問1　ログ管理システム（情報セキュリティ）　(H27秋-FE 午後問1)

【解答】

［設問1］　a－イ
　　b－イ，c－カ（b，cは順不同）
［設問2］　エ
［設問3］　イ
［設問4］　ア
［設問5］　ウ，オ

【解説】

ログ管理システムに関する問題である。最近ではサイバー攻撃や情報漏えい事件が増えており，事実関係を確認するためのログの重要性が高まっている。例えば，サーバが攻撃された場合，ログを参照することで発生した事象の詳細を確認し，影響範囲を知り，二次被害防止の対策を立てることができる。

しかし，ログは単に取得するだけではなく，解析できるように複数のサーバ間の時刻を合わせる必要がある。加えて，取得したログが改ざんされたり，削除されたりしないようにすることも重要である。したがって，暗号化や改ざん検知の機能が必要になるが，ログにはシステムのユーザ ID などの機密情報が含まれることもあるため，ログにアクセスできないようにするというアクセス管理も重要である。

この問題は，ログ管理に特化しているが，セキュリティの基本的な知識も必要になる。その基礎知識を駆使し，さらに問題文を丁寧に読み込むことで，解答できるように実力を養ってほしい。

［設問1］

・空欄a：表1の空欄aに入れる仕組みを答える。ログの問題といえば，時刻同期は必ずといっていいほど問われる。したがって，直感で（イ）の「各業務システムの時刻を同期させる」を選んだ人もいたであろう。もし，時刻がバラバラであれば，正確な時刻の把握や，複数のシステムのログを突き合わせること，時系列での分析が困難になる。表1の No.1 の要件には「いつ，誰が，どの端末からどの業務システムをどのように操作したかが追跡できる」とあり，「いつ」というキーワードがある。時刻を同期させることは，仕組みとして必要であることが分かる。

　他の四つの選択肢は，「要件」の内容を実現する仕組みになっていない。

　（ア）の「各業務システムの稼働状況」，（ウ）の「検知処理のログ管理システムへのアクセス」，（エ）の「ログ集積ファイルへのアクセス」を監視しても，システムの操作を追跡することには寄与しない。

　また，（オ）の「ログ集積ファイルを圧縮する」ことは，ディスク容量の削減に寄与するもので，要件の内容とは関係がない。

　したがって，（イ）が正解である。

・空欄b，c：表1の No.2 の要件は，「ログ管理システムから外部の機器に出力される外部ログ集積ファイルには，改ざんと漏えいを防止する対策を講じる」ことである。ここでのポイントは，セキュリティ面の「改ざん」と「漏えい」のリスクであり，この二つのリスクに対する仕組みを選ぶ。

　まず，「改ざん」対策は，（イ）の「ログ集積ファイルに電子署名を付加する」ことで検知できる。電子署名を復号したものと，ファイルをハッシュしたものを比較し，一致しなければ改ざんがされていると判断できる。

　次に，「漏えい」対策は，（カ）の「ログ集積ファイルを暗号化する」仕組みが必要になる。暗号化すれば，万が一漏えいした場合でも，情報を読み取られる心配がない。

　他の選択肢を見てみてみよう。

　（ア）の「同一内容の複数個のログ集積ファイルを出力する」は，一つのファイルだけが改ざんされた場合には，改ざんを検知できる。しかし，複数個のファイルが全て改ざんされる可能性もあり，効果は限定的である。

　（ウ）の「ログ集積ファイルの出力に当たっては，推測しにくい名称を付ける」ことや，（エ）の「ログ集積ファイルのログ中の個人情報を削除する」ことでも，改ざんと漏えいのリスクは残る。

　（オ）のように，「ログ集積ファイルを圧縮する」としても，セキュリティ上の効果はない。

　したがって，（イ）と（カ）が正解である。

［設問2］

ログに共通して含むべき項目であり，問題文を丁寧に読み込む必要がある。

まず，設問文の「ログ管理システムの要件」は，問題文の〔ログ管理システムの要件（抜粋）〕の(1)に「ログ集積ファイルを基に，いつ，誰が，どの端末からどの業務システムをどのように操作したかが追跡できる」と記述されている。

