医業経営情報

REPORT

Available Information Report for Medical Management

医業経営

サイバー攻撃からの
セキュリティ対策を明示！

医療情報システム安全管理ガイドラインの概要

1 医療情報システムを取り巻く現状と課題
2 ガイドライン改定の背景と概要
3 医療情報システムの安全性向上に向けた取組み
4 未来の医療情報と生成AIの影響

2025
3
MAR

税理士法人　向田会計

1｜医療情報システムを取り巻く現状と課題

臨床分野や医療情報システム等に対するサイバー攻撃の多様化・巧妙化が進み、医療機関における診療をはじめとする業務に大きな影響が生じています。個人情報や診療記録といった機密データを狙ったサイバー攻撃は、国内外で後を絶たず、医療機関が直面する深刻な問題となっています。

このような状況を受け、厚生労働省は令和５年５月に「医療情報システムの安全管理に関するガイドライン」を改定し、第 6.0 版を発表しました。本ガイドラインは、経営層から現場の従業員、技術担当者まで、医療機関全体が取り組むべきセキュリティ対策を具体的に示しています。

そこで本稿では、現状の課題、ガイドラインの概要、具体的な対策、そして未来の医療情報システム像について解説します。

1｜サイバーセキュリティ問題の深刻化

近年、医療機関を標的としたサイバー攻撃が世界的に増加しており、その深刻さが社会問題となっています。医療情報には患者の個人情報や診断記録、治療内容など、生命やプライバシーに直結する重要なデータが含まれています。これらの漏洩や改ざんがなされると、患者の生命に危機をもたらすだけでなく、医療機関の社会的信頼が大きく損なわれることになります。

これまでも、日本国内で様々なランサムウェア攻撃等を受け、医療機関が一時的に業務停止を余儀なくされるといった事例が発生しています。このようなサイバー攻撃は、個人、医療機関、そして社会全体に多大な影響を及ぼすため、早急な対応が求められています。

◆国内の医療業界で発生した主なサイバー攻撃事例

年月	医療機関名	事例概要	影響・被害
2017年8月	福島医大病院	ランサムウェア攻撃	パソコンや医療機器のデータが暗号化され機能停止
2018年10月	奈良県の病院	ランサムウェア攻撃	電子カルテシステムが使用不可、紙カルテでの運用を強いられる
2019年5月	東京都の医療センター	不正アクセス	職員端末のメールボックス内情報が流出

2020年12月	福島県の病院	コンピュータ ウイルス感染	検査機器の不具合が複数部署で発生
2021年10月	徳島県つるぎ 町立半田病院	ランサムウェア攻撃	電子カルテなどのデータが暗号化、 通常診療再開まで約２ヶ月を要した
2022年10月	大阪急性期・総合 医療センター	ランサムウェア攻撃	電子カルテシステムに障害、緊急以 外の手術や外来診療の一時停止
2024年5月	岡山県精神科 医療センター	サイバー攻撃	個人情報の流出

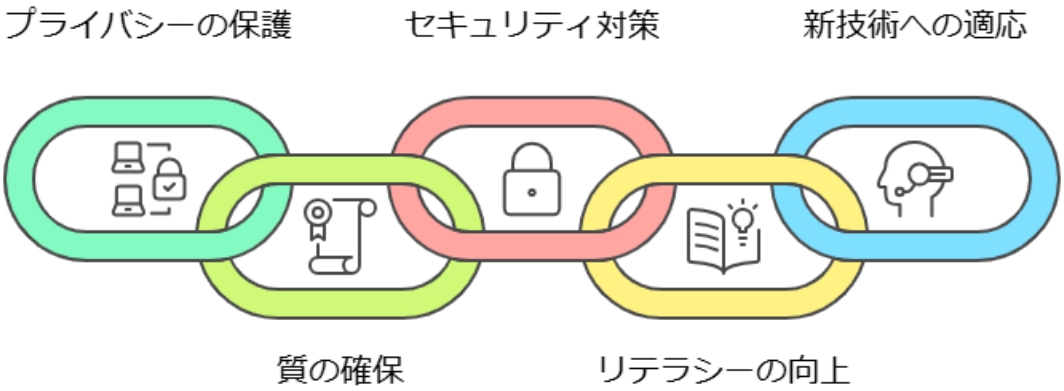
2 医療情報の重要性と保護の必要性

医療情報は、患者の生命や健康に直結するデータであり、その保護は医療機関にとって最も重要な責務の一つです。他の業界の情報資産とは異なり、医療情報は一度漏洩すれば患者のプライバシーを侵害するだけでなく、診療の質や安全性にも重大な影響を及ぼします。

