

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.

- 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製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。

1. 管理アクセス
 - 1-1. WebUIアクセス
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
 - 2-2. システムログ確認 – WebUI
3. 通信ログ確認
 - 3-1. ログの種類
 - 3-2. トラフィックログ
 - 3-3. 脅威ログ
 - 3-4. URLフィルタリングログ
 - 3-5. WildFireへの送信ログ
 - 3-6. 各ログにおける詳細ログ
 - 3-7. ログフィルタ
4. モニター・レポート確認
 - 4-1. ACC
 - 4-2. ボットネットレポート
 - 4-3. 事前定義済みレポート
 - 4-4. カスタムレポート

- 5. 復号化除外設定
 - 5-1.復号化除外(一部サイトの除外)設定
 - 5-2.復号化除外(一部ユーザーの除外)設定
- 6. 設定者パスワード変更
 - 6-1.管理者パスワード変更
- 7. 起動・停止・再起動
 - 7-1.起動
 - 7-2.停止
 - 7-3.再起動
- 8.商標
- 9.改訂履歴

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。



1-1.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。

The screenshot displays the Palo Alto Networks management interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The main content area is divided into several sections:

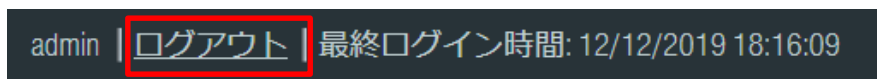
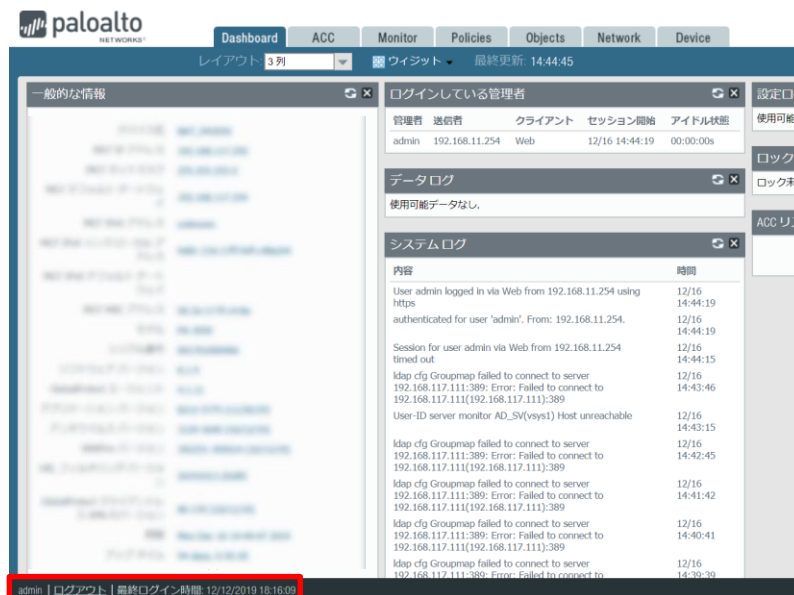
- 一般的な情報 (General Information):** Lists device details for VM-1, including MGT IP address (255.255.255.0), MGT MAC address (06:1b:26:1e:87:bc), and model (PA-VM).
- インターフェイス (Interfaces):** Shows a grid of interface status icons.
- ログインしている管理者 (Active Administrators):** A table showing active sessions for the 'admin' user.
- データログ (Data Log):** Displays a message: "使用可能データなし。" (No usable data).
- システムログ (System Log):** A log table with columns for content and time, showing connection and update-related events.

管理者	送信者	クライアント	セッション開始	アイドル状態
admin	10.201.100.28	Web	04/16 11:43:15	00:00:00s
admin	10.201.100.28	Web	04/16 11:43:14	00:53:18s

内容	時間
Connection to Update server closed: updates.paloaltonetworks.com, source: None	04/16 12:36:02
Cloud is not ready, There was no update from the cloud in the last 55 minutes.	04/16 12:34:57
Failed to perform task multiple times resulting in connection timeout with WildFire Cloud wildfire.paloaltonetworks.com	04/16 12:34:14
Failed to perform task resulting in connection timeout with WildFire Cloud wildfire.paloaltonetworks.com	04/16 12:32:13
Connection to Update server closed: updates.paloaltonetworks.com, source: None	04/16 12:31:02
Failed to perform task resulting in connection timeout with WildFire Cloud wildfire.paloaltonetworks.com	04/16 12:30:13

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。



2-1. 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。

The screenshot shows the Palo Alto Networks WebUI dashboard. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The main content area is divided into several sections, each with a red circle and a number indicating its location:

- ① 一般的な情報 (General Information): Lists device details such as 'デバイス名' (Kachidoki-PA3050-1), 'MGT IP アドレス' (10.194.120.234), 'MGT ネットマスク' (255.255.255.252), 'MGT デフォルトゲートウェイ' (10.194.120.233), 'MGT IPv6 アドレス' (unknown), 'MGT IPv6 リンクローカルアドレス' (fe80::21b:17ff:feff:c48a/64), 'MGT IPv6 デフォルトゲートウェイ' (00:1b:17ff:c4:8a), 'MGT MAC アドレス' (00:1b:17ff:c4:8a), 'モデル' (PA-3050), 'シリアル番号' (001701000466), 'ソフトウェアバージョン' (7.1.9), 'GlobalProtect エージェント' (0.0.0), 'アプリケーションバージョン' (725-4172 (08/16/17)), and '脅威バージョン' (725-4172 (08/16/17)).
- ② システムリソース (System Resources): Displays resource usage including '管理 CPU' (7%), 'データプレーン CPU' (0%), and 'セッション数' (16 / 524286).
- ③ 高可用性 (High Availability): Shows 'HA 無効' (HA Disabled).
- ④ インターフェイス (Interfaces): A grid of interface status icons, with green icons indicating an 'アップリンク状態' (uplink state).
- ⑤ システムログ (System Log): Shows a log entry: 'Syslog connection failed to server[AF_INET.10.195.66.34:514.]' on 08/21 at 16:15:53.

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。

2-2. 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



The screenshot shows the Palo Alto Networks web interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Monitor' tab is active. On the left, a sidebar menu shows various log categories, with 'システム' (System) selected. The main area displays a table of system logs.

受信日時	タイプ	重大度	イベント	オブジェクト	内容
08/15 20:53:26	general	informational	general		User admin accessed Monitor tab
08/15 19:33:15	general	medium	general		Failed password for admin from 5
08/15 19:33:15	general	medium	general		Failed password for admin from 5
08/15 19:33:15	general	medium	general		Failed password for admin from 1:
08/15 19:33:02	auth	medium	auth-fail		failed authentication for user 'adm
08/15 19:32:59	auth	medium	auth-fail		failed authentication for user 'adm
08/15 19:32:55	auth	medium	auth-fail		failed authentication for user 'adm
08/15 19:27:01	general	informational	general		User admin logged in via Web fro
08/15 19:27:01	auth	informational	auth-success		authenticated for user 'admin'. Fr
08/15 19:26:52	general	informational	general		Session for user admin via Web fr
08/15 19:26:52	general	informational	general		Session for user admin via Web fr

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。

3-2.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

3-3.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

3-3.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があります。
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る、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。

3-4.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がカテゴリ化される、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

