

# Today's Agenda

- 自己紹介、法人紹介
- Fast Forensics (ファスト・フォレンジック)の定義、現状
- 次のステップに向けて
- ・まとめ





# Corporate Profile

**Corporate name: Ernst & Young** 

**Established year: 1989** 

**Headquarters: London** 

Global Chairman/CEO: Mark A. Weinberger

Service Line: Assurance | Tax | Transactions | Advisory









# **EY Cyber Forensics**

Services

Skills

# Scenarios where FIS are engaged

Cyber Breach Response Management Cyber Crime and Fraud Investigations

Digital Investigations and Forensics

Cybercrime Intelligence and Threat Assessment

Log Identification & Analysis

Host based malware and attack analysis

Network attack forensics

Cyber Crime and Fraud Investigation

Digital Forensic Analysis

Cyber breach litigation and disputes support

Intelligence assessment and analysis

Breach impact assessment

Law enforcement, security and regulatory liaison

Board-level cyber breach response

Conducting forensically sound technical investigations into a damaging cyber-attack – including collection and analysis of evidence

Collecting digital forensic evidence to criminal litigation standards

Providing digital and cyber forensic expert witness services

Preservation, collection, transformation and integrated analysis of multiple forms of data (e.g. financial, email, audio, chat). Supporting commercial disputes with customers and supply chain relating to losses or damages from cyber-breaches

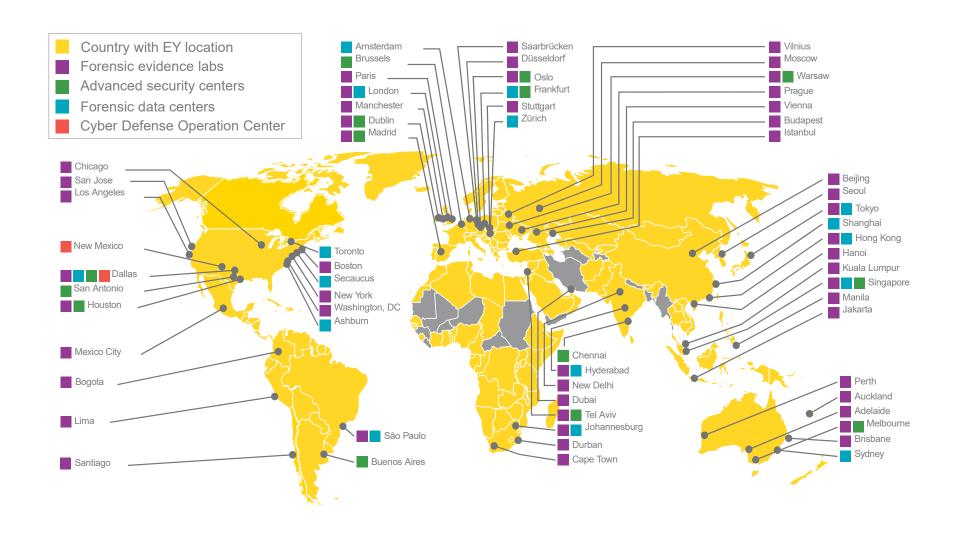
Collecting and analysing using eDiscovery and analytics the information / intellectual property compromised by cyberattackers – in order to assess losses

Supporting civil and criminal litigation relating to cyber breaches

Assisting CEO, CFO, Chief General Counsel, CSO, CIO and CISO with business consequence management and business level investigations



# **EY Infrastructure for Cyber**







# 証拠保全ガイドライン第7版

- 7-7. ファスト・フォレンジックによる証拠データ抽出
  - 対象機器が多岐に渡り揮発性データに残る証拠データが多いと見込まれ、かつ速やかな 実態解明や原因究明に偏ったフォレンジック調査が求められる場合、ファスト・フォレンジック (Fast Forensics)を実施することがある。
- 7-7-1. ファスト・フォレンジックとは
  - 早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出 及びコピーし、解析することである。
  - このニーズの背景には、業務利用されるシステムやサイバー攻撃に利用されるマルウェアの ネットワーク化(相互接続)、急増するファイルレス攻撃のメカニズム解明にあたりメモリ上の 揮発性情報の取得及び保全の高まり、SSD搭載デバイスとディスクの大容量化等がある。
  - インシデント発生の現場におけるファースト・レスポンダは、一つのデバイスを深く調査する 暇がなくなってきており、迅速な原因究明や侵入経路の特定をするために最低限のデータ 抽出・解析をすることが求められてきている。
- 7-7-2. ファスト・フォレンジックの実施
  - ファスト・フォレンジックにおいて抽出すべき主な証拠データについて、Windows OSの場合は、イベントログ、プリフェッチ、レジストリ、ジャーナル、メタデータ、インターネット(ブラウザによる閲覧履歴、メーラ等の設定及び送受データ)、メモリなどである。
  - これらの証拠データが消失する前に、発生現場におけるファースト・レスポンダが手作業 のみで迅速かつ最大限に取得することは困難であるため、専門ツールを利用して実施する。



