JAHIS

JAHIS標準 24-006

Japanese

Association of

Healthcare

Information

Systems Industry

JAHIS
保存が義務付けられた診療録等の電子保存ガイドライン
Ver.5

厚生労働省「医療情報システムの安全管理に関するガイドライン 第 6.0 版」対応

2024 年 9 月

一般社団法人 保健医療福祉情報システム工業会

医療システム部会 セキュリティ委員会

電子保存WG

JAHIS

保存が義務付けられた診療録等の電子保存ガイドライン Ver.5

厚生労働省「医療情報システムの安全管理に関するガイドライン第 6.0 版」対応

ま え が き

2005 年 3 月に厚生労働省より「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「安全管理ガイドライン」とする）として個人情報保護、電子保存、外部保存、e-文書法対応を統合したガイドラインが発行された。この「安全管理ガイドライン」では最新の技術動向を考慮した詳しい説明が行われているが、個別のシステムベンダが具体的に自社のシステムを実装する段においては、実際にどのようなシステム製品がその要件を満たすのか、どのような仕様で開発したらよいのかが分かりにくい部分があった。JAHIS としては電子保存の促進のため、「より具体的で実装寄り」のガイドラインが必要と考え、2007 年 5 月に本ガイドライン（初版）をまとめた。

また、総務省と経済産業省からは医療情報システムをサービス提供する場合に考慮すべきガイドラインが発行されており、システム実装するシステムベンダに関連する部分については本ガイドラインに取り込んでいる。

今般、「安全管理ガイドライン」が 2023 年 5 月に第 6.0 版として発行され、また、総務省と経済産業省のガイドラインが統合された「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（以下「サービス提供事業者ガイドライン」とする）が 2023 年 7 月に第 1.1 版が発行されたため、各々の改版内容を反映し、本ガイドラインを Ver.5 として発行することとなった。

本ガイドラインは、JAHIS 会員各社の意見を集約し、「JAHIS 標準」の一つとして発行したものである。従って、会員各社がシステムの開発・更新に当たって、本ガイドラインに基づいた開発・改良を行い、本ガイドラインに準拠していることをその製品のカタログ・仕様書等に示し、さらにその製品のユーザに運用で担保すべきことを説明する場合などに使われることを期待している。

また、本ガイドラインを診療録及び診療諸記録の電子保存機能を持つシステムを導入しようとしている施設が参照し利用することは歓迎するところであるが、当該システムが厚生労働省通知等に合致しているか否かの判断は、自己責任の下で自ら判断する必要があること、及び、上記の 3 省のガイドラインは今後も改定が行われることが予想されるため、本ガイドラインにおいても必要に応じて改版を行う予定であるので、常に最新版を参照することにご留意いただきたい。

なお、本ガイドラインで扱うセキュリティ要件は、社会状況にあわせて常に変化するものであり、利用いただく時点で必ずしも適当ではない内容である可能性もある。我々としても継続的に検討を重ねてゆく所存であるが、本ガイドラインの利用者はその点もご留意頂くとともに、お気づきの点をフィードバックして頂けるとありがたい。

本ガイドラインが「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」を扱うシステムの、また関連する医療情報システムの開発に多少とも貢献できれば幸いである。

2024 年 9 月

一般社団法人 保健医療福祉情報システム工業会
医療システム部会 セキュリティ委員会
電子保存 WG

＜＜　告知事項　＞＞

本ガイドラインは関連団体の所属の有無に関わらず、ガイドラインの引用を明示することで自由に使用することができるものとします。ただし一部の改変を伴う場合は個々の責任において行い、本ガイドラインに準拠する旨を表現することは厳禁するものとします。

本ガイドライン及び本ガイドラインに基づいたシステムの導入・運用についてのあらゆる障害や損害について、本ガイドライン作成者は何らの責任を負わないものとします。ただし、関連団体所属の正規の資格者は本ガイドラインについての疑義を作成者に申し入れることができ、作成者はこれに誠意をもって協議するものとします。

目　次

1. はじめに

「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」（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。）により、それまで紙でしか保存が許されなかった「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」の大半を電子的に保存できることとなった。その後「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）により外部保存が可能になった。そして「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2005年3月31日通知「『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」を受けて、2005年3月に厚生労働省より「安全管理ガイドライン」として個人情報保護、電子保存、外部保存、e-文書法対応を統合したガイドラインが発行された。

（1）初版

2005年3月に発行された「安全管理ガイドライン」の初版では、B項の「考え方」において最新の技術動向を配慮した詳しい説明が行われているが、個別のシステムベンダが具体的に自社のシステムに実装するにおいては、実際にどのようなシステム製品がその要件を満たすのか、どのような仕様で開発したらよいのかが分かりにくかった。JAHISとしては電子保存を促進するためには、各要件を実際のシステムの機能を反映した「機能要件」や、その機能を補完する内容を含む「運用要件」を整理した、より具体的で実装寄りのガイドラインが必要と考え、同ガイドラインに対して、「技術的にどの範囲まで担保することが望ましいか、また技術的に対応しにくい要件を運用でどのように担保することが期待されるか」を具体的に示すことにより、診療録等の電子保存およびネットワークを介した送受信を適切に行うための基準を示すことを目的として、2007年5月に本ガイドライン（初版）をまとめた。

（2）第2版

「安全管理ガイドライン」は技術の進歩や周辺環境の変化を受けて改定が実施され、2007年3月には第2版、2008年3月には第3版が発行された。JAHISの本ガイドラインについても、継続検討を行うこととしていたため、「安全管理ガイドライン」の改定を受けて検討を実施、同ガイドライン第3版までの内容を反映し、2009年10月に第2版として発行した。

（3）第3版

「安全管理ガイドライン」は2009年3月に第4版、2010年2月に第4.1版が発行された。また、総務省の「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（2009年7月）及び、経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」（2008年7月）も発行された。JAHISの本ガイドラインについても、継続検討を行うこととしていたため、上記の3つのガイドライン（更新版を含めると4つ。以下「3省ガイドライン」とする）の内容を反映し、2011年4月に第3版として発行した。

（4）第3.1版

総務省の「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」は2010年12月に第1.1版、及び、経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」は2012年10月に第2版が発行された。JAHISの本ガイドラインについても、継続検討を行うこととしていたため、上記に発行された2つのガイドラインの内容を反映し、第3.1版として発行することとなった。

（5）第3.2版

「安全管理ガイドライン」は2013年10月に第4.2版が発行された。JAHISの本ガイドラインについても関係する内容が有るので内容を反映することとしたが、作業範囲の検討の中で、本ガイドラインをより理解しやすい書

き方に整理するという提案にも対応することとし、合わせて第 3.2 版として発行することとした。

(6) Ver.3.3

「安全管理ガイドライン」は 2016 年 3 月に第 4.3 版、2017 年 5 月に第 5 版が発行された。第 4.3 版は本ガイドラインに関係する変更が無かったので本ガイドラインの改訂はしていない。第 5 版では本ガイドラインに関係する内容が有るので内容を反映し、Ver.3.3 として発行することとなった。本改訂から変更管理の表記を「版」から英字の略表記号「Ver.」を使用することにした。

(7) Ver.4

総務省の「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン(第 1.1 版)」は「ASP・SaaS における情報セキュリティ対策ガイドライン」と統合され「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」として 2018 年 7 月に第 1 版が発行された。その後、経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン(第 2 版)」と統合され「サービス提供事業者ガイドライン」として 2020 年 8 月に第 1 版が発行された。また、「安全管理ガイドライン」は 2021 年 1 月に第 5.1 版が発行され、さらに 2022 年 3 月に第 5.2 版が発行された。関係するガイドラインの改版内容を反映し、Ver.4 として発行することとなった。

(8) Ver.5

「安全管理ガイドライン」は 2023 年 5 月に第 6.0 版が発行され、医療情報システムの安全管理に共通する内容を整理した概説編(Overview)と、医療情報システムの安全管理を実施するための統制・管理について想定する読者類型ごとに整理した、経営管理編(Governance)、企画管理編(Management)及び、システム運用編(Control)の 4 編の構成となった。さらに 2023 年 7 月に「サービス提供事業者ガイドライン」第 1.1 版が発行された。関係するガイドラインの改版内容を反映し、Ver.5 として発行することとなった。

本ガイドラインは、JAHIS 会員各社の意見を集約し、「JAHIS 標準」の一つとして発行したものである。従って、会員各社がシステムの開発・更新に当たって、本ガイドラインに基づいた開発・改良を行い、本ガイドラインに準拠していることをその製品のカタログ・仕様書等に示し、さらにその製品のユーザに運用で担保すべきことを説明する場合などに使われることを期待している。

また、本ガイドラインを、診療録及び診療諸記録の電子保存機能を持つシステムを導入しようとしている施設が参照し利用することは歓迎するところであるが、当該システムが厚生労働省通知、総務省通知及び経済産業省通知に合致しているか否かの判断は、自己責任の下で自ら判断する必要があること、及び、上記の 3 省ガイドラインは今後も改定が行われることが予想されるため、本ガイドラインにおいても必要に応じて改版を行う予定であるので、常に最新版を参照することにご留意いただきたい。

なお、本ガイドラインで扱うセキュリティ要件は、社会状況にあわせて常に変化するものであり、利用いただく時点で必ずしも適当ではない内容である可能性もある。我々としても継続的に検討を重ねてゆく所存であるが、本ガイドラインの利用者はその点もご留意頂くとともに、お気づきの点をフィードバックして頂けるとありがたい。

本ガイドラインが「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」を扱うシステムの、また関連する医療情報システムの開発に多少とも貢献できれば幸いである。

2. 概要

本ガイドラインは、3 省ガイドラインのうち電子保存と外部保存の指針について、システムベンダの視点から解説を行った方が良いと思われる箇所について解説を行ったものである。そのため、本ガイドラインの読者は「安全管理ガイドライン」と「「医療情報システムの安全管理に関するガイドライン 第 6.0 版」に関するQ&A」(以下「安全管理ガイドラインQ&A」とする)を一読することを推奨する。第 6.0 版のQ&Aは第 5.2 版の本文から移設された内容もあり、「安全管理ガイドライン」の理解に役立つものとなっている。

なお、3 省ガイドラインのうちシステムベンダが対応すべき要件は「安全管理ガイドライン」の「システム運用編」に集中しているため、この編を軸に章立てを構成している。その他の編(概説編、経営管理編、企画管理編)や総務省、経済産業省のガイドラインについては、システムベンダが対応すべき要件に関連する箇所について、構成に取り入れ解説を行っている。

記載のルールを以下に説明する。

(1) 章立ておよび章のタイトル

ア) 章立ておよび章のタイトルは基本的に「安全管理ガイドライン」の「システム運用編」に合わせる。ただし、章番号はシフトすることがある。

(2) 章単位の対応表

ア) 章単位の「安全管理ガイドライン」との対応表を本ガイドラインの「4. 適用範囲」に記載する。

イ) また、「サービス提供事業者ガイドライン」との対応表を本ガイドラインの「6. 総務省、経済産業省の「サービス提供事業者ガイドライン」に関する事項」に記載する。

ウ) 本ガイドラインで対象外と判断した章は、対応表で“【システムベンダ側での対処事項なし】”と記載する

(3) 章の中の構成と記載内容

ア) 節、項目のタイトルも原則として「安全管理ガイドライン」の「システム運用編」に合わせる。

イ) 章の中で、下記の状況が有る場合は、章名(＊. 章名)、節名(＊. ＊. 節名)の直下に補足文章を記載する。

① 「安全管理ガイドライン」の構成との対応に追加がある場合

② 各章と各節の記載に対して解説・補足が必要と考えられる場合

③ 各章と各節の記載と【遵守事項】の結びつきがわかりにくい場合

ウ) 章の中は、「安全管理ガイドライン」の示す要件毎に【遵守事項】の要求項目を表形式で再掲する。

① 表形式のテンプレート

＜安全管理ガイドライン(システム運用編)の要求事項＞

遵守事項
① ○○･･･すること ② ◇◇･･･すること

② 「安全管理ガイドライン」の各節に合わせて、【遵守事項】も該当するものに分けて記載する。

③ 各節をさらに分類した方がわかりやすい場合は【遵守事項】を分類して記載する。

④ 本ガイドラインで対象外と判断した要求項目は、再掲した箇所に“【システムベンダ側での対処事項なし】”と記載する

エ）要件毎に「技術的対策」、「運用的対策」、「コラム」を記述する。

① 技術的対策

「安全管理ガイドライン」の記述に対して、以下のような補足説明する必要がある場合に記述する。無い場合は「追記事項なし」と記載する。

・技術仕様の具体化、解説、例示。

・あいまいな記述に対する JAHIS の理解した方針。

② 運用的対策

技術的対策がある場合も無い場合も、本ガイドラインで対象とする要件を実現するために運用的対策が必要であれば記載する。

③ コラム

システムベンダとして参考にすべき事項がある場合はコラムとして記載する。

3. 主な用語

アカウント　：　特定のコンピュータシステム、またはネットワークにアクセスするために「認証」される人を表現しており、権限属性をもつことがある。

アクセス制御　：　コンピュータセキュリティにおいて、ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすること。

アクセスログ　：　情報の作成、変更、参照、削除などの記録。

改ざん　：　情報を管理者の許可を得ずに書き換える行為。

外部保存　：　法令に基づく保存義務のある診療録、または診療に関する諸記録を、それらが作成された病院または診療所以外の施設に保存すること。

監査証跡　：　監査対象システムの入力から出力に至る過程を追跡できる一連の仕組みと記録のこと。

見読性　：　電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること。

個人情報（患者の個人情報）

：　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（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

残存リスク（または残留リスク）

：　リスクマネジメントの結果、未対応部分として残るリスクのこと。

システムベンダ　：　医療情報システムを提供するベンダ。

真正性　：　正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていること。

ぜい弱性　：　コンピュータやネットワークといった情報システムに対し、アクセス許可のない第三者からの侵入など脅威となる行為に利用できる可能性のあるシステム上の弱点。または仕様上の問題点。

相互運用性　：　異なったアプリケーションやシステム、構成コンポーネント間で情報の伝達または共有がなされ相互に接続、利用できる共通性を持つこと。

タイムスタンプ　：　電子データがタイムスタンプを付与した時刻から存在し、それ以降、改ざんされていないことを証明することができる電子情報。タイムスタンプトークンとも呼ばれ、正確、かつ適切に管理された時刻情報を有し、ハッシュや公開鍵暗号技術を用いて対象データの非改ざん性を担保することができる。特に、タイムスタンプに高い信頼性が求められる場合、一般財団法人日本データ通信協会の「タイムビジネス信頼・安心認定制度」の認定を受けたタイムスタンプが要求される。

デバイス　：　コンピュータに搭載あるいは接続されるハードウェア。

電子署名　：　電子データの正当性を保証するために付される電子的な署名情報。公開鍵暗号などを利用し、署名者本人が付与したものであることを確認することができ、また、署名対象情報が改ざんされていないことを証明することができる情報。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう場合もあるが、本ガイドラインでは、“電子署名

“で統一した。

保存性	：	記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されること。
リスクアセスメント	：	本書においては、情報資産に対して、その情報がもつ重要度、発生確率、影響度などを評価・分析し、情報資産が内包するリスクを測定すること。
リスクマネジメント	：	リスクアセスメントとそれによって特定されたリスクに対して、そのリスクを低減させるプロセスの組織活動。
PDCA サイクル	：	Plan（計画）、Do（実施）、Check（検証）、Act（改善）のマネジメントサイクル。

（記号および略語　このガイドラインでは、次の記号および略語・表記を用いる。）

ISMS	Information Security Management System 情報セキュリティマネジメントシステム
JIPDEC	Japan Information Processing Development Corporation 一般財団法人日本情報経済社会推進協会
PKI	Public Key Infrastructure 公開鍵基盤
VPN	Virtual Private Network 仮想的な専用通信回線

4. 適用範囲

4.1. 「安全管理ガイドライン」との関係

本ガイドラインは、「安全管理ガイドライン」で示されている三つのガイドライン等（個人情報保護、電子保存、外部保存）のうち、電子保存と外部保存のガイドラインについて、システムベンダの視点からより詳細な解説を行った方が良いと思われる箇所について、技術的な対策と運用的な対策に分けて基準を示し、解説を行ったものである。

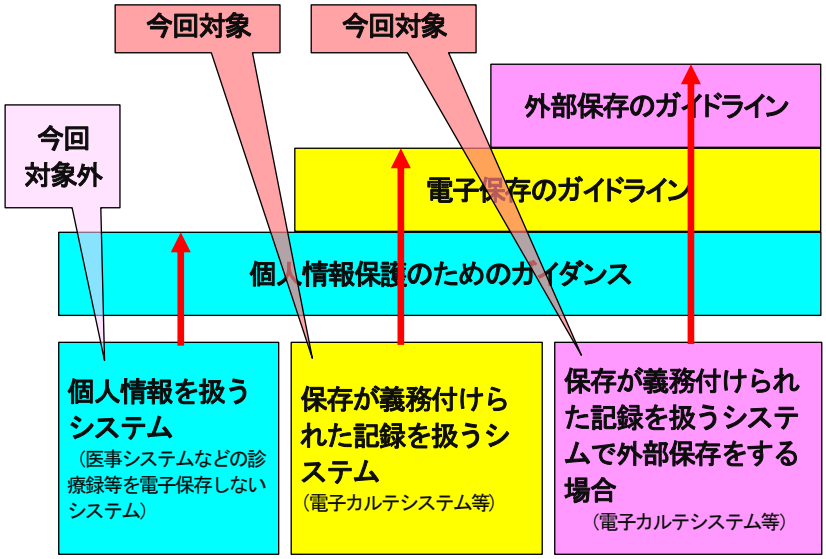


図 1.本ガイドラインと「安全管理ガイドライン」で示されている 3 つのガイドラインとの関係

「安全管理ガイドライン」と本ガイドラインとの対応する章は以下の通りである。

安全管理ガイドライン（システム運用編）	本ガイドライン
	1. はじめに
	2. 概要
	3. 主な用語
	4. 適用範囲
	5. 医療情報システムの実装・運用における安全管理
1. 情報セキュリティの基本的な考え方	5.1. 情報セキュリティの基本的な考え方
2. システム設計・運用に必要な規程類と文書体系	5.2. システム設計・運用に必要な規程類と文書体系
3. 責任分界	5.3. 責任分界
4. リスクアセスメントを踏まえた安全管理対策の設計	5.4. リスクアセスメントを踏まえた安全管理対策の設計
5. システム設計の見直し（標準化対応、新規技術導入のための評価等）	5.5. システム設計の見直し（標準化対応、新規技術導入のための評価等）

安全管理ガイドライン(システム運用編)	本ガイドライン
6. 安全管理を実現するための技術的対策の体系	5.6. 安全管理を実現するための技術的対策の体系
7. 情報管理(管理・持出し・破棄等)	5.7. 情報管理(管理・持出し・破棄等)
8. 利用機器・サービスに対する安全管理措置	5.8. 利用機器・サービスに対する安全管理措置
9. ソフトウェア・サービスに対する要求事項	5.9. ソフトウェア・サービスに対する要求事項
10. 医療情報ステム・サービス事業者による保守対応等に対する安全管理措置	5.10. 医療情報ステム・サービス事業者による保守対応等に対する安全管理措置
11. システム運用管理(通常時・非常時等)	5.11. システム運用管理(通常時・非常時等)
12. 物理的安全管理措置	5.12. 物理的安全管理措置
13. ネットワークに関する安全管理措置	5.13. ネットワークに関する安全管理措置
14. 認証・認可に関する安全管理措置	5.14. 認証・認可に関する安全管理措置
15. 電子署名、タイムスタンプ	5.15. 電子署名、タイムスタンプ
16. 紙媒体等で作成した医療情報の電子化	5.16. 紙媒体等で作成した医療情報の電子化
17. 証跡のレビュー・システム監査	5.17. 証跡のレビュー・システム監査
18. 外部からの攻撃に対する安全管理措置	5.18. 外部からの攻撃に対する安全管理措置

4.2.　本ガイドラインの対象システム及び対象情報

本ガイドラインの対象システムは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等（以下「医療機関等」とする）に対し保存が義務付けられている診療録等の電子保存を行うシステムである。「安全管理ガイドライン」は医療に関わる情報を扱う全ての情報システムを対象としているが、本ガイドラインでは電子保存を行うシステムに限定している。ただし、電子保存を行わないシステムにも非常に有用な内容になっており、ぜひ参考にしていただきたい。以下に対象となる可能性があるシステムの例を示す。

- 電子カルテシステム
- オーダエントリシステム
- 診療部門システム（看護支援システム、手術システムなど）
- 臨床・病理検査システム
- 医用画像システム
- 放射線システム
- 調剤録を電子保存するシステム
- 介護システム

また、対象情報については「安全管理ガイドライン」「概説編」の「2.2　医療情報・文書の範囲」並びに「安全管理ガイドライン「Q&A」の／「概Q－4　電子保存が認められている文書とは具体的に何か。」を参照願いたい。

4.3.　総務省及び経済産業省のガイドラインとの関係

本ガイドラインは、サービスを提供する事業者向けに発行された総務省及び経済産業省のガイドライン「サービス提供事業者ガイドライン」で要求されている項目の内、情報処理システムに関する要求と思われる部分について、システムベンダの視点から技術的な解説を行うものとする。

「サービス提供事業者ガイドライン」と本ガイドラインとの対応する章は以下の通りである。

サービス提供事業者ガイドライン	本ガイドライン
5. 安全管理のためのリスクマネジメントプロセス	6.2. 安全管理のためのリスクマネジメントプロセス
6. 制度上の要求事項	6.3. 制度上の要求事項

4.4.　他の JAHIS 標準・技術文書との関係

本ガイドラインの前提は「安全管理ガイドライン」であるが、他の JAHIS 標準や技術文書に規定されている規格やガイドラインがある場合には、相互運用性や見読性の確保などの観点から、技術的管理策などを選択する際に積極的に採用することを推奨している。また、現時点で JAHIS 標準や技術文書において規定されていない領域において、将来 JAHIS 標準や技術文書により規格やガイドラインが規定された場合にはそれらを優先的に採用することを妨げるものではない。

4.5.　引用規格・引用文献

・厚生労働省

医療情報システムの安全管理に関するガイドライン

第 6.0 版　令和５年５月

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

・総務省、経済産業省

医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

第 1.1 版　令和５年７月

https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000359.html

https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigyousyagl.html

・厚生労働省：保健医療福祉分野 PKI 認証局　署名用証明書ポリシ　1.91 版(令和５年 12 月)

https://www.mhlw.go.jp/content/10808000/001222110.pdf

・厚生労働省：保健医療福祉分野 PKI 認証局　認証用(人)証明書ポリシ　1.81 版(令和５年 12 月)

https://www.mhlw.go.jp/content/10808000/001222111.pdf

・厚生労働省：保健医療福祉分野 PKI 認証局　認証用(組織)証明書ポリシ　1.1 版(平成 22 年３月)

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/pki-policy/2203_03.html

5. 医療情報システムの実装・運用における安全管理

5.1. 情報セキュリティの基本的な考え方

5.1.1. 安全管理に関する法制度等による要求事項

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

5.2. システム設計・運用に必要な規程類と文書体系

5.2.1. システム運用担当者において作成すべき文書類

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。
② 医療情報システムに関する全体構成図(ネットワーク構成図・システム構成図等)、及びシステム責任者・関係者一覧(設置事業者、保守事業者等含む)を作成し、常に最新の状態を維持すること。
③ 医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。
④ 医療情報システムの利用者が適切に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。
⑤ 非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

5.3. 責任分界

5.3.1. 医療機関等の責任とシステムベンダの提供する医療情報システムの関係

「安全管理ガイドライン」の「経営管理編」において、医療機関等は医療情報を取り扱う医療情報システムを適正に管理する責任があると明記されている。

医療機関等は自らの責任で、表1にある責任を果たさねばならないが、自らの責任を果たすために技術的対策を施した製品を導入することや、業務を外部委託することが許されている。システムベンダは主として技術的対応を施した医療情報システムを提供することで、医療機関等が「説明責任」、「管理責任」を全うすることにおいて補助することが期待されている。医療機関等はシステムベンダが提供する技術的対策と自らが実施する運用的対策と組み合わせて「安全管理ガイドライン」の求める基準に適合させる必要がある。

そのため、システムベンダは提供する医療情報システムにおいて

(1)どのような技術的対策を実施しているのか。

(2)正しくシステムを利用するために注意すべきことは何か。

といったことを明らかにし、医療機関等(医療機関がクラウドサービスを利用する場合はクラウドサービス事業者)に正しく伝える必要がある。

表1 医療機関等における責任(経営管理編より引用)

<table>
<tr><td rowspan="5">全ての医療機関等における責任</td><td rowspan="3">通常時における責任</td><td>管理方法・体制等に関する説明責任</td></tr>
<tr><td>管理及び監査を実施する責任</td></tr>
<tr><td>定期的に見直し、必要な改善を行う責任</td></tr>
<tr><td rowspan="2">非常時における責任</td><td>情報セキュリティインシデントの原因・影響等に関する説明責任</td></tr>
<tr><td>再発防止策等の善後策を講じる責任</td></tr>
<tr><td colspan="2">第三者に業務を委託する場合</td><td>適切な事業者を選定する責任
受託事業者の過失等に対する管理責任</td></tr>
<tr><td colspan="2">第三者に医療情報を提供する場合</td><td>第三者提供が適切に実施されたかに対する責任</td></tr>
</table>

