

インシデントに対応して、そして進行中の脅威ハンティングと監視の結果として、許可/ブロックリストのコンテンツを更新する必要があります。また脅威ハンティングも戦略的な変更を引き起こす可能性があります。例えば、主に明示的な拒否に依存していて、しかしながらシステムが多数の侵入にさらされている場合は、「最小限の特権」モデルを採用し、リストに記載されていない限り拒否するアプローチを採用することを検討する必要があります。この種の変更により混乱に陥る可能性があるため、その前にリスク評価とビジネスインパクト分析を行う必要があります。

また、実行制御を効果的に構成するのは困難である可能性もあり、脅威アクターが制御を回避する機会も多くあります。攻撃の詳細な分析では、既存のメカニズムを変更する必要性や、より堅牢なシステムの使用を示す場合があります。

## 隔離

緩和策が不十分である場合や、結果が不確実な場合、エンドポイントはネットワークに再統合する前に注意深く管理する必要があります。さらなる証拠を集めめる必要がある場合、最適なアプローチは、エンドポイントまたは疑いがあるプロセス/ファイルを隔離するか、サンドボックスすることです。これにより、攻撃やツールの分析とデジタルフォレンジック技術を使用した証拠集めが可能になります。

## セキュリティのオーケストレーション、自動化、レスポンス

自動化は単一のアクティビティをスクリプト化するアクションで、オーケストレーションは複数の自動化（および場合によっては手動によるアクティビティ）を調整して複雑なマルチステップのタスクを実行するアクションです。**セキュリティのオーケストレーション、自動化、レスポンス(SOAR)**の場合、このタスクは主にインシデント対応ですが、この技術は脅威ハンティングなどのタスクにも使用できます。SOARは、平均応答時間(MTTR)として測定される、アナリストの応答能力を圧倒するアラートの量の問題に対する解決策として設計されています。SOARはスタンドアロン技術として実装するか、SIEMと統合（多くの場合次世代SIEMと呼ばれる）できます。SOARの基本は、組織内に蓄積されたセキュリティおよび脅威のインテリジェンスを精査し、機械学習/ディープラーニング技術を使用して分析し、そのデータを使用して、インシデント対応と脅威ハンティングを推進するワークフローのデータ強化を自動化して実現します。また、ユーザー アカウントの作成と削除、共有を利用可能にする、テンプレートからVMを起動するなどタスクのプロビジョニングをサポートして、設定エラーの排除を行います。SOARではクラウドやSDN/SDV API、オーケストレーションツール、サイバー脅威インテリジェンス(CTI)フィードなどの技術を使用して、管理しているさまざまなシステムを統合します。また、マルウェアのシグネチャーの自動生成やユーザーとエンティティの行動分析(UEBA)などの技術を活用して、脅威を検知します。

インシデント対応ワークフローは通常プレイブックとして定義されます。プレイブックは、特定の種類のインシデントを検知し、対応するために実行するアクションのチェックリストです。プレイブックには特定の種類のインシデントを検知するクエリ文字列やシグネチャを含めて、極めて具体的に記述する必要があります。またプレイブックには、インシデントを侵害として報告する必要があるかどうかと、通知はいつ、誰に対して行われる必要があるかなどのコンプライアンスの要因を含めます。プレイブックがSOARシステムから高度に自動化され、実装されている場合、**ランブック**と呼ばれます。2つの用語は同じ意味で広く使用されています。ランブックの目的は、できる限り多くのプレイブックの段階を自動化し、人による分析のために明確に定義された相互作用点を残すことです。こうした相互作用点では、アナリストがインシデントの緩和を進めるための最善の方法について、情報に基づいた迅速な決定を下すために必要な、すべての文脈情報とガイダンスを提示されるようにするべきです。



Rapid7では、SOARの用途を説明する電子書籍を作成しました([rapid7.com/info/security-orchestration-and-automation-playbook/?x=d67w-U](https://rapid7.com/info/security-orchestration-and-automation-playbook/?x=d67w-U))。Demistoによるホワイトペーパーでは、さまざまな組織におけるSOARの役割の概要について説明しています([cdn2.hubspot.net/hubfs/5003120/Content%20Downloads/White%20Papers/Demisto%20-%20State%20of%20SOAR.pdf](https://cdn2.hubspot.net/hubfs/5003120/Content%20Downloads/White%20Papers/Demisto%20-%20State%20of%20SOAR.pdf))。

## 敵対的な人工知能

人工知能(AI)タイプのシステムは、ユーザーとエンティティの行動分析(UEBA)に広く使用されています。UEBAは、顧客システムやハニーポットからのセキュリティデータを元に学習されます。これにより、AIでは悪意のあるコードとアカウントアクティビティの特徴を判断し、新しいデータストリームでその機能を認識できるようになります。UEBAを活用するために、ホストイベントデータとネットワークトラフィックがクラウドベースの分析サービスにストリーミングされます。検知されないネットワークへの持続的なアクセス権を持ちながらも、ラテラルムーブメントやデータの流出に影響を与える可能性が低い脅威アクターは、目的に対するアクションを達成できるツールを隠すという長期的な目標を持って、このデータストリームにトランザクションを注入する位置にいる可能性があります。脅威アクターは、独自のAIリソースをサンプルの生成手段、つまり**敵対的なAI**として使用する可能性があります。操作されたサンプルは、virustotal.comなどのパブリックリポジトリにアップロードされる場合もあります。

例えば、MLアルゴリズムは、ノイズに対して非常に敏感です。これは、画像認識ケースで実演されており、加工された亀の画像が提示されると、AIではこれをライフルとして識別します ([www.theregister.com/2017/11/06/mit\\_fooling\\_ai](http://www.theregister.com/2017/11/06/mit_fooling_ai))。人間の目には、画像はいたって普通の亀に見えます。AIに攻撃ツールをテキストエディタと誤認させるために、同様の技術が使用される可能性があります。

敵対的な攻撃の成功は、ほとんどの場合ターゲットのAIによって使用されるアルゴリズムの知識に依存します。これはホワイトボックス攻撃と呼ばれます。これらのアルゴリズムを機密にしておくと、敵対的なAIは、開発がより困難なブラックボックス技術を使用するようになります。ですがアルゴリズムの機密性はあいまいさによる機密性であり、保証するのは困難です。その他の解決策には、敵対的な例を生成し、システムでそれを認識するようにトレーニングすることが含まれます。また他のオプションとしては、敵対的なサンプルが送信されると検知し、ブロックできるフィルターの開発もあります。



