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

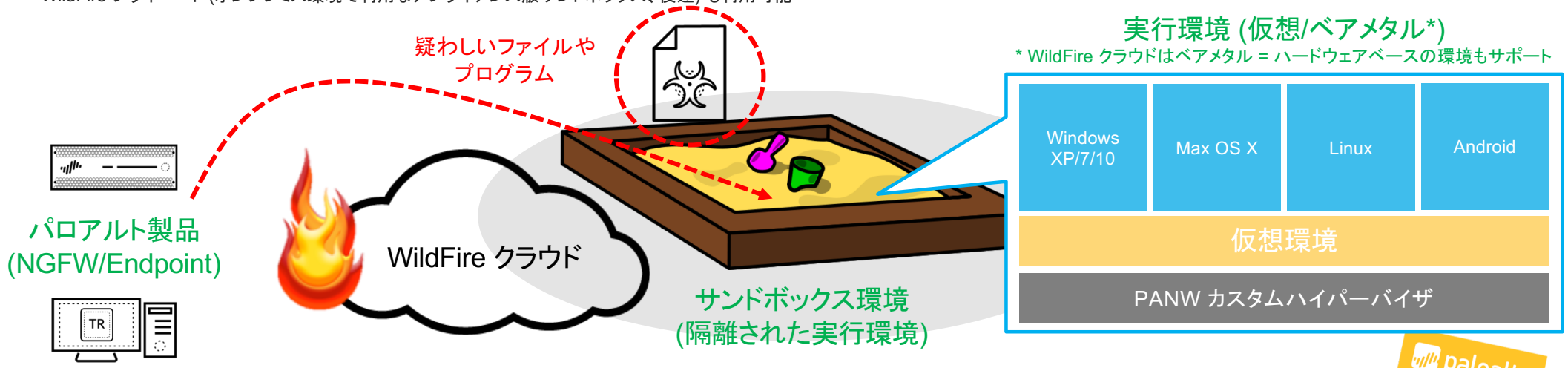
おさらい - サンドボックスとは？

“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”

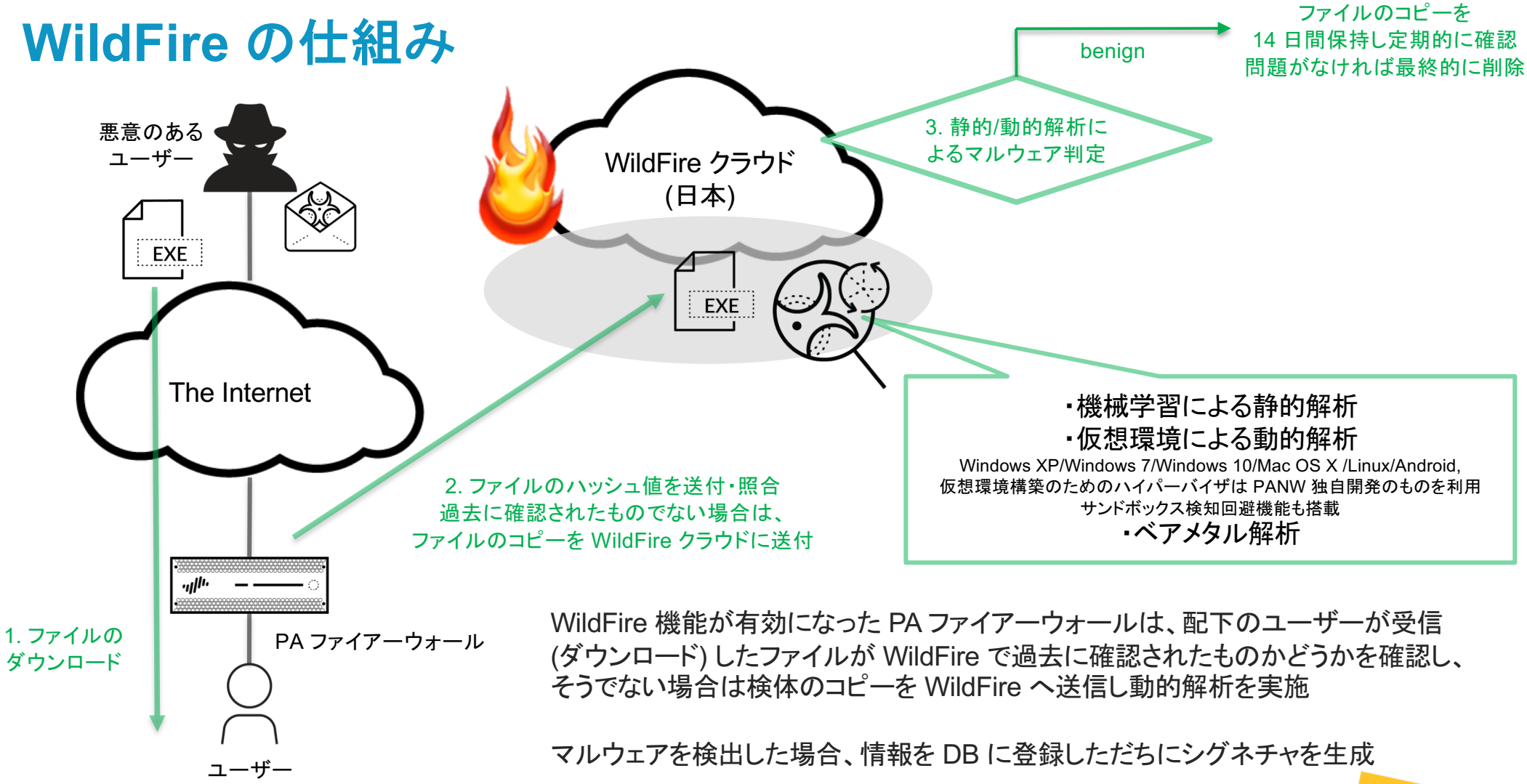
→ 疑わしいファイルやプログラムを実行し分析を行うことが出来る、「攻撃されても問題がない」隔離された仮想の実行環境のこと。未知の攻撃や標的型攻撃への対策として有効

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



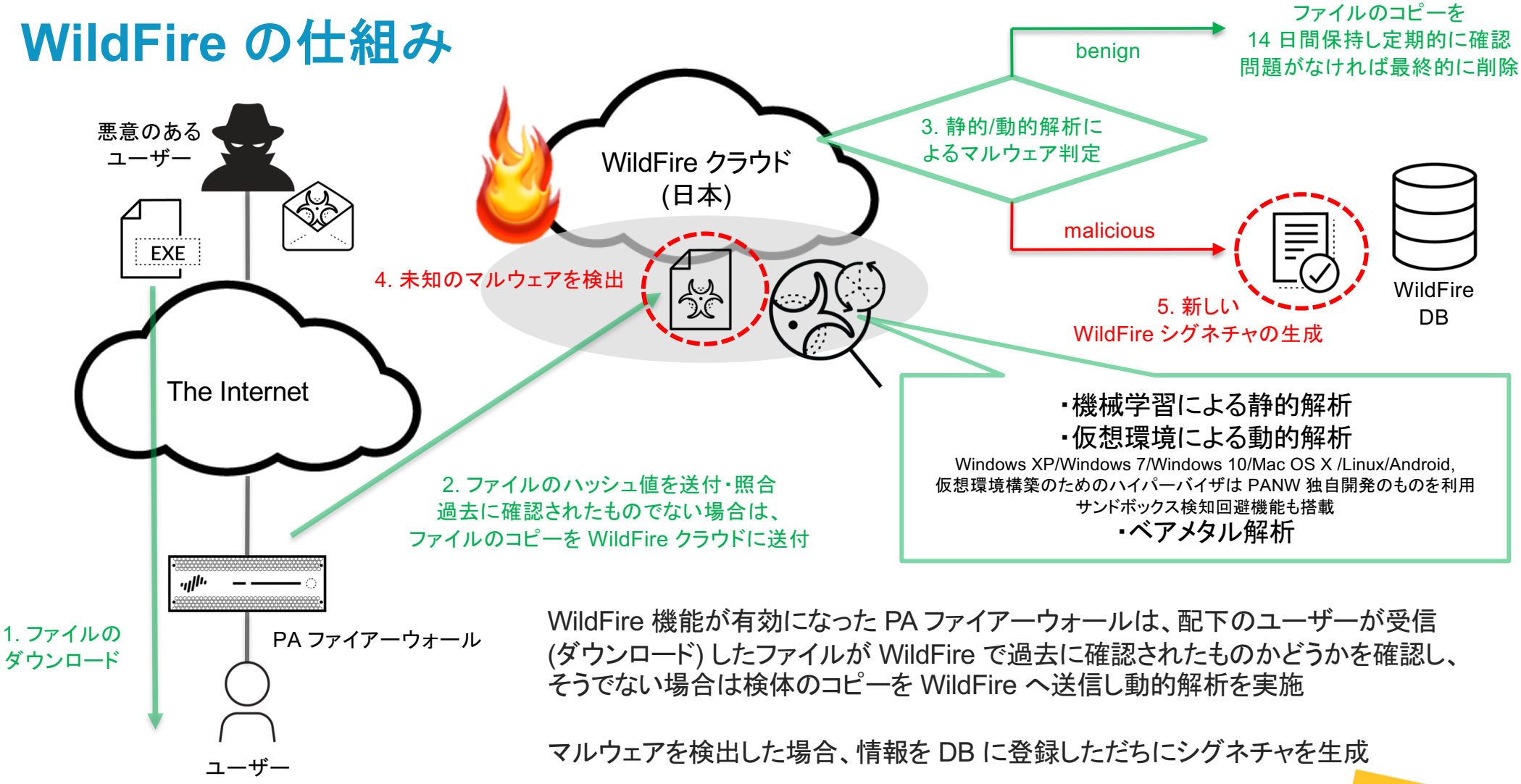
WildFire の仕組み



WildFire 機能が有効になった PA ファイアーウォールは、配下のユーザーが受信(ダウンロード) したファイルが WildFire で過去に確認されたものかどうかを確認し、そうでない場合は検体のコピーを WildFire へ送信し動的解析を実施

