

平成30年度 秋期 応用情報技術者試験 午後問7：電子扉システムの設計に関する詳細復習レポート

1. 電子扉システムの設計背景と戦略的意義

組込みシステム設計の本質は、ソフトウェアによる論理制御と、物理デバイスが持つ現実の「時間」や「慣性」をいかに同期させるかにあります。本事例の電子扉システムは、単なる自動施錠・開錠の仕組みを超え、組織のセキュリティガバナンスを物理層から担保するインフラとして設計されています。

入退室管理の基本コンセプト

本システムでは、「カード識別コード」によって「誰が（Who）」を特定し、「扉識別コード」によって「どこを（Where）」通過しようとしているかを管理します。これらの識別情報を組み合わせてサーバに問い合わせることで、従業員ごとの柔軟なアクセス制御を実現しています。

サーバー集中管理型のメリット

各扉ユニットで判定を完結させず、サーバで一元管理する設計には、以下の戦略的メリットがあります。

- **権限管理の柔軟性：** サーバ側のデータベースを更新するだけで、即座に全拠点の通行権限を動的に変更可能。
- **運用ログの完全性：** 「誰が・いつ・どの扉を・どちら向きに」通過したかをリアルタイムで集約でき、監査証跡としての信頼性が向上する。システムの全体像を確認したところで、次に具体的な通信プロトコルと識別情報の役割を分析します。

2. 通信プロトコルと識別情報の構成分析（設問1の深掘り）

制御部とサーバ間でやり取りされるデータの整合性は、セキュリティの穴を塞ぐための生命線です。情報の欠落は、そのまま権限の誤判定という深刻な脆弱性を招きます。

識別情報の論理的導出

ソースコンテキストに基づく、空欄 a と b は以下の通り定義されます。

- **a カード識別コード：** カードごとに割り当てられた固有情報。サーバが「所有者を特定」するために必須。
- **b 扉識別コード：** 扉ユニットごとに設定された固有情報。サーバが「入退室する場所を特定」するために必須。

「入室」と「退室」の峻別プロセス

本システムでは、同一の扉に対して室内・室外の両方にカードリーダが設置されています。ここに「リーダ設置区分コード」を付与することで、システムは「入室」と「退室」という通行の方向性を正確に把握します。これにより、エリア内の滞在人数把握（アンチパスバック等）を可能にする設計上の必然性が生まれます。

設計上の必然性：3要素の紐づけ

- **Who（個人）**： カード識別コード
- **Where（場所）**： 扉識別コード
- **Direction（方向）**： リーダ設置区分コード通信データによる識別が完了した後は、電子扉ユニット内部での具体的なプログラムフロー制御に焦点を当てます。

3. プログラム処理フローとタイマ制御の論理構造（設問2の詳解）

状態遷移設計において、例外処理（エラー音）とタイマによる時間監視は、システムの安全状態を維持するために不可欠です。

フローチャートのプロセス解説

図3における主要プロセスは、以下の仕様にに基づき論理的に構成されています。

- **c エラー音を発生する**： サーバからの応答が開錠許可でない（No）場合の例外処理。
- **d タイマに $t1$ 秒を設定する（オ）**： 開錠後、扉が開かれなかった場合の自動施錠用監視時間を起動。
- **e タイマに $t2$ 秒を設定する（カ）**： 扉が開いた後、開放が継続される時間を監視するためのタイマ。
- **f 閉扉**： 正常に扉が閉まったことを検知し、監視フェーズを終了させるトリガー。
- **g タイマ満了**： 規定時間内の動作がなかったことを示す、OSタイマ機能からの通知。

2つのタイマ設定と設計制約（ $t2 > t1 > 1$ ）

本システムでは $t1$ （未開封監視）と $t2$ （開放継続監視）の2つのタイマが使い分けられています。重要なのは、**「 $t2 > t1 > 1$ 秒」**という設計上の数学的制約です。これは、物理的な施錠・開錠に伴う1秒のタイムラグを考慮しつつ、セキュリティリスク（扉の放置）を段階的に管理するための安全マージンです。

