医療情報システムの安全管理に関するガイドラインの概要

医療情報システムの安全管理に関するガイドライン(安全管理ガイドライン)の目的

安全管理ガイドラインは、医療情報システムの安全管理やe-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。

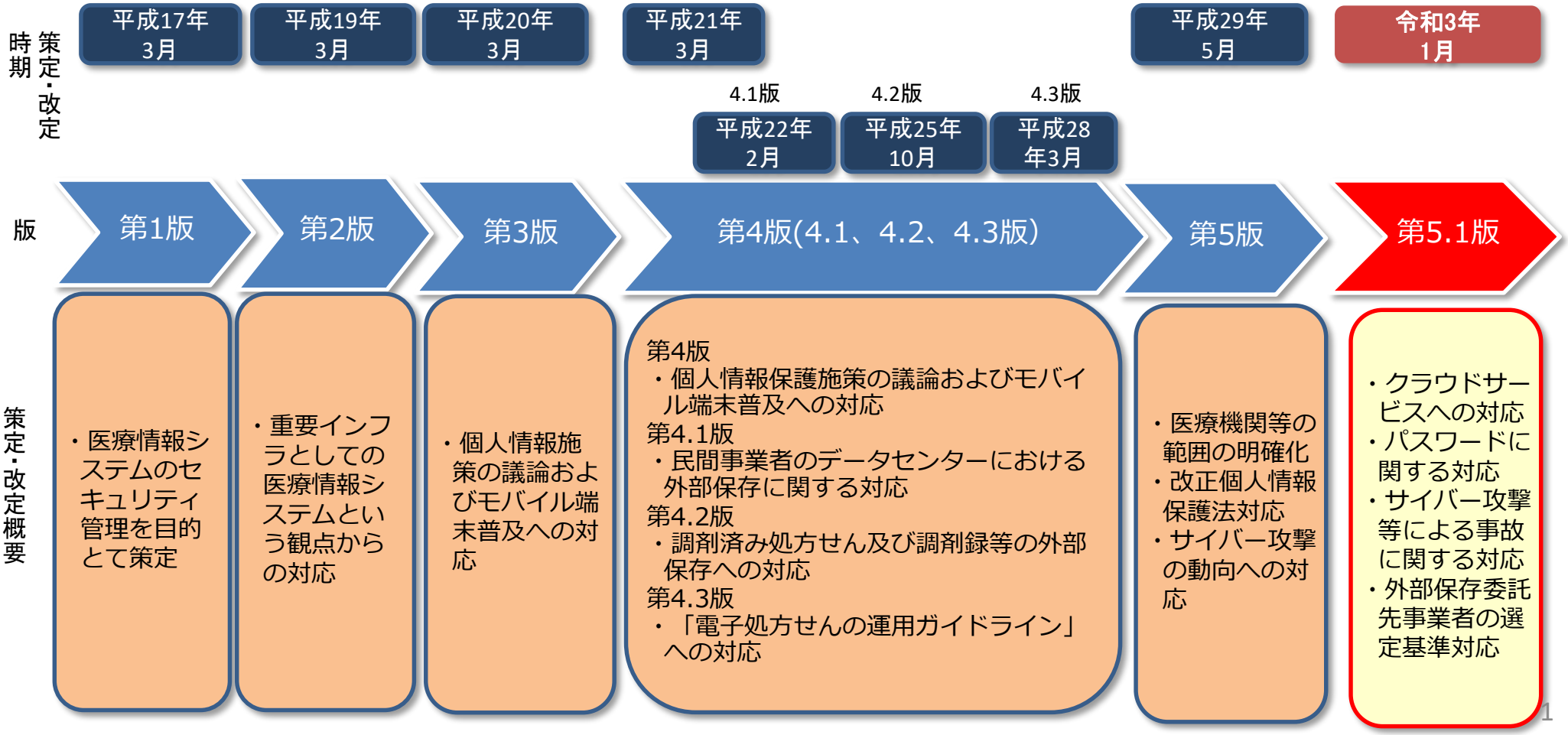
安全管理ガイドライン策定の背景

- ◆ 医療情報（法令対象外）を電子的に取り扱うことが技術的に可能となった。
  →作成や保存に関する具体的な要件を示すことが必要となった
- ◆ 医師法、医療法等の法令で、原則として書面での作成又は保存が義務付けられている文書を電子的に取り扱うことが可能となった。
  →そのための安全管理に関する指針が必要
- ◆ 技術の進展により医療機関等の内部ではなく、外部の施設に電子的に保存することが可能となった。
  →外部保存に必要な指針が必要

医療情報システムの安全管理に関するガイドラインとして
医療機関等に求められる対策を示す。

安全管理ガイドラインの経緯

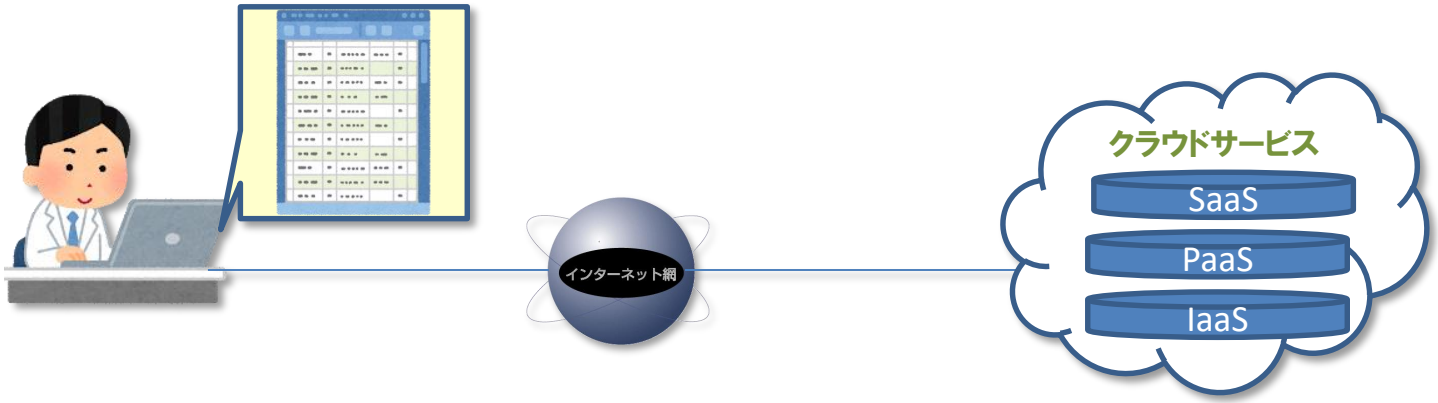
- 医療情報システムの安全管理に関するガイドラインは、e-文書法対応、個人情報保護対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第1版が策定。
- 以降、各種制度の動向や情報システム技術の進展等に対応して改定。
- 今般第5.1版に改定され、令和3年1月29日に公表。



第5.1版における主な改定内容～クラウドサービスへの対応

クラウドサービスへの対応

- ◆ 医療情報システムにおけるクラウドサービスの利用状況を鑑みて、医療機関等がクラウドサービスを用いる際に、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盛り込みました（「4.3. 例示による責任分界点の考え方の整理」「(4) オンライン外部保存を委託する場合」）
- ◆ 外部保存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ました（「8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」）



