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

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及び主な改定内容

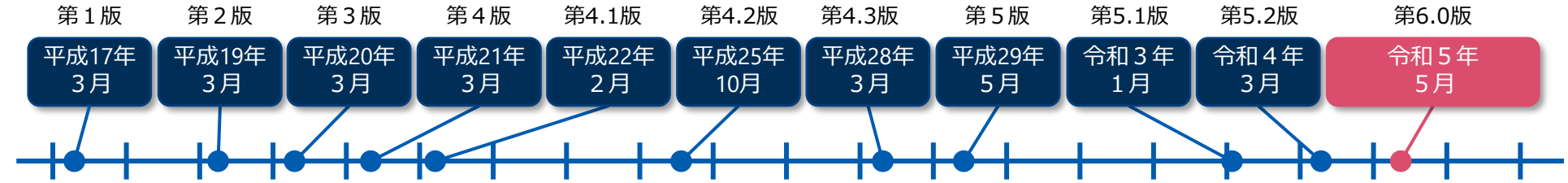
厚生労働省 医政局

特定医薬品開発支援・医療情報担当参事官室

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
策定の背景及び改定の経緯

- 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版を策定。
- 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、**令和５年５月に第6.0版を策定。**



版	第１版、第２版、第３版	第４版（第4.1版、第4.2版、第4.3版）	第５版（第5.1版、第5.2版）	第6.0版
策定・改定概要	**第１版** • 医療情報システムのセキュリティ管理を目的とて策定 **第２版** • 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 **第３版** • 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	**第5版** • 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 **第5.1版** • 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 **第5.2版** • ２省（総務省、経産省）GL等との整合性 • 改正個人情報保護法への対応 等 • 医療機関へのサイバー攻撃の多様化・巧妙化 • 「規制改革実施計画」等への対応 • 電子署名 • 外部ネットワーク 等	**第6.0版** 全体構成の見直し • 概説編、経営管理編、企画管理編、システム運用編の４編に再構成 • Q&Aの充実 等 技術的な動向 • 外部委託、外部サービスの利用に関する整理 • 情報セキュリティに関する考え方の整理 • 新技術、制度・規格の変更への対応 等

第5.2版 から 第6.0版 への改定方針

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化により、概ねすべての医療機関等において、本ガイドラインに記載されているネットワーク関連のセキュリティ対策が必要となる。これを踏まえ、第6.0版への改定では、第5.2版で中長期的に検討を継続することとした論点を中心に、全体構成の見直しとともに検討した。

