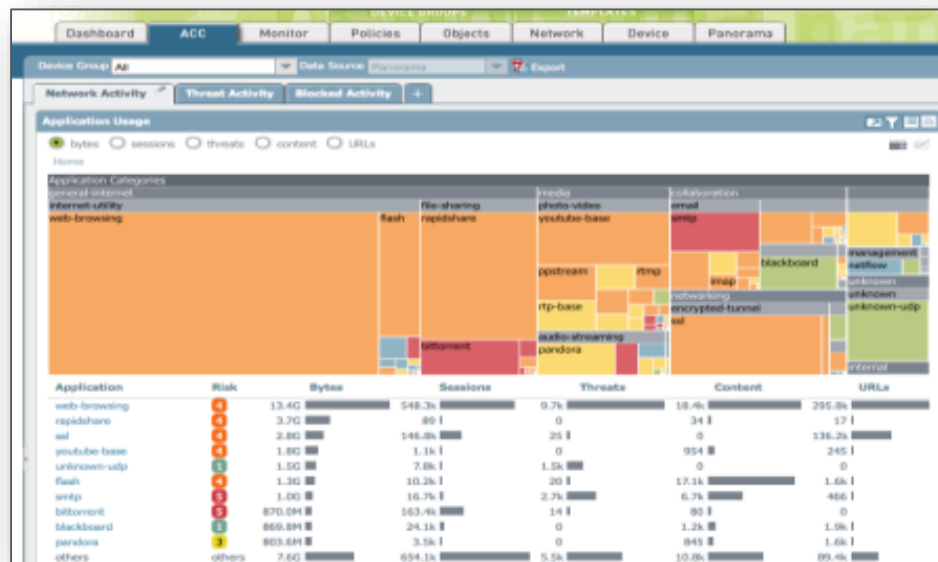


PAN-OS 7.0 アプリケーションコマンド・センター (ACC) 機能強化

Palo Alto Networks K.K.

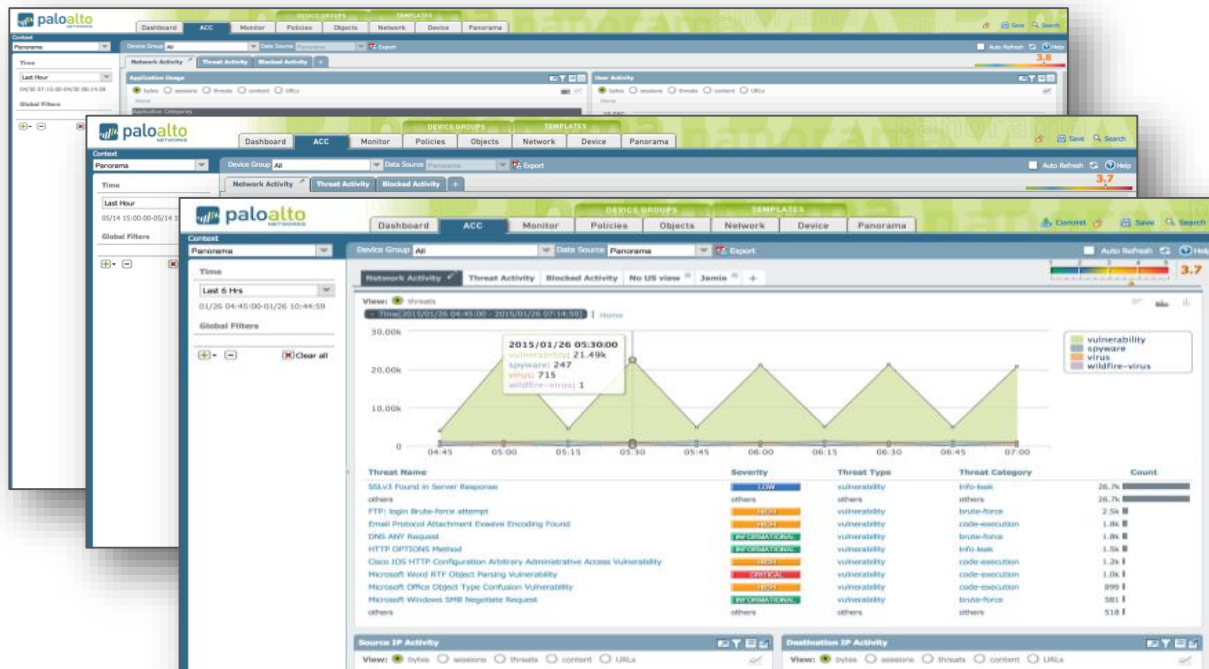
脅威の可視化とすぐに実用可能なデータの提供

- タブ形式で直感的なビジュアル・ディスプレイとウィジェットを持つ高度にインタラクティブなユーザーインターフェイス
- 数回のクリックで重要な情報を表示
- データの合理化と直感的な管理性
- 一意の脅威に対する迅速なレスポンスが可能



アプリケーションコマンド・センター (ACC) 機能強化

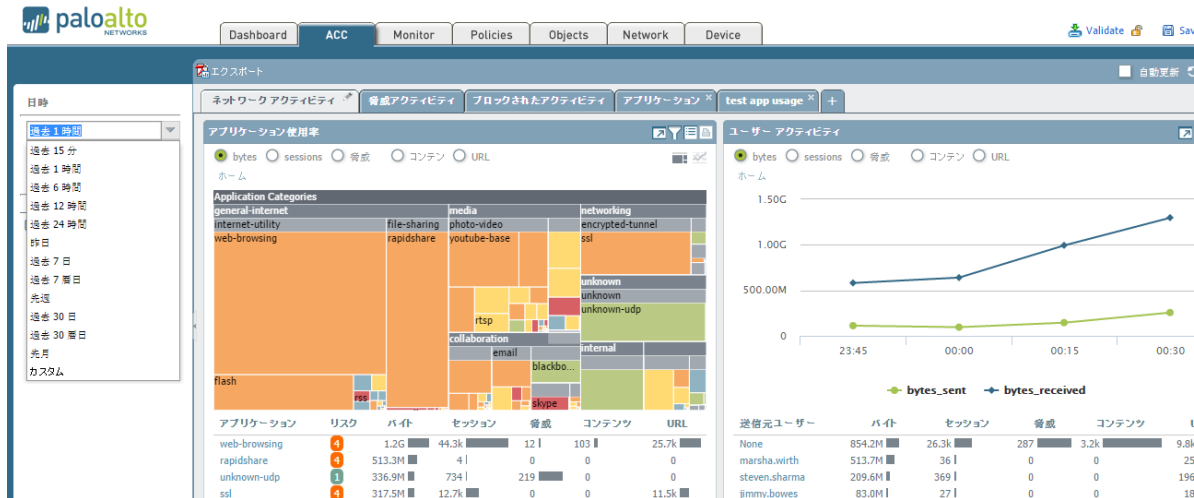
- インタラクティブに高度なカスタマイズが可能
- アプリケーション利用状況とユーザーアクティビティの可視化
- 送信元及び宛先のジオロケーション(国)の認識
- ネットワーク利用状況、脅威レベルの把握
- ドリルダウン機能により詳細調査が容易に



1. ACC タブ “ネットワークアクティビティ”

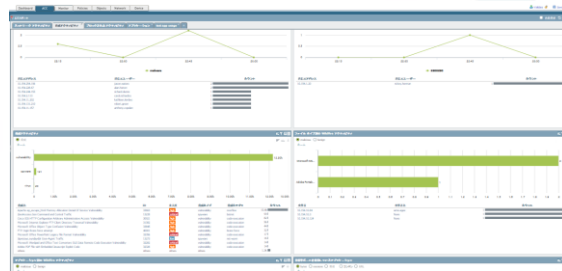
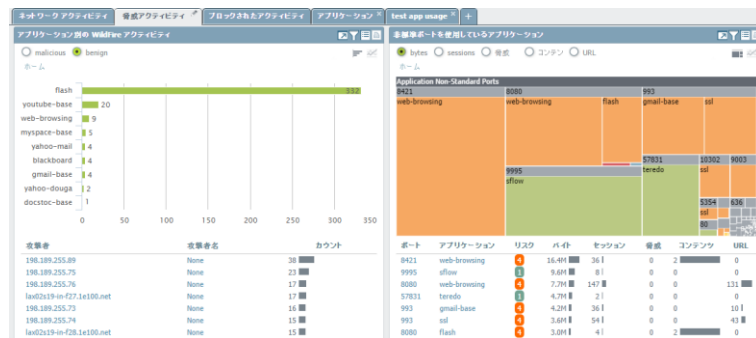
ネットワーク利用状況の表示と把握

