

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

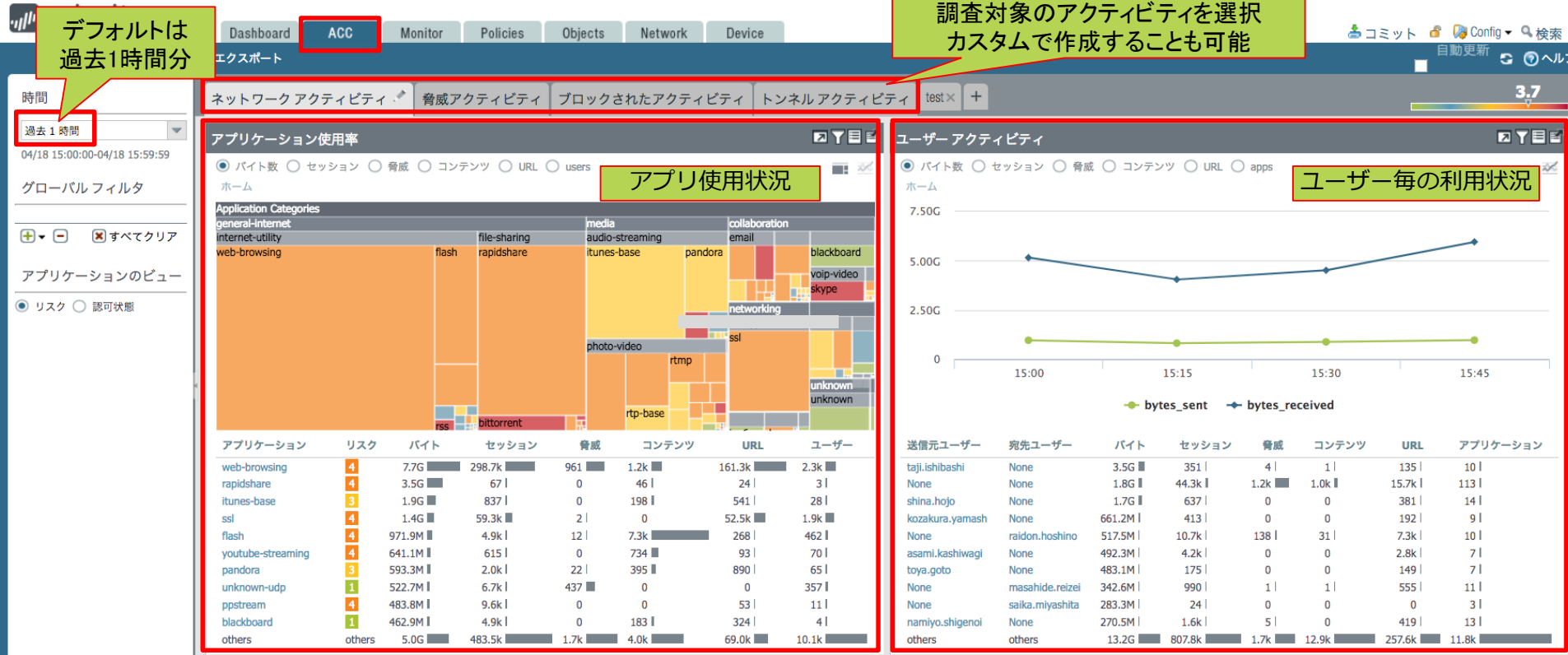


# ① ACC「概要」

→ 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

デフォルトは過去1時間分

調査対象のアクティビティを選択  
カスタムで作成することも可能



# 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)

The screenshot displays the Palo Alto Networks ACC interface. A red box on the left highlights the 'グローバルフィルタ' (Global Filter) section, which includes a time range selector (set to '過去1時間'), a search bar, and a list of application categories with checkboxes for filtering. A green callout points to the 'グローバルフィルタ' label. Another green callout points to the 'ローカルフィルタ' (Local Filter) section, which is a line graph showing 'bytes\_sent' and 'bytes\_received' over time. A second green callout points to the 'ローカルフィルタ' label. Below the graph is a table of user activity data.

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	ユーザー
web-browsing	4	7.7G	298.7k	961	1.2k	161.3k	2.3k
rapidshare	4	3.5G	67	0	46	24	3
itunes-base	3	1.9G	837	0	198	541	28
ssl	4	1.4G	59.3k	2	0	52.5k	1.9k
flash	4	971.9M	4.9k	12	7.3k	268	462
youtube-streaming	4	641.1M	615	0	734	93	70
pandora	3	593.3M	2.0k	22	395	890	65
unknown-udp	1	522.7M	6.7k	437	0	0	357
ppstream	4	483.8M	9.6k	0	0	53	11
blackboard	1	462.9M	4.9k	0	183	324	4
others		5.0G	483.5k	1.7k	4.0k	69.0k	10.1k

送信元ユーザー	宛先ユーザー	バイト	セッション	脅威	コンテンツ	URL	アプリケーション
tajishiibashi	None	3.5G	351	4	1	135	10
None	None	1.8G	44.3k	1.2k	1.0k	15.7k	113
shina.hojo	None	1.7G	637	0	0	381	14
kozakura.yamash	None	661.2M	413	0	0	192	9
None	raidon.hoshino	517.5M	10.7k	138	31	7.3k	10
asami.kashiwagi	None	492.3M	4.2k	0	0	2.8k	7
toya.goto	None	483.1M	175	0	0	149	7
None	masahide.reizei	342.6M	990	1	1	555	11
None	saika.miyashita	283.3M	24	0	0	0	3
namiyo.shigenoi	None	270.5M	1.6k	5	0	419	13
others	others	13.2G	807.8k	1.7k	12.9k	257.6k	11.8k

