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

経営とレジリエンスコース

インシデントによる経営インパクトに基づく対策の力の入れどころ

2025年9月3日

一般社団法人ソフトウェア協会

目次

研修の目的

サイバー・インシデントにおける経営インパクトの視点で、
攻撃手順と暗号化の時系列例からの分析に基づき、
強靭なシステム構築を目指した対策の力の入れどころに
ついて紹介し、経営者が認識するべきレジリエンスについて
学びます。

サイバー・インシデントにおける経営インパクト

大阪急性期･総合医療センター（OGMC）のランサムウェア事案


大阪の病院で電子カルテシステムに障害、「ランサムウェア」によるサイバー攻撃か

2022/10/31 22:23

大阪急性期・総合医療センター（大阪市住吉区、病床数８６５床）は３１日、電子カルテのシステムに障害が発生し、緊急以外の手術や外来診療などを停止したと発表した。外部から不正アクセスを受け、データを復旧するために金銭を要求する「ランサム（身代金）ウェア」と呼ばれるコンピューターウイルスに感染したとみられる。患者の個人情報の流出などは確認されていないという。

センターによると、システム障害が判明したのは３１日午前６時３８分。コンピューター上に「すべてのファイルが暗号化された」と英語のメッセージが記されていた。「復元のためにはビットコインを支払え」とあり、返信用のメールアドレスも示されていた。

センターは要求に応じないことを決め、３１日午前９時から診察を中止。この日は６００～１０００人の外来患者や入院患者の診療に影響が出たほか、救急患者の受け入れもできなくなった。通常業務の再開の見通しは立っておらず、病院から相談を受けた大阪府警が経緯を調べている。

概要

- 2022年10月31日、ランサムウェア攻撃を受け、電子カルテを含む総合情報システムが利用不能となった
- 救急や外来診療、予定手術などの診療機能に大きな支障が生じた

原因

- 委託先の給食事業者の端末を介しての病院給食サーバーへの侵入

被害額

- 調査復旧、逸失利益の被害額は20億円以上

出典：読売新聞（https://www.yomiuri.co.jp/national/20221031-OYT1T50162/）

大阪急性期･総合医療センター（OGMC）概要

項目	説明
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（125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
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）

項目	説明
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）

情報セキュリティインシデント調査委員会報告書について | 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（opho.jp）

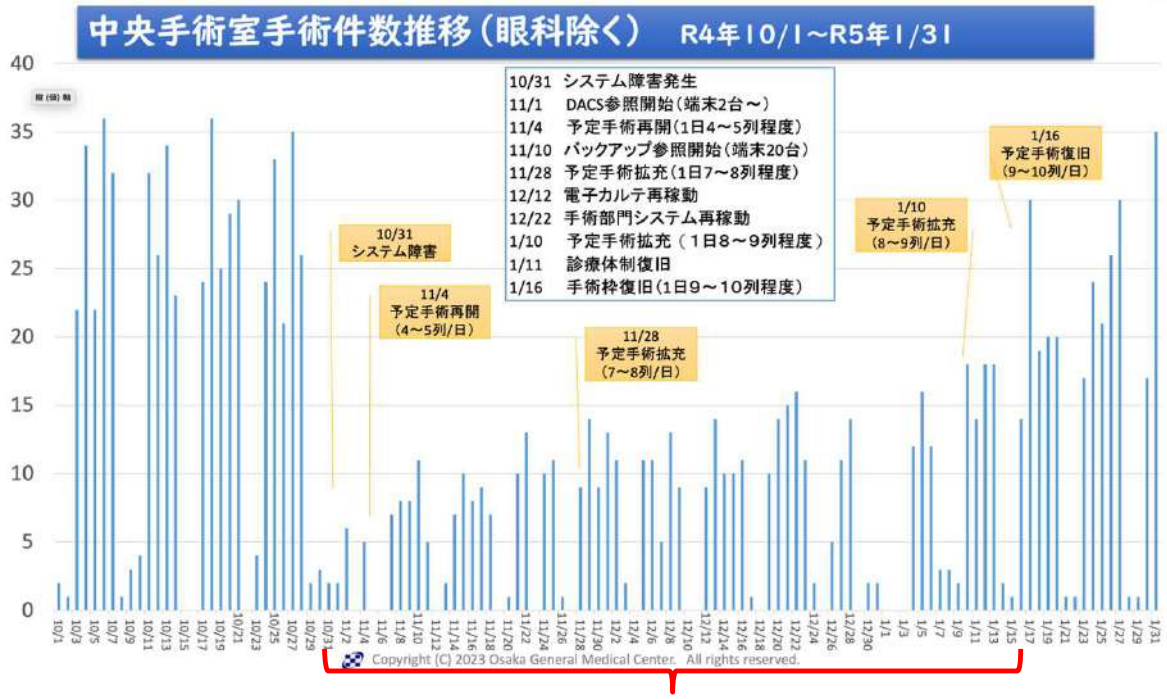
インシデント当日の経緯

5時台	各現場で**電子カルテの動作不良**を確認したものの、通常操作が出来たため**経過観察**
6時台	病院の職員や給食委託事業者の職員が**電子カルテシステムの障害発生を確認**。給食事業者からも（病院に）データが送信できないと連絡がある。
7時45分	システム運用管理を委託されている職員が、サーバーの画面上に**ランサムウェアのメッセージを確認**。
8時15分	給食事業者から**サーバーがウイルスに感染した可能性**があるとの連絡を受ける。
8時40分	病院から連絡を受け現地調査を行った電子カルテを構築したベンダー担当者と職員の判断で、**全てのサーバーのLANケーブルを抜線**して回る。
8時50分	幹部会議でシステム障害の深刻さが確認され、**外来、入院、救急受入停止と当日予定されていた手術の中止が決定**される。
9時30分	病院スタッフは**大阪府や警察、内閣サイバーセキュリティセンターへ連絡**を行う。
11時30分	厚生労働省から専門家チーム派遣の連絡が届く。
12時00分	**第一回BCP対策本部会議が開催**され**紙カルテ運用**による可能な限りの医療継続の方針、そして厚生労働省への専門家チームの派遣要請が決定される。
16時00分	WEB会議にて、システム関係者と専門家チームによる**インシデント状況の確認**が行われる。
17時00分	**職員向け説明会**と**病院HPで外来診療の一時停止の案内**が行われる。
19時00分	システム関係者と専門家チームが更なる調査を行う。
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情報公開が行われる。

