問1　安全なWebアプリケーションの開発に関する次の記述を読んで，設問1～5に答えよ。

X社は従業員数500名のソフトウェア会社で，10本程度の人事関連のソフトウェアパッケージ（以下，パッケージという）を開発，保守している。X社には，顧客から，パッケージを購入せず，利用料を払ってアプリケーションサービス（以下，サービスという）を受けられるようにしてもらえないかという問合せが増えている。また，競合他社の中には，そのようなサービスを提供するところも出てきている。このような状況を受けて，X社の経営陣は，パッケージに加え，サービスも商品ラインナップに加える方針を決定した。

X社は，手始めに，既存のパッケージではなく，新規の分野でサービスを提供することにした。具体的には，既存顧客から要望が出ていた，店舗で働くパートタイマやアルバイトの勤怠管理を行うシステム（以下，勤怠管理システムという）でサービスを提供することにした。また，システムの稼働率を高めるために，単一のシステムを複数の顧客で共用するマルチテナントのシステムとする方針を決定した。

一方，X社はこれまでイントラネット向けのパッケージ開発を専業としてきたので，インターネットに公開する安全なWebアプリケーションの開発ノウハウがなかった。X社の経営陣は，今後，サービス提供を拡大していくためには，安全なWebアプリケーション開発のノウハウ獲得が不可欠であると考えた。そこで，今回の開発プロジェクトを通じて，そのノウハウを身につけ，今後のほかの開発プロジェクトにも適用していくことにした。特に，今回のシステムはマルチテナントのシステムなので，顧客間でデータが漏えいしないよう，十分に検討して対策を行うことにした。

X社のシステム関連部署は四つあり，パッケージ開発部，システム技術部，システム運用部及びプロジェクト管理部である。パッケージ開発部はパッケージの開発・保守を行っている。システム技術部は，社内のネットワーク，サーバ，ミドルウェアなどのインフラ（以下，インフラという）の設計・構築を担当している。システム運用部は社内のインフラの運用を担当しており，セキュリティパッチ適用などの情報セキュリティ運用も行っている。プロジェクト管理部は，社内の開発プロジェクトを管理する部署である。

X社は勤怠管理システムの開発プロジェクトを立ち上げた。プロジェクト体制として，プロジェクトマネージヤをプロジェクト管理部のP課長が務め，その下に，開発チーム及びインフラチームが作られた。開発チームは，アプリケーションの設計・開発を担当し，開発の一部は複数の外部委託先に委託した。そして，開発チームのリーグはパッケージ開発部のBさんが務めることになった。また，アプリケーション開発のセキュリティ対策を支援するために，システム技術部からD課長とF主任が開発チームに参加することになった。インフラチームは，システム技術部のメンバで構成され，インフラの設計・構築及び本番稼働までの保守・運用を担当し，インフラチームのリーグはシステム技術部のEさんが務めることになった。本番稼働後は，勤怠管理システムの運用をシステム運用部に引き継ぐことになっている。

〔勤怠管理システムの概要〕

勤怠管理システムは，店舗ごとの従業員情報（氏名，従業員番号など）の管理機能，勤務予定の作成及び勤務実績の記録と参照のための機能，並びに給与システムへの勤怠データ出力機能をもつ。勤怠データは店舗ごとに管理される。また，複数店舗の情報を集約する機能があり，システムを利用する1顧客当たり50店舗まで管理すること

ができる。

〔勤怠管理システムのネットワーク構成〕

勤怠管理システムのネットワーク構成を図1に，ファイアウォール（以下，FWという）のアクセス制御ルールを表に示す。 Webサーバ上ではミドルウェアとアプリケーションが稼働する。

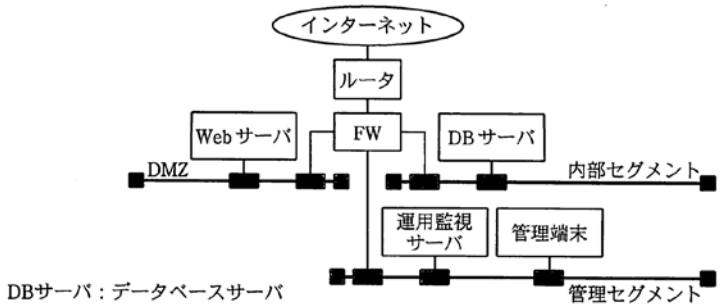

図1　勤怠管理システムのネットワーク構成

表　FWのアクセス制御ルール

項番	プロトコル	送信元	あて先	あて先ポート番号	動作
1	TCP	インターネット	Webサーバ	80，443	許可
2	TCP	Webサーバ	DBサーバ	DB(1)	許可
3	すべて	管理セグメント	Webサーバ	すべて	許可
4	すべて	管理セグメント	DBサーバ	すべて	許可
5	すべて	すべて	すべて	すべて	拒否

注(1)　“DB”は，データベースアクセスに必要なポート番号である。

注　項番の昇順に，最初に一致したルールが適用される。

〔プロジェクト計画の策定〕

本開発プロジェクトの開始に当たって，F主任はP課長から提示されたプロジェクト計画書を確認した。

図2は，プロジェクト計画書中で示された，開発プロジェクトのスケジュール概要(開発チームの関連部分を抜粋)である。要件定義には，セキュリティ要件の定義も含まれている。また，システムテスト期間の後半で本番稼働前に，ルータ，FW，各サーバ及びWebアプリケーションの脆弱性テストを外部の専門家に依頼する計画となっていた。

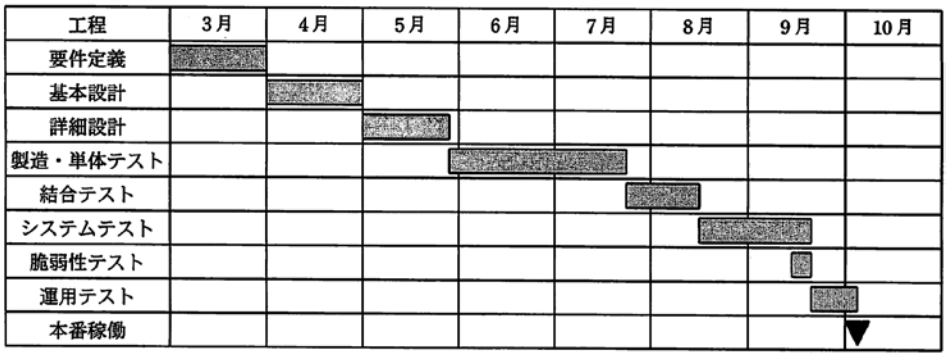

図2　開発プロジェクトのスケジュール概要（抜粋）

F 主任は，①本番稼働直前の脆弱性テストだけで安全な Web アプリケーションを開発しようとする計画には　プロジェクトマネジメント上，問題があると考え，P 課長に計画の変更を提案した。P 課長は，F 主任の提案を受けて，②レビューを設計工程（基本設計ー詳細設計）及び製造・単体テスト工程に追加する形で計画を変更した。

