: Peer device running degraded HA version < <i>version</i> >; incompatible version causes local device to stay in Non-functional state unless peer is put into Suspended state	ピアデバイスのバージョンが低いバージョンの互換性がない状態である。 < <i>ha_id</i> >デバイスに設定されたHA ID < <i>version</i> >デバイスのバージョン

表 18-3-5 url-filtering

タイプ	重要度	イベント	内容	意味
url-filtering	informational	cloud-election	CLOUD ELECTION: < <i>domain_name of cloud</i> >IP: < <i>ip_address</i> >was elected, measured alive test.	選ばれたクラウドの通知 < <i>domain_name of cloud</i> > クラウドのドメイン名 < <i>ip_address</i> >クラウドのIPアドレス
url-	informational	upgrade-	URL filtering database	URLフィルタリングデータベースがオートアップデートエ

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

filtering	onal	url-database-success	was upgraded from version old_< <i>old_version</i> > to < <i>new_version</i> > by the auto-pdate agent	一下载ました。ノーツノクレ < <i>old_version</i> > アップグレード前のバージョン < <i>new_version</i> > アップグレード後のバージョン
url-filtering	informational	url-database-is-latest	URL filtering database version < <i>version</i> > is already the latest version	現在のURLフィルタリングデータベースのバージョンは最新です。 < <i>version</i> > 現在のデータベースバージョン
url-filtering	informational	url-engine-stopped	URL filtering engine Stopped.	URLフィルタリングエンジンが終了しました。
url-filtering	informational	download-url-database-success	PAN-DB was downloaded successfully	PAN-DBのダウンロードに成功しました。
url-filtering	informational	download-url-database-success	PAN-DB download: Finished successfully.	PAN-DBのダウンロードが終了し、成功しました。
url-filtering	informational	failed-to-lock-update	Failed to lock URL database update process! Maybe another instance is running.	他のインスタンスが動作しているため URL-DB の更新プロセスが失敗しました。
url-filtering	informational	rfs-process-starts	PAN-DB refresh agent is starting....	PAN-DBのリフレッシュエージェントが起動しました。
url-filtering	informational	rfs-process-stopped	PAN-DB refresh agent is going down.	PAN-DBのリフレッシュエージェントが停止しました。
url-filtering	informational	starts-from-backup-seed	Starting with backup seed.	バックアップシードから開始しました。
url-filtering	informational	starts-from-download-seed	Failed to start with the backup seed (seed may be corrupted).	バックアップシードからの開始に失敗しました（可能ですが、シードが壊れている可能性があります）。

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

url-filtering	informational	starts-from-download-seed	Starting with download seed.	シードファイルのダウンロードを開始しました。
url-filtering	medium	starts-from-empty-see	Failed to load the URL seed database, starting with an empty database.	URLシードデータベースの読み込みが失敗しました。 シードなしで開始します。
url-filtering	informational	starts-from-empty-see	Starting with an empty SEED.	シードファイルなしで開始します。
url-filtering	critical	seed-out-of-sync	URL sw < version > is not compatible with the cloud sw < version > Upgrade sw is required!!!	URL SWのバージョンが、クラウドとの互換性がありません。URL SWのアップグレードが必要です。 < version >SWのバージョン
url-filtering	informational	upgrade-url-database-success	PAN-DB was upgraded to version < version >.	PAN-DBがアップグレードされました。 < version >アップグレード後のバージョン
url-filtering	informational	url-backup-seed-success	Backup of PAN-DB finished successfully.	PAN-DBのシードのバックアップが成功しました。
url-filtering	informational	url-cloud-connection-failure	Failed to open connection with the cloud after < number of trial > consecutive tries.	クラウドへの接続が失敗しました。< number of trial >試行回数
url-filtering	medium	url-download-failure	PAN-DB cloud list loading failed (ERROR:< reason of the failure >).	PAN-DBのクラウドのリストの読み込みが失敗しました。 < reason of the failure >
url-filtering	medium	url-backup-seed-success	Cloud is not ready, There was no update from the cloud in the last < duration > seconds	直近の何秒間、クラウドからアップデートがありません。 < duration >期間 [秒]

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

18.3.8. アプリケーションフィールドの意味

表 18-3-6 アプリケーションフィールドの意味

アプリケーション	意味
Incomplete	3 ウェイ TCP ハンドシェイクが完了しなかった、もしくは 3 ウェイ TCP ハンドシェイクは完了したがその後アプリケーションを特定するデータの送受信が無かったことを意味します。つまり、確認されたトラフィックが実際にアプリケーションではなかったことを意味します。例) クライアントがサーバに SYN を送信し、Palo Alto Networks デバイスがその SYN に対してセッションを生成したが、サーバが一度もクライアントに SYN ACK を返信しない場合、そのセッションは incomplete です。
Insufficient data	アプリケーションを特定するための十分なデータが無いことを意味します。例) 3 ウェイ TCP ハンドシェイクが完了した後、1 個のデータパケットの送受信があったが、その 1 個のデータパケットのみでは判定に不十分で、Palo Alto Networks のシグニチャのいずれにもマッチしなかった場合、Traffic ログの Application フィールドに Insufficient data の確認が可能です。
Unknown-tcp	ファイアウォールが 3 ウェイ TCP ハンドシェイクを確認したがアプリケーションを特定できなかったことを意味します。これは ファイアウォールが該当するシグニチャを持たないカスタム アプリケーションを使用していることによると考えられます。
Unknown-udp	Unknown-udp は未知の UDP トラフィックにより生成されます。
Unknown-p2p	Unknown-p2p は一般的な P2P ヒューリスティックに該当します。
Not-applicable	トラフィックが着信したポート／サービスが許可されていないために破棄されるデータを、Palo Alto デバイスが受信したこと、もしくは、そのポートまたはサービスを許可するルールやポリシーがないことを意味します。例) Palo Alto デバイスにルールが 1 つだけ設定されていて、そのルールが ポート／サービス 80 番のみ使用する Web-browsing のアプリケーションのみを許可しており、かつ、トラフィック (Web-browsing またはそれ以外のいかなるアプリケーション) が 80 番以外のポート／サービスを使用して Palo Alto デバイスに送信された場合、そのトラフィックは破棄またはドロップされ、Application フィールドに "not-applicable" が記録されたセッションが確認可能です。

18.3.9. セッション終了理由

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

表 18-3-7 セッション終了理由

セッション終了理由	意味
Aged out	3 セッションがタイムアウトにより終了しました。
TCP FIN	接続の一方または両方のホストが TCP FIN パケットを送信してセッションをクローズしました。
TCP RST	client - クライアントがサーバへ TCP リセットを送信しました。 server - サーバがクライアントへ TCP リセットを送信しました。
Appid policy lookup deny	セッションが、拒否またはドロップ アクションが指定されたセキュリティ ポリシーと一致しました。
mitigation tdb	脅威を検知したためセッションは終了しました。
resource limit	セッションがリソース制限の問題によりドロップされました。 例) セッションの順序外パケット数が、フローまたはグローバル順序外パケット キューごとに許容された数を超えた場合などが考えられます。他の多数の理由によっても表示される場合があります。
host service	トラフィックがファイアウォールへ送信されましたが、サービスが許可されていないあるいは有効になっていません。

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

18.4. ログアーカイブ出力

Panorama にて、フィルタ条件を指定してログをエクスポートする手順を記載します。

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

生成日時	タイプ	送信元ソース	宛先ソース	送信元	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先	宛先ダイナミックアドレスグループ	宛先ポート	アプリケーション	アクション	ルール	
06/12 17:35:30	end	Internal_SV_VP	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV_VP
06/12 17:35:30	end	Internet_WEST	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.19.122.2			10.19.124.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.9.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:25	end	Internal_SV_VP	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV_VP
06/12 17:35:25	end	Internet_WEST	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
06/12 17:35:25	end	Internet_WEST	Internet_WEST	10.9.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
06/12 17:35:21	end	Internal_SV_VP	Internet_WEST	10.19.122.2			10.19.204.15			514	syslog	allow	any_Internal
06/12 17:35:21	end	Internet_WEST	Internet_WEST	10.19.122.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maint...	10.9.64.2			10.9.66.101			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maint...	10.9.64.2			10.9.66.101			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internet_WEST	Internet_WEST	10.9.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maint...	10.19.122.2			10.9.66.301			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maint...	10.19.122.2			10.9.66.301			162	snmp-trap	allow	SenjaSystem
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.19.122.2			10.19.124.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.19.122.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.9.64.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internal_WEST	Internal_SV_VP	10.9.64.2			10.19.204.15			514	syslog	allow	any_Internal
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.9.64.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.9.64.2			10.19.124.101			162	snmp-trap	allow	intrazone-dt

図 18-4-1 M-300 Traffic Log

- 「+」ボタンをクリック（「+」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 18-4-2 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。

（フィルタ条件（属性）については「表 17-4-1」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



図 18-4-3 M-300 Traffic Log

表 18-4-1 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)	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 18-4-6 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

- ⑤ フィルタされたログリストの表示後、「CSV にエクスポート」ボタンをクリックします。（「CSV にエクスポート」ボタンにカーソルを合わせると、「CSV にエクスポート」と表示されます）

The screenshot shows the 'PANORAMA' interface with the 'MONITOR' tab selected. In the search bar, there is a filter '(flags has proxy)' highlighted with a red box. At the top right, there is a 'CSV' export icon also highlighted with a red box.

図 18-4-7 M-300 Traffic Log

- ⑥ Export 用のログ生成後、「ファイルのダウンロード」をクリックし、ログをダウンロードします。



図 18-4-8 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

18.5. ログ閲覧画面カラム変更

Panorama にて、ログ閲覧画面のカラムを変更する手順を記載します。

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

生成日時	タイプ	送信元ソース	宛先ソース	送信元	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先	宛先ダイナミックアドレスグループ	動的ユーザーグループ	宛先ポート	アフリケーション	アクション	ルール
06/12 17:05:30	end	Internal_SV_VP	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV
06/12 17:35:30	end	Internet_WEST	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.19.132.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.96.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:25	end	Internal_SV_VP	Internal_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV
06/12 17:35:25	end	Internet_WEST	Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
06/12 17:35:25	end	Internet_WEST	Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
06/12 17:35:21	end	Internal_SV_VP	Internal_WEST	10.19.132.2			10.19.204.15			514	syslog	allow	any_Internal
06/12 17:35:21	end	Internet_WEST	Internet_WEST	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:20	end	Internal_SV_Mainte...	Internet_WEST	10.96.64.2			10.96.66.101			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internet_WEST	Internal_SV_Mainte...	10.96.64.2			10.96.66.101			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internet_WEST	Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
06/12 17:35:20	end	Internal_WEST	Internal_WEST	10.19.132.2			10.96.66.101			162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internal_WEST	Internal_WEST	10.19.132.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.96.64.2			10.19.204.15			514	syslog	allow	any_Internal
06/12 17:35:18	end	Internal_SV_VP	Internet_WEST	10.96.64.2			10.19.204.15			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.96.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internal_WEST	Internal_WEST	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internal_WEST	Internal_WEST	10.19.132.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internal_WEST	Internal_WEST	10.96.64.2			10.19.204.15			514	syslog	allow	any_Internal
06/12 17:35:18	end	Internal_SV_VP	Internet_WEST	10.96.64.2			10.19.204.15			162	snmp-trap	allow	intrazone-dt
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.96.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt

図 18-5-1 M-300 Traffic Log

- カラム上の「▽」ボタンをクリック後、「カラム」と辿り、ログ閲覧画面に表示させるカラムをチェックボックスで選択/非選択します。

宛先ソース	送信元	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先	宛先ダイナミックアドレスグループ	動的ユーザーグループ	宛先ポート	アフリケーション	アクション	ルール
Internal_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV
Internet_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
Internet_WEST	10.19.132.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
Internet_WEST	10.96.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
Internal_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	Internal_SV
Internal_WEST	10.19.204.15			172.17.68.113			514	Incomplete	allow	intrazone-dt
Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
Internal_SV_VP	10.19.132.2			10.19.204.15			514	syslog	allow	any_Internal
Internal_WEST	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
Internal_SV_Mainte...	10.96.64.2			10.96.66.101			162	snmp-trap	allow	SenjaSystem
Internal_SV_Mainte...	10.96.64.2			10.96.66.101			162	snmp-trap	allow	SenjaSystem
Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
Internal_SV_Mainte...	10.96.66.101			10.96.66.101			162	snmp-trap	allow	SenjaSystem
Internal_SV_VP	10.19.132.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
Internet_WEST	10.19.132.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt
Internet_WEST	10.96.64.2			10.112.23.61			162	snmp-trap	allow	intrazone-dt
Internal_SV_VP	10.96.64.2			10.19.204.15			514	syslog	allow	any_Internal
Internet_WEST	10.96.64.2			10.19.33.212			162	snmp-trap	allow	intrazone-dt
Internal_SV_VP	10.96.64.2			10.19.134.101			162	snmp-trap	allow	intrazone-dt

(本項目は動作しているコンフィグと紐付かないため、コミットを実行する必要はない、画面表示が即時反映されます)

