令和7年度医療情報セキュリティ研修
及び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・調査等事業

IT-BCP組織体制コース

IT-BCP発動時の組織体制について

2025年10月1日

一般社団法人ソフトウェア協会

アジェンダ

- **当院の事例とIT-BCP**
  地方独立行政法人 岡山県精神科医療センター　山田 了士
- **「個人情報の保護に関する法律」に関して**
  ～個人情報保護委員会対応等～
  地方独立行政法人 岡山県精神科医療センター　松本 安治
- **IT-BCPの発動と組織体制**
  一般社団法人ソフトウェア協会　加藤 智巳

2025.10.1

IT-BCP 組織体制コース
当院の事例とIT-BCP

地方独立行政法人 岡山県精神科医療センター
山田　了士
松本　安治

Contents

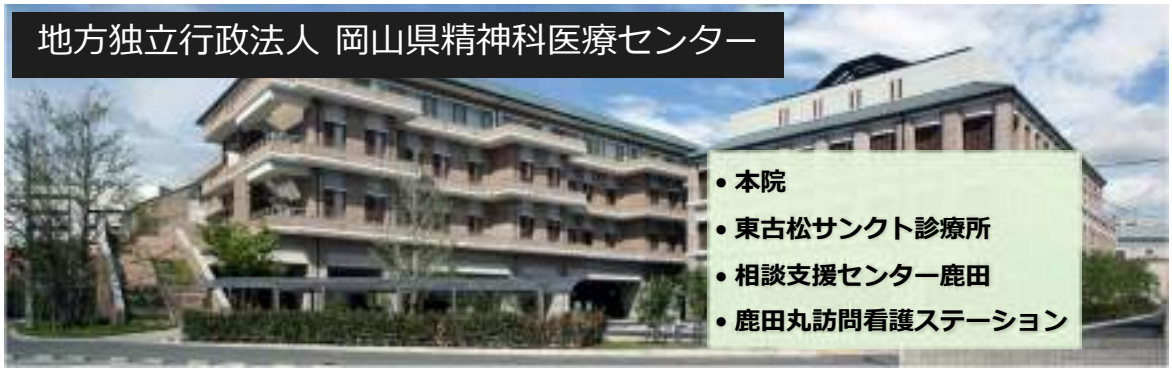
1. 病院の概要
2. 事案発生と初期対応
3. 以後の経過とカルテの復旧
4. 診療、経営への影響
5. 再発予防の対策
6. 情報漏えいへの対応

本院の概要

- 病床数 252
  救急急性期x 2、児童、依存症、医療観察法、地域包括ケア病棟など
- 病床利用率 94%
- 平均在院日数（医観法除く） 46.8 日　（cf 全国精神科病院 約270日）

- 1日あたり平均外来数　約250名 初診約12名
- 休日夜間対応件数　1,384人　そのうち入院 523人 （R4、県内の8割)

- 災害拠点精神科病院、日本DPAT登録隊員5名
- 東日本大震災、熊本地震、西日本豪雨、能登半島地震で活動



本院の概要

- 職員数　約370名
- 現行電子カルテ　2012年～　端末約250台
  本院と診療所で使用

- SEに該当する職員2名（それぞれ経営課長、医師支援班長を兼任）
  1人は独立系Sier企業出身、しかしセキュリティ専門家ではない

Contents

1. 病院の概要
2. 事案発生と初期対応（最初の２週間）
3. 以後の経過とカルテの復旧
4. 診療、経営への影響
5. 再発予防の対策
6. 情報漏えいへの対応

2024年5月19日（日）16時頃

岡山県精神科医療センター
ランサムウェア事案発生

初動　Day0 - 2

Day0　5/19（日）

16:00　**電子カルテシステムが閲覧不能（本院、サンクト診療所）**
直ちにベンダー（A社）に連絡し招集、データセンターで夜通しの対応

Day1　5/20（月）

6:30　暗号化されたファイルを発見し、サイバー攻撃の覚知。

7:00　幹部集結、**災害対策本部設置**

紙カルテで 診療を止めない！

7:40　県警、岡山県、厚生労働省に連絡

9:30　県警サイバー犯罪対策課、県職員が到着

10:00　**厚労省から初動対策チーム**の派遣が打診され依頼

12:40　**ランサムノートをプリンタサーバー内**に発見

交渉には応じない！

16:00　プレスリリース、病院HP告知

17:00　**厚労省初動対策チーム到着**　警察、県、ベンダーとともに詳細調査、対策会議

Day2　5/21（火）

ランサムウェアを発見、個人情報保護委員会へ速報提出、保険会社に連絡

ランサムノート（脅迫状）

様々な情報を窃取し、暗号化した。
最善の方法は我々にコンタクトすることである。
ファイルを編集したり、シャットダウンすると復活が困難になる。
連絡がない場合、数日内にデータは公開される。
（OnionサイトのURLが記述）

初動　Day0 - 2

Day0　5/19（日）

16:00　**電子カルテシステムが閲覧不能（本院、サンクト診療所）**
直ちにベンダー（A社）に連絡し招集、データセンターで夜通しの対応

Day1　5/20（月）

6:30　暗号化されたファイルを発見し、サイバー攻撃の覚知。

7:00　幹部集結、**災害対策本部設置** → 紙カルテで 診療を止めない！

7:40　県警、岡山県、厚生労働省に連絡

9:30　県警サイバー犯罪対策課、県職員が到着

10:00　**厚労省から初動対策チーム**の派遣が打診され依頼

12:40　**ランサムノートをプリンタサーバー内**に発見 → 交渉には応じない！

16:00　プレスリリース、病院HP告知

17:00　**厚労省初動対策チーム到着**　警察、県、ベンダーとともに詳細調査、対策会議

Day2　5/21（火）

ランサムウェアを発見、個人情報保護委員会へ速報提出、保険会社に連絡

焼け跡に残っていた家宝

- カルテのオンラインバックアップも全て暗号化
- 契約済みであったオフラインバックアップも正しく取得されていなかった

　➡　閉院の憂き目も…

- DWH（Data Warehouse）内のカルテデータが暗号化を免れていた

　➡　BCPカルテ（参照用オフライン端末）の作成
　　本カルテの復旧　　に繋げられた

復旧への経過 -1-

Day	月.日	経　緯	診　療
0	5.19	Day 0	
1	5.20	対策本部設置	紙カルテで継続（マニュアル作成）
		16時：ランサムウェアの攻撃である可能性をHPで公表、プレスリリース **外部問合せ対応係を固定**	**BCPカルテ**（参照のみのオフライン端末） DWHのデータから 5台作成　　→ 後に増強
2	5.21	15時半：ランサムウェアによる攻撃が特定されたことをHPで公表、プレスリリース 個人情報保護委員会に報告（速報）	
3	5.22	参照系中古サーバーを手配 端末総入れ替えと決定	
13	6.1	**新規電子カルテ50台**導入（完全閉域）	電子カルテ50台と紙カルテを併用 会計窓口再開

