医業経営情報

REPORT

Available Information Report for Medical Management

医業経営

デジタル時代の経営課題

医療機関に求められるサイバーセキュリティ対策

1 医療機関を取り巻くサイバーリスクの現状
2 制度対応と基本対策
3 現場実装モデルと職員・患者対応
4 今後の展望とまとめ

2026
6
JUN

税理士法人　森田会計事務所

医 業
情報レポート

1．医療機関を取り巻くサイバーリスクの現状

医療機関では、電子カルテ、医事会計システム、オンライン資格確認、電子処方箋など、日常診療にかかわる機器の多くがデジタル基盤に支えられています。これらのシステムが停止すれば、受付、診察、検査、処方、会計などの業務に影響し、診療継続そのものが困難になる可能性があります。

近年、医療機関を狙ったサイバー攻撃も確認されており、厚生労働省は、医療情報システムの安全管理やサイバーセキュリティ対策の徹底を求めています。

また、令和５年４月からは、病院・診療所・助産所の管理者が、サイバーセキュリティ確保に必要な措置を講じることが医療法施行規則上にも位置づけられました。

つまり、サイバーセキュリティ対策は、今や、単なる情報漏えい防止策ではなく、診療活動そのものを止めないための経営管理事項となっているのです。

そこで、本レポートでは、医療機関に求められる対策について、厚生労働省資料を中心に、現状、制度対応、現場での実装、今後の経営課題の順に整理します。

1　医療情報システムは診療の基盤

医療機関では、診療録、検査結果、画像データ、処方情報、会計情報、保険資格情報など、多くの情報がシステム上で管理されています。これらの情報は、医師・看護師・事務職員などが診療や業務を行うためには必要不可欠なものばかりです。

電子カルテが使えなければ、過去の診療経過、処方歴、アレルギー情報、検査結果をすぐに確認できないばかりか、医事会計システムが停止すれば、窓口会計や診療報酬請求にも大きく影響します。

つまり、デジタル化が進めば進むほど、サイバーセキュリティ対策は医療安全や診療継続と切り離せないものになっているのです。

■医療 DX の進展とサイバーセキュリティリスクの関係

デジタル化の領域	利便性	停止・障害時の影響
電子カルテ・部門システム	診療情報、検査結果、画像情報を迅速に確認できる	診療経過の確認、検査、処方、説明に支障が生じる
オンライン資格確認・電子処方箋	保険資格や薬剤情報を効率的に確認できる	受付、資格確認、処方・服薬情報確認に遅れが生じる
予約・会計・レセプト	受付、予約、会計、請求を効率化できる	窓口混雑、請求遅延、未収管理の混乱が生じる

厚生労働省：「医療分野のサイバーセキュリティ対策について」をもとに整理

2　サイバー攻撃は情報漏えいだけでなく診療停止に繋がる

医療機関にとって特に深刻なのは、ランサムウェアなどのサイバー攻撃により、長期間にわたって診療が停止する事態です。ランサムウェアとは、システムやデータを暗号化して使えない状態にし、復旧と引き換えに金銭を要求する攻撃を指します。

厚生労働省の病院調査では、病院に対するランサムウェア等のサイバー攻撃が増加し、長期にわたり診療が停止した事例が確認されていることから、リスク把握と有効な対策の実施が必要であるとされています。

この点から、サイバーセキュリティ対策は「情報を守る対策」であると同時に、「診療を止めない対策」として位置づける必要があります。

■医療機関が守るべき主な情報・システム

区分	主なシステム・情報	停止・漏えい時の影響
診療情報	電子カルテ、診療録、検査結果、処方歴	診療経過の確認困難、処方確認の遅延、診療継続への影響
画像情報	PACS、CT・MRI・X 線画像	画像診断、経過比較、読影依頼への影響
会計・請求	医事会計、レセプト請求	窓口会計の遅延、請求業務の停滞
資格確認	オンライン資格確認端末	保険資格確認の遅延、受付混雑
ネットワーク	VPN、ルーター、サーバ、外部保守回線	不正侵入、通信停止、感染拡大のリスク