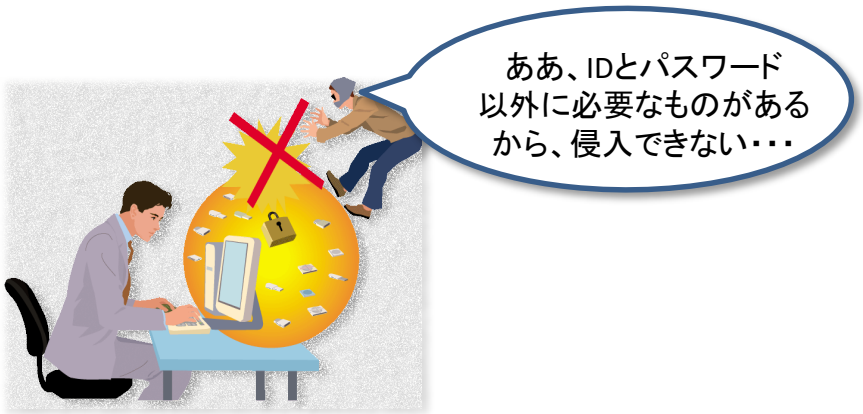
医療情報システムにおけるクラウドサービスの利用イメージ

第5.1版における主な改定内容～パスワードに関する対応～

パスワードに関する対応

- ◆ 医療情報システムに用いる認証方式について、二要素認証の導入を促進するため、令和９年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこととしました（「6.5.　技術的安全対策」「C.12」）
- ◆ 最近のIDとパスワードの認証による場合、近時の研究成果などを踏まえて、安全と考えられるパスワードに関するルールを定めました（「6.5. 技術的安全対策」「C.13」）

IDとパスワードのみによる認証の場合



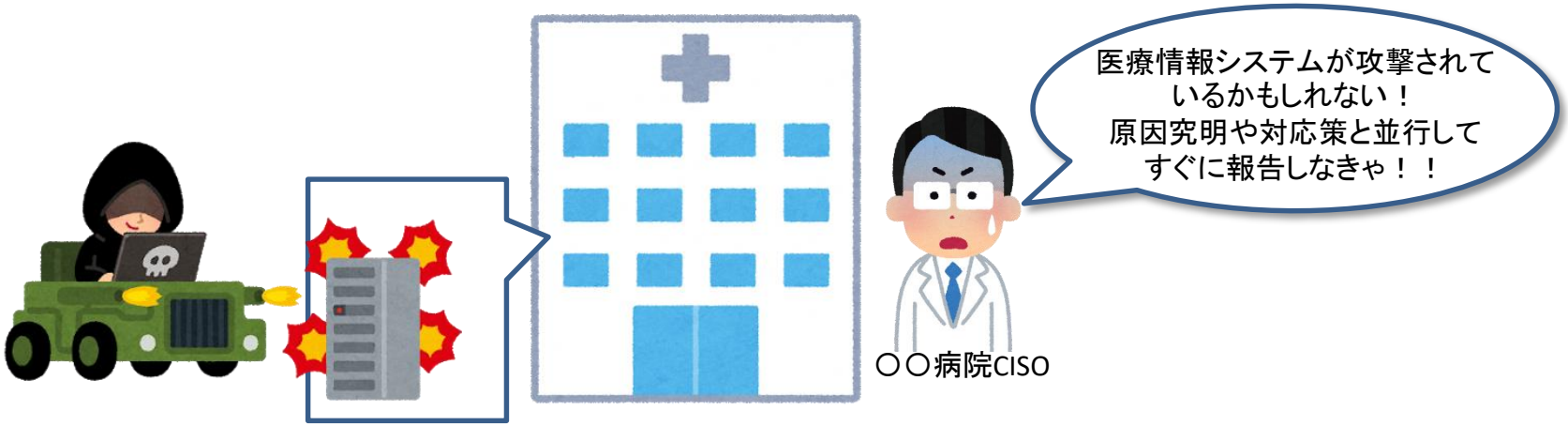
IDとパスワード以外の要素が必要な認証の場合

ID/パスワードのみによる認証と多要素認証の安全性の比較

第5.1版における主な改定内容～サイバー攻撃等による事故に関する対応～

サイバー攻撃等による事故に関する対応

- ◆ 非常時やサイバー攻撃を受けた場合のセキュリティ体制の構築等の必要性が示されました。特に、一定規模以上や地域で重要な機能を果たしている医療機関等においては、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）を整備するなどが強く求められることを示しました（「6.10. 災害、サイバー攻撃等の非常時の対応」「B.(4)」）
- ◆ 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）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、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としました（「6.10. 災害、サイバー攻撃等の非常時の対応」「C.5」）

