サイバーセキュリティ対策フレームワークを支援するツール選定ポイント とは？

# サイバーセキュリティ対策ツールとトレンド

株式会社ソリトンシステムズ
エバンジェリスト　荒木粧子

※第1回より内容を追記・改訂しています。

# アジェンダ

1. 重要10項目を支援するツール
2. 対策検討のポイント
3. 賢い利用者であるために

※本セッションでは、技術的な課題や、フレームワーク構築を支援するツールの検討を話題にします。

# 1.重要10項目を支援するツール

# 重要10項目を支援するツール

| 分類 | 10項目 |
| --- | --- |
| ■基本方針 | （1）リスク認識とグランドデザイン |
| | （2）リスク管理体制 |
| ■管理の枠組み | （3）目標と計画策定 |
| | （4）PDCAの構築 |
| | （5）系列とパートナー |
| ■防ぐ対策 | （6）経営資源の確保 |
| | （7）外部委託対策 |
| | （8）社外コミュニケーション |
| ■有事の対処 | （9）対応体制 |
| | （10）開示と広報 |

※(9)対応体制にもツールが影響するため、第2回にて追記しています。

# 2.ツール選定のポイント

# サイバーセキュリティ対策ツール例

① 可視化・ポリシーチェック
② メールフィルタ
③ エンドポイントでのマルウェア対策
④ PC操作ログ（内部不正・サイバー攻撃）
⑤ インシデント対応支援やトレーニング

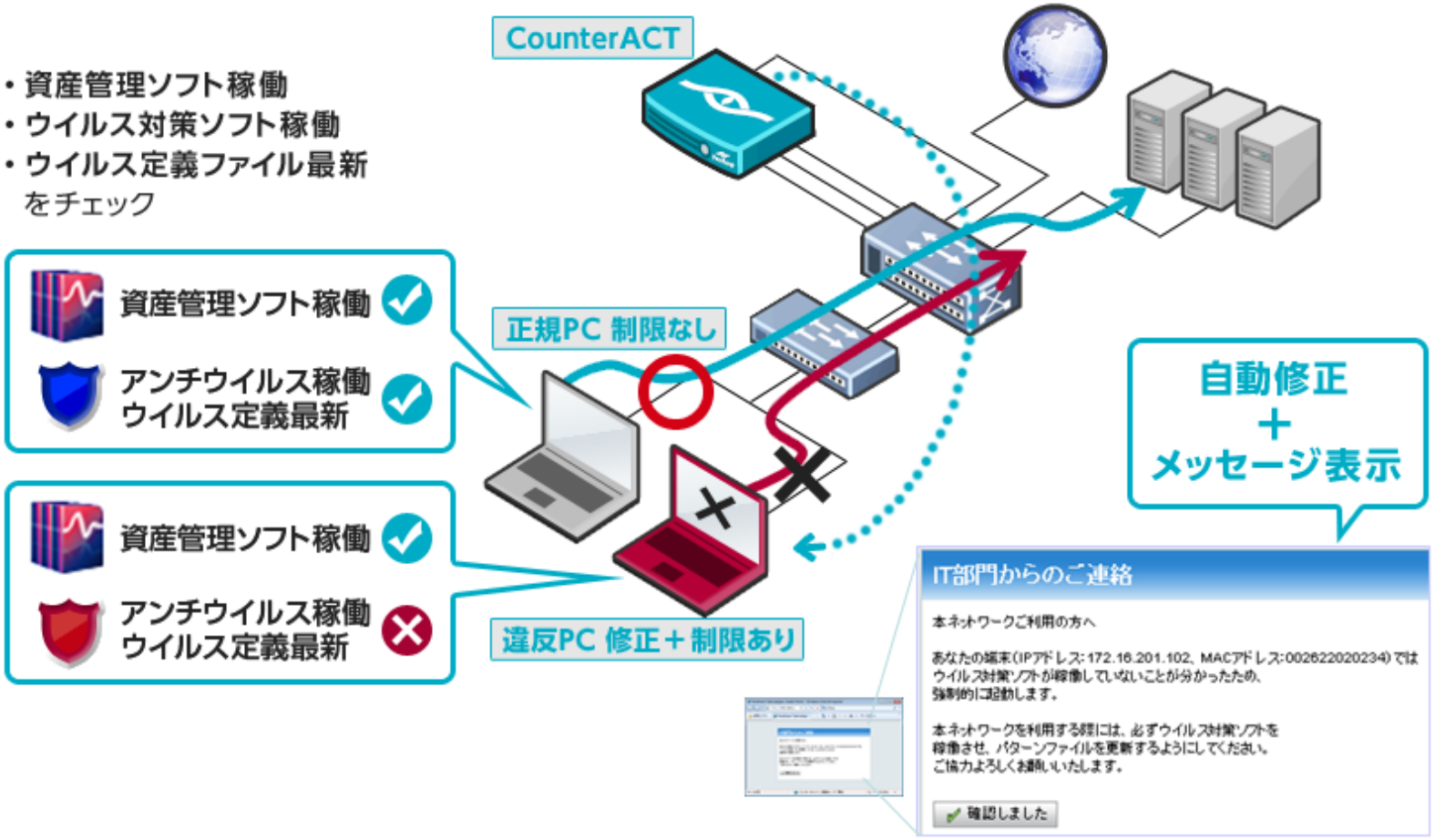
※あくまで一例であり、ガイドラインに記載されている対策のすべてを網羅しているわけではありません。