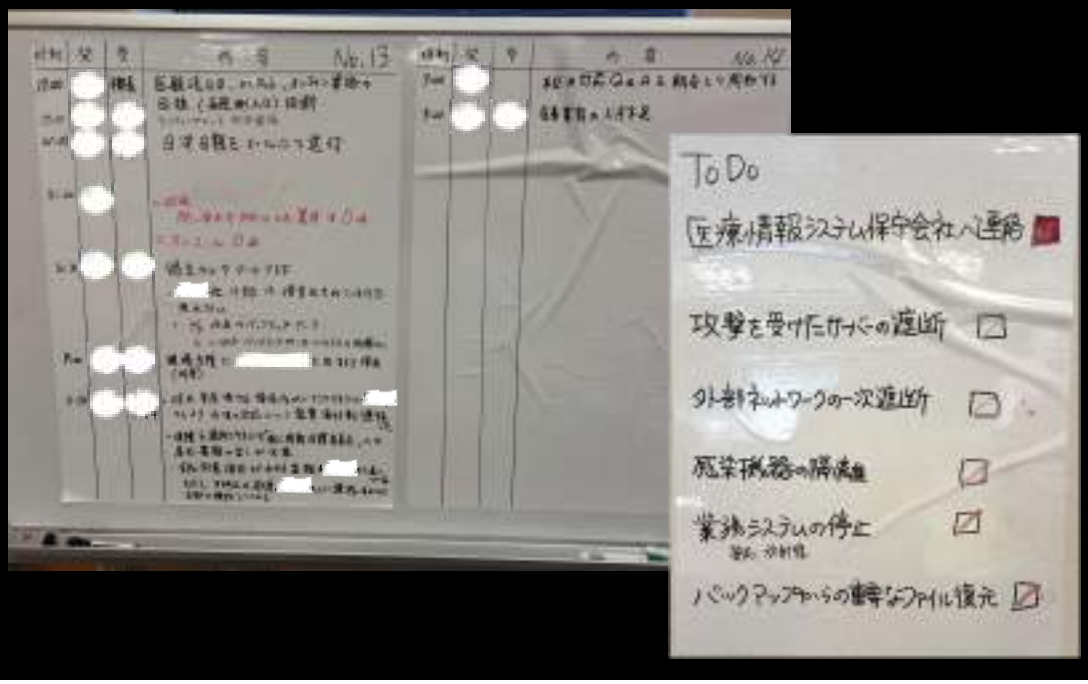
対策本部　情報統括、クロノロ、意思決定

●医療継続会議（各チームの報告）
病院主要メンバー数十名
1日3回実施　のち7月19日まで1日2回

●システム復旧の進捗管理
病院幹部、システム担当者とA社との連絡会議
1日2回開催
7月20日 - 11月末　1日1回
12月以降　週1回、現在も継続中

対策本部のクロノロ

対策本部のクロノロ



紙カルテ

マニュアル (Day5)

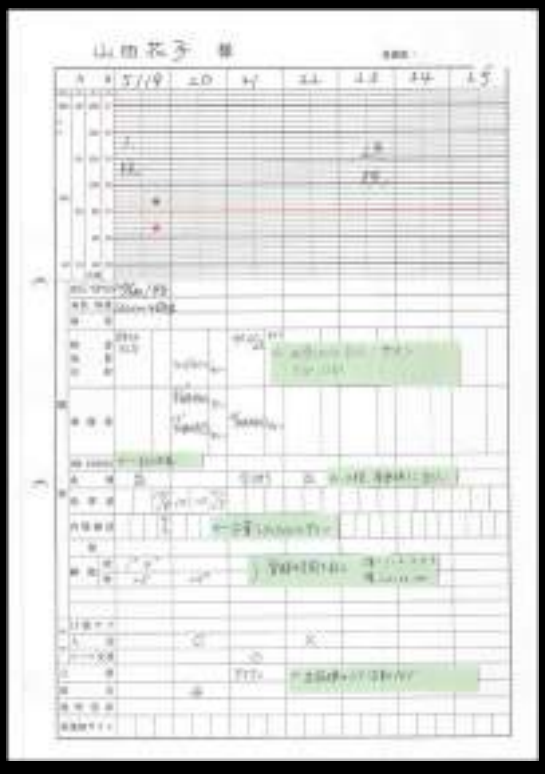
見本(Day1-2)

各用紙を１セットにして
リングファイルに
綴じ方の順番も統一

診療録（紙カルテ）綴じ方順番

1）診療録（緑の枠、字）（２枚）
2）保険証のコピー
3）指示簿
4）各種　指示箋
・一般撮影・CT・MRI・検査指示箋（兼所見用紙）
・栄養指導指示箋
・心理検査オーダー票
・リハビリテーション処方箋
・精神科訪問看護指示箋
5）処置指示録
6）外来診療録２号紙　（多職種の記録）
以下は２号紙に時系列で差し込む
・クロザリル副作用観察項目
・外来処方箋
7）診療情報提供書・各種診断書
8）入院時ウィザード
9）各入院届
10）入院診療計画書
11）入院時連携シート（在宅支援→入院様）
12）PSW が扱う精神保健福祉法上の書類
生活相談員説明文
退院支援委員会関連書式
13）精神科リスクアセスメントシート（自殺・暴力）
14）転棟・転落アセスメントシート
15）褥瘡対策に関する診療計画書
16）NST リスクアセスメントシート（SGA）
17）栄養管理計画書
18）入院患者基本情報
19）MSE
20）セルフケア６項目アセスメントシート
21）問題リスト
22）看護計画
23）入院以降の診療録２号紙
以下は２号紙に時系列で差し込む
・心理検査所見
・診療録（リハビリテーション）
・退院前訪問記録
24）外出・外泊申請書のコピー・外泊アンケート
25）精神科退院療養計画書
26）退院時連携シート（入院様→在宅支援）
27）退院ウィザード
28）医師退院時要約
29）チームカンファレンス記録
30）経過表
31）隔離観察表
32）隔離身体拘束観察表
33）ECT 関連様式
・ECT についての説明および同意文書
・承諾書
・ECT 準備パス
・ECT 実施パス
34）その他の同意書
35）病室に施錠をうけ療養することが必要である旨の説明
36）検査報告書
37）心電図（ビニールファイルに入れる）
38）入院注射処方箋・処方箋（定期・臨時）
39）入退院時の ADL スコア

記入サンプル



留意事項

紙カルテ　留意事項

患者に関する必要な患者情報が共有できる【みんなのカルテ】

- 必要な情報・記載とは

○ 患者の安全・安心をするための観察や実施記録、検査結果等
○ 退院後の生活を見据えた調整や自立に関する情報や実施記録
○ 各職種が行った診療行為および実施事項
○ 診療報酬・レセプトに対応できる情報や記録
○ 電子カルテ移行後に移行する情報や記録

