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。

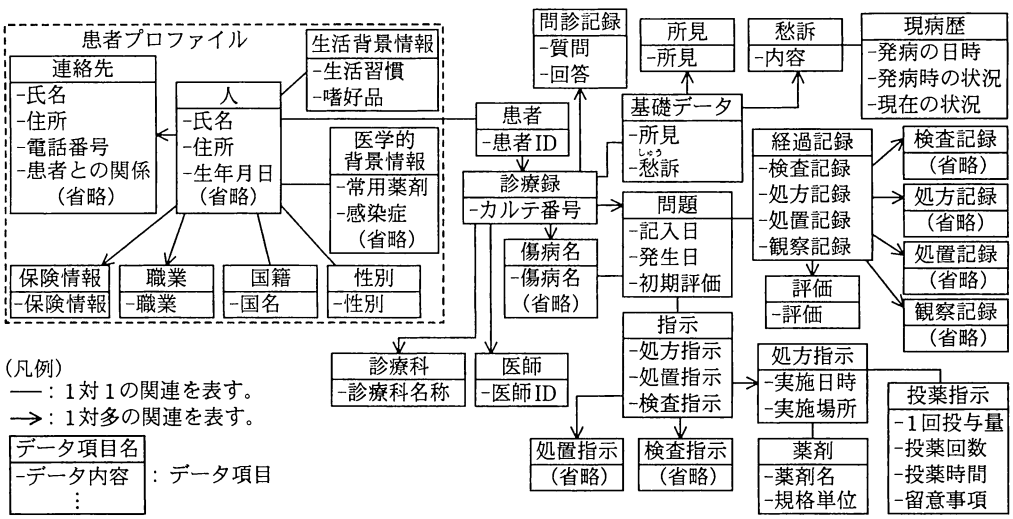


図 3　電子カルテの概念データモデル案（抜粋）

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テ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。

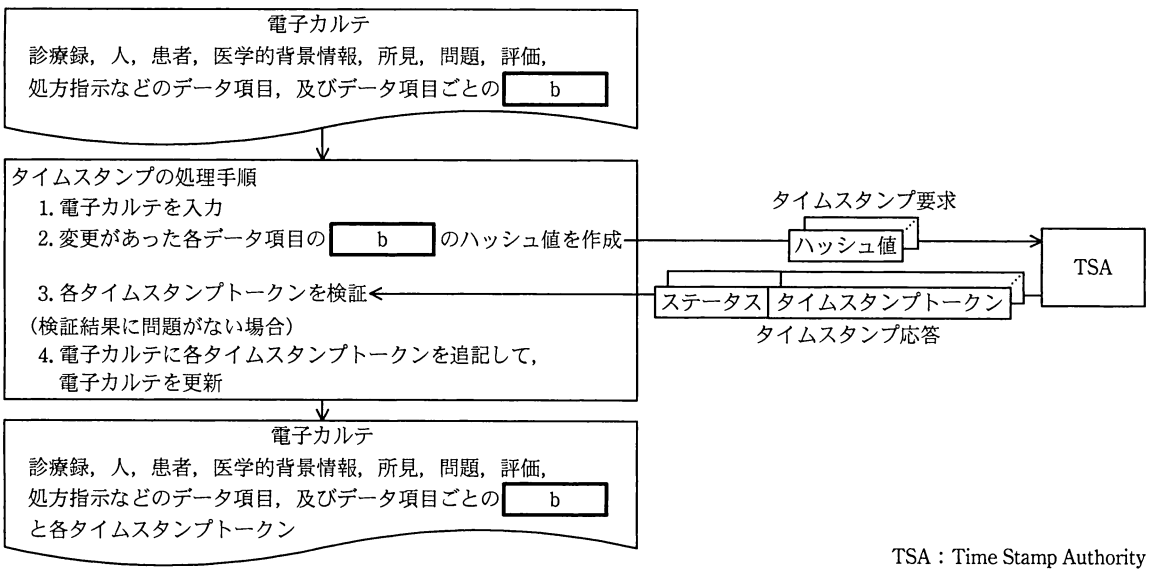


図 4　タイムスタンプ付与の仕組みの概要

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。

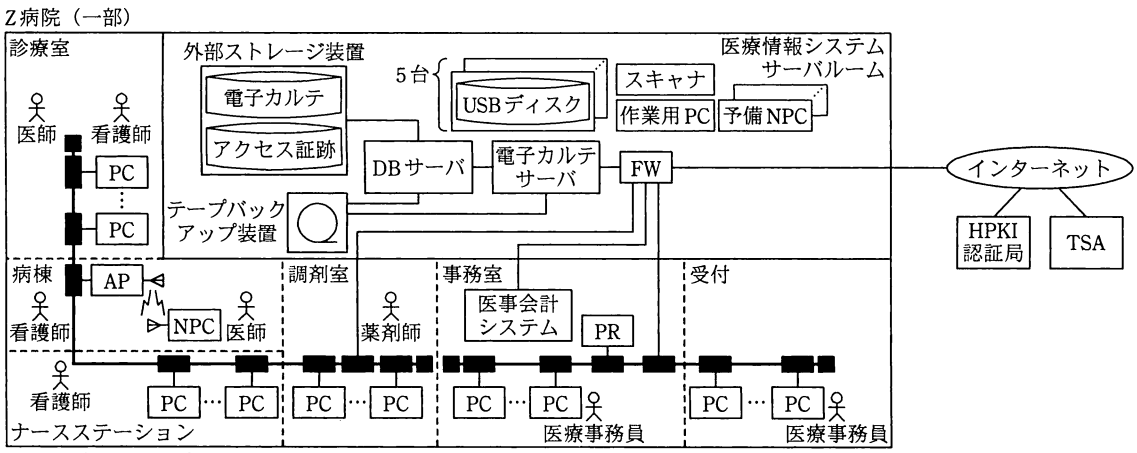
M氏　：加えて，“確定”登録が行われた電子カルテが改ざんされた場合に，単に検知するだけではなくて，⑤その後も，正しい電子カルテを用いて医療を提供する必要があります。

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。



PC：デスクトップPC　DBサーバ：データベースサーバ　FW：ファイアウォール
NPC：ノートPC　予備NPC：NPCの予備機　AP：無線LANアクセスポイント
PR：プリンタ　作業用PC：画像データ化作業用PC　USBディスク：USB接続可能なハードディスク装置

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IC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，IC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。