

令和5年度春期 応用情報技術者試験 午後問1「マルウェア対策」徹底復習レポート

1. インシデントの概要とサイバーキルチェーンによる現状分析

サイバー攻撃が高度化・隠密化する現代において、インシデント発生時の現状分析は単なる原因究明に留まりません。それは被害の拡大を阻止し、組織のレジリエンスを再構築するための「戦略的トリアージ」としての重要性を持ちます。旅行代理店R社で発生したランサムウェア感染事案を例に、初動対応の技術的妥当性と攻撃フェーズの特定について専門的見地から分析します。

インシデントの推移と初期対応の評価

本事案は、従業員SさんのPC（PC-S）において身代金要求メッセージが確認されたことで発覚しました。Sさんが窓口を把握しておらず数時間の遅延が生じた点は、組織的な「セキュリティ文化」の未醸成を露呈していますが、その後の情報システム部Tさんによる介入は迅速でした。初期対応として最も優先されるべきアクション：ネットワークからの切り離し設問1(1)の正解である「ネットワークからの切り離し（選択肢：ウ）」は、インシデントレスポンスにおける「封じ込め（Containment）」の最優先事項です。

- **技術的視点（Blast Radius Reduction）**： ランサムウェアは感染端末を起点にLAN内をスキャンし、共有サーバや他端末へ感染を拡大させる特性があります。物理的・論理的にネットワークを遮断することで、被害の「爆発半径（Blast Radius）」を最小限に抑え込みます。
- **管理的視点（Evidence Preservation）**： 通信を遮断することで、C&Cサーバによる証拠消去命令や追加のペイロード・ダウンロードを防ぎ、フォレンジック調査に必要な証拠保全の確実性を高めます。

サイバーキルチェーンを用いた攻撃段階の特定

Z社の調査結果に基づき、表1のサイバーキルチェーンと照合すると、攻撃は**項番5「インストール」**まで完了したと判断されます。

- **「インストール」完了の根拠**： PC-S内のファイルが暗号化されているという事実は、マルウェアがシステム内で実行権限を獲得し、その目的である破壊的コードが展開・定着したことを意味します。
- **次段階（C&C・内部探索）の阻止状況**： 調査では「インターネットに向けた不審な通信」や「LAN上のIPスキャン痕跡」が否定されています。これは、攻撃者が遠隔操作を確立する**「Internal Reconnaissance（内部探索）」**や、外部との接続を維持する項番6「C&C」フェーズへの進展を、防御側が瀬戸際で食い止めたことを示しています。この現状分析からは、境界防御を突破された後の「端末内での挙動」に対する検知能力の限界が明確になっています。この検知の空白地帯を埋めるためには、次章で述べるEDR等の高度なエンドポイント監視が不可欠となります。

2. エンドポイントにおける高度な監視・検知体制の構築

従来の境界防御（Perimeter Defense）は、正規の権限を悪用する標的型攻撃の前では無力化されつつあります。侵入を前提とした「Defense-in-Depth（多層防御）」の観点から、エンドポイントでの挙動監視を強化することは、攻撃の「可視化」という戦略的価値を組織にもたらしめます。

EDR（Endpoint Detection and Response）の役割と優位性

R社の課題解決において、下線②の正解である「EDR」の導入は決定的な意味を持ちます。Source Contextに挙げられた他の技術要素（APT, UTM, WAF）と比較すると、その差別化要因は「監視対象のレイヤ」にあります。

- **UTM/WAFとの比較：** UTMやWAFがゲートウェイでの「通信パケット」を監視するのに対し、EDRはOSレベルでのプロセスの挙動、レジストリ変更、ファイル操作を監視します。
- **戦略的優位性：** 今回のような添付ファイル実行による発症は、正規のプロセスを隠れ蓑にするため、境界での検知が困難です。EDRは「不審な挙動」そのものを直接捕捉するため、未知のマルウェアであっても実行の初期段階で検知・隔離を可能にします。

インシデント予兆把握のメカニズム

表2の課題1（実行検知の欠如）に対し、表3の改善策1（挙動監視）を適用することで、再発防止の精度は飛躍的に向上します。EDRによる継続的な監視体制が構築されていれば、ファイルが大量に書き換えられる予兆をミリ秒単位で検知し、自動的なプロセス遮断を実行できます。これにより、従業員の報告に頼ることなく、被害を最小限に封じ込めることが可能となります。技術的な検知体制は、それを運用する組織（CSIRT等）と連携して初めて実効性を持ちます。検知されたアラートを迅速な意思決定に繋げるための体制構築について、次章で詳述します。

3. 組織的なインシデント対応（CSIRT）と資産管理の高度化

技術対策を実効性あるものにするには、その運用基盤となる「組織体制」と「管理プロセス」の整備が不可欠です。これらは技術を機能させるための「OS」の役割を果たします。

CSIRT（Computer Security Incident Response Team）の構築

設問3(1)の正解である「CSIRT」の構築は、R社のような中規模組織において急務です。

- **中核的役割：** インシデント発生時の連絡窓口（PoC）を一本化し、トリアージ、被害範囲の特定、対外報告、および外部専門家との連携を統括します。従業員数150名程度のR社では、専任組織だけでなく、外部パートナーと連携した**「Hybrid CSIRT」や、他部門との兼務による「Virtual CSIRT」**モデルの採用が現実的かつ戦略的な選択となります。