5.3.2. システムベンダの責任

システムベンダは自らの提供する医療情報システムに対して民法上の責任と製造物責任法(PL 法)上の責任を果たさなければならない。

(ソフトウェア単独で提供を行う場合は PL 法の対象とはならないが、コンピュータ等の機器にあらかじめ組み込んで全体をシステムとして提供した場合は動産になるので対象になるとされている。)

PL 法では以下の三つの欠陥についてシステムベンダが責任を問われることとなっている。

(1) 設計上の欠陥(安全法規や基準に適合していない場合等)

(2) 製造上の欠陥(不良な原材料や部品を利用した場合等)

(3) 表示上の欠陥(マニュアルなどに適切な注意事項の記載がない場合等)

これらについては欠陥がないことの立証責任がシステムベンダ側にあるため、システムベンダがその旨を立証しなければならない。

また、民法の 709 条においては、

「故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う」

となっている。これについては権利侵害の立証責任は医療機関等側にあるため、医療機関等がその旨を立証しなければならない。

このような法律上の責任を問われないように、欠陥のない医療情報システムを提供することがシステムベンダにおける重要な責務の 1 つである。

さらに、その医療情報システムが「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」(以降、「薬機法」と記載)の規制対象となる場合は、医療機器とみなされ、前記の PL 法の責任に加えて、安全性、有効性の確保が求められる。薬機法ではソフトウェア単独でも医療機器となり、製造物の責任が存在することに注意が必要である。

5.3.3. 技術的な対応における責任分界決定の考慮事項

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
① 医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者(以下「事業者」という。)から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 医療機関等と保守サービス契約を締結する際は、約款、契約書、SLA 等の書面を用い、提供するシステム・サービスにおける保守サービス内容、対象機器、対象範囲およびそれらに関する責任分界の相互理解を深めた上で契約締結することが望ましい。

(イ) 医療機関等と保守サービス契約を締結する際は、保守事業者は当該医療機関等と守秘義務契約を締結し、保守要員にその内容を遵守させること。

(ウ) 保守事業者は当該医療機関等に保守要員各人を明示的に伝えておくことが望ましい。

5.3.4. 要求仕様適合性の確認を踏まえた調整

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
② 事業者と技術的な対応に関する責任分界を調整する際に、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。

（a）技術的対策

追記事項なし。

（b）運用的対策

（ア）医療機関等がリスク評価できる情報提供については、本ガイドライン 5.4.2 節を参照すること。

5.3.5. 医療機関等が負う責任に関する責任分界

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
③ 通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、企画管理者に対してその結果を報告すること。

（a）技術的対策

追記事項なし。

（b）運用的対策

（ア）医療情報システム・サービス提供に対し契約締結を行う際は、想定されるセキュリティ脅威に対し講じている技術的対策を医療機関に説明を行い、セキュリティ被害発生時、両者が保有する責任について、書面等を用い相互理解を深めた上で契約締結することが望ましい。

（イ）保守サービス提供に対し契約締結を行う際は平時のみならず、非常時も想定し、両者が保有する責任について、書面等を用い相互理解を深めた上で契約締結することが望ましい。

5.3.6. 提供される情報システム・サービスに応じた責任分界

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
④ サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。

（a）技術的対策

追記事項なし。

（b）運用的対策

（ア）サイバー攻撃等が生じた際、調査（支援含む）作業を請け負ったシステム事業者は、発注者に対して請負作業範囲の調査内容について説明責任を負う。

（イ）サイバー攻撃等が生じた際に医療機関等が公的機関への連絡を円滑に遂行するために、報告経路、公的機関連絡先などを運用管理規定等に記載し、院内周知徹底される様、システム事業者側からも提言すること。

5.3.7. 第三者提供における責任分界

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑤ 第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。

（a）技術的対策

追記事項なし。

（b）運用的対策

（ア）提供する医療情報システム・サービスがクラウド基盤を利用している場合は、医療機関等とその情報を共有し、採用しているクラウドサービス事業者が提供している責任共有モデル等を用いて、医療機関等、システムベンダ、クラウドサービス事業者が保有する、各々の責任について説明を行うこと。

5.4.　リスクアセスメントを踏まえた安全管理対策の設計

5.4.1. 情報資産の種別に応じた安全管理の設計

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

提供する医療情報システムで扱う情報について以下の例などを参考にして重要度に応じて分類し、提示できるようにしておくことが望ましい。

情報セキュリティ管理を構築する場合には、まず守るべき対象(保護資産)を識別することから始めなければならない。ここでの保護対象資産は、医療機関等に納入した情報システムに格納される情報と考える。システムベンダは、自社が納入し、稼働している情報システムに格納される情報を識別し、医療機関等に説明できなければならない。

識別された情報は、安全管理上の観点での分類がなされている必要がある。これはリスク分析を行う際の重要な判断基準となる。

なお、企画管理者の指示に基づき実施することを要求しているので、「安全管理ガイドライン 企画管理編」の「6. リスクマネジメント(リスク管理)」を一読することを推奨する。

5.4.2. リスクアセスメントを踏まえた安全管理対策の設計

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
② 事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」を利用することが考えられる。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

情報提供すべき内容を作成するにあたっては、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」において、『一般社団法人日本画像医療システム工業会(JIRA)および一般社団法人保健医療福祉情報システム工業会(JAHIS)による「製造業者/サービス事業者による医療情報セキュリティ開示書チェックリスト」(以下、「MDS/SDS」という。)があり、当該チェックリストが対象とする医療情報システム等を提供する対象事業者においては、当該チェックリストを参考とすることが有効である。』とも解説されている。

【コラム】

医療機関等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）

医療情報システムを安全にかつ有効に運用することに責任を負うのは医療機関等である。医療情報システム・サービス事業者の責任は二次的なものになるが、医療機関等が情報セキュリティ管理（以下、ISMS）を行う際に必要とする情報の提供に関する要望には、適切に応えられるようにしておかなければならない。

本ガイドラインでは、「安全管理ガイドライン」が医療機関等に求める ISMS の実施レベルを実現するために、医療情報システム・サービス事業者側がどのような情報提供をできるように用意しておくべきか、という観点で記述する。

上記で述べたように、ISMS を計画し、実際に導入する責任を負うのは医療機関等であるが、医療情報システム・サービス事業者からの正確な情報提供がなければ、実効力のある ISMS を企画し、構築することはできない。

参考までに、JIS Q 27001:2006 で規定されている、情報システム・サービスに直接関連すると考えられる管理項目（附属書 A による）の例を下記に示す。

A.9.2	装置のセキュリティ
A.10.1	運用の手順及び責任
A.10.3	システムの計画作成及び受け入れ
A.10.4	悪意のあるコードおよびモバイルコードからの保護
A.10.5	バックアップ
A.10.6	ネットワークセキュリティ管理
A.10.8	情報の交換
A.10.10	監視
A.11.2	利用者アクセスの管理
A.11.3	利用者の責任
A.11.4	ネットワークのアクセス制御
A.11.5	オペレーティングシステムのアクセス制御
A.11.6	業務用ソフトウェア及び情報のアクセス制御
A.11.7	モバイルコンピューティング及びテレワーキング
A.12.1	情報システムのセキュリティ要求事項
A.12.2	業務用ソフトウェアでの正確な処理
A.12.3	暗号による管理策
A.12.4	システムファイルのセキュリティ
A.12.5	開発及びサポートプロセスにおけるセキュリティ
A.12.6	技術的ぜい弱性管理

医療機関等が ISMS を構築する場合には、情報システム・サービスが上記の管理策を採用する際にどのような機能を提供実現できるかを説明できるようにしておかなければならない。そうでない場合でも、同様の情報提供が求められることになると考えられる。

（注意）

安全管理ガイドラインの企画管理編では、ISMS の構築時の説明として、継続的改善モデルとして理解し易いやすい旧版 JIS Q 27001:2006 で使用されている「PDCA サイクル」という言葉等を使用して説明を行っ

ている。本ガイドラインにおいても、これに倣い、最新版(JIS Q 27001:2023)の管理策ではなく、旧版を引用して解説を行うこととした。

ISMS で要求されるリスクアセスメントは医療機関等が行うべきものであるが、医療情報システム・サービス事業者は、医療機関等が想定した脅威に対してどの程度対抗できるか、また、そのためにどのような機能を実装しているかについて、説明できなければならない。この説明を確実に行うために、安全管理ガイドラインで紹介されている「『製造業者/サービス事業者による医療情報セキュリティ開示書』ガイド　チェックリスト」や「サービス提供事業者ガイドライン」(総務省・経済産業省)における『サービス仕様適合開示書』を積極的に医療機関等に提出することが望ましい。

下記に検討内容を整理した例を示す。

(1) 医療情報システムの全体構成図

リスク分析を行うにあたって使用したシステム構成図。「サービス提供事業者ガイドライン」の「5.2.1 リスクアセスメント」に記載された作成手順が参考になる。医療機関等に対しては、各システムベンダから提供されたシステム構成図をもとに、医療機関等における医療情報システム全体の構成図をまとめ、これを常に最新の状態に維持し、リスク分析に活用することを推奨すること。

(2) 想定リスク

当該の情報について想定されるリスクの一覧。例えば、想定される脅威として「ディスククラッシュによる破壊」、「端末を覗き見されることによる漏えい」、「通常業務とは関係ない興味本位の情報アクセス」など。

(3) 管理策

想定リスクごとの管理策(対抗策)。例えば、「ディスククラッシュによる破壊」であれば「バックアップ」、「端末を覗き見されることによる漏えい」であれば「スクリーンセーバーの設定」、「通常業務とは関係ない興味本位の情報アクセス」であれば「アクセスログの収集と日常的なログ解析による抑止」など。

(4) 利用できる機能

管理策を実施するために、当該の医療情報システムで利用可能な機能や運用方法など。例えば、「アクセスログの収集と日常的なログ解析による抑止」であれば、「収集可能なログ情報」。

(5) 効果、残存リスク等

上記の管理策を実行した結果、どの程度のリスク低減効果があるか。また、残存リスクはどのようなものがあるか。

なお、巻末の「付録－1. リスクアセスメントの実施例」にリスク分析の具体的な考え方と手順を示したので参考にされたい。

5.5. システム設計の見直し(標準化対応、新規技術導入のための評価等)

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
① システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。
② マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。
③ データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。
④ 電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態にすること。

(a) 技術的対策

(ア) 情報システムは、保持するすべての情報(オペレーティングシステムや、ソフトウェアの動作環境は除く)を標準的な形式(注 1)で出力する機能を備えること。

(注 1)ここでいう標準的な形式とは、格納情報の解析に特定のシステムベンダに固有の知識を必要としない、一般に知られた形式をいう。ここでいう「形式」は、情報コンテナとしての物理的なものを想定しており、情報の論理的な表現体系(病名等のマスタや HL7 等)については想定していない。下記にこのような形式の例を示す。
・CSV 形式のテキストファイル
・XML 形式のテキストファイル
・その他、ISO 等の国際標準や JIS 等の国内標準で定められた形式、または広く一般に知られた形式。

(イ) 情報システムは、保持する情報のうち、他のシステムから移行可能なものについては、標準的な形式で格納された情報から入力する機能を備えること。

(ウ) 薬剤、検査種別等を一意に識別するためのコード体系(いわゆるマスタ情報)を利用する情報システムは、その情報を変更した際に、以前に入力した情報の内容に影響を与えないようにすること。例えば、「γ-GTP」という表記名をもつ検査項目に「0102」というコードを適用していた情報システムにおいて、表記名をそのままに、コードを「00000102」に変更するケースを考える。この変更後、以前にコード「0102」を用いて登録された情報を表示した場合にも、正しく「γ-GTP」が表示されなければならない。

(エ) 上記、(ウ)を実現する方法として、情報格納の際にコードではなく表記名を格納するという方法、情報格納の際にマスタ情報のバージョン番号を格納して複数のマスタ情報を管理する方法、などいろいろな方法が考えられるが、ここでは具体的な実現方法は問わない。

(オ) データ移行を前提として、標準的な形式(安全管理ガイドラインシステム運用編 5 章参照)でのデータ出力を可能とする。

(カ) 受託先システムの OS、データベースマネージメントソフトなどのミドルウェアやアプリケーション業務システムのバージョンアップがあった場合でも、旧バージョンのソフトウェアを使用している委託元の業務に支障のないように、各委託元のバージョンに対応した機能を維持すること。

（キ）業務システムのバージョンアップ等に伴って、データのフォーマット等に変更が発生する場合でも、バージョンアップ前のデータの見読性を担保すること。

（ク）コード化されたデータがある場合は、データ本体が作成された際のコードデータの意味を表すテーブルなどを合わせて管理するなどによりデータが作成された際の見読性を確保する仕組みを提供すること。

（b）運用的対策

（ア）システムベンダは、上記の形式で出力される情報のデータ構造を文書により開示すること。また、この文書の内容は、最新のデータ構造を反映したものであること。

（イ）システムベンダは、自社の情報システムが、標準的な形式で格納された情報から入力する機能を標準的に備えていない場合は、必要に応じて移行用のプログラムを提供すること。

（ウ）情報システムがマスタ情報の変更に際して、過去の情報が受ける影響を回避できない場合には、これによる混乱が生じないように運用に留意するよう医療機関等に推奨すること。

（エ）定期的に安全対策が有効に機能することを点検するとともに、設備が良好に機能する状態を維持できるよう医療機関等に推奨すること。

（オ）機器の更新などによって、保存しているデータの見読性が損なわれることがないように、機器等の維持管理を行うよう医療機関等に推奨すること。

（カ）基本ソフトウェア、業務システムのバージョンアップや修正情報の適用などによって、保存しているデータの見読性が損なわれることがないように、ソフトウェア保守をする際は、試験システムなどで事前に影響がないことを確認した上で業務システムのバージョンアップを行うなどの管理ルールを設け、運用するよう医療機関等に推奨すること。

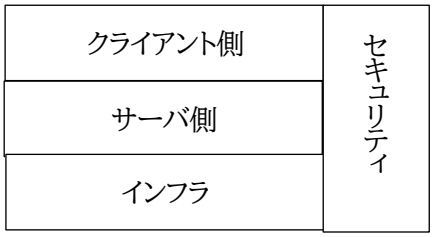
5.6.　安全管理を実現するための技術的対策の体系

5.6.1. 安全管理対策に関するシステムアーキテクチャ(クライアント側、サーバ側、インフラ、セキュリティ)

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】

① システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。



－クライアント側

・情報の持出し・管理・破棄等に関する安全管理措置

・利用機器・サービスに対する安全管理措置

–サーバ側

・ソフトウェア・サービスに対する要求事項

・事業者による保守対応等に対する安全管理措置

・事業者選定と管理

・システム運用管理(通常時・非常時等)

–インフラ

・物理的安全管理措置(サーバルーム等、バックアップ)

・ネットワークに関する安全管理措置

・インフラ運用管理(通常時・非常時等)

–セキュリティ

・認証・認可に関する安全管理措置

・電子署名、タイムスタンプ

・証跡のレビュー、システム監査

・外部からの攻撃に対する安全管理措置

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

5.7. 情報管理(管理・持出し・破棄等)

5.7.1. 外部へ持ち出す医療情報の管理対策

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】

① 医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。

② 保守業務を行う事業者に対して、原則として個人情報を含むデータの持出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。

③ 医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。

④ 持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。

⑤ 持ち出した情報機器等について、公衆無線 LAN の利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。

⑥ 持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認すること。

⑦ 医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。

(a) 技術的対策

(ア) 持ち出し機器、媒体については、必ず情報資産を暗号化できるものを利用すること。

(イ) 持ち出し機器(PC 等を想定)については、必ず起動パスワードでロックがかかるようにすること。その設定ができない機器は利用しないこと。また、パスワードの要件は他の記述と同じく、容易に破られないような内容で設定すること。

(ウ) 持ち出し機器(PC 等を想定)には、必ず不正ソフトウェア対策ソフトを導入し、最新のパターンファイルを適用しておくこと。

(エ) 持ち出し媒体の利用に際しては、適切に管理された媒体で、不正ソフトウェア等の混入が無いことをチェック済みのものを用いること。

(オ) パーソナルファイアウォールを適用できる機器であれば、その機能を有効に設定すること。

(カ) 持出しに際して不要なプログラムはインストールしないこと。

(キ) 覗き見防止フィルタは、装着することが望ましい。

(ク) 持ち出し機器で BYOD(個人の所有する、あるいは、個人の管理下にある端末の業務利用)を行う場合は、管理者により適切に設定された機器を用い、個人による設定変更を禁止すること。

(b) 運用的対策

(ア) のぞき見防止フィルタ等ののぞき見防止機能をシステムとして提供できない場合でも、患者や見舞客等に不用意に目に触れぬよう、適切なパーティションの設置などの工夫をすることが望ましい。

(イ) 保守事業者は医療機関等が定める運用管理規程を遵守すること。

（ウ）個人情報を含むデータが保守の目的で院外に持ち出される場合には、可能な限り詳細な作業記録を残し、当該医療機関等の監査に応じることができることが望ましい。

（エ）個人情報を含むテスト用データの扱いについては、「5.13.ネットワークに関する安全管理措置」を参照すること。

（オ）持ち出しの可否について、医療機関等で定める運用管理規程に従うこと。

（カ）医療機関等の運用管理規程によって持ち出しを許可され、実際に持ち出す場合には、同様に運用管理規程に従うこと。

（キ）医療機関等から持ち出した情報及び情報機器の取り扱いについては、持ち出した組織で定められた運用管理規程を遵守すること。

（ク）保守事業者の運用管理規程には、「安全管理ガイドライン」の少なくとも「遵守事項」の要求事項を盛り込むこと。

（ケ）保守事業者の運用管理規程は、医療機関等の求めに応じて開示できるようにしておくこと。

（コ）必要に応じて、医療機関等から持ち出した情報および情報機器を、当該の運用管理規程に従って取り扱う旨の契約を医療機関等と締結すること。

5.7.2. 医療機関等外から医療情報システムに接続する利用の場合への対策

（1）医療機関等の職員による外部からのアクセス

医療機関等の従業者がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可する場合、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。

外部からのアクセスに用いる機器の安全管理を運用管理規程で定める場合、以下のことに考慮する必要がある。

① PC 等の安全管理対策を確認するためには一定の知識と技能が必要で、医療機関等の従業者にその知識と技能を要求することは難しいこと。

② 運用管理規程で定めたことが確実に実施されていることを説明するためには適切な運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは通常は困難なこと。

③ 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC の場合はもちろん、医療機関等の管理下にある機器を必要に応じて使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性があること。

従って、通常は行うべきではないが、医師不足等に伴う医療従事者の過剰労働等に対応するために、やむを得ず行う場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術が普及しており、これらの導入を検討することが重要であるとともに、運用等の要件にも相当な厳しさが求められる。

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑬ 利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。

（a）技術的対策

（ア）ネットワークは専用線や VPN 技術などを使用し、データの送信元と送信先のエンティティ間の認証を行う方式を採用するのが有効となる。

（イ）データ送信元と送信者での拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなどの容易に解読されない方法を用いるのが望ましい。

（ウ）ネットワーク経路での改ざんを防止するために、専用線などのクローズなネットワーク、または、オープンネットワークを採用する場合は経路の暗号化通信を行うこと。後者の暗号化方式として、IPsec や TLS 等の技術が挙げられる。

（エ）改ざんを検知する方法として、電子署名を用いる等が想定される。

(b) 運用的対策

（ア）委託元である医療機関等内の基幹系ネットワークに接続されているシステムや機器経由で外部（保守ネットワークなど）からの侵入がないように、ネットワーク設計および管理を行うように医療機関等に助言するのが良い。

（2）患者等に診療情報等を提供する場合の外部からのアクセス

医療機関等の間における通信の安全管理とともに、医療機関等が患者との同意の上で情報提供を行うことは十分想定できる。ただし、診療録及び診療諸記録を外部に保存し、受託する事業者が独自に情報提供を行うことはあってはならないとされていることからも、情報を提供する医療機関等が患者の理解できる言葉で納得が行くまで十分に危険性を説明し、その提供の目的を明確にする責任があり、説明が不足している中で万が一情報漏えい等の事故が起きた場合は、その責任を逃れることはできないことを認識しなくてはならない。

また、患者等は自宅等からオープンなネットワークを利用して接続してくることが現実的であり、内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けしておく必要がある。そのため、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 個人認証等の技術を用いる必要がある。

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑧ セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。
⑭ 患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI（Public Key Infrastructure）：公開鍵暗号基盤認証等の対策を実施すること。

(a) 技術的対策

追記事項なし

(b) 運用的対策

（ア）ウェアラブル端末や在宅設置の機器を貸し出す際は、情報セキュリティ上のリスクについて事前に患者等に説明し、同意を得るよう医療機関等に推奨すること。

（イ）IoT 機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者

等に情報提供するよう医療機関等に推奨すること。さらに、医療機関等からシステムベンダへの問い合せ方法を確立すること。

（3）医療機関等が保有する医療情報システムに対して、事業者が外部からアクセスして保守等を行う場合

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑫ 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。

（a）技術的対策

（ア）保守要員であっても保守目的以外に、または、正当な操作者以外がデータにアクセスすることを制限できるようにするのが良い。

（b）運用的対策

（ア）保守作業の申請がされ承認された場合のみ、ルータ等の終端装置の電源を入れる、あるいはLANケーブルを接続するのが良い。

5.7.3. 医療情報の破棄

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑨ 破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な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職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。
⑩ 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。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。
⑪ 外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを証憑または事業者の説明により確認すること。

（a）技術的対策

（ア）医療情報システムの管理・保存している情報について、専用ツール等を用いてその格納領域にNULLデータを上書きするなど、完全消去を行うことが望ましい。その際、消去のための手順を具体的に明示すること。

（イ）マスタに関連している情報（過去分を含む）が使用できないものにならないように考慮しておくことが望ましい。

（b）運用的対策

（ア）次の要件を含む手順書を作成するよう医療機関等に推奨すること。

① 破棄を行う条件

② 破棄作業の従事者の特定

③ 具体的な破棄方法

④ 破棄の記録（項目、書式）

（イ）情報処理機器自体を破棄する場合は次の条件を満たすよう医療機関等に推奨すること。外部業者に

依頼するときは、「安全管理ガイドライン 概説編」の「7. 安全管理のための人的管理(職員管理、事業者管理、教育・訓練、事業者選定・契約)」に準じた委託先選定及び管理を行うとともに、確実に情報の破棄が行なわれたことを証明書等で確認すること。

(ウ) 運用管理規程に「不要になった個人情報を含む装置、媒体の破棄手順書の作成義務」を定めるよう医療機関等に推奨すること。

5.7.4. 医療情報を格納する記録媒体、情報機器等の紛失、盗難等が生じた場合の対応

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
⑮ 医療情報を格納する記録媒体や情報機器の盗難や紛失(ネットワークサービスの利用等による漏洩の可能性の発生含む)が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。

(a) 技術的対策

追記事項なし

(b) 運用的対策

(ア) 可搬媒体等は鍵付きの場所に保管する等、保管方法に考慮すること。

(イ) 可搬媒体等は個体毎に識別できるようにして、管理者を定め、定期的に棚卸をすること。

(ウ) 可搬媒体等に保存している情報は利用後可及的速やかに削除すること。

(エ) 配送サービスを使用する場合、セキュリティに特化した配送サービスを使用するのがよい。

5.8. 利用機器・サービスに対する安全管理措置

5.8.1. 不正ソフトウェア対策

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。
② 常時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(例えばパターンファイルの更新の確認・維持)を行うこと。
③ 医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。
④ メールやファイル交換にあたっては、実行プログラム(マクロ等含む)が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。
⑤ 情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること

(a) 技術的対策

(ア) 開発環境を構築する場合には、メールの閲覧等の一般業務を行う環境から独立した環境で構築することが望ましい。独立した環境を構築することが困難な場合には、コンピュータウイルス対策ソフトを最新の状態に保ち、かつ常時起動させた状態にしておくこと。その他にも必要に応じてファイアウォールの適切な設置や、IDS、IPS を利用すること。

(イ) 適切に管理されていないデバイスやソフトウェアは原則として使用しないこと。可能なら通信ポートの非活性化等を行うことが望ましい。やむを得ず適切に管理されていないデバイスやソフトウェアを使用する場合には、最新のコンピュータウイルス対策ソフト等を利用して十分な確認を行うこと。確認を行う端末は、開発環境とは接続されていないものを使用すること。ただし、コンピュータウイルス対策ソフトを利用したとしてもすべてのコンピュータウイルスを検出できるとは限らないことに注意すること。

(ウ) システムベンダが許可していないソフトウェアが、医療機関等で稼動するシステムにインストールされない仕組みが実装されるか設定されることが望ましい。

(エ) 医療機関等の LAN が外部のネットワークと接続されている場合には、コンピュータウイルス対策ソフトの導入とそのパターンファイルを常時最新の状態に保つことが出来るシステム構成にすること。

(b) 運用的対策

(ア) 提供する医療情報システムが持つ対策と、その耐性を維持するために必要な手順、利用者側で配慮すべき事項を明文化し、医療機関等に提示すること。

(イ) 保守等でやむなくセキュリティパッチソフトウェア等を送付する場合は、事前にコンピュータウイルス対策ソフトを用いて最新のパターンファイルにて無害であることを確認する運用とするよう医療機関等に推奨すること。

5.8.2. IoT 機器の管理

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑥ IoT 機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。 (1) IoT 機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。 (3) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。 ⑦ 企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。

(a) 技術的対策

(ア) IoT 機器を含むシステムが単独でそれぞれの状態を把握できることが望ましい。

(イ) 大量のログ管理やログの暗号化を行う等の対策を講じることが難しい機器・システムの場合、上位のシステムに監視装置を設置する等、システムやサービス全体での対策を検討することが望ましい。

