資料Ⅱ②

医療情報を受託管理する情報処理事業者向けガイドライン

平成 20 年 3 月

パーソナル情報研究会

【 目 次 】

1　はじめに

医療機関等で扱う文書類のうち、診療録、助産録、調剤録等（以下「診療録」という。）については、平成11年4月通知「診療録等の電子媒体による保存について[1]」によって、初めて診療録等の電子媒体による保存について基準が示された[2]。さらに、平成14年3月通知「診療録等の保存を行う場所について[3]」により、診療録等の電子保存及び保存場所に関する要件等が明確化された[4]。この通知においては、それまで認められていなかった診療録等の外部保存を行う場合の基準が明記されていた。また、それぞれの通知に対して「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン[5]」及び「診療録等の外部保存に関するガイドライン[6]」（以下「外部保存ガイドライン」という。）が示されていた。一方、平成15年に「個人情報の保護に関する法律」（平成15年法律第57号。以下「個人情報保護法」という。）が成立し、これを受けて医療・介護分野において平成16年12月には「医療・介護関係事業者における個人情報の適切な取扱のためのガイドライン」が公表され、平成17年4月の個人情報保護法の全面実施に際しての指針が示された。

さらに、平成17年3月、情報システムの導入及びそれに伴う外部保存を行う場合の取扱に関して、厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」にて「医療情報システムの安全管理に関するガイドライン」が策定された。このガイドラインは、「診療録等の電子媒体による保存について」及び「診療録等の保存を行う場所について」の各通知に基づき作成された各ガイドラインを統合し、新たに法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン（紙等の媒体による外部保存を含む）、及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインである。また、個人情報保護法及び「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成17年厚生労働省令第44号）に対する医療情報システムの具体的指針という側面も持ち合わせる。

1 平成11年4月22日付け健政発第517号・医薬発第587号・保発第82号厚生省健康政策局長・医薬安全局長・保険局長連名通知

2 民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成17年3月31日付け医政発第0331009号・薬食発第0331020号・保発第0331005号厚生労働省医政局長・医薬食品局長・保険局長連名通知）にて廃止

3 平成14年3月29日付け医政発0329003号・保発第0329001号厚生労働省医政局長・保険局長連名通知

4 「「診療録等の保存を行う場所について」の一部改正について」（平成17年3月31日付け医政発第0331010号・保発第0331006号厚生労働省医政局長・保険局長連名通知）にて一部改正

5 平成11年4月22日付け健政発第517号・医薬発第587号・保発第82号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付

6 平成14年5月31日付け医政発第0531005号通知に添付

その後、平成19年3月には医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件等を追加して、「医療情報システムの安全管理に関するガイドライン第2版」が策定された。

さらに、平成20年3月には、医療資格を持たないものが医療・健康情報を取扱う際のルール策定を検討した上で、責任のあり方についてまとめ、更に昨今の業務体系の多様化にも対応するため、モバイルアクセスで利用できるネットワークの接続形態毎の脅威を検討し、情報及び情報機器の持ち出し等について追記した、「医療情報システムの安全管理に関するガイドライン 第3版」（以下「医療情報安全管理ガイドライン」という。）が策定された。

このような一連の施策等により診療録等の情報を電子的に作成し保存することが許容されてきた。また、それらを外部に保存する場合も外部保存ガイドラインで具体的指針が示されている。しかし、外部保存ガイドラインでは医療に関連する情報は高度な機密性が求められるという理由により、医療機関等自らが外部保存を実施することを前提として策定されている。他方、医療機関が保有する診療録等を専門の民間情報処理事業者が管理することで、医療機関にとっては個人情報漏えい等のリスクを低減することが可能になると指摘されている。このため、厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」において、医療情報の外部保存が認められる際のルール化を進めるべく、現在、医療ガイドラインの改正作業が進められている。

医療機関から医療情報を受託する事業者となる立場の情報処理事業者については、現在、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の規定が適用されている。同ガイドラインは、多様な業種の事業者が広汎な種類の個人情報を取り扱うことを想定しているため、機微性の高い医療情報の取扱に携わる医療情報受託者に対しては、必ずしも十分な安全管理措置が規定されていない。

このため、本「パーソナル情報研究会[7]」は、医療情報の外部保存の安全性に万全を期す

7 「パーソナライゼーション時代の本格到来をにらみ、個人情報その他個人に関する情報について、将来想定される様々な利活用の方法を体系化すると共に、国民にとって安全・安心かつ適切な個人に関する情報の利活用を保証するための個人情報保護、セキュリティ、認証などのあり方について検討を行う」ことを目的に設置されている。

べく、医療情報受託者が義務的に講ずべき措置を具体的に明記した本ガイドラインを別途策定することとした。

すでに、安全基準、即ち情報セキュリティマネジメントシステムに関する標準規格としてJIS Q 27001:2006、個人情報保護マネジメントシステムに関する標準規格としてJIS Q 15001:2006が策定され多くの組織において活用されているが、既存の情報セキュリティ対策に関する各種の規格は広範な事業を対象として一般化されたものであり、本ガイドラインで扱う「医療情報取扱情報処理」事業の特殊性を鑑みて一段と具体化及び対策の深化を図る必要がある。このため、本ガイドラインでは「医療情報の外部委託」という事業特有の課題に配慮し、この分野において情報セキュリティマネジメントシステムを実装する上でのガイドラインを示すことを目的とする。

