標的型攻撃に備えるために

パロアルトネットワークス株式会社

Jan.2016

 © 2015, Palo Alto Networks. Confidential and Proprietary.

標的型攻撃対策

標的型攻撃

＝　未知の脅威（未知の実行ファイル（マルウェア）、未知の脆弱性）

未知の脅威は、既知のセキュリティ対策だけでは対策が難しい！！

未知の脅威　＝　サンドボックス？？

しかし、未知の実行ファイル（マルウェア）を判定する対策でも

回避されてしまうと効果は得られません！！

標的型攻撃　≠　サンドボックス

 © 2015, Palo Alto Networks. Confidential and Proprietary.

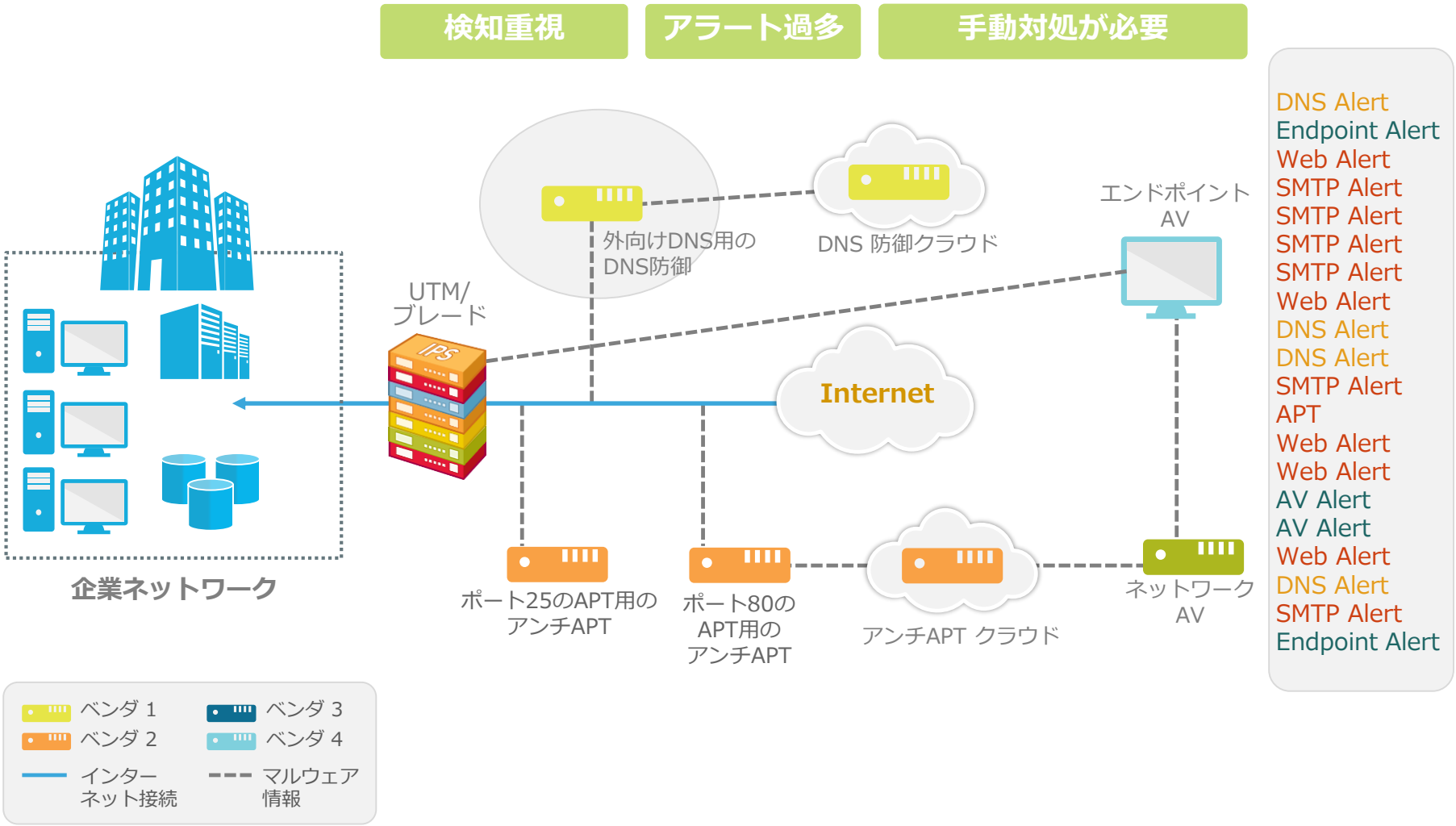
標的型攻撃対策 ≠ サンドボックス専用装置

- サンドボックス自体を検知してすり抜ける
  - 潜伏活動を行う前にInternet接続をチェックする等
  - ファイル自体を分割、暗号化、サイズを大きくすれば検査できない（例 Flame）
  - ネットワークを経由しない感染（例 USBやメディア）
- Web とメール以外の通信が検査できない
  - SSL通信（HTTPS, SMTP over SSL）
  - 独自暗号を行うP2P（i.e., SkypeやIM）、ファイル共有ソフト
  - ネットワーク内部での二次感染拡大で利用されるFTP等
- ブロックする場合にはURLやIPアドレスベース（基本検知がメイン）
  - マルウェア自体に対するシグネチャ vs URL・IPアドレスベースでのブロック

サンドボックスは抜け道があり、あくまで補完機器の１つ
ファイアウォールやアンチウィルスとの併用が大前提

 © 2015, Palo Alto Networks. Confidential and Proprietary.