# ①可視化・ポリシーチェック

ForeScout **CounterACT**


- ■資産把握と構成管理
- ■エージェントレス（ドメイン管理端末）
  - ■エージェント（ドメイン管理外端末）もあり
- ■既存環境へのインパクト無い導入
  - ■ユーザーに知らせないバックグラウンドでの運用も可能
- ■ATD連携
  - ■FireEye、PaloAlto WildFire検知情報との連携

# ①可視化・ポリシーチェック
# - 端末の自動修正まで



# ②メールフィルタ

## Cisco ESA
## (Cisco Email Security Appliance)

- 怪しい送信元からのメールをフィルタ
- マルウェアメールをフィルタ
  - シグネチャ型
  - アウトブレークフィルタ
  - AMP（Advanced Malware Protection）
  - URLフィルタ
- 高パフォーマンス

# ②メールフィルタ
# - アウトブレイクフィルタ

**未知のパターン検知**
- 疑わしいexe.tif等のファイル

疑わしいメールを隔離

**5分後**
- 疑わしいexe.tifファイル
- サイズ50～55KB

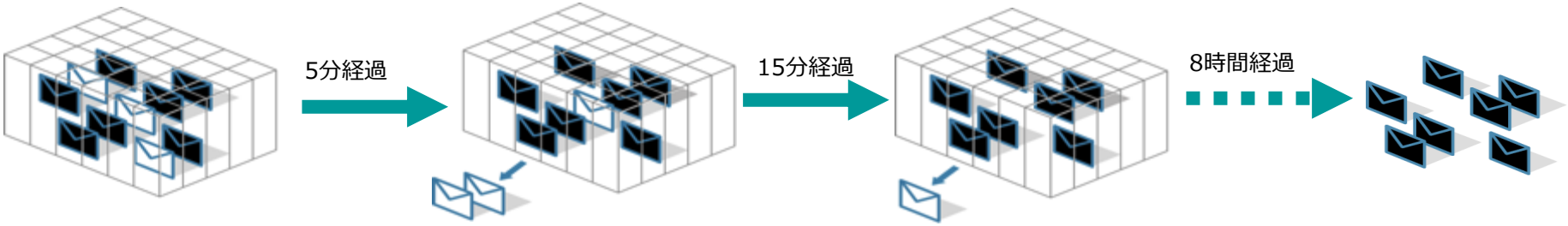
上記に該当しないメールはリリース

**15分後**
- 疑わしいexe.tifファイル
- サイズ50～55KB
- ファイル名に“Price”

上記に該当しないメールはリリース

**8時間後**

シグネチャ発行確認後
リリースし、対策シグネチャでマルウェア駆除




**マルウェアの危険にさらされる期間もアウトブレイクフィルタで保護**

新種マルウェア拡散開始

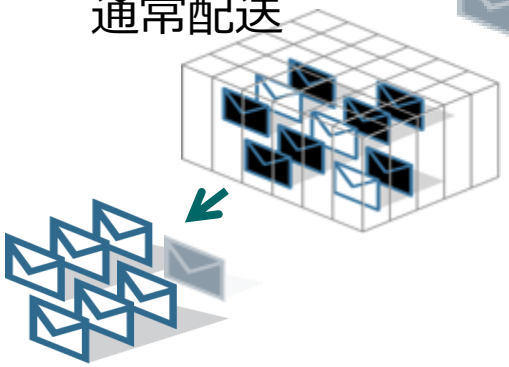
アンチウイルスベンダーにて
検体を入手し、マルウェアを解析
シグネチャを作成して配布

