愛知県臨床検査標準化ガイドライン

「個人情報の保護および漏えい事故防止の対策」

第１版
平成 21 年 11 月

愛知県臨床検査標準化協議会
AiCCLS：Aichi Committee for Clinical Laboratory Standardization

発刊によせて

愛知県臨床検査標準化協議会
会　長　　大野　和美

近年、医療界においてEBM（evidence based medicine）と言う概念が導入されてきた。
EBMは、日本語に訳すと「根拠に基づく医療」であり、簡単に言うと、現在利用可能な最も信頼できる情報を踏まえて、目の前の患者さんにとって最善の治療を行うことである。
EBMの手順は、step1：疑問の定式化、step2：情報収集、step3：情報の批判的吟味、step4：情報の患者さんへの適応、step5：step1～step4 のフィードバックとなり、より良い医療を効率的に行う方法として提唱された。

我々の医療を取り巻く環境は、大きく変化している。その1つに「チーム医療」があり、チーム医療を無くしては臨床検査技師の職域も成り立たない状況となっている。臨床検査技師は、今まで培った知識や経験によって質の高い検査データを管理でき、検査業務を通じて患者さんにとって身近な存在になることができる職種であることから、臨床検査技師がチーム医療に参画することは意義があると確信する。また、社会情勢に目を向けると、わが国は予想をはるかに超える勢いで少子高齢化社会を迎えつつある。このような社会情勢の中でも、国民は日々進歩する最新の医療サービスを安価に享受したいと考えている。これは、患者さんにとって見れば至極当たり前のことであり、それに答えるべく努力することが我々医療人の務めでもある。

このように、現代の医療に纏わる様々な要求に関して臨床検査は非常に重要な位置を占めている。そして、この様々な要求にこたえるために、臨床検査に必要とされていることは、精度管理と検査データの標準化である。これに関しては、愛知県は先輩諸氏の努力により愛知県医師会精度管理委員会、愛知県臨床検査標準化協議会（当会）など精度管理および検査データの標準化に関する活動が他県と比較して進んでいるものと自負している。

この一例として、当会は既に標準化ガイドラインを5冊出版した。また、これに続き、今回新たに「個人情報の保護および漏えい事故防止の対策」のガイドラインが完成した。
コンピュータは、日常業務には欠かせないものであるが、IT 技術の進歩は著しく、コンピュータ機能を使いこなすには知識と訓練が必要である。
このガイドラインが皆さんに利用され、個人情報の取り扱いや漏えい事故防止に寄与する事を期待する。

2009年7月

はじめに

近年、業務効率化の向上やコスト削減のため、各施設で保有する情報の多くが電子化されている。これら電子保管された情報は、ネットワークの進展に伴って運用面で利便性が向上したものの、紙で保管された情報に比べて大量のデータを持ち出し易く、より強固な情報の保管体制を整備しておく必要がある。個人情報保護法が施行され、情報の取り扱いについて様々な対策がなされているが、一方で新聞報道等により多くの情報漏えい事故が報告されている。情報漏えい事故は、USB メモリなどの外部記憶装置の紛失やファイル交換ソフトを介した漏えい事故が大部分を占めている。USB メモリなどの外部記憶装置は、容量の大きな製品が販売され持ち運びに便利であるが、サイズが小さいため紛失等には十分な配慮が必要である。最近では、セキュリティ対策がなされた製品が販売されており、これら製品の使用が望ましい。また、ファイル交換ソフトを介すると、不特定多数のユーザーに情報が漏えいしてしまうため 100%の回収および削除は困難である。情報漏えい事故は、個人の責任だけでなく施設全体に悪影響を及ぼす。特に、不特定多数の人が出入りする医療機関においては、内外部から信頼を得られるセキュリティレベルに達しなければならない。最近では、情報漏えい事故を起こした当事者へ賠償責任を問う事例もあり、施設内職員への教育および周知徹底が重要である。

今回、各施設における情報セキュリティ全体の向上を目的に、ユーザー数の多い Windows 機を中心とした「個人情報の保護および漏えい事故防止の対策」の概要をまとめた。このガイドラインを多くの方々にご活用いただければ幸いである。

目　　次

Ⅰ．個人情報の保護について

1．キーワードの解説[1)]

A）個人情報保護法

正式には「個人情報の保護に関する法律」といい、2003 年５月に成立した。この法律は、国・地方公共団体などの責務を明らかにするとともに、個人情報を取り扱う事業者が守るべき義務を定めている。個人情報保護法は、文字通り個人の権利利益の保護を目的とするとともに、個人情報を利用することの有用性にも配慮し、個人情報の適正な取り扱いについてルールを定めたものである。

B）個人情報

個人情報保護法では、「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの」【個人情報保護法２条１項】としている。個人情報保護法は、生存する個人に関する情報について適用されるものであるが、医療は死と向き合う分野であり、医療分野においては死者の情報についても安全管理や開示に配慮する必要があるため、死者の情報について他の分野の情報とは異なる格別の措置が必要と考える。[2)]･･･注１）参照

「識別」の対象には氏名・住所・生年月日・電話番号だけでなく顔写真や映像、音声など、それにより個人が特定できるものすべてを個人情報として含む。また、それだけでは特定の個人を識別できないような情報であっても、ほか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れば、これも個人情報となる。

※ 注 1）「診療情報の提供等に関する指針」において、患者が死亡した際、遅滞なく遺族に対して死亡に至るまでの診療経過や死亡原因等についての診療情報を提供しなければならないと定めており、既に遺族に対する診療情報の提供に向けた取り組みがなされている。また、厚生労働省の「医療介護分野のガイドライン」でも死者の個人情報の適切な管理が求められており、遺族等の同意を得ず開示、提供することを禁じている。

C）個人情報取扱事業者

個人情報保護法第２条第３項で「個人情報データベース等を事業の用に供している者をいう」としている。ここでいう「事業」は、原則として一定の目的を持って一定期間繰り返される行為であれば足りており、営利目的か否かは関係ない。法人のみならず任意団体や個人も含まれるため、かなり広い範囲の事業者がこれに該当することになる。ただし、「その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害する恐れが少ないものとして政令で定める者」は、個人情報取扱事業者から除外される。個人情報の量については、施行令で「過去６ヵ月以内のいずれの日においても個人データによって識別される特定の個人の数が 5000 を超えない者」とされた。個人情報取扱事業者に該当する場合は、個人情報保護法により利用目的の特定や適正な取得、利用目的の通

知または公表、データの正確性の確保、安全管理措置、第三者提供の制限、データの開示・訂正などの義務が課せられる。

D）第三者提供

個人情報取扱事業者が保有する個人データを第三者に提供する場合（ネットワーク等を通じて利用できる場合も含む）、原則としてあらかじめ本人の同意を得なければならないと定めている。

