EC-COUNCIL.312-49v11.v2026-06-24.q167

試験コード：	312-49v11
試験名称：	Computer Hacking Forensic Investigator (CHFI-v11)
認証ベンダー：	EC-COUNCIL
無料問題の数：	167
バージョン：	v2026-06-24
ページの閲覧量：	106
問題集の閲覧量：	1759

https://www.jpnshiken.com/shiken/EC-COUNCIL.312-49v11.v2026-06-24.q167.html

質問: **1**
ニューヨークの金融機関で行われたマルウェア調査中、フォレンジック調査員はWindowsフォレンジックワークステーション上で疑わしいファイルを実行した。netstat -anコマンドを使用して、ポートが
ポート1177は開設され、アクティブに接続されていました。捜査官は、観測されたポート活動が正当なサービスに関連するものか、悪意のある行為を示すものかを判断する必要があります。捜査官はこのポート活動の重要性をどのように評価すべきでしょうか？
A. ワークステーションで開かれている不審なポート番号がないかリストを確認してください。
B. オンライン港湾データベースを参照してください
C. フォレンジックワークステーションで容疑者ファイルを実行する
D. netstat -an を使用して、アクティブなすべての TCP/IP 接続とアクティブなポートの一覧を表示します。
正解: **(**正解を表示します**)**
正解はBです。調査担当者がnetstatでアクティブなポートを特定したら、次のステップはそのポートが一般的に何に関連付けられているか、またその使用が環境で想定されているかどうかを判断することです。オンラインのポートデータベースや信頼できるサービスポート参照を参照することで、アナリストはポート番号を既知のアプリケーション、登録済みのサービス、または疑わしい過去の使用パターンにマッピングできます。CHFI v11には、システムおよびネットワークレベルでのマルウェア動作分析が含まれており、ポートとネットワークアクティビティの監視も含まれているため、候補者は観察から解釈へと進むことが求められます。オプションDは、既に実行された手順を繰り返しているだけです。オプションAは、単にポートを疑わしいと呼ぶだけでは理由が説明されないため、曖昧すぎます。
オプションCは、ファイルが既に実行され、関連するネットワークアーティファクトが観測されているため、安全ではなく不要です。フォレンジックワークフローでは、未知のアクティブポートを特定した後、調査担当者は既知のサービスポート参照を通じてその意味を検証し、その知識をプロセス、宛先、およびタイミングの証拠と関連付ける必要があります。そのため、オンラインポートデータベースが最適な解決策となります。

質問: **2**
あなたは州警察のコンピュータ鑑識ラボに配属されました。注目度の高い刑事事件を担当するにあたり、あなたは適用されるすべての手順に従いましたが、上司は弁護側がラボ内で証拠が改ざんされたのではないかと疑うのではないかと懸念しています。証拠がラボに持ち込まれた時と同じ状態であることを証明するために、あなたは何ができるでしょうか？
A. 証拠のMD5ハッシュを作成し、NISTが開発した標準データベースと比較する。
B. 証拠品が研究所に持ち込まれた時と同じ状態であることを証明する声明書に署名する
C. 州立研究所は認証を受けているため、この可能性のある主張について心配する必要はありません。
D. 証拠のMD5ハッシュを作成し、証拠が最初に研究室に持ち込まれたときに取得された元のMD5ハッシュと比較する。
正解: **(**正解を表示します**)**

質問: **3**
調査担当者は、データの完全性を維持するために、ストレージメディアの内容を変更することなく、データ取得を実行する必要があります。調査担当者が採用するアプローチは、ストレージメディアへの読み取り専用アクセスを可能にする機能に依存しています。このタスクを実行するために、調査担当者はどのツールを手順に組み込むべきでしょうか？
A. 書き込みブロッカー
B. BitLocker
C. バックアップツール
D. データ複製ツール
正解: **(**正解を表示します**)**

質問: **4**
IISのデフォルトのログ保存場所はどこですか？
A. %SystemDrive%\inetpub\logs\LogFiles
B. %SystemDrive\logs\LogFiles
C. SystemDrive\logs\LogFiles
D. SystemDrive\inetpub\LogFiles
正解: **A (**コメントを発表する**)**

質問: **5**
システム管理者のアレックスは、Linuxマシン上の既存のEXT2ファイルシステムをEXT3ファイルシステムに変換する作業を任されました。EXT2ファイルシステムは現在使用中で、アレックスはそれをEXT3に変換するためにジャーナリングを有効にする必要があります。アレックスはこの変換を実行するために、以下のどのコマンドを使用すべきでしょうか？

A. C:>ECHO text_message > myfile.txt:stream1
B. C:>MORE < myfile.txt:stream1
C. dd if=mbr.backup of=/dev/xxx bs=512 count=1
D. # /sbin/tune2fs -j
正解: **(**正解を表示します**)**
CHFI v11のシラバスの「オペレーティングシステムフォレンジックとLinuxファイルシステム分析」によると、Linuxファイルシステムとその変換方法を理解することは、システム管理とフォレンジック調査の両方にとって不可欠です。EXT2ファイルシステムはジャーナリング機能を持たないファイルシステムですが、EXT3はジャーナリング機能を追加することでEXT2を拡張し、クラッシュや不適切なシャットダウン後のシステム復旧とフォレンジック追跡を大幅に改善します。
既存のEXT2ファイルシステムをEXT3に変換するための正しいコマンドは次のとおりです。
/sbin/tune2fs -j
このコマンドは、既存のデータを再フォーマットしたり破壊したりすることなく、EXT2ファイルシステムでジャーナリングを有効にします。
これにより、安全かつ効率的な変換方法となります。CHFI v11では、このコマンドがEXT2パーティションにジャーナルを追加するための標準的な方法として明示的に示されています。ジャーナリングが有効になると、ファイルシステムはEXT3として認識されます。
その他の選択肢は誤りであり、Linuxファイルシステムの変換とは無関係です。選択肢AとBはWindows固有のNTFS代替データストリームに関するものです。選択肢Cは、MBRのバックアップや復元など、RAWセクターをコピーするために使用されるディスクレベルのコマンドであり、ファイルシステムのジャーナリング機能を変更するものではありません。
CHFI試験ブループリントv4では、Linuxファイルシステム（EXT2、EXT3、EXT4）とtune2fsなどの管理コマンドに関する知識が重視されています。これらはフォレンジック分析や復旧シナリオで頻繁に参照されるため、オプションDが正解であり、試験内容に沿った回答となります。

質問: **6**
デジタルフォレンジック調査中に、MyISAMストレージエンジンを使用しているMySQLデータベースで発生したSQLインジェクション攻撃を発見しました。MySQLデータディレクトリ内で、攻撃を受けたテーブルの「MYD」ファイルと「MYI」ファイルを見つけました。また、SQLインジェクション攻撃の種類はUNIONベースの攻撃であると特定しました。調査において、以下の手順のうちどれが最も効果的でしょうか？
A. テーブルデータ内の攻撃の証拠を見つけるために「MYD」ファイルをチェックする
B. バイナリログ（HOSTNAME-bin.nnnnnn）を検査して異常なトランザクションを検出します
C. MySQLエラーログ（HOSTNAME.err）を分析して異常がないか確認する
D. '.MYI' ファイルを調査し、攻撃されたテーブルのインデックスを検査します。

正解: **B** (コメントを発表する)

質問: **7**
システム管理者は、重要なアプリケーション向けに新しいストレージアレイを構成しており、データストライピングと専用パリティを使用するRAIDレベルを選択します。このRAID構成では、最低3台のディスクが必要で、データがバイトレベルで複数のドライブにストライピングされ、1台のドライブが耐障害性のためのパリティ情報を格納するために確保されます。RAIDシステムの構成後、管理者は単一ドライブの障害に対する耐性をテストし、データ損失なしでシステムが引き続き機能することを確認します。このシナリオでシステム管理者が使用しているRAIDレベルはどれですか？
A. RAID 1
B. RAID 3
C. RAID 10
D. RAID 0
正解: (正解を表示します)
選択肢B。RAID 3が正解です。なぜなら、この問題では、専用のパリティディスクとバイトレベルのストライピングを使用し、少なくとも3つのディスクを必要とするRAIDレベルについて説明されているからです。この組み合わせはRAID 3に該当します。
CHFI v11では、デジタル証拠の基礎として、RAIDストレージシステム、RAIDと仮想化、およびストレージ構造に関するより広範な理解が明示的に含まれているため、受験者はRAIDの種類と、それらが証拠の取得と回復にどのように影響するかを認識することが求められます。
重要なポイントは、専用のパリティドライブと、ディスクが1台故障してもシステムが動作し続けることができる点です。RAID 3は、残りのストライピングされたディスクとパリティ情報からデータを再構築することで、1台のドライブの故障に対する耐障害性を提供するように設計されています。この点が、冗長性を持たないRAID 0、専用パリティを使用せずにデータをミラーリングするRAID 1、そしてストライピングとミラーリングを異なる方法で組み合わせるRAID 10とは異なります。
このシナリオは、バイトレベルのストライピングと1つのパリティディスク、そしてシングルディスクフォールトトレランスを正確に記述しているため、記述された構成に完全に適合する唯一の解決策はRAID 3です。

質問: **8**
ノースカロライナ州シャーロットにある金融会社でクラウド移行作業が行われている際、調査担当者は、高度なデータ永続性と管理機能を備えつつ、分析のスケールアウトをサポートし、高いパフォーマンスを提供する必要のあるミッションクリティカルなSQL Serverワークロード向けに、Google Cloudのストレージオプションを評価しています。これらの要件に最も適したGoogle Cloudのデータストレージサービスはどれでしょうか？
A. ローカルSSD
B. パーシステントディスク

C. ハイパーディスク
正解: **C** (コメントを発表する)
正解はCです。Google CloudはHyperdiskを推奨する耐久性のあるブロックストレージとして位置付けており、特にHyperdisk Throughputはスケールアウト分析ワークロードに適していると説明しています。Googleのドキュメントでは、HyperdiskはCompute Engine向けの最速かつ最も効率的な耐久性ディスクであると述べられており、ブロックストレージに関するガイダンスでは、スケールアウト分析のユースケース向けにHyperdisk Throughputが強調されています。これは、強力な永続性、スケーラブルなパフォーマンス、高度なストレージ管理を必要とするミッションクリティカルなSQL Server環境とよく合致しています。ローカルSSDは非常に高速ですが、ホストに紐づいており、この種のワークロードに期待されるような永続性特性は提供しません。Standard Persistent Diskは耐久性があり、幅広い用途に使用できますが、この質問ではスケールアウト分析と高性能が強調されており、ワークロードに最適化されたHyperdiskの製品の方がより適していることを示しています。CHFI v11にはクラウドプラットフォームとストレージ関連の証拠に関する考慮事項が含まれているため、受験者はクラウドサービスのパフォーマンスと耐久性プロファイルがシナリオに最も適しているかどうかを認識する必要があります。ここでは、Hyperdiskが最も適切な回答です。

質問: **9**
ある組織は、法的調査のためのデータ収集を効率的に管理することに重点を置いたeDiscovery戦略を策定しました。この戦略の一環として、法務チームは、適切な情報源から関連データのみが収集されるようにする責任を負っています。法務チームは、調査に必要な電子的に保存された情報（ESI）を含むデータソースを特定する責任があります。この場合、法務チームはeDiscoveryのどのベストプラクティスに従っているでしょうか？
A. データのマッピングを行い、管理者を特定し、データ収集場所を決定します。
B. 明確なガイドラインを提供せずに、保管者による自己回収に頼る。
C. 指示された収集を使用して、無関係なファイルも含め、管理者から入手可能なすべてのデータを取得します。
D. 収集時間とリソースを最小限に抑えるため、データは1つのソースからのみ収集します。
正解: **A** (コメントを発表する)
オプションAが最適な回答です。なぜなら、このシナリオは、収集前に関連する電子的に保存された情報（ESI）を特定し、正しい情報源を見つけることに重点を置いているからです。CHFI v11には、eDiscoveryプロセスフロー、電子情報開示参照モデル（EDRM）サイクル、eDiscoveryの収集方法/手法、およびコストとリスクを軽減するためのeDiscoveryのベストプラクティスが明示的に含まれています。また、eDiscoveryに関する法務チームとITチームの考慮事項についても言及しており、これは法務チームが必要なものだけを収集する方法を計画している状況に合致しています。
データのマッピングを行い、データ管理者を特定し、データの所在場所を突き止めることは、的を絞った収集を可能にし、不要なデータ量を削減し、コストを抑え、無関係な資料の

収集を回避するのに役立つため、中核となるベストプラクティスです。まさに質問の内容に合致しています。その他の選択肢は、健全なeディスカバリーの実践と矛盾します。ガイダンスなしでの自己収集はリスクを高め、入手可能なすべてのデータを収集することは比例性と関連性を無視することになり、単一の情報源からのみ収集することは範囲が狭すぎ、重要な証拠を見落とす可能性があります。
そのため、CHFIのeDiscoveryの目標に基づき、チームはデータ収集前にデータソースとデータ管理者をマッピングするというベストプラクティスに従っています。

質問: **10**
組織内で発生したサイバーセキュリティインシデントを受け、フォレンジック調査員は調査の一環として電子的に保存された情報（ESI）を収集する任務を負います。データ収集プロセスを効率化するため、調査員は保管者からESIの範囲とサイズを制限し、収集対象をコンピュータ上の特定のファイルタイプとディレクトリに限定します。このアプローチにより、関連情報のみが収集され、他のデバイスへの影響が最小限に抑えられます。このシナリオでは、どのeDiscovery収集手法が使用されていますか？
A. 捜査官は、保管者による自己収集を利用して、機密性の高い証拠データを収集します。
B. 調査員は増分収集を使用し、新しく作成されたデータまたは変更されたデータに焦点を当てます。
C. 調査員は、ネットワーク接続を介して保管者のシステムからデータを遠隔取得します。
D. 研究者は、特定のデータセットとシステム領域の方向性のある収集を採用します。
正解: **(正解を表示します)**
CHFI v11の手順と方法論の領域で定義されているように、指向型収集とは、調査担当者が、関連情報が含まれていることが既知または非常に高い特定のデータセット、ファイルの種類、ディレクトリ、管理者、またはシステム領域に証拠収集を意図的に限定するeディスカバリー手法です。このアプローチは、データ量を削減し、業務の中断を最小限に抑え、法的および運用コストを削減しながら、フォレンジック上の関連性を維持するために一般的に使用されます。
このシナリオでは、調査担当者はディスクイメージ全体やすべてのユーザーデータを収集するのではなく、特定のディレクトリやファイルタイプを対象とすることで、電子情報開示（ESI）の範囲を意図的に制限します。CHFI v11では、これを「指示型」または対象を絞った）収集と明確に定義しており、これは電子情報開示参照モデル（EDRM）のベストプラクティスに準拠しています。指示型収集は、調査担当者が法的比例原則を遵守し、無関係な第三者データやプライベートな第三者データへの接触を減らすのに役立ちます。
他の選択肢はシナリオに合致しません。保管者による自己収集はリスクを伴うため、証拠の完全性に関する懸念から一般的に推奨されません。増分収集は、選択的な範囲縮小ではなく、前回の収集以降の変更点に焦点を当てます。リモート取得とは、収集戦略そのものではなく、アクセス方法を指します。
CHFI v11では、捜査官が関連証拠の所在を既に把握しており、それを効率的かつ正当に収集する必要がある場合、指示収集を推奨される方法論として強調しています。したがっ

て、CHFI v11で検証された正解は、特定のデータセットとシステム領域に対する指示収集であり、選択肢Dが正解となります。

質問: **11**
法医学分析には、元の証拠からのデータファイルを使用するべきである。
A. 真
B. 偽
正解: **(**正解を表示します**)**

質問: **12**
調査員がSAMとシステムファイルからパスワードを抽出したいと考えています。この場合、調査員はどのツールを使用して、ユーザー、パスワード、およびそれらのハッシュのリストを取得できますか？
A. Nuix
B. PWdump7
C. ハッシュキー
D. ファイルマーリン
正解: **(**正解を表示します**)**

質問: **13**
次のうち、辞書ファイルや総当たり攻撃リストなどの単語リストとそのハッシュ値を含む、事前に計算されたテーブルはどれですか？
A. ディレクトリテーブル
B. パーティションテーブル
C. マスターファイルテーブル（MFT）
D. レインボーテーブル
正解: **(**正解を表示します**)**

質問: **14**
あなたは、Windowsベースのサーバーに対するウェブ攻撃を調査する任務を与えられました。
マシンが他のシステムと開いているセッションを確認するには、以下のどのコマンドを使用しますか？
A. 純利益
B. ネットワーク構成
C. ネットセッション
D. ネットの使用
正解: **(**正解を表示します**)**

質問: **15**

ある国際機関が、機密性の高い顧客データを含むデータベースへの重大な侵害被害を受けた。
事件後、組織は外部のフォレンジック調査員を雇うことを決定しました。しかし、取締役会は外部調査員の選定基準について意見が対立しています。彼らはあなたに助言を求めています。漏洩したデータの機密性と攻撃の規模を考慮すると、外部のフォレンジック調査員を雇う際に考慮すべき重要な要素は何でしょうか？
A. 会社の内部システムに関する知識。
B. 法医学における専門職倫理規定の遵守。
C. 類似の事例への対応経験。
D. 業界における評判。
正解: **(**正解を表示します**)**
選択肢Cが最も有力な回答です。なぜなら、機密性の高い顧客データに関わる大規模な侵害や広範囲にわたる攻撃の場合、外部調査員が同様の事案を扱った経験があるかどうかが、最も重要な実務上の採用要素となるからです。CHFI v11では、フォレンジック調査員の役割と責任、優れたコンピュータフォレンジック調査員の条件、そして目の前の事案に適したスキルと調査能力を持つ人材を選ぶことの重要性を強調しています。
倫理規範の遵守は重要であり、評判も影響を与える可能性があるが、この質問は、重大な情報漏洩調査という文脈において、重要な要素を問うている。類似事例の経験は、証拠保全、情報漏洩範囲の特定、法的機密事項への対応、システム横断的な分析、そして効率的に妥当な調査結果の作成といった、調査担当者の能力に直接影響を与える。そのため、一般的な評判や内部システムへの精通度よりも、運用面でより決定的な要素となる。
したがって、CHFI（サイバーセキュリティ情報機関）の観点からすると、取締役会は、同様のサイバー侵害およびフォレンジック事件への対応において実績のある外部調査員を優先的に選任すべきである。なぜなら、そうすることで、信頼性が高く、法廷で弁護可能な、技術的に妥当な結果が得られる可能性が最も高くなるからである。

質問: **16**
UEFIは、OSとプラットフォームファームウェア間のソフトウェアインターフェースを定義する仕様です。
このインターフェースは、ディスク上に存在するファイルに関する情報をどこに保存するのですか？
A. GUIDパーティションテーブル（GPT）
B. マスターブートレコード（MBR）
C. BIOSパラメータブロック
D. BIOS-MBR
正解: **(**正解を表示します**)**

質問: **17**
法医学鑑定士のスミスは、削除された機密ファイルを見つけて取得するためにハードディスクイメージを分析していた。彼はディスクのルートディレクトリに$Recycle.Binフォルダを発見した。使用されているオペレーティングシステムを特定せよ。
A. Windows 8.1
B. Linux
C. Windows XP
D. Windows 98
正解: **(**正解を表示します**)**

質問: **18**
法医学鑑定士のマイケルは、容疑者のマシンから入手したイメージファイルの法医学的分析を行っています。16進エディタを使用してファイルを調べているうちに、ファイルの16進数値が 89 50 4c」というシーケンスで始まっていることが分かりました。このファイルは疑わしいと思われるため、マイケルはファイルの構造を理解し、悪意のあるコンテンツが含まれているかどうかを判断するために、ファイルの種類を特定する必要があります。この情報に基づいて、マイケルが調べているファイルの種類は何でしょうか？
A. BMP
B. JPEG
C. PDF
D. PNC
正解: **(**正解を表示します**)**
選択肢Dが正解です。質問にはタイプミスがあるようです。 PNC」はほぼ間違いなくPNGの間違いです。CHFI v11には 16進エディタと16進表記の理解」、 画像ファイル分析：JPEGとBMP」、 一般的な画像ファイル形式の16進表示」が明示的に含まれており、受験者は16進表示の署名バイトからファイルの種類を認識できることが求められます。
よく知られている PNG ファイルの署名は、バイト 89 50 4E 47 で始まります。質問に示されているシーケンスは、
89 50 4c」は不完全またはわずかにタイプミスがあるように見えますが、明らかにBMP、JPEG、またはPDFではなくPNG署名パターンを指し示そうとしています。BMPファ

イルは異なる形式で始まり、JPEGファイルは通常FF D8 FFで始まり、PDFファイルは%PDFに対応する25 50 44 46で始まります。
CHFIでは、法医学捜査官が16進数のファイルヘッダー解析によってファイルの種類を特定することが求められているため、選択肢の中で唯一妥当な答えは、タイプミスのあるD PNGを表す）です。したがって、マイケルは試験問題が意図するPNG画像ファイルを調べていることになります。

質問: **19**
社内で発生したコンピューター改ざんの疑いのある事案を調査するため、現場対応チームが招集された。調査を開始する前に、CEOはチームに対し、この事案は軽微な事案として分類されると伝えた。チームは事案に対応するためにどれくらいの時間的猶予が与えられるか？
A. 2営業日
B. すぐに
C. 4時間
D. 1営業日
正解: **(正解を表示します)**

質問: **20**
Windowsセキュリティアカウントマネージャー SAM）は、パスワードをハッシュ形式で保存するレジストリファイルです。
WindowsにおけるSAMファイルは以下の場所にあります。
A. C:\windows\system32\con\SAM
B. C:\windows\system32\drivers\SAM
C. C:\windows\system32\config\SAM
D. C:\windows\system32\Boot\SAM
正解: **(正解を表示します)**

質問: **21**
疑わしいAndroidアプリケーションのトリアージを行う際、調査担当者はフォレンジックワークステーション上でMobSFを使用してローカル静的解析環境をセットアップします。アプリケーションのアーティファクトを送信したり、結果を確認したりする前に、調査担当者はMobSFのインターフェースが使用可能になるように解析環境を初期化する必要があります。
この環境を稼働可能にするには、どのような操作が必要ですか？
A. 開く
ウェブブラウザを開き、ホームページにアクセスするには http://localhost:8000 にアクセスしてください。
B. python manage.py runserver を実行します。
C. 分析に必要な疑わしいAPKファイルをアップロードしてください