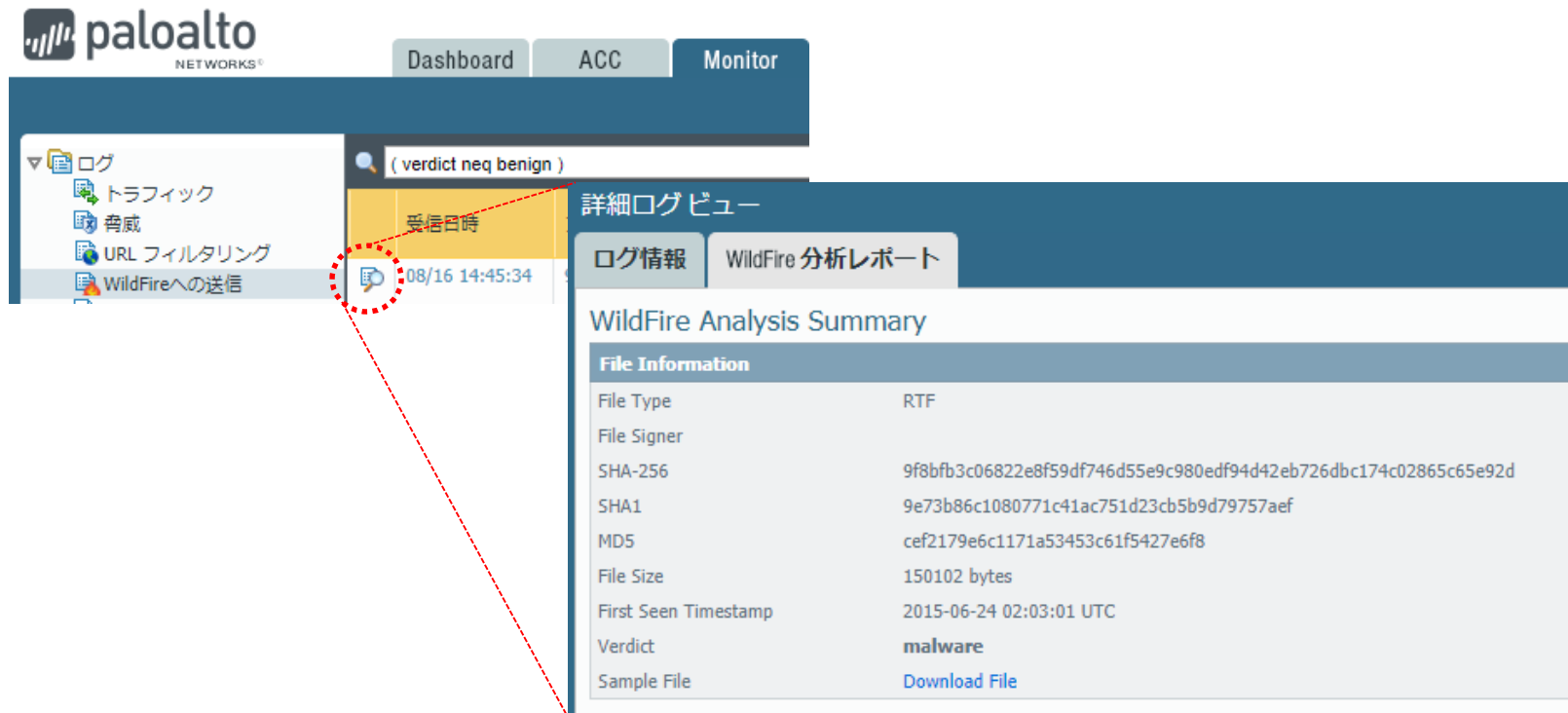
3-5.WildFireへの送信ログ

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がカテゴリ化される、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

3-5.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。



The screenshot shows the Palo Alto Networks WildFire interface. On the left, a navigation menu includes 'ログ' (Logs) with sub-items: 'トラフィック' (Traffic), '脅威' (Threats), 'URL フィルタリング' (URL Filtering), and 'WildFireへの送信' (Send to WildFire). A log entry is selected, showing a magnifying glass icon and the timestamp '08/16 14:45:34'. The main panel displays the '詳細ログビュー' (Detailed Log View) for this entry, with tabs for 'ログ情報' (Log Information) and 'WildFire 分析レポート' (WildFire Analysis Report). The analysis report is expanded, showing a 'WildFire Analysis Summary' table.

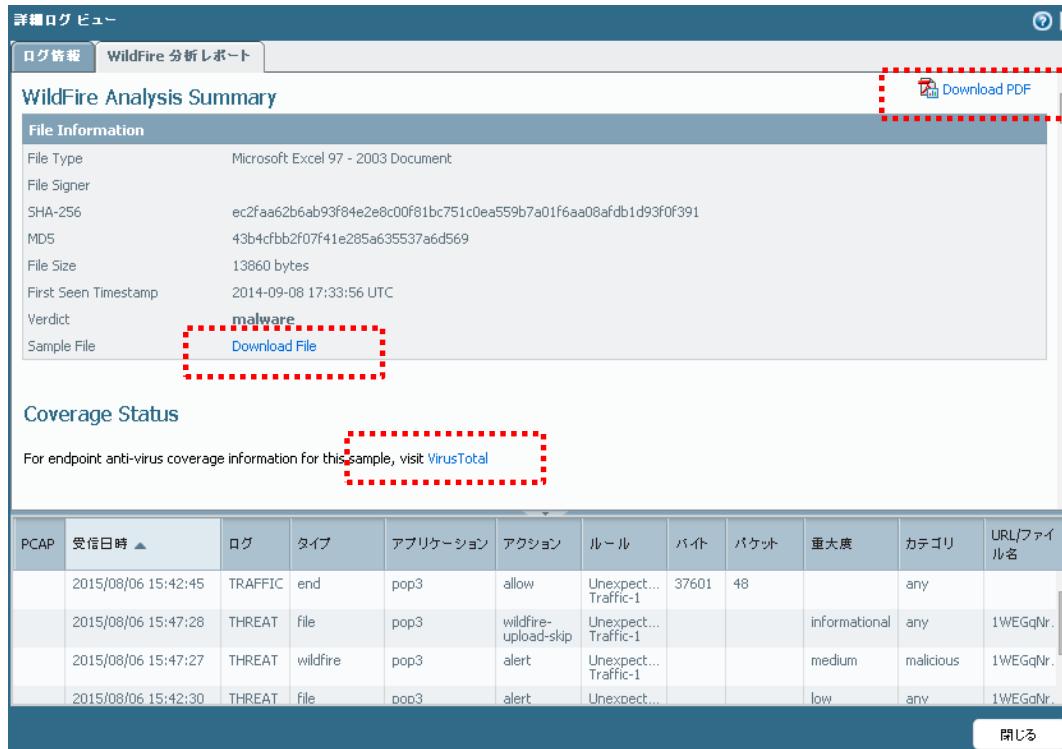
File Information	
File Type	RTF
File Signer	
SHA-256	9f8bfb3c06822e8f59df746d55e9c980edf94d42eb726dbc174c02865c65e92d
SHA1	9e73b86c1080771c41ac751d23cb5b9d79757aef
MDS	cef2179e6c1171a53453c61f5427e6f8
File Size	150102 bytes
First Seen Timestamp	2015-06-24 02:03:01 UTC
Verdict	malware
Sample File	Download File

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。

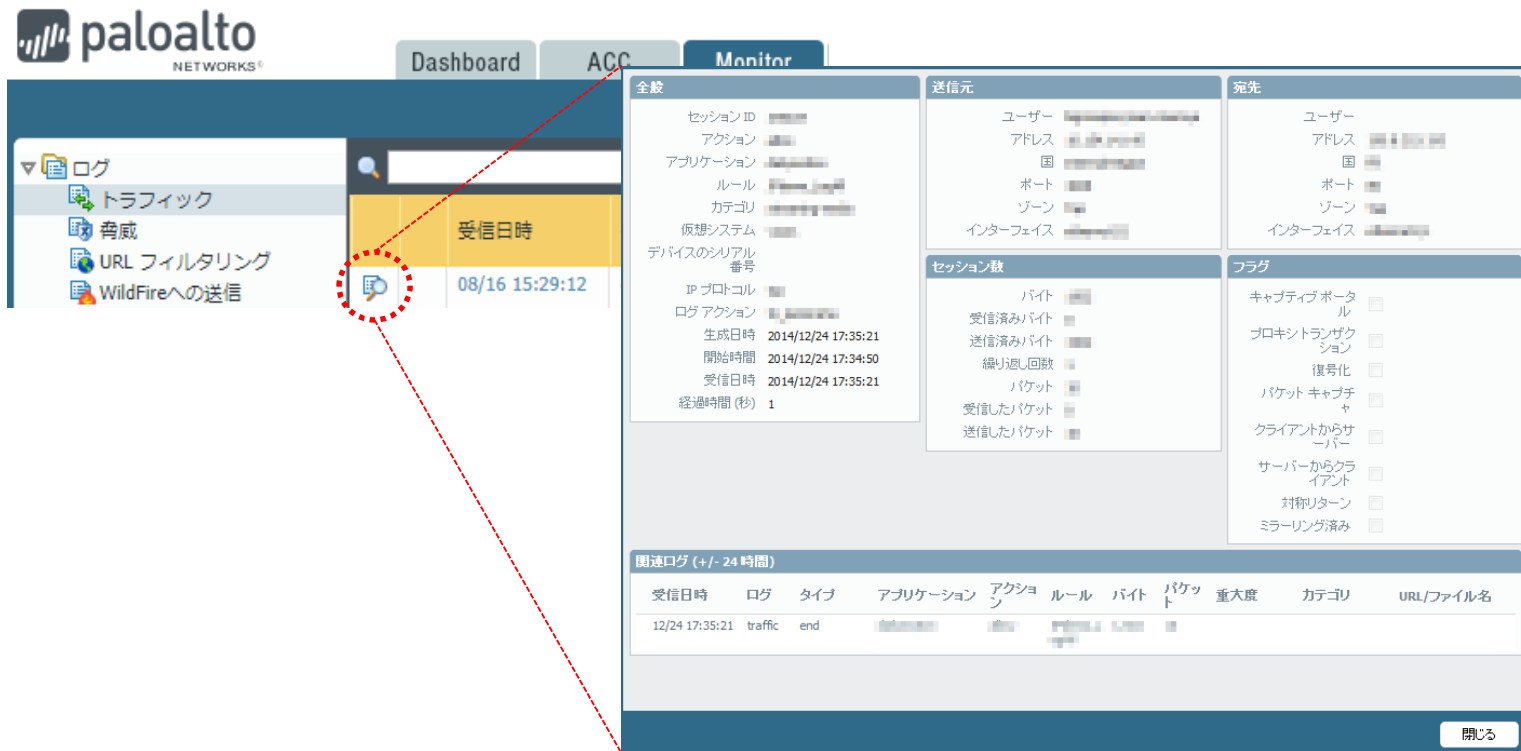


The screenshot shows the WildFire Analysis Summary page. It includes a 'Download PDF' button, a 'Download File' button, and a link to VirusTotal. Below is a table of PCAP logs.

