薬局に求められるサイバーセキュリティ対策

日本薬剤師会公式キャラクター
ふぁるみん

2026年3月22日

公益社団法人　日本薬剤師会
常務理事　田中千尋

薬局に求められる
サイバーセキュリティ対策

- 医療DXとサイバーセキュリティ
- 守るべき情報とは
- 医療情報システムの安全管理に関するガイドライン6版とサイバーセキュリティ対策
- サイバーセキュリティ対策まとめ

令和６年度診療報酬改定　Ⅱ－１　医療DXの推進による医療情報の有効活用、遠隔医療の推進－②

医療DXの推進による医療情報の有効活用の推進②

- オンライン資格確認により取得した診療情報・薬剤情報を調剤に実際に活用可能な体制を整備し、また、電子処方箋及び電子カルテ情報共有サービスを導入し、質の高い医療を提供するため医療DXに対応する体制を確保している場合の評価を新設する。

（新）　医療DX推進体制整備加算（調剤基本料）　４点（月に１回）

［算定要件］

医療DX推進に係る体制として別に厚生労働大臣が定める施設基準に適合しているものとして地方厚生局長等に届け出た保険薬局において調剤を行った場合は、医療DX推進体制整備加算として、月１回に限り４点を所定点数に加算する。

［主な施設基準］

(1)　療養の給付及び公費負担医療に関する費用の請求に関する命令（昭和51年厚生省令第36号）第１条に規定する電子情報処理組織の使用による請求を行っていること。
(2)　健康保険法第３条第13項に規定する電子資格確認を行う体制を有していること。
(3)　保険薬剤師が、オンライン資格確認を通じて取得した薬剤情報、特定健診情報等を閲覧又は活用し、調剤、服薬指導等を行う体制を有していること。
(4)　**電子処方箋を受け付ける体制**を有していること。
（紙の処方箋を受け付け、調剤した場合を含めて、調剤結果を電子処方箋管理サービスに登録する。）
(5)　**電磁的記録による調剤録及び薬剤服用歴の管理の体制**を有していること。
（オンライン資格確認、薬剤服用歴等の管理、レセプト請求業務等を担う当該薬局内の医療情報システム間で情報の連携が取られていることが望ましい。）
(6)　**電子カルテ情報共有サービスにより取得される診療情報等を活用する体制**を有していること。
(7)　**マイナンバーカードの健康保険証利用の使用について、実績を一定程度有している**こと。
(8)　医療DX推進の体制に関する事項及び質の高い調剤を実施するための十分な情報を取得し、及び活用して調剤を行うことについて、当該保険薬局の見やすい場所及びウェブサイト等に掲示していること。

［経過措置］

(1)　令和７年３月31日までの間に限り、（４）に該当するものと見なす。
(2)　令和７年９月30日までの間に限り、（６）に該当するものと見なす。
(3)　（７）については、令和６年10月１日から適用する。

29

医療DXと サイバーセキュリティ

医療DX推進体制整備加算

令和８年度診療報酬改定　Ⅲ－３　医療DXやICT連携を活用する医療機関・薬局の体制の評価－⓪

医療ＤＸ推進体制整備加算等の見直し

➢ 医療ＤＸ関連施策を踏まえ、医療情報取得加算及び医療ＤＸ推進体制整備加算の評価を見直す。

現行

［医療情報取得加算］
注６　調剤に係る十分な情報を取得する体制として別に厚生労働大臣が定める施設基準を満たす保険薬局において調剤を行った場合は、医療情報取得加算として、１年に１回に限り１点を所定点数に加算する。

［医療ＤＸ推進体制整備加算］
注13　医療ＤＸ推進に係る体制として別に厚生労働大臣が定める施設基準に適合しているものとして地方厚生局長等に届け出た保険薬局において調剤を行った場合は、医療ＤＸ推進体制整備加算として、月１回に限り、当該基準に係る区分に従い、次に掲げる点数をそれぞれ所定点数に加算する。
イ　医療ＤＸ推進体制整備加算１　10点
ロ　医療ＤＸ推進体制整備加算２　８点
ハ　医療ＤＸ推進体制整備加算３　６点

改定後

【医療情報取得加算】
注６　削除

［電子的調剤情報連携体制整備加算］
注13　医療ＤＸ推進に係る体制として別に厚生労働大臣が定める施設基準に適合しているものとして地方厚生局長等に届け出た保険薬局（注２に規定する別に厚生労働大臣が定める保険薬局を除く。）において調剤を行った場合は、**電子的調剤情報連携体制整備加算**として、**月１回に限り、８点**を所定点数に加算する。

［施設基準(通知)］
（７）電子的調剤情報連携体制整備加算を算定する月の３月前の件数ベースマイナ保険証利用率が、**30%以上**である。

様式 87 の３の６

医療ＤＸ推進体制整備加算の施設基準に係る届出書添付書類

医療ＤＸ推進体制整備加算の施設基準
（□には、適合する場合「✓」を記入すること）

1　療養の給付及び公費負担医療に関する費用の請求に関する命令（昭和51年厚生省令第36号）第１条に規定する電子情報処理組織の使用による請求を行っている。	□
2　健康保険法第３条第13項に規定する電子資格確認を行う体制がある。	□
3　オンライン資格確認等システムを通じて患者の診療情報、薬剤情報等を取得し、調剤、服薬指導等を行う際に当該情報を閲覧し、活用できる体制がある。	□
4　「電子処方箋管理サービスの運用について」に基づく電子処方箋により調剤する体制及び調剤結果を登録する体制を有している。	□
5　電磁的記録による調剤録及び薬剤服用歴の管理体制を有している。	□
6　国等が提供する電子カルテ情報共有サービスにより取得される診療情報等を活用する体制を有している。	□
7　次に掲げる全ての事項について、保険薬局の見やすい場所に掲示し、ウェブサイトに掲載している。 ・オンライン資格確認システムを通じて患者の診療情報、薬剤情報等を取得し、調剤、服薬指導等を行う際に当該情報を閲覧し、活用していること。 ・マイナンバーカードの健康保険証利用を促進する等、医療ＤＸを通じて質の高い医療を提供できるよう取り組んでいること。 ・電子処方箋や電子カルテ情報共有サービスを活用するなど、医療ＤＸに係る取組を実施していること。	□
8　サイバーセキュリティの確保のために必要な措置 ・医療情報システムの安全管理に関するガイドラインや薬局におけるサイバーセキュリティ対策チェックリストを活用するなどして、サイバー攻撃に対する対策を含めセキュリティ全般について適切な対応を行う体制を有していること。	□

［記載上の注意］
１　「６」については、令和８年５月31日までの間に限り該当するものとみなし、それまでの間に届出を行う場合は記載不要。
２　「７」については、自ら管理するホームページ等を有しない場合については、この限りではない。
３　「７」の「電子カルテ情報共有サービス」については、令和８年５月31日までの間に限り、掲示を行っているものとみなす。

サイバーセキュリティ対策チェックリスト

調剤報酬点数表関係

【連携強化加算、医療ＤＸ推進体制整備加算】

問１　連携強化加算及び医療ＤＸ推進体制整備加算の施設基準として、「サイバー攻撃に対する対策を含めセキュリティ全般について適切な対応を行うこと」とされており、「薬局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「薬局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～薬局・事業者向け～」を活用することとされているが、これらの資料が更新された場合には、いつまでに、その内容を踏まえて当該体制を見直すことが必要か。

（答）医療情報システムを取り巻く環境は刻一刻と変動していくものであり、セキュリティに関する内容も、最新のガイドライン、チェックリスト等を活用し、適切な対応を行う必要があることから、関係するガイドライン等が更新された場合には、速やかに対応する必要がある。

なお、現時点においては、「令和６年度版「薬局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「薬局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～薬局・事業者向け～」について」（令和６年５月 13 日付け医政参発 0513 第９号・医薬総発 0513 第２号医政局特定医薬品開発支援・医療情報担当参事官・医薬局総務課長通知）の別添１及び別添２が最新の資料となるが、厚生労働省のホームページに医療情報システムの安全管理に関するガイドラインに関する最新の情報が掲載されているので、適宜参照されたい。

最新は令和7年版

令和７年度版
薬局におけるサイバーセキュリティ対策チェックリスト

薬局確認用

*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 (/)	(/)	
	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	はい・いいえ		

後半で解説します

サイバーセキュリティの確保が必要な理由

医療法施行規則の改正
（2023/4/1施行）

第十四条 病院又は診療所の管理者はその病院又は診療所に存する医薬品、医療機器及び再生医療等製品につき医薬品医療機器等法の規定に違反しないよう必要な注意をしなければならない。
２ 病院、診療所又は助産所の管理者は、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（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ**なければならない。

薬機法施行規則の改正
（2023/4/1施行）

薬局の管理者の業務及び遵守事項）
第十一条（略）
２　法第八条第三項の薬局の管理者が遵守すべき事項は、次のとおりとする。
一　保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係る**サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ**、その他その薬局の業務につき、必要な注意をすること。
二　（略）

医療DXの基本的な考え方

医療DXの推進に関する工程表（概要）

資料2－1

第２回医療ＤＸ推進本部
（令和５年６月２日）資料２

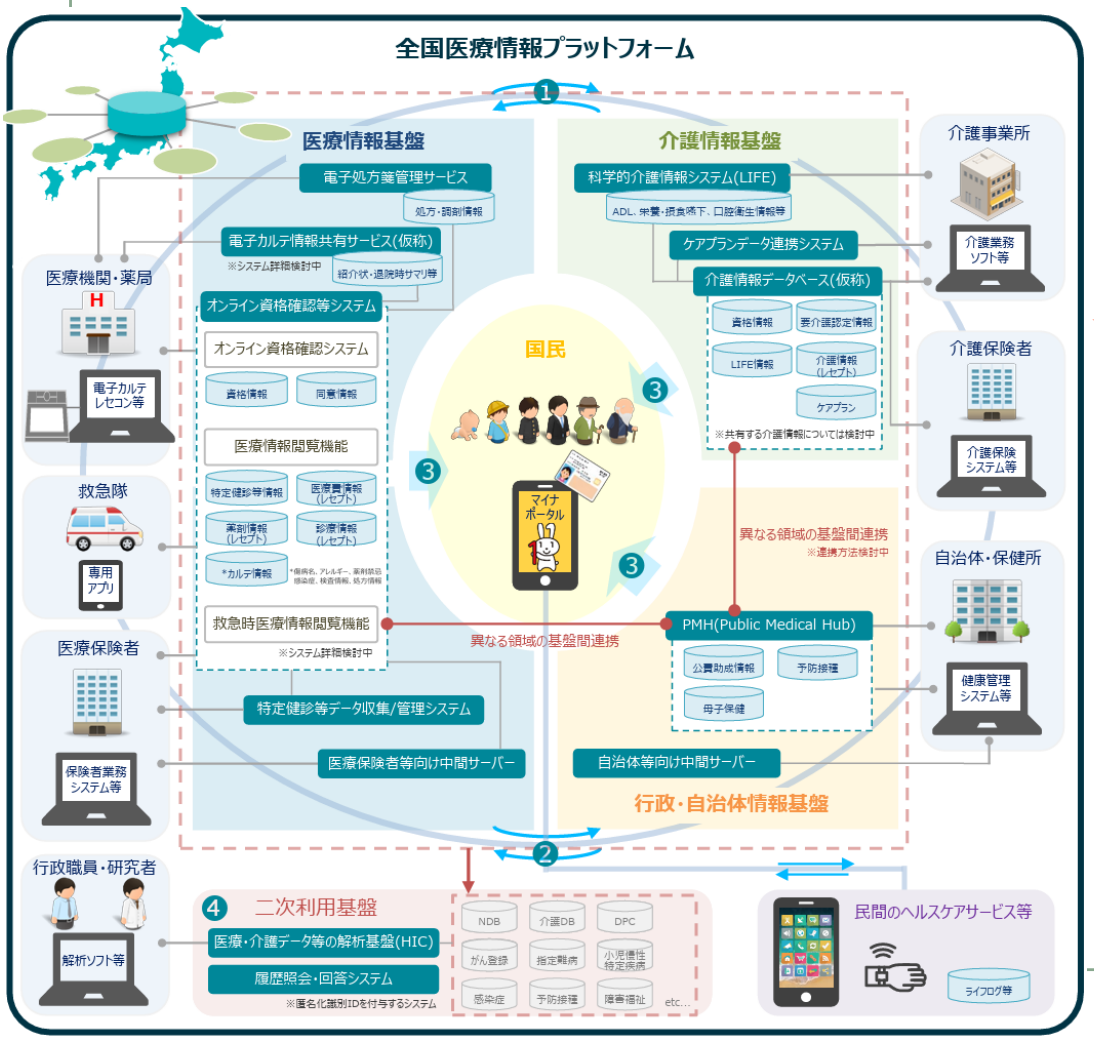
基本的な考え方

○　医療DXに関する施策の業務を担う主体を定め、その施策を推進することにより、①国民のさらなる健康増進、②切れ目なく質の高い医療等の効率的な提供、③医療機関等の業務効率化、④システム人材等の有効活用、⑤医療情報の二次利用の環境整備の5点の実現を目指していく

○　サイバーセキュリティを確保しつつ、医療DXを実現し、保健・医療・介護の情報を有効に活用していくことにより、より良質な医療やケアを受けることを可能にし、国民一人一人が安心して、健康で豊かな生活を送れるようになる

サイバーセキュリティ対策は医療DXの盾

医療DX＝さまざまなネットワークへの接続が前提の時代



インターネットを含むさまざまなネットワークへの接続＝セキュリティリスク

セキュリティ脅威は内部起因から外部起因へ

内部起因の例

外部記憶媒体（USB等）の紛失

メール誤送信

PC・スマホ等の紛失

医療従事者・内部関係者による施設内ルールに基づく対応（セーフティ）が徹底されないことに起因する事故(オペレーションミスやヒューマンエラー等による被害)

外部起因の例＝サイバー攻撃

フィッシングメールやサポート詐欺等による情報漏洩

ウェブサーバやメールサーバの乗っ取り

ランサムウェアによるシステム利用不可・脅迫

院内ルールの想定範囲を超えた、**セキュリティの不備**を悪用した、外部の攻撃者により引き起こされる事故
（ミス・エラー対策の死角を突く被害）

ランサムウェアによる被害

Asahi GROUP アサヒグループホールディングス 企業情報 ブランド サステナビリティ ニュースルーム IR・投資家情報 研究開発 採用情報 OUR STORIES EN

アサヒグループHD

お知らせ

2025.10.14

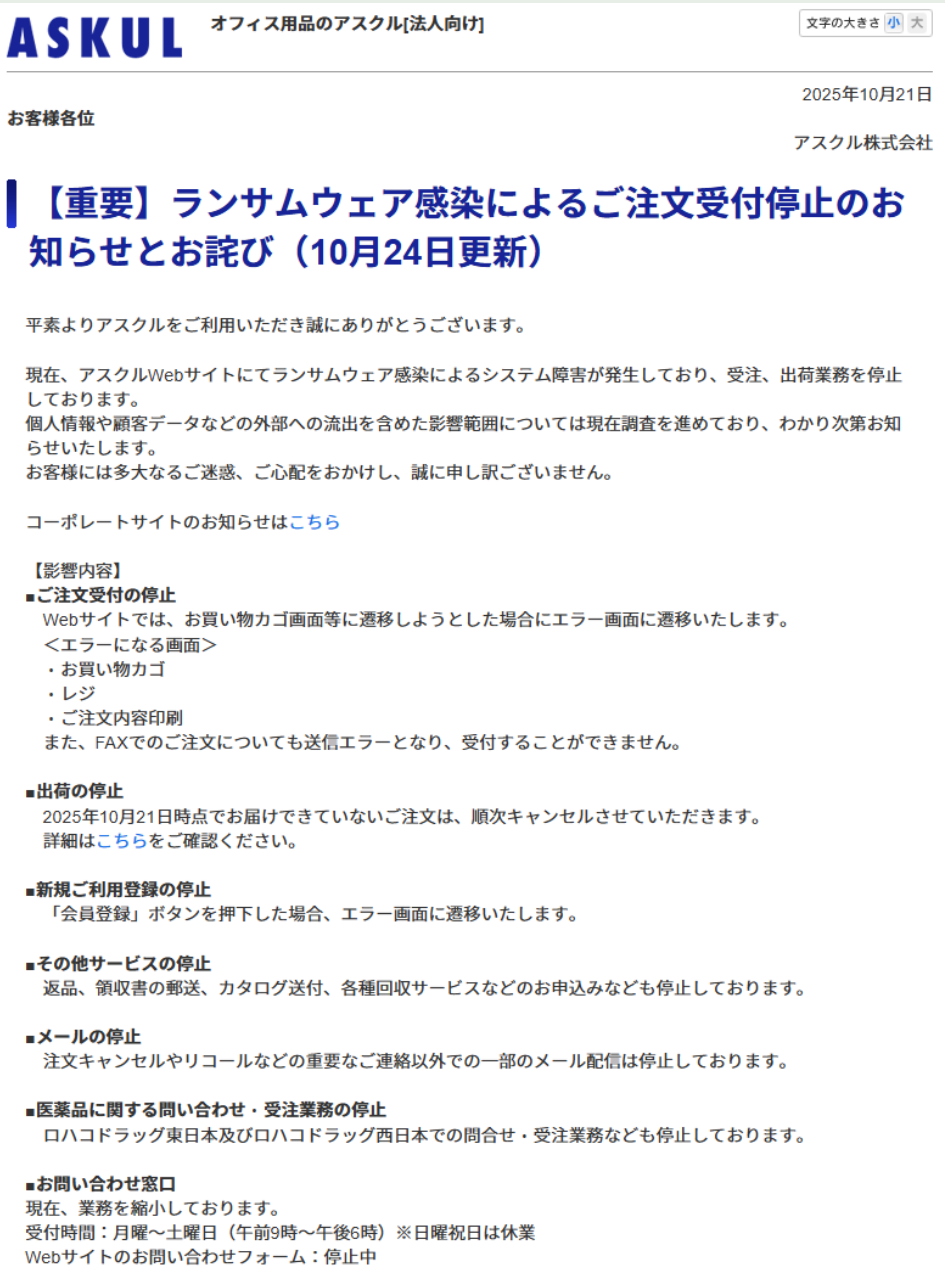
アサヒグループホールディングス株式会社

アサヒグループホールディングス株式会社（本社 東京、社長 勝木敦志）は9月29日付・10月3日付・10月8日付で、ランサムウエアの攻撃によるシステム障害発生について公表しています。