○ 外部委託、外部サービスの利用に関する整理

- クラウドサービスの特徴を踏まえたリスクや対策の考え方
- 医療機関等のシステム類型別に対応した責任等の整理　　等

○ 情報セキュリティに関する考え方の整理

- ネットワーク境界防御型思考／ゼロトラストネットワーク型思考
- 災害、サイバー攻撃、システム障害等の非常時に対する対応や対策　　等

○ 新技術、制度・規格の変更への対応

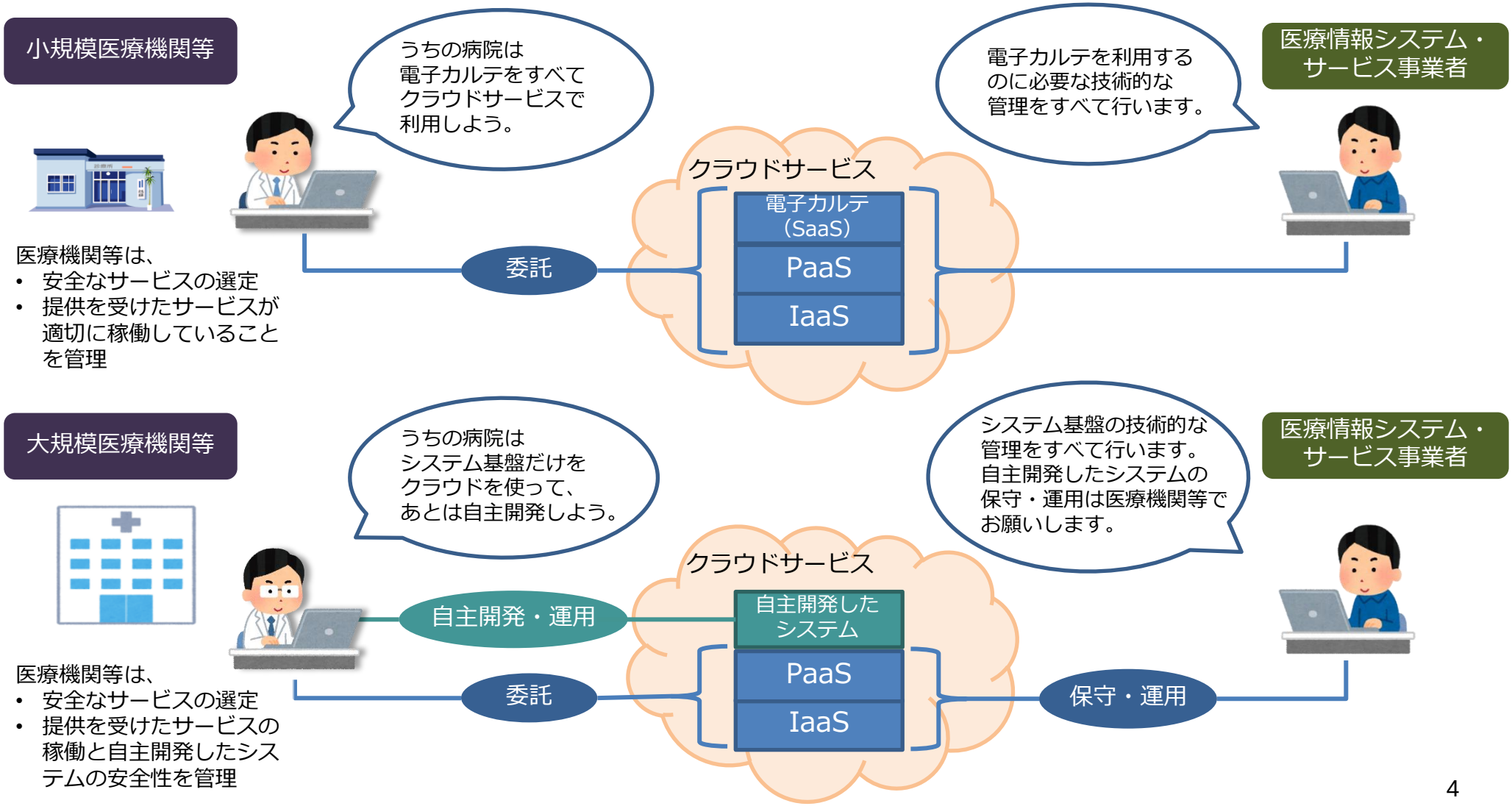
- 本人確認を要する場面での運用（eKYCの活用）
- オンライン資格確認の導入に必要なネットワーク機器等の安全管理措置
- 新たなネットワーク技術（ローカル５G）の利用可能性、利用場面
- 医療情報の共有・提供に関連する法令等の規定や技術・規格の動向

○ 全体構成の見直し

- 概説編（Overview）、経営管理（Governance）編、企画管理（Management）編、システム運用（Control）編の４編構成（各編は数十ページ程度、第5.2版の文章等を全面的に精査）
  - ※ 第5.2版 6.12章（電子署名）は、策定時に詳細な検討・調整を行ったため、原則、現行版を踏襲
- 概要、Q&A、用語集、特集（小規模医療機関等向け、サイバーセキュリティ）等、支援文書の整備

