PAユーザ必聴！
次世代ファイアウォールの運用の方法
トラブルシューティング

パロアルトネットワークス株式会社

May 2019

本日の目的

1. 調査の基本であるACC・Monitorの使い方を学ぶ

2. ウィルスや脅威を発見した際の一次対応方法について学ぶ
   - 導入後のお客様からの質問に対する対応
   - SLR実施時の詳細確認等のため
   - 各ツールの基本的な使い方を理解する

3. CSPアカウントについて学ぶ
   - CSPアカウント
   - デモサイト・CSPへのアクセスについて

Agenda

1. ACCとMonitorについて
2. 切り分けに利用するサービス
    - ① パロアルトネットワークスが提供するサービス
    - ② その他外部サービス
3. 検知時の対応方法
    - ① 脆弱性を狙った攻撃検出時の切り分け例
    - ② ウィルス検出時の切り分け例
    - ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. まとめ
6. 参考情報
    - ① デモサイトについて
    - ② NextWaveパートナー制度について

1. ACCとMonitorについて

2. 切り分けに利用するサービス
    - ① パロアルトネットワークスが提供するサービス
    - ② その他外部サービス
3. 検知時の対応方法
    - ① ウィルス検出時の切り分け例
    - ② 攻撃検出時の切り分け例
    - ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. まとめ
6. 参考情報
    - ① デモサイトについて
    - ② NextWaveパートナー制度について

1. ACCとMonitorについて

PAシリーズのGUI上でログを確認するための画面

① ACC（Application Commands Center)

- NWアクティビティに関する情報をグラフィカルに表示

NWの利用状況を俯瞰し、脅威や想定外の通信をあぶり出す

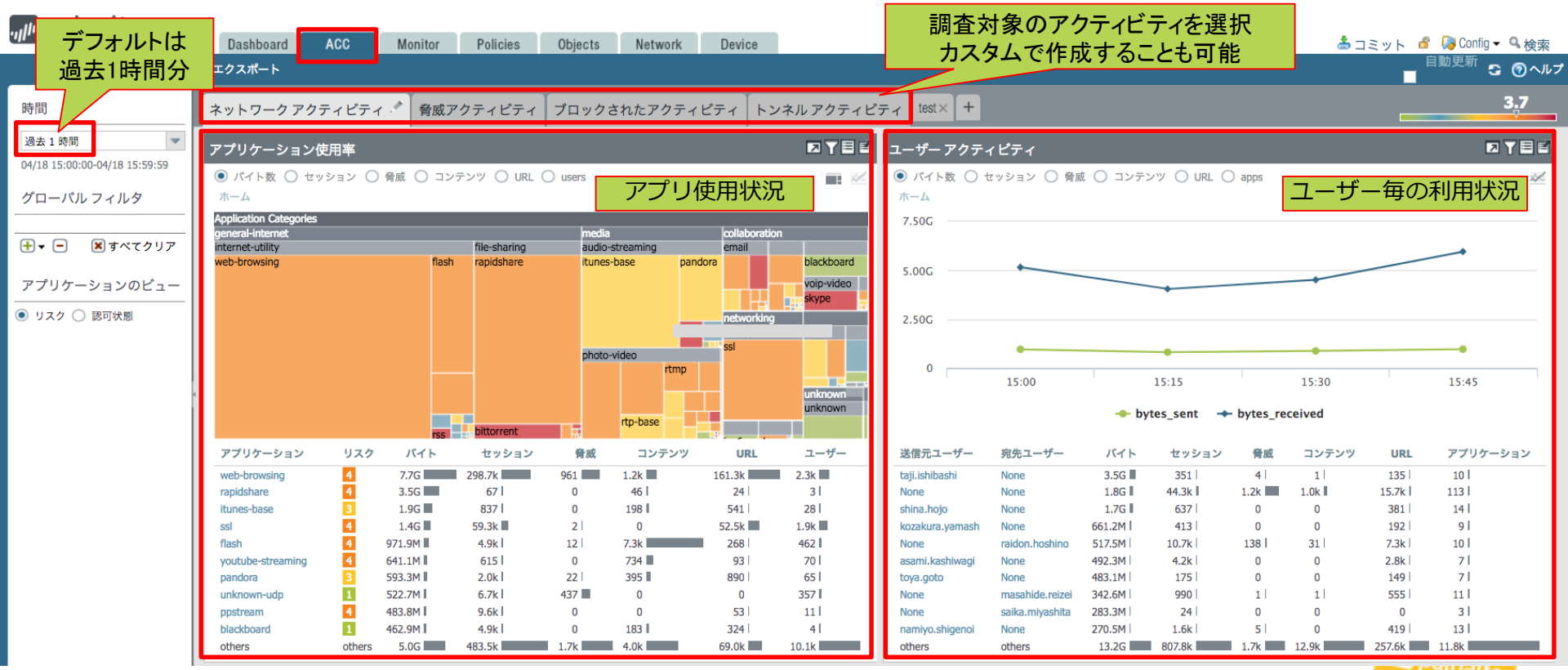
② Monitor

- Logs : Trafficログ、Threatログ等を詳細なログを表示
- App Scope : 直近のNW状況をグラフ表示
- Packet Capture : PA単体でパケットキャプチャ
- PDFレポート : 各種レポートの表示・作成

