次の問1は必須問題です。必ず解答してください。

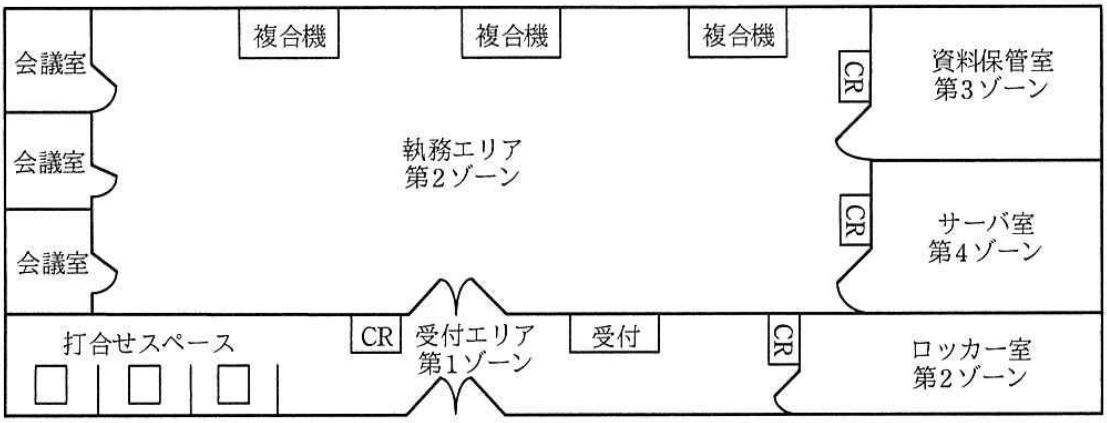
問1　オフィスのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

A社は，日用雑貨の通信販売会社である。A社では，会員にカタログ冊子を送付し，冊子にとじ込まれた注文書又はインターネットでの注文を受け付けている。

A社では，情報セキュリティ担当役員を委員長とする情報セキュリティ委員会を設置しており，情報セキュリティの適正な管理を目的として，情報セキュリティ管理規程を制定している。

A社の通信販売事業は順調に拡大し，大量の個人情報を管理するようになったことから，情報セキュリティ委員会は，今回，物理的対策を中心にオフィスのセキュリティを見直すことにした。

A社のオフィスレイアウトを図1に示す。



注記1　複合機は，プリンタ，ファックス，コピー，文書保存などの機能をもつ装置である。
注記2　CRは，入退室管理システムの非接触型ICカード読取り装置である。
注記3　ゾーンは，警戒レベルに合わせて管理された区域であり，第4ゾーンは警戒レベルが最も高い区域である。

図1　A社のオフィスレイアウト

〔オフィスの現状〕

A社のオフィスは，入退室管理システムによって，入室制限が行われている。第1ゾーンは，入退室管理システムでの入室制限を行っていない。第2ゾーンには全社員が，第3，4ゾーンには許可された社員だけが入ることができる。社員は，非接触型ICカードである社員カードを所持している。社員カードを部屋の入り口に設置されたCRにかざすと，社員カード内に記録されたIDによって入室の可否が判断される。入室が許可されるとドアが解錠される。

A 社では，ノート PC（以下，NPC という）を全社員に貸与している。オフィスの執務エリアは，間仕切りのない設計になっている。会議室は執務エリアと同じ第 2 ゾーンに含まれる。執務エリアには，3 台の複合機が設置され，複数の課で共有している。執務エリア内で社員が使用する机には鍵付きのサイドキャビネットがあり，個人が管理する書類や外出及び帰宅時の NPC の保管などに使用されている。

資料保管室とサーバ室は執務エリアと間仕切りされ，入室を許可された社員だけが使用できる。受付エリアの右手奥にロッカー室があり，鍵付きの個人用ロッカーが全社員分設置されている。

非接触型 IC カードでは，カード内に埋め込まれた［ a ］が，CR が発信する［ b ］を電気に変換し，その電気を利用して IC カード内のプログラムを動作させ，CR との間で無線通信を行う。複合機は，情報機器や情報システムなどの IT セキュリティを評価するための基準を定めた規格である［ c ］に基づく認証を取得している製品である。

