

保健医療福祉分野のプライバシーマーク認定指針

第 2.1 版

2010 年 4 月

財団法人 医療情報システム開発センター

プライバシーマーク付与認定審査室

改定履歴

版数	日付	内容
第1版	平成18年10月19日	JIS Q 15001:2006 に準拠した認定指針として発行
第2版	平成20年10月1日	本文：審査の実績から、審査で確認する内容は、できるかぎり” C. 最低限のガイドライン” に反映した。また、”3.4.3.2 安全管理措置”、”3.7.2 監査”、” 3.8 是正措置及び予防措置” の内容を重点的に見直した。 付録：第1版の付録9～13（申請の様式等）を削除し、「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」の要約を別冊として巻末に添付した。
第2.1版	平成22年4月1日	一部表現の修正、及び「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版の要約を、4.1版の第6章等と差し替える。

目次

はじめに	1
1 適用範囲	5
2 用語及び定義	6
3 要求事項	7
3. 1 一般要求事項.....	7
3. 2 個人情報保護方針	7
3. 3 計画.....	9
3. 3. 1 個人情報の特定	9
3. 3. 2 法令、国が定める指針その他の規範.....	11
3. 3. 3 リスク等の認識・分析及び対策	12
3. 3. 4 資源、役割、責任及び権限	14
3. 3. 5 内部規程.....	16
3. 3. 6 計画書.....	17
3. 3. 7 緊急事態への準備.....	18
3. 4 実施及び運用.....	20
3. 4. 1 運用手順.....	20
3. 4. 2 取得・利用及び提供に関する原則.....	20
3. 4. 3 適正管理.....	36
3. 4. 4 個人情報に関する本人の権利.....	45
3. 4. 5 教育.....	53
3. 5 個人情報保護マネジメントシステム文書.....	54
3. 5. 1 文書の範囲	54
3. 5. 2 文書管理.....	55
3. 5. 3 記録の管理	56
3. 6 苦情及び相談への対応	57
3. 7 点検.....	58
3. 7. 1 運用の確認	58
3. 7. 2 監査.....	59
3. 8 是正処置及び予防処置	60
3. 9 事業者の代表者による見直し.....	61
付録1 医療における個人情報保護に関連する法令条文及び規範など.....	63
付録2 保健医療分野の保存義務に関する法令等	67

付録 3	医療機関における個人情報を含む書類の例.....	71
付録 4	医療機関における個人情報保護方針の例	72
付録 5	内部規程体系の例	74
付録 6	医療機関における同意文書の例	77
付録 7	医療機関における個人情報の利用目的文書の例.....	79
付録 8	医療機関における開示対象個人情報の周知に関する文書の例.....	81
付録 9	「医療情報システムの安全管理に関するガイドライン」抜粋	83
6	情報システムの基本的な安全管理.....	83
6.1	方針の制定と公表.....	84
6.2	医療機関における情報セキュリティマネジメントシステム (ISMS) の実践..	85
6.3	組織的安全管理対策 (体制、運用管理規程)	89
6.4	物理的安全対策	90
6.5	技術的安全対策	91
6.6	人的安全対策.....	98
6.7	情報の破棄	100
6.8	情報システムの改造と保守	100
6.9	情報及び情報機器の持ち出しについて.....	102
6.10	災害等の非常時の対応.....	104
6.11	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.....	107
6.12	法令で定められた記名・押印を電子署名で行うことについて.....	124
付表 1	一般管理における運用管理の実施項目例.....	127
付表 2	電子保存における運用管理の実施項目例.....	131
付表 3	外部保存における運用管理の例	133
	用語解説	135

はじめに

1) 指針作成の背景と経緯

個人情報をコンピュータに蓄積し、ネットワークを通じて交換するネットワーク社会では、さまざまな媒体やネットワークサービスなどを通じて多くの個人情報が拡散することや、不正に入手した個人情報が悪用されることなど、従来にないプライバシーの侵害が行われることが想定される。わが国の民間部門における個人情報の保護については、従来から自主的な規制によって対応してきた。その根拠として、行政機関が独自に定めた、いわゆる個人情報保護ガイドラインを基準としてきた。例えば、経済産業省が1997年3月に改訂して制定した「民間部門における電子計算機処理に係る個人情報保護に関するガイドライン」が代表的なものである。

自主基準を一段と推進する必要から、あらゆる産業分野に適用する国内基準として、1999年3月にこれらのガイドラインをベースとした日本工業規格「個人情報に関するコンプライアンス・プログラムの要求事項」(JIS Q 15001:1999)が制定された。当該JISには、この利用方法として、事業者が自己の個人情報保護の取組みがJISに適合していることを自ら評価するために用いることができるとともに、第三者による評価の基準としても活用できることが記述されている。このことから、1998年4月から既にスタートしていた「プライバシーマーク制度」が、JISを基準とした第三者認証制度として本格的に運用を開始した。プライバシーマーク制度は、JIS Q 15001に基づいた個人情報の適切な保護のための体制を整備している事業者に対し、その申請に基づいて、審査を行い、認定の旨を示すプライバシーマークの付与を行う制度である。

JIS Q 15001は、あらゆる産業分野に適用することが可能であるが、そのために特定の産業分野に偏らない内容となっている。一方、分野によっては個人情報の取扱いにおいて、その分野独自の慣行等特殊な事情があることから、JIS Q 15001の適用においてはその分野の特殊性を勘案しなければならない。特に、個人情報の取扱いが複雑で多岐にわたっている医療関連機関においては、この傾向が強い。そのため、医療分野の個人情報保護の推進を加速させることを目的として、(財)日本情報処理開発協会は、医療分野の専門家による「医療機関の認定指針検討WG」を設定して、医療分野にJISを適用する際のガイドラインとなる解説書を作成し、2002年10月に「医療機関の認定指針」として公表した。

2003年7月に(財)医療情報システム開発センターがプライバシーマーク付与認定審査指定機関に指定され、「医療機関の認定指針」に基づく保健医療福祉分野の事業者に対する付与認定審査を実施している。その後、2004年12月に厚生労働省が「医療・介護関係事業者における個人情報保護の適切な取扱いのためのガイドライン」(以下、「厚生労働省のガイドライン」という)を公表、2005年4月の「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)の全面施行等、個人情報保護に関する大きな情勢変化があった。さらに2006年5月20日にはJIS Q 15001:1999が改訂され、

「個人情報保護マネジメントシステム—要求事項（JIS Q 15001:2006）」として公表された。

これらのことをふまえ「医療機関の認定指針」を改訂することとした。改訂に当たっては、これまでの保健医療福祉分野の付与認定審査の実績から、(財)医療情報システム開発センターが当たることとし、保健医療福祉分野の専門家による「医療機関の認定指針・改訂委員会」を設置して検討し、従来の「医療機関の認定指針」を見直し、「保健医療福祉分野のプライバシーマーク認定指針」とした。

2) 本指針の適用範囲

本認定指針は、保健医療福祉分野の事業者がプライバシーマークを取得する際の留意点を示しているが、特にことわりがない場合は医療機関を想定して解説している。保健医療及び介護福祉情報等の特定の機微な個人情報を主として取り扱う事業者であれば、医療機関との連携があること及び医療機関と個人情報の取り扱いに大きな差異はないことから、医療機関以外であっても本指針に従うこととする。

3) 指針の構成

指針は JIS Q 15001 の項目番号と項目名ごとに、下記の構成になっている。

A. JIS Q 15001 の要求事項

JIS Q 15001 の要求事項を原文通りに記載し、四角の枠で囲んでいる。

B. 保健医療福祉分野としての解釈

保健医療福祉分野に JIS Q 15001 を適用する場合の要求事項の解釈を記載している。

C. 最低限のガイドライン

最低限実施しなくてはならない方策の指針を記載している。

D. 推奨されるガイドライン

最低限のガイドラインに保健医療福祉分野の実情を配慮し、追加した方が望ましい方策を含めた指針を記載している。

4) 保健医療福祉分野におけるプライバシーマーク取得の概要

保健医療福祉分野の事業者がプライバシーマークを取得するには、JIS Q 15001 に基づき、事業者（以下、「医療機関等」という）が保有する個人情報を保護する為の方針、体制、計画、実施、監査及び見直しを含むマネジメントシステムを構築・運用して申請する。

具体的な内容は、医療機関等で取り扱う診療録、処方伝票、検査依頼伝票、検査結果報告書、看護記録、レセプト、介護記録等の個人情報を含む保護対象を特定し、リスク分析を行い、患者や利用者（以下、「患者等」という）から個人情報の取扱いについての同意をもらい、適切な安全管理のもとに同意の範囲内で利用を行う。さらに教育、点検、苦情及び相談窓口の設置及び代表者による見直しにより継続的運用と是正を行う。こうしたこと

が適切に運用されるようにルール化する。単に審査の時点で要求された水準を満足していることのみではなく、個人情報保護マネジメントシステムが継続して運用されるか否かも重要な審査ポイントである。

5) 保健医療福祉分野の個人情報保護の意義

1980年のOECDプライバシー・ガイドラインの採択により、プライバシーの概念はそれまでの「一人にしておかれる権利」から「自己に関する情報の流れを自身でコントロールする権利」となった。従来、医療機関等でプライバシーというと前者で捕らえられることが多く、一人部屋にすべきとか、中待合室で前の患者等の診察内容が聞こえないようにすべき等に注意が行きがちであったが、新しい個人情報保護の概念では、さらに個人情報を患者等の同意に基づいた利用目的に添って活用していくこと、逆に同意の得られない利用目的には利用しないことが要求される。

すなわち、個人情報保護を行うということは、患者等の情報が外部にもれないようにするため、できるかぎり利用しないように消極的に管理することではなく、活用を望む本人のデータは、その同意した利用目的や利用者の範囲が守られるように安全に管理し、同意に基づいた適切な活用を可能にすることである。

こうした個人情報保護のための活動は、医療情報の開示、医療の透明化を支援し、患者等からの信頼を高め、患者等が主体的に診療に参加する、開かれた医療を実現するために、必要であり、かつ重要な活動であると考えられる。

また、個人情報保護法では、第三条で以下の基本理念を示している。

(基本理念)

第三条 個人情報とは、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

この基本理念は、患者等の個人情報を保護することは、個人情報（データあるいは物）を保護することだけではないことを明確にしている。個人情報を大切に扱うということは、その人の人格を尊重することになるのである。逆に、個人情報を粗末に扱うということは、その人の人格を否定することに繋がると考えるべきである。

保健医療福祉分野の事業者は、常にこの基本理念を念頭に、業務を遂行する必要がある。患者等の個人情報を大切に扱うことは、患者等へのサービス向上にも繋がり、それによりさらなる信頼に繋がることを認識すべきである。

6) 「医療機関の認定指針・改訂委員会」の構成

<主査>

東京大学大学院
情報学環 学際情報学府 准教授 山本 隆一

<委員>

独立行政法人労働者健康福祉機構
医療事業部 医療企画調査役 清谷 哲朗

東京工業大学 統合研究院
ソリューション研究機構 特任教授 喜多 紘一

医療法人社団康人会
適寿リハビリテーション病院 医療管理部長 公文 敦

日本情報処理開発協会
プライバシーマーク推進センター 副センター長 関本 貢

<事務局>

(財) 医療情報システム開発センター

医療情報安全管理推進部 部長 相澤 直行

プライバシーマーク付与認定審査室 室長 山口 雅敏

研究員 吉田 健一郎

1 適用範囲

A. JIS Q 15001 の要求事項

この規格は、個人情報事業の用に供している、あらゆる種類、規模の事業者に適用できる個人情報保護マネジメントシステムに関する要求事項について規定する。

事業者は、次の事項を行う場合に、この規格を用いることができる。

- a) 個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善する。
- b) この規格と個人情報保護マネジメントシステムとの適合性について自ら確認し、適合していることを自ら表明する。
- c) 組織外部又は本人に、この規格に対する個人情報保護マネジメントシステムの適合性について確認を求める。
- d) 外部機関による個人情報保護マネジメントシステムの認証／登録を求める。

B. 保健医療福祉分野としての解釈

「事業の用に供している」の「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、かつ一般社会通念上事業と認められるものをいう。個人の住所録など個人が自己のために個人情報を取り扱っている場合はこの規格の対象外であるが、営利事業のみを対象とするものではない。従って、研究のために学会発表等に患者等の個人情報を利用する場合も対象となる。

JIS Q 15001 では患者等の個人情報だけではなく、それぞれの医療機関等が雇用する個人（以下、「従業者」という）に関する個人情報や採用情報も対象としている。ただし、従業者に関する個人情報の取扱いに関しては、他の業種と大きな違いはないと考えられるので、本ガイドラインにおいては医療機関等に特有な側面、すなわち患者等の個人情報に関する取扱いに焦点を絞って解説する（看護学校等を併設している場合は、その成績情報等を含めた個人情報も管理対象となる）。

医療機関等では窓口業務等を業務委託する例があるが、この場合は派遣業務と異なり医療機関等は業務委託された従業者への指揮命令権は持たない。しかし、個人情報の取扱いは医療機関等の従業者と変わりがないことから、業務委託であっても、本マネジメントシステムに従った運用を求めることに留意すべきである（3.4.3.4及び3.4.5に関連）。

C. 最低限のガイドライン

- ① 漏れなく個人情報保護マネジメントシステムが運用されるには、本マネジメントシステムに従った運用をする従業者の範囲も明確にしておくことが必要である。例えば、役員、職員だけでなく、パート、アルバイト、派遣職員、実習生、ボランティアなどの全従業者も含まれることを明確にする。
- ② 事業の用に供している個人情報を適用対象とすることを明確にする。特に、従業者に

関する個人情報や採用情報も対象となる点に留意する（3.3.1に関連）。

2 用語及び定義

A. JIS Q 15001 の要求事項

この規格で用いる主な用語及び定義は、次による。

- 2.1 **個人情報** 個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む）。
- 2.2 **本人** 個人情報によって識別される特定の個人。
- 2.3 **事業者** 事業を営む法人その他団体又は個人。
- 2.4 **個人情報保護管理者** 代表者によって事業者の内部の者から指名された者であつて、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限をもつ者。
- 2.5 **個人情報保護監査責任者** 代表者によって事業者の内部の者から指名された者であつて、公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。
- 2.6 **本人の同意** 本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて承諾する意思表示。本人が子ども又は事理を弁識する能力を欠く者の場合は、法定代理人等の同意も得なければならない。
- 2.7 **個人情報保護マネジメントシステム** 事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。
- 2.8 **不適合** 本規格の要求を満たしていないこと。

B. 保健医療福祉分野としての解釈

カルテ等の診療記録や介護関係記録については、媒体の如何にかかわらず個人情報に該当する。また、検査等の目的で、患者等から血液等の検体を採取した場合、それらは個人情報に該当し、利用目的の特定（3.4.2.1）等の対象となる。また、これらの検査結果については、カルテ等と同様に検索可能な状態として保存されることから、開示対象個人情報（3.4.4.1）に該当し、開示（3.4.4.5）の対象となる。個人情報には診療録等の文書情報のみならず、医師と患者、医師と看護師、等の間で交わされる患者等に関する会話、病床における名前の表示、点滴、薬袋などへの名前の表示等も含まれる。これらの個人情報は開示対象個人情報（3.4.4.1）には当たらないが、プライバシーを配慮した取扱いが求められる。

3 要求事項

3. 1 一般要求事項

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善しなければならない。その要求事項は、箇条3で規定する。

B. 保健医療福祉分野としての解釈

個人情報保護マネジメントシステムは、単に個人情報を保護するためのルールを策定すればよいのではなく、それを実現するための組織体制を整え、具体的な計画（Plan）を立て、それを実施（Do）し、その状況を監査（Check）し、運用状況を評価し見直す（Act）必要がある。さらに、その評価に基づき、個人情報を保護するための方針をより確実に実現できるように、計画を練り直すという具合に、このP→D→C→Aを繰り返すことが要求されている。こうした個人情報保護のためのマネジメントシステムは、医療情報の開示の促進や、医療の透明化に寄与することから、患者等からの信頼を高め患者等が主体的に診療に参加する、開かれた医療を実現するために、必要であり、かつ重要な活動であると考えられる。また、本規格では「事業者」をマネジメントシステムの単位として想定していることから、法人全体でマネジメントシステムを構築し運用することが前提となる。

3. 2 個人情報保護方針

A. JIS Q 15001 の要求事項

事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。

- a) 事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。）。
- b) 個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること。
- c) 個人情報の漏えい、滅失又はき損の防止及び是正に関すること。
- d) 苦情及び相談への対応に関すること。
- e) 個人情報保護マネジメントシステムの継続的改善に関すること。
- f) 代表者の氏名

事業者の代表者は、この方針を文書（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）化し、従業員に周知させるとともに、一般の人が入手可能な措置を講じなければならない。

B. 保健医療福祉分野としての解釈

個人情報保護に関する事業者としての考え方や取り組みに関する宣言が「個人情報保護方針」である。医療機関等において、法を遵守し、個人情報保護のため積極的に取り組んでいる姿勢を対外的に明らかにすることが必要である。当然ながら、個人情報保護の理念及び経営責任等を明確にするため、幹部会や運営会議等の決議を経るなど一定の手続を経て定める必要がある。

C. 最低限のガイドライン

- ① 個人情報保護方針は、事業者の個人情報保護に関する取組みを内外に宣言する公式文書と位置づけられるものであることから、どのような理念で個人情報保護活動を行うのかを事業活動と関連させて明記すること。
- ② 個人情報保護方針は、文書の範囲(3.5.1)に含まれていることから、文書管理(3.5.2)に則った管理をしなければならない。当然ながら、公開している方針とマネジメントシステム文書の方針が一致していることが求められる。
- ③ 個人情報保護方針は、単に内部の規程として従業員だけに周知徹底するだけではなく、書面等に文書化し、さらに、医療機関等を利用する患者等もその内容を知ることができるようにしなければならないことから、個人情報保護方針の外部への公表や従業員への周知方法について定めておくこと。具体的には、医療機関等の受付や診察室に掲示する、診療案内や診療券などに印刷する、診療時に書面を配布し説明する、ホームページ等で公開する(トップページから直接リンクすることが望ましい)、などの方法が考えられる。
- ④ 付録4に医療機関における個人情報保護方針の例を示すとともに、以下に、要求事項のa)～f)に対応する留意点を示す。

a) 事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること

医療機関等においては、業務行為が、本来個人情報の取得そのものと考えられることができる。従って、医療機関等においてマネジメントシステムを遵守するためには、個々の従業員が十分な自覚を持って適切な個人情報の取得、利用及び提供に努めなければならない。特に、現場においては、患者等の立場は弱く、また、健康上の問題から自分自身の個人情報保護に十分配慮することができない場面にも頻繁に遭遇するので、これらの点に関して適切な配慮が行われることが期待されている。また、当然のことながら、患者等から同意をいただいた目的以外に個人情報の利用を行わないこと及びそのための措置を講じることを明確にすることが必要である。

b) 個人情報の取り扱いに関する法令、国が定める指針その他の規範を遵守すること

医療機関等においては、患者等の情報は個人情報保護法、厚生労働省のガイドラインだけでなく、医師法及び刑法134条などによっても保護されており、これらの規範を遵守するためにも、患者等の個人情報を保護するように努めなければ

ならない。

c) 個人情報の漏えい、滅失又はき損の予防並びは是正に関すること

個人情報の漏えい、滅失、き損などに関して、物理的セキュリティ（建物や部屋の強度や出入りの制限など）、組織的セキュリティ（管理者やアクセス権限の設定など）、ネットワークセキュリティ（インターネットからのアクセス制限など）、コンピュータセキュリティ（ウィルスの混入防止など）をどのように確保し、予防に努めているのかを示す必要がある。

d) 苦情及び相談への対応に関すること

個人情報に関する苦情及び相談への対応窓口を明示する。担当部署名、電話番号、e-mail アドレスなど具体的に示すこと。

e) 個人情報保護マネジメントシステムの継続的改善に関すること

医療機関等の代表者は、その個人情報保護方針の中で、マネジメントシステムを実施し、管理する責任者を定め、どの程度の頻度で監査を定期的に行い、マネジメントシステムの遵守状況を評価し、計画を見直し、改善に努める旨を明確にしなければならない。特に、こうした努力を継続的に行う姿勢が重要である。

f) 代表者の氏名

個人情報保護方針を何時誰の責任で制定したのかを明確にしておくことが重要である。医療法人等で複数の医療機関がある場合などでは、法人全体の代表者である理事長と、医療機関の責任者である病院長の連名で明示することが望ましい。また、個人情報保護方針は、文書の範囲（3.5.1）に含まれており、文書管理（3.5.2）の対象として、文書の発行及び改訂に関することを明示することが要求されているため、その制定年月日や改訂年月日を明らかにする必要がある。

D. 推奨されるガイドライン

当該方針には、a)～f)の各事項の文言をそのまま記載するのではなく、a)～f)の各事項に関する保健医療福祉分野の事業者としての特徴をふまえた内容を具体的に記載するとともに、患者等が一読して理解できる簡潔な文章であることが望ましい。

3. 3 計画

3. 3. 1 個人情報の特定

A. JIS Q 15001 の要求事項

事業者は、自らの事業の用に供するすべての個人情報を特定するための手順を確立し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

(1) 保護すべき個人情報の対象及び管理単位

個人情報 を 特定 し 管理 する 単位 は、 管理 が 有効 に 働く レベル である 必要 が ある。 一般的 には、 ファイル 単位、 帳票 名 単位、 **情報 システム 単位 等** の レベル での 特定 及び 管理 が 良い と思 われる。 例 えば、 個人情報 管理 台帳 など による 特定 及び 管理 が 考え られる。 管理 台帳 の 管理 項目 として は、 個人情報 の 名称 ・ 種類 ・ 責任 者 ・ 利用 期間 ・ 利用 目的 ・ 取得 方法 ・ 保管 方法 ・ 保管 場所 ・ アクセス 可能 者 ・ 委託 や 提供 が ある 場合 は 相手 先 ・ 廃棄 方法 ・ 開示 対象 個人情報 の 識別 ・ 保管 期間 など が ある。 医療 機関 における 個人情報 が 含ま れる 書類 の 例 を 付録 3 に 示す。

(2) 日常業務としての個人業務の特定手順

個人情報 を 管理 する ため には、 取り 扱う 全て の 個人情報 について 洗い 出し を して おく 必要 が ある。 認識 されて いない 個人情報 は、 紛失 ある いは、 改ざん され た として も、 検知 する こと が 困難 だから である。 また、 取り 扱う 個人情報 は 経営 環境 等 により 変化 する ため、 全て の 個人情報 を 日々 の 業務 活動 の 中で、 漏れ なく 特定 できる 手順 や 仕組み を 確立 して おく 必要 が ある。

(3) 個人情報の範囲

プライバシー マーク 制度 は、 個人情報 の 取扱い について JIS Q 15001 に 準拠 した マネジメント システム が 構築 されて いる こと を 審査 する ものである。 管理 する 対象 は 個人情報 と なる。 従って、 そもそも 守ら なければ なら ない 個人情報 を どこ まで と する か といふ、 個人情報 の 定義 ・ 範囲 が 重要 と なる。 プライバシー (個人情報) の 侵害 は 人 それ ぞれ に 考え 方 の 相違 が あり、 一義 的に 定義 する こと は 困難 である。 よって、 個人情報 の 定義 について は 十分 議論 し 定義 する 必要 が あり、 特に 医療 機関 等 においては 極めて 機微 な 個人情報 を 組織 全体 で 取り 扱う こと を 鑑み ると、 本 ガイド ライン では 広範 な 観点 で 個人情報 を 捉えて おく もの と する。

(4) 保管期間

個人情報 を 永久 保管 と する こと は、 適切 な 管理 が され なく なる 恐れ が あり、 リスク 回避 の 面 から 不適切 である。 特定 し た 全て の 個人情報 に 保管 期間 を 定め、 保管 期間 を 経過 し た 個人情報 を 確実に 廃棄 する か、 少なくとも 所在 を 確認 して、 今後 も 保管 が 必要 なら、 さらに 保管 を 継続 する 等 の 対応 が 必要 である。

C. 最低限のガイドライン

- ① 全て の 個人情報 の 利用 目的 等 が 把握 できる よう に 管理 台帳 等 を 作成 する など、 業務 活動 の 中 に 個人情報 を 特定 できる 手順 や 仕組み を 確立 して いる こと (定期的 な 見直し に 関する 手順 を 含む)。 特に、 新た に 個人情報 の 取り 扱い が 発生 し た 場合 や、 特定 内容 に 変化 が あった 場合 の **管理 台帳 等 へ の 反映 手順** が 明確 である こと が 必要 である。 それ には、 個人情報 の 特定 で 使用 する 様式 (個人情報 取扱 申請 書 等) や 承認 手順 が 規定 されて いる こと が 求め られる。
- ② 特定 し た 個人情報 が 「開示 対象 個人情報」 か 否か の 識別 は、 開示 等 へ の 対応 と 関連 し

ており、個人情報の適正管理の面から必要である。管理台帳等で「開示対象個人情報」の識別が可能であること。

- ③ 全ての個人情報に保管期間（見直し時期という観点でも可）を定めていること。

D. 推奨されるガイドライン

医療機関等においては取り扱う個人情報が部署ごとに異なるというよりは、一人の患者等に関連して診療情報等を部署間で共有している場合が多い。従って、個人情報を特定、管理するに当たっては、部署毎で行うというよりは医療系(看護系含む)、事務系などで各々責任者等を定め、その責任者を中心としてマネジメントシステムの開始時、新たな業務の発生時及び不要となった個人情報の確認を定期的に行うことが望ましい。また、責任者以外の従業者も特定作業に漏れがないか意識させることも重要である。

3. 3. 2 法令、国が定める指針その他の規範

A. JIS Q 15001 の要求事項

事業者は、個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し参照できる手順を確立し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

個人情報に関する法令、国が定める指針及びその他の規範を調査収集し、従業者がいつでも参照できるようにする必要がある。特に、守秘義務を定めた法律がある職種については、これらを参照可能にしておくこと。

医療機関における個人情報保護に関連する法令条文及び規範などを付録1に示す。また、保健医療福祉分野の事業者は少なくとも以下の法令、国が定める指針その他の規範を特定し、参照・維持すること。

1. 個人情報保護マネジメントシステム—要求事項（JIS Q 15001）
2. 保健医療福祉分野のプライバシーマーク認定指針
3. 「個人情報の保護に関する法律」（平成15年法律第57号）
4. 事業拠点がある自治体が制定した**事業者が守るべき**個人情報保護に関する条例
5. 「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」
6. 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」
7. 「医療情報システムの安全管理に関するガイドライン」
8. 「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」
9. 「福祉関係事業者における個人情報の適正な取扱いのためのガイドライン」
10. 「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」
11. 「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」

12. 「診療情報の提供等に関する指針」
13. 認定個人情報保護団体が作成する指針等

C. 最低限のガイドライン

- ① 前記を例にその組織で参照すべき個人情報の取扱いに関する法令、国が定める指針その他の規範を特定し（名称、バージョン、発行日、発行者、URL等）、参照し、維持する手順が定められているとともに、すべての従業者が参照可能な状態におくこと。
- ② 参照している国が定める指針その他の規範を定期的に見直し（少なくとも半年以内）、それらが改廃された場合、可及的速やかに個人情報保護マネジメントシステム文書や関連内規などにその改廃内容を必要に応じて反映する手順を定めていること。

3. 3. 3 リスク等の認識・分析及び対策

A. JIS Q 15001 の要求事項

事業者は、3.3.1 によって特定した個人情報について、目的外利用を行わないため、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

事業者は、3.3.1 によって特定した個人情報について、その取扱いの各局面におけるリスク（個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれ）を認識し、分析し、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

個人情報に関する「原因系リスク」として、不正アクセス、紛失、破壊、改ざん、漏えいなどが代表的である。この原因系リスクが発生した場合の「影響リスク」として、原因究明中の業務中断による損失、患者等に対する賠償などの直接的影響及び、社会的信用の喪失や官公庁への報告、報道機関への公表、訴訟への対応など間接的影響などが考えられる。「リスクを認識する」とは、特定した個人情報の取扱いの一連の流れ（取得・利用・廃棄）に至る各局面において、想定されるリスクを洗い出すことである。また「リスクを分析する」とは、洗い出したリスクに対する現状の対策を評価することである。

すべてのリスクをゼロにすることは不可能であるから、現状で取り得る対策を講じた上で、不十分な点を把握し（残存リスク）、認識する必要がある。現状の対応が十分でないことを認識しながら日常業務に臨むのと、そうでないのでは結果は大きく異なると理解すべきである。リスクは技術の進展や環境の変化等により常に変動するものであり、リスクの認識・分析及び対策は、一度だけ実施すれば良いものではない。医療機関等は、講じた対策が十分であるかを常に検証し見直す姿勢が必要である。

（1）リスク顕在化の予防と発生時対策

対策は一つの方法のみで十分というわけではなく、総合的な検討が求められる。特に安全性の確保に対する対策は漫然と実施するのではなく、3.3.1で特定した個人情報を施設の部門別に特定し、その部門での取得、提供、委託、利用、廃棄、処理の各場面で、リスクすなわち脅威と脆弱性を明確に評価する。そして、そのリスクに対するさまざまな予防措置を検討し、その中で医療機関等が取り得る最良の措置を講じることにより、そのリスクの顕在化を防止する。脅威としては、故意及び過失や災害等が考えられる。また、内部や外部からのものが考えられる。さらに予防対策おこなったにもかかわらずリスクが顕在化した場合は是正措置も必要である。この場合、顕在化を誰がどのレベルでチェックし、誰に連絡し、誰が対策を行うのか等、責任体制の確立が重要である。これにより、リスクが発生しても最低限の損失に止めることができる。

(2) リスク発生時の是正措置

予防措置を講じていたにもかかわらず、個人情報に対するリスクが顕在化する場合も、可能性としては残されている。そのため、是正措置も予め検討して講じる必要がある。是正措置についても、医療機関等が取り得る最善の方法を検討しておかなければならない。なお、是正のための技術的な措置は、前述の予防措置の検討に含まれる場合が多く、例えば、アクセスログの取得、バックアップの作成等はこれに当たる。また、漏えい等が起こったときの患者等への対応、関係機関、マスコミ等への対応等の規定(3.3.7)も必要である。

(3) プライバシーの観点での分析

医療機関等ではプライバシーの観点での分析も必要である。患者等の呼び出し、病室の名前の表示、お見舞い対応など現状の取扱いを把握し、有用性と保護のバランスの上に適切な対応を実施すること。

C. 最低限のガイドライン

- ① 業務フロー等を活用し、特定した個人情報について取得から利用、廃棄までのライフサイクルに応じたリスクを分析し(取扱いの各局面におけるリスク)、対策を講じる具体的な手順を確立すること(リスクの定期的見直し手順を含む)。
- ② リスクに応じた対策を明確にし、実施することとした対策はマネジメントシステム文書に反映すること。
- ③ 新たな個人情報の取り扱いが発生した場合は当然として、取り扱いに変更があった際もリスクは変化することから、漏れなくリスク分析を実施する必要がある。常に台帳等によりリスクを把握し、取り扱いに変化が生じた場合においても「個人情報取扱申請書」等により特定し、リスク分析をするとともに、その結果を台帳等に反映するための具体的な手順を規定すること(承認手順を含む)。
- ④ リスク分析により実施することとした対策が適切に実施されているか、あるいは対策が妥当かどうかを定期的に確認することは重要である。特に残存リスクについては重点

的に確認することが必要で、運用の確認（3.7.1）で用いるチェックリスト等に反映させ、定期的に確認する手順を確立すること。

3. 3. 4 資源、役割、責任及び権限

A. JIS Q 15001 の要求事項

事業者の代表者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善するために不可欠な資源を用意しなければならない。

事業者の代表者は、個人情報保護マネジメントシステムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、従業員に周知しなければならない。

事業者の代表者は、この規格の内容を理解し実践する能力のある個人情報保護管理者を事業者の内部の者から指名し、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、事業者の代表者に個人情報保護マネジメントシステムの運用状況を報告しなければならない。

