

はじめに

本日は、「生成 AI 時代の病院 DX と医療関連サービスの新しい役割」についてお話しします。病院は、医師や看護師だけで動いているわけではありません。事務業務、情報システムなど、多くの医療関連サービスによって、日々の診療が成り立っています。



どれか一つの仕事が滞っても、患者の診療や病院の運営に影響が生じます。医療関連サービスを担う皆さんは、病院の仕事をともに成り立たせている存在です。

その病院の仕事は、いま大きな転換点にあります。

病院では、電子カルテを導入していても、必要な情報を探す、担当者に電話する、紙を運ぶ、別のシステムに同じ内容を入力するといった仕事が残っています。生成 AI は、情報を整理し、文書の下書きを作り、仕事を助けることができます。しかし、情報や仕事が分断されたままでは、AI を導入するだけで病院全体が便利になるわけではありません。

これからの病院では、電子カルテ、部門システム、職員の日常業務、そして医療関連サービスを、必要なときに必要な範囲でつなぐことが重要になります。クラウドネイティブ化や標準 API は、そうした病院を実現するための手段です。

一方で、つながる場所が増えることは、守るべき場所が増えることでもあります。外部からの接続や遠隔保守、職員と事業者の ID、システム間の権限を適切に管理しなければ、病院の診療を支える仕組みが、診療を止める経路にもなり得ます。病院 DX を進めることと、サイバー攻撃や障害が起きても診療が続けられることは、併せて考える必要があります。

本日は、まず「DX は医療現場の仕事をどう変えるか」を取り上げ、病院の情報の流れと職員の仕事の変化を考えます。続いて「生成 AI 時代の病院サイバー対策」を取り上げ、診療停止への経路をどう分断するかを考えます。そのうえで最後に、この二つの変化を踏まえ、医療関連サービス企業に求められる新しい役割をお話しします。

では、最初の問いから始めます。病院 DX とは、何を変えることなのでしょうか。

第 1 部：DX は医療現場の仕事をどう変えるか

— 「つながる病院」 への道 —

はじめに DX とは「仕事を変えること」である

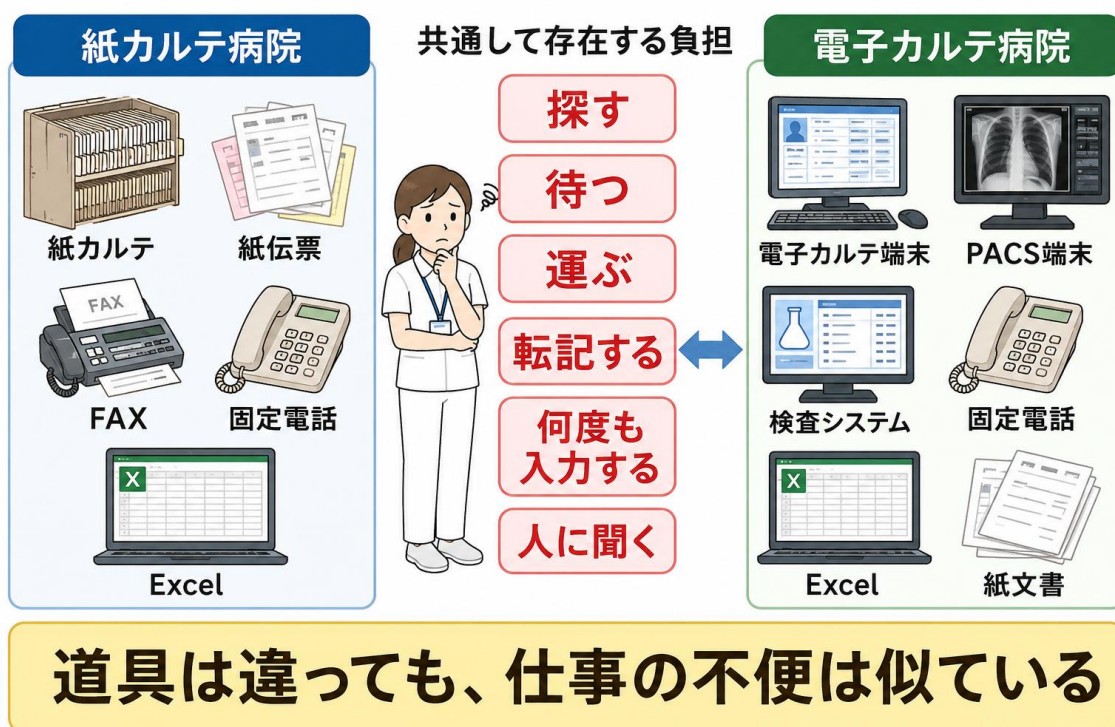
病院では、毎日非常に多くの情報が行き交っている。

患者の診療記録、検査結果、画像、処方、看護記録、リハビリテーション記録、会計情報、勤務情報、物品情報、会議資料など、その種類は多い。病院は、いわば大量の情報を扱う組織である。

ところが、これだけ多くの情報を扱っているにもかかわらず、現在も「人が情報を探す」「人が情報を運ぶ」という仕事が少ない。

紙カルテを使用している病院では、カルテや伝票を運び、必要な書類を探し、同じ情報を複数の帳票に記載することがある。

電子カルテを導入している病院でも事情はそれほど変わらないことがある。電子カルテを見るために PC へ戻る。画像を見るために PACS を開く。別のシステムに同じ情報を入力する。共有フォルダから資料を探す。担当者を探して電話する。電子化されていても、「探す」「待つ」「転記する」といった仕事が残っている。



【図 0-1：紙でも電子でも残っている「病院の不便」】

DX、すなわちデジタルトランスフォーメーションを考えると、最初に理解しておきたいのは、DX とは単なる「紙の電子化」ではないということである。

電子カルテを導入することそのものが DX なのでもない。クラウドを利用すること、スマートフォンを職員に配ること、生成 AI を利用することも、それだけでは DX とはいえない。これらはすべて、仕事を変えるための手段である。

DX の目的は、デジタル技術によって情報の流れを変え、それによって病院で行われている仕事そのものを、よりよい形に作り直すことである。

本書では、紙カルテ病院とオンプレミス型電子カルテを利用している病院の双方を念頭に置きながら、これからの病院情報システムと、そこで働く人の仕事がどのように変わっていくのかを考える。

第1章 スマートフォンではできるのに、なぜ病院ではできないのか

私たちは日常生活の中で、非常に高度な情報サービスを毎日利用している。

例えば、スマートフォン一台から地図を確認し、ホテルや航空券を予約し、支払いを行い、メッセージを送り、外国語を翻訳することができる。必要なサービスを、その都度自然に利用している。

ところが病院では、電子カルテを見るにはこの PC、画像を見るには PACS、勤務表は別のシステム、会議資料は共有フォルダ、連絡は電話、といった状況が珍しくない。



【図 1-1：スマートフォンの世界と病院の世界】

なぜ、このような違いが生まれたのだろうか。

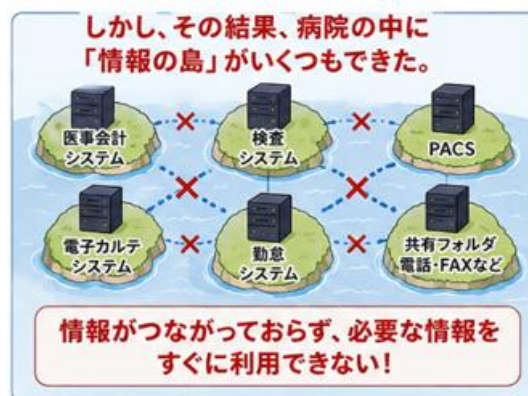
病院情報システムは、長い時間をかけて必要な機能の一つずつ追加する形で発展してきた。医事会計システムが導入され、検査システムが入り、PACS が入り、電子カルテが導入された。その後も、薬剤、リハビリテーション、勤怠、財務など、それぞれの目的に応じたシステムが追加されてきた。

それぞれのシステムには重要な役割があり、その導入自体が間違っていたわけではない。問題は、それぞれが別々に発展してきたことである。

その結果、病院の中にいくつもの「情報の島」ができた。情報が存在していても、必要な人が必要な時に簡単に利用できるとは限らない。

これからの病院情報システムでは、すべてを一つの巨大なシステムに入れるのではなく、それぞれのシステムが得意な役割を担い、必要な時につながるという考え方が重要になる。

 **なぜ、このような違いが生まれたのだろうか。**
大きな理由の一つは、病院情報システムが長年にわたり、必要な機能の一つずつ追加する形で作られてきたことである。



第2章 DXで病院職員の一日はどう変わるのか

「つながる病院」が実現すると、病院職員の仕事はどのように変わるのだろうか。

例えば、看護師が患者のところへ行く前に、手元のスマートフォンでその日の検査予定を確認する。患者から質問を受け、その場で答えられなければ、院内マニュアルを検索する。医師への確認が必要であれば、内線電話で院内を探し回るのではなく、メッセージを送る。患者を検査室へ搬送する必要があるれば搬送担当者へタスクを送り、退院後の病室清掃が必要なら清掃担当へ依頼する。

勤務の最後には、その日の重要事項を AI が整理し、申し送りの下書きを作る。



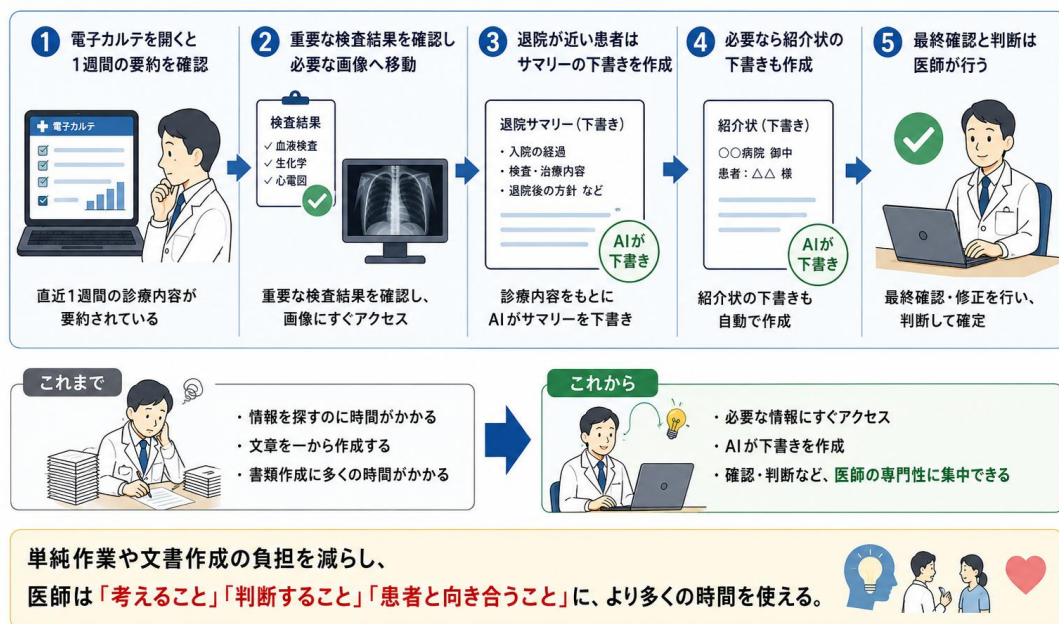
【図 2-1：未来の病院職員の一日】

医師の仕事も変わる。

電子カルテを開いたとき、直近の診療経過が要約されている。重要な検査結果を確認し、必要な画像へ移動する。退院が近い患者については、これまでの診療内容をもとに退院サマリーの下書きが作られる。

もちろん、最終的な確認と判断は医師が行う。しかし、一から情報を探し、一から文章を書く仕事は減らすことができる。

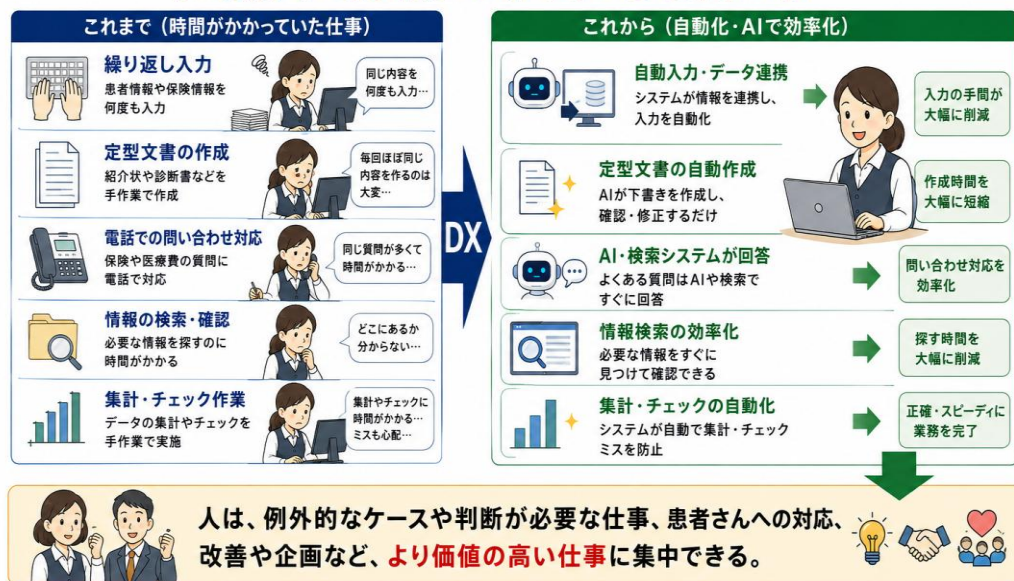
医師の働き方も変わる



医療事務職についても同様である。

繰り返し入力していた作業や定型的な文書作成は自動化され、問い合わせの多い内容は検索システムやAIが回答する。人は、例外的なケース、患者対応、制度判断、業務改善、AIが作成した内容の品質管理など、人でなければ難しい仕事に、より多くの時間を使えるようになる。

医療事務職の仕事も変わる



ここで重要なのは、スマートフォンやAIを導入したことではない。

患者、職員、情報、システム、そして仕事がつながっていることである。

第3章 未来の病院情報システムを3つに分けて考える

これからの病院情報システムを考えると、すべてを「電子カルテ」という一つの言葉で考えない方が分かりやすい。

本書では、病院情報システムを大きく三つの層に分けて考える。

第一層は、**Clinical Core** である。

中心となるのは電子カルテであり、診療記録、処方、指示など、患者を診療するための中核的な情報を扱う。

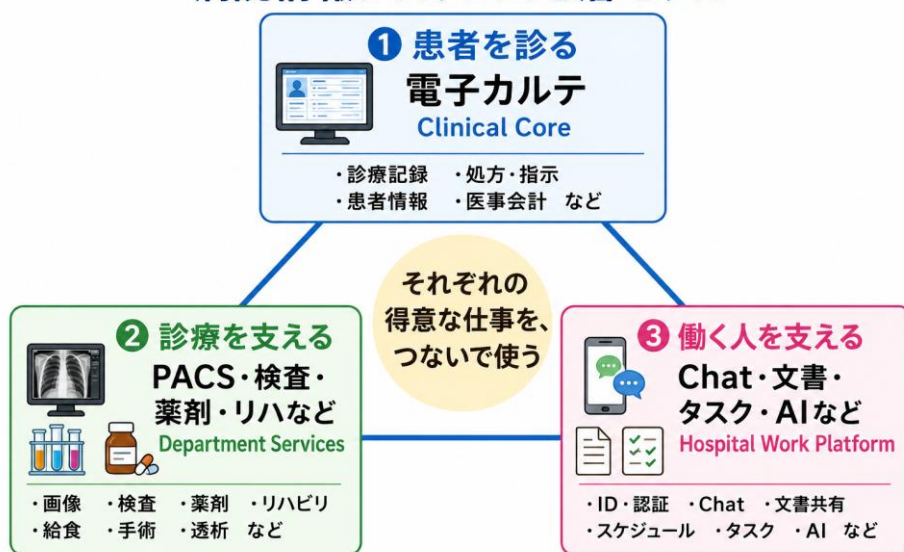
第二層は、**Department Services** である。

PACS、検査、薬剤、リハビリテーションなど、それぞれの専門部門の仕事を支えるシステムである。

第三層は、**Hospital Work Platform** である。

これは、医師、看護師、医療事務職など、病院で働く職員の日常業務を支える情報基盤である。Chat、文書共有、予定、タスク、ワークフロー、スマートフォン、AI などがここに位置する。

病院情報システムの3層モデル



【図 3-1：病院情報システムの3層モデル】

3層モデルで重要なのは、どれか一つを病院情報システムの「中心」にして、すべてをその中に入れようとしめないことである。

電子カルテには電子カルテの得意な仕事がある。PACS や検査システムにも専門的な役割がある。そして、職員間の連絡、文書共有、タスク、AI などは情報基盤の方が得意である。

それぞれのシステムに、それぞれの得意な仕事を任せればよい。

また、「情報基盤」という言葉から、電子カルテに匹敵する大規模な新システムを想像する必要はない。

Google Workspace や Microsoft 365 など、一般企業ですでに広く利用されているクラウドサービスを活用する方法もある。共通の職員 ID と認証を整え、Chat、文書共有、予定表、スマートフォンなどを安全に使えるようにするところから始めることができる。

重要なのは製品名ではなく、職員が共通の環境で情報を共有し、仕事を進められる土台を持つことである。

そして、この三つの層が必要に応じて情報をやり取りできることが、次の課題になる。

第4章 「つながる病院」とはどういうことか——API という共通の接続口

システム同士をつなぐために重要になる考え方が API である。

API という言葉は難しく聞こえるが、ここでは、

「違うシステム同士が情報を受け渡すための、共通の接続口」

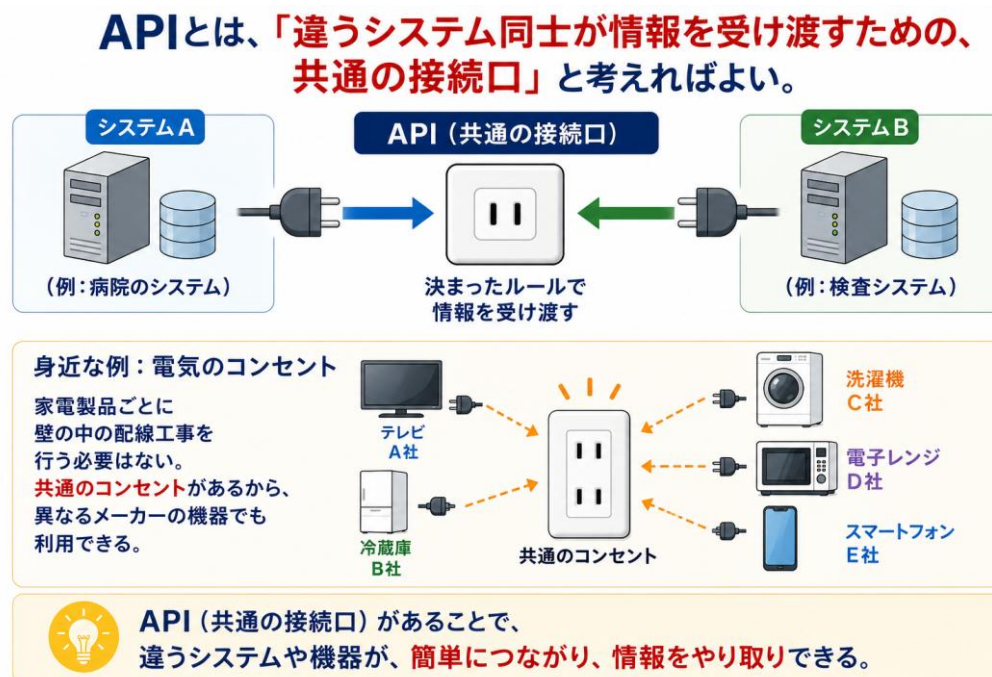
と考えればよい。

身近な例として、電気のコンセントを考えてみよう。家電製品ごとに壁の中の配線工事をする必要がないのは、共通のコンセントがあるからである。

病院情報システムでも、同じ考え方が重要になる。

これまでの病院では、電子カルテと検査、電子カルテと PACS、電子カルテと薬剤というように、システムの組み合わせごとに専用の接続を作ることが多かった。

システムが増えるほど接続は複雑になり、システムを一つ交換しただけでも、多くの接続を作り直さなければならないことがある。



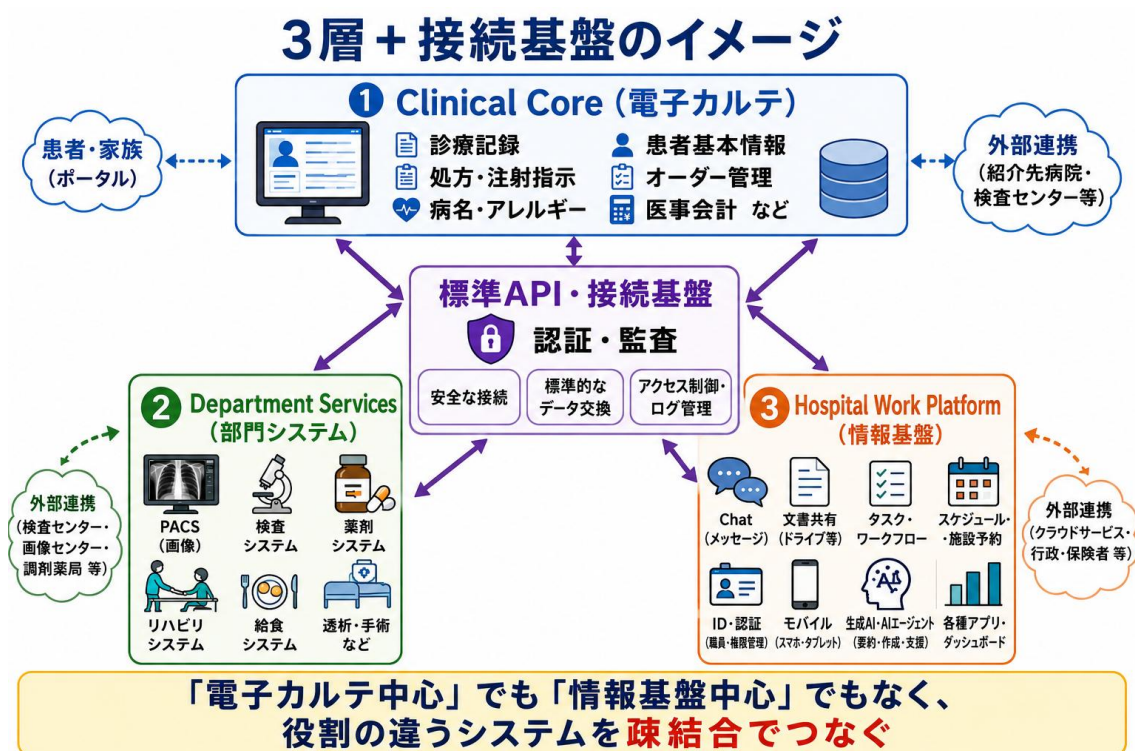
【図 4-1：専用配線から共通の接続口へ】

API を利用すると、各システムがあらかじめ決められた方法で情報をやり取りしやすくなる。

医療分野では FHIR など、医療情報を共通のルールで扱うための標準化も進められている。ただし、3 層の間に巨大な中央システムを置き、すべての情報をそこへ集めるという意味ではない。

Clinical Core、Department Services、Hospital Work Platform がそれぞれ独立した役割を持ちながら、必要な時に必要な情報だけを安全にやり取りする。

これを「疎結合」と呼ぶ。



【図 4-2：3 層 + 接続基盤】

これからシステムを選ぶ際には、現在必要な機能があるかだけでなく、

「将来、他のシステムや AI とつながることができるか」

という視点が重要になる。

第5章 クラウドになると何が変わるのか

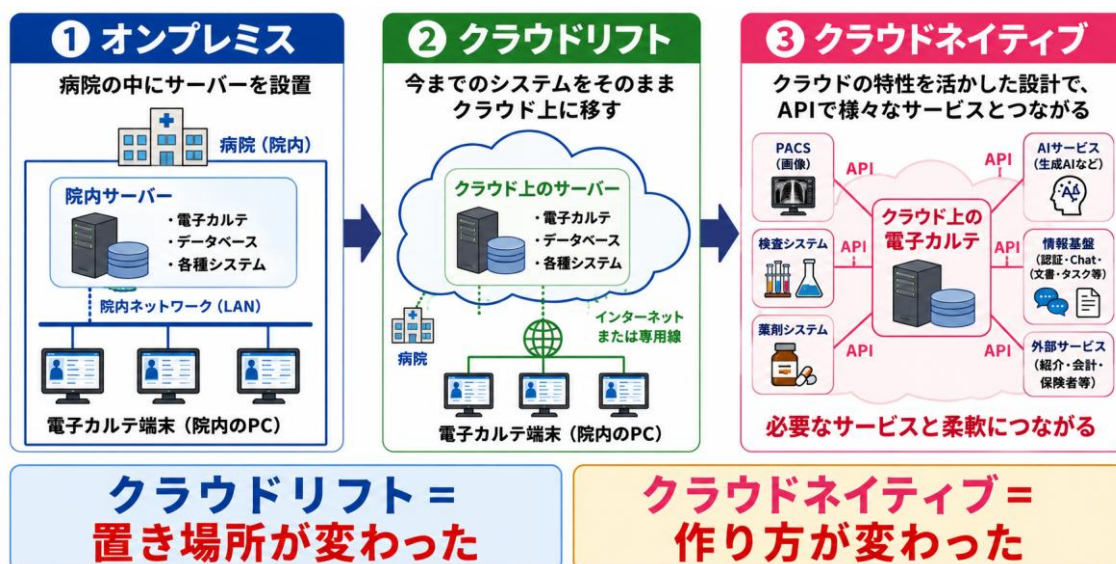
病院情報システムの将来を考えるうえで、「クラウド」という言葉を正しく理解することも重要である。

