⑥　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。
（医療情報システム全般）

▶システム運用編
8③
8.1
8.2
13.2

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが挙げられます。

なお、医療情報システムを、今後新規導入又は更新するに際しては、保守契約の見直しや運用管理規程の変更により、セキュリティパッチを定期的に適用できる等適切な安全管理体制の構築に努めることが重要です。その際、事業者等との契約時の取り決めについては、参考資料として「医療情報システムの契約における当事者間の役割分担に関する確認表」（※）が挙げられます。

（用語の解説）

パターンファイル：ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。

（補足）

古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

※医療情報システムの契約における当事者間の役割分担等に関する確認表 （METI/経済産業省）

⑦　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　（医療情報システム全般）

▶システム運用編
8.⑤

情報機器に対して起動時のパスワード等を設定すること、設定に当たっては出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば定期的なパスワードの変更等の対策を実施することが求められます（※）。

端末 PC のログインパスワードのみならず、サーバやネットワーク機器のパスワードが推定しやすいものであると、サイバー攻撃の起点となります。サーバ、ネットワーク機器のパスワードを事業者が管理している場合、医療機関等は事業者確認用チェックリストを用いて、事業者の設定、運用しているパスワードがガイドラインの要件を満たすものであるかを確認する必要があります。

この際、事業者側は各医療機関等のパスワードのリストについて、漏洩リスクを最小限とする様、厳重に管理する必要があります。

医療機関等の端末 PC においても、ユーザ向けログインパスワードをモニターに付箋で貼る等の管理は絶対に避けなければなりません。

なお、利用するパスワードが 13 文字以上のランダムな設定がなされており、パスワード管理の安全性などが担保されているシステムを用いている場合には、パスワードの定期的変更は必ずしも求められません。また、二要素以上の認証の場合、ID/パスワードのみの認証よりも安全性が高いことから、８文字以上の推定困難な文字列であれば定期的な変更は求めないこととしています。定期的な更新が難しい場合はこのような設定をご参考ください。

●強固なパスワードの例

･英数字、記号を混在させた 13 文字以上の推定困難な文字列

･英数字、記号を混在させた８文字以上の推定困難な文字列を定期的に変更させる

･二要素以上の認証の場合、英数字、記号を混在させた８文字以上の推定困難な文字列

･複数の機器や外部サービス等で、同一のパスワードを設定しない

⑧　パスワードの使い回しを禁止している。（医療情報システム全般）

パスワードの使い回しは漏えいリスクを高め、一度の漏えいにより被害範囲が拡大するため、複数の機器や外部サービス等で、同一のパスワードを設定しないことが必要です。

事業者においては、事業者内及び、医療機関等に設置したサーバ、ネットワーク機器等について、パスワードの使い回しが行われていないか確認してください。

〈危険なパスワード使い回し例〉

- 施設内のサーバ、ネットワーク機器等に同一のパスワードを用いている
- 事業者が契約している複数施設に対して同一のパスワードを用いて管理している
- 出荷時のパスワードから変更を行っていない

▶システム運用編 8.⑤

⑨　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。（医療情報システム全般）

記録媒体や情報機器等の利用は、持ち出し先での紛失や盗難のほか、医療情報システムの端末 PC やサーバに USB ストレージ経由での不正ソフトウェア混入が想定されます。

他の医療情報システムや医療機器等にマルウェア感染が広がる事を防ぐべく、USB ストレージ等の外部接続機器に対して接続の制限を行う必要があります。業務の必要性に応じて外部接続機器を利用する場合には、記録媒体及び記録機器の保管及び取扱いについて適切に行う必要があります。

・医療情報の持ち出しが可能となる記録媒体や情報機器等を限定する（※）。
・医療情報の持ち出しに対する手続等の運用管理規程を策定する。
・記録媒体・情報機器等を医療機関等に持ち帰った場合のそれらの確認に関する手続等の運用管理規程を策定する。

