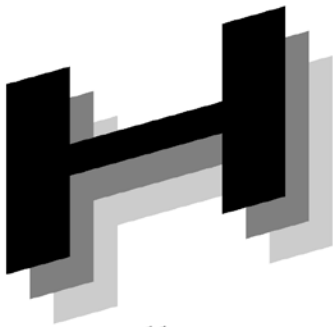




Japanese



Association of



Healthcare



Information



Systems Industry

J A H I S

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. 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」 対応

2017年12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. 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」対応

ま え が き

「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）ならびに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「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。「安全管理ガイドライン」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、個別のベンダー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かの分かりにくかった。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。

「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。

「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。以降「3省ガイドライン」と呼ぶ。）の内容を反映し、2011年4月に第3版として発行した。

上記の後、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。

上記の後、「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。

上記の後、「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及び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、上記の関係通知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。

2017年12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。

本ガイドラインならびに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	1
2.	概要	2
3.	主な用語	4
4.	適用範囲	6
4.1.	医療情報システムの安全管理に関するガイドラインとの関係	6
4.2.	本ガイドラインの対象システム及び対象情報	7
4.3.	総務省のガイドライン及び、経済産業省のガイドラインとの関係	7
4.4.	他の JAHIS 標準・技術文書との関係	7
4.5.	引用規格・引用文献	8
5.	ベンダーの責任のあり方	9
5.1.	医療機関等の責任とベンダーの提供する医療情報システムの関係	9
5.2.	ベンダーの責任	9
6.	情報システムの基本的な安全管理	10
6.1.	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	10
6.1.1.	ISMS 構築の手順	11
6.1.2.	取扱い情報の把握	12
6.1.3.	リスク分析	13
6.2.	技術的安全対策	14
6.3.	情報の破棄	26
6.4.	情報システムの改造と保守	28
6.5.	情報および情報機器の持ち出しについて	33
6.6.	災害、サイバー攻撃等の非常時の対応	35
6.7.	外部と個人情報を含む医療情報を交換する場合の安全管理	39
6.8.	法令で定められた記名・押印を電子署名で行うことについて	49
7.	電子保存の要求事項について	56
7.1.	真正性の確保について	57
7.1.1.	入力者及び確定者の識別及び認証	58
7.1.2.	記録の確定手順の確立と、識別情報の記録	61
7.1.3.	更新履歴の保存	64
7.1.4.	代行入力の承認機能	65
7.1.5.	機器・ソフトウェアの品質管理	68
7.2.	見読性の確保について	70
7.2.1.	情報の所在管理	71
7.2.2.	見読化手段の管理	71
7.2.3.	見読目的に応じた応答時間	72
7.2.4.	システム障害対策としての冗長性の確保	72
7.3.	保存性の確保について	74
7.3.1.	不適切な保管・取扱いによる情報の滅失、破壊の防止	75

7.3.2.	媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	77
8.	診療録及び診療諸記録を外部に保存する際の基準	79
8.1.	厚生労働省の医療情報システムの安全管理に関するガイドラインに関する事項	80
8.1.1.	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	81
8.1.2.	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見読性の確保	82
8.1.3.	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保存性の確保	83
8.2.	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に関する事項 85	
8.2.1.	情報資産管理	86
8.2.2.	技術的安全対策	87
8.3.	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 に関する事項	103
8.3.1.	真正性の確保におけるASP・SaaS事業者への要求事項	104
8.3.2.	外部保存におけるASP・SaaS事業者への要求事項	104
8.3.3.	ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項	105
9.	診療録等をスキャナ等により電子化して保存する場合について	106
9.1.	共通の要件	107
9.2.	診療等の都度スキャナ等で電子化して保存する場合	110
9.3.	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場合	111
9.4.	調剤済み処方せんをスキャナ等で電子化し保存する場合について	113
付録一	1. リスクアセスメントの実施例	115
1-1	リスクアセスメントの手法	115
1-2	情報セキュリティ基本方針	115
1-3	リスクアセスメントの実施例	115
付録一	2. 参考文献	128
2-1	ヘルスケアPKI関連文書	128
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	128
付録一	3. 要求項目／技術的対策／運用的対策の記述方針まとめ表	131
付録一	4. 作成者名簿	132

1. はじめに

2005年3月に、厚生労働省から「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」の電子保存に係るガイドラインとして「安全管理ガイドライン」（以下、「安全管理のガイドライン」と記載）が発行された。このガイドラインは、従来のガイドラインと比較して、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及するなど、細かな点にも踏み込んだ内容となっている。しかしながら、実際に医療施設にシステムを導入するベンダーの立場から見た場合、一部の内容についてはより具体的な基準を示す必要がある状況である。

このような状況に対し、本ガイドラインでは JAHIS の立場から、現在のセキュリティ技術水準を前提にネットワークによって外部と接続されたシステム環境のセキュリティ保護に関して、「安全管理のガイドライン」から「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」に関する要件を技術的な対策と運用的な対策に分けてより細かく示すこととした。その上で、「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も目的とした。

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をご留意頂きたい。

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ガイドラインについて、システムベンダー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。
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

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」にそろえる。但し、章番号はシフトすることがある。

(2) 章単位の対応表

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。

ア) 表形式のテンプレート（表記例）

＜安全管理ガイドラインとの章対応表＞

安全管理ガイドライン	本ガイドライン
3 章 本ガイドラインの対象システム及び対象情報	4. 2 本ガイドラインの対象システム及び対象情報
4 章 電子的な医療情報を扱う際の責任のあり方	5. ベンダーの責任のあり方

イ) 本ガイドラインで対象外と判断した章は、対応表で“【ベンダー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) 章、節、項目のタイトルは原則として「安全管理ガイドライン」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」の構成との対応に抜けや追加がある場合

② 「B. 考え方」に対して解説・補足が必要と考えられる場合

③ 「B. 考え方」と「C. 最低限のガイドライン」、[D. 推奨されるガイドライン]の結びつきがわかりにくい場合

ウ) 章の中での節単位の「安全管理ガイドライン」との対応表を、上記補足文章に続いて記載する。

① 表形式のテンプレート

＜厚生労働省：安全管理ガイドラインとの節対応表＞

安全管理ガイドライン	本ガイドライン
8.1 ○○・・・場合	8.1 ○○・・・場合
8.1.1 △△・・・の遵守	8.1.1 △△・・・の遵守
8.1.2 ▽▽・・・の遵守	8.1.2 ▽▽・・・の遵守
8.1.3 ◇◇・・・に関する基準	【ベンダー側での対処事項なし】

② 本ガイドラインで対象外と判断した節は、上記の対応表で“【ベンダー側での対処事項なし】”と記載し、以降の節の中では該当する小節を作らない。

エ) 章の中は、「安全管理ガイドライン」の示す要件毎に「C. 最低限のガイドライン」、「D. 推奨されるガイドライン」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

(n) ○○・・・対応

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. ○○・・・すること 2. ◇◇・・・すること 【ベンダー側での対処事項なし】	項目なし

② 「B. 考え方」が幾つかに分類されている場合に、「C. 最低限のガイドライン」、「D. 推奨されるガイドライン」も該当するものに分けて記載する。

③ 「B. 考え方」が分類されていなくても、「C. 最低限のガイドライン」、「D. 推奨されるガイドライン」を分類した方がわかりやすい場合に要件のみを分類して記載する。

④ 「最低限のガイドライン」と「推奨されるガイドライン」への区分けは、JAHIS 独自の判断によって変更するものも有る。

⑤ 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“【ベンダー側での対処事項なし】”と記載する

オ) 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

ベンダー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、もしく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
インシデント
改ざん : 情報の作成、変更、参照、削除などの記録。
: 情報セキュリティリスクが発現・現実化した事象。
: 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ならびに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。
- 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欠陥。または仕様上の問題点。
- システム提供者 : 医療情報システムを提供するシステムベンダー。
- 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
電子署名 : 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、その情報をもつ重要度、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
- 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。

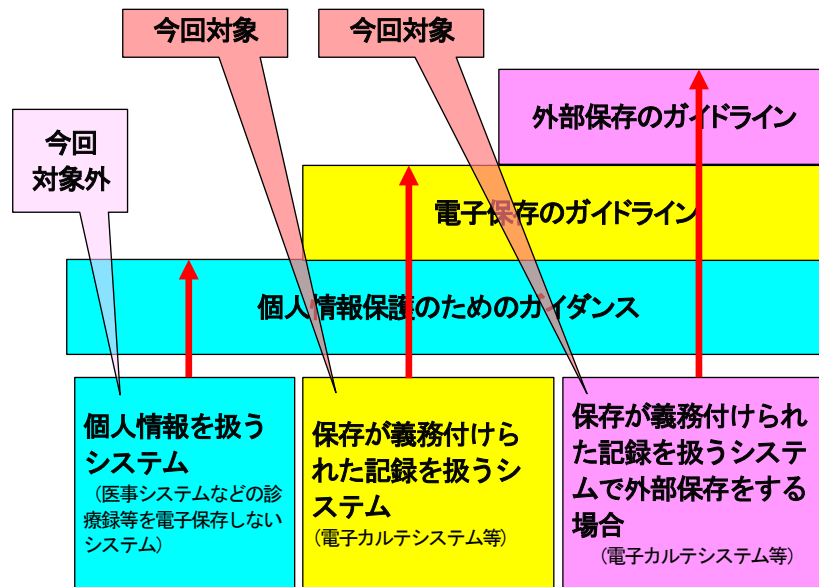
(記号および略語 このガイドラインでは、次の記号および略語・表記を用いる。)

- 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. 医療情報システムの安全管理に関する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（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、ベンダー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。



「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。（節については本ガイドラインの各章冒頭部の対応表を参照のこと。）

安全管理ガイドライン	本ガイドライン
3 本ガイドラインの対象システム及び対象情報	4 適用範囲 (4.1 医療情報システムの安全管理に関するガイドライン) (4.2 本ガイドラインの対象システム及び対象情報)
4 電子的な医療情報を扱う際の責任のあり方	5 ベンダーの責任のあり方
5 情報の相互運用性と標準化について	【ベンダー側での対処事項なし】
6 情報システムの基本的な安全管理	6 情報システムの基本的な安全管理
7 電子保存の要求事項について	7 電子保存の要求事項について
8 診療録及び診療諸記録を外部に保存する際の基準	8 診療録及び診療諸記録を外部に保存する際の基準
9 診療録等をスキャナ等により電子化して保存する場合について	9 診療録等をスキャナ等により電子化して保存する場合について
10 運用管理について	【ベンダー側での対処事項なし】

注意：安全管理ガイドラインの8章において「電子保存の3基準の記載については7章に統合したので、そちらを参照」(8.1.1)とあるが、医療機関等内部に保存する場合と、外部に保存する場合で具体的な対策が異なるため、本ガイドラインにおいては7章、8章併記とした。

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」という。）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、ぜひ参考にさせていただきたい。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」の「3章 本ガイドラインの対象システム及び対象情報」を参照願いたい。

4.3. 総務省のガイドライン及び、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、ベンダーの視点から技術的な解説を行なったものである。

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5版 2017年5月
(略称：安全管理ガイドライン)
<http://www.mhlw.go.jp/stf/shingi2/0000166275.html>
- ・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 2012年10月
(略称：医療情報受託管理ガイドライン)
http://www.meti.go.jp/policy/it_policy/privacy/iryougvlv2.pdf
- ・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 2010年12月 (略称：ASP・SaaS 医療情報ガイドライン)
http://www.soumu.go.jp/main_content/000166469.pdf
- ・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ー1.4版 (2015年2月)
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2603_01.html
- ・厚生労働省：保健医療福祉分野 PKI 認証局 認証用(人)証明書ポリシー1.3版 (2015年2月)
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2603_02.html
- ・厚生労働省：保健医療福祉分野 PKI 認証局 認証用(組織)証明書ポリシー1.1版 (2010年3月)
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2203_03.html

5. ベンダーの責任のあり方

5.1. 医療機関等の責任とベンダー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」において、情報の取扱いについても医療機関等の自己責任で行う必要がある旨が明記されている。自己責任は「説明責任」、「管理責任」、「結果責任」を果たすこととされており、特にその中でも「説明責任」と「管理責任」には特段の配慮が必要とされている。

医療機関等は自らの責任で「結果責任」はもとより、「説明責任」と「管理責任」を果たさねばならないが、自らの責任の下に自己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。ベンダー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、医療機関等の「説明責任」、「管理責任」を全うすることを補助することが期待されている。医療機関等はベンダー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、ベンダー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、医療機関等に正しく伝える必要がある。

5.2. ベンダーの責任

ベンダー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）上の責任を果たさねばならない。

（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、コンピュータなど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ベンダー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など）
- (2) 製造上の欠陥（不良な原材料や部品を利用した場合など）
- (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など）

これらについては欠陥がないことの立証責任がベンダー側にあるため、ベンダー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、

「故意または過失によって他人の権利を侵害したる者はこれによって生じたる損害を賠償する責めに任ず」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ベンダーにおける最も重要な責務である。

