サイバーインシデント対策と医療安全

サイバー攻撃を受けた経験とその後の取り組み

徳島県 つるぎ町立半田病院
つるぎ町病院事業管理者　須藤 泰史

2024年6月6日
令和6年度　国公私立大学附属病院医療安全セミナー

サイバー攻撃は大きな災害！

- 半田病院を襲ったサイバー攻撃の概略
-
-
-

ランサムウェアによる攻撃を受けた当初の様子、初期対応

- 2021年10月31日午前0時30分頃　病院内の電子カルテと接続され、電源が入っている全てのプリンターから英文の犯行声明が印刷。印刷は、自動で開始され、プリンターの用紙がなくなるまで継続。
- 当直医師に電子カルテの不具合が報告され、システム担当者が午前3時ごろに駆けつけて対応を開始。ほどなく、ランサムウェアによるサイバー攻撃ですべてのシステムが使えなくなっていることが判明。
- 午前8時過ぎ病院上層部へ連絡。（県内の電子カルテ共有ネットワーク・等）および県警のサイバー犯罪対策室へ連絡。
- 午前10時災害対策本部を立ち上げ、第1回目の対策会議を開始。
- 午後4時、県内の報道機関に事件について記者会見。

対策本部立ち上げの経緯とメンバー、対応の方針

- 当初は、2Fの小会議室（収容30名規模）で本部立ち上げ。
  - 本部の主なメンバーは、幹部職員＋病院DMATで、組織図は、災害対策用に作成したBCPに基づいて行った。
  - 具体的には・・本部長：病院長、マスコミ対応：事務長、記録・調整要員：当院DMAT等

- 以降、3F大会議室（収容80名規模）に移動。
  - 感染したPCの集積（計200台・うち40台がウイルスに感染）
  - 業者とのミーティングエリア
  - 休憩所設置
  - 壁には一面のクロノロ
  - 基本方針・組織図・今後の見通し・電子カルテネットワークの現状と今後の復旧後の模式図等
  - 各部署の責任者とのミーティング（当初は、AM11時・PM5時の2回。土日もAM11時に開催。）

基本方針（当初10･31）

1.今いる入院患者を守る

2.外来患者は基本的に予約再診のみ

3.電カル復旧に努める

4.皆で助け合って乗り切ろう

基本方針（11･27～）

1.随時通常診療に戻していく（11/15 小児科･11/19 産科 通常診療再開）

2.電子カルテ稼働1･4を目指す（11/24 ベンダーより 1/4にBプラン完成）

3.皆で助け合って乗り切ろう！

院内でのコミュニケーションと院外との情報共有について、特に工夫したこと

- 本部ミーティングを毎日行い、情報共有を促した。特に各部門ごとの復旧への進捗状況や現状（医事会計ができない紙カルテベースの診療）での問題点・改善点などの報告・情報共有が有用であった。
  - それぞれの部署でもミーティングを開き、常に創意・工夫を行った。
  - 他の部署で取り入れる方が、いい方法や、改善点は、報告し合い共有。
  - 使用していなかった古いPC（外部から提供してくださるところもあった）を持ち出してプリンターと接続し、ワープロとして使用。

  ＊大量の文具・PC・コピー機能付きプリンターが必要！（トヨタイムズ　小島プレス）
- マスコミ対応は事務長に一本化し、取材などは、個別に応じないように対応。
- 毎日のクロノロ・会議録等は記録係が本部のPCに記録し保存。

紙カルテベースの診療

- 電子カルテシステムと画像・医事会計・検査・処方・透析・リハビリなど、あらゆるものがつながっており、 10月末にシステムがストップしたので、10月分の診療報酬請求もできず。11月～12月は、診療費の請求はせず診療。そして、もちろんその診療も「再来・予約患者のみ。救急・新規の対応は不可。手術・入院も急ぐもの・他院へ送れないもの・今の当院の状況で対応できるもののみ対応」を基本としている状況。
- 当時院内では、南海トラフ地震への対策で運用する予定で用意していた紙カルテベースの診療が稼働。大変不自由で、かかりつけであったなじみの患者さんにも、「いつから当院へかかっていました？　手術したのはいつ頃でした？　アレルギーは特になかったですよね？」などと聞くことに。門前薬局から過去の処方歴などの資料を頂いたり、当院から紹介した紹介病院から当院からの診療情報をFAXして頂いたりしながら、患者情報をかき集めて対応。

＊患者さんの反応はおおむね当院の大変さに理解してくれており、同情の声を頂くことも多く、また、これまでにお渡しした検査結果のコピーを持参してくれるありがたい方も多くあり、大変助かった。

最終的な被害状況と復旧までのプロセス

1. 診療体制：　小児科11･15～　産科11･19～　放射線科11･30～　消化器内視鏡検査12･1～　健診部門12･13～　通常診療再開。その他は2022年1月4日～再開。

   ● 10月～12月分は、レセプトは作れず診療報酬は請求できていなかった！

2. ハッカー攻撃に対する対応：　徳島県警のサイバー犯罪対策室と引き続き連携して対応中。（不正指令電磁的記録供用疑い）

   ① 犯人側からの具体的な要求等の連絡はない。

   ② サイバー攻撃を受けたルートに関しては現在も捜査中。

   ③「電子カルテシステムに入るためのIDとパスワードが犯人側に漏洩していることがダークサイトで判明。」と報道されたが、まだ攻撃ルートは判明していません。

最終的な被害状況と復旧までのプロセス

３．2022年1月4日からの再稼働（それぞれAプラン・Bプラン・Cプランと呼称）

A)　感染したシステムの復旧（専門の業者に委託）

B)　レンタルサーバーでの同じ電子カルテシステムの再構築：電子カルテから取り出していた医事会計のデータ・新型コロナワクチン接種のための患者データなどがすぐに流用できること。また、攻撃にあったデータが復旧すればすぐに取り込めること。職員には慣れたシステムであることから

C)　別ベンダーの電子カルテシステムの導入は半導体不足でサーバーが手に入らないこと、SEが不足していることから断念

＊幸いにして、調査復旧を請け負った事業者の作業（Aプラン）や電子カルテ業者の仮システムの構築（Bプラン）、そして電子カルテより必要に応じて抽出していたデータなどを利用し、令和4年1月4日の通常診療の再開にこぎつけることが出来ました。

2022年1月4日通常診療再開以降の対応

- 紙ベースでの診療の電子カルテ入力
  - 11月～12月（10･31～1･4）までは医事会計システムと連動していない紙カルテの診療。（レセプトは作れず診療報酬は請求できていなかった！）
  - 10･31の分は早急に入力し、1/10にようやく10月分の診療報酬を請求
  - 11月～12月で紙カルテは約5000冊。これを2022年1月4日以降、復旧した電子カルテシステムに手入力し、診療報酬請求書を作成した！
  - 11月分は、何とか2/10に請求、12月分は3/10に。
  - 1月～3月は、4/10にまとめて請求！5月20日に入金あり！

