

GUIDANCE  
SOFTWARE  is now

**opentext™**

# フォレンジック技術で培った真のEDR ～「待ちかまえる」エンドポイント セキュリティ～

オープンテキスト株式会社  
代表取締役社長  
萩野 武志

**opentext™**

GUIDANCE SOFTWARE  is now

**opentext™**

# フォレンジック技術で培った真のEDR ～「待ちかまえる」エンドポイント セキュリティ～



Raymond Palmer  
APJエンタープライズ  
オープンテキスト株式会社

[rpalmer@opentext.com](mailto:rpalmer@opentext.com)  
+1-626-768-4683

**opentext™**

# 今日のアジェンダ

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

テーマ： サイバー攻撃を見破るヒント

1. 何がそんなに難しいのか
2. 経験則からみる3PC
  - a. Processes
  - b. Paths
  - c. Ports
  - d. Connections
3. まとめ：「受動的」から「能動的」なセキュリティへ
  - a. 守る以上に、「対応できる」が大切
  - b. 対処方法は、ある。

# OpenText = エンタープライズ情報マネジメント

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ



**EIM**

クラウド、オンプレ分野一位

**90%** フォーチュン1000 のお客様

**12,000** の従業員

**25** 年のイノベーション

# EnCase = 電子調査と情報セキュリティ

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

EnCase (エンケース)は、主に電子調査、脅威検出とレスポンス、データリスク管理に使われます。



EnCase Endpoint Investigator

全プロダクト共用、  
軽量エージェント



EnCase Mobile Investigator

統一エージェント数  
3800万



EnCase eDiscovery

フォレンジック技術  
をSecurityに応用



EnCase Endpoint Security



EnCase Risk Manager

業界スタンダードの  
研修と資格制度

# 攻撃を見破る:何がそんなに難しいのか

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

0. 「探せない」:「探せる」マルウェアは時代遅れ。

1. 「見えていない」

企業・組織アンケート回答

「**可視化**できていないコンポーネント」⇒

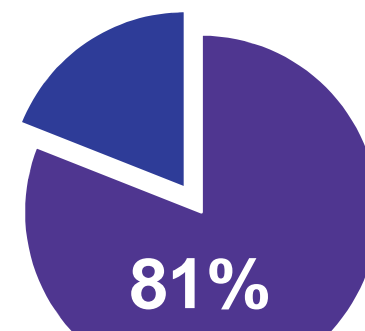
2. 「異常じゃない」

攻撃に使われる手法は、  
既存の「**普通の**」ツールを使う。

3. 「規則がない」

攻撃にルールなんてない。

頼れるのは「**経験**」と「**勘**」だけ。フォレンジックの経験は？



(機器の)異常な動き  
が見えない。

Sans Survey, 2016

# Exhibit a: Processes

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

注目:

