資料４

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

令和３年７月29日

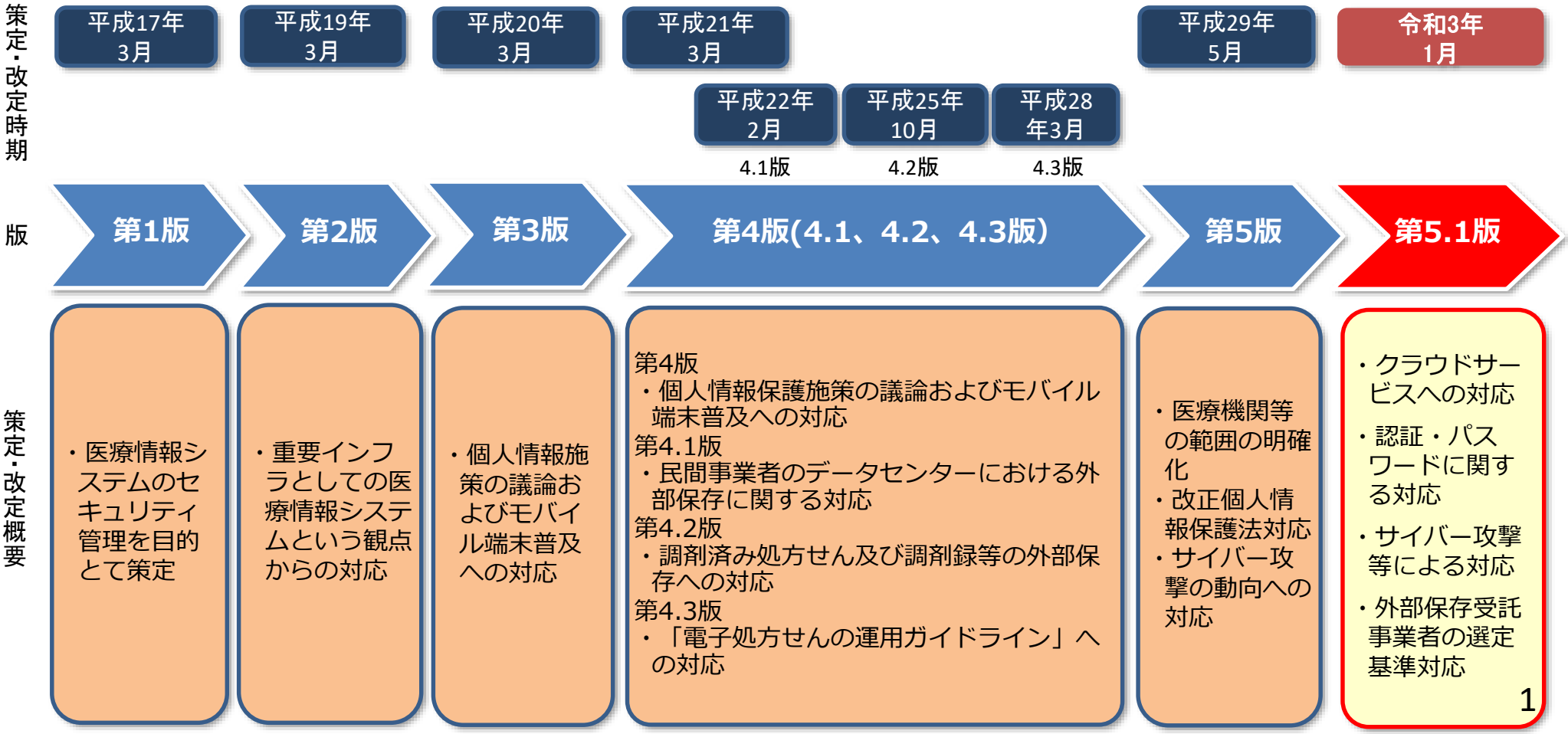
医療情報システムの安全管理に関するガイドラインについて

Ministry of Health, Labour and Welfare of Japan

医療情報システムの安全管理に関するガイドラインの経緯

安全管理ガイドラインの経緯

- 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第1版が策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。
- **今般第5.1版に改定され、令和3年1月29日に公表。**