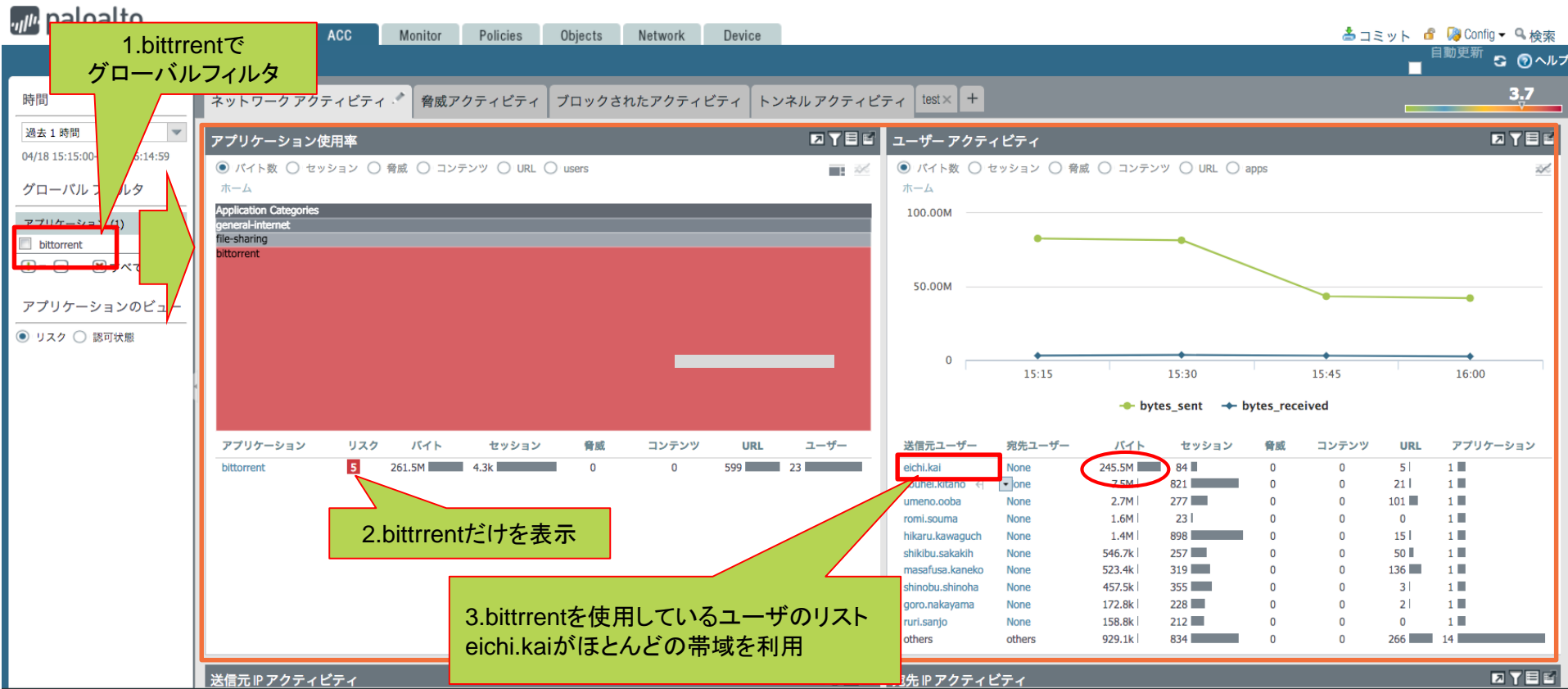
# ① ACC「グローバルフィルタ 1」

→ アプリケーションでグローバルフィルタ

1. bittorrentで  
グローバルフィルタ

2. bittorrentだけを表示

3. bittorrentを使用しているユーザのリスト  
eichi.kaiがほとんどの帯域を利用





# 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

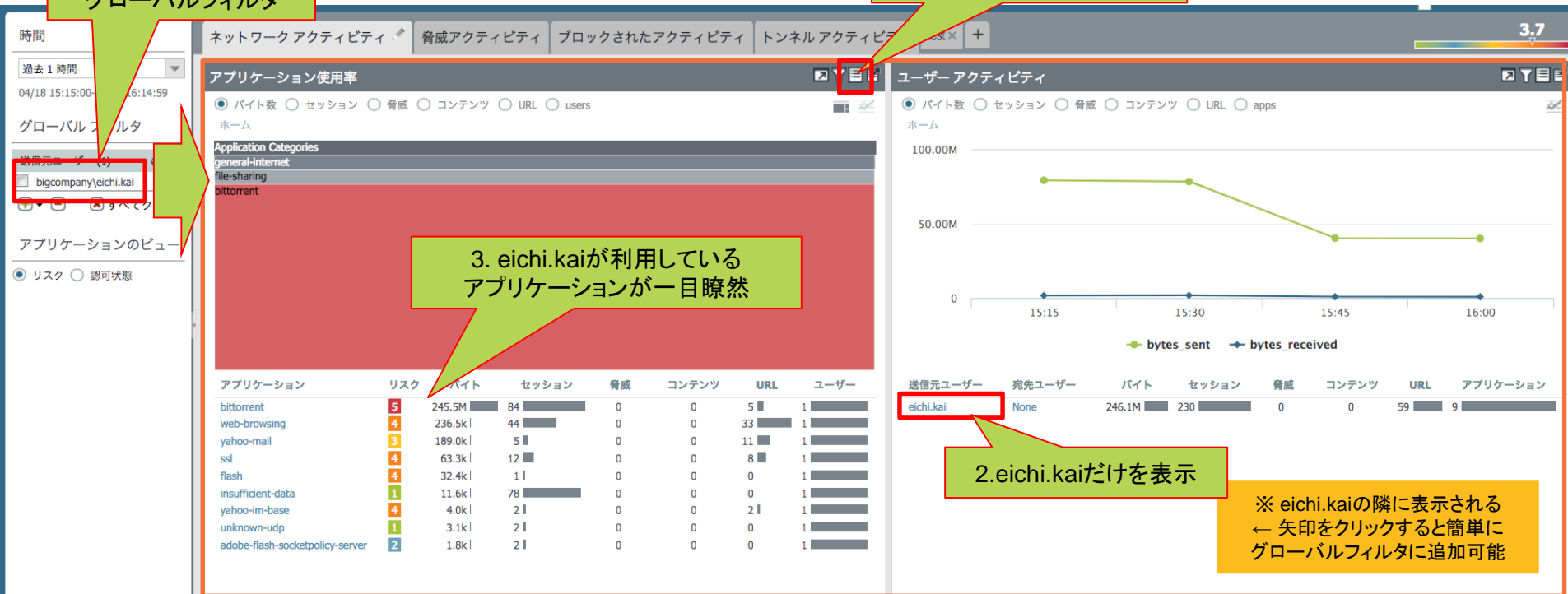
1.eichi.kaiで  
グローバルフィルタ

4. 詳細なログにジャンプ

3. eichi.kaiが利用している  
アプリケーションが一目瞭然

2.eichi.kaiだけを表示

※ eichi.kaiの隣に表示される  
← 矢印をクリックすると簡単に  
グローバルフィルタに追加可能



# ② Monitor 「概要」

→ 各種ログを確認するための画面

The screenshot shows the Palo Alto Networks Monitor interface. The 'Monitor' tab is selected in the top navigation bar. On the left, a sidebar menu lists various log categories, with 'ログ' (Logs) highlighted. The main area displays a table of log entries. The table has the following columns: 受信日時 (Received Date), タイプ (Type), 送信元ゾーン (Source Zone), 宛先ゾーン (Destination Zone), 送信元 (Source IP), 送信元ユーザー (Source User), 宛先 (Destination IP), 宛先ポート (Destination Port), アプリケーション (Application), アクション (Action), セッション終了理由 (Session End Reason), ルール (Rule), and バイト (Bytes).

