# 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.*

paloalto NETWORKS®
the enterprise security company™

# 脅威の可視化とすぐに実用可能なデータの提供

レスポンスタイムの削減

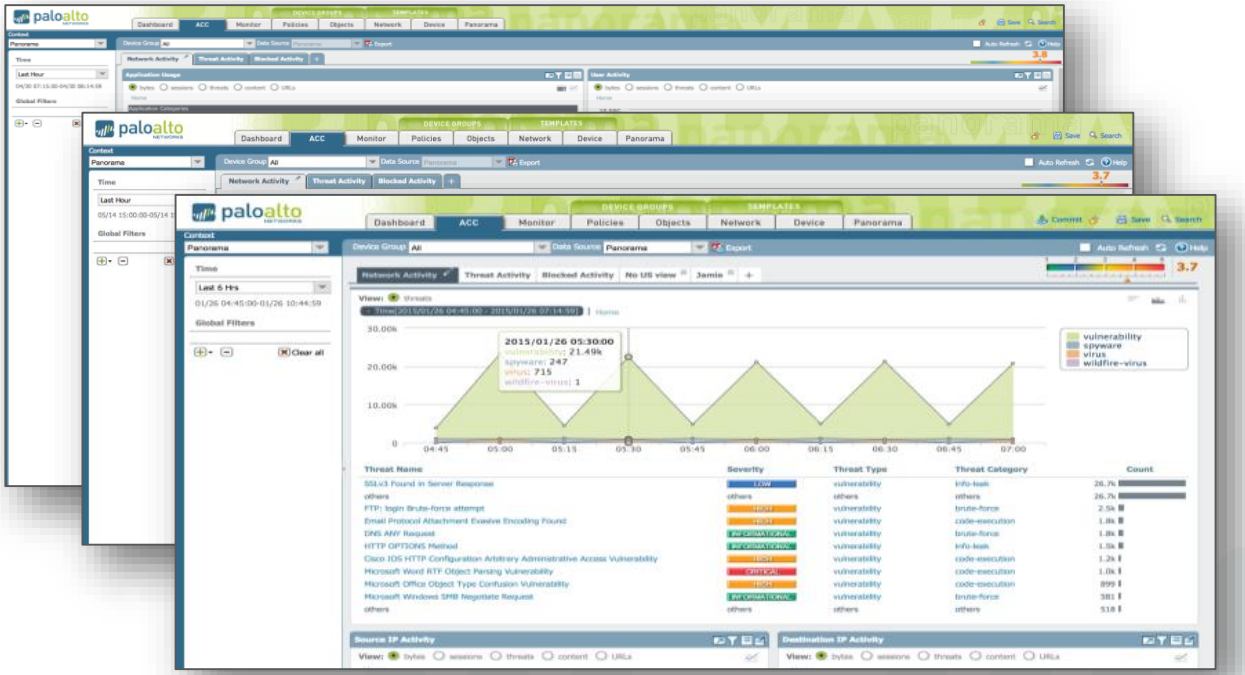
- タブ形式で直感的なビジュアル·ディスプレイとウィジェットを持つ高度にインタラクティブなユーザーインターフェイス
- 数回のクリックで重要な情報を表示
- データの合理化と直感的な管理性
- 一意の脅威に対する迅速なレスポンスが可能

# アプリケーションコマンド･センター（ACC）機能強化

レスポンスタイムの削減

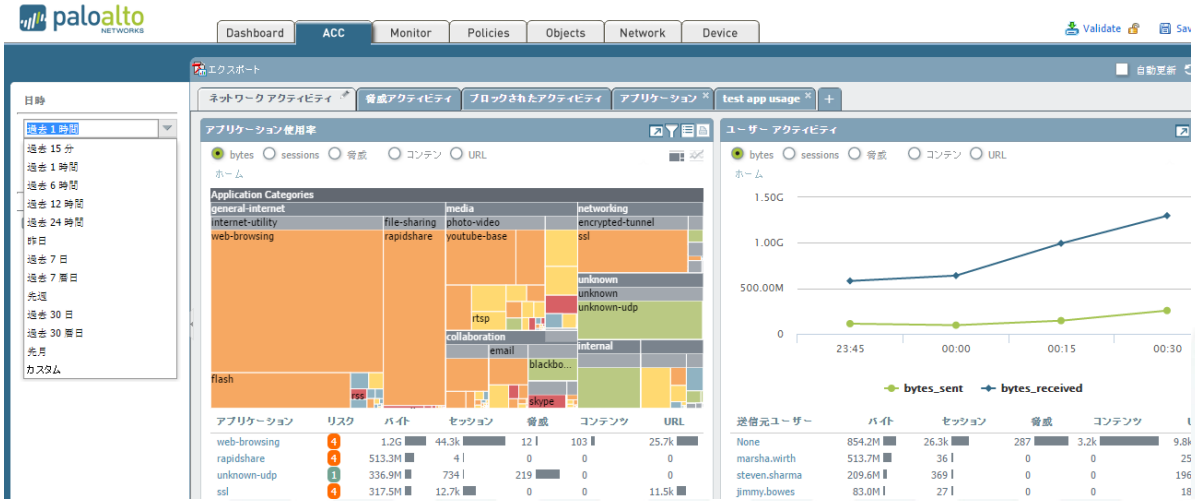
- インタラクティブに高度なカスタマイズが可能
- アプリケーション利用状況とユーザーアクティビティの可視化
- 送信元及び宛先のジオロケーション（国）の認識
- ネットワーク利用状況、脅威レベルの把握
- ドリルダウン機能により詳細調査が容易に



# 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

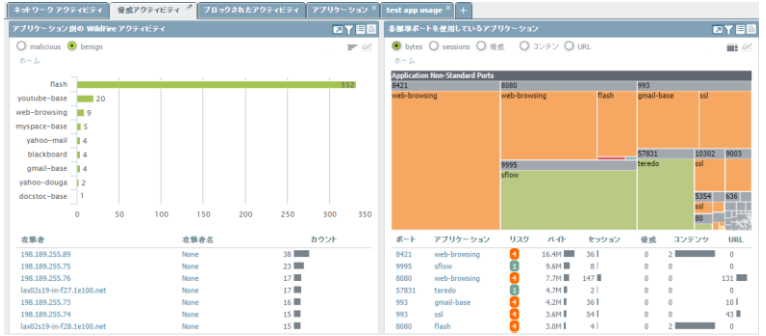
- タブ“ネットワークアクティビティ”は指定した時間帯における下記項目の利用率を多い順に表示
  - アプリケーション
  - ユーザー
  - 送信元、宛先　IP・国
  - ルールの使用率