- タブ“ネットワークアクティビティ”は指定した時間帯における下記項目の利用率を多い順に表示
 - アプリケーション
 - ユーザー
 - 送信元、宛先 IP・国
 - ルールの使用率



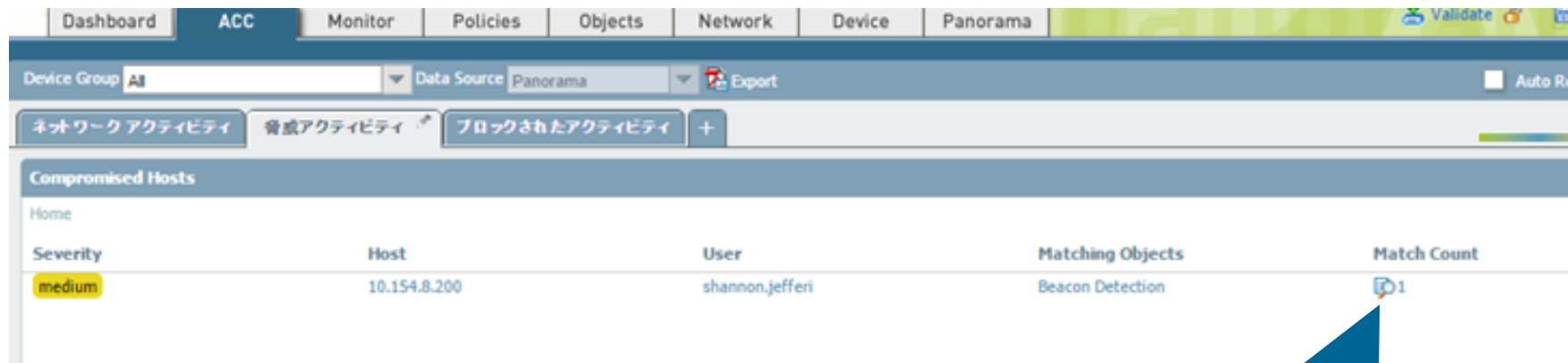
2. ACC タブ “脅威アクティビティ” 脅威発生状況の表示と把握

- タブ“脅威アクティビティ”は指定した時間帯における下記項目の検知状況を表示
 - 脅威のタイプ毎の集計
 - 脅威名、ID、重大度、脅威カテゴリ
 - 侵入(侵害)されたホスト
 - 有害なURLにアクセスしているホスト
 - 有害なドメインを解決しているホスト
 - ファイルタイプ別のWildFireアクティビティ
 - アプリケーション毎のWildFireアクティビティ
 - 非標準ポートを使用しているアプリケーション
 - 非標準ポートを使用するアプリケーションを許可するルール



2. ACC タブ ”脅威アクティビティ” 侵入(侵害)されたホストの表示と把握(1)

- 自動相関エンジンにて検出された「侵入(侵害)されたホスト」の表示



The screenshot shows the Palo Alto Networks ACC interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', 'Device', and 'Panorama'. Below the navigation bar, there are filters for 'Device Group' (AI) and 'Data Source' (Panorama), along with an 'Export' button. The main content area is titled 'Compromised Hosts' and contains a table with the following data:

Severity	Host	User	Matching Objects	Match Count
medium	10.154.8.200	shannon.jefferi	Beacon Detection	1

詳細情報へドリルダウン

2. ACC タブ ”脅威アクティビティ” 侵入(侵害)されたホストの表示と把握(2)

- 自動相関エンジンにて検出された「侵入(侵害)されたホスト」の表示
 - マッチした、相関オブジェクト
 - マッチした、エビデンスログ

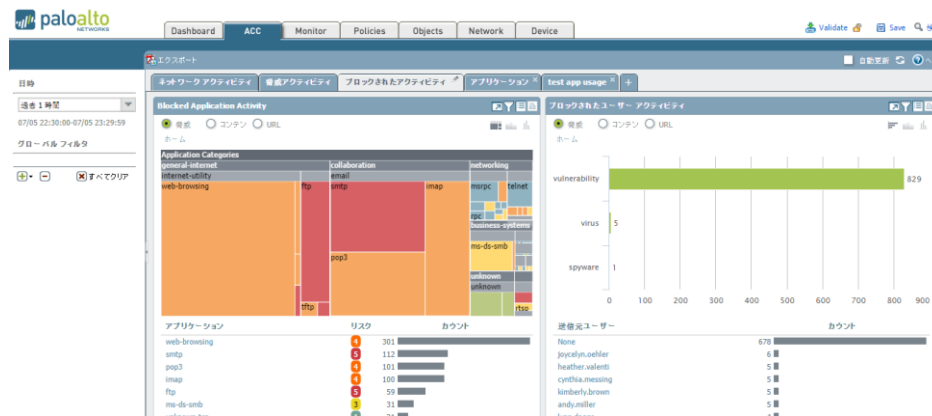
The screenshot displays the 'Correlation Log Detail - Compromised Host - Match #1' window. It is divided into several sections:

- Match Information:** Match # 1 - Beacon Detection
- Object Details:**
 - Title: Beacon Detection
 - ID: 6005
 - Detailed Description: This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
 - Category: compromised-host
- Match Details:**
 - Match Time: 2015/07/01 19:17:58
 - Last Update Time: 2015/07/03 00:25:23
 - Title: Beacon Detection
 - Severity: MEDIUM
 - Summary: Host repeatedly visited a dynamic DNS domain (103 times).
- Source:**
 - User: pancademo\shannon.j...
 - Address: 10.154.8.200
 - Country: 10.0.0.0-10.255.255.255
 - Port: 50670
 - Zone: TAP
 - Interface: ethernet1/2
- Destination:**
 - User: [blank]
 - Address: 202.93.87.249
 - Country: JP
 - Port: 80
 - Zone: TAP
 - Interface: ethernet1/2
- Flags:**
 - Captive Portal:
 - Proxy Transaction:
 - Decrypted:
 - Packet Capture:
 - Client to Server:
 - Server to Client:
- Details:**
 - Repeat Count: 1
 - URL: www.geocities.jp/gim...
- Evidence Table:**

Device Name	Evidence
us3demo.paloalton...	URL: www.geocities.jp/gimproject/gimp2.0.html
us3demo.paloalton...	URL: www.geocities.jp/gimproject/icon/bg01.gif
us3demo.paloalton...	URL: www.geocities.jp/gimproject/icon/wilber.gif
us3demo.paloalton...	URL: www.geocities.jp/gimproject/icon/new.gif
us3demo.paloalton...	URL: www.geocities.jp/gimproject/book/14.jpg
us3demo.paloalton...	URL: www.geocities.jp/gimproject/book/09.jpg

3. ACC タブ “ブロックされたアクティビティ” 防御状況の表示と把握

- タブ“ブロックされたアクティビティ”は指定した時間帯における下記項目の防御状況を表示
 - ブロックされたアプリケーションアクティビティ
 - ブロックされたユーザーアクティビティ
 - ブロックされた脅威
 - ブロックされたコンテンツ
 - アクティビティをブロックしているセキュリティポリシー



4. ACC カスタムタブの作成と追加

①「+」タブ選択し新規タブを追加

The screenshot shows the ACC interface with a custom tab labeled 'test app us' and a red circle around the '+' icon. The main content area displays 'Blocked Application Activity' with a bar chart and a table of application activity.

