資料２－２

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

第１３回 健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

２０２２（令和４）年１２月１５日

医療情報システムの安全管理に関するガイドライン 第6.0版 概要

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

Ministry of Health, Labour and Welfare of Japan

概説 編

Overview

ひと、くらし、みらいのために

厚生労働省

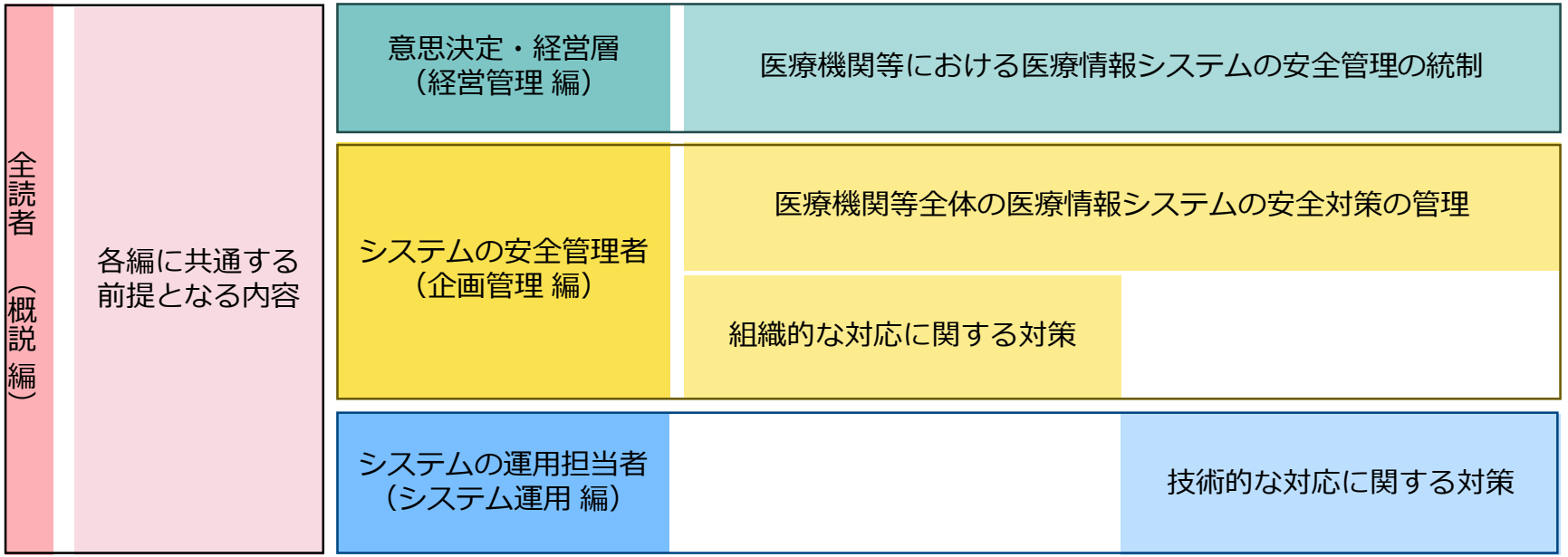
Ministry of Health, Labour and Welfare

医療情報システムの安全管理ガイドライン第6.0版の構成

◆ガイドライン第6.0版は、概説（Overview）編、経営管理（Governance）編、企画管理（Management）編、システム運用（Control）編で構成されています。

◆概説編では、各編を読むに際して、前提となる共通的な内容を示しています。

ガイドライン第6.0版を構成する各編



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、医療機関等において、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場合でも
オンライン資格確認等システムの導入により、オンライン資格確認等システムの端末上や、
医事会計システムとの連携により、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、参照パターンⅢ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っては、参照パターンⅣとなる場合もあるので、
情報システム・サービス提供事業者に、必要に応じて、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>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「運用管理者」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「運用管理者」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「運用管理者」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。

概説編　各章の概要

章	概要
1．目的	・ガイドラインの策定経緯の概要とガイドラインの目的について示しています。
2．対象	・ガイドラインの対象とする医療機関等の範囲、情報・文書の範囲、情報システムの範囲について示しています。
3．構成（概要）、読み方	・ガイドラインを構成する各編の目的と概要を示しています。 ・ガイドラインの読み方として、医療機関等が導入する医療情報システムの形態や専任のシステム運用担当者の有無に応じた参照箇所を示しています。
4．本ガイドラインの前提	・ガイドラインの各編を理解する上で、前提として理解すべき内容を示しています。 ・医療情報システムの安全管理の目的、医療情報システムの安全管理に関する法令の概要、統制等に関する考え方、リスク評価とリスク管理の考え方、医療情報システムにおける認証・認可の考え方、医療情報の外部保存などを示しています。

概説編　目次構成

Ministry of Health, Labour and Welfare of Japan

経営管理 編

Governance

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

医療機関等の経営と医療情報システムの安全性

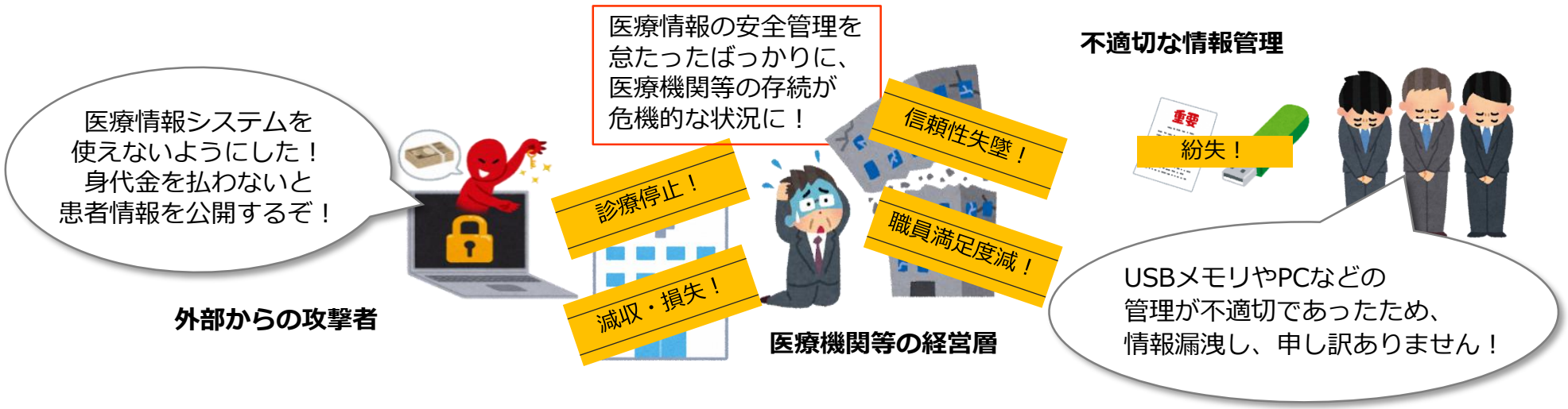
◆医療情報システムの安全管理（セキュリティ）対策は経営・運営に直接影響を及ぼす重要な課題