従来のオンプレミス型では、病院内にサーバーを置き、その病院専用のシステムとして運用する。

これをクラウド上へ移したものが、一般に「クラウドリフト」と呼ばれる方式である。

クラウドリフトでは、サーバーの置き場所は病院からクラウドへ変わる。しかし、システムそのものの基本構造は従来型のままとすることも多い。

これに対して、クラウドネイティブは、最初からクラウド上で利用することを前提として設計されたシステムである。



【図 5-1： オンプレ → クラウドリフト → クラウドネイティブ】

違いを一言で表すなら、

クラウドリフト＝置き場所が変わった

クラウドネイティブ＝作り方が変わった

ということである。

クラウドネイティブなシステムでは、継続的な機能更新、他サービスとの API 連携、AI などの新しいサービスとの接続を行いやすくなる。

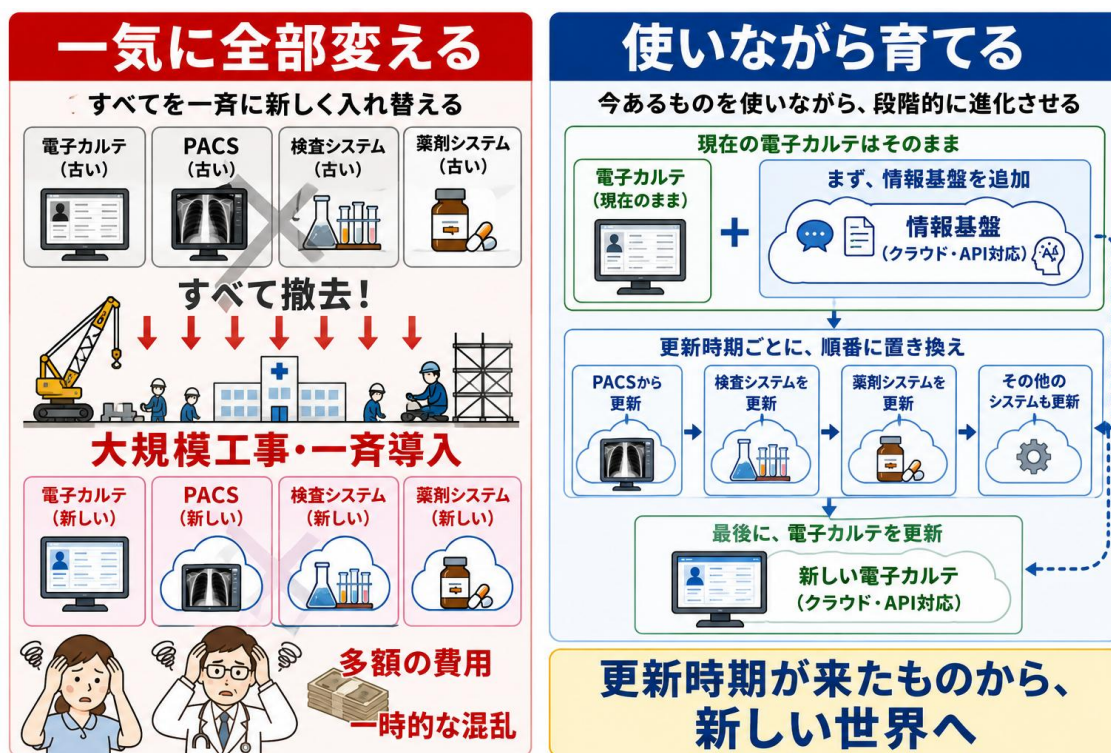
したがって、これから電子カルテや部門システムを選ぶ際には、「クラウドですか」と質問するだけでは不十分である。

API は利用できるのか。データを必要に応じて取り出せるのか。他のサービスと接続できるのか。機能は継続的に更新されるのか。

こうした点まで確認する必要がある。

第 6 章 すべてを一度に入れ替える必要はない

ここまで読むと、「自分たちの病院ではとても無理だ」と感じる人もいるだろう。紙カルテを使用している病院であれば、未来の姿との距離を大きく感じるかもしれない。オンプレミス型電子カルテを導入してまだ数年しか経っていない病院なら、「電子カルテをすぐに入れ替えることなどできない」と考えるのが当然である。しかし、すべてを一度に変える必要はない。



【図 6-1：一気に全部変える DX／育てながら変える DX】

例えば、現在の電子カルテはそのまま使いながら、職員の情報基盤を整える。PACS の更新時期が来たら、クラウドや API に対応した製品を検討する。検査システムの更新時期が来たら、同じ視点で選ぶ。そして電子カルテの更新時期が来たときに、クラウドネイティブ型への移行を検討する。つまり、使えるものは使う。しかし、これから新しく入れるものは、未来につながるものを選ぶ。という考え方である。病院 DX は、一度の大規模更新で完成させるものではない。現在の病院を動かしながら、少しずつ未来の構造へ近づけていく活動である。

第 7 章 今いる場所から、どう未来の病院へ進むのか

病院によって現在地は異なる。

紙カルテを使用している病院もあれば、オンプレミス型電子カルテを使用している病院もある。

したがって、DX への入口も一つではない。

1. 紙カルテ病院の場合

紙カルテ病院が最初に行うべきことは、いきなり電子カルテを購入することではない。

まず、現在どのように情報が動いているかを見える化する。

受付、診察、検査、薬局、会計、病棟などの間で、紙や電話によってどのように情報が運ばれているのかを確認する。

すると、

「なぜ同じことを何度も書いているのか」

「この紙は本当に必要なのか」

「この電話連絡は別の方法にできないか」

といった問題が見えてくる。

そのうえで、職員 ID、認証、Chat、文書共有、スマートフォンなど、電子カルテがなくても整備できる部分から始める。

そして電子カルテを導入するときには、紙の仕事をそのまま画面上に再現するのではなく、転記、紙伝票、電話連絡などを減らせないかを同時に検討する。

紙カルテ病院にとって、新しい電子カルテの導入は大きなチャンスでもある。古い構造を引き継がず、将来つながることを前提とした仕組みを選べるからである。

2. オンプレ電子カルテ病院の場合

オンプレミス型電子カルテを使用している病院では、最初に電子カルテを交換する必要はない。

まず現在のシステム構成を見える化する。

電子カルテ、医事会計、PACS、検査、薬剤、リハビリ、給食、人事、勤怠、財務、共有フォルダなどを並べ、どのようにつながっているのかを確認する。

次に、電子カルテの外側に職員の情報基盤を整える。

その後、既存電子カルテと情報基盤の間で、必要な情報を安全に受け渡す方法を検討する。

部門システムについては、更新時期が来たものから、新しい構造へ移行する。

そして電子カルテの更新時期に、クラウドネイティブ型への移行を検討する。



【図 7-1：二つの入口、一つの未来】

つまり、紙カルテ病院とオンプレ電子カルテ病院では出発点は異なるが、目指す方向は同じである。

つながる 3 層モデルへ、現在地から段階的に近づいていく。

これが現実的な DX の進め方である。

第 8 章 AI が働ける病院をつくる

生成 AI の進歩によって、病院で AI を利用できる場面は急速に増えていくと考えられる。

AI の利用は、大きく三つの段階で考えると分かりやすい。

第一段階は、**探す AI** である。

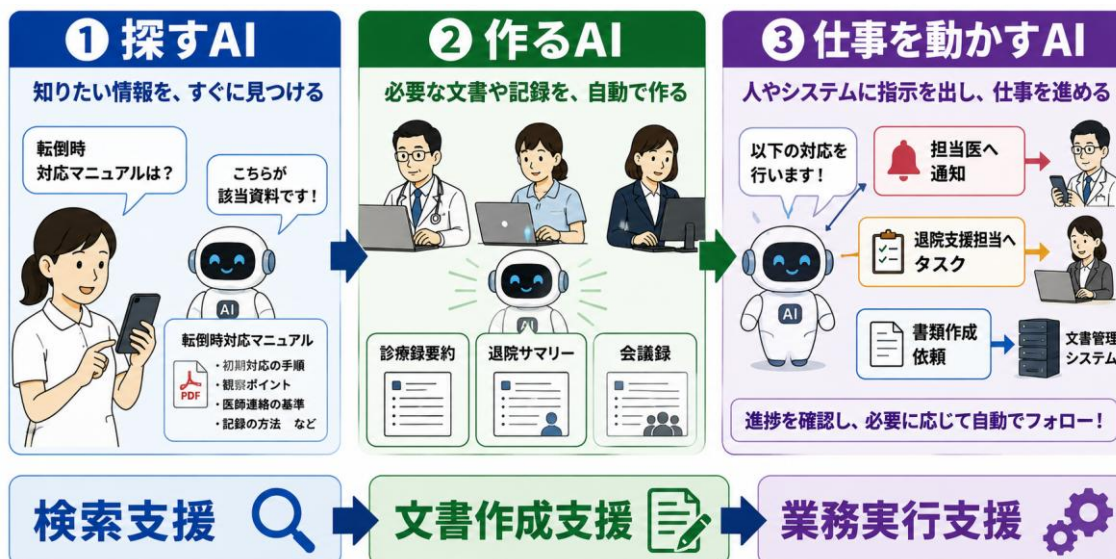
職員が「転倒時の対応マニュアルはどこか」と質問すると、AI が院内資料から必要な情報を探して提示する。

第二段階は、**作る AI** である。

診療録の要約、退院サマリー、紹介状、会議録、説明文書などの下書きを AI が作成し、人が確認する。

第三段階は、**仕事を動かす AI** である。

AI が情報を整理するだけでなく、必要な担当者へ通知する、タスクを作成する、書類作成を依頼するといった業務支援へ進む。



【図 8-1：探す AI → 作る AI → 仕事を動かす AI】

ただし、AI だけを導入しても十分な効果は得られない。

AI が働くためには、必要な情報へ安全にアクセスできること、情報が整理されていること、職員 ID とアクセス権限が管理されていること、誰が何を利用したかを確認できることなどが必要である。

つまり、AI を活用するためにも、これまで説明してきた「つながる情報基盤」が重要になる。

第 9 章 DX は医療事務・記録・情報共有をどう変えるのか

ここまで、DX を支えるシステムの構造を説明してきた。

しかし、DX の目的はシステムを作ることではない。

最終的に重要なのは、現場の仕事がどう変わるかである。

1. 医療事務の変化

これまでの病院事務には、人が情報を入力し、確認し、別の場所へ転記する仕事が多かった。同じ患者情報を複数の画面へ入力する。定型的な文書を作成する。ファイルを探す。問い合わせに答える。

今後、こうした仕事の一部は自動化される。

AI やシステムが入力候補を提示し、人が確認する。定型文書は AI が下書きを作る。院内手続きに関する問い合わせには、AI がマニュアルを参照して回答する。

これは、医療事務職の仕事がなくなるという意味ではない。

むしろ、例外処理、患者対応、制度判断、業務改善、AI が作成した内容の品質管理など、**人の判断が必要な仕事の比重が高まると考えるべきである。**

2. 記録の変化

医療現場では、記録そのものが大きな負担になっている。

患者のところで得た情報を覚えておき、後で PC へ戻って入力する。同じ内容を複数の職種が記録する。

DX が進めば、記録はより「その場」で行われるようになる。

スマートフォンや音声入力などを利用して現場で記録し、AI が文章を整理する。複数の記録から重要事項を抽出し、申し送り用に要約する。

人の役割は、一字一句文章を入力することから、

「内容が正しいかを判断し、必要な情報を確定すること」

へ移っていく。

3. 情報共有の変化

現在の病院では、情報を伝えるために多くの電話が使われている。

電話には優れた点もある。しかし、相手が出られなければ伝わらず、記録も残りにくい。

今後は、Chat、タスク、共有文書、ワークフローなどを目的に応じて使い分けるようになる。

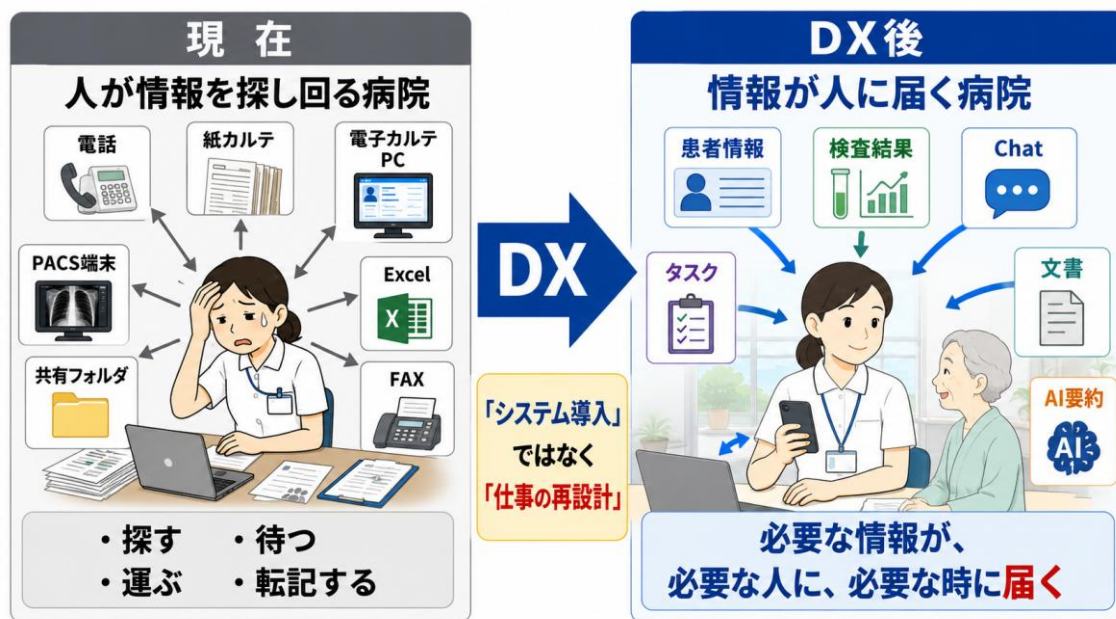
「今すぐ対応してほしい」という緊急連絡と、「今日中に確認してほしい」という仕事の依頼は同じではない。

単に電話を Chat に置き換えるのではなく、

どの情報を、誰に、いつまでに、どの方法で伝えるのか

を再設計する。

これが情報共有の DX である。



【図 9-1：人が情報を探す病院から、情報が人に届く病院へ】

終章 病院 DX の目的は、職員を本来の仕事に戻すことである

DX という言葉から、電子カルテ、クラウド、スマートフォン、AI などの技術を思い浮かべる人は多い。

しかし、本書で繰り返し述べてきたように、それらはすべて手段である。

病院の現場には、

探す。

待つ。

運ぶ。

転記する。

何度も入力する。

人に聞く。

という仕事が数多く残っている。

これらの仕事のすべてに、人が時間を使う必要があるのだろうか。

DX の目的は、こうした仕事をデジタル技術に置き換えることだけではない。情報の流れそのものを見直し、不要な仕事はなくし、必要な仕事はより簡単にし、人にしかできない仕事へ時間を戻すことである。

看護師には、患者と向き合う仕事がある。

医師には、患者の状態を理解し、診断し、治療方針を決める仕事がある。

医療事務職には、患者への対応、制度の判断、例外処理、病院業務を改善する仕事がある。

DX によって目指すべきなのは、こうした**本来、人が行うべき仕事に、職員がより多くの時間を使える病院**である。

そのためには、現在のシステムをすべて捨てる必要はない。

まず、自院で情報がどのように流れているのかを知る。そして、「探す」「待つ」「運ぶ」「転記する」がどこにあるのかを見つける。

今できるところから情報基盤を整える。更新時期が来たシステムについては、将来ほかのシステムとつながるものを選ぶ。電子カルテの更新時期が来れば、クラウドネイティブ型も検討する。そして、AI をその上で利用する。

重要なのは、最初から完成形を作ることではない。

小さく始め、実際に使い、効果を確認、改善し、少しずつ広げていく。

DX は一度きりのシステム更新ではない。

病院が、自分たちの仕事を継続的に見直し、よりよい働き方へ変わり続ける活動である。

そして、その先にあるのが、

「人が情報を探して働く病院」から、「必要な情報が、必要な人に、必要な時に届く病院」への転換
である。

第 1 部のエピローグ

なぜスマホは「イケている」のに、病院情報システムは「イケていない」のか
——巨大プラットフォームから考える、もう一つの病院 DX——

ここまで、病院 DX について、「つながる病院」、病院情報システムの 3 層モデル、情報基盤、API、クラウドネイティブ、生成 AI、そして現在のシステムを使いながら段階的に DX を進める方法について説明してきた。

最後に、少し視点を変えて、これまでの話を一つにつないでみたい。

その出発点は、非常に単純な疑問である。

1. なぜスマホは「イケている」のか

私たちは毎日、スマートフォンを使っている。

目的地を調べる。電車の時間を確認する。ホテルや航空券を予約する。店を探す。支払いをする。写真を撮る。メッセージを送る。外国語を翻訳する。分からないことがあれば生成 AI に質問する。

これだけ多くのことをしているにもかかわらず、利用者はそれぞれの情報システムの存在をほとんど意識していない。

一方、病院では事情が異なる。

電子カルテを見るために PC へ戻る。画像は PACS で確認する。検査結果を見るために別

の画面を開く。勤務表は別のシステムにある。会議資料は共有フォルダから探す。誰かに確認したければ電話をする。

電子化されていても、それぞれのシステムが別々に存在し、人がその間を行き来していることが少なくない。

本編で説明した「情報の島」である。

ここで、改めて一つの問いを考えてみよう。

なぜ、スマホはこれほど「イケている」のに、病院の電子カルテは「イケていない」のだろうか。



【図 E-1：スマホがイケている／電子カルテがイケていない理由】

この違いは、単にスマートフォンの性能が高く、電子カルテの性能が低いから生まれているわけではない。

その答えを考えるためには、スマートフォンの「中」ではなく、その「向こう側」を見る必要がある。

2. スマホの中に、すべてが入っているわけではない

この仕組みを直感的に理解するために、「ドラえものの四次元ポケット」を思い浮かべてみよう。

ドラえもんは、必要になるかもしれない道具をすべて手に持って歩いているわけではない。必要になったときに四次元ポケットに手を入れ、その時に必要な道具を取り出す。

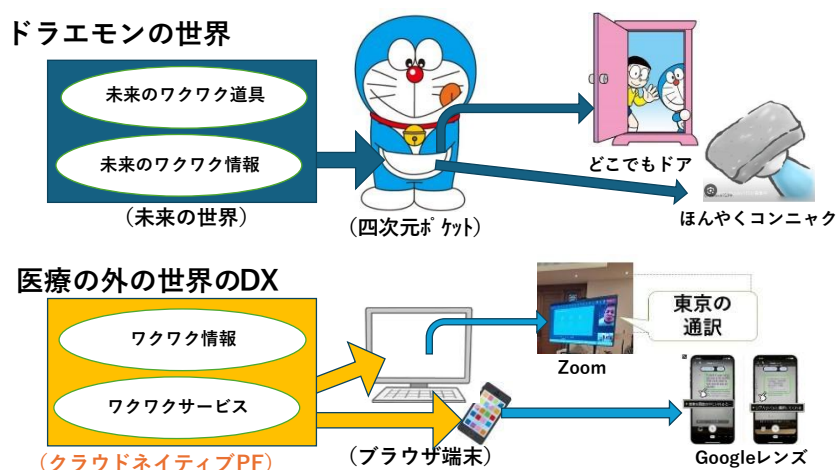
スマートフォンも、これと少し似ている。

スマートフォンの中に、地図会社の巨大なコンピュータが入っているわけではない。ホテル

予約会社のシステムも、銀行の決済システムも、生成 AI を動かす巨大なコンピュータも入っていない。

私たちはブラウザやアプリという「入口」を通して、ネットワークの向こう側にあるさまざまなサービスを利用している。

スマホがイケてる、 電子カルテがイケていない理由



【図 E-2：ドラえもんの四次元ポケットとブラウザ、その向こう側の世界】

つまり、スマートフォンが便利なのは、小さな端末の中にすべての機能を持っているからではない。

スマートフォンが、巨大なデジタルの世界につながっているから便利なのである。

必要な時に地図を使う。必要な時にホテルを予約する。必要な時に決済する。必要な時に生成 AI を呼び出す。

利用者は、それぞれのサービスがどこで動いているのかを意識する必要はない。必要なサービスへ簡単につながり、利用できればよい。

この考え方は、本編で説明してきた病院情報システムの 3 層モデルとも共通している。

すべての機能を一つの巨大な電子カルテの中に入れる必要はない。それぞれのシステムが得意な仕事を担当し、必要な時に安全につながればよいのである。

3. 四次元ポケットの向こう側にある「巨大プラットフォーム」

では、ブラウザという「入口」の向こう側には、どのような世界が広がっているのだろうか。

Google を例に考えてみよう。

Google というと、検索サービスを思い浮かべる人が多いかもしれない。しかし、実際にはその向こうに非常に大きなデジタルの世界が広がっている。

検索やブラウザは、いわばその世界への入口である。その先には、メール、地図、動画、写真、文書、予定表、オンライン会議など、私たちが日常生活や仕事で利用する多くのサービスがある。さらにその奥には、クラウド、データベース、AI、アプリケーション開発などを支える基盤が存在する。

生成 AI を用いて作成した Google の全体像を表す **Google Connected World** では、この Google の世界を、「①エントリー&検索エリア」「②日常アプリ・生活&仕事エリア」「③開発環境・クラウド」という三つの領域として捉えている。



【図 E-3 : Google Connected World／巨大プラットフォームの世界】

このような巨大なデジタル基盤を持っているのは Google だけではない。

Microsoft や Amazon など、それぞれ巨大なクラウド基盤を構築し、その上で多様なサービスを提供している。

ここで重要なのは、どの会社のサービスが優れているかを比較することではない。

情報システムの世界そのものが、

「必要なものをすべて自分で持つ」世界から、

「巨大な共通基盤につながり、必要なサービスを組み合わせて使う」世界へ

変わってきたことである。

スマートフォンは、その巨大な世界への入口として機能している。

だからこそ、小さな一台の端末から、地図、予約、決済、コミュニケーション、AI といった多種多様なサービスを自然に利用することができるのである。

4. 巨大プラットフォームを病院の仕事に持ち込む

では、この巨大プラットフォームの考え方を、病院の仕事に持ち込むことはできないのだろうか。

その分かりやすい例の一つが、Google Workspace である。

Google Workspace には、メール、Chat、文書共有、共同編集、予定表、オンライン会議など、職員が日常の仕事で利用できるさまざまな機能が用意されている。

しかし、ここで注目したいのは、機能の数ではない。

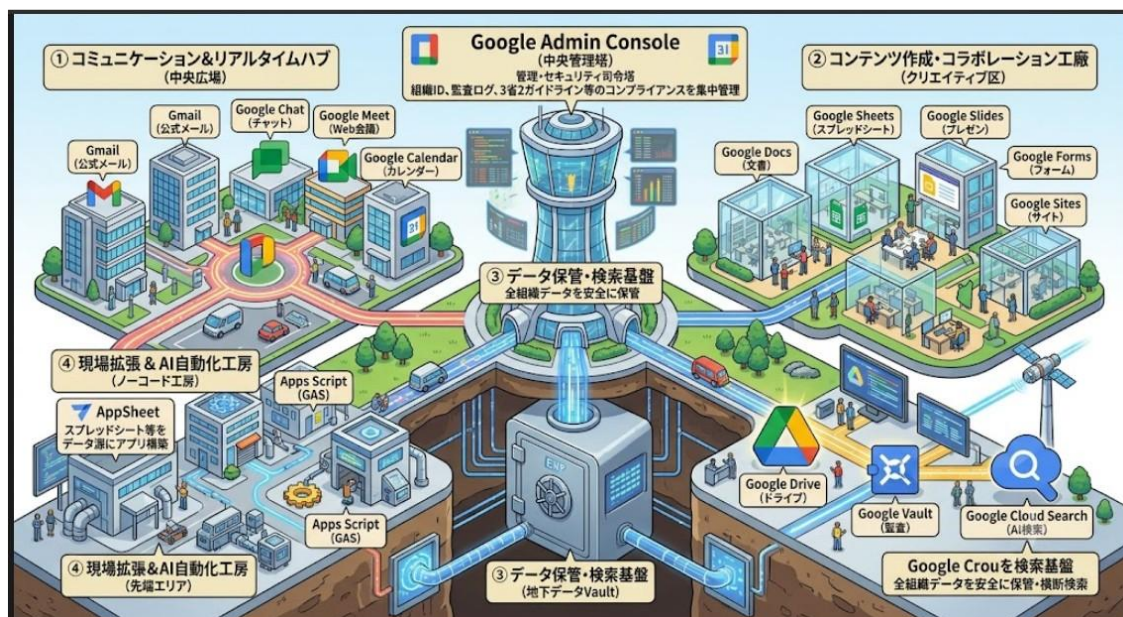
それを使うことで、仕事のやり方を変えられることである。

例えば、医師を探して内線電話を何度もかけていた仕事を、Chat による連絡へ変える。

Excel ファイルをメールに添付して何人もの職員へ送り、修正されたファイルを回収して一つにまとめる仕事を、同じ文書を複数の職員が共同編集する仕事へ変える。

会議資料を個人の PC や共有フォルダの中から探すのではなく、必要な人が共通の場所からアクセスできるようにする。

紙で行っていた申請や確認の一部を、デジタルのワークフローへ変えることもできる。



【図 E-4 : Google Workspace——職員が仕事をするための共通基盤】

本編では、このような職員共通の仕事の土台を「情報基盤」と呼んだ。

ここで大切なのは、「情報基盤」という言葉から、電子カルテに匹敵する巨大なシステムを新しく作らなければならないと考えないことである。

すでに世界で広く使われているクラウドサービスを利用し、共通 ID、認証、Chat、文書共有、スマートフォンなどから始めることができる。

そして、さらに重要なのは、Google Workspace を導入することそのものが DX なのではない、ということである。

従来の仕事をそのまま残して、新しい道具だけを追加しても、仕事はあまり変わらない。電話を減らせないか。紙を回す必要はないか。同じ情報を何度も入力していないか。Excel ファイルを何度も送り合う必要はないか。