物理的対策を中心としたオフィスのセキュリティの見直しを決定した情報セキュリティ委員会は，システム部の情報セキュリティリーダである B 主任を，担当者に指名した。B 主任は，見直し案を作成するために，現状の問題点の洗い出しと改善策の立案支援を，情報セキュリティ会社の C 社に依頼した。

〔現状の問題点〕

C 社のコンサルタントである D 氏は，オフィスの現状を調査し，四つの項目に関する六つの問題点を B 主任に報告した。D 氏が指摘した問題点を表 1 に示す。

表 1　D 氏が指摘した問題点

項番	項目	問題点
1	入退室管理について	共連れでの入室が散見される。
2		来訪者の執務エリア内などでの単独行動が散見される。
3	複合機の運用について	個人データが印刷された書類が複合機に放置されていることがある。
4	執務エリア内への私物の持込みについて	多くの社員が，私物を入れた鞄を執務エリア内に持ち込んでいる。
5	紙文書や NPC の管理について	書類や印刷物などを机の上に放置したままの離席が散見される。
6		NPC にログイン後の，操作が可能な状態での離席が散見される。

〔問題点についての打合せ〕

D氏から指摘された問題点について，B主任がD氏と打合せを行ったときの二人の会話を次に示す。

B主任：項番1，2については，どのような対策が有効でしょうか。

D氏：　低コストで実現できる項番1の対策としては，CRを入り口側と同様に出口側にも設置して，アンチパスバックを導入することが有効です。アンチパスバックでは，“入室状態になっていない人が退室しようとした場合は解錠しない”，という処理が行われます。①そのほかにも，アンチパスバックでは，通行を許可された社員カードをCRにかざしても，利用状況によっては異常と判断して解錠しない場合があります。項番2の対策としては，来訪者を入室させる場合は，入室から退室まで担当者が付き添うようにします。しかし，サーバの保守作業など担当者が付き添えない場合もありますから，サーバコンソールでの操作内容のログ取得などの技術的対策のほかに，②第4ゾーンでは，来訪者の行動を事後に確認できるようにします。

B主任：分かりました。アンチパスバックと来訪者の行動を事後に確認できる設備の導入を検討します。また，来訪者を入室させる場合の対応方法については，情報セキュリティ管理規程に明記するようにします。項番3については，印刷物の放置を禁止していますが徹底できていません。何か良い方策はないでしょうか。

D氏：　御社の複合機本体には，社員カードが使用できるICカードリーダを装備できますから，ICカードリーダを装備して，オンデマンド印刷機能を利用することを推奨します。③オンデマンド印刷機能を利用すると，NPCから印刷指示した文書の用紙への印刷は，社員カードを複合機のICカードリーダにかざして認証を受けた後に行われることになります。

B主任：運用方法を検討してみます。項番4については，社員の反対が多く，私物の持込みは禁止できていません。社員に受け入れられる方策はないでしょうか。

D氏：　私物の鞄の持込みは禁止し，代わりに［　d　］鞄を貸与して，その中に入れた私物については，持込みを許可するのが良いでしょう。その場合，持込みを禁止する私物の種類や持ち込んだ私物のオフィス内での使用上の禁止事項を，情報セキュリティ管理規程に明記してください。

B 主任：なるほど，その方策なら当社でも実施可能ですから，改善策として検討します。項番 5，6 については，実施すべき内容を情報セキュリティ管理規程に明記して徹底させるようにします。

D 氏：　それで良いと思います。

B 主任は打合せ結果を基に，オフィスの物理的対策を中心とした見直し案をまとめて，情報セキュリティ委員会に報告した。見直し案が承認され，情報セキュリティ管理規程の改定と対策案が実施されることになった。

設問 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　CC（Common Criteria）	イ　ISMS	ウ　JIS Q 15001
エ　UHF アンテナ	オ　Wi-Fi 電波	カ　アンテナコイル
キ　赤外線	ク　電磁波	ケ　ヘリカルアンテナ

