



サイバー攻撃観測情報配信サービス Active Defense Cyber Tactical Database 紹介資料

v1

2018/10/31

株式会社アクティブディフェンス研究所

提供会社概要

法人名：株式会社アクティブディフェンス研究所

設立日：2016年10月31日

資本金：127万円

所在地：東京都千代田区

代表取締役：忠鉢 洋輔

決算期：9月

従業員：4名

Web: <https://www.activedefense.co.jp/>

Active Defense Cyber Tactical Database (AD-DTD)

- 日本にフォーカスしたサイバー攻撃観測情報配信サービス
 - 自社で構築した攻撃観測システムにて、サイバー攻撃（バラ撒き）を観測、1時間以内にお客様にお届け
- 現在、以下の観測情報を配信中
 - Malvertising->Exploit Kit
 - コミュニティベースの脅威情報を弊社観測システムで検証し再配信
- 開発中の観測情報
 - malspam
 - IoT, Linuxマルウェア

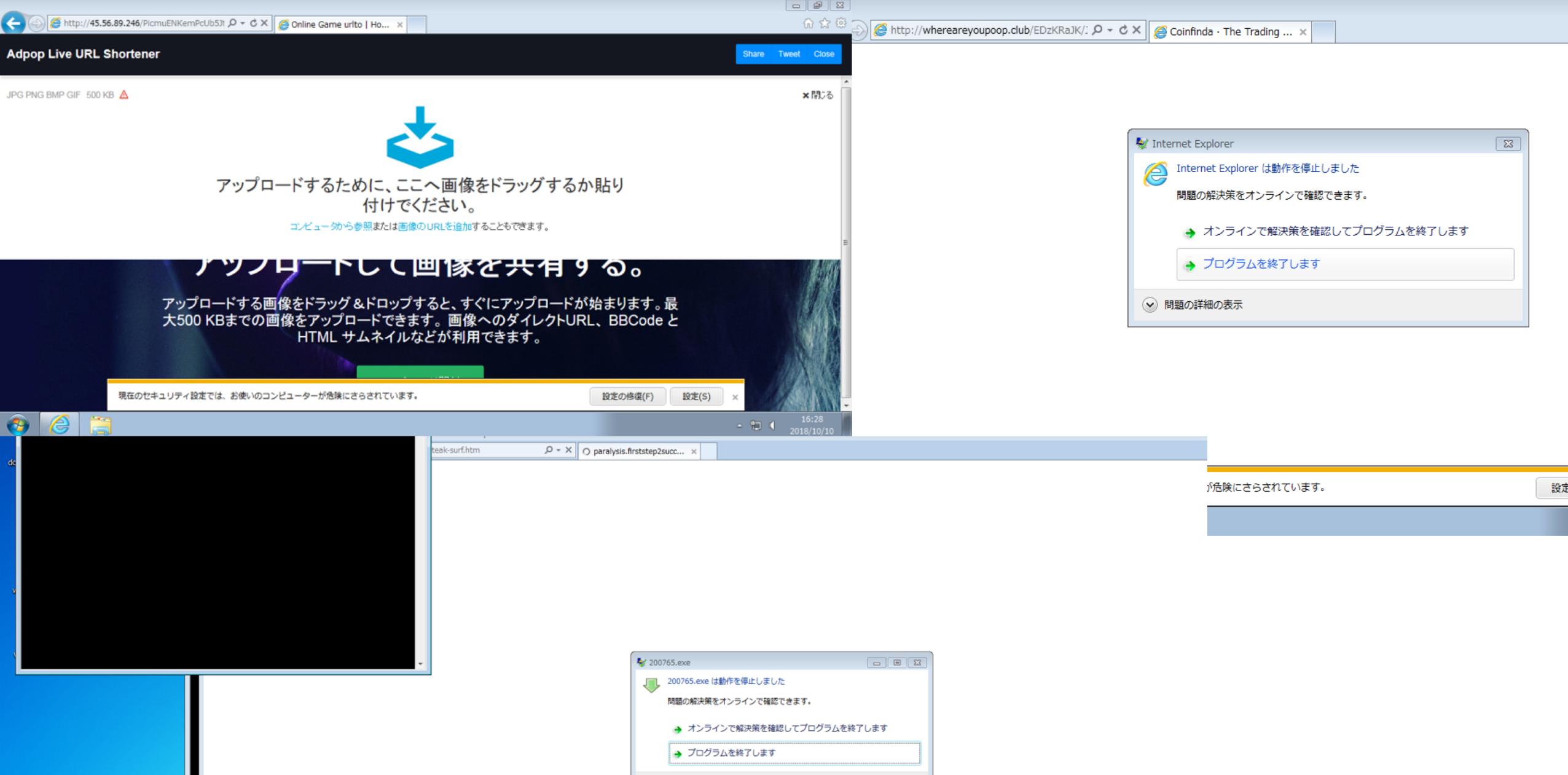
国内にフォーカスしたサイバー攻撃観測の基本的な考え方

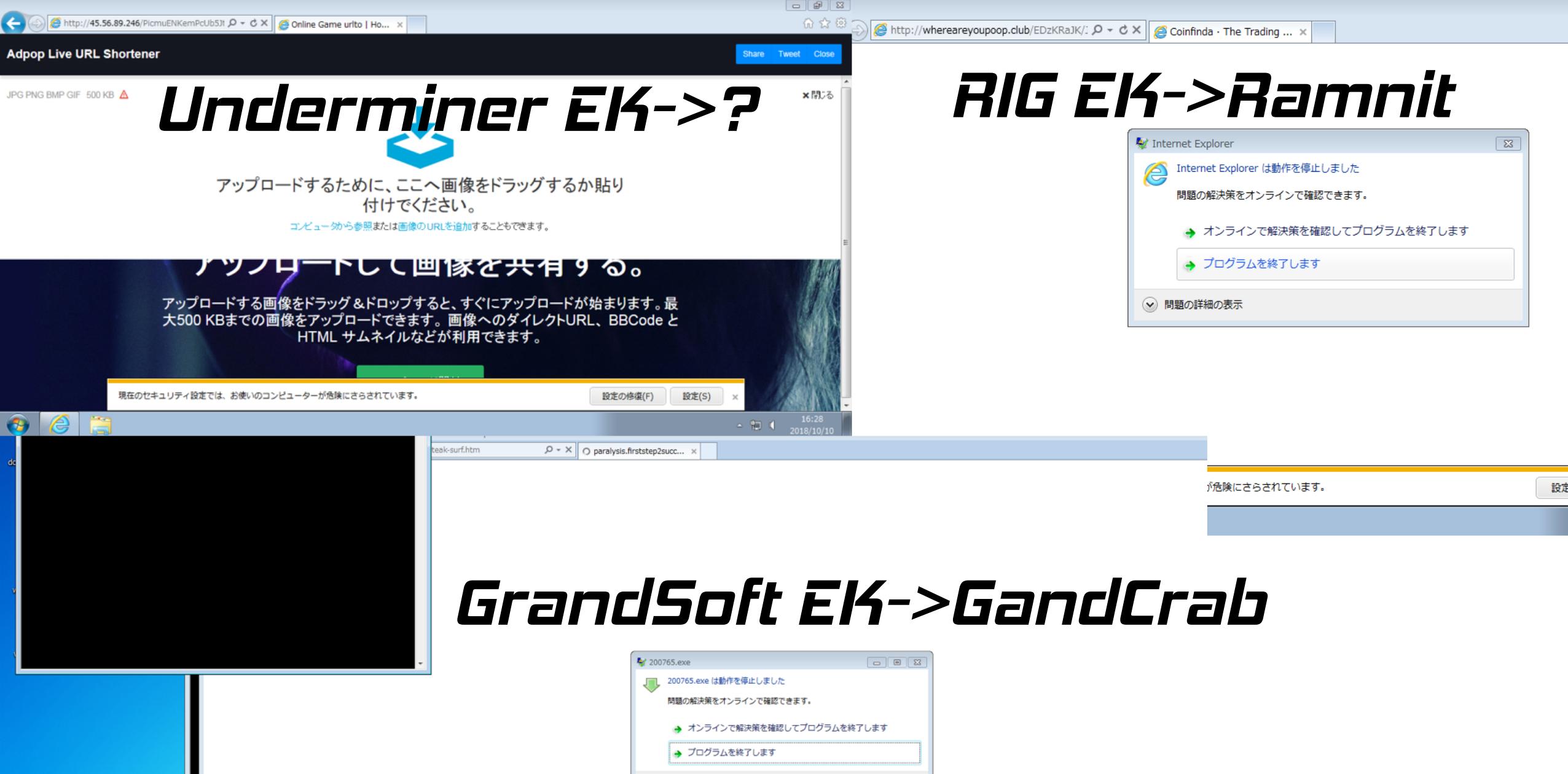
- インターネットには局所参照性がある
 - 主に言語の違い
 - また、国や地域によってサービスシェアが違う
- サイバー攻撃にもローカリティ（局所性）が存在する
 - 攻撃対象ユーザー、攻撃対象サービスそれぞれ局所性がある
- サイバー攻撃の90%はバラ撒き型
 - 弊社では、兎にも角にも日本をターゲットにしたバラ撒き型攻撃を正しく、正確に把握するため、AD-CTDとその観測システムを構築