共通の基盤を利用することをきっかけとして、それまで当たり前だと思っていた仕事のやり方を見直す。

そこに DX としての意味がある。

5. それは本当に病院でできるのか——京都桂病院から考える

ここまでの話を聞くと、「一般企業ならできるかもしれないが、病院では難しいのではないか」と感じる人もいるだろう。

病院には診療情報があり、安全性や個人情報保護も求められる。24 時間 365 日業務を止めることができず、医師、看護師、医療事務職など、多くの職種が働いている。

そこで具体例として考えたいのが、京都桂病院における取り組みである。

ここで注目すべきなのは、特定の製品を導入したことそのものではない。

Google Workspace をはじめとするクラウド上のサービスやスマートフォンなどを病院の仕事に取り入れ、それまで電話、紙、Excel、個別の仕組みで行われていた仕事を、少しずつ見直していくという考え方である。



【図 E-5 挿入：京都桂病院——巨大プラットフォームを病院の仕事へ】

この事例を、単なる「便利なアプリをたくさん導入した病院」と捉えると、本質を見失う。重要なのは、巨大なプラットフォームの上にすでに存在する共通の機能を利用し、それに合わせて病院の仕事のやり方を変えていくことである。

ここまで来ると、本編で説明してきた病院情報システムの 3 層モデルとの関係も見えてくる。

電子カルテには、診療記録、処方、指示などを扱う Clinical Core としての重要な役割がある。

PACS、検査、薬剤、リハビリテーションなどには、それぞれ専門的な Department Services としての役割がある。

一方、職員同士のコミュニケーション、文書共有、タスク、申請、AI などは、Hospital Work Platform、すなわち職員の情報基盤が得意とする仕事である。

一つのシステムにすべてを抱え込ませる必要はない。

それぞれが得意な仕事を担当し、必要なところを API などにつなぐ。

これは、本編で説明してきた「つながる病院」の考え方そのものである。

そして、もう一つ重要な変化がある。

従来の病院情報化では、「今の仕事のやり方をできるだけ変えず、それにシステムを合わせる」という発想が強かった。

この発想では、病院ごとにカスタマイズを重ねることになる。同じような仕事であっても、病院ごとに違うシステム、違う画面、違う接続が作られやすい。

これに対して、巨大な共通基盤を利用する世界では、発想を少し変える必要がある。

もちろん、医療固有の仕事まで無理に一般企業と同じにする必要はない。診療には診療の専門性があり、安全性や個人情報保護など、医療固有の要件もある。

しかし、連絡、文書共有、予定管理、申請、共同作業など、一般社会と共通する仕事まで、すべて病院独自に作る必要があるのだろうか。

共通化できる部分には、すでに存在する巨大な基盤やサービスを利用する。そして、それに合わせて病院側の仕事も見直す。

医療固有の部分は、電子カルテや専門的な部門システムが担う。それらを API などによって必要に応じてつなぐ。

このように考えると、スマートフォンが「イケている」理由と、これからの病院情報システムが目指す方向が、一本につながって見えてくる。

スマートフォンが「イケている」のは、小さな端末の中にすべての機能を持っているからではない。巨大なデジタルの世界につながり、必要な時に必要なサービスを利用できるからである。

病院情報システムも、その考え方から学ぶことができる。

巨大なクラウド基盤を活用して、人・情報・システム・仕事をつなぎ、それに合わせて仕事のやり方を変える。

これもまた、病院 DX を理解する一つの見方である。

第 2 部；生成 AI 時代の病院のセキュリティ

序章 生成 AI 時代の病院サイバー対策とは何か

0-1 病院サイバー対策は、情報システム部門だけの問題ではない

病院のサイバーセキュリティというと、多くの管理職は「情報システム部門の専門的な仕事」と考えがちである。ウイルス対策ソフトを入れる、ファイアウォールを設置する、パスワードを管理する、VPN を設定する——こうした言葉が並ぶと、医師、看護部長、事務長、部門責任者にとっては、自分の仕事から少し遠い話に見える。

しかし、現在の病院サイバー対策は、単なる情報管理の問題ではない。電子カルテが停止すれば、診療記録の確認、処方、検査依頼、画像参照、入退院管理、手術予定、会計、紹介状作成、退院調整など、診療の多くの場面に影響が及ぶ。救急、透析、手術、抗がん剤治療、精神科医療、入院管理では、情報システムの停止が患者安全に直結する。これは、情報漏えいを超えた診療継続の問題である。

つまり、病院サイバー対策の本質は、コンピュータを守ることではない。患者を守り、診療を守り、地域医療を守ることである。したがって、院長、事務長、看護部長、診療部門長、医療安全担当者、地域連携担当者も、自分ごととして理解する必要がある。

図0-1 情報漏えい対策に加え、診療継続対策へ

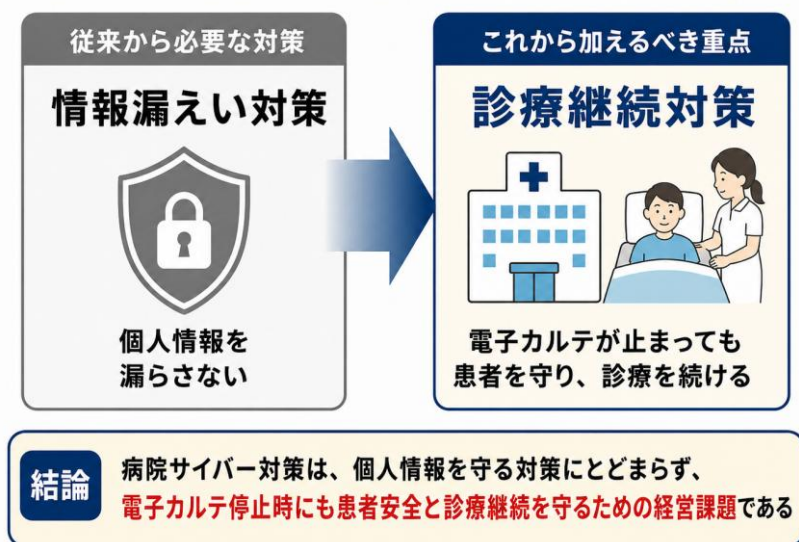


図 0-1 情報漏えい対策に加え、診療継続対策へ

図 0-1 に示すように、従来の病院サイバー対策は「個人情報を守る」「ウイルス感染を防ぐ」という文脈で語られることが多かった。しかし、電子カルテが病院業務の中心になった現在では、それだけでは不十分である。電子カルテ停止は、診療、看護、検査、薬剤、会計、救急、退院調整に波及する。したがって、病院管理職はサイバー対策を「情報シス

テム部門の専門課題」ではなく、「診療継続と患者安全を守る経営課題」として捉える必要がある。

0-2 電子カルテ停止は、病院全体の停止に近づく

紙カルテの時代であれば、カルテ庫から紙を取り出し、医師が記載し、看護師が申し送りを行い、医事課が会計を処理していた。もちろん不便はあったが、業務の多くは人の手で分散していた。

しかし、現在の病院では、電子カルテを中心に、医事会計、検査、画像、薬剤、給食、リハビリ、看護支援、健診、地域連携、退院調整などが結びついている。電子カルテが止まると、単に「記録が見られない」だけではない。処方が出せない、検査依頼ができない、画像が参照できない、病棟で指示が確認できない、会計が進まない、紹介状や診療情報提供書が作れない、という形で病院全体に影響が広がる。

中小病院では、一つの病院が地域の救急、慢性期、在宅支援、施設連携の要を担っていることも多い。その病院が止まることは、地域住民の受療機会を損なうことにつながる。サイバー攻撃は、病院内の情報システム障害で終わらず、地域医療の危機になり得る。

0-3 生成 AI 時代には、攻撃者の探索力が上がる

これまでのサイバー攻撃でも、攻撃者は病院の弱点を探していた。古い VPN、遠隔保守の入口、共有 ID、多要素認証の欠如、バックアップの不備、ネットワーク分離の不足などである。

生成 AI 時代が変わるのは、攻撃者がこうした弱点を探し、整理し、組み合わせる力が高まることである。生成 AI が自動的に病院を攻撃する、という話ではない。問題は、人間の攻撃者が AI を使うことで、探索、文面作成、攻撃経路の検討に要する時間が短くなることである。

従来は、攻撃者が一つひとつ手作業で調べていた弱点を、生成 AI が整理しやすくする。たとえば、「この古い入口」「この認証の弱さ」「このバックアップの弱点」を組み合わせれば、診療停止につながるかもしれない、と検討しやすくなる。生成 AI 時代の脅威は、一つの穴ではなく、複数の穴が連続する経路を短時間で探しやすくなる点にある。

0-4 本書の結論——完全防御ではなく、診療停止への経路を分断する

病院が目指すべきサイバー対策は、「絶対に侵入されない病院」を作ることではない。もちろん侵入を防ぐ努力は必要である。しかし、現実にはすべての攻撃を完全に防ぐことは難しい。

より現実的で重要なのは、侵入されても深く入らせないこと、認証を突破されても権限を広げさせないこと、院内ネットワークを一気に横展開させないこと、バックアップを消されないこと、電子カルテが止まっても診療を続けること、そして早く復旧できることである。

本書の中心メッセージは、次の一文である。

生成 AI 時代の病院サイバー対策は、完全防御ではなく、診療停止に至る経路を分断する多層防御である。

この考え方を、本書では「スイスチーズ型防御」として説明する。すべての穴を塞ぐのではなく、穴が一直線に並ばないようにする。これが、ICT 人材や資金が限られた病院にとって、最も現実的な考え方である。

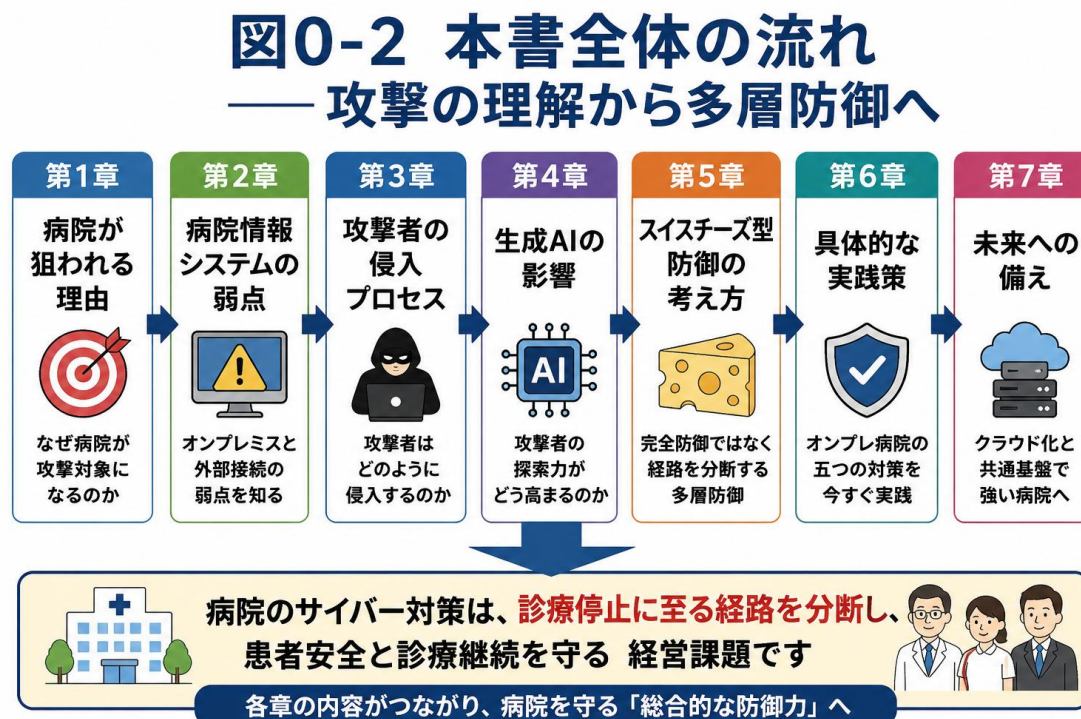


図 0-2 本書全体の流れ——攻撃の理解から多層防御へ

図 0-2 に、本書全体の流れを示す。まず、病院がなぜ狙われるのかを理解する。次に、日本の病院情報システムが抱える「オンプレミス+穴の開いた閉域網」という構造を確認する。そのうえで、攻撃者がどのように侵入し、院内を探索し、診療停止に至らせるのかを学ぶ。さらに、生成 AI が攻撃者の探索力をどう高めるのかを整理し、最後に、スイスチーズ型防御、オンプレミス病院の五つの対策、クラウドネイティブ化、共通接続管理基盤、病院管理職の役割へと進む。

序章のまとめ

病院サイバー対策は、情報システム部門だけの仕事ではない。電子カルテ停止は、患者安全、診療継続、地域医療に影響する。生成 AI 時代には、攻撃者が複数の弱点を短時間で組み合わせる可能性が高まる。したがって、病院は一つの完全な防御壁ではなく、複数の防御層で診療停止への経路を分断する必要がある。

第 1 章 なぜ病院は攻撃者に狙われるのか

1-1 医療情報は、再発行できない情報である

病院が攻撃者に狙われる第一の理由は、医療情報の価値が高いことである。

クレジットカード番号が漏えいした場合、カードを停止し、新しい番号を再発行することができる。もちろん被害は深刻であるが、一定の手続きによって被害を限定できる場合が多い。しかし、医療情報はそうではない。診断名、検査結果、処方歴、手術歴、感染症情報、精神科受診歴、生活習慣、家族構成、保険情報などは、一度漏えいしても「再発行」できない。過去の病気や治療歴を取り消すことはできない。本人の人生に長く関わる情報であり、場合によっては就職、保険加入、人間関係、家族関係にも影響し得る。

図1-1 医療情報は「再発行できない情報」である

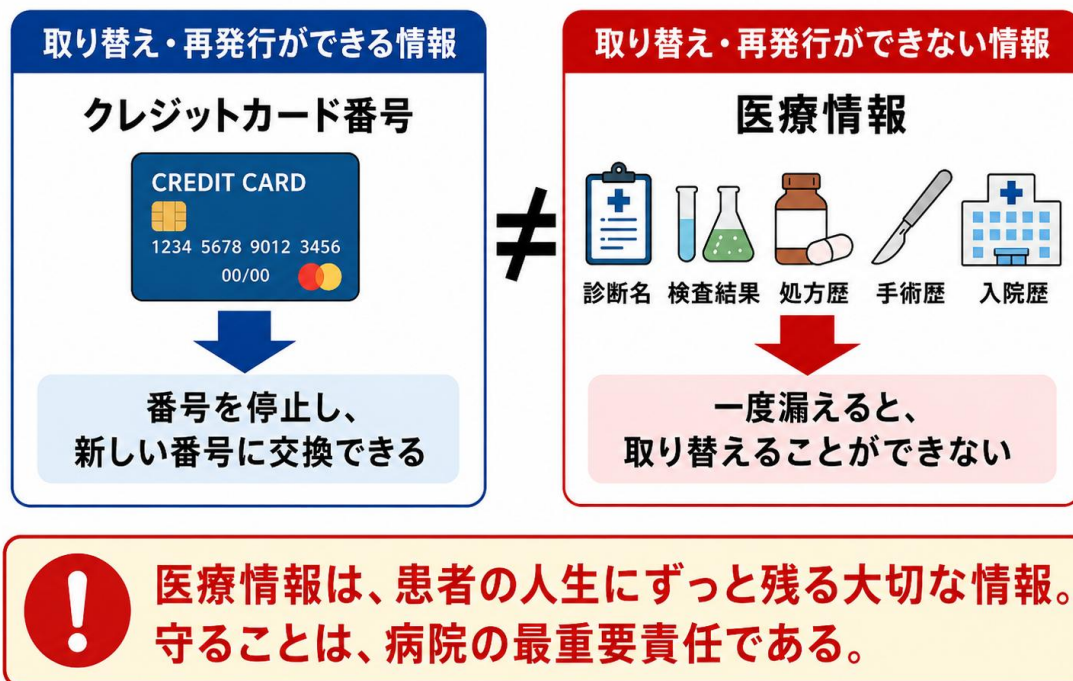


図 1-1 医療情報は「再発行できない情報」である

図 1-1 に示すように、医療情報はクレジットカード番号のように取り替えられる情報ではない。患者本人の人生に長に残る情報である。攻撃者から見ると、医療情報は、単なる住所や電話番号よりも悪用価値が高い。患者本人を脅す材料にもなり得るし、詐欺、なりすまし、闇市場での売買にも使われ得る。病院は、非常に重要で、しかも一度漏れると元に戻しにくい情報を大量に保有している組織なのである。

1-2 電子カルテ停止は、病院全体の停止につながる

病院が狙われる第二の理由は、病院が「止まると困る組織」だからである。

製造業の工場であれば、操業を止めれば大きな損害が出る。銀行のシステムが止まれば、決済や送金に影響が出る。病院の場合は、それに加えて患者の命と安全に直結する。

電子カルテが止まると、医師は過去の診療記録をすぐに確認できない。看護師は指示や観察記録を確認しにくくなる。薬剤部は処方内容の確認に時間がかかる。検査部門、画像部門、リハビリ部門、栄養部門、医事課、地域連携室にも影響が広がる。

図1-2 電子カルテ停止が病院全体に波及する流れ



図 1-2 電子カルテ停止が病院全体に波及する流れ

図 1-2 に示すように、電子カルテ停止は一部門の問題では終わらない。診療記録が見られない、処方が出せない、検査依頼ができない、画像が見られない、看護指示が確認できない、会計が止まる、紹介状・退院調整が遅れる、救急受入判断に影響する、という形で病院全体に波及する。

特に救急医療では、過去の病歴、アレルギー、内服薬、検査結果を確認できないことが、判断の遅れにつながる。入院医療では、指示、処方、検査、看護記録が見られないことが、患者安全上のリスクになる。

攻撃者は、この弱さを知っている。病院は止まると困る。だからこそ、攻撃者は身代金要求や脅迫の対象にしやすい。

1-3 中小病院は、防御投資に限界がある

病院が狙われる第三の理由は、防御投資が難しいことである。

大企業や金融機関であれば、専門のセキュリティ部門を置き、24 時間監視し、高度な対策機器を導入し、外部専門家とも継続契約を結ぶことができる。しかし、多くの病院、特に中小病院では、情報システム担当者が一人、あるいは兼務であることも少なくない。専門部署がない病院もある。

病院経営は、人件費、電気料金、医薬品費、建物老朽化、医師・看護師不足、診療報酬改定への対応など、多くの課題を抱えている。その中で、サイバーセキュリティに十分な予算を割くことは容易ではない。

攻撃者から見ると、病院は「重要情報を持ち、止まると困り、しかも守りが薄い可能性がある組織」である。この三つが重なることが、病院を攻撃対象にしやすくしている。

図1-3 病院が狙われる三つの理由

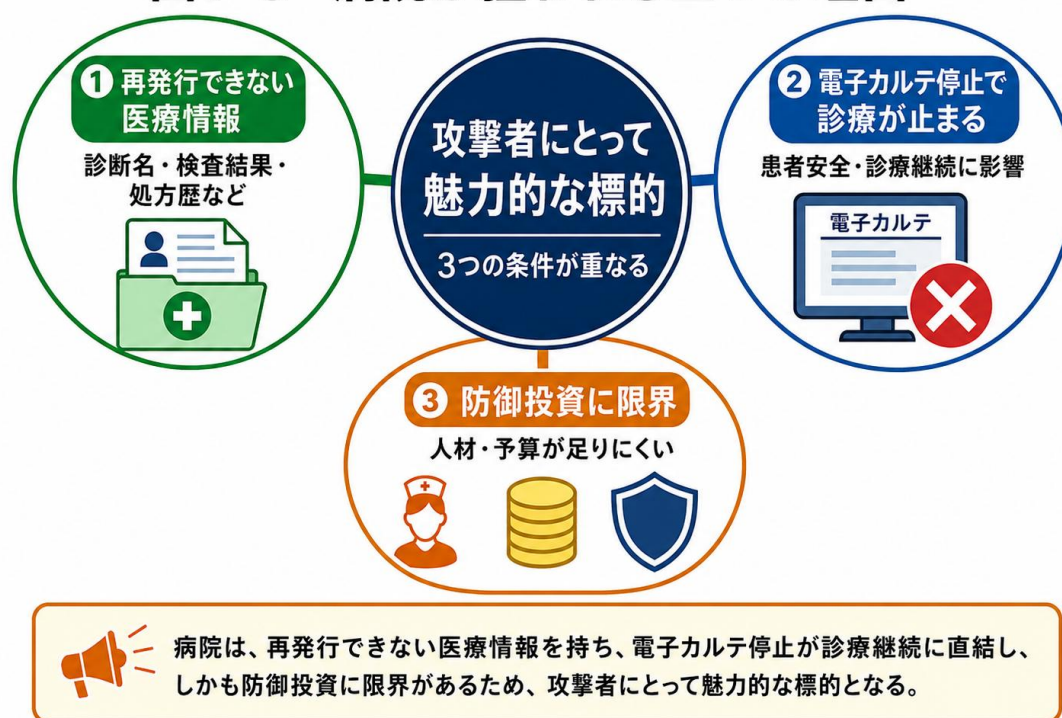


図 1-3 病院が狙われる三つの理由

図 1-3 に示すように、病院が狙われる理由は、医療情報の価値、診療停止への弱さ、防御投資の難しさの三つに整理できる。重要なのは、この三つが別々に存在するのではなく、同時に重なっていることである。病院は、高価値の情報を持ち、止まると患者安全に影響し、しかも十分な防御投資が難しい。攻撃者から見れば、これは極めて狙いやすい条件である。

1-4 攻撃者は、特定病院だけでなく、弱点のある病院を自動探索する

病院管理職の中には、「うちは有名病院ではないから狙われない」「地方の中小病院だから大丈夫」と考える人がいる。しかし、この考え方は現在の攻撃の実態に合わない。

攻撃者は、必ずしも最初から特定の病院名を決めて攻撃するわけではない。インターネットにつながっている機器やサービスを広く探索し、古い機器、設定不備、未修正の脆弱性、常時開放された保守口などを探す。見つけた入口から侵入を試み、侵入できた組織について内部を調べ、さらに深い攻撃へ進む。

これは、泥棒が特定の家だけを狙うのではなく、街を歩きながら鍵のかかっていない窓や壊れた裏口を探すようなものである。病院の規模や知名度ではなく、「外から見える弱点があるかどうか」が重要になる。

したがって、「自院は狙われない」という前提は捨てるべきである。ネットワークにつながっている以上、すべての病院が攻撃候補になり得る。

1-5 病院管理職に必要な発想転換

病院管理職に必要なのは、専門的な技術をすべて理解することではない。自院がなぜ狙われるのか、どのような停止リスクがあるのか、どこから対策を始めるべきかを理解し、優先順位を決めることである。

ここで重要なのは、「うちは狙われない」という発想から、「狙われても診療停止に至らせない」という発想へ転換することである。侵入を完全にゼロにすることは難しくても、診療停止に至る経路を途中で分断することはできる。そのためには、次章で述べる日本の病院情報システムの構造を理解する必要がある。

第1章のまとめ

病院は、再発行できない医療情報を保有し、電子カルテ停止が患者安全と診療継続に直結し、さらに防御投資が難しいため、攻撃者に狙われやすい。中小病院や地方病院であっても、インターネットにつながっている以上、攻撃候補になり得る。病院管理職は、「うちは狙われない」という発想から、「狙われても診療停止に至らせない」という発想へ転換する必要がある。

第 2 章 日本の病院情報システムの弱点

——オンプレミス+穴の開いた閉域網——

2-1 20 年前は、閉域網という発想に合理性があった

日本の病院情報システムは、長い間、「閉域網」という考え方で守られてきた。閉域網とは、病院情報システムをインターネットから切り離し、外部から直接入れないようにする考え方である。

20 年前であれば、この考え方には十分な合理性があった。電子カルテ、医事会計、検査、画像などを院内ネットワークの中に置き、インターネットと接続しなければ、外部からウイルスや攻撃者が入りにくい。病院情報システムの利用範囲も院内中心であり、外部とのリアルタイム連携は現在ほど多くなかった。

つまり、当時の閉域網は、「病院情報システムを外の危険な世界から離して守る」という、分かりやすく合理的な仕組みだった。閉域網は「インターネットから閉ざされたネットワーク」として説明できる。

