医療情報担当者に向けての IT-BCP策定に関する 手順と注意点

日本医療情報学会
研修企画委員会

福井大学　山下芳範

2024/6

福井大学 University of Fukui

1

医療系でのセキュリティ問題

- ウイルス感染が広がって端末が利用不能
- ウイルスによる内部サーバへの攻撃
- 電子カルテのデータが乗っ取られた
  - ファイルの暗号化ロックによる使用不能
  - 身代金の要求
  - バックアップも使用不能・戻せない
- 部門システムのデータが乗っ取られた

2024/6

福井大学 University of Fukui

2

セキュリティ問題の背景

- リモートメンテナンス等外部接続の増加
  - バックドア問題
- 医療情報システムと外部との関わりの拡大
- クローズドなネットワークが安全とは言い切れない現実
- 意図しない状況からのサイバー攻撃の可能性

2024/6

福井大学 University of Fukui

3

すべき対応とは

- ガイドライン第6版にある項目
  - リスク評価とマネジメント
    - 脆弱性などの把握・報告　→　MDS/SDS、チェックリスト
  - 異常事象発生時の対応
    - システムのログの扱い
    - 事故発生時の報告・原因究明・対策
  - 事業者からの情報提供
    - 経時的に発生するリスク
  - 非常時体制とリカバリ方法の確立

2024/6

福井大学 University of Fukui

4

セキュリティ対策が
すべてではない！！

何かあったときに
どうすべきか？？
が重要

2024/6

福井大学
University of Fukui

5

6

医療情報システムの安全管理に関するガイドライン　第6.0版（令和5年5月）

概説編（Overview）

医療情報システムの安全管理に関するガイドライン 第6.0版（概説編）（令和5年5月）［1.3MB］

経営管理編（Governance）

医療情報システムの安全管理に関するガイドライン　第6.0版（経営管理編）（令和５年５月）［1.5MB］

企画管理編（Management）

医療情報システムの安全管理に関するガイドライン　第6.0版（企画管理編）（令和５年５月）［2.4MB］

システム運用編（Control）

医療情報システムの安全管理に関するガイドライン　第6.0版（システム運用編）（令和５年５月）［2.4MB］

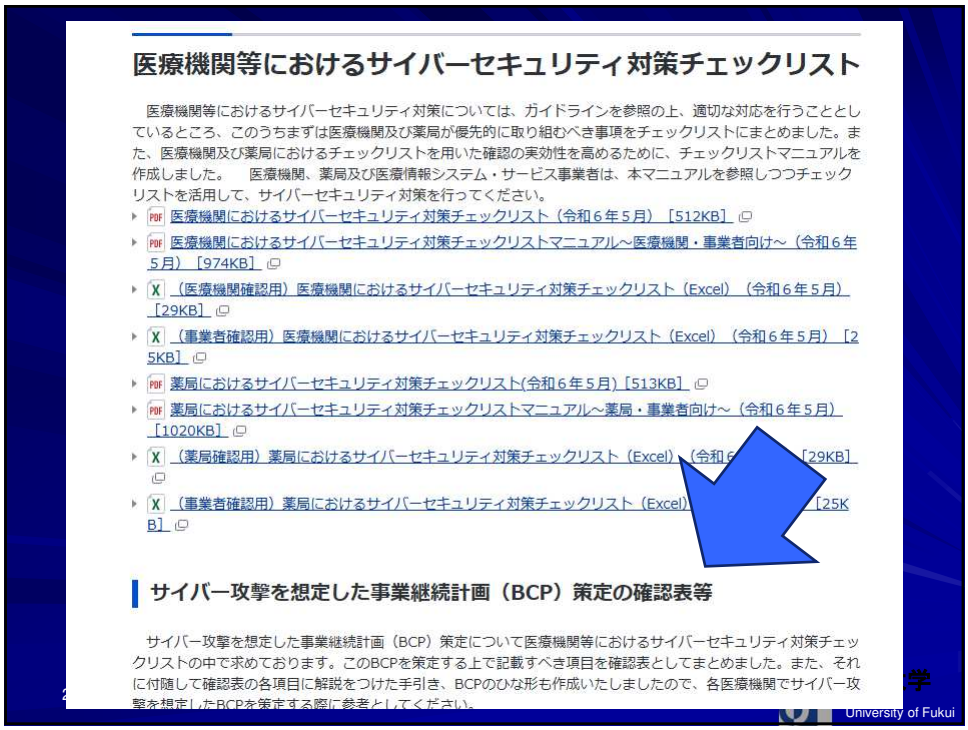
別添、特集、Q&A

別添

- 医療情報システムの安全管理に関するガイドライン　第6.0版（令和５年５月）用語集［1,464KB］［1.5MB］
- 医療情報システムの安全管理に関するガイドライン　第6.0版（令和５年５月）第5.2版→第6.0版項目移行対