なお，外部委託先については，X 社から開発ガイドライン準拠チェックリスト（以下，チェックリストという）を提供し，外部委託先からは工程ごとにチェック結果を提出してもらうことにした。

〔コーディングルールの作成〕

次に，F 主任が本開発プロジェクトでのガイドラインを確認したところ，開発チームでは X 社の標準である開発ガイドラインを適用する計画となっていた。X 社では開発ガイドラインを制定し，各パッケージの開発・保守に適用している。図 3 は開発ガイドラインの SQL 処理に関する記載の抜粋である。

```
〔SQL 処理〕
　SQL 文の組立てには，プレースホルダ及びバインド機構を使用すること
```

図 3　開発ガイドラインの SQL 処理に関する記載（抜粋）

F 主任は，基本設計に先立って，開発ガイドラインを基に，開発言語として使用する Java の具体的なコーディングルールも作成した。図 4 は，F 主任の作成したコーディングルールのうち SQL 処理に関する記載の抜粋である。

```
〔SQL 処理〕
1. SQL 文の組立てには，プレースホルダ及びバインド機構を使用すること
（サンプル）
 String param = "suzuki"; //検索クエリの入力値
 // SELECT * FROM atable WHERE name="suzuki"; を実行する。
 java.sql.Connection con = java.sql.DriverManager.getConnection(url, userName, password);
 String sql = "SELECT * FROM atable WHERE name=?";
   a
 stmt.setString(1, param);
   b
```

図 4　コーディングルールのうち SQL 処理に関する記載（抜粋）

F 主任は，コーディングルールを作成後，プロジェクトメンバが参照できるようにファイルサーバに配置した。その後，開発プロジェクトは基本設計に入り，勤怠管理システムの設計が開発チームを中心に進められた。

〔勤怠管理システムのデータベース構成〕

勤怠管理システムはマルチテナントのシステムなので，一つのシステムの中で複数の顧客のデータを扱うが，顧客間でデータは分離する。顧客間でデータを分離する方法として，開発チームは，③データベースの各テーブルで，顧客を識別するカラムを追加する方式を採用した。具体的には，顧客単位で区別するために，顧客 ID を各テーブルに入れることにした。詳細設計におけるデータベース論理設計結果のうち，主な

テーブルの概要を図5に，そのE-R図を図6に示す。

テーブル名：顧客テーブル

列名	データ型	内容	備考
CUST_ID	文字列	顧客ID	（省略）
CUST_NAME	文字列	顧客名	（省略）
⋮	⋮	⋮	⋮

テーブル名：従業員テーブル

列名	データ型	内容	備考
CUST_ID	文字列	顧客ID	（省略）
USR_ID	文字列	利用者ID	（省略）
STORE_ID	文字列	店舗ID	（省略）
PASSWORD	文字列	パスワード	ハッシュ値
⋮	⋮	⋮	⋮

テーブル名：店舗テーブル

列名	データ型	内容	備考
CUST_ID	文字列	顧客ID	（省略）
STORE_ID	文字列	店舗ID	（省略）
STORE_NAME	文字列	店舗名	（省略）
⋮	⋮	⋮	⋮

テーブル名：勤務実績テーブル

列名	データ型	内容	備考
CUST_ID	文字列	顧客ID	（省略）
USR_ID	文字列	利用者ID	（省略）
K_DATE	日付	日付	（省略）
START_TIME	時刻	開始時刻	（省略）
END_TIME	時刻	終了時刻	（省略）
⋮	⋮	⋮	⋮

注　下線は主キーを表す。

図5　主なテーブルの概要

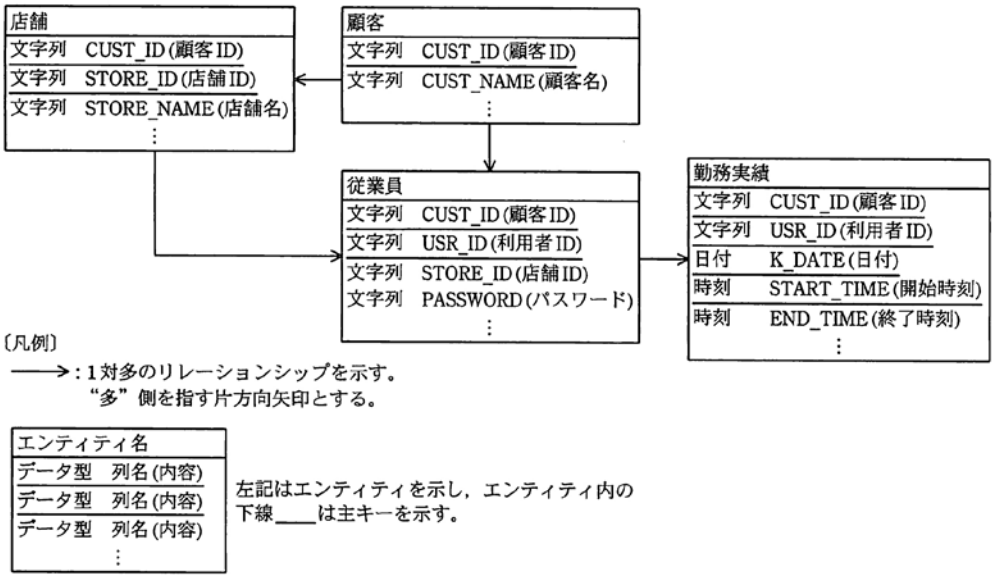

図6　主なテーブルのE-R図

〔アプリケーション設計のレビュー〕

詳細設計工程に進んだところで，社内メンバにセキュリティの観点でのレビュー経験がないことから，社内でのレビューではセキュリティ上の設計ミスやプログラム中の脆弱性を発見しきれないのではないかとB さんは考えた。そこで，セキュリティコンサルティング会社のH 社の支援を受けることを提案し，承認された。H 社は，アプリケーションセキュリティの専門家であるG さんを担当者としてアサインした。

詳細設計終了後，G さんは，B さん，F 主任とともに詳細設計結果に対するレビューを行ったところ，勤務実績表示の処理に問題があることを発見した。問題があった勤務実績表示の処理を図7 に示す。従業員選択画面には，ログイン中の利用者が所属している店舗の全従業員がリストに表示される。従業員をリストから選択すると，選択された従業員の勤務実績が勤務実績表示画面に表示される処理となっている。図7 の勤務実績表示のSQL 文は，図中の勤務実績表示画面を表示するためのSQL 文で。

