SC

平成27年度　秋期
情報セキュリティスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1～問3
選択方法	2問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

選択欄	
2問選択	○問1
	問2
	○問3

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ソフトウェアの脆弱性への対応に関する次の記述を読んで，設問1～5に答えよ。

Q社は従業員数300名の食品販売会社であり，消費者向けにインターネットを介して健康食品を販売している。

Q社の社外向け情報システムは，販売システム（以下，Eシステムという）と広報システム（以下，Fシステムという）から成り，G社のデータセンタに設置されている。Eシステムは Q 社の販売チャネルの大部分を担っており，保守のための時間帯を除き，常時稼働している。Fシステムは投資家などに対する財務情報・会社情報を提供している。両システムは，Q社のシステム部が構築，運用している。

Eシステムは，Eサーバ，待機サーバ，データベースサーバ（以下，DBサーバという）などから成る。Eサーバは，Eサーバ1とEサーバ2から成る冗長構成であり，ロードバランサ（以下，LBという）によって負荷分散を行っている。待機サーバは，Eサーバ1及びEサーバ2がともに停止した際に，Eシステムの利用者に停止を告知するためのものである。Q社の社外向け情報システムのネットワーク構成を図1に示す。

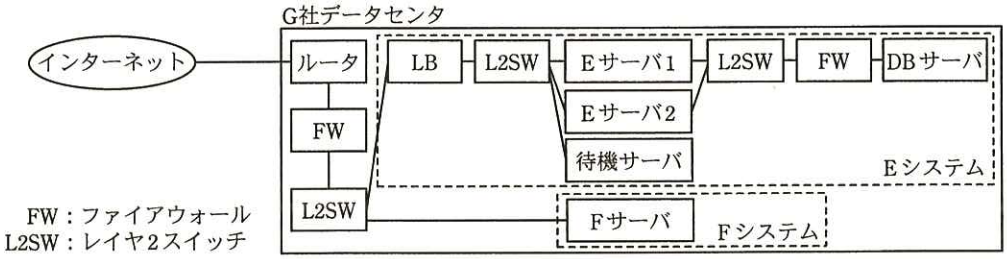


図1　社外向け情報システムのネットワーク構成

Eサーバでは，HTTPサーバ，Webアプリケーションサーバ（以下，WASという）及びWebアプリケーションソフトウェア（以下，Webアプリ Eという）が稼働している。Webアプリ Eは，オープンソースソフトウェアのWebアプリケーションフレームワーク（以下，WFという）を使用して開発された。Webアプリ EとWFは，WASと同じ権限で動作する。また，HTTPサーバにはオープンソースソフトウェアの WAF が付属しており，HTTPサーバの一部として動作する。WAF にはルールを設定することができるが，現在は何も設定していない。Webアプリ Eは，商品情報，購入者情報，購入履歴情報などが格納されたDBサーバにアクセスする。Eサーバの

ソフトウェア構成を表1に示す。

表1　Eサーバのソフトウェア構成

ソフトウェア	現在の動作権限設定	備考
OS	—	—
HTTP サーバ（WAF 含む）	管理者権限	—
WAS	管理者権限	—
Web アプリ E（WF 使用）	—	WAS の動作権限と同一

注記　HTTP リクエストは，LB → HTTP サーバ（WAF 含む） → WAS → Web アプリ E の順に処理される。

F システムは，F サーバ1台から成る。F サーバは HTTP サーバを搭載しており，静的な HTML コンテンツを公開している。F サーバには，WF，WAF を導入していない。Q 社では，社外向け情報システムの開発検証用に図 1 中の E システム，F システムと同一構成のシステムをそれぞれ別に用意している。

WAF のルールの記述形式を図2に，WAF の動作を図3に示す。

・ルールは，[検証対象]，[パターン]及び[動作]の三つを1行に記述する。
　（例：POST　abc¥.exe　検知）
・[検証対象]には，次のいずれかを指定する。
　　GET　　：GET メソッドのパラメタ名を検証対象とする。
　　POST　　：POST メソッドのパラメタ名を検証対象とする。
　　ANY　　：任意のメソッドのパラメタ名を検証対象とする。
　　COOKIE　　：Cookie の名前を検証対象とする。
　　Multipart　　：Multipart/form-data のフィールド名を検証対象とする。
・[パターン]には，次の要素で構成される正規表現を指定する。
　　^　　：文字列の先頭にマッチする。
　　¥W　　：任意の非英数字にマッチする。
　　x|*y*　　：*x* 又は *y* にマッチする。
　　(*x*|*y*)*z*　　：*xz* 又は *yz* にマッチする。
　　[*xyz*]　　：*x*，*y* 又は *z* のいずれかにマッチする。
　　.　　：任意の文字とマッチする。
　　¥.　　：“.” とマッチする。
　　*　　：直前の要素と0回以上マッチする。
・[動作]には，次のいずれかを指定する。
　　遮断：通信を遮断し，ログに記録する。
　　検知：通信を通過させ，ログに記録する。
　　許可：通信を通過させ，ログに記録しない。