# **@IDF Community 2013**

- 標的型攻撃をベースに記載
  - 想定しているTTPsも当時の流行を記載している

「今、現場で求められる Fast Forensics」

株式会社サイバーディフェンス研究所 杉山 一郎

・ここ1、2年でよく見られた標的型攻撃と対応してみて痛感したこと

組織のネットワークは人間の体と同じで、長く付き合えば付き合うほど変な癖(や病を抱えがちである。そして、長期間あるいは深く潜伏した病や癖ほど完全に難しい。最近の標的型攻撃も同様で、完全に悪の根源を除去するのは非常に困難対応(治療)が必要だと感じる。そして、その対応にフォレンジック技術は欠かないかと感じる。

- ・攻撃のフェーズ
- 1、最初の侵入と継続的な活動を行うためのシステム変更
- 2、情報収集と横展開(組織横断)
- 3、外部へのデータ送信準備
- 4、データ送信、送信データの消去
- ・攻撃のフェーズやクライアントの状況を考慮したフォレンジック対応

- 2、情報収集と横展開 (組織横断)
  - PSEXEC や PSEXECSVC等の SMB 経由での活動痕跡
  - ・ハッシュダンプ (pwdump、wce等) に代表されるグレーツールの痕跡

- 検索やフォルダアクセスの痕跡(Recent、ShellBag等)
- ・イベントログ (ログオン、プロセス作成、タスク等)
- ・ドメイン環境における情報収集(get-aduser等) 等々

44.4

- 3. 外部へのデータ送信準備
  - データの圧縮(典型的な例は RAR だが、最近は…)
  - ・ファイル一覧の痕跡 (DIRの実行および結果の痕跡等)
  - データを集約するための拠点(各端末の相関分析から見えてくることや、責任所在が 不明なテスト機などが多い)

等々

- 4、データ送信、送信データの消去
  - 消去行為の痕跡(sdelete等の実行、チェンジジャーナル、INDEXパッファのスラック等)
  - ・データ転送ツール (RAT、PSCP、HTran 等)
  - ・司令先 (C&C) と他の通信の相関分析

等く

× 関係する端末の完全コピー(完全なフォレンジックイメージの作成)が現実的に難しい。 ※誤解のない様に言うと、完全コピーは実施できるのであれば実施した方がいい。

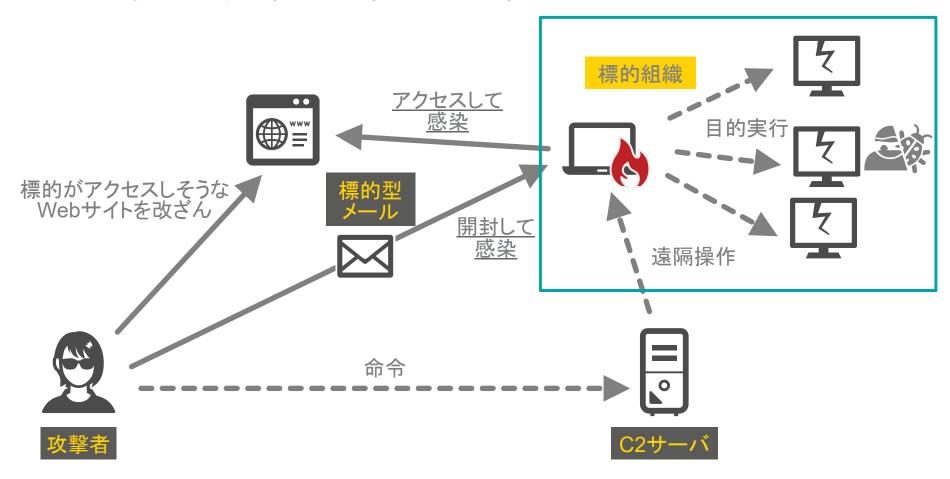
出典·

https://digitalforensic.jp/archives/2013/1308.pdf (2018/10/31アクセス)



# さておき、Fast Forensicsとは

・ 当初の想定環境例(標的型攻撃)





# 従来型フォレンジックとの違い

### **Fast Forensics**

- ▶数時間で実行
- ▶メモリダンプ、レジストリなど 対象範囲は限定的(要事前定義)
- ▶ ネットワーク上の複数デバイス に対して同時に実行
- ▶攻撃等の痕跡が残る傾向にある データの収集と解析に集中
- ▶次の対応を決めるために行う (発生事象の早期評価)
- ▶IOCスキャンと同時に実行する 場合もある

