…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…

…随時参照されたい

5.2 データ交換のための国際的な標準規格への準拠

…DICOM（Digital Imaging and Communications in Medicine）…国際的な標準…

これらの標準の中で、我が国の医療に適合するものについては、直接採用するか、少なくともこれらの標準に適合した情報形式に容易に変換可能な状態に…こと…

…JAHIS…

削除: あげる

削除: の用語集

削除: 標準案の

削除: より、

削除: 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
・
・
・
・

削除: 、HL7（Health Level Seven）等の規格及びこれらの規格の標準的な適用方法を定めたIHE（Integrating the Healthcare Enterprise）ほ、

削除: 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

削除: 国際的な

削除: や規格

削除: 情報の相互利用性の観点から

削除: これらの規格や標準を

削除: 規格や

削除: しておく

削除: か

削除: される

…

5.3 標準規格の適用に関わるその他の事項

…

…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、…に…独自に定義…表記文字であるか、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。

削除: ：

削除: JIS文字コード

削除: ような符号

削除: 移行可能な文字セット以外の文字を

削除: してもらいた

削除: そのような

削除: 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。

削除: 15年
削除: 第58号
削除: 15年
削除: 第59号

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。

（個人情報保護法）

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」では、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は、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。

削除: でも
削除: められているが、
削除: 上記の

a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること
b) 個人情報の安全管理（漏えい、滅失又は毀損の防止及び是正）に関すること
c) 法令、国が定める指針その他の規範を遵守すること
d) 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
e) 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）では、下記のように定めている。

ISMS 基本方針 トップマネジメントは、次の事項を確実にするための基本方針を確立する。
a) ISMS を確立するための目的を含むか、又はこれらの設定のための枠組みを与える。
b) 事業及び法令又は規制の要求事項、並びに情報セキュリティの契約上の義務を考慮する。
c) 現在及び将来の組織の情報セキュリティ環境との戦略的な整合を含む。
d) リスクを評価するための基準を確立する。
e) 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として、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、公開すること。
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することにより、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行い不要・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

B 考え方

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など）

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技術の日覚しい発展により、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。

削除: など
削除: など
削除: など
削除: など

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。

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、説明責任も情報に最も重要度の高い情報として分類される。

削除: 一般に

削除: が個人識別可能な状態で

削除: もっとも

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。

削除: 個人情報保護関連各法

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. 個人情報が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、点検等を含めたアクセス管理規程を作成すること。
1. 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. 推奨されるガイドライン

1. 情報システムで利用する機器の管理

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関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、情報システムで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 情報システム・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. 個人情報が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、点検等を含めたアクセス管理規程を作成すること。
1. 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

削除: 運用管理規程には次の項目を含めること。

削除: .

<#>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.

削除: および

削除: および

(d) [illegible]

(e) 障害を想定した冗長化機器の管理

(f) 個人情報の記録媒体の管理（保管・授受等）の方法

(g) 患者等への説明や同意を得る方法

(h) 監査

(i) 苦情・質問の受付窓口

削除: リスクに対する予防、発生時

削除: 対応の

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策の措置

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。

削除: および

削除: および

削除: および

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、[illegible]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。[illegible]
   - 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。

削除: 権限者

削除: こと

削除: こと

削除: 離席時にも端末等での正当な権限者以外の者による

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。

削除: 1.

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、技術的対策は強力な脅威対抗手段となりうる。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、情報又は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 情報又は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に限定するために、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とパスワードや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[illegible]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[illegible]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の設定されており、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な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[illegible]手段としては、ICカード等のセキュリティ・デバイスと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）やバイオメトリクス[illegible]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[illegible]

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[illegible]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[illegible]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[illegible]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。

削除: これら
削除: および
削除: および
削除: 置いて
削除: 用いられる
削除: 以下のような行為により、
削除: 防止策が取られなければ
削除: ＩＤ
削除: 、
削除: 、
削除: 用いられる
削除: なって

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るべきである。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るべきである。

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などと生体認証の組み合わせ等）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