大学
University of Fukui

7



医療機関等におけるサイバーセキュリティ対策チェックリスト

医療機関等におけるサイバーセキュリティ対策については、ガイドラインを参照の上、適切な対応を行うこととしているところ、このうちまずは医療機関及び薬局が優先的に取り組むべき事項をチェックリストにまとめました。また、医療機関及び薬局におけるチェックリストを用いた確認の実効性を高めるために、チェックリストマニュアルを作成しました。　医療機関、薬局及び医療情報システム・サービス事業者は、本マニュアルを参照しつつチェックリストを活用して、サイバーセキュリティ対策を行ってください。

- 医療機関におけるサイバーセキュリティ対策チェックリスト（令和６年５月）［512KB］
- 医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～（令和６年５月）［974KB］
- （医療機関確認用）医療機関におけるサイバーセキュリティ対策チェックリスト（Excel）（令和６年５月）［29KB］
- （事業者確認用）医療機関におけるサイバーセキュリティ対策チェックリスト（Excel）（令和６年５月）［25KB］
- 薬局におけるサイバーセキュリティ対策チェックリスト(令和６年５月)［513KB］
- 薬局におけるサイバーセキュリティ対策チェックリストマニュアル～薬局・事業者向け～（令和６年５月）［1020KB］
- （薬局確認用）薬局におけるサイバーセキュリティ対策チェックリスト（Excel）（令和６［29KB］
- （事業者確認用）薬局におけるサイバーセキュリティ対策チェックリスト（Excel）［25KB］

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等

サイバー攻撃を想定した事業継続計画（BCP）策定について医療機関等におけるサイバーセキュリティ対策チェックリストの中で求めております。このBCPを策定する上で記載すべき項目を確認表としてまとめました。また、それに付随して確認表の各項目に解説をつけた手引き、BCPのひな形も作成いたしましたので、各医療機関でサイバー攻撃を想定したBCPを策定する際に参考としてください。

学
University of Fukui

8

本日のセミナーはこの部分

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等

サイバー攻撃を想定した事業継続計画（BCP）策定について医療機関等におけるサイバーセキュリティ対策チェックリストの中で求めております。このBCPを策定する上で記載すべき項目を確認表としてまとめました。また、それに付随して確認表の各項目に解説をつけた手引き、BCPのひな形も作成いたしましたので、各医療機関でサイバー攻撃を想定したBCPを策定する際に参考としてください。

- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（PDF）（令和６年６月）［448KB］
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表（Excel）（令和６年６月）［33KB］
- 【医療機関用】サイバー攻撃を想定したBCP策定の確認表のための手引き（令和６年６月）［790KB］
- 医療情報システム部門等におけるBCPのひな形（PDF）（令和６年６月）［1.2MB］
- 医療情報システム部門等におけるBCPのひな形（Word）（令和６年６月）［418KB］

2024/6

福井大学 University of Fukui

9

気になる部分

～立入検査時、チェックリストを確認します～

医療法に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

令和 5 年度は、「医療機関確認用」、「事業者確認用」の全ての項目について、１回目の確認の日付と回答等が記入されていることを確認します（※）。このうち、３（１）の連絡体制図は現物を確認しますので、立入検査までに作成してください。

参考項目は令和５年度の立入検査では確認しません。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関は事業者からチェックリストを回収しておきましょう。

