令和6年度医療情報セキュリティ研修 及びサイバーセキュリティインシデント発生時初動対応支援・調査等事業　（一般社団法人ソフトウェア協会）

【立入検査研修】 準備コース

BC Signpost株式会社
松山 征嗣

立入検査研修
目次

準備コース

- チェックリスト概要
- チェックリストのマニュアルについて
- チェックリストの進め方
- 「医療情報システムの有無」について
- 用語解説

医療機関向け　前編

主に組織、システム全体的なもの

- １．体制構築
- ３．インシデント発生に備えた対応
- ２．医療情報システムの管理・運用
  - 全般

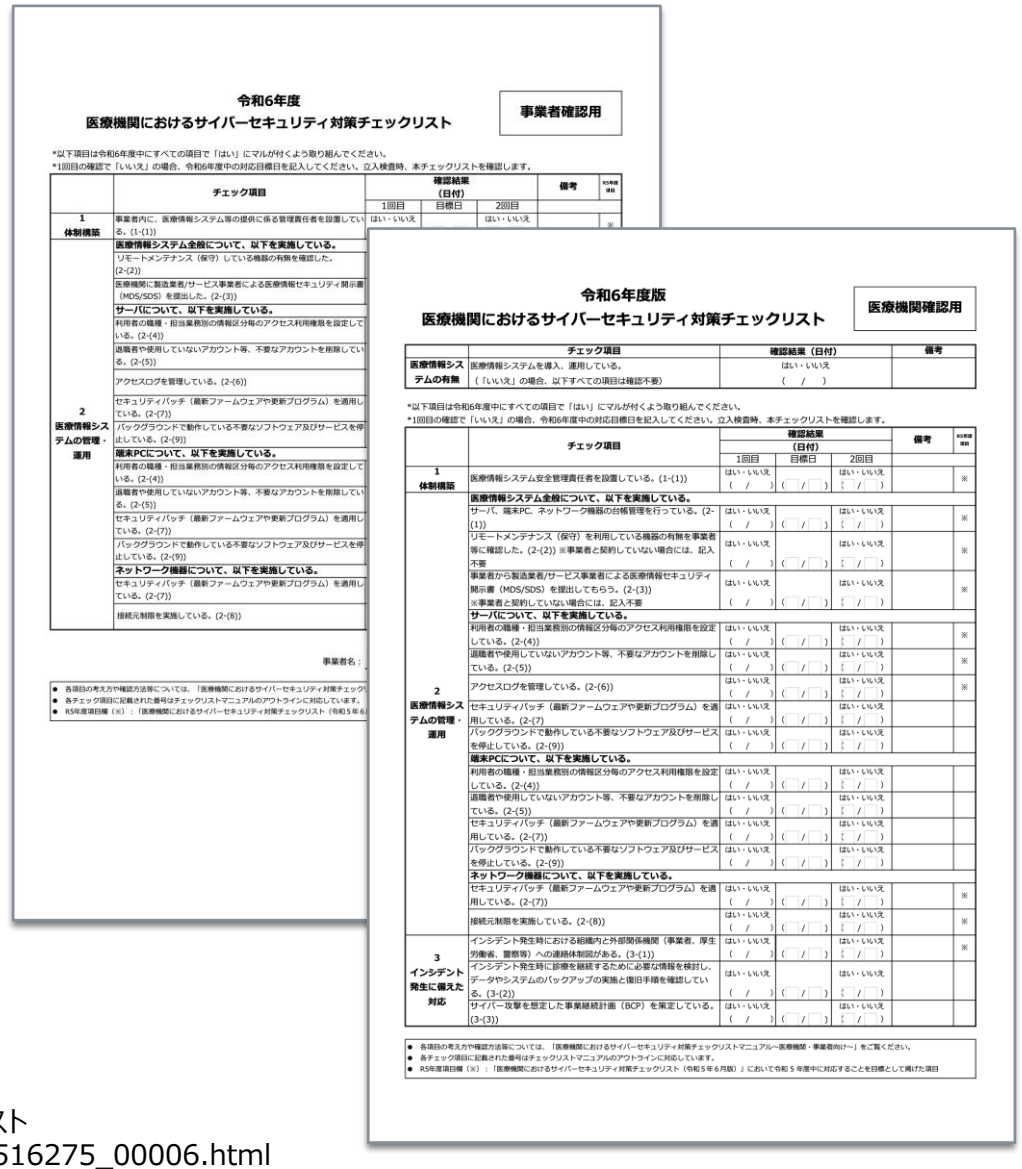
医療機関向け　後編

主に技術的なもの

- ２．医療情報システムの管理・運用
  - サーバおよび端末PC
  - ネットワーク

「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」について

- 医療機関等におけるサイバーセキュリティ対策については、「医療情報システムの安全管理に関するガイドライン」を参照の上、適切な対応を行う必要があります。
- このうち医療機関が**優先的に取り組むべき事項**をチェックリストとしてまとめられています。
- このチェックリストによってサイバー攻撃を回避できると約束されるものではありません。
- 令和５年度より、本チェックリストが医療法第25条第１項に基づく立入検査においてサイバーセキュリティ確保のために必要な取組を行っているかの確認に使用されています。


令和6年度
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
事業者確認用

令和6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

医療DX推進環境を整え
医療の向上を図る

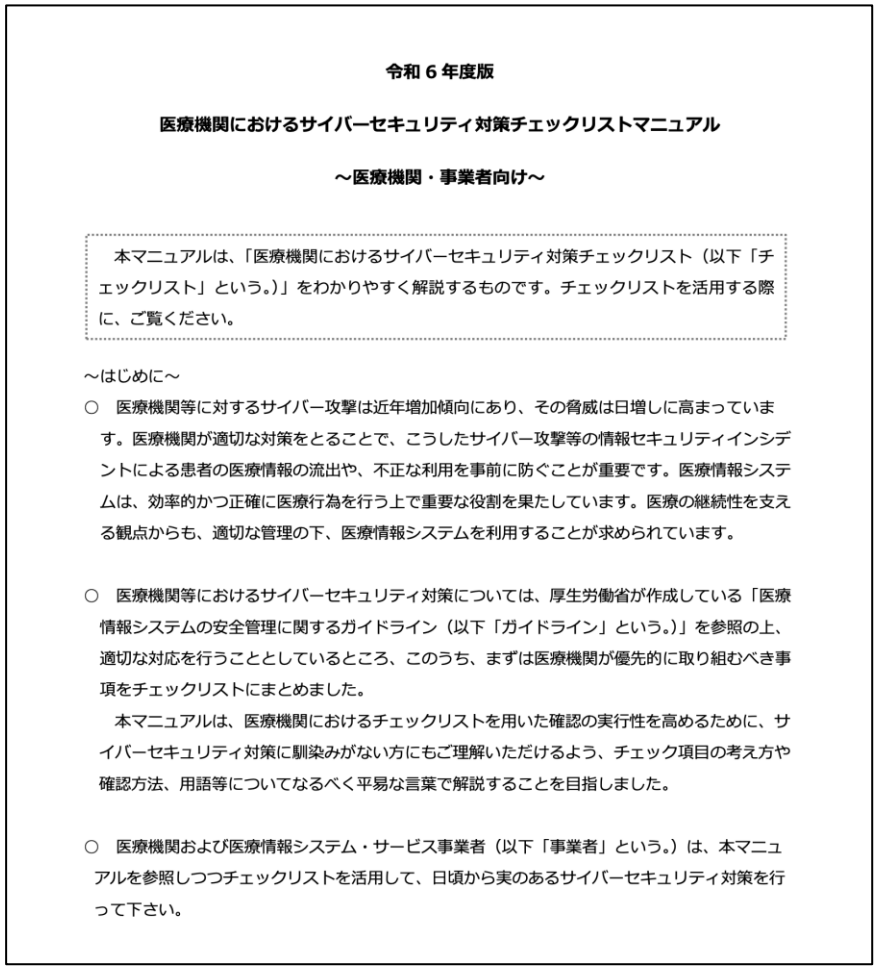
サイバーセキュリティの
実効性を高める

医療情報システムの安全管理に関するガイドライン
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
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