アプリケーション	リスク	カウント
web-browsing	4	302
smtp	5	114
imap	4	105
pop3	4	99
ftp	5	58

②「カスタムタブの追加」にてタブ名を入力「ウィジェットグループの追加」からWorkspaceを選択

The dialog box shows the 'Custom Tab Addition' process. The 'Widget Group Addition' section is highlighted with a red box. The 'Workspace' dropdown menu is open, showing '1 列' and '2 列' options.

③「ウィジェットの追加」から表示させたい情報を選択し「OK」にて保存

The dialog box shows the 'Widget Addition' process. The 'Application Usage' section is checked, and the 'vulnerability' widget is selected in the list.

ACC 「日時」 情報表示の変更

- 表示する情報の時間帯を指定することが可能
 - Last 15 Minutes 過去15分の情報を表示
 - Last Hour 過去1時間の情報を表示
 - Last 6 Hrs 過去6時間の情報を表示
 - Last 12 Hrs 過去12時間の情報を表示
 - Last 24 Hrs 過去24時間の情報を表示
 - Last Calendar Day 前日の情報を表示
 - Last 7 Days 過去7日の情報を表示(次スライド参照)
 - Last 7 Calendar Days 過去7暦日の情報を表示(次スライド参照)
 - Last Calendar Week 先週の情報を表示(次スライド参照)
 - Last 30 Days 過去30日の情報を表示
 - Last Calendar Month 先月の情報を表示
 - Custom 指定した期間の情報を表示

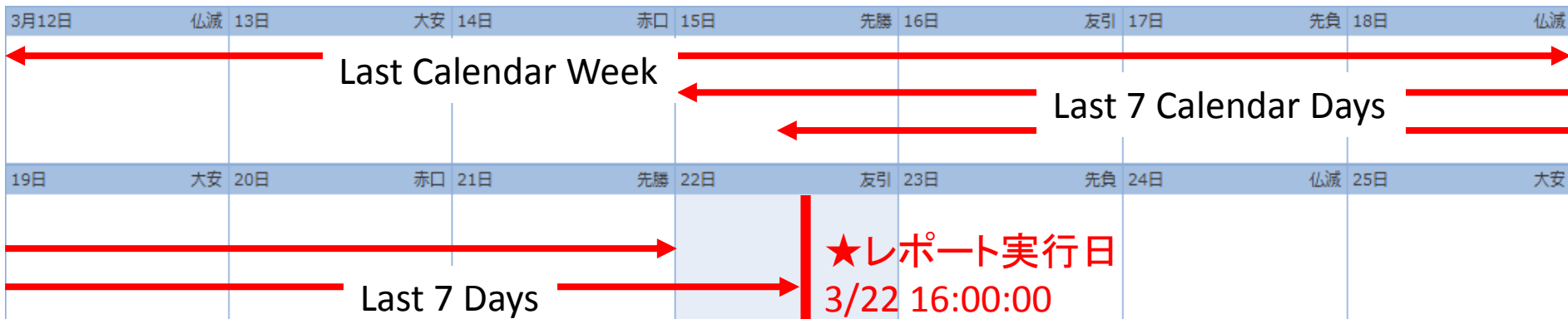
表示する情報の
時間帯を指定するこ
とが可能



ACC 「日時」 情報表示の変更

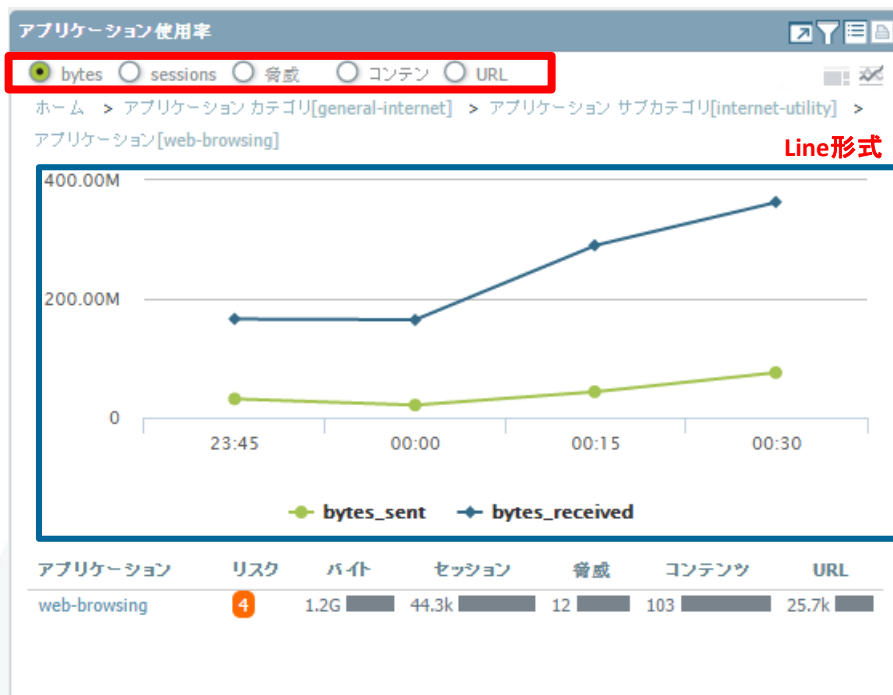
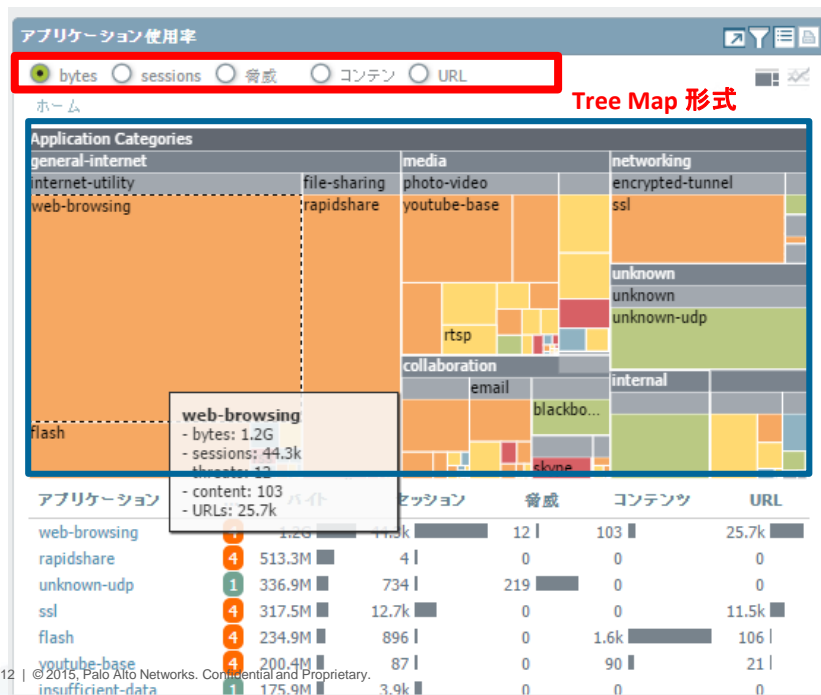
Last 7 Days Reportの違い

Last 7 Days	過去7日	2013/03/15 15:59:59 2013/03/22 16:00:00
Last 7 Calendar Days	過去7暦日	2013/03/15 – 2-12/03/21
Last Calendar Week	先週	2013/03/12 – 2-12/03/18