現在のアプローチの欠点



エンタープライズ セキュリティ プラットフォーム

次世代セキュリティクラウド

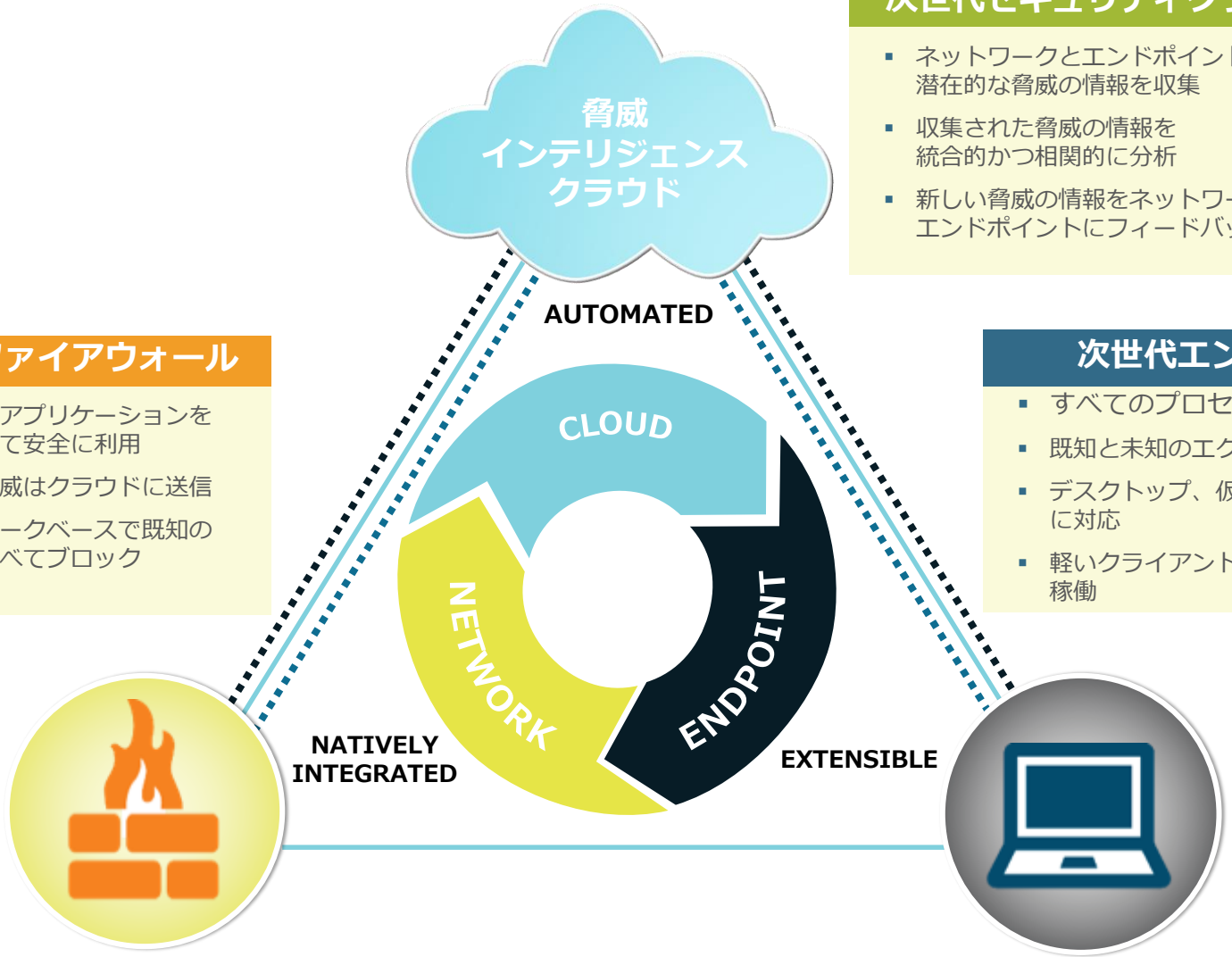
- ネットワークとエンドポイントから潜在的な脅威の情報を収集
- 収集された脅威の情報を統合的かつ相関的に分析
- 新しい脅威の情報をネットワークとエンドポイントにフィードバック

次世代ファイアウォール

- すべてのアプリケーションを可視化して安全に利用
- 未知の脅威はクラウドに送信
- ネットワークベースで既知の脅威をすべてブロック

次世代エンドポイント

- すべてのプロセスとファイルを検査
- 既知と未知のエクスプロイトから防御
- デスクトップ、仮想化、モバイル端末に対応
- 軽いクライアントが最小のリソースで稼働



次世代ファイアウォール

次世代エンドポイント

| ©2015, Palo Alto Networks. Confidential and Proprietary.