PCAP	受信日時 ▲	ログ	タイプ	アプリケーション	アクション	ルール	バイト	パケット	重大度	カテゴリ	URL/ファイル名
	2015/08/06 15:42:45	TRAFFIC	end	pop3	allow	Unexpect... Traffic-1	37601	48		any	
	2015/08/06 15:47:28	THREAT	file	pop3	wildfire- upload-skip	Unexpect... Traffic-1			informational	any	1WEGqNr.
	2015/08/06 15:47:27	THREAT	wildfire	pop3	alert	Unexpect... Traffic-1			medium	malicious	1WEGqNr.
	2015/08/06 15:42:30	THREAT	file	pop3	alert	Unexpect...			low	any	1WEGqNr.

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。



The screenshot shows the Palo Alto Networks GUI. On the left, the 'Log' menu is expanded, showing options like 'Traffic', 'Policies', 'URL Filtering', and 'Send to WildFire'. A magnifying glass icon is highlighted with a red dashed circle. The main content area displays a detailed log entry for '08/16 15:29:12'. The log details are organized into several sections:

- 全般 (General):** Includes fields for Session ID, Action, Application, Rule, Category, Policy System, Device Serial Number, IP Protocol, Log Action, Creation Time (2014/12/24 17:35:21), Start Time (2014/12/24 17:34:50), Receipt Time (2014/12/24 17:35:21), and Duration (1 second).
- 送信元 (Source):** Includes fields for User, Address, Country, Port, Zone, and Interface.
- 宛先 (Destination):** Includes fields for User, Address, Country, Port, Zone, and Interface.
- セッション数 (Session Count):** Includes fields for Bytes, Received Bytes, Sent Bytes, Retransmissions, Packets, Received Packets, and Sent Packets.
- フラグ (Flags):** Includes checkboxes for Captive Portal, Proxy Bypass, Reassembly, Packet Capture, Client-to-Server, Server-to-Client, Symmetric Return, and Mirroring.

At the bottom, there is a section for '関連ログ (+/- 24 時間)' (Related Logs +/- 24 hours) with a table of log entries:

受信日時	ログ	タイプ	アプリケーション	アクション	ルール	バイト	パケット	重大度	カテゴリ	URL/ファイル名
12/24 17:35:21	traffic	end								

A '閉じる' (Close) button is located at the bottom right of the log details panel.

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

	受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元
	08/16 15:37:42	end	L3-TAP	L3-TAP	77.54.71.89
	08/16 15:37:42	end	L3-TAP	L3-TAP	88.23.72.193
	08/16 15:37:41	end	L3-TAP	L3-TAP	113.6.255.191
	08/16 15:37:41	end	L3-TAP	L3-TAP	10.154.13.155

←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。



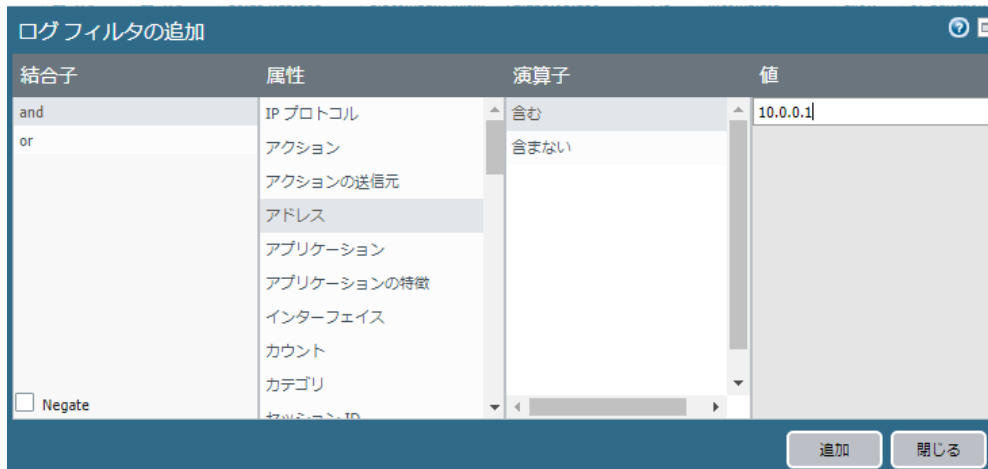
3-7.ログフィルタ（続き）

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。

4-1.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。

4-2. 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

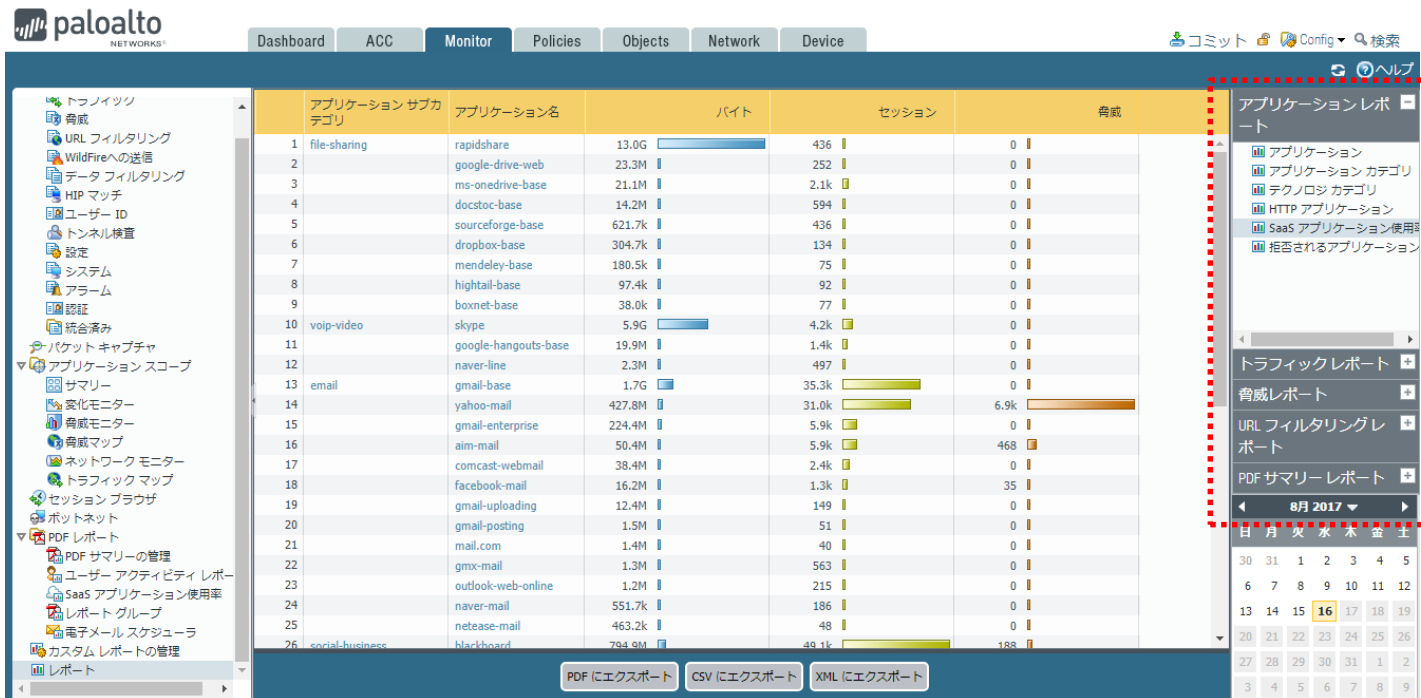
4または5が示された場合は、該当の端末をスキャンしたり、ネットワークから切り離す等、対処が必要な場合があります。

4-3. 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に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。



The screenshot shows the Palo Alto Networks Monitor interface. The main table displays application reports with columns for Application Category, Application Name, Bytes, Sessions, and Threats. The sidebar on the right contains a menu for 'Application Reports' (アプリケーションレポート) which is highlighted with a red dashed box. Below the menu is a calendar for August 2017.

