デジタル・フォレンジック・コミュニティ 2019 in TOKYO

Fast Forensicsの現状と動向、そして今後

EY新日本有限責任監査法人

杉山　一郎

2019年12月9日（月）

EY
Building a better working world

About Me

- EY新日本有限責任監査法人
  - Forensics事業部 プリンシパル
  - EY Japan Forensic Technology Leader
    - Digital Forensics／Cybercrime Investigation
    - eDiscovery
    - Forensic Data Analytics
    - Information Governance
- Forensic業界での経験15年以上
  - Investigator、Trainer、Expert Witness、Consultant
- GIAC Certified Forensic Analyst
- IDF技術分科会幹事
  - 証拠保全ガイドライン（第1版～現在）
  - IDF Community（2013、2018）

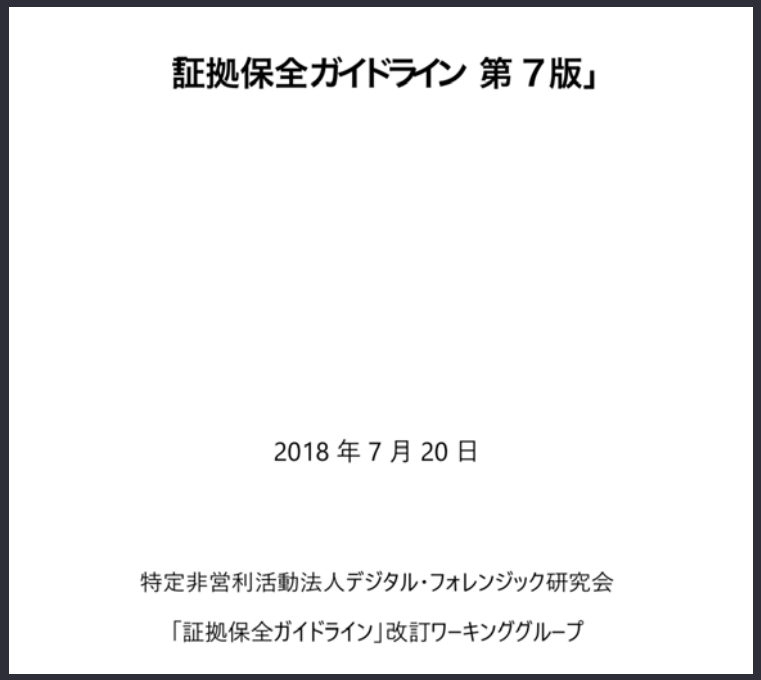
本日のアジェンダ

No	トピック
1.	Review:Fast Forensicsとは
2.	Fast Forensicsの課題
3.	解決に向けたアプローチ

Review: Fast Forensicsとは

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及びコピー し、解析することである。（証拠保全ガイドライン 第7版より）
  - 端末（Windows）の証拠データの抽出と解析に限定した話ではない