最新脅威にはポイント製品ではなくソリューションが必要

防御情報

1 攻撃面の削減

- アプリケーションのホワイトリストとハイリスクアプリのブロック
- 既知のウイルスやエクスプロイト防御
- 攻撃を受けやすいファイル種別をブロック

2 未知の脅威検知

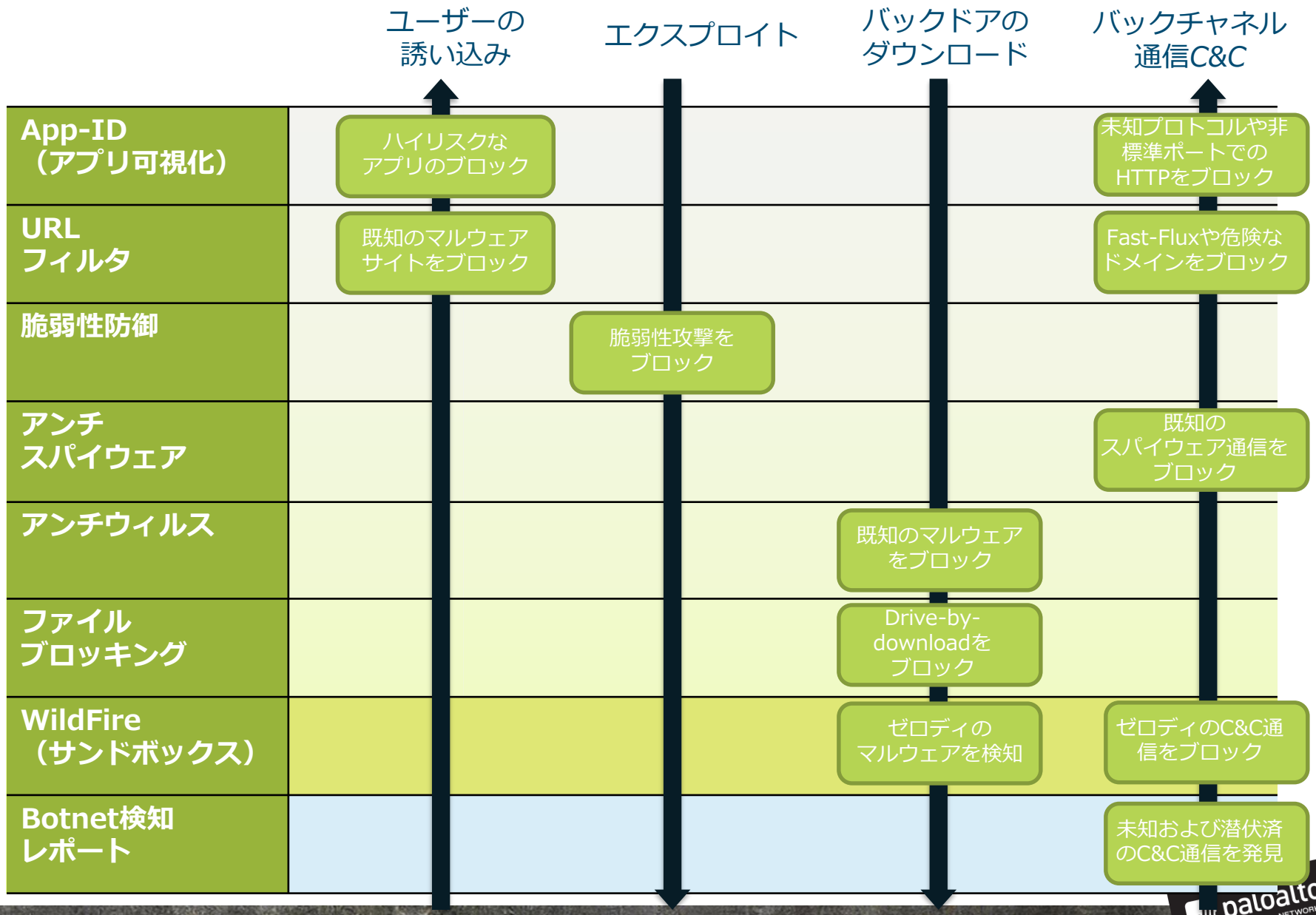
- 全アプリケーショントラフィックを分析
- SSL 復号化
- WildFire によるファイルのサンドボックス分析

3 防御情報生成

C&C通信の検知とブロック:

- DNSトラフィック内の悪意ドメイン
- URL (PAN-DB)
- C&C シグネチャ (アンチスパイウェア)

*Kill Chain*に対応した多層的な防御アプローチ



パロアルトネットワークスのプラットフォームを活用した対策

 © 2015, Palo Alto Networks. Confidential and Proprietary.

標的型攻撃に対する４つのアプローチ

対策 1

脅威の侵入経路を狭める（攻撃面の削減）
App-IDによるアプリケーションレベルで通信制御

- 危険性の高いアプリケーションは必要なユーザーにのみ通信制御
- すべてのアプリケーションの利用状況は必要なユーザーにのみ利用を限定
- 潜在的な攻撃の侵入経路をなくす

対策 2

マルウェアの侵入を食い止める
Content-ID＋WildFireによるマルウェア防御

- シングルエンジンによる高速スキャンニングで脆弱性攻撃・ウイルス本体のダウンロード・バックドア通信のすべてをブロック
- 他社製品では複数台必要な処理を1台でかつ高速に処理可能
- WildFireで新種のマルウェアにも迅速に対応

対策 3

侵入を許した感染端末をできる限り早く発見
ボットネット検知レポートで感染端末を洗い出す

- 振る舞いベースでバックドア通信を検出し、Dailyでレポート
- 不明なプロトコルやIRCなどの通信が多い端末をリストアップ
- スパイウェアサイト、IPアドレス、DDNSドメインなどのアクセス量から判断

 ©2014, Palo Alto Networks. Confidential and Proprietary.

標的型攻撃に対する４つのアプローチ

対策 4

エンドポイントで未知の脅威の感染を防止

Trapsによる未知の脅威の感染をブロック

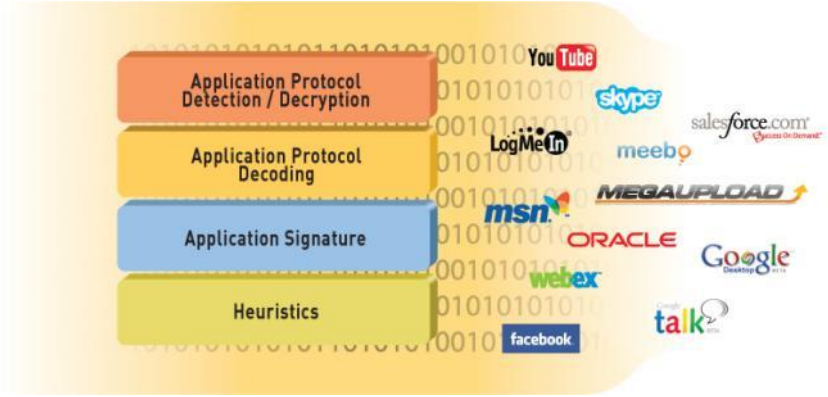
- 未知の脅威（エクスプロイト、未知の実行ファイル）が端末に感染する時点で、感染をブロック
- 既存のエンドポイントセキュリティ（AV）を補う

 ©2014, Palo Alto Networks. Confidential and Proprietary.