なお、本ガイドラインは、医療情報安全管理ガイドラインで示される医療機関等で実施される安全管理策と同等以上のセキュリティレベルを情報処理事業者に求めるものであるが、単にセキュリティレベルの高さに配慮するだけではなく、個々の安全管理策が要求されている理由及び背景について、医療情報安全管理ガイドラインに記されている事柄を十分に理解しておくことが必要である。

1.1 本ガイドラインで用いる医療情報用語の説明

本ガイドラインで扱う医療情報に関する特有の用語について、法令及びガイドライン類にて定義されている用語のうち、本ガイドラインの理解に必要なものについて以下に示す。

【 診療録 】

医師及び歯科医師が患者を診療した経過を記録したもの。カルテとも呼ばれ、診療終了後所定年限（5年等）の保存が義務づけられている。医師法施行規則第23条及び歯科医師施行規則第22条により「診療を受けた者の住所、氏名、性別及び年齢、病名及び主要症状、治療方法（処方及び処置）、診療の年月日」が記載事項とされている。

【 診療記録 】

診療諸記録ともいわれ、診療の過程で知りえた患者に関わる情報及び作成された記録から診療録を除いた部分のことで、検査結果、手術所見、医用画像（レントゲン写真等）、看護記録等を指す。本ガイドラインに基づき安全管理策を実施する際には、情報の種類に応じたリスク評価を行い、必要な安全レベルを考慮した安全管理策を選択することが求められる。

【 患者情報 】

上記の記録類に記載されている情報のうち、患者の既往症、家族歴、嗜好等のこと。高度なプライバシー情報であり、医療機関等にとっては守秘義務が課せられていることからも、機密性への高い配慮が求められる。なお、要介護者は言葉の定義としては患者には含まれないと考えられるが、その情報は同様に高度なプライバシーに関する情報であることから、要介護者の情報についても患者情報と同等と考え、要介護者情報を扱うシステムは下記の医療情報システムに含まれるものとする。

なお、これらのプライバシーに関する情報は、疾患に伴って医療機関等にかかった患者の情報に限らず、例えば介護認定時に医師が医師意見書を作成する際に行った問診情報も含まれると解される。したがって、患者情報は疾患に係わり収集された既往歴等だけに限らないことに留意しなくてはならない。

【 医療情報システム 】

患者を対象とする医療に関して、患者情報を含む医療情報及びその医療情報を扱うシステムを指す。

【 医療機関等 】

主に病院、診療所、薬局、助産所等を指す。

1.2　本ガイドラインで用いる制度及び技術用語の説明

本ガイドラインで扱う制度及び技術用語について、本ガイドラインの理解に必要なものについて以下に示す。

【 ISMS （Information Security Management System） 】

ISMS 適合性評価制度[8]では「ISMS とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することである。[9]」と定義している。ISO[10]のマネジメントモデルに準拠しており、P（Plan）、D（Do）、C（Check）、A（Act）サイクルを継続することで組織的な改善を図ることを特徴とする。

【 JIS Q 27001:2006 】

ISMS の国際標準規格として ISO/IEC 27001:2005 が定められており、これに対応する日本工業規格として JIS Q 27001:2006（情報セキュリティマネジメントシステム要求事項）が定められている（以下「JIS Q 27001」という。）。

【 ISMS 適合性評価制度 】

ISMS 適合性評価制度は、ある組織が構築した ISMS が JIS Q 27001 に適合しているかどうかを「認証機関」が審査して、認定された場合には「認定機関」に登録を行う仕組みである（以下「ISMS 評価制度」という。）。ISMS 認定を受けて登録されることを「ISMS 認証を取得する」とも呼ぶ。

【 JIS Q 15001:2006 】

日本工業標準調査会により審議された個人情報保護マネジメント要求事項の日本工業規格である（以下「JIS Q 15001」という。）。

【 プライバシーマーク制度 】

「日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度[11]」

[8] 財団法人 情報処理開発協会により運営されている
[9] http://www.isms.jipdec.jp/isms/index.html より引用
[10] International Organization for Standardization、国際標準化機構
[11] http://privacymark.jp/privacy_mark/about/outline_and_purpose.html より引用

【 情報資産 】

組織にとって価値のある情報のことである。記載される媒体は紙、電子媒体等の形態を問わない。情報資産を漏れなく識別し、その資産価値及びリスクを評価し、保護レベルを決定することが ISMS 構築において不可欠である。

【 機密性、完全性、可用性 】

機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）は CIA とも呼ばれ、情報セキュリティ上の要求事項の中でも最たるものと位置づけられる。ISMS 適合性評価制度における機密性とは「認可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性」、完全性とは「資産の正確さ及び完全さを保護する特性」、可用性とは「認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性」と定義されている。

【 安全管理策（Controls） 】

リスクに対して実施される対策のことを指す。

【 適用宣言書（statement of applicability）】

組織の確立する ISMS に関して適用される管理目的及び安全管理策を記述した文書のこと。一般には JIS Q 27001 付属書 A に沿って記述する。

【 専用線 】

特定の事業者間を接続する専用の回線であり、他事業者の通信の影響を受けず、通信回線上の機密性が高い性質を持つ。

【 VPN（仮想私設網、Virtual Private Network） 】

不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のこと。インターネット上に構築されたものをインターネット VPN と呼ぶ。

【 閉域網／閉域網 VPN（IP－VPN） 】

回線提供事業者が専有する回線上に構築された、特定加入事業者間のみを接続するネットワークの提供形態を指す。国内においては閉域 IP 網を提供する IP-VPN として利用されることが多い。