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 18-5-2 M-300 Traffic Log

③ カラムの位置を移動する場合は、該当のカラムをドラッグ＆ドロップにて移動可能です。

図 18-5-3 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

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

SSL 復号化している通信のトラフィックログを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。

生成日時	タイプ	送信元ゾーン	宛先ゾーン	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先ダイナミックアドレスグループ	動的ユーザーグループ	宛先ポート	アプリケーション	アクション	ルール
06/12 17:35:30	end	Internal_SV_VP	Internet_WEST	10.19.204.15		172.17.68.113		514	Incomplete	allow	Internal_SV
06/12 17:35:30	end	Internet_WEST	Internet_WEST	10.19.204.15		172.17.68.113		514	Incomplete	allow	Intrazone-di
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.19.132.2		10.19.134.101		162	snmp-trap	allow	Intrazone-di
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.96.64.2		10.19.134.101		162	snmp-trap	allow	Intrazone-di
06/12 17:35:26	end	Internal_SV_VP	Internal_WEST	10.19.204.15		172.17.68.113		514	Incomplete	allow	Internal_SV
06/12 17:35:26	end	Internet_WEST	Internet_WEST	10.19.204.15		172.17.68.113		514	Incomplete	allow	Intrazone-di
06/12 17:35:25	end	Internet_WEST	Internet_WEST	10.96.64.2		10.11.23.61		162	snmp-trap	allow	Intrazone-di
06/12 17:35:25	end	Internal_WEST	Internal_WEST	10.19.132.2		10.19.204.15		514	syslog	allow	any_Internal
06/12 17:35:25	end	Internal_WEST	Internet_WEST	10.19.132.2		10.19.33.212		162	snmp-trap	allow	Intrazone-di
06/12 17:35:25	end	Internal_SV_Maintain...	Internal_WEST	10.96.64.2		10.96.66.101		162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maintain...	10.96.64.2		10.96.66.101		162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internet_WEST	Internet_WEST	10.96.64.2		10.11.23.61		162	snmp-trap	allow	Intrazone-di
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maintain...	10.19.132.2		10.96.66.101		162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internal_WEST	Internal_SV_Maintain...	10.19.132.2		10.96.66.101		162	snmp-trap	allow	SenjaSystem
06/12 17:35:20	end	Internet_WEST	Internet_WEST	10.19.132.2		10.11.23.61		162	snmp-trap	allow	Intrazone-di
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.19.33.212		10.19.33.212		162	snmp-trap	allow	Intrazone-di
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.96.64.2		10.19.204.15		514	syslog	allow	any_Internal
06/12 17:35:18	end	Internal_WEST	Internet_WEST	10.96.64.2		10.19.33.212		162	snmp-trap	allow	Intrazone-di
06/12 17:35:18	end	Internet_WEST	Internet_WEST	10.96.64.2		10.19.33.212		162	snmp-trap	allow	Intrazone-di
06/12 17:35:18	end	Internal_WEST	Internal_WEST	10.96.64.2		10.19.134.101		162	snmp-trap	allow	Intrazone-di

図 18-6-1 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 18-6-2 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。

表 18-6-1 SSL 復号化通信フィルタ設定

図中番号	タブ	利用用途
(1)	結合子	「and」を選択
(2)	属性	「フラグ」を選択
(3)	演算子	「所有」を選択
(4)	値	「SSL プロキシ」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

ログ フィルタの追加

ファイルター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 or <input type="checkbox"/> Negate	(1) AND SST バイト パケット フラグ ポッドのネームスペース	(2) 所有 （3）	(4) PCAP NAT SSL プロキシ キャプティブ ポータル プロキシ トランザクション

追加 適用 閉じる

図 18-6-3 M-300 Traffic Log

- 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）

PANORAMA DASHBOARD ACC MONITOR PANORAMA Commit デバイスグループ：すべて

過去 24 時間

生成日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	送信元ダイナミック アドレス グループ	宛先	宛先ダイナミック アドレス グループ	動的ユーザーグループ	宛先ポート	アプリケーション	アクション

図 18-6-4 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

- ⑤ 「詳細ログビュー」をクリックし、フラグの復号化にチェックが入っていることを確認します。

The screenshot shows the 'Detailed Log View' window with the following details:

- Log Information:**
 - フレーバー/レコードID: 455d-9040-ffe41446c7bc
 - セッション終了理由: threat
 - カテゴリ: DefaultGroup_Block
 - デバイスのシリアル番号: 019901002766
 - IP プロトコル: tcp
 - ログアクション: Profile_Log_Forward...
 - 生成日時: 2023/06/07 14:00:07
 - 開始時間: 2023/06/07 14:00:02
 - 受信日時: 2023/06/07 14:00:07
- Log Details:**
 - タイプ: end
 - バイト: 673
 - 受信済みバイト: 0
 - 送信済みバイト: 673
 - 繰り返し回数: 1
 - パケット: 1
 - 受信したパケット: 0
- Flags:** The '復号化' (Decryption) checkbox is checked and highlighted with a red box.
- PCAP Table:**

PCAP	受信日時	タイプ	アプリケーション	アクション	ルール	UUID	バイト	重大度	カテゴリ	URL カテゴリリスト	判定	URL	ファイル名
	2023/06/07 14:00:07	end	web-browsing	allow	URLFil...	101d5...	673		Default...				
	2023/06/07 14:00:16	url	web-browsing	block-url	URLFil...	101d5...		informa...	Default...	Default... and-arts.lowl...		static-...	

図 18-6-5 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

18.7. サーバ証明書の問題によりブ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

サーバ証明書の問題によりブロックされているトラフィックログを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。

生成日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先	宛先ダイナミックアドレスグループ	動的ユーザーグループ	宛先ポート	アプリケーション	アクション	ルール	
06/12 17:41:30	end	Internal_SV_VP	internal_WEST	10.19.204.15		172.17.68.113				514	Incomplete	allow	Internal_SV	
06/12 17:41:30	end	Internet_WEST	Internet_WEST	10.19.204.15		172.17.68.113				514	Incomplete	allow	intrazone-di	
06/12 17:41:25	end	Internet_WEST	Internet_WEST	10.19.204.15		172.17.68.113				514	Incomplete	allow	intrazone-di	
06/12 17:41:25	end	Internal_SV_VP	internal_WEST	10.19.204.15		172.17.68.113				514	Incomplete	allow	Internal_SV	
06/12 17:41:25	end	Internet_WEST	Internet_WEST	10.19.132.2						162	snmp-trap	allow	intrazone-di	
06/12 17:41:16	end	Internet_WEST	Internet_WEST	10.19.132.2		10.11.23.61				162	snmp-trap	allow	intrazone-di	
06/12 17:41:16	end	Internet_WEST	Internet_WEST	10.19.64.2		10.19.134.101				162	snmp-trap	allow	intrazone-di	
06/12 17:41:10	end	Internet_WEST	Internet_WEST	10.19.64.2		10.11.23.61				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.64.2		10.19.33.212				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.64.2		10.19.33.212				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	internal_WEST	internal_WEST	10.19.64.2		10.19.134.101				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	internal_SV_VP	internal_WEST	10.19.64.2		10.19.204.15				514	syslog	allow	any_Internal	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.132.2		10.11.23.61				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.132.2		10.19.33.212				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.132.2		10.19.134.101				162	snmp-trap	allow	intrazone-di	
06/12 17:41:06	end	internal_SV_VP	internal_WEST	10.19.132.2		10.19.204.15				514	syslog	allow	any_Internal	
06/12 17:41:06	end	Internet_WEST	Internet_WEST	10.19.64.2		10.19.66.101				162	snmp-trap	allow	SeniSystem	
06/12 17:41:05	end	internal_SV_Maintain...	internal_WEST	10.19.64.2		10.19.66.101				162	snmp-trap	allow	SeniSystem	
06/12 17:41:05	end	Internet_WEST	Internet_WEST	10.19.64.2		10.11.23.61				162	snmp-trap	allow	intrazone-di	

図 18-7-1 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）

生成日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	送信元ダイナミックアドレスグループ	宛先	宛先ダイナミックアドレスグループ	動的ユーザーグループ	宛先ポート	アプリケーション	アクション	ルール

図 18-7-2 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

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。

表 18-7-1 SSL 復号化通信フィルタ設定

図中番号	タブ	利用用途
(1)	結合子	「and」を選択
(2)	属性	「セッション終了理由」を選択
(3)	演算子	「演算子」を選択
(4)	値	「Decrypt-cert-validation」を選択



図 18-7-3 M-300 Traffic Log

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 18-7-4 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

- ⑤ 「詳細ログビュー」をクリックし、セッション終了理由が decrypt-cert-validation、フラグの復号化にチェックが入っていることを確認します。

PCAP	収録日時	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	重複度	カテゴリ	URL カテゴリリスト	判定	URL	ファイル名
	2023/06/07 11:09:19	deny	ssl	allow	NEXCO-SHIKOKU	Bc1813a9f..._	3004		entertainme... and arts				
	2023/06/07 11:09:30	url	http-proxy	alert	NEXCO-SHIKOKU	Bc1813a9f..._		Informational	entertainme... and arts		dloney.co.jp...		

図 18-7-5 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

19. セキュリティゾーン追加

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

19. 1. セキュリティゾーン追加

新たなセキュリティゾーンを追加した場合、ネットワーク詳細設計書（別紙：セキュリティ設計）の内容から乖離するおそれがあります。追加を行う場合はネットワーク設計業者へご連絡をお願いします。

現在設定されている各ゾーンの設計内容（役割、定義など）については、ネットワーク詳細設計書（別紙：セキュリティ設計）の「4-2. ゾーン設計」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

20. 管理者アカウント作成

この項では管理者アカウントの新規追加、変更、削除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

20. 1. 管理者アカウント追加

管理者アカウントを追加する手順を記載します。

20. 1. 1. 管理者アカウント追加

- ① 「Device」タブ > 「管理者」を選択し、「追加」ボタンをクリックします。

図 20-1-1 PA-5450 Administrator Add

表 20-1-1 管理者アカウント設定

図中番号	名前	利用用途
(1)	名前	「管理者名」を入力 文字数制限は最小 1 文字～最大 31 文字まで。 大文字と小文字を区別します。 また、英数字、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。ハイフンから始まるユーザ名は設定できません。
(2)	パスワード	パスワードを入力 文字数制限は最小 1 文字～最大 31 文字まで。 大文字と小文字を区別します。英数字、記号（2byte 文字以外）が使用可能です。
(3)	再入力パスワード	確認のため再度同じパスワードを入力
(4)	管理者タイプ	「ダイナミック」を選択し、プルダウンより以下の権限より選択します。 - スーパーユーザー 全ての設定の読み書きが可能です。 - スーパーユーザー (read-only) 全ての設定の閲覧のみが可能です。 - デバイスの管理者 アカウント設定及び追加/削除/変更を除く 全ての設定の読み書きが可能です。 - デバイスの管理者 (読み取り専用) アカウント設定及び追加/削除/変更を除く 全ての設定の閲覧のみが可能です。

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

	また、管理系の設定（ホスト名、MGMT インターフェース、アカウント）など機器全体に関わるような設定は編集できません。
--	---

管理者タイプ補足

「ロールベース」を選択した場合、管理者アカウントへ任意のロールを設定することができます。

例) read-only ユーザであり、かつトラフィックログ(Monitor)のみ閲覧を許可する、といったアカウントを作成する場合に使用します。

- ② 上記(1)～(4)を設定（「表 20-1-1」を参照）し、「OK」ボタンをクリックします。

管理者

(1) 名前

認証プロファイル

クライアント証明書認証のみを使用 (Web)

(2) パスワード

(3) 再入力 パスワード

パスワード要件
• 最小パスワード長(カウント) 8

公開鍵認証 (SSH) の使用

管理者タイプ ダイナミック ロールベース

(4)

パスワードプロファイル

OK キャンセル

図 20-1-2 PA-5450 Administrator 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

20.1.2. 設定反映

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

（設定が反映されるまで5分程度かかることがあります。）

The screenshot shows the 'DEVICE' tab selected in the top navigation bar. On the left, there's a sidebar with various management options like 'Password Profile', 'Certificates', 'OCSP', 'SCEP', 'Logs', and 'Services'. The main area displays a table of administrators with columns for Name, Role, Certificate Profile, Password Profile, Client Authentication, Public Key Authentication, Profile, and Locked User. A new row 'test_admin' is being added, indicated by a checkmark in the 'Name' column. At the top right, there's a 'Commit' button with a red box drawn around it. The bottom status bar shows the user is 'admin'.

図20-1-3 PA-5450 Administrator Add

The screenshot shows the 'Commit' dialog box. It has two radio button options: 'Commitすべての変更' (selected) and 'Commit変更の実行者:(1) admin'. Below this is a table with two rows: 'policy-and-objects' (Policy and Objects) and 'device-and-network' (Device and Network Configuration). At the bottom, there are three buttons: '変更内容の確認', '変更サマリー', and 'コミットの検証'. A note below 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。'. There's also a '内容' input field and a large red box around the 'Commit' button at the bottom right.