医療情報システムの安全管理に関するガイドライン(第5.1版)改定について

○　背景

◆セキュリティ動向

「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)」（平成29年5月）から**２年以上が経過**しており、新たな技術的対策、各種指針※１等の改定なども行われてることから**最新化が必要**と考えられたこと。

※１　政府機関等の情報セキュリティ対策のための統一基準（平成30年度版）（サイバーセキュリティ戦略本部、2018年7月）
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5 版）改定版（サイバーセキュリティ戦略本部、2019年5月）　等

◆規制改革※２

「データヘルス改革を推進するに当たり、**クラウド技術の進展等の技術動向**を踏まえた上で、個別具体的な事例を収集し、それぞれについて、利用上の方針・留意点を整理し、**現行の医療情報システムの安全管理に関するガイドラインの改定素案を策定**する。（令和元年度検討・結論・措置）」とされたこと。

※２　規制改革実施計画　（閣議決定、令和元年6月21日）

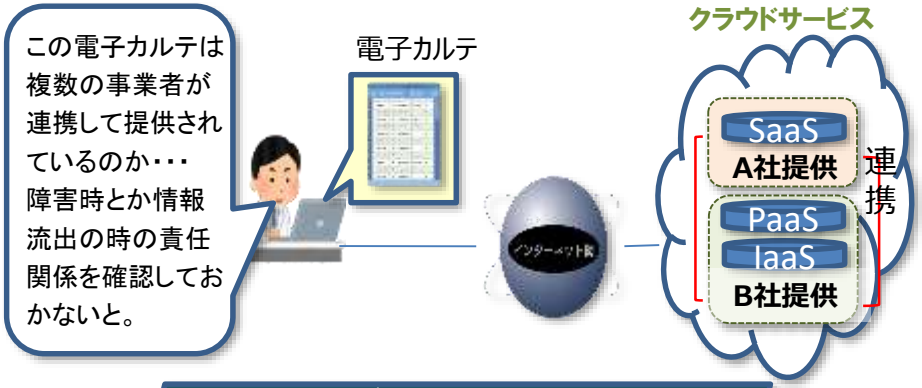
○　これまでの経緯

対応年月日	内　　容
令和元年10月～	令和元年医政局「『医療情報システムの安全管理に関するガイドライン』改定に向けた調査一式」にて、**ガイドライン改定素案の作成に向けた調査研究を実施**
令和２年３月９日	第1回健康・医療・介護利活用検討会にて、**医療等情報利活用WGにおいてガイドライン改定素案を審議することを了承**
同年　３月26日	第1回医療等情報利活用ＷＧでガイドライン改定素案を審議、事務局の整備を経て**パブコメ実施、改定を進めることを了承**（***改定素案の公表***）
同年　９月	パブコメ案について、健康・医療・介護利活用検討会、及び医療等情報利活用ＷＧの構成員からパブコメ前の意見収集・確認
同年　10月	**パブコメ実施**（10/2～11/2）
同年　12月	第6回医療等情報利活用ＷＧにて、**パブコメ結果、ガイドライン改定の意見照会**
令和３年１月29日	**正式改定（*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. 1版*）**

医療情報システム安全管理ガイドライン第5.1版　主な改定ポイント（概要）

1．クラウドサービスへの対応（追記）

- ◆ クラウドサービス事業者との責任分界に関する考え方を追記。
- ◆ 外部保存を受託する事業者の選定基準について、クラウドサービス事業者に関する内容も含め記載。



クラウドサービスの利用と責任関係の確認

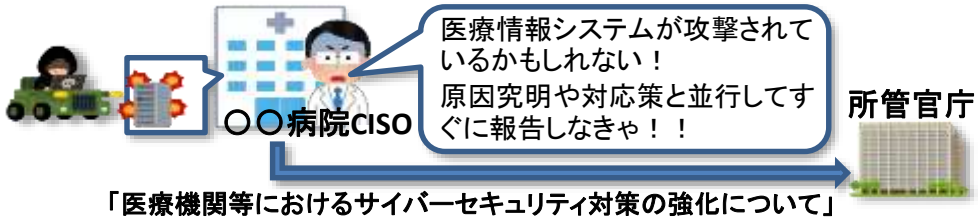
2．認証・パスワードの対応（見直し）

- ◆ 令和９年度時点での稼働が想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証又はこれに相当する対応を行うことを最低限のガイドラインとして記載。
- ◆ 安全と考えられる推定困難なパスワードに関する要件化。