3　病院調査から見える体制整備の課題

厚生労働省は、令和 7 年 1 月 27 日から令和 7 年 3 月 7 日まで、G-MIS を用いて病院のサイバーセキュリティ対策の実態に関する調査を実施しました。

調査対象は G-MIS ID が付与されている 8,117 病院で、有効回答数は 5,842 施設、回答率は 72.0％です。

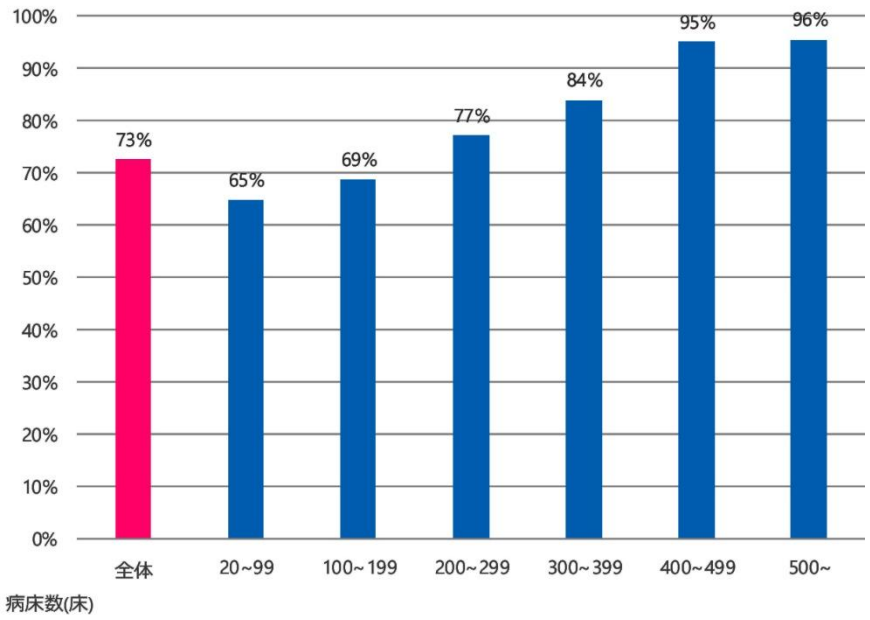
この調査は病院を対象としたものであり、クリニックの実態を直接示すものではありません。

ただし、体制整備、BCP、台帳管理、ネットワーク構成図、バックアップなど、医療機関が優先して確認すべき項目を把握するうえでは重要な参考資料となります。

同調査では、CISO（情報セキュリティを統括する責任者）を設置している病院の割合は全体で 73％でした。病床数の多い病院ほど設置割合が高い傾向があり、20～99 床では 65％、500 床以上では 96％とされています。

中小規模の医療機関では、専任担当者の確保が難しい場合であっても、院長・事務長・委託事業者などが役割を分担し、サイバーセキュリティ対策を進めることが現実的な第一歩と言えるのでしょう。

■CISO を設置している病院の割合



厚生労働省：
「病院における医療情報システムのサイバーセキュリティ対策に係る調査」の結果について（病床別分析結果）

前述の厚生労働省の調査は病院を対象としたものですが、電子カルテ、医事会計、ネットワーク、外部保守回線を利用するクリニックにとっても、確認すべき項目を整理するうえで参考になります。サイバーリスクは、情報管理だけでなく、受付、診療、処方、会計に影響する診療継続上の経営リスクです。

■病院における医療情報システムのサイバーセキュリティ対策調査の概要

背景・目的

○病院に対するランサムウェア等のサイバー攻撃が増加し、長期にわたり診療が停止した事例が確認されていることから、病院におけるランサムウェアのリスクを把握するとともに、長期に診療が停止することがないよう早急に有効な対策の実施を促すことが必要である。
○本調査の目的は、病院が保有する電子カルテシステム等の医療情報システムのサイバーセキュリティ対策の実態を調査し、これまでの政策の効果確認に加え、今後の政策方針の決定に資するものとすることである。