各部門の被害状況調査　1

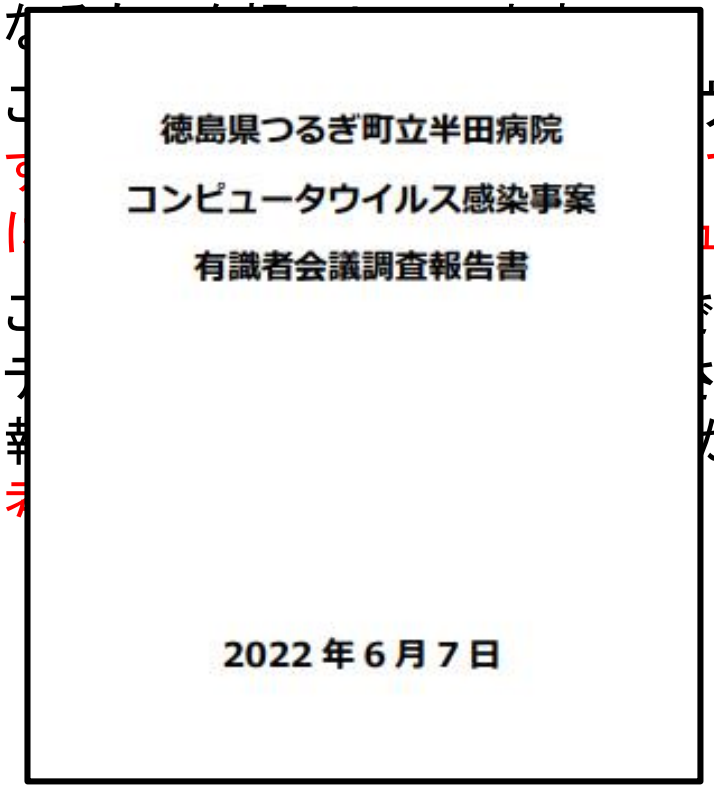
- 紙カルテの記録が慣れていない
  - 記載の仕方がわからない。整理ができない（置く場所が沢山必要で部屋が狭くなる）。手間がかかる等。
  - 誰かがカルテを持ちだしていると他のものが確認できない。紙カルテを使用していた頃と異なる書類が増加。
  - 細かい紙カルテの運用が統一されていない。どこまで物品請求していいのか？
  - 身体への影響・手の疲労・パソコン入力に慣れており、文字が出てこない。誤字・脱字が多く時間をとられる。
  - 患者ファイルにプロファイル・入院時医師指示をプリントアウトしておいてよかった。各個人の申し送りのメモやリーダー板（個々の患者情報の宝庫）が役に立った。
- 生命保険診断書・傷病手当・介護保険主治医意見書などの作成の際に、初診日が不明などで作成できない！
- 検査は手入力で採血項目を入れるので抜けもあり、手間と時間がかかる。また、検査結果を検査技師が手で運ぶ。
- レントゲンはフィルム印刷（MRIをフィルムで欲しいという医師がまだいたおかげ）。過去の画像との比較ができない。IDの転記ミス（数字が読み取れない。入力で間違っても機械がはじいてくれない。依頼文の文字が読めない（特に英語）。紙・フィルムの運搬にとにかく歩く。CDの持ち出しにウイルスチェックをするので待ち時間が長くなった。
- 処方箋が手書きで、カーボン紙。調剤薬局からの確認の電話が増えた！
- 受付で聞きとりに時間と人がとられ（高齢者は自分のことを知らない（病名・化学療法歴・検査結果等）、結果を紙で張るのに時間がかかる。紙が多すぎる。カルテ・予約情報の整理整頓ができにくい。紙・のり・インクなどの文具費用が相当掛かっている！
- コストの取り方がわからない：〇特（特定疾患）の記載漏れ等。リハシステムでは自動で点数計算がされていたことが出来ないため間違う可能性あり（実施時間や加算など・・）

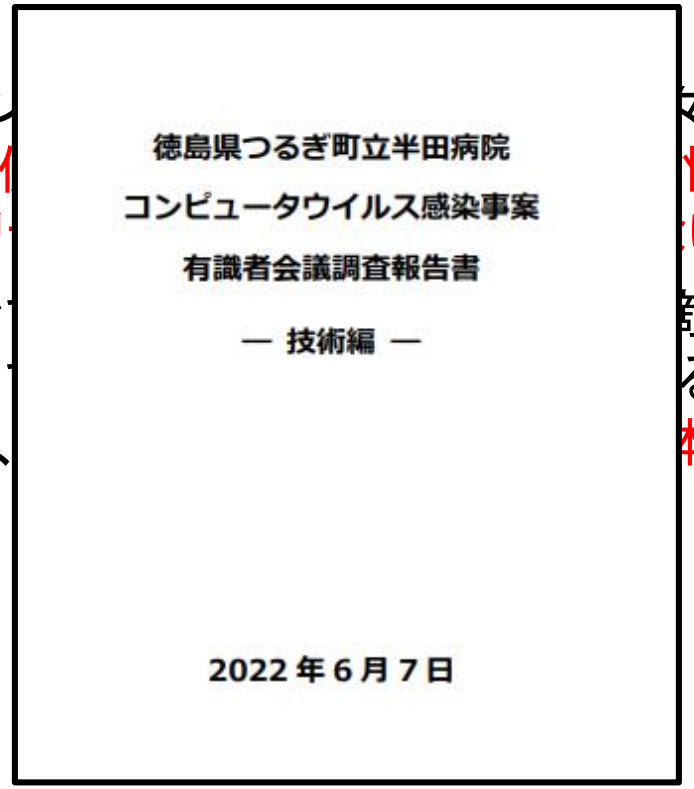
各部門の被害状況調査　２

- あと何人で受付が終了か、今患者が検査中・診療中なのかも不明。
- 他科受診等の情報共有（内服薬・アレルギー等）ができない。
- 明日来る予約患者がだれか不明！電話対応に困る。検査情報も不明。
- 本人確認しづらい。例）入籍して姓が変わっているのに旧姓での予約をしており、検索にかからない。
- カルテの検索は一苦労（手作業でカルテのボックスから探す）。
- 検査を延期できるかを外来に一度行っていただかなくてはいけないので患者に負担あり。
- 事情を知らずに来院した患者への説明や理解を得ることが難しかった。
- 健診部門：予約の人全員（350人くらい）に健診を止める旨を説明し、一旦ストップ。→連絡先・職場不明が多数あり。健診再開で、350人の振り替えの連絡、案内・各検査伝票（手書き）の準備に時間と手間。健診結果（10月分）が未送の方へ手書きで結果と基準範囲を比べながら結果を作成、判定・発送に時間がかかった。
- 患者サポート室：
  - 転院時に必要な退院証明が発行できない。
  - 入院受け入れを断るも、他院からの受け入れ要請が数件あった。押しが強く断る理由を伝えることに難渋した。
  - **患者情報を得るため過去の紹介状を探す作業が必要**、患者自身からの情報が実際とは異なることも多く難渋。
  - 11月以降、スキャンできていない紹介状が約400枚あり、名簿を作成し科別・あいうえお順に保管。
  - 紹介状のコピーを紙カルテに貼付するが、紙カルテが返却された夕方に作業を行うため時間外となる。
  - 訪問看護ステーション・ケアマネからの相談に患者データがなく回答に時間を要した。
- **12月医療安全委員会報告数23件中19件が紙カルテ運用でのミス（ノリ・Box・手渡しケース・ID入力等）**