外部委託、外部サービスの利用に関する整理

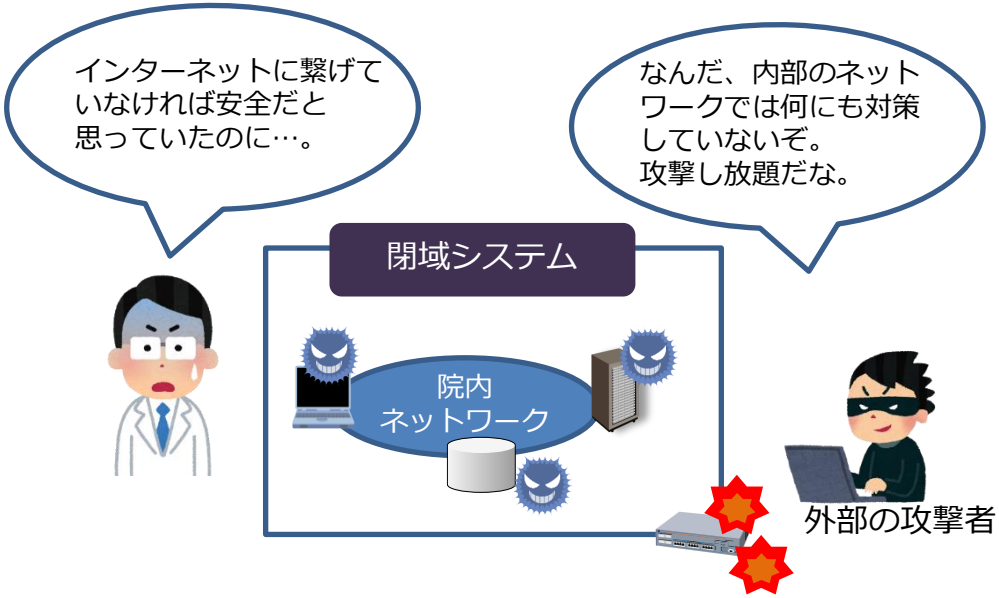
◆ 医療機関等のシステム類型別に対応した責任等の整理やクラウドサービスの特徴を踏まえたリスクや対策の考え方を整理しました。



情報セキュリティに関する考え方の整理
-ネットワーク境界防御型思考／ゼロトラストネットワーク型思考-

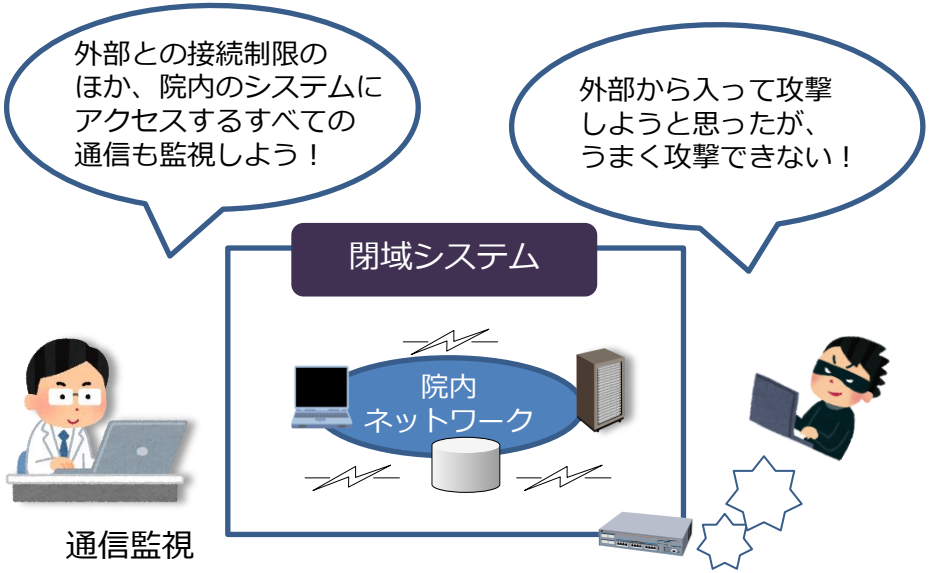
- ネットワークに関する整理を行うほか、対策のあり方として、ゼロトラストネットワーク型思考を取り入れることの有用性について示しました。
- 境界防御型思考とゼロトラスト思考をうまく組み合わせて対応することについて示しています。