（※） 事業者と契約していない場合には、「医療機関確認用」２（２）及び２（３）についての確認は求められません。

2024/6

福井大学 University of Fukui

10

法令改定によって医療機関に求められている情報収集

・医療機関のチェックシートの作成
・ベンダー（事業者）のチェックシートの収集
・ベンダー（事業者）からのシステムのMDS/SDSの収集

2024/6

福井大学 University of Fukui

11

「製造業者による医療情報セキュリティ開示書」チェックリスト

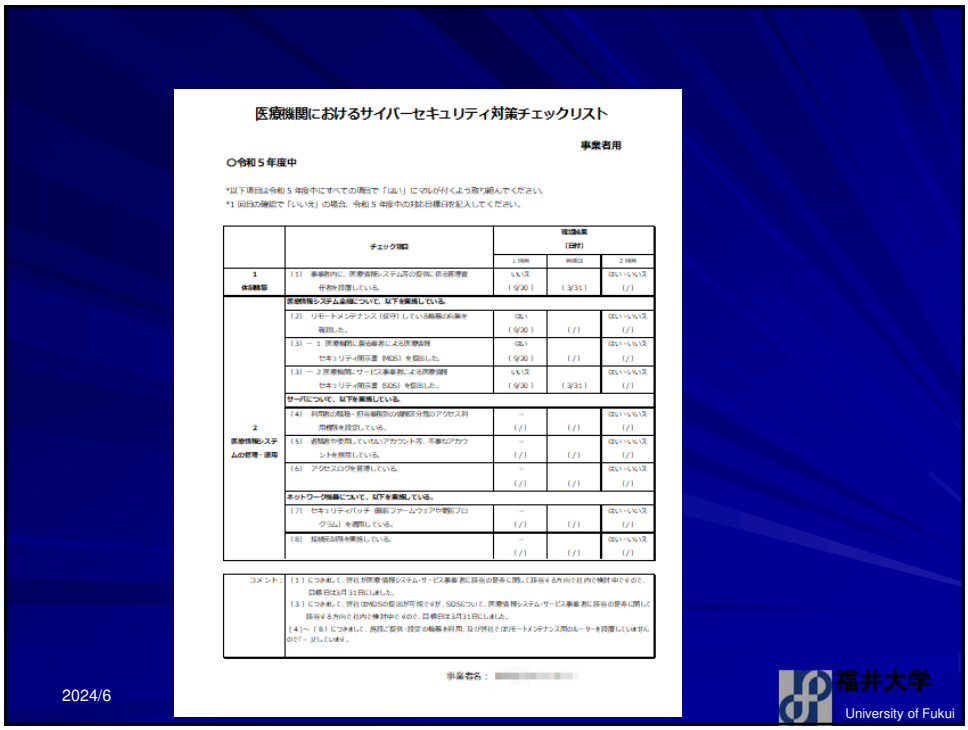
（医療情報システムの安全管理に関するガイドライン第 5.2 版対応）

製造業者　：	作成日　：			
製品名称　：	バージョン　：			
医療機関等における情報セキュリティマネジメントシステムの実践(6.2)				
1　扱う情報のリストを医療機関等に提示できるか？(6.2.C1)	はい	いいえ	対象外	備考＿＿
物理的安全対策(6.4)				
2　個人情報が入力・参照できる端末の覗き見防止の機能があるか？(6.4.C5)	はい	いいえ	対象外	備考＿＿
技術的安全対策(6.5)				
3　離席時の不正入力防止の機能があるか？(6.5.C4)	はい	いいえ	対象外	備考＿＿
4　アクセス管理の機能があるか？(6.5.C1)	はい	いいえ	対象外	備考＿＿
4．1　利用者の認証方式は？(6.5.C1、6.5.C13)				
・記憶（ID・パスワード等）	はい	いいえ	対象外	備考＿＿
・生体認証（指紋等）	はい	いいえ	対象外	備考＿＿
・物理媒体（IC カード等）	はい	いいえ	対象外	備考＿＿
・上記のうちの二要素を組み合わせた認証	はい	いいえ	対象外	備考＿＿
（具体的な組み合わせを備考に記入してください）				
・その他（具体的な認証方式を備考に記入してください）	はい	いいえ	対象外	備考＿＿
4．1．1　パスワードを利用者認証手段として利用している場合、パスワード管理は可能か？(6.5.C14)	はい	いいえ	対象外	備考＿＿
4．1．2　セキュリティ・デバイスを用いる場合に破損等で本人の識別情報が利用できない際の代替機能があるか？(6.5.C3)	はい	いいえ	対象外	備考＿＿
4．2　利用者の職種・担当業務別の情報区分ごとのアクセス管理機能があるか？(6.5.C6)	はい	いいえ	対象外	備考＿＿
4．3　アクセス記録（アクセスログ）機能があるか？(6.5.C7)	はい	いいえ	対象外	備考＿＿
4．3．1　アクセスログを利用者が確認する機能があるか？(6.5.C7)	はい	いいえ	対象外	備考＿＿