BlackHatでのMicrosoftのプレゼンテーションでは、敵対的なAIを低減するために使用できる手法の一部を図解しています([i.blackhat.com/us-18/Thu-August-9/us-18-Parikh-Protecting-the-Protector-Hardening-Machine-Learning-Defenses-Against-Adversarial-Attacks.pdf](http://i.blackhat.com/us-18/Thu-August-9/us-18-Parikh-Protecting-the-Protector-Hardening-Machine-Learning-Defenses-Against-Adversarial-Attacks.pdf))。

# レビュー アク ティビティ：

## 緩和策

次の質問にお答えください。

1. 侵入イベントを封じ込めるためのセグメンテーションベースのアプローチを容易にする低レベルのネットワーク機能は何ですか？
2. 開発者アカウントの不正使用を防ぐために、どのような構成の変更が有効ですか？
3. あなたは、ローカルネットワークからパブリッククラウドストレージネットワークに重要なIPが流失した後、ある種のアウトバウンドフィルタリングシステムを実装することにしました。フィルターを実装するのに最適な技術はどれですか？
4. ある脅威アクターはVPNを通じてリモートネットワークへのアクセスを得ました。あなたはその後、ハッキングされたアカウントのユーザーがパスワードを入力しているところが盗撮されている映像を発見しました。この侵害を防ぐことができたエンドポイントセキュリティソリューションの種類はどれですか？
5. 次の記述は正しいですか、誤りですか？SOARは完全に自動化されたインシデント対応ソリューションを提供することを目的としています。
6. あなたはエンドポイント保護ソフトウェアの更新を何日も行っていないクライアントワークステーションを調査しています。そのワークステーションで、ランダムな名前が付いた大量の実行可能ファイルを発見しました。ローカルエンドポイントログで、すべてのファイルがスキャンされ、マルウェアと識別されていることが明らかになりました。ネットワークにはそれ以上の侵入の形跡はありません。この脅威アクターの動機として、考えられるものは何ですか？

# レッスン17

## 概要

効果的なインシデント対応に関するプロセスと手順を説明し、侵入イベントを緩和するための戦略を実装できる必要があります。

### インシデント対応を実行する際のガイドライン

インシデント対応のポリシーと手順を作成または改善するには、次のガイドラインに従います。

- 準備、識別、封じ込め、根絶、回復、教訓の手順に従って、構造化されたインシデント対応を実装するための目標を特定します。
- 適切な通信リソースとポリシーを備えたCIRT/CERT/CSIRTを組織し、効果的なインシデント対応に備えます。
- 分析を容易にするために攻撃フレームワーク（キルチェーン、ダイヤモンドモデル、MITRE ATT&CK）を使用して、インシデント分類システムを開発し、個別のインシデントのシナリオ用のインシデント対応プラン(IRP)とプレイブックを準備します。
- 汚染されたトレーニングデータ攻撃からAI支援システムを保護するように注意しながら、SOARと自動化されたランプックを実装することでより効果的な対応を提供できるかどうかを検討します。
- SIEMまたはsyslogを構成し、適切なデータソースを集約して、ダッシュボードにアラート、ステータスインジケーター、傾向分析を表示する相関ルールを作成します。
  - ホストログファイルのデータソース（ネットワーク、システム、セキュリティ、脆弱性スキャン出力）。
  - アプリケーションログファイルのデータソース（DNS、Web、VoIP）。
  - ネットワークパケットと侵入検知データ。
  - ネットワークトラフィックとプロトコルフローの統計。
- インシデント対応の封じ込め、根絶、回復のプロセスを、フォレンジックな証拠の収集、災害復旧、事業継続の手順と統合します。
- 分離とセグメンテーションを介して封じ込めの標準戦術を特定します。
- 回復プロセスで、ファイアウォール、コンテンツフィルター、MDM、DLP、証明書セキュリティ、エンドポイントアプリケーション制御に必要な構成の変更が適用されているようにします。

# レッスン18

## デジタルフォレンジクスを説明する

### レッスン概要

インシデント対応で悪意のあるアクティビティの迅速な根絶が強調されるのに対し、デジタルフォレンジクスでは、持続的なキャプチャ、保存、検証可能な方法を使用した証拠の分析が必要となります。あなたは、セキュリティインシデントの詳細の調査支援と脅威アクターの特定のために呼ばれる可能性があります。こうした調査を支援するには、法的措置や戦略的な敵対情報活動に使用できるフォレンジックな証拠の収集と処理に関する基本的な概念を要約できる必要があります。

### レッスンの目的

このレッスンの内容は、以下のとおりです。

- デジタルフォレンジクス文書の主な側面について説明する。
- デジタルフォレンジクスの証拠取得の主な側面について説明する。

# トピック18A

## デジタルフォレンジクス文書の主な側面について説明する



### 対象試験範囲

4.5デジタルフォレンジックの重要な側面について説明できる

文書化は、有効なデジタル証拠の収集、保存、提示に重要になります。処理の記録にミスやギャップがあると、証拠が却下される場合があります。フォレンジクス文書の主な側面について説明し、調査員を効率的にサポートできるようになってください。

### デジタルフォレンジクスの主な側面

デジタルフォレンジクスは、裁判所で受け入れられる基準の証拠をコンピューターシステムから収集する手法です。フォレンジクス調査は多くの場合、特に機器の悪用や不正使用（卑猥なコンテンツをダウンロードしたり保存するなど）といったインサイダーの脅威から生じる犯罪に対して行われます。脅威アクターは別の国にいたり、有効な手順を講じて居場所や身元を隠蔽している可能性が高いため、多くの場合、外部の脅威ソースを起訴することは困難です。そうした起訴は通常法執行機関によって開始され、脅威は軍や政府機関に向けられているか、組織犯罪に関わっています。

### 証拠、文書化、許容可能性

DNAや指紋と同様に、デジタル証拠は潜在的なものです。「潜在」とは、証拠が裸眼では見えず、機械または処理を通じて解釈される必要があることを意味します。これは、デジタル証拠の許容可能性を確保するために慎重に扱う必要があることを意味しています。物的証拠（ハードドライブなど）と同様、デジタルフォレンジクスでも証拠が改ざんや偏見なく、どのように収集され、分析されたのかを示す文書が必要になります。

**デューブロセス**とは、米国や英国のコモンローで使用される用語で、その土地の法律が公平に適用されたあとにのみ、犯罪の有罪判決を受けることです。より一般的には、公平さを確保するために一連の手続き上の保護手段を設けることと捉えることができます。この原則は、フォレンジック調査の中核となります。フォレンジック調査が開始された場合（またはその可能性がある場合）、調査で実施されるプロセスについて技術者と管理者が認識しておくことが重要です。こうした人員は、調査員を補助できなければならず、調査を妨げるようなことをしてはなりません。裁判では、被告の弁護士は証拠またはその収集プロセスの完全性に関する不確実性や誤りを突こうとします。