マルウェアを検出した場合、情報を DB に登録しただちにシグネチャを生成

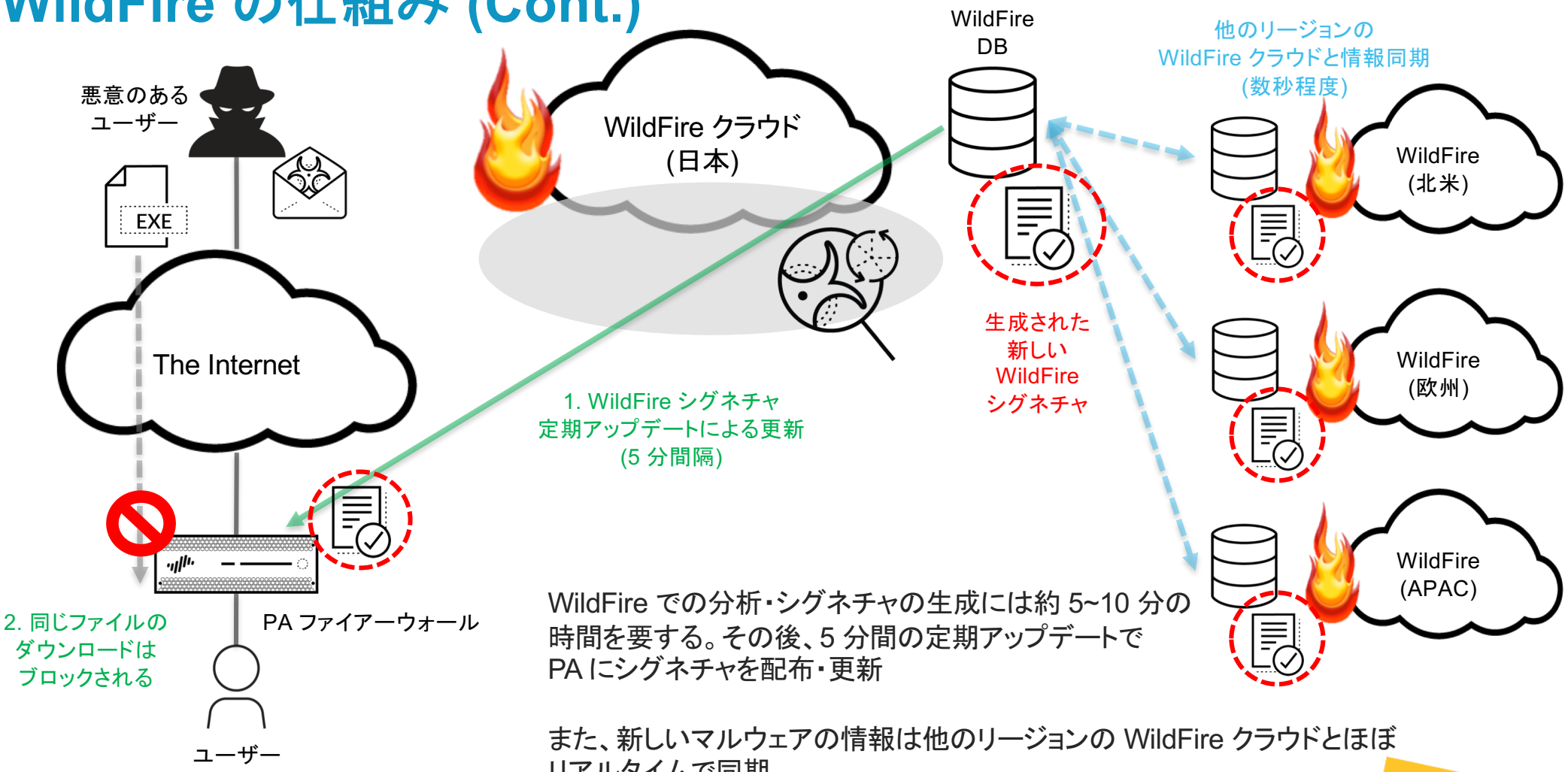
WildFire の仕組み



WildFire 機能が有効になった PA ファイアーウォールは、配下のユーザーが受信(ダウンロード) したファイルが WildFire で過去に確認されたものかどうかを確認し、そうでない場合は検体のコピーを WildFire へ送信し動的解析を実施

マルウェアを検出した場合、情報を DB に登録しただちにシグネチャを生成

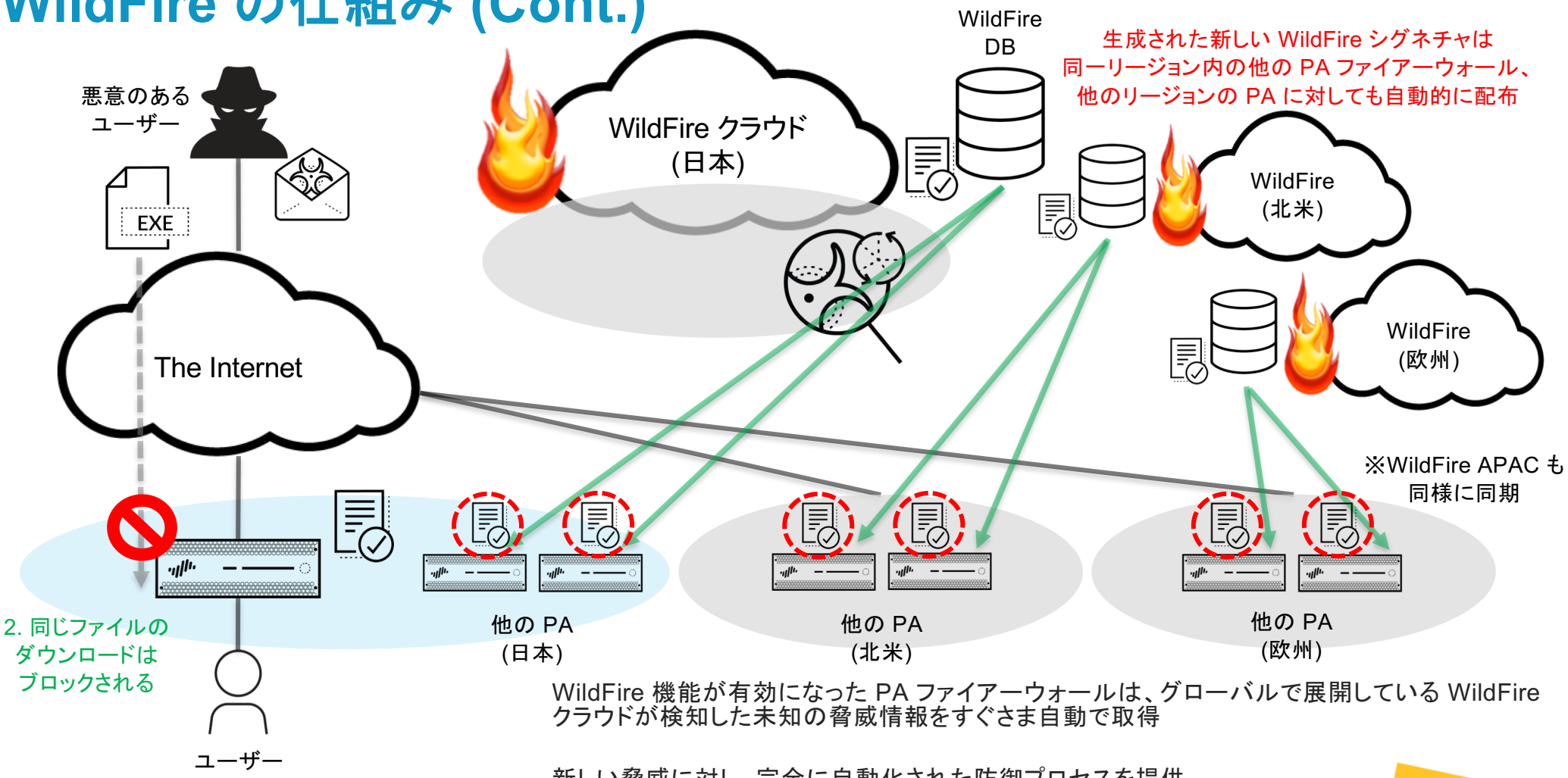
WildFire の仕組み (Cont.)