2024/6

福井大学 University of Fukui

12



13

医療情報部門・医療情報担当者が担うべきセキュリティ対応

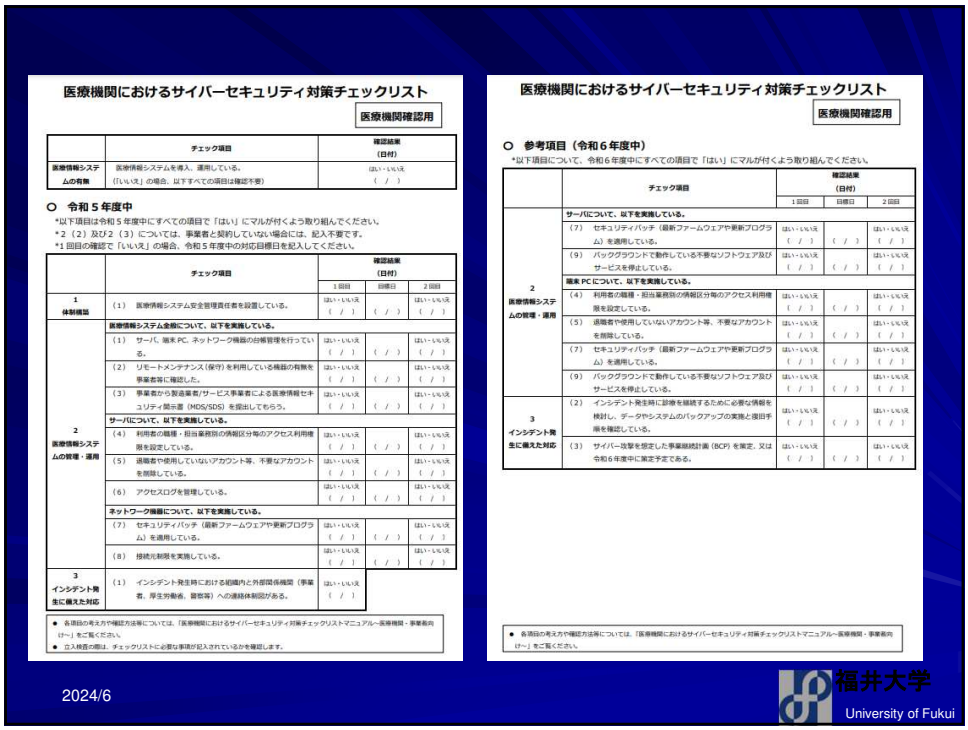
- チェックシートだけで大丈夫か？
- MDS/SDSをもらうだけで大丈夫？

- セキュリティの本質的対応が必要
- この機会に経営層の理解ももらって対応強化

2024/6

福井大学
University of Fukui

14



医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

	チェック項目	確認結果（日付）
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）

○ 令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
1 体制構築	（1） 医療情報システム安全管理責任者を設置している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（1） サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（2） リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（3） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	サーバについて、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（6） アクセスログを管理している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	ネットワーク機器について、以下を実施している。			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（8） 接続元制限を実施している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
3 インシデント発生に備えた対応	（1） インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（　/　）		

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。
● 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

医療機関におけるサイバーセキュリティ対策チェックリスト

医療機関確認用

○ 参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	端末 PC について、以下を実施している。			
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
3 インシデント発生に備えた対応	（2） インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）
	（3） サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）

● 各項目の考え方や確認方法等については、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」をご覧ください。

2024/6

福井大学 University of Fukui

15

どのように対応？？

- 院内におけるセキュリティのリスクを考える
  - ベンダー側の情報提供が重要！！
- どうしても、リスク評価は100%とはならない
  - 考えうる対策はするが、「お守り」という認識で
  - 継続的な情報提供をどうするか？
- 何かが起こる前提で考える
  - 起こった時の対応を考慮する
  - そのためにも、弱点を知ることが重要
    - 継続的なフォローも必要となる
  - 万一の時の対応手段を考慮する

2024/6

福井大学 University of Fukui

16

なぜバックアップか？

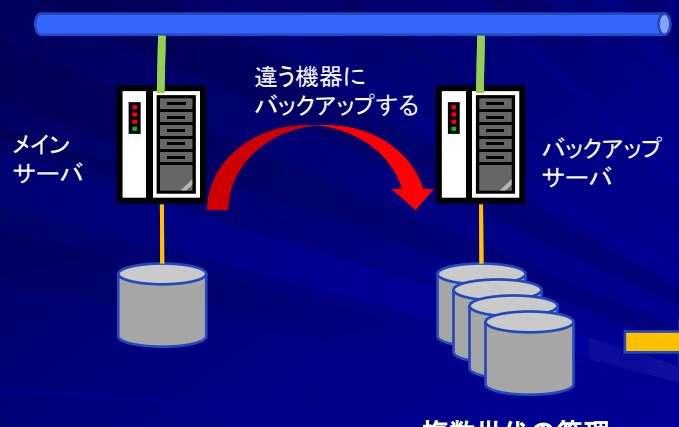
- 元に戻す唯一の方策
  - 滅多になくてもやはり必要
- ランサムウエアやウイルス対策だけでなく、システムのBCP対応としても重要
  - サイバー攻撃のためだけではない
  - 災害等非常時対応として考える

2024/6

福井大学 University of Fukui

17

バックアップに求められるもの



2024/6

福井大学 University of Fukui

18

なぜIT-BCP？？

- 何かが起こる
- リスク評価は多彩
  - サイバーセキュリティだけではない
  - 故障・災害などもリスクの1つ
- どのように継続するのか？？
  - サイバー攻撃でも運用継続ができないことが課題

2024/6

福井大学 University of Fukui

19

非常時の対応として

- サイバー攻撃を含む重大障害対応
  - もちろん災害や故障も含む
- BCPとしての対応として考える

2024/6

福井大学 University of Fukui

20

端末や機器のリスト化

機器の把握も求められる

端末名	申請者	OS	支払区分	機器名	MACアドレス	IP アドレス	登録情報コンセント番号	初
fhej0002	山下 芳範	Windows 11	病院負担	MS surface	00:d4:9e:3c:3f:d9	172.30.101.4		202
fhej2004	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:73	172.30.103.4		202
fhej2005	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:14	172.30.103.5		202
fhej2006	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:39:62	172.30.103.6		202
fhej2007	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:0f	172.30.103.7		202
fhej2008	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:25:99:96	172.30.103.8		202
fhej2009	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:39:21	172.30.103.9		202
fhej2010	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:08:66	172.30.103.10		202
fhej2011	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:0d:7a	172.30.103.11		202
fhej2012	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:78:e6	172.30.103.12		202
fhej2013	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:38:ef	172.30.103.13		202
fhej2014	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:32:e1	172.30.103.14		202
fhej2015	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:19:1e	172.30.103.15		202
fhej2016	山下 芳範	Windows 10	病院負担	IIYAMA NJ50PU	a0:29:42:23:66:1c	172.30.103.16		202

