医療機関向け
セキュリティ教育支援ポータルサイト

IT-BCP　中小病院編

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12月19日　日本ソフトウエア協会

自己紹介

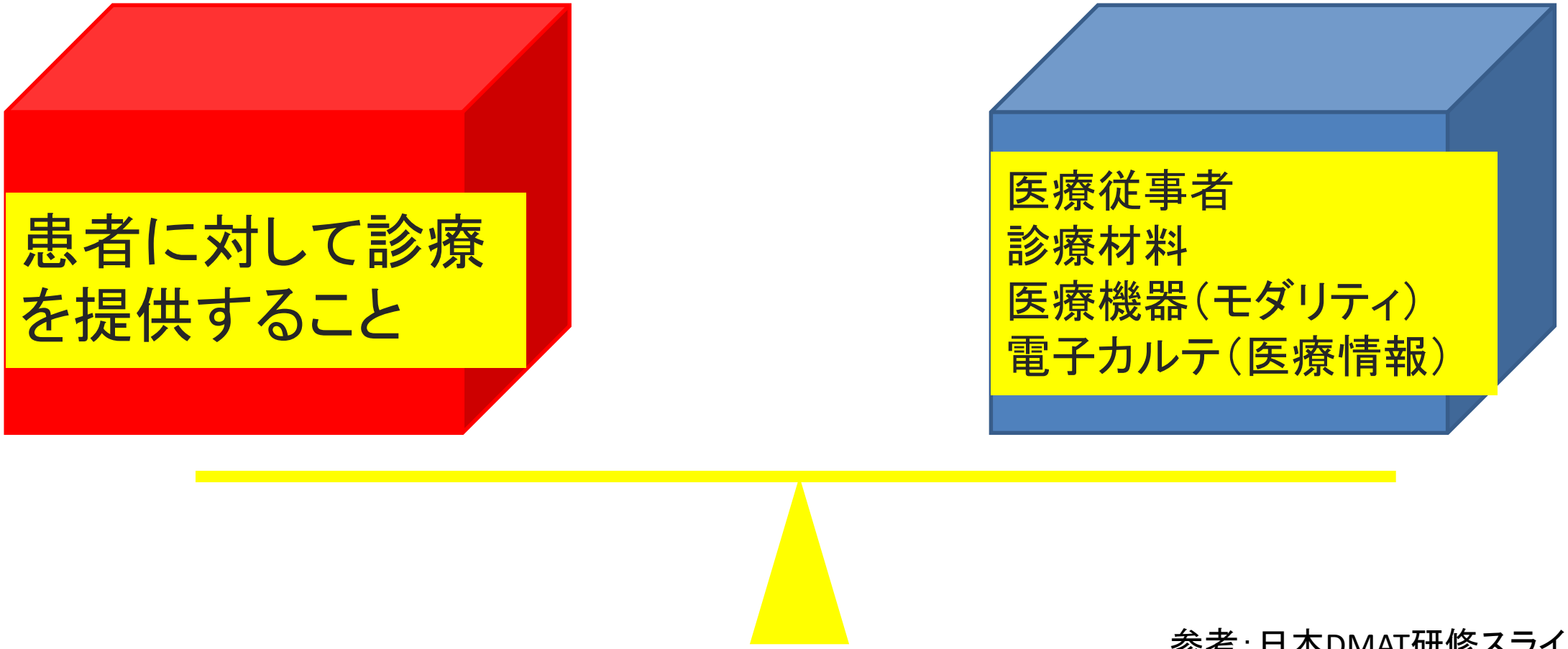
須藤　泰史（すとう　やすし）
つるぎ町　病院事業管理者（つるぎ町立半田病院）

【プロフィール】

- 1962年生まれ、大阪府出身
- 1986年　3月　　徳島大学医学部医学科卒業
- 1986年　5月　　徳島大学医学部泌尿器科学教室へ入局
  以降、関連施設での研修
- 1995年　4月　　徳島大学医学部附属病院助手（泌尿器科）
- 1999年　4月　　徳島大学医学部附属病院講師（泌尿器科）
- 2001年　4月　　徳島大学医学部講師（泌尿器科学講座）
- 2003年　6月　　町立半田病院　泌尿器科医長
- 2013年　9月　　つるぎ町立半田病院　病院長
- 2020年　1月　　つるぎ町　病院事業管理者（つるぎ町立半田病院　病院長兼任）
- 2020年　4月　　つるぎ町　病院事業管理者　現在に至る

- 【所属学会・資格】
- 日本泌尿器科学会（専門医・指導医）　日本透析学会（専門医）
- 地域包括医療・ケア認定医
- 総合診療専門研修特任指導医
- 徳島大学　総合医学分野　臨床教授
- 日本DMAT医師　（平成29年度徳島DMAT研修終了）
- 徳島県災害医療コーディネーター
- 【主な役職】
- 全国国民健康保険診療施設協議会　徳島県協議会会長
- 全国国民健康保険運営協議会　徳島県運営協議会副会長（医師部会長）

