正　誤　表

情報処理安全確保支援士試験　午後Ⅰ　問題

ページ	問題番号	行	誤	正	訂正の内容
12	2	図2 下から 4行目	…，2の112乗の計算量が必要だと言われている。	…，2の112乗の計算量が必要だと言われている。<u>しかし，暗号化されたコンテンツ鍵は入手できないと考えてよい。</u>	下線部分を追加する。

問2　システム開発での情報漏えい対策に関する次の記述を読んで，設問 1～3 に答えよ。

R 社は従業員 500 名の情報サービス事業者である。営業部門，システム開発部門及び管理部門があり，管理部門内の情報システム部が社内の情報システムを管理している。システム開発部門の従業員は，一つ以上のシステム開発プロジェクト（以下，プロジェクトという）に参加している。

同業他社でのシステム開発において，情報漏えいが発生したことから，情報システム部の K 部長は部下の Z 主任に，プロジェクトにおいて秘密として扱われている設計文書（以下，設計秘密という）の管理について，問題がないか調査するように指示した。

〔設計秘密の管理〕

R 社の規則では，設計秘密は次のように管理することになっている。

・設計秘密は，R 社指定の文書作成ソフトウェア（以下，W ソフトという）を使って PC 上で作成及び暗号化を行い，R 社のネットワーク内のファイルサーバだけに保管する。ファイルサーバでは，プロジェクト単位にディレクトリを分け，各ディレクトリにはプロジェクトメンバだけがアクセスできるように，各プロジェクトのマネージャがアクセス権限を設定する。

・W ソフトでは，パスワードを基に 256 ビットの鍵が生成され，その鍵を使って，ファイルが AES で暗号化される。ファイルを開くときには，パスワードの入力が求められる。設計秘密には，プロジェクト単位のパスワード（以下，P パスワードという）を使用する。

・プロジェクトごとに，協力会社の T 社と秘密保持契約を結び，設計秘密を共有する。設計秘密は，T 社内でも R 社と同様の設備に保管し，アクセス権限を設定する。

・R 社と T 社の間で設計秘密をやり取りする際には，Web ブラウザからクラウドストレージサービスを利用する。R 社は，このクラウドストレージサービスでは，プロジェクト単位にディレクトリを分け，各ディレクトリには R 社と T 社のプロジェクトメンバだけがアクセスできるようにアクセス権限を設定する。

・プロジェクトを離任する者が出た場合には，ファイルサーバとクラウドストレー

ジサービスに保管しているプロジェクトの設計秘密に対して，離任者がアクセスできないようにする。

〔管理についての問題〕

Z 主任が，各プロジェクトのマネージャに，設計秘密の管理についてヒアリングしたところ，表 1 に示す問題があることが分かった。

表 1　設計秘密の管理についての問題

名称	問題
問題 1	ファイルを開くたびに P パスワードの入力が必要となり，作業負荷が高い。
問題 2	P パスワードの強度が十分でないおそれがある。
問題 3	プロジェクト離任者が出た場合，P パスワードが設定されている全てのファイルに対して [a] を行う必要があり，作業負荷が高い。
問題 4	プロジェクトメンバが，プロジェクト参加期間中に R 社の規則に反して [b] した設計秘密は，当該メンバであれば離任後も参照できてしまう。

〔問題への対策の検討〕

Z 主任は問題の解決に向けて，IRM（Information Rights Management）製品による対策を検討することにした。

Z 主任は，導入実績の豊富な L 社の IRM 製品（以下，IRM-L という）によって表 1 中の問題が解決できるかどうかを確認することにした。IRM-L は，複数の利用者から成るグループ単位にアクセス権限の付与ができる。IRM-L は IRM クライアントと IRM サーバから構成される。IRM クライアントは，PC にインストールされ，ファイルの暗号化及び復号を行う。IRM サーバは，IRM クライアントの管理を行う。IRM-L の概要を図 1 に示す。

1. IRM サーバ及び IRM クライアントの RSA 鍵ペア

IRM サーバをインストールする際，2048 ビットの RSA 鍵ペアが生成される（以下，IRM サーバで生成された公開鍵を IRM サーバ公開鍵といい，秘密鍵を IRM サーバ秘密鍵という）。IRM サーバ公開鍵は各 IRM クライアントに配付される。