調査方法・対象

- G-MIS（Gathering Medical Information System）を用いて、病院のサイバーセキュリティ対策の実態に関するアンケート調査を実施。
- 調査対象は、G-MIS IDが付与されている、8,117の病院。
- 有効回答数：5,842（72.0%）施設（昨年度：65.5%）
- 令和 5 年 5 月 31 日に発出された「医療情報 システム の安全管理に関するガイドライン（6.0 版）」、令和 7 年 5 月に発出された「医療機関 における サイバーセキュリティ対策チェックリスト」 及び 厚生労働省等から発出された通知・事務連絡 等において周知した対策への取組状況について質問する。

調査期間

・令和7年1月27日（月）～　令和7年3月7日（金）

厚生労働省：「病院における医療情報システムのサイバーセキュリティ対策に係る調査」の結果について（病床別分析結果）

2．制度対応と基本対策

1　管理者が講じるべき対策

令和５年４月１日から、病院、診療所、助産所の管理者が遵守すべき事項に、サイバーセキュリティの確保が位置づけられました。厚生労働省資料では、医療法施行規則第 14 条第２項を新設し、医療の提供に著しい支障を及ぼすおそれがないよう、サイバーセキュリティを確保するために必要な措置を講じることが示されています。

ここで重要なのは、対象に「診療所」が含まれている点です。小規模クリニックであっても、電子カルテ、レセコン、予約システム、オンライン資格確認端末、院内ネットワーク、外部保守回線などを利用している場合、サイバーリスクが存在するのは当然のことです。

また、外部ベンダーにシステム管理を委託していても、診療継続、患者情報保護、職員教育、緊急時対応の確認責任は医療機関側に残ります。経営層は、ベンダー任せにせず、自院のシステム構成と緊急時の対応策を講じる必要があります。

2　確認すべき基本的な対策

厚生労働省は、医療機関等が優先的に取り組むべき事項を「令和７年度版 医療機関におけるサイバーセキュリティ対策チェックリスト」として整理しています。

同チェックリストは、専門的な知識が十分でない医療機関でも、現状を「はい・いいえ」で確認し、「いいえ」の項目について対応目標日を記入できる実務的な仕様となっています。

■令和７年度版チェックリストの主要項目

分類	主な確認項目	経営層が確認すべき視点
体制構築	医療情報システム安全管理責任者の設置	責任者・副担当者・報告先が決まっているか
機器管理	サーバ、端末 PC、ネットワーク機器の台帳管理	どの機器がどこにあり、誰が保守しているか
委託先管理	リモート保守機器の確認、MDS/SDS の確認	外部接続点とベンダーの責任範囲を把握しているか
アクセス管理	職種・担当業務別の権限設定、不要アカウント削除	退職者 ID や過剰権限を放置していないか
インシデント対応	連絡体制、バックアップ、BCP 策定の有無	停止時に誰へ連絡し、どう診療継続するか
規程整備	実施方法を運用管理規程等に定める	運用が担当者任せになっていないか

厚生労働省：「令和７年度版 医療機関におけるサイバーセキュリティ対策チェックリスト」をもとに整理

3　インシデント発生時の報告と対応

サイバー攻撃を完全に防ぐことは困難です。そのため、医療機関は「発生しない前提」ではなく、「発生した場合にどう動くか」を事前に決めておく必要があります。

厚生労働省は、医療機関等がサイバー攻撃を受けた場合、またはその疑いがある場合、さらに医療情報システムの障害が発生した場合には、速やかに厚生労働省へ連絡するよう求めています。

サイバー攻撃等により、患者の個人情報を含む医療情報など個人データの漏えい、または漏えいのおそれが発生した場合には、個人情報保護委員会への報告が必要とされています。現場で重要なのは、異常に気づいた職員が、どこへ報告すればよいか迷わないことです。

■サイバーインシデント発生時の初動対応フロー

段階	対応内容	確認ポイント
1	電子カルテが開かない、不審画面が出る、複数端末で異常がある等を確認	現場判断で再起動や操作を続けない
2	医療情報システム安全管理責任者、院長、事務長へ連絡	連絡先一覧を常備する
3	停止しているシステム、端末、部門、患者対応への影響を整理	記録は時系列で残す
4	電子カルテ、ネットワーク等専門の保守業者へ連絡	契約範囲と緊急連絡先を確認
5	サイバー攻撃または疑いがある場合、速やかに厚労省へ連絡	発生日時、状況、影響範囲を簡潔に整理
6	紙運用、予約変更、処方対応、会計対応を決定	BCP に沿って職員へ指示
7	復旧手順の実行、原因整理、再発防止策の検討	事後に規程・訓練を見直す

