問2　販売システムへの機能追加設計に関する次の記述を読んで，設問1～5に答えよ。

A社は，部品製造を営む従業員数250名の中堅会社である。インターネットを介した販売システム（以下，Nシステムという）を利用し，企業向けに自社製品を販売している。Nシステムは，A社の販売部が3年前に開発し，運用している。

Nシステムの利用者は，利用者ID（以下，UIDという）を保有しており，ブラウザからインターネット経由でNシステムにアクセスし，ログイン画面でUID名とパスワードを入力することによってログインした上で，製品の在庫確認，注文を行う。Nシステムを利用する企業（以下，契約企業という）は，Nシステムの利用契約時に，利用責任者を1名登録する。利用責任者は，ヘルプデスクに対して，UIDの新規登録の他，UIDの削除，パスワード初期化，サスペンド解除を申請できる。申請の際は，利用責任者が申請書を電子メール（以下，メールという）でヘルプデスクに送付する。

Nシステムでは，UIDに対して表1に示す属性を定義し，その値をログイン処理に利用している。NシステムのUID及びログイン処理に関する，セキュリティ要件は図1のとおりである。

表1　UIDに定義している属性（Nシステムの設計書からの抜粋）

属性名	属性の定義
password	ソルトを付加したパスワードの，ハッシュ関数 [a] によるハッシュ値を表す。
mailaddr	利用者のメールアドレスを表す。
status	当該UIDによるログインの可否を表す。 0：ログイン可能　　1：ロックアウト状態　　2：サスペンド状態
temppass	パスワードが仮パスワードか否かを表す。 0：仮パスワードではない　　1：仮パスワードである
fails	パスワード間違いによる連続したログイン失敗回数を表す。
lastlogin_t	ログインに成功した直近の時刻を表す。
lockout_t	ロックアウトが発生した直近の時刻を表す。

(ア) UIDは，複数の利用者での共用を禁止する。
(イ) UID名は，英数字6文字で構成する。
(ウ) パスワードは10文字以上とし，英字，数字，記号を，それぞれ1文字以上含める。Nシステムにはパスワード変更ページが準備されており，ログイン中の利用者はパスワードを変更できる。
(エ) UIDの新規登録時，及び利用者がパスワードを忘れた場合のパスワード初期化時には，UIDに対して仮パスワードを設定する。仮パスワードは十分に長いランダムな文字列とし，ヘルプデスク担当者又はNシステムが決定する。UIDに仮パスワードが設定されている状態を仮パスワード状態と呼ぶ。仮パスワード状態のUIDでNシステムにログインすると，ログイン処理の中で強制的にパスワード変更ページへ遷移する。このとき，利用者はパスワードを変更しない限り，Nシステムへのログインは完了しない。
(オ) ログイン時に，パスワードを連続して5回間違えた場合，そのUIDはログイン不可能になる。このUIDの状態をロックアウト状態と呼ぶ。ロックアウト状態は，60分以上経過した後の最初のログイン時に解除される。連続したログイン失敗回数は，ログイン成功時，パスワード初期化時，及びロックアウト解除時に，0回にリセットされる。ロックアウト状態のUIDに対してパスワード初期化を行うと，ロックアウトが解除される。
(カ) 90日間ログインに成功していないUIDは，ログイン不可能になる。このUIDの状態をサスペンド状態と呼ぶ。サスペンド状態は，契約企業の利用責任者からのサスペンド解除申請によってだけ解除でき，利用者自身では解除できないようにする。
(キ) 利用者のブラウザとNシステムの間の通信には，SSLを用いる。

図1　Nシステムの UID 及びログイン処理に関する，セキュリティ要件

ヘルプデスクでは，図2に示す運用手順でUIDを管理している。ヘルプデスクによるUIDの設定変更時には，表2に示す値をUIDの属性に設定する。サスペンド設定は，バッチ処理で行う。バッチ処理は，毎日00:00に実行し，現在時刻がlastlogin_tの値から90日以上経過した全てのUIDに対して，表2の設定変更(e)に示す各属性値を設定する。

また，Nシステムのログイン画面で，UID名とパスワードが入力された場合のログイン処理の流れを図3に示す。ログイン成功時とロックアウト発生時に，利用者にメールで通知することで，不正ログイン及びその試行を利用者が把握できるようにしている。

1. 利用責任者からの申請書がメールで送付された際に，メールヘッダに記載された送信者メールアドレスが契約時に登録された利用責任者のものであることを確認する。さらに，利用契約時に登録された利用責任者の電話番号に電話をして，メール送信者の本人確認を行った後に，申請された設定変更を 3 営業日以内に行う。利用責任者が，他の契約企業の UID に対する設定変更を申請した場合は，申請を受け付けない。
2. 申請に基づく設定変更は，ヘルプデスク専用の UID 管理画面で行う。UID 管理画面では，設定変更 (a)～(c) に対応し，UID の各属性を表 2 に示す各値に設定する。設定変更 (d) の場合は，UID を削除する。UID 管理画面は，契約企業に公開しておらず，ヘルプデスク担当者だけが利用できる。
3. 2. のうち，UID の新規登録申請，又はパスワード初期化申請では，図 1 のセキュリティ要件を満たす仮パスワードをヘルプデスク担当者が決定し，UID に対して設定する。設定した仮パスワードは，ヘルプデスク担当者が利用責任者に電話し，読み上げて通知する。
4. 設定変更の完了後は，利用責任者に完了通知メールを送付する。
5. サスペンド状態の UID に対しては，UID の削除とサスペンド解除の申請だけを受け付け，それ以外の申請は受け付けない。

