

Palo Alto Networks

WildFire 脅威分析および防御サービスのご紹介

パロアルトネットワークス株式会社

Mar. 25, 2019



アジェンダ

- WildFire サービスの機能概要
- WildFire グローバルインフラ・キャパシティ・市場評価
- WildFire のライセンスについて
- WildFire プライベート (オンプレミス用アプライアンス WF-500) について
- WildFire 設定イメージ
- WildFire ログイメージ
- WildFire API/ポータルによるファイルアップロード検査
- WildFire Japan アップデート – よくある誤解編
- まとめ

WildFire サービスの機能概要



WildFire の機能

1. サンドボックス機能

未知のサンプル (ファイルまたは電子メール内のハイパーリンク) を検出し、サンドボックス環境で分析を実施、対象の属性・振る舞いに基づき、それらがマルウェアやフィッシングなどの脅威であるかどうかを判別

2. シグネチャのダイナミック更新

WildFire は新しい脅威が発見されると直ちにシグネチャの生成を開始し、完成した新しいシグネチャを 5 分間隔のアップデートで動的に PA ファイアーウォールに配布。また、新しい脅威情報は各リージョンで稼働する WildFire クラウド間でほぼリアルタイムに同期・共有

一連の自動化された防御プロセスにより、PA ファイアーウォール/WildFire を利用するユーザーは常に最新のセキュリティを適用することが可能

3. WildFire API/ポータルサイトの利用 (オンデマンドでのサンドボックス利用)

疑わしいファイルを WildFire API/ポータルサイトを利用してアップロードし、検査を行うことが可能

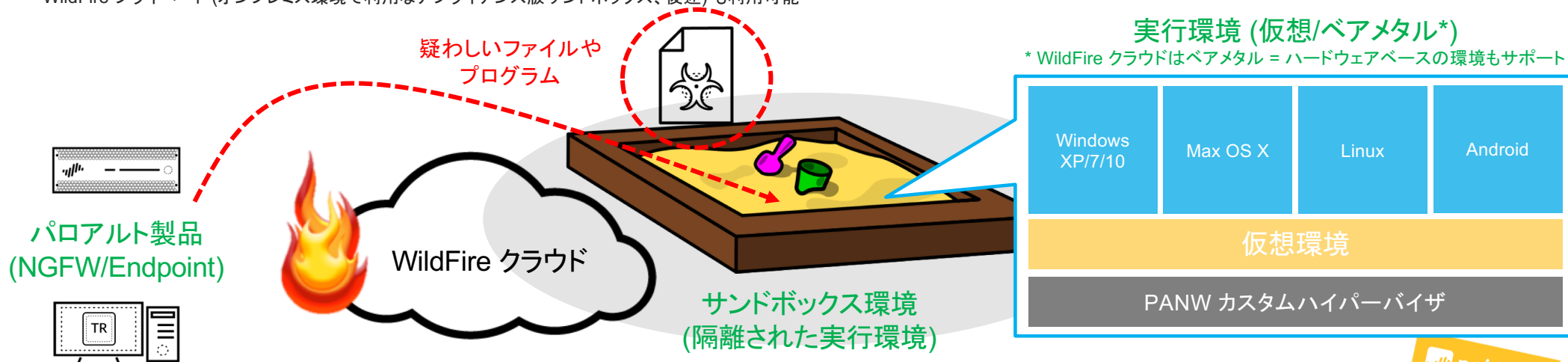
おさらい - サンドボックスとは？

“コンピュータセキュリティ技術において、サンドボックス (sandbox) は、外部から受け取ったプログラムを保護された領域で動作させることによって、システムが不正に操作されるのを防ぐセキュリティ機構のことをいう”

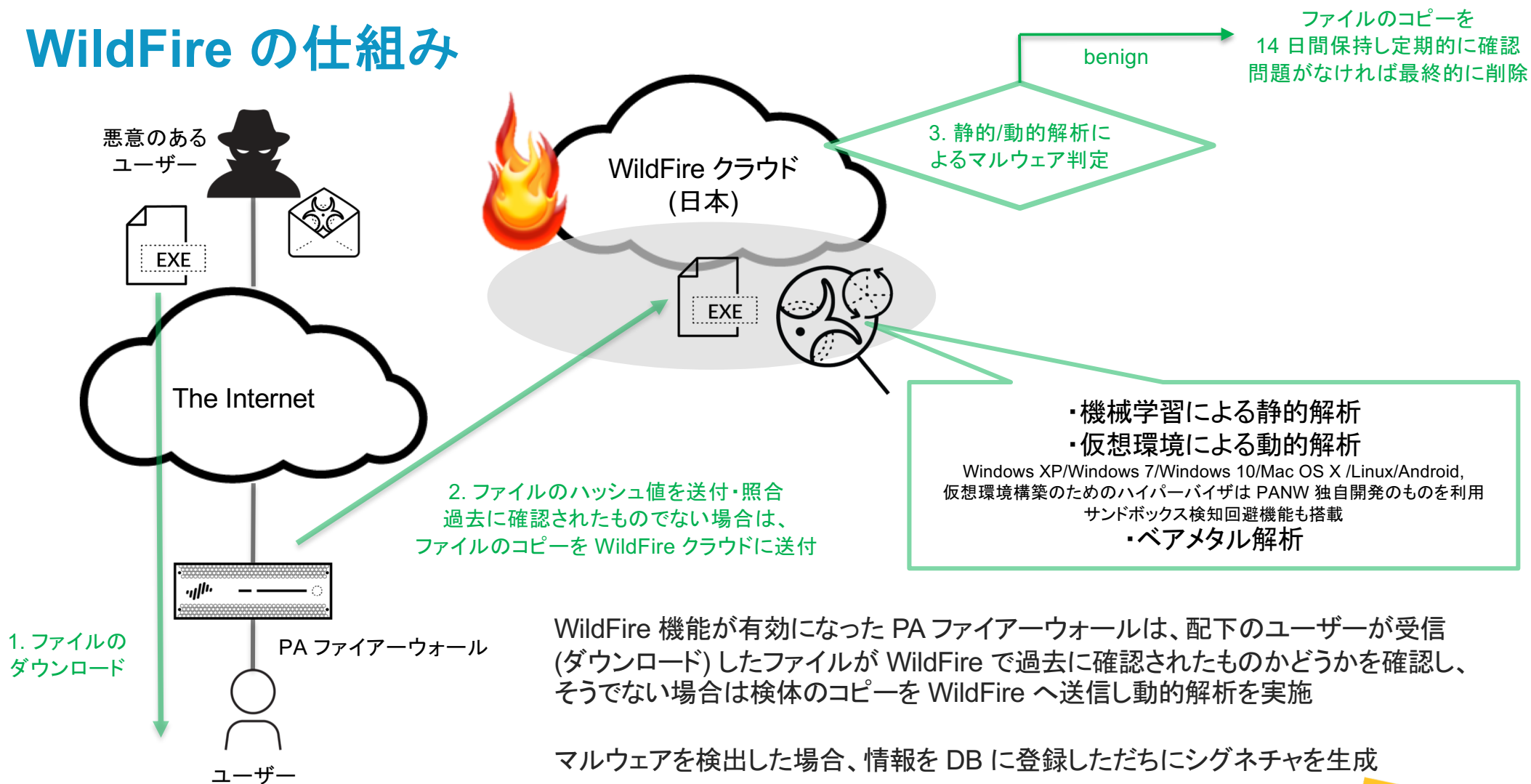
→ 疑わしいファイルやプログラムを実行し分析を行うことが出来る、「攻撃されても問題がない」隔離された仮想の実行環境のこと。未知の攻撃や標的型攻撃への対策として有効

WildFire はパブリッククラウド上に構築されたサンドボックス環境* で、PA ファイアーウォール・Traps エンドポイントセキュリティと連携

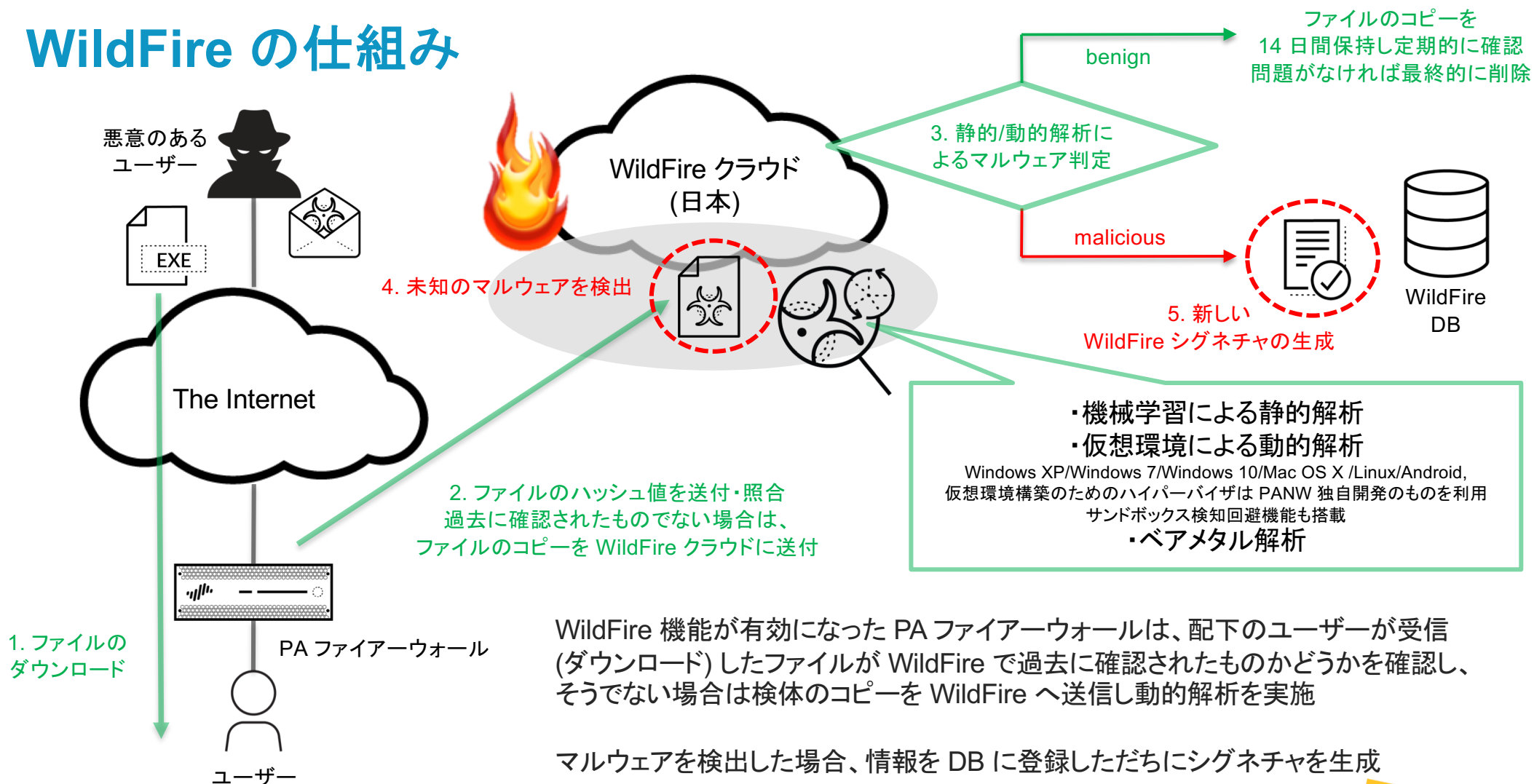
* WildFire プライベート (オンプレミス環境で利用可能なアプライアンス版サンドボックス、後述) も利用可能



