問1　Web アプリケーションシステムの脆弱性対策に関する次の記述を読んで，設問1～3に答えよ。

A社は従業員数500名の卸売会社で，メーカから事務用品を仕入れ，小売店向けに販売している。A社の情報システム部は，企画開発課と運用課で構成されている。企画開発課は受発注にかかる時間と経費を削減するために，商品の受発注処理を電子化したXシステムを3年前に自社開発し，運用課がXシステムの運用を担当している。

〔Xシステムの概要〕

図1にXシステムの構成を示す。Xシステムの利用者は，メーカの受注担当者，小売店の発注担当者及びA社の受発注担当者で，インターネットからアクセスし，事務用品の受発注を行う。ログインの際は，利用者IDとパスワードを入力する。入力されたパスワードからはそのハッシュ値（以下，パスワードハッシュという）が算出される。利用者の認証は，利用者IDとパスワードハッシュを，それぞれ表1の利用者テーブル（以下，利用者TBLという）のUSR_D，PASSWORDと照合して行われる。利用者に実行が許可されている機能は，利用者IDごとに定義されており，［　a　］制御されている。

なお，Xシステムの各サーバのOSはUNIX，通信プロトコルはHTTP over SSLである。

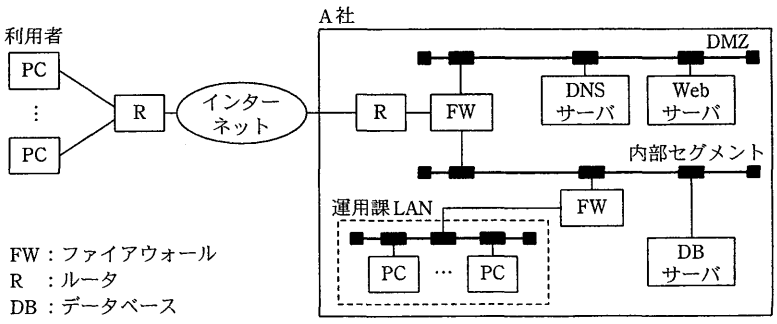

図1　Xシステムの構成

表1　利用者TBLの仕様

テーブル名：M_USER

列名	データ型（バイト数）	内容	備考
USR_ID	CHAR（12）	利用者ID	主キー
PASSWORD	CHAR（32）	パスワードハッシュ	
USR_NM	VARCHAR（40）	利用者氏名	
USR_ADDR	VARCHAR（60）	メールアドレス	
COM_ID	CHAR（8）	会社ID	業種区分＋連番で構成
⋮	⋮	⋮	⋮

〔インシデント発覚〕

休日明けの2007年10月15日（月），Xシステムの多数の利用者から，これまで利

用できていたパスワードでログインできなくなったという苦情が利用者問合せ窓口に殺到した。運用課の窓口担当者であるD君は重大なトラブルの可能性を考慮し，運用課のC課長に状況を報告した。その後，C課長は企画開発課のF課長に原因の調査と対策の検討を依頼した。F課長は，部下のE君に調査を命じた。E君はまず，認証情報が格納されている利用者TBLに異常がないかどうかを調査した。

次は，E君がF課長に調査結果を報告した際の会話である。

E君　：それでは今回の調査結果を報告します。結論から申しますと，利用者TBLのすべての行のPASSWORDが，同じ値に変更されていました。これは推測ですが，インターネットからの不正アクセスか，運用担当者によるSQLコマンドの発行ミスが原因だと思われます。念のため，C課長に問い合わせたところ，ここ数日間は利用者TBLを変更するような処理を実施していないとのことでした。一方，管理者の認証情報は，利用者TBLではなく別のテーブルに格納されていたので，管理者機能は現在でも利用できます。

F課長：君の推測はログから確認できるのかな。

E君　：いいえ。DBサーバのアクセスログ（以下，DBログという）が収集されていないので確認はできません。さらに，運用担当者であればC課長の許可なく利用者TBLを含むすべてのDBにアクセスできる状況であることと，DBにログインするためのDBMSの利用者ID（以下，DBアカウントという）を運用課の4名の担当者で共用していることも分かりました。これらの運用状況は改善する必要がありますね。

F課長：そのとおりだ。しかし，DBログを収集していなくても，DBのトランザクションログ（以下，TRNログという）を調べれば，更新時刻やどのDBアカウントによる更新なのかが分かるはずだ。

E君　：当社にはTRNログを本格的に解析できる者がいません。

F課長：そうか。では，TRNログの解析や，不正アクセスの可能性についての調査を，セキュリティ専門会社に依頼することにしよう。

F課長は，セキュリティ専門会社のB社に調査を依頼した。B社ではG氏をリーダとして調査することにした。

〔調査前のB社によるXシステムの概要確認〕

本格的な調査を開始する前に，F課長とG氏によって，図1～3，表1，2などの資料を使って，Xシステムの概要確認が行われた。次は，そのときの会話である。

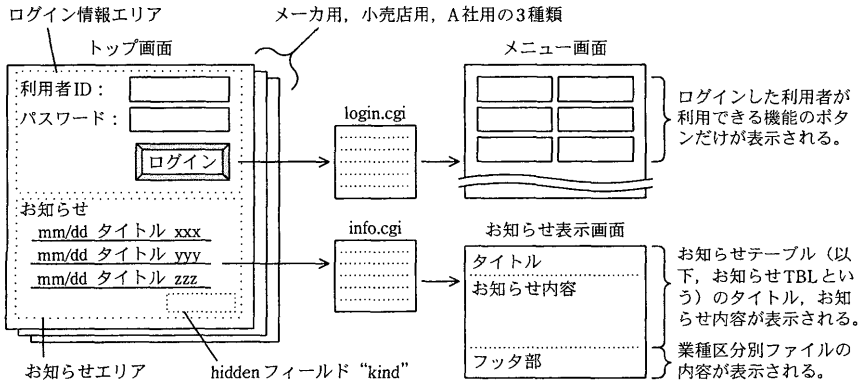

図２　Ｘシステムの入出力画面イメージ（抜粋）

F 課長：まず，X システムの入出力画面について説明します。トップ画面は，メーカ用，小売店用，A 社用の業種区分別に 3 種類あり，それぞれ別々の URL で閲覧するようにしてあります。しかし，それらのトップ画面から呼び出される CGI プログラム login．cgi，info．cgi は共通です。