平常時では・・・



参考：日本DMAT研修スライド

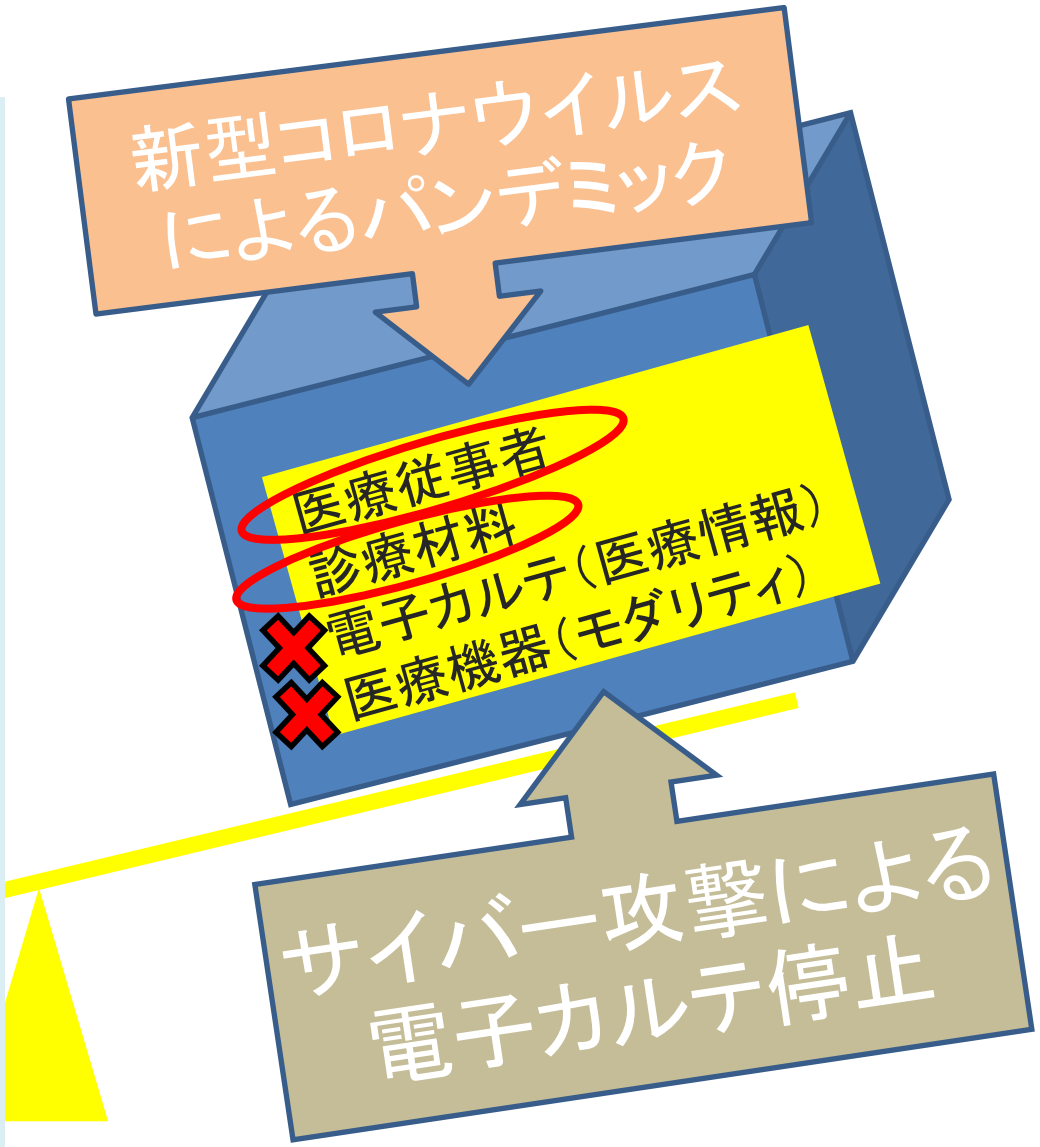
災害では・・・　大きなアンバランスが生じます！

当院BCPに、新たに以下を追記

第9章　サイバー攻撃対策

第10章　パンデミック対策

追記　2020年から世界中に広がったCovid-19によるパンデミックに対応し、当院でも**発熱外来、集団予防接種、コロナ病棟を運営**した。また、2021年10月末日、**ランサムウエアによるサイバー攻撃を受けて病院機能がストップ**してしまう事態を経験、これまで災害対策用であったBCPを応用して対応した。この経験から今回、新たに第9章としてサイバー攻撃対策を、そして、第10章にパンデミック対策を追記した。これまでのBCPと同じく、これも完成形でなく、日々の訓練や新たなガイドライン等により随時改訂していく必要がある。



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。）

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。

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！

サイバー攻撃は大災害と同レベルの対応が必要（対策本部の設置・基本方針の制定・紙カルテベースでの診療継続等）。
今回のサイバー攻撃を受けて各部門での具体的な対応、項目ごとにまとめを記載（当院BCPから転載）。

A：データの保存に関して

① 電子カルテ内の予約票の印刷（できれば2週間先程度まであれば、翌日以降の診療の準備に余裕あり）。

② ｸﾘﾆｶﾙﾊﾟｽ・指示内容・説明書・同意書を紙ベースで電子カルテ内のみでなく、残しておけばコピーで増刷できる。

③ スケジュールを紙のカレンダーに記載する習慣が有用（手術・処置・検査等のスケジュール管理が把握できる。）

④ 透析患者のｶﾝﾌｧﾚﾝｽ用に取り出してある検査結果一覧（CSV file）が電子カルテとは別の部署内のPCの中にあり、DW（ﾄﾞﾗｲｳｴｲﾄ）も分かり助かった。