D. ダッシュボード上のアプリケーションハッシュ値、コンポーネントの種類と数などの情報を確認します。
正解: **(**正解を表示します**)**
正解はBです。MobSFは、ブラウザでインターフェースにアクセスする前に、まずローカルWebアプリケーションとして起動する必要があります。MobSFのインストールと起動のワークフローには、Webインターフェースが利用可能になるようにサーバープロセスを起動することが含まれます。アプリケーションが既に実行されている場合にのみ、ブラウザでlocalhostを開くことが次のステップとなります。APKのアップロードとダッシュボードデータのレビューは、サービスが最初に動作している必要がある後のアクションです。CHFI v11にはマルウェア分析とモバイルアプリケーションフォレンジックが含まれており、この種の質問は、調査官が初期化ステップと後の分析使用を区別できるかどうかをテストします。実際のフォレンジックトリアージでは、アプリケーションの提出またはレビューを行う前に、分析環境をオンラインにする必要があります。そのため、サーバー起動アクションが正しい動作イネーブラーとなります。正確なコマンドはインストール方法またはバージョンによって若干異なる場合がありますが、リストされているオプションの中で、実際にローカル分析環境を初期化するのはサーバープロセスを実行することです。したがって、最適な回答はpython manage.py runserverを実行することです。(github.com)

質問: **22**
ナッシュビルの医療機関のサンドボックス環境で動的マルウェア解析を行ったところ、サンプルにはネットワークアクティビティがすぐには見られませんでした。制御された再起動後、実行ファイルはユーザーの操作なしにログオン時に自動的に起動しました。再起動サイクル全体にわたってこの動作を引き起こすシステム変更を把握するために、調査担当者はシステムアクティビティのどの領域を監視すべきでしょうか？
A. 監視プロセス
B. レジストリアーティファクトの監視
C. 監視サービスとスタートアッププログラム
D. イベントログの監視
正解: **(**正解を表示します**)**
正解はCです。なぜなら、説明されている動作は再起動後も継続する自動起動実行であり、これはサービスやスタートアッププログラムに最も直接的に関連しているからです。CHFI v11では、サービス、スタートアッププログラム、レジストリアーティファクト、および関連するオペレーティングシステムの変更を監視することで、マルウェアの永続化メカニズムとシステム動作分析を明示的にサポートしています。再起動後やログオン後にマルウェアが自動的に起動する場合、調査担当者はまず、再起動後も存続し、手動操作なしでプログラムの起動をトリガーする実行メカニズムに注目する必要があります。サービスやスタートアップエントリは、このような動作が永続化する典型的な場所です。
レジストリのアーティファクトも、特にRunキーを介して関与する可能性がありますが、質問は、再起動に関連する実行動作自体を捉えるために、システムアクティビティのどの領

域を監視すべきかということです。そのため、システム起動時またはユーザーログオン時に自動起動を直接制御するサービスとスタートアッププログラムが最適です。動的なマルウェア分析では、再起動サイクル全体にわたってこれらの永続化ポイントを追跡することで、マルウェアがサービスベース、スタートアップフォルダベース、または他の自動起動メカニズムに関連付けられているかどうかなど、マルウェアがどのように再出現するかを調査者が理解するのに役立ちます。

質問: **23**
次のうち、法医学的準備計画チェックリストの検討事項に含まれないものはどれですか？
A. 法医学的に妥当な方法で要件を満たす証拠を安全に収集するための手順を決定する。
B. デジタル証拠を必要とするビジネス状態を定義する
C. 組織の全従業員から許可を得る
D. 入手可能な証拠を特定する
正解: **(**正解を表示します**)**

質問: **24**
ある組織は、大量の電子データの詳細な分析に伴うeDiscoveryコストを最小限に抑えるべく取り組んでいます。そのため、高度な手法と自動化されたプロセスを採用し、詳細な調査が必要なデータ量を効果的に絞り込むことで、コンプライアンスを維持しながら効率性を向上させています。特定のプラットフォームとプロセスを活用することで、関連データのみが分析され、冗長なデータはワークフローの早い段階で除外されるようにしています。組織は、効率的なデータ分析を確実にするために、どのようなベストプラクティスを実施していますか？
A. 組織は、不要になったデータを安全に廃棄するために、データ保持ツールを導入しています。
B. 組織は、技術支援レビュー（TAR）とデータ削減ツールを使用して、レビュープロセスから無関係なデータを除外します。
C. 組織は、eDiscoveryプロセス全体を通して安全な保管管理体制を確保するためのツールを採用しています。
D. 組織はデータマッピングツールを使用して、データ管理者を特定し、関連データの所在を追跡します。
正解: **B (**コメントを発表する**)**
この質問は、CHFI v11の「コンピュータフォレンジックの基礎とeDiscoveryおよびデジタル証拠管理」の目標に合致しています。CHFI v11では、eDiscoveryのコストと期間を削減する最も効果的な方法の1つは、早期のデータ削減とインテリジェントなフィルタリングであると強調しています。組織は、重複排除、NIST準拠の削除、キーワードフィルタリング、関連性スコアリングなどのデータ削減技術と組み合わせた、予測コーディングとしても知られるテクノロジー支援レビュー（TAR）にますます依存するようになっています。

TARは機械学習アルゴリズムを活用して関連文書内のパターンを識別し、応答性が低いと考えられるデータを自動的に優先または除外します。これにより、手動レビューが必要なデータ量を大幅に削減しながら、法的および規制上の要件への準拠と正当性を維持します。CHFI v11では、特に訴訟や規制調査において、大規模な電子証拠を効率的に処理するためのベストプラクティスとしてTARを推奨しています。
その他のオプションはeDiscoveryをサポートするものの、レビュー範囲を直接的に縮小するものではありません。データ保持はライフサイクル管理に重点を置き、証拠保全は証拠の完全性を確保し、データマッピングはデータソースを特定します。
レビュープロセスの早い段階で無関係なデータを除外することについて直接言及しているものはありません。したがって、CHFI v11のeDiscoveryのベストプラクティスに沿って、テクノロジー支援レビュー（TAR）とデータ削減ツールを使用することが正しい解決策です。

質問: **25**
捜査官は、iPodをあらゆる種類のコンピューターから取り外す前に、どのような手順を踏むべきでしょうか？
A. iPodをマウント解除する
B. iPodをマウントする
C. iPodに参加しよう
D. iPodを切り離す
正解: **A (**コメントを発表する**)**

質問: **26**
法医学捜査官が、企業組織における機密ファイルへの不正アクセスを含むデータ侵害を調査している。捜査中、捜査官は関連データを慎重に特定し、元のソースを変更せずに収集し、データの完全性を維持し、プロセスの各ステップを文書化し、潜在的な法的措置に備えて調査結果を準備する。この調査において適用されているコンピュータフォレンジックの基本的な目的とは何か？
A. 事件が被害者に及ぼす潜在的な影響を推定し、加害者の意図を判断する。
B. 組織を将来同様の事件から守るため
C. サイバー犯罪の加害者を追跡し、訴追する
D. サイバー犯罪の証拠を法医学的に適切な方法で収集する
正解: **(**正解を表示します**)**
正解はDです。なぜなら、このシナリオにおけるすべての行動は、信頼性、検証可能性、法的正当性を維持する方法でデジタル証拠を収集および保存するという、法医学における中心的な目的を中心に据えているからです。
CHFI v11では、コンピュータフォレンジック、証拠保全、証拠管理、データ取得、報告といった、この主要目標を支えるすべての事項について解説しています。フォレンジック的に健全な実践に関する外部資料では、証拠の改ざんを最小限に抑え、完全性を維持し、変更点を記録し、法廷で通用するプロセスを維持しながら証拠を取得することと説明しています。その他の選択肢は、調査の可能性のある結果やより広範なメリットを説明するもので

すが、調査官の行動によって示される直接的な目的ではありません。このシナリオは、影響の推定、将来の事件の防止、犯人の特定を主な目的としていません。
むしろ、証拠の取得から法的準備に至るまでの適切な証拠処理を重視している。CHFI方式の推論では、慎重な識別、非破壊的な収集、完全性の保護、訴訟のための文書化といった点が問題で強調されている場合、適用される根本的な目的は、サイバー犯罪の証拠を法医学的に適切な方法で収集することである。

質問: **27**
デジタルフォレンジック調査中に、Google Cloud Platform（GCP）環境で不審なアクティビティが検出されました。調査チームは、GCPサービスからログとメタデータへのアクセス権を取得します。
Google Cloudのフォレンジック調査において、ログとメタデータはどのような役割を果たしますか？
A. GCPサービスへのアクセスに使用されるデバイスの種類に関する詳細情報を提供します。
B. GCPでのデータ保存に使用される暗号化アルゴリズムを決定します。
C. ユーザーの物理的な位置に関する情報を提供します。
D. GCP環境内でのユーザーの行動とインタラクションを追跡します。
正解: **(**正解を表示します**)**
この質問は、CHFI v11のクラウドフォレンジックに関する目標、特にGoogle Cloud Platform（GCP）などのクラウド環境における証拠の取得と分析に焦点を当てた目標と一致しています。従来のオンプレミスシステムとは異なり、クラウドインフラストラクチャは、捜査官が物理的なハードウェアに直接アクセスできないことが多いため、フォレンジック証拠の主要な情報源としてログとメタデータに大きく依存しています。
CHFI v11では、監査ログ、アクセスログ、アクティビティログ、リソースメタデータなどのクラウドサービスログが、クラウドベースのインシデントにおける事象の再現に不可欠であることを強調しています。GCPでは、これらのログに、ユーザーの操作、API呼び出し、認証試行、リソースの作成または削除、権限の変更、クラウドサービスとのやり取りに関する詳細情報が記録されます。これにより、調査担当者は悪意のある活動を追跡し、侵害されたアカウントを特定し、タイムラインを確立し、特定のユーザーまたはサービスアカウントに操作を帰属させることができます。
ログにはIPアドレスやデバイス関連のヒントが偶然含まれる場合もありますが、その主なフォレンジック上の価値は、どのような操作が、いつ、誰によって行われたかを追跡することにあります。暗号化メカニズムはクラウドプロバイダーによって事前に定義されており、調査中にログから推測されるものではありません。したがって、CHFI v11クラウドフォレンジック手法に準拠して、ログとメタデータはGCP環境内でのユーザーの操作とインタラクションを追跡するために不可欠であり、選択肢Dが正解となります。

質問: **28**

Microsoft セキュリティ ID は Windows レジストリ エディターで確認できます。Windows 7 で ID を見つけるパスは次のとおりです。
A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList
正解: **(**正解を表示します**)**

質問: **29**
リチャードはシステムから揮発性データを抽出するために、doskey/historyというコマンドを使用しています。彼は何を抽出しようとしているのでしょうか？
A. 以前に入力したコマンド
B. ブラウザの歴史
C. システム全体で使用されているパスワード
D. イベント履歴
正解: **(**正解を表示します**)**

質問: **30**
多国籍企業でセキュリティ侵害が発生しました。フォレンジック調査員は、疑わしいWindows 10システムに「SecureBox」などの特定のアプリケーションがインストールされていたかどうかを特定するよう依頼されました。調査員はこれを検証するためにどのようなアプローチを取るべきでしょうか？
A. 容疑機に類似した環境で様々な計画を実験・検証する
B. 観察を行い、事件について仮説を立て、特定のオペレーティングシステムディレクトリでSecureBoxの痕跡を確認する。
C. 市販の調査ツールを選択する理由は、それらが市場価値を持ち、多様かつ詳細な調査を可能にするためです。
D. 複数の証拠資料を精査し、SecureBoxがいつインストールされたかを正確に判断して意見を形成する。
正解: **(**正解を表示します**)**

質問: **31**
あなたは多国籍企業で発生したデータ漏洩の疑いに関するフォレンジック調査を行っています。調査中に、世界各地の複数のシステムで、一見無関係に見える複数のインシデントが発生していることが判明しました。これらのインシデントを理解し、潜在的な関連性を確立するために、どのようなアプローチを採用すべきでしょうか？
A. 各事件ごとに個別の調査を実施する
B. 調査全体を最初からやり直す
C. 最も深刻なインシデントについて詳細な分析を実施する

D. 事象相関を用いて、事件間の関連性を見出す
正解: **(**正解を表示します**)**
選択肢Dが最適な答えです。CHFI v11には、イベント相関の種類、イベント相関のアプローチ、および相関証拠を使用してシステム間のアクティビティを再構築する方法が明示的に含まれているからです。複数のインシデントが異なるホスト、地域、または期間にわたって無関係に見える場合、イベント相関は、共通のパターン、関連する指標、タイミングの関係、および共通のソースを特定するために使用されるフォレンジック手法です。
多国籍企業によるデータ漏洩事件では、捜査官は各事件が本当に個別のものなのか、それとも組織的な犯行の一環であるのかを判断する必要があります。相関分析は、ログ、タイムスタンプ、ネットワークイベント、認証記録、その他の証拠を統合して全体像を把握するのに役立ちます。これは、各事件を個別に処理したり、最も深刻な事件のみに焦点を当てたりするよりもはるかに効果的です。
オプションAは、より広範な関連性を見落とすリスクがある。Bは不要で非効率的である。Cは特定のホストには役立つかもしれないが、より広い環境における関連性を確立するものではない。したがって、CHFIの観点からすると、適切な調査手法は、イベント相関を用いてインシデントを関連付け、疑わしい情報漏洩活動の一貫した全体像を構築することである。

質問: **32**
次のうち、デバイス監視ツールはどれですか？
A. ドライバー探偵
B. カプサ
C. RAMキャプチャ
D. レグショット
正解: **(**正解を表示します**)**

質問: **33**
CAN-SPAM法では、以下のことが求められます。
A. 受信者に自分の居場所を教えないでください
B. 実際のヘッダー情報を使用しない
C. メッセージを広告として認識させないでください

D. 人を欺くような件名は使用しないでください
正解: **(**正解を表示します**)**

質問: **34**
MS-Exchange Serverのストレージアーカイブに変更があった疑いがあるとして、調査担当者はそれを分析しました。次のうち、アーカイブの実際の構成要素ではないものはどれですか？
A. PUB.STM
B. PRIV.STM
C. PRIV.EDB
D. PUB.EDB
正解: **(**正解を表示します**)**

質問: **35**
次のファイルのうち、他のオブジェクトを埋め込んだりリンクしたりするために、オブジェクトリンクおよび埋め込み（OLE）テクノロジーを使用していないものはどれですか？
A. MSオフィス Word OneNote
B. ポータブルドキュメントフォーマット
C. MSオフィスWord文書
D. MSオフィス Word PowerPoint
正解: **(**正解を表示します**)**

質問: **36**
以下のうち、データ取得フォレンジック調査の一部ではないものはどれですか？
A. 許可された担当者のみがアクセスできるようにしてください。
B. 複製されたコピーではなく、元の記憶媒体で作業してください。
C. 証拠を極端な温度変化から保護する
D. システムへのリモートアクセスをすべて無効にする
正解: **(**正解を表示します**)**

質問: **37**
多面的なサイバーセキュリティ対策において、アナリストはJuniper、Check Point、Snortといった最先端のIDSツール群を駆使し、ログを綿密に分析します。ネットワークイベントに関する複雑なデータが満載されたこれらのログは、防御の要となり、アナリストが膨大な情報の中から微妙な異常を識別することを可能にします。
複雑なサイバーセキュリティ対策の中で、侵入検知システム（IDS）は、イベントの監視と分析という役割に加え、主にどのような多面的な機能を担っているのでしょうか？
A. 進化する脅威に対抗するために、攻撃シグネチャを繰り返し改良する。
B. 電子メール、ページング、SNMPトラップなど、さまざまなチャネルを通じてセキュリティ管理者に常に警告を発します。

C. 監視対象イベントから得られた微妙な洞察をまとめた包括的なグラフィカルレポートを作成します。
D. 分散ログインフラストラクチャへのデータのシームレスな送信をオーケストレーションします。
正解: **B** (コメントを発表する)
この質問は、CHFI v11の「ネットワークおよびWeb攻撃」の項目、特にネットワークセキュリティ監視とインシデント対応における侵入検知システム（IDS）の役割と機能に関する目標に合致しています。
CHFI v11では、Snort、Juniper IDS、Check PointなどのIDSソリューションは、ネットワークトラフィックを監視および分析するだけでなく、疑わしいまたは悪意のある活動が検出された場合にセキュリティ担当者に積極的に警告するように設計されていることを強調しています。
IDS（侵入検知システム）は、定義済みのシグネチャ、動作モデル、または異常閾値に基づいて、パケット、セッション、およびイベントを継続的に検査します。潜在的な侵入、ポリシー違反、または攻撃パターンが検出されると、システムの主要な運用対応はリアルタイムアラートを生成することです。これらのアラートは、電子メール通知、ポケットベルアラート、ダッシュボード、syslogメッセージ、SNMPトラップなど、複数のチャネルを通じて配信され、セキュリティ管理者がタイムリーに状況を把握し、迅速に対応できるようにします。
IDSプラットフォームは、レポート作成、ログ転送、シグネチャ更新などをサポートする場合がありますが、これらは二次的な、あるいは補助的な機能です。フォレンジックおよび運用環境におけるIDSの重要な価値は、脅威が発生したり検出されたりした際に、防御側に迅速に通知できる能力にあります。したがって、CHFI v11のIDS原則に沿って、複数の通知チャネルを通じてセキュリティ管理者に常に警告を発することが正しい対応策となります。

質問: **38**
Linuxベースのシステムで、「last -F」コマンドを実行すると何が表示されますか？
A. 最近開いたファイル
B. 最後に実行された機能
C. 最後に実行されたプロセス
D. システムのログインおよびログアウトの日時
正解: **(**正解を表示します**)**

質問: **39**
通勤者のサラは、毎日の電車移動中に娯楽としてモバイル端末を利用している。彼女は時間をつぶすために高画質動画のストリーミングを好んで視聴する。途切れのない高速データ転送を必要とする彼女にとって、バッファリングによる中断のないスムーズなストリーミングを可能にする携帯電話ネットワーク技術は大きなメリットとなる。

サラの携帯端末には、どの携帯電話ネットワーク技術が最も適しているでしょうか？
A. ロングタームエボリューション（LTE）
B. 時分割多重アクセス（TDMA）
C. GSM進化のための拡張データレート（EDGE）
D. 符号分割多元接続（CDMA）
正解: **A** (コメントを発表する)
CHFI v11 モバイルおよび IoT フォレンジック領域によると、モバイル通信の動作、データ使用パターン、通話詳細記録 (CDR) を分析するには、セルラーネットワーク技術を理解することが不可欠です。挙げられている技術の中で、Long-Term Evolution (LTE) は、高解像度ビデオストリーミングなどの高帯域幅アクティビティに最も適しています。
LTE（一般的に4Gと呼ばれる）は、高いデータスループット、低遅延、効率的なパケット交換通信を実現するように設計されています。CHFI v11では、LTEをビデオストリーミング、VoIP、オンラインゲーム、クラウドベースのアプリケーションなど、データ集約型サービスをサポートできるブロードバンドセルラー技術として高く評価しています。直交周波数分割多重アクセス（OFDMA）や多入力多出力（MIMO）といった高度な技術を採用することで、列車などの移動環境でも安定した高速データ転送が可能になります。
その他の選択肢は、データ処理能力が著しく低いレガシー技術です。TDMAとCDMAは、主に音声通信に最適化された旧世代のアクセス方式です。EDGEは、
2.5G技術は、データ転送速度が限られており、安定したHDビデオストリーミングには不十分で、バッファリングや遅延の問題が発生しやすい。
フォレンジックの観点から、CHFI v11は、位置追跡、セッション分析、IPベースの通信、データ使用状況の再構築における重要性から、LTEネットワークを重視しています。したがって、サラの高速ストリーミングのニーズに最も適したセルラーネットワーク技術は、Long-Term Evolution（LTE）です。
したがって、オプションAが正解であり、CHFI v11で検証済みの回答となります。

質問: **40**
WindowsエクスプローラーまたはMS-DOSのdeleteコマンドによってファイルが削除されると、オペレーティングシステムはFATデータベース内のファイル名の最初の文字の位置に_____を挿入します。
A. 大文字のX
B. 空白スペース
C. アンダースコア記号
D. ギリシャ文字の小文字シグマ（σ）
正解: **D** (コメントを発表する)
ファイルが削除されると、最初のバイトが0xE5に置き換えられ、ファイルが削除済みまたは消去済みとしてマークされます。これはFAT12/16/32でも同様です。0xE5はASCIIコード229、チルダ付きの「σ」にも相当します。

しかし、ギリシャ文字を使用する場合（http://www.ascii.ca/iso8859.7.htm を参照）、ASCII コード 229 は「小文字のギリシャ文字イプシロン」であり、ASCII コード 243 は小文字のギリシャ文字シグマです。
http://chexed.com/ComputerTips/asciicodes.php によると、ASCII 229 はギリシャ文字の小文字シグマです。したがって、ここでは D が正解のように見えますが、質問の根本的な意図をより深く理解する必要があるかもしれません。