図2　WAF のルールの記述形式

・WAF は，HTTP リクエストにおける[検証対象]に対して，[パターン]とのマッチングを行う。
・設定されたルールを順に検証する。最初にマッチしたルールの[動作]に指定された処理を行い，残りのルールは検証しない。
・どのルールにもマッチしなかった場合，その HTTP リクエストを通過させる。

注記　Multipart/form-data による HTTP リクエストは，[検証対象]に Multipart が指定されたときだけ[パターン]とのマッチングを行う。

図 3　WAF の動作

〔脆弱性の確認〕

ある日，システム開発担当の S 主任に別の部署の社員から WF の特定バージョン（以下，バージョン Z という）の脆弱性（以下，脆弱性 X という）が公表されたという連絡があった。S 主任が，Q 社での WF のバージョン Z の使用の有無を調査したところ，E サーバの WF が該当していた。早速，脆弱性 X への対応を S 主任と部下の T さんとで行うことになった。

T さんが確認したところ，次のことが分かった。

・脆弱性 X は，HTTP リクエストが適切に処理されないバグを突いて，ClassLoader を不正に操作できるというものである。
・攻撃者が“class.classLoader”という文字列を含む HTTP リクエストを送信することによって，任意のファイルへの書込みなど，WAS の動作権限で任意の攻撃コードを実行できる。
・攻撃方法及び攻撃コードが既にインターネットで公開されており，攻撃は容易である。
・修正モジュールが既に提供されている。

S 主任は脆弱性 X の確認結果を経営陣に報告し，E サーバ 1 及び E サーバ 2 を停止させるとともに，LB の設定を変えて待機サーバに切り替えた。次は，その後の S 主任と T さんの会話である。

S 主任：E サーバに対して，攻撃者が脆弱性 X をどのように悪用できるのか具体的に説明してくれるかな。

T さん：表 2 の攻撃コードの例を使って説明します。攻撃者は攻撃コードを表 2 の項番の順に E サーバに送ることで，任意のコマンド“XXXX”を実行できま

す。表2の攻撃コードの送信後，WASのアクセスログ（以下，WASログという）のファイルが［ a ］に作成されます。

今回の脆弱性情報によると，GET メソッドに限らず POST メソッド，Multipart/form-data の POST メソッド，Cookie による攻撃の可能性もあります。さらに，攻撃者がWASログを細工する可能性もあります。

S主任：それでは，攻撃の有無を確認するには，WAS ログだけでなく，社外向け情報システムの全サーバとFWのログも調査する必要があるね。

表2　攻撃コードの例

項番	攻撃コード	説明
1	GET /app1/app.action?▲▲.directory=webapps/ROOT	WAS ログの出力先を公開ディレクトリ上に変更する。
2	GET /app1/app.action?▲▲.prefix=shell	WAS ログのファイル名を指定する。ファイル名のプレフィックスを“shell”という文字列にして，拡張子を jsp にする。
3	GET /app1/app.action?▲▲.suffix=.jsp	
4	GET /app1/app.action?▲▲.fileDateFormat=1	WAS ログの日付フォーマットの設定を“1”という文字にする。WAS ログのファイル名が，shell1.jsp となる。
5	GET /app1/app.action?a=<%Runtime.getRuntime().exec("XXXX");%>	任意のコマンド“XXXX”を実行させるためのコードが WAS ログに記録される。
6	GET /shell1.jsp	shell1.jsp を呼び出すことで，コマンド“XXXX”を WAS と同じ動作権限で実行する。

注記　▲▲は，“class.classLoader.resources.context.parent.pipeline.first”という文字列を示す。

S主任とTさんは念のため，Q社の社外向け情報システムの全サーバとFWのログを調査したが，不審な内容は見つからなかった。

〔脆弱性への対策〕

S主任とTさんは，脆弱性Xへの対策として，修正モジュールによる方法とWAFによる方法の二つを比較検討した。Q社では，ビジネス上の理由から，Eシステムを5日以内に再稼働させる必要がある。しかし，修正モジュール適用後のWebアプリEの動作検証に10日間を要することが分かった。一方，WAFによる対策は，脆弱性Xを悪用した攻撃を防ぐ効果があり，動作検証を含めて2日間で実施可能と分かった。

そこで，WAF による対策について，更に検討することにした。次は，WAF のルールについてのS主任とTさんの会話である。

S主任：WAF では，どのようにルールを記述するのかな。

Tさん：表3のように記述します。表3の[パターン]列には，正規表現で示された文字列を指定します。当初，①“^class¥..*”という[パターン]がセキュリティ専門家によって公表されましたが，これでは遮断されない攻撃が見つかりました。その後，表3に示す正しい[パターン]が別のセキュリティ専門家によって公表されました。

表3　WAF のルール例

項番	[検証対象]	[パターン]	[動作]
1	b	(^|¥W)[cC]lass¥W	c
2	d	(^|¥W)[cC]lass¥W	e
3	f	(^|¥W)[cC]lass¥W	g