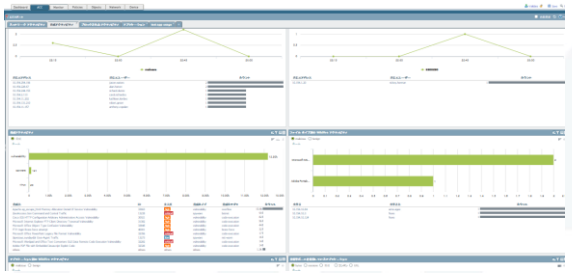


# 2. ACC タブ ”脅威アクティビティ” 脅威発生状況の表示と把握

- 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

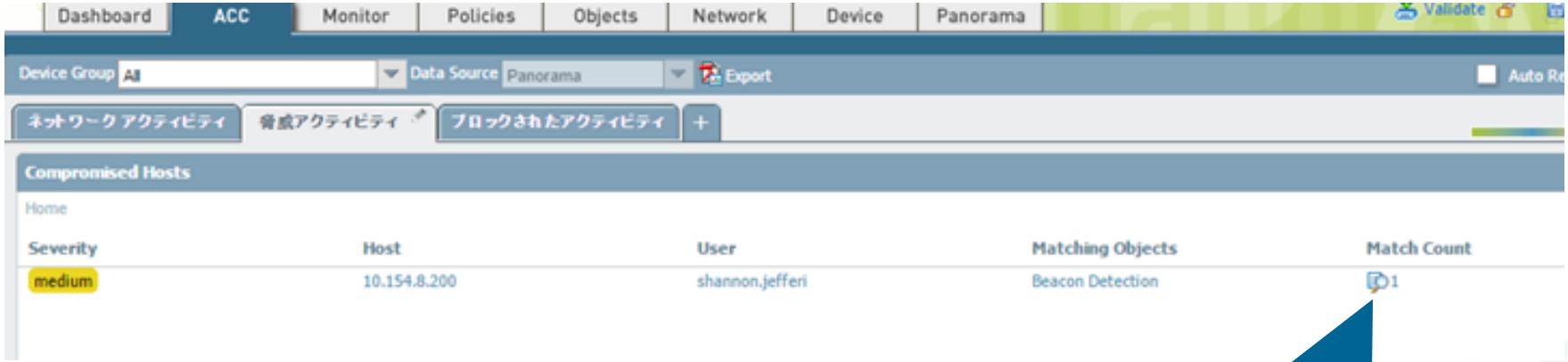




# 2. ACC タブ　”脅威アクティビティ”
# 侵入（侵害）されたホストの表示と把握（1）

- 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

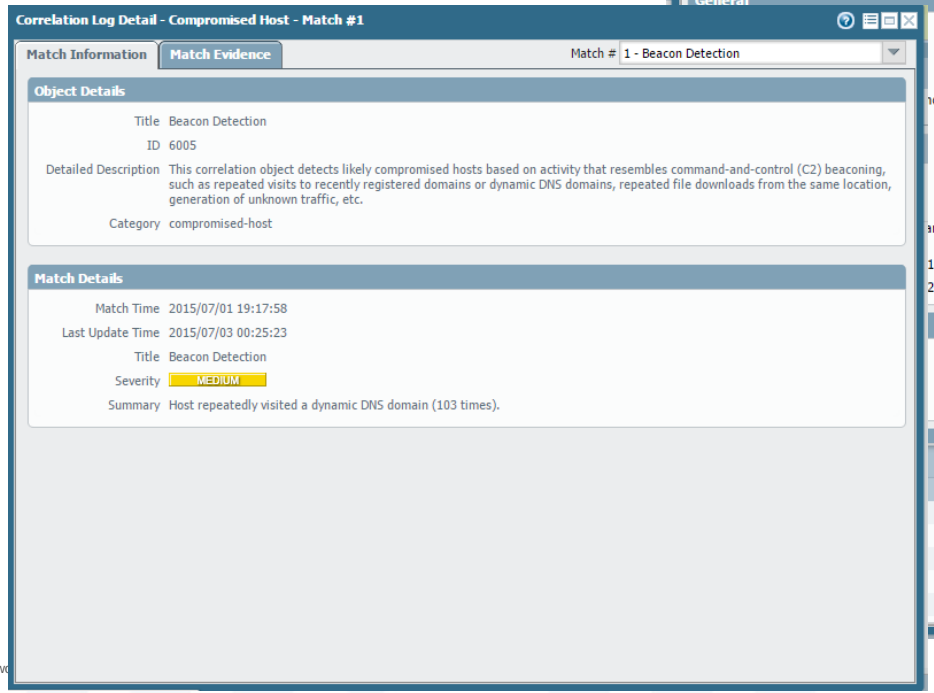


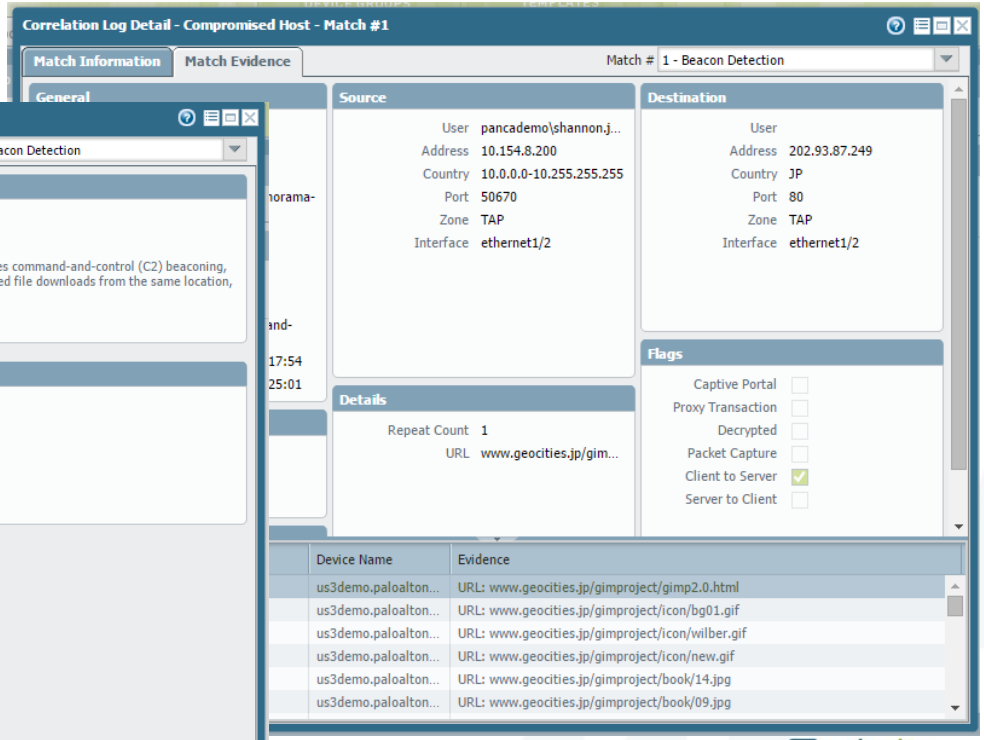

詳細情報へドリルダウン

# 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

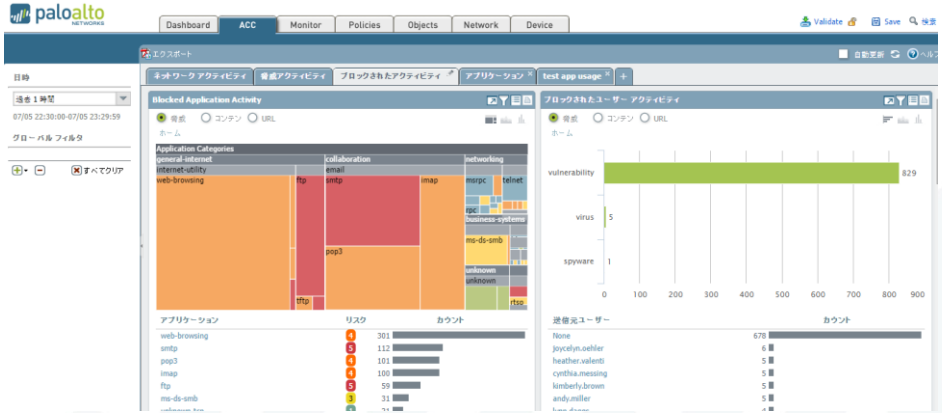


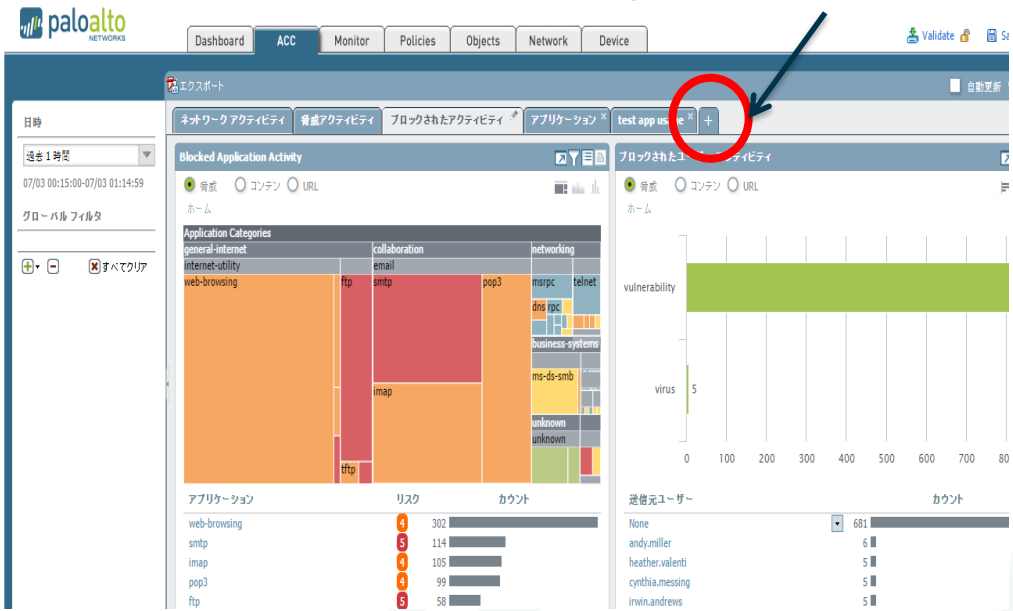
# 3. ACC タブ ”ブロックされたアクティビティ” 防御状況の表示と把握

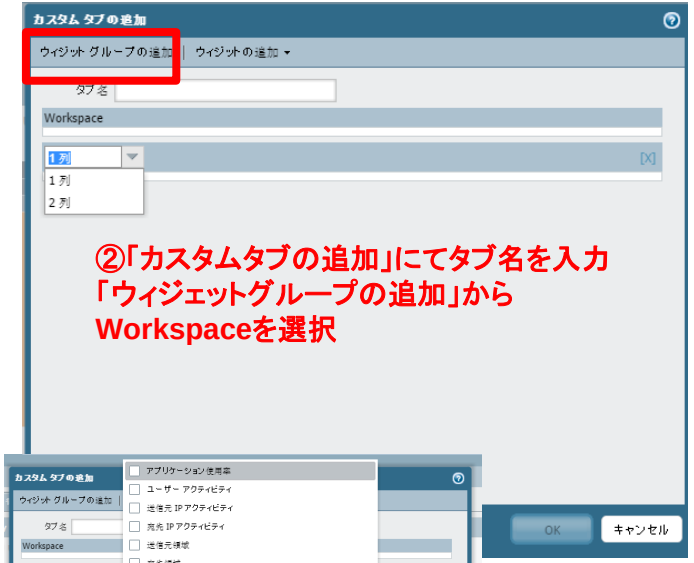
- タブ“ブロックされたアクティビティ”は指定した時間帯における下記項目の防御状況を表示
  - ブロックされたアプリケーションアクティビティ
  - ブロックされたユーザーアクティビティ
  - ブロックされた脅威
  - ブロックされたコンテンツ
  - アクティビティをブロックしている セキュリティポリシー



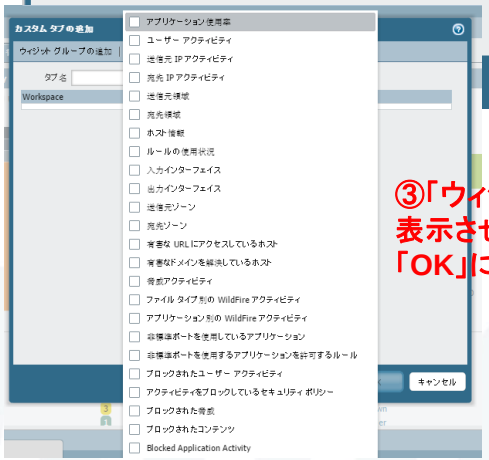

 

