

病院情報システム運用継続計画 (IT-BCP)

令和6年3月策定

令和7年10月改定（第1.3版）

徳島大学病院

目 次

1. 本計画の目的と基本方針
 1. 1. 本計画の策定趣旨
 1. 2. 基本方針
 1. 3. 本計画の適用範囲
 1. 4. 病院情報システム運用継続計画の策定・運用推進体制
 1. 5. 病院情報システム運用継続計画の発効、改訂
2. 重大情報セキュリティインシデント発生時の対応計画
 2. 1. 重大情報セキュリティインシデント発生時の基本方針
 2. 1. 1. 対象事象
 2. 1. 2. 参集要員
 2. 1. 3. 参集基準
 2. 1. 4. 参集場所
 2. 2. 重大情報セキュリティインシデント発生時の対応体制
 2. 2. 1. 対応体制・指揮命令系統図
 2. 2. 2. 関係部局・関係企業連絡先一覧
 2. 3. 重大情報セキュリティインシデント発生時における対応手順
 2. 3. 1. 全体フロー
 2. 3. 2. 対応手順
3. 事前対策計画
 3. 1. 病院情報システムを支える構成要素ごとの現状対策レベルとリスク
 3. 2. 事前対策の実施計画
4. 教育訓練計画・維持改善計画
 4. 1. 教育訓練計画
 4. 2. 維持改善計画
 4. 2. 1. 計画の実施に伴う維持改善
 4. 2. 2. 危機的事象の発生に伴う維持改善
 4. 2. 3. 定期的な見直しによる維持改善
5. 計画策定の根拠とした調査・分析・検討
 5. 1. 想定する危機的事象
 5. 2. 想定する被害状況
 5. 3. 病院情報システムの復旧優先度の設定
 5. 4. 病院情報システムを支える構成要素の関連整理
 5. 4. 1. 病院情報システムを支える構成要素の整理
 5. 4. 2. 病院情報システムを支える構成要素ごとの目標対策レベルの設定

6. 事後対応

6.1 報告

6.2 再発防止

6.2.1 再発防止策検討・策定

6.2.2 事業者への指示

6.3 情報公開

【別冊①】サイバー攻撃等によるシステム停止時の対応について

【別冊②】初動対応時の想定対応手順

1. 本計画の目的と基本方針

1.1. 本計画の策定趣旨

昨今、ランサムウェアによるサイバー攻撃は増加傾向にあり、政府機関やインフラ企業のほか、医療機関も攻撃のターゲットになっている。2021年10月には徳島県のとつぎ町立半田病院が、2022年10月には大阪急性期・総合医療センターが相次いで被害にあい、約2カ月間の診療停止に追い込まれた。その間、手術や検査を含めた診療行為が停止したことにより、地域医療の提供に大きな影響を及ぼしただけでなく、病院収入の落ち込みやシステム復旧にかかる経費など、病院経営にも多大な損失を計上した。

サイバー攻撃の対象が国立大学病院になった場合、損害額は1病院あたり少なくとも25億円以上と試算され、損害保険による補償内容も十分とは言えない状況にある。そんななか、サイバー攻撃を受けた際の復旧速度がカギとなっており、早く復旧できれば損失を最小限に食い止めることができる。

そこで、国立大学病院の大規模な病院情報システムに対応した事業継続計画（IT-BCP）を策定し、万一サイバー攻撃を受けた場合でも速やかな復旧を実現するための指針としたい。策定にあたっては、内閣官房内閣サイバーセキュリティセンターが発行する「政府機関等における情報システム運用継続計画ガイドライン（第3版）」を基本とし、発災時にはとつぎ町立半田病院及び大阪急性期・総合医療センターで発生した情報セキュリティインシデントにかかる調査報告書に記載されている初動対応やシステム復旧プロセスも参考に対応を行う。

1.2. 基本方針

病院情報システム運用継続計画

サイバー攻撃等による重大情報セキュリティインシデント発生時において、病院機能の継続及び病院情報システムの迅速な復旧を図るため、病院情報システム運用継続計画の策定と運用に取り組む。

基本方針

- (1) 重大な情報セキュリティインシデント発生時においても医療安全確保を最優先し、病院情報システムが作動しない場合等においても、最善の方法を柔軟に選択し、他の医療機関等とも連携し継続した医療提供を行う。
- (2) 病院機能の継続及び病院情報システムの復旧を脅かすリスクを評価し、適切な対策を実施する。
- (3) 重大情報セキュリティインシデント発生時に備え、病院機能の継続及び病院情報システムの復旧のための計画と手段を事前に整備する。
- (4) 本計画と徳島大学病院事業継続計画(BCP)の整合性を確保する。

1. 3. 本計画の適用範囲

本計画の適用範囲は、本院各部門が運用管理する病院情報システムとする。

上記以外の情報システムは本計画の対象範囲には含まないが、病院情報システム運用責任者（病院長）及び病院情報システム管理者（病院情報センター部長）は、今後、危機的事象発生時における優先度を考慮し、定期的に対象範囲の見直しを行う。

上記各システムの詳細は、「表 3. 1 病院情報システムの構成要素ごとの現状対策レベルとリスク」に示す通り。

1. 4. 病院情報システム運用継続計画の策定・運用推進体制

本院における病院情報システム運用継続計画は、病院情報システム運用責任者のもと策定し、対象システムを踏まえて病院情報システム運用継続計画推進体制を構築し、実施する。本院における病院情報システム運用継続計画推進体制、担当部署及び担当者、推進上の役割を以下に記す。

表 1. 4-1 本院における病院情報システム運用継続計画推進体制上の
担当部署及び担当者、推進上の役割

担当	所属・役職	役割の概要
病院情報システム 運用責任者	病院長	・病院情報システム運用継続計画の 策定・運用全般を統括し、最終的 な責任を負う。
病院情報システム 管理者	病院情報センター部長	・所管する病院情報システム運用継 続計画の策定・運用を統括する。
病院情報システム 運用担当者	病院情報センター副部長	・所管する病院情報システム運用継 続計画策定に関する各種検討作業を 行う。
中央診療部門等	看護部 医療技術部 放射線部 薬剤部 栄養部 等	・所管する病院情報システム運用継 続計画策定に関する各種検討作業を 行う。
病院事務部	事務部長 病院総務課長	・所管する病院情報システム運用継 続計画策定に関する各種検討作業を 行う。

表 1. 4-2 関連部局及び委託先等における情報システム運用継続計画推進体制上の
担当部署及び担当者、推進上の役割

区分	部署、役職	役割の概要
施設企画管理連携室	施設企画管理連携室長	・施設の電源供給状況・自家発電装置の設置状況に関する情報提供・対策調整
委託先	日本電気株式会社医療ソリューション統括部	・運用保守及び緊急時の状況に関する情報提供・対策調整

本体制は、本計画の病院情報システムの対象範囲を踏まえた体制であり、対象範囲が変更された場合は、適宜見直しを行う。

1. 5. 病院情報システム運用継続計画の発効、改訂

本院における病院情報システム運用継続計画の発効、改訂については、病院情報システム専門委員会で検討し、病院運営会議の承認を得るものとする。

2. 重大情報セキュリティインシデント発生時の対応計画

2. 1. 重大情報セキュリティインシデント発生時の基本方針

2. 1. 1. 対象事象

本書における重大情報セキュリティインシデント発生時の対応計画は、以下の事象を対象とする。

- ・サイバー攻撃等による情報セキュリティ重大インシデント発生時
(本院「病院情報システム障害時対応マニュアル」の障害時レベル別対応のレベル4に相当する場合)

