問４　ICカードを利用した入退室管理システム（情報セキュリティ）（H25春-FE 午後問4）

【解答】
［設問１］　ウ
［設問２］　ウ
［設問３］　a－ア
［設問４］　エ
［設問５］　エ

【解説】
近年，企業等の組織において機密情報や個人情報の保護のため，オフィスにICカードを応用した入退室管理システムを導入することがよく行われている。しかし，運用ルールを定め，ルールに従った運用を行わないと，本来の目的を達成することはできない。セキュリティの確保には，技術面だけでなく，それを適切に運用することが求められる。

この問題は，設問１はセキュリティ用のICカードの知識が求められるが，それ以外は本文の記述をよく読めば，解答できる問題である。

［設問１］
耐タンパ性の意味が問われている。耐タンパ性とは，不正な手段によって内部のデータを解析することの困難さのことである。ICカードには電極があり，読取り装置に挿入することによってICカードとの通信を行う接触型ICカードと，電磁波（電波）を用いて通信を行う非接触型のICカードがある。どちらのタイプでも，セキュリティ用途のICカードは，ICカードを不正な読取り装置に接続して，内部情報にアクセスされては困るので，通信の暗号化を行い，また内部データそのものも暗号化して，不正なアクセスから防御していることが多い。しかし，特殊な解析装置を接続して，物理的に内部情報を解析する手法やICチップから漏れ出る電磁波を解析するサイドチャネル攻撃という手法もある。更に，ICカードのICチップを裸にして，ICチップそのものにプローブ（探針）を接続して解析する攻撃方法もある。このような，物理的な攻撃に対処するため，不正な物理的な攻撃を受けた場合には，情報が消滅する仕組みや，ICチップそのものが破壊されるような工夫がされていることがある。このような，不正な手段によって内部のデータを解析することの困難さを，耐タンパ性と呼ぶ。したがって，解答は（ウ）である。

［設問２］
入退室管理システムの入退室のログとして収集するべき情報が問われている。〔J社の入退室管理システムのセキュリティ要件〕の(3)「②入退室管理システムは入退室のログを収集する」及び(4)「入退室のログから，開発室又は執務室への人退室ごとの出入りした社員又は協力社員，日時，出入口が特定できる」の記述から，入退室のログには，社員又は協力社員を一意に識別する情報，日時，出入口を一意に識別する番号が必要であることが分かる。表２の入退室情報には，「ICカード利用日時」，「ICカード読取り装置識別番号」，「ICカードID」の項目がある。ICカード利用日時は，ログの日時に対応し，ICカード読取り装置識別番号は，出入口を一意に識別する番号である。また，表１の利用者情報から社員又は協力社員を一意に識別する利用者情報が，利用者IDであることが分かる。

利用者IDは，ICカードIDとひも付けされているから，ICカードIDから利用者IDを一意に識別できる。ログとして収集するべき項目は，「ICカード利用日時，ICカード読取り装置識別番号，ICカードID，利用者ID」となる。したがって，（ウ）が正解である。

［設問３］
図１の状態遷移図において空欄aは，仮パスワード状態から一時利用停止状態への遷移である。表１のICカードの状態の説明には，「3回連続してパスワードを誤って入力した場合，“一時利用停止”になる」との記述がある。したがって，（ア）の「3回連続してパスワードを誤入力」が正解である。

［設問４］
図１の社員を対象とした状態遷移図から最少の変更で協力社員を対象にした状態遷移図を作成する問題である。図１にはICカードの状態が「有効」の状態における，入出許可の状態には，②の「執務室だけ許可」と⑤の「開発室許可」の二つがありこれは，問題文の〔入退室管理システムの運用の説明〕の(1)(a)にある「これで社員の執務室への入室が可能となる」の記述と，(b)の「プロジェクトマネージャ（以下，PMという）からの申請を受けて，開発室へのプロジェクトメンバの“入室許可の状態”の設定を変更する」の記述に対応している。次に，協力社員に対する運用を考える。〔J社の入退室管理システムのセキュリティ要件〕の(1)の「社員及び協力社員は，プロジェクトに参画している期間中だけ開発室に入室可能とする」の記述から，協力社員も⑤の「開発室許可」の状態が必要であることが分かる。また，〔入退室管理システムの運用の説明〕の(2)協力社員に対する運用を参照すると，協力社員には，執務室だけへの入室許可に関する記述が見当たらない。よって協力社員を対象とした状態遷移図の場合は，ICカードの状態が「有効」の状態においては，⑤の「開発室許可」だけとなり，②の「執務室だけ許可」の状態はあり得ないことになる。よって，協力社員が契約を終了した場合に遷移する矢印は，「開発室許可」から「返却」への線，δ（デルタ）となる。したがって，（エ）が正解である。

［設問５］
「入退室管理システムのログに，入室履歴のない退室履歴や退室履歴のない入室履歴が見つかった」とある。これは，自分のICカードを使わずに直前に入退室した者の後に付いて扉をくぐる不正行為で，一般にピギーバック又は，共連れ，複数人侵入行為などと呼ばれる行為である。この不正行為は，ICカードを読取り装置にかざす行為をしないため，パスワードによる認証もなく，ログにも残らないという問題がある。そこで，自分のICカードを必ず読取り装置にかざさせる対策として入退室管理システムで管理する現在の状態遷移を変更することになった。

この設問では，図１の状態番号のうち，入室履歴又は退室履歴のない者がICカードをかざして退室又は入室しようとした際に，遷移する先として適切な状態番号を答える問題である。強制力があるのは，不正を行うとICカードを使って入退室できなくすることである。そのための候補としては，①「仮パスワード」，④「一時利用停止」，③「返却」への状態遷移が考えられる。②もしくは⑤の「有効」から状態遷移の矢印があるのは，③「返却」，④「一時利用停止」の二つである。①「仮パスワード」への状態遷移は④の「一時利用停止」から，セキュリティ管理者によるパスワードの初期化が必要である。そのため，②もしくは⑤の「有効」から①「仮パスワード」への直接的な状態遷移は不可能であり，いったん，④の「一時利用停止」へ遷移するのは，妥当であると考えられる。また，③の「返却」に遷移すると，ICカードそのものを返却，すなわち取り上げることになる。すると，ICカードの新規発給作業が必要となり，セキュリティ管理者の作業及び，プロジェクトマネージャによる入室許可の申請など，運用における負荷が高くなる問題がある。以上から遷移する先として適切な状態は④「一時利用停止」となる。したがって，（エ）が正解である。