	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

The screenshot shows the Palo Alto Networks Panorama interface. The 'Monitor' tab is selected. The left sidebar contains various monitoring tools, with 'ログ' (Log) highlighted. The main area displays a table of traffic logs. A red box highlights the 'Monitor' tab and the left sidebar. A green box highlights a specific row in the table with the text '1.送信元IPをクリックすると' (Clicking the source IP).

	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...				complete	allow	aged-out	Allowed Personal Apps	186
	04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.95				complete	allow	aged-out	Allowed Personal Apps	186
	04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.1.95				http-browsing	allow	aged-out	General Web Infrastructure	68.3k
	04/19 04:23:30	end	L3-TAP	L3-TAP	10.154.5.216	bigc...			http-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

2.自動的にフィルタが作成され

3.フィルタを実行すると

4.フィルタが適用される

	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	206.110.12.2	80	incomplete	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	206.110.12.2	80	incomplete	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	206.110.12.2	80	incomplete	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



詳細ログビュー

全般

セッション ID 38529  
アクション reset-both  
アプリケーション web-browsing  
ルール DailyDecrypt-Transfer-Deny  
仮想システム  
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 ToUSIRAMA  
生成日時 2018/04/18 17:43:33  
受信日時 2018/04/18 17:43:33  
トンネルタイプ N/A

送信元

攻撃者名  
攻撃者 192.168.30.201  
国 192.168.0.0-192.168.255.255  
ポート 443  
ゾーン L3-TAP  
インターフェイス ethernet1/2  
NAT IP 192.168.30.201  
NAT ポート 443

宛先

被害者名  
被害者 192.168.130.157  
国 192.168.0.0-192.168.255.255  
ポート 39807  
ゾーン L3-Trust  
インターフェイス ethernet1/3  
NAT IP 192.168.30.239  
NAT ポート 12860

詳細

脅威タイプ virus  
脅威名 PWS/Win32.fareit.anza  
ID 190297512 (View In Threat Vault)  
カテゴリ pe  
コンテンツのバージョン Antivirus-1036-5130  
重大度 medium  
繰り返し回数 1  
ファイル名 66230eb6821ae3cc14fe1506ecf8a5a...  
URL  
PCAP ID 0  
送信元 UUID  
宛先 UUID

電子メールヘッダ

送信者のアドレス  
サブジェクト

フラグ

キャプティブポータル   
プロキシトランザクション   
復号化   
バケットキャプチャ   
クライアントからサーバー   
サーバーからクライアント   
トンネル検査済み

PCAP	受信日時 ▲	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2018/04/18 17:43:34	end	web-browsing	allow	DailyDecrypt-Transfer-Deny	114473		private-ip-addresses			
	2018/04/18 17:43:33	virus	web-browsing	reset-both	DailyDecrypt-Transfer-Deny		medium	private-ip-addresses			66230eb68...

閉じる

虫眼鏡  
アイコン

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



WHAT WE DO PRODUCTS SERVICES RESOURCES PARTNERS COMPANY

Get Support

EN

## THREAT VAULT

All Source Types  Search

Example queries:

- Hash (md5, sha1, sha256)
- CVE (i.e. CVE-2015-8650)
- Signature ID (i.e. 40020)
- Domain name, URL, or IP address (i.e. microsoft.com)

ここに、  
・ウィルスのハッシュ情報  
・CVE番号  
・シグネチャID  
・ドメイン・URL情報  
をいれて検索

<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



WHAT WE DO PRODUCTS SERVICES RESOURCES PARTNERS COMPANY

Get Support

EN

Home / Test a site

Log-in

### Test A Site

URL

www.eicar.org

SEARCH

**URL:** www.eicar.org

**Category:** Computer and Internet Info

**Description:** General information regarding computers and the internet.

**Example Sites:** www.redhat.com, www.freebsd.org, www.microsoft.com, www.symantec.com, www.oreilly.com, www.build-your-own-computers.com, www.alex.com

[Request Change](#)

ここに、URLをいれて検索

私はロボットではありません



reCAPTCHA

[プライバシー](#) - [利用規約](#)

<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



## WILDFIRE

Dashboard Reports Upload Sample Settings Account Hosoya, Yohai

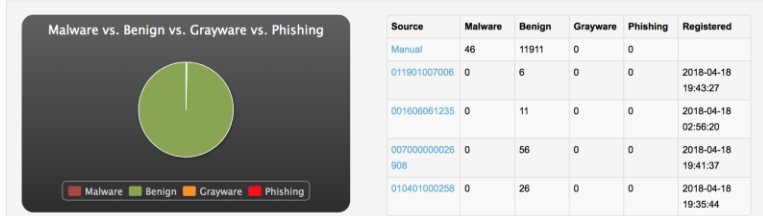
### DASHBOARD

Update your timezone preference in Settings to show report timestamps in your timezone.

#### PREVIOUS 1 HOUR



#### PREVIOUS 24 HOUR



### DYNAMIC ANALYSIS

Virtual Machine 1 Virtual Machine 2

This virtual machine is configured with the following software: Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007.

### BEHAVIORAL SUMMARY

This sample was found to be malware on this virtual machine.

Behavior	Severity
▲ This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	
▲ Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
▲ Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
▲ Started a process from a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Malware often runs executable content out of these folders to avoid detection, while legitimate applications are usually run out of the Windows, Windows system, or Program Files folders.	
▲ Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	

### NETWORK ACTIVITY

No network data available.

### HOST ACTIVITY (BY PROCESS)

Select a process below to view detailed forensics on the activities performed on the host by individual processes.

c:\documents and settings\administrator\sample.exe



# 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)



Common Vulnerabilities and Exposures

CVE List

CNAs

Board

About

News & Blog

NVD

Go to for:

[CVSS Scores](#)

[CPE Info](#)

[Advanced Search](#)

Search CVE List

Download CVE

Data Feeds

Request CVE IDs

Update a CVE Entry

TOTAL CVE Entries: 99655

HOME > CVE > CVE-2017-7600

[Printer-Friendly View](#)

## CVE-ID

**CVE-2017-7600** [Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

## Description

LibTIFF 4.0.7 has an "outside the range of representable values of type unsigned char" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.