S主任：では，表3どおりに記述することにしよう。他に注意することはあるかな。

Tさん：攻撃ではない HTTP リクエストを遮断してしまう［ h ］に注意する必要があります。例えば，表3のルールでは，“class.abc”を含む HTTP リクエストが遮断されてしまいます。さらに，WAF による対策に加えて，攻撃時のリスク軽減対策として，②現在の WAS の動作権限設定を見直します。

S主任は，修正モジュールが提供されている場合は，一般的には修正モジュール適用による対策が望ましいが，本ケースでは WAF による対策を選択すべきと判断し，経営陣に説明して了承を得た。開発検証用のシステムで③動作検証を実施し，問題ないことを確認後，本番環境のシステムで設定を行い，Eシステムを再稼働させた。

本来ならば，追加した WAF のルールで攻撃を遮断する前に，④本番環境のシステムに追加したルールの[動作]に“検知”を指定し，一定期間運用するのが望ましい。

しかし，今回は緊急対応のため，そのような運用はしなかった。

その後，Q 社では，脆弱性 X の修正モジュール適用による悪影響がないことを確認し，それを適用した。

設問1　E システム及び F システムそれぞれについて，Q 社のビジネスを踏まえて，情報セキュリティの 3 要素のうち重視すべき要素とその理由を，重視すべき要素は 5 字以内，理由は 25 字以内でそれぞれ述べよ。

設問2　本文中の［　a　］に入れる適切な字句を，表 2 中の字句を用いて 15 字以内で答えよ。

設問3　〔脆弱性への対策〕について，(1)～(4) に答えよ。

(1)　表 3 中の［　b　］～［　g　］に入れる適切な字句を，図 2 中の字句を用いて答えよ。

(2)　本文中の下線①に示した[パターン]にマッチする文字列を解答群の中から全て選び，記号で答えよ。

解答群

ア　anObject.class.classLoader　　イ　class.ClassLoader

ウ　class.classLoader　　エ　class['classLoader']

(3)　本文中の［　h　］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　フェールセーフ　　イ　フェールソフト

ウ　フォールスネガティブ　　エ　フォールスポジティブ

(4)　本文中の下線②について，設定をどのように見直すべきか。25 字以内で述べよ。

設問4　本文中の下線③について，WAF に関して具体的に何を検証すべきか。二つ挙げ，それぞれ 30 字以内で述べよ。

設問5　本文中の下線④について，WAF のルールの[動作]に“検知”を指定し，一定期間運用することにはどのような利点があるか。45 字以内で述べよ。

問2　特権 ID の管理に関する次の記述を読んで，設問 1～3 に答えよ。

Y 社は，従業員数 1,000 名の食品製造販売会社であり，一般消費者に食品を通信販売している。Y 社では，顧客情報管理システム（以下，Y システムという）を利用し，顧客情報を管理している。Y システムの保守作業は，開発元であるソフトウェア開発会社の S 社に委託している。保守作業のために，Y 社は S 社に対して，特権 ID の一部（以下，委託用特権 ID という）について使用を許可している。S 社に使用を許可した委託用特権 ID には，OS のシステム管理権限をもつ ID，DBMS の管理権限をもつ ID，及び DBMS 上のデータに対する操作権限をもつ ID（以下，それぞれ，システム管理 ID，DBMS 管理 ID，DBMS 操作 ID という）の 3 種類がある。

Y システムは，4 台の業務サーバ，1 台のデータベースサーバ（以下，DB サーバという）及び Y 社と S 社の PC から構成されており，業務サーバでは Y システムのサービスを提供するためのアプリケーションソフトウェア（以下，業務アプリという）が稼働している。各業務アプリは，DBMS 操作 ID を用いて，DB サーバから顧客情報を取得して Y 社の従業員にサービスを提供している。Y システムのサーバは，Y 社のグループ会社が運営するデータセンタ（以下，YDC という）に設置している。Y システムの構成を図 1 に示す。

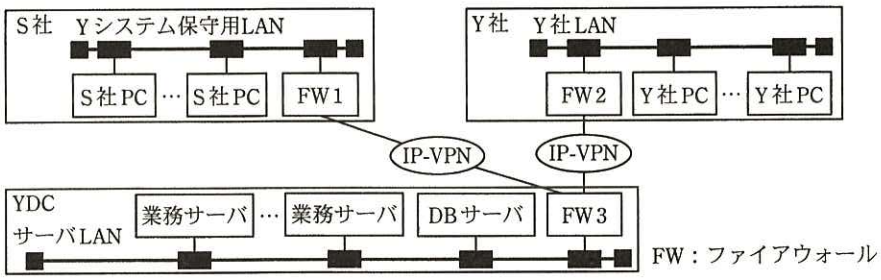


図 1　Y システムの構成

S 社に委託している保守作業は，機能追加などに際しての業務アプリの更新，Y システムに障害が発生した場合の原因調査，Y システムの設定変更などである。保守作業は，次の手順で依頼している。