資産管理と脆弱性情報の戦略的紐付け

表4のb～dに該当する表3の項番はそれぞれ、**b=3、c=6、d=5** となります。この「資産目録の更新（項番3）」と「脆弱性情報の収集（項番6）」のセットは、「**Risk Assessment lifecycle（リスクアセスメントのライフサイクル）**」の根幹です。

- **相互依存関係：** 自社が保有するデバイス、OS、ソフトウェアのバージョンが不明確（資産管理の欠如）であれば、どれほど高度な脆弱性情報を収集しても、自社への影響を判断できません。「守るべき対象を認識していないものは、守ることができない」という原則に基づき、資産管理はすべてのセキュリティ対策の絶対的必要条件となります。

過去事例の調査による継続的改善

下線④に関連し、設問3(3)で選択すべき「使用された攻撃手法（ア）」や「被害を受けた機器の種類（ウ）」の調査は、防御の最適化に直結します。

- **改善プロセス：** 攻撃手法を特定することで、EDRの検知ルール最適化や不要なサービスの停止といった具体的対策を導き出せます。これは、過去の教訓を組織の知恵へと変換し、レジリエンスを継続的に向上させるプロセスそのものです。組織体制が整い、管理基盤が強固になっても、最終的な「個人の行動」がセキュリティの成否を分けることに変わりはありません。次章では、最後の防御層としてのヒューマンファクターに焦点を当てます。

4. ヒューマンファクターへの対応：社員教育と実戦的訓練

従業員は、組織における最大の脆弱性となり得る一方で、最初の兆候を察知する「最大の防御層（Human Firewall）」にもなり得ます。教育と訓練は、個人の意識を組織の防御力へと昇華させる戦略的投資です。

インシデント対応フローにおける初動の重要性

図1のフローにおいて、全従業員が担うべき役割は**「ア．検知/通報（受付）」**です。Sさんの事例での「数時間の放置」は、単なる知識不足ではなく、通報の重要性が浸透していない「組織文化」の課題です。研修を通じて「些細な違和感でも即座に通報することを賞賛する文化」を醸成することが、組織全体の初動を加速させます。

バックアップメディアの物理的安全管理

ランサムウェア対策として、設問4(2)の正解である**「PCから切り離して保管する」**というオフラインバックアップの徹底は、攻撃に対する究極の防御策です。

- **有効性の根拠：** 近年のランサムウェアは、ネットワーク経由で到達可能なすべてのドライブや、Windowsの「ボリュームシャドウコピー（VSS）」を優先的に暗号化・破壊します。物理的に隔離された「Offline Storage」こそが、自動化された攻撃からデータを守る唯一の絶対的手段です。
- **保管ルール：** 物理的な紛失・盗難リスクを考慮し、鍵のかかる引き出しやロッカーへの保管といった物理的安全管理手順を教育に含める必要があります。

実戦的訓練（シナリオベース）の設計

全従業員と経営層を巻き込んだ訓練は、組織の回復力を高めます。経営層が参加することで、事業継続の判断や情報公開のタイミングといった「ビジネス判断」のシミュレーションが可能になり、有事の際の混乱を最小限に抑制できます。教育と訓練が形骸化せず、組織のDNAとして根付くことで、初めて技術と組織の対策が有機的に機能し始めます。

5. 総括：R社の事例から学ぶサイバーレジリエンスの要諦

本インシデントは、どれほど強固な技術対策を導入しても、それを運用する組織体制と人の意識が伴わなければ、防御には「死角」が生じることを示しました。技術・組織・人の三位一体による対策こそが、現代のサイバー脅威に対抗するための唯一の道です。

課題と改善策の対応マトリクス

表2の課題（リスク）、対応する改善策（表3・4）、リスク低減の効果

1. マルウェア実行の検知不能, 改善策1（EDR導入）、挙動監視によるプロセスの即時遮断
2. 予兆把握の仕組みの欠如, 改善策2（ログ分析整備）、侵入の兆候を早期に捕捉し可視化
3. 対応手順・体制の不備, 改善策5（CSIRT/手順明文化）、インシデントレスポンスの迅速化と正確性向上
4. 社員の対応手順周知不足, 改善策7（実戦的訓練）、初動通報の定着による「空白の時間」の解消
5. 標的型攻撃への意識不足, 改善策8（継続的教育）、従業員の「検知センサ」としての能力向上

結論としての学習ポイント

応用情報技術者試験および実務において、本問から得られる最重要の学びは以下の3点に集約されます。

- **事後対応の迅速化（Containment）：** 検知からネットワーク切り離しまでの時間を最短化し、被害の爆発半径を抑制すること。
- **資産管理の基盤化：** 最新のIT資産目録を維持し、脆弱性情報と紐付けることが、リスクアセスメントの絶対的な出発点であること。
- **オフラインバックアップの原則：** ネットワークから物理的に隔離された保管のみが、高度なランサムウェアに対する最終的な復元性を担保すること。これらの学びを単なる知識としてではなく、各対策がどのように相互作用してリスクを低減させているかという「論理の繋がり」として理解してください。それが試験合格、さらには実務におけるセキュリティ・スペシャリストとしての資質に繋がります。