ITKeeperシリーズ「Palo Alto Networks 運用パック」ユーザーマニュアル Version1.0

RICOH
imagine. change.

はじめに

- 本書は、弊社が「Palo Alto Networks 運用パック」をご契約いただいたお客様を対象として、対象機器に関する基本的な操作を記述した使用説明書です。
- お客様のパスワードの管理はお客様ご自身にてお願いいたします。
- お客様がご利用の ISP（インターネット サービス プロバイダー）の障害や、回線の障害時にはサービスをご利用いただけないことがあります。
- ブラウザーは最新版をご利用ください。
- 本ユーザーマニュアルは以下の環境にて作成しています。環境によっては、画面の表示が異なる場合や記載している操作ができない場合があります。
  - ✓ 動作検証PC：Windows10
  - ✓ 動作検証ブラウザ：Google Chrome
  - ✓ 動作確認機器：PA-220,PA-820,PA-850
- 本書の内容の一部または全部を無断で複写することは禁止されております。
- 本書の内容は事前の予告なく変更されることがあります。
- お客様データの消失による損害、その他本サービスおよび本書の使用または使用不能により生じた損害については、法令上損害賠償責任が認められる場合を除き、弊社は一切その責任を負えませんのであらかじめご了承ください。

目次

目次

1.管理アクセス

1-1.WebUIアクセス

・ブラウザを起動し、URL欄に機器の管理アドレスを入力します。
利用できるプロトコル (HTTPS又はHTTP)とアドレスはパラメータシート(別紙)をご参照ください。
例：https://<管理IPアドレス>

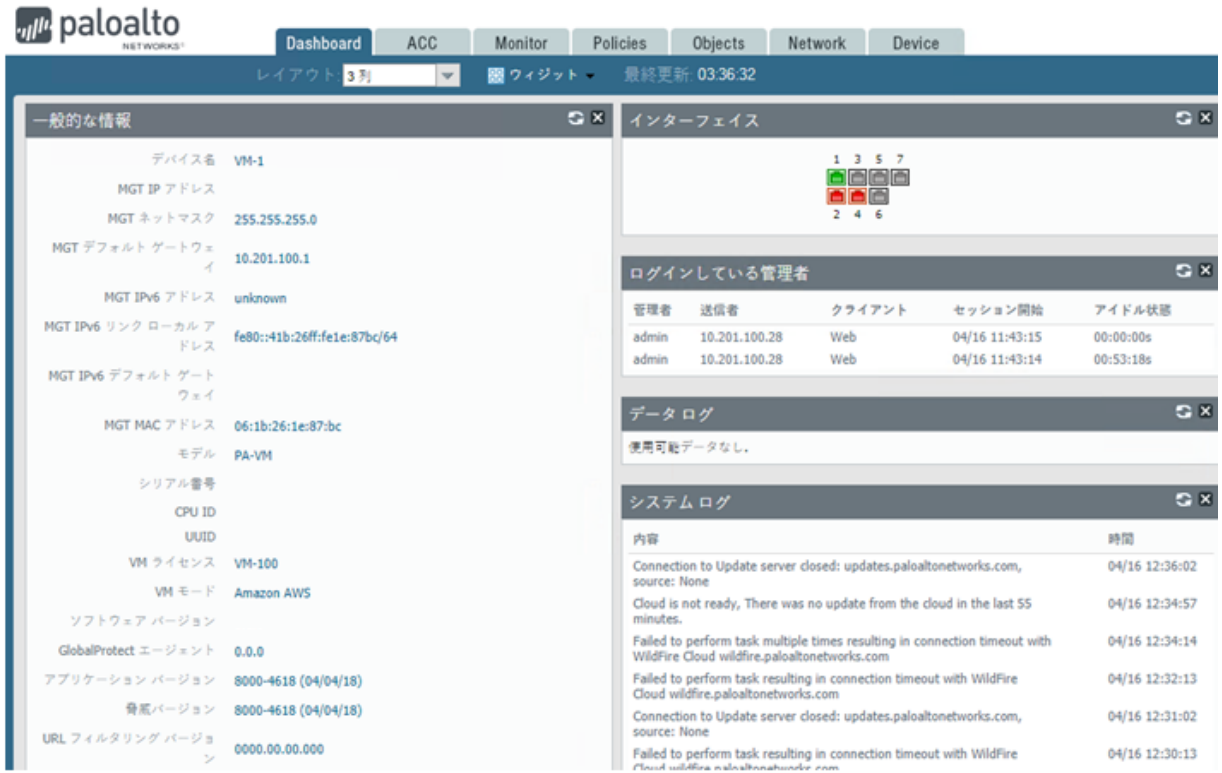
・ログイン画面(下図)に「名前」「パスワード」を入力し「ログイン」をクリックします。

1.管理アクセス

1-1.WebUIアクセス（続き）

・証明書に関するセキュリティ警告が表示されますが、「<アドレスにアクセスする>」
をクリックします。

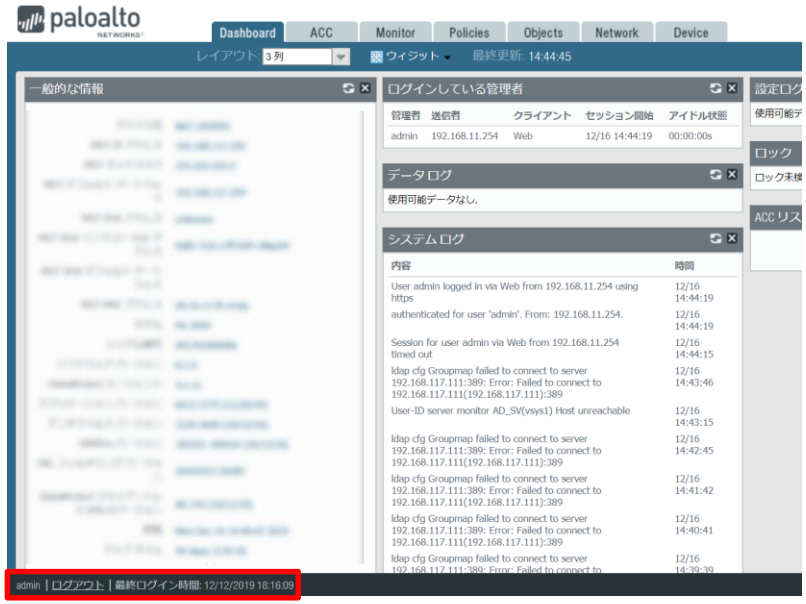
・ログインに成功すると、ダッシュボード画面(下図)が表示されます。



1.管理アクセス

1-1.WebUIアクセス（ログアウトの方法）

・管理画面左下にあるログアウトをクリックするとログアウトできます。



2.システムステータス確認

2-1.システムステータス確認 – WebUI

ダッシュボード画面にて、システムの基本的なステータスを確認できます。

①	一般的な情報	管理設定、モデル、OSバージョン、シリアル、各シグネチャのバージョン、システム日時、アップタイムを表示します。
②	システムリソース	管理プレーン、データプレーンのCPU使用状況を表示します。
③	高可用性 (利用している場合)	ステータス(アクティブ/パッシブ)、コンフィグ同期状況、シグネチャバージョン差異があるか等、高可用性の状況を表示します。
④	インターフェース	インターフェースステータスを表示します。緑がアップリンク状態を示します。
⑤	システムログ	直近のシステムログを表示します。

2.システムステータス確認

2-2.システムログ確認 – WebUI

機器に保存されているシステムログは、Monitor画面にて確認します。

・Monitor > ログ > システム

3.通信ログ確認

3-1.ログの種類

PaloAltoの主なログは下記の通りです。
ポリシーやプロファイル等で取得する設定となっている場合、 Monitor > ログ の各ログ画面に表示されます。

ログ種別	内容
トラフィック	各セッションの開始または終了時に取得したログが出力されます。
脅威	アンチウイルス、アンチスパイウェア、IPSの検知ログが出力されます。
URLフィルタリング	URLフィルタリングの検知ログが出録されます。
WildFireへの送信	WildFireにて検査し、マルウェアと判定された場合、ログが出力されます。
データフィルタリング	ファイルブロッキング及びデータフィルタリングプロファイルでの検知ログが出力されます。
設定	コンフィグの変更履歴が出力されます。
システム	システムに関するログが出力されます。
統合済み	トラフィック、脅威、URL フィルタリング、WildFire への送信、データフィルタリングログが一つの画面で表示されます。

3.通信ログ確認

3-2.トラフィックログ

トラフィックログの主なフィールドは下記の通りです。

ログ種別	内容
受信日時	通信が発生した時間
タイプ	セッションの開始または終了(start または end)
送信元/宛先ゾーン	送信元及び宛先ゾーン名
送信元	送信元IPアドレス
宛先	宛先IPアドレス
宛先ポート	宛先のポート番号
アプリケーション	識別されたアプリケーション名
アクション	セッションに適用されたアクション(allow、denyなど)
ルール	適用されたセキュリティポリシーのルール名

3.通信ログ確認

3-3.脅威ログ

脅威ログの主なフィールドは下記の通りです。

ログ種別	内容
受信日時	通信が発生した時間
タイプ	検知した脅威のタイプ。マルウェア(virus)、最新のマルウェア(wildfire-virus)、脆弱性防御 (vulnerability)、スパイウェア(spyware)
名前	検知した脅威の名称
送信元/宛先ゾーン	送信元及び宛先ゾーン名
攻撃者	攻撃者のIPアドレス
被害者	被害者のIPアドレス
宛先ポート/アプリケーション	宛先のポート番号、識別されたアプリケーション
アクション	適用されたアクション(allow、denyなど)
重大度	検知した脅威のレベル
ルール	適用されたセキュリティポリシーのルール名

