問1　医療情報システムの要件定義と設計に関する次の記述を読んで，設問1～4に答えよ。

Z病院は，病床数300の私立総合病院である。Z病院では，今年度，医療のサービス向上を目的に，医療情報システムの導入を決定した。今回導入する医療情報システムでは，診療録（カルテと呼ばれる）及び診療諸記録の両者を含む種々の医療情報を電子化する（以下，電子化された医療情報を電子カルテという）。

医療情報システムでは，次の機能を実現する。

(1) 医療情報の記録，更新，保管，検索の機能（以下，これらの機能を電子カルテ機能という）

(2) 検査や注射などの処置や薬の処方などの医師からの指示を担当部門に伝達する機能

(3) 診療費の会計処理などを行う医事会計システムに情報を伝達する機能

Z病院では，プロジェクトチーム（以下，Zチームという）を組織した。ZチームにはITに詳しいF医師がリーダとして，病院内組織から医師，看護師，薬剤師，医療事務員など医療従業者の職種ごとの代表者がメンバとして，また，医療情報システムの導入経験が豊富なコンサルタントのM氏がアドバイザとして，それぞれ参画することになった。

〔Z病院の情報セキュリティと個人情報保護に関する基本方針〕

Z病院の情報セキュリティ基本方針を図1に示す。

■目的

本方針では，Z 病院の，情報セキュリティ対策の適用の対象や情報資産の分類などを定め，Z 病院が保有する情報資産の機密性，完全性及び可用性を維持すべく，継続的に実施されるべき対策を定める。

■適用範囲

(1) 情報資産

Z 病院の情報資産とは，Z 病院が保有する医療情報を含む全ての情報，並びにそれらの情報の利用，管理，保管などに関わる機器，情報システム，情報システムを構成するプログラム，データ及び記録媒体である。

(2) 組織及び対象者

Z 病院の全ての組織，並びに Z 病院の情報資産に接する常勤，非常勤及び臨時を含む全ての従業者は，本方針を遵守しなければならない。

■情報資産の分類

（省略）

■情報資産へのアクセス制御

情報資産に対するアクセスは，業務上，必要最小限の範囲で許可する。

■情報資産への脅威

情報セキュリティ対策を講じるべき脅威は次のとおりである。

(1) 情報資産の漏えい，盗難，盗聴，改ざん，破壊

(2) 地震，落雷，火災，水害などの災害，情報資産の故障などによるシステム障害

■情報セキュリティ対策

次の対策を講じるものとする。

(1) 物理的セキュリティ対策

（省略）

(2) 人的セキュリティ対策

（省略）

(3) 技術的セキュリティ対策

（省略）

(4) 運用セキュリティ対策

上記 (1)～(3) の対策の実効性を確保するために，情報システムなどの稼働状況の監視や情報セキュリティ基本方針の遵守状況の確認を行うとともに，運用面における必要な対策を講じる。また，非常時に備えた危機管理対策を講じておくとともに，Z 病院以外の医療従業者に医療情報の参照を許可する場合には運用手順による特別な対策を講じる。

（省略）

図 1　Z 病院の情報セキュリティ基本方針

カルテは，取扱いに注意が必要な個人情報を含み，機密性や完全性の確保が必要である上，災害時などの非常時も含め，医療を提供するときには参照が必要なので，可用性の確保も重要である。

Z 病院は個人情報取扱事業者であり，図 2 に示す個人情報保護方針を策定している。

■個人情報の取得について
　患者の個人情報を取得する場合，患者の医療に関わる範囲で行う。
■個人情報の提供について
　患者の個人情報は，次の場合を除き，第三者に提供しない。
(1)　患者の了解を得た場合
(2)　個人を識別又は特定できない状態に加工して利用する場合
(3)　法令などによる場合
(4)　患者の生命，身体又は財産の保護のために必要な場合であって，患者の同意を得ることが困難な場合
■個人情報の適正管理について
　患者の個人情報は，正確かつ最新の状態に保つよう努めるとともに，漏えい，滅失，毀損の防止，その他の安全管理のために必要かつ適切な措置を講じる。
（省略）

図２　Ｚ病院の個人情報保護方針

〔現行のカルテに関する課題〕

Z 病院では，紙のカルテは患者ごと，診療科ごとに作成され，診療科ごとに患者単位でファイリングされている。医師は，診療を担当する患者のカルテだけを参照する。担当する患者が他診療科で診療を受ける場合は，その診療科から要求があれば患者のカルテをその診療科に貸し出すことができる。各診療科において，他診療科へのカルテの貸出しは，各診療科の医療事務員が帳簿に付けて管理している。

しかし，これには，診療上の観点から認識されている問題点が幾つかある。大量にファイリングされているカルテを取り出す際に取り違えて，別のカルテが医師に届くことがある。患者が他診療科も受診している場合には，検査や投薬の重複が発生しないようにその診療科のカルテも参照するが，その診療科のカルテが届くまで，患者を長時間待たせる事態も発生している。また，患者が複数の診療科で受診しているかどうかは，患者本人の申告がないと分からない。さらに，セキュリティの観点から認識されている問題点としては，カルテを物理的に Z 病院内で持ち回るので，紛失や情報漏えいの可能性が挙げられている。

電子カルテを導入することによってこれらの問題点を解決することが，Z チームの大きな目標である。紙のカルテは，電子カルテの導入後，スキャナで画像データ化を進め，医療情報システムで参照できるようにしたいと考えている。

〔電子カルテの保存に関する要件〕

カルテは医師法によって 5 年間の保存が義務付けられている。その電子媒体による保存も，厚生労働省の通知によって認められている。Z チームは，医療情報システムの要件を定義するために，関連する法令や，厚生労働省から公表されている“医療情報システムの安全管理に関するガイドライン”をはじめとする，省庁や業界団体による各種ガイドラインなどを調査した。

厚生労働省の通知では，カルテを電子保存する場合，真正性，見読性，保存性の確保が必要とされている。特に，カルテの真正性とは，正当な者が記録し，確認された情報に関して，記録の責任の所在が明確であり，かつ，故意又は過失による，虚偽入力又は誤入力，書換え，消去及び混同が防止されていることである。

そのため，電子カルテに対する全ての操作の前には，利用者の識別と認証が必要である。

また，電子カルテの入力などには，記録に対する責任の所在を明確にするため，正

当な入力，追記，書換え，消去の後，医師による電子カルテへの記録の“確定”登録という操作が必要である。ただし，研修中の医師である研修医による診療内容の記録は，最終的な確定とせず，“仮”登録として記録する。

紙のカルテの場合は，書き換えられたとしても書換えの痕跡は保存され，発見されやすいが，単純に電子化した場合は，このような特性は失われるので，何らかの対策が必要である。

Z 病院では，初診からの一連のカルテを診療終了後 5 年間保存する運用をしており，電子カルテの保存についても，同じ運用を続けることにした。

Z チームは，電子カルテの保存について，要件の検討を行った。厚生労働省などのガイドラインでは，必須対策と推奨対策が示されている。Z 病院の情報セキュリティ基本方針及び個人情報保護方針に照らし合わせ，M 氏のアドバイスを得ながら，電子カルテ機能の要件を整理し，表 1 にまとめた。

要件を踏まえ，具体的な実現方式の検討を行うとともに，導入するソフトウェアパッケージ（以下，パッケージという）を選定して，電子カルテの保存に関する運用管理規程の策定を行い，医療情報システムを構築することにした。