最終的な被害状況と復旧までのプロセス

4. 有識者会議を2/4・2/28・3/28・5/20に開催（計4回）。3/12～13 、3/28～29の2回現地調査。5月20日に第4回有識者会議で最終とりまとめを行い、6月初めに報告書を完成。
   - 6月7日つるぎ町議会で説明し、6月16日に報告書を当院HPで一般公開。
   - 報告書には、他に、**報告書（技術編）**や**「情報システムにおけるセキュリティ・コントロール・ガイドライン」**も併記し、サイバーセキュリティに関して知識が不十分である病院関係者が業者と交渉する際の指標と
   -
   -





最終的な被害状況と復旧までのプロセス

4. 有識者会議を2/4・2/28・3/28・5/20に開催（計4回）。3/12～13 、3/28～29の2回現地調査。5月20日に第4回有識者会議で最終とりまとめを行い、6月初めに報告書を完成。
   - 6月7日つるぎ町議会で説明し、6月16日に報告書を当院HPで一般公開。
   - 報告書には、他に、**報告書（技術編）**や**「情報システムにおけるセキュリティ・コントロール・ガイドライン」**も併記し、サイバーセキュリティに関して知識が不十分である病院関係者が業者と交渉する際の指標となるものを提示しています。
   - これらすべては、当院HPよりダウンロードできます。有識者の方々からは、電子カルテは閉域網で使用するものではなく、外とつながって使用される状況であり、また、外とつながることでup to dateなシステムにできることから、より深くセキュリティに取り組まなければいけないことを教えていただきました。
   - この報告書には、我々が対応できていなかったこともたくさん指摘されていますが、広く日本の電子カルテにおける問題も提起してくださっています。本来なら今後どうするかの具体的な対策も述べて皆様にご報告するべきだったと思いますが、まずはこれらを世に出して日本の医療機関の改善に貢献できればと考え公開するものです。

なお、被害総額は？　復旧・新たなシステム作りに2億円～・入院・外来制限による診療報酬の減収が2021年11月・12月の二か月では数千万程度～（あくまで試算ですが・・）