1. Y 社の管理者が作業依頼書を作成し，S 社へ送付する。
2. S 社では，作業依頼書を受け取ると，S 社の保守チーム責任者（以下，保守責

任者という）が，保守チームメンバから作業担当者（以下，作業者という）を選任する。

3. 保守責任者が，担当する作業ごとに，作業者氏名，作業期間，作業対象サーバ及び作業内容を記載した作業計画書を作成し，Y社に提出する。
4. 作業計画書が承認されて作業期間になると，Yシステム保守用LANからサーバLANへの接続が可能となるよう，YDCに常駐しているY社のグループ会社の作業員（以下，YDC作業員という）が，FW1と接続しているネットワークケーブル（以下，ケーブルAという）をFW3に結線し，S社に通知する。ケーブルAは，保守作業時以外は結線されていない。
5. 作業者は，共用のIDを用いてS社PCにログインした後に，委託用特権IDとパスワードを用いて，S社PCから作業対象サーバにアクセスし，作業する。システム管理IDは，作業対象サーバごとに異なっている。
6. 作業終了後，保守責任者が，作業の完了をY社の管理者に連絡し，作業報告書を提出する。
7. 作業完了の連絡を受けて，Y社の管理者は，ケーブルAをFW3から取り外すようYDC作業員に依頼し，作業報告書によって作業内容を確認する。

システム管理IDとDBMS管理IDのパスワードはY社が半年ごとに変更し，S社に通知している。S社PCとFW1は，S社の資産である。Yシステム保守用LANからサーバLANへのアクセスは，FW3で保守作業に必要となるプロトコルだけに限定しているが，送信元IPアドレスは限定していない。

〔調査の実施と対策方針の策定〕

Y社と同業のC社で，C社の保守作業委託先の従業員が個人情報を不正に持ち出して名簿業者に売却するという情報漏えい事件が起きた。持出しに特権IDが不正に使用されたが，それを検知できなかったというC社の委託先管理の不備が連日報道された。Y社の経営幹部は，C社の事件をきっかけに，自社においても同様の問題が起きる可能性がないか早急に調査をするよう，情報システム部長に指示した。表1に示す調査結果にあるように，Yシステムにおいても委託用特権IDを用いた保守作業に問題があることが判明し，情報システム部のL主任がリーダとなって対策を検討

することになった。

表1　調査結果（概要）

項番	項目	内容
1	委託用特権 ID 使用者の特定	委託用特権 ID が共用されており，使用した者を特定できないおそれがある。また，作業者以外も委託用特権 ID を使用するおそれがある。
2	サーバへのアクセスの制限	Y システム保守用 LAN からサーバ LAN へのアクセスについては，サーバごとのアクセス制御をしていない。そのため，作業計画書に記載された作業対象サーバ以外のサーバにもアクセスできてしまう。
3	委託用特権 ID の操作のモニタリング	作業計画書とアクセスログを突き合わせる手順が定められておらず，委託用特権 ID を使ったアクセスが作業計画書どおりに行われたかをチェックしていない。

〔要件と実現方式の検討〕

L 主任は部下の N 君に次の要件を示した上で，対策を実現する方式の検討を指示した。

要件1：委託用特権 ID の使用を作業者だけに限定すること

要件2：委託用特権 ID を使用した者を特定可能にすること

要件3：作業対象サーバだけにアクセス可能とすること

要件4：許可された作業内容と実際に実施された作業内容を突き合わせ，不正な作業を検知可能にすること

N 君は，要件を満たすためには，委託用特権 ID のパスワードの S 社への通知の停止，個人ごとに付与され特権をもたない ID（以下，個人 ID という）の作業者への付与，及び特権 ID を管理するソフトウェアパッケージの導入から成る対策案を考えた。そこで，ソフトウェアパッケージとして製品 P 及び製品 Q を候補に選び，次の案を検討した。

案1：製品 P を利用する。製品 P は，管理用サーバにインストールするプログラム（以下，プログラム H という）と，PC にインストールするプログラム（以下，プログラム J という）で構成される。管理用サーバはサーバ LAN 上に設置する。作業者は，プログラム J に個人 ID でログインし，プログラム J から作業対象サーバにアクセスし，操作する。作業対象サーバへアクセスする際に使用する委託用特権 ID とパスワードは，プログラム H からプログラム J に転送さ

れ，ログインに際して自動入力される。

案 2：製品 Q を利用する。製品 Q は，管理用サーバにインストールするプログラム（以下，プログラム K という）だけで構成される。管理用サーバはサーバ LAN 上に設置する。作業者は，S 社 PC から個人 ID でプログラム K にログインした後に，プログラム K から作業対象サーバへ自動ログインによってアクセスし，操作する。