WildFire での分析・シグネチャの生成には約 5~10 分の時間を要する。その後、5 分間の定期アップデートで PA にシグネチャを配布・更新

また、新しいマルウェアの情報は他のリージョンの WildFire クラウドとほぼリアルタイムで同期

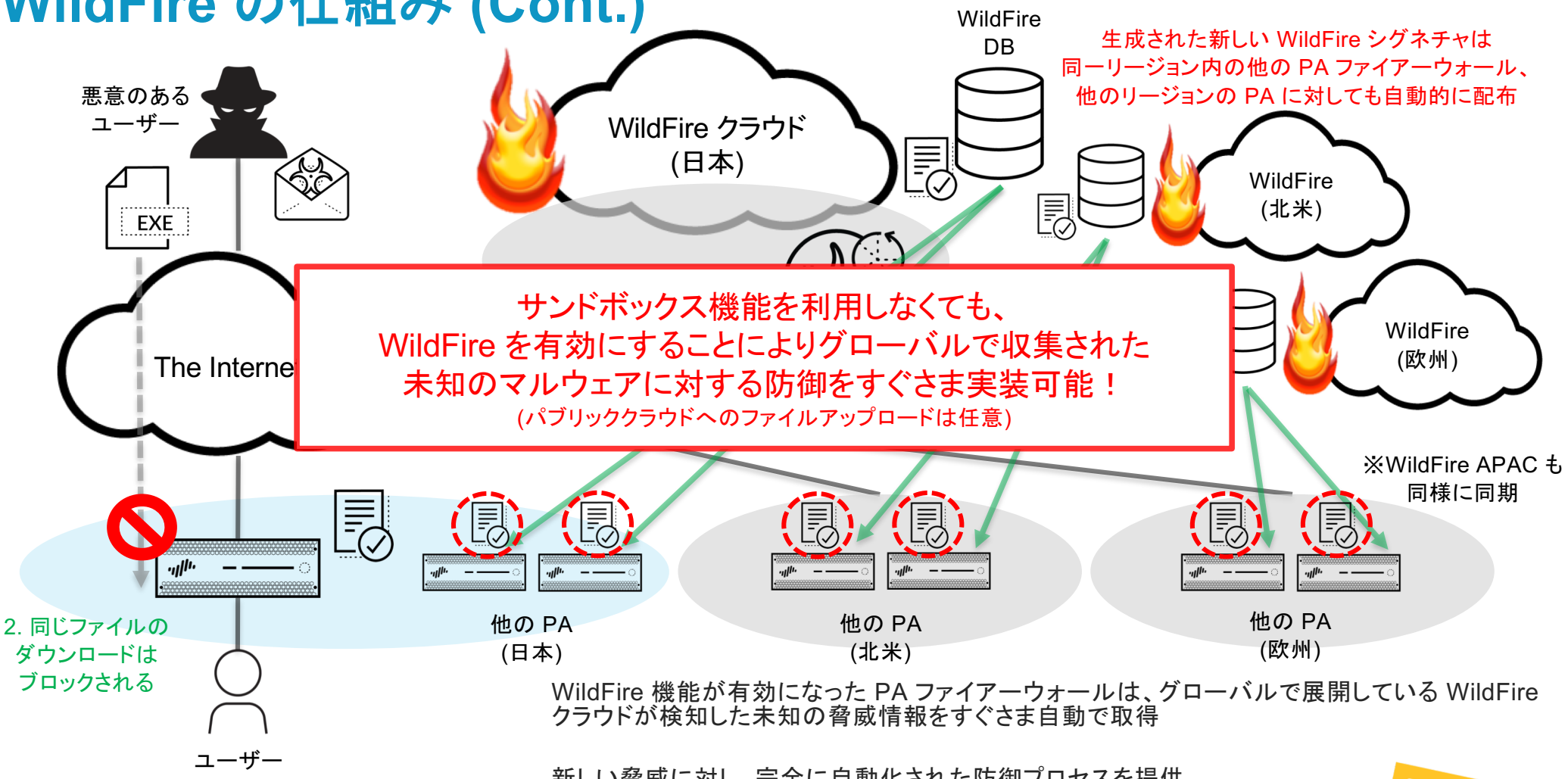
WildFire の仕組み (Cont.)



WildFire 機能が有効になった PA ファイアーウォールは、グローバルで展開している WildFire クラウドが検知した未知の脅威情報をすぐさま自動で取得

新しい脅威に対し、完全に自動化された防御プロセスを提供

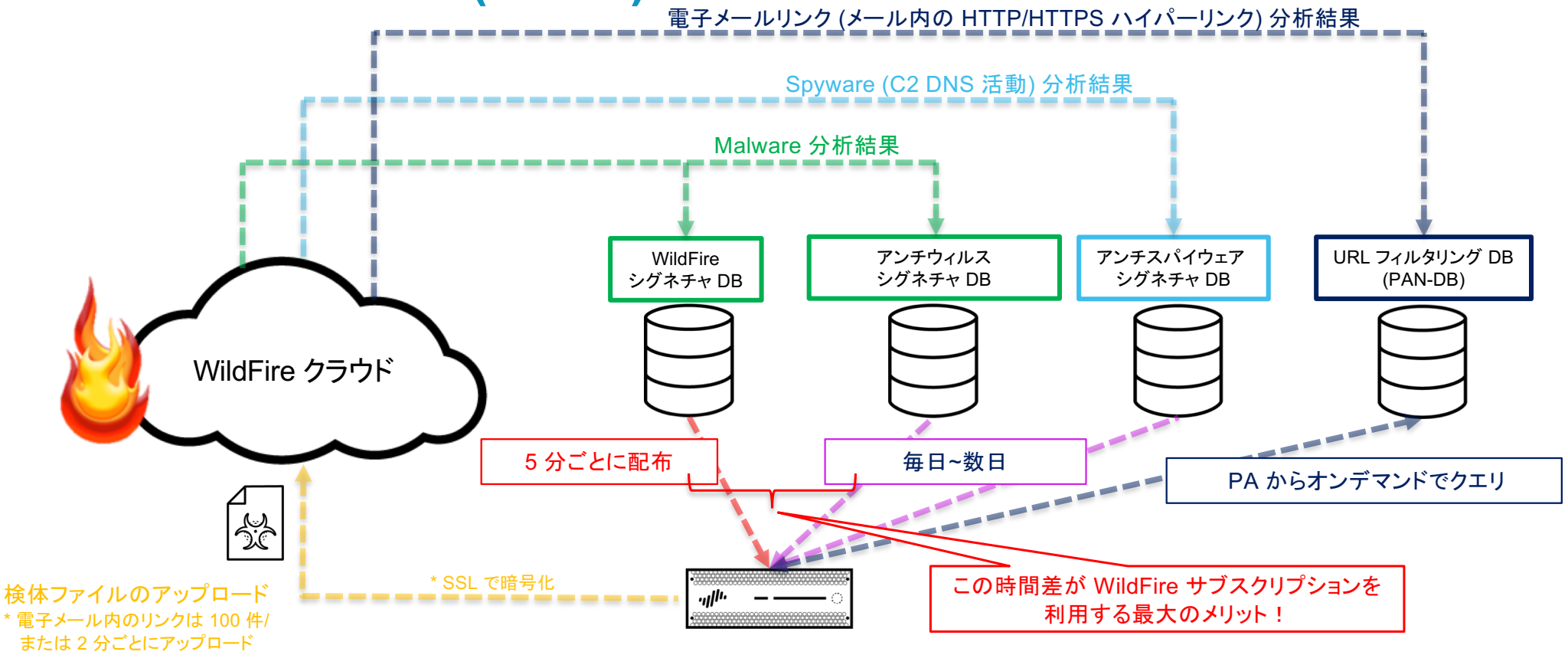
WildFire の仕組み (Cont.)



WildFire 機能が有効になった PA ファイアーウォールは、グローバルで展開している WildFire クラウドが検知した未知の脅威情報をすぐさま自動で取得

新しい脅威に対し、完全に自動化された防御プロセスを提供

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、アンチウィルス/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.)

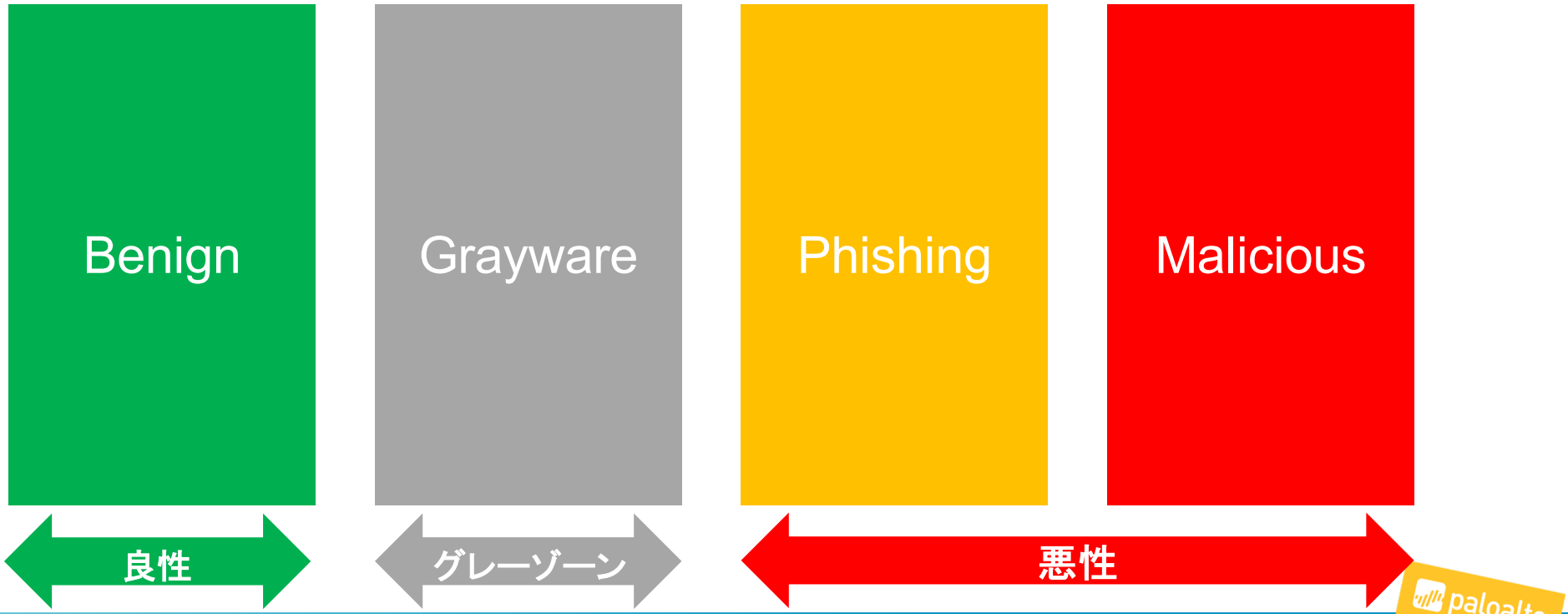
- 電子メールリンク分析
  SMTP/POP3 メール内の HTTP/HTTPS ハイパーリンク先にエクスプロイトやフィッシングなどが仕込まれていないかを分析することが可能。また、リンク先がマルウェアと判断された場合、その結果は URL フィルタリング DB に反映