新種マルウェアの
シグネチャで駆除

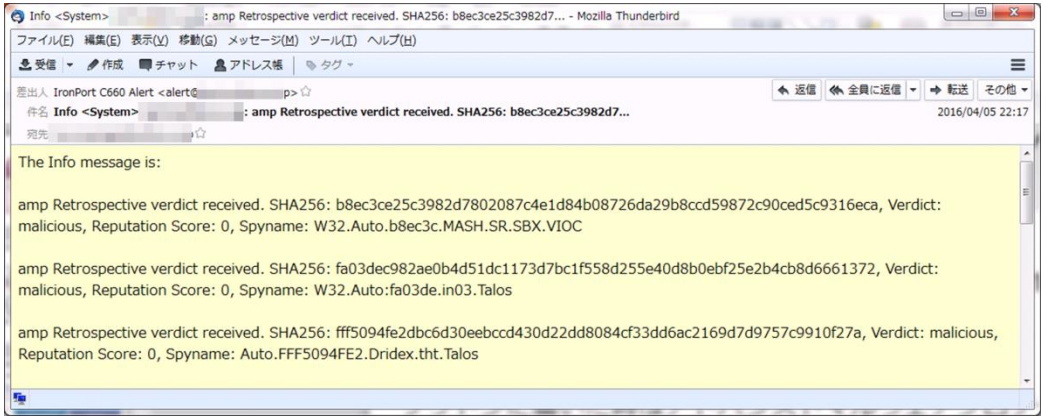
# ②メールフィルタ
# - AMPのレトロスペクション機能

Cisco Collective
Security Intelligence
TALOS

**メール受信時**
正常と判断され
通常配送

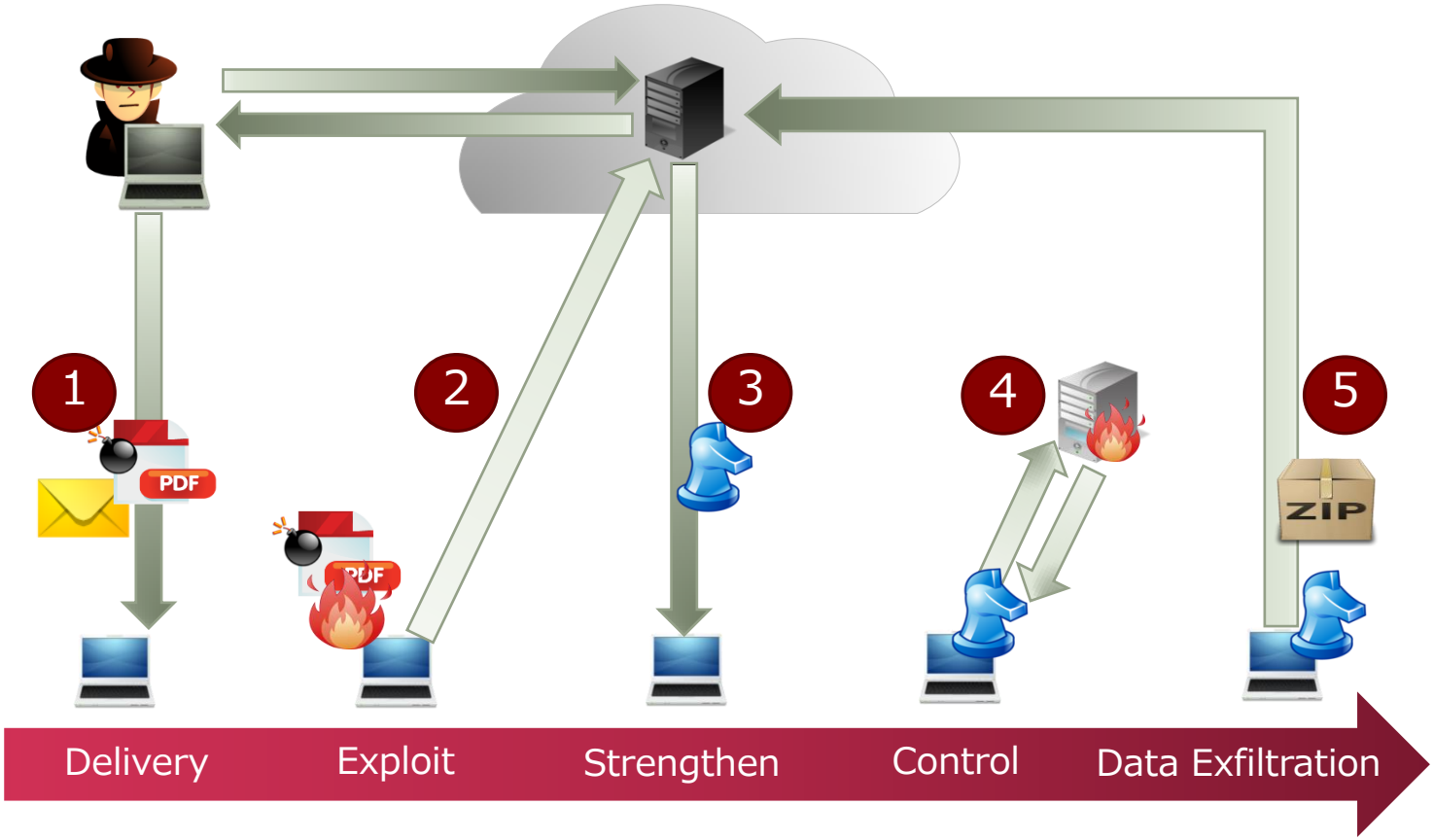


**その後**
配送済みメールが
マルウェア判断されると
管理者に通知



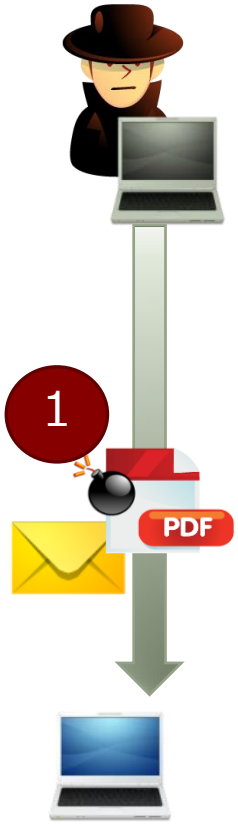

**のちに警戒レベルが上がった場合のフォローが可能**

# ③エンドポイントでのマルウェア対策
## - 攻撃シナリオから効率的な対応を検討




「（3）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定」における
「多層防御措置の実施 - マルウェア感染リスクの低減（マルウェア対策ソフトの導入） 」

# ③エンドポイントでのマルウェア対策
## - 2つの侵入の手口に対抗できるか？




■実行ファイル型マルウェア（従来型）

■パターンファイルが間に合わない
（例）VirusTotalでチェックして投下

➡ **パターンに依存しない検知方式が必要**

■データ型マルウェア（脆弱性攻撃）

■パッチが未だないゼロデイ攻撃には対応困難

➡ **パッチ適用では不十分、専用の対策が必要**

# ③エンドポイントでのマルウェア対策
## - マルウェア・脆弱性攻撃対策

Zerona


■エンドポイントにおける防御力UP

■パターン非依存で未知マルウェア検知・防御

■脆弱性攻撃からの防御

# ④PC操作ログ
## - フォレンジック対応のPC操作ログ

**InfoTrace® PLUS**


- ■サイバー攻撃・内部不正に
- ■独自ドライバによる
  カーネルレベルの操作ログ
- ■証拠隠滅を許さない各種保護技術
- ■外部デバイス制御も可能

# ⑤インシデント対応支援やトレーニング

- ゼロデイ攻撃初動支援サービス
  - 年間契約・チケット制でインシデント収束支援や内部不正対策支援を提供
    - Zeronaなどの防御策が不十分な場合、第三者の調査が必要な場合