今回攻撃を受けたシステムを中心に影響する範囲や内容の調査を進めている中で、個人情報が流出した可能性のあることが分かりました。調査結果に基づいて、情報漏えいが確認された場合には、速やかに該当する方にお知らせするとともに、個人情報保護に関わる法令にのっとり適切な措置を講じます。

緊急事態対策本部と外部の専門家が協力し、一刻も早い事態の収束に向けた対応を行っています。今回の攻撃の影響は、日本で管理しているシステムに限られます。

お客さまおよび関係先の皆さまにご迷惑をおかけしますことをおわび申し上げます。



ASKUL オフィス用品のアスクル[法人向け] 文字の大きさ 小 大

2025年10月21日

お客様各位

アスクル株式会社

【重要】ランサムウェア感染によるご注文受付停止のお知らせとお詫び（10月24日更新）

平素よりアスクルをご利用いただき誠にありがとうございます。

現在、アスクルWebサイトにてランサムウェア感染によるシステム障害が発生しており、受注、出荷業務を停止しております。
個人情報や顧客データなどの外部への流出を含めた影響範囲については現在調査を進めており、わかり次第お知らせいたします。
お客様には多大なるご迷惑、ご心配をおかけし、誠に申し訳ございません。

コーポレートサイトのお知らせはこちら

【影響内容】

■ご注文受付の停止
Webサイトでは、お買い物カゴ画面等に遷移しようとした場合にエラー画面に遷移いたします。
＜エラーになる画面＞
・お買い物カゴ
・レジ
・ご注文内容印刷
また、FAXでのご注文についても送信エラーとなり、受付することができません。

■出荷の停止
2025年10月21日時点でお届けできていないご注文は、順次キャンセルさせていただきます。
詳細はこちらをご確認ください。

■新規ご利用登録の停止
「会員登録」ボタンを押下した場合、エラー画面に遷移いたします。

■その他サービスの停止
返品、領収書の郵送、カタログ送付、各種回収サービスなどのお申込みなども停止しております。

■メールの停止
注文キャンセルやリコールなどの重要なご連絡以外での一部のメール配信は停止しております。

■医薬品に関する問い合わせ・受注業務の停止
ロハコドラッグ東日本及びロハコドラッグ西日本での問合せ・受注業務なども停止しております。

■お問い合わせ窓口
現在、業務を縮小しております。
受付時間：月曜～土曜日（午前9時～午後6時）※日曜祝日は休業
Webサイトのお問い合わせフォーム：停止中

ランサムウェア攻撃＝情報セキュリティの脅威No.1

◢ 情報セキュリティ10大脅威 2025 [組織]

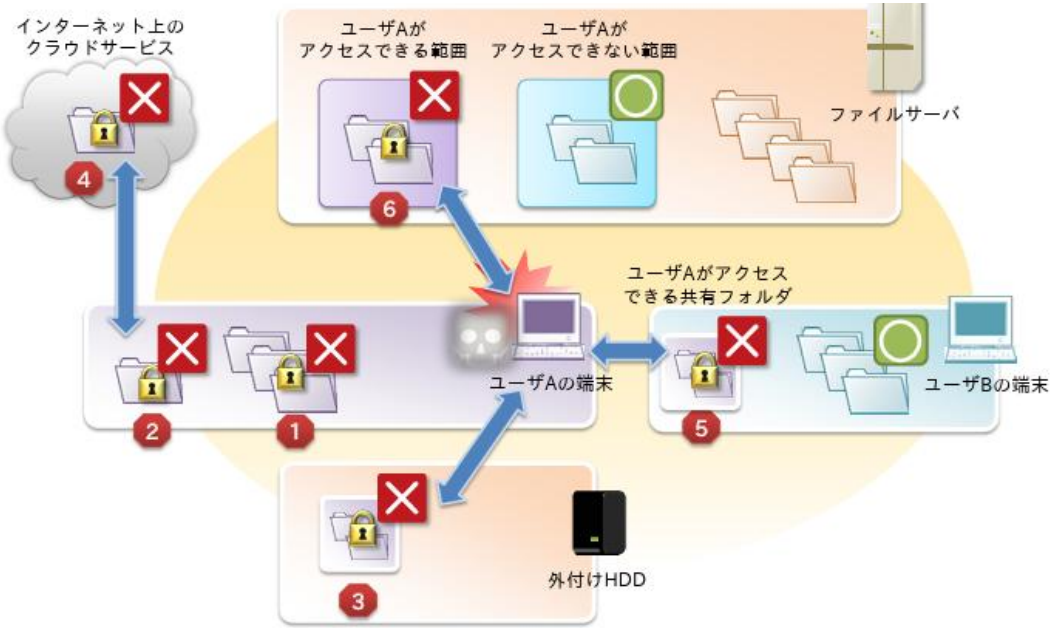
順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

ランサムウェアとは

ランサムウェアとは、パソコン等の端末およびネットワーク接続された共有フォルダ等に保管されたファイルを、利用者の意図に沿わず暗号化して使用不可にする、または画面ロック等により操作不可とするウイルスの総称である。それらを復旧することと引き換えに、身代金を支払うように促す脅迫メッセージを表示するソフトウェアであることから、「ransom」（身代金）と「software」（ソフトウェア）を組み合わせた造語で、ランサムウェアと呼ばれている。

図 2-1 WannaCryptor に感染させられた端末の画面

図 1-3-1：ランサムウェアのファイル暗号化の動作概要



ランサムウェアによる被害（医療機関）

【第1回】サイバーセキュリティ対策の重要性をどこまで理解できていたか / 【第2回】発生から1ヶ月以上、通常業務に支障が生じる被害 / 【第3回】このインシデントは「他人事」ではない

大阪急性期・総合医療センター
2022年10月31日～1月10日

発生から1ヶ月以上、通常業務に支障が生じる被害

――大阪急性期・総合医療センターでインシデント発生の一報を聞いた時の状況や心境についてお聞かせください。

嶋津（大阪急性期・総合医療センター）：最初に、院内のコンピュータがウイルスに感染して、「情報システムがちゃんと動きません」と聞きました。データが読めない、電子カルテが見られないということで、それによってどの程度の影響があるのか、回復するまでどの程度かかるのかを考える必要があったのですが、あまりに衝撃が大きかったので呆然としてしまいました。

岩瀬（大阪急性期・総合医療センター）：復旧にどれほどの時間がかかるのか誰も判断できない、見通しも立てられない状態でしたので、とりあえず基幹ベンダーに相談しました。ベンダーとしても異例の事態で、すぐには反応できないという結果でした。

つるぎ町立半田病院
2021年10月31日～1月3日

――半田病院の状況はいかがでしたか？

須藤（つるぎ町立半田病院）：私たちは、まず深夜にプリンターから英文の文章が自動で印刷されてくることから、看護師が電子カルテの異変に気が付きました。その後、当直医に連絡が入り、システム担当者に連絡し、彼がケーブルを抜く作業を行いました。

これはもう災害として対応すべきだろうという状況でしたので、災害対策本部の設置と災害対策会議を開く準備、そして、大学病院や中央病院の処方、検査内容等が見られる徳島県の医療情報ネットワークのウイルス感染を心配し、事務局への連絡も指示しました。また、警察への通報も行い、災害時に対応する紙カルテの運用も開始しました。

ランサムウェアによる被害（大阪急性期・総合医療センター）

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要　2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順　（調査報告書11～12頁）

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置･運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入（漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある）。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

◆被害状況　（調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテを含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。PC端末（院内に約2,200台）も不正アクセスの痕跡あり。 ⇒全てのサーバ、端末をクリーンインストール 基幹システムサーバ再稼働に43日間、部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数：558人（前年同月比33.3%）、延入院患者数：10,191人（前年同月比52.9%） 初診患者数　：465人（前年同月比17.9%）、延外来患者数：15,744人（前年同月比61.6%）
3	被害額	現在精査中　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

1

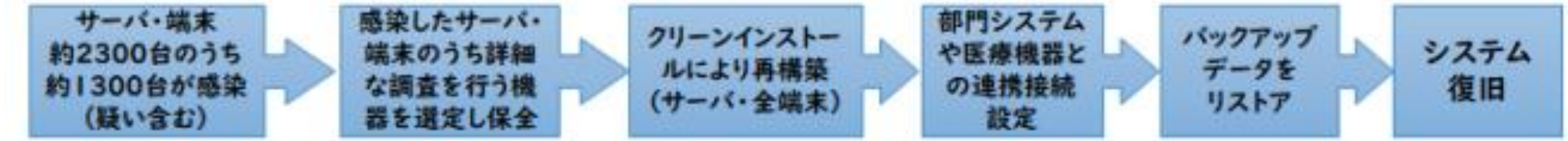
独立行政法人大阪府立病院機構　大阪急性期・総合医療センター　インシデント調査報告書について
https://www.gh.opho.jp/incident/1.html

ランサムウェアによる被害（大阪急性期・総合医療センター）

時間	事象
5時43分	サーバーでエラーが発生（ワーキングサーバーが異常シャットダウン）
6時03分	病棟師長が事務当直に「電子カルテが使えない」と連絡
7時00分	総務リーダーに連絡
7時45分	サーバーのコンソールでランサムノート（身代金要求文書）を確認
8時15分	給食事業者から連絡
8時30分	SE到着し、LANの抜線などの対応を開始
8時50分	自然災害用BCP（事業継続計画）による災害モードに切替え
9時50分	関係各所（法人本部、大阪府、府警など）へ連絡

独立行政法人大阪府立病院機構　大阪急性期・総合医療センター　インシデント調査報告書について
https://www.gh.opho.jp/incident/1.html

ランサムウェアによる被害（大阪急性期・総合医療センター）

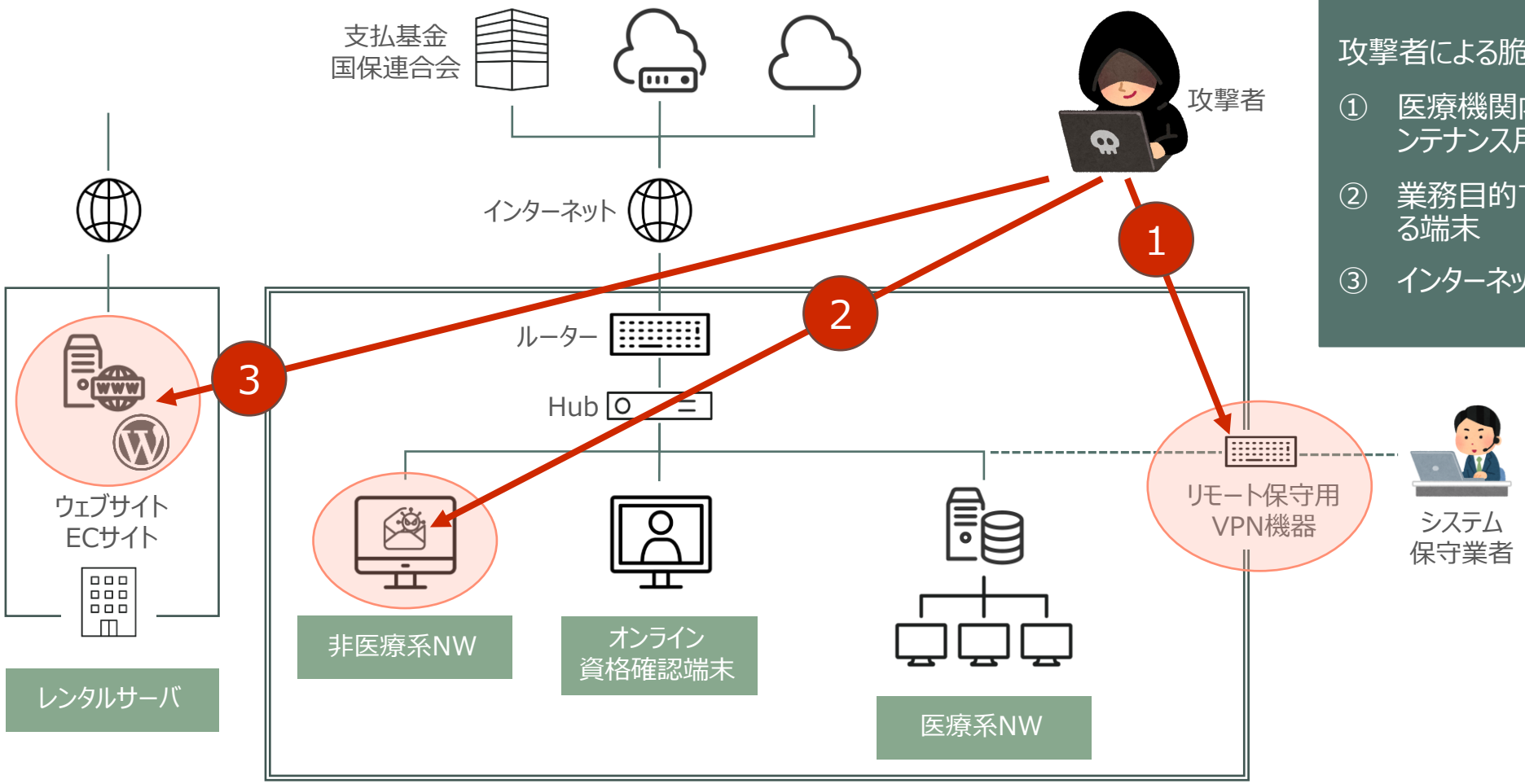


No	項目	概要	対応期間	稼働時期	主な診療再開状況(予定)
1	関連サーバや端末の保全	詳細調査を実施するために、また法執行機関の証拠としての保存や利用を踏まえ、感染した環境のデータを保護	11月1日 ～11月9日	-	・紙カルテ対応に切り替え ・DACS※の情報をもとに患者対応 ・11/4～予定手術再開
2	電子カルテ参照環境の構築	電子カルテシステムのバックアップが確認できたため、個別に電子カルテを参照できる環境を構築	11月1日 ～11月9日	11月10日	・患者対応を拡充 ・11/10～救急診療再開
3	電子カルテシステムの再構築	基幹システム（電子カルテ、オーダリング、医事会計）の再構築を行い、通常どおり電子カルテの参照や記事入力、オーダーができる環境を構築	11月7日 ～12月11日	12月中旬	・電子カルテ運用の順次再開 ・12月中旬に初診、新入院の受け入れを拡大
4	部門システムの再構築	各部門システムの再構築は、サーバ再セットアップのうえ、基幹システムとの接続やテスト等を実施し、システム全体の運用を再開できる環境を構築	11月下旬 ～1月上旬	順次稼働 *1月には全面復旧予定	・重要な部門システム（調剤、検査、画像、給食など）から順次連携接続を再開し診療機能を回復 ・1月に通常診療を完全復旧

※DACS：診療記録文書統合管理システム（Document Archiving and Communication System）
作成媒体を問わず電子カルテを含めた全ての診療記録文書を統合的に管理し、文書を時系列に文書種ごとに閲覧する事が可能となるシステム

独立行政法人大阪府立病院機構　大阪急性期・総合医療センター　インシデント調査報告書について
https://www.gh.opho.jp/incident/1.html

サイバー攻撃者の対象となる医療機関NWの脆弱性



攻撃者による脆弱性の標的対象は、主に

① 医療機関内システムに用いるリモートメンテナンス用VPN機器

② 業務目的でインターネットに接続している端末

③ インターネットに公開しているウェブサイト

セキュリティの責任空白地帯＝脆弱性が発生する構造
～医療機関等/ベンダ間の期待・認識ギャップ～


攻撃者

前提

- 医療機関等のシステム管理担当者の多くはIT管理のみでなく、その他の業務も兼務する等、忙殺されている。最新のセキュリティ動向をキャッチアップする余裕もない。小規模であればあるほどその傾向は強い。
- システム開発・保守、運用等に係る契約書の条項をしっかりチェックし、自局が求めるべきセキュリティ対応を指示するだけのリソース・ナレッジを確保することも困難（薬剤師は医療の専門家であり、ITや法律の専門家ではない）

医療組織の認識

- ベンダーが提示するひな形の契約書やSLA（サービスレベルアグリーメント）等を吟味することなく、医療に携わるのであれば、あうんの呼吸で、自分たちがやってほしいと思うシステム関連業務をベンダがすべて実施しているはずと思い込んでしまう。
- システムの保守・運用にとどまらず、適切なセキュリティ実装・対応も含めてベンダーがすべて担当してくれているという、ベンダにも＜医の倫理＝暗黙のプロフェッショナリズム＞を求める姿勢。（このパターンでよく聞かれる言葉は「セキュリティも含めて、システム関連はすべてベンダーがやっています」）

セキュリティの責任空白地帯

- 結果的に医療機関等と事業者間の認識ギャップに起因する、セキュリティ上の責任の空白地帯が生じ、それを起点としたサイバー攻撃が発生することに・・・
- ＜例＞レセコン会社が導入したPCやルーター（保守契約なし・ハード故障のみ対応等。契約内容にセキュリティパッチ対応が含まれない場合は、医療機関側の責任で管理する必要がある）

ベンダーの認識

- ベンダーは契約書に基づき必要なシステム保守等の業務は担うが、契約書で取り決めのないセキュリティ対応までは責任範疇に入っていない

日本デジタル医学会 第1回学術大会国際シンポジウム「国内医療分野におけるサイバーセキュリティ関連規制の動向と今後」 2025年10月18日
一般社団法人Health ISAC Japan 事務局長 江原悠介 氏 資料より一部改変して引用