(b) 運用的対策

(ア) セキュリティ上重要なアップデートについての情報は、適時、医療機関等に提供すること。アップデートが困難なことが考えられる場合は、代替措置を検討して情報提供すること。代替措置として、例えば、医療機器に影響する脆弱性を緩和するための IT 機器の構成、既知の悪用に対応する方法等が考えられる。

(イ) 使用を終えた又は停止した機器はネットワークから遮断し、主電源を切るよう医療機関等に推奨すること。なお、IoT 機器の持ち出しや並びに外部利用については、「5.7.1. 外部へ持ち出す医療情報の管理対策」を参照すること

【コラム】

IoT セキュリティに関しては「IoT セキュリティガイドライン ver1.0」(IoT 推進コンソーシアム、総務省、経済産業省;平成 28 年 7 月)、医療機器においては「医療機器におけるサイバーセキュリティの確保について」(平成 27 年 4 月 28 日付け薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号厚生労働省大臣官房参事官(医療機器・再生医療等製品審査管理担当)、医薬食品局安全対策課長連名通知)、「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」(令和 3 年 12 月 24 日付け薬生機審発 1224 第 1 号、薬生安発 1224 第 1 号厚生労働省医薬・生活衛生局医療機器審査管理課長、医薬安全対策課長連名通知)など、厚生労働省の下記のウェブサイトが参考になります。

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

5.8.3. 医療機関等が管理する以外の情報機器の利用に関する対策

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑧ BYOD の実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。
⑨ BYOD であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。

（a）技術的対策

追記事項無し

（b）運用的対策

（ア）BYOD を行う場合は、管理者以外による端末の OS の設定の変更を技術的あるいは運用管理上で制御する等、適切な技術的対策や運用による対策を選択・採用し、十分な安全性が確保された上で行うこと。

（イ）個人保有の情報機器（ノートパソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、医療情報システム安全管理責任者は①～⑤の対策を行うとともに、医療情報システム安全管理責任者の責任において上記の⑥、⑦、⑧、⑨と同様の要件を遵守させること。

5.9. ソフトウェア・サービスに対する要求事項

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
① システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。
② 情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。
③ 医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。
④ 医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるよう措置を講じること。

（a）技術的対策

（ア）各医療機関等の見読目的に対する見読化機能（手段）および平均的なスループットを提示できること。

（b）運用的対策

（ア）情報機器・ソフトウェア構成およびシステム機能仕様書を提示すること。

（イ）情報機器・ソフトウェアの改訂履歴および妥当性検証のプロセスについて明記した作業手順書を提示すること。

（ウ）情報機器・ソフトウェアの品質に関する作業内容を明記した品質管理規定を提示すること。

（エ）各医療機関等では、導入システムの各種の見読目的に応じた見読化手段とスループットをあらかじめ確認した上で、運用を決定すること。

5.10. 医療情報ステム・サービス事業者による保守対応等に対する安全管理措置

5.10.1. 保守作業で使用するデータ

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
① 動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。
⑥ 診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

（a）技術的対策

（ア）個人情報を含むデータは極力使用しないことが望ましい。

（イ）動作確認は原則としてオンサイトで実施することが望ましい。特に個人情報等を含むデータによる動作確認はオンサイトで実施し、データ漏洩等のリスクを極力減らすこと。

（ウ）やむを得ずデータを外部へ持ち出す場合には、データを匿名化することが望ましいが、困難な場合は転送経路の暗号化または暗号化機能を有するデバイスを使用すること。

（エ）個人情報を含むデータを外部へ持ち出した場合には、持ち出しに使用したメモリやディスクへのランダムビットの複数回書込みや物理的な裁断等の手段をとることによって、確認後のデータがメモリやディスク上に残らない確実な削除を実施すること。

（b）運用的対策

（ア）動作確認等で個人情報を含むデータを利用する場合には、明確な守秘義務を医療機関等とシステムベンダ間でルール化し明文化すること。

（イ）また、作業終了後には個人情報を含むデータが不要な場合は確実に当該データを消去すること。

（ウ）個人情報保護法等の法令を遵守することや、データの管理責任者を有する機関から個人情報の利用許可を受けることを医療機関等に推奨すること。

（エ）動作確認に使用するシステムがコンピュータウイルスに感染していないことや、近年の情報漏洩原因になっているファイル共有ソフト等がインストールされていないことを、個人情報を取り込む前に確認することを医療機関等に推奨すること。

5.10.2. 保守要員の登録と管理

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
② 診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。
③ 保守を実施するためにサーバに事業者の作業員(保守要員)がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。

(a) 技術的対策

(ア) 保守要員は個人単位の専用アカウントでシステムにログインできること。

(イ) 個人情報を含むデータへアクセスする場合、「いつ、誰が、誰の」を含む作業記録をシステムログ等、自動的に作成する機能を有すること。この機能の実装が困難な場合には、運用的対策(ア)で補うこと。

(ウ) 作業記録には、アクセスした個人情報を含むデータの識別情報を時系列順に並べて表示し、かつ指定した時間間隔内でどの患者に何回のアクセスが行なわれたかが確認できることが望ましい。

(エ) 保守要員の専用アカウントが含まれるファイルは、適切な暗号化とアクセス制御等の管理により不正使用を防止できること。

(b) 運用的対策

(ア) 個人情報を含むデータへアクセスする場合、「いつ、誰が、誰の」を含む作業記録を書面で作成し、作業後速やかに医療機関等へ提出すること。保守要員の専用アカウントでシステム利用者に模して操作確認等を行う場合にも同等とする。

(イ) 保守要員の専用アカウントは、保守作業の目的以外には利用しないこと。

5.10.3. リモートメンテナンス

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
④ リモートメンテナンス(保守)によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。
⑤ リモートメンテナンス(保守)において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。

(a) 技術的対策

(ア) 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が望ましい。詳細は、「5.17 証跡のレビュー・システム監査」を参照すること。

(イ) リモート保守に関する技術的対策については、「リモートサービスセキュリティガイドライン Ver.4.0」(JAHIS 標準 24-004)を参照すること。

(b) 運用的対策

（ア）オンサイトの保守作業のみならず、リモートによる保守においても作業の操作ログを採取し、作業終了後可及的速やかに操作ログの内容を当該医療機関等に提出すること。

（イ）リモート保守に関する運用的対策については、「リモートサービスセキュリティガイドライン Ver.4.0」（JAHIS 標準 24-004）を参照すること。

【コラム】

JAHIS のリモートサービスセキュリティ WG では、医療分野における遠隔保守（リモートサービス）のあり方と、情報セキュリティマネジメントと個人情報保護の視点からリモートサービスのリスクアセスメントを研究し、医療機関等と医療機器ベンダがそれぞれどのようなセキュリティ対策を取るべきかの検討を行ってきました。

その成果として、リモートサービスを安全に行うためのガイドラインとして「リモートサービスセキュリティガイドライン Ver.4.0」（JAHIS 標準 24-004）を公開しています。

5.11. システム運用管理(通常時・非常時等)

非常時においても医療機関等には患者安全に配慮した医療サービスの提供を優先することが求められる。非常時対応する起点となる「非常時」の定義も明らかにすることが求められる(企画管理編 11.1)が、本ガイドラインでは「非常時」とは、

1)医療情報システムが異常動作あるいは停止した場合

2)システム運用環境が非定常状態になる場合

の 2 種類の状態を言う。

1)の状態は、

(ア) 災害

・災害による医療情報システムの停止、あるいは損傷・破壊

・災害による医療情報システムの運用管理に必要な資源(要員、機材、電源等)の不足等に伴う運用等への支障など

(イ) サイバー攻撃

・外部からの攻撃による医療情報システムの停止、あるいは損傷・破壊

・医療情報の改ざんや漏洩など

(ウ) システム障害

・医療情報システム(サービス)の停止・パフォーマンス低下など

2)の状態は、

(ア) 災害時等に多数の患者が医療機関等に殺到し、通常のアクセス制御下あるいは通常のフローでは運用が困難になる場合

(イ) 災害時等の患者集中により、緊急処置が必要な状態にアクセス権限を持った利用者が不在か手が足りない、などの場合

などに非定常のアクセス制御あるいはフローでシステムを運用する状態である。

医療機関等は事前にこのような状況になった場合の事業継続計画(BCP: Business Continuity Plan)を策定し、それに従って対応することが安全管理ガイドラインで求められている。BCP の詳細な内容は、ガイドライン「企画管理編 11.1」を参照願いたい。

システムベンダは、医療機関等が策定する BCP の内容に沿った機能をシステムに装備することを求められる。あるいは、現状システムの機能を医療機関等に明確に提示し、医療機関等側の BCP 策定に協力することが求められる。また、広域災害時の復旧サポートなどを想定し、システムベンダ自身の BCP の整備も必要となる。

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。 － 「非常時のユーザアカウントや非常時用機能」の手順を整備すること。 － 非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。 － 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できないように変更すること。

- 医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。
- サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。
- 重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

② 医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。

(a) 技術的対策

(ア) 医療情報システムが異常動作あるいは停止する可能性が高いと判断または検知した場合、運用責任者や運用管理者などBCPで定められた人、場所、システムに通知する機能を有することが望ましい。

(イ) 原因に応じた技術的対策を有することが望ましい。例えば電力途絶の場合、非常用電力への自動的な切替機能や安全にシャットダウンする機能、ハードウェア故障時の代替機への切替機能や二重化が施されたハードウェアの採用など。コンピュータ本体関連だけでなくネットワーク機器への対処も必要である。

(ウ) 非常状態に応じた運用切替機能および復旧後の平常運用への切替機能を有することが望ましい。例えば一部の端末あるいは一部の機能のみの縮退運用可能にするなど。

(エ) 非常時回復ツールの装備を有することが望ましい。例えばバックアップからの復旧ツール、データベースの整合性チェックツールなど。

(オ) 復旧後の代替運用からの整合性処置をサポートする機能を有することが望ましい。例えば代替運用時の情報の取り込み機能や整合性確認機能など。

(カ) 非常時用機能を有すること。具体的には、非常時用アカウント制御への切替機能、通常フローでない運用のサポートなど。

(キ) 非常時用機能は、通常時には不必要に使用されないよう対策が取られていること。例えば、非常時用機能が使用されていることが多数の人にわかるようにするなど。

(ク) 非常時用機能に切り替わっていることが利用者に明確にわかるようにすること。

(ケ) 非常時用機能が使用された場合、その時点でそのことを適切な人に通知する機能があると望ましい。

(コ) 非常時用機能が使用された場合、非常時に切り替えたユーザが特定でき、利用記録が残る監査ログ機能を有すること。

(サ) 非常時でなくなった場合、通常運用に切り替える機能を有すること。

(シ) 非定常時に通常使用しない要員(例えば応援の医師など)が使うことを前提に患者番号、性別、年齢等で患者を選択し、最低限の診療記録を参照できる機能を有することが望ましい。(操作性については、全国共通仕様のようなものがあると望ましい)。

(ス) ネットワークの論理的な構成分割(ルータ、L3 スイッチもしくは VLAN を入れてセグメント分割する等)または物理的な分離(バックアップ取得時のみネットワークに接続すること等)を行って、サイバー攻撃の被害拡大を抑制するよう努めること。

(セ) サイバー攻撃やシステム不具合の検知、および非常時用機能に切り替わった際に適切に運用できているかの検知のために、パフォーマンス監視や死活監視できる機能を有すること。

(b) 運用的対策

(ア) システムベンダは導入業者等に対し、医療機関等の BCP 策定、運用、見直しに協力を要請すること。

（イ）システムベンダは導入業者等に対し、広域災害時の復旧サポートなどを想定し、自身の BCP を要請することが望ましい。

（ウ）システムベンダは導入業者等に対し、更に定期的に BCP に基づく障害時のサポート訓練を実施し、その結果を踏まえて BCP の改善を要請することが望ましい。

（エ）非常用ユーザアカウントによる対応を行う場合、以下のような運用を行うよう医療機関等に推奨すること。

① 非常用ユーザアカウント名は非常用であることが明らかにわかる入力しやすいものにすることが望ましい。逆に非常用ユーザアカウントのパスワードは類推しにくいものにすることが望ましい。

② 定常時に非常用ユーザアカウントが利用された場合、そのことを管理者だけでなく多数の人にわかるようにすること。

③ 非常用ユーザアカウントが利用された後、ポリシに従った適切な運用であったかどうかを利用者の報告内容やログなどで確認すること。非常用アカウントでの利用については重点的に監査するなどの対処を実施することが望ましい。

④ 非常用ユーザアカウントが利用された後に定常時に戻った際、非常時用ユーザアカウントの変更やパスワードを変更する等定常時に継続利用できない仕組みを設けること。

（オ）重要なファイルのバックアップについては、数世代バックアップを複数の方式で取得し、一部は不正ソフトウェアの混入による影響が波及しない手段で管理する方法として US-CERT（United States Computer Emergency Readiness Team）が提示したバックアップ 3-2-1 ルールが参考となる。

3: 重要なデータを 3 つの複製で保管（1 つのメインと 2 つのサブ）
2: 異なるタイプの脅威から保護できる、特性が異なる 2 種類の媒体で保管
1: 1 つの複製はオフサイトで保管

https://www.cisa.gov/uscert/sites/default/files/publications/data_backup_options.pdf

特にオフサイト保管の考え方として、災害に対する対策としては地理的に分離すること（遠隔地へのバックアップについては 5.12 章を参照）、ランサムウェアによるサイバー攻撃に対する対策としてはネットワーク的に分離すること（例えば、バックアップ作業時以外は物理的にネットワークから媒体を切り離す等）が重要である。

5.12. 物理的安全管理措置

5.12.1. サーバルーム等の物理的要件

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害(地震、水害、落雷、火災等並びにそれに伴う停電等)に耐えうる機能・構造を備え、災害による障害(結露等)について対策が講じられている建築物に設置することなどを考慮すること。
② 医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。
③ 個人情報が保管されている情報機器等の重要な情報機器には盗難防止を講じること。

近年は医療情報システムにおいても、クラウド基盤等が活用されており、施設内のサーバルームに医療情報を保存しないシステム、サービス提供を行う事業者も存在する。

(a) 技術的対策

(ア) 受託先は、耐震、防火、停電等の設備上の安全対策が施されていること。

(イ) システム障害対策として、外部保存を受託する事業者のシステムは下記のような障害を回避できる冗長構成を採用することが望ましい。

① ハードウェアの障害による長時間のシステム停止

② OS やミドルウェアの障害による長時間のシステム停止

(ウ) ネットワークの障害対策として、セキュリティの確保された複数の通信経路を提供することも有効となる。

(エ) 保存先のデータにアクセスできないことを想定して、診療に支障を来たさない最低限の診療記録を参照できるように委託元医療機関等内に保存できるようにすることが望ましい。

(オ) 大規模災害に備えて、遠隔地にデータバックアップを行い、セキュリティを確保しつつそのデータを参照できる機能を提供することが望ましい。

(カ) ネットワークを通じて外部にデータを保存する場合、災害や障害などによってネットワークが利用できなくても参照できるよう、過去のデータを参照可能なバックアップシステムを内部に準備することが望ましい。

(b) 運用的対策

(ア) 定期的に安全対策が有効に機能することを点検するとともに、設備が良好に機能する状態を維持できるよう医療機関等に推奨すること。

5.12.2. バックアップの管理

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
④ 医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。

医療機関等で利用される情報システムの多くは、データベース管理システム（DBMS）を利用しており、その機能は千差万別ではあるものの、システム障害からの復旧と情報保護を目的とした情報のバックアップについては、ほぼ共通した概念と機能を持つと考えて良い状況である。また、任意のバックアップ情報から、データベースの内容を復元することを、「リストア」と呼び、バックアップとリストアは常に対で考える必要がある。

バックアップ方法としては、下記の三つが一般的であり、情報システムの規模や情報の性質に応じて、適宜運用されている。

フルバックアップ

対象とする情報システムが、ある時点で保持するすべての情報（オペレーティングシステムや、ソフトウェアの動作環境は除く）をバックアップするやり方。これはバックアップ作業の基本的な方法で、すべての情報をバックアップするので作業には一般的に時間を要し、かつ保存に必要なディスク容量も大きくなるが、1回のリストア作業でディスクイメージを復元できるというメリットがある。

差分バックアップ

前回のフルバックアップを行った直後から、任意の時点（差分バックアップを実施する時点）までの差分を、差分バックアップとして管理する方法。フルバックアップに差分バックアップをマージすることで、差分バックアップを実施した時点の状態にリストアできる。一般に差分バックアップで必要とするディスクサイズはフルバックアップよりかなり小さいため、バックアップのために必要なディスク容量を節約できる。フルバックアップの後で差分バックアップを複数回実施すると、後の差分バックアップにはそれ以前の差分バックアップの情報を包含するので、常に最新の差分バックアップだけを管理すればよい。

増分バックアップ

前回のフルバックアップ、または増分バックアップを実施した時点から、任意の時点（今回の増分バックアップ実施時点）までの差分（増分）を増分バックアップとして管理する方法。増分バックアップは、差分バックアップと違って情報の重複がないため、よりコンパクトに管理でき、バックアップに要する時間も短縮できる。また、任意の時点に復帰できるメリットもある。ただし、フルバックアップと実施した全ての増分バックアップを管理しなければならず、リストアの際にはそれらの全てを時系列に従ってマージする必要があるので、管理負荷と作業負荷は一般に差分バックアップによる方法よりも大きくなる傾向がある。

これらの情報の他に、「ジャーナル」や「更新ログ」などの名で知られる、データベースへの変更操作を記録した情報をバックアップ操作に利用する方法もある。

ここでは、「フルバックアップ」を基本として、上記に示した何らかの補助情報を使って、バックアップを管理する際の要件について記述する。操作は利用する DBMS によって詳細が異なるため、ある時点における「フルバックアップ」に補助情報を適用し、その後の時点に更新することを、「変更分を反映する」という言葉で表現することにする。

(a) 技術的対策

（ア）重要なファイルのバックアップについては、数世代バックアップを複数の方式で取得し、一部は不正ソフトウェアの混入による影響が波及しない手段で管理する方法として US-CERT（United States-Computer Emergency Readiness Team）が提示したバックアップ 3-2-1 ルールが参考となる。

https://www.cisa.gov/uscert/sites/default/files/publications/data_backup_options.pdf

3: 重要なデータを 3 つの複製で保管(1 つのメインと 2 つのサブ)

2: 異なるタイプの脅威から保護できる、特性が異なる 2 種類の媒体で保管

1: 1 つの複製はオフサイトで保管

特にオフサイト保管の考え方として、災害に対する対策としては地理的に分離すること(遠隔地へのバックアップについては 7.2.4 章、8.1.2 章を参照)、ランサムウェアによるサイバー攻撃に対する対策としてはネットワーク的に分離することが重要である。

(イ) 医療機関等の特性にあった可用性を確保するために、下記のような冗長性のあるシステムを構成とすることが望ましい。

・デュアルシステム

・デュプレックスシステム

・サーバのクラスター化

・サーバの RAID 構成など

(ウ) 通常の業務システムが停止した場合でも、最低限下記データが参照できる手段を提供できることが望ましい。

・外来診療における前回診療内容

・入院診療における前日までの入院期間中の診療内容(当日以降の治療計画も含む)

(エ) 情報システムは、フルバックアップを実施可能なシステム構成とすること。ここで「実施可能」とは、この作業が妥当な時間内に終了できること、という意味を含んでいる。情報システムのフルバックアップを行う際には、業務の停止を伴うことが多く、この時間が長く(例えば 1 日以上)なると、運用上作業の実施が困難になるので、そのようなシステム構成は推奨されない。

(オ) 情報システムを運用する組織は、フルバックアップを少なくとも 2 世代は保持すること。

(カ) 情報システムは、フルバックアップからのリストアが実施可能なシステム構成とすること。

(キ) 情報システムは、フルバックアップされた情報について、改ざん、もしくは欠落を検知する仕組みを備えること。なお、これができない場合は、「(b) 運用的対策」の(カ)項により、運用で担保すること。

(ク) 情報システムは、前回のフルバックアップから次回のフルバックアップまでの間の差分情報を保持し、反映する機能を備えること。なお、これができない場合は、「(b) 運用的対策」の(オ)項により、運用で担保すること。

(ケ) 補助記憶装置の障害に備え、データのバックアップ機能を提供することが望ましい。この時のバックアップ媒体については、特に規定しなくとも良い。

(コ) システムに障害が発生した場合に備え、過去のデータを参照が可能なバックアップシステムを準備することが望ましい。

(サ) 大規模災害に備えて、遠隔地にデータバックアップを行い、セキュリティを確保しつつそのデータを参照できる機能を提供することが望ましい。

(シ) ネットワークを通じて外部にデータを保存する場合、災害や障害などによってネットワークが利用できなくても参照できるよう、過去のデータを参照可能なバックアップシステムを内部に準備することが望ましい。

(ス) バックアップデータからの復旧を行う場合の復旧時間を考慮して、システム構成およびバックアップ運用を決定するよう医療機関等に推奨すること。

①バックアップデータ格納用サーバの確保

②フルバックアップ、差分バックアップ、増分バックアップ

（セ）基幹システムのサーバ室とは別の場所に、参照サーバやバックアップデータを置くよう医療機関等に推奨すること。

（ソ）データの破壊に対する保護対策として、保管先のシステムの外部記憶装置はRAID構成やクラスター構成などの冗長構成を採用するとともに、万一のデータ破壊に備えてバックアップデータからの復旧ができる手段を備えていること。また、バックアップデータは一日単位で最低一週間以内の任意の日の状態に戻せるように保管すること。

（b）運用的対策

（ア）バックアップからの重要なファイルの復元手順を整備すること。

（イ）管理台帳等を用いてバックアップ媒体の保管先や媒体の耐久年次を管理するよう医療機関等に推奨すること。

（ウ）システムの入替を行う場合には、その前にバックアップを行うことで入替中および入替後に障害が発生しても入替前の状態に戻せるようにするよう医療機関等に推奨すること。

（ウ）技術的な対策で保障できない診療内容について、紙などに残すことを含めたシステム障害時の運用を事前に検討し、障害時の運用マニュアルを整備すること。また、万一障害が発生した場合に、その対応が確実かつ速やかに行えるように障害時運用の有効性を定期的に点検するよう医療機関等に推奨すること。

（ウ）システム障害時の業務停止時間を短縮化するために、ハードウェア、ソフトウェアの保守サポート契約を締結するよう医療機関等に推奨すること。

（エ）情報システムを運用する組織は、リスクアセスメントを行ってフルバックアップを計画（例えば、1 週間前に戻せる、等）し、実施すること。

（オ）前回のフルバックアップから次回のバックアップの間は、変更情報を収集すること。この収集間隔は当該組織の運用ルールで定めること。なお、情報システムに変更情報を収集する機能がない場合は、当該組織の運用ルールで、許容可能なフルバックアップの間隔を定め、そのとおり実施されるような管理を行うこと。

（カ）情報システムを運用する組織は、作成したフルバックアップを保護し、改ざん、もしくは欠落が起きないように運用（例えば、バックアップを作成した媒体に封をして、鍵のかかる保管庫へしまう、等）すること。

（キ）情報システムを運用する組織は、テスト環境等を使ったフルバックアップからのリストア手順を、少なくとも 1 年に 1 度は確認しておくことが望ましい（注 1）。

（注 1）データベースのフルバックアップをリストアし、その内容を検証することは、実際には極めて困難である場合が多いと想定される。これを行うには、検証用のプログラムを提供することに加えて、リストア用の環境を医療機関等に用意していただく等、費用的な困難さも伴う場合がある。フルバックアップからのリストアを実際に行わなければならないような事態の発生自体を回避するような運用が望まれるが、本件に関しては医療機関等にもリスクの大きさを理解いただいて、何とか実現するようにもって行くことが望まれる。

（ク）情報システムがフルバックアップの改ざんを検知する仕組みを備えることができない場合は、データベースの内容変更が通常のアプリケーションを介さない手段（管理ツールの利用等）でなされないような管理を行うこと。また、通常のアプリケーションを介した内容変更は、監査ログにより追跡可能な運用を行うこと。

（ケ）委託元の医療機関等内に電子データとして保存する場合は、保存データの改ざん、盗難等を防ぐための安全管理を行うよう医療機関等に推奨すること。

5.12.3. 記録媒体等の経年変化の管理・委託事業者への配送等

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑤ 記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

5.12.4. 端末・サーバ装置等の不適切な利用等に関する対策

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑥ 利用者が医療情報を入力・参照する端末から長時間離席する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。

(a) 技術的対策

(ア) 医療行為を妨げない範囲で、利用者端末の自動スクリーンロックを設定すること。

(イ) クローズ処理等(例えば、セッションの切断、スリープモードへの移行、使用していないアプリケーションの停止)の機能を有することが望ましい。実現することが困難な場合には、OS 附属のパスワード付きスクリーンセーバー等を利用できるように端末を設定すること。

(ウ) 利用者が離席する際に、利用者自らがスクリーンロックまたはログアウトできる仕組みを有すること。

(エ) 利用者が長時間離席し、正当な利用者以外の物による入力のおそれがある場合は、クリアスクリーン等の機能を設けること。

(b) 運用的対策

(ア) ログイン中の利用者以外の者が容易にアクセス可能な場所に設置してある端末に関しては、一定期間無操作後の自動ロックを利用するのではなく、離席時に速やかに手動でロックをかけるよう教育し徹底させるよう医療機関等に推奨すること。基本的に一定期間無操作後の自動ロックは補助的に使用することが望ましく、ログイン中のユーザが離席時に明示的にロックすることが望ましい。

