SC

平成21年度　春期
情報セキュリティスペシャリスト
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. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **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。**
5. 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4
選択方法	2問選択

6. 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，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**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。
   (4) **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。
   なお，○印がない場合は，採点の対象になりません。3問以上○印で囲んだ場合は，はじめの2問について採点します。
   (5) 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。
   (6) 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
○問1
問2
○問3
問4

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　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。

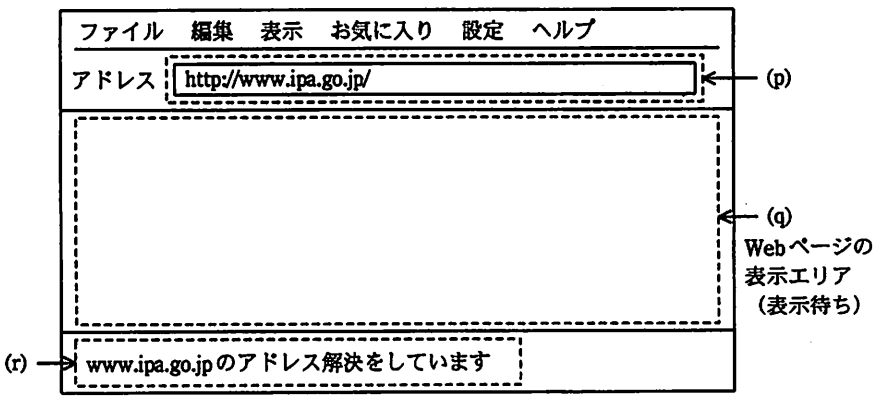

図1　Webページを閲覧しようとしたときのブラウザの状態

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。

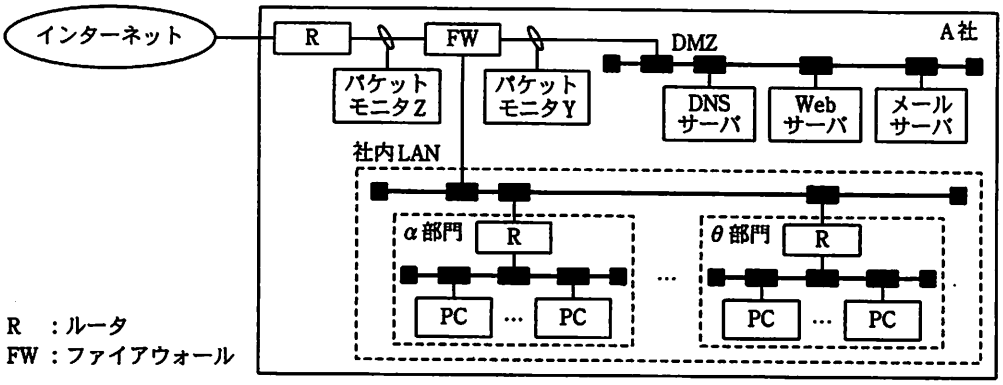

図2　A社の社内ネットワークの構成

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。①DNS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。

```
127.0.0.1    localhost
127.0.0.1    www.○○○.com
127.0.0.1    download.△△△.co.jp
127.0.0.1    get.□□□.com
127.0.0.1    update.◇◇◇.com
127.0.0.1    get.☆☆☆.com
```

ウイルス対策ソフトの
パターンファイルの配布サイト

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，ウイ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 DNS amplification 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 TCP-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。Web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。