G 氏　：お知らせ表示の機能（以下，お知らせ機能という）は，ログインしていなくても利用できるようにしているのですね。

F 課長：はい。年に数回実施する DB のメンテナンスやそのほかの作業で，X システムにログインできないときに，利用者に通知する必要があるからです。

G 氏　：なるほど。それから，お知らせ表示画面では，タイトルとお知らせ内容はお知らせ TBL から取得し，フッタ部は業種区分別ファイルの内容を表示しているのですね。

表２　お知らせ TBL の仕様

テーブル名：M_NEWS

列名	データ型（バイト数）	内容	備考
NWS_ID	CHAR（4）	お知らせ ID	主キー
NWS_NM	VARCHAR（100）	タイトル	
NWS_BODY	VARCHAR（4,000）	お知らせ内容	
⋮	⋮	⋮	⋮

F 課長：はい。そのために，それぞれのトップ画面のお知らせエリアの hidden フィールド“kind”（以下，kind という）には，業種区分を表す文字列がセットされており，お知らせ機能は，ログインしていなくても利用者の業種区分を識別できます。

（中略）

G 氏　：利用している DBMS に対して特殊な設定をしていませんか。

F 課長：標準の DBMS 初期設定値のままで，特殊な設定はしていません。

DBMS仕様

・DB管理テーブル（以下，DB管理TBLという）の仕様
0）共通事項
・DB管理TBLは，DBMSによって管理され，管理対象の属性が変更された場合は自動的に更新される。
・DB管理TBLに対するアクセス権限は，DBアカウント別に付与，削除が可能である。
1）DBアカウント情報管理テーブル（テーブル名はADMIN_ALL_USERS）
・DBMS内のすべてのDBアカウントのアカウント名（USER_NAME），パスワード文字列のハッシュ値（USER_PASSWORD）などのDBアカウント情報が管理されている。
2）テーブル情報管理テーブル（テーブル名はADMIN_ALL_TABLES）
・DBMS内のすべてのテーブルのテーブル名（TABLE_NAME），スキーマ（SCHEMA）などのテーブル情報が管理されている。

図3　Xシステムで利用しているDBMSの仕様（抜粋）

G氏：DBサーバにアクセスできるのは，Webサーバと運用課の専用PCだけですか。

F課長：はい。DBサーバ側でアクセス元のIPアドレスを制限しています。

G氏：運用課のC課長は，利用者TBLを変更するような処理はしていないと言っているのですね。社内の者がPASSWORDを改ざんしてもメリットはないので，まずはインターネットからの不正アクセスの可能性について調査します。10月13日（土）のWebサーバのアクセスログ（以下，Webログという）を見せていただけますか。

F課長：はい，すぐに用意します。

〔原因の判明とインシデント対応〕

G氏は，F課長が用意したWebログを調査した。次は，そのときのG氏とF課長の会話である。

G氏：思ったとおり，SQLインジェクションによる攻撃を受けていました。図4をご覧ください。左から順に，空白で区切って，リクエスト日，リクエスト時刻，クライアントのIPアドレス，HTTPのアクセスメソッド，パス名，クエリストリング，ステータスコードの各項目が並んでいます。どうやらPASSWORDの改ざんだけでなく，USR_NMとUSR_ADDRからも大量にデータが盗まれた可能性があります。
このような不正アクセス時の対応手順は策定されていますか。

```
#Fields: date time client-ip method pathname query-string status
（省略）
2007-10-13 02:24 aa.cc.kk.hh GET /mlogin.html - 200
2007-10-13 02:25 aa.cc.kk.hh GET /scripts/info.cgi "?nid=0701&kind=m" 200
2007-10-13 02:29 aa.cc.kk.hh GET /scripts/info.cgi "?nid=0701&kind=../etc/passwd"
 200
（省略）
2007-10-13 03:00 aa.cc.kk.hh GET /scripts/info.cgi "?nid=0701&kind=ls |" 200
2007-10-13 03:13 ff.aa.rr.pp GET /slogin.html - 200
2007-10-13 03:14 dd.ee.ss.tt GET /slogin.html - 200
2007-10-13 03:15 dd.ee.ss.tt GET /scripts/info.cgi "?nid=0701&kind=m" 200
2007-10-13 03:16 dd.ee.ss.tt GET /scripts/info.cgi "?nid=gf34' union select USER_
NAME,USER_PASSWORD from ADMIN_ALL_USERS where（省略）&kind=m" 200
（省略）
2007-10-13 03:17 dd.ee.ss.ll GET /scripts/info.cgi "?nid=as23' union select TABLE
_NAME,SCHEMA from ADMIN_ALL_TABLES where（省略）&kind=m" 200
2007-10-13 03:18 dd.ee.ii.jj GET /scripts/info.cgi "?nid=0701';update M_NEWS set
PASSWORD='fas7wgw4&kind=m" 200
2007-10-13 04:01 aa.cc.kk.hh GET /scripts/info.cgi "?nid=0701&kind=../ls |" 200
2007-10-13 04:17 dd.ee.ii.jj GET /scripts/info.cgi "?nid=0703' union（省略）&kind=
m" 200
2007-10-13 04:28 dd.ee.ii.jj GET /scripts/info.cgi "?nid=0701';update M_USER set
PASSWORD='fas7wgw4&kind=m" 200
```

注　Fields:に続く各項目は，ログの項目名を示す。
　　time の秒の部分は省略されている。
　　（省略）は，ログ出力内容の省略を意味する。
　　query-string は，二重引用符で囲まれ，URL デコード済の値である。