なお、本ガイドラインでは、回線の種別を表す用語として、専用線、閉域網 VPN（IP-VPN）、インターネット VPN の三種類を用いることにする。

1.3　本ガイドラインで用いる独自用語の説明

この他に、本ガイドラインで用いる用語のうち、特定の意味を持たせている用語について以下に示す。

【 作業者 】

情報処理事業者において情報処理機器を操作するものを作業者と呼ぶ。

【 情報処理事業者 】

本ガイドラインにおいては医療情報処理を受託する情報処理事業者を意味する。

【 医療情報処理施設 】

情報処理機器及び配置される物理的施設（データセンター、サーバーラック等）を含んだ情報処理施設全体を意味する。

【 医療情報処理システム 】

サーバ、端末、接続デバイス等、情報処理に関与する機器全体を意味する。

2　本ガイドライン策定の基本方針

本ガイドラインは外部保存等のために医療情報を受託管理する業務を提供する情報処理事業者にとって、預かっている情報の安全性[12]を確保するために実装すべき管理策（以下「安全管理策」という。）を具体化して提示することが主要な目的である。安全管理策を選考するために、提供される情報処理業務を想定し、業務で扱う情報、業務で利用する情報処理機器、業務を実施する職員及び組織構成等を情報資産として数え上げ、それぞれの潜在的リスクを、機密性、完全性、可用性といった情報セキュリティの要素、更に医療情報取扱に求められる真正性、見読性、保存性の要求事項から考察し、リスクの大きさにもとづいたリスク対応を選択、JIS Q 27001 のカテゴリに倣って具体的な安全管理策として記述及び整理する、という手順を行った。これは ISMS[13]ユーザーズガイド[14]に示される ISMS 構築ステップに倣ったものである。

本ガイドライン策定において重視した点は、医療情報及び医療情報処理に関わる機器を情報資産と考え、情報セキュリティ対策の原則として、情報資産へのアクセス可能領域、情報資産の流通経路、情報資産の可用性について認識し、リスクを極小化するため、移動経路を最小化すること、いずれの場所、時間においても制御可能とすること、迅速な異常の検出を可能とすることといった情報処理事業者の安全管理策に加えて法令及び医療情報安全管理ガイドライン等にて高い安全管理レベルを求められている医療機関に対して情報処理事業者の安全対策レベルを客観的に示すため、不足なく適用範囲を定めた適用宣言書に基づく情報セキュリティに関する認証及び認定を活用することである。

このような認証及び認定には、プライバシーマーク制度、ISMS 適合性評価制度等がある。情報処理事業者は本ガイドラインに示される安全管理策を適用した上で、適切な制度を選び、認証又は認定等を受けることが求められる。

---

12 6 章で説明する真正性、見読性、保存性を含む
13 Information Security Management System、情報セキュリティマネジメントシステム
14 （財）日本情報処理開発協会

2.1　安全管理策の整理と本ガイドラインの基本構成

安全管理策としては、「医療情報安全管理ガイドラインの最新の版である「医療情報システムの安全管理に関するガイドライン 第3版」に JIS Q 27001 を加え、JIS Q 27001 で示される管理策のカテゴリの形で整理して本ガイドラインを構成する（図 1）。

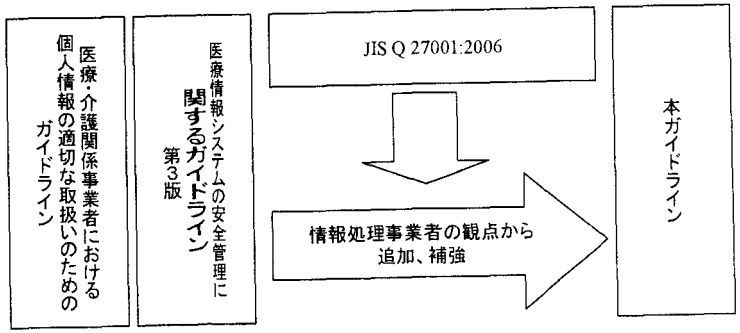

図 1 具体的な本ガイドラインの構成

医療情報安全管理ガイドラインでは、制度上の要求事項を満たすための管理策として「C. 最低限のガイドライン」及び「D. 推奨されるガイドライン」を示している。本ガイドラインでは、情報処理事業者の安全管理策として、C の必須事項は当然のこととして D の推奨事項の中でも、実施することが必要であると考えられる管理策についても合わせて必須事項として示している。これら、本ガイドラインで示される必須の安全管理策に加え、個人情報保護マネジメントシステムの要求事項である JIS Q 15001 及び情報セキュリティマネジメントシステムの要求事項である JIS Q 27001 等の標準規格に準拠するよう、包括的に安全管理策を具体化することが求められる。

医療情報安全管理ガイドラインでは、外部情報保存受託機関に対して「プライバシーマーク制度や不足なく適用範囲を定めた適用宣言書に基づく ISMS 認定制度等による公正な第三者の認定を受けていること」としている。医療情報の秘匿性の高さを考えれば、この方針は必要と考えられる。本ガイドラインにおいても同様にプライバシーマーク認定・ISMS 認証等の公正な第三者の認定を取得することを要件とする。

このため、適用範囲を医療情報処理システム全般として、上記の包括的安全管理策を記した適用宣言書を元にして、ISMS 評価制度に基づく第三者認証を取得することが推奨される。加えて、医療情報処理システムに対しては、本ガイドラインで示される安全管理策を基準とした第三者機関による情報セキュリティ監査等を定期的に（少なくとも一年に一回以上の頻度で）実施して、十分な情報セキュリティレベルを確保していることを検証することが望まれる。