6. 情報システムの基本的な安全管理

本章では、「安全管理ガイドライン」の以下の節について JAHIS の視点から基準を示し、解説を行ったものである。

安全管理ガイドライン	本ガイドライン
6.1 方針の制定と公表	【ベンダー側での対処事項なし】
6.2 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	6.1 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
6.3 組織的安全管理対策 (体制、運用管理規程)	【ベンダー側での対処事項なし】
6.4 物理的安全対策	【ベンダー側での対処事項なし】
6.5 技術的安全対策	6.2 技術的安全対策
6.6 人的安全対策	【ベンダー側での対処事項なし】
6.7 情報の破棄	6.3 情報の破棄
6.8 情報システムの改造と保守	6.4 情報システムの改造と保守
6.9 情報および情報機器の持ち出しについて	6.5 情報および情報機器の持ち出しについて
6.10 災害、サイバー攻撃等の非常時の対応	6.6 災害、サイバー攻撃等の非常時の対応
6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	6.7 外部と個人情報を含む医療情報を交換する場合の安全管理
6.12 法令で定められた記名・押印を電子署名で行うことについて	6.8 法令で定められた記名・押印を電子署名で行うことについて

6.1. 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。ベンダー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、ベンダー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。

また安全管理ガイドライン第5版ではベンダーからの情報収集が重要であり、その際「『製造業者による医療情報セキュリティ開示書』ガイド」で示されている「製造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」が参考になると紹介されている。

6.1.1. ISMS 構築の手順

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
項目なし	項目なし

冒頭にも述べたように、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、情報システムや情報機器を納入するベンダー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。医療機関等が JIS Q 27001:2006 に従って ISMS を構築する場合には、情報システムがこれら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思われる。

※JIS Q27001:2014 では「PDCA サイクル」という言葉は使用されていない。

しかし、安全管理ガイドラインでは「PDCA サイクル」という言葉が使用されているため、本ガイドラインにおいても旧版である JIS Q27001:2006 を引用している。

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

6.1.2. 取扱い情報の把握

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 情報システムで扱う情報を全てリストアップしていること。 2. リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。 3. このリストは、情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。	1. 上記の結果を文書化して管理していること。 (本文書内では「上記」は「左記」に相当)

(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含まれる情報と考える。ベンダーは、自社が納入し、稼働している情報システムに含まれる情報を識別し、医療機関等に説明できなければならない。

また、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。これは次節で述べるリスク分析を行う際の重要な判断基準となる。

6.1.3. リスク分析

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
4. リストアップした情報に対してリスク分析を実施していること。 5. この分析により得られた脅威に対して、6.3章～6.12章に示す対策を行っていること。 【ベンダー側での対処事項なし】	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

リスク分析は ISMS の実施に際して医療機関等が行うべきものであるが、ベンダー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。この説明を確実にを行うために、安全管理ガイドラインで紹介されている『製造業者による医療情報セキュリティ開示書』を積極的に医療機関等に提出することが望ましい。下記に保護対象とする情報ごとに整理した例を示す。

(1) 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。たとえば、「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。

(2) 管理策

想定リスクごとの管理策（対抗策）。たとえば、「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。

(3) 利用できる機能

管理策を実施するために、当該の情報システムで利用可能な機能や運用方法など。たとえば、「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」。

(4) 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。

「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。

6.2. 技術的安全対策

安全管理ガイドラインの「B.考え方」において対策が6種類に分類されているが、実際の機能との対応をよくするため、一部をさらに細分化した上で、技術的対策、運用的対策を解説した。

(1) 利用者の識別と認証

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。	項目なし

(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本人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、もしくは通知する機能があることが望ましい。
- (エ) 職員の退職等により不要となったアカウントは速やかに削除し、休職等により不用となったアカウントは速やかに無効化するよう医療機関等に推奨すること。
- (オ) 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。

(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、等の発行ルール、および、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) 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) 不要となった ID は速やかに削除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。

(2) パスワードを使用した認証

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>2. 本人の識別・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には、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行うこと。</p> <p>11. パスワードを利用者識別に使用する場合、システム管理者は以下の事項に留意すること。</p> <p>(1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。</p> <p>(2) 利用者がパスワードを忘れてたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知り得ない方法で再登録を実施すること。 【ベンダー側での対処事項なし】</p> <p>(3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)</p>	<p>4. パスワードを利用者識別に使用する場合、以下の基準を遵守すること。</p> <p>(1) パスワード入力不成功に終わった場合の再入力に対して一定不応時間を設定すること。</p> <p>(2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。</p>

(a) 技術的対策

- (ア) パスワード入力失敗による不応答時間の設定を行うことが可能な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。
- (イ) 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。
- (ウ) 交付時の初期パスワードの本人による変更や、パスワード変更を可能とする仕組みを実装すること。

(b) 運用的対策

- (ア) パスワード漏洩等の事故事例が見つかった場合の連絡を滞りなく行えるよう、連絡先や手順を明確にし、システム利用者に知らせるよう医療機関等に推奨すること。
- (イ) 必ず本人しか知り得ない状態を保つよう、モニタ等へのパスワードが記載されたメモ書き等の張

り紙行為を禁止するなどの対策を推奨すること。

(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の要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>3. 本人の識別・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には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。</p>	<p>5. 認証に用いられる手段としては、ID・パスワード+バイオメトリクス又は IC カード等のセキュリティ・デバイス+パスワード若しくはバイオメトリクスのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式 (2 要素認証) 等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上 (記憶・生体計測・物理媒体のいずれか 2 つ以上) の認証がなされていれば、2 要素認証と同等と考えてよい。</p>

(a) 技術的対策

(ア) 認証にバイオメトリ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。

(4) 利用者によるパスワード管理

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>11. パスワードを利用者識別に使用する場合、利用者は以下の事項に留意すること。</p> <p>(1) パスワードは定期的に変更し (最長でも 2 ヶ月以内 ※D.5 に規定する 2 要素認証を採用している場合を除く。)、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。</p> <p>(2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードに</p>	<p>項目なし</p>

© JAHIS 2017

最低限のガイドライン	推奨されるガイドライン
は、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。	

(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。その際、容易に推測されやすいパスワードを警告する機能を有することが望ましい。
- (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) 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、不可逆変換を施したパスワード履歴を保持することによって同一のシステム利用者が同一パスワードを設定することの抑制機能等の管理機能を実装することが望ましい。
- (エ) 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。

(b) 運用的対策

- (ア) パスワードの設定時に、推測しやすいパスワードを設定しないこと、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、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等を医療機関等の責任者またはその代行者はシステム利用者教育するよう医療機関等に推奨すること。
- (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教育することも医療機関等に推奨すること。

(5) 一時離席時の対応

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
4. 入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力のおそれがある場合には、クリアスクリーン等の防止策を講じること。	2. 離席の場合のクローズ処理等を実施すること（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。

(a) 技術的対策

- (ア) クローズ処理等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 付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。
- (イ) 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。
- (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。

(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。

(6) 情報の区分管理とアクセス制御

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
6. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。 また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。

(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）に応じて利用可能・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。

(b) 運用的対策

- (ア) 上記技術的対策を実現している場合には、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提供者は明文化し、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) 不要になった権限に関しては即座に削除するよう医療機関等に推奨すること。

(7) アクセス記録（アクセスログ）

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。	項目なし

「安全管理ガイドライン」では、上記要求事項以外にもアクセスログに対する削除／改ざん／追加等を防止する対策を講じることが要求されている。また、アクセスログの記録に使用する時刻は精度の高いものが要求されている。

これらの対策については本ガイドライン「6.2.技術的安全対策」および「7.1.3.更新履歴の保存」の関連箇所を参照のこと。

(a) 技術的対策

(ア) 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.2.0」(JAHIS 標準 13-009)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」(http://www.medical-it-link.jp/temporary/temp_1_445.pdf)も参考のこと。

(b) 運用的対策

(ア) 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。

(8) 時刻管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
9. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。	項目なし

(a) 技術的対策

(ア) 保存が義務付けられている記録を作成する全てのシステムにおいて時刻同期が必要であるが、その中でも、ネットワークに接続されるシステムは、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

(ア) 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。

(イ) 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働確認を行うよう医療機関等に推奨すること。

(ウ) 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に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。

(9) ログの真正性確保

個人情報を含むデータをやり取りする場合、全てのアクセスの記録（アクセスログ）を取得し、定期的にその内容を監査してシステムの不正な利用がないことを確認することが必要となる。このアクセスログは、セキュリティ事故などが発生した場合に、その調査のために重要な証拠性を確保していなければならないため、アクセスログ自体へのアクセス制限を行い、アクセスログの不当な削除や改ざんを防止する対策を講じなければならない。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
8. 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講じること。	項目なし

(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

- (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。

(10) 不正ソフトウェア対策

ウイルス等の不正なソフトウェアの混入を防ぐためには、医療機関等でのシステム構築・運用ではもちろん、開発ベンダー社内でのシステム開発時から対策を行う必要がある。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
10. システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時には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メディアを利用する際には、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。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	項目なし

(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、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 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、ウイルス対策ソフトを利用したとしてもすべての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) システム提供ベンダー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、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、医療機関等に示すこと。

(11) ネットワーク上からの不正アクセス

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
項目なし	3. 外部のネットワークとの接続点やDBサーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）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。

(a) 技術的対策

- (ア) 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。
- (イ) 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・報告することが望ましい。
- (ウ) 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) 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こと。

(12) その他

1) 動作確認時の配慮事項

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	項目なし

(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、データ漏洩等の可能性を極力減らすこと。
- (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き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) 個人情報保護法等の法令を遵守することや、データの管理責任を有する機関から個人情報の利用許可を受けること。
- (イ) 動作確認に使用するシステムがウイルス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。

2) 無線 LAN の利用時の対策

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ベンダーは、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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
12.. 無線 LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策を行うこと。 (2) 不正アクセスの対策を施すこと。少	7. 無線 LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせさせたセキュリティ強化をすること。

最低限のガイドライン	推奨されるガイドライン
<p>なくとも SSID や MAC アドレスによるアクセス制限を行うこと。</p> <p>(3) 不正な情報の取得を防止すること。例えば、WPA2/AES 等により、通信を暗号化し情報を保護すること。</p> <p>(4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。</p> <p>(5) 無線 LAN の適用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考にする事。</p>	

(a) 技術的対策

- (ア) ステルスモードおよび ANY 接続拒否により無線 LAN 利用を秘匿すること。
- (イ) SSID などによるアクセス制限を行うこと。MAC アドレスによる認証は、運用コストの増大要因になること、MAC アドレス詐称が可能であることから、単独での使用は推奨しない。運用負荷の増大を容認する場合は、追加的対策として MAC アドレスによるアクセス制限を行うことも可能である。
- (ウ) WPA/TKIP、WPA2/AES 等により、通信を暗号化すること。これらの暗号化方式の違いについては総務省発行の無線 LAN のセキュリティに関するガイドラインである「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考にする事。
- (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ー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に医療機関等に推奨すること。

【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「電波の医療機器等への影響に関する調査」の報告書が公開されています。

http://www.soumu.go.jp/main_content/000291919.pdf

3) IoT 機器の利用時の対策

IoT 機器により患者情報を取り扱う場合は、医療機器または非医療機器を問わず、製造販売業者からの情報提供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必要がある。また、施設外からネットワークに接続する場合の基準については、「6.7. 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照すること。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>13. IoT 機器を利用する場合、システム管理者は以下の事項に留意すること。</p> <p>(1) IoT 機器により患者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。</p> <p>(2) 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。</p> <p>(3) 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、適用すること。</p> <p>(4) 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、対策を講じること。</p>	<p>7. IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。</p>

(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) 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へ説明し、同意を得ること。
- (イ) IoT 機器に異常や不都合が発生した場合の問い合わせ方法を確立すること。
- (ウ) 使用を終えた又は停止した機器は電源を切り、接続を遮断すること。

【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」(厚生労働省医薬・生活衛生局：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) が参考になります。

6.3. 情報の破棄

「情報の破棄」は、「個別情報の消去（レコードの削除等）」と「装置そのものの廃棄に伴うデータ記憶装置・媒体の破棄（記憶装置自体の破棄等、修理時等における記憶装置交換等を含む）」が考えられるが、ここでは後者について示す。前者についてもこの内容を適応できる場合があるが、情報の格納方法が独立したファイルである場合からデータベース内の削除処理等様々な状況が考えられるので、実際の破棄に備えて個別に安全な管理・消去方法等の手順を明確化しておく必要がある。破棄された情報は参照、復元できてはならない。

(1) 情報種別ごとに破棄の手順を定める

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
1. 「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。【ベンダー側での対処事項なし】	項目なし
2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。【ベンダー側での対処事項なし】	項目なし
3. 外部保存を受託する機関に破棄を委託した場合は、「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託元の医療機関等が確実に情報の破棄が行なわれたことを確認すること。【ベンダー側での対処事項なし】	項目なし
4. 運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の廃棄を定める規程の作成【ベンダー側での対処事項なし】	項目なし