病院内機器の把握
ネットワーク上のリスク把握

2024/6

福井大学 University of Fukui

21

機器一覧に合わせての確認用シート

情報機器管理表　　部局名：

PC名	IPアドレス	所有者	OS	OSのバージョン	機密性	完全性	ウイルス対策の有無	OS等の脆弱性対策	機密性Aの場合：安全区域設定	機密性Aの場合：取り扱い情報の管理状態
ABC	123.234.345.1	○○	Win	10	A3	A	○	○	○	○
CDE	123.234.345.2	○○	Mac	10.15	A1	A	○	○	○	○
FGH	123.234.345.3	○○	Win	8	B	B	○	○		
PQR	123.234.345.4	○○	Win	10	B	B	○	○		

2024/6

福井大学 University of Fukui

22

どのようなリスクがあるか考えてもらうための一覧

リスク評価票（例）

脅威	意図的な要因	偶発的な要因	環境的な要因
地震			○
洪水	○	○	○
台風			○
落雷			○
争議行動	○	○	
爆破行為	○	○	
武器の使用	○	○	
火事	○	○	
故意の損害	○		
停電		○	
断水		○	
空調故障	○	○	
ハードウェアの故障		○	
電力の不安定		○	○
極端な温度および湿気	○	○	○
ほこり			○
電磁波放射	○	○	○
静電荷			○
盗難	○		
記憶媒体の不正使用	○		
記憶媒体の劣化			○
操作員のエラー	○	○	

福井大学 University of Fukui

23

機器管理票（例）

システム名	具体的なシステム名称など
利用目的	システムの利用目的を具体的に記入する
利用内容	システムの利用を行う内容などを記入する
利用範囲	システムの利用者などの範囲を記入する
設置部署	システムを設置する部署名を記入する
管理者	システムの管理者
システムの格付け	機密性：A・B・C　完全性：A・B　可用性：A・B
保有データ量	機密性 A 及び B、完全性 A のシステムが保有するであろうデータの件数及び記録容量を記載する。
外部記録媒体	
バックアップ	バックアップの具体的な方法及び使用する媒体を記入する。
○S	○Sの名称（バージョンを含む）を記載する。
設置場所	具体的な設置場所を記入する。
システム構成	• 複数からなる場合は、システム構成図は別紙とする
ネットワーク接続	• 施設内のネットワーク利用方法 • インターネット接続の有無
外部と情報交換の有無と相手先	外部の施設、機関、事業者等と情報交換をする場合の状況を記入する。

福井大学 University of Fukui

24

最低限の切り分け項目

1 機器の障害

確認すべき事項： 障害範囲の特定
対応すべき事項： 障害機器の交換
大規模影響の場合には、非常時運用への切り替え

2 サイバー攻撃

確認すべき事項： サイバー攻撃の有無及び特定
対応すべき事項： ネットワークの切り離し
広範囲影響の場合には、非常時運用への切り替え

3 電源喪失

確認すべき事項： 電源状況の確認と復旧までの時間
対応すべき事項： 医療情報系電源での運用
長時間の場合には、非常時運用への切り替え

4 災害等

確認すべき事項： 被害状況の確認と運用復旧の可否
対応すべき事項： バックアップセンターでの運用
オフライン PC の配布
被害甚大の場合には、非常時運用への切り替え

福井大学 University of Fukui

25

全体の流れの把握

1 障害状況の把握と対応

機器固有・限定的 → L1 個別対応
局所的 → L2 個別対応
広範囲だが特定機能 → L3 機能担当機器・SV の個別対応
広範囲影響（運用影響大） → L4 重大対応手順で対応
広範囲影響且つ重大障害 → L5 重大対応手順で対応