B. 保健医療福祉分野としての解釈

医療機関等は、個人情報の適正な取扱いを推進し、漏えい等の問題に対処する体制を整備することが求められている。このため、個人情報の取扱いに関し、専門性と指導性を有し、医療機関等の全体を統括する組織体制・責任体制を構築し、規則の策定や安全管理措置の計画立案等を効果的に実施できる体制を構築する必要がある。

（1）個人情報保護管理者

医療機関等における代表者は理事長又は院長と考えられる（以下、「代表者」という）。代表者は内部から個人情報保護管理者を定めなければならない。個人情報保護管理者は個人情報保護に対して十分な理解を持つ必要があり、法令で守秘義務が定められている職種に従業者などから選任すべきである。

個人情報保護管理者は専任である必要はないが、個人情報保護に関する権限と責任を与えられなければならない。例えば内科医局員の一人を個人情報保護管理者に選任した場合、個人情報保護に関する権限や責任は医局長や内科部長の干渉をうけないことを定める必要がある。そして個人情報保護管理者とその権限及び責任をすべての従業員に周知しなければならない。

（2）個人情報保護監査責任者

代表者は、内部から個人情報保護監査責任者を定めなければならない。個人情報保護監査責任者は「公平、かつ、客観的な立場」にあることが求められていることから、個人情報保護管理者との兼任は許されない。また、個人情報保護管理者を牽制する立場であることから、個人情報保護管理者の直接の指揮命令下でないものが望ましい。医療機関等にお

いては看護師長クラスが適当と考えられる。

医療機関等の内部で監査の独立性と公平性が確保できない等の場合は、監査の実務を外部に委託することも可能であるが、個人情報保護監査責任者は必ず内部から選任すること。

(3) 個人情報保護に必要な資源

代表者は、個人情報保護に必要な資源を用意しなければならない。資源とは、例えば必要要員、個人情報保管庫の鍵や入退室管理のための帳簿、不要になった個人情報を破棄するためのシュレッダーやディスク消去装置などが考えられる。必要な資源は個人情報保護管理者と代表者が合議の上で決定すること。

(4) 倫理委員会の設置

医療機関等における個人情報保護は微妙な問題が数多く存在する。このような問題に対処するために可能であれば外部の有識者を含めた倫理委員会を設けるとよいであろう。個人情報保護だけでなく医療には診療上の必要性和倫理に微妙な問題が多く、そのような場面でも倫理委員会は重要である。臓器移植法やヒトゲノムの臨床研究のガイドラインなど、倫理委員会の存在や構成が指定されている法律・規範があるので、倫理委員会を構成する場合は参照することが望まれる。また診療所などの小規模な医療機関等では単独で倫理委員会を設けるのは困難であるが、例えば地区医師会などで設けるなどの工夫が推奨される。

C. 最低限のガイドライン

- ① 個人情報保護体制に係る責任者、担当者（教育、苦情及び相談受付、監査員等）の役割・責任・権限を明確に規定すると共に、個人情報保護のための体制図等を整備し、従業者へ周知すること。
- ② 個人情報保護管理者は、事業者の個人情報保護体制を公式に説明できる立場の者であること。また、個人情報保護監査責任者は個人情報保護管理者を牽制する立場であることから、職制に大きな乖離がないこと。
- ③ 代表者は、個人情報保護管理者、個人情報保護監査責任者を兼務していないこと。
- ④ 電子カルテ等の情報システムを導入している場合は、システム管理者を内部から専任すること。

D. 推奨されるガイドライン

- ① 個人情報保護管理者は、法令で守秘義務が定められている職種の従業者から選任し、医療機関等における個人情報の取扱いに関する安全管理面だけではなく、医療機関等の運営に関する全体の情報管理職であることが望ましい（例えば、副院長クラス）。
- ② 個人情報保護と医療等の必要性との間で問題が生じた場合には、外部の学識経験者を含めた倫理委員会にて審議すること。倫理委員会については本ガイドライン以外にも臓器移植、ヒトゲノムの取扱い、疫学研究などに関してのガイドライン等で規定されている。本ガイドラインでは外部の学識経験者を含める以外に特に構成等を規定しな

いが、他のガイドラインに係る医療機関等にあつてはそれぞれのガイドラインでの倫理委員会の規程を満たす必要がある。また他のガイドラインに従って構成された倫理委員会であっても、外部の学識経験者が含まれている限り、本ガイドラインで規定する倫理委員会とみなしてよい。

- ③ 情報システムの管理者特権を持つ担当者の過失や故意による事故を防止するため、複数の担当者を選任し交代で担当することが望ましい。

3. 3. 5 内部規程

A. JIS Q 15001 の要求事項

事業者は、次の事項を含む内部規程を文書化し、かつ、維持しなければならない。

- a) 個人情報特定する手順に関する規定
- b) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定
- c) 個人情報に関するリスクの認識、分析及び対策の手順に関する規定
- d) 事業者の各部門及び階層における個人情報を保護するための権限及び責任に関する規定
- e) 緊急事態（個人情報が漏えい、滅失又はき損をした場合）への準備及び対応に関する規定
- f) 個人情報の取得、利用及び提供に関する規定
- g) 個人情報の適正管理に関する規定
- h) 本人からの開示等の求めへの対応に関する規定
- i) 教育に関する規定
- j) 個人情報保護マネジメントシステム文書の管理に関する規定
- k) 苦情及び相談への対応に関する規定
- l) 点検に関する規定
- m) 是正処置及び予防処置に関する規定
- n) 代表者による見直しに関する規定
- o) 内部規程の違反に関する罰則の規定

事業者は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改定しなければならない。

B. 保健医療福祉分野としての解釈

本要求事項は、内部規定に定めるべき最低限の事項を例示したものである。内部規程には、マネジメントシステムの中核をなす基本規程、及び従業者が組織として統一的、合理的に行動し得るよう細則、様式などから構成される。この基本規程及び細則等の文書を包括して内部規程という（内部規程体系の例を付録5に示す）。内部規程は、従業者に対し十分に教育し周知がなされなければならない。従業者が遵守すべきルールは、できるかぎり

明文化することが重要である。ルールを内部規程として明文化されていないと、ルールから逸脱した取り扱いがあっても違反に問えないことを認識すべきである。

C. 最低限のガイドライン

- ① a)～o) に該当する、具体的な規定（手順書・様式を含む）を定めるとともに、必要に応じて容易に従業者が参照できる環境を整備すること。
- ② 内部規程の制定・改廃手続きについては、文書管理（3.5.2）に基づく管理規程などを制定し、一定の手続きを経て規定・維持すること。
- ③ 医療情報を扱うシステム（電子カルテシステム、医事システム、介護システムなど）を導入している場合は、厚生労働省の定める運用管理規程（「医療情報システムの安全管理に関するガイドライン」巻末参照）を制定していること。

3. 3. 6 計画書

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステムを確実に実施するために必要な教育、監査などの計画を立案し、文書化し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

(1) 計画書の作成

個人情報を保護するためには、従業者に内部規程を遵守して行動させるための教育が不可欠である。また、内部規程どおりに運用を実施しているかをチェックするための監査が必要である。教育や監査などを効果的かつ効率的に実施するためには、計画書を策定することが求められる。計画書を策定するためには、担当部署(担当者)が計画書を立案し、責任者及び代表者の承認を得る必要がある。

教育及び監査の規定の中で、計画項目を定めておくか、書式を定めておき、その内容を埋めることで必要な項目が充当されるような仕組みを取る必要がある。

a) 教育計画書に必要な項目

年間カリキュラム（テーマ、回数、時期、対象、代表者の承認欄）

個別の研修プログラム

- 研修の名称
- 研修の目的・概要、使用テキスト
- 開催日時、場所、講師
- 任意参加か否かの別、予算
- 受講対象者及び予定参加者数
- 出欠状況の確認方法、教育効果の確認方法
- 欠席者への対応方法

- 承認欄

b) 監査計画書に必要な項目

年間計画（テーマ、回数、時期、対象、代表者の承認欄）

個別計画

- 監査テーマ
- 監査対象、監査員
- 目的、範囲、方法
- スケジュール
- 承認欄

(2) 他の計画との統合

これらの教育、監査は従来から医療機関等で行われてきたものと統合して行って良いが、個人情報保護の観点が明確になるようにすること。また、日勤、夜勤、準夜勤など保健医療介護分野特有の勤務体系も配慮し教育計画を立てる必要がある。

C. 最低限のガイドライン

- ① 計画立案の時期、内容、承認方法、立案者など具体的な教育、監査計画の立案手順を定めること。
- ② 計画書は代表者が承認すること。

D. 推奨されるガイドライン

- ① 教育計画書は、対象や勤務形態を考慮し、年間カリキュラムと個別の研修プログラムに分けて立案することが望ましい。
- ② 監査計画書は、対象や部門を考慮し、当該年度に実施する全体スケジュールと個別計画に分けて立案することが望ましい。

3. 3. 7 緊急事態への準備

A. JIS Q 15001 の要求事項

事業者は、緊急事態を特定するための手順、また、それらにどのように対応するかの手順を確立し、実施し、かつ、維持しなければならない。

事業者は、個人情報漏えい、滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするための手順を確立し、かつ、維持しなければならない。

また、個人情報の漏えい、滅失又はき損が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持しなければならない。

- a) 当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くこと。

- b) 二次被害の防止，類似事案の発生回避などの観点から，可能な限り事実関係，発生原因及び対応策を，遅滞なく公表すること。
- c) 事実関係，発生原因及び対応策を関係機関に直ちに報告すること。

B. 保健医療福祉分野としての解釈

個人情報に関する事故は、100%防ぐことは困難であることを認識し、緊急事態を想定し、対処方法を事前に準備しておくことが必要である。特に、医療機関等では取り扱う個人情報の重要性が高いことから、悪用されると本人への影響が大きいことを認識して緊急事態への準備を行うべきである。

医療機関等は他の事業者と異なり、医療過誤や医療事故に対する対応策を準備している場合が多い。これらの対応策をベースに緊急事態への対応策を策定することが適切であろう。また、1) 個人情報の漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合、2) 個人情報の取扱いに関する規程等に違反している事実が生じた場合、又は兆候が高いと判断した場合等における内部及び関係機関等への報告連絡体制の整備を行うことは必須である。個人情報の漏えい等の事例は、苦情及び相談等の一環として、外部から報告される場合も想定されることから、苦情及び相談の対応体制との連携も図ることも必要である。

C. 最低限のガイドライン

- ① 緊急事態の特定手順を策定するに当たっては、リスク分析(3.3.3)の結果を基に、リスクが顕在化した際の影響度に応じたレベル分けをして対応を定めること。
- ② 関係機関への報告に際して、具体的な報告先(担当部署、電話番号など)を事前に調査しておくこと。また、保健医療分野のプライバシーマークを取得している医療機関等は(申請準備中、申請中を含む)、付与認定指定機関である(財)医療情報システム開発センターへの報告手順も規定すること。
- ③ 緊急事態への準備のため、以下のような観点で具体的手順を規定すること。
 - 1) 実態の把握と応急処置
 - 2) 緊急連絡
 - 3) 速やかに本人及び関係者に通知する
 - 4) 二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を遅滞なく公表する
 - 5) 関係機関(厚生労働省、自治体、認定個人情報保護団体等)に直ちに報告する
 - 6) 事故原因、本人への影響度、二次被害の有無等が明確になった時点で、本人への謝罪を行う
 - 7) マネジメントシステムを見直し再発防止策を検討し実施する(対策の教育を含む)
 - 8) 監査を実施し、策定した再発防止策が問題なく機能しているか確認する

D. 推奨されるガイドライン

緊急事態は予測なしに発生する場合がほとんどであることから、緊急時対応についての教育訓練に関することも規定し、定期的実施することが望ましい。

3. 4 実施及び運用

3. 4. 1 運用手順

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステムを確実に実施するために、運用の手順を明確にしなければならない。

B. 保健医療福祉分野としての解釈

医療機関等における個人情報の取り扱いは、診療部門、事務部門など部門により個人情報の種類、取得方法、利用目的、管理方法等の運用手順は異なるはずである。部門別に運用の手順を明確にすることが望ましい。また、確立した運用手順（ルール）を文書化することは、担当者が変わっても一定の個人情報保護水準を維持できることにつながり、文書化されていないことは実施されなくなる可能性がある。従って、文書化していないことは、点検(3.7) から漏れる可能性が大きく、リスクとなることを認識すべきである。

C. 最低限のガイドライン

運用手順書や細則等は、あいまいさを作らないように“5W1H1A1R”を明確にして作成すること。

who（誰が）、what（何を）、when（いつ、何時までに）、where（どこへ、どこで）、why（なぜ：理由・目的）、how（どのように：手段・方法）、Authorize（誰かの承認が必要なのかどうか）、Record（記録を残すのかどうか）。

3. 4. 2 取得・利用及び提供に関する原則

3. 4. 2. 1 利用目的の特定

A. JIS Q 15001 の要求事項

事業者は、個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない。

B. 保健医療福祉分野としての解釈

医療機関等での個人情報の利用目的は、一義的には当該個人すなわち患者等の健康の維持及び回復であるが、そのほかに一般的に以下のものがありうる。このような目的にまったく必要のない情報取得がないことを確認する必要がある。利用目的の特定に当たっては、利用目的を具体的に明確に定めることが必要である。

また、住宅地図のような公開された資料などから個人情報を取得する際においても、組織としての利用目的を特定し、特定した利用目的の範囲内で取り扱う必要がある。

(1) 患者等の健康の維持と回復など直接的な利益が目的である場合

- 患者等の診療や説明
- 患者等の家族に対する説明
- 他の医療機関へ患者等を紹介する場合、又は患者の診療にあたって、他の医療機関の医師の意見を照会する場合
- 本人の調剤を現に行っている調剤薬局や本人が受診している他の医療機関からの照会に対する返答

(2) 病院事務あるいは経営上必要な場合

- 診療報酬の請求事務
- 医療機関の経営、運営のための基礎データ
- 医療機関の上部組織への報告
- 医療監視や医療指導監査への対応

(3) 医療の向上への寄与

- 臨床治験
- 臨床研究
- 医師や看護師、その他の医療従事者の教育や臨床研修

(4) 行政上の業務への対応

- がん登録のような公益性の高い疫学調査の実施
- 厚生労働省等の医療行政等にかかわる統計・調査、サーベイランス事業
- 保健所など公的機関に対する保健医療及び公衆衛生上の報告

(5) 保険業務への対応

- 労働者災害補償保険や自賠責の手続きなど
- 一般の保険会社等からの問合せ

(6) その他問合せ

- 患者等の職場、学校等に対する情報提供
- 警察からの問合せ
- 裁判所からの問合せ

C. 最低限のガイドライン

個人情報を利用するに当たっては、特定した利用目的の達成に必要な限度において行わなければならないことから、事前に、個人情報保護管理者等の承認手順を定めること（利用目的の特定手順は個人情報の特定（3.3.1）手順と兼ねても良い）。

D. 推奨されるガイドライン

- ① マネジメントシステム作成にあたっては、当該医療機関等で過去に診療情報が利用された実績を詳細に調査し、すべて列挙すること。そして利用する情報がこれらの目的にだけ利用されていることを定期的を確認すること。また、いずれの目的にも利用されない情報取得が行われていないか定期的を確認すること。
- ② 取得情報を厚生労働省が作成した「電子保存された診療情報を交換するためのデータ項目セット（J-MIX）」のような適切で網羅的な項目セットを用いて項目別に分類し、取得された情報が既知の目的だけに利用されていることを常時確認する。また、いずれの目的にも利用されない不必要な情報取得が行われていないことを常時確認することが望ましい。

3. 4. 2. 2 適正な取得

A. JIS Q 15001 の要求事項

事業者は、適法、かつ、公正な手段によって個人情報を取得しなければならない。

B. 保健医療福祉分野としての解釈

患者等から個人情報を得る場合、十分な説明を行った上での患者等による自発的な提供を原則とし、強要をしてはいけない。また、診療情報の取得は原則として当該個人から得られるもので、適法かつ公正と考えられる。しかし、次に列挙するものは適法性、公正性に配慮を必要とする。

- 1) 意識障害・精神障害のある患者、乳幼児である患者で、情報を家族から得る場合。
- 2) 意識障害・精神障害のある救急搬送患者で、情報を（家族でない）搬送員又は当該患者の所持物等から得る場合。
- 3) 生活環境に問題がある場合で、近隣の住民及び職場の人等から情報を得る場合。
- 4) 検査等で、対象項目外で偶発的に発見した異常値や、測定上同時に得られてしまう値等。
- 5) 紹介元に検診結果を問い合わせる場合。
- 6) 本人から家族歴等の調査の目的で当該個人以外の情報を取得する場合。

これらの場合でも基本的には医療上の必要性が十分あれば、適法かつ公正と考えることができるが、特に上記の2)の所持物の検査などは、可能な限り警察等にまかせるべきで、医療の遂行上やむをえない場合をのぞいて行ってはならない。また実施する場合は、その必要性を出来る限り速やかに診療録等に記載すること。意識の回復が期待できるが、事務手続きのために名前や住所が必要と言った場合には慎むべきで、緊急に連絡先が必要な場合などに限定することが求められる。

6) に関しては個人情報保護の対象となる個人が当該患者等以外であり、問題を含んでいる。ただ、家族歴は多くの場合医療の遂行上必須であり、また個々に対象個人の同意を得ることは極めて困難であるので、取得することはやむを得ないが、その扱いには十分な

配慮が求められる。

C. 最低限のガイドライン

- ① 当該患者等以外の情報を患者等から得る場合は、その情報の必要性を十分検討した後に行い、取得された情報の利用は当該患者等の診療遂行に必須のものに限定する。また、患者等以外から当該患者等に関する情報を取得する場合も必要性を十分検討した後に行い、可能であれば患者等に取得情報の内容と取得状況の説明を行うこと。
- ② 意識障害、精神障害、乳幼児などで、説明による同意が困難な場合は、診療の遂行上の必要性を十分検討し、必要性を記録した上で情報の取得を行うこと。
- ③ 親権者、保護者が定まっている場合はその了承を可能な限り得るようにすること。

D. 推奨されるガイドライン

C. に加えて患者等に関するもの以外の情報を患者等から得る場合で、対象個人了承を得られない場合と、患者等以外から当該患者等の情報を得る場合で当該患者等の了承を得ることができない場合は、診療遂行上の必要性を複数の従業者が検証を行うこと。また、当該個人情報内容に疑義が生じた場合には、記載内容の事実に関して本人又は情報の提供を行った者に確認をとること。

3. 4. 2. 3 特定の機微な個人情報の取得、利用及び提供の制限

A. JIS Q 15001 の要求事項

事業者は、次に示す内容を含む個人情報の取得、利用又は提供は、行ってはならない。ただし、これらの取得、利用又は提供について、明示的な本人の同意がある場合及び3.4.2.6のただし書きa)～d)のいずれかに該当する場合は、この限りでない。

- a) 思想、信条又は宗教に関する事項
- b) 人種、民族、門地、本籍地（所在都道府県に関する情報を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項
- c) 勤労者の団結権、団体交渉その他団体行動の行為に関する事項
- d) 集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項
- e) 保健医療又は性生活に関する事項

B. 保健医療福祉分野としての解釈

(1) 明示的同意の原則

本項目は保健医療福祉分野での事業者と、一般の事業者とで最も大きな違いが見られる事項である。人種、民族、身体・精神障害及び保健医療に関する個人情報の取得は、保健医療福祉サービスの提供に際して必須であり、これらの取得なしには事業が成り立たない。従って、保健医療福祉分野では、これらの機微な個人情報を主として取り扱うという観点

から、個人情報の取得・利用・提供に際しては、本人からの明示的同意を原則とすべきである。明示的同意とは、インフォームド・コンセントに近い概念であり、書面による本人の同意をいう。黙示的な同意は認められない。

同意を得ずに特定の機微な個人情報を取り扱う場合は、3.4.2.6のただし書きa)～d)に該当することを確認し、診療上の理由が自明でない限り、その理由を診療録等に明記した上で取り扱うこと。その場合も利用は診療上必要な範囲内にあることに特に注意しなければならない。診療上の理由が自明とは、性生活そのものが健康上の問題である場合の性生活に関する情報や、思想、宗教、犯罪歴などが妄想などの精神症状に強く関連している場合であって、安易に3.4.2.6のただし書きa)～d)に該当すると判断してはいけない。3.4.2.6のただし書きa)～d)に該当する事例は3.4.2.6で示す。

(2) 明示的同意を得られない時

保健医療福祉分野では、人種、民族、身体・精神障害及び保健医療情報だけでなく、思想、信条、犯罪歴でさえも、精神疾患などの治療において必要な場合がある。しかしながら、これらの情報の取得に際しては、本人から明示的同意を得ることが困難な場合がある。同意を得ずにこれらの情報を取得・利用・提供するには、3.4.2.6のただし書きに該当することを確認する必要がある。また、これらは特に個人情報保護に敏感な項目であるために挙げられたことに十分注意するべきで、同意なしにこれらの情報を取得する場合は、特に利用範囲が診療の遂行のための限度内であることが前提となる点にも留意すべきである。

(3) 倫理委員会での方針決定

個人情報保護に敏感で医療の遂行上必要な情報は少なからず存在する。これらの情報取得には慎重でなければならないが、複雑な手続きを規定すると診療の遂行が困難になることもあり得る。このような情報は診療の専門性によっても異なるために一概に判断することは困難である。その組織の実態をよく把握し、日常的な情報取得で少しでも曖昧さがある場合はあらかじめ倫理委員会の方針を決めるなどの、説明可能な対策が求められる。

(4) 宗教に関する取得の事前通知と拒否

特殊な例として、宗教法人が運営する医療機関などで信者か否かを受診時に確認する場合がある。これも宗教に関する情報取得に当たるが、医療面からの必要性は乏しく、安易に取得すればプライバシーの侵害となる恐れがある。このような場合は、初診申し込み前に宗教に関する質問があることを通知し、回答を拒否できるようにするべきである。またホスピス等で、本人の宗教によってケアが異なる場合のために情報を取得する場合がある。診療上の必要性はあると考えられるが、止むを得ないかどうかは判断が困難である。このような場合にも、事前に通知し、回答を拒否できるようにしておくべきである。

C. 最低限のガイドライン

- ① 特定の機微な個人情報は、原則として取得・利用・提供をしてはならない。しかし、保健医療福祉分野では、これらの機微な個人情報を主として取り扱うという観点から、

個人情報の取得・利用・提供に際しては、本人からの明示的同意を得ることが前提となる（安易に e 項を改変・削除してはならない）。

- ② **緊急時以外で**、ただし書きを適用して本人から明示的同意を得ずに特定の機微な個人情報の取得、利用及び提供を実施する際は、事前に個人情報保護管理者の承認を得ることを規定すること（個人情報取扱申請書等により承認の記録が残ること）。

D. 推奨されるガイドライン

同意を得ずに特定の機微な個人情報を取り扱う場合は、3.4.2.6 のただし書き a)～d) に該当することを確認するが、診療上の必要性が自明でない場合、可能な限り事前に倫理委員会の了承を得る。事前に倫理委員会に諮ることが出来なかった場合は、事後に倫理委員会に報告し、その際、不適と判断された場合は当該情報を抹消する。例えば不妊外来での性生活に関する情報取得のように、診療上の必要性があって、かつ日常的に取得されることが予想される場合は、あらかじめ一括して倫理委員会等で検討を行い、必要性を明確にし、個人情報保護上の配慮を具体的に定めておく。このような過程を経た情報取得はその必要性と配慮がある前提で、個々に特別な手続きを経ずに取得することができる。

3. 4. 2. 4 本人から直接書面により取得する場合の措置

A. JIS Q 15001 の要求事項

事業者は、本人から、書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。）に記載された個人情報を直接に取得する場合には、少なくとも、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、書面によって本人に明示し、本人の同意を得なければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合、3.4.2.5 のただし書き a)～d) のいずれかに該当する場合、及び 3.4.2.6 のただし書き a)～d) のいずれかに該当する場合は、この限りではない。

- a) 事業者の氏名又は名称
- b) 個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先
- c) 利用目的。
- d) 個人情報を第三者に提供することが予定される場合の事項
 - 第三者に提供する目的
 - 提供する個人情報の項目
 - 提供の手段又は方法
 - 当該情報の提供を受ける者又は提供を受ける者の組織の種類、及び属性
 - 個人情報の取扱いに関する契約がある場合はその旨
- e) 個人情報の取扱いの委託を行うことが予定される場合には、その旨
- f) 3.4.4.4～3.4.4.7 に該当する場合には、その求めに応じる旨及び問合せ窓口

g) 本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果

h) 本人が容易に認識できない方法によって個人情報を取得する場合には、その旨

3. 4. 2. 5 個人情報を3.4.2.4以外の方法により取得した場合の措置

A. JIS Q 15001 の要求事項

事業者は、個人情報を3.4.2.4以外の方法によって取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかにその利用目的を、本人に通知し、又は公表しなければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

- a) 利用目的を本人に通知し、又は公表することによって本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- b) 利用目的を本人に通知し、又は公表することによって当該事業者の権利又は正当な利益を害するおそれがある場合
- c) 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがあるとき
- d) 取得の状況からみて利用目的が明らかであると認められる場合

3.4.2.4と3.4.2.5は密接に関連する要求事項であるため、一緒に解説する。

B. 保健医療福祉分野としての解釈

(1) 明示的同意を原則とする

”3.4.2.4 本人から直接書面により取得する場合の措置”は、本人すなわち患者等から当該患者等に関する情報を直接書面（電子的方式、磁気的方式など人の知覚によっては認識できない方式で作られる記録を含む）により取得する場合の要求事項であり、それぞれ情報取得を行う前に患者等に明示し（口頭による説明は含まれない）、同意を得る必要がある。

一方、”3.4.2.5 個人情報を3.4.2.4以外の方法により取得した場合の措置”は、委託を受けた場合、第三者として提供を受けた場合、公開情報から取得した場合等、本人から直接書面により取得する場合以外は、この要求事項が適用される。つまり本人から直接取得しているが書面で取得しなかった場合（監視カメラによる取得、口頭による取得等）も含まれることとなる。

しかし、保健医療福祉分野では、患者等から直接書面により個人情報を取得する場合より、口頭（問診等）や第三者（家族等）からだけでなく、血液等の検体、X線フィルム等の画像からも個人情報を取得する事例がある。さらに、取得・利用・提供する個人情報のほとんどが”3.4.2.3 特定の機微な個人情報の取得、利用及び提供の制限”に該当する個人情報である。従って、保健医療福祉分野における個人情報の取得は、3.4.2.4及び3.4.2.5を適用するのではなく、3.4.2.5に該当する場合でも、3.4.2.3に基づき3.4.2.4の措置に

準じた明示的同意を得ることを原則とすべきである。

(2) 患者等本人以外からの取得

以上のことから、患者等の家族、職場や近隣の人々、検診記録、紹介元、ケースワーカー、ソーシャルワーカー、ケアマネージャー、介護福祉士、ヘルパー、搬送を担当した救急隊員、警察等から情報を得る場合等、本人以外から個人情報を取得する際も原則として当該患者等に通知の上で同意を得る必要がある。しかし保健医療福祉の現場では種々の事情で本人から同意を得ることが難しいことがある。意識障害がある場合や、本人が虚偽を述べている場合などがこれに当たる。このような場合は診療の遂行上の必要性が重要で、これを確認して行わなければならない。

(3) 患者等本人に理解能力がない場合の同意

乳幼児や意識障害、精神障害で本人に理解する能力がない場合は、可能な限り親権者や保護者の了解又は同意を得る必要がある。ただし乳幼児及び小児で親権者による虐待の可能性がある場合は、その親権者の同意や了解は必要ない。この場合は当然、法律に基づいて虐待の可能性を報告しなければいけない。

親権者や保護者が複数いて、意見に相違がある場合は原則として不同意を優先する。ただし、患者等や第三者の人命にかかわる場合や、身体に重大な損傷をあたえることが予想される場合は同意を優先してよい。その場合、優先した理由を速やかに診療録等に記載すること。

(4) 包括的同意と個別同意

個別同意とは、個人情報の特定の利用を行う都度、事前に利用目的等を明示し、本人の同意を得ることである。包括的同意とは、患者等の個別の状態によらず、予想される利用目的等を列挙並びに明示し、同意を得ることである。

JIS Q 15001 の要求は、項目毎の個別の同意か、包括的な同意かについて言及はしていない。医療機関等の健全な運営も含めて診療の遂行上必要な目的に関しては、包括的な同意でよいと考えられるが、教育・研修や医学研究といった診療遂行上の必要性が薄い項目に関しては、利用時に個別に同意を得るべきである。

直接診療に用いる場合や、診療報酬請求や病棟管理などの医療機関等の経営や管理上の利用は、本来目的であり包括的な同意でよいと考えられる。しかし、お見舞い客の案内に用いる入院名簿に掲載するといった利用目的は、利用できなくても診療にも病院の経営・管理にも重大な障害とはならない。このような目的は、患者等に個別に拒否できるオプションを用意することが必要と考えられる。付録6に医療機関における同意文書の例を示す。

(5) 同意を得られない場合の措置

患者等が意識障害・精神障害・乳幼児等で本人の同意が得ることができない場合、診療の遂行上の必要性を十分検討し、その必要性を診療録等に記載した上で情報の取得を行うこと。緊急事態等で事前の記載が不可能な場合は、可及的速やかに事後に記載すること。また親権者や保護者が定まっている場合は、可能な限り親権者や保護者の同意を得ること。

ただし患者等が乳幼児又は小児等で親権者による虐待が疑われる場合は、その親権者の同意は必要ない。

(6) 利用目的の公表

医療機関等においても、3.4.2.5 に該当する事例も必ず存在することから、利用目的を広く公表することが求められる。利用目的等を広く公表することについては、医療機関等で個人情報を利用される意義について患者等の理解を得るという趣旨であり、これにより同意が得られていると判断してはならない。また、委託された場合（検体検査の受託、遠隔画像診断の受託等）であっても、3.4.2.5 のただし書き d) には該当せず、その利用目的を本人に通知又は公表しなければならない。利用目的の公表方法としては、院内や事業所内等に掲示するとともに、可能な場合にはホームページへの掲載等の方法により、なるべく広く公表する必要がある。

3.4.2.5 のただし書き c) の事例としては、公開手配を行わないで、被疑者に関する情報を、警察から被疑者の立ち回りが予想される医療機関等に限って提供された場合、医療機関等が利用目的を本人に通知し又は公表することにより、捜査活動に重大な支障を及ぼす恐れがある場合などが該当する。

利用目的の公表に当たっては、診療に関して患者情報を用いるのは当然との意識があるが、どこまでが診療か、どこまでが病院管理かなど、明確な定義が出来ない場合もある。そのため、患者等の個人情報が何に利用されているのかを具体的に示しておくのが望ましい。例えば、「ご家族への病状説明に利用します」、「診療報酬の請求に利用します」など、これまで暗黙の内に当然の利用目的としていたものに関しても、明文化しておけば、患者等の理解をより得やすくなるであろう。付録7に医療機関における個人情報の利用目的文書の例を示す。

C. 最低限のガイドライン

- ① 保健医療福祉分野における個人情報の取得は、特定の機微な個人情報を取得することから、本人から直接書面で取得する場合以外でも、“本人から直接書面で取得する場合”の措置に準じた明示的同意を得ることを原則とすることを明確にすること。
- ② 個人情報を取得する場面（時期、対象）により同意を得るための手順や通知内容（利用目的等）は異なるはずである。a)～h)の事項を本人に通知し、明示的同意を得る手順を業務毎に規定する。例えば、職員（募集時、採用時等）、患者（入院、外来等）、利用者（健診時、介護サービスの開始時、入所時等）、看護学生（募集時、入学時等）など。
- ③ 同意は、本人の署名、同意欄へのチェック、ウェブサイト上での同意ボタンの押下などの明示的な方法により、本人の意思が確認できることが必要となる。
- ④ ホームページで登録フォーム等を利用して個人情報を取得する場合は、安全対策（SSL等により暗号化等）を講じると共に、本要求事項（3.4.2.4）を満たす内容を通知し同

