

# 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

(案)

平成\*年\*月

厚生労働省

## 改定履歴

版数	日付	内容
第1版	平成17年3月	<p>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」及び、平成14年3月通知「診療録等の保存を行う場所について」に基づき作成された各ガイドラインを統合。</p> <p>新規に、法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン（紙等の媒体による外部保存を含む）、及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインとして作成。</p>
第2版	平成19年3月	<p>平成18年1月の高度情報通信技術戦略本部（IT戦略本部）から発表された「IT新改革戦略」（平成18年1月）において、「安全なネットワーク基盤の確立」が掲げられたこと、及び、平成17年9月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係わる基本的考え方」において、医療をIT基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療におけるIT基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められたことを踏まえ、</p> <p>(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10章 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」として取りまとめる等の改定を実施。</p> <p>(2) 自然災害・サイバー攻撃によるIT障害対策等について、医療のITへの依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9章 災害等の非常時の対応」を新設して取りまとめる等の改定を実施。</p>

## 【目次】

1	はじめに.....	1
2	本指針の読み方.....	4
3	本ガイドラインの対象システム及び対象情報.....	6
4	電子的な医療情報を扱う際の責任のあり方.....	9
4.1	医療機関等の管理者の情報保護責任について.....	10
4.2	責任分界点について.....	12
4.3	例示による考え方の整理.....	15
5	情報の相互利用性と標準化について.....	19
5.1	標準的な用語集やコードセットの利用.....	19
5.2	国際的な標準規格への準拠.....	20
6	情報システムの基本的な安全管理.....	21
6.1	方針の制定と公表.....	21
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.....	22
6.2.1	ISMS 構築の手順.....	22
6.2.2	取扱い情報の把握.....	23
6.2.3	リスク分析.....	24
6.3	組織的安全管理対策（体制、運用管理規程）.....	27
6.4	物理的安全対策.....	29
6.5	技術的安全対策.....	30
6.6	人的安全対策.....	37
6.7	情報の破棄.....	39
6.8	情報システムの改造と保守.....	40
6.9	情報および情報機器の持ち出しについて.....	42
6.10	災害等の非常時の対応.....	44
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.....	48
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.....	65
7	電子保存の要求事項について.....	67

7.1	真正性の確保について.....	67
7.2	見読性の確保について.....	84
7.3	保存性の確保について.....	88
8	診療録及び診療諸記録を外部に保存する際の基準 .....	94
8.1	電子媒体による外部保存をネットワークを通じて行う場合.....	94
8.1.1	電子保存の3基準の遵守 .....	95
8.1.2	外部保存を受託する機関の選定基準および情報の取り扱いに関する基準.....	96
8.1.3	個人情報の保護.....	104
8.1.4	責任の明確化 .....	107
8.1.5	留意事項.....	108
8.2	電子媒体による外部保存を可搬型媒体を用いて行う場合 .....	109
8.3	紙媒体のまま外部保存を行う場合 .....	109
8.4	外部保存全般の留意事項について.....	110
8.4.1	運用管理規程 .....	110
8.4.2	外部保存契約終了時の処理について.....	111
8.4.3	保存義務のない診療録等の外部保存について .....	112
9	診療録等をスキャナ等により電子化して保存する場合について.....	113
9.1	共通の要件.....	113
9.2	診療等の都度スキャナ等で電子化して保存する場合 .....	116
9.3	過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合 .....	117
9.4	(補足) 運用の利便性のためにスキャナ等で電子化をおこなうが、紙等の媒体もそのまま保存をおこなう場合 .....	119
10	運用管理について .....	121
付則1	電子媒体による外部保存を可搬型媒体を用いて行う場合.....	130
付則2	紙媒体のまま外部保存を行う場合 .....	139
付表1	一般管理における運用管理の実施項目例	
付表2	電子保存における運用管理の実施項目例	
付表3	外部保存における運用管理の例	
付録	(参考) 外部機関と診療情報等を連携する場合に取り決めるべき内容	

## 1 はじめに

平成11年4月の通知「診療録等の電子媒体による保存について」（平成11年4月22日付け健政発第517号・医薬発第587号・保発第82号厚生省健康政策局長・医薬安全局長・保険局長連名通知）、平成14年3月通知「診療録等の保存を行う場所について」（平成14年3月29日付け医政発0329003号・保発第0329001号厚生労働省医政局長・保険局長連名通知）により、診療録等の電子保存及び保存場所に関する要件等が明確化された。その後、情報技術の進歩は目覚しく、社会的にも e-Japan 戦略・計画を始めとする情報化の要請はさらに高まりつつある。平成16年11月に成立した「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号。以下「e-文書法」という。）によって原則として法令等で作成または保存が義務付けられている書面は電子的に取り扱うことが可能となった。

平成15年6月より厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」においては、医療情報の電子化についてその技術的側面及び運用管理上の課題解決や推進のための制度基盤について検討を行い、平成16年9月最終報告が取りまとめられた。

上記のような情勢に対応するために、これまでの「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ガイドライン」（平成11年4月22日付け健政発第517号・医薬発第587号・保発第82号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付。）、「診療録等の外部保存に関するガイドライン」（平成14年5月31日付け医政発第0531005号厚生労働省医政局長通知）を見直し、さらに、個人情報保護に資する情報システムの運用管理にかかわる指針と e-文書法への適切な対応を行うための指針を統合的に作成することとした。なお、平成16年12月には「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」が公表され、平成17年4月の「個人情報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。）の全面実施に際しての指針が示されたが、この指針では情報システムの導入及びそれに伴う外部保存を行う場合の取扱いに関しては本ガイドラインで示すとされている。

今回のガイドラインは、病院、診療所、薬局、助産所等（以下「医療機関等」という。）における診療録等の電子保存に係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及した。従って本ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意されたい。

また、本ガイドラインは「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」と対になるものであるが、個人情報保護は決して情報システムにかかわる対策だけで達成されるものではない。従って、本ガイドラインを使用する場合、情報システムだけの担当者であっても、「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」を十分理解し、情報システムにかかわらない部分でも個人情報保護に関する対策が達成されていることを確認することが必要である。