多くの場合、検知と通知に続く、最初の応答期間は重要になります。しっかりと証拠を集めるには、従業員がパニックにならず、調査を危うくするような行動をしないことが重要です。

## 訴訟ホールド

訴訟ホールドとは、訴訟に関連する可能性のある情報は保存される必要があるという事実を指します。訴訟ホールドの対象となる情報は、監督機関や業界のベストプラクティスによって定義される場合や、法執行機関や民事訴訟を追求する被告の弁護士からの訴訟通知である場合があります。これは、コンピューターシステムが証拠として見なされ、それに伴ってネットワークが明らかに混乱する可能性があることを意味しています。

## 証拠保全の一貫性

**証拠保全の一貫性**の文書は、証拠の収集から分析、保管、そして最終的な提示に至るまで、証拠の完全性と適切な取り扱いを強化します。セキュリティ侵害が法廷に持ち込まれた場合、企業は、証拠保全の一貫性によって証拠の捏造や収集時点以降の改ざんという疑惑から保護されます。証拠を取り扱うすべての担当者は、使用した方法とツールを記録する必要があります。

## デジタルフォレンジクスレポート

デジタルフォレンジクスレポートでは、デジタルデータの重要な内容と調査員の分析からの結論が要約されています。フォレンジクス分析は、強力な倫理原則によって導かれる必要があることに注意してください。

- 分析は、偏見なく行われなければなりません。結論と意見は、分析における直接的な証拠からのみ述べられるべきです。
- 分析方法は、同じ証拠にアクセスできるサードパーティによって再現できる必要があります。
- 理想的には、証拠を変更または操作してはなりません。証拠として使用されたデバイスを、分析を促すために操作する必要がある場合（携帯電話のロック機能を無効にしたり、リモートワイプを防ぐなど）、そうする理由が適切であり、そのプロセスは記録される必要があります。

被告の弁護士は、フォレンジクス調査員の結果を却下するために、倫理的および専門的な行動の逸脱の活用を試みる可能性があります。

## eディスカバリー

電子的に保存された情報(ESI)が含まれる固定ドライブなどのデバイスのフォレンジック調査では、ドライブ全体（割り当てられたセクターと割り当てられていないセクターの両方など）の検索が必要になります。**eディスカバリー**とは、フォレンジック調査によって集められたすべてのデータから、関連する証拠を選別し、裁判の証拠として使用できるような形式でデータベースに保存する手段です。このプロセスを支援するために、eディスカバリーソフトウェアツールが開発されています。eディスカバリースイートの機能の一部は次のとおりです。

- ファイルとメタデータの特定と重複排除 - コンピューターシステムにある多くのファイルは、「標準」のインストール済みファイルまたは同じファイルのコピーです。eディスカバリーでは、この種のファイルをフィルタリングし、分析する必要のあるデータの量を減らします。
- 検索 - 調査員が訴訟に関連するファイルを検索できるようにします。キーワード検索のほか、ソフトウェアがセマンティック検索をサポートする場合もあります。セマンティック検索では、キーワードが特定のコンテキストに対応している場合に、キーワードに一致させます。
- タグ - 標準化されたキーワードまたはラベルをファイルやメタデータに適用し、証拠を整理できます。タグは、訴訟や訴訟の一部への関連性を示したり、機密性を示すためなどに使用される場合があります。
- セキュリティ - いかなる場合でも、証拠は改ざんされることなく保存、送信、分析されていることが示される必要があります。
- 開示 - 訴訟手続きでは、同じ証拠が原告と被告の両方で利用できるようにすることも重要です。eディスカバリーによりこの要件を満たすことができます。最近の訴訟では、訴訟の両当事者に対し、紙面による記録ではなく、検索可能なESIの提出が求められています。

## 動画と目撃者の事情聴取

フォレンジクス調査の最初の段階は、現場を記録することになります。写真や（理想的には）ビデオや音声を使用して、犯行現場を記録する必要があります。調査員は、証拠の特定、収集、処理において取った行動をすべて記録する必要があります。



問題が裁判に発展した場合、実際に裁判が行われるのは数か月後、ときには数年後になる可能性があることを忘れないでください。印象と行動を書き留めておくことが極めて重要です。また、配備されているCCTVシステムやWebカメラで貴重な証拠がキャプチャされている可能性も考慮してください。

可能であれば、フォレンジックソフトウェアツールを使用して、ライブシステムから証拠を収集します。キャプチャされたデジタルデータがこれらのツールによってできる限り変更されないようにすることが極めて重要です。

調査員は、デジタル証拠だけでなく、目撃者に事情聴取を行い、現場で何をしていたか、疑わしい振る舞いや行動を目撲したかどうか、そしてコンピューターシステムに関する情報を収集するべきです。調査員は、インシデントを取り巻く状況をまず理解するために、非公式に質問をして、その回答をメモとして記録する場合があります。また調査員は、目撃者が信頼できる情報を提供するようにし、特定の結論に証人を導くことを避けるために、慎重に質問する必要があります。目撃者の証言を音声または動画で記録することで、より信頼性の高い記録を作成できますが、証人が証言を行いたくなる可能性があります。証人が証言を強いられる場合、雇用契約（証人が従業員の場合）と法的代理人の権利に関する法的問題が発生します。

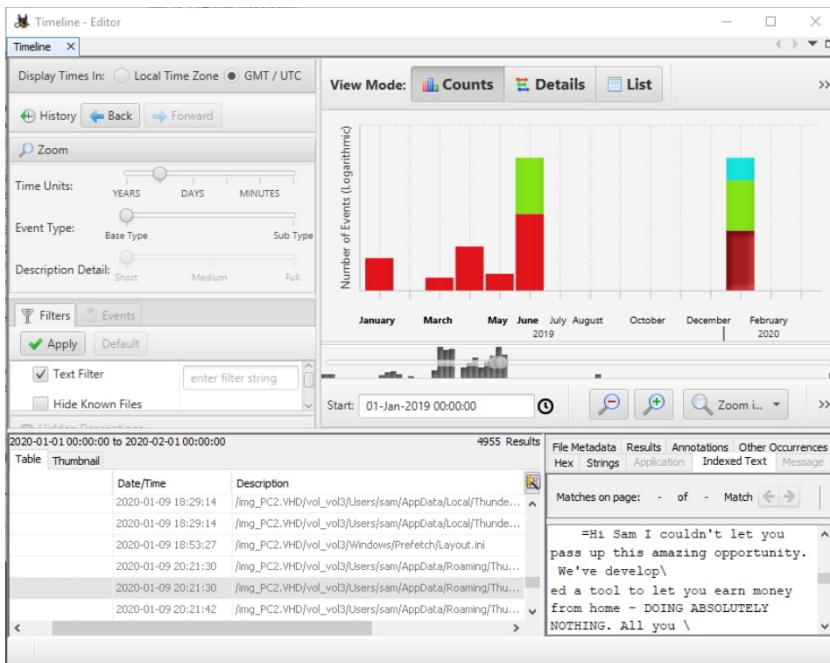
## タイムライン

フォレンジック調査の重要な部分は、一貫性のある検証可能な説明を行うために、イベントを特定の時間に関連付けることになります。時系列で発生するイベントの視覚的表現は、タイムラインと呼ばれます。

