



# 標的型攻撃に強いネットワークソリューション

葛生 晋一

公共システムズエンジニア  
シスコシステムズ合同会社

2014年 8月20日

# 学術機関をターゲットとした攻撃の実態

GhostShellと名乗るグループにより国内の複数の有名大学がサイバー攻撃を受け数千件を超える個人情報漏洩が発覚

- 漏洩した情報は本当に個人情報だけなのか？
- 最先端の学術機関として研究論文等の情報漏洩の可能性は？
- 少子化に伴う競争の中で学校の評判を下げないか？
- グローバル化を目指すに従い海外の学生や企業からみて評判を下げないか？

資産価値の高い  
情報資産

学術機関の  
ブランド

グローバル化

# はじめに

IPAの「標的型メール攻撃」対策に向けたシステム設計ガイドに加え必要と考える2つの追加対策についてご提案いたします

## 2つの追加対策

マルウェア感染に対する  
証跡機能



アプリケーションの認知  
とコントロール



「システム設定ガイド」で述べられている対策に加え今後必要性が増すであろう新しいセキュリティ対策についてご紹介いたします。

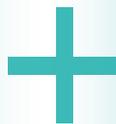
# システム設計ガイドに加え必要と考える追加対策

## 本日の実施テーマ概要

### 1

#### マルウェア感染に対する証跡機能

- マルウェアの脅威を100% 防ぐことができない現在、感染してしまうことを前提としてシステムのファイルI/Oに対する証跡機能が必要です。
- また、証跡のみではなく、ユーザーが既存知識で状況を把握できるための分かりやすい可視化のしくみを実装する必要があります。



### 2

#### アプリケーションの認知とコントロール

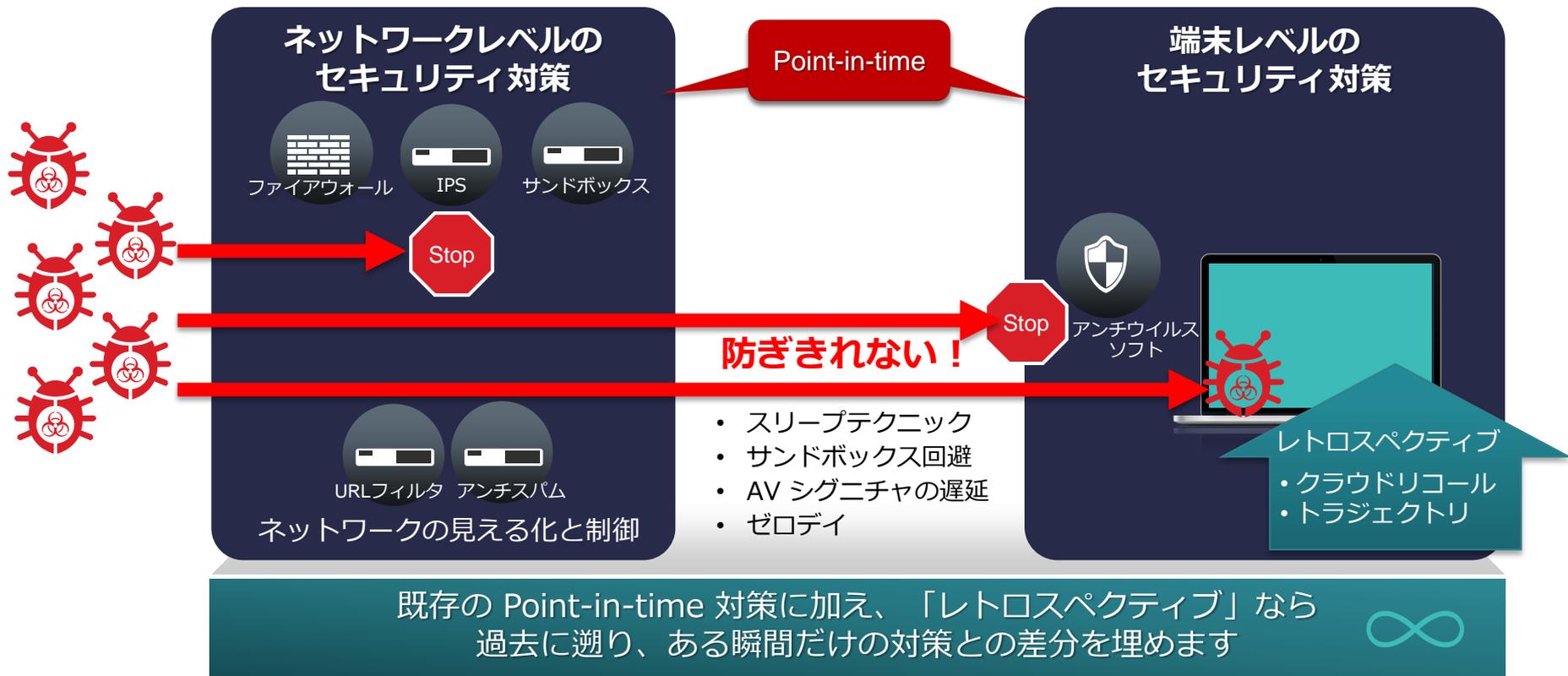
- 様々な脅威に対応するために、ネットワーク通信内容からアプリケーション、OSを判別することで、有効なセキュリティ対策を実装するための付加情報が必要です。