## 改定概要

### 【第2版】

本ガイドライン初版公開（平成17年3月）後の平成18年1月、高度情報通信技術戦略本部（IT戦略本部）から、「IT新改革戦略」が発表された。IT新改革戦略では、「e-Japan戦略」に比べて医療情報の活用が重視されている。様々な医療情報による連携がメリットをもたらすものと謳い、連携の手法、またその要素技術について種々の提言がなされており、そのひとつに「安全なネットワーク基盤の確立」が掲げられている。

他方、平成17年9月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係わる基本的考え方」において、医療をIT基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療におけるIT基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められた。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では、「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」、「(2) 自然災害・サイバー攻撃によるIT障害対策等」の検討を行い、本ガイドラインの改定を実施した。

「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」では、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10章 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」として取りまとめている。さらには、関連個所として「8章 診療録及び診療諸記録を外部に保存する際の基準」の中のネットワーク関連の要件について6.10章を参照すること、医療機関等における当該ネットワークの運用の指針となる「10章 運用管理について」の一部改定を実施している。

また、「(2) 自然災害・サイバー攻撃によるIT障害対策等」では、医療のITへの依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9章 災害等の非常時の対応」を新設して取りまとめ、情報セキュリティを実践的に運用して行くための考え方として「6.2章 医療機関における情報セキュリティマネジメント（ISMS）の実践」の概念を取り入れ、「10章 運用管理について」も該当個所の一部追記を行った。

なお、本ガイドライン公開後に発出、改正等がなされた省令・通知等についても制度上の要求事項として置き換えを実施している。基本的要件について変更はないが、制度上要求される法令等が変更されている点に注意されたい。

**【第 3 版】**

## 2 本指針の読み方

本指針は次のような構成になっている。医療機関等の責任者、情報システム管理者、またシステム導入業者が、それぞれ関連する個所を理解した上で、個々の対策を実施することを期待する。

なお、本指針では医療情報、医療情報システムという用語を用いているが、これは患者を対象とする医療に関して、患者情報（個人識別情報）を含む情報及びその情報を扱うシステムという意味で用いている。

### 【1章～6章】

個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容を含んでいる。

### 【7章】

保存義務のある診療録等を電子的に保存する場合の指針を含んでいる。

### 【8章】

保存義務のある診療録等を医療機関等の外部に保存する場合の指針を含んでいる。

### 【9章】

e-文書法に基づいてスキャナ等により電子化して保存する場合の指針を含んでいる。

### 【10章】

運用管理規程に関する事項について記載されている。主に電子保存や外部保存を行う場合の運用管理規程の作成に関する指針であるが、電子保存や外部保存を行わない場合でも参考にされたい。

なお、本指針の大部分は法律、厚生労働省通知、他の指針等の要求事項に対して対策を示すことを目的としており、そのような部分ではおおむね、以下の項目にわけて説明をしている。

#### A. 制度上の要求事項

法律、通知、他の指針等を踏まえた要求事項を記載している。

#### B. 考え方

要求事項の解説及び原則的な対策について記載している。



### C. 最低限のガイドライン

Aの要求事項を満たすためにならず実施しなければならない事項を記載している。

この項にはいくつかの対策の中の一つを選択する場合もあるが、選択を明記している場合以外はすべて実施しなければならない対策である。なお、この項の対策にあつては医療機関等の規模により実際の対策が異なる可能性がある。後述するように付表の運用管理表を活用し、適切な具体的対策を採用されたい。

### D. 推奨されるガイドライン

実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解が得やすい対策を記載している。

また、最低限のシステムでは使用されていない技術で、その技術を使用する上で一定の留意が必要となる場合についての記載も含んでいる。

なお、巻末の3つの付表は安全管理上の要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされてはじめて有効なものとなるが、技術的対策には複数の選択肢があることが多く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。

1. **運用管理項目**：安全管理上の要求事項で多少とも運用的対策が必要な項目
2. **実施項目**：上記管理項目を実施レベルに細分化したもの
3. **対象**：医療機関等の規模の目安
4. **技術的対策**：技術的に可能な対策、ひとつの実施項目に対して選択可能な対策を列挙した
5. **運用的対策**：4. の技術的対策をおこなった場合に必要な運用的対策の要約
6. **運用管理規程文例**：運用的対策を規程に記載する場合の文例

各機関等は実施項目に対して採用した技術的対策に応じた運用的対策を運用管理規程に含め、実際に規程が遵守されて運用されていることを確認することで、実施項目が達成されることになる。また技術的対策を選択する前に、それぞれの運用的対策を検討することで、自機関等で運用可能な範囲の技術的対策を選択することが可能である。一般に運用的対策の比重を大きくすれば情報システムの導入コストは下がるが、技術的対策の比重を大きくすれば利用者の運用的な負担は軽くなる。従って適切なバランスを求めることは非常に重要なので、これらの付表を活用されることを期待する。

### 3 本ガイドラインの対象システム及び対象情報

本ガイドラインは保存システムだけではなく、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、保守及び廃棄にかかわる人または組織を対象としている。ただし以下の3つの章は対象となる文書等が一部限定されている。

第7章の「電子保存の要求事項について」、第8章の「診療録及び診療諸記録を外部に保存する際の基準」、及び第9章の「診療録等をスキャナ等により電子化して保存する場合について」は、e-文書法の対象範囲となる医療関係文書等として、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成17年厚生労働省令第44号）、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成17年3月31日付け医政発第0331009号・薬食発第0331020号・保発第0331005号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下「施行通知」という。）及び「「診療録等の保存を行う場所について」の一部改正について」（平成17年3月31日付け医政発第0331010号・保発第0331006号厚生労働省医政局長・保険局長連名通知。以下「外部保存改正通知」という。）で定められた文書等を対象としている。

