問1　パケットログ解析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名の小売業者である。A社では，ネットワークの構築，運用を自社で行っている。ある朝，社内LANからインターネット上のWebページを閲覧しているときの応答が遅いといった苦情が寄せられ，システム管理部門のJ主任と運用担当のK君が調査を行うことになった。

〔原因調査と対処〕

J主任とK君は，Webページの閲覧状況の確認から始めることにした。

K君　：ブラウザでインターネット上のWebページを閲覧しようとすると，図1に示す状態が長く続き，表示までに時間が掛かります。

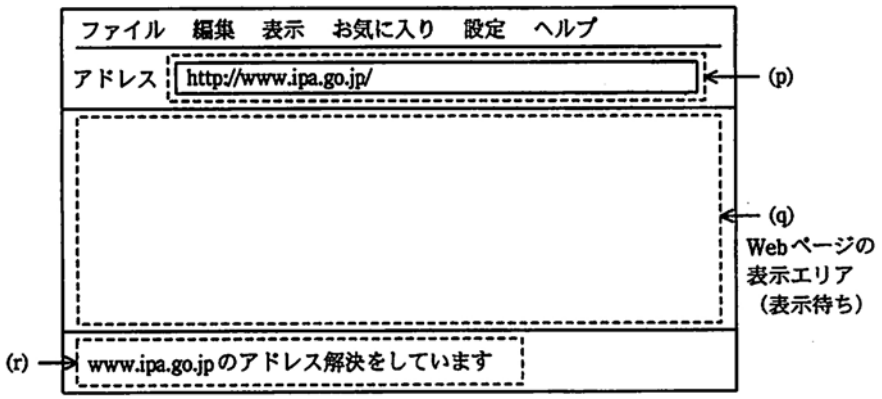


図1　Webページを閲覧しようとしたときのブラウザの状態

J主任：なるほど，図1中の［　a　］を見ると，DMZ上のDNSサーバに問題があるようです。当社の社内ネットワークの構成は図2のとおりです。設置してあるパケットモニタの，該当する時間帯のログを解析してみましょう。

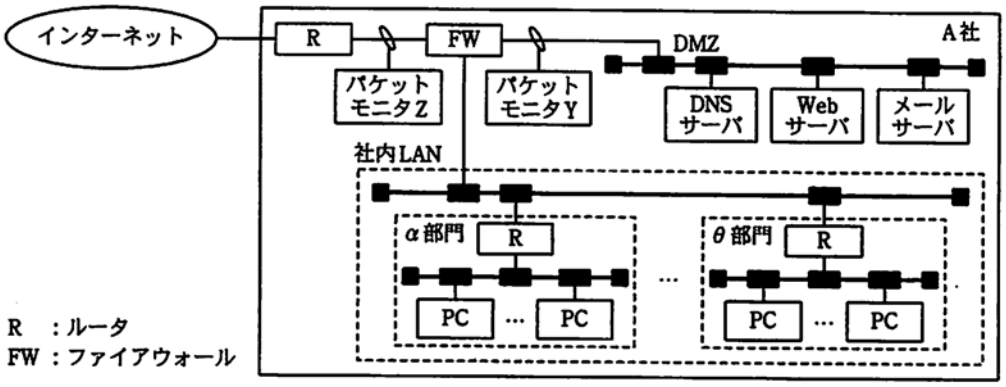


図2　A社の社内ネットワークの構成

K君　：パケットモニタYには，DNSクエリとそれに対応するDNSクエリレスポン

スが多量に記録されていました。しかし，パケットモニタ Z には，DNS クエリを伴わない DNS クエリレスポンスが多量に記録されていました。パケットモニタ Z のログを図 3 に示します。

番号	経過時間(秒)	送信元	あて先	プロトコル	詳細	
1	0.000	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, No such name	(Ⅲ)
2	0.001	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, No such name	
3	0.003	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A q1.q2.q3.q4	(Ⅳ)
4	0.004	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A q1.q2.q3.q4	
5	0.007	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A s1.s2.s3.s4	(Ⅴ)
6	0.008	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A s1.s2.s3.s4	
		(Ⅰ)	(Ⅱ)			

p1.p2.p3.p4：DMZ上のDNSサーバのIPアドレス
q1.q2.q3.q4：DMZ上のWebサーバのIPアドレス
r1.r2.r3.r4，s1.s2.s3.s4：インターネット上のIPアドレス

図 3　パケットモニタ Z のログ（抜粋）

J 主任：このようなログは，社内 LAN 上の PC が DNS クエリを送信するときに自身の IP アドレスを [b] の IP アドレスに [c] した場合に記録されます。
K 君　：不正な DNS クエリが多量に DMZ 上の DNS サーバに送りつけられたことで，Web ページを閲覧するときの応答が遅くなったのですね。確かに，すべての社内 PC からの名前解決を，DMZ 上の DNS サーバが担っていますから。
J 主任：こういった通信は [d] 攻撃と呼ばれています。至急，不正なパケットを棄却する設定をすべての部門のルータに適用してください。
K 君　：はい，分かりました。
J 主任：こうした事象は，ウイルス感染によってよく引き起こされます。今回の事象以外にも，異常な通信が観測される可能性があります。社内 LAN に接続されているすべての部門のルータにパケットモニタを設置して，原因となっている社内 PC を特定してください。
K 君　：ルータへの設定が終わり次第，パケットモニタによる調査を開始します。
J 主任：ところで，図 3 中の [e] と [f] の記録から，DMZ 上の DNS サーバが攻撃の踏み台に利用される危険性があることが分かります。①DINS サーバの不適切な設定も修正しておくべきですね。
K 君　：はい，分かりました。