表１　Ｚチームが作成した電子カルテ機能の要件

要件の分類	要件
利用者の識別及び認証	(A)　電子カルテの利用者に対して，利用者 ID 及びパスワードと，電子証明書を格納した認証機能付きの IC カードを組み合わせた識別及び認証を行うこと。
アクセス制御	(B)　電子カルテに対する全ての操作について，利用者の職種，所属などの区分，又は利用者の権限範囲に基づくアクセス制御を行うこと。 (C)　権限のある利用者以外の者による入力，追記，書換え，消去を防止すること。
記録の確定	(D)　診療内容の記録完了や検査結果などの入力完了を表す“確定”登録を行う仕組みを備えること。 (E)　“確定”登録が行われた記録に対しても，追記，書換え，消去を行った後，再度，“確定”登録が行えること。 (F)　記録を“確定”登録する際には，記録に対する責任者（以下，作成責任者という）の利用者 ID や氏名などの識別情報，及び信頼できる日時が含まれること。 (G)　記録を“確定”登録する際は，国際標準に準拠した保健医療福祉分野向けの PKI（以下，HPKI という）において発行された作成責任者の電子証明書を利用したディジタル署名を付与すること。このディジタル署名には，鍵生成機能と署名機能付きの IC カードを用いること。①ディジタル署名に用いる秘密鍵が，IC カードの外部に読み出されないこと。 (H)　ディジタル署名に対してタイムスタンプを付与し，法定保存期間中，タイムスタンプの有効性が継続されるようにすること。
更新履歴の保存と参照	“確定”登録が行われた記録に対して，追記，書換え，消去を行い，再度，“確定”登録を行う場合には，次の要件を満たすこと。 (I)　過去に“確定”登録が行われた記録が正しく保存されること。 (J)　記録に対する操作の履歴が後から確認でき識別できること。 (K)　記録の内容を容易に確認できること。
確定記録の原状回復	(L)　“確定”登録が行われた記録の改ざんを防止すること。 (M)　改ざんが検知された場合は，バックアップなどを用いて回復できること。
アクセス証跡の保存	(N)　電子カルテに対する全ての操作についてのアクセス証跡を残すこと。 (O)　アクセス証跡には，電子カルテを操作した日時を含むこと。 (P)　アクセス証跡が改ざんされないための対策を講じること。
非常時の電子カルテの参照	(Q)　非常時にも，電子カルテを参照できること。
⋮	⋮

〔医療情報システムのユースケース〕

Z チームは，現行業務を基に医療情報システムのユースケースを検討した。検討結果を表 2 に示す。

表２　医療情報システムのユースケース（抜粋）

アクタ	ユースケース
医師 [1)]	(1)　電子カルテに患者の診療経過を記録する。 (2)　患者の過去の電子カルテを参照する。 (3)　患者への説明などのために，検査記録などの印刷を行う。 (4)　診察結果に基づき，処置の指示を行う。 (5)　診察結果に基づき，院内処方の場合は，処方の指示を行う。院外処方の場合は，処方箋の印刷を行う。 (6)　診療を終えた後に診療内容の記録を確認して，必要に応じて修正し，“確定”登録を行う。 (7)　研修医が診療を終えた後に診療内容の記録を確認して，必要に応じて修正し，“確定”登録を行う。 (8)　患者の診療が終了したことを電子カルテに記録する。 (9)　患者を他医療機関に紹介するために診療情報提供書（以下，紹介状という）を作成する。作成した紹介状は，医師が印刷する場合と，医療事務員に印刷するよう指示する場合がある。 （省略）
⋮	⋮
管理者	(1)　利用者 ID のライフサイクル管理（新規発行，削除，一時停止など）を行う。 (2)　電子カルテのバックアップを行う。 (3)　電子カルテのアクセス証跡のバックアップを行う。 （省略）

注 [1)]　アクタ“医師”は，詳細化すると次の二つのアクタに分類できる。

研修医：研修中の医師。研修医による診療内容の記録は，“確定”登録にならず，“仮”登録になる。

医師（研修医以外）：独立して診療ができる医師。診療内容の記録が完了した場合は“確定”登録を行う。研修医を指導する役割をもった医師は，担当する研修医の診療結果を記録した“仮”登録の内容を確認して，妥当な内容ならば，“確定”登録を行う責任をもつ。

〔医療情報システムで利用する IC カードについての認証方式の検討〕

医療情報システムの利用者認証の方式は，要件に基づいて，パスワード及び IC カードによる 2 要素認証とする。医療情報システムを利用する Z 病院の医療従業者には，利用者認証に用いる IC カードを配布する。配布される IC カードには，個人ごとに HPKI の認証局に登録して発行される電子証明書及び対応する秘密鍵が格納される。医師の電子証明書には，医師資格を保有していることを示す情報が含まれ，医師の IC カードは利用者認証に加え，電子カルテや紹介状へのディジタル署名の付与にも用いることができる。 IC カードは，通常，申請から入手するまで 1 週間ほど掛かる。

Z チームでは，IC カードの携帯を忘れた利用者に一時貸与するためや，破壊・紛失による再発行までの間に一時貸与するための予備 IC カードを常時確保することにした。予備 IC カードは，医療情報システムの利用者設定機能を用いて，臨時利用者属性を付けて一時的な利用者認証に利用することができる。臨時利用者属性のアクセス権限は，一部の機能に利用制限があるが，医療行為には支障を来さないように権限を設定する。予備 IC カードで記録を“確定”登録することはできない。

〔医療情報システムのアクセス制御についての検討〕

紙のカルテは，医療事務員がキャビネットから取り出して，医師に渡している。電子カルテになると，システム設計によっては，担当外の患者の電子カルテの参照及び

職務権限外のアクセスも容易にできるようになるので，アクセス制御の構築とアクセス証跡の保存が重要になる。

Z チームでは，アクセス制御についての検討を進めるために，現行のカルテをモデル化し，電子カルテの概念データモデル案を作成した。電子カルテの概念データモデル案を図 3 に示す。

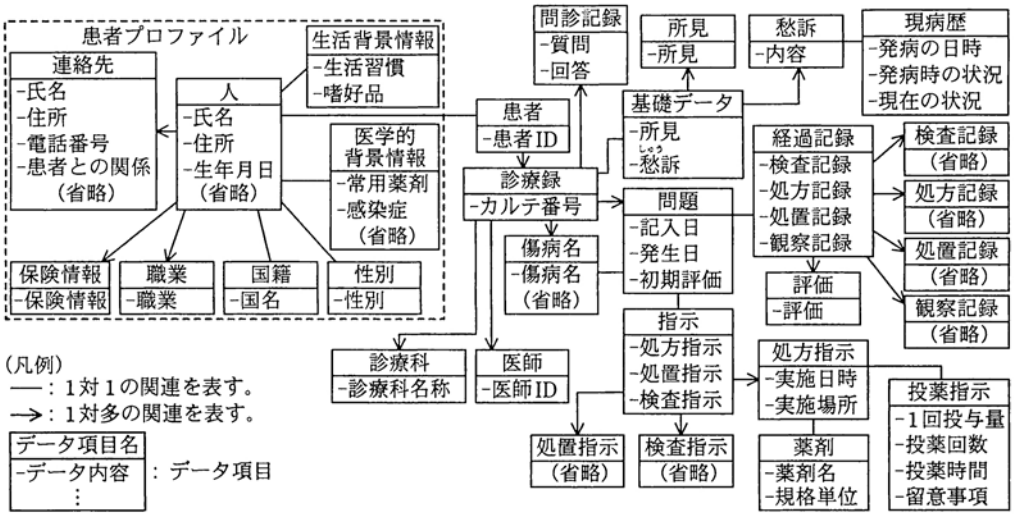

図 3　電子カルテの概念データモデル案（抜粋）

Z チームは，医療情報システムでの電子カルテに対するアクセス制御について，電子カルテの概念データモデル案に基づいて，ユースケースや課題を参照しながら検討を行った。

アクセス権限の設定については，アクセス制御の要件に基づいて，医療情報システムの利用者を職種などの観点で整理したアクタ種別と，電子カルテのデータ項目の組合せで制御する必要があるとの結論に至った。

各アクタ種別では，データ項目の追記（A），データ項目の参照（R），データ項目の書換え（U），データ項目の消去（D），データ項目の“確定”登録（F），電子カルテの印刷（P）のうちのどのアクセス権限が必要かを検討した。再診の外来患者の電子カルテのデータ項目に対する，アクタ種別ごとのアクセス制御案を表 3 に示す。