1. 第7章及び第9章の対象文書等（但し、※処方せんについては施行通知第二2（4）の要件を充足のこと。）

#### ○施行通知 第二 2（1）

- 一 医師法(昭和23年法律第201号)第24条の規定による診療録
- 二 歯科医師法(昭和23年法律第202号)第23条の規定による診療録
- 三 保健師助産師看護師法(昭和23年法律第203号)第42条の規定による助産録
- 四 医療法（昭和23年法律第205号）第52条の規定による財産目録及び貸借対照表並びに損益計算書
- 五 歯科技工士法(昭和30年法律第168号)第19条の規定による指示書
- 六 薬剤師法(昭和35年法律第146号)第28条の規定による調剤録
- 七 外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和62年法律第29号）第11条の規定による診療録
- 八 救急救命士法(平成3年法律第36号)第46条の規定による救急救命処置録
- 九 医療法施行規則（昭和23年厚生省令第50号）第30条の23第1項及び第2項の規定による帳簿
- 十 保険医療機関及び保険医療養担当規則(昭和32年厚生省令第15号)第9条の規定による診療録等
- 十一 保険薬局及び保険薬剤師療養担当規則(昭和32年厚生省令第16号)第6条の規定

による調剤録

- 十二 臨床検査技師、衛生検査技師等に関する法律施行規則（昭和33年厚生省令第24号）第12条の3の規定による書類
- 十三 医療法（昭和23年法律第205号）第21条第1項の規定による記録（同項第9号に規定する診療に関する諸記録のうち医療法施行規則第20条第10号に規定する処方せんに限る。）、第22条の規定による記録（同条第2号に規定する診療に関する諸記録のうち医療法施行規則第21条の5第2号に規定する処方せんに限る。）、及び第22条の2の規定による記録（同条第3号に規定する診療に関する諸記録のうち医療法施行規則第22条の3第2号に処方せんに限る。）※
- 十四 薬剤師法(昭和35年法律第146号)第27条の規定による処方せん※
- 十五 保険薬局及び保険薬剤師療養担当規則(昭和32年厚生省令第16号)第6条の規定による処方せん※
- 十六 医療法(昭和23年法律第205号)第21条第1項の規定による記録（医療法施行規則第20条第10号に規定する処方せんを除く。）、第22条の規定による記録（医療法施行規則第21条の5第2号に規定する処方せんを除く。）、及び第22条の2の規定による記録（医療法施行規則第22条の3第2号に規定する処方せんを除く。）
- 十七 歯科衛生士法施行規則(平成元年厚生省令第46号)第18条の規定による歯科衛生士の業務記録

○施行通知 第二 3

診療放射線技師法（昭和26年法律第226号）第28条第1項の規定による照射録

2. 第8章の対象文書等

○外部保存改正通知 第1

- 1 医師法(昭和23年法律第201号)第24条に規定されている診療録
- 2 歯科医師法(昭和23年法律第202号)第23条に規定されている診療録
- 3 保健師助産師看護師法(昭和23年法律203号)第42条に規定されている助産録
- 4 医療法（昭和23年法律第205号）第52条に規定されている財産目録及び貸借対照表並びに損益計算書
- 5 医療法(昭和23年法律第205号)第21条、第22条及び第22条の2に規定されている診療に関する諸記録及び同法第22条及び第22条の2に規定されている病院の管理及び運営に関する諸記録
- 6 歯科技工士法(昭和30年法律第168号)第19条に規定されている指示書
- 7 外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和62年法律第29号）第11条に規定されている診

## 療録

- 8 救急救命士法(平成3年法律第36号)第46条に規定されている救急救命処置録
- 9 医療法施行規則(昭和23年厚生省令第50号)第30条の23第1項及び第2項に規定されている帳簿
- 10 保険医療機関及び保険医療養担当規則(昭和32年厚生省令第15号)第9条に規定されている診療録等
- 11 臨床検査技師、衛生検査技師等に関する法律施行規則(昭和33年厚生省令第24号)第12条の3に規定されている書類
- 12 歯科衛生士法施行規則(平成元年厚生省令第46号)第18条に規定されている歯科衛生士の業務記録
- 13 診療放射線技師法(昭和26年法律第226号)第28条に規定されている照射録

## 4 電子的な医療情報を扱う際の責任のあり方

医療に関わるすべての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、情報の取扱いも同様である。

情報の取扱いについては、情報が適切に収集され、必要に応じて遅滞なく利用できるように適切に保管され、不要になった場合に適切に廃棄されることで、刑法等に定められている守秘義務、個人情報保護に関する諸法および指針の他、診療情報の扱いに係わる法令、通知、指針等により定められている要件を満たすことが求められる。故意にこれらの要件に反する行為を行えば刑法上の秘密漏示罪で犯罪として処罰される場合があるが、診療情報等については過失による漏えいや目的外利用も同様に大きな問題となりうるから、いずれにしろそのような事態が生じないよう適切な管理をする必要がある。問題はいかなる管理が適切であるか否かであるが、法律的な用語では、管理者に善良なる管理者の注意義務（善管注意義務）を果たすことが求められる。その具体的内容は、扱う情報や状況によって異なるものであり、本ガイドラインは、医療情報を電子的に取り扱う際の善管注意義務をできるだけ具体的に示したものである。

医療情報を電子的に取り扱う場合といっても、本来、医療情報の価値と重要性はその媒体によって変化するものではないから、医療機関等の管理者は、そもそも紙やフィルムによる記録を院内に保存する場合と少なくとも同等の善管注意義務を負うと考えられる。

ただし、電子化された情報は、紙の媒体やフィルムなどに比べてその動きが一般の人にとって分かりにくい側面があること、漏えい等の事態が生じた場合に一瞬かつ大量に情報が漏えいする可能性が高いこと、さらに医療者が情報取扱の専門家とは限らないためその安全な保護に慣れていないケースが多いことなど、固有の特殊性もある。したがって、それぞれの医療機関等がその事情によりメリット・デメリットを勘案して電子化の実施範囲及びその方法を検討し、導入するシステムの機能や運用計画を選択して、それに対し求められる安全基準等への対応を決める必要がある。

また、昨今のブロードバンドに代表されるようなネットワークおよびその技術の進展から、電子化された医療情報が医療機関等の施設内だけに存在するという状況から、空間的境界を越えてネットワーク上に広がって存在することも現実のものとなってきた。

このような状況の下では、医療情報の管理責任が医療機関等の管理ばかりでなく、ネットワーク上の空間を提供する事業者やネットワークを提供する通信事業者等にもまたがるようになる。その際、必要となる新たな概念としては責任分界点が挙げられる。