E）オプトアウト

オプトアウトとは、直訳すると「身を引く、脱退する」であるが、意味合いとして「本人による拒否権」と解釈する。

F）安全管理措置

個人情報取扱事業者に対しては、取り扱う個人データの安全確保を求めると共に、個人データを取り扱う従業者、さらには委託先の監督義務を定めている。

G）プライバシーマーク

「Pマーク」とも呼ばれるプライバシーマークとは、（財）日本情報処理開発協会(JIPDEC）が個人情報保護の規格である「JISQ15001 ： 2006」に準拠して、個人情報の取扱いを適切に行っている事業者に対してマーク（ロゴ）の使用を許諾する制度である。

プライバシーマーク　（提供：財団法人　日本情報処理開発協会）

2．利用目的の特定等（個人情報保護法第 15 条、第 16 条）[3)]

（利用目的の特定）

個人情報保護法第十五条 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

２ 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）

個人情報保護法第十六条 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

２ 個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

３ 前二項の規定は、次に掲げる場合については、適用しない。

一 法令に基づく場合

二 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。

三 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。

四 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。

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より

A）利用目的の特定及び制限

医療・介護関係事業者が医療・介護サービスを希望する患者・利用者から個人情報を取得する場合、当該個人情報を患者・利用者に対する医療・介護サービスの提供、医療・介護保険事務、入退院等の病棟管理などで利用することは患者・利用者にとって明らかと考えられる。

これら以外で個人情報を利用する場合は、患者・利用者にとって必ずしも明らかな利用目的とはいえない。この場合は、個人情報を取得するに当たって明確に当該利用目的の公表等の措置が講じられなければならない。

B）利用目的による制限の例外

医療・介護関係者は、あらかじめ本人の同意を得ないで個人情報保護法第 15 条の規定により特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならないが（個人情報保護法第 16 条第 1 項）、同条第 3 項に掲げる場合については、本人の同意を得る必要はない。

３．医療分野で遵守すべき事項

近年企業の顧客情報や医療機関の患者情報などの漏えい事件が、社会的に重大な問題として新聞紙上を時折賑わせている。政府は、各施設における個人情報の管理レベルを強化するため、ガイドラインの制定や法令化を進めている。

経済産業省の規格による個人情報は、氏名、住所、生年月日、電話番号、銀行口座番号、保険証番号、顔写真、声、家族、学歴、学校などの成績、健康情報、収入、資格などが含まれるとしている。

個人情報保護法では、個人情報の定義、個人情報保護の基本原則、個人情報取扱業者の義務、国・地方公共団体の施策や責務、違反者への罰則、民間団体による個人情報保護の推進などが法制化されている。特に今回の施行では、個人情報取扱業者の義務として、一部の例外を除き利用目的の通知・公表、正確性の確保、安全管理措置、従業者・委託先の監督、第三者提供の制限、本人からの開示請求、苦情処理などが規定された。

また、Ｗｅｂサイトにも個人情報保護の自主規制基準があり、個人情報保護ポリシーの公開とセキュリティ対策が必要であるとしている。その内容は以下のようである。

A）医療・介護関係事業者は、個人情報を取り扱うに当たって、その利用目的をできる限り特定しなければならない。

B）医療・介護関係事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

C）医療・介護関係事業者は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。なお、本人の同意を得るために個人情報を利用すること（同意を得るために患者・利用者の連絡先を利用して電話をかける場合など）、個人情報を匿名化するために個人情報に加工を行うことは差し支えない。

D）個人情報を取得する時点で、本人の同意があったにもかかわらず、その後、本人から利用目的の一部についての同意を取り消す旨の申出があった場合は、その後の個人情報の取り扱いについては、本人の同意が取り消されなかった範囲に限定して取扱う。

E）医療・介護関係事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

F）利用目的の制限の例外（個人情報保護法第１６条第３項）に該当する場合は、本人の同意を得ずに個人情報を取り扱うことができる。

医療分野における個人情報とは [4)]

患者の診療録（カルテ）や検査記録など診療を目的として作成した診療情報だけでなく、健康保険証や診療申込書など患者から病院が取得した書面記載の情報を含む。

都立病院における個人情報の取扱いについてより

4．学会発表で遵守すべき事項と対策例

A）遵守すべき事項　（日本病理学会、日本臨床細胞学会の指針から）[5),6)]

- 患者の氏名、イニシャル、雅号（著述家・画家・書家などが本名以外に付ける風流・風雅な別名）は記述しない。
- 患者の人種、国籍、出身地、現住所、職業歴、既往歴、家族歴、宗教歴、生活習慣・嗜好は、報告対象疾患との関連性が薄い場合には、記述しない。
- 日付は、第一病日、3 年後、10 日前という記述方法か、あるいは、患者の臨床経過、病態把握に必要な場合には個人を特定できないかたちで年月までの記載は許容される。
- 診療科名は省略するか、大まかな記述法とする（例：第一内科→内科）。
- 既に診断・治療を受けている場合、他院名やその所在地は記述しない。
- 顔面写真を提示する際には目を隠す。眼疾患の場合は、眼球部のみの拡大写真とする。
- 症例を特定できる生検、剖検、画像情報の中に含まれる番号などは削除する。

B）対策例

個人情報は、「氏名、生年月日、その他の記述等により特定の個人を識別することができるもの」と定義付けられている。患者 ID なども個人情報になるため、患者 ID の最後の桁に任意の数字を付け足すことで、特定の個人を識別できなくするなどの方法やファイルを暗号化して管理するなどの対策を実施する。また、学会、研修会等で発表者から預かった（個人情報の入っている可能性のある）発表用データは、「ごみ箱」より消去するなど適正に処分する。しかし、「ごみ箱」からファイルを消去しただけでは特殊なソフトを用いれば復元できてしまうため、必要な場合はハードディスクイニシャライズ用ソフトなどを使用して完全に消去する。コンピュータを業者からレンタルしている場合は、学会終了時に学会事務局立会の下データ消去を実施する。ただちにできない場合は、契約時にデータ消去まで盛り込む。

C）臨床検査を終了した検体の業務、教育、研究のための使用について[7)]

＜日本臨床検査医学会の見解＞

① 臨床検査室の管理者（以下、管理者）および業務・研究担当者はいずれも、被検者の個人情報や検査データについての守秘義務を順守し、被検者が不利益を被らないようにしなければならない。なお、管理体制については、各施設内で改めて討議し、定める必要がある。

② 残存検体の「業務への使用」は、通常、プール化および／または匿名化して行う。その限りにおいて、個々の同意を特に必要としないが、取り扱いには管理者が責任を持つ必要がある。「教育のための使用」についても、「業務への使用」に準じて処理、管理がなされなければならない。

③ 残存検体の「研究への使用」には、原則として、被検者から文書による同意を得る必要がある。ただし、測定法の改善や異常値の解明などの検査業務に直接関連する研究では、検体をプール化および／または連結不可能匿名化する場合はこの限りでない。一方、連結可能匿名

化して用いる場合は、研究担当者と管理者は被検者に対する守秘を厳重にし、その取り扱いには管理者が責任を持つ必要がある。検査業務に直接関係しない研究の場合は、各研究担当者と管理者の判断で、当該施設の倫理委員会の審査を受けることを原則とする。