⑤ 検査機械本体に記録されているデータもある。

⑥ 病棟での申し送りやリーダー板など紙ベースで行っているものを捨てずに保存していた。

⑦ 入院時の患者プロファイル・医師指示の内容をプリントアウトして残していた。

⑧ 薬剤情報（院内採用薬等）をCSVファイルで調査用にデータ抽出していた。

⑨ DPCデータなど電子カルテから抽出していたデータはその期間のバックアップデータになる。

⑩ 新型コロナワクチン接種のための個人情報（名前・ID・住所等）のデータ抽出あり（CSV file）。

＊②の項目や退院サマリー・診療情報提供書などをPDF fileとして電子カルテ外のPCに保存を検討。CSV fileやPDFであれば電子カルテシステムが再稼働できていなくても通常のPCで読み取ることが出来、患者を他院へ搬送する際の情報源として使える。個人情報であり厳重な管理が必要であるが・・。

サイバー攻撃は大災害と同レベルの対応が必要（対策本部の設置・基本方針の制定・紙カルテベースでの診療継続等）。
今回のサイバー攻撃を受けて各部門での具体的な対応、項目ごとにまとめを記載（当院BCPから転載）。

B：データの取集に関して（以下のものが有用であった）

① お薬手帳・母子手帳・共通診療ノートなどが貴重な情報源。
② 調剤薬局からの処方内容の提供。
③ 以前の紹介先からの当院からの診療情報提供書の写しの提供。
④ 患者自身からの検査結果などの記録の提供。
⑤ 各診療科外来等にある手術簿や病理検査結果・入院要約の綴り。
⑥ 各訪問看護ステーション・ケアマネ等の連携施設から受け持ち患者情報の提供。
⑦ レセプト・会計カードなど。

サイバー攻撃は大災害と同レベルの対応が必要（対策本部の設置・基本方針の制定・紙カルテベースでの診療継続等）。今回のサイバー攻撃を受けて各部門での具体的な対応、項目ごとにまとめを記載（当院BCPから転載）。

C：紙カルテベースの診療に関して

① 復旧後の電子カルテ入力時には、ダブルチェックが必要。
② 「特定疾患指導管理料」・「以下余白（処方箋に使用）」等の印鑑が有用。
③ 定期受診で検査項目を予測できる方はあらかじめ検査伝票の必要項目にチェック。
④ 整理整頓、分別、見出しの活用など文具を有効に利用。
⑤ 患者数を制限していないと対応できない。
⑥ 一患者一カルテの対応が望ましい（検査や処方の重複の防止・患者の院内で所在の確認）
⑦ カルテに検査結果などを貼る担当を決め同じように貼る。
⑧ 書式が決めていいものは本部で統一。
⑨ 復旧後に多くのスキャンすべき書類がたまる。
⑩ 栄養科が時間ごとに伝票を取りに来る（入院の食事に関して）。（定時の動きを作ることも大事。）
⑪ 透析記録・処方箋：使用しながら書きやすい形式に変更（使いながら工夫を。）
⑫ 復旧後を想定して病棟毎・日毎に内服・注射せんの綴りを作成。（内服1000枚・月、注射　4000枚・月）
⑬ 文具（のり・紙・インク・トナー等）・PC・コピー機・スキャナー等が多数いる。
⑭ 感染がない、正常と判断された医療機器の端末のみを結んだローカルネットワークを構築（画像保存、読影結果記録システム）。
⑮ 人が結果を運ぶ・人海戦術を覚悟（ただ、病院業務の経験者でないと誰でもが支援できない）。
⑯ 手書きのミス・読めない・英語などの使用も注意。

＊一番は、電子カルテと違い、カルテが持ち出されると他の者がカルテの内容を確認できない！！

サイバー攻撃は大災害と同レベルの対応が必要（対策本部の設置・基本方針の制定・紙カルテベースでの診療継続等）。今回のサイバー攻撃を受けて各部門での具体的な対応、項目ごとにまとめを記載（当院BCPから転載）。

D：病院運営に関して

①対策本部・ミーティングをこまめに（CSCAの確立。）

②ウイルス感染発覚時に超音波診断装置などの電子カルテとつながる各LANを抜くなどの緊急対応の取りまとめを（今後、情報システム委員会で規定予定）。

③病棟後の入退院・部屋替えの記録を本部で管理し記録したこと。

④復旧に関して：忙しい部署・忙しい人は時期により異なる。いつもと全く違う仕事をしないといけない。不平不満もたまる。病院管理職は聞く耳をもつことが肝要。

＊②に関して（システム担当者のやったこと）

- ネットワークの遮断
- 電源が入ってる、入っていないの切り分け作業
- 全端末の回収作業
- サーバー機器、修理依頼・発送作業
- 感染端末に対して修復業者からのフォレジング調査を開始
- 外部とつなぐ環境設定
- 全端末のアンチウイルスソフトによるウイルスチェック作業
- 全端末、ハードディスクの初期化、OSのイントール作業
- 院内のセキュリティー強化につき、患者様サービスのフリーWi-Fiのアクセスポイントにパスワード設定を行う。
- 心電図、CT、MRI、などのモダリティー機器の感染有無の確認と、システム初期化処理