「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」

- 医療機関におけるチェックリストを用いた確認の実効性を高めるために、チェックリストマニュアルが作成、公開されています。
  医療機関及び医療情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、サイバーセキュリティ対策を行ってください。

- 令和６年度版でチェックリストおよびマニュアルが更新されていますので見落としが無いようご注意ください。



令和６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マニュアル

～医療機関・事業者向け～

本マニュアルは、「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（以下「チェックリスト」という。）」をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

○　医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○　医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。
　本マニュアルは、医療機関におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○　医療機関および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

用意 記入 確認 提出

チェックリストの準備対応、進め方

用意

- 医療機関は「医療機関確認用」を使用してください。事業者には「事業者確認用」への記入を求め、回収してください。
- 「事業者確認用」については、事業者との契約がない場合は不要です。

記入

- 「はい」または「いいえ」に〇をつけて確認した日を記入してください。
- 確認しきれなかった場合は「いいえ」とした上で、対策に係る令和６年度中の目標日を記入してください。
- チェック項目の対象となるものが無いことが明らかな場合は、「いいえ」とした上で、備考に対象外と明記してください。

確認

- 回収した事業者向けの全てのリストを確認し、記入内容に相違が無いか確認してください。
- 医療機関確認用における回答は各項目それぞれについて施設全体を総合してください。

提出

- 提出方法は所管保健所の指示に従い対応してください。

用意　記入　確認　提出

チェックリストの掲載先

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）
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

用意　記入　確認　提出

シートの用意

医療機関は「医療機関確認用」を、事業者には「事業者確認用」を使用してください。
それぞれPDF版とExcel版が公開されていますので、使用、管理しやすい方をお使いください。

令和6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

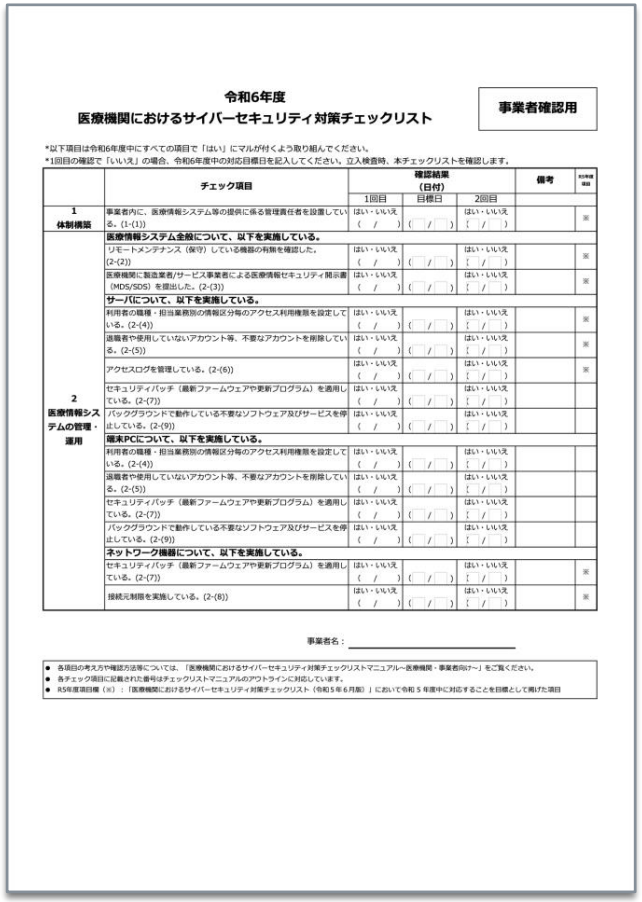
医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

*以下項目は令和6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。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	当該事項
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（　/　）	（　/　）	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（　/　）	（　/　）	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（　/　）	（　/　）	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（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（　/　）	（　/　）	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している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	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-(7)	はい・いいえ（　/　）	（　/　）	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-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（　/　）	（　/　）	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している。(2-(5))	はい・いいえ（　/　）	（　/　）	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-(7))	はい・いいえ（　/　）	（　/　）	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-(9))	はい・いいえ（　/　）	（　/　）	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。					
	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-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	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（　/　）	（　/　）	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（　/　）	（　/　）	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（　/　）	（　/　）	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。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和５年度中に対応することを目標として掲げた項目



令和6年度
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

事業者確認用

*以下項目は令和6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。
*1回目の確認で「いいえ」の場合、令和6年度中の対応目標日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	当該事項
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	はい・いいえ（　/　）	（　/　）	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。**					
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	医療機関に製造業者/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）を提出した。(2-(3))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	サーバについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（　/　）	（　/　）	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している。(2-(5))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（　/　）	（　/　）	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-(7))	はい・いいえ（　/　）	（　/　）	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-(9))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		
	端末PCについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（　/　）	（　/　）	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している。(2-(5))	はい・いいえ（　/　）	（　/　）	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-(7))	はい・いいえ（　/　）	（　/　）	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-(9))	はい・いいえ（　/　）	（　/　）	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。					
	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-(7))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）		※

事業者名：＿＿＿＿＿＿＿＿

- 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。
- R5年度項目欄（※）：「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（令和５年６月版）」において令和５年度中に対応することを目標として掲げた項目