厚生労働省：「医療分野のサイバーセキュリティ対策について」をもとに整理

漏えい等の有無が確定してから対応するのではなく、「漏えいのおそれ」がある段階でも、報告要否、患者説明、問い合わせ対応、復旧状況の確認を速やかに進めることが重要です。

4　個人情報漏えい時の考え方

医療情報には、病名、検査結果、服薬歴、手術歴、画像情報など、患者の私生活や健康状態に関わる極めて重要な情報が含まれます。サイバー攻撃によりこれらの情報が漏えいした場合、

患者本人だけでなく、家族や地域社会との信頼関係にも大きく影響します。

医療機関の経営層は、漏えい等の有無が確定してから対応するのではなく、「漏えいのおそれ」がある段階でも、報告要否、患者説明、問い合わせ対応、復旧状況の確認を速やかに進めるなど、患者情報を守ることを医療安全と同じ経営責任として捉える必要があります。

令和７年度版チェックリストは、医療機関が自院の対策状況を確認するための実務的な資料です。確認対象には、医療情報システム安全管理責任者、機器台帳、リモート保守、アクセス権限、不要アカウント、バックアップ、BCP、規程類の整備などが含まれます。

システム保守を外部ベンダーに委託している場合でも、委託先の責任範囲、緊急連絡先、復旧時の対応時間、リモート保守の接続経路は医療機関側で把握しておきます。

■令和７年度版 医療機関におけるサイバーセキュリティ対策チェックリスト

資料2-2

令和７年度版
医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

*立入検査時、本チェックリストを確認します。令和7年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*「いいえ」の場合、令和7年度中の対応目標日を記入してください。

	チェック項目	確認日	目標日	備考
1 体制構築	医療情報システム安全管理責任者を設置している。(1-①)	はい・いいえ (/)	(/)	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2-①)	はい・いいえ (/)	(/)	
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-②) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-③) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。※管理者権限対象者の明確化を行っている(2-④)	はい・いいえ (/)	(/)	
	退職者や使用していないアカウント等、不要なアカウントを削除または無効化している。(2-⑤)	はい・いいえ (/)	(/)	
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-⑥)	はい・いいえ (/)	(/)	
	パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(2-⑦)	はい・いいえ (/)	(/)	
	パスワードの使い回しを禁止している。(2-⑧)	はい・いいえ (/)	(/)	
	USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。(2-⑨)	はい・いいえ (/)		
	二要素認証を実装している。または令和９年度までに実装予定である。(2-⑩)	はい・いいえ (/)	(/)	
	サーバについて、以下を実施している。			
	アクセスログを管理している。(2-⑪)	はい・いいえ (/)	(/)	
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ (/)	(/)	
	端末PCについて、以下を実施している。			
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-⑫)	はい・いいえ (/)	(/)	
	ネットワーク機器について、以下を実施している。			
	接続元制限を実施している。(2-⑬)	はい・いいえ (/)	(/)	
3 インシデント発生に備えた対応	インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。(3-①)	はい・いいえ (/)	(/)	
	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。(3-②)	はい・いいえ (/)	(/)	
	サイバー攻撃を想定した事業継続計画（BCP）を策定している。(3-③)	はい・いいえ (/)	(/)	
4 規程類の整備	上記1-3のすべての項目について、具体的な実施方法を運用管理規程等に定めている。(4-①)	はい・いいえ (/)	(/)	

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 各チェック項目に記載された番号はチェックリストマニュアルのアウトラインに対応しています。

厚生労働省：令和７年度版医療機関におけるサイバーセキュリティ対策チェックリスト

3．現場実装モデルと職員・患者対応

1　優先すべき対策

中小規模の医療機関では、予算や人員に限りがあります。そのため、サイバーセキュリティ対策を「専門的で難しいもの」と捉えすぎると、何から始めればよいか分からなくなります。