IRM クライアントをインストールする際，2048 ビットの RSA 鍵ペアが生成される（以下，IRM クライアントで生成された公開鍵を IRM クライアント公開鍵といい，秘密鍵を IRM クライアント秘密鍵という）。

2. アカウントの種類

アカウントには次の 3 種類がある。

・利用者アカウント

利用者が使う。ファイルの保護及び保護されたファイルを開くことができる。利用者アカウントには利用者 ID，パスワード，メールアドレス，所属会社，所属部署，所属するグループなどの属性がある。

・グループ管理者アカウント

グループ管理者が使う。利用者アカウントをグループに所属させたり，グループから削除したりできる。

・IRM 管理者アカウント

IRM 管理者が使う。IRM サーバの設定，グループの管理，利用者アカウントの管理，グループ管理者アカウントの管理ができる。全てのグループに対して，グループ管理者アカウントと同様の権限をもつ。

3. 利用者とグループの管理

IRM 管理者は，IRM サーバ上にグループを作り，そのグループに対して，グループ管理者アカウントを作成する。

IRM 管理者は，IRM サーバ上に利用者アカウントを作成し，利用者 ID と初期パスワードを利用者に伝える。利用者は初回ログイン時に初期パスワードを変更する。

一つの利用者アカウントが，複数のグループに所属することもある。

4. IRM クライアントの起動とファイル保護の処理

IRM クライアントは，PC へのログイン時に自動起動される。利用者は IRM クライアントの起動画面に，利用者 ID とパスワードを入力する。IRM クライアントと IRM サーバとの通信は HTTPS で行う。

利用者がファイルの保護をするとファイルが暗号化され，ファイルの利用権限が自身の所属するグループのうち選択したグループに付与される。付与する権限は次から選ぶ。

参照：ファイルの参照だけを許可する。

編集：参照に加えて，ファイルの編集も許可する。編集後のファイルも IRM-L で保護される。

ファイルの保護では次の処理が行われる。

・ファイル単位に 256 ビットの AES 鍵（以下，コンテンツ鍵という）が生成され，ファイルはコンテンツ鍵で暗号化される。暗号化されたファイルには IRM-L 固有の拡張子が付与され，元のファイルと同じディレクトリに保存される。

・コンテンツ鍵は，IRM サーバ公開鍵で暗号化される。

・暗号化されたコンテンツ鍵は，暗号化後のファイルのハッシュ値及び付与された権限とともに IRM サーバに送信され，IRM サーバ内で保存される。

・IRM サーバへの送信後，PC 内のコンテンツ鍵と元のファイルは完全に削除される。

図 1　IRM-L の概要

5. 保護されたファイルを開くときの処理
保護されたファイルが開かれると，次の処理が行われる。
(i) IRM クライアントから利用者 ID，暗号化後のファイルのハッシュ値，及び IRM クライアント公開鍵が IRM サーバに送信される。
(ii) IRM サーバでは，暗号化後のファイルのハッシュ値が参照され，利用者アカウントがファイルに対する権限をもっている場合に，IRM サーバ秘密鍵でコンテンツ鍵が復号される。
(iii) IRM サーバでは，コンテンツ鍵が，IRM クライアント公開鍵で暗号化され，IRM クライアントに送られる。
(iv) IRM クライアントでは，送付されたコンテンツ鍵が IRM クライアント秘密鍵で復号される。
(v) IRM クライアントでは，コンテンツ鍵で対象ファイルが復号される。
(vi) 復号されたファイルに対しては，参照又は編集後に再びファイル暗号化の処理が行われる。

図 1　IRM-L の概要（続き）

Z 主任は，次のように IRM-L を利用することによって，表 1 中の問題を表 2 のとおり解決できると考えた。

・各プロジェクトにグループを一つ割り当てる。
・システム開発部門の従業員に IRM-L の利用者アカウントを割り当てる。
・設計秘密は，IRM-L で保護した上で，ファイルサーバに保管する。
・T 社のプロジェクトメンバも IRM-L を利用し，IRM-L で保護されたファイルを，クラウドストレージサービスにアップロードする。

表 2　設計秘密の管理についての問題に対する解決策

名称	IRM-L による解決策
問題 1	（省略）
問題 2	（省略）
問題 3	IRM-L では，ファイルの保護にパスワードを利用しない。また，①簡単な操作でプロジェクト離任者による設計秘密の参照を禁止できるので，従来と比較して大幅に作業負荷が減る。
問題 4	②プロジェクト離任者に対する操作を適切に行うことによって参照不可にできる。