図 4　2007 年 10 月 13 日（土）の Web ログ（抜粋）

F 課長：対応手順は策定していませんが，PASSWORD が改ざんされ，利用者がログインできない状態でしたので，CIO と相談し，指示に従って X システムを停止しておきました。

G 氏　：良い判断でしたね。そのまま運用を継続していたら被害が拡大したかもしれません。

F 課長：被害拡大は防げましたが，今後はどうすればよいでしょうか。

G 氏　：被害者への連絡，捜査機関への被害届出，場合によっては情報公開や監督官庁への報告をしていただく必要がありますので，証拠保全と正確な情報の把握から始めます。Web ログ，TRN ログに加えて，ソースコードの解析，図 4 で見られた攻撃の再現検証，及び疑似侵入テストを実施し，重要な箇所については詳細な調査を行いたいのですが，よろしいですか。

F 課長：部下の E 君をサポートに付けますので，調査をお願いします。

G 氏　：承知しました。明日の夕方に報告いたします。可能であれば，CIO も同席してくださるようお願いします。

〔調査結果の報告〕

次は，翌日夕方の調査結果の報告における G 氏と F 課長の会話である。

G 氏：それでは今回の調査結果を報告します。表 3 をご覧ください。Web ログから確認できる範囲の最初の攻撃は 2007 年 8 月 24 日（金）2 時 24 分で，それ以降も 41 回の攻撃を受け，累計で 834 件，325 人分の情報が盗まれていました。お知らせ機能だけが攻撃を受けており，そのほかの機能は無事でした。この

機能はログインしなくても利用でき，かつ，脆弱性があったからではないかと推測されます。

表３　攻撃一覧（抜粋）

攻撃の時間帯	攻撃元 IP アドレス	被害の概要
2007/08/24 02:24 ～ 2007/08/24 04:41	aa.bb.xx.yy	91 件の利用者氏名，メールアドレスの流出
⋮	⋮	⋮
2007/10/13 02:24 ～ 2007/10/13 06:01	aa.cc.kk.hh	OS コマンド実行結果の不正閲覧 想定外ファイルの不正参照
2007/10/13 03:14 ～ 2007/10/13 05:17	dd.ee.ss.tt	①DB 管理 TBL の不正参照
[redacted]	dd.ee.ii.jj	②パスワードハッシュの改ざん 329 件の利用者氏名，メールアドレスの流出
2007/10/14 01:18 ～ 2007/10/14 01:19	aa.bb.xx.zz	24 件の利用者氏名，メールアドレスの流出

注　網掛けの部分は，設問の関係上，表示していない。

F 課長：USR_NM と USR_ADDR が流出した可能性があるのですね。

G 氏　：はい。図 4 で見られた攻撃を再現させたところ，union 句を利用して利用者 TBL のデータを参照できることを確認しました。

G 氏は，調査結果の報告を終え，今後の対策について説明を進めた。

〔SQL インジェクション対策〕

次は，お知らせ機能における SQL インジェクション対策に関する会話である。

F 課長：図 2 のお知らせエリアには入力フィールドがないので，SQL インジェクション対策は必要ないと思っていました。

G 氏　：画面上の入力フィールドの有無とセキュアプログラミングの要否は関係ありません。SQL インジェクション対策について言えば，SQL 文の要素になる文字列に対しては，すべて，エスケープ処理や DB のバインド機構の利用が必要です。実際に攻撃を受けていたお知らせ機能の CGI プログラム（図 5）を基にもう少し詳しく説明します。このプログラムは Perl を用いて作成されています。

G 氏は，SQL インジェクション対策について説明した。

```
 1 #!/usr/bin/perl
 2 use CGI;                                  # 汎用 CGI 処理用モジュール CGI の使用を宣言
 3 use DBI;                                  # 汎用 DB 処理用モジュール DBI の使用を宣言
 4 $DOC_ROOT = "/home/info/";                        # お知らせファイルディレクトリ
 5 $cgi = new CGI;                                   # CGI クラスのオブジェクトを生成
 6 $nws_id = $cgi->param('nid');                     # nid パラメタを取得
 7 $kind = $cgi->param('kind');                      # kind パラメタを取得
 8 print "Content-Type: text/html¥n¥n";              # HTTP リプライヘッダを出力
 9 print "<HTML><BODY>";                            # HTML 開始部分を出力
10
11 $dbh = DBI->connect('DBI（省略）') or die;       # DB に接続
12 $sql = "select NWS_NM,NWS_BODY from M_NEWS ";# SQL 文組立てを開始
13 $whr = "where NWS_ID = '";
14 $qry = $sql.$whr.$nws_id."';";                   # SQL 文組立てを終了
15 $sth = $dbh ->prepare($qry) or die;              # SQL 文を準備
16 $sth->execute;                                   # SQL 文を実行
17
18 @ary = $sth ->fetchrow_array;                    # 先頭行を取得
19 print xss($ary[0])."¥n<HR>¥n";                   # お知らせタイトル，仕切り線を出力
20 print xss($ary[1])."¥n<HR>¥n<PRE>";              # お知らせ内容，仕切り線を出力
21 $sth->finish or die;                             # SQL 文使用を終了
22 $dbh->disconnect or die;                         # DB から切断
23
24 $filepath = $DOC_ROOT.$kind;                     # 業種区分別ファイルへのパスを決定
25 open(FILE, $filepath) or die;                    # ファイルを開く
26 while($line=<FILE>) {
27     print xss($line);                            # ファイル内容をエスケープして出力
28 }
29 close(FILE);                                    # ファイルを閉じる
30
31 print "</PRE></BODY></HTML>";                   # HTML 終了部分を出力
（省略）
42 sub xss {（省略）}    # 引数の文字列中の&, <, >, ", 'に対するクロスサイトスクリプティング
43                       # 対策処理をして返す
```