◆医療機関等の意思決定・経営層が、医療情報システムに関する適切な安全管理対策を実施せずに、情報セキュリティインシデントを生じさせた場合、地域・社会に対して損害を与えるほか、リスク管理やインシデント対応の是非、さらには経営責任や法的責任が問われることあります。

◆医療情報システムに対するサイバー攻撃は年々高度化、巧妙化しています。
診療行為の停止が余儀なくされたり、復旧に多大な費用を要したりするなどの被害のほか、地域の診療体制にも影響が生じるような深刻な事態に至り、地域医療の安全が脅かされます。

情報漏洩、サイバー攻撃などに関するセキュリティ対策は重要な経営課題！

深刻な事態に至った際には、地域医療の安全が脅かされることも発生！



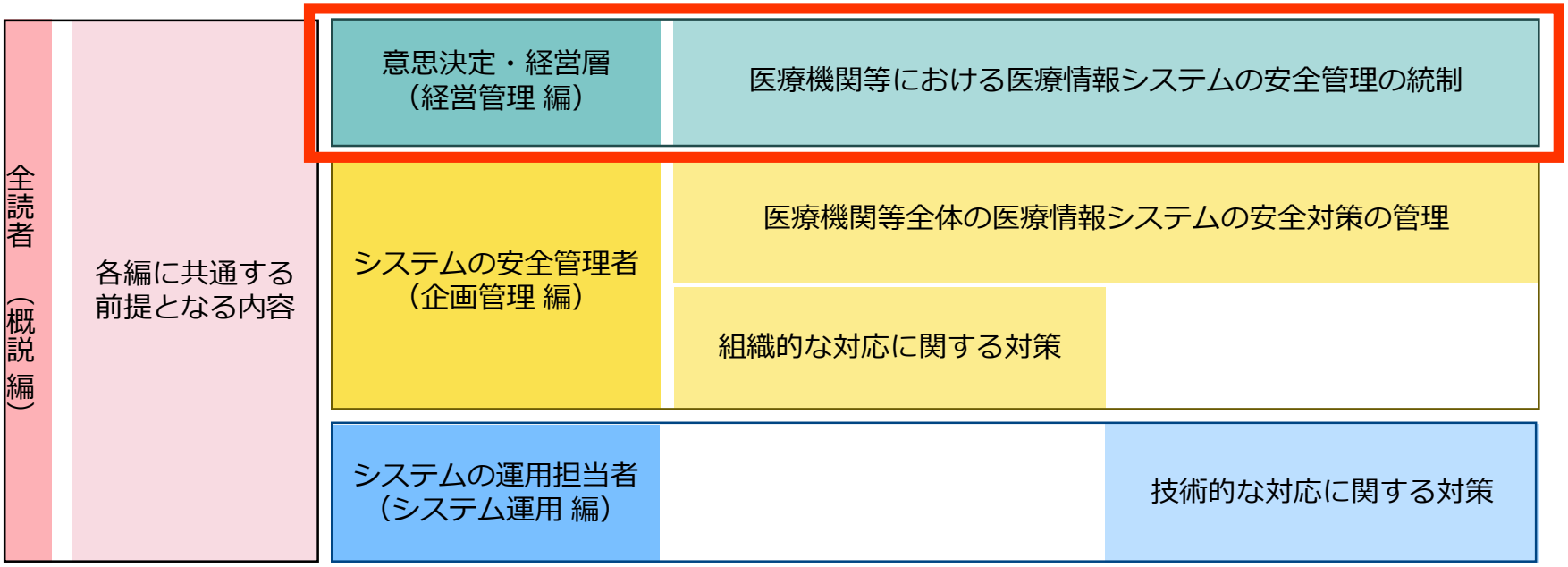
経営管理編の位置づけ

◆医療機関等における医療情報システムの安全管理の統制について、以下の内容等を示しています。

- 医療機関等が組織として遵守すべき基本的な考え方や果たすべき責任・責務に関する理解と実施
- 医療情報システムに関するリスク評価を踏まえた経営資源・資産の安全管理に関する方針策定と体制整備
- 安全管理方針に基づく各種安全管理対策事項の実施に関する管理責任
- 医療情報システム・サービス提供事業者（委託事業者）との責任分界・役割分担の明確化と協働体制の確立