(イ) 端末操作中にその場を離れる場合は、操作の終了手続きを取るなどにより、他の人が引き続いて(成り済まして)端末操作できないように運用で定めるよう医療機関等に推奨すること。

5.13. ネットワークに関する安全管理措置

5.13.1. はじめに

外部ネットワークを利用して外部と医療情報を交換する場合、情報の送信元から送信先に確実に情報を送り届ける必要がある。その際、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要がある。この端末間の通信路のセキュリティをチャネル・セキュリティと呼び、情報の内容に対するセキュリティのことをオブジェクトセキュリティと呼ぶ。

安全管理ガイドラインでは、医療情報システムが利用するネットワークの安全性を確保するために、チャネル・セキュリティとして利用するネットワーク回線の安全性の確保、及びオブジェクトセキュリティとして送信する医療情報に対して暗号化措置を講じることを求めている。また、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守られるよう、対策を講じることを求めている。

チャネル・セキュリティは確実に確保される必要があるとされており、原則、接続先が限定されている、あるいは接続先までの経路等が管理されている「セキュアなネットワーク」(「専用線」、「IKE+IPsec 接続」、「IP-VPN 接続」)を用いることと整理されている。ただし「オープンなネットワーク」を用いて医療情報を医療機関等の外部とやり取りする場合には、「セキュアなネットワーク」と同様の安全性を確保する措置を講じ、通信することが求められており、遵守事項が示されている。

そのため、「セキュアなネットワーク」を構築するために、ネットワークの論理的または物理的な構成の分割、接続機器の制御、通信するデータの制御等のセキュリティ対策を実施し、適切なネットワークを選択することが求められる。その際、事業者間の責任分界を明らかにする必要がある。更に、不正な通信の検知や遮断、監視を行うことで、巧妙化するサイバー攻撃への対応を検討する必要がある。

5.13.2. 外部との通信における責任分界

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 医療機関等の間の情報通信には、医療機関等だけでなく、電気通信事業者やシステムインテグレータ、運用を受託する事業者、遠隔保守を行う機器保守事業者等の多くの組織が関連する。そのため、次に掲げる事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。

・診療録等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定

・送信元の医療機関等がネットワークに接続できない場合の対処

・送信先の医療機関等がネットワークに接続できなかった場合の対処

・ネットワークの経路途中が不通の場合又は著しい遅延が発生している場合の対処

・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処

・伝送情報の暗号化に不具合があった場合の対処

・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処

・障害が起こった場合に障害部位を切り分ける責任

・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処

また、医療機関との責任分界を明確にするために下記の事項を確認しておくことも有効である。

・通信機器、暗号化装置、認証装置等の管理責任(責任分界点も含めた整理と契約の締結)

・医療機関による患者等に対する説明責任

・事故発生時における医療機関の専任の管理者

・交換した医療情報等に対する管理責任及び事後責任(個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項)

5.13.3. 外部との通信における脅威と対策

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
② セッション乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。
③ オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。
⑨ ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。
⑩ 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。

医療機関等において医療情報をネットワーク上で交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要があるとし、また、医療機関等は選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要があるとしている。リスクを鑑みた対応として、必要に応じて、ネットワークの分離や、これを踏まえた情報交換のルールに基づく管理を行うことが望ましいとされている。

また、外部から情報を取り込む際に、取り込む情報の安全性を確認する必要があり、標的型攻撃等によるリスクを減少する対応を図ることが求められている。

(a) 技術的対策

(ア)「セキュアなネットワーク」(「専用線」、「IKE+IPsec 接続」、「IP-VPN 接続」)を用いること。

(イ)「オープンなネットワーク」を用いて医療情報を医療機関等の外部とやり取りする場合には「5.13.6 オープンなネットワーク上で HTTPS を利用する際の安全対策」を適用すること。

(b) 運用的対策

追記事項なし。

【コラム】

クローズドなネットワークでの安全対策

これまでは通信上の脅威に対して、クローズドなネットワークによる接続とすることによって、外部からの脅威を低減させる対策が取られる場合があった。クローズドなネットワーク接続は、オープンな接続に比べて安全であることは変わりないが、医療提供の仕方の変化や、技術の進展、政策によって、複数拠点の接続が出てくる等、利用するネットワーク環境に変化が出てきており、脅威が侵入・拡散する可能性が無いとは言えなくなってきている。このため、内部に侵入があったことを想定した対策をとる必要がある。

5.13.4. 外部との通信における認証

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
④ オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。
⑫ 医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。

情報を送ろうとする医療機関等と、送信先の医療機関等は相互に適切な認証を採用して、相手が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であるかを確認しなくてはならない。

そのため、例えば通信の起点と終点で相互を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いて認証する等の対応を取ることが考えられる。

また、通信のなりすまし防止については、情報の改ざん防止と併せて、適切な認証の仕組みとともに医療情報等に対して電子署名を組み合わせることも考えられる。

(a) 技術的対策

(ア) ネットワークは専用線や VPN 技術などを使用し、データの送信元と送信先のエンティティ間の認証を行う方式を採用するのが有効となる。

(イ) データ送信元と送信者での拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の必要な単位で、相手の確認を行う必要がある。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなどの容易に解読されない方法を用いるのが望ましい。

(ウ) 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を実施すること。また、「14. 認証・認可に関する安全管理措置」の対策も参照すること。

(b) 運用的対策

（ア）委託元である医療機関等内の基幹系ネットワークに接続されているシステムや機器経由で外部（保守ネットワークなど）からの侵入がないように、ネットワーク設計および管理を行うように医療機関等に助言するのが良い。

（イ）施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐため、「14. 認証・認可に関する安全管理措置」の対策も参照すること。

5.13.5. 外部との通信に利用する機器の選定

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑤ ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特に VPN 接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。

（a）技術的対策

追記事項なし。

（b）運用的対策

追記事項なし。

5.13.6. オープンなネットワーク上で HTTPS を利用する際の安全対策

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑥ オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合には TLS1.2 の設定によることも可能とする。その際、TLS の設定はサーバ/クライアントともに「TLS 暗号設定ガイドライン 3.0.1 版」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型の IPsec 又は TLS1.2 以上により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。

オープンなネットワーク上で HTTPS を利用した暗号化通信が行われているが、昨今 TLS においてプロトコルやソフトウェアの脆弱性を突いた攻撃の報告が相次いでおり、安全性を確保するためには情報処理推進機構から発行されている「TLS 暗号設定ガイドライン」にて示される設定として「高セキュリティ型」を反映することに加え、TLS クライアント認証を行う必要がある。

なお、「高セキュリティ型」の設定の一つとして、利用可能なプロトコルバージョンを TLS1.3 に設定することになっているため、TLS のサーバについて TLS1.3 に対応しておく必要がある。システムやサービス等の対応上、TLS1.3 への対応が難しい場合には、TLS1.2 以上に限定して設定する必要がある。サーバ証明書、暗号スイートについては、「高セキュリティ型」設定を行う必要がある。

（参照：「TLS 暗号設定ガイドライン」

https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.1.0.pdf）

（a）技術的対策

（ア）オープンなネットワークを経由して HTTPS 通信を行う場合、下図のように TLS1.3 以上(システム・サービス等の対応が困難な場合には TLS1.2 で適切な設定によることも可能)を使用したセッションに関してはセキュアであるが、セッション間の回り込みにより医療機関等側のクライアント等がコントロールされ不正アクセスされるおそれがあるため下記のような対策が必要とされる。

・ルータ等の設定で接続可能なサイトを限定する。

・基幹系、情報系のネットワークを分離する。

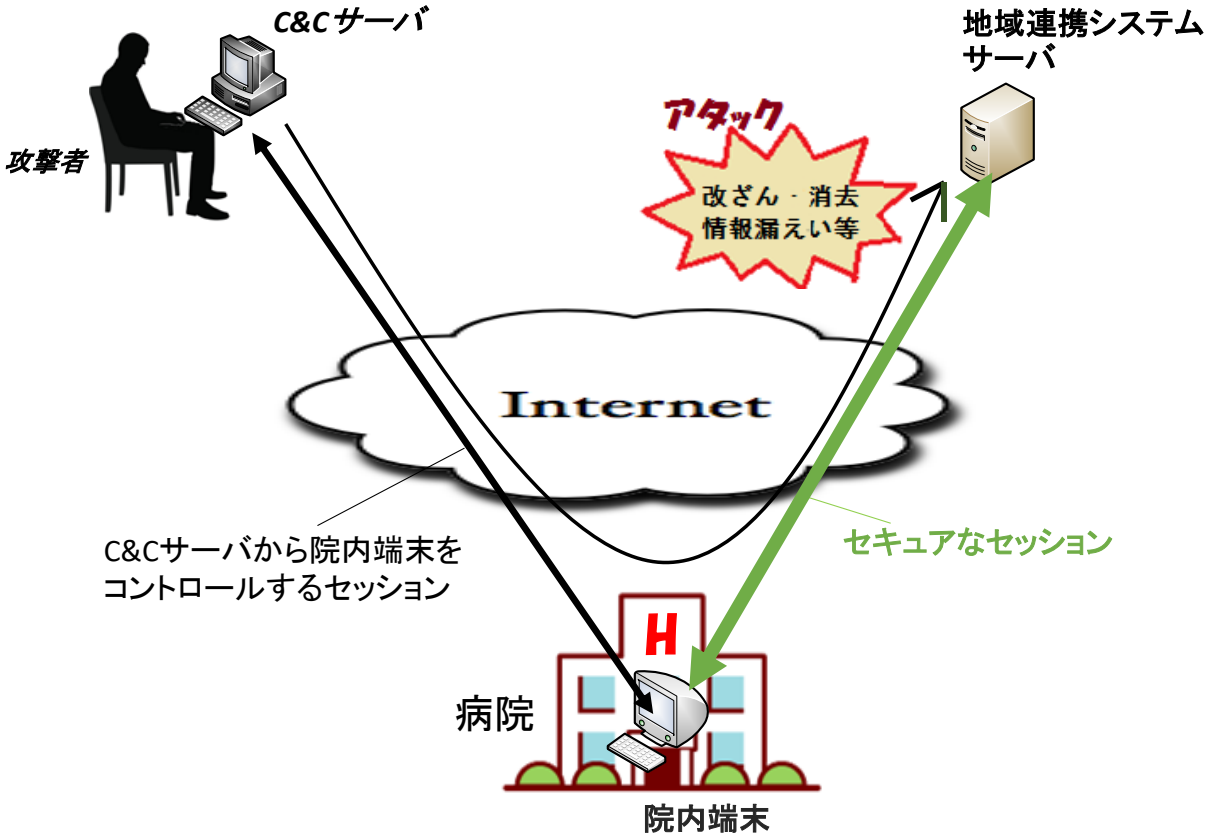


図 2.セッション間の回り込み

（b）運用的対策

追記事項なし。

5.13.7. 外部との通信における秘匿性の確保

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑦ 利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号

化等のセキュリティ対策を実施すること。

適切な認証の仕組みとともに、情報の機密度に応じたネットワーク種別と情報そのものに対する暗号化を採用しなければならない。暗号化技術にはそのアルゴリズム特有の脆弱性や、鍵強度の問題など定期的な保守や対応が必要となるが、安全管理ガイドラインでは電子政府推奨暗号を使用することとなっている。(参照:「暗号技術検討会」https://www.cryptrec.go.jp/method.html)

(a) 技術的対策

(ア) 例えば、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。

(b) 運用的対策

追記事項なし。

【コラム】

安全管理ガイドラインの Q&A「システム運用編」において、ネットワークを介してやり取りする情報に対する暗号化等のセキュリティ対策として「暗号化の鍵については電子政府推奨暗号のものを使用してください。」とされています。この状況では情報に対する暗号化の対策としては IPsec および TLS1.2 以上の利用によって通常対応していることと思います。一方、それ以外の方法によってネットワークを介してやり取りする情報そのものを暗号化する場合、その暗号化において電子政府推奨暗号を使用することに意味はあるのでしょうか？なお、安全管理ガイドラインの中にはそれに関する記述は見当たりません。

個人情報が情報漏洩した場合はその情報が暗号化されていても個人情報保護委員会への報告が必要となりますが、個人情報保護委員会からそれを不要とする条件が示されています。個人情報保護委員会の Q&A によると『「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合」とは、どのような場合が該当しますか』に対する回答として、該当すれば個人情報保護委員会への報告を要しないこと、そして該当する場合とは「適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていること」と説明されています。

上記によれば、個人情報保護委員会が情報漏洩しなかった場合と同等に扱っていることから、情報そのものに対する暗号化にも電子政府推奨暗号を用いるべきと考えられます。ただし、以下の点に注意が必要です。

1. 情報漏洩発生時点で、実装された暗号化技術が電子政府推奨暗号リストに含まれているとは限らないこと。

   →暗号技術は技術の進歩により安全ではなくなるため(危殆化)、電子政府推奨暗号リストの入れ替えが行われます。そのため、あらかじめ「個人情報保護委員会への報告を要しません」と言えるとは限らないため、顧客への説明の仕方に注意が必要です。

2. 高度な暗号処理の必要性とバランスを考慮すること。

   →高度で処理負荷の高い暗号化をやりすぎると、システムの可用性を損ねる場合があるためです。

3. 制度の変更に注意すること。

   →個人情報保護委員会の Q&A が変わる可能性にも留意が必要です。

5.13.8. ネットワークを通じて医療機関等の外部に保存する場合の真正性の確保

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑧ 医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。

ネットワークを通じて外部に保存を行う場合、委託元の医療機関等から委託先の外部保存施設への転送途中で、診療録等が書き換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。そのため、ネットワークを通じて医療機関等の外部に保存する場合は、ネットワーク特有のリスクにも留意しなくてはならない。

(a) 技術的対策

(ア) ネットワーク経路での改ざんを防止するために、専用線などのクローズなネットワーク、または、オープンネットワークを採用する場合は経路の暗号化通信を行うこと。後者の暗号化方式として、IPsec や TLS 等の技術が挙げられる。

(イ) 改ざんを検知する方法として、電子署名を用いる等が想定される。

(b) 運用的対策

追記事項なし。

5.13.9. 外部ネットワーク接続(不正な通信の検知や遮断、監視)

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
⑪ 医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。

(a) 技術的対策

(ア) 技術的対策については、「5.8.利用機器・サービスに対する安全管理措置」、「5.17. 証跡のレビュー・システム監査」の「(a) 技術的対策」を参照すること。

(イ) 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含む。)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。

(ウ) ファイアウォールや ACL の設定をデフォルトのまま放置せず、権限を持つ者のみがアクセス可能となるよう適切な設定を行うこと。これらを設定した後に脆弱性を診断し、その結果に基づいて修正または追加の対策を行うこと。

(エ) 医療機関等のネットワークがインターネットに接続されている環境では、ファイアウォールに加えて、不正アクセスを受けていることを早期に知るために IDS を併用し、不正アクセスを継続的に監視・報告する、または、IPS を併用し不正な攻撃を遮断することが望ましい。

(オ) 医療機関等のネットワークを外部と接続する経路として、インターネット、Internet-VPN、IP-VPN、

専用線がある。一般的に後者のものほど、送受信中のデータに対する盗聴や改ざんおよび医療機関等のネットワークへの不正アクセスに対して強固なセキュリティを確保することが可能である反面、コストが大きくなるという特徴がある。複数の経路を確保し目的別に利用できることが技術的には望ましいが、コスト的かつ運用的に現実的ではないため、医療機関等の接続目的から適切な経路を選択することが望ましい。

(b) 運用的対策

(ア) 運用的対策については、「5.8.利用機器・サービスに対する安全管理措置」、「5.17. 証跡のレビュー・システム監査」の「(b) 運用的対策」を参照すること。

(イ) システムベンダは外部ネットワーク接続に関するネットワーク構成や機器に関する情報を医療機関等へ適切に提供すること。

(ウ) 医療情報システムに関する全体構成図(ネットワーク構成図・システム構成図等)を利用し、外部のネットワークとの接続点にある機器を管理するよう医療機関等に推奨すること。

(エ) 適切に設定されたネットワークやシステムの各種設定内容を記録しておき、その記録と設定内容を定期的に突き合わせることによって、システム環境が脆弱な状態に変更されていないことを確認するよう医療機関等に推奨すること。

5.13.10. 無線 LAN の利用における対策

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
⑬ 医療情報システムにおいて無線 LAN を利用する場合、次に掲げる対策を実施すること。 − 適切な利用者以外に無線 LAN を利用されないようにすること。例えば、ANY 接続拒否等の対策を実施すること。 − 不正アクセス対策を実施すること。例えば MAC アドレスによるアクセス制限を実施すること。ただし、MAC アドレスは詐称可能であることや、最近のモバイル端末においてはプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることから、MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。 − 不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP 等により通信を暗号化すること。 − 利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること。

無線 LAN は、ケーブルの敷設や接続の必要がないという利点があり、昨今の無線 LAN ルータの低価格化とノートパソコンへの無線 LAN アダプタの標準装備により医療機関等内で一般的に使われる情報インフラとなっている。

ただし、適切に使用しない場合、「通信内容の傍受(盗聴)」、「不正利用」、「無線 LAN アクセスポイントのなりすまし」等の脅威がある。さらに、電波を利用しているため、ケーブル LAN に比較して電波干渉による通信の途絶や遅延など可用性に劣る面がある。

無線 LAN を利用するシステムを構築するシステムベンダは、医療機関等のシステム管理者と協力し、これらのリスクに留意し適切な対策を行わなくてはならない。

【コラム】

無線 LAN による電波が医療機器等へ及ぼす影響については、総務省のホームページには「電波の医療機器等への影響に関する調査」の報告書等の電波の医療機器等への影響の調査研究が公開されています。

（https://www.tele.soumu.go.jp/j/sys/ele/seitai/chis/）

(a) 技術的対策

（ア）無線 LAN は ANY 接続拒否で利用すること。

（イ）少なくとも MAC アドレスによる機器認証を行うこと。ただし、MAC アドレスによる認証は MAC アドレス詐称が可能であることから、802.1x による認証を行うことが望ましい。

（ウ）WPA-TKIP、WPA2-AES 等により、通信を暗号化すること。

（エ）認証方式としては、鍵管理方式により、事前配布方式(WPA-PSK、WPA2-PSK)と IEEE802.1X 認証を用いた認証サーバによる方式(WPA-EAP、WPA2-EAP)等がある。どの方式を選択するかは、無線基地局の数によるメンテナンスコストと認証サーバのシステム運用コストの差を算出し決定すること。無線基地局が多い場合は、認証サーバを用いる方式にトータルコストメリットが期待できる。

(b) 運用的対策

（ア）電波を発する機器(携帯ゲーム機、電子レンジ、デジタルコードレス電話、Bluetooth 利用機器等)によって電波干渉が起こり得る。無線 LAN を利用するシステムのベンダはこれらの機器が使われているかどうかをチェックするとともに、医療機関等のシステム管理者に対して、これらの機器の利用に関する対策を規定し、運用管理規程に反映するよう医療機関等に推奨すること。

5.14. 認証・認可に関する安全管理措置

5.14.1. 利用者の識別・認証

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証方法に関する手順等に関して、規則、マニュアル等で文書化すること。
⑦ 医療情報システムにおいて用いるIDについて、台帳管理等を行うほか、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。

(a) 技術的対策

(ア) システム利用者に対応する ID、及び後述するパスワード等の認証手段により利用者識別を行う仕組みを有すること。

(イ) システム利用者のユーザ登録権限を持つ者以外による登録が行われない仕組みを有すること。

(ウ) システム利用者の退職、長期休職等においてIDが有効になったままではパスワードが推測され、成りすまし等で悪用される可能性が高くなるため、IDを削除可能な仕組みを実装すること。可能であれば、ID 無効化・有効化の仕組みを有し、システム利用者が休職前と復職後で同一の ID を利用できることが望ましい。また、長時間利用されないIDについては容易に検索できる、または通知する機能があることが望ましい

(エ) ID 登録時に、過去に発行した同一の ID が存在する場合は、その旨警告し、同一の ID が複数登録されないような仕組みを有することが望ましい。

(オ) 利用者のログイン管理機能として以下のものが備わっていること

・システムへのログイン情報(ユーザ識別情報、ログイン時刻、使用時間)の採取・記録、および 1 ヶ月以上の期間のログイン情報を保持・管理する機能

・指定期間(年月日・時間帯)のログイン情報をサーチし、例えば以下のような事項の参照が容易に可能なこと

・利用者別の日別ログイン時刻、使用時間と使用端末 ID

・ログイン失敗者別のログイン操作時刻、失敗回数と使用端末 ID

利用者が長時間離席し、正当な利用者以外の物による入力のおそれがある場合は、クリアスクリーン等の機能を設けること。

(b) 運用的対策

(ア) システム利用者の ID・パスワードや IC カード、電子証明書、等の設定および発行ルール、並びに、本人への配布手段の規定化を医療機関等に推奨すること。

(イ) 医療情報システムの短期利用者に対して同じ ID を再利用する場合は、再利用開始までに一定の期間をおく、また、再利用初回に確実に本人のみが知りえる情報または持ちえる情報を識別情報として登録するよう医療機関等に推奨すること。また、ID の利用開始と終了日時を管理台帳等で管理・保管し、ある期間において誰が該当 ID を使用していたかを後日調査可能とするよう医療機関等に推奨すること。

(ウ) システム利用者の退職等により不要となった ID は速やかに削除し、休職等により不用となった ID は速やかに無効化するよう医療機関等に推奨すること。さらに、可能であればシステム利用者の勤務表等を用いて、勤務時間以外等の不審なアクセスが存在しないかを定期的に確認するよう医療機関等

に推奨することが望ましい。

（エ）一つの ID を複数人で共有しないよう医療機関等に推奨すること。

（オ）端末操作中にその場を離れる場合は、操作の終了手続きを取るなどにより、他の人が引き続いて（成り済まして）端末操作できないように運用で定めるよう医療機関等に推奨すること。

5.14.2. パスワードを使用した認証

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
② 利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。 ⑥ パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること － 類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。 － 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。 － 利用者のパスワードの失念や、パスワード漏洩のおそれなどにより、医療情報システムのシステム運用担当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うとともに、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）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。 － 医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。

（a）技術的対策

（ア）利用者によりパスワードを変更できる機能を有すること。

（イ）初期パスワードの変更をシステムが求める機能を有することによって、初期パスワードが利用され続けることがないようにすることが望ましい。

（ウ）パスワードを利用者の認証に使用する場合、次に掲げる対策を実施すること。

－ 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換による）した状態で保存可能なこと。

－ 医療情報システムの担当者であっても、利用者のパスワードを推定できないようにすること。（設定ファイル等にパスワードを記載しないこと）

（エ）パスワードの設定は、以下の要件を満たすよう強制できるようにすること。

－ 英数字、記号を混在させた 13 文字以上の推定困難な文字列

－ 英数字、記号を混在させた 8 文字以上の推定困難な文字列でかつ、定期的に変更させる（最長でも 2 ヶ月以内）

－ 二要素以上の認証の場合、英数字、記号を混在させた 8 文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用に PIN 等が設定されている場合には、この限りではない。

（オ）パスワードの設定は、以下の制限機能を設けることが望ましい。また、条件を満たさないパスワードの設定に対して警告する機能を有することが望ましい。

－ 利用者の氏名や生年月日、辞書に記載されている単語等の類推されやすいパスワード

－ 同一パスワードや類似パスワードの繰り返し使用

（カ）一定期間パスワードの変更が行われていないシステム利用者に対する警告機能が実装されていることが望ましい。また、管理者向けに、一定期間パスワードが変更されていないシステム利用者の検索機能を実装することが望ましい。

（キ）パスワード入力の失敗による不応答時間を設定できる機能を実装することが望ましい。不応答時間は医療機関等の判断によって設定可能であることが望ましい。

（ク）一定回数以上のパスワード入力失敗が連続した場合に、アカウントの利用を停止する機能を実装することが望ましい。利用停止されたアカウントの回復は、権限があるユーザのみによって可能であることが望ましい。

（b）運用的対策

（ア）パスワードを利用者の認証に使用する場合は、以下のように運用するよう医療機関等に推奨すること

－ パスワードを他者に教えないこと。

－ 他者にパスワードが漏れないようにすること

－ パスワードを記載したメモを作成しても良いが他人に渡らないようにすること

－ モニタ等へのパスワードが記載されたメモ書き等の張り紙を行わないこと

－ 入力するところを他の人に見られないように注意すること

－ 初期パスワードは必ず速やかに変更すること。

－ システム管理者は週 1 回以上、その期間の全利用者のログイン時刻、使用時間・回数から統計的に検出される非定常運用状況（例えば、ログイン時間が非常に長時間なケース、ログイン回数が非常に多いケース、複数端末から同時ログインを行おうとしたケース等）を確認し、問題の発生がないか確認すること。

－ 氏名や生年月日、辞書に記載されている単語等の類推されやすいパスワードを避けること。

－ 類似のパスワードの繰り返し使用を避けること。

－ 英数字、記号を混在させた 13 文字以上の推定困難な文字列のパスワードを設定すること。

－ 英数字、記号を混在させた 8 文字以上の推定困難な文字列のパスワードを設定し、定期的（少なくても 2 か月に 1 回）にパスワードを変更すること。

－ 二要素以上の認証の場合、英数字、記号を混在させた 8 文字以上の推定困難な文字列のパスワードを設定すること。ただし他の認証要素として必要な電子証明書等の使用に PIN 等が設定されている場合には、この限りではない。

（イ）ID やパスワードの漏洩事案が発生した場合には、速やかに責任者またはその代行者に連絡するよう連絡先や手順を明確にし、また、システム利用者の教育を行うことを医療機関等に推奨すること。

5.14.3. パスワード以外を使用した認証

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
③ 利用者の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、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ること