次世代ファイアウォールを構成するコア技術

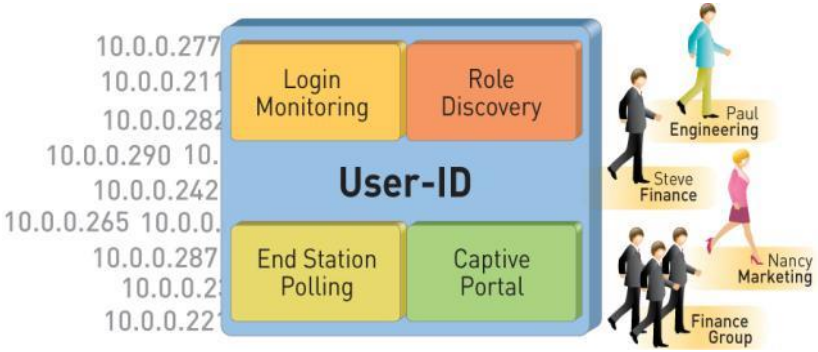
App-ID™

アプリケーションを識別



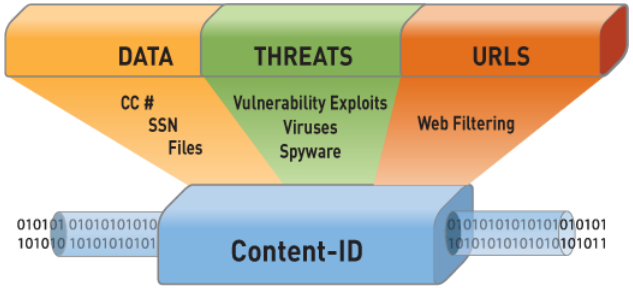
User-ID™

ユーザーを識別



Content-ID™

コンテンツをスキャン



App-ID™:
全てのトラフィックのアプリケーションを自動的に識別

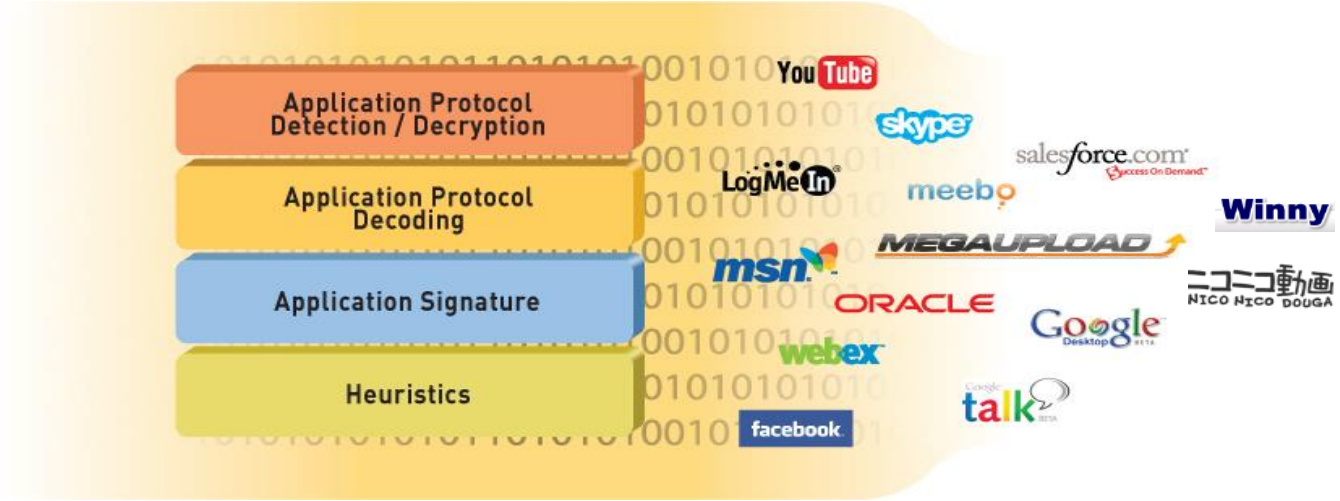
対策
1

- **攻撃面の削減**
  - **App-IDの使用**
    - Unknown TCP/UDP アプリケーションを調査して識別。App-IDを生成
    - すべてのUnknown-TCP と Unknown-UDP をブロック
  - **Application Command Center（ACC） の活用**
  - **ファイルブロッキング**
    - 潜在的に悪質なファイルを入れない

 © 2015, Palo Alto Networks. Confidential and Proprietary.

App-ID™:
全てのトラフィックのアプリケーションを自動的に識別

対策 1

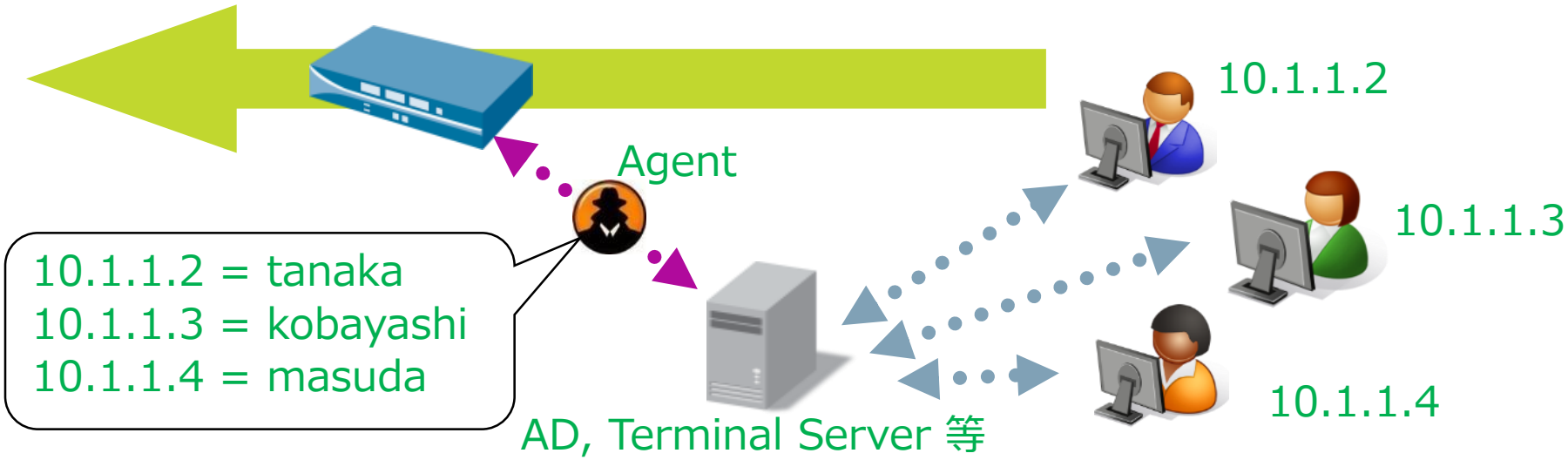


- ファイアウォール処理に完全統合されたアプリケーション識別エンジン
- 全トラフィックに対してアドレス、ポート番号、プロトコルに加え
  アプリケーション情報まで自動的に識別
- SSL暗号通信は一度復号化した上で中に隠れたアプリケーションを識別可能
- ビジネス、インターネット、ネットワーキングと幅広く、約2,000種類の
  アプリケーションとプロトコルをサポートし、DB更新により毎週続々と追加
- 自社開発のアプリケーションにもリクエストに応じて対応
- カスタムシグネチャにより即時対応も可能