意を得ること。

- ⑤ 意識障害、精神障害、乳幼児など本人に理解能力がない場合で、親権者や保護者が定まっている場合は可能な限り親権者や保護者に提示し同意を得ること。
- ⑥ 緊急時以外で、ただし書きを適用して同意なしに本人から直接書面により個人情報を取得する場合の承認手順を規定すること。
- ⑦ 以下に取得時、3.4.2.4 の要求事項に則った患者等に明示する内容の留意点を示す。
 - d)、e) については、事例がない場合でも省略せずに”・・・することはない”などと明示することが適切である。
 - a) 医療機関等の名称と代表者の氏名。医療法人の場合は、理事長と病院長の連名が望ましい。
 - b) 医療機関等の個人情報保護管理者の氏名又は職名と所属及び連絡方法。苦情及び相談の連絡先が異なる場合にはそれも記載。
 - c) 3.4.2.1 で特定した利用目的のなかで、診療目的及び医療機関等の健全な管理のためのものを挙げる。さらにこれらの項目のうち、特定の目的に限って患者等が拒否した場合に利用しないものがある場合はその項目。また、以下の項目についても配慮することが望ましい。
 - 列挙した利用目的の中で利用時に個別に同意を得るか、同意が得られない場合はその目的で利用しないもの
 - 列挙した利用目的の中で法律に基づくもの
 - 列挙した利用目的の中で公益性が強く、初診時の了解を持って取得及び利用に同意したこととする項目。さらにこれらの項目のうち、特定の目的に限って患者等が拒否した場合に利用しないものがある場合はその項目
 - d) 以下については診療の必要上、第三者に個人情報を提供する場合があることを明示する。
 - 患者等への医療の提供のため、他の医療機関等との連携を図ること
 - 患者等への医療の提供のため、外部の医師等の意見・助言を求めること
 - 患者等への医療の提供のため、他の医療機関等からの照会があった場合にこれに応じること
 - 患者等への医療の提供に際して、家族等への病状の説明を行うこと
 - e) 外注検査のように、契約を締結した外部機関への情報の提供の有無と、委託業務の概要（事業者名である必要はない）。
 - f) 開示・訂正等に応じる旨及び問い合わせ窓口。開示を求める方法と費用、及び開示を拒否する場合の理由。訂正を求められた場合に応じる条件。一括して削除を求められた場合に要求に応じない条件。（医師法、医療法、療養担当規則等で規定された保存期間など。）
 - g) 当該医療機関等が診療の遂行上（サービスの提供上）、必要と認め、患者等が

情報の利用又は提供を拒否した場合には、診療（サービス）が十分行われ
ない可能性があること。

h) 「本人が容易に認識できない方法により個人情報を取得する」とは、
例えばホームページによる cookie やウェブ・ビーコン情報の取得等が
挙げられるが、その場合には、当該方法により個人情報を取得している旨
及び取得する個人情報の内容を開示することが求められる。

⑧ 3.4.2.5 の要求事項に則った利用目的を公表する手順を定めること。

D. 推薦されるガイドライン

緊急時等で事前に同意を得ることができなかつた場合や、個人情報の取
り扱いについて十分な理解ができない患者等も想定されることから、患
者等が落ち着いた時期に改めて説明を行ったり、診療計画書、療養生活の
手引き等の医療サービス提供に係る計画書等に個人情報に関する取扱い
方法を記載するなど、患者等が個人情報の利用目的を理解できるよう
配慮することが望ましい。

3.4.2.6 利用に関する措置

A. JIS Q 15001 の要求事項

事業者は、特定した利用目的の達成に必要な範囲内で個人情報を利用し
なければならぬ。特定した利用目的の達成に必要な範囲を超えて個人情
報を利用する場合は、あらかじめ、少なくとも、3.4.2.4 の a)～f) に示す
事項又はそれと同等以上の内容の事項を本人に通知し、本人の同意を
得なければならない。ただし、次に示すいずれかに該当する場合は、
この限りではない。

- a) 法令に基づく場合
- b) 人の生命、身体又は財産の保護のために必要がある場合であつて、
本人の同意を得ることが困難であるとき
- c) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要があ
る場合であつて、本人の同意を得ることが困難であるとき
- d) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の
定める事務を遂行することに対して協力する必要がある場合であつて、
本人の同意を得ることによって当該事務の遂行に支障を及ぼすおそれ
があるとき

B. 保健医療福祉分野としての解釈

診療情報の利用を原則としてあらかじめ同意を得た範囲に限定するもの
である。ただし、本人が虚偽を申し立てている可能性が強い場合で、診
療の遂行上の必要性が高い情報である場合も本人の同意なく情報を取
得し利用することができるが、本人が虚偽を申し立てていると判断
した理由及びその情報が診療の遂行上必要である理由を診療録等に記
載するこ

とが必要。

ただし書き a) ～ d) に基づき、本人の同意を得る必要はない事例を以下に示す。

a) 法令に基づく場合

- 医療法に基づく立入検査、介護保険法に基づく不正受給者に係る市町村への通知、児童虐待の防止等に関する法律に基づく児童虐待に係る通告等、法令に基づいて個人情報を利用する場合
- 感染症予防法による保健所への報告や児童虐待防止法による報告
- 警察や検察等の捜査機関の行う刑事訴訟法第 197 条第 2 項に基づく照会（同法第 507 条に基づく照会も同様）は、相手方に報告すべき義務を課すものと解されている上、警察や検察等の捜査機関の行う任意捜査も、これへの協力は任意であるものの、法令上の具体的な根拠に基づいて行われるものであり、いずれも「法令に基づく場合」に該当すると解されている。

b) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき

- 意識不明で身元不明の患者について、関係機関へ照会する場合
- 意識不明の患者の病状や重度の痴呆性の高齢者の状況を家族等に説明する場合
- 意識不明で身元不明の患者について、関係機関へ照会したり、家族又は関係者等からの安否確認に対して必要な情報提供を行う場合
- 大規模災害等で医療機関に非常に多数の傷病者が一時に搬送され、家族等からの問い合わせに迅速に対応する場合等で、本人の同意を得るための作業を行うことが著しく不合理である場合
- 児童・生徒の治療に教職員が付き添ってきた場合についても、児童・生徒本人が教職員の同席を拒まないのであれば、本人と教職員を同席させて、治療内容等について説明を行うことができる
- 報道機関や地方公共団体等を経由して、身元不明の患者に関する情報が広く提供されることにより、家族等がより早く患者を探しあてることが可能になると判断できる場合
- 急病その他の緊急時に、付添者が患者の血液型や家族の連絡先等を医師や看護師等に提供する場合

c) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

- 健康増進法に基づく地域がん登録事業による国又は地方公共団体への情報提供
- がん検診の精度管理のために地方公共団体又は地方公共団体から委託を受けた健診機関に対する精密検査結果の情報提供
- 児童虐待事例についての関係機関との情報交換
- 医療安全の向上のため、院内で発生した医療事故等に関する国、地方公共団体又は

第三者機関等への情報提供のうち、氏名等の情報が含まれる場合

- 不登校児童生徒の問題行動について、児童相談所、学校、病院等の関係機関が連携して対応するために、当該関係機関等の中で当該児童生徒の情報を交換する場合

d) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

- 国等が実施する、統計報告調整法の規定に基づく統計報告の徴集（いわゆる承認統計調査）及び統計法第8条の規定に基づく指定統計以外の統計調査（いわゆる届出統計調査）に協力する場合
- 災害発生時に警察が負傷者の住所、氏名や傷の程度等を照会する場合等、公共の安全と秩序の維持の観点から照会する場合

C. 最低限のガイドライン

- ① 本措置を実施するための承認手順を規定すること（個人情報取扱申請書等により承認の記録が残ること）。事例がないなら、恣意的運用を防ぐ意味からもその旨を明確にし、禁止することが望ましい。
- ② 特定した利用目的の範囲外の利用に該当するかどうかの判断に迷う場合は、管理者の承認を求めることを規定すること。
- ③ 緊急時以外で、ただし書きを適用して同意なしに特定した利用目的の達成に必要な範囲を超えて個人情報を利用する場合の承認手順を規定すること。

D. 推奨されるガイドライン

- ① 法令による利用であってもその利用を通知しておくことが望ましい。
- ② 学会発表等で匿名化して利用する場合であっても、事前に本措置に則った明示的同意を得ることが望ましい。
- ③ 緊急避難的利用の場合も、事後にその利用を通知しておくことが望ましい。

3. 4. 2. 7 本人にアクセスする場合の措置

A. JIS Q 15001 の要求事項

事業者は、個人情報を利用して本人にアクセスする場合には、本人に対して、3.4.2.4の a)～f) に示す事項又はそれと同等以上の内容の事項、及び取得方法を通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

- a) 3.4.2.4の a)～f) に示す事項又はそれと同等以上の内容の事項を明示又は通知し、既に本人の同意を得ているとき
- b) 個人情報の取扱いの全部又は一部を委託された場合であって、当該個人情報を、そ

の利用目的の達成に必要な範囲内で取り扱うとき

- c) 合併その他の事由による事業の承継に伴って個人情報が提供され、個人情報を提供する事業者が、既に3.4.2.4のa)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき
- d) 個人情報が特定の者との間で共同して利用され、共同利用者が、既に3.4.2.4のa)～f)に示す事項又はそれと同等以上の内容の事項を明示又は通知し、本人の同意を得ている場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき
 - － 共同して利用すること
 - － 共同して利用される個人情報の項目
 - － 共同して利用する者の範囲
 - － 共同して利用する者の利用目的
 - － 共同して利用する個人情報の管理について責任を有する者の氏名又は名称
 - － 取得方法
- e) 3.4.2.5のただし書きd)に該当するため、利用目的などを本人に明示、通知又は公表することなく取得した個人情報を利用して、本人にアクセスするとき
- f) 3.4.2.6のただし書きa)～d)のいずれかに該当する場合

B. 保健医療福祉分野としての解釈

(1) 明示的同意を原則とする

個人情報を本人から直接取得せずに、公開情報や第三者から取得し、本人に対して電話、郵便、メール等によりアクセスをする場合の措置である。医療機関等では、入院時等に患者等から第三者（家族・親類等）の連絡先を記入してもらい（3.4.2.4以外による取得）、これにより患者等の健康状態等を家族や親類等に問い合わせる場合等（本人にアクセス）が想定される。

また、ただし書きに該当する事例としては、b) 健診業務の委託、介護相談窓口の委託など、c) 医療機関等の事業の継承など、d) 地域間、法人間での診療情報等の共有・連携などが想定されるが、いずれの場合であっても保健医療情報を取り扱う場合は、個人情報取得時に3.4.2.4の措置に準じた明示的同意を得ることを原則とすべきである。

(2) 委託される場合

個人情報の取り扱いを委託される場合は、本要求事項のただし書きb)に該当し、本人からの同意を不要とされている。しかし、健診業務の委託のように保健医療情報という特定の機微な個人情報を取り扱うこと及び本人と直接面談する機会があることから、本人から明示的同意を得ること。労働安全衛生法に基づく健診を委託された場合であっても、委託された事業者から見れば3.4.2.6のただし書きa)には該当せず、また、d)にも該当

しない（学童検診は除く）と理解すべきである。

（３）明示的同意を得る方法

健診業務等を委託された場合の明示的同意を得る方法としては、１）受診票あるいは別紙に 3.4.2.4 で規定された事項を明示し、受診票の同意欄あるいは不同意欄にチェックしてもらう。２）受診案内の際など、事前に 3.4.2.4 で規定された内容の文書を郵送等で明示し、内容について同意の上、来院してもらうなどが考えられる（この場合でも同意の記録が残るようにすることが望ましい）。

C. 最低限のガイドライン

- ① 本措置を実施するための承認手順を規定すること（個人情報取扱申請書等により承認の記録が残ること）。事例がないなら、恣意的運用を防ぐ意味からもその旨を明確にし、禁止することが望ましい。
- ② 保健医療情報等の特定の機微な個人情報の取り扱いを委託される場合は、できるかぎり本人から明示的同意を得ること。
- ③ **緊急時以外で**、ただし書きを適用して同意なしに個人情報を利用して本人にアクセスする場合の承認手順を規定すること。

3. 4. 2. 8 提供に関する措置

A. JIS Q 15001 の要求事項

事業者は、個人情報を第三者に提供する場合には、あらかじめ本人に対して、取得方法及び 3.4.2.4 の a) ～d) の事項又はそれと同等以上の内容の事項を通知し、本人の同意を得なければならない。ただし、次に示すいずれかに該当する場合は、この限りではない。

- a) 3.4.2.4 又は 3.4.2.7 の規定によって、既に 3.4.2.4 の a) ～d) の事項又はそれと同等以上の内容の事項を本人に明示又は通知し、本人の同意を得ているとき
- b) 大量の個人情報を広く一般に提供するため、本人の同意を得ることが困難な場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又はそれに代わる同等の措置を講じているとき
 - － 第三者への提供を利用目的とすること
 - － 第三者に提供される個人情報の項目
 - － 第三者への提供の手段又は方法
 - － 本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること
 - － 取得方法
- c) 法人その他の団体に関する情報に含まれる当該法人その他の団体の役員及び株主に
関する情報であって、かつ、法令に基づき又は本人若しくは当該法人その他の団体
自らによって公開又は公表された情報を提供する場合であって、b) で示す事項又は

それと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき

- d) 特定した利用目的の達成に必要な範囲内において、個人情報の取扱いの全部又は一部を委託するとき
- e) 合併その他の事由による事業の承継に伴って個人情報を提供する場合であって、承継前の利用目的の範囲内で当該個人情報を取り扱うとき
- f) 個人情報を特定の者との間で共同して利用する場合であって、次に示す事項又はそれと同等以上の内容の事項を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき
 - － 共同して利用すること
 - － 共同して利用される個人情報の項目
 - － 共同して利用する者の範囲
 - － 共同して利用する者の利用目的
 - － 共同して利用する個人情報の管理について責任を有する者の氏名又は名称
 - － 取得方法
- g) 3.4.2.6 のただし書き a)～d) のいずれかに該当する場合

B. 保健医療福祉分野としての解釈

民間保険会社等の求めに応じて診断書や意見書を作成する場合、学校や職場からの病状問い合わせ、警察等からの問い合わせ、医学教育及び研修への利用、外部評価機関の評価のための診療情報の閲覧などであらかじめ同意を得ていない場合がこの項に相当する。行政機関による医療監視や裁判所の命令による利用、感染症予防法等による情報提供は法令に基づくためにならざるも同意は必要としないが、公益目的による除外は慎重に判断しなければならない。当該個人情報の提供がおこなわれなければ公益を大きく損なう場合だけに限定するべきである。

患者等が意識障害、精神障害、乳幼児等で、同意を得られない場合がある。この場合、提供する情報が、診療の遂行上の必要性及び公益性が高い場合は、本人の同意なしに提供を行うことができると考えるべきである。しかし、これらの場合でも親権者、保護者が定まっている場合は、可能な限り親権者又は保護者の同意を得る必要がある（虐待の可能性がある場合を除く）。

ただし書き f) に該当する事例は、地域の医療機関などで患者情報を共有している場合や病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人情報を特定の者との間で共同して利用することが予定されている場合などが該当する。

警察や検察等捜査機関からの照会や事情聴取は、3.4.2.6 のただし書き a) に該当し、本人の同意を得ずに個人情報を提供することができる。ただし、提供の際には、当該情報

提供を求めた捜査官の役職、氏名を確認するとともに、提供内容、対応者、任意捜査か否か等の情報を記録しておくことが望ましい。

C. 最低限のガイドライン

- ① 本措置を実施するための承認手順を規定すること（個人情報取扱申請書等により承認の記録が残ること）。
- ② 緊急時以外で、ただし書きを適用して本人の同意なしに個人情報を第三者に提供する場合の承認手順を規定すること。
- ③ 意識障害、精神障害、乳幼児など本人に理解能力がない場合で、親権者や保護者が定まっている場合は可能な限り親権者や保護者に提示し同意を得ること。ただし、親権者等による虐待が疑われる場合を除く。
- ④ 警察や検察等捜査機関からの照会や事情聴取への対応手順を定めること。
- ⑤ 健診業務の場合、法定健診項目と法定外健診項目で結果報告の手順を分けていること。健診結果（法定外健診項目）を事業者へ報告する場合は本人の同意が前提となる。

D. 推奨されるガイドライン

法令上の定めにより個人情報を提供する場合は、3.4.2.6のただし書きのa)により本人の同意は不要であるが、保健医療福祉情報という特定の機微な個人情報の提供は、注意を要するため、できるかぎり本人に説明し、同意を得ておくことが望ましい。しかし、同意が得られない場合には、説明を行ったが拒否された旨を記録しておくこと。

3. 4. 3 適正管理

3. 4. 3. 1 正確性の確保

A. JIS Q 15001 の要求事項

事業者は、利用目的の達成に必要な範囲内において、個人情報を、正確、かつ、最新の状態で管理しなければならない。

B. 保健医療福祉分野としての解釈

本要求事項は、個人情報に関して誤った情報や古い情報によって個人の利益が侵害されることを防ぐため、利用目的に応じて必要な範囲において、正確かつ最新の状態で個人情報を管理することを求めるものである。特定された個人情報に関し正確性に対するリスクを認識し、その対策をルール化することが求められる。データの誤りは、誤った指示、誤処理、誤操作、機器等の故障等によっても発生するので、その原因を除去することにより防止しなければならない。次に正確性の確保に関する留意ポイントを示す。

(1) 入力時のチェック

情報システムへの入力時、確定操作前に入力データに誤りがないか、転記ミスがないか

を十分チェックする習慣及びチェックできるシステムにする必要がある。

(2) 変更の時間的ズレによる正確性の喪失

記録の遅れ、あるいは住所・姓名等の変更が迅速に反映されないため、正確性が喪失される場合がある。住所変更、保険証区分等の変更や診療録等の記載の訂正に対して誰が変更を行えるのか、またその変更や訂正に対する履歴はどのように管理するのかをルール化する必要がある。

(3) システムによる正確性確保とその検証

情報システムは指示書に基づく処理、データのタイムスタンプ、件数チェック、運用の自動化等により正確性が確保される。また処理結果の確認、実施記録の保管、指示書とオペレーションログの検証等が行われ正確性が検証される。

(4) 情報システムの技術的対策

- 用語・コードのマスターの種別あるいはバージョン管理を適正に行うこと
- 患者名により各データの所在管理が確実におこなわれる機構をもつこと
- 住所や保険区分等の変更があった場合に変更が可能でなお変更履歴が残ること
- 入力確定操作後は変更が出来ない機構であること

(5) 管理規程の整備

- 運用管理（データ利用、ジョブ処理、ファイル取扱、機器操作等）
- 入出力管理（入力処理、出力処理、本人確認方法、記録事項変更確認方法、誤データ更新方法等）
- データ管理（データ保管、バックアップ、保管期間・廃棄等）
- 委託先管理（自施設と同じ管理レベルの正確性の確保を委託先に要求する）

C. 最低限のガイドライン

- ① 正確性を損なうとどのようなリスクがあるのか、その発生可能性と発生した場合の重大性を評価し、予防対策及び発生時の対応策を定めること。3.3.3のリスク分析で実施することが適切である（分析の視点は正確性と安全性とは分けて行うこと）。
- ② 正確性の確保に関する具体的措置は、個人情報の媒体により異なるので（紙媒体、電子媒体等）取り扱いの方法毎に適切な対策を規定し実施すること。以下に規定すべき最低限の留意点を示す。
 - 個人情報の保管期間を定める手順（3.3.3に関連）
 - 個人情報のバックアップの手順（媒体の保管方法を含む）
 - 個人情報の入力誤り防止に関するチェックの手順
 - 患者等の取り違え防止に対する対策（特に、郵送先の誤りを防止する対策）
 - 個人情報の授受時における確認・記録の手順

D. 推奨されるガイドライン

- ① 論理的にありえない入力を行った時は、警告を発生する機能をシステムとして付加することが望ましい。特に正確性を要するデータやインデックスは2重化が望ましい。
- ② 確実に本人が署名を行ったことを確認することが必要な場合は、電子署名の手段によりデータの正確性をデジタル的に確認できるシステムの導入を推奨する。
- ③ データの前後関係を明らかにすることが必要なデータに対しては、証拠性のあるシステムによるタイムスタンプを付ける等の時刻管理を行うことが望ましい。
- ④ 個人情報の内容の正確性、最新性を確保するため、委員会等において、具体的なルールを策定したり、技術水準向上のための研修の開催などを行うことが望ましい。
- ⑤ アクセスログ等の情報システムに関する記録の正確性を確保するため、時刻情報は標準時刻と一致させておく仕組みを導入することが望ましい。

3. 4. 3. 2 安全管理措置

A. JIS Q 15001 の要求事項

事業者は、その取り扱う個人情報のリスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要、かつ、適切な措置を講じなければならない。

B. 保健医療福祉分野としての解釈

(1) 安全管理のために必要かつ適切な措置

「適切な措置」という意味は、脅威が発生した場合の損失や平常時の対策状況に対する社会的評価を配慮して、経済的に実行可能な最良の技術及び運用方法の適用に配慮することである。その為には3.3.3で認識したリスク及びその対策を技術的に配慮した管理規程の作成、及びそれに基づいた運用が必要である。

また、漏えい、滅失、き損の防止、その他の個人情報の安全管理のため、組織的、人的、物理的及び技術的安全管理措置を講じなければならない。その際、本人の個人情報が漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人情報の取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。なお、その際には、個人情報を記録した媒体の性質に応じた安全管理措置を講ずること。特に、施設全体及び個人情報取扱場所への入退に関する情報を記録し確認することは物理的安全管理のための基本である。少なくとも最初に開錠した時刻・人、最後に施錠した時刻・人を記録する手段を確立すること。

(2) 内部の脅威に対する抑制

一般的に、個人情報の漏えい事例は内部のものによって行われることが多いので、医療施設でもその脅威に対する対策が必要である。特に内部のものが安全性を脅かす誘惑にかられないようにするためにも、アクセスログを取っていることや個人認証を行っていることを周知させるような明確な規制が有効である。

(3) 一覧機能、検索機能、コピー機能の制限

特に患者等のデータを一覧表として表示できる機能、患者名等から診療データを検索できる機能のアクセス制限や表示データ等のFD等へのコピー制限機能が重要である。また、アクセス可能者が、患者等からの同意の得られた範囲で運用できるための機能が必要となる。

(4) 紙データや検体の授受を含めた管理

コンピュータ内のデータのみでなく、記入用紙あるいは出力用プリント・オーダ伝票あるいは診療録等の紙データの閲覧及び移動時の取扱いも管理規程を定め、入退出者を監視したり、第三者に覗き見されるような不用意な場所への放置や、搬送時の安全対策により紛失や第三者への漏えいを防止しなければならない。

また、臨床検査等を外部へ依頼する際も、検体等やレポートの授受に関する安全対策について委託業者も含めた形で管理規程を定めておく必要がある。

(5) 個人用コンピュータの管理

医師等が自己の研究用又は診療の必要から、パーソナルコンピュータに個人情報をデータベース化している場合も禁止するか、適正運用管理の為のルール化を行っておく必要がある。個人情報（診療情報等）の持ち出しについては、原則として禁止することが望ましい。

(6) 廃棄時の安全性

個人情報の漏えい事例には、破棄時の漏えいが多くみられることから、廃棄にあたっては、電子ファイルの場合は二重書き消去、あるいは、個人情報が打ち出された紙の場合は破砕処理あるいは溶解処理などによって、破棄されたデータが他者に流出することのないよう留意することが必要である。個人情報を取り扱った情報機器を廃棄する場合についても、記憶装置内の個人情報を復元不可能な形に消去して廃棄すること。特に、処方箋の廃棄については、管理者の承認の下に行うことが法令で求められていることから、具体的な廃棄の記録を残すことは重要である。

また、医療機関等で発生する点滴ボトル（ラベルに個人情報の記載有り）等の廃棄に際しても、個人情報が判読できないように確実に破砕されることを確認すること。廃棄業務を委託する場合には、これらのことを委託契約において明確に定めること。

(7) プライバシーへの配慮

受付での呼び出しや、病室・居室における患者等の名札の掲示などについては、取り違え防止など業務を適切に実施する上で必要と考えられるが、プライバシー保護の重要性にかんがみ、患者等の希望に応じて一定の配慮をすることが望ましい。

C. 最低限のガイドライン

- ① 安全性を損なうとどのようなリスクがあるか、その発生可能性と発生した場合の重大性を評価して対策を立てること。3.3.3のリスク分析で実施することが適切である（分析の視点は正確性と安全性とは分けて行うこと）。

- ② 情報システムを利用する場合は、厚生労働省の「医療情報システムの安全管理に関するガイドライン」（巻末参照）に則った運用管理規程を整備する必要がある。また、医療情報の保管・処理を受託する事業者は、経済産業省の「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」に準拠した体制を整備すること。
- ③ 情報システム等のメンテナンスを外注する際は、契約により安全性を担保すること（3.4.3.4に関連）。特に、外部からのリモートアクセスによるメンテナンス（リモートメンテ）を許可する場合は、その際の手順を規定すること（メンテナンス開始時や終了時の確認や記録、承認など）。
- ④ 個人情報に対する安全性の確保のための具体的対策を規定すること。すなわち、誰が何時どのように行うのか具体的手順を定める（5W1H1A1Rの観点）。安全性の確保のための対策として下記のような留意点が上げられる。関係するものを選択し規定すること。

I 組織的安全管理

- 1) 入退館（室）管理（来訪者・面会者への対応、記録・確認など）
- 2) 個人情報の搬送・移動時の対策（紛失・盗難予防、授受の記録など）
- 3) 法人全体の情報システム構成を俯瞰できるネットワーク図等の整備
- 4) 個人情報や可搬型パソコン等の持ち込み／持ち出し時の安全管理
- 5) 情報システムのリモートメンテナンス時の安全管理措置
- 6) OSのデフォルトの設定を残さない（Administrator等のIDを使わない）
- 7) 従業員の採用・異動・退職等に伴う、ID・パスワードの管理手順（登録・変更・廃棄）

II 物理的安全管理

- 1) 個人情報の取扱・保管場所（サーバ室等）へのアクセス制御（制限機構と記録・確認など）
- 2) 個人情報の記録媒体の保管場所の安全管理（施錠など）
- 3) 外部記憶媒体（FD,CD,USBメモリ等）の管理（パスワード、暗号化、個体識別など）
- 4) 機器・装置の物理的な保護についての対策（盗難、破壊、破損、漏水、火災、停電、地震等）
- 5) クリアデスク、クリアスクリーン
- 6) 個人情報毎（紙、電子媒体、情報機器）の廃棄手順（記録）
- 7) 電子カルテ等の業務システムとインターネットの併用時の安全対策（原則として物理的に分離する）

III 技術的安全管理

- 1) ネットワークの安全対策（専用線、VPN、ファイアウォール、IDSなど）
- 2) 情報システムへのアクセスにおける利用者の識別と認証（ID,パスワード）。パスワードは、2ヶ月毎の変更、8バイト以上の可変長の文字列が望ましい。
- 3) 職種毎の適切なアクセス制限

- 4) アクセスログの取得と定期的な確認
 - 5) 不正ソフトウェア対策（ファイル交換ソフト、ウィルス、パッチ当てなど）
 - 6) 無線LANを利用する場合の安全管理措置
- ⑤ 個人情報を取り扱うシステムとインターネットは、物理的分離を原則とする。しかし物理的分離が困難な場合は、業務上の必要性を明確にし（責任者の承認を含む）、少なくとも以下のすべての対応を実施すること（個人情報を取り扱うシステムとブラウザ等のインターネットアプリケーションを同一端末上で稼働できないことが原則）。
- 1) リスク分析を実施し、リスクに対する対策の実施と残存リスクを把握
 - 2) ファイアウォール等による外部からの脅威への対策
 - 3) L3スイッチ等による内部からの漏出脅威への対策
 - 4) 不適切な運用の抑止及び追跡のためアクセスログの記録・解析（誰が、いつ、誰の情報に、どのようなアクセスをしたか等の詳細な情報を記録し、定期的な記録の確認を行う）を定期的又はリアルタイムで実施し、異常なアクセスがあったときは警告を発生し、ネットワークを切断する機能等を付加する
 - 5) 論理的分離ポリシー及び機器のパラメータ設定を記録し、担当者が変わってもポリシーが維持されることを担保する

D. 推奨されるガイドライン

- ① 医療に関わる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人または組織は、平成17年3月に厚生労働省より公表された「医療情報システムの安全管理に関するガイドライン」（以下、「安全管理GL」という）に準拠した安全管理措置が求められている。この「安全管理GL」への準拠性を第三者が客観的に評価する制度として、医療情報システム安全管理評価制” Program of Rating Evaluation for Medical Information System Safety control (プレミス PREMISs)”がある。この評価制度を受審することが推奨される。
- ② 不正ソフトウェアを自動的に監視し、活性化しない機構を備えることが望ましい。
- ③ 秘密鍵等のシステム内での保管は、ハードウェアセキュアモジュールへの格納が望ましい。

3. 4. 3. 3 従業員の監督

A. JIS Q 15001 の要求事項

事業者は、その従業員に個人情報を取り扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該従業員に対し必要かつ適切な監督を行わなければならない。

B. 保健医療福祉分野としての解釈

医療機関等は、3.4.3.2の安全管理措置が図られるよう、従業員に対し必要かつ適切な

監督を行わなければならない。なお、「従業者」とは、医療資格者のみならず、当該医療機関等の指揮命令を受けて業務に従事する者すべてを含むものであり、また、雇用関係のある者のみならず、理事、派遣労働者、ボランティア等も含むものである。

医療法第15条では、医療機関の管理者には、勤務する医師等の従業者の監督義務が課せられていることを認識すべきである。薬局や介護関係事業者についても、薬事法や介護保険法に基づく「指定居宅サービス等の事業の人員、設備及び運営に関する基準」、「指定居宅介護支援等の事業の人員及び運営に関する基準」、「指定介護老人福祉施設の人員、設備及び運営に関する基準」、「介護老人保健施設の人員、施設及び設備並びに運営に関する基準」及び「指定介護療養型医療施設の人員、設備及び運営に関する基準」等に同様の規定がある。

C. 最低限のガイドライン

- ① 就業期間中はもとより離職後も含めた守秘義務を明記した誓約書等を取り交わすなど、雇用契約や就業規則において、従業者の個人情報保護に関する規程を整備し、徹底を図ること。従業者との守秘義務契約は、契約書（派遣職員等の場合）や就業規則に記載があれば個別に締結することは不要。
- ② 就業規則に含まれない者（実習生、ボランティア等）からも守秘誓約書を取得すること。
- ③ 守秘義務契約及び個人情報保護マネジメントシステムに違反した際の措置を規定（就業規則の準用など）すること。
- ④ ビデオ、及びオンラインにより従業者のモニタリングを実施する場合に、その実施に関する事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて協議を行うよう規定すること。

3. 4. 3. 4 委託先の監督

A. JIS Q 15001 の要求事項

事業者は、個人情報の取扱いの全部又は一部を委託する場合は、十分な個人情報の保護水準を満たしている者を選定しなければならない。このため、事業者は、委託を受ける者を選定する基準を確立しなければならない。

事業者は、個人情報の取扱いの全部又は一部を委託する場合は、委託する個人情報の安全管理が図られるよう、委託を受けた者に対する必要、かつ、適切な監督を行わなければならない。

事業者は、次に示す事項を契約によって規定し、十分な個人情報の保護水準を担保しなければならない。

- a) 委託者及び受託者の責任の明確化
- b) 個人情報の安全管理に関する事項

- c) 再委託に関する事項
- d) 個人情報の取扱状況に関する委託者への報告の内容及び頻度
- e) 契約内容が遵守されていることを委託者が確認できる事項
- f) 契約内容が遵守されなかった場合の措置
- g) 事件・事故が発生した場合の報告・連絡に関する事項

事業者は、当該契約書などの書面を少なくとも個人情報の保有期間にわたって保存しなければならない。

B. 保健医療福祉分野としての解釈

医療機関等が、検査や保険請求業務の外注を行うことは一般的となっており、外注に際して個人情報をどのように保護するかは重要な事項である。

検査や診療報酬又は介護報酬の請求に係る事務等、個人情報の取扱いの全部又は一部を委託する場合、3.4.3.2 に基づく安全管理措置を遵守させるように受託者に対し必要かつ適切な監督をしなければならない。「必要かつ適切な監督」には、委託契約において委託者である医療機関等が定める安全管理措置の内容を契約に盛り込み、受託者の義務とすること。および業務が適切に行われていることを、定期的に確認することなども含まれる。

