経営者向け研修　IT-BCPコース大規模編

令和6年度　厚生労働省委託事業　医療機関向けサイバーセキュリティ研修

主なタイムライン	
2022. 10.31	ランサムウェアによる大規模システム障害発生 救急受入、予定手術、初診受付等の停止 厚労省初動対応支援チーム活動開始（～11.6）
11.1	DACS参照開始
11.4	予定手術一部再開
11.10	バックアップによる参照環境構築⇒３次救急受入再開
11.17	参照環境を救急外来に設置⇒２次救急受入再開
11.28	参照環境を手術室に設置⇒予定手術枠の拡充
12.12	電子カルテ等基幹システム運用再開/部門システム一部再開
12.22	電子カルテ運用全面再開(入院・外来)/部門システム一部再開
1.11	部門システムの大部分再開　⇒　診療体制全面復旧

大阪急性期・総合医療センター
事務局　経営企画マネージャー　粟倉　康之

左記コードは
当センターHP医療情報セキュリティ特設サイトへの内容です。

本日の内容

① インシデントの概要と経営課題　（担当：粟倉）

② インシデント事例に基づくIT-BCPの考え方　（担当：粟倉）

③ 医療継続用のIT-BCP　（担当：仲桝）

詳細は、当センターホームページ掲載の
医療情報セキュリティ特設サイトを
ご確認ください。

大阪急性期・総合医療センター概要

項目	内容	詳細
病床数	865床	一般：831床（再掲ICU, CCU, SCU, HCU, MFICU, NICU, GCU計91床） 精神：34床
職員数	2,014人	医師数；259人、研修医：50人、看護師数；1,024人　　（2022年4月1日時点）
診療科	36診療科	基幹災害拠点病院、地域医療支援病院、臨床研修指定病院 高度救命救急センター、地域周産期母子医療センター、大阪府小児地域医療センター 地域がん診療連携拠点病院、がんゲノム医療連携病院、大阪府がん患者妊よう性温存治療実施医療機関　他

項目	2019年度	2020年度	2021年度	2022年度
医業収益	309.4億円	286.7億円	296.2億円	277.4億円
新入院患者数	23,649人/年	18,440人/年	18,256人/年	17,188人/年
延入院患者数	273,683人/年 748人/日	224,353/年 615人/日	218,529人/年 599人/日	208,794人/年 572人/日
初診患者数	35,828人/年	25,842人/年	27,262人/年	27,061人/年
外来患者数	335,114人/年 1,396人/日	289,309人/年 1,191人/日	294,942人/年 1,219人/日	283,266人/年 1,166人/日
紹介率	94.7%	98.6%	101.5%	102.8%
平均在院日数（一般病棟）	9.2日	9.7日	9.6日	10.0日
救急車搬入患者数	9,872人/年	5,628人/年	6,390人/年	7,402人/年
中央手術室手術件数（眼科除く）	6,940件/年	5,959件/年	6,164件/年	5,556件/年
医業収支比率	99.5%	93.2%	93.9%	91.8%
給与費比率	45.8%	50.9%	49.8%	51.4%
材料費比率	32.1%	31.3%	32.1%	33.7%

	11月比較			12月比較		
	2022年	2021年	比率	2022年	2021年	比率
新入院患者数（人）	558	1,674	33%	888	1,625	55%
延入院患者数（人）	10,191	19,267	53%	10,932	19,518	56%
初診患者数（人）	465	2,605	18%	1,078	2,499	43%
延外来患者数（人）	15,744	25,575	62%	17,955	25,680	70%
中央手術室手術件数（件）	168	597	28%	227	586	39%
救急車搬入件数（人）	88	679	13%	447	665	67%
入院診療行為額（百万円）						
外来診療行為額（百万円）						

2ヶ月で
約22億円の減収

電子カルテシステム障害期間：2022.10.31～12.11

病院全体のシステム概要（インシデント発生当時）

項目	内容
情報システムの概要	基幹システム 　電子カルテ 　オーダリング 　医事会計 　看護支援　他 部門システム：約67種類 　検体検査システム 　生理検査システム 　放射線情報システム 　医用画像情報システム 　栄養給食管理システム　他 連携医療機器；多数 　検体検査機器 　画像診断機器 　生理検査機器　他 ネットワーク設備・機器　多数
院内管理機器数情報	サーバ　：約100台（物理台数） 端末　：約2,200台（DT、ノート） プリンタ：約400台（A4モノクロ）
ネットワーク主な種別	①HIS系ネットワーク ②インターネット系ネットワーク ③機構系ネットワーク

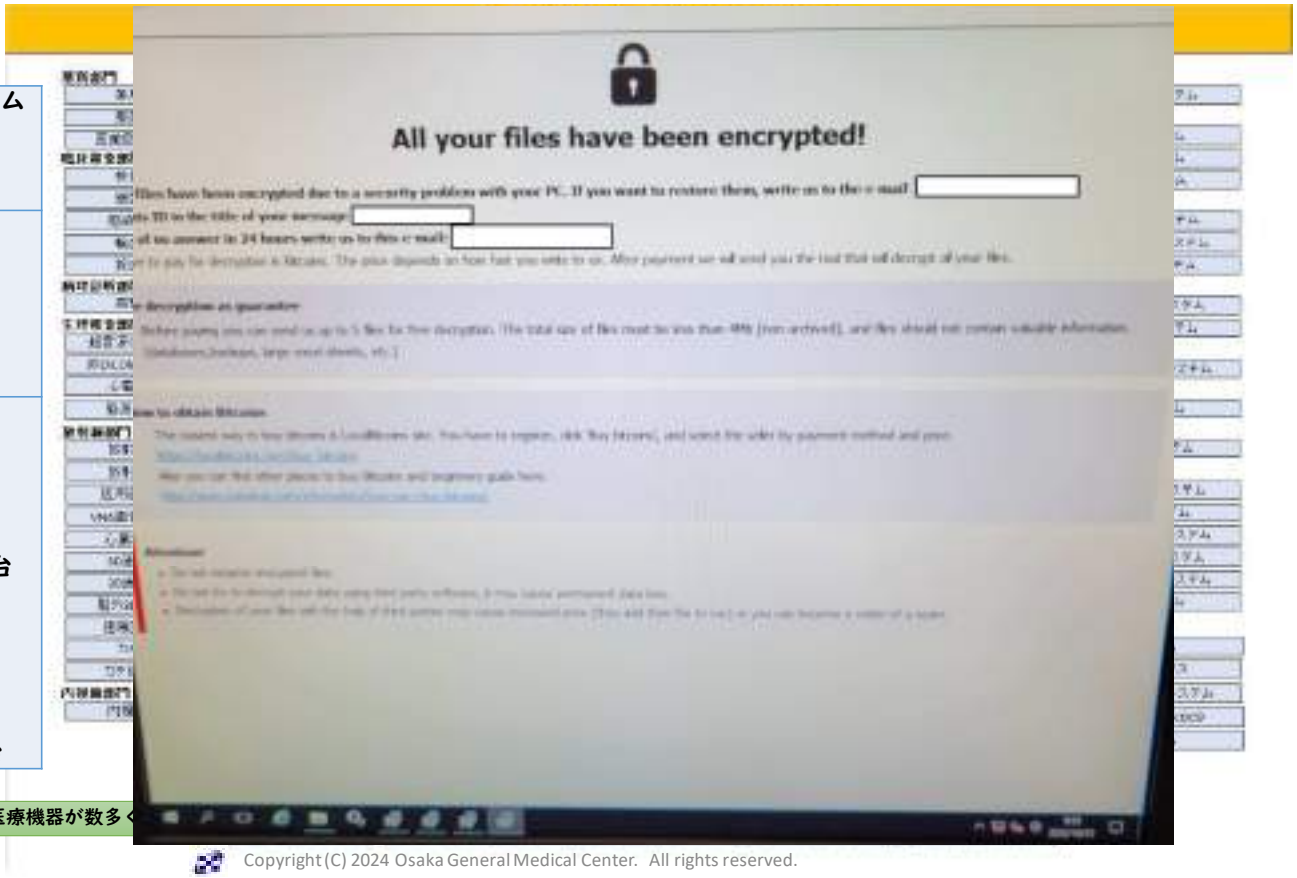
項目	内容
マネジメント体制	システム管理部門：情報企画室　（専従職員；7名） システム運用管理委託（平日：6名、休日：1名） システム構築事業者による運用・保守体制
システム構築時セキュリティ対策	● ネットワーク分離設計（診療系とインターネット系を論理分割） ● ファイアウォール設置による通信制限 ● 電子カルテ端末のネットワーク認証（802.1x認証） ● リモート保守のための中継サーバ設置 ● 認証システム（ICカード利用）による電子カルテ端末利用制限 ● 職種等毎の利用権限設定（電子カルテシステム） ● ウイルス対策ソフトの導入（サーバ、端末　全てに設定） ● 電子カルテ端末でのUSBメモリ使用制限
日常的セキュリティ対策	● サーバ稼働確認（3回/日　8:00、12:00、20:30） ● ウイルス対策ソフトのパターンファイル更新（週1回/土） ● ネットワーク機器定期点検（2回/年　4月、10月）
バックアップ方法	①　サーバ上のハードディスク（本体データ） ②　①のコピー（別室にあるハードディスク） ③　LTOテープ（サーバ内） ④　LTOテープ（遠隔地保管）
直近でのセキュリティ強化対策	● ファイアウォールのファームウェア更新（21年12月） ● 通信機器の脆弱性確認　（21年12月） ● ウイルス対策ソフト（本体）のバージョンアップ（22年3月） ● 電子カルテ端末でのUSBメモリ使用不可設定（22年7月）