図20-1-4 PA-5450 Administrator 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

20.2. 管理者アカウント変更

管理者アカウントの設定を変更する手順を記載します。

20.2.1. 管理者アカウント変更

- 「Device」タブ > 「管理者」を選択し、対象のアカウントをクリックします。

名前	ロール	認証プロファイル	パスワードプロファイル	クライアント証明書の認証(WEB)	公開キーの認証(SSH)	プロファイル	ロックされたユーザー
admin	スーパーユーザー			<input type="checkbox"/>	<input type="checkbox"/>		
test	スーパーユーザー			<input type="checkbox"/>	<input type="checkbox"/>		
test_admin	スーパーユーザー(読み取り専用)			<input type="checkbox"/>	<input type="checkbox"/>		

図 20-2-1 PA-5450 Administrator Modify

表 20-2-1 管理者アカウント設定

図中番号	名前	利用用途
(1)	パスワード	パスワードを入力 文字数制限は最小1文字～最大31文字まで。 大文字と小文字を区別します。 英数字、記号(2byte文字以外)が使用可能です。
(2)	再入力パスワード	確認のため再度同じパスワードを入力

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

(3) 管理者タイプ	<p>「ダイナミック」を選択し、プルダウンより以下の権限より選択します。</p> <ul style="list-style-type: none"> - スーパーユーザー 全ての設定の読み書きが可能です。 - スーパーユーザー (read-only) 全ての設定の閲覧のみが可能です。 - デバイスの管理者 アカウント設定及び vsys の追加/削除/変更を除く 全ての設定の読み書きが可能です。 - デバイスの管理者 (読み取り専用) アカウント設定及び vsys の追加/削除/変更を除く 全ての設定の閲覧のみが可能です。 - 仮想システム管理者 特定の vsys のみ設定の読み書きが可能です。 (※1) - 仮想システム管理者 (読み取り専用) 特定の vsys のみ設定の閲覧のみが可能です。 (※1) <p>(※1) : 例) vsys "A" のみを定義した場合 vsys "A" に紐付くポリシーやオブジェクトの設定（もしくは閲覧）が 可能ですが、vsys "B" に紐付く設定は閲覧すらできません。 また、管理系の設定（ホスト名、MGMT インターフェース、アカウント） など機器全体に関わるような設定は編集できません。</p>
------------	--

② 以下(1)～(3)（「表 20-2-1」を参照）の設定を変更し、「OK」ボタンをクリックします。

※管理者の名前を変更することはできません。

管理者

名前: test_admin

認証プロファイル: None

パスワード: (1)

再入力パスワード: (2)

パスワード要件:

- 最小パスワード長(カウント) 8

□ 公開鍵認証 (SSH) の使用

管理者タイプ: ダイナミック ロールベース (3) スーパーユーザー (read-only)

パスワードプロファイル: None

OK キャンセル

図 20-2-2 PA-5450 Administrator 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

20.2.2. 設定反映

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

(設定が反映されるまで5分程度かかることがあります)

名前	ロール	認証プロファイル	パスワードプロファイル	クライアント証明書の認証(WEB)	公開キーの認証(SSH)	プロファイル	ロックされたユーザー
admin	スーパーユーザー			<input type="checkbox"/>	<input type="checkbox"/>		
test	スーパーユーザー			<input type="checkbox"/>	<input type="checkbox"/>		
test_admin	スーパーユーザー(読み取り専用)			<input type="checkbox"/>	<input type="checkbox"/>		

図 20-2-3 PA-5450 Administrator 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			
▶ device-and-network	Device and Network Configuration			

図 20-2-4 PA-5450 Administrator 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

20.3. 管理者アカウント削除

管理者アカウントを削除する手順を記載します。

20.3.1. 管理者アカウント削除

- ③ 「Device」タブ > 「管理者」を選択し、対象のアカウントにチェックを入れ、「削除」ボタンをクリックします。

名前	ロール	認証プロファイル	パスワード プロファイル	クライアント証明書の認証 (WEB)	公開キーの認証 (SSH)
admin	スーパーユーザ			<input type="checkbox"/>	<input type="checkbox"/>
test	スーパーユーザ			<input type="checkbox"/>	<input type="checkbox"/>
test_admin	スーパーユーザ [読み取り専用]			<input checked="" type="checkbox"/>	<input type="checkbox"/>

図 20-3-1 PA-5450 Administrator Delete

- ④ 以下の確認画面で「はい」ボタンをクリックします。



図 20-3-2 PA-5450 Administrator 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

20.3.2. 設定反映

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

(設定が反映されるまで5分程度かかることがあります)

名前	ロール	認証プロファイル	パスワードプロファイル	クライアント証明書の認証(WEB)	公開キーの認証(SSH)	プロファイル	ロックされたユーザー
admin	スーパーユーザ			<input type="checkbox"/>	<input type="checkbox"/>		
test	スーパーユーザ			<input type="checkbox"/>	<input type="checkbox"/>		

図 20-3-3 PA-5450 Administrator 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			
▶ device-and-network	Device and Network Configuration			

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 20-3-4 PA-5450 Administrator 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

2.1. SSL 証明書のインポート/エクスポート

この項では、PA-5450 の証明書のエクスポート、および外部ルート認証局（CA）の証明書をインポートする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

2.1.1. SSL 証明書のエクスポート

証明書のエクスポート手順を記載します。

- ① 「Device」タブ > 「証明書の管理」 > 「証明書」を選択します。
- ② 「デバイス証明書」タブを選択します。

図 2.1.1.1 PA-5450 Certificate issuance

- ③ 発行したい証明書にチェックを入れ、「証明書のエクスポート」をクリックします。

図 2.1.1.2 PA-5450 Certificate issuance

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

- ④ ファイルフォーマットは、「Base64 エンコード済み証明書(PEM)」を選択し、「OK」をクリックします。



図 2 1 – 1 – 3 PA-5450 Certificate issuance

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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. 2. 外部ルート認証局の証明書インポート

外部ルート認証局（CA）の証明書を PA-5450 にインポートする手順を記載します。外部ルート認証局が発行している証明書の有効期限が切れて再発行された場合、および認証局が新設された場合など、PA-5450 に新しい証明書をインポートします。

① インポートする外部ルート認証局の証明書ファイルを用意します。

証明書ファイルはブラウザから取り出し、PEM 形式のテキストファイルとして保存します。ファイルを保存するときの使用可能な拡張子は「.txt」「.cer」「.crt」のいずれかです。

以下は PEM 形式の証明書の例です。

```
-----BEGIN CERTIFICATE-----
MIICAzZCAWwCCQCgYvbe6d0oLzANBgkqhkiG9w0BAQUFADBGMQswCQYDVQQGEwJK
UDEOMAwGA1UEC98543F9reW8xEDA0BgnVBAcTB1NoaWF1eWEFTATBgnVBAoTDFJp
cHBsZXggSW5jLjAeFw0xNTAxgero0Ag1MjJaFw0yNTgxMDMwNjU1MjJaMEYxCzAJ
BgNVBAYTAkpQMq4wDAYDVQQIEwVUb2t5bzEQMA4GA1UEBxMHU2hpYnV5YTEVMBMG
A1UEChMMUmlwcGxleCBJbmMuMIGfMA0GCSqGSIb3DQGBAQUAA4GNADCBiQKBgQDk
VqFrkM71VDdhyqS+muViD3DXf4n0QIIuPtarsn3S+1GxcmtoiPjDzTCG92iU1IY
6+r64I2t28IQz6xmAXwnVUkU2a5t0pmhLeLU7UW8GNYXfAg9WwUSUsUUHAA3UMco
4Id/0g/0DbT8KpJtfVMhfSge0pa04rQKsy5dDNvCHwIDAQABMA0GCSqGSIb3DQE
BQUAA4GBbC/D6RWTTeshiWvrwwyU98aP47DVxzUhUbfr3HHaAe3r++/FIUIRsvZN
PPKjAjLdIOuzHPOPFbm0Uzb+T8uPZp1P7oGe+g1MmjgyR9soKPETiLirCqa4sLfz
GTfdh3X/RrSfugcjHPJmfntpLDmI6K1iku1yPDH56I8/AKuIJxLx
-----END CERTIFICATE-----
```

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

- ② 「Device」タブ > 「証明書の管理」 > 「証明書」 > 「デバイス証明書」を選択します。

図 21-2-1 PA-5450 Certificate 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

③ 「インポート」をクリックします。証明書を選択し OK をクリックします。

表 2 1 – 2 – 1 ルート CA インポート

図中番号	名前	利用用途
(1)	証明書名	証明書の名前を入力（6 文字以上）
(2)	証明書ファイル	参照をクリックしあらかじめ保存した証明書ファイルを選択
(3)	ファイルフォーマット	以下を選択します。 「Base64 エンコード済み証明書(PEM)」 「暗号化された秘密鍵と証明書(PKCS12)」

証明書のインポート

①

証明書タイプ ローカル SCEP

証明書名 (1)

証明書ファイル 参照... (2)

ファイルフォーマット

秘密鍵はハードウェアセキュリティモジュール上にあります
 秘密鍵をインポート
 秘密鍵のエクスポートをブロック

キーファイル 参照...

パスフレーズ

パスフレーズの確認

OK キャンセル

図 2 1 – 2 – 2 PA-5450 Certificate 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 インポートした証明書の名前をクリックして証明書を表示させます。「信頼されたルート CA」のチェックを付けて OK ボタンをクリックします。

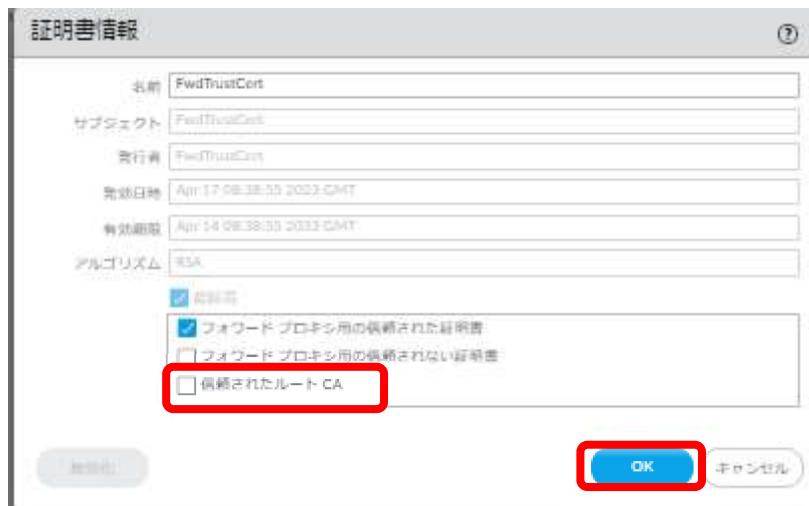


図 21-2-3 PA-5450 Certificate Name

- 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 21-2-4 PA-5450 Certificate Import

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

図 21-2-5 PA-5450 Certificate 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

2.1.3. DMZ サーバの証明書インポート

- ① 「Device」タブ > 「証明書の管理」 > 「証明書」を選択します。
- ② 「デバイス証明書」タブを選択します。
- ③ 「インポート」ボタンをクリックします。

The screenshot shows the 'Certificates' management interface. The left sidebar has a tree view with '証明書の管理' expanded, showing '証明書'. The main area shows a table of certificates with two entries: 'FwdTrustCert' and 'FwdUntrustCert'. The top navigation bar includes tabs for DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE (highlighted with a red box), and other device-specific tabs.

図 2.1-3-1 DMZ サーバの証明書インポート

- ④ (「表 2.1-2-1」) を参照 ※ここは例として「TEST_DMZ」を作成します。

- (1) 名前を設定します。
- (2) インポートする証明書を選択します。
- (3) ここは「暗号化された秘密鍵と証明書(PKCS12)」を選択します。
- (4) 密密鍵を2回入力します。

「OK」ボタンをクリックします。

The dialog box is titled '証明書のインポート'. It has a radio button for '証明書タイプ' (Local) selected. The '証明書名' field contains 'TEST_DMZ' (1). The '証明書ファイル' field contains 'C:\fakepath\server.pfx' (2). The 'ファイルフォーマット' dropdown is set to '暗号化された秘密鍵と証明書 (PKCS12)' (3). Below the fields are two password input fields, both containing '*****' (4). At the bottom are 'OK' and 'キャンセル' buttons, with 'OK' highlighted with a red box.

図 2.1-3-2 DMZ サーバの証明書インポート

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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, 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 by user(1) admin). A table lists the commit scope details:

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 changes), '変更サマリー' (Change summary), and 'コミットの検証' (Commit verification). A note states: '注: これによってすべての変更がログイン管理者のアクセス可能なドメインに表示されます。' (Note: This will display all changes in the domain accessible to the logged-in administrator.) A text input field labeled '内容' (Content) is present. The 'Commit' button at the bottom right is highlighted with a red box.