また、業務が再委託された場合で、再委託先が不適切な取扱いを行ったことにより、問題が生じた場合は、委託元である医療機関等や再委託した事業者が責めを負うこともあり得ることに留意すること。

(1) 委託先評価基準

個人情報保護に関する評価基準を明確にする必要がある。もちろん、プライバシーマークを取得している業者が好ましいといえるだろう。しかし、プライバシーマークを取得していない業者であっても、個人情報の保護に努めている事業者もあるので、次のような**具体的かつ客観的な評価基準**で個人情報を適切に取り扱っている事業者を委託先（受託者）として選定すること。

- 個人情報保護方針を制定している
- 個人情報保護に関する責任者及び情報システム管理者を選任している
- 委託された個人情報の取り扱い手順、安全管理方法が明文化されている
- 就業規則等で守秘義務を定めている
- 退職後も守秘義務を課している
- 個人情報保護に関する研修教育を定期的に行っている
- 情報システムのセキュリティ仕様を明示でき、その内容が十分である

(2) 委託先との契約書

委託先選定基準による評価の上、合格した事業者と委託契約を取り交わすことになる。契約内容は、a)～g)及び以下の点に留意すること。

- 契約において、個人情報の適切な取扱いに関する内容を加える（委託期間中のほ

か、委託終了後の個人情報の取扱いも含む)

- 受託者が、委託を受けた業務の一部を再委託することを予定している場合は、再委託を受ける事業者の選定において、個人情報を適切に取り扱っている事業者が選定されるとともに、再委託先事業者が個人情報を適切に取り扱っていることが確認できるよう契約において配慮する
- 受託者が個人情報を適切に取り扱っていることを定期的に確認する
- 受託者における個人情報の取扱いに疑義が生じた場合(患者等からの申出があり、確認の必要があると考えられる場合を含む。)には、受託者に対し説明を求め、必要に応じ改善を求める等、適切な措置をとる
- 委託する業務に応じ、関連する以下の通知等を遵守すること
 - 「医療法の一部を改正する法律の一部の施行について」(平成5年2月15日健政発第98号)の「第3 業務委託に関する事項」
 - 「病院、診療所等の業務委託について」(平成5年2月15日指第14号)
- 個人情報の取り扱いの外部委託(病理検査や遠隔画像診断等)に際して、後日の確認のため結果報告後も個人情報(組織標本や画像データ等)を長期間委託先に保管する場合は、その旨を委託契約書等に明記するとともに、保管期間も規定する必要がある。本人の知らない場所に、個人情報が長期間保管されることは、第三者提供及び個人情報の自己コントロール権の侵害に当たるとも考えられる。少なくとも、個人情報を委託先で保管すること、及び保管期間(廃棄手順を含む)について契約書等で明確にする必要がある。

C. 最低限のガイドライン

- ① 委託先選定基準を定める手順、及び選定基準が陳腐化しないための選定基準の定期的見直しに関する手順が定められていること。委託先選定基準は、具体的で運用可能なものであるとともに、承認手順が明確である必要がある。
- ② 委託先選定基準により選定した委託先を承認する手順、及び承認した委託先との契約締結までの具体的手順を定め、a)～g)の条項を含む契約書のひな形を準備し、契約内容に漏れがないようにすること。
- ③ 委託先を選定する基準は、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できるものでなければならない。
- ④ 個人に委託する場合であっても、委託先選定基準による選定が必要である。なお、優越的地位にある者が委託者の場合、委託先に不当な負担を課すことがあってはならない。
- ⑤ 再委託を認める場合には、委託先と同等かそれ以上の安全管理措置を実施している事業者を選定すること。
- ⑥ 医療機関等では窓口業務等を業務委託する例があるが、この場合は派遣業務と異なり

医療機関等は業務委託された従業者への指揮命令権は持たない。しかし、個人情報の取扱いは医療機関等の従業者と変わりがないことから、業務委託であっても、本マネジメントシステムに従った運用を求めること（業務委託契約書に明記するなど）。

D. 推奨されるガイドライン

- ① 基本的にプライバシーマーク取得者に対して委託を行うようにすることが望ましい。
- ② 人材派遣事業者との人材派遣契約、清掃事業者や廃棄事業者との契約、オフィスの賃貸借契約等は、個人情報の取扱いを含まない限り、本要求事項の対象外である。これらは安全管理措置(3.4.3.2)に含まれるものであり、このような事業者とは守秘義務に関する事項を盛り込んだ契約を締結することが望ましい。
- ③ 国が定めた資格が必要で、かつ法律により守秘義務を課されている者（弁護士、社会保険労務士、公認会計士、医師等）は、それだけで選定基準を満たしていると評価でき、選定基準による選定は必須ではないが、守秘義務に関する事項を盛り込んだ契約を締結することが望ましい。

3. 4. 4 個人情報に関する本人の権利

3. 4. 4. 1 個人情報に関する権利

A. JIS Q 15001 の要求事項

事業者は、電子計算機を用いて検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理、分類し、目次、索引、符合などを付すことによって特定の個人情報を容易に検索できるように体系的に構成した情報の集合物を構成する個人情報であって、事業者が、本人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の求めのすべてに応じることができる権限を有するもの（以下、3.4.4において“開示対象個人情報”という。）に関して、本人から利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止（以下、“開示等”という。）を求められた場合は、3.4.4.4～3.4.4.7の規定によって、遅滞なくこれに応じなければならない。ただし、次のいずれかに該当する場合は、開示対象個人情報ではない。

- a) 当該個人情報の存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの
- b) 当該個人情報の存否が明らかになることによって、違法又は不当な行為を助長し、又は誘発するおそれのあるもの
- c) 当該個人情報の存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの
- d) 当該個人情報の存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その

B. 保健医療福祉分野としての解釈

「開示対象個人情報」は、原則として個人情報保護法でいう「保有個人データ」と同様の概念であるが、保有個人データと異なり、消去までの期間は問わない。

保健医療福祉分野で取り扱うカルテ等の諸記録には、検査結果のような客観的なデータもあれば、それに対して医師等が行った主観的な判断や評価も書かれている。これら全体が患者等個人に関する情報に当たるものであるが、あわせて、当該診療録を作成した医師等の側からみると、自分が行った判断や評価を書いているものである。従って、診療録等に記載されている情報の中には、患者等と医師等双方の個人情報という二面性を持っている部分もあることに留意が必要である。ただし、診療録等の全体が患者等の開示対象個人情報であることから、本人から開示の求めがある場合に、その二面性があることを理由に全部又は一部を開示しないことはできない。

ただし書き a) ～ d) に該当する事例は次の通りである。医療機関等では a) 及び d) などが該当すると考えられる。特に、要人等の診療情報の有無などもただし書きに該当し、開示対象個人情報ではない。

- a) の場合とは、例えば、児童虐待の被害者の支援団体が、家庭内暴力の加害者（配偶者又は親権者）及び被害者（配偶者又は子）を本人とする個人情報を持っている場合などをいう。
- b) の場合とは、例えば、いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人情報を持っている場合や、不審者、悪質なクレマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人情報を保有している場合などをいう。
- c) の場合とは、例えば、製造業者、情報サービス事業者等が、防衛に関する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人情報を保有している場合や、要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合などをいう。
- d) の場合とは、例えば、警察からの捜査関係事項照会や捜査差押令状の対象となった事業者が、その対応の過程で捜査対象者又は被疑者を本人とする個人情報を保有している場合などをいう。

C. 最低限のガイドライン

- ① 個人情報に関する権利は、患者等の個人情報だけでなく従業者の個人情報も同様な対応が求められるため、従業者に対しても 3.4.4.2～3.4.4.7 の要求事項に対応した手続きを定めること。

- ② ただし書きを適用し、開示対象個人情報としない場合の承認手順を規定すること（「個人情報取扱申請書」等により承認の記録が残る）。

D. 推奨されるガイドライン

ただし書きに該当する可能性のある個人情報についての開示の可否については、医療機関等の内部に設置する倫理委員会等において検討した上で速やかに決定することが望ましい。

3. 4. 4. 2 開示等の求めに応じる手続

A. JIS Q 15001 の要求事項

事業者は、開示等の求めに応じる手続として次の事項を定めなければならない。

- a) 開示等の求めの申し出先
- b) 開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式
- c) 開示等の求めをする者が、本人又は代理人であることの確認の方法
- d) 3.4.4.4又は3.4.4.5による場合の手数料（定めた場合に限る。）の徴収方法

事業者は、本人からの開示等の求めに応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

事業者は、3.4.4.4又は3.4.4.5によって本人からの求めに応じる場合に、手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内において、その額を定めなければならない。

B. 保健医療福祉分野としての解釈

開示等に関して、受付窓口、請求のための様式、開示等の求めに応じる範囲（代理人等）、手数料の額等の具体的手続きを定める必要がある。判断項目・判断基準、対応スケジュール、本人確認の方法等についても定め、開示申し込み窓口には適切な対応が出来る従業員を配置すること。窓口は専用でなく、その他の相談業務の窓口と兼ねても良い。手数料の額は抑止的であってはならず、それに応じる上で必要な通信費などの実費を勘案して合理的であると認められる範囲内でその額を定めなければならない。

開示等については、本人のほか、①未成年者又は成年被後見人の法定代理人、②開示等の求めをすることにつき本人が委任した代理人により行うことができる。

開示の求めを行い得る者から開示の求めがあった場合（代理人等）、原則として本人に対し開示対象個人情報の開示を行う旨の説明を行った後、開示の求めを行った者に対して開示を行うものとする。代理人等からの求めがあった場合で、①本人による具体的意思を把握できない包括的な委任に基づく請求、②開示等の請求が行われる相当以前に行われた委任に基づく請求が行われた場合には、本人への説明に際し、開示の求めを行った者、及び開示する開示対象個人情報の内容について十分説明する必要がある。

手数料を徴収できるのは、”3.4.4.4 開示対象個人情報の利用目的の通知”及び”3.4.4.5 開示対象個人情報の開示”に係る場合のみである。

当該本人の開示対象個人情報が多岐にわたり、データ量が膨大であるなど、全体の開示等が困難又は非効率な場合は、本人の意思を尊重しつつ、本人に過去の受診の状況、病態の変化等の概要を説明するなど、本人が開示等の求めを行う情報の範囲を特定できるよう配慮すること。

開示手続きは、以下の点に留意しつつ開示対象個人情報の開示の手続を定めること。

- 請求のための様式、代理人等開示の求めに応じる範囲、応じない場合の判断基準・承認手順、対応スケジュール等の具体的手続き、本人（又はその代理人）確認の方法等
- 開示等の求めの方法は書面によることが望ましいが、患者等の自由な求めを阻害しないため、開示等を求める理由を要求することは不適切
- 開示等の求めがあった場合、主治医等の担当スタッフの意見を聴いた上で、速やかに開示対象個人情報の開示等をするか否か等を決定し、これを開示の求めを行った者に通知する
- 開示対象個人情報の開示を行う場合には、日常の医療サービス提供への影響等も考慮し、本人に過重な負担を課すものとならない範囲で、日時、場所、方法等を指定することができる

C. 最低限のガイドライン

- ① 開示等の求めに応じる手順を、具体的に規定すること（受付窓口、請求のための様式、本人確認、手数料の額、対応スケジュール、承認手順等）。
- ② 以下のような開示等の求めをすることができる代理人の範囲を明確にしておくこと。
 - －未成年者又は成年被後見人の法定代理人
 - －開示等の求めをすることにつき本人が委任した代理人
 - －患者が成人で判断能力に疑義がある場合は、現実に患者の世話をしている親族、及びこれに準ずる者（診療情報の開示）
- ③ 従業者への対応手続きも規定すること。

D. 推奨されるガイドライン

開示の判断・スケジュール等は標準的なものを明示することが望ましい。

3. 4. 4. 3 開示対象個人情報に関する事項の周知など

A. JIS Q 15001 の要求事項

事業者は、取得した個人情報が開示対象個人情報に該当する場合は、当該開示対象個人情報に関し、次の事項を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合

を含む。)に置かなければならない。

- a) 事業者の氏名又は名称
- b) 個人情報保護管理者（若しくはその代理人）の氏名又は職名，所属及び連絡先
- c) すべての開示対象個人情報の利用目的[3.4.2.5のa)～c)までに該当する場合を除く。]
- d) 開示対象個人情報の取扱いに関する苦情の申し出先
- e) 当該事業者が個人情報の保護に関する法律（平成15年法律第57号）第37条第1項の認定を受けた者（以下，“認定個人情報保護団体”という。）の対象事業者である場合にあっては，当該認定個人情報保護団体の名称及び苦情の解決の申し出先
- f) 3.4.4.2によって定めた手続

B. 保健医療福祉分野としての解釈

開示対象個人情報について、その利用目的、開示、訂正、利用停止等の手続の方法、及び利用目的の通知又は開示に係る手数料の額、苦情の申出先等について、少なくとも院内や事業所内等への掲示、さらにホームページ等によりできるかぎり明らかにするとともに、患者等からの要望により書面を交付したり、問い合わせがあった場合に具体的内容について回答できる体制を確保する必要がある。

開示対象個人情報に該当する限り、3.4.2.4～3.4.2.8によりa)～f)の事項を本人に通知している時であっても、家族等から開示等を求められることもある得るため、この要求事項に従い本人の知り得る状態においておく必要がある。付録8に医療機関における開示対象個人情報の周知に関する文書の例を示す。

C. 最低限のガイドライン

- ① 開示対象個人情報について、a)～f)の事項を院内や事業所内等への掲示、ホームページ等により本人の知る得る状態に置くこと。
- ② 患者等からの要望があった場合は、遅滞なく回答できる手順を確保すること。

3.4.4.4 開示対象個人情報の利用目的の通知

A. JIS Q 15001の要求事項

事業者は、本人から、当該本人が識別される開示対象個人情報について、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならない。ただし、3.4.2.5のただし書きa)～c)のいずれかに該当する場合、又は3.4.4.3のc)によって当該本人が識別される開示対象個人情報の利用目的が明らかな場合は利用目的の通知を必要としないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

B. 保健医療福祉分野としての解釈

本要求事項は、開示対象個人情報に関する周知事項として、医療機関等が 3.4.4.3 の c) に基づいて公表している利用目的について、本人から利用目的の通知を求められた場合に応じること、及び応じない場合について定めたものである。本人が、公表されている利用目的だけでは医療機関等が取り扱う開示対象個人情報の利用目的を十分に把握できない場合に該当する。利用目的を個別にできるかぎり詳細に特定し（”・・・の治療のため・・・に利用する” など）本人に通知することが望まれる。利用目的の特定・通知に際して手数料がかかる場合は、その手数料に対して実費を勘案して合理的であると認められる範囲内において、その額を定めることが出来る。

本人から求められた開示対象個人情報の利用目的の通知、開示、訂正等、利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨本人に通知する場合は、本人に対して、その理由を説明するよう努めなければならない。本人に対して理由を説明する際には、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが望ましい。

C. 最低限のガイドライン

- ① 本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。
- ② ただし書きを適用し、利用目的の通知を求められながら対応できない場合の承認手順を規定すること（「個人情報取扱申請書」等により承認の記録が残る）。

3.4.4.5 開示対象個人情報の開示

A. JIS Q 15001 の要求事項

事業者は、本人から、当該本人が識別される開示対象個人情報の開示（当該本人が識別される開示対象個人情報が存在しないときにその旨を知らせることを含む。）を求められたときは、法令の規定によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、当該開示対象個人情報を書面（開示の求めを行った者が同意した方法があるときは、当該方法）によって開示しなければならない。ただし、開示することによって次の a)～c) のいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

- a) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- b) 当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
- c) 法令に違反することとなる場合

B. 保健医療福祉分野としての解釈

本人から、当該本人が識別される開示対象個人情報の開示を求められたときは、本人に

対し、書面の交付による方法等により、遅滞なく、当該個人情報を開示しなければならない。しかし、a)～c)のいずれかに該当する場合は、その全部又は一部を開示しないことができる。個々の事例への適用については個別具体的に慎重に判断することが必要である。

a) の場合とは、患者等の本人の状況等について、家族や本人の関係者が医療機関等に情報提供を行っている場合に、これらの者の同意を得ずに本人自身に当該情報を提供することにより、本人と家族や関係者との人間関係が悪化するなど、これらの者の利益を害する恐れがある場合や、症状や予後、治療経過等について本人に対して十分な説明をしたとしても、本人に重大な心理的影響を与え、その後の治療効果等に悪影響を及ぼす場合などをいう。

b) の場合とは、同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ちゆかなくなる等、業務上著しい支障を及ぼす恐れがある場合などをいう。

開示の方法は、書面の交付又は求めを行った者が同意した方法によること。また、求められた開示対象個人情報の全部又は一部について開示しない旨を決定したときは、本人に対し、遅滞なく、その旨を通知しなければならない。また、本人に通知する場合には、本人に対してその理由を説明するよう努めなければならない。

法令の規定により、開示対象個人情報の開示について定めがある場合には、当該法令の規定によるものとする。ただし書き a)～c) に該当するため、開示できない旨を本人に対して理由を説明する際には、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが望ましい。

C. 最低限のガイドライン

- ① 開示のための具体的手順（様式、承認手順）を規定すること。
- ② ただし書きを適用し、開示対象個人情報の開示をしない場合の承認手順を規定すること（「個人情報取扱申請書」等により承認の記録が残る）。
- ③ 開示対象個人情報である診療情報の開示に当たっては、厚生労働省の「診療情報の提供等に関する指針」の内容にも配慮すること。
- ④ 法令上の義務について同意が得られない場合には、説明を行ったが拒否された旨を記録しておくことを規定すること。

D. 推奨されるガイドライン

- ① 開示の対象となる開示対象個人情報は、自己を本人とする個人情報である。従って、本人以外の者が識別される開示対象個人情報は、本要求事項に基づいて開示の求めがなされても、その対象には含まれない。その場合の開示に際しては本人以外の個人情報を削除するか判別できない状態にすることが望ましい。

- ② 委託を受けて取り扱っている個人情報、開示対象個人情報には当たらない。しかし、本人から開示の求めがあった時は、その旨を説明すると共に、当該個人情報の開示の権限を有する委託元を明らかにするなどの対応を行うことが望ましい。

3. 4. 4. 6 開示対象個人情報の訂正、追加又は削除

A. JIS Q 15001 の要求事項

事業者は、本人から、当該本人が識別される開示対象個人情報の内容が事実でないという理由によって当該開示対象個人情報の訂正、追加又は削除（以下、この項において“訂正等”という。）を求められた場合は、法令の規定によって特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該開示対象個人情報の訂正等を行わなければならない。また、事業者は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正等を行わない旨の決定をしたときは、その旨及びその理由を、本人に対し、遅滞なく通知しなければならない。

B. 保健医療福祉分野としての解釈

訂正又は削除を行うのは、当該情報が誤っていることが判明した場合に限ることが必要である。要求されたからといって客観的な事実で診療上必要な事項は変更や削除はできない。所見などについては、明確な誤りでない限り訂正はできない。なお、「削除」と、3.4.4.7の「消去」とは一般に区別無く用いられることが多いが、「消去」とは、開示対象個人情報を消してその効力を失わせることで（使えなくなる）、個人情報の内容が事実でない部分を削除して利用を続ける「削除」とは異なる。

訂正等、利用停止等又は第三者への提供の停止が求められた開示対象個人情報の全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明することが必要である。

開示対象個人情報の訂正等にあたっては、訂正した者、内容、日時等が分かるように行われなければならない。当然ながら字句などを不当に変える改ざんは、行ってはならない。

C. 最低限のガイドライン

本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。

3. 4. 4. 7 開示対象個人情報の利用又は提供の拒否権

A. JIS Q 15001 の要求事項

事業者が、本人から当該本人が識別される開示対象個人情報の利用の停止、消去又は第三者への提供の停止（以下、この項において“利用停止等”という。）を求められた場合は、

これに応じなければならない。また、措置を講じた後は、遅滞なくその旨を本人に通知しなければならない。ただし、3.4.4.5のただし書きa)～c)のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。

B. 保健医療福祉分野としての解釈

本人から開示対象個人情報の利用停止等を求められた場合は、原則として応じることを定めている。つまり、個人情報保護法（第27条）と異なり、開示対象個人情報の取り扱いに手続き違反がない場合であっても、本人から利用停止等の求めがなされたときには、原則として応じることが求められている。本要求事項は、開示対象個人情報が適切に取り扱われていても、開示対象個人情報の存在自体を消去したいという場合にも応じるという、プライバシー保護に重点を置いた規定と言える。

しかし、保健医療福祉分野の個人情報は、法令で保存期間が定められているものも多く存在するので、利用停止等の求めがあっても法令上の義務を優先する必要がある。法令上の義務について同意が得られない場合には、説明を行ったが拒否された旨を記録しておくことが求められる。

利用又は提供の拒否を求められた開示対象個人情報の全部又は一部について、これらの措置を行わない旨決定した場合、本人に対するその理由の説明に当たっては、書面により示すことを基本とする。その際は、苦情の対応体制についても併せて説明すること。

C. 最低限のガイドライン

- ① 本人への対応手順及び回答内容（求めに応じない場合を含む）に関する承認手順を定めること。
- ② ただし書きを適用し、利用目的の通知を求められながら対応できない場合の承認手順を規定すること（「個人情報取扱申請書」等により承認の記録が残る）。
- ③ 法令上の義務について同意が得られない場合には、説明を行ったが拒否された旨を記録しておくことを規定すること。

3. 4. 5 教育

A. JIS Q 15001 の要求事項

事業者は、従業者に、定期的に適切な教育を行わなければならない。事業者は、従業者に、関連する各部門及び階層における次の事項を理解させる手順を確立し、かつ、維持しなければならない。

- a) 個人情報保護マネジメントシステムに適合することの重要性及び利点
- b) 個人情報保護マネジメントシステムに適合するための役割及び責任
- c) 個人情報保護マネジメントシステムに違反した際に予想される結果

事業者は、教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

研修の頻度や方法等を内部規程で定め、それを遵守するものとする。採用時研修と定期研修では、もちろん内容は異なるであろうし、マネジメントシステムの制定や改定に伴う運用研修も行うことが必要である。全ての従業員が受講できるように年間計画を定め、人事記録上での取扱いも明記しておく方が効果的であると考えられる。特に、全ての従業員に個人情報保護に関する理念の理解と内部規程の遵守を求めること。また、医師や看護師等の守秘義務規定が設けられている職種については、その遵守を徹底することが重要である。研修プログラムを採用時と定期に分けて、回数・時期・内容・対象者を含めて具体的に策定すると効果的である。テキストは個人情報保護マネジメントシステム文書が基本となるが、市販されているものを利用することも可能である。

派遣労働者についても、「派遣先が講ずべき措置に関する指針」（平成11年労働省告示第138号）において、「必要に応じた教育訓練に係る便宜を図るよう努めなければならない」とされていることを踏まえ、個人情報の取扱いに係る教育研修の実施に配慮する必要がある。また、窓口業務等を業務委託した場合であっても、派遣労働者と同様に、業務委託された従業員に対する教育研修の実施に配慮すること（3.4.3.4に関連）。

C. 最低限のガイドライン

- ① 組織としての個人情報保護に対する理解度は、最下層の従業員のレベルとなることを認識し、全ての従業員にa)～c)の内容を含む適切な教育を定期的（最低年1回）に実施すること。
- ② 教育に際しては、個人毎に出欠を取り、欠席者にも漏れなく教育をすることが必要（欠席者のフォローアップ手順を定める）。また、教育対象を明確にし、従業員全員に教育を実施した記録を残すとともに承認手順を定めること。
- ③ 感想文やアンケート、小テストなどを実施することにより従業員の理解度を把握し、教育を受けたことを自覚させる仕組みを取り入れること（不合格者のフォローアップ手順を定める）。また、従業員の理解度等により、必要に応じて教育内容の見直しを図ること。

3. 5 個人情報保護マネジメントシステム文書

3. 5. 1 文書の範囲

A. JIS Q 15001 の要求事項

事業者は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。

- a) 個人情報保護方針
- b) 内部規程
- c) 計画書
- d) この規格が要求する記録及び事業者が個人情報保護マネジメントシステムを実施する上で必要と判断した記録

B. 保健医療福祉分野としての解釈

個人情報保護方針と 3.3.5 にある内部規程、及びそれを具体化した計画、記録類が、これらに当たる。印刷物として保管しておくのもよいが、記載内容の変更に備えて加除式にしておくことが望ましい。また、イントラネット上でいつでも従業員が参照可能な状態にしておくのも役立つと思われる。

情報セキュリティマネジメントシステムや品質マネジメントシステム等の他の目的で作成された文書を、個人情報保護マネジメントシステムの一部として参照し利用する際は、文書管理の対象から外れないように、それらの文書を個人情報保護マネジメントシステムの中で規定し、必要に応じ参照できるようにしておくこと。

C. 最低限のガイドライン

- ① 文書体系図等を作成し、個人情報保護マネジメントシステムとして管理すべき範囲が明確（様式、記録も含める）であること。
- ② マネジメントシステム文書を必要に応じて従業員が参照できる環境を整備すること。
- ③ 個人情報保護マネジメントシステム以外の目的で作成された文書を、参照し利用する際は、それらの文書を個人情報保護マネジメントシステムの中で規定し、参照しておくこと。

3. 5. 2 文書管理

A. JIS Q 15001 の要求事項

事業者は、この規格が要求するすべての文書（記録を除く。）を管理する手順を確立し、実施し、かつ、維持しなければならない。

文書管理の手順には、次の事項が含まなければならない。

- a) 文書の発行及び改訂に関すること
- b) 文書の改訂の内容と版数との関連付けを明確にすること
- c) 必要な文書が必要なときに容易に参照できること

B. 保健医療福祉分野としての解釈

庶務や総務部門あるいは各部門に文書管理責任者を定め、要件となる文書管理を行うこととする。各種の規程や実際の運用にかかわる文書（情報開示の請求書やその処理過程の記録等）も含めて適切な管理を行う必要がある。

C. 最低限のガイドライン

- ① 文書の管理について、少なくとも a)～c)を含む、具体的な管理ルール（発行、改訂、保管、破棄等）を定めること。
- ④ 各文書に目次や見出しラベルを付けるなど閲覧性を高める工夫をし、従業員が必要な文書を容易に参照することができるように努めること。

3. 5. 3 記録の管理

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録を作成し、かつ、維持しなければならない。
事業者は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

記録は紙媒体である必要はなく、医療機関等において運用しやすい合理的な方法で作成すると良い。医療機関等は、必要な記録を特定し、保管方法、保管期間、及び廃棄方法等についての手順を確立し、実施し、維持しなければならない。「必要な記録を特定し」とは、記録自体も個人情報である可能性があるから、とりあえず何でも記録として残すという姿勢ではなく、その必要性を判断すべきであるという意味である。

記録は、必要な時にすぐに検証できるように維持しておかなければならない。本要求事項で必要とする記録には以下のものが含まれる。

- a) 個人情報の特定に関する記録
- b) 法令、国が定める指針その他の規範の特定・維持に関する記録
- c) 個人情報に関するリスクの認識、評価及び対策に関する記録
- d) 教育・監査計画に基づき実施した教育・監査の実施記録
- e) 緊急事態（個人情報が漏えい、滅失又はき損をした場合）への対応に関する記録
- f) 個人情報の取得・利用・提供に関する記録（従業員、患者等からの同意の記録等）
- g) 個人情報の適正管理に関する記録（入退記録、アクセスログなど）
- h) 本人からの開示等の求めに関する記録
- i) 文書管理に関する記録
- j) 苦情及び相談への対応に関する記録
- k) 点検に関する記録
- l) 是正処置及び予防措置に関する記録

- m) 代表者の見直しに関する記録
- n) 例外事項を適用した際の承認の記録

C. 最低限のガイドライン

- ① 記録の管理について具体的な管理ルール（作成、保管、破棄等）を定めること。
- ② 法令で保存義務のある記録（診療録、処方箋等）は分けて管理し、廃棄の際には廃棄記録を残すこと（付録2に保健医療分野の保存義務に関する法令等を示す）。

3. 6 苦情及び相談への対応

A. JIS Q 15001 の要求事項

事業者は、個人情報取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順を確立し、かつ、維持しなければならない。

事業者は、上記の目的を達成するために必要な体制の整備を行わなければならない。

B. 保健医療福祉分野としての解釈

医療機関等は、個人情報の取扱いに関する苦情及び相談の適切かつ迅速な処理に努めなければならない。また、苦情及び相談の適切かつ迅速な処理を行うにあたり、苦情及び相談の対応窓口の設置や対応の手順を定めるなど必要な体制の整備に努めなければならない。

大規模な医療機関等の場合には、総合窓口等で受け付けるように定め、小規模な医療機関等では受診受付での対応とするのが適切である。情報開示申込窓口と同じとする場合もあるが、大規模医療機関等であれば、別にする方が客観性が保てると思われる。

代表電話の受付者に対して、苦情及び相談の担当者を告知するとともに、受診受付で苦情及び相談等の申し出があれば、相談室等へ案内し内容を担当者が聞き取る必要がある。担当者がいない場合の対応も予め策定しておく。もちろん、開示等の請求も受け付けられるようにしても良い。

C. 最低限のガイドライン

- ① 苦情及び相談の窓口を明確にするとともに、受付担当者を任命しておくこと。
- ② 本人に回答する内容の承認手順や、苦情及び相談の内容及び対応結果の記録及び代表者への報告手順を規定すること。
- ③ 認定個人情報保護団体の対象事業者であるときは、苦情受付時に当該団体の受付先も通知すること。

D. 推奨されるガイドライン

- ① 患者等からの苦情及び相談の対応にあたり、専用の窓口の設置や主治医等の担当スタ

ップ以外の従業員による相談体制を確保するなど、患者等が相談等を行いやすい環境の整備に努めること。

- ② 苦情対応だけでなく、患者等が疑問に感じた内容を、いつでも、気軽に問い合わせできる相談窓口機能等を確保することも必要である。
- ③ 患者等の相談は、医療サービス等との内容とも関連している場合が多いことから、個人情報取り扱いに関し、患者等からの相談や苦情対応等の受付を行う窓口を設置するとともに、その窓口がサービスの提供に関する相談機能とも有機的に連携した対応が行える体制とするなど、患者等の立場に立った対応を図ることが望ましい。
- ④ 苦情及び相談の対応にあたり、専用の窓口の設置や主治医等の担当スタッフ以外の従業員による相談体制を確保するなど、本人が相談を行いやすい環境の整備に努めること。また、当該施設における苦情及び相談の対応体制等について院内や事業所内等への掲示やホームページへの掲載等を行うことで周知を図り、地方公共団体、地域の医師会や国民健康保険団体連合会等が開設する医療や介護に関する相談窓口等についても周知することが望ましい。

3. 7 点検

3. 7. 1 運用の確認

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステムが適切に運用されていることが事業者の各部門及び階層において定期的に確認されるための手順を確立し、実施し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

個人情報の取り扱いに不備がないことを、部署毎に責任者を決めて定期的に確認する手順を定めることが必要である。

運用の確認とは、組織全体として実施する監査(3.7.2)と異なり、各部門及び各階層において行われるものである。従って、一連のマネジメントシステムの実施結果を受けて行うものではなく、日常業務において気付いた点があればそれを是正及び予防していくものであるため、大げさなものである必要はない。日常において継続的に実施できることが重要。部署毎の責任者が定期的に見回ってマネジメントシステムの運用状況を確認することも良い。診察時間終了後、診察室にカルテが所定の場所に返却されずに残っていないか、検査伝票が処理されずに残っていないか、施錠忘れはないか、離席時の対処が適切か(クリアデスク、クリアスクリーンなど)などを毎日確認する。

C. 最低限のガイドライン

- ① リスク分析(3.3.3)の結果実施することとした対策についてチェックリスト等を作成

し、定期的実施状況を確認する手順を定めること。

- ② 少なくとも以下の事項の記録を残し定期的に確認する手順を確立すること。
- 最終退出時（部門での業務終了時又は交代時など）の点検（施錠確認等）
 - 入退館（室）の記録（最初に出社した人と最後に退社した人の記録）
 - 個人情報を取り扱う情報システムのアクセスログの定期的確認