ガイドラインを構成する各編と想定する読者の役割

（赤枠が経営層向けの経営管理編）



経営管理編　各章の概要

章	概要
遵守事項	・医療機関等の意思決定・経営層として、遵守いただきたい項目全般を示しています。
1．医療機関等における情報や情報システムの安全管理に関する責任・責務	・医療情報の取扱いや安全管理に関する法令上の遵守事項や義務などについて示しています。 ・通常時や非常時における安全管理上の管理責任や説明責任について示しています。 ・医療情報や医療情報システムに関して委託や第三者提供を行う場合の責任について示しています。
2．リスク評価を踏まえた管理	・医療情報及び医療情報システムに対するリスク評価の重要性を示しています。 ・リスク評価を踏まえた経営資源・資産の安全管理に関する方針の策定、安全管理対策の必要性、情報セキュリティマネジメントシステム（ISMS）の確立について示しています。
3．安全管理全般（統制、設計、管理等）	・意思決定・経営層による統制のもと、組織的な対応・技術的な対応として必要な体制や文書を整備し、リスク評価に基づく安全管理方針に従って、適切な安全管理対策を設計し、管理することなどについて示しています。 ・安全管理対策の実効性を担保するための自己点検や監査の意義や必要性について示しています。 ・情報セキュリティインシデントが発生した場合の対応について示しています。
4．安全管理に必要な項目全般	・技術的な安全管理対策について、情報システムの構成を踏まえた分類（クライアント側、サーバ側、インフラ、セキュリティ）と各分類で採用する安全管理措置について示しています。
5．情報システム・サービス事業者との協働	・情報システム・サービス提供事業者に対して委託を行う場合の事業者の選定、委託契約や体制の管理、委託事業者との責任分界や役割分担の明確化と協働体制の確立と管理などについて示しています。

意思決定・経営層が遵守すべき事項　（1/5）

1．医療機関等における情報や情報システムの安全管理に関する責任・責務

◆医療機関等で取扱う医療情報や医療情報システムに関する法令を遵守

◆医療機関等が負う安全管理に関する責任（説明責任、管理責任など）の内容を理解した上で対応

医療情報を取扱うに際して
個人情報保護法やe-文書法等
遵守すべき法令を把握し、
必要な措置を整理せねば！

医療情報を扱うため
通常時や非常時それぞれの場面で
必要な説明責任・管理責任等を
把握し、体制を整えねば！

医療情報の取扱いや医療情報
システムの管理を委託する際、
委託先の管理責任が医療機関等
自身に生じるため、事業者選定や
委託先管理は厳正にせねば！

1．1　安全管理に関する法令の遵守

医療機関等及び職員等が医療情報に関する法令等を遵守するように、管理体制を整え、必要な措置が講じられるようにする。

医療情報や医療情報システムに対する安全管理を実施し、医療の継続性を維持する責任を有している。

1．2　医療機関等における管理責任

医療機関等に対する、個人情報保護法や医師法・歯科医師法・薬剤師法・医療法等に基づく行政法上の責任、刑法等に基づく刑事上の責任、民法や契約に基づく民事上の責任を理解し、医療情報や医療情報システムの安全管理に務める。

医療機関等における医療情報の管理責任として、通常運用時における説明責任や管理を実施・改善する責任や、非常時やその事後における説明責任や善後策を講じる責任を果たすための体制や措置を講じる。

1．3　委託における責任

委託に関する責任は医療機関等自身が負う管理責任であることを理解し、委託事業者に対しても法令の遵守を求め、適切に委託事業者の選定や委託先を管理する。

委託先と法律上の責任の範囲や委託する業務等の対象の範囲や役割の分担を明らかにし、委託契約を適切に締結する。

1．4　第三者提供おける責任

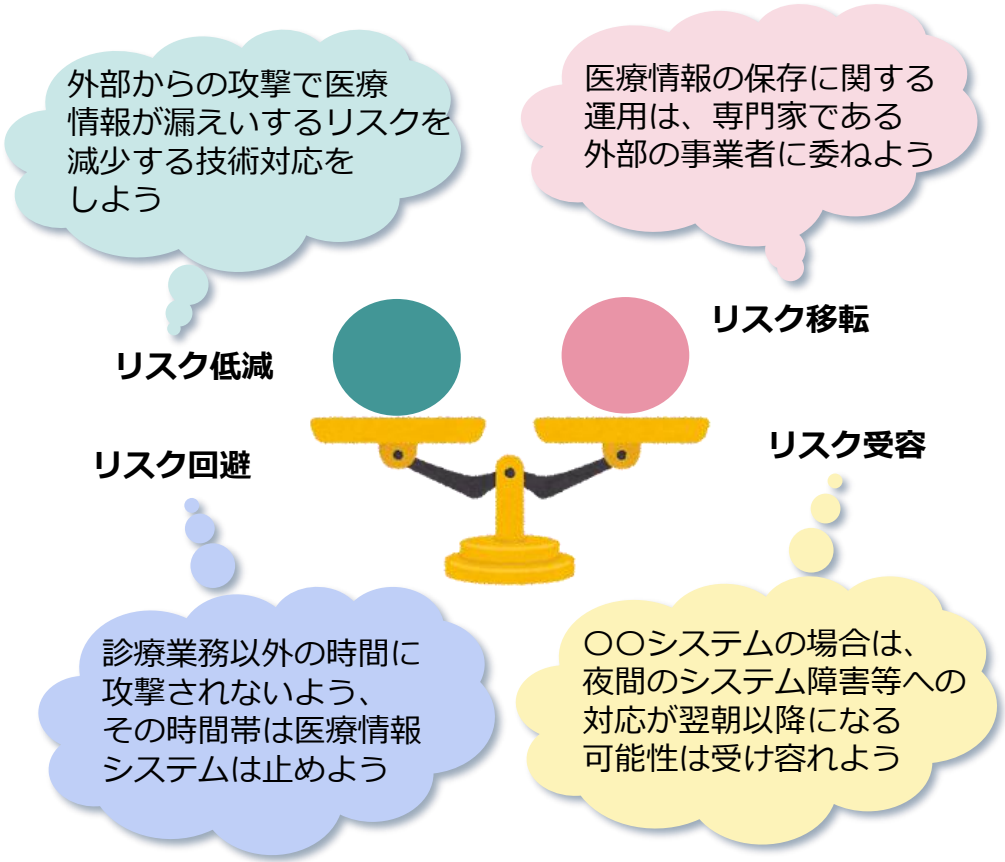
医療情報を第三者提供する場合には、個人情報保護法やガイダンス等の法令を遵守して、適切に手続を行うほか、提供先の第三者に適切な管理責任を課し、互いの業務や情報の利用目的を踏まえて責任の範囲を明確にする。