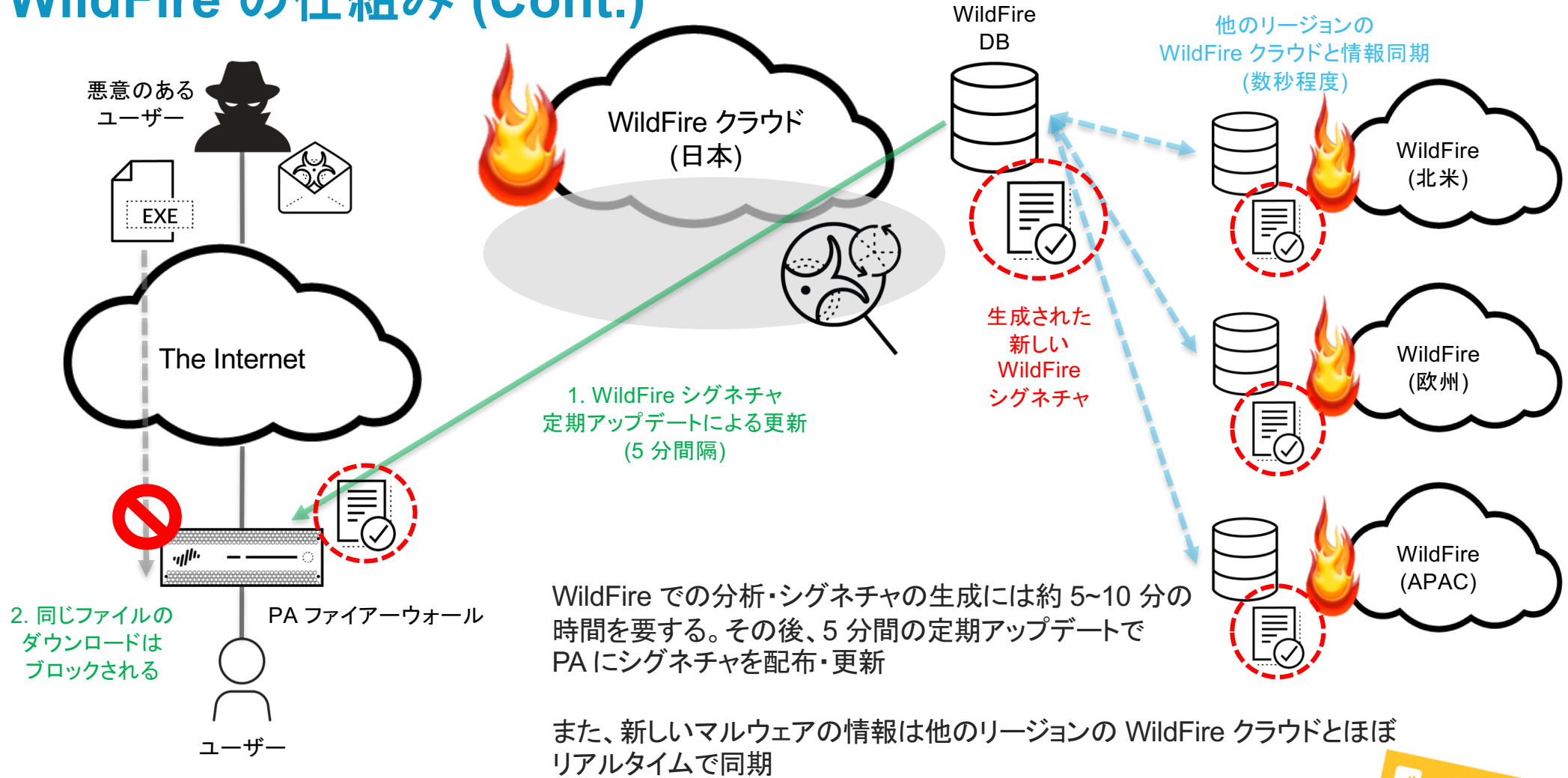
WildFire の仕組み



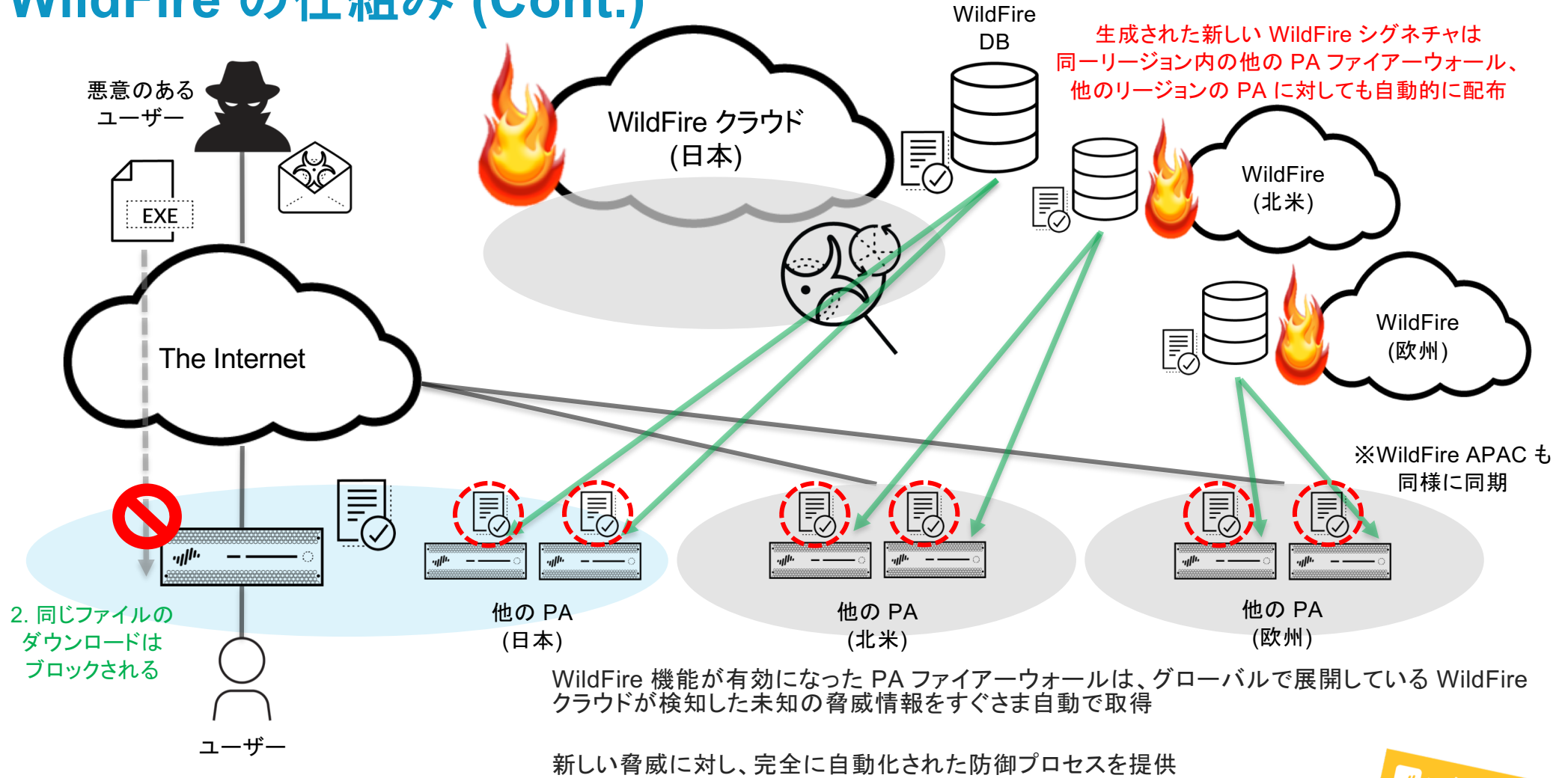
WildFire の仕組み



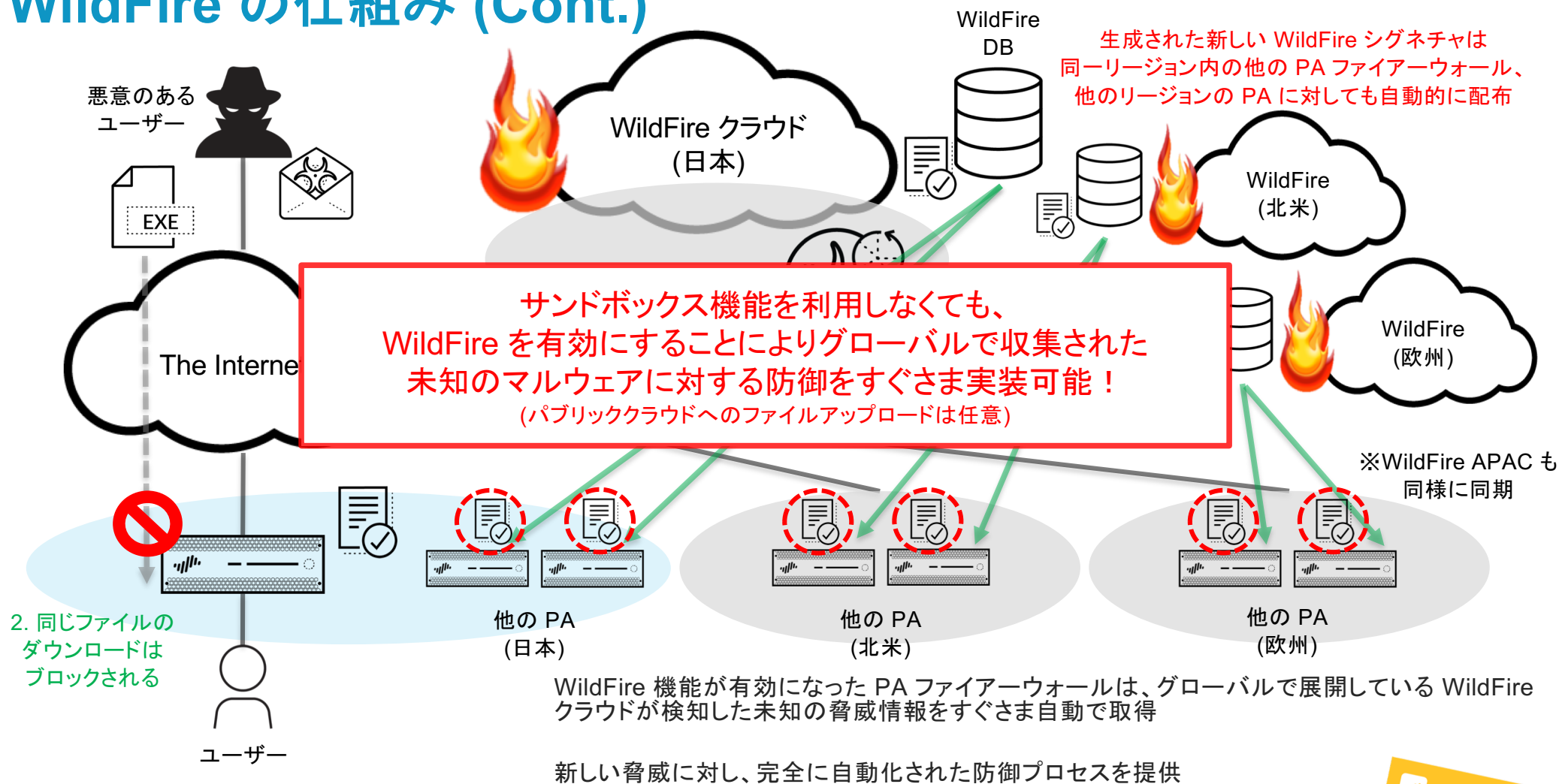
WildFire の仕組み (Cont.)