図 2 1 – 3 – 4 DMZ サーバの証明書インポート

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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. ファイアウォールポリシーによる通信制御の設定例

この項ではケースごとによる、ファイアウォールポリシーによる通信制御の設定例を記載しています。

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

2.2. 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

ここでは、本体からプロキシサーバを介してインターネットへ抜ける通信を URL フィルタリングで拒否する手順を記載します。

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

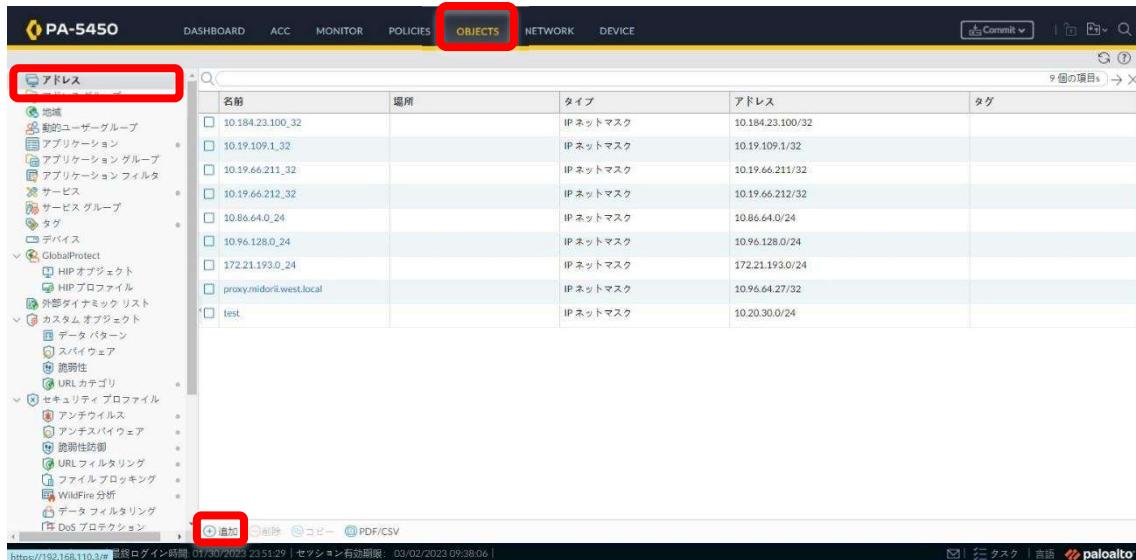


図 22-1-1 PA-5450 Security Policies Add

表 22-1-1 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

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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)で、送信元となる本体のアドレス（ホストまたはネットワーク）を設定（「表 22-1-1」を参照）し、「OK」ボタンをクリックします。



図 22-1-2 PA-5450 Security Policies Add

- ③ 「Objects」タブ > 「セキュリティプロファイル」 > 「URL フィルタリング」 > 「追加」ボタンをクリックします。

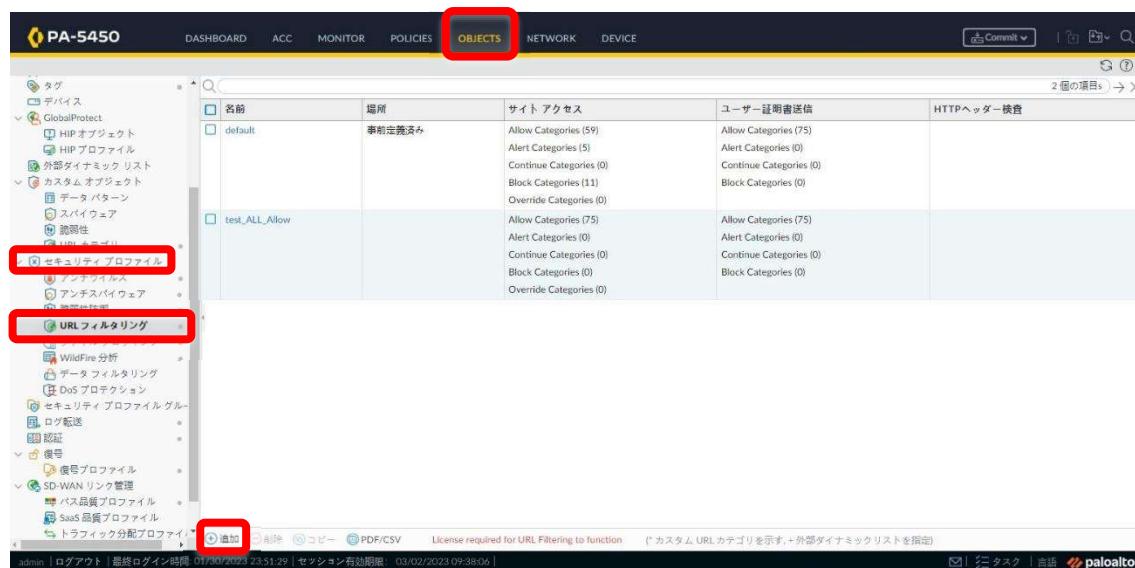


図 22-1-3 PA-5450 URLfilter Policies Add

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

④ 以下(1)～(3)を設定（「図中説明、表 22-1-2」を参照）し、「OK ボタン」をクリックします。

- (1) 任意の URL プロファイル名を指定します。
- (2) 全ての定義済みカテゴリの「サイトアクセス」に「block」を指定します。
- (3) 全てのカスタムカテゴリの（カテゴリ名の末尾に * が付くもの）Action に「none」を指定します。

表 22-1-2 URL フィルタリング URL プロファイル設定

図中番号	名前	利用用途
(1)	名前	「URL フィルタリング URL プロファイル名」を入力 (※) 文字数制限は 31 字迄 また、英数字、スペース、ハイフン (「-」)、アンダースコア (「_」)、ピリオド (「.」) を名前に含めることが可能
(2)	カテゴリ	URL カテゴリのリスト
(3)	サイトアクセス	「URL カテゴリ」のアクションを拒否：「block」を選択

The screenshot shows the 'URL フィルタリング プロファイル' configuration page. Step (1) highlights the '名前' (Name) input field where a profile name is being entered. Step (2) highlights the 'カテゴリ' (Category) section, which lists custom URL categories like 'test_category *'. Step (3) highlights the 'サイトアクセス' (Site Access) table, which shows actions for various categories, with 'block' selected for all entries.

サイトアクセス	ユーザー証明書	送信
block	allow	allow
allow	allow	allow
allow	allow	allow
allow	allow	allow

図 22-1-4 PA-5450 URLfilter 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 「Policies」タブ > 「セキュリティ」 > 「追加」ボタンをクリックします。

名前	タグ	タイプ	ゾーン	アドレス	ユーザー	デバイス	ゾーン	アドレス	送信元	宛先
									ゾーン	アドレス
rule1	none	universal	trust	any	any	any	untrust	any	any	any
test	none	universal	any	any	any	any	Internal_WEST	any	any	any
test_URLFilter_ALL_Allow	none	universal	Internal_WEST	any	any	any	Internal_SV_Critical	any	any	any
interzone-default	none	interzone	any	any	any	any	(Interzone)	any	any	any
interzone-default	none	interzone	any	any	any	any	any	any	any	any

図 22-1-5 PA-5450 Security Policies Add

表 22-1-3 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)	送信元	送信元ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「送信元ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(3)	送信元	送信元アドレス	「送信元アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(4)	宛先	宛先ゾーン ※『0.5.VR のゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(5)	宛先	宛先アドレス	「宛先アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(6)	アプリケーション	アプリケーション	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
(7)	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：「select」を選択し、「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

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

(8)	アクション	アクション	プルダウンより以下を選択 Action が「許可」の場合：「Allow」を選択 Action が「拒否」の場合：「Deny」を選択
(9)	アクション	プロファイルタイプ	プルダウンより以下を選択 ・「プロファイルタイプ」を指定する（UTM 機能を有効）場合： 「Profile」 ※各 UTM 機能を有効化する場合は、各 Profile 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」
(10)	アクション	ログ設定	以下を選択 セッション終了後にロギング：セッション終了時にログ Panorama へ通信ログを送付する場合は、「ログ転送」のプルダウ ンより「Profile_Log_Forwarding」を選択。

④ 以下(1)～(8)を設定（「図中説明、表 22-1-3」を参照）し、「OK」ボタンをク
リックします。

(1) 任意のポリシーネームを指定します。

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 WEST_Proxy_test (1)

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

監査コメント

監査コメント アーカイブ

OK キャンセル

図 22-1-6 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

(2) 「Internal_WEST」を指定します。



図 22-1-7 PA-5450 Security Policies Add

(3) 前の手順②で設定した例の NEXCO 西本体のアドレスを選択します。

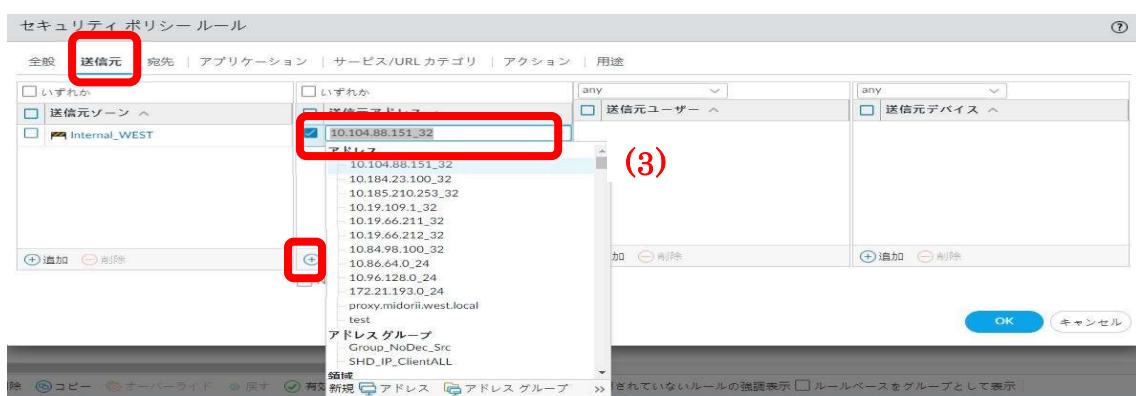


図 22-1-8 PA-5450 Security Policies Add

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

(4) 「Internal_SV_Critical」を選択します。



図 2 2 – 1 – 9 PA-5450 Security Policies Add

(5) プロキシサーバのアドレスを選択します。

（以下の例では、広島（旧緑井）のプロキシサーバ「proxy.midorii.west.local」を選択しています。）

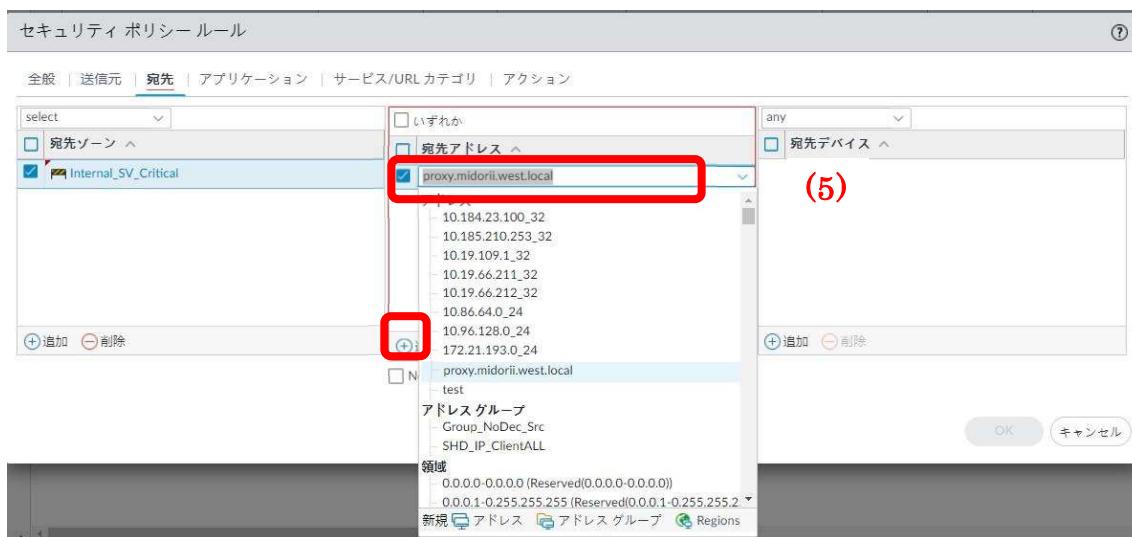


図 2 2 – 1 – 1 0 PA-5450 Security Policies Add

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

(6) 「TCP_8080」を選択します。



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

(7) 「Allow」を選択します。

(8) 「プロファイル」を選択します。

(9) 「JSOC」をします。

(10) 前の手順④で設定した URL プロファイルを選択します。

(11) 「Profile_Log_Fowarding」をします。

「OK」をクリックし設定画面を閉じます。



図 2 2 – 1 – 1 2 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 作成したポリシーを選択し、「移動」にて任意の位置へ移動させます。

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

※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。

1	rule1	none	universal	trust	any
2	test	none	universal	any	any
3	test_URLFilter_ALL_Allow	none	universal	Internal_WEST	any
4	WEST_Proxy_test	none	universal	Internal_WEST	10.1
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any

図 22-1-13 PA-5450 Security Policies Move

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 22-1-14 PA-5450 Commit

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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: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 22-1-15 PA-5450 Commit

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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. 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

ここでは、本体からプロキシサーバを介さずにインターネットへ抜ける全ての通信をファイアウォールポリシーで拒否する手順を記載します。

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

The screenshot shows the PA-5450 interface with the 'OBJECTS' tab selected. Under the 'Addresses' section, there is a table listing various IP address objects. At the bottom left of the table area, there is a red box around the '(+) Add' button.