その後、約2ヶ月間にわたる医業制限下での事業継続に尽力

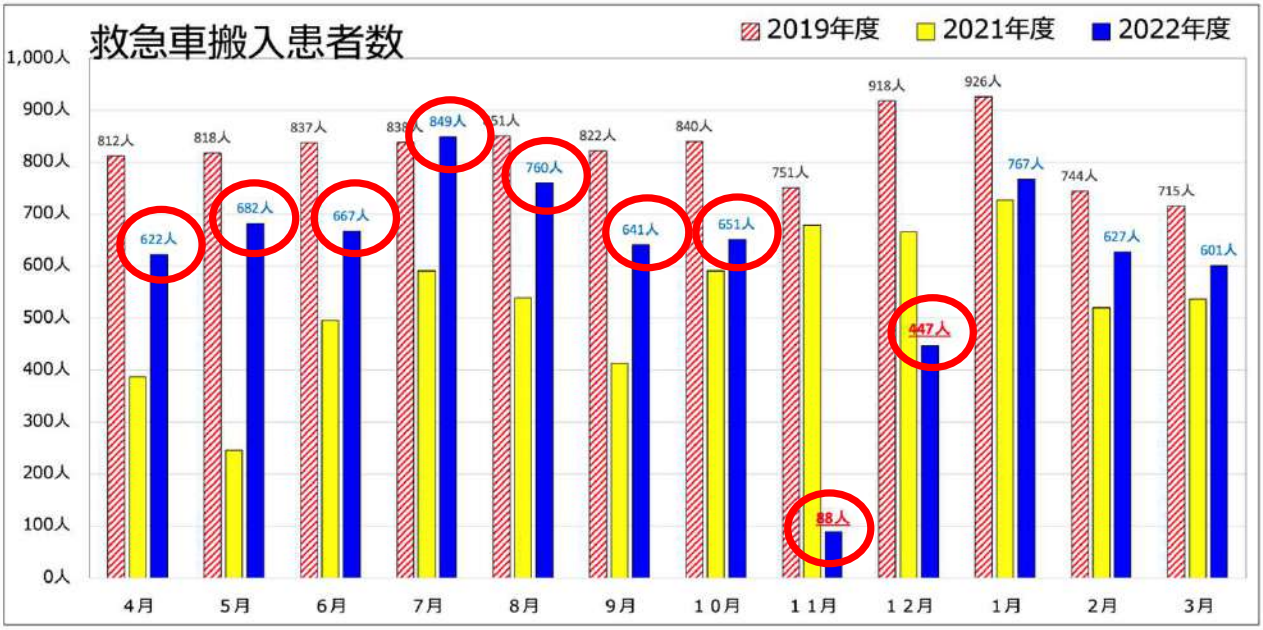
サイバー攻撃により直面する病院経営危機

病院経営への影響（中央手術室手術件数推移）



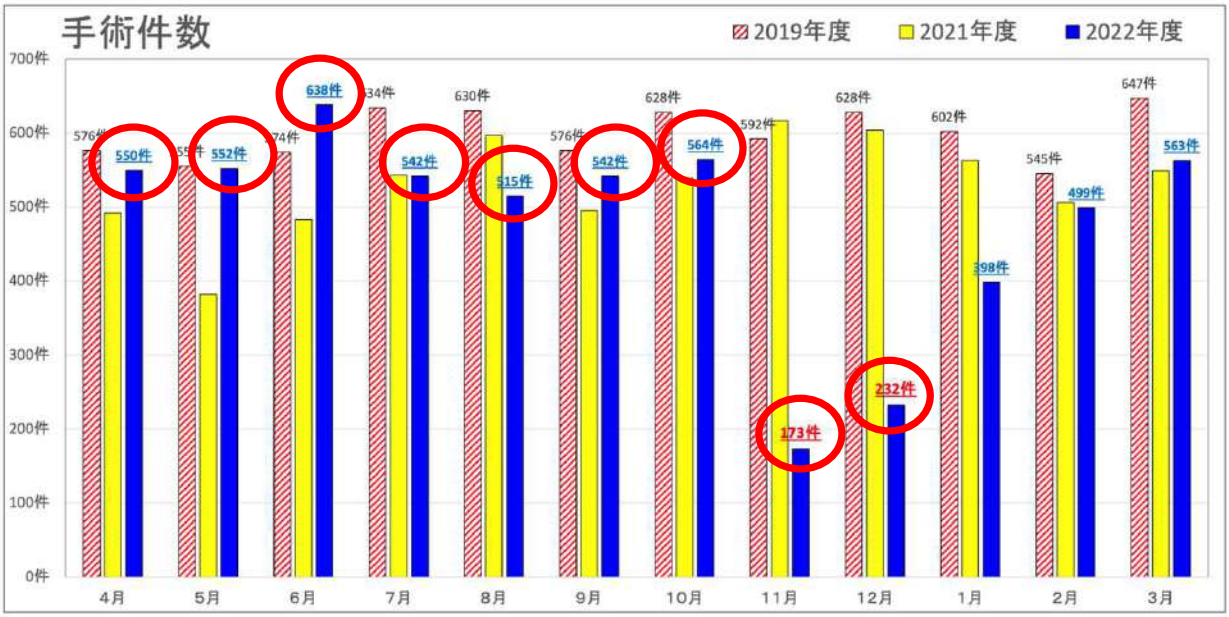
提供元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター （掲載許諾済み）