# 4. ACC カスタムタブの作成と追加




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




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

# ACC「日時」情報表示の変更

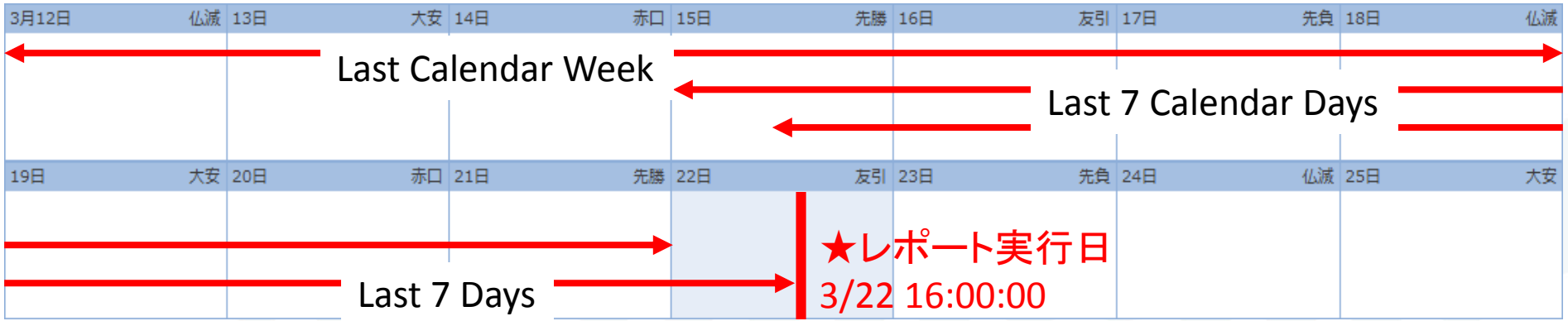
- 表示する情報の時間帯を指定することが可能
  - Last 15 Minutes　過去15分の情報を表示
  - Last Hour　過去1時間の情報を表示
  - Last 6 Hrs　過去6時間の情報を表示
  - Last 12 Hrs　過去12時間の情報を表示
  - Last 24 Hrs　過去24時間の情報を表示
  - Last Calendar Day　前日の情報を表示
  - Last 7 Days　過去7日の情報を表示（次スライド参照）
  - Last 7 Calendar Days　過去7暦日の情報を表示（次スライド参照）
  - Last Calendar Week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

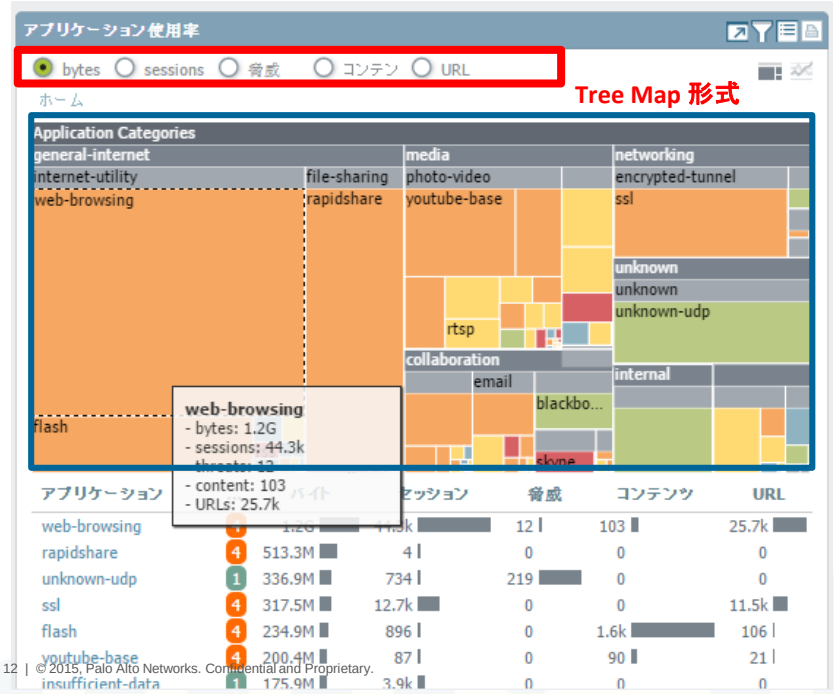
| | | |
|---|---|---|
| Last 7 Days | 過去7日 | 2013/03/15 15:59:59<br>2013/03/22 16:00:00 |
| Last 7 Calendar Days | 過去7暦日 | 2013/03/15 – 2-12/03/21 |
| Last Calendar Week | 先週 | 2013/03/12 – 2-12/03/18 |