オペレーティングシステムとファイルシステムでは、さまざまな方法で何かが発生した時間を特定します。基準となる時間は、主にグリニッジ子午線の時間である、協定世界時(UTC)になります。現地時間は特定のタイムゾーン内の時間であり、UTCから数時間（場合によっては30分単位）の時差があります。夏時間が設けられている場合、現地の**タイムオフセット**も異なる場合があります。

NTFSでは、「内部」でUTCを使用しますが、多くのOSやファイルシステムでは、現地のシステムの時間としてタイムスタンプを記録します。証拠を収集する場合、タイムスタンプがどのように計算されているかを確立し、現地のシステムの時間とUTCの間の時差を記録することが重要になります。

またフォレンジクスでは、ホストのシステムクロックが、有効なタイムソースに正確に同期されていない場合や、改ざんされている場合があることも考慮する必要があります。ほとんどのコンピューターは、ネットワークタイムプロトコル(NTP)サーバーに時計を同期するように構成されています。認証と監査システムが正しく機能するには、厳密に同期された時間が重要になります。通常、コンピューターの時間を変更する権限は、管理者レベルのアカウント（企業ネットワークの場合）に制限され、時間を変更する場合はログに記録されるべきです。



Autopsyを使用してディスクイメージからイベントのタイムラインを生成。  
(スクリーンショット : Autopsy - Sleuth Kit [sleuthkit.org/autopsy](https://sleuthkit.org/autopsy))

## イベントログとネットワークトラフィック

デジタル証拠は、ホストシステムのメモリとデータドライブの分析から引き出されるだけとは限りません。調査では、1つまたは複数のネットワークアプライアンスやサーバーホストのイベントログが取得されることもあります。同様に、ネットワークパケットのキャプチャとトレース/フローによって貴重な証拠が提供される可能性があります。通常のネットワーク、センサー、ロギングシステムは、すべてのネットワークトラフィックを記録するように構成されていません。これは、そのように構成すると大量のデータが生成される可能性があるためです。一方で、十分なITリソースを持つ組織では、大量のデータを保存できる場合もあります。遡及的ネットワーク分析(RNA)ソリューションでは、パケットヘッダーまたはペイロードレベルのいざれかでネットワークイベントを記録する方法を提供します。

フォレンジクスでは、物的証拠（データドライブ）でサポートされていないデータレコードが法廷で認められるためには、多くのテストを満たす必要があります。イベントログでは、ドライブにアクセスできない場合や、元のログが保持されていない場合があります。ネットワークトラフィックには、物的証拠はありません。ログとネットワークトラフィックがSIEMで取得される場合、SIEMでは正確度（関連するすべてのデータが取得されたこと）と完全性（どちらの当事者もデータを改ざんできなかったこと）を実証する必要があります。

## 戦略的インテリジェンスと敵対情報活動

組織は場合によって、法的措置を予期せずにフォレンジクス調査を実施することがあります。フォレンジクスは法的手続きで使用されるだけでなく、サイバーセキュリティにも役立てられます。フォレンジクスにより、利用可能なデジタル証拠を綿密に調査することで、過去の侵入または現在進行中の未知の侵入を検知できます。Ciscoの元CEOのJohn Chambers氏による有名な言葉：「企業には2種類ある。ハッキングされた企業と、ハッキングされたことに気付かない企業だ」は、その点を示しています。

デジタルフォレンジクスを情報収集に使用し、スパイ活動やハッキングから保護できます。このインテリジェンスは次の2つの方法で展開されます。

- 敵対情報活動 - 特定の敵の戦術、技術、手順(TTP)の識別と分析は、実際のログ・システムをどのように設定・監査すれば、侵入の試みと成功の証拠を捕らえる方法についての情報を提供します。
- 戰略的インテリジェンス - 実用的な知見を得るために分析されたデータおよび研究。これらの知見は、成熟したサイバーセキュリティ能力を構築するために、リスク管理とセキュリティ制御の設定に活用されています。

# レビュー アク ティビティ： デジタルフォレンジクス文書

次の質問にお答えください。

1. デジタル証拠が潜在的であるという事実の重要性は何ですか？
2. フォレンジック調査時の犯行現場での最初の行動は何であるべきですか？
3. ファイルのタイムスタンプで犯行時の時間が示されないことがある理由は何ですか？
4. あなたは、フォレンジックプロセスで自分の役割を遂行し、分析チームに証拠を提供しようとしています。この移行時に注意するべき重要なプロセスは何ですか？またその理由は何ですか？

# トピック18B

## デジタルフォレンジクスの証拠取得 の主な側面について説明する



### 対象試験範囲

- 4.1 与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティを評価することができる  
4.5 デジタルフォレンジックの重要な側面について説明できる

コンピューターhosutやネットワークからさまざまなデジタル証拠を取得する際のプロセスとツールは数多く存在します。こうしたプロセスでは、証拠がどのように取得されたか、そしてそれがイベント発生時のシステムの状態の真のコピーであることを正確に実証する必要があります。あなたは証拠取得を先導する責任はないかもしれません、使用されるプロセスやツールに精通し、必要に応じて支援できるようになるべきです。

### データ収集と揮発性の順序

**収集**とは、証拠として保全されたデバイスから法的にクリーンなデータのコピーを取得するプロセスです。コンピューターシステムやデバイスが当該組織の所有物でない場合、検索または没収が法的に有効であるかどうかの疑問が発生します。これは、**デバイス持ち込み(BYOD)**ポリシーに影響を及ぼします。例えば、ある従業員が詐欺の罪に問われている場合、その従業員の機器とデータを法的に押収して検索できることを確認する必要があります。そこを誤ると、検索によって入手した証拠がすべて認められなくなる可能性があります。