### **Deep Forensics**

- ▶数日~数週間
- ▶ 従来型のフォレンジック 調査
- 未使用領域に残存する 情報の復元 (削除されたマルウェア 本体や関連ファイルなど)
- ▶暗号化や難読化の解除
- Fast Forensicsの結果を 踏まえて必要に応じ実行
- ▶係争や不正調査での活用



# Fast Forensicsの位置付け

サイバーインシデント対応のライフサイクルにおけるFast Forensics

### 2 準備

アラート、SIEMやEDRなどで取得できるデータ、想定される脅威、利用できる技術などに基づき、データ収集の計画を立案する。

### 5 報告/意思決定

関係者や規制当局へのレポート準備、訴訟対応、クライアント等への 謝罪、再発防止策の公表などのクロージング対応を実施する。

### 4 現状復帰

インシデント対応中に得た情報や経験を基にビジネスを元の状態へ復帰する。類似した攻撃を防ぐために、ネットワークの再設計・企業内の認証基盤の改善(アカウント管理など)・SIEMの導入・モニタリングの改善・脆弱性診断などを実施する。

### 2)Fast Forensics(トリアージ)

### 重大なインシデント

- ▶ 顧客情報や重要な取引のデータ流出
- ▶ 重要な業務系インフラの破壊
- ▶ Webサイトの改ざん
- ▶ 知財や会計情報の流出
- ▶ 大規模なマルウェア感染
- 事業存続に影響するデータの破壊

### インシデント

- ▶ 許可されていないリモートアクセス
- ▶ DMZサーバーへの攻撃
- ▶ 既知のC&Cサーバーへの接続

### 軽微なインシデント

- ▶ IT機器の設定不備
- 素止されているクラウドサービスや機器利用
- ▶ ソフトウェアの著作権侵害
- ▶ 業務には関係ないWebサイトへのアクセス

発生したアラートや通報に含まれる 情報から仮説を立てて、影響範囲 や発生事象を推測していく。

- ▶ インシデント対応計画に基づく データ収集を実施
- ► 揮発性情報(RAMダンプやネットワーク情報など)やログを使った分析を実施し、発生事象の初期評価
- ▶ 収集データに加えて、サイバー スレットインテリジェンスを活用 し、関連するマルウェアや攻撃 キャンペーンを調査
- ▶ 影響範囲のスコーピング後に隔離などの対処を行う
- ▶ 必要に応じてフォレンジック調査を実施

### 3 フォレンジック調査

- ▶ 関連デバイスの特定とデータ保全
- ▶ 発見事項に基づいた仮説の検証
- ▶ 結果の取りまとめと次のアクションを検討

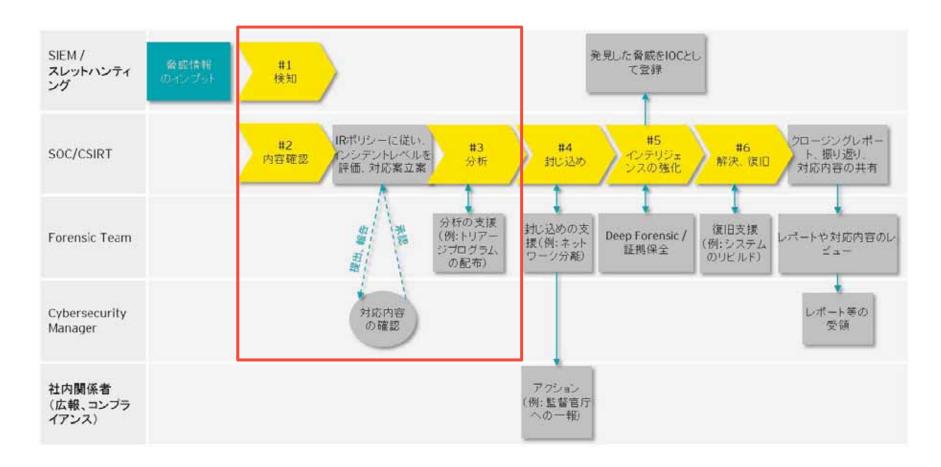
### 修復

トリアージで推測した影響範囲やシステム上の脆弱性を基に影響が拡大しないように措置を取り(ブラックリストの更新・特定プロセスの監視・IOCスキャンなど)、攻撃者が追加の攻撃を実施しづらい環境を構築する。