また，〔業務システムの利用とログの説明（抜粋）〕には，「B 社の社員は，固定の IP アドレスが設定されている端末から，一意に社員を特定できる社員 ID で，業務システムのうちの一つにログインし，“参照”，“更新”，“ダウンロード”の操作を行う」とあり，〔ログ管理システムの概要（抜粋）〕には「ログには，業務システムを識別するための業務 ID や，社員が実施した操作を示す，“参照”，“更新”，“ダウンロード”の操作種別などが含まれている」とある。

これらを踏まえて考えると，要件の「誰が」は「社員 ID」，「どの端末から」は「固定の IP アドレスが設定されている端末」，「どの業務システム」は「業務 ID」によって識別できることが分かる。

したがって，（エ）の「端末の IP アドレス，業務 ID，社員 ID」が正解である。

［設問3］

表2の空欄に当てはまるものを考える。この問題も丁寧な読込みと，理解が必要である。

まず，「ログ管理システムへのログイン」に関して確認すると，〔ログ管理システムの概要（抜粋）〕には「各業務システムに組み込まれている検知処理が，ログの書込みを検知し，そのログをログ管理システムのサーバ上の業務システム別のログファイルに書き込む」，〔ログ管理システムの要件（抜粋）〕の(2)には「ログ管理システムのサーバ上のログファイルに書き込む処理は，ログ管理システムへのログインを必要とする」とある。

このことから，検知処理では，ログファイルに書き込むためにログ管理システムへログインする。したがって，空欄 d1 は「可」である。この時点で正解は（ア）と（イ）に絞られる。

次の「ログファイルへのアクセス」は，表1の No.1 の仕組みにある「検知処理が，ログ管理システムのサーバ上のログファイルに書き込む」という記述から，書込みを示す「W」が入ることが分かる。加えて，R や E のアクセス権が付与されている可能性もあるが，問題文にはそれらしき記述はない。したがって，（イ）が正解である。

［設問4］

業務システムの検知処理にて，通信に必要な公開鍵の数が問われている。まず，問題文と図1を見て，どのような通信があるかを再確認する。

問題文の冒頭には「ログ管理システムの対象になる業務システムは，図1のネットワーク構成図に示す，勤務管理システム，販売管理システム，生産管理システム及び品質管理システムの四つである」という記述がある。このことから，ログ管理システムは，この四つのサーバと通信をすることが分かる。したがって，公開鍵は最大でも四つあれば十分である。

次に，具体的にどのように暗号化がされているのかを考える。この通信は，各業務システムからログ管理システムへの一方向の通信である。通信を第三者に見られないようにするには，ログ管理システムの公開鍵で通信を暗号化する。仮に各業務システムの公開鍵で暗号化した場合，それぞれの公開鍵とペアになっている秘密鍵は各業務システムがもつことになるため，ログ管理システムは通信を復号することができない。

したがって，四つの通信経路ともに，ログ管理システムの公開鍵で暗号化し，ログ管理システムが自身の秘密鍵で復号すればよいことになる。つまり，公開鍵は一つだけでよい。

したがって，（ア）の「1」が正解である。

［設問5］

設問文にある「業務システムへの不正アクセス」を問題文から探す。〔業務システムの利用とログの説明（抜粋）〕に「一人の社員が，同時に複数の業務システムを使わないこと」及び「業務システム全体からデータを1日に 5M バイトを超えてダウンロードしないことを業務システムの利用規程で定めている」という二つの内容が記述されている。よって，これに該当する選択肢を探せばよい。

まず，「一人の社員が，同時に複数の業務システムを使わないこと」に該当する選択肢は（ウ）の「ある業務システムの連続した“更新”のログの間に，別の業務システムのログが書き込まれたとき」である。連続した“更新”のログの間に，ログアウトと再ログインは行っていない。なぜなら，〔業務システムの利用とログの説明（抜粋）〕に「社員が，業務システムにログインしたときに“参照”のログがログファイルに書き込まれる」とあるからである。このことから，別の業務システムのログが書き込まれた原因は，同時に複数の業務システムを使用したからに他ならない。

次に，「1日に 5M バイトを超えてダウンロードしないこと」は簡単である。（オ）は「業務システムからダウンロードされたデータ量が1日で 5M バイトを超えたとき」とある。

したがって，（ウ），（オ）が正解である。