〔異常 PC の特定〕
K 君は社内 LAN に接続されたすべての部門のルータの配下にパケットモニタを設置して，異常な通信の監視を開始した。

番号	経過時間(秒)	送信元	あて先	プロトコル	詳細	
1	0.000	a1.a2.a3.a4	b1.b2.b3.b4	DNS	Query, MX ipa.go.jp	
2	0.328	b1.b2.b3.b4	a1.a2.a3.a4	DNS	Query response, MX 10 ipa.go.jp	
3	1.503	a1.a2.a3.a4	c1.c2.c3.c4	DNS	Query, MX jitec.ipa.go.jp	
4	1.632	c1.c2.c3.c4	a1.a2.a3.a4	DNS	Query response MX 20 jitec.ipa.go.jp	(VI)
5	1.982	a1.a2.a3.a4	d1.d2.d3.d4	DNS	Query, MX sec.ipa.go.jp	
6	2.036	d1.d2.d3.d4	a1.a2.a3.a4	DNS	Query response MX 10 sec.ipa.go.jp	
⋮	⋮	⋮	⋮	⋮	⋮	
16	2.421	a1.a2.a3.a4	e1.e2.e3.101	Netbios	TCP-SYN	
17	2.532	a1.a2.a3.a4	e1.e2.e3.102	Netbios	TCP-SYN	(VII)
18	2.592	a1.a2.a3.a4	e1.e2.e3.103	Netbios	TCP-SYN	
19	2.604	a1.a2.a3.a4	e1.e2.e3.104	Netbios	TCP-SYN	
⋮	⋮	⋮	⋮	⋮	⋮	

a1.a2.a3.a4：α部門内のIPアドレス
b1.b2.b3.b4，c1.c2.c3.c4，d1.d2.d3.d4，e1.e2.e3.101～104：インターネット上のIPアドレス

図4　社内 LAN からインターネットに向けたパケットログ（抜粋）

K 君　：図 4 がα部門に設置したパケットモニタのログです。
J 主任：②図 4 中の(VI)に示した箇所に，通常の社内 PC には見られない不審な通信挙動が記録されていますね。これは［　g　］におけるアドレス探索に見られる特徴です。また，図 4 中の(VII)に示した箇所にも，不審な通信挙動が記録されていますね。(VII)に示す通信によって，③通信の異常な偏りが発生します。
K 君　：なるほど，a1.a2.a3.a4 に該当する社内 PC が，原因となっている PC ですね。
J 主任：こうした視点で，ほかの部門に設置したパケットモニタのログも確認してみましょう。

〔異常 PC の対処と今後の対策〕
J 主任と K 君は，全部門のパケットモニタのログを調べた結果，IP アドレスが a1.a2.a3.a4 のログだけに異常が見られたことから，この IP アドレスの PC への対処を開始した。この対処として，通信プロセス名，実行ファイル名，通信のあて先の IP アドレスとポート番号を記録する通信プロセスモニタを，該当する Pc に設定して監視を行った。

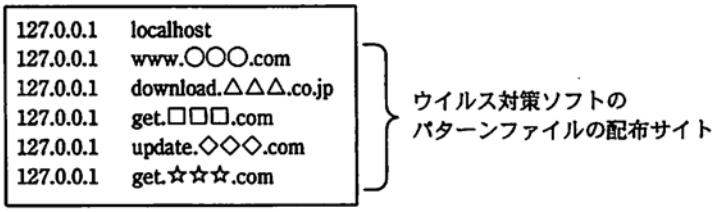
K 君　：該当する PC に設定した通信プロセスモニタのログから，起動していた④不審な通信プロセスを特定でき，それがウイルスであることが分かったので，その実行ファイルを削除しておきました。この PC ではウイルス対策ソフトが起動しており，そのパターンファイルの自動更新も設定されていました。検知できないウイルスもあるのですね。
J 主任：そのとおりです。昨今，次々と新たなウイルスが作られているので，完全な検知が難しくなっています。
K 君　：該当する PC にログインしたまま 1 日間操作しないで通信状況を監視したところ，DNS パケットだけでなくすべての TCP/UDP パケットの発信が止まったことを確認しました。
J 主任：それは変ですね。当社の設定では，操作しない PC でも PC にログインしていれば，⑤TCP/UDP パケットは自動的に発信されます。hosts ファイルが改ざ

んされているのではないでしょうか。

K 君　：図 5 が hosts ファイルです。確かに，ウイルス対策ソフトのパターンファイルの配布サイト情報が追加されているようです。

J 主任：hosts ファイルの改ざん以外にも，ほかの設定ファイルの改ざんや未知のウイルスへの感染の可能性があります。OS の再インストールで対処してください。

K 君　：はい，分かりました。



注　図中の“○○○”，“△△△”，“□□□”，“◇◇◇”，“☆☆☆”は，特定の文字列を表す。

図 5　異常 PC の hosts ファイル

その後，J 主任と K 君は，ウィルスの感染経路を特定し，再発防止策を講じた。

設問 1　〔原因調査と対処〕について，(1)～(4)に答えよ。

(1)本文中の [a] に該当する最も適切な箇所を図 1 中の(p)～(r)|から選び，記号で答えよ。

(2)本文中の [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。また，本文中の [c] に入れる適切な字句を，5 字以内で答えよ。

b に関する解答群

ア　DMZ 上の DNS サーバ　　イ　DMZ 上の Web サーバ

ウ　インターネット上

(3)本文中の [d] 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　DNS cache poisoning　　イ　DNS reflection

ウ　総当たり　　エ　ファーミング

(4)本文中の [e] に該当する適切な箇所を図 3 中の(Ⅰ)，(Ⅱ)から，[f] に該当する適切な箇所を(Ⅲ)～(V)からそれぞれ選び，記号で答えよ。また，本文中の下線①について，どのような修正を行うべきか。50 字以内で述べよ。

設問 2　〔異常 PC の特定〕について，(1)，(2)に答えよ。

(1)本文中の下線②の不審な通信挙動について，30 字以内で具体的に述べよ。また，本文中の [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　DNSamplicatilon 攻撃　　イ　UDP ポートスキャン

ウ　ゾーン転送　　エ　迷惑メール送信

(2)本文中の下線③の通信の異常な偏りについて，該当するものを解答群の中から二つ選び，記号で答えよ。

解答群

ア　DNS クエリなしに通信を試みたあて先アドレス数の増加

イ　TCR-RST パケット受信数の低下

ウ　コネクション接続成功率の低下

エ　平均パケットサイズの増加

設問 3　〔異常 PC の対処と今後の対策〕について，(1)，(2)に答えよ。

(1)本文中の下線④について，K 君はどのような通信挙動のプロセスに注目したか。40 字以内で述べよ。

(2)本文中の下線⑤について，正常な PC を放置した場合，どのような TCP/UDP パケットが観測されるべきなのか。図 5 を考慮して 40 字以内で述べよ。

問 2　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 1〜3 に答えよ。

B 社は，従業員数 400 名で昨年度の年間売上高が 80 億円の菓子製造業者であり，インターネット上の Web 販売システムにおいて自社製品の販売を行っている。この Web 販売システムの管理は社内のシステム運用部が行っている。Wbb 販売システムの構成を図 1 に，Web 販売システムの概略仕様を図 2 に示す。

