次の問1は必須問題です。必ず解答してください。

問1　Web サーバに対する不正侵入とその対策に関する次の記述を読んで，設問に答えよ。

A 社は，口コミによる飲食店情報を収集し，提供する会員制サービス業者である。会員制サービスを提供するシステム（以下，A 社システムという）を図1に示す。

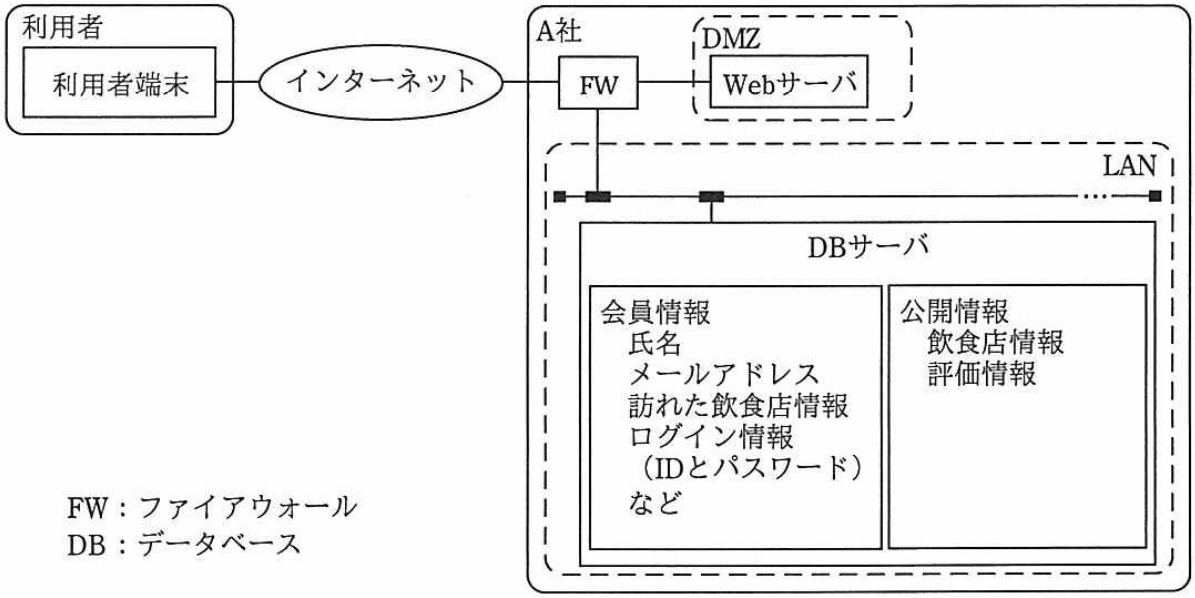

図1　A 社システム

(1) FW，Web サーバ及び DB サーバがあり，スマートフォンなどの利用者端末とはインターネットを介して接続されている。

(2) Web サーバは DMZ に置かれており，DB サーバは LAN に置かれている。また，利用者端末から Web サーバへの接続には，セキュリティを考慮して TLS を用いている。

(3) 会員登録を行った利用者（以下，会員という）には，ID とパスワードが発行される。

(4) DB サーバには，会員情報（氏名，メールアドレス，訪れた飲食店情報，ログイン情報（ID とパスワード）など）と公開情報（飲食店情報，評価情報）が保管されている。

(5) 会員は，公開情報を閲覧することができる。また，Web サーバにログインすることで，DB サーバに保管してある自分の会員情報と自らが書き込んだ公開情報の更新，及び新しい公開情報の追加が行える。

(6) 非会員は，公開情報の閲覧だけができる。

(7) 会員が Web サーバにログインするには，ID とパスワードが必要であり，A 社システムは DB サーバに保管してあるログイン情報を用いて認証する。

(8) Web サーバ及び DB サーバでは，それぞれでアクセスログ（以下，ログという）が記録されており，システム管理者が定期的に内容を確認している。また，システム管理者は，通常，LAN から Web サーバや DB サーバにアクセスして，メンテナンスを行っている。

なお，外部から Telnet や SSH で Web サーバに接続して，インターネットを介したリモートメンテナンスが行えるようにしてあるが，現在はリモートメンテナンスの必要性はなくなっている。