- 記載の記載：医師は青インク、看護師・コメディカルは黒インクを使用

- 医師－看護師間のカルテ情報に関する伝達の工夫　（依頼・指示等）

○ 依頼や指示に関する事項がある場合、カルテに目印として色クリップを使用する。

青クリップ：医師に依頼や伝達事項がある場合

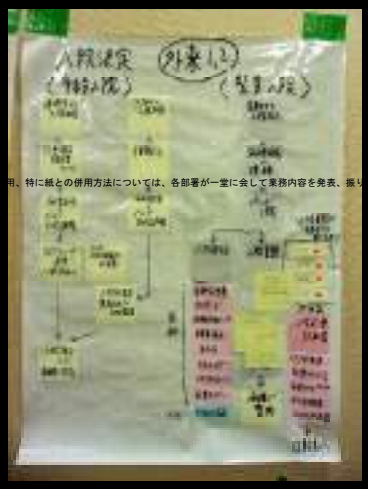
ピンククリップ：看護師に指示や伝達事項がある場合

○ 原則、指示・指示受け・等は口頭での伝達を行う。
（クリップは目印にすぎないため、お互いのコミュニケーションである前提で）

※ 必要事項があれば、随時更新

● 暫定電子カルテと紙カルテの併用運用についての打ち合わせ（5月30日）

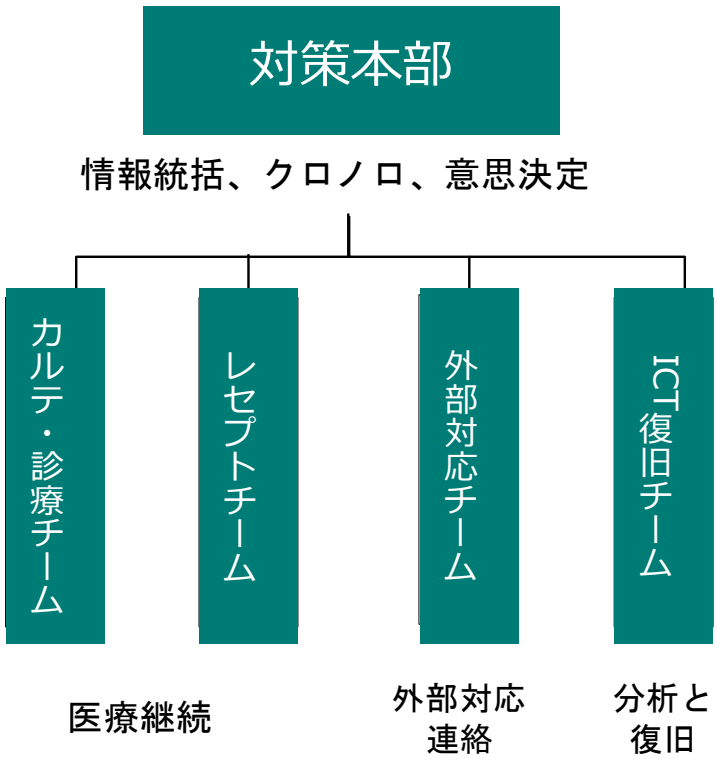
•一堂に会して各部署が診療プロセスを書き出し、
紙と電子の振り分けをして、手順書にまとめた



（例）外来（書類的手続きが多い）

復旧チームの構成

- Day1からのプロセスに応じて、自然発生的にチームを編成
- 各チームは医療継続会議で1日３回報告し、方針決定
- 職員の理解を進めることに重点
- 外部対応チームは、情報漏えい発覚後、人員を大幅に増強
- このまま当院IT-BCP手順書に掲載



Contents

1. 病院の概要
2. 事案発生と初期対応
3. 以後の経過とカルテの復旧
4. 診療、経営への影響
5. 再発予防の対策
6. 情報漏えいへの対応

復旧への経過 -2-

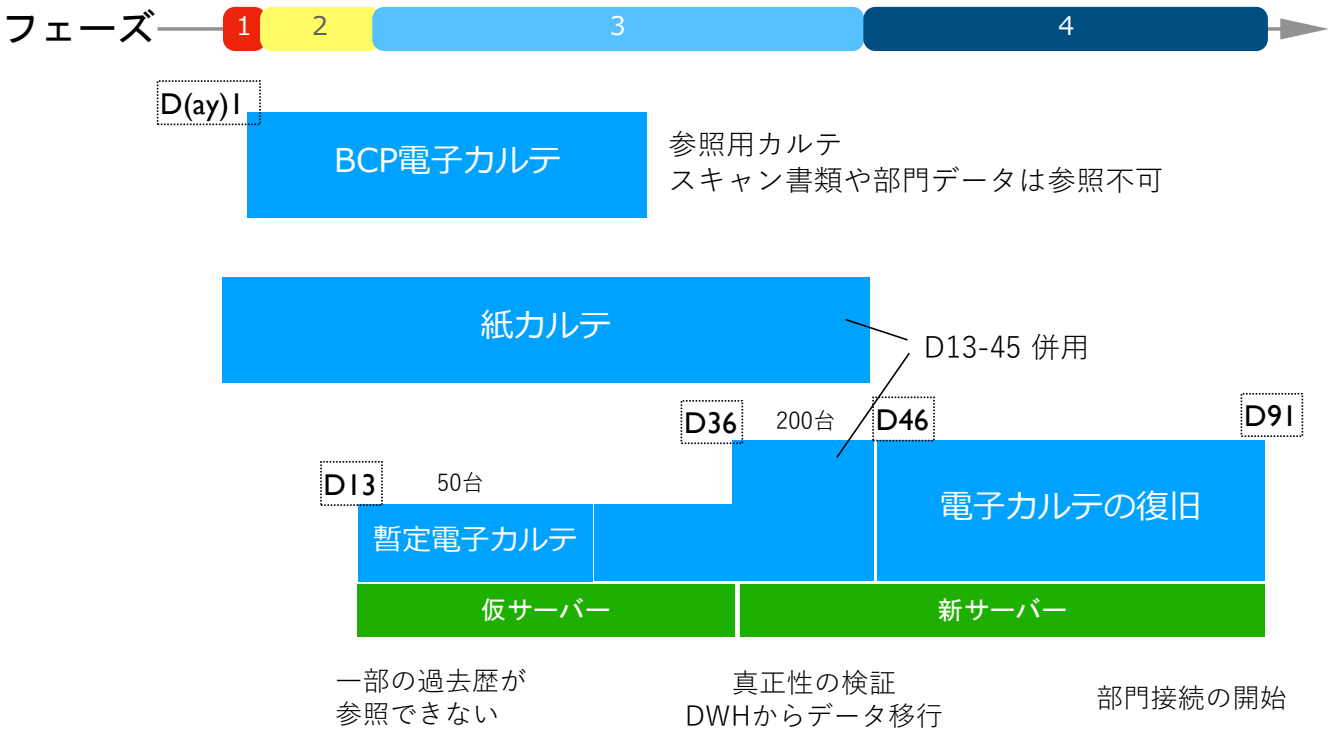
Day	月.日	経　緯	診　療
19	6.7	**県警から連絡　病院長が患者情報の流出を確認　（カルテそのものではなく、共有フォルダ書類）**	
23	6.11	**記者会見**　情報流出について公表、HPでも公表 院内患者相談窓口設置	
26	6.14	コールセンター運営開始	
36	6.24	患者さんへのお知らせを発送	
		新サーバーの導入 **新規電子カルテ150台**追加（完全閉域） 医療機器ベンダーへの聞き取り調査を開始	電子カルテ200台で運用開始 （一部、紙運用）
46	7.4	DWH からのデータ移行、検証が完了	電子カルテの復旧（紙停止）
91	8.17	サーバーストレージの入れ替え	電子カルテの完全復旧

大規模システム障害のBCP（IT-BCP）

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

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、医業全体をコントロールするなかでのイベント

（※）あらかじめ災害用のBCP電子カルテ端末を作っていたこと、DWH（dataware house）が被害を免れたこと、これらにより、システム障害発生直前までの診療録、処方箋、注射箋、血液検査などの参照・印刷が可能となった。