一見「異常なし」のプロセスに不審な点がないか？

シナリオ 1. 「プロセスを呼ぶ」

呼ぶプロセスがどんなものか、見てみる。

そのプロセスは、通常呼ぶものか？

シナリオ 2. 「パラメータがある」

そのプロセスは、通常パラメータを使うか？

使うパラメータは、一般的か？

シナリオ 3. 「なんだか癩に障る」

その他、不審な点はありませんか？

# Exhibit b: Paths

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

**注目:**

一見ただのパス。そのパス、「普通」ですか？

**シナリオ 1. 「インストールパスが、変」**  
インストールするパスを試してみる。  
そのパスは、**一般によく見られるものか？**

**シナリオ 2. 「プロセスの開始パスが、変」**  
そのプロセスは、**通常そこから**開始されますか？



# Exhibit c: Ports

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

**注目:**

「これ」に「この」ポート...気づく点は、ありませんか？

**シナリオ 1. 「ポート番号が、高い」**

ポートは、あるものから使っていく。

**5桁のポート**が使われるシチュエーションは？

**シナリオ 2. 「ポートの使い方が、変」**

ポートによっては、「一般に内部接続に使う」ものと、  
「外部接続にも使う」ものなど、パターンがある。

変な**ポートの使い方**をしているプロセスは？

# Exhibit d: Connections

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

**注目:**

コネクションをチェック。「一般的でない」場所への接続は？

**シナリオ 1. 「一般的ではない場所からの接続」**

普通はアクセスしない**地理的位置**からのDNS接続？

すでに「怪しい」**フラグ**が立っているところからの接続？

**シナリオ 2. 「外に接続しようとする」**

外部へ接続しようとしているプロセスは、怪しい。

リスニングのためのコネクションも、怪しい。

**でも、「一般的に」**使うときには使うものでもある...

# 対処1: まず「見る」 360° 可視化

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

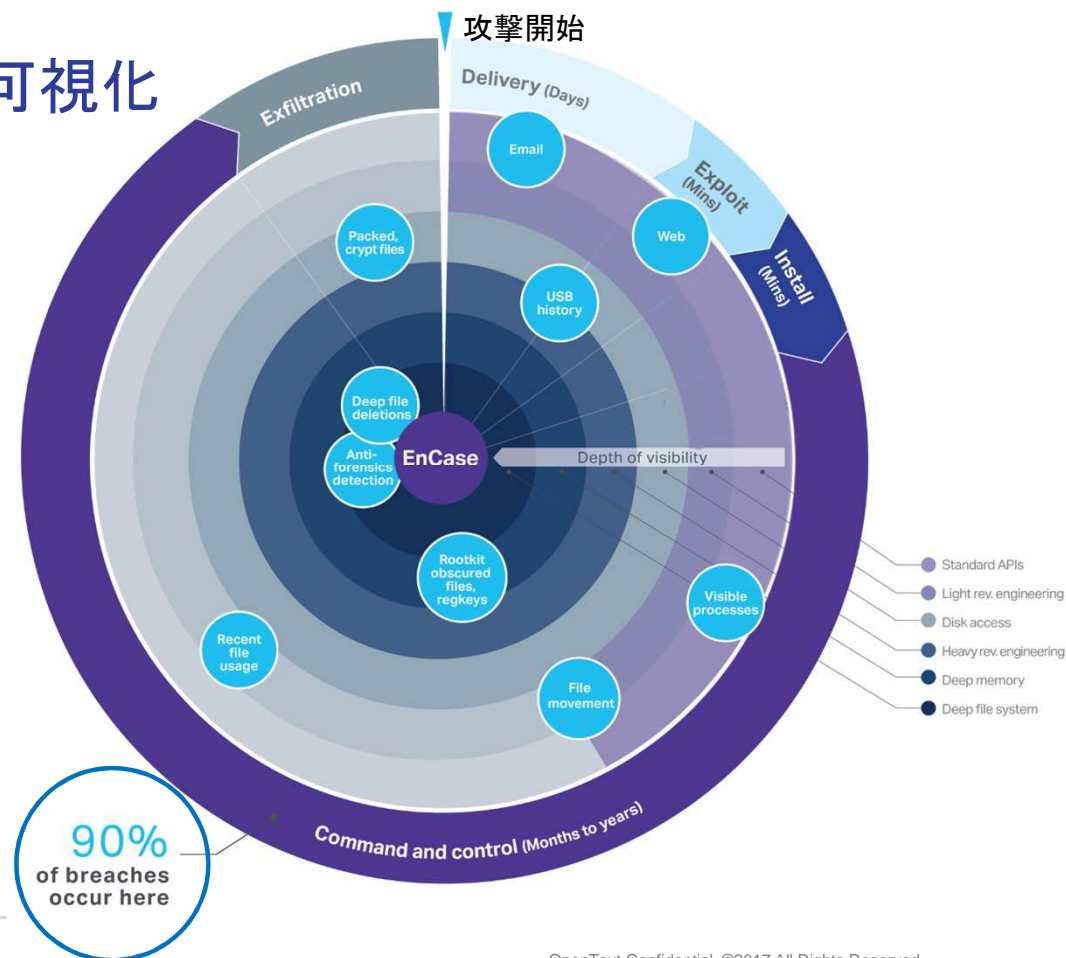
対処方法

まとめ

= カーネル層データの可視化

(ということは)

- サイバー攻撃の全ての段階で痕跡を取得できる。
- カムフラージュを見破れる。
- エンドポイントの状態を正確に把握できる。
- 検知漏れを発見できる。



# 対処2: 攻撃に立ち向かう準備をする

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

ツールは、ある。

膨大な量のフォレンジックデータを比較分析できるツールはリリースされている。

今すぐ: 「Protection」ではなく「Incident Response」を用意する。  
ブリーチされることを前提に組み立てたディフェンスは、  
それだけ強い。

そのうち: 「Responder」を育成する。  
「対応能力」をも包含したプランを。  
経験は、すぐには買えない。

# 例：3PCのProcessを整理

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

3PCのC

対処方法

まとめ

EnCase® Endpoint Security

INVESTIGATION

PROCESSES (554)

Process 'chrome.exe'

子・孫プロセスとそのかけら

explorer.exe

- CodeMeterCC.exe
- TSVNCache.exe
- tabstray.exe
- cmd.exe
- notepad.exe
- Q-Dir.exe
- B.exe
- devenv.exe
- Tree.exe
- chrome.exe
- firefox.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe
- chrome.exe

SUMMARY	DLLS	CONNECTIONS
NAME	chrome.exe	
PID	9432	
PATH	C:\Program Files (x86)\Google\...	
HASH	EC820250BBF2AC99B27DD3A...	
THREAT SCORE	-3	
PARAMETERS	"C:\Program Files (x86)\Googl...	
HIDDEN	No	
CHILD PROCESSES	0	
DLLS	48	
CONNECTIONS	0	

Inv-01 with 1 snapshot

STATE: Opened 5 days ago

ASSIGNED TO: RD\john.doe

HASH DETECTIONS: 6

IP DETECTIONS: 3

DOMAIN NAME DETECTIONS: 1

History

Remediate RD\james.jameson 5 hours ago

Event(s) RD\john.doe 2 days ago

Event(s) RD\john.doe 2 days ago

Snapshot RD\john.doe 2 days ago

Snapshot RD\john.doe 5 days ago

Created RD\john.doe 5 days ago

アンインストール、OSレベルで削除しても、コードやデータが隠れている

# まとめ:「怪しい」を見破るツールと経験を、今から。

はじめに

OpenText と EnCase

前提と現状整理

3PCのP

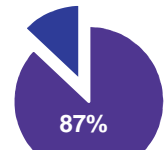
3PCのC

対処方法

まとめ



第一の問題「見えない」を突破するフォレンジック



カーネル層のデータ

「異常な」ものを早期発見できるツールはある。

**EDR**  
で対処

ブリーチされることを前提に、「対処」まで進んだ  
ディフェンス構築と育成開始。

**opentext™**

Thank you



[sales-jp@opentext.com](mailto:sales-jp@opentext.com)



[twitter.com/OpenTextJapan](https://twitter.com/OpenTextJapan)



[linkedin.com/company/opentext](https://linkedin.com/company/opentext)