サイバー攻撃の巧妙化などにより、閉域網にある医療情報システムおいても、外部からの侵入のリスクが高まっています。



境界防御だけに対策を頼っている場合

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。



ゼロトラスト思考を入れた対策をとっている場合

情報セキュリティに関する考え方の整理
-災害、サイバー攻撃、システム障害等の非常時に対する対応や対策-

- 災害、サイバー攻撃、システム障害等の非常時に対する対応や対策について整理し、記載しました。
- BCPへの対応やバックアップなど具体的な対策は、場面に応じて検討し整理することとしています。

「非常時への対応」と言っても、災害とサイバー攻撃とシステム障害では対応内容が違うんだ！

医療機関等の業務継続の考え方も、非常時の場面ごとに考えないと…。

大規模災害に備えたバックアップは分散して保存しないと…。

ランサムウェアなどの対応には、書き換えられない複数のバックアップが必要だな・・・

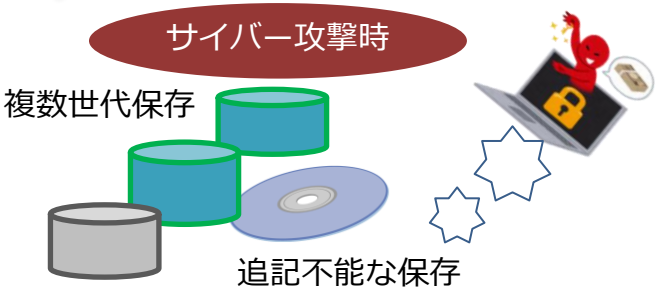
障害対策では、システムが止まらないすぐに復旧できる対応が必要だな。

非常時の場面に応じた対策の必要性

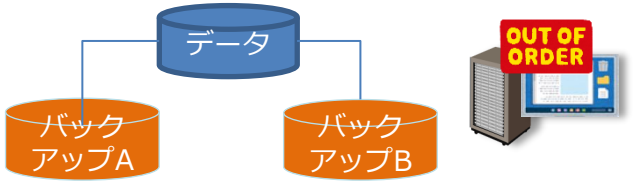
非常時場面ごとのバックアップの考え方の違い（例）

災害時

サイバー攻撃時



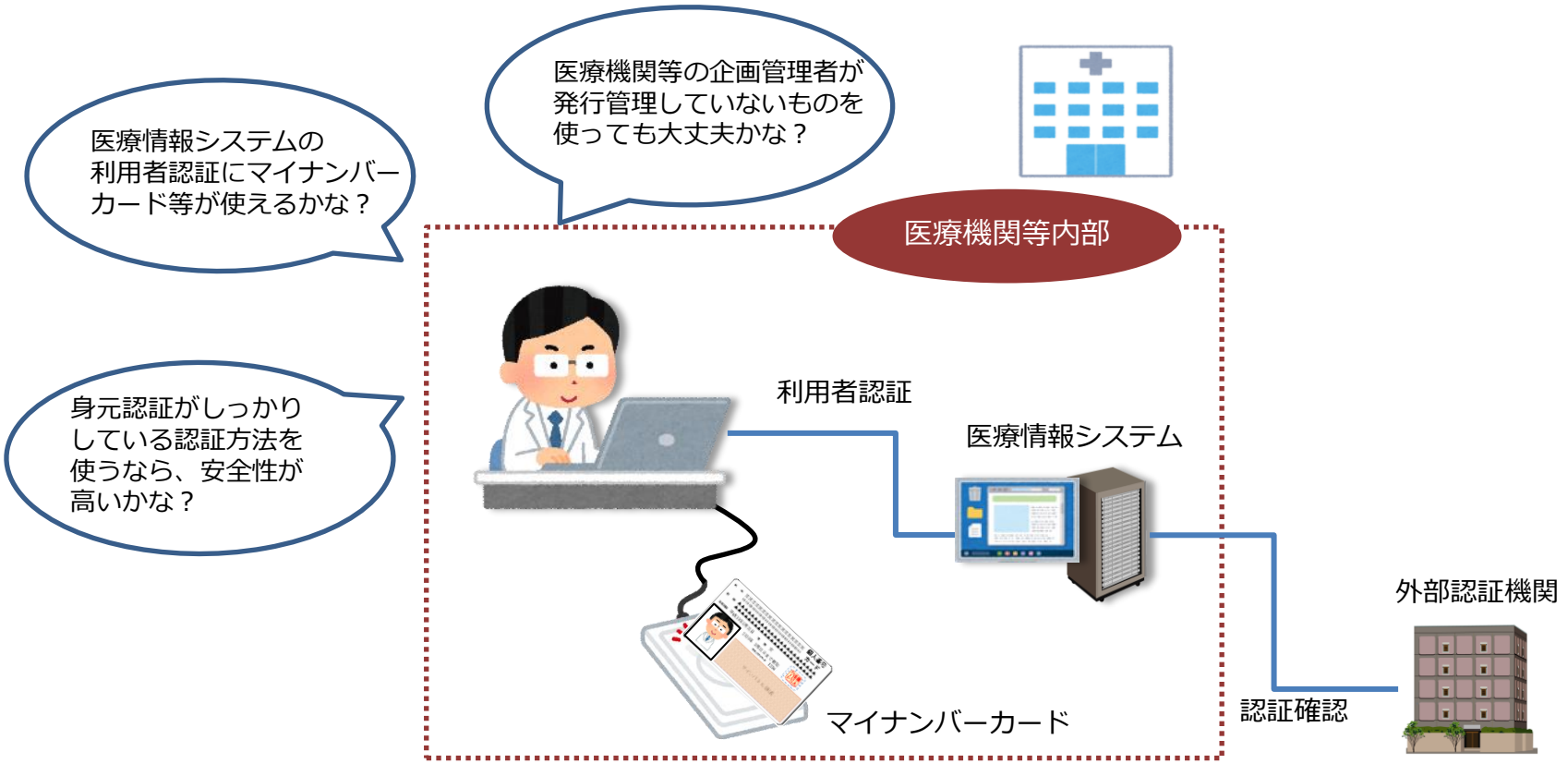
システム障害時



システム・保存機器の二重化

新技術、制度・規格の変更への対応
-本人確認を要する場面での運用（eKYCの活用） -

◆ 近時、身元確認をオンラインで行うための仕組みして各種サービスで用いられるeKYCについて、医療情報システムにおける本人確認を要する場面での活用について検討を行い、Q&Aに留意点等を記載しました。