注　（省略）は，記述を省略していることを意味する。

図５　お知らせ機能の CGI プログラム“info.cgi”（抜粋）

〔そのほかの脆弱性とその対策〕

G 氏は，テスト環境で X システムに対して疑似侵入テストを実施した際に，SQL インジェクション以外にも幾つかの脆弱性を発見した。次は，それらの脆弱性についての会話である。

G 氏：まず，表 3 中の下線①について再現できるか検証したところ，各プログラムから DB へのアクセスに利用されている DB アカウントで，“ADMIN_ALL_USERS”や“ADMIN_ALL_TABLES”のデータを参照できました。DB 管理 TBL に対する参照権限は本当に必要でしょうか。

F 課長：いいえ，必要ではありません。それが何か問題なのでしょうか。

G 氏：プログラムの修正漏れなどによって，万一脆弱性が残ってしまった場合に備えて，被害を最小にするために DB 側で，［　b　］するのが定石です。次に，そのはかの脆弱性とその対策に移ります。X システムでは利用者ごとに許可されている機能が定義され，［　a　］制御されているはずですが，一部の機能では，実行用の URL を直接入力することによって，テスト用アカウントには許可されていないはずの機能を実行できました。

F 課長：ログイン後のメニュー画面には，利用者に許可されている機能のボタンだけを表示していたのですが，実行用の URL を直接入力することで実行できてし

まったということですね。

G 氏：はい。ログインした利用者が各機能を実行してよいか否かをサーバ側で確認す［ a ］制御を，すべての機能に対して必ず実装してください。

F 課長：分かりました。全機能を確認し，修正します。

G 氏：また，ログアウト後にブラウザの“戻る”ボタンを押すことで，再びログインしなくても，それまで利用していたページを表示させ，X システムの機能を実行することができました。これを防ぐために，ログアウト処理で［ c ］をしてください。

F 課長：分かりました。ログアウト処理の部分を修正します。

引き続き，G 氏はそのほかの脆弱性についても報告した。

〔インシデント対応策の検討〕

検出されたすべての脆弱性についての報告が終了した。次は，インシデント対応策についての会話である。

F 課長：お蔭様でインシデント対応策のめどがつきました。あとは当社でプログラムの修正を実施すれば再開できますね。

G 氏　：いいえ。全プログラムを対象に調査を実施したわけではないので，まだすべての脆弱性を発見できたわけではありません。費用や期間の問題もありますが，できれば全プログラムを対象にセキュリティ検査を実施した方がよいので，ご検討ください。

F 課長：分かりました。ただ，X システムの場合，ほとんどの機能はログインしてから利用できるようになっており，利用者は取引先の受注，発注担当者と当社の受発注担当者だけですので，今回脆弱性を指摘された部分を中心に再検査をすればよいと思っています。それにしても今回は，Web ログをきちんと取っておいたことは不幸中の幸いでした。

G 氏　：そうですね。しかし，攻撃者が GET ではなく POST で攻撃してきたら，図 4 の項目の［ d ］に有益な情報が残らないので，漏えいした情報を確認することはできなかったでしょう。Web アプリケーションの場合，ログの種類としては，主に Web ログ，TRN ログ，DB ログがありますが，③各ログ単独では，いつ，だれが，何を，どうしたかの情報が不足しています。

G 氏は，その理由について説明した。続いて，運用課におけるシステム運用の問題点と対策についても説明した。

G 氏　：最後に，長期的な観点から，X システムにおける同様の不正アクセスに対する防止策の検討と，万一発生した場合の対応策を用意しておく必要があります。防止策については，先ほど申し上げたような対策を実施する必要があります。発生時に備える対応策としては，不正アクセスをできる限り早く検知するための対策や，④検知後の対応が迅速かつ正確に行えるようにする対策を実施しておく必要があります。

F 課長：今回はたまたま初動対応がうまくいきましたが，だれが対応しても同じようにできなくてはいけませんからね。

G 氏　：そのとおりです。

G 氏は，インシデント対応策について更に具体的に説明した。

その後，捜査機関によって攻撃者が逮捕された。幸いにも，盗まれた情報が二次利用されたとの報告はなかった。また，流出した個人情報にかかわる利用者に対する事情説明や情報公開なども適切に行われた。

脆弱性が発見されたプログラムは修正され，B 社によるセキュリティ検査を実施した上でリリースされた。そして，各利用者に新たなパスワードを発行して，X システムは，安全にサービスを再開することができた。

設問 1　脆弱性対策について，(1) ～ (3) に答えよ。

(1) 本文中の [a] ，[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　エラーログの採取　　イ　サニタイジング　　ウ　識別

エ　セッション情報の破棄　　オ　認可　　カ　認証

(2) 図 5 のプログラムに対して，コマンド ifconfig の実行結果を表示させる攻撃があった。攻撃時に kind に指定された文字列を，20 字以内で答えよ。ここで，コマンド ifconfig の絶対パスは，/bin/ifconfig であるものとする。

(3) 図 5 のプログラムにおいて，25 行目の open 関数を sysopen 関数に変更した場合，A 社が受けていたどの攻撃が防げるか。20 字以内で答えよ。また，open 関数に起因する問題点のうち，sysopen 関数に変更しただけでは解決できない問題点を，30 字以内で述べよ。

設問 2　SQL インジェクション対策について，(1) ～ (4) に答えよ。

(1) 表 3 中の下線②が実行された日付及び時刻を答えよ。

(2) 本文中の [d] に入れる適切な字句を，12 字以内で答えよ。

(3) 図 5 のプログラムにおいて，DBMS の特殊文字をエスケープ処理する SQL イ

ンジェクション対策用サブルーチンを利用するとした場合，このサブルーチンを適用すべき最も適切な変数はどれか。該当するものを解答群の中から選び，記号で答えよ。

解答群

ア　$cgi　　イ　$nws_id　　ウ　$qry　　エ　$ary【0】

(4) 本文中の [b] に入れる対策内容を，50 字以内で述べよ。

設問 3　DB サーバに対する運用上の問題とインシデント対応策について，(1) ～ (3) に答えよ。

(1) DB サーバに対する運用課における運用上の問題点を二つ挙げ，それぞれ 30 字以内で述べよ。

(2) 本文中の下線③で G 氏が言及している，TRN ログ単独及び DB ログ単独では不足している情報は何か。各ログについて該当するものを解答群の中からすべて選び，記号で答えよ。また，DB ログに不足している情報を補うためには X システムをどのように改修すべきか。50 字以内で述べよ。