⑤ 利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。

(a) 技術的対策

(ア) 管理区域以外に設置、使用されることが想定される場合、又は管理区域内に設置されていても管理区域以外からリモートで使用されることが想定される場合は、二要素認証を実装すること。

(イ) 認証にバイオメトリックスを使用する場合には、認証に使用する身体的特徴情報が読取装置の外部へ出ない構造か、身体的特徴情報を暗号化してから読取装置の外部へ送り出す構造のものを使用すること。

(b) 運用的対策

(ア) 二つの独立した要素の組み合わせとして、公開情報となっている ID と取得すると誰でも利用できる USB トークンのように比較的容易に他人が入手可能な要素同士のみの組み合わせは避けるよう医療機関等に推奨すること。

(イ) IC カード等のセキュリティ・デバイスを認証に使用する場合、少なくとも以下を運用ルールに含めるよう医療機関等に推奨すること。

- 他者に貸与しないこと。
- 定期的に所持確認をすること。(例:毎日 1 回)
- 所在不明となった場合は予め定めた報告先に速やかに報告すること。

(ウ) IC カード等のセキュリティ・デバイスを認証に使用する場合、IC カード等の破損等、セキュリティ・デバイスが利用できないときを想定し、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るよう医療機関等に推奨すること。

5.14.4. 情報の区分管理とアクセス制御

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】
④ アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。

(a) 技術的対策

(ア) 医療情報システムにおいて情報や機能を目的により分け、利用者の種類(職務、資格等)および利用者単位で、利用可能・不可能の設定ができるような機能を有すること。

(イ) アクセス権を設定する職種等の種類は固定でなく、医療機関等の業務実態に合わせて自由に設定できることが望ましい。

(ウ) 情報へのアクセス(参照・入力・更新)に際し、その処理内容を時刻情報とともにログ出力(アクセスログ)し、誰がどのような情報の入力・更新を行ったか識別できること。

(エ) アクセスログの解析機能として、例えば以下のものを備えること。

・情報の種別を指定し、その種別の情報にアクセスした実績(アクセス拒否やパスワード入力エラー等を含む処理内容)を指定した日時(時間帯)で時間軸に沿って画面等に表示する機能。

・利用者を指定し、その利用者がアクセスした実績(情報の種別とその処理内容)を指定した日時(時

間帯)で時間軸に沿って画面等に表示する機能。

・端末 ID を指定し、その端末からアクセスした実績(情報の種別とその内容)を指定した日時(時間帯)で時間軸に沿って画面等に表示する機能。

・管理上のスクリーニングチェック機能として、特殊な時間帯にアクセスした累積時間順の利用者リストや、指定期間内にアクセスした患者情報件数順の利用者リスト等を表示する機能。

・日時の順序性チェックなどにより、端末の不正な時刻変更を検出できる機能。

・ログを分析して緊急時にアラートを発する機能。

(b) 運用的対策

(ア) 情報がどのように分類されており、それぞれに対してどのような権限を設定可能であるかをシステムベンダは明文化し、医療機関等に情報提供すること。さらに、これらの設定方法についても明文化すると共に、医療機関等の適切な責任者に十分説明することによって、独自の判断で任意のタイミングにおいて設定できるようにすることを医療機関等に推奨すること。

(イ) 以下の運用的対策を実施するよう医療機関等に推奨すること。

・システム管理者は、アクセス権の設定・更新を必要に応じて行うこと。不要になった権限に関しては即座に削除すること。

・システム管理者は、アクセスログを必要な期間に渡って安全に保存し、後からの分析調査が行えるようにすること。

・アクセスログ管理は、スクリーニングチェックに関しては 1 回／週以上の頻度で行い、その他の機能は必要に応じて実施すること。また、個室等の従業者の眼が届かない所に置かれる端末の操作状況については、更に十分な管理を行うこと。

・抑制効果を高めるため、当該医療機関等の責任者は違反者に対する罰則規程等を定め、利用者全員に予め通知しておくこと。

5.14.5. 電子カルテシステム等における入力・確定者の識別

(1) 電子カルテシステムにおける記録の確定手順の確立と識別情報の記録 - PC 等の汎用入力端末により記録が作成される場合

<安全管理ガイドライン(システム運用編)の要求事項>

【遵守事項】

⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。

－ 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合

a 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定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時を含めること。

b 「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。

c 「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。

d 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

e 一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確な

ルールを運用管理規程に定めること。

f 確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。

－ 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合

a 運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報(又は装置の識別情報)、信頼できる時刻源を用いた作成日時を記録に含めること。

b 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

システムで診療録等の情報の作成、書換え、消去等の作業をする入力者(以下「入力者」という。)、記録の確定※を実施する権限を有する確定者(以下「確定者」という。)は、情報の保存を行う前に情報が正しく入力されており、過失による書換え・消去及び混同がないことを確認する義務がある。

※記録の確定とは、入力者により入力された情報に対して、確定を実施する権限を有する確定者によって入力の完了が確認されることや、検査、測定機器による出力結果の取り込みが完了することをいう。

(a) 技術的対策

(ア) 入力者及び確定者の識別及び認証が可能で、また、入力者と確定者が異なる場合は、確定者の識別及び認証が可能であること。

(イ) 登録対象の記録が確定記録であるか未確定な記録であるかを区別する仕組みと、それに従って正確に登録を行う仕組みを実装すること

(ウ) 確定記録を登録する場合は、以下に示すいずれかの対策を行うこと。

・確定記録となったことを示すフラグをデータベース上で管理し、記録が確定された時点で適切にフラグを変更する仕組みを実装すること。この場合には、確定された記録の範囲が解るよう管理すること。かつ、その確定記録と結び付けられた入力者及び確定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時が必ず存在すること。

・記録が確定された時点で確定範囲を明確に記録するために、その確定記録を単位として PDF 等のファイル形式で保存する仕組みを実装すること。このファイル内には、入力者及び確定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時が必ず含まれること。また、これらの情報の信頼性を高めるために電子署名やタイムスタンプを施す仕組みが実装されていることが望ましい。

・その他、実装上の仕組みから上記の対策が困難である場合には、上記と同等以上の技術的対策を行うこと。

(エ) 確定時に記録される入力者及び確定者の氏名等の識別情報は、確定者をシステム利用者が単純に入力または申告するような手順で得られる信頼の低い識別情報は使用せず、確定処理の過程で本ガイドライン「5.14.1. 利用者の識別・認証」で示す認証を行うことによって得られた信頼ある識別情報に基づいて作成される仕組みを実装すること。

(オ) 記録の確定は、確定を実施できる権限を持った確定者が実施できるような仕組みを実装すること。一定期間後の自動確定するような仕組みを提供するときには記録が確定されていることがわかる必要があるため。確定記録の PDF 化や、データベース上のフラグでの管理等が必要となる。

(カ) 記録の確定時は、内容を十分に確認が実施できるようが実施できるよう、確定対象の記録の内容を明

確に提示する仕組みを実装すること。

（キ）確定された記録を保持しているファイルや DB 等にシステム利用者が直接アクセスできない仕組みを構築することによって不正行為を防ぐか、それが困難な場合にはハッシュ関数を用いて生成した確定記録のハッシュ値を保存し、定期的にこのハッシュ値との比較を行うか、これと同等の手法によって不正行為の検知を行う仕組みを実装すること。不正が検知された場合には、本ガイドライン「5.5. システム設計の見直し（標準化対応、新規技術導入のための評価等）」、「5.12.2. バックアップの管理」を参考にリストア可能とすること。

（ク）IC カード方式、USB デバイス方式等による電子証明書による認証を行う場合は、信頼された CA が発行した証明書を用いて認証を行うこと。また、CRL を参照し、証明書の有効期限が切れていないか、または、失効していないかを確認すること。

（b）運用的対策

（ア）確定操作が何を意味するかについて医療機関等の責任者（または代行者）が利用者に確実に伝え、十分な確認を行わないうちに確定操作を行わないよう十分な説明を行うよう医療機関等に推奨すること。

（イ）システム障害の発生等により紙での運用等へ一時的に切り替える可能性がある場合には、確定記録の登録が行えなかった記録に対して、システム復旧後の登録手順を規則化しておくよう医療機関等に推奨すること

（ウ）一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用管理規程に明記するよう医療機関等に推奨すること

（エ）確定者が何らかの理由で確定操作ができない場合に備え、医療機関等の管理責任者が記録の確定を実施するなどのルールを運用管理規定に明記するよう医療機関等に推奨すること。

（オ）上記技術的対策と合わせて、確定操作が何を意味するかについて医療機関等の責任者（または代行者）が利用者に確実に伝え、十分な確認を行わないうちに確定操作を行わないよう十分な説明を行うよう医療機関等に推奨すること。

（カ）管理台帳等を用いてバックアップ媒体の保管先や媒体の耐久年次を管理するよう医療機関等に推奨すること。

（キ）確定記録がバックアップされる前に不正行為が行われた場合の原状回復方法や、不正行為が発覚するまでの間に不正行為が行われた確定記録に対して行われた追加及び訂正の確定記録の取扱い方法について規則化しておくよう医療機関等に推奨すること。

（ク）システムの入替を行う場合には、その前にバックアップを行うことで入替中および入替後に障害が発生しても入替前の状態に戻せるようにするよう医療機関等に推奨すること。

（ケ）電子証明書による認証を行う場合は、信頼された CA に証明書の発行を依頼し、失効させる場合はその情報を CRL へ登録すること。大規模病院等において、院内で認証局を運用する場合、CA 私有鍵の危殆化や、許可されない証明書発行の防止、私有鍵が本人以外の者に配布されない等の技術的対策や運用ルールを CP/CPS に定め、その通りの運用を実施するよう医療機関等に推奨すること。

（2）電子カルテシステムにおける記録の確定手順の確立と識別情報の記録 - 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。

－ 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合

a 運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。

b 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。

（a）技術的対策

（ア）記録の確定ルールの定義については、5.14.5 (1)の技術的対策を参照すること。

（イ）当該装置に対して、いつ記録が行なわれたかが分かるログを生成する仕組みを設けること。

（b）運用的対策

（ア）記録の確定ルールの定義については、5.14.5 (1)の運用的対策を参照すること。

（イ）当該装置に対して、紙などにより、システムで生成されるログと対応が取れる形式で、いつ・誰が記録を行ったかを残し管理するよう医療機関等に推奨すること。

（ウ）いつ・誰が記録を行ったかの履歴情報に対しては、定期的に管理責任者がチェックを行い、その結果を残すよう医療機関等に推奨すること。

（3）変更履歴の保存

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】

⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。

－ 一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。

－ 同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できるようにすること。

（a）技術的対策

（ア）更新時、それまでに確定し記録されている情報は変更せず、更新後の内容を別の記録単位として記録する機能を設けるか、及び／又は、更新前の情報と更新後の情報の差分を記録する機能を設けること。

（イ）更新後の内容を別の記録単位として記録する場合は、更新経過を表示し確認する機能を設けること。具体的には、変更前の記録を確認することができて、かつ、更新後に何処が変わったかが把握できる機能を設けることが望ましい。

（ウ）更新前の情報と更新後の情報の差分を記録する場合、例えば、更新前のデータを同時に表示する場合は更新前のデータに修正線を入れて更新後のデータと識別できる様にし、データを追加する場合は追加範囲を下線と更新日付で識別するような機能を設けること。

（エ）追記・書き換え・消去等の確定操作を行う際には、作成責任者の電子署名及び、信頼できる時刻源を用いたタイムスタンプを付けることが望ましい。

（オ）入力者が作成や追記・訂正・消去した内容について確定者が確定した旨の何らかの記録を残せる機能が必要である。

（b）運用的対策

（ア）確定操作にて電子署名を付ける場合は、必ず本人の証明書にて署名を行い、他者の証明書を用いることを禁止するよう医療機関等に推奨すること。

（4）代行プロシジャの定義、代行入力の記録

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。 － 代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。

代行入力とは、本来は自ら操作を行うべき情報システムの利用者（以下、「依頼者」と呼ぶ）が、何らかの理由によって、その操作を第三者（以下、「代行操作者」と呼ぶ）に依頼して行ってもらう操作のことをいう。このような状況には下記のようなケースが考えられる。

・依頼者が手術中等の理由で情報システムを操作できず、代行操作者に口頭等で直接指示を行うとき

・依頼者が医療現場におらず、代行操作者に電話等で指示を行うとき

・研修医等が主治医の指導の下に操作を行うとき

医療機関等において、代行操作が行われる際には、まずその基本方針および運用管理規程が明確に定まっていることが重要である。すなわち、「誰が」「誰を」「どういう場合に」行うことを認めるのか、そしてそれが「どのような手順で」行われるのかが周知徹底されており、情報システムがその規定に従って動作することが求められる。

医療機関等がその基本方針で代行入力を認める場合には、情報システムを利用したどういう手続き（以下、「代行プロシジャ」と呼ぶ）に対してそれを認めるのか、定義しなければならない。代行入力を行うためには、この代行プロシジャを定義する機能が、情報システムに実装されていることが望ましいが、必須ではなく、実装されてない場合は運用で担保すること。

代行が行われた場合には、必ずその事実が記録として残されなければならない。これは情報システムの機能として実装されることが望ましいが、必須ではなく、運用で担保することも可能である。

（a）技術的対策

（ア）情報システムは、ある利用者に実行権限が与えられた任意の操作について、その操作が第三者によって代行可能かどうか（以下、「代行ポリシ」と呼ぶ）を定義する機能を有していること。

（イ）情報システムは、代行可能と定義された操作を、どの利用者（代行入力者）が代行権限を持つか、定義する機能を有していること。ここで、代行入力者を定義する際の属性として、「特定の利用者名」、「職種」などが考えられる。

（ウ）情報システムは、権限のある代行入力者が代行入力を行う際には、「誰の」代行であるか（依頼者）を指定するための仕組みを備えていること。ここでいう「誰の」には、「主治医」等の特定の個人を識別できない属性や「医師」等の職種名等で行うのではなく、特定の依頼者を指定すること。

（エ）情報システムは、当該の操作が代行入力者によるものであることを認識したときには、下記を確認する機能を有していること。

・当該の操作が代行可能であること。

・代行入力者が当該の操作の代行を行う権限を有していること。

・代行を依頼した者が、その操作を行う権限を有していること。

（オ）情報システムは、代行入力者による操作を許可し、実際にその操作が行われた際には、その旨を記録する機能を有していること

（カ）記録には、「誰の指示によるものか」（依頼者）を示す情報が含まれること。

(b) 運用的対策

（ア）情報システムが上記技術的対策の（ア）～（カ）の機能のすべて、もしくは一部を実装していない場合には、医療機関等には、下記の運用をおこなわなければならないことを医療機関等に推奨すること。

・当該の情報システムにおいて提供されるすべての代行入力に対して、代行ポリシおよび運用管理規程を設定すること

・医師の事務作業補助者が、医師の指示の下で電子カルテに入力をすることも考えられる。このように、診療行為等の実施者でない者が、その者に代わって入力を行う場合は、代行入力に関する規定の策定と、その実施に関して記録を残さなければならない。

（イ）情報システムが、代行入力である旨を記録できないときは、その事実を他の方法（例えば記録簿など）に残すことで代用可能である。ただし、この場合には、情報システムが通常のアクセスログを収集する機能を備えていることが前提となる。

（5）代行入力の承認

＜安全管理ガイドライン（システム運用編）の要求事項＞

【遵守事項】
⑧ 電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。 － 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。

代行入力を行うにあたっては、承認操作が必要になる場合が想定され、医療機関等の基本方針として規定される必要がある。代行入力を行うにあたっての承認プロセスとして、現実には次のケースが考えられる。

① 事前承認 代行入力者が行う操作がシステム的に有効になる前に、依頼者の承認を必要とする場合

② 事後承認 代行入力者が行う操作は依頼者が承認を行う前に有効になるが、事後に依頼者の承認を必要とする場合

③ 承認不要 依頼者による承認を全く必要としない場合

実際の業務では、すべての代行プロシジャを、これらのうちのどれか一つに統一することは少ないと思われ、必然的に混在した形で行われると考えられる。情報システムの機能としては、任意の代行プロシジャに対し、どの承認プロセスを採用するのか、選択できることがベストであろうと考えられる。

ただ、すべての機能を実装することが困難な場合には、これらの承認プロセスの一部もしくは全部を運用で担保することも可能である。ここではすべてをシステムの機能として実装する場合を技術的対策として表し、それを実装しない場合の回避策を運用的対策で表すことにする。

(a) 技術的対策

（ア）医療情報システムは、代行可能とした任意の操作について、その承認プロセス（事前承認、事後承認、承認不要）を定義できること。

（イ）情報システムは、「事前承認」とされた代行入力が要求されると、その操作を有効にする前に依頼者に対して通知を行う。情報システムは、この通知を依頼者が確認するための仕組みを備えること。

（ウ）代行入力の事前承認を通知された依頼者は、内容を確認して承認操作を行う。情報システムは、この承認操作のための仕組みを備えること。

（エ）情報システムは、依頼者の承認操作が行われた時点で、要求された操作を有効にすること。

（オ）情報システムは、「事後承認」とされた代行入力が要求されると、その操作を有効にすると同時に、依頼者に対して通知を行う。情報システムは、この通知を依頼者が確認するための仕組みを備えること。

（カ）代行入力の事後承認を通知された依頼者は、内容を確認して承認操作を行う。情報システムは、この承認操作のための仕組みを備えること。

（b）運用的対策

（ア）情報システムが「事前承認」の機能を持たない場合は、下記の運用を行うよう医療機関等に推奨すること。

① 代行入力者は「事前承認」としたい操作を行う際に、その操作を行う前に何からの手段（口頭、メール、電話、書面等）で依頼者に操作の内容を確認する。

② この確認を行った記録をあらかじめ定めた方法によって、確認を行った記録を残しておく。

③ 代行入力者は当該の代行入力を実施する。

（イ）情報システムが「事後承認」の機能を持たない場合は、下記の運用を行うよう医療機関等に推奨すること。

① 代行入力者は「事後承認」としたい代行入力を、依頼者への確認をせずに（してもよいが）実行する

② 代行入力者は当該の操作を行った後、何からの手段（口頭、メール、電話、書面等）で依頼者に操作の内容を確認する。

③ この確認を行った記録は、何らかの方法で残しておく。

5.15. 電子署名、タイムスタンプ

5.15.1. 電子署名に用いる電子証明書について

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 法令で定められた記名・押印のための電子署名について、企画管理編「14. 法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。

安全管理ガイドライン(システム運用編)の要求事項では、安全管理ガイドライン(企画管理編)「14. 法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じることとされているため、本項を含めた本節では安全管理ガイドライン(企画管理編)「14. 法令で定められた記名・押印のための電子署名」の遵守事項に対応した技術的対策と運用的対策を示す。

＜安全管理ガイドライン(企画管理編)の要求事項＞

【遵守事項】

① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。

1. 以下の電子証明書を用いて電子署名を施すこと

(1) 「電子署名及び認証業務に関する法律」(平成 12 年法律第 102 号)第2条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。

(2) 法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)～(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いること。

(a) 厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす保健医療福祉分野 PKI 認証局の発行する電子証明書を用いて電子署名を施すこと。
保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野 PKI 認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。
ただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。

(b) 認定認証事業者(電子署名法第 2 条第 3 項に定める特定認証業務を行う者として主務大臣の認定を受けた者をいう。以下同じ。)又は認証事業者(電子署名法第 2 条第 2 項の認証業務を行う者(認定認証事業者を除く。)をいう。)の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者(認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14. 法令で定められた記名・押印のための電子署名」において同じ。を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること(ローカル署名のほか、リモート署

名、立会人型電子署名の場合も同様)。

・事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、オンラインの場合、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」第３条第１項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ(いずれも本項と同等の電子署名(資格確認を除く)を施すこと)により確認を行うこと。郵送の場合は、身分証明書のコピー(署名又は押印(実印が捺印され、印鑑登録証明書が添えてあること))、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用すること。

※身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか1種類により、又はその他の身分証明書であれば2種類以上により行うこと。

・事業者による利用者の医師等の国家資格保有の確認は、

①利用者が保健医療福祉分野 PKI 認証局の発行する署名用証明書を用いた電子署名を事業者へ提供することによりオンラインで行う方法

②利用者が官公庁の発行した国家資格を証明する書類(以下「国家資格免許証等」という。)の原本又はコピー等(紙媒体の場合は、国家資格免許証等のコピーに署名又は押印(実印が捺印され、印鑑登録証明書が添えてあること)があること。電子媒体の場合は、本項と同等の電子署名(資格確認を除く)をスキャンしたデータに施すこと。)を事業者へ持参、郵送又は送信する方法

③利用者が電子署名による確認方法以外の電子的に国家資格等情報と連携して提示できる仕組みを用いて事業者へ提示する方法

④利用者の所属又は運営する医療機関等が利用者の国家資格保有の事実の立証を事業者へ行う方法

のいずれかによって利用者の登録時において確認すること(電子署名を行う都度、事業者による医師等の国家資格保有の確認を求めるものではない)。なお、①～③の場合、事業者は、資格確認に用いた国家資格免許証等のコピーや証明書等について、保存年限を定めて保存しておくこと。④の場合、次に掲げる事項が適切に行われていることについて事業者が確認を行うこと。

－医療機関等の管理者が、自組織の実在性を事業者に対して立証すること。

－医療機関等の管理者が国家資格保有の確認を行った者の「氏名、生年月日、性別、住所」(以下「基本4情報」という。)を事業者へ提出すること(これによって、利用者が実在性、本人性及び利用者個人の申請意思を立証した際に、国家資格保有の立証もなされたものとみなすこととする。)。

－医療機関等による医師等の国家資格保有の立証に当たって、医療機関等が責任の主体としての説明責任を果たすため、資格確認を行った実施記録の作成を行うとともに、資格確認を実施した国家資格免許証等のコピーや利用者の基本4情報を提出した書類のコピー等について保存年限を定めて保存し、さらに医療機関等の内部の独立した監査部門による定期的な監査を行うこと。

・事業者が、上記の事項について、適切な外部からの評価を受けていること。

※①～④のいずれかによって資格確認を行った後、利用可能となった当該電子署名を利用者が他の事業者に提供した場合、提供を受けた事業者が別途資格の確認を行う必要はない。なお、この場合であっても以下の事項を行うこと。

・適切な外部からの評価を受けること。

・資格確認に用いた証明書等について、保存年限を定めて保存しておくこと。

(c)「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」平成 14 年法律第 153 号)に基づき、平成 16 年1月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること、当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証できることが必要である。

「電子署名法」や「e-文書法」(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(2005 年 4 月施行))の整備を受け、厚生労働省の「安全管理ガイドライン(第 1 版)」から記名・押印が義務づけられた医療関連文書等の電子保存が容認されることになった。また、電子署名済みの文書等は一定期間、信頼性を持って署名を検証できることが必要であるとされている。加えて、法令等によって保存、作成、交付等が定められている文書の場合は、有資格者等による正当な権限で作成された記録であり、虚偽入力、書換え、消去及び混同が防止され、かつ、第三者から見て作成の責任の所在が明確であることが求められている。

安全管理ガイドライン第 6.0 版では、電子署名を付与する際、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間などの一定の期間、電子署名の検証が継続できる必要がある事が明確に示されている。これを実現する手段として、ISO の長期署名プロファイルによる方法が例示され、標準技術を用いることの重要性について述べられている。また、リモート署名やクラウド技術を活用した立会人型電子署名についても記載があるが、締結する契約等の性質や、利用者間で必要とする本人確認レベルに応じて、適切なサービスを選択することが求められている。

(a) 技術的対策

(ア) 電子署名を施す場合には、電子署名法の要件を満たす必要があり、ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様であり、特に立会人型電子署名においては下記の Q&A を参照すること。

・総務省・法務省・経済産業省から令和 2 年 7 月 17 日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A(電子署名法 2 条 1 項に関する Q&A)」

・総務省・法務省・経済産業省から令和 2 年 9 月 4 日に示されている「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関する Q&A(電子署名法 3 条に関する Q&A)」

また、「主務三省 Q&A(電子署名法第 3 条関係)に関する解説」として、トラストサービス推進フォーラムと電子認証局会議の連名で下記 URL の解説書を公開しているので、参照されたい。

https://www.c-a-c.jp/download/cmsassets/denshishomei_qa_kaisetsu.pdf

(イ) 診療録等の電子保管においては、医師など一定の資格保有者が、その責任において文書に電子署名を施すことが、各種法令の遵守や証拠性の確保の観点から極めて重要な意味を持つ。医療関連文書等への電子署名を想定したときに、十分な厳密さで本人確認を行って発行される電子証明書を利用する必要がある。

(ウ) 診断書や処方箋など医師等の国家資格を持つ者が電子署名を行う必要がある場合には、下記の(1)～(3)のいずれかの電子証明書を利用して電子署名を行うとともに、医師等の国家資格の確認が電子的に検証できる必要がある。

(1)保健医療福祉分野 PKI(HealthcarePKI)の電子証明書

厚生労働省によって整備される保健医療福祉分野 PKI(HealthcarePKI、以下 HPKI と呼ぶ)によって定められた認証局証明書ポリシ(付録－2－1参照)に準拠した電子証明書で、HPKI で電子署名及び認証業務に関する法律(平成 12 年法律第 102 号)第 2 条第 1 項の要件を満たす署名が可能で、かつ医師等の国家資格が記述されており、検証する際に医師等の国家資格を同時に確認可能な電子署名を行うことができるため、HPKI の活用を推奨する。