# Fast Forensicsの位置付け

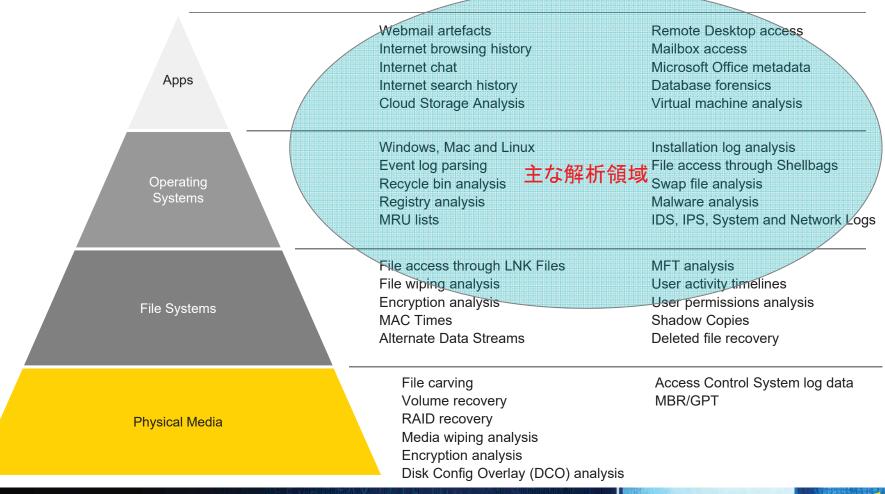
日常的なモニタリングやスレットハンティングへの適用例





# 一般的に実施される解析内容

Fast Forensicsでは、物理デバイスの複製を伴う分析や一部のファイルシステム分析は実施しない





# 収集するデータ例

・ 標的型攻撃等のサイバー攻撃を想定して収集するデータは、一般的に 次のようなデータが専用ツールで収集される

デバイス	収集データの例
Windows	<ul> <li>▶ メモリダンプ</li> <li>▶ ファイルシステムデータ(\$MFT、\$J、\$Logfile)</li> <li>▶ レジストリファイル</li> <li>▶ イベントログ</li> <li>▶ ブラウザ関連のデータ</li> <li>▶ SRUM</li> <li>▶ Prefetch</li> </ul>
macOS	<ul> <li>▶ メモリダンプ</li> <li>▶ timeline bodyファイル</li> <li>▶ システムログ、監査ログ、Unified Logging、メンテナンスログ</li> <li>▶ ユーザ特有およびシステム特有のplist</li> <li>▶ Launch AgentおよびLaunch Daemon</li> <li>▶ .bash_sessions等のbash関連ファイル</li> <li>▶ Spotlightデータベース</li> <li>▶ .FSEvents</li> </ul>
iOS/Android/l	Linux



# 収集するデータの活用例

### メモリダンプ

- ▶ 疑わしいプロセスおよび実行開始時期の特定
- ▶ マルウェア等不正コードのダンプと解析
- ▶横展開の情報

### ファイルシステム (\$MFT, Usrjrnl等)

- ▶ファイルの一覧(時間情報、各種メタ情報などを含む)
- ▶ 直近のファイルのアクティビティ(作成、更新、削除、データ追加など)
- ▶ MFTレコードの直近の変更ログ(フォルダのインデックス変更など)

### レジストリ

- ▶ファイルの閲覧、実行履歴
- ▶ サービスの登録状況
- ▶ マルウェアにより悪用されたキー(難読化されたコード、常駐方法など)

