サイバー攻撃を受けた経験と医療安全管理者へのメッセージ

令和6年度　国公私立大学附属病院医療安全セミナー
2024年6月6日

大阪急性期・総合医療センター
嶋津岳士

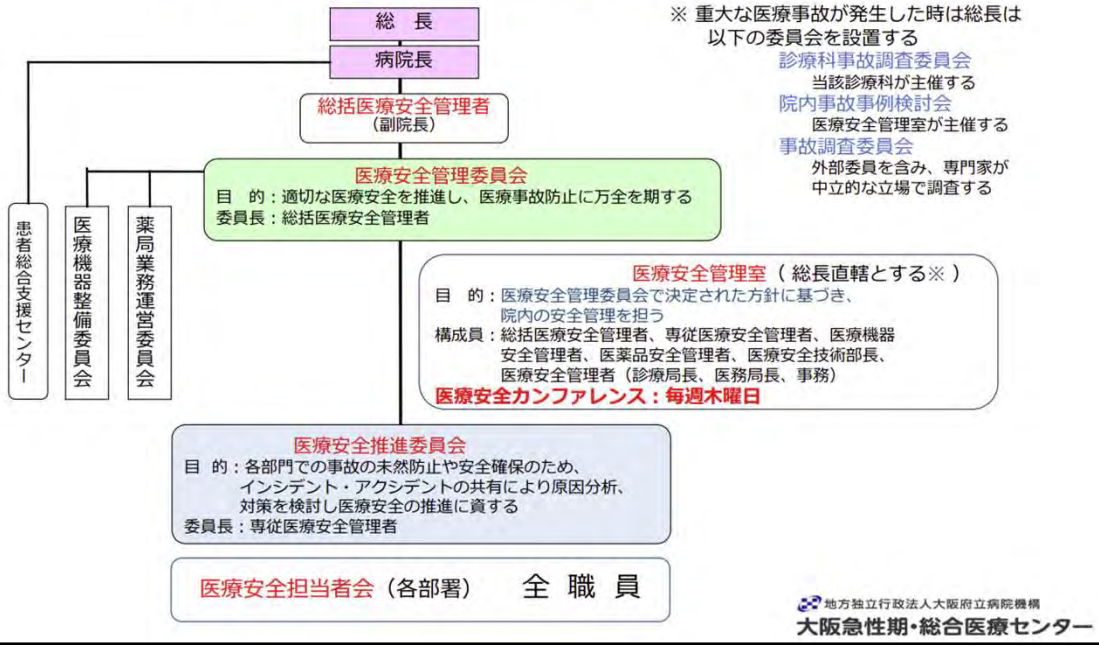
本日のTopics

- 大阪急性期・総合医療センターについて
- 何が起こったか：
  - インシデント発生当日の状況とその後の対応
- 今後の組織的セキュリティ強化計画
- システムダウンとインシデント発生
- 医療継続体制（BCP）について
- まとめ

大阪急性期・総合医療センターについて

病院名	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
病床数	865床（一般：831床、精神：34床） うちICU, CCU, SCU, HCU, MFICU, NICU, GCU 計91床 看護職員数（R4.4.1時点）；1,024人
診療科	36診療科 （医師数（R4.4.1時点）；259人、研修医50人）
病院の特徴	基幹災害拠点病院 高度救命救急センター（30床） 地域周産期母子医療センター（27床） 小児地域医療センター 地域医療支援病院 地域がん診療連携拠点病院 他
主な診療実績	【令和3年度実績】 延べ入院患者数 22.3万人（内コロナ患者約6千人） 延べ外来患者数 29.5万人 【直近令和4年9月実績】 新入院患者数 52.5人／日 延べ入院患者数 646人／日 平均在院日数 11.0日 初診外来患者数 123.0人／日 延べ外来患者数 1,268人／日 救急車搬入患者数 641人／月 中央手術室手術件数 542件／月

当センターの医療安全管理体制



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

すべてのファイルは暗号化されました！

- すべてのファイルは、あなたのパソコンのセキュリティーの問題により、暗号化されました。もし復元したければ、我々にメールを送ってください。　＊＊＊＊
- メールのタイトルにはこのIDを書いてください。　＊＊＊＊
- 24時間以内に返信がなければ、このアドレスに送ってください。　＊＊＊＊
- 復元のためには、ビットコインで支払ってください。金額はあなたがどれだけ早く我々にメールを送るかによって変わります。
  支払い後、すべてのファイルを復元するためのツールをおくります。
- **保証としての無料の暗号化**
- **ビットコインの入手方法**
- **注意！**