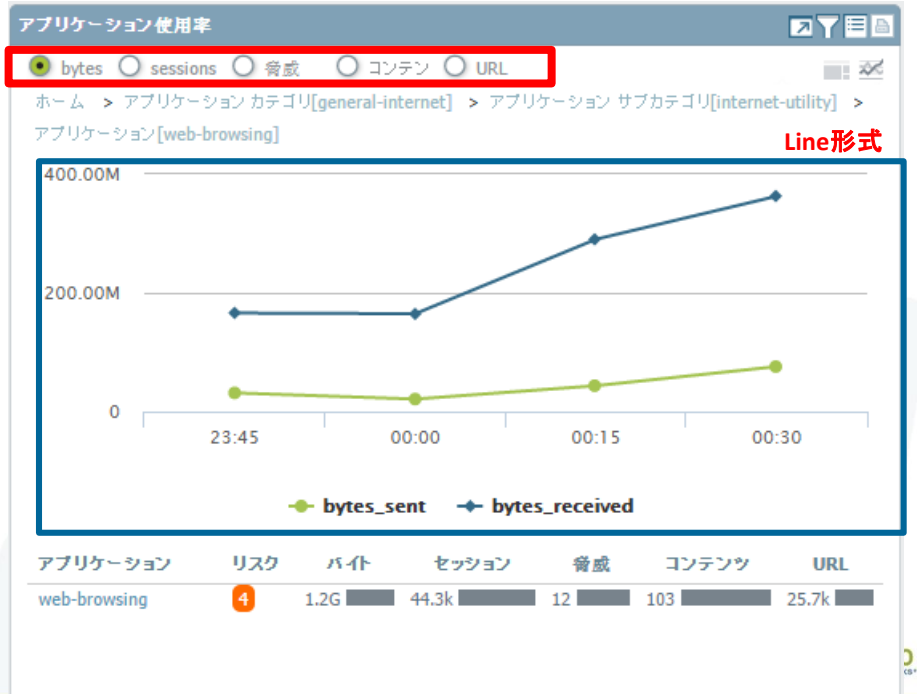


# ACC　表示情報のソート、グラフの切り替え

- 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



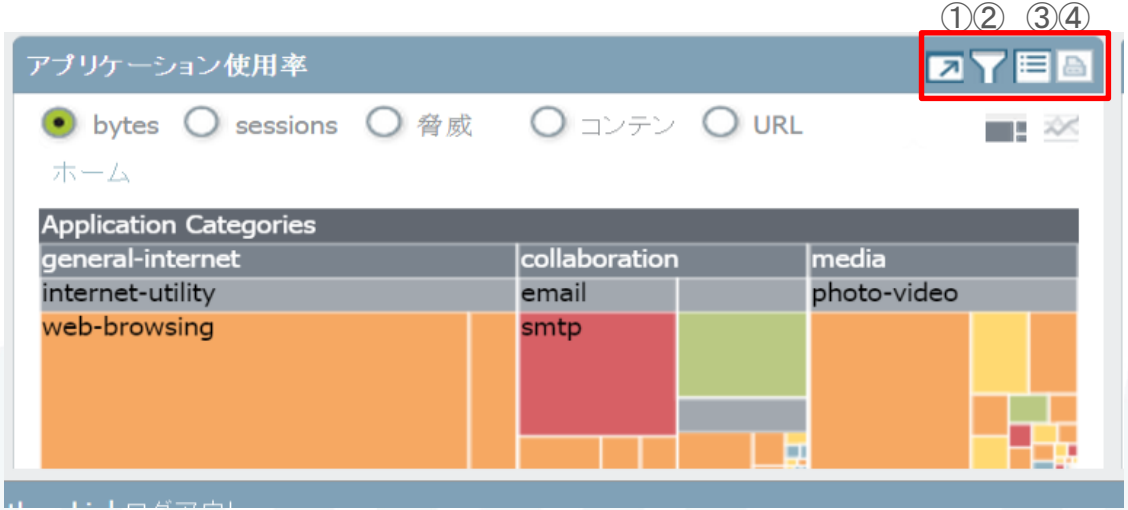
# ACC　各ウィジェットの操作

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 ログへジャンプ・・・ウィジェットから対象ログ画面へ遷移

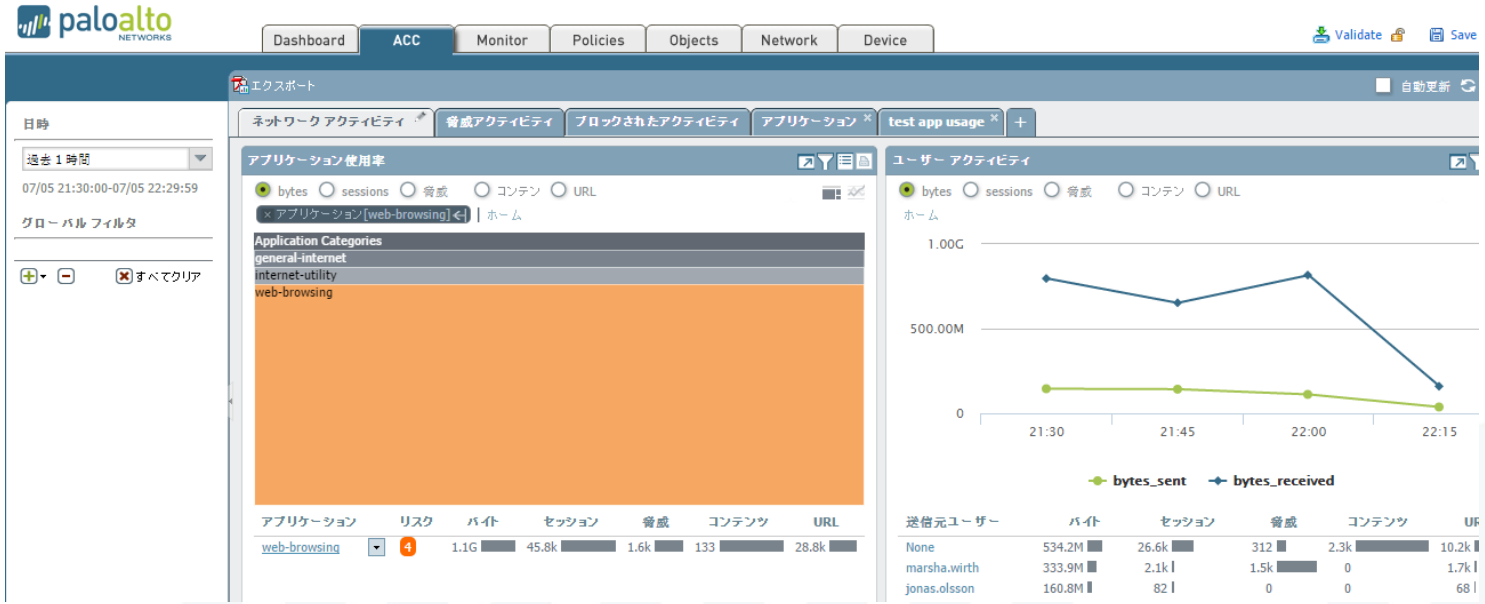
④ エクスポート・・・ウィジェットに表示されている情報のエクスポート



# ACC　表示情報のフィルタリング（ウィジェット単位）

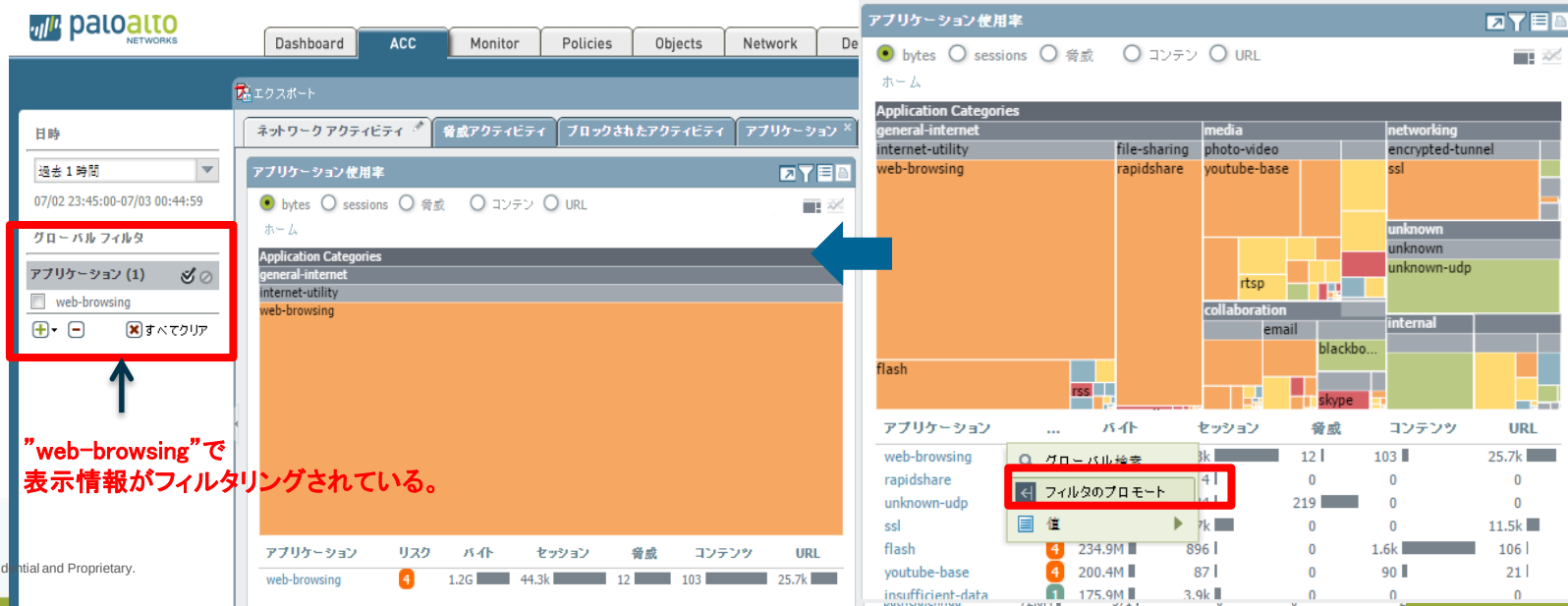
- 各ウィジェット表示情報をクリックし、調査に必要な情報を迅速に抽出
  - （例）「アプリケーション使用率」一覧から”web-browsing”の情報のみを抽出
    - タブ内の他のウィジェットには反映されない