3. 7. 2 監査

A. JIS Q 15001 の要求事項

事業者は、個人情報保護マネジメントシステムのこの規格への適合状況及び個人情報保護マネジメントシステムの運用状況を定期的に監査しなければならない。

事業者の代表者は、公平、かつ、客観的な立場にある個人情報保護監査責任者を事業者の内部の者から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、事業者の代表者に報告しなければならない。監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。

事業者は、監査の計画及び実施、結果の報告並びにこれに伴う記録の保持に関する責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならない。

B. 保健医療福祉分野としての解釈

監査が効果的にその目的を達成するためには、検討・評価の結果としての助言・勧告が、公正不偏かつ客観的なものでなければならない。また、監査活動そのものについても、他からの制約を受けることなく自由に、かつ、公正不偏な態度で客観的に遂行し得る環境であることが必要である。このため監査機能は、その対象となる諸活動についていかなる是正権限や責任も負うことなく、組織的に独立し、また、精神的にも客観的である必要がある。これらの内部監査における原則は、保健医療分野の業務が、専門性が高くかつ複雑であることから特に重要である。従って、監査で明らかになった不適合への対応は、「是正処置及び予防処置」で実施し、監査の延長と考えるはいけない。

当然ながら、個人情報保護監査責任者が必要に応じ「是正措置及び予防措置」の効果を確認し助言することを妨げるものではない（フォローアップ監査）。その際においても、個人情報保護監査責任者の責務は、効果の評価と支援であり、被監査部門及び代表者が決定した是正処置に対して承認や追加変更の指示は出来ないことを認識すべきである。

C. 最低限のガイドライン

- ① 個人情報保護監査責任者は、必要に応じ適切な監査員を選任し、監査計画書に従い、個人情報を取り扱う全部門に対し定期的（最低年1回）に監査を行うこと。

- ② 監査員は、原則として自己の所属する組織の監査をしてはならない（看護部を監査する場合は、看護部以外から監査員を選任するなど）。
- ③ 監査結果の報告は、個人情報保護監査責任者から直接代表者に行うこと。
- ④ 監査の実施に当たっては、事前に監査テーマに則ったチェックリスト等を作成し、漏れなく確認する手順を確立すること。
- ⑤ 代表者は、明らかになった不適合については、是正処置及び予防処置（3.8）により実施すること。

3. 8 是正処置及び予防処置

A. JIS Q 15001 の要求事項

事業者は、不適合に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を確立し、実施し、かつ、維持しなければならない。その手順には、次の事項を含めなければならない。

- a) 不適合の内容を確認する。
- b) 不適合の原因を特定し、是正処置及び予防処置を立案する。
- c) 期限を定め、立案された処置を実施する。
- d) 実施された是正処置及び予防処置の結果を記録する。
- e) 実施された是正処置及び予防処置の有効性をレビューする。

B. 保健医療福祉分野としての解釈

不適合は、点検（3.7）の結果並びに緊急事態の発生、及び外部機関の指摘等により本規格の要求を満たしていないと判断したものである。不適合の原因が特定されなければ、根本的な解決にはならず再発を防げない。被監査部門は、不適合の原因を特定した上で、再発防止のための是正処置及び予防処置を立案し、代表者の承認を受け実施しなければならない。最終的に不適合に伴うリスクは、代表者（医療法人の場合は理事長）が負うこととなる。

医療機関等は、運用の確認（3.7.1）、監査（3.7.2）又は緊急事態への準備（3.3.7）、外部機関の指摘（1.d）等により発見された不適合を改善するための手順を a）～ e）に則って定めるとともに承認、及び記録する手順・様式を整備すること。また、是正処置及び予防処置を確実に実施させるために期限を区切ることは有効であるが、不適合の内容によっては、長期にわたることもあり得る。不適合の内容に相応した期限の設定をすることも必要である。

C. 最低限のガイドライン

- ① 発見された不適合について、この要求事項により是正処置及び予防処置を実施するという関係が明確であること。

② 実施のための手順には a) ～ e) の内容が含まれているとともに、以下の点に留意していること。

- 不適合の内容を承認するのは代表者である
- 不適合の原因を特定し、是正処置及び予防処置案を立案するのは、不適合が発見された部門である
- 立案された是正処置及び予防処置案を承認（指示）するのは代表者である
- 個人情報保護監査責任者は、独立性の観点から改善案の立案・承認に関与しないことを原則とすること（有効性のレビューは除く）

3. 9 事業者の代表者による見直し

A. JIS Q 15001 の要求事項

事業者の代表者は、個人情報の適切な保護を維持するために、定期的に個人情報保護マネジメントシステムを見直さなければならない。

事業者の代表者による見直しにおいては、次の事項を考慮しなければならない。

- a) 監査及び個人情報保護マネジメントシステムの運用状況に関する報告
- b) 苦情を含む外部からの意見
- c) 前回までの見直しの結果に対するフォローアップ
- d) 個人情報の取扱いに関する法令，国の定める指針その他の規範の改正状況
- e) 社会情勢の変化，国民の認識の変化，技術の進歩などの諸環境の変化
- f) 事業者の事業領域の変化
- g) 内外から寄せられた改善のための提案

B. 保健医療福祉分野としての解釈

監査は組織の現状のルールを前提に、それが守られているかを点検するものであり、それに基づく是正も現状の枠内に止まるものである。代表者による見直し（3.9）は、それに止まらず、外部環境も考慮した上で、現状そのものを根本的に見直すことがあり得る点で、監査による是正とは本質的に異なることを理解すべきである。従って、監査報告に基づく是正のみでは JIS の要求を満たしているとは言えない。

C. 最低限のガイドライン

- ① 見直しの根拠として a) ～ g) を準備することを規定すること。
- ② 運用状況に関する報告には、事故、ヒアリハット等の発生状況や発生時の対応状況等の報告も含まれる。漏れなく報告されるようにすること。
- ③ 少なくとも代表者による見直しを年1回実施し（時期を明確にする）、その実施の記録（議事録等）を残すこと。

D. 推奨されるガイドライン

経営や運営に関する定期的な会議に報告できるように、比較的短いサイクルのプログラムも検討することが望ましい。

以上

付録 1 医療における個人情報保護に関連する法令条文及び規範など

法律：

憲法 20 条 「信教の自由」

- ① 信教の自由は、何人に対してもこれを保障する。いかなる宗教団体も、国から特権を受け、又は政治上の権力を行使してはならない。
- ② 何人も、宗教上の行為、祝典、儀式又は行事に参加することを強制されない。
- ③ 国及びその機関は、宗教教育その他いかなる宗教活動もしてはならない

刑法 35 条 「正当行為」

法令又は正当な業務による行為は、罰しない。

刑法 37 条 「緊急避難」

自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その程度を超えた行為は、情状により、その刑を減輕し、又は免除することができる。

- 2 前項の規定は、業務上特別の義務がある者には、適用しない。

刑法 134 条 「秘密漏示」

医師、薬剤師、医薬品販売業者、助産婦、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、6 月以下の懲役又は 10 万円以下の罰金に処する。

- 2 宗教、祈祷若しくは祭祀の職にある者又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときも、前項と同様とする。

(参考：上記条文に対する条文)

刑法 135 条 「親告罪」

この章の罪は、告訴がなければ公訴を提起することができない。

国家公務員法 100 条 「秘密を守る義務」

職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする。

- 2 法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表するには、所轄庁の長（退職者については、その退職した官職又はこれに相当する

官職の所轄庁の長) の許可を要する。

- 3 前項の許可は、法律又は政令の定める条件及び手続に係る場合を除いては、これを拒むことができない。
- 4 前三項の規定は、人事院で扱われる調査又は審理の際人事院から求められる情報に関しては、これを適用しない。何人も、人事院の権限によって行われる調査又は審理に際して、秘密の又は公表を制限された情報を陳述し又は証言することを人事院から求められた場合には、何人からも許可を受ける必要がない。人事院が正式に要求した情報について、人事院に対して、陳述及び証言を行わなかつた者は、この法律の罰則の適用を受けなければならない。

地方公務員法 34 条 「秘密を守る義務」

職員は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も、また、同様とする。

- 2 法令による証人、鑑定人等となり、職務上の秘密に属する事項を発表する場合においては、任命権者（退職者については、その退職した職又はこれに相当する職に係る任命権者）の許可を受けなければならない。
- 3 前項の許可は、法律に特別の定がある場合を除く外、拒むことができない。

労働安全衛生法 104 条 「健康診断に関する秘密の保持」

第 65 条の 2 第 1 項及び第 66 条第 1 項から第 4 項までに規定する健康診断の実施の事務に従事した者は、その実施に関して知り得た労働者の心身の欠陥その他の秘密を漏らしてはならない。

じん肺法 35 条の 3 「じん肺健康診断に関する秘密の保持」

第 7 条から第 9 条の 2 まで及び第 16 条第 1 項のじん肺健康診断の実施の事務に従事した者は、その実施に関して知り得た労働者の心身の欠陥その他の秘密を漏らしてはならない。

医療法 1 条の 4 「医師等の責務」

医師、歯科医師、薬剤師、**看護師**その他の医療の担い手は、第 1 条の 2 に規定する理念に基づき、医療を受ける者に対し、良質かつ適切な医療を行うよう努めなければならない。

- 2 医師、歯科医師、薬剤師、**看護師**その他の医療の担い手は、医療を提供するに当たり、適切な説明を行い、医療を受ける者の理解を得るよう努めなければならない。
- 3 医療提供施設において診療に従事する医師及び歯科医師は、医療提供施設

相互間の機能の分担及び業務の連係に資するため、必要に応じ、医療を受ける者を他の医療提供施設に紹介し、その診療に必要な限度において医療を受ける者の診療又は調剤に関する情報を他の医療提供施設において診療又は調剤に従事する医師若しくは歯科医師又は薬剤師に提供し、及びその他必要な措置を講ずるよう努めなければならない。

- 4 医療提供施設の開設者及び管理者は、医療技術の普及及び医療の効率的な提供に資するため、当該医療提供施設の建物又は設備を、当該医療提供施設に勤務しない医師、歯科医師、薬剤師、**看護師**その他の医療の担い手の診療、研究又は研修のために利用させるよう配慮しなければならない。

医療法 72 条 「秘密漏泄」

第 5 条第 2 項若しくは第 25 条第 2 項若しくは第 4 項の規定による診療録若しくは助産録の提出又は同条第 1 項若しくは第 3 項の規定による診療録若しくは助産録の検査に関する事務に従事した公務員又は公務員であつた者が、その職務の執行に関して知り得た医師、歯科医師若しくは助産婦の業務上の秘密又は個人の秘密を正当な理由がなく漏らしたときは、1 年以下の懲役又は 50 万円以下の罰金に処する。

- 2 職務上前項の秘密を知り得た他の公務員又は公務員であつた者が、正当な理由がなくその秘密を漏らしたときも、同項と同様とする。

保健師助産師看護師法 42 条の 2 「守秘義務」

保健師、看護師又は准看護師は、正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない。保健師、看護師又は准看護師でなくなつた後においても、同様とする。

診療放射線技師法 29 条 「秘密を守る義務」

診療放射線技師は、正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない。診療放射線技師でなくなつた後においても、同様とする。

救急救命士法 47 条 「秘密を守る義務」

救急救命士は、正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない。救急救命士でなくなつた後においても、同様とする。

臨床検査技師、衛生検査技師等に関する法律 19 条 「秘密を守る義務」

臨床検査技師又は衛生検査技師は、正当な理由がなく、その業務上取り扱つたことについて知り得た秘密を他に漏らしてはならない。臨床検査技師又は衛生検査

査技師でなくなつた後においても、同様とする。

理学療法士及び作業療法士法 16 「秘密を守る義務」

理学療法士又は作業療法士は、正当な理由がある場合を除き、その業務上知り得た人の秘密を他に漏らしてはならない。理学療法士又は作業療法士でなくなつた後においても、同様とする。

歯科技工士法 20 条の 2 「秘密を守る義務」

歯科技工士は、正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない。歯科技工士でなくなつた後においても、同様とする。

規範など：

ヒポクラテスの誓い

いかなる患者を訪れるときも、それはただ患者を利益するためであり、あらゆる勝手な戯れや墮落の行いを避ける。女と男、自由人と奴隷の違いを考慮しない。医に関する否とに関わらず、他人の生活についての秘密を守る。

医師の倫理（昭和 26 年 日本医師会）

第 1 章 第 3 節 疾病に関する秘密義務を守ること。

患者の権利と責任「勤務医マニュアル」（1983 年 日本病院協会）

4-4 患者の受療に対する倫理的権利として次の各項がある（カッコ内は生命倫理の原理を示す）。

- 1 医療上最適のケアを受ける権利（恩恵授受の原理）
- 2 適切な治療を受ける権利（公正の原理）
- 3 人格を尊重される権利（人権尊重の原理）
- 4 個人情報とプライバシーを保障される権利（守秘義務の原理）
- 5 医療上の情報、説明を受ける権利（真実告知の原理）
- 6 医療行為（法による許可範囲外）を拒否する権利（自己決定の原理）
- 7 関係法規と病院の諸規則などを知る権利

このうち真実の告知については、例えば、がんであることを知らせる雰囲気を見守るチームが中心となって醸成し、患者が安心立命の境地に入るようにしてから、主治医から説明を受けるようにする方法もある。

付録2 保健医療分野の保存義務に関する法令等

(1) 医師法（昭和23年法律第201号）第24条

〔診療録の記載及び保存〕医師は、診療をしたときは、遅滞なく診療に関する事項を診療録に記載しなければならない。

- 2 前項の診療録であって、病院又は診療所に勤務する医師のした診療に関するものは、その病院又は診療所の管理者において、その他の診療に関するものは、その医師において、5年間これを保存しなければならない。

(2) 歯科医師法（昭和23年法律第202号）第23条

〔診療録の記載及び保存〕歯科医師は、診療をしたときは、遅滞なく診療に関する事項を診療録に記載しなければならない。

- 2 前項の診療録であって、病院又は診療所に勤務する歯科医師のした診療に関するものは、その病院又は診療所の管理者において、その他の診療に関するものは、その医師において、5年間これを保存しなければならない。

(3) 保健師助産師看護師法（昭和23年法律第203号）第42条

〔助産録の記載及び保存の義務〕助産婦が分娩の介助をしたときは、助産に関する事項を遅滞なく助産録に記載しなければならない。

- 2 前項の助産録であって病院、診療所又は助産所に勤務する助産婦のなした助産に関するものは、その病院、診療所又は助産所の管理者において、その他の助産に関するものは、その助産婦において5年間これを保存しなければならない。
- 3 第一項によつて規定による助産録の記載事項に関しては、省令でこれを定める。

(4) 医療法（昭和23年法律第205号）

第21条

〔病院の法定人員及び施設の基準等〕病院は、厚生省令の定めるところにより、次に掲げる人員及び施設を有し、かつ、記録を備えて置かなければならない。ただし、政令の定めるところにより、都道府県知事の許可を受けたときは、この限りでない。

- 1 療養型病床群を有しない病院にあつては、厚生省令で定める員数の医師、歯科医師、**看護師**その他の従業者 1 の 2 療養型病床群を有する病院にあつては、厚生省令で定める員数の医師、歯科医師、**看護師**及び看護の補助その他の業務の従業者
- 2 各科専門の診察室
- 3 手術室

- 4 処置室
 - 5 臨床検査施設
 - 6 エックス線装置
 - 7 調剤所
 - 8 消毒施設
 - 9 給食施設
 - 10 給水施設
 - 11 暖房施設
 - 12 洗濯施設
 - 13 汚物処理施設
 - 14 診療に関する諸記録
 - 15 診療科名中に産婦人科又は産科を有する病院にあつては、分べん室及び新生児の入浴施設
 - 16 療養型病床群を有する病院にあつては、機能訓練室
 - 17 その他厚生省令で定める施設
- 2 療養型病床群を有する診療所は、厚生省令の定めるところにより、次に掲げる人員及び施設を有しなければならない。
- 1 厚生省令で定める員数の医師、歯科医師、[看護師](#)及び看護の補助その他の業務の従業者
 - 2 給水施設
 - 3 暖房施設
 - 4 機能訓練室
 - 5 その他厚生省令で定める施設
- 3 第一項第一号若しくは第一号の二又は前項第一号の規定に基づく厚生省令の規定によって定められた人員を有しない者については、政令で20万円以下の罰金の刑を科する旨の規定を設けることができる。

第22条

[地域医療支援病院の法定施設等] 地域医療支援病院は、前条第一項（第14号を除く。）に定めるもののほか、厚生省令の定めるところにより、次に掲げる施設を有し、かつ、記録を備えて置かなければならない。

- 1 集中治療室
- 2 診療に関する諸記録
- 3 病院の管理及び運営に関する諸記録
- 4 化学、細菌及び病理の検査施設
- 5 病理解剖室

- 6 研究室
 - 7 講義室
 - 8 図書室
 - 9 その他厚生省令で定める施設
- 2 [特定機能病院の法定人員及び施設の基準等] 特定機能病院は、第21条第一項（第一号、第一号の二及び第一四号を除く。）に定めるもののほか、厚生省令の定めるところにより、次に掲げる人員及び施設を有し、かつ、記録を備えて置かなければならない。
- 1 厚生省令で定める員数の医師、歯科医師、薬剤師、[看護師](#)その他の従業者
 - 2 集中治療室
 - 3 診療に関する諸記録
 - 4 病院の管理及び運営に関する諸記録
 - 5 前条第四号から第八号までに掲げる施設
 - 6 その他厚生省令で定める施設

(5) 歯科技工士法（昭和30年法律第168号）第19条

[指示書の保存義務] 病院、診療所又は歯科技工所の管理者は、当該病院、診療所又は歯科技工所で行われた歯科技工に係る前条の指示書を、当該歯科技工が終了した日から起算して2年間、保存しなければならない。

(6) 薬剤師法（昭和35年法律第146号）第28条

[調剤録] 薬局開設者は、薬局に調剤録を備えなければならない。

- 2 薬剤師は、薬局で調剤したときは、調剤録に厚生省令で定める事項を記入しなければならない。ただし、その調剤により当該処方せんが調剤済みとなったときは、この限りでない。
- 3 薬局開設者は第一項の調剤録を、最終の記入の日から3年間、保存しなければならない。

(7) 救急救命士法（平成3年法律第36号）第46条

[救急救命処置録] 救急救命士は、救急救命処置を行ったときは、遅滞なく厚生省で定める事項を救急救命処置録に記載しなければならない。

- 2 前項の救急救命処置録であつて、厚生省令で定める機関に勤務する救急救命士のした救急救命処置に関するものはその機関につき厚生大臣が指定する者において、その他の救急救命処置に関するものはその救急救命士において、その記載の日から5年間、これを保存しなければならない。

- (8) 保健医療機関及び保健医療養担当規則（昭和32年厚生省令第15号）第9条
〔帳簿等の保存〕保健医療機関は、療養の給付の担当に関する帳簿及び書類その他の記録をその完結の日から3年間保存しなければならない。ただし、患者の診療録にあっては、その完結の日から5年間とする。
- (9) 保険薬局及び保健薬剤師療養担当規則（昭和32年厚生省令第16号）第6条
〔処方せん等の保存〕保険薬局は患者に対する療養の給付に関する処方せん及び調剤録をその完結の日から3年間保存しなければならない。
- (10) 歯科衛生士法施行規則（平成元年厚生省令第46号）第18条
〔記録の作成及び保存〕歯科衛生士はその業務を行った場合には、その記録を作成して3年間これを保存するものとする。

付録3 医療機関における個人情報を含む書類の例

- 診察申込書
- 保険証
- 紹介状
- 診察券
- 予約票
- 入院申込書
- 入院療養計画書
- 診療録
- 処方せん
- 検査依頼伝票
- 検査結果報告書
 - －生化学検査
 - －生理検査
 - －超音波検査
 - －内視鏡検査
 - －放射線検査
- 看護記録
- レセプト
- 請求書／領収書
- 薬歴情報
- 退院証明書
- 退院療養計画書
- 手術管理情報
- 給食管理情報
- 行政官庁への報告のための各種届出書等

付録4 医療機関における個人情報保護方針の例

ここでは医療機関における個人情報の取扱いに関するポリシー例を示す。このポリシー例は、一般病院あるいは診療所を前提とした基本的なものであり、教育関連病院、研修指定病院などのように正規の従業者以外が患者情報にアクセスする必要のある医療施設や、研究機関附属病院のように患者情報が患者個人の診療のためだけでなく、臨床研究などを目的として利用される可能性のある施設は、こうした事項についてさらに詳細なポリシーを付加する必要がある。

当院における個人情報保護に関する基本方針

当会は、常日頃より患者さんの視点に立ち、質の高い医療の実現とよりよい患者サービスの提供を目標として、診療業務を営んでおります。患者さんの健康状態に応じて迅速に的確な医療を提供させていただくためには、患者さんに関する様々な情報が必要です。患者さんと確かな信頼関係を築き上げ、安心して医療サービスを受けていただくために、患者さんの個人情報の安全な管理は必須です。当会では下記の基本方針に基づき、個人情報保護に厳重な注意を払っております。

1. 個人情報の取扱いについて

当会は、個人情報の利用を診療及び病院の運営管理に必要な範囲に限定し、その範囲内のみ取り扱います。また、その利用目的に関しては患者さんに予めお知らせし、ご了解を得た上で利用します。本来の利用目的の範囲を超えて使用する場合は、匿名化（個人を識別できない状態に加工）して利用する場合及び法令の定めによる場合を除き、患者さんの同意なく個人情報の利用提供はいたしません。

2. 法令の遵守について

当会は、個人情報保護に関する日本の法令、国が定める指針その他の規範を遵守します。

3. 安全管理について

当会は、患者さんの個人情報への不正アクセス、紛失、破壊、改ざん、及び漏えいを防止し、安全で正確な管理に努めます。

4. 問い合わせ窓口

当会における個人情報の取扱いに関するお問い合わせは下記の相談窓口でお受け致します。
〇〇〇〇課 個人情報保護相談窓口 電話 xxx-xxx-xxxx e-mail privacy@xxxx.jp

5. 個人情報保護の仕組みの改善

当会は、JIS Q 15001 に即した個人情報保護マネジメントシステムを構築し、それに基づいて患者さんの情報を管理します。また、このマネジメントシステムは適宜見直し、継続的な改善を図ります。

平成〇〇年 4 月 1 日 制定

平成〇〇年 7 月 1 日 改訂

医療法人〇〇会 理事長 〇〇 太郎

〇〇病院 院長 〇〇 次郎

個人情報保護管理者 〇〇 三郎

*本方針は、患者さんの個人情報のみならず、当会の職員情報など、当会が取り扱う全ての個人情報についても適用します。

付録5 内部規程体系の例

個人情報保護マネジメントシステム文書・記録一覧表

001 個人情報保護方針

002 個人情報保護基本規程

1. 計画

011 個人情報保護体制図

012 個人情報保護マネジメントシステム文書一覧表

013 個人情報特定・リスク分析規定

0131 個人情報取り扱い申請書

0132 リスク評価、管理レベル基準表

0133 個人情報管理台帳

014 関連法規管理規定

0141 法令規範登録申請書

0142 法令規範台帳

015 就業規則（罰則規定）

016 個人情報保護職務権限規定

0161 役割及び責任権限一覧表

2. 実施及び運用

021 個人情報取扱規定

0210 当院における個人情報の利用目的

0211 個人情報の取り扱いに関する同意書

0212 個人情報の取り扱いに関する同意書（職員）

0213 個人情報授受管理票

0214 個人情報廃棄管理票

0131 個人情報取り扱い申請書

022 部門別業務手順規定

023 緊急事態対応規定

0231 事故報告書

0232 事故対応経過記録

3. 適正管理

031 施設入退管理規定

0311 IDカード発行・返却届出書

- 0 3 1 2 入退管理記録簿
- 0 3 2 情報セキュリティ管理規定
 - 0 3 2 1 アクセス権限一覧表
 - 0 3 2 2 ユーザ登録申請書
 - 0 3 2 3 過般型機器・媒体持ち出し・持ち込み許可願い
- 0 3 3 医療情報システム運用管理規定
- 0 3 4 電子保存システム運用管理規定
- 0 3 5 委託先管理規定
 - 0 3 5 1 機密保持契約書
 - 0 3 5 2 業務委託契約書
 - 0 3 5 3 委託先選定書（確認項目、選定基準）
 - 0 3 5 4 委託先管理シート
 - 0 3 5 5 授受確認書
 - 0 3 5 6 委託先リスト

4. 本人の権利

- 0 4 1 個人情報開示・訂正・削除規定
 - 0 4 1 0 診療情報の開示について
 - 0 4 1 1 開示・訂正・削除・利用又は提供の拒否・申請書
 - 0 4 1 2 開示・訂正・削除・利用又は提供の拒否・回答書
 - 外部文書 診療情報の提供等に関する指針（厚生労働省）

5. 教育

- 0 5 1 教育規定
 - 0 5 1 1 教育計画書
 - 0 5 1 2 教育実施記録
 - 0 5 1 3 教育実施報告書
 - 0 5 1 4 教育テキスト（試験問題、感想文、アンケート）

6. 文書管理

- 0 6 1 文書・記録管理規定
 - 0 6 1 1 文書一覧
 - 0 6 1 2 改定履歴表

7. 苦情及び相談

- 0 7 1 相談窓口受付規定

- 0711 相談窓口受付票
- 0712 相談窓口報告書

8. 点検

- 081 監査規定
 - 0811 監査計画書
 - 0812 監査実施計画書
 - 0813 監査報告書
 - 0814 改善指示書
 - 0815 改善計画書
 - 0816 改善報告書
- 082 是正・予防処置規定
 - 外部文書 指摘事項文書（外部機関）
 - 0821 是正・予防処置報告書
- 083 運用確認規定
 - 0831 運用確認チェックリスト

9. 事業の代表者による見直し

- 091 代表者による見直し規定

以上

付録6 医療機関における同意文書の例

以下の文書は、3.4.2.4 に則った同意文書の例である。患者の状態が許す限り、初診時に以下のような内容を記載した文書を手渡すか、見やすいところに掲示し、内容を理解し、同意したことを確認することが必要となる。例えば初診申し込み用紙の裏面に記載し、同意した趣旨を確認できる様式とすることが望ましい。

*当文書は診療申込書等の裏面に表示することを想定しているので氏名欄がない。

個人情報の取り扱いについて

当院では、患者様の個人情報を以下のように取り扱います。下記の内容をご確認いただき、同意の上、診察申し込みいただきますようお願い申し上げます。

1. 利用目的（詳細については別掲の「当院における個人情報の利用目的」をご参照ください）

1. 患者様へ適切な医療サービスの提供のため
2. 病院事務・管理を適切に行うため
3. 法令・行政上の業務への対応のため
4. 保険請求業務のため
5. ご家族への病状説明のため

以上の目的以外で患者様の情報を利用する場合、患者様ご本人に個別理由を説明し同意を得た上で行うものといたします。ただし、緊急の場合、治療上必要な場合等、当院が必要だと判断した場合は、利用を優先し、後ほどご説明させていただきます。

2. 個人情報の第三者提供について

患者様の個人情報は、あらかじめ患者様の同意をいただくことなく、外部に提供することはありません。ただし、以下の利用目的に該当する場合は、患者様から特にお申し出がない限り、医療サービスを提供するための通常業務として必要な範囲において、患者様の個人情報を第三者に提供する場合があります。

- (ア)医療の提供のため、他の医療機関等との連携を図ること
- (イ)医療の提供のため、外部の医師等の意見・助言を求めること
- (ウ)医療の提供のため、他の医療機関等からの照会があった場合にこれに応じること
- (エ)患者への医療の提供に際して、家族等への病状の説明を行うこと

3. 業務委託について

医療を提供するに当たり、業務の一部を外部に委託しています。委託先に対しては、契約等にて個人情報保護に関する監督を行っております。主な業務委託の内容は次の通りで

す。検査業務、医療事務関連業務、健診業務、清掃業務、情報システム管理、廃棄物処理。

4. 患者様の権利

当院の管理する全ての個人情報については、ご本人による開示請求・訂正・削除・利用停止等を求めることが可能です。個人情報相談窓口までご相談ください。

医療法人〇〇会〇〇病院 院長：〇〇 〇〇

個人情報保護管理者：〇〇 〇〇

個人情報相談窓口：99-999-9999

■個人情報の取り扱いについて

同意する

同意しない

- 万一上記の事項についてご同意をいただけない場合には、適切な医療サービスの提供に支障が出る場合がございます。
- 上記利用目的のうち、同意しがたい事項がある場合にはその旨をお申し出下さい。また、同意いただいた後でも個別に不同意の表明をすることが可能です。

付録7 医療機関における個人情報の利用目的文書の例

以下の文書は、3.4.2.5 に則った利用目的の通知・向上の例文である。見やすいところに掲示するか、ホームページ等で公表することが望ましい。

当院における個人情報の利用目的

当院は、個人情報を下記の目的で利用し、別掲の「個人情報保護方針」に基づき取り扱っております。個人情報の取扱いについてお気づきの点がありましたら、窓口まで気軽にお申し出下さい。

【医療の提供に必要な利用目的】

1. 適切な医療サービスの提供のため
2. 病院事務・管理を適切に行うため
 - －入退院等の病棟管理
 - －会計・経理
 - －質向上・安全確保・医療事故あるいは未然防止等の分析・報告
3. 法令・行政上の業務の対応のため
 - －医師賠償責任保険などに係る、医療に関する専門の団体、保険会社等への相談又は届出等
 - －第三者機関への質向上・安全確保・医療事故対応・未然防止等のための報告
4. 保険請求業務のため
 - －保険請求業務
 - －保険事務の委託
 - －審査支払機関又は保険者へのレセプトの提出
 - －審査支払機関又は保険者からの照会への回答
5. ご家族への病状説明等の適切な医療を提供するための情報提供
 - －他の病院、診療所、助産所、薬局、訪問看護ステーション、介護サービス事業者等との連携
 - －他の医療機関等からの照会への回答
 - －診療等に当たり、外部の医師等の意見・助言を求める場合
 - －検体検査業務の委託・その他の業務委託
 - －ご家族等への病状説明
 - －事業者等からの委託を受けて健康診断等を行った場合における、事業者等へのその結果の通知

【上記以外の利用目的】

1. 医療機関等の管理運営業務のうち、
 - －医療・介護サービスや業務の維持・改善のための基礎資料
 - －医師・看護師・薬剤師・検査技師・放射線技師・理学療法士・栄養士・医療事務等の学生実習への協力
 - －医師・看護師・薬剤師・検査技師・放射線技師・理学療法士・栄養士等の教育・研修
 - －症例検討・研究及び剖検・臨床病理検討会等の死因検討
 - －研究、治験及び市販後臨床試験の際は、関係する法令、指針に従う
 - －治療経過及び予後調査、満足度調査や業務改善のためのアンケート調査
 - －安全・防犯のための監視カメラによるモニタリング
2. 学会・医学誌等への発表

特定の患者・利用者・関係者の症例や事例の学会、研究会、学会誌等での報告は、氏名、生年月日、住所等を消去することで匿名化する。匿名化困難な場合は、本人の同意を得る。

○ ○ ○ ○ 病 院
院 長 医 療 太 郎
個人情報保護管理者 ○○○○

当院の個人情報保護に関するお問い合わせは以下にお願いいたします。

個人情報問い合わせ窓口：Tel 99-9999-99 e-mail:privacy@aaaa.jp

付録8 医療機関における開示対象個人情報の周知に関する文書の例

以下の文書は、3.4.4.3に則った開示対象個人情報に関する周知のための文例である。見やすいところに掲示するか、ホームページ等で公表することが望ましい。

診療情報の開示について

診療情報（個人情報）の提供、及び開示は、医療従事者の重要な責務です。当院では、診療情報を積極的に患者様に提供し、共有することによって、相互に信頼関係を築き、より質の高い開かれた医療を提供することを目指しています。

1. 診療情報の利用目的

- ① 患者様へ適切な医療サービスの提供のため
- ② 病院事務・管理を適切に行うため
- ③ 法令・行政上の業務の対応のため
- ④ 保険請求業務のため
- ⑤ ご家族への病状説明のため