重要なのは、厚生労働省のチェックリストに沿って、優先順位を決めて実施することです。

最初に取り組むべき点は、責任者の設置、機器台帳の整備、外部接続点の把握、アクセス権限の確認、不要アカウントの削除、バックアップの確認、インシデント時の連絡体制、BCP の作成です。これらは高度なセキュリティ製品の導入以前に、自院の管理状態を見える化するための基本対策となります。

特に重要なのが台帳管理です。サーバ、端末 PC、ネットワーク機器、オンライン資格確認端末、外部保守用機器など、院内にどの機器があるか分からない状態では、脆弱性対応や故障対応はおろか、感染拡大防止もできません。クリニックでは、エクセル等の簡易な形式で構わないので、機器名、設置場所、用途、保守業者、導入年月、更新期限、外部接続の有無を整理し、管理することを徹底します。

2　バックアップは「取る」だけでなく「戻せる」ことが重要

サイバー攻撃対策で最も重要な実務項目の一つがバックアップです。しかし、バックアップは「データを保存している」だけでは十分ではありません。

復旧できる形式で保存されているか、世代管理されているか、ネットワークから切り離されているか、復旧手順を確認しているかといった対応が求められます。

厚生労働省の病院調査では、電子カルテシステムのバックアップデータを作成している病院は 97%である一方、バックアップデータを 3 つ以上保管している割合は 43%、オフラインでバックアップデータを保管している割合は 64%とされています。

ランサムウェアでは、ネットワークに接続されたバックアップまで暗号化される可能性があるため、複数世代・複数方式・オフライン保管の確認が重要となります。

■バックアップ確認のポイント

確認項目	内容	確認時の質問例
バックアップデータの有無	電子カルテ等の重要データを保存しているか	どのシステムを対象に、どの頻度で取得しているか
世代管理	複数世代で保存しているか	直近データだけでなく、過去時点に戻せるか
保管方式	複数方式で保存しているか	院内サーバ、外部媒体、クラウド等の構成はどうか

オフライン保管	ネットワークから切り離した保管があるか	ランサムウェア感染時にも利用できるか
復旧手順	誰が、どの順番で復旧するか	ベンダーの対応時間、復旧目標は明確か
復旧訓練	実際に戻せるか確認しているか	机上訓練またはテスト復元を行っているか

厚生労働省：「医療分野のサイバーセキュリティ対策について」をもとに整理

3　サイバー攻撃を想定した BCP

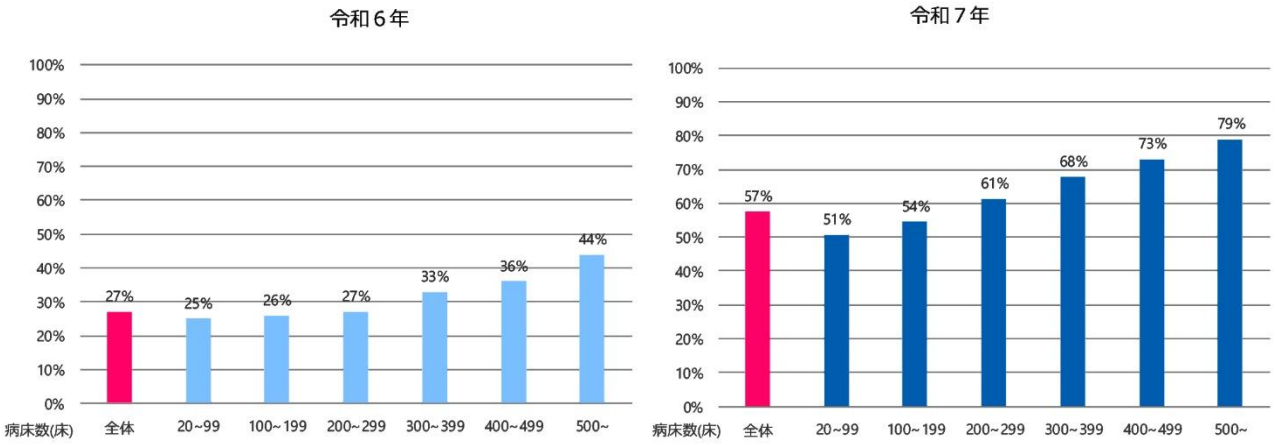
BCP とは、事業継続計画のことです。医療機関における BCP は、災害や感染症だけでなく、サイバー攻撃によるシステム停止にも対応することも忘れてはなりません。