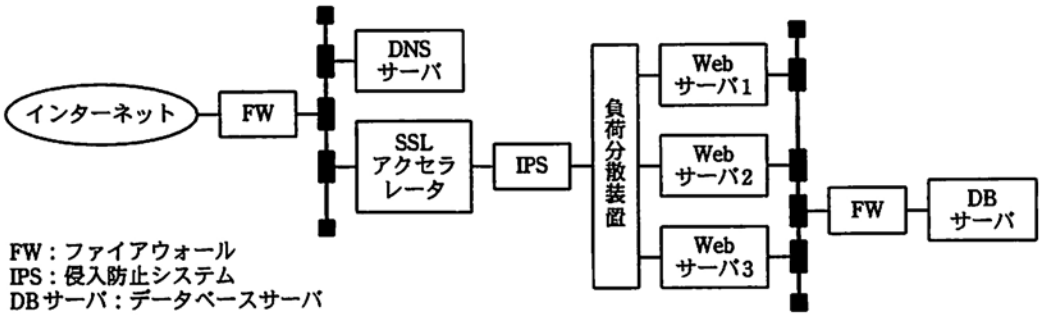


図 1　B 社の Web 販売システムの構成

(a) Web サーバ上では，主に HTTP 送受信を処理する Web サーバプログラムと，主に DB サーバと連携して動的コンテンツ生成を行う Web アプリケーションが稼働している。

(b) Web サーバプログラムと Web アプリケーションは，限定された権限でも動作可能である。

(c) SSL 暗号化，復号処理は SSL アクセラレータで行っている。

(d) いずれの FW も，アプリケーション層を解釈する機能はもっていない。

(e) DB サーバには，顧客の個人情報（住所，氏名，電話番号など機密性の高い情報）が格納されており，Web サーバ上の Web アプリケーションから参照，更新される。

(f) Web サーバプログラムは，システム管理者権限で動作している。

(g) Web 販売システムの開発のために，B 社のシステム開発部で図 1 とほぼ同一構成である動作試験用システムを別に用意している。

図 2　B 社の Web 販売システムの概略仕様（抜粋）

〔脆弱性情報の発見〕

B 社は情報セキュリティ専門会社からセキュリティ情報の提供を受けている。ある日，Web 販売システムで使用中の Web サーバプログラムに脆弱性が発見されたとの情報が提供された。この Web サーバプログラムの脆弱性情報を図 3 に示す。

・HTTP POST メソッドにおいて，HTTP ヘッダ内に RFC で定義されていない“X-Sender”というヘッダフィールドを指定することで，任意の OS コマンドを実行させることが可能である。その際，OS コマンドは Web サーバプログラムの動作権限で実行される。
・そのほかのメソッドでは，この脆弱性は報告されていない。
・Exploit コードが公開されている。

図 3　Web サーバプログラムの脆弱性情報（抜粋）

〔脆弱性の評価〕

次は，Web サーバプログラムの脆弱性に関する，システム運用部の P 君と Q 課長との会話である。

P 君　：当社が Web 販売システムで使用している Web サーバプログラムに脆弱性が存在することが報告されました。
Q 課長：まず対処の緊急性を検討しよう。図 4 に示す当社の脆弱性評価規程に当てはめると判定結果はどうなるのか。
P 君　：私は損害金額の算出が難しい場合の基準を適用し，①“緊急”に相当すると判定しました。

・ソフトウェアの脆弱性評価は，対処の緊急性の観点から，緊急，重要，注意の 3 段階判定とし，次の表に示す定義に基づき判定する。

表　脆弱性評価基準表

評価	脆弱性によって引き起こされることが想定される被害	
	損害金額が算出可能な場合 (*1)	損害金額の算出が難しい場合 (*2)
緊急	被害によって年間売上高の 1%に相当する金額を超える経済的損害が発生する。	次の事象によって顧客からの信頼を大きく損なう。 (1) 機密性の高い情報が漏えいする。 (2) システムの機能が全面的に停止する。
重要	被害によって年間売上高の 1%に相当する金額以下の経済的損害が発生する。	次の事象によって顧客からの信頼を損なう。 (1) 機密性の低い情報が漏えいする。 (2) システム性能が部分的に低下する。 (3) ログの内容が漏えいする。
注意	経済的損害は発生しない。	顧客からの信頼を損なうおそれは少ない。 例)・システム設定ファイルの内容が漏えいする。 ・CGI スクリプトファイルのソースコードが漏えいする（ほかの被害にはつながらない）。

注 損害金額が算出可能な場合は (*1) を使用し，算出が難しい場合は (*2) を使用して判定する。損害金額の算出には，間接的損害は算入しない。

図 4　B 社の脆弱性評価規程（抜粋）

Q 課長：私も“緊急”と判定する。それに，②図 3 の脆弱性情報から考えても。攻撃が実際に行われる可能性が高い。早速，対策の検討を開始しよう。運用管理クループリーダの S 君を呼んでくれ。

〔暫定的対策の検討〕

Q 課長：それでは今回の脆弱性について対策の検討を始めよう。P 君，考えられる対策には何があるのか。

P 君　：現在，開発元から Web サーバプログラムの修正プログラムが提供されていないので暫定的対策となりますが，POST メソッドでのアクセスを拒否する方法が考えられます。

S 君　:Web 販売システムで POST メソッドでのアクセスを拒否すると，HTML 文書の [a] 要素内に利用者が入力したデータを受け付けることができず，製品の販売ができなくなってしまいます。HTML 文書を修正して，POST メソッドを GET メソッドに置き換えた上で POST メソッドでのアクセスを拒否するという対策であれば，製品販売も続けられます。

Q 課長：いや，GET メソッドを使用するとクエリストリングに利用者が入力した情報が含まれることとなり，POST メソッドと比較して③新たな情報漏えいの可能性が生じる。その方法ではなく，Web 販売システムに設置してある IPS に暫定的対策として拒否条件を追加することはできないのか。

P 君　：この IPS では，④シグネチャをカスタマイズすることで実現可能だと思われます。

S 君　：IPS による対策であれば，システム運用上大きな問題はないと思われます。

Q 課長：それでは，IPS による暫定的対策を実施することとする。P 君は IPS のカスタマイズの準備にかかってくれ。また，修正プログラムの適用が完了するまで，Web アクセスログ，IPS の検出ログの確認頻度を 1 日 3 回に増やして，Web 販売システムに関する監視を強化することとする。