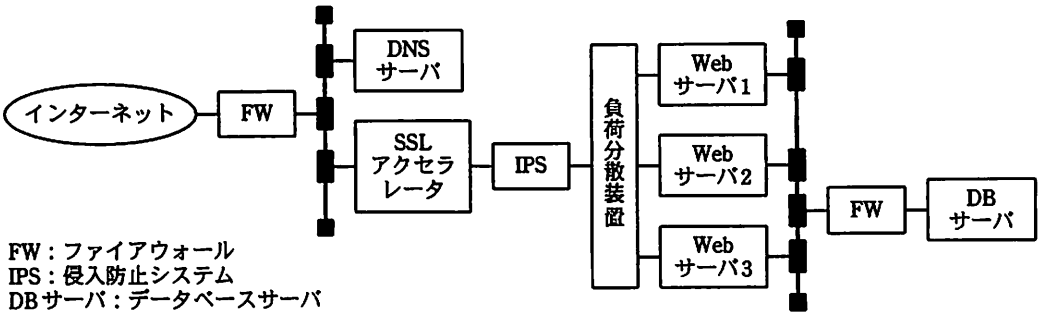

図1　B社のWeb販売システムの構成

(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，<u>①“緊急”に相当すると判定しました</u>。

・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。運用管理グループリーダの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。

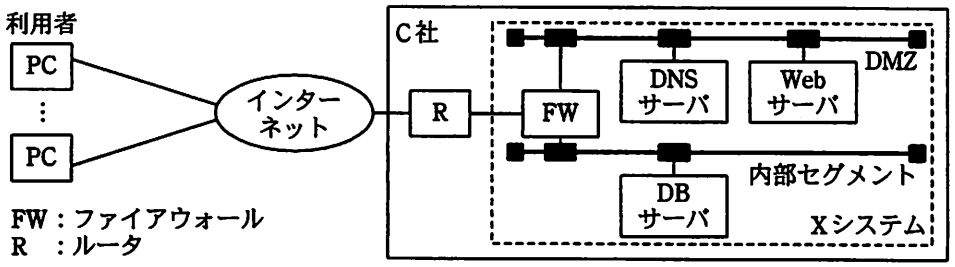

図1　Xシステムの構成

〔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，DBMS，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 DBMS に利用申請のない特権 ID の使用がありました。OS，DBMS，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，［　d　］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を操作したログを取得して保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。

プログラム言語 Perl の用例・解説

Perl を使用した問題では，各問題文中に注記がない限り，次に示す用例に従って記述する。

なお，用例は，解答で使用する演算子，関数，予約語などを制限するものではない。

種類	用例 解説

1. 注釈

#	#ここにコメントを書く 行末までが注釈となる。

2. リテラル

スカラ	123 10 進数 123 である。
	12.3 10 進数 12.3 である。
	4E-5 10 進数 4×10^{-5} である。
	0x9f 16 進数 9F である。
	0147 8 進数 147 である。
	0b010111 2 進数 010111 である。
	$var = "hello"; print '$var ', "$var ", `echo world`; 変数 var に文字列 “hello” を代入する。文字列のスカラ '$var ', "$var ", `echo world` を出力する。"$var " は変数を展開し，`echo world` はコマンドの出力を展開するので，出力は “$var hello world” となる。
	\n 制御文字（改行）である。
	\r 制御文字（復帰）である。
	\t 制御文字（水平タブ）である。

リストリテラル	('a', 'b', 'c')
	リスト ('a', 'b', 'c') である。
	('a', 'b', 'c')[0]
	リスト ('a', 'b', 'c') の 1 番目の要素 'a' である。
	()
	空リストである。
	('a' => 'alpha', 'b' => 'bravo', 'c' => 'charlie')
	キー a, b, c に，それぞれ値 alpha, bravo, charlie を結び付けたハッシュである。
ファイルハンドル	STDIN
	標準入力である。
	STDOUT
	標準出力である。
	STDERR
	標準エラー出力である。
	ARGV
	コマンドラインから指定されたファイル名のリストを順に読み込むためのファイルハンドルである。

3. 変数

スカラ変数	$var
	スカラ変数 var である。
配列変数	@ary
	配列変数 ary である。
配列要素	$ary[6]
	配列変数 ary の 7 番目の要素である。
ハッシュ変数	%hash
	ハッシュ変数 hash である。
ハッシュ要素	$hash{'a'}
	ハッシュ変数 hash の要素のうち，キー a に結び付けられた値である。
局所的な変数	{my $var;}
	{} 内を有効範囲とする変数 var の宣言である。
$_	$_ = "abc"; if (/b/) print "match";
	パターンマッチの演算子が省略されたとき，$_ の文字列 “abc” が // 内のパターン b と一致するかどうかを判定し，“match” が出力される。
@ARGV	@ARGV
	コマンドライン引数のリストを格納する配列変数である。
@_	@_
	サブルーチンに渡す引数のリストを格納する配列変数である。