たとえば、診断記録や治療履歴が不正アクセスを受けた場合、患者への誤診や治療ミスを引き起こす可能性もあります。また、医療情報のデジタル化が進む中で、医療機関の法的・社会的な責任も厳しく問われるようになり、医療従事者には、情報を適切に扱うためのリテラシーが求められ、医療機関全体でのセキュリティ対策が必須となっています。

さらに、生成 AI や IoT といった新技術の普及により、情報の取扱いに関する課題も複雑化しており、これらの背景を踏まえ、医療情報を安全に管理する仕組みを強化することは、患者の信頼を維持し、医療の質を向上させるために不可欠な取り組みといっても過言ではありません。

◆医療情報の保護



3　現行の医療情報システム運用の課題

現行の医療情報システムの運用については、多くの課題が指摘されています。まず、従来のセキュリティ対策では、日々高度化するサイバー攻撃に対応しきれていない点が問題視されています。特に、医療情報システムは従来型の古いシステムと最新のクラウド技術が混在している場合が多く、その複雑さが脆弱性を生む原因となっています。

さらに、技術的な問題に加えて、人為的エラーも大きなリスクです。例えば、不適切なアクセス管理やパスワードの管理不備、セキュリティ意識の低さによりサイバー攻撃を招くといったケースが多発しています。具体的には、共有アカウントの使用や、簡単に推測可能なパスワードの設定、外部からの不審なメールに対する警戒不足などが挙げられます。

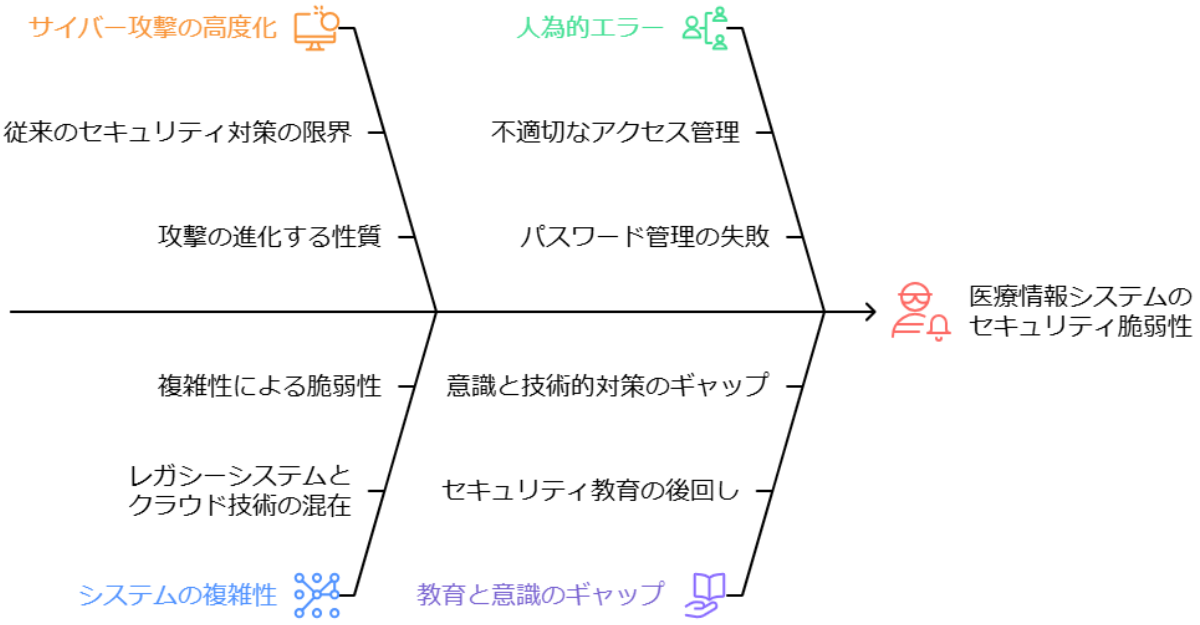
また、多忙な医療現場では、情報セキュリティ教育やリスクアセスメントが後回しにされがちです。

特に地方の中小規模の医療機関では、専門的な情報セキュリティ人材の不足や予算的な制約により、十分な対策が取れていない状況が続いています。これにより、現場レベルでのセキュリティ意識と技術的対策との間に大きなギャップが生じているのです。

以上の課題を解決するためには、システム全体のセキュリティの再設計と従業員教育の強化が必要であり、経営層から現場まで一貫した取り組みが求められます。具体的には、定期的なセキュリティ監査の実施、インシデント対応計画の策定、そして医療従事者向けの実践的なセキュリティトレーニングプログラムの導入などが重要となります。