通信の詳細を調査する際に利用

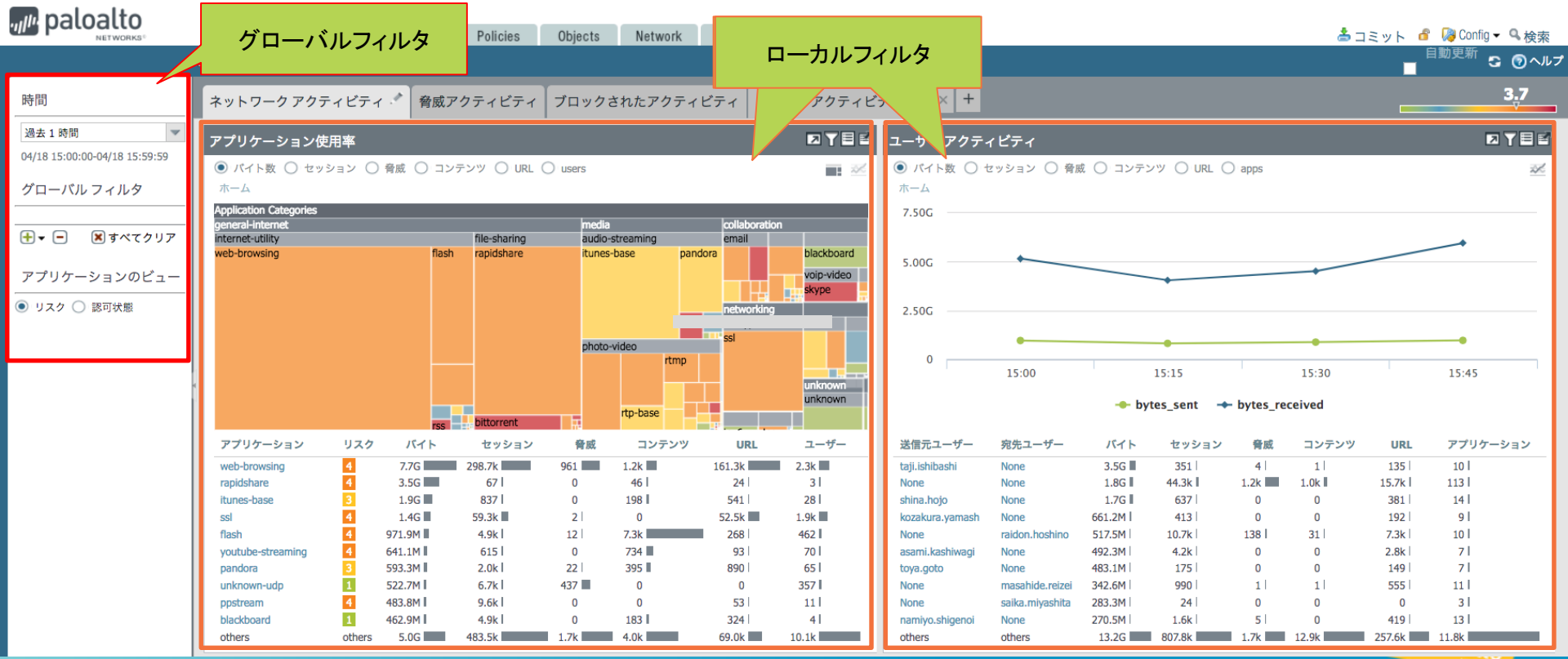
① ACC「概要」

→ ネットワーク、脅威、ポリシーでブロックした通信、GRE等のトンネル通信のアクティビティをグラフィカルに表示



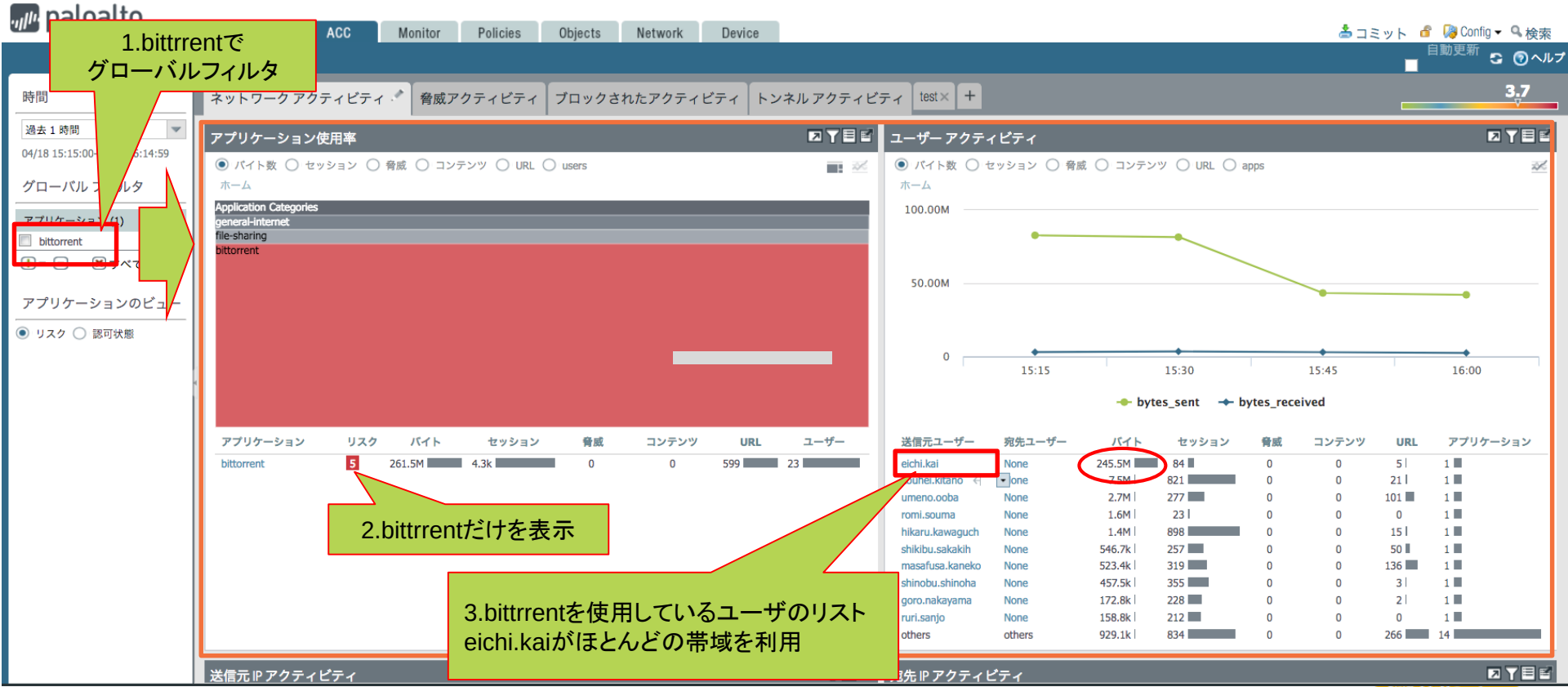
① ACC「グローバルフィルタとローカルフィルタ」

→ ローカルフィルタとグローバルフィルタがあり、どちらもマウスクリックのみでフィルタリングが可能（主にグローバルフィルタを利用）



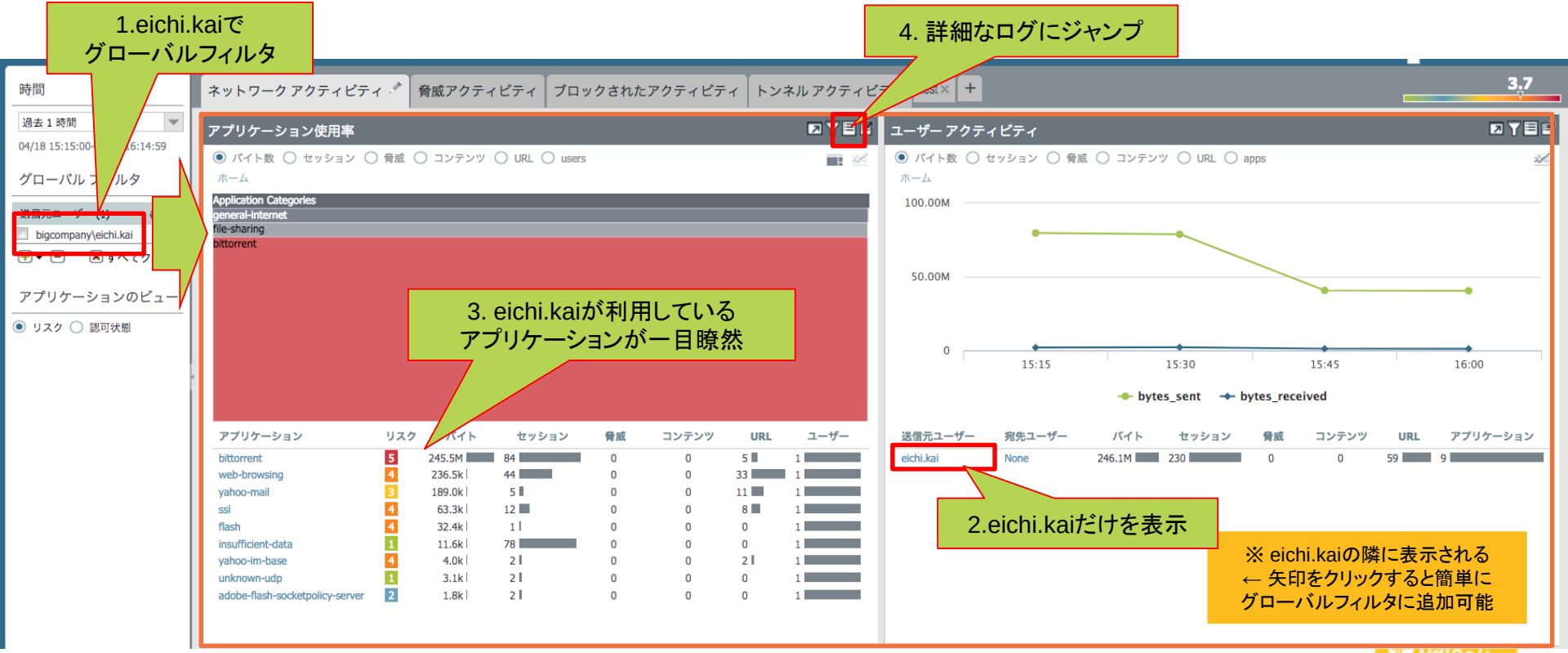
① ACC「グローバルフィルタ 1」

→ アプリケーションでグローバルフィルタ



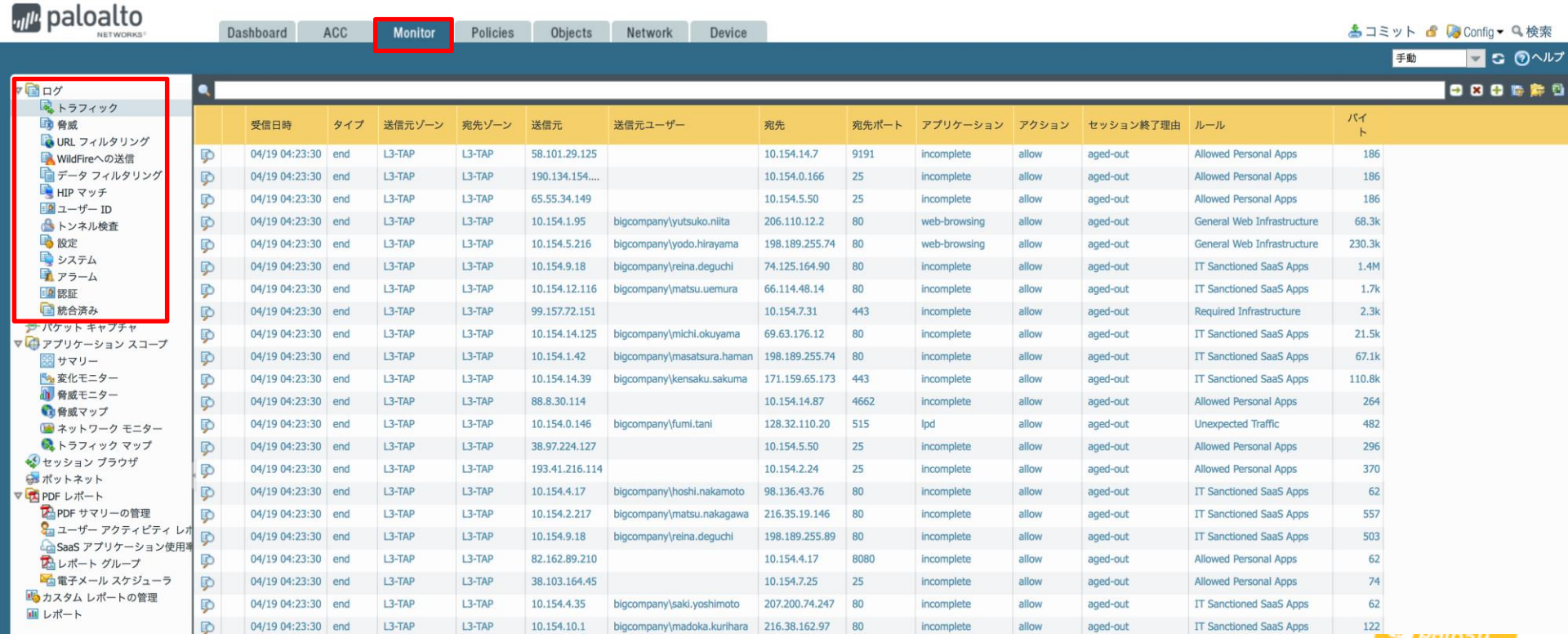
① ACC「グローバルフィルタ 2」

→ ユーザーでグローバルフィルタ



② Monitor「概要」

→ 各種ログを確認するための画面



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	セッション終了理由	ルール	バイト
04/19 04:23:30	end	L3-TAP	L3-TAP	58.101.29.125		10.154.14.7	9191	incomplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	190.134.154....		10.154.0.166	25	incomplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	65.55.34.149		10.154.5.50	25	incomplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	web-browsing	allow	aged-out	General Web Infrastructure	68.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.5.216	bigcompany\yodo.hirayama	198.189.255.74	80	web-browsing	allow	aged-out	General Web Infrastructure	230.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.9.18	bigcompany\reina.deguchi	74.125.164.90	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	1.4M
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.12.116	bigcompany\matsu.uemura	66.114.48.14	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	1.7k
04/19 04:23:30	end	L3-TAP	L3-TAP	99.157.72.151		10.154.7.31	443	incomplete	allow	aged-out	Required Infrastructure	2.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.14.125	bigcompany\michi.okuyama	69.63.176.12	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	21.5k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.42	bigcompany\masatsura.haman	198.189.255.74	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	67.1k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.14.39	bigcompany\kensaku.sakuma	171.159.65.173	443	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	110.8k
04/19 04:23:30	end	L3-TAP	L3-TAP	88.8.30.114		10.154.14.87	4662	incomplete	allow	aged-out	Allowed Personal Apps	264
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.0.146	bigcompany\fumi.tani	128.32.110.20	515	lpd	allow	aged-out	Unexpected Traffic	482
04/19 04:23:30	end	L3-TAP	L3-TAP	38.97.224.127		10.154.5.50	25	incomplete	allow	aged-out	Allowed Personal Apps	296
04/19 04:23:30	end	L3-TAP	L3-TAP	193.41.216.114		10.154.2.24	25	incomplete	allow	aged-out	Allowed Personal Apps	370
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.4.17	bigcompany\hoshi.nakamoto	98.136.43.76	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.2.217	bigcompany\matsu.nakagawa	216.35.19.146	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	557
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.9.18	bigcompany\reina.deguchi	198.189.255.89	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	503
04/19 04:23:30	end	L3-TAP	L3-TAP	82.162.89.210		10.154.4.17	8080	incomplete	allow	aged-out	Allowed Personal Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	38.103.164.45		10.154.7.25	25	incomplete	allow	aged-out	Allowed Personal Apps	74
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.4.35	bigcompany\saki.yoshimoto	207.200.74.247	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.10.1	bigcompany\madoka.kurihara	216.38.162.97	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	122

② Monitor「フィルタリング例 1-1」

→ 1クリックでフィルタも簡単

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	セッション終了理由	ルール	バイト
04/19 04:23:30	end	L3-TAP	L3-TAP	58.101.29.125		10.154.14.7	9191	incomplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	190.134.154....				mplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	[redacted]				mplete	allow	aged-out	Allowed Personal Apps	186
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.95				b-browsing	allow	aged-out	General Web Infrastructure	68.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.5.216				b-browsing	allow	aged-out	General Web Infrastructure	230.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.9.18	bigcompany\reina.deguchi	74.125.164.90	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	1.4M
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.12.116	bigcompany\matsu.uemura	66.114.48.14	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	1.7k
04/19 04:23:30	end	L3-TAP	L3-TAP	99.157.72.151		10.154.7.31	443	incomplete	allow	aged-out	Required Infrastructure	2.3k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.14.125	bigcompany\michi.okuyama	69.63.176.12	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	21.5k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.42	bigcompany\masatsura.haman	198.189.255.74	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	67.1k
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.14.39	bigcompany\kensaku.sakuma	171.159.65.173	443	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	110.8k
04/19 04:23:30	end	L3-TAP	L3-TAP	88.8.30.114		10.154.14.87	4662	incomplete	allow	aged-out	Allowed Personal Apps	264
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.0.146	bigcompany\fumi.tani	128.32.110.20	515	lpd	allow	aged-out	Unexpected Traffic	482
04/19 04:23:30	end	L3-TAP	L3-TAP	38.97.224.127		10.154.5.50	25	incomplete	allow	aged-out	Allowed Personal Apps	296
04/19 04:23:30	end	L3-TAP	L3-TAP	193.41.216.114		10.154.2.24	25	incomplete	allow	aged-out	Allowed Personal Apps	370
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.4.17	bigcompany\hoshi.nakamoto	98.136.43.76	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.2.217	bigcompany\matsu.nakagawa	216.35.19.146	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	557
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.9.18	bigcompany\reina.deguchi	198.189.255.89	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	503
04/19 04:23:30	end	L3-TAP	L3-TAP	82.162.89.210		10.154.4.17	8080	incomplete	allow	aged-out	Allowed Personal Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	38.103.164.45		10.154.7.25	25	incomplete	allow	aged-out	Allowed Personal Apps	74
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.4.35	bigcompany\saki.yoshimoto	207.200.74.247	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	62
04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.10.1	bigcompany\madoka.kurihara	216.38.162.97	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	122