等を行うことが求められます。

※例えば病院等の情報システム部門が管理する特定の記録媒体以外の読み込みを不能とし、利用前の記録媒体へのウイルススキャンや利用後の初期化を行う等の対策が想定されます。

事業者においては、医療機関等からの依頼に基づいて USB 等の接続制限を行っている、又は医療情報システムがその機能を有するか医療機関等への情報提供を行ってください。

▶企画管理編 8.2.2
▶システム運用編 8.①

⑩　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。
（医療情報システム全般）

ガイドラインでは令和３年１月に発出された 5.1 版以降すべての版において、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、新規導入または更新するに際しては、二要素認証を採用するシステムの導入、またはこれに相当する対応を行うことを求めています。二要素認証の導入・改修にあたっては、一定程度の費用が見込まれますので計画的なシステム更新を推奨します。

本項目は、医療情報システムの利用者認証のみならず、医療情報システム全般として、サーバ、端末 PC、ネットワーク機器への認証技術実装を指します。

なお、緊急時等で二要素認証が利用できない場合に代替手段を利用する場合には、システム運用担当者等においてシステム及び利用者を適切に管理できる体制を整えておくことが重要である。

●二要素認証の採用例（記憶・生体情報・物理媒体の２種類を組み合わせたもの）
①パスワード＋指紋認証　②IC カード＋パスワード　③IC カード＋指紋認証

▶システム運用編
14.⑤
14.1.1

⑪　アクセスログを管理している。（サーバ）

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに、企画管理者等はそのログを定期的に確認してください。例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録することが必要です。

アクセスログは立入検査の際に直接確認する可能性があります。

（補足）

アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を併せて講じてください。

●アクセスログの例

ユーザーID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16 8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16 8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16 8:31:00	入力メニュー	起動
abc@def	abcdef	2023/5/16 8:32:00	入力メニュー	カルテ入力
abc@def	abcdef	2023/5/17 12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17 8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 8:45:00	管理メニュー	ログオフ
・	・	・	・	・

▶経営管理編
4.2
▶企画管理編
5.3
▶システム運用編
17①②

⑫ 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。（サーバ、端末 PC）

不正ソフトウェアは電子メール、ネットワーク等の様々な経路を利用して医療情報システム内に侵入する可能性があります。

システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者等に相談の上、対策を講じてください。

▶システム運用編 8.1

⑬ 接続元制限を実施している。（ネットワーク機器）

外部ネットワークに接続する際には、ネットワークや機器等を適切に選定し、監視を行うことが必要です。

特に、無線 LAN を使用する際は不正アクセス対策として適切な利用者以外に無線 LAN を利用されないようにすることが重要です。システム運用担当者は、例えば、ネットワーク機器に接続出来る MAC アドレスが限定すること等、不正アクセス対策を実施してください。

（用語の解説）

MAC アドレス：Media Access Control アドレスの略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号。インターネットでは IP アドレス以外にも MAC アドレスを使用して通信を行っています。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはありません。

（補足）

MAC アドレスによるアクセス制限の効果は限定的であることに留意する必要がありますので、追加の対策はガイドラインや事業者とも確認をお願いします。

▶システム運用編 13⑪

3　インシデント発生に備えた対応　【医療機関等確認用】

①　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）の連絡体制図がある。

医療機関等の経営層等は情報セキュリティインシデント発生に備え、事業者や外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者等に指示することが重要です。

企画管理者等はサイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成して下さい。連絡体制図には施設内の連絡先に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定されます。

このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

立入検査時は、連絡体制図が作成されていることを確認します。

（用語の解説）

CSIRT: 「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるイシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