また**データ収集**は、物理的な犯行現場よりもデジタル犯行現場から証拠を取得する方が難しいという事実によっても複雑になっています。コンピューターシステムの電源が切られる一部の証拠は失われてしまいますが、逆にシステムの電源が切られるまで取得不可能な証拠もあります。さらに、システムがシャットダウンされたか、突然電源を遮断することによって「フリーズ」されたかによって、証拠が失われるかどうかが変わってくる場合もあります。

データの収集は通常、ターゲットデバイスに保存されるデータからイメージを作成するツールによって行われます。イメージは、揮発性または不揮発性のストレージから取得できます。一般的な原則として、揮発性の高いものから低いものへ、**揮発性の順序**で証拠を取得します。ISOCの証拠収集とアーカイブに関するベストプラクティスガイド([tools.ietf.org/html/rfc3227](http://tools.ietf.org/html/rfc3227))では、一般的な順序が次のように説明されています。

1. CPUレジスタとキャッシュメモリ（ディスクコントローラー、GPUなどのキャッシュを含む）。
2. ルーティングテーブル、ARPキャッシュ、プロセステーブル、カーネル統計などの非永続的なシステムメモリ(RAM)の内容。
3. 永続的な大容量ストレージデバイス (HDD、SSD、フラッシュメモリデバイス) のデータ：
  - ・パーティションとファイルシステムのブロック、スラックススペース、空きスペース。
  - ・スワップスペース/仮想メモリ、休止ファイルなどのシステムメモリのキャッシュ。
  - ・ブラウザのキャッシュなどの一時ファイルのキャッシュ。
  - ・ユーザー、アプリケーション、OSファイル、ディレクトリ。

4. リモートロギングと監視のデータ。
5. 物理的な構成とネットワークトポロジ。
6. アーカイブメディアと印刷された文書。



Windowsのレジストリはほとんどディスク上に保存されますが、特にHKLM\Hardwareなどメモリにしか存在しないキーもあります。レジストリの内容はメモリダンプを介して分析できます。

## デジタルフォレンジクスソフトウェア

デジタルフォレンジクスソフトウェアは、デジタル証拠の取得、文書化、分析をサポートするために設計されています。ほとんどの商用フォレンジクスツールは、Windowsプラットフォームでのみ使用できます。

- EnCaseフォレンジックは、Guidance Softwareが作成したデジタルフォレンジクスケース管理製品です([guidancesoftware.com/enckease-forensic?cmpid=nav\\_r](http://guidancesoftware.com/enckease-forensic?cmpid=nav_r))。ケース管理は、組み込みパスウェイまたはワークフローテンプレートによって支援され、さまざまな種類の調査の重要な手順を示します。中核的なフォレンジクスサイトに加え、eディスクバリ（デジタル証拠管理）やEndpoint Investigator（企業のデスクトップとサーバーのネットワーク分析用）向けに個別の製品があります。
- AccessDataの**Forensic Toolkit (FTK)** ([accessdata.com/products-services/forensic-toolkit-ftk](http://accessdata.com/products-services/forensic-toolkit-ftk))も、Windows Server（またはサーバークラスター）で実行するよう設計された商用調査スイートです。
- **Sleuth Kit** ([sleuthkit.org](http://sleuthkit.org))は、ディスクイメージングとファイル分析のためのコマンドラインツールとプログラミングライブラリのオープンソースコレクションです。**Autopsy**は、こうしたツールのグラフィカルなフロントエンドで、ケース管理/ワークフローツールとして機能します。さまざまな分析機能のためにプログラムはプラグインで拡張できます。AutopsyはWindowsで利用でき、ソースコードからコンパイルすればLinuxでも実行できます。
- X-Waysの**WinHex** ([x-ways.net/winhex](http://x-ways.net/winhex))は、バイナリデータのフォレンジックリカバリと分析のための商用ツールで、さまざまなファイルシステムとメモリダンプタイプ（バージョンによって異なります）をサポートしています。
- Volatility Framework ([github.com/volatilityfoundation/volatility](http://github.com/volatilityfoundation/volatility))はシステムメモリの分析に幅広く使用されています。

## システムメモリの取得

システムメモリは、ランダムアクセスメモリ(RAM)モジュールで保存される揮発性データです。揮発性とは、電源を切るとデータが失われることを意味します。システムメモリのダンプでは、実行しているプロセス、一時ファイルシステムの内容、レジストリデータ、ネットワーク接続、暗号化キーなどを特定するために分析できるイメージファイルを作成します。また、マスクトレージデバイスに保存される場合に暗号化されたデータにアクセスする方法にもなります。システムメモリの内容を収集する方法はさまざまあります。