④　残存検体の分与および廃棄は、管理者が責任を持って行わなければならない。

５．災害時における個人情報の取り扱いについて

災害時、意識不明となっている患者の病状や重度の認知症を認める高齢者の状況を家族等に説明する場合は、本人の同意を得ずに第三者提供できる場合と考えられる。この場合は医療・介護関係事業者が本人の家族等であることを確認した上で、治療等を行うに当たり必要な範囲で情報提供を行うとともに、本人の過去の病歴や治療歴等の情報を取得する。本人の意識が回復した際には、速やかに提供および取得した個人情報の内容とその相手について本人に説明する。本人からの申し出があった場合は、取得した個人情報の内容の訂正等、病状の説明を行う家族等の対象者の変更等を行う。

なお、患者の判断能力に疑義がある場合は、意識不明の患者と同様に対応する。判断能力の回復に合わせて、速やかに本人への説明を行い本人の同意を得なくてはならない。

６．紙媒体における個人情報の取り扱いについて[8)]

紙媒体には、デジタル化以前の文書もあれば、デジタルデータをプリントアウトしたものもある。いずれの場合でも、安易に院外に持ち出したり、シュレッダーなどにかけずに放置・廃棄することは厳禁のはずだが、漏えい事故は後を絶たない。特に廃棄に際しては、信頼できる企業が提供している廃棄サービスを利用することが望ましい。

ただ、「紙媒体経由」の情報流出が多いとは言うものの、１件あたりの流出人数で見てみると、「フロッピーディスク等可搬記録媒体」が56.5%に対して「紙媒体経由」は7.1%と、様相はがらりと変わる。やはり、ＵＳＢメモリなどでデジタルデータを大量に院外に持ち出すといった行為が、大きな被害を呼ぶことは間違いない。

扱う人数の多少にかかわらず、日頃から注意を喚起されているデジタルデータについてはもちろん細心の注意を払ったうえで、紙媒体についても、しっかり情報管理していくことが大切である。

７．「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」
に関するＱ＆Ａ（事例集）より[9)]
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805iryou-kaigoqa.pdf

Ｑ５－１７）大規模災害や事故等により、意識不明で身元の確認できない多数の患者が複数の医療機関に分散して搬送されている状況のとき、電話で患者の家族または関係者と称する人から患者が搬送されているかという問い合わせがありました。相手が家族等であるかどうかの確認が十分にできない場合、患者の存否情報を回答してもよいでしょうか。

回答）患者が意識不明であれば、本人の同意を得ることは困難な場合に該当します。また、個人情

報保護法第２３条第１項第２号の「人の生命、身体又は財産の保護のために必要がある場合」の「人」には、患者本人だけではなく、第三者である患者の家族や職場の人等も含まれます。このため、このような場合は、第三者提供の例外に該当し、本人の同意を得ずに存否情報等を回答することができ得ると考えられます。災害の規模等を勘案し、本人や家族等の安心や生命、身体または財産の保護等に資する場合は、迅速に本人の安否を家族等の関係者に情報提供を行うべきと考えます。なお、「本人の同意を得ることが困難な場合」とは、本人が意識不明等の場合および非常に多数の傷病者が一時に搬送された場合などが該当し、家族等からの問い合わせに対して迅速に本人の同意を得るための作業が著しく不合理と考えられる場合も含まれるものと考えます。

Ｑ５－１８）　上記の状況で、患者の家族等である可能性のある電話の相手から、患者の容態等についての問い合わせがあれば、どの範囲まで回答すべきでしょうか。
回答）電話による問い合わせで、相手と患者との関係が十分に確認できない場合には、存否情報やけがの程度等の情報提供に限定することも考えられます。患者の特徴を具体的に説明できるなど相手が患者の家族等であると確認できる場合には、より詳細な情報提供を行うことも可能と考えます。

Ｑ５－１９）　上記の方法により、連絡が取れた家族等から意識不明である患者の既往歴、治療歴等を聴取することに問題ありませんか。
回答）治療のため、必要な既往歴、治療歴等の情報を家族から取得することは個人情報の適正な取得であり問題ありません。この場合、本人の意識が回復した後に、家族等から取得した情報の内容とその相手について本人に説明することになります。

Ｑ５－２０）Ｑ５－１７のような状況において、報道機関や地方公共団体等から身元不明の患者に関する問い合わせがあった場合、当該患者の情報を提供することはできますか。
回答）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、家族等がより早く患者を捜索することが可能になると判断できる場合は、回答）５－１７のように「人の生命、身体また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」に該当する。この場合、医療機関は存否確認に必要な範囲で意識が不明な患者の同意を得ることなく患者情報を提供することが可能と考えられます。具体的な対応については、個々の事例に応じて医療機関が判断する必要があります。

＜参考資料＞
社団法人　日本臨床衛生検査技師会　個人情報保護ガイドライン
http://www.jamt.or.jp/materials/materials.html

＜参考資料＞

JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン

― 第 1 版 ―[10)]

財）日本情報処理開発協会　プライバシーマーク制度より

http://privacymark.jp/reference/index.html

【個人情報保護マネジメントシステムの作成指針】

1．　個人情報保護マネジメントシステムについて

個人情報保護マネジメントシステム規格である JISQ15001:2006 は、マネジメントシステムを作成する場合の国際的規約である ISO Guide 72 （「マネジメントシステム規格の正当性及び作成に関する指針（2001）」）に従って作成されている。したがって、品質マネジメントシステムや環境マネジメントシステムと共通のマネジメントシステム原則を採用している。

マネジメントシステム原則の趣旨は、方針を作成し、それに基づいて計画を作成し（Plan）、実施し（Do）、点検し（Check）、見直し（Act）を行うという、いわゆる PDCA サイクルをスパイラル的に継続することにより、事業者の管理能力を高めていくことにある。この仕組みを採用することで、事業者における個人情報保護の保護レベルが上がることを期待している。