(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こと。

外部業者に依頼するときは、「安全管理ガイドライン」「6.6 人的安全対策 (2) 事務取扱委託業者の監督及び守秘義務契約」に準じ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」を定めること。

6.4. 情報システムの改造と保守

医療情報システムを安全にかつ有効に運用するためには、定期的な保守が必要となる。保守には障害対応や予防保守、ソフトウェアのアップデートなどがあるが、特にデータベースを扱う作業やサーバ等の再起動が必要とされる作業など、情報システムを一時的に停止する場合が生じることがある。また、オペレーションミスによるデータの紛失や消去など、セキュリティ面においても十分な対策が求められる。情報システムの改造と保守について、「安全管理ガイドライン」で挙げられている4つの脅威はデータそのものに対する代表的な脅威がほとんどで、さらに情報システムに対する脅威も多く存在する。改造や保守作業は、医療機関等の適切な管理の下で実施されるものである。従って、保守ベンダーとの間で交わされる守秘義務契約や、保守要員の管理、作業内容の確認など、医療機関等の運用面での対策が必要である。

(1) 保守会社との守秘義務契約の締結

1) 保守会社との守秘義務契約の締結

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
6. 保守会社と守秘義務契約を締結し、これを遵守させること。	3. 作業員各人と保守会社との守秘義務契約を求めること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

- (ア) 保守ベンダー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。
- (イ) 保守ベンダー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。

2) 保守作業の再委託

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
9. 再委託が行なわれる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。	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。

(2) 保守要員の登録と管理

1) アカウント管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。	1. 詳細なオペレーション記録を保守操作ログとして記録すること。

(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。

(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。

2) アカウント流出防止

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
3. そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。	項目なし

(a) 技術的対策

- (ア) 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) 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。

3) アカウント削除管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
4. 保守要員の離職や担当替え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付け、また、それに応じるアカウント管理体制を整えておくこと。	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。

(3) 作業計画報告の管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	2. 保守作業時には医療機関等の立会いの下で行なうこと。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

(4) 作業時の医療機関等の関係者による監督

1) ログ管理 及び リモートメンテナンス

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
8. リモートメンテナンスによるシステムの改造や保守が行なわれる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	1. 詳細なオペレーション記録を保守操作ログとして記録すること。 5. 保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行なわれたかが確認できる仕組みが備わっていること。

(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、「6.2 技術的安全対策 (7) アクセス記録 (アクセスログ)」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.3.0」(JAHIS 標準 16-003)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.3.0」(JAHIS 標準 16-003)を参照すること。

2) 保守作業で使用するデータ

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	項目なし

(a) 技術的対策

追記事項なし。

(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、明確な守秘義務を病院とベンダー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。

3) 個人情報を含むデータの組織外への持ち出し

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
7. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。

(a) 技術的対策

「安全管理ガイドライン」自体が、かなり技術的対策に踏み込んで記述されているので、ここではその内容を踏まえた上で、持ち出し機器の対策に鑑み追記の必要のある内容のみ記述する。

- (ア) 持ち出し機器、媒体については、必ず内容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、必ずウイルス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、ウイルス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) 覗き見防止フィルタは、装着することが望ましい。
- (キ) 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) 保守ベンダーは医療機関等が定める運用管理規程を遵守すること。
- (ア) 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。
- (イ) 個人情報を含むテスト用データの扱いについては、「6.7 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照すること。
- (ウ) 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。
- (エ) 当該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。
- (オ) 医療機関等から持ち出した情報および情報機器の取り扱いについては、自組織内で運用管理規程を定め、遵守すること。
- (カ) システム提供者の運用管理規程には、上記「安全管理ガイドライン」の少なくとも「最低限のガイドライン」の要求事項を盛り込むこと。
- (キ) 当該の運用管理規程は、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。
- (ク) 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。

6.5. 情報および情報機器の持ち出しについて

「安全管理ガイドライン」の要求事項は、医療機関等から見た業務委託先であるベンダーにも適用される。ただし、ベンダーが医療機関等から情報や情報機器を持ち出すケースは、そのほとんどが保守用途と考えられるため、ここでの記述は「6.4 情報システムの改造と保守」での記述に委ねるものとする。また、情報の持ち出し方法として、データ回線による電子的な移動も考えられるが、これについても同様とする。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>1. 組織としてリスク分析を実施し、情報および情報機器の持ち出しに関する方針を運用管理規程で定めること。 【ベンダー側での対処事項なし】</p> <p>2. 運用管理規程には、持ち出した情報および情報機器の管理方法を定めること。 【ベンダー側での対処事項なし】</p> <p>3. 情報を格納した可搬媒体若しくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。 【ベンダー側での対処事項なし】</p> <p>4. 運用管理規程で定めた盗難、紛失時の対応に従業者等に周知徹底し、教育を行うこと。 【ベンダー側での対処事項なし】</p> <p>5. 医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。 【ベンダー側での対処事項なし】</p> <p>6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワードなどの利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。</p> <p>7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。</p> <p>8. 持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネット</p>	<p>1. 外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。</p> <p>2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。</p> <p>3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。</p> <p>4. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。</p> <ul style="list-style-type: none"> ・BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。

最低限のガイドライン	推奨されるガイドライン
<p>ワークに接続する場合は「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。</p> <p>9. 持ち出した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あるいは停止するか、業務に対して影響がないことを確認して用いること。 【ベンダー側での対処事項なし】</p> <p>10. 個人保有の情報機器（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、医療機関等々の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。【ベンダー側での対処事項なし】</p>	

(a) 技術的対策

技術的対策については、「6.4 情報システムの改造と保守 (4) 作業時の医療機関等の関係者による監督
3) 個人情報を含むデータの組織外への持ち出し」の「(a) 技術的対策」を参照すること。

(b) 運用的対策

運用的対策については、「6.4 情報システムの改造と保守 (4) 作業時の医療機関等の関係者による監督
3) 個人情報を含むデータの組織外への持ち出し」の「(b) 運用的対策」を参照すること。

6.6. 災害、サイバー攻撃等の非常時の対応

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。ここでいう「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正常状態になる場合

の2種類の状態を言う。

1) の状態は、

(ア) 広域災害

災害（地震、水害、落雷、火災等）による電力・通信途絶、施設・設備損壊、インフラ業者のIT機能不全

(イ) 局所被害

サイバー攻撃による不正侵入・改ざんを検知、あるいはウイルス攻撃・DoS 攻撃によるサービス不能

(ウ) システム障害

ハードウェアの故障、プログラムの欠陥、操作ミスによるサービス不能などにより、医療情報システムが縮退運用や全面停止状態になる状態である。

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 策定と運用のポイントとして、BCP 発動以降を、BCP 実行フェーズ、業務再開フェーズ、業務回復フェーズ、全面復旧フェーズの四つに分けている。尚、BCP の詳細な内容はガイドラインの「考え方」を参照願いたい。

システム提供者は、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、システム提供者自身の BCP の整備も必要となる。

(1) 非常時における事業継続計画 (BCP: Business Continuity Plan)

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	項目なし
2. 正常復帰後に、代替手段運用した間のデータ整合性を図る規約を用意すること。	項目なし

(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。

(b) 運用的対策

- (ア) システム提供者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) システム提供者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) システム提供者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。

(2) 医療システムの非常時運用への対応

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>3. 非常時の情報システムの運用</p> <ul style="list-style-type: none"> ・ 「非常時のユーザアカウントや非常時機能」の管理手順を整備すること。 ・ 非常時機能が定常時に不適切に利用されないことがないようにして、もし使用された場合には使用されたことが多くの人に分かるようにする等、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出来ないように変更しておくこと。 ・ 標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、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。 	<p>項目なし</p>

(a) 技術的対策

- (ア) 非常時機能を有すること。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。
- (イ) 非常時機能は、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。
- (ウ) 非常時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。
- (エ) 非常時機能が使用された場合、そのことを適当な人に通知する機能、非常時に切り替えたユーザを特定したり、利用記録が監査ログに残る機能を有すること。
- (オ) 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。
- (カ) 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と望ましい）。

(b) 運用的対策

- (ア) 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、ポリシー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。

(3) サイバー攻撃を受けた際の非常時の対応

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。</p> <p>連絡先 厚生労働省 医政局研究開発振興課医療技術情報推進室 (03-3595-2430)</p> <p>※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。</p> <p>なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。</p> <p>連絡先 情報処理推進機構 情報セキュリティ安心相談窓口 (03-5978-7509)</p>	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。

6.7. 外部と個人情報を含む医療情報を交換する場合の安全管理

外部と医療情報を外部ネットワークを利用して交換する場合、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ンネル・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。

オブジェクトセキュリティにおいては、医療情報をネットワークを通じて伝播させる場合に、「盗聴」、「改ざん」、「なりすまし」などの危険性に対する対応が必要とされる。

盗聴：パスワード盗聴、本文の盗聴など

改ざん：メッセージ挿入、ウイルス混入など

なりすまし：情報の流出・改ざんなどの原因となる

ガイドラインでは、改ざん検知のための電子署名や、PKI を利用したネットワーク接続時の認証の仕組みにより通信の起点と終点で医療機関等を適切に識別できるように求めている。

チャンネル・セキュリティにおいては、通信経路上での脅威への対策とともに、外部と医療機関等との間の責任分界点を明確にするために、ガイドラインではネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要があるとしている。この際の考え方として、外部と医療機関等を接続するために以下の二つの場合について類型化している。

- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合：回線事業者とオンラインサービス提供事業者が提供するクローズドなネットワークや、インターネット回線を利用した Internet-VPN のような通信形体のうち、ネットワーク上のセキュリティを上記業者が担保しているもの。
- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合：インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器・ソフトウェアを導入して双方を接続する場合などが考えられる。

(1) 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では、外部と診療情報等を交換するケースとして、以下の五つのケースを元に解説している。

- 地域医療連携で医療機関等や検査会社等と相互に連携してネットワークで診療情報等をやり取りする場合
- 診療報酬の請求のために審査支払機関等とネットワークで接続する場合
- ASP・SaaS 型のサービスを利用する場合
- 医療機関等の従事者がノートパソコンの様なモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する場合
- 患者等による外部からのアクセスを許可する場合

このように、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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>1. ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。</p> <p>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行うこと。</p> <p>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対策を行うこと。上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな通信路を確保することが挙げられる。チャネル・セキュリティの確保を閉域ネットワークの採用に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閉域性の範囲を事業者を確認すること。</p>	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。

(2) 外部との通信における認証

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こと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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>2. データ送信元と送信先での、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。</p> <p>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。</p>	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。

(3) 外部との通信における成りすましの防止

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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
3. 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行うこと。これに関しては、「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。	項目なし

(a) 技術的対策

技術的対策については、「6.2. 技術的安全対策」の「(a) 技術的対策」を参照すること。

(b) 運用的対策

運用的対策については、「6.2. 技術的安全対策」の「(b) 運用的対策」を参照すること。

(4) 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の要求事項>

最低限のガイドライン	推奨されるガイドライン
4. ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット若しくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。	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。

(5) 外部との通信における秘匿性の確保

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」<http://www.cryptrec.go.jp/method.html>)

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
5. 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などのセキュリティ対策を実施すること。例えば、SSL/TLS の利用、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。	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。

(6) 外部との通信における責任分界

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
6. 医療機関等との間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次の事項について、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。 <ul style="list-style-type: none"> ・ 診療情報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係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又は著しい遅延の場合の対処 	項目なし

最低限のガイドライン	推奨されるガイドライン
<ul style="list-style-type: none"> ・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 <p>また、医療機関等内においても次の事項において契約や運用管理規程等で定めておくこと。</p> <ul style="list-style-type: none"> ・通信機器、暗号化装置、認証装置等の管理責任の明確化（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置 ・交換した医療情報等に対する結果責任の明確化（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） 	

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

(7) リモート保守の限定

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
7. リモートメンテナンスを実施する場合は、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止すること。また、メンテナンス自体は「6.8 情報システムの改造と保守」を参照すること。	項目なし

(a) 技術的対策

技術的対策については、「6.2. 技術的安全対策」の「(a) 技術的対策」を参照すること。

(b) 運用的対策

運用的対策については、「6.2. 技術的安全対策」の「(b) 運用的対策」を参照すること。

【コラム】

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観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ー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.3.0」（JAHIS 標準 16-003）を公開しています。

(8) 責任範囲と品質保証

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。また、上記 1 および 4 を満たしていることを確認すること。	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。

(9) 患者の閲覧行為に関する安全対策

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、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 SSL 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の要求事項>

最低限のガイドライン	推奨されるガイドライン
9. 患者に情報を閲覧させる場合、情報を公開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、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た対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	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。

(10) オープンなネットワークを利用して HTTPS を利用する際の安全対策

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 SSL/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「SSL/TLS 暗号設定ガイドライン」にて示される設定に加え、TLS クライアント認証を行う必要がある。