質問: **41**
法医学捜査官のエレナは、マルウェア感染の疑いのある事象の挙動を分析しています。分析中に、彼女はWindowsイベントログにいくつかの異常なエントリ、特にイベントID 5156に気づきました。エレナはこれらのログから、悪意のある活動を追跡するのに役立つどのような重要な情報を期待できるでしょうか？
A. 不正アクセスに使用されたユーザー名とパスワード
B. マルウェアによって削除されたファイルの場所
C. 悪意のあるプロセスのレジストリキー変更の詳細
D. プロセス名と、そのプロセスが通信したIPアドレス
正解: **(**正解を表示します**)**
CHFI v11 オペレーティングシステムおよびマルウェアフォレンジックの目的によると、Windows イベント ID
5156はWindowsフィルタリングプラットフォーム（WFP）によって生成され、ネットワーク接続が許可されたことを示します。このイベントは、プロセスレベルのネットワークアクティビティに関する詳細な情報を記録するため、マルウェア調査において非常に有用です。ネットワークアクティビティは、侵害の一般的な指標となります。
イベントID 5156のログには通常、以下の情報が含まれます。
ネットワーク接続を開始したプロセス名とプロセスID（PID）
* 送信元および宛先IPアドレス
* 出発港と到着港
* 使用プロトコル（TCP/UDP）
* 接続の方向（受信または送信）
CHFI v11では、マルウェアの挙動を追跡する上で、特にコマンド＆コントロール（C2）通信、データ漏洩の試み、および横方向の移動を特定する上で、Windowsセキュリティイベントログの重要性が明確に強調されています。イベントID 5156を分析することで、調査担当者は特定の実行可能ファイルまたは悪意のあるプロセスを外部IPアドレスと直接関連付けることができ、攻撃者のインフラストラクチャとタイムラインの確立に役立ちます。
他の選択肢は誤りです。イベントID 5156は、認証情報、ファイル削除パス、レジストリ変更の詳細を記録しません。これらの情報は、他のイベントID、またはレジストリハイブ、ファイルシステムメタデータ、Sysmonログなどのフォレンジックソースで確認できます。

したがって、イベントID 5156の重要なフォレンジック的価値は、ネットワーク通信を担当するプロセスと、それが接続しているIPアドレスを明らかにすることにあるため、オプションDが正解であり、CHFI v11によって検証された回答となります。

質問: **42**
Mac OS X で使用されているファイルシステムは次のうちどれですか？
A. EFS
B. HFS+
C. EXT2
D. NFS
正解: **(**正解を表示します**)**
EFS（暗号化ファイルシステム）はNTFSの一部であり、Windowsで使用されます。EXT2はLinuxで使用されます。NFS（ネットワークファイルシステム）はTCP/IP経由でネットワークファイルシステムにアクセスするためのものです。

質問: **43**
ネットワーク管理者であるミアは、ネットワークのパフォーマンス低下に気づき、Ciscoルーターのログを確認しています。ログを調べているうちに、「必要なIPヘッダーオプションをすべて格納するのに十分なスペースがなかったため、システムはパケットを処理できませんでした」というメッセージを見つけました。ミアは、Cisco IOSログの中で、この特定の問題に対応するニーモニックを特定する必要があります。
ミアはこのメッセージを見つけるために、以下のログニーモニックのうちどれを探すべきでしょうか？
A. %SEC-4-TOOMANY
B. %IPV6-6-ACCESSLOGP
C. %SEC-6-IPACCESSLOGP
D. %SEC-6-IPACCESSLOGRL
正解: **(**正解を表示します**)**
CHFI v11ネットワークフォレンジックおよびログ分析の目的によると、Cisco IOSログメッセージは、特定のセキュリティおよびパケット処理条件を説明するために標準化されたニーモニックを使用します。「必要なIPヘッダーオプションすべてを格納するのに十分なスペースがありませんでした」というメッセージは、異常または過剰なIPヘッダーオプションに関連しており、これはパケットの形式が不正であること、偵察活動、またはサービス拒否（DoS）攻撃の試みを示している可能性があります。
%SEC-4-TOOMANY というニーモニックは、ルータが利用可能なバッファ容量に対して IP オプションが多すぎるパケットを受信した際に生成されます。Cisco デバイスはシステム リソースを保護するために IP ヘッダー オプションに制限を設けており、この制限を超えるとパケットは破棄され、このニーモニックがログに記録されます。CHFI v11 では、

ネットワーク パフォーマンスの低下、パケット操作、および潜在的な攻撃トラフィックを調査する際に、このようなログが重要なアーティファクトとして強調表示されます。
その他のオプションはこの状態とは関係ありません。%IPV6-6-ACCESSLOGPはIPv6アクセス制御のログ記録に適用されます。%SEC-6-IPACCESSLOGPと%SEC-6-IPACCESSLOGRLは、IPヘッダーオプションの枯渇ではなく、アクセスリストの許可/拒否のログ記録とレート制限されたACLメッセージに関連しています。
法医学的な観点から見ると、%SEC-4-TOOMANYを特定することで、調査官はパフォーマンスの問題と不正なトラフィックパターンや悪意のあるトラフィックパターンとの相関関係を把握しやすくなり、ネットワーク攻撃の調査における原因特定に役立ちます。
したがって、この問題に対応する正しいCisco IOSログニーモニック（CHFI v11に完全準拠）は次のとおりです。
%SEC-4-TOOMANY（オプションA）。

質問: **44**
企業のデータベースサーバーが予期せず停止した後、ITフォレンジックチームは、潜在的な問題を調査するために、データベースプランキャッシュからデータを収集する任務を負っています。キャッシュされたすべてのエントリのSQLテキストを取得し、追加の集計パフォーマンス統計を取得するには、どのようなクエリを使用すべきでしょうか？
A. 使用方法: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) の後に、select * from sys.dm_exec_plan_attributes(plan_handle) を実行します。
B. 使用方法: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_sql_text(plan_handle) の後に、select * from sys.dm_exec_query_stats を実行します。
C. 使用方法: select * from sys.dm_exec_sql_text(plan_handle) cross apply sys.dm_exec_cached_plans の後に、select * from sys.dm_exec_query_stats を実行します。
D. 使用方法: select * from sys.dm_exec_cached_plans cross apply sys.dm_exec_plan_attributes(plan_handle) の後に、select * from sys.dm_exec_query_stats を実行します。
正解: **(正解を表示します)**

質問: **45**
企業環境において、不正なデータアクセスの兆候が見られたことを受け、上級幹部のAndroidスマートフォンが内部フォレンジック調査のために保護されました。この調査は管理上のものであり、幹部は調査への協力のために待機しています。デバイスはパスコードで保護されており、潜在的な証拠への即時アクセスはできません。調査担当者は、既存のデータを変更したり、高度な技術的措置を講じたりすることなく、アクセス権を取得する

必要があります。証拠の完全性を維持しながら合法的に調査を進めるには、どの方法が最も適切でしょうか？
A. 従業員の協力を得てパスコードを自主的に開示し、調査の完全性を損なうことなく合法的なデータアクセスを確保する。
B. Android専用のフォレンジックソフトウェアを使用して、法令および倫理基準を遵守しながら、体系的に組み合わせを推測してデータにアクセスする、準拠した総当たりパスコード攻撃を実行します。
C. リモートMDMソフトウェアを使用してデバイスのパスコードをリセットし、証拠の完全性を維持しながらデータアクセスを有効にします。
D. 証拠の完全性を損なうことなくデータへのアクセスを確保するため、専用ツールを使用して物理デバイスの取得について管理承認を申請する。
正解: **(**正解を表示します**)**
CHFI v11では、法令遵守、同意の取得、証拠の保全、証拠保全の連鎖、および適切なフォレンジックプロセスに従うことが強く求められているため、オプションAが最も適切な回答です。このシナリオでは、問題は管理上のものであり、デバイスの所有者は連絡可能で、調査担当者はデータを改変したり、より侵襲的な技術的措置に頼ったりすることなくアクセスする必要があります。このような状況下では、従業員の自発的な協力とパスコードの開示を得ることが、最も正当で、かつ混乱を最小限に抑える方法です。この設計図には、法的要件および手続き上の要件に基づき、同意の取得、デジタル証拠の取り扱いに関するベストプラクティス、証拠の保全、および証拠保全の連鎖が明確に含まれています。
この回答は、CHFIのモバイルフォレンジック分野（携帯電話の証拠分析、データ取得方法、Androidデバイスの論理的および物理的取得、モバイルフォレンジックにおける課題など）にも合致しています。捜査官は、高度な取得技術を検討する前に、まず最も破壊的でなく、最も合法で、最もフォレンジック的に妥当なアプローチを用いるべきです。
オプションBはこの事例には過度に介入的であり、Cはデバイスの状態を変更し、Dは同意に基づくアクセスが既に利用可能な場合に不必要に権限を昇格させる。

質問: **46**
どのプログラムが、マルウェアのコードを隠蔽するために様々な技術を使用し、それによってセキュリティ機構による検出や削除を困難にしているのでしょうか？
A. スポイト
B. 難読化ツール
C. インジェクター
D. パッカー
正解: **(**正解を表示します**)**

質問: **47**
セキュリティ侵害の疑いがある企業において、フォレンジック調査員がドメインコントローラー上のイベントIDログを調査しています。調査員は、ドメインユーザーアカウントが短時間のうちに作成、変更され、グループに追加されたことに気づきます。調査員は、ローカルシステムの監査ポリシーを相互検証して、変更が加えられたかどうかを確認する必要があると認識します。調査員が正しい監査ポリシー設定を持っていると仮定した場合、調査員は次のどのイベントIDに注目すべきでしょうか？
A. イベントID 642
B. イベントID 612
C. イベントID 624
D. イベントID 644
正解: **(**正解を表示します**)**

質問: **48**
以下のコマンドのうち、Windowsベースのサーバーで実行されているすべてのネットワークサービスを表示するものはどれですか？
A. ネットセッション
B. ネットワーク設定
C. ネットスタート
D. ネット利用
正解: **C (**コメントを発表する**)**

質問: **49**
この組織は、既知のソフトウェアのハッシュ署名のデータベースを維持している。
A. 国立ソフトウェアリファレンスライブラリ
B. 国際標準化機構
C. 電気電子学会
D. 米国規格協会
正解: **A (**コメントを発表する**)**

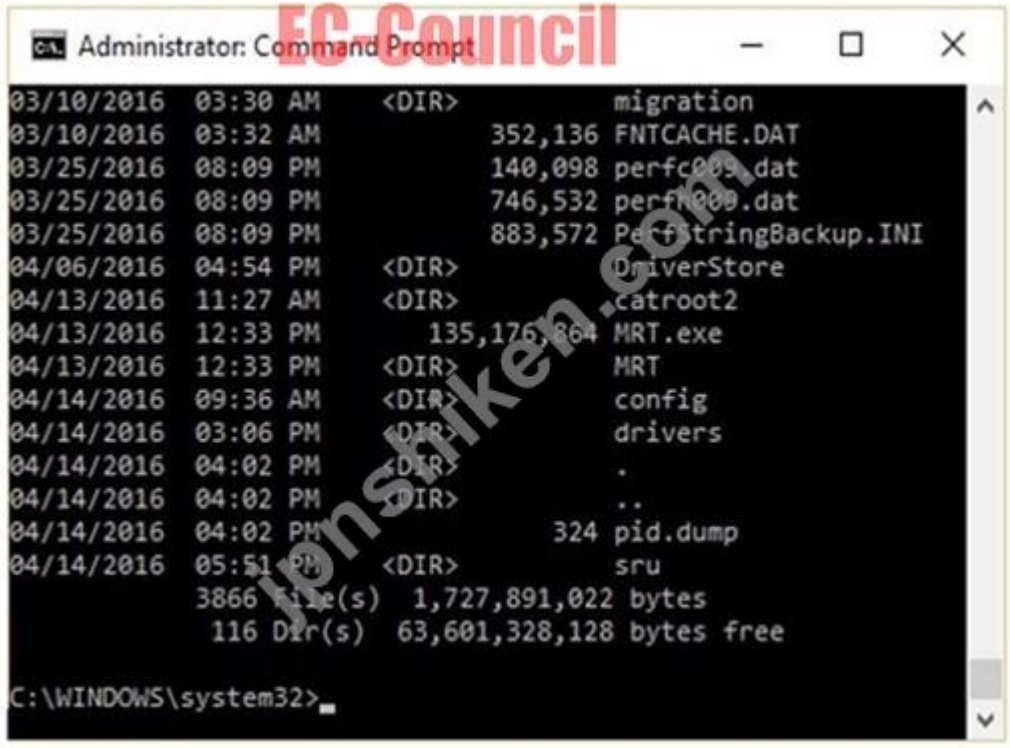
質問: **50**
システムBIOSパスワードを回避する方法の一つは何ですか？
A. CMOSバッテリーの取り外し
B. システムメモリをすべて削除する
C. Windowsにログインし、BIOSパスワードを無効にします。

D. プロセッサの取り外し
正解: **(**正解を表示します**)**

質問: **51**
巨大な単語リスト（辞書ファイルやブルートフォースリストなど）をパスワードハッシュに変換するために使用されるテーブルはどれですか？
A. マスターファイルテーブル
B. データベーステーブル
C. レインボーテーブル
D. ハッシュテーブル
正解: **(**正解を表示します**)**

質問: **52**
内部から侵入テストを実施するのが良いアイデアである理由は？
A. 内部から侵入テストを行うのは決して良い考えではありません
B. ハッカーの視点からネットワークを攻撃する
C. 内部からのハッキングの方が容易です
D. 攻撃の70%は組織内部から発生しているため
正解: **(**正解を表示します**)**

質問: **53**
提示された画像には、OSのインストール日時、サービスパック、パッチ、およびサブディレクトリに関する情報が表示されています。調査担当者はこの出力を表示するために、どのようなコマンドまたはツールを使用しましたか？



A. dir /o:s

B. dir /o:n
C. dir /o:d
D. /o:e と言う
正解: **(**正解を表示します**)**

質問: **54**
法医学捜査官は、侵害されたシステム上で、既知のプログラムパッカーを使用してパックされたと思われる疑わしい実行ファイルを発見し、パスワードで保護されていることを確認した。捜査官は、パックに使用されたツールとその解凍ツールを知っている。この実行ファイルを調査するために、次に取るべき最善の行動は何か？
A. 管理された環境で、パックされた実行ファイルに対して動的解析を実行する
B. 解析前に実行可能ファイルを解凍するためにパスワードを復号します。
C. リバースエンジニアリングを使用して、内部に隠された攻撃ツールを理解する
D. パスワードを扱わずに、解凍ツールを使用して実行ファイルを解凍します。
正解: **A (**コメントを発表する**)**

質問: **55**
次のうち、ウェブサイトから送信され、ユーザーのウェブブラウザによってユーザーのコンピュータに保存され、特定のユーザー情報を追跡、検証、維持するために使用される小さなデータはどれですか？
A. ウェブブラウザのキャッシュ
B. ファイルを開く
C. 一時ファイル
D. クッキー
正解: **D (**コメントを発表する**)**

質問: **56**
法医学捜査官が、起動中に障害が発生したシステムを調査している。捜査官は、BIOSがシステムハードウェアを初期化した後に起動プロセスが中断されたことを発見した。もし障害が発生していなかった場合、起動プロセスの次のステップは何だっただろうか？
A. ブートマネージャはブート可能なパーティションを見つけてMBRをロードします。
B. カーネルが起動し、システムのハードウェア抽象化レイヤー (HAL) をロードします。
C. システムはブートパーティションからntoskrnl.exeファイルをロードします。
D. ブートローダーはオペレーティングシステムのカーネルをロードします。
正解: **(**正解を表示します**)**
CHFI v11オペレーティングシステムフォレンジックモジュールによると、Windowsの起動プロセスを理解することは、起動障害の診断や、潜在的な改ざん、ルートキット、または起動レベルのマルウェアの特定に不可欠である。
BIOS-MBRブート方式を使用するシステムでは、ブートシーケンスは明確に定義された順序に従います。

BIOS（基本入出力システム）がハードウェアの初期化と電源投入時自己診断テスト（POST）を完了した後、次に行うべきことは、設定された起動順序に基づいて起動可能なデバイスを特定することです。
有効なブートデバイスが見つかると、BIOSはそのデバイスの最初のセクターからマスターブートレコード（MBR）をメモリにロードし、実行制御をMBRに移します。このステップは非常に重要です。なぜなら、MBRにはアクティブなパーティションを特定し、ブートプロセスの次の段階を実行するためのブートコードが含まれているからです。
MBRの実行後にのみWindowsブートマネージャ（bootmgr）がロードされ、その後Windows OSローダー（winload.exe）がロードされ、さらにntoskrnl.exeとハードウェア抽象化レイヤー（HAL）がロードされます。したがって、オプションB、C、Dはブートプロセスの後の段階を表しており、BIOS初期化直後には発生しません。
CHFI v11 では、このシーケンスを Windows ブートプロセス: BIOS-MBR メソッドで明示的に説明しており、BIOS 初期化直後に発生する障害は通常、MBR またはブート可能なパーティションの検出に関する問題を示していることを強調しています。
したがって、CHFI v11 で検証された正しい回答はオプション A です。ブートマネージャはブート可能なパーティションを見つけて MBR をロードします。

質問: **57**
あらゆる文字セットの組み合わせを使用するパスワード解析手法はどれですか？
A. 力任せの攻撃
B. レインボーテーブルアタック
C. 辞書攻撃
D. ルールベース攻撃
正解: **(正解を表示します)**

質問: **58**
高度なサイバー攻撃が組織を標的とし、フォレンジックチームがインシデント対応のために招集されました。組織の資産は主にAWS上にホストされており、特にS3とEC2インスタンスが使用されています。フォレンジック調査員として、EC2インスタンス内の貴重な証拠を保持するための最初のステップは次のとおりです。
A. 影響を受けたEC2インスタンスのEBSボリュームのスナップショットを作成し、分析のためにフォレンジックチームと共有してください。
B. 影響を受けたEC2インスタンスからログデータを取得して分析する
C. データ破損を防ぐため、影響を受けたEC2インスタンスを直ちにネットワークから隔離してください。
D. EC2インスタンス内のすべてのデータを暗号化し、不正アクセスを防止します。
正解: **(正解を表示します)**

質問: **59**

コンプライアンス担当官のスカーレットは、最近金融不正の疑いをかけられた上場企業に勤務している。調査中に、彼女は米国で可決された法律に遭遇する。
2002年の議会は、企業による不正な会計慣行から投資家を保護することを目的としていた。
この法律は、より厳格な企業財務報告基準、内部統制、および不正行為に対する罰則を義務付けている。
この事件において、スカーレットが最も検討している可能性が高い法律は次のうちどれですか？
A. PCI DSS
B. SOX
C. GLBA
D. ECPA
正解: **(**正解を表示します**)**
この質問は、CHFI v11の「規制、方針、倫理」の項目、特にフォレンジック調査や企業コンプライアンスに影響を与える法律に関する目標に直接的に合致しています。ここで取り上げられている法律は、エンロンやワールドコムといった大規模な企業会計スキャンダルを受けて2002年に制定されたサーベンス・オクスリー法（SOX法）です。CHFI v11では、SOX法を米国の上場企業を規制する重要な法律として位置づけています。
SOX法は、企業の財務報告、内部統制評価、経営幹部の責任、監査の独立性、記録の保存に関して厳格な要件を定めています。SOX法第302条では、経営幹部が財務諸表の正確性を自ら証明することを義務付けており、第404条では、不正行為を防止するための内部統制監査を義務付けています。これらの要件は、財務上の不正行為に関するフォレンジック調査において非常に重要です。なぜなら、調査官は監査記録、財務記録、およびSOX法に準拠したコンプライアンス文書に依拠することが多いからです。
他の選択肢は誤りです。PCI DSSは決済カードデータのセキュリティに適用され、GLBAは顧客の金融データのプライバシーを規定し、ECPAは電子通信のプライバシーを規定しています。したがって、CHFI v11の法的枠組みとコンプライアンス目標に照らし合わせると、スカーレットが検討している正しい法律はSOX（サーベンス・オクスリー法）です。

質問: **60**
集中ログ記録とは、複数のシステムのコンピュータシステムログを中央の場所に収集することと定義される。
これは、セキュリティ違反や異常な活動を検出するために必要な頻度で、コンピュータシステムのログを効率的に監視するために使用されます。
A. 偽
B. 真
正解: **(**正解を表示します**)**

質問: **61**

Windowsシステムを調査する際には、ページファイルまたはスワップファイルの内容を確認することが重要です。その理由は次のとおりです。
A. これは、Windowsがコマンドラインから実行された直近100個のコマンドの履歴を保存するために使用するファイルです。
B. Windows はこのファイルにすべてのシステム構成情報を保存します
C. これは、Windowsがレジストリと直接通信するために使用するファイルです。
D. スワップファイル内には、コンピュータユーザーが認識できない大量のデータが存在する可能性があります。
正解: **(**正解を表示します**)**

質問: **62**
ある企業のオンラインバンキングプラットフォームで最近、セキュリティ侵害が発生し、顧客アカウントへの不正アクセスが相次いでいる。調査の結果、ブルートフォース攻撃によって侵入が試みられている疑いがある。
上記のシナリオにおいて、「ブルートフォース攻撃」という用語は、おそらく何を指していると考えられますか？
A. ハッカーがユーザーインターフェースの要素を操作して機密データにアクセスする攻撃。
B. 従業員を騙してログイン認証情報を漏洩させるソーシャルエンジニアリングの手法。
C. 企業のネットワークインフラストラクチャの脆弱性を悪用する方法。
D. 攻撃者が不正アクセスを得るために、パスワードや暗号鍵を組織的に推測する手法。
正解: **(**正解を表示します**)**
選択肢Dが正解です。総当たり攻撃とは、攻撃者が有効なアクセス権を取得するまで、パスワードや暗号鍵を体系的に推測し続けるプロセスを指します。CHFI v11では、ネットワークおよびWeb攻撃の目標の一部として総当たり攻撃の調査が明示的に含まれており、これは受験者が理解しておくべき重要な概念となっています。
これは、ソーシャルエンジニアリング、パラメータ操作、または技術的な脆弱性の悪用とは異なります。ブルートフォース攻撃の特徴は、多くの可能なパスワードの組み合わせやキー値を使用して、多くの場合自動化された試行錯誤による認証試行を繰り返すことです。オンラインバンキングのシナリオでは、これは顧客アカウントへのログイン試行の繰

り返しとして現れ、多くの場合、同じソースから、または分散インフラストラクチャを介して行われます。
オプションAはインターフェース操作、Bはソーシャルエンジニアリング、Cはより一般的な脆弱性の悪用を表しています。これらのいずれも、ブルートフォース攻撃の本質的な意味を捉えていません。したがって、CHFIの攻撃調査フレームワークに基づくと、最も正確な解釈は、攻撃者が不正アクセスを得るために認証情報や鍵を体系的に推測している、ということになります。