復旧への経過 -3-　**部門システムの復旧戦略**　（画像、薬剤、検査、給食 etc）

Day 36（6/24）

部門システム接続準備開始（ヒアリング）

15部門（13社）にCISベンチマーク準拠設定を要求

Day 45（7/3）

1周目のヒアリング終了セキュリティ要件の詳細確認完了

Day 67（7/25）

検査、栄養システムから再連結開始

CIS ベンチマーク：サイバーセキュリティ防御を実装・管理するための世界的コンセンサス主導のベストプラクティス集。多くはWindowsの設定変更で対応可能。

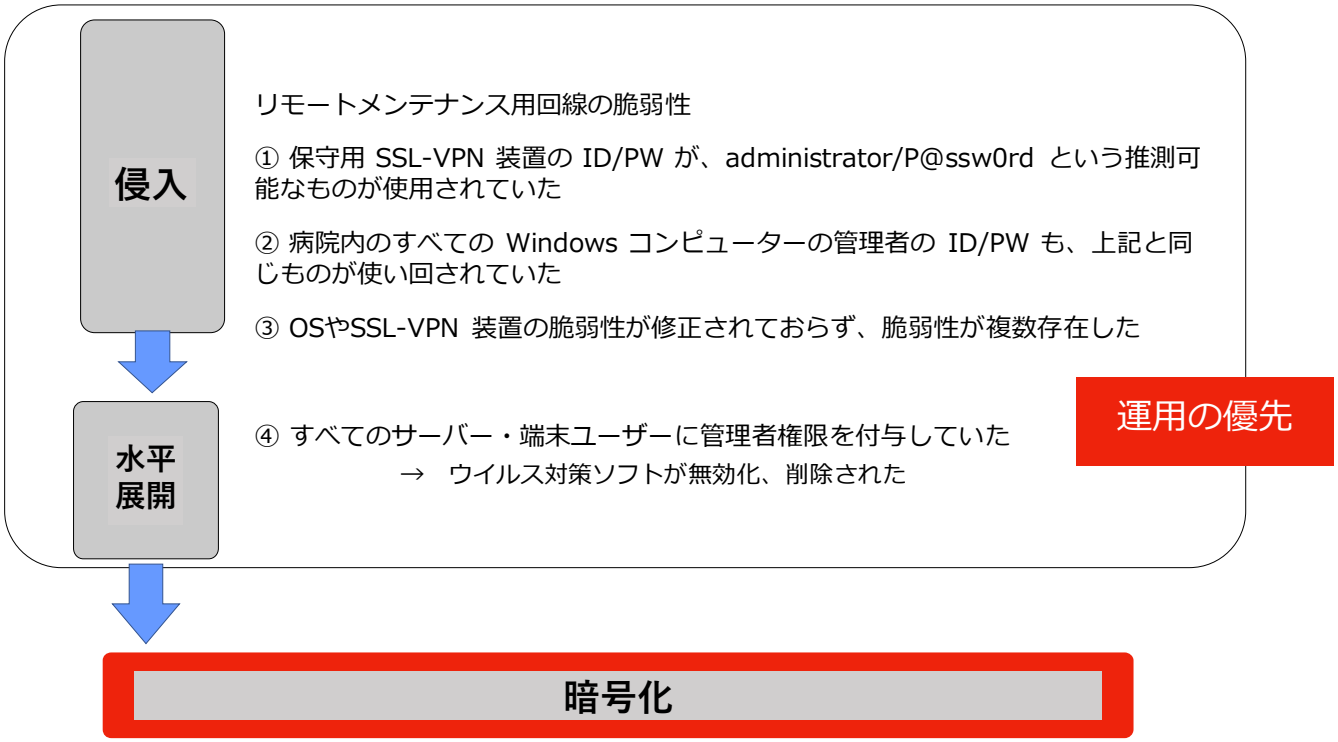
- 多くの部門システムでサポート切れOSやブラウザの使用、接続方法の問題
- **復旧には妥協しない**方針で対応

2025.2.13　有識者委員会による**ランサムウェア事案調査報告書**公表　**記者会見**


地方独立行政法人　岡山県精神科医療センター　ランサムウェア事案調査報告書について

PDFはこちら→ランサムウェア事案調査報告書

当院システムへの脆弱性と侵入機序



甘かった我々の備え

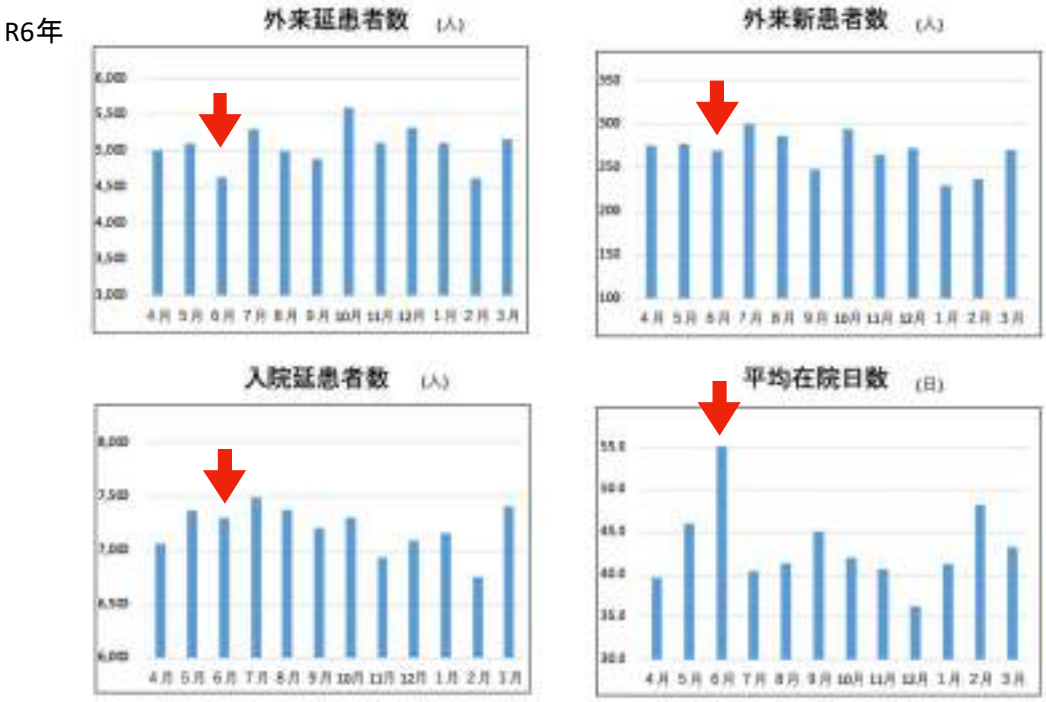
- ベンダーへの丸投げ体質
  - ベンダーはセキュリティの専門家ではない
- 電子カルテ閉域網神話
- 過去の事例に学べていなかった
  - 運用を優先し、脆弱性を軽視　など
- オフライン・バックアップが確認できていなかった
- 正常化バイアスが働き、事前に察知できなかった

Contents

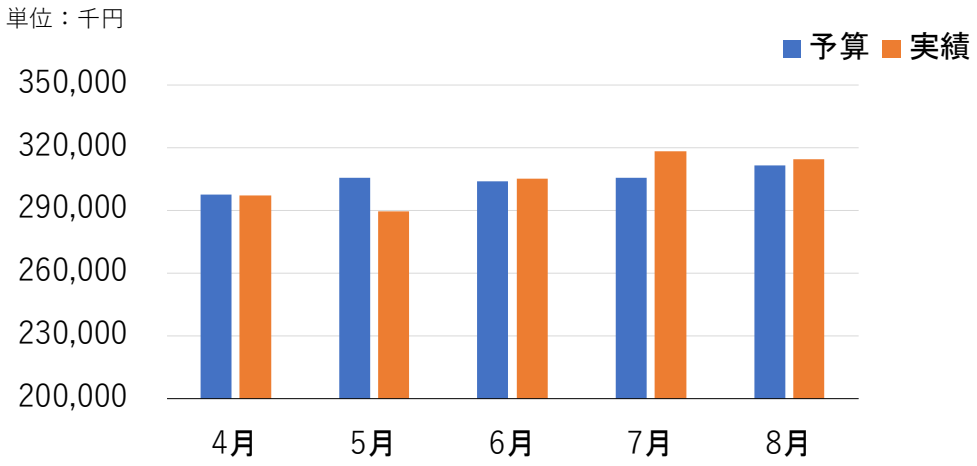
1. 病院の概要
2. 事案発生と初期対応
3. 以後の経過とカルテの復旧
4. 診療、経営への影響
5. 再発予防の対策
6. 情報漏えいへの対応

