

200501362A

厚生労働科学研究費補助金
医療技術評価総合研究事業
診療録等の電子保存の評価方法に関する研究

平成17年度 総括研究報告書

主任研究者 遠藤 明

平成18(2006)年3月

目 次

I. 診療録等の電子保存の評価方法に関する研究	1
遠藤 明	
II. 診療録等の電子保存の評価方法に関する研究の結果	5
1. 診療録等の電子保存調査	5
遠藤 明	
1. 1 調査概要	5
1. 2 調査票(チェックシート)と評価基準	7
1. 3 調査結果	29
1. 4 最低限のガイドラインに関する考察	62
1. 5 推奨されるガイドラインに関する考察	125
1. 6 診療録等の電子保存アンケートの結果	150
2. 「医療情報システムの安全管理に関するガイドライン」について	161
山本隆一	
2. 1 はじめに	161
2. 2 安全管理ガイドライン作成の背景	161
2. 3 安全管理ガイドライン概説	162
2. 4 安全管理ガイドラインの意義と問題点	169
2. 5 医療情報システムの安全管理に関するガイドラインについて	174
(スライド)	

3. 「診療録等の電子保存の評価」の病院機能評価における考察	201
高原亮治	
3. 1 病院機能評価とは	201
3. 2 病院機能評価における診療録等の電子保存の評価	201
3. 3 謄写員機能評価における安全管理の項目について	205
3. 4 安全管理ガイドラインの要求事項の病院機能評価から見た考察	206
3. 5 病院機能評価での安全管理ガイドラインへの取り組み	208
4. 「診療録等の電子保存システム」に関する ISO/IEC15408 (Common Criteria) の視点から見た概要設計	217
喜多絃一	
4. 1 ISO/IEC15408 : IT セキュリティの国際評価標準の ポイントと動向	217
4. 2 「医療情報システムの安全管理に関するガイドライン」の CC 的位置付け	224
4. 3 ガイドラインの規範化について	234
4. 4 プロテクションプロファイルとセキュリティターゲット (資料)	247

I. 診療録等の電子保存の評価方法に関する研究

遠藤 明

(財)医療情報システム開発センター

厚生労働科学研究費補助金（医療技術評価総合研究事業）

総括研究報告書

診療録等の電子保存の評価方法に関する研究

主任研究者 遠藤 明 （財）医療情報システム開発センター 専務理事

研究要旨

診療録等の電子保存については、これまでの経緯を踏まえ、平成 17 年 3 月、「医療情報システムの安全管理に関するガイドライン（以下、「新ガイドライン」という）」が取りまとめられ、公表された。本研究班では、医療機関の情報システムにおいて電子保存が新ガイドラインに基づいて一定の水準にあるかどうかを第 3 者が評価する手法を研究・開発した。評価手法については、新ガイドラインへの適合状況を現実的なレベルで出来るだけ曖昧さのない形でチェックシートにすることと、そのチェック結果に対する評価基準を作成することによった。続いてこの評価手法を実際に診療録等の電子保存を実施している医療機関に適用してみて、「新ガイドライン」への適合状況を調べてみることで、この評価手法の検証と見直しを行った。

また、新ガイドラインの個別要求事項ごとの電子保存実施状況に対する考察、及び医療機関等とベンダーに対する新ガイドラインの認知度や電子保存の実施状況に関するアンケートを実施した。また、病院機能評価との関連、及び情報通信機器の安全性に関する規格である ISO/IEC 15408 との関連を考察した。

分担研究者

山本隆一 （東京大学大学院情報学環 助教授）
喜多紘一 （東京工業大学情報工学研究施設 教授）
高原亮治 （（財）日本医療機能評価機構 副理事長）

A. 研究目的

新ガイドラインにより、電子保存に必要な技術的基準と要求事項が明確に示されているものの、その具体的手

法や技術、運用方針について細かく示されていないことから、電子カルテシステムのベンダーおよび医療機関等の利用者にとって、電子カルテの導入

が困難となっている可能性がある。このため、ベンダーや医療機関が実施しやすい具体的技術・運用方針が提供されるとともに、それを検証する仕組みが必要である。

医療機関を対象とした評価や監査には、(財)医療機能評価機構の実施する病院機能評価、厚生労働省の実施する医療監視、医療指導監査等があるが、いずれの制度においても、診療録等の電子保存の状況については十分評価されていないため、医療機関において、通知によって求められている3基準を満たさないまま電子保存がなされている可能性がある。このため、これら既存の評価や監査制度を補完する仕組みが必要である。

電子カルテ導入医療機関における医療指導監査は、監査に先立って診療録等の紙への打出しが求められ、これをもって指導が行われているが、極めて非効率である。電子カルテの普及に伴い、電子カルテの画面を利用した指導の必要性が議論されている。一方、画面での指導にあたっては、診療録の記録内容が改ざんされていないこと

(真正性)等があらかじめ立証されている必要がある。

B. 研究方法

(1) 現在電子保存を行っている医療機関等における新ガイドラインへの対応状況調査

既に電子カルテ等の電子保存システムを導入し、原本の電子保存を行っている医療機関等における新ガイドラインへ

の対応状況等について調査した。調査は11施設に対し、調査票と調査票回答を踏まえた現地調査を実施した。

(2) 評価方法の検討

(1)の調査結果と新ガイドラインにおける要求事項を吟味し、新ガイドラインへの対応度を確認するチェックシートや評価基準を作成した。また、この調査結果を踏まえ、新ガイドラインの各要求事項の考察を実施した。