2. 1. 2. 参集要員

重大情報セキュリティインシデント発生時の病院情報システムの運用継続に係る参集要員を以下のとおり定める。

表 2. 1-1 本院における重大情報セキュリティインシデント発生時の
情報システム運用継続体制

担当	所属・役職	役割の概要
病院情報システム 運用責任者	病院長	・対策本部（障害時対策検討会議）の招集及び参画を行う。 ・病院情報システム運用継続計画の発動に係る意思決定を行う。

病院執行部 障害時対策検討会議 メンバー	病院執行部 障害時対策検討会議メン バー	・対策本部（障害時対策検討会議）への参画及び報告を行う。 ・病院情報システム運用継続計画の発動に伴う対応方針の検討及び報告
病院情報システム 管理者	病院情報センター部長	・対策本部（障害時対策検討会議）への参画及び報告を行う。 ・病院情報システム運用継続計画の発動に伴う対応方針の検討及び報告
病院情報システムの インシデント 対応担当者	病院情報センター教職員 医療情報システム管理係 各部署障害時対策員	・報告管理、監視、分析の対応を行う。 ・被害の最小化、原因解析、再発防止等の対応を行う。 ・各組織との情報共有を行う。
病院情報システム運 用継続計画の発動に 伴う作業を実施する 責任者	病院総務課長	・病院情報システム運用継続方針を検討する。 ・病院情報システム復旧完了を利用者に通知する。 ・全学 CSIRT と連携する。
病院情報システムの 運用を継続する事務 局（情報システムの運 用を継続する担当者）	病院情報センター教職員 医療情報システム管理係	・被害状況又は情報システム復旧状況を取りまとめ関係者へ情報伝達する。 ・情報システムの運用を継続する責任者を支援する。
病院情報システム運 用継続計画の発動に 伴う作業を実施する 担当者	病院事務部各課職員	・情報システムの被害状況確認と、事務局への報告を行う。 ・被害拡大防止措置の実施、必要備品等の持ち出しを行う。 ・業務継続に必要な物資等を調達する。 ・復旧計画に必要な機器等を調達する。 ・手書き伝票類等の消耗品の在庫を確保する。
委託先	日本電気株式会社医療ソ リューション統括部	・SLA に基づいた復旧作業 ・担当者の支援、復旧状況報告

2.1.3. 参集基準

初動対応を実施するための参集基準を以下のとおり定める。なお、本書における参集は、参集場所への現地参集及びオンライン（電話会議、Web 会議等）への参集の両方の意味を含む。

重大情報セキュリティインシデント発生時

- ・病院情報システムによる検知や通報・発見等で、病院情報センター部長又は関係者に病院情報システムの停止等が認知され、病院長が病院情報システム運用継続計画を発動した場合、病院総務課長の指示のもと、重大情報セキュリティインシデント発生時の情報システム運用継続体制に記された要員が参集し、初動対応を開始するものとする。

2.1.4. 参集場所

参集場所を以下のとおり定める。病院総務課長から別に指示がある場合は、その指示に従う。

表 2.1-2 参集要員及び参集場所

参集要員	参集場所
重大情報セキュリティインシデント発生時の情報システム運用継続体制に記された要員	外来診療棟 5 階 日亜ホール White
病院情報センターの復旧担当者	中央診療棟 5 階 病院情報センタープロジェクト室
委託先の復旧担当者	中央診療棟 5 階 病院情報センター研修室
障害時対策員	各部署

参集場所は現地での参集、オンラインのいずれか適切な方法を選択する。上記参集場所が人命の安全や本部（障害時対策検討会議）機能の遂行の上で不適切と判断される場合、病院情報システムの継続と関連組織との情報共有のしやすさを踏まえ、病院総務課長が適切な場所を判断し参集を指示するものとする。

また、重大情報セキュリティインシデント発生時の初期段階で必要となる行動と連絡先は、「スタッフマニュアル」に記載する。

2.2. 重大情報セキュリティインシデント発生時の対応体制

2.2.1. 対応体制・指揮命令系統図

情報システムの継続及び復旧を目的とした重大情報セキュリティインシデント発生時の体制を以下のとおり定める。重大情報セキュリティインシデント発生時は通常の連絡手段が不通となる場合も考慮し、メールやWeb、SNS等の手段を想定する。

図 2.2-1 重大情報セキュリティインシデント発生時の体制

障害時対策検討会議メンバー		障害時対策員	
役職・部署		部署	役職
病院長		歯科	歯科カルテシステム管理者
副病院長(総務担当)		看護部	副看護部長
副病院長(診療担当)		手術部	手術部副部長
副病院長(歯科担当)		薬剤部	薬剤部副部長
副病院長(看護担当)・看護部長		放射線部	放射線診断科 読影・レポートシステム担当
病院長補佐(救急・災害・メディカル・IT担当)・救急集中治療部長			放射線治療科 放射線治療システム担当
病院長補佐(医療DX担当)・病院情報センター部長			放射線技術部門 放射線情報システム担当
病院長補佐(医薬品安全管理・研究支援担当)・薬剤部長		検査部	臨床検査技師 検体検査システム担当
病院長補佐(医療支援担当)・医療技術部長			臨床検査技師 細菌検査システム担当
			臨床検査技師 生理検査システム担当
病院長補佐(事務担当)・事務部長		輸血部	臨床検査技師 輸血部門システム担当
総務課長		病理部	臨床検査技師 病理部門システム担当
医事課長		栄養部	副栄養部長
経営企画課長			栄養管理部門長
経営企画課医療情報システム管理係長		医事課	副課長(報酬)
* 不在の場合は、副部長、副課長などの代理者			副課長(サービス)