2.2　医療情報安全管理ガイドラインとの対応関係

本ガイドラインと対となる医療情報安全管理ガイドラインに記載される安全管理措置との対応関係を表 1に示す。

表 1 医療情報安全管理ガイドラインと本ガイドラインの対応関係

医療情報安全管理ガイドライン	本ガイドラインの対応する部分
6 情報システムの基本的な安全管理	7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項
7 電子保存の要求事項について	6 電子保存の要求事項について
8 診療録及び診療諸記録を外部に保存する際の基準	8診療録及び診療諸記録を外部に保存する際の基準

なお、医療情報安全管理ガイドラインでは、「7 電子保存の要求事項について」の中で真正性、見読性、保存性を確保するための安全管理策をまとめているが、本ガイドラインでは、「医療情報を受託管理する情報処理事業者における安全管理上の要求事項」の中で、真正性、見読性、保存性を確保するための安全管理策を JIS Q 27001 の分類でまとめている。

3　本ガイドラインの対象システム及び対象情報

本ガイドラインは外部の情報処理事業者が医療機関等から情報処理業務を受託して医療情報を取扱う際の安全管理基準を示すものであり、扱う情報の種類としては、法令で外部保存が認められる医療情報（表 4 電子保存及び外部保存が許されている文書を参照）を対象とし、情報システムとしては、医療情報を電磁的記録として媒体経由及びネットワーク経由で受入れ、保管し、医療機関等の要請で検索する等、一定の処理を行うシステムを対象と考える。この全体概要は図 2 に示される。つまり、医療機関等においては医療情報安全管理ガイドラインに従ってシステム構築及び個人情報の保護に係る安全管理措置を適用し、情報処理事業者においては本ガイドラインに従ってシステム構築及び個人情報の保護に係る安全管理措置を適用するという関係にある。

本ガイドラインの対象とする情報処理に関する医療情報交換経路は、（1）電子媒体に情報を格納した上で物理的に運搬する経路、（2）電磁的記録として作成された電子ファイルをネットワーク経由で転送する経路、（3）情報処理事業者が提供するアプリケーションに情報を入力することで情報処理事業者側に電磁的記録が作成される経路の三通りを組み合わせることを想定する。

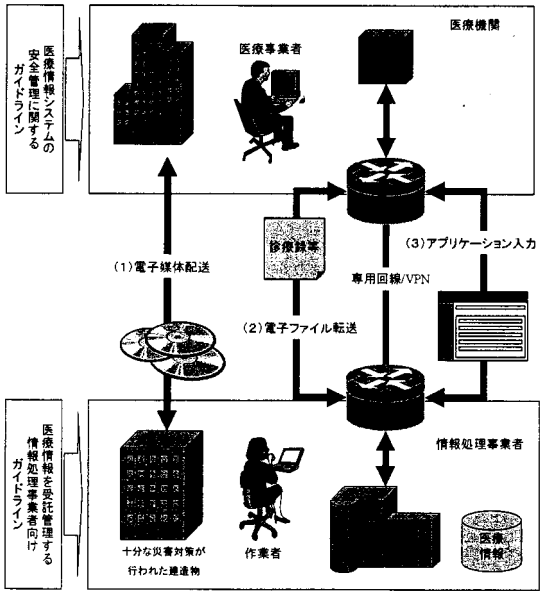

図 2 本ガイドラインで対象とする情報システムの概念

情報サービスの概念としては外部ストレージサービス及び情報検索サービスと呼ばれているシステムに類し、どの程度の検索機能や情報処理機能を提供するのかは医療機関等の要請に従うものである。ただし、医療情報安全管理ガイドラインに「外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、情報を閲覧、分析等を目的として取り扱うことはあってはならず、許されない。」、また「例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。さらに、外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理したり、あるいは情報処理事業者の管理者といえどもアクセスできない制御機構をもつことも考えられる。」（医療情報安全管理ガイドライン 8.1.2 章参照）とあるように、原則として、機密管理の観点から受託管理する医療情報の全体を情報処理事業者が閲覧・処理することを行うことは想定されていない。

他方、サービスの内容によって情報処理事業者が閲覧しなければならない情報の範囲は変わるため、医療機関等が求めるサービスの実現のために必要であるならば、上記の医療情報安全管理ガイドラインにおける記述を踏まえつつ、医療情報の秘匿性の高さに十分配慮して、適切なアクセス管理を実施した上で情報処理事業者が医療情報を閲覧することも考えられる。

なお、情報処理システムを設置する場所については、情報処理事業者が専有する建造物あるいはフロア（自社所有のデータセンター等）が望ましいが、現実的には外部事業者の運営するデータセンター内にサーバラック設置場所を借りて利用する場合が多いと考えられる。その場合には、本ガイドラインの物理的安全対策に準拠したデータセンターを選択すること。設置するサーバラックについては、情報処理事業者の専有とし、医療情報処理装置以外の機器を設置しない、扉の鍵管理を厳格に行う等の物理的対策を施すこと。

情報処理ソフトウェアをサーバ上で動作させる場合、サーバにアクセスするための端末の配置が問題になる。サーバはデータセンター内の入退室管理された領域に置いたとしても、端末を配置する領域の安全性が劣ることは避けなければならない。端末を同じサーバラック内に設置することは現実的ではないため、データセンター内に端末室があればデータセンター内の LAN を経由してサーバと端末室の端末を接続する、端末室が無い場合にはデータセンターの外部にある情報処理事業者自身の施設内に安全を確保した端末室を設けて、閉域網 VPN（IP-VPN）あるいは IPsec[15]と IKE[16]を併用したインターネット VPN を経由してサーバと端末を接続するといった方法が考えられる（図 3）。