図2-1 20年前なら合理的だった閉域網

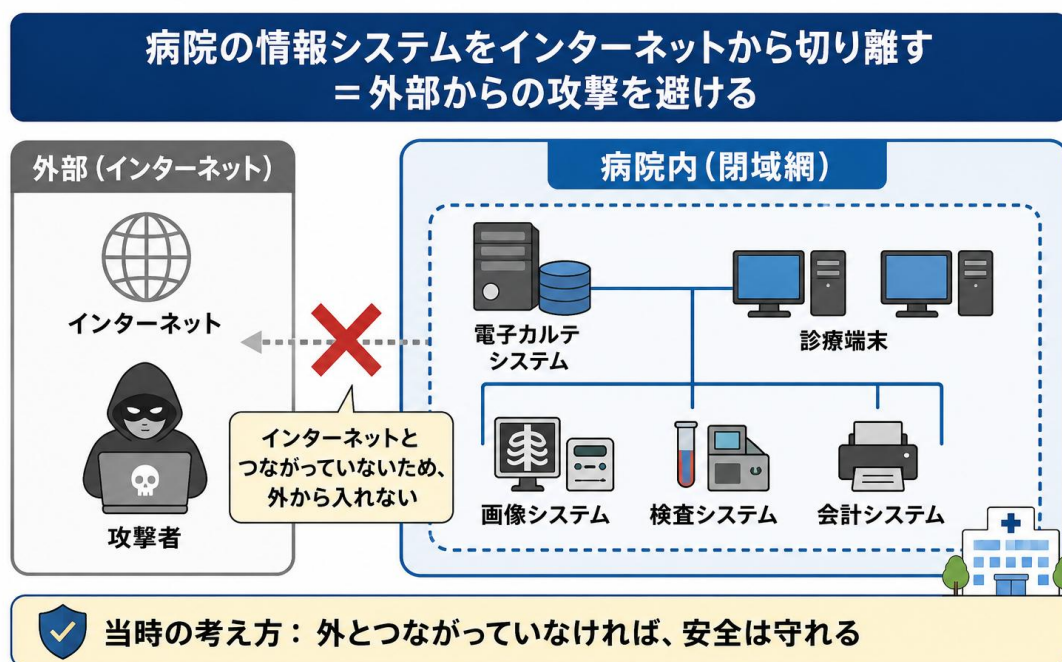


図 2-1 20 年前なら合理的だった閉域網

図 2-1 に示すように、閉域網は、病院情報システムを外部のインターネットから切り離すことで安全を確保しようとする考え方である。インターネット上にウイルスや攻撃者がいるとしても、病院情報システムがそこにつながっていなければ、侵入されにくい。20 年前の病院情報システムでは、この発想は合理的であった。

2-2 医療 DX により、閉域網に多くの「穴」が開いた

しかし、現在の病院情報システムは、20 年前とは大きく変わった。

オンライン資格確認、レセプト関連業務の電子化、電子処方箋、地域医療連携、外部ベンダーによる遠隔保守、検査会社との連携、クラウドサービスの利用、医療データの二次利用など、病院情報システムは外部との接続を必要とするようになった。

ここで問題になるのは、見かけ上は閉域網であっても、実際には外部接続の入口がいくつも存在することである。ベンダー保守用 VPN、リモートデスクトップ、外部公開サーバー、部門システムの保守口、クラウド管理画面などである。

図2-2 医療DXで閉域網に開いた複数の穴

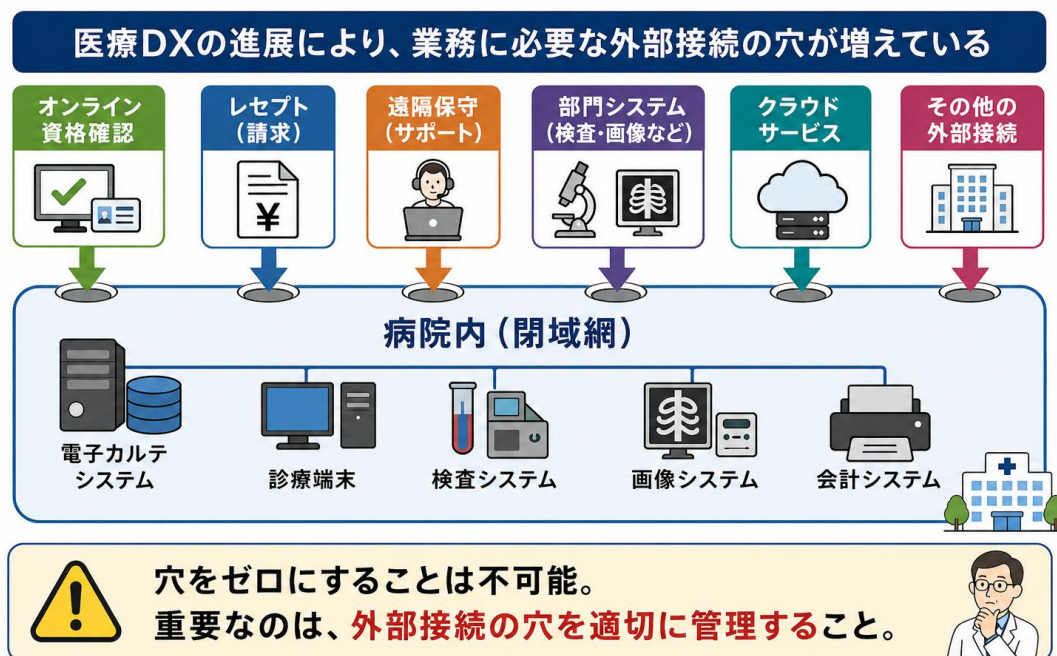


図 2-2 医療 DX で閉域網に開いた複数の穴

図 2-2 に示すように、医療 DX が進むほど、病院情報システムは外部との接続を必要とする。これは悪いことではない。オンライン資格確認も、レセプト電子化も、遠隔保守も、地域医療連携も、医療の効率化や質の向上に必要な仕組みである。

問題は、これらの接続が「どこにあり、誰が管理し、どのような認証で守られ、いつ使われ、記録が残っているのか」が十分に把握されていない場合である。城の正面玄関を閉めていても、裏口、通用門、搬入口、地下通路、業者専用入口が管理されていなければ、そこから侵入される。

2-3 「電子カルテ端末からネットを見られない」ことと「安全」は別である

病院ではよく、「電子カルテ端末からインターネットは見られないので安全です」と説明されることがある。しかし、この説明は不十分である。

電子カルテ端末から職員がインターネット検索やメールを使えないことと、病院情報システム全体が外部から安全であることは同じではない。たとえ職員端末からインターネットを見られなくても、オンライン資格確認、レセプト、遠隔保守、部門システム接続などを通じて、病院情報システムは外部と何らかの形でつながっている場合が多い。

この状態を「オンプレミス+穴の開いた閉域網」と表現できる。電子カルテ用端末から利用者がインターネットを利用できないにもかかわらず、病院情報システムがウイルス感染の危機にさらされる、という問題である。

図2-3 オンプレミス+穴の開いた閉域網

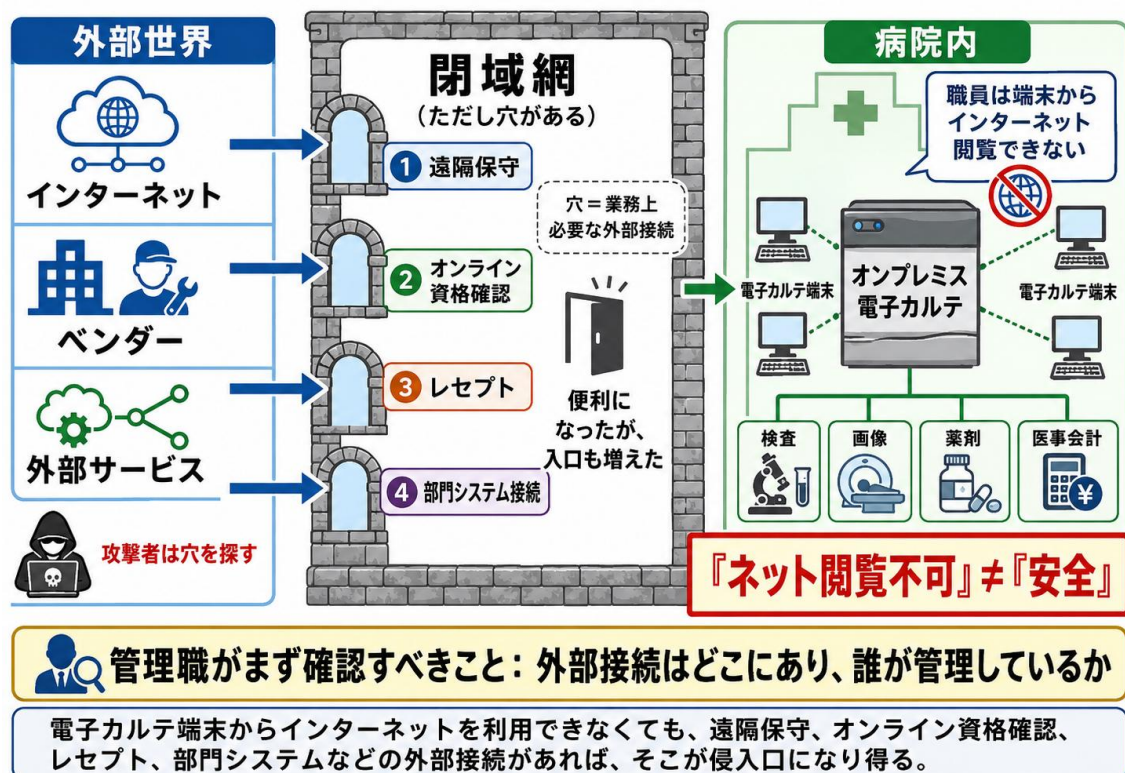


図 2-3 オンプレミス+穴の開いた閉域網

図 2-3 に示すように、病院情報システムの安全性を考えるとときには、「電子カルテ端末からインターネットが見られるかどうか」だけを見てはいけない。重要なのは、病院情報システム全体として、どこに外部接続の穴があるかである。

管理職が確認すべき問いは、次のように変わる。

「うちは閉域網ですか」ではない。

「外部接続はどこにありますか」

「誰が管理していますか」

「多要素認証はありますか」

「不要な保守口は開いたままになっていませんか」

「接続記録は残っていますか」

「緊急時に遮断できますか」

この問いに答えられない場合、閉域網であることを理由に安心することはできない。

2-4 オンプレミス病院の構造的弱点

オンプレミス型とは、電子カルテなどの主要サーバーやソフトウェアを病院内に設置し、病院または委託先が運用・保守する方式である。

オンプレミス型の問題は、院内のサーバー、端末、部門システム、バックアップが、一定の範囲で同じ病院内ネットワークに存在することである。もし外部接続の穴から攻撃者が侵入し、院内ネットワークの中で横に広がることができれば、電子カルテ、医事会計、検査、画像、薬剤、バックアップなどに被害が及ぶ可能性がある。

特に危険なのは、バックアップが本番システムと近い場所、同じネットワーク、同じ認証基盤の下に置かれている場合である。攻撃者が本番システムとバックアップを同時に暗号化・削除すれば、病院は復旧手段を失う。

閉域網に見えるが、実際には穴があり、しかも侵入後に院内で広がりやすい。これが、オンプレミス型病院の構造的弱点である。

2-5 三つの選択肢——穴を塞ぐ、人を増やす、クラウドを利用する

「オンプレミス+穴の開いた閉域網」に対して、病院が取り得る選択肢は、大きく三つある。第一は、閉域網の穴を塞ぎ、完全な閉域網に戻すことである。これは理屈としては分かりやすい。しかし、オンライン資格確認、レセプト電子化、医療 DX、外部保守、データ活用を進める現在の流れとは逆行する。穴を塞ぐことは医療 DX の道を閉じ、保守コストの増加にもつながる。

第二は、SE や ICT に詳しいスタッフを増員し、システムやアプリケーションを強化して、自院のセキュリティレベルを大きく上げることである。これも理想としては正しい。しかし、日本の病院、特に中小病院では、技術的にも資金的にも実現が難しい。この選択肢は中小病院にとって極めて困難とされている。

第三は、クラウドを利用することである。電子カルテや関連システムをクラウド上で運用し、クラウド事業者の監視、バックアップ、分散運用を活用する。ただし、クラウドを利用すれば安全になるという単純な話ではない。リスクの中心は、院内サーバーの破壊から、ID、認証、権限、API、操作記録、設定ミス、責任分界の管理へと移る。

したがって、クラウド利用は重要な方向性だが、単にサーバーを外に置くだけでは不十分であり、ID、認証、権限、API、操作記録、責任分界の設計が必要になる。

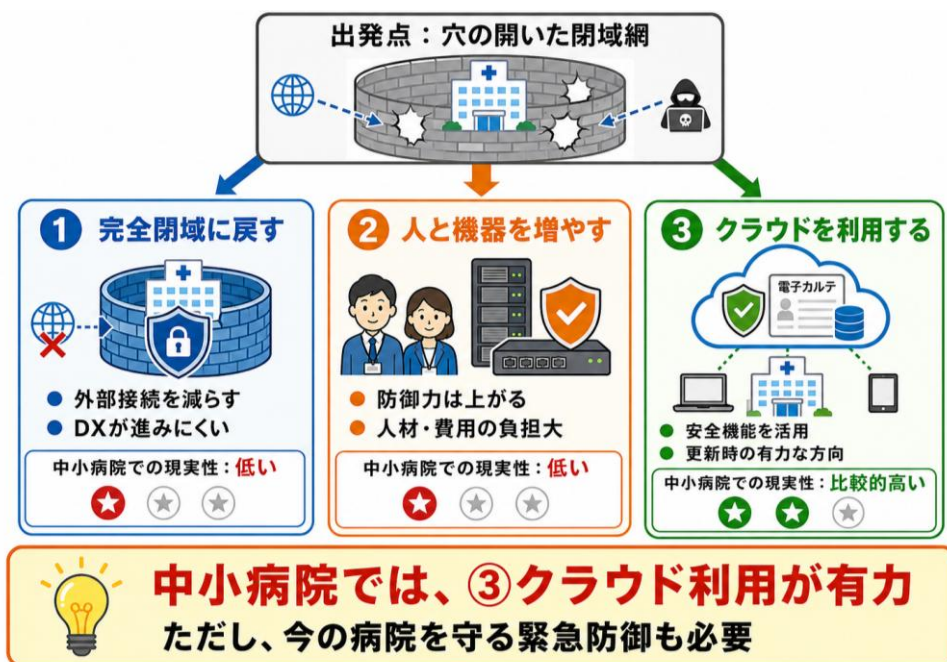


図 2-4 三つの選択肢——穴を塞ぐ・人を増やす・クラウドを利用する

図 2-4 に示すように、三つの選択肢には、それぞれ長所と限界がある。完全閉域に戻せば、外部接続リスクは下がるかもしれないが、医療 DX や保守効率に逆行する。人と機器を増やせば防御力は上がるが、中小病院には負担が重い。クラウド利用は重要な方向性だが、単にサーバーを外に置くだけでは不十分である。

2-6 中小病院にとって現実的な道は何か

中小病院にとって、完全閉域化は現実的ではない。医療 DX の流れに逆行し、保守コストも上がる。大企業並みに人員と高度な機器を増やすことも難しい。クラウド化は重要な方向性だが、すべての病院がすぐに移行できるわけではない。

したがって、現実的な道は二段階で考える必要がある。

第一に、現在のオンプレミス環境を前提に、直ちに危険な穴を見つけ、診療停止に至る経路を分断することである。具体的には、外部接続の棚卸し、多要素認証、ネットワーク分離、消されにくいバックアップ、紙運用訓練である。

第二に、システム更新やクラウド移行のタイミングで、クラウドネイティブ化、標準 API ゲートウェイ、共通接続管理基盤へ進むことである。

図2-5 中小病院にとって現実的な道は何か

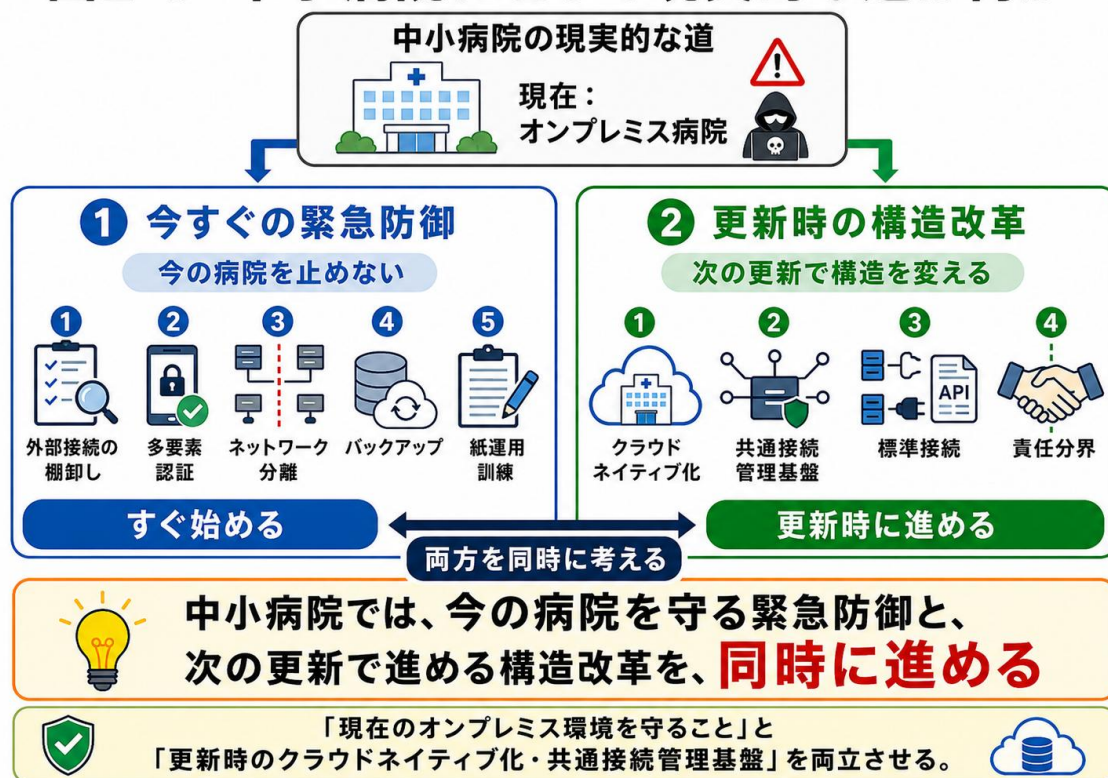


図 2-5 中小病院にとって現実的な道は何か

図 2-5 に示すように、中小病院が取るべき道は、今すぐの緊急防御と、将来の構造改革を分けて考えることである。

今すぐ行うべきことは、現在の病院を止めないための対策である。外部接続を棚卸しし、重要な ID に多要素認証を入れ、電子カルテ系、事務系、インターネット系、バックアップ系を分け、消されにくいバックアップを確保し、電子カルテ停止時の紙運用を訓練する。

一方で、システム更新やクラウド移行の時期には、単にサーバーの置き場所を変えるだけでなく、クラウドネイティブ化、標準 API ゲートウェイ、共通接続管理基盤、責任分界、データ移行性を契約条件として考える必要がある。

つまり、病院管理職が理解すべきことは、「今すぐ全部をクラウドに移すべきだ」という単純な話ではない。

**今の病院を止めない緊急防御と、
次の更新で構造を変える改革を、
同時に進めることが重要である。**

第 2 章のまとめ

日本の多くの病院情報システムは、オンプレミス型を基本とし、閉域網で守られているように見える。しかし、医療 DX により、オンライン資格確認、レセプト、遠隔保守、部門システム、クラウドサービスなど、外部接続の穴が増えている。電子カルテ端末からインターネットを見られないことと、病院情報システム全体が安全であることは別である。中小病院にとっては、完全閉域化や大規模人員増よりも、現在の穴を把握し、多層防御で診療停止への経路を分断することが現実的である。

第3章 攻撃者はどのように侵入し、診療停止に至らせるのか

3-1 攻撃は「いきなり電子カルテを止める」わけではない

病院のサイバー攻撃というと、多くの人は「ウイルスに感染して、突然電子カルテが使えなくなる」というイメージを持つ。しかし実際には、攻撃はもっと静かに、段階的に進むことが多い。

攻撃者は、最初から電子カルテを止めるとは限らない。まず入口を探し、小さく侵入し、内部に足場を作り、院内ネットワークを調べ、重要な ID や管理者権限を探し、バックアップの場所を確認し、最後に一斉に攻撃を実行する。攻撃は侵入、バックドア、夜間探索、権限拡大、一斉発火という流れで整理できる。

したがって、病院管理職が理解すべきことは、単に「ウイルス対策ソフトを入れているか」ではない。攻撃者が、どの入口から入り、どこまで広がり、どの時点で止められるかである。

図3-1 攻撃の典型的なプロセス



図 3-1 攻撃の典型的なプロセス

図 3-1 に示すように、攻撃は段階的に進む。重要なのは、この流れの途中に、病院側が攻撃を止める機会が複数あるということである。入口で防ぐこともできる。認証で止めることもできる。院内で広がる前に検知することもできる。バックアップを守ることもできる。紙運用で診療をつなぐこともできる。

この考え方が、後に述べるスイスチーズ型防御につながる。

3-2 入口は、怪しいメールだけではない

病院職員向けの研修では、しばしば「怪しいメールを開かないように」と教えられる。もちろんこれは重要である。添付ファイルを開いたり、偽サイトに ID とパスワードを入力した

りすれば、そこが侵入口になる。

しかし、入口はメールだけではない。古い VPN、遠隔保守の入口、外部公開サーバー、部門システムの保守口、クラウド管理画面、共有 ID、退職者の残ったアカウントなど、攻撃者が狙う入口は多い。第 2 章で見た「穴の開いた閉域網」は、まさにこうした入口を生み出しやすい構造である。

管理職に必要なのは、「職員が怪しいメールを開かなければ大丈夫」と考えないことである。メール対策は必要だが、それだけでは不十分である。病院情報システムに、どのような外部接続があり、誰が管理し、どのような認証で守られているのかを確認する必要がある。

3-3 侵入後、攻撃者はすぐには止めない

攻撃者が病院内に侵入しても、すぐに電子カルテを止めるとは限らない。むしろ、すぐに攻撃を実行すれば、病院側に気づかれやすい。そこで攻撃者は、まず内部に足場を作る。

この足場が、いわゆるバックドアである。バックドアとは、攻撃者が再び入り直すために作る裏口のようなものである。正面玄関から一度入った泥棒が、裏口の鍵を開けておくようなものである。

バックドアが作られると、攻撃者は時間をかけて院内を調べることができる。昼間は目立つため、夜間や休日に少しずつ探索することもある。診療部門から見れば、何も起きていないように見える。しかし、内部では攻撃者が病院の見取り図を作っている可能性がある。

図3-2 静かな侵入——バックドアと夜間探索

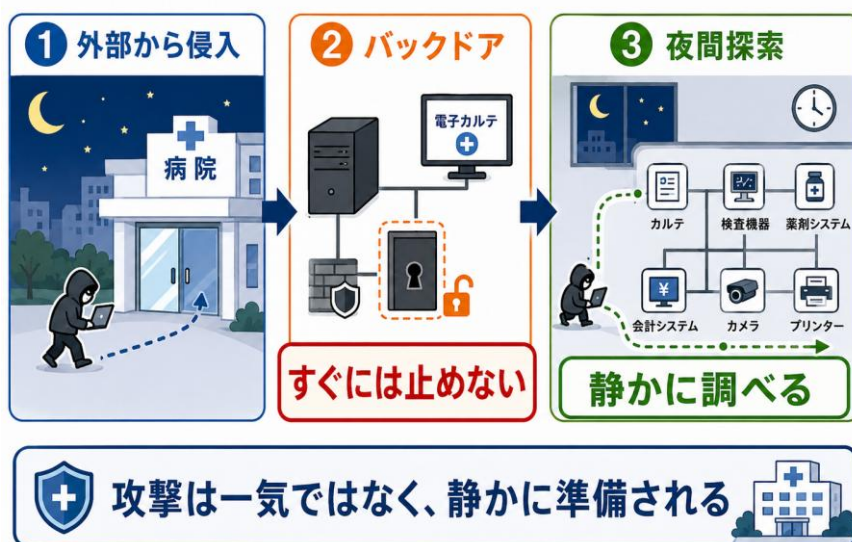


図 3-2 静かな侵入——バックドアと夜間探索

図 3-2 のポイントは、「侵入された瞬間に終わりではない」ということである。逆にいえば、侵入されても、その後の段階で気づき、広がり止めることができれば、診療停止を防げる可能性がある。

3-4 攻撃者は院内ネットワークの見取り図を作る

攻撃者が院内に入った後に行う重要な作業は、病院内のシステム構造を調べることである。電子カルテサーバーはどこにあるのか。医事会計システムはどこか。検査システム、画像システム、薬剤システム、バックアップはどこにあるのか。管理者 ID はどこで使われているのか。認証基盤はどこにあるのか。

これは、泥棒が建物の中に入り、金庫、鍵、非常口、警備室、監視カメラの位置を調べるようなものである。病院側が普段から自院のシステム構造を把握していなければ、攻撃者の方が病院の弱点に詳しくなるという逆転が起きる。