TOPページ - 医療機関向けセキュリテ

https://mhlw-training.saj.or.jp

https://mhlw-training.saj.or.jp/

医療機関向け

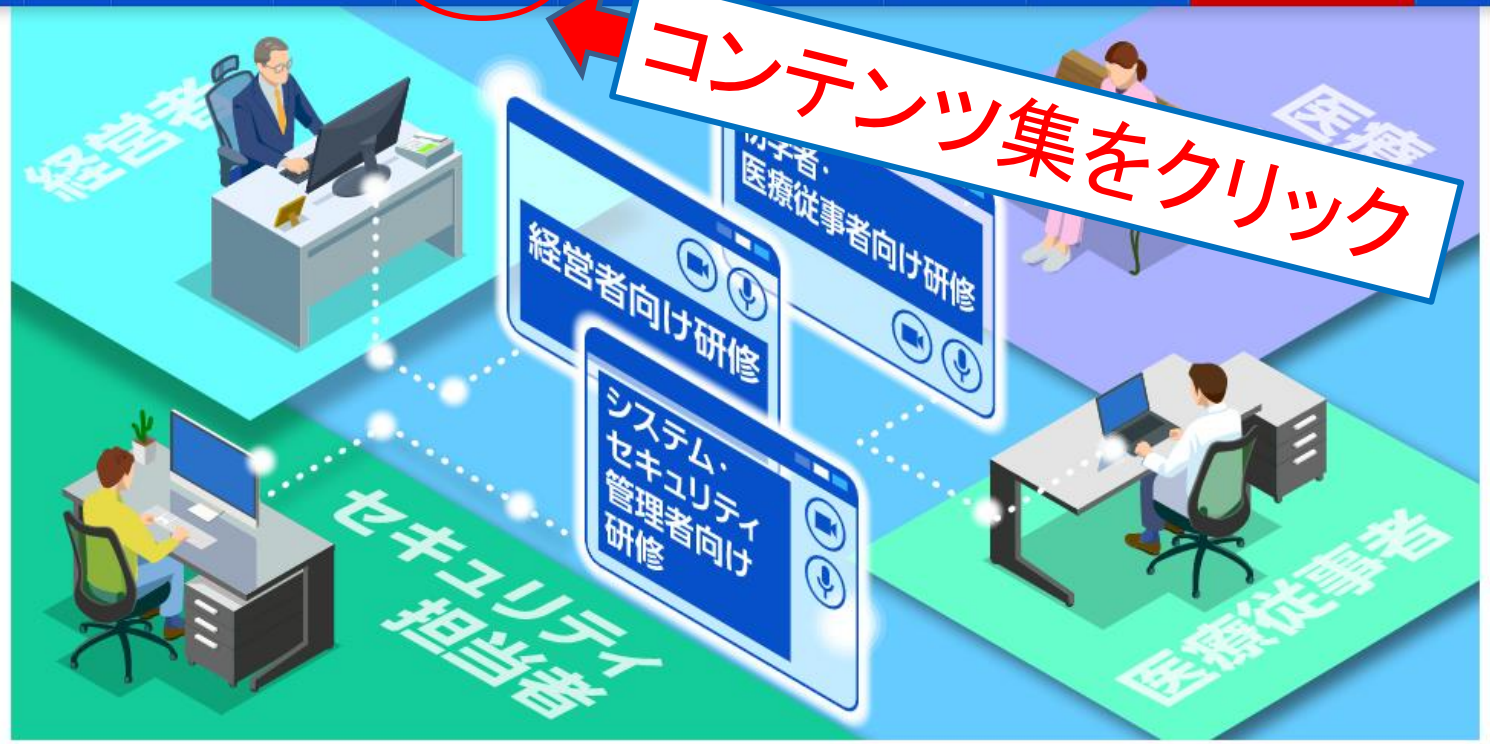
セキュリティ教育支援ポータルサイト

Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

事業について | 研修内容 | コンテンツ集 | コラム | 講師・技術者リスト | 関連リンク | お問い合わせ | インシデントかも？

コンテンツ集をクリック



お知らせ

ここに入力して検索

TSLA -4.99%

21:30
2023/03/10

サイバー攻撃は大きな災害！

- 半田病院を襲ったサイバー攻撃の概略
- サイバーセキュリティを高める！
  - バックアップは確実に
  - セキュリティー情報の取得
-
-

これまでに検討している内容　２

事　務　連　絡
令和３年６月28日

各都道府県衛生主管部（局）　御中

厚生労働省政策統括官付サイバーセキュリティ担当参事官室

厚生労働省医政局研究開発振興課医療情報技術推進室

厚生労働省医薬・生活衛生局医療機器審査管理課

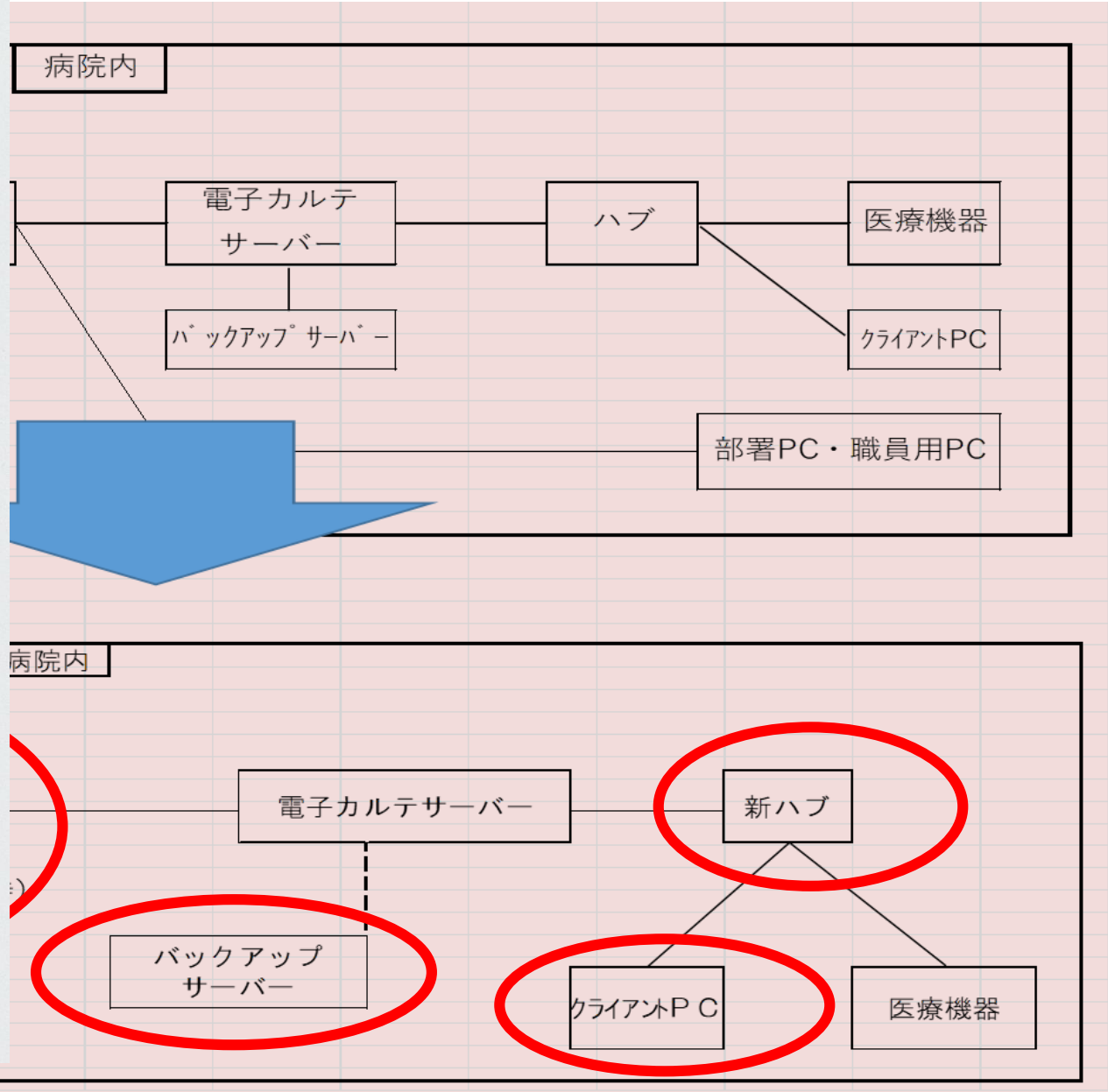
厚生労働省医薬・生活衛生局医薬安全対策課

医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）

近年、国内外の医療機関を標的とした、ランサムウェアを利用したサイバー攻撃による被害が増加している（別添１参照）。ランサムウェアによるサイバー攻撃は国境を超えて実行されており、我が国においても、世界各国と同様にリスクが高まっているところである。医療機関の情報システムがランサムウェアに感染すると、保有する情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなって診療に支障が生じたり、患者の個人情報が窃取されたりする等の甚大な被害をもたらす可能性がある。

また、新型コロナウイルスに関連した医療機関へのサイバー攻撃や７月から開催されるオリンピック・パラリンピック東京大会においても、大会関係機関等を狙ったサイバー攻撃等が予見されるところである。

ついては、４月30日付けで発出された内閣官房内閣サイバーセキュリティセンターからの注意喚起（別添２参照）について、改めて、貴管内の医療機関に対し周知するとともに、下記に示したランサムウェアによるサイバー攻撃の解説及び対策例を参考に、関係医療機関に対し注意喚起をお願いする。



再発防止に向けてこれまでに検討している内容　①

- 有識者会議のメンバー（Software ISAC)の指摘を基に、当院の電子カルテのベンダーとシステムを構築したベンダーも交え、新たな電子カルテシステムの作成に取り組みました。
- 昨年度より新規運用を開始しております。

（＊この結果で、最終的な復旧費用が増額される可能性あり。）

- この経過・詳細については、追って有識者会議報告書の第二版（仮）としてご報告する予定です。

セキュリティ対策について、参加者に伝えたいこと

- 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（2020年8月　総務省・経産省）
  - ３．１．２　対象事業者の説明義務 医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべ きである。このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために 必要な情報を適時適切に提供する義務を負う 。

いつも講演では、このGLのことを当院の事例を検討してくれた有識者の先生方に教えて頂いたと。有識者の先生からも、医療関係ではないけれども、このベンダーの善管注意義務を根拠に訴えて、サイバー攻撃の事案で勝訴した事例があることなどを教えて頂きましたが、GLは法律でないのでそこまで拘束力はないとも教えて頂きました。

医療情報を取り扱う情報システム・サービスの
提供事業者における安全管理ガイドライン
第 1.1 版

令和２年８月
（令和５年７月改定）

いて、参加者に伝えたいこと

業者における安全管理ガイドライン（2020年8月　総務省・経産省）

①～③のために適切に情報を取得する必要がある。しかし、医療機関等
門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療
事業者であり、セキュリティに関する専門的な知識・経験・人材を擁してい
事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務
行するために 必要な情報を適時適切に提供する義務を負う 。

そんな自分の講演での話が聞こえたのか
は解りませんが・・・。
つい最近新しいガイドラインが出ました！

3. 医療情報の安全管理に関する義務・責任

本章では、医療機関等及び対象事業者がそれぞれ負う義務と責任を法律に基づいて整理する。また、医療情報システム等のライフサイクルを構成する要素ごとに義務と責任を説明する。

3.1. 法律関係

3.1.1. 安全管理義務

(1) 善管注意義務と守秘義務

患者と医療機関等は、診療契約を締結し、医療機関等は診療契約（準委任契約）上の善管注意義務を負う。患者は、診療契約に基づいて、医療機関等に自己の医療情報を委ねているといえるため、医療機関等は、善管注意義務の一内容として、情報を適切に取り扱う義務を負っている。

また、医師等の医療従事者は、患者に対し、刑事上の守秘義務（刑法 134 条等）を負っている。医療機関等も、患者に対し守秘義務を負っていると解釈されている。この医療従事者及び医療機関等の患者に対する守秘義務は、故意による情報開示・漏洩（えい）だけではなく、過失による情報開示・漏洩（えい）も対象としていると解される。