多要素認証の安全性

3．サイバー攻撃等による対応（追記）

- ◆ 一定規模以上や地域で重要な機能の医療機関等について、情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT等）の整備等が強く求められることを記載。
- ◆ コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合等には、所管官庁への連絡等の必要な対応を行うほか、そのための体制を整備することを明記。

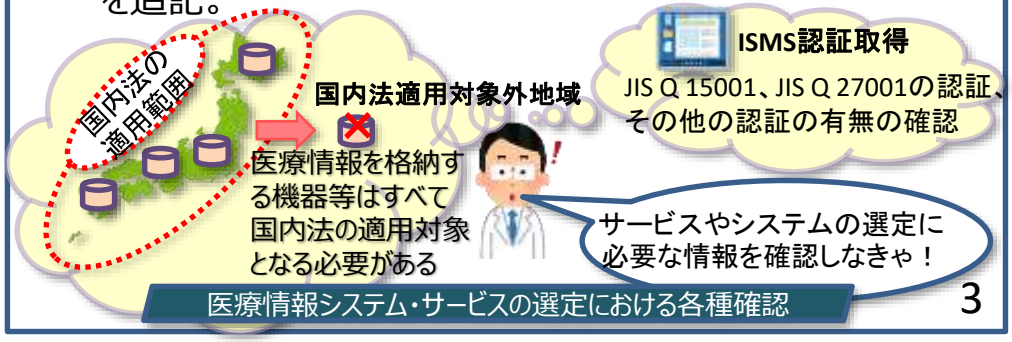


「医療機関等におけるサイバーセキュリティ対策の強化について」（医政局平成30年10月29日通知）に基づき報告

サイバー攻撃を受けた（疑い含む）場合の対応

4．外部保存受託事業者の選定基準対応（追記）

- ◆ 外部保存事業者の選定基準について、
  - ・ 行政機関等や民間事業者等の異なる基準を一本化。
  - ・ 医療情報を格納する機器等が、国内法の適用を受けることについて確認することを明記。
  - ・ 外部保存を受託する事業者の選定に当たっての確認事項を追記。



医療情報システム･サービスの選定における各種確認

医療機関のサイバーセキュリティ対策チェックリスト

- 医療機関のセキュリティ対策の一部として、医療機関における経営層向け、システム管理者向け、医療従事者向けのサイバーセキュリティ対策チェックリストについて、ガイドライン策定に係る通知の別添に追加する予定。
- ただし、ガイドラインはe-文書法、個人情報保護等への対応を行うためのセキュリティ管理なども含めて内容が多岐に渡る一方、本チェックリストはサイバーセキュリティ対策に特化した内容であることに留意。

経営層向けチェックリスト（一部抜粋）
【チェック項目数：18】

経営層向け　サイバーセキュリティ対策チェックリスト

記入者	日付

NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムの安全管理に関する方針について以下の内容を含めて策定されていますか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	予防	運用管理規程等において次の内容を定めていますか ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	
3	予防	経営者がサイバーセキュリティリスク（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃により損害を被るリスク）を経営リスクの1つとして認識されていますか	
4	予防	サイバー攻撃により医療情報が暗号化され、復元のための身代金を請求された医療機関等、公表されているサイバー攻撃の情報を定期的に確認されていますか	
5	予防	サイバーセキュリティ（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）にかかる外部監査を受けていますか	
6	予防	サイバーセキュリティリスク（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為や取組状況を外部に公開していますか	
7	予防	ウェブサイトの運営において、組織内部でセキュリティ対策を実施しているか確認した上で外部の組織によるサーバやネットワーク機器、ウェブアプリケーションに対する脆弱性検査（診断）を受けていますか	
8	予防	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）の現状を調査していますか	
9	予防	サイバーセキュリティ対策（コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況）の現状に基づいて、医療機関で可能な対策を実施していますか	