システムを提供している事業者ごとに確認、協力を求めてください

「事業者確認用」については、事業者との契約がない場合は不要です。

事業者の皆様は医療機関からの協力要請に対してご協力をお願いします

Excelシートの場合は施設、事業者毎にファイルを作成してください。
PDFの場合は施設、事業者毎に印刷し、記入してください。

用意 > 記入 > 確認 > 提出

シートの記入

少なくとも年1回はチェックリストを用いた点検を行なってください。

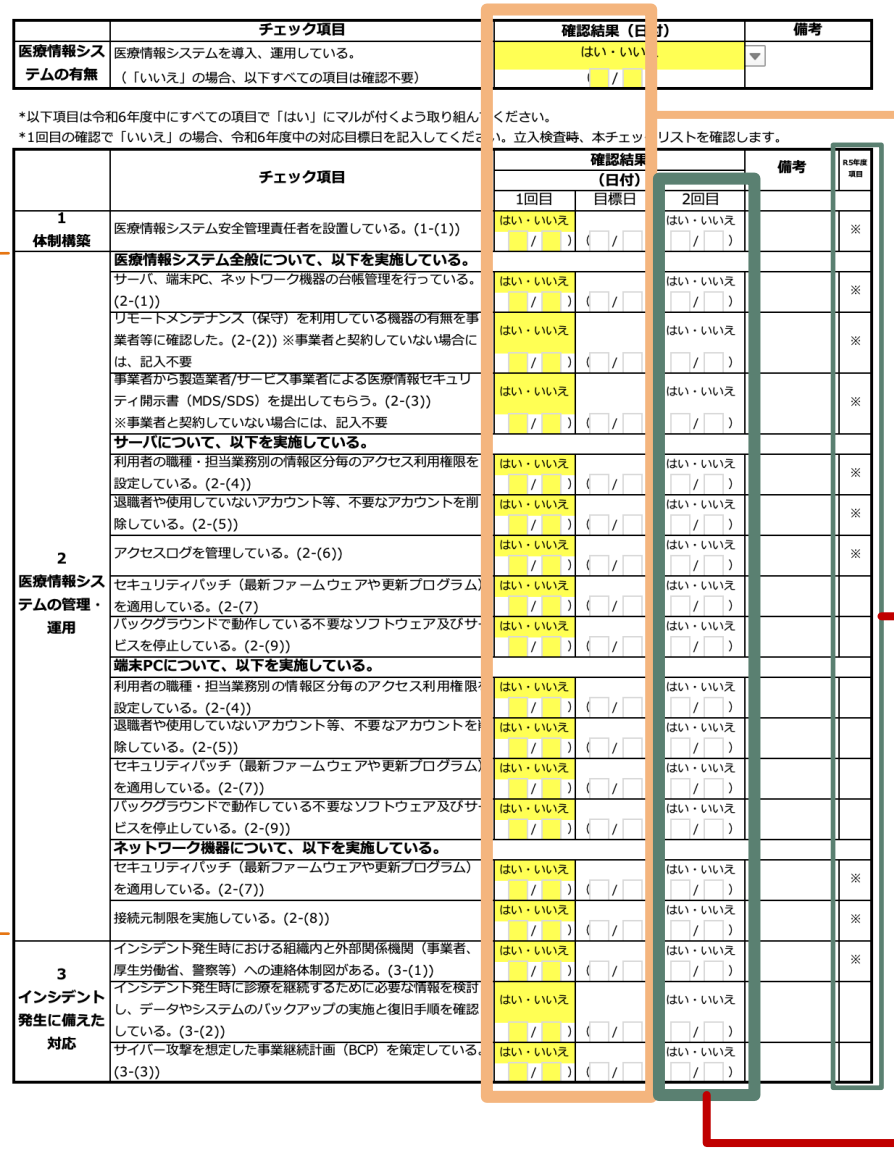
「はい・いいえ」を選択し、
確認日を記入してください。

「いいえ」の場合は、チェック項目内容を満たす「目標日」を記入してください。

全ての項目を「はい」にするよう努めましょう

各項目の対応状況を担当部門に確認し、
総合して評価してください。

多数の事業者からシステム提供を受けている場合は、医療機関として全体を総合して評価してください。



	チェック項目	確認結果（日付） 1回目	目標日	2回目	備考	R5年度項目
医療情報システムの有無	医療情報システムを導入、運用している。	はい・いいえ				
	（「いいえ」の場合、以下すべての項目は確認不要）	（ / ）				
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（ / ）	（ / ）	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（ / ）	（ / ）	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（ / ）	（ / ）	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（ / ）	（ / ）	はい・いいえ（ / ）		※
	サーバについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（ / ）	（ / ）	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している。(2-(5))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	アクセスログを管理している。(2-(6))	はい・いいえ（ / ）	（ / ）	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-(7))	はい・いいえ（ / ）	（ / ）	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-(9))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		
	端末PCについて、以下を実施している。					
	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。(2-(4))	はい・いいえ（ / ）	（ / ）	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している。(2-(5))	はい・いいえ（ / ）	（ / ）	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-(7))	はい・いいえ（ / ）	（ / ）	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-(9))	はい・いいえ（ / ）	（ / ）	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。					
	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-(7))	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）		※
	接続元制限を実施している。(2-(8))	はい・いいえ（ / ）	（ / ）	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（ / ）	（ / ）	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（ / ）	（ / ）	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（ / ）	（ / ）	はい・いいえ（ / ）		

※令和５年度から確認されている項目

目標日の後、2回目のチェックを各自実施してください。

はい・いいえを確認し、チェック日を記入してください。

確認

証跡は必要か？

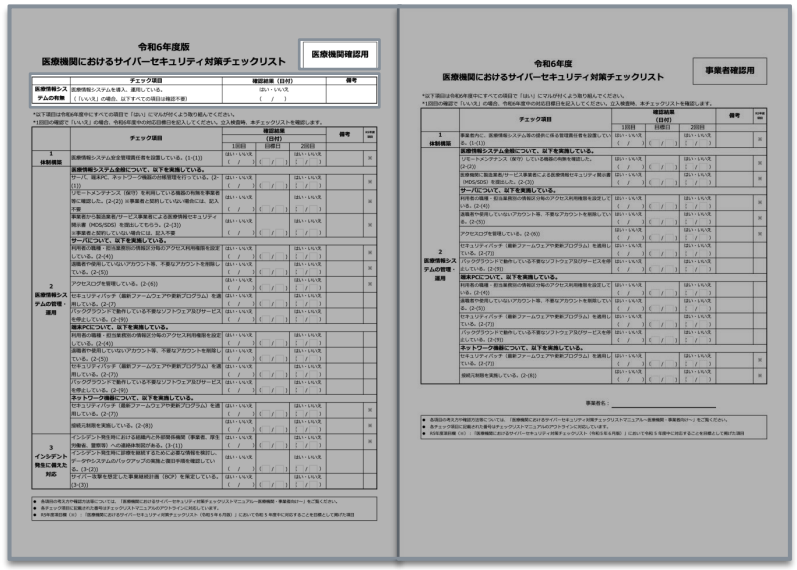
- 回答の根拠となる文書やデータを求められれば提示できるように準備しておきしましょう。

一部のシステムで実施できていない場合は？

- 「はい」は、医療情報システムの範囲(後述)において、網羅的に確認ができた状態を示します。
  そのため、一部のみの対応の場合は「いいえ」を選択し、対応するため期日を記載しましょう。
- 備考欄には「いいえ」となっている理由について記載してください。

事業者から提出されてこない場合は？

- 回答が得られない理由をメールや文書などで求めてください。


令和6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

チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　／　）

*以下項目は令和6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。
*1回目の確認で「いいえ」の場合、令和6年度中の対応日程日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付）1回目	確認結果（日付）1回目	確認結果（日付）2回目	確認結果（日付）2回目	備考	分析機関
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 （　／　）	（　／　）	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 （　／　）	（　／　）	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 （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	事業者から製品基準/サービス基準適合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 （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	サーバについて、以下を実施している。						
	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。(2-(4))	はい・いいえ （　／　）	（　／　）	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している。(2-(5))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ （　／　）	（　／　）	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-(7))	はい・いいえ （　／　）	（　／　）	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-(8))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		
	端末PCについて、以下を実施している。						
	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。(2-(4))	はい・いいえ （　／　）	（　／　）	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している。(2-(5))	はい・いいえ （　／　）	（　／　）	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-(7))	はい・いいえ （　／　）	（　／　）	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-(8))	はい・いいえ （　／　）	（　／　）	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。						
	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-(7))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ （　／　）	（　／　）	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 （　／　）	（　／　）	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 （　／　）	（　／　）	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 （　／　）	（　／　）	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ている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。
● 2/3年度目標（※）：「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（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目

令和6年度
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
事業者確認用

*以下項目は令和6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。
*1回目の確認で「いいえ」の場合、令和6年度中の対応日程日を記入してください。立入検査時、本チェックリストを確認します。

	チェック項目	確認結果（日付）1回目	確認結果（日付）1回目	確認結果（日付）2回目	確認結果（日付）2回目	備考	分析機関
1 体制構築	事業者内に、医療情報システム等の提供に係る管理責任者を設置している。(1-(1))	はい・いいえ （　／　）	（　／　）	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。**						
	リモートメンテナンス（保守）している機器の有無を確認した。(2-(2))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	医療機能と製品基準/サービス基準適合による医療情報セキュリティ開示書（MDS/SDS）を提出した。(2-(3))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	サーバについて、以下を実施している。						
	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。(2-(4))	はい・いいえ （　／　）	（　／　）	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している。(2-(5))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	アクセスログを管理している。(2-(6))	はい・いいえ （　／　）	（　／　）	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-(7))	はい・いいえ （　／　）	（　／　）	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-(8))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		
	端末PCについて、以下を実施している。						
	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。(2-(4))	はい・いいえ （　／　）	（　／　）	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している。(2-(5))	はい・いいえ （　／　）	（　／　）	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-(7))	はい・いいえ （　／　）	（　／　）	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-(8))	はい・いいえ （　／　）	（　／　）	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。						
	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-(7))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※
	接続元制限を実施している。(2-(8))	はい・いいえ （　／　）	（　／　）	はい・いいえ （　／　）	（　／　）		※

事業者名：＿＿＿＿＿＿＿＿

● 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ている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。
● 2/3年度目標（※）：「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（令和5年6月版）」において令和5年度中に対応することを目標として掲げた項目

医療情報システムの有無

医療情報システムの有無

医療情報システムを導入、運用している。

医療情報とは？

- 医療に関する患者情報（個人識別情報）を含む情報。

医療情報システムとは？

- 医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般
  サーバ、端末PC（≒エンドポイント,医療機器）、ネットワーク機器等を含む。

システムの例

- レセコン
- 電子カルテ
- オーダリングシステム

マニュアルにも例示

- 調剤システム、臨床検査システム等、各種部門システム
- PDI作成装置、インポート装置
- 各種撮影装置、検査装置（※）
- レポートシステム、遠隔画像診断システム