表 3　再診の外来患者の電子カルテのデータ項目に対する，アクタ種別ごとのアクセス制御案（抜粋）

データ項目 / アクタ種別	医学的背景情報	所見	問題	評価	処方指示
医療事務員	A，R，U，D，F，P	R，P	R，P	R，P	R，P
医師（研修医以外）	A，R，U，D，F，P	（左に同じ）	（左に同じ）	（左に同じ）	（左に同じ）
研修医	a	（左に同じ）	（左に同じ）	（左に同じ）	（左に同じ）
看護師	R，P	R，P	R，P	R，P	R，P
薬剤師	R，P	R，P	R，P	R，P	R，P

表 3 によって，アクタ種別ごとのアクセス制御の整理はできたが，これで十分であ

るか検討したところ，傷病名によっては，患者又は家族などの意向によって，診療記録の記載内容の開示を“特定の診療科の医師に限定する”という要件のあることが判明した。これに対応するためには，②アクタ種別ごとではない別のアクセス制御の併用が必要であると判断した。

次に，アクセス証跡の保存について検討し，表 1 に示された要件を満たす実装方式を具体化した。

〔医療情報システムにおける真正性についての検討〕

Z チームは，電子カルテのデータ項目について，真正性を保証する仕組みとその実現手段に関して，どのような選択肢があるかを調べるために，まず，市場の医療情報システムのパッケージを調査した。

市場のパッケージでは，電子カルテのデータ項目にカーソルを置いた際に，③過去に確定した全ての記録を表示する方式など，様々な方式が採られている。Z チームでは，後のパッケージ選定作業の際に，複数のパッケージの使い勝手を医療従業者の意見を聞きながら評価することにした。

次に，Z チームは，電子カルテの“確定”登録の際に表 1 の HPKI において発行された電子証明書を用いて付与するディジタル署名について検討を行った。その結果，ディジタル署名は，電子カルテのデータ項目ごとに付与することにした。ただし，電子証明書の有効期限は約 2 年となっている。

法令に基づくカルテの保存要件を満たすために，タイムスタンプを付与することが要件になっている。Z チームが検討した医療情報システムのタイムスタンプ付与の仕組みの概要を図 4 に示す。

M 氏は，タイムスタンプのサービスには，有効期限が 10 年など長期のものもあるが，10 年以上継続して受診する患者がいるので，図 4 に示したタイムスタンプ付与の仕組みでは不十分であると指摘し，④このような患者の初診からの電子カル重の真正性を保証するために図 4 の仕組みを改善する案を提案した。

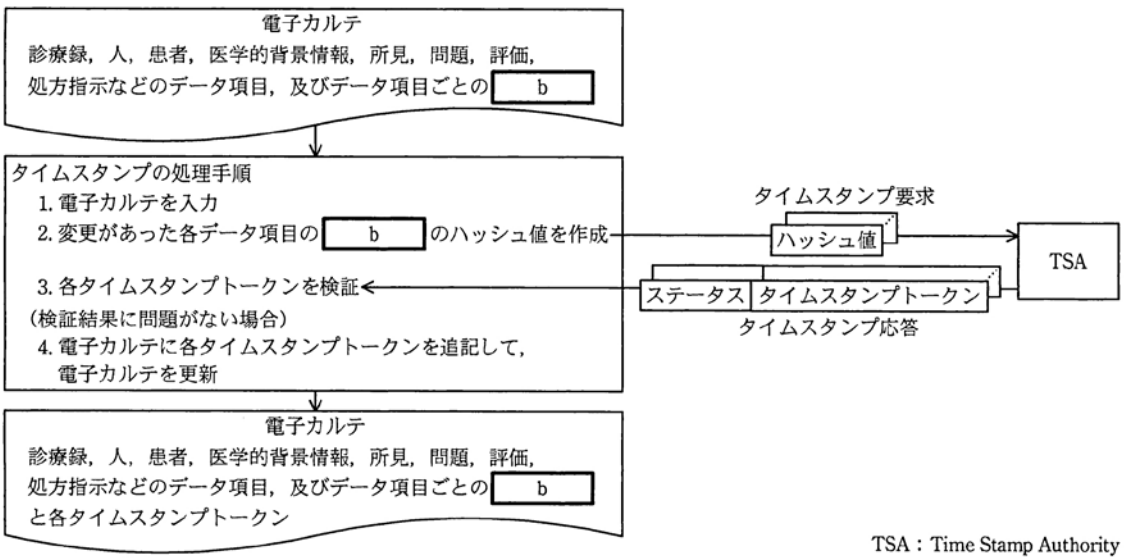

図 4　タイムスタンプ付与の仕組みの概要

F 医師と M 氏は，電子カルテの真正性を保証する仕組みについて漏れがないか検証

作業を行った。次は，その際の会話である。

F 医師：以上で，電子カルテの真正性を保証する仕組みについては，一通りの検討ができましたね。
M 氏　：そうですね。ただ一部未検討の点も残っていると思います。電子カルテの改ざんを検知するための前提となる仕組みについては検討済ですが，実際に検知する仕組みなどについて検討する必要があります。
F 医師：なるほど，改ざんが発生した場合に，実際にそれを検知できないといけないですね。
M 氏　：加えて，“確定”登録が行われた電子カルテが改ざんされた場合に，単に検知するだけではなくて，⑤その後も，正しい電子カルテを用いて医療を提供する必要があります。
F 医師：それでは，その方法を引き続き検討しましょう。

Z チームでは，電子カルテの真正性を保証する仕組みに関する基本設計の検討を済ませ，パッケージ選定を行った。

〔Z 病院の医療情報システムのシステム構成の検討〕
Z チームは，医療情報システムの稼働環境とシステム構成を検討した。医療情報システムのシステム構成の概要を図 5 に示す。

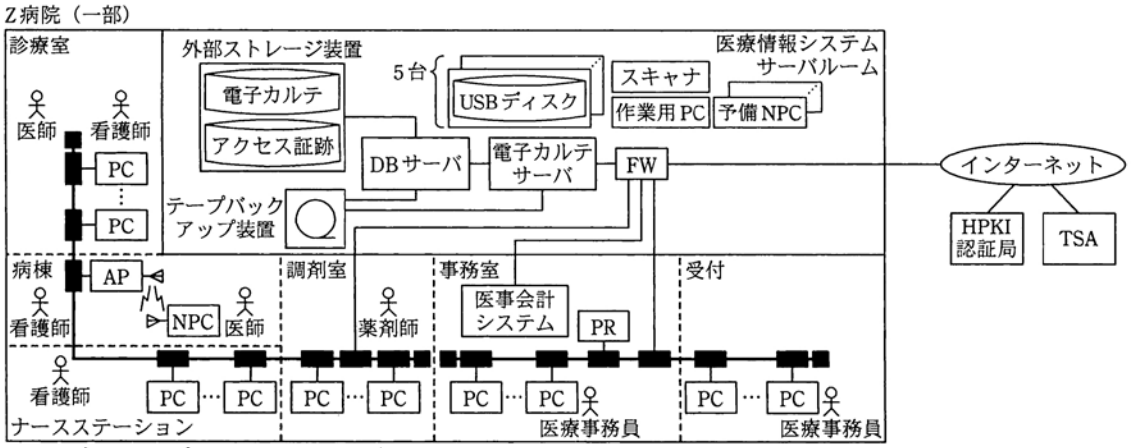

図 5　医療情報システムのシステム構成の概要

Z チームは，医療情報システムのシステム構成の検討と並行して，医療情報システムのネットワークセキュリティについても検討を行った。
診療室，ナースステーション，調剤室，事務室，受付で利用する端末には，PC を採用する。また，病棟で使用する端末は，長時間のバッテリ駆動が可能な NPC を採用する。NPC は，入院患者の診療などに用いるために，医師，看護師などが，病棟内で移動しながら使用する。いずれの端末も，IC カード読取装置，光ディスクドライブ，USB インタフェースを備えた仕様とするとともに，故障時などを想定し，予備 NPC を用意する。医療従業者への IC カードの発行や利用者 ID の付与は管理者が事務室の