3.通信ログ確認

3-3.脅威ログ（続き）

脅威ログの重大度は下記のように分類されます。

重大度	内容
Critical	一般的に使用されているサーバやソフトウェアに対し、認証や特殊な操作をせずに攻撃可能である脅威です。
High	重大度が Critical に変わる可能性があるものの、軽減要因が存在する脅威です。たとえば、悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害数が多くなかったりする場合です。
Medium	影響度が抑えられる小さな脅威です。たとえば、標的に侵入することのない DoS 攻撃や、攻撃者が被害端末と同じ LAN 上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。なお、アンチウイルスプロファイルでの検知結果は、Medium としてログに記録されます。
Low	影響がわずかな警告レベルの脅威です。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーや DoS の問題、情報漏洩などが発 生することがあります。
Information	直ちに脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベントです。URL フィルタリング ログ エントリと安全判定の WildFire 送信ログ エントリは Informational としてログに記録されます。

3.通信ログ確認

3-4.URLフィルタリングログ

URLフィルタリングログの主なフィールドは下記の通りです。

ログ種別	内容
受信日時	通信が発生した時間
カテゴリ	宛先URLがカテゴライズされる、PAN-DBのカテゴリまたはカスタムカテゴリの名称
URL	宛先URL
送信元/宛先ゾーン	送信元及び宛先ゾーン名
送信元/宛先	送信元及び宛先IPアドレス
アプリケーション	識別されたアプリケーション
アクション	適用されたアクション(allow、denyなど)
ルール	適用されたセキュリティポリシーのルール名

3.通信ログ確認

3-5.WildFireへの送信ログ

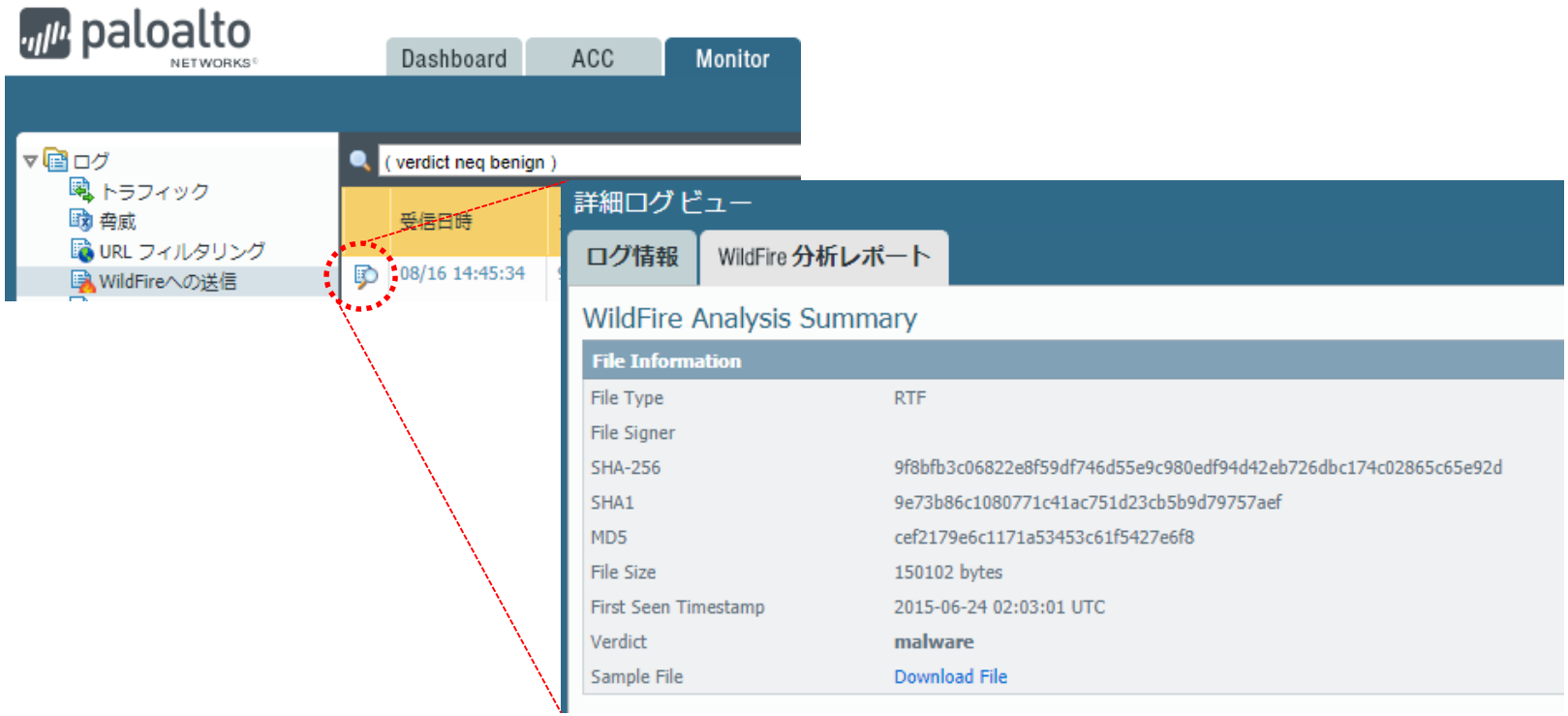
WildFireへの送信ログの主なフィールドは下記の通りです。

ログ種別	内容
受信日時	通信が発生した時間
ファイル名	宛先URLがカテゴライズされる、PAN-DBのカテゴリまたはカスタムカテゴリの名称
URL	宛先URL
送信元/宛先ゾーン	送信元及び宛先ゾーン名
攻撃者	攻撃者のIPアドレス
被害者	被害者のIPアドレス
宛先ポート/アプリケーション	宛先のポート番号、識別されたアプリケーション
判定	WildFireでの判定結果。デフォルトではマルウェアのみ表示されます。
ファイルタイプ	検査されたファイルのファイルタイプ

3.通信ログ確認

3-5.WildFireへの送信ログ（続き）

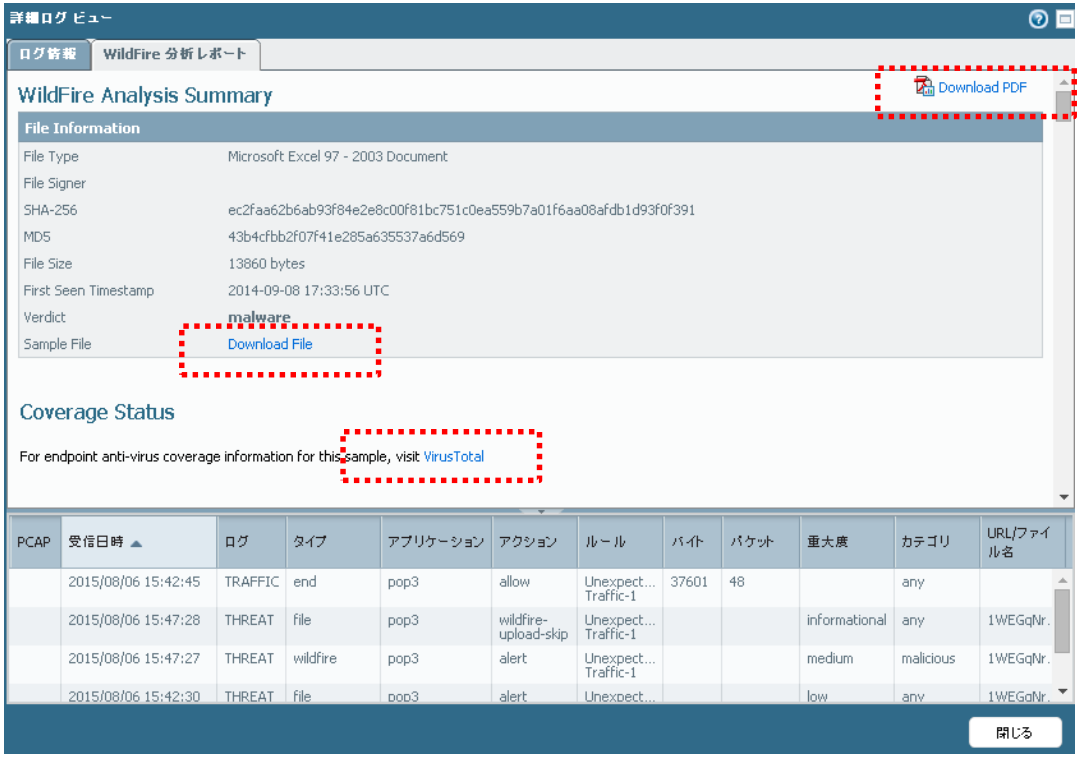
ログの左側にある、虫眼鏡のアイコンをクリックすると、WildFireでの詳細な検査結果が表示されます。