HIS: Hospital Information System

第6期総合情報システム
賃貸借契約期間
2018年3月1日
～2024年2月29日

【リース物件の構成】
・システム機器等
（ネットワーク含む）
・ソフトウェア等
・上記保守
・遠隔地データ保管

アプリケーション数
;42種類
サーバー
;85台
デスクトップ
;1,360台
ノートPC
;750台
プリンタ
;604台
ネットワークスイッチ
;229台



各部門システムに各種医療機器が数多く

①インシデントの概要と経営課題

【経営課題】

(1)現状の医療はシステムに頼り切ってしまったため、安全安心な医療提供を継続するためには、診療制限しかなかった（医療安全を最優先…）

⇒大幅な収益減少

(2)外部接続管理（通信監理）が不十分だったため、全台初期化に踏み切らざるを得なかった（バックドアを仕掛けられている可能性…）

⇒復旧期間が長期化　⇒　診療制限の長期化

(3)電子カルテが復旧しても、部門システムは段階的復旧、患者の戻りも段階的（地域紹介⇒初診⇒検査⇒入院⇒手術と段階が必要）

⇒医療体制が元に戻るのは復旧後数か月先（分娩はさらにその後…）

(4)診療報酬による収入が事実上2ヶ月停止（医事会計が停止しレセプト請求不可）

⇒資金不足の可能性（給与支払い、業者支払いのピンチ…）

不幸中の幸い…

◆オフラインバックアップがあってよかった

⇒診療記録の復旧・請求根拠の復旧（診療報酬請求には根拠の保存が必要）

◆ＤＡＣＳが暗号化を免れてよかった

⇒医療継続の切り札

バックアップ差分（欠損分）もリアルタイム保存で対応

◆個人情報の漏洩が無くてよかった

⇒漏洩事案だと、本人通知、コールセンター設置、そして慰謝料支払い…

◆専門家チームがすぐに駆け付けてくれてよかった

⇒医療情報システムベンダーにセキュリティ専門家は不在…

調査方針や復旧方針の決定など状況に応じたマネジメントに対応

よくある質問…

Q　なぜバックアップが生きていたのに、復旧まで時間がかかったのか？
（電子カルテ復旧まで6週間、システム全般の復旧まで10週間）

A　①脆弱な初期設定を強固なセキュリティ仕様に変更するための設計変更
【標準ユーザー運用、アカウントロックアウト、PW個別化、サーバウイルス対策…】
➡テストを繰り返す必要あり
➡部門システムとの連携テストも必要
②端末2200台全てを初期化し再インストールしなければならなかった
（回収⇒ＨＤ取り出し⇒クローン⇒再取り付け⇒再配置）
【なぜ全台初期化だったのか？】
➢　調査開始当時に1300台に及ぶ不正アクセス試行記録が確認。
➢　どこにどんなバックドアが仕掛けられていたか調査しないと不明。
➢　全台調査を進めるよりは、全台初期化の方が早期復旧できると判断。
➡職員が各端末に作成保存していたデータ消去をすることになったが、
電子カルテの早期復旧を最優先にした苦渋の決断
③データ連携する部門システムの数が多かった（約67種）

病院経営の問題　調査・復旧費用

項目	内容	課題
調査費用	①　専門業者調査委託 ②　フォレンジック調査 ③　情報漏洩（ダークウェブ）調査	①　医療情報システムベンダーでは対応力欠如 専門家に調査・復旧方針の委託 ②　フォレンジック調査は高額 1台100～300万円　調査対象の仕分けをしないと費用は嵩む一方 ③　被害後すぐに取り掛かる必要あり。調査期間をどうするか…
システム復旧費用（基幹ベンダ）	• セキュリティ設計見直・検証 • 端末再作成・展開（2200台）	どこまでが保守範囲で対応できるか契約書（仕様書）に明記無し
システム復旧費用（部門ベンダ）	• 計29のシステムベンダーより請求あり	• 一部ベンダーは保守費の中で対応してくれたベンダーも…
医療機器ウイルスチェック費用	• 医療機器ベンダーによっては、ウイルスチェック作業は実費を求めてくる。	• 医療機器の場合、初期化はできない…。通常は病院側で10本用意したUSBタイプのウイルスチェックツールをベンダーに貸し出し、ウイルスチェックしたうえで復旧 • ただし、病院側で用意したウイルスチェックUSBの使用を許可しないベンダー多数あり　➡　ウイルスチェックに多額の請求…
備品・消耗品購入	• PC、HDDなどPC関連 • 古いOS運用のため機器更新が必要な医療機器購入 • コピー・プリンタ印刷大量のため、トナー、コピー紙需要超大	• 復旧までに安全なPCが必要（参照系構築等） ⇒某PCメーカーより無償貸し出しオファーがあり助かった • 参照環境構築のサーバーが必要 ⇒基幹ベンダーがなかなか準備できずにバックアップ参照の開始が遅れた • 被害病院の一歩外は通常の平穏な社会。物品調達は容易だった
その他	• 電話回線増設費用 • 調査委員会運営費用	• 電話回線の増設は業務運営上必須（送信用・受信用の切り分け） • 外部委員による調査委員会運営にも経費が…

【医療継続の振り返り】（IT-BCPの参考に）

予備のサーバーは？
バックアップはどこ？

【反省点】

- **参照環境構築の訓練**を行うべきだった
  （医療継続の最大のポイントであることの認識がなかった）

字が汚い…
読めない…

- **長期間を想定した紙運用の訓練**を行うべきだった
  （長期システム障害を見据えた紙帳票の見直し・運用の確認など）

この紙を誰がどこに運ぶ？
コピーはいる？

- 障害発生時の連絡先を事前に整理しておくべきだった
  （混乱状況では統制がとれていなかった）

- システム障害時に利用するデータやツールは、
  電子カルテ端末に保管すべきでなかった（利用できなかった）

【医療継続の振り返り】（IT-BCPの参考に）

【良かった点】

- 情報コミュニケーションツールを複数準備・稼働しておいてよかった

- 当日に記者会見し状況を公表することで患者への理解が得られ、
  他医療機関への協力も得られやすかった

- 災害訓練を毎年行い、災害対応を組織的に行う風土があってよかった。

たまたま（運よく）
別のネットワーク、
別のセキュリティ
だった

- **過去カルテを閲覧できるDACSが被害を免れていて良かった！**
  ⇒手術の早期再開、医療継続、転院のための情報確認など大いに有用

はじめに　いったい何が起きたのか

- 病原体のようなウイルスが侵入し、感染（増殖）したわけではない。
- 強盗のように、土足でシステム内に外部から侵入され、電子カルテデータを人力で暗号化され、人質にとられ身代金を要求されたたもの。
- 安全安心かつ効率効果的な医療提供を実現するために、高度かつ複雑なシステム化により医療運営を行っていた病院は、その記憶（データ）を失い、その業務運営を行うための医療システムを使用できなくなった。
- システムが復旧されるまでの約2ヶ月の間、医療安全を担保できる程度にまで医療制限を行いながら、現場の努力により可能な医療を継続。

検討すべきは、ウイルス感染対策ではなく、防犯対策だった

なぜ　こんな被害になったのか…　答えは「鍵」

- 「鍵」はシステムではＩＤとパスワード。例えばホテルの鍵を想像してみましょう。
  - ◆ 鍵を紛失したら、そのまま放置しますか？
  - ◆ 針金で開くような簡易な鍵にしますか？
  - ◆ 宿泊客に渡す鍵が、他のどの部屋でも開く鍵にしますか？
  - ◆ 客室の鍵と、部屋内の金庫の鍵を同じにしますか？
  - ◆ マスターキーを、第３者に提供することがありますか？
  - ◆ 鍵のかかる入り口を、毎晩施錠確認していないことってありますか？

