# 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。

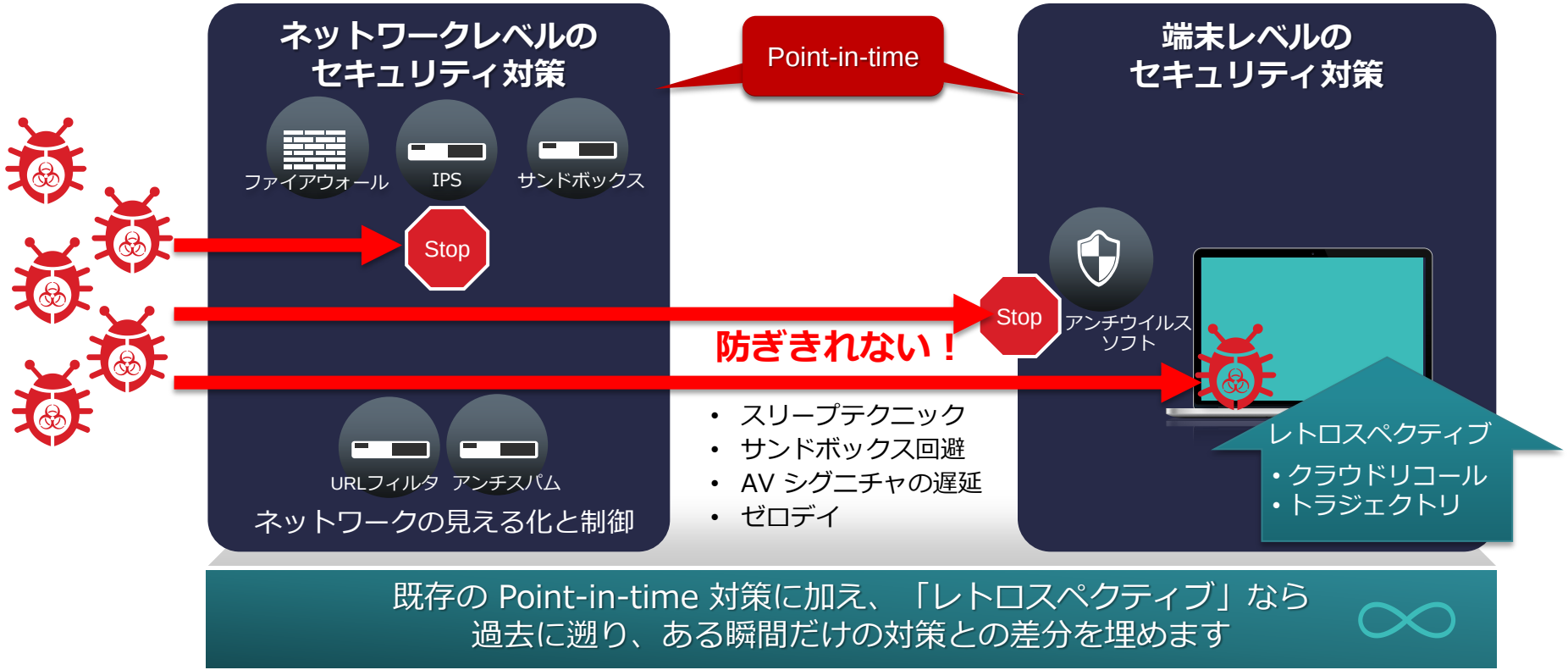

### 2
### アプリケーションの認知とコントロール

- 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い続けていませんか

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

# アンチウィルスだけではダメ？

- アンチウィルスの得意な領域
  - 検体とまったく同一でないウィルスでも検知できる可能性がある(パターンファイル)
- アンチウィ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

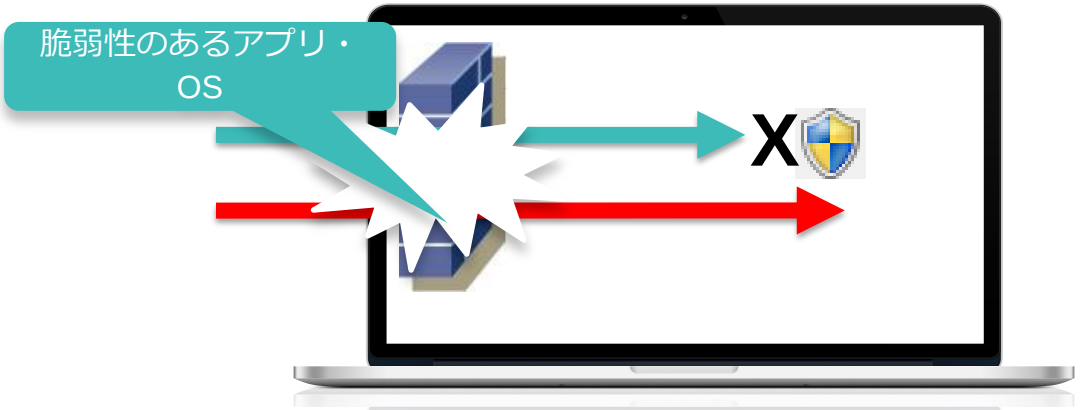
リアルタイムスキャンは基本的に、新規に得たファイルなどに対応するため、潜伏期間を有するようなウィルスや、取得後にウィルスと判定されたマルウェアはフルスキャンが走るまではシグネイチャが存在するにもかかわらず検知できない可能性あり