3.通信ログ確認

3-5.WildFireへの送信ログ（続き）

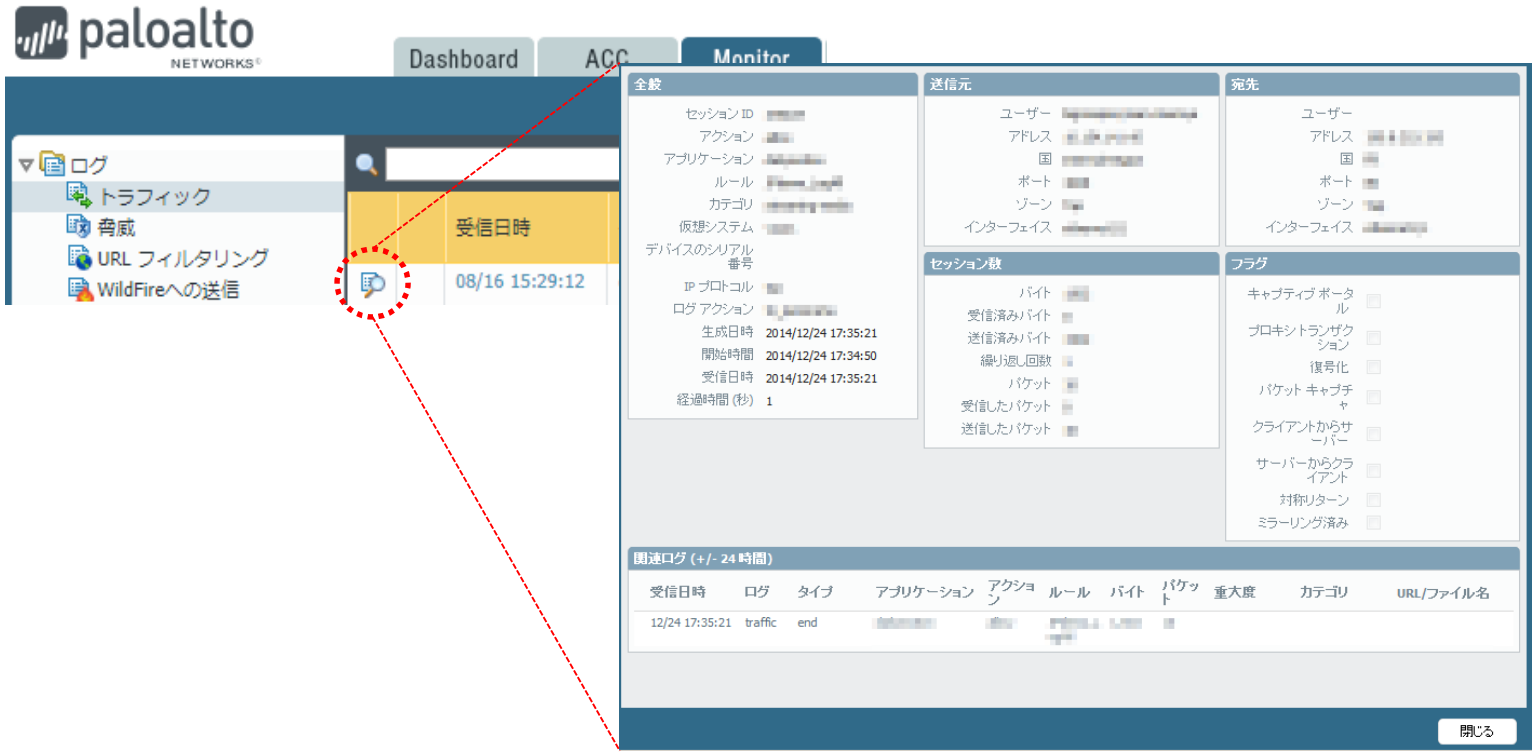
「Download PDF」 からレポートをダウンロードできます。
「Download File」 から解析したマルウェアの検体をダウンロードできます。
「VirusTotal」 のリンクから当該マルウェアに対する、他社セキュリティ製品での検出結果を確認できます。



3.通信ログ確認

3-6.各ログにおける詳細ログ

ログの左側にある、虫眼鏡のアイコンをクリックすると、より詳細なログを参照することができます。
また、下部には関連する他のログが表示されます。



3.通信ログ確認

3-7.ログフィルタ

各種ログを条件でフィルタすることができます。

・フィールドの値をクリックすると条件が追加されます。

↓②検索窓に追加される

←①IPをクリック

・適用ボタンをクリックすると、フィルタがかかります。

3.通信ログ確認

3-7.ログフィルタ（続き）

フィルタの追加メニューから、条件を設定することもできます。

・フィルタ追加ボタンをクリックします。

・条件を入力し、「追加」をクリックします。

・フィルタ適用ボタンをクリックします。条件でフィルタされます。

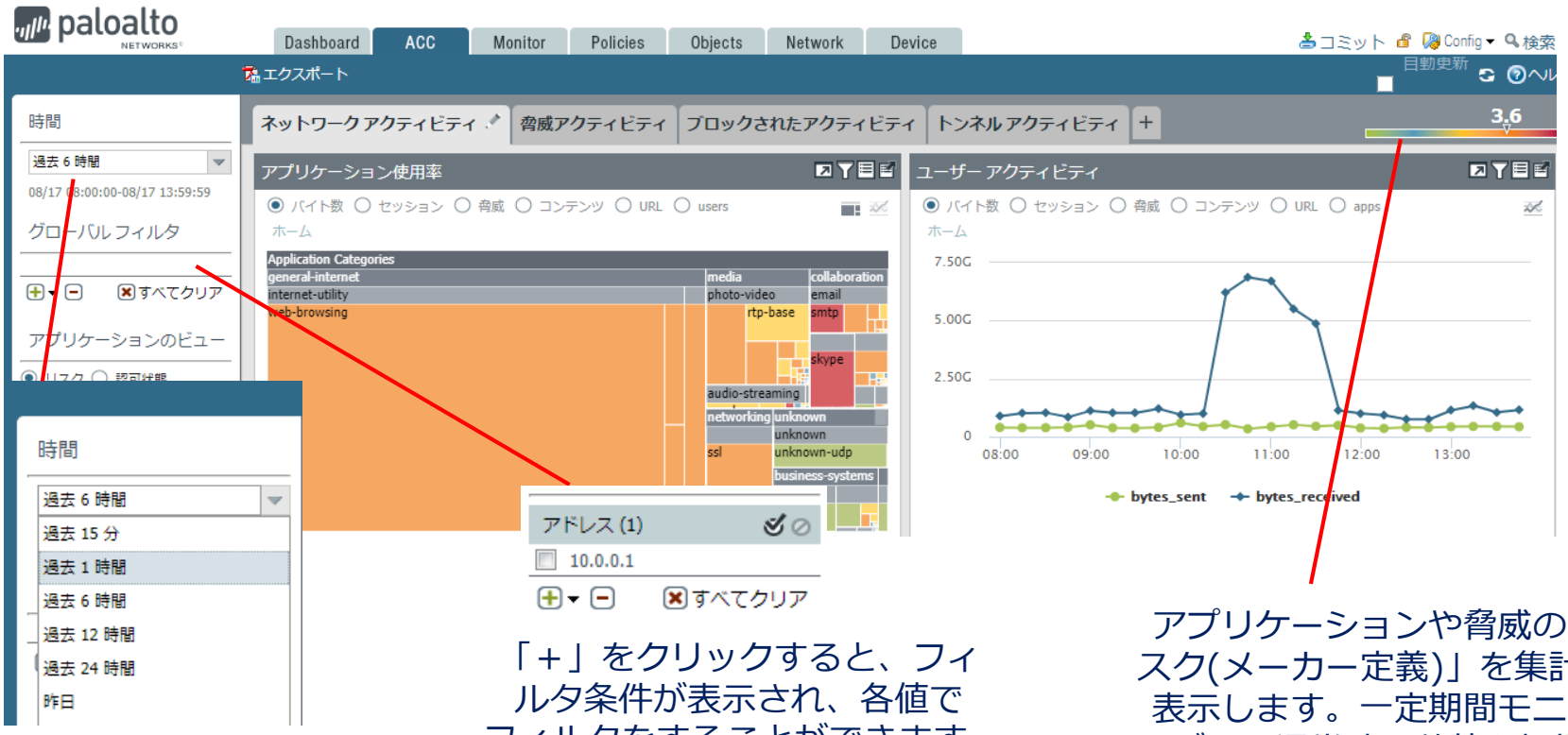
4.モニター・レポート確認

PaloAltoファイアウォールには、ネットワーク上のアプリケーション使用状況や脅威検知状況などを
モニタリングする機能が多数提供されています。
本書では「ACC」、「ボットネットレポート」、「事前定義済みレポート」の確認方法と、
「カスタムレポート」の作成・確認方法を記載します。

4.モニター・レポート確認

4-1.ACC

ACCではネットワーク上のアプリケーション使用状況や、脅威状況について、一定期間の統計を表示します。



表示する期間を指定できます。

「＋」をクリックすると、フィルタ条件が表示され、各値でフィルタをすることができます。

アプリケーションや脅威の「リスク(メーカー定義)」を集計し、表示します。一定期間モニタリングし、通常時の数値を把握し、リスク有無をご判断ください。

4.モニター・レポート確認

4-2.ボットネットレポート

振る舞いベースのメカニズムを使用して、ネットワーク上でマルウェアまたはボットネットに感染した可能性のあるホストをレポートします。毎日午前2時に、過去24時間のログが集計され、結果が表示されます。

・Monitor > ボットネット

Confidence	送信元アドレス	送信元ユーザー	内容
4	10.154.220.146	bigcompany\akikazu.y...	Repeatedly visited (132) the same malicious URL api.yontoo.com/LoadJS.ashx?id=fd5893cd-23de-4179-85da-144fb590c03d&loc=http://www.facebook.com/&apps=twittube,ezLooker,pagerage,buzzdock,toprelatedtopics

