

令和3年度 秋期 応用情報技術者試験 午後問1「物理的セキュリティ」 徹底復習レポート

1. はじめに：本事例の背景と組織における物理セキュリティの重要性

組織の情報セキュリティガバナンスを構築する上で、物理的セキュリティ対策はすべての防衛層の起点となる極めて重要な要素です。いかに強固なネットワーク防御を敷いても、オフィス内への不正侵入や重要情報の安易な持ち出しが許されれば、組織の信頼は根底から覆されます。本事例の対象であるA社（日用雑貨の通信販売会社）は、事業の順調な拡大に伴い、管理する個人情報の量が飛躍的に増大しました。この「急激な事業拡大」に対し、従来の物理的な管理習慣や設備が追いつかず、セキュリティ上のリスクが顕在化していたことが、今回の見直しの大きな背景です。情報セキュリティ委員会が物理的対策に焦点を当てたのは、デジタルな防御だけでは解決できない「現場の行動」に起因する脆弱性を是正するためです。大量の個人情報を守る社会的責任を果たすべく、A社は技術的・物理的な制約を導入することで、社員の意識改革とリスク低減を目指しました。本レポートでは、まずその防衛の要となる「ゾーン設計」と「入退室管理」の技術的構造から分析を開始します。

2. ゾーン設計と入退室管理システムの技術的構造

オフィスにおける「ゾーニング」は、情報の重要度に応じてエリアを区分し、段階的に防護レベルを引き上げる戦略的な手法です。**ゾーン管理レベルの比較（A社の事例）**

- **第1ゾーン（受付エリア）**： 入室制限なし。来訪者が最初に立ち入る公共性の高い境界領域。
- **第2ゾーン（執務エリア・ロッカー室・会議室）**： 全社員がアクセス可能。非接触型ICカードによる認証が必須。
- **第3ゾーン（資料保管室）**： 許可された特定の社員のみが入室可能。
- **第4ゾーン（サーバ室）**： 最も警戒レベルが高い区域。特定の権限者のみが立ち入りを許される最重要エリア。このゾーニングの実効性を支えるのが、非接触型ICカードを用いた入退室管理システムです。その通信原理を専門的な視点から詳述すると、まずカード読取り装置（CR）が一定の **電磁波**（空欄b）を発信しています。カードがCRに近づくと、内部の **アンテナコイル**（空欄a）がこの電磁波を **電磁誘導**によって電気へと変換します。このプロセスで得られた電力を利用してICチップ内のプログラムが動作し、CRとの間で無線通信を行ってID照合と解錠判断を下す仕組みです。また、物理的な境界に設置される複合機などのIT機器にも高い信頼性が求められます。A社が導入している複合機は、**CC（Common Criteria）**（空欄c）と呼ばれる、ITセキュリティ評価基準の国際標準規格（ISO/IEC 15408）に基づいた認証を取得しています。これは、製品が適切に設計・実装されていることを第三者機関が保証するものであり、ハードウェアの選定自体がセキュリティレベルを左右することを示しています。しかし、どれほど技術的基盤が強固であっても、それを扱う「人間」の運用に隙があれば、セキュリティは容易に形骸化します。次に、監査視点から浮き彫りになった現状の「隙」を深掘りします。

3. 現状の問題点(Table 1)に対する深掘り分析

A社では事業拡大による業務量の増加が優先され、セキュリティ意識が日常の行動に浸透していない実態がありました。表1に挙げられた6つの問題点は、以下の3つの重大なリスクカテゴリに再編できます。

1. 物理的侵入リスク：共連れ、来訪者の単独行動 これらは物理的な境界防御を無効化する行為です。特に「共連れ」は、一人分の認証で複数人が入室することを許し、記録（証跡）のない侵入を可能にします。また、来訪者の単独行動を許している現状は、物理的な破壊やのぞき見のリスクを放置している状態に他なりません。これらは組織の拡大に伴い、社員相互の「顔見知り」という心理的安心感が悪い方向に作用した結果と言えます。

2. 情報漏洩リスク：複合機への放置、離席時の書類・PC放置 「印刷物の放置」や「机上への書類放置」は、悪意のない第三者に対しても容易に機密情報を曝露する行為です。これらは、社内は安全であるという過度な思い込みが生んだ脆弱性であり、事業規模に見合った「クリアデスク」の規程が形骸化していたことを示しています。