意思決定・経営層が遵守すべき事項　（2/5）

2．リスク評価を踏まえた管理

◆医療機関等で取扱う医療情報や医療情報システムを取り巻くリスクを理解

◆リスク評価結果への対応判断を行い、適切なセキュリティ対策を実施



2．1　医療情報システムにおけるリスク評価の実施

経営層は、医療機関等で管理する医療情報等の重要度に応じて、リスク対応のポリシーを判断して、リスク管理方針を決定する。

リスク決定方針を踏まえて、医療機関等における安全対策の体制やルール等の整備、具体的な対応措置などを行うようにする。

2．2　リスク評価を踏まえた判断

経営層は、リスク管理方針について、医療情報の重要性や医療の継続性と併せて、医療機関等における経営資源や対策の継続性などを鑑みて、経営判断の観点から決定するとともに、その説明責任を果たせるようにする。

医療機関等における医療情報の安全対策を継続するため、情報セキュリティマネジメントシステムを構築する。

医療機関が実施したリスク評価の結果を委託先と調整して、適切な委託内容を決定する。

意思決定・経営層が遵守すべき事項　（3/5）

3．安全管理全般（統制、設計、管理等）

◆医療機関等において組織として体系的に医療情報システムの安全管理を実施

◆安全管理に必要な統制（規程、体制）や設計（セキュリティ対策、教育・訓練）、管理（自己点検、内部/外部監査）を実施

3．1　統制

医療機関等における医療情報システムの安全性確保のための統制の体系を理解し、必要な体制構築、規程類、対策等が整備されていることを確認する。

統制を実務的に実施するために、運用管理者を設置する等の対応を行う。

安全性の運用管理は、組織内の人事統制とは区別し、組織全体の統制として構築する。

3．2　設計

リスク管理方針等を踏まえて、セキュリティ方針を整備し、適切な安全管理対策の整備を行えるようにする。

職員等に対して、必要な教育・訓練を適切に講じる。

3．3　安全管理対策の管理

安全管理対策が適切に実施されていることを、自己点検や内部監査・外部監査などにより確認すること。

3．4　情報セキュリティインシデントへの対応

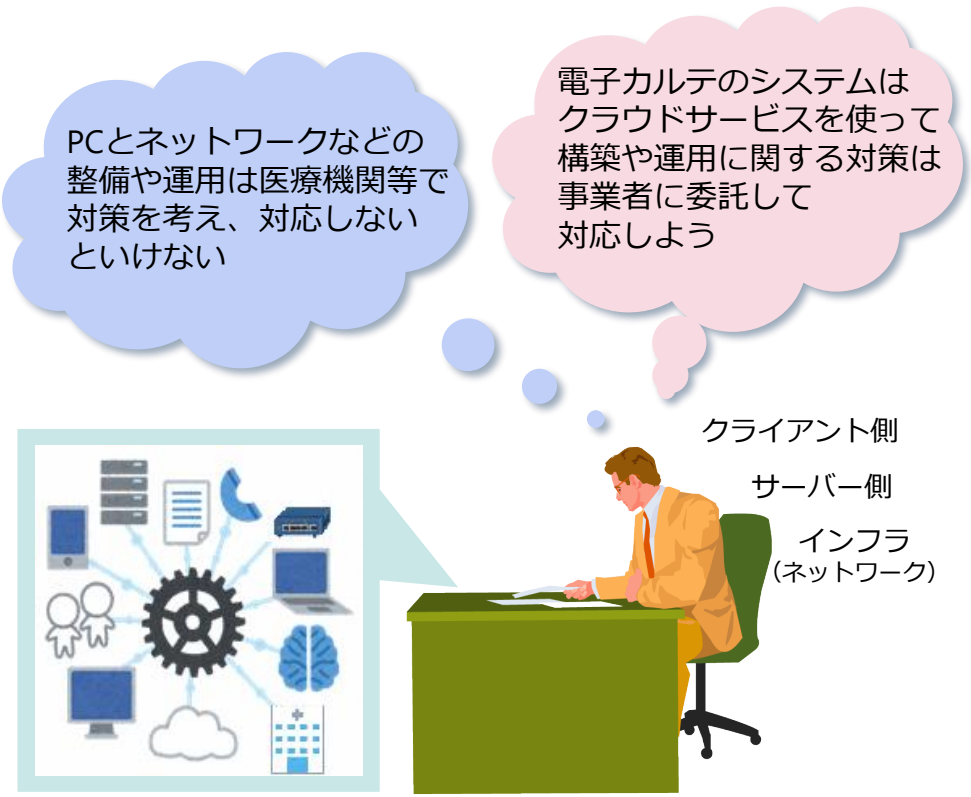
情報セキュリティインシデントが生じた場合の対応体制や対応内容等を整備する。

情報セキュリティインシデントの発生により、医療機関等の業務継続事態に影響が出る危険性も想定されるため、業務継続の可否の判断基準や判断手続、事業継続計画（BCP：Business Continuity Plan）を整備する。

意思決定・経営層が遵守すべき事項　（4/5）

4．安全管理に必要な対策項目

◆医療機関等の特性や医療情報システムの構成を踏まえて、安全管理に必要なセキュリティ対策の概要を把握し、管理されていることを確認



4．1　必要な対策項目の概要

医療機関等が行うべき医療情報システムの安全管理対策項目の概要を認識し、運用管理及び運用担当の部署や者に対して、それぞれの対策項目等に対する具体的な実施方法について整理する旨を指示し、それぞれの対策項目が対応できている旨を確認する。

医療情報システムへの対策として、予防的措置や発見的措置などの特徴などがあることを認識する。そのうえで、必要に応じた対策項目を採用できるようにする。

【本ガイドラインにおける技術的な対応の対策項目】

- クライアント側：
  システムの利用者に近いクライアント側
- サーバ側：
  利用者の医療情報の利用を支える
  情報システム・サービスの基幹側または提供元側
- インフラ：
  情報システム・サービスを支えるインフラや基盤サービス
- セキュリティ：
  医療機関等が利用する医療情報システム全般に共通して
  求められるセキュリティの観点で必要な対策項目