HPKI の認証局証明書ポリシによれば、証明書発行対象者は以下の自然人となる。

「保健医療福祉分野 PKI 認証局　署名用証明書ポリシ　1.91 版」より

・保健医療福祉分野サービスの提供者及び利用者

・上記の提供者の内、以下の者がその有する資格において、あるいは管理者として署名を行う場合は、「その資格を有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。

・保健医療福祉分野に関わる国家資格を有する者

・医療機関等の管理者

また、証明書に国家資格(資格情報は、ISOIS17090 において定義される hcRole によって記述される。HPKI では X.509 電子証明書の標準拡張である subjectDirectoryAttribute の attrType 領域に、hcRole の属性値として資格情報を示す hcActor を記述する。hcActor の例としては、MedicalDoctor＝医師、Dentist＝歯科医師などが挙げられる。)を記載することが可能となっている。HPKI は、保健医療福祉分野において、電子署名に利用する証明書として厚生労働省の定める証明書ポリシにより標準化されている。

なお、JAHIS では、「安全管理ガイドライン」に示された電子署名、タイムスタンプを付与する際の具体的な実装技術を規定、解説した「ヘルスケア PKI を利用した医療文書に対する電子署名規格」を 2008 年 3 月に策定、公開し、その後、最新動向を踏まえ、2024 年 4 月に Ver.3.0(JAHIS 標準 24-001)として改定しているので併せて参照されたい。

(2)認定認証事業者の発行する電子証明書

電子署名法(電子署名及び認証業務に関する法律)に基づく特定認証業務の認証を受けた事業者(認定認証事業者)が発行する証明書を利用する際は、証明書や私有鍵の利用目的に反していないことを、該当する認証局の証明書ポリシ(CP)を参照の上、確認する必要がある。(認定認証事業者の中には、公的な電子調達等、特定のアプリケーションに特化した利用を目的として証明書を発行している場合があるため。)

なお、認定認証事業者は、法務省の以下の URL で確認できる。

https://www.moj.go.jp/MINJI/minji32.html

その他の要件については、企画管理編14.①1.(2)(b)を満たす必要がある。

ただし、企画管理編「16. 紙媒体等で作成した医療情報の電子化」において、スキャニング画像に付与する電子署名は、国家資格を証明する必要が無いため認定認証事業者の証明書、または同等の厳密さで本人確認を行なって発行される民間認証事業者の証明書の利用が可能である。なお、行政機関等で電子署名の検証を行える必要があるため、認定認証業務以外の証明書を用いる場は、「信頼されたルート証明機関」として OS 等に登録されたパブリックルート証明書と繋がる証明書を用いることが望ましい。

(3)公的個人認証サービスの電子証明書

公的個人認証サービスは、現時点では、行政機関や特定の法人・団体などに対してのみ電子証明

書の失効情報が提供されており一般の民間事業者などが電子証明書の検証を行う場合は、総務大臣認定を受けるか、または総務大臣認定を取得している事業者の検証サービスを利用する必要がある。

また、公的個人認証サービスが発行する証明書には、署名者の基本 4 情報(住所、氏名、生年月日、性別)が記されている。一般に署名文書には署名者の証明書が添付されるため、これら基本 4 情報が署名対象の文書と共に流通・保管されることとなる。この事は医師等の国家資格を有する署名者の個人情報が広く開示されることになり、過剰な負担となる場合が考えられる。従って、公的個人認証サービスが発行する証明書を利用する場合は、個人情報保護等の観点から、署名者の基本 4 情報の取扱いについて留意する必要があり、署名者に事前に充分に説明の上、同意を得る必要がある。

なお、電子署名を付した電子署名文書には、認証局や署名者の証明書が埋め込まれる場合が一般的であり、公的個人認証サービスが発行する証明書を利用して電子署名を付した場合は公的個人認証法の規定により総務大臣認定を取得している事業者以外の民間側の利用者に電子署名文書を公開することができないため留意が必要である。

その他の要件については、企画管理編14.①1.(2)(c)を満たす必要がある。

(b) 運用的対策

(ア) 電子署名を利用した業務の運用を行う際は、事前に上記(a)の要件を満たす認証局に対して、あらかじめ電子証明書発行を申請し、証明書及び対応する私有鍵を入手する必要がある。

(イ) 本人の私有鍵は、本人の意図しない利用を防止するために厳格に管理される必要がある。私有鍵を格納した IC カードや PC 等は本人以外の利用を防止する対策がなされるべきである。

5.15.2. タイムスタンプの付与について

<安全管理ガイドライン(企画管理編)の要求事項>

【遵守事項】

① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。

2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること

(1) タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者(認定事業者)が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者(タイムビジネスに係る指針等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者。以下「認定時刻認証事業者」という。)については、令和4年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。

(2) 法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。

(3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。

(a) 技術的対策

(ア) 電子署名がなされた文書にタイムスタンプを付与することで、その電子署名が行われた時刻(厳密には、当該署名文書が存在した時刻)を証明することができる。一方、電子署名だけでは署名時刻を特定できないため、署名に用いた証明書が失効もしくは期限切れ等の理由によって検証不能となったと

き、署名がなされた時点において当該証明書が有効であったかどうかを確認できない。そこでタイムスタンプを付与することで、そのタイムスタンプの有効期間内であれば、電子署名の有効性を常に確認することが可能となる。このように、電子署名とタイムスタンプは互いに機能を補完し合うことで、電子署名が付与された文書の証拠性(いつ・何を・誰が)を確実なものとすることができる。

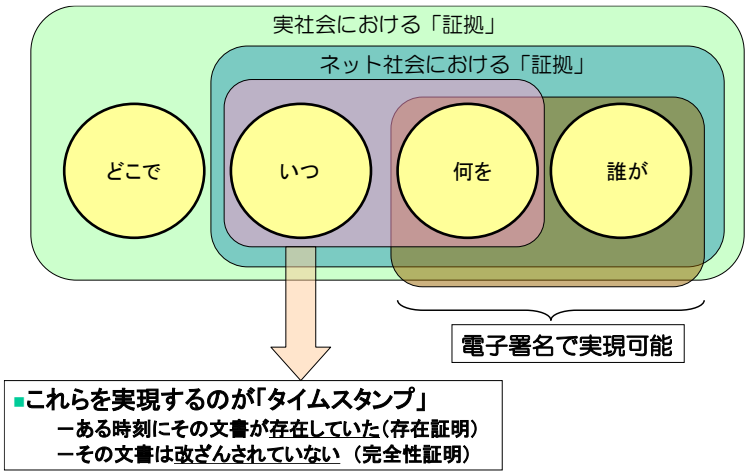


図 3.電子署名とタイムスタンプの機能補完

このとき、タイムスタンプを付与する対象として、

①電子署名を含む文書全体(文書＋署名値)

②文書全体に対してなされた電子署名の値

③文書のみ

の 3 種類が挙げられる。遵守事項では「電子署名を含む文書全体にタイムスタンプを付与すること」を定めており、①の方式は当該ガイドラインを満たす。さらに②についても、署名が文書から一意に生成されるハッシュ値に対して付与されたものであることから、同ガイドラインを満足すると考えられる。なお、③の方式は同ガイドラインを満足しない。

従って、タイムスタンプを付与する対象として、①電子署名を含む文書全体(文書＋署名値)または、②対象文書全体に対してなされた電子署名の値、のどちらかの方式を採用すること。なお、タイムスタンプについての詳細や動向については、関係府省の通知や指針等(後述)を参照されたい。

(1)時刻認証事業者と第三者によるタイムスタンプの検証

時刻認証業務の認定に関する規程(令和 3 年総務省告示第 146 号)で認定された時刻認証事業者は、本ガイドライン執筆時点において、以下の URL で公開されている。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

また、第三者がタイムスタンプを検証することが可能である必要があるので、タイムスタンプが付与された電子文書の受領者等の検証者がタイムスタンプを検証することが可能である必要がある。デジタル署名技術を用いたタイムスタンプを検証する際は、タイムスタンプ局(TSA)の電子証明書(TSA 証明書)が、検証者にとって信頼できるルート認証局の証明書リストに基づいて検証可能なものであることを確認する必要がある。また当該 TSA 証明書について、最新の失効情報(CRL)等に基づく失効検証を行う必要がある。なお、TSA 証明書がタイムスタンプトークンに含まれない場合は、信頼のおけるリポジトリからそれを取得する必要がある。

タイムスタンプ検証サービスを用いて検証者がタイムスタンプを検証する際は、セキュリティ対策(なりすまし、改ざん、盗聴)が行われた通信路上で、利用者とタイムスタンプ検証サービス間の検証プロトコルを実行することが望ましい。

(2)法定保存期間中のタイムスタンプの有効性維持

本ガイドラインの執筆時点では、一般財団法人日本データ通信協会が審査した時刻認証事業者のタイムスタンプの有効期間は概ね 10 年間が一般的である。電子保存を行う文書の法定保存期間がタイムスタンプの有効期間を越える場合、タイムスタンプが有効な間に、新たにタイムスタンプを付与する等の手段により、有効性を延長する必要がある。この処理を繰り返し行うことで、長期に渡ってタイムスタンプの有効性を継続させることが可能となる。この場合、新たなタイムスタンプの付与対象には旧いタイムスタンプを含む必要があることに留意されたい。

こうした技術は一般に、長期署名(Long-term electronic signatures)と呼ばれる。法定保存期間中(もしくはそれ以上の長期)においてタイムスタンプの有効性を継続し、電子署名の有効性を維持するためには、長期署名技術の利用が必要となる場合がある。(詳細は次の(3)を参照)

(3)関係府省の通知や指針

タイムスタンプの利用や長期保存に関する指針や標準の例として、「付録－2. 参考文献:2－2 タイムスタンプ及び長期保存に関する標準やガイドライン」に一覧を記載した。なお、実際にこれら標準・規格を参考とする場合は、その時点での最新版を用いることを推奨する。

(b) 運用的対策

(ア) 文書種別ごとの保存期間については、事前に医療機関等の定める文書管理規定等を確認し、最低限、法定保存期間を満たしていることを確認する必要がある。また、法定保存期間を越えて保存する場合は、必ずしもタイムスタンプの有効性を維持する必要は無いが、その有効性をどの期間まで維持するか、事前に医療機関等に確認し、再スタンプの必要性を明らかにすべきである。

5.15.3. 電子証明書の有効性について

<安全管理ガイドライン(企画管理編)の要求事項>

【遵守事項】
① 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。 2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること (4) タイムスタンプを付与する時点で有効な電子証明書を用いること。

(a) 技術的対策

(ア) 電子署名に用いる証明書は、署名時点において有効である必要があるが、タイムスタンプを付与する時点においても有効でなくてはならない。即ち、期限切れの証明書や失効された証明書を用いてはならない。また、法定保存期間中、署名検証を可能とさせるために、署名当時、証明書が有効で有ったことを後日に検証可能である必要がある。
法定保存期間中(もしくはそれ以上の長期)において有効な電子証明書を用いて電子署名を行ったことを検証可能とするためには、タイムスタンプ付与時点において電子署名が有効であったことを示すために、証明書検証に必要となる認証パス上の証明書や失効情報(CRL/ARL)などの情報について真正性を保って保存する必要がある。
このように署名文書の検証の継続性を確保して長期間保存するために、前述の長期署名技術の利用が有効である。長期署名では、署名値や証明書検証に必要な情報を付加し、タイムスタンプを付与したデータフォーマットを形成する。そのため、後日の検証時は長期署名フォーマット単独で第三者が署名検証可能であり、特定のシステムやサービスに依存することなく長期間署名の検証が維持可能と

なる。
下図は、長期署名の国際標準である「RFC3126」によって定められたフォーマットの概念図である。タイムスタンプの有効性が切れる前に次のタイムスタンプを繰り返し付与することで、署名の有効性を延長するアプローチをとっている。この中には、タイムスタンプ付与時点において証明書が有効であったことを示すために、当該時点における証明書検証に必要な各種情報が順番に記述されている。このように RFC3126 では、署名、タイムスタンプ及び検証のための各種情報が完全性を保ったまま構成されており、現時点において署名されたデータの長期保存を実現するための最も確立された技術の一つであるといえる。本ガイドラインでは、電子署名が付与された文書を保存する場合、このような長期署名の標準技術の採用を推奨する。
なお、長期署名の標準技術は、汎用的な署名ファイル形式である CMS をベースとした CAdES、XML 署名をベースとした XAdES(XMLAdvancedElectronicSignatures)、PDF ファイルを対象とした PAdES(PDFAdvancedElectronicSignatures)などがあり、署名対象文書種別や利用用途に応じて採用する長期署名形式を選択することが望ましい。また、署名システムを導入する際には、タイムスタンプの追加付与による署名延長処理や署名検証機能を持たせ、法定保存期間中は電子署名の検証を正しく行えるようにすることが必須となる。

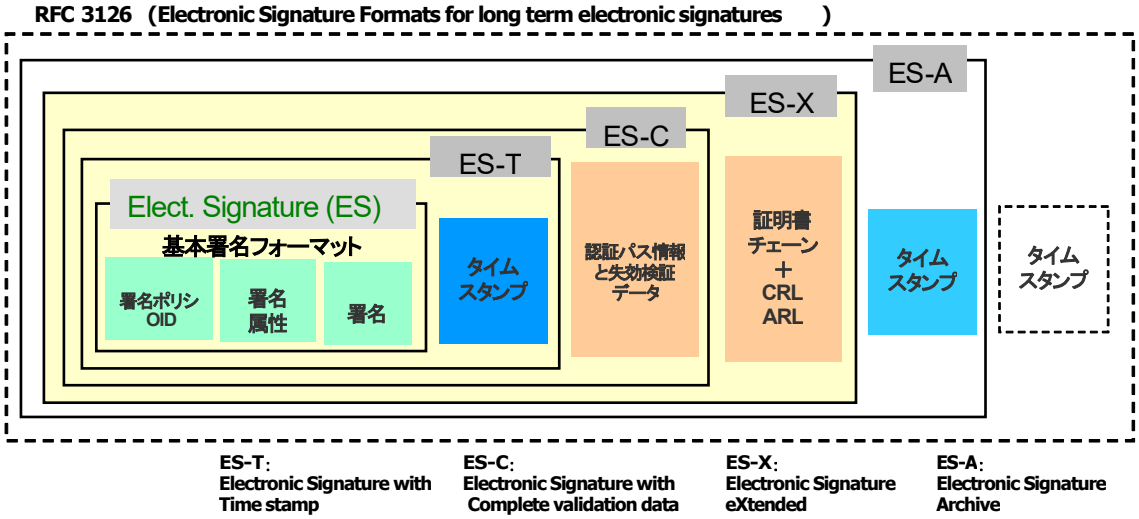


図 4.長期署名フォーマット

なお、長期署名技術についての詳細や動向については、「付録－2. 参考文献:2－2 タイムスタンプ及び長期保存に関する標準やガイドライン」を参照されたい。
また、上記のような長期署名技術を用いて電子署名、タイムスタンプを付与する場合、自ら保存義務がある文書については、ES-A フォーマットまで作成して保存する必要があるが、自らは保存義務がない外部提出用の文書については、ES-A フォーマットで渡すことが望ましいが、最低でも ES-T フォーマットまでは、署名者側の責任範囲として作成すべき点に留意されたい。

(b) 運用的対策

(ア) 有効期間が切れた証明書の利用を防止するため、認証局において証明書更新に関する本人への通知ルールが定められていることが望ましい。また、万一私有鍵を紛失した場合、速やかに認証局に証明

書の失効を申請しなくてはならない。

（イ）証明書の取り扱いや、更新、失効に関するルールを医療機関等が策定し、証明書所持者にその運用が徹底されるよう支援することが望ましい。

5.15.4. 鍵の管理に関する安全対策について

＜安全管理ガイドライン（企画管理編）の要求事項＞

【遵守事項】
② 電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。

経路の暗号化や、電子署名・電子認証によるなりすましの防止や情報の改ざん防止を図る場合には、暗号／復号、デジタル署名に用いる鍵（特に共通鍵や、秘密鍵）の管理を適切に行うことが重要である。

鍵管理に求められる具体的な対応は、暗号鍵の利用目的に応じて異なるが、電子署名や電子証明書を利用した本人認証などで使われる必要な秘密鍵では、電子証明書の認証を行う認証局が定める「証明書ポリシー」（Certificate Policy、以下 CP）に従って、管理することが求められる。

また、共通鍵や暗号鍵を格納する機器や媒体についても、一定の安全性が求められる。機器等の安全性を担保するためには、米国連邦標準規格である FIPS140-2（Federal Information Processing Standardization 140-2）の最低限のレベルである Level1 で求められる要件「製品レベルのコンポーネントの基本要件を満たす物理的セキュリティメカニズムが存在すればよい」を具備することが望ましい。

（a）技術的対策

（ア）共通鍵や暗号鍵を格納する機器や媒体について、安全性を担保するため FIPS140-2 の Level1 で求められる要件である、製品レベルのコンポーネントの基本要件を満たす物理的セキュリティメカニズムを有することが望ましい。

（b）運用的対策

（ア）利用する鍵ごとに、鍵の利用目的（署名用、利用者証明用など）を明確にすること。

（イ）鍵の利用目的を医療機関に提示し、鍵の利用目的に応じた重要性を鑑みたうえで、それぞれの鍵の管理を適切に行うよう医療機関等に推奨すること。

（ウ）電子署名や電子証明書を利用した本人認証などでは、電子証明書の認証を行う認証局が定める CP に従って秘密鍵を管理するよう医療機関等に推奨すること。

5.16. 紙媒体等で作成した医療情報の電子化

5.16.1. はじめに

2005 年 4 月に施行された e-文書法により、書面での保存が義務付けられた文書を電子保存することが容認され、厚生労働省所管の文書について「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 3 月 25 日 厚生労働省令第 44 号。以下「e-文書法省令」という）、及び、平成 17 年 3 月 31 日の「施行通知」にてスキャナによる電子化やその範囲が示され、さらに安全管理ガイドライン第 5.2 版 9 章で具体的な方法が規定された。その状況は、安全管理ガイドライン第 6.0 版においても踏襲されている。従って、安全管理ガイドラインの要件を満たして、スキャナによる電子保存を行なう場合は、同ガイドライン企画管理編「1.1.2 医療情報システムに関係する法令」の「表1－3 電磁的記録の保存、作成及び交付等を行うことができる文書」で示された法令での保存義務を満たすことができるので、スキャニング画像を原本として取り扱うことが可能となり紙での保存義務は無くなる。

ただし、スキャン後に紙を廃棄する場合は係争時などにおいて電子保存されたスキャン画像の証拠性を問われた場合の対応も想定しておく必要がある。スキャン画像には安全管理ガイドライン第 6.0 版の企画管理編 14 章、システム運用編 15 章に示された方法で電子署名とタイムスタンプを用いて長期署名を行う必要があるが、電子署名の有効性検証を行うことでスキャン画像の真正性を立証できるよう署名検証結果の提出なども考慮しておくことが重要となる。

「安全管理ガイドライン」と本ガイドラインとの対応する章節は以下の通りである。

安全管理ガイドライン		本ガイドライン
企画管理編	システム運用編	
16. 紙媒体等で作成した医療情報の電子化	16. 紙媒体等で作成した医療情報の電子化	5.16 紙媒体等で作成した医療情報の電子化
16.1 診療録等をスキャナ等により電子化して保存する場合の共通要件	16.1 保存義務がある書面等に関する紙媒体等の電子化における技術的な対応	5.16.1 診療録等をスキャナ等により電子化して保存する場合の共通要件
16.2 診療等の都度スキャナ等により電子化して保存する場合	—	5.16.2 診療等の都度スキャナ等により電子化して保存する場合
16.3 過去に蓄積された紙媒体等をスキャナ等により電子化して保存する場合	—	5.16.3 過去に蓄積された紙媒体等をスキャナ等により電子化して保存する場合
16.4 紙の調剤済み処方箋をスキャナ等により電子化して保存する場合	—	5.16.4 紙の調剤済み処方箋をスキャナ等により電子化して保存する場合
16.5 運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合	16.2 運用の利便性のためにスキャナ等で電子化を行う場合における技術的な対応	5.16.5 運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合

5.16.2. 診療録等をスキャナ等により電子化して保存する場合の共通要件

(1) スキャンによる情報量の低下、情報の欠落防止の手段

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
項目なし	① 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。

(a) 技術的対策

（ア）スキャンによる情報量の低下を防止するため、スキャンの精度は(放射線フィルム等の特に高精細な画像が求められるもの以外)、医療に関する業務等に差し支えない程度とする。

（イ）放射線フィルム等の特に高精細な画像が求められるものについては、日本医学放射線学会の「デジタル画像の取り扱いに関するガイドライン 3.0 版」に記載されている以下の精度でスキャンを行うこと。

①サンプリングピッチ:200μm 以下

②空間分解能:CTF(0.25)≧0.9、CTF(0.5)≧0.8、CTF(1.0)≧0.7

ここで CFT(n)は、n lp/㎜の Contrast Transfer Function を示す。

③濃度階調数:1024 以上(10 ビットグレイスケール以上)

④デジタイズ濃度範囲:0.0D－3.0D 以上

（ウ）スキャンした画像を非可逆圧縮する際は、画像再現時の画質劣化を医療の業務等に支障がない精度にすること。放射線フィルム等については日本医学放射線学会の「デジタル画像の取り扱いに関するガイドライン 3.0 版」で、JPEG 非可逆圧縮の圧縮率 1/10 までは非圧縮画像と臨床上同等としている。

（エ）スキャンした画像は 5 年以上の長期に渡って保存する事が想定されるので、保存の形式は公開され広く活用されているフォーマットを選択することが必要であり、可視化するソフトウェアに困らないものとする。

(b) 運用的対策

追記事項なし。

(2) 改ざんの防止(スキャンされた画像の真正性担保の手段)

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
① 紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規程等に定めること。 ② スキャナにより読み取った電子情報と元の文書等から得られる情報と同等であることを担保する情報作成管理者を配置すること。 ③ 紙媒体で作成した医療情報を含む文書等をスキャナにより電子化する場合、ス	項目なし

キャナによる読み取りに係る責任を明確にするため、作業責任者(実施者又は情報作成管理者)が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規程等に定めること。なお、電子署名については「14. 法令で定められた記名・押印のための電子署名」を参照すること。	

(a) 技術的対策

スキャンされた画像を長期に渡って保存するにあたり、スキャニング作業の責任の所在の明確化や、データの改ざん防止や原本性確保を行うため、以下の機能を有する必要がある。

(ア) 真正性検証機能

スキャン作業の責任の明確化や、スキャン画像の改ざんを防止、改ざんの有無の検証のため作業責任者の電子署名を付与する機能を持つこと。
また、電子署名の検証機能を持つこと。
なお、スキャン画像に対する、電子署名の付与やその検証に関しての詳細は「5.15 電子署名、タイムスタンプ」を参照されたい。

(b) 運用的対策

(ア) 医療機関等ではスキャン対象となる文書の作成(あるいは患者からの入手)からスキャンの実施、スキャン対象文書の保存(あるいは破棄)までの一連の運用について、スキャナによる読みとり作業が適正な手続きで確実に実施されるよう、運用管理規程を定め、情報作成管理者を配置する必要がある。システムベンダは作業責任者への電子証明書の発行や更新、日々の電子署名の付与や検証に関係する運用上の必要事項が明確になるよう医療機関等に情報提供を行い、医療機関等による運用管理規程の作成を支援する必要がある。

(3) スキャナによる読み取りに係る運用管理規程の遵守

<安全管理ガイドラインの遵守事項>

企画管理編	システム運用編
④ 情報作成管理者に対して、スキャナによる読み取り作業が運用管理規程に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) スキャナによる読取作業については、読み込み書類の準備、作業単位に合わせたバッチ化、スキャンし易くするための複写、スキャニングプロセスの詳細手順化、品質管理、スキャナ性能検査、再スキャニングやイメージ処理などに関しては必要に応じて ISO 国際標準[1]、JIS[2]や日本文書情報マネジメント協会 JIIMA のガイドライン[3]などを参考にすると良い。

[1] ISO/TR 15801「ドキュメント管理―電子的に保存された情報―信頼性と信頼性に関する推奨事項」
[2] JIS Z 6016「紙文書及びマイクロフィルム文書の電子化プロセス」
[3] 日本文書情報マネジメント協会(JIIMA)の「電子取引 取引情報保存ガイドライン」
(https://www.jiima.or.jp/activity/policy/#guideline)

5.16.3. 診療等の都度スキャナ等により電子化して保存する場合

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
⑤ 診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うことを運用管理規程等に定めること。	項目なし

（1）改ざん防止のための情報作成後の迅速なスキャン

（a）技術的対策

（ア）スキャンの対象となる診療録等の日々の発生枚数を見積もり、日常の業務でスキャンが延滞無く行われるよう、スキャナ装置の読みとり速度やスキャナの設置台数などをシステム導入時に検討しておくこと。

（イ）スキャナ装置のハードウェアトラブルに際しても延滞なくスキャンが行えるよう、予備機を用意しておくこと。

（b）運用的対策

（ア）診療録等の書類作成からスキャンまで遅滞なく完了するように運用を検討すること。ここでの「遅滞なく」とは１日を目処とするよう医療機関等に推奨すること。

5.16.4. 過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
⑥ 過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。 ・対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。 ・必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。 －運用管理規程の作成と妥当性の評価方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を確保した委員会等で行うこと（倫理委員会を用いることも可）） －作業責任者 －患者等への周知の手段と異議の申立てに対する対応方法 －相互監視を含む実施体制 －実施記録の作成と記録項目（次項の監査に耐え得る記録を作成すること） －事後の監査人と監査項目 －スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法 ・事後の監査は、システム監査技術者や Certified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ外部監査人によって実施すること。	項目なし