| Offset(V)           | Name           | PID  | PPID | Thds | Hnds | Sess  | Wow64 | Start                        | Exit |
|---------------------|----------------|------|------|------|------|-------|-------|------------------------------|------|
| 0xfffffa83020a7040  | System         | 4    | 0    | 106  | 632  | ----- | 0     | 2020-01-09 21:20:03 UTC+0000 |      |
| 0xfffffa8303d6d1d0  | smss.exe       | 308  | 4    | 2    | 29   | ----- | 0     | 2020-01-09 21:20:03 UTC+0000 |      |
| 0xfffffa8303f26a0   | csrss.exe      | 396  | 388  | 8    | 378  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83034fe060  | wininit.exe    | 432  | 388  | 3    | 75   | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83036295e0  | csrss.exe      | 444  | 424  | 8    | 293  | 1     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa8303716b30  | winlogon.exe   | 492  | 424  | 3    | 109  | 1     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83035fab30  | services.exe   | 528  | 432  | 10   | 276  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa830373db30  | lsass.exe      | 536  | 432  | 8    | 636  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa830373db30  | lsm.exe        | 544  | 432  | 10   | 142  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83037436a0  | svchost.exe    | 652  | 528  | 10   | 349  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83037e66a0  | svchost.exe    | 716  | 528  | 7    | 235  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83036566a0  | svchost.exe    | 772  | 528  | 18   | 445  | 0     | 0     | 2020-01-09 21:20:05 UTC+0000 |      |
| 0xfffffa83038b0e60  | svchost.exe    | 892  | 528  | 18   | 417  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa83038fcb30  | svchost.exe    | 936  | 528  | 32   | 948  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa830393c660  | svchost.exe    | 324  | 528  | 17   | 385  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa8303960060  | svchost.exe    | 744  | 528  | 15   | 379  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa83039b7060  | spoolsv.exe    | 1068 | 528  | 12   | 271  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa83039dd060  | svchost.exe    | 1096 | 528  | 19   | 316  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa8303a58960  | vmicsvc.exe    | 1192 | 528  | 5    | 126  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa8303a7b030  | vmicsvc.exe    | 1216 | 528  | 7    | 217  | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa8303a8c060  | vmicsvc.exe    | 1264 | 528  | 4    | 78   | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa83039accb30 | vmicsvc.exe    | 1296 | 528  | 5    | 92   | 0     | 0     | 2020-01-09 21:20:06 UTC+0000 |      |
| 0xfffffa8303b2920   | vmicsvc.exe    | 1348 | 528  | 3    | 82   | 0     | 0     | 2020-01-09 21:20:07 UTC+0000 |      |
| 0xfffffa8302ab2310  | svchost.exe    | 1436 | 528  | 10   | 179  | 0     | 0     | 2020-01-09 21:20:07 UTC+0000 |      |
| 0xfffffa8303bcf800  | svchost.exe    | 1528 | 528  | 3    | 43   | 0     | 0     | 2020-01-09 21:20:08 UTC+0000 |      |
| 0xfffffa8303c963a0  | svchost.exe    | 1816 | 528  | 5    | 99   | 0     | 0     | 2020-01-09 21:20:08 UTC+0000 |      |
| 0xfffffa8303ac5b30  | svchost.exe    | 1976 | 528  | 14   | 323  | 0     | 0     | 2020-01-09 21:20:10 UTC+0000 |      |
| 0xfffffa830315b30   | taskhost.exe   | 1964 | 528  | 9    | 157  | 1     | 0     | 2020-01-09 21:20:14 UTC+0000 |      |
| 0xfffffa83031c3830  | sppsvc.exe     | 2072 | 528  | 7    | 158  | 0     | 0     | 2020-01-09 21:20:14 UTC+0000 |      |
| 0xfffffa8303262060  | dwm.exe        | 2352 | 892  | 3    | 70   | 1     | 0     | 2020-01-09 21:20:18 UTC+0000 |      |
| 0xfffffa8303238060  | explorer.exe   | 2376 | 2344 | 24   | 784  | 1     | 0     | 2020-01-09 21:20:18 UTC+0000 |      |
| 0xfffffa8303a2b30   | jusched.exe    | 2528 | 2456 | 8    | 233  | 1     | 1     | 2020-01-09 21:20:18 UTC+0000 |      |
| 0xfffffa8303ba0b30  | SearchIndexer. | 2568 | 528  | 11   | 656  | 0     | 0     | 2020-01-09 21:20:24 UTC+0000 |      |
| 0xfffffa830326a060  | procexp64.exe  | 2900 | 2376 | 8    | 382  | 1     | 0     | 2020-01-09 21:20:45 UTC+0000 |      |
| 0xfffffa83036406a0  | WmiPrvSE.exe   | 3024 | 652  | 7    | 118  | 0     | 0     | 2020-01-09 21:20:51 UTC+0000 |      |
| 0xfffffa8303703190  | Tcpview.exe    | 916  | 2376 | 6    | 139  | 1     | 1     | 2020-01-09 21:21:27 UTC+0000 |      |
| 0xfffffa8302839b30  | salter.exe     | 1808 | 2376 | 6    | 134  | 1     | 1     | 2020-01-09 21:23:49 UTC+0000 |      |
| 0xfffffa8303818230  | WMIADAP.exe    | 380  | 936  | 5    | 85   | 0     | 0     | 2020-01-09 21:24:08 UTC+0000 |      |

Volatility Frameworkを使用してメモリダンプでプロセスリストを表示。  
(スクリーンショット : Volatility Framework [volatilityfoundation.org](http://volatilityfoundation.org))

## ライブ取得

特別なハードウェアやソフトウェアツールを使用すると、ホスト実行中にメモリの内容を取得できます。残念なことにこのタイプのツールは、関心のあるデータをダンプするためにカーネルモードのドライバーを必要とするため、プレインストールされる必要があります。Windows用の例には、WinHex ([x-ways.net/winhex](http://x-ways.net/winhex))、FireEyeのMemoryze ([fireeye.com/services/freeware/memoryze.html](http://fireeye.com/services/freeware/memoryze.html))、F-Response TACTICAL ([f-response.com/software/tac](http://f-response.com/software/tac))などがあります。

Linuxでは、[memdump \(porcupine.org/forensics/tct.html\)](http://memdump.porcupine.org/forensics/tct.html)やddなどのユーザー モードツールを /dev/mem デバイスファイルに対して実行できますが、ほとんどの最新ディストリビューションでは、このファイルへのアクセスはブロックされています。Volatility Framework ([github.com/volatilityfoundation/volatility](https://github.com/volatilityfoundation/volatility))には、カーネルドライバー (pmem) をインストールするツールが含まれています。fmemとLiMEのカーネルユーティリティでは同様の機能が提供されます。

## クラッシュダンプ

Windowsで回復不能なカーネルエラーが発生する場合、メモリの内容を \Windows\MEMORY.DMP のダンプファイルに書き込むことができます。最近のシステムでは、ディスク領域が大量に占有されるため、メモリのすべての内容がダンプされる可能性はほとんどありませんが、C:\Windows\Minidumps に保存されるミニダンプファイルでも、貴重な情報源になる可能性があります。

## 休止ファイルとページファイル

休止ファイルは、Windowsホストがスリープ状態になったときに、ブートボリュームのルートフォルダー内に作成されます。データが回復可能な場合は、分析のために解凍し、ソフトウェアツールに読み込むことができます。欠点は、ネットワーク接続が閉じられ、マルウェアによりスリープ状態の使用が検知され、[フォレンジクス対策](#)が実行される可能性があることです。

ページファイル/スワップファイル/スワップパーティションには、ホストのRAMモジュールの容量を超える使用中のメモリのページが保存されます。ページファイルは分析ツールで解釈できるように構成されていませんが、文字列は検索できます。

## ディスクイメージの取得

ディスクイメージの取得とは、非揮発性ストレージからデータを取得することを指します。非揮発性ストレージには、ハードディスクドライブ(HDD)、ソリッドステートドライブ(SSD)、ファームウェア、その他の種類のフラッシュメモリ(USBフラッシュドライブやメモリカード)、光学メディア(CD、DVD、Blu-Ray)が含まれます。これはデバイスの取得とも呼ばれ、スマートフォンやメディアプレーヤーのSSDストレージを意味します。またブートボリュームが含まれる場合、ディスクの取得では、OSインストールもキャプチャします。