患者動向への影響は部分的であった

R6年



売上の月次推移（予算比較）



・他の事例よりは遺失利益が少なかった

復旧費用

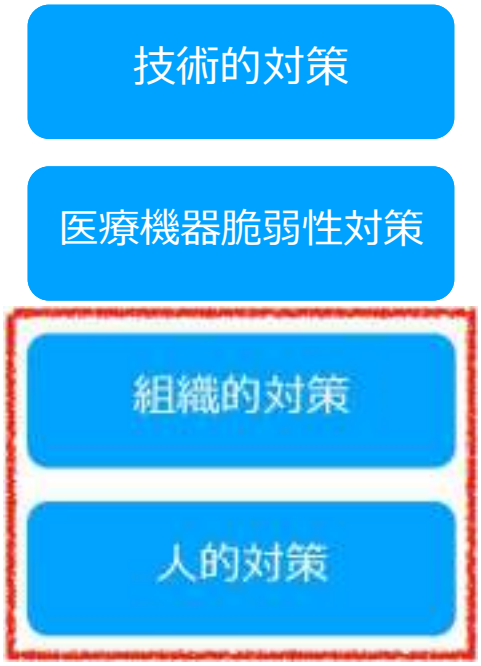
3,200万	3,000万	200台
対応費用	**サイバー保険**	**端末更新**
復旧対策・調査費用	復旧費用 （更新は対象外）	令和7年予定の 更新を前倒し

他の事例と比較して遺失利益は比較的少なく抑えることができた。事前のサイバー保険加入と迅速な対応により、経済的影響を最小限に留められた。

Contents

1. 病院の概要
2. 事案発生と初期対応
3. 以後の経過とカルテの復旧
4. 診療、経営への影響
5. 再発予防の対策
6. 情報漏えいへの対応

対策の4つの領域　調査報告書より



組織的対策

岡山県精神科医療センター　ランサムウェア事案調査報告書より

課題・脆弱	状況	実施策
HIS 系での USB メモリの厳格運用	実施済	ウイルス対策ソフト内蔵型 USB メモリのみ利用を許可。HIS 系へのファイルの持ち込み、持ち出しは、すべて IT 担当者が複数のウイルス対策ソフトでスキャンを確認する。
組織的な IT ガバナンスの欠如 情報セキュリティ規程の見直し	整備中	医療情報システム安全管理委員会を設置し、規程の見直しを計画。 ISO27002：2022 5.1~5.8、5.14~5.18 を採用。

2025年5月19日　第１回委員会開催
　議題：情報資産管理の棚卸

目的は、ITガバナンスの醸成と
「情報セキュリティ規程　第1版」作成

組織的対策

岡山県精神科医療センター　ランサムウェア事案調査報告書より

課題・脆弱	状況	実施策
システム管理台帳の不在	実施中	システム管理台帳（機器名、IP アドレス、接続先制限、VLAN、脆弱性情報入手先、脆弱性対策適用状況、サポート状況及びサポート切れ等）の整備。ISO27002：2022 5.9~5.11 を採用。
データー分類、ラベル付け基準の策定とアクセス制御等	策定中	データー分類、ラベル付けによるデーターの暗号化、保存、廃棄手順の策定。ISO27002：2022 5.12~5.13、5.14~5.18 を採用。
部門システムベンダー、医療機器ベンダーへのセキュリティ対策ヒヤリングの実施と是正	一部、実施済	すべての部門システムベンダー、医療機器ベンダーへのセキュリティ体制、脆弱性管理に関するヒヤリングを実施、脆弱性管理に対する管理強化を要請済み（一部、ベンダー未対応）。3 省 2 ガイドライン及び ISO27002：2022 5.19~5.23 を採用。
ベンダーとの契約の見直し	一部、実施済	仕様書のセキュリティ仕様の厳格化と、厚労省医療情報システムの契約における当事者間の役割分担等に関する確認表、3 省 2 ガイドライン遵守の要求。検収時の、設計書・手順書・設定報告書の厳格チェック、受入試験での実施確認。ISO27002:2022 5.31~5.32、5.37 を採用。
IT-BCP の策定	策定中	大阪急性期・総合医療センターの IT-BCP をベースに病院 BCP との整合性を図り策定を実施する。ISO27002:2022 5.24~5.30 を採用。

手順書（β版）完成

人的対策

岡山県精神科医療センター　ランサムウェア事案調査報告書より

課題・脆弱	状況	実施策
定期的な脅威情報、攻撃手法の教育が実施されていない	実施予定	半期に一度をめどに、最新のフィッシング、ランサムウェア攻撃事例を共有し、異常時のLAN抜線、無線LAN停止や保全、平時のウイルス対策ソフトの最新化やスキャンの実施手順を教育する。
ランサムウェア攻撃等初動対応教育が実施されていない	実施予定	年１回をめどに、ITスタッフ、病院幹部に対して、ランサムウェア攻撃、ウイルス感染における初動対応、IT-BCP発動に関するシミュレーションやトレーニングする。
システム脆弱性情報及び対策案が共有されていない	整備中	ITスタッフ、関連ベンダーにシステム脆弱性情報の共有を実施する。

サイバー攻撃初動対応のトレーニング実施（2025年2月）
今後も年１回は実施予定

各病棟の災害時備品保管場所に
紙カルテ手順書、様式、病床数分のカルテセットを配置

eラーニングで実施

メールで脆弱性情報の共有

自然災害と比べて

- 組織的対応の基本原則は共通
  - クロノロは重要、今どうなっているかの共有
- IT災害は犯罪被害であり、
  かつ情報漏えいがあると二次加害者になりうる
- 受傷者やライフライン障害はなく、サプライもあって、外は平常事態を誤解されやすい
- 孤独感
  - 職員の士気に影響　← リーダーシップ、対話、情報共有
- 外部対応が大変
  - 患者・利用者の不安、関係機関、メディア、ネット
- 専門家、業者の協力が必須（普通の医療機関では無理）

ここまでのまとめ

- 優れた専門家の強力な支援と、職員の高い士気のおかげで診療行動を1日も止めなかった。精神科ゆえのメリットもあった。
- 復旧以上のアップグレード。
- 情報システム安全管理委員会、紙カルテマニュアル、IT-BCP策定と初動対応研修、サプライチェーンの検証など、備えの充実。
- サイバー保険は財政上有用であった。
- まだやることは沢山ある。
- システム全体の防御が非常に甘かったこと、また平時、病院は丸投げをしていたことから攻撃を許した。
- 要配慮個人情報の漏えいが起きてしまった。