(3) 電子保存アンケートの実施

医療機関やベンダーに対し、新ガイドラインの認知度や電子保存の実施状況に関するアンケートを実施した。対象は300床以上の約900病院と保健医療福祉情報システム工業会医療システム部会会員約180社とした。

(4) 新ガイドラインに対する既存評価制度からの考察の実施

新ガイドライン策定の背景と意義及び新ガイドラインと病院機能評価との関連について考察し、新ガイドラインをISO/IEC15408(Common Criteria)の視点から見た設計を実施した。

C. 研究結果

(1) 現在電子保存を行っている医療機関等における新ガイドラインへの対応状況調査

既に電子カルテ等の電子保存システムを導入し、原本の電子保存を行っている医療機関等における新ガイドラインへの対応状況等について調査した。調査は11機関（病院5、診療所3、薬局3）に対し、調査票への機関回答と調査票回答を踏まえた調査員による現地調査を実施した。

その結果、電子保存について、新ガイドラインへの対応状況は機関種別毎、機関毎、個別要求事項毎に大きなバラツキがあることが分かった。機関種別では病院は最低限の要求水準に近かったが、診療所や薬局の基本的な安全管理への対応状況は低かった。病院は、職員数も多く、各種のマニュアル等を整備して組織的にものごとを進めていく必要性が高いのに対し、診療所、薬局は規模が小さく、責任者の目の届く範囲でものがと進められているため、手順を規定化し、客観的に安全性を高める習慣が乏しいものと考えられた。

個々の項目では、アクセスログの定期的な確認を行うことが難しい。確認のためのツールの作成など、容易にする工夫が必要である。

また、電子署名やタイムスタンプはまだ使っているところが多かったが、真正性を主張す

るためにこれらは重要な意味を持つ技術である。インターネットにつながれていない環境が多いという現実も踏まえ、使いやすい環境の実現が必要である。

（2）評価方法の検討

（1）の調査結果と新ガイドラインにおける要求事項を吟味し、新ガイドラインへの対応度を確認するチェックシートや評価基準を作成した。また、この調査結果を踏まえ、新ガイドラインの最低限及び推奨の各要求事項の考察を実施した。

病院ではガイドラインの要求事項に対する必要性の認識が欠落している部分が目立った。（アクセス記録の確認、メディア管理、パスワード管理、再委託の管理、廃棄管理）

診療所や薬局では情報に対してアクセスできるスタッフが少数であるため、規定化やシステム対応が行なわれていないという背景が目立った。

（3）電子保存アンケートの実施

医療機関等へ新ガイドラインの認知度や電子保存の実施状況に関するアンケートを実施した。対象は300床以上の約900病院と保健医療福祉情報システム工業会医療システム部会会員約180社とした。

その結果、約350の病院と24社から回答を得た。新ガイ

ガイドラインを基準又は参考にしている病院は51%にのぼり、33%でカルテの部分的電子保存が行なわれ、38%でフィルムの部分的電子保存が行なわれている。また、49%が新ガイドラインに準拠した電子保存について、第三者認証制度を望んでいた。また、ベンダーでは新ガイドラインを意識した取り組みをしているが、システムの新ガイドラインへの対応状況を医療機関等へ明示はしていなかった。

(4) 新ガイドラインに対する既存評価制度からの考察の実施

山本は新ガイドライン作成の作業班で主査を勤めた立場から、新ガイドラインの作成の背景、内容の概説、意義と問題点について記述した。高原は、新ガイドラインと病院機能評価との関連について考察し、今後の病院機能評価における評価項目案を提案した。喜多は、ISO/IEC 15408 (Common Criteria : CC) を概説し、新ガイドラインをCCの観点から解説するとともに、真正性についてプロテクションプロファイル化を試みた。

D. 考察

本研究により、医療機関等及びベンダーの対応状況や認識は高いものであることが明らかにされた一方で、新

ガイドライン対応状況は機関種別毎、機関毎、個別要求事項毎に大きなバラツキがあることが分かった。また、電子保存アンケートにおいても、病院やベンダーによるバラツキが目立った。今後さらに新ガイドライン普及への努力が必要であると同時に、新ガイドライン遵守を容易にするシステム側の環境整備や、第三者による評価制度が求められる。

E. 結論

本研究は、電子保存の現状を把握し、新ガイドラインの対応チェックシートや評価基準、電子保存対応のバラツキの考察を提供することにより、新ガイドラインの活用を進め、ひいては医療のIT化に資することを期待するものである。

F. 健康危険情報

特記事項なし。

G. 研究発表

特記事項なし。

H. 知的財産権の出願・登録状況

特記事項なし。

Ⅱ．診療録等の電子保存の評価方法に関する研究の結果

1. 「医療情報システムの安全管理に関するガイドライン」について

遠藤 明

(財)医療情報システム開発センター

1. 1 調査概要

(1) 名称

診療録等の電子保存に関する調査

(2) 目的

「医療情報システムの安全管理に関するガイドライン」(平成17年3月厚生労働省)が実際に電子カルテ等を運用している医療機関等で適用されている状況を調査し、電子保存の外部評価基準の作成に役立てる。

(3) 対象施設

全国11ヶ所(病院5箇所、クリニック3箇所、薬局3箇所)

(4) 調査方法

対象施設に対し、医療情報システムの安全管理に関するガイドライン(6章、7章、9章)に基づくアンケート形式の調査票(Ⅱ1.2参照)を送付し、回答を返送してもらう。また、後日に対象施設を調査員が訪問し、現地調査(補足調査)を行う。