図 22-2-1 PA-5450 Security Policies Add

表 22-2-1 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

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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)で、送信元となる本体のアドレス（ホストまたはネットワーク）を設定（「表 22-2-1」を参照）し、「OK」ボタンをクリックします。

図 22-2-2 PA-5450 Security Policies Add

- ③ 「Policies」タブ > 「セキュリティ」> 「追加」ボタンをクリックします。

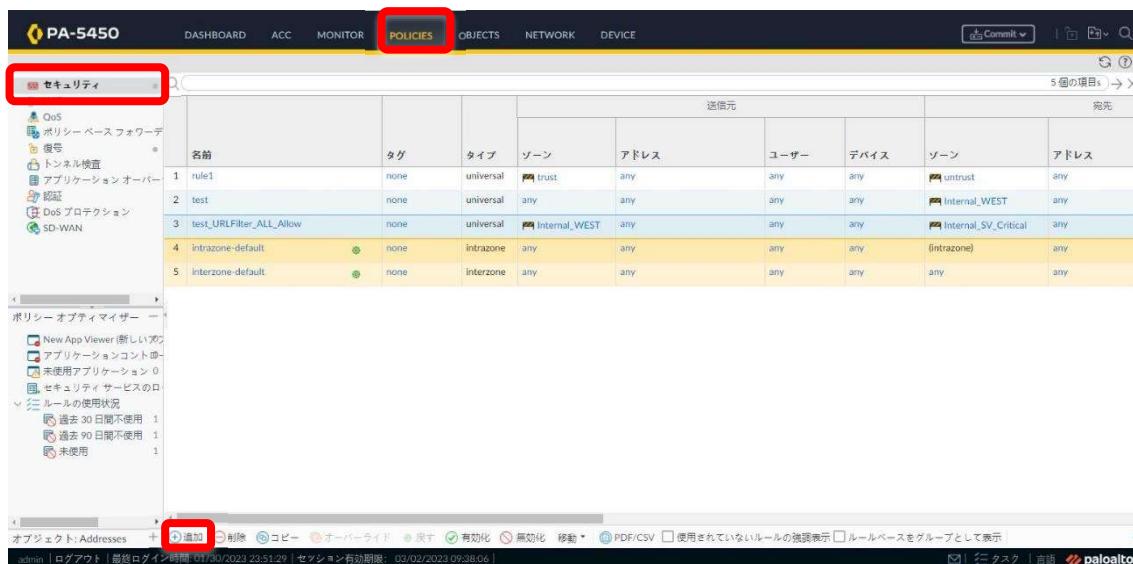


図 22-2-3 PA-5450 Security Policies Add

表 22-2-2 ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「セキュリティポリシー名」を入力 （※）文字数制限は31字迄 また、英数字、スペース、ハイフン（「-」）、アンダースコア（「_」）、ピリオド（「.」）を名前に含めることが可能
(2)	送信元	送信元ゾーン ※『0.5. VR のゾーン名一覧表』を参照	「送信元ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 （「追加」ボタンをクリックして選択）

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

(3)	送信元	送信元アドレス	「送信元アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 （「追加」ボタンをクリックして選択）
(4)	宛先	宛先ゾーン ※『0.5.VRのゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 （「追加」ボタンをクリックして選択）
(5)	宛先	宛先アドレス	「宛先アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 （「追加」ボタンをクリックして選択）
(6)	アプリケーション	アプリケーション	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
(7)	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：「select」を選択し、「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
(8)	アクション	アクション	プルダウンより以下を選択 Action が「許可」の場合：「Allow」を選択 Action が「拒否」の場合：「Deny」を選択
(9)	アクション	プロファイルタイプ	プルダウンより以下を選択 ・「プロファイルタイプ」を指定する（UTM 機能を有効）場合：「Profile」 ※各 UTM 機能を有効化する場合は、各 Profile 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」
(10)	アクション	ログ設定	以下を選択 セッション終了後にロギング：セッション終了時にログ Panorama へ通信ログを送付する場合は、「ログ転送」のプルダウンより「Profile_Log_Forwarding」を選択。

④ 以下(1)～(7)を設定（「図中説明、表 22-2-2」を参照）し、「OK」ボタンをクリックします。

(1) 任意のポリシーネ名を指定します。

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

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: WEST_Proxy_test

ルール タイプ: universal (default)

内容 (1)

タグ

監査コメント

監査コメント アーカイブ

OK キャンセル

図 2 2 – 2 – 4 PA-5450 Security Policies Add

(2) 「Internal_WEST」を指定します。

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

<input type="checkbox"/> いずれか	<input checked="" type="checkbox"/> いずれか	any	any
<input type="checkbox"/> 送信元ゾーン	<input type="checkbox"/> 送信元アドレス	<input type="checkbox"/> 送信元ユーザー	<input type="checkbox"/> 送信元デバイス
<input checked="" type="checkbox"/> Internal_WEST			

(2)

追加 削除 追加 削除 追加 削除 追加 削除

Negate

OK キャンセル

図 2 2 – 2 – 5 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

(3) 前の手順②で設定した本体のアドレスを選択します。

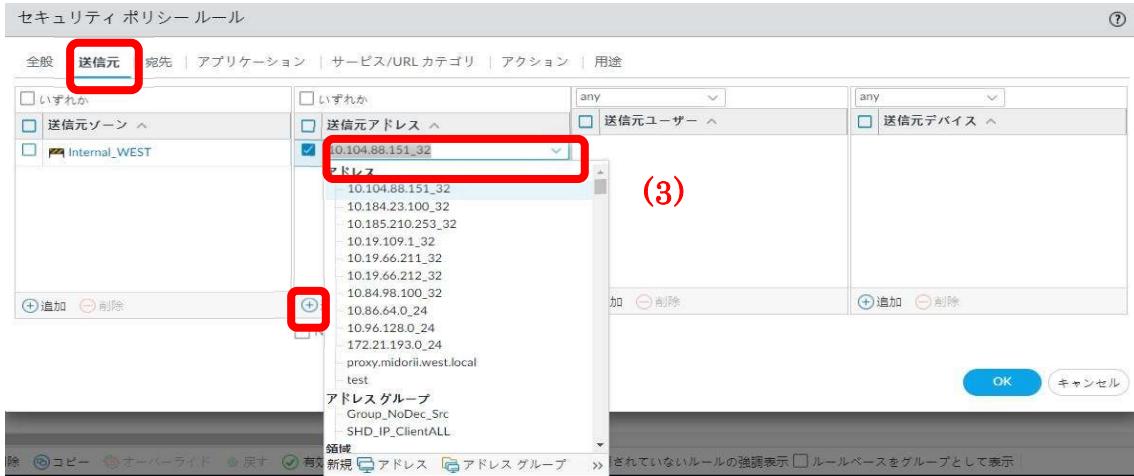


図 22-2-6 PA-5450 Security Policies Add

(4) 「Internal_Untrust」を選択します。



図 22-2-7 PA-5450 Security Policies Add

(5) 「any」を選択します。



図 22-2-8 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

- (6) 「Deny」を選択します。
(7) 「Profile_Log_Fowarding」を選択します。



図 22-2-9 PA-5450 Security Policies Add

- ⑤ 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。
※新規で作成したポリシーは「intrazone-default」の上に作成されます。
※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。

1	rule1	none	universal	trust	any
2	test	none	universal	any	any
3	test_URLFilter_ALL_Allow	none	universal	Internal_WEST	any
4	WEST_Proxy_test	none	universal	Internal_WEST	10.1
5	intrazone-default	none	intrazone	any	any
6	interzone-default	none	interzone	any	any



図 22-2-10 PA-5450 Security Policies Move

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

- ⑥ 「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 22-2-11 PA-5450 Commit

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 22-2-12 PA-5450 Commit

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

2.2.3. 特定のプロトコルのみを拒否する方法

ここでは、本体からプロキシサーバを経由してインターネットへ抜ける特定の FTP サイトへの通信をファイアウォールポリシーで拒否する手順を記載します。

URL フィルタでは FTP プロトコルのみを指定することは不可能な為、ポリシーにより制御します。

※プロキシサーバから特定の FTP サイト宛ての通信を拒否する設定となる為、プロキシサーバを経由し、設定した FTP サイトへアクセスする通信は全て拒否されます。

表 22-3-1 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。

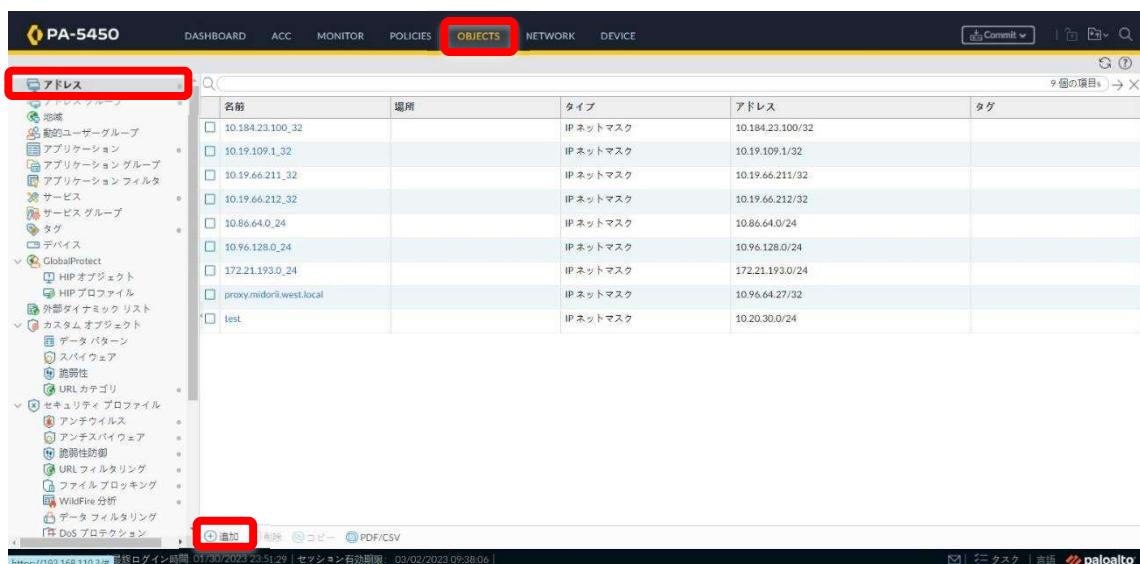


図 22-3-1 PA-5450 Security Policies Add

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

- ② 以下(1)～(3)で、宛先となるサイトを設定（「表 22-3-1」を参照）し、「OK」ボタンをクリックします。

※以下、例として「Address 名:TESTxxx」、「FQDN:ftp. xxx」を入力します。

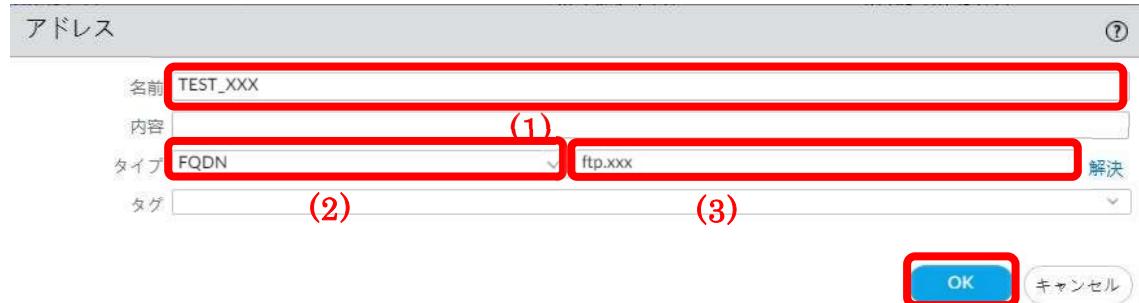


図 22-3-2 PA-5450 Security Policies Add

- ③ 「Policies」タブ > 「セキュリティ」> 「追加」ボタンをクリックします。

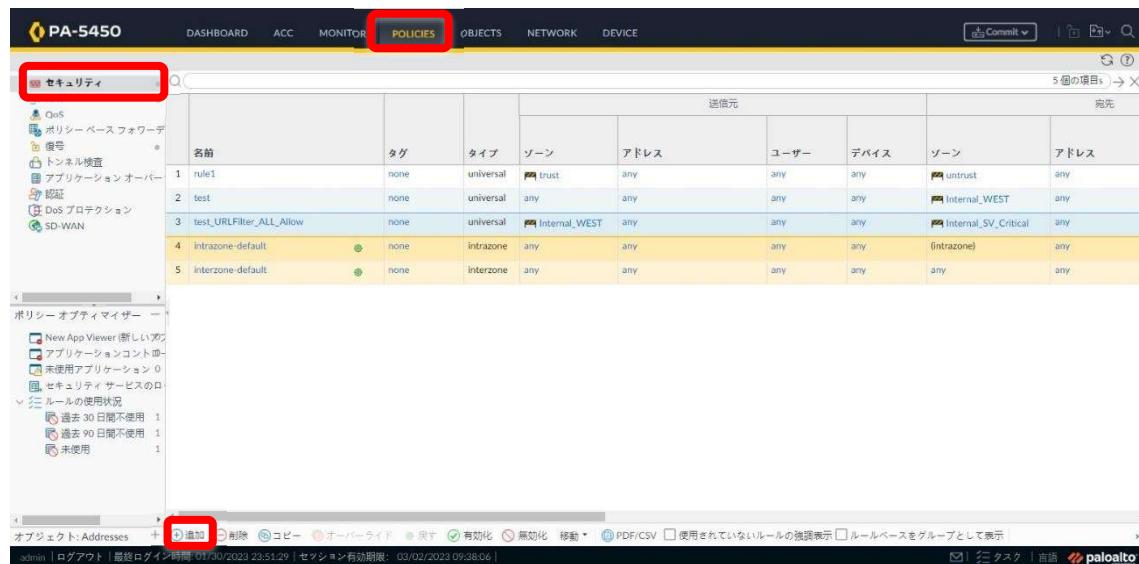


図 22-3-3 PA-5450 Security Policies Add

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 22-3-2 ポリシー設定

図中番号	タブ	名前	利用用途
(1)	全般	名前	「セキュリティポリシー名」を入力 (※) 文字数制限は31字迄 また、英数字、スペース、ハイフン（「-」）、アンダースコア（「_」）、ピリオド（「.」）を名前に含めることが可能
(2)	送信元	送信元ゾーン ※『0.5.VRのゾーン名一覧表』を参照	「送信元ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(3)	送信元	送信元アドレス	「送信元アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(4)	宛先	宛先ゾーン ※『0.5.VRのゾーン名一覧表』を参照	「宛先ゾーン」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(5)	宛先	宛先アドレス	「宛先アドレス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(6)	サービス/ URL カテゴリ	サービス/URL カテゴリ	「サービス」を選択、登録したい対象を検索して、プルダウンからその対象を選択 (「追加」ボタンをクリックして選択)
(7)	アクション	アクション	プルダウンより以下を選択 Action が「拒否」の場合：「Deny」を選択
(8)	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。