アプリケーション サブカテゴリ	アプリケーション名	バイト	セッション	脅威
1 file-sharing	rapidshare	13.0G	436	0
2	google-drive-web	23.3M	252	0
3	ms-onedrive-base	21.1M	2.1k	0
4	docstoc-base	14.2M	594	0
5	sourceforge-base	621.7k	436	0
6	dropbox-base	304.7k	134	0
7	mendeley-base	180.5k	75	0
8	hightail-base	97.4k	92	0
9	boxnet-base	38.0k	77	0
10 voip-video	skype	5.9G	4.2k	0
11	google-hangouts-base	19.9M	1.4k	0
12	naver-line	2.3M	497	0
13 email	gmail-base	1.7G	35.3k	0
14	yahoo-mail	427.8M	31.0k	6.9k
15	gmail-enterprise	224.4M	5.9k	0
16	aim-mail	50.4M	5.9k	468
17	comcast-webmail	38.4M	2.4k	0
18	facebook-mail	16.2M	1.3k	35
19	gmail-uploading	12.4M	149	0
20	gmail-posting	1.5M	51	0
21	mail.com	1.4M	40	0
22	gmx-mail	1.3M	563	0
23	outlook-web-online	1.2M	215	0
24	naver-mail	551.7k	186	0
25	netease-mail	463.2k	48	0
26	social-business	794.9M	49.1k	188

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。

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: untitled

データベース: Application Statistics

スケジュール設定

期間: 過去 15 分

ソート基準: None

グループ化基準: None

クエリビルダー

結合子	属性	演算子	値
and	アプリケーション		
or	アプリケーション カテゴリ		

OK キャンセル

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。

4-4. カスタムレポート（続き）

The screenshot shows the 'Custom Report' configuration window. At the top, there is a 'Report Settings' tab. Below it, there are two buttons: 'Load Template' (with a folder icon) and 'Run Now' (with a play icon). The main area contains several input fields and checkboxes:

- 名前 (Name):** A text input field containing 'untitled'.
- データベース (Database):** A dropdown menu currently showing 'Application Statistics'.
- スケジュール設定 (Schedule Setting):** An unchecked checkbox.
- 期間 (Period):** A dropdown menu currently showing '過去 15 分' (Past 15 minutes).
- ソート基準 (Sort Criteria):** A dropdown menu currently showing 'None', with a secondary dropdown showing 'トップ 10' (Top 10).
- グループ化基準 (Grouping Criteria):** A dropdown menu currently showing 'None', with a secondary dropdown showing '10 グループ' (10 groups).

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。

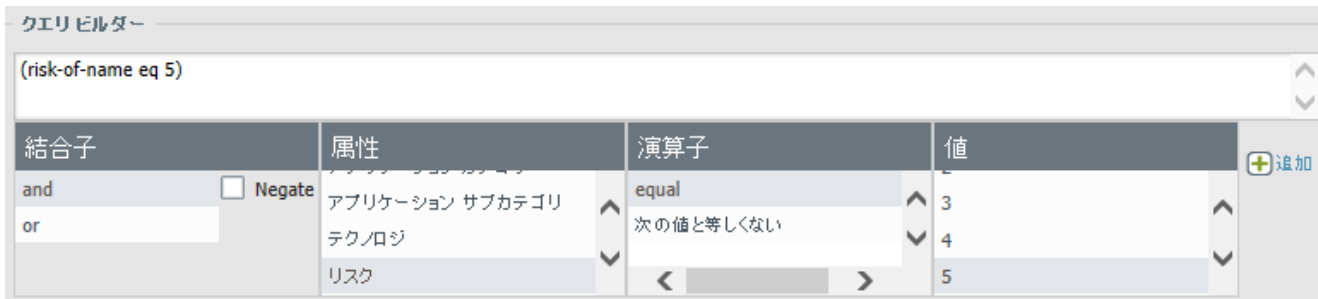
4-4. カスタムレポート（続き）



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。

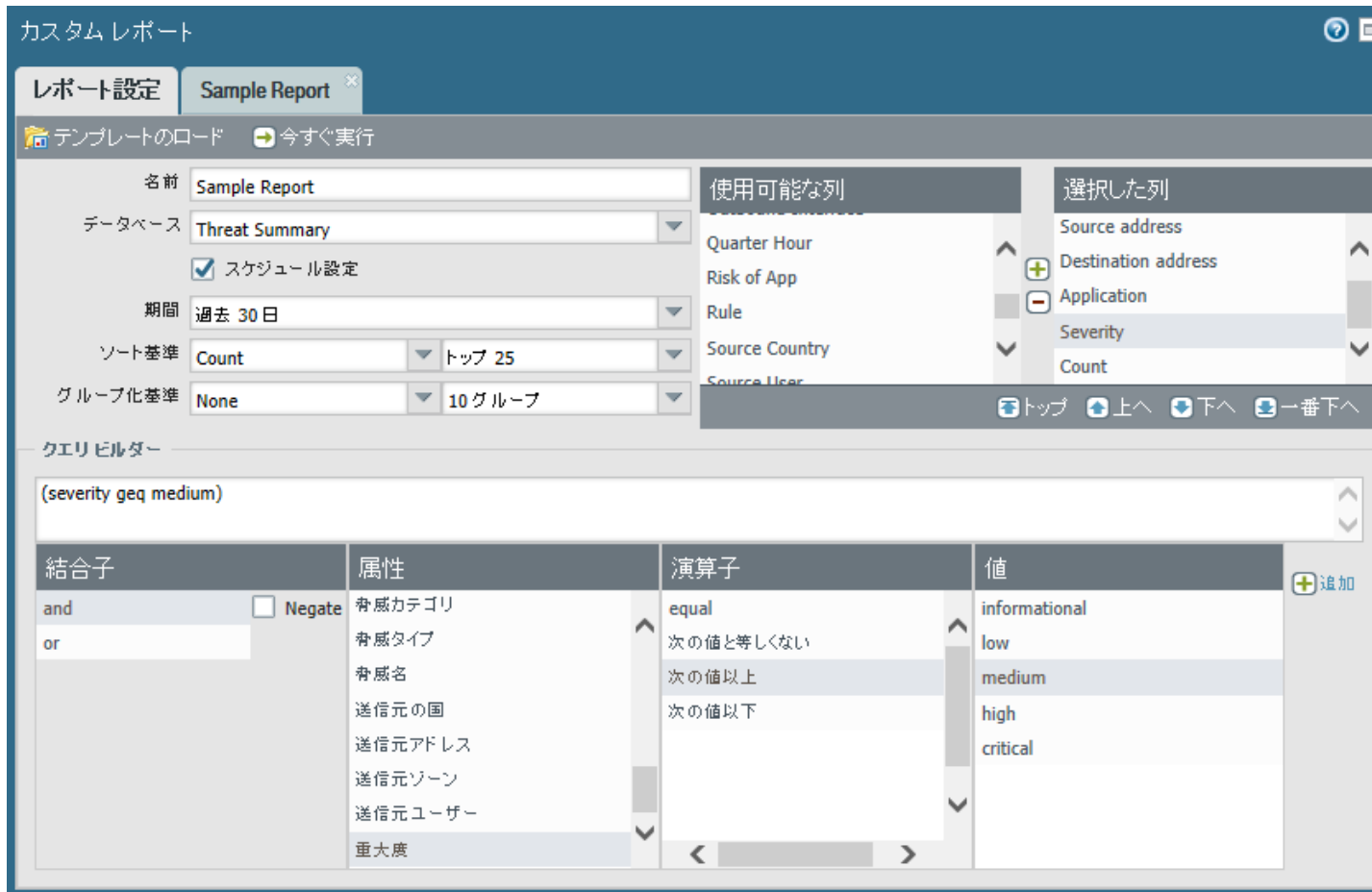


クエリビルダー

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に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。

4-4. 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。



カスタムレポート

レポート設定 Sample Report

テンプレートのロード 今すぐ実行

名前: Sample Report

データベース: Threat Summary

スケジュール設定

期間: 過去 30 日

ソート基準: Count トップ 25

グループ化基準: None 10 グループ

使用可能な列

- Quarter Hour
- Risk of App
- Rule
- Source Country
- Source User

選択した列

- Source address
- Destination address
- Application
- Severity
- Count

クエリビルダー

(severity geq medium)

結合子	属性	演算子	値
and <input type="checkbox"/> Negate	脅威カテゴリ	equal	informational
or	脅威タイプ	次の値と等しくない	low
	脅威名	次の値以上	medium
	送信元の国	次の値以下	high
	送信元アドレス		critical
	送信元ゾーン		
	送信元ユーザー		
	重大度		

4. モニター・レポート確認

4-4. カスタムレポート (続き)