日本に必要十分な脅威情報を目指します

- ・果たして、日本国内から到達可能で、かつ将来に渡って日本で感染がありえる情報はどれだけあるのか？
- ・量や情報源でアピールすることが多いが、実際に日本で使うに当たり有用なIoCは限られているのでは無いか？

弊社はCTDにて観測をベースとしたデータを蓄積し、この問題を明らかにしていきます





株式会社アクティブディフェンス研究所

2018年8月27日月曜日

日本を標的とした新たなDrive-by Download攻撃キャンペーンPseudoGate

概要

弊社ではCyber Tactical Databaseという脅威情報配信サービスを提供していますが、そのためのThreat Huntingの一環として、Drive-by Download攻撃の観測・解析を行っています。これまで日本を標的としたDrive-by Download攻撃キャンペーンとしては、Seamlessと呼ばれるRIG Exploit KitとRamnitを用いた攻撃キャンペーンが知られていました。SeamlessはCisco Umbrellaによって報告され、Malwarebytesなど様々な研究者がレポートを公開してきました。弊社の小池もこれまでに2度SeamlessとRamnitについての調査レポートを公開しています。しかし、Seamlessは2018年3月末頃から観測報告が減少し、現在ではその活動は停止したのではないかと考えられています。

Seamless localized to Japan - www.nao-sec.org

Analyzing Ramnit used in Seamless campaign - www.nao-sec.org

そうしたSeamlessとは入れ違いに台頭し、日本を標的としている攻撃キャンペーン（我々は"PseudoGate"という名称で識別しています）を、弊社では2018年7月頃から観測しています。PseudoGateはRIG Exploit KitやGrandSoft Exploit Kitを用いてPanda BankerやKronosなどのBanking Trojanを送り込みます。それらのBanking Trojanは主に日本の金融機関のWebサイトを閲覧した際に悪性コードを挿入し、ユーザが入力した機密情報を窃取します。

今回はPseudoGateのトラフィックの全貌と、実行されるBanking Trojanについて行った調査・解析について紹介します。

<https://blog.activedefense.co.jp/2018/08/drive-by-downloadpseudogate.html> 3000PVぐらい