徳島大学病院におけるサイバーインシデント発生時の連絡体制図

2024.12.1 更新

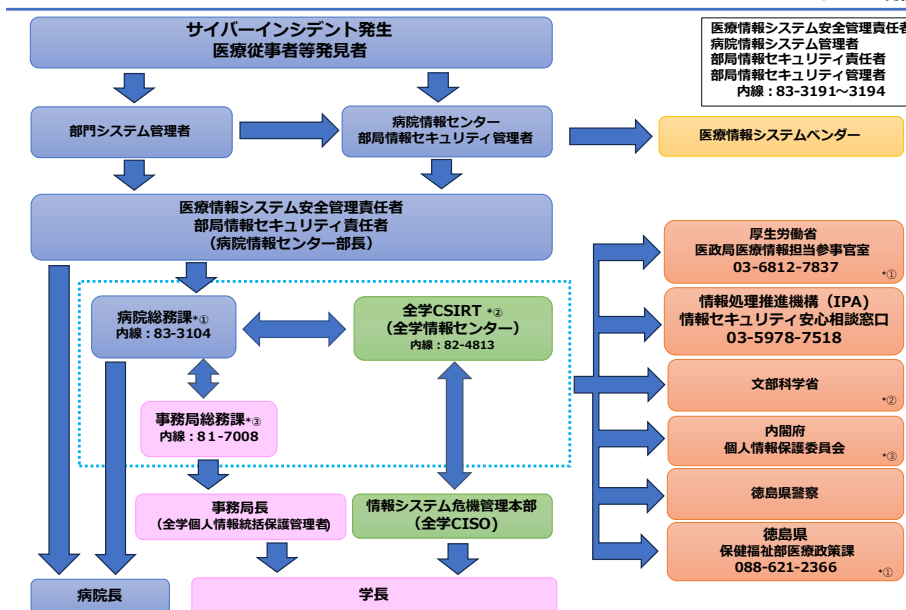


表 2.2-1 関係部署における連絡先

部署名	責任者 担当者	電話	携帯電話	メール
病院情報センター	若田 好史	(3194)	070-6586-0043	wakata@tokushima-u.ac.jp
総務課	兒玉 実和	(3102)	070-6586-0003	bsoumuka@tokushima-u.ac.jp
経営企画課	中野 栄司	(3131)	070-6586-0006	bkeieikacho@tokushima-u.ac.jp
経理調達課	原井 由美	(3130)	070-6586-0005	bchoutatsukacho@tokushima-u.ac.jp
医事課	安部 修司	(3170)	070-6586-0010	bikkachou@tokushima-u.ac.jp
検査部	松岡 賢市	(2300)	070-6586-0582	k-matsu@tokushima-u.ac.jp
手術部	滝沢 宏光	(3235)	070-6586-0187	takizawa@tokushima-u.ac.jp
放射線部	原田 雅史	(9282)	070-6586-0312	masafumi@tokushima-u.ac.jp
救急集中治療部	大藤 純	(9347)	070-6586-0442	joto@tokushima-u.ac.jp
リハビリテーション部	松浦 哲也	(9313)	070-6586-0213	tmatsu@tokushima-u.ac.jp
視能訓練部	三田村 佳典	(2365)	070-6586-0278	ymitaymitaymita@yahoo.co.jp
輸血・細胞治療部	三木 浩和	(7120)	070-6586-0826	mikihiro@tokushima-u.ac.jp
病理部	上原 久典	(9379)	070-6586-0570	uehara.h@tokushima-u.ac.jp
安全管理部	池本 哲也	(9377)	070-6586-0182	ikemoto.tetsuya@tokushima-u.ac.jp
感染制御部	松岡 賢市	(2300)	070-6586-0582	k-matsu@tokushima-u.ac.jp
総合歯科診療部	北村 直也	(9180)	070-6586-0371	nkitamura@tokushima-u.ac.jp
高次歯科診療部	湯本 浩通	(5260)	070-5348-3318	yumoto@tokushima-u.ac.jp
薬剤部	石澤 啓介	(3392)	070-6586-0620	ishizawa@tokushima-u.ac.jp
栄養部	高橋 章	(9428)	070-6586-0479	akiratak@tokushima-u.ac.jp
医療技術部	中尾 隆之	(7187)	070-6586-0431	nakao@tokushima-u.ac.jp
周産母子センター	加地 剛	(3276)	070-6586-0327	tkaji@tokushima-u.ac.jp
総合臨床研究センター	石澤 啓介	(3392)	070-6586-0620	ishizawa@tokushima-u.ac.jp
総合診療部	八木 秀介	(7110)	070-6586-0036	syagi@tokushima-u.ac.jp
患者支援センター	原田 雅史	(9282)	070-6586-0312	masafumi@tokushima-u.ac.jp
移植・免疫細胞療法センター	松岡 賢市	(2300)	070-6586-0582	k-matsu@tokushima-u.ac.jp
内視鏡センター	高山 哲治	(3209)	070-6586-0058	takayama@tokushima-u.ac.jp
超音波センター	山田 博胤	(7172)	070-6586-0041	yamadah@tokushima-u.ac.jp
高次脳センター	和泉 唯信	(2308)	070-6586-0116	yizumi@tokushima-u.ac.jp
卒後臨床研修センター	大藤 純	(9359)	070-6586-0442	joto@tokushima-u.ac.jp
医療支援センター	滝沢 宏光	(3235)	070-6586-0187	takizawa@tokushima-u.ac.jp
脳卒中センター	高木 康志	(2350)	070-6586-0140	ytakagi@tokushima-u.ac.jp

部署名	責任者 担当者	電話	携帯電話	メール
高度画像診断センター	原田 雅史	(9283)	070-6586-0312	masafumi@tokushima-u.ac.jp
口腔管理センター	青田 桂子	(5277)	070-6586-0396	aota.keiko@tokushima-u.ac.jp
がん診療連携センター	荻野 広和	(3213)	070-6586-0080	Ogino@tokushima-u.ac.jp
物流センター	高木 康志	(3246)	070-6586-0140	ytakagi@tokushima-u.ac.jp
ME管理センター	大藤 純	(9347)	070-6586-0440	joto@tokushima-u.ac.jp
アンチエイジング医療センター	松久 宗英	(7119)	070-6586-0571	matuhisa@tokushima-u.ac.jp
パーキンソン病・ジストニア治療研究センター	和泉 唯信	(2308)	070-6586-0116	yizumi@tokushima-u.ac.jp
高次脳機能障害支援センター	高木 康志	(2350)	070-6586-0140	ytakagi@tokushima-u.ac.jp
キャリア形成支援センター	脇野 修	(3238)	070-6586-0109	shuwakino@tokushima-u.ac.jp
糖尿病対策センター	松久 宗英	(7119)	070-6586-0571	matuhisa@tokushima-u.ac.jp
徳島県地域医療支援センター	西良 浩一	(6116)	070-6586-0000	t-cmsc@tokushima-u.ac.jp
口腔インプラントセンター	友竹 偉則	(5550)	070-6586-0775	tomotake.dent@tokushima-u.ac.jp
クリニカルアナトミー教育・研究センター	古川 順也	(3256)	070-6586-0263	jfurukawa@tokushima-u.ac.jp
てんかんセンター	高木 康志	(3246)	070-6586-0140	ytakagi@tokushima-u.ac.jp
国際医療センター	高木 康志	(2350)	070-6586-0140	ytakagi@tokushima-u.ac.jp
クリニカルパスセンター	岩佐 武	(2380)	070-6586-0451	iwasa.takeshi@tokushima-u.ac.jp
総合スポーツ医学センター	松浦 哲也	(9313)	070-6586-0213	matsuura@tokushima-u.ac.jp
口唇口蓋裂センター	橋本 一郎	(2396)	070-6586-0360	ichiro.h@tokushima-u.ac.jp
周術期管理センター	田中 克哉	(2387)	070-6586-0343	katsuya.tanaka@tokushima-u.ac.jp
看護師特定行為研修センター	田中 克哉	(2387)	070-6586-0343	katsuya.tanaka@tokushima-u.ac.jp
総合アレルギーセンター	北村 嘉章	(3266)	070-6586-0295	ykitamura@tokushima-u.ac.jp
再生医療細胞調整センター	森根 裕二	(2326)	070-6586-0172	ymorine@tokushima-u.ac.jp
総合腎臓病センター	脇野 修	(3538)	070-6586-0109	shuwakino@tokushima-u.ac.jp
痛みセンター	川人 伸次	(5388)	070-6586-0344	kawahito.shinji@tokushima-u.ac.jp
下肢救済・創傷治療センター	橋本 一郎	(2396)	070-6586-0360	ichiro.h@tokushima-u.ac.jp
脳卒中・心臓病等総合支援センター	佐田 政隆	(7170)	070-6586-0031	masataka.sata@tokushima-u.ac.jp
ゲノム医療センター	森野 豊之	(2241)		morino@tokushima-u.ac.jp
技工室	永尾 寛	(9129)	070-6586-0425	kan@tokushima-u.ac.jp
歯科衛生室	片岡 宏介	(5532)	070-6586-0417	kataoka-k@tokushima-u.ac.jp
子と親のこころ診療室	漆原 真樹	(3224)	070-6586-0633	urushihara@tokushima-u.ac.jp

部署名	責任者 担当者	電話	携帯電話	メール
褥瘡対策室	橋本 一郎	(2396)	070-6586-0360	ichiro.h@tokushima-u.ac.jp
人工透析室	脇野 修	(3538)	070-6586-0109	shuwakino@tokushima-u.ac.jp
排尿ケア管理室	山本 恭代	(9239)	070-6586-0273	yasuyoyamamo@tokushima-u.ac.jp

2.2.2. 関係部署・関係企業連絡先一覧

関係部署・関係企業の連絡先を以下に示す。

表 2.2-2 関係企業（委託先等）における連絡先

会社名	担当者	役割	電話	メール
N E C		システム 復旧	0120-553-818	tokushimadai-h30-nec @med.jp.nec.com
G E		システム 復旧	0120-055-919	電話のみ