設問 2　表 1 中の項番 5 の問題点への対策はクリアデスクと呼ばれるが，項番 6 の問題点への対策は何と呼ばれているか。10 字以内で答えよ。

設問 3　〔問題点についての打合せ〕について，(1)～(4)に答えよ。

(1)　本文中の下線①について，どのような場合に解錠しないかを，30 字以内で答えよ。

(2)　本文中の下線②について，具体的な対策内容を，25 字以内で述べよ。

(3)　本文中の下線③の機能が，表 1 中の項番 3 の問題を低減させる対策になる理由を，30 字以内で述べよ。

(4)　本文中の［　d　］に入れる適切な字句を，10 字以内で答えよ。また，その鞄の貸与によって，禁止された私物の持込みのほかに，低減できる可能性のある不正行為を，15 字以内で答えよ。

次の問1は必須問題です。必ず解答してください。

問1　DNSのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

R社は，Webサイト向けソフトウェアの開発を主業務とする，従業員約50名の企業である。R社の会社概要や事業内容などをR社のWebサイト（以下，R社サイトという）に掲示している。

R社内からインターネットへのアクセスは，R社が使用するデータセンタを経由して行われている。データセンタのDMZには，R社のWebサーバ，権威DNSサーバ，キャッシュDNSサーバなどが設置されている。DMZは，ファイアウォール（以下，FWという）を介して，インターネットとR社社内LANの両方に接続している。データセンタ内のR社のネットワーク構成の一部を図1に示す。

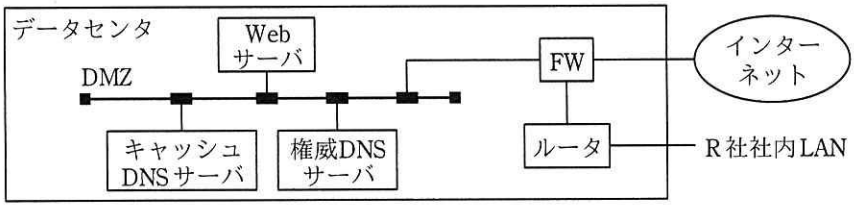


図1　データセンタ内のR社のネットワーク構成（一部）

R社サイトは，データセンタ内のWebサーバで運用され，インターネットからR社サイトへは，HTTP Over TLS（以下，HTTPSという）によるアクセスだけが許されている。

〔インシデントの発生〕

ある日，R社の顧客であるY社の担当者から，“社員のPCが，R社サイトに埋め込まれていたリンクからマルウェアに感染したと思われる”との連絡を受けた。Y社は，Y社が契約しているISPであるZ社のDNSサーバを利用していた。

R社情報システム部のS部長は，部員のTさんに，R社のネットワークのインターネット接続を一時的に切断し，マルウェア感染の状況について調査するように指示した。Tさんが調査した結果，R社の権威DNSサーバ上の，R社のWebサーバのAレコードが別のサイトのIPアドレスに改ざんされていることが分かった。R社のキャッシュDNSサーバとWebサーバには，侵入や改ざんされた形跡はなかった。

Tさんから報告を受けたS部長は，①Y社のPCがR社の偽サイトに誘導され，マルウェアに感染した可能性が高いと判断した。

〔当該インシデントの原因調査〕

S部長は，当該インシデントの原因調査のために，R社の権威DNSサーバ，キャッシュDNSサーバ及びWebサーバの脆弱性診断及びログ解析を実施するよう，Tさんに指示した。Tさんは外部のセキュリティ会社の協力を受けて，脆弱性診断とログ解析を実施した。診断結果の一部を表1に示す。

表1　R社サーバの脆弱性診断及びログ解析の結果（一部）

診断対象	脆弱性診断結果	ログ解析結果
権威DNSサーバ	・OSは最新であったが，DNSソフトウェアのバージョンが古く，［　a　］を奪取されるおそれがあった。 ・インターネットから権威DNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	業務時間外にログインされた形跡が残っていた。
キャッシュDNSサーバ	・OS及びDNSソフトウェアは最新であった。 ・インターネットからキャッシュDNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	不審なアクセスの形跡は確認されなかった。
Webサーバ	・OS及びWebサーバのソフトウェアは最新であった。 ・インターネットからWebサーバへのアクセスはHTTPSだけに制限されていた。	Y社のPCがマルウェア感染した時期に②R社サイトへのアクセスがほとんどなかった。

