問040011解説

◆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

入退室のセキュリティ管理に関する問題である。

入退室管理システムのセキュリティ要件

① 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。
② ＩＣカードは耐タンパ性をもつものを使用し，ＩＣカードＩＤだけを情報としてもつ。
③ 入退室管理システムは入退室のログを収集する。
④ 入退室のログから，開発室又は執務室への入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。
⑤ パスワードは８桁の数字(00000000～99999999)とする。
⑥ 有効期間中はＩＣカードとパスワードによって開発室や執務室への入室ができる。
⑧ 入室時又はパスワードの変更時に，３回連続してパスワードを誤って入力した場合，開発室や執務室への入室はできなくなる。

耐タンパ性

耐タンパー性はコンピュータシステムの内部構造の解析のしにくさ、見破られにくさのことである。ハードウェアの回路構成やソフトウェアのプログラム構造など、特殊な技術を用いている製品は、リバースエンジニアリングによって仕組みを分析されることを嫌い耐タンパー性を向上させる試みが行われている。リバースエンジニアリングは、製品やプログラムを分解したり解析したりすることで、その構造や仕様、技術などを明らかにする技法のことであり、製造する側は自社製品の優位の秘訣となっている構造を探られないために、回路の暗号化やプログラムの冗長化などを施す。耐タンパー性を向上させる方法としては、回路のアルゴリズムを複雑にしたり、プログラムデータの暗号化を行ったりする。

入退室管理システムの運用の説明

セキュリティ管理者は，入室申請の受付，入退室管理システムへの利用者情報の設定，ＩＣカードの発給を担当する。

社員に対する運用

① 社員の入社時に，入退室管理システムの運用ルールを説明した後，ＩＣカードを発給し，パスワードを仮パスワードから変更させる。これで社員の執務室への入室が可能となる。

② プロジェクトの開始時及び終了時に，ＰＭ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。

③ 退職時には，ＩＣカードを返却させるとともに，″有効期間の終了日″に退職日を，″ＩＣカードの状態″に″返却″を設定する。

協力社員に対する運用

① プロジェクトの開始時に，ＰＭからの申請を受けて，当該協力社員の利用者情報を登録すると同時に″入室許可の状態″を設定し，ＰＭに協力社員用のＩＣカードを発給する。ＩＣカードを受領したＰＭは入退室管理システムの運用ルールを協力社員に説明した後，ＩＣカードを配布してパスワードを仮パスワードから変更させる。

② 契約の終了時は，協力社員に配布していたＩＣカードの返却をＰＭ経由で受けて，″有効期間の終了日″に契約の終了日を，″ＩＣカードの状態″に″返却″を設定する。

利用者情報の削除処理

① ″有効期間の終了日″を過ぎ，かつ，″ＩＣカードの状態″が″返却″の利用者情報は，週末のバッチ処理でバックアップメディアに保存した上で，入退室管理システムから削除する。