特に復旧段階で行ったこと

- 修復業者からサーバー類が順次修復完了し、返却される。
- 電子カルテシステム、医事システム等のクライアントシステムのセットアップを行う。
- ミニマムなネットワークを構築し、サーバーの動作確認
- 各サーバー設定作業(ハード・システム)
- 電子カルテシステム、医事システム、各部門システムの動作確認作業
- 回収した、全端末を元の箇所に設置。
- システム再稼働。
- 画像サーバーに不具合発生、もう一度、システム再構成を行う。

- ※システムの部署からの困りごとは得になく必要な物の準備とか、逆に支援して頂けていたので助かった方が多かったです。
- あと、『頑張れよ』、とか、『頑張ってください。』とか、声をかけてくれたりして元気つけられました。

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

【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

第43回医療情報学連合大会

産官学連携企画　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）

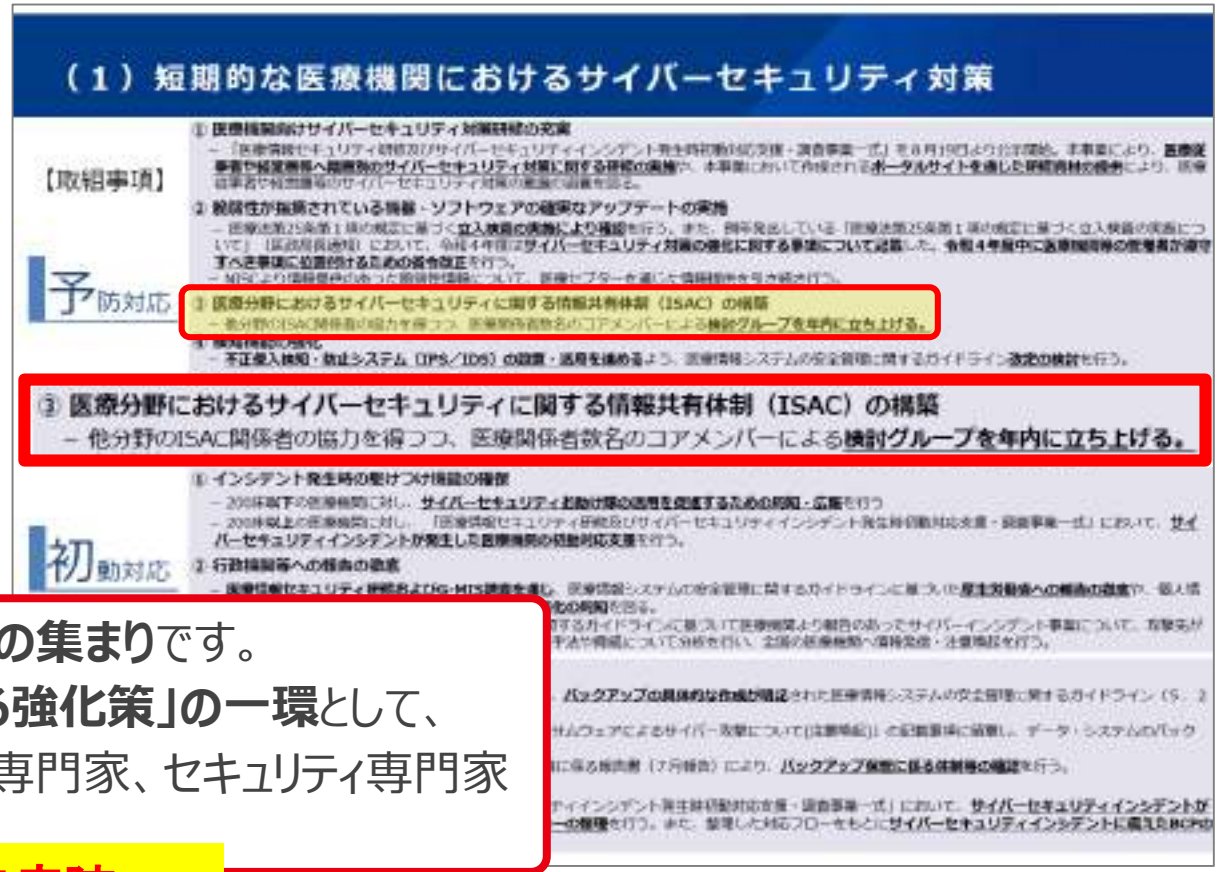
4-A-4-01　医療分野におけるサイバーセキュリティ対策の厚生労働省の取組について
新畑　覚也　（厚生労働省 医政局 特定医薬品開発支援・医療情報担当参事官室）

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　（読磐会 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
酒田　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！

- IT-BCPとして必要なこと
  - セキュリティ規程
  -

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

IT-BCPの考え方

大阪急性期・総合医療センター

BCPの整理：　一般災害・システム障害

	一般災害		特殊災害	システム障害	
正式名称	General Disaster BCP		Extraordinary Disaster BCP	System Failure BCP (SF-BCP)	
				医療事業継続計画	病院情報事業継続計画
略式名称	GD-BCP		ED-BCP	SF-BCP (for Medical)	SF-BCP (for HIS)
主な対象	自然災害・人為災害		NBC・新興感染症・テロ等	システム障害	システム障害
BCP策定状況	広域自然災害対応BCP：2023/3/31第7版改定		今後策定するかも含め検討予定	2024/4/15 初版制定	2024/4/12 初版制定（予定）
	BCP策定状況				
		自然	人為		
	広域	○	-		
	局地	-	-		