実は、こんな状況がすべて行われていた結果のサイバー攻撃
起きるべきして起きた事案で、執るべき再発防止策も単純明快
「鍵の設定・管理方法」の見直し

インシデントの概要と直接的発生要因

ポイント

・外部接続管理

（水際対策の不備）

・内部設定の不備

（水平展開を引き起こした脆弱性）

キーワード：リモートデスクトップ（RDP）

便利：リモートワーク、リモート保守

危険：セキュリティリスク

（ID/パスワード流出、サイバー攻撃）

直接的発生要因

【業者（サプライチェーン）側の直接的問題点】

- 脆弱性管理の不備
- 簡易なパスワード設定

【病院側の直接的問題点】

- 外部接続の管理不備
- 内部設定（Windows初期設定）の不備
  - ・全ユーザー管理者権限運用
  - ・サーバーパスワード共通

    （クライアントパスワードも共通：職員認証はICカード＋PIN）
  - ・アカウントロックアウト未設定
  - ・電子カルテサーバーにウイルス対策未設定

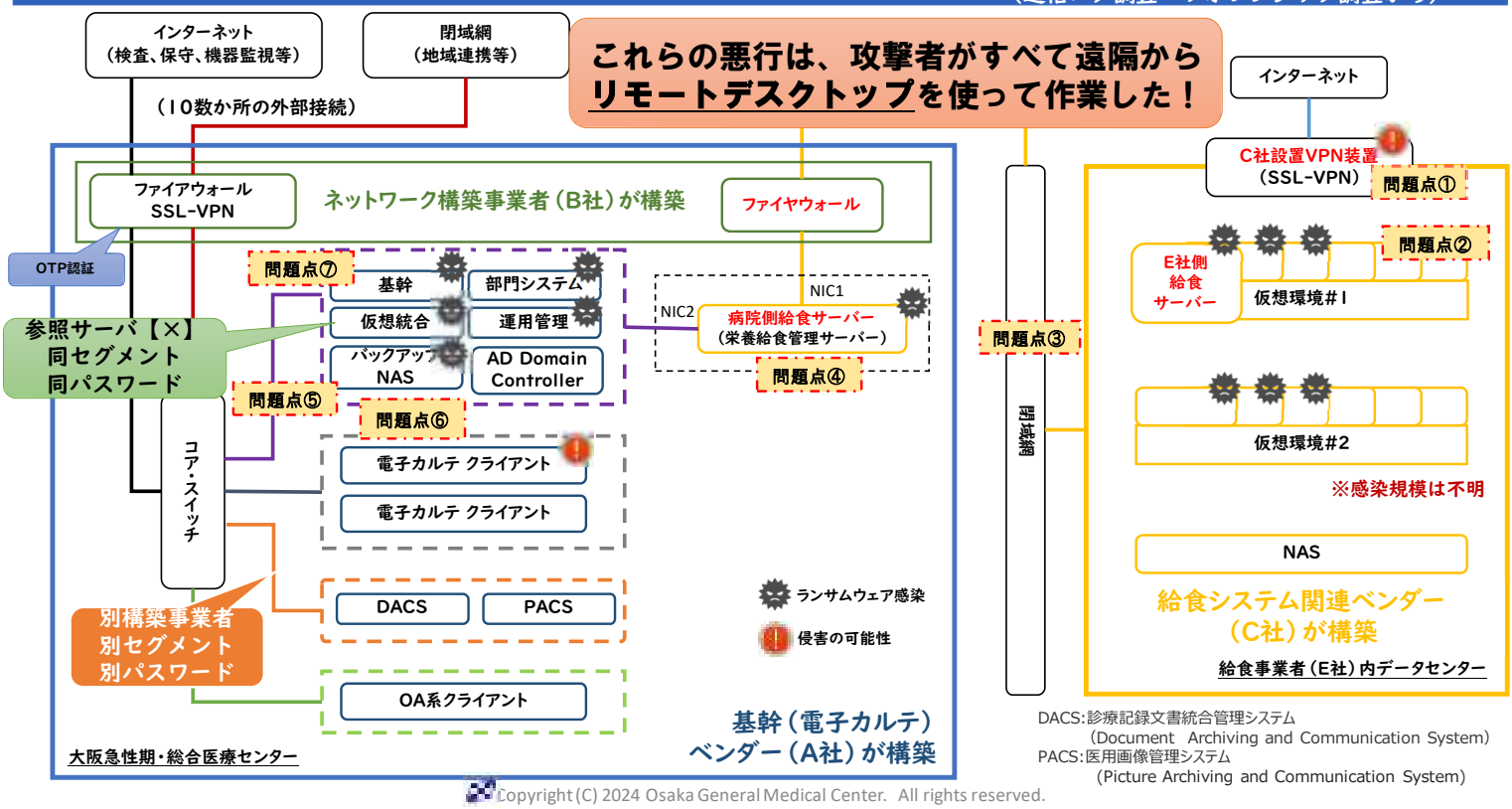
侵入経過

	項目	Xの手順
①	XがE社給食センターに侵入	E社給食センターに、C社が設置したVPN機器の脆弱性（または、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。
②	E社探索・情報窃取	E社給食センターのサーバーのID・パスワードが脆弱だったことから、X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、給食センター内での攻撃拡大。
③	病院給食サーバー侵入	病院側ファイアウォールを通じて、病院とE社が常時接続のRDP通信で結ばれていたことから、E社給食センターで窃取した病院のサーバー認証情報を用いて、病院側給食サーバーに侵入。ウイルス対策ソフトをアンインストールした。
④	病院のシステム情報の窃取	病院側給食サーバーを踏み台に、病院の他サーバーの認証情報等を、Xがツールを用いて窃取。なお、給食サーバーと他サーバーのID・パスワードが共通だったため、認証情報の窃取は容易であった。
⑤	他サーバー侵入	窃取した認証情報等を用いて、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（暗号化ツールの実行）させ、ランサムノート（身代金要求文書）を表示した。

A社：当センター基幹システム構築・保守事業者　D社：給食アプリケーション提供事業者
B社：当センターネットワーク構築・保守事業者　E社：給食提供事業者
C社：給食システム構築・保守業者　X　：攻撃者

ネットワーク構成図と感染状況

▶個人情報漏洩の可能性は極めて低い
（通信ログ調査・フォレンジック調査から）



DACS:診療記録文書統合管理システム
(Document Archiving and Communication System)
PACS:医用画像管理システム
(Picture Archiving and Communication System)

問題点一覧

	内容	詳細
問題点① 給食事業者側	VPN機器の脆弱性を放置	VPN機器メーカーからの重大な脆弱性情報を、VPN機器を設置したE社が委託したシステム管理運営会社（C社）が放置していた。
問題点② 給食事業者側	簡易なパスワードのため容易に侵入	E社内のシステムを構築したC社が、サーバーのパスワードを容易に推測できるありふれた設定にしていた。
問題点③	外部接続(リモートデスクトップ)の管理不備	結果的に不要だったRDP常時接続を、C社の要求により開通し、その後、接続状況の管理・監視をすることなく放置していた。
問題点④	全てのアカウントユーザーに管理者権限あり	A社がすべてのアカウントを管理者権限で設定していたため、窃取されたID・PWでウイルス対策ソフトをアンインストールされた。
問題点⑤	アカウントロックの未設定	A社がシステム構築の段階でアカウントロックを未設定にしていたため、ブルートフォース攻撃（パスワード総当たり攻撃）を許してしまった。
問題点⑥	サーバーパスワードがすべて同じ。端末パスワードもすべて同じ。	A社がシステム構築の段階でA社管轄のサーバー群のパスワードをすべて同一に設定しており、一つのサーバーパスワードが窃取されると他の全ても容易に侵入される設計になっていた。
問題点⑦	電子カルテサーバーにアンチウイルス対策が未設定。	A社が構築したサーバーの大部分についてウイルス対策ソフトを設定していたが、電子カルテのデータベースサーバーだけは未設定だった。