診断結果を確認したS部長は，R社の権威DNSサーバのDNSソフトウェアの脆弱性を悪用した攻撃によって［　a　］が奪取された可能性が高いと考え，早急にその脆弱性への対応を行うようにTさんに指示した。

Tさんは，R社の権威DNSサーバのDNSソフトウェアの脆弱性は，ソフトウェアベンダが提供する最新版のソフトウェアで対応可能であることを確認し，当該ソフトウェアをアップデートしたことをS部長に報告した。S部長はTさんに，R社の権威DNSサーバ上のR社のWebサーバのAレコードを正しいIPアドレスに戻し，R社のネットワークのインターネット接続を再開させたが，Y社のPCからR社サイトに正しくアクセスできるようになるまで，③しばらく時間が掛かった。R社は，Y社に謝罪するとともに，当該インシデントについて経緯などをとりまとめて，R社サイトなどを通じて，顧客を含む関係者に周知した。

〔セキュリティ対策の検討〕

S 部長は，R 社の権威 DNS サーバに対する④同様なインシデントの再発防止に有効な対策と，R 社のキャッシュ DNS サーバ及び Web サーバに対するセキュリティ対策の強化を検討するように，T さんに指示した。

T さんは，R 社の Web サーバが使用しているディジタル証明書が，ドメイン名の所有者であることが確認できる DV（Domain Validation）証明書であることが問題と考えた。そこで T さんは，EV（Extended Validation）証明書を導入することを提案した。R 社の Web サーバに EV 証明書を導入し，Web ブラウザで R 社サイトに HTTPS でアクセスすると，R 社の［ b ］を確認できる。

また T さんは，⑤R 社のキャッシュ DNS サーバがインターネットから問合せ可能であることも問題だと考えた。その対策として，FW の設定を修正して R 社社内 LAN からだけ問合せ可能とすることを提案した。また，R 社のキャッシュ DNS サーバに，偽の DNS 応答がキャッシュされ，R 社の社内 LAN 上の PC がインターネット上の偽サイトに誘導されてしまう，［ c ］の脅威があると考えた。DNS ソフトウェアの最新版を確認したところ，ソースポートのランダム化などに対応していることから，この脅威については対応済みとして報告した。

設問 1　本文中の下線①で，Y 社の PC が R 社の偽サイトに誘導された際に，Y 社の PC に偽の IP アドレスを返した可能性のある DNS サーバを，解答群の中から全て選び，記号で答えよ。

解答群

ア　DNS ルートサーバ　　イ　R 社のキャッシュ DNS サーバ

ウ　R 社の権威 DNS サーバ　　エ　Z 社の DNS サーバ

設問 2　〔当該インシデントの原因調査〕について，(1)～(3)に答えよ。

(1)　表 1 及び本文中の［ a ］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　管理者権限　　イ　シリアル番号

ウ　ディジタル証明書　　エ　利用者パスワード

(2) 表 1 中の下線②で，R 社サイトへのアクセスがほとんどなかった理由を 20 字以内で述べよ。

(3) 本文中の下線③で，Y 社の PC が正しい R 社サイトにアクセスできるようになるまで，しばらく時間が掛かった理由は，どの DNS サーバにキャッシュが残っていたからか，解答群の中から選び，記号で答えよ。

解答群

ア DNS ルートサーバ　　イ R 社のキャッシュ DNS サーバ

ウ R 社の権威 DNS サーバ　　エ Z 社の DNS サーバ

設問3 〔セキュリティ対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線④で，同様なインシデントの再発防止に有効な対策として，R 社の権威 DNS サーバに実施すべきものを，解答群の中から選び，記号で答えよ。