### SRUM

- ▶ 各アプリケーションの通信容量
- ▶ 各NICのネットワーク使用量

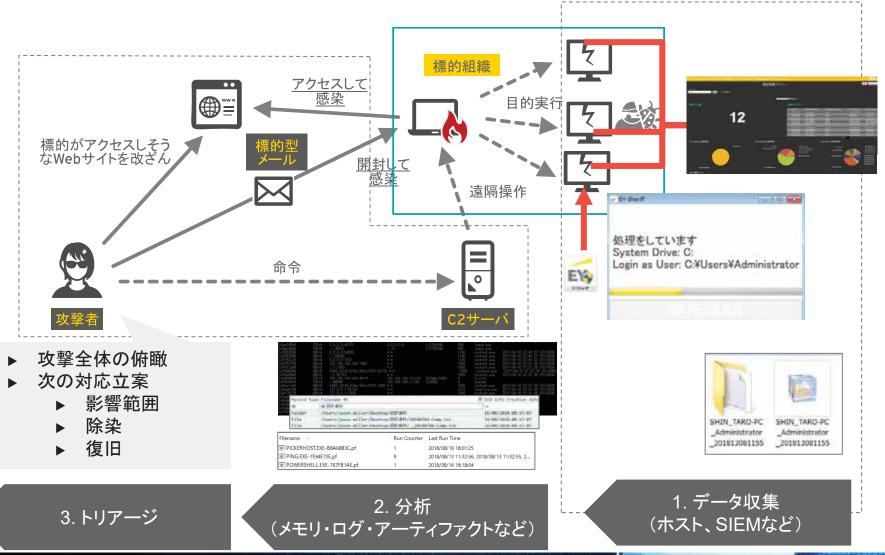


# データ収集時の課題

- トリアージ時のAdmin権限利用
  - 組織を超えた交渉
  - NW型フォレンジック、資産管理ツールやEDR等でのデータ代用検討
- 取得範囲の検討
  - 使用OSの種類やバージョン、想定する脅威により範囲は変わる
  - 既に配備済みのセキュリティ製品でトリアージに必要な情報が 取得できているケース
- Security Improvements
  - メモリ取得等に制限が発生するケース
- ログ
  - 必要なログが取れていない、残っていない



# Fast Forensicsのイメージ





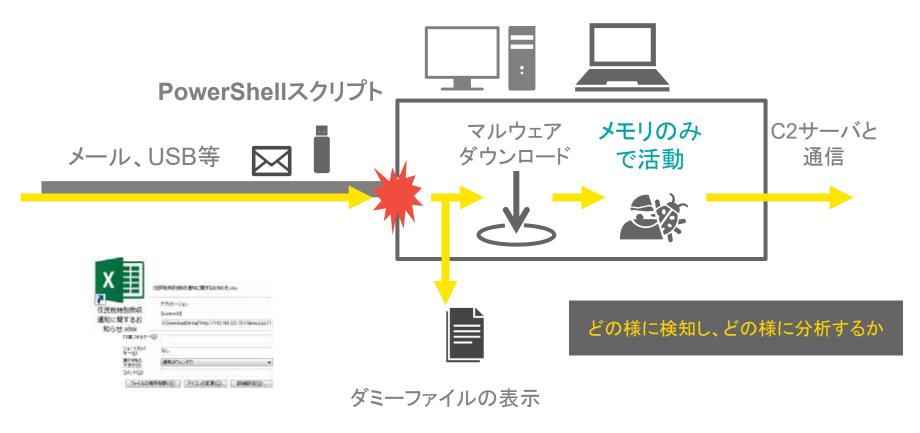
# 2013年以降の環境変化

- ファイルレス攻撃の増加
  - レジストリキーやメモリへのスクリプト保管など
- Lateral Movementの利用範囲、手法が拡大
  - 利用範囲:標的型攻撃以外のランサムや諜報活動まで
  - 攻撃手法:多くの戦術や技術が使われる
- 短い時間でのレスポンスが必要なケース増加
  - C2サーバー等が一定時間後にダウン
  - GDPR等の規制への対応(迅速な事実確認と報告)
- 攻撃者のモチベーション変化
  - 個人情報、クレジットカード情報の窃取だけでなく、ビジネスメール詐欺に使う請求書フォーマットから業務可用性(ランサム)まで
- ネットワークに接続するデバイスが多様化
  - 脆弱性、保有データ、ソフトウェアなどが多岐に渡る
  - クラウド同様に表面レベルしかアクセスできないデバイスがフォレンジック等の対象に
- インテリジェンスを活用したインシデント対応
  - サイバースレットインテリジェンスを活用した能動的なインシデント予兆の検出
- APFS等のコンテナ型ファイルシステムやT2など
  - ・ 従来型の保全は更に難しくなる傾向
- 非サイバー領域(不正調査等)にも変化
  - ワードクラウド、クラスタリング、機械学習により効率的な調査が普及



# ファイルレスの例

- PowerShellスクリプトによる攻撃
  - マルウェアそのものはメモリのみに存在
  - PowerShellのコードはレジストリ等に難読化されて保存





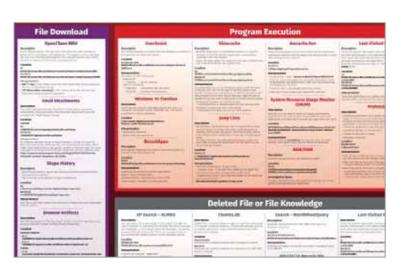
# Lateral Movement(最初の攻撃以降)

- ・ 検知、インシデントレスポンスは攻撃者が利用するTTPs(戦術・技術・ 戦略)を定期的にキャッチアップし、Fast Forensics(迅速かつ効率的な 対応)や侵害の極小化を図る
  - TTPsは攻撃者にとって柔軟に変更できない領域であり、TTPsの理解がFast Forensicsや日常 監視を高度化する
  - TTPsを理解したら、攻撃者の動きを捕捉するためにFast Forensicsで必要な情報収集について 整理をする
    - データコレクションツール、SIEMの設定の見直し
    - 解析用のプログラムやプロシージャの見直し
    - EDR運用チーム、SOC等との連携