② Monitor「フィルタリング例 1-2」

→ 1クリックでフィルタも簡単

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	セッション終了理由	ルール	バイト
04/19 04:33:38	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	37.3k
04/19 04:33:21	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	web-browsing	allow	tcp-rst-from-client	General Web Infrastructure	47.6k
04/19 04:33:19	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	web-browsing	allow	tcp-rst-from-client	General Web Infrastructure	68.2k
04/19 04:33:19	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	72.14.213.17	80	gmail-base	allow	tcp-rst-from-client	Allowed Personal Apps	31.8k
04/19 04:33:18	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	web-browsing	allow	tcp-rst-from-client	General Web Infrastructure	21.2k
04/19 04:33:16	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	63.0k
04/19 04:33:15	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	216.115.220.254	443	incomplete	allow	tcp-fin	IT Sanctioned SaaS Apps	362
04/19 04:33:15	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	216.115.219.126	443	incomplete	allow	tcp-fin	IT Sanctioned SaaS Apps	362
04/19 04:33:15	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	216.115.220.254	443	incomplete	allow	tcp-fin	IT Sanctioned SaaS Apps	362
04/19 04:33:13	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	38.7k
04/19 04:33:11	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita				allow	aged-out	IT Sanctioned SaaS Apps	53.8k
04/19 04:33:09	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita				allow	tcp-rst-from-client	General Web Infrastructure	51.0k
04/19 04:33:07	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita				allow	aged-out	IT Sanctioned SaaS Apps	55.5k
04/19 04:32:51	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	web-browsing	allow	tcp-rst-from-client	General Web Infrastructure	68.5k
04/19 04:32:51	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	29.1k
04/19 04:32:51	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	5.9k
04/19 04:32:50	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	50.4k
04/19 04:32:50	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	27.8k
04/19 04:32:49	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	11.8k
04/19 04:32:46	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	24.9k
04/19 04:32:46	end	L3-TAP	L3-TAP	10.154.1.95	bigcompany\yutsuko.niita	206.110.12.2	80	incomplete	allow	aged-out	IT Sanctioned SaaS Apps	50.5k

② Monitor「ログ詳細の確認」

→ 虫眼鏡アイコンでログの詳細を表示

ログ詳細

関連するログ

1. ACCとMonitorについて
2. **切り分けに利用するサービス**
    - **① パロアルトネットワークスが提供するサービス**
    - **② その他外部サービス**
3. 検知時の対応方法
    - ① ウィルス検出時の運用方法の例
    - ② 攻撃検出時の運用方法の例
    - ③ WildFireによる未知のマルウェア検出時の運用方法の例
4. CSPアカウントについて
5. まとめ
6. 参考情報
    - ① デモサイトについて
    - ② NextWaveパートナー制度について

2. 切り分けに利用するサービス

パロアルトネットワークスが提供するサービス

① THREAT VAULT

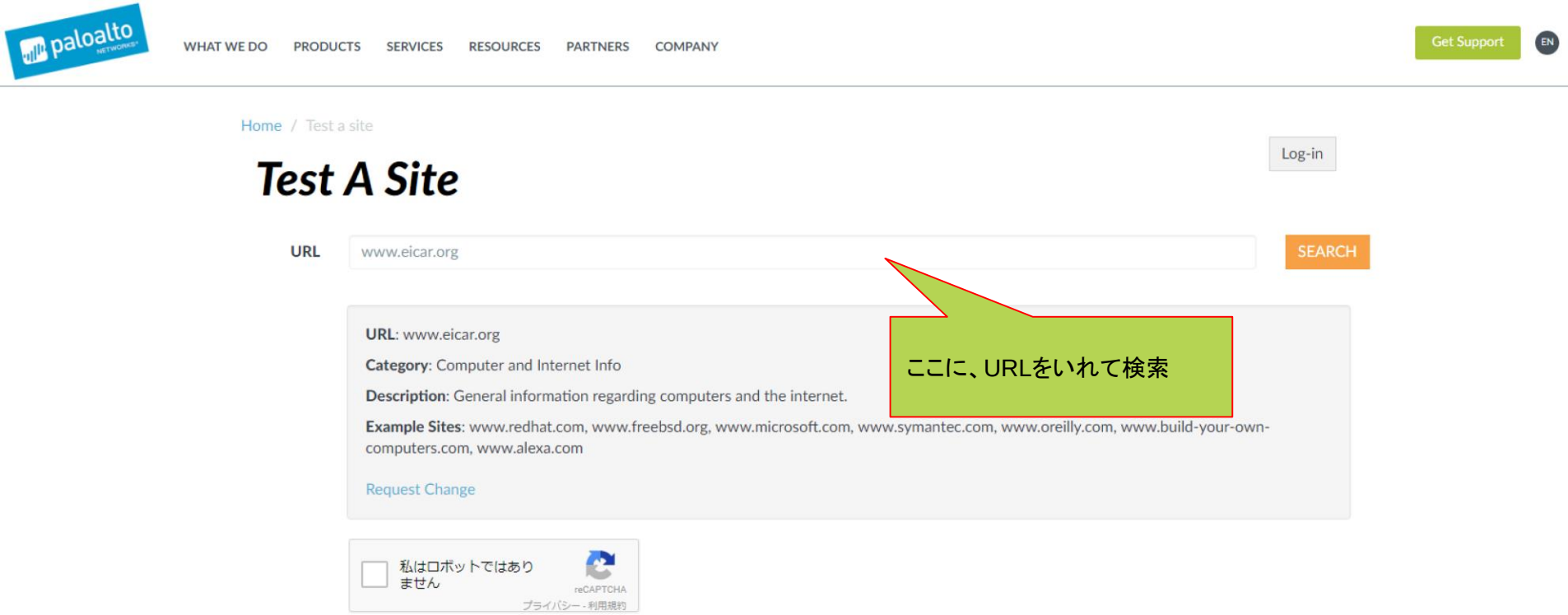
→ パロアルトネットワークスが提供するシグネチャ情報を提供

※ CSPアカウントが必要

https://threatvault.paloaltonetworks.com/

② TEST A Site

→ パロアルトネットワークスが提供するURLフィルタリングDBの確認サイト
URLがどのカテゴリに属するかの確認や修正依頼が可能

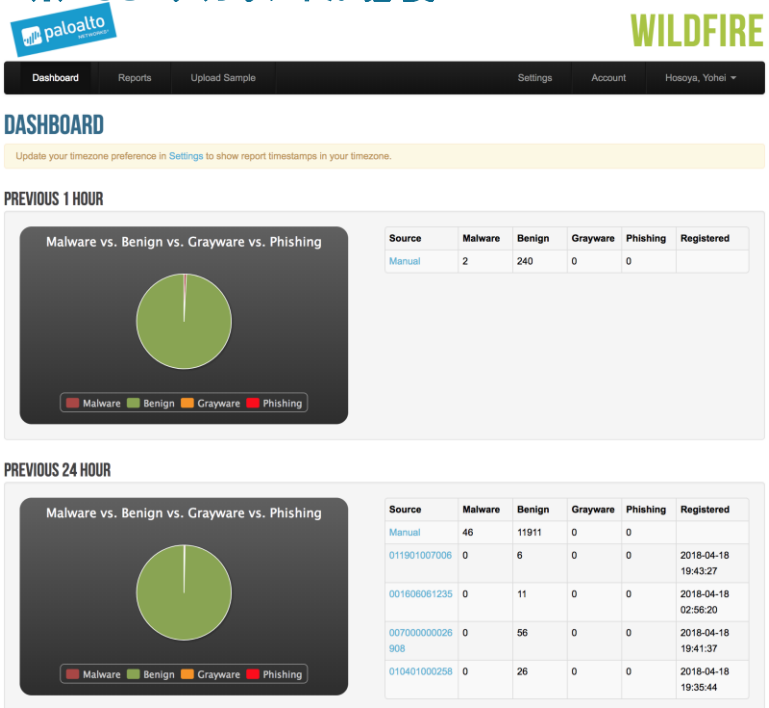


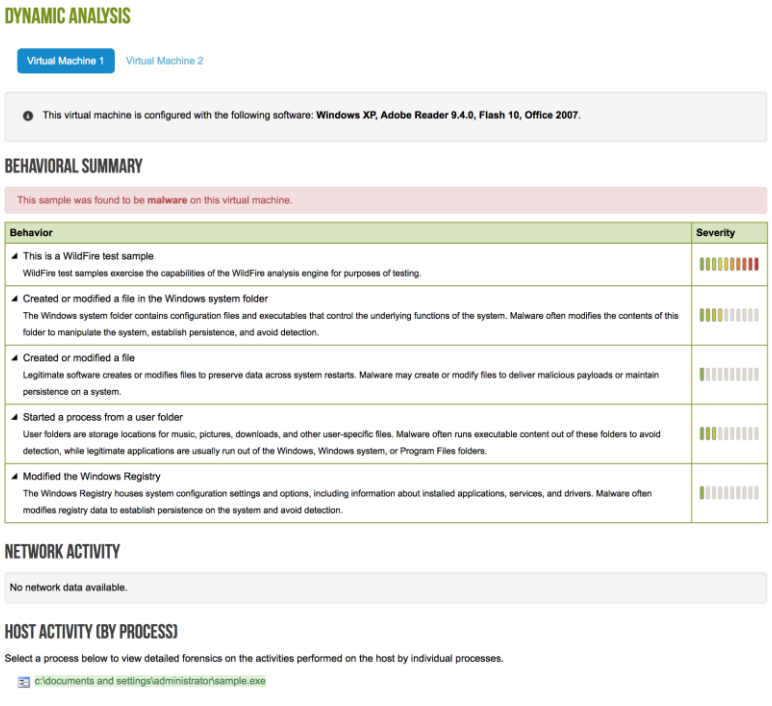
https://urlfiltering.paloaltonetworks.com/