- 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

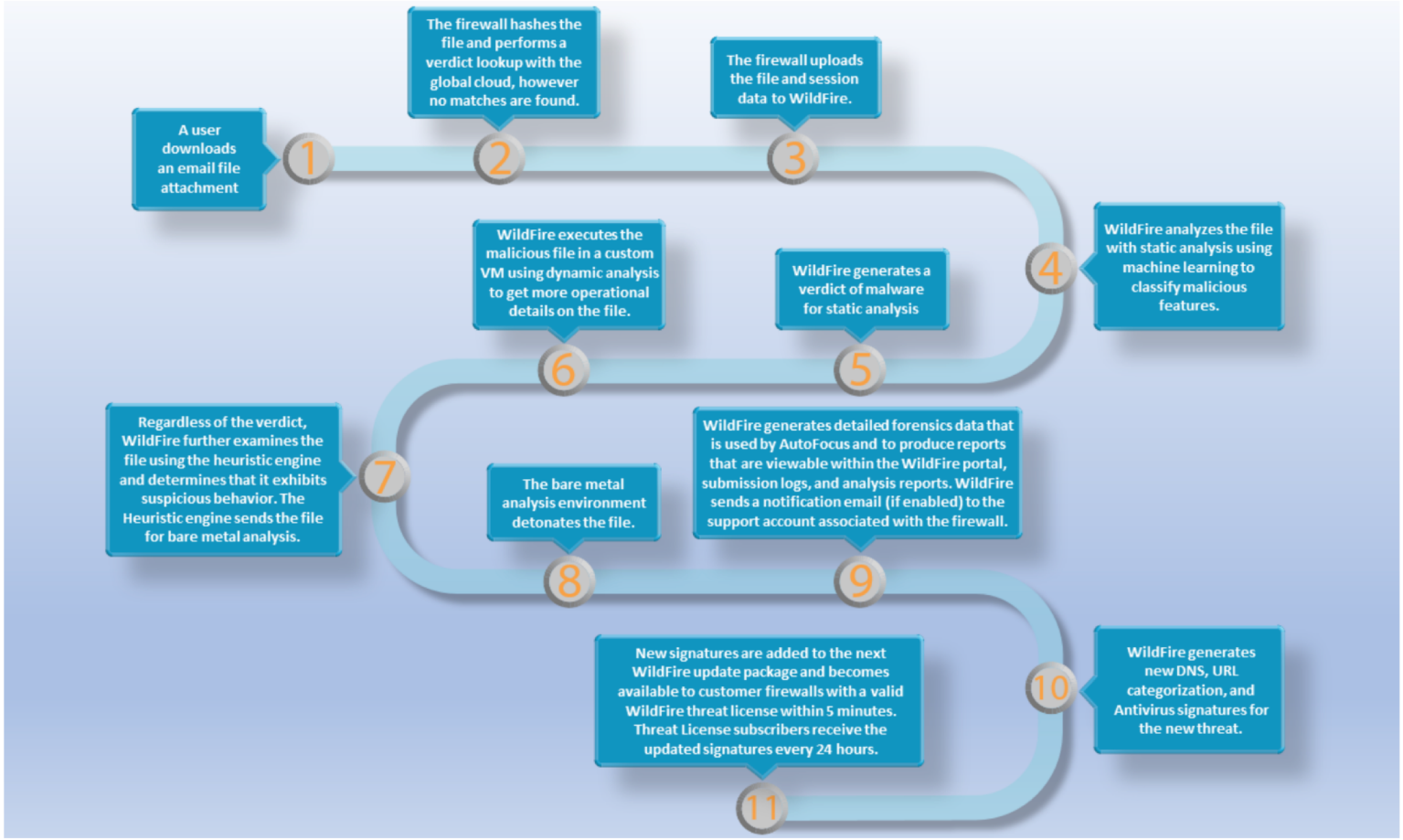
- SSL/TLS 通信の分析について
  HTTPS (Web), SMTPS/POPS メール内のリンクの分析には、SSL/TLS 通信の復号が必要

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

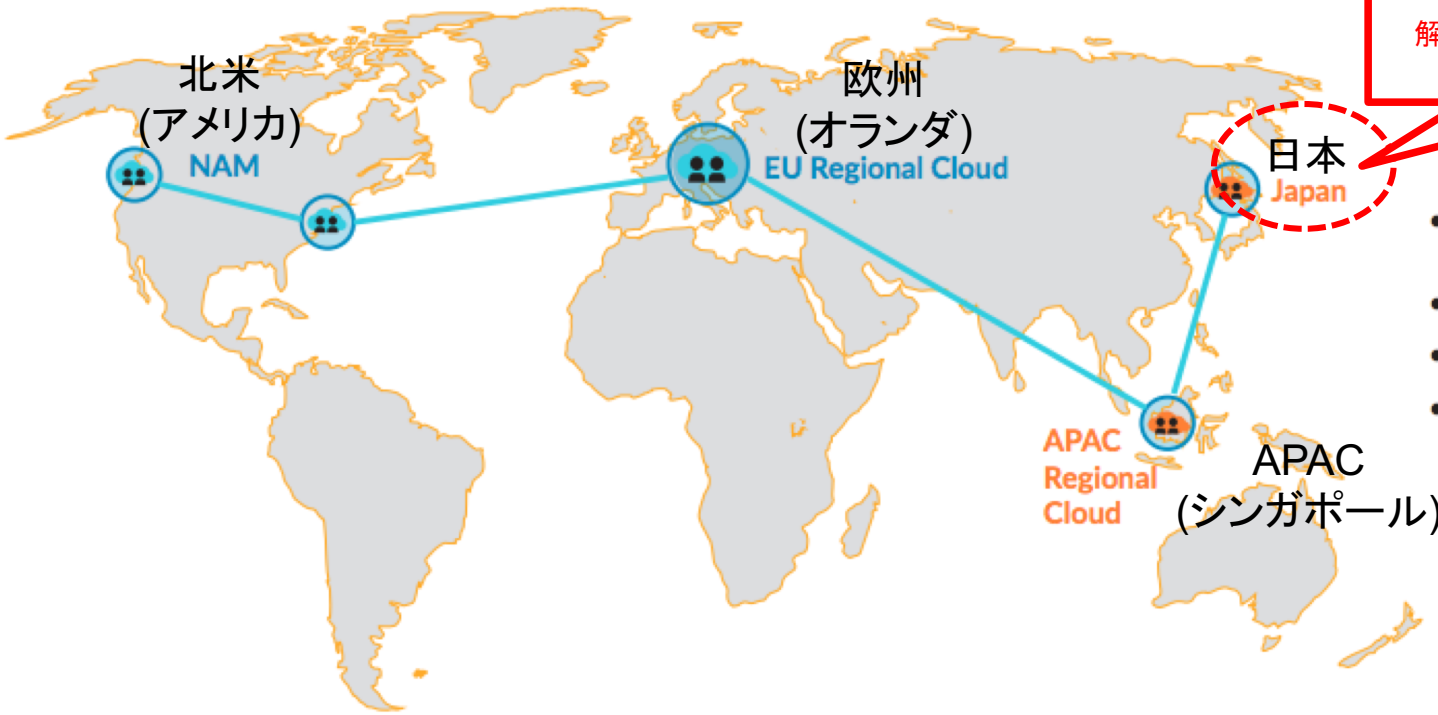


1. ユーザーが電子メールの添付ファイルをダウンロード
2. PA ファイアーウォールはファイルのハッシュ値を取得し、WildFire の判定履歴を確認
3. 履歴がない場合、PA はファイルのコピーとセッション情報を WildFire にアップロード
4. WildFire は機械学習を利用した静的解析で悪意のある特性を分類
5. WildFire は静的解析の判定結果を生成
6. WildFire は仮想環境でファイルを実行・動的解析を実施、ファイルのオペレーション詳細を取得
7. 判定結果に関わらず、WildFire はヒューリスティックエンジンにより疑わしい振る舞いをしないかを確認
8. 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 カテゴライゼーション、およびアンチウィ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



WildFire Japan を利用する場合、
解析は日本国内のデーターセンターで
実施

- SOC 2 Type 2 Compliant
- Regional Data Privacy
- Identical Capabilities
- Distributed Threat Research