解答群

ア　いつ（実行日時）　　イ　だれが（利用者 ID）

ウ　何を（どのテーブル）　　エ　どうした（参照，更新，削除）

(3) 本文中の下線④で G 氏が言及している，実施すべき対策を二つ挙げ，それぞれ 25 字以内で述べよ。

問 2　認証システムの企画・設計に関する次の記述を読んで，設問 1～5 に答えよ。

L 学園は，傘下に情報専門学校，ビジネス専門学校，建築・インテリア専門学校の三つの専門学校をもつ学校法人である。3 校の学生数は合わせて 3，000 名，学校法人本部（以下，本部という）の職員を含めて教職員数は 150 名である。表 1 に示す L 学園の情報システムは，本部の情報システム課で開発管理を行い，本部の人事課と各校の学生課などの各主管部署で運用を行っている。このほか，本部には Web サーバがあり，各校の一般向け Web サイトと学生向け Web サイトをインターネット経由で公開している。

表１　L 学園の情報システム

種別	システム名	クライアントソフト	利用者	サーバ名（設置場所）	現行の認証方式
事務系	人事給与システム	Web ブラウザ	教職員	人事給与サーバ（本部）	Web サーバによるフォーム認証
	財務会計システム	専用クライアントソフト	職員	財務会計サーバ（本部）	専用サーバソフトによる認証
教務系	学籍管理システム	Web ブラウザ	教職員	教務系サーバ（本部）	Web サーバによるフォーム認証
	成績管理システム	Web ブラウザ	教職員，学生		
	就職情報システム	専用クライアントソフト	教職員	就職情報サーバ（各校）	専用サーバソフトによる認証
	学生実習環境（Web 閲覧を含む）	市販ソフト，Web ブラウザ	教職員，学生	PC 実習サーバ（各校）	ディレクトリサーバによる認証
				UNIX 実習サーバ（各校）	UNIX OS による認証
共通	ファイルサーバ	（OS の標準機能）	教職員	ファイルサーバ（本部，各校）	ディレクトリサーバによる認証
	グループウェア	専用クライアントソフト	教職員	グループウェアサーバ（本部，各校）	グループウェアサーバによる認証
	電子メール	メールソフト	教職員，学生	メールサーバ（本部，各校）	IMAP4 による認証

学園全体でのシステム化が進むに従って，学生や教職員が利用する利用者 ID とパスワードの数は増加する一方である。事務系，教務系の各情報システムでは主管部署が個別に利用者 ID とパスワードを発行しており，学生の入学や卒業，教職員の異動などのたびにアカウントの追加や削除を行っている。各校では授業で利用するノート PC を一括購入して新入学生に配布していることもあって，年度末から新年度にかけては各部署での業務上の負担が特に大きくなってきている。

また，各利用者に対して情報システムごとに利用者 ID が付与されることが多くなったことから，複数校の授業を兼任する教員などからは，複数の利用者 ID とパスワードを覚えるのが難しいという声が頻繁に聞かれるようになってきている。一方，一部の情報システムでは職員個人には利用者 ID が割り当てられておらず，数人の職員が一つの利用者 ID を共用しているケースもある。

こうした状態はパスワードや情報の漏えいにつながりかねないとの経営陣からの指摘や，将来の想定される用途を踏まえ，情報システム課は，安全な利用者認証を実現する手段や，利用者認証の新たな用途への応用について検討することにした。

次は，情報システム課の P 課長とその部下の Q さんの会話である。

〔学生向け Web サイトの認証方式〕

P 課長：まず，公開している Web サーバについて考えていくことにしよう。現在，一般向けに公開している各校の Web サイトには利用者認証が必要なページはないが，各校の学生向け Web サイトには認証が必要なページがあるね。

Q さん：各校の学生向け Web サイトでは，入学の際に利用者 ID と初期パスワードを学生に通知し，最初のアクセス時に初期パスワードを変更してもらっています。Web サーバでは HTTP でベーシック認証を行い，学生はシラバス（講義要領）などの資料や休講連絡のページにアクセスしています。

P 課長：今は SSL を使用していないから，HTTP 上でのベーシック認証ではパスワードが漏えいする可能性があるのが一番の問題だね。これは一般的に Web サイトでよく使われるフォーム認証でも同様だ。

ベーシック認証よりも安全な方法として知られているものには，［ a ］認証がある。この方法では，ハッシュ関数を用いたチャレンジ・レスポンス方式を採用することでパスワードの漏えいを防ぐことができる。しかし，古いブラウザなどでは対応していないという問題がある。

Q さん：学生は携帯電話からアクセスすることが多いのですが，携帯電話でも［ a ］認証には対応していないものがあると聞いたことがあります。

P 課長：今はあまり重要な情報を提供してはいないが，将来は学生向けポータルサイトとして履修登録や成績の確認，学生の出欠管理もできるようにしたいという要求が各校から出ている。

Q さん：そうなると，Web サイト上で重要な個人情報を取り扱うことになりますから，やはり① ［ a ］認証を採用するだけでは不十分ですね。

P 課長：そうだね。学生向けポータルサイトには SSL の導入が必要になりそうだ。

Q さん：SSL を導入する場合には外部のサーバ証明書発行サービスを利用することになると思いますが，携帯電話への対応はどうしましょうか。

P 課長：利用者側で SSL に対応した携帯電話を利用するのはもちろんだが，携帯電話会社や機種の違いも考慮する必要がある。多くの機種に対応したサイトを構築するには，サーバ側で適切な配慮が必要になりそうだね。