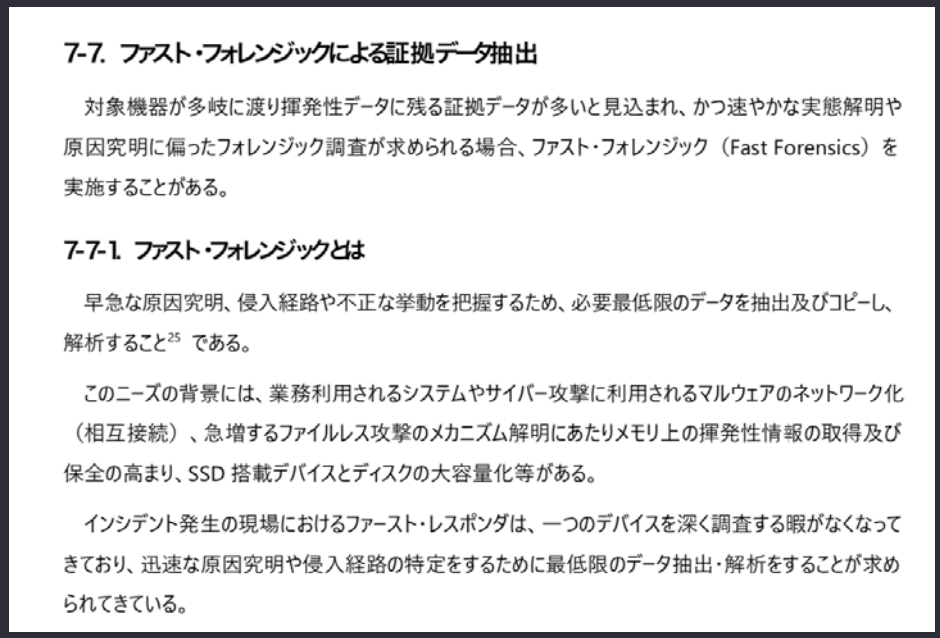


証拠保全ガイドライン 第 7 版」

2018 年 7 月 20 日

特定非営利活動法人デジタル・フォレンジック研究会

「証拠保全ガイドライン」改訂ワーキンググループ



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[25] である。

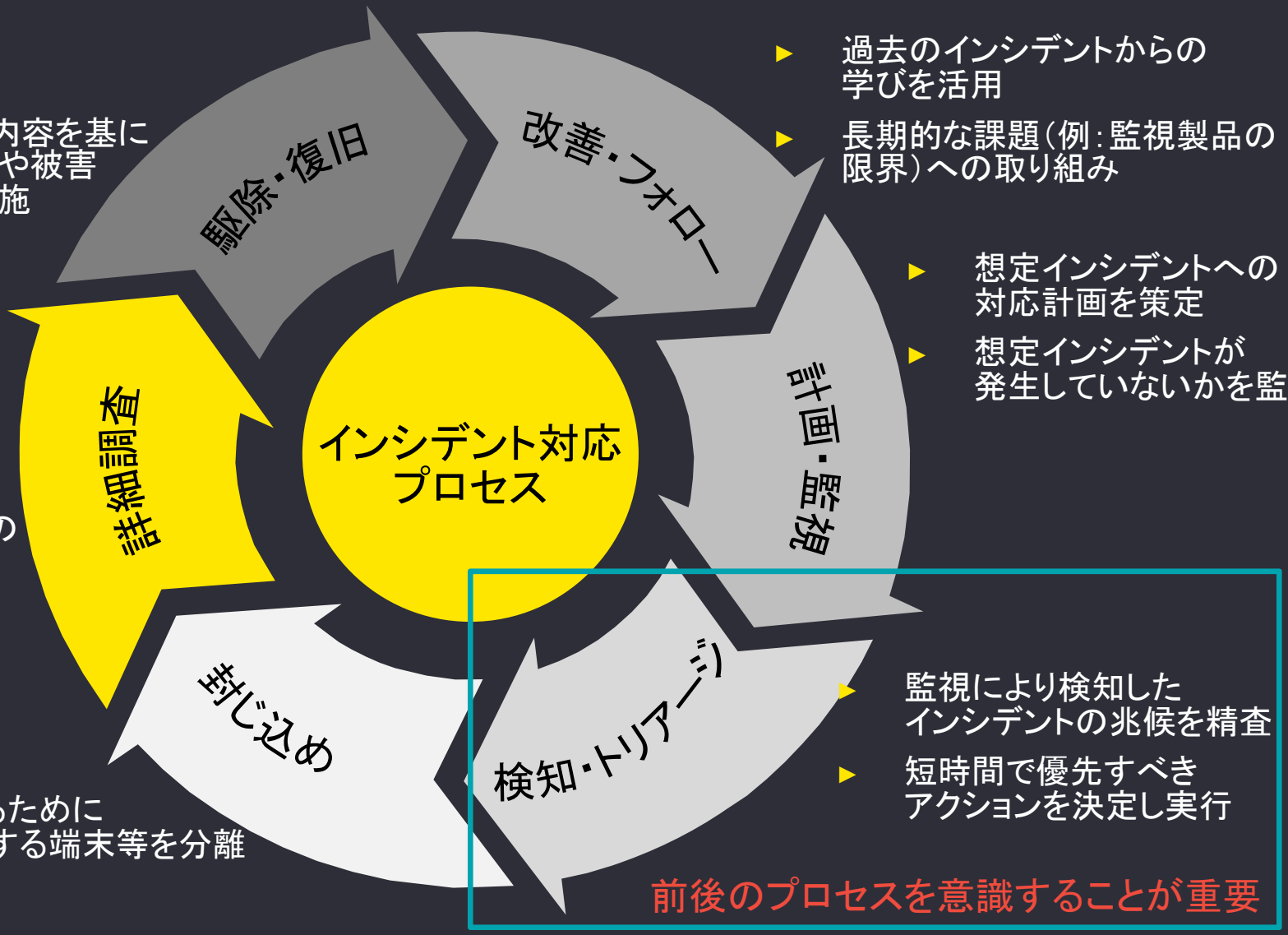
このニーズの背景には、業務利用されるシステムやサイバー攻撃に利用されるマルウェアのネットワーク化（相互接続）、急増するファイルレス攻撃のメカニズム解明にあたりメモリ上の揮発性情報の取得及び保全の高まり、SSD 搭載デバイスとディスクの大容量化等がある。

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。

Fast Forensicsとは

- Fast Forensics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Forensic調査が求められる場合、Fast Forensicsを実施することがある。
- 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及びコピーし、解析することである。（≠ディスクイメージ、ディスクコピー）
  - 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、一つのデバイスの精査よりも、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。
- Fast Forensicsの実施
  - Fast Forensics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・レスポンダー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。

Fast Forensicsとは



- 過去のインシデントからの学びを活用
- 長期的な課題（例：監視製品の限界）への取り組み
- 想定インシデントへの対応計画を策定
- 想定インシデントが発生していないかを監視
- 監視により検知したインシデントの兆候を精査
- 短時間で優先すべきアクションを決定し実行
- 影響を最小限にするためにインシデントに関連する端末等を分離
- これまでに発覚した内容を基にマルウェア等の駆除や被害システムの復旧を実施
- 必要に応じ全貌解明のためにフォレンジック調査等を実施

前後のプロセスを意識することが重要

Fast Forensicsとは

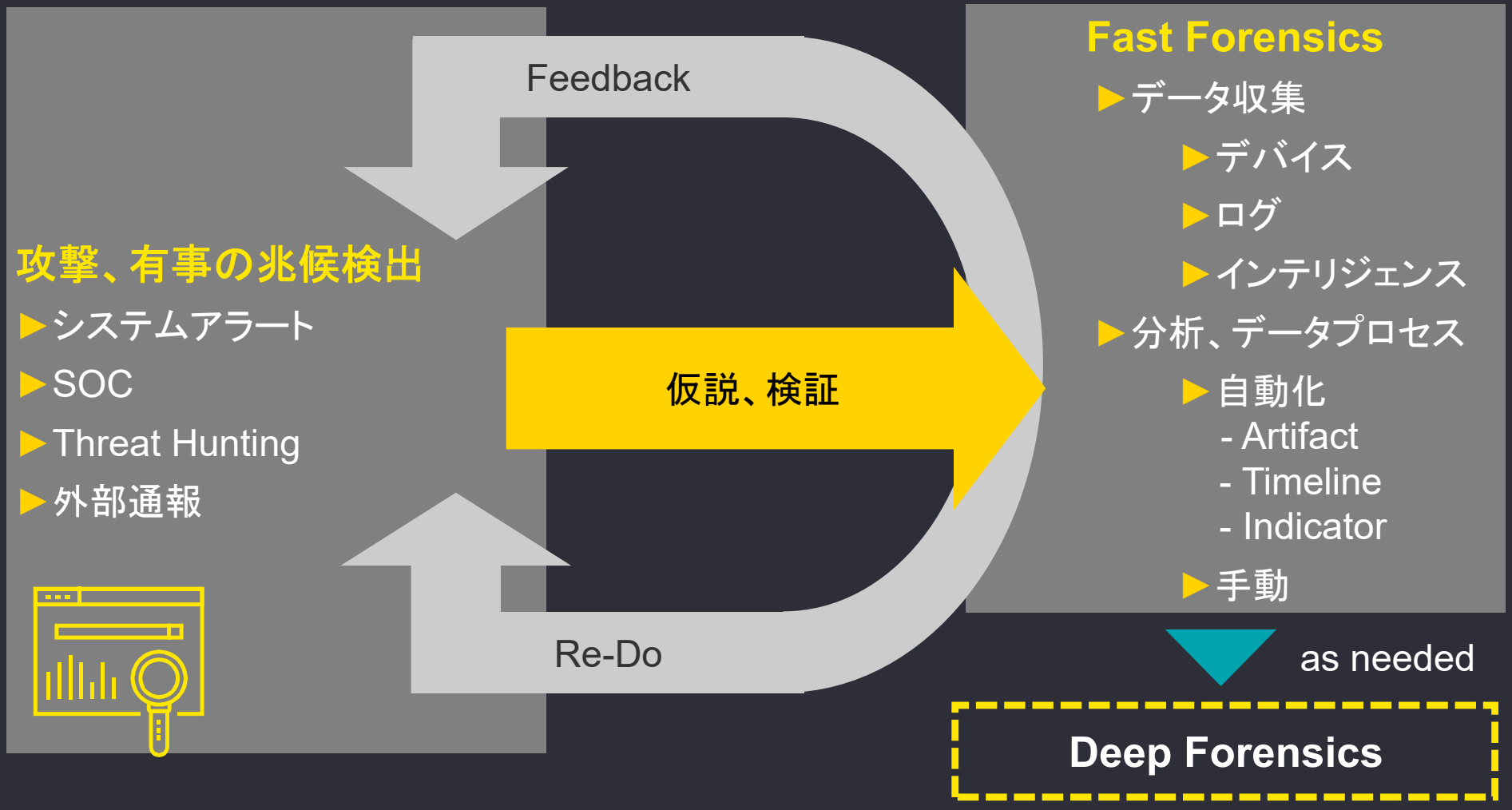
- 海外でも“Triage／Quick Forensics”などの呼称で議論されている
  - SANS DFIR Summit、DFRWS等
  - ①データのコレクション②分析③トリアージを実施
  - EDRに搭載されたTriage・Case Seepなどの機能に類似