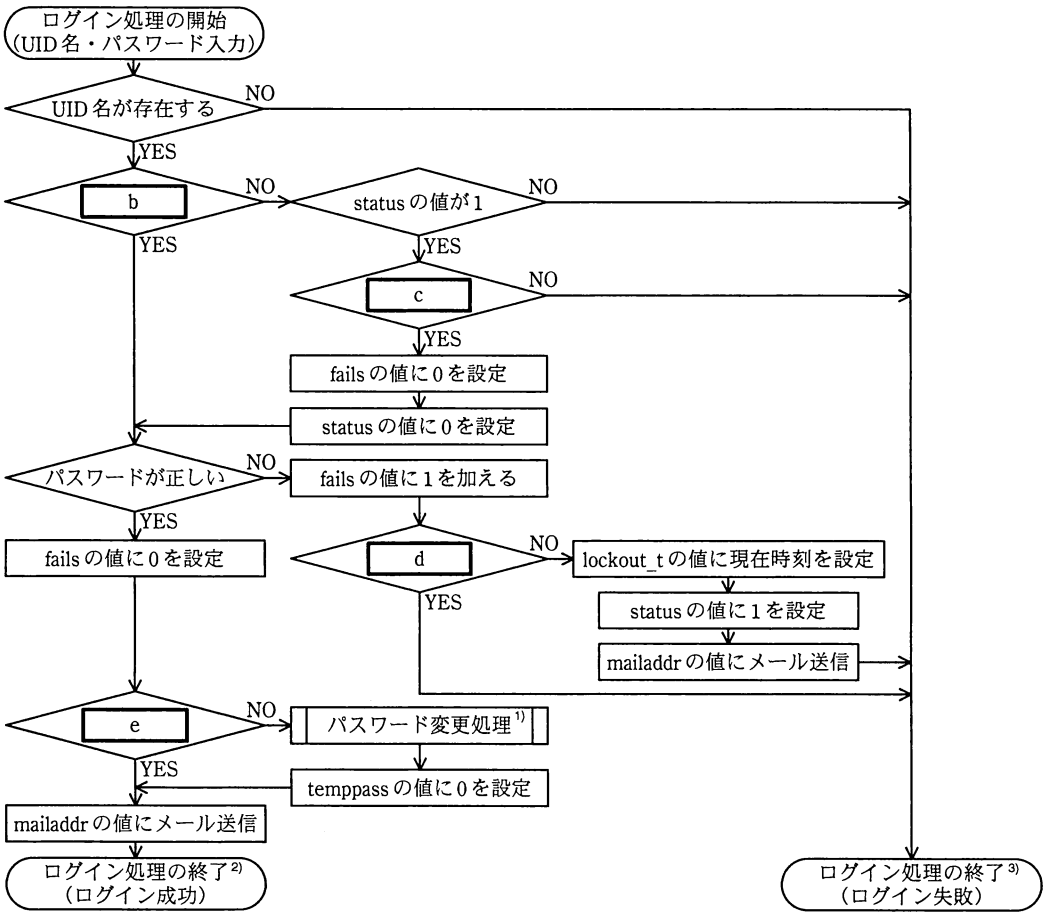
図 2　UID 管理に関するヘルプデスクの運用手順

表 2　設定変更時に UID の属性に設定する値

設定変更項目	設定変更内容	設定変更対象となる属性					
		password	mailaddr	status	temppass	fails	lastlogin_t
設定変更 (a)	新規登録	仮パスワード	メールアドレス	0	1	0	現在時刻
設定変更 (b)	パスワード初期化	仮パスワード	−	0	1	0	−
設定変更 (c)	サスペンド解除	−	−	0	−	−	現在時刻
設定変更 (d)	削除	UID を削除する					
設定変更 (e)	サスペンド設定	−	−	2	−	−	−

注記 1　表中の“−”は，値を変更しないことを意味する。表中に記載がない属性の値は変更されない。

注記 2　表中の“仮パスワード”はソルトを付加した仮パスワードのハッシュ値を，“メールアドレス”は利用者のメールアドレスを，また“現在時刻”は設定変更時の現在時刻を，それぞれ表す。



注 1) パスワード変更処理では，利用者にパスワード変更ページを表示し，新しいパスワードが図1のセキュリティ要件を満たす場合に，password の値を更新する。パスワード変更処理の流れ図は省略する。