PC で行う。また，紙のカルテの画像データ化作業用に作業用 PC を 1 台，スキャナ及び 5 台の USB ディスクを用意する。

医療情報システムのために，PC 用にイーサネット LAN を，病棟を移動しながら利用する NPC 用に無線 LAN をそれぞれ新たに構築する。

医療情報システムは，電子カルテサーバ，DB サーバ，外部ストレージ装置，テープバックアップ装置及び FW から構成される。DB サーバの外部ストレージ装置には，電子カルテ及びアクセス証跡を保存する。選定したパッケージでは，パッケージの機能によって，電子カルテ機能の各操作が可能であり，電子カルテのデータは，複数の表から構成される関係データベースに格納される。

ウイルス対策，不正侵入防御機能も必要であり，FW には，これらの機能を兼ね備えた製品を導入する。

〔非常時運用についての検討〕

医療情報システムに障害が発生すると，患者の電子カルテを参照できなくなるので，医療への影響が非常に大きい。災害時などの非常時に障害が発生すると，電子カルテを参照できないことに加えて，外来患者が増加することが考えられるので，更に影響は大きいと言える。Z チームは，非常時の対応を考慮した医療情報システムの機能，構成及び運用について検討した。次は，非常時運用についての議論の一部である。

F 医師：医療情報システムの非常時運用を検討する前提として，非常時には，どのような事態があり得るのか，確認しておく必要があると思います。

M 氏　：主に二つの事態があり得ます。一つはサービスの停止です。その原因には。災害時の停電やサーバやネットワークの損壊，サイバー攻撃，システム障害などが考えられます。停電対策としては，Z 病院は医療機関として非常用電源設備をもっているので，停電時でも，電子カルテの参照だけはできるよう，医療情報システムに電力が供給されるようにするという対策が考えられます。

F 医師：なるほど，医療情報システムが非常用電源を利用することで，医療機器に対する電力供給可能時間に影響がないかを確認する必要がありますね。次に，サービス停止の事態に際してのデータ保全に関しては，日次に電子カルテのデータベースのバックアップを取ることで，復旧に備えることができると思います。

M 氏　：なるほど，そうですね。それだけではなく，システム障害の対策としては，電子カルテサーバの冗長化構成が考えられます。通常は，ここまででも十分なレベルの対策だと思います。ただし，冗長化構成を採ったとしても，電子カルテサーバ全てで同時に障害が発生する場合も考えられます。

F 医師：なるほど，確かにあり得ますね。

M 氏　：今回はそういった，非常時に医療情報システムのサーバ類が全て稼働しない事態においても，⑥最低限，NPC で USB ディスクを活用して電子カルテを参照できるレベルの対策を講じる方がよいと思います。

F 医師：そうですね。具体的にどのように対応するのかを詳細に検討し，事業継続計画（BCP）に盛り込みたいと思います。

M 氏　：もう一つの事態は，災害時などに，医療情報システムが稼働できたとしても医療情報システムのアクセス権限をもった医療従業者が不在又は対応できない事態です。

F 医師：⑦非常時には，外部から医療従業者が応援に駆け付けてくることがあります。

この場合でも，医療情報システムさえ稼働していて，管理者がいれば，何とか運用できますよね。

M 氏　：そうですね。ただし，医療情報システムは稼働していて，IC カードや利用者 ID を付与する管理者もいるが，医師が応援者だけとなってしまった場合の対応が必要です。

F 医師：では，それを検討して BCP に盛り込んでおきましょう。

Z チームは，以上の検討に基づき，運用管理規程と BCP の策定を行い，医療情報システムを構築し，予定どおりにサービスインの日を迎えた。

設問 1　電子カルテの保存について，(1)，(2)に答えよ。

(1)表 1 中の下線①について，秘密鍵が lC カードの外部に読み出された場合に起こり得る，医療情報システムの安全管理に対する侵害行為は何か。25 字以内で具体的に述べよ。

(2)表 1 中の下線①を実現するために，lC カードが備えるべき性質は何か。8 字以内で述べよ。

設問 2　医療情報システムのアクセス制御について，(1)～(3)に答えよ。

(1)医療情報システムにおいて，電子カルテのディジタル署名を付与する仕組みの他に，医療従業者のアクセス証跡を保存する仕組みを整えるのは，どのような抑止効果を期待してのものか。 45 字以内で述べよ。

(2)表 3 中の [a] に入れる適切なアクセス制御案を，表 3 中のアクセス制御の記号に倣って答えよ。

(3)本文中の下線②にある，別のアクセス制御とはどのようなものか。アクセス制御のアクセス主体とアクセス対象の関係を示しながら，40 字以内で述べよ。

設問 3　医療情報システムにおける真正性について，(1)～(4)に答えよ。

(1)本文中の下線③が示す実装方式は，表 1 中のどの要件を満たしていると考えられるか。表 1 中から該当する要件を二つ挙げ，(A)～(Q)の記号で答えよ。

(2)本文中の下線④について，改善案を 65 字以内で述べよ。

(3)図 4 中の [b] に入れる適切な字句を，10 字以内で答えよ。

(4)本文中の下線⑤について，医療の提供を継続するために医療情報システムが備えるべき機能を 30 字以内で述べよ。

設問 4　Z 病院の医療情報システムの非常時運用について，(1)，(2)に答えよ。

(1)本文中の下線⑥について，対策を講じる上で，日々行うべき業務及び災害時に行うべき業務を，それぞれ 60 字以内で具体的に述べよ。

(2)本文中の下線⑦について，非常時に外部から応援に駆け付けてくる医師に，医療情報システムへのアクセスを許可する場合，BCP に盛り込むべき事項をセキュリティの観点から二つ挙げ，それぞれ 40 字以内で具体的に述べよ。

問 2　ログ管理システムの設計に関する次の記述を読んで，設問 1～4 に答えよ。

A 社は，従業員数 20,000 名の製造会社であり，東日本と西日本にそれぞれ 10 の支社をもっている。A 社は，内部統制強化の一環として，システムの運用に関わる内部統制について外部監査人による監査を受けた。監査の結果，システムの特権を与えら

れた管理者やオペレータなど（以下，特権 ID 利用者という）の操作（以下，特権操作という）に対する監視について，次の 2 点が指摘された。
・特権操作のログを取得していないシステムがある。
・どのシステムにおいても特権操作のログに対する分析が行われていない。

これまで，A 社情報システム部では，特権操作に対する監視方法をシステムごとに個別に検討，実装してきたことから，特権操作のログを取得，収集保存及び分析（以下，合わせてログ管理という）する方法がシステムごとに異なっていた。情報システム部は，監査における指摘を踏まえ，特権操作に対して全システム共通のログ管理方法を定め，共通のログ管理システムを構築することとし，システムのログ管理について，次のとおり計画した。
・大量の個人情報又は財務データを処理している，本社営業管理システム，会計管理システム，経理システム及び支社営業管理システム（以下，主要 4 システムという）のログ管理のため，本年度中に，ログ管理システムを稼働させる。
・主要 4 システムへの適用後の評価に従って，ログ管理システムの設計及び運用の見直しを行い，ログ管理システムを利用してログ管理を行うシステムを順次増やす。

〔A 社のシステム環境〕
A 社は，東京と大阪に自社のデータセンタ（以下，DC という）を構えており，東京 DC では本社及び東日本の支社における業務処理を，大阪 DC では西日本の支社における業務処理を行っている。両 DC 間は広域イーサネットで接続されており，本社及び各支社からは広域イーサネットを介して両 DC のシステムを利用できる。
各 DC 内のマシン室には，汎用機が 2 台ずつ，UNIX サーバが 150 台ずつ，PC サーバが 150 台ずつ配置されている（以下，汎用機，UNIX サーバ及び PC サーバを合わせてサーバという）。両 DC には，マシン室に隣接してオペレータ室があり，マシン室とオペレータ室は LAN で接続されている。
各 DC では電源設備の定期保守作業のために，半年に 1 回，4 時間程度，DC 内の全サーバを停止する。電源設備の保守作業は，東京 DC と大阪 DC では異なる日に行われるように調整されている。