上記に示した以外に、医療の質向上や医療従事者の育成を目的として、次のような利用を行う場合があります。

- ① 当院内部において行われる医学・看護学等の症例研究
- ② 当院内部において行われる院内の事故防止、及び医療の質向上のための研究
- ③ 当院内部において行われる学生の実習への協力
- ④ 外部監査機関への情報提供

2. 手続き

診療情報の開示は、原則としてご本人に開示します。予め、諸手続きが必要となりますので相談窓口にお申し出ください。ご本人以外の方が、診療情報の開示を希望される場合は、ご本人のプライバシーを尊重することから確認の手続きが必要です。いずれにしても開示できない場合は、その理由をご説明させていただきます。

開示手続きについては以下の書類が必要です

- 1) 診療情報開示申請書（相談窓口に様式が用意されています）
- 2) 本人又は代理人であることを確認できる公的文書（免許証など）

3. 費用

診療情報録の開示には別に定めた費用をご負担いただきます。詳細については相談窓口にてご確認ください。

4. 相談窓口

個人情報に関するお問い合わせは、各部署責任者又は以下の窓口をご利用下さい。また、当院は個人情報保護法（第37条第1項）による次の「認定個人情報保護団体」の対象事

業者です。第三者による解決が必要な事項については本団体にご相談ください。

認定個人情報保護団体 ○○○○○○○○

個人情報苦情対応窓口 電話 999-999-9999

○○病院 院長：○○ ○○

個人情報保護管理者：○○ ○○

個人情報相談窓口：99-999-9999

付録 9 「医療情報システムの安全管理に関するガイドライン」 抜粋

本付録は、厚生労働省が平成 22 年 2 月に公表した「医療情報システムの安全管理に関するガイドライン第 4.1 版」から医療情報システムの基本的安全管理に必要な第 6 章、及び付表 1～3 を抜粋したものである。未収裁の事項については（責任のあり方、標準化、電子保存、外部保存、スキャナ等での電子化保存など）必要に応じて以下の URL により原本を参照すること。

<http://www.mhlw.go.jp/shingi/2010/02/s0202-4.html>

6 情報システムの基本的な安全管理

情報システムの安全管理は、刑法等で定められた医療専門職に対する守秘義務等や個人情報保護関連各法（個人情報保護法、行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）、独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号））に規定された安全管理・確保に関する条文によって法的な責務として求められている。守秘義務は医療専門職や行政機関の職員等の個人に、安全管理・確保は個人情報取扱事業者や行政機関の長等に課せられた責務である。安全管理をおろそかにすることは上記法律に違反することになるが、医療においてもっとも重要なことは患者等との信頼関係であり、単に違反事象がおこっていないことを示すだけでなく、安全管理が十分であることを説明できること、つまり説明責任を果たすことが求められる。この章での制度上の要求事項は個人情報保護法の条文を例示する。

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

（従業員の監督）

個人情報取扱事業者は、その従業員に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業員に対する必要かつ適切な監督を行わなければならない。

（委託先の監督）

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

（個人情報保護法 第 20 条 第 21 条 第 22 条）

6.1 方針の制定と公表

B. 考え方

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」において、個人情報保護に関する方針を定め公表することが求められている。本ガイドラインが対象とする情報システムの安全管理も、個人情報保護対策の一部として考えることができるため、この方針の中に情報システムの安全管理についても言及する必要がある。

個人情報保護に関する方針に盛り込むべき具体的内容について、「JIS Q 15001:2006（個人情報保護マネジメントシステム-要求事項）」では、下記のように定めている。

- a) 事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること
- b) 個人情報の取り扱いに関する法令、国が定める指針その他の規範を遵守すること
- c) 個人情報の漏えい、滅失又はき損の予防及び是正に関すること
- d) 苦情及び相談への対応に関すること
- e) 個人情報保護マネジメントシステムの継続的改善に関すること
- f) 代表者の氏名

また、情報システムの安全管理については、「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）」で、下記のように定めている。

ISMS 基本方針を、事業・組織・所在地・資産・技術の観点から、次を満たすように定義する。

- 1) 目的を設定するための枠組みを含め、また、情報セキュリティに係る活動の方向性の全般的認識及び原則を確立する。
- 2) 事業場及び法令又は規制の要求事項、ならびに契約上のセキュリティ義務を考慮する。
- 3) それのもとで ISMS の確立及び維持をする、組織の戦略的なリスクマネジメントの状況と調和をとる。
- 4) リスクを評価するに当たっての基軸を確立する。
- 5) 経営陣による承認を得る。

個人情報を取り扱う情報システムを運用する組織は、これらの要求事項を勘案して組織の実情に合った基本的な方針を策定し、適切な方法で公開することが重要である。

C. 最低限のガイドライン

1. 個人情報保護に関する方針を策定し、公開していること。
2. 個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実にし、不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践

A. 制度上の要求事項

(安全管理措置)

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

(個人情報保護法 第 20 条)

B. 考え方

安全管理を適切に行うための標準的なマネジメントシステムが ISO（ISO/IEC 27001:2005）ならびに JIS（JIS Q 27001:2006）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。

6.2.1 ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 では PDCA の各ステップを次の様に規定している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実施 (ISMS の導入及び運用) (ISMS の監視及び見直し)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P では ISMS 構築の骨格となる文書（基本方針、運用管理規程等）と文書化された ISMS 構築手順を確立する。

D では P で準備した文書や手順を使って実際に ISMS を構築する。

C では構築した ISMS が適切に運用されているか、監視と見直しを行う。

A では改善すべき点が出た場合には是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのようにおこなわれているかについて JIPDEC（財団法人 日本情報処理開発協会）の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されている。

【医療の安全管理の流れ】

事故やミスの発見と報告

「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告



原因の分析

- ・ 「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。（例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方箋が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
- ・ 作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。



予防／是正策

- ・ 再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底等）

上記を見ると、主にD→C→Aが中心になっている。これは医療分野においては診察、診断、治療、看護等の手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みが出来上がっているためと言える。

反面、情報セキュリティでは IT 技術の目覚ましい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため情報セキュリティ独自の管理方法が必要であり、ISMS はそのために考え出された。ISMS は医療の安全管理と同様 PDCA サイクルで構築し、維持して行く。

逆に言えば、医療関係者にとって ISMS 構築は P のステップを適切に実践し、ISMS の骨格となる文書体系や手順等を確立すれば、あとは自然に ISMS が構築されていく土壌があると言える。

P のステップを実践するために必要なことは何かについて次に述べる。

6.2.2 取扱い情報の把握

情報システムで扱う情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理されなければならない。

安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。・なくとも患者等の視点からの影響の大きさと、継続した業務を行う視点からの影響の大きさを考慮する必要がある。この他に医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類する。

個人識別可能な医療に係る情報の安全性に問題が生じた場合、患者等にきわめて深刻な影響を与える可能性があり、医療に係る情報は最も重要度の高い情報として分類される。

6.2.3 リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、6.3～6.11の対策を行うことになる。

特に安全管理や、個人情報保護法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障することであり、これが限界である。従って、人の行為も含めた脅威を想定し、運用管理規程を含めた対策を講じることが重要である。

医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。

- ① 医療情報システムに格納されている電子データ
 - (a) 権限のない者による不正アクセス、改ざん、き損、滅失、漏えい
 - (b) 権限のある者による不当な目的でのアクセス、改ざん、き損、滅失、漏えい
 - (c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、滅失、漏えい

- ② 入力の際に用いたメモ・原稿・検査データ等
 - (a) メモ・原稿・検査データ等の覗き見

- (b) メモ・原稿・検査データ等持ち出し
 - (c) メモ・原稿・検査データ等のコピー
 - (d) メモ・原稿・検査データの不適切な廃棄
- ③ 個人情報等のデータを格納したノートパソコン等の情報端末
- (a) 情報端末の持ち出し
 - (b) ネットワーク接続によるコンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、滅失、漏えい
 - (c) ソフトウェア（Winny 等のファイル交換ソフト等）の不適切な取扱いによる情報漏えい
 - (d) 情報端末の盗難、紛失
 - (e) 情報端末の不適切な破棄
- ④ データを格納した可搬媒体等
- (a) 可搬媒体の持ち出し
 - (b) 可搬媒体のコピー
 - (c) 可搬媒体の不適切な廃棄
 - (d) 可搬媒体の盗難、紛失
- ⑤ 参照表示した端末画面等
- (a) 端末画面の覗き見
- ⑥ データを印刷した紙やフィルム等
- (a) 紙やフィルム等の覗き見
 - (b) 紙やフィルム等の持ち出し
 - (c) 紙やフィルム等のコピー
 - (d) 紙やフィルム等の不適切な廃棄
- ⑦ 医療情報システム自身
- (a) サイバー攻撃による IT 障害
 - ・ 不正侵入
 - ・ 改ざん
 - ・ 不正コマンド実行
 - ・ 情報かく乱
 - ・ ウイルス攻撃
 - ・ サービス不能（DoS : Denial of Service）攻撃

- ・ 情報漏えい 等
- (b) 非意図的要因による IT 障害
 - ・ システムの仕様やプログラム上の欠陥（バグ）
 - ・ 操作ミス
 - ・ 故障
 - ・ 情報漏えい 等
- (c) 災害による IT 障害
 - ・ 地震、水害、落雷、火災等の災害による電力供給の途絶
 - ・ 地震、水害、落雷、火災等の災害による通信の途絶
 - ・ 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
 - ・ 地震、水害、落雷、火災等の災害による重要インフラ事業者等における IT の機能不全

これらの脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要になる。

C. 最低限のガイドライン

1. 情報システムで扱う情報をすべてリストアップしていること。
2. リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。
3. このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。
4. リストアップした情報に対してリスク分析を実施していること。
5. この分析の結果得られた脅威に対して、6.3～6.11 に示す対策を行っていること。

D. 推奨されるガイドライン

1. 上記の結果を文書化して管理していること。

6.3 組織的安全管理対策（体制、運用管理規程）

B. 考え方

安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

- ① 安全管理対策を講じるための組織体制の整備
- ② 安全管理対策を定める規程等の整備と規程等に従った運用

- ③ 医療情報の取扱い台帳の整備
- ④ 医療情報の安全管理対策の評価、見直し及び改善
- ⑤ 情報や情報端末の外部持ち出しに関する規則等の整備
- ⑥ 情報端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その情報端末等の管理規程
- ⑦ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程はきわめて重要であり、必ず定めなければならない。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9 情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

C. 最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。
2. 個人情報参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。
5. 運用管理規程等において次の内容を定めること。
 - (a) 理念（基本方針と管理目的の表明）
 - (b) 医療機関等の体制
 - (c) 契約書・マニュアル等の文書の管理
 - (d) リスクに対する予防、発生時の対応の方法
 - (e) 機器を用いる場合は機器の管理
 - (f) 個人情報の記録媒体の管理（保管・授受等）の方法
 - (g) 患者等への説明と同意を得る方法
 - (h) 監査
 - (i) 苦情・質問の受付窓口

6.4 物理的安全対策

B. 考え方

物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端

末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

- ① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
- ② 盗難、窃視等の防止
- ③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9 情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

C. 最低限のガイドライン

1. 個人情報が入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。
 - ・ 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。
 - ・ 入退者の記録を定期的にチェックし、妥当性を確認する。
4. 個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
5. 窃視防止の対策を実施すること。

D. 推奨されるガイドライン

1. 防犯カメラ、自動侵入監視装置等を設置すること。

6.5 技術的安全対策

B. 考え方

技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。

しかし、その有効範囲を認識し適切な適用を行えば、技術的な対策は強力な安全対策の手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。

- (1) 利用者の識別及び認証
- (2) 情報の区分管理とアクセス権限の管理
- (3) アクセスの記録（アクセスログ）

- (4) 不正ソフトウェア対策
- (5) ネットワーク上からの不正アクセス

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9 情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

(1) 利用者の識別及び認証

情報システムへのアクセスを正当な利用者のみ限定するために、情報システムは利用者の識別と認証を行う機能を持たなければならない。

小規模な医療機関等で情報システムの利用者が限定される場合には、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、一般的にこの機能は必須である。

認証を実施するためには、情報システムへのアクセスを行う全ての職員及び関係者に対し ID・パスワードや IC カード、電子証明書、生体認証等、本人の識別・認証に用いる手段を用意し、統一的に管理する必要がある。また更新が発生する都度速やかに更新作業が行われなければならない。

このような本人の識別・認証に用いられる情報は本人しか知り得ない、または持ち得ない状態を保つ必要がある。例えば、本人の識別・認証に用いられる情報が第三者に漏れないように以下のようなリスクに対処しなければならない。

- ・ ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- ・ パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- ・ 代行作業等のために ID・パスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- ・ ひとつの ID を複数の利用者が使用している。
- ・ 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- ・ パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- ・ 認証用の個人識別情報を格納するセキュリティ・デバイス（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
- ・ 退職した職員の ID が有効になったままで、ログインができてしまう。
- ・ 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- ・ コンピュータウイルスにより、ID やパスワードが盗まれ、悪用される。

＜認証強度の考え方＞

ID・パスワードの組合せは、これまで広く用いられてきた方法である。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務づける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。

このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。

認証に用いる手段としては、ID・パスワードの組合せのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」(バイオメトリクス)によるもの、ICカードのような「物理媒体」(セキュリティ・デバイス)によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難である。そこで、ICカード等のセキュリティ・デバイス+パスワードやバイオメトリクス+ICカードのように利用者しか持ち得ない2つの独立した要素を用いて行う方式(2要素認証)を採用することが望ましい。

また、入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。

＜ICカード等のセキュリティ・デバイスを配布する場合の留意点＞

利用者の識別や認証、署名等を目的として、ICカード等のセキュリティ・デバイスに個人識別情報や暗号化鍵、電子証明書等を格納して配布する場合は、これらのセキュリティ・デバイスが誤って本人以外の第三者の手に渡ることのないような対策を講じる必要がある。また、万一そのセキュリティ・デバイスが第三者によって不正に入手された場合においても、簡単には利用されないようにしていることが重要である。

従って、利用者の識別や認証、署名等が、これらセキュリティ・デバイス単独で可能となるような運用はリスクが大きく、必ず利用者本人しか知りえない情報との組合せによってのみ有効になるようなメカニズム、運用方法を採用すること。

ICカードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替え手段による一時的なアクセスルールを用意すべきである。その際、安全管理のレベルを安易に下げることがないように、本人確認を十分におこなった上で代替手段の使用を許し、さらにログ等を残し後日再発行された本人の正規の識別情報により、上記緊急時の操作のログ等の確認操作をすることが望ましい。

＜バイオメトリクスを利用する場合の留意点＞

識別・認証に指紋や虹彩、声紋等のバイオメトリクスを用いる場合は、その測定精度に

も注意を払う必要がある。医療情報システムで一般的に利用可能と思われる現存する各種のバイオメトリクス機器の測定精度は、1対N照合（入力された1つのサンプルが、登録されている複数のサンプルのどれに一致するか）には十分とは言えず、1対1照合（入力されたサンプルが、特定の1つのサンプルと一致するか）での利用が妥当であると考えられる。

従って、バイオメトリクスを用いる場合は、単独での識別・認証を行わず、必ずユーザID等個人を識別できるものと組合せて利用すべきである。

また、生体情報を基に認証するために以下のような、生体情報特有の問題がある。

- ・事故や疾病等による認証に用いる部位の損失等
- ・成長等による認証に用いる部位の変化
- ・一卵性の双子の場合、特徴値が近似することがある
- ・赤外線写真等による“なりすまし”(ICカード等の偽造に相当)

上記の事を考慮のうえ、生体情報の特徴を吟味し適切な手法を用いる必要がある。

欠損への対処としては異なる手法や異なる部位の生体情報を用いること。なりすましへの対処としては二要素認証（ICカードやパスワードとバイオメトリクスの組み合わせ等）を用いること。

(2) 情報の区分管理とアクセス権限の管理

情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。

知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定を行う機能があれば、さらにリスクを低減できる。

アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行う必要があり、組織の規程で定められていなければならない。

(3) アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。従って、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。

また、アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いも

のを使用し、管理対象の全てのシステムで同期を取らなければならない。

(4) 不正ソフトウェア対策

ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正ソフトウェアの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正ソフトウェアの侵入に気づくことになる。

対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が最も効果的であると考えられ、このソフトウェアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できる。また、このことは医療機関等の外部で利用する情報端末やPC等についても同様であるが、その考え方と対策については、「6.9 情報及び情報端末の持ち出しについて」を参照されたい。

ただし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。

たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。

(5) ネットワーク上からの不正アクセス

ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。

ファイアウォールは「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。単純なパケットフィルタリングで十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望ましい。システム管理者はその方式が何をどのように守っているかを認識するべきである。このことは、医療機関等の外部から医療機関等の情報システムに接続されるPC等の情報端末に対しても同様であるが、その考え方と対策については、「6.9 情報及び情報端末の持ち出しについて」を参照されたい。

不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、医療情報

システムと外部ネットワークとの関係に応じて、IDS の採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的実施し、パッチ等の対策を講じておくことも重要である。

無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS : Denial of Service 等）を行ったり、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて PC を識別するケースが多いが、MAC アドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。また、ネットワーク上を流れる情報の窃視を防止するために、暗号化等による”情報漏えい”への対策も必要となる。

(6) その他

無線 LAN は、看護師等が情報端末を利用し患者のベッドサイドで作業する場合等に利便性が高い反面、通信の遮断等も起こる危惧があるので、情報の可用性が阻害されないように留意する必要がある。また、無線電波により重大な影響を被るおそれのある機器等の周辺での利用には注意が必要である。

最近では、電力線搬送通信（PLC : Power Line Communication）が利用可能になった。しかし、医療機関等において PLC を利用する場合、医療機器に対する安全性が確認されておらず、厚生労働省医薬食品局から「広帯域電力線搬送通信機器による医療機器への影響に関する医療関係者等からの照会に対する対応について」(平成 18 年 11 月 9 日付け薬食安発第 1109002 号) の通知が出されているため可用性の確保と他の医療機器への影響の双方に留意する必要がある。

C. 最低限のガイドライン

1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。
2. 本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。
3. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のある場合には、クリアスクリーン等の防止策を講じること。
4. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。
5. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能がある

ことが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。

6. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は、なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。

情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。

7. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。
8. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。
9. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。

10. パスワードを利用者識別に使用する場合

システム管理者は以下の事項に留意すること。

- (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。(利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること)
- (2) 利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。
- (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)

また、利用者は以下の事項に留意すること。

- (1) パスワードは定期的に変更し(最長でも 2 ヶ月以内)、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。
- (2) 類推しやすいパスワードを使用しないこと。

11. 無線 LAN を利用する場合

システム管理者は以下の事項に留意すること。

- (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。
- (2) 不正アクセスの対策を施すこと。・ なくとも SSID や MAC アドレスによるアクセス制限を行うこと。
- (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。
- (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。
- (5) 無線 LAN の適用に関しては、総務省発行の「安心して無線 LAN を利用するために」を参考にすること。

D. 推奨されるガイドライン

1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
2. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。
3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。
4. パスワードを利用者識別に使用する場合以下の基準を遵守すること。
 - (1) パスワード入力不成功に終わった場合の再入力に対して一定不応時間を設定すること。
 - (2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。
5. 認証に用いられる手段としては、ID+バイOMETRICSあるいはICカード等のセキュリティ・デバイス+パスワードまたはバイOMETRICSのように利用者しか持ち得ない2つの独立した要素を用いて行う方式（2要素認証）等、より認証強度が高い方式を採用すること。
6. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。

6.6 人的安全対策

B. 考え方

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるた

め、人による誤りの防止を目的とした人的安全管理対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。

医療情報システムに関連する者として、次の5種類を想定する。

- (a) 医師、看護師等の業務で診療に関わる情報を取扱い、法令上の守秘義務のある者
- (b) 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取扱い、守秘義務を負う者
- (c) システムの保守業者等の雇用契約を結ばずに医療機関等の業務に携わる者
- (d) 見舞い客等の医療情報にアクセスする権限を有しない第三者
- (e) 診療録等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a) (b)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の2つに分けて説明する。

(d)の第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏えい等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、いわゆる「外部保存」を受託する機関等に該当するが、これに関しては詳細を8章に記述する。

(1) 従業者に対する人的安全管理措置

C. 最低限のガイドライン

医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
2. 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。
3. 従業者の退職後の個人情報保護規程を定めること。

D. 推奨されるガイドライン

1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

(2) 事務取扱委託業者の監督及び守秘義務契約

C. 最低限のガイドライン

1. 医療機関等の事務、運用等を外部の事業者へ委託する場合は、医療機関等の内部にお

ける適切な個人情報保護が行われるように、以下のような措置を行うこと。

- ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
 - ② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業員・作業内容・作業結果の確認を行うこと。
 - ③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
 - ④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。
2. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

6.7 情報の破棄

B. 考え方

医療に係る電子情報は破棄に関しても安全性を確保する必要がある。破棄は確実にを行う必要がある。しかし、例えばデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もあり、注意しなくてはならない。

実際の破棄に備えて、事前に破棄の手順を明確化しておくべきである。

C. 最低限のガイドライン

1. 「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業員の特典、具体的な破棄の方法を含めること。
2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものを行うこととし、残存し、読み出し可能な情報がないことを確認すること。
3. 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
4. 運用管理規程において下記の内容を定めること。
 - (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成

6.8 情報システムの改造と保守

B. 考え方

医療情報システムの可用性を維持するためには定期的なメンテナンスが必要である。メ

メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があり、十分な対策が必要になる。具体的には以下の脅威が存在する。

- ・ 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
- ・ 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
- ・ 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
- ・ 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等

これらの脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。すなわち、①保守会社との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の医療機関等の関係者による監督、等の運用面を中心とする対策が必要である。

保守作業によっては保守会社からさらに外部の事業者修理等を委託することが考えられるため、保守会社との保守契約の締結にあたっては、再委託する事業者への個人情報保護の徹底等について保守会社と同等の契約を求めることが重要である。

C. 最低限のガイドライン

1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。
4. 保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。
5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
6. 保守会社と守秘義務契約を締結し、これを遵守させること。

7. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
8. リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。
9. 再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。

D. 推奨されるガイドライン

1. 詳細なオペレーション記録を保守操作ログとして記録すること。
2. 保守作業時には医療機関等の関係者立会いのもとで行うこと。
3. 作業員各人と保守会社との守秘義務契約を求めること。
4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
5. 保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。

6.9 情報及び情報機器の持ち出しについて

B. 考え方

昨今、医療機関等において医療機関等の従業者や保守業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生している。

情報の持ち出しについては、ノートパソコンのような情報端末やフロッピーディスク、USB メモリのような情報記録可搬媒体が考えられる。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられる。

まず重要なことは、「6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」の「6.2.2 取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3 リスク分析」を実施することである。

その上で、医療機関等において把握されている情報もしくは情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。切り分けを行った後、持ち出してよいとした情報もしくは情報機器に対して対策を立てなくてはならない。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器の管理

状況が明確になる。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等も管理状況を把握するための方策となる。

一方、自宅等の医療機関等の管轄外のパソコン（情報機器）で、可搬媒体に格納して持ち出した情報を取り扱う時に、コンピュータウイルスや不適切な設定のされたソフトウェア（Winny 等）、外部からの不正アクセスによって情報が漏えいすることも考えられる。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報もしくは情報機器の持ち出しについては組織的な対策が必要となり、組織として情報もしくは情報機器の持ち出しをどのように取り扱うかという方針が必要といえる。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることからリスク分析を実施し、対策を検討しておくことは必要である。

ただし、この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が医療機関等に設置されている情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

従って、情報もしくは情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策をさらに施す必要がある。

C. 最低限のガイドライン

1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。
2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。
3. 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。
4. 運用管理規程で定めた盗難、紛失時の対応に従業者等に周知徹底し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。
6. 情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。
8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネッ

トワークに接続する場合は「6.11 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」の規定を順守すること。

9. 持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなソフトウェアをインストールしないこと。
10. 個人保有の情報機器（パソコン等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。

D. 推奨されるガイドライン

1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。
2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせる用いること。
3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。

6.10 災害等の非常時の対応

B. 考え方

医療機関等は医療情報システムに不具合が発生した場合でも患者安全に配慮した医療サービスの提供が最優先されなければならない。

ここでは、「6.2.3 リスク分析」の「⑦医療情報システム自身」に掲げる自然災害やサイバー攻撃による IT 障害等の非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における留意事項について述べる。

「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非正常状態になる場合がある。

前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。

後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合である。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。

(1) 非常時における事業継続計画 (BCP : Business Continuity Plan)

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは

難しく、可能な限り計画内容を事前演習等で検証することが望ましい。
医療施設として定められる BCP においては、医療情報システムについての計画を含め、全体としての整合性が必要である。
以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。

① BCP として事前に周知しておく必要がある事項

事前に対応策を知ってもらい、信頼してもらっておくべきである。

- ・ ポリシと計画
何が「非常事態」なのかを理解し、定義すべきである。
- ・ 非常事態検知手段
災害や故障の検知機能と発生情報の確認手段
- ・ 非常時対応チームの連絡先リスト、連絡手段及び対策ツール
- ・ 非常時に公にすべき文書及び情報

② BCP 実行フェーズ

災害や事故の発生（或いは発生の可能性）を検知してから、BCP 実行か通常の障害対策かの判断を行い、BCP 発動と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡・協力依頼を行い、システムの切替／縮退等の準備を行う。例えば、ネットワークから切り離れたスタンドアロンでの使用や、紙での運用等が考えられる。業務を受託する事業者との間の連絡体制や受託する事業者と一体となったトラブル対処方法等が明示されるべきである。

具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」及び「影響度の確認」である。

③ 業務再開フェーズ

BCP を発動してから、バックアップサイト・手作業等の代替手段により業務を再開し、軌道に乗せるまでフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員等の人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。

最も緊急度の高い業務（基幹業務）から再開する。

具体的項目は「人的資源の確保」、「代替施設及び設備の確保」、「再開／復旧活動の両立」及び「リスク対策によって新たに生じるリスクへの対策」である。

④ 業務回復フェーズ

最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混

乱に配慮した慎重な判断がポイントとなる。

具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」及び「制限の確認」である。

⑤ 全面復旧フェーズ

代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。

具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」及び「総括」である。

⑥ BCP の見直し

正常な状態に復帰した後に、BCP に関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCP の見直しを行い、次の非常時に備えることが重要である。

(2) 医療システムの非常時使用への対応

① 非常時用ユーザアカウントの用意

- ・ 停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えなくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データへのアクセス制限が医療サービス低下を招かないように配慮している。ブレークグラスでは非常時用ユーザアカウントは通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更をすることを基本としている。

② 災害時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮する等、必要に応じて非常時の運用に対応した機能を実装すること。

上記の様な非常時使用への対応機能の用意は、関係者に周知され非常時に適切に用いる必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

C. 最低限のガイドライン

1. 医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 非常時の情報システムの運用
 - ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。
 - ・非常時機能が定常時に不適切に利用されないことがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。
 - ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。
4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。

6.11 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

B. 考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。ここでは、双方向だけではなく、一方向の伝送も含む。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS型のサービスを利用する、医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する、患者等による外部からのアクセスを許可する、等が考えられる。

医療情報をネットワークを利用して外部と交換する場合、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、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について

記述する。

なお、可搬媒体や紙を用いて情報を搬送する場合は、付則 1 及び 2 を参照願いたい。

B-1. 医療機関等における留意事項

ここでは 4 章の「電子的な医療情報を扱う際の責任のあり方 4.2 委託と提供における責任分界点について」で述べた責任の内、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は送信元の医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の機関に受け渡しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、ここでいう管理責任とは電子的に記載されている情報の内容に対して負うべきものでありその記載内容や記載者の正当性の保持（真正性の確保）のことを指す。つまり、後述する「B-2. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。このような情報の内容に対するセキュリティのことをオブジェクト・セキュリティと呼ぶことがある。一方、「B-2. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。このような回線上の情報に対するセキュリティのことをチャネル・セキュリティと呼ぶことがある。

このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

①「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。例えば、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取る等、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。一方、ネットワーク機材の不適切な設定により、意図しない情報漏えいや誤送信等も想定され、このような場合には医療機関等における責任が発生する事例も考えられる。

このように様々な事例が考えられる中で、医療機関等においては、万が一、伝送途中で情報が盗み取られたり、意図しない情報漏えいや誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報の暗号

化が考えられる。ここでいう暗号化とは、先に例示した情報そのものの暗号化（オブジェクト・セキュリティ）のことを指している。

どのような暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密度や医療機関等で構築している情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ではあるが、・なくとも情報を伝送し、医療機関等の設備から情報が送られる段階においては暗号化されていることが望ましい。

この盗聴防止については、例えばリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託事業者等に確認し、監督する責任を負う。

② 「改ざん」の危険性への対応

ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えなければならない。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。また、後述する「B-2. 選択すべきネットワークセキュリティの考え方」のネットワークの構成によっては、ネットワーク自体に情報の秘匿化機能が不十分な場合もあり、改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

③ 「なりすまし」の危険性への対応

ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の機関が確かに意図した相手であることを確認しなくてはならない。逆に、情報の受け手となる送信先の機関は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であることを確認しなくてはならない。これは、ネットワークが非対面による情報伝達手段であることに起因するものである。

そのため、例えば通信の起点と終点の機関を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。また、改ざん防止と併せて、送信元が正当な送信元であることを確認するために、医療情報等に対して電子署名を組み合わせることも考えられる。

また、上記の危険性がサイバー攻撃による場合の対応は「6.10 災害等の非常時の対応」を参照されたい。

B-2. 選択すべきネットワークのセキュリティの考え方

「B-1. 医療機関等における留意事項」では主に情報内容が脅威に対応するオブジェクト・セキュリティについて解説したが、ここでは通信経路上での脅威への対応であるチャネル・セキュリティについて解説する。

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、情報を受信する機関の外部ネットワーク接続点までや、業務の必要性から並びに患者からのアクセスを許可する等、外部から医療機関等の情報システムにアクセスする接続点までのことを指し、医療機関等の内部で構成される LAN は対象とならない。ただし、4 章「電子的な医療情報を扱う際の責任のあり方 4.2 責任分界点について」でも触れた通り、接続先の医療機関等のネットワーク構成や経路設計によって意図しない情報漏えいが起こる可能性については留意をし、確認をする責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等としては交換しようとする情報の機密性の整理をする必要がある。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、予約システムが扱う再診予約情報の様な機密性の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

- ・ 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPN サービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等においては、善管注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確認しなくてはならない。

・ 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入したネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。

そのため、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り扱いに関する契約の締結、脅威が発生した際に備えて、通信事業者がネットワーク経路上のセキュリティを委託する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等を考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定して留意点を述べる。

また、想定するケースの中でも、携帯電話・PHS や可搬型コンピュータ等のいわゆるモバイル端末等を使って医療機関等の外部から接続する場合は、利用するモバイル端末とネットワークの接続サービス及びその組み合わせによって複数の接続形態が存在するため、これらについては特に「Ⅲ モバイル端末等を使って医療機関等の外部から接続する場合」を設けて考え方を整理している。

I. クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、いわゆるインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低い。ただし、「B-1. 医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できない。

いため、伝送しようとする情報自体の暗号化については考慮が必要である。また、ウイルス対策ソフトのパターン定義ファイルや OS のセキュリティ・パッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特長を述べる。

①専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（「帯域」という）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある。



図 B-2-① 専用線で接続されている場合

②公衆網で接続されている場合

公衆網とは ISDN (Integrated Services Digital Network) やダイヤルアップ接続等、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続はインターネットサービスプロバイダ（以下、ISP）に接続する接続方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ. オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイヤルしてネットワーク接続を確立するため、ネットワーク接続を確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様に拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため大量の情報もしくは画像等の容量の大きな情報の送信には不向きであるため、適用範囲を適切に見定める必要がある。



図 B-2-② 公衆網で接続されている場合

③閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を言う。このような接続サービスを本ガイドラインでは IP-VPN (Internet Protocol-Virtual Private Network) と呼び、クローズドなネットワークとして取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