paloalto NETWORKS

User-ID™:
IPアドレスから自動的に利用ユーザを識別

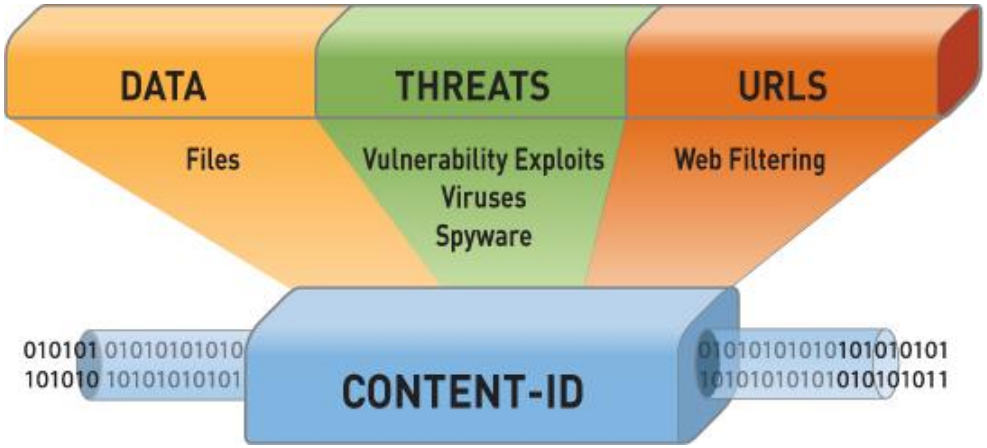
対策
1



- 外部サーバーからユーザー名とIP アドレス、そして、所属グループ情報を取得し、それを元に自動的にマッピングテーブルを作成
  - Active Directory, Novell eDirectory , Microsoft Terminal Server, Citrix XenApp Server, LDAP（Web認証＋Directory内のグループ検索）, Radius（Web認証のみ）に対応
- **ユーザーまたはグループ情報を基にポリシーを適用し、ログ・レポートも生成**

対策 2

Content-ID™：様々な脅威を防ぐ高速コンテンツ スキャンニング



1つのエンジンで3つのコンテンツ セキュリティ機能を提供

- **脅威防御（*）**
  脆弱性攻撃、スパイウェア、マルウェアなどを防御
- **情報漏えい対策**
  ファイルタイプやデータのパターン（クレジット番号や特定文字列）によってブロック
- **Web フィルタリング（*）**
  URL カテゴリ情報を元にしたWeb アクセスを制御

（*）：別途サブスクリプションが必要

 ©2014, Palo Alto Networks. Confidential and Proprietary.

Content-ID™：様々な脅威を防ぐ高速コンテンツ スキャンニング

対策 2

- **攻撃面の削減**
  - **ファイルブロッキング**
    - 潜在的に悪質なファイルを入れない

 © 2015, Palo Alto Networks. Confidential and Proprietary.

ファイルブロッキング
– なぜ潜在的に悪質なファイルを組織内に入れるのか?

対策 2

- ファイルブロッキングを使ってPE (.scr, .exe) やLNK ファイル、Help ファイルをブロックする
  - .LNK や .HLP を通さなければならない理由があるか？
  - 従業員が .exe をダウンロードしたらポップアップで警告を出す – ドライブバイダウンロード防御
  - 悪質な RTF 緩和
  - PE ファイル種別: .exe, .cpl, .pif, .bat, .dll, .scr

“LNK” Attacks are Back Again

Targeted Attacks Make WinHelp Files Not So Helpful

Created: 15 Oct 2012 20:58:12 GMT • Updated: 23 Jan 2014 18:12:02 GMT • Translations available: 日本語

It's 2014 and you can pwn a PC by opening a .RTF in Word, Outlook

The Register®

paloalto NETWORKS

ファイルブロッキング
– 搾取

対策 2

- 知的財産を会社に置いたままですか？
- Target の事件 – .zipファイルを使ったFTPでの搾取
- 暗号化ファイル種別: 何が会社に置かれているか可視化を提供
  - **暗号化 .rar**
  - **暗号化 .pdf**
  - **暗号化 .zip**
  - **.CAD ファイル**

全脅威防御

対策 2

- 脅威防御 = アンチウイルス, IPS, スパイウェア/C&C通信
- **IPS:**
  - 既知の脆弱性に対する脆弱性防御
  - MAPP (Microsoft Active Protections Program) のパートナー
  - 適切なIPSポリシーを実施
  - 日次レポートをスケジュール – ログを確認
  - 誤検知をレポート
- **スパイウェア/ C&C/IoC: 感染端末を見つける**
  - 全スパイウェアイベントをブロック – C&C および DNS イベント
  - 1日当たり8,000件の DNS シグネチャ (PAN-OS 5.0以降)
  - これらイベントを見る。精度と信頼性が高いため
  - Wildfireからの提供もある
- **ネットワークベースのアンチウイルス**
  - ストリーミングベースのアンチウイルス
  - WildFireからの提供もある

paloalto NETWORKS

脆弱性リサーチと防御

対策
2

- MAPP (Microsoft Active Protections Program) の活動メンバ
- 2014年は50以上のMicrosoftとAdobeの脆弱性を発見
  - 3件の重要な IE 脆弱性 (2014年11月)
  - 15件の重要な IE 脆弱性 (2014年9月)
  - 3件の重要な IE 脆弱性 (2014年8月)
  - 10件の重要な IE 脆弱性 (2014年7月)
  - 22件の重要な IE 脆弱性 (2014年6月)
  - 4件の重要な IE 脆弱性 (2014年2月)
- MicrosoftやAdobeとの緊密な協力関係
- Virus Bulletin, Black Hat Europe, Microsoft BlueHat 2014で講演
- BlackHatのスピーカー
- Unit 42 脅威インテリジェンスチーム

 © 2015, Palo Alto Networks. Confidential and Proprietary.