- 基本的にはセキュリティインシデント発生時のトリアージにフォーカスした議論である事が多い
  - Forensics（証拠保全・解析等）とインシデントレスポンスの中間的な立ち位置

- Digital Forensic Readinessの中で議論される機会が増えている
  - Fast Forensics用のコレクションツールの準備
  - コレクションの実施順序
  - 短時間で十分な情報を得るための準備、取得範囲

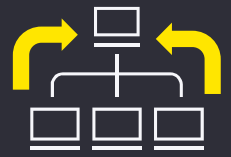
Fast Forensicsとは

- Fast Forensicsのプロセス



Fast Forensicsとは

- 現状のアプローチ
  - コレクションツールの活用
    - USBデバイス等に保存されたツールを実行し、メモリ等の重要なアーティファクトを収集
    - 収集とともにパースを実施する場合もあり
    - 従来型のForensic的なアプローチ（ドライバ／APIを未使用）
      - APIを利用してデータを集める場合もあり
  - エージェントの活用
    - EDRなどのエージェントを介して取得
    - 事前取得データや都度取得したデータを対象
    - Rawデータよりもエージェントを介して取得したデータが中心
  - 基本的にエンドポイントに存在するデータへForensicを実施
    - ツールによる収集は、クラウドのデータは同期ログなどが中心



従来型（イメージング等）のプロセスを高速化する試みもある（後述）

コレクションツールの活用例

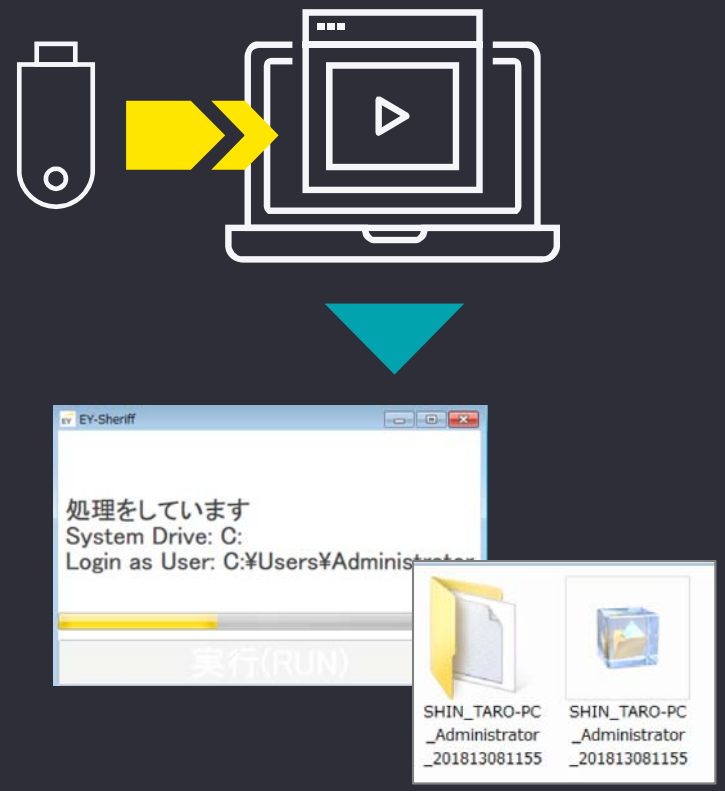
- 一般的なコレクションツールの実行
  - 収集対象：ファイルシステム（MFT／Usnjrnl）、メモリ、アーティファクト等
    - ネットワークログ、クラウド等は対象にしていないことが殆ど
    - 解析時間を短縮するためにライブでの解析結果（履歴、各種メタデータの抽出）も合わせて収集することもある
  - 収集方法：ファイルシステムドライバ、API等のOS機能を極力利用しないようにする（コピー制限の迂回）
    - Live Response Collection等のツールセットの利用
    - OSの機能を利用した収集方法もあり：PowerShell（Windows）、Python（Mac）
      - 例：AutoMacTC：Automated Mac Forensic Triage Collector
  - 収集形式：ファイルタイプ毎にディレクトリを作成し、そこにコピー
    - L01、AD1等のメタデータを保持するコンテナファイルを利用するツールは少ない
    - 最近はVHD(X)の利用増？

コレクションツールの活用例

- Fast Forensicsのツールに備わるデータ収集以外の機能例
  - Forensically Soundへの配慮
    - 収集データのアーカイブ（zip、tar、7zなど）
    - Hash
    - コピーログ
  - 暗号化
  - 解析
    - コマンド／API等を介したデータ出力（ライブフォレンジック）
    - IOCスキャン
    - html／csv等のレポート出力
      - ソースのアーティファクトの収集を行わない場合もあり
  - Batch／Script
    - 事前のConfiguration（ターゲット、実行するプロセスの選択）