〔特権 ID の利用〕
特権 ID 利用者は，各個人に 1 台ずつ割り当てられた管理端末からネットワークを介して各サーバにアクセスしてシステム管理又は運用の作業を行っている。管理端末は，本社に 200 台，東京 DC と大阪 DC のオペレータ室にそれぞれ 10 台ずつ配置されており，利用者 ID とパスワードによる認証機能によって，本人でなければ操作できない仕組みになっている。管理端末の IP アドレスは，東京 DC 及び大阪 DC それぞれにある［ a ］サーバによって動的に割り当てられる仕組みになっており，同じ管理端末でも割り当てられる IP アドレスが異なることがある。
主要 4 システムにおいては，A 社の情報セキュリティポリシに従い，マシン室の内部・外部間で個人情報又は財務データを通信する場合の暗号化，並びに個人情報又は財務データを外部記憶媒体に保管する場合の暗号化を行っている。特権 ID 利用者が管理端末から各サーバにアクセスする際の通信においても，暗号化を行っている。
サーバと管理端末の配置場所，時刻設定の方法及び特権 ID 利用者の利用者 ID の割当て方法を表 1 に，特権 ID 利用者の役割名称，担当者，作業場所及び作業内容を表 2 に，それぞれ示す。

表１　サーバと管理端末の配置場所，時刻設定の方法及び特権 ID 利用者の利用者 ID の割当て方法

	配置場所	時刻設定の方法	利用者 ID の割当て方法
汎用機	東京 DC 内のマシン室及び大阪 DC 内のマシン室	オペレータが，起動時に，電話の時報サービスで提供されている時刻を設定する。	OS，DBMS を含むミドルウェア（以下，DBMS を含めてミドルウェアという）及び業務アプリケーションにおいて，統一された ID 体系が定義されており，情報システム部が各特権 ID 利用者個人に各サーバの利用者 ID を割り当てている。
UNIX サーバ及び PC サーバ		社内の［ b ］サーバがインターネットの［ b ］サーバと時刻同期を行い，社内のサーバは社内の［ b ］サーバと時刻同期を行う。	
管理端末	本社，東京 DC 内のオペレータ室及び大阪 DC 内のオペレータ室	各管理端末は，管理端末を管理するドメイン管理サーバと時刻同期されている。ドメイン管理サーバの時刻は，オペレータが，毎週月曜日の朝に，自分の腕時計を基に設定するが，時刻の正確さは重視されていない。	管理端末の利用者 ID 8 桁のうち，上 2 桁が A 社及び役割ごとの委託先各社に割り当てられており，各社の管理責任者が特権 ID 利用者個人に下 6 桁を割り当てている。

表２　特権 ID 利用者の役割名称，担当者，作業場所及び作業内容

役割名称	担当者	作業場所	作業内容
アプリケーション管理者	A 社情報システム部の従業員及び業務アプリケーション保守の委託先である B 社の従業員（担当する業務アプリケーションごとに A 社情報システム部の従業員 2 名以上を含むグループに分かれている。）	本社	業務アプリケーション及び業務データの管理を行う。
インフラ管理者	A 社情報システム部の従業員及びインフラ管理の委託先である C 社の従業員（担当範囲ごとに A 社情報システム部の従業員 2 名以上を含むグループに分かれている。）		ネットワーク機器を含むハードウェア並びに OS 及びミドルウェアの管理（一部，パッチ適用などの定型のシステム運用を含む）を行う。
オペレータ	運用委託先 D 社の従業員	東京 DC 内のオペレータ室及び大阪 DC 内のオペレータ室	定型のシステム運用を行う。

特権 ID 利用者は合計 220 名である。特権 ID 利用者は，定型のシステム運用以外に特権操作を含む作業を行う場合，事前に自分の氏名と所属，作業で使用する利用者 ID，作業開始日時，作業時間，作業目的及び作業の概要を記載した作業申請書を自社の管理責任者に提出する。各社の管理責任者は，作業内容が業務上必要なものであることを確認し，承認印を押印する。通常時，各社の管理責任者は，担当者に対する作業指示や作業の管理を行っている。何かの事情で担当者の手が足りなくなった場合，各社の管理責任者が特権操作を行うことがあるので，各社の管理責任者は特権 ID 利用者を兼務しており，利用者 ID が割り当てられている。

特権 ID 利用者のうち情報システム部の従業員は，アプリケーション管理者又はイ

ンフラ管理者のどちらか一方を担当しており，自分が所属するグループの作業内容を詳しく理解している。各システムの構築はSIベンダに委託している。各システムのオペレータが行う運用手順は，手順の概要を記した引継ぎ資料と口頭説明によって委託先のSIベンダからオペレータに直接引き継がれてきた。さらに，情報システム部の従業員の中にオペレータの役割をもつ者がいないこともあり，オペレータが行うシステム運用の詳細を知っている者はいない。

〔設計の前提条件〕

情報システム部のX部長は，ログ管理システムの基本設計をY主任に指示した。Y主任がログ管理に関する十分な経験と知識をもっていなかったことから，X部長は，専門家の参加が必要と判断し，SIベンダのE社にログ管理システムの基本設計への参加を依頼した。E社の情報セキュリティスペシャリストのT氏は，最初にY主任から，ログ管理システムを開発することになった経緯やA社のシステム環境についての説明を受けた。後日，Y主任は，T氏の助言を受けながら，設計の前提条件を次のように整理し，X部長の承認を得た。

(1)ログ管理システムを次の三つの機能からなるシステムとする。

ログ取得機能：監視の対象とする特権操作について，記録すべきデータをログファイルとして出力する機能

ログ収集保存機能：複数のログファイルを収集し，フォーマットの変更を行って。一つのログデータベースに統合し，ログファイルと併せて保存する機能

ログ分析機能：与えられた条件に従い，ログデータペースから疑わしい特権操作のログを抽出する機能

(2) 監視の対象とする特権操作を，次の3種類とする。

特権操作1：特権ID利用者による各サーバへのログオン及びログオフ

特権操作2：各システムのデータベース（DB）に保管された個人情報及び財務データに対する参照及び更新

特権操作3：各サーバのOS及びミドルウェアのコマンド，スクリプト及びプログラムの実行，並びに設定情報の参照及び更新

主要4システムにおいて監視の対象とする特権操作を表3に示す。

表３　主要４システムにおいて監視の対象とする特権操作

項番	システム名	サーバ種別	特権操作の分類	特権操作の内容	操作インタフェース
1	本社営業管理システム	汎用機	特権操作１	・特権 ID 利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作２	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DB で SQL 文として処理される。）	テキストインタフェース
			特権操作３	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
2	会計管理システム	UNIX サーバ	特権操作１	・特権 ID 利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作２	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DB で SQL 文として処理される。）	表形式の GUI
			特権操作３	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
				・バッチ処理のスケジュールの参照及び更新	GUI
3	経理システム	UNIX サーバ	特権操作１	・特権 ID 利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作２	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DB で SQL 文として処理される。）	表形式の GUI
			特権操作３	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
				・ERP 業務パッケージにおける利用者権限の設定情報の参照及び更新	GUI
				・バッチ処理のスケジュールの参照及び更新	GUI
4	支社営業管理システム	PC サーバ	特権操作１	・特権 ID 利用者による各サーバへのログオン及びログオフ	GUI
			特権操作２	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DB で SQL 文として処理される。）	表形式の GUI
			特権操作３	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ

(3) 各特権操作に対して記録すべきデータ項目は，次の五つとする。

① 特権操作が行われた日時
② 特権操作に利用された利用者 ID
③ 特権操作が行われたサーバのホスト名又はサーバの IP アドレス
④ 特権操作の内容
⑤ 特権操作の結果（成功又は失敗。エラーメッセージなどの補助的情報で成功と失敗が判別できる場合は，結果が記録されなくてもよい。）