(5) 調査時期

平成17年10月初旬	調査票送付
平成17年10月中旬～18年1月下旬	調査票回収
平成17年11月上旬～18年1月下旬	現地調査

(6) 現地調査

(病院1)、(医院8)、(薬局10)については、施設の都合により現地調査は実施せず。その他の8施設に対し、現地調査を実施した。

(7) 結果の集計と考察

調査票を回収し、「アンケート項目別評価基準」(Ⅱ1.2参照)にしたがって集計した後、医療機関を個別訪問し補足調査を行い、補足調査の結果を踏まえて整理した。そして、「医療情報システムの安全管理に関するガイドライン」の構成に基づき、以下の5つのグループに分けて調査結果を集計した。

- | |
|----------------|
| 1. 最低限のガイドライン |
| (1) 基本的な安全管理 |
| (2) 電子保存 |
| (3) スキャナ |
| 2. 推奨されるガイドライン |
| (1) 基本的な安全管理 |
| (2) 電子保存 |

集計結果に基づき、「医療情報システムの安全管理に関するガイドライン」の「最低限のガイドライン」と「推奨されるガイドライン」に分け、ガイドラインの各々の項目に対し、大規模な医療機関である病院（5箇所）と比較的小規模であるクリニック・薬局（6箇所）に分け、各々の傾向、背景、対策案について考察を行った。

（８）調査依頼文

平成17年 月 日

〇〇〇病院 病院長様

平成17年度厚生労働科学研究事業
「診療録等の電子保存の評価方法に関する研究」班

主任研究者 遠藤 明
(財団法人医療情報システム開発センター専務理事)

診療録等の電子保存に関する調査協力へのお願い

拝啓 時下益々ご清祥のこととお慶び申し上げます。

さて、今春厚生労働省から「医療情報システムの安全管理に関するガイドライン」が出されました。本研究班では、電子保存の外部評価について、その評価基準等を取りまとめるべく、実際に電子カルテ等を利用されている医療機関等における上記ガイドラインの適合状況を調査することとしました。つきましては、別添調査票にご回答いただきますとともに、後日10月から1月までの間に訪問させていただき、補足調査をさせていただきたいと存じます。

ご多忙のところぶしつけなお願いではありますが、研究成果は外部評価のみならず内部評価にも利用できるものとして公表し、国内の電子保存のレベル向上に役立てたいと考えておりますので、ご協力いただきますようお願い申し上げます。

なお、ご協力の可否について、別紙FAXにてご連絡いただきたく、あわせてお願い申し上げます。

敬具

<同梱内容物一覧>

- 別紙1:調査の概要
- 別紙2:ご協力可否のFAX連絡票
- 別紙3:調査票記入要領(調査票記入例を含む)
- 別紙4:診療録等の電子保存に関する調査票
- 別紙5:調査票用語集
- 別紙6:FAX質問票
- 小冊子:「医療情報システムの安全管理に関するガイドライン」資料集

1. 2 調査票（チェックシート）と評価基準

「医療情報システムの安全管理に関するガイドライン」に基づくアンケート形式の調査票を作成し、協力医療機関（病院 5 箇所、クリニック 3 箇所、薬局 3 箇所）に郵送した。回答方式は、複数選択肢からの択一または複数選択とした。この際、「医療情報システムの安全管理に関するガイドライン」も同封した。調査票には、アンケート質問の項番と「医療情報システムの安全管理に関するガイドライン」の該当章番号・ページ番号を明記した。繰り返し同じ質問を行う部分については、その旨を明記した。（例：アンケート項番 1.3.1.(9) と 1.3.1.(11)）

回答の評価基準は、「アンケート項目別評価基準」の通りである。評価基準については協力医療機関には知らせていない。

アンケート項目別評価基準	
アンケート項目別評価	評価方法表記
回答	
ガイドライン	
頁	項目
回答	
・ 調査の対象となる情報システムについて	
0. 1. 1.(1) 当調査の回答をいただく情報システムについてお伺いします。	1. 電子診療録(電子カルテシステム) 2. 放射線診断システム 3. 電子調剤録(調剤支援システム) 4. その他の部門システム(具体的に:)
・ スキャナによる電子保存について	
0. 2. 1.(1) スキャナによる電子保存を行っていますか。	はい/いいえ
0. 2. 1.(2) スキャナによる電子保存と紙保存を併用していますか。	はい/いいえ
1. 情報システムの基本的な安全管理	
1. 1 組織的安全管理対策(体制、運用管理規程)	
1. 1.1 最低限のガイドライン	15
1. 1. 1.(1) 情報システム運用責任者及び担当者を定める規定がありますか。	15 63C1 Y/N Y:可
1. 1. 1.(2) サーバ室、診療室、医局など、個人情報情報を参照できる区画に対して入退室管理規定がありますか。	15 63C2 Y/N Y:可
1. 1. 1.(3) システムへのアクセス管理規定(アクセス制限、アクセス記録、記録の点検)を定めていますか。	15 63C3 Y/N Y:可
1. 1. 1.(4) 個人情報の取り扱いを外部業者に委託する場合、委託契約において安全管理に関する条項を定めていますか。	15 63C4 Y/N Y:可
1. 1. 1.(5) 運用管理規定に、個人情報漏洩などのリスクに対する予防策、発生時の対処方法を明記していますか。	15 63C5 1 1,2共に○で可 2 1,2共に○で可 3 不可
1. 1. 1.(6) 運用管理規定に、個人情報の記録メディアの管理ルールを定めていますか。	15 63C5 1 1,2共に○で可 2 1,2共に○で可 3 不可
1. 2 物理的安全対策	17
1. 2.1 最低限のガイドライン	17
1. 2. 1.(1) 個人情報保存されているハードウェアの設置場所及び記録メディアの保管場所は施錠されていますか。	17 64C1 Y/N Y:可
1. 2. 1.(2) 診療室、医局など、個人情報情報を扱うパソコンが設置されている区画には、業務時間帯以外は、許可を受けた担当者以外が立ち入ることができないような対策を講じていますか。	17 64C2 1 可 2 可 3 可 4 具体的内容によって判定 5 不可
1. 2. 1.(3) サーバ室、診療室、医局など、個人情報情報を参照できる区画に対して入退室管理記録を付けていますか。	17 64C3 Y/N Y:可