（a）技術的対策

追記事項なし。

（b）運用的対策

追記事項なし。

【コラム】

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必要がある場合の例として、以下の事例に関して、複数の問い合わせが寄せられたため、Q&A の形で対応方法を示します。

Q:＜想定事例＞

・従来から紙をスキャンして電子保存していたが、紙は保存していたため電子署名は付与していなかった。

・その後、電子署名を導入したが、過去にスキャンした画像ファイルに電子署名を新たに付与することにより、保存義務を満たすことができるか？（紙を捨てられるか？）

A:認められない。

安全管理ガイドライン第 6.0 版　企画管理編「16.1 診療録等をスキャナ等により電子化して保存する場合の共通要件」を満たしていない以上、スキャニング画像の管理状況にかかわらず原本は紙文書のままであると考えられる。従って、過去に蓄積された紙原本を電子保存することになるため、同ガイドライン「16.3 過去に蓄積された紙媒体等をスキャナ等により電子化して保存する場合」に従って再度、紙原本をスキャンするか、又は、紙原本を継続して保存する必要がある。

5.16.5. 紙の調剤済み処方箋をスキャナ等で電子化して保存する場合

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
⑦ 企画管理者は、紙の調剤済み処方箋をスキャナ等で電子化して保存する場合、以下の措置を講じること。 ・紙の調剤済み処方箋の電子化のタイミングに応じて、⑤又は⑥の措置を講じること。 ・「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。	項目なし

（1）電子化した調剤済み処方箋の修正

（a）技術的対策

（ア）元の調剤済み処方箋を書面上で修正し再スキャンを行う場合
調剤済み処方箋のスキャン後、元の紙を電子原本のバックアップ等の理由により適切に管理された状態で一定期間保存されている場合は元の調剤済み処方箋を書面上で修正し、再スキャンして保存することができる。安全管理ガイドライン第 6.0 版　企画運用編 16 章に従い作業責任者の電子署名が付与して電子保存するが、修正前の画像データは削除せずに修正後の画像データと紐付けて管理することにより修正履歴を残す必要がある。

（イ）スキャン画像データを印刷し書面上で修正の後、再スキャンを行う場合
この運用は認められていない。「「医療情報システムの安全管理に関するガイドライン 第 6.0 版」に関するQ&A」には「調剤済み処方箋をスキャナ等により電子化し、電子化した情報を原本とした後に修正を行う場合、真正性の確保の観点から、過去の電子署名の検証が可能な状態を維持する真正性の確保の観点から、過去の電子署名の検証が可能な状態を維持する形で電子的に修正し、薬剤師の電子署名を付す必要があります。そのため、プリントアウトしたものに訂正を行い、再度スキャナ等により電子化して保存することは、真正性の確保の観点から適切ではないと考えます。」と解説されている。

（ウ）スキャン画像データを電子的に修正する場合
スキャン画像データを修正した後に薬剤師の電子署名とタイムスタンプを付与して電子保存する。修正前の画像データは削除せずに修正後の画像データと紐付けて管理することにより修正履歴を残す必要がある。

（エ）スキャン画像データに修正コメントを付加する場合
スキャン画像データに対する修正コメントを作成した後に薬剤師の電子署名とタイムスタンプを付与して電子保存する。修正前の画像データは削除せずに修正コメントと紐付けて管理することにより修正履歴を残す。

なお、上記(ア)～(エ)において、修正前の画像データや修正後のデータに付与された電子署名とタイムスタンプは運用規定で定めた保存期間を通じて検証できる必要があることに変わりはない。

（b）運用的対策

（ア）医療機関等は調剤済み処方箋のスキャン運用管理規程を作成し、上記の場合に従って修正方法を明記しておく必要があるので、システムベンダは自社システムがサポートしている修正方法を医療機関

等に明示すること。なお、一旦修正が発生した場合は、最新の修正版が原本となる。従って、特に上記（ウ）に従ってスキャン画像データを電子的に修正した場合それ以降の修正は、例え元の調剤済み処方箋の紙がまだ残っていたとしても、修正した画像データを元にして修正する必要があることに留意されたい。

5.16.6. 運用の利便性のためにスキャナ等により電子化を行うが、紙等の媒体もそのまま保存を行う場合

＜安全管理ガイドラインの遵守事項＞

企画管理編	システム運用編
⑧ 企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。 ・情報作成管理者が、スキャナによる読み取り作業が適正な手続で確実に実施される措置を講じる旨を運用管理規程等に定めること。 ・電子化した後、元の紙媒体やフィルムの安全管理を行うこと。	② 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、緊急に閲覧が必要になったときに迅速に対応できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。

（a）技術的対策

追記事項なし。

（b）運用的対策

追記事項なし。

5.17. 証跡のレビュー・システム監査

5.17.1. 証跡のレビュー

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。

(a) 技術的対策

(ア) 不正アクセスやその予兆を検知できるよう、ログインの失敗や時間外、担当外のアクセスなどのアラートを発する仕組みを有することが望ましい。

(イ) 電子カルテシステムの入力端末以外の臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合は、当該装置に対して、いつ記録が行なわれたかが分かるログを生成する仕組みを設けること。

(ウ) システム利用者のアクセスを記録として有すること。さらに監査証跡(Audit Trail)を記録できることが望ましい。
監査証跡の標準規約としては「ヘルスケア分野における監査証跡のメッセージ標準規約 Ver.2.1」(JAHIS 標準 21-001)を参照のこと。また、MEDIS-DC から出されている、医療における監査証跡について平易にかつ具体的に解説している「個人情報保護に役立つ監査証跡ガイド」(https://www.medis.or.jp/7_kikaku/hanbai/file/DL_P200703.pdf)も参考のこと。

(b) 運用的対策

(ア) アクセスログの確認手順、真正性確保のための注意点などを医療機関等に提示すること。

(イ) 管理台帳等を用いて時刻源となっているサーバ等を明記しておくことを医療機関等に推奨すること。

(ウ) 院内時刻源となっているサーバを保守等で長期間停止させる場合は、代替の時刻源を用意すること。また、障害等で長期間停止した状態で放置されないよう定期的な稼動確認を行うよう医療機関等に推奨すること。

(エ) ネットワークに接続されず独立して記録を作成するシステムであっても、実際の時刻と大きな差が生じないよう定期的に点検を行うよう医療機関等に推奨すること。点検の時期及び方法を明記し、また点検したことを示す台帳等を作成することを推奨すること。

(オ) 電子カルテシステムの入力端末以外の臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合で、当該装置にいつ記録が行なわれたかが分かるログを生成する仕組みがないときは紙などにより、システムで生成されるログと対応が取れる形式で、いつ・誰が記録を行ったかを残し管理するよう医療機関等に推奨すること。

(カ) 紙などにより、システムで生成されるログと対応が取れる形式で、いつ・誰が記録を行ったかを残し管理する場合は、いつ・誰が記録を行ったかの履歴情報に対しては、定期的に管理責任者がチェックを行い、その結果を残すよう医療機関等に推奨すること。

(キ) 有する機能が監査証跡として不足の場合、運用による記録や確認方法を医療機関等に示すこと。

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
② アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。

(a) 技術的対策

（ア）アクセスログへのアクセス制御を行う仕組みを有すること。

（イ）アクセスログを制御できる管理者のアクセス記録を取得できる仕組みを有すること。

（ウ）アクセスログの改ざんや故意による削除などを防止するため、日または時間単位でのアクセスログに対するタイムスタンプを行うことが望ましい。

(b) 運用的対策

追記事項なし。

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
③ アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で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。

(a) 技術的対策

（ア）NTP 等を使用して基準となる時刻源と同期をとることが可能な仕組みを有すること。

（イ）時刻源となりうるサーバにおいては、院外の信頼ある時刻源と同期をとることが出来る仕組み、または、標準電波等を使用して自動的に調時を行う仕組みを有することが望ましい。

(b) 運用的対策

追記事項なし。

5.17.2. 監査の実施支援

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
④ 監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。

(a) 技術的対策

（ア）監査が円滑に実施できるようにアクセスログ内容を確認できる仕掛けを有することが望ましい。

(b) 運用的対策

（ア）監査に関連するシステム機能について、マニュアル等で提示すること。

（イ）業務運用に影響を及ぼすことなく、証跡の監査が実施できるように監査用のアカウント(医師、患者、管理者等)を準備しておくことを推奨すること。

5.18. 外部からの攻撃に対する安全管理措置

5.18.1. サイバーセキュリティ対応

＜安全管理ガイドライン(システム運用編)の要求事項＞

【遵守事項】
① 医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。 － 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断 － 他の情報機器への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離 － 他の情報機器への波及の調査等被害の確認のための業務システムの停止 － バックアップからの重要なファイルの復元(重要なファイルは数世代バックアップを複数の方式(追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等)で確保することが重要である)

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 最新のセキュリティパッチに関する情報を医療機関に適宜提供すること。

(イ) 自社製品を使用している医療機関で発生したインシデントに関して、同じ製品を使用している医療機関へ同じインシデント防止に有用な注意点などを適宜提供すること。

(ウ) システムの重要データのバックアップ方法および復元方法について、環境構築、操作手順等を医療機関等に提示すること。

(エ) システム導入時にシステムの重要データを復元する際に必要なリソースも含めて、提案を行うこと。

6. 総務省、経済産業省の「サービス提供事業者ガイドライン」に関する事項

6.1. はじめに

本章では、総務省、経済産業省の「サービス提供事業者ガイドライン」に関してシステムベンダの視点からJAHIS の基準を示し、情報処理システムに関する要求と思われる部分について、技術的な解説を行なったものである。

本章は 3 省のガイドラインにおける技術的要求事項の内、システムベンダがサービス事業者へシステムを提供する際に求められる技術的要求事項のみを対象としている。3 省のガイドラインの各要求事項はそれぞれのガイドラインが対象としている医療機関等、サービス事業者等を対応主体として記述されているが、本章ではそれぞれのガイドラインの対応主体がシステムベンダとなることを意識願いたい。また、本章ではサービス契約に係る要求事項などサービス事業者に求められる事項については範囲外としているので注意願いたい。

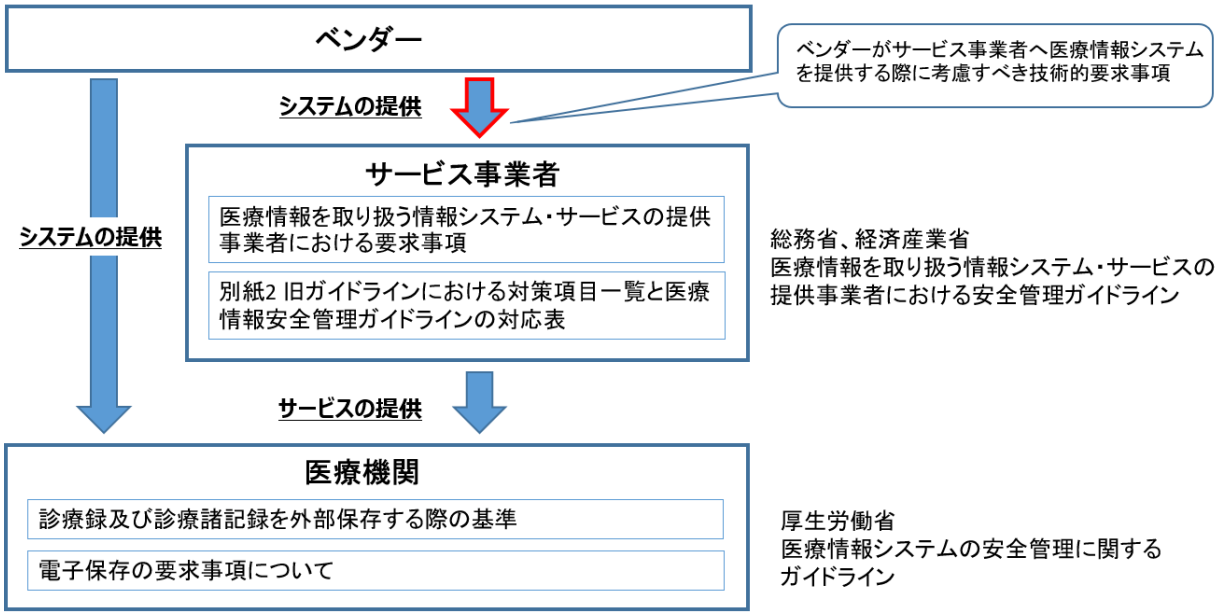


図 5.各ガイドラインとの関係

＜サービス提供事業者ガイドラインとの対比＞

サービス提供事業者ガイドライン	本ガイドライン
5. 安全管理のためのリスクマネジメントプロセス	6.2. 安全管理のためのリスクマネジメントプロセス
5.1. リスクマネジメントの実践	【システムベンダ側での対処事項なし】
5.1.1. リスク特定	6.2.1. リスク特定
5.1.2. リスク分析	6.2.2. リスク分析
5.1.3. リスク評価	【システムベンダ側での対処事項なし】
5.1.4. リスク対応の選択肢の選定	
5.1.5. リスク対応策の設計・評価	
5.1.6. リスクコミュニケーション	
5.1.7. 継続的なリスクマネジメントの実践	
5.2. リスクアセスメント及びリスク対応の実施例	
5.2.1. リスクアセスメント	
5.2.2. リスク対応	
6. 制度上の要求事項	6.3. 制度上の要求事項
6.1. 医療分野の制度が求める安全管理の要求事項	【システムベンダ側での対処事項なし】
6.2. 電子保存の要求事項	6.3.1. 電子保存の要求事項
6.3. 法令で定められた記名・押印を電子署名に代える場合の要求事項	6.3.2. 法令で定められた記名・押印を電子署名に代える場合の要求事項
6.4. 取扱いに注意を要する文書等の要求事項	【システムベンダ側での対処事項なし】
6.5. 外部保存の要求事項	

6.2.　安全管理のためのリスクマネジメントプロセス

6.2.1.　リスク特定

システムベンダは医療情報システム等を提供する際に想定されるリスクと、この対応策をとりまとめ、サービス事業者へ提示することが求められる。

具体的には提供する医療情報システム等の全体構成図やセキュリティ仕様を明らかにし、これに関わる情報及びリスクをサービス事業者が特定出来るよう、情報提供することが求められる。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) システムベンダは自らが提供する医療情報システム等の製品仕様(例えば、医療情報システムの構成図等)や、セキュリティ仕様を医療情報システム・サービス事業者に提示すること。

(イ) 本ガイドライン 5.4.1 節を参考に、医療情報システム等で扱う情報について情報の種別や重要度に応じて分類し、サービス事業者に提示できるようにしておくことが望ましい。

6.2.2.　リスク分析

サービス事業者による、リスクの影響度と顕在化の程度の算出にあたり、システムベンダは医療情報システム等の機能や想定される脅威に対してどの程度対抗できるかを提示することが求められる。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 本ガイドライン 5.4.2 節を参照のこと。

6.3.　制度上の要求事項

6.3.1.　電子保存の要求事項

医療分野において法令等で作成・保存が義務付けられた医療情報の安全管理に関して、システムベンダは自らが提供するシステムの法令、ガイドライン等への適合状況をサービス事業者に対して提示する必要がある。

法令等で作成・保存が義務付けられた医療情報の電子保存の要件として、真正性、見読性、保存性の確保が求められおり、システムベンダは自らが提供する医療情報システム等における電子保存に関する安全管理対策をサービス事業者に提示することが求められる。具体的な対応については、本ガイドライン 5.4、5.5、5.9、5.12、5.14、5.17 節を参照のこと。

6.3.2.　法令で定められた記名・押印を電子署名に代える場合の要求事項

本ガイドライン 5.15 節を参照のこと。

付録―1. リスクアセスメントの実施例

本付録の目的

情報システムに実装されるべきセキュリティ機能と、その運用において実施されるべき管理策の選択は、基本的にはリスクアセスメントを実施した結果から導出されるべきものである。これらがリスクアセスメントの結果に基づいていないと、セキュリティ対策に漏れ(セキュリティ・ホール)が発生したり、逆に過剰なセキュリティ対策によって運用上の可用性を損ねたり、対策費用が必要以上にかかったりする弊害が懸念される。

完全なリスクアセスメントを実施するためには、当該の情報システムの構成や機能、それを運用する組織の体制などがすべて正確に把握できている必要があるが、一度実施しておけば、運用の開始後に情報システムの変更が行われたとしても、その変更部分についてのみリスクアセスメントを実施することで整合性を保つことができる。

採用するリスクアセスメントの手法と手順は情報モデルに依存しないので、予め組織でこれを制定することが望ましい。これらを予め定めておくことにより、対象システムのリスクアセスメントを効果的、かつ効率的に行えるようになることが期待できる。

1―1 リスクアセスメントの手法

本付録で行うリスクアセスメントの手法は、

「一般財団法人日本情報経済社会推進協会(JIPDEC)」が発行している「ISMS ユーザーズガイド-JIS Q 27001:2014(ISO/IEC 27001:2013) 対応 -- リスクマネジメント編 - 」(https://contact.jipdec.or.jp/m?f=263)(以下「ISMS ガイド リスクマネジメント編」と記載)に記載された手法を参考とした。

1―2 情報セキュリティ基本方針

リスクアセスメントを行う際には、評価の拠り所として当該組織の情報セキュリティ基本方針が重要となる。これらは組織が独自に決める必要がある。ここでは、どのような医療機関等でも共通に有するような基本方針、例えば、「患者の個人情報とプライバシーの保護を重視する」や、「預託・管理している患者の診療情報の保護を重視する」といった観点を念頭に置いて考察した。

これらの基本方針は、識別されたリスクを評価する際に重要になる。

1―3 リスクアセスメントの実施例

上記の前提条件に従って、本付録では、表 A.1 のような訪問介護系の業務シナリオを例として、リスクアセスメントを部分的に実施した例を示す。なお、この実施例は「平成 21 年度地域見守り支援システム実証事業」の運用ガイドライン(暫定版)の中で記述したものを引用ならびに改訂している。

対象とする情報資産の抽出
下記のような業務シナリオのユースケースを想定する。

表 A.1 訪問介護系業務シナリオのユースケース

	項目	イベント	アクター	シナリオ
連携調整	1-1	提供記録確認	本人、家族 看護師 ケアマネ	訪問看護ステーションの看護師は、訪問介護系情報システムを使って、前日に訪問したホームヘルパーのサービス提供記録を確認している。
	1-2	状態確認	本人、家族 看護師 かかりつけ医	Ａさんが「最近は、あまり体調が良くない。食欲がない」と訴えていることを確認し、かかりつけ医と相談してＡさんの病気の状態を確認することにした。
サービス提供	2-1	状況		看護師がバイタルデータを測定したところ、血圧と血糖値が低下していることがわかった。Ａさんに、空腹感や身体のだるさがないかと確認したところ、「ある」との答えだったため、低血糖の症状が疑われた。
	2-2	報告・指示依頼	本人、家族 看護師 かかりつけ医	そのため、看護師が、携帯電話を使って、かかりつけ医にＡさんの症状とバイタルデータを伝え、指示を仰いだ。
	2-3	指示受け	本人、家族 看護師 かかりつけ医	かかりつけ医から「処方されているブドウ糖を飲ませるように。無ければ、砂糖水でも構わない」との指示があったために、Ａさんにブドウ糖の場所を聞き、飲めるように準備し、病状の変化を見守ることにした。
	2-4	結果記録	本人、家族 看護師 かかりつけ医 専門医	訪問看護師は、Ａさんのバイタルデータと症状、かかりつけ医からの指示などを看護記録に残し、訪問介護系情報システムを使って、かかりつけ医と中核病院の担当医からアクセスできるようにした。
課題対応	3-1	専門医に報告	本人、家族 かかりつけ医 専門医	後日、かかりつけ医が訪問診療し、テレビ電話を使って中核病院の専門医にバイタルデータと現在の病状を報告。
	3-2	精密検査	本人、家族 かかりつけ医 専門医	念のために、中核病院で精密検査することになった。

まず、この業務シナリオの表現から「情報資産」を登場する順に抽出する。業務モデルの解釈により多少の揺らぎは想定されるが、ここでは下記のように抽出した。

表 A.2 資産のリストアップ

資産番号	情報資産名	種別	所在
A1	訪問介護系情報システム	システム	データセンター
A2	サービス提供記録	電子情報	訪問介護系情報システム
A3	バイタルデータ測定機器	情報機器	訪問看護師が所持
A4	バイタルデータ	電子情報	訪問介護系情報システム
A5	携帯電話	情報機器	訪問看護師が所持
A6	看護記録(紙)	紙情報	訪問看護師が所持
A7	看護記録(電子)	電子情報	訪問介護系情報システム
A8	テレビ電話	情報機器	患者の自宅

リスクアセスメントは、すべての情報資産について個別に行うことが理想であるが、情報システムの規模が大きくなるにつれて、情報資産の数は飛躍的に増大するため、非常に多大な作業となってしまう。これを省力化するために、グループ分けという概念を導入する。情報の種別(形態)や重要度、管理場所等によって分類し、同じグループに属する情報資産には、同じリスクが存在すると考えるのである。

ここではサンプル的に上記を「種別」と「所在」という観点でグループ分けすると、下記のようになる。

表 A.3 グループ分けの例

Gr 番号	種別	所在	該当する情報資産
G1	システム	データセンター	A1
G2	電子情報	訪問介護系情報システム	A2 A4 A7
G3	情報機器	訪問看護師が所持	A3 A5
G4	紙情報	訪問看護師が所持	A6
G5	情報機器	患者の自宅	A8

実際のグループ分けは、上記の観点だけでは粗すぎる可能性があり、もっと細かな観点(例えば、個人情報を含むかどうか、現状施されている管理策の詳細な相違など)を加える必要があるかもしれないが、考え方としては同じである。

ここでのリスクアセスメントは、これらグループごとに実施した。

想定される脅威

上記で抽出したそれぞれの情報資産(のグループ)に対し、想定される脅威を考える。情報セキュリティでのリスクの観点は、機密性(C)、完全性(I)、可用性(A)の3つである。地域見守り支援のビジネスとしては、患者の安全性、システム運用の経済性等、より広い観点でのリスクも考えられるが、ここではこれらは対象としない。

ここで留意すべきことは、脅威の抽出の際に評価をしないということである。すなわち、その脅威の発現の頻度が低いからと言って、最初から除外しないということである。これはリスク分析を実施した担当者と、組織の経営陣のリスクに対する評価が異なる可能性があるからである。抽出の際に実施者によるフィルタリングがかかっていると、リスク分析が正確に行われない可能性がある。したがって、このようなフィルタリングの作業は後の「リスク評価」のところで行う。

脅威は、その情報資産の固有の管理状況に大きく依存するため、ここでは通常考えられる代表的なもののうち、ごく一部の抽出に留めた。実際に脅威を抽出する際には、それぞれの組織の実態に合わせて行う必要がある。

表 A.4 脅威のリストアップ

Gr 番号	脅威番号	観点	脅威の内容
G1	T1-I1	I	非作為的な事故により DB が壊れる
	T1-A1	A	通信回線の定期保守により利用できない
	T1-A2	A	利用者による負荷が集中しシステムの応答が遅くなる
G2	T2-C1	C	何者かに不正に閲覧される
	T2-I1	I	何者かによって内容が削除または改ざんされる
	T2-I2	I	利用者が操作を誤ってデータを消してしまう
	T2-A1	A	システムの定期保守によりアクセスできなくなる
G3	T3-C1	C	何者かに不正に操作される
	T3-I1	I	何らかの理由により正確な測定が行えない
	T3-A1	A	機器の扱い方がわからない
	T3-A2	A	紛失する
G4	T4-C1	C	何者かに不正に閲覧される
	T4-I1	I	物理的に破損して読めなくなる
	T4-A1	A	紛失する
G5	T5-I1	I	何らかの理由により通信ができない
	T5-A1	A	機器の扱い方がわからない

ここでは「何らかの理由により」とか「何者かによって」という表現を使った部分があるが、これをより具体的な表現とすることで、リスク分析の精度はより向上する。

ぜい弱性

次に、上記で抽出した、想定される脅威に関して、現在の管理策(想定)を踏まえたぜい弱性の一部を、下記のようにサンプル的に抽出した。

表 A.5 脅威に対するぜい弱性のリストアップ

脅威番号	ぜい弱性番号	ぜい弱性	現在の管理策
T1-I1	F1-I1-1	DB を保存する記憶媒体が通常運用で壊れうる	１日１回のバックアップ
	F1-I1-2	火災により焼失する	サーバ室の消火設備
T1-A1	F1-A1-1	通信回線が使えないとシステムにアクセスできない	計画保守スケジュールを利用者に周知
T1-A2	F1-A2-1	サーバの処理能力に限界がある	特になし
T2-C1	F2-C1-1	ぜい弱なパスワードを使用している	特になし(パスワードの設定ポリシを定めず、ユーザに委ねている)
T2-I1	F2-I1-1	共有アカウントが利用されている	特になし(共有アカウントに関する規制がない)
T2-I2	F2-I2-1	誤操作に対する警告機能がない	特になし
T2-A1	F2-A1-1	システムを定期的に停止しなければならない	計画保守スケジュールを利用者に周知
T3-C1	F3-C1-1	パスワードを設定できない	特になし
T3-I1	F3-I1-1	定期的な補正が必要	特になし
T3-A1	F3-A1-1	使い方が複雑	操作マニュアルを配布
T3-A2	F3-A2-1	小型軽量なので簡単に持ち運びができる	特になし
T4-C1	F4-C1-1	通常の書架に保管しているため誰でも閲覧できる	特になし
T4-I1	F4-I1-1	原本しかない	特になし
T4-A1	F4-A1-1	通常のバッグに入れて持ち歩いている	特になし
T5-I1	F5-I1-1	通信回線の定期メンテナンスがある	計画保守スケジュールを利用者に周知
T5-A1	F5-A1-1	お年寄りが使っている	操作マニュアルを配布