削除: （生体計測情報）

削除: より

削除: "なりすまし"や

削除: 等

削除: 、

削除: 用いたり、

削除: 等のセキュリティ・デバイスと

削除: 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

削除: 規程

削除: が

削除: される

削除: は

削除: される

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、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、医療機関の全てのシステムで同期をと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

削除: 組織内

削除: とらなけれ

削除: コード

削除: コード

削除: コード

削除: コード

削除: コード

削除: および

削除: コード

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」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。[illegible]パケットフィルタリング[illegible]以外の手法[illegible]からの攻撃[illegible]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[illegible]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、[illegible]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）を定期的に実施し、ハッチ等の対策を講し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[illegible]、不正にネットワーク上のデータを傍受したり改ざん[illegible]等が可能となる。不正なPCに対する対策を[illegible]場合、一般的にMACアドレス[illegible]PCを識別する場合が多いが、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[illegible]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[illegible]であり、特に、"なりすまし"の[illegible]は[illegible]。また、ネットワーク上を流れる情報の[illegible]を防止するために、暗号化[illegible]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[illegible]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[illegible]に利便性が高い反面、通信の遮断[illegible]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[illegible]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」[illegible]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。

削除: [illegible]
削除: を用いて、[illegible]
削除: から保護
削除: および
削除: 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ほぼ同様な対策[illegible]をいくつかのものとして提供している商品もある
削除: の使用環境に合わせて、[illegible]システムとの組み合わせを行う必要が
削除: 行なったり
削除: 行なう
削除: にて
削除: 行なう
削除: 問題
削除: 問題
削除: 絶えずついて廻る
削除: 傍受
削除: など
削除: 。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
削除: 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[illegible]
削除: など
削除: など
削除: など
削除: それとは別に、
削除: などへ
削除: また、

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

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。[illegible]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[illegible]、次項の操作記録を[illegible]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[illegible]とも利用者のログイン時刻[illegible]時間、[illegible]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。

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[illegible]、外部からの情報[illegible]にはウイルス等の不正なソフトウェア[illegible]混入[illegible]か確認すること。[illegible]

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（[illegible]不可逆変換[illegible]）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

削除: 現状[illegible]
削除: [illegible]
削除: 行なう
削除: [illegible]
削除: および
削除: や
削除: を
削除: したり
削除: を受け取る際
削除: [illegible]
削除: [illegible]
削除: 7.

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。

12. 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。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有す)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) パスワード入力が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とバイオメトリックスあるいはICカード等のセキュリティ・デバイスとパスワードまたはバイオメトリックス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行うこと。

削除: IC
削除: される
削除: (
削除:)
削除: 、不注意による
削除: の盗用は、盗用された本人の責任になる
削除: を認識すること
削除: 8
削除: など
削除: 、WPA/TKIP、
削除: <#>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。。<#>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。。
削除: が望ましい
削除: 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図るため、人による誤りの防止を目的とした人的安全対策を確定する必要がある。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、次の各種類を想定する。

(a) 医師、看護師等の業務で診療に[redacted]情報を取扱い、法令上の守秘義務のある者
(b) 医事課職員、事務委託者等の病院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) システムの保守要員等の雇用契約を結ばずに[redacted]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か、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[redacted]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[redacted]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。

削除: 係わる

削除: 診療を維持するため

削除: 患者、

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. 病院事務、運用等を外部の事業者に委託する場合は、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、作業者・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。

削除: [redacted]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

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、注意しなければならない。

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. 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

削除: 運用、保存する場合だけでなく

削除: また

削除: ある

削除: 廃棄

削除: 廃棄プログラム等

削除: したものを作成

削除: 外部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、受託する機関等も、委託する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。

削除: 行なわれた

削除: 廃棄

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。

保守作業によっては保守会社からさらに外部の事業者に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。

削除: 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、

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

削除: および

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. 再委託が行われる場合は再委託する事業者にも保守会社と同等の義務を課すこと。

削除: 行なわれる

削除: 行なわれる

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、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扱った時に、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、人的安全対策を更に施す必要がある。

削除: および

削除: [illegible]

削除: [illegible]

削除: [illegible]

削除: 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