固定記憶領域の取得では次の3つのデバイス状態があります。

- ライブ取得 - これは、ホストが実行している間にデータをコピーすることを意味します。これは、分析用により多くの証拠やデータを取得し、全体的なサービスへの影響を低減できる可能性がありますが、実際のディスクにあるデータが変更されるため、この方法では法的に認められる証拠が得られない場合があります。また、脅威アクターにもアラートするので、フォレンジクス対策を講じる時間を与えてしまう可能性があります。
- ホストをシャットダウンすることによる静的取得 - これは、マルウェアがシャットダウンプロセスを検知し、フォレンジクス対策を実行してマルウェアのトレースを排除しようとするリスクがあります。
- プラグを外すことによる静的取得 - これは、コンセントから電源を抜くことを意味します(ハードウェアの電源ボタンをオフにするではありません)。これは、フォレンジック的にクリーンな状態でストレージデバイスを保全する可能性は高いのですが、データが破損するリスクがあります。

現場で十分な時間が与えられる場合、ライブ取得と静的取得の両方を実施できます。どの方法を使用しても、講じた手順を記録し、行動のタイムラインを取得する必要があります。

Forensic ToolkitとFTK Imagerなどスイートでパッケージ化されたものを含め、数多くのGUIイメージングユーティリティがあります。EnCaseフォレンジクススイートでは、ddなどのLinuxのツールで使用される未加工ファイルではなく、ベンダーファイル形式(.e01)が使用されることに注意してください。イメージの分析にツールを選択する際は、ファイル形式が重要になります。.eo1形式を使用すると、イメージのメタデータ(チェックサム、ドライブジオメトリ、取得時間など)を同じファイル内に保存できます。オープンソースのAdvanced Forensic Format (AFF)では、同様の機能が利用できます。

専用のツールを利用できない場合、Linuxホストでは**ddコマンド**を使用して入力ファイル(if=)を出力ファイル(of=)にコピーして、そのファイルデータに任意の変換を適用できます。次のsdaは固定ドライブです。

```
dd if=/dev/sda of=/mnt/usbstick/backup.img
```

最新のddの派生ツールはdcflddで、複数の出力ファイルや完全一致検証などの追加機能を提供します。

```
root@kali:~# dcfldd if=/dev/sda hash=sha256 of=/root/FORENSIC/ROGUE.dd bs=512 co
nv=noerror
134217728 blocks (65536Mb) written.Total (sha256): 7a72be231f393d40e0ac72c62b3a7
3798f29f0ca7e0e279b8aececa291a34137

134217728+0 records in
134217728+0 records out
root@kali:~# sha256sum /dev/sda
7a72be231f393d40e0ac72c62b3a73798f29f0ca7e0e279b8aececa291a34137  /dev/sda
root@kali:~#
```

*dcfldd (DoDによって作成された追加フォレンジクス機能のあるddのバージョン) を使用し、ソースディスクデータ(sda)のハッシュを生成。*

## 証拠の保全と完全性

犯行現場で収集された証拠が有効な**タイムライン**と合致することが極めて重要です。デジタル情報は改ざんされやすいため、証拠へのアクセスを厳格に制限する必要があります。プロセス全体を記録することで、犯行現場から直接得た証拠の出所が確立されます。

不揮発性ストレージからフォレンジック的に健全なイメージを取得するには、ソースディスクやファイルシステムのデータまたはメタデータ（プロパティ）を変更しないようにする必要があります。書き込みブロックバーは、ドライバーとOSレベルで書き込みコマンドをフィルタリングすることにより、ディスクまたはボリューム上のデータが変更されないようにすることで、このプロセスを保証します。データ収集は通常、ターゲットデバイスを書き込みブロックバーが搭載されたフォレンジクスワークステーションまたはフィールドキャプチャデバイスに取り付けて行います。

### 完全性と否認防止を伴うデータ収集

ターゲットディスクがフォレンジクスワークステーションに安全に取り付けられたら、データ収集は次のように実行されます。

1. ディスクメディアの暗号化ハッシュが、MD5またはSHAハッシュ関数のいずれかで作成されます。関数の出力はチェックサムとして記述できます。
2. メディアのビットごとのコピーが、イメージングユーティリティを使って作成されます。
3. 次にイメージの第2のハッシュが作成されます。これは元のメディアのハッシュに一致しているはずです。
4. コピーが参照イメージから作成され、チェックサムで再検証されます。分析はコピーで実行されます。

この完全性の証明により、否認防止が保証されます。証拠の出所が確実である場合、証拠の分析によって特定された脅威アクターは、その行動を否定することはできません。チェックサムは、イメージに変更が加えられていないことを証明します。



実際には、イメージ取得ソフトウェアが取得プロセスの一部として検証ステップを実行しますが、理論的には、個別のツールを使用して各段階を個別に実行できます。

## 証拠の保全

犯行現場からのホストデバイスとメディアはラベル付けし、不正開封を防止する袋に入れて密閉されるべきです。また、袋に静電気防止処理が施されたものを使用して、静電放電(ESD)によって電子メディアのデータが損傷または破損する可能性を低減する必要があります。証拠は1個ずつ、証拠保全の一貫性フォームによって記録されるべきです。これには証拠の収集場所、日時、担当者、その後の取扱者、保管場所が記録されます。

証拠はセキュアな施設に保管する必要があります。これは、アクセス制御だけでなく、結露、ESD、火災、その他の危険によって電子システムが損傷しないようにする環境制御も意味します。同様に、証拠を運搬する場合は、運搬にも安全策を講じる必要があります。

## その他のデータの収集

コンピューターシステムとネットワーク内には、他にも潜在的なフォレンジックデータのソースがありますが、取得や証拠能力があることを証明するのが難しい場合があります。

## ネットワーク

パケットキャプチャとトラフィックフローには、インシデントを記録するのに適切な時間と場所でキャプチャが実行されていた場合、非常に貴重な証拠が含まれている可能性があります。メモリフォレンジクスと同様、フォレンジクスの問題は、データの完全性を確立することにあります。ほとんどのネットワークデータは、SIEMで取得します。