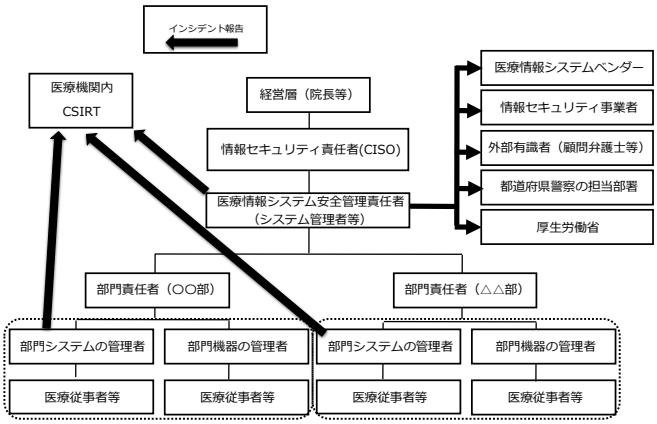
（補足）

サイバー攻撃を受けた疑いがある場合は、下記の厚生労働省の連絡先に御連絡ください。

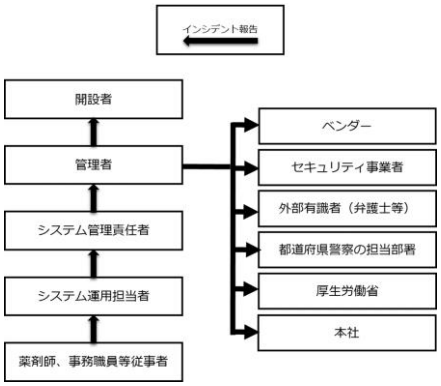
【連絡先】厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室　03-6812-7837

▶経営管理編
3.4.2①
3.4.3①
▶企画管理編
12.3

●連絡体制図の例１（医療機関）



●連絡体制図の例２（薬局）



② 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。

非常時でも、稼働が損なわれた医療情報システムを復旧できるよう、情報システムやデータ等のバックアップを適切に確保し、その復旧手順を整備・確認しておくことが求められます。企画管理者等はバックアップを確保する際、重要なファイルについては、不正ソフトウェアの混入による影響が波及しないよう複数の方式で世代管理するよう設計し、システム運用担当者は手順に従いバックアップを確保してください。復旧手順の整備については、例えば、BCP に復旧手順を定めるなどの方法が挙げられます。

（用語の解説）

世代管理：バックアップの一種で、最新データだけでなく、それ以前のデータもバックアップする方法を指します。例えば、３世代以上で管理する場合、日次でバックアップを行うならば、「3 世代以上」とは「３日以上」のバックアップを確保することになります。

（補足）

３世代目以降のバックアップはオフライン（物理的あるいは論理的に書き込み不可の状態）にする等の対策が望ましいです。

▶経営管理編
3.4.1
▶企画管理編
11.2
12.2
▶システム運用編
11.1
12.2
18.1

③ 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。

医療機関等の経営層等は企画管理者等と連携して非常時における業務継続の可否の判断基準や継続する業務選定等の意思決定プロセスを検討し、サイバー攻撃を想定した BCP 等を整備することとしています。この BCP を整備しておくことにより、万が一サイバー攻撃を受けても重要業務が中断しない、または中断しても短い期間で再開することが期待できます。

▶経営管理編
3.4.1
▶企画管理編
11.1

4　規程類の整備　【医療機関等確認用】

①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。
（医療情報システム全般）

医療情報システムの安全管理が適切に行われるためには、組織内において明文化されたルールが必要となります。例えば、

・医療情報システムの利用ができる機器の管理方法

例）システム管理者は不正な利用の防止および発見に向け、情報システムの利用者ごとに適切なアクセス権限を付与したアカウントを登録し、定期的に操作ログを確認する。

・医療情報システムに異常が生じた場合の対応

例）災害、サイバー攻撃等により、一部医療行為の停止等、医療サービス提供体制に支障が発生する非常時の場合、別途定める事業継続計画（BCP）に従って運用を行う。

・職員の情報セキュリティなどに関する教育や訓練に関すること

例）システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行う。

などが挙げられ、経営層や企画管理者が管理できるようにすることが求められます。これらの内容について、医療情報システムの安全管理に関するガイドラインや小規模医療機関等向けガイダンス等を参考にして策定してください。

立入検査時は、本規程類も確認対象となります。

▶企画管理編 4.1