直近の国内医療分野のサイバー被害事例（一部）

時期	公開有無	該当組織	被害種別
25年1月	無し	無床診療所 / 四国地方	②：情報漏洩（サポート詐欺）
25年1月	無し	無床診療所 / 関東地方	②：情報漏洩（サポート詐欺）
25年2月	有り	宇都宮セントラルクリニック	①：ランサムウェア（情報漏えいあり）
25年２月	有り	広島市立北部医療センター 安佐市民病	②：情報漏洩（サポート詐欺）
25年２月	有り	武蔵小金井クリニック	③：サイト侵入（情報漏えい）
25年3月	有り	静岡県看護協会	③：サイト侵入（情報漏えい）
25年3月	無し	無床診療所/関東地方	②：情報漏洩（サポート詐欺）
25年4月	無し	歯科診療所 / 関東地方	②：情報漏洩（サポート詐欺）
25年5月	無し	無床診療所/近畿地方	②：情報漏洩（サポート詐欺）
25年6月	無し	病院（100床未満）	①：ランサムウェア
25年8月	無し	無床診療所/東北地方	②：ランサムウェア（InfoStealer系）
25年9月	有り	いまきいれ総合病院	③：メールサーバ不正アクセス

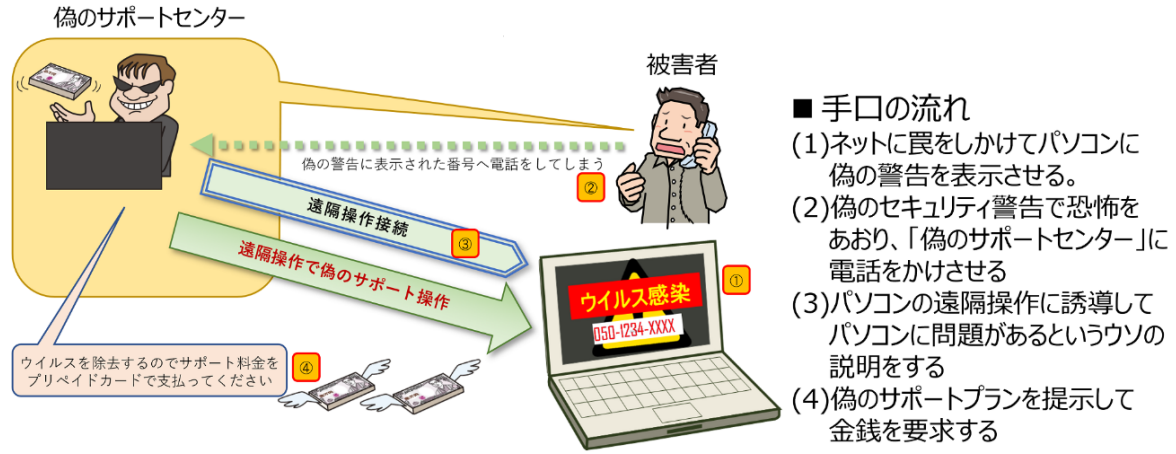
日本デジタル医学会 第1回学術大会国際シンポジウム「国内医療分野におけるサイバーセキュリティ関連規制の動向と今後」 2025年10月18日
一般社団法人Health ISAC Japan 事務局長 江原悠介 氏 資料より引用

サポート詐欺

パソコンでウェブサイトを閲覧中に、突然パソコンがトロイの木馬などのウイルスに感染しているという警告が出ることがあります。画面一杯に広がった警告には「今すぐ○○のサポートに電話してください」と書いてあります。加えて、警告音が鳴りやまず不安をあおることがあります。この場合、表示された警告は「偽のセキュリティ警告」の可能性が非常に高いです。パソコンのウイルス感染はおきていません。

電話をかけると、相手はウイルスを除去するためのサポート料金と称して金銭の支払いを要求します。偽のウイルス感染で被害者をだまして高額の金銭をだまし取ろうとします。そのため、この手口は「サポート詐欺」と呼ばれています。

パソコンに偽のセキュリティ警告が表示された場合は、落ち着いて偽の警告画面を閉じるだけで対処できます。この手口では、電話をかけることで被害が発生します。そのため、**偽のセキュリティ警告に記載された電話番号には「絶対に電話をしない」でください。**電話をかけなければ被害は発生しません。



■手口の流れ
(1)ネットに罠をしかけてパソコンに偽の警告を表示させる。
(2)偽のセキュリティ警告で恐怖をあおり、「偽のサポートセンター」に電話をかけさせる
(3)パソコンの遠隔操作に誘導してパソコンに問題があるというウソの説明をする
(4)偽のサポートプランを提示して金銭を要求する

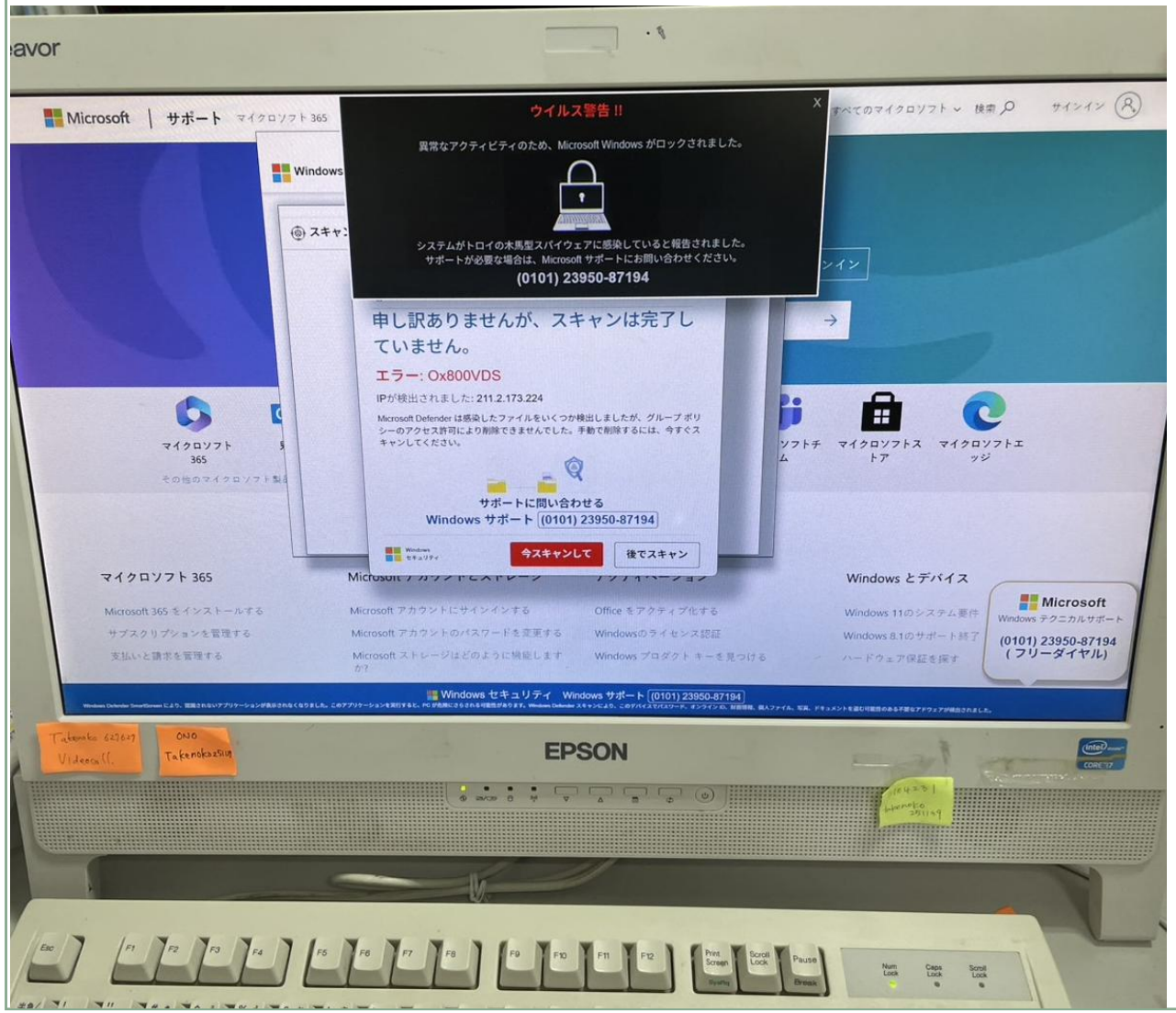
図3：サポート詐欺の手口の流れ

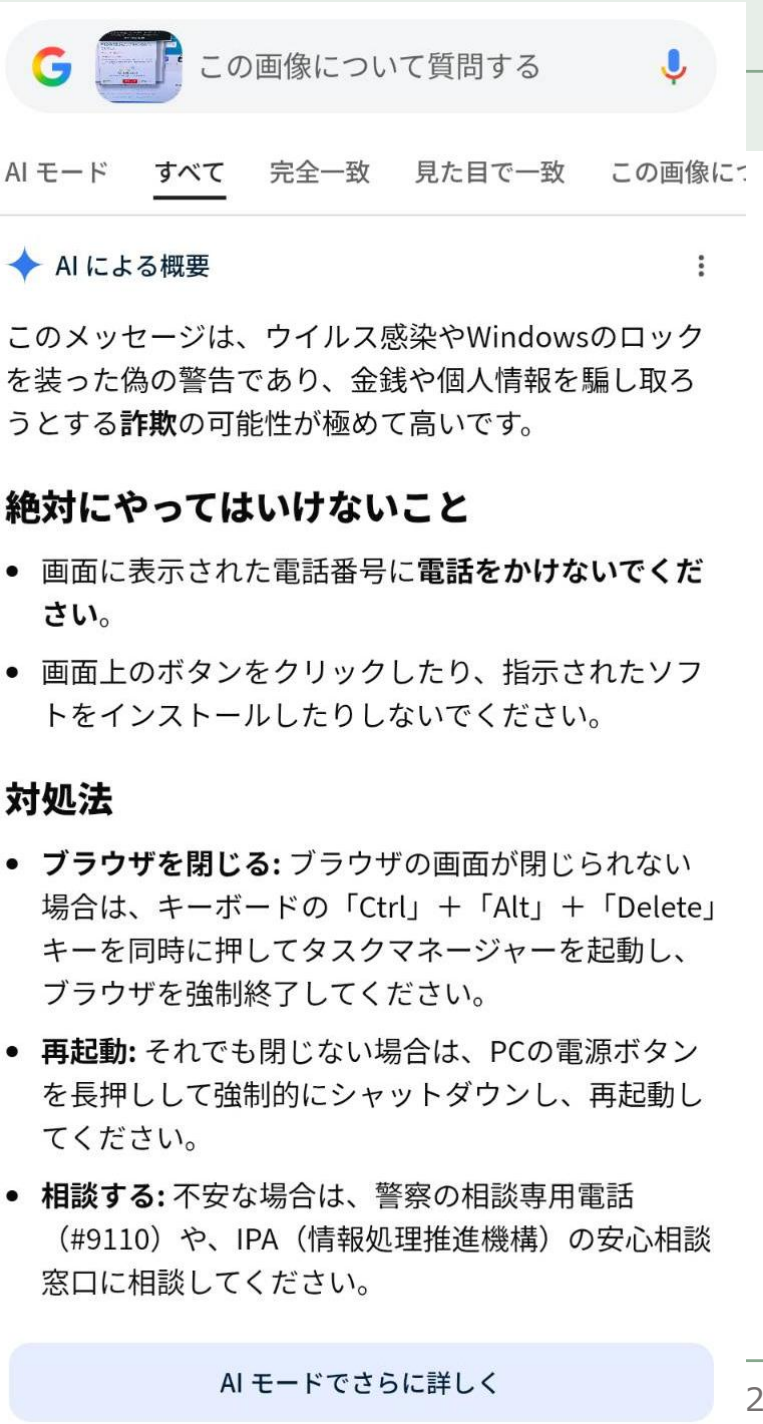
図5：検索結果から偽のセキュリティ警告が表示される例

図6：被害者の恐怖心をあおるしかけの例

「パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意」独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html

サポート詐欺　未遂事例





有限会社インフィニティ　たけのこ薬局　提供

サイバー攻撃者の標的「脆弱性」

攻撃者

２つの「脆弱性」を悪用し、攻撃対象のシステム・ネットワークへ侵入し、データ窃取やシステム暗号化等の攻撃を行う

組織の弱さがあると脆弱性が増して、リスクが高まる

人の脆弱性（弱さ）

楽をしたい、忘れやすい、誘惑に弱い・・・

単純なパスワードの設定・使いまわし

メール添付ファイルを確認せずに開封　等

システムの脆弱性（脆さ）

システムは時間の経過とともにセキュリティホールが必ず発生する（常時メンテしないと安全性が保てない）

セキュリティパッチの未適用
ウイルス対策の不徹底
初期パスワードの未変更　　等

組織の脆弱性（弱さ）

サイバーセキュリティ意識の低い経営者
お金をかけたくない、一人情シス（担当者任せ）
自分（自組織）は大丈夫だと思っている

社員へのセキュリティ教育不足
予算不足→担当者不可増大
担当者が退職→引継ぎなし

サイバー攻撃は進化する～いまの攻撃トレンド（流行）は？

サイバー攻撃も人が仕掛けているため、人を取り巻く社会・技術環境とともに変化することは当然である。

コロナ禍によるリモートワーク環境の浸透に伴い、攻撃のブームも特定の組織に計画的に攻撃を行う**第1波のパターン**から、攻撃ツールの開発・実行、攻撃先偵察・身代金交渉等を行う各部門が分業体制のもとで、脆弱性を長期放置している組織へ無差別に攻撃を行う**第２波のパターン**へ移行していった。**いわゆる国内医療機関におけるランサム事案の多くはこの第2波に該当する。**

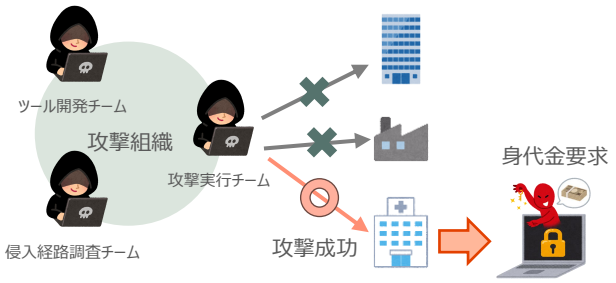
一方で、**こうした攻撃パターンへの防御策が被害者側に浸透し始めた**ため、今は**AI技術**を用いて、システム・機器の脆弱性を悪用した裏口型のリアルタイム型侵入に加え、**ヒトの脆弱性をターゲットにして正面から攻撃環境へ侵入するためのサポート詐欺（AIによる日本語音声での自動応答）、あるいは洗練された日本語文面によるメールフィッシング等の第3波のパターン**が流行し始めている。

第1波(~2019)：コロナ前

特定の組織に標的を絞り、計画的に攻撃を行い、大きな収益（金銭）を得ようとするベーシックな攻撃

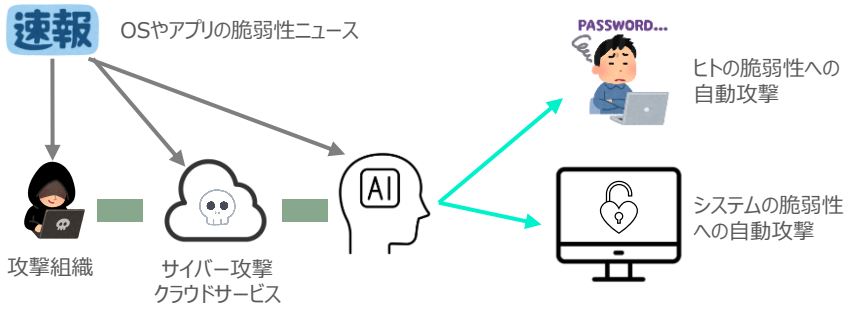
第2波(2020～22：コロナ下)

分業した攻撃組織が、脆弱性を放置する組織に対して無差別に攻撃を行い、効率的に収益（金銭）を得ようとする、技術進歩型の攻撃



第３波(コロナ後：2023～)