このような課題に対応するため、令和５年５月には医療情報システムの安全管理を強化するガイドラインが改定され、より具体的な対策要件や評価基準が示されました。

◆医療情報システムにおけるセキュリティの課題



2 ガイドライン改定の背景と概要

1 ガイドライン改定の背景と目的

医療情報システムの安全管理に関するガイドラインが第 6.0 版に改定された背景には、医療機関を取り巻く環境の変化と、これに伴う新たな課題への対応が求められていたという状況があります。また、令和５年４月からオンライン資格確認の導入が原則義務化されたことを受け、医療分野を狙ったサイバー攻撃による診療業務等に重大な影響を及ぼす事例も増加するなかで、ネットワーク関連のセキュリティ対策が多くの医療機関等に共通して必要とされたこともガイドラン改定を促す要因になったといえます。

◆改定の趣旨

保険医療機関・薬局においては令和５年４月からオンライン資格確認の導入が原則義務化されており、今後は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より多くの医療機関等に共通して求められることとなる。よって、医療機関等にガイドラインの内容の理解を促し、医療情報システムの安全管理の実効性を高めるため、構成の見直しを行う。

また、医療等分野及び医療情報システムに対するサイバー攻撃の一層の多様化・巧妙化が進み、医療機関等における診療業務等に大きな影響が生じていること等を踏まえ、医療機関等に求められる安全管理措置を中心に内容の見直しを行う。

厚生労働省：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（令和５年５月）

今回の改定では、医療機関等が必要な安全管理措置を理解し、実効性のある対策を講じられるよう内容が整理されました。本文は概説編、経営管理編、企画管理編、システム運用編の４つの区分に分けられ、読者層に応じた遵守事項や考え方が示されています。

例えば、経営管理編では病院長や理事長などの経営層向けに組織としての責任や投資判断の考え方が示され、システム運用編では情報システム部門の実務者向けに具体的な技術要件が詳述されています。また、現場で発生しやすい質問やトラブルを Q&A 形式で補足し、構成を分かりやすく解説しています。

クラウドサービスのリスクや責任分担が整理され、ゼロトラスト思考（すべてのアクセスを信頼せず、常に検証するセキュリティモデル）に基づくネットワーク対策や非常時の対応も明確化されました。オンライン資格確認に必要な機器の安全管理措置も盛り込まれ、最新の技術や制度に対応した内容となっています。

◆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

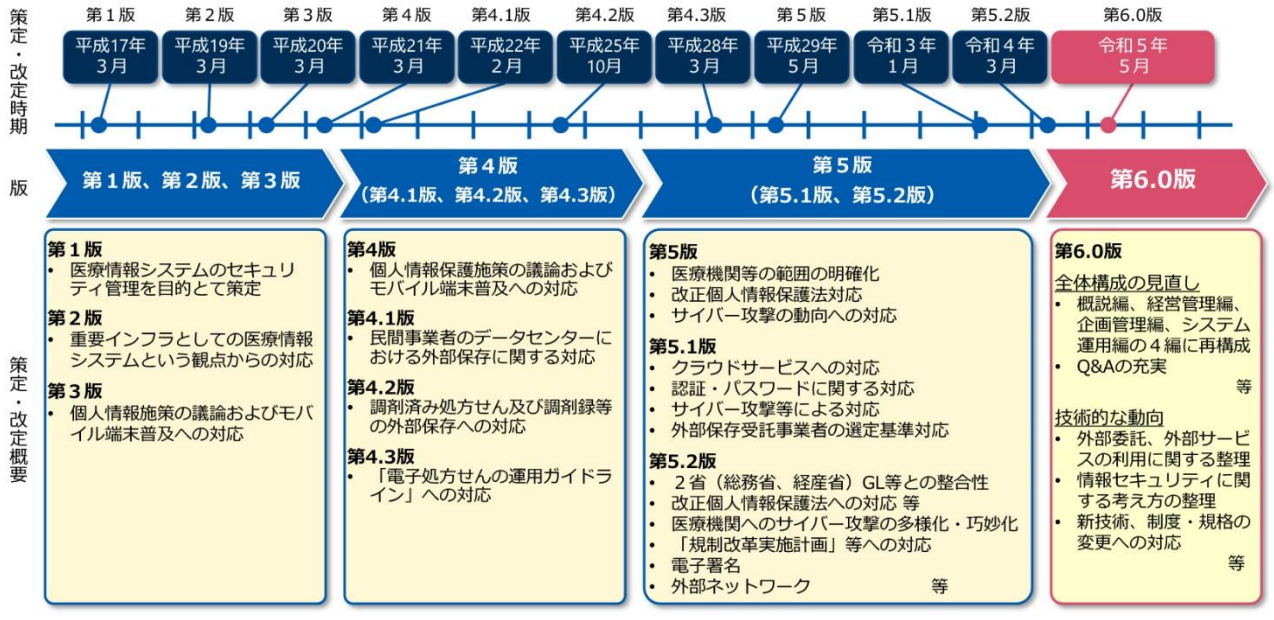
○ 全体構成の見直し

・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

厚生労働省：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

◆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。**



厚生労働省：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

2｜地域医療の充実に向けた「かかりつけ医機能」の確立と情報提供

地域医療の質を向上させるためには、患者と医療機関をつなぐ『かかりつけ医』の役割が重要です。今回のガイドラインの改定では、さまざまな規模や形態の医療機関が安全に患者情報を扱えるよう、情報管理体制の整備に焦点を当てました。