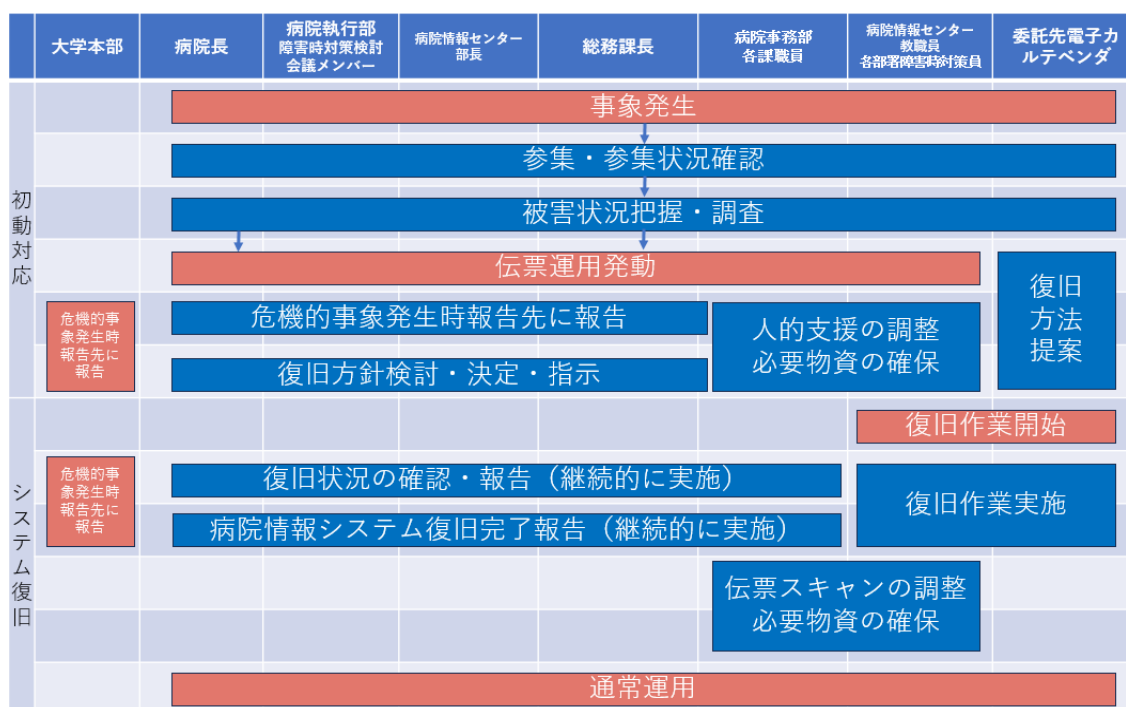
2.3. 重大情報セキュリティインシデント発生時における対応手順

2.3.1. 全体フロー

重大情報セキュリティインシデント発生時の病院情報システムの継続及び復旧に係る対応の流れについて、全体フローを以下に示す。

- ・重大情報セキュリティインシデント発生時の全体フロー

図 2.3-1 情報セキュリティインシデント発生時の全体フロー



2.3.2. 対応手順

重大情報セキュリティインシデント発生時の全体フローの具体的な対応手順を以下に示す。

- ・重大情報セキュリティインシデント発生時の対応手順

表2.3-1情報セキュリティインシデントが発生した場合の対応手順

項番	情報セキュリティインシデントが発生時の対応内容	参照文書
1	初動対応 ・発見者 感染拡大の防止と可及的かつ速やかな報告を行う。 ・病院情報システム運用責任者 的確な判断をするための情報の収集、関係者の健康の維持、混乱した状況での新たなインシデント誘発の防止 ・総務課（広報担当） 積極的な情報公開に基づく取材攻勢の鎮静化、患者・家族の不安を取り除くためのコミュニケーションとイメージダウンの最小化 ・病院情報システム管理者・運用担当者 被害範囲を特定するために状況を把握する。	【別冊②】 初動対応時の想定対応手順
2	参集 ・すべての担当者は、「徳島大学病院におけるサイバーインシデント発生時の連絡体制図」により、連絡を受けた後、速やかに指定された場所に参加する。	図2.2-1 重大情報セキュリティインシデント発生時の体制
3	要員の参集状況の確認 ・病院総務課長は、参集場所における病院情報システム運用継続計画の発動に伴う作業を実施する担当者の参集状況を確認し、病院長及び病院情報システムの運用を継続する事務局に報告する。 ・病院長及び病院情報システムの運用を継続する事務局は、参集場所における病院情報システム運用継続計画の発動に伴う作業を実施する担当者の参集状況を確認する。	図2.2-1 重大情報セキュリティインシデント発生時の体制
4	情報共有手段の確立 ・病院情報システム管理者は、委託先等の関連組織に、連絡先や早急に依頼すべき事項を連絡する。 ・病院総務課長及び病院情報システム運用継続計画の発動に伴う作業を実施する担当者は、パソコンや貼り紙等を準備し、重大情報	表2.3-2 各現場におけるインシデント状況及

	セキュリティインシデント発生時報告先や、病院情報システムの運用を継続する事務局との情報共有手段を確立する。	び医療状況の確認
5	被害状況の確認 ・病院総務課長は、調査箇所の優先順位を決定し、病院情報システムの被害状況の確認を病院情報システム運用継続計画の発動に伴う作業を実施する担当者に指示する。病院総務課長は確認結果を病院長及び病院情報システムの運用を継続する事務局に報告する。 ・病院情報システムの運用を継続する事務局は、随時被害状況の確認結果を記録する。 ・電話、メール予備文書にて職員への周知を行う。 ・院内放送により職員及び来院者に被害状況の周知を行う。	表2.3-3 医療の提供状況、患者の対応状況、システムの障害状況の報告 青字は日中
6	復旧方針の決定 ・病院総務課長は、確認した被害状況をもとに、患者の生命を最優先に考慮した優先順位を定め、今後の病院情報システムの復旧水準、復旧方式等の対応方針を検討する。また、重大情報セキュリティインシデント発生時報告先や各部署に対する依頼事項を取りまとめる。 ・病院長は、病院執行部メンバーと協議し、復旧方針を決定する。	表2.3-4 被害状況調査の方針や参照環境の構築方針の確認
7	復旧指示 ・診療における伝票運用の指示 病院長は、短時間での病院情報システム復旧が困難と判断した場合、病院総務課長を通じて、全部署に診療業務の伝票運用への切り替えを指示する。伝票運用の手順は本書の別冊①「サイバー攻撃等によるシステム停止時の対応について」に記す。 ・病院情報システムの復旧作業の指示 病院長は、病院情報センター部長に復旧方針に基づき病院情報システムを復旧するよう指示する。 ・HPにより、障害の影響により通常診療ができない旨公表し、職員向け説明会を実施する。また、メディアに報道資料提供を行った上で記者会見を開催する。	青字は日中
8	病院情報システムの復旧作業の実施 ・病院情報センター部長は、復旧指示や復旧方針に基づき、病院情報システムの復旧作業を行う。必要に応じ委託先に対応を依頼する。また、病院総務課長は、適宜復旧状況を病院長及び病院情報システムの運用を継続する事務局に報告するとともに、必要な支	