今回の問題点に対する改善ポイント　※ これらは高額な費用が必要のない対策ばかり

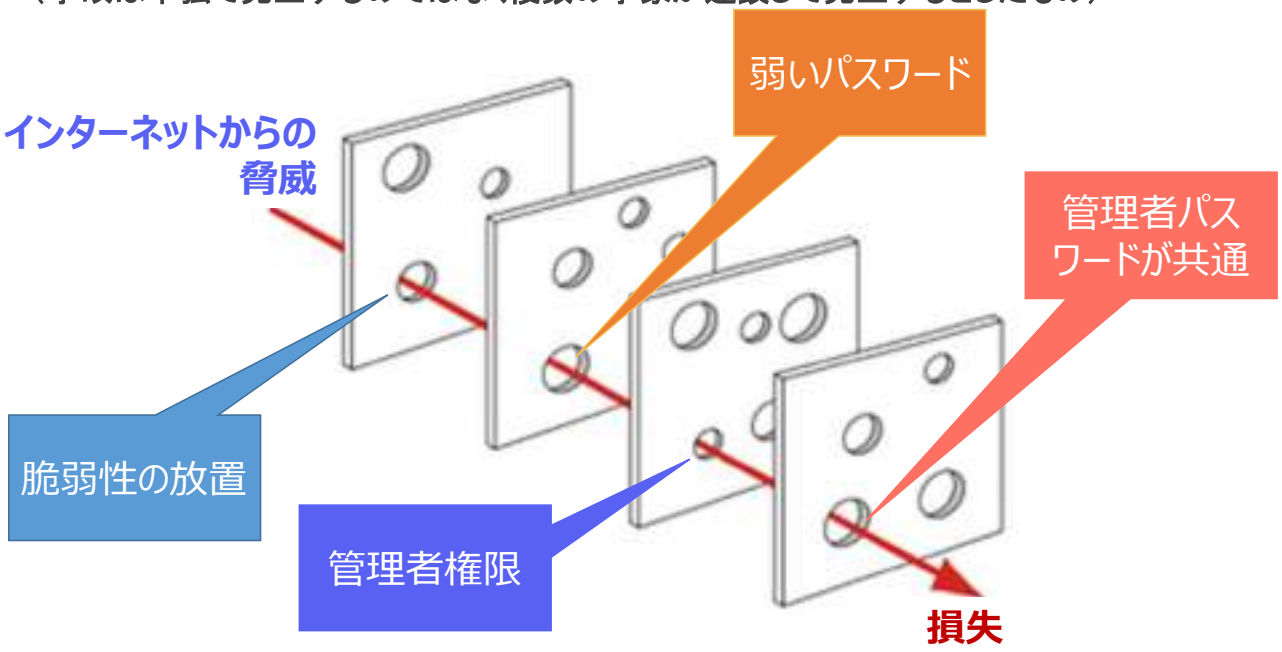
	問題点	改善ポイント
問題点① 給食事業者側	VPN機器の脆弱性を放置	脆弱性情報をいかにキャッチする情報力 ⇒ そもそも院内にどのような機器があるのか 一覧管理しておく必要がある（情報資産管理）
問題点② 給食事業者側	簡易なパスワードのため容易に侵入	強力な（長い）パスワードの設定 ⇒ サイバー以降の当センターポリシーは16桁以上
問題点③	外部接続（リモートデスクトップ）の管理不備	VPN等で外部接続（RDP）している通信は、その状況を確実に管理 ⇒ 当センターでは外部接続基準を策定し運用開始
問題点④	全てのアカウントユーザーに管理者権限あり	一般（標準）ユーザーでの運用 ⇒ 管理者権限のID/PWは一部の担当者のみで利用 一般利用者は全て標準ユーザー運用
問題点⑤	アカウントロックの未設定	アカウントロックの設定 ⇒ 試行期間：15分、失敗回数：5回まで、 ロック後のリセットまでの時間：15分
問題点⑥	サーバーパスワードがすべて同じ。端末パスワードもすべて同じ。	全てのサーバー・端末のパスワードを個別化 ⇒ 電子カルテのログインパスワードだけではダメ Windowsログインパスワードに対する意識改革が必要
問題点⑦	電子カルテサーバーにアンチウイルス対策が未設定。	電子カルテも含め全てのサーバー・端末にアンチウイルス対策 ⇒ 電子カルテネットワークに接続している 設備系のサーバー（ナースコール）にも適用

システム復旧後約2年運用しているが、問題は無い

一社）ソフトウェア協会提供資料

Swiss Cheese Model

（事故は単独で発生するのではなく複数の事象が連鎖して発生するとしたもの）



なぜインシデントが発生したのか？

- サプライチェーン側の**脆弱なシステム管理体制**（VPN機器管理不備、安易なPW）
  業務上の必要性で外部接続するのであれば、
  接続元のシステム管理体制を確認・監視すべきであった
- リモートデスクトップ接続の管理不備（**水際対策の不備**）
  リモートデスクトップによるリモート保守を許可するならば、
  その必要性やリスク評価、通信毎の接続管理など、厳格な管理を行うべきであった
- **水平展開を容易**にした共通サーバーパスワードと管理者権限運用
  管理者権限を持たせたアカウント運用では、悪意ある第三者に乗っ取られたら無力化に…
  さらには乗っ取られたID/PWを他のサーバーでも共通であれば、容易に水平展開可能に…

病院／システムベンダー／サプライチェーンそれぞれでの
システムセキュリティに対する意識・知識の向上が必要

IT-BCP策定の視点　外部接続機器の台帳管理

【大きな反省点】　外部接続機器の台帳管理ができていなかった

- 給食事業者との外部通信接続ポイントであったファイアウォールの通信ログ確認により、不正侵入経路はある程度特定された

↓

- 他の外部接続機器での通信ログの確認を行わなければ、侵入経路の特定ができないし、システム障害の特定もできない。

↓

- システム管理部門で把握していた外部通信機器は当初８カ所

↓

- 調査を進めていくと、いつの間にか医療機器の保守メンテ用外部接続機器が20カ所まで増大していた…

どこに外部への扉があり、扉の鍵の在りかもわからないような状況では、何か障害が発生した場合でも、どこの線を遮断すればいいのか解らず、どこを調査すべきか、混乱を極めることになり、初動対応時の大きな障壁となった

⇒医療機器保守用も含め、全ての外部接続機器を一元管理し、
その脆弱性管理および接続元等の厳重管理が極めて重要だった

皆さんの病院では、情報の把握をしていますか？

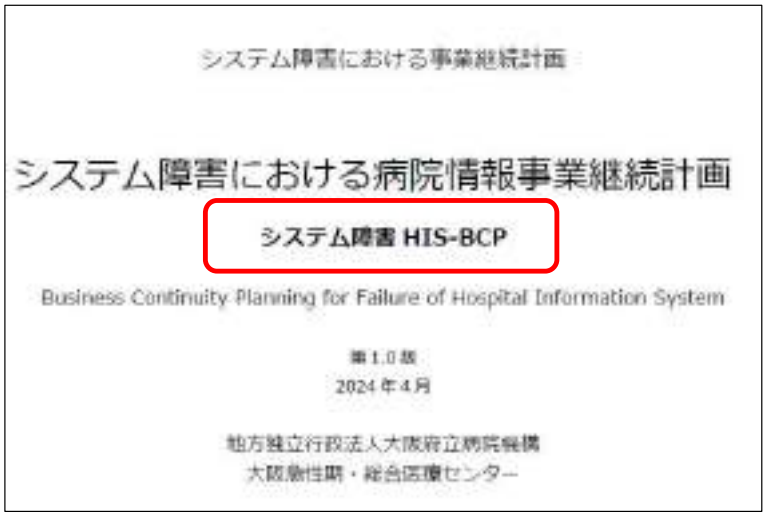
- 院内に設置の外部通信機器のリスト整備と脆弱性管理
  ⇒初期ID変更/PWの変更強化は当たり前！

- 外部からのリモート保守（リモートデスクトップ）の接続元確認
  ⇒システムベンダーはもちろん、医療機器ベンダーも対象に！

↓

**最近の病院でのランサムウェア事案は
外部接続管理の不備ばかり！！**

② インシデント事例に基づくIT-BCPの考え方


システム障害における事業継続計画

システム障害における病院情報事業継続計画

システム障害 HIS-BCP

Business Continuity Planning for Failure of Hospital Information System

第1.0版
2024年4月

地方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


システム障害における事業継続計画

システム障害における医療事業継続計画

システム障害 医療-BCP

System Failure Business Continuity Planning for Medical

第1.0版
2024年3月

地方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

当センターでは、システム障害に対応するBCP を2種類作成

3種類のBCP（2024.4月時点）

BCP 名称・組織体 整理表

		一般災害における事業継続計画	特殊災害における事業継続計画	システム障害における事業継続計画	
正式名称		GD-BCP General Disaster business continuity planning	ED-BCP Extraordinary Disaster business continuity planning	SF-BCP System Failure business continuity planning	
				事業継続計画統括管理部門：運営会議	
				システム障害における医療事業継続計画	システム障害における病院情報事業継続計画
略式名称		一般災害BCP	特殊災害BCP	システム障害-医療-BCP SF-BCP（for Medical）	システム障害-HIS-BCP 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
目的		自然災害（地震・風水害等）や人為災害（局地災害全般）発生時において、事業継続に支障が生じる事案が発生した場合の事業を継続するための計画	一般災害におけるBCPでは適用できないような特殊災害（NBC・原子力発電事故、新興感染症、テロ等。システム障害を除く）発生時において、事業継続に支障が生じる事案が発生した場合の事業を継続するための計画	ランサムウェアを含むサイバー攻撃等により大規模システム障害が発生した場合の医療事業の継続を行うための計画	ランサムウェアを含むサイバー攻撃等により大規模システム障害となった場合のシステム障害対応を視点とした病院情報システム事業継続および復旧に係る計画
BCP承認・改編組織		災害対策委員会	災害対策委員会	災害対策委員会	医療情報システム安全管理委員会
運営本部組織		災害対策本部	災害対策本部	医療継続対策本部	システム復旧対策本部
	本部長	総長	総長	総長	病院長
	副本部長	病院長	病院長	病院長	医療情報部長 （医療情報システム安全管理者）
	庶務等運営主体	災害対策室	災害対策室	災害対策室	医療情報部
	構成員	運営会議 災害対策室	運営会議 災害対策室	運営会議 災害対策室 各管理部門 常設委員	医療情報システム安全管理委員会 医療情報部 基幹ベンダー 主要部門ベンダー ネットワークベンダー セキュリティベンダー
	初動対応時本部設置場所	総長応接室	総長応接室	第7会議室	コンピューター研修室
BCP策定状況		広域自然災害対応BCP：2023/3/31第7版改定 BCP策定状況 自然 人為 広域 ○ - 局地 - -	今後策定するかも含め検討予定	2024/3/15 初版制定	2024/4/12 初版制定（予定）