医療情報システムにおける認証方法にeKYCの活用する際の留意点

eKYC：electronic Know Your Customer（電子本人確認）

全体構成の見直し

医療機関等の様々な規模と多様なシステム構成・サービス提供形態を踏まえ、安全な情報資産管理を基礎とし、意思決定・方針策定・戦略立案（Governance）、企画管理・システム運営（Management）、管理方法・運用手段（Control）の３つの視点で整理。

概説 編 Overview	ガイドラインの各編を読むに際して、まずはじめに、前提として必要な知識や各編の基本的な概要をまとめる。	・ガイドラインの目的 ・対象とする情報・文書・システム ・関連する法令等の規定との関係や経緯 ・各編の位置付けと目次構成、概要 等
経営管理 編 Governance	組織の経営方針を策定し、情報化戦略を立案する経営管理層に必要な考え方や関連法制度等をまとめる。	・取り扱う情報の重要性と関連法規 ・情報資産管理や情報システム運用に伴い生じる責任・責務 ・情報システムの有用性と安全管理 等
企画管理 編 Management	経営方針・情報化戦略に基づき、システム利用者・管理者・事業者で情報資産を運営、情報化を管理する考え方や方法論をまとめる。	・情報資産管理体制と責任分界 ・リスクアセスメントと対策 ・情報の種類に応じた管理・監査 ・非常時の対応と非常時への対策 等
システム運用 編 Control	安全な情報資産管理やシステム運用を実現するために、関連法制度を遵守した考え方とその実装手法、活用する技術等、具体的な考え方や技術をまとめる。	・個人情報保護法、e-文書法、電子署名法等により求められる技術 ・システム利用者、クライアント側/サーバ側/インフラ領域等それぞれで活用する安全管理対策・措置技術 等

