

令和2年度秋期 応用情報技術者試験「午後問1：内部不正対策」徹底復習レポート

1. ケーススタディ：A社の組織背景と現状のセキュリティガバナンス

情報セキュリティ対策を立案する際、技術的なソリューションの導入はあくまで手段に過ぎません。真に実効性のある対策は、組織のビジネス形態、守るべき資産の定義、そしてそれらを運用するための統治体制（ガバナンス）の整合性が取れて初めて成立します。本事例が扱うA社のケースは、まさにこの「ガバナンスと技術の乖離」が招くリスクを浮き彫りにしています。通信教育事業を展開するA社は、受講生の個人情報や受講履歴という、極めて秘匿性の高い情報をビジネスの核としています。ネットワーク構成は、DMZ内にプロキシサーバやメール管理サーバを配置し、オフィスエリアからはDHCPサーバによって動的に割り当てられたIPアドレスを用いて通信を行う標準的な構成を採っています。運用面では、既に「情報セキュリティ管理規程（管理規程）」を策定しており、以下の2点を運用の柱としていました。

- 「**秘密**」区分の設定： 保有情報にマークを表示・押印し、重要度に応じた取扱方法を明確化する。
- 「**権限**」の最小化： 各種システムの操作に関して、業務上必要な最低限の機能のみを付与する。しかし、こうした「ソフト面」の規程が存在するにもかかわらず、現場では「業務上不要なWebサイトへのアクセス」や「メールの私的利用」が常態化していました。これは、既存のガバナンスが個人の良心や自律性に過度に依存しており、運用の実態を監視・制限する強制力を欠いていたことを示唆しています。管理規程がある一方で、物理的に可搬型記憶媒体へのダウンロードが可能であるという現状は、悪意ある内部者にとって極めて容易に情報を持ち出せる環境、すなわち重大なセキュリティホールとなっていたのです。このような組織的な脆弱性を解消するためには、現状の課題をフレームワークに基づいて構造化し、対策の優先順位を明確にする必要があります。

2. 不正のトライアングルに基づいた問題点の特定

内部不正対策を検討するにあたって、場当たりの技術導入はコスト対効果を低下させます。IPAの「組織における内部不正防止ガイドライン」でも推奨されている「不正のトライアングル」という標準的なフレームワークを適用することで、問題の所在を客観的に特定し、戦略的な防御線を構築することが可能になります。A社の情報セキュリティリーダーであるB主任は、チェックシートを用いた現状分析により、以下の3つの問題点を特定しました。

1. **可搬型記憶媒体の運用不備**： 規程に反するデバイス接続が物理的に可能な状態。
2. **Web/メール利用の管理不足**： 禁止事項が技術的に制限されておらず、個人の裁量に委ねられている状態。
3. **ログ管理の不備**： 重要情報へのアクセスや操作履歴が適切に取得・管理されていない状態。これらはいずれも、不正のトライアングルにおける「機会（不正を行おうと思えばできてしまう環境）」を構成しています。ソースコンテキストにおいて指摘されている通り、「悪意をもった行動に対しては管理規程だけでは対処できな

い」のが現実です。規程というソフト面の対策を、技術というハード面で補完し、不正の「機会」を物理的に消失させることが、内部不正対策の本質的な意義となります。次に、これらの特定された「機会」を最小化するために講じられた、具体的な技術的・運用の対策を詳述します。

3. 技術的対策の深度：デバイス制御、メール、Webアクセス管理

セキュリティ強度の向上は、往々にして業務の利便性とトレードオフの関係に陥ります。優れたセキュリティ戦略とは、高い防壁を築きつつも、正当な業務の継続性を損なわないための「例外処理の設計」にあります。A社が導入した技術的対策の核となるのは、以下の3点です。