4. 演算子

->	$object->method1
	オブジェクト object のメソッド method1 を呼び出す。
	Class->method2
	クラス Class のメソッド method2 を呼び出す。
++, --	$a++
	変数 a を評価した後に 1 を加算する。
	--$b
	変数 b から 1 を減算した後に評価する。
!, + (単項), - (単項)	!$a
	変数 a の論理否定である。
	+123
	正の数 123 である。
	-123
	負の数 123 である。
=~, !~	$html_contents =~ /<b>/
	変数 html_contents の値に，文字列 “<b>” が含まれているときに真を返す。
	$html_contents !~ / /
	変数 html_contents の値に，文字列 “ ” が含まれていないときに真を返す。
*, /, %	314 * 34
	314 と 34 の乗算である。
	6 / 469
	6 を 469 で割る除算である。
	34 % 6
	34 を 6 で割る剰余演算である。
+, -, .	3.14 + 2.72
	3.14 と 2.72 の加算である。
	220 - 8125
	220 から 8125 を引く減算である。
	"IPA"."JITEC"
	文字列 “IPA” と “JITEC” の連結である。
<, >, <=, >=, lt, gt, le, ge	1 < 2
	数値 1 と 2 を比較し，演算子の左側が右側より小さいので真を返す。数値の関係演算子には，ほかに >, <=, >= がある。
	"b" lt "a"
	文字列 “b” と “a” を比較し，演算子の左側が右側より小さくないので偽を返す。文字列の関係演算子には，ほかに gt, le, ge がある。

==, !=, <=>, eq, ne, cmp	1 <=> 2 数値 1 と 2 を比較し，演算子の左側が右側より大きければ 1，等しければ 0，小さければ −1 を返すので，この場合は −1 を返す。数値の比較演算子には，ほかに ==，!= がある。
	"b" cmp "a" 文字列 “b” と “a” を比較し，演算子の左側が右側より大きければ 1，等しければ 0，小さければ −1 を返すので，この場合は 1 を返す。文字列の比較演算子には，ほかに eq，ne がある。
&&	$x >= 0 && $x < 10 変数 x の値が 0 以上かつ 10 未満なら真を返す。
||	$x < 0 || $x >= 10 変数 x の値が 0 未満又は 10 以上なら真を返す。
..	@card = (1 .. 52) 1 から 52 までの連続する整数を配列変数 card に代入する。
=, +=, -=, *=, /=, %=	$a = 1 変数 a に 1 を代入する。
	$a += 10 変数 a の値に 10 を加算して a に代入する。 代入演算子には，ほかに -=，*=，/=，%= がある。
=>, ,	%hash = ('a' => 'alpha', 'b' => 'bravo', 'c' => 'charlie') a に alpha，b に bravo，c に charlie を結び付けたハッシュをハッシュ変数 hash に代入する。
not	not $a 変数 a の論理否定である。
and	$a < 0 and $b == 0 変数 a が 0 より小さいか，変数 b が 0 と等しいかという二つの関係式の論理積である。
or, xor	$a < 0 or $b == 0 変数 a が 0 より小さいか，変数 b が 0 と等しいかという二つの関係式の論理和である。
	$a < 0 xor $b == 0 変数 a が 0 より小さいか，変数 b が 0 と等しいかという二つの関係式の排他的論理和である。