ATT&CK Matrix for Enterprise										
	-	2000	Problems Excitation	No.	(metastad)	24	Section 1		Ballerman	Section 2
Solve by . Spingrooting:	Number 1	Jank professor Seaton	Sainte Titler Marquister	States Tries Marquistics	State of Sta	States of States of the	districts.	Aurille Temula	hand-and distransi	Sammely Swiften
Tenta talent	Della		-	0170 000	-	-	lasteries lasteries	imes.	-	Ξ
The Park of the Pa	Commandium Posterio	Assert Hartsonian	mornia	Street Printers	015110		(married to a second to the se	Spinore. Pers	- September -	Separate Printers
Through Rompushie Media	Tie Control			Account Cormul	Durtury	Descript Descript	of Remote Services	her bear	Berlines	Control Control Photocur
Sperghaning Attachment	Corred Panel Items	Apparel DLCa	Application (bonning	EMSTP	Crydenitals in Files	Newski Service Scenting	Surport Serrigray	Data from Mormalium Repositories	Exfitration liver Alternative Protocol	Cryptographic Promocel

出典: ATT&CK Matrix for Enterprise

"https://attack.mitre.org"

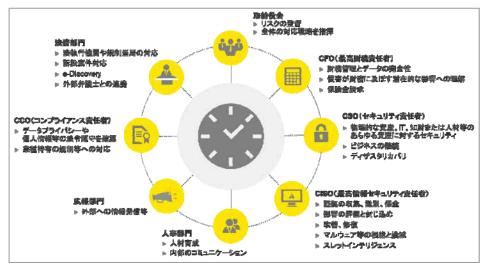


出典: SANS Institute "https://www.sans.org/security-resources/posters/dfir"

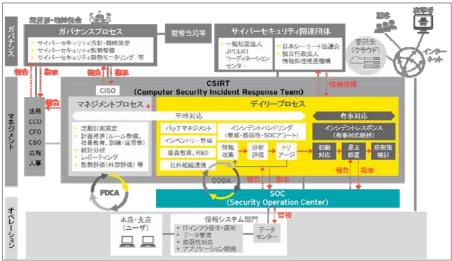


# 短時間での対応、規制等への対応

- Fast Forensicsを構成する要素は技術的な要素が多い一方で、実行に際しては 組織の危機管理対応、インシデント対応などのプロシージャに組み込む必要が あるため、関連部署との連携等が必要になる
  - ・ 攻撃者のモチベーション変化、業界におけるサイバーリスク動向や規制状況、自社が対峙するサイバー犯罪、開発や営業などのビジネス部門のインフラ活用状況、自社のインフラ変化への理解等を共有し、Fast Forensics含むインシデント対応のプロシージャを定期的に見直す
- ▶ インシデントレスポンスにおける役割・責任の明確化



### インシデント対応のコンテクストの整理





# 環境変化等を踏まえて再考

## これからのFast Forensicsを考えるうえでのキーワード

- 日々のモニタリング・検知・対応への活用
  - 能動型(ハンティング)と受動型の両方で利用することを想定
  - データコレクション、IOCスキャン等
- 対峙するサイバー犯罪全体を俯瞰的に捉える
  - プロセス全体やコンテキスト(サイバー犯罪の性質)への理解が必要
  - 狙われるリスクと保有する情報のマッピング
  - どこから情報をすばやく収集するのか。
  - 集めたインテリジェンスをどの様に活用するのか。
- Fast Forensicsを適切に行うための準備
  - どの様に判断し、保全し対応するのか(プロシージャの整備)
  - 増加するデータソースへの対応(新しいOS、IOT、クラウドなど)
  - 収集するべきデータの特定と方法を検討