Contents

「個人情報の保護に関する法律」に関して

個人情報保護委員会対応等

法第26条第1項の対応について

日付	内容	根拠法令等
R6年5月20日	ランサムウエア事案発生	
5月22日 （発生3日目）	漏洩等の報告（第１報）新規・速報 毀損のおそれ、滅失のおそれ 氏名、生年月日、性別、住所、電話番号 人数不明	法第26条第1項 第三者による当該個人データーの取得の経緯を報告
（6月7日	職員作成の共有フォルダーの流出確認）	
（6年11日	上記内容を記者会見で公表	規則第10条）
7月17日 （発生59日目）	漏洩等の報告（確報） 5.22報告に加えて 漏洩対象人数40,000人、病名、入院期間 情報流出対象への対応を詳細に記載 フォレンジック調査未完	
（9月27日	フォレンジック調査報告書報告種入手）	
10月3日	フォレンジック調査報告書を委員会へ提出	規則第8条
	メールでの質問、回答　　10.3～最終7.1.16	
令和7年2月7日	委員会から文書による指導	法第147条

委員会：個人情報保護委員会
法　：個人情報の保護に関する法律
規則　：個人情報の保護に関する法律施行規則

本人への対応実施状況（規則第8条6項）

5/20～6/10　対策本部で相談受電

6/7　院内共有フォルダーの流出を確認
　　ケース会議資料、所轄庁報告データ等
　　患者氏名・病名・年齢・住居市町村名

6/11　要配慮個人情報流出プレスリリース
　→　即日、病院内相談窓口設置
　　役職者が主に対応（受電実績1カ月：142件）

6/14　コールセンター設置（外部委託）

6/20～　本人への説明文書の発送
　　精神科病院特有の理由により対象者の約10%・4,842人に対し当事案の説明、謝罪文を郵送。

費用（6/14～7/13）
・コールセンター委託費　4,026千円
・文書発送関係費　763千円
} サイバー保険で補填

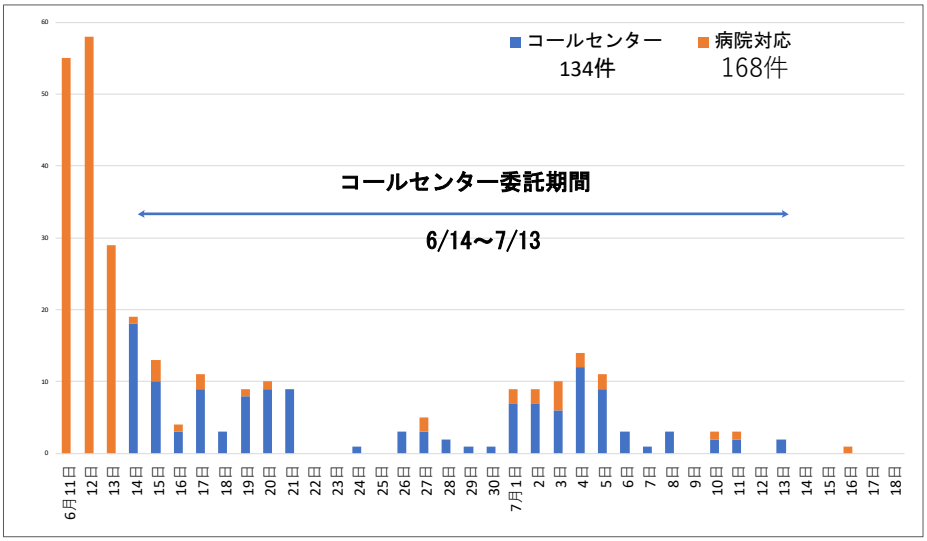
6/11～6/13　病院内相談窓口

受付時間
8:30～17:00
専用8回線

6/14　コールセンター設置
【委託内容：３回線　1カ月　1,330件に対応】
実際は、6/14～7/13受電実績：132件

◎コールセンター業者コメント
3日間でピークは過ぎる
依頼者の多くは２週間設置
電話対応は対象者の最大５%

6/11～7/18の院内相談窓口・コールセンター対応状況（詳細）



6/11記者会見

・6/7　県警から院内フォルダーの流出情報入手
　　院内相談窓口設置準備
　　院外コールセンター設置準備

・6/11　県庁内記者クラブで漏洩情報を発表
　　院内相談窓口開設

・6/14　院外コールセンター開設

・7/13　院外コールセンター閉鎖

・7/18　個人情報保護委員会への確報提出

　　院内相談窓口は現在も継続中
　　対応者は、幹部職員1名
　　その後1年間で電話4件対応、対面2件

10月3日以降の個人情報委員会対応について

◎主なやりとり：個人が不利益を被る内容。個人情報取扱事業者の責任。

規則8条	条文	内容
第4項	原因	システム説明、管理責任、具体的な管理方法　⇒管理責任
第5項	二次被害又はそのおそれの有無及びその内容	電子カルテが流出していない理由 フォレンジック調査書の説明 外部からの具体的なアクセス数、時間 システムの詳細な説明
第6項	本人への対応の実施状況	記者会見の内容 文書発送数の説明（全体の10%の理由、精神科特有の説明）
第8項	再発防止のための措置	具体策 具体策の内容説明 その実効性 いつ、誰が、どのように

総括：委員会への説明は専門的な知識を有する者でなければできない。

感想：委員会との対応により個人情報保護に必要な対策が明確になった。
「 病院事業者は個人情報管理に対する意識が高い」という自負だけで実効性がない。

まとめ・施行規則に対応した報告書の構成

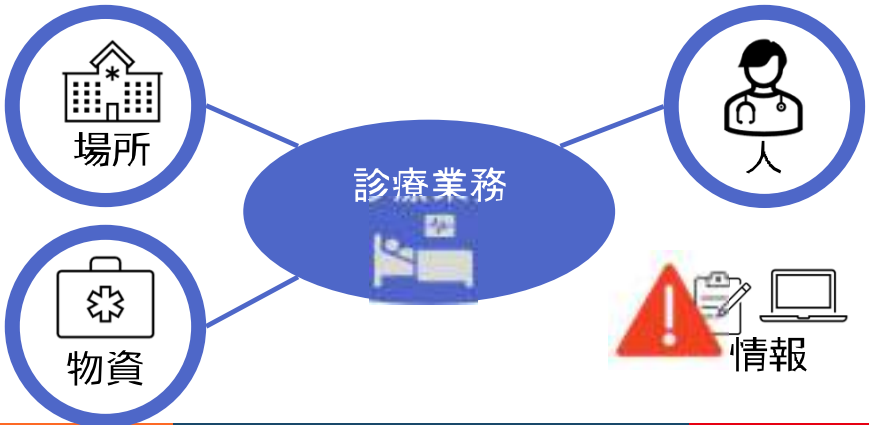
個人情報の保護に関する法律施行規則 （個人情報保護委員会への報告） 第８条	当センター　ランサムウエア事案報告書 ５ 概要編（P12～P29）
1. 概要	P12　5.1 インシデント概要 P17　5.6 事案の時系列
2. 漏えい等が発生し、又は発生したおそれがある個人データ	P14　5.3 情報漏洩 P15　5.4 仮想基盤の破壊及び共有ストレージ喪失
3. 漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数	P14　5.3 情報漏洩
4. 原因	P15　5.5 原因
5. 二次被害又はそのおそれの有無及びその内容	P14　5.3 情報漏洩
6. 本人への対応の実施状況	P14　5.3 情報漏洩（概要を記載） （P55　11 資料）
7. 公表の実施状況	P14　5.3 情報漏洩（概要を記載） （P55　11 資料）
8. 再発防止のための措置	P20　5.8 復旧方針と再発防止策
9. その他参考となる事項	ランサムウエア事案調査報告書 フォレンジック調査報告書