本章では、電子的な医療情報を取り扱う際の責任のあり方として、医療機関等の管理者の責任の内容と範囲および他の医療機関等や事業者の情報処理の委託や他の業務の委託に付随して医療情報を提供する場合と第三者提供した場合の責任分界点について整理する。

## 4.1 医療機関等の管理者の情報保護責任について

医療機関等の管理者が医療情報を保護するべく善管注意義務を果たすためには、さまざまな局面で注意を払う必要がある。ここでは、医療情報保護の体制を構築し管理する局面での責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合にいかなる対処をすべきかという意味での責任とに分けて解説する。便宜上、本ガイドラインでは前者を通常運用における責任、後者を事後責任とする。

### (1) 通常運用における責任について

ここでいう通常運用における責任とは、医療情報の適切な保護のために医療機関等の管理者が何をすべきかを示す概念である。それは何よりも適切な情報管理ということになるが、実際には、単に適切な情報管理を行っているばかりでなく、そういう体制がきちんととられていることを患者をはじめとする外部に示す責任（説明責任）と、定期的に情報保護システムを評価し改善を図る責任を含む必要がある。

そこで、本ガイドラインにおける医療機関等の管理者の通常運用における責任は、「説明責任」、「管理責任」、「定期的に見直し必要に応じて改善を行う責任」に3分し、以下にそれぞれの責任内容を整理する。

#### ① 説明責任

電子的に医療情報を取り扱うシステムの機能や運用計画が、その取り扱いに関する基準を満たしていることを患者等に説明する責任である。

説明責任を果たすためには、システムの仕様や運用計画を明確に文書化する必要がある。また、仕様や計画が当初の方針の通りに機能しているかどうかを定期的に監査し、その結果もあいまいさのない形で文書化し、また監査の結果問題があった場合は、真摯に対応するのはもちろんのこと、その対応の記録も文書化し、第三者が検証可能な状況にすることが必要である。

#### ② 管理責任

当該システムの運用管理を医療機関等が行う責任である。医療情報を取り扱うシステムの管理を請負事業者にまかせきりにしているだけでは、これを果たしたことはない。少なくとも管理状況の報告を定期的を受け、管理に関する最終的な責任の所在を明確にする等の監督を行う必要がある。

個人情報保護法上は個人情報保護の担当責任者を定める必要があり、電子情報化された個人情報の保護について一定の知識を有する担当責任者を決めて、請負事業者との対応にあたる必要がある。

#### ③ 定期的に見直し必要に応じて改善を行う責任

当該情報システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任である。特に、情報保護に関する技術は日進月歩であり、旧態依然の情報保護体制ではすぐに時代遅れになる可能性がある。

従って、医療機関等の管理者は、医療情報保護のシステムの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う必要がある。

## (2) 事後責任について

### ① 説明責任

医療情報について何らかの事故（典型的には漏えいの事態）が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明する責任がある。

説明は個々の患者に対するものであると同時に、特に医療機関等は一定の公共性を有しているため、監督機関である行政機関や社会への説明・公表が求められている。

### ② 善後策を講ずる責任

医療情報について何らかの事故が生じた場合、医療機関等の管理者には善後策を講ずる責任が発生する。

その責任は、1) 原因を追及し明らかにする責任、2) 損害を生じさせた場合にはその損害填補責任、3) 再発防止策を講ずる責任に分けられる。

事故が、適切な委託契約に基づき医療情報の処理を委託した事業者の責任による場合、法律上、医療機関等の管理者の善管注意義務については、委託先の事業者の選任監督に適切な注意を払っていれば責任はないことになるが、本ガイドラインの下では、患者に対する関係では、選任監督の注意を払っていてもなお上記3つの意味での善後策を講ずる責任を免れるものではない。

本章冒頭に述べたように、医療機関等では医療情報の管理を医療機関等の管理者の責任において行うことが求められており、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、管理者の責任を免れさせるのは不相当と考えられるからである。また、現実的にも、委託先の事業者が医療情報のすべてを管理しているとは限らないから、事故を契機として、医療情報保護の仕組み全体について善後策を講ずる責任は医療機関等の管理者が負うほかないこともある。

ただし、事故の原因が委託先の事業者にある場合に、医療機関等と当該事業者との間の責任分担をどのようにするかはまた別の問題であり、この問題は次の責任分界点の項目で扱う。

## 4.2 責任分界点について

医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託（第三者委託）と第三者提供の2種類があり、医療機関等の管理者の責任のあり方には大きな違いがある。

委託の場合、それが第三者委託と呼ばれることがあるにしても、医療情報は医療機関等の管理者の業務遂行目的のために委託されるのであり、大きな意味で管理者の支配下にある。前項で述べたように、本ガイドラインでは、患者に対する関係では、委託先の事業者の過失による事故についても医療機関等の管理者が責任を免れるものではないと整理したところでもある。

これに対し、医療情報の第三者提供は第三者が何らかの目的で医療情報を利用するために行われるものであり、提供された部分の情報については、もはや管理者ではなく第三者に情報を適切に保護する責任が生ずる。医療機関等の管理者にとっては、原則として、第三者提供の正当性だけが問題となり、適切な第三者提供がなされる限り、その後の情報保護に関する責任は医療機関等の管理者から離れることになる。

ただし、情報の特異な性格のため、医療機関等の側で当該情報を削除しない限り、情報が第三者提供されたからといってなお医療機関等のもとにも残るため、それに関し適切な情報管理責任が残ることはいうまでもない。さらに、情報処理関連事業者の手を経て情報提供が行われる場合には、いかなる時点で、第三者に提供されたことになるかということ を明らかにすべきである。

### A. 委託

委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は患者に対する関係では、委託先の事業者の助けを借りながら、前項に掲げた説明責任・管理責任・定期的に見直し必要に応じて改善を行う責任を果たす義務を負い、万一、何らかの事故が生じた場合にも、同様に委託先の事業者と連携しながら説明責任と善後策を講ずる責任を果たす必要がある。

ただし、これとは別に、委託先事業者の責任による事故が生じた場合については、善後策を講ずる責任を医療機関等と委託先事業者との間でいかに分担するか、委託契約で明記しておくべき事項であり、以下にその原則を掲げる。