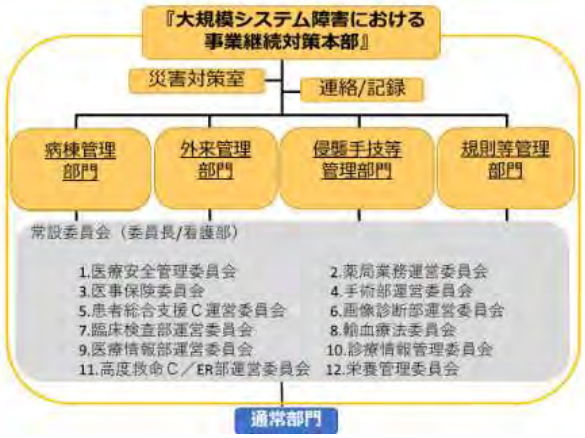
インシデント発生当日（2022/10/31）の状況

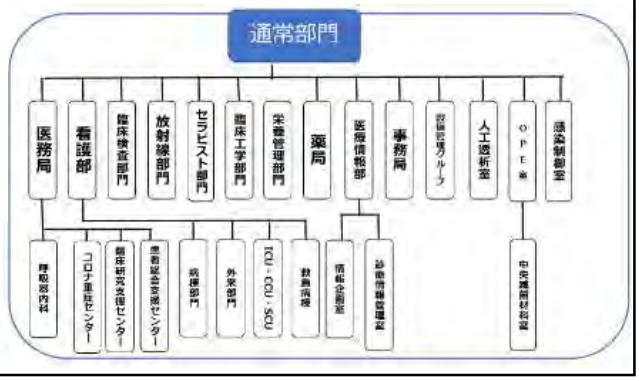
5時台	各現場で電子カルテの不良動作を確認するも、その後通常操作ができたため経過観察
6時台	医療職員や給食委託職員が電子カルテシステム等の障害発生を確認 給食事業者からもデータ送信ができないとの連絡あり
7時45分	システム運用管理委託職員がサーバの画面上にランサムウエアのメッセージを確認
8時15分	給食事業者からサーバがウイルスに感染した可能性との連絡あり
8時40分	電子カルテ等の基幹システムベンダーがネットワークを遮断
8時50分	病院幹部会議においてシステムの障害状況を確認 ⇒外来診療停止、救急受入停止、 ⇒12時に対策本部会議招集を決
9時30分～	関係各方面に連絡 ⇒府立病院機構本部、大阪府、大 ⇒内閣府サイバーセキュリティセン
11時40分	厚生労働省から初動対応支援チー
12時00分	第1回BCP対策本部会議開催 ⇒診療現場の状況把握、紙カルテ ⇒専門家チームの派遣受入を了承
16時00分	システム関係者、専門家チームによ
17時00分	職員向け説明会の開催、ホームペー
19時00分	システム関係者、専門家チーム、給 （※専門家チーム3名は翌日には来
20時00分	記者会見を開き、インシデントの状況と当面の診療体制について説明

10/31 早朝
ランサムウェアによるシステム障害発生
- **8:50：方針決定**：
  外来診療、予定手術、救急対応　すべて一時中止
- 関係各所への報告（厚労省、大阪府、府警他）
- **12:00：BCP対策本部会議**
- 紙カルテによる診療再開へ
- 原因究明と診療再開へ
- システム復旧会議（専門家）
- **17:00：職員向け説明会**
- **20:00：**メディア対応（記者会見）