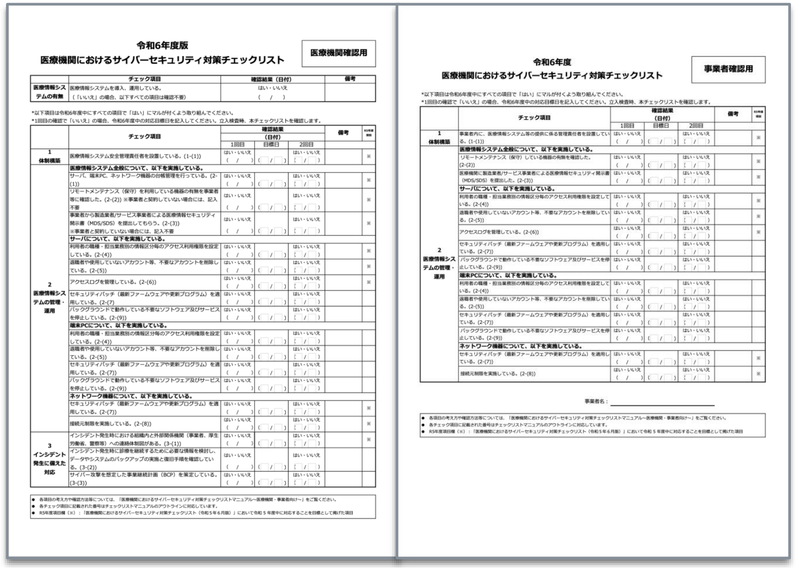
医療情報が発生するもの
医療情報を参照するもの

- オンライン資格確認端末
- 医事会計システム
- 予約システム
- 受付機・精算機
- 受付案内表示システム

患者の個人情報、
患者個人識別情報に紐づくもの

- これらシステムを構成する機器およびそこで動作するソフトウェアは全て安全管理の対象です
- インターネットへの接続の有無は関係ありません
- 製品化されたシステムではなく、内製したシステムや、汎用のソフトウェアなどを使用して医療情報を扱う業務を行っている場合も対象となります
  - PC
  - サーバ
  - ストレージ
  - テープ装置、外部ディスク装置
  - タブレット、携帯端末
  - モニター
  - ネットワーク機器（ファイアウォール、スイッチ、ルータ、VPNルータ　等）

※薬機法上の「管理医療機器」であっても、サーバや他の端末等と連携して動作する情報システムの側面を持つものは対象として考える必要があります


令和6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
令和6年度
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
事業者確認用

用語解説

1. 体制構築

- 医療情報システム安全管理責任者

医療行為は機器やシステムなしでは提供が難しい現実

システムの安全性確保のための継続的な活動

インシデント発生時の対応の中心

＜医療情報システム安全管理責任者の役割＞

教育・訓練を含む情報セキュリティ対策の推進

情報セキュリティ方針の策定

- 経営層の就任が望ましい
- 企画管理者（システム部門長等）による兼務の場合、経営層によるバックアップ、裁量が与えられているか

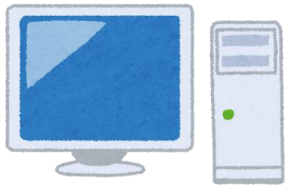
2. 医療情報システムの管理・運用

■ サーバ　端末PC　ネットワーク機器

WindowsやLinux（リナックス）、MacOSといったOS（基本ソフト）で稼働

端末PC

ノートパソコン



デスクトップパソコン

ミニPC

- 職員の手元で使用されるパソコン

・デスクトップパソコンとしての利用
・案内表示用モニタの表示用等に利用される場合もある

サーバ

タワー型サーバ

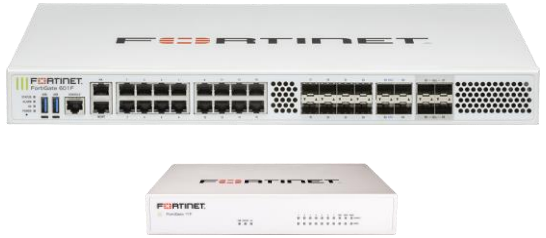
ラックマウント型サーバ

例）NEC社サーバ製品

- ファイルサーバなどネットワーク経由で共用するものを稼働させる

各社専用のファームウェア（OS,基本ソフト）で稼働

ネットワーク機器



例）Fortinet社ルーター製品

例）Yamaha社ルーター製品

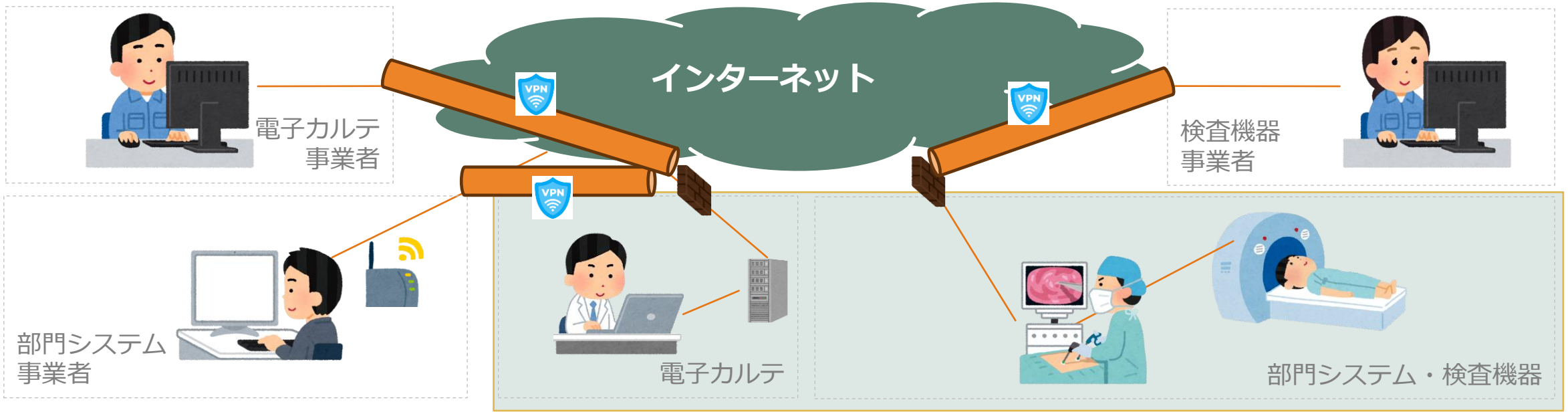
例）Cisco社ネットワークスイッチ製品

2. 医療情報システムの管理・運用

リモートメンテナンス（保守）

リモートメンテナンスとは？

- 機器やシステムの保守や運用を行うにあたって、遠隔で医療情報システムに接続し、作業を行う仕組み全般のことです。
- 専用線相当の回線サービスや、IPSec-VPNやSSL-VPNなどインターネット間を暗号通信で繋ぐVPN接続などさまざまな接続形態があり機密性を確保した通信手段により実施されるものですが、構成や運用に不備があるとセキュリティホールになる可能性があります。
- 近年では、LTEや5GなどのSIMを装着したモバイルルーターが設置されている場合があります。その場合、有線での導入と異なりインターネット回線は引き込み工事がないため気が付きにくくなりますので一層の注意が必要となります。



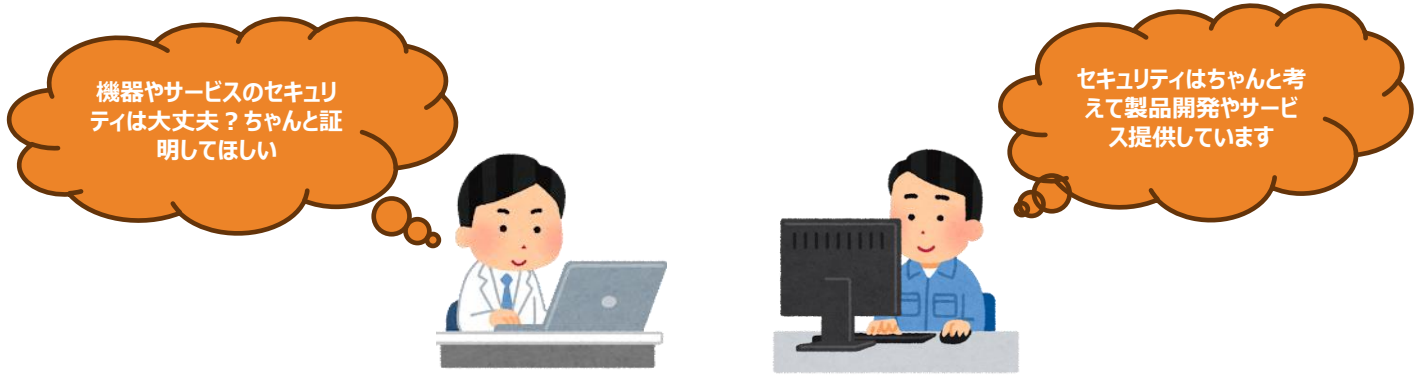
特定の人だけが通れる裏口を作るイメージです

2. 医療情報システムの管理・運用

■ 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）

MDS/SDSとは

- 製造業者による医療情報セキュリティ開示書（Manufacturer Disclosure Statement for medical information security, MDS）、サービス事業者による医療情報セキュリティ開示書（Service provider Disclosure Statement for medical information security, SDS）を意味し、各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する標準的な記載方法を業界団体（JAHIS/JIRA）が定めたものです。