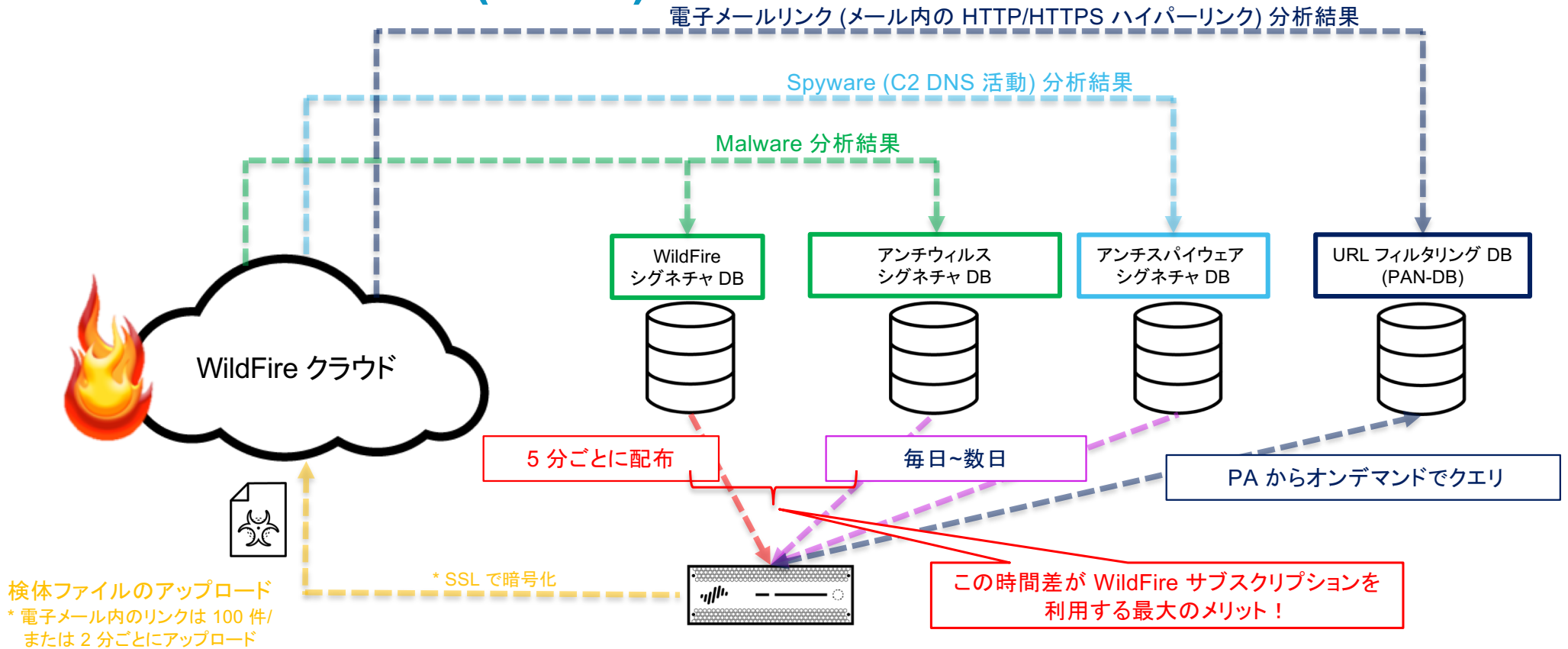
WildFire の仕組み (Cont.)



WildFire の仕組み (Cont.)



WildFire の仕組み (Cont.)



WildFire の分析結果は WildFire シグネチャとして即時に配布されるだけでなく、アンチウイルス/脅威 (アンチスパイウェア) シグネチャの定期アップデート、URL フィルタリング DB のアップデートとしても PA ファイアーウォールに配布・利用可能

WildFire クラウドが分析対象とするファイルタイプ/プロトコル

WildFire クラウド* は、以下のファイルタイプ/通信プロトコルを分析対象としてサポート

- ファイルタイプ
PE (実行可能ファイル、オブジェクトコード、DLL およびフォント)、Microsoft Office (ドキュメント、ワークブック、パワーポイントおよび Office Open XML 2007+ ドキュメント)、Mac OS X (Mach-O, dmg, pkg)、Android apk、PDF、Flash、Java アプレット (jar and class)、アーカイブ (rar および 7-zip)、Linux ELF、Script (JavaScript、VBScript、PowerShell Script)
- プロトコル
 - HTTP/HTTPS (Web)
 - SMTP, IMAP, POP3 (電子メール)
 - FTP, SMB (ネットワークファイル転送・共有)

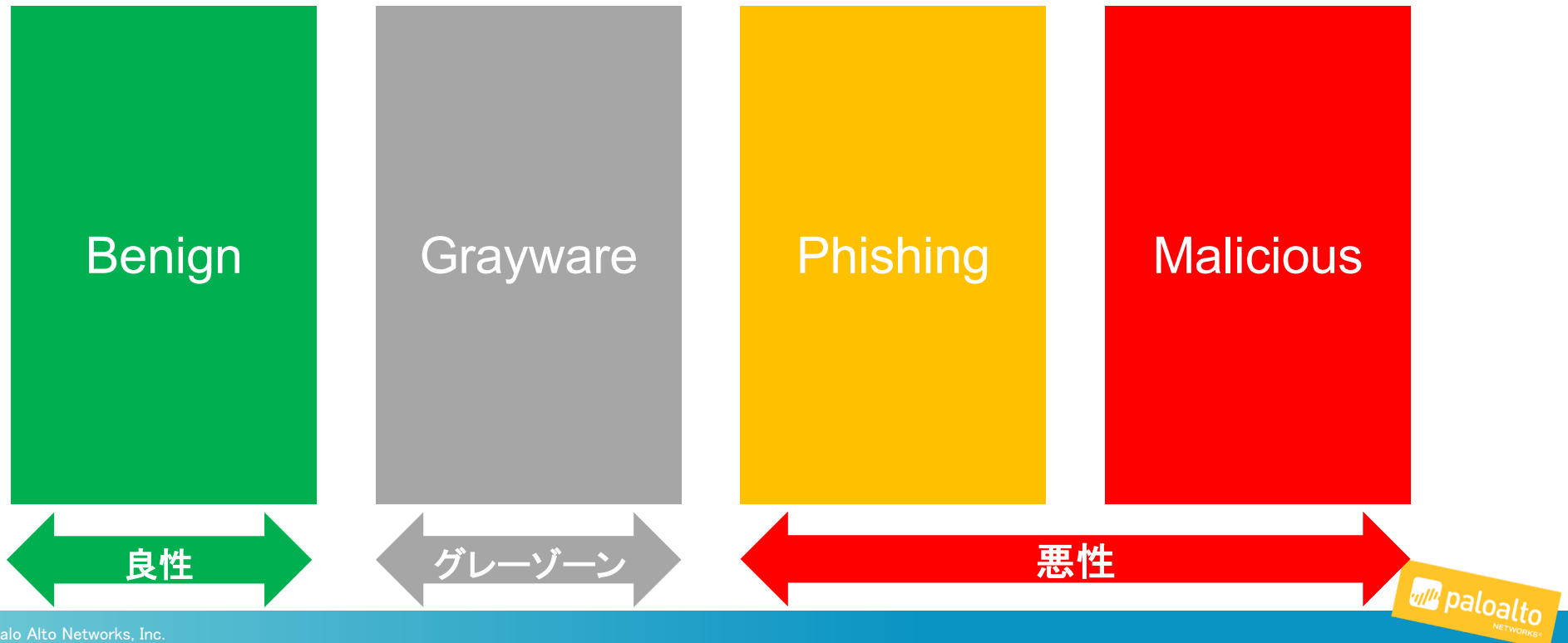
* WildFire プライベートではサポートされる解析環境・ファイルタイプが異なります (後述)

WildFire クラウドが分析対象とするファイルタイプ/プロトコル (Cont.)