## References

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- [MISC:https://blogs.gentoo.org/ago/2017/04/01/libtiff-multiple-ubsan-crashes](https://blogs.gentoo.org/ago/2017/04/01/libtiff-multiple-ubsan-crashes)
- DEBIAN:DSA-3844
- [URL:http://www.debian.org/security/2017/dsa-3844](http://www.debian.org/security/2017/dsa-3844)
- GENTOO:GLSA-201709-27
- [URL:https://security.gentoo.org/glsa/201709-27](https://security.gentoo.org/glsa/201709-27)
- UBUNTU:USN-3602-1
- [URL:https://usn.ubuntu.com/3602-1/](https://usn.ubuntu.com/3602-1/)

## Assigning CNA

MITRE Corporation

Date Entry Created

[http://cve.mitre.org/cve/search\\_cve\\_list.html](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

### 脆弱性対策情報データベース検索

検索キーワード:  検索 [検索の使い方](#)

類義語:

ベンダ名:

製品:

公表日: 年 月 ~ 年 月

最終更新日: 年 月 ~ 年 月

深刻度(CVSSv3):  緊急: (9.0~10.0)  重要: (7.0~8.9)  警告: (4.0~6.9)  注意: (0.1~3.9)  なし: (0)

深刻度(CVSSv2):  危険: (7.0~10.0)  警告: (4.0~6.9)  注意: (0.0~3.9)

CWE:

※「ベンダ名/製品名検索」ボタンはInternet Explorer 11、Microsoft Edgeでのみご利用いただけます。

1件中1~1件表示中

ID	タイトル	CVSSv3	CVSSv2	公表日	最終更新日
<a href="#">JVND-2017-003039</a>	<a href="#">LibTIFF におけるサービス運用妨害 (DoS) の脆弱性</a>	7.8	6.8	2017/04/01	2017/05/12

1件中1~1件表示中

LibTIFF におけるサービス運用妨害 (DoS) の脆弱性

Copyright © 2007-2018 IPA. All rights reserved.

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

JVN iPedia 脆弱性対策情報データベース

最終更新日: 2017/05/12

【活用ガイド】

### JVND-2017-003039

#### LibTIFF におけるサービス運用妨害 (DoS) の脆弱性

概要

LibTIFFには、"unsigned char 型の表現可能な範囲外"の未定義の動作問題により、サービス運用妨害 (アプリケーションクラッシュ) 状態にされるなど、不特定の影響を受ける脆弱性が存在します。

#### CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度	CVSS v2 による深刻度
基本値: 7.8 (重要) [NVD値]	基本値: 6.8 (警告) [NVD値]
<ul style="list-style-type: none"><li>攻撃元区分: ローカル</li><li>攻撃条件の複雑さ: 低</li><li>攻撃に必要な特権レベル: 不要</li><li>利用者の関与: 要</li><li>影響の想定範囲: 変更なし</li><li>機密性への影響(C): 高</li><li>完全性への影響(I): 高</li><li>可用性への影響(A): 高</li></ul>	<ul style="list-style-type: none"><li>攻撃元区分: ネットワーク</li><li>攻撃条件の複雑さ: 中</li><li>攻撃前の認証要素: 不要</li><li>機密性への影響(C): 部分的</li><li>完全性への影響(I): 部分的</li><li>可用性への影響(A): 部分的</li></ul>

#### 影響を受けるシステム

LibTIFF

- LibTIFF 4.0.7

#### 想定される影響

リモートの攻撃者により、巧妙に加工された画像を介して、サービス運用妨害 (アプリケーションクラッシュ) 状態にされるなど、不特定の影響を受ける可能性があります。

#### 対策

ベンダ情報および参考情報を参照して適切な対策を実施してください。



# ⑦ VirusTotal

→ Googleの提供するウィルス情報サイト



VirusTotal は、**疑わしいファイルや URL を分析する無料**のサービスです。ウィルス、ワーム、トロイの木馬、あらゆる種類のマルウェアを素早く検出できます。

📁 ファイル   🔗 URL   🔍 検索

ファイルを選択していません   **ファイルを選択**

ファイルの最大サイズ: 64 MB

「スキャンする」をクリックすることで、サービス利用規約に同意したと見なし、このファイルを VirusTotal がセキュリティ コミュニティで共有することに同意したと見なします。  
詳細は [プライバシー ポリシー](#) を参照してください。

**スキャンする**

ウィルスファイルやHash情報で検索

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

SHA256: 9992b05296cbc39c4274b5d16dabab865ff14e09314299fd7b889ca37f0615ff

ファイル名: fb45f3ca7ed8ac9bca3b36779e920f0f.virus

検出率: 46 / 67

分析日時: 2018-02-05 10:53:47 UTC (1 ヶ月, 3 週間前)

分析結果   🔍 ファイルの詳細   追加情報   💬 コメント 0   🗳️ 投票   📄 挙動情報

ウイルス対策ソフト	結果	更新日
Ad-Aware	Trjant.Zusy.274891	20180225
AegisLab	W32.GandCrypt.tpia	20180225
Abolab.V2	W32.CoinMiner.B220400	20180225

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

The screenshot shows the Palo Alto Networks interface. The 'Monitor' tab is selected. In the left sidebar, 'Threat' is highlighted. A search filter is applied: '( subtype eq vulnerability ) and ( severity eq critical ) and ( action eq alert )'. A table of logs is displayed with the following columns: Receive Time, Severity, Action, Type, Recipient Address, From Zone, and To Zone. The first row of data is: 10/25 19:28:32, critical, alert, vulnerability, [empty], L3-TAP, L3. A magnifying glass icon is visible in the first column of the table, and a red box highlights it.

