次の問1は必須問題です。必ず解答してください。

問1　個人情報保護の強化に関する次の記述を読んで，設問1，2に答えよ。

C 社は，服飾・雑貨のインターネット販売業者である。約 50,000 人の顧客が同社の会員制 Web サイトを利用している。会員制 Web サイトには HTTPS を使用してアクセスする必要がある。

顧客が会員制 Web サイトにログインするには会員番号が必要であり，会員登録時に，重複しない6桁の数字列をランダムに割り振っている。

C 社には，商品販売部門の他に，服飾類を扱う X 部門，生活雑貨を扱う Y 部門，そして輸入雑貨を扱う Z 部門の三つの商品開発部門がある。

〔C 社の現状〕

C 社の会員制 Web サイトは DMZ 内に設置してあり，セキュリティ専門会社に委託してインターネットからの不正アクセスの検知と対応を行っている。

C 社のネットワーク構成（抜粋）を図1に示す。

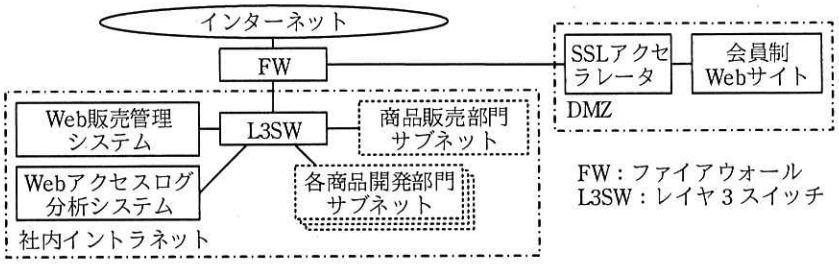

図1　C 社のネットワーク構成（抜粋）

C 社の会員制 Web サイトで扱う顧客情報や販売情報は，社内イントラネット内の Web 販売管理システムに蓄積されている。Web 販売管理システムの顧客情報データベースには，顧客の会員番号をキーとして，氏名，メールアドレス，電話番号，性別，年齢，住所などが格納されている。また，Web 販売管理システムの販売情報データベースには，顧客の会員番号をキーとして，該当顧客の販売情報が格納されている。二つのデータベースは磁気テープを用いて，月次でフルバックアップを行い，日次で増分バックアップを行っている。C 社の方針で過去1年間のバックアップデータを保管している。

C 社では，会員制 Web サイトの Web アプリケーションが出力する会員閲覧ログ（以下，Web サイト閲覧履歴という）を，毎日，社内イントラネット内の Web アクセスログ分析システムに転送して，その中に含まれる顧客の会員番号を基に，顧客ごとの閲覧履歴を分析している。

各商品開発部門は，Web サイト閲覧履歴や販売情報を参考にして，定期的に商品の品ぞろえを見直している。各商品開発部門では，有資格者だけが Web 販売管理システムにログインして，販売情報を PC で閲覧したり，CSV 形式のファイルで PC に出力したりすることができる。全顧客の Web サイト閲覧履歴も，有資格者だけが Web アクセスログ分析システムにログインして PC で閲覧したり，CSV 形式のファイルで PC に出力したりすることができる。有資格者が出力した Web サイト閲覧履歴や販売情報の CSV 形式のファイルは，分析完了後に PC から削除することになっている。

各商品開発部門の有資格者は有資格者リストで管理している。各商品開発部門からの申請に基づいて，システム部門が有資格者リストを更新するとともに，Web 販売管理システムや Web アクセスログ分析システムへのアクセス権限を設定する。

顧客情報データベースは，各商品開発部門には公開していない。各商品開発部門の有資格者が Web サイト閲覧履歴と販売情報を関連付け，閲覧した商品と売れ筋商品を分析する。その際，性別や地域，年齢などを必要とする場合，システム部門は，顧客情報から必要がない個人情報の箇所をマスクしたデータ（以下，加工個人情報という）を提供している。加工個人情報は，CSV 形式のファイルを暗号化して，電子メール（以下，メールという）に添付して有資格者に送付している。暗号化したファイルを復号するためのパスワードは別メールで送付することになっている。