このように、医療機関等は、患者に対して善管注意義務及び守秘義務を負っており、その内容は重なりあう。そして、いずれも適切なセキュリティ体制を構築、維持、運用する義務（以下、「安全管理義務」という。）を含む。

また、対象事業者は、医療機関等と委託契約を締結しているが、これが準委任契約である場合は、医療機関等に対し善管注意義務を負う（民法 644 条）。契約の形式が準委任契約でない場合（請負契約等）においても、医療情報の取扱いを委託する以上、当該委託契約には他人の事務の処理の委託関係という準委任契約の要素が含まれており、対象事業者は、善管注意義務又はこれと実質的に類似の義務を負う。また、契約上、守秘義務が規定されるのが一般的である。このような善管注意義務及び守秘義務には、契約内容及びその解釈によって定まる一定の事項についての安全管理義務が含まれる。

したがって、対象事業者は、医療機関等に対し、一定の事項についての安全管理義務を負っており、患者との関係では、医療機関等の患者に対する安全管理義務（の一部）の履行補助者の地位に立っている。

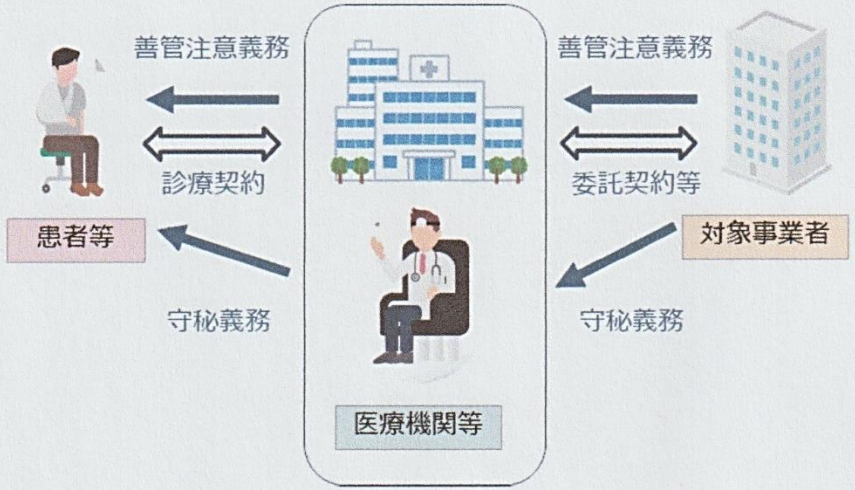


図 3-1 善管注意義務と守秘義務について

(2) 安全管理措置を講じる義務

個人情報保護法では、医療機関等と対象事業者は、それぞれその取り扱う個人データの安全管理のために必要かつ適切な措置を講ずる義務を負う（個人情報保護法 23 条[13]）。そして、医療機関等が対象事業者に対して個人データの取扱いを委託している場合、委託元は、委託先においてその取扱いを委託した個人データの安全管理が図られるよう、委託先を監督する義務（以下、「監督義務」という。）を負うと規定されている（個人情報保護法 25 条[14]）。

監督義務の内容としては、①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握という 3 点が挙げられている[15]。

前回のGLより、さらに法律の根拠に基づいてこのGLはあります。遵守すべき法的な義務的な意味をより強く書いているように感じます！

5.1.6. リスクコミュニケーション

(1) 医療機関等とのリスクコミュニケーションの実施

対象事業者は、自らが提供する医療情報システム等の安全管理に係る説明義務を果たし、医療機関との共通理解を形成するために、医療機関等に対して第 4 章で情報提供すべき内容として示した事項を含む必要な情報を文書化して提供すること。具体的には、5.1.5 で作成した「リスク対応一覧」や後述の運用管理規程に定められた事項に係る情報提供を通して、医療機関等との役割分担、対象事業者として受容したリスクの内容等について、医療

このGLには、我々には何の通知も特になかったですが、半田病院の事例が紹介されています。やはり自分は“しくじり先生”としての役目かも！？

意形成を図り、合意すること。

【コラム：リスクコミュニケーション不足がサイバー攻撃による被害発生の一因となった例】

通常時や非常時へ対応するために、医療機関等と医療情報システム等事業者の間でリスクコミュニケーションを行い、リスク内容やその対応に関する認識や、両者での責任分界などについて共通理解を得ることが求められる。特に昨今のサイバー攻撃に対しては、両者の間で不一致がある場合、行うべき対策が漏れてしまう危険性もある。

その事案例として、「徳島県つるぎ町立半田病院」において発生したランサムウェア攻撃による被害事案を紹介する。本事案ではランサムウェアによる被害により、長期間診療が停止したほか、復旧に多額の費用を要した。また、その原因を分析するための報告書が示されている[34]。

以下では同報告書において、課題として挙げられている内容をまとめた。この中では、いくつかの点について、医療機関等と事業者の間でリスクへの対応などについてのコミュニケーションが不足し、それが原因となって適切な対策が講じられなかったことがみられる。

1. 責任分界上の課題
   - 医療機関と事業者の間でのセキュリティ対策及び緊急時の対応に関する責任分界や委託業務範囲が不明瞭
   - 機器等の管理（脆弱性対策）に関する管理責任の範囲が不明瞭
   - 電子カルテシステム等を導入した事業者と保守事業者の間での責任分界が不明瞭
   - セキュリティ情報の取り扱いに関する当事者間での責任分界が不明瞭
2. 初動対応上の課題
   - 初動に関する全体的な対応計画が不足（事業者における情報不足に伴う不適切な対応等）
3. サービス提供上の課題
   - 事業者における脆弱性情報の取り扱いに対する知見不足
   - 情報セキュリティにおける脅威対応への知見不足を補うための体制構築
   - 情報システム・サービスの運用において考慮すべき基本的セキュリティ（機密性）についての意識不足（可用性優先に伴い、脆弱性対策がおろそかになっていた）と、これに関する医療機関側との共通認識が不足
4. 設計上の課題
   - 「医療情報システムの安全管理に関するガイドライン」に示す安全対策への未対応（バックアップ対応等）及び代替策に対する対応不足への認識が不明瞭（リスクコミュニケーション不足）

セキュリティ対策について、参加者に伝えたいこと

- 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（2020年8月　総務省・経産省）
  - ３．１．２　対象事業者の説明義務 医療機関等は、上記①～③のために適切に情報を取得する必要がある。しかし、医療機関等は医療の専門機関であって、セキュリティについての専門性は乏しいことが十分に想定される。これに対し、対象事業者は、医療機関等に対し専門的な医療情報システム等を提供する事業者であり、セキュリティに関する専門的な知識・経験・人材を擁しているべ きである。このような専門性の格差に鑑みて、対象事業者は、医療機関等に対し、委託契約又は信義則に基づく付随義務として、医療機関等が患者に対する安全管理義務を履行するために 必要な情報を適時適切に提供する義務を負う 。
- 医療情報システムの安全管理に関する　ガイドライン5.2 （2022年3月　厚生労働省）
  - 付表1～3　がひな型で利用しやすい。システム管理者・情報システム委員会・監査責任者・運営責任者等
  - ４．２．１　委託における責任分界：委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は、患者に対する関係では、受託する事業者の助けを借りながら、前節に掲げた「説明責任」、「管理責任」及び「定期的に見直し必要に応じて改善を行う責任」を果たす義務を負う。万一、何らかの不都合な事態が生じた場合にも同様に、受託する業者と連携しながら「説明責任」及び「善後策を講ずる責任」を果たす必要があるため、受託する事業者との契約において、受託する事業者の義務を明記すべきである。また受託する事業者の責任によって不都合な事態が生じた場合に、受託する事業者との間で「善後策を講ずる責任」をどのように分担するかについても、受託する事業者との契約で明記すべきである。