この検討の後，速やかに IPS による暫定的対策を実施した。

〔修正プログラムの適用〕

暫定的対策を実施した日から 10 日後に，P 君は，脆弱性に対応する修正プログラムの提供が開始されたことを Q 課長に報告した。報告には S 君も同席した。

P 君　:Web サーバプログラムの脆弱性に対応する修正プログラムの提供が開始されました。早急に，Web サーバに適用したいと思います。

Q 課長：今回の脆弱性と対策について営業課の T 課長に説明したところ，“1 週間前に当社の製品がテレビ番組で取り上げられた。その直後から，Web 販売システムでの販売が著しく伸びているので，システムを停止されては困る。”との意見が返ってきた。この意見も尊重した上で適用時期と適用方法について検討してほしい。

P 君　：しかし，暫定的対策は完全なものとはいえず，速やかに修正プログラムを適用すべきだと考えます。例えば，夜間など一時的に負荷が軽くなる時間帯を選んで適用作業をしてはいかがでしょうか。

S 君　：過去 1 週間の傾向では，昼間の時間帯はサーバ 3 台の処理能力がフルに必要なほどアクセスが多いのですが，深夜 2 時から朝 8 時までの間はアクセスが

少なく，サーバ 1 台でも処理が可能な状態となっています。

P 君　：修正プログラムの適用に必要な作業時間は，サーバ 1 台当たり何時間と想定されるのでしょうか。

S 君　：サーバの停止から修正プログラムの適用，再起動まで含めておおよそ 30 分程度で完了すると見込まれます。

P 君　：それでは，図 5 に示す手順で作業を行えば，Web 販売システムを停止させることなく修正プログラムを適用することができるのではないでしょうか。

次の(1)～(3)の手順を，Web サーバ 1～3 の全 3 台に対して順次適用する。
(1) 対象となる Web サーバを [b] ために，負荷分散装置の設定を変更する。
(2) 対象となる Web サーバの Web サーバプログラムに修正プログラムを適用する。
(3) 負荷分散装置の設定を元に戻す。

図 5　修正プログラム適用手順案

Q 課長：確かに，この手順であれば修正プログラムの適用が可能だ。⑤T 課長に修正プログラム適用手順，実施日時を説明した上で速やかに修正プログラムの適用を実施しよう。

その後，T 課長への説明も済み，図 5 の手順によって速やかに修正プログラムの適用を実施することになった。その結果，Web 販売システムの停止を伴うことなく脆弱性の対策が完了した。

設問 1　〔脆弱性の評価〕について，(1)，(2) に答えよ。

(1) 本文中の下線①において，P 君が脆弱性について緊急”に相当すると判定した具体的根拠は何か。50 字以内で述べよ。

(2) 本文中の下線②において，Q 課長が，攻撃が実際に行われる可能性が高いと考えた根拠は何か。25 字以内で述べよ。

設問 2　〔暫定的対策の検討〕について，(1) ～ (4) に答えよ。

(1) 本文中の [a] に入れる適切な HTML の要素名を，英文字 6 字以内で答えよ。

(2) 本文中の下線③について，情報漏えいの可能性が生じる理由を，“クエリストリング”という語を用いて 70 字以内で述べよ。

(3) 本文中の下線④について，暫定的対策を実現するために拒否条件として IPS に登録すべきシグネチャの具体的内容を，40 字以内で述べよ。

(4) 本文で述べている IPS による対策に加えて，図 2 中の仕様の一部の設定を変更する対策も可能である。この一部とは図 2 中の (a) ～ (g) のいずれであるかを記号で答えよ。また，対策の内容について 30 字以内で述べよ。

設問 3　〔修正プログラムの適用〕について，(1)，(2) に答えよ。

(1) 図 5 中の [b] に入れる適切な字句を，15 字以内で述べよ。

(2) 本文中の下線⑤について，Web 販売システムにおける修正プログラム適用後のトラブルを予防するために，T 課長への説明の前に実施すべき作業がある。適切と思われる作業内容を，40 字以内で述べよ。

問3　アプリケーション開発時の脆弱性対策に関する次の記述を読んで，設問1，2に答えよ。

C社は，一般消費者向けにファックスや電話による，生活用品の通信販売を行っている，従業員数50名の会社である。C社の企画開発課は申込方法の多様化を目的として，インターネットで申込みを受けるためのXシステム（図1）を開発してきた。Xシステムでは，Webアプリケーション（以下，Webアプリという）のログイン画面で，利用者IDとパスワードによって利用者認証を行う。C社の開発ポリシには，サービス開始前に第三者によるセキュリティ検査を実施することが規定されている。そこで，企画開発課のF課長は，部下のG君に指示してWebアプリを対象とした疑似侵入テストと，データベース（以下，DBという）サーバを対象とした脆弱性診断を，セキュリティ専門会社のD社に依頼した。

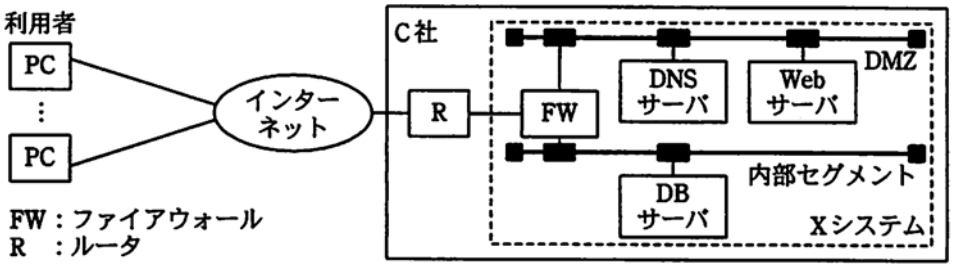


図1　Xシステムの構成

〔Webアプリのセキュリティに関する問題点〕

D社のH氏から疑似侵入テストと脆弱性診断の結果が報告された。次は，疑似侵入テストで見つかった脆弱性に関する会話の一部である。

H氏　：まず，各ログインセッションを識別するセッション識別子は，ログイン日と会員番号を組み合わせた文字列として構成され，図2のようにcookieにセットされますね。このままでは，悪意をもつ者に他人のセッション識別子を推定され，①容易になりすましアクセスができてしまいます。影響と対策については報告書に記述しましたので参照してください。

G君　：分かりました。セッション識別子の生成部分を修正します。

```
session_id = 20081223309804
```

注　会員番号309804の利用者が2008年12月23日にログインしたときのcookieの値を示している

図2　cookieにセットされたセッション識別子の例

H氏　：次は，クロスサイトスクリプティング（以下，XSSという）についてです。Webアプリでは，XSSの脆弱性が多数見つかりました。

G君　：XSS対策については，図3のプログラムのように，利用者からの入力データに＜scriptや＜iframeなどの文字列が含まれていた場合は，入力チェックで，処理を中止するようにしていました。