# 1. マルウェア感染に対する 証跡機能の必要性



# ある瞬間の対策だけでなく継続的な対策も必要

Point-in-time でのセキュリティ対策の限界



# マルウェアに感染した際の一般的な対応



マルウェアは日々  
巧妙化



通常、何らかの情報  
漏えいや不正通信の  
検知などで発覚



調査会社に依頼して  
も現状が把握できる  
のみ

どの情報が漏えいし  
たか、いつ感染した  
か、感染原因は何か、  
などは不明

また、社内の他の  
パソコンへの拡散  
情報も調査が必要



調査会社に依頼  
もしくは社内ITが担当

1台10万円程度の復旧  
費用（良心的な会社で  
あれば、調査費用に含  
まれるが、社内に1000  
台パソコンがある場合、  
すべてのパソコンの  
調査費用は単純計算で  
1億円）



感染原因を元に対策  
を実施。  
パッチ適用やバー  
ジョンアップ、不要  
なアプリケーション  
の削除など

# マルウェアに感染した際の実情



50%のマルウェアが  
すり抜けてしまう  
事をご存じですか

できるだけ早く  
パターンを提供する  
システムが必要です



IPS 等を導入して  
トラフィックの検査  
を行っていないければ、  
発覚はどんどん遅く  
なります



調査費用は、経費と  
してあらかじめ計上  
されていますか

自己消滅及びログの  
改ざんを行うマル  
ウェアがあることを  
ご存じですか



復旧費用が捻出できず、  
大事なファイルを消す  
ことになっていません  
か

もしくは、危険を承知  
で元のファイルを検査  
もせずに使っていて  
ませんか



OS を入れ直すだけ  
で、同じ脆弱性を  
突かれて、別なマル  
ウェアに再感染して  
いませんか

# アンチウイルスだけではダメ？

- アンチウイルスの得意な領域
  - 検体とまったく同一でないウイルスでも検知できる可能性がある(パターンファイル)
- アンチウイルスソフトはシグネイチャ(パターンファイル)モデルです。
- シグネイチャが作られていない新規のMalwareに対する対応

所要時間例

1. パターンファイルが生成
2. 組織内のシグネイチャ管理システムもしくは各PCがダウンロード } Hourly update
3. **新しいシグネイチャが各PCに入った状態でのフルスキャン** } Daily Full scan

リアルタイムスキャンは基本的に、新規に得たファイルなどに対応するため、潜伏期間を有するようなウイルスや、取得後にウイルスと判定されたマルウェアはフルスキャンが走るまではシグネイチャが存在するにもかかわらず検知できない可能性あり