既知の攻撃をブロック

対策
2

- **URLフィルタリング:** URL フィルタリング (PAN-DB) を使う
  - アダルトやギャンブルサイト対策、カテゴリ用途だけではない
  - WildFireからのマルウェア URL 防御

URLフィルタリングによるWeb 防御 – PAN-DB

対策 2

- URLフィルタリング (PAN-DB) を使う
  - アダルトやギャンブルサイト対策、カテゴリ用途だけではない
  - WildFireからのマルウェア URL 防御
- FBI/Infragard/DHS の様な諜報機関からの脅威情報が PAN-DB に追加
- UnknownカテゴリのWebサイトからダウンロードをさせないことで感染を防ぐ
  - 最低限 'コンティニュー' ページを使う
  - URLフィルタリングとファイルブロッキングポリシーを併用する
- 感染端末からのC&C通信を切断する – unknownカテゴリのWebサイトへの外向けWebリクエストに対してコンティニューページを適用

paloalto NETWORKS

WildFire™：サンドボックスによる未知のマルウェア検知

対策 2

- 仮想サンドボックス環境でファイルを実行することで振る舞いベースでマルウェアを検知
  - 100以上の振る舞いを検査
  - クラウドサーバーは日本にも設置
  - Web/Email/FTP 等複数のプロトコルをサポート
- 特定されたマルウェアに対するシグネチャを自動的に生成
  - マルウェア本体と C&C 通信に対する防御
  - 定期アップデートでシグネチャを全てのファイアウォールに対して配信
- マルウェアの活動に関するフォレンジックと分析を提供
  - ターゲットとなったマシン上での動作
  - マルウェアの伝染に用いられたアプリケーション
  - マルウェアの配信に利用されている URLのリスト

2011年よりサービス開始、現在WWで5,000社以上の利用実績

未知の攻撃からの防御

対策
2

- **Wildfireを有効化**
  - サポートする全ファイル種別に対してWildfireを有効化
    - 特に外部からのファイル
  - 悪質なPDF, 悪質なOfficeファイル, ゼロデイRTFファイルの防御
  - ゼロデイ脆弱性の緩和