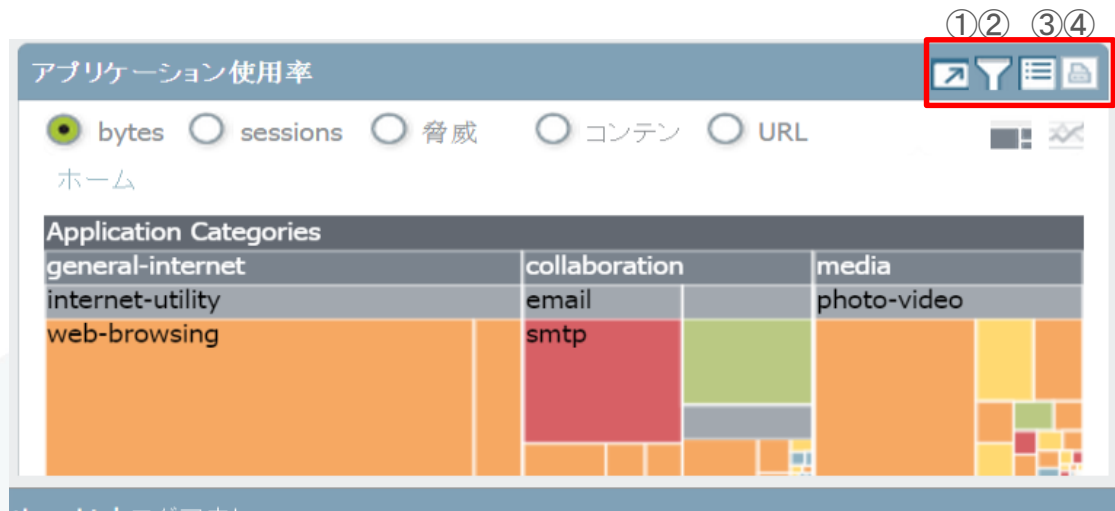
ACC 表示情報のソート、グラフの切り替え

- タブ内、各ウィジェットの表示のカスタマイズ
 - グラフ形式 – Tree Map形式 or Line形式の切り替え
 - ソート条件 – 「byte」、「sessions」、「脅威・コンテンツ・URL 検知数」を基準にソート



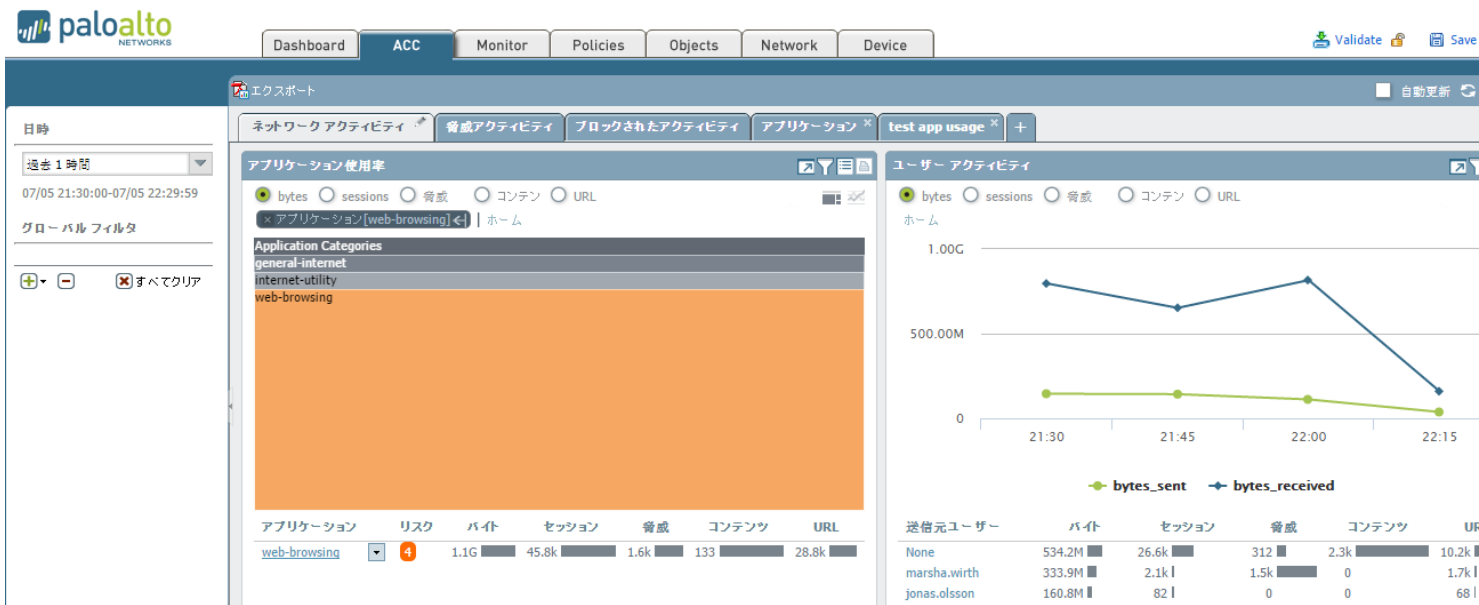
ACC 各ウィジェットの操作

- ① 最大化してもっとデータを表示・・・ウィジェット画面の最大化
- ② ローカルフィルタ・・・ウィジェット単位でのフィルタ(表示情報のフィルタリング)
- ③ ログヘジャンプ・・・ウィジェットから対象ログ画面へ遷移
- ④ エクスポート・・・ウィジェットに表示されている情報のエクスポート



ACC 表示情報のフィルタリング(ウィジェット単位)

- 各ウィジェット表示情報をクリックし、調査に必要な情報を迅速に抽出
 - (例)「アプリケーション使用率」一覧から”web-browsing”の情報のみを抽出
 - タブ内の他のウィジェットには反映されない



ACC 表示情報のフィルタリング(タブ単位)

- グローバルフィルタを使用し、タブ内の全ウィジェット表示情報を更新、調査に必要な情報を迅速に抽出
 - (例)「アプリケーション使用率」から”web-browsing”の情報のみ抽出
 - アプリケーション一覧から”web-browsing”を選択しドロップBOXから「フィルタのプロモート」にてフィルタを入力またはグローバルフィルタにフィルタ条件を直接入力

The screenshot displays the Palo Alto Networks ACC interface. The main view is the 'Application Usage' (アプリケーション使用率) widget, which is currently filtered to show only 'web-browsing'. A red box highlights the 'Global Filter' (グローバルフィルタ) section on the left, where 'web-browsing' is selected. A blue arrow points from this filter to the 'web-browsing' application in the main treemap. A red box highlights the 'Promote Filter' (フィルタのプロモート) button in the application list table below the treemap. A red arrow points from this button to the 'web-browsing' application in the table.

Application Usage (アプリケーション使用率) widget showing filtered data for 'web-browsing'.

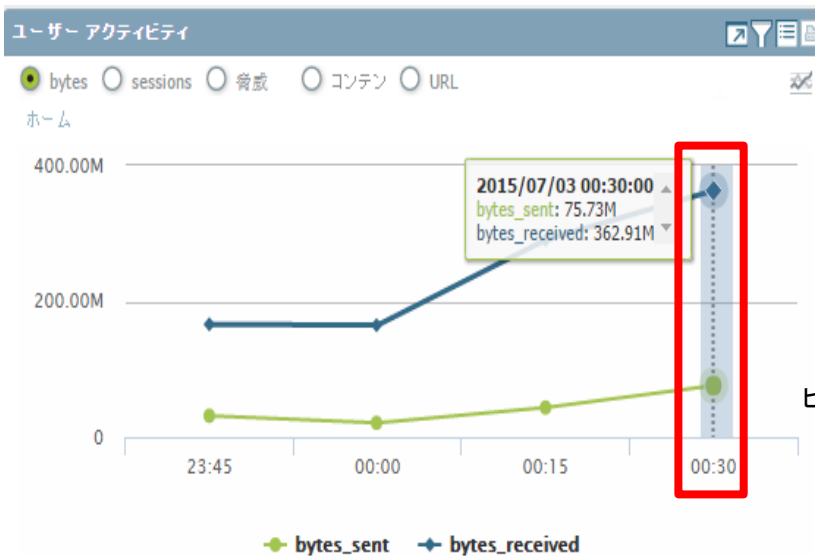
アプリケーション	リスク	バイト	セッション	脅威	コンテンツ	URL
web-browsing	4	1.2G	44.3k	12	103	25.7k

Application List Table:

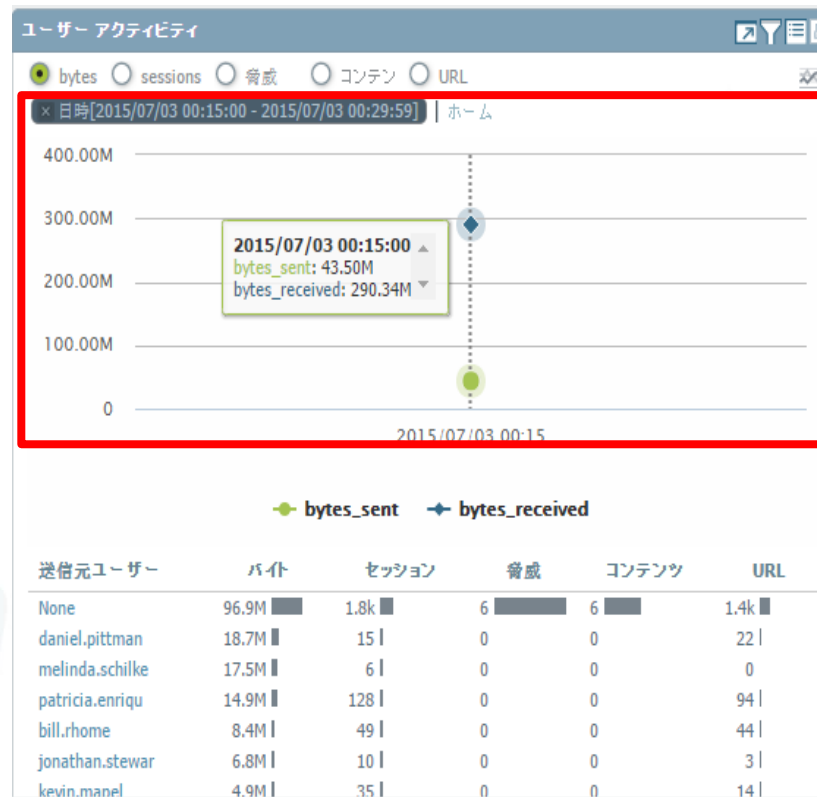
アプリケーション	...	バイト	セッション	脅威	コンテンツ	URL
web-browsing	グローバル検索	3k	12	103	25.7k	
rapidshare	フィルタのプロモート	4	0	0	0	
unknown-udp		219	0	0	0	
ssl		7k	0	0	11.5k	
flash		234.9M	896	0	1.6k	106
youtube-base		200.4M	87	0	90	21
insufficient-data		175.9M	3.9k	0	0	0

”web-browsing”で表示情報がフィルタリングされている。

ACC 表示情報の特定時間帯の抽出(ドリルダウン)



ピークの時間帯を
ドリルダウンし
該時間帯の
詳細情報表示



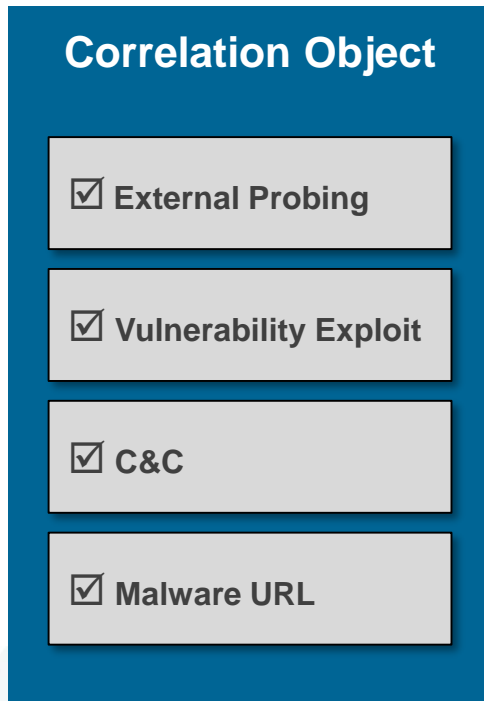
自動相関 (Automatic Correlation) エンジン

PAN-OS 7.0

自動相関 (Automatic Correlation) エンジン

- 関連付けオブジェクトは被害の兆候(Indicators of Compromise)の組み合わせを探す
- 自動的に侵害されたホストを検出
- コリレーションオブジェクト群は、脅威調査チームにより提供され、Weekly のContent update で更新される
- コリレーションオブジェクトの提供は脅威防御サブスクリプションが必要