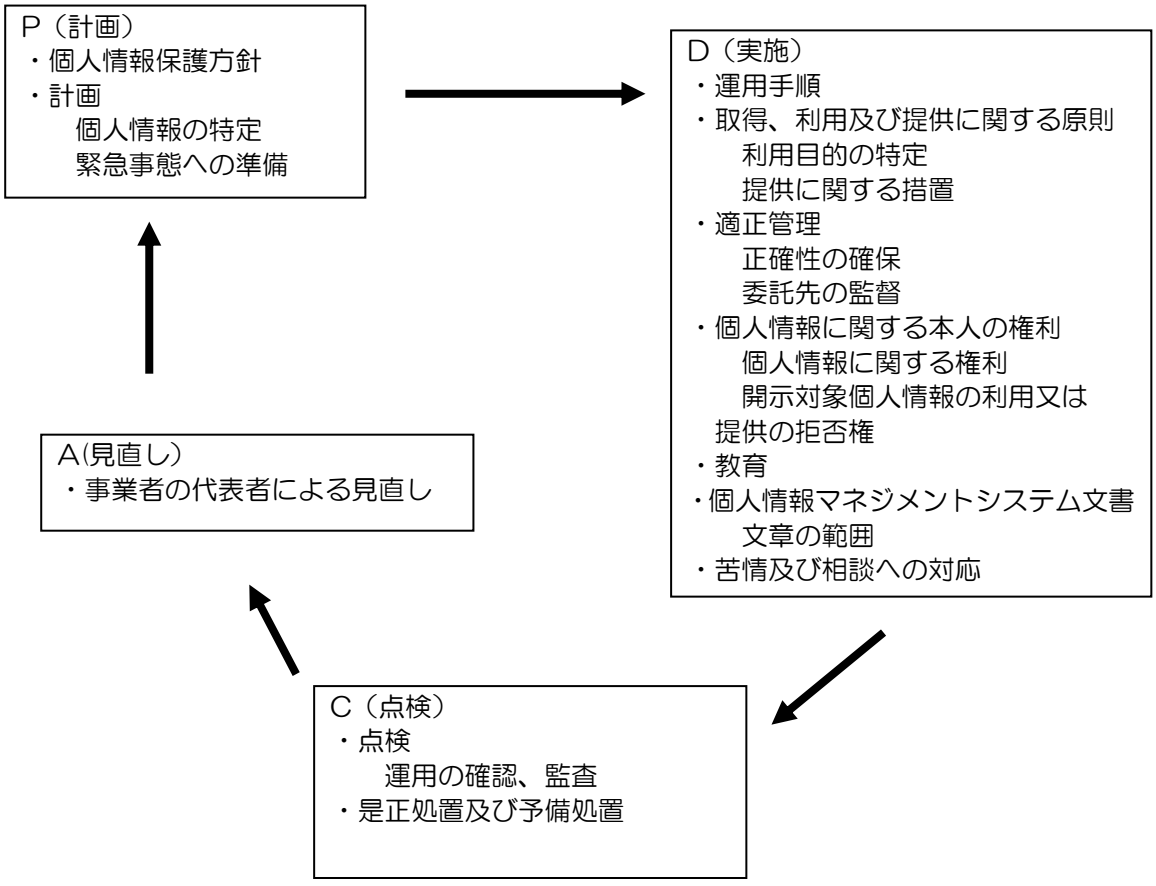

図 1　JISQ15001:2006 における PDCA サイクル

1． JISQ15001:2006 に適合した個人情報保護マネジメントシステムを構築するメリット

改定前の JISQ15001:1999 は、個人情報保護に関する法律（以下、「個人情報保護法」という。）よりも前に策定されたため、個人情報保護法によって新しく導入された概念に対応していないところがあった。また、個人情報保護法と用語が異なるため、法への適合状況が分かりづらい面もあった。JISQ15001:2006 は、個人情報保護法を取り込むことを最大の目標にして改訂されたものである。したがって、JISQ15001:2006 に適合した個人情報保護マネジメントシステムを構築し、それを適正に運用することは、個人情報保護法を遵守しているものと考えて良く、個人情報保護法に違反しないためにどのようにすれば良いか分からないという事業者にとって、この JISQ15001:2006 は、非常に有効な指針となると言える。

また、JISQ15001:2006 は、個人情報保護法を取り込んだだけでなく、個人情報保護法よりも高いレベルを求めている。このため、個人情報保護法は適法であっても規格上では不適合となる場合がある。個人情報保護法を遵守することは事業者として当然の義務であるが、さらに高いレベルの保護水準を確立していることを対外的にアピールすることが、事業者にとって大きなメリットになるはずである。

2． 個人情報保護マネジメントシステム構築の具体的な進め方

個人情報保護マネジメントシステム（以下、「PMS」という。）は、以下の手順で構築し、運用することができる。

ステップ１　：個人情報保護方針を定めて文書化する
ステップ２　：PMS 策定のための組織を作る
ステップ３　：PMS 策定の作業計画をたてる
ステップ４　：個人情報保護方針を組織内に周知する
ステップ５　：個人情報を特定する
ステップ６　：法令、国が定める指針その他の規範を特定する
ステップ７　：個人情報のリスクを認識し、分析と対策を検討する
ステップ８　：必要な資源を確保する
ステップ９　：PMS の内部規程を策定する。
ステップ 10　：PMS を周知するための教育を実施する
ステップ 11　：PMS の運用を開始する
ステップ 12　：PMS の運用状況を点検し改善する
ステップ 13　：PMS の見直しを実施する

プライバシーマークの認定申請においては、申請時にこのステップ 13 までを実施していることが必要である。

Ⅱ．漏えい事故防止について

１．各施設の個人情報漏えい防止に向けて

各施設が保有する個人情報については、各施設の個人情報の保護に関する関係法令等に基づき、適正な取り扱いに努めている状況であるが、昨今、新聞報道等で病院や企業等から持ち出された個人情報の漏えい事故が多く報じられているのが現状である。最近の傾向として、職員が許可無く職務上取り扱う個人情報を持ち出し、個人所有のコンピュータを利用したことにより、ファイル交換ソフト等を介して流出するという事故が多く発生している。各施設におかれては、患者個人情報漏えい等を防止するため、既に諸々の対策が講じられているものと思われるが、①患者個人情報等の持ち出し、②職場外で利用するコンピュータのセキュリティ、③ファイル交換ソフトへの対策を行い、患者個人情報の漏えい等の防止について再度徹底することをお願いしたい。

＜原則＞　「持ち出さない、持ち込まない」を徹底する。

個人情報保護管理者の管理の下において、個人情報の取り扱いを担当する各部門レベルで、部門管理者、権限および責任を明確に規定する。（誓約書の提出）

具体的な対策など周知するための教育を実施する。（Windows 機） コンピュータのセキュリティ設定を行う。 １）Windows 起動時のログインパスワードを設定する。 ２）Windows Update を実施する。 ※インターネットへ接続できる環境にあるコンピュータの場合のみ。 ３）ウイルス対策ソフトを導入する。 ４）表計算ソフト、ワープロソフトをパスワード保護する。 ５）フォルダをパスワード保護する。 ６）暗号化ソフトを利用して保護する。 漏えい事故の主な原因 １）ファイル交換ソフトによる漏えい。 ２）コンピュータ本体や USB メモリなどの外部記憶装置の盗難や紛失による漏えい。 ファイル交換ソフトで漏えい事故が起こった場合の対策 外部記憶装置の盗難、紛失が起こった場合の対策

2．病院情報システム利用誓約書と診療情報二次利用書の雛形

例）病院情報システム利用契約書

私は、病院情報システムの利用にあたって〇〇〇〇病院　病院情報システム運用管理規程を順守することを誓います。尚、違反時は、〇〇〇〇病院　就業規則　第××章「懲戒」に基づく罰則を受けることや、氏名を公表されても異議を申し立てません。