# 日々の活動計画の再考

### 重要となる要素



サイバー犯罪に対する情報の受信と理解



サイバー脅威の検出試行



クラウドシステムの融合



インシデントへの対応



フォレンジック調査、規制対応



インシデント対応後の復旧



モニタリング 監視による可視性向上









SOC

ログの集約 セキュリティ



- 振る舞いベース
- ・インテリジェンス
- ・調査で得た情報のインプット



検知 調査と評価





- フォレンジック視点で診断
- ・IOCスキャンなど
- ・メモリ/ログ/アーティファ クト分析
- マルウェア解析
- ・フォレンジック



対応 企業ポリシーに従う



- ・ステークホルダー、規制当 局などへ報告
- 開示義務への対応
- ・捜査当局への相談
- システム復旧
- ・再発防止

スレットハンティング

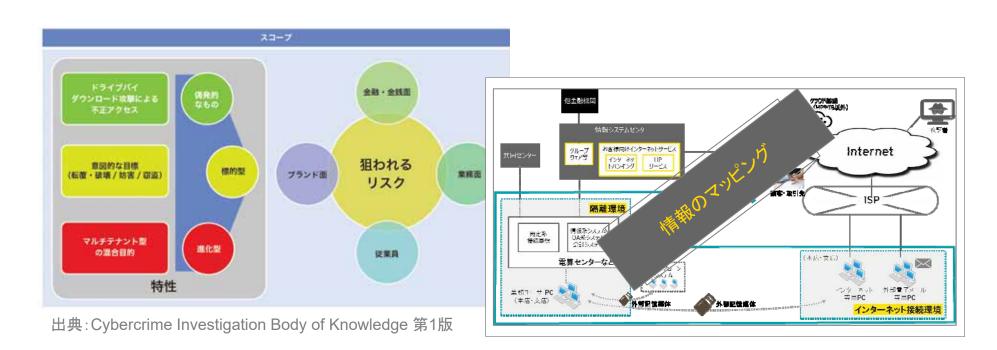


発見した脅威情報を用いた回帰的分析 受動的なハンティング、検知、調査



# 対峙するサイバー犯罪の特性

- 「どの様な性質を持つ犯罪か」俯瞰的に捉え、トリアージ計画に活用
  - 狙われるリスクは何か、情報のマッピングに加えて多面的な視点で捉える
  - スコープの策定から保有インフラにおけるトリアージプランを策定する
- 集めたデータのマイニング(情報・知識等の取り出し)と活用



# 狙われるリスク(産業毎)

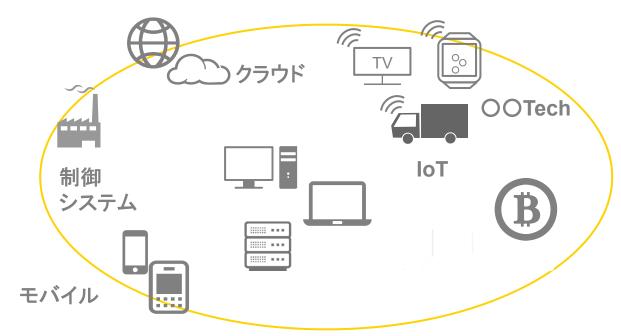
- 一般的な産業毎のリスク
  - モニタリング>検知>インシデント対応のプロセスに大きな影響を与える

産業	サイバー犯罪の例	産業	サイバー犯罪の例			
自動車	▼ マルウェア感染等による設計情報や研究中の 技術情報の漏洩	銀行	<ul><li>オンラインバンキング詐欺(不正送金)</li><li>DDoSや銀行内部を狙った攻撃</li></ul>			
	<ul><li>パートナシップのジョイントベンチャー等からの 情報漏えい</li></ul>	保険	<ul><li>▶ 偽りの保険請求やインシデントの報告</li><li>▶ 「リスクモデリング」データを含む内部情報流出</li></ul>			
防衛産業	<ul><li>▶機密情報の窃取</li><li>▶重要な防衛資産に対するサイバー攻撃</li></ul>	ライフサイエンス	<ul><li>研究と臨床試験データの漏洩</li><li>学術パートナーおよび/または下流のジョイントベンチャーを介した不注意による漏洩</li></ul>			
公的機関	<ul><li>■要な国家インフラへの攻撃や破壊</li><li>機密文書やデータ等の漏洩</li></ul>	ヘルスケア	▶ 患者データとメディカルID番号の盗難 ▶ 不正請求			
鉱業	<ul><li>▶ 国内の石油やガスの埋蔵量等を含んだ契約 や研究情報の漏洩</li><li>▶ ハクティビストによる業務妨害</li></ul>	メディア	► 著作権侵害とIPの盗難 ト 放送の妨害			
			<ul><li>元従業員による研究開発の盗難(ソースコードの窃取など)</li><li>第三者へのデータ漏洩</li></ul>			
石油・ガス	<ul><li>業務中断や試掘に関する情報の漏洩</li><li>規制基準の未達成(失敗)</li></ul>	テクノロジー				
	7,000		<ul><li>モバイルネットワークと放送時間の詐欺活動による妨害</li><li>規制基準の違反につながる個人顧客データの漏洩</li></ul>			
電力	<ul><li>SCADA制御システムへの攻撃による業務妨害 行為</li><li>スマートメーターの改ざん</li></ul>	テレコム				
コンシューマー 製品販売	<ul><li>→ 研究やマーケティングに関する情報の窃取</li><li>→ 情報流出等に起因した模倣品や海賊版</li></ul>	小売り	<ul><li>→ 顧客のPIIの盗難</li><li>→ 顧客のクレジットカードデータの盗難</li></ul>			