- 自然災害用のBCPでは対応できなかった長期システム障害
- 様々な医療現場での紙運用や参照環境稼働後の運用など、医療継続用のBCPも必要に

大規模システム障害時の
医療継続におけるIT-BCP検討テーマ

① 参照環境の構築
② 紙運用の整備
③ コミュニケーション（内部・外部）

なぜ参照環境の構築が必要なのか？

- 電子カルテサーバーが侵害された場合は、**連携する部門システムおよび端末も汚染されている可能性**が十分にある。
- 全体の調査を進め、発生原因を確認しない限り、復旧作業に移行できない。
- その間にも、電子カルテに眠る患者情報の確認は、現場での医療継続における喫緊の要求事項となる

（転院時の紹介、手術実施、患者家族への連絡先確認など…）

システム復旧までの期間、現場での医療継続を行うためには、
☑ バックアップデータを活用し、
☑ 安全なサーバーにリストアしたうえで、
☑ 安全確認（安全を確保した）ネットワーク上で、
☑ 安全確認された可能な限り多くの端末より、
参照できる環境を構築する必要がある
（現場で情報を参照するには紙印刷が必要！）

大規模システム障害時の医療継続に対するIT-BCP上の課題 ① 参照環境の構築

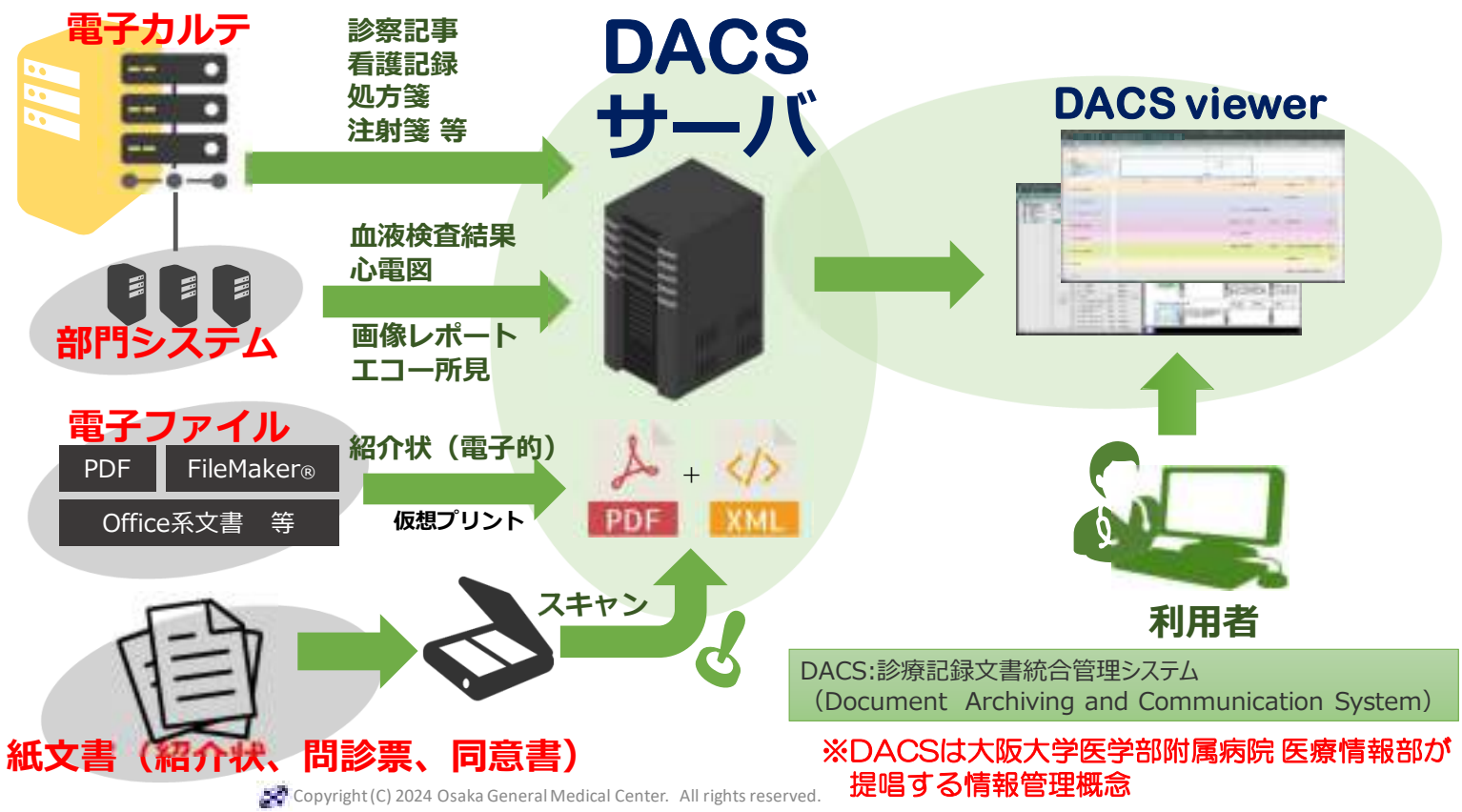
①参照環境の構築　：　参照環境は電子カルテ障害発生時の医療継続の切り札
医療継続のためには最優先に考えるべきテーマ

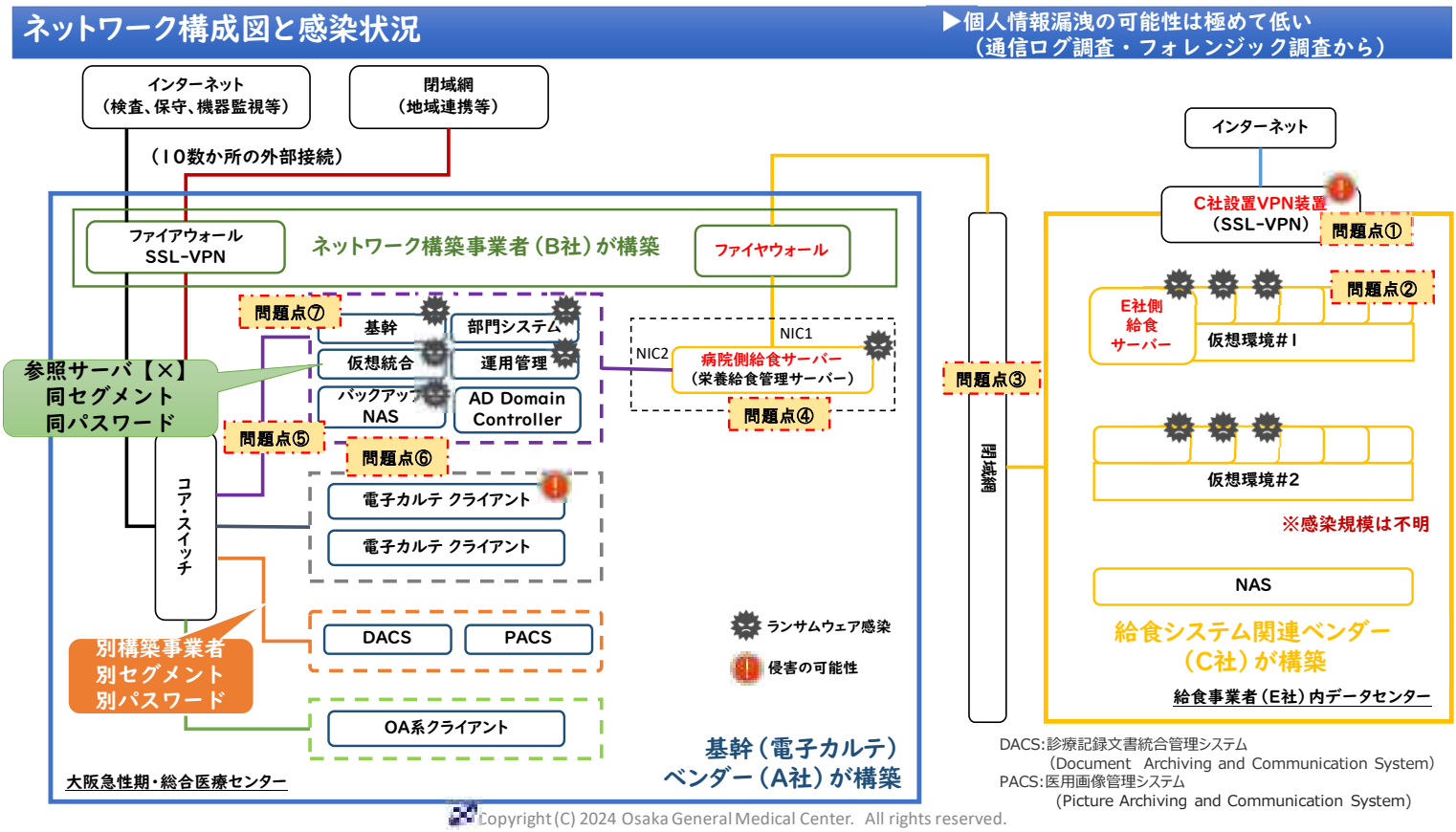
課題となったポイント	バックアップによる参照環境構築に10日間
理由	バックアップをマウントする安全なサーバー確保に7日間
視点	• 参照環境の早期構築により、医療継続・拡充が可能 • 医療継続には患者情報は必須。 • バックアップ参照は安全なバックアップデータが必須。 • オフラインバックアップの確立
当センターの状況	• 運よく被害を免れたDACSの参照を障害発生翌日から開始 DACS参照開始により予定手術の一部再開、転院時患者情報提供の開始 （これがなければ医療継続にかなりのダメージ） • バックアップ参照開始から救急受入再開 • バックアップ参照場所の拡充　⇒　予定手術枠の拡充、救急受入拡充