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

* SOC 2 Type 2 認定
受託業務のセキュリティ、可用性、整合性、機密性、
プライバシーの観点で内部統制に問題がないことを
第三者機関により評価・保証

 |

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

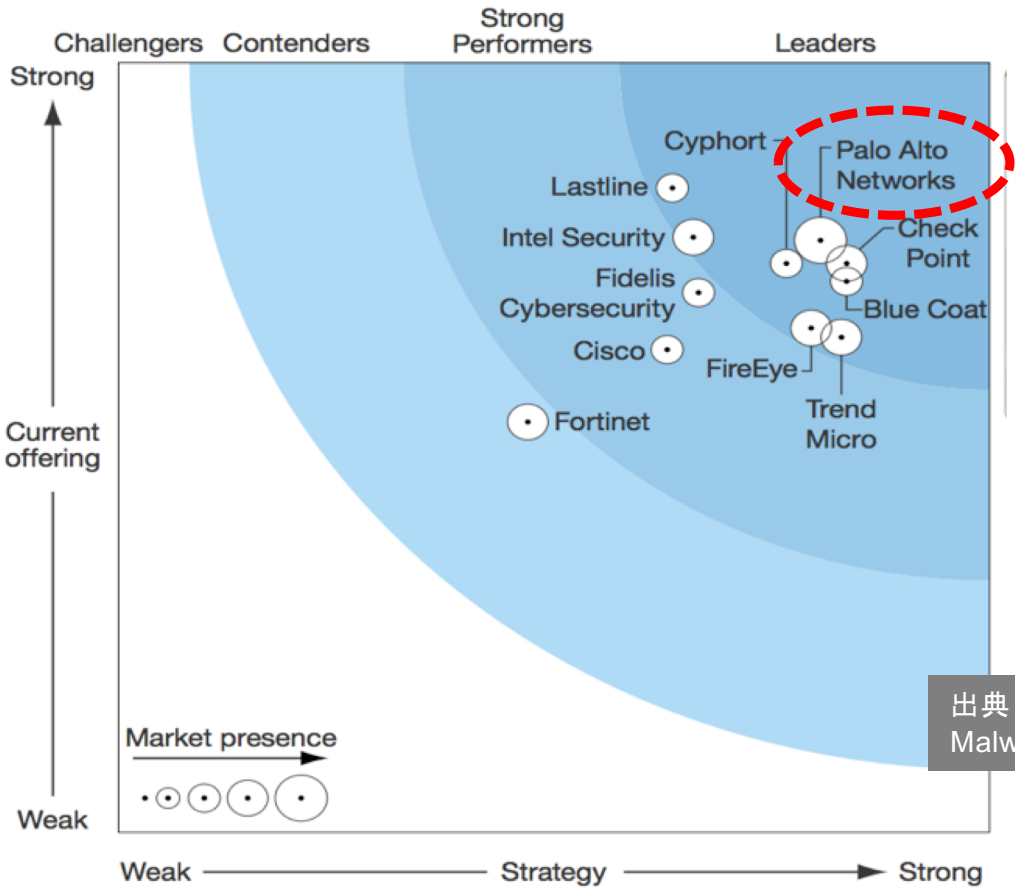
※1 Average monthly values as of January 2016. Source: Palo Alto Networks WildFire and Multi-Scanner

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

 |

サンドボックス市場においてどんな評価を受けてい流のか？

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

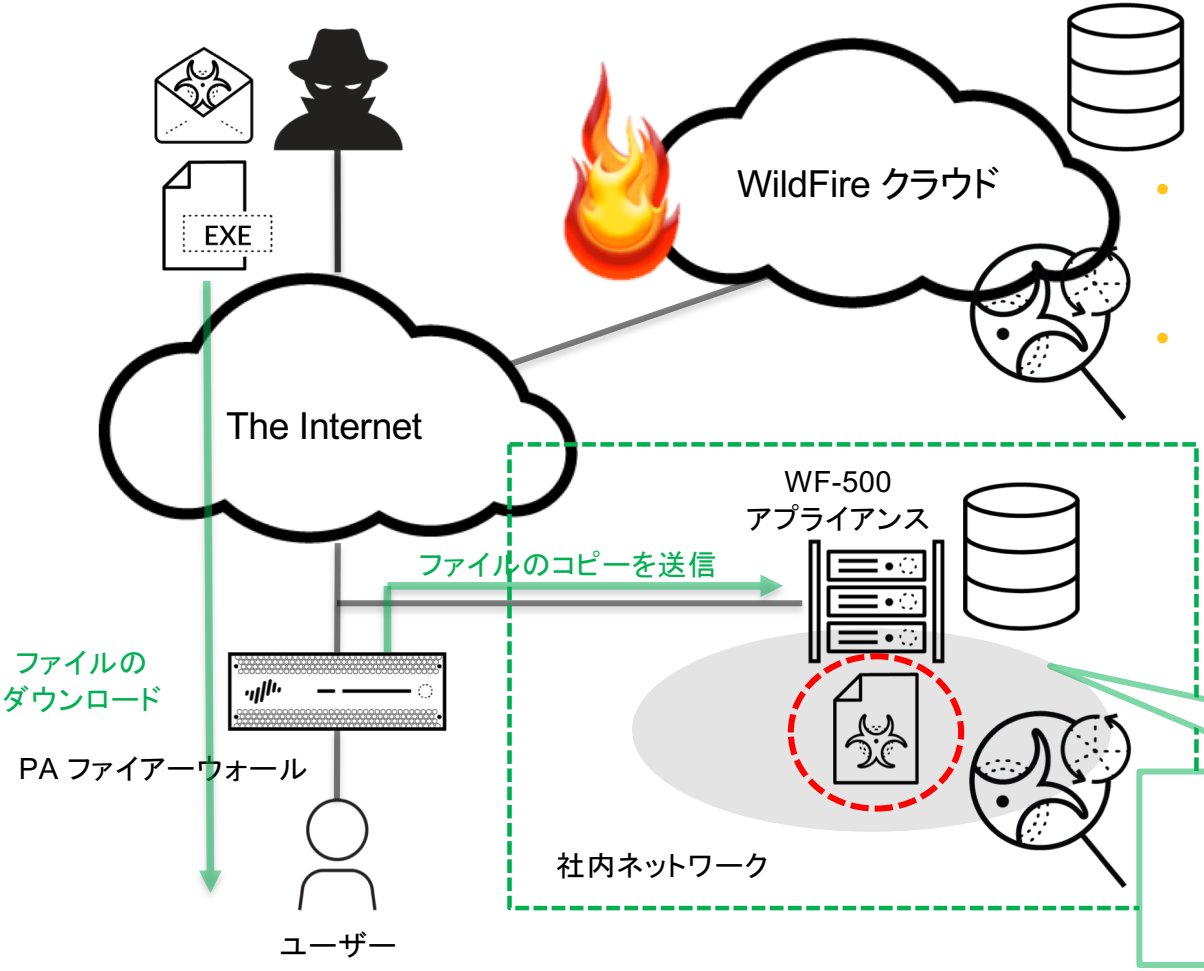
PA シリーズファイアーウォールは WildFire サブスクリプションライセンスの追加なしでも一部の基本機能 (以下表を参照) を利用可能ですが、サポートされる環境・ファイルタイプが Windows/PE ファイルのみに制限され、最大のメリットである シグネチャのダイナミック更新 (グローバルで展開される WildFire クラウドが検知した未知の脅威に対し直ちに対応) が利用出来ません。

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 アンチウィルス/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

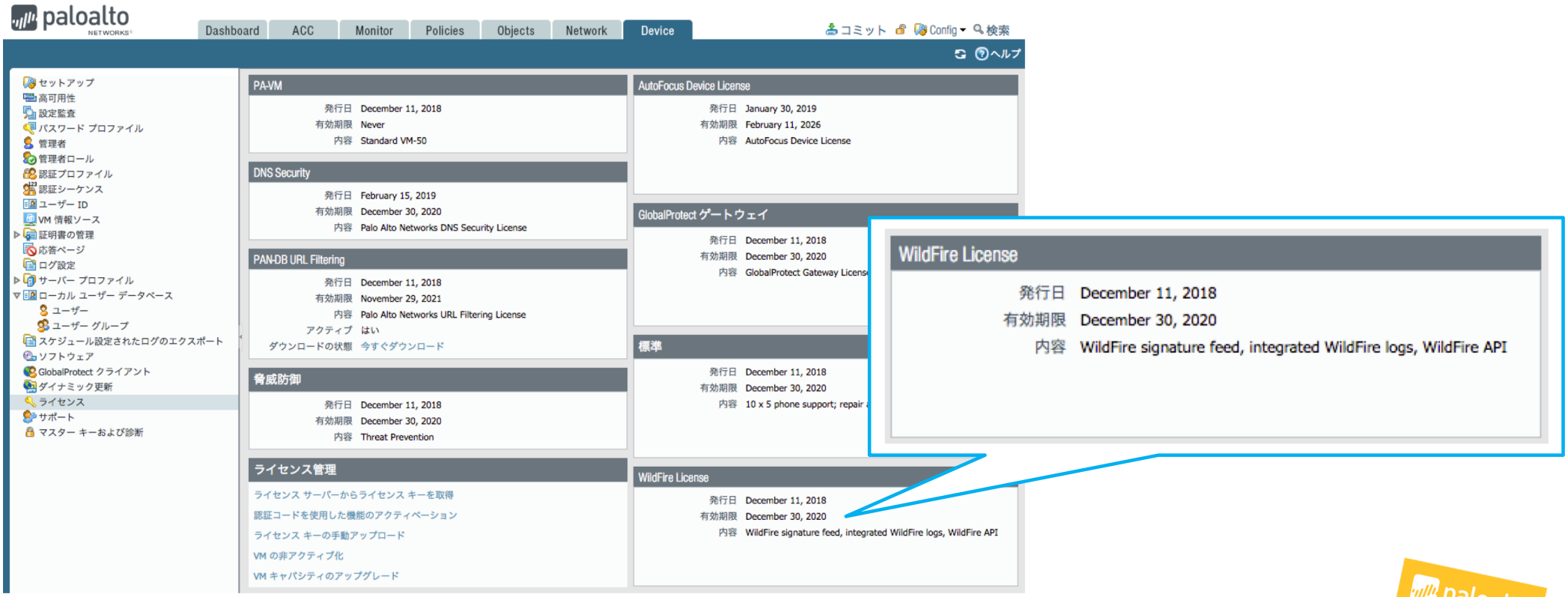
機能	WildFire クラウド	WildFire プライベート (WF-500) アプライアンス
提供形態	サービス型 (パブリッククラウド)	アプライアンス型 (オンプレミス)
WildFire サブスクリプション	ライセンスなしでも一部機能を利用可能 (Windows/PE ファイルのみ)	必須
解析環境	Windows, Mac OS X, Linux, Android	Windows XP/7 のどちらかを選択
ベアメタル解析サポート	○	×
ファイルサポート	PE (実行可能ファイル, オブジェクトコード、DLL およびフォント), Microsoft Office (ドキュメント、ワークブック、パワーポイントおよび Offide 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 Offide 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