WildFire™：動作イメージ

対策 2

ファイル解析は *WildFire*™ で実施
サンドボックス分析は数分以内で完了

WildFire™ Japan
日本国内に構築された
サンドボックス環境

マルウェアファイルだけが
本社に送信され、対応の
シグネチャを生成

未知のファイルは
サンドボックス分析
のため*WildFire*™に
送信

マルウェア が検知され
ると対象機器にログで
通知*

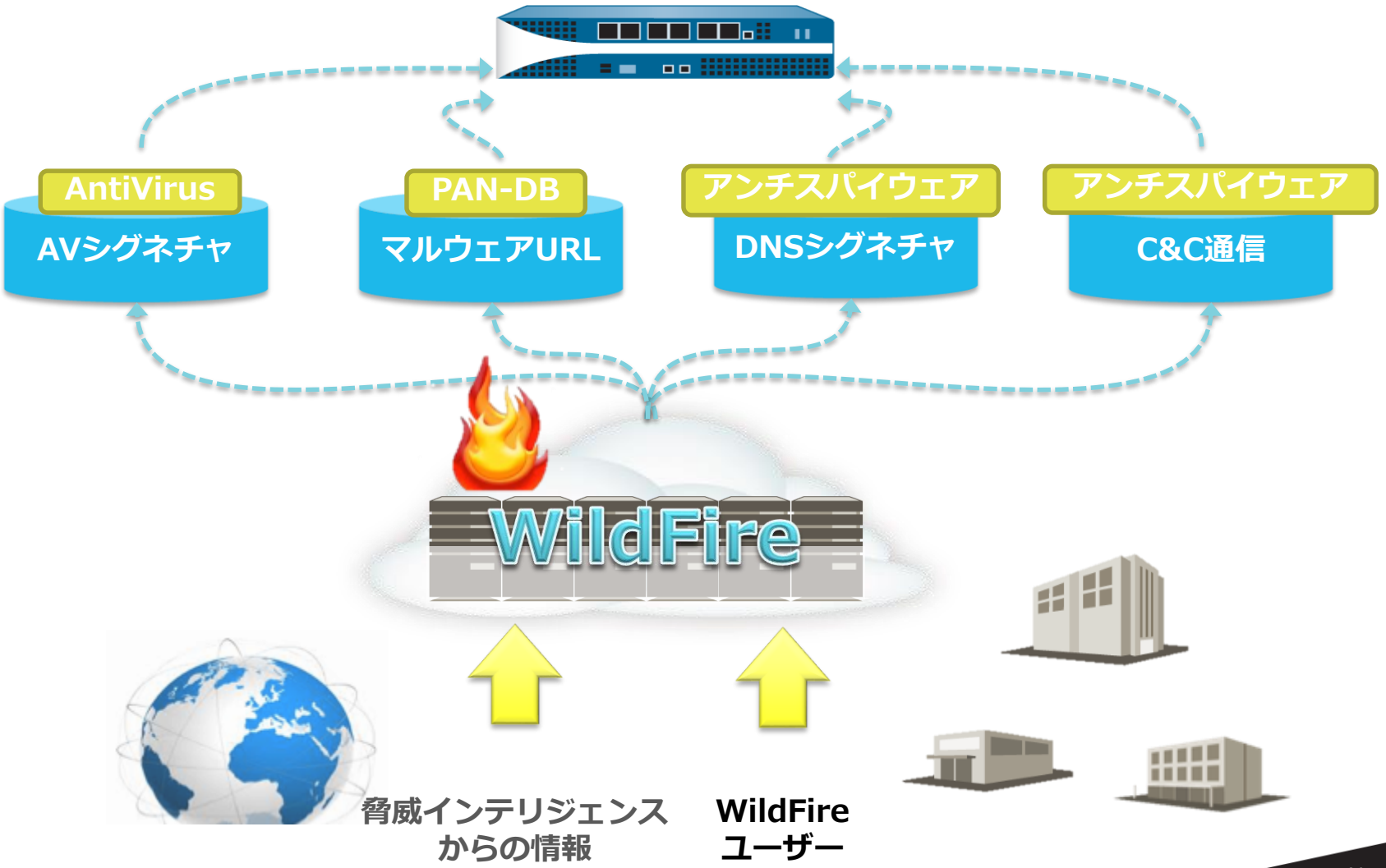
シグネチャ は、
5分間隔で
世界中のお客様に
一斉配信*

*別途サブスクリプション購入が必要

あくまでクラウド上で実績がない"未知の"ファイルのみが解析対象、
ファイルをクラウドへ送信せずにシグネチャ配信を受けるだけでもOK! *

“WildFire™”の波及効果

対策 2



paloalto NETWORKS

ボット感染端末を早期に発見・防御

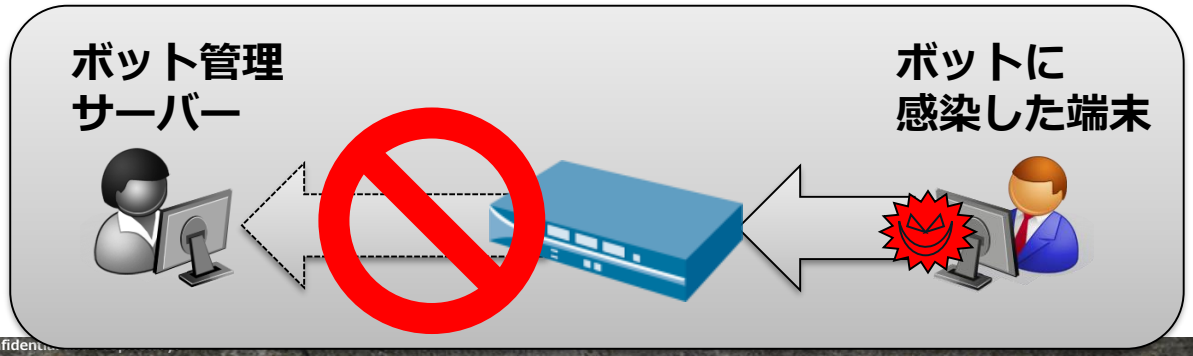
対策 3

ボットネットレポート

1日のログから、端末がボットに感染した可能性を分かり易くレポート

- 感染の可能性をレベル1～5で表示（レベル4、5は感染の可能性が高い）
  - 1日前のアクセスログ、脅威ログ等をベースに各端末の行動を分析
    - マルウェアサイトに定期的に通信を行っている
    - *IP*アドレスで直接インターネットに接続
    - 不明なサイトから実行ファイルをダウンロードしている

	Confidence	送信元アドレス	内容
1	5	.30	Downloads executable(s) from malicious URL exrexycheck.ru/file.php . Repeatedly visited (56) the same malicious URL "gatareykahera.ru/"
2	4	.12	Repeatedly visited (6) the same malicious URL "kougeihin.jp/facilities/fancybox/fancy_shadow_e.png"