大規模システム障害時の医療継続に対するIT-BCP上の課題 ① 参照環境の構築

①参照環境の構築

IT-BCP検討事項	【一般的にはDACSを備えている病院は僅か。バックアップからの参照構築を検討すべき】 • 参照環境を構築する手順の確認 （サーバー確保、端末参照場所など） • オフラインバックアップの確保 • 参照環境用のサーバー、参照用端末の調達確保 • 大量のコピー用紙やトナーの確保が必要 • 参照環境を1カ所に集めて行う場合は、電源容量の確認も必要 • 通常運用のサーバーダウンを想定した参照サーバーはセグメントを分けるなど、万が一に備えた万全なシステム設計を行う （マイクロセグメンテーションの考え方） • ランサムウェア被害に遭った場合でも、直ちに安全な参照環境へ移行できるシステム設計であれば、医療継続へかなりの助力になるのでは… （バックアップのクラウド化など）。





DACS参照/バックアップ参照の違い（当センターの場合）

	DACS参照 （初期設定次第で相違）	バックアップ参照 （電子カルテ製品により相違）
患者情報	PACS以外のほぼ全ての患者情報が収載 （看護記録、スキャンデータ、画像レポートなど） ※アレルギー情報など患者基本情報は不可 ※部門システム側情報も初期設定すればDACS参照可	医師の診療録（カルテ記事、オーダー情報など） 血液検査データ、患者基本情報 ※部門システム側に参照する情報は不可
予約情報	病院側業務系の情報は不可 （予約患者一覧、入院患者一覧など参照不可）	予約患者一覧など電子カルテの機能にある業務系情報が参照可能
参照期間	記事等作成（更新）時にタイムリーに保存されるため、システム障害直前まで参照可能	バックアップ取得期間に限られる （最終のバックアップからシステム障害まではデータ欠損） ⇒診療記録の保存に問題（請求の根拠が消失）
本件システム障害時	・セグメントが異なっていた （意図せず結果的にﾏｲｸﾛｾｸﾞﾒﾝﾃｰｼｮﾝが成立していた） ・サーバーパスワードが異なっていた （構築事業者が異なっていたため意図せず結果的に） ⇒　無事が確認できたため、直ちに参照環境準備	• オンラインバックアップは暗号化 • 土曜日夜から開始（通常48時間以上必要）のフルバックアップ中にサイバー攻撃 • LTO遠隔地保管（オフラインバックアップ）の生存確認 ⇒バックアップ参照環境構築に１０日必要

サーバ確保に１週間

医療復旧状況経過

10/31（Day1）	救急受入停止、予定手術停止、新規患者受入停止、外来原則休止、紙カルテ・紙伝票運用開始
11/1（Day2）	DACS参照開始 外来化学療法再開（抗がん剤混注監査システムの無事確認）
11/4（Day5）	予定手術再開（1日4～5列程度）
11/10（Day11）	バックアップ参照開始 三次救急一部受け入れ再開
11/14（Day15）	内視鏡室再開
11/17（Day18）	救急外来（ER）再開（バックアップ参照端末を救急外来に設置）
11/28（Day23）	PACS参照センター開設 予定手術枠拡充（1日7～8列程度）（バックアップ参照端末を中央手術室に設置）
12/12（Day43）	外来電子カルテ運用再開（基幹システム運用再開）/部門システム一部再開（調剤、検体検査　他）
12/20（Day50）	部門システム一部再開（生理、輸血、DACS　他）　※先行して12/14にPACS、RISを再開
12/22（Day53）	病棟電子カルテ運用再開/部門システム一部再開（給食、手術、重症　他） 予約初診患者受入再開
12/27（Day58）	部門システム一部再開（微生物、病理、内視鏡、心電図、脳波、診断書作成、DPC情報他）
1/4（Day66）	外来当日会計再開
1/10（Day72）	予定手術枠拡充（1日8～9列程度）
1/11（Day73）	部門システム一部再開（周産期、リハビリ、NST、透析、DWH、麻酔管理他） 診療体制全面復旧宣言
1/16（Day78）	手術枠100%再開（1日9～10列）

BCP訓練の視点①　バックアップデータ

バックアップデータから、参照環境の構築およびシステム復旧ができるか

【データ自体の確認】

① バックアップデータの安全確認（汚染状況確認）の手順確認

② バックアップデータが計画通りのデータになっているか確認

- ■ オフラインバックアップが取得されていることが前提
- ■ バックアップデータの真正性を確保するため、全サーバーでのウイルス対策ソフトの稼働が必須

【参照環境構築手順の確認】

③ 参照環境構築までの手順確認（機器調達・参照場所）

④ バックアップデータより正しく参照環境構築・運用ができるか確認

【システム復旧手順の確認】

⑤ システム復旧までの手順確認

⑥ バックアップデータより正しくシステム復旧できるか確認

- ■ システム稼働中は、バックアップ確認用サーバーが別途必要となるため、確認が困難。
  - ➡システム更新時のテスト仕様に必ず含め、試験手順書と、合格確認書を取得する。

大規模システム障害時の医療継続に対するBCP上の課題 ② 紙運用の整備

②紙運用の整備　：　システム障害時の医療継続には昔ながらの紙運用。ただし昔と今では時代が違う。

課題となったポイント	• システム更新時や自然災害用の短期間の紙運用しか想定していなかった • 紙様式の見直しが行えていなかった • 紙様式データが電子カルテ内のグループウェアに保管され、取り出せずに最初から作成 • 紙を動かす「人」の想定（デリバリー運用）を行っていなかった • 紙記載の慣れていない若手から中堅層の苦手意識が強かった • 字が汚い職員が多く、医療安全上のリスクが高くなった（確認作業が増大）
視点	• 紙運用への切り替えは、人の動きも物の動きも情報の動きも全てが変わる • 患者安全管理手段についても、大きな変更が伴う（バーコードなしの患者認証など）
当センターの状況	• 当初準備していた紙様式が使い物にならず、大至急で新様式を作成し運用を開始 • 医師の字の汚さが目立ち、至る所で問い合わせや照会作業が発生 • 職員（特に医師）からパソコン入力による患者情報記載の要望が多数発生 • 慣れない紙運用のため、スタッフによる複数・多重チェックの業務量増大

大規模システム障害時の医療継続に対するBCP上の課題 ② 紙運用の整備

②紙運用の整備

IT-BCP 検討事項	• 長期間の紙運用を行う前提で、紙伝票の運搬も含めた訓練を通じて実践し確認 • 紙様式のレビューを定期的に行い、実際の運用に適合しているか確認しておく • 紙様式のデータは、電子カルテ系ネットワークとは別に保管しておく • 安全なPC端末を利用した診療記録作成や指示作成の運用を予め検討しておくと、指示出し、指示受けの各担当のストレスがかなり軽減され、医療安全上のリスクも低減 ➤ 相当数の安全な端末PC確保が必要 ➤ 患者センシティブ情報を入力できる環境であるかの確認が必要 ☆ 電子カルテ復旧後の紙カルテ保存方法にも留意 （どこまで再入力するか？ 当Cではほぼ全てスキャンでDACS参照） ☆ 復旧後に医事会計手入力処理を行うことが前提。会計入力を想定した様式作成と運用フローの構築が必須！

BCP訓練の視点②　紙運用切り替えの確認

長期間の電子カルテ障害から紙カルテ運用に円滑に移行できるか

【紙カルテ運用移行決定手順の確認】

① システム障害に伴う長期の紙カルテ移行運用の決定手順確認

② 各紙帳票の準備手順確認／紙カルテ運用時の運用ルール確認（診療記録記載要領など）

【各紙帳票（伝票）の運用確認】

③ 各帳票の内容確認・運用手順の確認
（コピー枚数：発生現場保管用・依頼先用・医事会計用など）
（搬送担当、依頼先確認方法、疑義照会方法、システム復旧後の保存方法）