システム管理者向け向けチェックリスト（一部抜粋）
【チェック項目数：94】

システム管理者向け　サイバーセキュリティ対策チェックリスト

記入者	日付

NO	視点	チェック項目	チェック欄（○or×）
1	予防	中小企業の情報セキュリティ対策ガイドライン第3版「(6)詳細リスク分析の実施方法」や医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（5. 安全管理のためのリスクマネジメントプロセス）等を参考にして、リストアップした情報資産に対してリスク分析を実施しているか	
2	予防	医療情報システムベンダ及びサービス事業者から役割分担や医療情報システムの安全管理に関する評価、リスクアセスメントの結果、リスクに応じた技術的対策、運用管理規定等の情報を収集しているか	
3	予防	中小企業の情報セキュリティ対策ガイドライン第3版「(6)詳細リスク分析の実施方法」医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（5. 安全管理のためのリスクマネジメントプロセス）等を参考にして、リスク分析の結果に対して、医療情報システムの安全管理に関するガイドライン第5.1版 6.3章～6.12章に示す対策等を実施しているか	
4	予防	個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めているか	
5	予防	医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか	
6	予防	個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めているか	
7	予防	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティベンダーからの情報発信等）の収集を実施しているか	
8	予防	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関の他の情報システムへの影響を確認した上で、従業員に対応方法について指示をしているか	
9	予防	セキュリティに関する脅威や対策等について、収集した情報を他の医療機関等と共有しているか	
10	予防	セキュリティベンダー等と協力して脆弱性検査を実施し、既知の脆弱性の有無を点検しているか	
11	予防	情報機器の設置場所や記録媒体の保存場所について、施錠管理、盗難防止対策を行っているか	
12	予防	医療情報システムへのアクセスにおける利用者の識別・認証を行っているか	
13	予防	利用者の識別・認証にユーザID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施しているか	
14	予防	利用者の識別・認証にIC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意しているか	
15	予防	利用者の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行っているか。また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、アクセス権限の変更を行うことを、運用管理規程で定めているか。なお、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、操作記録を行うことでアクセス管理を実施しているか	
16	予防	アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施しているか	
17	予防	アクセスログの記録に用いる時刻情報は、日本標準時等の信頼できるものを利用しているか また利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保っているか	