大規模システム障害発生時の事業継続体制 ①

組織図





大規模システム障害発生時の事業継続体制 ②

BCP対策本部会議の開催状況

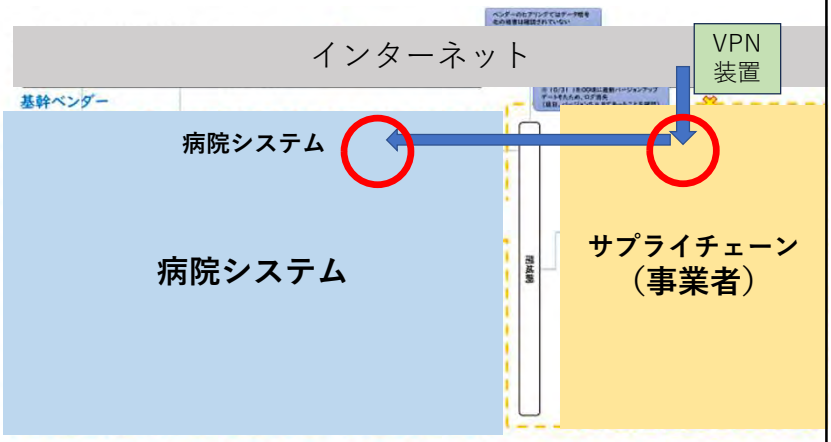
回数	開催日	主な決定事項等
1回目	10月31日	・災害時の紙カルテ運用の実施とともに、直近1週間の方針を決定 ⇒手術は緊急のみ　⇒外来は緊急のみ ⇒救急や時間外はやむを得ない理由がある場合以外は停止 ⇒新規入院は延期　⇒入院中の患者の診療は継続
2回目	11月1日	・外来開始方針、外来化学療法再開 ・診療記録文書統合管理システム（DACS）の活用を開始 （優先順位：①手術、②転院） ・各検査、処方、カルテなどの個人情報の取扱いを確認
3回目	11月2日	・11/4からの予定手術の一部再開を決定 ・紙カルテ運用における安全な診療継続を確認 ・図書室を閲覧スペースとしてDACS参照センター（10台）の設置を決定
4回目	11月4日	・院内での情報共有方法を確認 ・検査、手術など可能件数を確認
5回目	11月7日	・対策本部の組織や指示命令系統などを再構成 ・11/8からDACS参照センターの運用を開始
6回目	11月8日	・11/10から三次救急の一部受け入れ再開
7回目	11月9日	・11/10からバックアップデータを利用した参照系端末の運用開始（20台） ・DACS参照センターの端末の拡充を決定（最大20台）
8回目	11月10日	・11/14から内視鏡再開
9回目	11月11日	・11/11から術前麻酔外来を再開
10回目	11月14日	・12月第三週での基幹システム稼働を想定し、端末の順次配置方法を確認 ・11/17から救急外来（ER）を再開

病院が医療を継続できた要因：
1)事業継続対策本部が設置できる体制であったこと。
2)インシデントを認知して短時間で幹部を含めて招集できたこと。
3)紙カルテ運用に移行できる体制であったこと。
4)対策本部会議で決定した事項を速やかに職員に周知できる体制であったこと
（**インシデント調査報告書**より）

以後、週1～2回ペースで開催し、12/28の19回目会議開催にて終了
BCP対策本部会議での決定事項は、別システム掲示板や一斉メール配信で周知

病院情報システム概要とネットワーク

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）



9

大規模システム障害の概要と主なタイムライン

- ✓ 2022年10月31日（月）に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害発生
- ✓ 電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得ない状況
- ✓ 同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧
- ✓ 発生要因は、VPNネットワーク接続していた給食提供事業者のサーバーに攻撃者が侵入し、その巻き添えを受けたこと

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）
11.4	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

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

10

システム障害発生要因と対応策

◆ 大規模システム障害を生じさせた理由と要因、即時対応策

	理由	要因	即時対応策
1	サプライチェーン経由での不正侵入	病院側の外部接続管理方法の不備により不正アクセスを許してしまった	外部接続管理方法の強化
2	システム初期設定不備による不正アクセス助長①	アカウントロックの設定が無く、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	アカウントロック設定有効化
3	システム初期設定不備による不正アクセス助長②	共通パスワード使用により不正アクセスの横展開を容易に許してしまった	各サーバー、端末毎の16文字以上個別パスワード設定
4	全ユーザーが管理者権限所持	管理者権限によりウイルス対策をアンインストールでき、ランサムウェア（暗号化ツール）を容易に実行できた	一般ユーザーでは管理者権限を持たせない。 UACを有効化
5	一部サーバにウイルス対策未設定	ウイルス対策ツールによる負荷を避けるために基幹システムのサーバに対しウイルス対策を設定していなかった	全てのサーバにウイルス対策設定