BCP策定に関して（病院がすべき必須事項時なりました！）

2022年11月24日　保健所の医療法第25条第1項の規定に基づく立ち入り調査

サイバーセキュリティ対策について

（1）医療情報システム（＊）を利用してい

＊医療情報システム・・医療に関す（電子カルテ、レセプトコンピューター　等）

（1）が「はい」の

①PCやVPNの脆弱性情

②それに対す

③診療継続に必要な情

④バックアップシス

⑤不正ソフトウェア対策

に基づく訓練

⑧ベンダーとの連携

⑨行政（県や厚労省）への連絡体制

ガイドライン　6.0
チェックリストの
記載義務

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

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

○　令和５年度中

*以下項目は令和５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。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
1 体制構築	（1）　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	（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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（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している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（6）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	（7）　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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（8）　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
3 インシデント発生に備えた対応	（1）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）			

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

医療機関におけるサイバーセキュリティ対策チェックリスト

事業者確認用

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
1 体制構築	（1）　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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（2）　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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（3）　医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	（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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（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している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（6）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	（7）　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。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（8）　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

事業者名：＿＿＿＿＿＿＿＿＿＿

- 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

【告知】医療分野におけるサイバーセキュリティに関する情報共有体制の構築

産官学連携企画　第43回医療情報学連合大会　11月25日（土）14:00～16:00　A会場

みんなでつくるセキュリティの医療現場改革に向けて　情報共有体制の重要性

オーガナイザー　木村　通男　（川崎医療福祉大学）
座長　武田　理宏　（大阪大学）

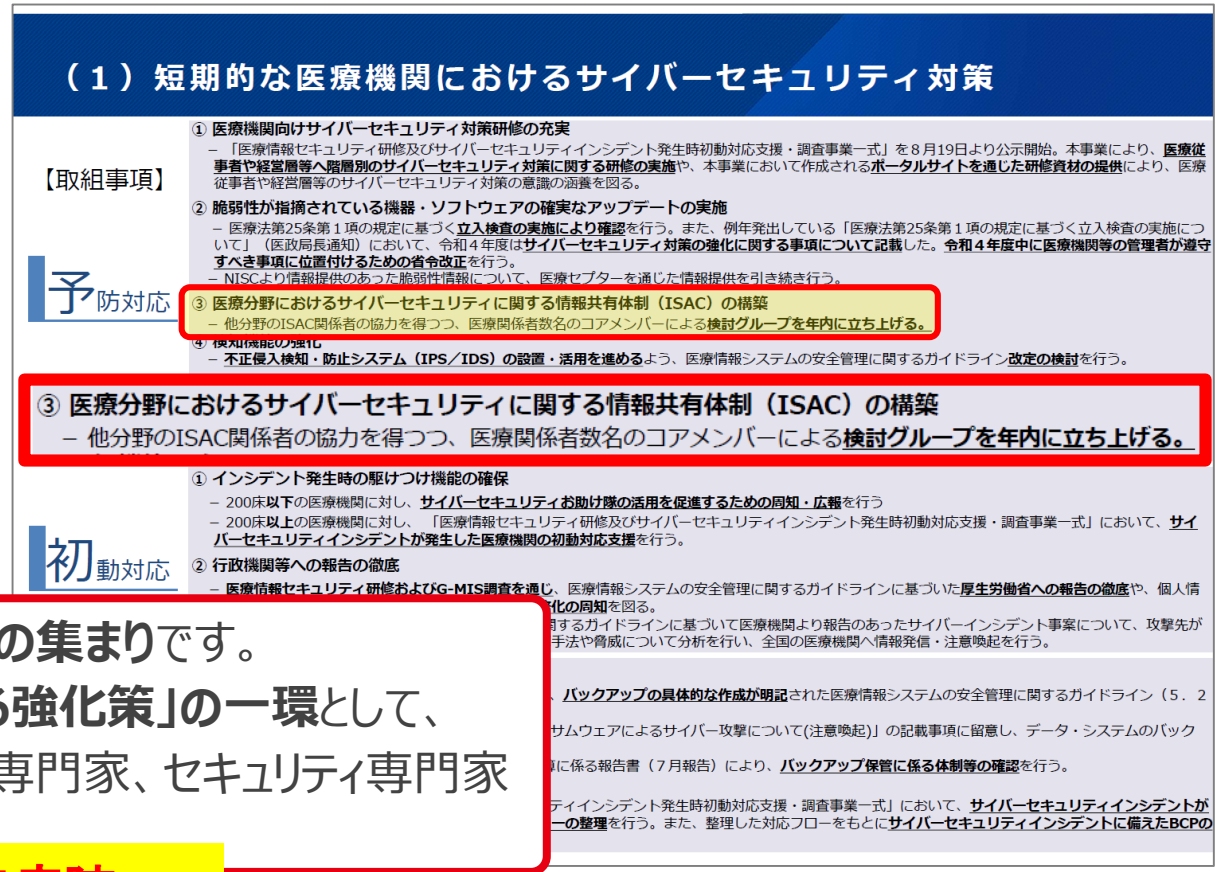
4-A-4-01　医療分野におけるサイバーセキュリティ対策の厚生労働省の取組について
新畑　覚也　（厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室）

4-A-4-02　医療情報技師の観点からの医療分野のISACの必要性
谷川　琢海　（北海道科学大学）

4-A-4-03　医療分野における医療機関関係者・医療従事者を中心としたISAC設立に向けた検討
大谷　俊介　（誠馨会 千葉中央メディカルセンター）

4-A-4-04　ISAC等で使用するサイバーセキュリティに関連する情報共有ツールSIGNALに関して
洞田　慎一　（JPCERTコーディネーションセンター）

CISSMED（シスメド）
Cyber Intelligence Sharing SIG for Medical
※SIG: special interest group



医療機関が主体となってサイバーセキュリティについて考える有志の集まりです。
厚生労働省「医療機関におけるサイバーセキュリティ対策の更なる強化策」の一環として、
医療機関職員(医師・コメディカル・事務職員)、他分野のISACの専門家、セキュリティ専門家からなるメンバーで結成しました。

大津赤十字病院
橋本 智広氏より提供

出典：第12回健康・医療・介護情報利活用検討会
医療等情報利活用ワーキンググループ（2022年9月5日）
医療機関におけるサイバーセキュリティ対策の更なる強化策（厚生労働省）
https://www.mhlw.go.jp/content/10808000/000985159.pdf

【告知】医療分野におけるサイバーセキュリティに関する情報共有体制の構築

CISSMED（シスメド）
Cyber Intelligence Sharing SIG for Medical
※SIG: special interest group