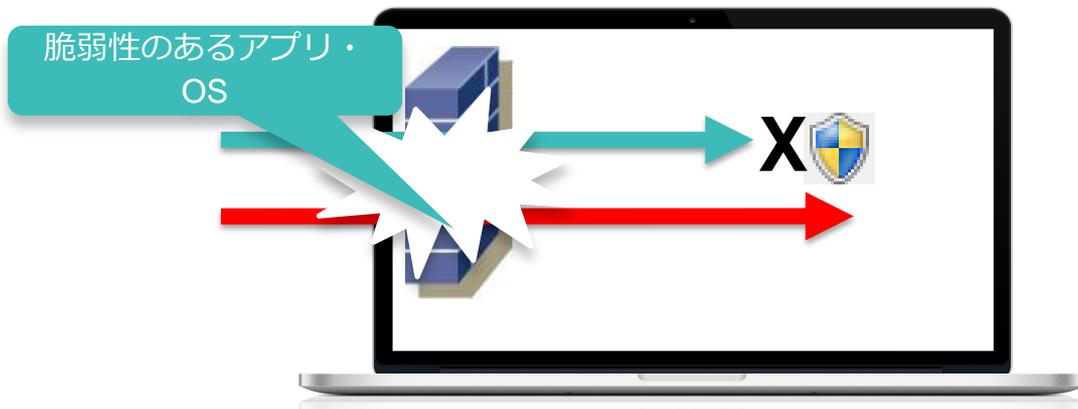


対応したパターンファイルも入っているのに  
駆除できていない状態があり得る

# アンチウイルスだけではダメ？

脆弱性を放置できるのはAVソフトがすべてのマルウェアを検知できる前提であれば可能です。しかし、全マルウェアを検知することは現実的には不可能です。

- アンチウイルスでは脆弱性は修復できません
  - ウィルスそのものを止めることを目的としているため、既存の脆弱性(穴)は残ったままとなり、新規のウィルスの侵入を許してしまう可能性がある
  - 脆弱性を埋めるためには別途脆弱性の元(Javaなど)がなんであるのかを特定する必要がある
  - ウィルスは毎回異なるものが侵入してくる可能性がある



脆弱性の残ったアプリやOSの入ったPC

脆弱性の原因を突き止め、アプリやOS側を修復をしないと空いた穴から新たなマルウェアがずっと来る状態。すべて個別にパターンファイルが必要

※アプリ、OS側で直接の修復が難しい場合はIPSでネットワーク側でBlock

# 調査、復旧、対策のために必要な証跡機能

## ▶ フォレンジック

- 専門性の高い技術
- コンピュータセキュリティ侵害に対して証跡などから専門技術者が原因を特定する

証跡収集

熟練解析者の技術

攻撃ポイントの補足、対応、対策

## ▶ レトロスペクティブ セキュリティ

- フォレンジックをより簡単に提供するシステム+α セキュリティ侵害に対して、予め収集されたログを可視化し誰にでも分かりやすく、原因を特定する
- 過去に遡って、マルウェアを発見する

トラジェクトリ

クラウド  
リコール

# マルウェア対策の今後

Point-in-Time のセキュリティ対策に加え、レトロスペクティブセキュリティを実現する AMP (Advanced Malware Protection)が必要になると考えます。  
特に端末側には、挙動の可視化を実現するトラジェクトリ機能が必須です。



# 前提 レトロスペクティブセキュリティの要、ハッシュ値とは

- ハッシュ値とは
    - あるデータ(ファイル)に対して、それを(電子的に)要約した値
    - 1bitでも異なる元データのファイルがあれば別のハッシュ値が得られる
    - 要約の手法によって、計算式が異なる。
      - 主要な方式 MD5やSHAなど
    - 例えばある250MBのファイルをMD5で処理すると要約した値として“BDFD5208312751B3C69B4660361A0654”が得られる。
  - ハッシュ値を使ってできること
    - どのサイズのファイルであっても一意に特定するIDとして使える
    - あるファイルがマルウェアのファイルと同一であるかを確認するにはハッシュ値を比較することで可能
- ※例 OSのダウンロードサイトにハッシュ値が記載してあり、ちゃんとダウンロードできたか確認できます

# レトロスペクティブ セキュリティとは？

AMP (Advanced Malware Protection) は、すり抜けてしまうマルウェアを時間を遡って検出し、感染原因を特定します。以下の2つの仕組みにより、マルウェアを隔離、可視化します。