# 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




 | 

# 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
該当時間帯の
詳細情報表示

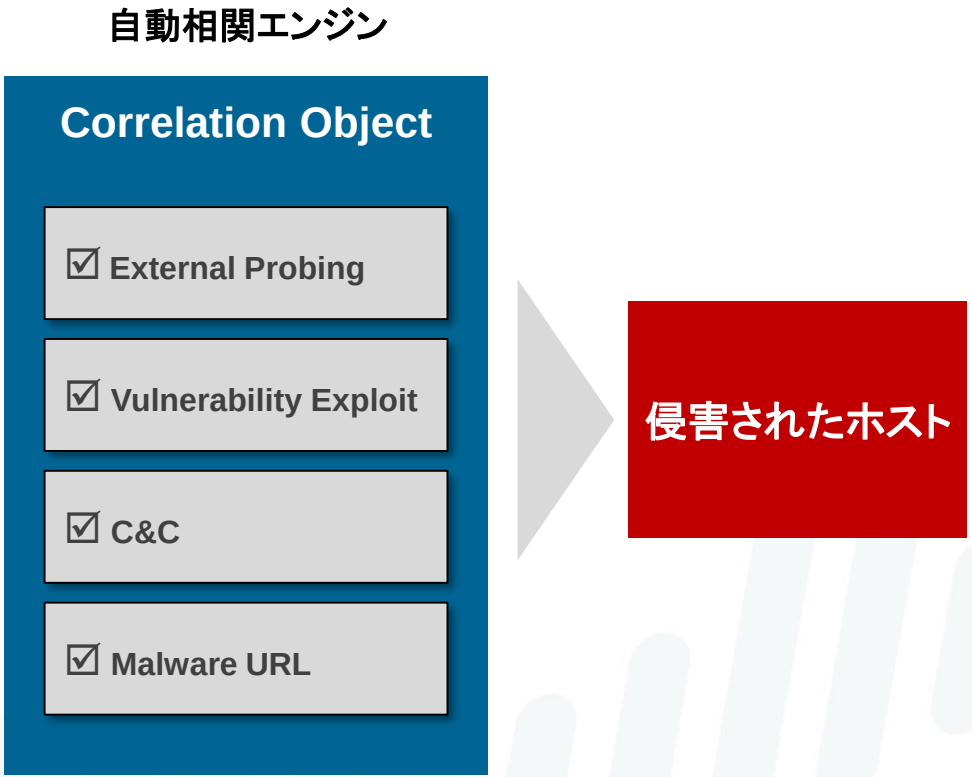
# 自動相関（Automatic Correlation) エンジン

*PAN-OS 7.0*

paloalto NETWORKS®
the enterprise security company™

# 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

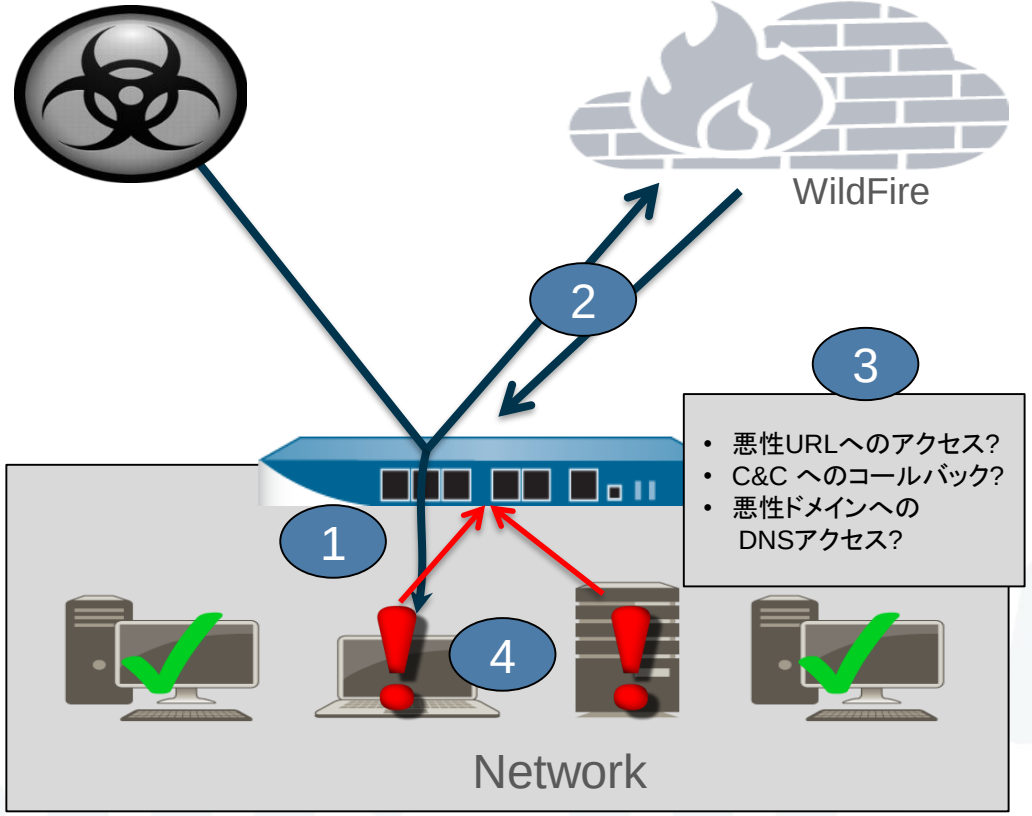


# 侵害されたホストの発見と迅速な封じ込め

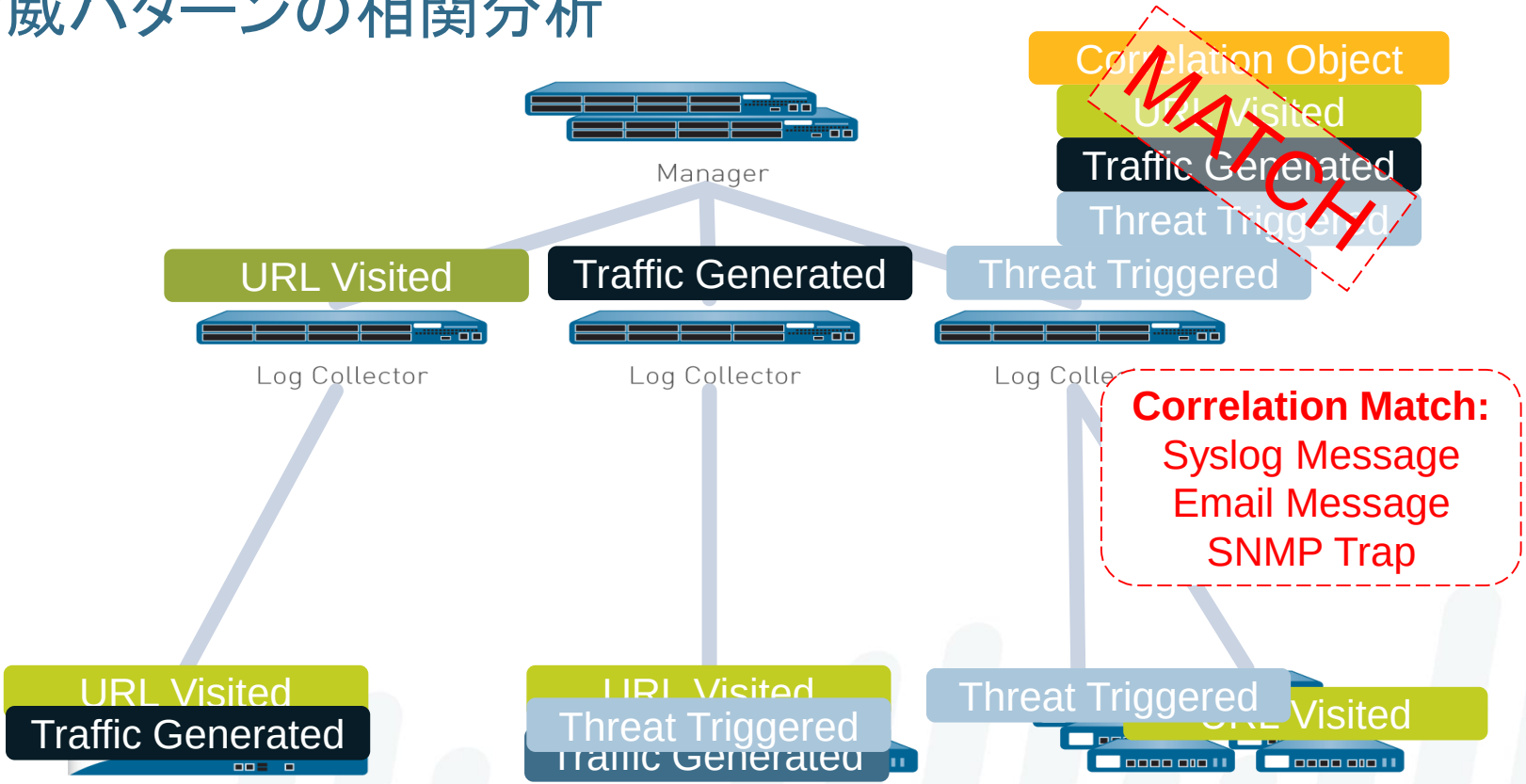
未知脅威の発見

1. ユーザーによるマルウエアダウンロード
2. WildFire によるマルウエア解析とレポート
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



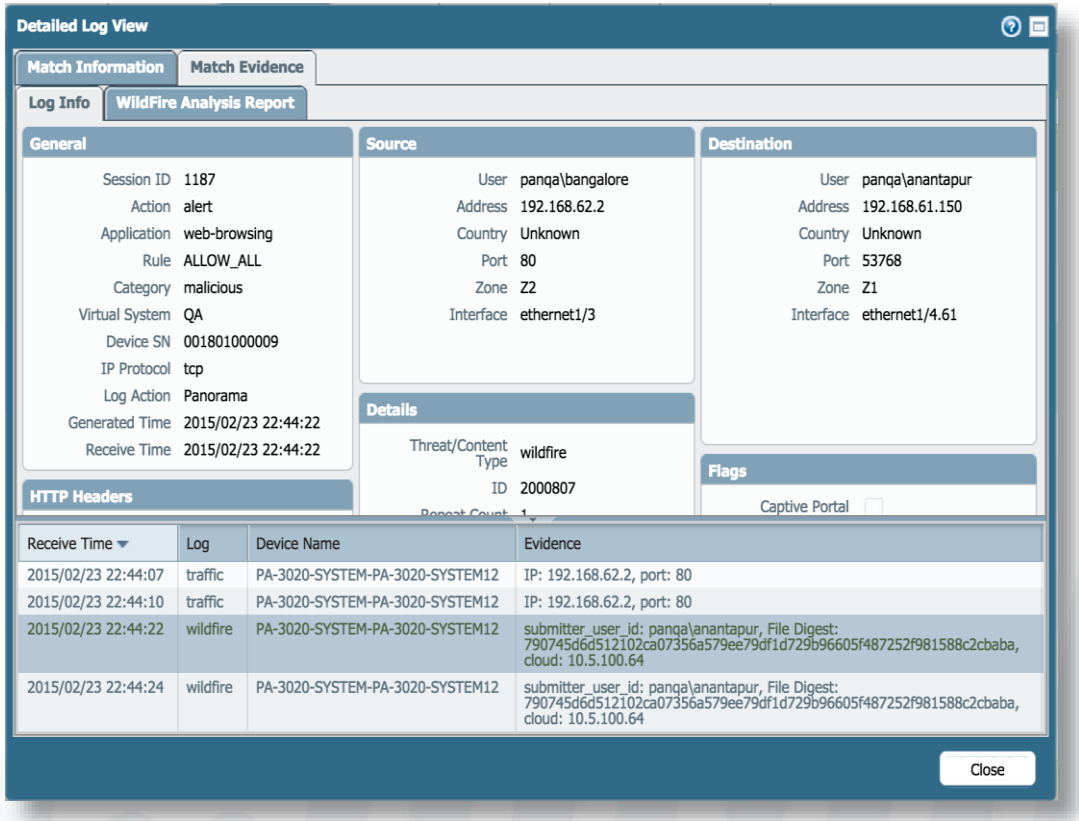

 