③ WildFire Portal

→ パロアルトネットワークスの提供するサンドボックス（WildFire）にお客様がアップロードしたサンプルの情報

※ お客様毎にポータルページが作成される
※ WildFireサブスクリプションが必要
※ CSPアカウントが必要

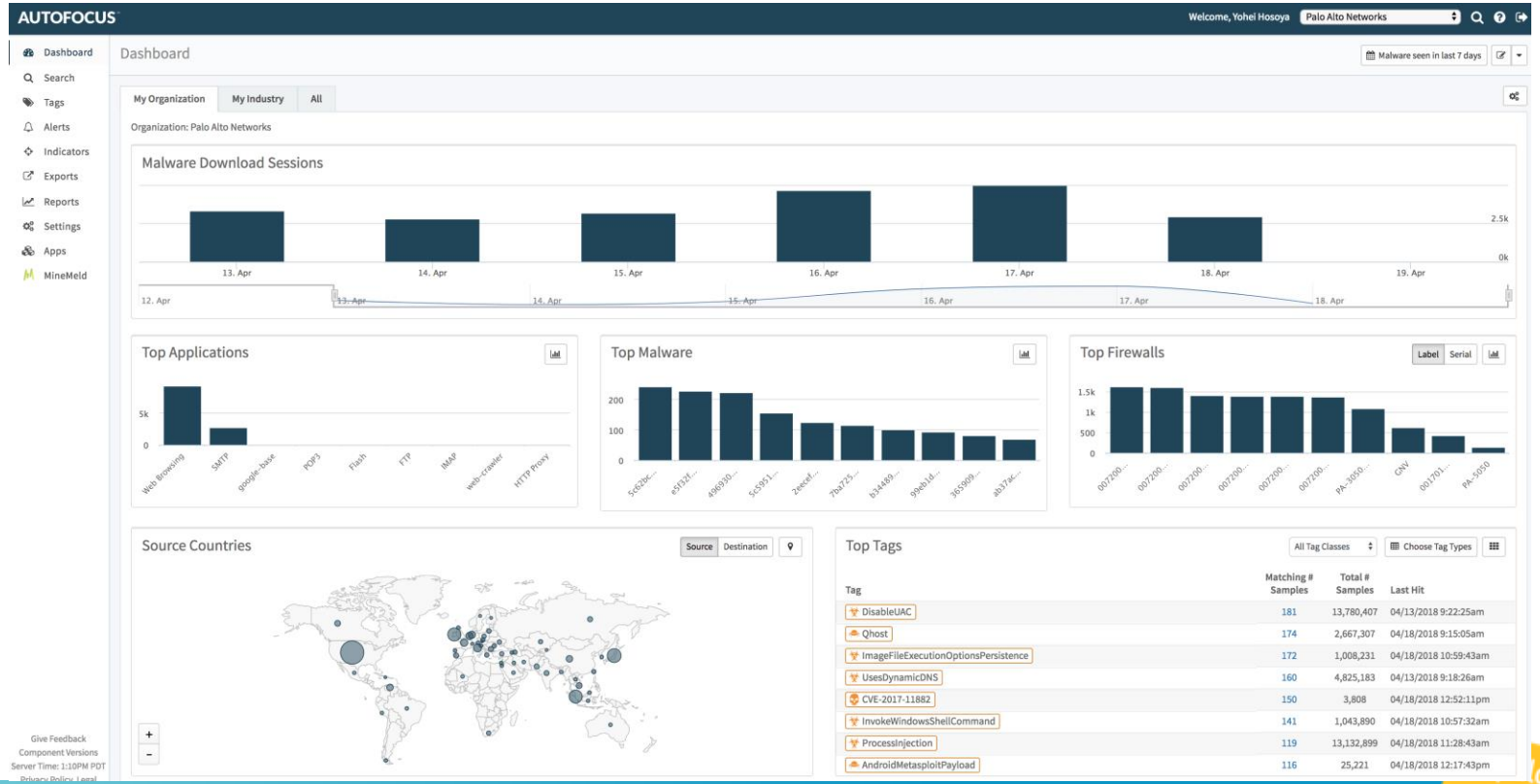




④ AutoFocus

→ WildFire内のデータベースを有償で提供するサービス

※ AutoFocus サブスクリプションが必要

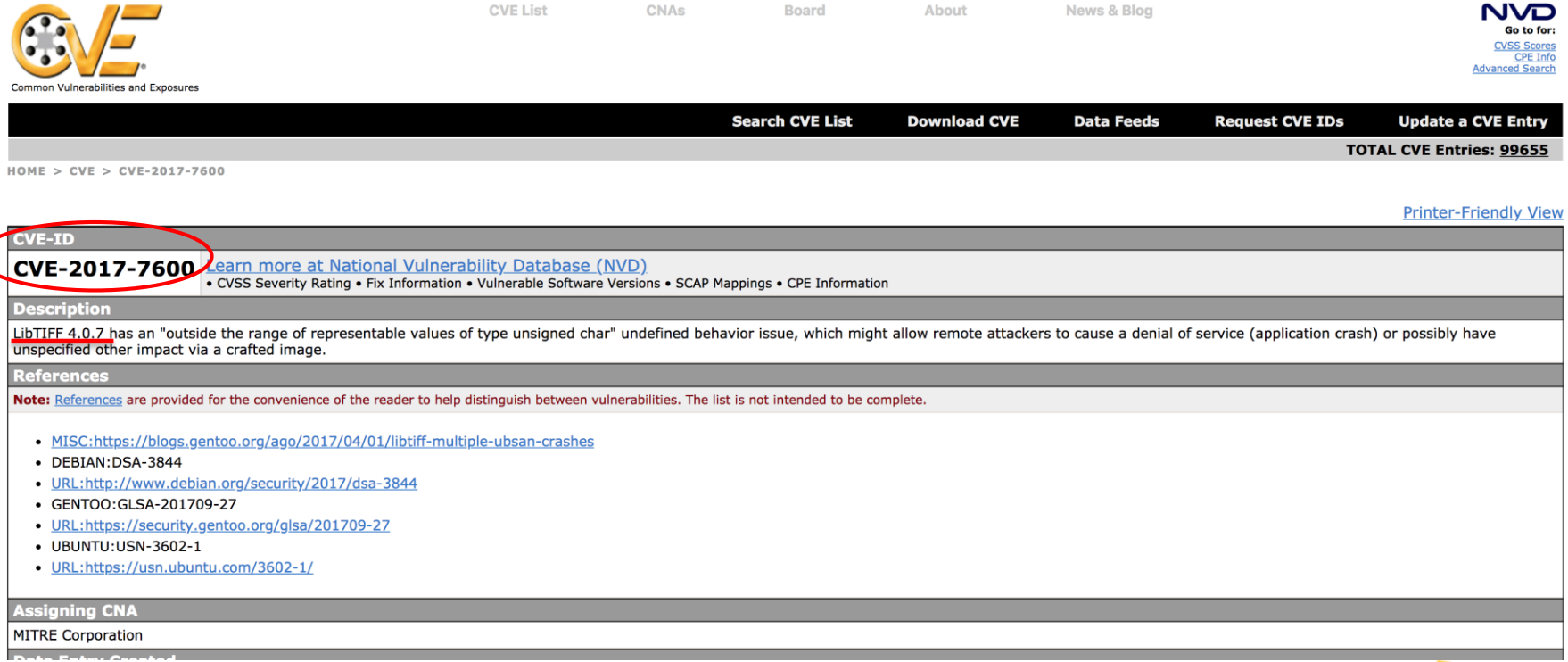


2. 切り分けに利用するサービス

他社が提供しているサービス

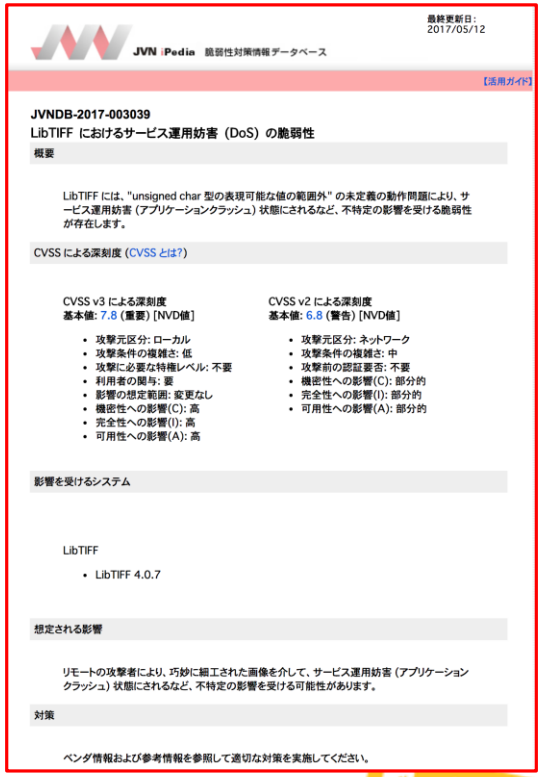
⑤ CVE

→ 米国の非営利団体が提供する脆弱性情報のDB
脆弱性にCVE-IDという識別子をつけて管理（英語）



http://cve.mitre.org/cve/search_cve_list.html

⑥ JVN DB
→ IPAが運用する日本語でCVEが検索できるサイト
JVN独自の番号でも管理



https://jvndb.jvn.jp/index.html

⑦ VirusTotal
→ Googleの提供するウィルス情報サイト

ウィルスファイルやHash情報で検索

https://www.virustotal.com/ja/

ウィルスに対応している製品がどれだけあるか表示される

※ ウィルスファイルはサービスを受けている各社で共有されるため、アップロードの際は注意すること。

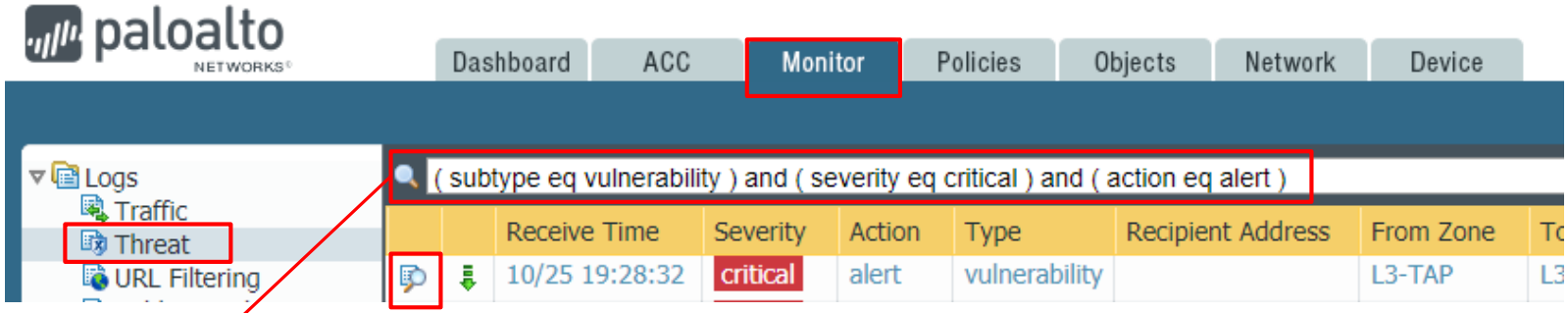
1. ACCとMonitorについて
2. 切り分けに利用するサービス
    ① パロアルトネットワークスが提供するサービス
    ② その他外部サービス
3. **検知時の対応方法**
    ① ウィルス検出時の切り分け例
    ② 攻撃検出時の切り分け例
    ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. まとめ
6. 参考情報
    ① デモサイトについて
    ② NextWaveパートナー制度について

3. 検知時の対応方法

①脆弱性を狙った攻撃検出時の切り分け

①-1まずはトラフィックの調査

1. Monitorタブ → 脅威をクリック
2. サンプル抽出のため、ブロックしていないクリティカルな攻撃でフィルタリング
3. 虫眼鏡アイコンをクリックし、ログの詳細を表示



(subtype eq viulnerability) and (severity eq critical) and (action eq alert)