## クラウドリコール

一度調査したファイルを覚えておき、合致するマルウェアが見つかった場合に瞬時にそのファイルを隔離する仕組み



## トラジェクトリ

すべてのファイルの挙動をあらかじめ記録しておき、マルウェア感染時もしくは、過去に通過してしまったマルウェアが見つかった場合に、どの脆弱性を元に感染したのか、どのようなルートで感染したのかを可視化する仕組み

# レトロスペクティブ：クラウドリコールとは？

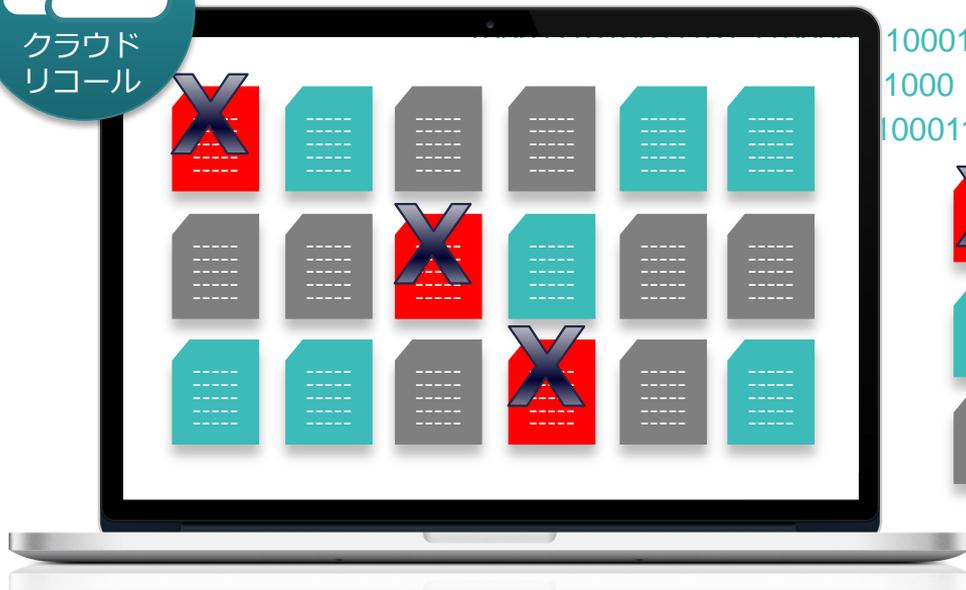


- クラウド内で管理されている情報に対してステータス変化があった場合に通知する機能です
- シスコの場合、リコール対象の判別はハッシュ値（SHA-256）を使用します
- どのサイズのファイルにおいても、一定長のハッシュ値に置き換えることで世界中に存在するすべてのファイルを一意に特定します
- このハッシュ値をクラウド上に記録することで、保存したタイミング（初めて調査したタイミング）ではマルウェアとして判定されなくても、後からマルウェアと判定されれば、リコールを行い隔離します

# ファイルのハッシュ値をクラウド上で記憶する



クラウド  
リコール



ハッシュ値

クラウド

10001110 1001 1101 1110011  
1000 0110 00 0111000 11101  
10001110 1001 1101 1110011 0110 0110 00