【選択した従業員の利用者ID】には，従業員選択画面のリストで選択した従業員の利用者!D が指定される。

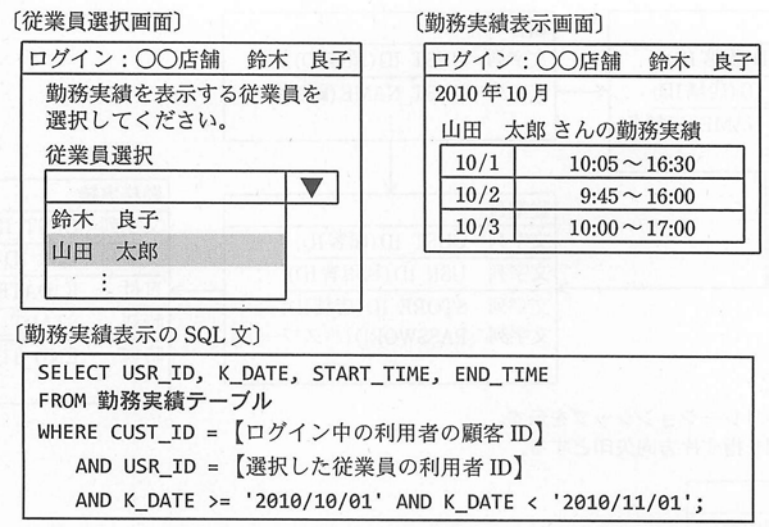

図7　問題があった勤務実績表示の処理

G さん：勤務実績表示画面では，他人の勤務実績を参照することができますね。

F 主任：はい，この機能では，同じ店舗に所属しているほかの従業員の勤務実績が参照できるようになっています。

G さん：同じ店舗だけならばよいのですが，このままではほかの店舗の従業員の勤務実績も参照することができます。具体的には，従業員選択画面のリストから従業員を選択して表示する処理に問題があります。

F 主任：リストには，店舗に所属している従業員の一覧を表示し，HTML の OPTION タグの VALUE 属性には，選択した従業員の利用者ID を指定するようになっています。従業員の一覧では，ログイン中の利用者と同じ店舗に所属している従業員だけが表示されますので，ほかの店舗の従業員を選択することはできないのではないでしょうか。

G さん：いいえ，可能です。選択された従業員の勤務実績を表示する処理では，VALUE 属性として送信されてきた利用者ID に対し，データの型をチェックした後，図7 中のSQL 文にそのまま使用する設計なので，これでは④ほかの

店舗の従業員の勤務実績を権限なく閲覧される可能性があります。

F 主任：なるほど。分かりました。早速，対策を検討して対応します。

F 主任は G さんのアドバイスを基に対策を考え，同様の問題がほかにないかどうかの確認も含めて，B さんを通して対策を開発チームに依頼した。

〔SQL インジェクション脆弱性の発見と対策〕

製造・単体テスト，結合テストが終了し，システムテストに入った。一方，F 主任はプロジェクト計画に基づき，外部の専門家による脆弱性テストを実施した。

脆弱性テストの結果，ある処理で SQL インジェクション脆弱性の作り込みが発見された。開発チームリーダの B さんに確認したところ，開発プロジェクトの途中で，外部委託先 Z 社に新規に開発を委託しており，その開発部分で発見されたことが分かった。

Z 社から提出を受けていたチェック結果には“コーディングルールに適合”と記入されていたので，F 主任は Z 社に事実関係を確認した。Z 社は，X 社のコーディングルールの内容は十分に理解していたが，コーディングルール違反をレビューで見逃したままチェック結果を X 社に提出していたと回答した。F 主任は B さんに報告した。B さんは，Z 社の開発部分全体についてコーディングルールの遵守を確認するよう，開発チームに指示した。

〔ミドルウェアの脆弱性〕

システムテストが終了し，システム運用部が加わり勤怠管理システムをインターネットに接続して運用テストを進めていた。本番稼働の 2 日前に，システム運用部のメンバがインターネットのニュースサイトを見ていたところ，勤怠管理システムで使用しているミドルウェアにおける脆弱性が 1 か月前に公表されていることを，偶然見つけた。

X 社のこれまでのパッケージ開発では，テスト期間中にミドルウェアのバージョンを見直すことはなかった。システム運用部は，インフラチームのリーダである E さんに相談した。E さんはベンダが発表している脆弱性情報と勤怠管理システムのミドルウェアのバージョンを確認し，その内容と影響を報告書にまとめた。図 8 は E さんのまとめた報告書である。

○概要
9月1日に，勤怠管理システムで使用しているミドルウェアにおける脆弱性情報及びセキュリティパッチが公表された。
○脆弱性の内容
ミドルウェアには管理画面があり，TCP ポート番号 8080 で利用できるようになっている。ネットワーク経由でこの管理画面にアクセスすることによって，ログインしなくても DoS 攻撃が可能である。ただし，ベンダはどのようなパケットで DoS 攻撃が可能か公表しておらず，ベンダのその後の報告では，10 月 1 日現在，脆弱性による不正な動作を再現する［ c ］は公開されていない。また，任意のコード実行が可能となる脆弱性ではない。
○影響
勤怠管理システムで使用しているミドルウェアは，この脆弱性の影響を受けるバージョンである。ただし，セキュリティ対策として，当初から次の対策を実施していたので，インターネットから直接に攻撃を受けるわけではない。
実施済対策：［ d ］
○根本対策
ベンダからのセキュリティパッチを適用すること。ミドルウェアのセキュリティパッチ適用時の動作検証には3日掛かる。
○監視方法
IDS（侵入検知システム）を導入していないが，現在公開されている情報によれば，この脆弱性が悪用された場合には，勤怠管理システムにおいてサービス停止や性能低下が発生するので，通常のサービス稼働監視によって検知することができる。

図8　Eさんのまとめた報告書

X社内で，関係者で検討した結果，Eさんのまとめた報告書にある脆弱性の内容及び影響に変化がなければ，サービスの本番移行は予定どおり実施するとの判断をした。また，根本対策として，次回の定期メンテナンスでセキュリティパッチを適用することにした。

その後，本番稼働までの2日間，脆弱性情報の更新を確認したが，特に更新はなかった。また，サービス稼働監視でも異常は発見されず，無事，本番稼働を迎えた。

〔本番稼働後の報告〕

本番稼働後，D課長はプロジェクト管理部に対して，今回の開発プロジェクトで発生したセキュリティ上の問題点と対応について報告を行った。プロジェクト管理部は，SQL インジェクション脆弱性の作り込みを踏まえた⑤開発委託先管理の問題点と，開発プロジェクトにおける本番稼働前のシステムに対する⑥脆弱性情報の管理の問題点を指摘し，今回の開発プロジェクトで得られた経験を，今後のシステムの開発，運用，保守に生かすため，D課長に具体的な解決策の提案を依頼した。

D課長はP課長，Bさん，F主任にも解決策の検討を依頼し，検討結果を取りまとめ，プロジェクト管理部に提案を行った。X社の経営陣は提案を承認し，X社のプロセスとしてシステムの開発，運用，保守に適用することにした。