電子カルテが使えない場合、受付をどう行うか、診療録をどう記録するか、処方をどう出すか、検査結果をどう確認するか、会計をどう処理するかを事前に決めておくべきでしょう。

厚生労働省の病院調査では、サイバー攻撃によるシステム障害発生時に備えて BCP を策定している病院は 57％でした。

一方、BCP を策定している病院のうち、対処手順が適切に機能するか訓練等で確認している病院は 38％とされています。BCP は作成するだけではなく、実際に使えるかを確認しておく必要があります。

■サイバー攻撃を想定した BCP 策定・訓練状況



厚生労働省：病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について

クリニックでは、簡易な BCP でも構いません。例えば、電子カルテが使えない場合の紙問診票、紙カルテ様式、紙処方箋の運用、予約患者への連絡方法、会計処理の一時対応、復旧後の入力方法などを決めておくことが現実的です。

重要なのは、緊急時に職員が迷わず動けることです。

また、職員教育も不可欠です。厚生労働省は、医療機関向けセキュリティ教育支援ポータルサイト「MIST」を公開しており、経営層や医療従事者など階層別の研修、院内教育に活用できるコンテンツ、インシデント発生時の相談・初動対応依頼窓口を案内しています。

4　職員教育と患者への説明

サイバーセキュリティ対策は、機器やシステムだけでは完結しません。職員が不審なメールを開く、USB メモリを不用意に接続する、パスワードを使い回す、退職者アカウントを放置するなど、日常業務の小さな行動もリスクとなります。

職員教育では、専門用語を多用するよりも、まずは「不審な添付ファイルを開かない」「不審な画面が出たら自分で操作せず報告する」など、日常行動に落とし込むことが肝要です。

■セキュリティ教育支援ポータルサイト

厚生労働省：医療機関向けセキュリティ教育支援ポータルサイト

また、患者への説明も重要です。システム障害により受付や会計が遅れる場合、オンライン資格確認が一時的に使えない場合、紙運用に切り替える場合など、あらかじめ患者に対して分かりやすく説明することで、不安や混乱を抑えることができます。

4．今後の展望とまとめ

1　サイバーセキュリティは診療継続への投資

医療 DX が進むほど、医療機関の業務はデジタル基盤に依存することになります。したがって、電子カルテ、オンライン資格確認、電子処方箋、医療情報連携、オンライン診療などが広がる中で、サイバーセキュリティ対策は、医療 DX と一体で考える必要があります。

経営層に求められるのは、サイバーセキュリティを単なる費用ではなく、診療継続、患者情報保護、医療機関の信用維持のための投資として位置づけることです。

患者数の多い時間帯にシステムが停止すれば、短時間であっても外来診療、処方、会計、予約管理に影響します。

医療機関の信用は、一度大きく損なわれると回復に時間がかかります。患者情報の漏えいや診療停止が発生すれば、患者、家族、地域住民、取引先、行政からの信頼に影響します。そういった事態を避けるためにも、サイバーセキュリティ対策は、経営リスク管理の一部として考えるべきでしょう。

2　確認すべき７つの実装項目

経営層は、技術的な細部をすべて理解する必要はありません。しかし、自院が最低限の対策を実施しているか、緊急時に診療を継続できるか、ベンダー任せになっていないかは確認する必要があります。