今後の組織的セキュリティ強化計画

◆ 今回の反省点と今後の組織的取り組み

	反省点	内容	今後の取り組み
1	バックアップの不備	• バックアップが十分でなく、部門システムの一部について、データベースや設定ファイルを復旧できなかった。	バックアップ運用の見直し バックアップ管理台帳の作成
2	情報資産管理の不備	• HIS系ネットワークに接続されている医療機器を含めた情報機器が一元管理できておらず、調査に時間を要した。	IT資産管理システムの運用開始 HIS接続申請書の運用開始
3	ITガバナンスの不備	• 外部接続や資産管理など、組織的な情報管理ができていなかった。 • 組織的なセキュリティポリシーを策定できていなかった。	ITガバナンス体制の構築に向けた病院内の仮想組織を発足 情報セキュリティポリシーの策定
4	契約内容の不備	• 物品調達や保守委託などの契約仕様書内に、情報セキュリティに関する事項が明示されていなかった。 • 責任分界点が曖昧であった。特に脆弱性管理の役割分担が曖昧であった。 • 委託事業者に対するIT監査を含む監督権が明記されていなかった	特記仕様書で「セキュリティ取扱特記事項（役割分担、監査権を含む）」を追記
5	インシデント対応体制の不備	• サイバー攻撃を想定した対応手順や医療継続に係るBCPが未整備であった。	BCPの改定 サイバー攻撃対応手順の策定

復旧時のセキュリティ強化対策（windowsセキュリティポリシー対策）

項目	これまで	今後	備考・説明
パスワードポリシー（長さ）	3文字以上（実際にはサーバ12文字、ユーザ9文字で運用）	16文字以上(全ユーザ)	ユーザはICカード&PINコードでログインされる為、パスワード長による運用影響無し
パスワードポリシー(アカウントロック)	アカウントロックの設定無し	アカウントロックを設定(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)	試行期間内のログイン失敗回数によりログインを制限
パスワードポリシー(一意性)	サーバのパスワードがすべて同じユーザのパスワードがすべて同じ	サーバ毎、ユーザID毎に全て異なるパスワードを設定	
セキュリティパッチ	構築時点で評価されているものまでを適用	全てのサーバ、端末のセキュリティパッチを最新化(2022年11月時点のものを適用)	Windows Updateのセキュリティ関連のものを適用
アンチウィルス	電子カルテ基幹系サーバ4台については未導入/その他は導入	電子カルテ基幹系サーバ4台にも導入	
アプリ実行ユーザ	管理者権限で実行⇒強力な権限を保持	一般ユーザで実行⇒重要なシステム変更などができない適切な範囲の権限のみを保持	
UAC(サーバ)	無効	有効	UAC：管理者権限を要する重要な操作が意図せず自動実行されるのを防ぐ機能
UAC(クライアント)	無効	有効	
RDPポート	デフォルト(3389)⇒第三者に推察され易い	デフォルトから変更(新たな番号)⇒第三者に推察され難い	RDP：リモートで端末を操作する機能
Active Directory の強化設定	ベンダー設定	サーバー：CIS Benchmarkクライアント：IPA ガイドライン	CIS Benchmark

● 例えランサムウェアの侵入を許しても、横展開を許さない（被害拡大を防止する）施策の強化構築

UAC: User Account Control
RDP：Remote Desktop Protocol

今回のインシデントについて

- 医療事故が発生しなかった
- 外部への情報漏洩の可能性が極めて低い（顕著なデータ転送なし）
- DACS を含む画像系のシステムが無事であった（参照系構築）
- バックアップ：遠隔地（オフライン）があった
- 職員との情報共有
- 紙カルテの運用
- 厚労省、**初動対応支援チーム**（専門家チーム）の迅速な支援開始

データバックアップについて

- オンラインバックアップ＋オフライン（遠隔地）バックアップ
- バックアップされている情報の確認（契約書＋実態の確認）
- バックアップからの復旧の訓練
- バックアップによる迅速な参照環境の構築

紙カルテ・伝票の手書き運用について

- 運用のための訓練が不可欠：
  - 若い職員は紙カルテ使用の経験がない！
  - 書式（format）の事前準備（印刷？：短期・長期のシステム障害）
- 運用時の留意点：
  - **情報量、処理速度、便利さが大きく違う　⇒　遅くて不便**
  - **リスクマネジメントの観点　⇒　インシデントが増える**
- 紙カルテから電子カルテへの復旧時の注意：
  - 診療録はスキャンをして電子媒体として電子カルテに保存
    ⇒せめてテキスト入力ができていれば、との意見
  - 医事・会計データは復旧後にすべて手入力した