解答群

ア 逆引き DNS レコードを設定する。

イ シリアル番号の桁数を増やす。

ウ ゾーン転送を禁止する。

エ 定期的に脆弱性検査と対策を実施する。

(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。

解答群

ア 会社名　　イ 担当者の電子メールアドレス

ウ 担当者の電話番号　　エ ディジタル証明書の所有者

(3) 本文中の下線⑤で，R 社のキャッシュ DNS サーバがインターネットから問合せ可能な状態であることによって発生する可能性のあるサイバー攻撃を，解答群の中から選び，記号で答えよ。

解答群

ア DDoS 攻撃　　イ SQL インジェクション攻撃

ウ パスワードリスト攻撃　　エ 水飲み場攻撃

(4) 本文中の［ c ］に入れるサイバー攻撃手法の名称を，15 字以内で答えよ。

次の問1は必須問題です。必ず解答してください。

問1　通信販売サイトのセキュリティ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。

R社は，文房具やオフィス家具を製造し，店舗及び通信販売サイトで販売している。通信販売サイトでの購入には会員登録が必要である。通信販売サイトはECサイト用CMS（Content Management System）を利用して構築している。通信販売サイトの管理及び運用は，R社システム部門の運用担当者が実施していて，通信販売サイトに関する会員からの問合せは，システム部門のサポート担当者が対応している。

〔通信販売サイトの不正アクセス対策〕

通信販売サイトはR社のデータセンタに設置されたルータ，レイヤ2スイッチ，ファイアウォール（以下，FWという），IPS（Intrusion Prevention System）などのネットワーク機器とCMSサーバ，データベースサーバ，NTPサーバ，ログサーバなどのサーバ機器と各種ソフトウェアとで構成されている。通信販売サイトは，会員情報などの個人情報を扱うので，様々なセキュリティ対策を実施している。R社が通信販売サイトで実施している不正アクセス対策（抜粋）を表1に示す。

表1　通信販売サイトの不正アクセス対策（抜粋）

項番	項目	対策
1	ネットワーク	IPSによる，ネットワーク機器及びサーバ機器への不正侵入の防御
2		ルータ及びFWでの不要な通信の遮断
3	ログサーバ	各ネットワーク機器，サーバ機器及び各種ソフトウェアのログを収集
4	CMSサーバ データベースサーバ	不要なアカウントの削除，不要な［　a　］の停止
5		OS，ミドルウェア及びCMSについて修正プログラムを毎日確認し，最新版の修正プログラムを適用
6		CMSサーバ上のWebアプリケーションへの攻撃を，［　b　］を利用して検知し防御

IPSは不正パターンをシグネチャに登録するシグネチャ型であり，シグネチャは毎日自動的に更新される。

項番4の対策をCMSサーバ及びデータベースサーバ上で行うことで不正アクセスを受けにくくしている。R社では，①項番5の対策を実施するために，OS，ミドルウ

エア及び CMS で利用している製品について必要な管理を実施して，脆弱性情報及び修正プログラムの有無を確認している。また，項番 6 の対策で利用している［ b ］は，ソフトウェア型を導入していて，シグネチャは R 社の運用担当者が，システムへの影響がないことを確認した上で更新している。

〔セキュリティインシデントの発生〕

ある日，通信販売サイトが改ざんされ，会員が不適切なサイトに誘導されるというセキュリティインシデントが発生した。通信販売サイトを閉鎖し，ログサーバが収集したログを解析して原因を調査したところ，特定のリクエストを送信すると，コンテンツの改ざんが可能となる CMS の脆弱性を利用した不正アクセスであることが判明した。