項番	アンケート内容	回答	アンケート項目別評価基準	
			回答項目別評価	評価方法表記
1. 2. 1.(4)	個人情報情報が保存されている区画で業務を行う職員には名札の着用を義務づけていますか。	はい/いいえ	17 64C3	Y/N Y:可
1. 2. 1.(5)	個人情報情報が保存されているパソコンの盗難防止対策を施していますか。	1. 盗難防止チェーンをつけている 2. その他の盗難防止対策を施している(具体的に:) 3. 盗難防止対策はとっていない	17 64C4	1 可 2 具体的内容によって判定 3 不可
1. 2. 1.(6)	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講じていますか。(例: パスワード付きスクリーンセーバー)	はい/いいえ	17 64C5	Y/N Y:可
1. 2. 2. 推奨されるガイドライン			17	
1. 2. 2.(1)	個人情報情報が保存されている区画に対し、防犯カメラや自動侵入監視装置などのセキュリティ機材を設置していますか。	はい/いいえ	17 64D	Y/N Y:可
1. 3 技術的安全対策			22	
1. 3. 1. 最低限のガイドライン			22	
1. 3. 1.(1)	システムへログインする際に、ID・パスワードまたはICカードや生体認証などによる利用者の識別と認証を行い、IDまたはパスワードと組み合わせでログインできるようにしていますか。	1. ID、パスワードによる認証を行っている 2. ICカードによる認証を行っている 3. 生体認証を行っている 4. 上記1～3の方法を組み合わせてログインできるようにしている 5. 上記以外の認証を行っている(具体的に:) 6. 認証は行っていない (複数回答可)	22 65C1	1 可 2 可 3 可 4 可 5 具体的内容によって判定 6 不可
1. 3. 1.(2)	個人情報を含むデータを用いた情報システムの動作確認を行う際、動作確認を行う端末を制限するなど、データの漏洩対策を行っていますか。	1. 動作確認を行うパソコンを制限している 2. 動作確認作業と守秘義務契約を締結している 3. 動作確認を行う作業室に対する入室管理を行っている 4. その他の情報漏洩対策を講じている(具体的に:) 5. ともに情報漏洩対策は講じていない (複数回答可)	22 65C2	1 可 2 可 3 可 4 具体的内容によって判定 5 不可
1. 3. 1.(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っていますか。	はい/いいえ	22 65C3	Y/N Y:可
1. 3. 1.(4)	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りますか。	1. 職種のアクセス管理機能がある 2. 運用管理規定でアクセス可能範囲を定めている 3. 複数の職種の利用者がアクセスすることはない 4. その他(具体的に:)	22 65C3	1 可 2 可 3 NAとする 4 具体的内容によって判定
1. 3. 1.(5)	アクセス記録及び定期的なログの確認を行っていますか。ここでいうアクセス記録には、少なくとも利用者のログイン時刻及び時間、ログイン中に操作した患者が特定できる情報が必須です。	1. アクセス・ログをとっている 2. 操作記録を業務日誌に記録している 3. アクセス・ログまたは業務日誌を定期点検している 4. 上記のいずれも行っていない (複数回答可)	22 65C4	1 可 2 可 3 可 4 不可
1. 3. 1.(6)	システムにアクセス記録機能(アクセス・ログ)がない場合には、業務日誌などで操作の記録を必ず行っていますか。システムが利用する時刻情報はシステム全体で同期がとれており、定期的に日本標準時と一致させていますか。	1. システム内に時刻サーバを設け、すべてのハードウェアの時刻を同期させている 2. システム内の時刻サーバは日本標準時に合うよう調整している 3. インターネット上の時刻サーバを利用し、すべてのハードウェアの時刻を日本標準時に同期させている 4. 随時手動で時刻を同期させている 5. 上記以外の方法で時刻の同期を行っている(具体的に:) 6. 時刻の同期は行っていない (複数回答可)	22 65C5	1 可 2 可 3 可 4 可 5 具体的内容によって判定 6 不可