	援を依頼する。	
9	被害状況・復旧状況の報告と支援依頼 (以下、継続的に実施) ・病院長は、被害状況と復旧方針、復旧の見込み及び関係部局への依頼事項を、重大情報セキュリティインシデント発生時報告先に報告する。 また、病院情報システムの復旧優先度と目標復旧時間を考慮し、重大情報セキュリティインシデント発生時報告先に必要な支援を要請する。 ・病院情報システムの運用を継続する事務局は、重大情報セキュリティインシデント発生時報告先や掲示板等により、病院情報システムの復旧見込みや依頼事項を関係部局に周知する。病院長は、学長（大学本部）と必要に応じて協議する。	表2.3-5 病院事務部の初動対応時の役割
10	病院情報システム復旧完了報告 ・病院長は、病院情報システムが復旧した場合、復旧の完了を重大情報セキュリティインシデント発生時報告先及び学長（大学本部）に報告する。 ・病院情報システムの運用を継続する事務局は、重大情報セキュリティインシデント発生時報告先や掲示板等により、病院情報システムの復旧と依頼事項を関係部局に周知する。	
11	記録物の整理 全ての担当者は、復旧作業で記載した記録物が紛失しないよう情報を整理する。 被災時に記録した内容については、今後の計画の見直しにおける重要な参考資料となることから、特に対応に苦慮した点等があれば、確実に記録に残しておく。	

表2.3-2 各現場におけるインシデント状況及び医療状況の確認

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)
障害時対策検討会議	☐ 障害時対策検討会議の設置確認 初回会議開始時間の確認 災害対策室主導で運用開始
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連絡実施 ☐ 院内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

表 2.3-3 医療の提供状況、患者の対応状況、システムの障害状況の報告

内容	主な確認事項
外来運用状況	☐ 外来受付状況、初診患者受入状況、システム運用状況
病棟運用状況	☐ 新入院受入れ状況、在院患者管理状況、要転院患者状況、システム運用状況
手術運用状況	☐ 予定手術対応状況、緊急手術対応状況
救急運用状況	☐ 救急受入状況、救急隊連絡状況、他医療機関支援要請状況
医療技術部門運用状況	☐ 各部門運用状況(薬剤部・検査部・放射線部・病理部・輸血部・栄養部・リハビリテーション部・臨床工学部 他)
地域連携運用状況	☐ 予約受入状況、他機関情報発信状況、地域連携システム運用状況

医事関連運用状況	☐	受付会計対応状況
医療情報運用状況	☐ ☐	システム被害状況・復旧時期見込の情報共有 参照環境構築状況
決定事項	☐ ☐ ☐	紙カルテ運用方針 患者対応方針(外来・入院・救急・手術・その他) 広報対応方針(地域・ホームページ・報道)
職員説明	☐	職員に対する説明方法、連絡方法の確認
会議運営方針	☐ ☐ ☐	障害時対策検討会議の運営方法(頻度時間、運営等)確認 会議場所、対策本部の場所、情報共有方法の確認 優先順位の確認
システム稼働状況	☐ ☐ ☐ ☐ ☐	基幹システムの稼働状況・被害状況の把握 部門システムの稼働状況・被害状況の把握 その他システムの稼働状況の確認 医療機器の稼働状況確認 ネットワークの運用状況の確認

表 2.3-4 被害状況調査の方針や参照環境の構築方針の確認

内容	主な確認事項	
システム障害発生要因	☐	各現場からの情報に基づき、障害発生要因を検討し、調査の方向性を決定
証拠保全	☐ ☐	証拠保全対象の機器分類 警察との調整
調査	☐ ☐	情報漏洩調査(ダークウェブ調査)の実施確認 フォレンジック調査の実施確認
参照環境構築	☐ ☐ ☐ ☐ ☐	オフラインバックアップデータの確認 参照システム(Gemini)の稼働状況確認 参照環境構築までの手順確認 安全なサーバ、端末、プリンターの確認 参照環境端末の運用会場の確認(電力容量の確認含む)
復旧計画	☐	再感染防止対策の確認

表 2.3-5 病院事務部の初動対応時の役割

内容	主な確認事項	
総務課	☐	大学本部、徳島県との調整
	☐	国、警察との調整
	☐	プレスリリースを含めたマスメディア対応
	☐	ホームページ更新
	☐	クロノロ等障害時対策検討会議サポート
医事課	☐	患者電話対応
	☐	玄関付近患者案内
	☐	医事委託事業者調整
	☐	国オンライン系システム調整
	☐	会計ルール策定・調整・周知
経営企画課	☐	クロノロ等障害時対策検討会議サポート
	☐	システム障害による経営に関する影響調査
経理調達課	☐	備品・消耗品調達
	☐	コピー関係確保(消耗品含む)
	☐	電話回線確保
施設整備連携室	☐	電源確保
	☐	通信回線確保
	☐	クロノロ等障害時対策検討会議サポート

3. 事前対策計画

3.1. 病院情報システムを支える構成要素ごとの現状対策レベルとリスク

病院情報システムの現状対策レベルとリスクの評価結果について、以下に記す。

表 3.1 病院情報システムの構成要素ごとの現状対策レベルとリスク

No.	担当部署	システム名	リスク分類		現状対策レベル
			可用性	発生時の影響度	
1	歯科	歯科システム	3	3	3
2	歯科	歯科技工・レポート	2	2	3
3	看護部	看護勤務管理システム	1	1	1
4	看護部	看護キャリア開発支援システム	1	1	1
5	看護部	一般病棟用生体モニタシステム	1	1	1
6	看護部	看護ポータルシステム	1	1	1
7	看護部	ナースコールシステム	3	3	3
8	看護部(物流センター)	滅菌物品管理システム	2	2	3
9	褥瘡対策室	褥瘡管理システム	2	2	3
10	ICU	集学病棟システム	3	3	3
11	ICU	NICU、産科システム	3	3	3
12	検査部	検体検査部門システム	3	3	3
13	検査部	採血・採尿受付機・採血管準備システム	3	3	3
14	検査部	細菌検査システム	3	3	3
15	検査部	生理検査部門システム	3	3	3
16	検査部	生理画像ファイリングシステム	3	3	3
17	検査部	脳波検査システム	3	3	3
18	輸血部	輸血部門システム	3	3	3
19	病理部	病理部門システム	3	3	3
20	病理部	病理診断バーチャルスライド	3	3	3
21	手術部	手術室・麻酔管理システム	3	3	3
22	手術部	旧手術システム	1	1	1

23	超音波センター	超音波ファイリングシステム	3	3	3
24	内視鏡センター	内視鏡ファイリングシステム	3	3	3
25	放射線部	放射線部門システム、読影レポート	3	3	3
26	放射線部	放射線治療管理システム	3	3	3
27	放射線部	カンファレンス支援システム	1	1	1
28	放射線部	PACS	3	3	3
29	放射線部	徳島画像診断ネットワーク	3	3	3
30	放射線部	被ばく線量管理システム	1	1	1
31	放射線部	汎用画像診断装置ワークステーション	1	1	1
32	放射線部	胸部 CT 読影支援システム	1	1	1
33	放射線部	放射線部グループワーク	1	1	1
34	放射線部	患者情報連携	2	2	3
35	放射線部	画像診断支援システム	1	1	1
36	放射線部	J-MID アノテーションシステム	1	1	1
37	薬剤部	調剤支援システム	3	3	3
38	薬剤部	注射薬自動払出システム	3	3	3
39	薬剤部	物品管理システム	1	1	1
40	薬剤部	薬剤管理指導支援システム	2	2	3
41	薬剤部	医薬品情報検索システム	1	1	1
42	薬剤部	病棟薬剤業務支援システム	1	1	1
43	リハビリテーション部	リハビリテーション部門システム	2	2	3
44	栄養部	栄養管理・栄養指導システム	3	3	3
45	栄養部	N S T 支援	2	2	3
46	安全管理部	安全管理対策部門システム	1	1	1
47	安全管理部	安全管理 e-Learning システム	1	1	1
48	感染制御部	感染症管理システム	1	1	3
49	感染制御部	感染ネットワークシステム	1	1	1
50	人工透析室	透析部門システム	2	2	3
51	ME 管理センター	医療機器管理システム	1	1	3
52	脳卒中センター	脳卒中遠隔診断支援システム	3	3	3
53	経営企画課	DPC 分析システム	1	1	1
54	医事課	医事システム	3	3	3
55	医事課	DPC ナビ	2	2	3
56	医事課	医学管理サポート	2	2	3