検討の結果，N 君は，案 2 の方が製品の導入が容易であると判断し，案 2 による実現方式案をまとめて，L 主任に報告した。実現方式案の概要を表 2 に示す。

表 2　実現方式案の概要

項目	概要
ID の登録	・ [a] が，プログラム K の ID 登録画面において，委託用特権 ID をあらかじめ登録する。また，作業者の個人 ID をあらかじめ登録する。個人 ID は，プログラム K にログインするために付与される。
作業計画の入力と特権 ID の使用申請	・ プログラム K の作業計画入力・委託用特権 ID 使用申請画面において，保守責任者が，作業者の個人 ID，作業者氏名，作業期間，作業対象サーバ及び作業内容を入力し，委託用特権 ID の使用を申請する。
特権 ID の使用許可	・ [a] が，使用申請を確認した後に，委託用特権 ID の使用許可操作を行う。この操作によって，作業対象サーバでの委託用特権 ID の使用が可能になる。
作業対象サーバへのログイン	・ 作業者は，個人 ID を用いてプログラム K にログインし，作業対象サーバへの接続要求を行う。 ・ プログラム K は，作業者の個人 ID による委託用特権 ID の使用が許可されていることを確認する。確認できた場合は，委託用特権 ID とパスワードを用いて作業対象サーバに自動ログインする。
操作履歴の取得	・ プログラム K は，委託用特権 ID による操作履歴を入力コマンドはテキストで，操作画面は動画で記録する。 ・ 作業対象サーバでの操作履歴は管理用サーバに保存される。保存された操作履歴へのアクセスには管理用サーバのシステム管理権限が必要であり，Y 社内の限られた者だけがアクセスできる。 ・ 操作履歴のうち，入力コマンドのテキストは作業対象サーバにも保存される。
作業完了報告	・ 作業終了後，プログラム K の報告画面において，保守責任者が作業完了報告を行う。
特権 ID の使用解除	・ [a] が，作業完了報告を確認した後に，プログラム K の管理画面において，委託用特権 ID の使用解除操作を行う。 ・ 使用解除操作を行うと，作業対象サーバでの委託用特権 ID の使用が不可となる。
作業内容の確認	・ プログラム K の機能によって，操作履歴と委託用特権 ID の使用申請で入力された作業内容を突き合わせ，その結果をレポートに出力する。 ・ [a] が，レポートを確認する。

〔実現方式案の要件の確認〕

L主任はN君の対策案に対して，要件1と要件3について補足説明を求め，要件2と要件4について問題を指摘した。

要件1について，N君は，作業者以外は委託用特権IDを使用できないことを説明し，L主任の了解を得た。

要件2について，L主任は，次のように指摘した。

指摘1：製品Qの導入だけではこの要件を満たすのに不十分である。

指摘2：①使用される委託用特権IDによっては，DBサーバへアクセスした者をDBサーバ上のアクセスログから特定することができない。

指摘1に対してN君は，追加対策を検討すると回答した。また，指摘2に対しては，DBサーバ上のアクセスログを利用せずとも，DBサーバへアクセスした者を特定できることとその理由を回答した。

要件3について，N君は，［ b ］からは［ c ］へのアクセスだけを許可するようにFW3の設定を変更することによって，アクセス先を作業対象サーバに限定できると説明し，L主任の了解を得た。

要件4について，L主任は，作業者が作業対象サーバ上のアクセスログを書き換えると，作業計画の作業内容以外の操作，つまり不正操作が検知できなくなるのではないかと指摘した。これに対してN君は，②不正操作を検知できることとその理由を回答した。

〔追加対策の検討〕

N君は，要件2についての指摘1を踏まえて，次の追加対策をL主任に提案した。

・③S社におけるプログラムKの個人IDの管理状況をY社が確認する。
・④委託用特権IDを使った者が特定されることをプログラムKのログイン画面に表示し，作業者に周知させる。

最後にL主任は，案2を採用すべき理由を再確認した。N君は，要件を満たすためには製品を適切に運用するための資産管理が必要だが，Y社の状況においては⑤案1に比べて案2の方が必要な資産管理を実施しやすいと説明した。L主任は，案2に

よる実現方式案と追加対策を承認した。

〔対策の実施〕

案 2 による実現方式案と追加対策は，経営幹部に報告され，実施された。対策によって，保守作業時のケーブル A の結線と取外しが不要となった。

設問 1　表 2 中の［　a　］に入れる適切な字句を，10 字以内で答えよ。

設問 2　〔実現方式案の要件の確認〕について，(1)～(3)に答えよ。

(1) 本文中の下線①について，DB サーバへアクセスした者を特定することができない委託用特権 ID を 10 字以内で答えよ。また，特定することができない理由を 35 字以内で述べよ。