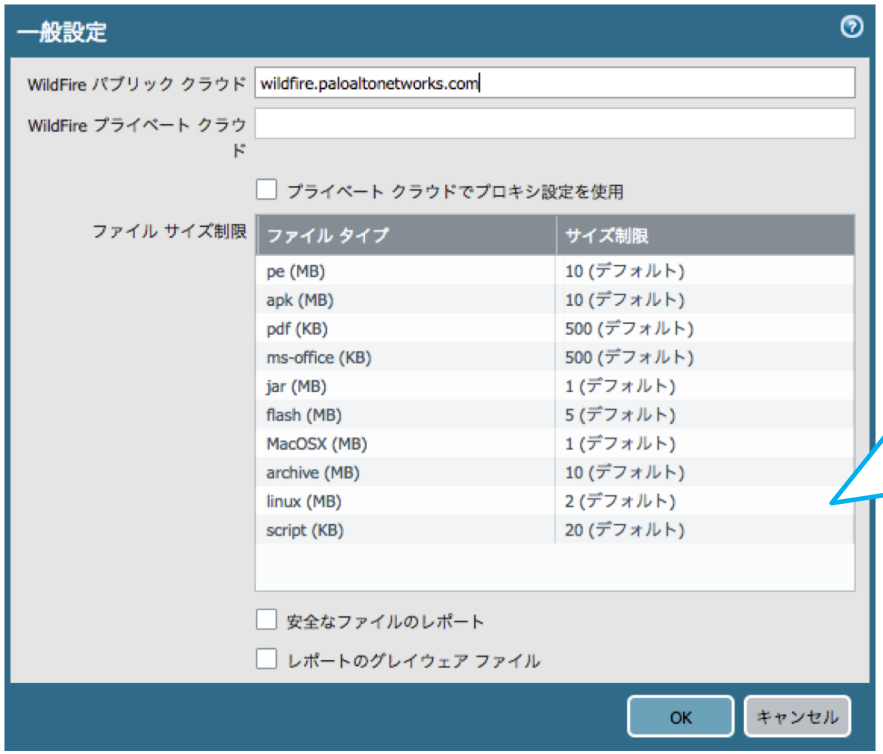


 |

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



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

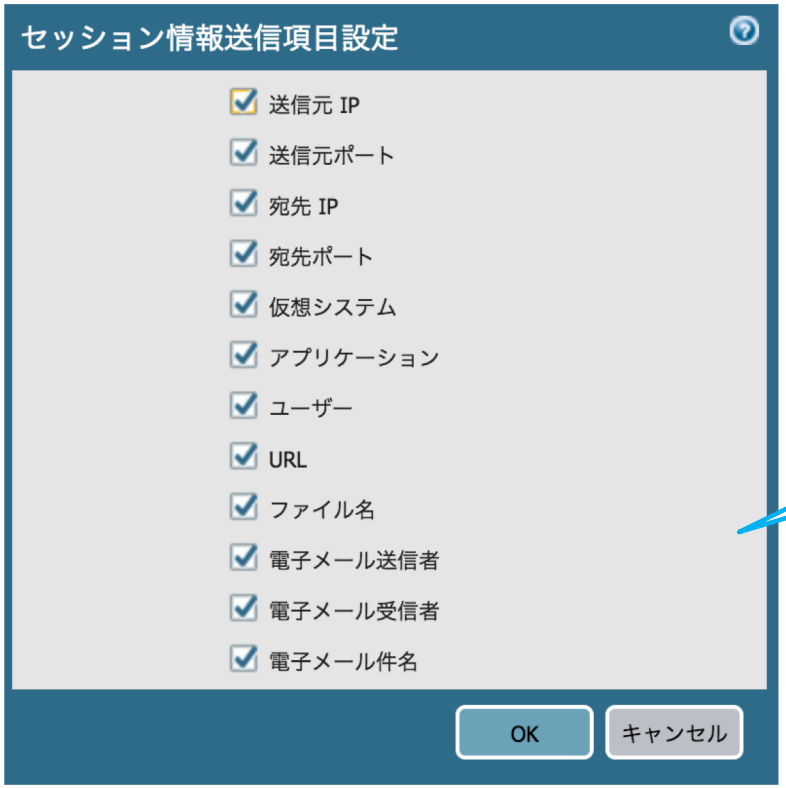
安全なファイルのレポート:
安全 (Benign) と判定されたファイルの転送をログを記録
* 電子メールリンクは対象外

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



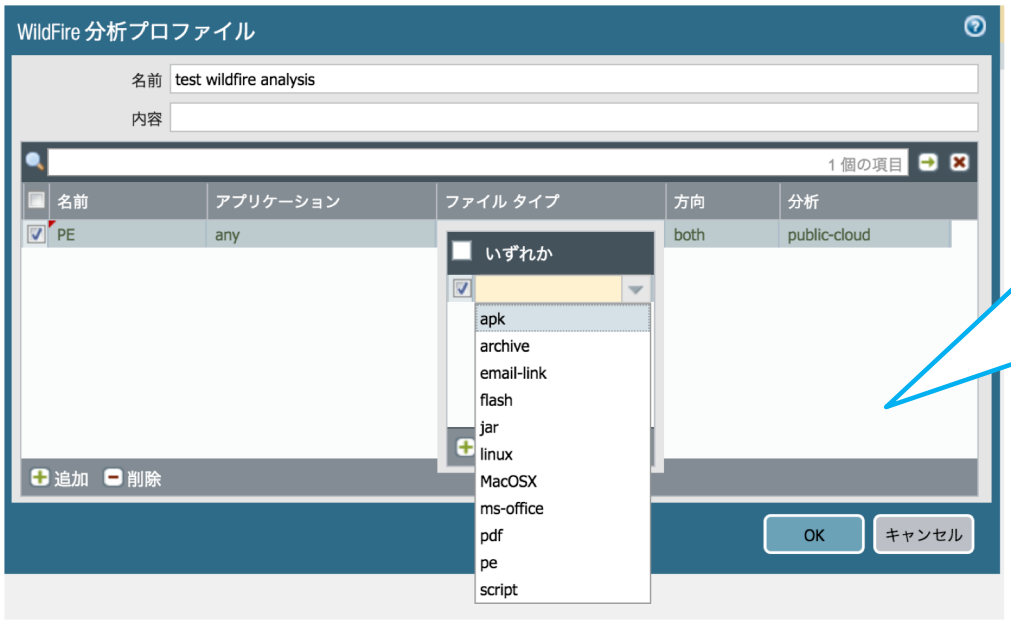
サンプルに関連するネットワークセッションの情報を送信することにより、
疑わしいネットワークイベントのコンテキストをより詳細に把握出来る
場合があります

