

令和4年度 秋期 応用情報技術者試験：マルウェア対策とEDR導入に関する復習レポート

1. はじめに：本事例の戦略的背景

IT製品の卸売業を営むP社にとって、300社の販売代理店との情報連携を支えるネットワークインフラは経営の生命線です。昨今、Emotetに代表される標的型攻撃は、取引先を装った巧妙な手口で組織内部へ侵入し、機密情報の窃取やさらなる感染拡大を引き起こします。従業員400名を抱え、インターネット上に代理店サーバ、内部に顧客サーバを運用するP社にとって、こうした脅威は単なるシステム障害ではなく、サプライチェーン全体を巻き込む経営リスクへと直結します。本レポートの目的は、既存の「境界防御」の限界を特定し、EDR導入による「侵入を前提としたレジリエンス」への質的転換について、試験対策上の重要ポイントを交えて論理的に整理することにあります。

2. 既存セキュリティインフラの評価と脆弱性の特定

多層防御においては、ネットワークの各境界に適切なセキュリティ機器を配置し、脅威のステージに応じた遮断を行う必要があります。しかし、静的な防御策には必ず「隙間」が存在します。

ネットワーク機器の最適配置（設問1関連）

図1のネットワーク構成に基づき、P社の主要なセキュリティ機器の配置と役割を以下の通り整理します。

符号	機器名	主な役割と配置理由
a	ファイアウォール (FW)	インターネット、DMZ、内部LANの境界に位置し、ポリシーに基づき業務に必要な通信のみを許可・ログ保存する。
b	メール中継サーバ	DMZに配置。SPF機能によるドメイン認証を行い、不審なメールを内部ネットワークに到達する手前で隔離する。
c	配布サーバ	内部LANに配置。OSのセキュリティパッチ等を一元管理し、検証済みのアップデートを各PCへ迅速に配布する。

メールの隔離において、社内メールサーバではなくDMZ上の**「メール中継サーバ」**を利用するのは、悪意あるコンテンツを社内ネットワークから物理的・論理的に切り離された領域で処理し、内部へのリスク流入を最小化するという多層防御の基本原則に基づいています。

外部脅威への耐性評価

P社の外部DNSサーバには、**DNSリフレクション攻撃**（設問1-2）の踏み台にされるリスクが存在します。これは、攻撃者が送信元IPを標的のものに偽装し、DNSサーバに問い合わせを行うことで、増幅された応答パケットを標的に送りつけるDDoS攻撃の一種です。特に「キャッシュサーバ機能」が有効な場合、外部からの再帰的な問い合わせを許可することになり、攻撃の増幅器（スプリングボード）として悪用される危険性が高まります。

3. マルウェアXの攻撃メカニズムと検知の困難性

攻撃者はOSの脆弱性だけでなく、人間の心理やマクロ機能を悪用します。マクロ付き文書ファイルは、難読化技術によってシグネチャ型のマルウェア対策ソフトを容易に回避するため、エンドポイントでの挙動監視が不可欠となります。

攻撃プロセスのフェーズ分析（設問2関連）

マルウェアXは、侵入後に以下の「内部探索」フェーズを経てラテラルムーブメント（横展開）を試みます。

- **偵察（ホスト探索）**：下線②（ICMPエコー要求）の目的は、ネットワーク上で**「稼働中のホストの IP アドレス」**を特定することです。
- **侵入準備（サービス探索）**：下線③（ポートスキャン）の目的は、特定したホストにおいて**「攻撃対象のサービスの稼働状態」**を確認し、悪用可能な脆弱性を探ることにあります。これらの行為は、単一の通信で見れば正規のネットワーク診断と区別が付きにくいですが、短時間の連続実行という「振る舞い」に着目することで、攻撃の予兆として捉えることが可能になります。

認証の限界と巧妙化するなりすまし

P社が導入しているSPF機能が、下線④（社外の感染PCからのメール）に対して無力である理由は、「送信者のドメインが詐称されたものでないから」（設問2-3）です。SPFはあくまで「送信元メールサーバのIPアドレスが、送信元ドメインのDNSに登録されているか」を検証する仕組みです。感染した取引先の正規PCから、その組織の正規メールサーバを経由して送られるメールは、ドメイン認証を正当にパスしてしまいます。これがサプライチェーン攻撃の恐ろしさであり、境界防御の限界を示す典型的な事例です。

4. EDR導入による高度なインシデントレスポンスの構築

「侵入を100%防ぐことはできない」という現実に関し、侵入後の活動をいかに早期に検知・抑制できるかが、企業のレジリエンス（回復力）を左右します。

EDRの機能的優位性（設問3関連）

EDRは、PC上のプロセスや通信をリアルタイムで監視し、以下のインパクトを組織にもたらしめます。

- **可視化と即時対応**：管理サーバが各エージェントからログを集約することで、攻撃の全体像を即座に把握できます。
- **緊急措置（隔離）**：マルウェアXが**「ICMPエコー要求パケットの連続した送信」（設問3-1）という不審な挙動を見せた際、EDRは即座に「マルウェアに感染したPCを隔離する」**（設問3-2）といった緊急措置を自動的または遠隔で実施できます。これにより、C&Cサーバとの通信や内部探索の拡大を物理的なLANケーブル抜去に近い速度で阻止します。

事後解析とフォレンジックの強化

インシデント発生時、被害範囲を早期に特定するためには、「EDRが保存するログの分析」（設問3-3）が極めて重要です。これらのログはPC端末内ではなく、改ざん耐性の高い

「管理サーバ」に保存されているため、たとえマルウェアが端末上の痕跡を消去したとしても、攻撃者の足跡を辿り、確実な再発防止策を講じることが可能になります。

5. 総括：試験対策における重要ポイント

本事例は、応用情報技術者試験の受験者に対し、単なる用語の暗記ではなく「技術の相互作用」と「運用の実効性」を問うています。

重要用語の再定義と関連

- **FW / メール中継サーバ**：境界で「入り口」を固めるが、正規ルートを通る脅威は防げない。
- **DNSリフレクション**：キャッシュサーバ機能の不適切な設定が招く二次被害。
- **SPF**：ドメインの正当性は保証するが、送信元PCのクリーンさは保証しない。
- **ICMP/TCPスキャン**：ラテラルムーブメントの前兆となる、攻撃者の偵察行為。
- **EDR**：「侵入後」の振る舞いを検知し、隔離によって被害を最小化する最後の砦。

実務への応用とガバナンス

本事例での教訓を、企業のセキュリティガバナンスに寄与する3つの視点で抽出します。

1. **パッチ適用のタイムラグ解消**：検証期間（本事例では1週間）における脆弱性の「窓」を意識し、その間の代替策を講じること。
2. **ログ検査の即時性確保**：週1回の目視確認という運用上の遅れを、EDR等のリアルタイム検知・自動分析によって補完すること。
3. **内部可視性の向上**：境界防御に依存せず、内部ネットワーク内の不審な通信（ICMPの連続送信等）を監視する体制を構築すること。

結論

高度IT人材に求められるのは、SPFのような特定の技術が「何を防げて、何を防げないのか」という境界を明確に定義し、それを組織全体の多層防御のデザインに落とし込む能力です。技術的な「点」の知識を、ビジネスを守るための「面」の戦略へと昇華させることが、試験合格、そして実務におけるアーキテクトとしての成功への鍵となります。