- 技術トレーニング
  - 証拠保全と解析の基礎
  - メモリ・フォレンジック
  - データ復旧　など

詳細はWebサイトをご参照下さい： http://www.ji2.co.jp/

# ⑤ゼロデイ攻撃初動支援サービス

## ■デジタルフォレンジック技術を活用した年間契約の即応サービス

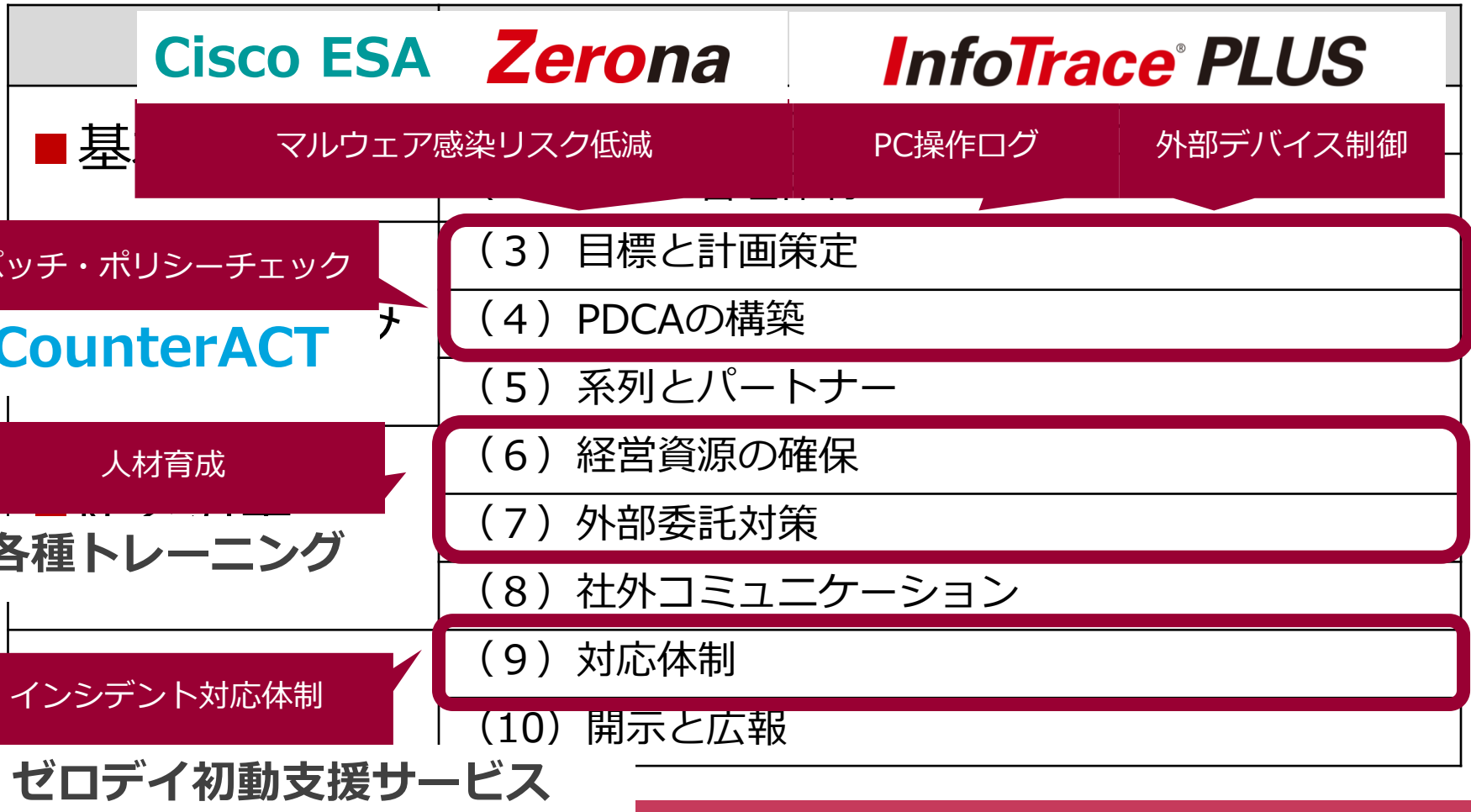
サイバー攻撃・内部不正インシデント発生時
フォレンジック技術を駆使して
マルウェア検体の特定や、拡散防止を支援
早期のインシデント収束・被害の最小化を実現


## このようにお悩みのお客様に最適！

- 脅威対策製品を導入したが不審PCの調査は専門家に依頼したい
- CSIRTを構築したが、初動対応について専門家のアドバイスが欲しい
- 内部不正のフォレンジック対応は専門家に依頼する体制にしたい

サービス詳細：http://www.ji2.co.jp/Service/zeroday/zeroday.html

# 重要10項目を支援するツール



# 3.賢い対策はあり得るか？