上記は、24時間以内に悪意あるURLに132回アクセスしたことを示します。

Confidenceは1～5のスコアが表示されます。
1: 情報、2: 低、3: 中、4: 高、5: 重要

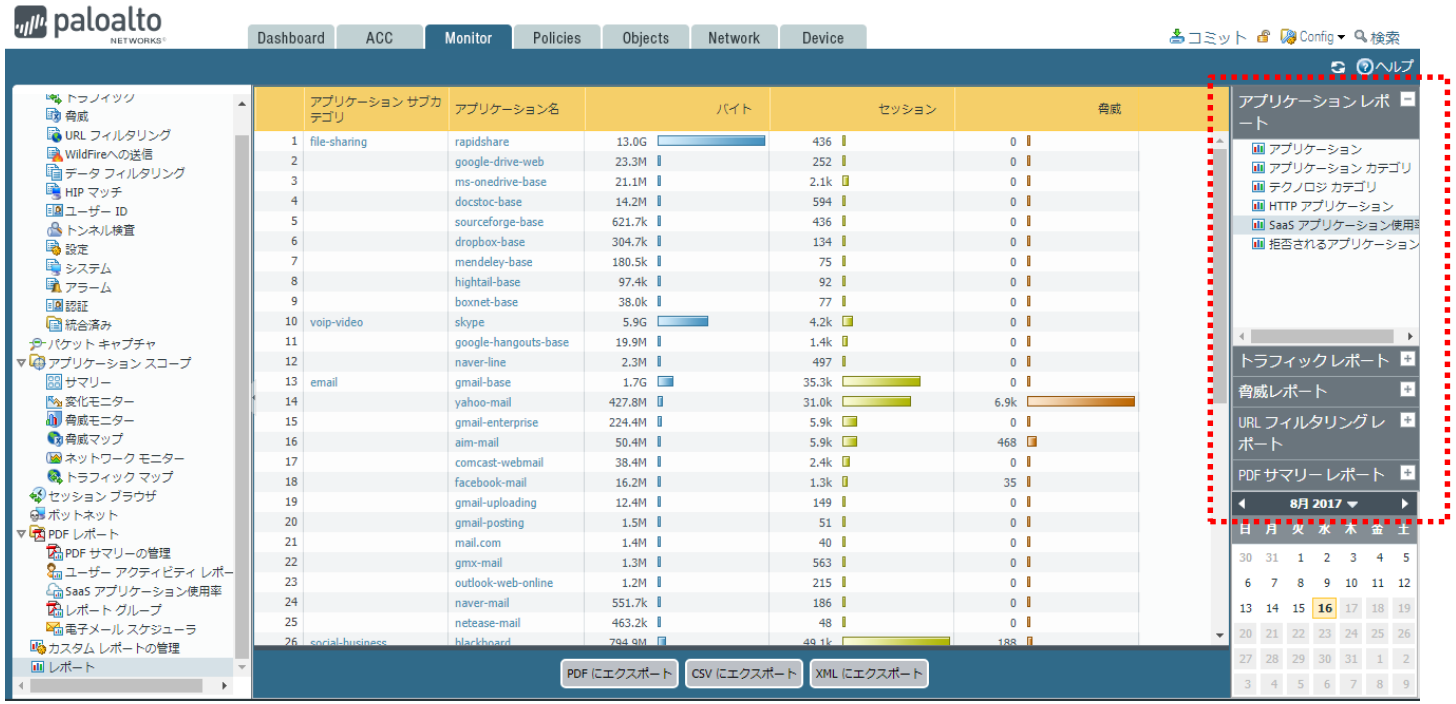
4または5が示された場合は、該当の端末をスキャンしたり、ネットワークから切り離す等、
対処が必要な場合があります。

4.モニター・レポート確認

4-3.事前定義済みレポート

事前定義済みレポートはPaloAltoファイアウォールにデフォルトで作成するよう定義されたレポートで、ネットワーク上のトラフィックのサマリーを簡単に表示できます。
アプリケーション、トラフィック、脅威、および URL フィルタリングの4つのカテゴリがあります。

・Monitor > レポート をクリックし、右側の一覧から、閲覧したいレポートを選択します。



4.モニター・レポート確認

4-4. カスタムレポート

分析する情報の属性や重要な項目について、目的に合ったレポートを生成することもできます。
レポート作成手順を記載します。

・Monitor > カスタムレポートの管理 > 追加(左下) をクリックします。

4.モニター・レポート確認

4-4. カスタムレポート（続き）

・カスタムレポート作成画面にて、各パラメータを設定します。

データベース
- サマリーデータベース
  レポート生成時の応答時間を高速化できるよう、各詳細ログを集約したものです。
- 詳細ログ
  すべてのログエントリを選択することができます。サマリーに含まれない属性や列を表示する必要がある場合に使用します。

期間
  レポート化する時間の範囲指定を指定します。

スケジュール設定
  チェックをすると、毎日AM2:00に「期間」で指定された範囲のレポートを自動生成します。

ソート基準/グループ化基準
  選択された属性により、データをソートまたはグループ化したうえで、表示します。

4.モニター・レポート確認

4-4. カスタムレポート（続き）

スケジュール設定

チェックをすると、毎日AM2:00に「期間」で指定された範囲のレポートを自動生成します。
生成されたレポートは Monitor > レポート の右側のメニュー「カスタムレポート」に保存されます。

今すぐ実行

指定のレポートが即時出力されます。

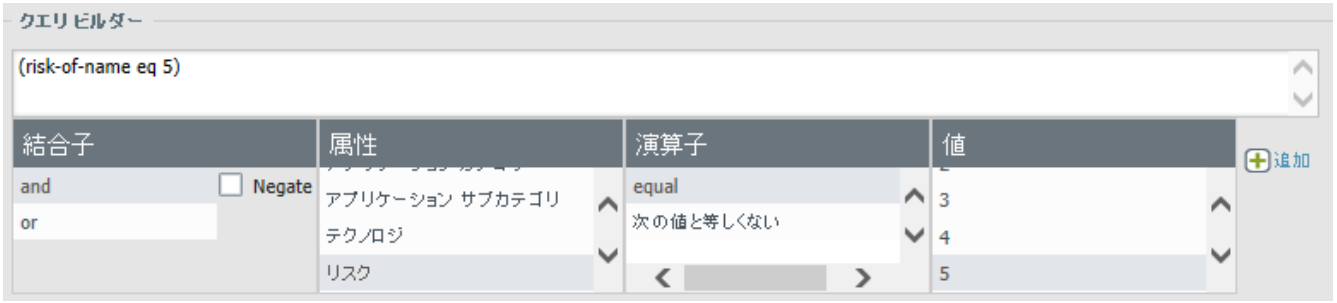
テンプレートのロード

予め機器内に設定されたテンプレートをロードし、必要に応じカスタマイズして使用することも可能です。

4.モニター・レポート確認

4-4. カスタムレポート（続き）

使用可能な列/選択した列
　レポートに表示する項目です。
　データベースにより選択できる項目が変わります。

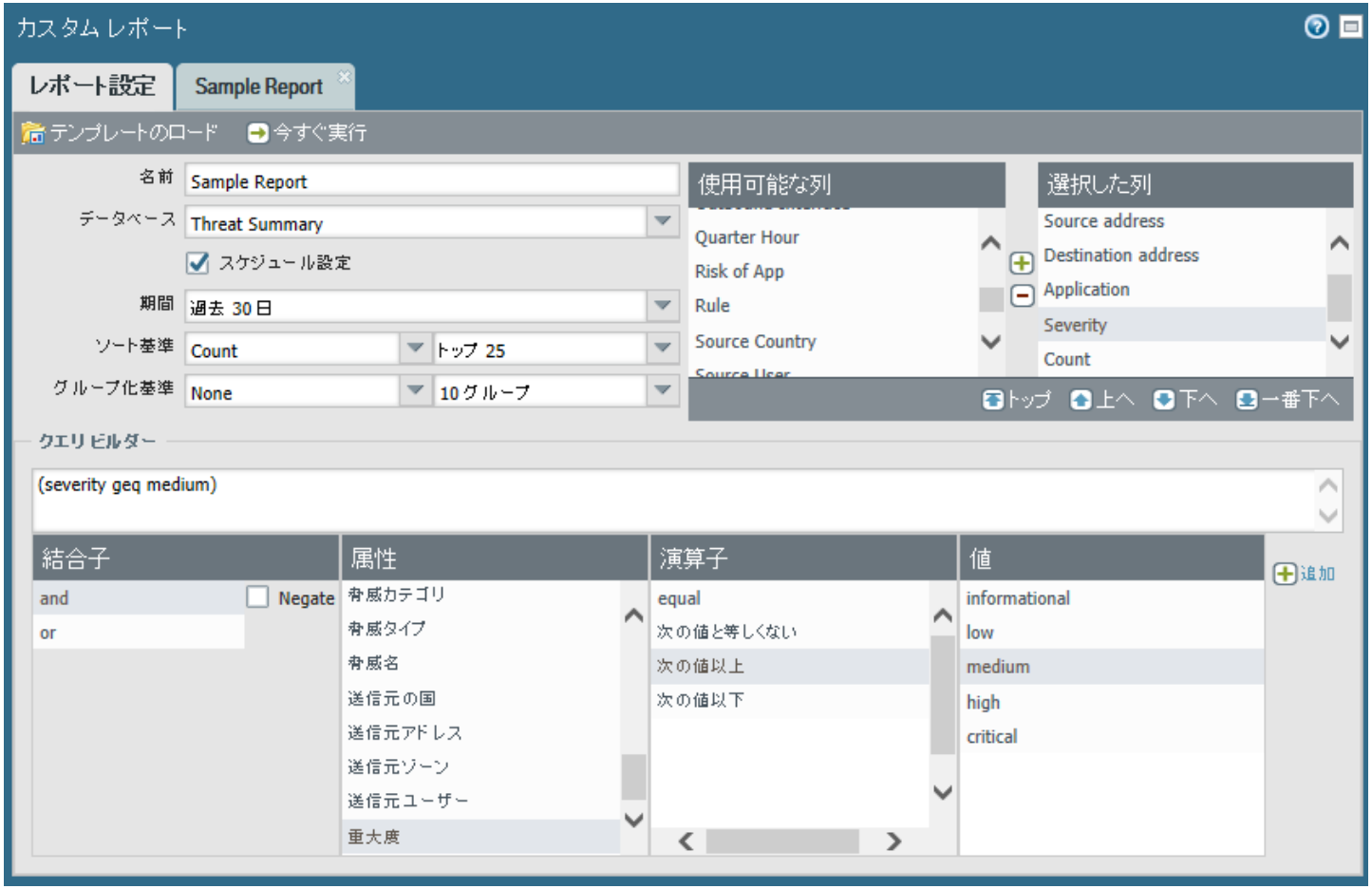


クエリビルダー
　特定のクエリを定義して、選択した属性をさらに絞り込むことができます。and および or 演算子を使用してレポートで必要なもののみを表示し、次に、レポートのクエリに適合する、またはクエリを否定するデータを含めたり除外したりできます。