■優先対策ロードマップ

優先順位	実施項目	内容
1	責任者を決める	医療情報システム安全管理責任者を設置し、院長・事務長・担当者・ベンダーの役割を明確にする
2	現状を見える化する	機器台帳、ネットワーク構成、外部接続点、保守業者を一覧化する
3	委託先を確認する	ベンダーの保守範囲、緊急連絡先、MDS/SDS、復旧対応時間を確認する
4	アカウントを整理する	退職者 ID、不要 ID、管理者権限、共有 ID の有無を確認する
5	バックアップを確認する	複数世代、オフライン保管、復旧手順、テスト復元の有無を確認する
6	BCP を作成する	電子カルテ停止時の紙運用、処方、会計、患者連絡、復旧後の入力方法を決める
7	職員教育を行う	年 1 回以上、不審メール、パスワード、USB 利用、異常時報告を確認する

3　従業員・患者に求められる行動

サイバーセキュリティ対策は、経営層だけでなく、すべての従業員が関わる問題です。

医師、看護師、医療事務、検査技師、リハビリ職、管理部門職員など、システムを使う全員が、基本的なルールを理解しておかなくてはなりません。

従業員に求められる行動は、決して難しいものではありません。不審なメールや添付ファイルを開かない、パスワードを共有しない、離席時に画面をロックする、USB メモリなど外部記録媒体を無断で使わない、不審な画面や動作を見つけたらすぐ報告する、といった日常的な行動です。

特に重要なのは、「おかしい」と感じたときに、すぐ報告できる文化をつくることです。職員が叱責されることを恐れて報告を遅らせると、被害が拡大する可能性があります。

経営層は、ミスを責めるよりも、早期報告を評価する姿勢を明確にする必要があります。

■医療情報の取扱いに関する法律上の責任

●説明責任

医療情報システムの機能や運用を、必要に応じて患者等に説明できるように、システム機能仕様やシステム運用手順等について、システム関連事業者の協力を得ながら文書化し、管理しておく。

●管理責任

個人情報保護法第 23 条において「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定されているとおり、医療機関等は個人情報取扱事業者として、医療情報システムの管理実態や責任の所在を明確にする必要があり、システム関連事業者の協力を得ながら、システムの管理や運用が適切に行われているかどうかを監督する。

●定期的な見直し、必要に応じた改善を行う責任

医療機関等で利用している医療情報システムを提供するシステム関連事業者の協力を得ながら、医療機関等として安全管理の改善に必要な情報を収集し、必要に応じて、文書化して管理しているシステム運用手順を改善する。