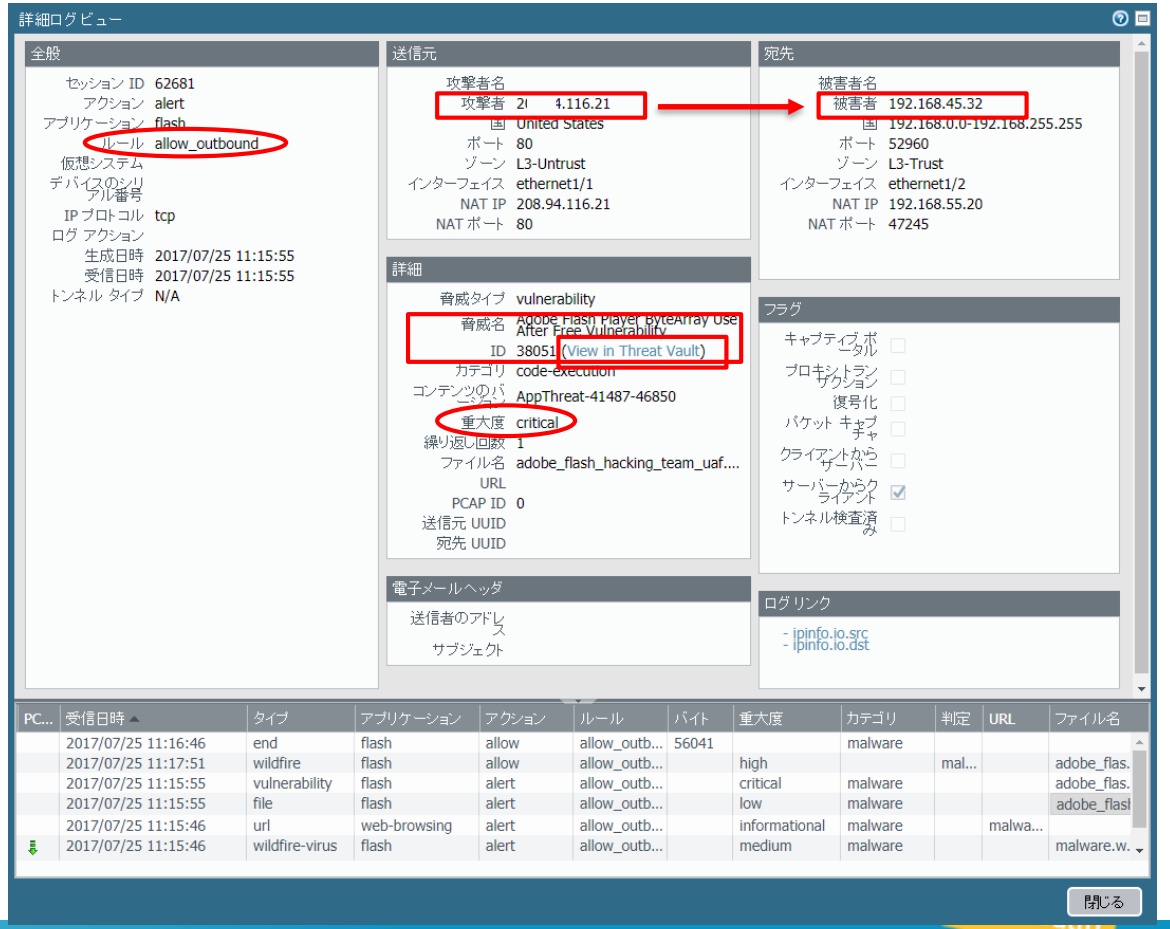
脆弱性関連ログ　　クリティカルな脆弱性　　アラート（ブロックしてない）

①-2 トラフィックを見つけたら詳細を確認

ここから分かること

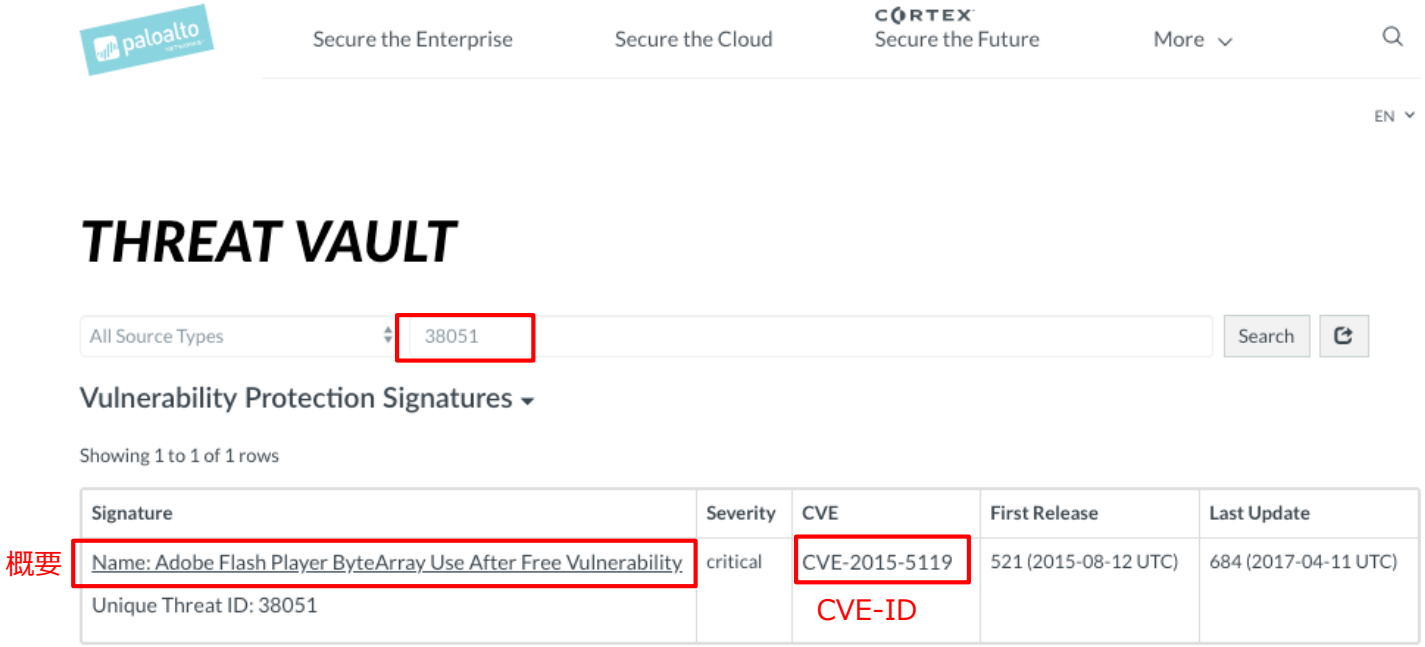
1. 外部(US)から攻撃を受けている
2. 攻撃は[Adobe Flash Player ByteArray Use After Free Vulnerability]であり、シグネチャID38051で管理されている
3. アプリケーションはFlash

4. View in Threat Vault をクリック



①-3 ThreatVaultでの調査

1. シグネチャID38051でフィルタされた状態で表示される
2. Adobe Flash Playerに関する脆弱性
3. CVE-2015-5119で管理されている



①-4-1 PA本体を使った攻撃の調査

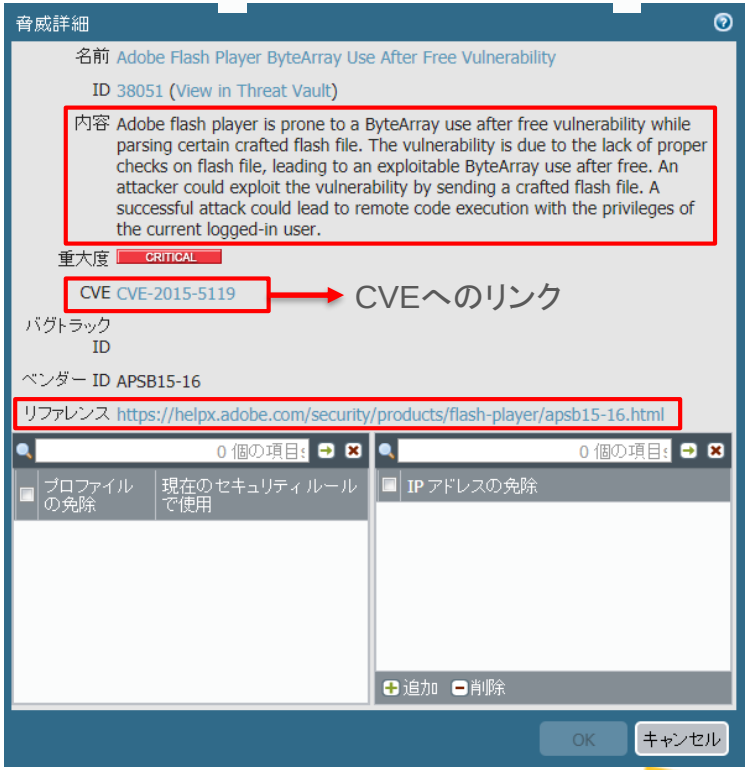
1. 攻撃の名前の上にマウスカーソルを置くと、▼マークが表示されるのでクリック → [例外]をクリック

①-4-2 PA本体を使った攻撃の調査

ここから分かること

1. Adobe flashに関する攻撃の概要が記載
2. CVE-2015-5119 で管理

3. JVNDBで確認



①-5 攻撃の調査

1. JVN DBでCVEの詳細を確認
2. 影響を受けるシステムを確認
3. リンクから各ベンダの対策ページの内容を確認

ID	タイトル	CVSSv3	CVSSv2	公表日	最終更新日
JVNDB-2015-003793	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/08/21
JVNDB-2015-003528	Adobe Flash Player および Adobe AIR におけるヒープベースのバッファオーバーフローの脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003527	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003526	Adobe Flash Player および Adobe AIR における同一生成元ポリシーを回避される脆弱性	-	5.0	2015/07/08	2015/07/13
JVNDB-2015-003525	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003524	Adobe Flash Player および Adobe AIR におけるヒープベースのバッファオーバーフローの脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003523	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003522	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003521	Adobe Flash Player および Adobe AIR におけるサービス運用妨害 (DoS) の脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003520	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003519	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003518	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003517	Adobe Flash Player および Adobe AIR におけるヒープベースのバッファオーバーフローの脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003516	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003515	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003514	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003513	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003512	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003511	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003510	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003509	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003508	Adobe Flash Player および Adobe AIR におけるサービス運用妨害 (DoS) の脆弱性	-	7.5	2015/07/08	2015/07/13
JVNDB-2015-003507	Adobe Flash Player および Adobe AIR における同一生成元ポリシーを回避される脆弱性	-	5.0	2015/07/08	2015/07/13
JVNDB-2015-003506	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003505	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003504	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003503	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003502	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13
JVNDB-2015-003501	Adobe Flash Player および Adobe AIR における任意のコードを実行される脆弱性	-	10.0	2015/07/08	2015/07/13