設問1　〔コーディングルールの作成〕について，図4中の［ a ］，［ b ］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　`java.sql.PreparedStatement stmt＝con.prepareStatement(sql);`
イ　`java.sql.ResultSet rs ＝stmt.executeQuery();`
ウ　`java.sql.ResultSet rs ＝stmt.executeQuery(sql);`

エ　`java.sql1.Statement stmt＝con.bind(sql1);`
オ　`java.sql1.Statement stmt＝con.doFilter(sql1);`

設問 2　〔プロジェクト計画の策定〕について，(1)〜(3)に答えよ。

(1)本文中の下線①で F 主任が，問題があると指摘した理由を，35 字以内で述べよ。

(2)本文中の下線②で P 課長は，設計工程(基本設計，詳細設計)にレビューを追加した。その内容を，40 字以内で具体的に述べよ。

(3)本文中の下線②で P 課長は，製造・単体テスト工程にレビューを追加した。その内容を，50 字以内で具体的に述べよ。

設問 3　〔アプリケーション設計のレビュー〕で発見された，勤務実績表示の処理の問題について，(1)，(2)に答えよ。

(1)本文中の下線④の指摘は，具体的にどのような HTTP リクエストによって閲覧されると指摘したものか。 55 字以内で述べよ。

(2)この問題を避けるためには，データの型をチェックした後，どのようなチェック処理を行うべきか。60 字以内で述べよ。

設問 4　SQL インジェクション脆弱性の対策について，(1)，(2)に答えよ。

(1)SQL インジェクションが発生したときでも，ほかの顧客のデータを SQL で操作されにくいようにするためには，本文中の下線③の方式をどのように変更すべきか。 45 字以内で述べよ。

(2)本文中の下線⑤の開発委託先管理の問題点を解決するために，X 社が行うべきことを 50 字以内で述べよ。

設問 5　ミドルウェアの脆弱性発見時の対応について，(1)〜(3)に答えよ。

(1)図 8 中の [c] 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　エクスプロイトコード　　イ　セキュリティパッチ
ウ　セキュリティポリシ　　エ　ゼロデイ攻撃手法
オ　バッファオーバフロー

(2)図 8 中の [d] に入れる適切な実施済対策の内容を，50 字以内で述べよ。

(3)本文中の下線⑥の問題点に対する解決策を，今後の開発プロジェクトの在り方の観点から，40 字以内で述べよ。

問 2　社内認証システムの統合に関する次の記述を読んで，設問 1〜5 に答えよ。

A 社は，従業員数 700 名の業務用ソフトウェアパッケージの開発販売会社である。都心に本社を構える A 社は，営業部，人事部，経理部，総務部，情報システム部，製品サポート部，製品開発部及び研究部から構成されている。

A 社は，長らくソフトウェアパッケージの販売を事業の中心としてきたが，最近刷新された経営陣の決定によって，SaaS（Software as a Service）型のインターネットサービスの提供及び関連 SI 事業（以下，SaaS 型サービス事業という）を立ち上げる計画を開始した。

〔A 社の情報システム〕

A 社における社内向けの情報システムは，表に示すように分類される。このうち，社内の情報技術基盤となる情報システム群（以下，インフラ系という）及び基幹業務に関する情報システム群（以下，基幹業務系という）は，情報システム部の所管である。インフラ系には，Web アプリケーション（以下，Web アプリという）向けに A 社が独自に開発したシングルサインオン（以下，A-SSO という）システムが含まれている。他方，製品サポート部，製品開発部及び研究部が，部署ごとに導入して運用管理をしている情報システム群（以下，部署運用系という）があり，それらの一部は，認証に A-SSO システムを採用している Web アプリ（以下，A-Web アプリという）である。

表　A 社における社内向けの情報システムの分類

分類	所管部門	含まれるシステム名	備考
インフラ系	情報システム部	プロキシ，電子メール，A-SSO，NTP（Network Time Protocol）など	・インフラ系のサーバマシン群のベンダサポートは 2012 年末に終了する(1)。 ・電子メールは UNIX OS 上で稼働
基幹業務系	情報システム部	財務会計，勤怠管理，人事管理，施設予約，経費精算など	勤怠管理と施設予約は A-SSO システムで認証
部署運用系	製品サポート部	顧客管理，製品管理など	顧客管理と製品管理は A-SSO システムで認証
	製品開発部	グループウェア，e ラーニングなど	グループウェアと e ラーニングは A-SSO システムで認証
	研究部	研究サーバ，ナレッジベースなど	・研究サーバは UNIX OS 上で稼働 ・ナレッジベースは A-SSO システムで認証

注(1)　A 社では，ベンダのサポートが終了する前に，情報システムをリプレースすることになっている。

〔認証統合プロジェクトの発足〕

A 社では，社内に A-SSO システムを含む複数の認証システムが混在しており，システム監査において，図 1 に示す課題が指摘されていた。ここで，認証システムとは，アカウント情報の管理，利用者の認証及びアクセス許可を行うシステムのことをいう。

(1)　情報システム全体では 3 種類の利用者 ID が使用されており，使い分けが面倒との利用者の声が多くある。
(2)　情報システムごとにパスワードルールが異なるので，同じレベルのパスワードの強度が確保されていない。
(3)　認証システムを管理する部署が複数に分かれているので，アカウントの運用及び認証システムの運用管理に関しても，同じレベルのセキュリティが確保されていない。
(4)　アカウント情報を管理するディレクトリ間の反映が一部手動で行われており，過去，アカウント情報を誤って削除するなどのトラブルが発生した。これに対する防止対策が必要である。
(5)　緊急に対処すべき課題とまでは言えないが，セキュリティ管理の現状を踏まえると，A-SSOシステムには脆弱性がある。

図 1　A 社の認証システムに関して指摘されていた課題

そこで，認証システムを統合することになり，情報システム部を中心とした社内プロジェクトチーム（以下，S チームという）が発足した。また，経営陣から，当該プロジェクトは，SaaS 型サービス事業に活用できる成果を出すようにという指示があった。この指示を考慮し，プロジェクトの開始に先立ち，認証システムの統合の基本方針を図 2 にまとめた。

(1) アカウント情報の一元化によって，認証の利便性を向上させる。
(2) 認証システムの運用コストを削減する。
(3) 新たに導入する認証システムは，将来にわたって継続的に利用できるものにする。
(4) 情報システムのセキュリティを向上させる。
(5) 認証システム自体のセキュリティを向上させる。
(6) 各部署が独自に情報システムを導入し，運用管理も独自に実施する方針を継続する。
(7) 上記(1)～(6)を妨げない程度で，SaaS 型サービス事業で用いる新技術を積極的に取り入れる。