[15] Security Architecture for Internet Protocol、IP レイヤにて認証、完全性、機密性を提供するプロトコル
[16] Internet Key Exchange、IPsec において通信に用いる鍵に関するパラメータ交換及び、定期的な鍵更新を行う仕組み

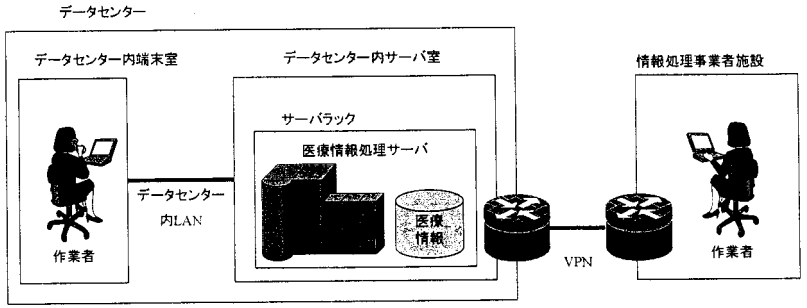

図 3 データセンターの利用とサーバ及び端末の配置

いずれの場合も、ネットワークの安全管理を厳密に行うとともに、端末へのアクセス、ログオンアカウント管理を厳密に行うこと。

以下で述べるように医療機関と情報処理事業者間をネットワークで接続して情報交換を行う場合には、図 2 にあるように専用線あるいは VPN といった第三者による傍受のリスクが低いネットワークを利用すること。更に医用画像（レントゲンデータ等）等、転送する情報量が相当に大きくなることもあることから、必要なネットワーク容量の見積もりを適切に行い、十分なネットワーク容量を確保すること。

3.1　電子媒体の選択についての考慮事項

電磁的記録としての医療情報は電子媒体上に保管することとなる。「診療録等の電子媒体による保存に関する解説書[17]」によると電子媒体とは「保存による情報の劣化を防ぐためデジタル記録ができる媒体及び機器」のこととされている。具体的な媒体及び機器としては、MO[18]等の光磁気ディスク、CD、DVD 等の光学ディスク、USB[19]メモリ、コンパクトフラッシュカード、SD メモリーカード[20]等の半導体メモリ、ハードディスク等の磁気ディスク等が考えられる。

医療情報は長期保存が求められる性質上、紫外線による劣化が進むといわれる色素を用いた書き込み型の光学ディスクよりも、経年変化に強いとされる光磁気ディスクが望ましいといえるが、光学ディスクであっても保管環境を整備することで寿命を延ばすことができる。長期保存を目的として、これらの電子媒体を利用する場合には、製造元の保存仕様に準拠した保管を行い、見読性、保存性を損なわないように配慮すること。

長期保存が主目的であり頻繁に情報を閲覧する必要がない場合には、光学ディスク、光磁気ディスクに記録し、適切な保管環境で管理することが望ましいが、頻繁に情報を閲覧する場合には情報処理装置に接続された磁気ディスクに記録して管理することになる。この場合には、情報処理装置上のアクセス権限管理を厳密に行い、不正なアクセスから情報を保護することが必要である。また、適切に暗号技術を利用することで情報を保護する方策も検討すること。

なお、媒体としての半導体メモリについては micro SD のような極めて小型で記憶容量が大きな媒体が存在する。衣服などのわずかな隙間にも隠すことができるため、不正に情報の持ち出しを行おうとするものにとっては便利なものである。医療情報を格納する電子媒体としての有益性は認められるものの、大きなリスクも認められることから、原則として医療情報処理機器では外部デバイスとして半導体メモリの使用を行うことができないよう配慮することが望ましい。必要により使用する場合、使用前には不要なデータが書き込まれていないことを確認し、使用後には媒体上の全てのデータを削除すること。また、利用時間及び媒体の移動範囲を最小にするなどの管理を行うこと。

[17] 平成 11 年 10 月 厚生省健康政策局研究開発振興課医療技術情報推進室監修 （財）医療情報システム開発センター 編集
[18] Magneto Optical Disc
[19] Universal Serial Bus
[20] Secure Digital Memory Card

3.2　ネットワーク利用上の考慮事項

医療情報安全管理ガイドライン「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」には「外部と医療情報を外部ネットワークを利用して交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送受信データに対する「傍受」及び「改ざん」、ネットワークに対する「侵入」及び「妨害」などの脅威から守らなければならない。」とある。

このため、保管のためのデータ移動等、ネットワーク経由での情報管理機能を提供する場合には、医療機関等と情報処理事業者側設備をつなぐネットワーク部分に適切な安全管理措置を施す必要がある。この際、安全面への配慮からは専用線と同等の回線を用いるべきである。しかし、一般に専用線は利用コストが高価であることから、公衆回線上に仮想の閉域網を構築する技術の一種である、広域イーサネット、VPN 等を採用することも検討対象と考えることができる。

インターネット等、不特定事業者と共有するネットワーク上の VPN は、専用線及び閉域網 VPN（IP-VPN）では存在しない、サービス不能攻撃、ブルートフォース攻撃[21]等を受けるリスクがあり、安全性が比較的低いと考えられる。しかし、運用を適切に行うことで十分な安全性を確保することは可能であり、これまでに例として上げた種類の回線と比べて回線コストが格段に安いというメリットもあることから、適切に運用すること及び医療機関の合意を得ることを前提として、IPsec に IKE を組み合わせ、自動鍵更新を行う設定にて、インターネット上の VPN を採用することも可能とする。