図3-3 院内ネットワークの見取り図を作る攻撃者

攻撃者は院内システムの見取り図を作る

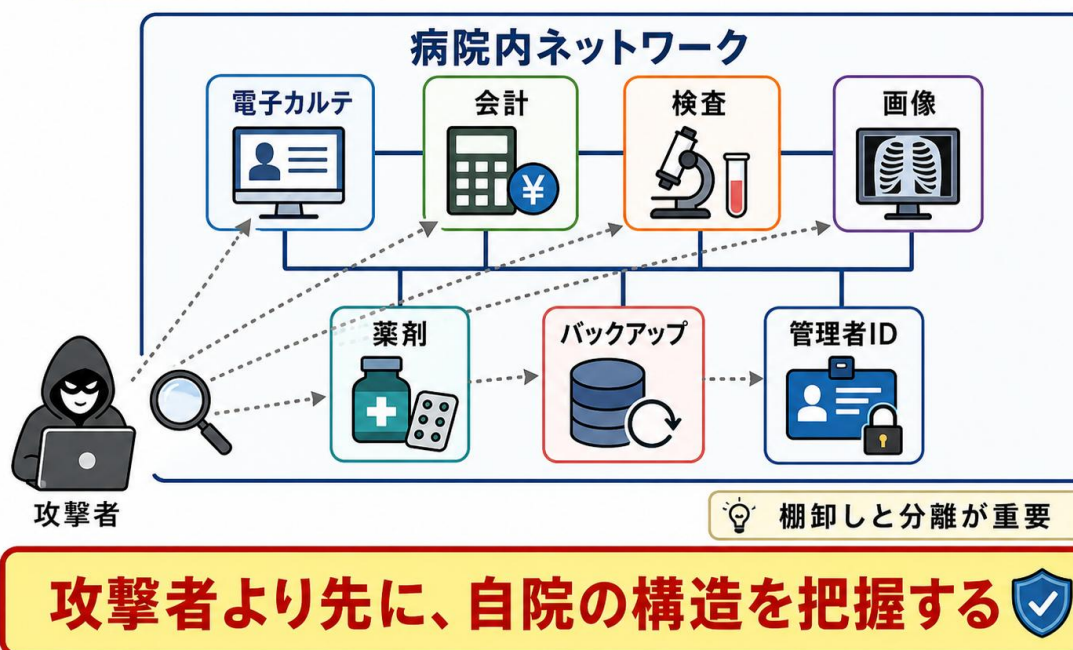


図 3-3 院内ネットワークの見取り図を作る攻撃者

図 3-3 で示すように、攻撃者は単に一つのパソコンを壊すのではない。病院全体のシステムのつながりを調べ、どこを攻撃すれば最も大きな被害を出せるかを考える。

だからこそ、管理職は「情報システム担当者に任せている」だけでは不十分である。主要システム、ベンダー、外部接続、バックアップ、緊急連絡先を、病院として把握しておく必要がある。

3-5 最後に一斉発火する

攻撃者が院内の構造を理解し、必要な権限を手に入れ、バックアップの場所を見つけると、最後に攻撃を一斉に実行する。これが、病院側から見ると「突然、電子カルテが使えなくなった」と見える。

しかし、実際にはその前に、侵入、潜伏、探索、権限拡大、バックアップ確認という準備段階がある。最後の一斉発火は、長い準備の結果である。

特に危険なのは、本番システムとバックアップが同時に暗号化・削除されることである。電子カルテが止まっても、消されにくいバックアップがあり、実際に復旧できる手順が確認されていれば、被害を限定できる可能性がある。しかし、バックアップまで破壊されれば、復旧に長い時間を要し、診療継続に大きな支障が出る。



図 3-4 マルチステージ・ランサムウェア攻撃

図 3-4 の目的は、恐怖を煽ることではない。攻撃の流れを分解すれば、途中で止める場所が見えるということを理解するためである。入口対策、認証対策、権限管理、ネットワーク分離、監視、バックアップ、紙運用は、それぞれこの流れのどこかを止める役割を持つ。

3-6 半田病院事例から学ぶこと

実際の病院サイバー攻撃では、閉域網であることへの過信が問題になることがある。半田病院事例でも、「閉域網なら安全」という考え方の危うさが指摘された。報告書には、セキュリティ対策ソフトが作動していなかったことや、閉域網安全神話による過信などが述べられている。(徳島県つるぎ町立半田病院『コンピュータウイルス感染事案 有識者会議調査報告書』つるぎ町立半田病院コンピュータウイルス感染事案有識者会議、2022 年 6 月 7 日) もちろん、一つの事例を単純化して、すべての病院にそのまま当てはめるべきではない。しかし、そこから学ぶべきことは明確である。病院は「閉域網です」「ベンダーに任せています」「バックアップがあります」という言葉だけで安心してはいけない。

確認すべきなのは、外部接続はどこにあるか、認証は十分か、ログは見ているか、バックアップは本当に復旧できるか、電子カルテ停止時に紙運用へ切り替えられるかである。



図 3-5 半田病院事例から見る閉域網神話の危険

第 3 章のまとめ

病院サイバー攻撃は、突然電子カルテが止まる一瞬の出来事ではない。多くの場合、入口探索、侵入、バックドア、夜間探索、権限拡大、バックアップ確認、一斉発火という段階を経る。管理職が理解すべきことは、攻撃の各段階には防御の機会があるということである。侵入を完全にゼロにできなくても、診療停止に至る経路を途中で分断することはできる。

第 4 章 生成 AI は攻撃者の何を増幅するのか

4-1 問題は AI そのものではなく、攻撃者が AI を使うことである

生成 AI という言葉を聞くと、「AI が自動で病院を攻撃するのか」と不安になるかもしれない。しかし、管理職向けにまず強調すべきことは、問題は AI そのものではなく、攻撃者が AI を使うことである。

生成 AI は、文章を作る、情報を整理する、候補を比較する、手順を考える、似た事例を探す、といった作業を得意とする。これは病院側が業務改善や教育に使えば有用である。しかし、攻撃者が使えば、弱点探索、フィッシング（だまし）文面作成、攻撃経路の検討を助ける道具にもなる。

その結果、生成 AI を使う攻撃者の攻撃の効率が高まると同時に、攻撃者になる技術的なハードルが低くなり、攻撃者のなり手が増えることも予想される。

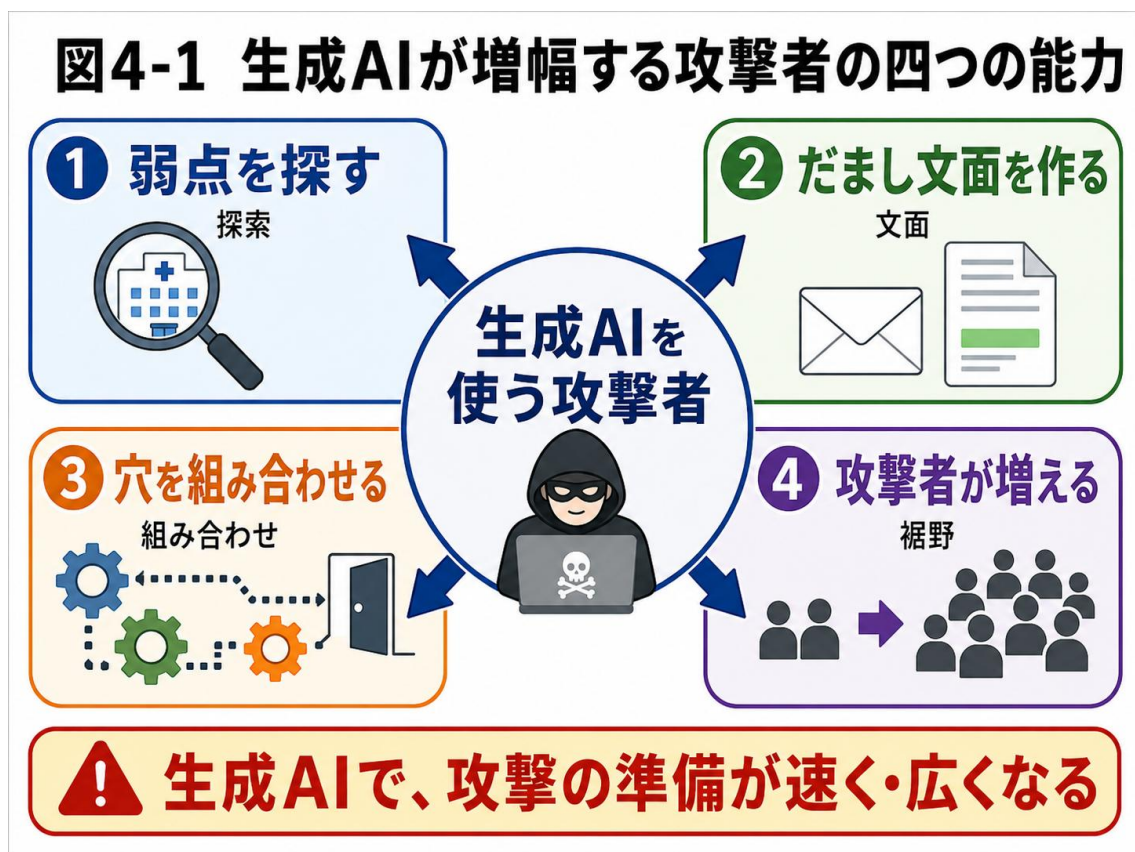


図 4-1 生成 AI が増幅する攻撃者の四つの能力

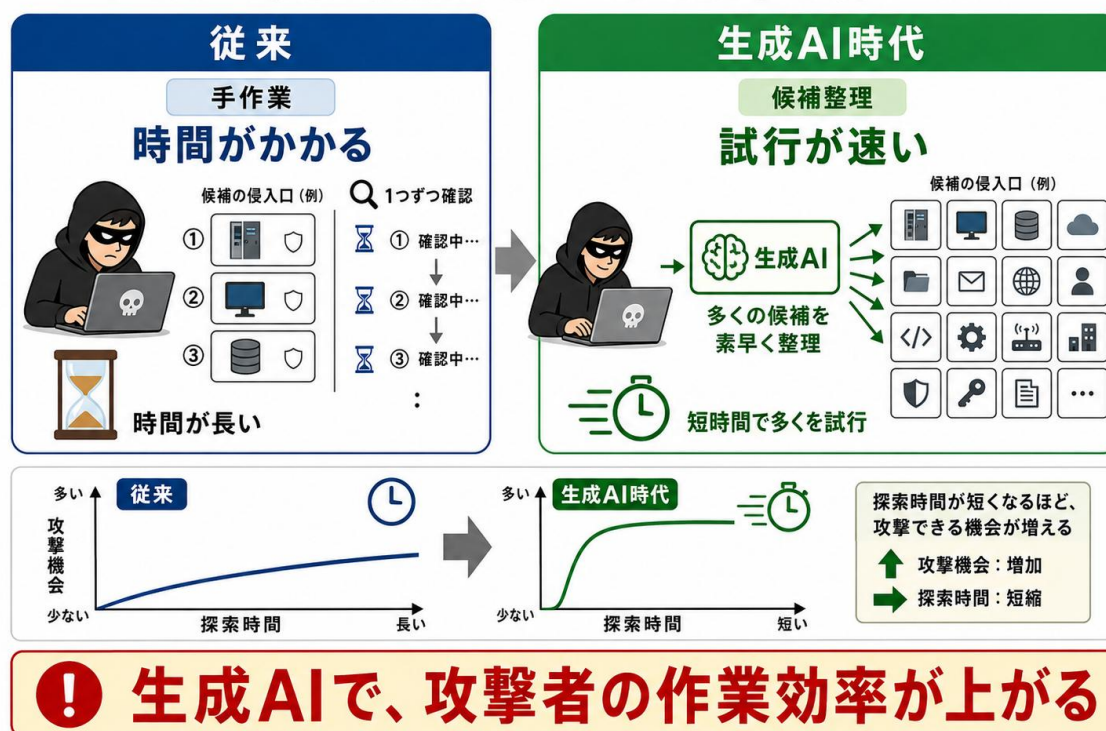
4-2 生成 AI は弱点探索の時間を短縮する

攻撃者にとって、時間は重要である。多数の病院や組織を調べ、どこに古い機器があり、どこに外部接続があり、どの入口が弱そうかを探すには手間がかかる。

生成 AI は、この探索作業を助ける。公開情報、過去の攻撃事例、一般的なシステム構成、よくある設定ミス、ベンダー保守の典型的な入口などを整理し、「どこを確認すべきか」を考えやすくする。

ここで重要なのは、生成 AI が魔法のように何でも突破するわけではないという点である。しかし、攻撃者の調査時間を短くし、試行錯誤の効率を上げる可能性がある。これにより、これまでなら攻撃対象になりにくかった中小病院にも、攻撃の目が向きやすくなる。

図4-2 探索時間短縮 × 成功確率上昇のイメージ



AIが直接攻撃するのではない

図 4-2 探索時間短縮 × 成功確率上昇のイメージ

4-3 生成 AI は病院らしいフィッシング文面を作る

生成 AI の分かりやすい影響の一つは、だまし文面の品質向上である。以前の迷惑メールは、日本語が不自然で、明らかに怪しいものも多かった。しかし生成 AI を使えば、自然な日本語で、病院業務に合った文面を作ることができる。

たとえば、「院内研修資料の確認」「診療報酬改定対応」「医療安全講習」「ベンダー保守のお知らせ」「電子カルテ更新案内」「人事・給与関連通知」など、病院職員が日常的に受け取りそうな文面を作ることができる。さらに、管理職向け、医師向け、看護師向け、医事課向けに文面を変えることもできる。

ICT に詳しくない職員だけでなく、多忙な管理職ほど、もっともらしいメールを確認せずに開いてしまう可能性がある。

図4-3 病院職員がだまされやすいAIフィッシング

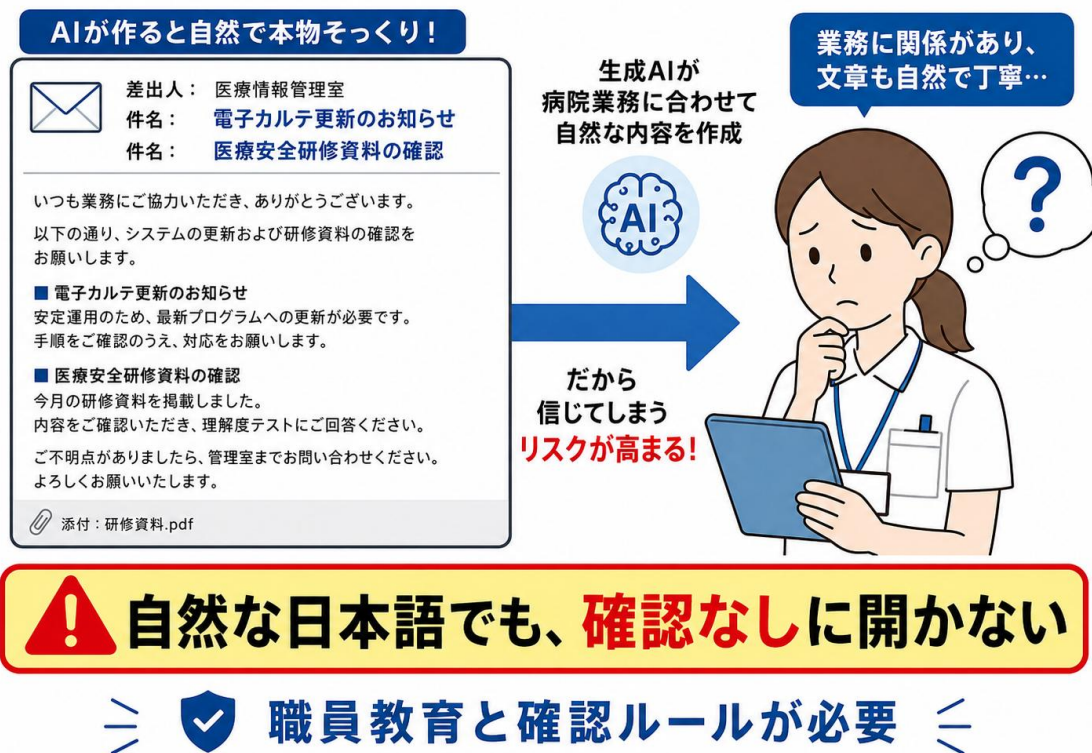


図 4-3 病院職員がだまされやすい AI フィッシング

4-4 生成 AI は複数の穴を組み合わせる作業を助ける

病院のサイバー被害は、一つの穴だけで起きるとは限らない。遠隔保守の入口がある。多要素認証が弱い。管理者 ID が共有されている。ネットワークが分離されていない。バックアップが本番環境と近い。紙運用訓練がない。こうした複数の弱点が組み合わさることで、診療停止に至る。

生成 AI 時代に注意すべきなのは、攻撃者がこうした弱点の組み合わせを考えやすくなることである。単独の穴では小さな問題に見えても、複数の穴が一直線に並ぶと、大きな事故につながる。

この考え方は、第 5 章のスイスチーズ型防御に直結する。病院側の目標は、すべての穴を完全に塞ぐことではない。穴が一直線に並ばないようにすることである。



図 4-4 複数の穴を組み合わせる診療停止に至る経路

4-5 攻撃者の裾野が広がる

生成 AI は、専門家だけでなく、知識の少ない人にも高度な作業をしやすくする。これは、教育や業務改善では大きな利点である。一方で、攻撃の世界では、これまで高度な知識を持たなかった人が、攻撃の準備や文面作成をしやすくなる可能性がある。

もちろん、すべての攻撃が高度化するわけではない。しかし、低レベルの攻撃者でも、より自然な日本語文面を作り、一般的な弱点を調べ、攻撃手順を整理しやすくなる。結果として、攻撃の件数や試行回数が増える可能性がある。

病院側は、これに対して「一つの壁」で守る発想から離れる必要がある。入口で防ぎ、認証で止め、権限を絞り、ネットワークを分け、監視し、バックアップを守り、紙運用で診療をつなぐ。複数の層で守る考え方が必要である。

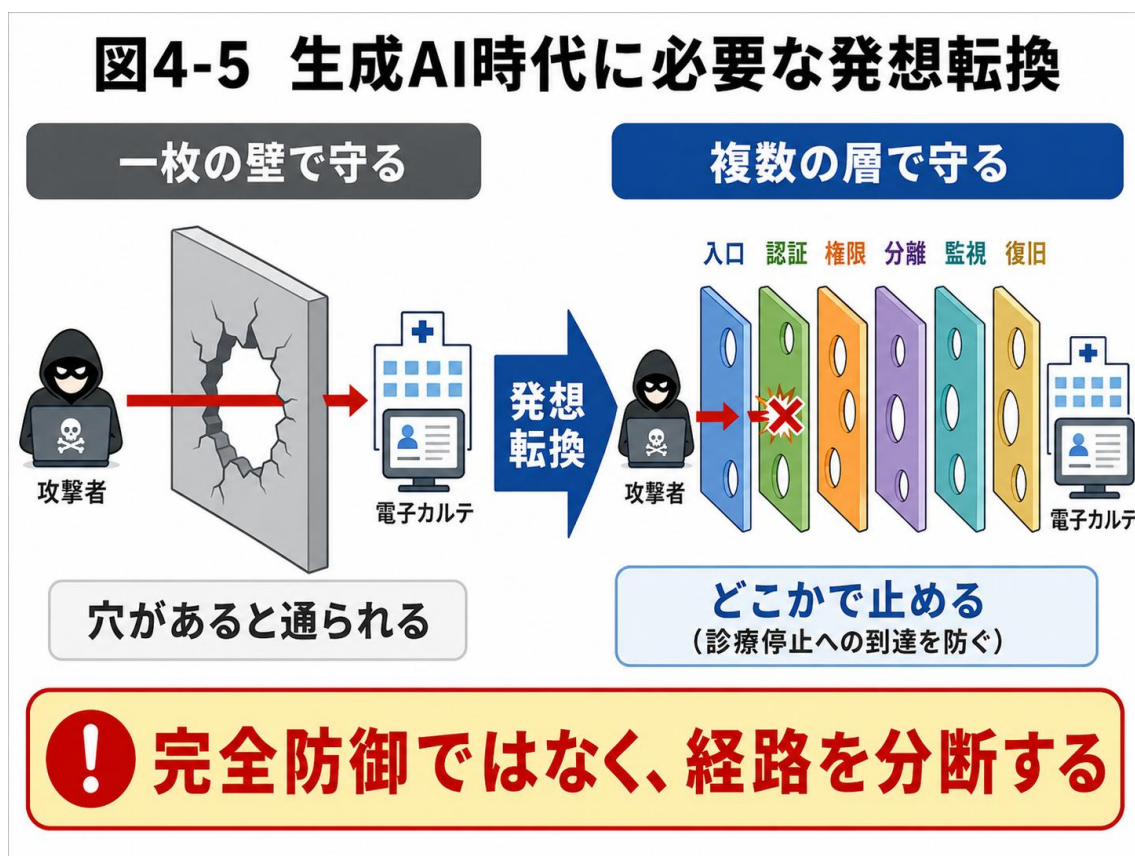


図 4-5 生成 AI 時代に必要な発想転換

第4章のまとめ

生成 AI 時代の脅威は、AI が自動的に病院を攻撃するという単純な話ではない。攻撃者が生成 AI を使うことで、弱点探索、フィッシング文面作成、複数の穴の組み合わせ、攻撃者層の拡大が起きる可能性がある。病院側は、一つの防御壁に頼るのではなく、複数の層で診療停止への経路を分断する発想に切り替える必要がある。

第 5 章 スイスチーズ理論で考える病院防御

5-1 スイスチーズ理論とは何か

スイスチーズ理論とは、安全対策を複数の層として考える方法である。チーズの一枚一枚には穴がある。しかし、複数のチーズを重ねると、穴の位置がずれていれば、危険は最後まで通り抜けない。

病院のサイバー対策も同じである。入口対策には穴がある。認証対策にも穴がある。権限管理にも穴がある。ネットワーク分離にも穴がある。監視にも限界がある。バックアップにも不備があるかもしれない。組織対応にも弱さがある。

しかし、これらの穴が一直線に並ばなければ、攻撃が診療停止まで到達する可能性を下げることができる。

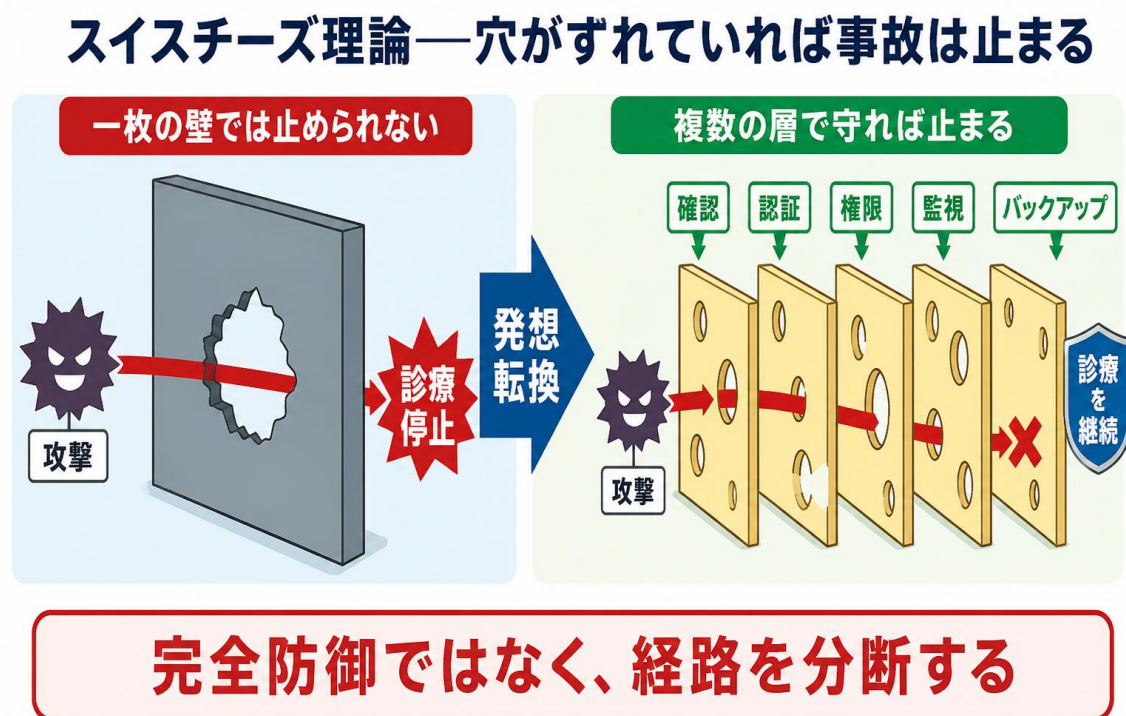


図 5-1 スイスチーズ理論—穴がずれていれば事故は止まる

5-2 穴が一直線に並ぶと重大事故になる

スイスチーズ理論で最も重要なのは、穴があること自体ではない。穴が一直線に並ぶことである。

たとえば、外部接続の穴がある。多要素認証がない。管理者 ID が共有されている。ネットワークが分離されていない。監視されていない。バックアップが本番環境と同じ場所にある。紙運用訓練がない。これらが重なると、攻撃者は入口から最後まで進みやすくなる。

中小病院では、すべてを完璧にすることは難しい。だからこそ、どこか一か所でも経路を切ることが重要である。多要素認証を入れるだけでも、攻撃の進行を止められることがある。バックアップを守るだけでも、診療停止期間を短くできることがある。紙運用訓練があれば、救急・入院・透析・急変対応など、止められない診療を一部継続できることがある。