	Receive Time	Severity	Action	Type	Recipient Address	From Zone	To Zone
	10/25 19:28:32	critical	alert	vulnerability		L3-TAP	L3

→ ( 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  
(ブロックしていない)

# 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



詳細ログビュー

全般	送信元	宛先
セッション ID 62681 アクション alert アプリケーション flash ルール allow_outbound 仮想システム 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 生成日時 2017/07/25 11:15:55 受信日時 2017/07/25 11:15:55 トンネル タイプ N/A	攻撃者名 攻撃者 21 4.116.21 国 United States ポート 80 ゾーン L3-Untrust インターフェイス ethernet1/1 NAT IP 208.94.116.21 NAT ポート 80	被害者名 被害者 192.168.45.32 国 192.168.0.0-192.168.255.255 ポート 52960 ゾーン L3-Trust インターフェイス ethernet1/2 NAT IP 192.168.55.20 NAT ポート 47245

詳細

脅威タイプ vulnerability	脅威名 Adobe Flash Player ByteArray Use After Free Vulnerability
ID 38051	(View in Threat Vault)
カテゴリ code-execution	コンテンツID AppThreat-41487-46850
重大度 critical	繰り返し回数 1
ファイル名 adobe_flash_hacking_team_uaf...	URL
PCAP ID 0	送信元 UUID
宛先 UUID	

電子メールヘッダ

送信者のアドレス	
サブジェクト	

フラグ

- キャプティブポ
- プロキシション
- 復号化
- パケット キャプ
- クライアントから
- サーバーからク
- ライアント
- トンネル検査済

ログリンク

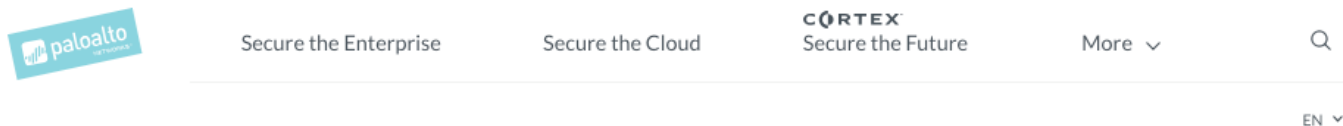
- ipinfo.io.src
- ipinfo.io.dst

PC...	受信日時 ▲	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2017/07/25 11:16:46	end	flash	allow	allow_outb...	56041		malware			
	2017/07/25 11:17:51	wildfire	flash	allow	allow_outb...		high	malware	mal...		adobe_flas...
	2017/07/25 11:15:55	vulnerability	flash	alert	allow_outb...		critical	malware			adobe_flas...
	2017/07/25 11:15:55	file	flash	alert	allow_outb...		low	malware			adobe_flas...
	2017/07/25 11:15:46	url	web-browsing	alert	allow_outb...		informational	malware		malwa...	
↓	2017/07/25 11:15:46	wildfire-virus	flash	alert	allow_outb...		medium	malware			malware.w...

閉じる

# 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



## THREAT VAULT

All Source Types  Search

### Vulnerability Protection Signatures ▾

Showing 1 to 1 of 1 rows

Signature	Severity	CVE	First Release	Last Update
Name: Adobe Flash Player ByteArray Use After Free Vulnerability Unique Threat ID: 38051	critical	CVE-2015-5119 CVE-ID	521 (2015-08-12 UTC)	684 (2017-04-11 UTC)

概要



# 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

The screenshot shows the Palo Alto Networks Monitor interface. The 'Monitor' tab is selected. A search filter '(severity eq critical) and (action eq alert)' is applied. The table below shows two vulnerability alerts. The first alert, 'Adobe Flash Player ByteArray Use After Free Vulnerability', has an '例外' (Exception) button highlighted with a red box. The second alert is 'WordPress Login Brute Force Attempt'.

	受信日時	タイプ	名前	送信元ゾーン	重大度	アクション	ID
	07/25 11:15:55	vulnerability	Adobe Flash Player ByteArray Use After Free Vulnerability	Trust	critical	alert	38051
	07/25 10:51:54	vulnerability	WordPress Login Brute Force Attempt	Trust	critical	alert	40044

# 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

The screenshot displays the '脅威詳細' (Threat Details) window for the vulnerability 'Adobe Flash Player ByteArray Use After Free Vulnerability'. The interface includes the following elements:

- 名前:** Adobe Flash Player ByteArray Use After Free Vulnerability
- ID:** 38051 (View in Threat Vault)
- 内容:** Adobe flash player is prone to a ByteArray use after free vulnerability while parsing certain crafted flash file. The vulnerability is due to the lack of proper checks on flash file, leading to an exploitable ByteArray use after free. An attacker could exploit the vulnerability by sending a crafted flash file. A successful attack could lead to remote code execution with the privileges of the current logged-in user.
- 重大度:** CRITICAL
- リファレンス:** <https://helpx.adobe.com/security/products/flash-player/apsb15-16.html>
- バグトラック ID:** CVE CVE-2015-5119 (with a red arrow pointing to 'CVEへのリンク')
- ベンダー ID:** APSB15-16

At the bottom, there is a table with columns for 'プロファイルの免除' (Profile Exemption) and '現在のセキュリティルールで使用' (Used in Current Security Rules). The table contains one entry: 'IP アドレスの免除' (IP Address Exemption). Buttons for '追加' (Add) and '削除' (Remove) are located at the bottom right of the table. The window also features 'OK' and 'キャンセル' (Cancel) buttons at the very bottom.

# 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

最終更新日:  
2015/08/21

**JVN iPedix** 脆弱性対策情報データベース

【活用方】

### 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

概要

Adobe Flash Player および Adobe AIR には、任意のコードを実行される、またはサービス運用妨害 (メモリ破損) 状態にされる脆弱性が存在します。

本脆弱性は、CVE-2015-3117、CVE-2015-3123、CVE-2015-3130、CVE-2015-3133、CVE-2015-3134、および CVE-2015-4431 とは異なる脆弱性です。

CVSS による深刻度 (CVSS とは?)

CVSS v2 による深刻度  
基本値: 10.0 (危険) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低
- 攻撃前の認証要素: 不要
- 機密性への影響(C): 全面的
- 完全性への影響(I): 全面的
- 可用性への影響(A): 全面的

情報不足のため、「攻撃条件の複雑さ」のスコアは、「低」に設定されています。

影響を受けるシステム

Google

- Google Chrome

アドビシステムズ

- Adobe AIR デスクトップランタイム 18.0.0.180 未満 (Windows/Macintosh)
- Adobe AIR SDK 18.0.0.180 未満 (Windows/Macintosh/Android/iOS)

## 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

The screenshot shows the Palo Alto Networks interface. The 'Monitor' tab is selected. A search filter is applied: `(subtype eq virus) and (action eq alert) and ((app eq pop3) or (app eq imap))`. Below the filter, a table displays log entries. The first entry is highlighted with a red box, showing a virus alert for 'Exploit/Win32.execod.r' detected in a PDF file.