関連する脅威情報

詳細確認

①-6 対処方法の例

- FWのシグネチャで検出できているので、
  ブロック設定の場合は暫定対処はできていると判断

- 脆弱性に対する根本的な対処は、ソフトウェアのアップデートやパッチの適用
  対策済みのパッチやバージョンであれば影響なしと判断

- 対象のアプリケーション・OSが存在しない場合も
  影響なしと判断

- それ以外の場合、対象ソフトウェアのアップデートを実施

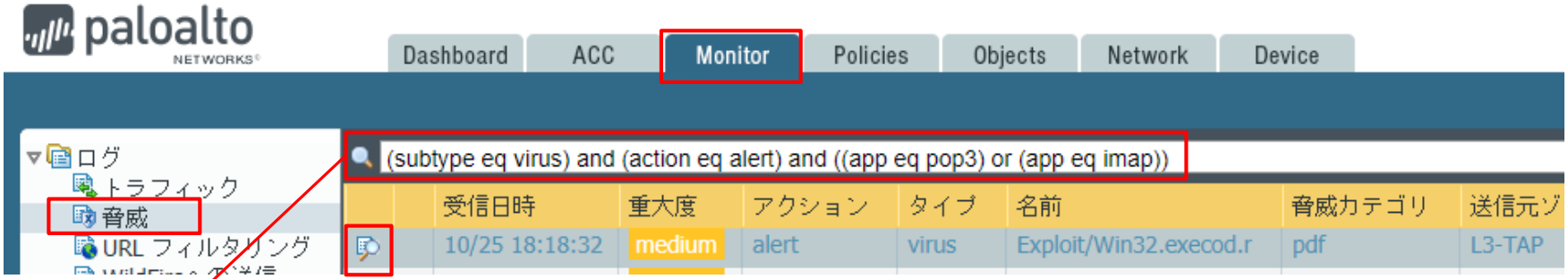
3. 検知時の対応方法

②ウィルス検出時の切り分け例

 |

②-1 まずはトラフィックの調査

1. Monitorタブ → 脅威をクリック
2. サンプル抽出のため、POP3/IMAPで検出したウィルスでフィルタリング
3. 虫眼鏡アイコンをクリックし、ログの詳細を表示



(subtype eq virus) and (action eq alert) and ((app eq pop3) or (app eq imap))

ウィルス関連ログ

アラート
（ブロックしてない）

アプリケーションがPOP3かIMAP

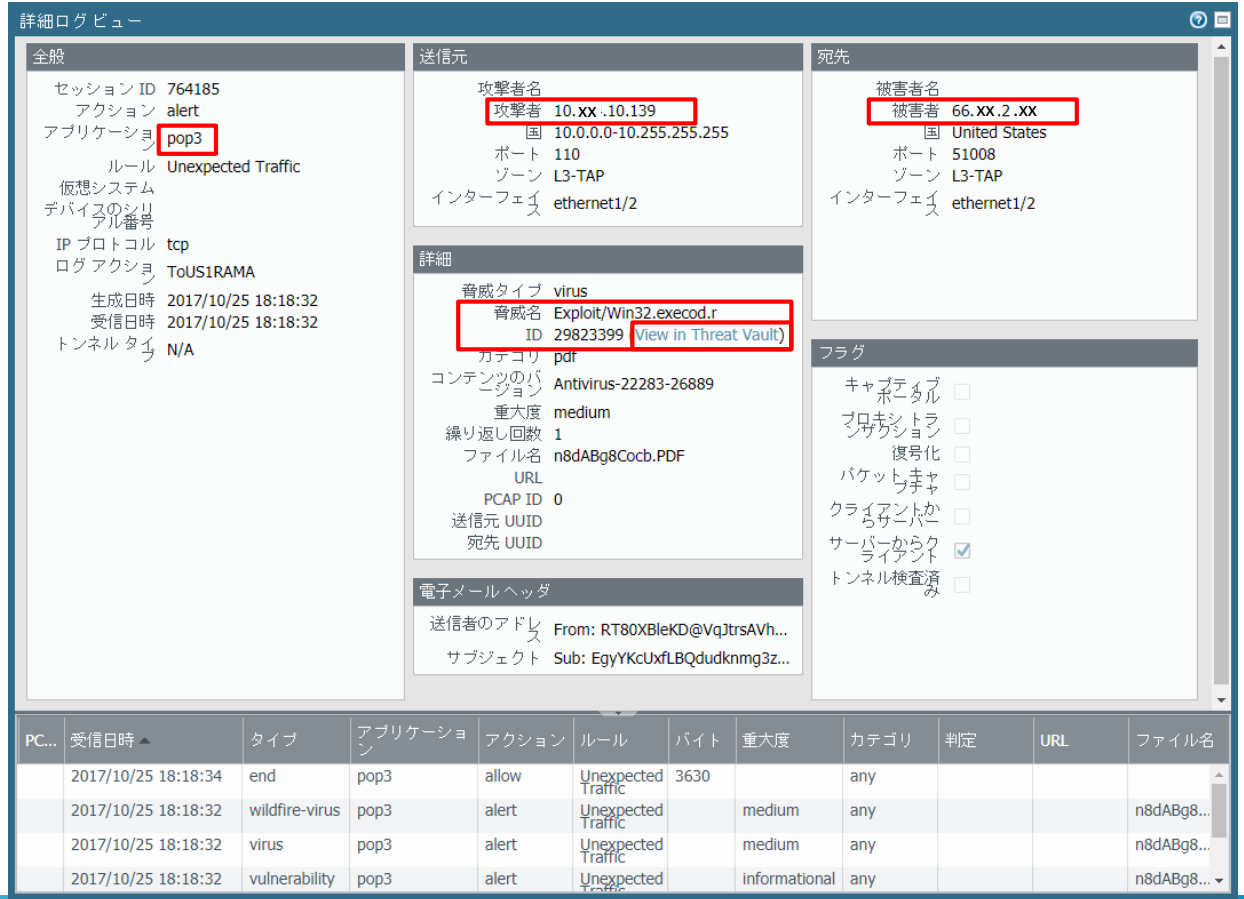
②-2 トラフィックを見つけたら詳細を確認

ここから分かること

1. ウィルスメールをPOPで受信

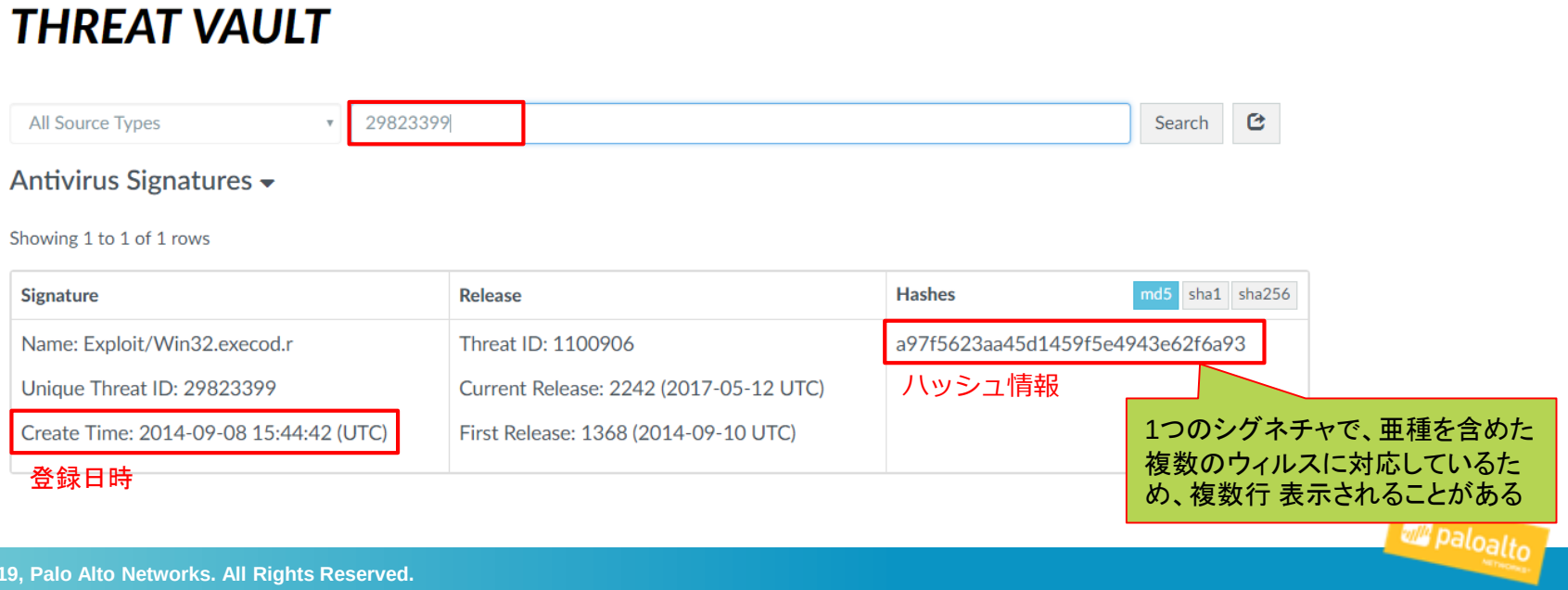
2. ウィルス名は、[Exploit/Win32.execod.r]であり、シグネチャID29823399で管理

3. View in Threat Vault をクリック



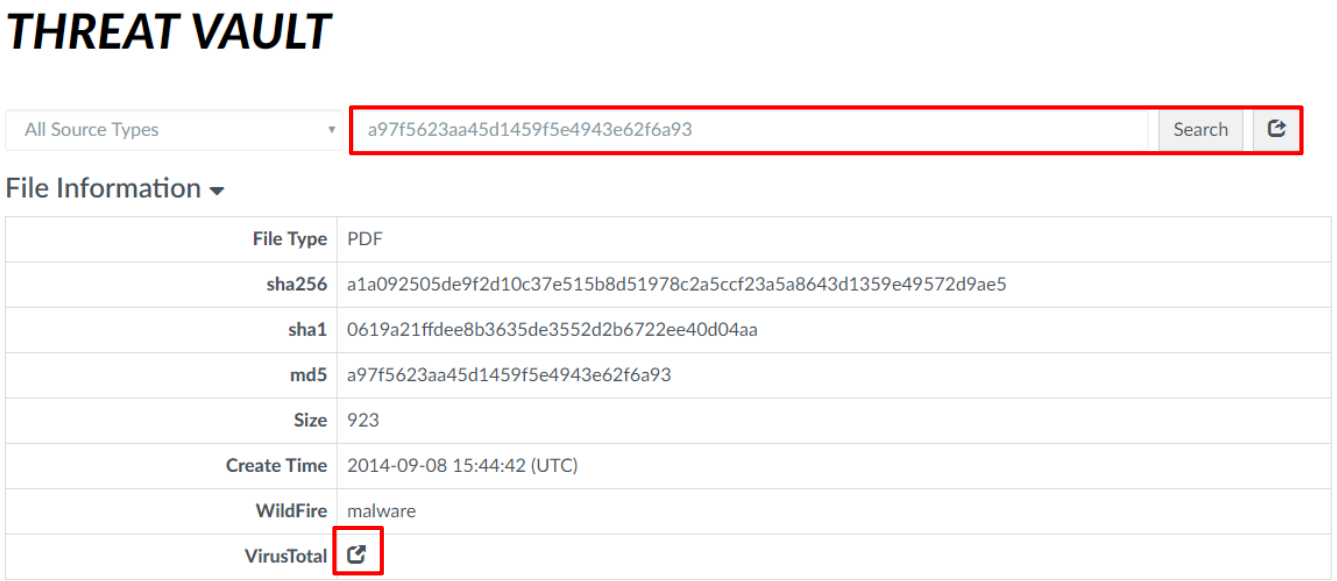
②-3 ThreatVaultでの調査

1. シグネチャID29823399でフィルタされた状態で表示
2. 2014年9月8日に登録されたウィルス
3. ウィルスのハッシュ情報をコピーして今度はハッシュ情報で検索