マルウェア→自動駆除



信頼できるベンダのファイル



現時点ではマルウェアでないファイル

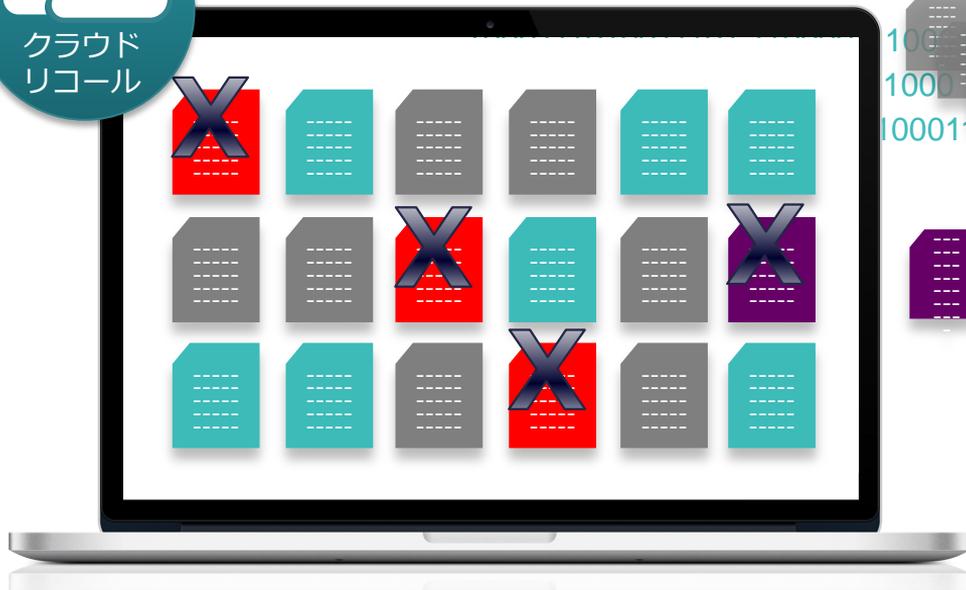
このファイルが将来マルウェアと  
判定される可能性がある

ファイルそのものではなくハッシュ値をクラウドで記憶

# ファイルを継続して調査する



クラウド  
リコール



20万件/日以上



ハッシュ値

クラウドビッグデータ解析  
(サンドボックス)



- 新しく見つかったマルウェアは、XXというファイル名で、YYのディレクトリに保存されているから、駆除

AVソフトと異なり、「マルウェアとメーカーにて判定された後のフルスキャン」を待たない**積極的**な駆除が可能！

継続的にデータを蓄積、調査し新たなマルウェアに対応

# 継続調査の結果、マルウェアを検知



The screenshot shows the Cisco FireAMP console interface. The main heading is "3706b205...b08480b4のネットワーク ファイル トラジェクトリ". The interface includes a navigation bar with tabs like "概要", "分析", "ポリシー", etc. A "Trajectory" section shows a timeline for two IP addresses: 10.0.0.1 and 10.1.0.1. A red box highlights the 17:29 event for 10.1.0.1, which is marked with a gear icon. A callout bubble points to this event with the text: "この例では17時間ほど前に既存セキュリティを抜けてしまったマルウェアを検知できています". Below the trajectory, there are sections for "Events" and "Dispositions". The "Events" table shows a transfer event at 00:39 and a retrospective event at 17:29.

時間	イベントタイプ	送信側IP	受信側IP	ファイル名	傾向	アクション	プロトコル	クライアント	ウェブアプ...	説明
2014-06-08 00:39:19	転送	10.0.0.1	10.1.0.1		Unkno...	Malware Cloud Loo...	HTTP	Internet Ex...	CNET	Retrospective Event, Sun Jun 8 08:...
2014-06-08 17:29:39	回顧的イベント				Malware					

# レトロスペクティブ：トラジェクトリとは？



- 直訳すると「軌跡」
- 操作等で使われる用語で、銃犯罪時の弾道を解析する行為
- シスコの場合、トラジェクトリの機能の要素となるデータとして、すべてのファイルの挙動を収集しています。
  - ファイルごとに、一意に決まるハッシュ値
  - どのファイルによって生成されたのか
  - どのファイルによって実行されたのか
  - どこへ通信したのか
  - どのホストに拡散しているか
- これらを可視化することで誰にでも分かりやすいレトロスペクティブ セキュリティを実現します。



## 2つのトラジェクトリ

- トラジェクトリのキーに何をを使うかによって2つの方法がある
- ファイルトラジェクトリ
  - 1ファイル(ハッシュ)に着目し、ネットワーク上どのように分散しているかなどを追跡します
- デバイストラジェクトリ
  - 1デバイスに着目し、そのデバイス内でどのようなファイルがどのような振る舞いをしているかを追跡します