平成　　年　　月　　日

〇〇〇〇病院長殿

職種　＿＿＿＿＿＿＿＿
コード　＿＿＿＿＿＿＿＿
ふりがな
氏　名（自署）　＿＿＿＿＿＿＿＿＿＿

例）診療情報二次利用依頼書

運用管理者

依　頼　日＿＿＿＿＿＿＿＿
依頼者氏名＿＿＿＿＿＿＿＿
部　　署＿＿＿＿＿＿＿＿

データ抽出の目的	
内　　容	
出力項目	
抽出期間	
条　　件	
抽出期限	
希望媒体	紙面、FDD、MO、その他（　　）
特記事項等	

申請者の方へ
・患者情報の漏洩等が起こらないようデータの取り扱いに十分留意すること。
・情報システムで処理、保管されているデータに関するいかなる情報もこのシステムに関係ない者には公表しないこと。
・一度暴露等の事故が発生すると、取り戻すことができないという情報固有の特性を考え、その保護に優先で取り組むこと。
（備考欄）

データ出力担当者＿＿＿＿＿＿＿＿
出力ファイル名＿＿＿＿＿＿＿＿

３．コンピュータのセキュリティ設定

※以下、Windows 機における一般的なセキュリティの設定方法を解説する。

A）Windows 起動時のログインパスワードを設定する。

管理者権限をもつユーザーアカウントには、パスワードを設定する。

スタート　→　コントロールパネル　→　ユーザーアカウントの順にクリックする。

管理者のユーザーアカウントにパスワードを設定する。パスワードを設定することで Windows 起動時にパスワードの入力が必要となる。

B）Windows Update を実施する。

インターネットに接続できる環境でコンピュータの電源が ON のとき、「自動更新」が有効である場合は自動的に Windows Update が実施される。手動で実施することも可能である。

＜手動方法＞

スタート　→　すべてのプログラム　→　Windows Update

※毎月、第２火曜日の翌日（米国は毎月、第２火曜日）に更新される。

C）ウイルス対策ソフトを導入する。

Symantec 社、Trend Micro 社、McAfee 社などセキュリティベンダーよりウイルス対策ソフトが市販されている。必ず、ウイルス対策ソフトを導入する。

D）表計算ソフト、ワープロソフトのファイルをパスワード保護する

表計算ソフトファイル

名前を付けて保存 → ツール → 全般オプション → パスワード設定

※パスワードを忘れるとファイルが開けなくなるので注意する。

ワープロソフトファイル

名前を付けて保存 → ツール → セキュリティオプション → パスワード設定

※パスワードを忘れるとファイルが開けなくなるので注意する。

E）フォルダをパスワード保護する。（圧縮ソフトを利用しても可能）

必要なファイルをいれたフォルダを右クリック → 送る → 圧縮フォルダをクリックする。

圧縮フォルダが作成される（圧縮フォルダ A とする）。

圧縮フォルダ A をダブルクリックで開く。ファイル→パスワードの追加の順に開き、パスワードを設定する。圧縮フォルダ A を開いて、ファイルを開くとパスワードが要求される。

F）ファイル暗号化ソフトを利用して保護する[11)]

「ED」というフリーのファイル暗号化ソフトを例にして説明する。

http://type74.org/　　（2008 年 5 月現在　ED 本体安定版　バージョン 3.21）

ダウンロード後、解凍する。解凍してできたフォルダの中に「E_D.exe」があるのでダブルクリックする。暗号化するファイルを「E」へドラッグアンドドロップすると暗号化される。（パスワードの設定）

暗号化を解除する場合は、解除するファイルを「D」へドラッグアンドドロップするとパスワードの入力画面になり、パスワードを入力して暗号化が解除される。

※パスワードを忘れるとファイルが開けなくなるので注意する。

※ファイル暗号化ソフトは、無料・有料のものがあります。利用条件にあったものをご使用下さい。

4．個人情報の持ち出し等による漏えい等の防止について

A）個人情報等の持ち出しについて

① 各施設から個人情報等を持ち出す場合には、情報管理者の許可を得るなどのルールを明確化し、漏えい等（データの滅失、き損など）への防止対策を徹底する。許可を得て持ち出す場合は、持ち出したファイル名、ファイルの種類、個人情報の範囲、件数、日時（返却日時も）、利用目的など必要事項も管理する必要がある（管理表の作成）。

② 電子メールにより非公表の情報を施設外へ送信する場合も、当該情報にパスワードを設定した上で送信するなど、必要に応じた保護対策を行う。

③ 個人情報の持ち出しによる漏えい事故では、職員の認識不足によって発生する例が多い。漏えいの危険性について、職員一人ひとりへ的確に周知を図るとともに、必要に応じて教育研修を実施することが望ましい。

B）各施設以外で利用するコンピュータのセキュリティ対策について

① 施設内で利用するコンピュータのセキュリティ対策はもちろんのこと、施設外で業務に利用するコンピュータについても、ウイルス対策ソフトがインストールされていることを確認し、パターンファイルが最新の情報に更新されていることも確認する。

② OS 等の脆弱性が改善されるよう、最新の修正プログラムを適用する。

③ 秘密情報、個人情報等の関係者のみが閲覧すべき情報については、パスワードで保護するなどアクセス制限の措置を行う。

C）病院システム等の個人情報を取り扱うネットワークについて

① 個人情報を取り扱うシステムは、できる限りイントラネットで構築するべきであり、インターネットとは切り離すべきである。

② ネットワークを分けることで、ウイルス対策や外部からのアクセス等を防ぐことができる。

また、個人情報を取り扱うネットワークに接続されたコンピュータについては、FDD、CD類やUSBメモリ等の媒体を利用できない仕組みとしておき、外部へのデータの持ち出しは必ずシステム管理者を介する仕組みにする。そうすることで持ち出すデータの管理ができる。

③ 無線LANを使用している場合は、暗号化や登録したコンピュータしか接続できないなどセキュリティ対策を行う。

5．ファイル交換ソフト（Winnyなど）による情報の漏えいを防止するために [12)]

A）ファイル交換ソフト（Winny等）について

最近多発している情報漏えい事故は、職場外で利用したコンピュータにファイル交換ソフト（Winny等）がインストールされている場合、コンピューターウイルスに感染したことでコンピュータに保存されていたファイルが漏えいしたケースが多い。このため、職場外で利用されるコンピュータにファイル交換ソフト（Winny等）がインストールされていないことの確認を徹底する。特に、自宅で利用する個人用のコンピュータについては、以下の点に留意して欲しい。