④ 院外処方箋など外部への紙帳票の発行手順から疑義照会対応手順の確認

【その他】

⑤ 外来患者受付方法・会計案内方法の手順確認、患者ID発番方法の確認

⑥ 入院患者リスト（病院全体）の管理方法の確認（院内・院外からの問い合わせ対応）

⑦ システム復旧時に入院履歴、病名、食事歴、看護必要度の入力は必須。手順を確認。
（字を書くのに慣れない若手職員の手書き訓練／ワープロ端末準備手順確認　など）

大規模システム障害時の医療継続に対するBCP上の課題 ③ コミュニケーション

③コミュニケーション ： 非常時には内部および外部のコミュニケーション手段の確立が重要

課題となったポイント	• 病院全体に病院方針を周知するためのコミュニケーションツールが必要 （当センターで通常利用していた電子カルテ上のグループウェアは利用不可に） • セキュリティインシデント発生時の外部連絡リストは必要 （本事案で一番の要であった厚生労働省への連絡が一番最後に…） （救急指令本部への連絡が抜けていた。担当を指示していなかった…）
視点	非常時には各方面への情報の伝達・共有は必須だが、混乱期には十分に対応できない 患者に対する周知も必要なため、報道発表は効率・効果的なツール
当センターの状況	【内部】 • 災害BCP用のツールと、別系統のグループウェアとを組み合わせて病院運営方針を院内周知 【外部】 • 事務局を中心に、思いつくまま重要な関係先および警察に報告 • システム関係者にはシステム部門より連絡 • 発生当日夜に報道発表・記者会見を開催し、広く周知

大規模システム障害時の医療継続に対するBCP上の課題 ③ コミュニケーション

③コミュニケーション ： 非常時には内部および外部のコミュニケーション手段の確立が重要

IT-BCP検討事項	• 院内のコミュニケーションツールは複数準備しておく • セキュリティインシデント発生時の外部連絡先リスト整備の際には担当部署も定める • （組織的な事情もありますが） 報道発表は効果抜群。患者や関係ステークホルダーへの周知だけでなく、医療関係者から多くの支援が受けられる • システム障害の原因調査や復旧には専門家の力なくしてあり得ない。専門家のコンタクトリストも準備しておく （厚労省事業で初動対応支援チームの派遣を受けられる可能性あり）

BCP訓練の視点③　コミュニケーション確認

電子カルテというコミュニケーションツール喪失時の情報伝達・共有手段の確認

【院内の情報伝達方法の確認】

① 病院内にあるコミュニケーションツールの死活確認

② 病院の方針決定を、現場に対して、だれがどのように周知するかを確認

【院外への連絡方法の確認】

③ 外部への連絡先、連絡担当、連絡優先順位の確認（地域医療機関、救急含む）

④ ホームページやSNSの発信、報道発表の確認（実施確認、手順も含む）

⑤ 電話回線の確保手順、患者電話対応担当の確認

【その他】

⑥ ネットワーク接続が行われている機関への抜線依頼も必要（オンライン資格確認など）
（医療機器ベンダー等が独自に回線を開設している場合もありうることに留意）

大阪急性期・総合医療センターにおけるIT-BCPの作成視点

① 医療継続とシステム調査・復旧は別の動きに

- システム障害になっても患者は目の前に。システム長期使用不可の際に医療を継続するための現場BCPと、システムを早期復旧させるためのBCPとは、概念が異なる。

【当センターのIT-BCP】2系統のIT-BCPを整備

➡ システム障害を想定した現場医療レベルでの医療継続BCP（災害対策委員会管轄）

➡ システム部門におけるBCP（医療情報システム安全管理委員会管轄）

② 夜間休日の発生時の運用（一般的な病院の体制を想定）

- 自然災害とは異なり、在宅勤務者は病院の異常事態がわからない
- 夜間休日に、病院にはシステムの異常がわかり、迅速に対応できる人材がいない
- システム担当に連絡が入っても、夜間休日の場合は適切な処置や円滑な業者連絡ができない

【当センターのIT-BCP】発見者の一次対応を明確に

➡ 発見者が行うべき行動を明確に

➡ 連絡体制は、医療継続（災害対策）とシステム運用（医療情報）の2系統

③ システム障害の状況や規模、範囲は千差万別

- 細かいBCPはかえって足枷に
- 事務局の役割を明確に（内部・外部コミュニケーション担当）

【当センターのIT-BCP】初動対応における枠組みと検討すべき視点を事前に整理

医療継続BCPの目次

HIS-BCPの目次

サイバー攻撃かなっと思ったら、まずやるべきこと

① 可能な限り、付近の電子カルテ端末（HIS端末）のネットワークを切断する。

② 各種窓口へ連絡する。

【平日 8:00 ～ 21:00】 【休日 8:00 ～ 17:00】	ヘルプデスク（内線：2600、2601）
【上記以外】	事務当直：2350

徳島大学病院画像提供

初回緊急会議　確認・協議事項（当C　IT-BCP　4.3.4）

初回緊急幹部会議の場では、以下の情報確認および当面の方針を決定する。

内容	主な確認事項
現状確認	□ 発生からの時系列確認 □ 各システム運用状況 □ ランサムウェア等ウイルス感染状況 □ 医療提供体制状況（患者数確認）
対策本部会議	□ 事業継続計画対策本部会議の設置確認 ➢ 初回会議開始時間の確認 ⇒ 災害対策室主導で運営開始 □ システム障害復旧対策本部会議の設置確認 ➢ 医療情報部内で初回会議開催時間を調整し運営開始
コミュニケーション	□ 院内職員への周知情報の確認（院内放送含む） □ 報道提供・記者会見の実施を確認 □ 予め作成している外部連絡先リストに基づき各分担で連絡実施 □ 院内の情報共有ツールの死活確認及び職員との情報共有手段の確認 □ 警察への通報実施の必要性を確認
その他	□ 初回会議までに必要な情報及びその担当を確認 □ 会議・作業場所の確保（予約済みの会議室は病院管理者権限により予約解消を通知） □ 電話回線（外部通信手段）の確保 □ コピー機，コピー用紙、トナーの確保

システム障害における訓練の視点（医療継続）

電子カルテ等が長期間使用不能になると確認された時点での訓練を想定しておくべき

	視点	考え方
外来患者対応	来院患者をどのようにトリアージし、帰宅させていくか。	• 医師によるトリアージが患者には安心、混乱も縮減 • 次回予約をどのように行い管理をしておくか • 投薬対応の場合、どのように院外処方箋を発行するか • 患者を他院へ紹介する場合の診療情報発信手段は？
入院患者対応	入院患者の安全管理をどのうに行うか	• 各病棟在院患者のリストや治療情報をどう再作成するか • 既存の紙情報はどこに何があるか。アレルギー情報は？ • リストバンドは使えない。どうやって患者認証を行うか • 病院全体の入院患者リストの作成と更新はどこで誰が？
救急患者対応	救急車受入れ判断をどのように行うか	• やむをえず受入れとなった場合、患者IDをどう発番するか • かかりつけ患者の搬送依頼をどこまで対応するか
紹介患者対応	紹介初診予定、入院予定の患者に、どうやって連絡をとるか	• 連絡先の情報をどのように取得するか。 • 状況を知らずに来院した患者にどのように対応するか

**システム障害は自然災害と異なり、「ヒト」「モノ」は潤沢にあり、
システム以外のインフラも無事。病院の一歩外は平穏な社会。
職員全員で知恵を出し合いながら、活用できる資源を活かして「全開」で対応
患者安全を確保しながら徐々に医療規模の増加に取り組む**

システム障害における訓練の視点（システム復旧）

ランサムウェア等による電子カルテ等が長期間使用不能になると確認された時点での復旧工程訓練を想定しておくべき

	視点	考え方
バックアップ	バックアップデータの死活が今後の医療継続に左右する	• バックアップデータの安全確認の手順確認 • バックアップデータが適切に利用できるか確認
参照環境	システム復旧までの医療継続の切り札	• 参照環境の構築手順を確認 • 安全なサーバーや参照端末の手配確認
安全確保	復旧作業中に再感染しないこと、個人情報漏洩を絶対に起こさないことに留意する	• ウイルスチェックツールの運用手順確認 • ネットワーク監視手順の確認 • 医療機器のスタンドアロン運用再開手順確認
外部通信	復旧に着手するには一定の調査が必要。全ての外部接続箇所の通信状況を確認しないと発生原因の絞り込みができない	• 外部接続箇所のリストは作成されているか • 外部接続機器の通信ログは取得されているか • 外部接続機器の通信状況に異常がないか • 情報漏洩の可能性はないか

**異常事態時は全ての職員がストレスフルな状況に陥る。
休息を確実にとりながら（とらせながら）
メンタルヘルスを維持しましょう。
「こんなときだからこそ休息を」を合言葉に。**

さいごに　鍵のお話

- 電子カルテの「鍵」は、ユーザー（医療者）が、電子カルテアプリケーションにログインするための「鍵」だけではない。
  （もちろん、電子カルテを「診療録」として扱うためには重要）

- 電子カルテアプリケーションを動かすためのＯＳ（Windowsなど）にログインするための「鍵」こそが、システムの安全管理を行う上で、重要なことと気付かされた今回の事案。

- みなさまの医療機関でも、サーバーや端末、VPN機器などの「鍵」の管理を、「自分の家の鍵のように今一度見直し」てみれば、自施設に合った適切な管理方法が見えてくるのではないでしょうか。
  ⇒この鍵管理の見直しこそが、平時におけるBCP