図２　A 社の認証システムの統合の基本方針

〔認証システムの洗い出し〕

S チームは，A 社で利用している認証システムについて精査する必要があると判断し，まず，他社製の認証システムに関して，仕様を詳しく調査することにした。

A 社は，PC 端末，ファイルサーバ及び一部の Web アプリにおける認証の仕組み，並びにディレクトリとして，C 社製ディレクトリシステム（以下，C-DIR という）を，導入している。C-DIR では，利用者，PC 端末，プリンタ及びサーバから構成されるドメインという管理単位を定め，ドメインコントローラ(以下，DC という)によって管理する。また，DC では，C-DIR のディレクトリに保持されるアカウント情報を用いて認証を行う。認証には，C 社独自仕様のチャレンジレスポンス認証(以下，C-CR 認証という)，又は Kerberos 認証を利用することが可能である。

C-CR 認証では，図 3 に示すプロトコルの(b)-1～(b)-4 において，①DC が生成した疑似乱数をチャレンジとし，それを受信したクライアントで，利用者 ID，パスワード及びチャレンジの連結をハッジュ化したレスポンスを DC に返信し，アクセス許可を受ける。

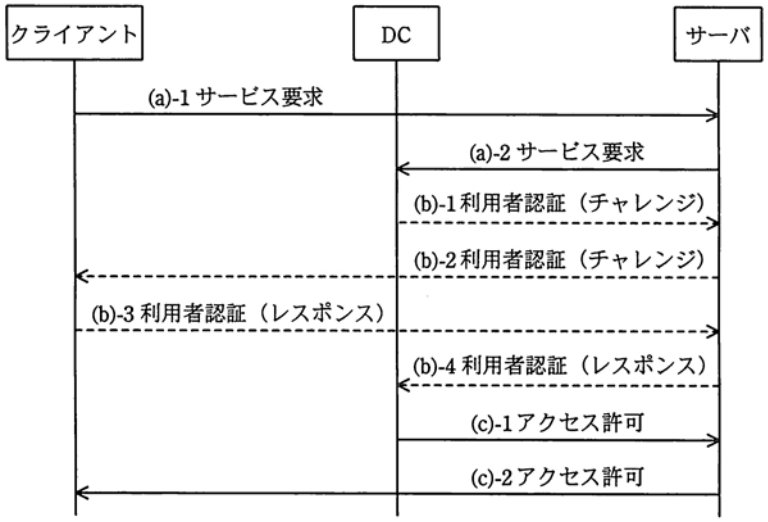

図３　C-CR 認証のプロトコル

他方，Kerberos 認証では，図 4 に示すように，クライアントが，DC における認証後，有効期限付のチケットが発行され，それをサーバに提示し，アクセス許可を受ける。

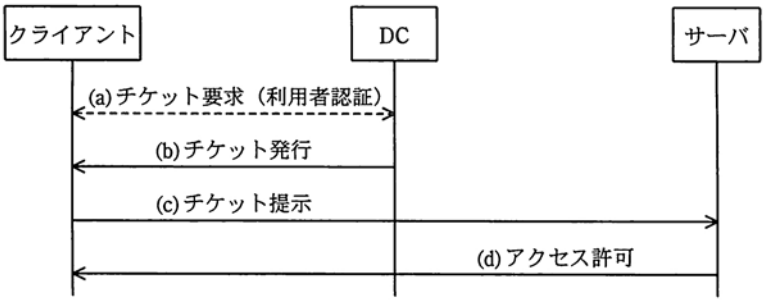

図４　Kerberos 認証のプロトコル

C-CR 認証の場合，クライアントはサーバへの接続のたびに DC において認証を行う必要があるが，Kerberos 認証の場合，有効期限内であればチケットをサーバに提示するだけでサービスを受けられる。A 社では，トラフィックが少なくなるなどのメリットが多い Kerberos 認証だけを利用している。また，Kerberos 認証において，②有効期限切れのチケットが悪用されないように，DC とサーバを［　a　］させて運用している。

研究サーバ用及び電子メール用のサーバマシンでは，UNIX OS が稼働しており，利用者認証のために，NIS（Network Information Service）が導入されている。ここで，NIS とは，NIS ドメインと呼ばれる管理単位において，UNIX OS が稼働するマシン間で，利用者のアカウント情報を共有するための仕組みである。

社外から社内 LAN へのアクセスのための SSL-VPN での認証，及び社内の無線 LAN での認証には，RADIUS が使用されている。ここで，RADIUS とは，サーバにおいて，利用者の認証及びアカウンティングを実現するための仕組みである。

以上の認証システム以外に，LDAP を用いて，パスワード認証を行う情報システムがある。

〔A-SSO システムの仕様の確認〕

S チームは，次に，A 社が独自に開発した A-SSO システムの仕様を確認した。

A-SSO システムは，A-SSO サーバ及び A-SSO 用のディレクトリで構成される。A-SSO サーバは，A-Web アプリの利用者を認証するために，A-SSO 用のディレクトリに保持されるアカウント情報を用いる。認証には，図 5 に示すプロトコルを利用する。

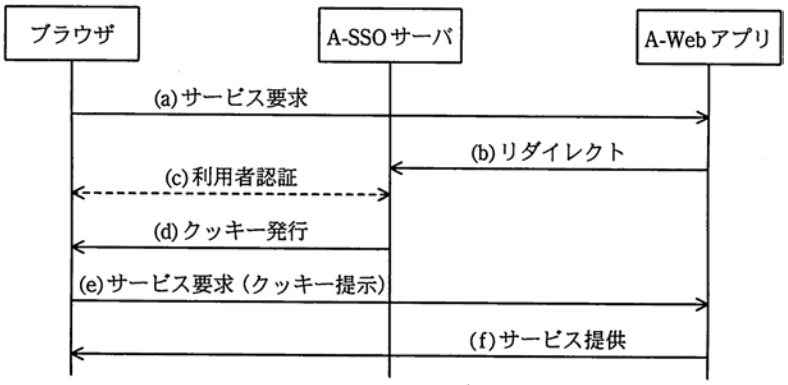

図５　A-SSO システムのプロトコル

次は，A-SSO システムのプロトコルの動作概要である。

（a）利用者のブラウザは，A-Web アプリにサービスを要求する際，A-SSO 用のクッキーがあれば，それを A-Web アプ引こ提示する。その場合には（f）に進む。

（b）A-Web アプリは，サービス要求を A-SSO サーバにリダイレクトする。

（c）利用者は，利用者 ID とパスワードを入力し，認証を受ける。

（d）A-SSO サーバは，認証が成功すれば A-SSO 用のクッキーを発行する。

（e）ブラウザは，クッキーを A-Web アプリに提示し，サービスを要求する。

（f）A-Web アプリは，クッキーを検証し，有効ならば，サービスを提供する。

ここで，A-SSO 用のクッキーには，セッション ID やクッキーの発行日時などが設定されており，トリプル DES を用いて暗号化されている。また，すべての A-Web アプリには，クッキーを復号するために暗号化鍵を配布している。ブラウザは，一度，クッキーの発行を受けると，有効期間内であれば，（b）～（e）の手続なしに，すべての A-Web アプリにアクセスできる。