<コアメンバー>

大谷俊介	千葉中央メディカルセンター 、CISSMED代表
鎌田敬介	金融ISAC
近藤博史	協立記念病院、日本遠隔医療学会
須藤泰史	つるぎ町病院事業管理者
谷川琢海	北海道科学大学
橋本智広	大津赤十字病院
長谷川高志	日本遠隔医療協会
洞田慎一	JPCERTコーディネーションセンター
宮内雄太	金融ISAC

※50音順（2023年10月現在）

情報共有ツール「SIGNAL(JPCERT/CC)」を用いて、医療現場の担当者が情報共有できる環境を提供します。

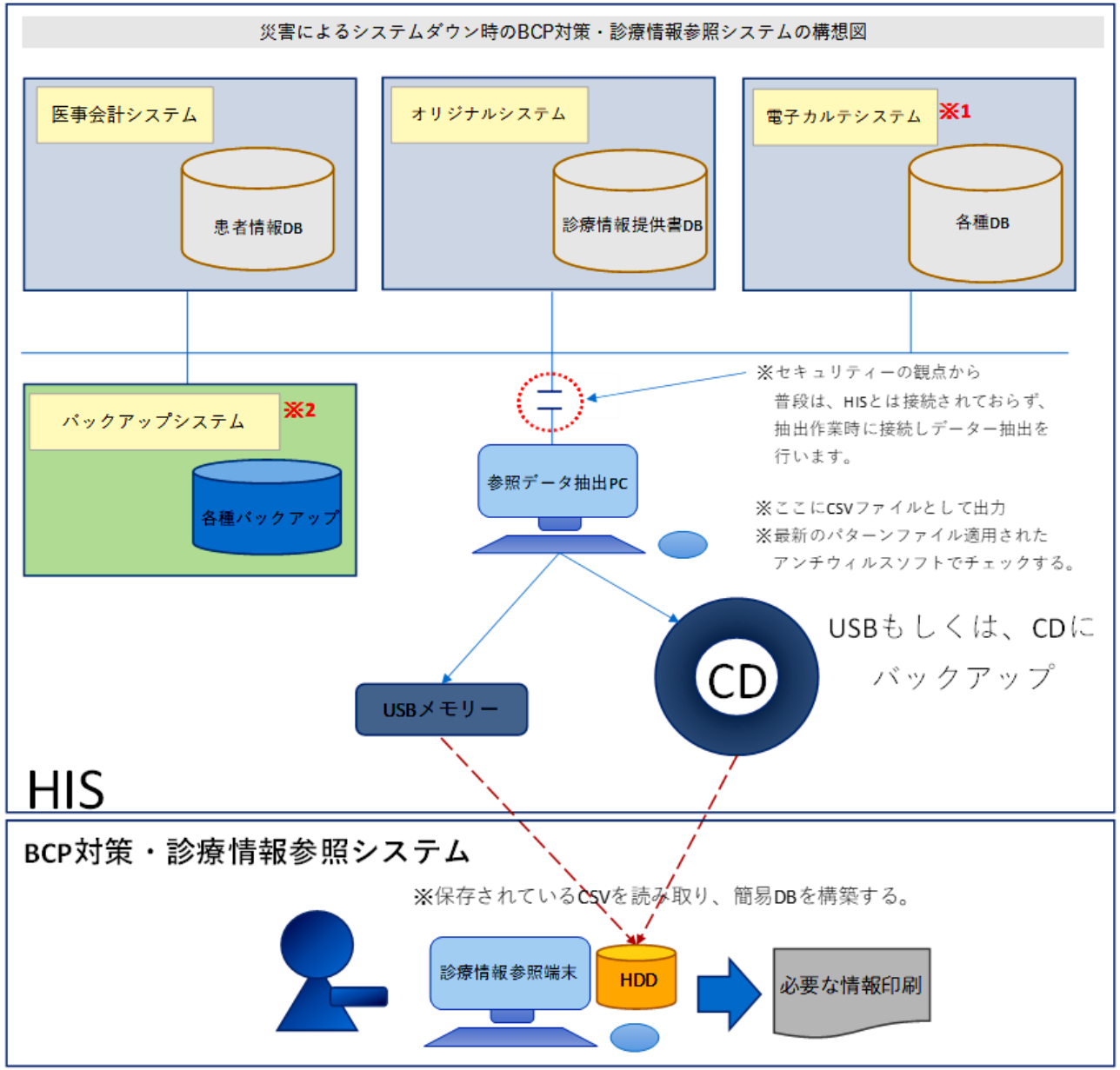
大津赤十字病院
橋本 智広氏より提供

サイバー攻撃は大きな災害！

- 半田病院を襲ったサイバー攻撃の概略
- サイバーセキュリティを高める！
  - ・バックアップは確実に
  - ・セキュリティー情報の取得
- サイバー攻撃を想定した訓練・BCPの作成！
  - 簡易バックアップも有用
  - 自治体に備蓄のPC・プリンター等の配備を！
-

院内医療情報セキュリティ規程
・有識者会議のSoftware ISACの監修
・厚労省のGLに従って作成
・インシデント発生時の体制
・記者会見の想定問答集・等

再発防止に向けてこれまでに検討している内容　②



電子カルテシステムが動いていなくても参照利用が可能な簡易バックアップシステムの構築や入院中の患者の情報を随時更新して紙にプリントする（申し送りのメモの保存）などオフラインでのデータ管理、など二重三重の対策を講じておくことを勧めます。

月刊　新医療　2022年7月号に掲載

※災害時、システム復旧までの間、過去歴を見れないのでは、
診療に影響が出るため参照システムです。
【システムの特徴】
稼働可能なクライアント端末があれば簡単に設定、複数に展開も容易で各部署への配布も可能
LANケーブルを用いた簡易ネットワークを構築し、医師の記録情報を共有も可能。

サイバー攻撃は大きな災害！

- 半田病院を襲ったサイバー攻撃の概略
- サイバーセキュリティを高める！
  - ・バックアップは確実に
  - ・セキュリティー情報の取得
- サイバー攻撃を想定した訓練・BCPの作成！
  - – 簡易バックアップも有用
  - – 自治体に備蓄のPC・プリンター等の配備を！
-

院内医療情報セキュリティ規程
・有識者会議のSoftware ISACの監修
・厚労省のGLに従って作成
・インシデント発生時の体制
・記者会見の想定問答集・等

昨年12月に電子カルテを止めて
ID・ﾊﾟｽﾜｰﾄﾞ更新の作業
・紙カルテの準備
・アクションカードの作成
・復旧をフェーズで考えて作成

電子カルテ停止中の各部門のアクションカードと復旧のプロセスのフェーズ管理（腎センター）

アクションカード　リーダー用

1. 被害状況の確認（透析装置・透析システム・電子カルテ等）
2. コンタクトリストに則り各部門へ連絡

2－1．部署内メンバーに役割分担（復旧プロセスに則り）

2－2．ニプロ（透析装置）、ホーピング（透析システム）への連絡と調整

3．部署内の対応状況を表示、透析施行有無の把握、本部に報告

4．患者への説明方法、内容の検討

5. システム管理課・本部を通じて今後の方針を聞く

アクションカード　メンバー用

1. 透析装置の動作確認
2. 透析システムの動作確認
3. 当日の透析患者数の確認
4. 紙カルテの準備
5. 透析記録の準備（紙媒体）
6. オフラインPC・プリンターの準備