具体的には、情報の適切な管理（ガバナンス）、効果的な運営（マネジメント）、セキュリティ対策（コントロール）の観点から、医療機関の支援を行っています。このようなガイドラインの整備によって、かかりつけ医がより安全で迅速な医療サービスを提供し、地域全体の医療連携を強化することを目指しています。

◆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。

厚生労働省：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

3｜新規追加および変更点

第 6.0 版では、進化するサイバーリスクや技術に対応するため、ゼロトラストモデルの導入が推奨されています。また、災害時の対応強化として、BCP（事業継続計画）や DRP（災害復旧計画）の策定が義務化され、多要素認証による安全なアクセス管理も求められています。さらに、新技術への対応を強化しつつ、適切なリスク管理を促進しています。これらの変更は、医療現場の課題に対応し、実効性の高いセキュリティ強化を目指したものです。では、医療機関は具体的にどのような対策を講じるべきなのでしょうか。

3 医療情報システムの安全性向上に向けた取組み

1 経営層と現場の連携強化

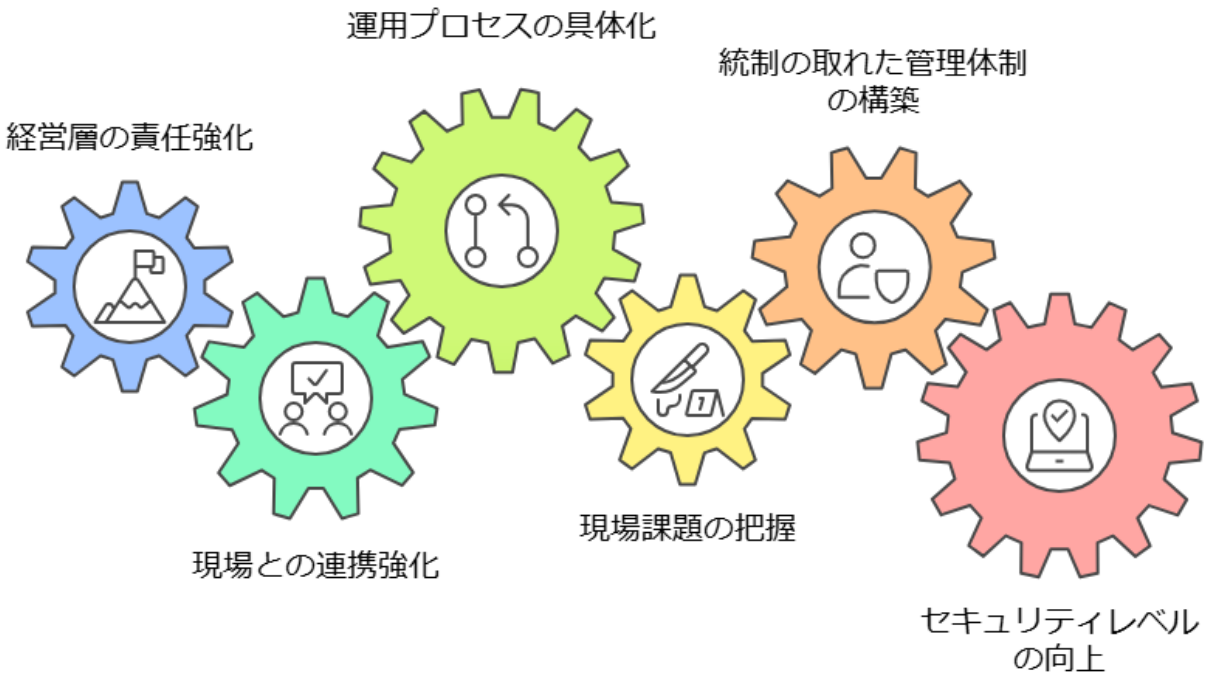
医療情報システムの安全管理を効果的に実現するには、経営層と現場の連携強化が不可欠です。ガイドライン第 6.0 版では、経営層の責任強化が明確に打ち出されており、情報セキュリティ対策への積極的な関与が求められています。