# 脅威パターンの相関分析



# 自動相関エンジン　検知画面（1）



# 自動相関エンジン　検知画面（2）

# 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 相関オブジェクト

- WildFire送信ログをベースにした2つの相関オブジェクト
  - **WildFire Correlated C2 -**この相関オブジェクトは、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 -** この相関オブジェクトは、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

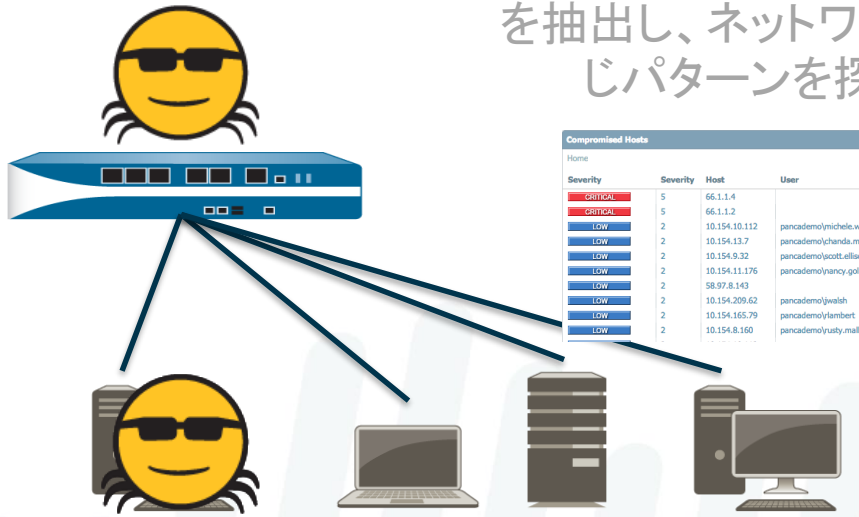
WildFireによる
マルウエアの分析レポート
を送信

ユーザーがマルウエアを
ダウンロード

マルウエアのコピーを
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




Compromised Hosts
Home
Severity
CRITICAL
CRITICAL
LOW
LOW
LOW
LOW
LOW
LOW
LOW
LOW