(2) 本文中の［　b　］，［　c　］に入れる適切な機器名を答えよ。

(3) 本文中の下線②について，不正操作を検知できる理由を 35 字以内で述べよ。

設問 3　〔追加対策の検討〕について，(1)～(3)に答えよ。

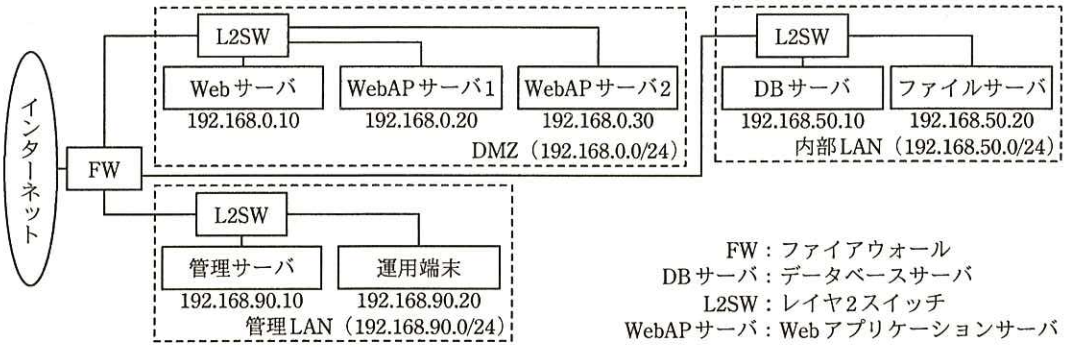
(1) 本文中の下線③について，具体的には何を確認すべきか。35 字以内で述べよ。

(2) 本文中の下線④には，顧客情報の不正持出し対策として何と呼ばれる効果があるか。効果の名称を“効果”という字句を含めて 5 字以内で答えよ。

(3) 本文中の下線⑤について，案 2 の方が資産管理を実施しやすい理由を 40 字以内で述べよ。

問3　Web サイトにおけるインシデント対応に関する次の記述を読んで，設問 1～4 に答えよ。

W 社は，精密機器を製造している従業員数 500 名の会社である。W 社では，取引先との間で設計データを共有するために Web サイト（以下，サイト X という）を利用している。サイト X は，W 社の情報システム部が開発，運用しており，W 社の従業員と取引先の従業員が利用している。サイト X のネットワーク構成を図 1 に，システム概要を図 2 に示す。



注記 1　192.168.0.0/24，192.168.50.0/24，192.168.90.0/24 は，ネットワークアドレスを示す。
注記 2　DMZ の各サーバに対しては FW で NAT の設定がされている。

図 1　サイト X のネットワーク構成

・Web サーバでは，インターネットに静的コンテンツを公開している。
・負荷分散のために，WebAP サーバ 1 及び WebAP サーバ 2 の 2 台構成になっており，Java で開発した Web アプリケーションソフトウェア（以下，Web アプリケーションという）がサーブレットコンテナで稼働している。Web アプリケーションは，JDBC[1]接続を使って DB サーバに，OS のファイル共有機能を使ってファイルサーバにそれぞれアクセスする。
・WebAP サーバ 1 及び WebAP サーバ 2 のサーブレットコンテナの管理画面には，管理画面用の利用者 ID でログインできる。管理画面へのログインは，ベーシック認証で行われる。成功時は 200，失敗時は 401 のステータスコードを返す。管理画面では，Web アプリケーションのアップロードと配置ができる。
・DB サーバでは，DBMS の監査ログを取得するよう設定している。
・管理サーバでは，各サーバに導入したエージェントソフトを使ってログを集中管理している。
・運用端末では，ファイル共有とリモートデスクトップのサービスを使用して各サーバを操作できる。
・各サーバ及び運用端末では，OS として Windows を使っている。各サーバ及び運用端末には，利用者 ID として，“administrator” と “unyou” の二つを用意している。いずれも管理者権限の利用者 ID である。
・サーブレットコンテナのプロセスは，“administrator” の権限で動作しており，管理画面と Web アプリケーションも，“administrator” の権限で動作する。
・各サーバ及び運用端末では，Web サーバ上で稼働している NTP サーバとの間で，NTP を用いて時刻同期をしている。

注 1)　JDBC は，Java からデータベースに接続するための API である。

図 2　サイト X のシステム概要

〔セキュリティインシデントの発生〕

ある日，DMZ に設置している 3 台のサーバで，同様のタスク実行失敗を示すイベントが出力されたので，サイト X の運用を担当している B 氏は，システム障害として調査を行った。DMZ の各サーバのイベントログを表 1 に示す。

表 1　DMZ の各サーバのイベントログ

日時	ログメッセージ
2015/01/22 12:52:00	タスクスケジューラは，利用者 ID “administrator” の “printer” タスクを開始できませんでした。

調査の結果，図 3 の事象が確認できたことから，B 氏は，不正侵入のセキュリティインシデントが発生したと判断した。

・OS のタスクスケジューラに，業務上必要のないタスクが登録されており，そのタスクは実行が失敗していた。
・“C:¥Temp¥printer” の場所に，“info.bat” と “info.txt” というファイルが作成されていた。“info.bat” は，バッチファイルであり，システム構成情報と利用者情報を取得するコマンドを実行して，結果を “info.txt” という名前のファイルに出力する。

図 3　DMZ の各サーバで発生した事象

B 氏は，DMZ のサーバ 3 台をネットワークから切り離し，取引先にサイト X の停止を通知した後，セキュリティ担当 A 氏の協力を得て，侵入経路の調査を開始した。