経営層が担うべき役割として、情報セキュリティポリシーの策定や全体的なリスクマネジメント体制の構築が挙げられます。

一方で、現場の実務者は、これらのポリシーを具体的な運用プロセスに落とし込み、日常業務の中で実践することが重要です。経営層と現場の連携を強化するためには、定期的なミーティングや情報共有の場を設けることが有効です。さらに、経営層が現場の課題を正確に把握することで、現場が抱えるリソース不足や技術的な制約にも対応しやすくなります。ガイドラインの実践を通じて、経営層と現場が協働し、全体として統制の取れたセキュリティ管理体制を構築することが求められているのです。

こういった取り組みにより、医療機関全体のセキュリティレベルを向上させることが可能となります。また、組織全体でセキュリティ意識が高まることで、新たな脅威に対しても柔軟に対応できる体制が整うことが期待されます。

◆医療情報セキュリティの強化



2｜技術的セキュリティ対策の強化

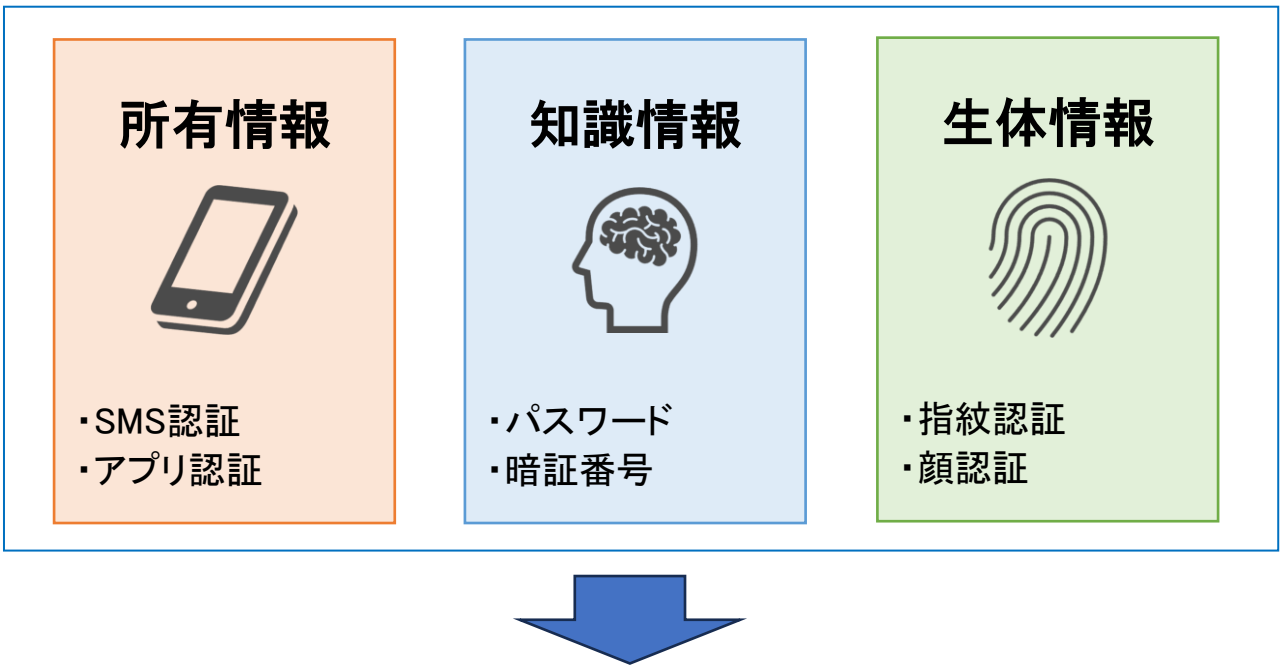
医療情報システムの安全性を高めるためには、技術的なセキュリティ対策の強化が不可欠です。ガイドライン第 6.0 版では、多要素認証（MFA）の導入やデータの暗号化が強く推奨されています。多要素認証には、パスワードだけでなく生体認証やデバイス確認を組み合わせることで、不正アクセスを大幅に減らす効果が期待されています。特に、電子カルテシステムへのアクセスや院外からのリモートアクセスにおいては、多要素認証の導入が必須とされています。

また、暗号化技術の導入により、システム内外でのデータ通信や保存における情報漏洩リスクを軽減できます。暗号化の対象には、患者の診療情報だけでなく、医療機器から出力されるデータや医療従事者の業務記録なども含まれます。

さらに、ゼロトラストネットワークモデルの採用も重要なポイントです。このモデルは、内部ネットワークであってもアクセスを厳密に管理するため、ランサムウェアや不正侵入の被害を抑えることが可能です。加えて、ネットワーク分離やファイアウォールの強化、定期的なシステムアップデートも推奨されています。