項目	アンケート内容	回答	ガイドライン		回答	アンケート項目別評価		評価方法表記
			頁	項番		回答	回答項目別評価	
1. 3. 1. (7)	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外部からの情報を受け取る際にはコンピュータウイルス対策を講じていますか。	1. すべてのパソコンにアンチウイルスソフトを導入している 2. アンチウイルスソフトウェアを導入している 3. その他のウイルス対策を行っている(具体的に: 4. ウイルス対策は行っていない	22	65C6	1 2 3 4	可 可 具体的内容によって判定 不可		
1. 3. 1. (8)	外部から持ち込まれた記録メディアをシステムに接続されているパソコンに挿入することがありますか。	はい/いいえ	22	65C6	Y/N	N: 可 Y: 可		管理されている適切な外部メディアを使用している場合は、可。
1. 3. 1. (9)	システム内にあるパスワードファイルに暗号化(不可逆)を施していますか。	はい/いいえ	22	65C7(1)前	Y/N	Y: 可		
1. 3. 1. (10)	システム管理者がパスワードを変更する場合は、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し、本人以外が知れない方法で再登録を実施していますか。	1. 利用者の本人確認を行っている 2. 本人確認方法を台帳に記載している 3. 本人以外が知れない方法で再登録を行っている 4. 上記のいずれも行っていない (複数回答可)	22	65C7(2)前	1 2 3 4	1,2,3共に○で可 1,2,3共に○で可 1,2,3共に○で可 不可		
1. 3. 1. (11)	システム内にあるパスワードファイルに暗号化(不可逆)を施していますか。	※ガイドライン6章5.0.7(1)(アンケート項番1.3.1.(9))に同じ。 はい/いいえ	23	65C7(3)	Y/N	Y: 可		
1. 3. 1. (12)	利用者は、パスワードは定期的に変更していますか。	1. 週に1回以上の頻度で変更している 2. 週に1回～月に1回の頻度で変更している 3. 2ヶ月に1回程度の頻度で変更している 4. 不定期に変更している 5. 変更していない (上記いずれかに○)	23	65C7(1)後	選	1,2,3: 可 4: 最多2ヶ月まで可 5: 不可		
1. 3. 1. (13)	パスワードは8文字以上の長さ不定の文字にしていますか。	はい/いいえ	23	65C7(1)後	Y/N	Y: 可		Nの場合、パスワードの長さを確認し、極端に短くなければ可。
1. 3. 1. (14)	類推しやすいパスワード、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職員に認識させていますか。	はい/いいえ	23	65C7(2)後	Y/N	Y: 可		
1. 3. 2. 推奨されるガイドライン			23					
1. 3. 2. (1)	情報の種類、重要性に応じた区分管理を行い、各々の区分毎にアクセス管理を行っていますか。	はい/いいえ	23	65D1	Y/N	Y: 可		
1. 3. 2. (2)	アクセス記録及び定期的なログの確認を行っていますか。ここでいうアクセス記録には、少なくとも利用者のログイン時刻及び時間、ログイン中に操作した患者が特定できる情報が必要です。	※ガイドライン6章5.0.4(アンケート項番1.3.1.(6))に同じ。 1. アクセス・ログをとっている 2. 操作記録を業務日誌に記載している 3. アクセス・ログまたは業務日誌を定期点検している 4. 上記のいずれも行っていない (複数回答可)	23	65D2	1 2 3 4	不可 不可 可 不可		
1. 3. 2. (3)	情報システムにアクセス記録機能(アクセス・ログ)がない場合には、業務日誌などで操作の記録を必ず行っていますか。	1. すべてのパソコンにアンチウイルスソフトを導入している 2. アンチウイルスソフトウェアを導入している 3. その他のウイルス対策を行っている(具体的に: 4. ウイルス対策は行っていない	23	65D3	選	1,2,3: 可4: 不可		
1. 3. 2. (4)	常時、コンピュータウイルス対策を講じていますか。	1. 常時インターネットから最新パターンファイルダウンロードしている 2. 院内にウイルスパターンファイル更新用サーバを用意している 3. ウイルスパターンファイルは不定期に更新している 4. パターンファイルを更新していないパソコンがある (複数回答可)	23	65D3	1 2 3 4	可 可 可 不可		4が選択されれば不可。

アンケート内容	アンケート項目別評価基準	評価方法追記
項目	回答	評価項目別評価
1. 3. 2. (6) 常にOSを最新状態にしていますか。(例:Windowsの場合は、Windows Updateを実施していること)	1 可 2 可 3 可 4 不可	4が選択されれば不可。
1. 3. 2. (6) 離席の際のクローズ処理についてお伺いします。	1 可 2 可 3 可 4 不可	
1. 3. 2. (7) 外部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を設置していますか。	1 可 2 可 3 可 4 不可	
1. 3. 2. (8) 上記ファイアウォールにはACL(アクセス制御リスト)を設定していますか。	1 可 2 可 3 可 4 不可	
1. 3. 2. (9) パスワード入力に誤っていた場合は、再入力できるようになるまで一定の不応答時間(待ち時間)が設定できますか。	1 可 2 可 3 可 4 不可	
1. 3. 2. (10) 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仕組みになっていますか。	1 可 2 可 3 可 4 不可	
1. 3. 2. (11) システムへログインする際に、ID・パスワードまたはICカードや生体認証などによる利用者の識別と認証を行い、IDまたはパスワードと組み合わせさせてログインできるようにしていますか。	1 可 2 可 3 可 4 不可	
1. 4 人的安全対策	1 可 2 可 3 可 4 不可	
1. 4 .1.従業者に対する人的安全管理措置	1 可 2 可 3 可 4 不可	
1. 4 .1.最低限のガイドライン	1 可 2 可 3 可 4 不可	
1. 4. 1. (1) 新たに登用した職員に対して個人情報保護に関する教育を実施していますか。	1 可 2 可 3 可 4 不可	
1. 4. 1. (2) 派遣職員・非常勤職員を採用するにあたり、雇用及び契約時に守秘・非開示契約を締結していますか。	1 可 2 可 3 可 4 不可	
1. 4. 1. (3) 定期的に、職員に対して教育訓練を行っていますか。	1 可 2 可 3 可 4 不可	
1. 4. 1. (4) 職員が退職した場合、就業中に知り得た個人情報保護に関する規則を定めていますか。	1 可 2 可 3 可 4 不可	
1. 4 .2.推奨されるガイドライン	1 可 2 可 3 可 4 不可	
1. 4. 2. (1) 個人情報閲覧できる区画では、モニタカメラなどを設置し、職員の行動を管理していますか。	1 可 2 可 3 可 4 不可	