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

# アンチウィルスだけではダメ？

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。

- アンチウィ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り




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

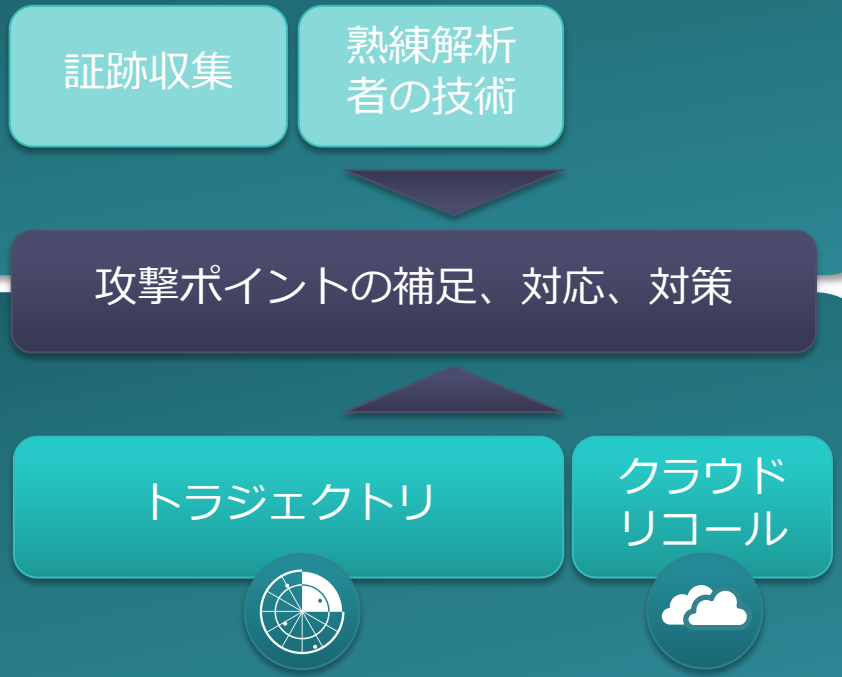
# 調査、復旧、対策のために必要な証跡機能

## 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

## 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



# 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。


AMP： Advanced Malware Protection