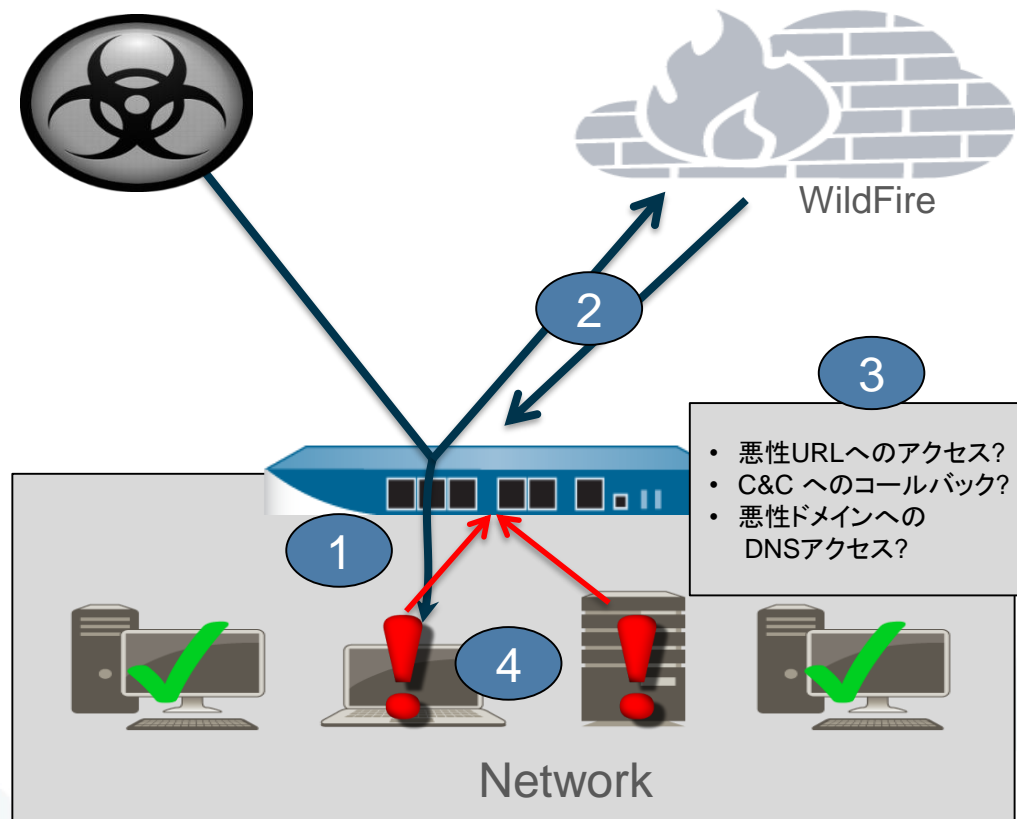
自動相関エンジン



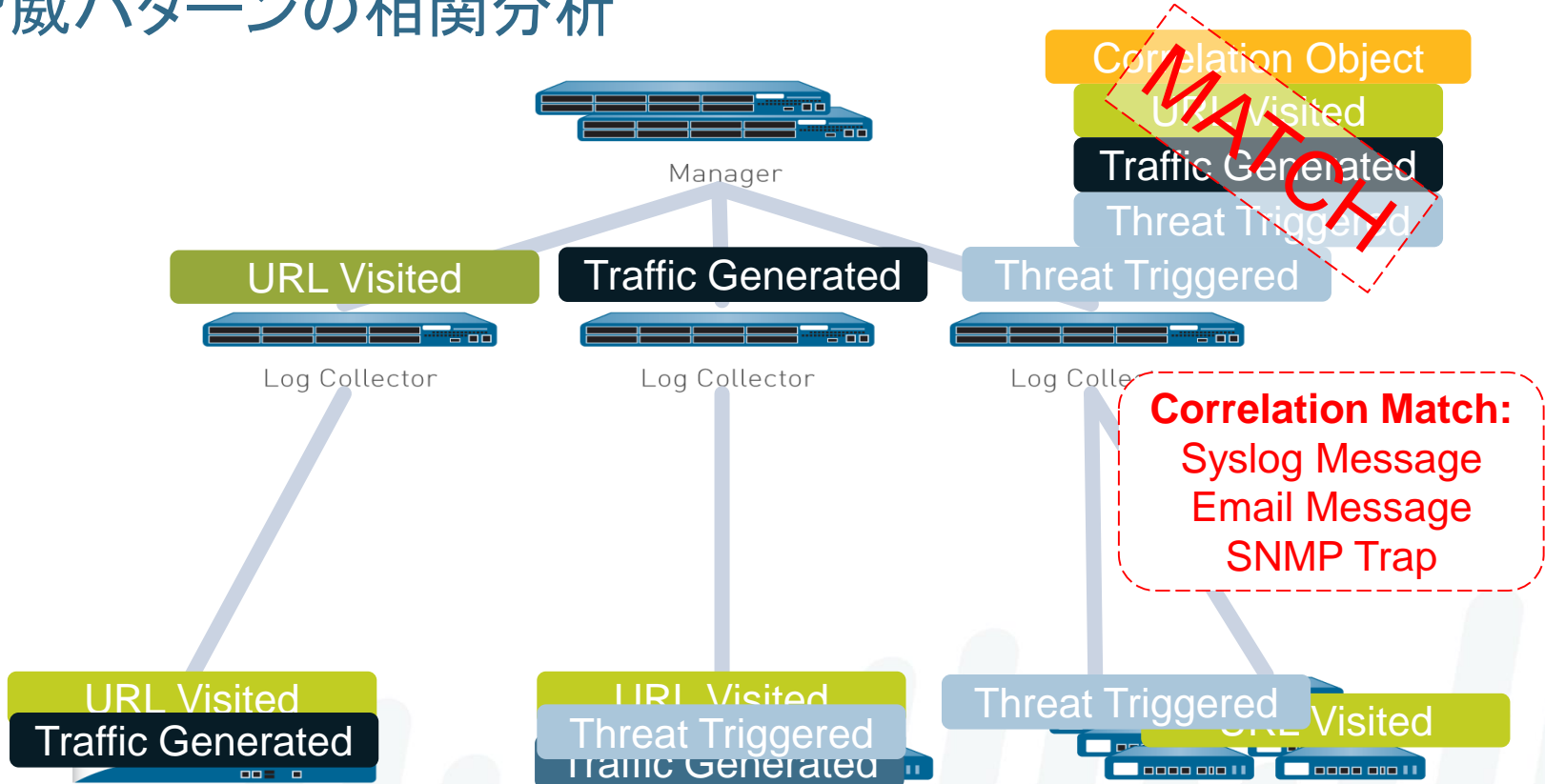
侵害されたホスト

侵害されたホストの発見と迅速な封じ込め

- 1 ユーザーによるマルウェアダウンロード
- 2 WildFire によるマルウェア解析とレポート
- 3 ファイアウォールは、レポートから振る舞いを抽出し、脅威が存在する痕跡を探します。
- 4 該当の振る舞いの相関一致をトリガーしたホストを検出



脅威パターンの相関分析



自動相関エンジン 検知画面(1)

Detailed Log View

Match Information | **Match Evidence**

Log Info | **WildFire Analysis Report**

General

Session ID	1187
Action	alert
Application	web-browsing
Rule	ALLOW_ALL
Category	malicious
Virtual System	QA
Device SN	001801000009
IP Protocol	tcp
Log Action	Panorama
Generated Time	2015/02/23 22:44:22
Receive Time	2015/02/23 22:44:22

Source

User	panqa\bangalore
Address	192.168.62.2
Country	Unknown
Port	80
Zone	Z2
Interface	ethernet1/3

Destination

User	panqa\anantapur
Address	192.168.61.150
Country	Unknown
Port	53768
Zone	Z1
Interface	ethernet1/4.61

Details

Threat/Content Type	wildfire
ID	2000807
Repeat Count	1

Flags

Captive Portal

HTTP Headers

Receive Time	Log	Device Name	Evidence
2015/02/23 22:44:07	traffic	PA-3020-SYSTEM-PA-3020-SYSTEM12	IP: 192.168.62.2, port: 80
2015/02/23 22:44:10	traffic	PA-3020-SYSTEM-PA-3020-SYSTEM12	IP: 192.168.62.2, port: 80
2015/02/23 22:44:22	wildfire	PA-3020-SYSTEM-PA-3020-SYSTEM12	submitter_user_id: panqa\anantapur, File Digest: 790745d6d512102ca07356a579ee79df1d729b96605f487252f981588c2cbaba, cloud: 10.5.100.64
2015/02/23 22:44:24	wildfire	PA-3020-SYSTEM-PA-3020-SYSTEM12	submitter_user_id: panqa\anantapur, File Digest: 790745d6d512102ca07356a579ee79df1d729b96605f487252f981588c2cbaba, cloud: 10.5.100.64

Close

自動相関エンジン 検知画面(2)

The screenshot displays two overlapping windows from the Palo Alto Networks security management interface. The primary window, titled "Detailed Log View", is open to the "Match Evidence" tab. It contains two main sections: "Object Details" and "Match Details".

Object Details:

- Title: WildFire Correlated C2
- ID: 6001
- Detailed Description: This correlation object detects hosts that have received malware detected by WildFire, and have also exhibited command-and-control (C2) network behavior corresponding the detected malware.
- Category: compromised-host

Match Details:

- Match Time: 2015/02/23 22:43:53
- Last Update Time: 2015/02/24 11:14:13
- Title: WildFire Correlated C2
- Severity: **CRITICAL**
- Summary: Host received malicious file (sha256:6241940f8a13fc5098ebc77ea4ca19d095dc4026366f065ab9d975aaf39d350f) and performed associated callbacks, visiting 96 IPs including: 192.168.62.2,192.168.62.2,192.168.62.2,192.168.62.2,192.168.62.2,192.168.62.2

The secondary window, partially visible behind the first, shows the "Destination" tab with the following information:

- User: panqa\anantapur
- Address: 192.168.61.150
- Country: Unknown
- Port: 53768
- Zone: Z1
- Interface: ethernet1/4.61

Below the destination information, there is a "Flags" section with a "Captive Portal" checkbox that is currently unchecked. At the bottom of this window, there is a "Close" button.

The primary window also has a "Close" button at the bottom right.