病院経営への影響（救急車搬入患者数）



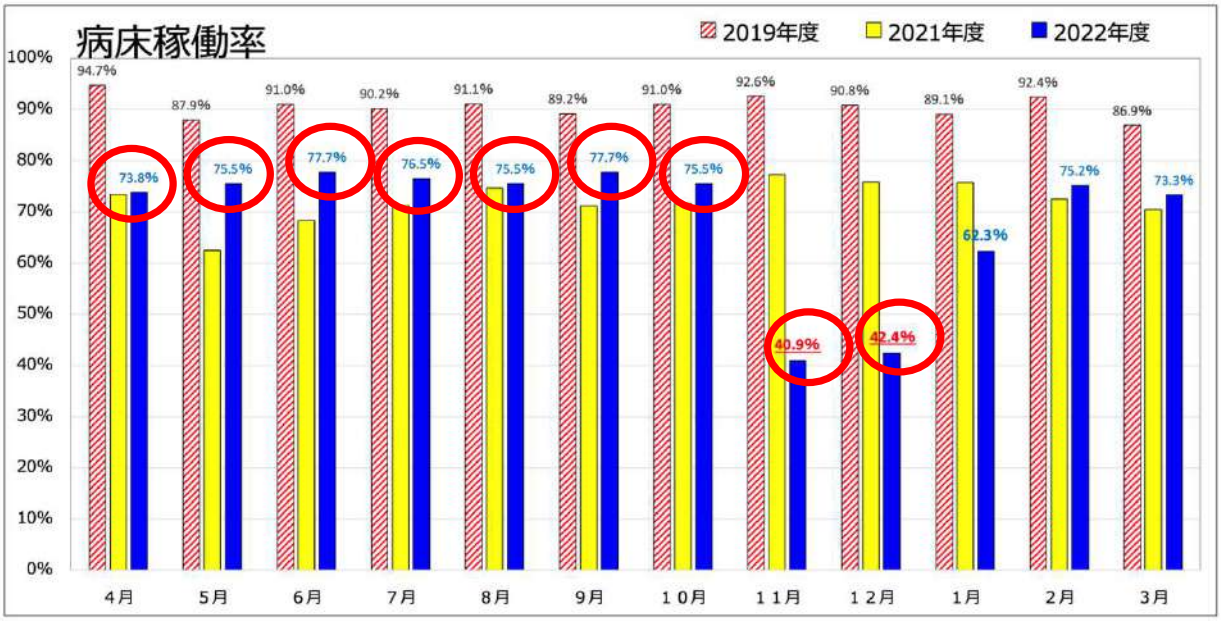
提供元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター （掲載許諾済み）

病院経営への影響（手術件数）



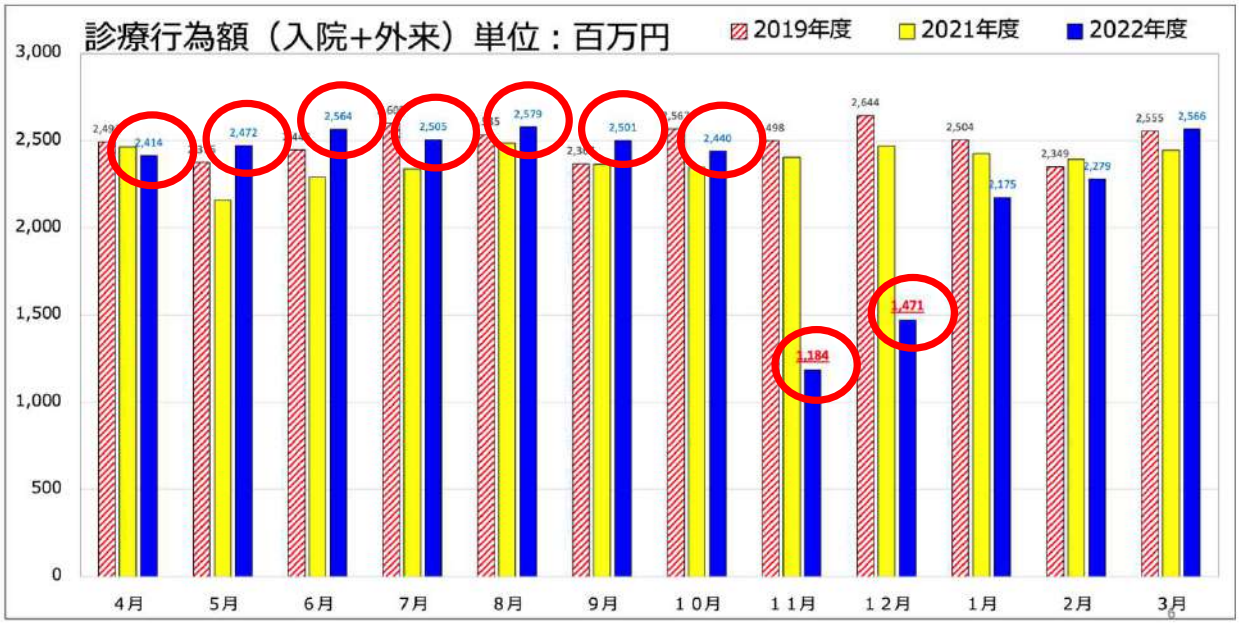
提供元：地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター （掲載許諾済み）

病院経営への影響（病床稼働率）



提供元：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 （掲載許諾済み）

病院経営への影響（診療行為額）



提供元：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 （掲載許諾済み）

診療制限に伴う収益減少

システム障害期間中の対前年同月比較での各種指標値

	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）	807	1,727	47%	1,016	1,773	57%
外来診療行為額（百万円）	376	675	56%	454	696	65%

提供元：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 （掲載許諾済み）

サイバー攻撃により直面する病院経営危機

①システム障害は診療制限に直結
大幅な収益減少（前年同月対比 2 か月間で約 22 億円の減収）

②診療報酬請求ができない
現金収入が途絶え、資金不足の可能性（2 ヶ月間、診療報酬請求ができなかった）

③サイバー被害の復旧費用が嵩み、収支差も悪化。（約5億円の対応費用が発生）

④さらに個人情報漏洩の可能性が生じた場合は、その患者対応費用が発生。
（漏洩は確認されなかった）

診療報酬請求遅延に伴う現金収入の停止

・10月31日にシステム障害発生、レセプト請求が再開されたのが1月以降
・10月、11月診療分のレセプト請求は、それぞれ2か月遅れ
→医事会計システムが復旧した 12月12日以降に、全て目視による手入力作業
・12月、1月診療分は3月に請求
・2月、3月診療分は4月に請求
※事実上、12 月と 1 月の審査支払機関からの入金が途絶えた
※職員の給与や賞与、業者に対する材料費や委託費・光熱水費の支払いなどに苦慮

資金ショートによる破産の可能性があった

バックアップがあったにも関わらず障害が長期化した理由

①すべてのサーバーや端末の初期化を行うという決断（約2,200台　初期化200台/日）

・ADサーバのログからは端末のログオン失敗が1,000台程度確認。
・半年前からのサイバー攻撃の確認
・把握し切れていない外部接続箇所が複数ある可能性
・侵害されたサーバからの横展開が容易な環境（PWが共通、アカウントロックなし）
・電子カルテシステム、部門システム、医療機器など、確認した殆どのシステムや機器で、
最新のバージョンのOSではなく、パッチも適用されておらず、サポート切れOSの利用も散見