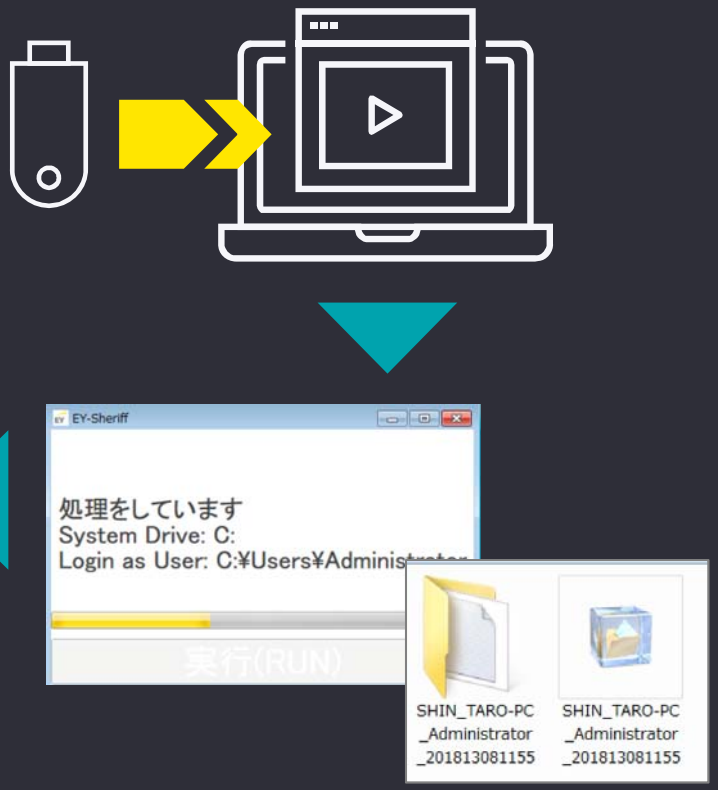
Fast Forensicsの実行例

- スタンドアロンコレクションツールでは、任意のモジュールを選択して
  データの収集および解析を実施



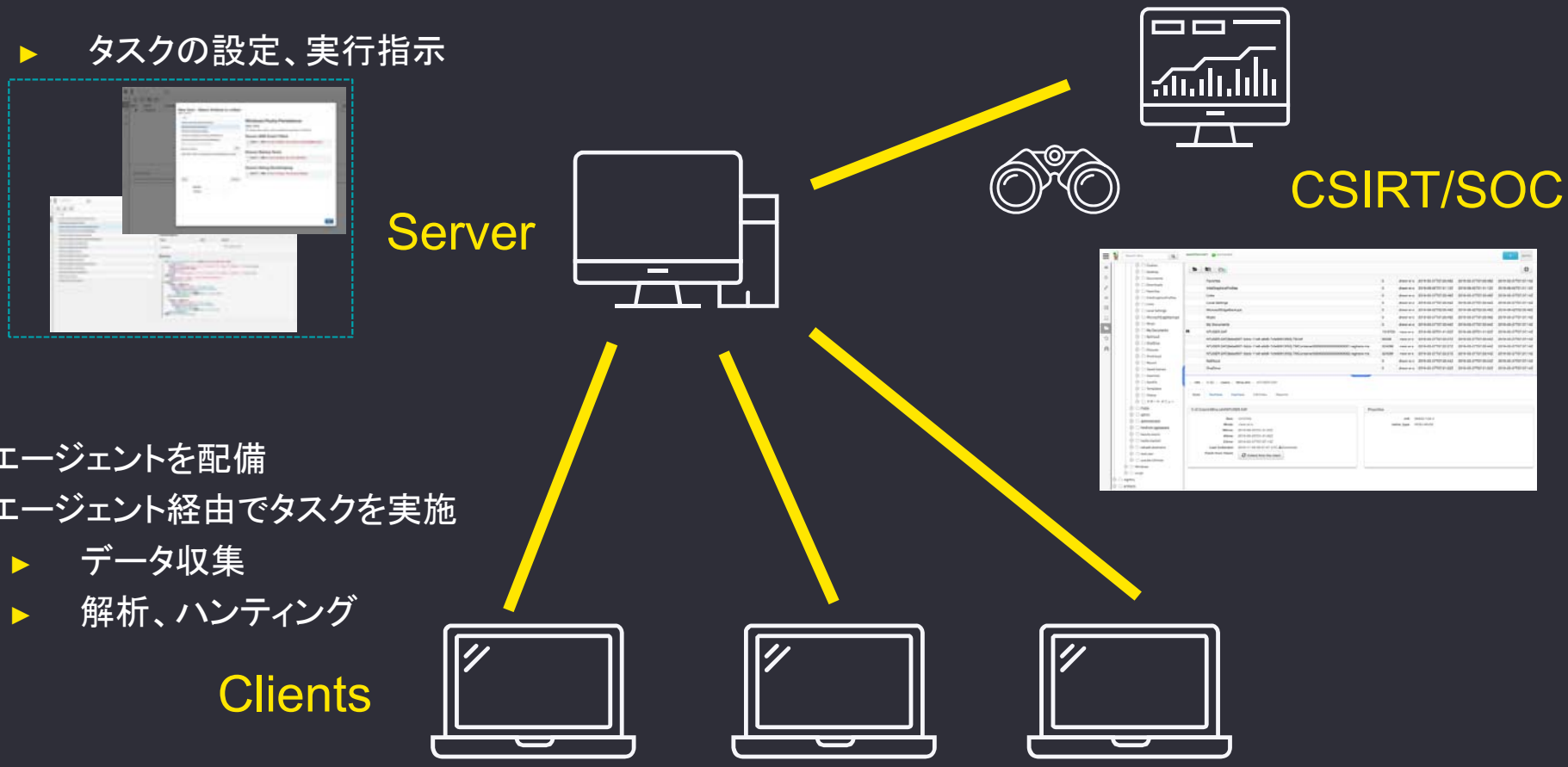
Fast Forensicsの実行例

- 収集データを分析（Timeline、Artifactベース、Indicatorベース）



Fast Forensicsの実行例

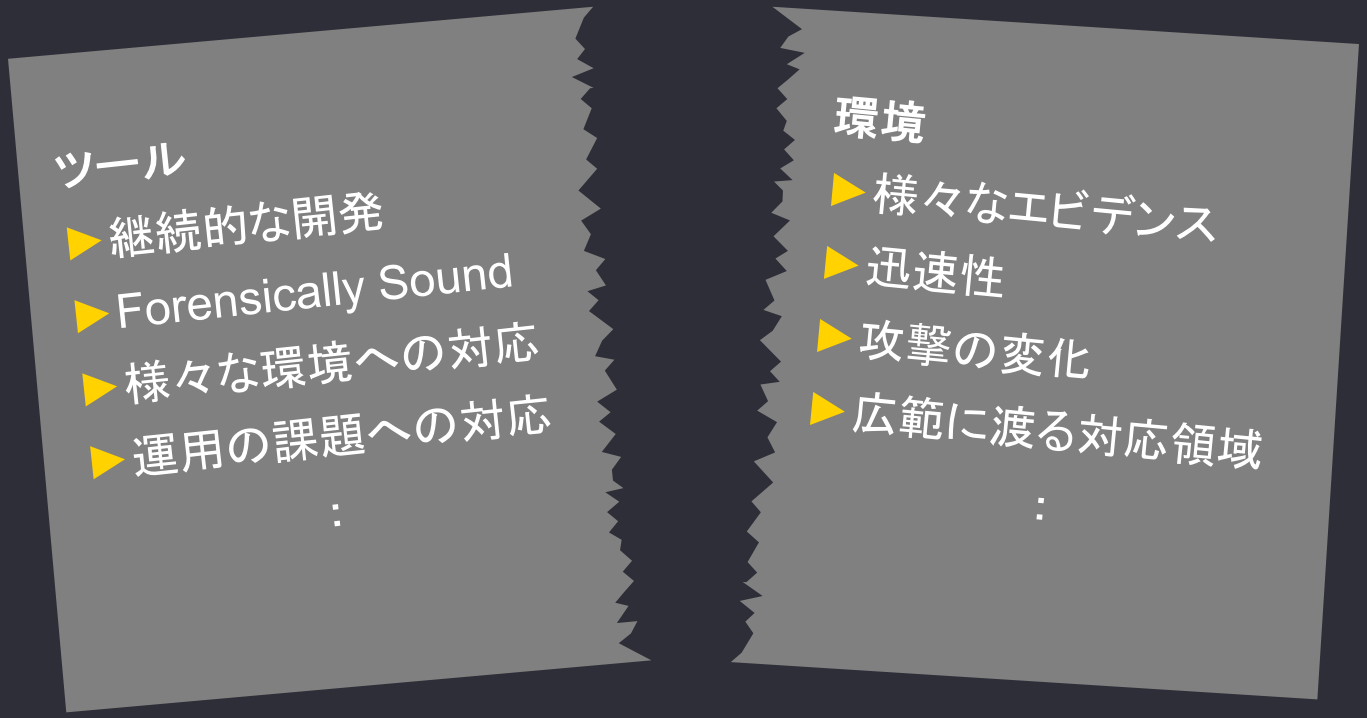
- ネットワーク越しに各エンドポイントのデータを収集・解析するツールにも Fast Forensicsを実行するための機能が備わっている
  - 例：Velociraptor（ https://www.velocidex.com ）



Fast Forensicsの課題

Fast Forensicsの課題

- 継続的な課題が多数
  - Fast Forensicsツールの課題
  - Fast Forensicsを取り巻く環境の課題



Fast Forensicsツール・実行環境の課題

- アーティファクトの追加等への柔軟な対応
  - コード修正のしやすいオープンソースの利用
  - 収集面ではセキュリティ機能の迂回、解析面では様々なパーサーの開発が必要
- 非ライブ状態からの収集
  - 必ずしもライブ（稼働状態）のシステムを対象としない
  - Shadow CopyやSnapshot
- Forensic的に最低限必要な要件
  - 各アーティファクトの収集ログ、ハッシュ
  - ファイルのコンテナ化（VHD(X)、アーカイブファイル）
  - 任意の完全Imaging実行
- Miscellaneous
  - クラウドデータの収集
  - リモート対応、SFTPやクラウドへのアップロード機能
  - 複数ホストからの同時収集
  - 収集ファイルへのパスワード付与

Fast Forensicsツール・実行環境の課題

- 解析のしやすさ、スピード、安定性、自動化