⑦ 以下(1)～(7)を設定（「図中説明、表 22-3-2」を参照）し、「OK」ボタンをクリックします。

セキュリティポリシールール

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

名前: Internal_WEST_Internal_Untrust_TEST

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 22-3-4 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

表 22-3-2 (2) 送信元ゾーンを入力します。



図 22-3-5 PA-5450 Security Policies Add

表 22-3-2 (3) 送信元アドレスを入力します。



図 22-3-6 PA-5450 Security Policies Add

表 22-3-2 (4)宛先ゾーンを入力します。



図 22-3-7 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 22-3-2 (5)宛先アドレスを入力します。

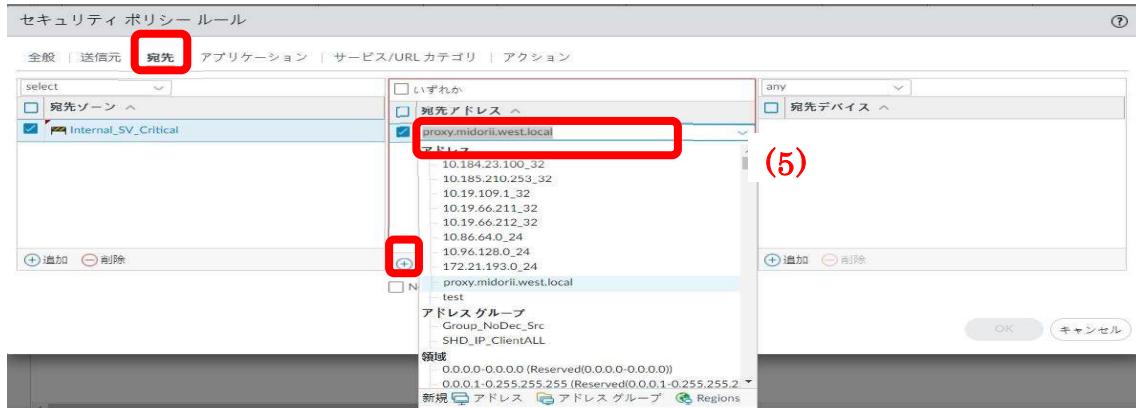


図 22-3-8 PA-5450 Security Policies Add

表 22-3-2 (6) サービス/URL カテゴリを入力します。

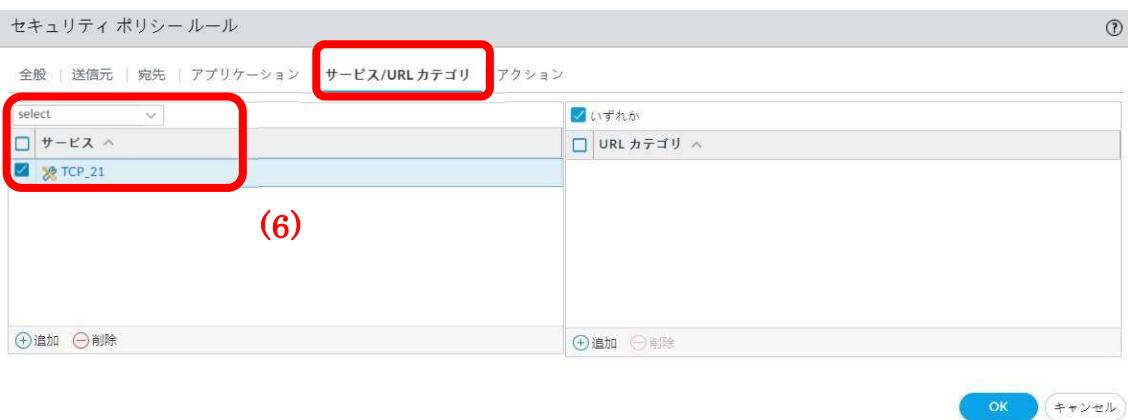


図 22-3-9 PA-5450 Security Policies Add

表 22-3-2 (7) アクションを入力します。※拒否するため Deny を選択します。

表 22-3-2 (8) ログ転送を入力します。



図 22-3-10 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

⑦ 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。

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

※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。

	名前	タグ	タイプ	ゾーン	アドレス
1	rule1	none	universal	trust	any
2	test	none	universal	any	any
3	test_URLFilter_ALL_Allow	none	universal	Internal_WEST	any
4	WEST_Proxy_test	none	universal	Internal_WEST	10.10.10.1
5	Internal_WEST_Internal_Untrust_TEST	none	universal	Internal_WEST	test
6	intrazone-default	none	intrazone	any	any
7	interzone-default	none	interzone	any	any

図 22-3-11 PA-5450 Security Policies Move

⑧ 「コミット」ボタンをクリックし、必要に応じて内容欄に変更内容等の備考を記載後、「コミット」ボタンをクリックします。（設定が反映されるまで 5 分程度かかることがあります）

図 22-3-12 PA-5450 Commit

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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 22-3-13 PA-5450 Commit

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



23. カスタムレポート作成

この項では、Panorama で収集したログを基にレポートを作成する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

2.3. 1. カスタムレポート作成

Panorama にて、出力条件を指定してカスタムレポートを作成する手順を記載します。

- ① 「Monitor」タブ > 「カスタムレポート管理」を選択し、「追加」ボタンをクリックします。

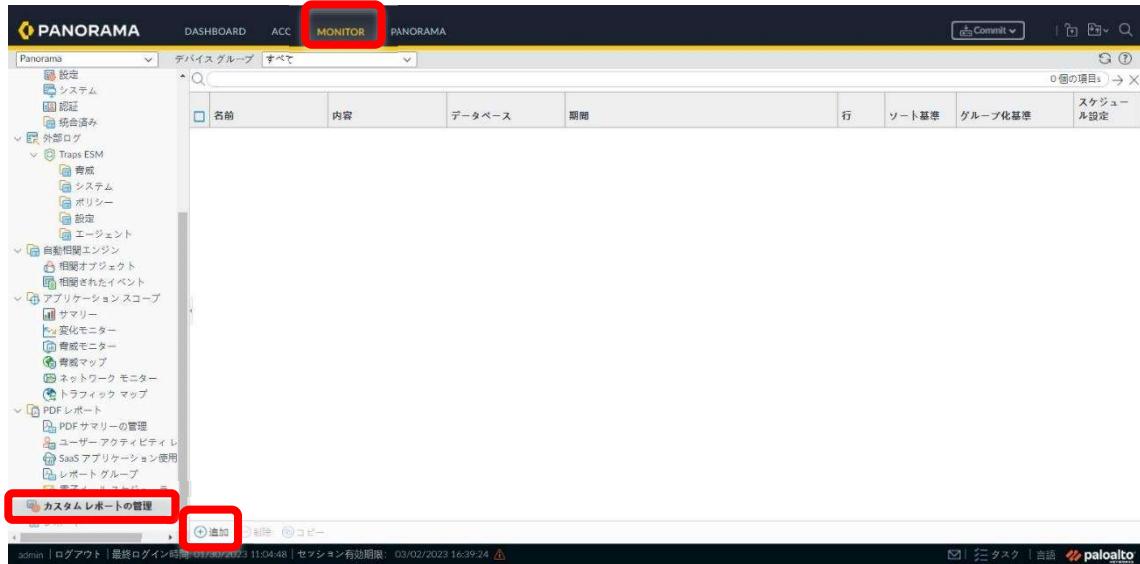


図 2.3-1-1 M-300 Custom Reports

表 2.3-1-1 Custom Reports

図中番号	名前	利用用途
(1)	名前	「カスタムレポート名」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 (‘_’) を名前に含めることができます。
(2)	データベース	レポートの抽出元となるデータベースを指定します。 トラフィックログの場合 : Panorama Traffic Summary URL フィルタログの場合 : Panorama URL Summary
(3)	期間	抽出元となるデータベースの日時範囲を指定します。 あらかじめ定義されている時間枠を選択するか、カスタムを選択して任意の範囲を指定します。
(4)	ソート基準	レポートの内容をソートする基準となる値と、レポートに含める情報の量を指定します。
(5)	使用可能な例, 選択した例	レポートに出力する列を指定します。使用可能な例から出力する列を選択し、「+」ボタンをクリックし選択した例へ移動します。また、トップ、上へ、下へ、一番下へで列の並び替えが可能です。必要に応じて、不要な列は選択した例で選択し、「-」ボタンをクリックし除外します。

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

(6)	クエリビルダー	レポートに抽出するデータのフィルタ条件を指定します。 フィルタできる項目はトライックログ等に定義されている項目と同等です。 結合子 - 追加する条件式の前に設定する結合子 (and/or) を選択します。 属性 - フィルタする項目を選択します。 (項目の種類は表 2 2 – 1 – 2 を参照) 演算子 - 判別基準を選択します。 (イコールなど) 値 - 照合する値を指定します。 値を入力し終えたら、「追加」をクリックします。すべての条件式が完成するまで繰り返します。
-----	---------	--

表 2 3 – 1 – 2 Custom Reports 「属性」例（抜粋）

名前	利用用途
アクション	ログ内の項目「アクション」
送信元アドレス	ログ内の項目「送信元アドレス」
送信元ゾーン	ログ内の項目「送信元ゾーン」
送信元インターフェース	ログ内の項目「送信元インターフェース」
宛先アドレス	ログ内の項目「宛先アドレス」
宛先ポート	ログ内の項目「宛先ポート」
宛先ゾーン	ログ内の項目「宛先ゾーン」
宛先インターフェース	ログ内の項目「宛先インターフェース」
仮想システム	ログ内の項目「仮想システム」
デバイスのシリアル番号	ログ内の項目「シリアル番号」

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

カスタム レポート

レポート設定

(1) 名前: test_report
(2) データベース: Panorama Traffic Summary
(3) 期間: 過去 30 日
(4) ソート基準: Bytes
(5) フィルタ条件: Source Zone (selected in the list)
(6) クエリビルダー: 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。