56

大阪急性期・総合医療センター　嶋津 岳士 総長の講演スライドより

つるぎ町立半田病院

病院のBCP

白：平常業務

緑：一部診療制限

黄色：通常診療中止・傷病者受け入れ態勢（病院周辺で大事故等）

赤色：通常診療中止・傷病者受け入れ態勢（大規模地震等で病院自体が機能不全）

黒：病院避難（大規模火災・病院倒壊等）

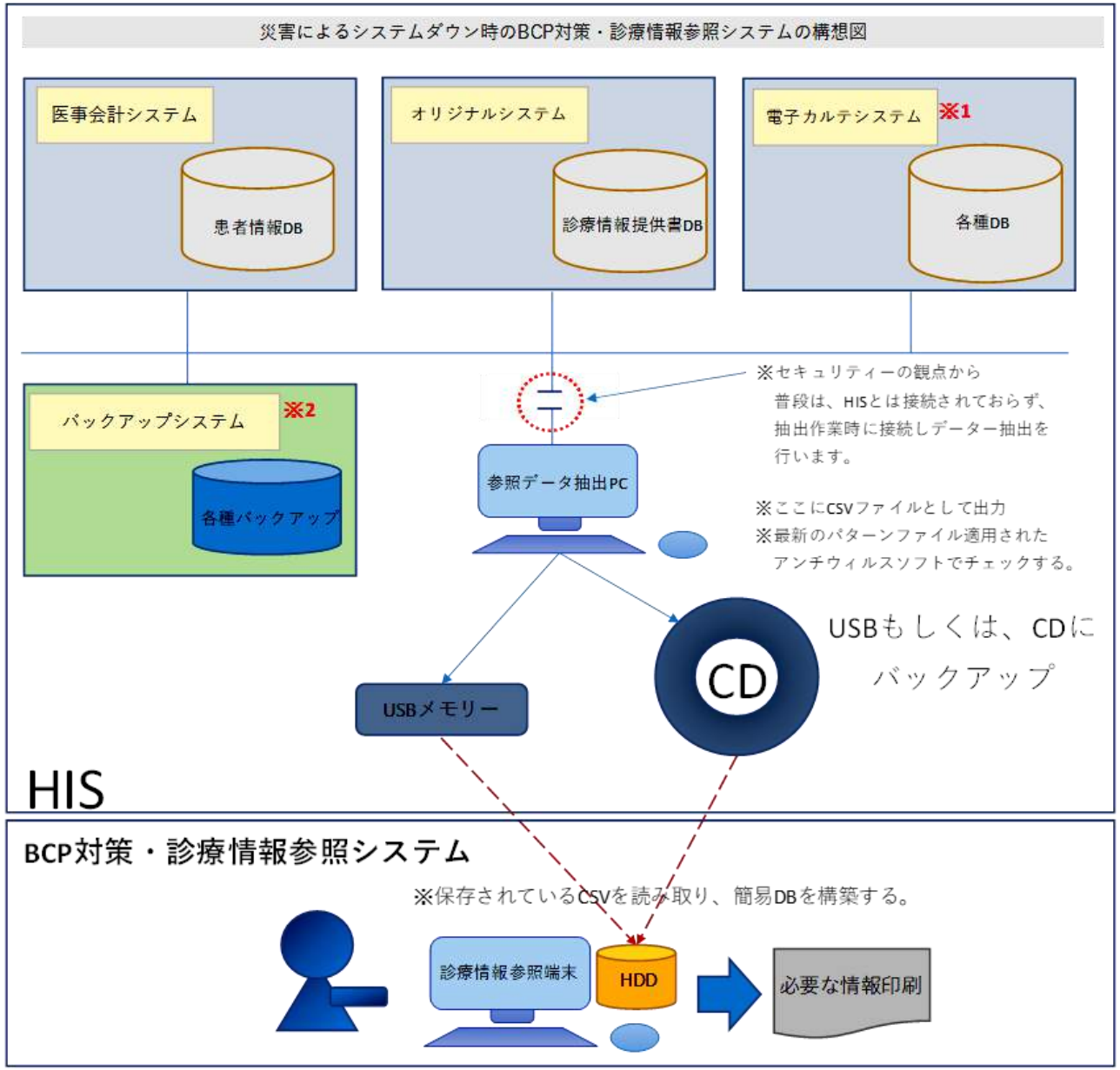
- 地震・火災等のBCP
- パンデミックのBCP
- システム障害のBCP

サイバー攻撃は大きな災害！