職員全体への連絡方法

- 病院に来なくても確認できるツールが必要
- 普段より使っているデバイスを利用する

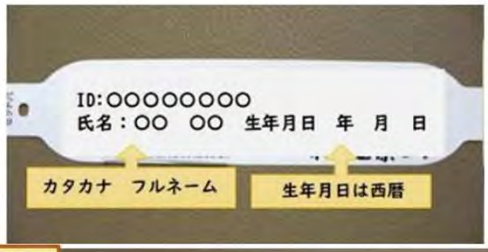
全員のメールアドレスやLINEアカウントが紐づいて連絡を取れるようになっていた

27

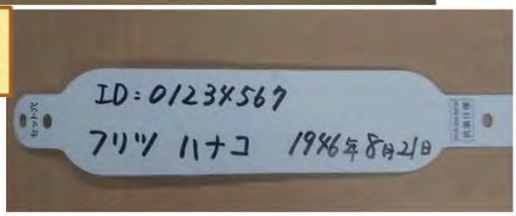
2. 患者確認方法：リストバンドの表示統一

リストバンド表示：
ID・患者カナ氏名・
バーコード・血液型・病院名

患者確認は、フルネームとバーコード認証



リストバンドの
付け替えを実施



患者確認は、
IDと**フルネーム**と**生年月日（西暦）**で行う

院内に周知徹底

安全に紙運用できる限界とは　検査の場合

モニタリング：現状分析　状況評価

システム停止後延べ検査件数推移（検体・微生物・輸血検査）

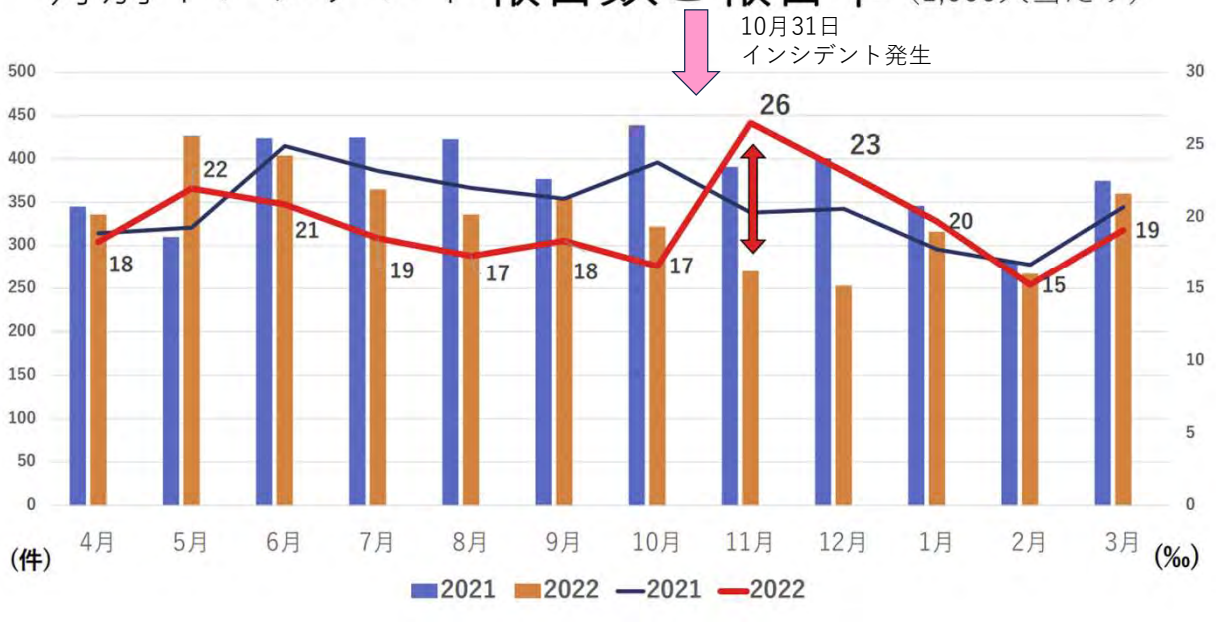
集計日：11/10

11月			1日	2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日	21日	22日	23日	24日	25日	26日	27日	28日	29日	30日
			（火）	（水）	（木）	（金）	（土）	（日）	（月）	（火）	（水）	（木）	（金）	（土）	（日）	（月）	（火）	（水）	（木）	（金）	（土）	（日）	（月）	（火）	（水）	（木）	（金）	（土）	（日）	（月）	（火）	（水）
検体	入院		81	113	48	163	34	27	168	82	96																					
	外来		67	111	－	139	－	－	173	129	175																					
	分野別	検血	125	171	58	291	46	31	318	149	199																					
		止血	51	60	13	77	17	10	78	52	56																					
		尿定性	43	71	7	92	4	7	98	49	88																					
		尿沈査	0	17	0	27	0	0	45	38	51																					
		生化学	83	168	47	240	34	27	288	175	223																					
		免疫	11	38	2	49	3	2	88	65	72																					
		その他*	0	0	0	5	0	0	7	5	19																					
微生物	微生物総計		158	36	0	65	11	11	76	34	26																					