質問: **63**
コンピューターフォレンジックの専門家であるロンは、企業スパイ事件を捜査している。彼は犯行現場から複数のモバイルコンピューティングデバイスを回収した。ロンが所持している証拠品の一つに、電源が入ったまま放置されていたノキア製の携帯電話がある。ロンは、デバイスの所有者を特定するために、そのデバイスのIMEI番号を復元する必要がある。ロンは、IMEI番号を復元するために、次のうちどのキーの組み合わせを使用できるだろうか？
A. #06#*
B. *IMEI#
C. *#06#
D. #*06*#
正解: **(**正解を表示します**)**

質問: **64**
通話設定の際、通信サービスプロバイダーは、発信者と着信者の両方の身元を確認するために多面的なアプローチを採用し、関係するユーザーの正当性を確保します。プロバイダーのセキュリティアナリストであるサラは、固有の識別子を組み合わせて加入者情報を取得し、位置追跡を実行することで、このプロセスを監督します。
サービスプロバイダーが通話設定時にユーザーの本人確認を行うための主要な手段として、具体的にどのような仕組みが挙げられますか？
A. 通話時間を分析することによって。
B. 発信者の位置のみを追跡します。
C. 通話内容を監視することによって。
D. IMSIとIMEI情報を利用する。
正解: **(**正解を表示します**)**
CHFI v11モバイルおよびIoTフォレンジックドメインによると、通信サービスプロバイダーが通話設定時にユーザーの身元を確認するために使用する主要なメカニズムは、IMSI（国際モバイル加入者識別番号）とIMEI（国際モバイル機器識別番号）の使用です。これらの識別子は、セルラーネットワークの認証と加入者管理の基本となります。
IMSIは加入者を一意に識別する識別子であり、SIMカードに保存されます。一方、IMEIは携帯端末自体を一意に識別する識別子です。通話設定時、携帯電話ネットワークは、プロバイ

ダのホームロケーションレジスタ（HLR）またはホーム加入者サーバー（HSS）に対してIMSIを検証することにより、加入者を認証します。
同時に、IMEIがチェックされ、デバイスが正規のものであり、ブラックリストに登録されていないことが確認されます。CHFI v11では、これらの識別子が加入者の特定、通話詳細記録（CDR）の分析、および位置追跡のための重要なフォレンジックアーティファクトとして強調されています。
他の選択肢は誤りです。なぜなら、通話時間と通話内容は本人確認には使用されないからです。
通話内容の監視は、プライバシーおよび法的制約のため制限されています。位置情報の追跡だけでは本人確認はできません。位置情報は、認証が完了した後にのみ位置情報を提供するものです。
CHFI v11では、IMSIとIMEIの相関関係がモバイルフォレンジック調査に不可欠であり、調査官が通話、デバイス、場所、加入者を正確に関連付けることができると強調されています。したがって、通話設定時にユーザーの身元を確認するための正しい、そしてCHFI v11で検証済みのメカニズムは、IMSIとIMEI情報を使用することであり、選択肢Dが正解となります。

質問: **65**
デジタル捜査において、容疑者がクラウドストレージプラットフォームに有罪となる可能性のあるデータを保存していたことが証拠から示唆された。捜査チームはクラウドストレージサービスのログとメタデータへのアクセス権を取得する。クラウドストレージのフォレンジックにおいて、ログとメタデータは捜査プロセスでどのような役割を果たすのか？
A. 保存データに使用される暗号化アルゴリズムを決定します。
B. 容疑者の物理的な位置に関する情報を提供します。
C. これらは、クラウドストレージへのアクセスに使用されたデバイスの種類を特定するのに役立ちます。
D. ユーザー認証とアクセス活動に関する詳細情報を提供します。
正解: **(**正解を表示します**)**
CHFI v11クラウドフォレンジックの目標によると、ログとメタデータは、クラウドベースの調査において最も重要なデジタル証拠源の一つです。従来のオンプレミスシステムとは異なり、クラウド環境では調査員が物理ストレージに直接アクセスできないことがよくあります。そのため、サービスプロバイダーが生成するログとメタデータが主要な証拠となります。
クラウドサービスのログには通常、ログインタイムスタンプ、ユーザーID、認証方法（パスワードやMFAなど）、IPアドレス、セッション期間、アクセス結果（成功または失敗）などのユーザー認証イベントが記録されます。クラウドストレージオブジェクトに関連付けられたメタデータには、ファイルの作成時間、変更時間、アクセス時間、所有権の詳細、共有アクティビティ、アクセス権限などの情報も含まれています。

これらの証拠を総合的に活用することで、捜査官は誰がクラウドデータにアクセスしたのか、いつアクセスされたのか、どのような操作が行われたのかを再構築することができ、これは犯人の特定や時系列分析にとって不可欠である。
ログやメタデータは、デバイスや位置情報を間接的に示唆する場合もありますが、CHFI v11では、それらの主なフォレンジック価値は、暗号化アルゴリズムや物理的な所在ではなく、認証およびアクセス活動の証拠であることを強調しています。暗号化メカニズムは通常、クラウドプロバイダーによって抽象化および管理されており、ログ分析によって物理的な位置を特定できるとは限りません。
したがって、クラウドストレージのフォレンジックでは、ログとメタデータは主にユーザー認証とアクセス行動の分析に使用されるため、オプションDが正解であり、CHFIによって検証された回答となります。

質問: **66**
ユーザーがファイルを削除すると、システムはその詳細を保存するために$Iファイルを作成します。$Iファイルには含まれていない詳細は何ですか？
A. ファイル名
B. 削除日時
C. ファイルサイズ
D. ファイルの起源と変更
正解: **(**正解を表示します**)**

質問: **67**
以下のアプリケーションのうち、コンピュータ上のパスワードで保護されたすべてのアイテムを検出し、復号化できるパスワードクラッキングツールはどれですか？
A. Windowsパスワード回復ブートディスク
B. R-Studio
C. Windows用テストディスク
D. パスウェアキットフォレンジック
正解: **(**正解を表示します**)**

質問: **68**
あなたのチームは、社内ネットワーク内のサーバーから異常なトラフィックパターンを検出しました。調査の結果、見慣れない外部IPアドレスへの接続が複数確立されていることが判明しました。ネットワークトラフィックをキャプチャして分析したところ、トラフィックの内容はランダムで、既知のプロトコルと一致しないことがわかりました。これは何を示唆しているでしょうか？
A. このサーバーはボットネットの一部です。
B. サーバーはコマンド＆コントロールサーバーと通信しています。
C. サーバーがランサムウェアに感染しています。
D. サーバーはDDoS攻撃を受けています。

正解: **B** (コメントを発表する)
シナリオでは、見慣れない外国のIPアドレスへの確立されたアウトバウンド接続と、ランダムまたは非標準的なトラフィックが説明されており、これはコマンドアンドコントロール（C2）サーバーとの暗号化または難読化された通信を強く示唆しているため、オプションBが最適な回答です。CHFI v11には、マルウェア活動の検出、侵害の指標（IoC）、およびマルウェア操作に関連する疑わしいネットワーク動作の特定のためのトラフィック分析が明示的に含まれています。
コマンド＆コントロール通信は、通常の業務アプリケーションとは異なる独自のプロトコル、暗号化されたペイロード、あるいは秘密通信を使用する可能性があるため、しばしば異例に見える。接続が永続的で、未知の外部インフラストラクチャに発信されているという事実は、侵害されたホストが攻撃者によって制御されているシステムとの接続を維持していることを示す典型的な兆候である。
ボットネットはより広範なレベルで発生する可能性もあるが、観測されたトラフィックを最も直接的に解釈すると、C2サーバーとの活発な通信が考えられる。ランサムウェアはネットワーク証拠だけでは最適な答えとは言えず、DDoS攻撃の場合は通常、異なるトラフィック特性を示す。したがって、CHFIのネットワークフォレンジックの目的においては、このパターンはコマンド＆コントロールサーバーとの通信を最も強く示唆している。

質問: **69**
あなたは州警察のコンピュータ鑑識ラボに配属されました。注目度の高い刑事事件を担当するにあたり、あなたは適用されるすべての手順に従いましたが、上司は弁護側がラボ内で証拠が改ざんされたのではないかと疑うのではないかと懸念しています。証拠がラボに持ち込まれた時と同じ状態であることを証明するために、あなたは何ができるでしょうか？
A. 証拠のMD5ハッシュを作成し、証拠が最初に研究室に持ち込まれたときに取得された元のMD5ハッシュと比較する。
B. 州立研究所は認証を受けているため、この可能性のある主張について心配する必要はありません。
C. 証拠のMD5ハッシュを作成し、NISTが開発した標準データベースと比較する
D. 証拠品が研究所に持ち込まれた時と同じ状態であることを証明する声明書に署名する
正解: (正解を表示します)

質問: **70**
コンピュータハッキングのフォレンジック調査官が、「payload.exe」という名前のマルウェアサンプルを分析している。
彼らはテスト用ワークステーションでマルウェアを実行し、WhatChanged Portableというツールを使用して、マルウェア実行前後のシステム状態をキャプチャすることでホストの整合性を監視した。

これら2つのスナップショットを比較した結果、調査員は、Runレジストリキーの下にCjNWWyUJという名前のエントリが作成され、その値がC:\Users\\AppData\Local\Temp\xKNkeLQI.vbsであることを確認しました。この情報に基づいて、調査員はどのような結論を導き出すことができるでしょうか？
A. マルウェアがワークステーション上のシステムファイルを削除しました
B. マルウェアは起動時にマシンとの永続的な接続を確立します
C. マルウェアがWindowsレジストリを破損しました
D. マルウェアがサービス拒否攻撃を実行しています
正解: **B** (コメントを発表する)

質問: **71**
管理者が疑わしいネットワークトラフィックについて Cisco IOS ログを確認している際に、 %SEC-6-IPACCESSLOGP.」というニーモニックを含むログメッセージに遭遇しました。このメッセージは、指定されたアクセスリストのログ条件に一致するパケットが、TCP または UDP トラフィックのいずれかで検出されたことを示しています。このログエントリを説明しているのは次のうちどれですか？
A. アクセス制御リスト (ACL) ルールによりパケットが破棄されました。
B. ネットワーク上で接続試行の失敗が検出されました。
C. ネットワークトラフィック過多に関連するシステムレベルのエラーが発生しました。
D. アクセスリストで定義された基準に一致するパケットが許可または拒否され、監視のためにログに記録されました。
正解: (正解を表示します)

質問: **72**
Etherealを使用してPOP3トラフィックをチェックする場合、調査担当者はどのポートを検索すればよいでしょうか？
A. 143
B. 110
C. 125
D. 25
正解: (正解を表示します)

質問: **73**
サイバー犯罪捜査官が、ある企業のAWSインフラストラクチャにおけるデータ侵害を調査している。侵害されたサービスはAWSコンテナサービスに分類される。捜査官がまず重点的に調査すべき主要なセキュリティ面は、AWSではなく企業によって管理されていた可能性が高いが、それはどれだろうか？
A. 物理インフラおよび基盤サービス
B. コンテナサービスのネットワーク構成
C. アプリケーションプラットフォームとオペレーティングシステム (OS) のセキュリティ

D. データ管理とファイアウォール設定
正解: **C** (コメントを発表する)

質問: **74**
展示」ボタンをクリックします。ウェブサイトの脆弱性をテストするには、ユーザー名フィールドに引用符（？を入力します。「OK」をクリックすると、次のエラーメッセージウィンドウが表示されます。
このエラーウィンドウから何が推測できますか？

A. SQLインジェクションは不可能です
B. SQLインジェクションの可能性あり
C. 引用符（？は有効なユーザー名です
D. SQLデータベースの3306行目のユーザーのパスワードが脆弱です
正解: (正解を表示します)

質問: **75**
Windowsマシンにインストールした場合、TorブラウザはTorノードを介してネットワーク接続を確立するためにどのポートを使用しますか？
A. 49664/49665
B. 9150/9151
C. 49667/49668
D. 7680
正解: (正解を表示します)

質問: **76**
疑わしいPDFファイルの分析中に、調査員はファイル内に既知の脆弱性を持つJavaScriptコードを含むオブジェクトを発見しました。調査員は、この脆弱性のリスクと潜在的な影響を十分に評価するために、最も適切な対応策を決定する任務を負っています。脅威を包括的に分析するために、調査員は次に何をすべきでしょうか？
A. 脆弱性を特定するために、追加のスキャンを実行せずに、PDF 内の隠されたコンテンツや難読化されたコンテンツを探します。
B. エクスプロイトスキャンツールを使用して、特定された脆弱性に関連する既知のエクスプロイトのシグネチャを確認します。
C. JavaScript を安全なサンドボックス環境で実行して、その動作を観察し、潜在的な影響を理解します。

D. ファイルを別のツールで開き、別の形式で内容を調べて、より明確な情報を得るようにします。
正解: **(**正解を表示します**)**
調査担当者は既に疑わしいJavaScriptコードを特定しており、そのコードの実際のリスクと影響を理解する必要があるため、選択肢Cが最適な回答です。CHFI v11には、マルウェア分析：静的および動的分析、管理されたマルウェア分析ラボのセットアップの重要性、疑わしいWord、Excel、およびPDFドキュメントの分析が明示的に含まれています。また、サンドボックス環境でマルウェア分析を実行することも強調されています。
PDFファイル内に悪用可能なスクリプトが発見された場合、安全なサンドボックス内で動的に監視を行うことが、攻撃試行、ファイルのドロップ、プロセス生成、ネットワーク接続、永続化関連のアクションといった動作を特定する最も包括的な方法です。これは、既知のシグネチャを照合するだけの場合よりも、実際の影響について遥かに深い洞察を提供します。
オプションBは既知の悪用パターンを確認するのに役立つかもしれないが、範囲が狭く、行動を完全に評価することはできない。
オプションAはより詳細な分析の必要性を無視しており、Dは間接的すぎるため、最適な次のステップとは言えません。CHFIのマルウェアフォレンジックの目標に基づくと、包括的な対応策は、アーティファクトの特定から、サンドボックス内での制御された動的分析へと移行し、脅威を安全かつ徹底的に観察することです。

質問: **77**
テキサス州ダラスのデータセンターを標的としたサービス拒否攻撃の調査の結果、ネットワークアナリストは、攻撃者が特定のTCPフラグの組み合わせを持つパケットを継続的に送信し、接続が完了する前にサーバーのリソースを枯渇させる、非常に多くの半開TCPセッションを確認した。
パケットキャプチャの結果、SYNフラグとFINフラグの両方が同時に設定されたパケットが時折使用されていることも明らかになった。
観測された挙動を最もよく表す攻撃パターンはどれですか？
A. TCP SYNフラッド攻撃
B. TCP RSTフラッド攻撃
C. TCP ACKフラッド攻撃

D. TCP SYN-FINフラッド攻撃
正解: **(**正解を表示します**)**
最も正確な答えは D です。なぜなら、この質問では 2 つの異なる指標が明示的に一緒に言及されているからです。SYN フラッディングに典型的な半開き TCP セッションと、SYN フラグと FIN フラグの両方が設定されているパケットです。通常の TCP パケットでは、正当な接続設定で SYN と FIN を同時に使用することはないため、このフラグの組み合わせは非常に疑わしく、SYN-FIN フラッドパターンに直接対応します。純粋な SYN フラッドであれば半開きセッションを説明できますが、パケットキャプチャで SYN と FIN が同時に設定されているという指摘を完全に説明することはできません。CHFI v11 では、受験者はネットワーク トラフィックを分析してサービス拒否動作を検出し、異常な TCP フラグの組み合わせからパケット レベルの証拠を認識することが求められます。フォレンジック レビューでは、正確なフラグが重要になります。なぜなら、一般的なハンドシェイクの悪用と、リソースを枯渇させたり、単純なフィルタリングを回避したり、防御ロジックを混乱させたりするように設計された細工されたパケットを区別するのに役立つからです。このシナリオでは、珍しいSYN-FINの組み合わせが決定的な要素として含まれているため、より広範なSYNフラッド攻撃というラベルではなく、より正確なTCP SYN-FINフラッド攻撃というラベルが最適な回答となります。この選択は、パケットキャプチャで説明されているトラフィックの証拠を最もよく反映しています。

質問: **78**
サイバー攻撃事件の調査において、あなたはデジタル証拠の収集を担当するコンピュータハッキングフォレンジック調査官です。標的となったシステムは予期せずシャットダウンされており、攻撃中に重要なプロセスが実行されていたことが分かっています。システムがシャットダウンされたことで、どのような種類の証拠が失われる可能性があるでしょうか？
A. コマンド履歴やプロセスとポートのマッピングなどの揮発性データと、イベントログや隠しファイルなどの不揮発性データの両方
B. イベントログや隠しファイルなどの不揮発性データ。ただし、コマンド履歴やプロセスとポートのマッピングなどの揮発性データは除く。
C. コマンド履歴やプロセスとポートのマッピングなどの揮発性データは対象となりますが、イベントログや隠しファイルなどの不揮発性データは対象外となります。
D. コマンド履歴やプロセスとポートのマッピングなどの揮発性データも、イベントログや隠しファイルなどの不揮発性データも含まれません。
正解: **C (**コメントを発表する**)**

質問: **79**
侵入検知システム（IDS）は、コンピュータやネットワーク内部から情報を収集・分析し、不正アクセスや悪用など、セキュリティポリシーへの違反の可能性を特定します。

以下の侵入検知システムのうち、特定のホスト上で発生したイベントを監査するのはどれですか？
A. ログファイルの監視
B. ファイル整合性チェック
C. ホストベースの侵入検知
D. ネットワークベースの侵入検知
正解: **C** (コメントを発表する)

質問: **80**
フォレンジックアナリストのソフィアは、侵害されたサーバーのイベントログファイルを調査している。調査中に、イベントログヘッダーに異常と思われるエントリを発見した。そのエントリのELF_LOGFILE_HEADER値は、ログに記録が書き込まれたものの、イベントログファイルが正しく閉じられていないことを示している。
この情報に基づくと、SophiaはどのELF_LOGFILE_HEADER値を識別するでしょうか？
A. ELF_LOGFILE_HEADER_DIRTY 0x0001
B. ELF_LOGFILE_HEADER_ARCHIVE_SET 0x0008
C. ELF_LOGFILE_HEADER_WRAP 0x0002
D. ELF_LOGFILE_LOGFULL_WRITTEN 0x0004
正解: (正解を表示します)
オプション A. ELF_LOGFILE_HEADER_DIRTY 0x0001 が正解です。イベント ログ ヘッダーのダーティ フラグは、レコードが書き込まれたものの、ログが正常に閉じられなかったことを示しています。フォレンジックの観点からは、これは重要です。ログが不適切に閉じられていると、突然のシャットダウン、クラッシュ動作、または通常のシステム動作への意図的な干渉を示す可能性があるためです。CHFI v11 では、Windows イベント ログやその他の監査イベント、イベント ログ分析、およびログベースの証拠の信頼性と完全性を評価する必要性が明示的に含まれています。
その他の値は、異なる状態または条件を表します。WRAPは循環ログにおけるレコードの上書き動作に関連し、ARCHIVE_SETはアーカイブの状態を反映し、LOGFULL_WRITTENは質問で説明されている状態ではありません。手がかりは、レコードは存在するがログが適切に閉じられていないということなので、DIRTYの値がフォレンジック条件に最もよく一致します。
したがって、CHFI スタイルのイベントログ分析シナリオでは、Sophia はヘッダー値を ELF_LOGFILE_HEADER_DIRTY 0x0001 として識別する必要があります。

質問: **81**
マサチューセッツ州ボストンで発生した知的財産窃盗事件において、保管担当者が電子的に保存されたすべての情報を保持し、関連する可能性のあるデータの削除や変更を防止するよう正式に指示された場合、EDRMサイクルのどの段階が適用されていると言えるでしょうか？
A. 生産

B. 処理
C. 情報ガバナンス
D. 保存
正解: **D** (コメントを発表する)
正解はDです。保存は、潜在的に関連性のある電子的に保存された情報が、保持する法的義務が生じた際に、そのままの状態で保持され、変更または破壊されないようにすることに焦点を当てたEDRMの段階だからです。このシナリオでは、データを保持し、削除や変更を防止するよう管理者に正式に指示が出されている状況が説明されており、これはeDiscoveryの実践における典型的な保存ステップです。情報ガバナンスはより広範で、特定の問題が発生する前に一般的なデータ管理ポリシーを扱います。処理と出力は、データがすでに保存され収集された後に行われます。CHFI v11にはeDiscoveryプロセスフローと電子情報開示参照モデルサイクルが含まれているため、受験者は法的保留スタイルの活動を適切なEDRMフェーズに関連付けることが求められます。実際のフォレンジックおよび訴訟支援業務では、保存は証拠集団を汚染から保護し、後の収集とレビューが正当性を保つことを保証する段階です。質問は関連するESIを保持し、その変更を凍結することに焦点を当てているため、保存はまさに適用されている段階です。

質問: **82**
複雑な調査において、調査担当者は組織のメールクライアントによって生成された破損したファイル形式からメールデータを抽出する任務を負っています。調査担当者は、このファイルを広く互換性のあるEML形式に変換し、分析のためにデータに容易にアクセスできるようにするツールを必要としています。また、このツールは、さまざまなメールサーバーやWebベースのプラットフォームへの移行をサポートし、関連データのみを選択的に移行するための高度なフィルタリングオプションを備えている必要があります。このタスクに最も適したツールはどれでしょうか？
A. OSTからPSTへの変換用カーネル
B. メールチェッカー
C. ZeroBounce
D. EmailSherlock
正解: (正解を表示します)
CHFI v11の 電子メールフォレンジックとデジタル証拠の調査」の目標によると、調査官は、独自形式または破損した形式で保存されている電子メールデータを抽出、変換、分析できる必要があります。Microsoft Outlookは通常、メールボックスデータをOST オフラインストレージテーブル）ファイルに保存しますが、システムクラッシュ、内部犯行、マルウェア感染などのインシデントが発生すると、これらのファイルにアクセスできなくなったり、破損したりする可能性があります。
Kernel for OST to PSTは、OSTファイルをPST、EML、MSG、MBOXなどのアクセス可能な形式に復元および変換するように設計された、フォレンジックおよびeDiscovery専用のツールです。EML形式へのメールのエクスポート機能は、フォレンジック調査において特