(参照：「SSL/TLS 暗号設定ガイドライン」<https://www.ipa.go.jp/files/000045645.pdf>)

<安全管理ガイドラインの要求事項>

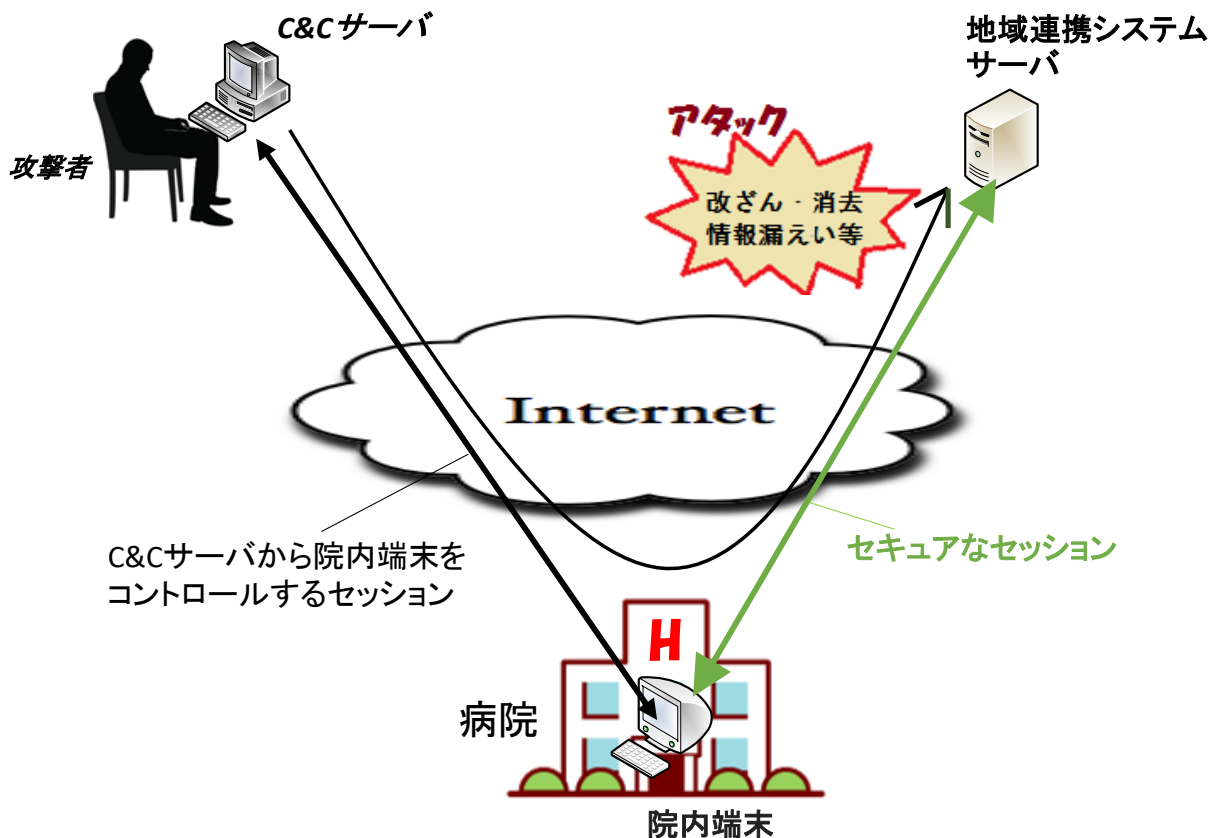
最低限のガイドライン	推奨されるガイドライン
10. オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、	項目なし

最低限のガイドライン	推奨されるガイドライン
<p>SSL/TLSのプロトコルバージョンを TLS1.2 のみに限定した上で、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。その際、 TLS の設定はサーバクライアントともに「SSL/TLS 暗号設定ガイドライン」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。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 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）等による攻撃からの防護について、適切な対策を実施すること。</p>	

(a) 技術的対策

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 TLS1.2 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。



(b) 運用的対策

追記事項なし。

(11) 従業者による外部からのアクセスに関する安全対策

医療機関等の職員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、職員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 を使用する場合はもちろん、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の要求事項>

最低限のガイドライン	推奨されるガイドライン
項目なし	1. やむを得ず、従業者による外部からのアクセスを許可する場合は、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を用いるとともに、運用等の要件を設定すること。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

6.8. 法令で定められた記名・押印を電子署名で行うことについて

「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。

尚、第 4 版からは、2014 年度からの暗号アルゴリズム（SHA1、RSA1024）の移行問題にも触れ、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た。さらに、これを実現する手段として、JIS の長期署名プロファイルによる方法を例示し、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。

(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の要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>(1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと</p> <p>1. 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。従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ことが推奨される。ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。</p> <p>2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても A の要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能である必要がある。</p> <p>3. 「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、行政機関以外に当該電子署名を検証しなければならない者が全て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。</p>	<p>項目なし</p>

(a) 技術的対策

診療録等の電子保管においては、医師など一定の資格を持つ自然人が、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。また、診断書や処方せん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ことが推奨される。この場合、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできる事が必要である。

以下に、電子署名に用いる証明書を例示する

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、2013 年 3 月に Ver.1.1 として改定しているので合わせて参照されたい。

(ア) 認定特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（認定特定認証事業者）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ー（CP）を参照の上、確認する必要がある。（認定特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、認定特定認証事業者は、法務省の以下の URL で確認できる。

<http://www.moj.go.jp/MINJI/minji32.html>

また、本ガイドライン執筆時点では、標準的なポリシーに従って医師などの国家資格属性が証明書の中に記載された証明書を発行する認定認証局は存在しない。従って、その証明書を利用して電子署名を付与した場合、署名を検証するだけでは医師等の国家資格を有する個人が署名したものであるか判断出来ない。署名者の国家資格の確認が必要な場合、別に確認する必要がある。従って、保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は認定特定認証事業者の証明書を利用することは推奨しない。但し、「9. 診療録等をスキャナ等により電子化して保存する場合について」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特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。尚、行政機関等が電子署名を検証可能である必要があるため、認定認証業務以外の証明書を用いる場合は、「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。

(イ) 保健医療福祉分野 PKI（Healthcare PKI）の電子証明書

本ガイドラインでは、認定特定認証事業者の発行する電子証明書と同様の厳密さで本人確認を行って発行される電子証明書として、厚生労働省によって整備される保健医療福祉分野 PKI（Healthcare PKI、以下 HPKI と呼ぶ）によって定められた認証局証明書ポリシー（付録 2-1 参照）に準拠した電子証明書の利用を推奨する。

HPKI は、医療機関等における連携・情報共有等を行うためのセキュリティ基盤として定義されるもので、医師等による電子署名を行うための証明書を発行する。HPKI の認証局証明書ポリシーによれば、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ー1.4 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、ISO IS17090 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、Medical Doctor=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ーにより標準化されている。記名・押印が必要な文書を電子的に作成する際に付与する電子署名に用いる証明書として適したものであるといえる。

(ウ) 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幅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る、署名者に事前に充分に説明の上、同意を得る必要がある。

従って、公的個人認証サービスが発行する証明書の利用は推奨しない。

(b) 運用的対策

電子署名を扱う運用を行う際は、事前に上記(a)の認証局に、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。

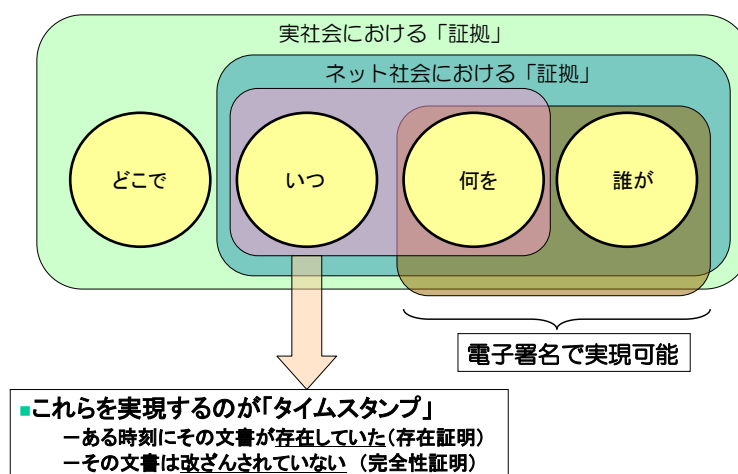
また、本人の私有鍵は、本人の意図しない利用を防止するために厳格に管理される必要がある。私有鍵を格納した IC カードや PC 等は本人以外の利用を防止する対策がなされるべきである。

(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の要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>(2) 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</p> <ol style="list-style-type: none"> 1. タイムスタンプは、「タイムビジネスに係る指針—ネットワークの安心な利用と電子データの安全な長期保存のために—」（総務省、平成 16 年 11 月）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のものを使用し、第三者がタイムスタンプを検証することが可能であること。 2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。 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講じる必要がある。 	<p>項目なし</p>

(a) 技術的対策

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ができる。



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。最低限のガイドラインでは「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事。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。

(ア) 時刻認証事業者と第三者によるタイムスタンプの検証

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。

<http://www.dekyo.or.jp/tb/list/index.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ため、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。

(イ) 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認定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古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）

(ウ) 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

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。

(3) 電子証明書の有効性について

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>(3) 上記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</p> <p>1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点で有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要な情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。</p>	<p>項目なし</p>

(a) 技術的対策

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、証明書が有効であったことを後日に検証可能である必要がある。

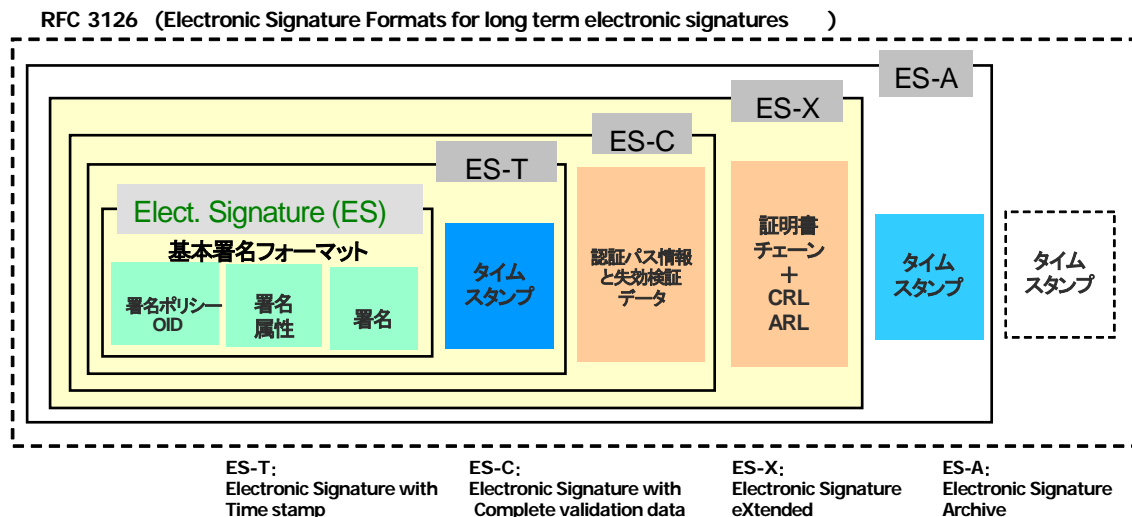
法定保存期間中（もしくはそれ以上の長期）において有効な電子証明書を用いて電子署名を行ったことを検証可能とするためには、タイムスタンプ付与時点において電子署名が有効であったことを示すために、証明書検証に必要な認証パス上の証明書や失効情報（CRL/ARL）などの情報を真正性を保って保存する必要がある。

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「RFC 3126」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 RFC 3126 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。

尚、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
© JAHIS 2017

をベースとした XAdES (XML Advanced Electronic Signatures)、PDF ファイルを対象とした PAdES (PDF Advanced Electronic Signatures) 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。



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

有効期間が切れた証明書の利用を防止するため、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。

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。

(4) 9章での電子署名、タイムスタンプの付し方

本章は記名・押印が必要な医療関連文書を電子保存する際の電子署名、タイムスタンプの付し方として解説されているが、「9. 診療録等をスキャナ等により電子化して保存する場合について」にて、作成責任を明確にし改ざんを防止するための措置として付与される電子署名、タイムスタンプも、本章の要件を満たす必要が有ることを留意されたい。

7. 電子保存の要求事項について

本章では、「安全管理ガイドライン」の以下の節について JAHIS の視点から基準を示し、解説を行ったものである。

安全管理ガイドライン	本ガイドライン
7.1 真正性の確保について	7.1 真正性の確保について 一部は 8.1.1.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
7.2 見読性の確保について	7.2 見読性の確保について 一部は 8.1.1.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
7.3 保存性の確保について	7.3 保存性の確保について 一部は 8.1.1.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

7.1. 真正性の確保について

「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」の記載については、8章にそれぞれ統合したので、そちらを参照されたい。