H 氏　：入力チェックだけで完全な XSS 対策を行うのは困難です。まず HTML 出力の際に“<”，“>”，“””，“’”，“&”をそれぞれ“<”，“>”，“"”，“'”，“&”に置換することが基本です。その上で，プログラムが HTML タグの②ある特定の属性に値を出力する場合は，個別の対処が必要です。

G 君　：（報告書を見ながら）なるほど，そのように対応します。

```
 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 $cgi = new CGI;                                  # CGI クラスのオブジェクトを生成
 5 $uname = $cgi->param('uname');                   # uname パラメタを取得
 6 die if (chkstr($uname));                         # uname に対する入力チェック
（省略）
11 $dbh = DBI->connect('DBI（省略）') or die;       # DB に接続
（省略）                                            # uname を基に SQL 文を組み立て，実行
18 $dbh->disconnect or die;                         # DB から切断
（省略）
24 print "<img src=\"http://www.c-sha-△△.com/img/a0.png\" alt=\"（省略）\">";
（省略）
29 print "<img src=\"../img/a1.png\" alt=\"（省略）\"></div>";
30 print "<form action=\"../cgi-bin/shori-a.cgi\" method=\"post\">";
31 print "<p>利用者名：<input name=\"uname\" type=\"text\" value=\"$uname\">";
（省略）
50 print "<img src=\"https://www.c-sha-△△.com/img/a9.png\" alt=\"（省略）\">";
51 print "</div></body></html>";                    # HTML 終了部分を出力
52
53 sub chkstr {                                    # 引数内に特定キーワードが存在した場合
54   my $str = shift;                              # true を返す
55   if ($str=~/(<script|<iframe|（省略）)/) {return(true)};
56 }
```

注　（省略）は，記述を省略していることを意味する。
　　www.c-sha-△△.com は，X システムが利用しているドメイン名である。
　　△△は，特定の文字列を表す。

図 3　プログラム（抜粋）

H 氏　：次に，図 3 のプログラムは HTTPS でアクセスする画面を出力するものですが，その画面を御社で推奨されているブラウザで見たときに，③HTTPS での正常なアクセスを意味する鍵マークが表示されなくなっています。

F 課長：これは注意が足りませんでした。ほかのプログラムも含めて確認し，修正します。

〔DB セキュリティに関する問題点〕

脆弱性診断によって，DB セキュリティに関する問題点も報告された。次は，その問題点に関する会話である。

H 氏　:DB サーバには，利用者の個人情報が平文で格納される仕様になっています。万が一，不正アクセスによって個人情報が流出した場合に備えて，Web アプリで個人情報を暗号化して格納することをお勧めします。

G 君　：実は，DBMS 側で自動的に暗号化／復号する透過的データ暗号化機能（以下，透過的暗号化という）を利用する予定です。

H 氏　：残念ながら④透過的暗号化の効果は限定的です。

H 氏は透過的暗号化について説明した。

F 課長：防止できる脅威を考えると，Web アプリによる暗号化を採用すべきだな。個人情報の登録と参照をしている箇所を洗い出して，実装してくれ。
G 君　：承知しました。ざっと見積もって 1 週間以上は掛かると予想されます。
F 課長：仕方ない。よろしく頼む。
H 氏　：今後システム開発をするときにはもっと早い段階で暗号化について検討し，実装すべきですね。次に，X システムのログイン認証用のパスワード情報について確認します。DB に格納されているパスワード情報はハッシュ値のように見えますが，どのような方法で算出しているのですか。
G 君　：パスワードを MD5 関数の引数にして算出しています。
H 氏　：パスワードだけからハッシュ値を算出すると，悪意ある第三者にハッシュ値が知られた場合，検索エンジンや専用ツールを使って，元の値であるパスワードを突き止められてしまう可能性があります。
F 課長：パスワードを突き止められることで，X システムに不正ログインされる可能性があるのは理解できますが，ほかに何か問題があるのですか。
H 氏　：利用者の多くは，ほかのサイトでも同じパスワードを使用しているようです。攻撃者は不正に入手した利用者 ID，パスワードを使ってほかのサイトに不正ログインを試みるでしょう。したがって，万が一，情報流出した際には，御社に対する非難の声が大きくなりかねませんし，利用者にほかのサイトのパスワードを変更する負担を強いることにもなります。そういう最悪の事態にならないようにするためにも，⑤より工夫してパスワードのハッシュ値を算出した方がよいでしょう。
F 課長：なるほど，当社だけの問題ではないのですね。ハッシュ値の算出方法を変更します。

その後，H 氏から指摘された脆弱性に関する対策を完了し，C 社は正式にサービスを開始した。

設問 1　〔Web アプリのセキュリティに関する問題点〕について，(1) ～ (3) に答えよ。
(1) 本文中の下線①について，悪意をもつ者が，どのようにして他人になりすますことができるのか。その方法を 50 字以内で具体的に述べよ。
(2) 本文中の下線③の原因となっている図 3 のプログラムの部分を，その行番号で答えよ。また，どのように修正すればよいかを 25 字以内で述べよ。ここで，a0.png～a9.png の画像ファイルは同じフォルダに配置されているものとする。
(3) 本文中の下線②の属性に該当するものを二つ挙げ，それぞれ 15 字以内で答えよ。

設問 2　〔DB セキュリティに関する問題点〕について，(1)，(2) に答えよ。
(1) 本文中の下線④について，DB に格納されている情報に対する不正閲覧のうち，透過的暗号化によって防止できるものを解答群の中から一つ選び，記号で答えよ。
解答群
ア　SQL インジェクションによる不正閲覧
イ　サーバ管理者による SQL 文を利用した不正閲覧

ウ　図 1 中の内部セグメントにおける通信傍受による不正閲覧
エ　バックアップ媒体を入手した第三者による不正閲覧

(2) 本文中の下線⑤について，よく使われる文字列をパスワードにしていた場合でも，ハッシュ値から元のパスワードを突き止められないようにするためのハッシュ値の算出方法を，50 字以内で述べよ。

問 4　情報システムの特権管理に関する次の記述を読んで，設問 1，2 に答えよ。

E 社は，従業員数 2,000 名の上場している運輸会社である。E 社の情報システム部では 80 台のサーバを管理しており，複数種の OS と，複数の DBMS 及びアプリケーション（以下，AP という）が稼働している。