※参照マニュアル

○サーバ管理運用マニュアル
○HIS 端末管理運用マニュアル
○ネットワーク管理運用マニュアル
○操作手順書（システム）

○電子カルテシステム障害発生時 紙カルテ・伝票 のバイン

2 サイバー攻撃が疑われる場合

サイバー攻撃の有無確認
拡散がない場合 → 個別対応
拡散が疑われる場合 → L4 重大対応手順で対応
障害に発展した場合 → L5 重大対応手順で対応

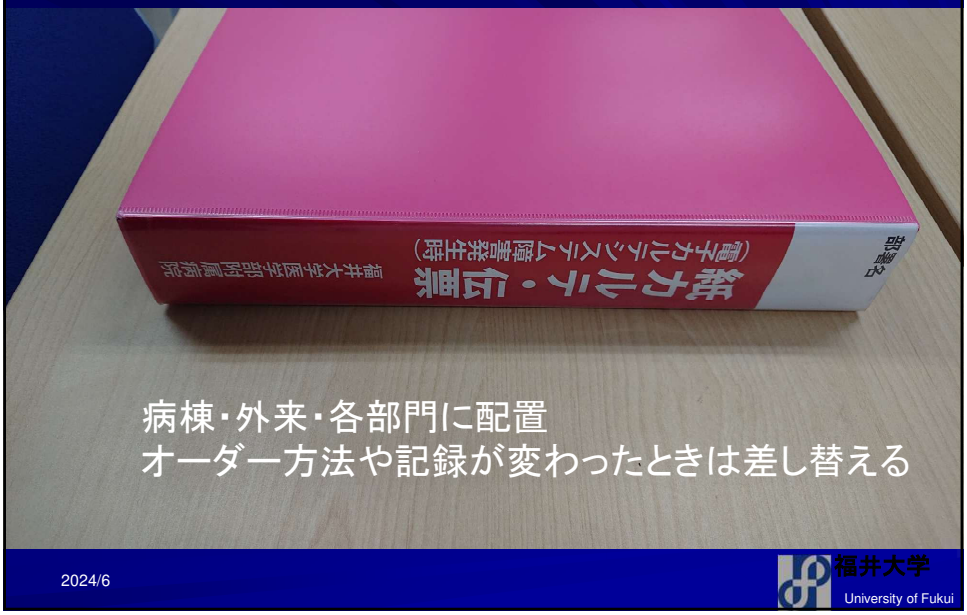
3 災害等での運用影響の場合

病院被害が軽微でも継続不能 → 緊急用PC，バックアップセンター運用に切り替え

福井大学 University of Fukui

26

電子カルテシステム障害発生時用の紙媒体セット

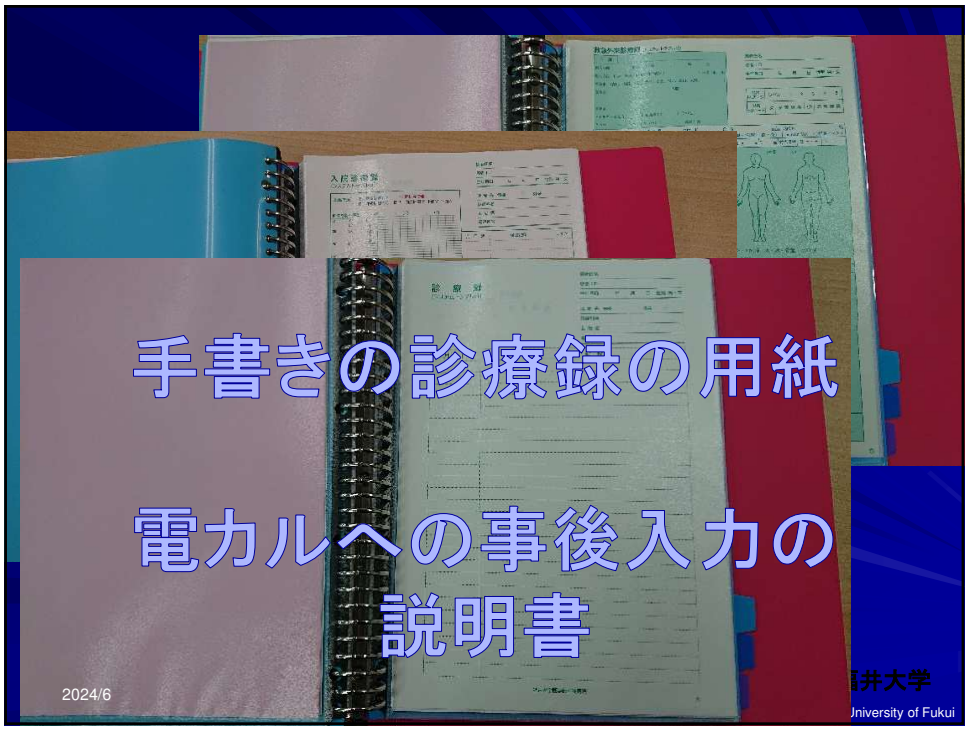


病棟・外来・各部門に配置
オーダー方法や記録が変わったときは差し替える