未知の攻撃からの防御

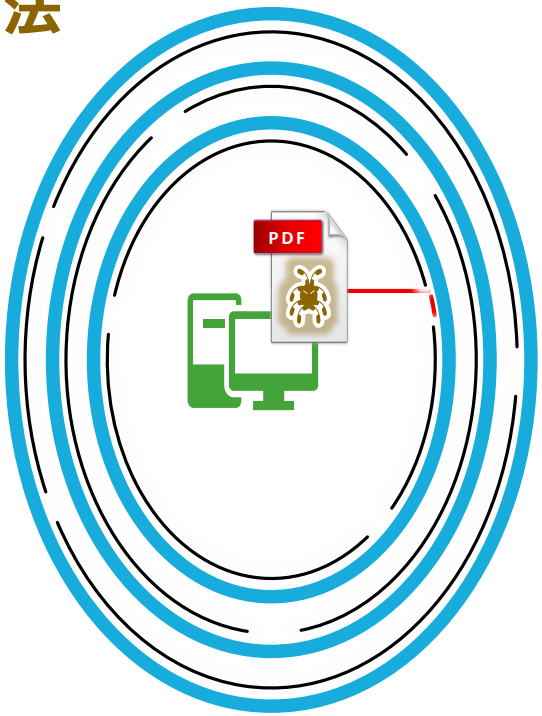
対策
3

- **ボットネットレポート**
  - 多くの顧客で感染システムを発見
  - 新しく登録されたドメインなど感染に関連する通信を分析

アドバンスト エンドポイント プロテクション - *Traps*

対策 4

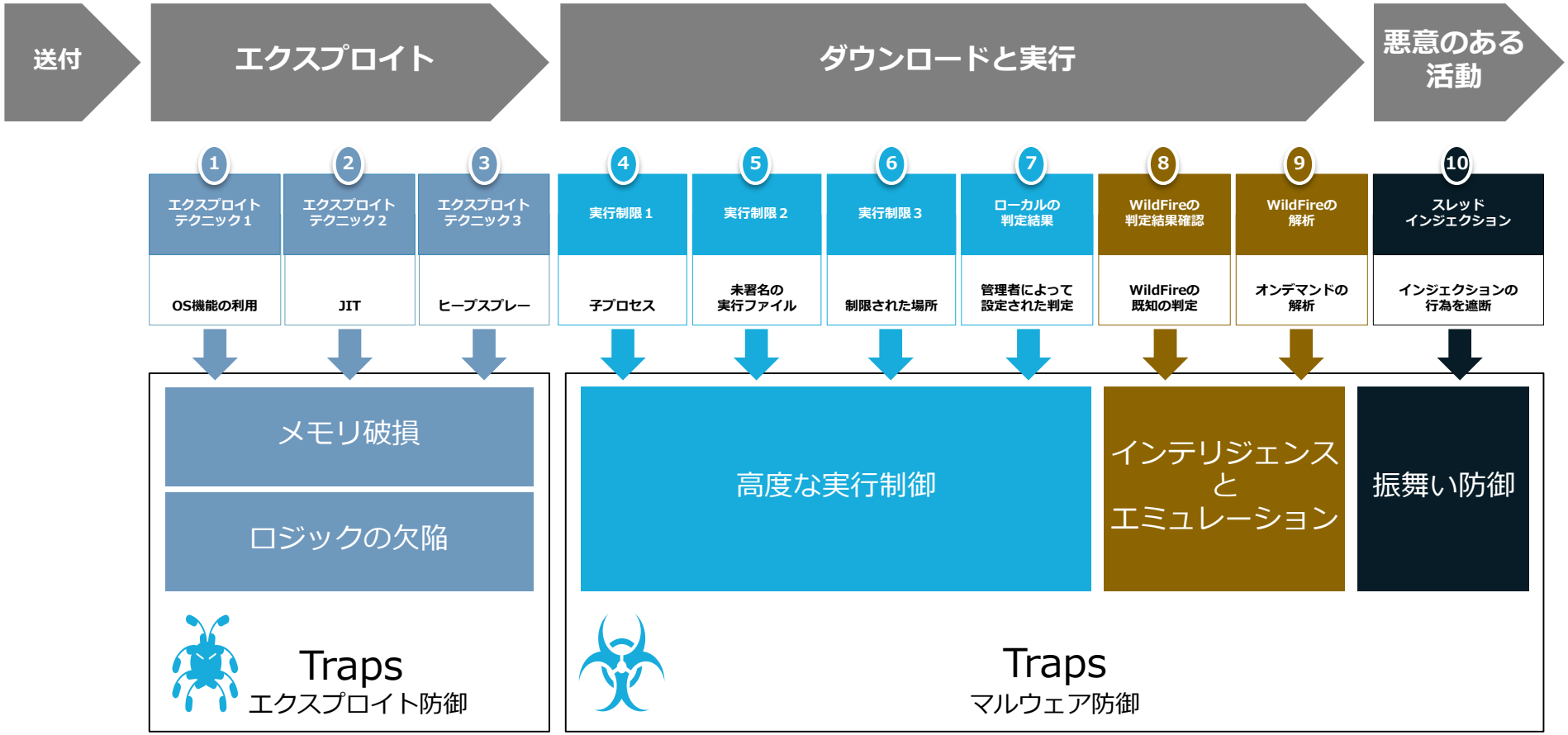
高度なサイバー攻撃に対峙するための正しい方法



- **エクスプロイトを阻止**
  - ゼロデイエクスプロイトを含む
- **悪意のある実行ファイルを阻止**
  - 高度かつ未知のマルウェアを含む
- **攻撃試行の証拠を収集**
  - 後の解析に必要となる証拠取得
- **拡張性、軽快性、フルカバレッジ**
  - 最小限のユーザインパクトで、全てのアプリケーションに保護を適用
- **ネットワーク・クラウドセキュリティとの統合**
  - **脅威**データの共有と、組織間をまたいだ保護の提供

攻撃の流れの中にあるTrapsの阻止ポイント

対策 4



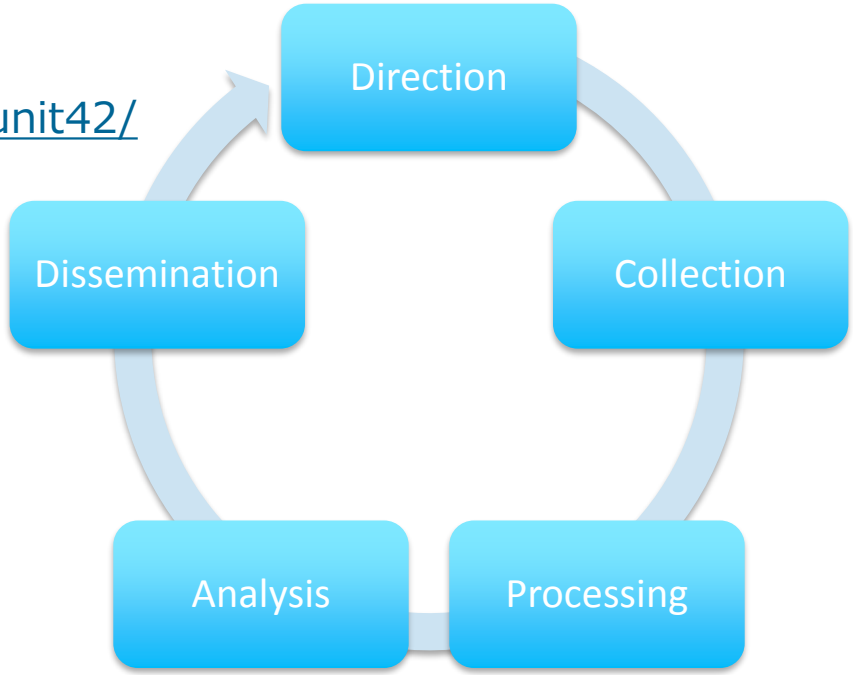
脅威のリサーチ

 © 2015, Palo Alto Networks. Confidential and Proprietary.

Unit 42 - 脅威リサーチチーム

- パロアルトネットワークスの脅威インテリジェンス チーム
  - 元NSA, US Army, US Air Forceなどのメンバーで構成
- 情報入手
  - 社内： WildFire, Passive DNS…
  - 社外: コミュニティ, 有料データフィード等
- 情報発信
  - ブログ, ホワイトペーパー 他…
  - researchcenter.paloaltonetworks.com/unit42/

Intelligence Cycle



Unit42 が世界初でレポートした代表的な脅威

- ❖SilverSpaniel
  - ❖419詐欺の進化
- ❖WireLuker
  - ❖MacOS X, iOS を狙った新しいマルウェア
- ❖CoolReaper
  - ❖中国製タブレット製品に組込まれたバックドア

 © 2015, Palo Alto Networks. Confidential and Proprietary.

CYBER THREAT ALLIANCE

Cyber Threat Appliance はサイバーセキュリティのエリアで活動する会社を中心としたグループで、世界中の脅威の情報をお互いに共有することで、進化する高度な脅威に対する防御を向上することを目的として設立

参加企業

paloalto NETWORKS
Symantec.
FORTINET
McAfee
BARRACUDA NETWORKS
REVERSING LABS
Telefonica
zscaler Secure. Everywhere.

 © 2015, Palo Alto Networks. Confidential and Proprietary.

paloalto NETWORKS

the network security company™