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

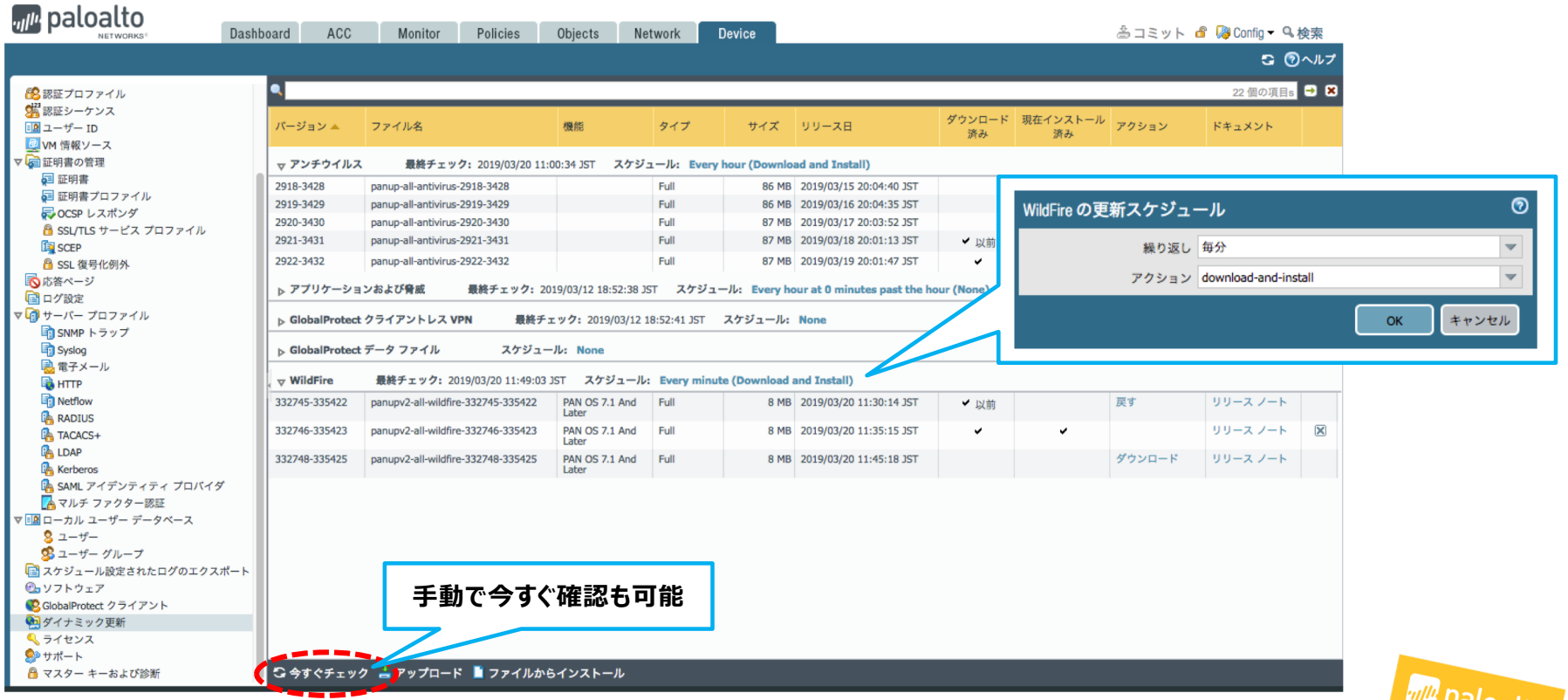
作成した WildFire プロファイルをセキュリティルールに適用

 |

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

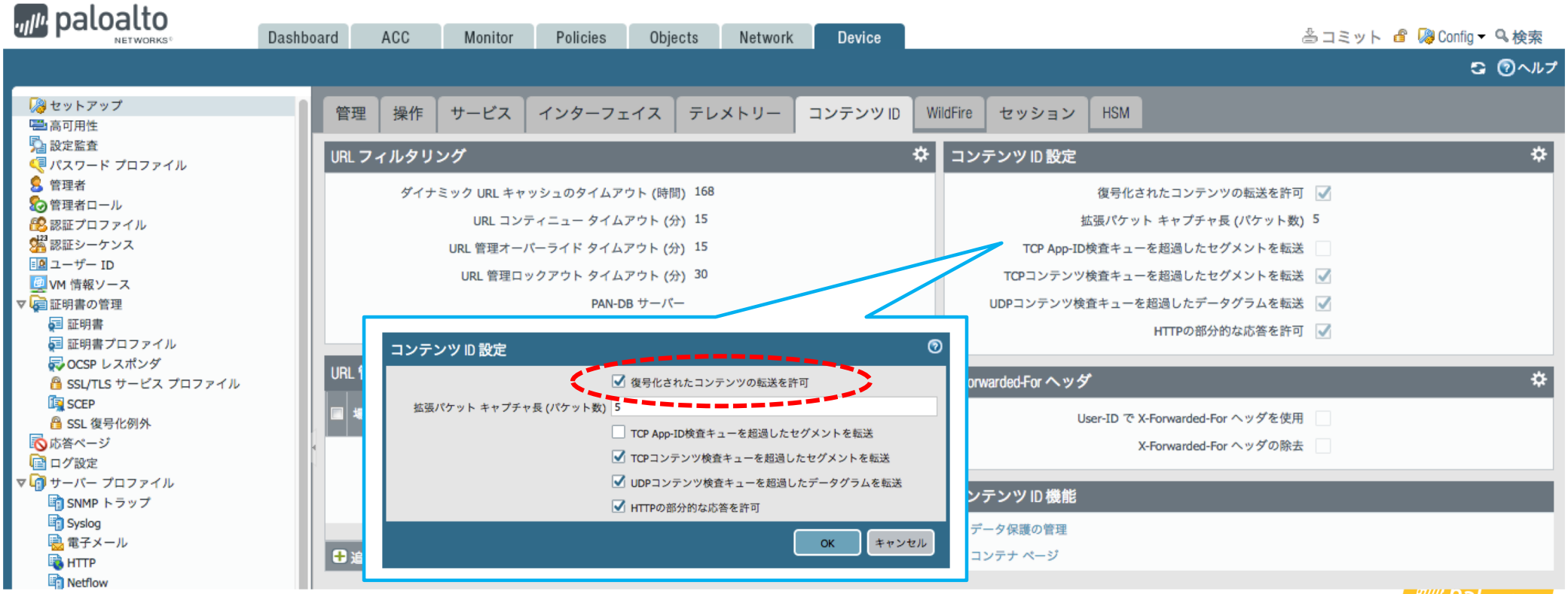
Web UI の Device > ダイナミック更新 > WildFire



設定イメージ (SSL 復号ポリシー適用時の追加設定)

- PA ファイアー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



WildFire ログイメージ

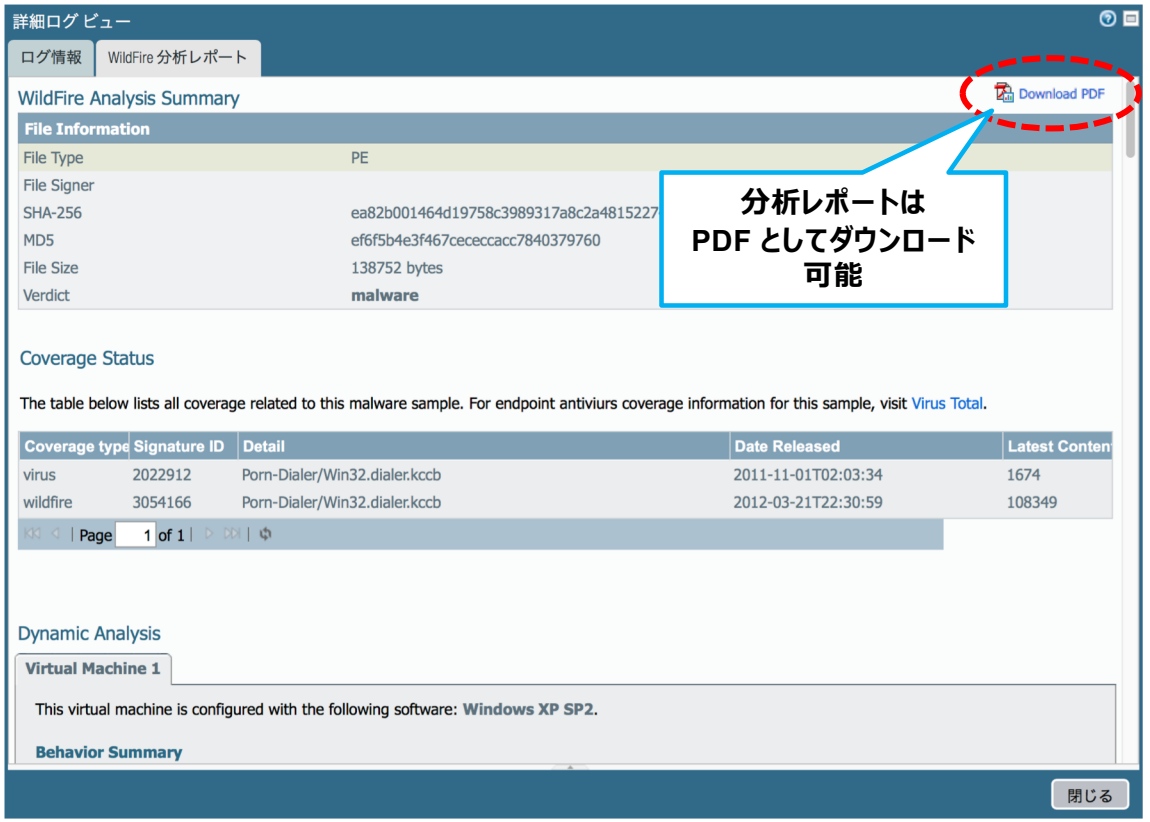
WildFire ログ (Web UI)

Monitor > ログ > WildFire への送信

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	lxKwNJNXuYTC.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



* 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)