意思決定・経営層が遵守すべき事項　（5/5）

5．情報システム・サービス事業者との協働

◆委託する情報システム・サービス事業者との間で、責任分界、役割分担を明確化

◆委託する事業者との協働を前提とした適切な安全管理の体制を構築

5．1　事業者選定

本ガイドライン、法令等が求める要件を満たす事業者を選定する。

JIS Q 15001またはJIS Q 27001（これと同等の規格含む）の認証を受けていることを確認する。

5．2　委託管理

委託契約の内容として、委託業務の内容や委託先の体制、利用する資産の管理範囲、委託先との責任分界、委託先における委託した情報の取扱いの状況に対して合理的に把握できることなどを含め、それらが実施することを確認する。

委託先が再委託を用いる場合には、再委託の内容を確認し、委託内容全体の適切な管理を行う。

5．3　責任分界管理

医療機関と委託先事業者との間での責任分界を可能な限り明確にする。

医療情報システムの安全管理ガイドライン第6.0版　経営管理編　目次構成

遵守事項

Ministry of Health, Labour and Welfare of Japan

企画管理 編

Management

ひと、くらし、みらいのために

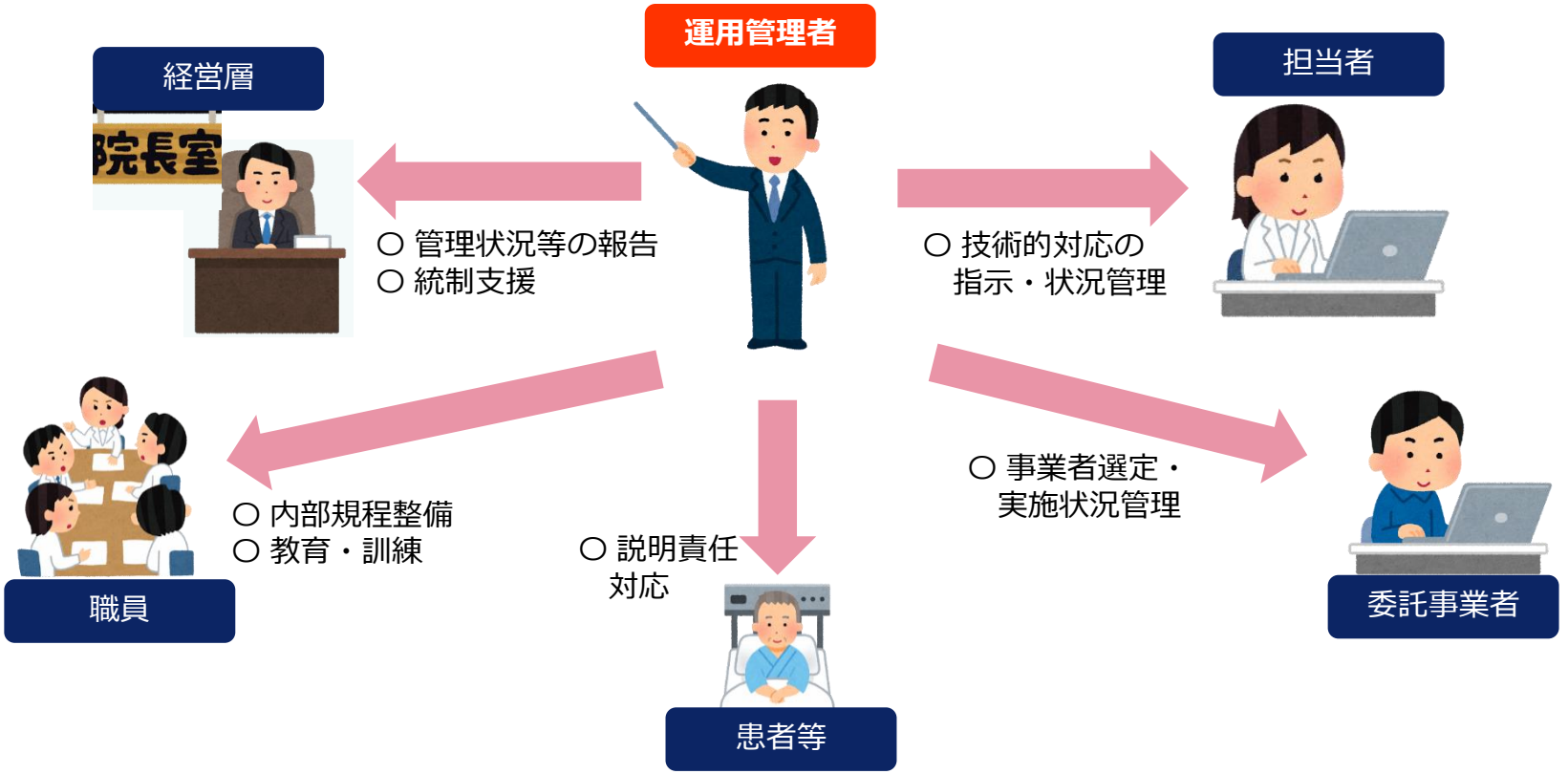
厚生労働省

Ministry of Health, Labour and Welfare

医療情報システムにおける企画管理

◆医療情報システムの運用管理者は、医療情報システムに関する安全管理の実務的司令塔

◆医療機関等における医療情報システムの安全管理は、経営層による組織としての統制、運用管理者による組織全体での管理、担当者による技術的な対応などから構成されます。



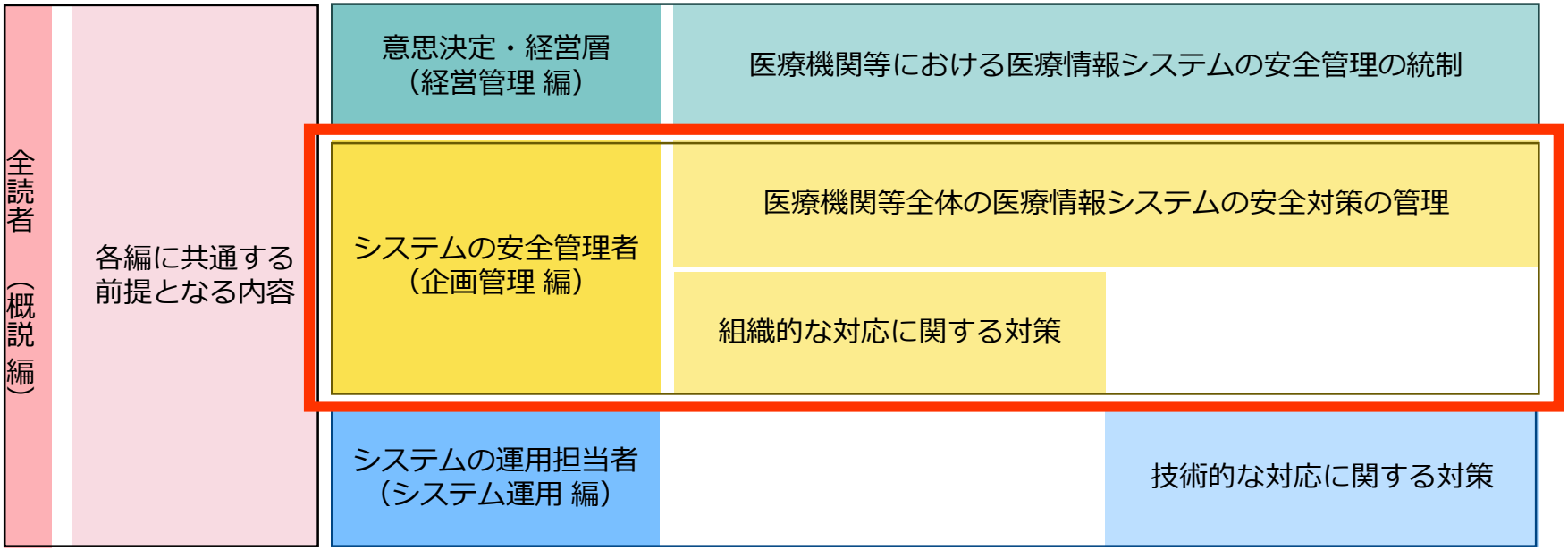
企画管理編の位置づけ

◆医療情報システムの安全管理のための運用管理に関する内容をまとめています。

◆組織的な対応と技術的な対応の医療機関等全体の医療情報システムの安全対策の管理と、組織的な対応に関する対策を実施することが求められます。

ガイドラインを構成する各編と想定する読者の役割

（赤枠が運用管理者向けの運用管理編）



企画管理編　各章の概要

章	概要
1．管理体系	医療機関等において遵守すべき安全管理に関連する法制度等についての詳細や、 策定すべき医療情報システムの安全管理に関する方針について示しています。
2．責任分界	医療機関等が外部委託、その他外部の医療機関等との関係で医療情報を取扱う際に取り決めるべき 責任分界について、運用管理の観点からの考え方や決め方について示しています。