4.モニター・レポート確認

4-4. カスタムレポート（続き）

・設定値を確認し、「今すぐ実行」をクリックするとレポートが出力されます。



4.モニター・レポート確認

4-4. カスタムレポート（続き）

出力イメージです。


カスタム レポート

レポート設定 | Sample Report

	脅威/コンテンツ名	ID	攻撃者	送信元のホスト名	被害者	宛先ホスト名	アプリケーション	重大度	カウント
1	FTP: login Brute Force attempt	40001	61.136.188.83	61.136.188.83	10.154.2.26	10.154.2.26	ftp	high	343.0k
2	FTP: login Brute Force attempt	40001	61.136.188.83	61.136.188.83	10.154.14.37	10.154.14.37	ftp	high	34.9k
3	Trojan-Virtumondo.Phonehome	19862	82.98.235.78	82.98.235.78	10.154.2.217	10.154.2.217	web-browsing	high	16.5k
4	My Amazon Signature	41154	10.154.213.17	10.154.213.17	64.94.107.18	pixel.quantserve.com	web-browsing	high	14.7k
5	Worm.rimecud:butterfly.bigmo...	3811163	10.154.1.5	10.154.1.5	204.16.173.31	ns1.changeip.org	dns	medium	12.7k
6	My Amazon Signature	41154	10.154.9.118	10.154.9.118	64.236.79.53	64.236.79.53	web-browsing	high	10.6k
7	Worm.rimecud:butterfly.bigmo...	3811163	10.154.1.5	10.154.1.5	204.16.175.12	ns2.changeip.org	dns	medium	9.8k
8	Worm.rimecud:butterfly.bigmo...	3811163	10.154.1.5	10.154.1.5	204.16.173.33	ns3.changeip.org	dns	medium	8.4k
9	My Amazon Signature	41154	10.154.227.49	10.154.227.49	184.85.52.46	a184-85-52-46.deploy.static.akamait	web-browsing	high	6.6k
10	My Amazon Signature	41154	10.154.14.124	10.154.14.124	64.94.107.22	pixel.quantserve.com	web-browsing	high	5.7k
11	My Amazon Signature	41154	10.154.111.193	10.154.111.193	50.17.185.151	ec2-50-17-185-151.compute-1.amazonaws.com	web-browsing	high	5.7k
12	My Amazon Signature	41154	10.154.11.177	10.154.11.177	198.189.255.75	198.189.255.75	facebook-base	high	5.3k
13	My Amazon Signature	41154	10.154.14.124	10.154.14.124	64.236.79.53	64.236.79.53	web-browsing	high	5.2k
14	Bot: Mariposa Command and Control	12652	87.106.179.75	mail.ce3formacion...	10.154.6.197	10.154.6.197	unknown-udp	critical	4.8k

5.復号化除外（一部サイトの除外）設定

RICOH
imagine. change.

5-1.復号化除外が必要なサイトを登録します。

・Device > 証明書の管理 > SSL復号化例外 > [追加]

5.復号化除外（一部サイトの除外）設定

5-1.復号化除外が必要なサイトを登録します。（続き）

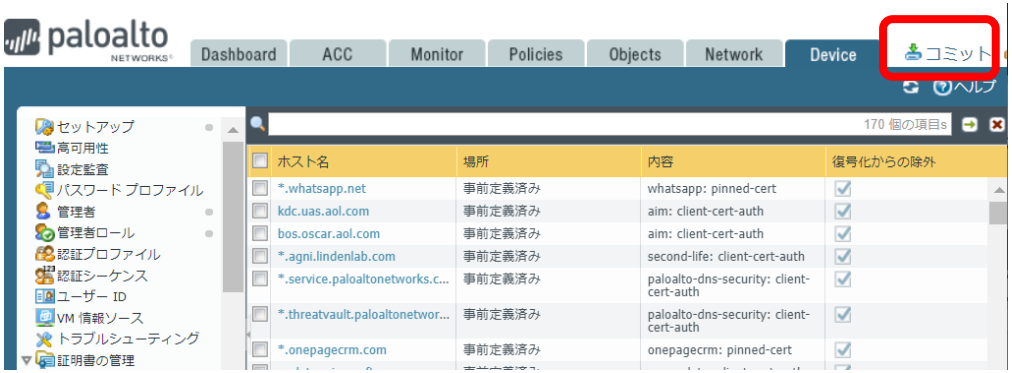
・SSL復号サイトの情報を[ホスト名]欄に入力し、除外のチェックボックスにチェックを入れ[OK]をクリックします