〔情報システムの認証方式〕

P 課長：次に，現状での情報システムの問題点について見ていこう。

Q さん：教職員からは，個別の利用者 ID とパスワードが情報システムごとに割り振られているので使いにくいという話をよく聞きます。

P 課長：各情報システムによって構築された時期が違うし，利用形態や稼働している OS もそれぞれ違っているからね。そもそも財務会計システムなどでは，職員一人一人ではなく係単位でしか利用者 ID が割り振られていないから，セキュリティ上大きな問題がある。

Q さん：どういったところが問題なのでしょうか。

P 課長：ID は英語で identifier（識別子）というくらいだから利用者の識別が主な目的ではあるが，もう一つ大事な目的として［ b ］制御がある。つまり，どの利用者に，どのリソースに対して，どのようなアクセスを許可するのかということだ。個別に利用者 ID を割り当てないと，権限の管理が適切に行えないおそれがある。また，最近は内部統制の観点から［ c ］性という要素も重視されるようになってきている。

Q さん：事務系も教務系も，利用者抄とパスワードの管理が煩雑になっているのが一番の問題ですね。シングルサインオン（以下，SSO という）を実現して，一度の利用者認証で複数の情報システムを利用できるようにするのがよいのではないでしょうか。

P 課長：いや，それよりも現状では各情報システムの利用者の登録や削除に伴う運用コストの方が問題だ。まずは，個々の利用者に対して学園内の各情報システム共通に利用できる利用者 ID を発行したい。これを仮に共通 ID と呼ぶことにしよう。その上で，この共通 ID を含む認証情報と，利用者の氏名や所属などの属性情報を併せて一元管理するシステムを作るのがよさそうだ。これは仮に共通 ID システムと呼ぶことにしよう。②個々の情報システムがこの共通 ID システムの提供する認証情報を利用して認証を行えるようにすれば，最初に利用者 ID の移行に伴う作業が発生するが，各情報システムの主管部署での運用コストは低減できる。その次の段階ですべての情報システムを SSO に統合するのがよいだろう。その際，すべての情報システムを一度に SSO に対応させることが難しいなら，一部の情報システムから対応させていってもいい。

Q さん：すべての情報システムが SSO に統合されると，共通 ID システムももちろんですが，SSO 機能を提供するサーバの可用性も重要になってきますね。

P 課長：それに加えて，利用者側での利用者 ID やパスワードの管理の問題もある。先日ビジネス専門学校に打合せに行った時，利用者 ID とパスワードが書かれた付せん紙が PC のディスプレイにはってあったのを見つけたよ。このような実態では SSO を導入するとかえって危険だから，パスワードに代わる認証方式を導入したいところだ。

Q さん：生体認証や IC カードなどの認証トークンを検討してはどうでしょうか。どんなデバイスを選ぶかにもよりますが，学生の出席確認や入退室管理など，将来いろいろな用途が想定されます。

P 課長：そうだね。ただ，当学園の情報システムには，クライアントとして Web ブラウザを使うものと専用クライアントソフトを使うものが混在しているから，認証トークンを導入すると SSO への対応が難しくなるかもしれない。更に言うと，認証トークンを使うかどうかにかかわらず，現行の情報システムはできるだけ改修せずに SSO への対応を図りたいところだね。

Q さん：そうですね。ちょっと欲張りな要件のような気もしますが，ベンダの提案を聞いてみることにしましょう。

〔無線 LAN と利用者認証〕

P 課長：ネットワークの構成に関しても，様々な要望があるね。学生からは，インタ

ーネットに接続可能な無線 LAN アクセスポイント（以下，AP という）を食堂やラウンジに設置してほしいという要望が出ている。実習スペースのデスクトップ PC や校内の情報コンセントからでもインターネットにアクセスできるが，数年前から学生に配布しているノート PC には無線 LAN の機能があるからね。

Q さん：複数校を兼任してノート PC を持ち歩いている教員からは，どの学校からでも同じように無線 LAN を使って成績管理システムにアクセスしたいという声を聞きました。個人情報を扱うことになるので十分な対策が必要だと思いますが，無線 LAN でよく使われ［ d ］フィルタリングによる接続の制限や，WEP による暗号化だけで十分なのでしょうか。

P 課長：無線 LAN のセキュリティ対策には，利用者認証と暗号化方式の二つの側面がある。利用者認証の面から言うと，知識のある人なら［ d ］は偽装することができるから十分な対策とはいえない。さらに，各校の AP に利用者のノート PC の［ d ］をすべて登録する必要があるから，管理上の手間もかかる。また，暗号化方式の面では，WEP では利用者が同じ暗号鍵を共用する上，解読が比較的容易だという脆弱性が知られている。

Q さん：利用者認証と暗号化方式の強化を考えなければいけないのですね。利用者認証の強化にはどのような方法があるのですか。

P 課長：利用者認証には，IEEE 802．1 X という規格を採用するのがよさそうだ。これと暗号化方式の強化を組み合わせることでセキュリティの強化を図ることができるだろう。

Q さん：そういえば，私が駅やファストフード店でときどき使う公衆無線 LAN の AP でも IEEE 802．1 X を利用していたと思います。IEEE 802．1 X では，利用者の認証はどのように行うのですか。

P 課長：IEEE 802．1 X では，利用者の認証情報は AP ではなく認証サーバと呼ばれる別のサーバに格納されており，AP はこの認証サーバにアクセスの可否を問い合わせる。そのプロトコルとしては［ e ］を利用する実装が多いようだ。

Q さん：以前はダイヤルアップのアクセスサーバなどでよく使われていたプロトコルですね。各校に認証サーバを設置して共通 ID システムと連携させれば，各校の間で共通に無線 LAN が利用できるわけですね。

P 課長：そういうことだ。IEE E802．1 X で使われる EAP（Extensible Authentication Protocol）というプロトコルは PPP を拡張したものだから，［ e ］とは親和性が高い。EAP では，まず端末と AP の間で認証を行い，認証が完了した時点で端末に個別のセッション鍵を配送する。セッション鍵をもっていない未認証の端末は，AP を超えて LAN 側にパケットを送出することができな