に重要です。EMLは、多くのフォレンジックツールやメール分析プラットフォームで広くサポートされているためです。CHFI v11では、選択的抽出、フィルタリング、移行をサポートする信頼性の高いツールを使用することの重要性が強調されており、調査官は証拠の完全性を維持しながら、関連するメール、添付ファイル、ヘッダー、メタデータを分離することができます。
さらに、OSTからPSTへのカーネルは、さまざまなメールサーバーやウェブベースのプラットフォームへの移行をサポートしています。
これは、異種環境全体にわたる企業メール証拠の取り扱いに関するCHFIの要件に準拠するものです。
他の選択肢は不適切です。Email CheckerとZeroBounceはメールアドレスの検証ツールであり、EmailSherlockはメールボックスデータの抽出ではなく、メールアドレスの調査に重点を置いています。
したがって、CHFI v11の電子メール証拠の取得と変換に関するベストプラクティスに準拠して、OSTからPSTへのカーネルが正しい試験対応の回答となります。

質問: **83**
鑑識捜査官が重要な証拠を収集するためにスマートフォンを分析しています。デバイスの動作とデータフローを完全に理解するには、さまざまなモバイルアーキテクチャ層を把握する必要があります。デバイスの周波数変換を調査する際、捜査官は次のどのハードウェアコンポーネントに注目するでしょうか？
A. DAC/ADC
B. ベースバンド部
C. RF部
D. アンテナ
正解: **(**正解を表示します**)**

質問: **84**
フェニックスの物流倉庫で、捜査官は裁判所の許可を得て、悪意のある通信を中継している疑いのある複数のデバイスを組織的に押収した。デバイスの取り扱いと梱包の際、チームは、外部データ、環境干渉、または取り扱いミスによってデバイスの元の状態が損なわれることを防ぐことに重点を置いている。押収の時点で、この目的を最も効果的にサポートする手順上の重点は何か？
A. 権利の保護
B. 明瞭さと文書化
C. 汚染を避ける
D. 総合コレクション
正解: **C (**コメントを発表する**)**
正解はCです。このシナリオは、押収および梱包中の証拠の改ざん防止について具体的に扱っているからです。CHFI v11では、証拠保全が中心的な要件であり、これには、デジタル機器を物理的、環境的、または手続き上の汚染から保護し、機器の元の状態を変化させない

ようにすることが含まれます。質問では、外部データ、干渉、および取り扱いエラーについて言及していますが、これらはすべて汚染リスクに直接関係しています。権利の保護と文書の明確化は、重要な法的および手続き上の懸念事項ですが、説明されている直接的な取り扱い目的を最もよく捉えているとは言えません。包括的な収集とは、関連するすべての証拠を収集することですが、質問は既に押収されたものの完全性を維持することに焦点を当てています。法医学の実務において、汚染を回避するとは、慎重な梱包、適切なラベル付け、管理された取り扱い、および押収の瞬間から証拠を可能な限り変化させない保存方法を使用することを意味します。これは、機器が後で潜在的な痕跡、メタデータ、または不適切な取り扱いによって影響を受けた揮発性の状態について調査される可能性がある場合に特に重要です。CHFI試験の目的上、この目的を最もよくサポートする手続き上の焦点は、汚染の回避です。

質問: **85**
ルーターはOSI参照モデルのどの層で機能しますか？
A. 1
B. 5
C. 3
D. 4
正解: **(**正解を表示します**)**

質問: **86**
次のWindowsベースのツールのうち、ローカルまたはリモートでコンピュータにログインしているユーザーを表示するものはどれですか？
A. トークンモン
B. TCPView
C. プロセスモニター
D. PSLoggedon
正解: **(**正解を表示します**)**

質問: **87**
Linuxシステムが調査対象となっています。システムが電源オン状態の場合、調査担当者はどのディレクトリで現在の状態データを探すべきでしょうか？
A. /auth
B. /var/log/debug
C. /var/spool/cron/
D. /proc
正解: **D (**コメントを発表する**)**

質問: **88**
次のうち、サイバー犯罪の例ではないものはどれですか？

A. ソフトウェアの不正コピーを含む知的財産権侵害
B. コンピュータ記録の操作によって行われた詐欺
C. コンピュータセキュリティシステムの意図的な回避
D. 従業員の不正行為による解雇
正解: **(**正解を表示します**)**

質問: **89**
通話詳細記録（CDR）は、電話サービスで行われた通話に関するメタデータを提供します。次のデータフィールドのうち、CDRに含まれていないものはどれですか。
A. 通話時間
B. 着信を受けた電話番号
C. レコードを識別する固有のシーケンス番号
D. 通話の言語
正解: **(**正解を表示します**)**

質問: **90**
法執行官は、有効な令状に基づいて合法的な捜索を実施している。
捜索中に、警察官は令状に含まれていない、無関係の犯罪に関する証拠品を発見した。その証拠品は警察官の目にはっきりと見え、すぐに証拠品として認識された。この証拠が証拠能力を有することを説明する用語は何か？
A. ロカード交換原則
B. 明白な見解の原則
C. 犯罪行為そのもの
D. 一方的命令
正解: **(**正解を表示します**)**

質問: **91**
システムデータの抽出の一環として、ジェニファーはnetstatコマンドを使用しました。このツールは何を明らかにするのでしょうか？
A. ネットワーク接続に関する情報
B. コンピュータ使用状況のネットステータス
C. インターネットに接続しているユーザーの状況
D. ネットワークハードウェアの状態
正解: **(**正解を表示します**)**

質問: **92**
テキサス州オースティンで行われた組織的なおとり捜査において、捜査官はダークネット市場を支援する複数のプロバイダーに対し、法的手続きを実施した。複数のサービスからログや登録情報を入手したにもかかわらず、アカウント記録と加入者情報を関連付ける試みは繰り返し失敗し、犯人の特定は依然として困難を極めている。この障害を最もよく説明できるダークウェブフォレンジックの課題はどれか？
A. ダークウェブは犯人の身元を隠すため、犯人の特定は困難である。
B. 特殊ツールの使用に関する訓練と専門知識の不足がダークネット分析の課題となっている
C. 暗号化されたネットワークのため、犯人の物理的な位置を特定することは困難です。
D. 最新技術を用いてサイバー犯罪者が開発したダークウェブアプリケーションの検出は、従来の証拠抽出・分析ツールでは困難になる。
正解: **(**正解を表示します**)**
正解はAです。このシナリオにおける根本的な障害は、帰属の失敗です。捜査官は既にログやサービス側の記録を入手していますが、それでもなお、それらの証拠を現実世界の身元に確実に結びつけることができません。これがダークウェブのフォレンジックにおける決定的な難しさの一つです。ダークウェブの匿名化メカニズムは、ユーザーの身元を隠蔽し、追跡を困難にするように意図的に設計されています。CHFI v11のブループリントには、ダークウェブの概念、TORの動作、ダークウェブ調査のリスク、ダークウェブのフォレンジック上の課題が含まれています。これらの目標は、最大の障壁はデータの不足ではなく、匿名の活動を特定の人物に確実に結びつけることができないことだと受験者が認識できるようにするためのものです。オプションCは物理的な場所と暗号化されたネットワークに言及しており、関連性はありますが、質問は地理的位置よりも、身元相関と帰属の失敗に直接焦点を当てています。オプションBはアナリストの能力に焦点を当て、オプションDはツールの制限に焦点を当てていますが、どちらも説明されている主な問題ではありません。CHFIの用語で言えば、証拠は存在するものの、匿名性によって犯人が特定できない場合、最も適切な答えは、ダークウェブが犯人の身元を隠しているため、犯人を追跡するのは困難である、ということである。

質問: **93**
IoTアーキテクチャのどの層が、センサー、RFIDタグ、データ収集において重要な役割を果たすデバイスなどのハードウェア部品で構成されていますか？
A. エッジテクノロジーレイヤー
B. アプリケーション層
C. ミドルウェア層

D. アクセスゲートウェイ層
正解: **(**正解を表示します**)**

質問: **94**
認定倫理的ハッカーであるあなたは、ある民間企業から、侵入テストによる外部セキュリティ評価を実施するよう依頼されました。テストの詳細、関連する違反事項を記述し、組織の利益とテスターとしてのあなたの責任の両方を保護する文書はどれでしょうか？
A. 交戦規則
B. サービスレベル契約
C. 秘密保持契約
D. プロジェクトの範囲
正解: **(**正解を表示します**)**

質問: **95**
あなたは中西部の企業で侵入テストを実施しているセキュリティアナリストです。初期偵察の後、その企業が使用しているCiscoルーターのIPアドレスをいくつか発見しました。
ルーターのIPアドレスを含む以下のURLを入力します。
http://172.168.4.131/level/99/exec/show/config
このURLを入力すると、そのルーターの設定ファイル全体が表示されます。
あなたはどんな発見をしましたか？
A. Cisco IOSのオンラインにおける任意の管理者アクセス権限の脆弱性
B. HTML設定における任意の管理者アクセス権限の脆弱性
C. HTTP設定による任意の管理アクセス脆弱性
D. URL難読化による任意の管理者アクセス脆弱性
正解: **(**正解を表示します**)**

質問: **96**
サイバーセキュリティ調査官として、あなたは疑わしいシステムに対してシステム動作分析を行い、隠れたトロイの木馬を検出します。その方法の一つとして、起動プログラムを監視し、マルウェアによって加えられた変更を特定することが挙げられます。
捜査官はコマンドプロンプトでどのコマンドを使用すれば、ブートマネージャのすべてのエントリを表示し、起動メニューに追加された可能性のあるトロイの木馬をチェックできますか？
A. bootrec
B. bootcfg
C. msconfig
D. bcdedit
正解: **(**正解を表示します**)**
この質問は、CHFI v11の 「オペレーティングシステムフォレンジック」の目的、特にWindowsのブートプロセス分析とマルウェアが使用する永続化メカニズムに該当します。

最新のWindowsオペレーティングシステムは、ブート構成データ（BCD）ストアを使用して、ブート時の設定と起動エントリを管理します。マルウェアや高度なトロイの木馬は、BCDを改変して悪意のあるブートエントリを挿入したり、既存のエントリを変更してブートプロセスの早い段階で悪意のあるコードを実行させたりすることで、永続化を確立する可能性があります。
bcdeditコマンドラインユーティリティは、BCDエントリの表示、作成、変更、削除に使用される主要なWindowsツールです。CHFI v11では、bcdeditをブートマネージャ構成の調査、不正なブートローダーの特定、ルートキットやブートレベルのトロイの木馬を示す疑わしい起動変更の検出に不可欠なフォレンジックコマンドとして強調しています。
他の選択肢はあまり適していません。bootrecは主にブートレコードの修復に使用され、bootcfgはboot.iniを使用するレガシーシステムに適用され、msconfigはGUIベースのユーティリティであり、BCDブートエントリを完全に可視化することはできません。したがって、起動ベースの永続性を検出するためのCHFI v11フォレンジックのベストプラクティスに準拠して、bcdeditisは潜在的なトロイの木馬活動を検出するためにすべてのブートマネージャエントリを検査する適切なコマンドです。

質問: **97**
マイアミのテクノロジー企業で行われたマルウェア調査において、フォレンジックアナリストは、攻撃者が侵害されたワークステーション上で以前に実行されたプログラムの痕跡を削除することで、活動を隠蔽しようとした疑いがあるとみている。
捜査官が処刑行為や過去のプログラムの痕跡を消そうとする試みを再現する上で、最も有効な証拠源は何か？
A. Openfilesコマンドの出力
B. クリップボードの内容
C. ハッシュ値
D. ファイルのプリフェッチ
正解: **D** (コメントを発表する)
正解はDです。プリフェッチファイルは、どのプログラムが実行されたか、いつ実行されたか、どのくらいの頻度で起動されたかを再構築する上で最も有用なWindowsアーティファクトの1つだからです。Magnet Forensicsは、プリフェッチファイルはシステム上で実行されたアプリケーションに関する情報を提供し、貴重な実行履歴データが含まれていると指摘しています。そのため、調査官が攻撃者が他のプログラム活動の痕跡を削除しようとしたと疑う場合に特に重要になります。バイナリが後で削除されたとしても、プリフェッチアーティファクトは実行が行われたことを立証するのに役立つ可能性があります。CHFI v11にはWindowsファイルと実行関連のアーティファクトの分析が含まれており、プリフェッチはマルウェアの実行タイムラインをサポートするために使用される古典的なソースです。Openfilesの出力は一時的なもので履歴アーティファクトではなく、クリップボードの内容は以前のプログラム実行履歴とは無関係であり、ハッシュ値はファイルが存在する場合にのみファイルの識別または整合性を検証します。質問では、以前の実行活動を最

もよく再構築し、痕跡削除の試みの分析をサポートするソースを求めているため、プリフェッチファイルはリストされたオプションの中で最も強力なフォレンジックアーティファクトです。

質問: **98**
大規模なデータ漏洩事件において、サイバー攻撃者がフォレンジック対策としてプログラムパッカーを使用している疑いがあります。あなたは主任サイバーセキュリティ調査官として、この事態に対処するよう命じられました。このフォレンジック対策を無効化するために、次のうちどの対策が最も効果的でしょうか？
A. すべてのシステムでウイルス対策ソフトウェアを定期的に更新してください。
B. 解凍ツールを使用して、梱包プロセスを逆にして元のコードを明らかにします。
C. 安全なコーディング手法を導入する。
D. ネットワーク脆弱性スキャンの頻度を増やす。
正解: **(**正解を表示します**)**
選択肢Bが正解です。なぜなら、CHFI v11ではプログラムパッカーをフォレンジック対策技術として明確に特定しており、そのような技術を無効化または分析するために使用される関連フォレンジックツールの中に、プログラムパッカーの解凍ツールを別途リストアップしているからです。
パッカーは、悪意のあるコードを圧縮、難読化、またはラップして、その実際の内容を静的検査や一部のセキュリティツールから隠すためによく使用されます。。パックされたマルウェアを効果的に調査するには、調査担当者はラッパーをリバースまたは削除して、元の実行可能コードを検査できるようにする必要があります。これこそがアンパックツールの役割です。これは、CHFIが重点を置くフォレンジック対策とツール、そして調査担当者が詳細な調査の前に悪意のあるコンテンツを特定して抽出することを必要とするマルウェア分析の目標と一致しています。
他の選択肢は、パッキング技術そのものを直接的に無効化するものではありません。アンチウイルスソフトを更新することで検出精度が向上する場合もありますが、隠蔽されたコードを明らかにするものではありません。安全なコーディング手法や脆弱性スキャンは有効なセキュリティ対策ですが、パッキングされたマルウェアに対するフォレンジック的な対策ではありません。
したがって、最も効果的な対応策は、アンパックツールを使用して、分析対象となる基となるプログラムを露出させることである。

質問: **99**
刑事事件における証拠の取り扱い手順は、民事事件における証拠の取り扱い手順とどのように異なるのでしょうか？
A. 民事訴訟における証拠は、刑事訴訟における証拠よりも厳重に保管されなければならない。
B. 法執行機関に勤務していない限り、証拠手続きは重要ではありません

C. 刑事事件の証拠は、民事事件の証拠よりも厳重に保管されなければならない。
D. 証拠は事件の種類に関わらず、同じように取り扱われなければならない。
正解: **(**正解を表示します**)**

質問: **100**
「最良証拠原則」とは何ですか？
A. オープンなネットワーク接続、ユーザーのログアウト、メモリに常駐するプログラム、キャッシュデータなどの情報が含まれています。
B. 隠しファイル、スラック領域、スワップファイル、index.datファイル、未割り当てクラスタ、未使用パーティション、隠しパーティション、レジストリ設定、イベントログが含まれます。
C. システム時刻、ログオン中のユーザー、開いているファイル、ネットワーク情報、プロセス情報、プロセスとポートのマッピング、プロセスメモリ、クリップボードの内容、サービス/ドライバ情報、コマンド履歴が含まれます。
D. 裁判所は、文書、写真、録音の原本のみを証拠として認め、コピーは認めないと規定している。
正解: **D (**コメントを発表する**)**

質問: **101**
サイバー攻撃を受け、大手eコマースプラットフォームは広範囲にわたるシステムダウンに見舞われ、多大な経済的損失と顧客からの信頼失墜を被った。プラットフォーム側が制御を取り戻そうと奔走する中で、機密性の高い顧客データが侵害されたことが明らかになり、データセキュリティとプラットフォームの評判に脅威を与えている。eコマースプラットフォームへのサイバー攻撃の余波の中で、次のうち、フォレンジック対策の不備が原因ではない結果はどれか？
A. データの改ざん、削除、盗難
B. システムダウンタイム
C. 法務およびIT部門との連携は限定的である。
D. 法的に有効な証拠を収集できない
正解: **(**正解を表示します**)**
CHFI v11の「コンピュータフォレンジックの基礎」、「フォレンジック対応準備」、「インシデント対応統合」の目標によると、フォレンジック対応準備とは、組織が調査のコストと影響を最小限に抑えながら、デジタル証拠を効率的に収集、保存、分析、提示できる能力を指します。フォレンジック対応準備の不足は、主にインシデント発生後の組織による対応、調査、法的弁護能力に影響を与え、インシデントが業務の中断を引き起こすかどうかには影響しません。
システムダウンタイム（オプションB）は、DDoS攻撃、ランサムウェア感染、システム侵害などのサイバー攻撃による直接的な運用上の影響です。準備不足は復旧を遅らせる可能性がありますが、ダウンタイム自体はフォレンジック対策の不備によって引き起こされるも

のではなく、攻撃の技術的および運用上の影響によって引き起こされます。したがって、システムダウンタイムはフォレンジック対策の不備の結果ではありません。
それとは対照的に、他の選択肢は、CHFI v11におけるフォレンジック対応の不備に起因する、十分に立証された結果である。
準備不足は、法的に有効な証拠（オプションD）を収集できないという結果を招くことが多く、これは法廷での証拠能力に影響を与えます。役割、手順、エスカレーション経路が事前に定義されていない場合、法務チームやITチームとの連携が不十分になる（オプションC）ことがあります。さらに、適切な管理と監視が行われていない場合、データの改ざん、削除、盗難（オプションA）が見過ごされたり、追跡不能になったりする可能性があります。
CHFI試験ブループリントv4では、フォレンジック対応能力を、証拠の完全性、コンプライアンス、および捜査効率に焦点を当てた戦略的能力として強調しており、システムダウンタイムの防止や発生を目的としているわけではないため、オプションBが正解であり、試験内容に沿った回答となります。

質問: **102**
バッファオーバーフローの脆弱性は、Webアプリケーションがバッファを適切に保護できず、最大サイズを超える書き込みを許可した場合に発生します。そのため、_____が上書きされます。
バッファオーバーフローには、ヒープバッファオーバーフローやフォーマット文字列攻撃など、複数の種類があります。
A. 隣接するメモリ位置
B. 隣接する文字列の位置
C. 隣接するバッファ位置
D. 隣接するビットブロック
正解: **(**正解を表示します**)**

質問: **103**
犯罪現場で電子証拠を収集する際は、揮発性の高いものから低いものへと順に収集を進めるべきである。
A. 偽
B. 真
正解: **(**正解を表示します**)**

質問: **104**
デビッドソン・トラッキングは、ミシガン州デトロイトに3つの支店を持つ小規模な運送会社です。同社の女性従業員10人が弁護士に相談し、男性従業員から繰り返し嫌がらせを受け、経営陣が何の対策も講じなかったと訴えています。デビッドソン社には、嫌がらせに関する意識向上や、嫌がらせは容認されないことなど、すべての社内規定を定めた従業員ポリシーがあります。この件が裁判になった場合、検察官は会社のポリシーを遵守しなかったとして、誰を訴えるべきでしょうか？

A. IT担当者
B. 従業員自身
C. 方針書作成担当の事務アシスタント
D. 監督者
正解: **(**正解を表示します**)**

質問: **105**
企業調査の一環として、フォレンジック調査員のメリッサは、容疑者のノートパソコンのウェブブラウザの履歴、Cookie、キャッシュを調査するよう依頼されました。ノートパソコンには、Google Chrome、Firefox、Safariなど、複数のウェブブラウザがインストールされています。メリッサは、複数のウェブブラウザからこれらのデジタルアーティファクトを包括的に抽出・分析できるツールを必要としています。彼女はどのツールを使用すべきでしょうか？
A. ネットアナリシス
B. 探偵キット
C. エンケース
D. ディスクエクスプローラー
正解: **(**正解を表示します**)**
選択肢AのNetAnalysisが最適な回答です。なぜなら、この質問は複数のWebブラウザにわたるブラウザ履歴、Cookie、キャッシュの抽出と分析について具体的に尋ねているからです。CHFI v11では、ツールベースのオペレーティングシステムおよびアーティファクト分析の目的として、「Webブラウザに記録されたキャッシュ、Cookie、履歴を調査するツール」と「プライベートブラウジングおよびブラウザアーティファクトの復元」が明示的に含まれています。
ブラウザを跨いだインターネット活動の再構築に重点を置く場合、専用のブラウザアーティファクトツールが最も適切な選択肢となります。NetAnalysisはそのような作業のために設計されており、Chrome、Firefox、Safariなどのブラウザのトレースを単一のワークフローで分析できる点で、他の選択肢よりもはるかに的を絞ったツールです。
Sleuth Kitはファイルシステム分析には非常に優れていますが、ブラウザの痕跡を包括的に調査するには最適なツールとは言えません。EnCaseは幅広いフォレンジックツールですが、今回の質問はブラウザの履歴、Cookie、キャッシュに特化して最適なツールを求めています。DiskExplorerはこの要件にはあまり適していません。
したがって、CHFIのブラウザアーティファクトツールの目的に基づけば、NetAnalysisが最も正確かつ適切な回答となる。

質問: **106**
ノースカロライナ州の銀行コールセンターで発生したフィッシング攻撃への対応中に、チームは正常に開くもののマクロロジックが隠されている疑いのあるExcelスプレッドシートを受け取りました。マクロコードを抽出する前に、調査担当者はどのコマンドを実