ただし、インターネットからの第三者による不正なアクセスを防止するため、医療機関等の機器と情報処理事業者側の機器において、VPN チャンネル[23]上のプライベートネットワークインタフェースではプライベートアドレス[24]のみを利用して接続することとし、ネットワーク境界のファイアウォール又は VPN 装置等により、適切なアクセス制御を行うこと（「3.5.2 ネットワーク利用上の考慮事項」を参照）。いずれの種別の回線であっても、通信ログ及び通信状況を監視し、異常が発生した場合には迅速に対処すること。

[21] brute force attack（力任せの攻撃）、ここではログインに成功するまで ID とパスワードの様々な組み合わせを試しつづける攻撃を意味する。
[23] VPN として確立される仮想回線を指す
[24] インターネット上で通信可能な IP アドレスをグローバルアドレスと呼び、インターネットと直接の通信を行わない IP アドレスをプライベートアドレスと呼ぶ。

3.3　電子媒体による外部保存を可搬型媒体経由で行う場合の手順

医療情報を CD、DVD、MO 等の可搬型媒体を利用して情報処理事業者の施設に保存する場合の一連の手順を例として以下のように考える。

- 医療機関等の医療従事者の作業手順

(1) 医療情報を外部保存することに関する内部申請及び承認プロセスの実施

(2) 外部保存対象の電子ファイルについて電子署名を付与（必要に応じて暗号化を行う）

(3) 外部保存対象の電子ファイルを可搬型媒体に書き込み、施錠可能な容器等に納める等、配送経路上での開封を検知できるように封印を行う

(4) 信頼できる配送業者に配送を指示する（信頼確保の手順は後述）

(5) 情報処理事業者に対し、配送する可搬型媒体の数量、配送業者の作業者情報、予想到着時刻等を通知

- 情報処理事業者の作業手順

(1) 到着した配送業者の身分確認後に受領

(2) 受け取った可搬型媒体の数量、封印が正常であること等を確認

(3) 医療情報処理システムとネットワーク接続されていない機器上で媒体に悪意のあるコードが混入していないことを検証及び添付された電子署名を検証（悪意のあるコードについては「7.7.3 悪意のあるコードに対する管理策」を参照）

(4-1) 可搬型媒体そのものを保管する場合には可搬型媒体を保管庫に格納

(4-2) 可搬型媒体上の電子ファイルを情報処理機器上で保管する場合には医療情報処理機器に媒体中の電子ファイルを複写し、可搬型媒体は適切な手段で廃棄処分（廃棄手順については「7.7.7 媒体の取扱」を参照）

(5) 受領した電子ファイル又は可搬型媒体の情報を管理台帳に記載

(6) 医療機関等に受付情報を通知

このような可搬型媒体の交換手順について医療事業者と合意し、手順書として双方で管理すること。なお、受領した可搬型媒体そのものを保管する場合には、情報を破棄する際に媒体ごと破棄できるように電子ファイルを整理して記録するよう医療機関等と協調して配慮すること。

配送事業者の信頼性については、機密保持契約の締結が可能である、機密情報の配送に特化した配送サービスを提供している、配送状況を利用者が把握する機能を提供している等の条件により事業者を選択することで確保すること。

3.4　電子媒体による外部保存をネットワーク経由で行う場合の手順

医療情報をネットワーク経由で情報処理事業者の施設に保存する場合の一連の手順を例として以下のように考える。

- 医療機関等の医療従事者の作業手順

(1) 医療情報を外部保存することに関する内部申請及び承認プロセスの実施

(2) 外部保存対象の電子ファイルについて電子署名を付与（必要に応じて暗号化を行う）

(3) 医療機関等と情報処理事業者を接続するネットワーク上の機器に電子ファイルを複写（なお、医療機関等の内部ネットワークと電子ファイル転送用のネットワークが接続されている場合は不要な通信が行われないよう適切な安全管理対策、アクセス制御を適用すること）

(4) ネットワークを経由して情報処理事業者の受入れ機器に電子ファイルを複写

(5) 情報処理事業者に送出完了を通知

- 情報処理事業者の作業手順

(1) 医療事業者からの電子ファイル転送を常時監視するようシステムを整備

(2) 電子ファイルが転送されてきたことを検知した際は悪意のあるコードが混入していないことを検証及び電子ファイルに添付された電子署名を検証（異常を検出した場合には即座に医療事業者に通知すること）

(3) 医療機関等から電子ファイルを転送するフォルダは一時フォルダとし、上記検証後に電子ファイルを保管用フォルダに移動（一時フォルダ内の電子ファイルは削除する）

(4) 複写した電子ファイルの受付情報をまとめて管理台帳に記載

(5) 医療機関等に受付情報を通知

このようなネットワーク経由の交換手順について医療事業者と合意し、手順書として双方で管理すること。なお、ファイル転送についてインターネット標準技術であるFTP[25]プロトコルを用いる場合においては専用回線あるいはVPN技術等を利用してネットワーク上で