① ファイル交換ソフトは、安易にインストールしないこと。

② ファイル交換ソフトの有無を点検し、同ソフトがインストールされたコンピュータでは、患者情報等の個人情報を扱わないこと。

③ 当該コンピュータに患者情報等の個人情報等が保存されているか否かを点検し、保存されている場合は適切に削除する等の措置をとること。

④ ウイルスに感染した場合には、直ちに情報流出を遮断する措置を講ずること。

B） Winnyネットワークを介して感染するウイルス（W32/Antinny）の特徴

新聞やテレビの報道によると漏えいした情報の種類こそ違うが、ほとんどの事件に共通した点は、職員がファイル交換ソフト Winny をインストールした個人所有のコンピュータに学校や企業等で取り扱う個人情報や機密情報等をコピーして使用していた際、ウイルス（W32/Antinny）に感染して情報漏えいに繋がっていることである。

※ファイル交換ソフト： 自分のコンピュータにあるファイルを、ネットワーク経由で他人がアクセスできる状態におき、複数人でファイルを「共有」することができるソフトウェアのこと。ファイル共有ソフトとも言われ、大変多くのファイル交換ソフトが出回っている。

Winnyがインストールされたコンピュータで、ウイルス（W32/Antinny）に感染すると、コンピュータ内の送受信メールや表計算ソフトやワープロソフト等のデータファイルが、コンピュータ内の公開フォルダにコピーされる。公開フォルダにコピーされたファイルは、世界中のWinny利用者が入手できる状態になったということになる。

インターネット（Winnyのネットワーク）に流出したデータは、不特定多数のWinny利用者

が保有することになり、回収することは不可能である。このため、情報漏えいを未然に防ぐことがとても重要となる。

なお、中小企業や個人事業者、一般の個人ユーザーの情報漏えいがニュースに取り上げられないのは、漏えいした情報がどこからのものか特定できない、重要ではないと考えられた場合などで、ニュース性が低いため報道機関が取り上げなかっただけであり、 情報漏えいが「ない」ということではない。情報漏えい事故は、他人事と考えずに自分に当てはめて考えることが重要である。

C）管理的対策のポイント（コンピュータ利用のルールを策定して運用）

① ファイル交換ソフトの使用条件を定めておく。

組織（委託先を含む）で業務上使用するコンピュータについては、ファイル交換ソフトの使用条件を定めておくことが重要である。コンピュータ内の情報が漏えいする危険性を考慮すると、個人情報や機密情報等が保存されているコンピュータではファイル交換ソフトの使用を控えるべきである。

② 個人所有コンピュータの利用条件を定めておく。

個人所有コンピュータは組織的に管理することが困難なため、業務で使用することが望ましいこととは言えない。さらに、個人所有コンピュータで患者個人情報や機密情報等を取り扱うことが極めて危険なため、避けるべきである。しかし、止むを得ずに個人所有コンピュータを業務で使用する場合は、利用条件等を定めておくことが重要である。

③ 個人情報や機密情報等の外部への持ち出しについてのルールを定めておく。

個人情報や機密情報等を含む業務情報を記録媒体などにコピーして外部へ持ち出すことは外部のコンピュータからの情報漏えいや記録媒体の紛失などのリスクがあり、厳に避けるべきである。 しかし、止むを得ずに持ち出す場合は、厳重に管理することが重要である。

④ 職場におけるクライアントコンピュータのウイルス対策状況を把握しておく。

サーバーを介さずに P2P により外部と接続することが可能なクライアントコンピュータは、サーバーの段階でウイルスチェックがされていても、クライアントコンピュータにウイルス対策ソフトを導入していない場合は感染する危険性が高い。新種や亜種のウイルスに対応するため、ウイルス対策ソフトのパターンファイルの更新を定期的に行うことが肝要である。

⑤ 職員にウイルス対策の重要性を再認識させる。

ニュースで取り上げられた Winny 経由による情報漏えい事件は、ほとんどが個人所有のコンピュータを業務で使用したことにより被害が生じている。このことから、職員にウイルス対策の重要性に関する教育を繰り返し実施することが重要である。

D）技術的対策のポイント

以下の技術的対策は、オペレーティングシステム（OS）の機能として提供されるものと、ツールを導入して運用するものがある。

① 重要情報はアクセス制限を設ける。
② 重要な情報はコピー制限を設ける。
③ USB メモリ、取り外し容易な外部記憶装置（USB、IEEE1394）、書き込み可能メディア(DVD-R 等、CD-R 等、FD）の利用制限。
④ 個人所有のコンピュータを病院など職場内ネットワークに接続する際の制限を設ける。

６．具体的な対策

A）その１

Winny などのファイル交換ソフトによる情報漏えい事故を防ぐには、次のような対策が考えられ、それらを組み合わせて実施することが有効とされている。

① 漏えいしては困る情報を取り扱うコンピュータに Winny などファイル交換ソフトをインストールしない。
② 職場コンピュータに許可無くソフトウェアをインストールしない。もしくはインストールできない設定にする。
③ 職場のコンピュータを外部に持ち出さない。
④ 職場のネットワークに個人所有コンピュータを接続しない。もしくは接続できない設定にする。
⑤ 自宅に仕事を持って帰らなくて済むように適切な作業量の管理を行う。
⑥ 職場のコンピュータから USB メモリや CD 等の媒体に情報をコピーしない。もしくはコピーできない設定にする。
⑦ 漏えいしては困る情報を許可無くメールで送らない。もしくは送信できない設定にする。
⑧ ウイルス対策ソフトをインストールし、最新のウイルス定義ファイルで常に監視する。
⑨ 不審なファイルは開かない。

コンピュータの管理者や利用者が自ら実施できる対策もあれば、上司が行うべき対策もある。また、職場のルールを変更したり、ネットワークシステムや設備の変更を伴う対策もある。どの対策を組み合わせるかは、簡単なもの、効果がありそうなものというような単純な選択ではなく、取り扱う情報と漏えい時の影響、導入コスト等を考慮し総合的に検討することが重要となる。

個人情報や機密情報等の情報漏えいを防ぐためにどのような対策を行うべきか、以下に管理対策と技術的対策をまとめた。各施設においては対策のポイントを参照し、トラブルの発生を未然に防ぐよう対処していただきたい。

B）その2

・ウイルス（W32/Antinny）の感染を確認する方法

① セキュリティベンダーのウイルス対策ソフトによるスキャン
市販またはフリーソフトウェアのウイルス対策製品を利用し、コンピュータ内のウイルス感染の有無をスキャンする。

② マイクロソフト社の「悪意のあるソフトウェアの削除ツール」を使い、ウイルスの検索と駆除を行う。

TREND MICRO「Winny 悪用ウイルス専用駆除ツール」[13]：
http://jp.trendmicro.com/jp/threat/solutions/winny/
Winny 使用禁止 Tool[14]：
http://www.asahi-net.or.jp/~tz2s-nsmr/soft/winnychk/WinnyChk.htm
ファイル共有ソフトによる情報の流出について[15]：
http://www.microsoft.com/japan/athome/security/online/p2pdisclose.mspx

・情報が漏えいしているかを確認する方法

① Winny を使用している場合、公開用の「UP」フォルダに何らかのファイルが保存されており、それが自分の指定したファイルでなければ漏えいしている危険性が高い。また、「UP」フォルダにファイルが無い場合でも、Winny が保存されているフォルダの「UpFolder.txt」ファイルに他のフォルダが公開用として指定されている可能性もある。当該ファイルを開いて記載内容を確認し、「UP」フォルダ以外に指定されているフォルダが無いことを確認する。