※病院全体のシステム障害状況（範囲・深度）や潜在的な脅威の有無を
明確にできず、やむを得ず初期化

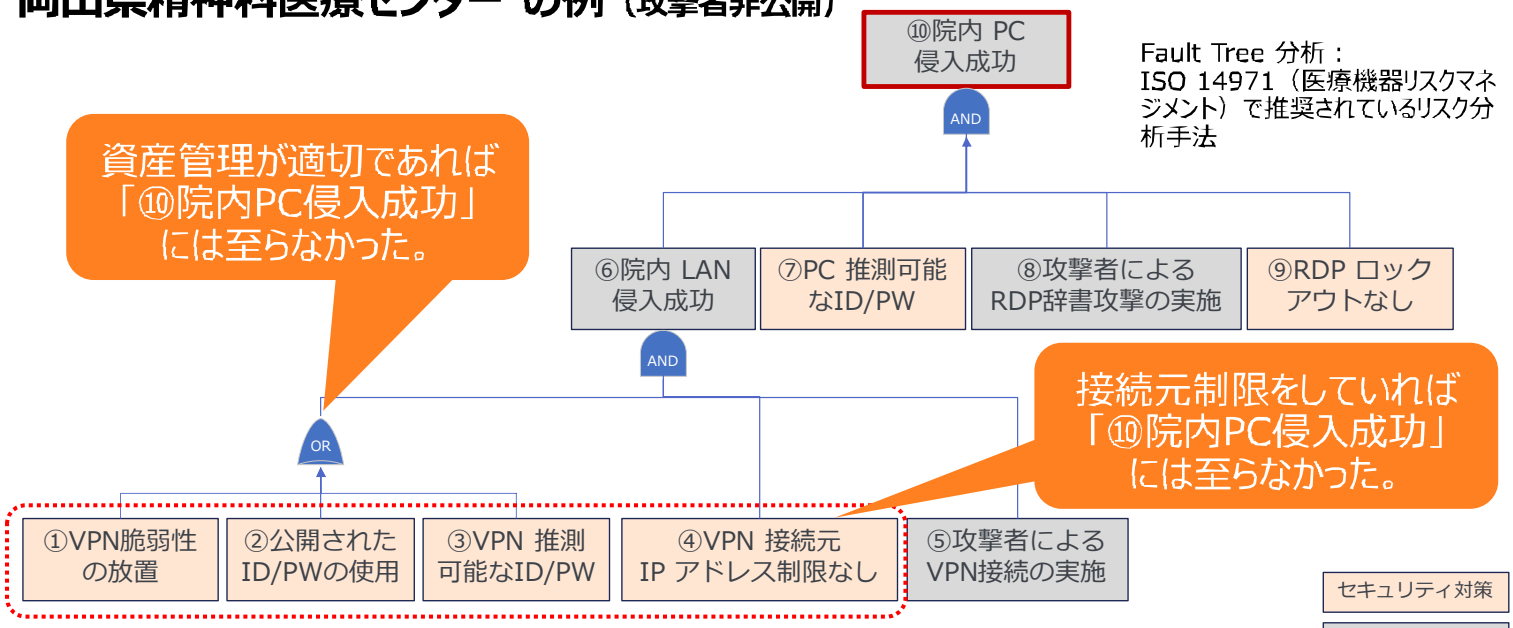
②再発防止策として、新たなセキュリティ設計によるテストを実施

侵害原因がシステムの初期設定の脆弱性が要因となったことから、再発防止策を講じるにあたり、
新たなセキュリティ設計によるテストを行う必要があった

障害の長期化を防ぐ施策がレジリエンスの向上につながる

ランサムウェアの攻撃手順と医療制限

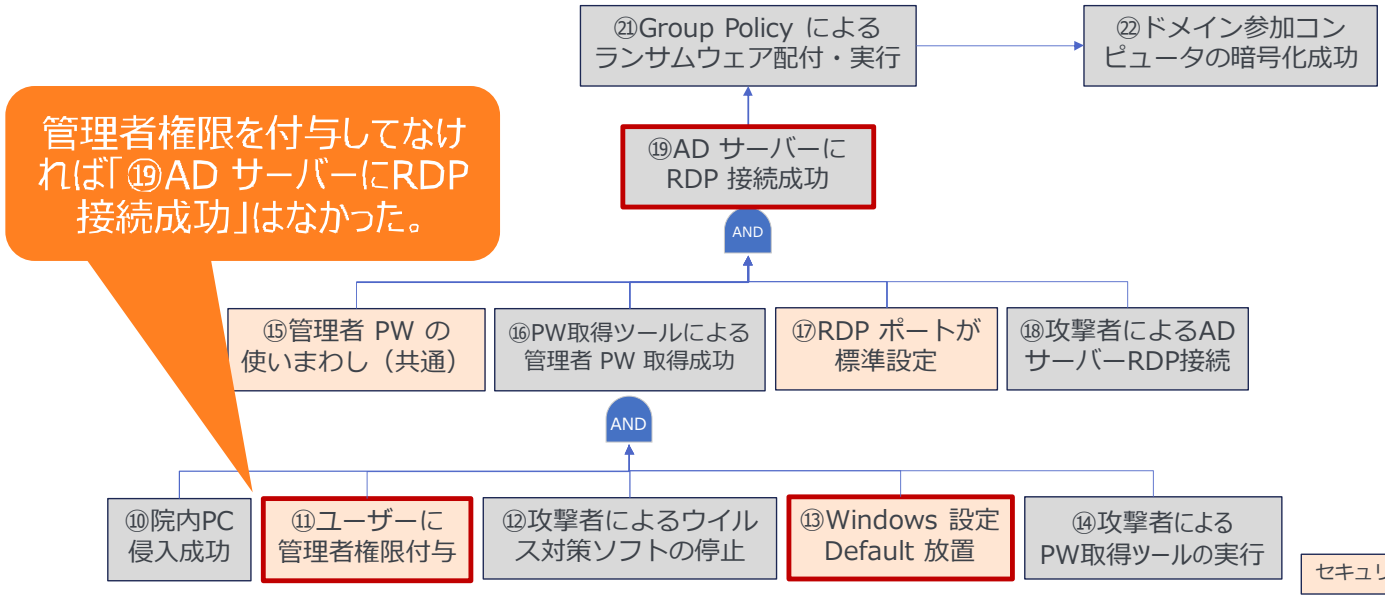
【ランサムウェアの攻撃手口のポイント】
ランサムウェア初期侵入での攻撃手口と攻撃成功の条件
岡山県精神科医療センター の例（攻撃者非公開）