自動相関エンジンの有効化

- コリレーションオブジェクトをサポートしている、プラットフォームは以下の通りです。
 - PA-3000 シリーズ
 - PA-5000 シリーズ
 - PA-7000 シリーズ
 - 全てのPanorama プラットフォーム
- 各コリレーションオブジェクトを有効・無効に設定可能
 - PAデバイス上のリソースを使用したくない場合はPanorama側で対応が可能
 - 顧客が指定したオブジェクトがあまりにも多くの検知をする場合
- 全てのコリレーションオブジェクトはデフォルトで有効になっている
- 脅威防御ライセンスが必要

WildFire 関連オブジェクト

- WildFire送信ログをベースにした2つの関連オブジェクト
 - **WildFire Correlated C2** -この関連オブジェクトは、WildFireによってマルウェアを検出、また、検出されたマルウェアに対応するコマンド・アンド・コントロール(C2)ネットワークへのアクセスなどの挙動を示したホストを検出します。
 - **WildFire C2** - この関連オブジェクトは、他の場所でネットワーク上のWildFireによって検出されたマルウェアに対応するコマンド・アンド・コントロール(C2)ネットワークへのアクセスなどの挙動を示したホストを検出します。
- これらのオブジェクトの両方がWildFireのレポートを使用し、お客様のネットワーク上において同様の振る舞いを行うホストが存在するかを監視



侵害されたホストの発見

WildFire Report

URL Visited

Traffic Generated

DNS Requests

WildFireによる
マルウェアの分析レポート
を送信

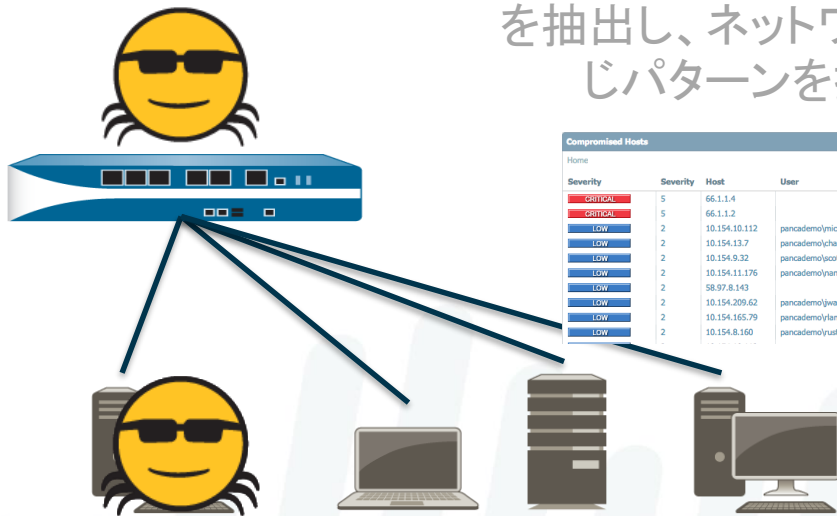
ユーザーがマルウェアを
ダウンロード



マルウェアのコピーを
WildFireに送信
振る舞い分析

ファイアウォールは、
WildFireの報告から振る舞い
を抽出し、ネットワーク内の同
じパターンを探します

相関は、それが元のホストでは
なかった場合でも、サンドボックス
内で見られる同じ挙動を示す
任意のホストから起動されます
マッチします



Severity	Severity	Host	User
CRITICAL	5	66.1.1.4	
CRITICAL	5	66.1.1.2	
LOW	2	10.154.10.112	pancedemo/nichole.white
LOW	2	10.154.13.7	pancedemo/charida.mena
LOW	2	10.154.9.32	pancedemo/scott.ellison
LOW	2	10.154.11.176	pancedemo/nancy.golladay
LOW	2	58.97.8.143	
LOW	2	10.154.209.62	pancedemo/jweah
LOW	2	10.154.165.79	pancedemo/lambert
LOW	2	10.154.8.160	pancedemo/rusty.malkin

Compromised Hosts	
Home	
Severity	
CRITICAL	5
CRITICAL	5
LOW	2
LOW	2
LOW	2
LOW	2
LOW	2
LOW	2
LOW	2
LOW	2

Compromise Activity Sequence 相関 オブジェクト

- この相関オブジェクトは、リモートからの侵害を示すスキャンで始まるまたはアクティビティをプロービング、不正侵入へと進行し、既知の悪質なドメインにコネクタバックしている関与ホストを検出します。
- このオブジェクトは、ネットワーク内の攻撃を受けたホストに基づいています。



Compromise Activity Sequence のアクション



- ホストへの侵入の試み
- ブルートフォースなど

- 次に攻撃者は、より多くのマルウェアをダウンロードするために、脆弱性を悪用

- ホストが侵害されると、攻撃者はコマンドおよび制御のためにコールバックします。

Exploit Kit Activity 相関 オブジェクト

- このオブジェクトは、ネットワーク上のホストをターゲットとするエクスプロイトキットのアクティビティを検出します。エクスプロイトキットは、脆弱性の悪用やマルウェアを検出するシグニチャまたは既知のコマンド・アンド・コントロールのシグニチャのいずれかと組み合わせたシグニチャを、利用しています。



Beacon Detection 相関 オブジェクト

- この相関オブジェクトは、ダイナミックDNSドメインへの複数アクセス、同じサイトから繰り返しファイルのダウンロード、不明なトラフィックの発生、などのコマンド・アンド・コントロール(C2)へのビーコンアクティビティに基づいてホストを検出します。
- これは、私たちの現在のボットネットのレポートに似ています
- これは、ボットネットのレポートがパノラマにも存在することを意味します



GUI – 自動化された関連エンジン

- Monitor tab has new field

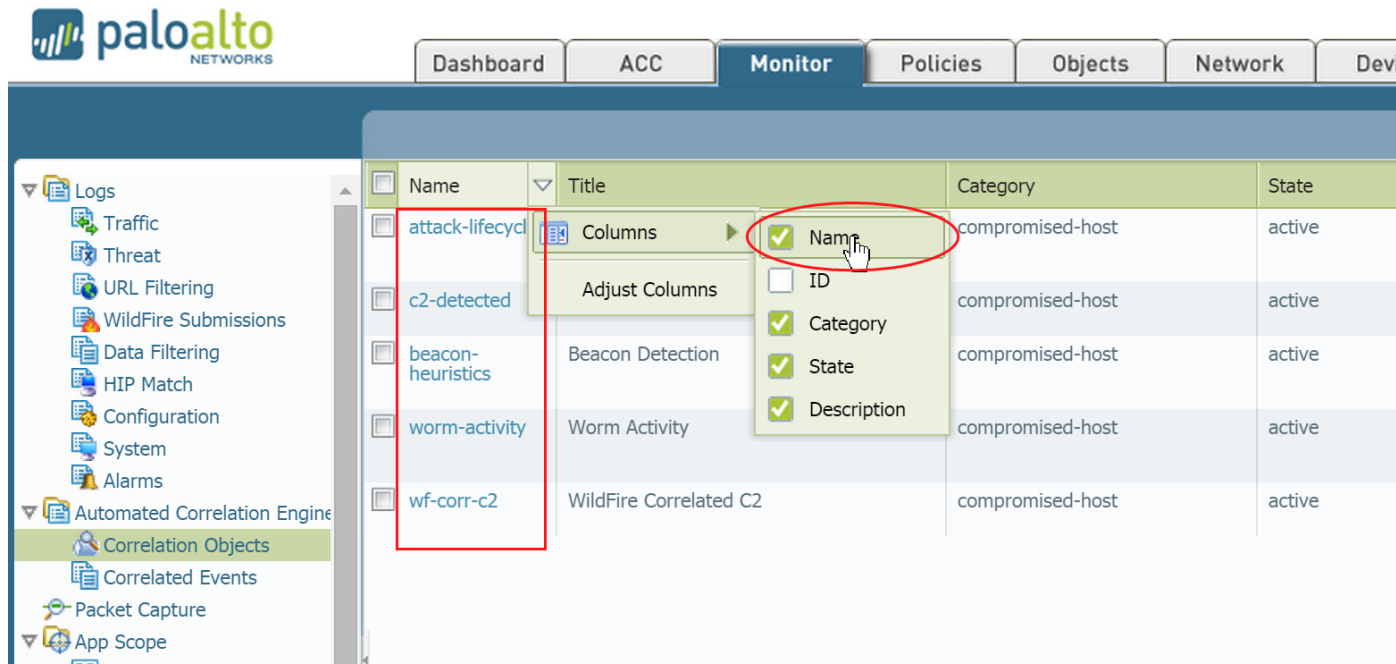
The screenshot shows the Palo Alto Networks GUI interface. The top navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Monitor' tab is active. On the left sidebar, the 'Automated Correlation Engine' section is expanded, with 'Correlation Objects' and 'Correlated Events' highlighted. The main content area displays a table of correlation objects.

Title	Category	State	Description
Compromise Lifecycle	compromised-host	active	This correlation object detects a host involved in a complete attack lifecycle, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
C2 Detected	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Worm Activity	compromised-host	active	This correlation object detects a worm spreading throughout the network by identifying hosts that are targeted by an exploit, perform command-and-control communications, and finally download a known malware variant.
WildFire Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire, and have also exhibited command-and-control (C2) network behavior corresponding to the detected malware.