問題 2 について，P パスワードの利用状況を調査したところ，英数字と一部の記号を用いた 10 字程度のパスワードの利用が多いことが分かった。それに基づいて，W ソフトによって暗号化されたファイルと IRM-L によって保護されたファイルの解読に必要な計算量を比較し，結果を図 2 にまとめた。

Wソフトによって暗号化されたファイルの解読：
鍵を総当たりで特定するには，最大で 2 の 256 乗の計算量が必要になる。また，その鍵を生成するためのPパスワードが文字種64種類で長さ10字とすると，Pパスワードの推測には最大で2の [c] 乗の計算量が必要になる。
IRM-Lによって保護されたファイルの解読：
コンテンツ鍵を総当たりで特定するには，最大で 2 の 256 乗の計算量が必要になる。また，コンテンツ鍵を保護するIRMサーバ公開鍵は2048ビットであり，NIST SP 800-57によると，RSA-2048のセキュリティ強度は112ビットの共通鍵暗号と同等であることから，RSA-2048を破るには，2の112乗の計算量が必要だと言われている。

以上から，IRM-Lによって保護されたファイルの解読はWソフトによって暗号化されたファイルの解読と比較して 2 の [d] 乗倍の計算量が必要になるので，より安全だと考えられる。

図2　比較結果

IRM-Lでは，一定時間当たりのログイン試行回数を制限する機能や，一定回数のログイン失敗でアカウントをロックする機能によって，攻撃者がログインに成功するリスクを下げることができる。しかし，利用者 ID とパスワードによる認証だけでは，推測が容易なパスワードを利用者が設定してしまうと，長さが 10 字であったとしても [e] 攻撃に対して脆弱(ぜい)となるので，[f] への変更が可能か検討することにした。

〔社外とのやり取り〕

T社ネットワークからIRMサーバにアクセスするには，IRMサーバをR社のDMZに設置し，インターネットからアクセス可能にする必要がある。Z主任は，IRMサーバをDMZに設置した場合のリスクと対策を表3のとおりまとめた。

表3　IRMサーバをDMZに設置した場合のリスクと対策（抜粋）

リスク	対策[1]
グループ管理者及びIRM管理者へのなりすまし	・[f] への変更 ・ログイン及びその試行の監視
IRM-L の既知の脆弱性を悪用したサーバへの侵入	・脆弱性修正プログラムの定期的な確認と適用 ・IPSの利用

注[1]　T社の一部の事業所はIPアドレスを固定できないので，T社のIPアドレスだけからアクセスを許可するという対策は取れない。

IRM-Lの運用について情報システム部で検討した結果，ここまで検討した対策を全て採用した場合でも，③PC がマルウェアに感染してしまうと，設計秘密の内容を不正に取得されてしまう場合があることが分かった。そこで，マルウェア対策の強化も導入計画に盛り込んだ上で，IRM-Lの導入を進めることにした。その後，IRM-Lを導入し，設計秘密に対する情報漏えい対策を強化することができた。

設問1　表1中の［　a　］に入れる適切な字句を15字以内で，表1中の［　b　］に入れる適切な字句を10字以内でそれぞれ答えよ。

設問2　〔問題への対策の検討〕について，(1)～(5)に答えよ。

(1)　表 2 中の下線①について，操作を行えるアカウントだけを解答群から全て選び，記号で答えよ。また，操作を35字以内で具体的に述べよ。

解答群

ア　IRM 管理者アカウント　　イ　グループ管理者アカウント

ウ　利用者アカウント

(2)　表2中の下線②について，参照不可になるのは，図1中の5.のどの処理でエラーになるからか。(i)～(vi)の記号で答えよ。

(3)　図2中の［　c　］，［　d　］に入れる適切な整数を答えよ。

(4)　本文中の［　e　］に入れる適切な字句を答えよ。

(5)　本文中及び表3中の［　f　］に入れる適切な字句を10字以内で答えよ。

設問3　本文中の下線③について，どのような動作をするマルウェアに感染すると不正に取得されるか。不正取得時のマルウェアの動作を 45 字以内で具体的に述べよ。