② 自社の情報が Winny ネットに流出していないかを確認する場合、Winny を利用してやり取りされているファイルをダウンロードして確かめる以外に方法がない。各種報道を見ると、他者から指摘されて気付くケースがほとんどである。また、Winny ネットワークで流れているデータを検索してくれるサービスもある。このようなサービスを利用して、自社の情報が流出していないかを確認する方法もある。

・Winny がインストールされているかの確認と削除する方法

セキュリティベンダーから、 Winny そのものを検出するツールが無償で提供されている。そのツールを利用して Winny として検出されたファイルを全て削除する。検出されたファイルが Winny.exe の場合は、そのファイルが入っていたフォルダも含めて削除する。これは、Winny を起動した際に Winny.exe と同じフォルダ内に設定ファイルが作成されるので、これらのファイルも同時に削除するためである。また、Windows コンピュータ等で複数のユーザーで１台の PC を使用している場合、ユーザーアカウント毎に同様の検出、削除の処置を行う必要がある。

なお、当会として上記作業にて生じたトラブル・損失・損害には、一切の責任を負いかねる。くれぐれも自己責任、自己判断の下、実施していただきたい。

・ウイルス（W32/Antinny）により情報漏えいしていることが発覚した場合の対応

① 当該コンピュータをネットワークから切り離す（LAN ケーブルを抜く）。
② Winny を削除する前に、漏えいしたファイルを特定する。
③ 事後調査のため、漏えいしたファイルを CD や DVD 等の記憶媒体にコピーする。
④ 漏えいしたファイルの中の個人情報、機密情報を特定する。
⑤ 各施設の情報ファイルである場合は、当該組織に速やかに報告する。
⑥ ウイルス対策ソフトでスキャンし、感染した原因を特定する（Antinny 亜種の特定）。
⑦ 当該コンピュータ上で保存すべきデータをバックアップする。
⑧ ウイルスを駆除する。もしくはコンピュータのリカバリを行う（初期状態へ戻す）。
⑨ IPA にウイルス被害を届け出る。

7. コンピュータや USB メモリなどの外部記憶装置の盗難や紛失、修理時の注意点 [16)]

業務上使用しているコンピュータには、業務に関連した各種ファイルが記録されている。このため、盗難や紛失に伴い、記録ファイル中に顧客リストがあれば個人情報の流出に繋がり、社外秘のファイルがあれば企業の機密情報が漏えいしてしまうことになりかねない。部外者の出入りがある場所の業務上使用しているコンピュータには、ワイヤーロックなどの鍵をつけ盗難防止策を講ずる。業務用システム更新時には、委託業者との間で個人情報漏えい対策などチェックしておくべき点について確認する。できる限り契約書などの書面に残すことが望ましい。また、このような危険性は個人用のコンピュータでも同様に存在する。よく「大したファイルはないから大丈夫」などと耳にするが、安易な考え方は被害をより拡大させることもある。連絡先や住所録などのデータは個人情報であり、デジタルカメラで撮影した記念の写真やメールなども永久に失われることがある。

さらに、インターネットに接続するための設定も重要な情報である。たとえばコンピュータを入手した人物がプロバイダーにアクセスし、接続のためのパスワードを変更すれば、本来のユーザーが設定した情報にアクセスできなくなり、解約すらできないことも考えられる。

Windows コンピュータではログインパスワードを設定し、さらに指紋認証などのセキュリティ機能がある製品を利用することが望ましい。コンピュータは、決して車内などに放置しない。

USB メモリなどの外部記憶装置についても、指紋認証や暗号化対策などセキュリティ機能のある製品を利用することが望ましい。

また、エクスプローラ等を用いて「削除」を実施しただけでは表向きデータがみえないが、実際は後に別途データの書き込みを実施した時に上書きされるまでそのまま残されている状態であり、完全に削除されていない。市販の復元ソフトやデータ復旧サービス会社を使うと多くは復活できてしまう。コンピュータ、外部記憶装置等を破棄する場合は、ハードディスク装置を物理的に破壊する。または、

ハードディスクイニシャライズ用ソフトを利用して全てをフォーマットする等の対策が望まれる。

コンピュータの修理は利用者レベルでの対応は困難なものであるため、納入業者等への修理を依頼することになるが、修理時等のハードディスク内のデータの取り扱いについて予め個人情報保護に関する覚書などを交わしておくことが望まれる。

システム導入時には、各種アプリケーションの納入業者、コンピュータ本体（ハードウェア）の納入業者、コンピュータ本体（ハードウェア）の保守業者等とそれぞれがバラバラになる可能性があり、修理時に情報が漏えいした場合責任の所在があやふやになるケースが考えられる。購入から保守までひとつの業者で対応できるパターンが望ましい。

A） 他人の手に渡ってしまった場合の備え

業務上使用するコンピュータや個人で使用しているパソコンは、盗難や紛失時の対策を講じておく必要がある。また、コンピュータを買い換えて下取りに出す場合も注意が必要である。

中古コンピュータを購入した場合、以前使用していたユーザーのデータが残っていたというニュースをしばしば耳にする。これは、下取りなどで引き取った使用済みコンピュータが、適切な処理をされずに中古品販売ショップに流れてきたケースである。

コンピュータに記録されているデータは、ユーザー自身が管理し保護しなければならない。そのため、データの暗号化やパスワードによる保護といった手段があるが、このような処理を実施する際は何をどのように保護しているかを正しく理解することが重要となる。

B） コンピュータや USB メモリなどの外部記憶装置を盗難や紛失した場合

① 個人情報、機密情報が保存されていないかを確認する。

② 当該組織（個人情報管理責任者）に速やかに報告する。

③ 対策委員会の指示に従い対処する。

8．情報漏えいが起こった場合の対処 [17)]

＜情報漏えい対応の基本ステップ＞

A）発見・報告：情報漏えいに関する具体的な事実を確認した場合は、責任者に報告する。

B）初動対応：対策本部を設置し当面の対応方法を決定する。

C）調査

D）通知・報告・公表：漏えいした個人情報の本人などへ連絡、監督官庁、警察、IPA などへ届け出、ホームページ、マスコミ等による公表を検討する。

E）抑制措置と復旧：情報漏えいによって発生した被害の拡大の防止と復旧のための措置を行う。

F）事後対応：抜本的な再発防止策を検討し実施する。

透明性・開示の原則から、発生した情報漏えいについてなるべく早く公表を行うことを考える。

個人情報が漏えいした場合は、本人にその事実を知らせ謝罪するとともに、詐欺や迷惑行為などの被害にあわないように注意喚起する。個人情報漏えいの被害者や関係者に通知し意向を確認した上で、一般に公表が必要と判断される場合は、ホームページでの掲載、マスコミ等への公表を行う。