AIを用いて、脆弱性発生に伴い、対応前に攻撃をしかけようとするアプローチ、及び「ヒトの脆弱性」を標的とした正面型攻撃の隆盛



サイバーセキュリティー対策　難しいところ

1.目に見えない

守るべきものは何か？　敵は誰？　侵入経路は？

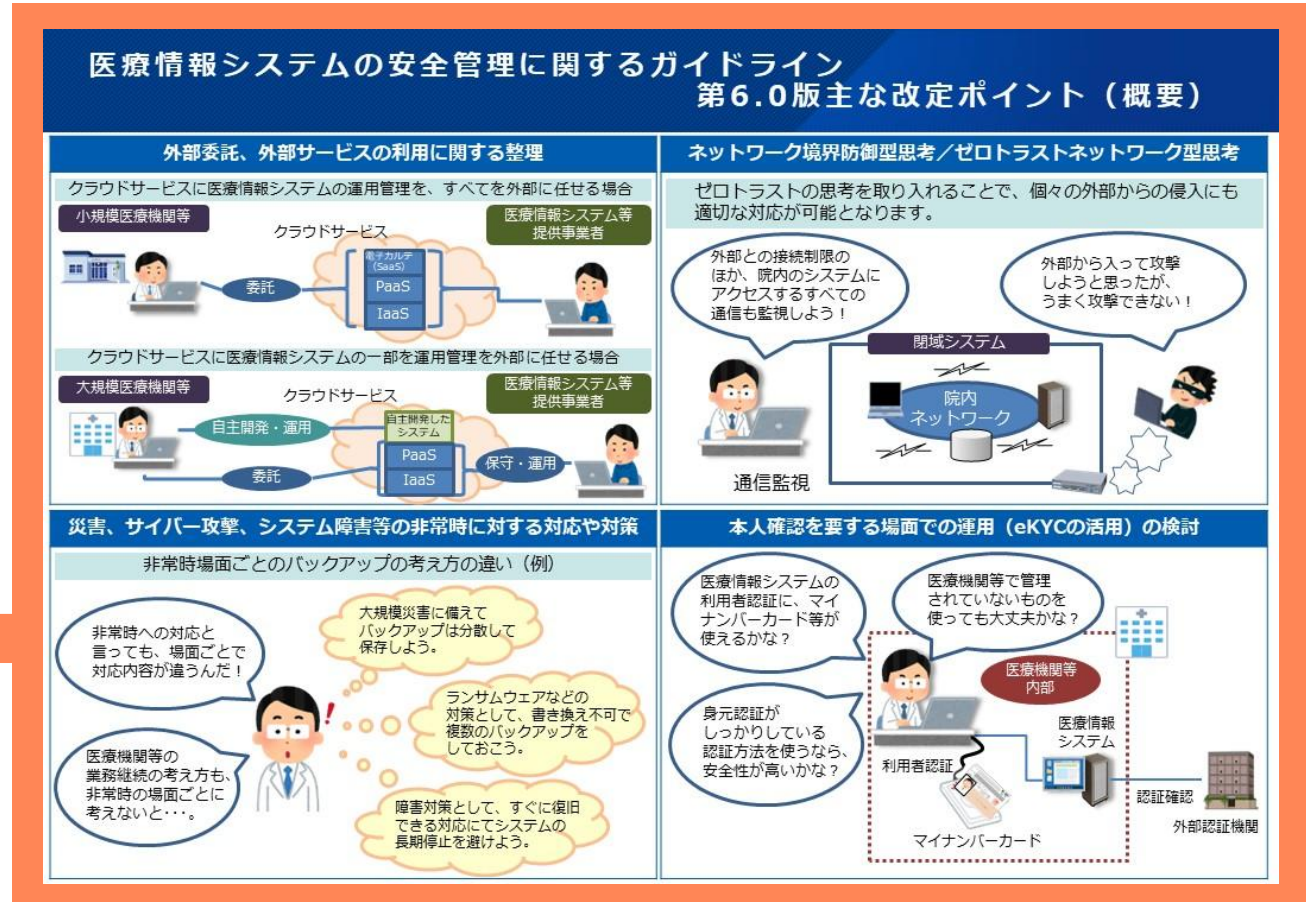
3.100%がない

例：OSのセキュリティーパッチ、
時代の変化＝閉域網神話の崩壊、サイバー攻撃手法の変化
リスク分析と費用対効果の検討

３.知識レベル･危機意識がバラバラ

基礎教育からスタートさせる必要
定期的な知識アップデートと対策の継続的実施が必要

医療DXの盾（サイバーセキュリティ対策）
＝医療情報システムの安全管理に関するガイドライン6版



医療DXの盾（サイバーセキュリティ対策チェックリスト）
＝まずは医療機関等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

令和７年度版

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

～医療機関等・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」または「薬局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。医療機関等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、まずは医療機関等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。

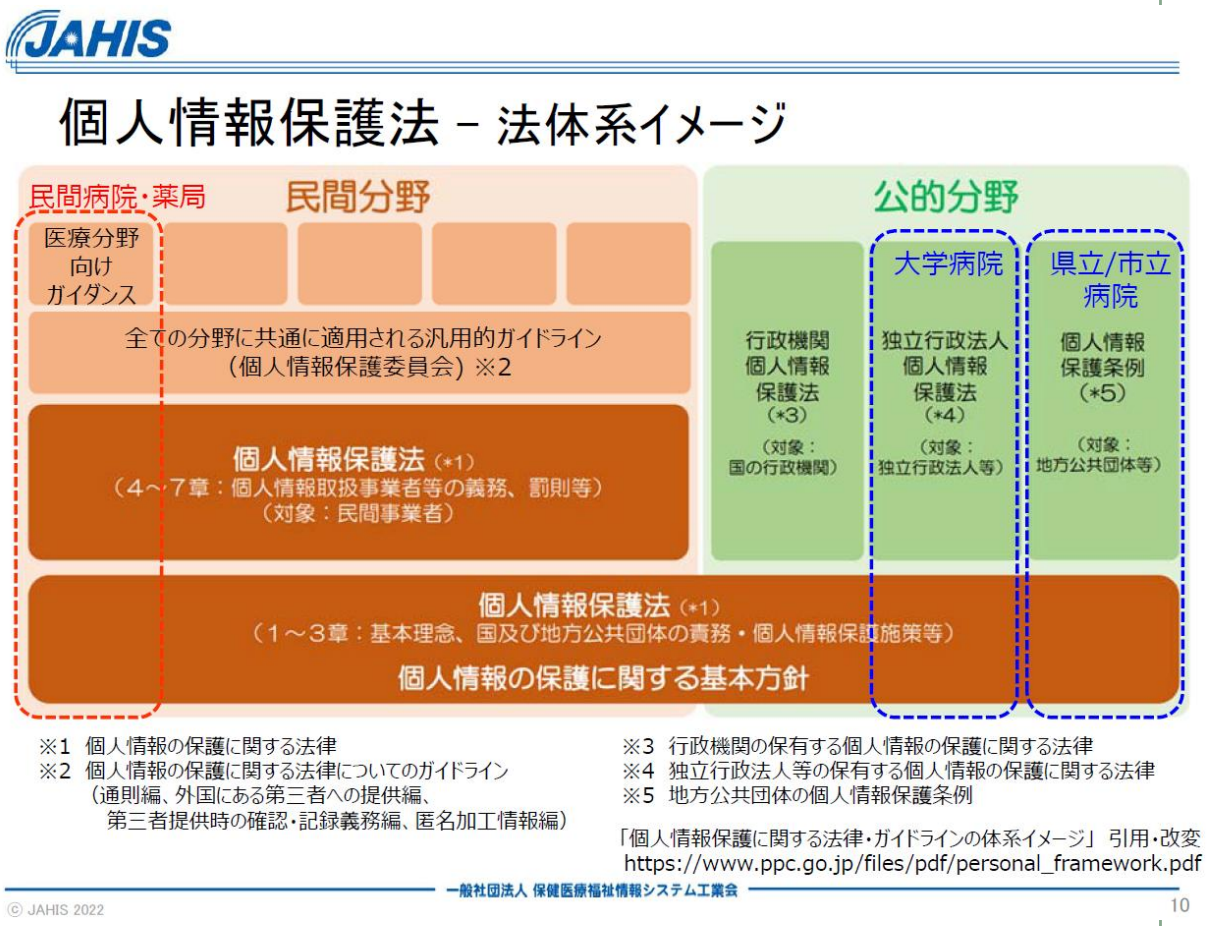
本マニュアルは、医療機関等におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

守るべき情報とは

個人情報保護法

氏名や性別、生年月日、住所などの情報は、個人のプライバシーに関わる大切な情報です。一方、それらの情報を活用することで、行政や医療、ビジネスなど様々な分野において、サービスの向上や業務の効率化が図られるという側面もあります。
そこで、個人情報の有用性に配慮しながら、個人の権利や利益を守ることを目的とした「個人情報保護法」（正式名称：個人情報の保護に関する法律）が平成15年（2003年）5月に制定され、平成17年（2005年）4月に全面施行されました。
その後、デジタル技術の進展やグローバル化などの経済・社会情勢の変化や、世の中の個人情報に対する意識の高まりなどに対応するため、個人情報保護法は、これまでに3度の大きな改正が行われました。

https://www.gov-online.go.jp/useful/article/201703/1.html



個人情報とは

個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報をいいます。
これには、他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも含まれます。例えば、生年月日や電話番号などは、それ単体では特定の個人を識別できないような情報ですが、氏名などと組み合わせることで特定の個人を識別できるため、個人情報に該当する場合があります。
また、メールアドレスについてもユーザー名やドメイン名から特定の個人を識別することができる場合は、それ自体が単体で、個人情報に該当します。このほか、番号、記号、符号などで、その情報単体から特定の個人を識別できる情報で、政令・規則で定められたものを「個人識別符号」といい、個人識別符号が含まれる情報は個人情報となります。
例えば、次のようなものです。
（1）　身体の一部の特徴を電子処理のために変換した符号で、顔認証データ、指紋認証データ、虹彩、声紋、歩行の態様、手指の静脈、掌紋などのデータがあります。
（2）　サービス利用や書類において利用者ごとに割り振られる符号で、パスポート番号、基礎年金番号、運転免許証番号、住民票コード、マイナンバー、保険者番号などがあります。
（以上、政府広報オンラインより　https://www.gov-online.go.jp/useful/article/201703/1.html）

（医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス ）
例えば、細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列、健康保険法に基づく保険者番号や被保険者等記号・番号などが該当する。したがって、当該保険者番号及び被保険者番号・記号のいずれもが含まれる情報は、個人情報となる。

https://www.gov-online.go.jp/useful/article/201703/1.html

要配慮個人情報

- 不当な差別や偏見などの不利益が生じないように、その取扱いに特に配慮を要する個人情報
- 人種、信条、社会的身分、病歴、犯罪の経歴、犯罪の被害に遭った事実などに関する個人情報

→調剤にかかる情報、　業務で薬剤師が知り得た情報全て、調剤を受けたことも含む

要配慮個人情報には、要配慮個人情報を推知させるにすぎない情報（例：宗教に関する書籍の購買や貸出しに係る情報等）は含まないとされています（個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」１２頁）。「推知」とは、ある事実をもとにおしはかって知ることをいいます。
もっとも、要配慮個人情報を推知させる情報であっても慎重な取扱いをすべき場合があることには留意が必要です。

https://www.ppc.go.jp/files/pdf/01_iryoukaigo_guidance5.pdf

JAHIS

要配慮個人情報

個人情報のうち、以下のいずれかに該当する情報。

- 人種、信条、社会的身分、病歴、前科、犯罪被害情報
- その他本人に対する不当な差別、偏見が生じないように特に配慮を要するものとして政令で定めるもの

病歴とは：

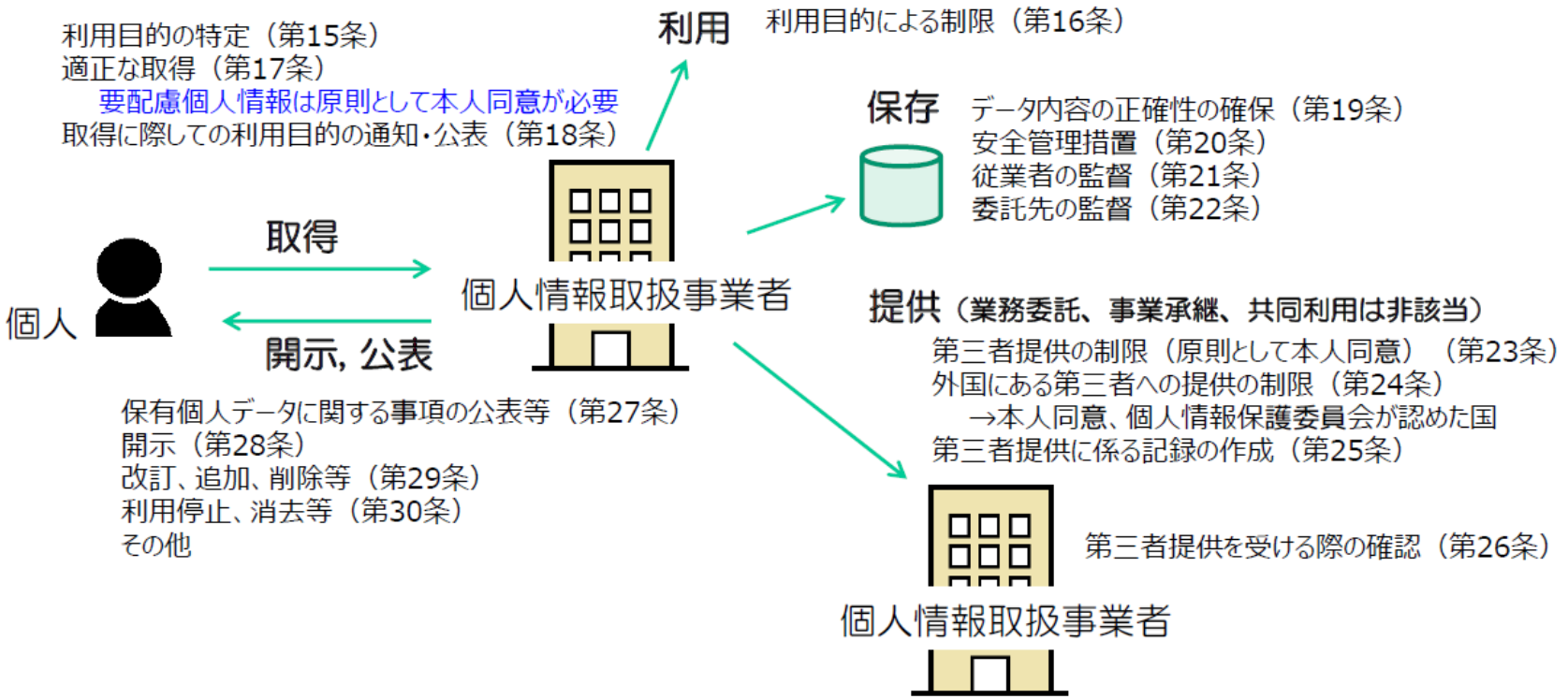
- 身体障害、知的障害、精神障害等があること
- 医師等により行われた健康診断その他の検査の結果
- 医師等により保健指導、診療、調剤等が行われたこと

要配慮個人情報を取得したり、第三者提供したりするには、原則として事前に本人の同意を得る必要がある。

引用：「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」
一般社団法人 保健医療福祉情報システム工業会

個人情報取扱事業者の義務

個人情報取扱事業者は、個人情報の取り扱いに関する主な義務として、以下を負う。



医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

「個人情報」とは、生存する「個人に関する情報」であって、当該情報に含まれる氏名、生年月日、その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）又は個人識別符号が含まれるものをいう。
「個人に関する情報」は、氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているか否かを問わない。
また、例えば診療録には、患者について客観的な検査をしたデータもあれば、それに対して医師が行った判断や評価も書かれている。これら全体が患者個人に関する情報に当たるものであるが、あわせて、当該診療録を作成した医師の側からみると、自分が行った判断や評価を書いているものであるので、医師個人に関する情報とも言うことができる。したがって、診療録等に記載されている情報の中には、患者と医師等双方の個人情報という二面性を持っている部分もあることに留意が必要である。
なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。
本ガイダンスは、医療・介護関係事業者が保有する医療・介護関係個人情報を対象とするものであり、診療録等の形態に整理されていない場合でも個人情報に該当する。

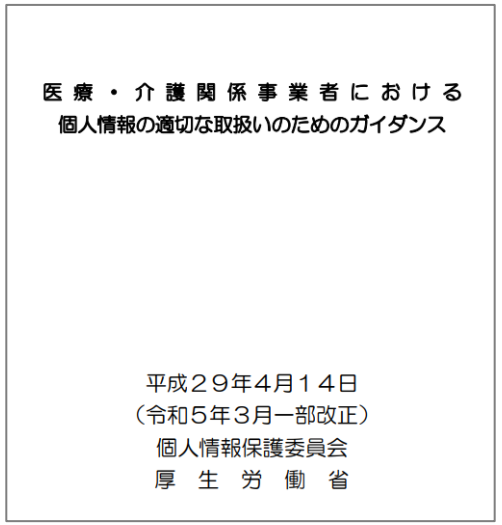
本ガイダンスでは、患者・利用者が死亡した後においても、事業者が当該患者・利用者の情報を保存している場合には、情報の漏えい等の防止のため、生存する個人の情報と同様の安全管理措置を講ずるよう求めています（参照：ガイダンスｐ２）。
また、患者・利用者が死亡した際に、遺族に対して診療情報・介護関係記録を提供する場合には、厚生労働省において平成１５年９月に作成した「診療情報の提供等に関する指針」の「９ 遺族に対する診療情報の提供」の取扱いに従って提供を行うことを求めています（参照：ガイダンスｐ４）。

○医療機関等における個人情報の例

診療録、処方せん、手術記録、助産録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約、調剤録 等

○介護関係事業者における個人情報の例

ケアプラン、介護サービス提供にかかる計画、提供したサービス内容等の記録、事故の状況等の記録 等


医療・介護関係事業者における
個人情報の適切な取扱いのためのガイダンス

平成２９年４月１４日
（令和５年３月一部改正）
個人情報保護委員会
厚 生 労 働 省

https://www.ppc.go.jp/files/pdf/01_iryoukaigo_guidance5.pdf

医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

医療における個人情報の特殊性

- 患者・利用者が死亡した後においても、医療・介護関係事業者が当該患者・利用者の情報を保存している場合には、漏えい、滅失、き損等の防止のため、個人情報と同等の安全管理措置を講じる
- 死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合、生存する個人に関する情報として扱う
- 診療録全体が患者個人に関する情報に当たるものであるが、あわせて、当該診療録を作成した医師の側からみると、自らが行なった判断や評価を　書いているものであり、医師個人に関する情報にもなる。

  診療録等の情報は、患者個人の情報と医師個人の情報の二面性を持つ部分が含まれるため留意が必要だが、患者本人から開示の請求がある場合に、その二面性があることを理由に全部又は一部を開示しないことはできない。

医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス

医療における本人同意（黙示の同意）

- 患者が受診を申し出ることは、患者自身が自己の要配慮個人情報を含めた個人情報を医療機関等に取得されることを前提としていると考えられるため、患者の受診申し出をもって、要配慮個人情報の取得についての本人の同意があったとみなされる。
- 取得された要配慮個人情報は、患者自身の医療サービスの提供のために利用されることは明らかであるため、院内掲示等により患者に提供する医療サービスに関する利用目的を公表することにより、患者からの明示的な留保の意思表示がない限り、患者の黙示による同意があったものと考える。