また、サイバーセキュリティ対策は、患者にとっても無関係ではありません。

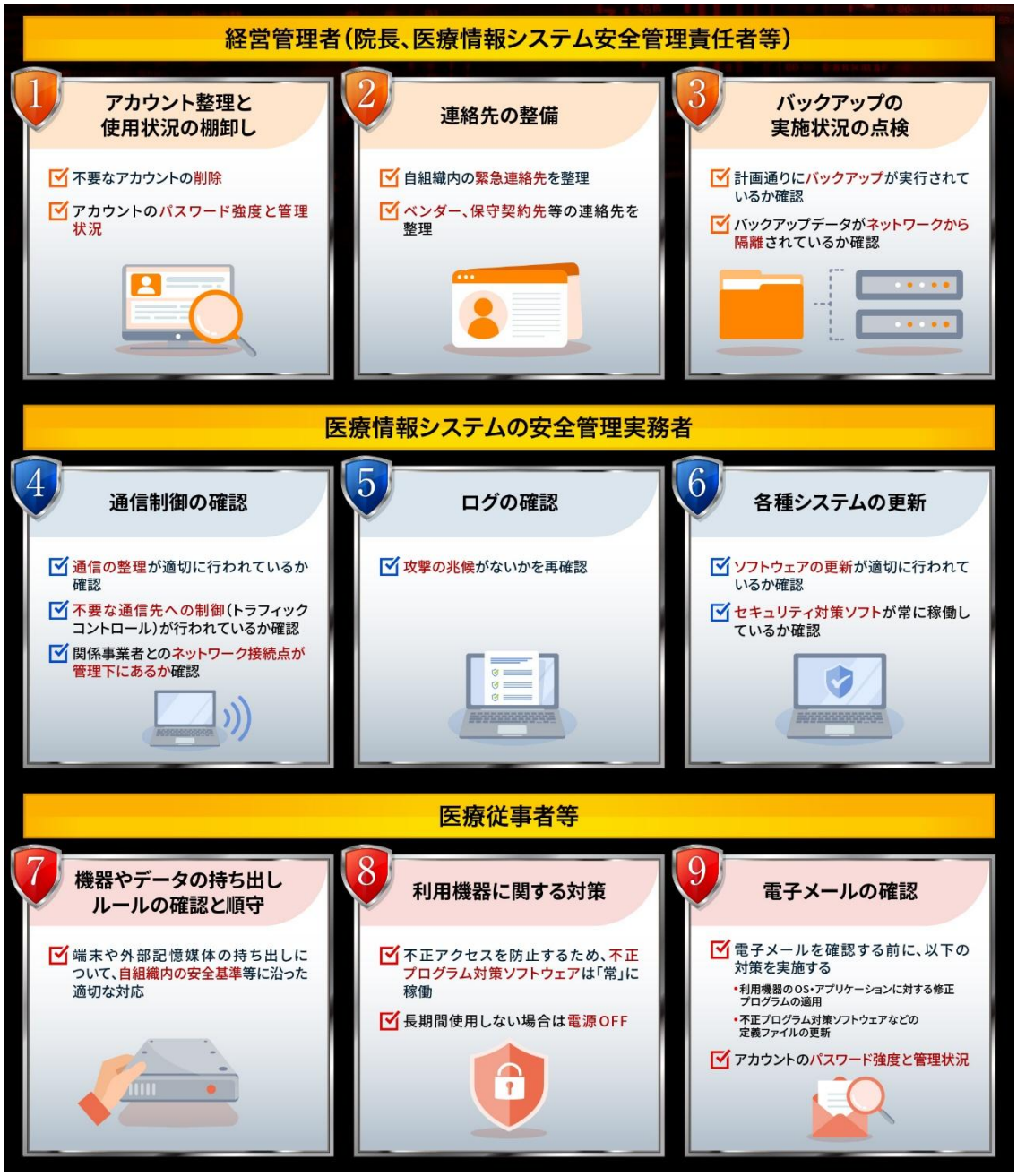
医療機関が本人確認を行う、保険証やマイナンバーカードの確認を丁寧に行う、診療情報の取り扱いについて説明する、システム障害時に紙で対応することは、患者情報を守り、診療を継続するための対応です。

4　まとめ

医療機関におけるサイバーセキュリティ対策は、デジタル時代必須の経営課題です。電子カルテや医事会計システムが日常診療の基盤となった現在、サイバー攻撃やシステム障害は、情報漏えいだけでなく、診療停止、患者対応の混乱、経営上の損失につながります。

サイバーセキュリティ対策の目的は、システムを守ることだけではありません。最終的な目的は、患者の診療を止めないこと、患者情報を守ること、地域から信頼される医療機関であり続けることです。医療機関の経営層は、サイバーセキュリティを「専門部署の仕事」ではなく、「経営の基本」として位置づけ、継続的に確認・改善していくことが求められます。

■サイバーセキュリティ９の心得



厚生労働省：サイバーセキュリティ９の心得

■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 第 6.0 版、概説編、経営管理編

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［特集］
医療機関等におけるサイバーセキュリティ
小規模医療機関等向けガイダンス

医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル

令和７年度版 医療機関におけるサイバーセキュリティ対策チェックリスト

病院における医療情報システムのサイバーセキュリティ対策に係る調査の結果について
（病床別分析結果）

医療分野のサイバーセキュリティ対策について

医療法施行規則の一部を改正する省令について（通知）

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表、策定の確認表のための手引き

医療情報システム部門等における BCP のひな形

医療機関向けセキュリティ教育支援ポータルサイト MIST

サイバーセキュリティ９の心得

医業経営情報レポート

デジタル時代の経営課題医療機関に求められるサイバーセキュリティ対策

【著 者】日本ビズアップ株式会社

【発 行】税理士法人　森田会計事務所

〒630-8247　奈良市油阪町 456 番地　第二森田ビル 4F

TEL 0742-22-3578　　FAX 0742-27-1681