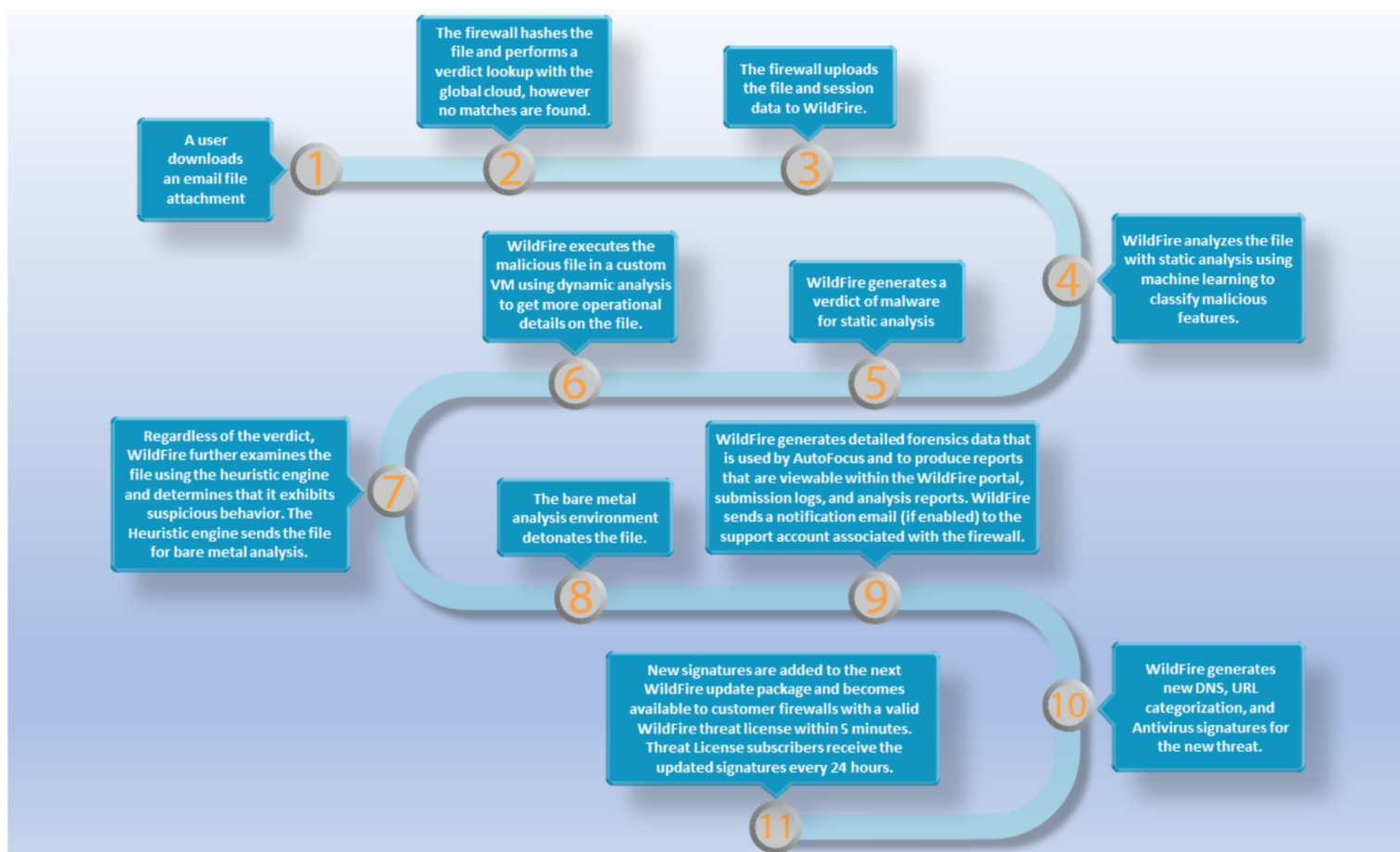
- 電子メールリンク分析
SMTP/POP3 メール内の HTTP/HTTPS ハイパーリンク先にエクスプロイトやフィッシングなどが仕込まれていないかを分析することが可能。また、リンク先がマルウェアと判断された場合、その結果は URL フィルタリング DB に反映
- 圧縮・アーカイブされたファイルの扱い
ZIP ファイル、HTTP 圧縮 (GZIP) は最大 4 階層の圧縮まで展開を試みます。RAR ファイル、7-Zip ファイルは WildFire に送付後、展開されます。パスワードが設定されている場合は展開が出来ないため、分析の対象外
- SSL/TLS 通信の分析について
HTTPS (Web), SMTPS/POPS メール内のリンクの分析には、SSL/TLS 通信の復号が必要

WildFire Verdict (判定 = 分析結果の種別)

- Benign: ファイルは安全で悪意のある振る舞いを行わなかったもの
- Grayware: 直接の脅威となるものではないが、システムに影響を及ぼす振る舞いをする可能性があるもの
- Phishing: フィッシングサイトへのリンクでセキュリティ脅威となるもの
- Malicious: ファイルはマルウェアでセキュリティ脅威となるもの



<ご参考> WildFire 分析 ワークフロー



1. ユーザーが電子メールの添付ファイルをダウンロード
2. PA ファイアウォールはファイルのハッシュ値を取得し、WildFire の判定履歴を確認
3. 履歴がない場合、PA はファイルのコピーとセッション情報を WildFire にアップロード
4. WildFire は機械学習を利用した静的解析で悪意のある特性を分類
5. WildFire は静的解析の判定結果を生成
6. WildFire は仮想環境でファイルを実行・動的解析を実施、ファイルのオペレーション詳細を取得
7. 判定結果に関わらず、WildFire はヒューリスティックエンジンにより疑わしい振る舞いをしないかを確認
8. 必要に応じてベアメタル分析を実施
9. WildFire は AutoFocus* 向けの詳細なフォレンジックデータ生成、レポートやログの出力、PA 管理者への電子メール送信 (設定されている場合) を実施
10. WildFire は新しい DNS, URL カテゴリゼーション、およびアンチウイルスシグネチャを生成
11. 新しいシグネチャが次の WildFire アップデートパッケージに追加。WildFire サブスクリプションライセンスの場合は 5 分、Threat Prevention の場合は 24 時間ごとにシグネチャのアップデートとして受信

WildFire グローバルインフラ・ キャパシティ・市場評価



WildFire インフラストラクチャはどのような形で展開されているのか？

- 北米、欧州、APAC、および日本国内にデータセンターを展開

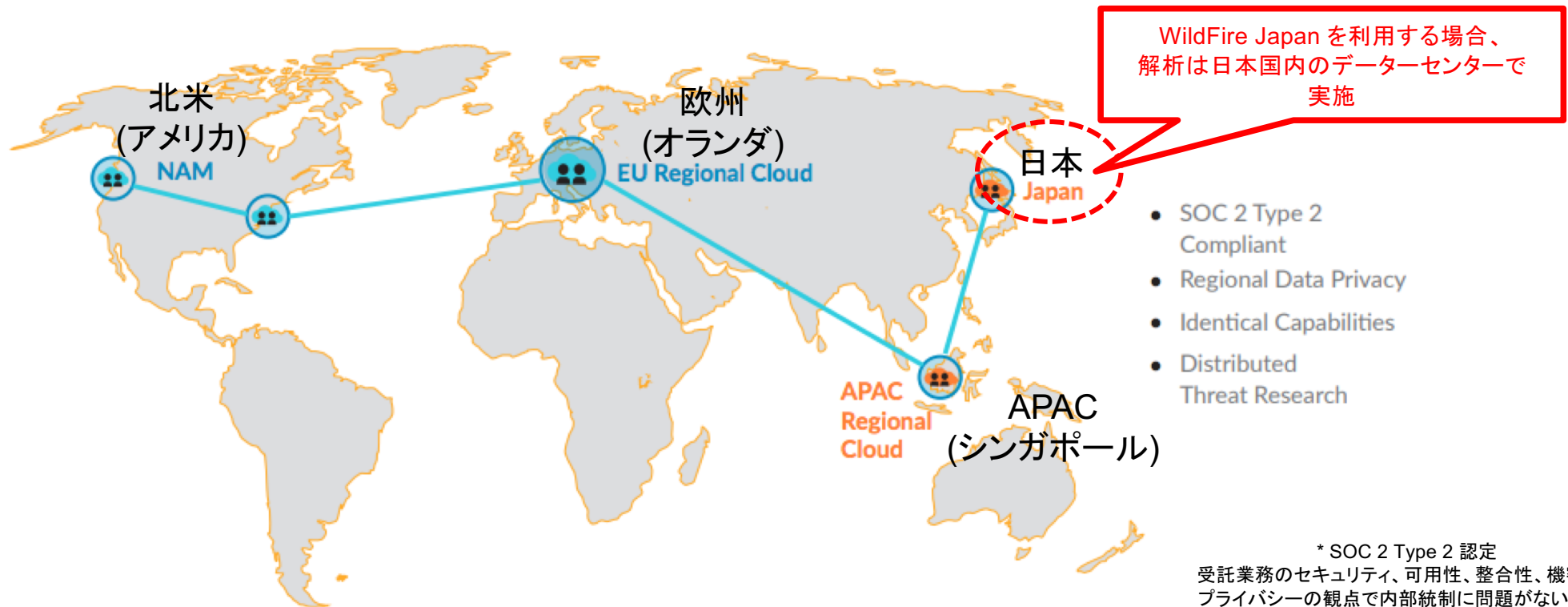


Figure 4: Global WildFire infrastructure provides scale, agility and leverage

WildFire の検体収集能力 - 日々どれくらいの処理を行っているのか？

3 億 5 千万以上

毎月パロアルトネットワークスのサンドボックス
WildFire で実行解析されるファイル数

37.5%

パロアルトネットワークスのサンドボックスWildFire
で発見されたマルウェアの内、
企業向けアンチウイルスソフトウェア
(上位 6 社) で検出した割合 ※1

※1 Average monthly values as of January 2016. Source: Palo Alto Networks WildFire and Multi-Scanner

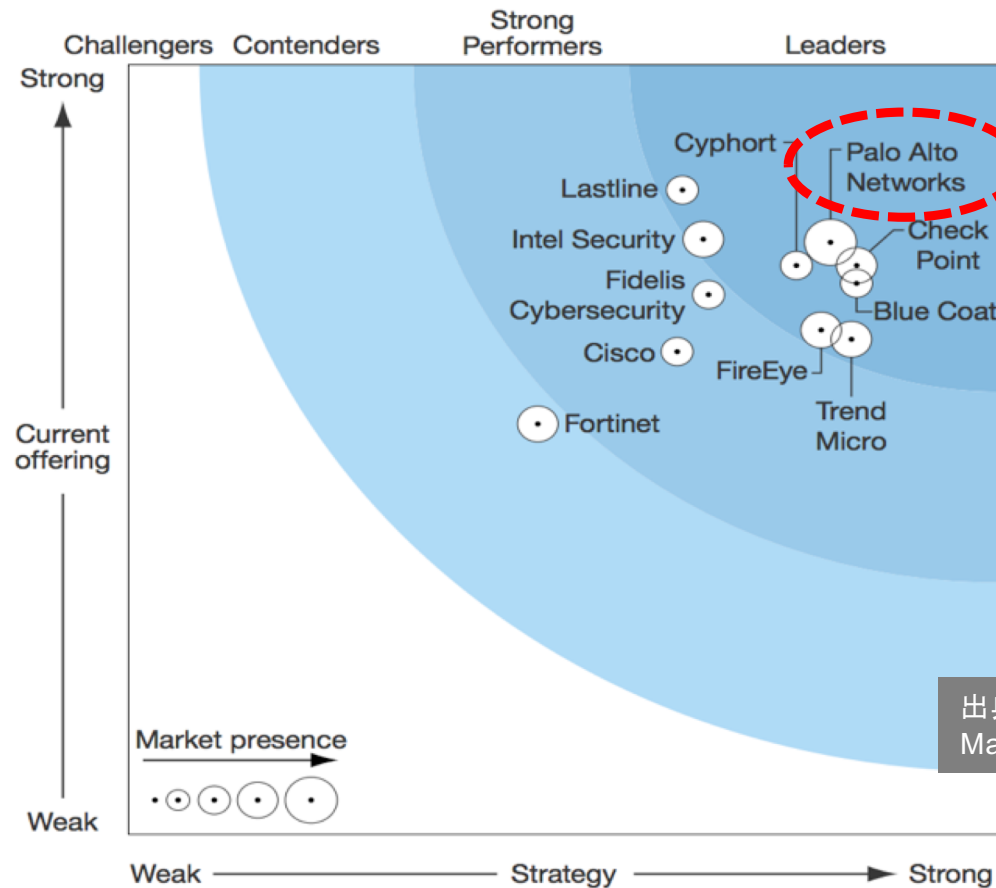
パロアルトネットワークスでは日々、650 万以上のユニークなファイル
を解析し、3~5 万の未知のマルウェアを発見