〔侵入経路の調査〕

A 氏は，DMZ に設置しているサーバの OS へのログイン履歴を基に，タスク実行失敗を示すイベントが出力された日時の前後のログを調査して，どのサーバが最初に侵入されたかを特定した。Web サーバ，WebAP サーバ 1 及び WebAP サーバ 2 の 3 台の 2015 年 1 月 1 日以降のログイン履歴は，表 2～4 のとおりである。

表 2　Web サーバのログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/07 19:30:16	192.168.90.20	unyou	成功
2015/01/07 19:38:14	192.168.90.20	unyou	成功
2015/01/22 12:03:00	192.168.90.20	unyou	成功
2015/01/22 12:23:00	192.168.90.20	unyou	成功
2015/01/22 12:42:07	192.168.0.20	administrator	成功
2015/01/22 18:11:25	192.168.90.20	unyou	成功

表 3　WebAP サーバ 1 のログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/05 19:28:46	192.168.90.20	unyou	成功
2015/01/08 20:23:00	192.168.90.20	unyou	成功
2015/01/22 12:32:20	192.168.0.30	administrator	成功

表 4　WebAP サーバ 2 のログイン履歴

日時	接続元 IP アドレス	利用者 ID	ログインの成功失敗
2015/01/06 19:28:21	192.168.90.20	unyou	成功
2015/01/06 19:30:16	192.168.90.20	unyou	成功
2015/01/23 12:03:00	192.168.90.20	unyou	成功

次は，侵入経路の調査の過程における A 氏と B 氏の会話である。

A 氏：ログイン履歴には，複数の利用者 ID のログインが記録されています。利用者 ID はどのように使い分けているのですか。

B 氏：運用では，“unyou”を使用しており，“administrator”は使用していません。

A 氏：そうだとすると，“administrator”という利用者 ID を使ってサーバにログインした者が攻撃者であると推測できます。［ a ］から［ b ］に，［ b ］から［ c ］にという順番でログインしていますね。

B 氏：それでは，最初に侵入されたサーバは，［ a ］ということでしょうか。

A 氏：その可能性が高いですね。侵入された原因を特定するためには，［ a ］のアクセスログを調査する必要があります。

B 氏：ところで，ログイン履歴を見ると，失敗することなく短時間で他のサーバへのログインが成功しています。攻撃者は，どのような方法で他のサーバにロ

グインしたのでしょうか。

A 氏：DMZ の各サーバには，“unyou”，“administrator” という利用者 ID が，全サーバに同じパスワードで設定されているようです。そうした設定では，あるサーバから他のサーバにアクセスする際，自動的にログインが行われます。攻撃者は，そのような OS の仕様を利用して，他のサーバにもログインしたようです。

〔侵入された原因の特定〕

A 氏は，インターネットから侵入された原因を特定するために，［ a ］のアクセスログを調査した。担当者にヒアリングしたところ，設定に誤りがあり，インターネットから管理画面にアクセスできるようになっていたことが分かった。［ a ］のアクセスログのうち，攻撃者の IP アドレスからのものを表 5 に示す。調査の結果，①サーブレットコンテナの管理画面に対して，よく使われる利用者 ID とパスワードでログインが試行され，その結果，ログインが成功したものと推測された。管理画面から，バッチファイルを［ a ］にアップロードされた後，タスクが登録されたり，バッチファイルが実行されたりしたと推測された。

表5 [a] のアクセスログ

No.	時刻	リクエスト	ステータスコード	応答のバイト数
1	10:36:04	GET /test/ HTTP/1.1	404	1,277
2	10:36:23	GET /demo/ HTTP/1.1	404	1,277
3	10:59:12	GET /manager/html HTTP/1.1	401	2,550
4	10:59:12	GET /manager/html HTTP/1.1	401	2,550
5	10:59:12	GET /manager/html HTTP/1.1	401	2,550
6	10:59:12	GET /manager/html HTTP/1.1	401	2,550
7	10:59:13	GET /manager/html HTTP/1.1	401	2,550
8	10:59:13	GET /manager/html HTTP/1.1	401	2,550
9	10:59:13	GET /manager/html HTTP/1.1	401	2,550
10	10:59:13	GET /manager/html HTTP/1.1	401	2,550
11	10:59:14	GET /manager/html HTTP/1.1	200	19,689
12	11:02:09	GET /manager/html HTTP/1.1	200	19,689
13	11:02:27	POST /manager/html/upload HTTP/1.1	200	21,453
14	11:02:34	GET /demo/index.jsp HTTP/1.1	200	2,588
15	11:39:23	GET /demo/index.jsp HTTP/1.1	200	2,588
16	11:39:33	GET /demo/index.jsp?sort=1&dir=C%3A%5C HTTP/1.1	200	3,453
17	11:39:47	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp HTTP/1.1	200	2,129
18	11:39:52	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp%5Cprinter HTTP/1.1	200	1,347
19	11:41:02	POST /demo/index.jsp HTTP/1.1	200	3,697
20	11:42:05	POST /demo/index.jsp HTTP/1.1	200	3,697
21	11:42:09	POST /demo/index.jsp HTTP/1.1	200	2,506
22	11:42:18	POST /demo/index.jsp HTTP/1.1	200	2,506
23	11:42:39	GET /demo/index.jsp?sort=1&dir=C%3A%5CTemp%5Cprinter HTTP/1.1	200	1,896