項目	アンケート内容	回答	アンケート項目別評価基準		
			ガイドライン	回答	評価方法表記
項目	アンケート内容	回答	頁	項目	回答
1. 4. 3.事務取扱委託業者の監督及び守秘義務契約			25		
1. 4. 3.最低限のガイドライン			25		
1. 4. 3.(1) 外部委託業者および保守業者を採用する場合、委託先の罰則を定めた包括的な守秘義務契約を締結していますか。		はい/いいえ	25	66(2)G1①	Y/N Y:可
1. 4. 3.(2) 委託先業者が保守作業との医療情報システムに直接アクセスする作業において、医療機関等の担当者は委託先作業担当者および作業内容、作業結果を確認していますか。		1. 医療機関等の関係者の立会いの下で行っている 2. 委託先作業担当者および作業内容、作業結果を確認している 3. 保守操作の内容を逐一ログとして記録している 4. 上記のいずれも行っていない (複数回答可)	25	66(2)G1②	1 可 2 可 3 可 4 不可
1. 4. 3.(3) 清掃業者など、直接システムにアクセスしない作業において、業者が個人情報情報の管理されている区画に入った場合には、作業後に個人情報情報が保全されているかどうか確認を行っていますか。		はい/いいえ	25	66(2)G1③	Y/N Y:可
1. 4. 3.(4) 委託先業者が再委託を行う場合には、再委託先業者に対して包括的な守秘義務契約を締結していますか。		はい/いいえ	25	66(2)G1④	Y/N Y:可
1. 4. 3.(5) 外部委託業者および保守業者を採用する場合、委託先の罰則を定めた包括的な守秘義務契約を締結していますか。		※ガイドライン6第66(2)G1①(アンケート項目1.4.3.(1))に同じ。 はい/いいえ	25	66(2)C2	Y/N Y:可
1. 5 情報の破壊			26		
1. 5.1.最低限のガイドライン			26		
1. 5. 1.(1) 情報の種別毎に破壊する手順を定めていますか。その手順には、破壊を行う条件、破壊を行うことができる職員、具体的な破壊方法を明記していますか。		1. 破壊条件を明記している 2. 破壊担当者を明記している 3. 破壊手順を明記している 4. 上記のいずれも行っていない (複数回答可)	26	67C1	1 1,2,3共に○で可 2 1,2,3共に○で可 3 1,2,3共に○で可 4 不可
1. 5. 1.(2) パソコン、ハードディスク装置などを破壊する場合、個人情報が残っていないことを確認していますか。		1. 専門業者に委託しデータ消滅証明書をとっている 2. 専門知識のある職員が行いデータ消滅の証拠を残している 3. 上記のいずれも行っていない (複数回答可)	26	67C2	1 可 2 可 3 不可
1. 5. 1.(3) 破壊を外部業者に委託した場合、その業者と守秘義務契約を結んでいますか。		はい/いいえ	26	67C3	Y/N Y:可
1. 5. 1.(4) 破壊を外部業者に委託した場合、確実に情報の破壊が行われたことを確認していますか。		1. 医療機関等の関係者の立会いの下で行っている 2. 委託先作業担当者および作業内容、作業結果を確認している 3. 上記のいずれも行っていない (複数回答可)	26	67C3	1 可 2 可 3 不可
1. 5. 1.(5) 個人情報が入った記録メディアを廃棄する規定は定められていますか。		1. 専門業者に委託しデータ消滅証明書をとっている 2. 専門知識のある職員が行いデータ消滅の証拠を残している 3. 院内でシュレッダーにかけて物理的に遮断してから破壊している 4. 上記のいずれも行っていない (複数回答可)	26	67C4(a)	1 可 2 可 3 可 4 4の場合、1～3以外の何らかの規定の有無を確認し、規定があれば可。