行してOLEストリームを一覧表示し、マクロを含むストリーム（大文字のMでフラグ付けされている）を特定すべきでしょうか？
A. python oledump.py
B. python oledump.py -s
C. python oledump.py -v
D. python oledump.py -x
正解: **A** (コメントを発表する)
正解はAです。oledumpによる最初のトリアージ手順は、最初にストリームを選択せずにツールをファイルに対して実行し、OLEストリームを一覧表示してマクロを含むストリームを大文字でマークすることだからです。
M. Didier Stevens 氏の oledump ガイダンスでは、このツールは OLE ファイルの解析に使用され、最初の検査手順はドキュメントに存在するストリームを一覧表示することであると説明されています。通常、調査担当者は一覧表示後に -s などのオプションを使用して、より詳細な検査のために特定のストリームを選択します。これは、マクロ抽出が行われる前にストリームを一覧表示し、マクロコンテンツがどこにあるかを特定するコマンドを求める質問と一致します。CHFI v11 では、マルウェアフォレンジックに疑わしい Word、Excel、および PDF ドキュメントの解析が含まれているため、正しい最初のドキュメントトリアージワークフローを認識することが試験に関連しています。タスクは抽出やデコードではなく疑わしい OLE ストリームの発見であるため、基本的な oledump の呼び出しが、提供されているオプションの中で最良の回答です。

質問: **107**
メールアーカイブとは、メールに含まれるデータを体系的に保存 保護し、後日容易にアクセスできるようにする手法です。
A. 偽
B. 真
正解: (正解を表示します)

質問: **108**
ペンシルベニア州フィラデルフィアにある出版社で発生した職場ハラスメント調査の一環として、フォレンジック調査官は、macOSシステム上での勤務時間外のアプリケーション

使用状況と標的型メッセージの活動との相関関係を分析する必要があります。この分析では、集中管理インターフェースを通じて、ユーザーアクティビティ、システムログ、アプリケーション起動、エラーメッセージ、その他のイベント記録を確認する必要があります。調査官は、この分析を行うために何を開くべきでしょうか？
A. コンソール
B. ~/Library/Mail/ および ~/Library/Messages/ ディレクトリ
C. ターミナルに表示
D. /Users//フォルダ
正解: **(**正解を表示します**)**
正解はAです。macOSコンソールアプリケーションは、ログメッセージ、アクティビティ、エラー、および関連するシステムイベント情報を確認するために使用される集中型インターフェイスだからです。Appleのドキュメントには、コンソールはログメッセージとレポートを収集し、調査担当者がシステムおよび接続されたデバイスからログメッセージとアクティビティを検索できると記載されています。これは、ユーザーのアクティビティ、アプリケーションの起動、エラー、およびその他のイベントレコードを1か所で調査するという質問の要件に合致しています。MailおよびMessagesディレクトリにはアプリケーションデータとコンテンツアーティファクトが含まれており、後で役立つ可能性はありますが、ここで説明されている集中型ログ表示インターフェイスではありません。ターミナルはコマンドを使用してログにアクセスできますが、質問ではこの種の確認のために何を開くべきかを尋ねており、コンソールはまさにその目的のために直接構築されたmacOSのネイティブツールです。
CHFI v11にはmacOSのフォレンジックデータ、ログファイル、ディレクトリ、およびユーザーアクティビティ分析が含まれているため、受験者はコンソールがmacOS上のイベントログとアクティビティログを確認するための主要な入り口であることを認識しておく必要があります。営業時間外の使用状況とシステムイベントを相互チェックするには、コンソールが最適な開始インターフェースです。

質問: **109**
Androidデバイスに関するフォレンジック調査では、調査担当者はデバイスとAndroidソフトウェア開発キット（SDK）を実行しているコンピュータとの間で通信を確立する必要があります。この通信により、調査担当者はシステムファイル、ログ、およびその他の関連データにアクセスして分析を行うことができます。これを容易にするため、調査担当者はデバイス上で特定のAndroid開発者向け機能を有効にします。
デバイスがAndroid SDKを実行しているワークステーションと通信できるようにするには、どの機能を有効にする必要がありますか？
A. 鑑識調査員は、外部ワークステーションに接続されたAndroidデバイスでUSB制限モードを有効にすることができます。
B. 研究者は、実験室のセットアップで検査対象デバイス上でアップグレードモードをオンにすることができます。

C. 鑑識調査員は、ワークステーションに接続する前にデバイス上でリカバリーモードを起動できます。
D. 調査員は、分析対象となっている疑わしいデバイスでUSBデバッグモードを有効にすることができます。
正解: **(**正解を表示します**)**
この質問は、CHFI v11 のモバイルおよび IoT フォレンジックの目標、特に Android デバイスの取得と分析手順に直接対応しています。Android フォレンジックでは、デバイスと Android SDK を実行するフォレンジック ワークステーション間の通信は、主に Android Debug Bridge (ADB) を使用して行われます。ADB を使用すると、調査担当者はデバイスのファイルシステムとやり取りしたり、ログを取得したり、コマンドを実行したり、フォレンジック アーティファクトを制御された方法で収集したりできます。
ADBを使用するには、AndroidデバイスでUSBデバッグモードを有効にする必要があります。CHFI v11では、Androidデバイスにおける論理データ取得、ライブデータ収集、およびアプリケーションレベルの分析において、USBデバッグが重要な前提条件であることを明示的に強調しています。USBデバッグを有効にすると、証拠を不必要に改変する可能性のある侵襲的な方法を用いることなく、デバイスとフォレンジックワークステーション間の認証済み通信が可能になります。
USB制限モードではデータ通信が制限され、リカバリーモードは主にシステム修復やファームウェアの書き換えに使用され、「アップグレードモード」は標準的なAndroidフォレンジック機能ではありません。これらのいずれも、フォレンジック分析のための通常のSDKベースのインタラクションを可能にしません。したがって、CHFI v11 Androidフォレンジック手法に準拠するには、USBデバッグモードを有効にすることが、Android SDKワークステーションとの通信を確立するための正しく不可欠な手順となります。

質問: **110**
ある企業が、起動に失敗するWindowsサーバーの不具合を調査しています。ITフォレンジックチームが問題の原因究明を依頼されました。標準のWindowsブートプロセス（BIOS-MBR方式）に基づくと、BIOSが電源投入時自己診断テスト（POST）を完了した直後、マスターブートレコード（MBR）がロードされる前にシステムが失敗した場合、考えられる問題は何でしょうか？
A. OSカーネルntoskrnl.exeの読み込みに失敗しました
B. ブート構成データ（BCD）の障害
C. システム起動ディスクが検出されません
D. Bootmgr.exe の実行失敗
正解: **(**正解を表示します**)**

質問: **111**
鑑識捜査において、捜査官は容疑者のスマートフォンからデータを収集する必要があります。捜査官は、収集したデータが法廷で証拠として認められるよう、適切な手続きに従う必

要があることを認識しています。また、個人情報や機密情報が含まれている可能性のある携帯端末を取り扱う際には、法的および倫理的な問題にも留意しなければなりません。捜査官は、携帯端末からデータを収集する際に、法的要件を確実に遵守するために、どのような措置を講じるべきでしょうか？
A. デバイス所有者から許可を得て、証拠収集プロセスが適用される規制に準拠していることを確認してください。
B. データ収集中に外部からの干渉を避けるため、デバイスをインターネットから切断しますが、この操作を記録しないでください。
C. 互換性や規制遵守を確認せずに、利用可能なフォレンジックツールを何でも使用する。
D. 調査を迅速化するため、プロセスを文書化せずにモバイルデバイスからデータを収集します。
正解: **(**正解を表示します**)**
選択肢Aが正解です。CHFI v11は、特にデータに個人情報や機密情報が含まれる可能性がある状況において、証拠の法的かつ倫理的な取り扱いを非常に重視しています。この設計図には、同意の取得、デジタル証拠の取り扱いに関するベストプラクティス、法的問題、プライバシー問題と法令遵守、証拠の保全、および証拠保全の連鎖が明確に含まれています。これらの要件は、多くの場合、非常にプライベートなデータが含まれているため、慎重かつ合法的な取り扱いが求められるモバイルデバイスに直接適用されます。
デバイス所有者からの許可を得ること、または適切な法的権限を確保することは、証拠能力と専門的なフォレンジック実務の基礎となります。同様に重要なのは、証拠収集プロセスが適用される規制を遵守し、適切に文書化されていることです。CHFIはモバイルフォレンジックプロセスについても解説しており、適切なフォレンジック作業には手順、文書化、そして法的にも有効な証拠の取り扱いが必要であることを強調しています。
オプションBは運用上有用な場合もあるが、その行為を記録しないことは、法医学上の重大な弱点となる。オプションCは、ツールの適合性や法的遵守を無視している。オプションDは、記録されていない収集行為が証拠の信頼性を損なうため、証拠能力を直接的に損なう。したがって、CHFIの原則に最も合致し、法的にも妥当な対応策は、許可を得て、プロセスが関連する法的要件に準拠していることを確認することである。

質問: **112**
ボブはシステムクラッシュに見舞われ、Windowsコンピューターのハードドライブに保存されていた重要なデータを失ってしまいました。クラウドストレージやバックアップ用のハードドライブは持っていません。彼は、個人の写真、音楽、文書、ビデオ、公式メールなど、すべてのデータを復元したいと考えています。ボブの目的を達成できるツールは次のうちどれでしょうか？
A. レキュバ
B. コラソフトのカプサ
C. エクスプリコ
D. カインとアベル

正解: (正解を表示します)

質問: **113**
CHFI（企業不正調査の専門家であるジェニーは、大手銀行における企業不正の可能性に関する事件を担当することになった。銀行の内部告発者がテラバイト規模のデータをオンラインに流出しており、ジェニーはそのデータを証拠として調査しなければならない。膨大なデータ量に加え、証拠保全の義務と、調査結果が法廷で使用できることを保証する必要があるため、ジェニーの任務は非常に困難だ。誤ったアプローチを取ると事件が危うくなることをジェニーは理解しており、最初のステップを慎重に選択する必要がある。この膨大なデジタル証拠に効果的に対処するために、ジェニーはどのような戦略をとるべきだろうか？
A. 漏洩したデータを漏洩元から直接調査する
B. 内部告発者の情報に基づいて漏洩データを優先し、選択的に調査する。
C. データ整合性と保管管理の連鎖を維持するため、調査前に漏洩したすべてのファイルのハッシュ値を作成する。
D. 流出したデータをダウンロードし、チーム内で共有して並行分析を行う。
正解: (正解を表示します)
選択肢Cが最も有力な答えである理由は、このシナリオが2つの重要な鑑識要件を強調しているからである。
証拠の保管管理の連鎖を維持し、調査結果が法廷で使用できることを保証する。CHFI v11は、証拠の保全、保管管理の連鎖、データ取得方法、およびデータ取得の検証を非常に重視している。これらの目標は、詳細な分析を開始する前に、調査官がまず証拠の完全性を維持し、それを正当性のある方法で文書化する必要があることを明確に示している。
漏洩したファイルのハッシュ値を最初に作成することで、証拠が取り扱い、保管、またはその後の検証中に改ざんされていないことを証明するための基準が得られます。これは、非常に大規模なデータセットを扱う場合や、複数の捜査官が関与する場合、あるいは後日法廷で精査される場合に特に重要です。ハッシュ化は整合性の検証をサポートし、より広範な証拠保全プロセスに直接結びつきます。
オプションAは、検証されていない証拠を検証するリスクを伴います。オプションBは、後々のトリアージに役立つ可能性がありますが、整合性管理の前に実施すべきではありません。オプションDは、適切な保存と検証の前に実施すると、証拠管理が不十分になるリスクを高めます。したがって、CHFIのデータ取得および法的証拠の原則に基づき、ジェニーは実質的な分析を行う前に、まずファイルをハッシュ化し、証拠の整合性を維持する必要があります。

質問: **114**
コンピュータハッキングフォレンジック調査官として、あなたは疑わしい侵害発生時のネットワークトラフィックのTCPダンプを分析しています。調査中に、kernel?countによってドロップされたパケット数が異常に多いことに気づきました。

ネットワークの負荷が高いことを考えると、この状況の最も可能性の高い原因は何でしょうか？
A. Tcpdumpで使用したブール式が厳しすぎたため、一部のパケットが欠落していました。
B. Tcpdumpを実行しているOSのバッファ領域が不足していたため、パケットがドロップされました。
C. TCPパケットがTcpdumpの入力式と一致しませんでした。
D. Tcpdumpツールを-cフラグなしで実行したため、パケットを無期限にキャプチャし続けた。
正解: **B** (コメントを発表する)

質問: **115**
Windows は、以下のどれを調べて、どのアプリケーションでファイルを開くかを判断しますか？
A. ファイル拡張子
B. ファイル属性
C. ファイル末尾のファイル署名
D. ファイルの先頭にあるファイル署名
正解: (正解を表示します)

質問: **116**
プロファイリングとは、犯人の様々な活動から犯人を特定することを目的として証拠を分析する鑑識手法です。ハッカーによってコンピュータが侵害された後、事件のプロファイルを作成する上で最も重要なのは次のうちどれでしょうか？
A. 攻撃に使用されたコードの論理、フォーマット、および洗練度
B. 攻撃の性質
C. システムの製造元が侵害された
D. 今回の事件で悪用された脆弱性
正解: **A** (コメントを発表する)

質問: **117**
NTFSはFATよりもスラック領域が少ないため、スラック領域にデータを隠す可能性が低い。その理由は以下のとおりである。
A. NTFSはクラスタサイズスペースが小さい
B. FATは古くて非効率的なファイルシステムです
C. NTFSはジャーナリングファイルシステムです
D. FATはファイルのインデックスを作成しません
正解: (正解を表示します)

質問: **118**

テキサス州ヒューストンで発生した医療IoTシステムの侵害事件において、調査官は複数のウェアラブルデバイスが初期設定の認証情報を使用していることを発見した。攻撃者はこれらの設定を悪用し、基本的なアクセス制御を回避してデータを傍受した。この侵害を最も直接的に引き起こしたIoTスタックの問題点はどれか？
A. 安全でないAPI
B. 不適切な通信暗号化
C. デフォルトパスワード
D. ストレージと通信に暗号化は適用されません
正解: **C** (コメントを発表する)
正解はCです。このシナリオでは、デバイスが初期設定の認証情報を使用していたことが明記されており、これはデフォルトパスワードによって直接的に脆弱性が露呈したことを意味します。OWASPのガイダンスでは、デフォルト認証情報に関して、adminなどの一般的な工場出荷時のユーザー名とパスワード、あるいは単純なプリセット値は、攻撃者が推測したり再利用したりして不正アクセスを行う可能性があるため、重大な脆弱性であると説明されています。CHFI v11にはIoTセキュリティの問題とOWASP Top 10 IoT脆弱性が含まれているため、受験者は接続されたデバイスにおける侵害の直接的かつ一般的な原因としてデフォルト認証情報を認識することが求められます。他の選択肢は異なるセキュリティ上の脆弱性について説明していますが、ここで使用されているアクセス経路とは一致しません。
安全性の低いAPIや脆弱な暗号化は他のリスクを生み出す可能性がありますが、質問では攻撃者が変更されていないデフォルト設定を利用してアクセス制御を回避したと述べています。これは、デフォルトパスワードが攻撃を可能にした条件であることを具体的に示しています。フォレンジック分析において、侵害経路が変更されていないメーカーの認証情報と結びついている場合、最も正確で妥当な答えはデフォルトパスワードです。

質問: **119**
一連の動作や出来事の後、システムや機械に生じた変化を調査するプロセスを何と呼びますか？
A. Windowsサービス監視
B. システムベースライン設定
C. ホスト整合性監視
D. スタートアッププログラムのモニタリング
正解: (正解を表示します)

質問: **120**
ユタ州ソルトレイクシティにある製造会社で発生した内部犯行によるデータ漏洩事件の調査中、捜査官はキャプチャしたパケットファイルをNetworkMinerに読み込み、オフライン分析を行いました。トラフィックには様々なアプリケーション層プロトコルが含まれており、チームはファイル再構築やホストプロファイリングに進む前に、トラフィックから解

析されたユーザー名とパスワードをまとめて表示する必要があります。どのタブを開くべきでしょうか？
A. ファイル
B. 資格情報
C. ホスト
D. セッション
正解: **B** (コメントを発表する)
正解はBです。NetworkMinerの 認証情報」タブは、パケットキャプチャから抽出されたユーザー名、パスワード、その他の認証情報を表示するために特化して使用されているからです。NetworkMinerのドキュメントとチュートリアルでは、このツールはPCAPデータを解析して、ファイル、メール、証明書、認証情報などの上位レイヤーのアーティファクトを抽出できると説明されています。調査担当者は、他の分析タスクに進む前にユーザー名とパスワードをまとめて確認したいと考えているため、 認証情報」タブが最も直接的に情報を確認できる場所です。 ファイル」タブは再構築された転送オブジェクト、 ホスト」タブはエンドポイントとトラフィックの概要、 セッション」タブは会話レベルの詳細に使用されますが、いずれも認証情報専用のビューではありません。
CHFI v11にはネットワークフォレンジックとパケット分析が含まれているため、受験者はどのツールが有用かだけでなく、それらのツール内のどの特定のインターフェースが特定の調査目的をサポートするのかを理解していることが求められます。
ネットワークトラフィックで検出された可能性のあるユーザー名とパスワードを迅速にトリアージすることが目的の場合、適切なNetworkMinerタブは 認証情報」です。

質問: **121**
鑑識捜査官とは、証拠の保全、特定、抽出、文書化といった捜査プロセス全体を担当する人物です。捜査官は、サイバー犯罪分析に関連する多くの役割と責任を担っています。鑑識捜査官の役割は以下のとおりです。
A. 証拠を極秘扱いとし、法執行機関から証拠を隠す
B. 調査を行うにあたり、組織の全従業員から許可を得る。
C. 潜在的な証拠を改ざんすることなく、元の証拠のイメージバックアップを作成する
D. 組織のネットワークセキュリティを強化する
正解: **C** (コメントを発表する)

質問: **122**
上記のNMAPコマンドは、次のうちどれを実行しますか？
> NMAP -sn 192.168.11.200-215
A. トレーススイープ
B. オペレーティングシステムの検出
C. ピングスキャン
D. ポートスキャン
正解: **(**正解を表示します**)**

質問: **123**
以下の記述のうち、事例評価を裏付けていないものはどれですか？
A. 事件調査員のサービス依頼内容を確認する
B. 証拠に対して他の法医学的手続きを行う必要があるかどうかを検討する
C. 法医学鑑定依頼の法的根拠を特定する
D. 保管履歴を記録しないでください
正解: **(**正解を表示します**)**

質問: **124**
サイバー犯罪者がWindowsコンピュータから証拠を隠滅しようとしています。彼はevldence1.docというファイルを削除し、Windowsのごみ箱に移動させました。その後、サイバー犯罪者はごみ箱を空にしました。ごみ箱から削除された後、データはどうなりますか？
A. データは上書きされるまで元のクラスター内に保持されます
B. データはゼロで上書きされます
C. データは未割り当て領域内の新しいクラスターに移動されます
D. データが破損し、復元不可能になります
正解: **A (**コメントを発表する**)**

質問: **125**
ワシントン州シアトルの病院で発生しているランサムウェア攻撃において、捜査官は厳しい時間的制約の中でストリーミングログを分析し、出力結果に基づいて判断を下さなければならない。この要件に合致するログのフォレンジック調査のカテゴリーはどれか？
A. 進行中の攻撃中にリアルタイム分析が実行され、その結果も生成されます
B. 事件の正確な原因と、将来同様の事態が発生しないようにするために必要な一連の行動に関する詳細を含む成果物が作成される。
C. 捜査官は、ネットワーク内で既に発生した事件を検出 -調査するために、事後分析を実施する。

D. 捜査官はログファイルを複数回調べることができます
正解: **(**正解を表示します**)**
回答Aが正解です。質問では、進行中のインシデント中にログをリアルタイムで確認し、運用上の意思決定を支援するために即座に結果を生成するという分析が明確に説明されています。これはリアルタイムログ分析の定義であり、事後分析ではありません。CHFI v11は事後分析とリアルタイム分析の両方を網羅しており、この区別は試験シナリオにおいて重要です。リアルタイム分析は、インシデントがまだ進行中で、調査担当者が攻撃者の行動、システムへの影響、および対応の優先順位を即座に把握する必要がある場合に使用されます。一方、事後分析はインシデント発生後に行われ、既に発生した事象を理解することに重点を置いています。オプションBは、後日報告または教訓として得られた結果を説明しており、オプションDは特定の試験カテゴリを表すには一般的すぎます。ランサムウェア危機では、封じ込め、影響を受けるシステムの隔離、および進行中の悪意のあるアクションの特定をガイドするために、ストリーミング証拠を継続的にレビューする必要がある場合がよくあります。シナリオでは、アクティブな攻撃状況と即時の分析出力が強調されているため、CHFIに準拠した正しいカテゴリはリアルタイム分析です。これは、説明されている試験のタイミングと目的の両方に一致する唯一の選択肢です。

質問: **126**
起動プロセス後の悪意のあるプログラムの影響を理解し、ディスクパーティションから最新の情報を収集するために、調査担当者は次の内容を評価する必要があります。
A. MBR
B. UEFI
C. BIOS
D. GRUB
正解: **(**正解を表示します**)**

質問: **127**
CHFI（認定セキュリティ情報担当者）は、非常に複雑で多層的なセキュリティ侵害調査において、Windowsセキュリティログの分析を任されました。この侵害では、アカウントの作成、権限昇格、サービスのインストールが短時間のうちに連続して発生しました。調査担当者は、これらの事象を時系列的に裏付けるイベントIDの組み合わせを取得する必要があります。調査担当者は、どのイベントIDの組み合わせに注目すべきでしょうか？
A. イベントID 624、イベントID 500、およびイベントID 7045
B. イベントID 624、イベントID 4670、およびイベントID 6011
C. イベントID 4720、イベントID 500、およびイベントID 6011
D. イベントID 4720、イベントID 4672、およびイベントID 7045
正解: **D (**コメントを発表する**)**

質問: **128**

POP3（Post Office Protocol 3）は、ユーザーがメールをダウンロードするとすぐにサーバー上のメールを削除する、メール受信のための標準プロトコルです。メッセージが到着すると、POP3サーバーはそれを受信者のアカウントファイルの末尾に追加し、メールクライアントはいつでも好きなときにそのファイルを取得できます。メールクライアントは、デフォルトでは_____にあるPOP3サーバーに接続してメールを取得します。
A. ポート115
B. ポート109
C. ポート123
D. ポート110
正解: **(**正解を表示します**)**