これらの技術的対策を統合的に運用することで、医療情報システムの堅牢性を高め、患者情報を安全に保護する体制を構築することが求められています。

◆多要素認証のイメージ



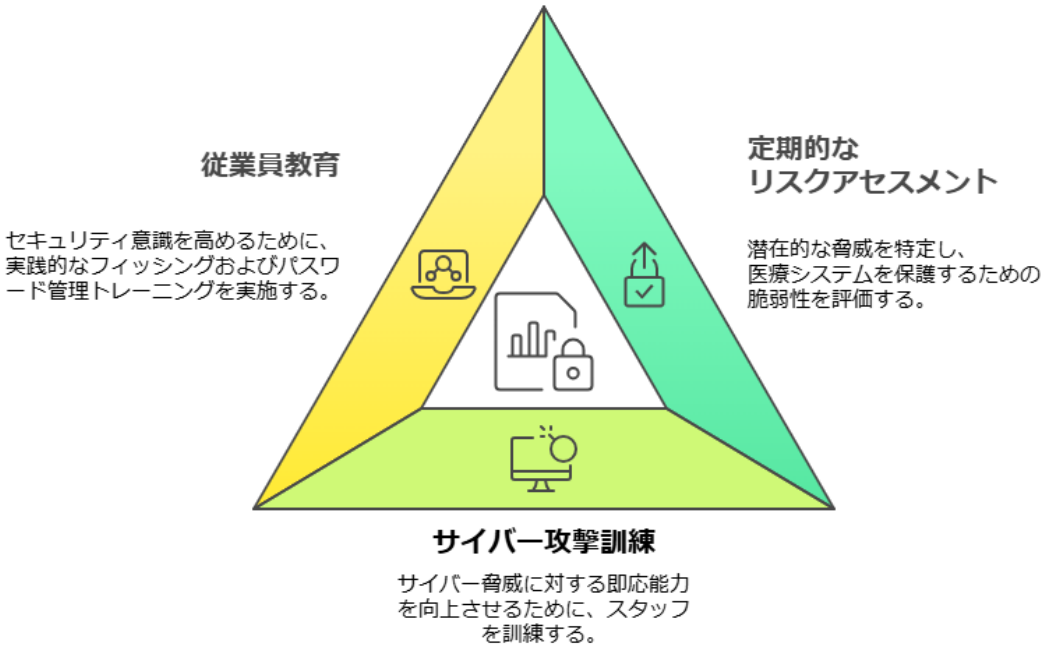
3｜リスク管理と教育の重要性

医療情報システムの安全管理を確実なものにするには、リスク管理と従業員教育が欠かせません。リスク管理では、医療機関が直面する多様な脅威を定量的かつ定性的に評価し、適切な対応策を講じることが求められます。具体的には、定期的なリスクアセスメントの実施や、サイバー攻撃を想定した訓練の導入などです。特に、医療機関特有のリスクとして、医療機器の制御システムへの不正アクセスや、診療の継続性が損なわれるリスクなどを重点的に評価する必要があります。これにより、脅威発生時の即時対応能力を向上させることが可能となります。

一方で、従業員教育も重要な柱です。多くのサイバー攻撃や情報漏洩の原因が人的ミスに起因している現状を踏まえ、全従業員がセキュリティ意識を高めることが強く求められます。その教育プログラムには、フィッシングメールの識別訓練やパスワード管理の適切化など、実践的な内容を含めるべきでしょう。さらに、経営層から現場まで一貫したセキュリティ教育を徹底することで、医療機関全体でリスクに強い組織文化を築くことができます。リスク管理と教育を強化する取り組みは、医療情報の安全性を飛躍的に向上させる鍵となります。

これまで、医療現場におけるセキュリティ対策の強化にふれてきました。では今後、AIや IoT といった新技術が登場する中で、未来の医療情報はどのように変化していくのでしょうか。

◆リスク管理と従業員教育



4 | 未来の医療情報と生成AIの影響

1 | 生成AI活用の可能性と課題

生成 AI の進化により、医療分野では多くの可能性が広がっています。AI を活用することで、診断支援や患者データの効率的な管理が可能となり、医療従事者の負担軽減や業務効率化が期待されています。たとえば、画像診断における AI 活用により、がんの早期発見や診断精度の向上が報告されており、生成 AI を用いた患者情報の整理や問診内容の自動生成も注目を集めています。

しかし、その一方で、プライバシーやセキュリティに対する課題も多くあります。AI が学習する際に大量の医療データを扱うため、データ漏洩や不正利用のリスクが高まるからです。また、生成 AI が生成する情報の正確性や信頼性に対する懸念も払拭できません。