インストールされたそれぞれの OS ，DBMS，AP に対して，システム管理特権が付与された利用者 ID（以下，特権 ID という）が一つずつ登録されており，情報システム部内のシステム管理チームに所属するシステム管理者 10 名がすべての特権 ID とパスワードを共用している。例えば，OS ，DBMS，AP がそれぞれ一つずつ稼働しているサーバでは，OS に一つ，DBMS に一つ，AP に一つの特権 ID が登録されており，システム管理者 10 名がこれらの特権 ID を共用している。特権 ID の使用は，基本的にはネットワーク経由で行われているが，コンソールからでないと行えない特定の作業については，サーバが保管されているラック内に設置されたコンソールから行われている。

E 社は, システム運用の安全性を確認するために, セキュリティ専門会社の F 社に, サーバの設定や運用に関するセキュリティ診断を依頼した。診断の結果，情報システムの特権 ID 管理が十分でないとの指摘を受けたことから，経営陣は情報システム部に対して特権 ID の管理を改善するように指示した。

〔特権 ID 管理の要件〕

F 社による指摘は，“特権 ID の使用において，内部者の不正使用を防止及び発見する仕組みが構築されていない”というものであった。システム管理チームの N 課長と M 君は，この指摘に基づき，必要な管理要件を明確にすることにした。

N 課長：M 君，現状の特権 ID 管理において必要な管理要件とは具体的に何だろう。
M 君　：現在の当社のシステムでは，特権 ID を使用したときのログがほとんど取得されていないので，不正使用があったとしても発見できないおそれがあります。ログインやログアウトなどの基本的なイベントと，システムの設定変更や利用者 ID 登録などの重要な操作については，ログを取得する必要があると思います。当社の全システムが，特権 ID に関するこれらのログを取得する機能をもっていることは確認できています。
N 課長：なるほど。それらのログを取得することにしよう。
M 君　：ただし，今の状態では，ログを取得したとしても [a] をやめないと，ログからはだれが不正使用を行ったのかを特定できないので意味がありません。
N 課長：なるほど。それは①上場企業に求められる内部統制の観点からも改善が必要だな。近々内部統制を評価するための内部監査が行われることになっている

が，今回の診断はその準備にもなっている。早速すべての OS ， DBM S ， AP で改善してくれ。

M 君　：分かりました。すぐに改善することにします。

N 課長：F 社からは，内部不正を発見する仕組みも必要と言われているが，これはどう考えるかね。

M 君　：はい。特権 ID の使用が業務目的であることを確認するために，使用目的，使用者，使用する特権 ID を記入した特権 ID 利用申請書を使用日ごとに課長に提出し，事前に承認していただくという運用にします。その上で，月に 1 回程度 [b] を実施して不正な使用がなかったことを確認します。この [b] が，内部不正を発見する仕組みに当たります。

N 課長：よし，ではそれで試験的に運用してみよう。

新たな特権 ID 管理の仕組みが試験的に運用され，1 か月が経過した。

〔特権 ID 管理の運用〕

N 課長：先月の [b] の結果はどうだったかね。

M 君　：ある DBM S に利用申請のない特権 ID の使用がありました。OS ， DBM S ， AP の特権 ID を必要に応じて追加作成し，一つの特権 ID は 1 人のシステム管理者だけが使用する環境を実現できましたので，だれが使ったのかすぐ分かりました。その特権 ID を使った者に確認したところ，状況監視のために毎日使用していました。しかし，一般権限でも問題ないということでしたので，②データの参照だけを行うことができる．状況監視用の利用者 ID を作成し，それを使用させることにしました。また，あるサーバの OS では，特権 ID の利用申請があったのに，ログが残っていないものがありました。チーム全員に確認してみたところ，ある従業員が誤ってシステムのリストアの際にログファイルを上書きしてしまったということでした。

N 課長：ログがちゃんと保存されないのは問題だな。

M 君　：そう思います。追記型記憶装置を使えばログが消えてしまうことを防止できるのですが，すべてのサーバに導入するとコストが掛かりすぎます。実は UNIX でログを収集，転送する方式として一般的に使われている [c] を使ったログサーバについて調査していました。これを導入して，ログサーバで追記型記憶装置を使用し，OS ， DBMS，AP のログを保存するというのはどうでしょう。

N 課長：なるほど。しかし，今年度の予算では，ログサーバを購入できたとしても，追記型記憶装置までは購入できないな。そこまでしなくても，もっと簡単な方法でログサーバのログは保護できるのではないだろうか。例えば，[a] することにすれば，ログサーバの中にログが保存された状態であっても，ほかのサーバ管理者による故意のログ削除を防止できるし，誤操作によるログ喪失の可能性も低下させることができるだろう。

M 君　：そうですね。そうすれば大丈夫だと思います。

N 課長：では，ログサーバだけを導入することにしよう。ログは，当社の情報セキュリティ規程に従って，2 年間保存するようにしておいてくれ。しかし，問題の発見に最悪で 1 か月も掛かるというのは遅すぎるな。ほかに方法はないのかね。

M 君　：例えば，不正の可能性が考えられる特権 ID の使用が発見されたときにだけア

ラートを発生させ，それを電子メール（以下，メールという）で通知する仕組みをログサーバに導入すれば，もっと早期に発見することができると思います。例えば，サーバへのログイン回数が多かった場合にアラートを発生させればよいかもしれません。

N 課長：しかし，サーバへのログイン回数が多かったからといって不正使用というわけではないだろう。

M 君　：はい，そのとおりです。アラートが発生したからといって特権 ID の不正使用があったとは断言できないので，特権 ID 利用申請書などを基に確認を行う必要がある，という意味です。

N 課長：なるほど。では，どのようなアラートの発生条件を設定するか，案を作ってくれ。

M 君　：分かりました。

数日後，M 君から特権 ID の使用に関するアラートの発生条件案（表）が提出された。

表　特権 ID の使用に関するアラートの発生条件案

項番	アラートの発生条件
1	一つのサーバにおいて，過去 1 か月間ログインしたことがない特権 ID によるログインが行われたとき（普段使わない特権 ID の使用）
2	全サーバ累計で，1 人が 1 日で 10 回以上のログインを行ったとき（頻繁な使用）
3	ログアウト（又はタイムアウト）時に，ログインからの時間が 2 時間を超えているとき（長時間のログイン）
4	特権 ID の追加が行われたとき
5	システム設定が変更されたとき
6	DBMS に対して SQL 文を実行したとき (1)