# 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



マルウェア→自動駆除

信頼できるベンダのファイル

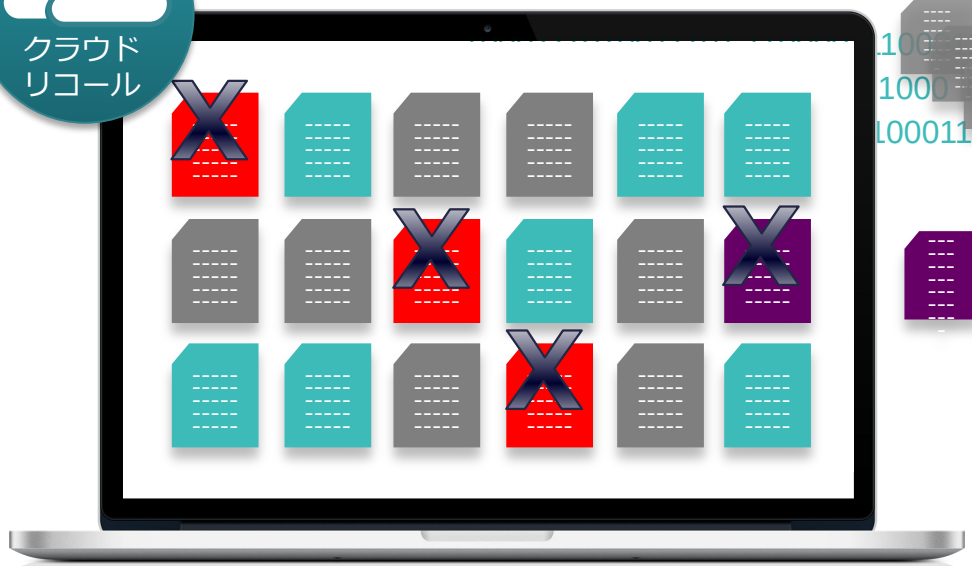
現時点ではマルウェアでないファイル

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

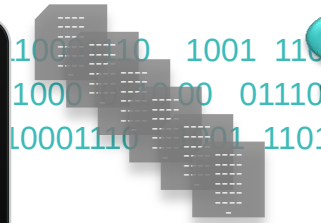
**ファイルそのものではなくハッシュ値をクラウドで記憶**

# 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）



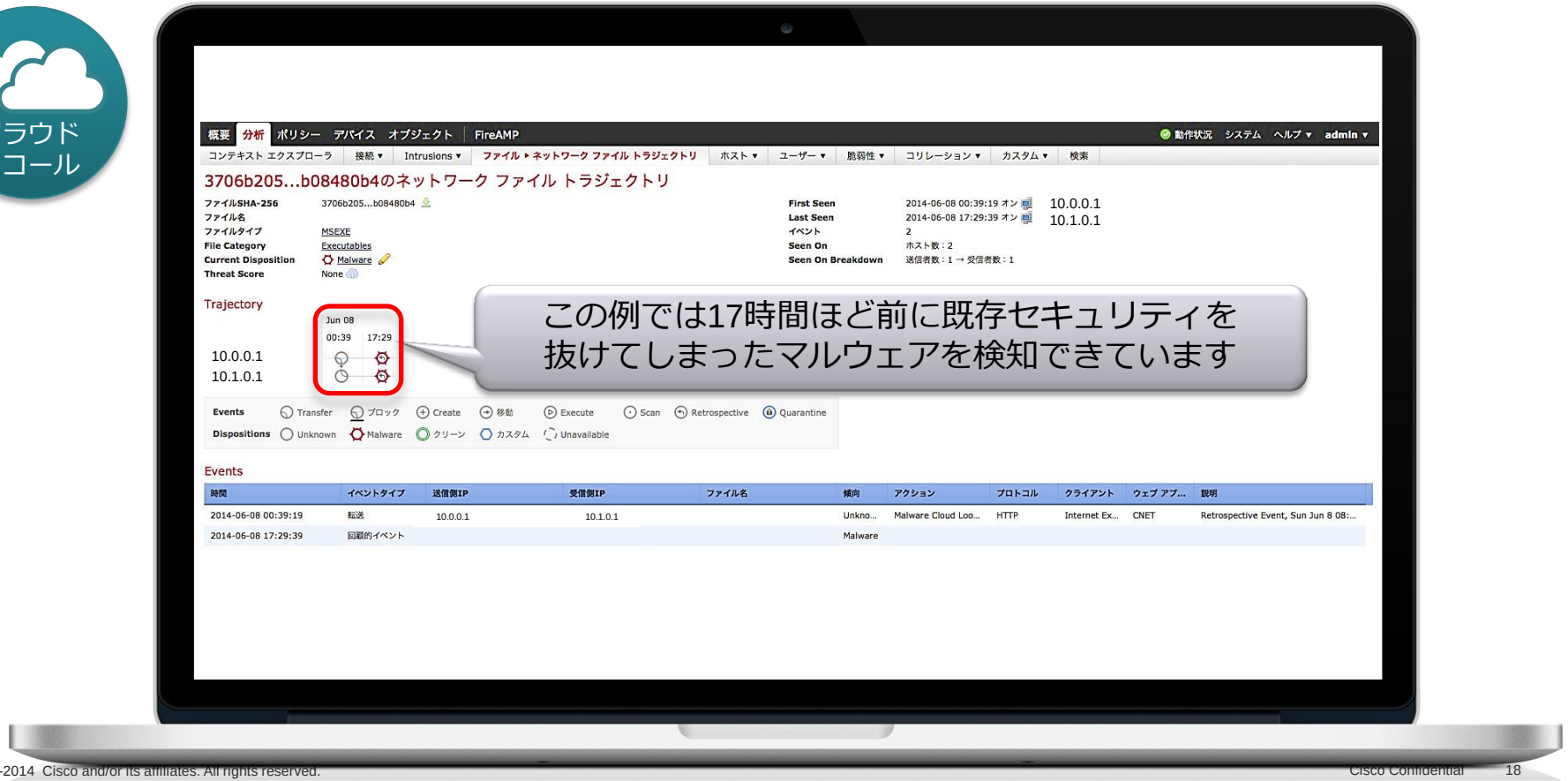
**！** 新しく見つかったマルウェアは、XXというファイル名で、YYのディレクトリに保存されているから、駆除