Fault Tree 分析：
ISO 14971（医療機器リスクマネジメント）で推奨されているリスク分析手法

セキュリティ対策
攻撃者の手口

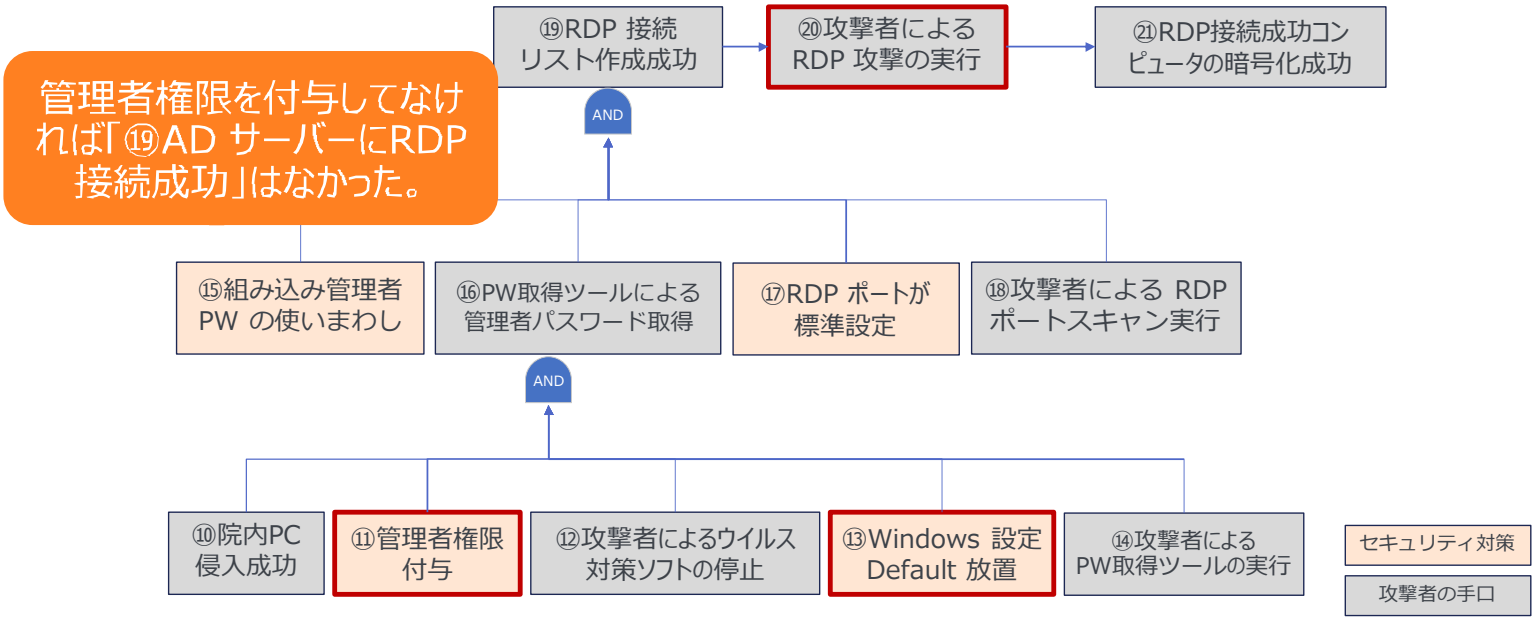
【ランサムウェアの攻撃手口のポイント】
院内 PC ログオン成功後の攻撃手口と攻撃成功の条件
徳島県つるぎ町立半田病院の例（LockBit2.0による攻撃）



セキュリティ対策
攻撃者の手口

【ランサムウェアの攻撃手口のポイント】

院内 PC ログオン成功後の攻撃手口と攻撃成功の条件
大阪急性期・総合医療センターの例 （Phobosによる攻撃）



【ランサムウェアの攻撃手口のポイント】

「⑲AD サーバーにRDP 接続成功」「⑳攻撃者によるRDP 攻撃の実行」まで成功すると 10万ファイル、53GB の暗号化にかかる時間

Family	暗号化にかかる中央値
LockBit	0:05:50
Babuk	0:06:34
Avaddon	0:13:15
Ryuk	0:14:30
Revil	0:24:16
BlackMatter	0:43:03
Darkside	0:44:52
Conti	0:59:34
Maze	1:54:33
Mespinoza (PYSA)	1:54:54
平均値	0:42:52

出典：An Empirically Comparative Analysis of Ransomware Binaries
https://www.splunk.com/en_us/form/an-empirically-comparative-analysis-of-ransomware-binaries.html

【ランサムウェアの攻撃手口のポイント】
「⑩院内 PC侵入成功」すると

漏えい等の報告及び本人通知（個人情報保護法第26条）
個人の権利利益を害するおそれがあるときに該当する事態

【例1.】
不正アクセスにより個人データが漏えいした場合

【例2.】
ランサムウェア等により個人データが暗号化され、復元できなくなった場合

不正の目的をもって行われた漏えい等が発生した事態

速報（新規）
発覚日から、3～5日以内

確報（続報）
発覚日から、30日以内
不正な目的 60日以内

【ランサムウェアの攻撃手口のポイント】

ウイルス対策ソフトウェアは機能していた（2021/10/31 03:20:05）

Timestamp	EventI	Summary
2021-10-30T11:06:58.0616417	1150	エンドポイント保護クライアントは正常に稼働しています。
2021-10-30T12:06:57.9366254	1150	エンドポイント保護クライアントは正常に稼働しています。
2021-10-30T13:06:57.8161794	1150	エンドポイント保護クライアントは正常に稼働しています。
2021-10-30T14:06:57.6894984	1150	エンドポイント保護クライアントは正常に稼働しています。
2021-10-30T15:06:57.5643429	1150	エンドポイント保護クライアントは正常に稼働しています。
2021-10-30T15:17:34.5541457	2000	Microsoft Defender ウイルス対策 のセキュリティ インテリジェンスのバージョンが更新されました。
2021-10-30T15:17:34.5543393	2000	Microsoft Defender ウイルス対策 のセキュリティ インテリジェンスのバージョンが更新されました。
2021-10-31T03:20:05.3777937	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:20:05.7826577	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:20:06.0369943	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:20:07.2442199	2010	Microsoft Defender ウイルス対策 はクラウド保護を使用して、追加のセキュリティ インテリジェンスを取得しました。
2021-10-31T03:20:07.2442421	2010	Microsoft Defender ウイルス対策 はクラウド保護を使用して、追加のセキュリティ インテリジェンスを取得しました。
2021-10-31T03:20:07.6106346	2010	Microsoft Defender ウイルス対策 はクラウド保護を使用して、追加のセキュリティ インテリジェンスを取得しました。
2021-10-31T03:20:07.6106554	2010	Microsoft Defender ウイルス対策 はクラウド保護を使用して、追加のセキュリティ インテリジェンスを取得しました。
2021-10-31T03:20:11.5937749	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:20:21.7133307	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。
2021-10-31T03:20:32.8332166	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。
2021-10-31T03:20:32.8346453	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。
2021-10-31T03:20:32.8359403	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。