57	医事課	自動精算機システム	2	2	3
58	医事課	窓口精算機システム	2	2	3
59	医事課	診察券発行機	2	2	3
60	医事課	自動再来受付機	2	2	3
61	医事課	歯科レセチェック	1	1	1
62	医事課	退院サマリ、診療録管理、がん登録	1	1	1
63	医事課	紙カルテスキャン	2	2	3
64	医事課	文書管理システム	3	3	3
65	医事課	診療情報提供書交換サービス	2	2	3
66	経理調達課	物流システム（SPD）	2	2	3
67	病院情報センター	ポータル・統合認証	3	3	3
68	病院情報センター	グループウェア	1	1	1
69	病院情報センター	患者ポータル	2	2	3
70	病院情報センター	部門カルテ	3	3	3
71	病院情報センター	画像ファイリング	3	3	3
72	病院情報センター	文書等タイムスタンプ	2	2	3
73	病院情報センター	資産管理システム	1	1	1
74	病院情報センター	仮想インターネット	1	1	1
75	病院情報センター	紹介状管理システム	2	2	3
76	病院情報センター	地域連携（阿波あいネット）	3	3	3
77	病院情報センター	統合ストレージ	3	3	3
78	病院情報センター	脳画像解析プログラム	1	1	1
79	病院情報センター	循環器画像管理システム	3	3	3
80	病院情報センター	外来診療支援システム （受付チェックイン、呼び込み）	3	3	3
81	病院情報センター	手術動画送信	2	2	1
82	病院情報センター	生体情報モニタリングシステム	3	3	3
83	病院情報センター	インスリンポンプデータ管理システム	2	2	1
84	病院情報センター	糖尿病管理システム	2	2	1
85	病院情報センター	内視鏡手術支援ロボット	3	3	3
86	病院情報センター	国立大学病院遠隔バックアップシステム	2	2	3
87	病院情報センター	全国糖尿病データベース事業	1	1	1
88	病院情報センター	症例登録支援システム	1	1	1
89	病院情報センター	電子カルテシステム	3	3	3

4. 教育訓練計画・維持改善計画

4.1. 教育訓練計画

(1) 教育訓練の目的

病院情報システム運用継続計画の実効性を維持改善していくため、災害対策訓練の一環として、定期的に教育訓練を実施するものとする。

(2) 教育訓練の内容

病院長及び病院情報センター部長は、毎年4月に年間の教育訓練計画を作成し、計画に沿った訓練が適切に実施されるよう監督するものとする。

(3) 教育訓練の評価

病院長及び病院情報センター部長は、教育訓練の目標を定め、その結果を評価し「4.2.維持改善計画」の参考情報として活用する。

年間の教育訓練計画を以下のとおりに示す。

表 4.1 IT-BCP 教育訓練計画

教育訓練 内容	受講対象	教育訓練実施時期											備考								
		4	5	6	7	8	9	10	11	12	1	2		3							
		病院情報システム 運用継続計画見直し ▼												災害対策訓練 IT-BCP訓練 ▼							
手順書 確認訓練	危機的事象発生時の対応体制メンバー								○												
	一般職員								○												
システム リカバリ 訓練	病院情報センター 電子カルテベンダ				○									リカバリ手順を確認する 電子カルテベンダ参加依頼							
伝票運用 訓練	危機的事象発生時の対応体制メンバー						○														
	一般職員								○												

4. 2. 維持改善計画

4. 2. 1. 計画の実施に伴う維持改善

病院長及び病院情報センター部長は、以下の契機にて、病院情報システム運用継続計画の見直しを行う。

表 4. 2-1 運用継続計画の見直し契機

No.	契機	実施内容
1	主要な事前対策の完了後	・ 事前対策に係る現状対策レベルを更新する。 ・ 必要に応じて重大情報セキュリティインシデント発生時の対応計画の改訂を行う。
2	訓練実施後	・ 訓練結果により、事前対策や重大情報セキュリティインシデント発生時の対応計画等に解決すべき課題が発生した場合、随時課題の解決を図る。 ・ 短期間での解決が困難な場合は、事前対策の実施計画の見直しを行い、適切に対応する。
3	新規システムの構築時	・ 新規システムの構築時に、病院情報システム運用継続計画作成の有無を検討する。作成する場合、ガイドラインに基づき当該システムの病院情報システム運用継続計画を作成し、必要な対策を調達時の仕様書に盛りこむ。

4. 2. 2. 危機的事象の発生に伴う維持改善

病院長及び病院情報センター部長は、病院情報システム運用継続計画で対象とする事象、又はそれに近い事象が発生した際は、事態の収束後、以下の事項についての報告を整理し、病院情報システム運用継続計画を改訂する。

①発生事象の分析

- 1) 発生事象の性質について
- 2) 発生原因について

②重大情報セキュリティインシデント発生時対応の評価

- 1) あらかじめ役割を割り当てられた担当者の対応の適切さ
- 2) 職員の対応の適切さ

③RT0（目標復旧時間）の達成度合い

- 1) 実際の復旧時間について
- 2) 対応の実効性について

④病院情報システム運用継続計画の改善点

- 1) RT0 実対応ギャップの原因について
- 2) その他、病院情報システム運用継続計画の有効性向上につながる改善点について

4.2.3. 定期的な見直しによる維持改善

病院長及び病院情報センター部長は、毎年4月頃定期的に以下の内容について確認し、記録（見直し実施日や実施担当者等）を残すものとする。見直しの結果、改善の必要がある場合は適切な措置を講ずる。

表 4.2-2 見直し事項

見直し事項	見直し内容
事前対策計画	・ 計画に基づき、事前対策は確実に実施されたか。
	・ 実施した事前対策を踏まえて内容を更新したか。（現状対策レベル、事前対策計画、その他計画については後述）。
	・ 事前対策計画に基づき、来年度予算で取り上げる対策を検討したか。また、実施未定の対策について予算化を検討したか。
	・ 訓練の結果を踏まえて計画の見直しを行ったか。
	・ 業務部門及び業務継続計画事務局を交えて業務継続計画との整合性を確認したか。
重大情報セキュリティインシデント発生時対応計画	・ 連絡網や担当者は最新化されているか。
	・ 実施完了した事前対策がある場合、対応手順を適切に見直したか。
	・ 教育訓練の結果を踏まえて計画の見直しを行ったか。
教育訓練計画	・ 計画に基づき、訓練は確実に実施されたか。
	・ 訓練の結果を踏まえて計画の見直しを行ったか。
病院情報システム運用継続計画の策定の根拠とした分析・策定・検討	・ 病院情報システム運用継続計画の適用範囲を広げることを検討したか。
	・ 外部環境の変化や社会的な要求の高まり等による、病院情報システム運用継続計画の見直しの必要性がないか検討したか。
	・ 新しい病院情報システムが追加された場合、情報システム復旧優先度の設定や必要な事前対策計画、重大情報セキュリティインシデント発生時の対応計画及び教育訓練計画を検討したか。
	・ 最新の技術動向に基づき、目標対策レベルの見直しを検討したか。

5. 計画策定の根拠とした調査・分析・検討

5.1. 想定する危機的事象

(1) 対象とする危機的事象

本書で対象とする危機的事象は、以下を対象とする。

- ・ 情報セキュリティインシデント

(2) 危機的事象の発生時の条件 それぞれの危機的事象の発生時の条件については、徳島大学病院の業務継続計画の想定を踏まえるとともに、病院情報システム運用継続の条件が最も厳しくなるケースを想定し、以下のとおり特定する。