  - Timelineの自動生成
    - メモリも対象に実施
    - 各パーサーの定期的なメンテナンス
  - Indicatorベースの解析（Compromise、Attack、Fraud、．．．）
    - 取り込み、スキャン
    - ケース毎に定義
  - 可視化
    - ダッシュボードを利用したデータの絞り込み
  - サンドボックス環境との連携
    - 疑わしいファイルの解析
  - 様々なデータソースへの対応
    - macOS、Linux、Mobile、IOT、Cloudなど

Fast Forensicsを取り巻く環境の課題

- ストレージ量
  - ローカルストレージの増加
  - メモリも同様に増加（メモリダンプの必要性の増加）
- 多岐にわたるエビデンスソース
  - スマートフォンやタブレット、様々なOS
    - イメージングできないエビデンスの増加
  - 攻撃・不正等の起点の多様化
  - クラウド領域
    - 追加オプションでの取得可能な領域（例：SlackのCorporate exportなど）
  - 3rd Party／IOT／サプライチェーン
- 迅速な判断の必要性
  - データの揮発性、EDR等の製品が保持する情報期間（ログ等）の短さ
  - EDRとの連携
  - コンプライアンス、当局（規制）対応
  - 捜査機関として求められる迅速性

Fast Forensicsを取り巻く環境の課題

- サイバー攻撃の変化
  - サイバー攻撃者
    - 攻撃者のテクニック多様化、モチベーション・能力の高さ
    - 初期侵害から横展開までのスピード
    - 悪用するインフラ
  - ユーザ
    - 守備範囲の拡大
      - 初期攻撃のアクセスポイント増加
      - ビジネスオペレーションの変化
      - BECやレピュテーション低下を目的とした攻撃は標的が変わる可能性あり
    - トリアージに利用するデータ・技術（モノ）の増加
    - 内部犯行（Insider Threatも考慮する必要）
      - 従業員開発のマルウェア
      - IP／PIの窃取