注(1)　アプリケーションから DBMS へのアクセスでは，DBMS の特権 ID は使用していない。

N 課長：これらの条件だけでは，本人に割り当てられている特権 ID を使用したときにしか検出できないな。③特権 ID をもっていない人が特権 ID を使用しようとする行為があったときにも検出できるようにしてくれないか。それから，アラートを通知するメールは管理職の私が受け取って確認しよう。ところで，④アラートを設定していることはシステム管理者に周知してほしいが，⑤具体的なアラートの発生条件は伝えないようにしておいてもらえるかね。

M 君　：分かりました。アラートを通知するメールへの対応はよろしくお願いします。

M 君の案に基づき，アラートを発生させる仕組みが導入され，1 週間が経過した。

N 課長：M 君，アラートを通知するメールが多くて確認が大変だよ。特に，表の項番 6 の条件のときに発生させるアラートの通知メールが必ず毎日届くんだ。

M 君　：すみません。どうも最近，DBMS に対して特権 ID を使用して SQL 文を実行する運用作業が増えたことが原因のようです。アラートの数を減らす方法として，SQL 文の中身を解釈し，その内容に応じてアラートを発生させること

ができるツールを使うことも考えているのですが，まだ調査中で導入にはしばらく時間が掛かりそうです。

N 課長：これではほかの仕事ができないな。この条件はそのツールを導入するまでいったん外してくれないか。

M 君　：分かりました。当面，特権 ID を使用した SQL 文の実行に関するログの取得はやめましょう。

N 課長：M 君，それは駄目だよ。⑥データベース（以下，DB という）では当社の財務にかかわる重要なデータが管理されているから，財務報告の信頼性を担保するためにも，特権 ID を使用して DB を擾作したログを取得して俣存することは重要なんだ。

M 君　：なるほど，分かりました。アラートの発生条件からは外しますが，ログは取得するようにしておきます。

N 課長：よし，ではこの状態でしばらく運用することにしよう。

その後，SQL 文の中身を解釈してアラートを発生させるツールが導入され，再度の試験運用が行われた。その 1 か月後，アラート発生の設定が適切であることが確認され，本格運用が開始された。これによって，E 社システムの特権 ID 管理が改善され，より安全なシステム運用が実現された。

設問 1　〔特権 ID 管理の要件〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線①で，上場企業を対象に，内部統制の評価及び報告を求める法律（又はその通称）を解答群の中から選び，記号で答えよ。

解答群

ア　割賦販売法　　イ　金融商品取引法

ウ　個人情報保護法　　エ　不正アクセス禁止法

(2) 本文中の [a] に入れる適切な字句を，10 字以内で答えよ。

(3) 本文中の [b] に入れる適切な字句を，10 字以内で答えよ。

設問 2　〔特権 ID 管理の運用〕について，(1)～(6)に答えよ。

(1) 本文中の下線②を実施するに当たって適用した考え方を，解答群の中から選び，記号で答えよ。

解答群

ア　最小権限の原則　　イ　職務の分掌

ウ　多層防御　　エ　要さい化

(2) 本文中の [c] に入れる方式を，英文字 10 字以内で答えよ。

(3) 本文中の [d] に入れる，N 課長がログサーバに対して実施しようとしている対策を，40 字以内で述べよ。

(4) 本文中の下線③を検出するために，表に項番 7 を追加したい。このとき，アラートの発生条件として何を設定すべきか。20 字以内で述べよ。

(5) 本文中の下線④及び下線⑤の指示のセキュリティ上の目的を，それぞれ 35 字以内で述べよ。

(6) 本文中の下線⑥において，財務報告の信頼性を担保するために，特権 ID に関する DB のログの個々の記録について何を確認し，全体として何を立証しようとしているか。特権 ID に関する DB のログの個々の記録に対して確認する内容を 50 字以内で，立証しようとしていることを 35 字以内で述べよ。

解答例

問 1

出題趣旨

社内 LAN 上の異常を解析するツールとして，パケツトモニタは有効である。ウイルスに感染した PC が外部と通信を行う際に DNS サーバを利用した名前解決を行うことが多く，DNS クエリに注目すると異常を特定しやすい。特に，スパムメールの踏み台になった PC の場合，メールの配送先を示す MX レコードを検索して，該当するメールサーバにスパムメールを送りつける。また，DNS 通信はステートレスな UDP プロトコルであるので，発信元 IP アドレスを詐称した DNS Reflection 攻撃の踏み台にされる危険性がある。

本問では，パケツトモニタを利用して，このような異常を解析する手順と，DNS サーバの危険性についての理解を問う。

設問 1（1）a（r）

（2）b　ウ

c　詐称

（3）d　イ

（4）　e　（Ⅱ）

f　（V）

修正　インターネットからの A 社以外のドメイン上のアドレスに関する DNS クエリを拒否する。

設問 2（1）**不審な**　・名前解決のために 3 台以上の DNS サーバと通信している。

通信挙動・A 社以外の DNS サーバに MX レコードを問い合わせている。

g　　エ

（2）ア，ウ

設問 3（1）・OS やアプリケーションが本来通信しないあて先ホストと通信するプロセス

・OS やアプリケーションが本来通信しないあて先ポートを利用するプロセス

（2）ウイルス対策ソフトによるパターンファイルの更新確認パケット

問 2

出題趣旨

今日，システムの安全な運用を継続するためには，脆弱性情報の適切な取扱いと，修正プログラムの迅速な適用などの情報セキュリティ運用は，必須要件となっている。

本問では，コンピュータシステムの日常運用で必要とされる脆弱性管理のポイント，具体的には，日々公表される脆弱性情報に関して，その内容から自社システムにおいて必要な対応を決定するための判断，脆弱性が大きな問題となる Web サーバで使用される http の理解，OS ，アプリケーションプログラムなどへ修正プログラムを適用する作業に関する理解について問う。

設問 1（1）・攻撃者が指定したコマンドが実行されると，システムが全面的に停止するおそれがある。

・管理者権限が奪われ，DB サーバ内の個人情報が漏えいする可能性がある。

（2）・攻撃手法が公開されている。

・Exploit コードを基にした攻撃が予想される。

設問 2（1）a　form　又は　input

(2)・Referer ヘッダにクエリストリングが記載されるので，リンク先などの外部サーバに入力データが送信されるおそれがある。
・Web サーバのアクセスログにクエリストリングが記録されるので，ログから入力データが読み取られるおそれがある。
(3)・X-Sender というフィールドを含んだ HTTP ヘッダを検出する。
・HTTP ヘッダから X-Sender で始まる行を検出する。
(4) **記号**（f）
対策の内容　Web サーバプログラムの動作権限を必要最小限とする。