  患者自身の医療サービスの提供のための第三者提供は、院内掲示により「黙示の同意」に含めることができる。

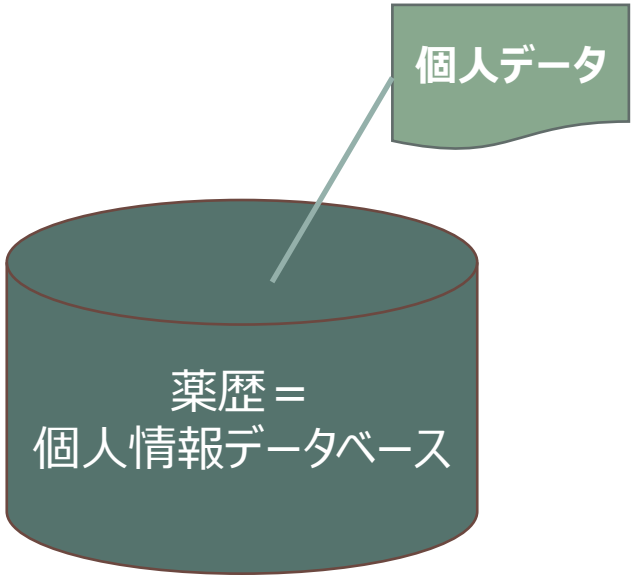
  例：　他の医療機関等との連携する
  外部の医師等の意見・助言をもとめる
  他の医療機関等からの照会に応える
  家族等への病状説明を行う

個人情報データベース等と個人データ

「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した個人情報を含む情報の集合体、又はコンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば、五十音順、生年月日順など）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものをいう。なお、個人情報データベース等に該当しないものとしては、市販の電話帳や住宅地図などが該当するが、詳細は「通則ガイドライン」を参照されたい。

「個人データ」とは、「個人情報データベース等」を構成する個人情報をいう。診療録等の診療記録や介護関係記録については、媒体の如何にかかわらず個人データに該当する。
また、検査等の目的で、患者から血液等の検体を採取して検査結果を得た場合、これらの検査結果は個人情報に該当し、利用目的の特定等（Ⅳ３．参照）、利用目的の通知等（Ⅳ５．参照）等の対象となることから、患者の同意を得ずに、特定された利用目的の達成に必要な範囲を超えて当該個人情報を取り扱ってはならない。なお、検体についても、その分析等により個人情報を取得し得ること等に鑑み、個人情報と同様の取扱いとすることが望ましい。また、これらの検査結果については、診療録等と同様に検索可能な状態として保存されることから、個人データに該当し、第三者提供の制限（Ⅳ９．参照）や開示（Ⅳ１４．参照）の対象となる。

https://www.ppc.go.jp/files/pdf/01_iryoukaigo_guidance5.pdf



個人情報データベース等＝特定の個人情報を検索できるように体系的にまとめられたもの**→例：薬歴全体**

個人データ＝個人情報データベースを構成する個人情報をいう **→例：個人の薬歴**

医療情報・医療情報システムとは

＜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＞

２．２ 医療情報・文書の範囲

本ガイドラインで対象とする医療情報とは、医療に関する患者情報（個人識別情報）を含む情報を想定する。

本ガイドラインで対象とする文書は、医療情報を含む文書全般を想定し、法定の保存義務の有無を問わない。

２．３ 医療情報システムの範囲

本ガイドラインが対象とする医療情報システムは、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を想定する。これには、医療情報システム・サービス事業者（※）により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれる。

なお、医療情報を含まない患者への費用請求に関する情報しか取り扱わない会計・経理システム等は、本ガイドラインにおける医療情報システムには含まない。

（※）本ガイドラインで用いる「医療情報システム・サービス事業者」とは、医療情報システムの製造、開発、販売及び保守を行う事業者や、医療情報システムを活用したサービスの提供、保守等を行う事業者など、医療機関等が医療情報システムを利用・管理する上で関係する事業者全般を想定する。

要配慮個人情報の漏えい → 個人情報保護委員会への報告、本人への通知

漏えい＝「個人データが外部に流失すること」

【事例】

- 個人データが記載された書類を第三者に誤送付した場合
- 個人データを含むメールを第三者に誤送信した場合
- システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となっていた場合
- 個人データが記載又は記録された書類・媒体等が盗難された場合
- 不正アクセス等により第三者に個人データを含む情報が窃取された場合

→閲覧されないうちに回収した場合は漏えいに該当しない

2．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。
  （※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
- **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

（個人の権利利益を害するおそれが大きいもの）

規則第七条 法第二十六条第一項本文の個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

一 **要配慮個人情報が含まれる個人データ**（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）**の漏えい、滅失若しくは毀損**（以下この条及び次条第一項において「漏えい等」という。）**が発生し、又は発生したおそれがある事態**

二 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

三 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

四 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

https://www.ppc.go.jp/files/pdf/01_iryoukaigo_guidance5.pdf

漏えい等事案が発覚した場合に講ずべき措置

① **事業者内部における報告及び被害の拡大防止**
責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

② **事実関係の調査及び原因の究明**
漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

③ **影響範囲の特定**
上記②で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

④ **再発防止策の検討及び実施**
上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

⑤ **個人情報保護委員会への報告及び本人への通知**

→漏えい等事案の内容等に応じて公表

◆速報

- 事態を知ってから「速やかに」（概ね3～５日）
- その時点で把握している内容

◆確報

- 事態を知ってから30日以内
- 全ての報告事項

個人情報の保護に関する法律についてのガイドライン（通則編）
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

個人情報保護法違反

- **刑事責任（罰則強化）**
- **民事　損害賠償**
- その他のリスク（**社会的信用の失墜、復旧コストなど**）

秘密漏示罪（守秘義務違反）

刑法（秘密漏示）
第百三十四条　医師、薬剤師、医薬品販売業者、助産師、弁護士、弁護人、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、六月以下の懲役又は十万円以下の罰金に処する。

サイバー攻撃を受けた場合の報告

医療機関等がサイバー攻撃を受けた際は速やかに厚生労働省に報告願います

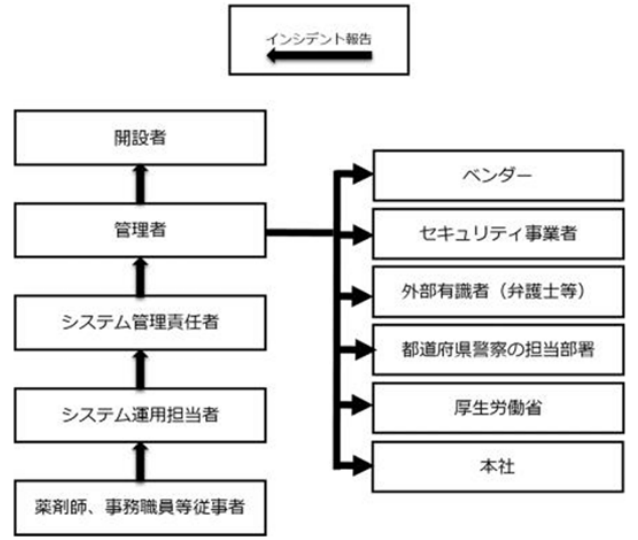
「医療情報システムの安全管理に関するガイドライン」では、医療機関等がサイバー攻撃を受けた（疑い含む）場合等の際には、厚生労働省等の所管省庁への連絡等、必要な対応を行うことを示しています。
医療機関等がサイバーインシデント（サイバー攻撃やその疑いを含む）を受けた場合、以下の連絡先へ、インシデント発生後速やかにご連絡ください。

医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先
医政局・医療情報担当参事官室
TEL： 03-6812-7837
MAIL： igishitsu@mhlw.go.jp。

サイバー攻撃等により個人情報等が漏洩したおそれが発生した場合

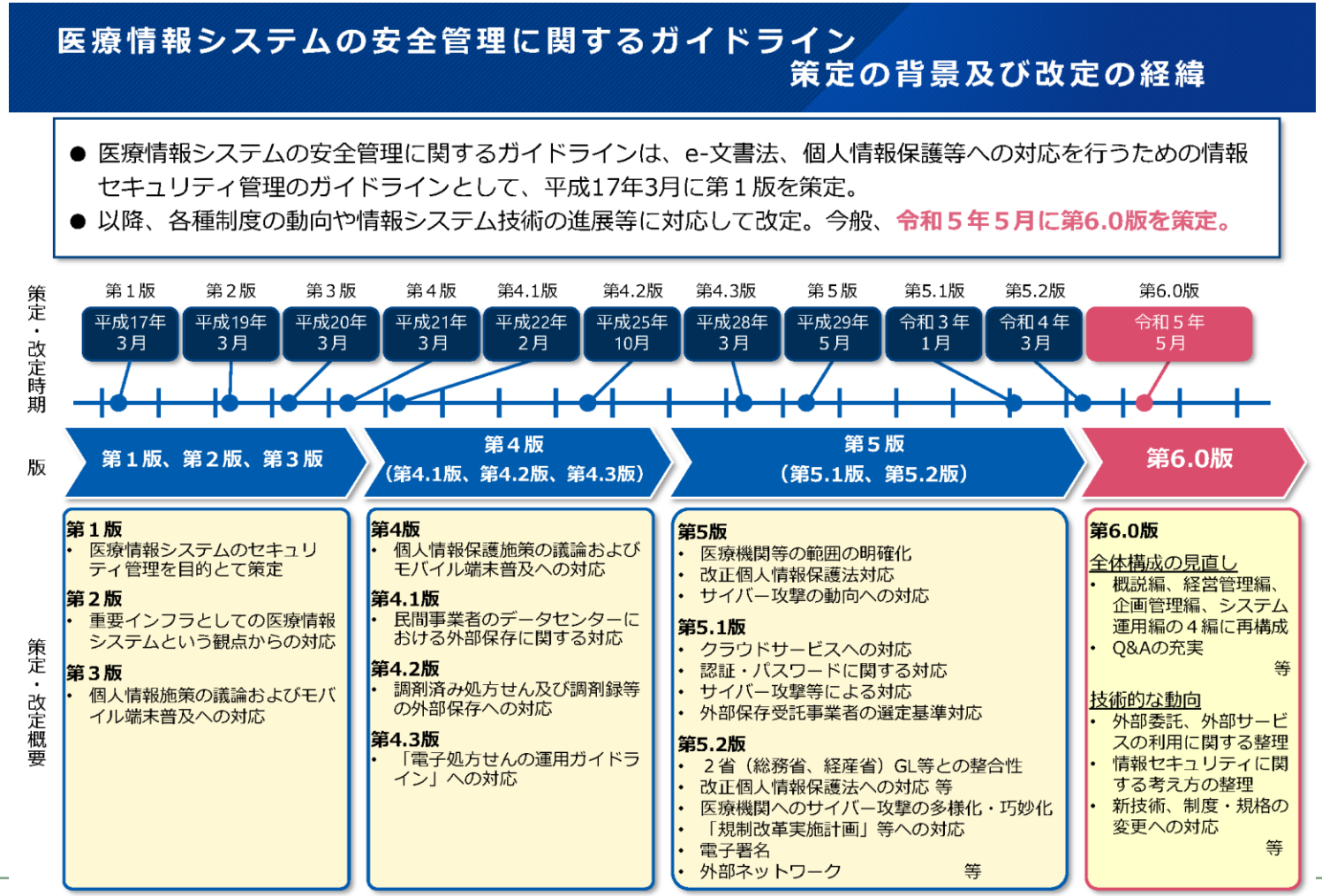
サイバー攻撃等により、患者の個人情報を含む医療情報等、個人データの漏えい（漏えいのおそれを含む）等が発生した場合は、個人情報保護委員会への報告が必要です。
詳細は、個人情報保護委員会のHPを確認してください。
＜漏えい等の対応とお役立ち資料＞
https://www.ppc.go.jp/personalinfo/legal/leakAction/

●連絡体制図の例２（薬局）



医療情報システムの安全管理に関するガイドライン6版とサイバーセキュリティ対策チェックリスト

医療情報システムの安全管理に関するガイドライン6版　令和5年5月31日



個別指導時 「最新版に準拠していることの確認」

10. 医療情報システムの概況等（電子薬歴システムチェック表） ＜様式８＞

保険薬局コード　　保険薬局の名称：

保険薬局の電話番号：

電子薬歴システムの基本情報

ベンダー社名：　　機種：

ベンダー担当者名：

※[□いる　□いない]等該当するものに印：☑を付け、（　）に具体的な取扱状況をご記入ください。

１　「 医療情報システムの安全管理に関するガイドライン」（最新版）に準拠していることを開設者・管理者（院長）が確認しているか。・・・・・・・・・・・・・・□していない　□している

２　真正性、見読性、保存性の３基準を満たしているか。

（１）真正性について

○システム管理者 ・・・・ □いない　☑（職名　管理薬剤師　氏名　　）

○システム操作業務日誌 ・・・・・・・・ □設置している　☑設置していない

○アクセスログ情報の参照 ・・・・・・ ☑参照できる　□参照できない

アクセスログへのアクセス制限があるか ・・・・・・ ☑ある　□ない

○電子薬歴システムの利用申請書及び誓約書 ・・・・・・ ☑ない　□ある　（ 見本：　☑有　□無 ）

個別指導時　運用管理規程等も「最新版に準拠している」のが前提

3　運用管理規程等の留意事項は守られているか。

○電子保存に関する運用管理規程 ・・・・ □定めていない　☑定めている（　　～運用開始）
　運用マニュアル ・・・・・・・・・・・・・・・・ ☑ない　□ある（利用可能にしてある）
　操作訓練 ・・・・・・・・・・・・・・・・・・・・・・ ☑実施していない　□定期的に実施している（　　）
○患者のプライバシー保護
　クライアントに診療情報が残るか ・・・・・・・・ □残らない　☑残る
　患者情報が含まれた情報の抽出 ・・・・・・・・・・ □抽出できない　☑抽出できる（ＵＳＢ）
　患者情報の院外持ち出し ・・・・・・・・・・・・・・・ ☑禁止している　□自由に持ち出しできる
　入力、修正、参照等のアクセスログ情報 ・・ ☑記録されている　□記録されない
　個人情報保護対策 ・・・ ☑局内にプライバシーポリシーを貼っている　□何もしていない
　個人情報漏洩に対する規則 ・・・ □ない　☑ある（個人情報漏洩者に対する罰則：　☑有　□無）
○開示請求への対応 ・・・・・・・・・・・・・・ □対応していない　☑対応している
○情報の安全性及びプライバシー保護に関する職員への教育及び研修 ・・・・・ □未実施　☑実施
○監査体制又は第三者機関への監査依頼を規定しているか ・・・ □何もない　☑規定している

医療情報システムの安全管理に関するガイドラインの全体構成

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。

概説 編 Overview

ガイドラインの各編を読むに際して、
まずはじめに、前提として必要な知識や
各編の基本的な概要をまとめる。

- ガイドラインの目的
- 対象とする情報・文書・システム
- 関連する法令等の規定との関係や経緯
- 各編の位置付けと目次構成、概要 等

経営管理 編 Governance

組織の経営方針を策定し、
情報化戦略を立案する
経営管理層に必要な考え方や
関連法制度等をまとめる。

- 取り扱う情報の重要性と関連法規
- 情報資産管理や情報システム運用に伴い生じる責任・責務
- 情報システムの有用性と安全管理 等

企画管理 編 Management

経営方針・情報化戦略に基づき、
システム利用者・管理者・事業者で
情報資産を運営、情報化を管理する
考え方や方法論をまとめる。

- 情報資産管理体制と責任分界
- リスクアセスメントと対策
- 情報の種類に応じた管理・監査
- 非常時の対応と非常時への対策 等

システム運用 編 Control

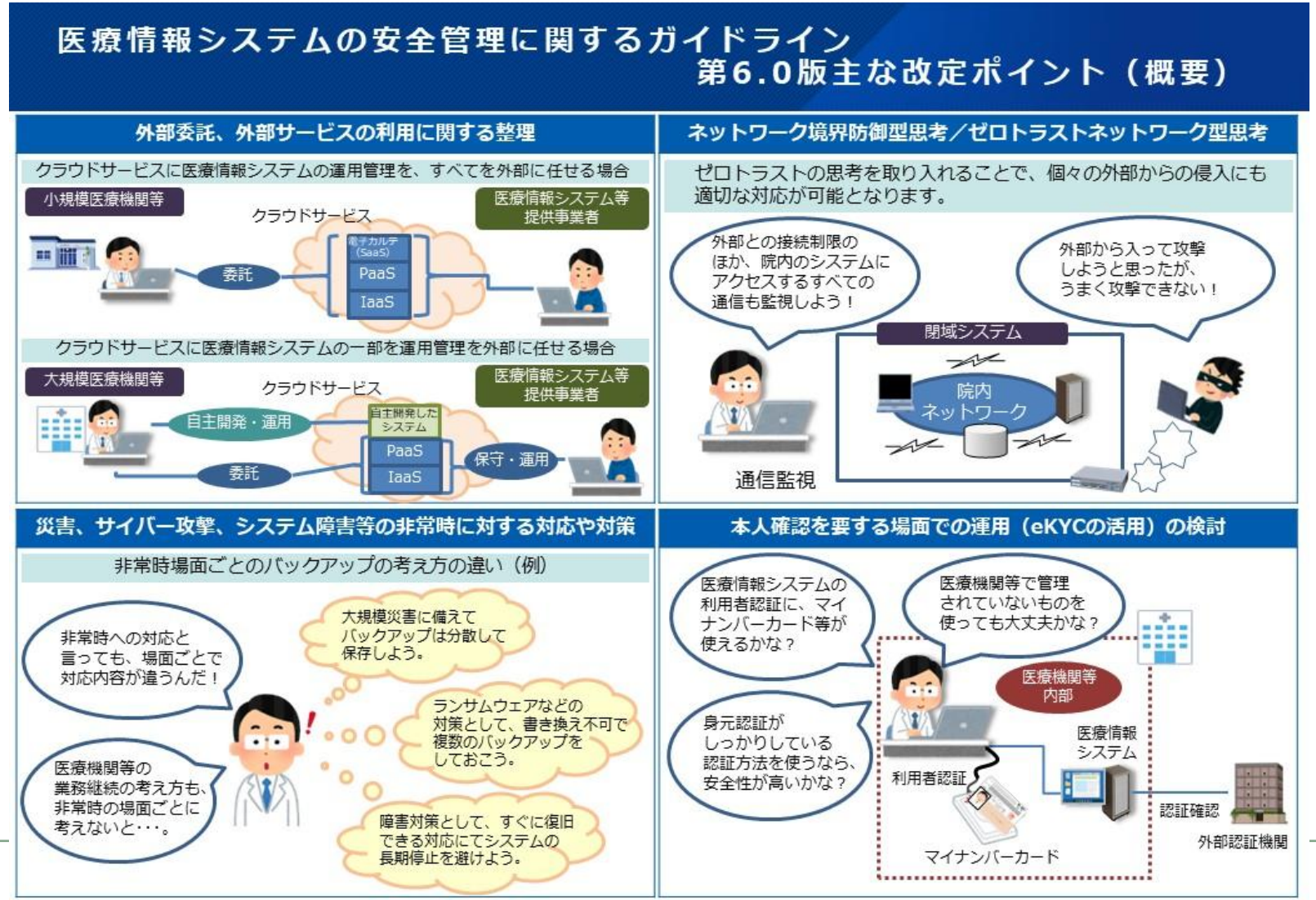
安全な情報資産管理やシステム運用を
実現するために、関連法制度を遵守した
考え方とその実装手法、活用する技術等、
具体的な考え方や技術をまとめる。