#### (1) 通常運用における責任について

##### ① 説明責任

医療情報を実際に扱う委託先事業者と医療機関等の管理者との間における説明責任の分担については、次のように考えられる。

患者等に対し、いかなる内容の医療情報保護のシステムが構築されどのように機能しているかの説明責任は、いうまでもなく医療機関等の管理者にある。



ただし、医療機関等の管理者が説明責任を果たすためには、委託先事業者による情報提供が不可欠の場合があり、委託先事業者は医療機関等の管理者に対し説明責任を負うとよい。委託先事業者に対し適切な情報提供義務・説明義務を委託契約事項に含め、その履行を確保しておく必要がある。

## ② 管理責任

同様に、管理責任の分担については、次のように考えられる。

管理責任を負う主体はやはり医療機関等の管理者にある。しかし、現実に情報処理に当たりその安全な保守作業等を行うのは、委託先事業者である場面が多いと考えられる。医療機関等の管理者としては、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要がある。

## ③ 定期的に見直し必要に応じて改善を行う責任

当該システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任の分担、また、情報保護に関する技術進展に配慮した定期的な再評価・再検討について委託先事業者との契約事項に含めるべきである。

## (2) 事後責任について

### ① 説明責任

前項で述べたように、医療情報について何らかの事故（典型的には漏えいの事態）が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明する責任が求められている。

しかし、情報に関する事故は、説明に際して委託先事業者の情報提供や分析が不可欠な場面が多いと考えられる。そのため予め可能な限りの事態を予想し、委託先事業者との間で、説明責任についての分担を契約事項に含めるべきである。

### ② 善後策を講ずる責任

前項で述べたように、医療情報について何らかの事故が生じた場合、医療機関等の管理者には善後策を講ずる責任が発生する。

その責任は、1) 原因を追及し明らかにする責任、2) 損害を生じさせた場合にはその損害填補責任、3) 再発防止策を講ずる責任に分けられる。

事故が委託先事業者の業務範囲と関係する場合、委託先事業者との協力と責任分担の下に上記の責任を果たす必要がある。

既に述べたように、患者に対する関係では、医療機関等の管理者は、委託先事業者の選任監督に十分な注意を払っている場合でも善後策を講ずる責任を免れることはできない。ただし、委託先事業者との間での責任分担はそれとは別の問題であり、特に、

事故が委託先事業者の責任で生じた場合、医療機関等の管理者がすべての責任を負うことは、原則としてあり得ない。

しかし、医療情報について何らかの事故が生じた場合、医療機関等と委託先事業者の間で責任の押し付け合いをするよりも、まず原因を追及し明らかにすること、そして再発防止策を講ずることが重要であるため、委託契約においては、医療機関等と委託先事業者が協力してこれらの措置を優先させることを明記しておく必要がある。委託内容によっては、より詳しく委託先事業者の責任での原因追及と再発防止策の提案義務を明記することも考えられる。

損害填補責任の分担については、事故の原因が委託先事業者にある場合、最終的には委託先事業者が負うのが原則である。ただし、この点は、原因がどの程度のものかや、原因究明の困難や、責任分担の定め方によっては原因究明の妨げとなるおそれもあること、あるいは保険による損害分散の可能性など、さまざまに考慮すべき要素があり、それらを考慮した上で、委託契約において損害填補責任の分担を明記することが必要である。

## B. 第三者提供

医療機関等が医療情報について第三者提供を行う場合、個人情報の保護に関する法律（平成15年5月30日 法律第57号）第23条および「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」を遵守する必要がある。

いったん適切・適法に提供された医療情報については提供元の医療機関等に責任はない。ただし、例外的に、提供先で適切に扱われないことを知りながら情報提供をするような場合は、提供元の医療機関等の責任が追及される可能性がある。

また、医療情報が電子化され、ネットワーク等を通じて情報を提供する場合、第三者提供の際にも、医療機関等から提供先へ直接情報が提供されるわけではなく、情報処理関連事業者が介在することがある。この場合、いつの時点で、第三者提供が成立するのか、言い換えれば、情報処理関連事業者の処理する段階にある時点で何らかの事故が生じた場合の責任の所在について明らかにする必要がある。

第三者提供の主体は提供元の医療機関等であることからみて、患者に対する関係では、少なくとも情報が提供先に到達するまでは、原則として医療機関等に責任があると考えることができる。その上で、情報処理関連事業者および提供先との間で、前項にいうところの善後策を講ずる責任をいかに分担するかは、医療機関等・情報処理関連事業者・提供先の間で予め協議し明確にしておくことが望ましい。選任監督義務を果たしており、特に明記されていない場合で情報処理関連事業者の過失によるものである場合は、情報処理関連事業者がすべての責任を負うのが原則である。

### 4.3 例示による考え方の整理

本項では「4.2 責任分界点について」について、いくつか例を挙げて解説する。ただし、本項は4.2の考え方を例として考えた場合であるため、医療情報システムの安全管理や接続時のネットワークの考え方、保存義務のある書類の保存、外部保存が受託可能な機関の選定基準等は、それぞれ6章、7章、8章を参照すること。

#### A. 地域医療連携で患者情報を交換する場合

##### I 医療機関等における考え方

- ① 情報処理関連事業者の提供するネットワークを通じて医療情報の提供元医療機関等と提供先医療機関等で患者情報を交換する場合の責任分界点

提供元医療機関等と提供先機関はネットワーク経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意しておく。

その上で、自らの責任範囲において、情報処理関連事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにしておく。

ただし、通常運用における責任、事後責任は、委託の場合は、原則として提供元医療機関等にあり、第三者提供において適切に情報が提供された場合は、原則として提供先医療機関等にあり、情報処理関連事業者に瑕疵のない場合は、情報処理関連事業者に生じるのは管理責任の一部のみであることを留意する必要がある。

- ② 提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界点

ここでいう独自とは、情報処理関連事業者のネットワークではあるが、接続しようとする医療機関同士がルータ等の接続機器を自ら設定して1対1や1対Nで相互に接続する場合や電話回線等の公衆網を使う場合について述べる。

この場合、あらかじめ提供先または提供先となる可能性がある機関を特定できる場合は、委託または第三者提供の要件に従って両機関が責務を果たさなければならない。

情報処理関連事業者に対しては、管理責任の分担は発生せず、通信の品質確保は発生するとしても、情報処理関連事業者が提示する約款に示される一般的な責任しか存在しない。

更に、提供元医療機関等と提供先機関が1対N通信で、提供先機関が一つでも特定できない場合は原則として医療情報を提供できない。ただし、法令で定められている場合等の例外を除く。