図5-2 穴が一直線に並ぶと診療停止に至る

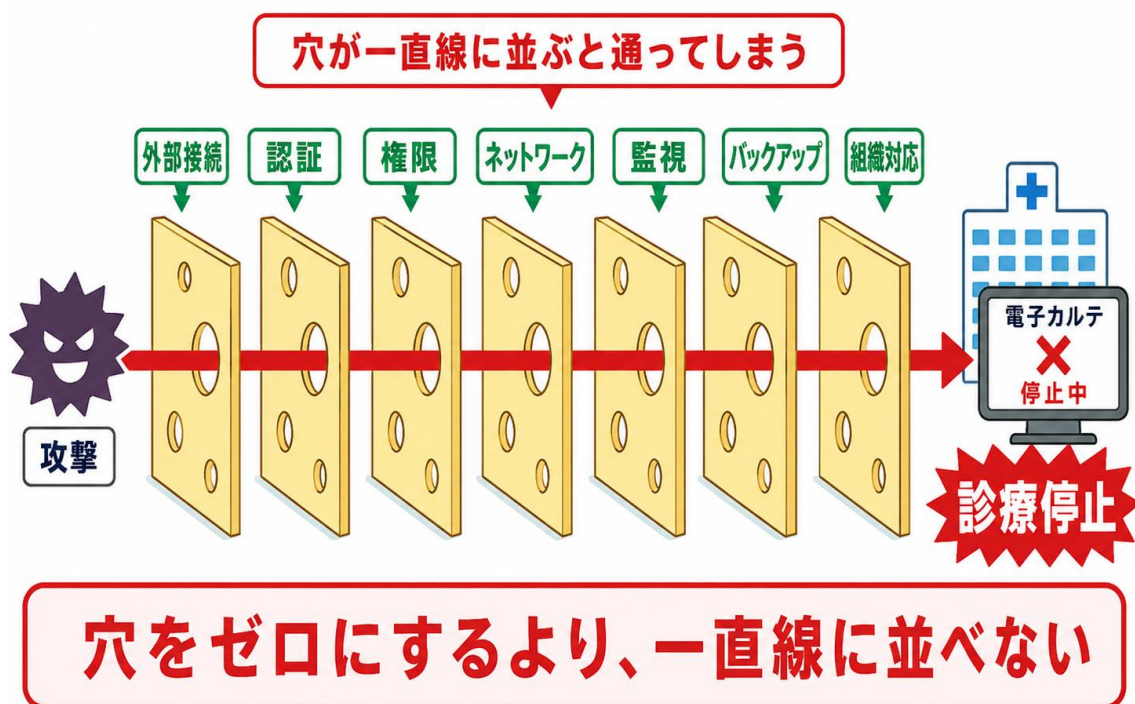


図 5-2 穴が一直線に並ぶと診療停止に至る

5-3 病院サイバー防御の七層

病院サイバー防御は、七つの層で考えると分かりやすい。

第1層は入口対策である。外部接続、メール、VPN、遠隔保守、公開サーバーなど、攻撃者が入ろうとする入口を管理する。

第2層は認証対策である。パスワードだけに頼らず、多要素認証を導入し、特に管理者ID、ベンダーID、リモートアクセスを重点的に守る。

第3層は権限管理である。誰でも何でもできる状態を避け、必要な人が必要な範囲だけ使えるようにする。

第4層はネットワーク分離である。電子カルテ系、事務系、インターネット系、バックアップ系を分け、侵入されても一気に広がらないようにする。

第5層は監視・検知である。普段と違う動き、夜間の不自然なアクセス、大量のファイル操作、管理者権限の異常利用などを見つける。

第6層はバックアップ・復旧である。バックアップを取るだけでなく、消されにくくし、実際に復旧できるかを確認する。

第7層は組織対応である。電子カルテ停止時の連絡体制、紙運用、ベンダー連絡、院内判断、患者説明、地域連携を準備する。



図 5-3 病院サイバー防御の七層

5-4 侵入されても診療停止に至らせない

従来のセキュリティ説明では、「侵入されないこと」が強調されがちである。しかし、病院管理職にとって重要なのは、侵入された場合にどうするかである。

侵入されたとしても、認証で止める。認証を突破されても、権限を広げさせない。権限を取られても、ネットワークを横展開させない。ネットワーク内に入られても、監視で気づく。監視をすり抜けても、バックアップを守る。電子カルテが止まっても、紙運用で診療をつなぐ。

このように、各層が完全でなくても、どこかで止めることができれば、診療停止の被害を小さくできる。スイスチーズ型防御の目的は、侵入を完全にゼロにすることではなく、診療停止に至る可能性を下げ、停止した場合の範囲・時間・患者影響を最小化することである。

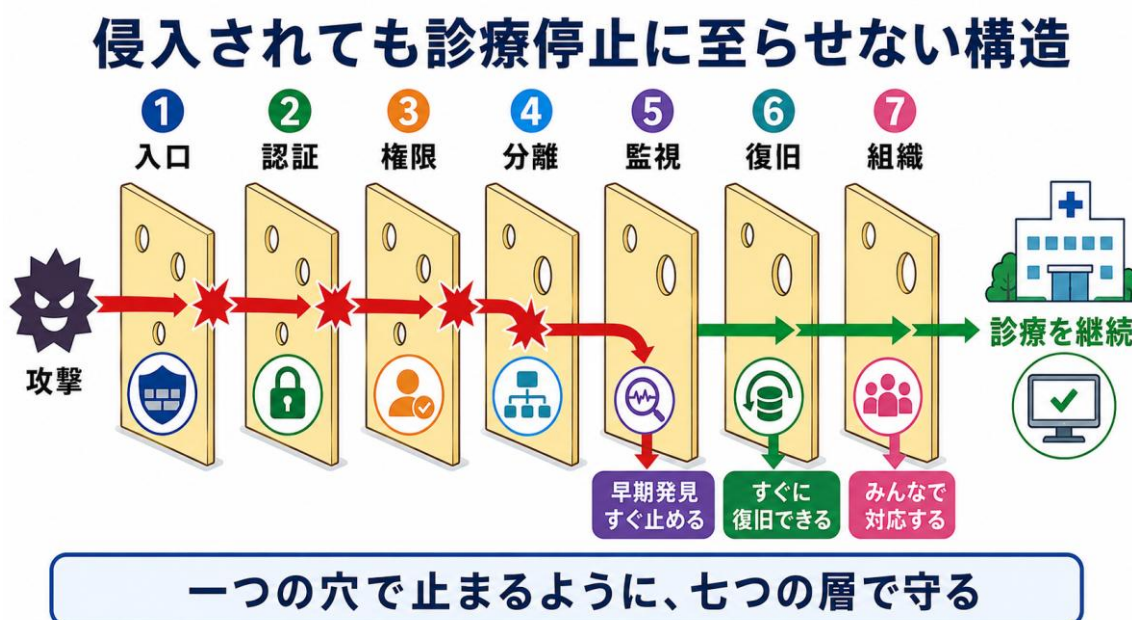


図 5-4 侵入されても診療停止に至らせない構造

5-5 中小病院は、全部ではなく重点防御から始める

中小病院にとって、七層すべてを一度に完璧にすることは難しい。情報システム担当者が少なく、予算も限られる。だからといって、何もしないという選択肢はない。

重要なのは、診療停止に直結しやすい経路から優先して切ることである。まず外部接続を棚卸しする。リモートアクセス、管理者 ID、ベンダー ID に多要素認証を入れる。電子カルテ系、事務系、インターネット系、バックアップ系を分ける。消されにくいバックアップを確保する。電子カルテ停止時の紙運用を一度訓練する。

これは第 6 章で詳しく述べる「オンプレミス病院が直ちに行う五つの対策」である。第 5 章のスイスチーズ理論は、第 6 章の実践策の考え方そのものである。

中小病院の重点防御——全部ではなく、経路を切る



図 5-5 中小病院の重点防御——全部ではなく、経路を切る

第 5 章のまとめ

スイスチーズ理論は、病院サイバー対策を管理職が理解するうえで非常に有効である。一つひとつの対策には穴がある。しかし、入口、認証、権限、ネットワーク、監視、復旧、組織対応という複数の層を重ね、穴が一直線に並ばないようにすれば、診療停止への到達を防ぎやすくなる。中小病院に必要なのは、すべてを完璧にすることではなく、診療停止に直結する経路を優先して分断することである。

第 6 章 オンプレミス病院が直ちに行う五つの対策

6-1 オンプレミス病院の最大リスク

第 2 章で述べたように、日本の多くの病院情報システムは、院内に電子カルテサーバーなどを置くオンプレミス型を基本としている。かつては、病院情報システムをインターネットから切り離す閉域網という考え方に合理性があった。しかし、現在はオンライン資格確認、レセプト、遠隔保守、部門システム、クラウドサービスなど、業務上必要な外部接続が増えている。

問題は、外部接続そのものではない。問題は、外部接続がどこにあり、誰が管理し、どのような認証で守られ、緊急時に遮断できるのかが、病院側で把握されていないことである。オンプレミス病院の最大リスクは、外部接続の穴から侵入され、院内ネットワークを横に広がられ、電子カルテ、医事会計、検査、画像、薬剤、バックアップまで同時に被害を受けることである。オンプレミス病院のリスクとして、外部接続からの侵入、院内横展開、バックアップ同時破壊を挙げることができる。

したがって、オンプレミス病院がまず行うべきことは、完璧なセキュリティ体制を一気に作ることではない。診療停止に直結する経路を、優先順位をつけて切ることである。

図6-1 オンプレミス病院が直ちに行う五つの対策



図 6-1 オンプレミス病院が直ちに行う五つの対策

6-2 対策 1：外部接続の棚卸し

最初に行うべき対策は、外部接続の棚卸しである。

病院管理職が最初に確認すべき問いは、「うちは閉域網ですか」ではない。「外部接続はどこにありますか」である。具体的には、次のような接続を確認する。

オンライン資格確認、レセプト請求、ベンダー遠隔保守、部門システムの保守口、外部検査会社との接続、クラウドサービス、VPN、リモートデスクトップ、外部公開サーバー、退職者や旧ベンダーの残ったアカウントなどである。

これらの接続は、医療 DX や業務効率化のために必要なものも多い。したがって、「すべて閉じる」ことが目的ではない。必要な接続と不要な接続を分け、必要な接続は安全に管理し、不要な接続は閉じる。これが棚卸しの目的である。

外部接続の棚卸しでは、少なくとも次の項目を一覧化する必要がある。

どのシステムにつながっているか。

どのベンダーが利用しているか。

接続方法は何か。

利用者 ID は誰のものか。

多要素認証はあるか。

利用記録は残るか。

緊急時に誰が止められるか。

オンプレミス病院が優先すべき対策の第一として、外部接続の棚卸しが挙げられている。

図6-2 外部接続の棚卸しで病院の弱点を見つける

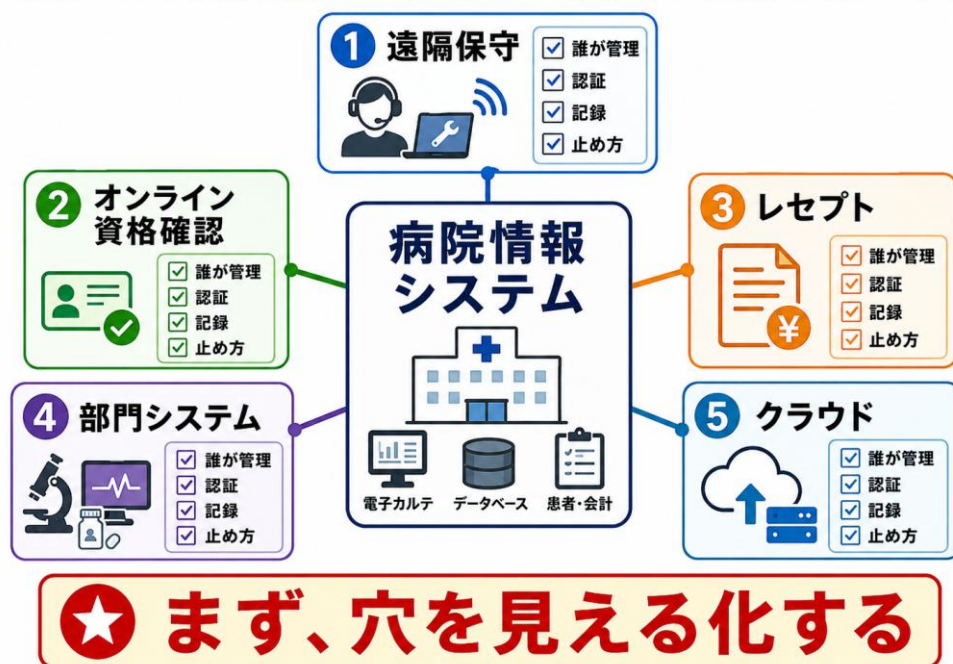


図 6-2 外部接続の棚卸しで病院の弱点を見つける

6-3 対策 2：多要素認証

二つ目の対策は、多要素認証である。

パスワードだけで守る時代は終わりつつある。パスワードは盗まれる。使い回される。退職者のものが残る。ベンダーID が共有される。紙に書かれる。メールで送られる。したがって、特に重要な入口には、パスワードだけでなく、もう一つ別の確認手段を加える必要がある。

多要素認証とは、パスワードに加えて、スマートフォン認証、ワンタイムコード、専用アプリ、物理キーなどを組み合わせる方法である。管理職向けには、細かな方式の違いよりも、「パスワードが盗まれても、それだけでは入れないようにする仕組み」と理解すればよい。多要素認証にも強弱がある。メールや SMS のワンタイムコードより、認証アプリや物理キーの方が望ましい場合がある。特に管理者 ID、ベンダーID、リモートアクセスでは、共有 ID をやめ、個人ごとに識別できる認証と記録を求める。

優先順位が高いのは、リモートアクセス、管理者 ID、ベンダーID である。すべての職員 ID に一度に入れるのが難しい場合でも、外部から入れる入口と、強い権限を持つ ID から始めるべきである。

図6-3 多要素認証——パスワードが盗まれても入らせない



図 6-3 多要素認証——パスワードが盗まれても入らせない

6-4 対策3：ネットワーク分離

三つ目の対策は、ネットワーク分離である。

攻撃者に侵入された場合でも、院内全体に一気に広がられないようにする必要がある。電子カルテ系、医事会計系、検査・画像などの部門システム、事務系、インターネット系、バックアップ系が無秩序につながっていると、攻撃者は横に広がりやすい。

ネットワーク分離とは、システムを用途や重要度ごとに分け、必要最小限の通信だけを許す考え方である。管理職向けには、「病院内に防火区画を作る」と説明すると分かりやすい。火災が起きても建物全体に燃え広がらないように、サイバー攻撃でも院内全体に広がらないようにする。

特に重要なのは、バックアップ系を本番システムから分けることである。バックアップが本番環境と同じ認証、同じネットワーク、同じ管理権限の下にあると、攻撃者に同時に破壊される危険がある。

図6-4 ネットワーク分離——院内に防火区画を作る



図 6-4 ネットワーク分離——院内に防火区画を作る

6-5 対策4：消されにくいバックアップ

四つ目の対策は、バックアップである。ただし、単にバックアップを取っているだけでは不十分である。

管理職が確認すべきことは、「バックアップがありますか」ではない。

「そのバックアップは、攻撃者に消されませんか」

「実際に復旧できますか」

である。

バックアップが本番環境と同じネットワーク、同じ管理者 ID、同じ認証の下に置かれている場合、攻撃者が本番システムと同時にバックアップを暗号化・削除する可能性がある。そうなれば、復旧の道が失われる。

バックアップには、少なくとも三つの条件が必要である。第一に、変更・削除されにくいこと。第二に、本番環境と一定程度切り離されていること。第三に、復旧テストを実施していること。

また、バックアップがあっても、復旧に何日かかるか分からなければ、診療継続計画としては不十分である。

バックアップは保険である。しかし、事故が起きた時に使えない保険では意味がない。バックアップは、①消されにくいこと、②本番環境から切り離されていること、③実際に復旧テストを行っていること、の三点がそろって初めて意味を持つ。

図6-5 バックアップと復旧テストは別物である あるだけでは不十分 戻せることが重要



図 6-5 バックアップと復旧テストは別物である

6-6 対策 5：紙運用訓練

五つ目の対策は、紙運用訓練である。

電子カルテが止まったとき、病院は完全に診療を止めるわけにはいかない。もちろん通常通りの診療は難しくなる。しかし、救急、入院、透析、手術予定、抗がん剤治療、急変対応など、止められない医療がある。

そのためには、電子カルテ停止時に、誰が判断し、どの診療を継続し、どの診療を制限し、どの書式を使い、どこに記録し、後でどのように電子カルテへ戻すのかを決めておく必要がある。また、紙で記録した内容を、復旧後に誰が確認し、どの範囲を電子カルテへ反映し、二重入力や記録漏れをどう防ぐかまで決めておく必要がある。

紙運用訓練とは、通常診療を紙で完全再現することではなく、電子カルテ停止時に、どの診療を継続し、どの診療を制限し、誰が判断し、どの記録を残し、復旧後にどう電子カルテへ戻すかを確認する縮退運用訓練である。

図6-6 電子カルテ停止時の紙運用訓練

電子カルテが止まっても、紙で最低限の診療を継続できるようにする



図 6-6 電子カルテ停止時の紙運用訓練

6-7 病院単独でできること、外部支援が必要なこと

五つの対策のうち、病院単独で始められることもあれば、ベンダーや外部専門家の支援が必要なこともある。

外部接続の一覧作成、院内連絡責任者の決定、保守契約書の確認、紙運用訓練の準備は、病院側が主体的に始められる。一方、多要素認証の導入、ネットワーク分離、バックアップ方式の変更、監視の強化は、ベンダーや専門事業者との調整が必要になる。

管理職の役割は、技術作業を自分で行うことではない。優先順位を決め、責任者を置き、ベンダーに必要な質問をし、費用とリスクを比較し、実行を止めないことである。

第 6 章のまとめ

オンプレミス病院が直ちに行うべきことは、診療停止に至る経路を優先して切ることである。具体的には、外部接続の棚卸し、多要素認証、ネットワーク分離、消されにくいバックアップ、紙運用訓練の五つである。これらはすべてを完璧にするための対策ではなく、攻撃が進んでも途中で止め、診療停止に至る可能性を下げ、停止した場合の範囲・時間・患者影響を小さくするための重点対策である。

第7章 クラウドネイティブ化と共通接続管理基盤

7-1 クラウド化とクラウドネイティブ化は違う

病院サイバー対策を考えるうえで、クラウド化は重要な選択肢である。ただし、ここで注意しなければならないのは、「クラウド化」と「クラウドネイティブ化」は同じではないということである。

クラウド化とは、これまで院内に置いていたサーバーを、外部のクラウド環境に移すことである。一方、クラウドネイティブ化とは、クラウドの特性を前提に、システムの設計、認証、権限管理、API、監視、バックアップ、責任分界を作り直すことである。

単にサーバーの置き場所を院内から院外へ変えるだけでは、十分ではない。古い設計のままクラウドへ移せば、クラウド上に古い弱点を移すだけになりかねない。

図7-1 クラウド化とクラウドネイティブ化の違い

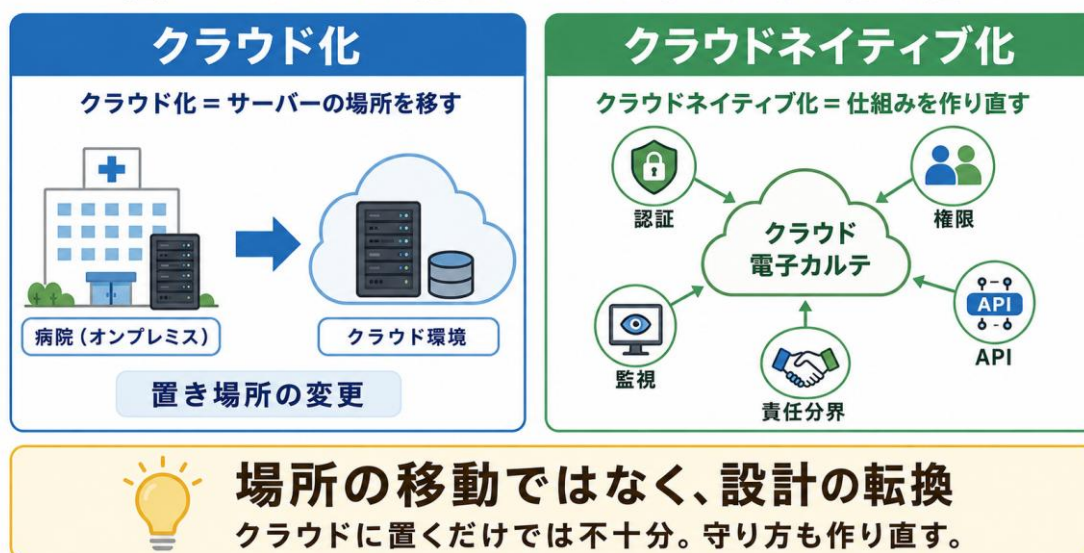


図 7-1 クラウド化とクラウドネイティブ化の違い

7-2 クラウドネイティブ化で下がるリスク、残るリスク

クラウドネイティブ化には、大きな利点がある。院内サーバーが攻撃され、病院内で電子カルテサーバーやバックアップが同時に破壊されるリスクを下げられる可能性がある。クラウド事業者の監視、バックアップ、冗長化、セキュリティ基盤を活用できるからである。しかし、クラウドにすればリスクが消えるわけではない。リスクの場所が変わるのである。クラウド時代の主戦場は、ID、認証、権限、API、操作記録、設定ミス、責任分界になる。誰がアクセスできるのか。どの端末から入れるのか。どの API を通じてデータが動くのか。操作記録は残るのか。異常時に誰が止めるのか。クラウド事業者、電子カルテベンダー、病院の責任はどこで分かれるのか。

クラウドネイティブ病院では、院内サーバー破壊リスクは下がる一方で、ID、API、権限、操作記録の管理が主戦場になる。

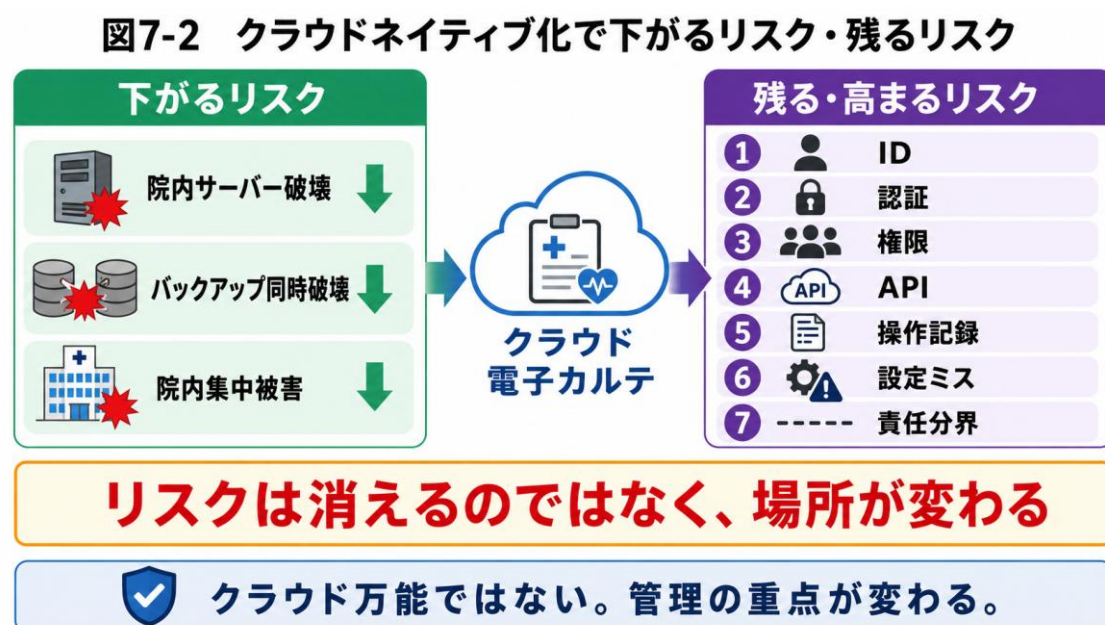


図 7-2 クラウドネイティブ化で下がるリスク・残るリスク

7-3 クラウド時代の主戦場——ID・API・権限・操作記録

クラウドネイティブ化が進むと、守るべき中心は、院内サーバーだけではなくなる。むしろ重要になるのは、誰が、どの権限で、どのデータに、どの経路でアクセスしたかである。

ID は、クラウド時代の鍵である。ID が盗まれれば、院外からでも重要システムにアクセスされる危険がある。したがって、多要素認証、ID の棚卸し、退職者 ID の削除、ベンダーID の管理が重要になる。

API は、システム同士がデータをやり取りする通路である。標準 API は医療 DX には不可欠だが、管理されていない API は新しい穴にもなる。

権限管理は、誰にどこまで許すかを決める仕組みである。すべての人が広い権限を持てば便利かもしれないが、攻撃された時の被害は大きくなる。

操作記録は、何が起きたかを後から確認するための証拠である。記録が残っていなければ、異常の発見も、原因究明も、責任分界の確認も難しくなる。

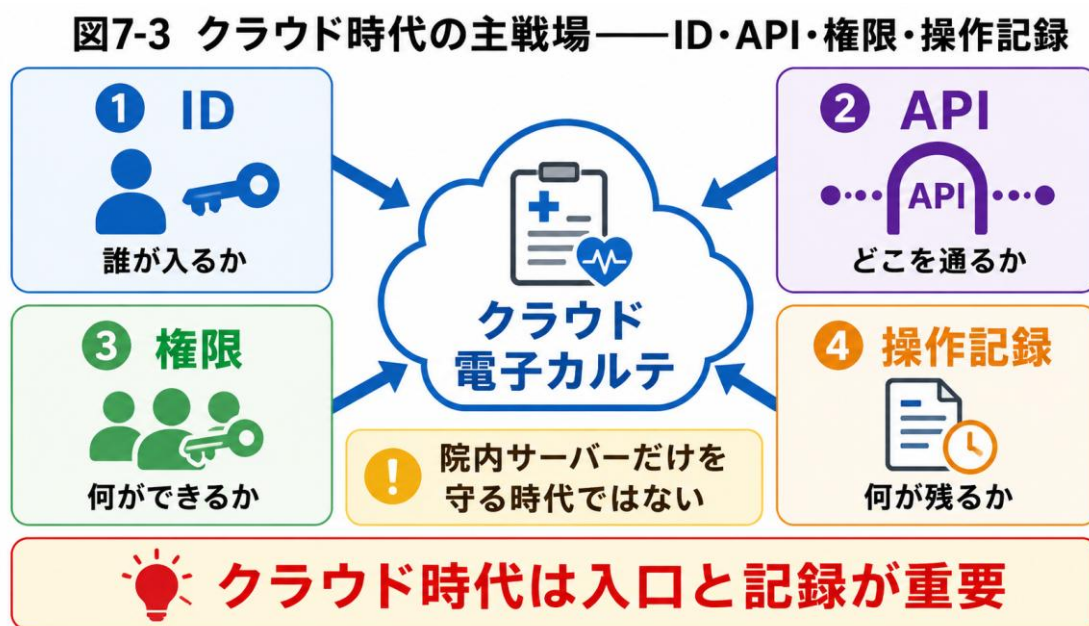


図 7-3 クラウド時代の主戦場——ID・API・権限・操作記録

7-4 共通接続管理基盤とは何か

病院情報システムの外部接続が増えるほど、個別接続をそのまま放置することは危険になる。ベンダーごと、部門システムごと、クラウドサービスごとに接続方式がばらばらであれば、どこに穴があるのか分からなくなる。

