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）

安全管理ガイドラインの経緯

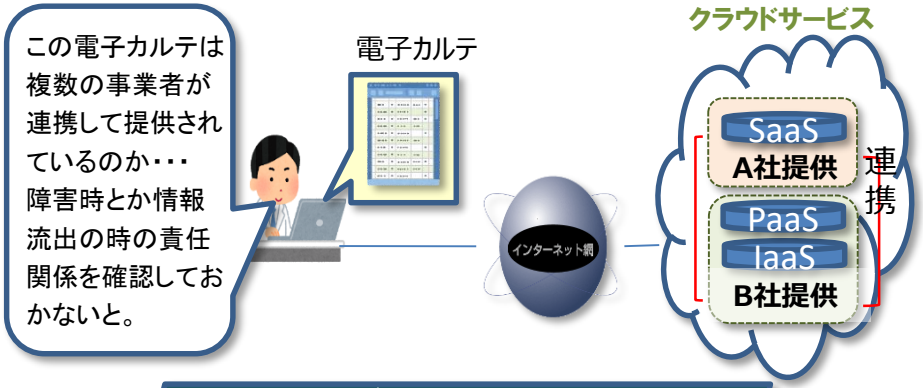
- 医療情報システムの安全管理に関するガイドラインは、e-文書法対応、個人情報保護対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第1版が策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。
- **今般第5.1版に改定され、令和3年1月に公表。**

	平成17年3月	平成19年3月	平成20年3月	平成21年3月	平成22年2月	平成25年10月	平成28年3月	平成29年5月	令和3年1月
策定・改定時期									
版	第1版	第2版	第3版	第4版(4.1、4.2、4.3版)	4.1版	4.2版	4.3版	第5版	第5.1版
策定・改定概要	・医療情報システムのセキュリティ管理を目的とて策定	・重要インフラとしての医療情報システムという観点からの対応	・個人情報施策の議論およびモバイル端末普及への対応	第4版 ・個人情報保護施策の議論およびモバイル端末普及への対応 第4.1版 ・民間事業者のデータセンターにおける外部保存に関する対応 第4.2版 ・調剤済み処方せん及び調剤録等の外部保存への対応 第4.3版 ・「電子処方せんの運用ガイドライン」への対応				・医療機関等の範囲の明確化 ・改正個人情報保護法対応 ・サイバー攻撃の動向への対応	・クラウドサービスへの対応 ・認証・パスワードに関する対応 ・サイバー攻撃等による対応 ・外部保存受託事業者の選定基準対応

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

- ◆ 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

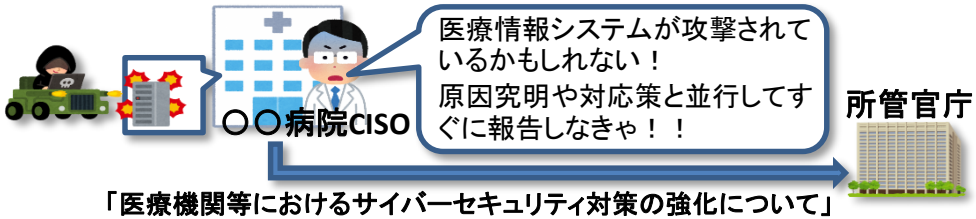
2．認証・パスワードの対応

- ◆ 令和９年度時点で稼働してい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

- ◆ 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）の整備等を要請。
- ◆ 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、所管官庁への連絡等への必要な対応、そのための体制を整備構築等を明記。

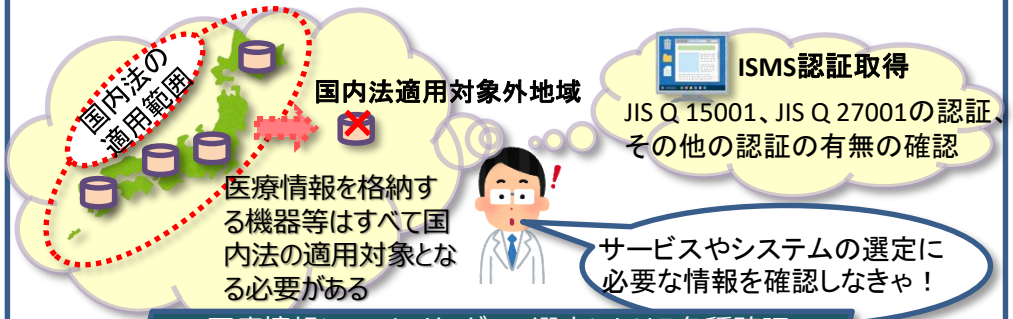


「医療機関等におけるサイバーセキュリティ対策の強化について」（医政局平成30年10月29日通知）に基づき報告

サイバー攻撃を受けた場合の対応

4．外部保存受託事業者の選定基準対応

- ◆ 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の確認を追記
  - ・外部保存を受託する事業者選定の確認事項を追記



医療情報システム・サービスの選定における各種確認