	受信日時	重大度	アクション	タイプ	名前	脅威カテゴリ	送信元ゾ
	10/25 18:18:32	medium	alert	virus	Exploit/Win32.execod.r	pdf	L3-TAP

(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

詳細ログビュー

全般	送信元	宛先
セッション ID 764185 アクション alert アプリケーション <b>pop3</b> ルール Unexpected Traffic 仮想システム 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 ToUS1RAMA 生成日時 2017/10/25 18:18:32 受信日時 2017/10/25 18:18:32 トンネルタイプ N/A	攻撃者名 <b>攻撃者 10.XX.X.10.139</b> 国 10.0.0.0-10.255.255.255 ポート 110 ゾーン L3-TAP インターフェイス ethernet1/2	被害者名 <b>被害者 66.XX.X.2.XX</b> 国 United States ポート 51008 ゾーン L3-TAP インターフェイス ethernet1/2

詳細

脅威タイプ virus 脅威名 <b>Exploit/Win32.execod.r</b> ID <b>29823399</b> <a href="#">View in Threat Vault</a> カテゴリ pdf コンテンツのバリエーション Antivirus-22283-26889 重大度 medium 繰り返し回数 1 ファイル名 n8dABg8Cocb.PDF URL PCAP ID 0 送信元 UUID 宛先 UUID
--

電子メールヘッダ

送信者のアドレス From: RT80XBleKD@VqJtrsAVh...
サブジェクト Sub: EgyYKcUxfLBQdudknmg3z...

フラグ

- キャプティブポータル
- プロキシション
- 復号化
- パケットキャプチャ
- クライアントから
- サーバーからクライアント
- トンネル検査済み

PC...	受信日時 ▲	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2017/10/25 18:18:34	end	pop3	allow	Unexpected Traffic	3630		any			
	2017/10/25 18:18:32	wildfire-virus	pop3	alert	Unexpected Traffic		medium	any			n8dABg8...
	2017/10/25 18:18:32	virus	pop3	alert	Unexpected Traffic		medium	any			n8dABg8...
	2017/10/25 18:18:32	vulnerability	pop3	alert	Unexpected Traffic		informational	any			n8dABg8...

## 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

### THREAT VAULT

All Source Types ▾  Search

#### Antivirus Signatures ▾

Showing 1 to 1 of 1 rows

Signature	Release	Hashes <span>md5 sha1 sha256</span>
Name: Exploit/Win32.execod.r Unique Threat ID: 29823399 Create Time: 2014-09-08 15:44:42 (UTC)	Threat ID: 1100906 Current Release: 2242 (2017-05-12 UTC) First Release: 1368 (2014-09-10 UTC)	a97f5623aa45d1459f5e4943e62f6a93

登録日時


ハッシュ情報

1つのシグネチャで、亜種を含めた複数のウィルスに対応しているため、複数行表示されることがある


## 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

### THREAT VAULT

All Source Types ▾ a97f5623aa45d1459f5e4943e62f6a93 Search 

#### File Information ▾

File Type	PDF
sha256	a1a092505de9f2d10c37e515b8d51978c2a5ccf23a5a8643d1359e49572d9ae5
sha1	0619a21ffdee8b3635de3552d2b6722ee40d04aa
md5	a97f5623aa45d1459f5e4943e62f6a93
Size	923
Create Time	2014-09-08 15:44:42 (UTC)
WildFire	malware
VirusTotal	

## 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



SHA256: a1a092505de9f2d10c37e515b8d51978c2a5ccf23a5a8643d1359e49572d9ae5

File name: a1a092505de9f2d10c37e515b8d51978c2a5ccf23a5a8643d1359e49572d9ae5.pdf

Detection ratio: 35 / 55 55社のウィルス対策製品のうち、35社がウィルスと判定

Analysis date: 2016-09-21 15:02:56 UTC ( 1 year, 1 month ago )

Analysis File detail Relationships Additional information Comments 0 Votes

Antivirus	Result	Update
Ad-Aware	Exploit.RealPir.K	20160921
AegisLab	Exploit.Script.Generic[2]781c	20160921
ALYac	Exploit.CVE-2009-4324.Gen	20160921
Arcabit	Exploit.RealPir.K	20160921
Avast	JS:Pdfka-gen [Exp]	20160921
AVG	Exploit	20160921
Avira (cloud)	EXP:Pdfka-gen [Exp]	20160921

ウイルス解析エンジンの一覧



## 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

The screenshot shows the Palo Alto Networks Monitor interface. The 'Monitor' tab is selected. In the left sidebar, the 'WildFireへの送信' (Send to WildFire) menu item is highlighted. The search bar contains the filter '( verdict eq malicious )'. Below the search bar, a table of traffic logs is displayed with the following columns: 受信日時 (Received Time), URL, 送信元ゾーン (Source Zone), 宛先ゾーン (Destination Zone), 攻撃者 (Attacker), 攻撃者名 (Attacker Name), 被害者 (Victim), and 宛先ポート (Destination Port).

受信日時	URL	送信元ゾーン	宛先ゾーン	攻撃者	攻撃者名	被害者	宛先ポート
08/29 11:05:20		L3-TAP	L3-TAP	66.1.1.5		10.154.10.167	25
08/29 11:05:18		L3-TAP	L3-TAP	66.1.1.2		10.154.10.151	25
08/29 11:05:17		L3-TAP	L3-TAP	66.1.1.0		10.154.10.103	25

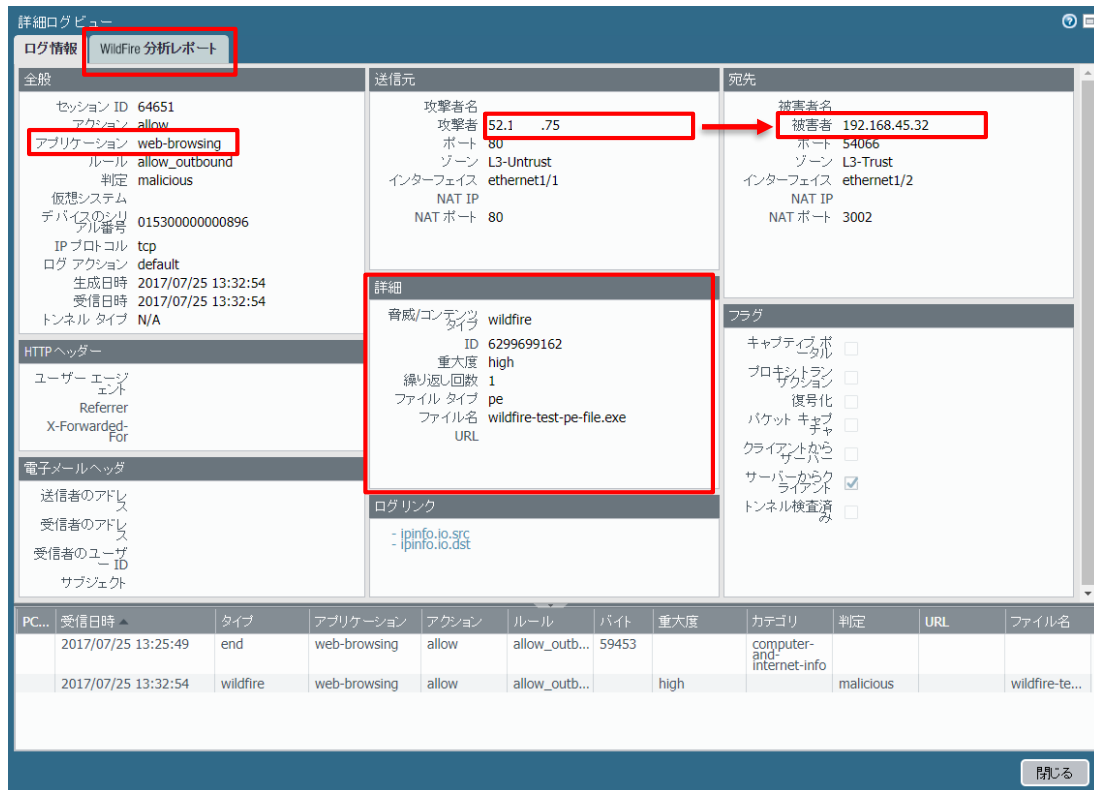
→ ( verdict eq malicious )