製造やサービス提供している事業者が、適切にセキュリティを実装できているか、医療情報システムの安全管理に関するガイドラインに沿ったものになっているのかをまとめた文書です。
医療機関はリスクアセスメントやレビューを行いやすくなります。

サービス事業者による医療情報セキュリティ開示書（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版対応）

		回答欄	
作成日			
サービス事業者			
サービス名称			
バージョン			
※本書式を作成したJAHIS/JIRAは、製品設計・設置・保守等の認証・試験・検査等は行っていません。また、特定の医療機関等における特定の目的・ニーズを満たすこと、あるいは個々の製品またはサービスの性能を保証するものではありません。この書式への記入内容は、記入した製造業者/サービス事業者が全責任を負います。		プルダウン選択（はい/いいえ/対象外/該当/非該当）	備考番号の入力（数字）（なし="-"）
診療録及び診療諸記録等の医療情報の取扱いを受託する際の基準			
1 診療録及び診療諸記録等の外部保存を受託するか？	該当 非該当 備考		
1．1 保存場所が「病院、診療所、医療法人等が適切に管理する場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？	はい いいえ 対象外 備考		
1．2 保存場所が「医療機関等が外部の事業者との契約に基づいて確保した安全な場所」の場合、安全管理ガイドラインで示された選定基準と情報の取扱い要件を満たすか？	はい いいえ 対象外 備考		
医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践			
2 扱う情報のリストを医療機関等に提示できるか？	はい いいえ 対象外 備考		
組織的安全管理対策（体制、運用管理規程）			
3 医療情報システムを運用する際に、医療情報システムの企画管理者を設置しているか？	はい いいえ 対象外 備考		
4 医療情報システムを運用する際に、技術担当者を指定しているか？	はい いいえ 対象外 備考		
5 個人情報が参照可能な場所に対しては、入退管理のルールを定めているか？	はい いいえ 対象外 備考		
6 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか？	はい いいえ 対象外 備考		
7 医療機関等との契約に安全管理に関する条項を含めているか？	はい いいえ 対象外 備考		
8 個人情報を含む医療情報システムの業務を外部委託する場合、委託元である医療機関等との契約に再委託先を含めた安全管理に関する条項を含めているか？	はい いいえ 対象外 備考		
9 運用管理規程等において組織的安全管理対策に関する事項等を定めているか？	はい いいえ 対象外 備考		
物理的安全対策			
10 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠しているか？	はい いいえ 対象外 備考		
11 個人情報を入力・参照できる端末が設置されている区画は、許可されたもの以外立ち入ることができないように対策されているか？	はい いいえ 対象外 備考		
12 個人情報が保存されている機器が設置されている区画への入退管理を実施しているか？	はい いいえ 対象外 備考		
12．1 入退出の事実を記録しているか？	はい いいえ 対象外 備考		
12．2 入退者の記録を定期的にチェックし、妥当性を確認しているか？	はい いいえ 対象外 備考		
13 個人情報が保存されている機器等の重要な機器に盗難防止策を講じているか？	はい いいえ 対象外 備考		
14 個人情報が入力・参照できる端末に覗き見防止の機能があるか？	はい いいえ 対象外 備考		
15 サービス事業者の管理端末に覗き見防止対策が取られているか？	はい いいえ 対象外 備考		
技術的安全対策			
16 離席時に権限を持たない者による不正入力を防止する対策が行われているか？	はい いいえ 対象外 備考		
17 アクセス管理の機能があるか？	はい いいえ 対象外 備考		

JAHIS「製造業者による医療情報セキュリティ開示書」
https://www.jahis.jp/standard/detail/id=1119

2. 医療情報システムの管理・運用

アカウント

システムにおいて、ユーザー管理は構成ごとに異なることが多くなります。それぞれのアカウント情報の趣旨とあわせて、混同しないよう整理、管理する必要があります。

サーバのアプリケーション機能を利用する際の「アカウント」
→電子カルテ　メールサーバ　ECサイト　ネットバンク　など

PCへログインする「アカウント」
→ ユーザーID　利用者ID

端末PC/OS　アカウント

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバ/アプリケーション　アカウント登録状況

ID名	役割	アカウント種別	使用者
systemadmin	システム管理者	管理者	IT管理部門メンバー
d0200123	医師	医師	XX先生
n0220246	看護師	看護師	YYさん

サーバ/OS　アカウント登録状況

ID名	役割	Windows アカウント種別	使用者
Administrator	システム管理者	管理者	IT管理部門メンバー
user	一般利用者	標準ユーザー	一般職員

サーバのOS機能を利用する際の「アカウント」
→　実際は端末PCからネットワーク越しに使用することが大半なので
　　サーバ自体に個別の利用者IDは登録されていないことが多い
　　ファイル共有サーバ　プリントサーバ　など

2. 医療情報システムの管理・運用

アクセス利用権限

誰が、どの情報に、どんなことができるかを決めるルール

目的

誰がどの情報を操作したか、責任の所在を明確にする（真正性）

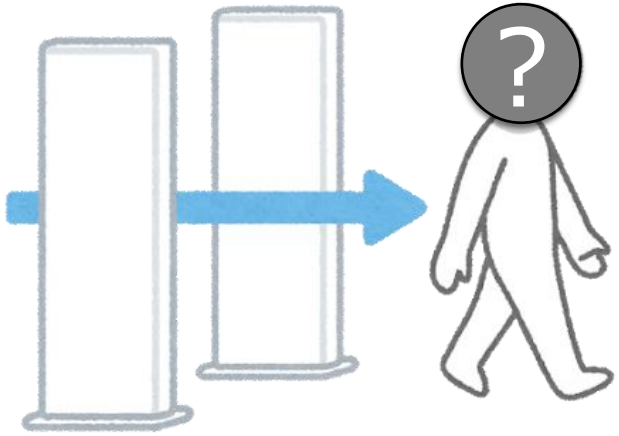
重要な情報に、関係のない人がアクセスしてしまうのを防ぐ（機密性）

不正な操作を防ぎ、システムやデータの安全性を確保する（完全性）

電子カルテをイメージした例	記事入力	病名	検査結果	処方オーダ
 システム管理者	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 医師	○ 入力可能	○ 入力可能	△ 閲覧のみ	○ 入力可能
 看護師	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	△ 閲覧のみ
 医事事務員	○ 入力可能	△ 閲覧のみ	△ 閲覧のみ	✕ 閲覧不可

2. 医療情報システムの管理・運用

- 退職者、使用していないアカウント、不要なアカウント



退職された方がそのままIDを保持していたら？

放置	• 入館ゲートを通過 • 不正侵入を誘発
削除	• 入館ゲートでブロック • 過去の記録との名寄せ確認ができない
無効化	•入館ゲートでブロック •過去の記録との名寄せ確認が可能になる •個人情報の保有期限に考慮が必要となる場合も

2. 医療情報システムの管理・運用

アクセスログ

業務システムでは処理が正しく行われていたことの裏付け、記録を「ログ」と呼びます。
アクセスログは、対象の「サーバ」または、機能である「アプリケーション」によって記録されることで
何かあったときにそこで起きた事象を確認する証拠となります。

