

応用情報技術者試験 復習レポート：境界型防御からゼロトラストへの移行とセキュリティ対策の高度化

1. 序論：Q社におけるビジネス変革とセキュリティ要件の変化

現代のビジネス環境において、ITインフラの在り方は劇的な変革を迫られています。学習塾を経営するQ社の事例は、その典型的な転換点を示しています。

戦略的背景とリモート環境構築の必要性

Q社では現在、生徒や保護者からの「ハイブリッド型授業（対面とリモートの併用）」の導入要望、および従業員からの「テレワーク勤務」の導入要望という、切実なビジネスニーズに直面しています。これらを実現するためには、従来の「校舎や本社の中にいれば安全」という前提を捨て、場所を問わず安全に業務を遂行できるリモート環境の構築が不可欠となりました。

「ゼロトラスト」という新たな基本概念

このような環境変化に対応するため、情報システム部のR課長が打ち出し、部下のS君と共に具体化したのが**「ゼロトラスト」**という基本概念です。これは「いかなる通信も信頼しない」という考え方に基づいています。従来の境界型防御が「ネットワークの内外」を分けることに注力していたのに対し、ゼロトラストでは接続元を問わず、すべての通信を検証・認証の対象とします。これは、守るべきデータがクラウド上に分散し、アクセス元が多様化した現代のIT環境において、極めて重要な戦略的パラダイムシフトとなります。

2. 現状分析：境界型防御の限界と顕在化する運用課題

Q社がこれまで採用してきた「境界型防御」は、ルータとファイアウォール（FW）によって内部ネットワークとインターネットの境界を区切る手法ですが、現代のサイバー攻撃や運用負荷に対して限界を迎えています。

境界型防御の評価と限界

従来の構成におけるFWの主目的は、パケットフィルタリングポリシーに基づき、**「ポリシーで許可していない通信による、内部ネットワークへの侵入」**を遮断することにあります。しかし、この手法では以下の攻撃を防ぎきれません。

- 許可された通信（Web閲覧やメール）の中に攻撃コードが含まれている場合。
- 標的型メール攻撃によって、内部の人間が自らマルウェアを実行してしまう場合。
このように「境界を一度突破される、あるいは境界の内側で問題が発生する」事態に対して、従来の仕組みは極めて脆弱です。

ビジネス継続性を阻害する運用負荷

また、インフラの維持管理面でも深刻な課題が顕在化しています。

1. **EOL (End Of Life) 対応：** 物理的なネットワーク機器やサーバの更新期限が迫り、多大なコストと工数が必要となっていました。

2. **脆弱性対応の遅延：** **「セキュリティパッチ提供の調査及び適用可否の判断」** に多大な時間を要しており、その間に脆弱性を突かれるリスクを抱えていました。これらの運用負荷は、単なるIT部門の工数問題に留まらず、セキュリティホールの放置に繋がり、ビジネス継続性への大きな脅威となっていました。

3. 戦略的転換：ゼロトラスト・アーキテクチャの採用とその核心

Q社は、物理的な機器の更新という「延命措置」ではなく、クラウド活用による抜本的な解決を図りました。

SaaS型クラウドサービス導入の劇的なメリット

S君の検討案に基づき、新環境ではクラウドサービスとして **SaaS型** を採用しました。これにより、従来Q社の負担となっていたOSやアプリケーションのソフトウェア更新、メンテナンス、およびセキュリティパッチの適用作業はすべてサービス提供者側で行われるようになります。結果として、Q社は「セキュリティパッチの提供調査や適用判断」という煩雑な業務から解放され、より戦略的な業務にリソースを集中させることが可能になりました。

セキュリティレベルの維持：Web閲覧の管理

インフラをクラウドへ移行しても、セキュリティレベルを低下させることは許されません。貸与PCからWebサイトを閲覧する際は、引き続きプロキシを経由する構成とし、そこで**「URLフィルタリング」**（および「業務上不要なサイトへの接続禁止」）を実施します。これにより、リモート環境下においても、従来と同等以上のアクセス制御を担保しています。

4. 技術的ソリューションの深掘りとリスク低減効果

ゼロトラスト環境を実現するため、Q社では「検知」「防御」「認証」の各コンポーネントを、相互に補完し合う一連のワークフローとして統合しています。

認証の要：多要素認証（MFA）の戦略的意義

IDとパスワードという「知識情報」のみに頼る認証は、不正ログインのリスクを孕んでいます。これに対しS君は、知識情報に「スマートフォンへのワンタイムパスワード送信」などの「所持情報」を組み合わせた**「多要素認証（MFA）」**（または2要素認証）を採用しました。ここで試験対策上の重要なポイントは、「要素（Factor）」と「段階（Step）」を混同しないことです。多要素認証とは、異なるカテゴリの要素を組み合わせることであり、同じパスワードを2回入力する「2段階認証」とは根本的に安全性の強度が異なります。MFAにより、万が一パスワードが漏洩しても、第2の要素がなければアクセスできない強固なゲートキーパーを構築しています。

エンドポイント防御と迅速な検知：EDRとSIEMの連携

- **EDRの機能：** 「ゼロデイ攻撃」や「ファイルレス攻撃」など、従来のパターンマッチングでは防げない脅威に対し、EDRがPCの挙動を監視します。異常を検知した際は、即座に**「貸与PCをネットワークから遮断し、不審なプロセスを終了する」** という初動アクションを実行し、被害の拡散を封じ込めます。

- **SIEMの役割：** これらEDRのログや各コンポーネントのログを統合的に収集・分析するのが **SIEM** です。SIEMの導入目的は、断片的な情報を集約し、**「セキュリティインシデントの発生を迅速に検知する」**ことにあります。

ゼロトラスト・ワークフローの相互作用

これら個別のツールは、以下のような「一連の防衛線（チェーン）」として機能します。

1. **MFA** が、SaaSにアクセスする「ユーザーの正当性」を厳格に保証する。
2. **EDR** が、そのアクセスに使用される「端末（エンドポイント）の安全性」を常時監視する。
3. **SIEM** が、認証からアクセス、端末の挙動に至る「経路全体の可視化」を行い、他をすり抜ける異常を捕捉する。さらに、物理的な端末紛失・盗難リスクに対しては、*「ストレージ全体の暗号化」と「リモートロック・ワイプ」*を組み合わせることで、データの機密性を物理レイヤーでも保護しています。

5. 総括：現代のIT環境に求められる多層的な防御戦略

Q社の事例は、単なるツール導入ではなく、ITインフラの変化に伴う「管理思想の根本的な転換」を示しています。今回の出題趣旨にもある通り、クラウドサービスの普及によって、**「保護すべきデータが外部ネットワークに置かれることが多くなった」**ことが、この転換の最大の要因です。もはや境界線を引くこと自体が物理的に不可能であり、従来のような「境界の内側は安全」という前提は成り立ちません。本事例で確認した通り、新たな態勢では以下の3つのレイヤーで高度化が図られました。

1. **エンドポイント：** EDRによる動的な振る舞い検知と、暗号化・ワイプによる物理対策。
2. **ネットワーク：** 境界に依存せず、SaaSとプロキシを活用した安全なサービス利用。
3. **ユーザー認証：** IDaaSと多要素認証による、徹底した「個人」の特定と信頼の検証。これからのシステム設計においては、境界型防御の限界を正しく理解し、今回Q社が実践したような「ゼロトラスト」に基づいた多層的な防御戦略を標準として採用すべきです。本レポートが、今後のシステム設計やセキュリティ態勢の検討、ならびに応用情報技術者試験における理解の深化に寄与することを願います。