3．医療機関等における 安全管理のための体制と 責任・権限	医療情報システムの安全管理を行う上で、医療機関等において構築すべき体制に関して、 決めるべき内容等を示しています。
4．医療情報の安全管理に おいて必要な規程・文書類 の整備	医療機関等の内部で、安全管理の運用を行うのに必要な文書等について、 考え方や体制などを示しています。
5．安全管理における エビデンス	医療情報システムの安全管理が適切になされているかを確認するための証跡管理等に関して、 考え方や具体的な内容、レビューの必要性等を示しています。
6．リスクマネジメント	医療機関等において行う、医療情報システムに関連するリスクマネジメントに関して、 考え方や組織内での役割、実施したリスク評価等を踏まえた運用等を示しています。
7．安全管理のための人的管理 （職員管理、委託先管理、 教育・訓練、委託先選定・ 契約）	医療機関等内における人的管理に関する対策の内容を示しています。 職員、委託先に対する管理や教育・訓練、委託先の選定時及び終了時における 遵守事項等を示しています。

企画管理編　各章の概要

章	概要
8．情報管理（管理、持出し、破棄等）	医療機関等からの情報の持出し（ネットワーク経由での持出し含む）や情報の破棄等に関する考え方や遵守事項を示しています。
9．医療情報システムに用いる機器等の資産管理	医療情報システムで用いる機器等の管理に関する遵守事項や考え方を示しています。
10．運用に対する点検・監査	医療情報システムの安全管理が適切になされていることの確認や改善の必要性などを確認するための運用に対する点検や監査について示しています。
11．非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	非常時を想定した、医療情報システムに関連する、医療機関等が対応すべき内容について示しています。
12．サイバーセキュリティ	サイバーセキュリティに関連したインシデント対応の必要が生じた場合を想定した対策として、サイバーセキュリティ対応計画に関する内容などを示し、特にサイバー攻撃被害を受けた際に講じるべき内容を示しています。
13．医療情報システムの利用者に関する認証等及び権限	医療情報システムに用いる利用者の登録や認証、権限に関する考え方や内容を示しています。
14．法令で定められた記名・押印のための電子署名	医療従事者が作成する書面において、法令で定められた記名・押印のための電子署名に関する遵守事項を示しています。
15．技術的な対策の管理	医療情報システムの安全管理のうち、運用管理者が行うべき技術的な対応等について示しています。
16．紙媒体等で作成した医療情報の電子化	医療機関等が紙媒体等で作成した医療情報を電子化する際に求められる内容について場面ごとの遵守事項や考え方を示しています。