When いつ	Where どこで	Who 誰が	What 何を	How どのように	Result 結果	Why なぜ
日時	発生箇所	利用者ID	対象データ	アクション	OK / NG	理由

入館の記録は何のため？

セキュリティ確保
- 不審者の侵入を防ぐ
- 来訪者の安全を守る

責任の所在の明確化
- 事故発生時、誰がいつ出入りしていたか明確にする

利用状況の把握
- 混雑状況を把握し、利便性を向上させる

●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
・	・	・	・	・

2. 医療情報システムの管理・運用

ソフトウェア　脆弱性

ハードウェア（機械）の不具合は部品の交換修理が必要だが、ソフトウェアはプログラムデータの更新によって修理が可能となる

ソフトウェアとは

脆弱性など不具合が見つかれば、それを修正する更新プログラム適用により修復する必要がある

インターネット経由での更新が行われるものが増えている

古いソフトウェアはサポート打ち切りで不具合発生しても修正できなくなる

脆弱性とは・・・？

- ソフトウェアで発覚したバグ、不具合
- 設計時点では想定されなかった箇所や、想定を超えるの方法によって問題となるもの

ピッキングに弱いという脆弱性が発覚

脆弱性を修正した部品へのアップデート（鍵・シリンダー交換）

2. 医療情報システムの管理・運用

セキュリティパッチ　ファームウェア　更新プログラム

総務省　国民のためのサイバーセキュリティサイトより
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/03