WildFire に送信されるファイル数

(2年前と比較して、WildFireに送信される
ファイルの数は 50 倍以上)

サンドボックス市場においてどんな評価を受けているのか？

FIGURE 2 Forrester Wave™: Automated Malware Analysis, Q2 '16



第三者リサーチ機関 (Forrester 社) のレポートにて業界リーダーのポジションを獲得

出典: The Forrester Wave™: Automated Malware Analysis, Q2 2016

WildFire のライセンスについて



WildFire のライセンスについて

PA シリーズファイアーウォールは WildFire サブスクリプションライセンスの追加なしでも一部の基本機能 (以下表を参照) を利用可能ですが、サポートされる環境・ファイルタイプが Windows/PE ファイルのみに制限され、最大のメリットである シグネチャのダイナミック更新 (グローバルで展開される WildFire クラウドが検知した未知の脅威に対し直ちに対応) が利用出来ません。

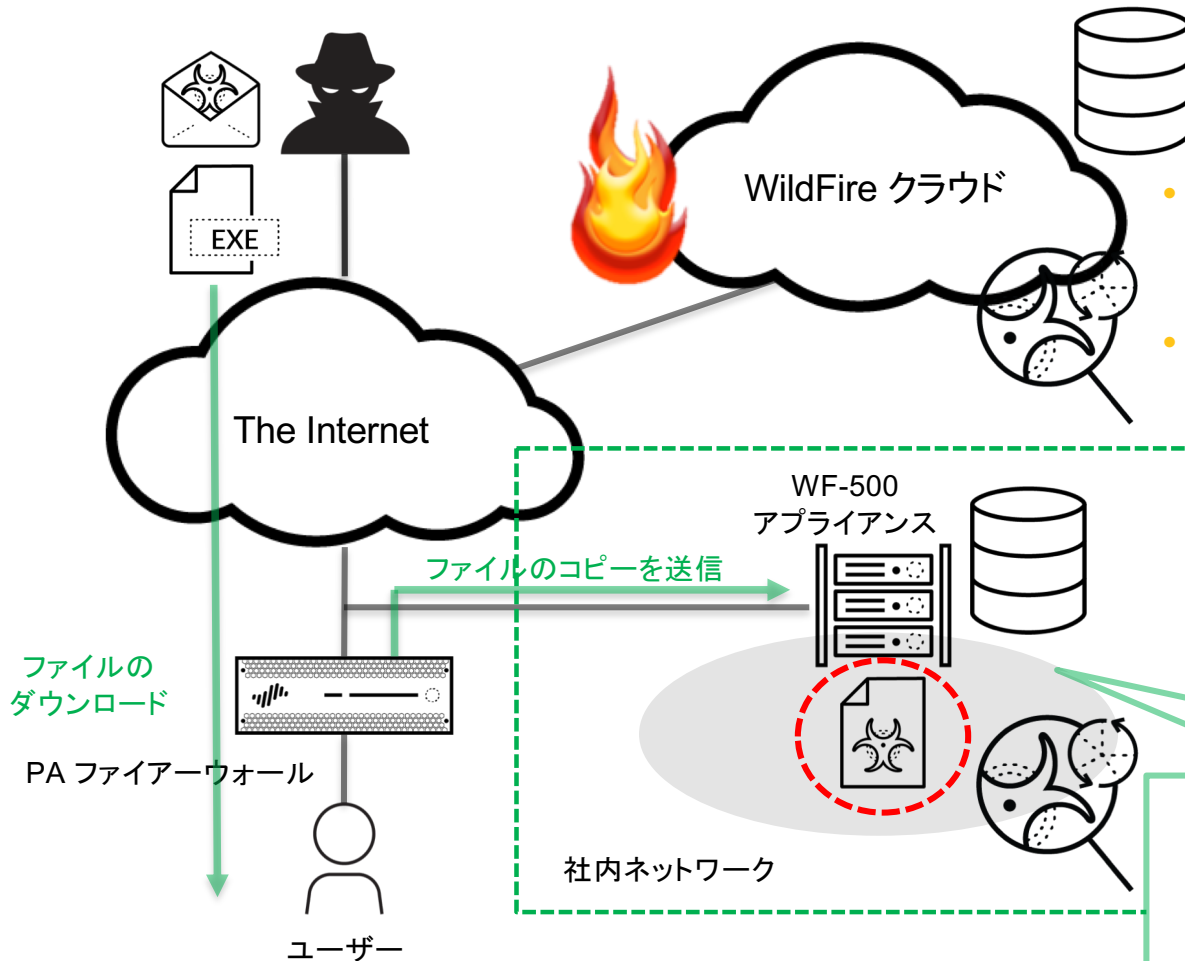
特別な理由がない限り、PANW としては WildFire サブスクリプションを適用頂くことを推奨します。

機能	WildFire サブスクリプションライセンスあり	WildFire サブスクリプションライセンスなし
サポートされるファイルタイプ	Advanced File Type も含め、 全てのファイルタイプをサポート*	PE ファイル (.exe, .obj, .dll, .sys) のみ サポート
WildFire Dynamic アップデート (5 分間隔でのシグネチャアップデート)	○	× (脅威防御サブスクリプションライセンスがあれば、24-48 時間間隔の アンチウイルス/脅威防御シグネチャのアップデートとして利用可)
WildFire API/ポータルの利用	○	×
Archive File Type サポート	○	×
WildFire プライベート/ハイブリッド構成 サポート	○ (プライベート/ハイブリッド = WF-500 利用時はライセンス必須)	×

WildFire プライベート (オンプレミス用アプライアンス WF-500) について



WildFire プライベート (WF-500)



- オンプレミス環境にサンドボックスを配置することが可能
- WildFire クラウドとの併用 (ハイブリッド構成*) も可能

* 一部の機密性の高いファイルのみローカルのサンドボックス環境 (WF-500) を利用し、他は WildFire クラウドを利用、など

オンプレミス環境にサンドボックスを配置することが可能。検体となるファイルが社外のネットワーク (パブリッククラウド) に送出されることはありません！

WildFire クラウド/アプライアンス (WF-500) 機能比較

機能	WildFire クラウド	WildFire プライベート (WF-500) アプライアンス
提供形態	サービス型 (パブリッククラウド)	アプライアンス型 (オンプレミス)
WildFire サブスクリプション	ライセンスなしでも一部機能を利用可能 (Windows/PE ファイルのみ)	必須
解析環境	Windows, Mac OS X, Linux, Android	Windows XP/7 のどちらかを選択
ベアメタル解析サポート	○	×
ファイルサポート	PE (実行可能ファイル, オブジェクトコード, DLL および フォント), Microsoft Office (ドキュメント, ワークブック, パワーポイントおよび Office Open XML 2007+ ドキュメント), Mac OS X (Mach-O, dmg, pkg), Android apk, PDF, Flash, Java アプレット (jar and class), アーカイブ (rar 及び 7-zip), Linux ELF, Script (JavaScript VBScript, PowerShell Script)	PE (実行可能ファイル, オブジェクトコード, DLL および フォント), Microsoft Office (ドキュメント, ワークブック, パワーポイントおよび Office Open XML 2007+ ドキュメント), PDF, Flash, Java アプレット (jar and class),アーカイブ (rar 及び 7-zip)
プロトコルサポート	HTTP/HTTPS, SMTP, POP3, IMAP, FTP, SMB	HTTP/HTTPS, SMTP, POP3, IMAP, FTP, SMB
ファイル解析数/日	無制限	7,000 ファイル/日 (単一構成) 120,000+ ファイル/日 (クラスタ構成)
シグネチャ更新間隔	5 分間隔	5 分間隔
接続可能な NGFW の台数	無制限	100 台 (単一構成)
AutoFocus インテグレーション	○	×
手動ファイルアップロード	○	○

WildFire 設定イメージ



設定イメージ (WildFire サブスクリプションライセンスの確認)

- WildFire の機能をフルで利用する場合、サブスクリプションライセンスの購入、および機器でのアクティベートが必要

Web UI の Device > ライセンス

The screenshot shows the Palo Alto Networks Web UI interface. The left sidebar contains navigation options such as 'セットアップ', '高可用性', '設定監査', 'パスワード プロファイル', '管理者', '管理者ロール', '認証プロファイル', '認証シークエンス', 'ユーザー ID', 'VM 情報ソース', '証明書の管理', '応答ページ', 'ログ設定', 'サーバー プロファイル', 'ローカル ユーザー データベース', 'ユーザー', 'ユーザー グループ', 'スケジュール設定されたログのエクスポート', 'ソフトウェア', 'GlobalProtect クライアント', 'ダイナミック更新', 'ライセンス', 'サポート', and 'マスター キーおよび診断'.