リスク値の計算

上記で情報資産およびそれぞれに関する脅威とぜい弱性が抽出できたので、次はこれらを定量的に評価することで、リスクの大きさ(実際に脅威が発顕する可能性)を計算する。

ここでは「ISMS ガイド リスクマネジメント編」での例示を基に評価を行う。基本的には結果のみを示すので、そこに至った考え方などの詳細については、同書を参考して自組織の現状に合わせる必要がある。

情報資産の価値

上記にリストアップした情報資産について、その価値を算定する場合には、資産の価値を評価するよりも、資産の機密性(C)、完全性(I)、可用性(A)が損なわれた場合の事業上の影響(損害)を評価するとした方が考えやすい。

この考えに沿って、「ISMS ガイド リスクマネジメント編」では、下記のような例が示されている。自組織に合ったものを選択してそのまま使ってもよいし、適宜修正して使ってもよい。

表 A.6 機密性の評価基準例

資産価値	クラス	説明
1	公開	内容が漏えいした場合でも、ビジネスへの影響はほとんどない
2	社外秘	内容が漏えいした場合、ビジネスへの影響は少ない
3	秘密	内容が漏えいした場合、ビジネスへの影響は大きい
4	極秘	内容が漏えいした場合、ビジネスへの影響は深刻かつ重大である

表 A.7 影響度の評価基準例

資産価値	影響度	金銭・機会損失(短期)	金銭・機会損失(中長期)	信用・ブランド損失
1	非常に小さい	当期経営にはほとんど影響はない	中長期的な経営には影響はない	ほとんど影響はない
2	小さい	当期経営に軽微な影響(当期利益の 1%以下)を及ぼす	中長期的な影響はない	弦された人に対して悪い風評が及ぶ
3	中程度	当期経営に影響(当期利益の 3%以下)を及ぼす	中長期的な経営にはほとんど影響はない	多くの人に対して悪い風評が及ぶ
4	大きい	当期経営に重大な影響(当期利益の 10%未満)を及ぼす	2 年程度の経営に影響が及ぶ	限定された人に長期的に悪いイメージが残る
5	非常に大きい	当期経営に極めて重大な影響(当期利益の 10%以上)を及ぼす	3 年以上の経営に影響が及ぶ	多くの人に対し長期的に悪いイメージが残る

*脅威*の評価

*脅威*の評価に関しては、単純な発生頻度によるもの、*脅威*の発生要因によるものが示されている。自組織に合ったものを選択してそのまま使ってもよいし、適宜修正して使ってもよい。

表 A.8 *脅威*の分類基準例(1)

脅威		
レベル	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回以上である。

表 A.9 脅威の分類基準例(2)

脅威			
レベル	意図的(計画的) 脅威	偶発的脅威	環境的脅威
1	実施による利益はない	通常では発生しない	3 年以内に一度も発生しない
2	実施による利益はあまりない	特定の状況下での発生が考えられる	3 年に一度程度発生する
3	実施による利益は多少ある	専門能力のあるものの不注意で発生する	1 年に一度程度発生する
4	実施による利益がある	一般者の不注意で発生する	1 ヶ月に一度程度発生する
5	発生が具体的に予想される	通常の状態で発生する	1 ヶ月に一度以上発生する

ぜい弱性の評価

ぜい弱性の評価は、その資産の持つ弱点がどの程度であるかを評価することになる。すなわち、現在実施されている対策を考慮して、ぜい弱性の評価を行うことになる。表現は脅威の場合と同様のものが示されている。

表 A.10 ぜい弱性の分類基準例(1)

ぜい弱性		
レベル	区分	説明
1	低い	現状の対策でほぼ完全に防御できる。
2	中程度	現在の対策で、かなりの場合防御可能であるが、万全とは言えない。
3	高い	現在の対策では、ほとんど防御できない。

表 A.11 ぜい弱性の分類基準例(2)

ぜい弱性			
レベル	意図的(計画的) 脅威 に対するぜい弱性	偶発的脅威 に対するぜい弱性	環境的脅威 に対するぜい弱性
1	最高程度の対策を実施済み	最高程度の対策を実施済み	最高程度の対策を実施済み
2	高度な専門知識や設備を持つ者によって可能な状況	通常の利用状況ではほとんどリスクが顕在化する恐れがない状況	通常の利用状況ではほとんどリスクが顕在化する恐れがない状況
3	専門能力を持つ者によって可能な状況	専門能力があるものの不注意によりリスクが顕在化する恐れがある状況	専門能力があるものの不注意によりリスクが顕在化する恐れがある状況
4	一般者が調査を実施すれば可能な状況	一般者の不注意によりリスクが顕在化する恐れがある状況	一般者の不注意によりリスクが顕在化する恐れがある状況
5	一般者が普通に実施可能な状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況	特段の対策を実施しておらず、いつリスクが顕在化してもおかしくない状況

ここでリストアップした資産(グループ)、脅威、ぜい弱性に対して、その環境を考慮して値を入れてみると下記

のようになった。なお、ここでは脅威およびぜい弱性の評価に、3 段階のもの(表 A.8、表 A.10)を利用した。どの評価尺度を使うかは、組織の実情を考慮して決めればよい。

表 A.12 資産、脅威、ぜい弱性の評価値

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値
G1	3	T1-I1	2	F1-I1-1	2
			2	F1-I1-2	2
		T1-A1	1	F1-A1-1	2
		T1-A2	2	F1-A2-1	2
G2	4	T2-C1	1	F2-C1-1	2
		T2-I1	1	F2-I1-1	1
		T2-I2	1	F2-I2-1	1
		T2-A1	1	F2-A1-1	1
G3	1	T3-C1	1	F3-C1-1	3
		T3-I1	1	F3-I1-1	1
		T3-A1	3	F3-A1-1	2
		T3-A2	1	F3-A2-1	2
G4	2	T4-C1	2	F4-C1-1	2
		T4-I1	2	F4-I1-1	2
		T4-A1	2	F4-A1-1	2
G5	1	T5-I1	1	F5-I1-1	1
		T5-A1	2	F5-A1-1	2

リスクの値は、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「ぜい弱性の度合い」を用いて、例えば、簡易的に次のような式で算出することができる。

リスクの値 ＝ 「資産の価値」×「脅威の大きさ」×「ぜい弱性の度合い」

この式を用いて、表 A.12 でリスク値を計算すると下記のようになった。

表 A.13 リスク値の計算結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	2	12
			2	F1-I1-2	2	12
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	2	12
G2	4	T2-C1	1	F2-C1-1	2	8
		T2-I1	1	F2-I1-1	1	4
		T2-I2	1	F2-I2-1	1	4
		T2-A1	1	F2-A1-1	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	2	8
		T4-I1	2	F4-I1-1	2	8
		T4-A1	2	F4-A1-1	2	8
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

リスクの評価

計算して得られたリスク値は表 A.13 のとおりである。これでそれぞれの資産に対するリスクの相対的な大きさがわかった。次はこのうちのどこまでが受容可能であるかを評価する。この結果、受容できないとなったリスクについては対策を施し、リスクを受容できるレベルにまで低減する必要がある。

この際、次のようなリスク受容の一覧表を作成すると考えやすい。

表 A.14 リスク受容一覧表

	脅威								
	1			2			3		
	ぜい弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	8	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

ここで、組織の実情に合わせて、受容範囲を決める。下記のような例を参考にして決めるとよい。

受容範囲決定方針の例

資産価値が最大のものは、脅威とぜい弱性がともに最低レベルより上のものは受容しない。すなわち、＜資産価値＞＜脅威＞＜ぜい弱性＞の組み合わせが、4×2×1または4×1×2となるものとする。したがって、リスク値8未満は受容する。

上記の受容範囲決定方針に従って、表 A.14 に受容範囲を表現すると下記のようになる。

表 A.15 リスク受容範囲の例

	脅威								
	1			2			3		
	ぜい弱性								
資産価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	8	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

（灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要）

この評価基準を用いて表 A.13 を評価すると下記のようになる。

表 A.16 リスク値の評価結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	2	12
			2	F1-I1-2	2	12
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	2	12
G2	4	T2-C1	1	F2-C1-1	2	8
		T2-I1	1	F2-I1-1	1	4
		T2-I2	1	F2-I2-1	1	4
		T2-A1	1	F2-A1-1	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	2	8
		T4-I1	2	F4-I1-1	2	8
		T4-A1	2	F4-A1-1	2	8
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

（灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要）

これによると、G1 の資産については完全性と可用性の観点での対策が、G2 については機密性観点での対策が、G4 については機密性・完全性・可用性すべての対策が必要であることがわかる。

管理策とリスクの再評価

リスク評価で管理策が必要となった情報資産には、何らかの対策を施して、脅威もしくはぜい弱性のレベルを

低減しなければならない。この対策のことを「管理策」と呼び、ISMS として知られる JIS Q 27001 および「安全管理ガイドライン」などで記述されているものが利用可能である。

一般的には、脅威のレベルを下げることは難しく、管理策はぜい弱性のレベルを下げることが主体となる。資産価値が大きく、かつ脅威のレベルが高いものについては、その資産自体を廃止する(「リスクの回避」という)といった対策を考慮せざるを得ないような場合も想定されるので、注意が必要である。

何らかの有効な管理策を採用することで、脅威またはぜい弱性のレベルが下がることがわかったら、その値を用いて再度リスクの評価を行う。これを「リスクの再評価」と呼ぶ。

表 A.16 で対策が必要となった資産のぜい弱性を下げる方策の例と、それによる効果を下記に示す。

表 A.17 リスク値の評価結果

Gr 番号	ぜい弱性番号	評価値	管理策	再評価値
G1	F1-I1-1	2	ディスク構成を RAID-6 に変更する	1
	F1-I1-2	2	バックアップを別の建屋に保管する	1
	F1-A2-1	2	高速なディスクに変更する	1
G2	F2-C1-1	2	パスワードの設定方針を定める	1
G4	F4-C1-1	2	鍵付きの書架に保管する	1
	F4-I1-1	2	物理コピーを毎日とる	1
	F4-A1-1	2	携行する際のルールを定める	1

上記の管理策を施すことで、表 A.16 は下記のようになり、全てのリスクが受容可能となったことがわかる。

表 A.18 リスク値の再評価結果

Gr 番号	評価値	脅威番号	評価値	ぜい弱性番号	評価値	リスク値
G1	3	T1-I1	2	F1-I1-1	1	6
			2	F1-I1-2	1	6
		T1-A1	1	F1-A1-1	2	6
		T1-A2	2	F1-A2-1	1	6
G2	4	T2-C1	1	F2-C1-1	1	4
		T2-I1	1	F2-I1-1	1	4
		T2-A1	1	F2-A1-1	1	4
			1	F2-A1-2	1	4
G3	1	T3-C1	1	F3-C1-1	3	3
		T3-I1	1	F3-I1-1	1	1
		T3-A1	3	F3-A1-1	2	6
		T3-A2	1	F3-A2-1	2	2
G4	2	T4-C1	2	F4-C1-1	1	4
		T4-I1	2	F4-I1-1	1	4
		T4-A1	2	F4-A1-1	1	4
G5	1	T5-I1	1	F5-I1-1	1	1
		T5-A1	2	F5-A1-1	2	4

(灰色の網掛け部分が受容可能、それ以外は何らかの対策が必要)

経営陣による残留リスクの承認

表 A.18 に示したように、新たな管理策を施すことで、すべてのリスクは受容可能なレベルに下がったことが確認できたが、リスクが全くなくなったわけではない。このように、対策を行ってもまだ残るリスクのことを「残留リスク」という。

残留リスクが具体的にどのようなリスクであるかを下記に示す。

表 A.19 残留リスクの具体的な内容の例

Gr 番号	脅威番号	ぜい弱性番号	リスク値	残留リスクの具体な内容
G1	T1-I1	F1-I1-1	6	RAID-6 構成でも復旧できないディスク障害が発生し、障害発生時点から前日バックアップ時点までのデータが失われる
		F1-I1-2	6	同上、およびサービス再開までの時間と費用が大きなものになる
	T1-A1	F1-A1-1	6	通信回線の復旧までに予想以上の時間がかかり、利用者への影響が大きくなる
	T1-A2	F1-A2-1	6	混雑時にシステムの応答が遅くなり、利用者への影響が出る
G2	T2-C1	F2-C1-1	4	設定方針の遵守をシステム機能でなく運用ルールで担保することで、ルールを遵守しない利用者のパスワードが破られて個人情報が漏えいする
	T2-I1	F2-I1-1	4	利用方針の遵守をシステム機能でなく運用ルールで担保することで、ルールを遵守しない利用者の操作が追跡できなくなる
	T2-I2	F2-I2-1	4	誤ってデータを消してしまった利用者から、操作性の悪さに関するクレームが寄せられる
	T2-A1	F2-A1-1	4	計画保守スケジュールの通知漏れにより、利用者からクレームが寄せられる
G3	T3-C1	F3-C1-1	3	紛失もしくは盗難にあった機器からシステムに不正アクセスされる
	T3-I1	F3-I1-1	1	機器の測定誤差により、不適切なバイタルデータをアップしてしまう
	T3-A1	F3-A1-1	6	機器の操作に不慣れな操作員に対する利用者からのクレームが寄せられる
	T3-A2	F3-A2-1	2	所定のサービスが行えず、利用者からのクレームが寄せられる、利用者の個人情報が漏えいする
G4	T4-C1	F4-C1-1	4	書類の置き忘れ、盗難等により利用者の個人情報が漏えいする
	T4-I1	F4-I1-1	4	所定のサービスが行えず、利用者からのクレームが寄せられる
	T4-A1	F4-A1-1	4	所定のサービスが行えず利用者からのクレームが寄せられる、または利用者の個人情報が漏えいする
G5	T5-I1	F5-I1-1	1	所定のサービスが行えず利用者からのクレームが寄せられる
	T5-A1	F5-A1-1	4	所定のサービスが行えず利用者からのクレームが寄せられる

これらの残留リスクは、リスクアセスメントの結果からは「発生頻度が十分に低い」もしくは「発生しても被害が小さい」等の理由で「受容可能」となったものであるが、内容を見る限りでは、必ずしも放置して良いものばかりと

は言えないはずである。

経営陣は、これらの残留リスクが存在することを容認できるかどうか、再度検討しなければならない。容認できないと結論した場合には、さらなる対策を行い、容認できるレベルにまで低減する必要がある。中には効果的な低減策が立案できないものもあるであろう。そういう場合には、損害を見越して保険をかける（リスクファイナンス）ことや、資産そのものの利用をやめる（リスクの回避）などの方策を講じることも検討する必要がある。

そして、いったん容認した後には、万一それらが発現した際の責任と対応を考えておく必要がある。

付録―2. 参考文献

2―1 ヘルスケア PKI 関連文書

ここで紹介する文書は本ガイドライン執筆時点の最新版である。実際にこれら標準・規格を参考とする場合は、その時点での最新版を用いることを推奨する。

- 厚生労働省:保健医療福祉分野 PKI 認証局 署名用証明書ポリシ 1.91 版(令和 5 年 12 月)
  https://www.mhlw.go.jp/content/10808000/001221669.pdf
- 厚生労働省:保健医療福祉分野 PKI 認証局 認証用(人)証明書ポリシ 1.81 版(令和 5 年 12 月)
  https://www.mhlw.go.jp/content/10808000/001221670.pdf
- 厚生労働省:保健医療福祉分野 PKI 認証局 認証用(組織)証明書ポリシ 1.1 版(平成 22 年 3 月)
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/pki-policy/2203_03.html
- ISO17090: Health Informatics Public Key Infrastructure
  Part1: Framework and overview
  (Health Care PKI の要件定義、アクセス制御のための属性証明書)
  Part2: Certificate profile
  (X.509 および RFC2459 に基づく証明書のプロファイル)
  Part3: Policy Management of Certification Authority
  (ポリシの規定)
  Part4: Digital Signatures for healthcare documents
  (デジタル署名)

2―2 タイムスタンプ及び長期保存に関する標準やガイドライン

(1) 総務省

- タイムスタンプについて
  時刻認証業務の認定に関する規程に関連した認定制度や関係情報が整理されている。
  https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html
  時刻認証業務の認定に関する規程 令和三年四月一日
  https://www.soumu.go.jp/main_content/000742664.pdf
  時刻認証業務の認定に関する実施要項(令和 3 年 11 月 8 日時点版)
  https://www.soumu.go.jp/main_content/000743330.pdf

(2) 電子商取引推進協議会(ECOM)

- 電子署名文書長期保存に関する中間報告(2001 年)
  長期署名の必要性、仕組み、フォーマット、タイムスタンプ等、電子署名文書の長期保存の基本的事項について記載されている。
  https://www.jipdec.or.jp/archives/publications/J0004116.pdf
- 電子文書の長期保存と見読性に関するガイドライン(2005 年)

長期保存のフォーマットだけでなく、電子文書のライフサイクルに関するモデル、保存媒体(メディア)の要件や運用上の留意点などについて広く記載されている。

https://www.jipdec.or.jp/archives/publications/J0004225.pdf

- ECOM 長期署名プロファイル

  CAdES や XAdES などの標準に基づく長期署名フォーマットを日本国内で普及定着させるべく、データ構造や処理手順の必要条件をまとめた「長期署名フォーマットのプロファイル」を策定している。同プロファイルは、CAdES や XAdES に基づく、実用的な長期署名のためのシンプルなものとなっている。

  CMS 長期署名プロファイル(CAdES)

  https://www.jipdec.or.jp/archives/publications/J0004022.pdf

  XAdES 長期署名プロファイル

  https://www.jipdec.or.jp/archives/publications/J0004024.pdf

- 長期署名フォーマットの相互運用性実験報告書

  ECOM で実施した実験プロジェクトの詳細な報告書。ECOM 長期署名プロファイルに基づいたテスト仕様、十数社の製品(一部プロトタイプを含む)の相互運用性テストの結果等を記載している。

  https://www.jipdec.or.jp/archives/publications/J0000406.pdf

(3) 日本 HL7 協会:CDA 文書電子署名規格(HL7J-CDA-002)

- CDA 文書に電子署名を付与する際に適用されるガイドライン。XML 文書に対する長期署名の標準である、XAdES を採用している。

  http://www.hl7.jp/intro/std/HL7J-CDA-002.pdf

(4) 長期署名に関する国際標準等

- EN 319 122-1: CAdES digital signatures; Part1: Building blocks and CAdES baseline signatures
- EN 319 122-2: CAdES digital signatures; Part2: Extended CAdES signatures

  ETSI によって定められた CMS 署名をベースとしたバイナリ形式のデジタル署名のためのフォーマットの欧州規格。
- EN 319 132-1: XAdES digital signatures; Part1: Building blocks and XAdES baseline signatures
- EN 319 132-2: XAdES digital signatures; Part2: Extended XAdES signatures

  ETSI によって定められた XML 形式のデジタル署名フォーマットの欧州規格。
- EN 319 142-1: PAdES digital signatures; Part1: Building blocks and PAdES baseline signatures
- EN 319 142-2: PAdES digital signatures; Part2: Additional PAdES signatures profiles

  ETSI によって定められた PDF 形式のデジタル署名フォーマットの欧州規格。
- TS 119 182-1: JAdES digital signatures; Part1: Building blocks and JAdES baseline signatures

  ETSI によって定められた JSON 形式のデジタル署名フォーマットの欧州規格。

- RFC 3126 Electronic Signature Formats for long term electronic signatures

CAdES を基に、RFC によって定められた長期署名のためのフォーマット。タイムスタンプを繰り返し付与することで、署名の有効性を延長するアプローチをとっている。
※現在は RFC5126 にアップデートされている。

- ISO 14533-1 Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part1: Long term signature profiles for CMS Advanced Electronic Signatures(CAdES)

  ETSI で定められた CAdES に基づく長期署名プロファイルを ISO として相互運用性に配慮し制定したもの。

- ISO 14533-2 Processes, data elements and documents in commerce, industry and administration — Long term signature — Part2: Profiles for XML Advanced Electronic Signatures(XAdES)

  ETSI で定められた XAdES に基づく長期署名プロファイルを ISO として相互運用性に配慮し制定したもの。

- ISO 14533-3 Processes, data elements and documents in commerce, industry and administration — Long term signature profiles — Part3: Long term signature profiles for PDF Advanced Electronic Signatures(PAdES)

  ETSI で定められた PAdES に基づく長期署名プロファイルを ISO として相互運用性に配慮し制定したもの。

(5) 長期署名に関する JIS 規格

- JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル
- JIS X 5093:2008 XML 署名利用電子署名(XAdES)の長期署名プロファイル

  前述の「ECOM 長期署名プロファイル」をベースとして ETSI の最新仕様との整合性を図り作成されたもの。CMS ファイル形式と XML ファイル形式による二つのフォーマット規格がある。

(6) JAHIS の電子署名規格

- ヘルスケア PKI を利用した医療文書に対する電子署名規格

  「安全管理ガイドライン」に示されている電子署名・タイムスタンプの要件を受け、JAHIS により具体的な技術規格を定めたもの。署名方式は CAdES(JIS X 5092、ISO 14533-1)および XAdES(JIS X 5093、ISO 14533-2)、PAdES(ISO 14533-3)、JAdES(ETSI/TS 119 182-1 V1.1.1、ただし参照標準としている)を採用し、署名用の証明書は厚生労働省の「保健医療福祉分野 PKI 認証局 署名用証明書ポリシ」に基づくものを前提としている。

(7) 日本ネットワークセキュリティ協議会(JNSA)

- デジタル署名検証ガイドライン

  公開鍵暗号技術に基づくデジタル署名(CAdES/XAdES/PAdES 等のいわゆる長期署名を含む)の検証方法について詳細に記したガイドライン。

  https://www.jnsa.org/result/e-signature/2021/index.html

付録―3. 要求項目／技術的対策／運用的対策の記述方針まとめ表

<table>
<tr><td rowspan="3">要件</td><td colspan="2" rowspan="3">JAHISの判断</td><td colspan="3">本ガイドラインの記載</td></tr>
<tr><td rowspan="2">安全管理GLの要求項目</td><td colspan="2">本ガイドラインの解説</td></tr>
<tr><td>技術的対策</td><td>運用的対策</td></tr>
<tr><td rowspan="6">C項
D項</td><td rowspan="3">技術的対策が必要</td><td rowspan="2">最低限
（必須）</td><td rowspan="2">再掲する</td><td>運用を伴わずに技術的対策だけで安全管理ガイドラインの要件を満たす</td><td>運用的対策を記載しないか、追加することで更に良い状態となることを示す。</td></tr>
<tr><td>技術的対策と運用的対策をあわせて安全管理ガイドラインの要件を満たす</td><td>必ず運用的対策を記載し、その運用を病院側に求める必要があることも記載する。</td></tr>
<tr><td>推奨</td><td>再掲する</td><td colspan="2">同上。（最低限）の欄と同じ</td></tr>
<tr><td rowspan="2">全て病院の運用またはサービス提供に関わること</td><td>システムベンダとして行うことが有る</td><td>再掲する</td><td>“追記事項なし”と記載する</td><td>システムベンダとして病院に対して行うことを記載する</td></tr>
<tr><td>システムベンダとして行うことが無い</td><td>要求項目を再掲し“【システムベンダ側での対処事項なし】”と記載する</td><td>“追記事項なし”と記載する</td><td>“追記事項なし”と記載する</td></tr>
</table>

付録―4. 作成者名簿

作成者（社名五十音順）

永野　友裕	ウィーメックス㈱	
武者　義則	ウィーメックスヘルスケアシステムズ㈱	
有馬　一閣	㈱NTTデータ	
木戸　須美子	キヤノンメディカルシステムズ㈱	
齋須　亨	キヤノンメディカルシステムズ㈱	
川名　雄太	キヤノンメディカルシステムズ㈱	
下野　兼揮	㈱グッドマン	
山本　智仁	セコム㈱	
藤井　友樹	㈱ソフトウェア・サービス	
近藤　誠	日本電気㈱	◎主査
龍田　岳一	富士フイルム㈱	
村田　公生	富士フイルム㈱	
梶山　孝治	富士フイルム㈱	
茗原　秀幸	三菱電機㈱	
深尾　卓司	三菱電機インフォメーションシステムズ㈱	

改定履歴		
日付	バージョン	内容
2007 年 5 月		初版
2009 年 10 月	第 2 版	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 2 版・第 3 版に対応
2011 年 4 月	第 3 版	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 4 版・第 4.1 版、総務省「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」、及び経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン」に対応
2013 年 4 月	第 3.1 版	総務省「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」第 1.1 版、及び経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン」第 2 版に対応
2015 年 7 月	第 3.2 版	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 4.2 版に対応 全体構成の見直しを実施
2017 年 12 月	Ver.3.3	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 5 版に対応
2022 年 6 月	Ver.4	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 5.2 版、総務省、経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」第 1 版に対応
2024 年 9 月	Ver.5	厚生労働省「医療情報システムの安全管理に関するガイドライン」第 6.0 版、総務省、経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」第 1.1 版に対応

（JAHIS標準 24-006）

2024 年 9 月発行

JAHIS保存が義務付けられた診療録等の電子保存ガイドライン Ver.5
厚生労働省「医療情報システムの安全管理に関するガイドライン第 6.0 版」対応

発行元 一般社団法人 保健医療福祉情報システム工業会
〒105－0004 東京都港区新橋2丁目5番5号
（新橋2丁目MTビル5階）

電話 03-3506-8010 FAX 03-3506-8070