##### II 情報処理関連事業者に対する考え方

- ① 医療情報が発信元／送信先で適切に暗号化される場合の責任分界点

患者情報を送信しようとする医療機関等の情報システムにおいて、送信前に患者情報が暗号化され、情報を受け取った医療機関等の情報システムにおいて患者情報が復号される場合、情報処理関連事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係であり、4.2 で述べた責任は限定的になる。

この場合、情報処理関連事業者に存在するのは管理責任であり、ネットワーク上の情報の改ざんや侵入、妨害の脅威に対する管理責任の範囲やネットワークの可用性等の品質に関して契約で明らかにしておく。

なお、暗号化等のネットワークに係る考え方や最低限のガイドラインについては、「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」を参照されたい。

## ② 医療情報が情報処理関連事業者の管理範囲の開始点で適切に暗号化される場合の責任分界点

情報処理関連事業者の中には、例えば暗号化された安全なネットワーク回線の提供を主たるサービスとしている事業者も存在する。

そのようなネットワーク回線を使う場合、事業者が提供するネットワーク回線上における外部からの情報の盗聴や改ざん、侵入等やサービスの可用性等の品質については事業者が管理責任が発生する。従って、それらの責任については契約で明らかにしておく。

ただし、事業者が提供するネットワーク回線に到達するまでの管理責任やネットワーク回線を流れる情報に対する管理責任は医療機関等に存在するため、「I 医療機関等における考え方 ①医療情報の提供元医療機関等と提供先医療機関等の責任分界点」に則った考え方の整理が必要である。

なお、ネットワーク回線上とネットワーク回線を流れる情報に対する考え方や最低限のガイドラインについては、「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」を参照されたい。

## III 外部保存機関が介在する場合の考え方

この場合、保存する情報は外部保存機関に委託することになるため、通常運用における責任、事後責任は医療機関等にある。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等における管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要がある。

また、外部保存機関とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておく。

なお、医療機関等が外部保存機関を通じて患者情報を交換する場合の医療機関等および外部保存機関に対する考え方は、「8.1.2 外部保存を受託する機関の選定基準および情報の取り扱いに関する基準」で定める保存機関毎に「2. 情報の取り扱い」および

「3. 情報の提供」として別途、詳細に規定しているため 8.1.2 を参照されたい。

B. 業務の必要に応じて医療機関等の施設外から情報システムにアクセスする場合

I 自機関の情報システムにアクセスし業務を行う、いわゆるテレワーク

昨今、医療機関等においても医療機関等の施設外から自機関の情報システムにアクセスし業務を行う、いわゆるテレワークも一般的になってきた。

この場合、責任分界の観点では自施設に閉じているが、情報処理関連事業者が間に入って通信回線の両端で一医療機関等の従業者が係わることになる。

更に、この場合には通信回線がインターネットだけでなく携帯電話網、公衆回線など多彩なものが利用されることになり、個人情報保護について広範な対応が求められることになる。

特に、医療機関等の管理責任者でない医療機関等の従業者についても管理責任が問われる事態も発生することに注意を払う必要がある。

この例の場合、責任分界点としては基本的に自施設に閉じているため、責任のあり方の原則としては、「4.1 医療機関等の管理者の情報保護責任について」となることに留意しなくてはならない。

II 第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス

この例のような、リモートログインを用いた保守業者の遠隔保守のためのアクセスが考えられる。この場合、適切な情報管理や情報アクセス制御がなされていないと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。

従って、保守の利便性と情報保護との兼ね合いを見極めつつ実施する必要がある。

ただし、この場合でも、当然、医療機関等に対して「通常運用における責任」、「事後責任」が存在するため、管理状況の報告を定期的に受け、管理に関する最終的な責任の所在を明確にする等の監督を行い、管理責任を果たす必要がある。

なお、リモートログインも含めた、保守の考え方については「6.8 情報システムの改造と保守」を参照されたい。

なお、「I 自機関の情報システムにアクセスし業務を行う、いわゆるテレワーク」、「II 第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス」のどちらにおいても、施設外から情報システムにアクセスする場合のネットワークの考え方については、「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、特に「B-2. 選択すべきネットワークのセキュリティの考え方 III. モバイル端末等を使って医療機関の外部から接続する場合」を参照されたい。

#### C. 診療を目的とした第三者委託の場合

ここでいう第三者委託とは遠隔画像診断、臨床検査、治験等、診療を目的とした第三者委託であり、一時的にせよ情報を第三者が保管する。

委託元である医療機関の管理者は委託先に対して、委託先の選定や委託先への（セキュリティ等の）改善指示を含めた管理責任があるとともに、情報の保存期間の規定等の管理監督を行う必要がある。

ただし、委託先は保存した情報の漏洩防止、改ざん防止等の対策を講じることは当然であるが、感染症情報や遺伝子情報など機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。

#### D. 法令で定められている場合

法令で定められている場合などの特別な事情により、情報処理関連事業者が暗号化されていない医療情報が送信される場合は、情報処理関連事業者もしくはネットワークにおいて盗聴の脅威に対する対策を施す必要がある。

そのため、当該医療情報の通信経路上の管理責任を負っている医療機関等は、情報処理関連事業者と医療情報の管理責任についての明確化を行わなくてはならない。

また、情報処理関連事業者に対して管理責任の一部もしくは全部を委託する場合は、それぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

### 【参考】技術的対策と運用による対策

情報システムの安全を担保するためには、「技術的な対応」と「組織的な対応（運用による対策）」の総合的な組み合わせによって達成する必要がある。

技術的な対応は医療機関等の総合的な判断の下、主にシステム提供側（ベンダー）に求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。

総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により一定レベルの安全性を確保することである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化により異なってくるので、その動向に注意を払う必要がある。

運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として「基準適合チェックリスト」等を作成して整理しておく必要がある。このようなチェックリストは第三者へ説明する際の参考資料に利用できる。