The main content area is titled 'Device' and shows the following license information:

- PA-VM**
 - 発行日: December 11, 2018
 - 有効期限: Never
 - 内容: Standard VM-50
- DNS Security**
 - 発行日: February 15, 2019
 - 有効期限: December 30, 2020
 - 内容: Palo Alto Networks DNS Security License
- PAN-DB URL Filtering**
 - 発行日: December 11, 2018
 - 有効期限: November 29, 2021
 - 内容: Palo Alto Networks URL Filtering License
 - アクティブ: はい
 - ダウンロードの状態: 今すぐダウンロード
- 脅威防御**
 - 発行日: December 11, 2018
 - 有効期限: December 30, 2020
 - 内容: Threat Prevention
- ライセンス管理**
 - ライセンス: サーバーからライセンス キーを取得
 - 認証コードを使用した機能のアクティベーション
 - ライセンス キーの手動アップロード
 - VM の非アクティブ化
 - VM キャパシティのアップグレード
- AutoFocus Device License**
 - 発行日: January 30, 2019
 - 有効期限: February 11, 2026
 - 内容: AutoFocus Device License
- GlobalProtect ゲートウェイ**
 - 発行日: December 11, 2018
 - 有効期限: December 30, 2020
 - 内容: GlobalProtect Gateway License
- 標準**
 - 発行日: December 11, 2018
 - 有効期限: December 30, 2020
 - 内容: 10 x 5 phone support; repair...
- WildFire License (Callout Box)**
 - 発行日: December 11, 2018
 - 有効期限: December 30, 2020
 - 内容: WildFire signature feed, integrated WildFire logs, WildFire API
- WildFire License (Bottom Panel)**
 - 発行日: December 11, 2018
 - 有効期限: December 30, 2020
 - 内容: WildFire signature feed, integrated WildFire logs, WildFire API

設定イメージ (WildFire 一般設定)

- 利用する WildFire リージョン (または WF-500 アプライアンス) の指定や送信されるファイルのサイズの上限、ログ出力の実施有無などを設定

Web UI の Device > セットアップ > WildFire > 一般設定

ファイル サイズ制限	ファイル タイプ	サイズ制限
	pe (MB)	10 (デフォルト)
	apk (MB)	10 (デフォルト)
	pdf (KB)	500 (デフォルト)
	ms-office (KB)	500 (デフォルト)
	jar (MB)	1 (デフォルト)
	flash (MB)	5 (デフォルト)
	MacOSX (MB)	1 (デフォルト)
	archive (MB)	10 (デフォルト)
	linux (MB)	2 (デフォルト)
	script (KB)	20 (デフォルト)

WildFire パブリッククラウド/プライベートクラウド URL:
接続先の WildFire を指定

プライベートクラウドでプロキシ設定を使用:
プロキシ経由で WildFire アプライアンスと接続する場合にチェック

ファイルサイズ制限:
WildFire に送信されるファイルサイズの上限を設定

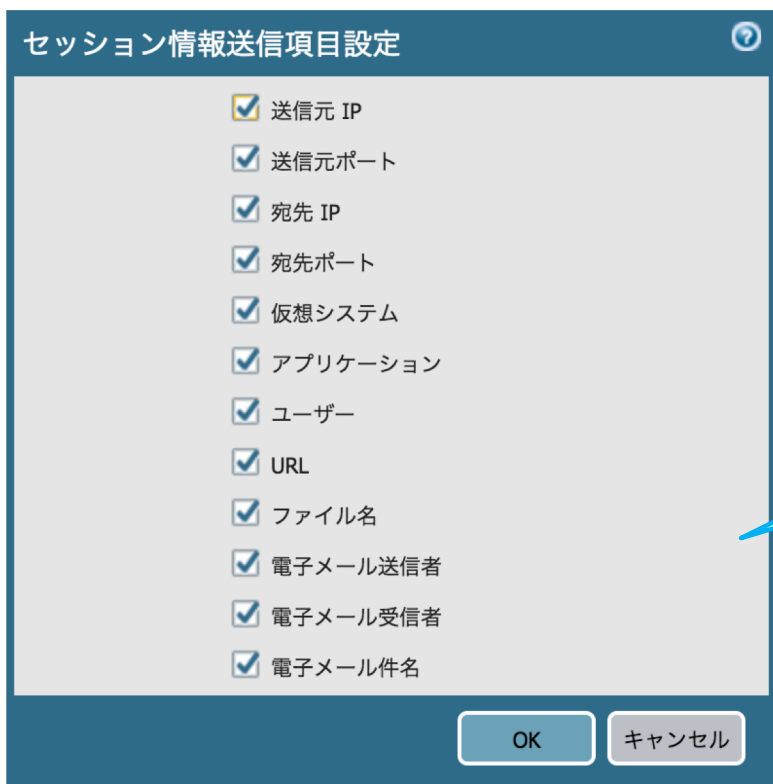
安全なファイルのレポート:
安全 (Benign) と判定されたファイルの転送をログを記録
* 電子メールリンクは対象外

レポートのグレイウェアファイル:
グレイウェア (Grayware) と判定されたファイルの転送をログに記録

設定イメージ (WildFire セッション情報送信項目設定)

- ファイル分析の際、WildFire に対して送信するネットワークのセッション情報を指定

Web UI の Device > セットアップ > WildFire > セッション情報送信項目設定



The screenshot shows a dialog box titled "セッション情報送信項目設定" (Session Information Transmission Item Settings). It contains a list of 14 items, each with a checked checkbox:

- 送信元 IP
- 送信元ポート
- 宛先 IP
- 宛先ポート
- 仮想システム
- アプリケーション
- ユーザー
- URL
- ファイル名
- 電子メール送信者
- 電子メール受信者
- 電子メール件名

At the bottom of the dialog are two buttons: "OK" and "キャンセル" (Cancel).

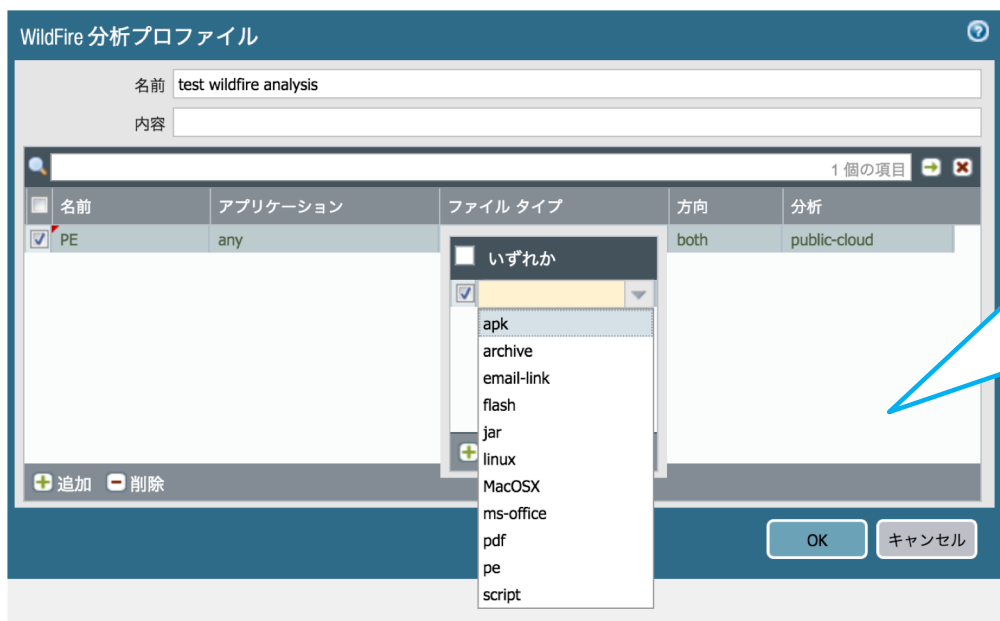
サンプルに関連するネットワークセッションの情報を送信することにより、疑わしいネットワークイベントのコンテキストをより詳細に把握出来る場合があります

例: マルウェアへの感染が疑われるホストやクライアント端末、マルウェアの送信に利用されたアプリケーションの情報など

設定イメージ (WildFire 分析プロファイル)

- WildFire 分析時に行う処理 (対象となるアプリケーション・ファイルタイプ、通信の方向、パブリック/プライベートの指定など) のセットをプロファイルとして作成

Web UI の Objects > セキュリティプロファイル > WildFire 分析



アプリケーション:
アプリケーションを元に検査対象を指定

ファイルタイプ:
ファイルタイプを元に検査対象を指定

方向:
通信の方向 (アップロード or/and ダウンロード) の指定

分析:
分析環境 (パブリッククラウド or プライベートクラウド) を指定

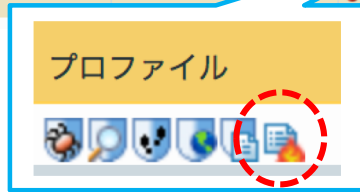
設定イメージ (セキュリティルールにプロファイルを適用)

- 作成した WildFire 分析プロファイルをセキュリティルールに適用
* ルールで許可されたトラフィックに対し WildFire 分析が実施

Web UI の Policies > セキュリティ

名前	タグ	タイプ	送信元			宛先		ルールの使用状況		アプリケーション	サービス	アクション	プロファイル
			ゾーン	アドレス	ユーザー	ゾーン	アドレス	ヒット数					
1	phishing inspection	none	universal	trust	any	any	server	any	0	any	any	許可	
2	allow-iiis-inbound	none	universal	untrust	any	any	trust	msft-iiis-victim...	647	icmp ping ssl web-browsing	application-d...	許可	
3	allow DNS traffic	none	universal	trust	any	any	untrust	any	1881	dns	application-d...	許可	
4	allow NTP traffic	none	universal	trust	any	any	untrust	any	0	ntp	application-d...	許可	none
5	allow web traffic	none	universal	trust	any	any	untrust	any	2732	any	service-http service-https	許可	
6	allow all	none	universal	any	any	any	any	any	55117	any	any	許可	
7	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	0	any	any	許可	none
8	interzone-default	none	interzone	any	any	any	any	any	0	any	any	拒否	

作成した WildFire プロファイルをセキュリティルールに適用



設定イメージ (ダイナミック更新間隔設定)

- ダイナミック更新のチェック間隔、およびアクション (チェックのみ、ダウンロードのみ、ダウンロードおよびインストール) を設定

Web UI の Device > ダイナミック更新 > WildFire

The screenshot displays the Palo Alto Networks Web UI configuration page for WildFire updates. The main table lists various update packages with columns for version, filename, function, type, size, release date, download status, and action. The WildFire section is expanded, showing a table of updates with columns for ID, filename, version, type, size, release date, and action. A modal window titled "WildFireの更新スケジュール" (WildFire Update Schedule) is open, allowing configuration of the update frequency and action. The frequency is set to "毎分" (Every minute) and the action is "download-and-install". A callout box points to the "今すぐチェック" (Check now) button at the bottom of the WildFire section, with the text "手動で今すぐ確認も可能" (Manual check now is also possible).