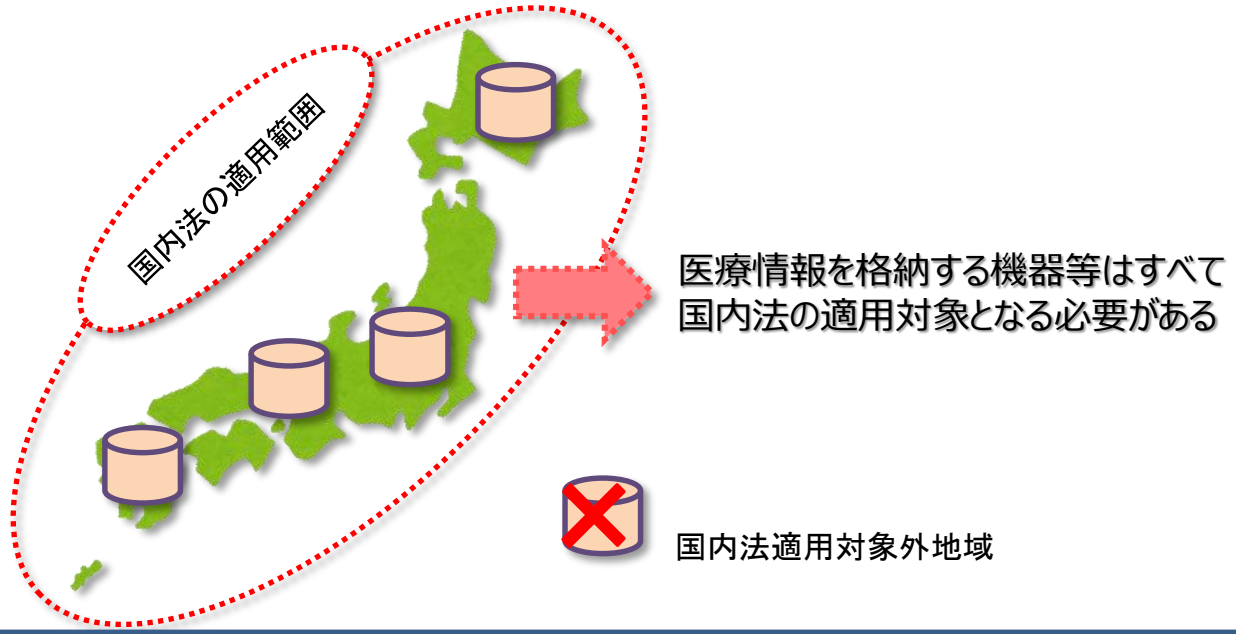


サイバー攻撃を受けた（疑い含む）場合の対応

第5.1版における主な改定内容～外部保存委託先事業者の選定基準対応～

外部保存委託先事業者の選定基準対応

- ◆ 外部保存を受託する事業者の選定基準について、サービス提供主体が行政機関等や民間事業者等の違いにより、異なる基準を設けていた点について、一本化しました（「8.1.2. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」）
- ◆ 外部保存を受託する事業者の選定基準として、保存された情報を格納する機器等が、国内法の適用を受けることを確認することを求めることとしました（「8.1.2.外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」「C.2(8)」）
- ◆ 外部保存を受託する事業者選定に際して、確認すべき事項を定めました（「8.1.2.外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準」「C.2(9)」）



医療情報が保存された情報を格納する機器等に国内法適用に関するイメージ