を電子媒体での保存で法的な責務を果たすという、いわば特殊な作業を行う場合の指針であり、個人情報保護の観点に立てば、個人情報を扱うすべての情報システムが対象になるのは当然で、その意味でこれらの指針はスコープが異なる。特に前者は技術的対策のみで安全管理を実現しようとしたもので、医用画像を電子媒体に保存するだけといった、きわめて限られたユースケースでは成立するが、診療情報の利活用における個人情報保護といった、システムを離れた部分にも十分な考慮が必要なスコープでは適応できない。後者の診療録等の電子保存に関する指針では、技術的対策と運用敵対策の組み合わせで安全管理を実現することを求めており、また基準にも留意事項ではあるが、プライバシー保護が取り上げられていて、その意味では本研究で作成を目指す指針の土台として検討に値する。しかし、電子媒体への保存のみを想定した指針であり、また技術的中立を強く打ち出しているために、必然的に技術要素に具体性がなく、そのために技術的対策に呼応して講じられるべき運用的対策も限定することが非常に難しい。電子保存という、いわば特殊な作業をあえて行う医療機関であれば、それなりに情報技術の素養が求められ、そのようなスキルを前提にすればこのような指針でもよいが、本研究で作成する指針はすべての医療情報システムが対象で、小さな診療書のレセコンまで含まれる。そのため、特別なスキルがなくても可能な限り容易に具体的対策が立てられることが必要で、その意味では技術的中立は不適であろう。

したがってこの平成１１年の指針をベースにしながらも、個人情報保護法に関連する厚労省指針や経産省指針の要件を満たし、利用可能な技術的対策をできるだけ具体的に取り入れ、それぞれに応じた運用的対策を明確にし、指針を作成した。結果的に、具体的で、電子保存に関する指針よりは容易に理解できるものにはなった。

しかし問題もある。一つは技術的対策を網羅することの困難さで、情報セキュリティの分野での技術開発は日進月歩で、網羅することは難しい。また、コストも問題で、大雑把に言って技術的対策にコストをかければかけるほど、運用的対策は利用者に負担の少ないものとなる。その典型例が利用者認証における生体計測認証であろう。この分野の技術的進歩はめざましく、高精度の識別が可能な装置もすでに存在する。しかしかなり高価であり、特別な部屋の入退室管理程度なら大規模な医療機関であれば

利用できるかも知れないが、個々の病院情報システムのクライアントで導入することは不可能である。したがって純粋に技術的な観点からは生体計測認証だけで、利用者を識別することは可能であるが、現実的には、すなわち実現可能な程度のコストでは他の方法と組み合わせることが必要になる。

また、技術の進歩が早いことは、具体的な技術的対策を積極的に取り入れたこの指針が陳腐化するのも早いことを意味している。技術的に中立に記載すれば、いわばセキュリティの基本方針が変わらない限り有効な指針となるが、現実の技術的対策を具体的に記述すれば、技術の進歩に応じて改定する必要がある。技術開発の速度を予測することは難しいが、１～２年のスパンで見直しは必須と考えられる。

なお、本研究で作成した安全管理指針は、１７年３月３１日に厚生労働省から公表された「医療情報システムの安全管理に関するガイドライン」に反映されている。この指針は個人情報保護法の要請だけに対応するものではなく、いわゆる電子署名法、やe-文書法に対応するための指針で、電子保存や外部保存の指針のリライトも含まれており、大部なものとなっている。

E．結論

HIVネットのセキュリティポリシーの見直しと患者等のプライバシーを確保した上での利活用を推進するにあたって、前提となる医療情報システムの安全管理指針を作成した。わが国の70%以上の医療機関を対象とした指針であるために、可能な限り具体的に記述し、わかりやすさの点では成果をあげたが、反面短い期間での見直しが必要となった。なお、本研究で作成した指針は厚労省の「医療情報システムの安全管理に関するガイドライン」の一部として反映されている。

F．健康危険情報

特になし。

G．発表

論文

１．　山本隆一、電子カルテの進展と医療情報保護、診療録管理、Vol. 16、No. 1、2004

２．　山本隆一、医療情報とセキュリティー、クリニカルプラクティス、Vol. 23、No.11、2004

H．知的財産権の登録・出願状況

現在のところなし。

付録

情報システムの基本的な安全管理指針

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（平成十五年法律第五八号）、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（平成十五年法律第五九号））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。この指針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。

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り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、取り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。

2．情報の取り扱いの把握とリスク分析

2.1　取り扱い情報の把握

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。

2.2　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、6.3～6.8 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のが限界である。したが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

(b) 権限のある者による不当な目的でのアクセス、改ざん

(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

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 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) 非可搬型媒体（ハードディスクを搭載したパーソナルコンピュータ等（以下、PC等という。）の不適切な廃棄

④ 参照表示した端末画面等

(a) 端末画面の覗き見

⑤ 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

上記の脅威に対し、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。

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 医療情報取り扱い台帳の整備

④ 医療情報の安全管理対策の評価、見直し及び改善

⑤ 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

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. 個人情報の取り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

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・情報媒体等の物理的な保護

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

防犯カメラ、自動侵入監視装置等を設置すること。

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「2.2 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

(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）やバイオメトリクス等、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。

したがって、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功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（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。

したがって、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。

・事故や疾病等により認証に用いる部位の損失等

・成長等に認証に用いる部位の変化

・一卵性の双子の場合、特徴値が近似する手法がある

・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。したがって、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。しかし、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。

ただし、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、ハ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。

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。

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、ネットワーク機器に対して攻撃を行なったり、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行なう必要がある。不正アクセスの防止は、いかに保証を確実に確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。

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、漏洩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。

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。
7. 認証に用いられる手段としては、ID＋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＋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が望ましい。

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り扱い、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り扱い、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

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洩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。

(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