OK キャンセル

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

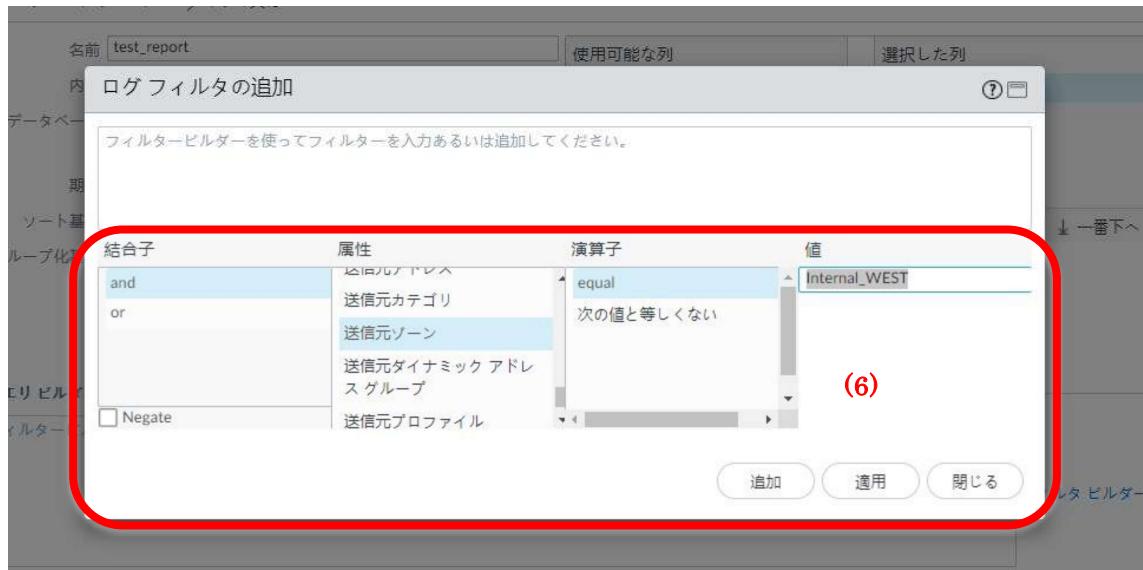


図 23-1-2 M-300 Custom Reports

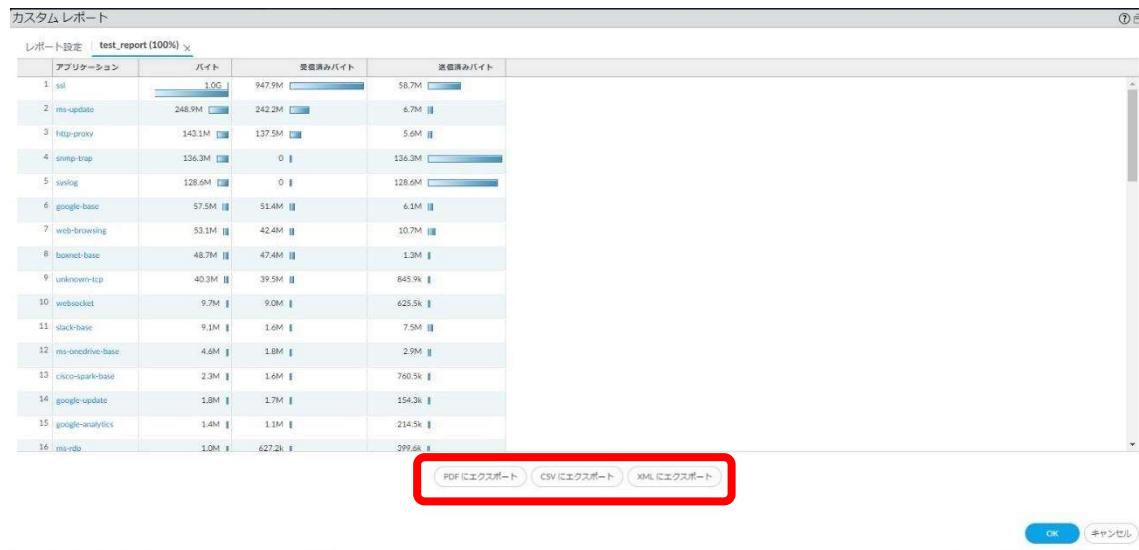
③ 出力条件を設定後、「今すぐ実行」ボタンをクリックし、レポートを作成します。

The screenshot shows the 'カスタム レポート' configuration screen. Under the 'レポート設定' tab, the '今すぐ実行' button is highlighted with a red box. The report settings include: Name: test_report, Content: (empty), Database: Panorama Traffic Summary, Schedule: Not set, Period: Past 30 days, Sort Criteria: Bytes, Top 500, Grouping Criteria: None, 10 Groups. On the right, under '選択した列' (Selected Columns), 'Source Zone' is listed. Below, the 'クエリ ピルダー' section shows the query '(zone.src eq Internal_WEST)'. At the bottom, there are 'OK' and 'キャンセル' (Cancel) buttons.

図 23-1-3 M-300 Custom Reports

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

- ④ レポート名のタブが作成され、自動的に画面が切り替わりレポートが表示されます。
 「PDF にエクスポート」「CSV にエクスポート」「XML にエクスポート」いずれかのボタンで、任意の形式のレポートを出力します。



The screenshot shows the 'カスタムレポート' (Custom Report) settings page for a report named 'test_report (100%)'. The main area displays a table of application statistics. At the bottom, there are three buttons: 'PDF にエクスポート', 'CSV にエクスポート', and 'XML にエクスポート'. The 'CSV にエクスポート' button is highlighted with a red box.

図 2 3 – 1 – 4 M-300 Custom Reports

- ⑤ 「OK」ボタンをクリックし設定画面を閉じます。



The screenshot shows the same 'カスタムレポート' (Custom Report) settings page after clicking 'OK'. The 'OK' button is highlighted with a red box. The report table and export buttons are visible at the bottom.

図 2 3 – 1 – 5 M-300 Custom Reports

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

- ⑥ 「コミット」ボタンをクリックします。
- ⑦ 「Panoramaへのコミット」を選択し、「コミット」をクリックします。



図 23-1-6 M-300 Custom Reports

The screenshot shows a 'Commit' dialog box. At the top, it says 'コミット' and has 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 button options: 'Commit すべての変更' (selected) and 'Commit 変更の実行者(1) admin'. A table below lists the commit scope: 'policy-and-objects' (場所タイプ: Policy and Objects, オブジェクトタイプ: None, エンティティ: None, 管理者: None). At the bottom, there are three buttons: '変更内容の確認' (Change Content Confirmation), '変更サマリー' (Change Summary), and 'コミット' (Commit), which is highlighted with a red box. There is also a 'キャンセル' (Cancel) button.

図 23-1-7 M-300 Custom Reports

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

2.3. 2. カスタムレポート作成例

2.3. 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

ここでは、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通信量の上位 500 までを抽出したレポートの作成例を記載します。

- ① 「Monitor」タブ > 「カスタムレポートの管理」を選択し、「追加」ボタンをクリックします。

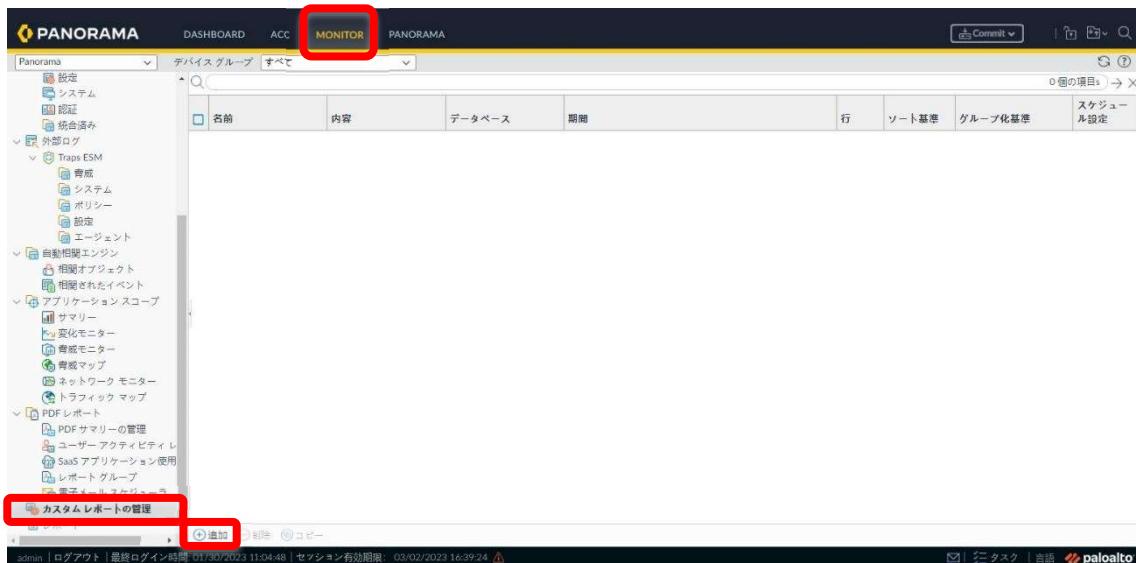


図 23-2-1 M-300 Custom Reports

表 23-2-1 Custom Reports

図中番号	名前	利用用途
(1)	名前	「カスタムレポート名」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（「_」）を名前に含めることができます。
(2)	データベース	レポートの抽出元となるデータベースを指定します。 トラフィックログの場合 : Panorama Traffic Summary URL フィルタログの場合 : Panorama URL Summary
(3)	期間	抽出元となるデータベースの日時範囲を指定します。 あらかじめ定義されている時間枠を選択するか、カスタムを選択して任意の範囲を指定します。
(4)	ソート基準	レポートの内容をソートする基準となる値と、レポートに含める情報の量を指定します。
(5)	使用可能な例、選択した例	レポートに出力する列を指定します。使用可能な例から出力する列を選択し、「+」ボタンをクリックし選択した例へ移動します。また、トップ、上へ、下へ、一番下へで列の並び替えが可能です。必要に応じて、

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

		不要な列は選択した例で選択し、「-」ボタンをクリックし除外します。
(6)	クエリビルダー	<p>レポートに抽出するデータのフィルタ条件を指定します。 フィルタできる項目はトラフィックログ等に定義されている項目と同等です。</p> <p>結合子 - 追加する条件式の前に設定する結合子 (and/or) を選択します。</p> <p>属性 - フィルタする項目を選択します。（項目の種類は表 22-1-2 を参照）</p> <p>演算子 - 判別基準を選択します。（イコールなど）</p> <p>値 - 照合する値を指定します。</p> <p>値を入力し終えたら、「追加」をクリックします。すべての条件式が完成するまで繰り返します。</p>

表 23-2-2 Custom Reports 「属性」例（抜粋）

名前	利用用途
アクション	ログ内の項目「アクション」
送信元アドレス	ログ内の項目「送信元アドレス」
送信元ゾーン	ログ内の項目「送信元ゾーン」
送信元インターフェース	ログ内の項目「送信元インターフェース」
宛先アドレス	ログ内の項目「宛先アドレス」
宛先ポート	ログ内の項目「宛先ポート」
宛先ゾーン	ログ内の項目「宛先ゾーン」
宛先インターフェース	ログ内の項目「宛先インターフェース」
仮想システム	ログ内の項目「仮想システム」
デバイスのシリアル番号	ログ内の項目「シリアル番号」

- ② 以下(1)～(7)を設定（「図中説明、表 23-2-3」を参照）し、「OK」ボタンをクリックします。
本手順で作成するレポートの設定内容は以下の通りです。

表 23-2-3 Custom Reports

図中番号	名前	設定内容
(1)	名前	ToInternet_report
(2)	データベース	Panorama Traffic Summary (Panorama で取集したトラフィックログ)
(3)	期間	Last Calendar Month (先月分)
(4)	ソート基準	Bytes、Top500 (通信量の上位 500 までを抽出)
(6)	使用可能な列、選択した列	Source Zone、Destination Zone、Source address、Destination address、Application、Virtual System Name、Bytes、Bytes Received、Bytes Sent
(7)	クエリビルダー	フィルタ条件全文：

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

	(zone.dst eq Untrust) and (serial eq 0008C101214) and (vsys eq vsys1) フィルタ条件内訳： (zone.dst eq Untrust) - Destination zone が Untrust (serial eq 0008C101214) - シリアル番号が 0008C101214（広島 DC の PA-5450 で処理した通信） ※シリアル番号の確認方法は、「付録 1. CLI コマンドリスト システム情報確認」を参照。 (vsys eq vsys1) - vsys が vsys1（インターネット FW） ※これらの条件を and で結合しているため、全ての条件を満たしたデータが抽出される。
--	---

カスタム レポート

レポート設定 (5)

テンプレートのロード → 今すぐ実行

(1) 名前 ToInternet_report
 内容
 (2) データベース Panorama Traffic Summary
 スケジュール設定
 (3) 期間 過去 30 曜日
 (4) ソート基準 Bytes トップ 500
 グループ化基準 None 10 グループ

使用可能な列
 App Technology
 Apps
 Association ID
 Bytes
 Source Zone
 Source Address
 Destination Zone
 Destination Address

下 トップ 上へ 下へ 下へ 一番下へ

クエリビルダー (6)
 (zone.src eq Internal_WEST)

If using Headers Inserted field, then Report will contain truncated header values

OK キャンセル

図 2 3 – 2 – 2 M-300 Custom Reports

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

③ 出力条件を設定後、「今すぐ実行」ボタンをクリックし、レポートを作成します。

カスタム レポート

レポート設定

テンプレートのロード → 今すぐ実行

名前 ToInternet_report

内容

データベース Panorama Traffic Summary

スケジュール設定

期間 過去 30 曜日

ソート基準 Bytes トップ 500

グループ化基準 None 10 グループ

使用可能な列

- App Technology
- Apps
- Association ID
- Bytes

選択した列

- Source Zone
- Source Address
- Destination Zone
- Destination Address

クエリ ビルダー

(zone.src eq Internal_WEST)

フィルタ ビルダー

If using Headers Inserted field, then Report will contain truncated header values

OK キャンセル

図 23-2-3 M-300 Custom Reports

④ レポート名のタブが作成され、自動的に画面が切り替わりレポートが表示されます。
「PDF にエクスポート」「CSV にエクスポート」「XML にエクスポート」いずれかのボタンで、任意の形式のレポートを出力します。

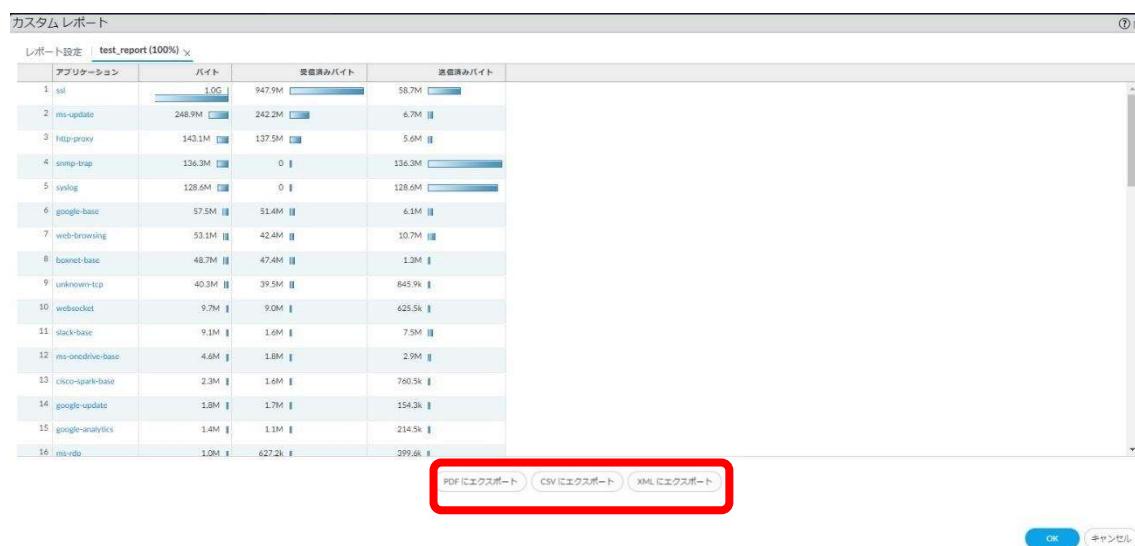


図 23-2-4 M-300 Custom Reports

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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設定画面を閉じます。