- IT-BCPとして必要なこと
  - セキュリティ規程
  - 簡易バックアップなどの参照システム

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



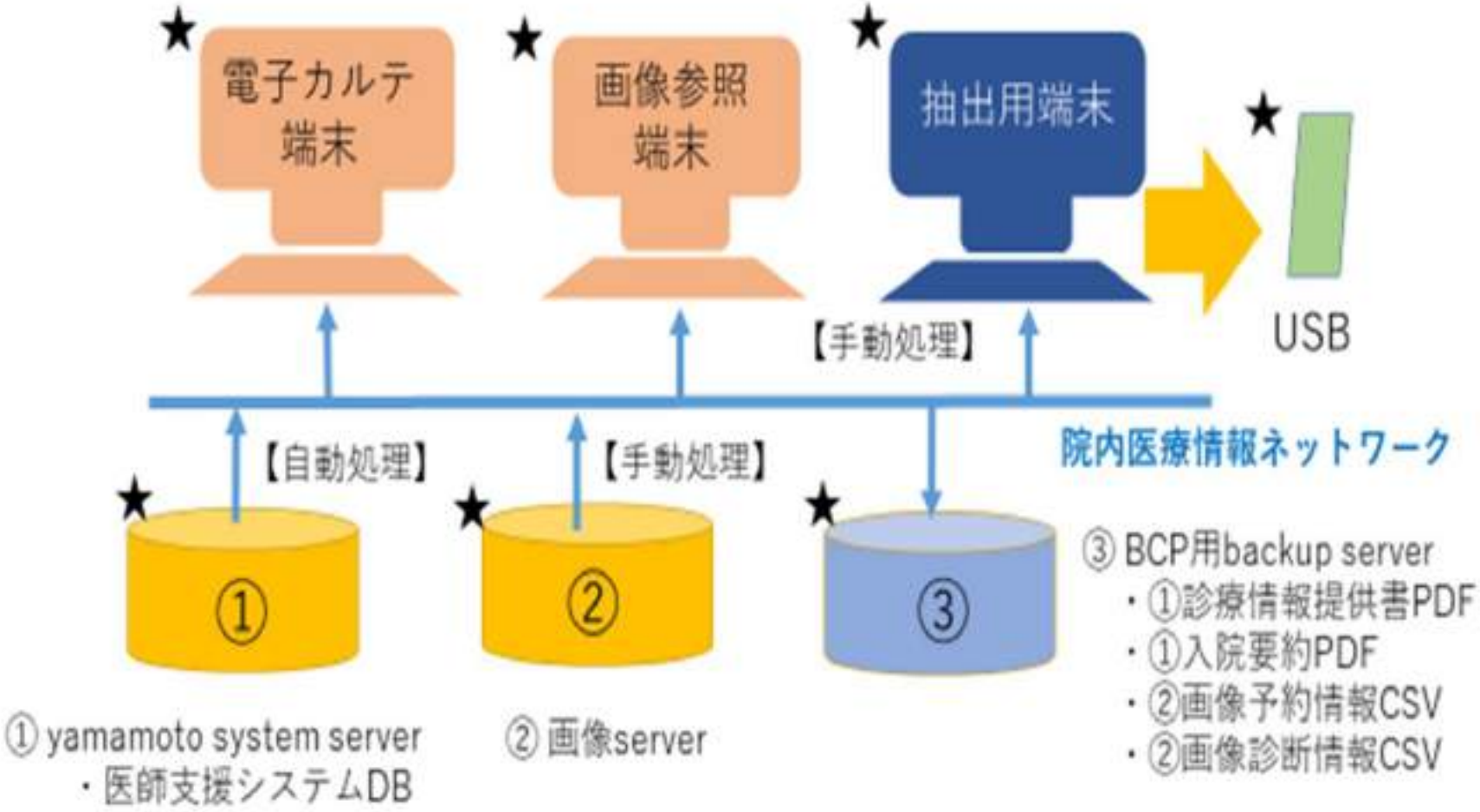
電子カルテシステムが動いていなくても参照利用が可能な簡易バックアップシステムの構築や入院中の患者の情報を随時更新して紙にプリントする（申し送りのメモの保存）などオフラインでのデータ管理、など二重三重の対策を講じておくことを勧めます。