パッチ
セキュリティパッチ

- パッチとはソフトウェアの不具合を修正するための更新プログラムを指します
- セキュリティ上の問題を修正するものをセキュリティパッチよ呼びます

ファームウェア

- ネットワーク機器など組み込み型の装置、アプライアンスと呼ばれる機器のOS、ソフトウェアをイメージすることが多いです

更新プログラム

- バージョンアップなども含め、更新、アップデート用のプログラムなど広い解釈があります

2. 医療情報システムの管理・運用

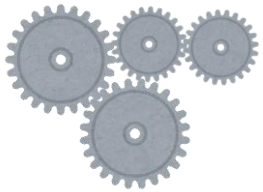
バックグラウンド

優先度の高い処理（プロセス、ジョブ）
画面上のアプリなど

フォアグラウンド

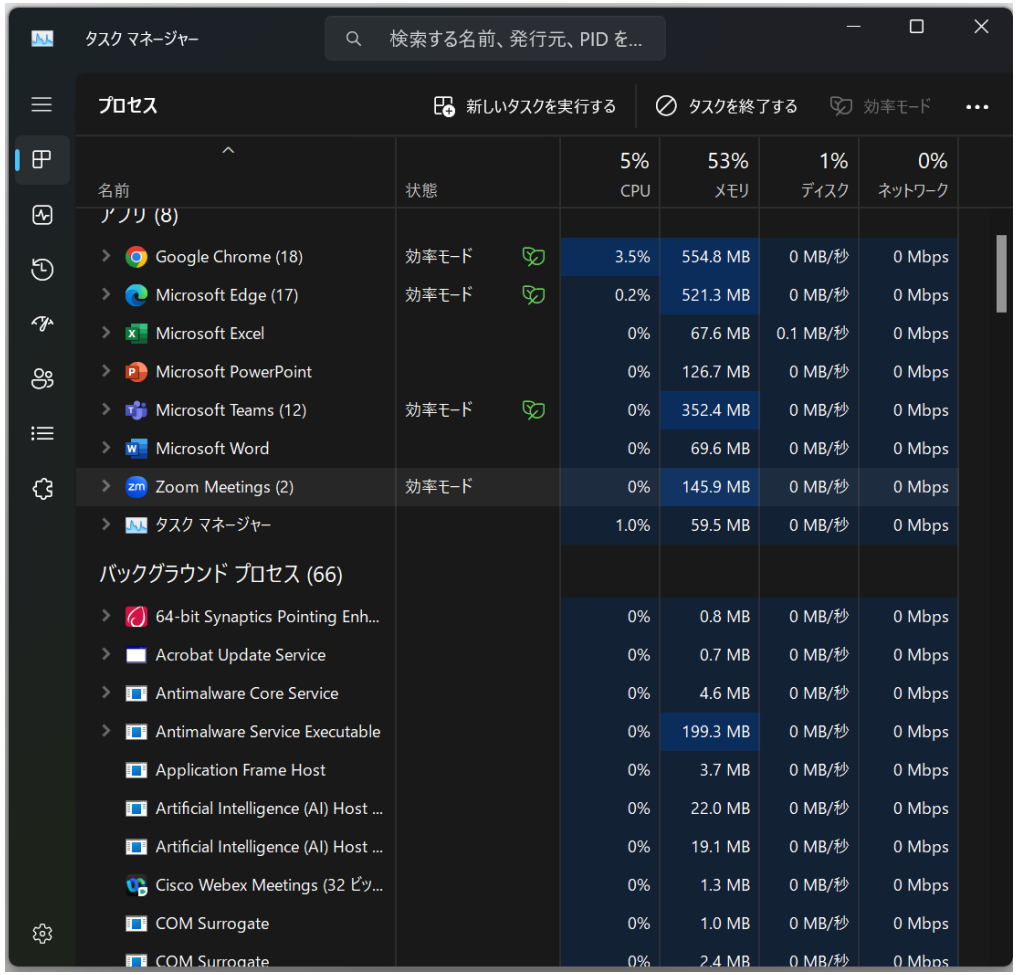
バックグラウンド

ウイルス対策などの保護機能



見えないところで動いているプロセス、ジョブ

使用されないプロセス、ジョブが蓄積しているとシステム全体の動作に影響することがあるため、無駄なものは停止する、立ち上げない

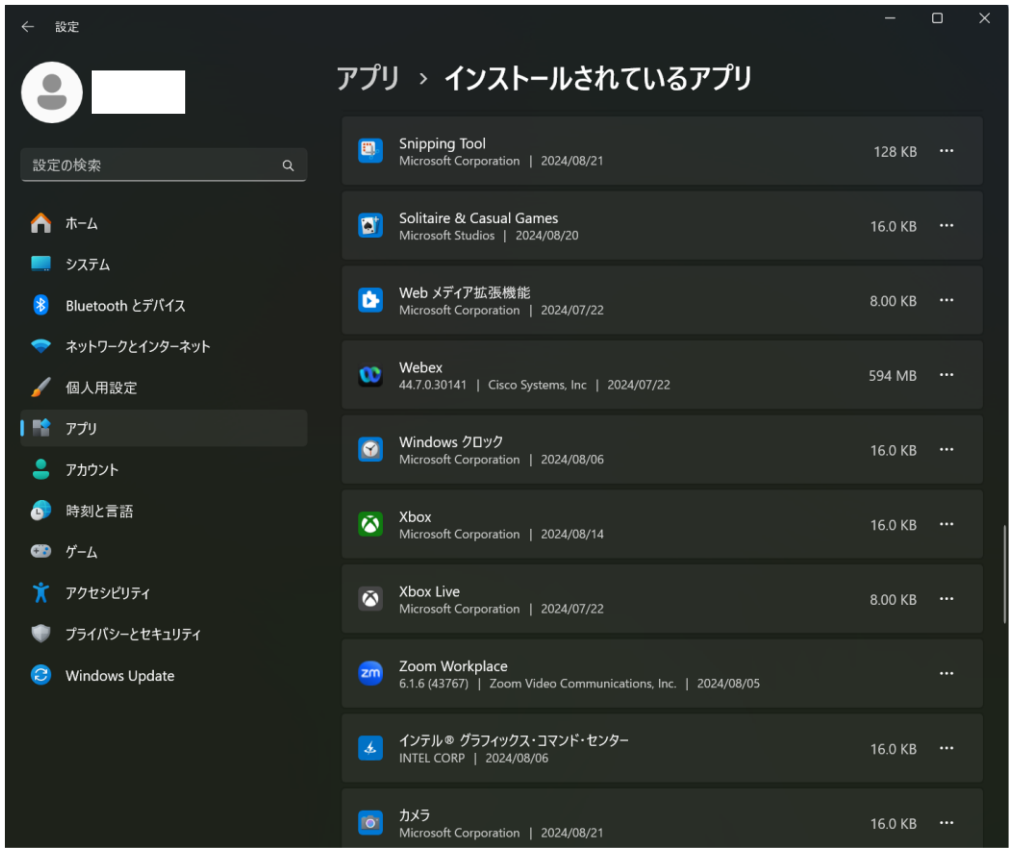


2. 医療情報システムの管理・運用

■ 不要なソフトウェア及びサービス

業務上必要なもの

ウイルス対策などの保護機能



業務上不要なもの

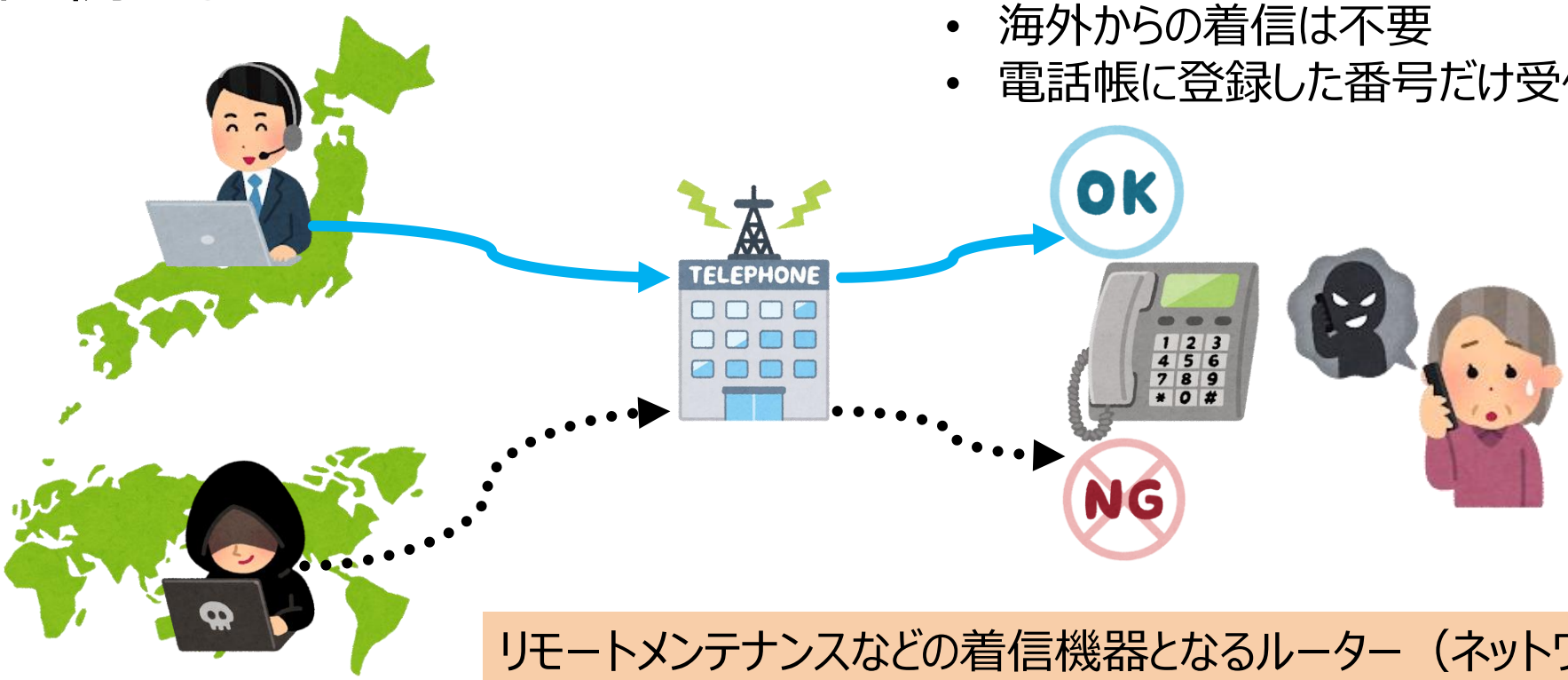
- 組織として確認していない、認めていないアプリはインストールすべきではない
- 不必要なアプリ、サービスが起動されていることによってシステムのパフォーマンスを浪費することになる
- セキュリティ上の問題があった場合に無駄な対応労力を要することになる

2. 医療情報システムの管理・運用

■ 接続元制限

電話に例えると・・・

- 海外からの着信は不要
- 電話帳に登録した番号だけ受信



リモートメンテナンスなどの着信機器となるルーター（ネットワーク機器）においても同様の考えで、グローバルIPアドレスによる地域や、番号を制限する方法があります。

3.インシデント発生に備えた対応

インシデント

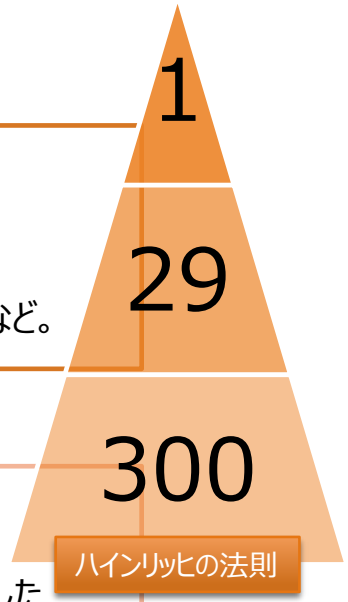
医療の場合

アクシデント

- 実際に**患者に被害**が及んだ医療事故
- 誤った薬剤を投与して**患者の容体が悪化**した場合など。

インシデント

- 患者に実害が発生しなかったが、ミスやエラーが発生した事象。
- 誤った薬剤を投与しようとしたが、投与前に気づいて修正した場合など。
- いわゆる「**ヒヤリハット**」。



サイバーセキュリティの場合

アクシデント

- アクシデントという表現はあまり使われない。

インシデント

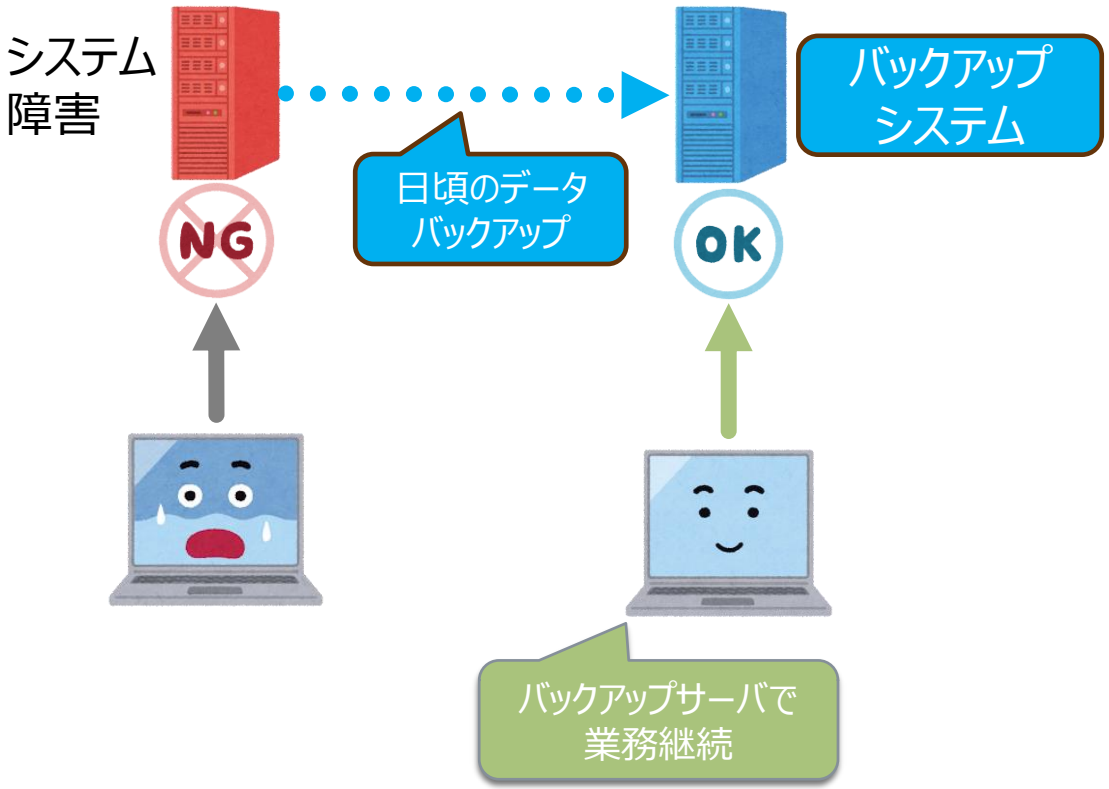
- 情報セキュリティ上の脅威となる事象。
- サイバーセキュリティインシデントは、企業や組織の情報資産が管理者の意図しない状態に置かれることを意味する。
- **マルウェア感染**、**不正アクセス**、**情報漏洩**など。