- 個人情報保護法、e-文書法、電子署名法等により求められる技術
- システム利用者、クライアント側/サーバ側/インフラ領域等それぞれで活用する安全管理対策・措置技術 等

別添 資料 Appendix

- Q&A
- 用語集
- 診療所、薬局等の小規模医療機関等向けの特集
- 医療機関におけるサイバーセキュリティに関する特集
- ガイドラインの改定と関連法規の遷移
- ガイドラインと関連法規との関係性、遷移
- 第5.2版から第6.0版への各項目の移行対応表
- 第6.0版の各編の各項目の相関表
- サイバーセキュリティ対策チェックリスト
- システム障害発生時の対応フローチャート 等

医療情報システムの安全管理に関するガイドライン６版改定ポイント

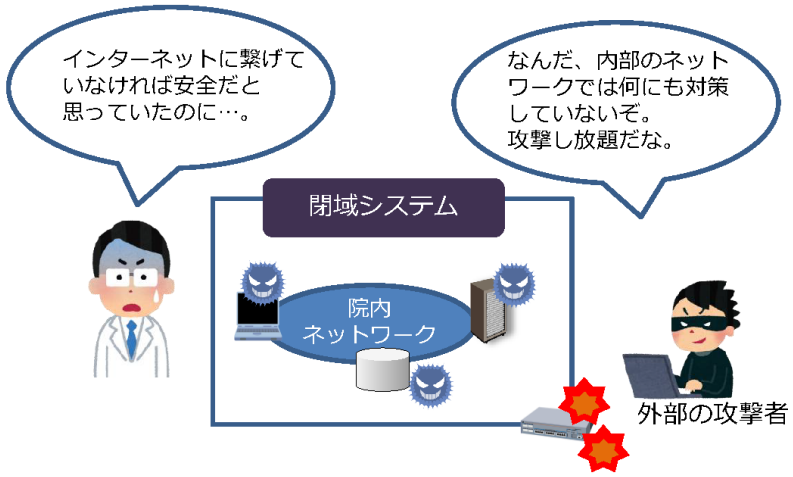


医療情報システムの安全管理に関するガイドラインの全体構成

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-

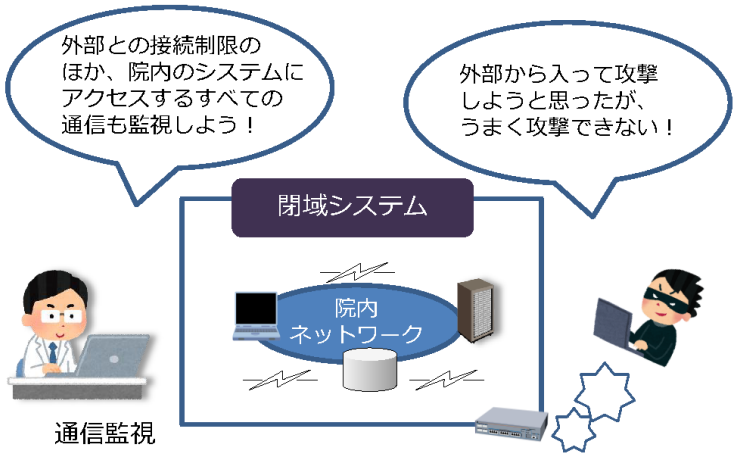
- ネットワークに関する整理を行うほか、対策のあり方として、ゼロトラストネットワーク型思考を取り入れることの有用性について示しました。
- 境界防御型思考とゼロトラスト思考をうまく組み合わせて対応することについて示しています。

サイバー攻撃の巧妙化などにより、閉域網にある医療情報システムおいても、外部からの侵入のリスクが高まっています。



境界防御だけに対策を頼っている場合

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。



ゼロトラスト思考を入れた対策をとっている場合

薬局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７年度版
薬局におけるサイバーセキュリティ対策チェックリスト

薬局確認用

*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。(2-②) ※事業者と契約していない場合には、記入不要	はい・いいえ (/)	(/)	
	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～医療機関等・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。

令和７年度
薬局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	(日付) 確認日	(日付) 目標日	備考
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 (/)	(/)	
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 (/)	(/)	
	薬局に製造業者/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。(2-②)	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接続機器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 (/)	(/)	

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～医療機関等・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。

1．チェックリストの用意

○　チェックリストを使用するにあたり、医療機関等においては「医療機関確認用」または「薬局確認用」、事業者においては「事業者確認用」を用いて確認してください。事業者と契約していない*医療機関等においては「事業者確認用」による確認は不要です。

＊以下、「事業者と契約していない」とは製品購入の売買契約のみで、運用又は管理・保守に関する契約等がない場合を指します。

○　医療機関等は事業者に「事業者確認用」を送付し、対策の状況を確認するよう求めてください。複数の医療情報システムを利用している場合、システムを提供している事業者ごとに確認を求めてください。なお、事業者に対しても別途本取組について周知を行っていきます。

レセコン・電子薬歴以外のシステムや機器でも、個人情報取り扱う（例：NSIPSを受信して活用する）システムは対象となります

↓

事業者確認用の提出を求めてください

サイバーセキュリティ対策チェックリスト　マニュアル

～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。医療機関等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、まずは医療機関等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、医療機関等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。

○　医療機関等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。

～立入検査時、チェックリストを確認します～

医療法第 25 条第１項に基づく立入検査では、病院、診療所および助産所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を確認することとしています。また、薬機法に基づく立入検査では、薬局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を確認することとしています。

立入検査では「医療機関確認用」または「薬局確認用」、「事業者確認用」の全ての項目について、確認日と回答等が記入されていることを確認します（※）。このうち、２-①の台帳、３-①の連絡体制図、３-③の事業継続計画（BCP）、４の規程類は現物を確認しますので、立入検査までに作成してください。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関等は各事業者からチェックリストを回収しておきましょう。

（※）事業者と契約していない場合には、「医療機関確認用」または「薬局確認用」２-②及び２-③についての確認は求められません。

～参考資料～

◇[特集]　小規模医療機関等向けガイダンス

診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する人材が十分に確保できないというケースも多くみられます。本ガイダンスは、小規模医療機関等において、ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示しています。

◇[特集]　医療機関等におけるサイバーセキュリティ

本ガイダンスはサイバーセキュリティに関係する部分を要約し、サイバー攻撃の典型例など具体的な事例などもまとめています。チェックリストを用いた確認と併せてご一読いただき、ぜひサイバーセキュリティに対する理解をさらに深めてください。

※　**厚生労働省 HP「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」に掲載しています。**

サイバーセキュリティ対策チェックリスト

各項目の対応状況を担当部門や事業者に確認して下さい。

「はい・いいえ」を選択し、日付を記入。
「いいえ」を選択した場合は、目標日を記入する。
（令和7年度中にすべて「はい」に〇がつくように取り組む）

*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 （ / ）	（ / ）	

1 -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　体制構築　【医療機関等確認用・事業者確認用】

① 医療情報システム安全管理責任者を設置している。

医療機関において、医療機関の経営層は安全管理を直接実行する医療情報システム安全管理責任者を設置する必要があります。医療情報システム安全管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。情報セキュリティ対策の実効性を確保するために、経営層が医療情報システム安全管理責任者に就くことが望ましいですが、医療機関の規模・組織等によっては企画管理者が兼務することもあります。

また、薬局においては、医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う「企画管理者」や医療情報システムの安全管理を直接実行する「医療情報システム安全管理責任者」（以下併せて「システム管理責任者」という。）や、医療情報システムの実装・運用を担う「システム運用担当者」を設置する必要があります。システム管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。なお、小規模な薬局の場合には、薬局の管理者が、システム管理責任者やシステム運用担当者を兼任する場合があると考えられます。

また、事業者においても医療情報システム等の提供に係る管理責任者を設置する必要があります。

（用語の解説）

企画管理者：医療機関等において医療情報システムの安全管理の実務を担う担当者を指します。

▶経営管理編
3.1.2②
3.2

小規模薬局の場合は、薬局開設者か管理薬剤師で設定してください。

※運用管理規程に記載する必要があります。

2－①★ 【医療情報システムの管理・運用】

サーバ、端末PC、ネットワーク機器の台帳管理を行っている。

① 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。（医療情報システム全般）

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者等は医療機関等で所有する医療情報システムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。また、医療機関等の経営層等は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

（用語の解説）

情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。

（補足）

サーバ、端末 PC、ネットワーク機器のうち、自身の医療機関等で保有するすべての医療情報システムについて台帳管理を行っていれば、「はい」にマルをつけてください。

▶経営管理編
1.2.1
〈管理責任〉②
▶企画管理編
9.1

●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC1	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC1	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

ハードウェアの所在や利用者だけでなく、ソフトウェアのバージョンも台帳で管理してください。

＜具体的な管理方法＞

1. Excel等で機器台帳を作成して管理する
2. IT資産管理ソフトウェアで管理する

２－② 【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）を利用している機器の有無を事業者に確認した。（医療情報システム全般）

② 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。
（医療情報システム全般）

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、企画管理者等に報告する必要があります。そのため、システム運用担当者は、２-①で整理した情報をもとにリモートメンテナンスを利用している機器の有無を事業者に確認し、企画管理者等へ報告してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

システム運用担当者：医療機関等において医療情報システムの実装・運用を担う担当者を指します。

▶企画管理編 9.1
▶システム運用編 10.1

レセコン・電子薬歴以外のシステムや機器（調剤機器、過誤防止システム、電子お薬手帳、会計ソフトなど）もリモートメンテナンス（保守）を利用しているか確認をしてください。

※ベンダーが直接サポートの場合以外に、代理店がサポートする場合もあります。その場合は、その代理店からリモートメンテナンスに関するSDS（次項参照）提出を求めてください。

２－② 【医療情報システムの管理・運用】

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。（医療情報システム全般）

③　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。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。企画管理者等は事業者へ当該医療情報システムに関するMDS/SDS の有無を確認し、事業者から回収してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security：医療情報セキュリティ開示書（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の略称です。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説明の標準的記載方法（書式）を JIRA(一般社団法人 日本画像医療システム工業会)/JAHIS で定めた物で、厚生労働省標準規格として認定されています。製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、医療機関等側において必要な対策の理解を容易にすることなどの用途に用いられることが想定されています。

▶概説編 4.5

「事業者確認用チェックリスト」の提出を求めている事業者に対して、医療情報セキュリティ開示書の提出を求めてください。

MDS＝オンプレシステム
SDS＝クラウドシステム

MDS/SDSは、システムに関するもの以外に、リモートメンテナンスに関するSDSも必要です。リモートメンテナンスをする事業者に対して提出を求めてください。

MDS/SDSを入手したら、内容を確認し、疑義があれば事業者に確認を行ってください（＝リスクコミュニケーション）

2－③ 【医療情報システムの管理・運用】

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。（医療情報システム全般）

③　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。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。企画管理者等は事業者へ当該医療情報システムに関するMDS/SDS の有無を確認し、事業者から回収してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security：医療情報セキュリティ開示書（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の略称です。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説明の標準的記載方法（書式）を JIRA(一般社団法人 日本画像医療システム工業会)/JAHIS で定めた物で、厚生労働省標準規格として認定されています。製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、医療機関等側において必要な対策の理解を容易にすることなどの用途に用いられることが想定されています。

▶概説編 4.5

医療情報セキュリティ開示書（MDS/SDS）は、医療情報サービス提供事業者がどのようにセキュリティを確保しているのかを確認し、必要に応じてユーザー側から改善を求めていくための書面です。
「事業者確認用チェックリスト」の提出を求めている事業者に対して、医療情報セキュリティ開示書の提出を求めてください。

MDS＝オンプレシステム
SDS＝クラウドシステム

MDS/SDSは、システムに関するもの以外に、リモートメンテナンスに関するSDSも必要です。リモートメンテナンスをする事業者に対して提出を求めてください。

MDS/SDSを入手したら、内容を確認し、疑義があれば事業者に確認を行ってください（＝リスクコミュニケーション）

２－③ 【医療情報システムの管理・運用】

サービス事業者による医療情報セキュリティ開示書（SDS）サンプルとチェックポイント

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）			
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。			
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		
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	-

最新版の医療情報システムの安全管理に関するガイドラインに対応しているか確認

「いいえ」「対象外」となっている場合に、問題がないか確認してください

２－④ 【医療情報システムの管理・運用】

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 （医療情報システム全般）

④ 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 （医療情報システム全般）

医療情報システムの利用権限は、医療従事者の資格や医療機関等内の権限規程に応じて設定することが重要です。企画管理者等は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。

特に管理者権限を与えるアカウントは最低限のユーザに付与することを徹底してください。これはサイバー攻撃を受けた際の水平展開を防ぐためです。

利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、所属部署・氏名・ユーザ ID・権限等が想定されます。

▶企画管理編
13④
13.1.3

●利用者 ID 台帳の例

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可

No.	利用者属性	性	名	電話番号	ユーザ ID	説明	権限	状態
001	薬剤師	abc	def	****	abc@def	使用者	Admin	使用可
002	非常勤薬剤師	efg	hij	****	efg@hij	使用者	User	使用可
003	事務	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23 年３月まで）
004	非常勤事務	qrs	tuv	****	qrs@tuv	使用者	User	使用可

各システムごとに確認をしてください。

●管理者権限を付与するアカウントは最低限にすること
×全員が管理者権限
×特別な規定がなく、管理者権限が複数いる
（例：別店舗に移動した管理者がそのまま）

●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設定
×登録薬剤師全員が管理薬剤師と設定
×事務員に薬剤師権限付与

利用者ID台帳は、各システムのユーザー管理画面等で設定・確認してください（立ち入り検査の提出物には含まれていないので、書面での管理は不要）

２－⑤ 【医療情報システムの管理・運用】

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をしている。（医療情報システム全般）

⑤　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をしている。（医療情報システム全般）

企画管理者等は２-④で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。長期間使用されていない等の不要なIDは不正アクセスに利用されるリスクがありますので、適宜削除や無効化をする等の対応をしてください。

▶企画管理編 13⑦

各システムごとに確認をしてください。

退職者、店舗異動した方、長期間使用されていない等の不要なID（アカウント） は不正アクセスに利用されるリスクがありますので、速やかに削除してください。

●退職時の事務処理チェックリストに各システムの「ID削除（非活性化）」処理を加えると漏れが出にくいです。（医療系システムだけでなく、メールや社内チャット等を使用している場合も注意）

利用者IDの使いまわしや、退職者のアカウントを別人がずっと利用し続けるのはもちろんNGです！

2－⑥ 【医療情報システムの管理・運用】
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）

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）

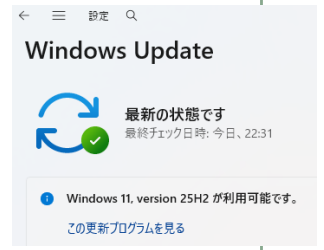
古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

※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）

▶システム運用編
8③
8.1
8.2
13.2

各端末ごとに確認をしてください。

- ☐ 使用しているOSはサポート期限が切れていない
- ☐ OSの更新プログラムを適用している
  （Windows Updateを適用している）
- ☐ アンチウィルス等の不正対策ソフトウェアが最新の状態である。
  （Windows Defender や ESET等）



OS	サポート終了日（Extended Support）	備考
Windows 7 SP1	2020-01-14	ESU適用で2023-01-10まで延長可
Windows 8.1	2023-01-10	Windows 8からの移行対象
Windows 10 (Home/Pro)	2025-10-14	22H2が最終バージョン。サポート終了後はESU登録で2026年10月13日までの1年間（法人・教育向けは最大3年間）セキュリティ更新可（条件あり、新機能・技術支援は対象外）
Windows 11 (Home/Pro)	未定（Modern Lifecycle）	サポート中
Windows Server 2012 / 2012 R2	2023-10-10	ESUで2026-10-13まで延長可
Windows Server 2016	2027-01-12	—
Windows Server 2019	2029-01-09	—
Windows Server 2022	2031-10-14	—