主要 4 システムの各特権操作に対して記録すべき特権操作の内容を表 4 に示す。

表４　主要４システムの各特権操作に対して記録すべき特権操作の内容

特権操作の分類	記録すべき特権操作の内容
特権操作１	(A)　ログオン (B)　ログオフ
特権操作２	(C)　参照要求（又は SQL 文）及び参照されたデータの内容 (D)　更新要求（又は SQL 文）及び更新されたデータの内容
特権操作３	(E)　コマンド，スクリプト又はプログラムの実行文 (F)　参照された設定ファイルの内容又は更新された設定ファイルの内容 (G)　参照された ERP 業務パッケージにおける利用者権限の内容又は更新された ERP 業務パッケージにおける利用者権限の内容 (H)　参照されたバッチ処理のスケジュール又は更新されたバッチ処理のスケジュール

(4)構築費用を抑えるため，製品の標準機能を最大限に活用する。

〔利用する製品の仕様〕

T 氏は，ログ管理システムに利用できる製品として，次の二つの製品を選んだ。

製品 R：管理端末でログを取得し，収集保存及び分析を PC サーバで行う製品

製品 S：各サーバの OS 及びミドルウェアが取得したログを UNIX サーバで収集保存及び分析する製品

T 氏は，0S 及びミドルウェアの標準機能，製品 R の機能並びに製品 S の機能に関する調査を行った。主要 4 システムの OS 及びミドルウェアの標準機能で共通に取得できるログのデータ項目を図 1 に，主要 4 システムの DBMS における DB アクセスに関するログ取得機能を表 5 に，製品 R の仕様を図 2 に，製品 S の仕様を図 3 に，それぞれ示す。

・操作が行われた日時
・操作に利用された利用者 ID
・操作が行われたサーバのホスト名
・次の操作内容
  - サーバに関するログオン及びログオフ
  - ファイルアクセスの内容（ファイル名，並びに作成，参照，更新及び削除の操作種別）
  - コマンド，スクリプト及びプログラムの実行文
・操作の結果（成功又は失敗）

図１　主要４システムの OS 及びミドルウェアの標準機能で共通に取得できるログのデータ項目

表５　主要４システムの DBMS における DB アクセスに関するログ取得機能

システム名	本社営業管理システム	会計管理システム	経理システム	支社営業管理システム
システムが使用している DBMS の製品名	G 社製品 H（汎用機版）	G 社製品 H（UNIX 版）	K 社製品 L（UNIX 版）	K 社製品 L（PC 版）
取得できるログのデータ項目	各 DB アクセスに対して，日時，利用者 ID，実行した SQL 文，SQL 文の実行結果がログファイルに出力される。			
ログ取得機能の設定方法	ログ取得を行うか否かを表ごとに設定する。		各利用者 ID が所属するユーザグループを定義し，ログ取得を行うか否かをユーザグループごとに設定する。	

・管理端末に導入するエージェントプログラム（以下，R エージェントという）と，ログ収集保存及び分析用の PC サーバに導入するサーバプログラム（以下，R サーバという）からなる。
・R エージェントは，キーボード，マウス及びディスプレイのデバイスドライバの動作を監視する。R エージェントは，R サーバ側で設定された，ログ取得開始の事象（管理端末での操作）を検知すると，取得するデータ項目及び取得時間の定義に従い，定期的に画面の画像データ並びにキーボード入力及び画面出力のテキストデータを取得する。複数ウィンドウを使って操作する場合は，取得したキーボード入力及び画面出力のテキストデータがどのウィンドウで入出力されたものか判別できない。
・取得したデータには，管理端末の認証機能で使われる利用者 ID と日時が付加される。
・R エージェントは，取得したログを，リアルタイム又はバッチ処理で R サーバに転送する。ネットワーク障害などで転送が失敗した場合，R エージェントは，ログを管理端末のハードディスクにファイルとして蓄積しておき，転送が可能になった時点で R サーバに転送する。
・R サーバに転送されたログは，毎日，画像データとテキストデータのそれぞれについて，一つずつのファイルとして保存される。ファイル名には日付を含む名前が付けられる。
・R サーバは，利用者 ID，日時及び取得したテキストデータに対する検索画面をもち，検索結果の利用者 ID，日時又はテキストデータをクリックすると対応する画像データが表示される。
・R サーバが提供するコマンドを利用して，利用者 ID，日時及びテキストデータに対する検索条件を指定して，画像データとテキストデータをファイルとして抽出することができる。

図２　製品 R の仕様

・各サーバに導入するエージェントプログラム（以下，S エージェントという）と，ログ収集保存及び分析用の UNIX サーバに導入するサーバプログラム（以下，S サーバという）からなる。
・S エージェントは，各サーバのログファイルにログデータが 1 レコード書き込まれるごとにそのレコードを S サーバに転送することでログの収集を行う。ネットワーク障害などでログデータの転送が失敗した場合，最大 1 時間再送を試行し，再送が成功しない場合は再送エラーとする。
・S サーバに収集されたログデータは，事前定義された変換ロジックに従い，標準のログフォーマットに変換され，ログデータベースに保存される。
・ログデータベースの内容は表形式で表示され，各データ項目に対する整列処理，検索処理を GUI から定義することで分析ロジックを組み立てることができる。
・分析結果のデータをグラフ化して表示したり，ファイルとして保存したりすることができる。

図３　製品 S の仕様

〔ログ取得機能の設計〕

以上の検討結果に基づき，T 氏は，ログ取得機能の実装方法として，次の二つの案を Y 主任に説明した。

・各サーバの OS 及びミドルウェアの標準機能を利用する。
・製品 R を利用する。

なお，製品 S はログ取得機能をもたないので，ログ取得機能には利用できない。

Y 主任は，T 氏の案以外にも，通信経路でログを取得する，ネットワークフォレンジックと呼ばれている案もあるのではないかと質問した。T 氏は，通信経路でログを取得する案は採用できないことを説明した。

T 氏は，図 1 を基に，主要 4 システムにおける特権操作 1 については，OS 及びミドルウェアの標準機能で必要なログのデータ項目を取得できると判断した。一方，ログオフの操作に，パラメタなしの“exit”，“logoff”，“logout”といったコマンドが使われることから，製品 R では必要なデータ項目が取得できず，分析の際にもそのデータ項目の値を判別できない場合があると判断した。

T 氏は，これらの検討結果から，特権操作 1 について設計の前提条件を満たすためには，製品 R でなく，OS 及びミドルウェアの標準機能を使うべきだと判断した。

次に T 氏は，特権操作 2 に関するログ取得機能の実装方法を検討するために，主要 4 システムの DBMS が稼働している各サーバについて，サーバ資源の利用状況及び DB アクセス数全体に占める特権操作 2 の割合を調査した。T 氏は，サーバ資源の利用状況から，DBMS の標準機能によってログを取得すると，各システムの業務処理への影響が大きいと考えた。また，T 氏は，各システムの DB アクセス数は同程度で，その中での特権操作の割合が 5%だったことから，システムによってはログの保存及び分析のために大量のディスク資源を追加する必要があると考えた。T 氏は，これらの検討結果から，特権操作 2 に対しては，DBMS の標準機能よりも製品 R を使う方が適切と判断した。

さらに，T 氏は，図 1 及び図 2 を基に，特権操作 3 に対しては，OS 及びミドルウェアの標準機能よりも製品 R を使う方が適切と判断した。

Y 主任は，T 氏の案をまとめ，X 部長の承認を得た。

〔ログ収集保存機能の設計〕

次に，Y 主任と T 氏は，特権操作 1 のログに対する収集保存機能の設計を行った。製品 R の収集保存機能は，製品 R で取得したログを対象とした機能である一方，製品 S の収集保存機能は，主要 4 システムの管理及び運用に使われている OS 及びミドルウェアのログ全てに適用できることから，T 氏は，製品 S を採用することを提案した。

そこで，Y 主任は，東京 DC に S サーバを配置し，両 DC のログデータを一括して収集する方法（以下，案 1 という）を考えた。案 1 の構成を図 4 に示す。

