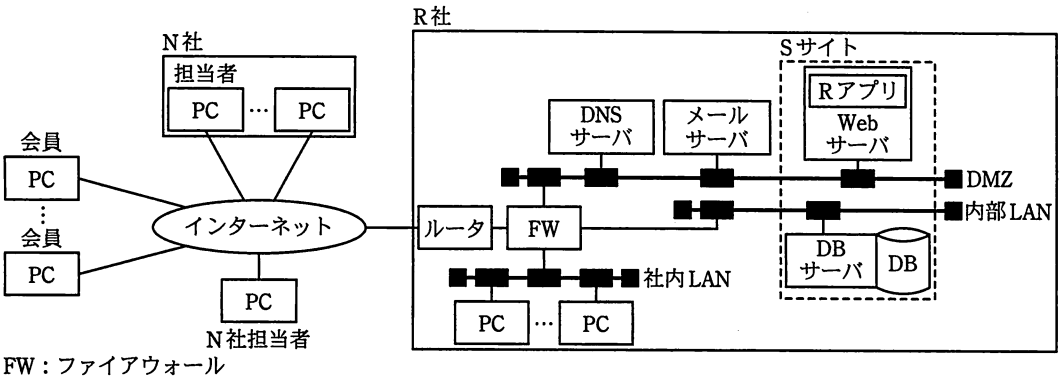
問4　Web サイトのセキュリティ対策に関する次の記述を読んで，設問 1，2 に答えよ。

R 社は，おもちゃの会員制オークションサイト（以下，S サイトという）を運用し，その販売手数料を主な収入源としている従業員数 40 名のネットオークション会社である。

S サイトは図 1 のとおり，主に Web サーバ及び Web サーバ上で動作する Web アプリケーションであるオークションアプリケーション（以下，R アプリという），並びにデータベース（DB）で構成されている。



FW：ファイアウォール

注記　FW ではドロップログ（通信を拒否したログ）だけを収集している。

図 1　R 社のシステム構成

S サイトのサーバの管理と R アプリの保守は R 社のシステム課が担当しており，社内 LAN からアクセスしている。DB の保守においては，Web サーバにある DB 接続用クライアントツール（以下，DB 接続ツールという）を使って接続する。

一方，HTML ファイルや画像ファイルなどのコンテンツファイルの保守はホームページデザイン会社である N 社に委託している。N 社の担当者には FTP で Web サーバにコンテンツファイルを転送するためのアカウント（以下，CNT-MGR という）が付与されており，N 社内で作成されたファイルを Web サーバに転送している。

R アプリは，Perl で開発されたスクリプトである。R アプリのスクリプトには，DB への接続情報（DB 利用者 ID，パスワード），ビジネスロジック，及び画面表示処理が含まれている。R アプリが DB に接続するときには，DB 接続ツールとは異なる Perl 用の DB 処理モジュールを利用している。DB には，会員データが約 3 万件あり，暗号化されていない状態で格納されている。

Sサイトでは，会員のメールアドレスを会員IDとしており，会員はSサイトのログインページで，会員IDとパスワードを入力してログインする。

R社のシステム課はK課長を中心に，会員向けの機能追加を目的としてRアプリの改修に取り組んでおり，現在は設計フェーズである。

〔ペネトレーションテストによる現状確認〕

他社のオークションサイトで，会員情報の流出事件が起きたことから，R社の経営陣はK課長にSサイトのセキュリティ対策を確認するように指示した。K課長は現状のセキュリティ対策の有効性を確認するために，セキュリティ専門会社であるW社に，インターネット及びN社のオフィスからのペネトレーションテスト（以下，Pテストという）を依頼した。表1は，W社が報告したPテストの結果である。

表1　Pテストの結果

項番	問題点
V-1	Sサイトのログインページで，Pテスト用の会員IDによるログインが何度も失敗したにもかかわらずアカウントがロックされなかった。
V-2	Sサイトからいったんログアウトした後に，再びログインせずに，URLを直接指定することでSサイトの会員個人の専用情報ページを閲覧できた。
V-3	Webサーバの HTTP サービスの脆弱性を突いて，Webサーバに侵入できた。
V-4	V-3の侵入方法によってWebサーバに侵入後，Webサーバ内のファイルをFTPでR社の外部に送信できた。
V-5	CNT-MGRのパスワードを推測して，Webサーバへの FTP 接続を何度か試行し，最終的に成功した。
V-6	Webサーバへのコンテンツファイル転送時の通信を盗聴して，CNT-MGRのパスワードを窃取できた。
V-7	CNT-MGRでWebサーバにログインした後，Webサーバ内の DB 接続ツールを実行し，DBMS 標準アカウントの初期パスワードでDBに接続できた。

〔セキュリティ対策の検討〕

K課長は，表1の結果を踏まえて対策の検討を行うために，W社のG氏に相談した。G氏は表1を見ながら，システム課のメンバから状況を聞いた上で，対策について助言した。次は，検討時の会話である。

K課長：V-1の対策としては，ログインページで，3回連続してログインが失敗したらアカウントをロックし，5分間は当該会員IDによるログインを受け付けなくします。また，V-2の対策としては，ログアウト時に［　a　］処理を実装します。