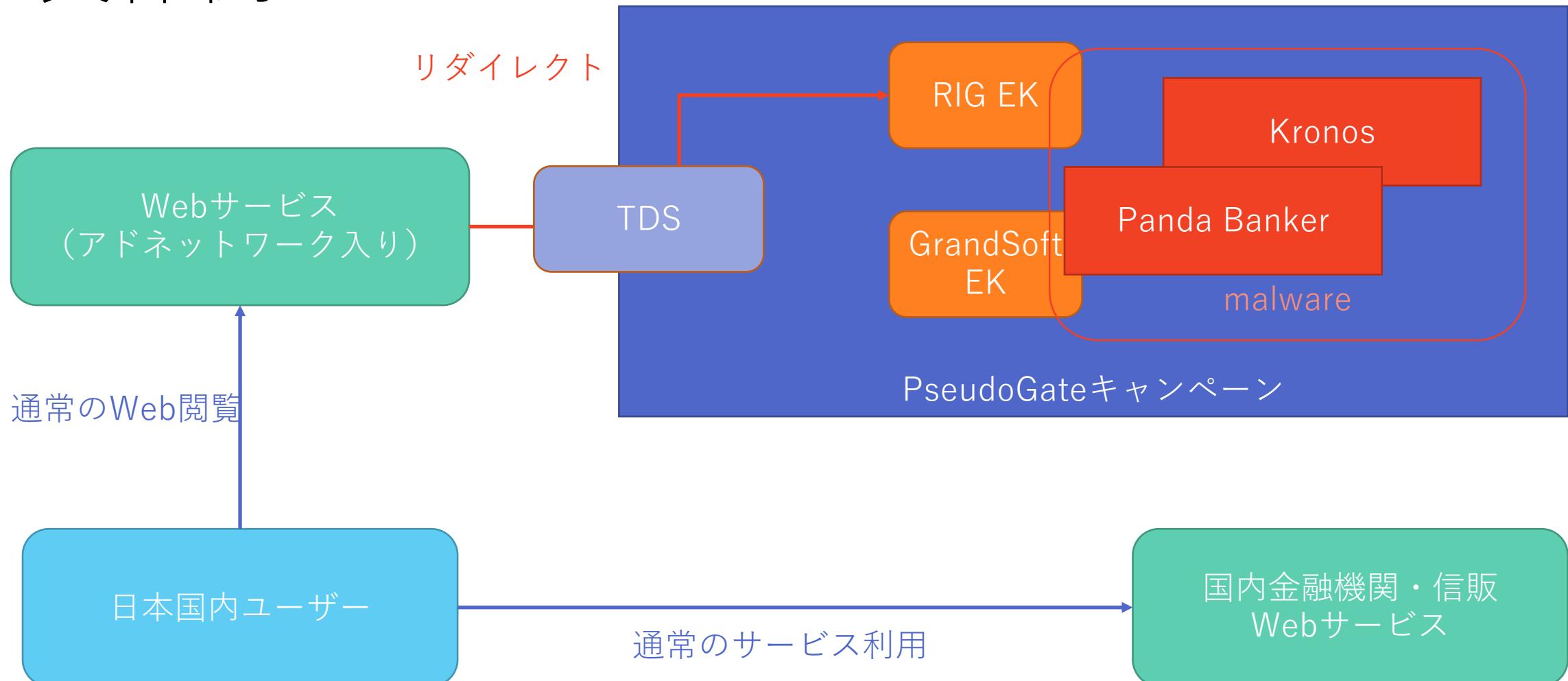
参加ユーザー

-  Keita Nomura
-  Rintaro Koike
-  Yuto Maeda
-  株式会社アクティ
所

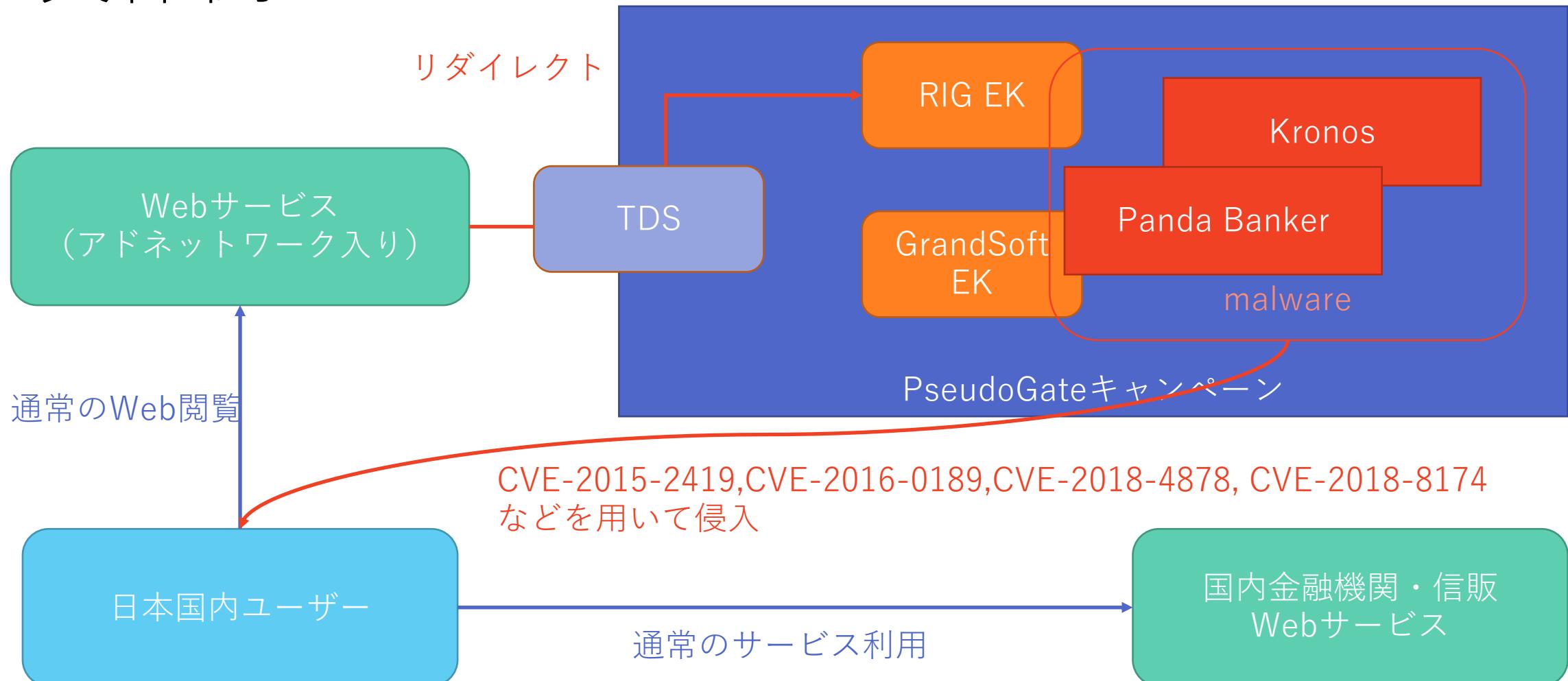
ブログ アーカイブ

- ▼ 2018 (3)
 - ▶ 9月 (1)
- ▼ 8月 (2)
 - 日本を標的としたDrive-by Download攻撃キャンペーンPseudoGate
 - Black Hat USA 201ト