[25] File Transfer Protocol

のパスワード及びデータ漏えいのリスクを低減すること。若しくはSFTP[26]等、セキュリティ機能が組み込まれたファイル転送プロトコルを利用すること。

上記手順を図 4 に示す。

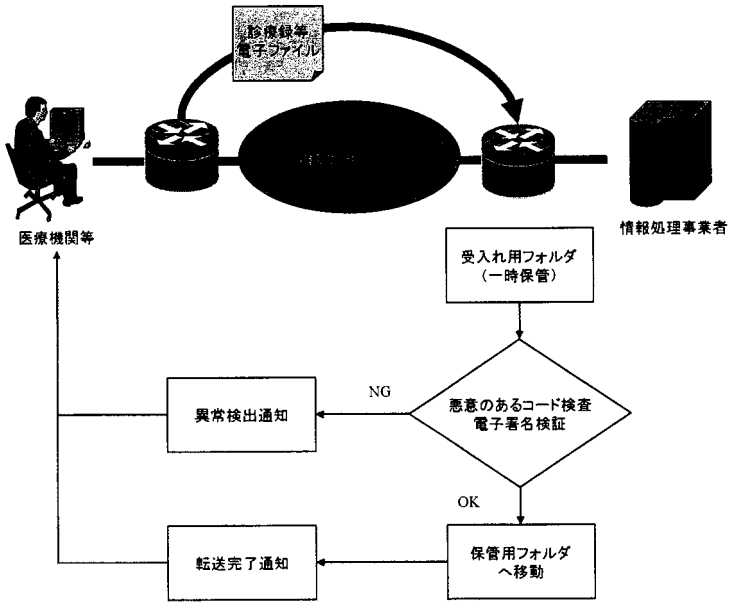

図 4 電子媒体による外部保存をネットワーク経由で行う場合

悪意のあるコード検査及び電子署名検証の過程で問題が発見された場合はただちに医療機関等に通知すること。なお、問題が発見された電子ファイルは原因特定を行う必要があることから、削除せずに情報処理機器から隔離したかたちで保管すること。

ここまでに示した電子媒体の外部保存に関して、その経路に拠らず実施すべき作業について以下に示す。

- 医療機関等の医療従事者の作業手順

(1) 情報処理事業者からの定時報告を確認、検証する。

[26] Secure File Transfer Protocol

(2) 不審な点があれば、ただちに確認を行う。

- 情報処理事業者の作業手順

(1) 一日ごとに、受入れた電子ファイル、払出した電子ファイル、預かっている電子ファイルの数量、発生したイベント等について医療機関等に通知する。

(2) 検証手続き中に異常が検出された場合は、直ちに医療機関等に連絡し、適切な事故対応手順を実施する。

なお、ここでは情報の受入れ手順について記述したが、廃棄手順については「7.6.4 情報処理装置の廃棄及び再利用に関する要求事項」及び「7.7.7 媒体の取扱」、「7.9 情報の破棄」等に示される管理策を適用すること。

3.5 アプリケーション入力による外部保存をネットワーク経由で行う場合の手順

外部の情報処理事業者が所有する情報処理システムで実施される情報処理サービスを、ネットワーク経由で提供する形態を ASP（Application Service Provider）又は SaaS（Software as a Service）と呼ぶ（以下「SaaS・ASP」という。）。SaaS・ASP とは利用者別に開発したアプリケーションあるいはカスタマイズしたパッケージソフトウェアの運用と稼働環境である情報処理システムの運用を合わせて提供するサービス、いわゆるアプリケーションホスティングと呼ばれる形態から、共同アウトソーシングのように施設を共同で利用する形態、更に全ての利用者が情報処理システムを共有し、更に同一のアプリケーションを利用することで価格面のメリットを追及した形態（この形態を特に SaaS という）まで様々なものがある。

本ガイドラインの対象とする情報処理システムは「医療機関等の要請で検索等、一定の処理を行うシステム」であることを述べた。このシステムの提供形態としても SaaS・ASP が想定される。しかし、SaaS・ASP では計算機環境を共有する場合があり、利用者間の悪影響が発生する可能性が存在すると考えられるため、システム構築、システム運用時の考慮事項について、「3.5.2 ネットワーク利用上の考慮事項」に従い、適切な対策を行うことが要求される

SaaS・ASP 形式のサービス等を利用して医療情報をアプリケーション入力する場合の一連の手順を以下のように考える。

- 医療機関等の医療従事者の作業手順

(1) アプリケーションにログオン

(2) アプリケーションに医療情報を入力

(3) 医療情報の送信又は保存

(4) アプリケーションからログオフ

- 情報処理事業者の作業手順

(1) 入力された医療情報の暗号化（必要に応じて）

(2) データベースへの登録

このようなアプリケーション入力による医療情報の交換手順について医療事業者と合意し、手順書として双方で管理すること。また、電子署名の付与が求められる情報については、電子ファイルとして作成してファイルを転送する形をとることが望ましく、その場合には、情報処理事業者にて受け取ったファイルの電子署名を検証することになる。

なお、SaaS・ASP ではウェブブラウザをクライアントとした、いわゆるウェブアプリケーションを提供することが多いと考えられる。ウェブアプリケーション特有のセキュリティ上の要求事項に配慮して、サービス提供時はもちろん、リスク評価を行い、必要に応じて定期的にアプリケーションの脆弱性検査[27]を実施して、安全性を確認すること。