資料提供・許諾：
徳島県つるぎ町立半田病院

【ランサムウェアの攻撃手口のポイント】
「⑪管理者権限付与」で、
ウイルス対策ソフトウェアは停止させられた
（2021/10/31 03:23:39）

2021-10-31T03:23:17.6791161	5007	Microsoft Defender ウイルス対策 の構成が変更されました。予期しないイベントだった場合は、マルウェアによる変更の可能性があるため、設定を確認する必要があります。
2021-10-31T03:23:17.6791318	5007	Microsoft Defender ウイルス対策 の構成が変更されました。予期しないイベントだった場合は、マルウェアによる変更の可能性があるため、設定を確認する必要があります。
2021-10-31T03:23:17.6791427	5007	Microsoft Defender ウイルス対策 の構成が変更されました。予期しないイベントだった場合は、マルウェアによる変更の可能性があるため、設定を確認する必要があります。
2021-10-31T03:23:27.6235933	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:23:27.8171385	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:23:27.9550645	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。
2021-10-31T03:23:33.4512974	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:23:33.5773243	1116	Microsoft Defender ウイルス対策 でマルウェアまたは他の望ましくない可能性のあるソフトウェアが検出されました。
2021-10-31T03:23:33.7089243	1117	Microsoft Defender ウイルス対策 により、マルウェアまたは他の望ましくない可能性のあるソフトウェアからこのコンピューターを保護する操作が実行されました。
2021-10-31T03:23:37.7380084	5012	Microsoft Defender ウイルス対策 スキャンがウイルスに対して無効になっています。
2021-10-31T03:23:37.7380275	5010	Microsoft Defender ウイルス対策 スキャンがスパイウェアおよび他の望ましくない可能性のあるソフトウェアに対して無効になりました。
2021-10-31T03:23:37.7570346	3002	Microsoft Defender ウイルス対策 リアルタイム保護機能でエラーが発生して失敗しました。
2021-10-31T03:23:39.9015754	5001	Microsoft Defender ウイルス対策 リアルタイム保護スキャンが、マルウェアおよび他の望ましくない可能性のあるソフトウェアに対して無効になりました。

資料提供・許諾：
徳島県つるぎ町立半田病院

ランサムウェアの攻撃手口のポイントと医業への影響のまとめ

近年のランサム事案のポイント		事例	影響	医業制限（紙カルテ運用）	信頼失墜（患者減少）	対策コスト支出
暗号化の時間	53GB の暗号化	最速5分50秒	「⑳攻撃者によるRDP攻撃の実行」に至れば瞬く間に医業制限、信頼失墜、対策コストの影響	**必至**	**必至**	**必至**
	仮想基盤の暗号化	数十秒				
個人情報保護委員会への対応	法26条に基づく個人情報保護委員会への報告と本人通知	不正アクセスの場合、必須コールセンターの設置費用	「⑩院内PC侵入成功」に至れば、個人情報漏えいの有無を調査しなければない ※セキュリティ会社、有識者による調査	調査結果次第	調査結果次第	**必至**
	個人情報保護委員会への報告用フォレンジック費用	クライアント： 200万円/台～ サーバー： 400万円/台～ ※復旧費用は含まれないことに留意	不正アクセスの場合、再発防止策策定のための原因究明が必要となる。	調査結果次第	調査結果次第	**必至**
ウイルス対策ソフトの有効性		ランサムウェアやツールに対して、ウイルス対策ソフトは有効である ※但し、バイパス手法が存在する	「⑪管理者権限付与」もしくは「⑬Windows設定Default放置」に当てはまらなければ、ウイルス対策ソフトが機能し検知・駆除の可能性がある	状況次第	状況次第	状況次第

・資産管理の徹底を実施し、外部侵入経路となる通信機器の把握と脆弱性の排除
・Windows設定を堅牢化と、全てのPC・サーバOSを最新に維持
・推測可能なID/PWを避け、一般ユーザPCに管理者権限を付与しない

レジリエンス向上に向けた対策の優先順位

レジリエンス向上に向けた対策の優先順位

万が一に備え、医業制限時の安全な医業継続と医業制限期間の短縮化をめざす

～いわゆる適切なBCPの整備～

1. 大規模システム障害下での安全な医業継続のための備え

2. 基幹システム再開までの期間を短縮するための対策

3. BCPを適切に機能させるための管理

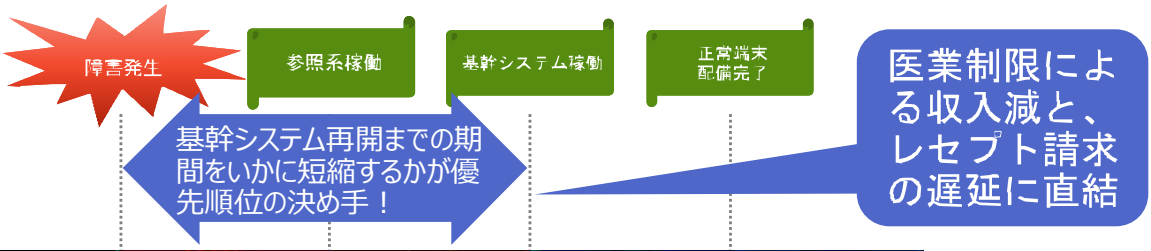
大規模システム障害のBCP（IT-BCP）

フェーズ1	• 患者の過去（病歴、検査結果等）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

（※）OGMCは、電子カルテなどの基幹システムとセグメントが異なっていたおかげで、 参照環境である診療記録文書統合管理システム DACS(Document Archiving and Communication System)の運用を開始できた。これにより、システム障害発生直前までの診療録、処方箋、注射箋、血液検査や心電図の結果、画像所見、紹介状、同意書などの参照・印刷が可能となった。