そこで重要になるのが、共通接続管理基盤である。本書では、外部接続を共通の入口で管理する考え方を、便宜的に「共通接続管理基盤」と呼ぶ。

共通接続管理基盤とは、病院情報システムと外部システムの接続を、できるだけ共通の入口で管理する仕組みである。標準 API ゲートウェイ、本人確認、権限管理、多要素認証、暗号化、操作記録、監視、異常検知、緊急遮断などを組み合わせる。共通接続管理基盤は、標準 API ゲートウェイ、本人確認、権限管理、多要素認証、操作記録、監視、異常検知、緊急遮断を組み合わせた機能群として整理できる。これは製品名ではなく、ID 管理、認証、権限、API 管理、ログ、監視、緊急遮断、契約責任を組み合わせた運用設計である。

管理職向けに言えば、共通接続管理基盤は、病院情報システムに出入りする外部接続を、ばらばらの裏口から、管理された正面ゲートへ集約する考え方である。

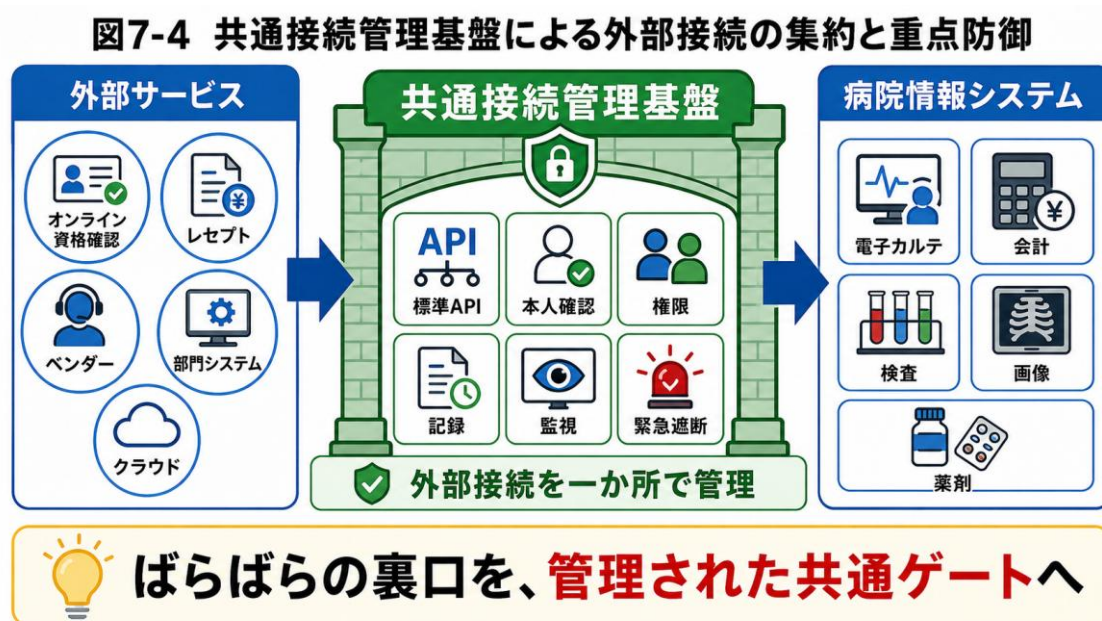


図 7-4 共通接続管理基盤による外部接続の集約と重点防御

7-5 標準 API ゲートウェイの役割

共通接続管理基盤の中心になるのが、標準 API ゲートウェイである。

API とは、システム同士が情報をやり取りするための通路である。病院管理職にとっては、「システム同士の出入口」と考えればよい。標準 API ゲートウェイは、その出入口を標準化し、誰が、どのシステムに、どのデータを取りに行き、どの操作をしたのかを管理する関所のようなものである。

標準 API が整備されれば、部門システム、周辺機器、地域連携、外部アプリ、クラウドサービスとの接続を管理しやすくなる。一方で、標準 API を無秩序に開放すれば、新しい侵入口になる。したがって、API は「開くこと」と「守ること」を同時に設計しなければならない。

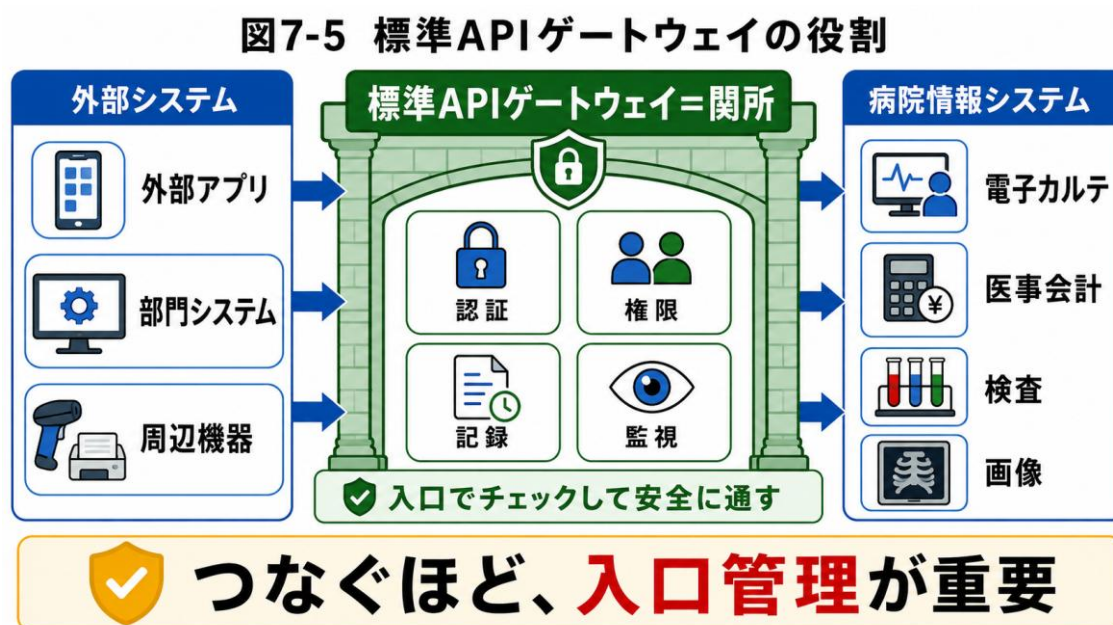


図 7-5 標準 API ゲートウェイの役割

7-6 レガシー機器をどう接続するか

病院には、古い部門システムや医療機器が多く存在する。すべてをすぐに最新のクラウド対応機器に置き換えることは難しい。したがって、クラウドネイティブ化を進める場合でも、レガシー機器との接続をどう扱うかが重要になる。

古い機器を直接外部につなぐと危険である。しかし、完全に切り離せば業務に支障が出ることもある。そこで、エージェントやラッパーのような仕組みで、古い機器を直接外にさらさず、接続を管理する方法が必要になる。

管理職向けには、「古い機器をむき出しでつながない」と理解すればよい。古い機器は、包み込んで、監視し、必要な通信だけを通す。

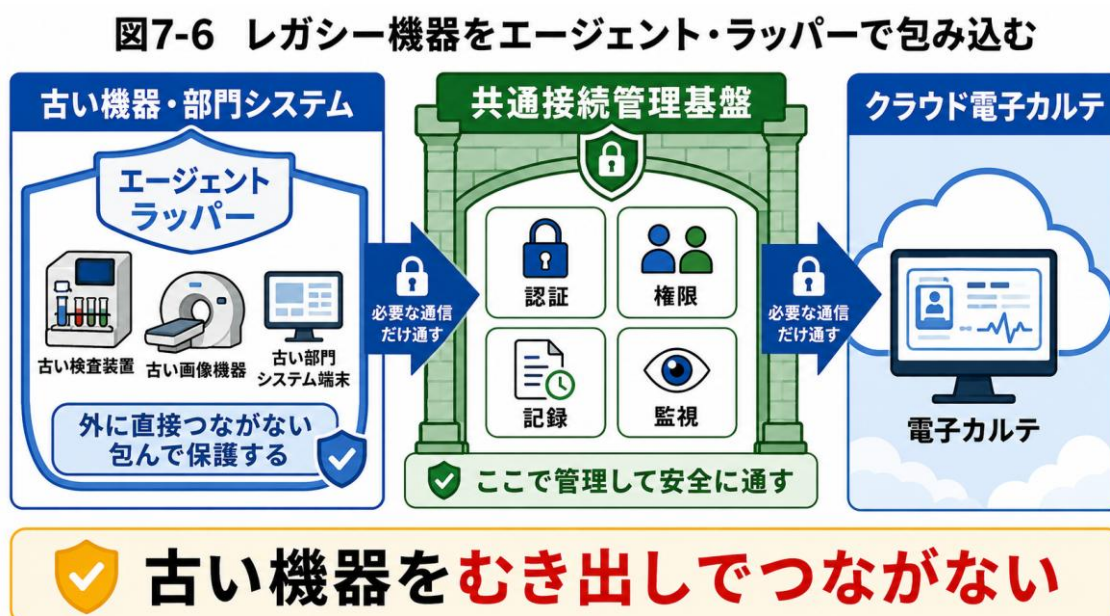


図 7-6 レガシー機器をエージェント・ラッパーで包み込む

7-7 責任分界——病院・ベンダー・クラウド事業者の役割

クラウドネイティブ化が進むほど、責任分界が重要になる。

オンプレミス型では、病院内にサーバーがあり、電子カルテベンダーが保守し、病院が運用するという構造が比較的分かりやすかった。しかし、クラウド時代には、クラウド事業者、電子カルテベンダー、部門システムベンダー、ネットワーク事業者、病院が関わる。

障害が起きたとき、誰が原因を調べるのか。

攻撃を検知したとき、誰が止めるのか。

バックアップは誰が管理するのか。

データを取り出す責任は誰にあるのか。

契約終了時にデータをどう移すのか。

クラウド障害時の代替手順はどうするのか。

これらを曖昧にしたままクラウド化を進めると、いざという時に対応が遅れる。病院管理職は、システム更新やクラウド移行時に、責任分界を契約条件として確認する必要がある。

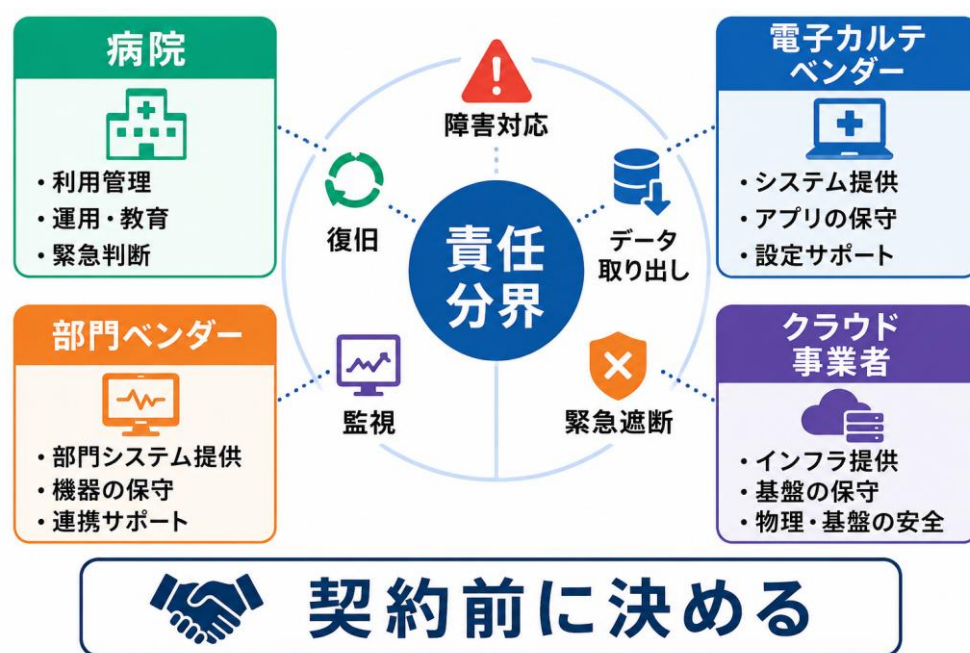


図 7-7 責任分界——病院・ベンダー・クラウド事業者の役割

第7章のまとめ

クラウドネイティブ化は、病院サイバー対策の重要な方向である。しかし、クラウドにすれば安全という単純な話ではない。院内サーバー集中破壊リスクは下がる一方で、ID、API、権限、操作記録、責任分界の管理が重要になる。将来的には、外部接続をばらばらにせず、共通接続管理基盤や標準 API ゲートウェイで管理することが、病院情報システムの安全性と医療 DX を両立させる鍵になる。

第 8 章 病院管理職は何を決めるべきか

8-1 情報システム担当者がある病院と、いない病院を分ける

病院のサイバー対策を考えると、最初に分けるべきなのは、情報システム担当者がある病院と、いない病院である。

情報システム担当者がある病院では、管理職は担当者に具体的な確認を指示し、進捗を管理することができる。一方、情報システム担当者がない病院では、事務長、総務課長、医事課長、看護部、医療安全担当者などが兼務で対応している場合も多い。その場合、最初から高度な技術対策を求めても進まない。

情報システム室のない病院でも最初に行うべきこととして、院内連絡責任者を決めること、ベンダー情報・契約書を集めること、外部接続とバックアップの書面診断を行うことが大切である。

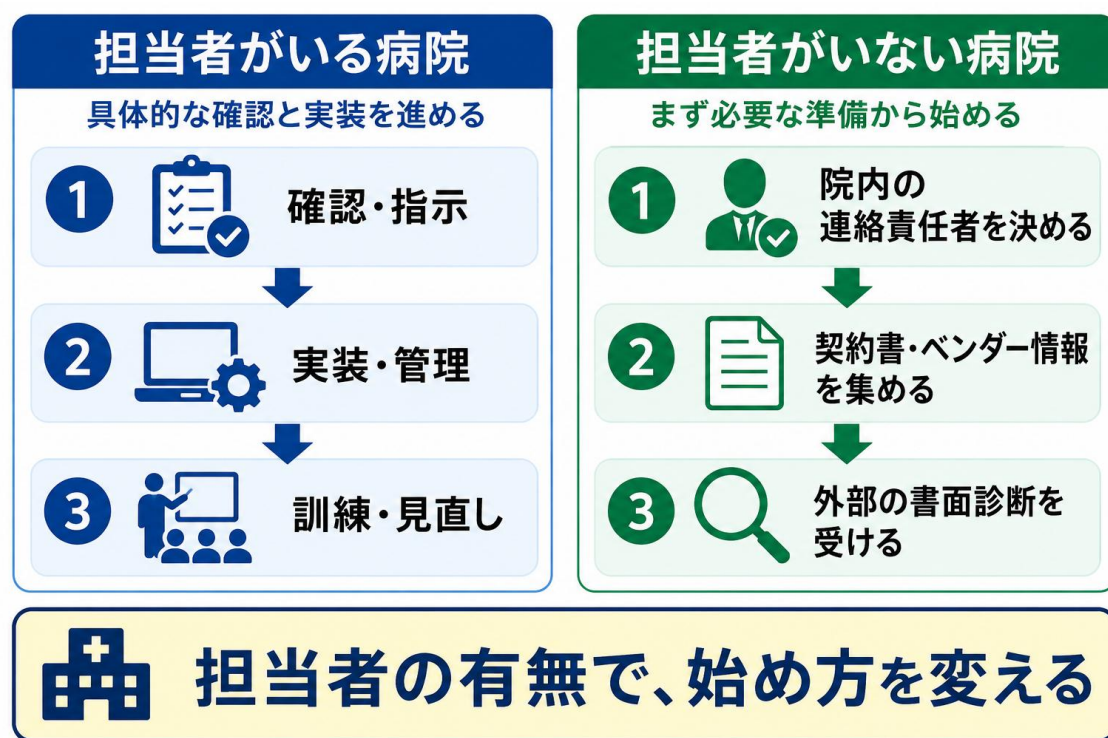


図 8-1 情報システム担当者がある病院・いない病院の進め方

8-2 最初の三か月に行う三つのこと

情報システム体制が十分でない病院でも、最初の三か月に行うべきことは三つに絞ることができる。

第一に、院内連絡責任者を一人決める。これは高度な技術者である必要はない。重要なのは、院内で情報を集め、ベンダーと連絡を取り、管理職へ報告する窓口を明確にすることである。第二に、主要システムのベンダー名、連絡先、保守契約書を集める。電子カルテ、医事会計、検査、画像、薬剤、ネットワーク、バックアップ、オンライン資格確認などについて、誰に連絡すればよいかを一覧にする。

第三に、外部接続とバックアップの書面診断を申し込む。病院内で詳細な技術調査ができなくても、ベンダーや外部専門家に書面で確認することはできる。

最初から完璧な対策を目指す必要はない。まず、自院の状態を見える化することが重要である。



図 8-2 最初の三か月に行う三つのこと

8-3 一年以内に行う八つの対策

三か月で自院の状態が見える化した後、一年以内に進めるべき対策を整理する。

第一に、外部接続一覧を整備する。

第二に、リモートアクセス、管理者 ID、ベンダー ID に多要素認証を導入する。

第三に、不要な接続や使われていない ID を削除する。

第四に、ネットワーク分離の方針を決める。

第五に、バックアップを消されにくい形にする。

第六に、復旧テストを行う。

第七に、電子カルテ停止時の紙運用訓練を行う。

第八に、サイバー攻撃時の院内連絡・判断・患者説明の手順を決める。

これらは一度に完璧に終える必要はない。しかし、優先順位を決め、期限を置き、病院として進捗を確認する必要がある。



図 8-3 一年以内に行う八つの対策

8-4 システム更新時に契約条件とすべきこと

病院情報システムの大きな対策は、日常運用だけでは進みにくい。最も重要な機会、電子カルテ更新、部門システム更新、ネットワーク更新、クラウド移行のタイミングである。この時に、サイバー対策を「オプション」ではなく、契約条件として確認する必要がある。確認すべき項目は、少なくとも次の八つである。

外部接統一覧を提出できること。

多要素認証に対応できること。

操作記録を残せること。

異常時に緊急遮断できること。

バックアップ方式と復旧手順を明示できること。

クラウド障害時の対応を示せること。

データを取り出せること。

責任分界を明文化できること。

システム更新時に契約条件として確認すべき事項が、病院管理職の重要な役割である。



図 8-4 システム更新時に契約条件とすべき八項目

8-5 国・病院団体・ベンダー・病院の役割分担

病院サイバー対策を個々の病院任せにするには限界がある。特に中小病院では、人材も予算も限られている。したがって、国、病院団体、ベンダー、病院がそれぞれの役割を担う必要がある。

国は、標準化、補助、ガイドライン、最低限防御パッケージ、クラウドネイティブ化のロードマップを整える必要がある。病院団体は、共同契約、相談窓口、研修、チェックリスト、共同監視や外部支援を利用しやすくする役割を持つ。ベンダーは、外部接続、認証方式、操作記録、バックアップ方式、復旧手順、緊急連絡、責任分界を明確に説明する責任がある。病院は、管理職が自院のリスクを理解し、優先順位を決め、対策を実行する責任がある。筆者は、国への提言として、個々の病院任せの限界、緊急防御と構造改革の二つの速度を説明し、共通照会票、最小機能、ロードマップ、役割分担、費用支援の必要性を訴えている。

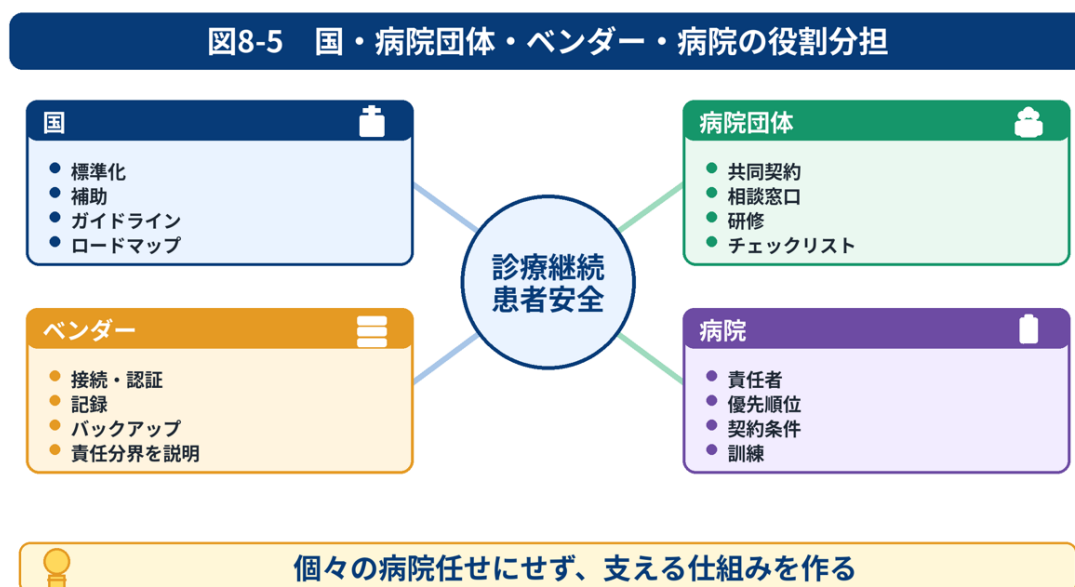


図 8-5 国・病院団体・ベンダー・病院の役割分担

8-6 病院管理職が確認すべきチェックリスト

最後に、病院管理職が自院で確認すべき問いを整理する。

外部接続は一覧になっているか。

リモートアクセスに多要素認証はあるか。

管理者 ID とベンダー ID は把握されているか。

退職者 ID や不要 ID は残っていないか。

電子カルテ系、事務系、インターネット系、バックアップ系は分けられているか。

バックアップは消されにくいのか。

復旧テストを行ったことがあるか。

電子カルテ停止時の紙運用訓練をしたことがあるか。

サイバー攻撃時の院内連絡責任者は決まっているか。

ベンダーの緊急連絡先は一覧になっているか。

このチェックリストにすべて「はい」と答えられる病院は多くない。重要なのは、現状を知ることである。現状が分かれば、優先順位を決められる。優先順位が決まれば、対策は始められる。

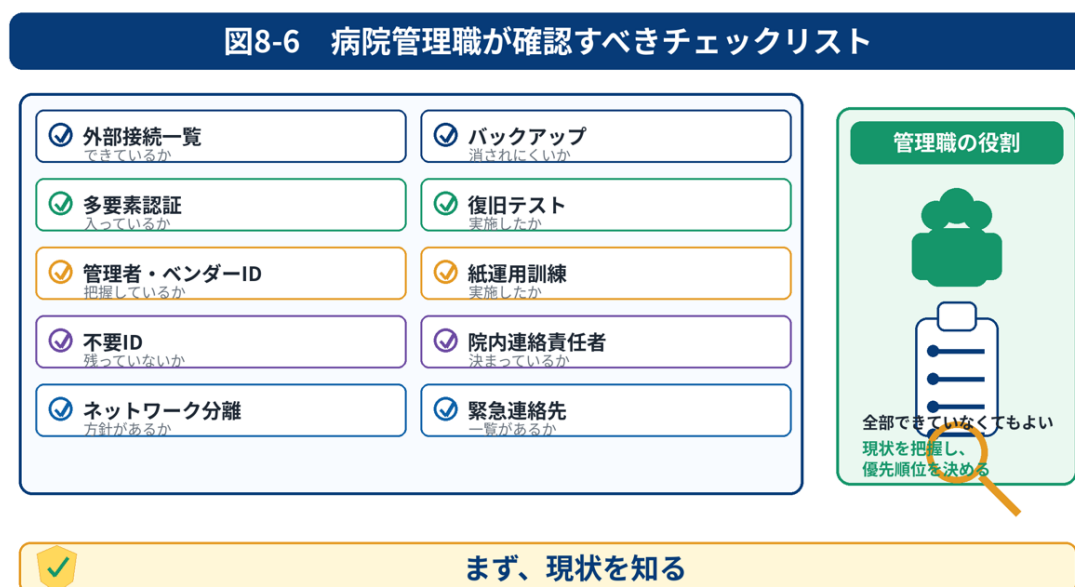


図 8-6 病院管理職が確認すべきチェックリスト

第 8 章のまとめ

病院管理職の役割は、専門技術をすべて理解することではない。自院のリスクを把握し、責任者を決め、ベンダー情報を集め、外部接続とバックアップを確認し、優先順位を決めることである。最初の三か月は見える化、一年以内は重点対策、システム更新時には契約条件として安全対策を組み込む。個々の病院だけで抱え込まず、国、病院団体、ベンダー、外部専門家の支援を活用することも重要である。