解決に向けたアプローチ

課題解決に向けて

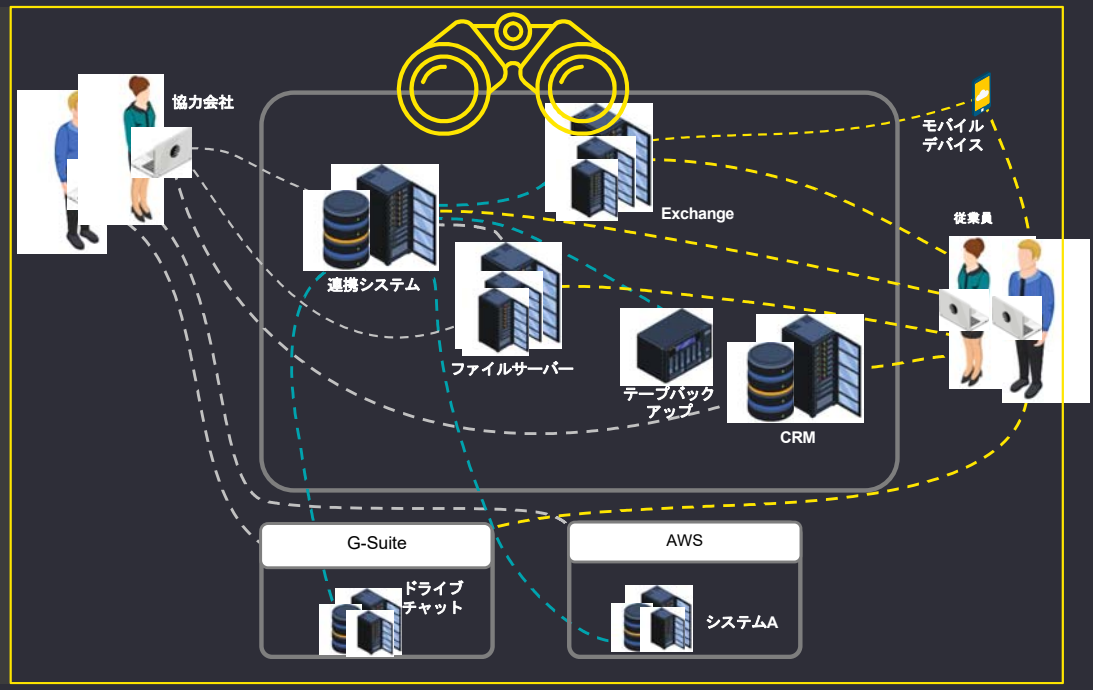
- 基本的なアプローチ

1. Data Mapping	▶重要なデジタル資産の特定や保護を通じたデータとリスクの整理 ▶トリアージに必要なデータの取得方法の整理
2. Adapt to Attack & IR Process	▶利用可能なインシデント対応時間の算出 ▶脅威シナリオの前後関係、悪用される技術等への理解 ▶Forensically Soundな対応の必要性
3. Technical Measures	▶収集と解析の対象となるアーティファクトの継続的なアップデート ▶収集するデータの強化（各デバイス、Cloud、IoTなど） ▶横断的なログ（SIEM）との連携や脅威情報の活用

1. Data Mapping

- 重要なデジタル資産をマッピング

- デジタル資産＝データ（ファイルの中身）＋コンテキスト（メタ情報）
- 収益創出、事業運営、または規制の面で、高い価値を示す必要不可欠な重要なファイル等
- 一般的には、企業の機密データや規制の対象となるデータに分類
- 上記をベースにリスクシナリオを検討し、トリアージに必要なデータや対応の時間軸を整理する



2.Attack & IR Process

- Fast Forensicsに必要なエビデンスの取得方法、取得の制限など

- リスクの顕在化を示すIndicator、アーティファクト

3. Technical Measures

- Collectorの調整
- SIEM／EDR／Asset toolによる情報収集

1.Data Mapping

- マッピングの過程でFast Forensicsに影響を与えるポイントを確認
  - Fast Forensicsに限らず、eDiscoveryや不正対応（Forensics）にも大きな影響を与える

1. 想定外のOS

- あるリスクに関連する部門が利用している端末はmacOSであり、EDR／Assetツール、Fast Forensicsツールいずれも対応が十分でない
- Forensicsも十分な手続きがない

2. トリアージに必要なログがない

- Slack
- Office365
- Assetツールの活用

3. Indicatorの定義

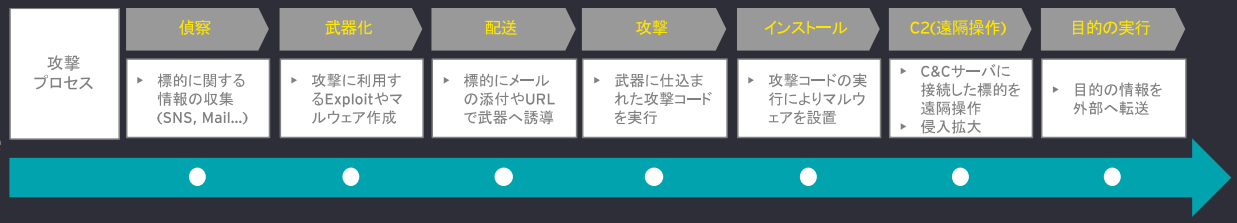
- サイバー
  - Compromise（侵害）
  - Attack（攻撃）
- 内部不正

4. 複雑化とデータの分散

- ソーシャルメディア
- モバイル
- クラウド

2. Adapt to Attack & IR Process

- サイバー攻撃のIndicatorとArtifact
  - ATT&CK等同様に攻撃プロセスごとにアーティファクトを整理する
    - Initial Attack
    - Lateral Movement
    - Malware Persistence
    - Defensive Evasion



  - 後述のマトリックスなどを利用し、整理する
    - トリアージのベースとなるデータ、ケース特有のデータを整理
    - 整理したデータの取得・分析方法を整理
  - macOS等の他のOSにも応用する

  - 脅威情報の活用
    - Indicatorの収集
    - 攻撃トレンドの把握

2. Adapt to Attack & IR Process

- 例：WindowsのPersistence（継続的な活動）に利用される技術

Persistence Tech

Windows標準	Program Loader	System Behavior
▶Startup	▶Image File Execution	▶Winlogon
▶Run等のキー	▶Shim	▶DLL Hijacking
▶タスク	▶Extension Hijacking	▶AppInit DLLs
▶サービス	▶COM Hijacking	▶Active Setup

Artifact

Characteristics and Detectability of Windows Auto-Start Extensibility Points in Memory Forensics を参考に作成