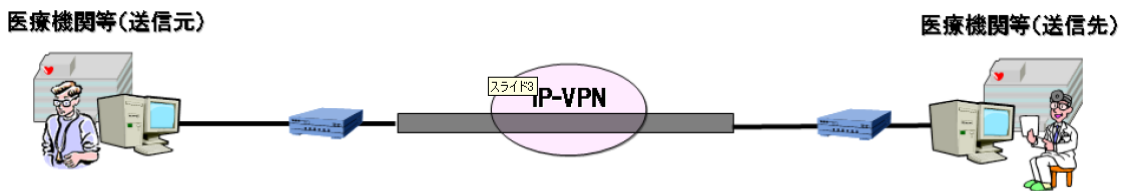


図 B-2-③-a 単一の通信事業者が提供する閉域ネットワークで接続されている場合

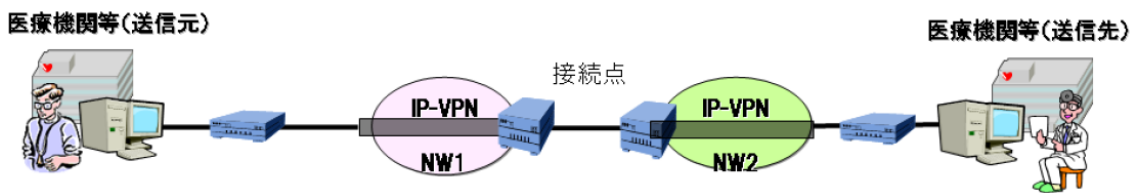


図 B-2-③-b 途中で複数の閉域ネットワークが相互接続して接続されている場合

以上の3つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。また異なる通信事業者のクローズドなネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。こ

の際、偶発的に情報の中身が漏示する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。そのほか、医療機関等から閉域 IP 通信網に接続する点等、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

これらの接続サービスでは、一般的に送られる情報そのものに対する暗号化は施されていない。そのため、クローズドなネットワークを選択した場合であっても、「B-1. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入する等の措置を取る必要がある。

II. オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。すなわち、オブジェクト・セキュリティの考え方に沿った対策を施す必要がある。

ただし、B-2 の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の判断で導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI (Open Systems Interconnection) 階層モデル※」で定義される 7 階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平成 19 年 2 月」が参考になる。

※OSI 階層モデル (Open System Interconnection)

開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコル。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択のための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電氣的、物理的に変換。機器の形状・特性を規定している層

例えば、SSL-VPN を用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPSec を用いる場合は、2 階層目もしくは3階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE (Internet Key Exchange) といわれる標準的手順を組み合わせる等して、確実にその安全性を確保する必要がある。

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要がある。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。



図 B-2-④ オープンネットワークで接続されている場合

Ⅲ. モバイル端末等を使って医療機関等の外部から接続する場合

ここでは、携帯電話・PHS や可搬型コンピュータ等の、いわゆるモバイル端末を用いて、医療機関の外部から医療機関内部のネットワークに接続する場合のセキュリティ要件を整理しておく。

外部からの接続については、「6.8 情報システムの改造と保守」で述べた保守用途でのアクセス、医療機関の職員による業務上のアクセス、さらには本章「B-3 患者等に診療情報等を提供する場合のネットワークに関する考え方」で述べる患者等からのアクセス等、さまざまなケースが想定される。

従って、実際の接続において利用されるモバイル端末とネットワークの接続サービス及びそれらの組み合わせが、本章で説明する接続形態のどれに該当するかを明確に識別する

ことが重要になる。

外部から医療機関の内部ネットワークに接続する場合、現状で利用可能な接続形態の俯瞰図を図 B-2-⑤に示す。

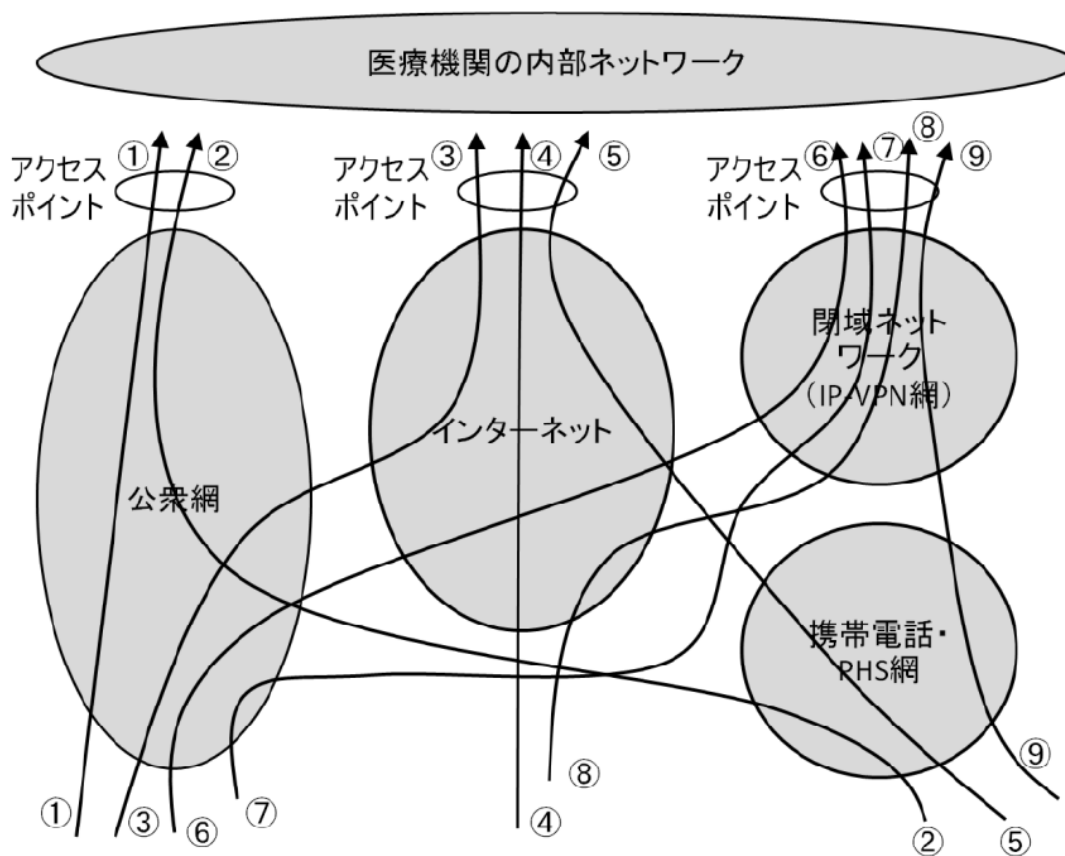


図 B-2-⑤ モバイル環境における接続形態

図 B-2-⑤に示したように、接続形態は下記の 3 つの系統に類型化できる。(括弧内の丸数字はそれぞれ図 B-2-⑤と対応する)

- 1) 公衆網 (電話網) を経由して直接ダイヤルアップする場合 (①、②)
- 2) インターネットを経由して接続する場合 (③、④、⑤)
- 3) 閉域ネットワーク (IP-VPN 網) を経由して接続する場合 (⑥、⑦、⑧、⑨)

ここでは、本章の「Ⅰ. クローズドなネットワークで接続する場合」と「Ⅱ. オープンなネットワークで接続する場合」で説明したどのケースに該当するかを示し、それぞれのケースにおけるセキュリティ上の留意点をまとめる。

1) 公衆網（電話網）を經由して直接ダイアルアップする場合

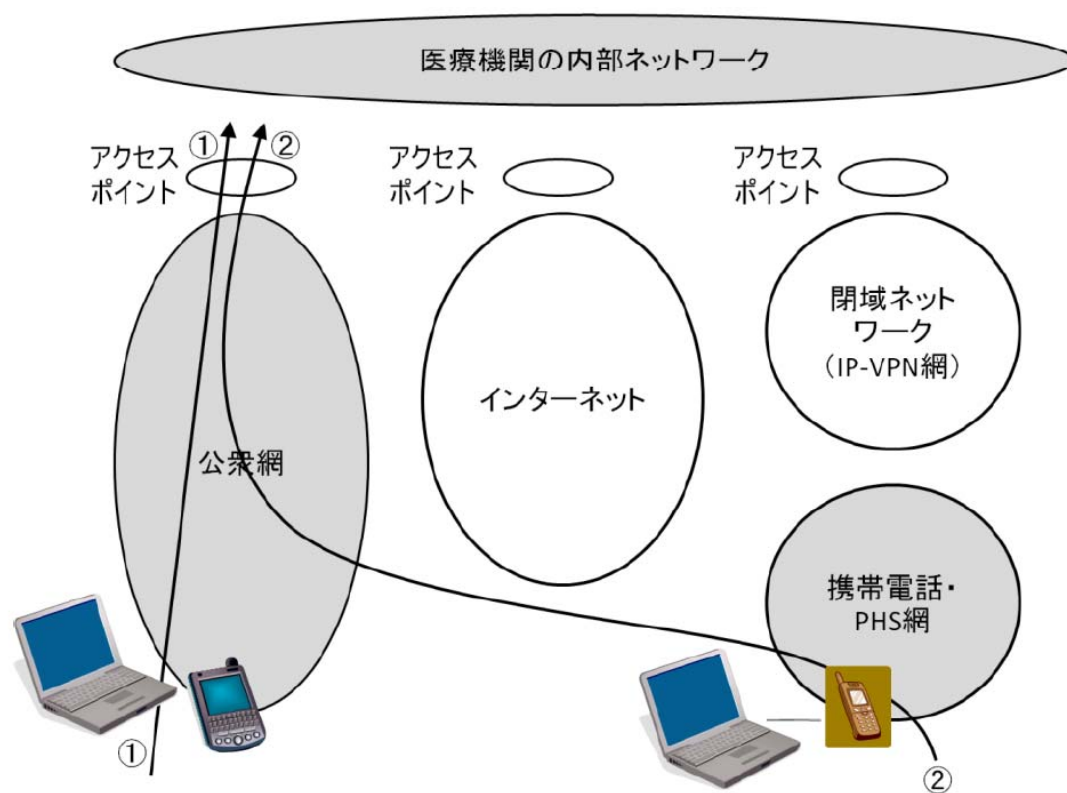


図 B-2-⑥ モバイル環境における接続形態（公衆網経由）

①は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続し、医療機関内に設けられたアクセスポイントに直接ダイアルアップするケースである。

②は①における電話回線の代わりに、携帯電話・PHS やその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS 網に接続ケースである。①と②は携帯電話・PHS 網を經由するかどうかの違いがある。

いずれも「I. クローズドなネットワークで接続する場合」における「②公衆網で接続されている場合」に相当するため、セキュリティ的な要件は、そこでの記述を適用すること。すべてクローズドなネットワークを經由するため、比較的安全性は高い。

2) インターネットを経由して接続する場合

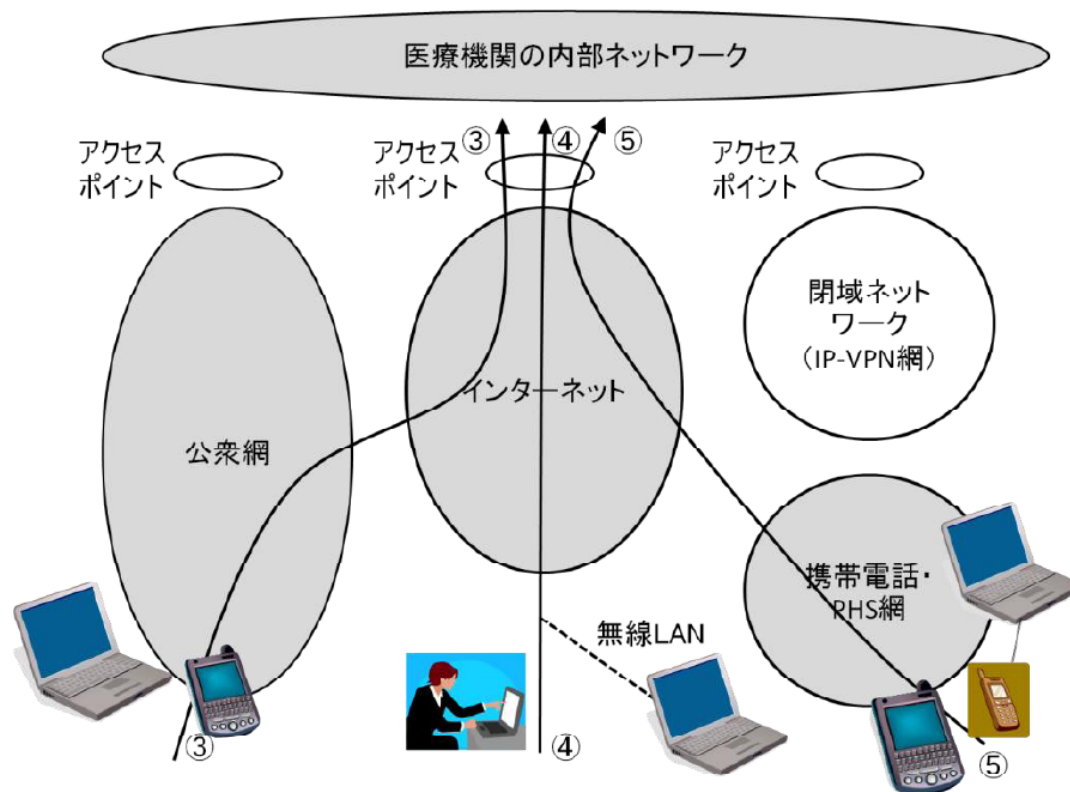


図 B-2-⑦ モバイル環境における接続形態（インターネット経由）

③は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続してインターネットのサービスプロバイダのアクセスポイントにダイヤルアップし、インターネット経由で医療機関のアクセスポイント接続するケースである。

④は③における電話回線の代わりに、自宅やホテル等インターネットへの接続インタフェースのあるところで LAN を使って接続するケースである。LAN として有線の LAN の代わりに無線 LAN を利用するケースもある。いわゆる公衆無線 LAN を利用した接続もこの形態に含まれる。

⑤は携帯電話・PHS 網を経由して、携帯電話・PHS 等のサービス提供会社の提供するサービスを利用してインターネットへ接続するケースである。

③から⑤のいずれのケースも「Ⅱ. オープンなネットワークで接続されている場合」に相当する。従って、セキュリティ的な要件は、そこでの記述を適用すること。オープンなネットワークを経由するので、「B-1 医療機関等における留意事項」で述べたオブジェクト・セキュリティとチャネル・セキュリティを担保するための対策が必要である。

具体的には、モバイル端末として携帯電話・PHS 機や、より高機能な端末装置（いわゆるスマートフォン等）を利用する場合には、その端末で SSL/TLS が利用できるのか、接続経路に IPSec と IKE が適用されているのか、等のサービス内容を確認する必要がある。

なお、これらのケースは、いずれも操作者が自分のモバイル端末を用いて接続することを想定しているが、いわゆるネットカフェ等の備え付けの端末を利用して医療機関内の情報にアクセスするケースも考えられる。このようなアクセス方法はリスクが大きい。

医療機関が組織の方針として、このようなアクセス形態を認めるかどうかについては、慎重な検討が必要である。

3) 閉域ネットワークを経由して接続する場合

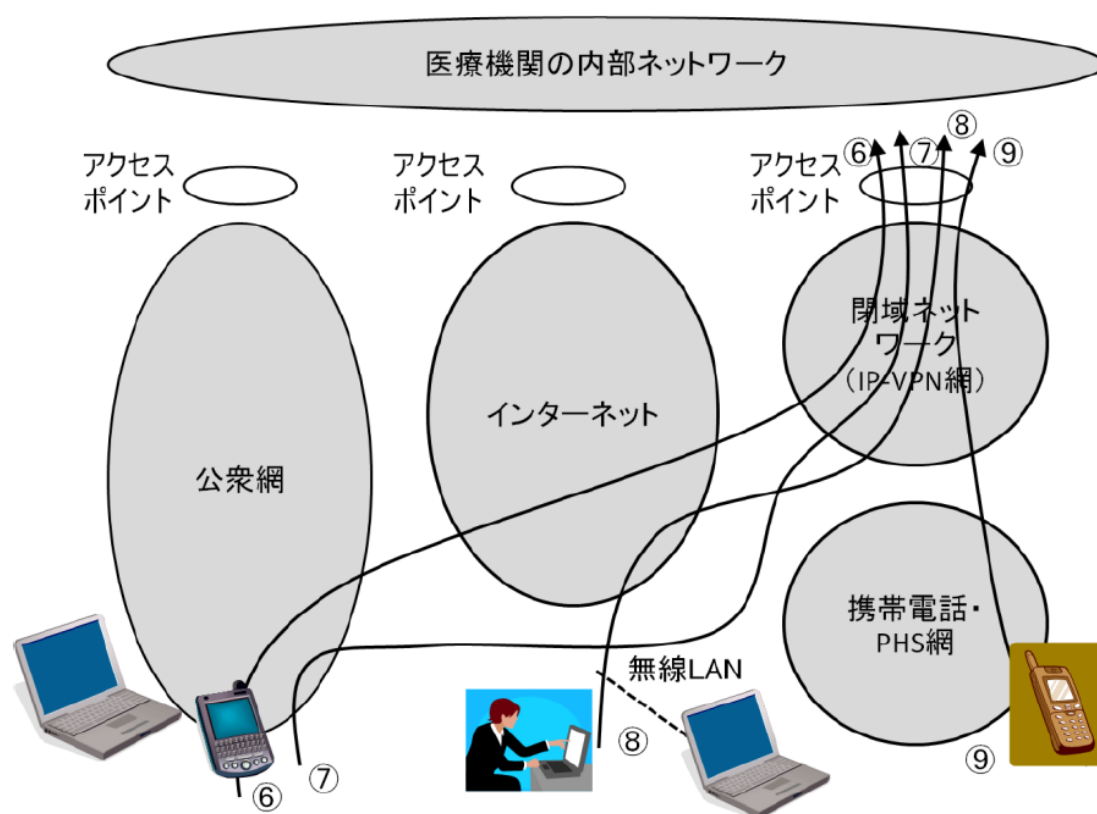


図 B-2-⑧ モバイル環境における接続形態（閉域ネットワーク経由）

⑥と⑦はいずれも自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続して閉域ネットワークのサービスプロバイダのアクセスポイントにダイヤルアップし、閉域ネットワーク経由で医療機関のアクセスポイント接続するケースである。

⑥は⑦とよく似ているが、⑥がダイヤルアップする際に一度オープンなネットワーク（インターネット）を提供するプロバイダを経由するのに対して、⑦では閉域ネットワークを提供するプロバイダに直接ダイヤルアップするという違いがある。

⑧は⑥における電話回線の代わりに、自宅やホテル等インターネットへの接続インターフェースのあるところで LAN を使って接続するケースである。このケースのバリエーションとして、LAN として有線の LAN の代わりに無線 LAN を利用するケースもあり、いわゆる公

衆無線 LAN 等もこのケースに含まれる。

⑨は携帯電話・PHS 網を経由して、閉域ネットワークへ接続するケースである。この場合の携帯電話・PHS 網から閉域ネットワークへの接続は、携帯電話・PHS サービス提供会社によって提供されるサービスである。

いずれも「I. クローズドなネットワークで接続する場合」における「③閉域 IP 通信網で接続されている場合」に相当するため、セキュリティ的な要件は、そこでの記述を適用すること。クローズドなネットワークを経由するため、比較的安全性は高い。

ただし、⑥と⑧のケースでは、閉域ネットワークに到達するまでにオープンなネットワーク（インターネット）を経由するため、サービス提供者によってはこの間でのチャンネル・セキュリティが確保されないこともありうる。チャンネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前にサービス提供者との契約をよく確認して、チャンネル・セキュリティが確実に確保されるようにしておく必要がある。

なお、ここで述べたようなモバイル接続形態に関連するセキュリティ要件に加え、医療機関の外部で情報にアクセスするという行為自体に特有のリスクが存在する。

例えば、機密情報が格納されたモバイル端末の盗難や紛失等の管理面のリスク、さらには公共の場所で情報を閲覧することによる他者からの窃視等による機密漏えいのリスク等である。

これについては「6.9 情報及び情報機器の持ち出しについて」に詳細を記述したので、参照すること。

B-3 従業者による外部からのアクセスに関する考え方

医療機関等の職員がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可することもあり得る。このような場合のネットワークに関わる安全管理の要件はすでに述べたが、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。加えて、外部からのアクセスに用いる機器の安全管理を運用管理規程で定めることは重要ではあるが、考慮すべきことが 3 点ある。

- ① PC 等と言ってもその安全管理対策を確認するためには一定の知識と技能が必要で、職員にその知識と技能を要求することは難しいこと。
- ② 運用管理規程で定めたことが確実に実施されていることを説明するためには適切な運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは通常は困難なこと。
- ③ 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等の管理下にある機器を必要に応じて使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性があること。

従って、通常は行うべきではないが、医師不足等に伴う医療従事者の過剰労働等に対応するために、やむを得ず行う場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術が普及しており、これらの導入を検討することが重要であるとともに、運用等の要件にも相当な厳しさが求められる。

B-4. 患者等に診療情報等を提供する場合のネットワークに関する考え方

診療情報等の開示が進む中、ネットワークを介して患者（または家族等）に診療情報等を提供する、もしくは医療機関内の診療情報等を閲覧させる可能性も出てきた。本ガイドラインは、医療機関等の間における医療情報の交換を想定しているが、患者に対する情報提供も十分想定される状況にある。ここではその際の考え方について触れる。

ここでの考え方の原則は、医療機関等が患者との同意の上で、自ら実施して患者等に情報を提供する場合であり、診療録及び診療諸記録の外部保存を受託する事業者が独自に情報提供を行うことはあってはならない。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、情報を閲覧する患者等のセキュリティ知識と環境に大きな差があるということである。また、一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。しかし、セキュリティ知識に大きな差がある以上、情報を提供する医療機関等が患者等の納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏えい等の事故が起きた場合は、その責任を逃れることはできないことを認識しなくてはならない。

また、今まで述べてきたような専用線等のネットワーク接続形態で患者等に情報を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、提供に用いるネットワークとしては、一般的にはオープンなネットワークを介することになる。この場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

医療機関等における基本的な留意事項は、既に4章やB-1で述べられているが、オープンなネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。特に、患者等に情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。そのため、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いる必要がある。

このように、患者等に情報を提供する場合には、ネットワークのセキュリティ対策のみならず、医療機関等内部の情報システムのセキュリティ対策、情報の主体者となる患者等へ危険性や提供目的の納得できる説明、また非ITに関わる各種の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にした上で実施しなくてはならない。

C. 最低限のガイドライン

1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策をとること。
施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策をとること。
セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。
上記を満たす対策として、例えば IPSec と IKE を利用することによりセキュアな通信路を確保することがあげられる。
チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者を確認すること。
2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。
3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとること。これに関しては、医療情報の安全管理に関するガイドライン「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
4. ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。
5. 送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。
6. 医療機関等間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。
 - ・ 診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定
 - ・ 送信元の医療機関等がネットワークに接続できない場合の対処
 - ・ 送信先の医療機関等がネットワークに接続できなかった場合の対処
 - ・ ネットワークの経路途中が不通または著しい遅延の場合の対処

- ・ 送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処
- ・ 伝送情報の暗号化に不具合があった場合の対処
- ・ 送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処
- ・ 障害が起こった場合に障害部位を切り分ける責任
- ・ 送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。

- ・ 通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。
- ・ 患者等に対する説明責任の明確化。
- ・ 事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。
- ・ 交換した医療情報等に対する管理責任及び事後責任の明確化。

個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。

7. リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。

また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。

8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また上記1及び4を満たしていることを確認すること。
9. 患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信のSSL暗号化、PKI個人認証等の技術を用いた対策を実施すること。

また、情報の主体者となる患者等へ危険性や提供目的の納得できる説明を実施し、ITに係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。

D. 推奨されるガイドライン

1. やむを得ず、従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。

6.12 法令で定められた記名・押印を電子署名で行うことについて

A. 制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

- 一 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。
- 二 当該情報について改変が行われていないかどうかを確認することができるものであること。

（電子署名及び認証業務に関する法律（平成12年法律第102号）第2条1項）

B. 考え方

平成11年4月の「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通知」においては、法令で署名または記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていた。

しかし、平成12年5月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書等として、e-文書法省令において指定された文書等においては、「A. 制度上の要求事項」に示した電子署名によって、記名・押印にかわり電子署名を施すことで、作成・保存が可能となった。

ただし、医療に係る文書等では一定期間、署名を信頼性を持って検証できることが必要である。電子署名は紙媒体への署名や記名・押印と異なり、「A. 制度上の要求事項」の一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり失効させた場合は検証ができないという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。例えば現在、電子署名に一般的に用いられている暗号方式のRSA 1024bit や、ハッシュ関数のSHA1 は、政府機関の情報システムからの移行スケジュールが決まっており、2008年4月の情報セキュリティ政策会議が決定した「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA1及びRSA1024に関わる移行指針」によれば、2014年度以降、RSA 2048bit やSHA2等へ移行される予定となっている。

従って、電子署名を付与する際はこのような点を考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名

の検証が継続できる必要がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。近年、デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、JIS規格としても制定された（JIS X 5092:2008 CMS 利用電子署名 (CAAdES) の長期署名プロファイル、JIS X 5093:2008 XML 署名利用電子署名 (XAdES) の長期署名プロファイル）。

長期署名方式では、下記により、署名検証の継続を可能としている。

- (1) 署名に付与するタイムスタンプにより署名時刻を担保する（署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること）。
- (2) 署名当時の検証情報（関連する証明書や失効情報等）を保管する。
- (3) 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。

医療情報の保存期間は5年以上の長期に渡るものも有り、システム更新や検証システムの互換性等の観点からも、標準技術を用いることが望ましい。従って、例えば、前述の標準技術を用い、必要な期間、電子署名の検証を継続して行うことが出来るようにすることが重要である。

C. 最低限のガイドライン

法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。

- (1) **厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと**
 1. 保健医療福祉分野 PKI 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用するのが望ましい。
ただし、当該電子署名を検証しなければならない者すべてが、国家資格を含めた電子署名の検証が正しくできることが必要である。
 2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。
 3. 「電子署名に係る地方公共団体の認証業務に関する法律」（平成 14 年法律第 153 号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。

(2) 電子署名を含む文書全体にタイムスタンプを付与すること。

1. タイプスタンプは、「タイムビジネスに係る指針—ネットワークの安心な利用と電子データの 安全な長期保存のために—」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。
2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。
3. タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。

(3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いること。

1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。

以上

付表1 一般管理における運用管理の実施項目例

A：医療機関の規模を問わない
 B：大／中規模病院
 C：小規模病院、診療所 ※「運用管理規程文例」は巻末にまとめる

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策
①	総則	理念(基本方針と管理目的の表明)	A		・情報システムの安全管理に関する方針に基づき、本規程の目的を述べる
		対象情報	A		・対象システム、対象情報を定める ・対象システム、対象情報を安全管理上の重要度に応じて分類し、リスク分析を行う
		標準規格	B		・医療機関側でフォローすべき標準規格の列挙を行い、システム改定時に変更の対象とする
C			・ベンダに対しシステムで使われている標準規格に関する情報提供を求め、システム改訂時に変更の対象とする		
②	管理体制	運用責任者、個人情報保護責任者、システム管理者	B		・運用責任者、個人情報保護責任者、システム管理者、機器管理者、安全管理者等の任命規程
			C		・院長が運用責任者、個人情報保護責任者とシステム管理者を兼ねる場合、その旨を明記する
		契約書・マニュアル等の文書管理	A		・別途定めてある文書管理規程に従うことを規程する
		監査体制と監査責任者	B		・監査体制(監査の周期、監査結果の評価・対応等)を規程 ・監査責任者の任命規程
			C		・院内で監査体制を整えることができない場合、第三者監査機関への監査依頼を規程する
		患者及びシステム利用者からの苦情・質問の受付体制	A		・患者及びシステム利用者からの苦情・質問受付窓口の設置 ・受付後の処置を規程
		事故対策	A		・緊急時あるいは災害時の連絡、復旧体制並びに回復手段を規定する
		システム利用者への教育・訓練など周知体制	A		・各種規程書、指示書、取扱説明書等の作成 ・定期的な利用者への教育、訓練
③	管理者及び利用者の責務	システム管理者や運用責任者の責務	A		・機器、ソフトウェア導入時の機能確認・運用環境の整備と維持 ・情報の安全性の確保と利用可能な状況の維持 ・情報の継続的利用の維持・不正利用の防止 ・利用者への教育、訓練・患者または利用者からの問合せ ・苦情窓口設置
		監査責任者の責務	B		・監査責任者の役割、責任、権限を規定

			C		<ul style="list-style-type: none"> ・第三者機関へ監査依頼している場合は、監査実施規程は不要 ・監査結果に対する対応を規定
		利用者の責務	B		<ul style="list-style-type: none"> ・自身の認証番号やパスワードあるいはICカード等の管理 ・利用時にシステム認証を必ず受けること ・確定操作の実施による入力情報への責任の明示 ・権限を超えたアクセスの禁止・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常、不正アクセスを発見した場合の速やかな運用管理者へ通知 ・離席対策
			C		<ul style="list-style-type: none"> ・利用者が限定される運用の場合、その旨を明記し、責任の所在を明確にする ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常時の対応を規程
④	一般管理における運用管理事項	来訪者の記録・識別・入退の制限等の入退管理規程	B	<ul style="list-style-type: none"> ・IDカード利用による入退者の制限、名札着用の実施 ・PCの盗難防止チェーンの設置 ・防犯カメラの設置 ・施錠 	<ul style="list-style-type: none"> ・入退者の名簿記録と妥当性チェックなどの定期的チェック
			C	施錠	<ul style="list-style-type: none"> ・スタッフの常駐
		情報システムへのアクセス制限の決定方針及び、記録、点検等のアクセス管理	B	<ul style="list-style-type: none"> ・ID、パスワード等により診療録データへのアクセスにおける識別と認証を行う ・監査ログサーバを設置し、アクセスログの収集を行う。 	<ul style="list-style-type: none"> ・管理規則に則ったハードウェア・ソフトウェアの設定を行う ・アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行う ・誰が、いつ、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行う
			C	(上記技術的対策が行えない場合)	<ul style="list-style-type: none"> ・システム操作業務日誌を備え、システムを操作するものはシステム操作業務日誌に操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象を記載する ・システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を確認する
		個人情報を含む記録媒体の管理(保管・授受等)規程	A		<ul style="list-style-type: none"> ・保管、バックアップ作業を的確に行う
		個人情報を含む媒体の廃棄の規程	A	<ul style="list-style-type: none"> ・技術的に安全(再生不可)な方式で破棄を行う 	<ul style="list-style-type: none"> ・情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従事者の特定、具体的な破棄の方法を含めること
		リスクに対する予防、発生時の対応	A		<ul style="list-style-type: none"> ・情報に対する脅威を洗い出し、そのリスク分析の結果に対し予防対策を行う ・リスク発生時の連絡網、対応、代替手段などを規定する
		技術的と運用的対策の分担を定めた文書の管理規程	A	<ul style="list-style-type: none"> ・6章全般に基づいて取られる技術的対策 	<ul style="list-style-type: none"> ・左記の項と対応する、運用事項
無線LANに関する事項	A	<ul style="list-style-type: none"> ・ステルスモード、ANY接続拒否設定、不正アクセス対策、暗号化を行う。 	<ul style="list-style-type: none"> ・利用者への規則の説明を行う ・電波発生機器の利用に当たっての規則を定める 		