注 演算の優先順位は，上表の枠の順である。

5. 文

if	if ($var == 1) {
	  print "a";
	} elsif ($var == 2) {
	  print "b";
	} else {
	  print "c";
	}
	変数 var の値が 1 なら “a” を，2 なら “b” を，それ以外なら “c” を出力する。

while	$i = 1;
	while ($i <= 10) {
	  print $i++, "\n";
	}
	変数 i の値を 1 から 1 ずつ増やし，10 回出力する。

for	for ($i = 1; $i <= 10; $i++){
	  print "$i\n";
	}
	変数 i の値を 1 から 1 ずつ増やし，10 回出力する。

foreach	foreach $i (1, 3, 5) {
	  print "$i\n";
	}
	変数 i にリストの各要素 1，3，5 を順に代入し，3 回出力する。

next	for ($i = 1; $i <= 10; $i++) {
	  next if $i % 2;
	  print "$i\n";
	}
	変数 i が 2 で割り切れないとき，ループ本体の next 行より後を実行しないので，偶数を出力する。

6. 正規表現

\	/\.\^\$\[|\+*\?\{\(\)\/\\/ 次の 1 文字そのものを表す。“.^$[|+*?{()/\” と一致する。
.	/www.ipa.go.jp/ 改行文字以外の任意の 1 文字と一致する。“wwwdipa,go@jp” と一致する。
^	/^ab/ 先頭が “ab” である文字列と一致する。“abc” と一致するが，“cab” とは一致しない。
$	/yz$/ 末尾が “yz” である文字列と一致する。“xyz” と一致するが，“yza” とは一致しない。
+	/go+d/ 直前の 1 文字 o の 1 回以上の繰返しと一致する。“god” や “gooood” と一致するが，“gd” とは一致しない。

*	/go*d/
	直前の 1 文字 o の 0 回以上の繰返しと一致する。“gd”, “god” や “gooood” と一致する。
?	/colou?r/
	直前の 1 文字 u の 0 回又は 1 回の出現と一致する。“color” 又は “colour” と一致する。
{m}, {m,n}	/co{2}l/
	直前の 1 文字 o の 2 回の繰返しと一致する。“cool” と一致するが, “col” や “coool” とは一致しない。
	/go{1,3}d/
	直前の 1 文字 o の 1 ～ 3 回の繰返しと一致する。“god” や “good” と一致するが, “gd” や “gooood” とは一致しない。
(…)	/<(h.)>/
	() 内の文字列と一致するパターンを部分パターンとしてまとめる。“<h1>” と一致した場合は “h1” が, “<hr>” と一致した場合は “hr” が, まとめられる。
\1, \2, …	/<(..)><([bp])>JITEC<\/\2><\/\1>/
	左から順に () 内のパターンと一致した文字列が \1, \2, … に割り当てられる。“<h1>JITEC</h1>” と一致するが, “<td>JITEC</p></td>” とは一致しない。
[…]	/<h[12r]>/
	[] 内で指定した文字 1, 2 又は r のどれか一つと一致する。“<h1>”, “<hr>” と一致するが, “<h3>” や “<HR>” とは一致しない。
	/[^0-9]/
	[] 内で指定した 0 ～ 9 以外の 1 文字と一致する。“a” と一致するが, “3” とは一致しない。
…|…	/<(a href|img src)=/
	| で区切られた “a href” 又は “img src” のどちらか一方と一致する。“<a href=” や “<img src=” と一致するが, “<A HREF=” や “<img height=” とは一致しない。

7. サブルーチン

定義	sub greeting {
	  print "hello Perl\n";
	}

	“hello Perl” を出力するサブルーチン greeting を定義する。
呼出し	subroutine ($arg1, $arg2);
	サブルーチン subroutine を引数 arg1 と arg2 で呼び出す。() を省略して “subroutine $arg1, $arg2;” とする表記もある。
戻り	return -1;
	サブルーチンから抜け出し, 値 −1 を返す。

8. モジュール

use	use CGI; モジュール CGI を 1 度だけ読み込み，利用可能にする。

9. メソッド呼出し

->	$object->method1(arg1); 演算子 -> を使って，オブジェクト object のメソッド method1 を引数 arg1 で実行する。
	Class->method2(arg1, arg2); 演算子 -> を使って，クラス Class のメソッド method2 を引数 arg1 及び arg2 で実行する。