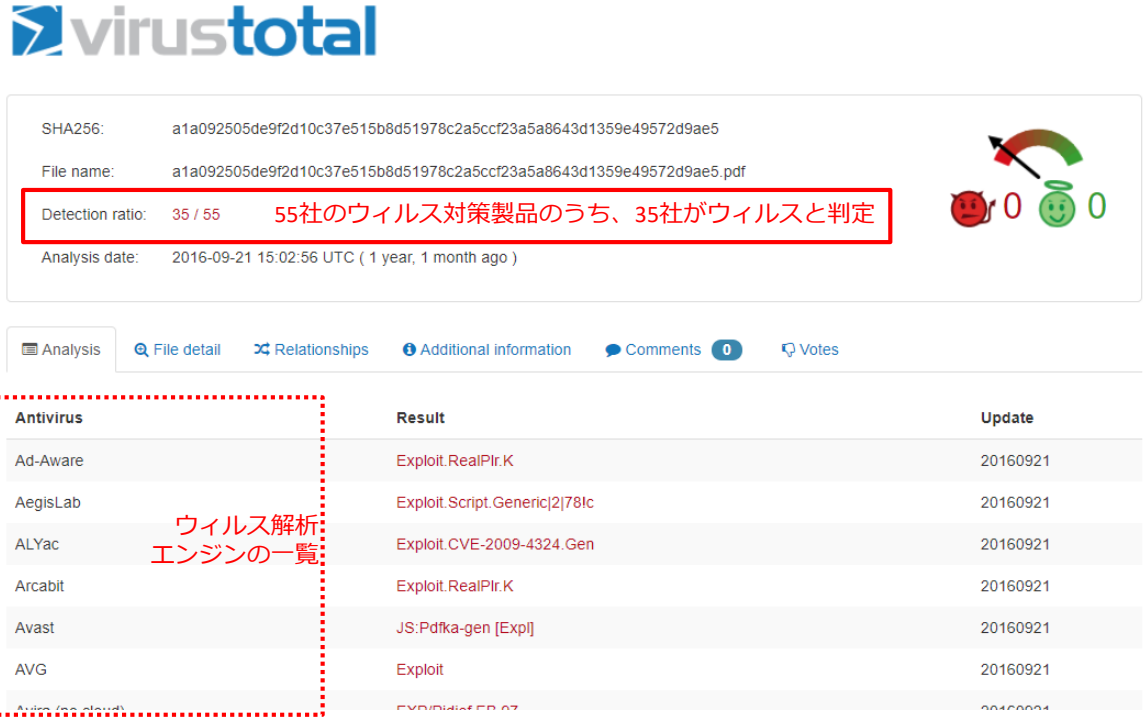
②-4 ThreatVaultでの調査その2

1. ハッシュ値でフィルタをかけることで、そのウィルスに特化した情報が表示
2. 一番下のVirusTotalのマークをクリック



②-5 VirusTotalを利用した調査

1. Virus Totalで、ハッシュ値を検索
2. 55社のウィルス対策製品のうち、35社がウィルスと判定
3. 怪しい



②-6 対処方法の例

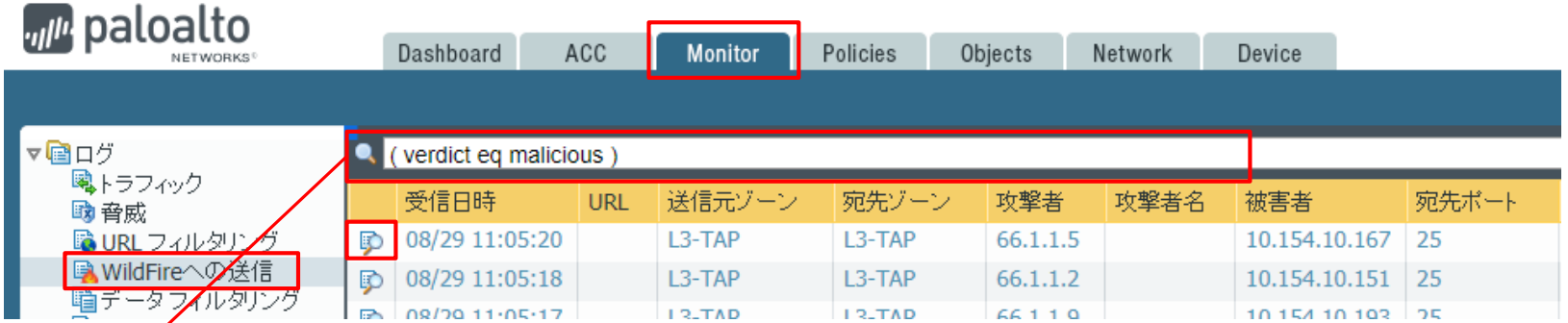
- 自社が利用しているウィルスソフトが対応しているか確認
- 対応していない場合は、隔離等の処置を実施
- ウィルスベンダーへの問い合わせも併せて実施

3. 検知時の対応方法

③ WildFireによる未知のマルウェア検出時の切り分け

③-1 まずはトラフィックの調査

1. Monitorタブ → WildFireへの送信をクリック
2. サンプル抽出のため、マルウェア判定されたログでフィルタリング
3. 虫眼鏡アイコンをクリックし、ログの詳細を表示



(verdict eq malicious)

WildFire上でマルウェア判定

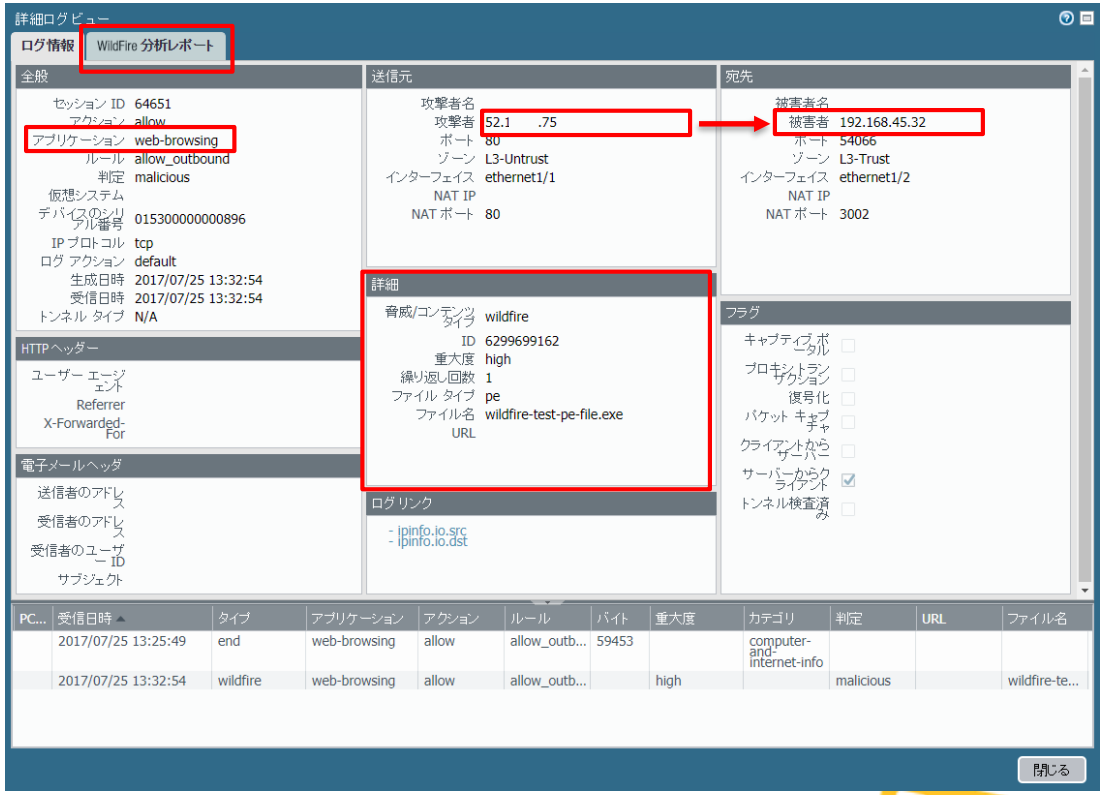
③-2 トラフィックを見つけたら詳細を確認

ここから分かること

1. 外部からweb経由でファイルをダウンロード

2. ファイル名は、[wildfire-test-pe-file.exe]