大規模システム障害のフェーズと復旧イベント



復旧イベント			フェーズ1			フェーズ2		フェーズ3		フェーズ4
			当日	次フェーズまで		当日	次フェーズまで	当日	次フェーズまで	
共通		(1) 紙対応開始	○							
共通		(2) 院外への情報発信	○							
共通		(3) 外部医療機関への患者依頼	○							
外来	再診	(4) 制限下開始		○						
外来	再診	(5) 制限下増強				○				
外来	再診	(6) 通常開始						○		
外来	新患	(7) 制限下開始			○					
外来	新患	(8) 制限下増強					○			
外来	新患	(9) 通常開始							○	
入院病棟	在院	(10) 診療継続	○							
入院病棟	緊急	(11) 侵襲手技等開始					○			
入院病棟	緊急	(12) 制限下開始				○				
入院病棟	予定	(13) 通常開始								○
入院病棟	予定	(14) 制限下開始						○		
入院病棟	予定	(15) 通常開始								○

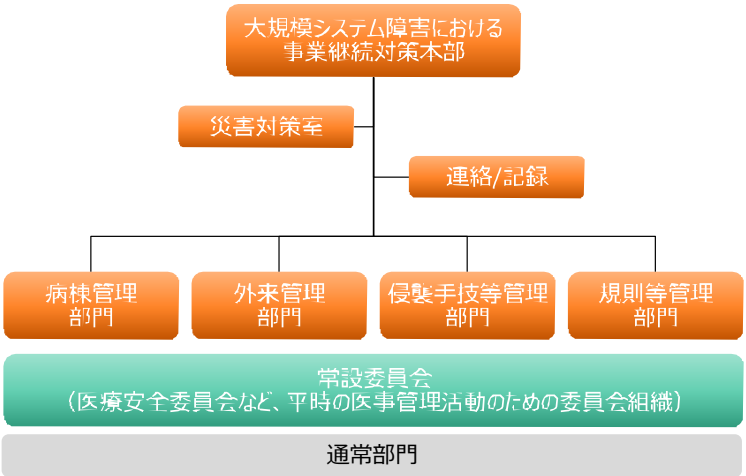
レジリエンス向上に向けた対策の優先順位

1. 大規模システム障害下での安全な医業継続

- 会議体の設立
- 患者情報を把握する
- 医業プロセスのボトルネックの把握
- メンタルを正常に保つ

大規模システム障害時にIT-BCPを機能させるための体制と会議体

～CSCAの「Command & Control」を具現化するICSの導入例～



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。

指揮命令系統・責任と役割の明確と管理責任者と、
実施責任者の両者を任命により、多職種のシームレスな横断的対応と周知徹底のマネジメントを実行する

※CSCA：災害医療において「CSCATTT（Command & Control、Safety、Communication、Assessment、Triage、Treatment、Transport）」という 7 つの原則の前半部分を指し、日本では災害時の医療活動における組織的対応を表す行動指針として広く使われている。災害時の情報サージによる混乱を抑えて意思決定プロセスを明確化することがねらい。
※ICS：「Incident Command System」CSCA の「C（Command & Control）」を具現化する仕組み。指揮系統の一本化・安全確保・通信の標準化を担い、CSCA の各要素を実行する役割を持つ。

患者情報を把握する

～フェーズ1では参照系環境ができるまでID番号がある患者をいかに把握するかが重要～

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

入院患者：
主治医、担当ナース、担当薬剤師、担当セラピスト等の紙媒体での記録・メモや記憶を紙カルテに記録する。
※入院患者本人から聞き取りも（連絡先も紙印刷で用意）

掛かりつけ患者：
お薬手帳、処方箋、診療情報提供書から情報を得る。

【解決策の例（OGMCの例）】
入院患者：　平時から、週間サマリーの作成や一日の終わりにカルテをプリントアウトを実施し管理。
掛かりつけ患者：本人に管理してもらうしかない。

律速段階を把握する

～フェーズ1、2では入院患者の安全確保のために律速段階を把握する必要がある～

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

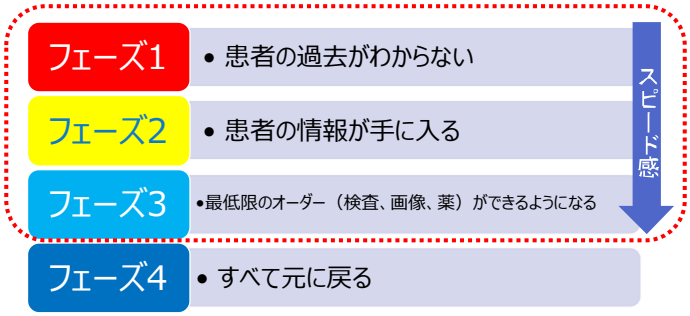
紙運用の限界を把握する（OGMCの例）

OGMCにおける緊急受入再開に向けてのボトルネック分析
・紙運用の習熟度
・画像検査結果の確認方法
・緊急検査の判明時間
※対策本部にて採血検査件数、画像診断件数、受入患者数を共有し分析

【律速段階のコントロール例（OGMCの例）】
紙運用の習熟度：　平時の訓練と、有事のモニタリングおよびフィードバック
採血検査：　外来検査の1日あたりの限度をモニタリングしながら調整
画像検査：　画像機器の画像保存容量から対応人数の割り出し
治療（薬剤投与、手術、血管造影等）：モニタリングしながら手術件数を徐々に増やすしかない

メンタルを正常に保つ

～フェーズ1、2、3では特に緊急事態ストレスマネジメントが重要～



平時のストレスチェックやでブリーフィング以外に、

有事での情報の共有と紙運用のスピードに意識を合わせる（OGMCの例）

情報の共有：職員の不安を除去するためには、今何が起こっているか、BCPで用意されたマニュアル以外に、規則等管理部門が作成するマニュアルを都度共有できることが重要。さらに、回復計画の行程表も有用で、全てにおいてある程度オープンにしておく方がよい

「遅さ」の認識：紙運用にともなう律速段階に合わせ、平時のスピード感を無視した雰囲気を作る

【職員の不安を低減する施策例（OGMCの例）】
伝達ツール：災害時の安否確認システムに存在したメール送信に機能に
添付ファイル機能を追加
スピード感の無視：　遅いことはやむを得ないという認識を共有