〔A 社のアカウント情報の反映のフロー〕

A 社で利用している認証システムの仕様の確認後，S チームは，アカウント情報の反映のフローを確認した。

図 6 は，認証システム間で，アカウント情報をどのように反映しているかのフローを示している。まず，人事マスタデータベース（以下，人事マスタという）から CSV 形式のファイル（以下，人事マスタファイルという）を手動で，適時，出力しておく。アカウント作成の際，人事マスタファイルを基に，利用者 ID，パスワードなどのアカウント情報を，アカウント情報を管理する LDAP サーバのデータベース（以下，LDAP マスタという）に追加する。併せて，C-DIR のディレクトリにも追加する。さらに，LDAP マスタから，LDAP 1 には即時に，LDAP2 には日次で，データ転送される。ここで，LDAP1 は A-SSO サーバから参照され，LDAP2 はそれ以外の LDAP を利用する認証システムから参照される。NIS と RADIUS のアカウント情報については，利用者からの申請後，手入力で NIS に追加する。その後，RADIUS に，即時，データ転送される。

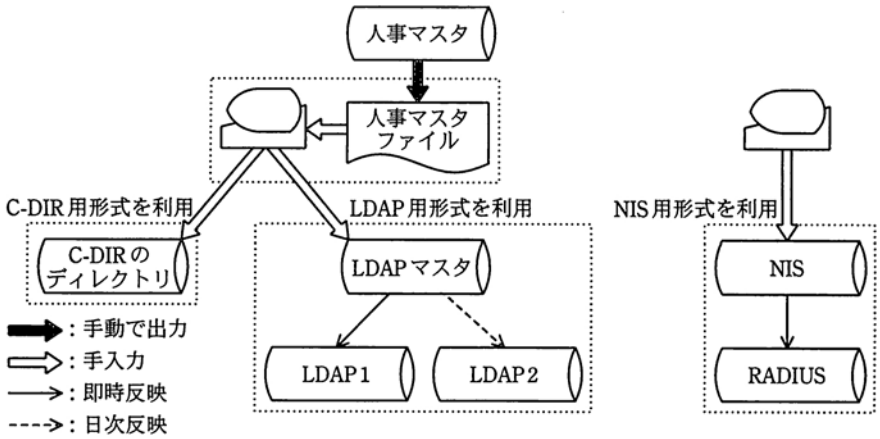

図 6　アカウント情報の反映のフロー

A 社では，アカウント情報に関して，C-DIR 用，LDAP 用及び NlS 用の 3 種類のデータ形式を用いている。 LDAP のアカウント情報では，inetOrgPerson といったオブジ

ェクトクラスによって組織の利用者の情報を管理する標準的な [b] を用いている。例えば，製品開発部のスズキタロウ氏が社内で利用する LDAP 用のアカウント情報を [c] によってテキスト形式で示すと，図 7 となる。

```
dn: uid=suzuki, ou=seihin-kaihatsu, dc=a-company, dc=com
cn: Taro Suzuki
sn: Suzuki
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
ou: 製品開発部
telephonenumber: 03-xxxx-5555
```

図 7　LDAP におけるスズキタロウ氏のアカウント情報（抜粋）

〔統合認証システムの基本設計〕

社内の認証システムの仕様を洗い出した後，S チームでは，図 8 に示すとおり，新たに導入する認証システム（以下，統合認証システムという）の基本設計を行った。

アカウント情報は，エントリの属性を定義する [b] を拡張して，A 社で必要とする利用者 ID，パスワード，所属，電話番号などの属性を管理できるようにした。また，統合認証システムではアカウント情報を一元的に管理することとした。

アカウント情報のシステム間の反映に関しては，人事マスタから ID 管理サーバ（以下，IDM という）にアカウント情報を日次で反映し，IDM のディレクトリ（以下，IDM マスタという）で保持し，変換後，IDM から C-DIR のディレクトリ及び LDAP にアカウント情報を即時反映する方式を採用した。 LDAP は，シングルサインオンシステム及び RADIUS での認証に利用される。NIS は DC と連携することができる。

利用者がパスワードを変更したい場合は，IDM の Web インタフェースを通して，利用者が自ら変更することが可能で，C-DIR 又は LDAP サーバなどに，即時反映される仕組みとした。

A-SSO システムには，図 1 の（5）の指摘があることに加え，③A-SSO 用のクッキーの利用が原因となり，A-SSO サーバと A-Web アプリが同じインターネットドメイン上にないとシングルサインオンを実現できないという技術的課題があった。社内ドメインだけでの運用では問題はないが，SaaS 型サービス事業を展開する上で，事業形態の制約となるので，製品開発部と研究部との検討の結果，統合認証システムでは，SAML（Security Assertion Markup Language）に準拠したシングルサインオン（以下，SAML 型 SSO という）システムを採用することにした。

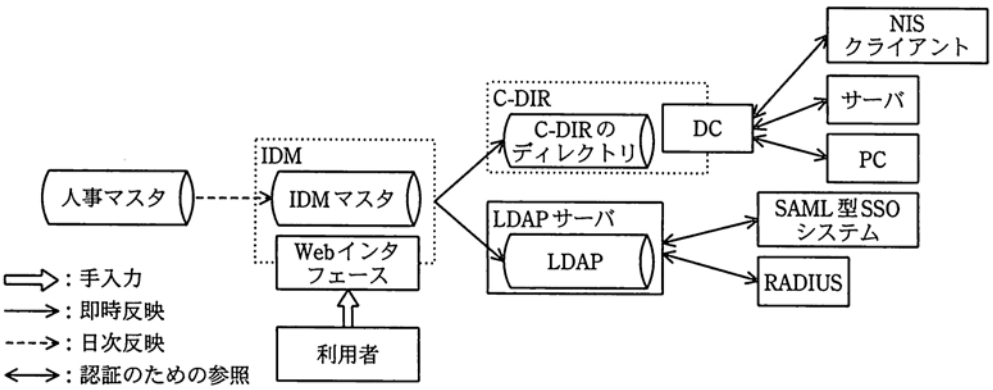

図 8　統合認証システムの基本設計概念

SAML とは，記述言語として [d] を用いて，認証及び [e] に関する情報を交換するための標準規格である。今回，A 社で採用した SAML 型 SSO システムにおける認証及び [e] を実現するプロトコルは，図 9 のとおりである。 Web アプリ上には，SP(サービスプロバイダ)と呼ばれるモジュールが稼働しており，IdP(ld プロバイダ)と呼ばれる Web アプリと連携して，利用者認証を行う。 IdP においては，様々な認証方式を採用できるが，A 社では，入力フォームを活用した，利用者 ID とパスワードを用いる方式を採用し，図 8 の統合認証システムにおける LDAP サーバと連携させることにした。