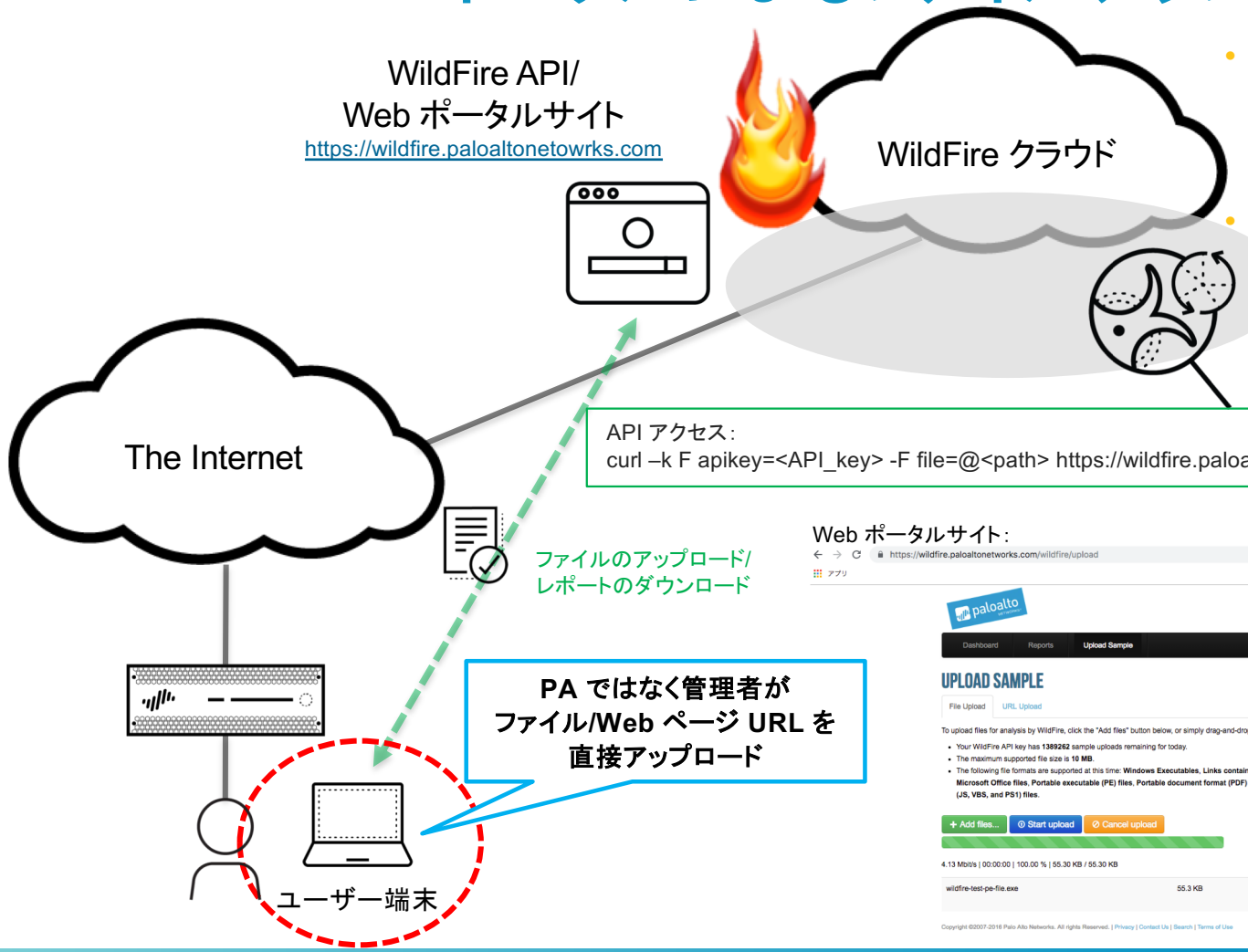
debug wildfire upload-log show channel public コマンド出力結果

knarasaki — ssh admin@192.168.55.10 — 80×31

```
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



- 疑わしいファイルを API/Web ポータル経由で直接 WildFire へアップロードし、オンデマンドで検査を行うことが可能
- サブスクリプションライセンスごとに API キーを発行。キーごとの日時のファイルアップロード/クエリの上限数はそれぞれ 1,000/10,000

Web ポータルサイト:

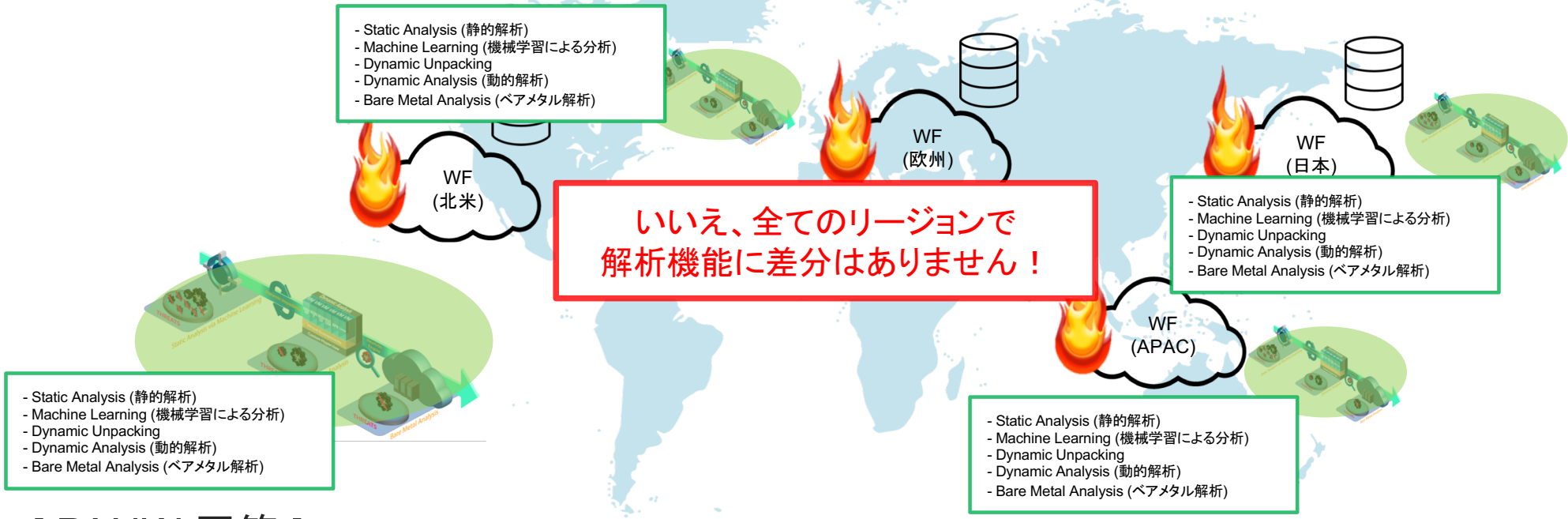
 |

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)

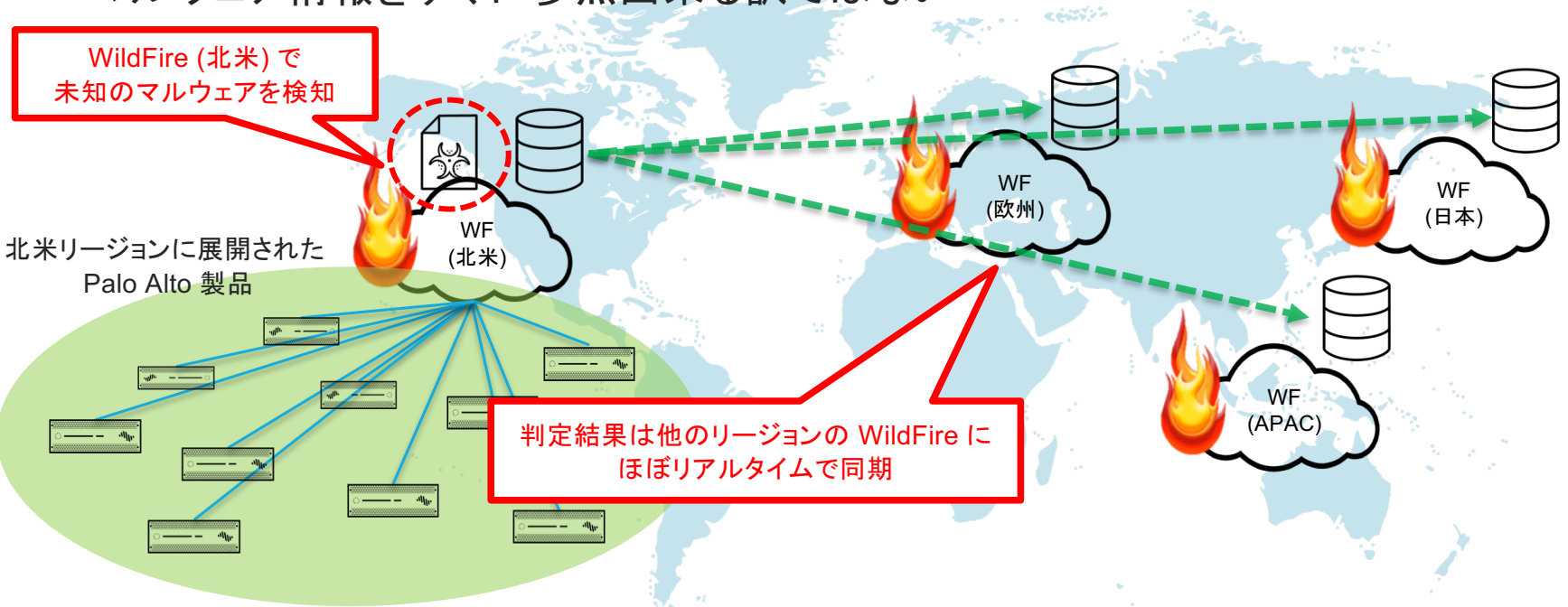
- 日本リージョンの WildFire は北米のものと比較し分析機能が少なくバージョンアップも遅いので、マルウェアの検出精度が落ちる。そのため、可能であれば北米の WildFire を利用した方が良い



[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


paloalto
NETWORKS®