安全管理ガイドライン	本ガイドライン
7.1 真正性の確保について	7.1 真正性の確保について
7.1C	
【医療機関等に保存する場合】	
(1) 入力者及び確定者の識別及び認証	7.1.1. 入力者及び確定者の識別及び認証
(2) 記録の確定手順の確立と、識別情報の記録	7.1.2. 記録の確定手順の確立と、識別情報の記録
(3) 更新履歴の保存	7.1.3. 更新履歴の保存
(4) 代行入力の承認機能	7.1.4. 代行入力の承認機能
(5) 機器・ソフトウェアの品質管理	7.1.5. 機器・ソフトウェアの品質管理
【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】	8. 診療録及び診療諸記録を外部に保存する際の基準 8.1. 厚生労働省の医療情報システムの安全管理に関するガイドラインに関する事項
(1) 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	8.1.1. 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
(2) 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	8.1.1. 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
(3) リモートログイン機能を制限すること	8.1.1. 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

7.1.1. 入力者及び確定者の識別及び認証

(1) 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

1) 本人認証、識別

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 入力者及び確定者を正しく識別し、認証を行うこと。	項目なし

(a) 技術的対策

(ア) 電子保存システムは利用者の識別・認証をシステムへのログイン時および必要な時点で以下のいずれかの方式で行えること。

- ① ID・パスワード方式
- ② ICカード方式（電子証明書による認証）
- ③ USBデバイス方式（電子証明書による認証）
- ④ バイオメトリックス方式
- ⑤ 上記①～④相当以上の識別・認証方式
- ⑥ 上記の組み合わせ

ただし、④バイオメトリックス方式を用いる場合は、1対1の照合となるように他の方式と合わせて用いること。また、①のみによる認証方式は、「安全管理ガイドライン」では推奨されていない。

(イ) 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。

(ウ) 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

(エ) 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なシステムであること。

(b) 運用的対策

(ア) ID・パスワード方式で認証を行う場合は、以下のように運用すること。

- ・ 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。
- ・ パスワードは、8桁以上でかつ数字、アルファベット、使用が許されている記号等を組み合わせて容易に推測できないものとする。
- ・ 2ヶ月に1回以上の頻度でパスワード更新すること。
- ・ 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正常運用状況（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。

- (イ) IC カード方式の場合は、他者に貸与しないこと。また、紛失の恐れがあるので以下を義務づけること。
 - ・ 毎日 1 回の所持確認をすること。
 - ・ 所在不明となった場合は速やかに届け出ること。
- (ウ) 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こと。
- (エ) 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こと。

2) アクセスコントロール

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
2. システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。	項目なし

(a) 技術的対策

- (ア) アクセス権の基本機能として以下のものが満たされること。
 - ・ システムの業務メニュー単位でその業務の運用操作が可能か否かを職務および利用者単位に設定できること。
 - ・ 必要に応じて、上記以上に細かいアクセス権を設定できること。例えば、情報の種類（区分）や内容に応じた参照・更新制限が必要に応じてできること。
- (イ) 情報へのアクセス（参照・入力・更新）に際し、その処理内容をログ出力（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。
- (ウ) 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。

(b) 運用的対策

- (ア) 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。
- (イ) 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。
- (ウ) 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。
- (エ) 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。

3) アクセス端末の制限

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
3. 業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。	項目なし

(a) 技術的対策

- (ア) 業務アプリケーションが稼動可能な端末を IP アドレスなどにより識別し、それ以外の端末から業務アプリケーションが稼動するサーバへのアクセスを拒否する仕組みを設けること。

(b) 運用的対策

- (ア) 業務アプリケーションが稼動可能な端末には、利用者毎に端末へのログインアカウントを作成すること。

(2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合

1) 装置の操作者の制限

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。	項目なし
2. 当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	

(a) 技術的対策

- (ア) 当該装置に対して、いつ記録が行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) 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こと。
- (イ) 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、その結果を残すこと。

7.1.2. 記録の確定手順の確立と、識別情報の記録

(1) 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

1) 確定記録の登録

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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、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含まれること。</p> <p>3. 「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すること。</p> <p>5. 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こと。</p> <p>6. 確定者が、何らかの理由で確定操作ができない場合、例えば医療機関等の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で定め、記録の確定の責任の所在を明確にすること。</p>	項目なし

(a) 技術的対策

(ア) 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。

(イ) 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。

- 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。
- 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。
- 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。

- (ウ) 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「7.1.1. 入力者及び確定者の識別及び認証」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。
- (エ) 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。

(b) 運用的対策

- (ア) 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ことを医療機関等に推奨すること。
- (イ) 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ことを医療機関等に推奨すること。
- (ウ) 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ことを医療機関等に推奨すること。

2) 確定記録の確認

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
2. 「記録の確定」を行うに当たり、内容の十分な確認が実施できるようにすること。	項目なし

(a) 技術的対策

- (ア) 内容の十分な確認が実施できるよう、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。

(b) 運用的対策

- (ア) 上記技術と合わせて、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ことを推奨すること。

3) 確定記録の原状回復

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
4. 確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防止対策を講じておくこと、また原状回復のための手順を検討しておくこと。	項目なし

(a) 技術的対策

(ア) 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「7.3 保存性の確保について」を参考にリストア可能とすること。

(b) 運用的対策

- (ア) 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ことを医療機関等に推奨すること。
- (イ) 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ことを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こと。

(2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合

1) 確定記録の取扱い

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 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が定義されていること。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）、信頼できる時間源を用いた作成日時が記録に含まれること。	項目なし
2. 確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防止対策を講じておくこと及び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

「7.1.2. 記録の確定手順の確立と、識別情報の記録」の「(a) 技術的対策」を参照すること。

(b) 運用的対策

「7.1.2. 記録の確定手順の確立と、識別情報の記録」の「(b) 運用的対策」を参照すること。

7.1.3. 更新履歴の保存

(1) 更新履歴の保存と参照

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 一旦確定した診療録等を更新した場合、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こと。 2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	項目無し

(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、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こと。

7.1.4. 代行入力 of 承認機能

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った操作のことをいう。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。

(1) 代行プロシジャの定義

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、実装されていない場合は運用で担保すること。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 代行入力を実施する場合、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	項目無し

(a) 技術的対策

- (ア) 情報システムは、ある利用者 to 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、「代行ポリシー」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、特定の利用者を指定すること。
- (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。
 - ① 当該の操作が代行可能であること。
 - ② 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。
 - ③ 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。

(b) 運用的対策

情報システムが上記技術的対策の（ア）～（エ）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、医療機関等は、下記の運用を行わなければならない。

- (ア) 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、代行ポリシーおよび運用管理規程を設定すること。
- (イ) 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。

(2) 代行入力の記録

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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
2. 代行入力が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。	項目なし

(a) 技術的対策

- (ア) 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。
- (イ) 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、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。

(3) 代行入力の承認

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の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る、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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
3. 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	項目なし

最低限のガイドライン	推奨されるガイドライン
作（承認）」が行われること。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。	

*確定者： 確定の実施できる権限を持った者

(a) 技術的対策

- (ア) 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」とされた代行入力及要求されると、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」とされた代行入力及要求されると、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何らかの方法で残しておく。
 - 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。

7.1.5. 機器・ソフトウェアの品質管理

(1) 機器、ソフトウェアの構成の明確化

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
1. システムがどのような機器、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が明らかにされており、システムの仕様が明確に定義されていること。	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 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。

(2) 機器、ソフトウェアの改訂、導入作業のプロセスの規定

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
2. 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が規定されていること。	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 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プロジェクト計画書を提示すること。

(3) 機器、ソフトウェアの品質管理に関する内容の運用管理規程への記載

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) 機器・ソフトウェアの品質に関する作業内容を明記したプロジェクト計画書を提示すること。

(4) 機器、ソフトウェアの品質管理に関する内部監査

＜安全管理ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
4. システム構成やソフトウェアの動作状況に関する内部監査を定期的実施すること。	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。

7.2. 見読性の確保について

「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」の記載については、8章にそれぞれ統合したので、そちらを参照されたい。

安全管理ガイドライン	本ガイドライン
7.2 見読性の確保について	7.2 見読性の確保について
7.2 C	
(1) 情報の所在管理	7.2.1. 情報の所在管理
(2) 見読化手段の管理	7.2.2. 見読化手段の管理
(3) 見読目的に応じた応答時間	7.2.3. 見読目的に応じた応答時間
(4) システム障害としての冗長性の確保	7.2.4. システム障害対策としての冗長化の確保
7.2 D	
【ネットワークを通じて外部に保存する場合】	8. 診療録及び診療諸記録を外部に保存する際の基準 8.1 厚生労働省の医療情報システムの安全管理に関するガイドラインに関する事項
(1) 緊急に必要になることが予測される診療録等の見読性の確保	8.1.2 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見読性の確保
(2) 緊急に必要になるとまではいえない診療録等の見読性の確保	8.1.2 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見読性の確保

7.2.1. 情報の所在管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの情報の全ての所在が日常的に管理されていること。	項目なし

(a) 技術的対策

(ア) 電子カルテシステムや PACS など大量のデータを扱うシステムにおいて、記憶装置の容量の制約などから、通常のオンライン業務でアクセスできない媒体にデータを部分的に保管することがある。このように複数の媒体に分散してデータを保管する場合は、患者の情報がどの媒体（オンライン、オフライン（どの外部媒体））に保管されているのかを管理ができる必要がある。

(b) 運用的対策

(ア) 紙カルテ、電子化されていない紹介状などの紙を含めた患者の情報の保管場所について、院内で各種情報の保管ルールを定め、必要な時間内に患者の情報の所在が判別でき、アクセスできるように管理する必要がある。

7.2.2. 見読化手段の管理

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(2) 電子媒体に保存されたすべての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	(2) 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。

(a) 技術的対策

(ア) 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。
 (イ) 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。
 (ウ) システム間のデータ移行を前提として、標準的な形式にてデータ出力する機能を有すること。

(b) 運用的対策

(ア) 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こと。
 (イ) 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、運用すること。

© JAHIS 2017

7.2.3. 見読目的に応じた応答時間

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(3) 目的に応じて速やかに検索表示若しくは書面に表示できること。	項目なし

(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) 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。

7.2.4. システム障害対策としての冗長性の確保

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(4) システムの一系統に障害が発生した場合でも、通常の診療に差し支えない範囲で診療記録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読手段を用意すること。	(1) バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。
	(3) 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。

(a) 技術的対策

(ア) 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

(イ) 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

(b) 運用的対策

(ア) 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こと。

(イ) 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しておくことが望ましい。

7.3. 保存性の確保について

「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」の記載については、8章にそれぞれ統合したので、そちらを参照されたい。

安全管理ガイドライン	本ガイドライン
7.3 保存性の確保について	7.3 保存性の確保について
7.3 C	
【医療機関等に保存する場合】	
(1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	【ベンダー側での対処事項なし】
(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	7.3.1. 不適切な保管・取扱いによる情報の滅失、破壊の防止
(3) 記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止	【ベンダー側での対処事項なし】
(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止	7.3.2. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止
【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】	
(1) 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	8.1.3 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保存性の確保
(2) ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと	8.1.3 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保存性の確保

7.3.1. 不適切な保管・取扱いによる情報の滅失、破壊の防止

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うよう関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。 【ベンダー側での対処事項なし】	1. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。 【ベンダー側での対処事項なし】
2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。 【ベンダー側での対処事項なし】	項目なし
3. 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。 【ベンダー側での対処事項なし】	2. サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。 【ベンダー側での対処事項なし】
4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。 【ベンダー側での対処事項なし】	項目なし
5. 各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	3. 診療録等のデータのバックアップを定期的に取り得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。

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に至っている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スペースも大きくなる

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ため、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) 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。
- (イ) 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。
- (ウ) 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。
- (エ) 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(イ)項により、運用で担保すること。

(b) 運用的対策

- (ア) 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（たとえば、1週間前に戻せる、等）し、実施すること。
- (イ) 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、そのとおりに実施されるような管理を行うこと。
- (ウ) 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。

- (エ) 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（たとえば、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。
- (オ) 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）。
- (カ) 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。

（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で、何とか実現するようにもって行くことが望まれる。

7.3.2. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止

(1) 標準的な形式での入出力

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
1. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	項目なし

(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。
- (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。

（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ベンダー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

(b) 運用的対策

- (ア) システム提供者は、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) システム提供者は、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。

(2) マスタ変更への考慮

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
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ていること。	項目なし

(a) 技術的対策

- (ア) 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。たとえば、「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。
- (イ) 上記（ア）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。