注記　日付は，2015年1月22日である。

次は，[a] のアクセスログの調査過程における A 氏と B 氏の会話である。

A 氏：侵入された後，demo ディレクトリに index.jsp という名前のファイルをアップロードされたようです。アクセスログの No. [d] のステータスコードが [e] であり，No. [f] のステータスコードが [g] であるということから，demo ディレクトリは攻撃者が No. [f] の直前で作成したことが分かります。

B 氏：確かに，[a] には，demo ディレクトリは元々ありませんでした。

A 氏：index.jsp を調査したところ，攻撃ツールであることが分かりました。指定した

ファイルをインターネット上のサーバにアップロードする機能，OS のファイル共有機能を使って他のサーバにファイルを転送する機能，OS のファイル共有機能を使って他のサーバ上で OS コマンドを実行する機能，及び DBMS に対して SQL を発行する機能をもっています。

〔影響範囲の特定〕

A 氏は，内部 LAN 及び管理 LAN への影響を特定するために，FW のフィルタリングルールを確認して，侵入されたサーバからどの範囲がアクセス可能だったかを調査することにした。FW のフィルタリングルールを表 6 に示す。W 社のポリシでは，業務上必要なサービスだけを FW で許可することになっているが，②FW のフィルタリングルールにはポリシを満たしていないものがあることが判明した。

表 6　FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
1	インターネット	192.168.0.10	HTTP	許可
2	インターネット	192.168.0.20，192.168.0.30	HTTP，HTTPS	許可
3	192.168.0.20，192.168.0.30	192.168.50.10	JDBC 接続	許可
4	192.168.0.20，192.168.0.30	192.168.50.20	ファイル共有	許可
5	192.168.90.20	192.168.0.0/24，192.168.50.0/24	全て	許可
6	192.168.90.10	192.168.0.0/24，192.168.50.0/24	ログ収集	許可
7	192.168.50.0/24，192.168.90.0/24	192.168.0.10	NTP	許可
8	192.168.0.10	公的機関の NTP サーバ	NTP	許可
9	全て	全て	全て	拒否

注記 1　項番が小さいものから順に，最初に一致したルールが適用される。
注記 2　FW は，ステートフルインスペクション型のものである。
注記 3　全てのルールについて，ログを取得する設定となっている。

次に，A 氏は，タスク実行失敗を示すイベントが発生した日以降の，FW のログを調査し，内部 LAN 及び管理 LAN への影響がないことを確認した。

〔対策とシステム再稼働〕

A 氏と B 氏は，影響範囲が DMZ のサーバ 3 台だけであったことから，それらのサーバの再構築を行った後，次の対策を実施した。

(a)　WebAP サーバ 1 と WebAP サーバ 2 に，図 4 のアクセス制御の設定を行うことで，送信元の IP アドレスが 127.0.0.1 である場合だけ，サーブレットコンテナの管

理画面へのアクセスを許可する。

```
<Location /manager/>
Order deny,allow
Deny from all
Allow from 127.0.0.1
</Location>
```

図4　アクセス制御の設定

(b)　各サーバの利用者 ID “administrator” を無効化し，利用者 ID “unyou” は，サーバごとに異なる利用者 ID に変更し，さらに，パスワードもサーバごとに異なるものに変更する。

W 社では，B 氏が経営幹部に不正アクセスの調査結果を報告し，承認を得てシステムを再稼働させた後，取引先に通知し，インシデント対応を完了した。

設問1　本文中の［ a ］～［ c ］に入れるサーバ名を，図1中の字句を用いて答えよ。

設問2　〔侵入された原因の特定〕について，(1)，(2)に答えよ。

(1)　本文中の［ d ］～［ g ］に入れる適切な数値を答えよ。

(2)　本文中の下線①のように推測された理由を，表5のログに基づいて 60 字以内で述べよ。

設問3　〔影響範囲の特定〕について，(1)，(2)に答えよ。

(1)　内部 LAN への影響を調査するには，FW のどのフィルタリングルールで取得されるログを確認すればよいか。該当するものを全て，表 6 の項番で答えよ。

(2)　本文中の下線②について，ポリシを満たしていないことが判明したルールはどれか。表 6 の項番で答えよ。また，当該ルールがポリシを満たすように設定すべきサービスを二つ答えよ。

設問4　〔対策とシステム再稼働〕について，本文中の(a)，(b)の対策は，今回のインシデントにおける一連の攻撃のうち，どのような攻撃を防ぐために実施するものか。(a)，(b)について，防ぎたい攻撃をそれぞれ 40 字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。

午