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。

BCP対策用参照システムバックアップ方法

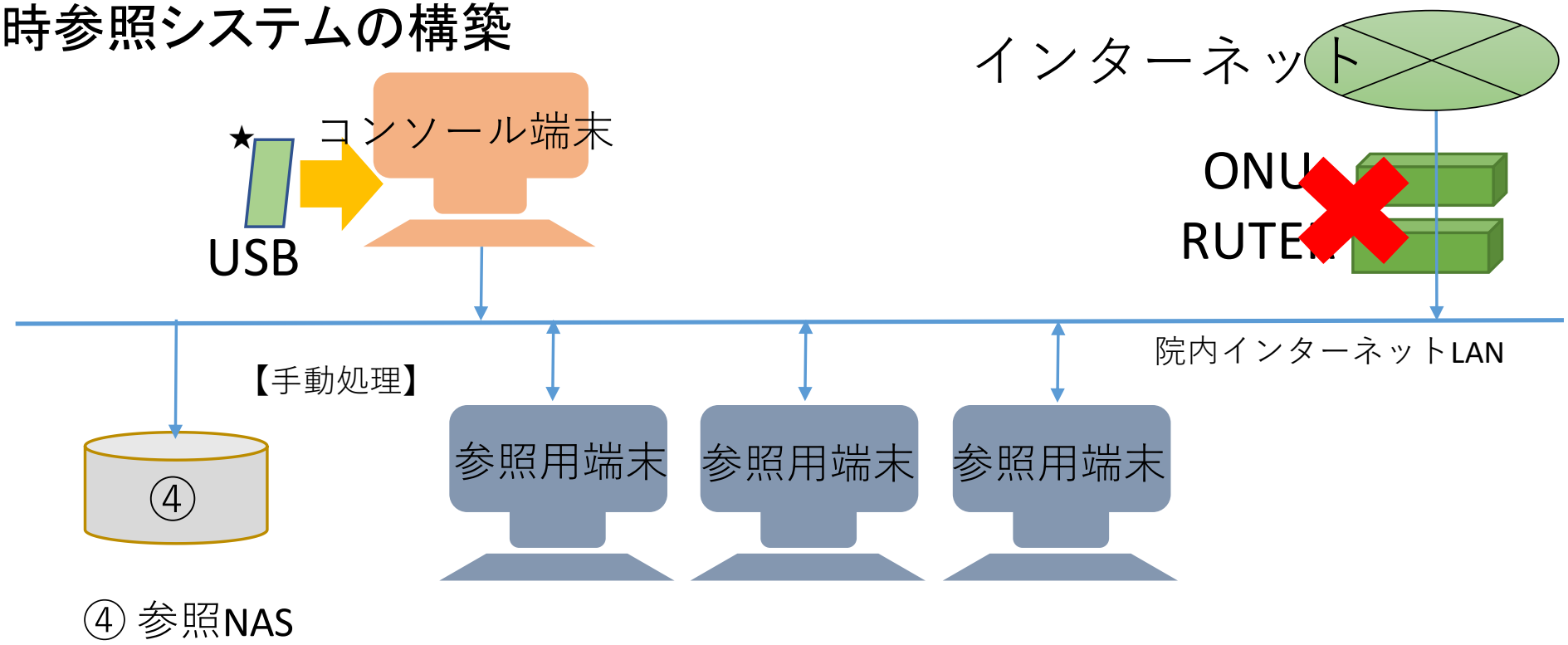
■参照データーの確保



■流れ

1. 医師支援システムDBから、自動処理で①のPDFを③へ出力されます。
2. 画像サーバーから定期的に②のCSVを③へ出力します。
3. 抽出用端末から③のバックアップサーバーから、ファイルをUSBへ出力します。

■　BCP時参照システムの構築



■流れ

4. インターネット上のONU、ルーターを切り離します。
5. 参照用端末をインターネット回線上に設置します。
6. 保存されたUSB内のファイルを④へ出力します。
7. システム稼働(参照用端末を稼働し、参照・必要があればコメント入力も可能になります。)

＊コメント情報は電子カルテが復旧した後コピーアンドペーストでカルテにも記載できます。

サイバー攻撃は大きな災害！

- IT-BCPとして必要なこと
  - セキュリティ規程
  - 簡易バックアップなどの参照システム
  - 訓練

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

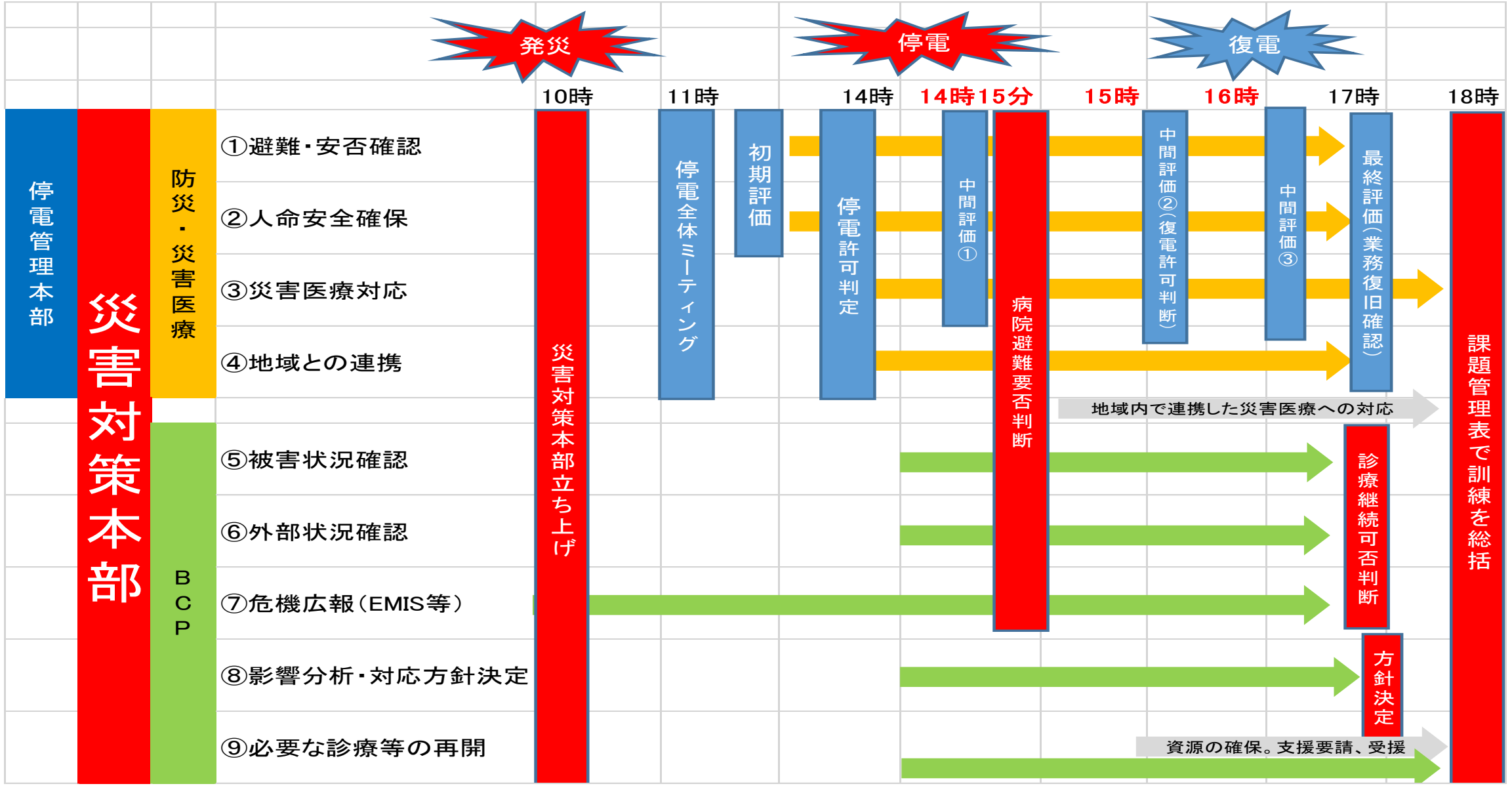
昨年12月に電子カルテを止めて
ID・ﾊﾟｽﾜｰﾄﾞ更新の作業
・紙カルテの準備
・アクションカードの作成
・復旧をフェーズで考えて作成