10. 文字列操作関数

chomp	chomp @lines; 配列変数 lines の各要素の末尾にある改行文字を削除する。
eval	eval $exp_str; 変数 exp_str の内容を Perl プログラムとして解釈し実行する。
length	length $long_str; 変数 long_str に格納される文字列の文字数を返す。

11. 配列・ハッシュ操作関数

keys	%hash = ('a' => 'alpha', 'b' => 'bravo', 'c' => 'charlie');
	foreach $key (keys %hash) {
	  print "$key\n";
	}
	ハッシュ変数 hash のキーのリストを取り出し，各キーを出力する。この場合は，“a”，“b”，“c” を順不同に出力する。

shift	$next = shift @queue; 配列変数 queue の先頭要素を取り除いて詰め，取り除いた値を変数 next に代入する。
sort	@pile = sort @jumble; 配列変数 jumble の値を文字列の大小比較によって昇順に整列し，配列変数 pile に代入する。
	@pile = sort {$b <=> $a} @jumble; 配列変数 jumble の値を数値の大小比較に従って降順に整列し，配列変数 pile に代入する。
split	@fields = split ',', $csv; 変数 csv の値をコンマで区切って分割したリストを配列変数 fields に代入する。

12. 検索・置換関数

m/…/ 又は /…/	$html_contents =~ /<b>/i; 変数 html_contents の値が，文字列 “<b>” 又は “<B>” を含んでいるかどうかを判定する。i は，大文字，小文字の区別をしないオプションである。
s/…/…/	$html_contents =~ s/ /\n/gi; 変数 html_contents の中の文字列 “ ”，“ ”，“ ” 又は “ ” を改行文字に置換する。g は，一致したすべての文字列を置換するオプションである。
$`，$&，$'， $1，$2，…	'The date is 1970-01-23.' =~ /([0-9]{4})-([0-9]{2})-([0-9]{2})/; print "String before the date: $`\n"; print "Date: $&\n"; print "String after the date: $'\n"; print "Year: $1\n", "Month: $2\n", "Day: $3\n"; 文字列 “The date is 1970-01-23.” に対して，一致した部分の前の文字列，一致した文字列，一致した部分の後ろの文字列をそれぞれ変数 `，&，' に代入する。また，() で囲まれた部分パターンと一致した文字列を，1 番目から順に変数 1，2，3 に代入する。これらを利用し，“String before the date: The date is ”，“Date: 1970-01-23”，“String after the date: .”，“Year: 1970”，“Month: 01”，“Day: 23” の 6 行を出力する。

13. 入出力操作関数

open	open LOG, '>>cgi.log'; ファイル cgi.log を追記モードで開き，ファイルハンドル LOG に対応付ける。
<*filehandle*>	$line = <USER_FILE>; ファイルハンドル USER_FILE から 1 行を読み込んで変数 line に代入する。
<>	@records = <>; 標準入力（コマンドライン引数があるときは，コマンドライン引数で指定されたファイル）から順にデータを読み込み，すべての行を配列変数 records に代入する。
print	print LOG "sync.\n"; ファイルハンドル LOG に対応するファイルに文字列を出力する。
close	close LOG; ファイルハンドル LOG に対応するファイルを閉じる。

14. システムインタフェース

die	open(FILE, 'a_file') or die 'cannot open a_file'; ファイル a_file を開く。開くのに失敗したとき，“cannot open a_file” というメッセージを出力して実行を終了する。
system	system 'a.out'; コマンド a.out を実行し，コマンドが終了するまで待機する。

7. 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

8. **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。
9. 問題冊子の余白などは，適宜利用して構いません。
10. プログラム言語 Perl の用例・解説は，この冊子の末尾を参照してください。
11. 試験中，机上に置けるもの及び使用できるものは，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，黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ
    これら以外は机上に置けません。使用もできません。
12. 試験終了後，この問題冊子は持ち帰ることができます。
13. 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。
14. 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。
15. 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。