設問 3（1）b　・運用系から切り離す
・待機系にする
・スタンバイ状態にする
（2）動作試験用システムで，修正プログラム適用後の動作の正常性を確認する。

問 3

出題趣旨

Web をベースとしたシステム開発が主流となっているが，アプリケーションレベルのセキュリティ対策は正しく実施されていないことがまだ多い。

本問では，Web アプリケーションに対する疑似侵入テストで，クロスサイトスクリプティング（XSS）への対応や，セッション管理の不備が見つかった状況，及び DB サーバに対する脆弱性診断で，格納しているデータ保護の不備が見つかった状況を想定し，それらの脆弱性に対する適切なアプリケーション設計，プログラミング手法，データベースセキュリティ対策などの理解を問う。

設問 1（1）cookie にセットされたセッション識別子のうち，会員番号部分を他人のものに変える。
（2）　**行番号**　24
修正方法　・画像ファイルを相対パス名で指定する。
・http の部分を https にする。
（3）①　・タグの href 属性
②　・タグのイベントハンドラ属性

設問 2（1）エ
（2）・鍵付きハッシュ関数でパスワードからハッシュ値を算出して格納する。
・パスワードとランダムな文字列を連結した文字列からハッシュ値を算出して格納する。

問 4

出題趣旨

近年，企業活動を支える情報システムの完全性を担保することが重要な課題となっている。特に上場企業においては，金融商品取引法の改正（いわゆる日本版 SOX 法）に基づき，重要なシステムの開発・運用プロセスにおける内部統制を評価，報告し，そのシステムが担う財務情報の適正性を立証することが求められている。システムの内部統制について理解し，評価や改善を行っていくためには，システムがもつ機能だけでなく，人による運用も含めた検討が必要であり，開発・運用にまたがる広範な知識とリスクに対する総合的な

判断力が求められている。
本問では，システムの完全性を担保する重要な要素の一つである特権 ID の管理に焦点を当て，特権 ID 管理に関する知識と，機能と運用の両面から改善を行っていくための能力を問う。

設問 1（1）イ
（2）a　特権 ID の共用
（3）b　ログのレビュー
設問 2（1）ア
（2）c　syslog
（3）d　ログサーバの特権 ID 使用者とほかのサーバの特権 ID 使用者を分離
（4）特権 ID の認証が失敗したとき
（5）**下線④**　システム管理者による不正行為の実行を抑止するため
下線⑤　・アラートの発生条件を回避しようとする行為を防止するため
・アラートが発生しないような不正使用方法を発見されないようにするため
（6）**確認する内容**　・特権 ID で DB のデータを変更した処理のログに対応する特権 ID 利用申請書が提出されていること
・DB のデータを変更した処理が，すべて業務目的に基づいていること
立証しようとしていること　・DBMS 内の財務データが特権 ID によって改ざんされていないこと
・DBMS 内の財務データの完全性

採点講評
問 1
問 1 では，社内ネットワークから発信される攻撃に対して，踏み台となっている PC や DNS サーバの不備を，ネットワークモニタを使って突き止める手法について出題した。全体として正答率はやや低かった。
設問 1(4)は，正答率が低かった。企業の DNS サーバにおいて，本来応答する必要のない外部ホストからの外部アドレスの問合せを許していると，DNS Reflection 攻撃の踏み台に悪用されるおそれがある。“修正"についての解答には，問合せ元と問合せ対象の両者を含めてほしかった。 DNS サーバには，そのプロトコル上の性質から様々な脆弱性が指摘されており，設定には細心の注意が必要であることを理解してほしい。
設問 2(1)では，パケットモニタの状況から異常を読み取る能力を問うている。正しい通信手順とマルウェアの通信パターンの差異についての理解を求めているが，“パケット量が多い"などのあいまいな解答が散見された。
設問 3(2)は，マルウェアが hosts ファイルを改ざんして，ウイルス対策ソフトのアップデート機能を無効にすることで，PC に現れる異常について考える問いであった。マルウェアは自身の発見を逃れるために，様々な設定を改ざんするが，パケットの送信状況を外部からモニタすることで異常を検知できる場合があることを理解しておいてほしい。

問 2

問 2 では，Web サーバプログラムの脆弱性対策について出題した。全体として正答率は想定どおりだった。

設問 1 は，正答率がやや低かった。(2) では，攻撃が成功する可能性や，攻撃が成功した場合の被害の大きさを解答した誤答が散見された。攻撃が試みられる可能性が高いことと，その攻撃が成功する可能性が高いことは，それぞれ別の特性であることを考えて解答してほしかった。

設問 2 は，正答率が低かった。特に (2) は正答率が著しく低く，その中でも，“クエリストリングは暗号化されない”という誤った解答が目立った。今後も Web アプリケーションの利用は増加すると思われるので，HTTPS において暗号化される範囲と GET，POST メソッドの動作の違いについて，確実に理解しておいてほしい。

設問 3 は，正答率が高かった。修正プログラムは日々提供されるものだが，修正プログラムそのものに起因してトラブルが発生する可能性について考えた上で適用作業を実施する必要があることは，おおむね理解できていた。

問 3

問 3 では，Web アプリケーション開発時の脆弱性対策について出題した。全体として正答率は，低かった。

設問 1(1)では，どのような方法で他人になりすますかを問うたが，“cookie の値が容易に書き換えられるから"のように原因だけを述べ，方法が明示されていない解答が多かった。また，クロスサイトスクリプティング対策を問うた(3)は，正答率が低かった。<>&'" などの HTML 構造に影響を与える文字を適切に置換しても，出力される箇所によってはスクリプトが動作してしまうことを理解しておいてほしい。

設問 2 は，全体的に正答率が高かった。透過的データ暗号化機能によるリスク対策や，Web アプリケーションで管理される利用者のパスワード情報の保護については，適切に理解されているものと推察できる。

問 4

問 4 では，特権 ID 管理の重要性と課題，及びその改善方法について出題した。全体として，正答率は低かった。

設問 1(1)は，選択肢からの解答であったにもかかわらず正答率が低かった。セキュリティの関連技術と同様に，セキュリティの関連法規についても世の中の動向を知っておいてもらいたい。

設問 2(3)は，正答率が低かった。特に，ログサーバ内のログに対してアクセス権を設定することだけを記述した解答が多かった。特権 ID は，システムに対して強力な権限をもった ID であるので，その管理を改善する際には，システム設定などの技術的側面だけでなく，使用者の範囲や使用手続など，運用に関する部分も含めて検討する必要があることを理解しておいてほしい。