# Deep Forensicsは困難に

- 対象の根幹へのアクセスが困難になり、表層レベルでの解析が中心になる
  - ・ デバイスの全領域複製は不可
    - アクセス手段の欠落、T2チップ(Apple)などのセキュリティ機能
  - アプリ、ユーザーレベルでのアクセスが前提
    - ・ システム導入時のフォレンジック設計(ログ取得等)が重要に
    - Fast Forensicsに類似するアプローチが必要に



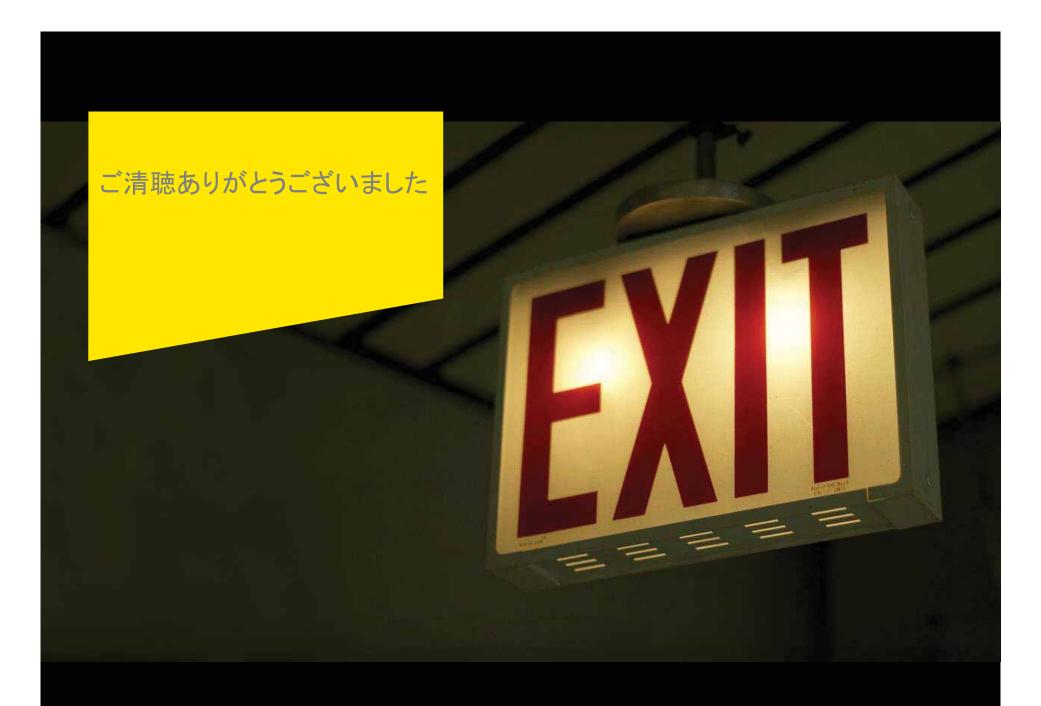




# まとめ

- Fast Forensicsとは、早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出し、解析すること
- Fast Forensicsは、これからの組織におけるサイバーセキュリティ活動で 有用な手法の一つになりえる
  - 早急な事実確認、次の行動計画の策定、既知脅威の検出など
  - 実行に際しては組織連携、リスクの識別、サイバー犯罪全体への俯瞰などが 必要になる
- 活用には事前の準備が不可欠
  - 新しいデバイス、サービス利用時にはセキュリティアセスメントの中でFast Forensicsについて考慮する(当然、フォレンジックも)
  - 想定されるサイバー犯罪リスクは産業により異なり、インシデントの検知等の 日々の活動やトリアージプランも変化する
  - 環境変化を吸収するためのアセスメント、インシデント対応計画の継続的な 見直し等が必要





### EY | Assurance | Tax | Transactions | Advisory

### EYについて

EYは、アシュアランス、税務、トランザクションおよびアドバイザリーなどの分野における世界的なリーダーです。 私たちの深い 洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より 良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、ey.comをご覧ください。

### EY新日本有限責任監査法人について

EY新日本有限責任監査法人は、EYの日本におけるメンバーファームであり、監査および保証業務を中心に、アドバイザリーサービスなどを提供しています。詳しくは、www.shinnihon.or.jp をご覧ください。

© 2018 Ernst & Young ShinNihon LLC. All Rights Reserved.

### **ED None**

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものでは ありません。EY新日本有限責任監査法人および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。