3.インシデント発生に備えた対応

バックアップ

バックアップの主な目的、理由

システム業務を「継続」するための方策



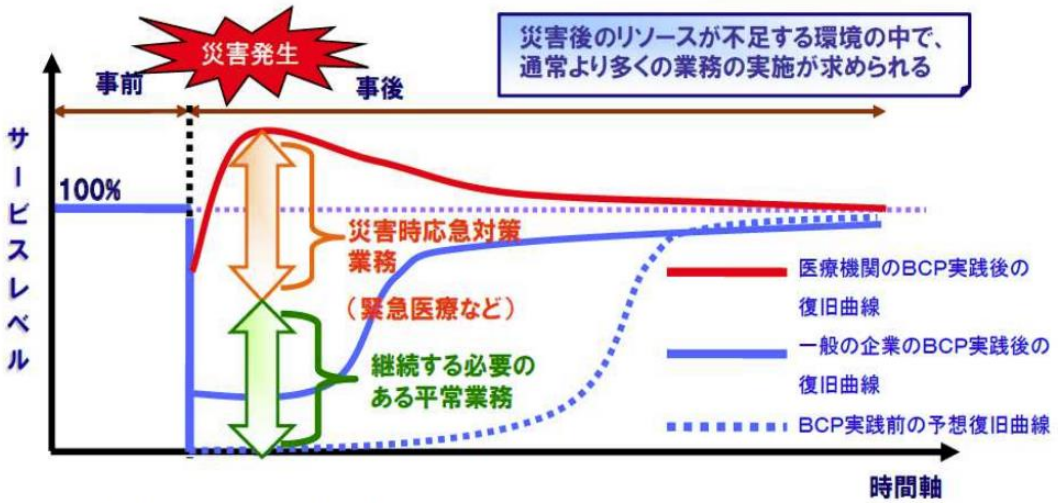
システム障害から「復元」するための方策

3.インシデント発生に備えた対応

事業継続計画（BCP）

- 事業継続計画（Business Continuity Planning）とは？
  - 大規模災害等の発生時にも医療を継続的に提供できるようにするための計画です。

医療機関に期待されるレベルのBCP



（出典）「高知県医療機関災害対策指針」（平成25年3月発行）p.51参照

医療施設の災害対応のための事業継続計画（BCP）

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/kenkou/kekkaku-kansenshou/infulenza/kenkyu_00001.html

- 災害拠点病院用のBCP策定について
  - 病院BCPを策定するための手引き
  - 病院BCP：（災害拠点病院用）改訂第２版
- 災害拠点病院以外の医療機関のBCP策定について
  - 医療機関（災害拠点病院以外）における災害対応のためのBCP作成の手引き
  - 医療機関（災害拠点病院以外）における災害対応のためのBCP作成指針
  - 災害拠点病院以外の医療機関におけるBCPチェックリスト

サイバー攻撃等によるシステム障害は、災害時における医療機関の復旧曲線とは異なり、一般企業の復旧曲線と同様となりますので
災害による事業継続計画とは別に、サイバー攻撃を想定した事業継続計画の策定が必要となっています。

参考情報

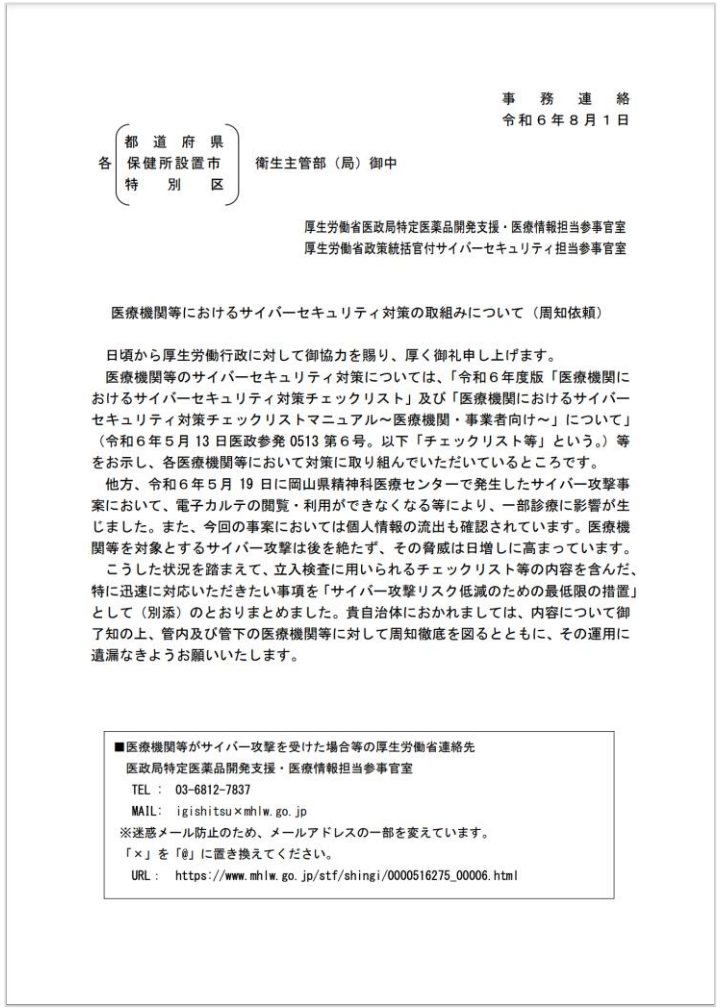
医療機器におけるサイバーセキュリティについて（厚生労働省 医薬局）

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

「医療情報システムの安全管理に関するガイドライン」だけでなく、医療機器に関するセキュリティの管理についても手引書等が発出されていますのでご参考ください

医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）（令和６年８月１日）

https://www.mhlw.go.jp/content/10808000/001283914.pdf



事　務　連　絡
令和６年８月１日

各 都道府県 保健所設置市 特別区 衛生主管部（局）御中

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
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。
医療機関等のサイバーセキュリティ対策については、「令和６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」及び「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～」について」（令和６年５月 13 日医政参発 0513 第６号。以下「チェックリスト等」という。）等をお示し、各医療機関等において対策に取り組んでいただいているところです。
他方、令和６年５月 19 日に岡山県精神科医療センターで発生したサイバー攻撃事案において、電子カルテの閲覧・利用ができなくなる等により、一部診療に影響が生じました。また、今回の事案においては個人情報の流出も確認されています。医療機関等を対象とするサイバー攻撃は後を絶たず、その脅威は日増しに高まっています。
こうした状況を踏まえて、立入検査に用いられるチェックリスト等の内容を含んだ、特に迅速に対応いただきたい事項を「サイバー攻撃リスク低減のための最低限の措置」として（別添）のとおりまとめました。貴自治体におかれましては、内容について御了知の上、管内及び管下の医療機関等に対して周知徹底を図るとともに、その運用に遺漏なきようお願いいたします。

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先
医政局特定医薬品開発支援・医療情報担当参事官室
TEL： 03-6812-7837
MAIL： igishitsu×mhlw.go.jp
※迷惑メール防止のため、メールアドレスの一部を変えています。
「×」を「@」に置き換えてください。
URL： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

サイバー攻撃リスク低減のための最低限の措置

- パスワードを強固なものに変更し、使い回しをしない
- IoT 機器を含む情報資産の通信制御を確認する
- ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する

詳細は別添文書をご確認ください

立入検査研修
準備コース　終了

別途、医療機関向け前編、後編、

または、保健所向けについても

お申し込みの上、ご受講ください