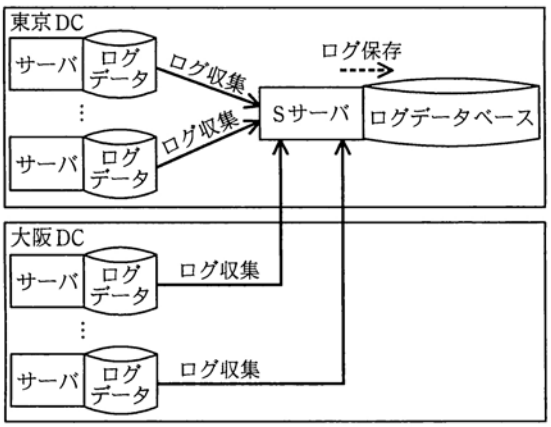

図 4　案 1 の構成

サーバの中には，ログデータに割り当てられたディスク領域が一杯になると，新しいログデータで古いログデータを先頭から上書きするものがある。このことから，T 氏は，ログが収集できない時間帯が発生する案 1 では，特別な運用対策が必要となることを指摘し，そうした対策の必要がないように，DC ごとに S サーバを配置してログデータを収集する方法（以下，案 2 という）を提案した。案 2 の構成を図 5 に示す。

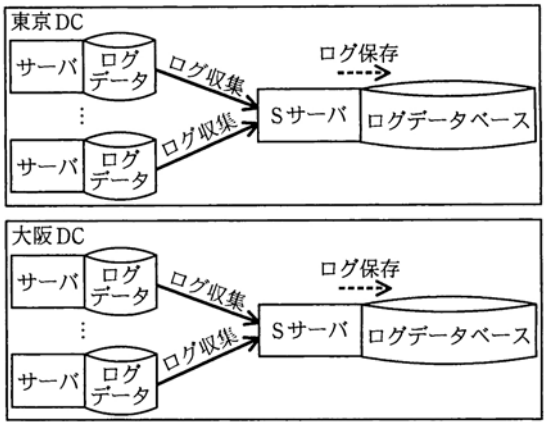

図５　案２の構成

Y 主任は T 氏の指摘を認め，X 部長も案 2 の構成とすることを承認した。

次に，Y 主任と T 氏は，特権操作 2 及び特権操作 3 のログに対する収集保存の方法を検討した。Y 主任は，東京 DC に R サーバを配置してログを収集保存する方法を考えた。図 6 に特権操作 2 及び特権操作 3 のログに対する収集保存の方法案を示す。

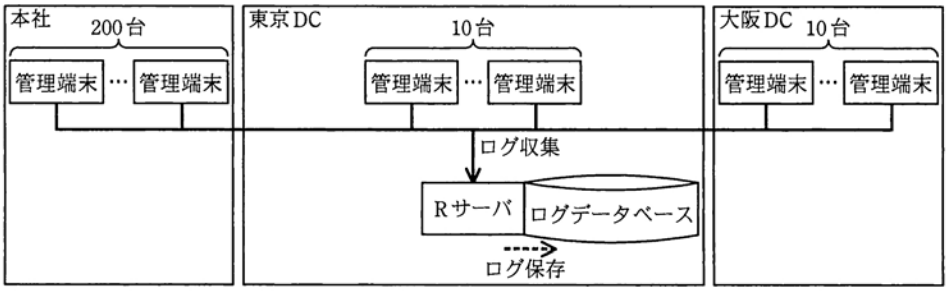

図６　特権操作２及び特権操作３のログに対する収集保存の方法案

T 氏は，収集保存の対象となる特権操作 2 及び特権操作 3 のログが大量になることから，ログの最大データ量とログ収集に必要なネットワークの伝送速度を見積もり，現在のシステム環境への影響を評価することを Y 主任に提案した。Y 主任は，見積りに関する基礎数値を設定し，①A 社全体で発生する特権操作 2 及び特権操作 3 に対する 30 日分のログの最大データ量と②製品 R を使って本社の管理端末 200 台から東京 DC にログを収集するために必要なネットワークの伝送速度を見積もった。見積りに関する基礎数値を図 7 に示す。

・１台の管理端末を８時間使用した場合，その間のログの最大データ量は，画像データとテキストデータを合わせて 70M バイトである。
・各管理端末は，年間を通じて１日平均８時間利用されている。
・製品 R を使って管理端末のログを R サーバに収集した場合，管理端末 1 台当たりに必要なネットワーク伝送速度は 30k ビット／秒である。

図７　見積りに関する基礎数値

Y 主任と T 氏は，見積結果から，現在のシステム環境への影響はないと判断し，東

京 DC に R サーバを配置してログを収集保存する方法について，X 部長の承認を得た。

次に，Y 主任は，ログファイル及びログデータベースのバックアップに関する運用規程を定める必要があると考え，現在のシステム運用を考慮して，その案を作成した。図 8 にログファイル及びログデータベースのバックアップに関する運用規程案を示す。

1. ログを保存する際は，一度データを書き込むと再書込みが不可能な磁気テープ媒体（以下，WORM（Write Once Read Many）テープという）を用い，正副の二つの媒体に保存する。
2. ログの保存期間は 1 年間とし，保存期間満了後は 1 週間以内に媒体を物理的に破壊し，廃棄する。
3. WORM テープには通番を付与し，台帳管理を行った上で，正の媒体はオペレータ室内の保管庫で，副の媒体は遠隔地で，それぞれ保管する。
   なお，副の媒体を遠隔地に運搬する際は安全な運搬手段を利用する。

図 8　ログファイル及びログデータベースのバックアップに関する運用規程案

T 氏は，特権操作 2 に関するログのデータ項目の内容を考慮し，運用規程案に追加すべき点を指摘した。③Y 主任は運用規程案に項目を追加し，これまでの検討結果をまとめ，X 部長の承認を得た。

〔ログ分析機能の設計〕

次に Y 主任と T 氏は，ログ分析機能の設計を行った。Y 主任は，他社で発生している情報漏えい事件の内容から，業務時間（月曜日から金曜日の 9:00 から 17:00）外に行われた特権操作を優先的に監視する必要があると考えた。Y 主任は，毎月第 2 金曜日に行われる運用報告会議において，前月のログに対する確認作業の結果を，各社の管理責任者が X 部長に報告することを考えた。Y 主任が考えたログ分析機能及び確認作業の内容は次のとおりである。

ログ分析機能：特権操作 1 に関するログから，業務時間外に行われた特権操作 1 のログを抽出する。

確認作業：抽出された特権操作 1 のログについて，関連する作業申請書と特権操作 2 及び特権操作 3 に関するログを基に，操作内容の必要性を確認し，確認者の氏名と確認結果を記録する。

Y 主任は，情報システム部の従業員では一部の特権 ID 利用者について個々の操作内容の必要性を十分に確認できないことから，各社の管理責任者が確認作業を行う案に修正した。しかし，T 氏は，その修正案には，特権操作の確認として不十分な点が別にあることを指摘し，改善案を提案した。Y 主任は改善案に従って手順を修正し，これまでの検討結果をまとめ，X 部長の承認を得た。

Y 主任と T 氏は引き続きログ分析機能の設計を行い，無事にログ管理システムの基本設計を完了した。

設問 1　本文中の［ a ］及び表 1 中の［ b ］に入れるプロトコル名を，それぞれ英字 4 字以内で答えよ。

設問 2　〔ログ取得機能の設計〕について，(1)～(5)に答えよ。

(1)T 氏が，通信経路でログを取得する案を採用しなかった理由を，30 字以内で述べよ。

(2)ログオフの操作について記録すべきデータ項目のうち，製品 R では取得できないデータ項目は何か。 25 字以内で述べよ。その場合でも，ある条件の下では

分析の際にそのデータ項目の値を判別できるが，それはどのような場合か。30字以内で述べよ。その際，判別の根拠となる情報は何か。 45字以内で述べよ。

(3)DBMSの標準機能によるログ取得を行った場合，各システムの業務処理への影響が大きいとT氏が考えたのはなぜか。サーバ資源という用語を用いて30字以内で述べよ。

(4)DBMSの標準機能によるログ取得を行った場合，ログの保存及び分析に大量のディスク資源が必要になるシステムを，表3中の項番で二つ答えよ。また，その理由を30字以内で述べよ。

(5) 記録すべき特権操作の内容のうち，特権操作3に対して，主要4システムのOS及びミドルウェアの標準機能では取得できないものは何か。表4中から該当するものを全て挙げ，(A) ～ (H) の記号で答えよ。