例1

例2

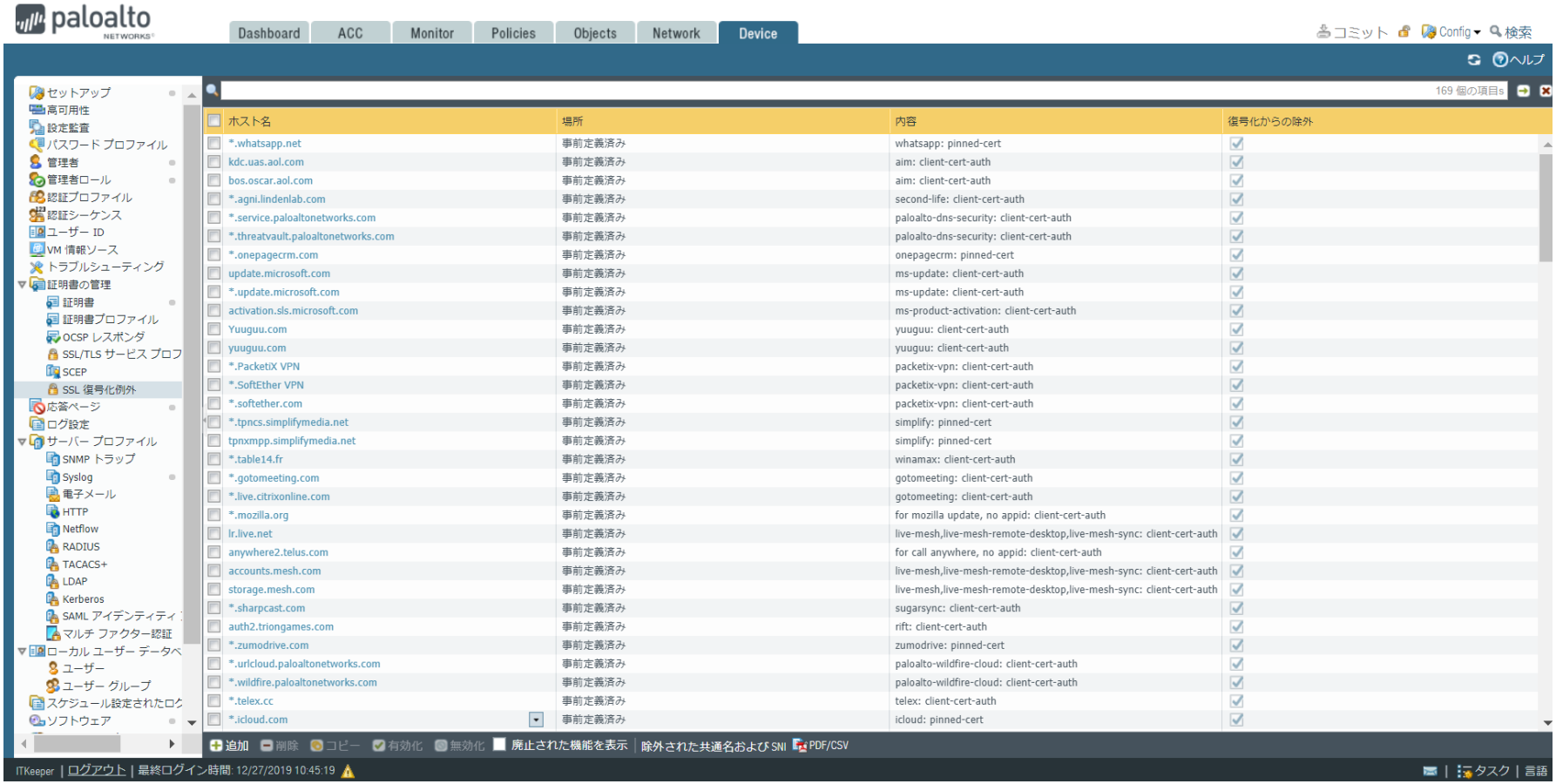
※ワイルドカード“ * ”を使用することが可能です

・コミットを実行し、設定を反映させます。



5.復号化除外（一部サイトの除外）設定

※復号化することで通信が失敗するなど何らかの不具合があることが分かっているサイトは既に登録されています。

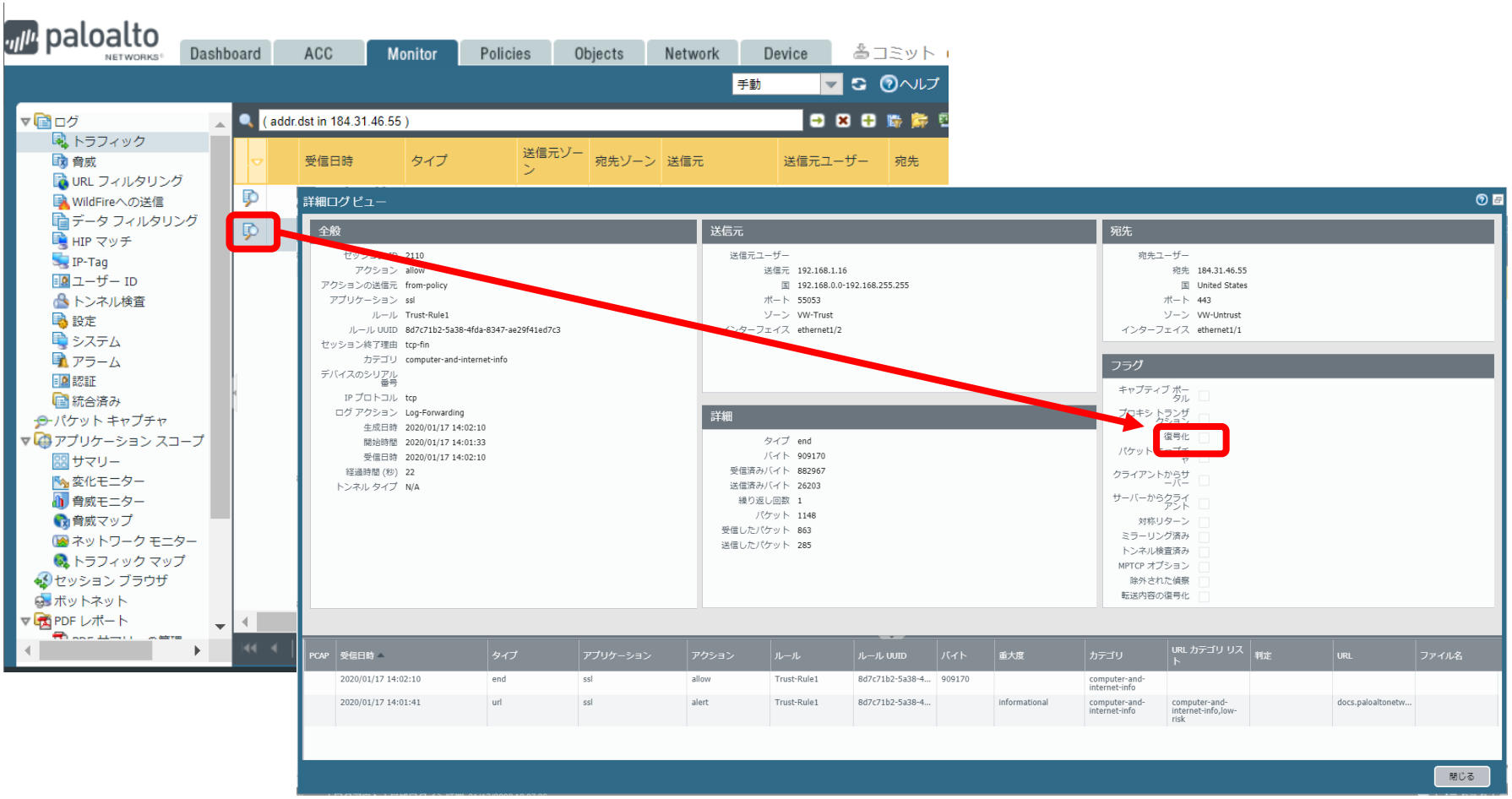


5.復号化除外（一部サイトの除外）設定

5-1.復号化除外が必要なサイトを登録します。（続き）

対象サイトが復号化されないことを確認（WEB-GUI）

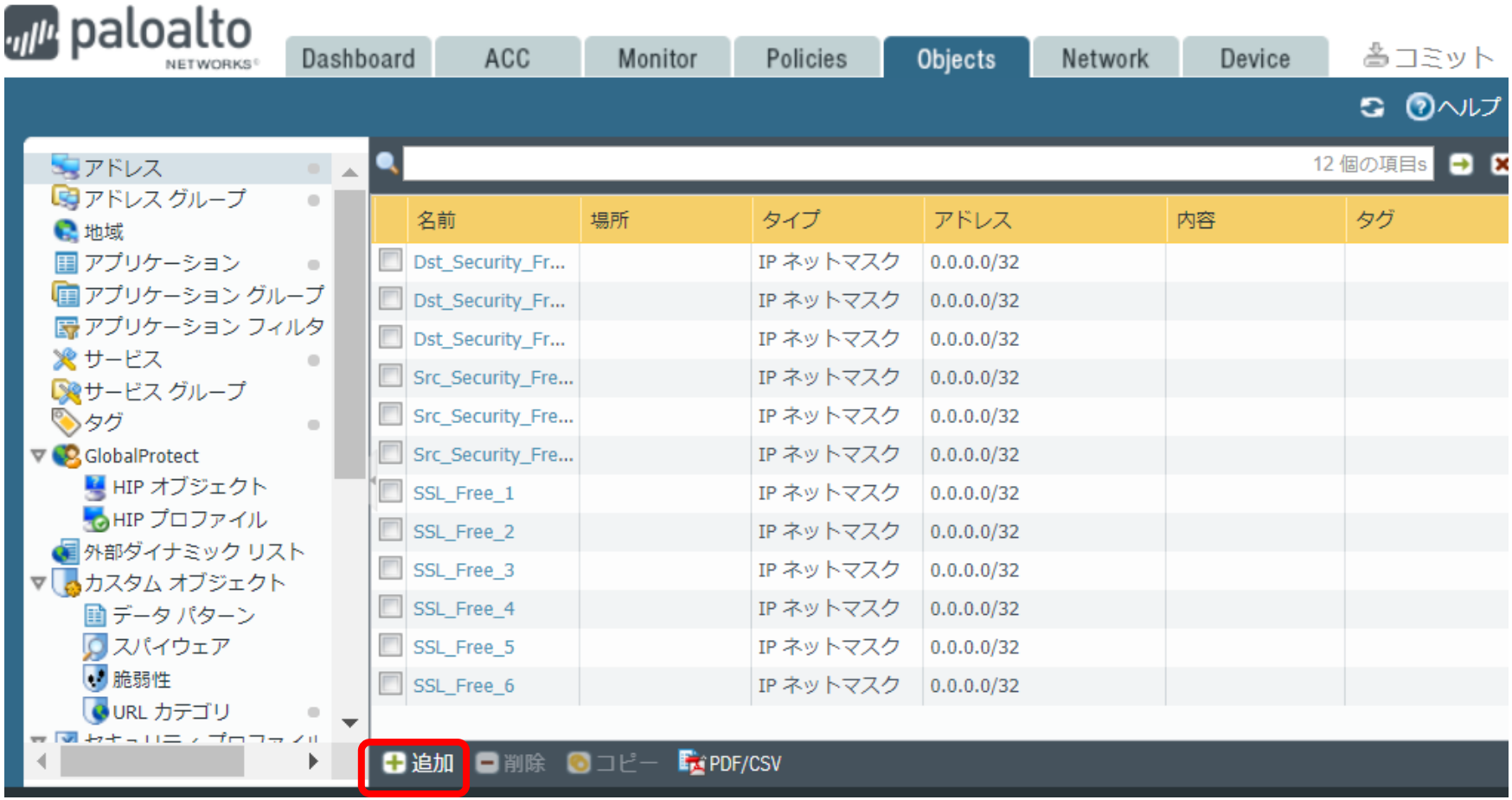
・Monitor > ログ > トラフィック　より該当の通信をクリックし、復号化にチェックが入っていないことを確認できます。



5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。

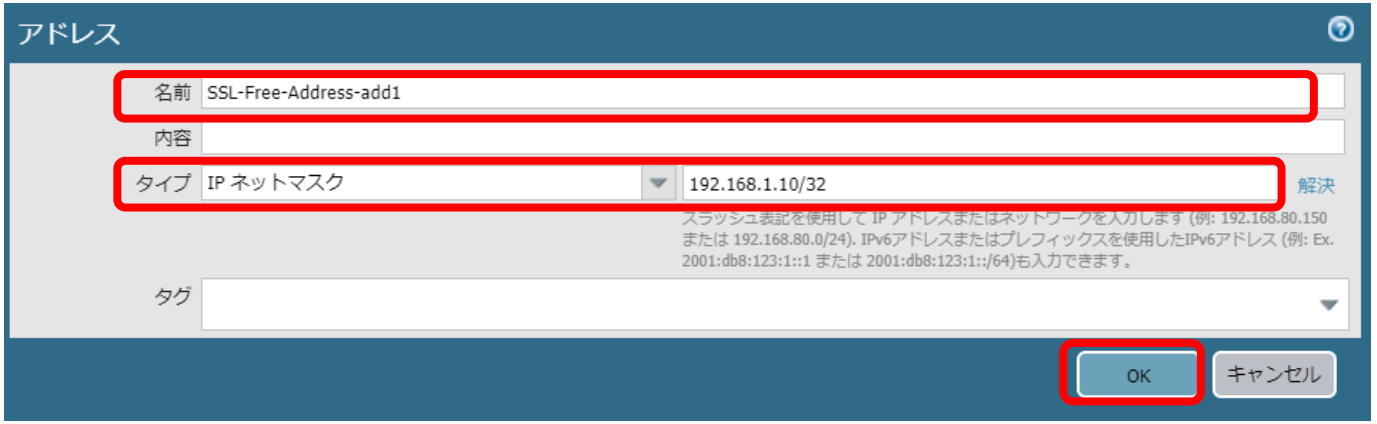
・Object > アドレス > [追加]



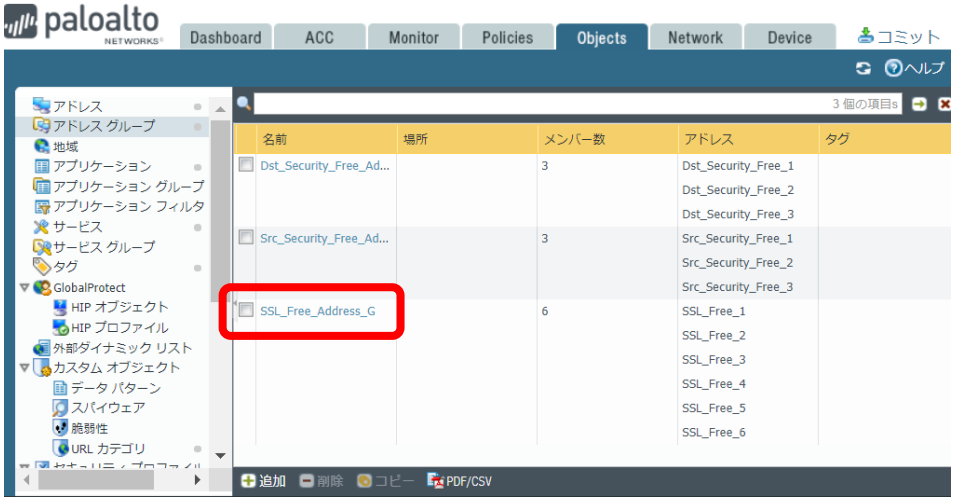
5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