2. Adapt to Attack & IR Process

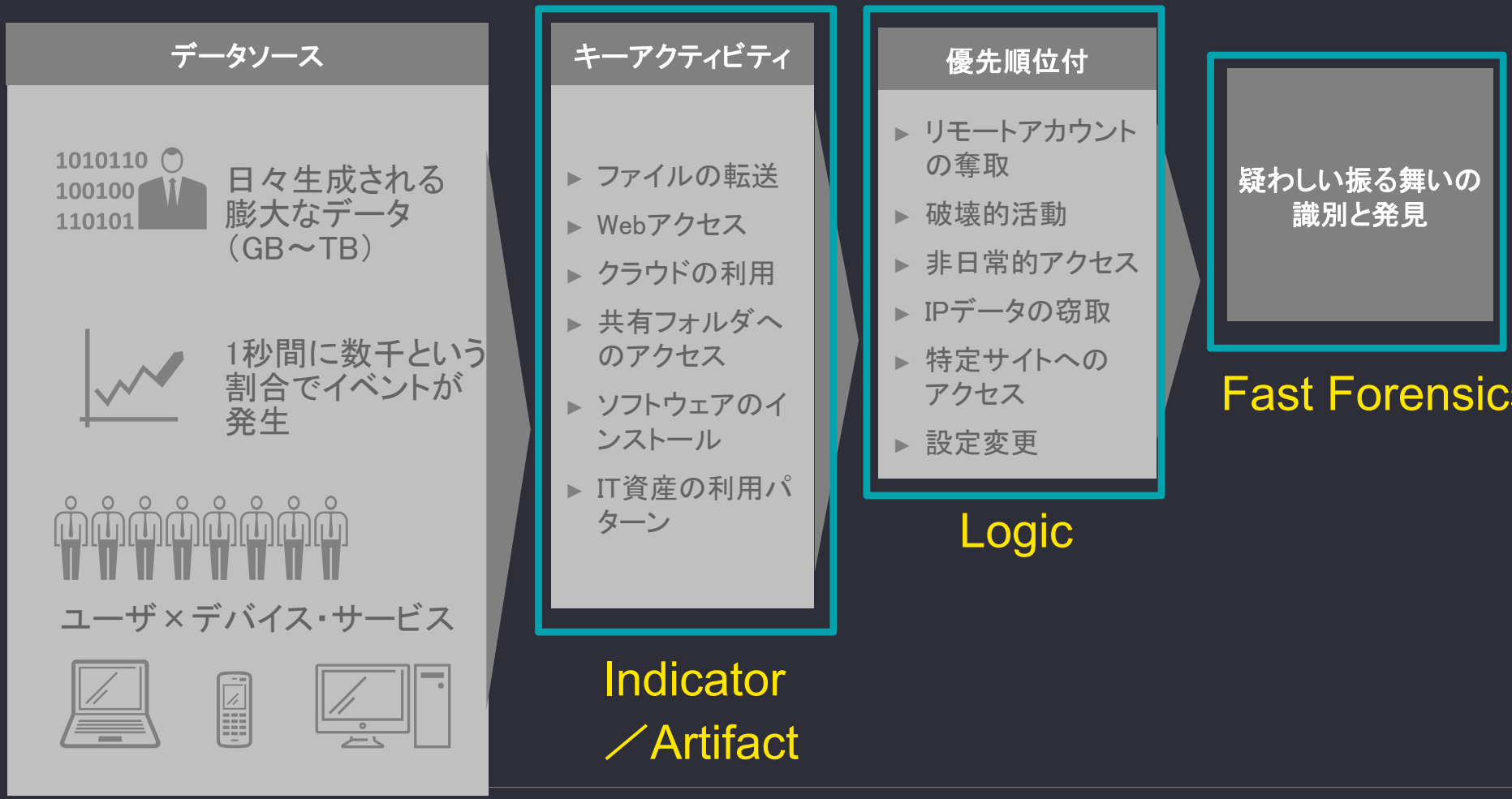
- 例：macOSを標的としたサイバー攻撃

Process	例	Artifactの例
Initial Attack	• O365偽ログイン • 侵害済みのWindows からのログイン	• Webブラウザ • MRU • Spotlight
Persistence	• マルウェアの機能を利用 • スクリプト	• LaunchAgents/Daemon • LoginItems • backgrounditems
Lateral Movement	• SSH • 画面共有 • Remote Desktop • 3rd Party	• ASL • system.log • Unified Logging
Defense Evasion	:	:

Artifact

2. Adapt to Attack & IR Process

- 内部不正については、様々な研究により自動検出などが試行されているが、まずは不正行為を構成するIndicatorを複数定義することが基本のアプローチとなる



2. Adapt to Attack & IR Process

- インシデント対応（特に内部不正）にてCloudサービスが関与する場合、Forensicsでどの様にCloudサービスからデータを取得するか事前に検討する必要がある
- 米国をベースとするクラウドサービスの多くが、フォレンジック等に必要なデータはオプションでの提供となっていることが多い（以下、Slackの例）ことに留意する必要がある

例）Slackで利用できるExport Options

Standard Export

- ワークスペースのOwnerとAdminがワークスペースの全パブリックチャンネルのデータをエクスポートできる
- エクスポート結果にはチャンネルが利用された日ごとのJSONファイルとリンク（Attachmentファイルそのものでなく）が含まれる

Corporate Export

- プラスプランが必要
- ワークスペースオーナーがこのタイプのエクスポートへのアクセスを申請でき、この手法であればパブリックに加えてプライベートチャンネルとダイレクトメッセージをエクスポートできる
- **このエクスポート設定が有効な間、すべてのファイルが維持されるリテンション設定が有効になる**
- 設定が有効になってから作成されたプライベートチャンネルとダイレクトメッセージのみが収集できる

Discovery API

- エンタープライズプランが必要
- 許可されたサードパーティアプリによるコンテンツのエクスポート（実際のファイル含む）が可能となる

2. Adapt to Attack & IR Process

- Fast Forensicsの課題の一つ：Forensically Sound

	Full Disk Imaging	Live Forensics & Triage
Which evidence is preserved:	Entire disk	Reports, results, and files the examiner chooses to copy
Adequate speed	✘ *Up to ten hours per disk*	✓
Reproducible	✓	✘
Verifiable	✓	✘
Duplicates evidence automatically	✓	✘
Duplicates at device level	✓	✘
Duplicates entire disk	✓	✘
Alternate lines of investigation are possible in the future	✓	✘

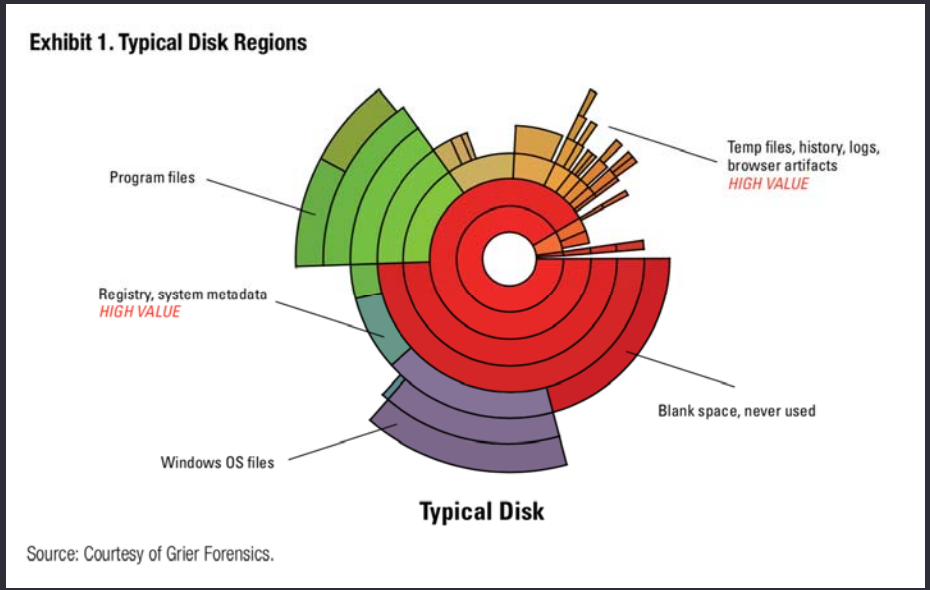
- 再現性（ライブでの実施のため、困難）
- 自動的な分析はある程度可能
- ディスク全体は複製しない（複製対象外領域の解析ができない）
- 違う視点・事案での分析が困難