企画管理編　目次構成

企画管理編　目次構成

企画管理編　目次構成

Ministry of Health, Labour and Welfare of Japan

システム運用 編

Control

ひと、くらし、みらいのために

厚生労働省

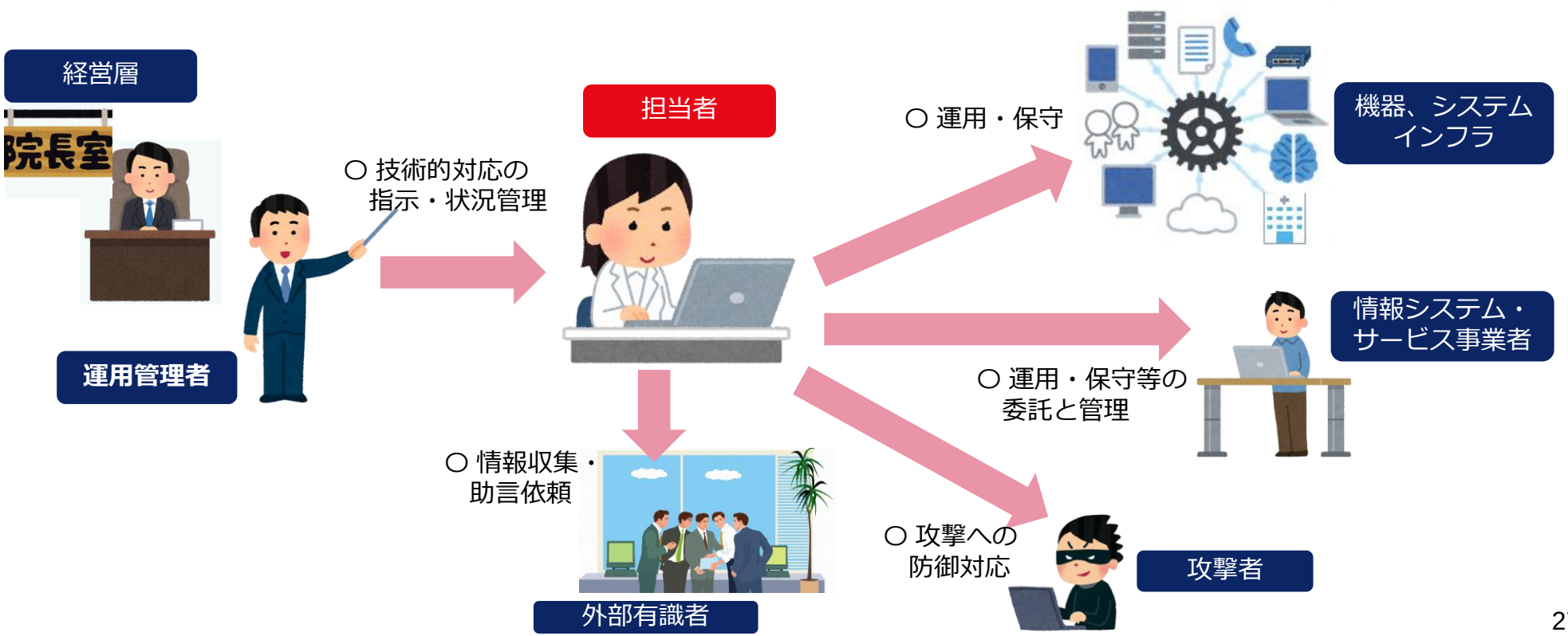
Ministry of Health, Labour and Welfare

医療情報システムにおける運用

◆医療情報システムの運用に関する担当者は、安全管理対策・措置の実行者

◆医療情報システムの運用担当者は、医療情報システムの安全管理に関する技術的な対策の実装と運用を担います。

◆専任の担当者の有無や情報システム・サービスの形態によっては、実装要件の確認や運用を情報システム・サービス事業者に委託することも想定されます。



システム運用編の位置づけ

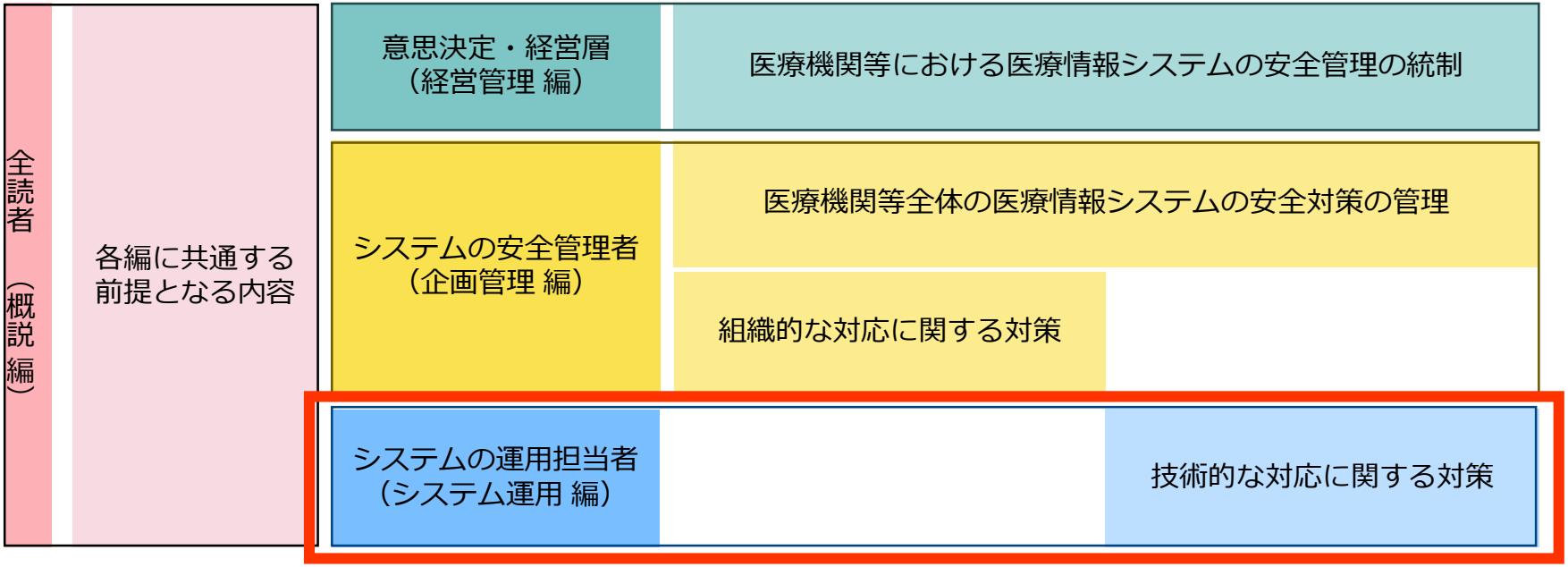
◆医療情報システムの安全管理に関して、担当者が講じるべき技術的な対応内容を示しています。