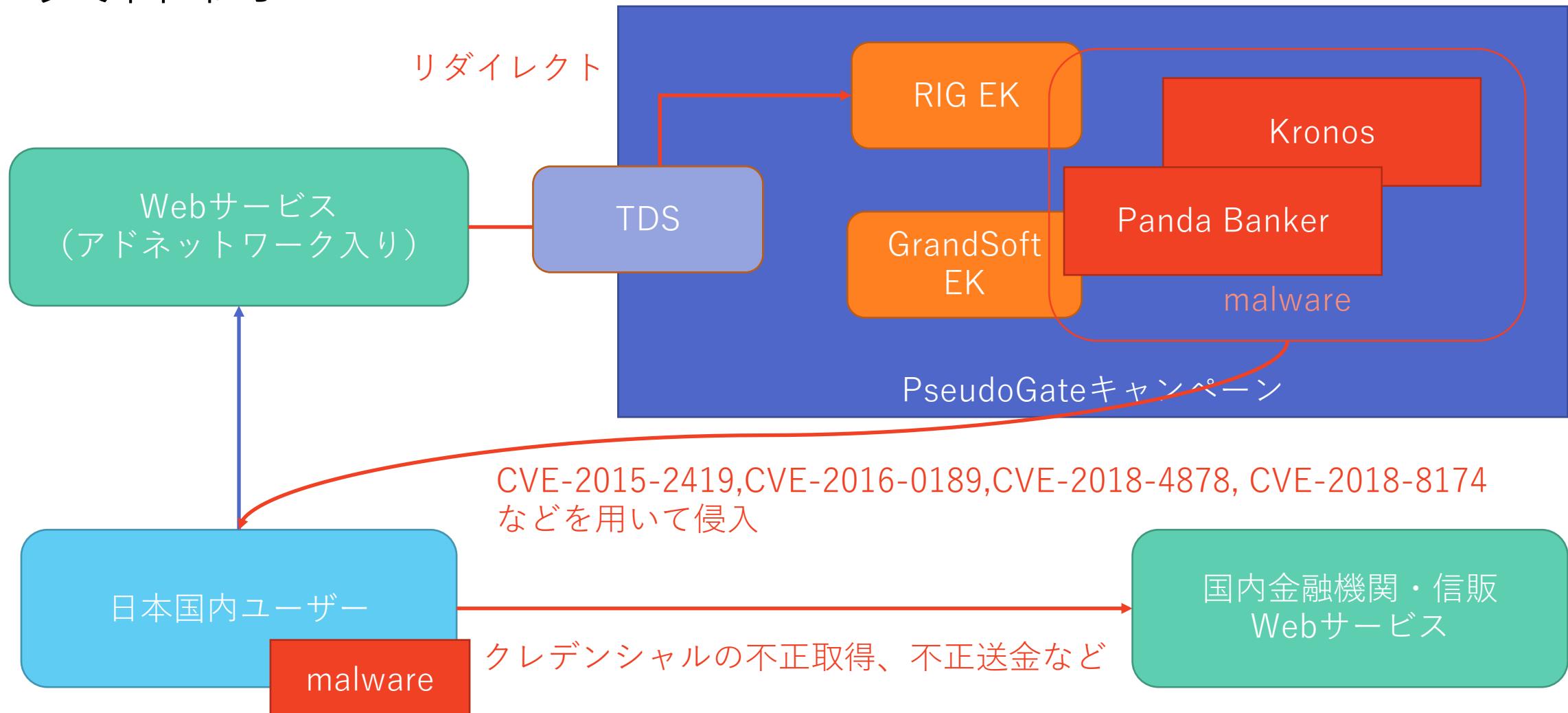
具体例：PseudoGate



具体例：PseudoGate



具体例：PseudoGate



AD-CTD提供内容

- サイバー攻撃観測情報配信サービスをJSONで提供中
 - MISPフィードについても将来的に対応予定
- ”踏めばマルウェアに感染するIndicator of Compromise(IoC)”を観測後即時に配信

```
{  
  "id": "20d398f9-5f49-4ac1-97a1-3bd6bc4165c9",  
  "type": "url",  
  "url": "http[:]//narrowlandscaping.semzo.info/getversoinpd/1/2/3/4",  
  "domain": "narrowlandscaping.semzo.info",  
  "ip": "95.46.114.197",  
  "description": "GrandSoft EK (Landing Page)",  
  "cve_numbers": [  
    "CVE-2018-8174"  
,  
    "confidence": "high",  
    "created_at": "2018-10-25 15:13:58",  
    "updated_at": "2018-10-25 15:13:58",  
    "expired_at": "2018-10-25 17:00:25"  
,  
},
```

配信内容の詳細

- “URL”
- “domain”
- “ip”
- “description”
 - 脅威の識別名が分かっている場合、例えば特定のExploit Kitである場合などはそれを配信
- “cve_numbers”
 - Exploit Kitが利用する脆弱性について、識別できている場合はそれを配信しています

現在（v2）での機能

1. 悪性広告→Exploit Kit→マルウェア感染の観測
 - malspamはほぼ完成、観測数の問題で未提供状態
2. Third-party sourceのマルウェア感染情報について、日本からの到達可否を再観測
 - ライセンスフリーの感染情報を情報源として利用
 - 国内経路でのDNSの問い合わせの結果と、到達可否を弊社内で確認したものをお配信