別添 資料 Appendix

- Q&A
- 用語集
- 診療所、薬局等の小規模医療機関等向けの特集
- 医療機関におけるサイバーセキュリティに関する特集
- ガイドラインの改定と関連法規の遷移
- ガイドラインと関連法規との関係性、遷移
- 第5.2版から第6.0版への各項目の移行対応表
- 第6.0版の各編の各項目の相関表
- サイバーセキュリティ対策チェックリスト
- システム障害発生時の対応フローチャート　等

医療機関等の特性に応じたガイドライン参照箇所　（１／２）

◆医療機関等における専任のシステム運用担当者の有無や導入している医療情報システムの形態の違いに応じて、ガイドラインの参照パターンを、以下の４つに分類しています。

	医療情報システムを 医療機関等に保有し運用 （いわゆるオンプレミス型）	医療情報システムを 医療機関等に保有しない運用 （いわゆるクラウドサービス型）
システム運用専任の 担当者が いる	Ⅰ	Ⅱ
システム運用専任の 担当者が いない	Ⅲ	Ⅳ

補）なお、カルテ等の医療情報は紙運用で、医療情報を取り扱わない医事会計のみシステムで行なっている医療機関等においても、オンライン資格確認等システムを導入することにより、オンライン資格確認等システムの端末上、又は医事会計システムとの連携等により、医療情報へのアクセスが発生します。

このような医療機関等は、パターンⅡまたはⅣで、本ガイドラインを参照ください。

ただし、システム全体の構成等により、参照パターンが異なるので、必要に応じ、医療情報システム・サービス提供事業者に、参照パターンを確認ください。

医療機関等の特性に応じたガイドライン参照箇所　（２／２）

<table>
<tr><th>参照パターン</th><th>経営管理編</th><th>企画管理編</th><th>システム運用編</th></tr>
<tr><td>Ⅰ</td><td rowspan="4">すべて
参照</td><td colspan="2">すべて 参照</td></tr>
<tr><td>Ⅱ
担当者
いる
・
クラウド</td><td>基本的に すべて 参照
※ 医療情報システムの構成に応じて、
当該情報システム・サービス事業者に
確認し、事業者と締結する契約等に
含まれている場合は、以下を簡略化可能。
４．４　マニュアル等及び各種資料の整備
５．安全管理におけるエビデンスの考え方
１５．技術的な対策の管理
遵守事項：④、⑥、⑦、⑧、⑬以外</td><td>以下項目は 参照
１～４、６～８、１１、１２．３
※ 他の項目は、医療情報システムの構成に
応じて、当該情報システム・サービス
事業者に確認し、事業者と締結する契約等
に含まれている場合は、簡略化可能。</td></tr>
<tr><td>Ⅲ</td><td colspan="2">すべて 参照
※各編内の「担当者」という記載を「企画管理者」に置換し、参照。</td></tr>
<tr><td>Ⅳ
担当者
いない
・
クラウド</td><td>基本的に すべて 参照
※「担当者」という記載を「企画管理者」に
置換し、参照。
※医療情報システムの構成に応じて、
当該情報システム・サービス事業者に
確認し、事業者と締結する契約等に
含まれている場合は、以下を簡略化可能。
４．４　マニュアル等及び各種資料の整備
５．安全管理におけるエビデンスの考え方
１５．技術的な対策の管理
遵守事項：④、⑥、⑦、⑧、⑬以外</td><td>以下項目は 参照
１～４、６～８、１１、１２．３
※「担当者」という記載を「企画管理者」に
置換し、参照。
※ 他の項目は、医療情報システムの構成に
応じて、当該情報システム・サービス
事業者に確認し、事業者と締結する契約等
に含まれている場合は、簡略化可能。</td></tr>
</table>

補）なお、医療機関等において、電子署名を用いるシステムがない場合は「法令で定められた記名・押印のための電子署名」、紙媒体等から医療情報の電子化を行わない場合は「紙媒体等で作成した医療情報の電子化」の項目の参照の必要はない。