項目	アンケート内容	回答	アンケート項目別評価基準	
			項目別評価	評価方法表記
1. 6 情報システムの改造と保守				
1. 6. 1. 最低限のガイドライン				
1. 6. 1. (1) 個人情報を含むデータを用いた情報システムの動作確認を行う際、動作確認を行う端末を制限するなど、データの漏洩対策を行っていますか。				
		※ガイドライン6章5.0.2(アンケート項目3.1.1(2))に同じ。 1. 動作確認を行うパソコンを制限している 2. 動作確認作業者と守秘義務契約を締結している 3. 動作確認を行う作業室に対する入室管理を行っている 4. その他の情報漏洩対策を講じている(具体的に:) 5. 上記の情報漏洩対策は講じていない (複数回答可)	68C1 1 不可 2 可 3 不可 4 具体的な内容によって判定 5 不可	
1. 6. 1. (2) システムの動作確認において個人情報を含むデータを使用した場合、使用後に当該データを消滅するための手順を定めていますか。		1. 専門業者に委託しデータ消滅証明書をとっている 2. システム導入業者に委託しデータ消滅証明書をとっている 3. 専門知識のある職員が行いデータ消滅の証拠を残している 4. 上記のいずれも行っていない (複数回答可)	68C1 1 可 2 可 3 可 4 不可	
1. 6. 1. (3) 動作確認や保守のために保守業者の作業員がシステムにアクセスするための専用のアカウントを用意していますか。		はい/いいえ	68C2 Y/N Y:可	
1. 6. 1. (4) マ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していますか。		はい/いいえ	68C2 Y/N Y:可	
1. 6. 1. (5) 保守業者用のアカウント情報が外部に流出したり不正に利用されないために適切な管理を行っていますか。		1. 保守業者が作業する期間だけ利用できるアカウントを用意している 2. 保守業者がアクセスするたびにパスワードを変えている 3. その他の管理方法(具体的に:) 4. 管理は行っていない (複数回答可)	68C3 1 可 2 可 3 具体的な内容によって判定 4 不可	
1. 6. 1. (6) 保守要員の配置転換や離職した場合には保守業者からの報告を義務づけ、速やかに当該アカウントを削除していますか。		はい/いいえ	68C4 Y/N Y:可	
1. 6. 1. (7) 保守時には、保守業者から日単位で作業報告書を送やかに提出することを義務づけていますか。また、医療機関等側の責任者は、この報告書を逐一承認していますか。		1. 作業報告書の提出を義務づけている 2. 医療機関等の担当者が作業報告の承認を行っている 3. 上記いずれも行っていない (複数回答可)	68C5 1 1,2共にOで可 2 1,2共にOで可 3 不可	
1. 6. 1. (8) 外部委託業者および保守業者を採用する場合、委託先の罰則を定めた包括的な守秘義務契約を締結していますか。		※ガイドライン6章6.0.2(2)G.1.①(アンケート項目4.3.1(1))に同じ。 はい/いいえ	68C6 Y/N Y:可	
1. 6. 1. (9) 保守業者が個人情報を含むデータを医療機関外に持ち出すことは避けるべきだが、やむを得ない状況で持ち出す場合には、運用管理規定を定めていますか。また、持ち出し後の作業について、医療機関等側の責任者が逐一確認・承認を行っていますか。		1. 個人情報等を外部に持ち出さない 2. 外部での作業報告書の提出を義務づけている 3. 医療機関等の責任者が作業報告の承認を行っている 4. 上記いずれも行っていない (複数回答可)	68C7 1 可 2 2,3共にOで可 3 2,3共にOで可 4 不可	
1. 6. 1. (10) 電話回線などによる遠隔保守によるシステムの改造、保守が行われる場合には、逐一メッセージログを残していますか。また、当該作業の終了後、速やかに医療機関等側責任者がメッセージログの内容を承認していますか。		1. 遠隔保守を行っていない 2. メッセージログを残している 3. 医療機関等の責任者がメッセージログの内容の承認を行っている 4. 上記いずれも行っていない (複数回答可)	68C8 1 NAとする 2 不可 3 可 4 不可	遠隔保守を行っていない場合は、評価外(NA)とする。
1. 6. 1. (11) 保守作業の再委託が行われる場合、再委託先業者に対しても委託契約において安全管理に関する条項を定めていますか。		はい/いいえ	68C9 Y/N Y:可	

項目	アンケート内容	回答	アンケート項目別評価基準		
			ガイドライン	回答	評価方法
項目	アンケート内容	回答	項目	回答	評価方法
1. 6. 2. 推奨されるガイドライン			28		
1. 6. 2. (1) 委託先業者がシステムにアクセスする作業において、詳細なオペレーション記録を保守操作ログとして記録していますか。		はい/いいえ	68D1	Y/N	Y:可
1. 6. 2. (2) 保守作業時には、医療機関等の担当者立会いのもとで行っていますか。		はい/いいえ	68D2	Y/N	Y:可
1. 6. 2. (3) 外部委託業者および保守業者を採用する場合、罰則を含めた包括的な守秘義務契約を締結していますか。		はい/いいえ	68D3	Y/N	Y:可
1. 6. 2. (4) 保守業者が個人情報を含むデータを医療機関外に持ち出すことは避けるべきだが、やむを得ない状況で持ち出す場合には、詳細な作業記録を残すことを義務づけていますか。また、必要に応じて医療機関の監査に応じるよう求めていますか。		1. 個人情報等を外部に持ち出さない 2. 外部での作業報告書の提出を義務づけている 3. 医療機関による監査に応じるようにしている 4. 上記いずれも行っていない (複数回答可)	68D4	1 NAとする 2 2,3共に○で可 3 2,3共に○で可 4 不可	1の場合、評価外(NA)とする。
1. 6. 2. (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ますか。		はい/いいえ	68D5	Y/N	Y:可
2. 電子保存の要求事項について					
2. 1 真正性の確保について			40		
2. 1 最低限のガイドライン			40		
2. 1. 1. 作成者の識別及び認証			40		
2. 1. 1. (1) システムへログインする際に、ID・パスワードまたはICカードや生体認証などによる利用者の識別と認証を行い、IDまたはパスワードと組み合わせでログインできるようにしていますか。		※ガイドライン6章5.0.1(アンケート項目3.3.1.(1))に同じ。 1. ID、パスワードによる認証を行っている 2. ICカードによる認証を行っている 3. 生体認証を行っている 4. 上記1～3の方法を組み合わせてログインできるようにしている 5. 上記以外の認証を行っている(具体的に:) 6. 認証は行っていない (複数回答可)	71C(1)a1	1 可 2 可 3 可 4 可 5 具体的内容によって判定 6 不可	
2. 1. 1. (2) システムへログインする際に、ID・パスワードまたはICカードや生体認証などによる利用者の識別と認証を行い、IDまたはパスワードと組み合わせでログインできるようにしていますか。		※ガイドライン6章5.0.1(アンケート項目3.3.1.(1))に同じ。 1. ID、パスワードによる認証を行っている 2. ICカードによる認証を行っている 3. 生体認証を行っている 4. 上記1～3の方法を組み合わせてログインできるようにしている 5. 上記以外の認証を行っている(具体的に:) 6. 認証は行っていない (複数回答可)	71C(1)a2	1 評価対象外 2 評価対象外 3 評価対象外 4 可 5 具体的内容によって判定 6 不可	ICカード使用時のみ評価。 未使用時は評価外(NA)とする。
2. 1. 1. (3) システムへログインする際に、ID・パスワードまたはICカードや生体認証などによる利用者の識別と認証を行い、IDまたはパスワードと組み合わせでログインできるようにしていますか。		※ガイドライン6章5.0.1(アンケート項目3.3.1.(1))に同じ。 1. ID、パスワードによる認証を行っている 2. ICカードによる認証を行っている 3. 生体認証を行っている 4. 上記1～3の方法を組み合わせてログインできるようにしている 5. 上記以外の認証を行っている(具体的に:) 6. 認証は行っていない (複数回答可)	71C(1)a3	1 評価対象外 2 評価対象外 3 評価対象外 4 可 5 具体的内容によって判定 6 不可	生体認証使用時のみ評価。 未使用時は評価外(NA)とする。
2. 1. 1. (4) 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っていますか。		※ガイドライン6章5.0.3(アンケート項目3.3.1.(3))に同じ。 はい/いいえ	71C(1)a4	Y/N	Y:可
2. 1. 1. (5) 権限のある利用者以外による情報の作成、追記、変更を防止していますか。		はい/いいえ	71C(1)a4	Y/N	Y:可