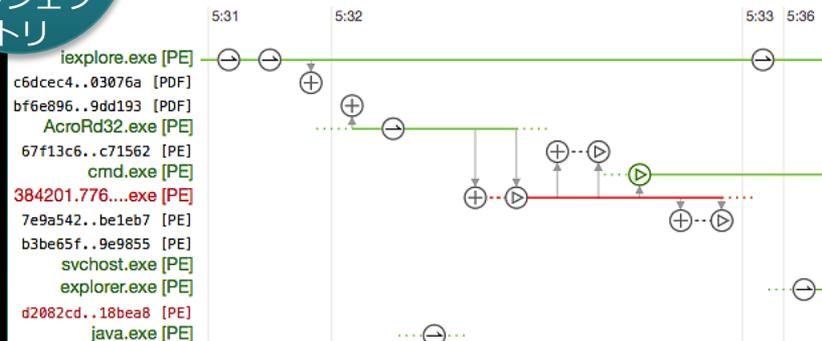
The screenshot shows a network management interface with a header bar containing the text '-1-PC updated policy with serial number 1073742805' and a 'Policy Update' button with a gear icon. Below the header, there is a table with columns for device names (e.g., '-1-PC') and icons representing file and device tracking. Two teal callout boxes are overlaid on the interface:

- A callout box on the left points to the file tracking icons and contains the text: **ファイルトラジェクトリ  
このファイルをキーとして  
データを表示させる**
- A callout box on the right points to the device tracking icons and contains the text: **デバイストラジェクトリ  
このデバイスをキーとして  
データを表示させる**