バージョン	ファイル名	機能	タイプ	サイズ	リリース日	ダウンロード済み	現在インストール済み	アクション	ドキュメント
▼ アンチウイルス 最終チェック: 2019/03/20 11:00:34 JST スケジュール: Every hour (Download and Install)									
2918-3428	panup-all-antivirus-2918-3428		Full	86 MB	2019/03/15 20:04:40 JST				
2919-3429	panup-all-antivirus-2919-3429		Full	86 MB	2019/03/16 20:04:35 JST				
2920-3430	panup-all-antivirus-2920-3430		Full	87 MB	2019/03/17 20:03:52 JST				
2921-3431	panup-all-antivirus-2921-3431		Full	87 MB	2019/03/18 20:01:13 JST	✓ 以前			
2922-3432	panup-all-antivirus-2922-3432		Full	87 MB	2019/03/19 20:01:47 JST	✓			
▶ アプリケーションおよび脅威 最終チェック: 2019/03/12 18:52:38 JST スケジュール: Every hour at 0 minutes past the hour (None)									
▶ GlobalProtect クライアントレス VPN 最終チェック: 2019/03/12 18:52:41 JST スケジュール: None									
▶ GlobalProtect データ ファイル スケジュール: None									
▼ WildFire 最終チェック: 2019/03/20 11:49:03 JST スケジュール: Every minute (Download and Install)									
332745-335422	panup2-all-wildfire-332745-335422	PAN OS 7.1 And Later	Full	8 MB	2019/03/20 11:30:14 JST	✓ 以前		戻す	リリース ノート
332746-335423	panup2-all-wildfire-332746-335423	PAN OS 7.1 And Later	Full	8 MB	2019/03/20 11:35:15 JST	✓	✓		リリース ノート [X]
332748-335425	panup2-all-wildfire-332748-335425	PAN OS 7.1 And Later	Full	8 MB	2019/03/20 11:45:18 JST			ダウンロード	リリース ノート

設定イメージ (SSL 復号ポリシー適用時の追加設定)

- PA ファイアウォールはデフォルトで復号されたコンテンツを外部のサービス (ここでは WildFire) に転送しない設定になっているため、下記の追加設定が必要

Web UI の Device > セットアップ > コンテンツ ID > コンテンツ ID 設定

The screenshot shows the Palo Alto Networks Web UI interface. The main navigation bar includes 'Dashboard', 'ACC', 'Monitor', 'Policies', 'Objects', 'Network', and 'Device'. The 'Device' tab is active, and the 'Content ID' sub-tab is selected. The 'Content ID Settings' page is displayed, with a modal window open for editing. The modal window, titled 'コンテンツ ID 設定', contains the following settings:

- 復号化されたコンテンツの転送を許可 (This checkbox is highlighted with a red dashed circle in the image.)
- 拡張パケット キャプチャ長 (パケット数) 5
- TCP App-ID検査キューを超過したセグメントを転送
- TCPコンテンツ検査キューを超過したセグメントを転送
- UDPコンテンツ検査キューを超過したデータグラムを転送
- HTTPの部分的な応答を許可

Buttons for 'OK' and 'キャンセル' are visible at the bottom of the modal. The background page shows other settings like 'URL フィルタリング' and 'Forwarded-For ヘッダ'.

WildFire ログイメージ



WildFire ログ (Web UI)

Monitor > ログ > WildFire への送信

虫眼鏡アイコンをクリックすると詳細表示 (次スライド)

受信日時	ファイル名	送信元アドレス	宛先アドレス	宛先ポート	アプリケーション	ファイル ダイジェスト	ルール	判定	アクション	重大度
03/20 10:15:33	tjIQnoCZTYiYOMEFeC.EXe	66.1.1.10	10.154.10.9	25	smtp	ea82b001464d19758c398...	Watch Public DNS and SMTP	malicious	allow	high
03/20 10:15:33	uRUvWhgWNeIZExdxgeD...	66.1.1.10	10.154.10.100	25	smtp	e73635bb05234d810999fb...	Watch Public DNS and SMTP	malicious	allow	high
03/20 10:15:33	XqfYQshrQ.PdF	66.1.1.8	10.154.10.87	143	imap	dc5244fc949e549b9675e6...	Unexpected Traffic	malicious	block	informational
03/20 10:15:33	GkCbw.eXE	66.1.1.5	10.154.10.184	25	smtp	0c3f6774c3a71d2b039571...	Watch Public DNS and SMTP	malicious	allow	high
03/20 10:15:33	FLOhvSj.YaT	66.1.1.10	10.154.10.211	25	smtp	253ae81e2088f90e7b7f91...	Watch Public DNS and SMTP	malicious	block	informational
03/20 10:15:33	ZYrjFhjeNrqdI.exe	66.1.1.3	10.154.10.208	25	smtp	0341d65a6a4d50bdfd20d2...	Watch Public DNS and SMTP	malicious	allow	high
03/20 10:15:33	MunWQR9G.PdF	66.1.1.9	10.154.10.68	110	pop3	32f85e865b018825b44739...	Unexpected Traffic	malicious	block	informational
03/20 10:15:33	fD8aSkL2VGeekD.pDf	66.1.1.10	10.154.10.94	25	smtp	80526f1335180ff7c710f43...	Watch Public DNS and SMTP	malicious	block	informational
03/20 10:15:33	6ZKP.pDf	66.1.1.10	10.154.10.135	143	imap	cffc35190a628442e6e7db...	Unexpected Traffic	malicious	block	informational
03/20 09:57:33	IxKwNjNXuYTC.EXe	66.1.1.9	10.154.10.252	25	smtp	db93627451493edafc5503...	Watch Public DNS and SMTP	malicious	allow	high
03/20 09:57:33	UcHcoWAKIHaPicCKpmqv...	66.1.1.6	10.154.10.147	25	smtp	f4aed1b24065a7c15138a1...	Watch Public DNS and SMTP	malicious	allow	high
03/20 09:55:43	RXRihhJqLdQxBAdOMmB...	66.1.1.10	10.154.10.42	25	smtp	a94fc1de2c6c78d5aea947...	Watch Public DNS and SMTP	malicious	allow	high
03/20 09:55:40	ZYrjFhjeNrqdI.exe	66.1.1.3	10.154.10.208	25	smtp	0341d65a6a4d50bdfd20d2...	Watch Public DNS	malicious	allow	high

WildFire ログ (Web UI, Cont.)

Monitor > ログ > WildFire への送信から各エントリの詳細表示

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 248686 アクション allow アプリケーション smtp ルール Watch Public DNS and SMTP 判定 malicious 仮想システム デバイスのシリアル番号 007000016487 IP プロトコル tcp ログ アクション ToUS1RAMA 生成日時 2019/03/20 10:15:33 受信日時 2019/03/20 10:15:33 トンネル タイプ N/A	送信元ユーザー 送信元 66.1.1.10 ポート 11308 ゾーン L3-TAP インターフェイス ethernet1/2	宛先ユーザー 宛先 10.154.10.9 ポート 25 ゾーン L3-TAP インターフェイス ethernet1/2
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 VV04wQJExRdKn@BARILu... 受信者のアドレス likTKRsFf@axbuRgXlcIvbGsC...	脅威/コンテンツタイプ ID 14523412983 重大度 high 繰り返し回数 1 ファイルタイプ pe ファイル名 tjiQnoCZTyYOMEFeC.Exe URL	フラグ キャプティブポータル <input type="checkbox"/> プロキシトラッキング <input type="checkbox"/> 復号化 <input type="checkbox"/> パケットキャプチャ <input type="checkbox"/> クライアントからサーバー <input checked="" type="checkbox"/> サーバーからクライアント <input type="checkbox"/> トンネル検査 <input type="checkbox"/>

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
	2019/03/20 10:15:04	end	smtp	allow	Watch Public DNS and SMTP	200077		any			
	2019/03/20 10:15:33	wildfire	smtp	allow	Watch Public DNS and SMTP		high		malicious		tjiQnoCZ...
	2019/03/20 10:15:03	file	smtp	alert	Watch Public DNS and SMTP		low	any			tjiQnoCZ...
	2019/03/20 10:15:03	file	smtp	alert	Watch Public DNS and SMTP		low	any			tjiQnoCZ...
	2019/03/20 10:15:03	wildfire-virus	smtp	alert	Watch Public DNS and SMTP		medium	any			tjiQnoCZ...
	2019/03/20 10:15:03	virus	smtp	alert	Watch Public DNS and SMTP		medium	any			tjiQnoCZ...

閉じる

詳細ログビュー

ログ情報 WildFire 分析レポート

WildFire Analysis Summary

Download PDF

File Information

File Type	PE
File Signer	
SHA-256	ea82b001464d19758c3989317a8c2a4815227
MD5	ef6f5b4e3f467cececcacc7840379760
File Size	138752 bytes
Verdict	malware

分析レポートは PDF としてダウンロード可能

Coverage Status

The table below lists all coverage related to this malware sample. For endpoint antivirus coverage information for this sample, visit [Virus Total](#).

Coverage type	Signature ID	Detail	Date Released	Latest Content
virus	2022912	Porn-Dialer/Win32.dialer.kccb	2011-11-01T02:03:34	1674
wildfire	3054166	Porn-Dialer/Win32.dialer.kccb	2012-03-21T22:30:59	108349

Page 1 of 1

Dynamic Analysis

Virtual Machine 1

This virtual machine is configured with the following software: Windows XP SP2.

Behavior Summary

閉じる

* 上のスクリーンショットはレポートのごく一部です (他のパートはスクロールダウンにより確認可能)

WildFire ログ (WildFire へのファイルアップロード送信履歴, CLI)