## 5 情報の相互利用性と標準化について

本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において情報処理システムを導入する目的は当初は事務処理の合理化だけであったが、現在は平成13年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報の共有の推進や、医療安全、医療の質の向上に寄与できるものであることが求められている。

これらの目的を実現するためには情報の適切な標準化が必要であることは論を待たない。本ガイドラインは医療に係る情報システムの安全な管理・運用を目的としているが、情報の安全性の重要な要素として、必要時に利用可能であることを確保する可用性を上げることができる。

可用性は情報を保持しなければならない任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い新旧のシステム間での情報の互換性を保ち旧システムで保存された医療情報を確実に読み出せるという、「新旧システムで医療情報の相互利用性」を確保することは、電子保存の見読性及び保存性原則確保の点からみても医療情報システムの必須の要件である。

医療に有用な意味のある情報を長期間にわたり読み出し可能な形で保存するためには、将来にわたりメンテナンスを継続することが期待される標準的な用語集やコードセットを出来る限り利用して保存を行うことが望ましい。

### 5.1 標準的な用語集やコードセットの利用

すでに公開されている用語集やコードセットのうち、日本での各分野における実質的な標準的用語コード集と考えられるものについては情報の保存の際にこれらを利用することが強く推奨される。使用しない場合でもこれらの用語集やコードセットに容易に変換できることが必要である。以下に標準的な用語集やコードセットの例をあげるが、医療情報標準化推進協議会（Health Information and Communication Standards Board：HELICS 協議会）がわが国での用語集やコードセットの標準案の登録を進めており、随時参照されたい。

病名：ICD10 対応電子カルテ用標準病名マスタ

医薬品名：標準医薬品マスタ

臨床検査：JAHIS 臨床検査データ交換規約

## 5.2 国際的な標準規格への準拠

DICOM (Digital Imaging and Communications in Medicine)、HL7 (Health Level Seven) 等の規格及びこれらの規格の標準的な運用方法を定めた IHE (Integrating the Healthcare Enterprise) は、国際的な標準や規格として提唱され、一部はわが国でも利用が進んでいる。

これらの国際的な標準や規格の中で、我が国の医療に適合するものについては、情報の相互利用性の観点から直接これらの規格や標準を採用するか、少なくともこれらの規格や標準に適合した情報形式に容易に変換可能な状態にしておくことが強く推奨される。

また、注意しなければならない点として外字の問題がある。外字とは JIS 文字コードのような容易に移行可能な文字セット以外の文字を独自に定義してもちいた表記文字であるが、そのような外字を使用したシステムではあらかじめ使用した外字のリストを管理し、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要がある。標準化の観点から見れば外字を使用する必要がない文字セットが検討されることを期待したい。



## 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)

法第二十条 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。

#### (従業者の監督)

法第二十一条 個人情報取扱事業者は、その従業者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。

#### (委託先の監督)

法第二十二条 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。

### 6.1 方針の制定と公表

「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」でも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が、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、上記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。

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

### 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 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 の監視及び見直し)	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、運用管理規程など）と文書化された ISMS 構築手順を確立する。

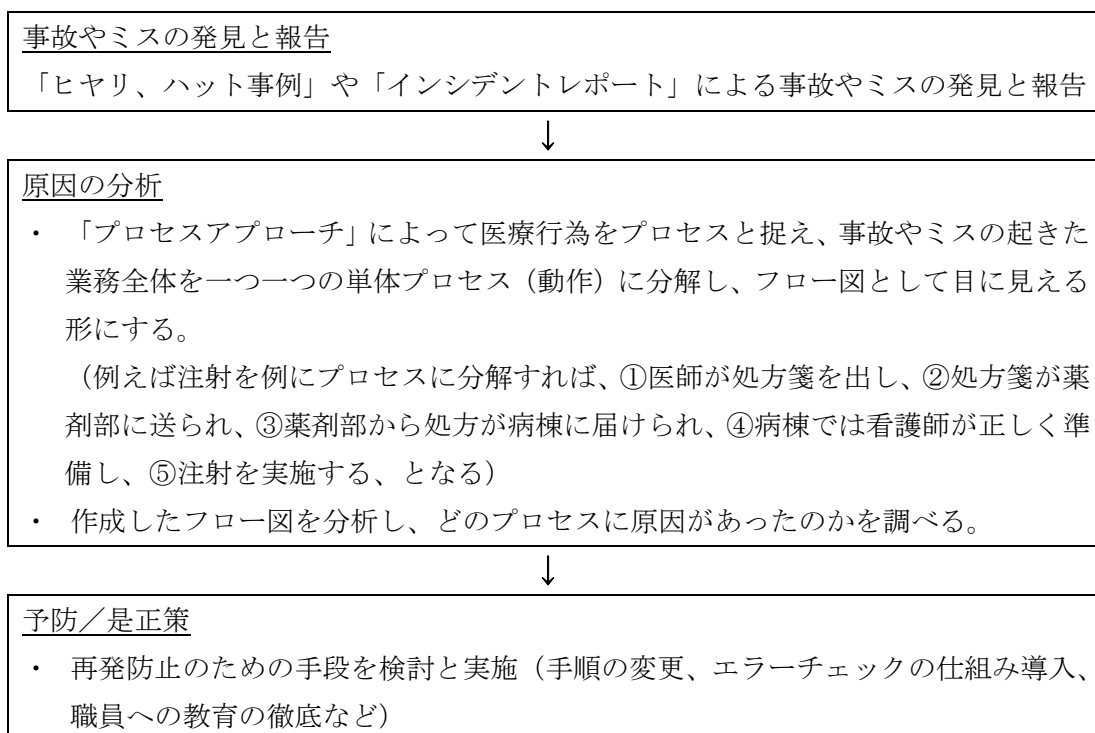
D では P で準備した文書や手順を使って実際に ISMS を構築する。

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】



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、看護など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などを確立すれば、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。少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。

一般に医療に係る情報が個人識別可能な状態で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、もっと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、6.3～6.10の対策を行うことになる。

特に安全管理や個人情報保護関連各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、毀損、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、毀損、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、毀損、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、毀損、滅失、漏えい
  - (c) ファイル交換ソフト（Winny 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型媒体等
  - (a) 可搬型媒体の持ち出し
  - (b) 可搬型媒体のコピー
  - (c) 可搬型媒体の不適切な廃棄
  - (d) 可搬型媒体の盗難、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、リスクを實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。