3.5.1 データベース利用上の考慮事項

アプリケーション入力による外部保存では、一般的に入力データはデータベースに格納されることになると考えられる（図 5）。

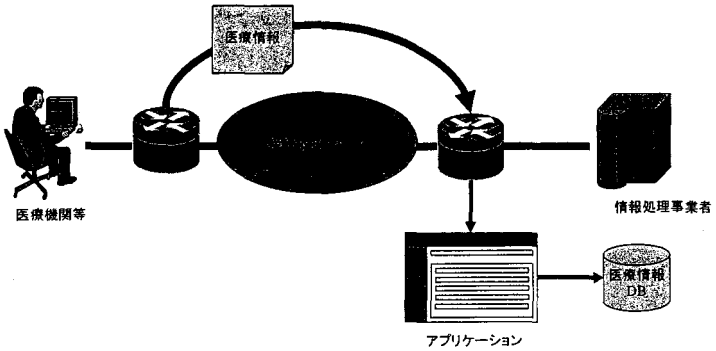

図 5 アプリケーション入力による外部保存をネットワーク経由で行う場合

ここで検討しなければならないことの一つは情報漏えい対策として暗号化を行うことである。データベース及びデータベースシステムにおける暗号化とは、データベースファイルをハードディスクのパーティションとして構成してパーティション全体を暗号化すること、電子ファイルとしてデータベースファイルを暗号化すること、データベース中のデータ（テーブル、行、カラム等）を個々に暗号化すること等、いくつかの手法が知られている。ここで配慮しなければならないリスクとしては、データベースを格納した機器の盗難等による情報漏えい、電子ファイルとしてのデータベースファイルの盗難等による情報漏えい、データベースにアクセスすることによる個々のデータの盗難等による情報漏えい等である。

ここであげた三つの情報漏えいリスクに対する三つの暗号化手法の効果を表 2 にまとめる。

[27] 検査すべき脆弱性としては「安全なウェブサイトの作り方 改訂第 3 版」IPA を参照のこと

表 2 情報漏えいリスクに対する暗号化対象別の効果

	機器の盗難等による情報漏えい	電子ファイルとしてのデータベースファイルの盗難	データベースアクセスによる情報漏えい
パーティションの暗号化	○	×	×
データベースファイルの暗号化	○	○	×
データベース中のデータの暗号化	○	○	○

パーティション全体を暗号化した場合、機器の盗難に対しては一定の効果があるが、機器の稼動中はオペレーティングシステムに対しては復号された状態になり、ログオンユーザ、特に特権ユーザに対しての保護策にはならない。このため、不正にログオンする行為、あるいはログオンユーザの不正行為には効果が薄い。電子ファイルとしてデータベースを暗号化した場合、オペレーティングシステムからも暗号化されたままの状態であるため、ユーザアカウントからデータベースを保護することができる。しかし、データベースプロセスに対しては復号された状態であるため、データベースアクセスを悪用した情報漏えい行為に対しては効果がない場合がある。このため、データベースのユーザアカウントに対しては保護にならない。データベース中のデータを個別に暗号化した場合には、そのデータに対するアクセス権限をデータベースシステム上で与えられていなければデータを復号された状態で知ることはできないため、機器及びデータベースファイルの盗難等、データベースアクセスを悪用した情報漏えい行為の全てに対して保護を提供することが可能である。ただし、データ毎に細かい粒度のアクセス設定を間違いなく行う必要があり、管理運用のコスト及び設定ミスによるリスクも高くなるという側面があることに注意すること。

なお、データベースを利用したシステムでは、内部関係者による不正行為、情報漏洩を視野に入れて対策を講じる必要がある。一般的にウェブアプリケーションの利用環境ではデータベースに直接アクセスする管理者、開発者といったアカウントはその職責上多くの権限が付与されているケースがあり、リスクが大きい。そのため「なりすまし」によってこれらのアカウントの不正使用を防ぐため、パスワードの管理を厳密に行うだけでなく、必要に応じて多要素認証などの技術を利用し十分な認証強度を確保しなければならない。

このように、アプリケーション入力による外部保存をネットワーク経由で行ってデータをデータベースにより保管する場合には、システムの構成に配慮したリスク評価を行い、暗号技術等を利用した適切なリスク低減策を適用すること。

3.5.2 ネットワーク利用上の考慮事項

アプリケーション入力をおこなう場合には、第三者による傍受のリスクを避けるため、アプリケーションを提供する情報処理事業者と医療機関を接続するネットワークは専用回線あるいは VPN を利用することが要求される。VPN はインターネット等の不特定多数が接続されるネットワーク上に構築されたものであっても、医療機関の理解と合意があれば利用することができるとするが、インターネット VPN には傍受以外にも第三者による不正な中継（man in the middle）、サービス不能攻撃等のリスクが存在し、回線品質も比較的低いため、閉域網上に構築された VPN を利用することが望ましい。

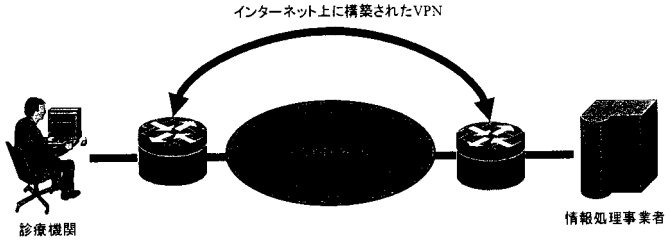

図 6 インターネット上に構築された VPN

インターネット上の VPN を利用する場合には、第三者からの不正なアクセスを防止するため、以下に示す制約に従うこと。

- 医療機関側機器と情報処理事業者側機器を接続する VPN チャンネル上のプライベートネットワークインタフェースに割り当てるアドレスをプライベートアドレス[28]に限定すること（VPN チャンネル上のインターネットインターフェースアドレスはグローバルアドレスで良い）。
- インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に経路を設定しないこと。

また、複数の医療機関等から情報処理業務を委託している場合には、医療機関等の間で

[28] RFC1918 “Address Allocation for Private Internets” で規定される。RFC は国際団体 IETF が発行するインターネット標準文書。

情報が混同するリスクを避けるため VPN チャンネルを医療機関別に構築すること。