debug wildfire upload-log show channel public コマンド出力結果

```
knarasaki — ssh admin@192.168.55.10 — 80x31
[admin@pan-panos-vm50> debug wildfire upload-log show channel public

Upload Log disk log rotation size: 2.000 MB.
Public Cloud upload logs:

log: 0, filename: wildfire-test-pe-file.exe
processed 1830 seconds ago, action: upload success
vsys_id: 1, session_id: 5828, transaction_id: 3
file_len: 55296, flag: 0x801c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.45.64/50588 to 52.193.2.75/80
SHA256: f7a2b1e3d3118b90c212ecb17971f0008394b41e93bb46f90a40b1b1df93b735

log: 1, filename: wildfire-test-pe-file.exe
processed 1938 seconds ago, action: skipped - remote verdict pending dup
vsys_id: 1, session_id: 5795, transaction_id: 2
file_len: 55296, flag: 0x201c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.45.64/50578 to 54.250.96.197/80
SHA256: 8ec96f2cf6e01449d11553aa646fcbad566206afb18efb5e23160753146b8fcc

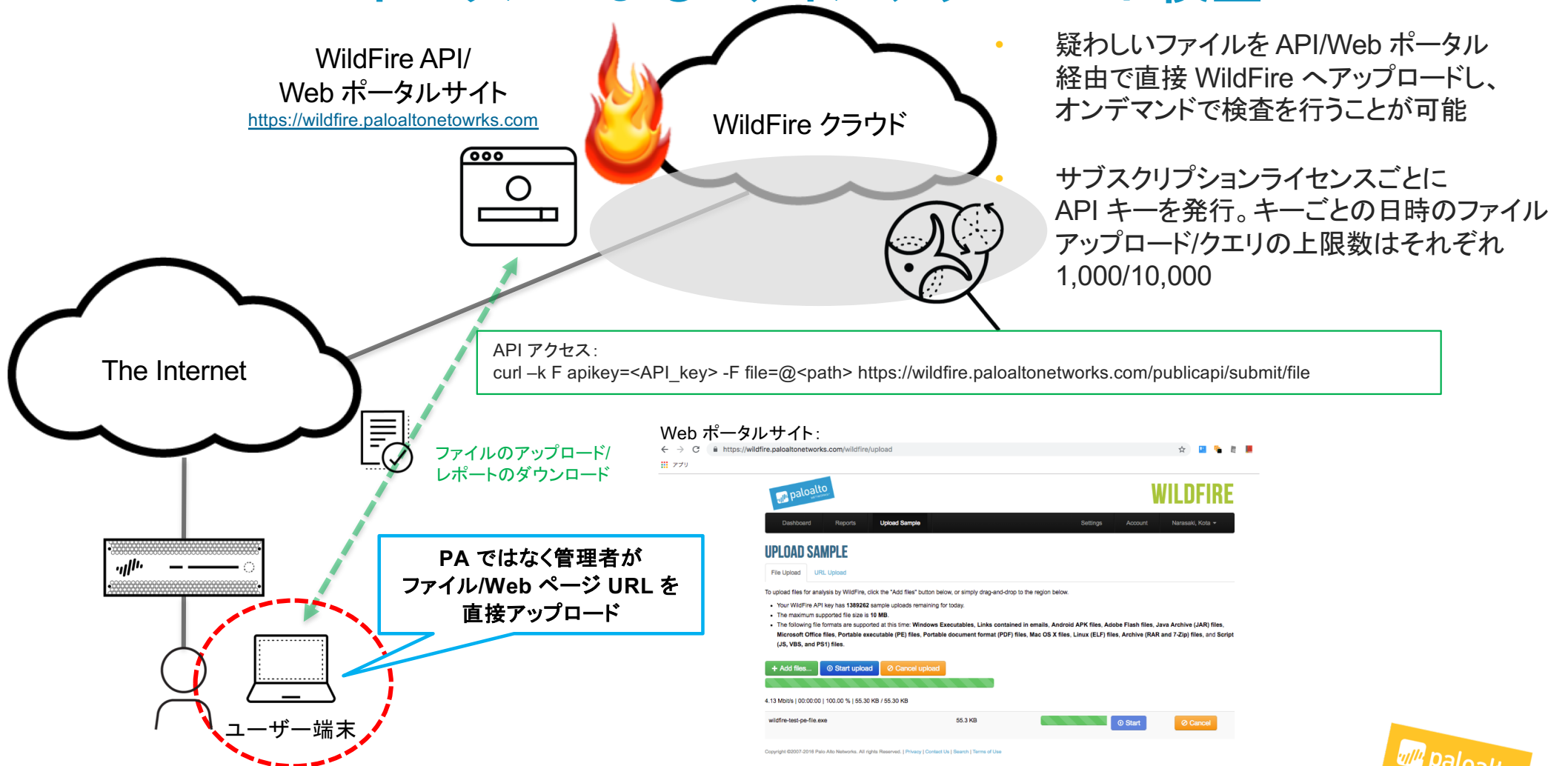
log: 2, filename: wildfire-test-pe-file.exe
processed 2108 seconds ago, action: skipped - remote verdict pending dup
vsys_id: 1, session_id: 5755, transaction_id: 1
file_len: 55296, flag: 0x201c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.45.64/50570 to 54.250.96.197/80
SHA256: 9352522b1b8a703dc5e9f6a0a59150b0ac3a90f2c88e87262d3e2008932e54fd

admin@pan-panos-vm50>
```

WildFire API/ポータルによる ファイルアップロード検査



WildFire API/ポータルによるファイルアップロード検査



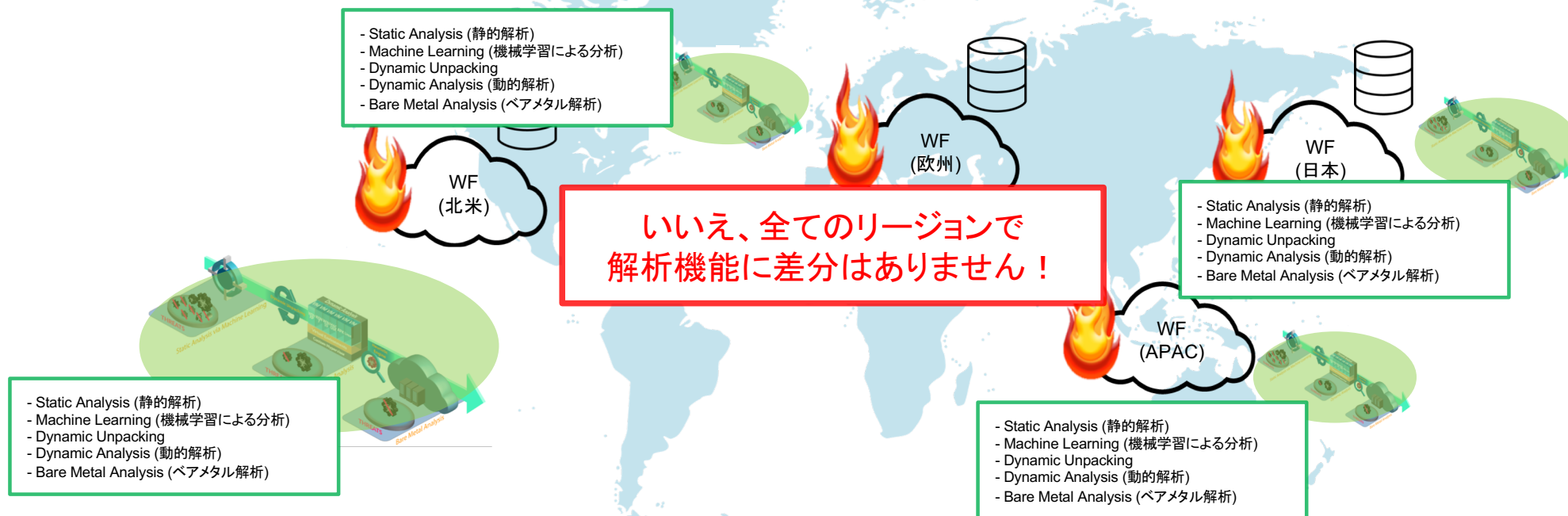
WildFire Japan アップデート

こんな誤解していませんか？ 編



WildFire にまつわるよくある誤解 (1)

- 日本リージョンの WildFire は北米のものと比較し分析機能が少なくバージョンアップも遅いので、マルウェアの検出精度が落ちる。そのため、可能であれば北米の WildFire を利用した方が良い

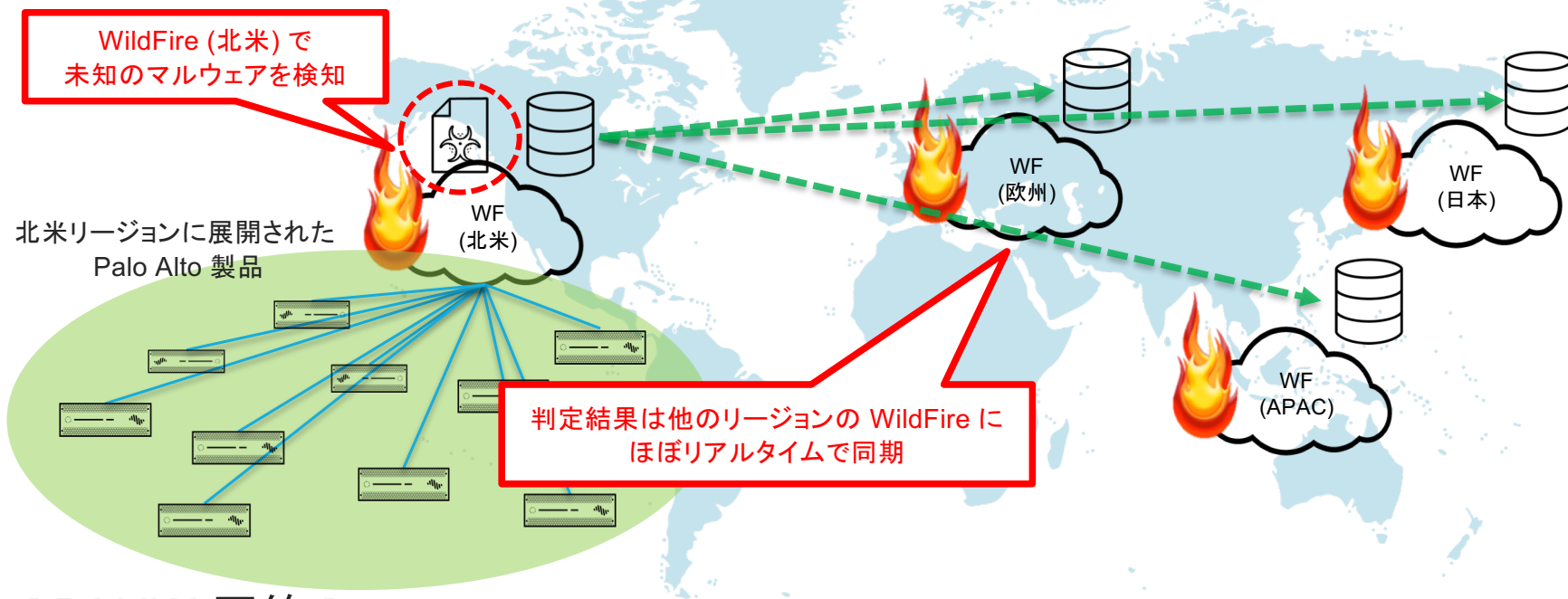


[PANW 回答]

リージョン間の解析機能に差はありません！

WildFire にまつわるよくある誤解 (2)

- データセンター間での情報の同期には時間が掛かるため、他のリージョンで発見された未知のマルウェア情報をすぐに参照出来る訳ではない



[PANW 回答]

ファイルの判定結果 (Verdicts) 情報および生成されたシグネチャは各リージョンのデータセンター間でほぼリアルタイム (数秒程度)* で同期が行われます！

* 目安値、WF の負荷やネットワーク状況に依存して変化

WildFire にまつわるよくある誤解 (3)

- 日本にデータセンターがあるが、情報共有のためマルウェアと判定された検体ファイルが他のリージョンの WildFire クラウドに送られてしまう



[PANW 回答]

元のファイルが WildFire Japan の外部に共有されることはありません！

まとめ

WildFire まとめ

- パロアルトネットワークスがグローバルで展開するクラウド型サンドボックスソリューション
- 未知のマルウェア・標的型攻撃に対し直ちに対応可能な自動防御プロセスを提供
- シグネチャのダイナミック更新のみの利用も可能
(パブリッククラウドへのファイルアップロードなしでも利用可能)
- 第三者リサーチ機関のレポートにおいて、マーケットリーダーのポジションを獲得
- 日本国内にデータセンターを展開、他のリージョンと同一の最新の解析機能を提供
- パブリッククラウド環境の利用が難しいユーザーに向け、オンプレミス環境向けアプライアンス (WF-500) も提供