出カイメッセージです。

カスタムレポート

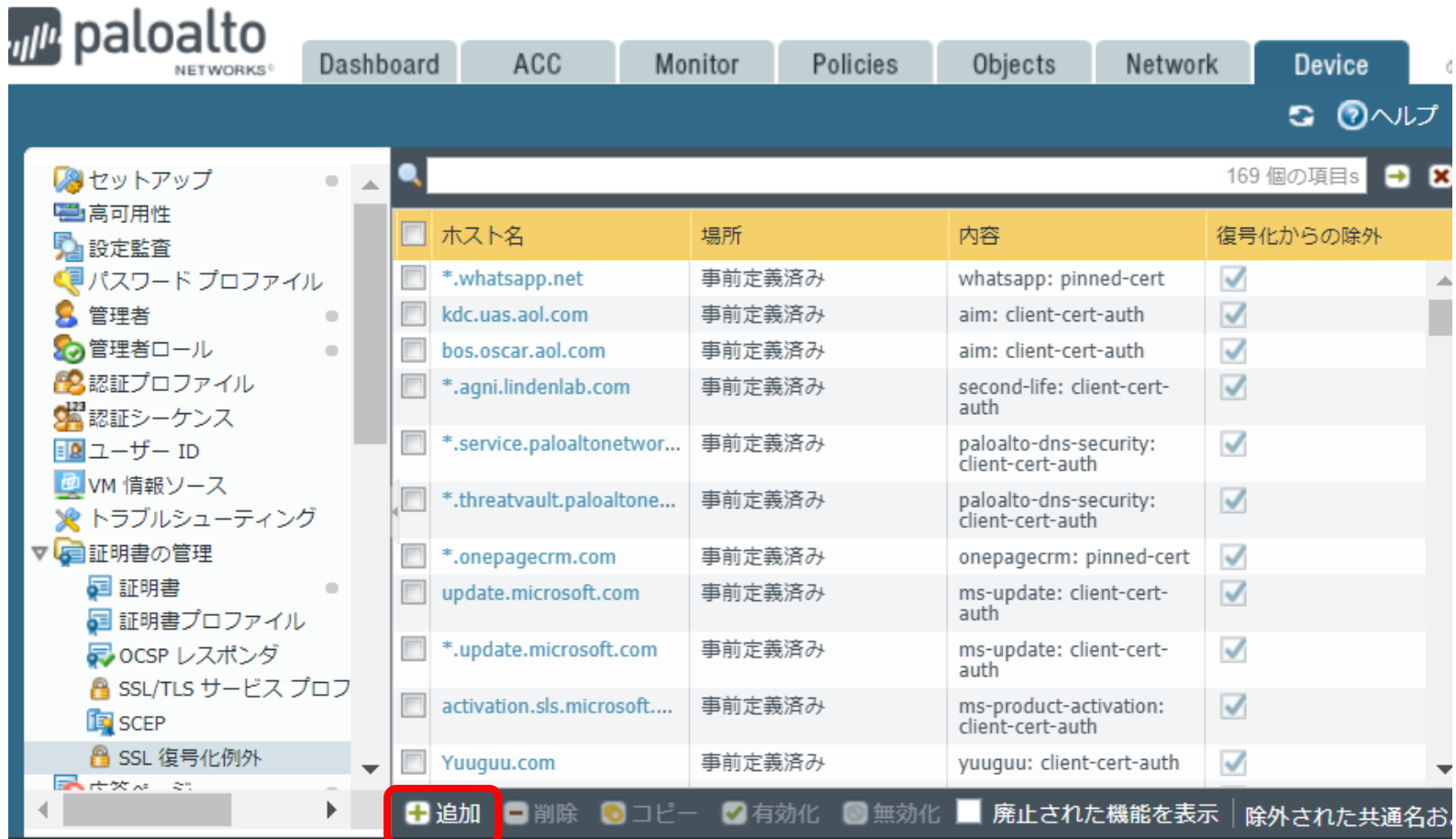
レポート設定 Sample Report

	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.akamaitechnologies.com	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.com	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

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]



The screenshot shows the Palo Alto Networks management interface. The left sidebar has a menu with '証明書の管理' (Certificate Management) expanded to 'SSL復号化例外' (SSL Decryption Exceptions). The main area displays a table of exceptions. At the bottom, a red box highlights the '+ 追加' (Add) button.

ホスト名	場所	内容	復号化からの除外
<input type="checkbox"/> *.whatsapp.net	事前定義済み	whatsapp: pinned-cert	<input checked="" type="checkbox"/>
<input type="checkbox"/> kdc.uas.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> bos.oscar.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.agni.lindenlab.com	事前定義済み	second-life: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.service.paloaltonetwor...	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.threatvault.paloaltone...	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.onepagecrm.com	事前定義済み	onepagecrm: pinned-cert	<input checked="" type="checkbox"/>
<input type="checkbox"/> update.microsoft.com	事前定義済み	ms-update: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.update.microsoft.com	事前定義済み	ms-update: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> activation.sls.microsoft....	事前定義済み	ms-product-activation: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> Yuuguu.com	事前定義済み	yuuguu: client-cert-auth	<input checked="" type="checkbox"/>

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

SSL 復号化例外

ホスト名

内容

除外

注: 復号化からエントリを除外するにはチェックします

OK キャンセル

例2

SSL 復号化例外

ホスト名

内容

除外

注: 復号化からエントリを除外するにはチェックします

OK キャンセル

※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。

paloalto NETWORKS

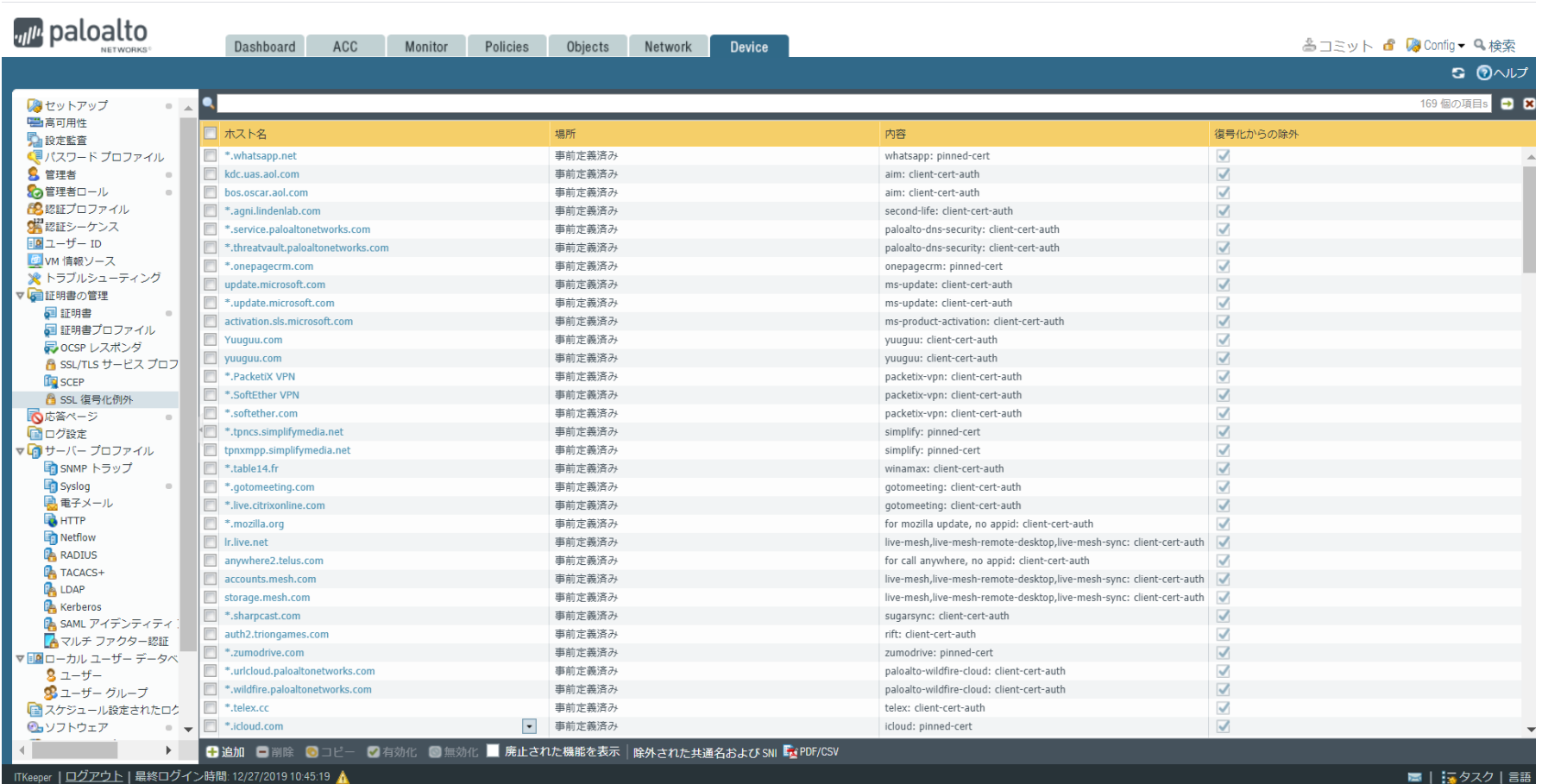
Dashboard ACC Monitor Policies Objects Network Device **コミット**

170 個の項目

ホスト名	場所	内容	復号化からの除外
<input type="checkbox"/> *.whatsapp.net	事前定義済み	whatsapp: pinned-cert	<input checked="" type="checkbox"/>
<input type="checkbox"/> kdc.uas.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> bos.oscar.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.agni.lindenlab.com	事前定義済み	second-life: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.service.paloaltonetworks.c...	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.threatvault.paloaltonetwor...	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
<input type="checkbox"/> *.onpagecrm.com	事前定義済み	onpagecrm: pinned-cert	<input checked="" type="checkbox"/>

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。



The screenshot shows the Palo Alto Networks configuration interface for a device. The 'SSL 復号化例外' (SSL Decryption Exceptions) section is expanded, displaying a table of exceptions. The table has four columns: 'ホスト名' (Host Name), '場所' (Location), '内容' (Content), and '復号化からの除外' (Exclusion from Decryption). Each row represents an exception for a specific host, with a checkbox in the final column indicating that decryption is disabled for that host.