## 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定
- 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。運用管理規程には必ず以下の項目を含めること。

- ・ 理念（基本方針と管理目的の表明）
- ・ 医療機関等の内部の体制、外部保存に関わる外部の人及び施設
- ・ 契約書・マニュアル等の文書の管理
- ・ 機器を用いる場合は機器の管理
- ・ 患者等への説明と同意を得る方法
- ・ 監査
- ・ 苦情の受け付け窓口

なお、情報およ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 情報およ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) 個人情報の記録媒体の管理（保管・授受等）の方法
  - (b) リスクに対する予防、発生時の対応の方法



## 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および措置

なお、情報およ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 情報およ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. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、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、権限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、本体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。
  - ・ 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こと。
  - ・ 入退者の記録を定期的にチェックし、妥当性を確認すること。
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. 離席時にも端末等での正当な権限者以外の者による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、これらは強力な手段となりうる。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、情報およ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 情報およ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、一般的に言って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・認証に用いられる手段を用意し、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、以下のような行為により、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防止策を取らなければならない。

- ・ 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。

- ・ 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トークン（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。

認証に用いられる手段としては、IC カード等のセキュリティ・デバイス+パスワ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）やバイOMETRICS 等、より認証強度が高い方式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なっ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（生体計測情報）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。

- ・事故や疾病等により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。

"なりすまし"や欠損等の対処として、異なる手法や異なる部位の生体情報を用いたり、ICカード等のセキュリティ・デバイスと組み合わせを行う方法や、従来のパスワードを付加する方法も有効である。

## (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、重要性和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が低減される。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、さらにリスクは低減される。

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

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、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、組織内の全てのシステムで同期をとらねばならない。

#### (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コードは、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。これら不正コード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、不正コードの侵入に気づくことになる。

対策としては不正コード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、不正コード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 情報およ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、全ての不正コード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・ホールが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」および「ステートフルインスペクション」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。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護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 情報および情報端末の持ち出しについて」を参照されたい。

また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS : Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。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事も重要である。

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等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて 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、その事を念頭に置いた上で対策を行なう必要がある。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問題であり、特に、“なりすまし”の問題は絶えずついて廻る。また、ネットワーク上を流れる情報の傍受を防止するために、暗号化などによる”情報漏えい”への対策も必要となる。その際、暗号化技術として、容易に解読されない手法を選択する必要がある。

昨今は無線 LAN を用いてコンピュータをネットワークに接続する構成にしている医療機関等も見受けられる。無線 LAN は、看護師などが使用する情報端末を利用し患者のベッドサイドで作業する場合などに利便性が高い反面、通信の遮断など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、それとは別に、無線電波により重大な影響を被るおそれのある機器などへの利用には注意が必要である。

また、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」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. 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。
3. 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。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、現状でそのような機能がない場合は、システム更新までの期間、運用管理規定でアクセス可能範囲をさだめ、次項の操作記録を行なうことで担保する必要がある。

4. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録はすくなくとも利用者のログイン時刻および時間、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。

5. 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。
6. システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認すること。
7. 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(不可逆)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規程にて定めること)

- (2) 利用者がパスワードを忘れていたり、盗用され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(8バイト以上の可変長の文字列が望ましい)。

- (2) 類推しやすい、不注意によるパスワードの盗用は、盗用された本人の責任になることを認識すること。

8. 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 接続拒否などの対策をとること。

- (2) 不正アクセスの対策を施すこと。少なくとも 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、WPA/TKIP、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) 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. アクセスの記録として、誰が、何時、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こと。
3. 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）を行なうこと。
4. 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）。
5. 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）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。
6. 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。
7. 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が望ましい。

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が望まれる。



## 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係わる情報を取扱い、法令上の守秘義務のある者
- (b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元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診療を維持するための業務に携わる者
- (d) 患者、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」の委託先の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る、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. 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病院事務、運用等で、外部受託業者を採用する場合は、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 包括的な委託先の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・作業結果の確認をおこなうこと。
  - 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。
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運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。また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る。

実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化したものを作成しておくべきである。

外部の委託機関等に保存を委託している診療録等について、その委託の終了により診療録等を破棄する場合には、速やかに破棄を行い、処理が厳正に執り行われたかを監査する義務（または 監督する責任）を果たさなくてはならない。また、受託先の機関等も、委託元の医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を明確に示す必要がある。

### 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者の特定、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が行うこととし、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. 破棄を外部事業者に委託した場合は、「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、さらに委託元の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廃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作業時の病院関係者の監督、等の運用面を中心とする対策が必要である。

また、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。

なお、保守作業によっては保守会社からさらに外部委託業者に修理等を依頼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、再委託先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、およ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なわれる場合には、必ずアクセスログを収集すると共に、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. 再委託が行なわれる場合は再委託先にも保守会社と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. 保守作業時には病院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. 保守作業にかか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 情報およ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および情報機器の持ち出しによる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。

従って、本項ではノートパソコンや可搬媒体、シンクライアントのような機器等による情報、また、情報機器そのものの持ち出しについて考え方と留意点を述べる。

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ったり、医療機関等の情報システムにアクセスしたことで、コンピュータウイルスや不適切な設定のされたアプリケーション（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、この際留意しなくてはならないことは、可搬媒体や情報機器による情報の持ち出しは、医療機関等に設置されているような情報機器よりも、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、人的安全対策を更に施す必要がある。

### 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、情報および情報機器の持ち出しに関する方針を運用管理規定で定めること。
2. 運用管理規定には、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。
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定に定めること。
4. 運用管理規定で定めた盗難、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。
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、このようなアプリケーション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取り扱ったり、医療機関等のシステムへアクセスするような場合は、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。  
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を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「⑥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 障害などの非常時に、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、使用環境が非定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など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、連絡手段および対策ツール
- ・ 非常時に公にすべき文書および情報

##### 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。

業務委託先との間の連絡体制や委託先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」、および「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・手作業など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、要員など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」、「代替施設および設備の確保」、「再開／復旧活動の両立」、および「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」および「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」および「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など、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る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、適切に管理および監査をすること。
  - ・ 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。