設問3 〔ログ収集保存機能の設計〕について，(1) ～ (5) に答えよ。

なお，1Gバイト＝1,000Mバイト，1Mビット／秒＝1,000kビット／秒とする。

(1) 案1において，システムの障害発生時以外でログが収集できないのはどのようなときか。20字以内で答えよ。

(2) 本文中の下線①について，見積もった最大データ量（Gバイト）を求めよ。

(3) 本文中の下線②について，見積もった伝送速度（Mビット／秒）を求めよ。

(4) ログの保存にWORMテープを用いる目的を，15字以内で答えよ。

(5) 本文中の下線③について，Y主任が，運用規程案に追加した項目の内容を，20字以内で述べよ。

設問4 〔ログ分析機能の設計〕について，(1) ～ (3) に答えよ。

(1) 抽出した特権操作1のログに関連する，特権操作2及び特権操作3のログを，自動的に抽出できるようにログ分析機能を強化するためには，〔特権IDの利用〕における，サーバと管理端末の運用や利用の方法に関して変更又は追加が必要である。その内容を二つ挙げ，それぞれ25字以内で述べよ。

(2) 情報システム部の従業員では，どの特権ID利用者についての操作内容の確認が不十分となるか。表2中の役割名称で答えよ。また，その理由を，40字以内で述べよ。

(3) 各社の管理責任者が確認作業を行った場合，どのような特権操作に対する確認が不十分となるか。その操作を20字以内で述べよ。また，T氏が提案した改善案の内容を25字以内で述べよ。

解答例

問1

出題趣旨

社会インフラを担う情報システムでは，非常時にも業務を継続することが求められる。BCP策定においては，情報システムに関する技術的な知識だけでなく，業務そのものに対する理解も必要となる。セキュリティ技術者には，こうした業務の観点からの取組みも求められるため，常日頃より幅広い視点でスキルの研さんと経験の積み重ねが要求される。

本問では，医療情報システムを題材にして，業務要件に応じたアクセス制御や，長期に渡るデータの真正性確保に関する技術についての知識と応用力を問うとともに，情報システムの可用性に加え，業務の非常時への対応についての経験と対応力を問う。

設問 1（1）作成責任者以外の者による電子カルテへの署名
（2）耐タンパ性
設問 2（1）医療行為に必要な範囲を超えて患者の医療情報にアクセスすることを抑止する効果
（2）a　A，R，U，D，P
（3）個別の利用者ごとに，電子カルテのデータ項目ごとに行うアクセス制御
設問 3（1）①（J）
②（K）
（2）電子カルテのディジタル署名の有効期限が切れる前に，署名検証に必要な情報を含むアーカイブタイムスタンプを付与する。
（3）b　ディジタル署名
（4）バックアップから改ざん前の電子カルテを復旧する機能
設問 4（1）　**日々行うべき業務**　患者ごとに，見読可能な画像データを電子カルテから生成し，USB ディスクに書き出しておく。
災害時に行うべき業務　電子カルテの画像データを保管した USB ディスクを端末に接続して，患者の電子カルテの画像データを医師に配布する。
（2）①・本人確認の方法と，認証に用いる IC カードの貸与及び利用者 ID の付与②　の方法
・応援者の資格の確認方法と，応援者に付与するアクセス権限の内容と付与方法

問 2
出題趣旨
ログ管理システムの設計においては，セキュリティ技術だけでなく，既存システムの環境や運用全体を見渡す広い視野が必要になる。近年，実務を担当するセキュリティ技術者には，セキュリティに関する専門知識だけでなく，システムに求められる要件及び制約の一つとしてセキュリティをとらえ，多岐にわたる前提条件を収集整理した上で他の要件及び制約とのバランスをとりながら全体で最適となるセキュリティ機能を設計する能力が求められている。
本問では，大規模システムにおける，ログ管理システムの全体設計に関する，これらの能力と経験を問う。

設問 l　a　DHCP
b　NTP
設問 2（1）通信内容が暗号化されており，ログの内容が分析できないから
（2）**データ項目**　サーバのホスト名又はサーバの IP アドレス
判別できる場合　一つのウィンドウだけを使って特権操作を行った場合
判別の根拠となる情報　ログに記録された直前のログオン操作成功におけるサーバのホスト名又はサーバの IP アドレス
（3）DBMS のログ取得機能がサーバ資源を大量に消費するから
（4）**システム**　①　1
②　2
理由　特権操作 2 以外の DB アクセスのログが大量に取得されるから
（5）（F），(G)，（H）

設問 3（1）東京 DC の電源設備の保守作業のとき
（2）**最大データ量**　462
（3）　**伝送速度**　　6
（4）ログの改ざん防止のため
（5）ログを保存する際は暗号化を行う。
設問 4（1）①・管理端末と各サーバの時刻を同期させる。
②・管理端末と各サーバの ID 体系を統一する。
（2）**役割名称**　オペレータ
理由　　情報システム部の従業員はオペレータの具体的な作業内容を知らないから
（3）　**操作**　　各社の管理責任者が行う特権操作
内容　　特権操作を行った本人以外による確認

採点講評

問 1

問 1 では，医療情報システムを題材に，個人情報の取り扱い，ディジタル署名やタイムスタンプを用いたデータの完全既及び真正性，社会インフラにおける重要なシステムの事業継続について出題した。

設問 1(1)は，正答率が低かった。複数存在するアクタのうちどのアクタになりすますのかによって，発生するセキュリティ上のリスクが異なってくることを理解して解答してほしかった。(2)は，基礎的な技術に関する出題で，解答の多くは正しい技術用語で解答できていなかった。正しく理解し覚えてほしい。

設問 2(3)は，“アクセス主体"の意味を正しく理解していない解答が多かった。アクタ種別ごとのアクセス制御では不十分なことを踏まえ，“アクセス主体"を更に細かな単位で制御する必要があることに着眼してほしい。

設問 3(2)，(3)は，正答率が低かった。タイムスタンプ技術の目的と適用方法について，曖昧なまま理解している解答が多いように見受けられたので，基本的な技術を正確に理解してほしい。(4)は，改ざん検知後，電子カルテを回復する場合，どの時点の状態に戻るのかを認識して解答してほしい。

設問 4(1)は，緊急時にはシステム環境などに関する制約がある中で業務遂行上の優先順位付が必要になることを認識した上で，実行既のある方式を具体的に解答してほしい。(2)は，非常時に医療情報システムを利用する者の識別及び資格の有無など，アクセスの許可を判断する上で必要となる手続などを具体的に解答してほしい。

問 2

問 2 では，複数種類のサーバからなる既存システムに対して，統一したログ管理システムを適用する際の設計について出題した。全体として正答率は想定どおりであり，実務経験をもつ受験者にとっては，正解を導きやすい問題であったと思われる。

設問 2(2)は，正答率が低かった。特権操作 1 に対して記録すべきデータ項目と製品 R の仕様とを比較することで，解答を導き出すことを期待したが，製品 R の仕様や本文中に記載されている条件を十分に理解していないと思われる解答が多かった。実装方法の検討においては，要件や制約の抽出及び整理を行う必要があることを再認識してほしい。また，設問の趣旨を誤解した解答も多かった。解答においては，設問の趣旨を十分に理解してほ

しい。

設問 2(4)では，システムを正しく選択できているのに，理由を正確に記述できていない解答が多かった。大量のディスク資源が必要になる真の理由は，製品 H の仕様上の制約の結果，必要のないログが大量に取得されてしまうことである。ログ管理においては，ログの保存や分析のために大量のディスク資源が必要になるので，必要なログだけを取得する必要があることを理解しておいてほしい。

設問 4(1)は，正答率が低かった。“管理端末に固定の IP アドレスを割り当てる"とした解答が多く，本文に記載されている，各特権操作に対して取得すべきデータ項目を，正確に理解していない受験者が多かった。ログ管理においては，どのようなデータ項目を取得し，どのような分析を行うかを要件として具体的に定義した上で，最適な実装方法を検討する必要があることを再認識してほしい。