(b) 運用的対策

- (ア) 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こと。

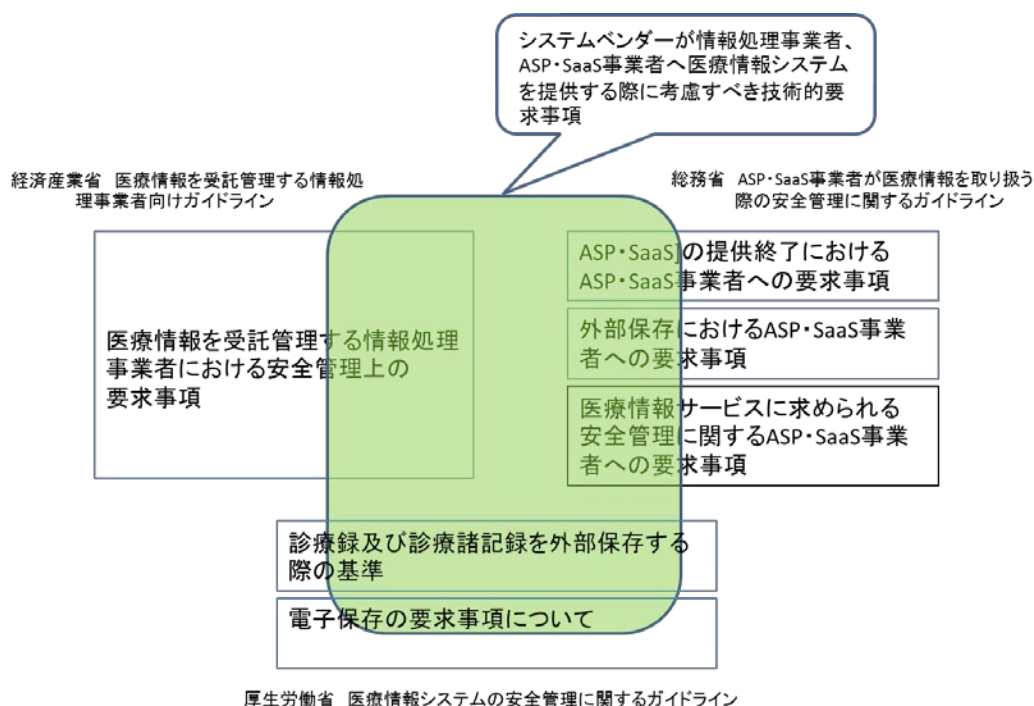
8. 診療録及び診療諸記録を外部に保存する際の基準

外部保存の形態として、下記の三つのパターンがあるが、(2)、(3)については、従来から行われていることであり、本ガイドラインでは、(1)に関する対応について記述する。

- (1) 電子媒体による外部保存をネットワークを通じて行う場合
- (2) 電子媒体による外部保存を磁気テープ、CD-R、DVD-Rなどの可搬型媒体で行う場合
- (3) 紙やフィルム等の媒体で外部保存を行う場合

本章では、厚生労働省の「医療情報システムの安全管理に関するガイドライン(第5版)」、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)」、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)」に関して以下の節(8.1節 厚生労働省、8.2節 経済産業省、8.3節 総務省)にてベンダーの視点から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。

本章は三省のガイドラインにおける技術的要求事項の内、システムベンダーが情報処理事業者及びASP・SaaS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(下図における網掛け部)を対象としている。三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、システムベンダー、サービスプロバイダー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ーとなることを意識願いたい。また、本章ではサービス提供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。



8.1. 厚生労働省の医療情報システムの安全管理に関するガイドラインに関する事項

本節では厚生労働省の「安全管理ガイドライン」においてシステムベンダーが電子媒体による外部保存をネットワークを通じて行う情報処理事業者及びASP・SaaS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を対象に解説を行う。

＜厚生労働省：安全管理ガイドラインとの対比＞

安全管理ガイドライン	本ガイドライン
7.1 真正性の確保について C【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】	8.1.1 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
7.2 見読性の確保について D【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】	8.1.2 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見読性の確保
7.3 保存性の確保について C【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】	8.1.3 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保存性の確保
7.3 保存性の確保について D【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】	同上
8.1.1 電子保存の3基準の遵守	8.1.1 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 8.1.2 ネットワークを通じて医療機関等の外部に保存場合の見読性の確保 8.1.3 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保存性の確保
8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準	【ベンダー側での対処事項なし】
8.1.3 個人情報の保護	【ベンダー側での対処事項なし】
8.1.4 責任の明確化	本ガイドライン 6.7 (安全管理ガイドライン 6.11) を参照のこと
8.1.5 留意事項	対象外 (電子媒体による外部保存を可搬媒体を用いて行う場合)
8.2 電子媒体による外部保存を可搬媒体を用いて行う場合	対象外 (電子媒体による外部保存を可搬媒体を用いて行う場合)
8.3 紙媒体のままで外部保存を行う場合	対象外 (紙媒体のまま外部保存を行う場合)
8.4.1 運用管理規程	【ベンダー側での対処事項なし】

安全管理ガイドライン	本ガイドライン
8.4.2 外部保存契約終了時の処理について	安全管理ガイドラインに C、D 記載なし

8.1.1. 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

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。

従って、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。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>(1) 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</p> <p>診療録等のオンライ外部保存を受託する機関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が必要である。</p>	項目なし
<p>(2) 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</p> <p>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こと。なお、可逆的な情報の圧縮・解凍並びにセキュリティ確保のためのタグ付けや暗号化・平文化などは改ざんにはあたらない。</p>	項目なし
<p>(3) リモートログイン機能を制限すること</p> <p>保守目的等、どうしても必要な場合を除いて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。</p>	項目なし

(a) 技術的対策

- (ア) 外部保存をする場合のネットワークは、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こと。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。
- (イ) ネットワーク経路での改ざんを防止するために SSL 等の暗号化通信を行うこと。その際、暗号方式については十分な強度のもの（電子政府推奨暗号に記載されているもの）を使用すること。
- (ウ) 保守目的以外に、委託元の操作者以外がデータアクセスすることを制限できること。

(b) 運用的対策

- (ア) 委託元医療機関等内の電子カルテ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ネットワーク設計および管理を行う様に医療機関等を指導すること。

8.1.2. 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見読性の確保

ネットワークを通じて外部に保存する場合は、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、予め「責任分界点」を明確化しておき、速やかなる復旧が図られるように配慮しておく必要がある。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
項目なし	(1) 緊急に必要なことが予測される診療録等の見読性の確保 緊急に必要なことが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。 (2) 緊急に必要なとまではいけない診療録等の見読性の確保 緊急に必要なとまではいけない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。

(a) 技術的対策

- (ア) システム障害対策として、受託先のシステムは下記のような障害を回避できる冗長構成であること。
- 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
- (イ) 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。
- (ウ) 保存先のデータをアクセスできないことを想定して、診療に支障を来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こと。
- (エ) 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。バックアップ媒体については、特に規定しない。
- (オ) 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。
- (カ) 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。
- (キ) 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) 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こと。
- (イ) 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こと。
 - ・バックアップデータ格納用サーバの確保
 - ・フルバックアップ、差分バックアップ、増分バックアップ
- (ウ) 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ことが望ましい。

8.1.3. 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保存性の確保

ネットワークを通じて外部に保存する場合、診療録等を転送している途中でシステムが停止したり、ネットワークに障害が発生したりして正しいデータが外部の委託先に保存されないことも起こり得る。その際は、再度、外部保存を委託する医療機関等からデータを転送する必要がでてくる。そのため、委託する医療機関等は、医療機関等内部のデータを消去する等の場合には、外部保存を受託する機関において、当該データが保存されたことを確認してから行う必要がある。

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>(1) 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</p> <p>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機関は、以前のデータ形式や転送プロトコルを使用している施設が存在する間に対応を維持しなくてはならない。</p>	<p>項目なし</p>
<p>(2) ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと</p> <p>ネットワークや外部保存を受託する機関の施設の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。</p>	<p>(1) ネットワークや外部保存を受託する機関の設備の互換性を確保すること</p> <p>1. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。</p>

(a) 技術的対策

- (ア) 受託先システムの OS、データベースマネ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。
- (イ) 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第5章参照）でのデータ出力が可能であること。
 - (ウ) 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1日単位で1週間以上前の状態に戻せるように保管すること。
 - (エ) 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。

(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すること。

8.2. 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に関する事項

本節では経済産業省の「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」においてシステムベンダーが電子媒体による外部保存をネットワークを通じて行う情報処理事業者及びASP・SaaS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を対象に解説を行う。

＜経済産業省：医療情報受託ガイドラインとの対比＞

医療情報受託ガイドライン	本ガイドライン
7.1.医療情報に係る情報処理事業を受託する上で推奨される認証及び認定	【ベンダー側での対処事項なし】
7.2 情報資産管理	8.2.1 情報資産管理
7.2.1 資産台帳	【ベンダー側での対処事項なし】
7.2.2 情報の分類	8.2.1.1 情報の分類
7.3 組織的安全管理策（体制、運用管理規程）	【ベンダー側での対処事項なし】
7.4 医療情報の伝達経路におけるリスク評価	【ベンダー側での対処事項なし】
7.5 物理的安全対策	【ベンダー側での対処事項なし】
7.6 技術的安全対策	8.2.2 技術的安全対策
7.6.1 情報処理装置及びソフトウェアの保守	8.2.2.1 情報処理装置及びソフトウェアの保守
7.6.2 開発施設、試験施設と運用施設の分離	【ベンダー側での対処事項なし】
7.6.3 悪意のあるコードに対する管理策	8.2.2.2 悪意のあるコードに対する管理策
7.6.4 ウェブブラウザを使用する際の要求事項	【ベンダー側での対処事項なし】
7.6.5 第三者が提供するサービスの管理	【ベンダー側での対処事項なし】
7.6.6 ネットワークセキュリティ管理	【ベンダー側での対処事項なし】
7.6.7 電子媒体の取扱	【ベンダー側での対処事項なし】
7.6.8 情報交換に関するセキュリティ	8.2.2.3 情報交換に関するセキュリティ
7.6.9 医療情報システムに対するセキュリティ要求事項	8.2.2.4 医療情報システムに対するセキュリティ要求事項
7.6.10 アプリケーションに対するセキュリティ要求事項	8.2.2.5 アプリケーションに対するセキュリティ要求事項
7.6.11 暗号による管理策	8.2.2.6 暗号による管理策
7.6.12 ログの取得及び監査	8.2.2.7 ログの取得及び監査
7.6.13 アクセス制御方針	8.2.2.8 アクセス制御方針
7.6.14 作業アクセス及び作業IDの管理	8.2.2.9 作業アクセス及び作業IDの管理
7.6.15 作業者の責任及び周知	【ベンダー側での対処事項なし】

8.2.1. 情報資産管理

8.2.1.1 情報の分類

情報の保護の程度を識別するため、情報のそれぞれについて適切な分類を行い、外形的に分類が判断できるようにしておくことが必要である。

＜医療情報受託ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
(1) 情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。 【ベンダー側での対処事項なし】	項目なし
(2) 情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的を確認すること。 【ベンダー側での対処事項なし】	項目なし
(3) 預託される情報に対して分類にもとづいたリスク分析を実施すること。 【ベンダー側での対処事項なし】	項目なし
(4) リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。 【ベンダー側での対処事項なし】	項目なし
(5) 分類がわかるように情報にラベルをつけること（電磁的記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。	項目なし
(6) 各ラベルに応じた処理方式（保存、配送、複製、廃棄等）を定めること。	項目なし
項目なし	(1) 情報の処理について履歴を取得し、資産台帳等に記録することが望ましい。

(a) 技術的対策

追記事項なし

(b) 運用的対策

- (ア) どのような情報が管理されているかを提示できること。
- (イ) 情報処理の履歴を資産台帳等に記録することは、電子カルテ等については変更履歴を採取することに含まれると考えられる。

8.2.2. 技術的安全対策

医療情報システムの管理、運用における責任体制、扱い手順を確立すること。全ての手順を文書化し、定期的に改善することで、時々刻々と変化するリスクに対処すること。

8.2.2.1 情報処理装置及びソフトウェアの保守

情報処理装置の更新、補修などのために文書化された保守手順を確立し、適切に運用しなければならない。以下の管理策を適用すること。

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。	項目なし
(2) 変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。	項目なし
(3) 医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。	項目なし
(4) 情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施すること。	項目なし
(5) 情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。	<p>(1) 変更手順に含まれる事項には次のようなものが考えられる。</p> <ul style="list-style-type: none"> ・ 変更についての影響が及ぶ関係者への通知プロセス ・ 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等） ・ 申請承認プロセス ・ 変更試験プロセス ・ 変更作業に支障が発生した場合の復旧手順 ・ 変更終了確認プロセス ・ 変更に伴う影響を監視するプロセス、等

最低限のガイドライン	推奨されるガイドライン
(6) 不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。	項目なし
(7) 医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。	項目なし
(8) 潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。	項目なし
(9) 修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。	項目なし
(10) 保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「7.6.5 第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。 【ベンダー側での対処事項なし】	項目なし