2) ログイン処理の終了（ログイン成功）では，lastlogin_t の値に現在時刻を設定する。

3) ログイン処理の終了（ログイン失敗）では，ログイン失敗というメッセージを表示し，ログイン画面を再度表示する。

図3　Nシステムのログイン処理の流れ（Nシステムの設計書からの抜粋）

〔契約企業からの要望〕

Nシステムの利用者数と利用頻度が増えるにつれて，利用者がパスワードを忘れた場合のパスワード初期化に要する期間を短縮してほしいという要望が，利用責任者からヘルプデスクに多く寄せられるようになった。パスワード初期化の申請から完了までの期間に利用者がNシステムを利用できないことで，契約企業によっては業務に悪影響が発生していることが背景にあった。

販売部では，Nシステムの利便性向上を目的として，利用責任者とヘルプデスクを介さずに，利用者自身がパスワード初期化を短時間で行えるパスワード初期化機能をNシステムに追加することを決定した。

販売部のH部長は，新人のF君に対して，G主任の支援を受け，パスワード初期化機能を設計するように指示した。また，H部長は，アプリケーションへの不用意な機能追加が原因で，セキュリティ上の問題が発生する事例が一般的に少なくないことを挙げ，現状のNシステムの仕様を十分に理解した上で検討を進め，社内の有識者によるレビューを受けるようF君とG主任に伝えた。

〔パスワード初期化機能の設計〕

F君は，図1に示すセキュリティ要件に従って，Nシステムのパスワード初期化機能を検討した。F君が作成した設計案を，図4に示す。

- Nシステムにパスワード初期化の申請ページを準備する。Nシステムのログイン画面に，申請ページへのリンクを設定する。
  次の(i)～(v)に示す手順に従って，仮パスワードを発行する。
  (i) 利用者は，申請ページにブラウザでアクセスし，自身のUID名を入力する。
  (ii) 入力されたUID名が存在する場合は，プログラムがパスワード取得ページのURL（以下，取得ページURLという）を発行し，利用者にメールで通知する。取得ページURLには十分に長いランダムな文字列を含める。入力されたUID名が存在しない場合は，取得ページURLは発行されない。
  (iii) 利用者が，メールで通知された取得ページURLにブラウザでアクセスすると，プログラムが仮パスワードを発行し，ブラウザに表示する。このとき，UIDの各属性に対して，表2の設定変更(b)に示す値を設定する。
  (iv) パスワード初期化の完了通知メールを，利用者に送付する。完了通知メールには仮パスワードは記載しない。
  (v) 一度アクセスされた取得ページURLは無効にする。また，取得ページURLを発行後，10分以内にアクセスがない場合は，取得ページURLを無効にする。
- 利用者のブラウザと，申請ページ及びパスワード取得ページとの間の通信には，SSLを用いる。
- 発行する仮パスワードは，図1のセキュリティ要件を満たし，ヘルプデスク担当者でも推測できない文字列とする。

図4　パスワード初期化機能の設計案

G主任はF君の設計案に対して，次の点を指摘した。

指摘1：この設計案では，ある状態のUIDに対してパスワード初期化を行った場合に，図1に示すセキュリティ要件が満たされなくなる。

F君はG主任の支援を受け，指摘1の問題点に対して図4の設計案を修正した。その後，社内の有識者による設計案のレビューが実施された。そのレビューでは，指摘1とは別に，次の2点が指摘された。

指摘2：今回設計したパスワード初期化機能によって仮パスワードを発行した場合に

は，図1のセキュリティ要件のうち，(エ) に記されているログイン処理中の強制的なパスワード変更ページへの遷移は不要ではないか。

指摘3：現行のヘルプデスクによるパスワード初期化運用と比較した場合に，図4の設計案に示す (i)～(v) の手順には，攻撃者に不正に仮パスワードを取得されるリスクがある。

指摘2については，販売部での検討の結果，今回の機能追加においては図1のセキュリティ要件を変更しないという判断に基づき，指摘対象となったログイン処理中の強制的なパスワード変更ページへの遷移は残すこととした。

指摘3については，今回予定していた開発予算を考慮すると，これ以上のセキュリティ強化は困難であると販売部では判断した。また，設計したパスワード初期化機能の利用を契約企業単位で選択できるようにした。その後，販売部では，F君の設計に基づいてパスワード初期化機能の開発に着手した。

設問1　表1中の［　a　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　AES　　イ　RC4　　ウ　RSA　　エ　SHA-256

設問2　図3中の［　b　］～［　e　］に入れる適切な字句を，表1中の属性名を用いて，［　b　］，［　d　］，［　e　］は15字以内で，［　c　］は30字以内で，それぞれ答えよ。

設問3　指摘1について，(1)，(2) に答えよ。

(1)　図1のセキュリティ要件がどのように満たされなくなるか。45字以内で具体的に述べよ。

(2)　上記 (1) の問題点の発生を防止するためには，パスワード初期化機能にどのような修正が必要か。表1中の属性名を用いて，35字以内で述べよ。

設問4　指摘2の内容が指摘された理由を，図2のヘルプデスクによる運用手順との違いを踏まえて，30字以内で述べよ。

設問5　指摘3について，攻撃者が不正に仮パスワードを取得する手口を45字以内で述べよ。