◆医療情報システムにおいて求められる技術的な内容（システム上の仕様等）や、
システムの運用に関連して作成すべき手順や資料などを示しています。

◆医療機関等における専任の担当者の有無や導入する情報システム・サービスの形態によっては、
情報システム・サービス事業者に確認や委託等を求める内容を含みます。

ガイドラインを構成する各編と想定する読者の役割

（赤枠が運用管理者向けの管理実装編）



システム運用編　各章の概要

章	概要
1．情報セキュリティの基本的な考え方	法令上求められる医療情報システムに関する要件等に関して、必要な技術的な対応を抽出し、各システムの整備、必要な手順、資料の作成などを行うことを示しています。
2．システム設計・運用に必要な規程類と文書体系	各種規程等に基づき、技術的な対応に関する運用の手順や、医療情報システム等を構築するのに必要な資料等を整備し、最新性を維持する必要性を示しています。 整備する手順や資料類は、通常時に必要なものだけではなく非常時やセキュリティインシデントが生じた場合の対応の必要性等についても示しています。
3．責任分界の考え方	外部委託などにおいて、技術的な対応における責任分界を決定する際の考慮事項や、医療機関等が負う各責任に応じた具体的な分担の内容、それらを決定する際に行うべき調整などに関して示しています。 クラウドサービスなどを利用する場合の、特性に応じた考慮の必要性や、第三者提供における技術的な分担範囲の考え方の例などを示しています。
4．リスクアセスメントを踏まえた安全対策の設計	情報資産の種別に応じて講じるべき安全管理（バックアップ等）の技術的な設計の必要性や、リスク評価を踏まえた技術的な対応の必要性について示しています。 リスクアセスメントの負担が大きい医療機関等においては、情報システム・サービス事業者からの情報提供を踏まえた対応の重要性を示しています。
5．システム設計の見直し（標準化対応、新規技術導入のための評価等）	医療情報システム等において情報の相互運用性と標準化の重要性を示したうえで、電子カルテにおける標準化対応、データ形式・プロトコルの互換性の確保が必要なことについて示しています。

システム運用編　各章の概要

章	概要
6．安全管理を実現するための技術的対策の体系	技術的な対応に関する本ガイドラインにおける項目の考え方や、導入する医療情報システム・医療機関等における体制の違いによる対応の仕方の違いなどを示しています。
7．情報の持出し・管理・破棄等	医療機関等の外部に情報を持ち出す際の技術的な対応や、外部から医療情報システムに接続して医療情報を利用する場合の対応を示しています。 また情報の破棄を行う際の技術的な対応を示すほか、医療情報を格納する媒体、機器等の紛失、盗難等が生じた場合に担当者として行う必要がある内容を示しています。
8．利用機器・サービスに対する安全管理措置	医療情報システムで利用される端末等の機器やサービスにおける技術的な対応について示しています。 不正ソフトウェア対策、機器等の脆弱性への対策、端末やサーバの安全な利用のための管理、機器等の棚卸、医療機関等が管理する以外の機器の利用に対する対策などを示しています。
9．ソフトウェア・サービスに対する要求事項	医療情報システム、特にサーバ側におけるソフトウェア・サービスにおける構成管理や品質管理などについて、担当者が講じるべき内容を示しています。 施行通知により求められる対策も示しています。
10．システム・サービス事業者による保守対応等に対する安全管理措置	医療情報システムの保守に関する技術的対応や、保守を委託している場合に担当者が対応すべき内容について示しています。
11．システム運用管理（通常時・非常時等）	通常時と非常時に講じるべき運用対策について示しています。 通常時の対策は特に、非常時を想定した技術的な対応を示しており、 非常時の対策は、実際に非常時が発生した場合に求められる技術的な対応を示しています。

システム運用編　各章の概要

章	概要
12. 物理的安全管理措置	医療情報を格納するためのデータセンタ等の物理的要件、入退管理や、バックアップの管理で技術的な対応として求められる内容、機器や媒体の不適切な管理や利用に対する対策について示しています。
13. ネットワークに関する安全管理措置	本ガイドラインにおけるネットワークについての考え方と安全管理について整理しています。 境界防御を基本としつつ、多層防御の考え方を取り入れた対応を行う旨を示しています。 オープンなネットワークでの利用も考慮した暗号化や盗聴対策の必要性、無線LANの利用における対策なども示しています。
14. 認証・認可に関する安全管理措置	医療情報システムにおいて採用すべき利用者認証につき、特に当人認証に関する技術的な対応としての対策を示すほか、アクセス権限やID・権限の棚卸等の手順を示しています。 電子カルテのデータの確定に関して、施行通知で求める対策について示しています。
15. 電子署名、タイムスタンプ	医療情報システムにおいて、電子署名等を求める場合の対応について示しています。
16. 紙媒体等で作成した医療情報の電子化	紙媒体等で作成した医療情報を電子化する際に、技術的な対応として必要な内容を示しています。
17. 証跡のレビュー・システム監査	医療情報システムの適切な運用を確認するための証跡の要件として求められる技術的な対応における措置のほか、証跡のレビューに関する対応について示しています。 監査を行う際の監査実施計画における技術的な対応に関して示しています。
18. 外部からの攻撃に対する安全管理措置	外部から攻撃を受けた際に対応すべき技術的な対応について示しています。

システム運用編　目次構成

システム運用編　目次構成

システム運用編　目次構成