ホスト名	場所	内容	復号化からの除外
*.whatsapp.net	事前定義済み	whatsapp: pinned-cert	<input checked="" type="checkbox"/>
kdc.uas.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
bos.oscar.aol.com	事前定義済み	aim: client-cert-auth	<input checked="" type="checkbox"/>
*.agnl.lindenlab.com	事前定義済み	second-life: client-cert-auth	<input checked="" type="checkbox"/>
*.service.paloaltonetworks.com	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
*.threatvault.paloaltonetworks.com	事前定義済み	paloalto-dns-security: client-cert-auth	<input checked="" type="checkbox"/>
*.onepagecrm.com	事前定義済み	onepagecrm: pinned-cert	<input checked="" type="checkbox"/>
update.microsoft.com	事前定義済み	ms-update: client-cert-auth	<input checked="" type="checkbox"/>
*.update.microsoft.com	事前定義済み	ms-update: client-cert-auth	<input checked="" type="checkbox"/>
activation.sls.microsoft.com	事前定義済み	ms-product-activation: client-cert-auth	<input checked="" type="checkbox"/>
Yuuguu.com	事前定義済み	yuuguu: client-cert-auth	<input checked="" type="checkbox"/>
yuuguu.com	事前定義済み	yuuguu: client-cert-auth	<input checked="" type="checkbox"/>
*.PacketIX VPN	事前定義済み	packetix-vpn: client-cert-auth	<input checked="" type="checkbox"/>
*.SoftEther VPN	事前定義済み	packetix-vpn: client-cert-auth	<input checked="" type="checkbox"/>
*.softether.com	事前定義済み	packetix-vpn: client-cert-auth	<input checked="" type="checkbox"/>
*.tpncs.simplifymedia.net	事前定義済み	simplify: pinned-cert	<input checked="" type="checkbox"/>
tpnxmpp.simplifymedia.net	事前定義済み	simplify: pinned-cert	<input checked="" type="checkbox"/>
*.table14.fr	事前定義済み	winamax: client-cert-auth	<input checked="" type="checkbox"/>
*.gotomeeting.com	事前定義済み	gotomeeting: client-cert-auth	<input checked="" type="checkbox"/>
*.live.citrixonline.com	事前定義済み	gotomeeting: client-cert-auth	<input checked="" type="checkbox"/>
*.mozilla.org	事前定義済み	for mozilla update, no appid: client-cert-auth	<input checked="" type="checkbox"/>
lr.live.net	事前定義済み	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth	<input checked="" type="checkbox"/>
anywhere2.telus.com	事前定義済み	for call anywhere, no appid: client-cert-auth	<input checked="" type="checkbox"/>
accounts.mesh.com	事前定義済み	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth	<input checked="" type="checkbox"/>
storage.mesh.com	事前定義済み	live-mesh, live-mesh-remote-desktop, live-mesh-sync: client-cert-auth	<input checked="" type="checkbox"/>
*.sharpcast.com	事前定義済み	sugarsync: client-cert-auth	<input checked="" type="checkbox"/>
auth2.triongames.com	事前定義済み	rift: client-cert-auth	<input checked="" type="checkbox"/>
*.zumodrive.com	事前定義済み	zumodrive: pinned-cert	<input checked="" type="checkbox"/>
*.urcloud.paloaltonetworks.com	事前定義済み	paloalto-wildfire-cloud: client-cert-auth	<input checked="" type="checkbox"/>
*.wildfire.paloaltonetworks.com	事前定義済み	paloalto-wildfire-cloud: client-cert-auth	<input checked="" type="checkbox"/>
*.telex.cc	事前定義済み	telex: client-cert-auth	<input checked="" type="checkbox"/>
*.icloud.com	事前定義済み	icloud: pinned-cert	<input checked="" type="checkbox"/>

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。

The screenshot shows the Palo Alto Networks GUI. The left sidebar contains a navigation menu with 'ログ' (Log) expanded. Under 'ログ', 'トラフィック' (Traffic) is selected. The main area displays a traffic log entry for 'addr dst in 184.31.46.55'. A red box highlights the '復号化' (Decryption) checkbox in the 'フラグ' (Flags) section, which is currently unchecked. A red arrow points from this checkbox to the 'トラフィック' menu item.

受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先
2020/01/17 14:02:10	end	ssl	Trust-Rule1	8d7c71b2-5a38-4...	909170	informational
2020/01/17 14:01:41	url	ssl	Trust-Rule1	8d7c71b2-5a38-4...		informational

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]

The screenshot shows the Palo Alto Networks management console interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Objects' tab is active, and the 'Addresses' sub-tab is selected. The left sidebar shows a tree view with 'Addresses' selected. The main area displays a table of existing addresses, all of which are IP network masks (0.0.0.0/32). At the bottom, a red box highlights the '+ 追加' (Add) button.

名前	場所	タイプ	アドレス	内容	タグ
<input type="checkbox"/> Dst_Security_Fr...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> Dst_Security_Fr...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> Dst_Security_Fr...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> Src_Security_Fre...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> Src_Security_Fre...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> Src_Security_Fre...		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_1		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_2		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_3		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_4		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_5		IP ネットマスク	0.0.0.0/32		
<input type="checkbox"/> SSL_Free_6		IP ネットマスク	0.0.0.0/32		

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。

アドレス

名前 SSL-Free-Address-add1

内容

タイプ IP ネットマスク 192.168.1.10/32 解決

タグ

OK キャンセル

スラッシュ表記を使用して IP アドレスまたはネットワークを入力します (例: 192.168.80.150 または 192.168.80.0/24)。IPv6 アドレスまたはプレフィックスを使用した IPv6 アドレス (例: Ex. 2001:db8:123:1::1 または 2001:db8:123:1::/64) も入力できます。

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

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device コミット ヘルプ

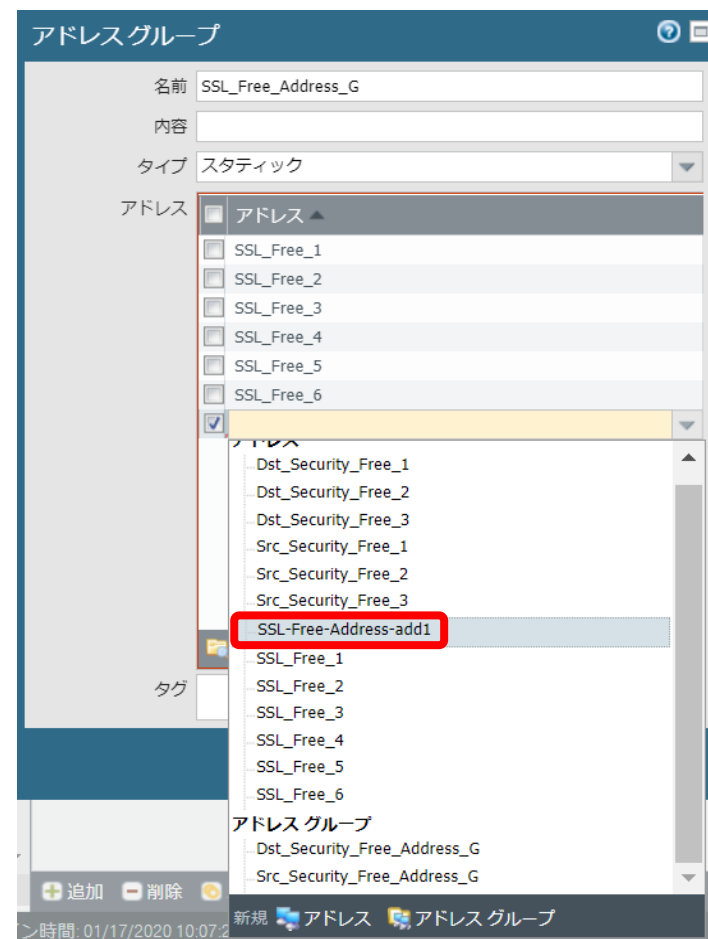
3 個の項目

名前	場所	メンバー数	アドレス	タグ
Dst_Security_Free_Ad...		3	Dst_Security_Free_1 Dst_Security_Free_2 Dst_Security_Free_3	
Src_Security_Free_Ad...		3	Src_Security_Free_1 Src_Security_Free_2 Src_Security_Free_3	
SSL_Free_Address_G		6	SSL_Free_1 SSL_Free_2 SSL_Free_3 SSL_Free_4 SSL_Free_5 SSL_Free_6	