い仕組みになっている。これに加え，EAP では各種の認証方式を利用することができる。代表的な認証方式を挙げると，表 2 のようになる。

表 2　EAP の代表的な認証方式の比較

認証方式	クライアント認証	サーバ認証	セッション鍵の自動生成	ノート PC の OS での対応
EAP-MD5	利用者 ID/パスワード	なし	なし	現在は実装なし
EAP-TLS	ディジタル証明書	あり	あり	標準対応
EAP-TTLS	利用者 ID/パスワード	あり	あり	追加ソフトが必要
PEAP	利用者 ID/パスワード	あり	あり	標準対応

Q さん：サーバ認証というのは，クライアント認証とは逆に，クライアントが認証サーバを認証するためのものですね。

P 課長：そのとおり。EAP-MD5 は③サーバ認証の仕組みをもたないのでリスクがあるし，学生に配布しているノート PC の OS でのサポートも打ち切られている。クライアント認証について言うと，EAP-TTLS では OS で標準的にサポートされていないので，追加ソフトが必要になる。したがって，共通 ID システムに公開鍵基盤（PKI）を導入するなら EAP-TLS を，そうでなければ PEAP を使うことになるだろう。

Q さん：セッション鍵の自動生成というのは，暗号化方式の強化に関係するものですね。

P 課長：そうそう，暗号化方式を強化するという話がまだだったね。IEEE 802．1 X では，利用者ごとに異なった WEP 鍵が使用されることになっている。これに加え，セッション中も自動的に WEP 鍵を更新することで，暗号化された通信の解読をより困難にするというわけだ。

無線 LAN の暗号化方式に関しては，近年になってより安全な規格が提案されている。WEP の後継規格である WPA と IEEE 802．11i（WPA2）という規格では，利用者認証に IEEE 802．1 X を採用した上で，更に暗号化方式の強化を図っている。WPA では，暗号化には WEP と同じ［　f　］を使うものの，TKIP という鍵交換方式の採用によって暗号鍵を動的に変更することができる。また，WPA2 では，暗号化に［　g　］を用いて暗号自体の強度を高めることができる。

Q さん：なるほど，暗号化方式の強化にもいろいろな方法があるのですね。

〔共通認証システム〕

以上の検討を基に，P 課長と Q さんは共通 ID システム及びそれを利用して利用者認証を行うシステム（以下，両システムを併せて共通認証システムという）の要件をまとめ，図に示す提案依頼書をベンダ各社に提示した。

この提案依頼書に対し，数社のベンダから提案書が寄せられた。その採否を検討する過程で，L 学園は Z 社に対してヒアリングを行うことになった。

Z 社の提案によると，利用者である個々の学生や教職員の認証情報と属性情報は，L 学園本部に新たに設置する LDAP サーバにすべて格納される。このサーバが個々の情報システムに利用者の認証情報や属性情報を配信することで，情報システムが利用者認証を行うことができるようになっている。また，利用者認証には PKI を利用することとし，公開鍵証明書と秘密鍵は，学生証又は教職員証を兼ねた IC カードに格納して利用者本人に配布することとしている。

共通認証システムに関する提案依頼書

1. L 学園の情報システムの現状とネットワーク構成
（省略）
2. 共通認証システムの目的
当学園に在籍する学生と教職員を対象とした共通認証システムを新たに構築することによって，セキュリティを保ちつつ［ア］ことと［イ］ことを目的とする。また，教務系の各情報システムでの学生情報の利用などへの活用も目的とする。
3. 共通認証システムの概要及びその要求仕様
3.1 本部及び各校のすべての情報システム利用者に対する共通的な認証基盤である共通 ID システムの構築
(1) 共通 ID システムでは，利用者に対して本部及び各校で共通の利用者 ID を付与すること
(2) 共通 ID システムでは，利用者の認証情報（共通 ID を含む）及び属性情報（氏名，所属など）を一元管理し，当学園の情報システムに対して配布できること
(3) 共通 ID システムを利用した利用者認証には④二要素認証を採用すること。ただし，学生向け Web サイトでの認証を除く
(4) 共通 ID システムは，業務のサービスレベルの観点から可用性に配慮すること
3.2 主要な情報システムにおけるシングルサインオン（SSO）機能の導入
(1) 利用者が複数の業務アプリケーションにアクセスする際，それぞれにログインし直す必要がないよう，表 1 の情報システムに対して SSO 機能を提供すること
(2) SSO 機能には，共通 ID システムが提供する認証情報を用いること
(3) SSO 機能を提供するサーバは，業務のサービスレベルの観点から⑤可用性に配慮すること
(4) SSO 機能の提供に当たっては，既存の情報システムの改修を極力少なくすること
3.3 学生向け Web サイトの SSL 化
(1) 各校の学生向け Web サイトを SSL に対応させること
(2) 携帯電話からの SSL によるアクセスに対応させるために，サーバ証明書はすべての携帯電話会社の主要な機種に組み込まれたルート証明書によって検証可能であること
3.4 各校における無線 LAN アクセスポイントの設置
(1) 各校に無線 LAN アクセスポイント及び認証サーバを設置し，IEEE 802.1X による利用者認証を行うこと
(2) 各校に設置された IEEE 802.1X の認証サーバと共通 ID システムの連携を図り，利用者が 3 校間で同様に無線 LAN を利用できるようにすること
(3) EAP の認証には，クライアントとサーバ間の相互認証が可能な方式を利用すること
(4) 通信の暗号化方式として WPA 又は WPA2 を採用すること
（以下省略）

図　提案依頼書

次は，P 課長，Q さんと Z 社の担当者X氏との会話である。

〔SSO 機能の実現方式〕

P 課長：SSO 機能の実現方式についてお聞かせください。

X 氏　：今回は Web の SSO 機能と専用クライアントソフトの SSO 機能を両立できるシステムを提案しています。

Web において SSO を実現させる場合には，クッキーにセッション ID などの情報を格納することで，認証された利用者に対するセッションを維持するのが一般的です。しかし，貴学園の場合は⑥本部と各校がそれぞれ別個のドメイン名を使用しているので，本部と各校をまたがって，クッキーを利用してセッションを維持することができません。