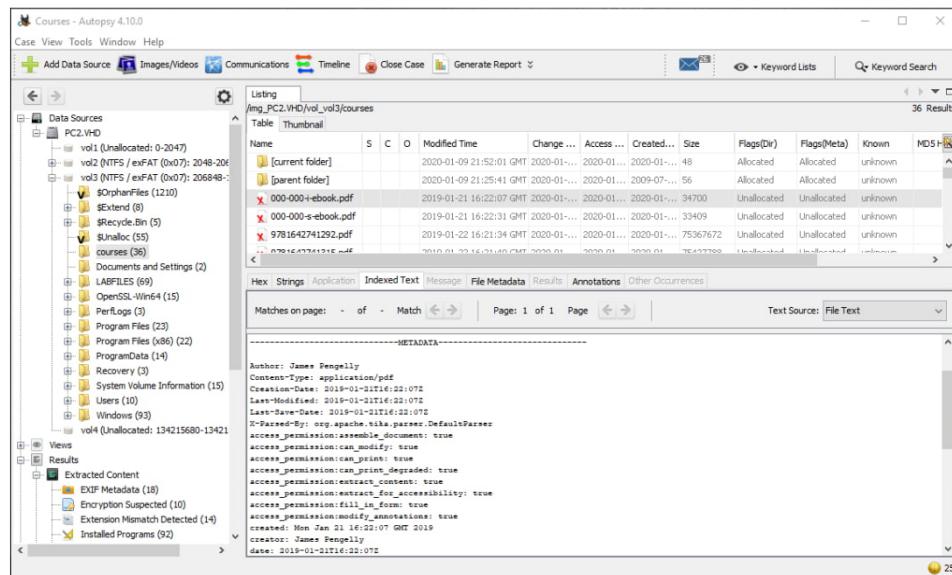
## キヤッシュ

キヤッシュは、ハードウェアのコンポーネントまたはソフトウェアのいずれかを意味します。ソフトウェアベースのキヤッシュは、ファイルシステムに保存され、ディスクイメージの一部として取得できます。例えば、各ブラウザには一時ファイルのキヤッシュがあり、各ユーザー プロファイルには一時ファイルのキヤッシュがあります。OSやアプリケーションが生成するキヤッシュの中には、レジストリの一部、暗号キー、パスワードハッシュ、ある種のCookieなど、メモリ上にのみ保持されるものがあります。ハードウェアキヤッシュ（CPUレジスタとディスクコントローラーの読み取り/書き込みキヤッシュなど）は通常回復できません。

## アーティファクトとデータ復旧

アーティファクトは、オペレーティングシステムのメインストリームデータ構造の一部ではないあらゆるデータの種類を指します。例えば、Windows **Alternate Data Streams (ADS)**機能はしばしばファイルデータを隠すために利用されます。また、PrefetchやAmecacheなどさまざまなキヤッシュは疑わしいプロセスの挙動のインジケーターを発見するために使用できます。

データ復旧とは、ディスク（またはディスクのイメージ）を分析し、空き領域に保存されているファイル断片を探し出すことです。これらのファイル断片は、削除されたファイルや上書きされたファイルである可能性があります。この復旧プロセスは、**カーピング**と呼ばれます。



Autopsyを使用したディスクイメージのファイルカーピング。選択した「コース」のフォルダとその中にあるPDFファイルは削除され、未割り当てとしてフラグされていますが、このイメージは削除直後に取得されたため、ファイルコンテンツは簡単に回復できます。（スクリーンショット：

Autopsy - Sleuth Kit [sleuthkit.org/autopsy](http://sleuthkit.org/autopsy)

## スナップショット

スナップショットは永続ディスクのライブ取得イメージです。これは書き込みブロックを使用してデバイスから取得したイメージより有効性は低い場合がありますが、仮想マシンやクラウドプロセスからデータを取得する唯一の手段である可能性があります。

## ファームウェア

ファームウェアは通常、フラッシュメモリとして実装されます。PCファームウェアなどの一部のタイプでは、デバイスまたはイメージングユーティリティを使用してシステムメモリから抽出できる可能性があります。ただし専用のハードウェアを使用して、デバイスをフォレンジクスワークステーションに取り付ける必要があることもあります。

## クラウド向けデジタルフォレンジクス

オンプレミスの調査では、デバイスを没収して分析する権利は通常、ほとんど問題はありません。システムのサービスを停止すると可用性の問題が発生し、個人所有デバイスの持ち込みポリシーがより複雑になる可能性がありますが、基本的にすべての機器は会社の所有物であるため、サードパーティの障害はありません。

企業ではプライベートクラウドを運用できますが、パブリッククラウドのフォレンジクスの場合は、クラウドプロバイダーとのサービスレベル合意書(SLA)によって許可される監査権限のために複雑になります。クラウドによってホストされる処理サービスとデータサービスのフォレンジクス調査には他にも、次の2つの問題があります。

- クラウドサービスのオンデマンドの性質のため、インスタンスは頻繁に作成され、破棄されるので、データのフォレンジックリカバリを実行する機会がありません。クラウドプロバイダーは、広範なロギングと監視のオプションにより、これをある程度軽減することができます。またCSPは、SIEMによって生成されたアラート条件に応じて、コンテナーやVMからファイルシステムとメモリのスナップショットを生成できるオプションを提供する可能性があります。
- 証拠保全の一貫性の問題は複雑で、データの選択とパッケージ化をCSPに依存しなければならない場合があります。プロセスは、できる限り厳密に文書化され、記録されるべきです。
- 管轄権とデータ主権により、CSPが公開しようとする証拠が制限される場合があります。
- CSPがデータプロセッサの場合、データ侵害通知法および規制によって制約されます。組織とCSP間における通知のタイミングと監督機関との連絡を調整することは、機密性が要求されるインシデントが発生している場合は特に、極めて複雑になる可能性があります。

# レビュー アク ティビティ：

## デジタルフォレンジクスの証拠取得

次の質問にお答えください。

1. あなたは中間者攻撃の重要な証拠として、ARPキャッシュの内容を回復する必要があります。パソコンをシャットダウンした場合、ハードドライブのイメージは保存されますか？
2. Linuxホストでディスクメディアのイメージ作成ができるコマンドラインツールは何ですか？
3. 次の記述は正しいですか、誤りですか？証拠の完全性を確保するために、イメージを作成する前にメディアのハッシュを作成する必要があります。
4. カービングツールを使用して回復できるフォレンジックデータの種類は何ですか？

# レッスン18

## 概要

証拠のセキュアな取得と取り扱いを含む、デジタルフォレンジクスの主な侧面について説明できる必要があります。

### デジタルフォレンジクスのガイドライン

フォレンジクス調査を支援する場合は、次のガイドラインに従います。

- フォレンジックデータを取り扱い、保存するための、インシデント対応担当者向けの一貫したプロセスを作成するか、導入します。
  - ホストがシャットダウンしたり、電源が切られる場合の証拠の揮発性の順序と潜在的な損失を考慮します。
  - 動画で証拠収集の記録を取り、目撃者の事情聴取をして証言を集めます。
  - WinHex、AutopsyまたはFTK Imagerなど、永続的なメディアや非永続的なメディアから証拠を取得して検証できるツールを導入します。
  - CSPからフォレンジックデータを回復する方法を確立します。
  - 証拠保全の一貫性を使用して証拠を記録します。
- 戰略的インテリジェンスと敵対情報活動のソースとしてのフォレンジック証拠の可能性に注意します。