図 23-2-5 M-300 Custom Reports

⑥ 「コミット」ボタンをクリックします。

⑦ 「Panoramaへのコミット」を選択し、「コミット」をクリックします。



図 23-2-6 M-300 Custom Reports

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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 23-2-7 M-300 Custom Reports

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

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

ここでは、送信元がG会社から吹田DC(旧電算室)プロキシサーバ宛の通信で、URLフィルタのアラートログ（URLフィルタで検査され通過したログ）を宛先URL毎にアクセス回数の上位500までを抽出したレポートの作成例を記載します。

- 「Monitor」タブ > 「カスタムレポートの管理」を選択し、「追加」ボタンをクリックします。

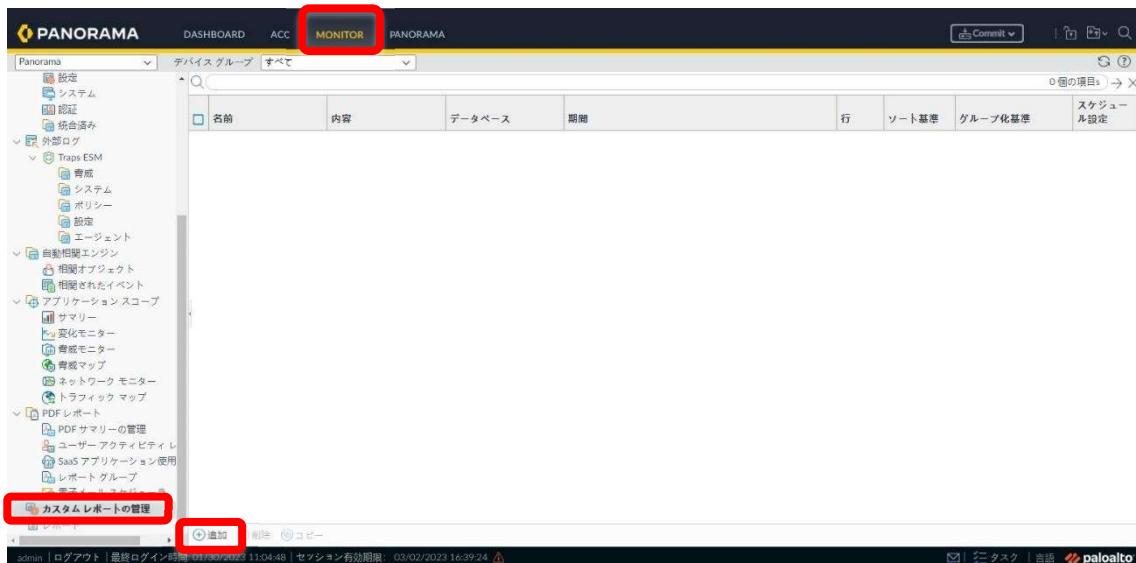


図23-2-8 M-300 Custom Reports

表23-2-4 Custom Reports

図中番号	名前	利用用途
(1)	名前	「カスタムレポート名」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（「_」）を名前に含めることができます。
(2)	データベース	レポートの抽出元となるデータベースを指定します。 トラフィックログの場合：Panorama Traffic Summary URLフィルタログの場合：Panorama URL Summary
(3)	期間	抽出元となるデータベースの日時範囲を指定します。 あらかじめ定義されている時間枠を選択するか、カスタムを選択して任意の範囲を指定します。
(4)	ソート基準	レポートの内容をソートする基準となる値と、レポートに含める情報の量を指定します。
(5)	使用可能な例、選択した例	レポートに出力する列を指定します。使用可能な例から出力する列を選択し、「+」ボタンをクリックし選択した例へ移動します。また、トップ、上へ、下へ、一番下へで列の並び替えが可能です。必要に応じて、

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

		不要な列は選択した例で選択し、「-」ボタンをクリックし除外します。
(6)	クエリビルダー	<p>レポートに抽出するデータのフィルタ条件を指定します。 フィルタできる項目はトラフィックログ等に定義されている項目と同等です。</p> <p>結合子 - 追加する条件式の前に設定する結合子 (and/or) を選択します。</p> <p>属性 - フィルタする項目を選択します。（項目の種類は表 22-1-2 を参照）</p> <p>演算子 - 判別基準を選択します。（イコールなど）</p> <p>値 - 照合する値を指定します。</p> <p>値を入力し終えたら、「追加」をクリックします。すべての条件式が完成するまで繰り返します。</p>

表 23-2-5 Custom Reports 「属性」例（抜粋）

名前	利用用途
アクション	ログ内の項目「アクション」
送信元アドレス	ログ内の項目「送信元アドレス」
送信元ゾーン	ログ内の項目「送信元ゾーン」
送信元インターフェース	ログ内の項目「送信元インターフェース」
宛先アドレス	ログ内の項目「宛先アドレス」
宛先ポート	ログ内の項目「宛先ポート」
宛先ゾーン	ログ内の項目「宛先ゾーン」
宛先インターフェース	ログ内の項目「宛先インターフェース」
仮想システム	ログ内の項目「仮想システム」
デバイスのシリアル番号	ログ内の項目「シリアル番号」

② 以下(1)～(7)を設定（「図中説明、表 23-2-6」を参照）し、「OK」ボタンをクリックします。

本手順で作成するレポートの設定内容は以下の通りです。

表 23-2-6 Custom Reports

図中番号	名前	設定内容
(1)	名前	URL_Filter_report
(2)	データベース	Panorama URL Summary (Panorama で収集した URL フィルタログ)
(3)	期間	Last Calendar Month (先月分)
(4)	ソート基準	Count、Top500 (アクセス回数の上位 500 までを抽出)
(6)	使用可能な例、選択した例	Category、URL Domain、Action、Virtual System、Count
(7)	クエリビルダー	フィルタ条件全文：

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

	(addr.src in '10.80.0.0/13') and (addr.dst in '10.19.132.27/32') and (action eq alert) and (serial eq 001901000693) and (vsys eq vsys2) フィルタ条件内訳： (addr.src in '10.80.0.0/13') - 送信元アドレスが 10.80.0.0/13 (G 会社の NAT アドレス) (addr.dst in '10.19.132.27/32') -宛先アドレスが 10.19.132.27/32 (吹田 DC(旧電算室)プロキシサーバ) (action eq alert) - URL フィルタで Alert 処理された通信 (URL フィルタで検査され通過した通信) (serial eq 001901000693) - シリアル番号が 001901000693 (吹田 DC(旧電算室)の PA-5450 で処理した通信) ※シリアル番号の確認方法は、「付録 1. CLI コマンドリスト システム情報確認」を参照。 (vsys eq vsys2) - vsys が vsys2 (内部接続用 FW) ※これらの条件を and で結合しているため、全ての条件を満たしたデータが抽出される。
--	---

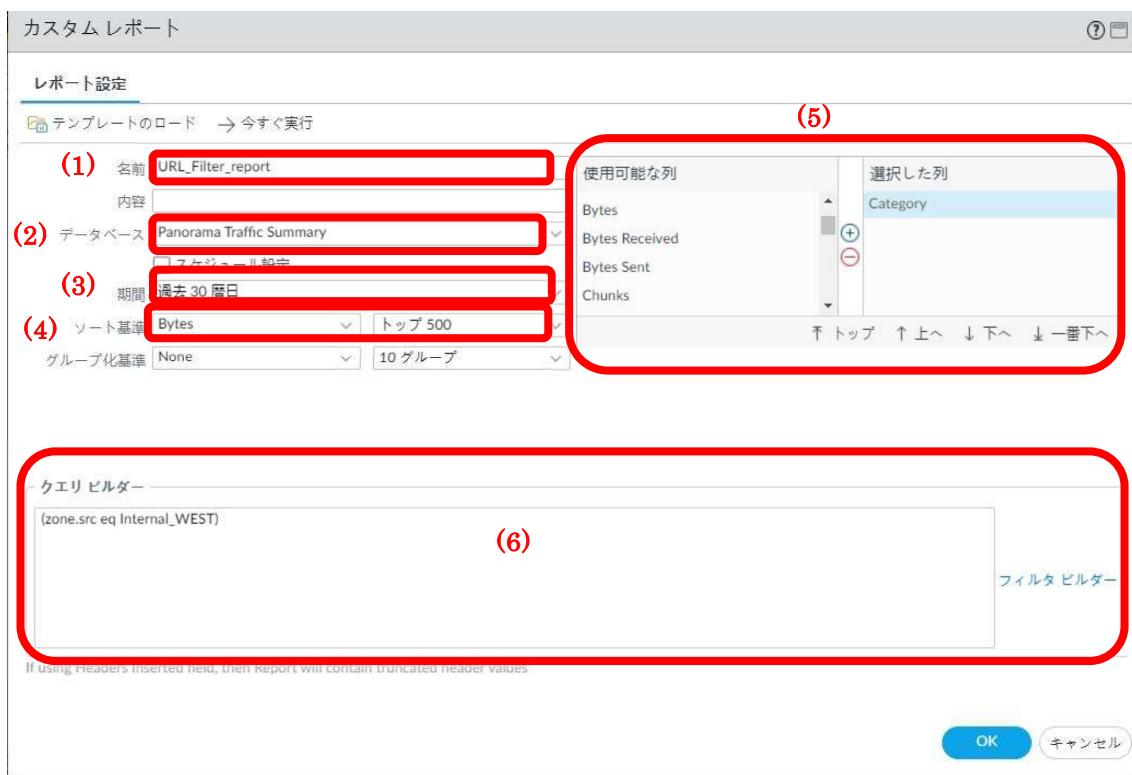


図 2 3 – 2 – 9 M-300 Custom Reports

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

③ 出力条件を設定後、「今すぐ実行」ボタンをクリックし、レポートを作成します。

カスタム レポート

レポート設定

テンプレートのロード → 今すぐ実行

名前 URL_Filter_report

内容

データベース Panorama Traffic Summary

スケジュール設定

期間 過去 30 曜日

ソート基準 Bytes トップ 500

グループ化基準 None 10 グループ

使用可能な列

選択した列 Category

Bytes Bytes Received Bytes Sent Chunks

↑ トップ ↑ 上へ ↓ 下へ ↓ 一番下へ

クエリ ビルダー

(zone.src eq Internal_WEST)

フィルタ ビルダー

If using Headers Inserted field, then Report will contain truncated header values.

OK キャンセル

図 2 3 – 2 – 1 0 M-300 Custom Reports

④ レポート名のタブが作成され、自動的に画面が切り替わりレポートが表示されます。
「PDF にエクスポート」「CSV にエクスポート」「XML にエクスポート」いずれかのボタンで、任意の形式のレポートを出力します。

カスタム レポート

レポート設定 | URL_Filter_report (100%)

	アプリケーション	バイト	受信済みバイト	送信済みバイト
1	snmp-trap	12.4G	3.1M	12.4G
2	paloalto-updates	7.2G	7.0G	250.0M
3	ssl	6.4G	6.1G	261.5M
4	ms-update	1.0G	990.0M	23.2M
5	ms-onedrive-base	934.6M	30.0M	904.6M
6	http-proxy	467.0M	453.9M	13.1M
7	netflow	3811M	0	381.1M
8	google-base	317.5M	259.1M	58.4M
9	panorama	228.9M	57.7M	171.2M
10	web-browsing	201.1M	187.4M	13.6M
11	paloalto-iot-	191.7M	85.5M	106.2M

PDF にエクスポート CSV にエクスポート XML にエクスポート

OK キャンセル

図 2 3 – 2 – 1 1 M-300 Custom Reports

ドキュメント名	運用手順書（セキュリティ機器）			最終更新日	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設定画面を閉じます。



図 2 3 – 2 – 1 2 M-300 Custom Reports

- ⑥ 「コミット」ボタンをクリックします。
⑦ 「Panoramaへのコミット」を選択し、「コミット」をクリックします。

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

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 キャンセル

図 2 3 – 2 – 1 4 M-300 Custom Reports

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

24. 障害時に取得するログ情報について

この項では、初動問い合わせ時に取得するログ、パケットキャプチャを取得する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

24.1. テクニカルサポートに必要なログ

障害内容によって、取得すべきログは異なる為、初動時に必要なログのみ記載します。

- Tech Support File

※GUI から Tech Support File を作成するには、Super User の権限が必要です。

取得する手順について記載します。

- 「Device」タブ > 「サポート」を選択します。

※Panorama の場合は、「Panorama」タブ > 「サポート」を選択します。

- 「テクニカルサポートファイル」の下にある「テクニカルサポートファイルの生成」をクリックします。



図 24-1-1 PA-5450 Tech Support File

- 「はい」をクリックします。



図 24-1-2 PA-5450 Tech Support File