3. 不正持ち出しリスク：私物の持ち込み、NPCの操作可能状態での放置 ノートPC（以下、NPC）をログイン状態のまま放置して離席することは、なりすましによる不正操作の機会を与えます。また、私物の鞆を執務エリアに持ち込める環境は、情報の不正持ち出しに対する物理的なチェック機能を失わせます。これらは情報セキュリティ投資がビジネスの成長スピードに追いついていなかった典型的な例です。これらの具体的リスクを解決するため、A社が導入した「技術による強制」と「運用の改善策」を次に評価します。

4. 改善策の評価と実装上の留意点

提案された対策は、利便性とセキュリティのバランスを技術的仕組みによって解決しようとするものです。

- **アンチパスバックの論理：** 下線①にある「通行を許可された社員カードをCRにかざしても解錠しない」ケースの典型は、**入室状態となっている人が再度入室しようとした場合** です。入室と退室の記録が論理的に一致しない場合に解錠を拒否することで、一枚のカードで複数人が入室する「共連れ」を確実に防止します。
- **来訪者管理の事後検証：** 下線②の対策として、第4ゾーンなどの重要エリアに **監視カメラを設置して来訪者の行動を記録する** ことは極めて有効です。これは不正に対する心理的な抑制効果（抑止）を生むだけでなく、インシデント発生時の確実な証跡管理を実現します。
- **オンデマンド印刷の効果：** 下線③の機能は、**複合機の側に行かないと用紙への印刷ができないから** という物理的制約を利用しています。カード認証後に初めて印刷が開始されるため、印刷物の放置という課題を根本から解決します。
- **クリアスクリーンの重要性：** 設問2の正解である「**クリアスクリーン**」は、離席時にNPCの画面を他人が操作・閲覧できない状態にするための統制です。操作しないまま一定時間が経過した際に、自動的にパスワード付きスクリーンセーバを起動させる、あるいは自動ログオフさせる設定は、不正操作の機会を最小化する基本的な防御策です。これらの技術的・物理的制約は、個人の意識に頼るだけでなく、システム側で「不正ができない状態」を強制する点にその実効性があります。

5. 人的・物理的統制の統合：透明鞆と情報セキュリティ管理規程

厳格な物理セキュリティは、時に社員の利便性と衝突し、反発を生む可能性があります。そのため、マネジメント層はいかに「受け入れ可能な妥協点」を見出すかが問われます。A社が導入した、中が透けて見える「**中が透けて見える**」（空欄d）鞆の貸与はその好例です。私物の鞆の持ち込みを一律に禁止するのではなく、透明な鞆に入れ替えて持ち込むことを許可することで、社員の最低限の利便性を確保しつつ、会社側は **秘密書類の持出し**（設問3-4行為）といった不正行為を視覚的に監視・抑制することができます。これは物理的な「見える化」による心理的抑止と物理的統制を両立させた対策です。また、これらの設備を導入するだけでなく、「情報セキュリティ管理規程」にこれらの遵守事項を明記し、全社員に周知徹底することが不可欠です。規程という「根拠」があることで、対策の実効性は組織的に担保されます。物理的な制約が個人の行動習慣を強制的に変え、それが規程の遵守へとつながる好循環を構築することが、セキュリティ管理の要諦です。

6. 結論：本事例から学ぶ、物理セキュリティ設計の黄金律

A社の事例を抽象化すると、物理セキュリティを成功に導くためには、以下の3要素を相互補完的に機能させることが不可欠であると結論づけられます。

- **多重防御の設計（技術・物理・行政的統制）**： ICカードや監視カメラといった「物理設備」を、アンチパスバックやオンデマンド印刷という「技術的制御」で動かし、それらを「規程」という行政的統制で裏付けること。
- **心理的抑止と物理的強制の調和**： 監視カメラによる「見られている」という意識の醸成（心理的抑止）と、認証がなければ物理的に扉が開かない、印刷されないという「物理的強制」を組み合わせること。
- **利便性と実効性のバランス**： 透明鞆の事例のように、社員の抵抗を抑えつつ、目的（不正持ち出し防止）を達成するための「受け入れ可能なルール」を設計すること。物理セキュリティの核心は、単なる設備の導入に留まらず、その技術をいかに組織のルール（規程）と個人の行動（運用）に統合し、持続可能な文化として定着させるかにあります。本事例は、事業の成長に伴うリスクの変化に合わせ、これら3要素を再構築することの重要性を我々に示唆しています。