IT-BCPの発動と組織体制

一般社団法人ソフトウェア協会　加藤 智巳

診療継続の視点

- BCPの目的は「**診療を止めないこと**」
- インシデント初動の次に求められるのは、**現場で診療を継続するための条件**
- **人・物・場所があっても「情報」が止まれば医療は止まる**
- だからこそ、**医療継続の要件を明確にし、部門ごとに準備しておくことが必要**

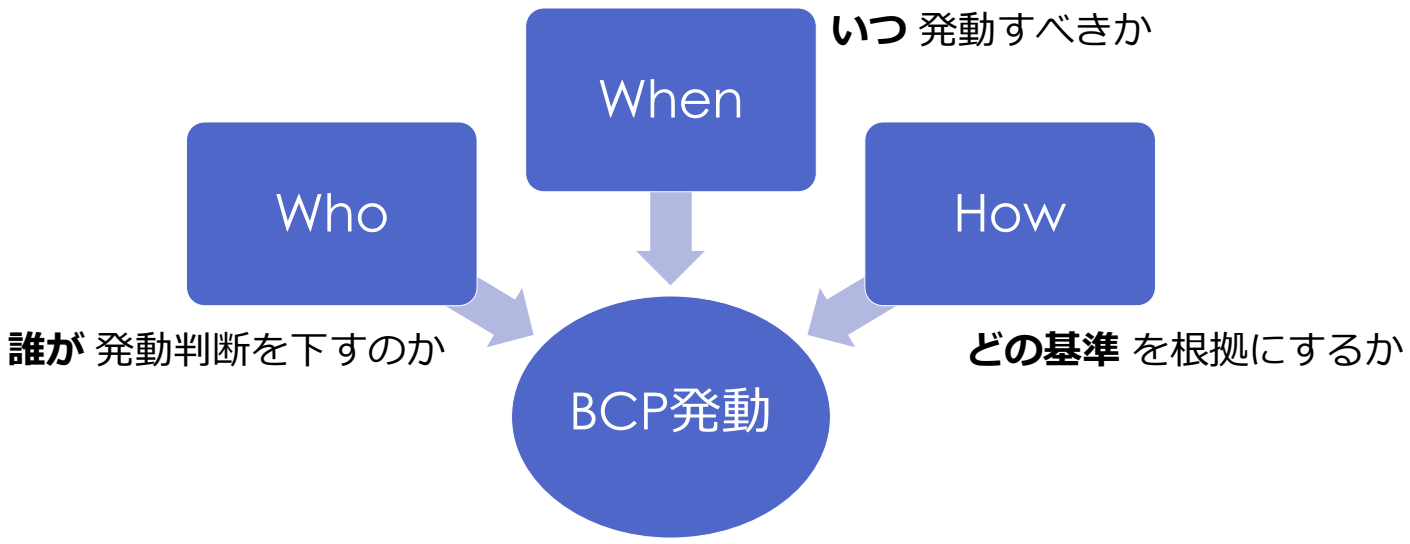


しかし、IT-BCP発動の判断は難しい

- 判断が遅れる → 被害拡大・診療停止の長期化
- 判断が早すぎる → 混乱・不要なコスト発生
- **BCP発動＝大規模な組織行動** → 根拠が必要

時間との勝負。迷っている間に被害は広がる

しかし、IT-BCP発動の判断は難しい



既存の判断材料（初動で得られる情報）

初報

- 職員からの通報（「カルテが遅い」「オーダーできない」など）
- システムからのアラート通知（監視サーバ、ベンダー通知など）

一時対応

- **機器管理台帳・システム構成図・ネットワーク構成図**
- IT部門内のヘルプデスク／担当者のヒアリング確認（局所的か、システム全体か）
- 実機環境の切り分け確認（セキュリティリスクの可能性含めて確認）

エスカレーション

- **医療情報システム安全管理責任者へ報告**
- 重大障害の可能性があれば **執行部（院長・副院長など）への連絡**
- 責任者と連絡が取れない時の副責任者

今後準備しておくべき判断材料

発動判断フロー

- 誰が → 誰に → どのタイミングで報告・判断するか

業務影響度マトリクス

- システム停止 × 業務影響の関係図
- 「どの領域でBCP発動が必要になるか」を明確に可視化
  - 例：電子カルテ停止 → 全診療に影響
  - 例：院内LAN一部停止 → 部門等に限定

発動時チェックリスト

- BCP発動を判断する前に確認すべき項目をテンプレート化
- 停止システム名／影響範囲／復旧見込み時間／代替手段の有無 など

業務影響度マトリクス・ケーススタディ（例）

障害ケース	規模・範囲	業務影響度	発動判断の目安
端末トラブル	個別	軽微 （代替端末で対応可能）	発動せず、現場内で解決
プリンタ不調	部署単位	局所的（伝票印刷に影響）	発動せず、部門調整
PACS障害	部分システム	中等度（画像診断の遅延）	部分発動、関連業務を制限
電子カルテ障害	全院的	重大（診療全体に影響）	全面発動
地域連携システム障害	外部連携	中規模（地域調整に支障）	部分発動、代替手段を活用
院内LAN障害	部分または全域	中～重大（アクセス制限）	範囲次第で部分～全面発動
クラウドサービス障害	広域・外部依存	重大 （外部クラウド利用不能）	速やかに発動、外部機関連携

発動時チェックリストの例

	重要度	項目	記入欄（メモ）
□	★	発生を認知した日時	
□	★	判断材料（通報／アラート／ログ／その他）	
□	★★★	停止システム名	
□	★★★	影響範囲（部署／全院／地域連携）	
□	★★★	復旧見込み時間（数時間以内／半日以上／不明） ＜xx時間以上見込まれる場合は発動＞	
□	★★	代替手段の有無（紙カルテ、参照バックアップなど）	
□	★★★	安全上のリスク （患者安全に直結するか、患者データ安全に影響するか）	
□	★★	エスカレーション実施状況（責任者・執行部への報告）	

- 特に重要なのは **システム・影響範囲・復旧見込み・患者安全**
- チェックリストはただの記録ではなく、**発動の根拠を整理するためのツール**
- 重要度にメリハリをつけることで、判断がブレにくくなる

判断材料に必要なもの

既存の「職員からの通報」「アラート」だけでは発動判断はできない

判断フロー × 影響度マトリクス × チェックリスト の3点セットを整備することで、発動判断の根拠が揃う

→BCP発動は重い責任を伴う。

判断材料を整備しないと、説明責任が果たせない。

災害医療の原則 CSCATTT - IT障害への応用

災害医療で用いられる CSCATTT

あらゆるハザードを想定した大規模災害発生時の体系的な対応の7つの基本原則

	項目	内容
C	Command & Control（指揮・統制）	指揮官および指示命令系統を明確にする
S	Safety（安全確保）	自分自身、現場、患者の安全を確保する
C	Communication（情報伝達）	迅速・簡潔・正確な情報伝達と共有を確保する
A	Assessment（評価）	収集した情報を基に状況を評価する
T	Triage（トリアージ）	限られた資源で最大多数を救助するため振り分けを行う
T	Treatment（治療）	限られた資源で最大多数に対応し、状態の安定化と搬送につなげる
T	Transport（搬送）	適切な患者を、適切な場所へ、適切な時間に移送する