医療従事者向け向けチェックリスト（一部抜粋）
【チェック項目数：10】

医療従事者向け　サイバーセキュリティ対策チェックリスト

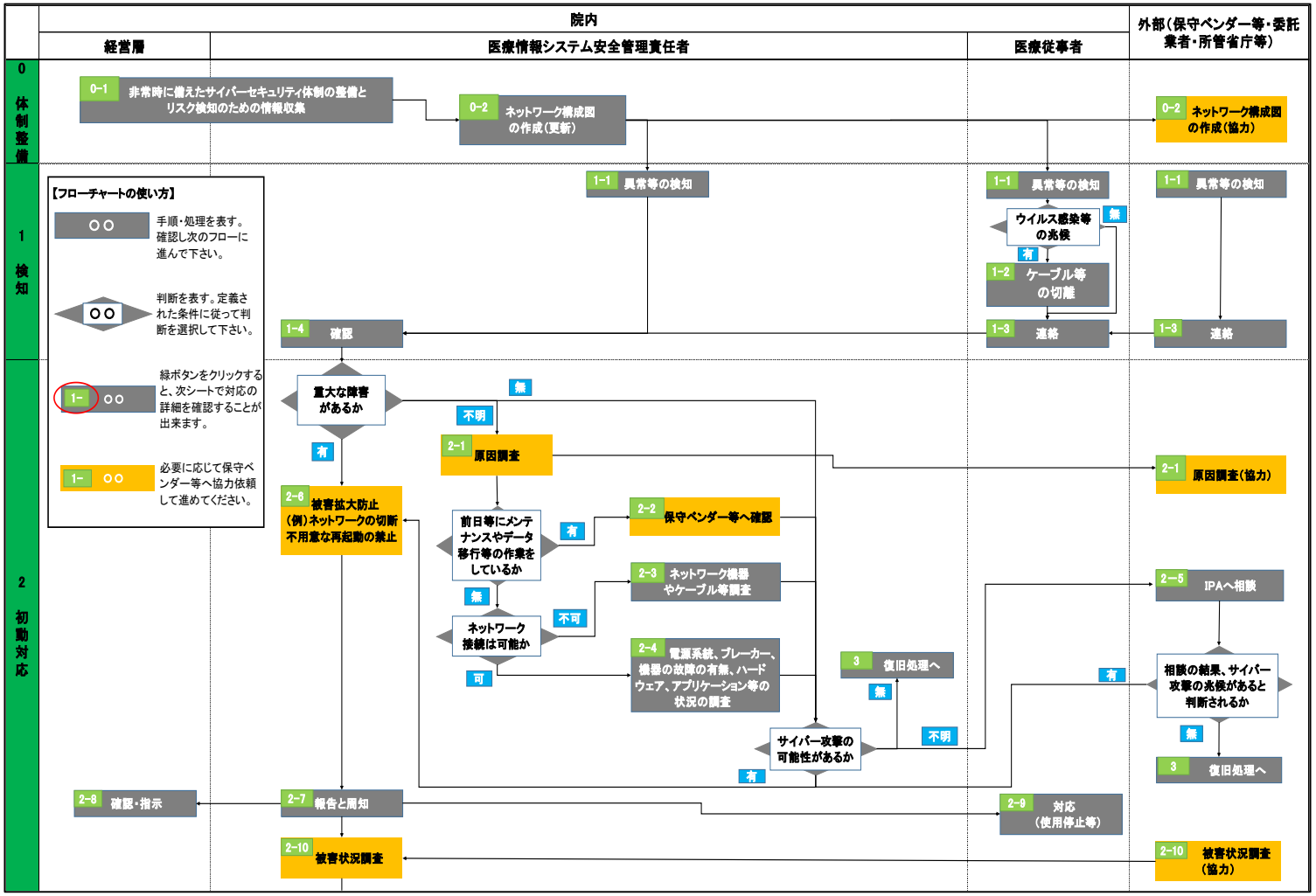
記入者	日付

NO	チェック項目	チェック欄（○or×）
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っていますか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用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（画面が他人から見えないようにするために操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体の使用を使用していないか又は業務上、外部媒体の使用が必要な場合は事前申請とし、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）に等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	

医療情報システム等の障害発生時の対応フローチャート

- 医療機関等での対応体制の整備に資するよう、医療情報システム等の障害発生時の対応フローチャートについて、ガイドライン策定に係る通知の別添に追加する予定。
- 各医療機関の個別の状況に応じて適宜加工できるよう、編集可能なファイルとして提供する。

【医療機関における医療情報システム障害発生時の対応フローチャート（一部抜粋）】



医療情報システムの安全管理に関するガイドラインの次回改定に向けた現行の課題

○ 短期的な課題（年度内の結論・措置を想定）

1．今後求められる情報ネットワークの仕組みについて

・HL7 FHIRの規格を用いてAPIで接続する仕組みの実現に向けて、アプリケーションごとに外部の利用者（自院職員以外）の認証・認可を行うための考え方等について整理することが必要。

2．医療現場におけるスマートフォン等の活用、BYODについて

・個人情報の目的外利用や流出・漏洩等への対策を前提とした医療現場におけるスマートフォン等の活用、BYOD（Bring Your Own Device）への指摘があることを踏まえ、記載の検討が必要。

3．ガイドラインの記載の見直し

・本ガイドラインの記載は、制度的な要求事項を主とし、技術的な記載や措置は例示として分けて整理すること、特に、ISMSの実践（リスク分析の結果）にもとづき、適用する安全対策が変わること（必ずしも例示の全てを求めるものではないこと）を分かりやすく記載することが必要ではないか。

・規制改革実施計画（令和３年６月18日閣議決定）において、

- 電子署名の利用が可能である旨を医師法等の法令を踏まえ、規定する。その際、医療現場のニーズを踏まえ、電子署名の活用促進につながるようなガイドラインの見直しを検討する。
- 医療機関や関係者が電子カルテ等医療情報を授受するに当たって当事者が講ずべき安全措置やセキュリティ対策と併せて、外部ネットワーク等が活用可能であることを分かりやすく周知する。

等の指摘があることを踏まえ、記載を整理することが必要。

○ 中・長期的な課題

4．今日的なセキュリティ対策の記載について

・ゼロトラストセキュリティを含め、今日的なセキュリティ対策について記載が必要（既存のセキュリティガイドラインを参照しつつ、本ガイドラインで適宜例示を示すことも検討）。

5．ガイドラインの対象の整理

・介護事業者、訪問看護ステーション等で取り扱う医療情報について、ガイドラインでの対応を整理することが必要。