- **デバイス制御機能による物理遮断：** 新たに導入したPC管理システムにより、管理規程で許可されていない可搬型記憶媒体の接続を拒否します。これにより、物理ポートからの情報流出経路を確実に封鎖します。
- **メール送信の二重チェック（承認プロセス）：** 送信メールをシステムで一旦保留し、「あらかじめ指定された上司に通知し、上司の承認後に送信する」機能を有効化しました。これにより、送信者本人以外の第三者によるチェックが介在し、誤送信と意図的な漏えいの双方を防ぎます。
- **ホワイトリスト方式によるWebアクセス管理：** プロキシサーバでのURLフィルタリングを「ホワイトリスト方式」へと切り替えました。これは、許可されたサイト以外を原則遮断する強力な制限です。ここで特筆すべきは、ホワイトリストに含まれないサイトが必要な場合の「認定申請」というプロセスの導入です。これは、セキュリティを単なる「一律の禁止」に留めず、「正当な理由に基づく許可」へと転換させる仕組みです。情報セキュリティ委員会の認定を介することで、例外処理が組織的に可視化され、業務上の必要性和セキュリティリスクの評価を同時に行うガバナンス体制が確立されました。このように技術的な遮断策を講じる一方で、万が一の事態に備えた事後の検証能力と、不正を思い留まらせる心理的抑止策の構築が不可欠となります。

4. デジタルフォレンジックスと心理的抑止効果

ログの取得と管理は、単なる「記録」の保持ではありません。それは、事後の徹底した原因究明を可能にする法的証拠性の確保であり、同時に「見られている」という認識を植え付けることによる心理的な防壁です。A社では、法的証拠性を明らかにするための「デジタルフォレンジックス」の観点から、ログ取得体制を再構築しました。具体的には、プロキシサーバの通信ログ、PC管理システムによる操作ログ、そしてメール管理システムによるアーカイブの統合的な管理を実施しています。ここで重要な技術的ポイントは、プロキシサーバにおける「利用者認証」の導入です。A社のネットワークでは、PCに対してDHCPサーバから動的にIPアドレスが割り当てられています。IPアドレスが頻繁に入れ替わる環境下では、通信ログに記録されたIPアドレスだけでは、特定の操作を「誰が」行ったのかを後から確実に特定することができません。そのため、プロキシサーバ経由のアクセス時に利用者認証を強制し、ログに作業者のIDを直接記録することで初めて、個人の特定と証拠能力の担保が可能になるのです。また、これらの対策を「社内に告知」することは、不正のトライアングルにおける「機会」を心理的に消失させる効果があります。不正を企てる側に対し、「不正を働い

でもすぐに発覚する」「隠し通すことは不可能である」という認識を与えることは、物理的な制限以上に強力な抑止力として機能します。

5. 試験対策ポイントと学習のまとめ

応用情報技術者試験の午後問題において、正解を導き出すためには、問題文の文脈（コンテキスト）から適切な専門用語を抽出する能力が求められます。特に内部不正のテーマでは、組織のルール（規程）と技術的実装の対応関係を読み解くことが合格への鍵となります。以下に、本事例の重要語句と導出根拠を整理しました。

設問	解答キーワード	コンテキスト上の導出根拠
-----	-----	-----
設問1	秘密 / 権限	「区分を設定し、マークを表示（秘密）」 「最低限の機能を利用できる（権限）」という記述から。
設問2	デバイス制御 / 認定申請	許可外媒体の接続を拒否する機能の名称、 およびホワイトリスト例外時の申請手順。
設問3	デジタルフォレンジックス / 利用者認証	「法的証拠性を明らかにすること（フォレンジックス）」の定義、およびDHCP環境下で作業者を特定する手段。

※設問3(1)の「デジタルフォレンジックス」は、試験の採点基準に合わせ正確な表記を意識してください。単に正解を覚えるのではなく、「なぜその対策が選ばれたのか（例：DHCP環境だから利用者認証が必要）」という論理的な背景を理解することは、高度IT人材としての洞察力を養うことに繋がります。本レポートで解説した「デバイス制御」「承認フロー」「ログ監視」「告知による抑止」のスキームは、実務における情報漏えい対策のチェックリストとしても極めて有効です。合格の先にある実務を見据え、多角的な視点からセキュリティガバナンスを構築する能力を磨いてください。