G 氏　：それでよいでしょう。少し気になることがありますが，後ほど説明します。

K 課長：P テストの時点では Web サーバのセキュリティパッチの適用を忘れていましたが，V-3 と V-4 の対策としては，システム課が DMZ に配置された全サーバに最新のセキュリティパッチを適用するよう徹底します。

G 氏は，サーバへのセキュリティパッチの適用だけでは V-4 の対策として不十分であるので，外部向けの不要な通信を拒否するように FW のフィルタリングルール（以下，FW ルールという）を変更することを提案した。さらに，①FW ルールに違反してファイルを外部送信する試みの有無をシステム課の担当者が調べるための方法についても説明した。

K 課長：なるほど，そうします。V-5，V-6 の対策としては，パスワードを複雑なものに設定し直した上で，コンテンツファイル転送時の認証方法を FTP の認証ではなく SSH のパスワード認証に変更しようと思います。その場合，ログインが連続失敗したらアカウントをロックするよう SSH を設定します。しかし，N 社の担当者が N 社以外からもアクセスする必要があるので，アクセス元を IP アドレスで制限できません。アクセス元を限定できないのが不安です。

G 氏　：SSH では，IP アドレス制限に頼らなくても，認証方式を［　b　］にすることによって，更にアクセス者を限定できます。

K 課長：なるほど，そうします。最後に V-7 の対策ですが，現状の Web サーバで CNT-MGR に付与されているファイルアクセス権限は図 2 のようになっています。第三者によって CNT-MGR が不正に使われた場合の対処も必要ですし，N 社の担当者にも DB 内の会員データの閲覧はもちろん DB 接続もさせたくないので，DBMS 標準アカウントの初期パスワードを変更した上で，CNT-MGR からコンテンツファイルの保守には必要のない DB 接続ツールの実行権限を削除します。それから，R アプリで鍵長 256 ビットの AES を使って，会員データを暗号化しようと考えています。その場合，暗号鍵は定数としてスクリプト内に定義します。

・スクリプトファイルに対して，読取り，書込み及び実行が可能である。
・コンテンツファイルに対して，読取り及び書込みが可能である。
・コンテンツ保守に必要なコマンドと，DB 接続ツールの実行が可能である。
（以下，省略）

図２　CNT-MGR に付与されているファイルアクセス権限

G 氏は，CNT-MGR に付与されているファイルアクセス権限の現状を考慮すると，K 課長が示した対策だけでは②N 社の担当者に会員データを閲覧されてしまう可能性が残ることを説明した。さらに，本来であればコンテンツファイルの確認のために新たに独立したテスト環境を構築し，N 社にはそのテスト環境にだけアクセスさせ，本番環境にはアクセスさせないようにすべきであることを説明した。その上で，テスト環境を用意するまでの③暫定対策を提示した。

G 氏　：先ほどの S サイトへのログインに関する件ですが，多くの会員は，S サイトに登録しているメールアドレスとパスワードの組合せ（以下，認証情報という）と同じものを，ほかの Web サイトでも登録していると思われます。④ほかの Web サイトで大量に盗まれた認証情報が悪用されて S サイトにログイン試行が行われ，結果として幾つかの会員 ID でのログインが成功してしまう可能性があります。V-1 の対策のアカウントロックは一つの会員 ID に対するログイン試行を想定しているので，大量のほかの Web サイトの認証情報を悪用するログイン成功を防ぐことはできません。

K 課長：それは，S サイトの脆弱性ではなく会員のパスワード設定の問題ですが，なりすまして S サイトにログインされた場合には，我々が会員への対応に追われることになるので，何らかの手を打った方がよさそうですね。

G 氏は，下線④のようなログイン試行をできる限り R アプリで検知して遮断するための方法を説明した。こうして K 課長は P テストの結果について対策案をまとめ，経営陣から承認を得た。その後，対策を順調に終え，無事に新しい R アプリをリリースすることができた。

設問1　Pテストの結果と対策について，(1)～(5)に答えよ。

(1) 本文中の［　a　］に入れる適切な処理を解答群の中から選び，記号で答えよ。

解答群

ア　クッキーにパスワードをセットする　　イ　再認証を行う

ウ　セッション情報を破棄する　　エ　ログを採取する

(2) 表1中のV-6の対策として，コンテンツファイル転送時に使用するサービスをSSHに変更した際，N社の担当者がコンテンツファイル転送時に使用するコマンドを，5字以内で答えよ。

(3) 本文中の［　b　］に入れるべき，表1中のV-5の問題を解決できるSSHの認証方式を10字以内で答えよ。

(4) 本文中の下線①の，FWルールに違反してファイルを外部送信する試みの有無を調べるための方法を35字以内で具体的に述べよ。

(5) 本文中の下線②の可能性について，N社の担当者がスクリプトファイルを悪用して会員データを閲覧するための方法を50字以内で具体的に述べよ。また，本文中の下線③の暫定対策の内容を40字以内で述べよ。

設問2　本文中の下線④に示すログイン試行を，Rアプリで検知して遮断するためには，どのような条件を用いて検知することが適切か。60字以内で述べよ。