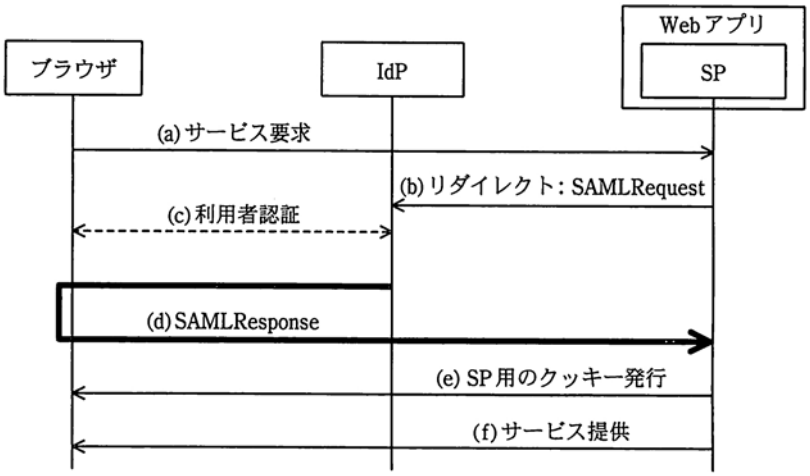

図 9　SAML 型 SSO システムのプロトコル

次は，A 社で採用した SAML 型 SSO システムのプロトコルの動作概要である。ここで，各主体は，ほかの主体の公開鍵証明書を保持しているとする。

(a)利用者のブラウザは，Web アプリにサービスを要求する際，SP 用のクッキーがあれば，それを提示する。提示したクッキーが有効であることが検証された場合は(f)に進む。

(b)SP は，SAMLRequest メッセージをエンコーディングした上で URI に含め，サービス要求を IdP にリダイレクトする。

(c)利用者は，利用者 ID とパスワードを入力し，認証を受ける。

(d)IdP は，利用者 ID などの属性を暗号化及びディジタル署名した SAMLResponse メッセージを発行し，ブラウザ上の JavaScript を用いて，それを SP に転送する。

(e)SP は，SAMLResponse メッセージのディジタル署名などを検証し，有効であれば，SP 用のクッキーを発行する。

(f)SP が稼働する Web アプリは，該当するサービスを提供する。

S チームは，SaaS 型サービス事業への展開を視野に入れ，SAML 型 SSO を複数の IdP でも適用できるように設計した。 SAML 型 SSO システムの導入によって A-SSO システムの課題に対処できるので，SAML 非対応の既存の Web アプリを，情報システムのリプレース時に，SAML に対応するように改修を行うことにした。将来的には，全社で SAML 型 SSO システムを採用することにし，統合認証システムの導入後，適切なタイミングで A-SSO システムを廃止することを決定した。

SaaS 型サービス事業への展開としては，A 社のソフトウェアパッケージを SP と連携するように改修し，Web アプリとして A 社のデータセンタに配備し，サービスを提供する予定である。このサービスを導入する企業は，自社のイントラネットに IdP を用意すれば，導入する企業のイントラネットにある PC 端末からインターネット経由で，A 社のデータセンタに配備された SaaS 型サービス事業の Web アプリを利用することが可能となる。導入する企業は，Web アプリの運用を A 社に委託できるので，自社内での運用に比べてコストの削減が期待できる一方で，④A 社にとっても，IdP を顧客のイントラネットに構築することは運用管理上のメリットがある。

〔移行計画の策定と実施〕

基本設計に続き，S チームは，図 10 のとおり，情報システムのリプレース及び認証システムの統合化計画案を策定した。

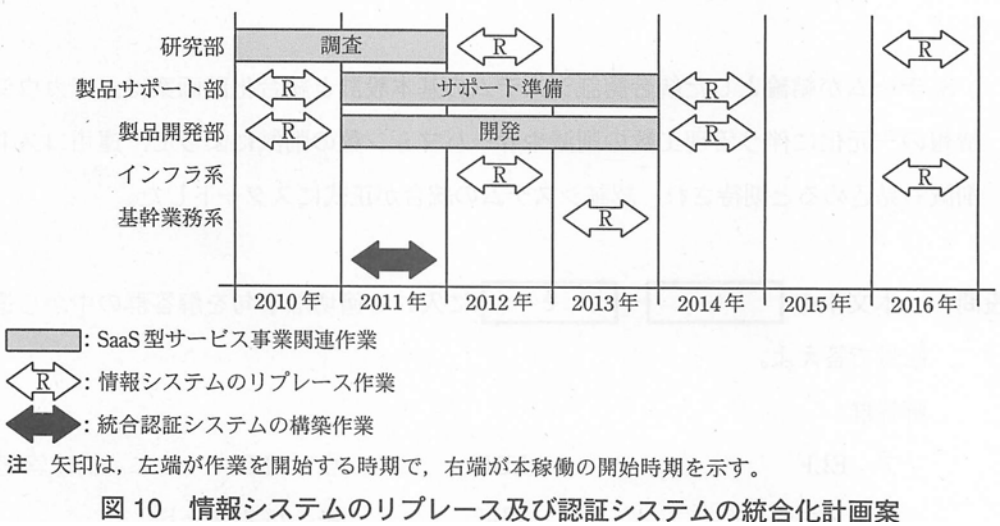

図 10　情報システムのリプレース及び認証システムの統合化計画案

A 社は，情報システムをリース契約で導入しており，4 年ごとにリプレースを実施している。2012 年にはインフラ系のリプレースが予定されており，2013 年には基幹業務系のリプレースが予定されている。いずれの作業も，情報システム部が行う。他方，部署運用系のリプレース作業については，所管部門がそれぞれ行うことになっており，現在，製品サポート部及び製品開発部所管の情報システムのリプレース作業を行っている。また，2012 年に，研究部所管の情報システムのリプレースを実施する予定である。

なお，A 社では，ハードウェアの故障などのトラブルの発生が増えるのを避けるため，リース契約の延長は行わない。

図 10 の計画案の策定では，このような前提の下，認証システムの統合のスケジュールを検討し，次の 3 点を決定した。

・SaaS 型サービス事業は最優先であり，さらに，引き続きソフトウェアパッケージの開発及びサポート業務もあるので，製品サポート部，製品開発部及び研究部所管の情報システムのリプレースの時期は変更しない。
・統合認証システムの構築作業を 2011 年に実施する。
・A-SSO システムのリプレースは，インフラ系のほかの情報システム群のリプレースとともに予定どおり行う。A-SSO システムの廃止が可能になるのは，早くても，［ f ］年の末である。それまでは，継続利用しようと考えたが，［ g ］

という理由から，次回のインフラ系のリプレース時に，A-SSO システムも，ほかのインフラ系の情報システム群と併せてリプレースしておく必要があると判断した。

S チームが結論とした統合認証システムの基本設計と統合化計画案は，アカウント情報の一元化に伴う管理工数の削減やサーバマシン数の削減によって，運用コストの削減も見込めると期待され，認証システムの統合が正式にスタートした。

設問 1　本文中の [b] ～ [e] 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　ELF　　イ　LDIF　　ウ　XML　　エ　構成管理
オ　スキーマ　　カ　認可　　キ　パスワード
ク　パスワードファイル