# マルウェア感染経路を可視化する：簡易画面



トラジェクトリ



## 色：3種類

赤：マルウェア

緑：正規のベンダーのファイル

黒：現時点ではマルウェアとは判定されていないファイル

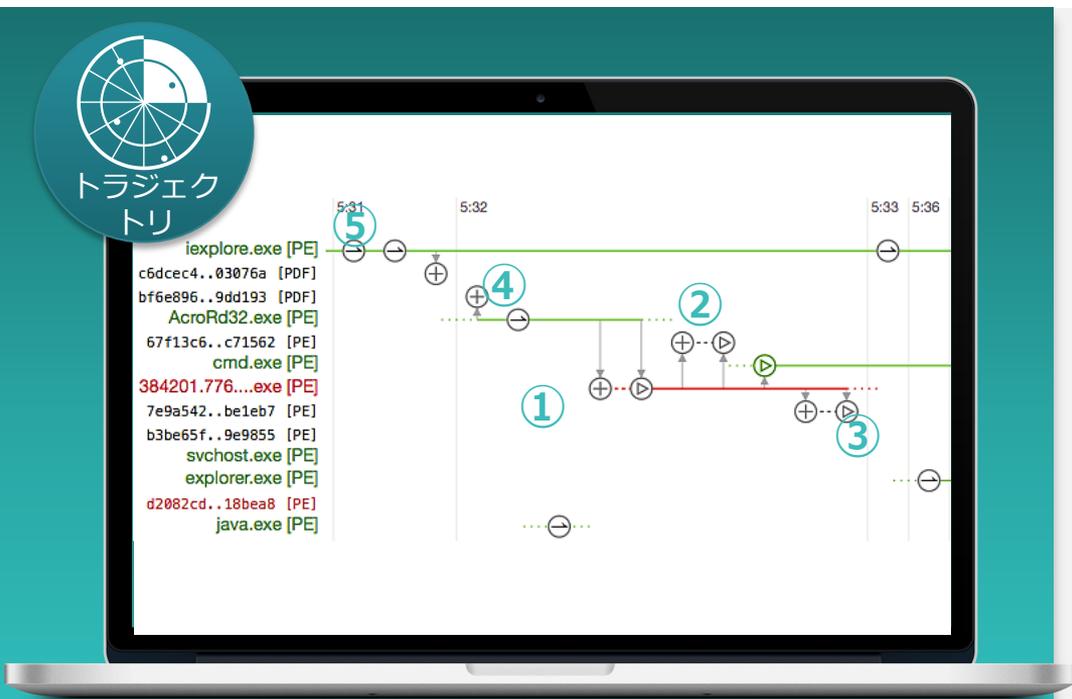
## アイコン：3種類

⊕ ファイルが作られた

▶ ファイルが実行された

◀ ファイルが通信をした

# 1. マルウェア感染経路を可視化する：時間軸で分かる



①

マルウェアが作られた

②③

マルウェアが何かファイルを作り出し実行した

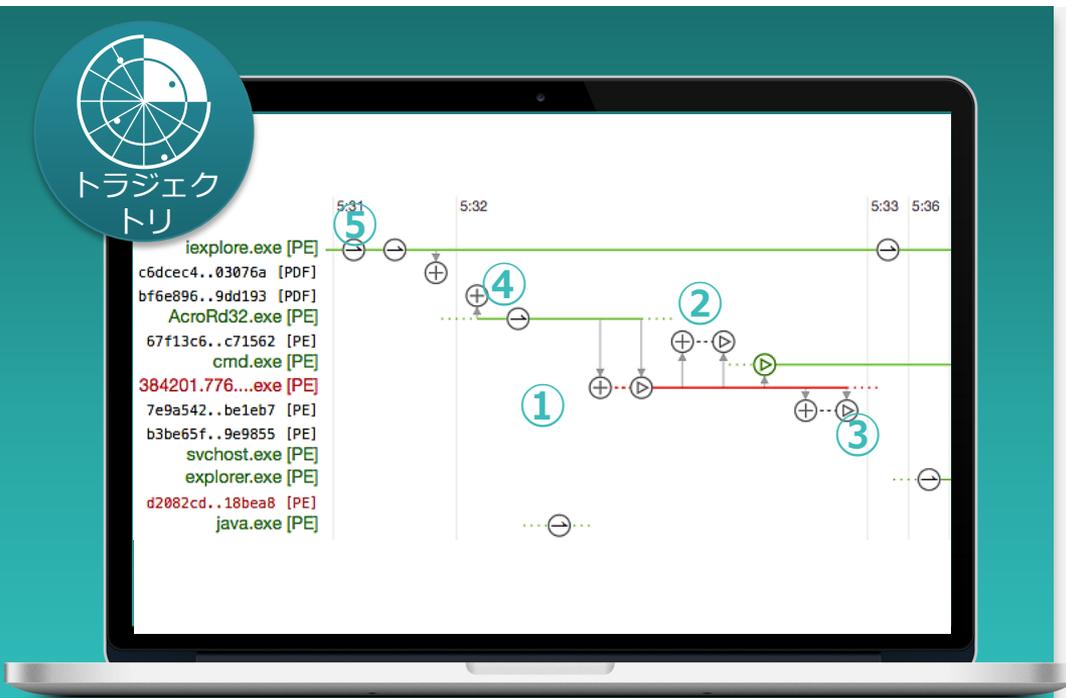
④

アクロバットリーダーが通信をした後マルウェアが作られ、さらにアクロバットリーダーがそのマルウェアを実行した

⑤

IEでどこかに通信した後PDFをダウンロードしてきた

## 2. マルウェア感染原因を推理する



- ユーザは何かの方法で悪意のあるサイトへ誘導され、PDF をダウンロードさせられた。
- このPDF にはアクロバットリーダーの脆弱性を突くコードが埋め込まれていたユーザは、そのPDF を開くことで、アクロバットリーダーの脆弱性を利用され、悪意のあるサイトに誘導され、マルウェアをダウンロードする。(感染)
- ダウンロードされたマルウェアもアクロバットリーダーに実行され起動

# 3. マルウェア感染への対策と駆除を実施する



同じハッシュ値を持つファイルを  
保有しているホスト一覧

- ②や③で作成された実行ファイルを削除
- ⑤で作成されたPDF を削除
- 可能であればURL フィルタなどで④⑤でアクセスした悪意のあるサイトをフィルタする
- アクロバットリーダーにパッチ適用（すぐに適用できない場合は、アクロバットリーダーを起動させない）
- マルウェアのハッシュ値から、内部の他のホストへの感染状況を把握し、同様の対応を行う

# Mini Hands-on

# まとめ

- 感染方法の特定
  - なぜ感染したかが分からなければ、同じ方法で感染する次のマルウェアを防げない
- 拡散状況の可視化
  - そのマルウェアがどこまで広がっているのかが分からなければ、対策ができない
- 瞬間ではなく継続した対応
  - 今だけのセキュリティ対策では防ぐことはできない脅威が増えている



Thank you.