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！

**継続的してデータを蓄積、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

クラウド
リコール



# レトロスペクティブ：トラジェクトリとは？

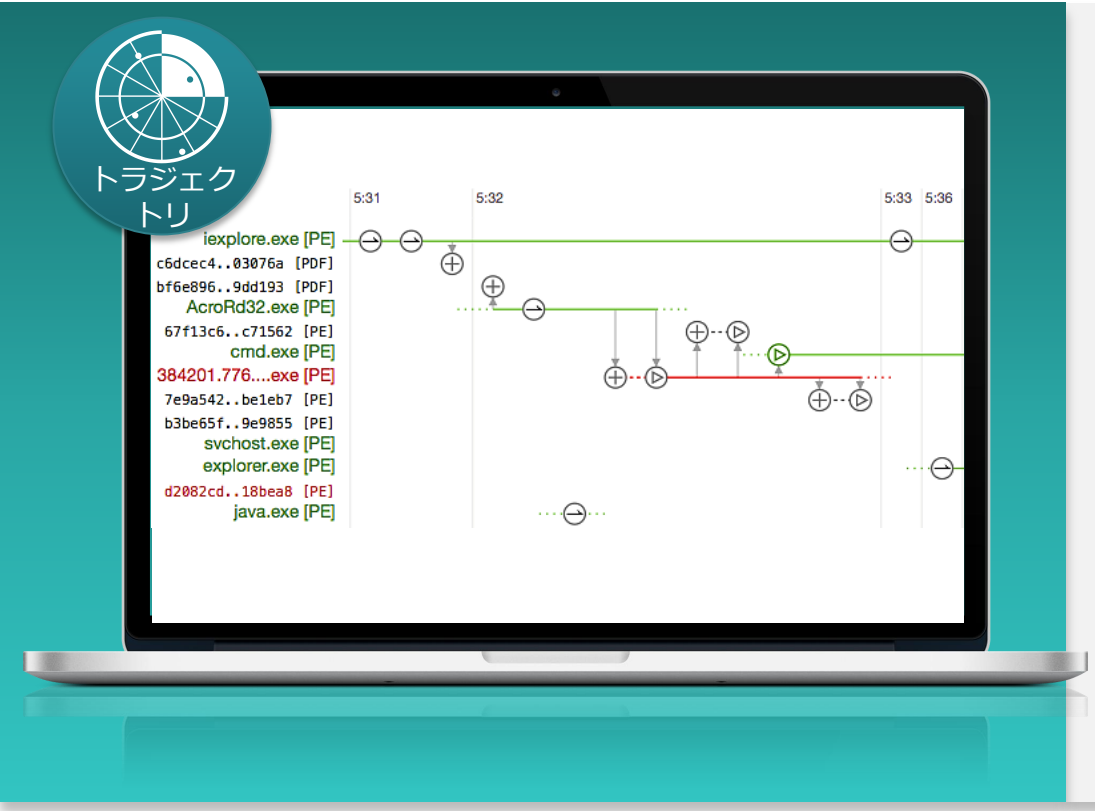
トラジェクトリ

- 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