追加 削除 コピー PDF/CSV

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。

アドレスグループ

名前 SSL_Free_Address_G

内容

タイプ スタティック

アドレス

- アドレス ▲
- SSL_Free_1
- SSL_Free_2
- SSL_Free_3
- SSL_Free_4
- SSL_Free_5
- SSL_Free_6
- SSL-Free-Address-add1

参照 追加 削除

タグ

OK キャンセル

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）

The screenshot shows the Palo Alto Networks Security Policy configuration interface. The 'Policies' tab is active, and the '復号' (Decryption) section is selected. A table lists three policies:

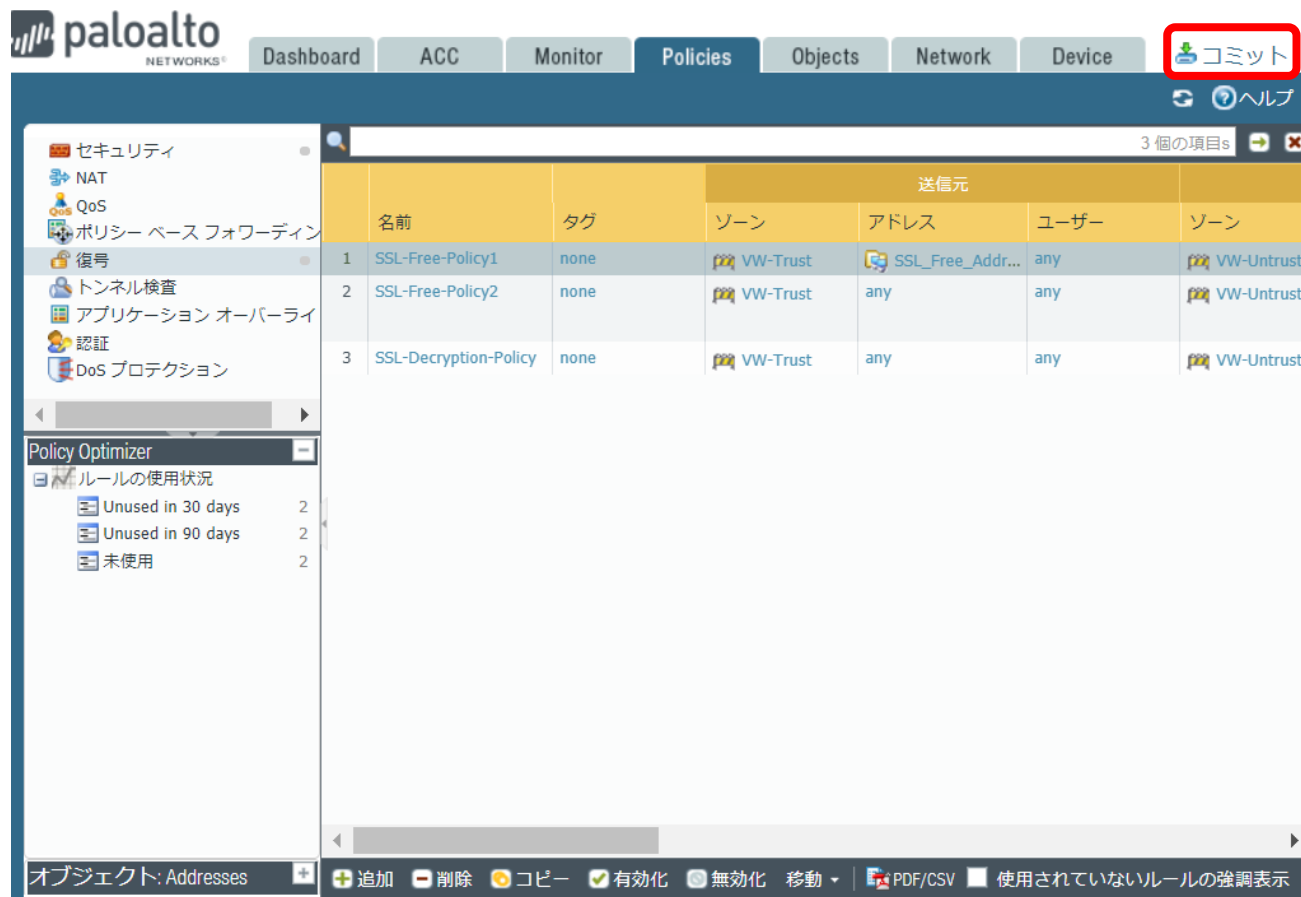
		送信元			宛先		復号オプション					
名前	タグ	ゾーン	アドレス	ユーザー	ゾーン	アドレス	URL カテゴリ	サービス	アクション	タイプ	復号プロファイル	ヒット
1 SSL-Free-Policy1	none	VW-Trust	SSL_Free_Addr...	any	VW-Untrust	any	any	any	no-decrypt	ssl-forward-proxy	なし	0
2 SSL-Free-Policy2	none	VW-Trust	any	any	VW-Untrust	any	financial-services health-and-medi...	any	no-decrypt	ssl-forward-proxy	なし	0
3 SSL-Decryption-Policy	none	VW-Trust	any	any	VW-Untrust	any	any	any	decrypt	ssl-forward-proxy	decrypt-profile	235

The bottom toolbar contains the following options: オブジェクト: Addresses, 追加, 削除, コピー, **有効化** (checked), 無効化, 移動. A red arrow points from the ID '1' in the first row to the '有効化' checkbox.

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



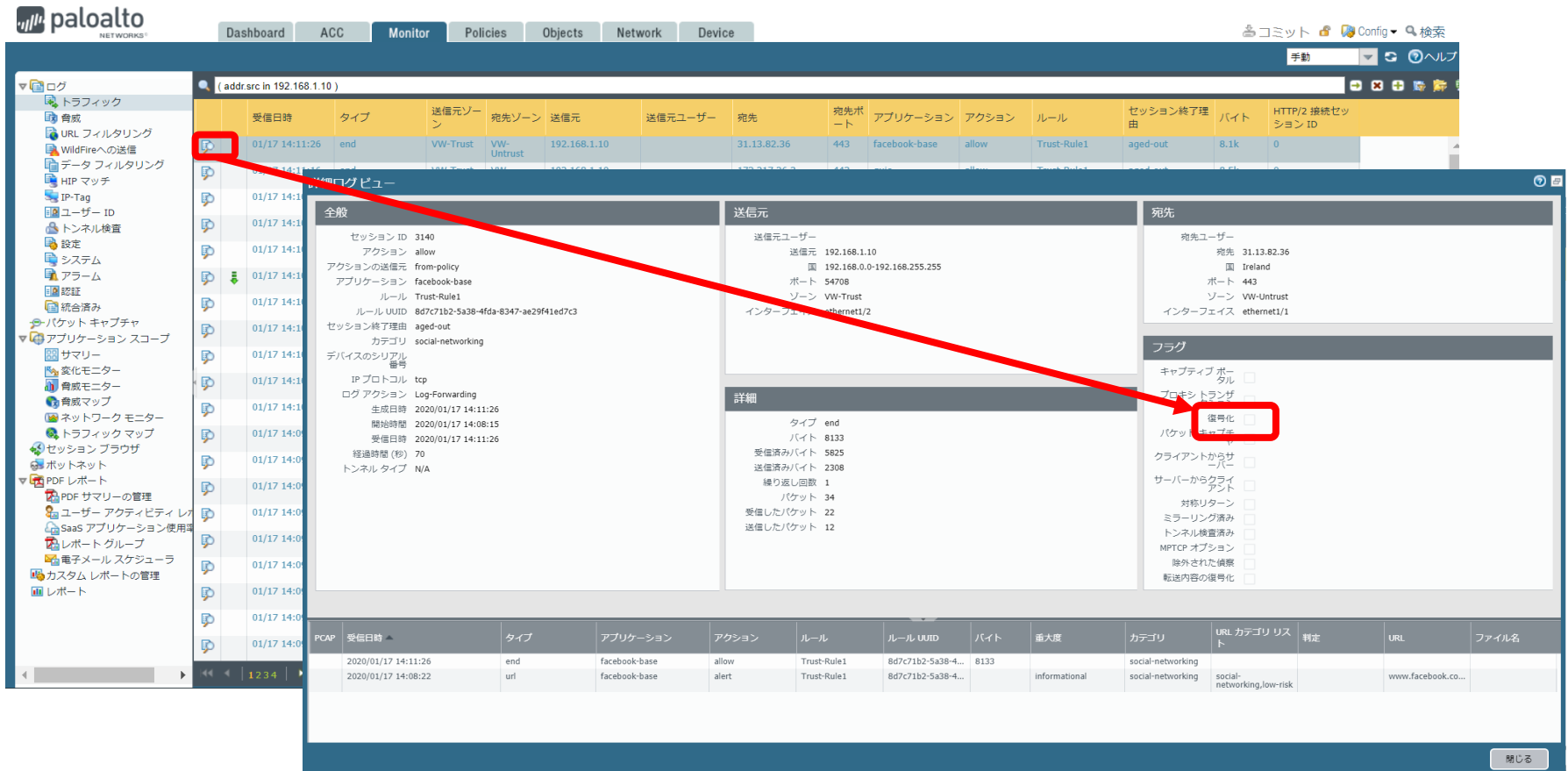
The screenshot shows the Palo Alto Networks GUI with the 'Policies' tab selected. A red box highlights the 'コミット' (Commit) button in the top right corner. Below the navigation bar, a table displays the configuration for three policies. The table has columns for '名前' (Name), 'タグ' (Tag), 'ゾーン' (Zone), '送信元' (Source), 'アドレス' (Address), 'ユーザー' (User), and 'ゾーン' (Zone). The '送信元' column is further divided into 'ゾーン' and 'アドレス' sub-columns.