(a) 技術的対策

追記事項なし。

(b) 運用的対策

(ア) リリースに関する情報を適宜提供すること

(イ) 変更履歴を管理すること

(ウ) リリース時にリリースに伴う障害が発生したときの復旧手順を提供すること

8.2.2.2 悪意のあるコードに対する管理策

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。	項目なし
(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 <ul style="list-style-type: none"> リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信） リスク評価の結果として必要であれば定期的にスキャンを実施 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 管理者以外による設定変更やアンインストールの禁止 	項目なし
(3) 一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止または隔離措置をとるといった対策が行われていること。	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。

8.2.2.3 情報交換に関するセキュリティ

医療機関等と情報処理事業者間の情報交換に関しては、互いの十分な合意の下に必要な対策を実施する必要がある。

＜医療情報受託ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>(1) 次の情報交換方法について予め合意しておくこと。</p> <ul style="list-style-type: none"> ・ 情報を電子媒体に記録して交換する際の手順 ・ 情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・ 情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・ 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順 	<p>項目なし</p>
<p>(2) 情報交換手順では搬送の形態によらず次の事項を確実にすること。</p> <ul style="list-style-type: none"> ・ 発送者、受領者を識別し記録すること。 ・ 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名、アプリケーションログオン時の確実な認証を行うこと。 ・ 交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと）。 ・ 交換された情報に悪意のあるコードが含まれていないことを確実にすること。 	<p>項目なし</p>
<p>(3) 物理的に情報を搬送する際には以下の対策を実施すること。</p> <ul style="list-style-type: none"> ・ 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。 ・ 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。 ・ 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。 ・ 配送業者等による電子媒体からの情報 	

最低限のガイドライン	推奨されるガイドライン
<p>の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。</p> <ul style="list-style-type: none"> 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。 <p>【ベンダー側での対処事項なし】</p>	
<p>(4) 電子的に情報を転送する際には以下の対策を実施すること。</p> <ul style="list-style-type: none"> 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 送受信する経路は適切な方法で傍受のリスクから保護されていること。 受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。 	項目なし

(a) 技術的対策

ベンダーは以下の4つの手順をユーザに提供すること。

- ・情報を電子媒体に記録して交換する際の手順
- ・情報をネットワーク経由で文書ファイル形式にて交換する際の手順
- ・情報をネットワーク経由でアプリケーション入力にて交換する際の手順
- ・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

(b) 運用的対策

追記事項なし。

8.2.2.4 医療情報システムに対するセキュリティ要求事項

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 運用システムの混乱を避けるため、開発用コードまたはコンパイラ等の開発ツール類を運用システム上に置かないこと。 【ベンダー側での対処事項なし】	項目なし
(2) 情報処理に不必要なファイル等を運用システム上におかないこと。 【ベンダー側での対処事項なし】	項目なし
(3) 業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。	項目なし
(4) 運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。	項目なし
(5) システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。	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。

8.2.2.5 アプリケーションに対するセキュリティ要求事項

アプリケーションにて情報を入力・出力する場合には、アプリケーションに起因する問題の発生を避けるため、以下の管理策を適用すること。

＜医療情報受託ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
(1) 提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。	(1) アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。
(2) アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。	項目なし
(3) アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。	項目なし
(4) アプリケーションにて医療事業者側の作業者を認証する情報（ID/パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。	項目なし
(5) アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。	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。

8.2.2.6 暗号による管理策

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。	項目なし
(2) 暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。 【ベンダー側での対処事項なし】	項目なし
(3) 電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとする。	項目なし
(4) 暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。	項目なし
項目なし	(1) 暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。
項目なし	(2) 暗号鍵の生成は耐タンパー性を有する IC カード、USB トークンデバイスといった安全な環境で実施することが望ましい。
項目なし	(3) 暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。
項目なし	(4) 電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できることが望ましい。

(a) 技術的対策

(ア) 暗号に関しては、6. 7節を参照のこと。

(イ) 電子署名に関しては、6. 8節を参照のこと。

(b) 運用的対策

追記事項なし。

8.2.2.7 ログの取得及び監査

医療情報システムの運用に関わるすべてのイベントに対する監査及び事故発生時の原因追及等のためにログを取得する必要がある。以下の管理策を適用すること。

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し、管理すること。	<p>(2) 監査ログに記録する事項としては次のようなものが考えられる。</p> <ul style="list-style-type: none"> 作業者情報（作業者 ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス） ファイル及びデータへのアクセス、変更、削除記録（作業者 ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） データベース操作記録（作業者 ID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容） 修正パッチの適用作業（作業者 ID、変更されたファイル） 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容） システム起動、停止イベント ログ取得機能の開始、終了イベント 外部デバイスの取り外し IDS・IPS 等のセキュリティ装置のイベントログ サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）
(2) 監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。 【ベンダー側での対処事項なし】	項目なし
(3) ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。	** ログを集中させ問題の検出を一箇所で確実にを行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理することが望ましい。
(4) 標準時刻に同期するための時刻提供元は信	項目なし

最低限のガイドライン	推奨されるガイドライン
<p>頼できる機関を利用すること。</p> <p>【ベンダー側での対処事項なし】</p>	
<p>(5) ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。</p> <ul style="list-style-type: none"> ・ログデータにアクセスする作業員及び操作を制限すること。 ・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。 ・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。 	項目なし
項目なし	<p>(1)* 監査ログを検証するため、作業員がアクセスした医療情報等を迅速に確認できるよう、作業員 ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備することが望ましい。</p>

*:医療情報受託ガイドライン P70 の(1)を指す

** :医療情報受託ガイドライン P70 の 12 行目の項目を指す

(a) 技術的対策

- (ア) アクセス記録、より厳密には監査証跡 (Audit Trail) の記録は、「個人情報へのアクセスの履歴の確認」、「医療機関等が説明責任を果たすために利用」、「副次的効果としての目的外アクセスの抑止」などを目的としている。これらの目的を満たすように実装すること。なお、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. 2.0」(JAHIS 標準文書 13-009) 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」(http://www.medical-it-link.jp/temporary/temp_1_445.pdf) も参考のこと。
- (イ) アクセスログへのアクセス制御を行う仕組みを実装すること。
- (ウ) 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すること。
- (エ) アクセスログの改ざんや故意による削除などを検知するため、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

- (ア) アクセスログの改ざんや消去から回復させるために定期的なバックアップを取ることが望ましい。

8.2.2.8 アクセス制御方針

業務上の要求事項及びセキュリティ上の要求事項にもとづいてアクセス制御方針を確立し、文書化する必要がある。以下の管理策を適用すること。

＜医療情報受託ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
(1) 情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること 【ベンダー側での対処事項なし】	項目なし
(2) 情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること 【ベンダー側での対処事項なし】	項目なし
(3) アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。 【ベンダー側での対処事項なし】	項目なし
(4) それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。	項目なし
(5) 業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。	項目なし
項目なし	(1) 作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。
項目なし	(2) 定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証することが望ましい。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

記事項なし。

8.2.2.9 作業者アクセス及び作業者 ID の管理

作業者による情報処理装置へのアクセス管理について以下の事項を規定すること。

作業者 ID について実施すべき安全管理策

＜医療情報受託ガイドラインの要求事項＞

最低限のガイドライン	推奨されるガイドライン
(1) 作業者は情報処理装置上においてユニークな作業者 ID により識別されること。 【ベンダー側での対処事項なし】	項目なし
(2) 作業者 ID を発行する際に、既存の ID との重複を排除する仕組みを導入すること。	項目なし
(3) 複数作業者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者 ID でログオンしてからグループ ID に変更する仕組みを利用すること。	項目なし
(4) 作業者 ID の発行は医療情報システムの管理に必要な最小限の人数に留めること。 【ベンダー側での対処事項なし】	項目なし
(5) 作業者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とすること。 【ベンダー側での対処事項なし】	項目なし
(6) 監視ログの監査時に作業者を確実に特定するため、作業者 ID は過去に使われたものを再利用しないこと。 【ベンダー側での対処事項なし】	項目なし
(7) 不要な作業者 ID が残っていないことを定期的に確認すること。 【ベンダー側での対処事項なし】	項目なし
項目なし	(1) アクセスを許可された作業者 ID のアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認することが望ましい。 【ベンダー側での対処事項なし】

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

特権 ID について実施すべき安全管理策

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 特権 ID の発行は必要な最小限のものに留めること。 【ベンダー側での対処事項なし】	項目なし
(2) 特権使用者に昇格可能な作業者 ID を制限すること。	項目なし
(3) 特権の使用時には作業実施内容を記録すること。	項目なし
(4) 管理端末以外からの特権 ID による直接ログインを禁止すること。	項目なし
項目なし	(1) システムの機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。
項目なし	(2) システムの機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改ざん、削除など不正な行為を防止することが望ましい。 【ベンダー側での対処事項なし】

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

パスワード管理について実施すべき安全管理策

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。 【ベンダー側での対処事項なし】	項目なし

最低限のガイドライン	推奨されるガイドライン
(2) 医療情報システムログオン用のパスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。	項目なし
(3) 医療情報システムログオン用のパスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。	項目なし
(4) 医療情報システムログオン用のパスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。	項目なし
(5) パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。	項目なし
(6) パスワード発行時には、乱数から生成した仮の医療情報システムログオン用のパスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。	項目なし
(7) パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実にすること。 【ベンダー側での対処事項なし】	項目なし
(8) パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。 【ベンダー側での対処事項なし】	項目なし
(9) パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。	項目なし
項目なし	(1) 作業者が医療情報システムログオン用のパスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、作業者が設定しようとする品質の低いパスワードを認めないシステムの導入等を検討することが望ましい。

最低限のガイドライン	推奨されるガイドライン
項目なし	(2) パスワードの品質基準としては、パスワードを十分に長くすること（8文字以上等）、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。 【ベンダー側での対処事項なし】

- (a) 技術的対策
追記事項なし。
- (b) 運用的対策
追記事項なし。

作業者のログオンについて実施すべき安全管理策

<医療情報受託ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
(1) 端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。	項目なし
(2) パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受け付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。	項目なし
項目なし	(1) 不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示することが望ましい。
項目なし	(2) 不正なアカウントの利用を防ぐため、作業者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限することが望ましい。
項目なし	(3) 認可されていない作業者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると作業者 ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の

最低限のガイドライン	推奨されるガイドライン
	情報を与えないようなメッセージのみの表現に留めることが望ましい。
項目なし	(4) 緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定することが望ましい。 【ベンダー側での対処事項なし】
項目なし	(5) ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号 (PIN)、パスワード等の記憶要素、生体情報 (バイオメトリクス) 等を組み合わせることが望ましい。

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

8.3. 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 ガイドラインに関する事項

本節では総務省の「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」においてシステムベンダーが電子媒体による外部保存をネットワークを通じて行う ASP・SaaS 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を対象に解説を行う。

＜総務省：ASP・SaaS 医療情報ガイドラインとの対比＞

ASP・SaaS 医療情報ガイドライン	本ガイドライン
3.3 外部保存における ASP・SaaS 事業者への要求事項	8.3 外部保存における ASP・SaaS 事業者への要求事項
3.3.1 外部保存に対する要求事項が求められる文書	【ベンダー側での対処事項なし】
3.3.2 真正性の確保における ASP・SaaS 事業者への要求事項＜表 3-12＞	8.3.1 真正性の確保における ASP・SaaS 事業者への要求事項
3.3.3 見読性の確保における ASP・SaaS 事業者への要求事項＜表 3-13＞	【ベンダー側での対処事項なし】
3.3.4 保存性の確保における ASP・SaaS 事業者への要求事項＜表 3-14＞	【ベンダー側での対処事項なし】
3.3.5 外部保存における ASP・SaaS 事業者への要求事項 (1) 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準における ASP・SaaS 事業者への要求事項 ＜表 3-15＞	8.3.2 外部保存における ASP・SaaS 事業者への要求事項
(2) 個人情報の保護における ASP・SaaS 事業者への要求事項＜表 3-16＞	【ベンダー側での対処事項なし】
3.4 ASP・SaaS の提供終了における ASP・SaaS 事業者への要求事項 ＜表 3-17＞	8.3.3 ASP・SaaS の提供終了における ASP・SaaS 事業者への要求事項

8.3.1. 真正性の確保における ASP・SaaS 事業者への要求事項

<ASP・SaaS 医療情報ガイドライン 表 3-12>

医療機関等以外に保存する際の要求事項

最低限のガイドライン	推奨されるガイドライン
① 利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（厚生労働省ガイドライン 7.1 C）	項目なし

(注) 項番は原文にはないが、順番に項番を付している。

(a) 技術的対策

(ア) アクセス制御機能及びなりすまし対策機能として利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための認証機能、特定の場所及び装置からの接続を認証する機能等を提供すること。

(b) 運用的対策

追記事項なし。

8.3.2. 外部保存における ASP・SaaS 事業者への要求事項

<ASP・SaaS 医療情報ガイドライン 表 3-15>

最低限のガイドライン	推奨されるガイドライン
項目なし	② 利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。また、運用管理規程を作成すること。ID・パスワードを用いる場合は、その運用管理方法と、パスワードの有効期限を規定に含めること。（厚生労働省ガイドライン 8.1.2 D(ウ)) ③ 同上(厚生労働省ガイドライン 8.1.2D(エ))