At the bottom of the table, there are 'Enable' and 'Disable' checkboxes. The 'Enable' checkbox is checked.

GUI – コリレーションオブジェクト(1)

- Name column

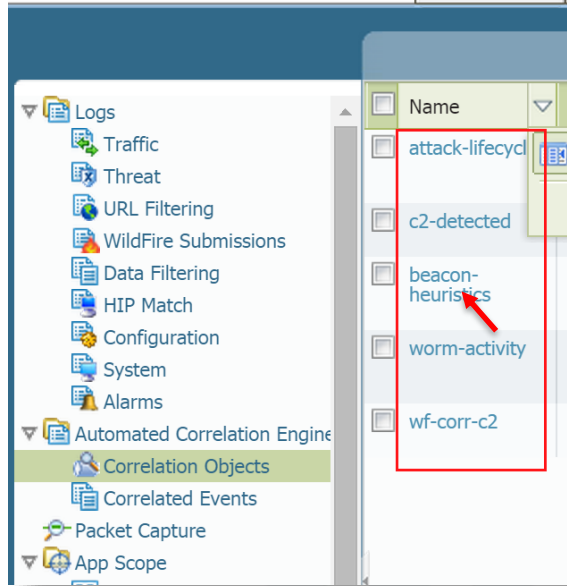


The screenshot shows the Palo Alto Networks GUI with the 'Monitor' tab selected. A table of correlation objects is displayed. The 'Name' column is highlighted with a red box. A context menu is open over the table, showing a list of columns to display. The 'Name' checkbox is highlighted with a red circle.

Name	Title	Category	State
<input type="checkbox"/> attack-lifecycle	Columns	compromised-host	active
<input type="checkbox"/> c2-detected	Adjust Columns	compromised-host	active
<input type="checkbox"/> beacon-heuristics	Beacon Detection	compromised-host	active
<input type="checkbox"/> worm-activity	Worm Activity	compromised-host	active
<input type="checkbox"/> wf-corr-c2	WildFire Correlated C2	compromised-host	active

GUI – コリレーションオブジェクト(2)

Object Details



```
Correlation Object
1 <entry id="6005" name="beacon-heuristics" minver="7.0">
2 <category>compromised-host
3 </category>
4 <description>Beacon Detection
5 </description>
6 <detailed-description>This correlation object detects likely compromised hosts based on activity that resem
7 </detailed-description>
8 <inputs>
9 <input source="opaque" type="botnet.db"/>
10 </inputs>
11 <filters>
12 <filter name="f1" log-type="data">
13 <match>(file_url in '/botnet.db:malware_domain/') and ((threatid eq 52020) or (threatid eq 52060))
14 </match>
15 </filter>
16 <filter name="f2" log-type="url">
17 <match>(url in '/botnet.db:malware_domain/')
18 </match>
19 </filter>
20 <filter name="f3" log-type="data">
21 <match>(file_url in '/botnet.db:recent_domain/') and ((threatid eq 52020) or (threatid eq 52060))
22 </match>
23 </filter>
24 <filter name="f4" log-type="url">
25 <match>(url in '/botnet.db:recent_domain/')
26 </match>
27 </filter>
28 <filter name="f5" log-type="url">
29 <match>(url in '/botnet.db:ddns_domain/')
30 </match>
31 </filter>
32 <filter name="f6" log-type="traffic">
33 <match>app eq "irc"
34 </match>
35 </filter>
36 <filter name="f7" log-type="traffic">
37 <match>(app eq "unknown-tcp") or (app eq "unknown-udp")
38 </match>
39 </filter>
40 <filter name="f8" log-type="data">
41 <match>(category eq "unknown") and ((threatid eq 52020) or (threatid eq 52060))
42 </match>
43 </filter>
44 <filter name="f9" log-type="url">
45 <match>category eq "malware"
46 </match>
```


GUI – 自動化された相関エンジン(1)

- Correlated Events

The screenshot displays the Palo Alto Networks GUI 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 categories like 'Logs', 'Automated Correlation Engine', and 'PDF Reports'. The 'Correlated Events' option is selected. The main content area shows a table of log entries. A red arrow points to the first entry, which is highlighted in blue. The table has columns for Match Time, Update Time, Object Name, Source address, Source User, Severity, and Summary.

Match Time	Update Time	Object Name	Source address	Source User	Severity	Summary
2015/03/12 11:49:39	2015/03/12 11:49:39	Beacon Detection	10.0.0.53		medium	Host has made use of Internet Relay Chat (IRC), a protocol popular with command-and-control activity.

At the bottom of the interface, there is a status bar with 'admin | Logout', 'Displaying logs 1 - 1', '20 per page', and 'DESC' sorting options.

GUI – 自動化された相関エンジン(2)

- Correlated Events Detailed Match Information

The screenshot displays the Palo Alto Networks GUI interface. On the left is a navigation pane with a tree view containing categories like Logs, Automated Correlation Engine, Packet Capture, App Scope, PDF Reports, and Reports. The 'Automated Correlation Engine' > 'Correlated Events' path is selected. The main content area is titled 'Detailed Log View' and has two tabs: 'Match Information' (active) and 'Match Evidence'. Under 'Match Information', there are two sections: 'Object Details' and 'Match Details'. 'Object Details' shows: Title: Beacon Detection, ID: 6005, Detailed Description: This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc., and Category: compromised-host. 'Match Details' shows: Match Time: 2015/03/12 11:49:39, Last Update Time: 2015/03/12 11:49:39, Title: Beacon Detection, Severity: MEDIUM (highlighted in yellow), and Summary: Host has made use of Internet Relay Chat (IRC), a protocol popular with command-and-control activity. A 'Close' button is at the bottom right of the window. The background shows a blurred view of the main logs table.

GUI – 自動化された相関エンジン(3)

■ Correlated Events Detailed Match Evidence

The screenshot shows the Palo Alto Networks GUI with the 'Detailed Log View' window open. The left sidebar shows the navigation menu with 'Correlated Events' selected. The main window is divided into several sections:

- Match Information:** Contains a 'General' tab with the following details:
 - Session ID: 30311
 - Action: allow
 - Action Source: from-policy
 - Application: irc-base
 - Rule: Allow-trust-untrust
 - Session End Reason: tcp-rst-from-client
 - Category: any
 - Virtual System: vsys1
 - Device SN: 001701000018
 - IP Protocol: tcp
 - Log Action: traffic
 - Generated Time: 2015/03/12 11:49:39
 - Start Time: 2015/03/12 11:49:37
 - Receive Time: 2015/03/12 11:49:39
 - Elapsed Time(sec): 15
- Match Evidence:** Contains two sub-sections:
 - Source:**
 - User: User
 - Address: 10.0.0.53
 - Country: 10.0.0.0-10.255.255.255
 - Port: 1424
 - Zone: trust
 - Interface: ethernet1/11
 - Destination:**
 - User: User
 - Address: 64.161.255.2
 - Country: US
 - Port: 6667
 - Zone: untrust
 - Interface: ethernet1/12
- Details:**
 - Bytes: 901
 - Bytes Received: 0
 - Bytes Sent: 901
 - Repeat Count: 1
 - Packets: 15
 - Packets Received: 0
 - Packets Sent: 15
- Flags:** A list of checkboxes for various flags, all of which are currently unchecked:
 - Captive Portal
 - Proxy Transaction
 - Decrypted
 - Packet Capture
 - Dummy Direction
 - Client to Server
 - Server to Client
- Log Links:** A table at the bottom showing related log entries:

Receive Time	Log	Device Name	Evidence
2015/03/12 11:49:39	traffic	PA-3050	Application: irc-base
2015/03/12 13:11:01	traffic	PA-3050	Application: irc-base
2015/03/12 13:12:01	traffic	PA-3050	Application: irc-base