質問: **129**
あなたは法医学捜査官として、製造会社における産業スパイ事件を調査しています。内部関係者が機密のCAD設計を盗んだ疑いがあります。容疑者のコンピュータはWindows OSで動作しており、隔離されています。会社のITチームが誤ってコンピュータをシャットダウンしたため、揮発性データが失われた可能性があります。このような状況で、不揮発性データを取得する最善の方法は何でしょうか？
A. フォレンジックブートディスクを使用してコンピュータを起動し、取得を進めます。
B. ネットワークベースの取得ツールを使用して、リモートでデータにアクセスして取得します。
C. 通常のOSを使用してコンピュータを起動し、ソフトウェアの書き込みブロッカーを使用します。
D. ハードドライブを取り外し、フォレンジックワークステーションに接続してから、データ取得を実行します。
正解: **(**正解を表示します**)**
選択肢Dが最適な答えです。システムは既にシャットダウンされているため、揮発性証拠は失われている可能性が高く、残された最優先事項は、可能な限りフォレンジック的に安全な方法で不揮発性データを保存および取得することです。CHFI v11では、データ取得方法論、最適な取得方法の選択、証拠の完全性の維持、およびソースメディアの変更を避けるための管理された手順の使用が重視されています。この状況では、ハードドライブを取り外してフォレンジックワークステーションに接続することが、信頼性の高いディスクイメージを取得するための最も安全で標準的な方法です。
容疑者のコンピュータを、フォレンジックブートディスクまたは通常のオペレーティングシステムのどちらで起動する場合でも、ファイルシステムのメタデータ、ログ、一時ファイル、その他のアーティファクトを変更する可能性があるため、リスクが伴います。特に通常のOSを使用することは危険です。また、マシンは既に隔離され電源が切られているため、ネットワークベースの取得も適切ではありません。
取り外したドライブから直接フォレンジックデータを取得することで、証拠源への不要な変更を最小限に抑え、CHFIの原則である保存、管理された取り扱い、再現可能なイメージ

ングに合致させることができます。したがって、不揮発性データ取得における正しい次のステップは、ドライブを取り外し、フォレンジックワークステーションからイメージングすることです。

質問: **130**
コンピューター技術者のゲイリーは、職場のコンピューターを使って子供たちと知り合いになり、わいせつな成人向け画像を送信したとして、オンラインで子供たちを虐待した疑いが持たれています。この事件にはどのような種類の捜査が必要でしょうか？
A. 刑事捜査と行政捜査の両方
B. 刑事捜査
C. 民事調査
D. 行政調査
正解: **(**正解を表示します**)**

質問: **131**
ディスクの損傷した部分で、読み書き操作が実行できない部分は、
_____。
A. 空きセクター
B. 不良セクター
C. 未使用セクター
D. ロストセクター
正解: **B (**コメントを発表する**)**

質問: **132**
_____とは、攻撃者が攻撃手順を手動で実行するのではなく、コンピュータプログラムによって実行される攻撃のことです。
A. ブラックアウト攻撃
B. 自動攻撃
C. 中央処理装置への攻撃
D. 分散型攻撃
正解: **(**正解を表示します**)**

質問: **133**
Microsoft Azure環境における設定ミスによる侵害に関するフォレンジック調査において、調査担当者は、クライアント組織がユーザーID、エンドポイントデバイス、およびデータを管理し、Microsoftが物理ホスト、ネットワーク、およびデータセンターの運用を担当していることを確認しました。このような責任分担を最もよく表しているクラウドサービスモデルはどれでしょうか？
A. オンプレミス展開
B. サービスとしてのソフトウェア $aaS）

C. サービスとしてのインフラストラクチャ（IaaS）
正解: **(**正解を表示します**)**
正解はCです。質問で説明されている責任の分担は、Infrastructure as a Service（IaaS）に最も近いからです。MicrosoftのAzure共有責任に関するドキュメントでは、サービスモデルがSaaS、PaaS、IaaSのいずれであるかによって責任が異なると説明されています。IaaSでは、プロバイダーは物理データセンター、物理ホスト、ネットワークファブリック、コアインフラストラクチャを担当し、顧客はID、エンドポイント、データ、オペレーティングシステム、ワークロード構成など、環境内で実行されるものの大部分を担当します。これは、Microsoftがスタックの大部分を管理するSaaSよりも、シナリオにずっと近いものです。オンプレミス展開では、組織自体がほぼすべての責任を負うことになり、これも当てはまりません。CHFI v11には、クラウドコンピューティングサービスモデル、クラウドの脅威、クラウドフォレンジックが含まれているため、受験者は、どのレイヤーを誰が管理しているかを調べて、フォレンジックシナリオを適切なサービスモデルに関連付けることが求められます。Microsoftが物理的なクラウドインフラストラクチャを管理し、顧客がコアとなる使用側のコンポーネントとデータを管理するため、最適な答えはInfrastructure as a Serviceです。

質問: **134**
複雑なサイバー犯罪捜査において、法医学専門家は、使用可能なファイルシステムメタデータが欠落した、著しく断片化されたハードドライブに遭遇した。彼らは高度なファイルカービング技術を用いることで、データ難読化のために意図的にファイル拡張子を操作した容疑者によって隠蔽された重要な証拠の復元に成功した。
ファイルシステムメタデータが欠落した断片化されたハードドライブから隠しファイルを復元するために、法医学捜査官はどのような高度な手法を用いるのでしょうか？
A. ファイルシステムアーキテクチャをゼロから再構築する。
B. 高度なアルゴリズムを使用して暗号化されたファイルを復号します。
C. ファームウェアレベルのアクセスを使用して、アクセスできないセクターからファイルを抽出します。
D. 未割り当て領域内のファイルシグネチャとパターンを分析します。
正解: **(**正解を表示します**)**
CHFI v11のアンチフォレンジック技術とデジタル証拠分析の目的によると、攻撃者はファイルの削除、ファイルシステムメタデータの破損、データの断片化、ファイル拡張子の操作などによって検出を回避しようとすることが多い。MFT、FAT、ディレクトリエントリなどのファイルシステム構造が欠落または破損している場合、従来のファイル復元方法は機能しない。このような状況では、捜査官はファイルカービングに頼る。

。
ファイルカービングは、ファイルシステムのメタデータではなく、ファイルシグネチャ（ヘッダーとフッター）とコンテンツパターンに基づいてファイルを復元する高度なフォレンジック技術です。CHFI v11では、ファイルカービングは未割り当て領域、スラック領域、

および生ディスクセクターをスキャンして、特定のファイルタイプに関連付けられた既知のバイトパターン（たとえば、JPEGヘッダーFFD8FFE0やPDFヘッダー%PDFなど）を識別すると説明されています。これにより、ファイル名、拡張子、およびディレクトリ情報が意図的に変更または破壊されている場合でも、捜査官はファイルを復元できます。
この手法は、ファイル拡張子の不一致やメタデータの消去といったフォレンジック対策に対して特に効果的です。ファイルカービングでは必ずしも元のファイル名やタイムスタンプが復元されるとは限りませんが、隠蔽または削除されたファイルの実際の内容を復元するには非常に有効です。その他の方法はCHFIの手法とは合致しません。ファイルシステムをゼロから再構築するのは非現実的であり、復号化は別の問題に対処するものであり、ファームウェアレベルのアクセスは標準的なフォレンジック復元方法ではありません。
CHFI v11では、メタデータが欠落した断片化ドライブから証拠を復元するための正しいアプローチとして、シグネチャベースおよびパターンベースのカービングが明確に示されています。したがって、正解は未割り当て領域のファイルシグネチャとパターンを分析することであり、オプションDが正解となります。

質問: **135**
マルウェアのフォレンジック調査中に、侵害されたシステム上でマルウェアが実行された後、Windowsの自動起動レジストリキーに新たに追加されたエントリが特定されました。このエントリは、「CaoCIboog.vbs」という名前のVBスクリプトファイルが「Run」キーにインストールされ、永続化を実現し、ユーザーログイン時に自動的に実行されることを示しています。コンピュータハッキングフォレンジック調査官（CHFI）として、レジストリハイブのどこにこの疑わしいエントリがあると予想しますか？
A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup
C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
正解: **(正解を表示します)**

質問: **136**
イリノイ州シカゴの市当局で発生したスマートシティ監視システムの侵害事件において、捜査官は現場センサーからクラウドサービスへの異常なデータフローを特定した。クラウドサービスでは、データ集約、データフィルタリング、アクセス制御、デバイス情報検出などの中間処理が行われており、ポリシー違反が明らかになる可能性がある。
ハードウェアとアプリケーション間のインターフェースとして機能するIoTアーキテクチャのどのレイヤーに焦点を当てるべきでしょうか？
A. エッジテクノロジーレイヤー
B. ミドルウェア層
C. アプリケーション層

D. アクセスゲートウェイ層
正解: **B** (コメントを発表する)
正解はBです。IoTアーキテクチャのミドルウェア層はデバイスとアプリケーションの間に位置し、データ集約、フィルタリング、変換、アクセス処理、情報発見などの機能を担当します。IoTミドルウェアに関する文献では、異種混在のIoTコンポーネントを管理し、ハードウェア側の活動をアプリケーション層に接続するソフトウェア層を提供すると述べられています。これは、調査担当者が集約、フィルタリング、アクセス制御、デバイス発見動作を通じてポリシー違反が明らかになる可能性のある中間処理段階に関心を持っているため、シナリオと完全に一致します。CHFI v11にはIoTアーキテクチャ、IoTの脅威、IoTフォレンジック分析が含まれているため、受験者はデバイスと上位レベルのサービス間の調整と処理を実行する層を特定することが求められます。アプリケーション層はユーザー向けサービスが存在する場所であり、エッジとゲートウェイの概念は通信に参加する可能性がありますが、質問に挙げられている広範なインターフェースと処理の責任は、ミドルウェアと最も明確に一致します。したがって、最適な答えはミドルウェア層です。

質問: **137**
サイバー攻撃のフォレンジック調査において、チームは侵害されたネットワーク内での攻撃者の行動を追跡するために、一連の出来事の時系列を再構築する任務を負う。しかし、システムログや重要な文書を詳しく調べていくうちに、フォレンジックチームは矛盾点に気づく。攻撃中に変更されたはずのファイルには、攻撃者が既にシステムを離れた後に変更されたことを示すタイムスタンプが表示されているのだ。バックアップやシステムログにはさらに異常なパターンが見られ、一部のファイルは通常の運用時間中に変更されたようで、実際の出来事の順序を隠蔽するために改ざんが行われた可能性が示唆される。
これらの矛盾点から、捜査官は、攻撃者がフォレンジックのタイムラインを混乱させるために、重要なファイルのタイムスタンプを意図的に操作したのではないかという疑念を抱いている。この戦術は、捜査チームを混乱させ、侵害の再現を妨害することを目的としており、悪意のある活動が通常の業務の一部であったかのように見せかけ、捜査を意図的に誤導しようとする意図的な試みを示している。このような行動は、どのフォレンジック対策技術に最も該当する可能性が高いか？
A. システムから不正な活動の痕跡をすべて削除するためのアーティファクト消去。

B. 代替データストリーム (ADS) を使用して、検出を回避する方法で悪意のあるファイルを保存および隠蔽します。
C. ファイルメタデータを破損させることでトレイルを難読化する。
D. プログラムパッカーは実行可能ファイルを圧縮および隠蔽し、分析を困難にします。
正解: **C** (コメントを発表する)
シナリオでは、捜査官を混乱させ、事件のタイムラインを歪めるために、タイムスタンプとメタデータを意図的に操作することが説明されているため、オプションCが最適な回答です。CHFI v11では、主要なフォレンジック対策技術として、トレイルの難読化とデータ/メタデータの上書きが明示的に挙げられており、タイムライン分析、メタデータ調査、およびフォレンジック再構築を誤導することを目的とした行為を検出する必要性も強調されています。
このような行為は、痕跡隠蔽の典型的な形態です。攻撃者は、ファイル時刻や関連するメタデータを改ざんすることで、悪意のある行為を正常なもの、あるいは無関係なものに見せかけ、捜査官が事件を正確に再現する能力を損なおうとします。これは、一般的な痕跡削除よりも具体的であり、質問の事実により合致しています。
アーティファクト消去は証拠の完全な除去に重点を置き、ADSは代替ストリームにデータを隠蔽し、プログラムパッカーは実行可能コンテンツを隠蔽します。これらのいずれも、時系列を偽装することを目的としたタイムスタンプの操作を直接説明するものではありません。したがって、CHFIのフォレンジック対策フレームワークにおいて、最も正確な分類は、ファイルメタデータの改ざんによる痕跡の難読化です。

質問: **138**
鑑識捜査官はサイバー犯罪捜査に配属され、犯罪現場にある電源の入ったコンピュータから重要な証拠を記録する必要がある。そのコンピュータには、進行中の捜査に関連する重要なファイルやプログラムが含まれていると疑われている。現場に到着した捜査官は、コンピュータのモニターにスクリーンセーバーが表示されており、アクティブなプログラムや開いているファイルが隠されていることに気づく。鑑識チームは、コンピュータ上のデータを改変したり改ざんしたりすることなく、証拠の完全性を維持するというプレッシャーにさらされている。
捜査官は、証拠を適切に記録するために、画面上で実行されているプログラムの鮮明な画像をキャプチャする必要があります。しかし、コンピュータ上の情報を改ざんする可能性のある事態を避けるため、どのように進めるべきか迷っています。捜査官は、画面上で実行中のプログラムをキャプチャし、効果的に証拠を記録するために、どのような手順を踏むべきでしょうか？
A. マシンを再起動して、再起動後に実行中のプログラムをシステムに表示させます。
B. マウスを少しゆっくりと動かしてスクリーンセーバーから画面を起動し、アクティブなプログラムを撮影して記録します。
C. コンピュータの主電源コードを抜いてシステムをリセットし、揮発性データをすべて消去します。

D. 証拠を記録する間、リモートアクセスを防ぐためにネットワークケーブルを外してください。

正解: **B** (コメントを発表する)

調査員の当面の目標は、電源が入っているシステムに現在表示されている内容やアクティブな内容を、できる限りシステムへの影響を最小限に抑えながら記録することであるため、選択肢Bが最適な回答です。CHFI v11では、デジタル証拠の取り扱い、証拠の保全、揮発性情報の収集、稼働中のシステム上で行われた操作の結果の理解に関するベストプラクティスが強調されています。

マウスを軽く動かして画面を起動させる方法は、提示された選択肢の中で最も邪魔にならない方法で、アクティブな画面を表示させ、適切な写真撮影による記録を可能にします。マシンを再起動したり、電源ケーブルを抜いたりすると、揮発性の証拠が失われ、システムの状態が大きく変化します。ネットワークケーブルを抜くことは、他の運用状況では検討される場合もありますが、スクリーンセーバーによって隠されたアクティブな画面上の証拠を記録するという差し迫った問題を解決するものではありません。

CHFI（犯罪現場証拠管理の観点からすると、現場での記録は、発見された証拠を可能な限りそのまま保存しつつ、変更を最小限に抑えるべきです。したがって、適切な対応は、画面を静かに起動させ、可燃性の証拠を損なうような破壊的な行為を行わずに、目に見えるプログラムを撮影・記録することです。

質問: **139**

コンピューターフォレンジック調査官が、従業員が24時間365日勤務している大手金融機関のファイアウォールログを調査している。

捜査官は、以下のスクリーンショットから何を推測できるでしょうか？

A. ファイアウォールでバッファオーバーフローが発生しました。

B. スマーフによる攻撃が試みられました

C. サービス拒否攻撃が試みられました

D. ネットワーク侵入が発生しました
正解: **(**正解を表示します**)**

質問: **140**
デジタル鑑識捜査官が、サイバー犯罪事件の容疑者から押収された携帯端末を調べている。
このデバイスは、特権昇格とシステムリソースへの無制限アクセスを可能にするカスタムオペレーティングシステム構成を実行しているようです。
この構成を実現するために最も可能性の高い方法はどれですか？
A. Android端末にカスタムROMをインストールする
B. iOSデバイスのファームウェアの脆弱性を悪用する
C. Android端末のルート化
D. iOSデバイスのジェイルブレイク
正解: **C (**コメントを発表する**)**
CHFI v11モバイルおよびIoTフォレンジックドメインによると、Androidデバイスのルート化は、管理者権限（スーパーユーザー権限）を取得し、システムリソースへの無制限アクセスを実現するための最も一般的で直接的な方法です。ルート化により、ユーザーはAndroidに組み込まれたセキュリティ制限を回避し、保護されたディレクトリ、システムバイナリ、カーネルパラメータ、ハードウェアインターフェースへのアクセスなど、オペレーティングシステムを完全に制御できるようになります。
CHFI v11によると、Androidデバイスがルート化されると、ユーザーはシステムファイルを変更したり、許可されていないアプリケーションをインストールしたり、セキュリティ制御を無効にしたり、ログを操作したり、悪意のある活動を隠蔽したりすることが可能になるため、ルート化はサイバー犯罪やフォレンジック対策において頻繁に用いられる手法となっています。フォレンジックの観点から見ると、ルート化は証拠の完全性に大きな影響を与え、サブバイナリの存在、変更されたブートイメージ、ルート管理アプリケーションなどの痕跡によって特定されることがよくあります。
カスタムROMをインストールするとオペレーティングシステムが変更されますが、デバイスがルート化されていない限り、システムへの無制限アクセスが保証されるわけではありません。脱獄はiOSデバイスに特有のものであり、Androidには適用されません。iOSファームウェアの脆弱性を悪用することで脱獄できる可能性はありますが、このシナリオはiOS環境を示唆するものではありません。
CHFI v11では、モバイル調査において、デバイスがルート化されているかどうかを特定することが非常に重要であると強調しています。これは、データ取得方法、証拠の信頼性、およびフォレンジック対策リスク評価に影響を与えるためです。
したがって、このシナリオで特権昇格と無制限のシステムアクセスを実現するために最も可能性の高い方法は、Android デバイスのルート化であり、オプション C が正解となります。

質問: **141**

ミシガン州デトロイトにある自動車部品サプライヤーで発生したサプライチェーン攻撃の調査において、フォレンジックチームは、エンドポイントのウイルス対策システムから発せられた不審なファイルダウンロードを示すアラートと、ネットワークIDSセンサーから報告された異常な送信DNSクエリを検証した。これらのアラートは単独では限られた情報しか提供しないため、チームはこれらの情報源を統合し、関連性を特定して、より広範な侵害シーケンスを再構築した。
この統合は、どのような事象相関分析手法を示しているのでしょうか？
A. 経路相関
B. ドメイン間イベント相関
C. 多変量相関
D. トポロジーに基づくイベント相関
正解: **(**正解を表示します**)**
回答Bが最も適切です。調査担当者は、異なるセキュリティドメイン（この場合はエンドポイント保護データとネットワーク侵入検知テレメトリ）からの証拠を関連付けているからです。クロスドメインイベント相関は、アナリストが個別のドメインまたは制御レイヤーからのイベントを組み合わせて、各アラートストリームを単独で確認しただけでは明らかにならない、より広範なインシデントパターンを明らかにする場合に使用されます。CHFI v11ブループリントには、イベント相関アプローチ、イベント相関の前提条件、およびインシデントタイムラインの再構築が具体的に含まれています。まさにここで起こっているのはこれです。アンチウイルスアラートはホスト上の疑わしいアクティビティを示し、IDSアラートはネットワーク上の関連するアウトバウンドDNS動作を明らかにします。これらのデータソースを組み合わせることで、マルウェアのステージング、コマンドアンドコントロールの試み、またはデータ漏洩経路を明らかにすることができます。ルート相関とトポロジベースの相関は、質問がインフラストラクチャトポロジを通るパスを強調していないため、あまり適切ではありません。多変量相関は通常、変数間の統計的関係をより広く指し、個別の調査ドメインからのアラートの明示的な結合を指すものではありません。したがって、CHFIに準拠した最も強力な解釈は、クロスドメインイベント相関です。

質問: **142**
アプリケーションまたはマルウェアの動的リンクライブラリを調査するのに適したツールを選択してください。
A. システムアナライザー
B. リソース抽出
C. PEiD
D. DependencyWalker
正解: **(**正解を表示します**)**

質問: **143**

自己監視、分析、報告技術（SMART）は、システムアクティビティを監視および報告するためにハードドライブに組み込まれています。SMARTによって生成されるレポートには、次のうちどれが含まれますか？
A. 電源オフ時間
B. ドライブが到達した高温のログ
C. OSに関連付けられたすべての状態（実行中および停止中）
D. 実行中のプロセス一覧
正解: **(**正解を表示します**)**

質問: **144**
次のうち、実験室用画像システムの技術仕様に含まれていないものはどれですか？
A. 非常に低い画像キャプチャレート
B. 高性能ワークステーションPC
C. 否認防止技術
D. リモートプレビューおよびイメージングポッド
正解: **A (**コメントを発表する**)**

質問: **145**
鑑識捜査官のマディソンは、メール詐欺事件の捜査を担当することになった。容疑者は、不正に入手したメールアカウントを使って複数の被害者にフィッシングメールを送信した疑いがある。捜査の一環として、マディソンはまず、容疑者のコンピュータと、詐欺メールの送信に使用されたメールサーバーの現地調査を行う許可を得なければならない。
マディソンが法医学的検査を進める前に最初にとるべき手順は何ですか？
A. コンピュータとメールアカウントの押収
B. メールヘッダーの取得
C. 削除されたメールメッセージの復元
D. メールヘッダーの分析
正解: **(**正解を表示します**)**
この質問は、CHFI v11の「規制、方針、倫理」および「デジタル証拠の捜索と押収」の目的に合致しています。フォレンジック調査、特にコンピュータや電子メールサーバーを含むオンサイト調査を合法的に実施するには、調査員は適切な法的許可を取得する必要があります。
実際には、この権限は、捜索令状、裁判所命令、またはシステム所有者からの明示的な同意のいずれかによって、システムおよびアカウントを合法的に押収することによって執行されます。
CHFI v11では、デジタルフォレンジック調査は証拠の許容性を確保し、プライバシーや適正手続きの侵害を回避するために、法的手続きを厳格に遵守しなければならないと強調しています。コンピュータシステムと電子メールアカウントを押収することで、証拠に対する法的管理が確立され、適切な保管記録の作成が可能になり、データの改ざんや破壊を防ぐことができます。押収と承認が得られた後でなければ、調査員は電子メールヘッダーの