9．漏えい事故が起こった場合の賠償について[18)]

＜2006 年＞

2006 年の個人情報漏えいに於ける被害者の数は 2223 万人である。漏えい事故・事件 1 件あたりの平均被害者数は 2 万 3000 人（被害者数が不明の事例を除外して計算）。単純計算すると、日本国民の 6 人に 1 人が個人情報漏えいの被害に遭っている。1 人あたりの賠償額は、平均 3 万 6000 円という結果である。すべての漏えい事故・事件を合計すると 4570 億円（1 件当たりの平均賠償額 4 億 8000 万円）になる。

個人情報漏えい事故　被害者総数　2223 万人

1 件当たりの平均賠償額　4 億 8000 万円

※nikkei BPnet　第 66 回個人情報の漏洩、すべて金銭で賠償したら 4570 億円に相当より

10．関係する法律（罰則規程）について

A）個人情報の保護に関する法律

六ヶ月以下の懲役又は三十万円以下の罰金

B）臨床検査技師、衛生検査技師等に関する法律第十九条

第十九条の規定に違反した者は、五十万円以下の罰金

C）不正アクセス行為の禁止等に関する法律

一年以下の懲役又は五十万円以下の罰金

D）地方公務員法　第三十四条

最高一年の懲役又は最高三万円以下の罰金

Ⅲ．ガイドラインの目的と留意事項

１．本ガイドラインの対策は、主として職場における対策である。

職場の個人情報や機密情報等を自宅のコンピュータにコピーしなければ情報漏えいが起きないということではない。家族や友人の個人情報が漏えいする可能性と同様である。Winny などのファイル交換ソフトを導入したコンピュータには、情報漏えいのリスクがあり、ウイルス対策が必要となる。

２．Winny を使用しなければ情報漏えいしないということではない。

Winny に感染するウイルス（W32/Antinny）以外にも情報漏えいするウイルスが出現しているので、ウイルス対策を行うことが情報漏えいを防止するために大変重要である。また、情報漏えいを起こす手段をなくすことが大切である。（ファイル交換ソフト類は使用しないなど）

３．コンピュータを使用する限り、常に最悪の状況を想定してセキュリティ対策を実施する必要がある。

４．本内容にて生じたトラブル・損失・損害には、一切責任を負いかねる。自己責任、自己判断の下ご検討いただきたい。

Ⅳ. 参考文献

1） 田淵義朗, 萩原栄幸：45 分でわかる個人情報保護, 6-9, 日経ＢＰ社, 2005

2） 経済産業省：個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン, 2004
http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf

3） 厚生労働省：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, 2004
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805-11a.pdf

4） 東京都病院経営本部：都立病院における患者情報の取扱いについて, 2005
http://www.byouin.metro.tokyo.jp/osirase/sonota/kojinjouhou.html

5） 社団法人 日本病理学会：症例報告における患者情報保護に関する指針, 2001
http://jsp.umin.ac.jp/guidelines/guideline_20011126.html

6） 特定非営利活動法人 日本臨床細胞学会：症例報告における患者情報保護に関するに指針, 2006
http://www.jscc.or.jp/shorei.html

7） 日本臨床検査医学会：臨床検査を終了した検体の業務、教育、研究のための使用について, 2002
http://www.jscp.org/kentai.htm

8） 宮島理：ネット危険地帯, 第27回「紙」のセキュリティーが問題だ――情報流出ルート第1位、実は紙媒体, 2007
http://it.nikkei.co.jp/security/column/web_miyajima.aspx?n=MMITzt000005062007

9） 厚生労働省：「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」に関するＱ＆Ａ（事例集）, 2005
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805iryou-kaigoqa.pdf

10） 財団法人 日本情報処理開発協会： JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン　－ 第１版 － , 2006
http://privacymark.jp/reference/index.html

11） Type74 Software：ファイル暗号化ソフト「ED」関連（ED 安定版）, 2005
http://type74.org/

12） 独立行政法人　情報処理推進機構：「Winny」による情報漏えいを防止するために, 2006
http://www.ipa.go.jp/security/topics/20060310_winny.html

13） TREND MICRO：「Winny 悪用ウイルス専用駆除ツール」
http://jp.trendmicro.com/jp/threat/solutions/winny/

14） 西村誠一：Winny 使用禁止 Tool ver1.3
http://www.asahi-net.or.jp/~tz2s-nsmr/soft/winnychk/WinnyChk.htm

15） Microsoft：ファイル共有ソフトによる情報の流出について, 2006
http://www.microsoft.com/japan/athome/security/online/p2pdisclose.mspx

16） FUJITSU：もしもパソコンが盗難にあったら？：前編, 2006
http://azby.fmworld.net/soho/special_issue/security2006autumn/stolen/index.html?sohofrom=navifollowpage

17） IPA 独立行政法人　情報処理推進機構　セキュリティセンター: 情報漏えい発生時の対応ポイント集,2007
http://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf

18） Nikkei BPnet：第 66 回　個人情報の漏洩、すべて金銭で賠償したら 4570 億円に相当, 2007
http://www.nikkeibp.co.jp/style/biz/skillup/spam/071029_66th/index.html

Ⅴ．編集後記

AiCCLS 活動において、臨床検査情報システム研究班の愛知県臨床検査値統一化ガイドラインとして「情報マネジメントシステム」ガイドラインを作成し、第 1 版として「個人情報保護および漏えい事故防止の対策」を作成した。各施設の個人情報の保護に関する関係法令等に基づき、適正な取り扱いの確保に努めていただいていると思われる。しかし昨今、新聞報道等で病院や企業等から持ち出された個人情報の漏えい事故が多く報じらており、USB メモリやファイル交換ソフトによる情報漏えいが大部分を占めている。データの暗号化、コンピュータのセキュリティを再度見直し被害者、加害者とならいよう日頃から対策を取るよう心がけていただきたい。本書は、指針とする部分はあるものの、IT 技術の進化などによりまだまだ検討の余地があると思われるため、個人情報の取り扱いや情報漏えい事故に対する問題提起として考えていただき、今一度、自分自身の情報の取り扱いについて考えていただく礎になれば幸いである。

臨床検査情報システム研究班

濱島　剛

ガイドライン作成委員会

作成委員長　　濱島　剛　　（藤田学園　法人本部　情報マネージメント部）

ガイドライン作成協力

愛知県臨床衛生検査技師会　　臨床検査情報システム研究班

問い合わせ先

愛知県臨床検査標準化協議会事務局

〒450－0002

名古屋市中村区名駅五丁目 16 番 17 号

花車ビル南館 1 階

（社）愛知県臨床衛生検査技師会事務所

Tel　052－581－1013

Fax　052－586－5680

愛知県臨床検査標準化ガイドライン
「個人情報保護および漏えい事故防止の対策」
第 1 版

発行　　平成 21 年 11 月
発行所　愛知県臨床検査標準化協議会
発行者　大野 和美
編集者　岸 孝彦・平松 久美子・濱島 剛