# 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ト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。

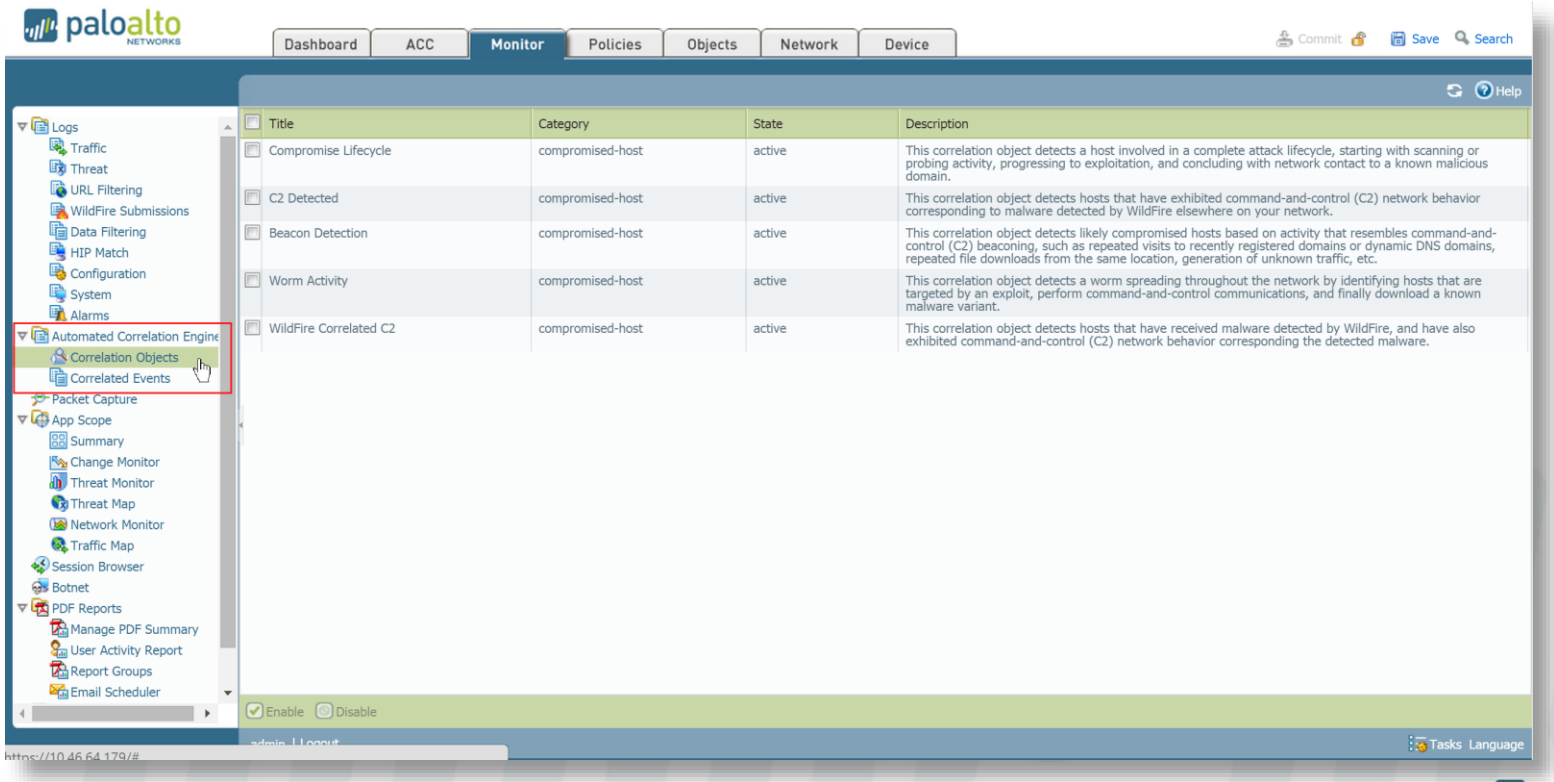
# Beacon Detection 相関 オブジェクト

- 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 – 自動化された相関エンジン

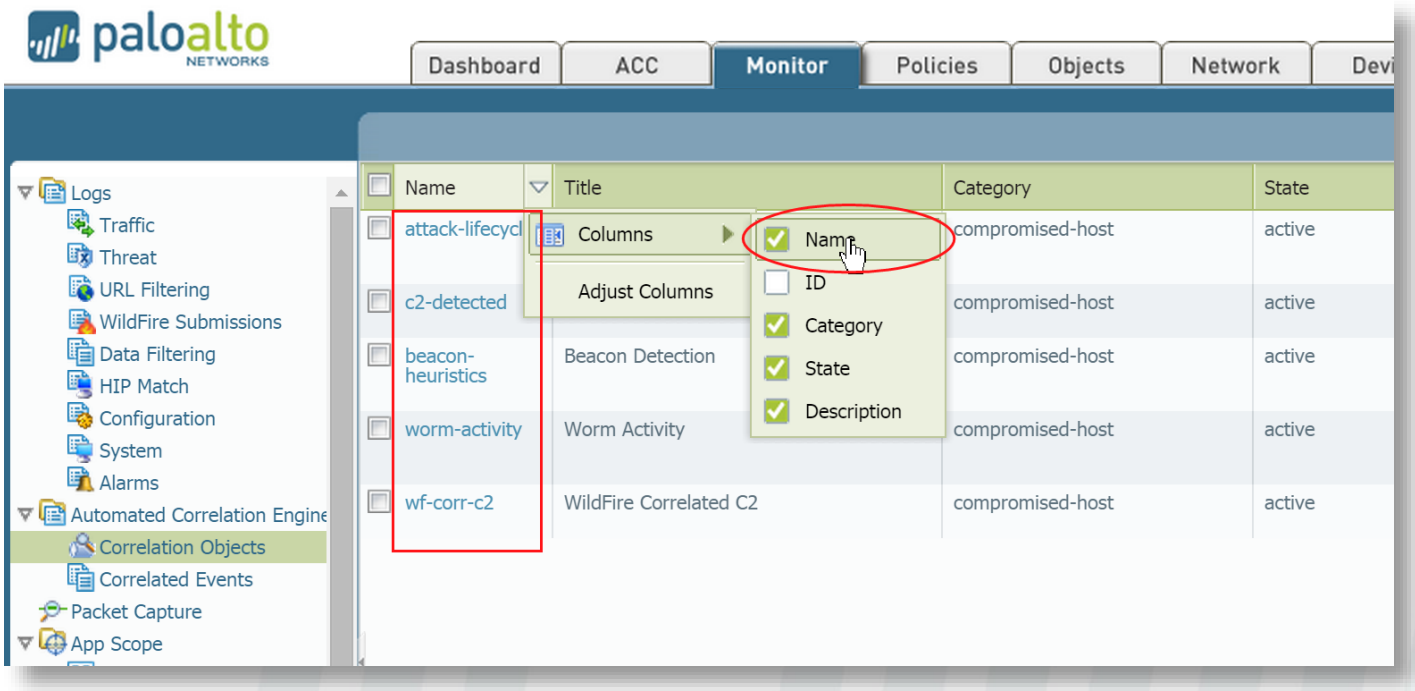
- Monitor tab has new field



# GUI – コリレーションオブジェクト（1）

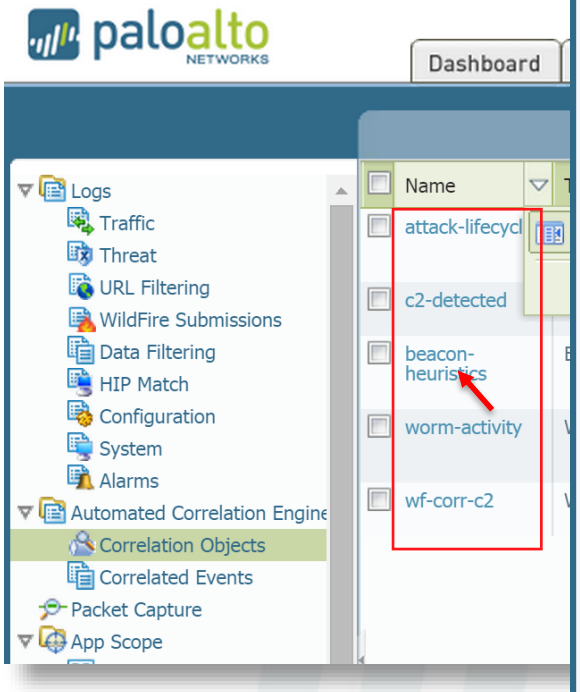
- Name column



# GUI – コリレーションオブジェクト（2）

- Object Details



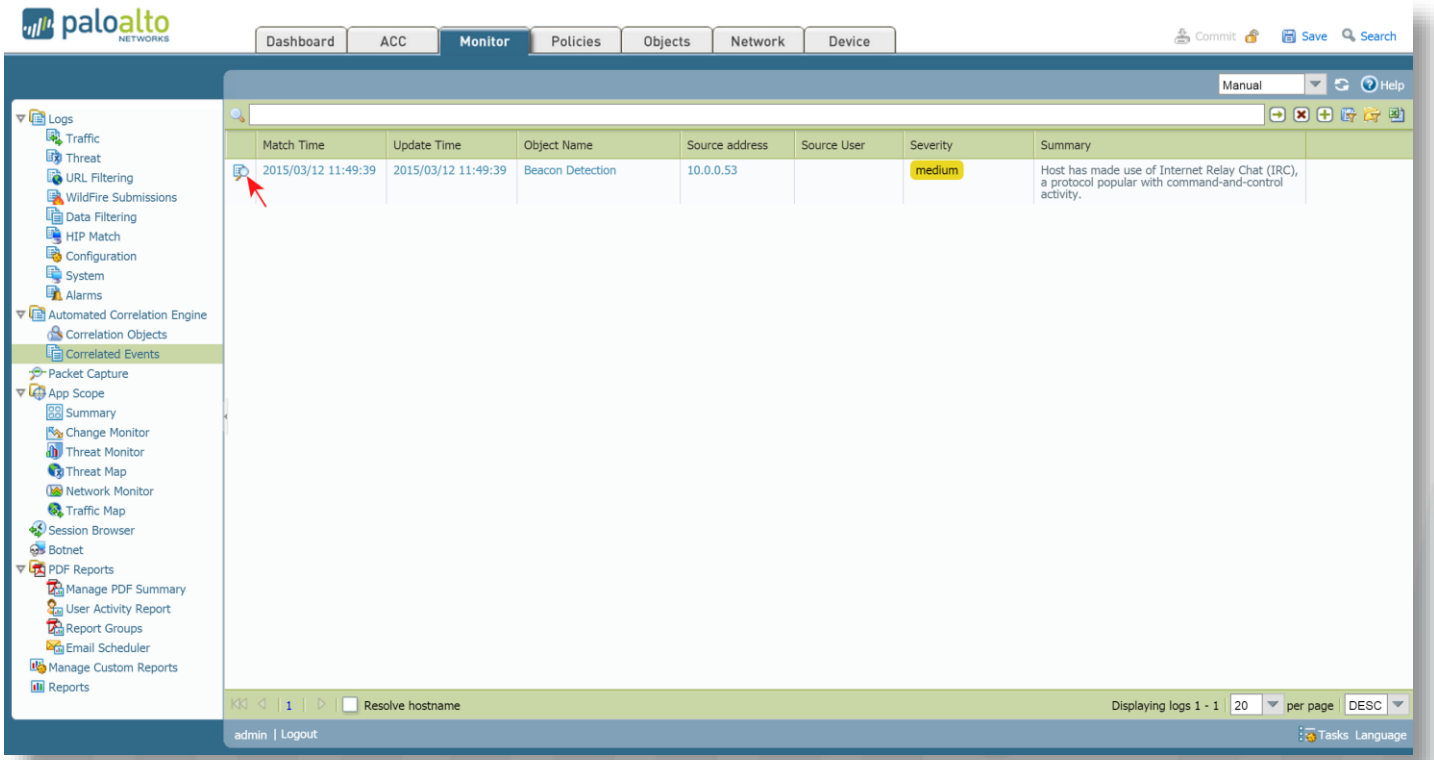

**Correlation Object**

```
<entry id="6005" name="beacon-heuristics" minver="7.0">
  <category>compromised-host
  </category>
  <description>Beacon Detection
  </description>
  <detailed-description>This correlation object detects likely compromised hosts based on activity that resem
    </detailed-description>
  <inputs>
    <input source="opaque" type="botnet.db"/>
  </inputs>
  <filters>
    <filter name="f1" log-type="data">
      <match>(file_url in '/botnet.db:malware_domain/') and ((threatid eq 52020) or (threatid eq 52060))
      </match>
    </filter>
    <filter name="f2" log-type="url">
      <match>(url in '/botnet.db:malware_domain/')