情報セキュリティインシデント発生想定

- ・ 日曜日の午前2時に病院情報システムが停止。
- ・ ランサム攻撃により、バックアップを含む病院情報システムのデータが暗号化され利用不可（2週間前から半年前までの15世代のテープバックアップは無事に保管されている）。
- ・ 一切の患者情報が閲覧さえできない。
- ・ 部門システムも停止し、医療機器が単体で利用できる状況。
- ・ 病院情報システム端末もウイルスに感染し、使用不可（ネットワーク切り離し）。
- ・ 警察による捜査もあり、被害を受けた機器は利用できない。
- ・ 数日程度でのシステム復旧は見込めない。
- ・ システム復旧まで、全ての業務について伝票を使用した紙運用で対応せざるを得ない。

5.2. 想定する被害状況

重大情報セキュリティインシデント発生時の被害想定 情報セキュリティインシデント発生時の被害状況の想定結果について、下表に示す。

表 5.2-1 情報セキュリティインシデント発生時の被害状況の想定の結果

被害想定対象		被害想定概要
人的資源	病院情報システム運用業務に従事する要員	被害はないが、職員や委託先、協力者が業務に対応できない可能性がある。
建物・設備	病院情報システムの設置場所	被害はなく平常どおり利用可能。
	交通インフラ	被害はなく平常どおり利用可能。
	電力	被害はなく平常どおり利用可能。
	水道	被害はなく平常どおり利用可能。
病院情報システム	情報通信ネットワーク	音声通話、メール、アプリ（通話・チャット等）のサービスは被害がなく、平常どおり利用可能。 物理的被害はないが、病院情報システムネットワークは、コンピュータウィルス感染の可能性があるため利用できない。
	情報システム機器	物理的被害はないが、コンピュータウィルスによるシステムの暗号化等が予想され、機能停止が考えられる。
	データ	病院情報システムで使用しているデータファイルが暗号化などの改ざんや消去されて使用不能となる可能性がある。

病院情報システムが利用できなくなることを除き、ライフライン等に対する影響は生じないと想定されるため、上記のとおり被害を想定した。

5.3. 病院情報システムの復旧優先度の設定

病院情報システムに復旧優先度を設定した。検討結果を以下に示す。

(1) 各システムのリスク分析を基に復旧優先度を検討

病院情報センターは、各システムのリスク分析結果を利用し、病院情報システムの復旧優先度を6段階（S、A、B、C、D、E）に整理した。整理結果を以下に示す。

表 5.3-1 病院情報システムの復旧優先度

No.	担当部署	システム名	リスク分類		復旧優先度
			可用性	発生時の影響度	
1	歯科	歯科システム	3	3	S
2	歯科	歯科技工・レポート	2	2	S
3	看護部	看護勤務管理システム	1	1	B
4	看護部	看護キャリア開発支援システム	1	1	B
5	看護部	一般病棟システム	1	1	B
6	看護部	看護ポータルシステム	1	1	B
7	看護部	ナースコールシステム	3	3	S
8	看護部（物流センター）	滅菌物品管理システム	2	2	A
9	褥瘡対策室	褥瘡管理システム	2	2	A
10	ICU	集学病棟システム	3	3	S
11	ICU	NICU、産科システム	3	3	S
12	検査部	検体検査部門システム	3	3	S
13	検査部	採血・採尿受付機・採血管準備システム	3	3	S
14	検査部	細菌検査システム	3	3	S
15	検査部	生理検査部門システム	3	3	S
16	検査部	生理画像ファイリングシステム	3	3	S
17	検査部	脳波検査システム	3	3	S
18	輸血部	輸血部門システム	3	3	S
19	病理部	病理部門システム	3	3	S
20	病理部	病理診断バーチャルスライド	3	3	S
21	手術部	手術室・麻酔管理システム	3	3	S
22	手術部	旧手術システム	1	1	B

23	超音波センター	超音波ファイリングシステム	3	3	S
24	内視鏡センター	内視鏡ファイリングシステム	3	3	S
25	放射線部	放射線部門システム、読影レポート	3	3	S
26	放射線部	放射線治療管理システム	3	3	S
27	放射線部	カンファレンス支援システム	1	1	B
28	放射線部	PACS	3	3	S
29	放射線部	徳島画像診断ネットワーク	3	3	S
30	放射線部	被ばく線量管理システム	1	1	B
31	放射線部	汎用画像診断装置ワークステーション	1	1	B
32	放射線部	胸部 CT 読影支援システム	1	1	B
33	放射線部	放射線部グループワーク	1	1	B
34	放射線部	患者情報連携	2	2	A
35	放射線部	画像診断支援システム	1	1	B
36	放射線部	J-MID アノテーションシステム	1	1	B
37	薬剤部	調剤支援システム	3	3	S
38	薬剤部	注射薬自動払出システム	3	3	S
39	薬剤部	物品管理システム	1	1	B
40	薬剤部	薬剤管理指導支援システム	2	2	A
41	薬剤部	医薬品情報検索システム	1	1	B
42	薬剤部	病棟薬剤業務支援システム	1	1	B
43	リハビリテーション部	リハビリテーション部門システム	2	2	A
44	栄養部	栄養管理・栄養指導システム	3	3	S
45	栄養部	N S T 支援	2	2	A
46	安全管理部	安全管理対策部門システム	1	1	B
47	安全管理部	安全管理 e-Learning システム	1	1	B
48	感染制御部	感染症管理システム	1	1	B
49	感染制御部	感染ネットワークシステム	1	1	B
50	人工透析室	透析部門システム	2	2	S
51	ME 管理センター	医療機器管理システム	1	1	B
52	脳卒中センター	脳卒中遠隔診断支援システム	3	3	S
53	経営企画課	DPC 分析システム	1	1	B
54	医事課	医事システム	3	3	S
55	医事課	DPC ナビ	2	2	A
56	医事課	医学管理サポート	2	2	A

57	医事課	自動精算機システム	2	2	A
58	医事課	窓口精算機システム	2	2	A
59	医事課	診察券発行機	2	2	A
60	医事課	自動再来受付機	2	2	A
61	医事課	歯科レセチェック	1	1	B
62	医事課	退院サマリ、診療録管理、がん登録	1	1	B
63	医事課	紙カルテスキャン	2	2	A
64	医事課	文書管理システム	3	3	S
65	医事課	診療情報提供書交換サービス	2	2	A
66	経理調達課	物流システム（SPD）	2	2	A
67	病院情報センター	ポータル・統合認証	3	3	S
68	病院情報センター	グループウェア	1	1	B
69	病院情報センター	患者ポータル	2	2	A
70	病院情報センター	部門カルテ	3	3	S
71	病院情報センター	画像ファイリング	3	3	S
72	病院情報センター	文書等タイムスタンプ	2	2	A
73	病院情報センター	資産管理システム	1	1	B
74	病院情報センター	仮想インターネット	1	1	B
75	病院情報センター	紹介状管理システム	2	2	A
76	病院情報センター	地域連携（阿波あいネット）	3	3	S
77	病院情報センター	統合ストレージ	3	3	S
78	病院情報センター	脳画像解析プログラム	1	1	B
79	病院情報センター	循環器画像管理システム	3	3	S
80	病院情報センター	外来診療支援システム	3	3	S
81	病院情報センター	手術動画送信	2	2	B
82	病院情報センター	生体情報モニタリングシステム	3	3	S
83	病院情報センター	インスリンポンプデータ管理システム	2	2	A
84	病院情報センター	糖尿病管理システム	2	2	B
85	病院情報センター	内視鏡手術支援ロボット	3	3	S
86	病院情報センター	国立大学病院遠隔バックアップシステム	2	2	S
87	病院情報センター	全国糖尿病データベース事業	1	1	B
88	病院情報センター	症例登録支援システム	1	1	B
89	病院情報センター	電子カルテシステム	3	3	S