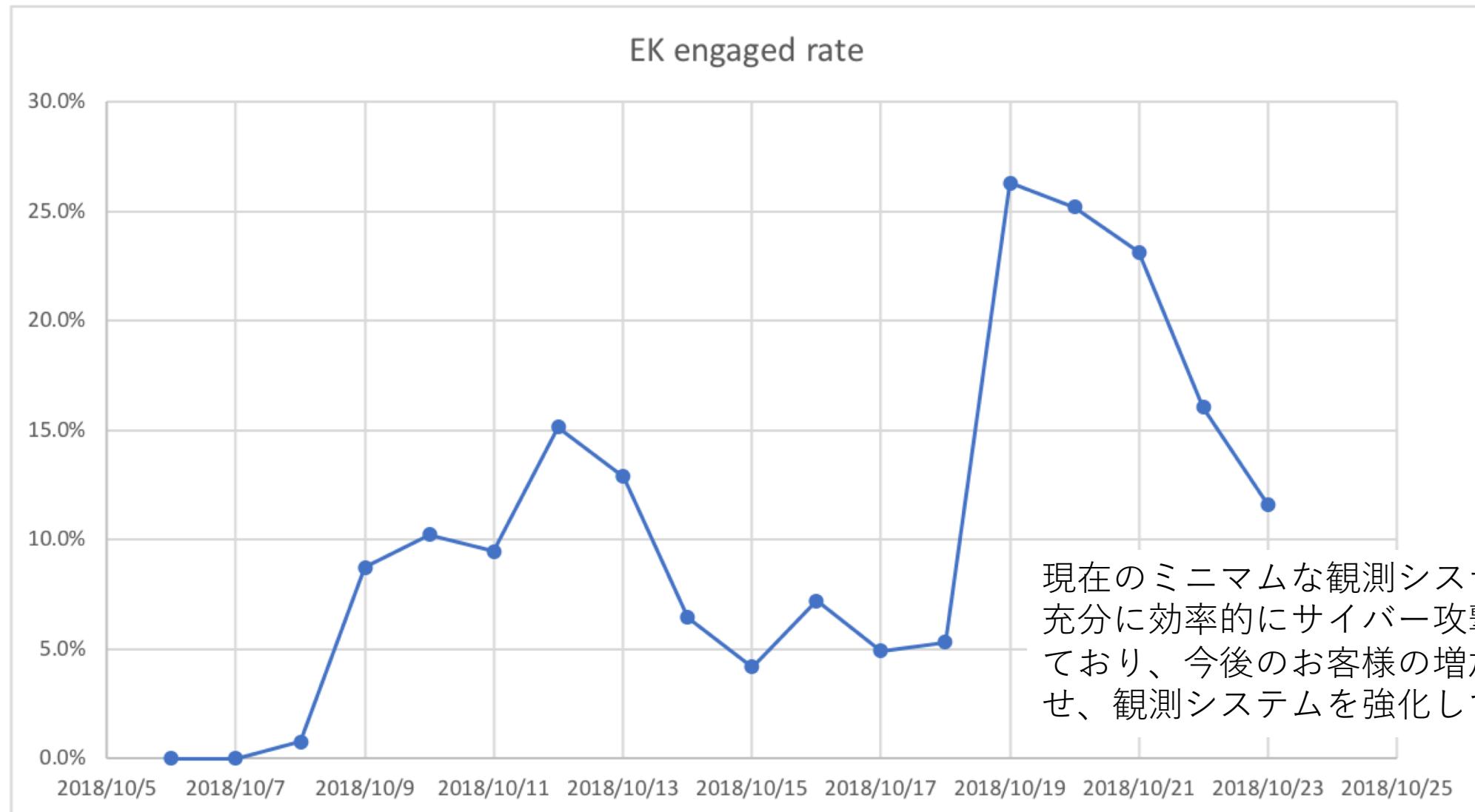
AD-CTDの強み

- 悪性広告を“踏みに行く”ためのURL収集、選定、クロール対象の決定について工夫しています
- Exploit Kitなどのマルウェア配信基盤にはセキュリティベンダーの攻撃観測を回避する仕組みがありますが、AD-CTDはそれを迂回
 - 例えば、クロールを行う出口IPは一時間に1度変更し再利用も行いません
- “踏みに行く”工夫と自動化により、とにかく“素早く”新しいIoCを観測・識別し、お客様にお届けします