	名前	タグ	ゾーン	送信元		ゾーン
				ゾーン	アドレス	
1	SSL-Free-Policy1	none	VW-Trust	any	any	VW-Untrust
2	SSL-Free-Policy2	none	VW-Trust	any	any	VW-Untrust
3	SSL-Decryption-Policy	none	VW-Trust	any	any	VW-Untrust

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。



The screenshot shows the Palo Alto Networks GUI. The 'Monitor' tab is active, and the 'Log' section is expanded to 'Traffic'. A log entry is selected, and a detailed view is shown. A red box highlights the 'Decryption' checkbox in the 'Flags' section, which is currently unchecked. A red arrow points from the log entry table to this checkbox.

受信日時	タイプ	送信元ゾーン	宛先ゾーン	送信元	送信元ユーザー	宛先	宛先ポート	アプリケーション	アクション	ルール	セッション終了理由	バイト	HTTP/2 接続セッション ID
01/17 14:11:26	end	VW-Trust	VW-Untrust	192.168.1.10		31.13.82.36	443	facebook-base	allow	Trust-Rule1	aged-out	8.1k	0

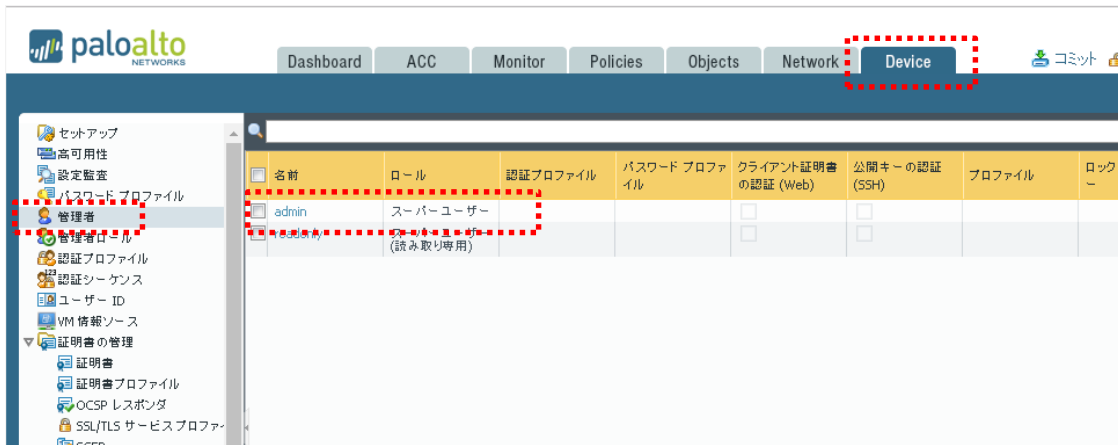
全般		送信元		宛先	
セッション ID	3140	送信元ユーザー		宛先ユーザー	
アクション	allow	送信元	192.168.1.10	宛先	31.13.82.36
アクションの送信元	from-policy	国	192.168.0.0-192.168.255.255	国	Ireland
アプリケーション	facebook-base	ポート	54708	ポート	443
ルール	Trust-Rule1	ゾーン	VW-Trust	ゾーン	VW-Untrust
ルール UUID	8d7c71b2-5a38-4fda-8347-ae29f41e7c3	インターフェイス	ethernet1/2	インターフェイス	ethernet1/1
セッション終了理由	aged-out				
カテゴリ	social-networking				
デバイスのシリアル番号					
IP プロトコル	tcp				
ログアクション	Log-Forwarding				
生成日時	2020/01/17 14:11:26				
開始時間	2020/01/17 14:08:15				
受信日時	2020/01/17 14:11:26				
経過時間 (秒)	70				
トンネルタイプ	N/A				

PCAP	受信日時	タイプ	アプリケーション	アクション	ルール	ルール UUID	バイト	重大度	カテゴリ	URL カテゴリ リスト	判定	URL	ファイル名
	2020/01/17 14:11:26	end	facebook-base	allow	Trust-Rule1	8d7c71b2-5a38-4...	8133		social-networking	social-networking			
	2020/01/17 14:08:22	url	facebook-base	alert	Trust-Rule1	8d7c71b2-5a38-4...		informational	social-networking	social-networking,low-risk		www.facebook.co...	

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。

The dialog box titled '管理者' (Admin) contains the following fields and options:

- 名前: admin
- 現在のパスワード: [password field]
- 新しいパスワード: [password field]
- 新しいパスワードの確認: [password field]
- 公開鍵認証 (SSH) の使用
- Buttons: OK, キャンセル

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。



7-1.起動

- ・電源ケーブルを挿します。
※電源ボタンはありません。

7-2.停止

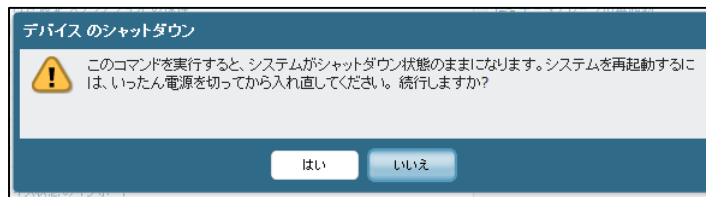
停止時は、PAファイアウォールの管理画面でシャットダウンします。

- ・ 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。

The screenshot shows the Palo Alto Networks management interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Device' tab is selected. Below the navigation bar, there are sub-tabs: '管理', '操作', 'サービス', 'インターフェイス', 'Telemetry', 'コンテンツ ID', 'WildFire', 'セッション', and 'HSM'. The '操作' (Operations) sub-tab is active. The main content area is divided into two sections: '設定の管理' (Configuration Management) and 'デバイスの操作' (Device Operations). In the 'デバイスの操作' section, the 'デバイスの再起動' (Restart Device) and 'デバイスのシャットダウン' (Shutdown Device) options are visible. The 'デバイスのシャットダウン' option is highlighted with a red dashed box. Below this, there is a 'その他' (Other) section with options like 'カスタム ログ' (Custom Log) and 'SNMP のセットアップ' (SNMP Setup). At the bottom, there is a section for 'AWS CloudWatch の設定' (AWS CloudWatch Configuration) with a checkbox for 'CloudWatch モニタリングの有効化' (Enable CloudWatch Monitoring).

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。

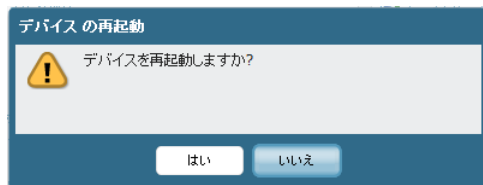
7-3.再起動

- 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。

The screenshot shows the Palo Alto Networks management console interface. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The left sidebar contains a tree view of configuration categories such as Setups, High Availability, Configuration Monitoring, Password Profiles, Administrators, Administrator Roles, Authentication Profiles, Authentication Schemes, User ID, VM Information Sources, and Certificate Management. The main content area is divided into sections: 'Settings Management' (with options like Return, Save, Load, Export, Import) and 'Device Operations' (with options like Restart Device and Shutdown Device). The 'Restart Device' option is highlighted with a red dashed box. Other sections include 'Others' (Custom Logo, SNMP Setup) and 'AWS CloudWatch Settings' (CloudWatch Monitoring Enabled checkbox).

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。

- 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。

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.