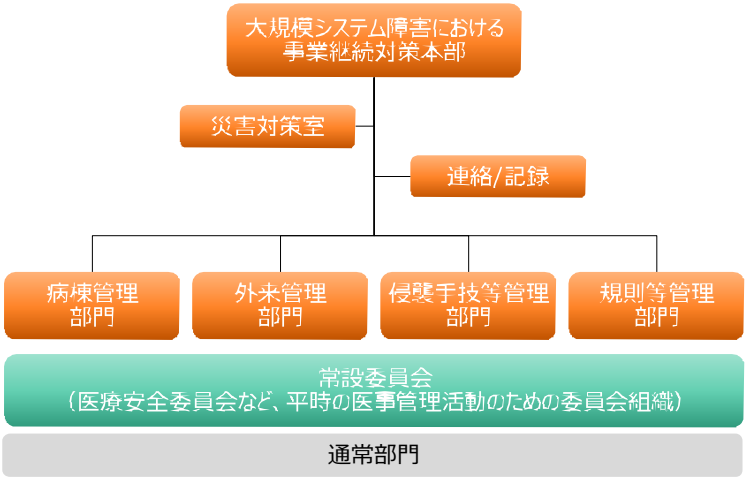
参考　日本災害看護学会用語 https://jsdn.info/glossary/cscattt/

CSCAの原則は災害医療だけでなく、IT障害時の医療継続にも応用できる

C: Command & Control（指揮・統制）

＜大阪急性期・総合医療センターの例＞

- 平時と非常時では「意思決定の体制」を切り替える必要がある
- 会議体を立ち上げ、各部門から情報を集約・調整する
- 対策本部会議で病院の意思決定、方針を共有する



事業継続対策本部：
指揮官（Incident Commander）を含む会議体と体制を形成
災害対応の最高責任者（通常は院長や副院長）意思決定と全体統制を行う。

災害対策室（本部機能）：
各部門の状況を集約し、全体の調整・指示伝達を補助。
事務局的な機能を持ち、会議運営や情報掲示も担う。

病棟管理部門：
入院患者の安全確保（避難、転棟、ベッド管理）。
病棟医師・看護師を中心に運営し、限られた病床を効率的に運用する。

外来管理部門：
救急外来・トリアージエリア・一般外来を統括。
傷病者受け入れ、トリアージ分類、初期診療を担当。

侵襲手技等管理部門：
手術室、ICU、透析室、処置室などを統括。
緊急手術・集中治療のリソース配分や優先度調整を行う。

規則等管理部門：
資材・医薬品・人員の調達（Logistics 相当）。
規則・マニュアル・方針を基準に、業務を統一化。
BCP（業務継続計画）の発動管理や内部調整も担う。

連絡・記録担当：
外部機関（消防・保健所・行政・DMAT）との窓口（Liaison Officer 的役割）。
全ての意思決定・活動内容を記録し、時系列で整理（Finance/Planning 相当）。
情報共有とエビデンス確保を行い、事後の検証にも資する。

S: Safety（安全確保）

- **患者誤認防止が最優先**
  - 患者の識別、IDでの確認を可能にする
- **診療継続に必須の情報**
  - 禁忌・アレルギー情報
  - 現在の処方状況（内服薬・注射薬）
  - 検査値など急変リスクを見極める情報

入院患者	かかりつけ 外来患者
• 患者本人からの聞き取り確認 • 主治医、担当看護師等の記憶 • 紙で残るメモ	• お薬手帳 • 処方箋 • 診療情報提供書
解決策（例）： 平時からサマリーやカルテを印刷しておく	解決策（例）： 患者本人に渡して管理してもらう

•律速段階の把握、安全に業務を運用できる限界を知ることまでが安全確保となる

- 紙や記憶に依存する対応では件数に制約がある
-限界を超えると誤薬・誤処置など重大インシデントにつながる

律速段階のコントロール例

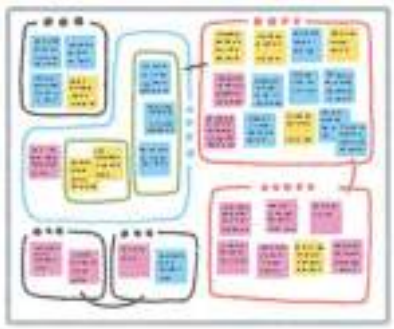
・紙運用の習熟度
- 平時の訓練
- 有事におけるモニタリングとフィードバック

・検査の対応レベル
- モダリティの保存容量からの検査数上限算定
- 生理検査の所要時間から1日あたりの上限を算定

・治療(手術、薬剤投与、血管造影等)
- モニタリングしながら件数を徐々に増やす

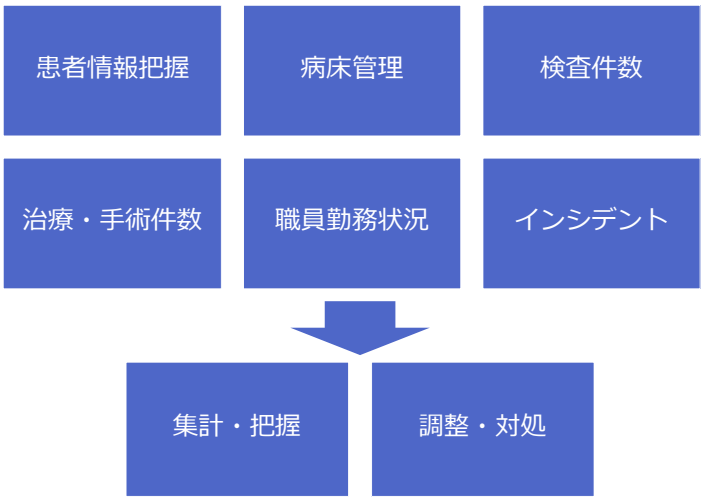
C: Communication（情報伝達）

- **正しい情報の拠り所と伝え方**
  - 職員の不安低減と混乱の防止
- **複数の伝達手段を確保する**
  - 掲示板・ホワイトボードによる当日情報の整理
  - 内線電話による確認、疑義照会
  - メール、グループウェア（Teams等）による周知
- **電子カルテと比べると、伝達スピードは圧倒的に遅くなる**
  - 遅いことはやむを得ないとの割り切り
  - 発信側：簡潔・正確に伝える工夫が必要
  - 受信側：確実に確認・共有する意識が必要



A: Assessment（評価）

- **状況を把握しなければ改善も判断もできない**
  - モニタリングの対象
  - 対応件数（診療・検査・処方など）
  - ミス・インシデントの発生状況
  - 業務時間や人員負荷
- **流れ**
  - 部門内での検討：ブレーキをかけるか、アクセルを踏むか
  - 全体会議体で共有：上限を引き上げるか、現状維持か、引き下げるかを判断
- **目的**
  - 「安全に業務を回せる限界」を見極める
  - フェーズ移行や業務縮小・拡大の判断材料に



CSCA ― 医療継続の基本枠組み

CSCAを整えることが初期の混乱を押さえ、回復途中段階の業務拡張にもつながる

C：Command & Control（指揮・統制）

平時→非常時で体制を切り替え
会議体を立ち上げ、情報を集約し一本化

S：Safety（安全確保）

患者誤認防止：ID番号・禁忌・アレルギー・処方を確認
安全に業務を回せる限界を把握

医療継続の基盤

A：Assessment（評価）

件数・時間・ミス・負荷をモニタリング
部門内検討（ブレーキ／アクセル）→全体会議体で判断

C：Communication（情報共有）

電子カルテより遅い＝発信側の工夫と受け側の意識が必要
多層的に伝達、共有手段を準備し、正確かつ確実に

まとめ

まとめ

・IT-BCPは策定はした　→ 発動条件や発動方法を整備しておく

・災害医療の原則 CSCATTTは、IT障害への応用が可能

※IT-BCP発動条件やCSCATTTのIT障害への応用に関する詳細は、
【R7年度：講師育成コース】を受講してください。