・任意の名前、該当のIPアドレスを入力し、[OK]をクリックします。



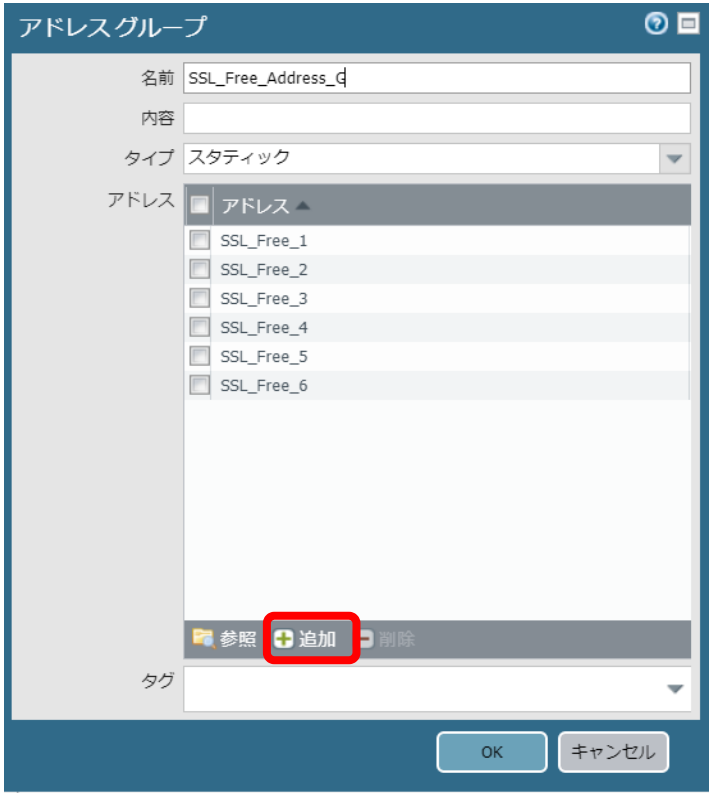
・Object > アドレスグループ にて 「SSL_Free_Address_G」をクリックします。

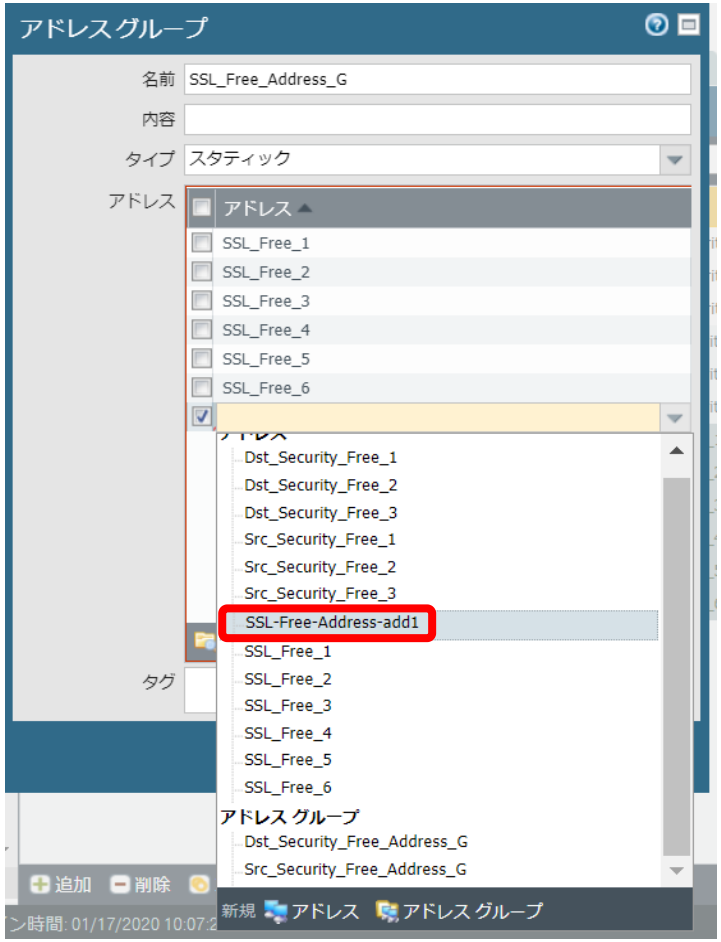


5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

・[追加]をクリックし、先ほど作成したアドレスオブジェクトを選択します。





5.復号化除外（一部ユーザーの除外）設定

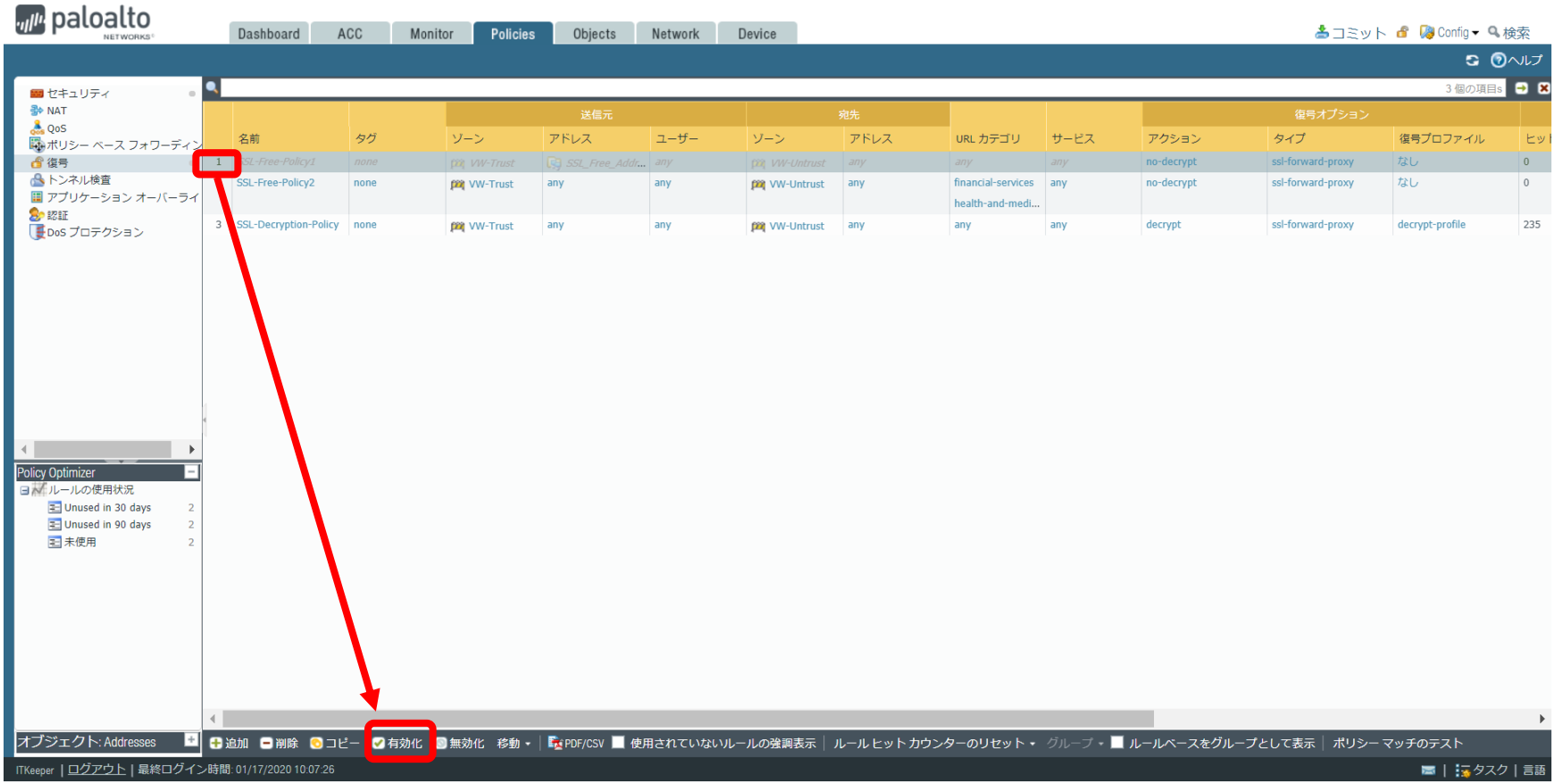
5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

・追加されたことを確認し、[OK]をクリックします。

5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

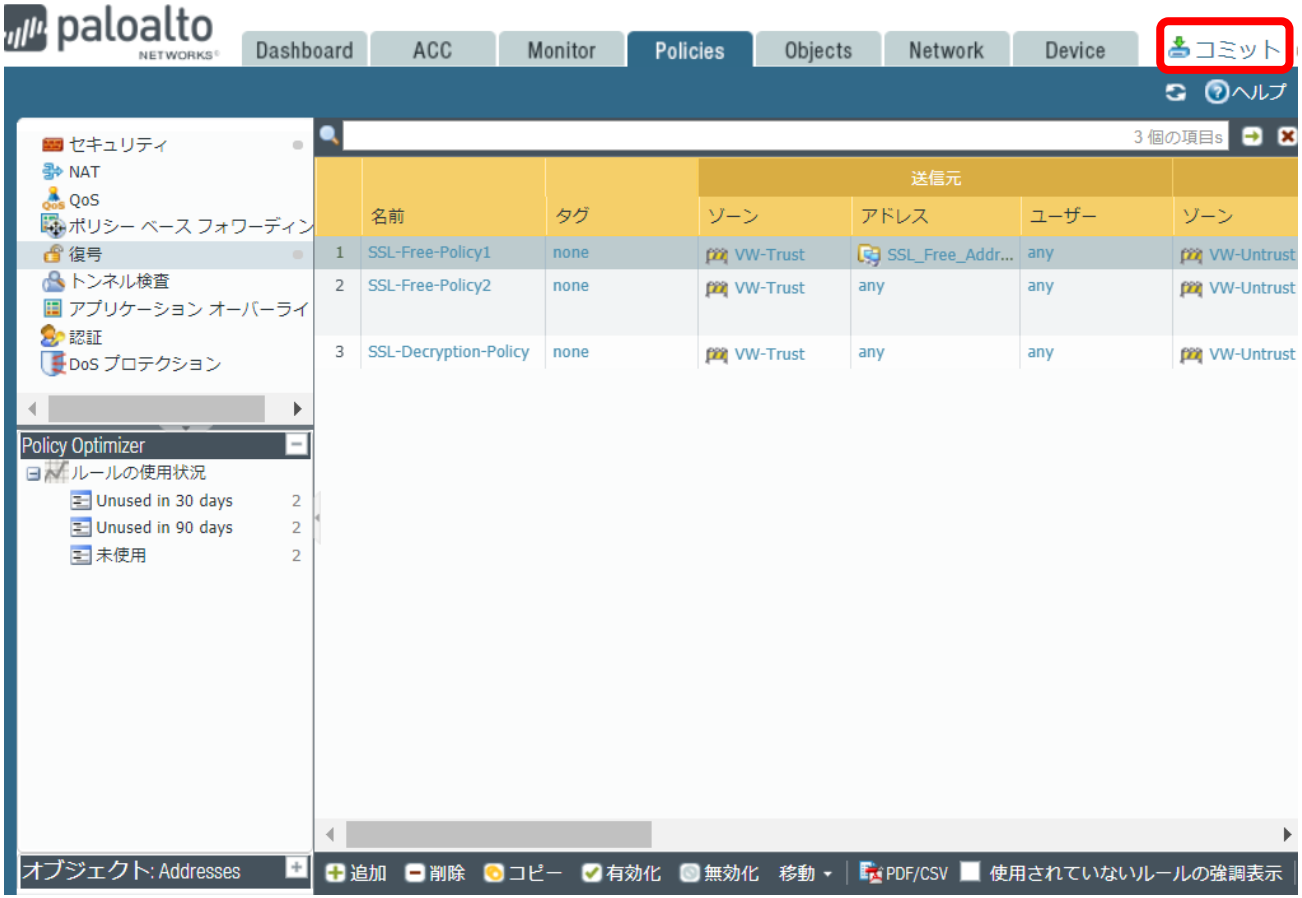
・Policies > 復号 にて、「SSL-Free Policy1」を有効化します。
　(既に有効化済の場合はスキップしてください)