さらに、AI を悪用したサイバー攻撃のリスクも増加しています。これらの課題を解決するためには、AI 活用のルール整備や、AI が生成するデータを検証する仕組みが不可欠となります。このように生成 AI を安全かつ効果的に活用するには、医療機関全体での体制整備と技術的セキュリティ対策の強化が求められます。

◆保健医療分野におけるAI活用推進懇談会報告書概要

【AIの実用化が比較的早いと考えられる領域】

領域	我が国の強み/課題	AIの開発に向けた施策
ゲノム医療	×欧米に比べて取組に遅れ	・実用化まで最も近いのは『がん』であり、実現に向けた推進体制を構築（『がんゲノム医療推進コンソーシアム』で別途検討）
画像診断支援	○診断系医療機器について日本の高い開発能力 ○診断系医療機器の貿易収支も黒字（1,000億円）	・病理・放射線・内視鏡等について、国内には質の高いデータが大量に存在しており、効率的な収集体制の確立が必要 ⇒・関連学会が連携して**画像データベースを構築** ・AIの開発をしやすくするため、薬事審査の評価指標の策定や評価体制の整備も実施
診断・治療支援（問診や一般的検査等）	×医療情報の増大によって医療従事者の負担が増加 ×医師の地域偏在や診療科偏在への対応が必要 ×難病では診断確定までに長い期間	・AIの開発をしやすくするため、**医師法上や医薬品医療機器法上の取扱を明確化** ・各種データベース（ゲノム解析データを含む）の集約等により、難病を幅広くカバーする情報基盤を構築し、AIの開発に活用
医薬品開発	○日本は医薬品創出能力を持つ数少ない国の１つ ○技術貿易収支でも大幅な黒字（3,000億円）	・健康医療分野以外でもAI人材は不足しているため、効率的なAI開発が必要（IT全体で30万人不足、うちAIで5万人不足）であり、製薬企業でもAI人材が不足 ⇒AI人材の有効活用の観点から、**製薬企業とIT企業のマッチングを支援**

【AIの実用化に向けて段階的に取り組むべきと考えられる領域】

介護・認知症	×高齢者の自立支援の促進 ×介護者の業務負担軽減	・現場のニーズに基づかずに開発されたAI（技術指向のAI）では、現場には普及せず ⇒**介護現場のニーズを明確化**し、ニーズに基づく研究開発を実施
手術支援	○手術データの統合の取組で日本が先行 ×外科医は数が少なく、負担軽減が必要	・手術時のデジタル化データ（心拍数、脳波、術野画像等）は相互に連結されていない状態で、手術行為と各種データがリンクせず、AIによる学習が困難 ⇒手術関連データを相互に連結するための**インターフェースの標準化を実施**

厚生労働省：保健医療分野におけるＡＩ活用推進懇談会 報告書

2　新技術による医療情報システムの進化

医療分野では、IoT やブロックチェーンといった新技術の活用が急速に進んでおり、医療情報システムに新たな可能性をもたらしています。

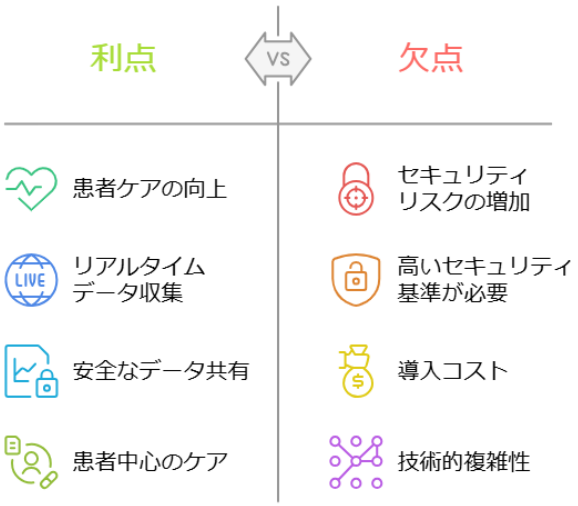
IoT 機器の普及により、患者のバイタルデータをリアルタイムで収集し、遠隔医療や在宅ケアを効率化する取り組みが進行中です。例えば、ウェアラブルデバイスによる心拍数や血圧の継続的なモニタリング、在宅患者の服薬管理を支援するスマートデバイスなど、様々な用途での活用が始まっています。

さらに、ブロックチェーン技術を活用することで、患者情報の真正性を確保し、改ざんを防ぐ仕組みが注目されています。この技術により、医療機関間での安全なデータ共有や患者へのデータアクセス権限の提供が可能となり、患者中心の医療が実現しやすくなります。特に、診療情報の履歴管理や、臨床研究データの信頼性確保において、その効果が期待されています。