引用：https://www.dfrws.org/sites/default/files/session-files/pres-rapid_forensic_imaging_of_large_disks_with_sifting_collectors.pdf

Sifting Collector (Alternative Approach)

- Fast Forensics（&Triage）の欠点を補完しつつ、Disk Imagingとの互換を持たせるアプローチ
- DFRWS 2015で考案
  - Rapid Forensic Imaging of Large Disks with Sifting Collectors By Jonathan Grier and Golden Richard
- 従来型のDisk Imagingと同様にフォレンジックイメージのフォーマット（raw、e01等）で証拠品のデータをイメージングする
- 従来型とは異なり、自動的にフォレンジック調査に関連するセクタを認識し、集めてイメージングする
  - 不必要な箇所（セクタ）はイメージングしない
  - イメージング速度は3倍以上（著者の実験ベース）
- 開発元であるGrier Forensicsから幾つかの法執行機関へ依頼し実地検証の段階

参考）https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis



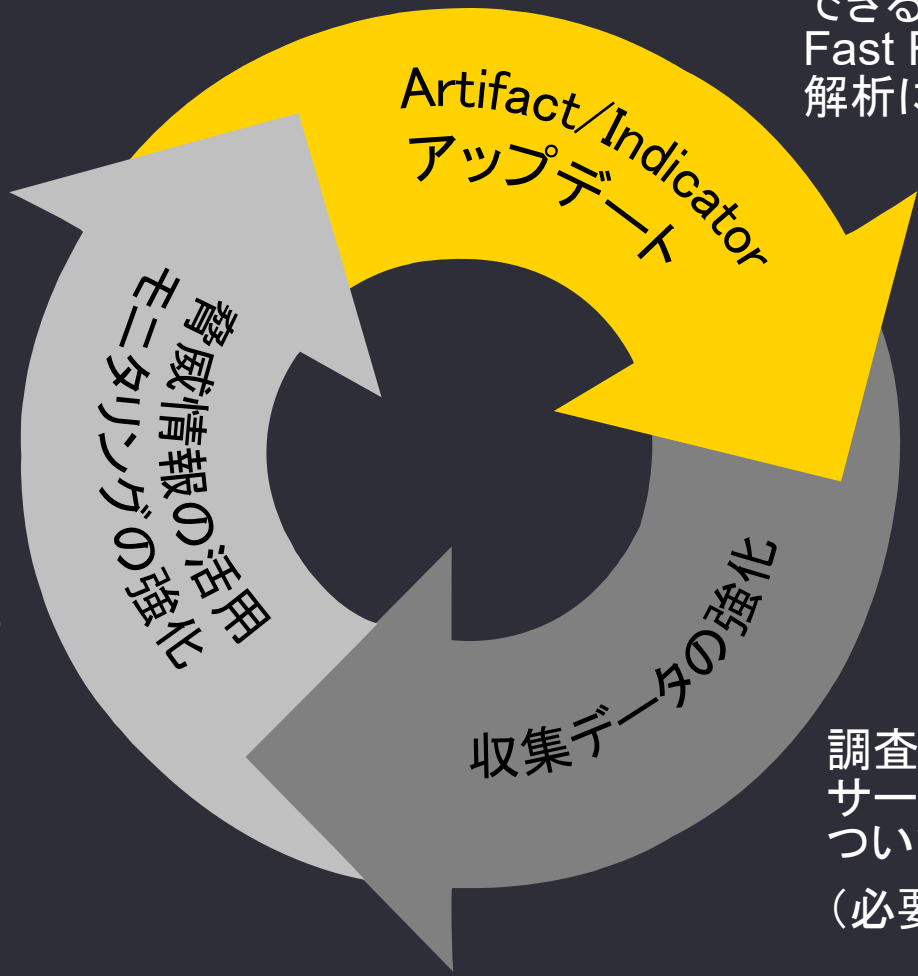
Sifting Collector (Alternative Approach)

	Full Disk Imaging	Live Forensics & Triage	Sifting
Which evidence is preserved:	Entire disk	Reports, results, and files the examiner chooses to copy	Identified sectors & regions
Adequate speed	✗ *Up to ten hours per disk*	✓	✓
Reproducible	✓	✗	✓
Verifiable	✓	✗	✓
Duplicates evidence automatically	✓	✗	✓
Duplicates at device level	✓	✗	✓
Duplicates entire disk	✓	✗	✗
Alternate lines of investigation are possible in the future	✓	✗	?

引用：https://www.dfrws.org/sites/default/files/session-files/pres-rapid_forensic_imaging_of_large_disks_with_sifting_collectors.pdf

3. Technical Measures

発見したい兆候に応じて、対応できるアーティファクトを見直し、Fast ForensicsのCollectorや解析に反映させる



Indicatorを追加するために脅威情報や既存のモニタリングを活用する

調査対象となりえるデバイスやサービスからのデータ収集について改善や範囲拡大を行う（必要に応じ）

3. Technical Measures

- 収集データの強化（例：IoTが対象となる可能性がある場合）
  - Forensicsのメソッド検討
    - テスト環境の構築、文献等のリサーチ
    - 基本アプローチ
      - Physical：活用できそうなVulnerabilityの検索、Test Port(s)等
        - Fast Forensicsではあまり使わないと想定
      - Logical：管理コンソールやモバイルアプリ、Backup等
        - モバイルフォレンジック
      - Network：ログ・トラフィック分析、ポートスキャン等
  - Fast Forensicsの必要性と現実的にできる範囲の検討

3. Technical Measures

- アプローチの例
  - 攻撃情報等から発見したIndicator、新しいアーティファクトを収集および解析できる様にCollectorやParserをメンテナンス
  - Parserで処理した複数のデータをフォレンジックツールなどで処理できるようにスクリプトやアプリケーションを整備

まとめ

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及びコピーし、解析すること
- Fast Forensicsにはツールや環境変化への対応などの課題がある
- 課題の解決に向けては下記のプロセスを実施する
  - 「組織におけるデータの場所や対応するインシデント（リスク）の把握」
  - 「攻撃や不正のフォレンジックで必要なアーティファクトの整理」
  - 「時間軸やデータ収集の手続き等のFast Forensics実施プロセスの整理」
  - 「上記の結果に基づいたFast Forensicsツールの整備等の技術的対策の実施」

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。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYについて詳しくは、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。

ED None

shinnihon.or.jp