ご清聴ありがとうございました。各医療機関で適切なBCPを策定し、日本の医療を守りましょう。

自然災害用 BCP

システム障害用 BCP

医療継続用のIT－BCP

大阪急性期・総合医療センター災害対策室　仲桝哲

システム障害（サイバー攻撃）

10月31日の朝

各所属で院内PCの異変に気付

ランサムウェアによる被害

災害

被害の規模からすぐに災害のスイッチを入れることに

システム障害（サイバー攻撃）

災害のスイッチ

すぐに幹部を招集して会議体を設置

コロナ対応のノウハウを生かして当時

迅速に現状分析のため情報収集を行った

各部署でなにが問題なのか？
紙運用に戻すために何が必要なのか？

対応方針

当院の災害対応

今回のシステム障害
における被害状況

対応方針の術として

自然災害用のBCP

- 電子カルテのみ
- 職員の被害なし
- PC以外のインフラは問題なし
- 被害は当院のみ

対応不可

当院の災害対応

自然災害用のBCP

対応不可

- 南海トラフ地震の対応
- インフラの破綻
- 職員の未充足
- 多数傷病者対応

災害の本質
が全く違う

電子カルテシステムの破綻

電子カルテシステムの破綻

対応方針の術としてマニュアルがない

システム復旧

- ✓ 情報管理室
- ✓ システムベンダー
- ✓ 厚労省アドバイザー

今できる診療を模索する

- ✓ 診療の規模縮小（priority）
- ✓ 紙カルテ運用
- ✓ 紙カルテ運用ルール策定

新しい概念のBCP作成

システム復旧

- ✓ システムの早期回復を目指した専門的な対応

今できる診療を模索する

- ✓ 対応能力の限界
- ✓ 紙カルテ・RULEの整備

システム障害BCP ＝ SF－BCP（医療）
SF－BCP（HIS）

自然災害BCPとSF-BCPの違い

自然災害BCP

- ✓ 大地震を想定
- ✓ インフラ破綻時のダメージコントロール
- ✓ 多数傷病者受け入れ・対応方法
- ✓ 職員未充足における業務の優先順位
- ✓ 安否確認
- ✓ 地域・各種関係機関との連携・調整

自然災害BCPとSF-BCPの違い

SF-BCP［システム障害］

- ✓ 電子カルテシステムの機能破綻を想定
- ✓ システム復旧に向けた初期対応
- ✓ 紙カルテ運用における初動対応
- ✓ 全部署の紙カルテ様式の統一と共通認識
- ✓ 紙カルテ運用におけるルール策定

自然災害BCPとSF-BCPの違い

自然災害BCP

- ✓ 横軸に発災後の**時間経過**
- ✓ 縦軸に**業務内容**
- ✓ **優先順位**の決め方
- ✓ 通常業務を何から始めるか
- ✓ 復興させるプロセス

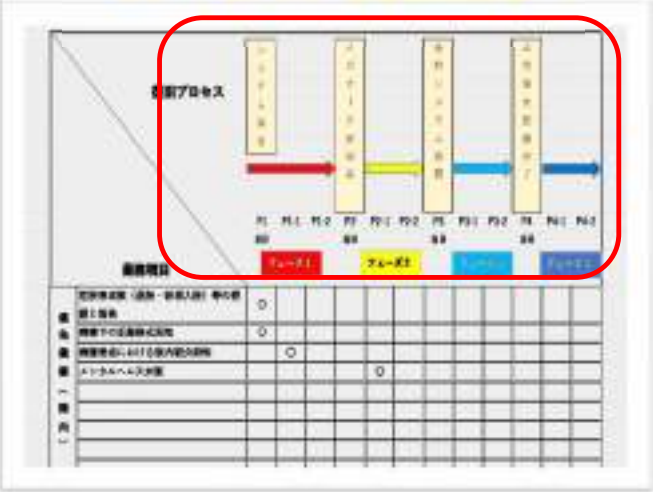
自然災害BCPとSF-BCPの違い

SF-BCP（医療）

- ✓ 横軸にシステム復旧プロセス
- ✓ 縦軸にプロセスに合わせた業務
- ✓ **基本的に紙カルテ運用方法**
- ✓ 院内業務と院外業務
- ✓ サージ業務への対応方法
- ✓ 紙カルテから電子カルテへの移行段階

自然災害BCPとSF-BCPの違い

SF-BCP（医療）



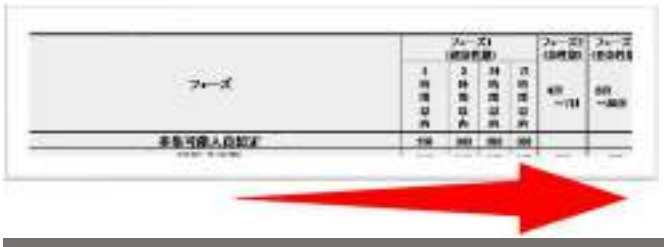
自然災害BCP

横軸の変数に、「復旧プロセス」「発災後の時間経過」

自然災害BCPとSF-BCPの違い

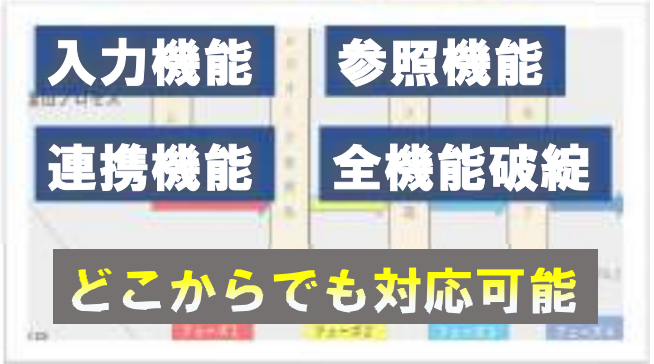
横軸の変数に、「復旧プロセス」「発災後の時間経過」

自然災害BCP



対応する順序が決まっている

SF-BCP（医療）



どこからでも対応可能

SF-BCPの特徴

システム障害

- 患者情報が分からない
- 治療の継続が困難
- 転院させるのも困難
- 患者・地域への影響が大きい
- しかし、人も物も充足している

SF-BCP（医療）

✓ 暗闇の中手探りにもがくのではなく、効率的に事業継続させるためのマニュアルである。

- システム復旧と同時並行
- 復旧プロセスに合わせた業務

SF-BCPの特徴

SF-BCPを運用するポイント

CSCA

- ✓ 組織やチームを動かすとき
- ✓ 問題を抽出して対応する際
- ✓ 全ての災害を対応可能にする

再構築

組織

SF-BCPの特徴

SF-BCPを運用するポイント

C：Command & Control　指揮と連携
S：Safety　安全
C：Communication　情報伝達
A：Assessment　評価

常にモニタリングを実施し
状況を把握し、紙運用の限界点を
知る

- ✓ 紙カルテ使用における安全
- ✓ 紙カルテにおける処理能力
- ✓ 紙カルテにおける処理の限界
- ✓ 薬、検査、手術等

安全確保

SF-BCPの特徴

SF-BCPを運用するポイント

C：Command & Control　指揮と連携
S：Safety　安全
C：Communication　情報伝達
A：Assessment　評価

情報共有方法と発信ツールの
確保

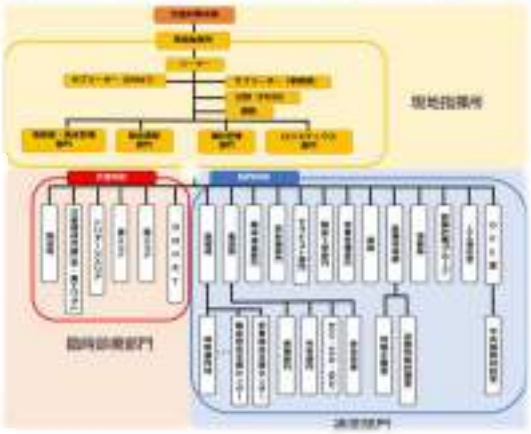
- ✓ 情報伝達は、ITを活用せざるを得ない
- ✓ 電子カルテシステムの代替ツール
- ✓ 勤怠システムのPCネットワーク
- ✓ 災害時の安否確認ツール

情報伝達と共有

SF-BCPの特徴

SF-BCP組織図

自然災害BCP組織図



役割を明確化

既存の委員会

副院長と看護部

情報共有 ← **組織横断的** → **情報発信**

システム障害を3か月で乗り越えた勝因

システム障害を経験して

ただ単に、紙カルテ（昔の運用）にもどすことではない

- 電子媒体を活用している医療現場の扱う情報量はとてつもなく膨大である。
- 昔と同じような紙運用には、簡単に戻れない。
- 電子カルテの不敗神話は存在しない。
- すぐに紙運用に戻れる体制作りが必要。
- 紙カルテ書式の用意が必要。
- システムの中に、セーフティーネットを必ず構築する。