# マルウェア感染経路を可視化する：簡易画面




**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

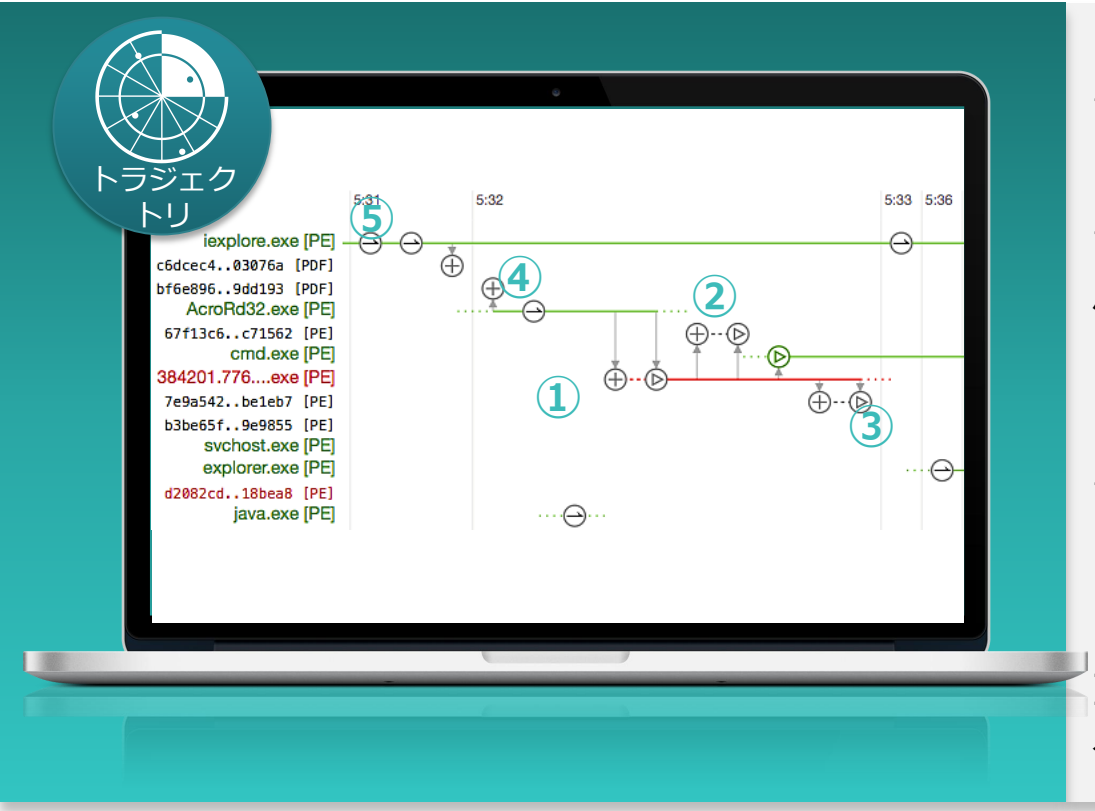
**アイコン：3種類**

⊕ 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

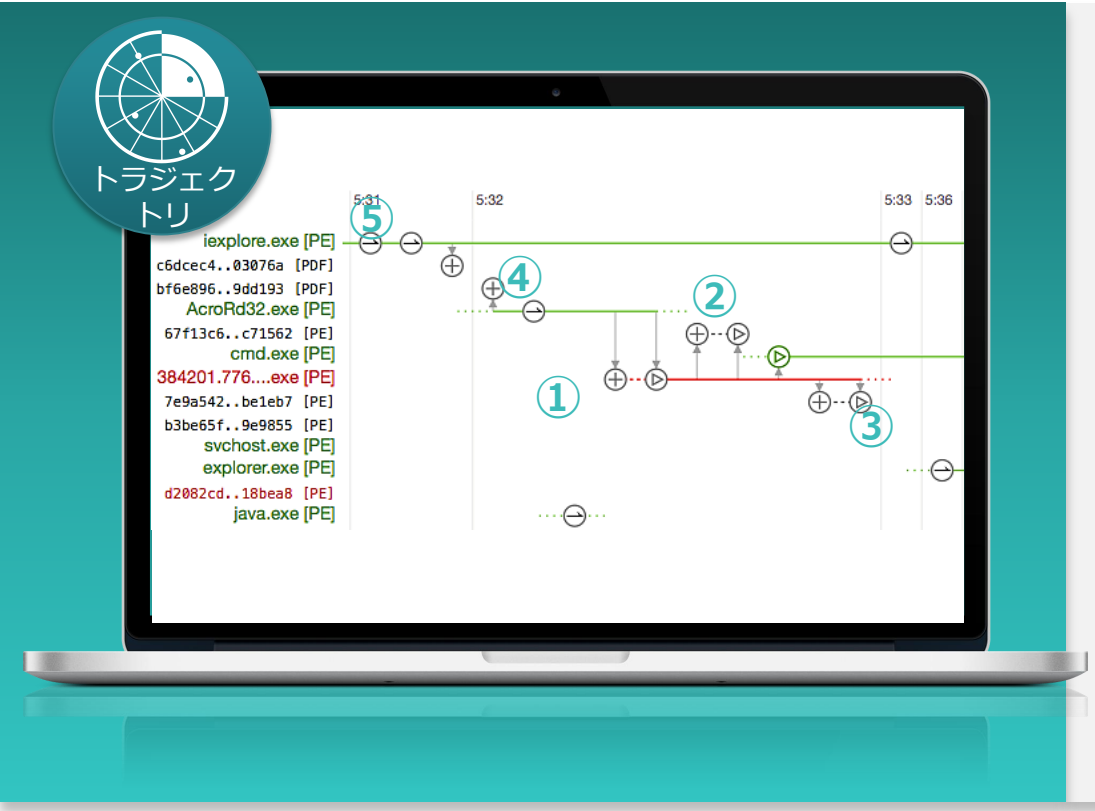
④

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


- 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.