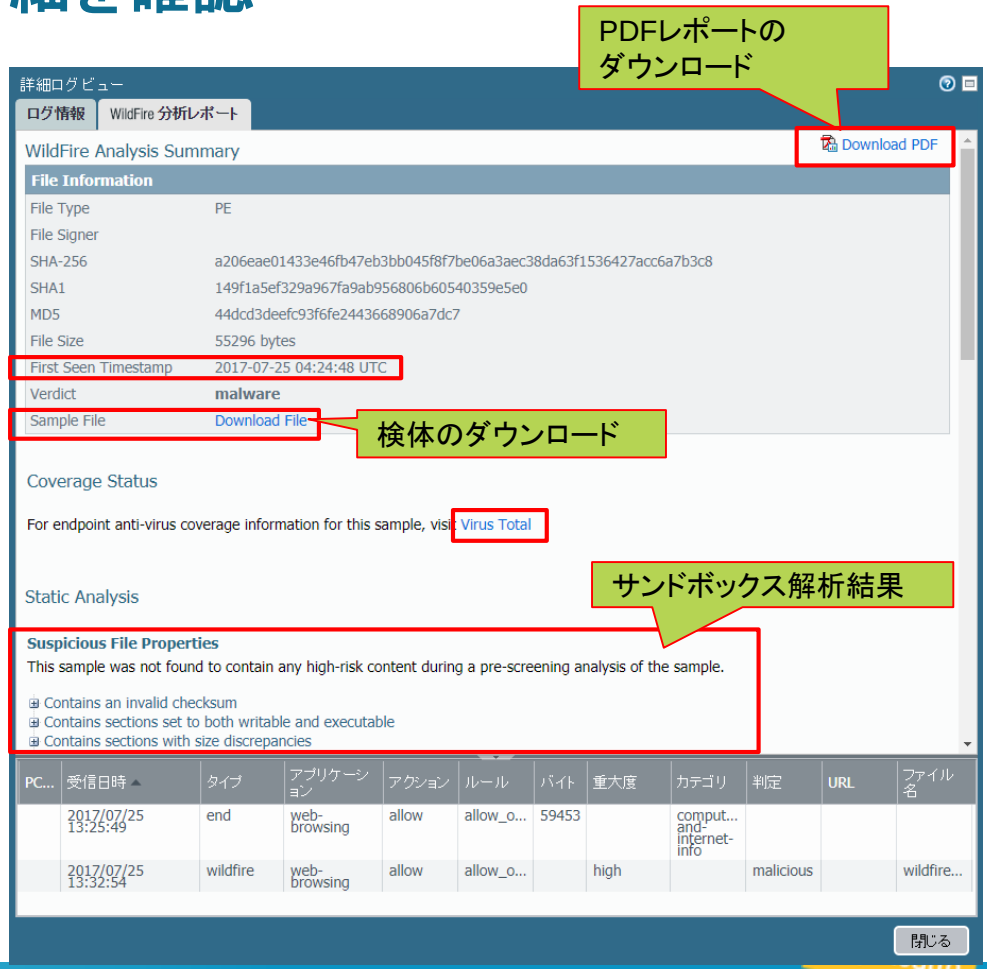
3. **WildFire分析レポートタブをクリック**



③-3 トラフィックを見つけたら詳細を確認

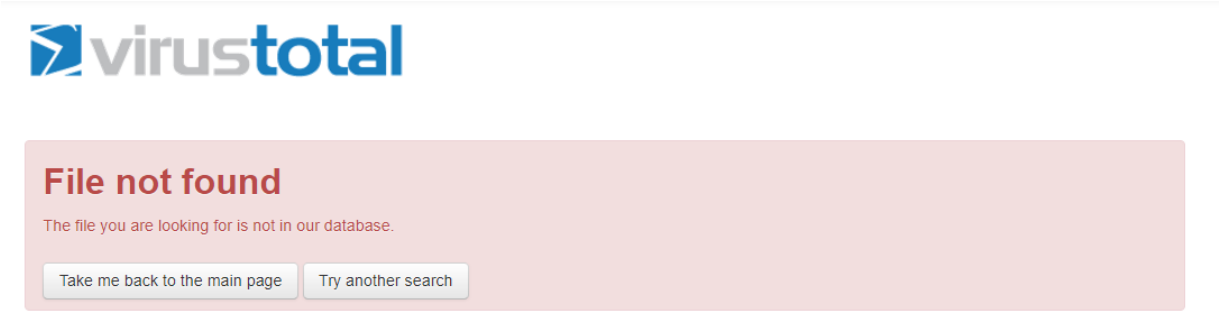
1. 詳細な挙動が記載されているので、内容を確認
2. 2017年7月25日04:24:48UTCに発見したマルウェア
3. ウィルスベンダへの提供等で、検体が必要な場合、ファイルをダウンロードすることも可能

4. **VirusTotal**をクリック



 |

③-4 Virus Totalでの調査結果



1. ②ウィルス検知時と同様にVirus Totalで確認
2. File not foundと表示 → 現時点で他社が対策できていない
3. 未知のマルウェアである可能性が高い

③-5 対処方法の例

- 自社が利用しているウィルスソフトが対応しているか確認
- マルウェアをダウンロードした端末が感染している可能性がある
  - 該当端末のIPアドレスとUser-ID情報を使って端末を特定
  - C&Cへの通信がないか、ログ上から確認
  - WildFire分析レポートのNetwork Activityを確認
- 隔離等の処置を実施
- ウィルスベンダーへの問い合わせも併せて実施

1. ACCとMonitorについて
2. 切り分けに利用するサービス
    ① パロアルトネットワークスが提供するサービス
    ② その他外部サービス
3. 検知時の対応方法
    ① ウィルス検出時の切り分け例
    ② 攻撃検出時の切り分け例
    ③ WildFireによる未知のマルウェア検出時の切り分け例
4. **CSPアカウントについて**
5. まとめ
6. 参考情報
    ① デモサイトについて
    ② NextWaveパートナー制度について

CSPアカウントとは

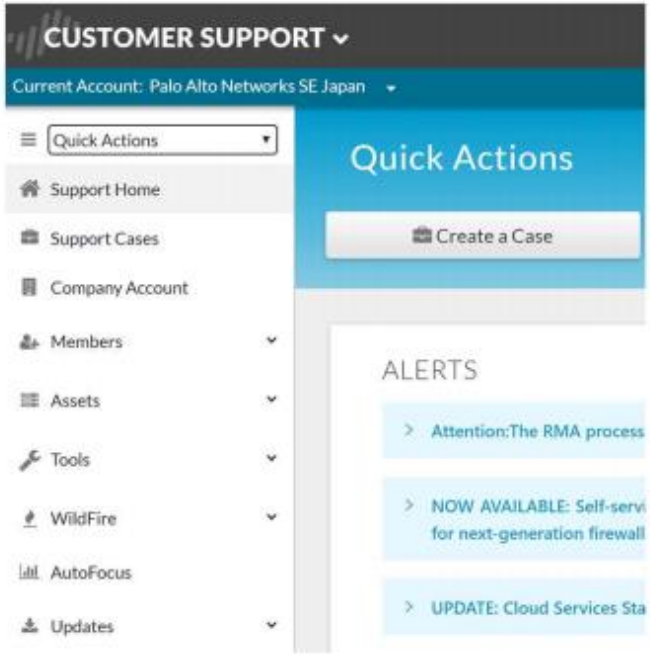
- パロアルト製品を購入すると、**購入ユーザごと**にIDが発行され、CSPアカウントの作成が可能になる

- CSPアカウントを作成すると、以下のサービスが利用可能
  - CSPサイトへのログイン
  - Threat Vault（弊社シグネチャIDの情報）やWildFireポータルサイト等の情報サイトへのアクセス
  - SLRレポートの作成
  - ケースオープン

- パートナーにもCSPアカウントは発行される
  - 原則として**評価機の購入**が必要

CSPサイトとは

- CSP(Customer Support Portal)サイトは、パロアルトネットワークスのサポート ポータル(https://support.paloaltonetworks.com)で、以下を提供
- CSPアカウントにてログインを行う



各種情報

- PAN-DB URL CATEGORIZATION (URLフィルターのカテゴリー確認)
- APPLIPEDIA (認識可能なアプリケーションDB)
- THREAT DB (IPS/アンチスパイウェアのシグネチャ情報)
- TECHNICAL DOCUMENTAION (製品マニュアル)

PAN-OS・シグネチャのダウンロード

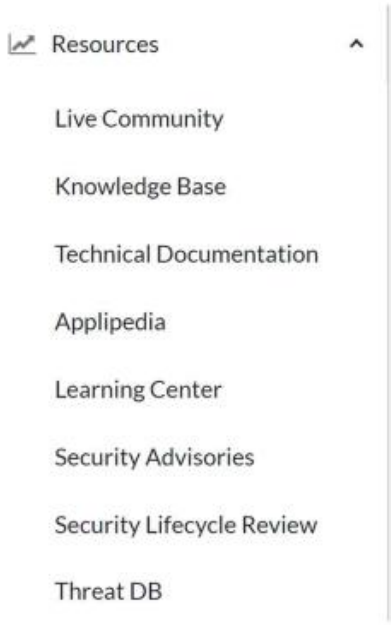
- SOFTWARE UPDATES (PAN-OSのダウンロード)
- DYNAMIC UPDATES (アプリ/IPS/AV/WFシグネチャのダウンロード)

パロアルトネットワークスの各種サービスへのログイン

- WILDFIRE PORTAL (CSPのログインアカウントをSSOとして利用)
- AUTOFOCUS (CSPのログインアカウントをSSOとして利用)

CSPサイトでの各種情報の参照

各種ドキュメントの参照が可能



Knowledge Base

Technical Documentation

Applipedia

CSPアカウントの発行について

- CSPアカウントの管理は各社に設定されたSuper Userが実施
- アカウントの追加は各Super Userに依頼する必要がある
- SLRレポート等の作成はSuper Userである必要がある
  - PA案件に携わる方はできるだけSuper Userであることが望ましいが、ユーザーの削除等もできてしまうので注意が必要

Super Userが登録されていない場合や、
CSPアカウントを1次代理店が代理で作成している場合があります。
まずは、購入元の代理店にご確認ください。

1. ACCとMonitorについて
2. 切り分けに利用するサービス
    ① パロアルトネットワークスが提供するサービス
    ② その他外部サービス
3. 検知時の対応方法
    ① ウィルス検出時の切り分け例
    ② 攻撃検出時の切り分け例
    ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. **まとめ**
6. 参考情報
    ① デモサイトについて
    ② NextWaveパートナー制度について

まとめ

1. 脆弱性への対処
   - ソフトウェアの脆弱性（バグ）をつく攻撃は、CVEにて管理されている
   - CVE番号を元に、影響を受けるシステムを特定

2. 既知のウィルスへの対処
   - 亜種が多く、詳細の確認は困難であるケースが多い
   - 利用しているアンチウィルスソフトで検出可能か確認

3. 未知のウィルスへの対処
   - 他社のアンチウィルスソフトでは検出できない可能性が高い
   - 早急に隔離等の対処を行う

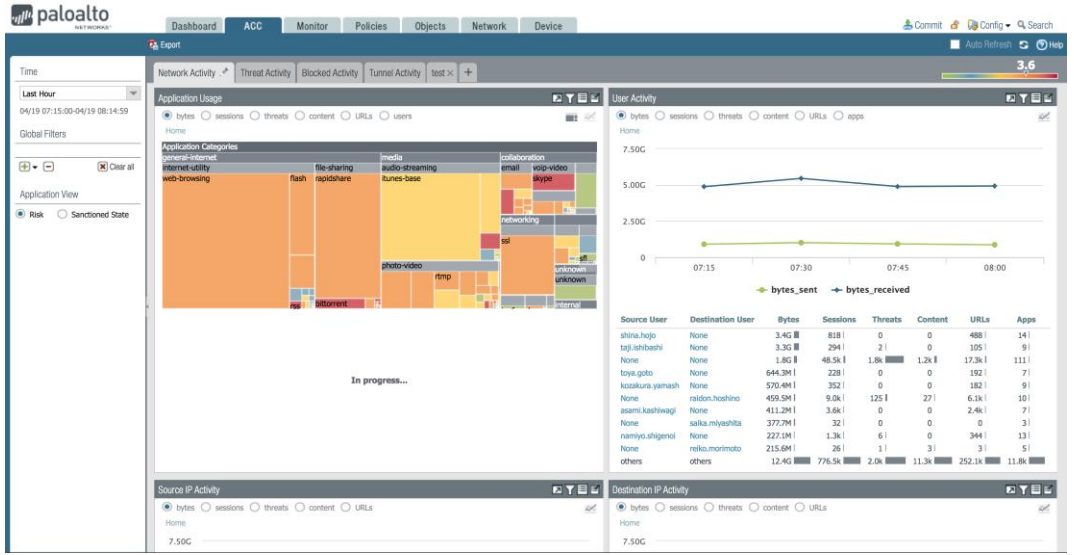
4. CSPアカウントについて
   - PA構築に携わる方々は登録を推奨！

1. ACCとMonitorについて
2. 切り分けに利用するサービス
    ① パロアルトネットワークスが提供するサービス
    ② その他外部サービス
3. 検知時の対応方法
    ① ウィルス検出時の切り分け例
    ② 攻撃検出時の切り分け例
    ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. まとめ
6. **参考情報**
    ① デモサイトについて
    ② NextWaveパートナー制度について

6. 参考情報

デモサイトについて

パートナーの皆様にご提供しているデモサイト



https://jp3.demo.paloaltonetworks.com
https://jp4.demo.paloaltonetworks.com
} PAシリーズ(VM)

https://jp1rama.demo.paloaltonetworks.com ← Panorama

パートナーポータルアカウントが別途必要となります。
購入元の代理店にご確認ください。

NextWaveパートナー制度

- パートナーポータルアカウントの登録が必要
- できること
  - 各種無料トレーニングの受講
  - 資格試験の受験
  - 評価機の購入
  - デモサイトの利用
  - パートナーポータルの利用
  - SKO/TechSummit/Ignite等のイベントへの参加

https://www.paloaltonetworks.jp/partners/request-access

※詳細は、1次代理店もしくは弊社のチャネルチームにご確認ください。