終章 今日から始める三つの行動

終-1 院内連絡責任者を決める

本書では、病院が狙われる理由、オンプレミス+穴の開いた閉域網、攻撃者の侵入プロセス、生成 AI による攻撃者の能力増幅、スイスチーズ型防御、オンプレミス病院の五つの対策、クラウドネイティブ化、共通接続管理基盤、管理職の役割を説明してきた。

しかし、講義や教科書を読んだだけでは、病院は安全にならない。最初に必要なのは、院内でこの問題を受け止める責任者を決めることである。高度な技術者である必要はない。院内情報を集め、ベンダーに確認し、管理職へ報告し、対策の進捗を管理する人を決めることが第一歩である。

終-2 外部接続一覧を作る

第二に、外部接続一覧を作ることである。

電子カルテ、医事会計、検査、画像、薬剤、オンライン資格確認、レセプト、ベンダー遠隔保守、クラウドサービスについて、どこが外部とつながっているのかを一覧にする。分からなければ、ベンダーに書面で確認する。

これは、すべてを閉じるためではない。必要な接続を安全に管理し、不要な接続を減らすためである。

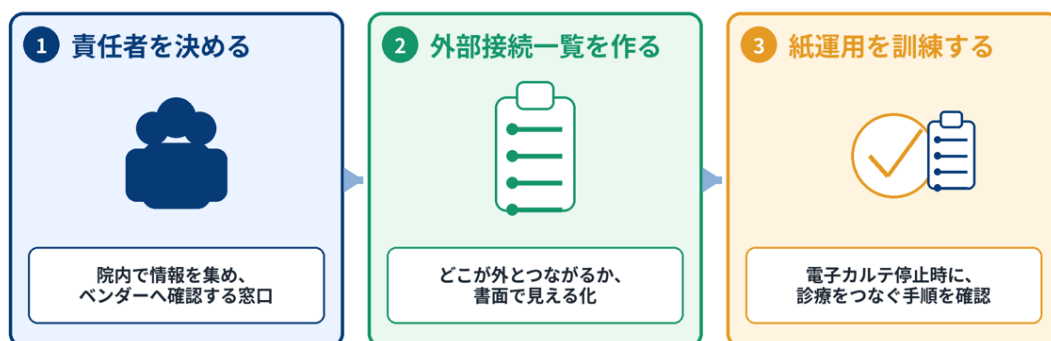
終-3 電子カルテ停止時の紙運用を一度訓練する

第三に、電子カルテ停止時の紙運用を一度訓練することである。

訓練をしない病院は、電子カルテ停止時に何が起きるか分からない。誰が判断するのか。救急を受けるのか。外来を止めるのか。入院患者の処方をどうするのか。検査依頼をどうするのか。会計をどうするのか。紹介状や退院調整をどうするのか。

一度訓練すれば、足りないものが見える。足りないものが見えれば、改善できる。

図終-1 今日から始める三つの行動



図終-1 今日から始める三つの行動

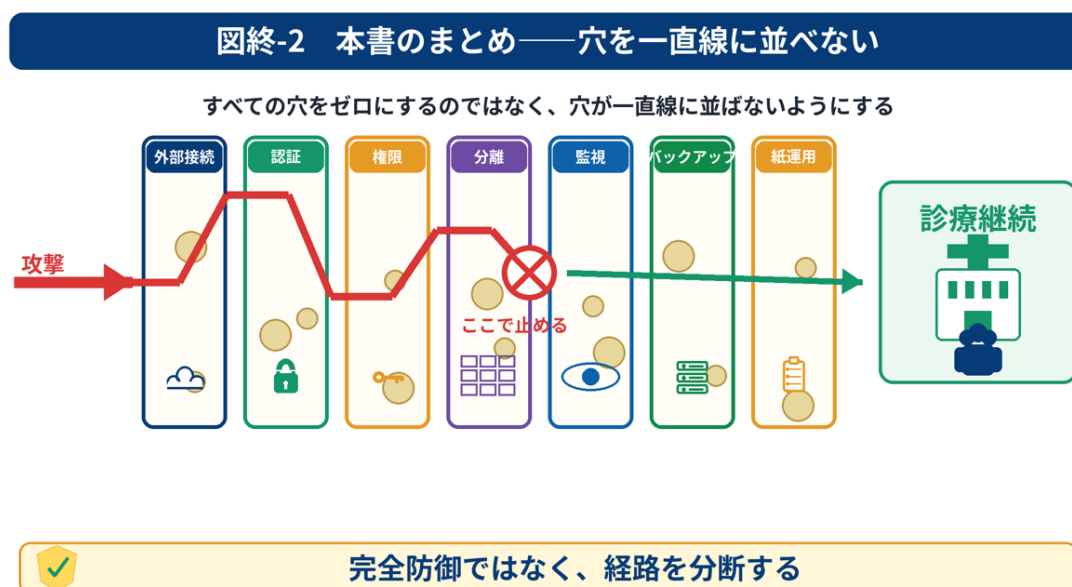
終-4 完璧を目指すのではなく、診療停止への経路を分断する

病院サイバー対策で最も重要な発想は、完璧を目指すことではない。もちろん、できる限りの対策は必要である。しかし、限られた人材と予算の中で、すべての穴をゼロにすることは難しい。

重要なのは、穴が一直線に並ばないようにすることである。外部接続で止める。認証で止める。権限で止める。ネットワーク分離で止める。監視で気づく。バックアップで戻す。紙運用で診療をつなぐ。どこかで止まれば、どこかで止まれば、診療停止に至る可能性を下げることができる。

本書の結論は、序章で示した一文に戻る。

生成 AI 時代の病院サイバー対策は、完全防御ではなく、診療停止に至る経路を分断する多層防御である。



図終-2 本書のまとめ——穴を一直線に並べない

終章のまとめ

今日から行うべきことは、難しい技術論ではない。院内連絡責任者を決める。外部接続一覧を作る。電子カルテ停止時の紙運用を一度訓練する。この三つから始めれば、自院の弱点が見える。弱点が見えれば、診療停止への経路を分断する対策を進められる。病院サイバー対策は、情報システムを守るだけでなく、患者安全と地域医療を守るための経営課題である。

第 3 部——病院の仕事をつなぎ、診療を止めないために——

第 2 部では、病院がサイバー攻撃を完全に防ぐことだけを目指すのではなく、侵入から診療停止に至る経路を、複数の対策によって分断する必要があると述べた。その対策は、病院だけでは完成しない。

病院には、医療機器を保守する事業者、検査や画像を支える事業者、給食、清掃、搬送を担う事業者、事務業務や情報システムを支える事業者など、多くの医療関連サービス企業が関わっている。事業者が病院からどのように依頼を受け、何を確認し、仕事の結果をどう返すかによって、病院の仕事の流れは変わる。また、事業者がどこから病院のシステムに接続し、障害時にどう対応するかによって、診療継続の条件も変わる。

第 1 部で考えた「つながる病院」と、第 2 部で考えた「診療を止めない病院」を実現するために、医療関連サービス企業には何が求められるのだろうか。

3-1 仕事を引き受けることから、仕事の流れをとともに作ることへ

医療関連サービスは、病院から依頼された仕事を正確に行うことで評価されてきた。給食を届ける。病室を清掃する。医療機器を点検する。その大切さは変わらない。ただ、病院 DX が進むと、自社の仕事を病院の情報システムや、その前後の仕事につなぐことも求められる。外部の検査会社とのやり取りは、その一例である。かつては紙で検査を依頼し、結果も紙で受け取っていた。病院の職員は、届いた結果を患者や依頼と照らし合わせ、必要に応じて電子カルテに入力していた。病院と検査会社のシステムがつながり、結果が電子カルテに届くようになると、こうした作業が減り、医師や看護師も結果を確認しやすくなった。



医療関連サービス（検査）が病院情報システムとつながり、業務が大きく変わった例

病棟では、体温計や血圧計の測定値を電子カルテに送る仕組みを導入する病院もある。看護師が測定値を紙に控え、後から入力する作業を減らせる。ただし、患者を正しく確認し、異常な値に対応するのは人の仕事である。機器を提供する企業には、病院の仕事に合うよう機器を安全につなぎ、使い続けられるよう支える役割がある。



今後、さらに大きな変化が期待できるのは、病床の運用である。退院予定や実際の退院時刻が清掃・リネン事業者伝われば、事業者は人員やリネンを前もって準備し、退院後すぐに作業を始められる。清掃とシーツ交換の完了を病院に返せば、病院は次の患者を迎える準備が整った病床を把握できる。予定変更も共有すれば、事業者は、退院予定の変更を早く知ること、清掃担当者やリネンの手配を無駄なく調整できる。病院は次の患者を迎えるまでの待ち時間を減らせる。医療関連サービス企業の新しい役割は、依頼された仕事を終えるだけでなく、その前後の病院の仕事も見て、よりよい流れをともに作ることである。

病院と事業者がつながると、病床の準備が早くなる



3-2 必要な情報を、必要な範囲で安全につなぐ

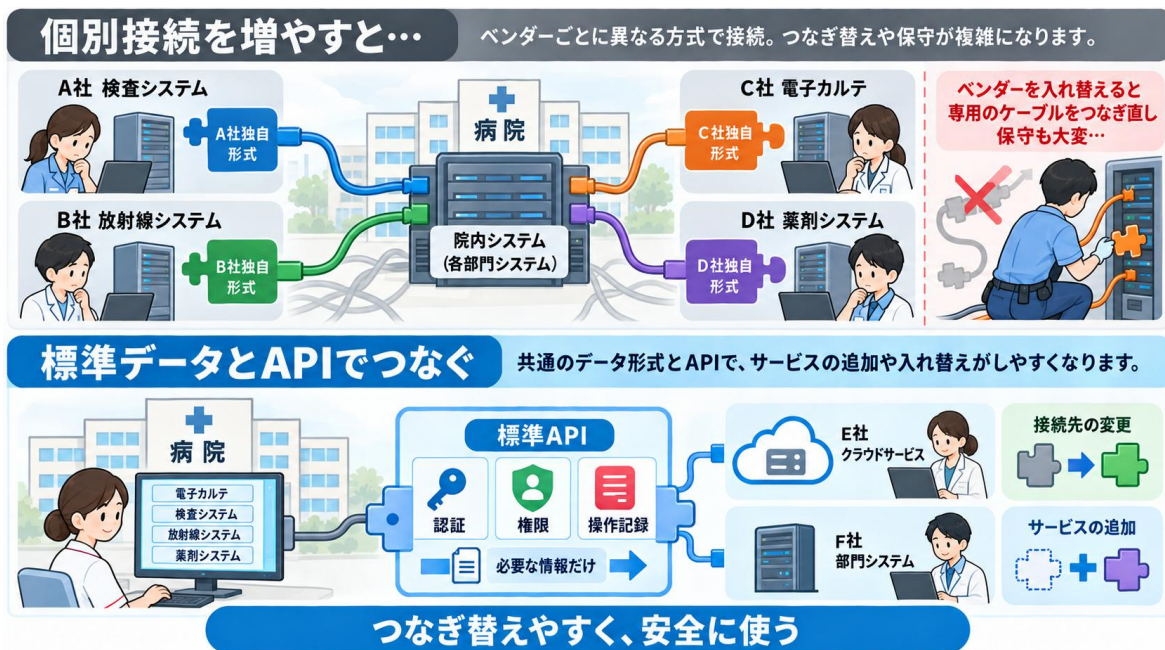
病院のすべての仕事が、電子カルテにつながる必要はない。また、すべての医療関連サービス企業が標準 API を持たなければならないわけでもない。まず確認すべきなのは、自社の仕事にどの情報が必要で、どの情報は必要ないかである。

例えば、清掃の担当者は、仕事の対象となる場所や実施時刻は必要だが、患者の詳細な診療情報は通常必要ない。一方、検査や画像などの部門サービスでは、患者や依頼を正しく識別し、結果を病院へ返すために、システム間の情報連携が重要になる。

このように、業種と仕事によって必要な接続は異なる。共通して求められるのは、「何のために、誰が、どの情報を、いつ利用するか」を病院と明確にすることである。



情報システムを提供する企業や、病院の部門システムと連携する企業では、標準に沿ったデータの扱いと API への対応が、将来の接続先の変更やサービス追加を容易にする。クラウドネイティブなサービスを利用する場合も、病院ごとに独自の接続を増やすのではなく、認証、権限、操作記録を管理しながら、必要な情報だけをやり取りすることが重要である。



一方、紙、電話、メールで依頼を受ける事業者であっても、情報の流れを改善する余地はある。病院と事業者が同じ依頼一覧を使い、仕事を頼んだか、事業者が受け付けたか、終わったかを互いに確認する。これだけでも、依頼漏れや同じ内容の二重入力を減らせる。技術の選択は、仕事をどう変えたいかという問いの後に置くべきである。



3-3 事業者は自社の接続を安全に管理し、病院の診療継続を支える

第2部で見たように、病院の外部接続や遠隔保守は、病院の業務を支えるために必要である。しかし、誰がどこから接続し、どの権限で何を操作できるのかが分からなければ、病院は自院のリスクを管理できない。

医療機器や情報システムの遠隔保守を行う企業は、病院に対して接続の入口、利用する ID、認証方法、操作の範囲、記録の残し方を説明できるようにする必要がある。不要な接続や使われなくなった ID を残さないこと、異常時に病院と協力して接続を止められることも重要である。

これは「安全です」と一言で説明する話ではない。例えば、事業者側の ID が悪用されたときに誰が気づき、誰が病院へ連絡し、どの接続を止めるのか。保守作業が必要なとき、誰が許可し、作業後に何を確認するのか。病院と事業者が、それぞれの役割を決めておく必要がある。



情報システムを使わないサービスにも、診療継続を支える役割がある。電子カルテが停止したとき、給食の変更はどう伝えるのか。清掃の優先順位は誰が決めるのか。情報システム会社だけが対応を準備しても、病院の仕事は続かない。各事業者が自社の代替手順を病院の訓練に持ち寄ることで、停止時に実際に動く手順を作ることができる。

3-4 「提供できる機能」に加えて「続けられる仕事」を示す

これから病院がサービスを選ぶ際には、平常時の機能や価格に加え、他の仕事との接続、安全な運用、障害時の対応を確認する場面が増えると考えられる。医療関連サービス企業にとって、これらは病院から質問されて初めて答える事項ではなく、自社の提供内容として準備しておきたい事項である。



病院へ説明する内容は、仕事に応じて異なる。情報連携を行う企業なら、扱う情報、接続方式、認証と権限、操作記録、データの取り出し方を示す。遠隔保守を行う企業なら、接続の管理、緊急連絡、停止と再開の手順を示す。給食、清掃、搬送などを担う企業なら、依頼と完了の受け渡し、予定変更への対応、システム停止時の代替手順を示す。

どの業種にも共通するのは、病院との責任分担を曖昧にしないことである。障害が起きたとき、誰が最初に連絡するのか。誰が仕事を止める、または続ける判断をするのか。復旧したことを誰が確認するのか。契約書や運用手順に書かれていても、現場の担当者が知らなければ役に立たない。平常時に確認し、必要に応じて一度試しておくことが重要である。

クラウドネイティブ化、標準 API、サイバー防御が「新たな市場条件になる」とは、すべての企業が同じシステムを導入するという意味ではない。病院の仕事につながる方法を持ち、その接続を安全に管理し、障害時にも自社が担う仕事をどう続けるかを説明できることが、取引先としての評価に関わるという意味である。

第3部のまとめ

生成 AI 時代の医療関連サービス企業は、病院から仕事を受けるだけでなく、病院の情報と仕事の流れをともに改善する役割を担う。必要な情報だけを安全につなぎ、事業者の接続を管理し、システムが止まったときにも自社の仕事をどう続けるかを病院と決める。その積み重ねが、病院 DX と診療継続をともに支える。

結び 医療関連サービス企業が今日から始める三つの行動

本日は、病院 DX によって「人が情報を探す病院」から「必要な情報が人に届く病院」へ変わることで、そしてサイバー対策によって、侵入から診療停止に至る経路を分断することを考えてきた。この二つは、病院の中だけで完結する話ではない。病院とともに働く医療関連サービス企業にも、具体的な行動が求められる。

第一に、自社と病院の間で、仕事と情報がどう行き交っているかを確認してほしい。依頼が届くまで、仕事を実施するまで、結果を返すまでに、電話で人を探し、紙を運び、同じ内容を入力し直しているところはないだろうか。まず一つの仕事をを選び、病院の担当者と、その流れを見えるようにする。

第二に、自社が病院へ接続する方法と、障害時の連絡・責任分担を確認してほしい。遠隔保守を行う企業は、接続の入口、ID、権限、緊急時に止める方法を示す。情報システムに接続しない企業も、病院のシステムが止まったとき、依頼をどう受け、自社の仕事をどう続けるかを確かめる。

第三に、病院と小さな改善か訓練を一つ実行してほしい。検査依頼を届ける方法を変える。清掃の完了を知らせる方法を変える。停止時に紙の依頼書で仕事を受ける練習をする。机上で決めた手順を一度使い、うまくいかなかったところを直す。そこから次の改善が始まる。

病院 DX の目的は、職員が本来の仕事に時間を使えるようにすることである。サイバー対策の目的は、患者の診療を守ることである。医療関連サービス企業が病院と一緒に情報の流れを変え、停止時にも仕事をつなぐことは、この二つの目的の双方に貢献する。

これからの医療関連サービス企業は、病院の仕事を引き受ける存在から、病院の仕事の流れと診療継続をともに作る存在へ進む。それが、生成 AI 時代の新しい役割である。

巻末資料（サイバーセキュリティ）

本書の五つの対策と、厚労省チェックリスト・BCP 確認表との対応

本書の五つの対策は、厚生労働省の公式チェックリストをそのまま置き換えるものではない。

本書では、病院管理職が実行順に理解しやすいように、公式チェックリストおよび BCP 確認表の関連項目を、五つの重点対策に整理し直している。

対策 1 外部接続の棚卸し

—「どこから外とつながっているか」を見える化する—

公式資料との対応

厚労省チェックリストとの主な対応項目

- 2-① サーバ、端末、ネットワーク機器の台帳管理を行っている。
- 2-② 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等に確認した。
- 2-③ 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。
- 2-⑬ アクセスログを管理している。
- 2-⑭ 接続元制限を実施している。
- 3-① インシデント発生時における組織内と外部関係機関への連絡体制図がある。
- 4-① 上記 1～3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。

これらは、台帳管理、リモート保守の把握、事業者確認、アクセスログ、接続元制限、連絡体制に関わる項目であり、本書の「外部接続の棚卸し」と対応する。チェックリストでは、リモート保守機器の有無、MDS/SDS、アクセスログ、接続元制限などが明示されている。

BCP 確認表との主な対応項目

- 1-1 情報機器等の把握と適切な管理、全体構成図の作成。
- 1-2 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集。
- 3-1 原因調査（必要に応じて事業者に依頼）。
- 3-2 事業者等への連絡と作業履歴の確認。
- 3-3 被害拡大防止。
- 3-6 組織対応方針確認と外部関係機関への報告等の対応。

BCP 確認表では、サーバ、端末 PC、ネットワーク機器の把握、ネットワーク構成図・システム構成図の整備、外部関係機関への連絡体制、原因調査、事業者連絡、被害拡大防止が確認項目として示されている。

対策 2 多要素認証の導入

ー「パスワードが盗まれても、それだけでは入れない」仕組みを作るー

公式資料との対応

厚労省チェックリストとの主な対応項目

- 2-④ 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。
- 2-⑤ 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している。
- 2-⑦ パスワードは英数字の混在した 8 桁以上としている。二要素認証を採用するまでの期間は 13 桁以上としている。
- 2-⑧ パスワードの使い回しを禁止している。
- 2-⑪ アプリケーションログイン時の二要素認証を実装している。または令和 9 年度以降初回のシステム更改時に実装予定である。
- 2-⑫ OS ログイン時の二要素認証を実装している。または令和 9 年度以降初回のシステム更改時に実装予定である。
- 2-⑬ アクセスログを管理している。
- 2-⑭ 接続元制限を実施している。

本書では「多要素認証」と表現しているが、厚労省チェックリストでは「二要素認証」と記載されている。アプリケーションログイン時、OS ログイン時の二要素認証、不要アカウントの削除、パスワード管理、アクセス権限設定が対応する。

BCP 確認表との主な対応項目

- 1-2 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集。
- 2-3 CSIRT／経営者によるシステム異常の覚知。
- 3-3 被害拡大防止。
- 3-4 経営層への報告、経営層による確認と指示、組織内周知と対応。

BCP 確認表には「多要素認証」という直接項目はないが、ID 悪用時の被害拡大を防ぐという意味で、異常覚知、被害拡大防止、経営層による使用中止判断と関係する。

対策3 ネットワーク分離

一院内に「防火区画」を作り、攻撃の横展開を防ぐー

公式資料との対応

厚労省チェックリストとの主な対応項目

- 2-① サーバ、端末、ネットワーク機器の台帳管理を行っている。
- 2-⑥ セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
- 2-⑨ USB ストレージ等の外部記録媒体や情報機器に対して接続を制限している。
- 2-⑩ 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。
- 2-⑬ アクセスログを管理している。
- 2-⑭ 接続元制限を実施している。
- 3-① インシデント発生時における組織内と外部関係機関への連絡体制図がある。
- 4-① 上記 1～3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。

ネットワーク分離そのものの語はチェックリスト上に大きく出ていないが、台帳管理、接続制限、不要サービス停止、アクセスログ、接続元制限が、ネットワークを無秩序につなげないための基礎項目として対応する。

BCP 確認表との主な対応項目

- 1-1 情報機器等の把握と適切な管理、全体構成図の作成。
- 3-1 原因調査（必要に応じて事業者に依頼）。
- 3-3 被害拡大防止。
- 3-4 経営層への報告、経営層による確認と指示、組織内周知と対応。
- 4-2 医療情報システム等の事業者等へ復旧対応依頼。

BCP 確認表では、ネットワーク構成図・システム構成図の整備、原因調査、被害拡大防止、経営層による医療情報システム使用中止等の判断が確認項目となっている。これらは、攻撃時にどこを遮断し、どこを残すかを判断するための基礎になる。

対策 4 消されにくいバックアップと復旧テスト

—「バックアップがありますか」ではなく「実際に戻せますか」を確認する—
公式資料との対応

厚労省チェックリストとの主な対応項目

- 2-① サーバ、端末、ネットワーク機器の台帳管理を行っている。
- 2-⑬ アクセスログを管理している。
- 3-② インシデント発生時に診療を継続するために必要な情報を検討し、バックアップを確保のうえ、復旧手順を確認している。
- 3-③ サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。
- 4-① 上記 1～3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。

この対策に最も直接対応するのは、**3-②「バックアップを確保のうえ、復旧手順を確認している」**である。厚労省チェックリストでは、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、バックアップを確保し、復旧手順を確認することが明示されている。

BCP 確認表との主な対応項目

- 1-2 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集。確認項目として「バックアップの実施と復旧手順が確認できているか」を含む。
- 4-1 経営層からの復旧指示の確認と実施。
- 4-2 医療情報システム等の事業者等へ復旧対応依頼。
- 4-3 再設定や再インストール、バックアップデータの復旧等。
- 4-4 復旧結果の確認。
- 5-1 復旧結果と情報漏えい事実の有無の報告。

BCP 確認表では、バックアップと復旧手順、復旧指示、事業者への復旧依頼、再設定・再インストール・バックアップデータ復旧、復旧結果確認が項目化されている。

対策 5 電子カルテ停止時の紙運用訓練

—通常診療を紙で完全再現するのではなく、止められない診療をつなぐ—

公式資料との対応**厚生労働省チェックリストとの主な対応項目**

- 3-① インシデント発生時における組織内と外部関係機関への連絡体制図がある。
- 3-② インシデント発生時に診療を継続するために必要な情報を検討し、バックアップを確保のうえ、復旧手順を確認している。
- 3-③ サイバー攻撃の想定を含む事業継続計画（BCP）を策定している。
- 4-① 上記 1～3 のすべての項目について、具体的な実施方法を運用管理規程等に定めている。

紙運用訓練は、チェックリスト上では「紙運用」という名称で直接出てくるわけではない。しかし、診療継続に必要な情報の検討、バックアップ確保、復旧手順確認、BCP 策定、連絡体制図の整備と密接に対応する。

BCP 確認表との主な対応項目

- 1-2 非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集。教育訓練、バックアップ実施と復旧手順確認を含む。
- 2-1 システム異常の報告先の把握。
- 2-2 システム異常の検知。
- 2-3 CSIRT／経営者によるシステム異常の覚知。
- 3-4 経営層への報告、経営層による確認と指示、組織内周知と対応。
- 4-1 経営層からの復旧指示の確認と実施。
- 5-1 復旧結果と情報漏えい事実の有無の報告。
- 5-6 外部関係機関への報告と情報公開の検討。

BCP 確認表では、システム異常の報告、異常の覚知、経営層による使用中止等の判断、復旧指示、復旧結果の報告、外部関係機関への報告が整理されている。紙運用訓練は、これらの項目を実際に動かせるかを確認する訓練として位置づけるとよい。

本対応表は、厚生労働省の公式チェックリストおよび BCP 確認表を、本書の五つの対策に沿って読み替えた整理である。公式な確認・提出・監査対応では、必ず最新版の厚生労働省チェックリスト、チェックリストマニュアル、BCP 確認表の原文を確認すること。