		電子署名・タイムスタンプに関する規程	A	<ul style="list-style-type: none"> 電子証明書による電子署名環境 タイムスタンプ付与環境 電子署名の検証環境 	<ul style="list-style-type: none"> 利用する電子証明書がガイドラインが求める信用性を有していることを記載した文書の作成 署名が必要な文書に電子署名があることの確認手順の作成 タイムスタンプを付与する作業手順の作成 電子的な受領文書の電子署名検証手順の作成
⑤	業務委託の安全管理措置	委託契約における安全管理・守秘条項	A		<ul style="list-style-type: none"> 包括的な委託先の罰則を定めた就業規則等で裏付けられた守秘契約を締結すること
		再委託の場合の安全管理措置事項	A		<ul style="list-style-type: none"> 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること
		システム改造及び保守での医療機関関係者による作業管理・監督、作業報告確認	A	<ul style="list-style-type: none"> 保守要員用のアカウントを設定する 保守作業におけるログの取得と保存 	<ul style="list-style-type: none"> 保守要員用のアカウントを確認する 保守作業等の情報システムに直接アクセスする作業の際には、作業内容 作業結果の確認を行うこと 清掃等直接情報システムにアクセスしない作業の場合、定期的なチェックを行うこと 保守契約における個人情報保護の徹底・保守作業の安全性についてログによる確認
⑥	情報および情報機器の持ち出しについて	持ち出し対象となる情報および情報機器の規程	A		<ul style="list-style-type: none"> 組織としてリスク分析を実施し、情報および情報機器の持ち出しに関する方針を運用管理規程で定めること
		持ち出した情報および情報機器の運用管理規程	A		<ul style="list-style-type: none"> 持ち出した情報および情報機器の管理方法を定めること 情報が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること
		持ち出した情報および情報機器への安全管理措置	A	<ul style="list-style-type: none"> 情報機器に対して起動パスワードを設定すること。 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。 	<ul style="list-style-type: none"> 設定にあたっては推定しやすいパスワードなどの利用を避けたり、定期的にパスワードを変更する等の措置を行うこと 持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなアプリケーションをインストールしないこと
		盗難、紛失時の対応策	A	<ul style="list-style-type: none"> 情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。 	<ul style="list-style-type: none"> 情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応
		利用者への周知徹底方法	A		<ul style="list-style-type: none"> 運用管理規程で定めた盗難、紛失時の対応に従業者等に周知徹底し、教育を行うこと
⑦	外部の機関と医療情報を交換する場	安全を技術的、運用的面から確認する規程	A	<ul style="list-style-type: none"> 6.11章に基づいて取られる技術的対策 	<ul style="list-style-type: none"> 左記の項と対応する、運用事項
		リスク対策の検討文書の管理規程	A		<ul style="list-style-type: none"> 上記のリスク対策の検討文書を作成し管理する

	合情報を交換する場合	情報処理事業者との通常運用時、事故処理時それぞれで責任分界点を定めた契約文書の管理と契約状態の維持管理規程	A		<ul style="list-style-type: none"> 医療機関等との間の情報通信に関連する医療機関等、通信事業者やシステムインテグレータ、運用委託事業者等、関連組織の責任分界点、責任の所在を契約書等で明確にすること またその契約状態を維持管理する規程を定めていること
		リモートメンテナンスの基本方針	A	<ul style="list-style-type: none"> 適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。 	<ul style="list-style-type: none"> 遠隔保守を行う事業者との間で、責任分界点、責任の所在を契約書等で明確にすること
		従業者による医療機関等の外部からアクセスする場合の運用管理規程	A	<ul style="list-style-type: none"> 医療機関等の内部のシステムに不正な侵入等を防止する技術的対策 	<ul style="list-style-type: none"> 外部からアクセスを許容する機器及びその状態を規定する 外部からアクセスを許容した機器が、その許容状態を保持しているのかを確認する
⑧	災害等の非常時の対策	BCPの規程における医療情報システムの項	A		<ul style="list-style-type: none"> 医療サービスを提供し続けるためのBCPの一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと
		システムの縮退運用管理規程	A	<ul style="list-style-type: none"> 技術的な縮退運用時機能 	<ul style="list-style-type: none"> システムが縮退運用を行っている際の、運用管理規程
		非常時の機能と運用規程	A	<ul style="list-style-type: none"> 技術的な非常時機能 	<ul style="list-style-type: none"> 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約 「非常時のユーザアカウントや非常時機能」の管理手順
		報告先と内容一覧	A	<ul style="list-style-type: none"> サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、別途定める所管官庁への連絡を行うこと 	
⑨	教育と訓練	マニュアルの整備	A		<ul style="list-style-type: none"> マニュアルの整備
		定期または不定期なシステムの取り扱い及びプライバシー保護に関する研修	A		<ul style="list-style-type: none"> 定期または不定期な電子保存システムの取扱及びプライバシー保護に関する教育、研修
		従事者に対する人的安全管理措置	A		<ul style="list-style-type: none"> 守秘契約、業務規程 退職後の守秘規程 規程遵守の監査
⑩	監査		B		<ul style="list-style-type: none"> 定期的な監査の実施 監査責任者の任命、役割、責任、権限を規定 監査結果の検討、規程見直しといった手順の規定
			C		<ul style="list-style-type: none"> 第三者機関に監査を委託している場合、その旨を記載する
⑪	その他		A		<ul style="list-style-type: none"> 運用管理規程の公開について規定 運用管理規程の改定の規定

付表2 電子保存における運用管理の実施項目例

A：医療機関の規模を問わない
 B：大／中規模病院
 C：小規模病院、診療所 ※「運用管理規程文例」は巻末にまとめる

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	
①	真正性確保	作成者の識別及び認証	B	<ul style="list-style-type: none"> 利用者識別子、パスワードによる識別と認証 	<ul style="list-style-type: none"> 利用者識別子とパスワードの発行、管理 パスワードの最低文字数、有効期間等の規程 認証の有効回数、超過した場合の対処・利用者への認証操作の義務づけ 識別子、パスワードの他人への漏えいやメモ書きの禁止 利用者への教育・緊急時認証の手順規程 	
				<ul style="list-style-type: none"> ログアウト操作、自動ログアウト機能、スクリーンセーブ後の再認証等 	<ul style="list-style-type: none"> 利用者への終了操作義務づけ 離席時の対処の規程と周知 	
			A	<ul style="list-style-type: none"> 運用状況において作成者が自明の場合は、技術的対策なし 	<ul style="list-style-type: none"> 作成責任者を明記すること 定期的な実施状況の監査 	
			情報の確定手順と、作成責任者の識別情報の記録	B	<ul style="list-style-type: none"> 技術的に入力した情報の確定操作を行う機能 	<ul style="list-style-type: none"> 利用者への確定操作法の周知・教育 代行入力の場合、責任者による確定を義務づけ
		B		<ul style="list-style-type: none"> 技術的に情報に作成責任者の識別情報を記録する機能 	<ul style="list-style-type: none"> 利用者への確定操作法の周知・教育 	
		A		<ul style="list-style-type: none"> 運用において確定の状況が自明の場合は、「確定」操作はなし 	<ul style="list-style-type: none"> 「確定」を定義する状況を運用規程に明記する 	
			更新履歴の保存	B	<ul style="list-style-type: none"> 技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能 	<ul style="list-style-type: none"> 利用者への確定操作法の周知・教育
			代行操作の承認記録	A	<ul style="list-style-type: none"> 技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能 	<ul style="list-style-type: none"> 代行者を依頼する可能性のある担当者に、確定の任務を徹底すると同時に適宜履歴の監査を行う
	機器・ソフトウェアの品質管理、動作状況の内部監査規程	A		<ul style="list-style-type: none"> 定期的な機器、ソフトウェアの動作確認。機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスの規定。 		
②	見読性確保	情報の所在管理	A	<ul style="list-style-type: none"> 技術的に情報の論理的所在確認を行う 	<ul style="list-style-type: none"> 情報機器・媒体のリストを作成し、物理的所在場所の確認を行う 	
		見読化手段の管理	A	<ul style="list-style-type: none"> 見読に必要な機器(モニタ、プリンタ等)の整備を行う 	<ul style="list-style-type: none"> 見読化手段の維持、管理(例えば、モニタ・プリンタの管理やネットワークの管理)要件を明記する 	
		見読目的に応じた応答時間とスループット	A	<ul style="list-style-type: none"> 応答時間の確保が出来る、システム構成、機器の選定。 	<ul style="list-style-type: none"> システム利用における見読目的の定義と、システム管理により業務上から要請される応答時間の確保を行う 	
		システム障害対策	A	<ul style="list-style-type: none"> システムの冗長化 	<ul style="list-style-type: none"> システム障害時に備えた機器・システムの維持体制を決める・データのバックアップ 	

③	保存性確保	ソフトウェア・機器・媒体の管理	A		<ul style="list-style-type: none"> 定期的な機器、ソフトウェアの動作確認 媒体の保存場所、その場所の環境、入退出管理
		不適切な保管・取り扱いによる情報の滅失、破壊の防止策	A		<ul style="list-style-type: none"> 作業の管理を行う・データのバックアップを行う 業務担当者の変更に当たっては、教育を行う
		記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止策	A		<ul style="list-style-type: none"> 記録媒体劣化以前の情報の複写を規定
		媒体・機器・ソフトウェアの整合性不備による復元不能の防止策	A	<ul style="list-style-type: none"> マスタDB変更時に過去の情報に対する内容変更が起こらない機能 標準形式でのデータ入出力機能 	<ul style="list-style-type: none"> システムの移行時のデータベースの不整合、機器・媒体の互換性不備に備えたシステム変更 移行時の業務計画の作成・定期的なバグフィックスやウイルス対策の実施
④	相互利用性確保	システムの改修に当たっての、データ互換性の確保策	A	<ul style="list-style-type: none"> 標準的な規約(例えば、HL7、DICOM、HELICS、IHE等)に従った情報形式を持つシステム構築 	<ul style="list-style-type: none"> システム更新時の継続性確保策 異なる施設間の場合、契約により責任範囲を明確にすることを規程
		システム更新に当たっての、データ互換性の確保策	A		
(4)	スキャナ読み取り書類の運用	スキャナ読取の対象にする文書の規程	A		<ul style="list-style-type: none"> 対象文書を定める
		スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者の任命	A	<ul style="list-style-type: none"> 適切な精度のスキャナの使用 	<ul style="list-style-type: none"> スキャナ読み取りの運用管理を規定する
		スキャナ読み取り電子情報への作業責任者の電子署名及び認証業務に関する法律に適合した電子署名・タイムスタンプ	A	<ul style="list-style-type: none"> 電子署名・タイムスタンプ環境の構築 	
		診療の都度、スキャンするタイミングの規程	A	<ul style="list-style-type: none"> タイムスタンプ機能 	<ul style="list-style-type: none"> 情報が作成されてから、または情報入手してから一定期間以内(1~2日程度以内)にスキャンを行うことを運用管理規程で定め、遅滞なくスキャンを行うこと

付表3 外部保存における運用管理の例

A：医療機関の規模を問わない
 B：大／中規模病院
 C：小規模病院、診療所 ※「運用管理規程文例」は巻末にまとめる

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策
①、⑨	管理体制と責任	管理体制の構築、受託する機関の選定、責任範囲の明確化、契約	B		管理体制の構築、受託する機関の評価・選定、契約
			C		管理体制の構築、受託する機関の評価・選定、契約
		受託する機関への監査	A		受託する機関に対する保管記録の監査規程作成、契約
					受託する機関での管理策の承認、実施監査規程作成、契約
		責任の明確化	A		通常運用における責任、事後責任の分界点を定める
		動作の監査	B	委託する機関での送信記録、受託する機関での受信記録の保持	委託する機関での送信記録、受託する機関での受信記録の合致監査
			C	(監査目的に耐える記録レベル、保存期間であること)	監査(上記を含む全)を第三者へ委託した場合は、定期的報告(6ヶ月程度)を受けること
不都合な事態への対処	A		受託する機関との間で、異常時(異常の可能性も含む)の責任対処作業範囲を定める		
②	外部保存契約終了時の処理	A		保管データの破棄契約と管理者による確認、守秘義務契約	
③	真正性確保	相互認証機能の採用	A	SSL/TLSあるいは相互認証付きVPNの使用	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。
		通信上で「改ざんされていない」ことの保証	A	SSL/TLSあるいはメッセージ認証付きのVPNの使用	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。
④	見読性確保	情報の所在管理 見読化手段の管理 見読目的に応じた応答時間とスループット システム障害対策	A		付表2の見読性確保と同じ技術的対策・運用的対策がとられていることの確認
⑤	保存性確保	外部保存を受託する機関での保存確認機能	A	受託する機関との間で、改ざんされることの無いデータとして保存されたことを確認できる機能、たとえばネットワークを介した Strage への保管確認機能、あるいは 保存を委託する機関への保管内容送信機能(1時間～1日単位)	・付表2の保存性確保と同じ技術的対策・運用的対策がとられていることの確認 ・受託先での保存が確認された時点まで委託元でのデータ削除を行わない作業規程
		標準的なデータ形式及び転送プロトコルの採用	A	DICOM、HL7、標準コードの使用 あるいはこれらへの変換機能	
		データ形式及び転送プロトコルのバージョン管理と継続性確保	A		継続性の保証契約を交わす

⑥	診療録等の個人情報を電気通信回線で伝送する間の個人情報保護策	秘匿性の確保のための適切な暗号化	A	メッセージの暗号化が可能な通信手段 暗号の強度は、電子署名法に準じること	
		通信の起点・終点識別のための認証	A	SSL/TLSあるいは相互認証付きVPNの使用 暗号の強度は、電子署名法に準じること	認証局を使う場合は、両機関間でお互いに相手方の証明書を認証可能な認証局を選定する事 双方が合意すれば、特に独立した第三者の認証局である必要性は無い。
⑦	外部保存を受託する機関内での個人情報保護策	外部保存を受託する機関における個人情報保護	A		受託する機関と受託する機関側における業務従事者への教育、守秘義務
		外部保存を受託する機関における診療情報へのアクセス禁止	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログの監査
		外部保存を受託する機関における障害対策時のアクセス通知	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	アクセス許可、秘密保持に関する契約と委託する機関によるアクセスログの監査
		外部保存を受託する機関におけるアクセスログの完全性とアクセス禁止	A	アクセスログファイルへのアクセス制御とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託する機関によるアクセスログへのアクセスの監査
⑧	患者への説明	外部保存を行っている旨を院内掲示等を通じて周知し、同意を得ること	A		外部保存を行っている旨を院内掲示等を通じて周知すること。

用語解説

AES (Advanced Encryption Standard)

無線 LAN の暗号化方式の規格である WPA2 が採用している (WPA2/AES) 米国政府の次世代標準暗号化方式。現在標準暗号として用いられている DES が制定されたのは 1977 年であり、近年のコンピュータの高性能化、暗号理論の発展に伴い、その信頼性は年々低下している。そこで、NIST は DES に代わる次世代の暗号標準として、AES 候補となる暗号方式を全世界から公募した。世界中から集まった 15 の方式が審査を受けていたが、2000 年 10 月に、ベルギーの暗号開発者 Joan Daemen 氏と Vincent Rijmen 氏が開発した「Rijndael」という方式が選ばれた。

IDS (Intrusion Detection System)

通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステム。ネットワーク上を流れるパケットを分析し、パターン照合により不正アクセスと思われるパケットを検出して、管理者に通知する。製品によっては疑わしい通信を切断するなどして防衛措置を講じる場合もある。不正アクセスでよく用いられる手段をパターン化して記録しておき、実際に流れてくるパケットとパターンを比較することによって、正常な通信であるかどうか判断する。

IKE (Internet Key Exchange)

IPsec で暗号化通信を行なうのに先立って、暗号鍵を交換するために利用される通信プロトコル。その場限りの暗号化通信を行なって、IPsec に必要な暗号化アルゴリズムの決定と暗号鍵の共有を行なう。IKE では Diffie-Hellman 鍵交換と呼ばれる手順によって暗号鍵を交換し、IKE 限定の暗号化通信を行なう。その際に IPsec での通信に必要な各種の情報の交換などの手続きが行なわれ、IPsec による通信を開始する。IKE の通信を盗み見られても、それ自体が暗号化されているため、IPsec の通信を解読される恐れはない。

ISDN (Integrated Services Digital Network)

電話や FAX、データ通信を統合して扱うデジタル通信網。日本では NTT が「INS ネット」の名称でサービスを提供している。国際電気通信連合電気通信セクタ (ITU-TS) によって標準化されている。現在各国で提供されているサービスのほとんどはハードウェアとして通常の電話線を使った N-ISDN であり、3 本のチャネル (論理回線) で構成される。通信速度 16kbps の D チャネル (1 本) は制御用、64kbps の B チャネル (2 本) は通信用である。2 回線同時に使用できるので、電話をかけながらインターネットに接続したりできる。また、2 回線を束ねて 128kbps の高速通信を行なうことも可能である。

ISMS (Information Security Management System)

企業などの組織が情報を適切に管理し、機密を守るための包括的な枠組み。コンピュータシステムのセキュリティ対策だけでなく、情報を扱う際の基本的な方針(セキュリティポリシー)や、それに基づいた具体的な計画、計画の実施・運用、一定期間ごとの方針・計画の見直しまで含めた、トータルなリスクマネジメント体系のことを指す。

1999年にイギリス規格協会(BSI)がISMSの標準規格として「BS7799」を策定し、翌2000年、実践規範である「BS7799 Part 1」が国際標準化機構(ISO)によって「ISO/IEC 17799」として国際標準化された。国内では同規格に沿ったガイドラインが2002年に「JIS X 5080」として標準化されている。

これを受けて、日本では、財団法人日本情報処理開発協会(JIPDEC)が企業のISMSがISO/IEC 17799に準拠していることを認証する「ISMS 適合性評価制度」を運用している。JIPDECの定義によれば、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、自らのリスク評価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。

IPsec(Security Architecture for Internet Protocol)

インターネットで暗号通信を行なうための規格。IPのパケットを暗号化して送受信するため、TCPやUDPなど上位のプロトコルを利用するアプリケーションソフトはIPsecが使われていることを意識する必要はない。現在インターネットで使われているIPv4ではオプションとして使用することができるが、次世代のIPv6では標準で実装される。

IP-VPN(Internet Protocol- Virtual Private Network)

通信事業者の保有する広域IP通信網を経由して構築される仮想私設通信網(VPN)のこと。IP-VPNを経由することによって、遠隔地のネットワーク同士をLANで接続しているのと同じように運用することができる。本来、バックボーンがIPベースで運用されているネットワークであれば、インターネットとの接続の有無に関わらずIP-VPNと呼ばれるが、通常は、通信事業者が独自に構築した閉域IP網を介して構築されたものをIP-VPNと呼ぶ。インターネットを介さないIP-VPNは、セキュリティや通信品質を向上させることができる。

IP-VPNサービスとしては、IP網上にネットワーク同士を直結する仮想専用線を構築するものと、仮想ルータを提供してルーティングまでを引き受けるものがあり、後者のサービスが特に注目されている。ルーティングサービスを提供するIP-VPNサービスでは、プライベートIP網内の通信経路探索にMPLSを採用しており、どのVPNの通信であるかを確実に判別することができるため、VPN同士でのプライベートアドレスの衝突や、他VPNへの誤送信などの危険がなくなるよう設計されている。

Kerberos(ケルベロス)

「Kerberos」とは、ギリシャ神話に登場する3つの頭を持った冥界の番犬のこと。暗号による認

証方式の一つで、通信経路上の安全が保障されないインターネットなどのネットワークにおいて、サーバとクライアントの間で身元の確認を行なうのに使う。X Window System の開発で知られるマサチューセッツ工科大学(MIT)の「Athena」プロジェクトによる、認証サービスや関連するプロトコル、プログラムなどの総称である。

秘密鍵暗号(共通鍵暗号)を用いることにより、クライアント/サーバアプリケーションに強固な認証システムを提供できるように設計されている。Kerberos はクライアントとサーバの ID を検証するだけでなく、プライバシーを確保するためとデータの保全のためにクライアントとサーバの間の通信の全てを暗号化する。

L3 スイッチ (Layer 3 switch)

ネットワークの中継機器の一つで、OSI 参照モデルのネットワーク層(第 3 層)のデータでパケットの行き先を判断して転送を行なうもの。ネットワーク層のプロトコルとしては使われるのは IP がほとんどであるため、レイヤ 3 スイッチの多くも IP の情報や機能を利用して経路制御を行なう。レイヤ 3 スイッチは、IP アドレスによる経路制御、ルーティング機能(RIP、OSPF、BGP など)を使用して、パケットを目的の IP アドレスに対応する出力ポートに転送する。

同じくネットワーク層レベルで処理を行う個人・SOHO 向けのルータは IP のみをサポートするが、レイヤ 3 スイッチでは多数のプロトコルをサポートしているものがある。また、プロトコル別にルーティング制御を行なうことができる機器もあり、1 つのレイヤ 3 スイッチで複数のネットワークを形成することができる。レイヤ 3 スイッチはハードウェアレベルでルーティング処理を行っているため、ルーティング速度は接続している回線のスピードと同等となり、ルータと比べて桁違いに高いスループットが得られる。

レイヤ 3 スイッチという名称は OSI 参照モデルによる分類を根拠としているが、詳細な機能は製品によって大きく異なる。高機能なレイヤ 3 スイッチでは、ルータと同等のフィルタリング機能(トランスポート層以上の層に対しても処理する)などを有するものもある。また、カットスルールーティング(ネットワーク層レベルの中継処理を ATM・Ethernet のスイッチング動作に置き換えること)のみを行なう機器もある。レイヤ 3 スイッチは主に企業の基幹ネットワークなど、複数のサブネットを連結する大規模なシステムのルーティングに使用されている。

MAC アドレス (Media Access Control address)

各 Ethernet カードに固有の ID 番号。全世界の Ethernet カードには 1 枚 1 枚固有の番号が割り当てられており、これを元にカード間のデータの送受信が行われる。IEEE が管理・割り当てをしている各メーカーごとに固有な番号と、メーカーが独自に各カードに割り当てる番号の組み合わせによって表される。

PKI (Public Key Infrastructure: 公開鍵基盤)

公開鍵暗号を用いた技術・製品全般を指す言葉。RSA や楕円曲線暗号などの公開鍵暗号

技術、SSL を組みこんだ Web サーバ/ブラウザ、S/MIME・PGP などを使った暗号化電子メール、デジタル証明書を発行する認証局(CA)構築サーバなどが含まれる。

PLC (Power Line Communications: 高速電力線通信)

電力線を通信回線として利用する技術。電気のコンセントに通信用のアダプタ(PLC モデム)を設置してパソコンなどをつなぐことにより、数 Mbps～数百 Mbps のデータ通信が可能となる。ほとんどの建物には電気配線が張り巡らされているため、PLC を使うことにより新たにケーブルなどを敷設することなく手軽に構内通信網を構築できる。また、電力会社の配電網を PLC に利用すれば電力網をそのまま通信インフラとして利用することができ、インターネット接続サービスなどが提供できる。

PREMISs (プレミス)

(財)医療情報システム開発センターが、2009年10月より運用している「医療情報システム安全管理評価制 (Program of Rating Evaluation for Medical Information System Safety control)」の略名。厚生労働省の定める「医療情報システムの安全管理に関するガイドライン」(以下、「安全管理 GL」という)への準拠性を第三者が客観的に評価する制度。PREMISs により、「安全管理 GL」に準じた安全性の担保力を、技術面、運用面の観点から客観的に評価し、システムを利便性と安全性のバランスの取れたものとする事ができる。さらに「安全管理 GL」の管理者向け読本である「医療情報システムを安全に管理するために」で示された、医療機関等の管理者に求められている「善管注意義務」を担保することも目的としている。

S/MIME (Secure Multipurpose Internet Mail Extensions: エスマイム)

電子メールの暗号化方式の標準。RSA Data Security 社によって提案され、IETF によって標準化された。RSA 公開鍵暗号方式を用いてメッセージを暗号化して送受信する。この方式で暗号化メールをやり取りするには、受信者側も S/MIME に対応している必要がある。

SSID (Service Set Identifier)

IEEE 802.11 シリーズの無線 LAN におけるアクセスポイントの識別子。混信を避けるために付けられる名前で、最大 32 文字までの英数字を任意に設定できる。複数のアクセスポイントを設置したネットワークを考慮してネットワーク識別子に拡張したものを ESSID という。現在では ESSID の意味で SSID という語を使う場合が多い。

無線 LAN は電波を使って通信するため、有線 LAN と違って複数のアクセスポイントと交信可能になる「混信」状態が生じる可能性がある。このため、無線 LAN のアクセスポイントと各端末には SSID を設定することができ、SSID が一致する端末としか通信しないようにすることができる。どのアクセスポイントにも接続できる「ANY」という特殊な SSID もあるが、製品によってはセキュリティに配慮して「ANY」設定の端末からの接続を拒否する機能をもったものもある。

無線 LAN ネットワークの識別子としては他に BSSID という 48 ビットの数値があり、こちらはアクセスポイントの MAC アドレスと同じものである。

SSL (Secure Socket Layer)

Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われている WWW や FTP などのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。SSL は公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。OSI 参照モデルではセッション層(第 5 層)とトランスポート層(第 4 層)の境界で動作し、HTTP や FTP などの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

SSL は公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。OSI 参照モデルではセッション層(第 5 層)とトランスポート層(第 4 層)の境界で動作し、HTTP や FTP などの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

SSL-VPN (Secure Socket Layer Virtual Private Network)

暗号化に SSL を利用する VPN 技術。多くの Web ブラウザやメールソフトは標準で SSL に対応しているため、リモートアクセス用途などで手軽に導入できる。

インターネットなどの公衆回線網に暗号化された仮想回線を構築し、企業の拠点間などを安全に結ぶ技術を VPN という。従来は IPsec などを使いネットワーク層レベルで仮想的な回線を用意し、アプリケーションからは透過的にネットワークを利用できる技術が主流だったが、このアプローチは汎用性が高い反面、回線の両端に専用の VPN 装置を用意する必要があるなど本格的で、導入に手間とコストがかかった。

SSL-VPN は WWW の暗号化などで標準的に用いられている SSL で仮想回線を構築する技術であり、サーバ側には SSL-VPN 装置が必要だが、クライアント側はアプリケーションが SSL に対応していればよく、簡単に導入できる。アプリケーションが個別に SSL を実装していなければ利用できないが、主要な Web ブラウザやメールソフトは HTTPS や POP over SSL に対応しているため、イントラネットの Web 閲覧やメールの送受信などに用途を限れば十分実用になる。出先から社内に接続するといったリモートアクセス用途に適した VPN 技術である。

TLS (Transport Layer Security)

インターネット上で情報を暗号化して送受信するプロトコルの一つ。現在インターネットで広く使われている WWW や FTP などのデータを暗号化し、プライバシーに関わる情報やクレジッ

トカード番号、企業秘密などを安全に送受信することができる。TLS は公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができる。OSI 参照モデルではトランスポート層(第 4 層)にあたり、HTTP や FTP などの上位のプロトコルを利用するアプリケーションソフトからは、特に意識することなく透過的に利用することができる。

VPN (Virtual Private Network)

公衆回線をあたかも専用回線であるかのように利用できるサービス。企業内ネットワークの拠点間接続などに使われ、専用回線を導入するよりコストを抑えられる。データ通信の拠点間接続サービスのことを指し、企業内 LAN を通信キャリアの持つバックボーンネットワークを通じて相互に接続するサービスをいう。かつては各拠点の間に専用線を導入して直接通信していたが、キャリアのバックボーンに「相乗り」することにより低コストで拠点間接続が可能となる。バックボーンでは様々な企業のデータが混在して流れることになるが、データは認証や暗号化で厳重に保護・管理されるため、混信や漏洩、盗聴などの危険性は低い。最近ではバックボーンにインターネットを利用する「インターネットVPN」も登場しており、通常のVPNサービスよりもさらに低コストでの利用が可能だが、インターネットの特性上、セキュリティや通信品質の確保はキャリアの通信網を利用するよりも難しくなる。

Winny (ウィニー)

日本で開発されたファイル交換ソフトの一つ。高い匿名性と、独自の P2P 型匿名掲示板システムが特徴。Winny は中央サーバを持たない純粋型の P2P ソフトで、所持ファイルのリストなどの情報は利用者間をバケツリレー式に転送される。ユーザ ID ではなく、どのファイルがどこから送受信されているのか利用者はわからないようになっている。ただし、自分がダウンロードを指定したファイルの受信状況だけは知ることができる。ユーザを指定してメッセージを送信したり、共有ファイルのリストを見たり、ダウンロードを指定したりすることはできない。利用者として利用実態を割り出しやすい WinMX など他のファイル共有ソフトが著作権侵害などによる逮捕者を出す中で急激に利用者を増やしていったが、2003 年後半以降、Winny を利用した著作権侵害や児童ポルノの配布などで逮捕者が出続けている。また、2004 年 5 月には、著作権侵害行為を幫助した疑いで、開発者の 47 氏が逮捕されたが、2009 年 10 月に無罪の高裁判決が出ている。ファイル共有ソフトの開発者の逮捕は世界的にも稀な事例である。

WPA (Wi-Fi Protected Access)

無線 LAN の業界団体 Wi-Fi Alliance が 2002 年 10 月に発表した、無線 LAN の暗号化方式の規格。従来採用されてきた WEP の弱点を補強し、セキュリティ強度を向上させたもの。従来の無線 LAN に採用されてきた暗号化規格である WEP には様々な脆弱性が発見・報告

されており、WEP に替わる暗号化が待望されていた。WPA は、従来の SSID と WEP キーに加えて、ユーザ認証機能を備えた点や、暗号鍵を一定時間毎に自動的に更新する「TKIP」(Temporal Key Integrity Protocol)と呼ばれる暗号化プロトコルを採用するなどの改善が加えられている。

WPA2 (Wi-Fi Protected Access 2)

無線 LAN の業界団体 Wi-Fi Alliance が 2004 年 9 月に発表した、無線 LAN の暗号化方式の規格。2002 年に発表された WPA の新バージョンで、より強力な AES 暗号に対応している。米標準技術局(NICT)が定めた暗号化標準の「AES」を採用しており、128～256 ビットの変長鍵を利用した強力な暗号化が可能となっている。それ以外の仕様は WPA とほとんど変わらない。WPA 互換モードが用意されており、WPA2 対応機器であれば従来使われてきた WPA 対応機器とも通信できる。

タイムスタンプ (Time stamp)

電子データに属性として付与される時刻情報。そのデータの作成や最終更新、最終アクセスなどの日時を記録するに利用される。ハードディスクなどでファイルやフォルダに記録されているものが馴染み深い。

また、法的な文書や契約書など公正性を求められる電子書類を扱う際に、ある時点で書類が存在したことやその時点から改ざんされていないことを証明するために、第三者機関の発行した日時情報を電子署名化して書類に添付したものをタイムスタンプという。

パーソナルファイアウォール (Personal firewall)

個人向けのファイアウォール製品。自宅でインターネットにブロードバンド接続しているようなユーザが、ウイルスやクラッカーなどの脅威から身を守るために導入する。

ファイアウォールとは、コンピュータやネットワークにインターネットを通じて外部から侵入してくるウイルス(ワーム)やクラッカーをシャットアウトするソフトウェアやハードウェアのことで、かつては企業のネットワークを守るための高額で高性能・高機能な製品が主流だったが、最近ではブロードバンドで常時接続する個人ユーザが増えたため、機能を限定して低価格にした個人向けの製品が増えている。

ファイル交換ソフト (File exchange software)

インターネットを介して不特定多数のコンピュータの間でファイルを共有するソフト。著作権侵害をはじめとする違法な情報流通の温床になっているとして非難の対象となっている。日本では、中央サーバ型としては WinMX が、純粹型としては Winny が広く使われており、WinMX では 2001 年 11 月に、Winny では 2003 年 11 月に著作権侵害の疑いで逮捕者が出ている。

インターネット VPN (Internet VPN)

インターネットを経由して構築される仮想的なプライベートネットワーク(VPN)のこと。インターネット VPN を経由することによって、機密を保持したまま遠隔地のネットワーク同士を LAN で接続しているのと同じように運用することができる。

インターネット VPN ではバックボーンにインターネットを使うため、回線を維持するための費用が非常に低く、専用線などと比べて極めて低コストで運用することができる。インターネットを流れるデータはそのままでは盗聴されてしまう恐れがあるため、インターネット VPN では IPsec を使用して通信内容を暗号化し、機密性の高いデータを通信できるようにしている。

IP ベースのネットワークを利用した仮想 LAN としては他に IP-VPN があるが、一般にコストではインターネット VPN が優れ、品質や信頼性では IP-VPN が優れているとされる。

以上

<参考文献>

I T用語辞典 e-words (<http://e-words.jp>)

保健医療福祉分野のプライバシーマーク認定指針

2010年4月1日 第2.1版

編 纂 財団法人医療情報システム開発センター
プライバシーマーク付与認定審査室
〒113-0024
東京都文京区西片1丁目17番8号 KSビル3F
TEL 03-5805-8207
FAX 03-5805-8209
<http://privacy.medis.jp>

— 禁 無 断 転 載 —

MEDIS⁺
DC