5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

・コミットを実行し、設定を反映させます

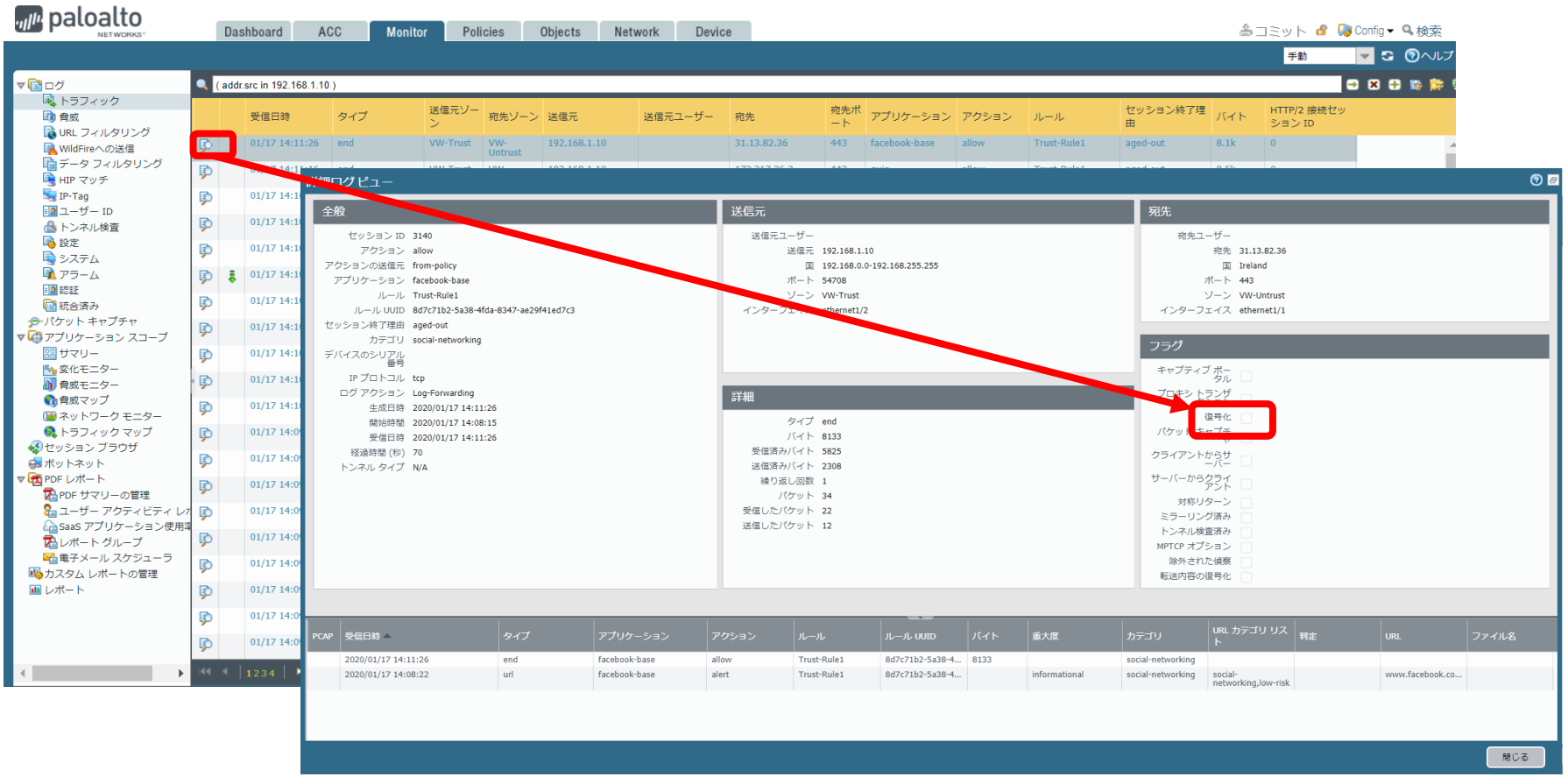


5.復号化除外（一部ユーザーの除外）設定

5-2.復号化除外が必要なユーザーのIPアドレスを登録します。（続き）

対象サイトが復号化されないことを確認（WEB-GUI)

・Monitor > ログ > トラフィック　より該当の通信をクリックし、復号化にチェックが入っていないことを確認できます。

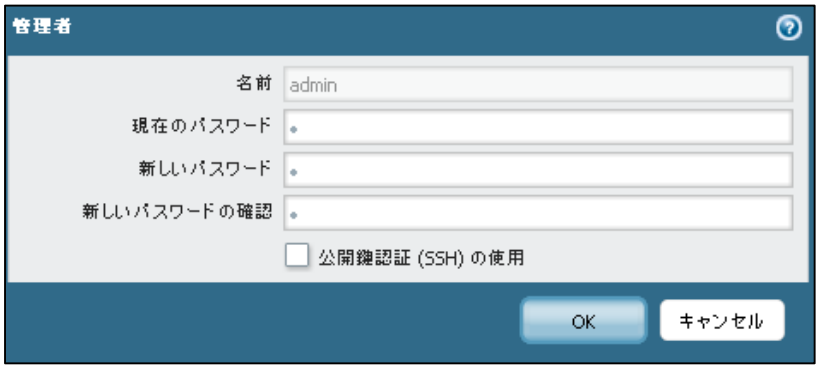


6.管理者パスワード変更

6-1.管理者パスワード変更

・Device > 管理者 を選択し、パスワードを変更するユーザ名をクリックします。

・現在のパスワードと新しいパスワードをそれぞれ入力し、OKをクリックします。

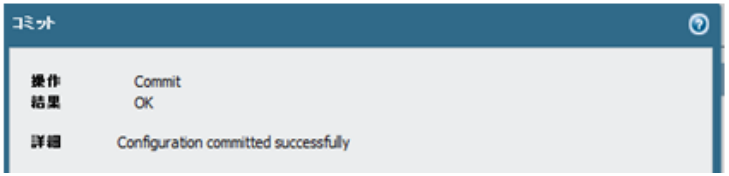


6.管理者パスワード変更

6-1.管理者パスワード変更（続き）

・コミット を実行します。

・結果が successfully となるのを確認します。



7.起動・停止・再起動

7-1.起動

・電源ケーブルを挿します。
　※電源ボタンはありません。

7.起動・停止・再起動

7-2.停止

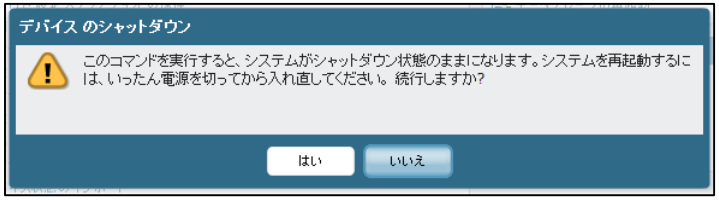
停止時は、PAファイアウォールの管理画面でシャットダウンします。

・Device > セットアップ > 操作 をクリックします。
・「デバイスのシャットダウン」をクリックします。

7.起動・停止・再起動

7-2.停止（続き）

・確認メッセージが表示されるので、「はい」をクリックします。



・「はい」をクリックすると、システムが停止します。

7.起動・停止・再起動

7-3.再起動

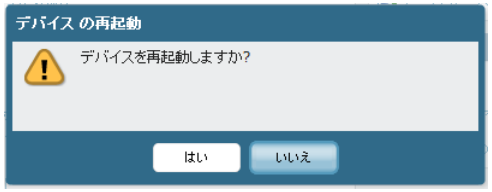
・Device > セットアップ > 操作 をクリックします。

・「デバイスの再起動」をクリックします。

7.起動・停止・再起動

7-3.再起動（続き）

・確認メッセージが表示されるので、「はい」をクリックします。



・前面LEDの「STS(ステータス)」が緑色に点灯することを確認します。
オレンジ色の場合は、AutoCommit（起動処理）実行中となります。

・管理コンソールにて、AutoCommitが正常に完了していること(結果がFIN OKであること)
を確認します。

8.商標

- GoogleおよびGoogle Chrome™ ブラウザはGoogle Inc.の商標です。
- Microsoft、Windows、Internet Explorer は、米国Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- Windows 10の製品名は以下のとおりです。
  Microsoft® Windows® 10 Home
  Microsoft® Windows® 10 Pro
  Microsoft® Windows® 10 Enterprise
- その他の製品名、名称は各社の商標または登録商標です。

9.改訂履歴

本マニュアルは最終改定日現在の情報をもとに作成しております

Version	発行日・改定日	更新内容
1.0	2020年1月24日	初版作成

RICOH

imagine. change.