状態管理の要「タイマ取消し」

フロー内の「タイマ取消し」は、単なる停止ではなく**「状態のクリーンアップ」**としての役割を持ちます。これを確実に行うことで、例えば「扉を閉めたのに以前の監視タイマが発火して警告音が鳴る」といった状態の不整合を防止しています。

- **開扉イベント**： 正当な通過を確認。 $t1$ を取消し、 $t2$ 監視へ移行。
- **閉扉イベント**： 正常な通過完了。 $t2$ を取消し、処理を終了。
- **タイマ満了イベント**： 異常な放置を検知。自動施錠または警告音鳴動を実行。

4. 物理的遅延とソフトウェアの不整合：不具合の根本原因（設問3の徹底検証）

組込み設計の盲点は、ソフトウェアの命令実行と物理デバイスの動作完了の間に存在する「物理的遅延」にあります。本システムにおける「1秒の壁」が、状態の不整合を引き起こします。

「Atomic Processing」中の盲点

仕様上、「①施錠する」の通知から実際に施錠されるまでには1秒掛かり、**その間、次の処理は行われません。** プログラムはこの1秒間、一種の「不可分 (Atomic) な処理ブロック」の中にあり、外部からの「扉が開いた」という非同期イベントに対して事実上の「盲目状態」となります。

不具合が発生するエンジニア視点での条件

この不具合（警告音が鳴動しない現象）は、ソフトウェアが想定していない**「状態遷移の隙間」**を突かれた際に発生します。

- **不具合条件：** 「①施錠する」の処理（1秒間）の最中に扉が開けられ、そのまま \$t2\$ 秒が経過する。

実行パスの逸脱プロセス

1. 誰も扉を開けずに $t1$ 秒が経過し、タイマ満了により「①施錠する」が実行される。
2. この「施錠命令の物理的待ち時間（1秒）」の間に、レバーが開錠状態であるため扉が開けられる。
3. しかし、プログラムは「①施錠する」の処理を完了させると、そのまま **フローの「終了」へと抜けてしまう。**
4. 本来、扉が開いた際に実行されるべき「 $t2$ タイマの設定」や「警告監視のイベント待ち」というパスを完全に逸脱するため、警告音が鳴動しない。

5. 本事例から学ぶ設計上の教訓とまとめ

本問題の分析を通じて、高信頼性システムを設計するためのクリティカルな知見が得られます。

実務における設計上の教訓

- **物理的遅延の考慮：** 命令完了と物理状態の完了は同時ではない。この不整合 (State Inconsistency) を考慮した設計が必要。
- **非同期イベントの受付能力：** 特定の処理実行中に発生した割り込みイベントを破棄せず、適切にバッファリングまたは状態に反映させる構造が不可欠。
- **例外パスの網羅性：** 「自動施錠」という安全系処理の最中に、新たな「違反（開扉）」が発生する複合的な例外パターンを予見すること。

応用情報技術者試験の攻略アドバイス

午後問題の組込み分野では、問題文中の「時間に関する記述」が正解への最大のヒントです。

- **制限字数内でのモデル回答：** 設問3の不具合条件を35字以内で表現する場合、以下の回答が「満点」の構成となります。
- 「①施錠する」の処理中に扉が開けられ、そのまま \$t2\$ 秒経過したとき。 (33文字)

- **テクニック：** 数値条件（1秒、 $t1$ 、 $t2$ ）を見つけたら、それらが重なり合う「タイミングの矛盾」を探してください。フローチャートの出口（終了）に向かうパスに「監視の漏れ」がないかを確認する癖をつけることが合格への近道です。本レポートが、物理層と論理層を統合して捉える「動的なシステム思考」の深化に役立つことを期待します。