参考：OSサポート終了に伴う主なリスク

1. セキュリティリスクの増大
    1. 脆弱性への対応が停止：新たに発見された脆弱性に対して、セキュリティパッチや更新プログラムが提供されなくなります。
    2. 攻撃対象として狙われやすくなる：サポートが終了したOSは既知の脆弱性が放置されるため、攻撃者にとって格好の標的となります。
    3. セキュリティソフトの非対応化：主要なウイルス対策ソフトやEDR製品が順次サポート対象外となり、防御層が弱体化します。
    4. ネットワーク全体への影響：感染した端末を経由して、同一ネットワーク内の他システム（サーバ・NAS・電子薬歴等）にも被害が波及するおそれがあります。
2. ソフトウェア・アプリケーションの非対応
    1. 最新アプリや業務ソフトが利用不可に：Office、ブラウザ、会計・レセプトソフトなどが新OS専用となり、旧OSではインストールや更新ができなくなります。
    2. 動作不安定・障害発生のリスク：新しいドライバや周辺機器との互換性が保証されず、印刷・スキャン・クラウド同期などで不具合が発生する場合があります。
    3. サポート契約の対象外化：ソフトウェアメーカーやベンダーが旧OS環境での動作保証・問い合わせ対応を打ち切る可能性があります。
3. 法令・コンプライアンス上のリスク
    1. 個人情報保護・セキュリティ規程違反：医療・介護・金融などの分野では、「サポートが継続されているOSを使用すること」が指針・ガイドラインで明記されています。
    2. 監査・認証審査での指摘リスク：ISO27001、医療情報システム安全管理ガイドライン、プライバシーマークなどの審査で不適合と判断される可能性があります。
4. 業務停止・経済的損害のリスク
    1. ランサムウェア感染による業務停止：サポート切れOSは標的となりやすく、感染によりファイル暗号化・業務停止が発生するリスクがあります。
    2. 復旧コスト・信用失墜：システム復旧、データ復旧、被害報告対応などに多大な時間・費用を要し、取引先や利用者からの信頼を損なうおそれがあります。
    3. 医療現場・薬局等での実務影響：調剤システム・電子薬歴・レセプト請求が停止することで、患者対応や請求業務に重大な支障をきたす可能性があります。

２－⑦ 【医療情報システムの管理・運用】
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）

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。

▶システム運用編
8.⑤

●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

使いまわしを回避するパスワードの作成方法
→次ページ以降参照

使いまわしを回避するパスワードの作成方法①

IPA 独立行政法人 情報処理推進機構

IPAについて　お問い合わせ　English　公式S

情報セキュリティ　試験情報　デジタル人材

使い回しを回避するパスワードの作成方法

ここでは、使い回しを回避するパスワードの作成方法の一つを紹介します。

1. コアパスワードの作成

まず、自分の趣味や興味のあることなどから決めた短いフレーズを基に、任意の変換ルールを適用して、憶えやすく、強度の高いパスワードを作成します。これを全てのパスワードに共通して使用する“コアパスワード”とします。

例えば、「テレビが好き」というフレーズを決めた場合、このフレーズをローマ字に変換します。ヘボン式ローマ字で変換すると、「terebigasuki（12文字）」となり、これだけである程度の長さ（桁数）を確保した憶えやすいパスワードが作成できます。

次に、ローマ字に置き換えた文字列の一部を大文字、記号、数字に置き換えたり、数字や記号を追加したりなど、任意の変換ルールを適用します。

図1：コアパスワード作成の例

2. サービス毎に異なるパスワードの作成

次に、サービス名の略称や頭文字、URLの一部などから、サービス毎に任意の短い文字列を決めます。これをサービス毎の識別子として、コアパスワードの前または後に追加します。

2：識別子をコアパスワードの前に追加した例

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

使いまわしを回避するパスワードの作成方法①　つづき

パスワードの管理方法

前述のように作成したコアパスワードと識別子で構成されるパスワードの管理は、コアパスワードのみを暗記し、サービス毎の識別子は電子ファイルや紙で記録します。コアパスワードと識別子は別々に管理されるため、万が一、識別子を記録した電子ファイルの流出や紙を紛失した場合でも、その情報だけでは悪用できず、サービスへの不正利用などの被害にならずに済みます。

図3：紙に記録してパスワードを管理する方法例

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

使いまわしを回避するパスワードの作成方法②

パスワード生成サービスを利用する方法もあります。「パスコード生成」で検索してください。

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

パスワード管理方法の比較表

業務端末・薬局PCでの「パスワードのブラウザ保存」は避けましょう。

業務情報を扱う環境では「パスワード管理ツール or 紙＋鍵付き保管」の組み合わせが望ましいです。

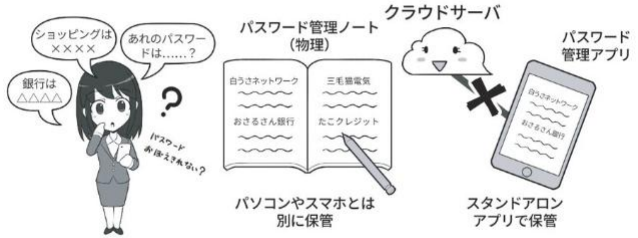
管理方法	メリット	デメリット
自分の頭の中で記憶する	・他者やシステムに依存せず、外部流出リスクが最も低い。・ネットワークを介さないため、サイバー攻撃の影響を受けにくい。	・複雑で長いパスワードを複数記憶するのは現実的に困難。・覚えやすくするために簡単・使い回しのパスワードを設定してしまう傾向。・アカウント数が多い場合は、記憶方式では運用が破綻しやすい。
ノート・紙に手書きで記録する	・NISC（内閣サイバーセキュリティセンター）も一定条件下で推奨しており、オフライン管理として安全性が高い。・サイバー攻撃やマルウェア感染の影響を受けない。・書き残しておけば忘れた場合でも復元可能。	・紙の紛失・盗難・劣化のリスク。・保管場所を物理的に安全にする必要がある（鍵付き引き出し等）。・外出先などで参照が難しく、利便性に欠ける。
Excelやスマホのメモ帳に記録する	・デジタル化により、入力や更新が簡単。・アカウントごとの分類・整理がしやすい。・バックアップも容易。	・端末がウイルス感染や不正アクセスを受けた場合、流出リスクが高い。・ファイル暗号化やパスワード設定を怠ると危険。・クラウド同期設定によっては他端末にもリスクが波及する。
ブラウザに保存する	・自動入力機能によりログインが簡単で利便性が高い。・複数端末での同期が容易。	・ブラウザを狙うマルウェア（情報窃取型）の被害報告が多い。・共有PC・業務端末での利用は重大リスク。・ブラウザの脆弱性やアカウント侵害で一括流出する可能性。
パスワード管理ツール・アプリを使う	・複雑で安全なパスワードを自動生成・自動入力できる。・ゼロ知識暗号化や多要素認証対応のものも多く、安全性が高い。・多数のアカウントを一元管理できる。	・有料版はコストが発生する。・ツール自体が攻撃対象になるリスク（ただし信頼性の高いものは極めて低い）。・複数端末での同期設定やマスターパスワード管理が必要。

※パスワード管理ツールを使う場合の選定基準：AES-256などの暗号化方式を採用していること。多要素認証（MFA）が利用可能であること。クラウド同期時にゼロ知識設計（運営側でも閲覧不能）であること。国内利用者実績・サポート体制があること。

パスワードを使用する場所に置かない。パソコンの中も×

オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。内部の人間が勝手に使うリスクもあります。

パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリのバグや過去のトラブルは、アプリ名＋「トラブル」などで検索します。

NISC（内閣サイバーセキュリティセンター）
「インターネットの安全・安心ハンドブック Ver5.10

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

2－⑧【医療情報システムの管理・運用】

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）

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

各システム・NW機器ごとに確認をしてください。

□ 初期パスワードから変更済みである

□ 各システムやNW機器で別の管理者PWが設定されている

2－⑨ 【医療情報システムの管理・運用】

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

薬局規模に応じた形でリスク対策をすることをお勧めします→

区分	対応方法	対応ツール／具体的手法
① **最低限**（小規模薬局・単独端末想定）	**運用ルールで制限**	- 医療情報を含むファイルをUSBメモリ等で持ち出す行為を原則禁止とする。- 持ち出しが必要な場合は、管理者承認・記録簿（申請書）を必須とする。- 持ち出した媒体は、使用後すぐに返却・破棄を行い、チェックリストに基づいて確認。- 外部PC・私物PCでの利用禁止を明文化。
② **標準**（中規模薬局・複数端末管理）	**端末単位で接続制限設定**	-【無料】Windows 10/11 Proの**グループポリシー**で以下を設定： ・「リムーバブル記憶域へのアクセスを拒否」 ・「特定のデバイスID以外のUSBを無効化」-【有料】セキュリティソフトのデバイス制御機能を利用： ・例：**ESET Endpoint Security**, **Microsoft Defender for Endpoint**, **Trend Micro Apex One** など。- 承認済みUSBメモリのみ使用可とする「ホワイトリスト方式」も有効。
③ **組織的対応**（法人本部・複数拠点運用）	**資産・端末管理ツールで集中管理**	- **SKYSEA Client View**, **Microsoft Intune + Defender for Endpoint**, **LanScope Cat** 等を導入。- 可能な運用： ・端末／媒体単位で接続許可を一元管理（例：薬歴端末はUSB禁止、事務端末のみ限定許可）。 ・利用申請～承認～ログ記録までを自動化。 ・IT資産棚卸機能でUSB機器の接続履歴や不明機器検出。 ・インシデント発生時に即時隔離・調査（感染端末特定、影響範囲分析）。
④ **補足対策（共通）**	**追加的な安全措置**	- **データ暗号化**：持ち出しが必要な場合は暗号化USBを使用（AES256対応、パスワード付）。- **自動検知**：USB接続時に自動通知・ログ送信設定。- **教育・啓発**：年1回以上、職員へのUSB使用禁止ルールの再確認と周知徹底。

２－⑩ 【医療情報システムの管理・運用】

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。

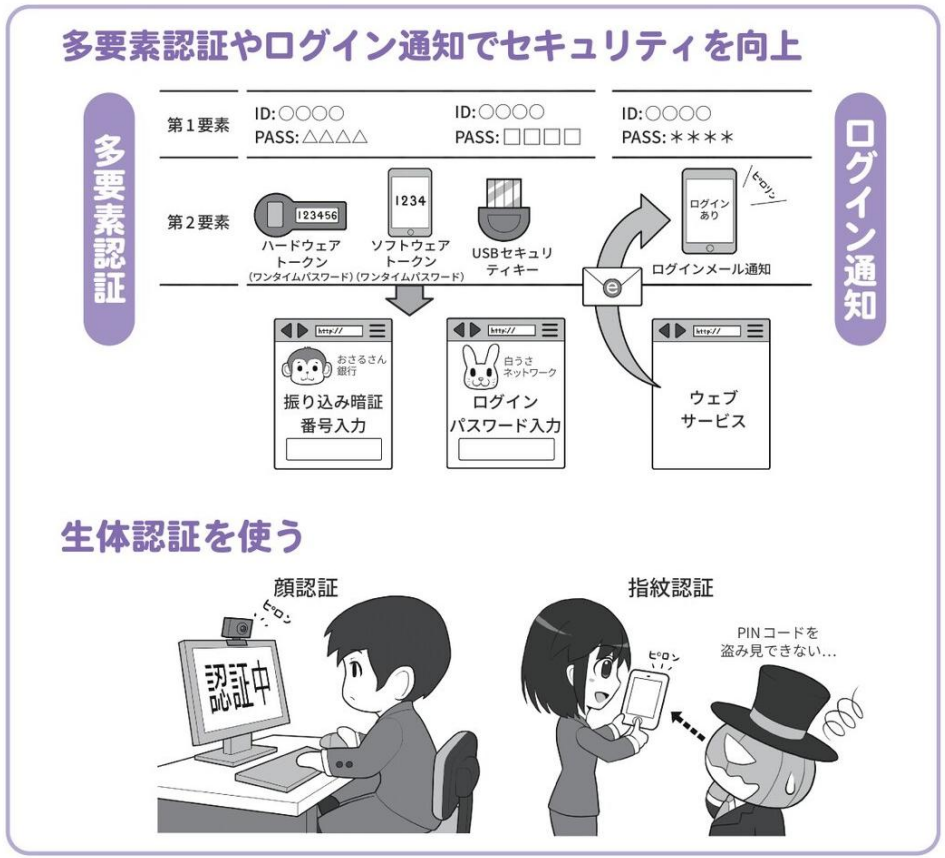
なお、緊急時等で二要素認証が利用できない場合に代替手段を利用する場合には、システム運用担当者等においてシステム及び利用者を適切に管理できる体制を整えておくことが重要である。

●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

医療情報システムに対して「二要素認証」が実装、もしくは実装予定としていることを確認してください。



NISC（内閣サイバーセキュリティセンター）
「インターネットの安全・安心ハンドブック Ver5.10

2－⑪★ 【医療情報システムの管理・運用】
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

各システムごとに確認して下さい

□ アクセスログの管理方法を確認

□ アクセスログを定期的に確認

＜定期的に確認するときのポイント＞

チェック項目	見るポイント	注意する点
1. アクセス日時	いつ誰がアクセスしたかを確認。深夜や休日など、通常利用しない時間帯のアクセスがないか。	見慣れない時間帯の記録はメモしておく。
2. アクセスしたユーザー名／端末	ログに記載されているユーザーIDやパソコン名。知らないユーザーが入っていないか。	共用アカウントを使っていないかも確認。
3. アクセス元の場所（IPアドレス）	通常使っている薬局内・事務所のIPアドレス以外からのアクセスがないか。	見慣れない数字（例：海外のIPなど）は不正の可能性。
4. 失敗したログイン回数	ログイン失敗（パスワード間違い）を繰り返している記録がないか。	何度も失敗している場合は、外部からの攻撃やパスワード共有ミスの可能性。
5. ファイルやデータの操作履歴	重要なデータの削除・変更・ダウンロードなどが記録されていないか。	操作した本人に確認し、不審な場合は管理者へ報告。

２－⑫ 【医療情報システムの管理・運用】

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

サーバ・端末PCごとに、Windowsの設定やタスクマネージャーなどから不要なソフトウェアが動いていないか確認し、不要なソフトウェアがあった場合は停止してください。

Windows 11での「バックグラウンド アプリ」設定方法	操作内容	補足説明・ポイント
① **設定を開く**	スタートボタン → ⚙「設定」をクリックまたは **Windowsキー ＋ I** を押す	「設定」アプリが開きます。
② **アプリ一覧を開く**	左側のメニューから **「アプリ」** を選択	左メニューは青色のアイコン群の中にあります。
③ **「インストール済みアプリ」を開く**	「アプリ」画面の中で **「インストール済みアプリ」** をクリック	PCにインストールされているすべてのアプリが表示されます。
④ **アプリを選ぶ**	一覧から対象のアプリ（例：Teams、OneDriveなど）を探す	アプリの右端にある「：（縦3点）」をクリックします。
⑤ **詳細オプションを開く**	表示されたメニューから **「詳細オプション」** を選択	一部のWindows標準アプリで利用可能です。
⑥ **バックグラウンド実行の設定を変更**	下にスクロールし、「バックグラウンド アプリのアクセス」を探す	「常に許可する」「電源接続時のみ」「許可しない」から選択できます。
⑦ **不要アプリを停止する**	不要なアプリは **「許可しない」** を選択	常駐が止まり、PCの動作が軽くなります。業務アプリは除外します。
⑧ **変更を保存・閉じる**	設定画面を閉じるだけで自動保存されます	再起動は不要です。設定直後から有効になります。

アプリ例	設定	理由
3D Builder 3D ビューアー Cortana	許可しない	医療業務に不要。PC動作を軽くする。
Xbox Game Bar Xbox Console Companion / Xbox Live	許可しない	ゲーム関連機能。不要。
Microsoft News / MSN天気 / スポーツ / マップ	許可しない	通信・更新が多く、業務用途には関係なし。
Groove ミュージック / 映画 & テレビ	許可しない	音楽・動画再生用。薬局端末では不要。

２－⑬ 【医療情報システムの管理・運用】
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

接続元制限例	対策内容
① 管理者パスワードの強化・変更	ルータやアクセスポイントの設定画面に入るためのパスワードを、初期値から強固なものに変更する。
② リモート管理（外部アクセス）を無効化	外部（インターネット）からルータ設定にアクセスできる機能をOFFにする。
③ 無線LANのSSIDを分離（職員用と来客用）	「業務用Wi-Fi」と「来客用Wi-Fi」を分ける。もしくは「来客用Wi-Fi」を設定しない
④ 業務用SSIDの接続パスワード（WPA2/WPA3）を強化	短く簡単なWi-Fiパスワードを使用しない。英数字・記号を混ぜた16文字以上を設定。
⑤ 不要なポート・通信を閉じる（ファイアウォール設定）	一部ルータでは、外部からの通信（ポート）を遮断する設定が可能。薬局でわからない場合は、設置業者に相談。
⑥ 接続履歴（ログ）の確認	どの端末がWi-Fiに接続しているかを定期的に確認。ルータの「接続デバイス一覧」または「ステータス画面」を確認。

ネットワーク機器（ルーター・無線LANアクセスポイント等）の接続元制限を確認してください。

※上記にMACアドレス制限を除外した理由
MACアドレス制限は確かに「登録した機器しか接続できない」ように見えますが、アドレスは簡単に偽装可能（MAC Spoofing）なのと、新しい端末を追加するたびに手動登録が必要（運用負担）で、職員のPCやタブレットが入れ替わるたびに更新が必要という理由から、セキュリティ効果が低く、かつ運用コストが高いため、ここでは除外しています。

３－①★ 【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）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）

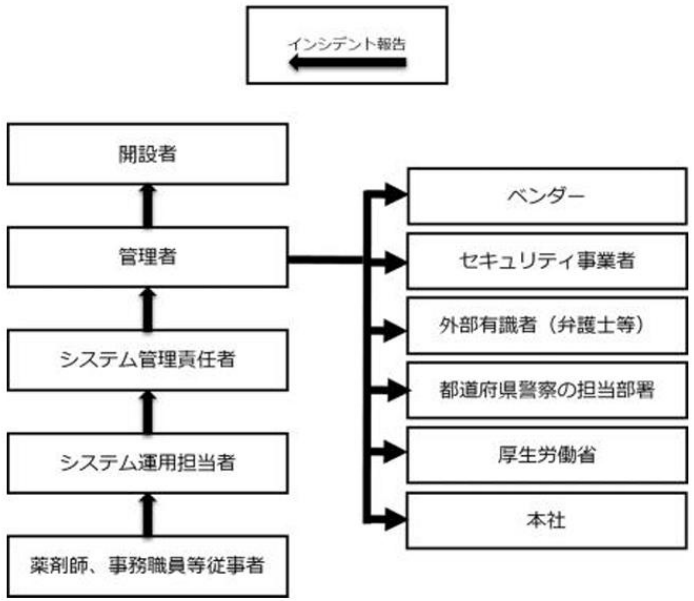
サイバー攻撃を受けた疑いがある場合は、下記の厚生労働省の連絡先に御連絡ください。