取得、削除されたメッセージの復元、電子メールコンテンツの分析といった技術的な作業を安全に進めることができません。
その他の選択肢は、法的アクセスが許可された後に行われるフォレンジック分析の手順を説明しています。許可なくこれらの手順を実行すると、証拠が無効になり、調査担当者が法的責任を負う可能性があります。したがって、CHFI v11のベストプラクティスおよび法的要件に準拠し、フォレンジック調査を進める前に、コンピュータと電子メールアカウントを押収することが正しい最初の手順です。

質問: **146**
IoTフォレンジック調査官として、あなたは侵害されたスマートテレビやその他のIoTデバイスが関与するサイバー犯罪の調査を担当しています。調査では、ドローン、ウェアラブルデバイス、SDカードなど、さまざまなIoTデバイスからデータを抽出して重要な証拠を収集する必要があります。Android、iOS、Tizen OSを搭載したモバイルデバイスやチップオフメモリソースなど、これらのデバイスから物理的および論理的なデータ抽出を実行できるツールが必要です。この調査に最も適したツールは次のうちどれでしょうか？
A. ダブルスペース
B. MD-NEXT
C. エポックコンバーター
D. Systemctl
正解: **B** (コメントを発表する)
この質問は、CHFI v11の「モバイルおよびIoTフォレンジック」および「IoTデバイスフォレンジック用ツール」の目標に直接対応しています。IoT調査では、オペレーティングシステム、ストレージメカニズム、取得に関する課題が異なる異種デバイスが関わることがよくあります。CHFI v11では、包括的な証拠収集を確実にするために、チップオフやSDカード分析などの高度な技術を含む、論理的および物理的な抽出の両方をサポートする専門的なフォレンジックツールの必要性を強調しています。
MD-NEXTは、モバイルおよびIoT調査向けに設計された専用のデジタルフォレンジックツールです。Android、iOS、Tizen OS、ウェアラブルデバイス、ドローン、スマートテレビ、リムーバブルメディアなど、幅広いプラットフォームにおけるフォレンジックデータの取得と分析をサポートします。特に、MD-NEXTは論理抽出、物理イメージング、ファイルシステム解析、チップオフメモリ解析といった機能を備えており、破損、ロック、または非標準のIoTデバイスを扱う際に不可欠な機能を提供します。
他の選択肢はこのシナリオには適していません。DoubleSpaceはディスク圧縮ユーティリティ、EpochConverterはタイムスタンプ変換に使用され、SystemctlはLinuxのサービス管理コマンドです。
いずれもフォレンジックデータ取得機能を提供していません。したがって、MD-NEXTは、包括的なIoTおよびモバイルデバイスのフォレンジック調査に最も適しており、CHFI v11に準拠したツールです。

質問: **147**
外部のIT監査を受けた後、ジョージは自分のネットワークがDDoS攻撃に対して脆弱であることに気づいた。
彼はDDoS攻撃を防ぐためにどのような対策を講じることができるだろうか？
A. BGPを無効にする
B. ダイレクトブロードキャストを有効にする
C. ダイレクトブロードキャストを無効にする
D. BGPを有効にする
正解: **(**正解を表示します**)**

質問: **148**
企業ワークステーションにおけるマルウェア侵入調査において、フォレンジックアナリストはMagnet AXIOMを使用して、疑わしい実行ファイルがどのように導入され、時間経過とともに実行されたかを再構築します。この調査では、元のバイナリがディスク上に存在しない場合でも、実行されたプログラムに関するメタデータ（ファイルパスや実行コンテキストなど）を記録するアーティファクトが必要です。このアーティファクトは、他のシステム証拠と併せて実行タイムライン分析をサポートするために使用されます。調査担当者は、この目的のためにどのアーティファクトを優先すべきでしょうか？
A. UserAssistエントリ
B. ShimCache AppCompatCache
C. アムキャッシュ
D. ファイルのプリフェッチ
正解: **(**正解を表示します**)**
正解はDです。プリフェッチファイルは、プログラム実行履歴の再構築や実行タイムラインの構築において、Windowsの最も強力なアーティファクトの一つだからです。Magnetは、プリフェッチファイルが貴重なのは、アプリケーションが特定の場所から実行される際にWindowsがプリフェッチファイルを作成し、そのアプリケーション履歴に関する有用なメタデータを保持するためだと指摘しています。プリフェッチファイルは、元の実行ファイルがなくなっても利用可能な状態を維持できるため、バイナリが使用後に削除されるマルウェアの場合に特に役立ちます。CHFI v11では、Windowsアーティファクト分析に実行済みプログラムの証拠とタイムラインの再構築が含まれるため、受験者は実行分析を最も直接的にサポートするアーティファクトを特定することが求められます。UserAssistは有用ですが、特定のユーザー主導のGUIアクティビティに限定されます。ShimCacheとAmcacheは重要なアーティファクトですが、それ自体が実行の決定的な証拠となるよりも、存在または互換性追跡の証拠として扱う方が適切な場合が多いです。この質問は、実行済みプログラム、ファイルパス、およびAXIOMのタイムラインサポートを重視しているため、プリフェッチファイルが最も正確で説得力のある回答となります。プリフェッチファイルは、マルウェアの起動と永続化のストーリーを強化するために、他のアーティファクトと関連付けられることがよくあります。

質問: **149**
以下のツールのうち、調査員がウェブサーバーのログを分析するのに役立つのはどれですか？
A. ディープログアナライザー
B. ディープログモニター
C. LanWhois
D. XRY LOGICAL
正解: **A** (コメントを発表する)

質問: **150**
あなたはボストンの法律事務所に雇われたITセキュリティ監査員として、同社の顧客に関する機密情報にアクセスできるかどうかをテストする任務を負っています。あなたは彼らのゴミ箱を漁りましたが、ほとんど情報は見つかりませんでした。ネットワーク上で警報を鳴らしたくないため、Webサーバーに対してパッシブフットプリンティングを実行する予定です。
どのツールを使うべきですか？
A. Nmap
B. ネットクラフト
C. ピングスイープ
D. あなた
正解: **B** (コメントを発表する)

質問: **151**
NTLM認証を使用するActive Directoryネットワークにおいて、ドメインコントローラー上のどこにパスワードが保存されますか？
A. シャドウファイル
B. AMS
C. 私は
D. Password.conf
正解: (正解を表示します)

質問: **152**
NTFSディスクのマスターファイルテーブル（MFT）において、コロン（:）とその後に続くファイル名で表されるファイルの種類は何ですか？
A. 暗号化されたファイル
B. 予約ファイル
C. 圧縮ファイル
D. データストリームファイル
正解: **(**正解を表示します**)**

質問: **153**
無線攻撃を調査する際に、なぜデバイスのゲートウェイを特定する必要があるのでしょうか？
A. ゲートウェイは、攻撃者が攻撃を開始するために使用するプロキシサーバーのIPアドレスになります。
B. ゲートウェイは攻撃者のコンピュータのIPアドレスになります
C. ゲートウェイは、アクセスポイントを管理するために使用されるIPアドレスになります。
D. ゲートウェイは、RADIUSサーバーを管理するために使用されるIPアドレスです。
正解: **C (**コメントを発表する**)**

質問: **154**
調査員がデータベースからプライマリデータファイルとログを収集する過程で、sqlcmd -S WIN-CQQMK62867E -e -s"," -E というコマンドを入力しました。「WIN-CQQMK62867E」は何を表していますか？
A. データベースのネットワーク認証情報
B. データベース名
C. システムのオペレーティングシステム
D. SQL Server の名前
正解: **D (**コメントを発表する**)**

質問: **155**
ネットワークの脆弱性をテストするために、既知のエクスプロイトをネットワークに対して実行しています。ウイルス対策ソフトウェアの強度をテストするために、本番ネットワークを模倣したテストネットワークを構築しています。
あなたのソフトウェアは、単純なマクロウイルスや暗号化ウイルスを正常にブロックすることに成功しました。そこで、コードが完全に書き換えられ、子プロセスごとに署名が変わるものの、機能は同じままのウイルスコードを使って、ソフトウェアの性能を本格的にテストすることにしました。あなたがテストしているこのウイルスは、どのような種類のウイルスでしょうか？
A. 乏形性

B. 変形
C. 変成岩
D. 多形性
正解: **(**正解を表示します**)**

質問: **156**
あなたはMyISAMストレージエンジンに関連するログファイルを調査するタスクを割り当てられました。調査中に、MyISAMログファイルに対してリカバリ操作を実行するように求められました。以下のMySQLユーティリティのうち、どれを使用するとリカバリ操作を実行できますか？
A. myisamaccess
B. mysqldump
C. myisamchk
D. myisamlog
正解: **(**正解を表示します**)**

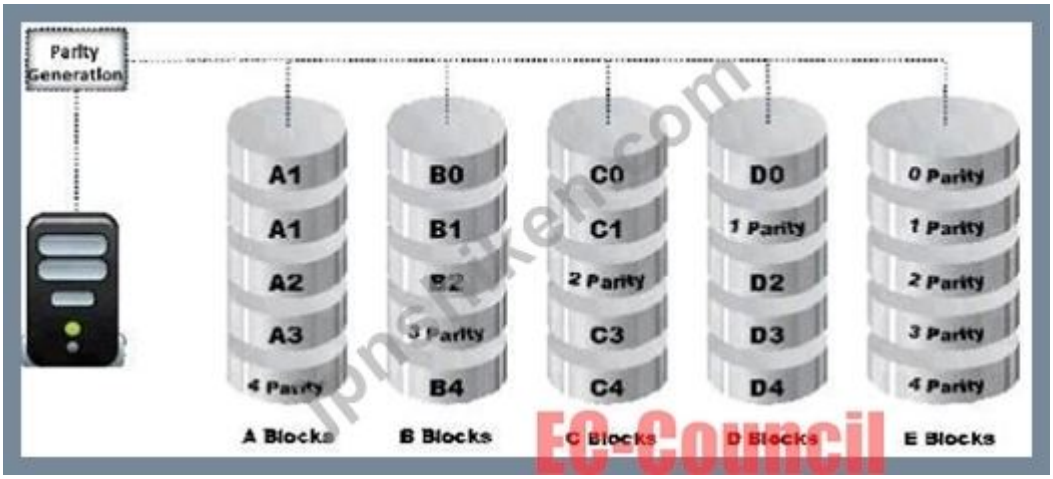
質問: **157**
ある多国籍企業が最近、深刻なサイバー攻撃の被害に遭いました。あなたはインシデント対応チームの一員として、攻撃者の活動を追跡するためにApacheウェブサーバーのログを分析しています。
ApacheコアのHTTP.REQUESTコンポーネントに変更が加えられていることに気づき、リクエスト処理に変更があったことが示唆されます。どのような変更が加えられたかを判断するために、Apacheウェブサーバーアーキテクチャの以下の要素のうち、どれを重点的に調査すべきでしょうか？
A. http_configモジュール: 設定ファイルとモジュール管理の変更をチェックします
B. http_protocolモジュール: クライアントとサーバー間のデータ交換の詳細を識別する
C. http_mainモジュール: サーバーの起動とタイムアウトを識別する
D. Apacheモジュール: 改ざんされた可能性のある拡張機能を明らかにする
正解: **D (**コメントを発表する**)**

質問: **158**
16進数コードにおけるオフセットは次のとおりです。
A. コロンの後の最後のバイト
B. コードの先頭にある0x
C. コードの末尾にある0x
D. コロンの後の最初のバイト
正解: **B (**コメントを発表する**)**

質問: **159**

攻撃者はリモートのWindowsシステムへのアクセスに成功し、そこに永続的なバックドアをインストールしようと計画している。その前に、将来的に検出されないように、マシンの最終アクセス時刻のタイムスタンプを無効にして痕跡を消したいと考えている。攻撃者はこれを実現するためにどのような行動をとるだろうか？
A. コマンド fsutil behavior set disablelastaccess 0 を実行します
B. レジストリ値を設定します HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate を 1 に変更
C. コマンド fsutil behavior set enablelastaccess 0 を実行します
D. レジストリ値を設定します HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate を 0 に変更
正解: **B** (コメントを発表する)

質問: **160**
データはバイト単位で複数のドライブにストライピングされ、パリティ情報はすべてのメンバードライブに分散されます。



これはどのRAIDレベルを表していますか？
A. RAIDレベル1
B. レイドレベル3
C. RAIDレベル5
D. RAIDレベル0
正解: (正解を表示します)

質問: **161**
次のコマンドは、Windowsのどの機能を利用しようとしているのでしょうか？

A. AFS
B. 広告
C. Slackファイル
D. 空白
正解: **B** (コメントを発表する)

質問: **162**
ノースカロライナ州ローリーにあるニュースポータルで営業時間外に発生したインシデントにおいて、アナリストは短時間のうちに同じIPアドレスからログインページへのアクセスが多数発生していることを確認した。数分後、以前のパターンとは異なる単一のエントリが検出された。ブルートフォース攻撃の継続と、認証後の管理エリアへのアクセスを区別するために、ログ内のどの要素が後者を最も強く示唆しているだろうか？
A. 非常に短い時間枠内でのログイン試行」
B. HTTP 302ステータスはURLリダイレクトを示します」
C. 同じIPアドレスから」
D. URLが/wordpress/wp-admin/に変更されました」
正解: (正解を表示します)
正解はDです。認証後のナビゲーションの最も明確な兆候は、要求されたリソースがログインエンドポイントからWordPress管理エリアに変更されたことです。同じIPアドレスからのログイン試行の繰り返しはブルートフォース攻撃を示唆しますが、侵入の成功を証明するものではありません。302リダイレクトは複数の状況で発生する可能性があり、それ自体では決定的な証拠にはなりません。攻撃者が認証情報の推測を超えて認証済みエリアに侵入したことを示す最も強力な指標は、管理インターフェースパスである/wordpress/wp-admin/への後続のリクエストです。CHFI v11には、ブルートフォース攻撃の調査とWebサーバーログによるWebアプリケーションのフォレンジック分析が含まれているため、受験者はログイン失敗時のプレッシャーとアクセス取得後に発生するナビゲーションを区別することが求められます。フォレンジック解釈では、要求されたURLは、タイミングや送信元IPアドレスだけよりも強力なコンテキストを提供することがよくあります。質問は、ブルートフォース攻撃の継続ではなく、認証後のアクティビティを最も強く示すものは何かを尋ねているため、管理URLへの変更が最良の答えです。

質問: **163**

コンピュータハッキングのフォレンジック調査員が、物理的にアクセスできないLinuxベースの容疑マシンから揮発性データを取得しようとしています。彼らはシステムのRAMのダンプをリモートで取得する必要があります。フォレンジック的に安全な抽出を行うには、以下のどのコマンドとツールを使用すべきでしょうか？
A. 容疑者のマシンで: insmod lime-.ko "path=tcp: format=lime": 鑑識ワークステーションで:
nc : > filename.mem
B. 鑑識ワークステーションで insmod lime-.ko "path= format=lime"; 容疑者マシンで nc : > filename.mem
C. 鑑識ワークステーションで: nc -l > filename.dd; 容疑者マシンで: dd if=/dev/fmem bs=l024 | nc
D. 容疑対象マシン上で: dd if=/dev/fmem of= bs=lMB; フォレンジックワークステーション上で: nc -l > filename.dd
正解**: (**正解を表示します**)**

質問**: 164**
デジタルフォレンジック調査官のトムは、ある企業の内部脅威の可能性を調査するよう命じられた。現場に到着すると、ワークステーションが侵害されていることが判明した。容疑者は元従業員で、逮捕される前に悪意のあるUSBデバイスを使用して機密ファイルにアクセスしたとされている。トムはすぐに調査を開始し、ワークステーションをネットワークから隔離した後、制御された環境でシステムを起動した。彼の最初の任務は、アクティブなプロセス、ネットワーク接続、クリップボードの内容など、システムのメモリに保存されているデータを収集することである。トムは、この種のデータが攻撃時の容疑者の行動に関する重要な情報を提供できることを知っている。なぜトムはこの事件で他の種類の証拠よりもこのデータを優先しているのだろうか？
A. 変動性の高いデータは、最も安定した証拠を提供する。
B. 揮発性データは時間依存性があり、システムの電源が切れると失われる可能性があります。
C. 不揮発性データがこのケースに最も関連しています。
D. 不揮発性データは揮発性データよりも復旧しやすい。
正解**: (**正解を表示します**)**
正解はオプションBです。CHFI v11では、ライブ取得、揮発性の順序、揮発性情報と不揮発性情報の収集、そして揮発性証拠が消滅する前に取得する必要性を明確に強調しています。アクティブなプロセス、ネットワーク接続、クリップボードの内容、セッションデータなどのメモリ常駐アーティファクトは時間的制約が非常に大きく、システムの電源が切れたり、何らかの変更が加えられたりした瞬間に失われる可能性があります。
そのため、トムはメモリの収集を最優先事項としている。フォレンジック手法において、揮発性データは最も安定しているデータではなく、最も失われやすいデータであることが多い。不揮発性データはディスク上に残るため、通常は後から取得できるが、RAM上の証拠はすぐに消えてしまう可能性がある。これは、内部犯行やライブシステム攻撃のケースにお

いて特に重要であり、ユーザーの行動に関する最も決定的な痕跡は、押収時点ではメモリ上にしか存在しない可能性がある。
選択肢A、C、Dはいずれも、テストの対象となる重要な原則を誤解しています。正しい理由は、揮発性データは迅速に収集されないと失われる可能性があるため、CHFIの収集規則に基づく緊急対応において最優先事項となるからです。

質問: **165**
法医学調査官のスティーブは、所属組織で発生した電子メール関連のインシデントの調査を依頼されました。組織では、電子メール通信にMicrosoft Exchange Serverが導入されています。スティーブは、メッセージヘッダー、メッセージ本文、および標準添付ファイルを分析するために、次のうちどのファイルを確認するでしょうか？
A. PRIV.STM
B. PRIV.EDB
C. PUB.EDB
D. PUB.STM
正解: **(**正解を表示します**)**

質問: **166**
コロラド州デンバーで発生した財務記録改ざん事件において、容疑者が高度なフォレンジック対策を用いてファイルの整合性を損ない、重要なデータセットの名前を変更し、ドライブを暗号化したため、鑑識官はデジタル証拠の分析に苦慮した。このような捜査において、フォレンジック対策が引き起こす障害の種類を最もよく表しているのは、次のうちどれか。
A. 偽造証拠を作成すると、捜査官を誤った結論に導く可能性があります。
B. パッカープログラムで難読化されたファイルは、マルウェア対策ツールによる検出を回避できます。
C. 意図的なデータ改ざんは、デジタル証拠の完全性と信頼性を低下させる。
D. タイムスタンプを変更することでサーバーログが削除され、デジタルフットプリントが消去されます
正解: **C (**コメントを発表する**)**
正解はCです。このシナリオは、証拠自体の信頼性を直接損なうフォレンジック対策に焦点を当てています。ファイルの整合性が損なわれ、重要なデータの名前が変更され、ドライブが暗号化されている場合、フォレンジックにおける最大の障害は、デジタル証拠の信頼性と完全性が弱まることです。CHFI v11では、フォレンジック対策技術と、それが捜査官にもたらす課題、具体的には、データの破損、消去、暗号化、メタデータの操作、および証拠の正確な解釈を妨げるその他の行為について具体的に説明しています。オプションAは、考えられるフォレンジック対策の1つを説明していますが、この質問は、捏造されたリダイレクトではなく、既に手元にある証拠の完全性の低下を強調しています。オプションBはより限定的で、説明されているより広範な証拠の問題よりも、マルウェアの回避についてより言及

しています。オプションDは誇張されており、技術的に不正確です。タイムスタンプの変更自体は、サーバーのログ記録を完全に削除するものではないからです。
CHFI方式の推論では、反フォレンジックによって調査官がデータの完全性、真正性、信頼性に疑念を抱く場合、最も直接的な課題は証拠の完全性と信頼性の低下である。ここで最もよく示されているのが、まさにその障害である。

質問: **167**
鑑識捜査官のイーサンは、容疑者のコンピュータを分析中に、サイバー犯罪に関連している可能性のある不審なファイルを発見した。ファイルのメタデータを調べたところ、ファイルが複数回変更されており、最後にアクセスされたのは犯罪発生直前であることが判明した。ファイルが改ざんまたは操作されたかどうかを判断するために、イーサンにとって最も有用な鑑識手法は次のうちどれか？
A. ファイルのファイルシステムログを確認する
B. 隠れた属性や代替データストリームを探す
C. ファイルのアクセス制御リスト（ACL）を確認する
D. ファイルのハッシュ値を調べる
正解: **(**正解を表示します**)**
CHFI v11カリキュラムでは、デジタル証拠の完全性を検証することが、フォレンジック調査官の重要な責務とされています。ファイルが改ざんされたかどうかを判断する最も確実な方法は、その暗号化ハッシュ値を調べることです。ハッシュ値（MD5やSHA-256など）は、ファイルの内容から生成される固定長のデジタル指紋です。意図的か偶発的かを問わず、ファイルへのわずかな変更でもハッシュ値は全く異なるものになるため、ハッシュ値の比較は改ざんを検出する確実な方法となります。
ファイルシステムログ（オプションA）は、アクセスや変更イベントを表示することでタイムラインの再構築に役立ちますが、ログは削除、変更、または不完全な場合があり、ファイルコンテンツの完全性を直接検証するものではありません。隠し属性または代替データストリーム（オプションB）は、フォレンジック対策技術の可能性を示す指標となりますが、それらが存在するからといって、主要なファイルデータが改ざんされたとは限りません。アクセス制御リスト（オプションC）は、アクセス許可の設定と所有権のみを記述し、ファイル自体が変更されたかどうかは示しません。
CHFI v11のデジタル証拠、データ取得、証拠検証の目的によると

捜査官は、証拠の保管管理を維持し、証拠の完全性を確保し、法的証拠能力を裏付けるために、取得および分析中にハッシュ値を計算および検証する必要があります。このため、ハッシュ値の検証は、このシナリオにおいて最も適切で法医学的に妥当な選択肢となります。