参考1

計画停電を経験しながらの災害訓練　2019.3.21

- 災害対策本部は
  - 別図の全体フローに合わせた災害訓練・停電対応を行う。
  - 出来たばかりのBCPの問題点をチェックリストで検証。
- 各部署は
  - “もし、この停電が災害の発災による停電であったとしたら”と想像し、各部署で作成しているアクションカードの見直しや、災害対策本部報告用紙の運用などの見直しを行う。
  - 訓練終了後、課題管理表に問題点を記載して、災害対策委員会へ提出。

追記1　2019年の計画停電を利用したBCPに基づく訓練 ①



追記1　2019年の計画停電を利用したBCPに基づく訓練 ③

部　門	災害対策本部

目標(完了状態)	人命の安全確保、病院避難可否判断がなされている	目標時間	1時間	□

No.	アクション項目(目的)	アクションの実施手順(具体的内容)	必要なリソース	担当者(指示者)	所要時間	累積時間	完了確認
①	避難・安否確認 災害対策本部立ち上げと役割分担	災害対策本部立ち上げを指示 ・災害対策本部設置場所の決定。対策本部用資器材の調達 ・災害対策本部を立ち上げた旨の通達	・対策本部用資器材・場所リスト ・資器材調達責任者 ・持出品リスト	本部長			□
		本部職員への役割分担とタイムライン提示 ・必要な役割の確認、本部要員の役割指示 ・災害情報の把握(TV、ラジオ等から災害情報を確認)	・役割分担表、タイムライン ・本部要員の能力適正リスト ・TV、ラジオ	本部長			□
		通信・連絡手段の確保、連絡要員の配置 ・院内の連絡手段の確保 ・(想定連絡手段利用不能の場合)代替連絡手段手配	・通信・連絡手段 ・無線(代替連絡手段) ・情報連絡員(リエゾン)、自転車	災害対策本部			□

目標時間	1時間	□

担当者(指示者)	所要時間	累積時間	完了確認
本部長	30分		□
本部長	10分		□
災害対策本部	3分		□

課題管理表

部署	4階南病棟

19年 3月 21日	1	1.建物・施設 (2).設備・備品 3.システム 4.組織・体制 (5).行動ルール 6.その他			災害本部が設置されるまでの間、当直者がリーダーとなるが災害用の備品や設備を把握していない	当直者が使用可能な備品・設備を明確化		1.個人で解決できる課題 2.自分の所属部署で解決できる課題 3.他部署で解決すべき課題 (4).全体で解決すべき課題 5.院外でなければ解決できない課題 6.その他	(部署名) (担当者)	確認日 (　19年　4月　18日) 1.対策済 2.対策開始 (3).対策中 4.対策保留 5.対策せず 6.その他 (　　)	BCPマニュアルの第4章に各部署ごとがするべき項目に追加
19年 3月 21日	2	1.建物・施設 (2).設備・備品 3.システム 4.組織・体制 5.行動ルール 6.その他			停電となっても身障トイレ利用が望ましいが、真っ暗となる。懐中電灯でも暗い	ランタンの設置		1.個人で解決できる課題 2.自分の所属部署で解決できる課題 3.他部署で解決すべき課題 (4).全体で解決すべき課題 5.院外でなければ解決できない課題 6.その他	(部署名) (担当者)	確認日 (　19年　4月　18日) 1.対策済 2.対策開始 (3).対策中 4.対策保留 5.対策せず 6.その他 (　　)	現在ランタン5つ、今後も追加購入予定。

参考2

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） 2023年12月

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

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。』

ご清聴ありがとうございました。