【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

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、外部連絡リストを作成してください。

●連絡体制図の例２（薬局）



3－②【インシデント発生に備えた対応】

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

次のことを各システムごとに確認して下さい。

- ☐ インシデント発生時の運用方法
  - ☐ マニュアルの有無
  - ☐ BCPモードへの判断基準と切り替え手順
  - ☐ 運用制限の有無
  - ☐ 復旧手順等
- ☐ オンプレシステムについては、バックアップの世代管理について確認（何世代、保存メディア、保存場所）

近年、大雨による浸水被害を受ける薬局が増えています！
端末の設置場所の見直し（足元に置かない）、PCはリースで購入する等の対策を！

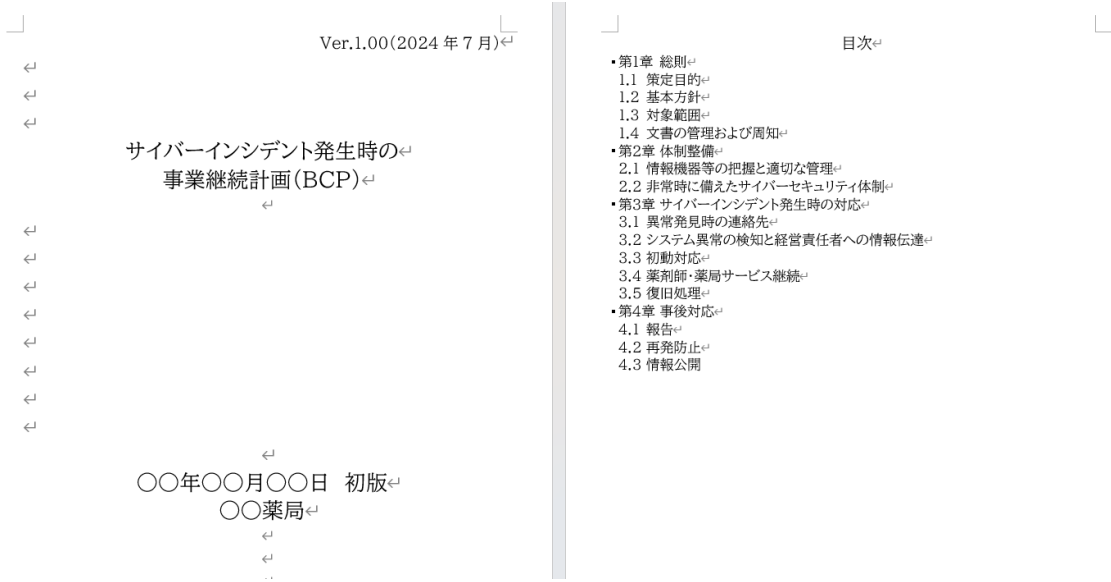
3－③ 【インシデント発生に備えた対応】

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

BCPひな型をベースに作成してください。
日本薬剤師から提供されているひな型
https://www.nichiyaku.or.jp/yakuzaishi/pharmacy-info/cybersecurity

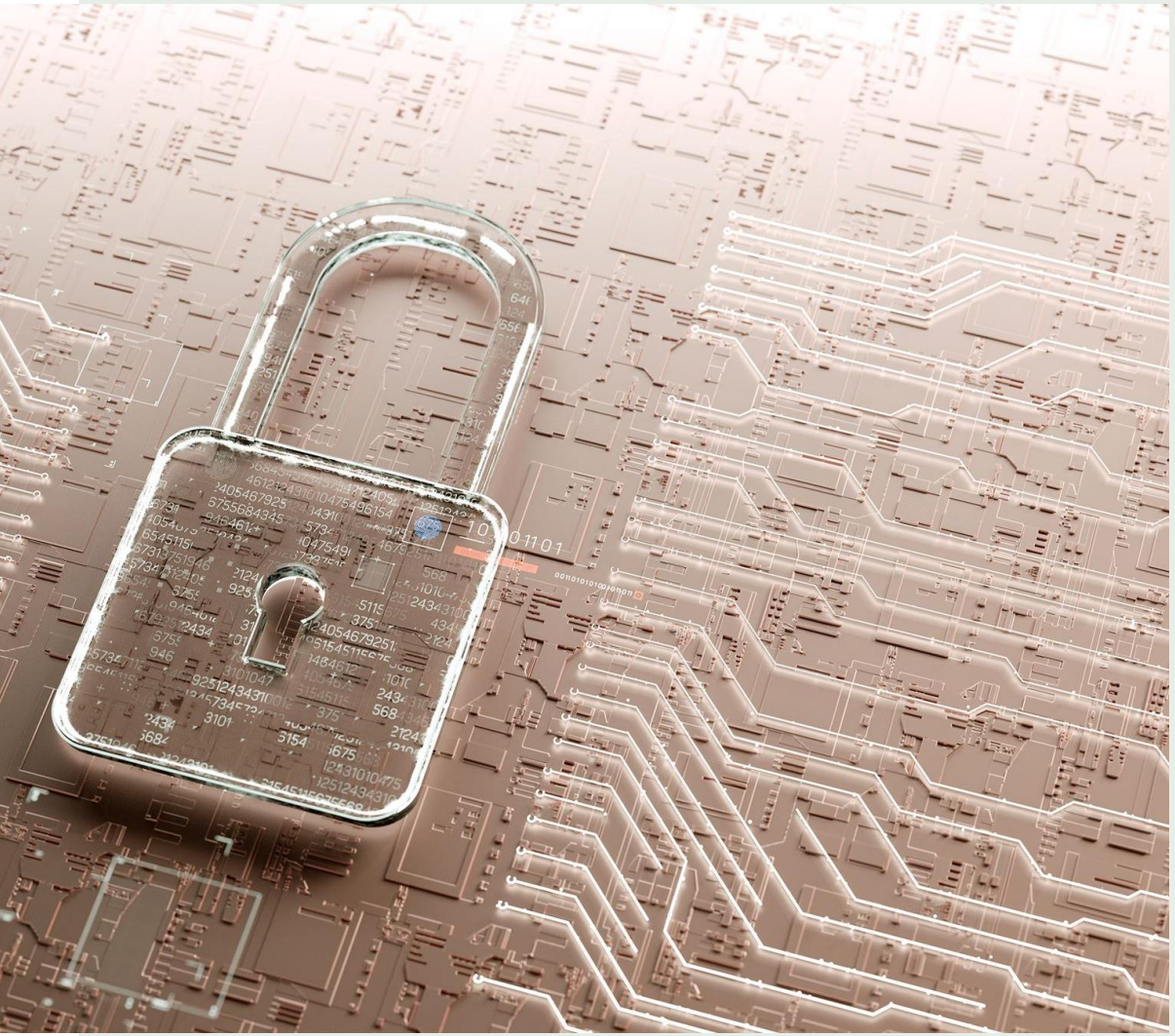


Ver.1.00(2024 年 7 月)

サイバーインシデント発生時の
事業継続計画(BCP)

○○年○○月○○日　初版
○○薬局

目次



サイバーセキュリティ対策まとめ

サイバーセキュリティー対策　難しいところ

1.目に見えない

守るべきものは何か？　敵は誰？　侵入経路は？

3.100%がない

例：OSのセキュリティーパッチ、
時代の変化＝閉域網神話の崩壊、サイバー攻撃手法の変化
リスク分析と費用対効果の検討

３.知識レベル･危機意識がバラバラ

基礎教育からスタートさせる必要
定期的な知識アップデートと対策の継続的実施が必要

サイバーセキュリティー対策　要点

1.見える化

守るべきものの明確化、チェックリスト、定期的な監査、外部コンサル

2.リスク分析・リスクコミュニケーション

リスクの明確化と対策優先順位、コストとベネフィット
規模や実情に応じた現実的な対策

3.役割ごと、知識・危機意識の向上、継続実施

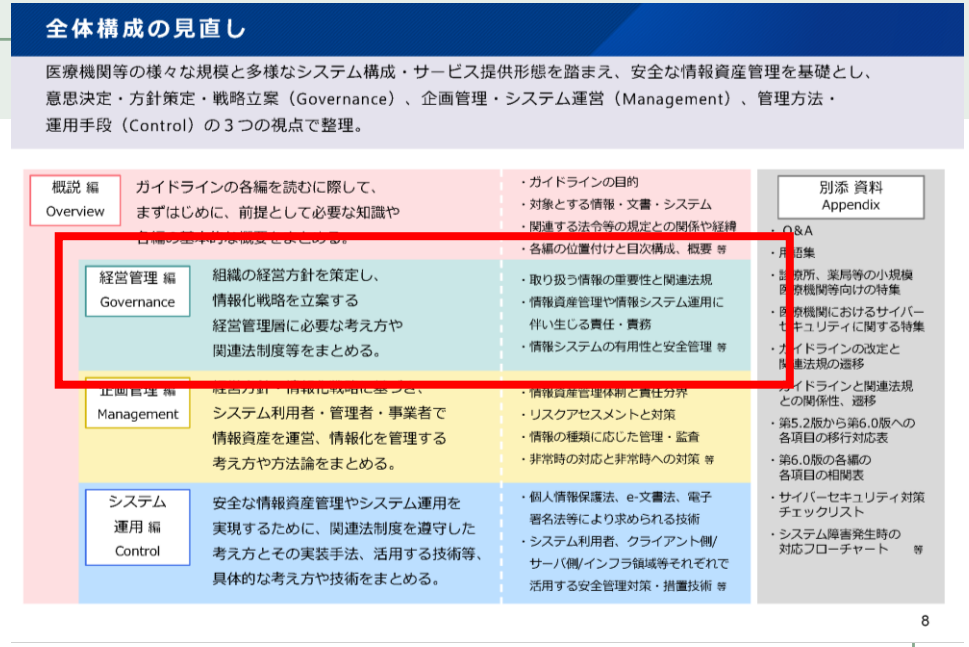
スタッフ・情シス・経営者
Eラーニング等を活用して定期的な知識アップデートと対策の継続的実施、
PDCAサイクルをまわす

経営者の理解と協力が最重要

1. 組織的対策が必要

経営陣がリスク理解

→全従業員がサイバーセキュリティー対策必要との認識



2. 対策に必要なヒト･カネ（ツール）･タイム

セキュリティー対策はタダではできない

3. 適切なインシデント対応

万一のインシデント発生時に被害を最小限に抑える司令塔

インシデントが発生した場合は、経営者に説明責任

サイバーセキュリティー教育支援ポータルサイト（無料）

コース一覧　経営者向け研修

Software Association of Japan

経営者向け研修

階層	コース名	時間	資料ダウンロード	概要
経営者向け研修				
令和5年度 コンテンツ				
	医療現場で考えるべきセキュリティ	約57分	○	経営者にセキュリティの重要性を認識および医療界におけるITガバナンスについて解説。
令和6年度 コンテンツ				
ITガバナンスコース				
	ITガバナンス	約57分	○	ITガバナンスの基本や重要性について解説。
経営者視点コース				
	コンテンツ1	約58分	○	経営者としてサイバーセキュリティを考える重要性を「経営指標」「経営資源の最適配置」の視点で解説。
	コンテンツ2	約57分	○	
経営者向け研修				
IT-BCPコース				
	大規模編	約53分	○	大阪急性期・総合医療センター（大規模病院）におけるIT-BCPの作成や運用状況の事例を紹介。
	中小規模編	約48分	○	つるぎ町立半田病院(中小規模病院)におけるIT-BCPの作成や運用状況の事例を紹介。
令和7年度 コンテンツ （R7年 9月より公開予定）				
経営とレジリエンスコース				
	インシデントによる経営インパクトに基づく対策の力の入れどころ	約60分	○	サイバー攻撃の時系列分析をもとに、急性期の経営影響を踏まえた強靭なシステム構築の重点対策を紹介。
ITガバナンスコース				
	経営者はどこまでセキュリティを理解するべきか	約60分	○	令和6年度のITガバナンス研修を再構成し、経営者向けにリスクとセキュリティの理解ポイントを解説。
IT-BCP組織体制コース				
	IT-BCP 発動時の組織体制について	約60分	○	岡山県精神科医療センターの事例から、IT-BCP発動時の医療継続と復旧体制、連携の仕組みを解説

国家サイバー統括室「みんなで使おうサイバーセキュリティポータルサイト」（無料）

サイバー攻撃はいまもどこかで行われています

サイバー保険

日本薬剤師会　正会員向け保険制度のご案内　2025年加入版

薬剤師賠償責任保険
サイバー保険
New クレーム対応費用保険

加入のご案内

保険期間　2025年2月15日～2026年2月15日

New 2025年2月15日始期契約からweb加入手続きが開始します！

制度の特長　日本薬剤師会のスケールメリットを最大に活用した、正会員だけの補償制度です。

公益社団法人
日本薬剤師会
Japan Pharmaceutical Association

(2) サイバー保険

※加入対象者は薬局契約に準じます。

■なぜサイバー保険が必要？

近年、ICT化の進展に伴い、薬局でも医療機関との情報共有や患者へのオンライン服薬指導、在宅医療にかかわる多職種連携などにおいて、インターネット等のネットワークを通じたコミュニケーションが一般的となっています。また、レセプトコンピューター（レセコン）の他にも、スマートフォンやタブレットなど、薬剤師業務の質的向上や患者へのサービス向上のために使用される機器も多様化しています。一方、医療機関での情報セキュリティ事故も発生しており、不正アクセスを受け個人情報が含まれたメールが流出した可能性があるなどの深刻な事例もあります。多くの個人情報を取り扱う薬局は、狙われやすい業種の一つで、セキュリティ対策を含めたサイバーリスクへの備えが急務となっています。

2022年4月1日施行改正個人情報保護法により、事業者の責務が厳格化され、罰金の強化や漏えい報告の義務化等、規制が更に強化されています。

■対象となる事故

①サイバー攻撃
不正アクセスやDDos攻撃、データの改ざん・破壊など薬局のシステムに対する外部からの攻撃などによる損害

②情報漏えい・おそれ
薬局の業務における情報漏えい、またはそのおそれによる損害

③デジタルコンテンツ不当事由
薬局の業務の一環としてのデジタルコンテンツの提供などによる名誉毀損やプライバシー侵害、著作権侵害などによる損害

④ITユーザー業務による偶然な事由
左記①～③の薬局の業務の一環としてのシステムの所有・使用・管理に起因する偶然な事由による損害
（薬局内でのシステム運用や利用における操作誤り、システムの不具合などの事故をいいます）

※使用人等の犯罪行為・背任行為等に起因して生じた損害も補償します。ただし、犯罪行為や背任行為等を行った使用人等自身の被る損害については補償しません。

■補償の内容

補償内容（対象
第三者に対する賠償責任
● サイバー攻撃、デジタルコンテンツ 不当 ユーザー業務による偶然な事由によっ よって被る、損賠賠償金や訴訟費用など
事故発生時の各種対応費用
● サイバー攻撃の発生および情報漏えい等 費用」「サイバー攻撃対応費用」「情報 4種で、事故調査から解決／再発防止ま

※勤務薬剤師単位でのご加入はできません。
※お支払いの時は縮小てん補割合９０％が適用

緊急時サポート総合サービス（サイバー保険に自動セット）

サイバー攻撃?? 情報漏えい発生?! まず何をすれば良いの？

SNSで炎上！苦情の電話が鳴りやまない… 一体どうしたら？！

誰か相談にのってくれないかしら。でも、信頼できる専門業者はわからないし…

どれだけの対応コストがかかるのか不安…

サイバー保険では、そのような不安や課題を解消する『緊急時サポート総合サービス』が自動セットされています。

損保ジャパンのグループ会社であるSOMPOリスクマネジメント(株)を通じて、緊急時に必要な一連の対応をワンストップで支援します！

『緊急時サポート総合サービス』の主なサポート機能

加入薬局の要請に基づき、下記の機能をSOMPOリスクマネジメント㈱と提携事業者により提供します。
対応にかかる費用は、サイバー保険の保険金としてお支払いします。

コーディネーション機能	調査・応急対応支援機能	緊急時広報支援機能	コールセンター支援機能	信頼回復支援機能
■必要となる各種サポート機能の調整 ■事故対応窓口との連携・アドバイス　など	■事故判定 ■原因究明・影響範囲調査支援 ■被害拡大防止アドバイス　など	■記者会見実施支援 ■報道発表資料のチェックや助言 ■謝罪広告支援 ■事故に関し信用を毀損するSNS投稿などへの対応支援 ■WEBモニタリング・緊急通知　など	■コールセンター立上げ ■コールセンター運営 ■コールセンターのクローズング支援　など	■再発防止策の実施状況について報告書を発行　など

※緊急時サポート総合サービスはサイバー保険で保険金がお支払いできる事故の場合にかぎり、ご利用いただけます。
※緊急時サポート総合サービスは日本国内での対応に限ります。※対応内容によって、全額をサイバー保険の保険金としてお支払いできない場合があります。

今日からできるサイバーセキュリティー対策

1. パスワードの見直し

パスワード設定はできる限り長く、複雑にし、絶対に使い回さないことが重要
Eメールアドレスの他に、ID設定が行える場合は、Eメールアドレスと異なる
多要素認証を使用する

2. 薬局内掲示

厚生労働省からのリーフレット

3. サイバーセキュリティチェックリスト

最低限のすべきことが記載されています

4. 自社HPやメール環境のチェック

地元のITベンダー（大塚商会・キヤノン・リコーなど）に相談してみてください

ご清聴ありがとうございました

日本薬剤師会公式キャラクター

ふぁるみん