〔個人情報保護の強化〕

システム部門の F 部長は，Web 販売管理システムのデータベースにある情報や，PC に保存されている Web サイト閲覧履歴や販売情報，加工個人情報について，社内からの不正アクセスや従業員の人的ミスによる漏えいのリスクが高いと考えた。会員番号を含めた個人情報が漏えいするおそれをできるだけ減らすためには，個人情報を含むデータの秘匿性を高める必要があると考え，社内で対策を協議した。

その結果，個人情報保護を強化するために，次の(1)～(4)の対策を実施することと

し，具体的な実現方法をシステム部門のD課長が検討することになった。

(1) Web販売管理システムへのアクセスはHTTPSによるものに限定する。

(2) 顧客情報データベースと販売情報データベースは，暗号化鍵を用いて暗号化する。バックアップデータからの情報漏えいを防ぐために，暗号化されたデータのままバックアップを行う。

(3) Web サイト閲覧履歴は，その中に含まれる会員番号を，元に戻せない仮の ID（以下，仮 ID という）に変換してから，Web アクセスログ分析システムに転送する。

(4) 各商品開発部門の有資格者が Web 販売管理システムにログインした場合は，［ a ］情報に含まれる会員番号を同じ方法で仮 ID に変換して提供する。

D課長は検討した結果をF部長に報告した。

D課長：データベースの暗号化アルゴリズムには，共通鍵暗号方式の［ b ］を採用しようと考えています。暗号化鍵は四半期に 1 回変更します。新しい暗号化鍵でのデータベースの再暗号化が完了次第，古い暗号化鍵は削除する予定です。

F部長：①古い暗号化鍵を削除する運用だと問題があります。過去の暗号化鍵も含めて鍵を管理するように検討し直してください。

D課長：分かりました。それから，仮 ID に変換する際には，変換後の ID が衝突しないように，会員番号に［ c ］を適用した結果を採用しようと考えています。

F部長：仮 ID から直接元の会員番号に戻すことはできませんが，万一，採用した［ c ］が知られてしまった場合には，②間接的に仮 ID から元の会員番号を特定できてしまいます。これを防ぐために，公開しない文字列と会員番号を文字列連結した結果に対して，［ c ］による変換を行ってください。

〔加工個人情報の提供方法の改善〕

加工個人情報をメールに添付して送付する方法には，次のリスクが存在することが

分かった。

・パスワードを別メールで送付する運用だと，［ d ］に対して効果がない。

・間違って別のファイルや暗号化していないファイルを添付してメールを送付するおそれがある。

・間違って［ e ］にメールを送付するおそれがある。

D 課長は，メールで送付する現状の受渡し方法ではリスクが高いと考え，加工個人情報を Web 販売管理システムに格納して，有資格者だけがアクセスできるように変更することにした。

設問 1　〔個人情報保護の強化〕について，(1)～(4)に答えよ。

(1)　本文中の［ a ］に入れる適切な字句を 4 字以内で答えよ。

(2)　本文中の［ b ］，［ 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。

b に関する解答群

ア　AES　　イ　MAC　　ウ　RSA　　エ　SHA

c に関する解答群

ア　共通鍵暗号方式　　イ　公開鍵暗号方式

ウ　ディジタル署名　　エ　ハッシュ関数

(3)　本文中の下線①について，どのような問題があるか。40 字以内で述べよ。

(4)　本文中の下線②について，仮 ID から元の会員番号をどのようにして特定することが可能か。35 字以内で述べよ。

設問 2　〔加工個人情報の提供方法の改善〕について，(1)，(2)に答えよ。

(1)　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　DoS 攻撃　　イ　盗聴

ウ　パスワードリスト攻撃　　エ　ブルートフォース攻撃

(2)　本文中の［ e ］に入れる適切な字句を 10 字以内で述べよ。