(注) 項番は原文にはないが、順番に項番を付している。

(a) 技術的対策

(ア) アクセス制御機能及びなりすまし対策機能として利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための認証機能、特定の場所及び装置からの接続を認証する機能等を提供すること。

(b) 運用的対策

追記事項なし。

8.3.3. ASP・SaaSの提供終了におけるASP・SaaS事業者への要求事項

<ASP・SaaS医療情報ガイドライン 表3-17>

ガイドライン
② 利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（厚生労働省ガイドライン 8.4.2）

（注）項番は原文にはないが、順番に項番を付している。

(a) 技術的対策

(ア) 利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）機能を提供すること。

(b) 運用的対策

追記事項なし。

9. 診療録等をスキャナ等により電子化して保存する場合について

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、厚労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、さらに厚労省ガイドライン9章で具体的な方法が規定された。従って厚労省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「3.1 7章および9章の対象となる文書について」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。

但し、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6.8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
9 診療録等をスキャナ等により電子化して保存する場合について	9 診療録等をスキャナ等により電子化して保存する場合について
9.1 共通の要件	9.1 共通の要件
9.2 診療等の都度スキャナ等で電子化して保存する場合	9.2 診療等の都度スキャナ等で電子化して保存する場合
9.3 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場合	9.3 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場合
9.4 調剤済み処方せんをスキャナ等で電子化し保存する場合について	9.4 調剤済み処方せんをスキャナ等で電子化し保存する場合について
9.5（補足）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	【ベンダー側での対処事項なし】

9.1. 共通の要件

(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要求事項＞

最低限のガイドライン	推奨されるガイドライン
<p>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たりすることで、スキャンによる電子化で情報が欠落することがないことを確認すること。</p> <ul style="list-style-type: none"> ・ 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンを行うこと。 ・ 放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「デジタル画像の取り扱いに関するガイドライン 3.0 版（平成 27 年 4 月）」を公表しており、参考にされたい。 ・ このほか心電図等の波形情報やポラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度が必要であり、その点に十分配慮すること。 ・ 一般の書類をスキャンした画像情報は汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がない精度であること、及びスキャンの対象となった紙等の破損や汚れ等の状況も判定可能な範囲であることを念頭に行う必要がある。放射線フィルム等の医用画像をスキャンした情報は DICOM 等の適切な形式で保存すること。 	<p>項目なし</p>

(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 サンプルングピッチ：200 μ m 以下
 - ② 空間分解能：CTF(0.25) \geq 0.9、CTF(0.5) \geq 0.8、CTF(1.0) \geq 0.7
ここで CTF(n)は、n lp/mm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要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>2. 改ざんを防止するため、医療機関等の管理責任者は以下の措置を講じること。</p> <ul style="list-style-type: none">・ スキャナによる読み取りに係る運用管理規程を定めること・ 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の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・ スキャナで読み取った際は、作業責任者(実施者または管理者)が電子署名法に適合した電子署名・タイムスタンプ等を遅滞なく行い、責任を明確にすること。なお、電子署名については「6.12 法令で定められた記名・押印を電子署名で行うことについて」を参照すること。	項目なし

(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。

(イ) 作成時期検証機能

スキャンされた画像の作成日時を担保するため、電子署名済みのスキャン画像に対して「一般財団法人日本データ通信協会」が認定するタイムスタンプを付与する機能を持つこと。

また、必要に応じて第三者が上記タイムスタンプを検証できる機能を持つこと。

なお、スキャン画像に対する、電子署名、タイムスタンプの付与やその検証に関する詳細は「6.8. 法令で定められた記名・押印を電子署名で行うことについて」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。ベンダー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要求事項>

最低限のガイドライン	推奨されるガイドライン
3. 情報作成管理者は、上記運用管理規程に基づき、スキャナによる読み取り作業が、適正な手続きで確実に実施される措置を講じること。	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、JIS²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 ISOTR15801 「エレクトロニックイメージングー電子的に保存された情報ー信頼度および信頼性の推奨事項」

² JISZ6016 「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「国税関係書類等の電子化文書取扱ガイドライン案」(<http://www.jiima.or.jp/pdf/050517zei.pdf>)

9.2. 診療等の都度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要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>1. 9.1 章 の対策に加えて、改ざんを防止するため情報が作成されてから、又は情報を入力してから一定期間以内にスキャンを行うこと。</p> <ul style="list-style-type: none">一定期間とは改ざんの動機が生じないと考えられる 1～2 日程度以内の運用管理規程で定めた期間で、遅滞なくスキャンを行わなければならない。時間外診療等で機器の使用ができない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行うこととする。	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無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。

9.3. 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場合

<安全管理ガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>9.1 章 の対策に加えて、以下の対策を実施すること。</p> <ol style="list-style-type: none"> 1. 電子化を行うに当って事前に対象となる患者等に、スキャナ等で電子化を行い保存対象とすることを掲示等で周知し、異議の申立てがあった場合はスキャナ等で電子化を行わないこと。 2. 必ず実施前に実施計画書を作成すること。実施計画書は以下の項目を含むこと。 <ul style="list-style-type: none"> ・運用管理規程の作成と妥当性の評価（評価は、大規模医療機関等にあつては、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）） ・作業責任者の特定。 ・患者等への周知の手段と異議の申立てに対する対応。 ・相互監視を含む実施の体制。 ・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） ・事後の監査人の選定と監査項目 ・スキャン等で電子化を行ってから紙やフィルムとの破棄までの期間及び破棄の方法 3. 医療機関等の保有するスキャナ等で電子化を行う場合の監査を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行うこと。 4. 外部事業者に委託する場合は、9.1 章 の要件を満たすことができる適切な事業者を選定すること。適切な事業者とみなすためには、少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認する必要がある。また、実施に際しては、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の監査を受けることを含めて、契約上に十分な安全管 	<p>項目なし</p>

理を行うことを具体的に明記すること。	
--------------------	--

(a) 技術的対策

追記事項なし。

(b) 運用的対策

追記事項なし。

【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あったので、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、電子署名とタイムスタンプを導入したが、過去にスキャンした画像ファイルに電子署名とタイムスタンプ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。

「9.1. 共通の要件」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、「9.3. 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場合」に従って再度、紙原本をスキャンするか、もしくは、紙原本を継続して保存する必要がある。

9.4. 調剤済み処方せんをスキャナ等で電子化し保存する場合について

<安全管理のガイドラインの要求事項>

最低限のガイドライン	推奨されるガイドライン
<p>9.1 の対策に加えて、以下の対策を実施すること。</p> <ol style="list-style-type: none"> 1. 調剤済み処方せんの電子化のタイミングにより、9.2 章 または 9.3 章 の対策を実施すること。 2. 電子化した調剤済み処方せんを修正する場合、「『元の』電子化した調剤済み処方せん」を電子的に修正し、「『修正後の』電子化した調剤済み処方せん」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』電子化した調剤済み処方せん」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せんの修正

(a) 技術的対策

(ア) 元の調剤済み処方せんを書面上で修正し再スキャンを行う場合

調剤済み処方せんのスキャン後、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せんを書面上で修正し、再スキャンして保存することができる。9.1 章に従い作業責任者の電子署名とタイムスタンプ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、「医療情報システムの安全管理のガイドライン第5版」に関するQ&Aの「Q-67」の回答にもあるように認められていない。

(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。

尚、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せん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ため、ベンダー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。尚、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せん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。

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://isms.jp/JIP-ISMS111-30.html>）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、たとえば、「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」といったところ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てみた例を示す。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。

(ア) 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、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、飲むように準備し、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（たとえば、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。

(イ) 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。

(ウ) 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ーを定めず、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	通常の本棚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

(エ) 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 JIPDEC の「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」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。

① 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、JIPDEC のガイドでは、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

② 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	通常の状態が発生する	1ヶ月に一度以上発生する

③ 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、たとえば、簡易的に次のような式で算出することができる。

$$\text{リスクの値} = \text{「資産の価値」} \times \text{「脅威の大きさ」} \times \text{「ぜい弱性の度合い」}$$

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

(オ) 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。

(カ) 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のが主体となる。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	物理コピーを毎日取る	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
			1	F2-A1-1	1	4
		T2-A1	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)

(キ) 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	残留リスクの具体的な内容
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くなる
	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ー1.4 版（2015 年 2 月）
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2603_01.html
- ・ 厚生労働省：保健医療福祉分野 PKI 認証局 認証用(人)証明書ポリシー1.3 版（2015 年 2 月）
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2603_02.html
- ・ 厚生労働省：保健医療福祉分野 PKI 認証局 認証用(組織)証明書ポリシー1.1 版（2010 年 3 月）
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/pki-policy/2203_03.html
- ・ ISO 17090 : Health Informatics Public Key Infrastructure（2008 年）
 - ・ Part 1: 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)
 - ・ Part 2: Certificate profile
(X.509 および RFC2459 に基づく証明書のプロファイル)
 - ・ Part 3: Policy Management of Certification Authority
(ポリシーの規定)
 - ・ Part 4: 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) タイムビジネス協議会(TBF)

<https://www.dekyo.or.jp/tbf/contents/seika/index.html>

- ・ タイムスタンプ長期保証ガイドライン（2006 年）
タイムスタンプを用いた電子文書の完全性維持のための手法が詳細に紹介された上で、タイムスタンプ局（TSA）、認証局（CA）の要件が整理されている。
- ・ 信頼されるタイムスタンプ技術・運用基準ガイドライン（2005 年）
トレーサビリティが確保され、信頼されるタイムスタンプを実現するための、各事業者における技術・運用基準について示されている。
- ・ 「電子署名検証ガイドライン」（2013 年）
署名検証システムあるいはサービスの利用者、調達者、開発者を対象としたガイドライン。特に長期署名の検証について基本概念から詳細要件までが解説されている。

(2) 電子商取引推進協議会(ECOM)

- ・ 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)

<https://www.jipdec.or.jp/archives/publications/J0004225>

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。

- ・ ECOM 長期署名プロファイル

RFC 3126 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、RFC 3126 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。

<https://www.jipdec.or.jp/archives/publications/J0004022>

<https://www.jipdec.or.jp/archives/publications/J0004024>

- ・ 長期署名フォーマットの相互運用性試験プロジェクト

ECOM 長期署名プロファイルこのプロファイルに基づいたテスト仕様を作成し、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を実施している。

<https://www.jipdec.or.jp/archives/publications/J0000406>

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

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

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 (下記参照)を採用している。

(4) 長期署名に関する国際標準等

- ・ RFC 3126 Electronic Signature Formats for long term electronic signatures

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。

- ・ ETSI TS 101 733 Electronic Signature Formats (CAAdES)

ETSI によって定められた長期署名のためのフォーマット。RFC 3126 とほぼ同じ内容となっている。

- ・ ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

ETSI によって定められた長期署名のための XML フォーマットを定義している。CAAdES の XML 版といえる。

(5) 長期署名に関する JIS 規格

- ・ JIS X 5092:2008 CMS 利用電子署名(CAAdES)の長期署名プロファイル

- ・ JIS X5093:2008 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 ECOM 長期署名プロファイル、JIS X 5092、5093 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 認証局証明書ポリシー」に基づくものを前提としている。

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

要件	JAHISの判断		本ガイドラインの記載		
			安全管理G Lの要求項 目	本ガイドラインの解説	
				技術的対策	運用的対策
C項 D項	技術的対策が必要	最低限 (必須)	再掲する	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	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。
				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	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。
		推奨	再掲する	同上。(最低限)の欄と同じ	
	全て病院の運用またはサービス提供に関わること	ベンダーとして行うことが有る	再掲する	“追記事項なし”と記載する	ベンダーとして病院に対して行うことを記載する
	ベンダーとして行うことが無い	要求項目を再掲し“【ベンダー側での対処事項なし】”と記載する	“追記事項なし”と記載する	“追記事項なし”と記載する	

付録—4. 作成者名簿

作成者（社名五十音順）

下野 兼揮	(株)グッドマン	
西田 慎一郎	(株)島津製作所	
西山 晃	セコム(株)	
深尾 卓司	セコム(株)	
藤木 俊樹	(株)ソフトウェア・サービス	
江崎 智	日本電気(株)	◎主査
近藤 誠	日本電気(株)	
藤咲 喜丈	日本光電工業(株)	
梶山 孝治	(株)日立製作所	
山岡 弘明	富士通(株)	
長谷川 英重	(一社)保健医療福祉情報システム工業会 特別委員	
茗原 秀幸	三菱電機(株)	

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	厚生労働省ガイドライン第4版・第4.1版、総務省ガイドライン、及び経済産業省ガイドラインに対応
2013年4月	第3.1版	総務省ガイドライン第1.1版、及び経済産業省ガイドライン第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	厚生労働省ガイドライン第5版に対応

(JAHIS標準 17-008)

2017年12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.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」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

(無断複写・転載を禁ず)