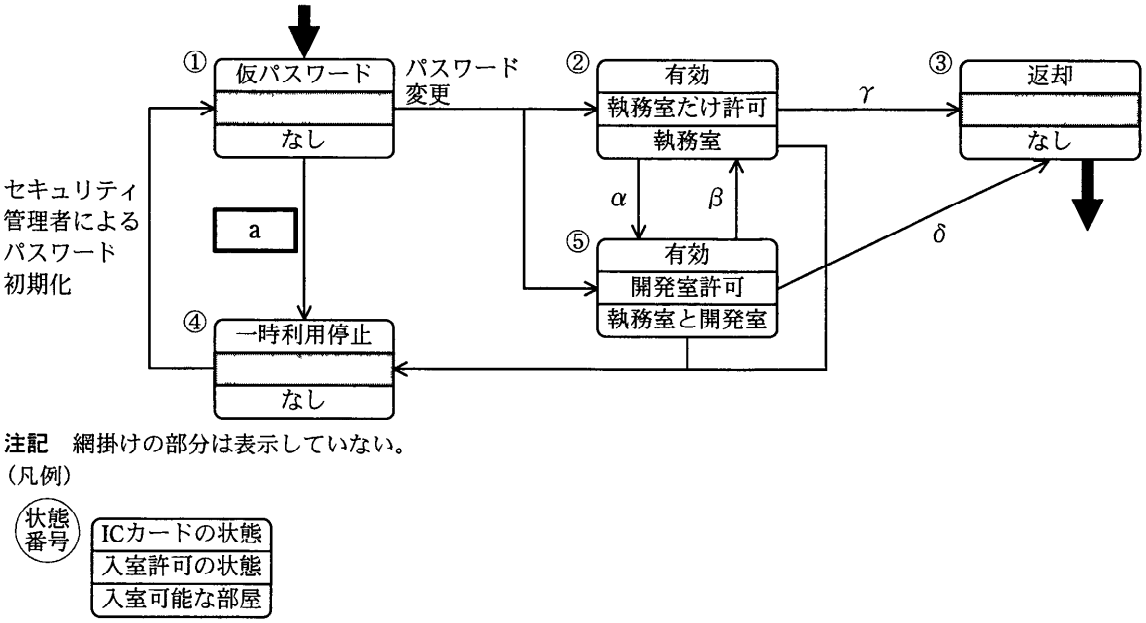
② 返却されたＩＣカードは，後日再利用する。

表１　主な利用者情報

利用者情報	説明
利用者 ID	社員の場合は社員番号を設定し，協力社員の場合は契約時に個人ごとに付与される契約番号を設定する。
IC カード ID	IC カードを識別する一意の ID
IC カードの状態	“仮パスワード”，“有効”，“返却”，“一時利用停止”のいずれかである。IC カードを発給したときは，“仮パスワード”を設定する。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。
入室許可の状態	“開発室許可”，“執務室だけ許可”，“入室不可”のいずれかである。
有効期間の終了日	社員の場合は，退職予定の年月日を設定しておく。協力社員の場合は契約期間に基づいて契約終了予定の年月日を設定しておく。
（上記以外の利用者情報） 氏名，有効期間の開始日，利用者区分，プロジェクト番号，パスワードなど	

表２　主な入退室情報

入退室情報	説明
IC カード利用日時	出入口で IC カードをかざした年月日時分秒
IC カード読取り装置識別番号	出入口に設置している IC カード読取り装置を識別する一意の番号
IC カード ID	出入口でかざした IC カードの ID



社員を対象とした状態遷移図

社員を対象とした入退室管理の状態遷移図の説明

① 仮パスワードが発行される。（状態①）

② 仮パスワードから本パスワードへ変更し執務室への入室が許可される。（状態①から状態②へ遷移）

③ プロジェクト開始時に開発室許可となり、執務室と開発室で業務が可能になる。（状態②から状態⑤へ遷移α）

④ プロジェクト終了時に開発室への入室が不許可となり、執務室のみで業務が可能になる。（状態⑤から状態②へ遷移β）

⑤ プロジェクトと関係ない状態での退社は、執務室だけ許可からカードの返却となる。（状態②から状態③へ遷移γ）

⑥ プロジェクトと関係中の状態での退社は、開発室だけ許可からカードの返却となる。（状態⑤から状態③へ遷移δ）

⑦ 入室時やパスワード変更時に連続して３回の誤入力を行うと、状態①、状態②、状態⑤のいずれかから状態④に遷移する。

協力社員を対象とした入退室管理の状態遷移図の説明

① プロジェクト契約時に仮パスワードが発行される。（状態①）

② 仮パスワードから本パスワードへ変更し開発室への入室が許可され、開発室での業務が可能となる。（状態①から状態⑤へ遷移）

③ プロジェクト終了時や退社時に契約が終了し、開発室への入室が不許可となり、カードの返却となる。（状態⑤から状態③へ遷移δ）

④ 入室時やパスワード変更時に連続して３回の誤入力を行うと、状態①、状態⑤のいずれかから状態④に遷移する。

設問１

ＩＣカードの「耐タンパ性をもつ」内容の説明問題である。耐タンパー性はコンピュータシステムの内部構造の解析のしにくさ、見破られにくさのことであり、ウの内部情報に外部から不正にアクセスできないＩＣカードのことである。求める答えはウとなる。

設問２

ログ情報は、ログはコンピュータの利用状況やデータ通信など履歴や情報の記録を取る事であり、集めた情報をログ情報という。通常は、操作やデータの送受信が行われた日時と、行われた操作の内容や送受信されたデータの中身などが記録される。

入退室管理システムでは、ＩＣカードを利用した日時、利用したＩＣカード読取装置識別番号、ＩＣカードＩＤ、利用者ＩＤとなる。求める答えはウとなる。

アはＩＣカード利用日時が不明、イはＩＣカード読取装置識別番号が不明、エはＩＣカードＩＤ、利用者ＩＤが不明であり、入室許可の状態は期間的に固定した情報であるから入退室時の情報としては不要である。

設問３

仮パスワードから本パスワードに変換手続きする場合の処理であり、入室時又はパスワードの変更時に，３回連続してパスワードを誤って入力した場合，開発室や執務室への入室はできなくなるに該当するため、アの３回連続してパスワードをご入力となり、求める答えはアとなる。

設問４

社員の場合はプロジェクト終了時は、開発室への入室が不許可になるが執務室では業務を継続するため状態⑤から状態②に遷移する矢印βの処理を行うが、協力社員の場合は契約終了と同時に開発室許可が取り消され、返却処理となるため、状態⑤から状態③への遷移の矢印δとなる。

設問５

入退室時に自分のカードを使用せずに他人の使用したカードに便乗して入退室する現象を改善する対策の検討である。常に他人のカードに便乗して入退室する人に対する防止手段は現在のシステムでは不可能である。そこで、意識改革として各関係者に対して入退室時には各自のＩＣカードを使用するように教育を実施し、それでも各自のＩＣカードを使用しなかった場合の検知対策を講じるために、入退室時の処理が適切でない場合にセキュリティ管理者が検知できる仕組みを導入する。そのための手段が状態④への遷移である。

入室時のＩＣカード使用なしの状態で退室時にＩＣカードを使用したり、退室時のＩＣカ

ード使用なしの状態で入室時にＩＣカードを使用すると、状態④に遷移してＩＣカードの一時使用停止になる。一時停止となったＩＣカードはセキュリティ管理者が対応しないと使用することができなくなり、適切に状態把握が可能になる。求める答えはエとなる。