P 課長：そうですか。ドメイン名のことまでは考えが及びませんでした。

X 氏　：そこで，現在のドメイン名を変更することなく複数のドメインにまたがって SSO を実現するために，今回の提案ではリバースプロキシという方式を採用した製品を選択しました。

この方式では，利用者と Web サーバの間にリバースプロキシサーバと呼ばれるサーバを設置します。利用者からのアクセスは，このリバースプロキシサーバが認証を行った上で各 Web サーバに中継することによって SSO が実現できます。新たに機器を設置することになるので，ネットワークの構成や Web アプリケーションへのアクセスの方法は変わりますが，Web アプリケーション自体の改修は基本的には不要です。

Q さん：専用クライアントソフトでの SSO 機能についてはどのように考えていますか。

X 氏　：利用者の PC にエージェントモジュールをインストールすることで，SSO 機能を導入したいと思います。専用クライアントソフトの起動時に，エージェントモジュールが認証情報の入力を自動的に代行することで SSO を実現することができます。今回提案する SSO システムのエージェントモジュールは，今お使いになっている専用クライアントソフトにすべて対応しています。

〔PKI による利用者認証〕

P 課長：次に，共通 ID システムを利用した利用者認証の方式についてお聞かせください。

X 氏　：利用者認証には幾つかの方式が考えられます。ワンタイムパスワードや生体認証も考えられますが，PKI であれば公開鍵暗号を利用してお互いの公開鍵証明書を検証することができるので，より確実な認証方法となります。この方式であれば，共通 ID システムと IEEE 802．1 X の認証サーバを LDAP で連携させることで，無線 LAN のクライアント認証も実現可能です。

P 課長：SSO や無線 LAN の認証に PKI を利用するとなると，ディジタル証明書と秘密鍵を格納するデバイスをどうするかという問題が出てきますね。御社で IC カードを提案されたのは，どのような理由からでしょうか。

X 氏　：認証用デバイスとしては，USB トークンや IC カードを利用することが考えられます。どちらもデバイスの機能によってディジタル証明書と秘密鍵が保護されており，PIN を入力することで二要素認証が実現できます。

一般的には，それぞれ表 3 のようなメリットとデメリットがあります。これらの特徴に加え，⑦将来の想定される用途を踏まえて両者を比較した結果，IC カードを採用すべきであると判断しました。

表3　認証用デバイスのメリットとデメリット

評価＼デバイス	USB トークン	IC カード
メリット	・機器の USB ポートに挿すだけで使える。 ・デバイス自体に鍵のようなイメージがあり，利用者にとってなじみやすい。	・配布方法が既に確立されている学生証や教職員証を兼ねることができる。 ・USB トークンよりも安価である。 ・用途に応じて接触方式又は非接触方式を選択できる。
デメリット	・IC カードよりも高価である。 ・USB ポートのある機器でしか利用できない。	・機器に IC カード読取り機が必要である。

Q さん：新学期が始まる前には IC カードを大量に発行する必要がありますが，どのような方法で対応されますか。

X 氏　：IC カードの発行は外部に委託し，各校で本人確認を行った上で配布していただくことを提案しています。

Q さん：IC カードの発行を外部に委託できるのであれば，年度末の負担もそれほど増えずに済みますね。

L 学園は更に検討を進めた結果，Z 社の提案を採用し，共通認証システムの構築を完了することができた。

設問 1　学生向け Web サイトの認証の手法について，(1)，(2) に答えよ。

(1) 本文中の [a] に入れる適切な字句を答えよ。

(2) 本文中の下線①について，Q さんが不十分としている理由を，25 字以内で述べよ。

設問 2　情報システムの認証方式について，(1) ～ (3) に答えよ。

(1) 本文中の [b] ，[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　効率　　イ　真正　　ウ　信頼

エ　責任追跡　　オ　認可　　カ　認証

(2) 本文中の下線②について，個々の情報システムで行っていた利用者 ID の発行を共通 ID システムに移行するとき，個々の情報システムの主管部署と情報システム課の間で必要となる調整事項を，30 字以内で述べよ。

(3) 図中の下線④は，共通 ID システムを利用して SSO を実現する際に考慮すべき，どのようなリスクの低減を意図したものか。60 字以内で述べよ。

設問 3　SSO の実現方式について，(1)，(2) に答えよ。

(1) 図中の下線⑤は，SSO 機能を提供するサーバにおいてどのようなリスクの低減を意図したものか。60 字以内で述べよ。

(2) 本文中の下線⑥について，クッキーを利用したセッションの維持ができない

理由を，クッキーの動作原理に基づいて 40 字以内で述べよ。

設問 4　無線 LAN と利用者認証の方式について，(1)，(2) に答えよ。

(1) 本文中の [da] ～ [g] 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　CHAP	ウ　ESSID	エ　IP アドレス
オ　MAC アドレス	カ　RADIUS	キ　RC4	ク　RC5
ケ　SASL	コ　URL	サ　トリプル DES	シ　パケット

(2) 本文中の下線③について，無線 LAN のサーバ認証によってどのような脅威を防ぐことができるか。また，その脅威が防げない場合には，どのような直接の被害が発生する可能性があるか。それぞれ 30 字以内で述べよ。

設問 5　共通認証システムの設計について，(1)，(2) に答えよ。

(1) 現状での情報システムの問題点に関する P 課長と Q さんの会話を踏まえて，図中の [ア] ，[イ] に入れる共通認証システムの目的を，それぞれ 15 字以内で述べよ。

(2) 本文中の下線⑦の観点から，USB トークンと IC カードを比較した結果，X 氏が IC カードを採用すべきであると判断した理由を，30 字以内で述べよ。