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



詳細ログビュー

ログ情報 WildFire 分析レポート

全般	送信元	宛先
セッション ID 64651 アクション allow アプリケーション web-browsing ルール allow_outbound 判定 malicious 仮想システム デバイスID 01530000000896 IP プロトコル tcp ログ アクション default 生成日時 2017/07/25 13:32:54 受信日時 2017/07/25 13:32:54 トンネル タイプ N/A	攻撃者名 攻撃者 52.1.75 ポート 80 ゾーン L3-Untrust インターフェイス ethernet1/1 NAT IP NAT ポート 80	被害者名 被害者 192.168.45.32 ポート 54066 ゾーン L3-Trust インターフェイス ethernet1/2 NAT IP NAT ポート 3002

HTTP ヘッダー

ユーザー エージェント	Referrer
X-Forwarded-For	

電子メールヘッダー

送信者のアドレス	受信者のアドレス	受信者のユーザー ID	サブジェクト
----------	----------	-------------	--------

詳細

脅威/コンテンツタイプ	wildfire
ID	6299699162
重大度	high
繰り返し回数	1
ファイルタイプ	pe
ファイル名	wildfire-test-pe-file.exe
URL	

フラグ

キャプティブル	<input type="checkbox"/>
プロキシラン	<input type="checkbox"/>
復号化	<input type="checkbox"/>
パケットキャプ	<input type="checkbox"/>
クライアントから	<input type="checkbox"/>
サーバーからク	<input checked="" type="checkbox"/>
トンネル検査済	<input type="checkbox"/>

ログリンク

- ipinfo.io.src
- ipinfo.io.dst

PC...	受信日時	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2017/07/25 13:25:49	end	web-browsing	allow	allow_outb...	59453		computer-and-internet-info			
	2017/07/25 13:32:54	wildfire	web-browsing	allow	allow_outb...		high		malicious		wildfire-te...

閉じる

## 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

The screenshot shows the WildFire Analysis Summary page. Key elements are annotated with callouts:

- PDFレポートのダウンロード**: Points to the "Download PDF" button.
- 検体のダウンロード**: Points to the "Download File" link under the "Sample File" section.
- サンドボックス解析結果**: Points to the "Suspicious File Properties" section.

**File Information**

File Type	PE
File Signer	
SHA-256	a206eae01433e46fb47eb3bb045f8f7be06a3aec38da63f1536427acc6a7b3c8
SHA1	149f1a5ef329a967fa9ab956806b60540359e5e0
MDS	44dcd3deefc93f6fe2443668906a7dc7
File Size	55296 bytes
First Seen Timestamp	2017-07-25 04:24:48 UTC
Verdict	malware
Sample File	Download File

**Coverage Status**

For endpoint anti-virus coverage information for this sample, visit [Virus Total](#)

**Static Analysis**

**Suspicious File Properties**

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

- Contains an invalid checksum
- Contains sections set to both writable and executable
- Contains sections with size discrepancies

PC...	受信日時	タイプ	アプリケーション	アクション	ルール	バイト	重大度	カテゴリ	判定	URL	ファイル名
	2017/07/25 13:25:49	end	web-browsing	allow	allow_o...	59453		comput... and-internet-info			
	2017/07/25 13:32:34	wildfire	web-browsing	allow	allow_o...		high		malicious		wildfire...

## ③-4 Virus Totalでの調査結果



### File not found

The file you are looking for is not in our database.

[Take me back to the main page](#)

[Try another search](#)

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

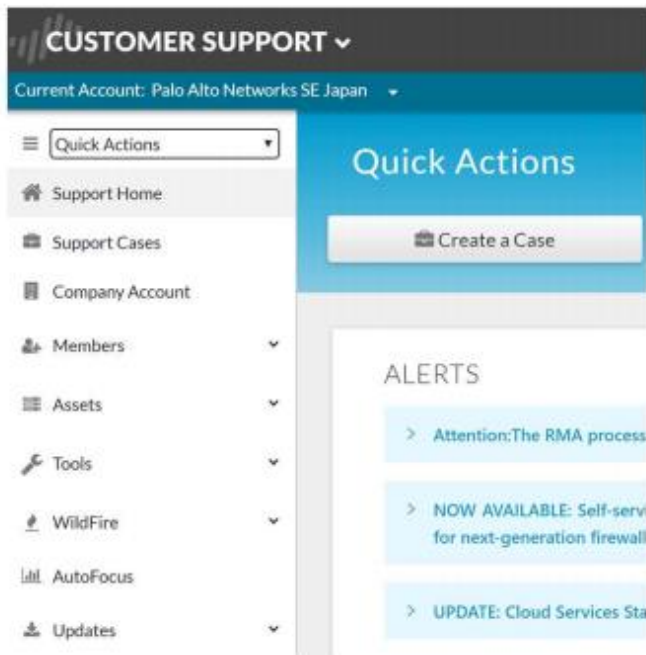
1. ACCとMonitorについて
2. 切り分けに利用するサービス
  - ① パロアルトネットワークスが提供するサービス
  - ② その他外部サービス
3. 検知時の対応方法
  - ① ウィルス検出時の切り分け例
  - ② 攻撃検出時の切り分け例
  - ③ WildFireによる未知のマルウェア検出時の切り分け例
4. **CSPアカウントについて**
5. まとめ
6. 参考情報
  - ① デモサイトについて
  - ② NextWaveパートナー制度について