R 社の公式ホームページでセキュリティインシデントを公表し，通信販売サイトの復旧と CMS の脆弱性に対する暫定対策を実施した上で，通信販売サイトを再開した。

今回の事態を重く見たシステム部門の S 部長は，セキュリティ担当の T 主任に今回のセキュリティインシデント対応で確認した事象と課題の整理を指示した。

〔セキュリティインシデント対応で確認した事象と課題〕

T 主任は関係者から，今回のセキュリティインシデント対応について聞き取り調査を行い，確認した事象と課題を表 2 にまとめて，S 部長に報告した。

表 2　セキュリティインシデント対応で確認した事象と課題（抜粋）

項番	確認した事象	課題
1	CMS の脆弱性を利用して不正アクセスされた。	CMS への修正プログラム適用は手順どおり実施されていたが，今回の不正アクセスに有効な対策がとられていなかった。
2	［ b ］のシグネチャが更新されていなかった。	［ b ］は稼働していたが，運用担当者がシグネチャを更新していなかった。
3	通信販売サイトが改ざんされてからサイト閉鎖まで時間を要した。	サイト閉鎖を判断し指示するルールが明確になっていなかった。
4		改ざんが行われたことを短時間で検知できなかった。
5	原因調査に時間が掛かり，R社の公式ホームページなどでの公表が遅れた。	ログサーバ上の各機器やソフトウェアのログを用いた相関分析に時間が掛かった。

S部長はT主任からの報告を受け，セキュリティインシデントを専門に扱い，インシデント発生時の情報収集と各担当へのインシデント対応の指示を行うインシデント対応チームを設置するとともに，今回確認した課題に対する再発防止策の立案をT主任に指示した。

〔再発防止策〕

T主任は，再発防止のために，表2の各項目への対策を実施することにした。

項番1については，CMSサーバを構成するOS，ミドルウェア及びCMSの脆弱性情報の収集や修正プログラムの適用は実施していたが，②今回の不正アクセスのきっかけとなった脆弱性に対応する修正プログラムはまだリリースされていなかった。このような場合，OS，ミドルウェア及びCMSに対する③暫定対策が実施可能であるときは，暫定対策を実施することにした。

項番2については，［ b ］の運用において，新しいシグネチャに更新した際に，デフォルト設定のセキュリティレベルが厳し過ぎて正常な通信まで遮断してしまう［ c ］を起こすことがあり，運用担当者はしばらくシグネチャを更新していなかったことが判明した。運用担当者のスキルを考慮して，運用担当者によるシグネチャ更新が不要なクラウド型［ b ］サービスを利用することにした。

項番3については，［ d ］がセキュリティインシデントの影響度を判断し，サイト閉鎖を指示するルールを作成して，サイト閉鎖までの時間を短縮するようにした。

項番4については，サイトの改ざんが行われたことを検知する対策として，様々な検知方式の中から未知の改ざんパターンによるサイト改ざんも検知可能であること，誤って検知することが少ないことから，ハッシュリスト比較型を利用することにした。

項番5については，④各ネットワーク機器，サーバ機器及び各種ソフトウェアからログを収集し時系列などで相関分析を行い，セキュリティインシデントの予兆や痕跡を検出して管理者へ通知するシステムの導入を検討することにした。

T主任は対策を取りまとめてS部長に報告し，了承された。

設問1　表1中の［　a　］に入れる適切な字句を5字以内で答えよ。

設問2　本文及び表1，2中の［　b　］に入れる適切な字句をアルファベット3字で答えよ。

設問3　本文中の下線①で管理するべき内容を解答群の中から全て選び，記号で答えよ。

解答群

ア　販売価格　　イ　バージョン

ウ　名称　　エ　ライセンス

設問4　〔再発防止策〕について，(1)～(5)に答えよ。

(1)　本文中の下線②の状況を利用した攻撃の名称を8字以内で答えよ。

(2)　本文中の下線③について，暫定対策を実施可能と判断するために必要な対応を解答群の中から選び，記号で答えよ。

解答群

ア　過去の修正プログラムの内容を確認

イ　修正プログラムの提供予定日を確認

ウ　脆弱性の回避策を調査

エ　同様の脆弱性が存在するソフトウェアを確認

(3)　本文中の［　c　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　過検知　　イ　機器故障　　ウ　未検知　　エ　予兆検知

(4)　本文中の［　d　］に入れる適切な組織名称を本文中の字句を用いて15字以内で答えよ。

(5)　本文中の下線④のシステム名称をアルファベット4字で答えよ。