ある日，システム管理者が，ログの確認において，通常とは異なるログが記録されているのを発見した。そのログを詳しく調査したところ，システム管理者以外の者が管理者 ID と管理者パスワードを使って Web サーバに不正侵入したことが明らかになった。

そこで，システム管理者は上司と相談し，会員制サービスを直ちに停止した。次に，今回の不正侵入に対する被害状況の特定と対策の検討を行った。不正侵入による被害状況と対策の一部を抜粋したものを表 1 に示す。

表 1　不正侵入による被害状況と対策（抜粋）

被害状況	対策
Web サーバへの不正侵入があったことが確認された。秘密鍵への不正アクセスがあったかは確認できなかった。	a
FW を経由し，Web サーバに不正侵入され，さらにそこから DB サーバに不正侵入された。	リモートメンテナンス用ポートについて， b
一部の会員については会員情報が漏えいしたことが分かっているが，それ以外の会員については漏えいの有無を特定できていない。	パスワードを変更することにし， c

また，パスワードの変更に合わせて，パスワードの強度（パスワードの候補数）の検討を行った。これまでパスワードは，英小文字 26 文字だけを受け付け，長さは 6 文字だった。これに対し，他の 3 通りのパスワードの強度を比較した。その比較結果を表 2 に示す。

表 2　パスワードの強度比較（抜粋）

パスワードとして受け付ける文字種と長さ	強度の比較
(a) 英小文字，6 文字（不正侵入前の設定）	−
(b) 英小文字，8 文字	(a)と比較して［　d　］倍
(c) 英大文字・英小文字，8 文字	(b)と比較して［　e　］倍
(d) 英大文字・英小文字・数字・記号，8 文字	(c)と比較して更に多い

この強度の比較結果を踏まえ，次のように A 社システムを変更し，対策を実施した後に会員制サービスを再開することにした。

(1)　パスワードの文字種としては，英大文字と英小文字，数字，記号を受け付ける。

(2)　長さが 8 文字以上 16 文字以下から成るパスワードを受け付ける。

(3)　辞書に登録されている文字列など推測されやすいパスワードは受け付けない。

設問 1	a	設問 2	b	設問 3	c	設問 4	d	設問 5	e

設問　表1，2中の［　　］に入れる適切な答えを，解答群の中から選べ。

aに関する解答群

ア　TLS を使用していても不正侵入が行われたことから，TLS の使用を直ちに中止し，通常の HTTP で通信を行う。

イ　新たな秘密鍵と公開鍵を生成し，その鍵に対する公開鍵証明書の発行手続を行う。

ウ　公開鍵証明書の再発行手続を行い，同じ秘密鍵を使用する。

エ　秘密鍵へのアクセスが確認できていないことから，秘密鍵の変更や公開鍵証明書の再発行は行わず，念のため秘密鍵の保管場所を，ネットワーク経由でアクセスできないディレクトリに変更する。

bに関する解答群

ア　Telnet や SSH 以外に HTTP も利用できるようにするために，HTTP のポートを開放する。

イ　インターネットからのアクセスを FW で禁止し，Telnet や SSH のポートは閉じる。

ウ　システム管理者がどこからでもすぐに A 社システムのメンテナンスができるように，Telnet や SSH のポートの開放は継続する。

エ　パスワードや A 社システムの実装情報の漏えいを防ぐために，Telnet のポートは閉じ，SSH に限定してポートを開放する。

cに関する解答群

ア　管理者パスワードは変更し，全会員にパスワードの変更を依頼する。

イ　管理者パスワードは変更し，漏えいした会員だけにパスワードの変更を依頼する。

ウ　管理者パスワードはそのままにし，全会員にパスワードの変更を依頼する。

エ　管理者パスワードはそのままにし，漏えいした会員だけにパスワードの変更を依頼する。

dに関する解答群

ア　2×8　　イ　26　　ウ　2×26　　エ　7×8　　オ　10×26　　カ　26^2

eに関する解答群

ア　2　　イ　2×8　　ウ　26　　エ　208　　オ　2^8　　カ　26^8

問 1	a	イ
	b	イ
	c	ア
	d	カ
	e	オ