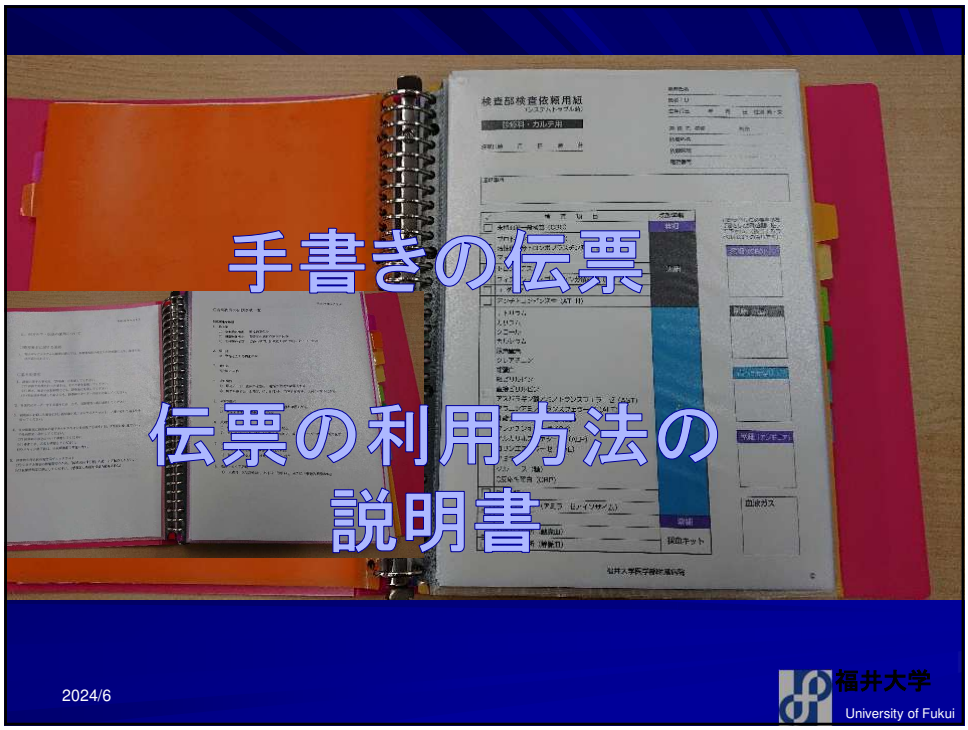
2024/6

福井大学
University of Fukui

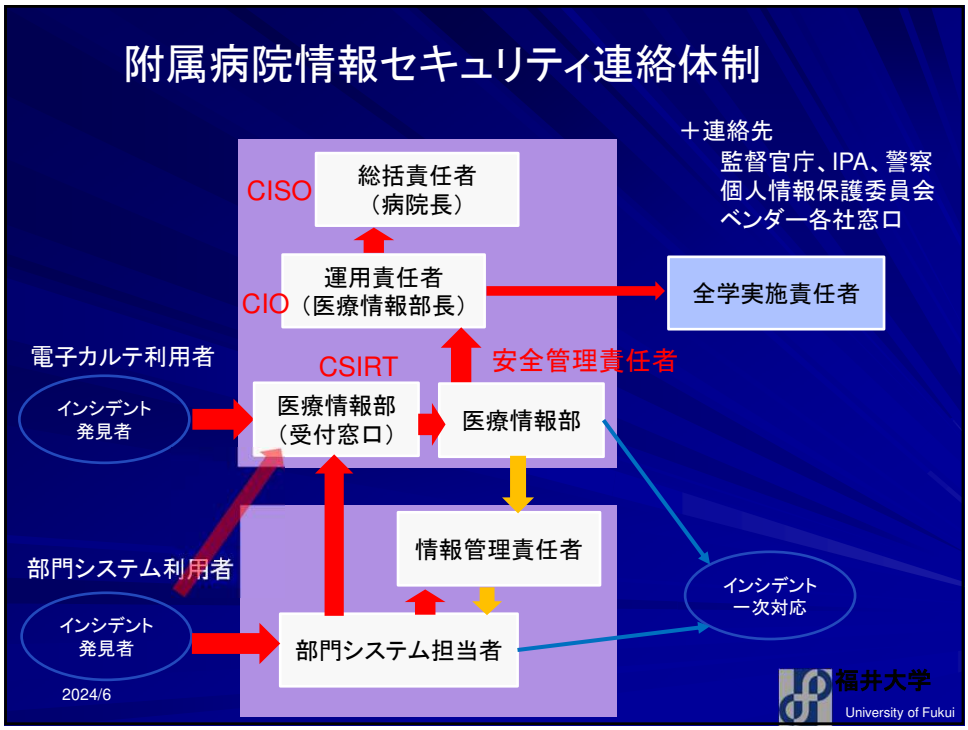
27



28

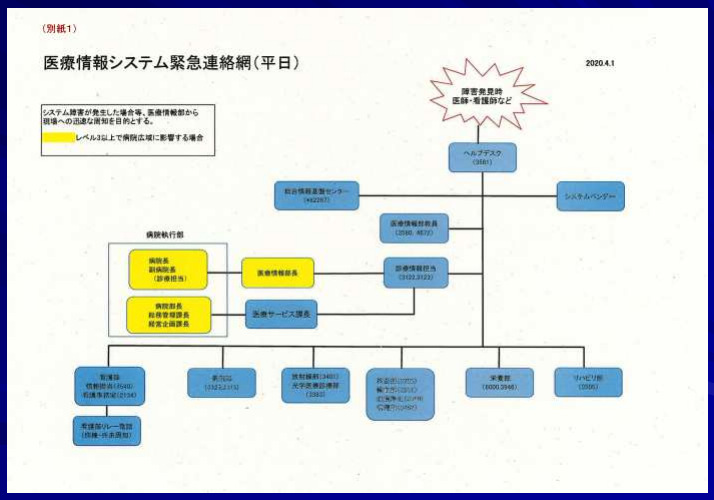

手書きの伝票
伝票の利用方法の
説明書
2024/6
福井大学
University of Fukui

29


附属病院情報セキュリティ連絡体制
＋連絡先
監督官庁、IPA、警察
個人情報保護委員会
ベンダー各社窓口
CISO
総括責任者
（病院長）
CIO
運用責任者
（医療情報部長）
全学実施責任者
電子カルテ利用者
CSIRT
安全管理責任者
インシデント
発見者
医療情報部
（受付窓口）
医療情報部
情報管理責任者
部門システム利用者
インシデント
発見者
部門システム担当者
インシデント
一次対応
2024/6
福井大学
University of Fukui