しかし、新技術の導入には高いセキュリティ基準を満たすことが求められます。ゼロトラストネットワークモデルの採用や暗号化技術の併用によって、これらの技術のリスクを軽減し、安全な運用体制を確立する必要があります。特に、IoT 機器の脆弱性診断や定期的なファームウェアアップデート、ブロックチェーンネットワークの参加者認証など、きめ細かな対策が重要です。新技術の進化は、医療情報システムに革新をもたらす一方で、万全なセキュリティ対策がその鍵を握っています。

◆医療における IoT とブロックチェーンの統合

◆新しい医療技術の利点と欠点



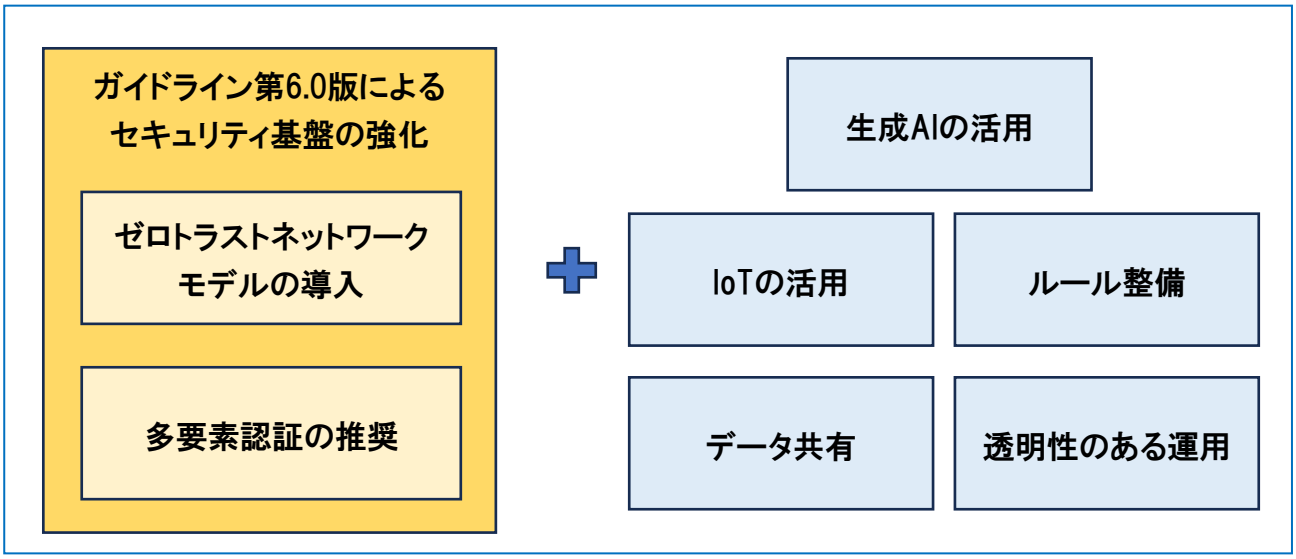
3｜医療機関が目指すべき方向性

医療情報システムの進化とともに、医療機関はデータ主導型の医療を推進する方向性を目指す必要があります。患者情報や診断データの活用により、より正確な診断や治療計画の立案が可能になる一方で、情報の安全性とプライバシー保護は重要な課題として浮上しています。ガイドライン第 6.0 版は、安全性と利便性の両立を図るための具体的な道筋を示しています。特に、ゼロトラストネットワークモデルの導入や多要素認証の推奨など、セキュリティ基盤を強化する施策が重要です。

また、生成 AI や IoT を活用することで、患者中心の医療が実現しやすくなりますが、新技術導入の際にはリスクアセスメントを徹底し、適切なセキュリティ対策を講じる必要があります。さらに、データ共有や活用のルール整備、透明性のある運用が求められます。

医療機関は、技術的な進化を取り入れる一方で、患者の信頼を守るための努力を怠らないことが、今後の成功の可否を握るといっても過言ではありません。

◆医療情報システムにおける目指すべき方向性



医療情報システムの安全性を確保することは、患者の信頼を守り、医療サービスの質を向上させるために欠かせません。ガイドライン第 6.0 版は、サイバーセキュリティ対策をさらに強化し、医療機関全体でのリスク管理を徹底するための道標といえます。

また、生成 AI や IoT など新たな技術の活用により、医療の効率化や精度向上が期待される一方で、これら技術がもたらすセキュリティリスクに対応する必要性も浮き彫りになっています。今後、医療機関は、技術革新とセキュリティ対策を両立させながら、安全で信頼できる医療環境を構築していくことが求められます。

本稿が貴院の医療情報システムのさらなる充実と発展に向けた一助となれば幸いです。

■参考資料

厚生労働省：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
保健医療分野におけるAI開発の方向性について
保健医療分野におけるAI活用推進懇談会　報告書概要