設問 2　C-DIR で用いられている認証について，(1)，(2)に答えよ。

(1)本文中の下線①の疑似乱数の生成方法に問題があり，同じ乱数が生成される場合，どのような脅威が考えられるか。攻撃の手順とともに，50 字以内で具体的に述べよ。

(2)本文中の下線②を実現するために，[a] に入れる適切な字句を 10 字以内で答えよ。

設問 3　シングルサインオンシステムについて，(1)，(2)に答えよ。

(1)図 1 中の(5)の脆弱性とは何か。セキュリティ管理の現状と A-SSO システムの仕様から判断して，45 字以内で述べよ。

(2)本文中の下線③の技術的課題に，SAML 型 SSO システムではどのように対処しているか。図 9 中の字句を用いて，70 字以内で具体的に述べよ。

設問 4　統合認証システムについて，(1)，(2)に答えよ。

(1)統合認証システムにおいて，図 1 中の(2)の指摘にどのように対処しているか。 60 字以内で述べよ。

(2)本文中の下線④にある A 社にとっての運用管理上のメリットとは何か。SAML 型 SSO システムの特徴に基づいて 60 字以内で述べよ。

設問 5　移行計画について，(1)，(2)に答えよ。ここで，リプレースされた情報システムは，本稼働後から利用可能とする。

(1)本文中の [f] に入れる適切な年を答えよ。また，S チームがそのように判断する理由を 40 字以内で具体的に述べよ。

(2)本文中の [g] に入れる適切な理由を 45 字以内で具体的に述べよ。

解答例

問 1

出題趣旨

クラウドコンピューティングの広がりによって，アプリケーションがサービスとして提供される機会が増えている。そのため，アプリケーション全体のセキュリティ対策をより適切に実施することが求められる。

本問では，アプリケーションサービスの開発プロジェクトを題材として，安全なシステムの開発に必要な開発工程，アプリケーション実装及び共同利用型のシステムにおけるデ

ータ分離の知識を問う。また，開発プロジェクトでの組織的な問題を解決する能力を問う。

設問1　a　ア
　　b　イ
設問2（1）修正に期間が掛かり，本番稼働が延期となる可能性があるから
（2）セキュリティ要件が正しく設計に反映されているかどうかをレビューする。
（3）開発ガイドライン及びコーディングルールに基づきコーディングされていることを確認する。
設問3（1）【選択した従業員の利用者 ID】を表すリクエストパラメタの値としてほかの店舗の利用者 ID を与える。
（2）【選択した従業員の利用者 ID】の値がログイン中の利用者と同じ店舗の従業員の利用者 ID かどうかをチェックする。
設問4（1）データベースのテーブルとアカウントを顧客ごとに分離し，アクセス権を設定する。
（2）・開発委託先の成果物に対して，委託先のレビューに加えて，X 社でも受入検査を詳細に実施する。
・チェックリストの各項目を判定する基準を示し，その判定結果と根拠を提出させる。
設問5（1）c　ア
（2）d　ファイアウォールで，インターネットからの TCP ポート番号 8080 への通信を拒否する。
（3）X 社の標準開発プロセスに脆弱性情報の収集と管理責任を規定する。

問2
出題趣旨
本問は，組織内の認証システムの統合を進める上で，情報システム部門が解決すべき課題を幅広く扱っている。
認証及び関連技術に関しては，旧来の技術から最新の技術までを対象にして出題した。認証システムを統合する上での，基本的な設計能力及び重要な課題の一つであるスケジューリングに関する能力を問う。旧認証システムである A-SSO システムを利用しているシステムが，新方式である統合認証システムに連携し終わるまで A-SSO システムを廃止できず，A-SSO のサービスを継続させなければならないということへの“気づき”を確認する。また，A-SSO のサービスを継続するための阻害要因を状況から見いだす能力に加えて，連携しているシステムのリプレース時期を見据え，A-SSO の廃止時期の判断を問う。

設問1　b　オ
　　c　イ
　　d　ウ
　　e　カ
設問2（1）チャレンジとレスポンスのペアを盗聴し，正規のレスポンスを用いてリプレイ攻撃によるなりすましをする。
（2）a　時刻同期
設問3（1）所管部門の異なる A-Web アプリのすべてに同一の暗号化鍵を配布していること
（2）暗号化及びディジタル署名した SAMLResponse メッセージを用いて，ldP から

SP へ認証情報を転送している。

設問 4（1）管理フォーマットを一つにし，工圓でパスワードを一元的に管理し，それを各情報システムが参照する仕組みを導入した。

（2）SaaS 型サービスのアカウント管理と運用を，必要に応じて，A 社から切り分けることが可能となる。

設問 5（1） f 2014

S チームが判断する理由 A-SSO システムと連携した情報システム群のリプレースがすべて完了するから

（2）g A-SSO システムが稼働するサーバマシンのベンダサポートが 2012 年末で切れる

採点講評

問 1

問 1 では，開発プロジェクトにおいて安全なシステム開発のために情報セキュリティスペシャリストが支援すべきテーマについて幅広く出題した。全体として正答率は想定どおりだった。

設問 2(1)は，プロジェクトマネジメント上の問題を問うたが，手戻りがあるとだけ解答したものが散見された。プロジェクトをセキュリティ面で支援するときには，納期やコストなどの問題を考慮して解答してほしかった。

設問 2(2)は，正答率が高かった。しかし，設計工程において求められる，セキュリティ要件の実現方法を設計するという観点が漏れている解答が散見された。脆弱性対策だけではなく，開発プロジェクトにおける工程ごとに行うべき作業を幅広く理解しておいてほしい。

設問 4(1)は，正答率が低かった。アクセス権の設定についての記述がない解答が散見された。 SQL インジェクションは知っているものの，データベースのアクセス権に関する知識が十分活用されていなかった結果と思われる。本設問では，問題文の状況の下でマルチテナントのシステムにおけるデータベースの分離方法をセキュリティ面から検討している。これをきっかけにデータベースのアクセス権について理解しておいてほしい。

問 2

問 2 では，組織内の認証システムの統合に関する技術及び統合におけるスケジューリングについて出題した。全体として正答率は想定どおりだった。

設問 2(1)は，正答率が低かった。チャレンジレスポンス認証は，ネットワークにおける認証の基本であるので，よく理解しておいてほしい。

設問 3(1)は，正答率が低かった。セキュリティレベルの異なる部門において同じ暗号化鍵を用いることが問題であることを，旧認証システムである A-SSO システムの設計及び問題文中の状況設定から理解してほしかった。

設問 3(2)は，正答率が低かった。 SAML ではドメインをまたいだ Web アプリケーションの認証に SAMLResponse メッセージを用いていることに加えて, SAMLResponse メッセージでは，暗号化とディジタル署名を用いて，セキュリティを確保していることを理解しておいてほしい。