レジリエンス向上に向けた対策の優先順位

万が一に備え、医業制限時の安全な医業継続と医業制限期間の短縮化をめざす

～いわゆる適切なBCPの整備～

2. 基幹システム再開までの期間を短縮

- ランサムウェアの基本的対策による、攻撃影響範囲の局所化
（ランサムウェア攻撃以外にも有効）
- バックアップ・参照系システムの適切な運用

ランサムウェアの基本的対策による、攻撃影響範囲の局所化

～フェーズ1、2の期間をいかに短縮するか～

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

短縮したい

平時のセキュリティ対策で、万が一の障害を局所化

資産管理：守るべき情報システム資産を全て把握していなければ、最新OS管理（脆弱性対策）、適切な設定（通信機器、サーバ・端末、医療機器の堅牢化）はできない。

横展開防止：不幸にも外部から侵入された場合、攻撃の影響範囲を局所化できるか否かは、フェーズ1、2の期間短縮に直接影響。以下の基本対策の実施が重要。

さらに、**オンラインバックアップや参照系を守る**ことにもつながる。

【基本的な対策】

・資産管理の徹底を実施し、外部侵入経路となる通信機器の把握と脆弱性の排除

・Windows設定の堅牢化と全てのPC・サーバOSを最新に維持

・推測可能なID/PWを避け、一般ユーザPCに管理者権限を付与しない

※脆弱性の排除・堅牢化の詳細は、【R7年度：CYNEX研修標準防御ワークショップ・実機演習コース】を受講を推奨

※OSを最新にできない機器は、【R7年度：医療機器の安全確保コース】を受講またはe-Learningで

バックアップ・参照系システムの適切な運用

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

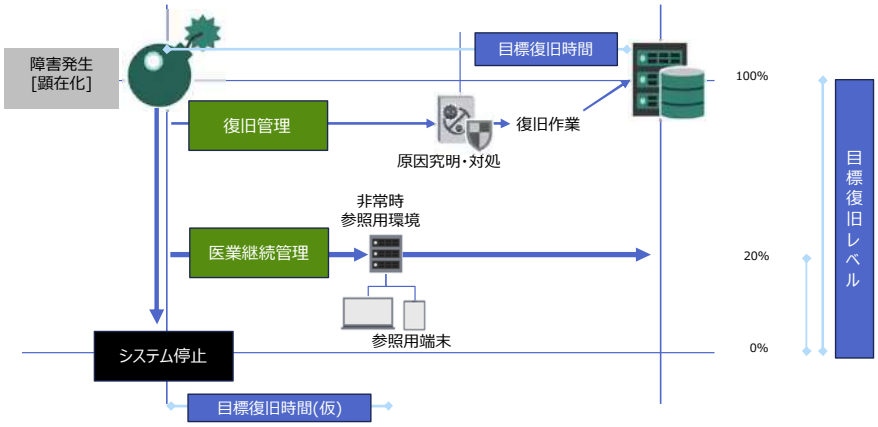
短縮

適切な「目標復旧時間」(RTO)を設定する

（RTO: Recovery Time Objective）

・医業制限による減益や診療報酬請求遅延の可能性を想定し、自組織の経営状況に適したRTOを検討する。

・医業制限の拡張を早めるため、カルテ情報参照に特化したシステム環境を早期に用意するなどの対策も有用



RTOを定める際のボトルネック

・原因究明：復旧方針を決定づけるためおろそかにできない。

・復旧作業：PCの初期化やサーバー再構築台数次第。

基本的セキュリティ対策は原因究明期間や復旧作業期間を劇的に短縮する。

レジリエンス向上に向けた対策の優先順位

万が一に備え、医業制限時の安全な医業継続と医業制限期間の短縮化をめざす
～いわゆる適切なBCPの整備～

3. BCPを適切に機能させるための管理

- なんといってもBCP訓練の実施
- BCP訓練のPDCAを回す

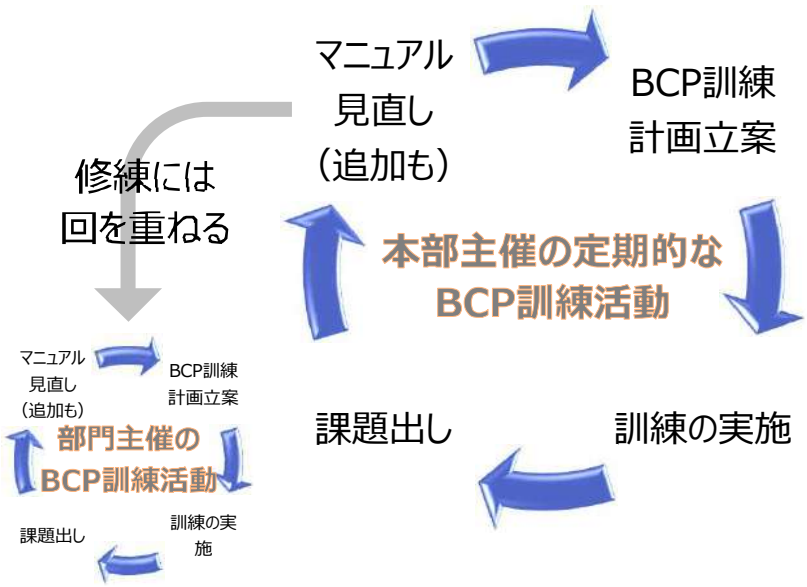
BCPを適切に機能させるには訓練しかない

[P] BCP訓練計画立案
- 最低年1回の実施（前回の反省を反映）

[D] 訓練の実施
- 院内全部門参加（部分的では不十分）

[C] 課題出し
- 必須（100点はあり得ない）
  修練を重ねれば、課題は増え、より高度に

[A] マニュアル見直し（追加も）
- マニュアルが適切かは訓練実施で確認



まとめ

1. 大規模システム障害下での安全な医業継続のための備え

- 会議体の設立：　指揮命令系統・責任と役割の明確化を前提に、多職種のシームレスな横断的対応と周知徹底
- 患者情報を把握する：フェーズ1では参照系環境ができるまでID番号がある患者をいかに把握するかが重要
- ボトルネックの把握：　どこのプロセスが律速段階にあるかを把握し、常にモニタリングしながら安全に医業を継続する
- メンタルを正常に保つ：メンタルが正常でなければ、安全に医業を継続できない

2. 基幹システム再開までの期間を短縮するための対策

- 医業制限を強いられる期間は、キャッシュフローに直接影響する
- 資産管理は情報セキュリティの一丁目一番地、サイバー攻撃の手順を知り最低限のセキュリティ対策を施す
- バックアップ運用は医業制限期間短縮の重要項目（故に、資産管理や最低限のセキュリティ対策は必須）

3. BCPを適切に機能させるための管理

- BCP訓練あるのみ
- BCP訓練のPDCAをまわして、BCPを適切に機能させる