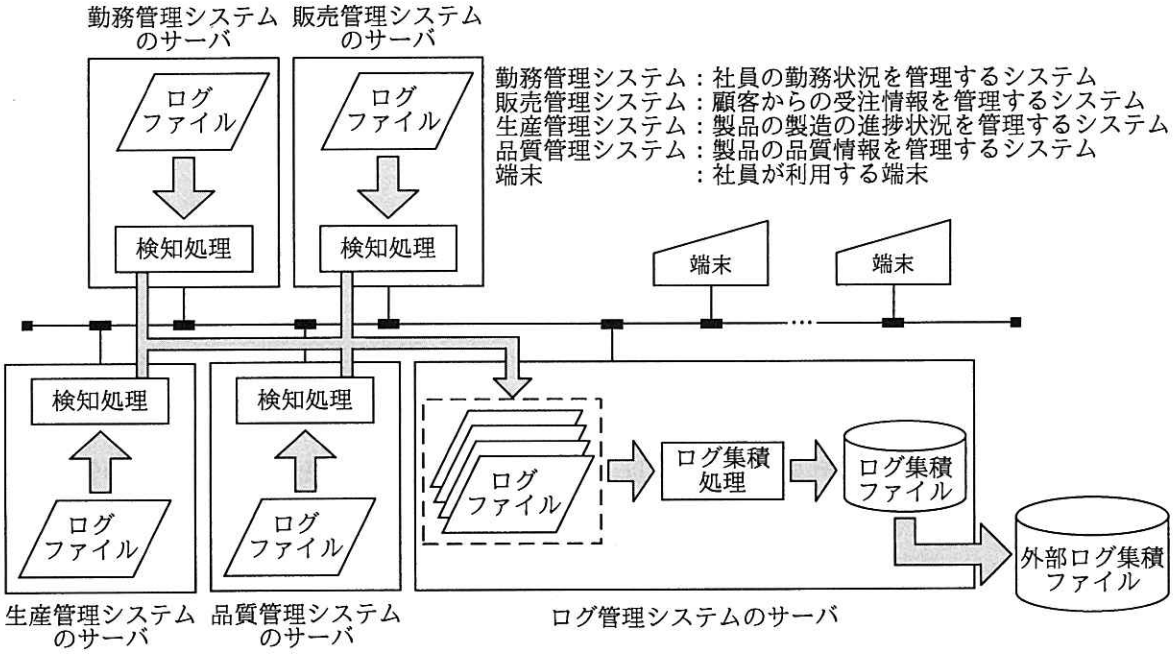
次の問１は必須問題です。必ず解答してください。

問１　ログ管理システムに関する次の記述を読んで，設問1～5に答えよ。

中堅の製造業である B 社では，他社で発生した情報漏えい事件を受けて，社内の業務システムへの不正アクセスを早期に検知するための仕組みを強化することになった。B 社では，業務システムのアクセスログ（以下，ログという）を一元管理するために，ログ管理システムを構築することにした。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。各管理システムには，1台のサーバが割り当てられている。



注記　⇨はログを収集する流れを示す。

図１　ネットワーク構成図

〔業務システムの利用とログの説明（抜粋）〕

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。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。また，ダウンロードの都度，そのデータ量を記録したログがログファイルに書き込まれる。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。

〔ログ管理システムの概要（抜粋）〕

業務システムの各サーバ上のログファイルにログが書き込まれると，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。書き込まれたログは，ログ管理システムのログ集積処理が，各業務システムのログを一元管理するログ集積ファイルに書き込む。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。

〔ログ管理システムの要件（抜粋）〕

(1) 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。

(2) 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。

(3) ログ管理システムの管理者（以下，ログ管理者という）と業務システムの管理者（以下，業務システム管理者という）だけが，ログ集積ファイルを参照できる。

(4) ログ管理者は，ログ集積ファイルをログ管理システムから外部の機器に出力することができる。

(5) 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。

(6) 各サーバ間の通信には，公開鍵暗号方式を利用する。

(7) ①ログ集積ファイルに書き込まれたログが一定条件を満たした際には，電子メールでログ管理者に通報する。

〔ログ管理システムの概要（抜粋）〕及び〔ログ管理システムの要件（抜粋）〕を基に，表1のログ管理システムの仕組み（抜粋）と，表2のログ管理システムへのアクセス権限表（抜粋）を作成した。

表1　ログ管理システムの仕組み（抜粋）

No.	要件	仕組み
1	ログ管理システムの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。	・業務システムに組み込まれた検知処理が，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。 ・ログファイルのログをログ集積ファイルに書き込む。 ・［ a ］。
2	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。	・［ b ］。 ・［ c ］。

表2　ログ管理システムへのアクセス権限表（抜粋）

	ログ管理システムへのログイン	ログファイルへのアクセス	ログ集積ファイルへのアクセス
ログ管理者	可		RE
業務システム管理者	可		R
検知処理	［ d1 ］	［ d2 ］	

注記　網掛けの部分は表示していない。
　　Rは参照，Eは外部へ出力，Wは書込みを示す。

設問1　表1中の［　　］に入れる要件を満たす仕組みとして適切な答えを，解答群の中から選べ。

aに関する解答群

ア　各業務システムの稼働状況を監視する

イ　各業務システムの時刻を同期させる

ウ　検知処理のログ管理システムへのアクセスを監視する

エ　ログ集積ファイルへのアクセスを監視する

オ　ログ集積ファイルを圧縮する

b，cに関する解答群

ア　同一内容の複数個のログ集積ファイルを出力する

イ　ログ集積ファイルに電子署名を付加する

ウ　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

エ　ログ集積ファイルのログ中の個人情報を削除する

オ　ログ集積ファイルを圧縮する

カ　ログ集積ファイルを暗号化する

設問2　ログ管理システムの要件を満たすために，日時，操作種別以外で全てのログに共通して含むべき項目を全て挙げた適切な答えを，解答群の中から選べ。

解答群

ア　業務ID，社員ID

イ　業務システムのサーバのIPアドレス，業務ID

ウ　業務システムのサーバのIPアドレス，業務ID，社員ID

エ　端末のIPアドレス，業務ID，社員ID

オ　端末のIPアドレス，社員ID

設問3　表2中の［　　］に入れる適切な答えを，解答群の中から選べ。ここで，d1とd2に入れる答えは，解答群の中から組合せとして適切なものを選ぶものとする。

解答群

	d1	d2
ア	可	RE
イ	可	W
ウ	不可	E
エ	不可	RE
オ	不可	RW
カ	不可	W

設問4　業務システムの検知処理はログ管理システムのサーバ上のログファイルへ書き込む。この通信を暗号化するために最低限必要な公開鍵の数として適切な答えを，解答群の中から選べ。

解答群

ア　1　　イ　4　　ウ　8　　エ　12

設問5　ログ集積ファイルを基に，業務システムへの不正アクセスを早期に検知するために，〔ログ管理システムの要件（抜粋）〕の下線①で言及している一定条件として適切な答えを，解答群の中から二つ選べ。ここで，解答群は，同じ社員 ID のログに対する条件とする。

解答群

ア　1日中“参照”のログだけが書き込まれたとき

イ　1日の間に“更新”のログが1回以上，書き込まれたとき

ウ　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

エ　同じ業務システムの“参照”と“更新”のログが連続して書き込まれたとき

オ　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

カ　特定の業務システムの“参照”のログが 15 分間，書き込まれていないとき