# 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 카테고리 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

Resources

Live Community

Knowledge Base

Technical Documentation

Applopedia

Learning Center

Security Advisories

Security Lifecycle Review

Threat DB



Knowledge Base

Technical Documentation

Search:

CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	2018 Application Characterist
533 business-systems	04 audio-streaming	1097 browser-based	1000	822 Evolve
620 collaboration	22 auth-service	1201 client-server	738	640 Executive Bandwidth
498 general-internet	30 database	775 network-protocol	812	372 Phone to Mouse
328 media	08 email	103 peer-to-peer	281	708 SaaS
466 networking	04 encrypted-tunnel		140	1234 Transfer Files
	60 esp-ctrl			389 Transfer Other Appl
	021 file-sharing			218 Used by Malware
	02 gaming			1163 Vulnerabilities
	103 general-business			1015 Wholly Used
	103 infrastructure			

NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
100saa	general-internet	file-sharing	23	peer-to-peer
10vertpkts	business-systems	esp-ctrl	2	client-server
2und3-viral	collaboration	email	20	browser-based
24spvncflls	business-systems	esp-ctrl	21	browser-based
2stl				
10-base	collaboration	social-networking	21	browser-based
10-posting	collaboration	web-posting	21	browser-based
365-safep-upd-ckts	business-systems	software-update	21	client-server
3pc	networking	ip-protocol	21	network-protocol
4share1	general-internet	file-sharing	23	browser-based
4sync	general-internet	file-sharing	20	client-server

DOCUMENTATION

Best Practices and Methodology Center

Documents, checklists, videos, webinars, best practice assessment tools, and more. Help you learn about and apply security best practices.

New in PAN-OS 9.0: Policy Optimizer

Palo Alto Optimizer strengthens your security posture by closing dangerous policy gaps. Using single workflows, you can leverage intelligence gathered by PAN-OS to easily raise your legacy rules to App-ID based rules.

Applopedia



# 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！

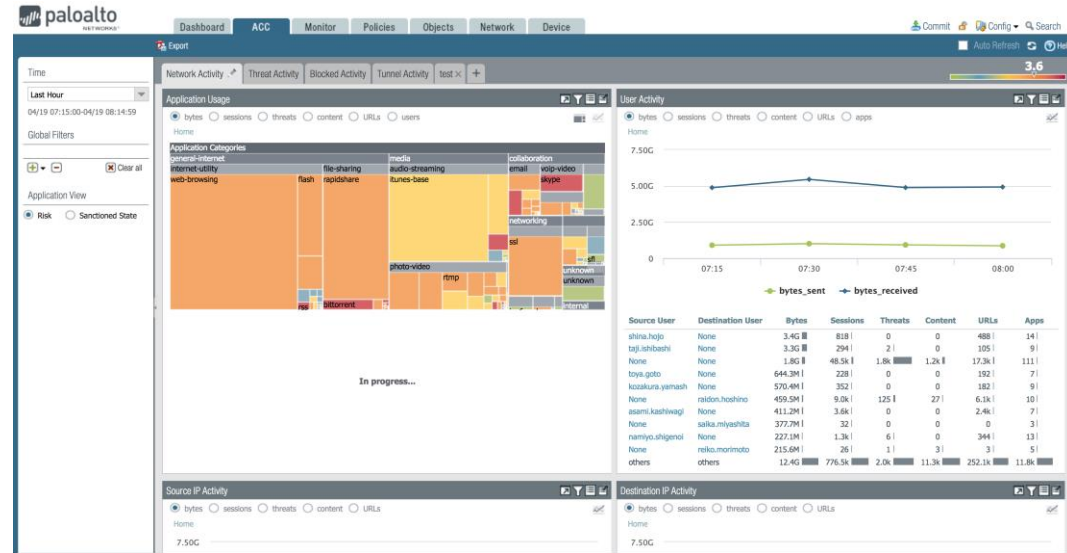


1. ACCとMonitorについて
2. 切り分けに利用するサービス
  - ① パロアルトネットワークスが提供するサービス
  - ② その他外部サービス
3. 検知時の対応方法
  - ① ウィルス検出時の切り分け例
  - ② 攻撃検出時の切り分け例
  - ③ WildFireによる未知のマルウェア検出時の切り分け例
4. CSPアカウントについて
5. まとめ
6. **参考情報**
  - ① **デモサイトについて**
  - ② **NextWaveパートナー制度について**

## 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>  
<https://jp1.rama.demo.paloaltonetworks.com>

} PAシリーズ(VM)  
↳ 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



課題別 製品 サービス 各種情報 パートナー 会社案内

サポート



JP

## パートナーの概要

NextWave/パートナー プログラムは、パロアルトネットワークスのセキュリティ ソリューションを顧客へマーケティング、販売、管理、および提供するリセラー、システムインテグレータ、サービス プロバイダ、マネージドセキュリティ サービス プロバイダ、アライアンス パートナーに対し、ビジネスの成長へ向けて様々な支援を行いながらエコシステムを確立することを目的としています。

NextWaveを活用することで、パートナー様は顧客に、プリセールスおよびポストセールスの付加価値サービスを提供できます。また、販売が促進され、利益が生み出されます。

[詳細はこちら](#)

ここから申請可能

NextWave Partner Portal

Login  
Request Access »

Follow Us | Contact Us »

## パロアルトネットワークスのパートナーになる理由

パロアルトネットワークスは、革新的なプラットフォームを開発することで次世代のネットワーク セキュリティを開拓し続けています。このプラットフォームを導入すると、ネットワークを保護するだけでなく、ネットワーク上で急激にその数を増やし続ける複雑なアプリケーションを安全に使用できるようになります。当社には、世界中で以下の販売先があります。

- 企業
- 政府機関
- サービス プロバイダ

当社の次世代ネットワーク セキュリティ プラットフォームで対応できる市場は、年間支出で100億ドルを超えています。当社は、当社製品のマーケティングと販売、およびユーザーへのサービス提供において、パートナーと協業する多くの機会を創出できるユニークな立場にあります。

## WHY PARTNER WITH PALO ALTO NETWORKS?

### RIGHT MARKET



Increased investment levels for security: \$22.1B opportunity growing with 7.5% CAGR '18-2019\*



Traditional approaches CANNOT PREVENT advanced attacks  
Customers are having to re-architect their systems and networks off legacy point products

<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。