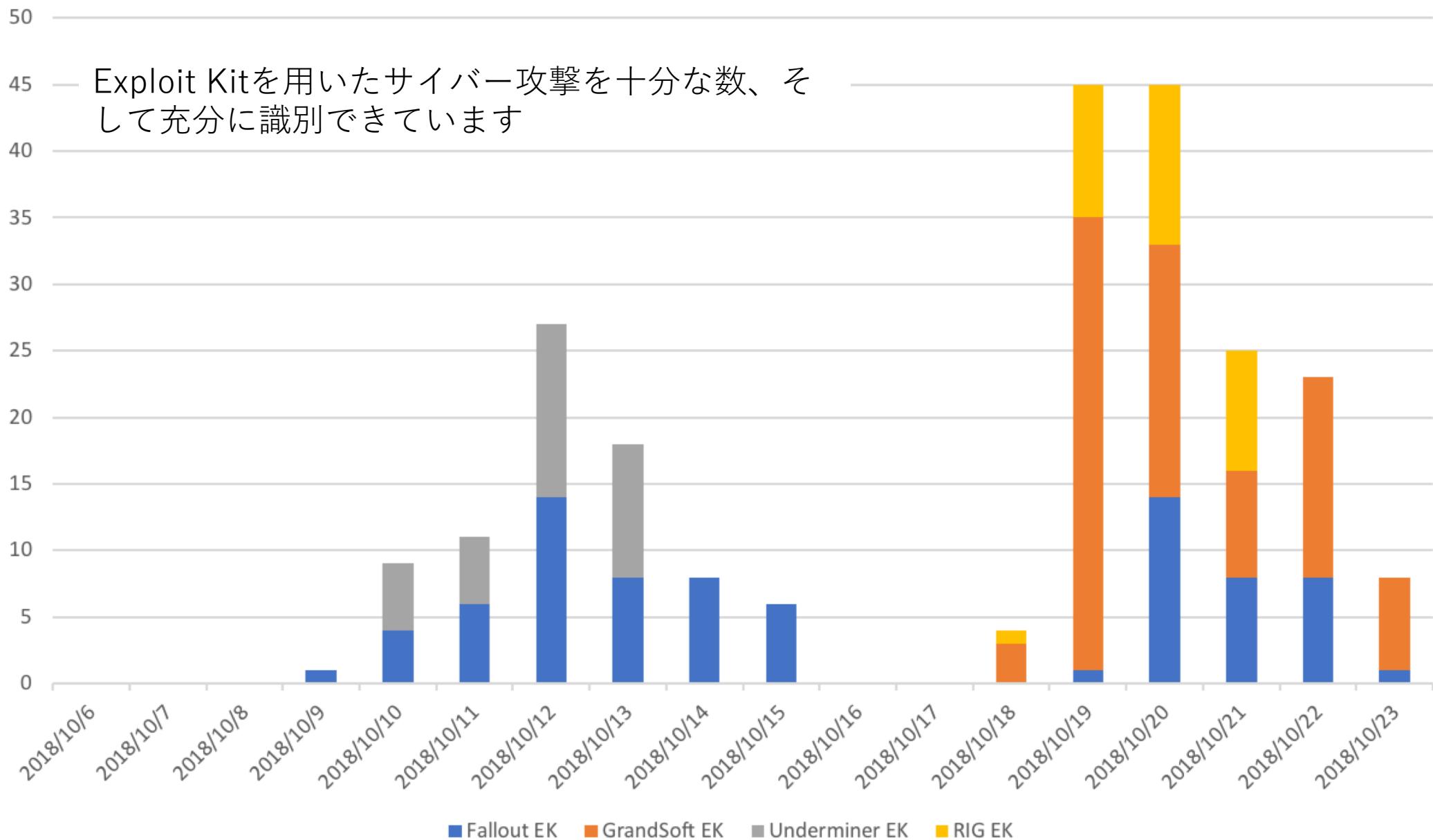
OSSの活用

- 弊社では自動的にサイバー攻撃を観測するシステムの一部にOSSを活用し、システム構築・運用しています
 - 繼続性の観点も含め、OSSへの貢献・開発協力にも積極的です

10/06-10/23の観測システムによるEK遭遇率



Observed EKs(2018/10/06-23)



サブスクリプションプラン

- **二次配信不可ライセンス (No redistribution License)**
 - 価格: 月額35万円 (税抜)
 - ご契約組織内及びご契約組織が利用するサービス・プロダクトでのご利用のみを許可
- **二次配信可能ライセンス (Redistribution License)**
 - 費用: ご相談
 - 制限無し
- **コミュニティライセンス (Community License)**
 - 費用: なし
 - 本サービスのサイバー攻撃識別機能で利用しているOSSのコントリビュータは、本サービスを1年間単位で無償でご利用可能です