30

実際の連絡体制



2024/6

福井大学 University of Fukui

31

レベル4:ネットワーク等含む全域障害
レベル5:電子カルテ系大規模（ハード等）障害

障害発生

対応

部門システム障害連絡は
対策本部３１２３へ

30分以内(目標10分以内)
①IPメッセージ(1)(障害告知:医療情報部教員)
②連絡網(ヘルプデスク)
③院内放送(1)(障害告知:医療サービス課)

★医療情報部教員１名は、執行部（医療サービス課長）に対して15分毎に進捗報告を行う。

CIS(参照)が使用可能であれば周知する。

60分以内

復旧可能性

60分以内(目標10分以内)
①IPメッセージ(2)(状況報告:医療情報部教員)
②状況分析(診療情報担当＆ベンダー)→医療サービス課長→
総務管理課長→執行部へ連絡(60分以内は紙運用を避ける)
③院内放送(2)(医療サービス課)

60分以上

紙運用決定

①重大障害・紙運用判断(執行部) ＊新患は仮ID発行(8888001～)
②障害告知: IPメッセージ(3)(紙運用:医療情報部教員)
③院内放送(3)(医療サービス課)
④対策本部設置(診療情報担当3123)
復旧本部設置(医療情報演習室3580:復旧作業が必要な場合)

参照系復旧

①IPメッセージ(4)(参照系復旧通知:医療情報部教員)
②院内放送(4)(医療サービス課)

復旧案内

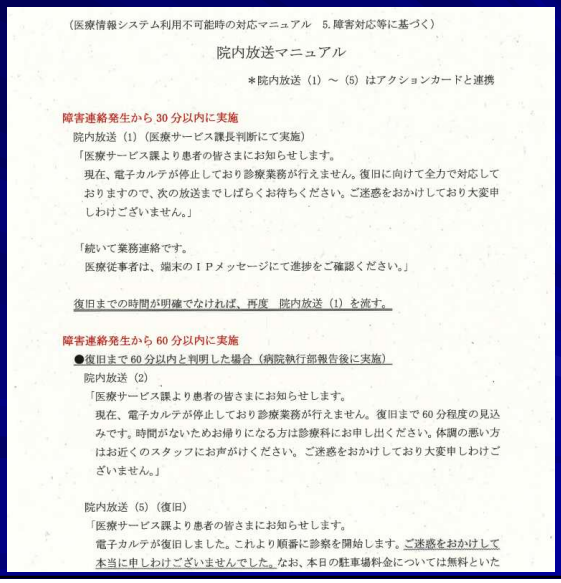
①IPメッセージ(5)(復旧通知:医療情報部教員)
②院内放送(5)(医療サービス課)

2024/6

福井大学 University of Fukui

32

非常時の院内放送マニュアル



（医療情報システム利用不可能時の対応マニュアル　5.障害対応等に基づく）

院内放送マニュアル

＊院内放送（1）～（5）はアクションカードと連携

障害連絡発生から 30 分以内に実施

院内放送（1）（医療サービス課長判断にて実施）

「医療サービス課より患者の皆さまにお知らせします。
現在、電子カルテが停止しており診療業務が行えません。復旧に向けて全力で対応しておりますので、次の放送までしばらくお待ちください。ご迷惑をおかけしており大変申しわけございません。」

「続いて業務連絡です。
医療従事者は、端末のＩＰメッセージにて進捗をご確認ください。」

復旧までの時間が明確でなければ、再度　院内放送（1）を流す。

障害連絡発生から 60 分以内に実施

●復旧まで 60 分以内と判明した場合（病院執行部報告後に実施）

院内放送（2）

「医療サービス課より患者の皆さまにお知らせします。
現在、電子カルテが停止しており診療業務が行えません。復旧まで 60 分程度の見込みです。時間がないためお帰りになる方は診療科にお申し出ください。体調の悪い方はお近くのスタッフにお声がけください。ご迷惑をおかけしており大変申しわけございません。」

院内放送（5）（復旧）

「医療サービス課より患者の皆さまにお知らせします。
電子カルテが復旧しました。これより順番に診察を開始します。ご迷惑をおかけして本当に申しわけございませんでした。なお、本日の駐車場料金については無料といた

33

その他の欄の活用

- 項目は、ガイドラインの項目の対応のみ
- 脆弱性としての認知ができない
  - 考慮すべきリスクの記載を求める
  - 責任範囲を明確にする

→ 責任分界点

↓

契約内容での確認
例：範囲・非常時

34

御清聴ありがとうございました。

2024/6

福井大学
University of Fukui

35