なお、上記表の病院情報システムの復旧優先度は、以下を基準とする。

表 5.3-2 情報システムの復旧優先度

求められる目標復旧時間	復旧優先度
0～3 時間以内に復旧	S
3 時間から 1 日以内に復旧	A
1 日から 3 日以内に復旧	B
3 日から 1 週間以内に復旧	C
1 週間から 2 週間以内に復旧	D
2 週間を超える停止が許容できる	E

5.4. 病院情報システムを支える構成要素の関連整理

5.4.1. 病院情報システムを支える構成要素の整理

危機的事象の発生に備え、病院情報システムを支える構成要素について整理する。ガイドラインの例、徳島大学病院の業務継続計画内で作成している重大情報セキュリティインシデント発生時の対応手順、既に作成している病院情報システム運用継続の対応手順等を参考にしながら、危機的事象が発生した際の対応をイメージし、必要な要素に漏れがないように洗い出す。

(1) 病院情報システムを支える構成要素の整理

表 5.4-1 病院情報システムを支える構成要素の整理

病院情報システムを支える構成要素		説明
人的資源	病院情報システム運用体制	システムの被害状況の早期確認や適切な対応を実施するための運用体制と役割分担、手順書の整備及び連絡手段の確保
建物・設備	施設	病院情報システム機器の設置環境
病院情報システム	ハードウェア	サーバ等のハードウェア機器の台数及び所在
〃	システム領域	アプリケーションやシステム設定情報等の病院情報システム復旧に必要なデータの所在及び管理状況（バックアップ媒体の外部保管等）
病院情報システム	データ領域	重要なデータの所在及び管理状況（バックアップ媒体の外部保管等）
〃	情報通信ネットワーク	病院情報システムを利用するために必要な情報通信ネットワークの敷設状況
外部組織	委託先	重大情報セキュリティインシデント発生時における委託先の支援・協力体制、委託先の事業継続能力把握、SLA の締結等

5.4.2. 病院情報システムを支える構成要素ごとの目標対策レベルの設定

病院情報システムの復旧優先度に対応する対策目標（目標対策レベル）を目標復旧時間を踏まえ情報システムを支える構成要素ごとに整理した。設定結果を以下に示す。

(1) 病院情報システムの復旧優先度に対応する対策目標

表 5.4-2 病院情報システムの復旧優先度に対応する対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	ホットスタンバイ用ハードウェアの確保 ・専用の代替機を、現在の拠点と同時に被害を受けない拠点に設置する。被害時は代替機に切り替えることで、冗長化システムによる復旧を行う。	4
A	ウォームスタンバイ用ハードウェアの確保 ・現在の拠点と同時に被害を受けない拠点にOS、アプリケーションをインストールし、起動している状態の予備機を準備する。被害時には専用の代替機として利用することにより、バックアップシステムによる復旧を行う。	3
B		
C	コールドスタンバイ用ハードウェアの確保 ・現在の拠点と同時に被害を受けない拠点にOS、アプリケーションをインストールしていない状態で予備機を準備する。	2
D		
E	遠隔地にバックアップ用ハードウェア準備なし(被害拠点での復旧) ・販売が終了しており、保守契約の締結や再調達できないハードウェアを利用しないようにしておく。 ・ハードウェアの損壊時に修理部品や代替機を入手できるよう、保守契約を締結する。生産年数、在庫の保管年数等も確認する。	1

(2) システム領域における復旧優先度別の対策目標

表 5.4-3 システム領域における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	ホットスタンバイ方式 ・本番機のシステムメンテナンス時に、本番機のシステム領域のバックアップデータを代替拠点の代替機上に転送している。 ・代替機についてもシステムメンテナンスを行い、切替可能な環境を保っている。	4
A	ウォームスタンバイ方式 ・本番機のシステムメンテナンス時に、本番機のシステム領域のバックアップデータを代替拠点の代替機上に転送している。	3
B		
C	コールドスタンバイ方式 ・システムメンテナンス時にシステム領域をバックアップし、予備機の準備してある代替拠点に転送（配送）、保管している。 ・被害発生時は、バックアップからリストアし、予備機に反映する。	2
D		
E	外部サービス（データセンター、クラウドサービス等）への移行 ・システムメンテナンス時にバックアップ媒体（テープ等）にシステム領域をバックアップし、本番機と同時に被害を受けない場所に保管している。被害発生時は、バックアップを取り寄せる。又は堅牢なデータセンターなどのデータを保存している外部サービスを利用する。	1

(3) データ領域における復旧優先度別の対策目標

表 5.4-4 データ領域における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	・代替拠点で、データ同期を利用して本番環境における被害発	4

	生直前のデータを保全している。	
A	・代替拠点で、オンラインバックアップを利用し本番環境における被害発生時数時間前のデータを保全している。	3
B		
C	・代替拠点で、オンラインバックアップを利用し本番環境における被害発生時 1 日前のデータを保全している。	2
D		
E	・本番機と同時に被害を受けない堅牢な場所に、災害発生時 1 週間前のデータを保存している。被害発生時は、バックアップを取り寄せる。又は堅牢なデータセンターなどのデータを保存している外部サービスを利用する。	1

(4) 委託先の事業継続能力における復旧優先度別の対策目標

表 5.4-5 委託先の事業継続能力における復旧優先度別の対策目標

情報システムの復旧優先度	対策目標	対策レベル
S	契約の締結 (対策レベル 2 に加え) ・委託先との S L A、災害時協定に関する条項を、契約書や仕様書の中に含めている。	3
A		
B		
C	事業継続能力の把握 (対策レベル 1 に加え) ・事業継続への取り組みについて委託先に質問するアンケートを配布する等して、情報システムの復旧対応において必要不可欠な委託先の事業継続能力を把握している。	2
D		
E	連絡先の明確化 ・情報システムの復旧対応において必要不可欠な委託先（ハードウェア・ソフトウェアの調達先、システム構築業務の委託先等）が明確になっている。 ・同委託先の緊急連絡先（窓口及び代替拠点先）が代理者も含め明確になっている。	1

6. 事後対応

6.1 報告

復旧後、復旧結果と情報漏えい事実の有無等について、連絡体制により学内組織に報告する。

不足していたと考えられる事前対策、連絡先ならびに連絡内容について振り返りを行う。

6.2 再発防止

6.2.1 再発防止策検討・策定

6.1 の後、サイバー攻撃により発生した被害を抑止する手段について検討を行い、実施可能な選択肢を整備し、病院執行部に提案する。病院執行部は長期的視点と事業継続性の両立について検討し、安全性を維持するため再発防止策の選択を決定する。病院情報システム管理者は決定した再発防止策について、連絡経路を用いて全職員に周知する。

6.2.2 事業者への指示

病院執行部によって決定された再発防止策は、医療情報システム安全管理責任者により、事業者が有するサービスや機器に対して対策を講じる必要があるかどうかを調査し、再発防止策の効果が出るよう対策実施を事業者へ打診する。事業者は、対策実施の時期や方法について、当院と誠実に議論し、計画を立てて実施する。

6.3 情報公開

病院情報システム運用責任者は、類似のサイバー攻撃による被害拡大に対する警鐘を鳴らす目的、また当院を受診する患者への診療に関連する注意を喚起する目的で、速やかに情報公開を行う。情報公開内容は、知覚日時、現象、被害範囲、想定される攻撃経路、1次対応、患者対応、復旧状況、事後対策などを含める。報告については、サイバー被害が発生した可能性が高い段階から迅速に行い、情報の更新を含めて複数回行う中で情報の確度を高めていく。