      </match>
    </filter>
    <filter name="f3" log-type="data">
      <match>(file_url in '/botnet.db:recent_domain/') and ((threatid eq 52020) or (threatid eq 52060))
      </match>
    </filter>
    <filter name="f4" log-type="url">
      <match>(url in '/botnet.db:recent_domain/')
      </match>
    </filter>
    <filter name="f5" log-type="url">
      <match>(url in '/botnet.db:ddns_domain/')
      </match>
    </filter>
    <filter name="f6" log-type="traffic">
      <match>app eq "irc"
      </match>
    </filter>
    <filter name="f7" log-type="traffic">
      <match>(app eq "unknown-tcp") or (app eq "unknown-udp")
      </match>
    </filter>
    <filter name="f8" log-type="data">
      <match>(category eq "unknown") and ((threatid eq 52020) or (threatid eq 52060))
      </match>
    </filter>
    <filter name="f9" log-type="url">
      <match>category eq "malware"
```

# GUI – 自動化された相関エンジン（1）

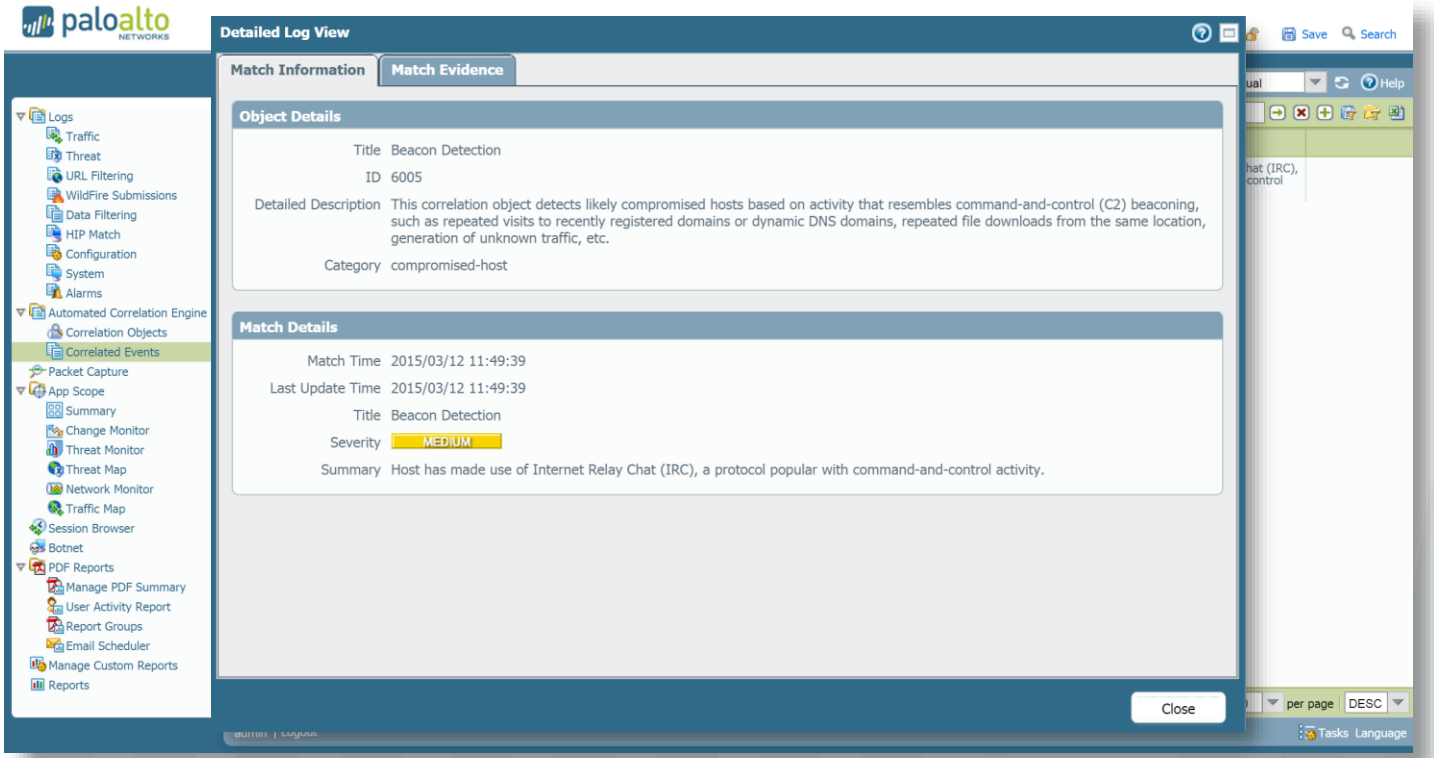
- Correlated Events



# GUI – 自動化された相関エンジン（2）

- Correlated Events Detailed Match Information



# GUI – 自動化された相関エンジン（3）

- Correlated Events Detailed Match Evidence