	SARS-CoV-2-PCR総計		99	45	1	55	4	3	49	54	40																					
輸血	血液型		11	10	4	10	5	8	17	23	22																					
	輸血製剤依頼オーダー総数		17	4	9	11	13	7	16	31	15																					

外来検査が200件を
超えないようにしてほしい

14

月別インシデント報告数と報告率（1,000人当たり）



システム障害時の事業継続(BC)に必要な事

1. 会議体をつくる
2. ID番号を持っている患者の情報を得る
   ① 入院中患者
   ② かかりつけ患者
3. 安全に紙運用できる限界を知る
   ① 検査（採血、画像など）
   ② 治療（薬剤投与、手術、血管造影等）が行える
4. メンタルを正常に保つ
   ① 情報共有と発信ツールを持つ
   ② スピード感を無視する

システム障害のBCP

自然災害のBCPとは異なり、時間で復旧プロセスは決められない。

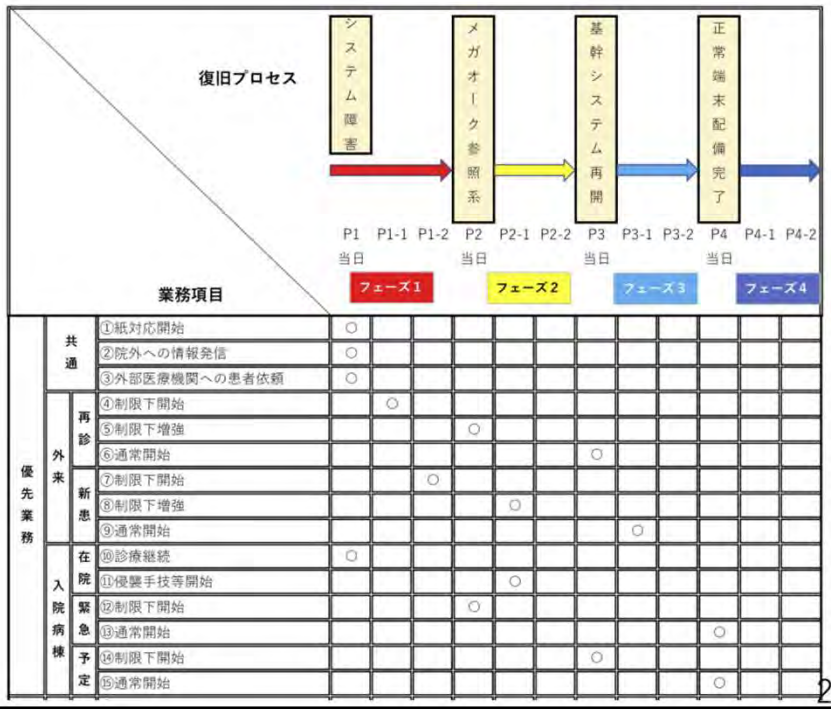
システム障害の復旧プロセスは、イベントです

フェーズ１
患者の過去がわからない

フェーズ２
患者の情報が手に入る

フェーズ３
最低限のオーダー（検査、画像、薬）ができるようになる

フェーズ4
すべて元に戻る



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	2024/3/15　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

一般災害における事業継続計画

一般災害BCP

General Disaster Business Continuity Planning

第7版

2023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

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

まとめ に代えて

- サイバー攻撃（ランサムウェア）は被害にあった病院を狙ったものではないが、どの病院も攻撃を免れることはできない
- 防御のためには、基本的な対策をしっかりとすることから始める（パスワード、パスワードロック、管理者権限、バックアップ）
- ITガバナンスとセキュリティーポリシーを確立し、IT資産の管理、機器の契約の見直しを行う
- サイバー攻撃によるシステムダウン時のためのBCPの策定
- システム障害時には、まず閲覧機能の回復に努める（バックアップ）
- 紙カルテの運用の訓練を行うとともにその限界、リスクを知る