項目	アンケート内容	回答	ガイドライン		回答	アンケート項目別評価基準	
			頁	項番		回答項目別評価面	評価方法適配
2. 1. 1.(6)	業務アプリケーション稼働パソコンを管理し、権限を持たない者が利用できないようにしていますか。	はい/いいえ	40	71C(1)a5	Y/N	Y:可	
2. 1. 1.(7)	システムに医療機関等外からリモート接続する場合は、暗号化、ネットワーク接続端末のアクセス制限等のセキュリティ対策を実施していますか。	1. 暗号化通信経路(VPN)によってリモートアクセスできる 2. 特定の端末のみ接続を許可している 3. ユーザーによるアクセス制限をしている 4. リモートアクセスは可能だが制限は設けていない 5. リモートアクセスはできない (複数回答可)	41	71C(1)a6	1 2 3 4 5	可 可 可 不可 NAとする	リモートアクセスができない場合は評価外(NA)とする。
2. 1. 1.(8)	部門システムに管理責任者や操作者が運営管理規程で明文化され、管理責任者、操作者以外の機器の操作が運営上防止されていますか。	はい/いいえ	41	71C(1)b	Y/N	Y:可	
2. 1. 2 記録の確定手順の確立と、作成責任者の識別情報の記録			41				
2. 1. 2.(1)	診療録等の作成・保存を行うおうとする場合、システムは確定された情報を登録できる仕組みを備えていますか。	はい/いいえ	41	71C(2)a1	Y/N	Y:可	
2. 1. 2.(2)	確定された情報を登録する際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日付を含んでいますか。	1. 作成責任者の氏名を登録している 2. 信頼できる時刻源を用いた作成日付を登録している 3. その他(具体的に: 4. これらの情報は登録していない (複数回答可)	41	71C(2)a1	1 2 3 4	12共に○で可 12共に○で可 具体的内容によって判定 不可	
2. 1. 2.(3)	記録を確定するために、作成責任者による内容の十分な確認が実施できるような仕組みになっていますか。	1. 確定前に内容確認画面が表示される 2. その他の方法で確認できる(具体的に: 3. 登録前確認は行っていない (複数回答可)	41	71C(2)a2	1 2 3	可 具体的内容によって判定 不可	
2. 1. 2.(4)	確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることを運用も含めて防止できるような措置をとっていますか。	はい/いいえ	41	71C(2)a3	Y/N	Y:可	
2. 1. 2.(5)	方が一、確定された記録が変更されてしまった場合、記録の改ざん・削除が起きた場合は、変更・改ざん・削除を検知し、原状回復するような仕組みを備えていますか。	1. 変更を検知できる 2. 記録の改ざん・削除を検知できる 3. バックアップファイルから現状回復できる 4. その他の方法で現状回復できる(具体的に: 5. 上記いずれも行っていない (複数回答可)	41	71C(2)a3	1 2 3 4 5	可 可 可 具体的内容によって判定 不可	回復できることで可
2. 1. 2.(6)	外部から入力された情報を参照・再利用する際、外部情報は確定情報のみですか。	はい/いいえ	41	71C(2)a4	Y/N	Y:可	
2. 1. 2.(7)	外部から入力された情報の参照元が「保存された記録」でない場合は、コピー等の移動手段を経て取り込み操作を行った後に、その情報も含めた「記録の確定」を行っていますか。	はい/いいえ			Y/N	Y:可	
2. 1. 2.(8)	部門システムにおける記録の確定の際、作成責任者の氏名またはID番号、信頼できる時刻による作成日時が記録されていますか。	1. 作成責任者の氏名が登録される 2. 作成責任者のIDが登録される 3. 時刻が登録される 4. 上記のいずれも登録されない (複数回答可)	41	71C(2)b	1 2 3 4	可 可 可 不可	(1または2)と3の組合せで可
2. 1. 2.(9)	部門システムにより作成された記録の確定ルール(作成責任者の確認手続きなどが運用管理規定に定められていますか。	はい/いいえ	41	71C(2)b	Y/N	Y:可	
2. 1. 2.(10)	確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることを運用も含めて防止できるような措置をとっていますか。	※ガイドライン第10.(2).a.3(アンケート項目2.1.2.(4))に同じ はい/いいえ	41	71C(2)b	Y/N	Y:可	