復旧のプロセス

フェーズ1

1. 被害状況確認（透析装置・透析システムの使用可能の有無
2. ニプロ・ホーピングへ連絡し、対応確認
3. 本部に報告
4. 紙カルテ・透析記録（紙媒体）運用開始

＊毎月第1月・火曜日に透析患者のプロファイルを更新する

フェーズ2

1. 透析システムのみ電子カルテシステムから切り離しての使用が可能な場合、透析システム利用（ローカルネットワークの確立）
2. 山本システム参照サーバーで利用できる内容をとりこめるようにすること
3. 本部に復旧状況報告

フェーズ3

1. 修復できた透析装置・システムの確認
2. 完全復旧までの最終確認
3. 本部に復旧予定日の報告
4. 電子カルテ復旧後に入力する内容の整理

復旧

TOPページ - 医療機関向けセキュリテ

https://mhlw-training.saj.or.jp

https://mhlw-training.saj.or.jp/

医療機関向け

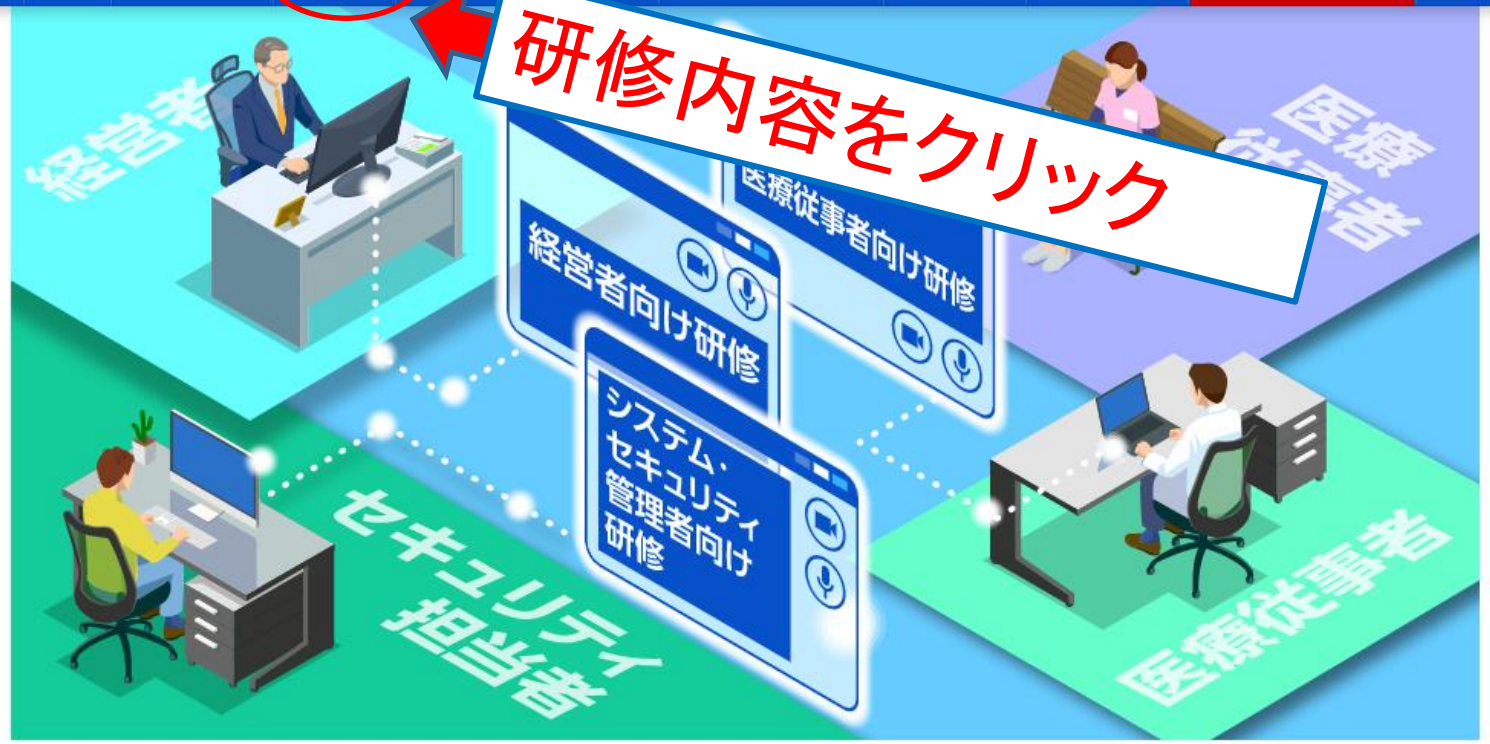
セキュリティ教育支援ポータルサイト

Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

事業について | 研修内容 | コンテンツ集 | コラム | 講師・技術者リスト | 関連リンク | お問い合わせ | インシデントかも？

研修内容をクリック



お知らせ

ここに入力して検索

TSLA -4.99%

21:30
2023/03/10

医療機関向けサイバーセキュリティ教育

経営者向け研修

システム・セキュリティ管理者向け研修

初学者等向け研修

導入研修

一般社団法人ソフトウェア協会 理事（Software ISAC 共同代表）
萩原 健太氏　作成　スライドより転用

© Interval Link Inc.

サイバー攻撃は大きな災害！

- 半田病院を襲ったサイバー攻撃の概略
- サイバーセキュリティを高める！
  - ・バックアップは確実に
  - ・セキュリティー情報の取得
- サイバー攻撃を想定した訓練・BCPの作成！
  - 簡易バックアップも有用
  - 自治体に備蓄のPC・プリンター等の配備を！
- もしサイバー攻撃にあった場合は・・。

サイバーセキュリティインシデント発生時初動対応支援

【インシデントかも？】

- ウイルスに感染してしまったなど、気になる点がございましたらご連絡ください。
- 厚生労働省には統計情報や重大なインシデントが発生した場合に連絡。

【派遣依頼方法】

以下のいずれかの方法でご連絡ください。

A.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にご連絡

B.本事業の専用サイト「インシデントかも？」からご連絡ください。

https://mhlw-training.saj.or.jp/

一般社団法人ソフトウェア協会 理事（Software ISAC 共同代表）
萩原 健太氏　作成　スライドより転用

© Interval Link Inc.

終わりに

- 徳島県警サイバー犯罪対策室より
  - 『システム担当責任者は、すべてのシステムを把握しておいてください。』
  - 『部署毎で勝手に、機器の接続・LANケーブルの増設、知らない内に業者による部門システムの設置などはさせず、システム担当責任者を通して行うように、改善をしてください。』
  - 『システム構成図・ネットワークシステム構成図・ネットワーク配線図は、常に最新にしておいてください。』
- アメリカのランサムウェア対策をしている識者から
  - 『ランサムウェアとの戦いは、勝つことはできないが、降りることもできないゲームであり。侵入されることを前提に、“バックアップデータをいかに守るか”と“感染した際に事業継続をいかに行うか（BCP）”を備えておくべきである。』