IT-BCP策定に関するチェックリスト

2024年6月13日

徳島大学大学院医歯薬学研究部　医療情報学分野
徳島大学病院　病院情報センター
田木真和

徳島大学
TOKUSHIMA UNIVERSITY

医療機関のサイバー攻撃対策強化に関する政策等

医療法第25条第1項の規定に基づく立ち入り検査（2022年度の留意事項）	医療機関においてサイバーセキュリティ対策の強化を図るため、以下に掲げる事項について確認を行う。 ① PCやVPN機器等の脆弱性情報を収集し、速やかに対策を行える体制の確保 ② 診療継続のためのデータやシステムのバックアップの確実な実行 ③ **復旧手順の検討とBCP策定**、サイバー攻撃を想定した訓練 ④ 医療情報システムの保守会社等への連絡体制や厚生労働省への連絡体制の確保
医療情報システムの安全管理に関するガイドラン 第6.0版（2023年5月改定）	【11.2】非常時に備えた通常時からの対応（サイバー攻撃） ●緊急時対応体制（CSIRT）の整備 ●利用者等の関係者の教育・訓練 ●脆弱性対策等 ●情報共有体制の構築（外部有識者、事業者） ●攻撃を受けた際の代替運用や手段の確保 など ●**BCPを踏まえた情報システムに関する手順整備** ●ネットワークやバックアップ等に関する安全性の確保 など ●医療情報システムに関する各種ドキュメントの整備 ●臨時措置に必要な情報システム資源の確保方法の準備 など
診療報酬改定（2024年度）	【診療録管理体制加算１】200床以上の保険医療機関について、 第1：専任の医療情報システム安全管理責任者を配置 第2：非常時に備えた医療情報システムのバックアップを複数の方式で確保し、その一部はネットワークから切り離したオフラインで保管 第3：**非常時を想定した医療情報システムの利用が困難な場合の対応や復旧に至るまでの対応についての業務継続計画を策定**し、少なくとも年１回程度、定期的に当該業務継続計画に基づく訓練・演習を実施

IT-BCPの策定により損失を最小限に

国立大学病院は増収・減益傾向が続いており、コロナの影響もあって収益の回復していない大学病院もあるなかで、サイバー攻撃による**十数億以上の損害を補填できない**恐れがある

損害保険の実情は･･･

利益損失を全額補てんできる損害保険を取扱う保険会社は少ない・・・

・自己防衛は大事だが➢サイバー攻撃を受けた際の復旧スピードもカギに・・・

・IT-BCPを策定し、訓練等による事前の備えが速やかな復旧を可能にする

脇元直彦. サイバー攻撃を受けた際の利益損失とIT-BCPの策定について. 第43回医療情報学連合大会, 2023.

BCPとは

- 大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、または中断しても**可能な限り短い期間で復旧させるための方針、体制、手順等を示した計画**のことを事業継続計画（Business Continuity Plan、BCP）と呼ぶ。

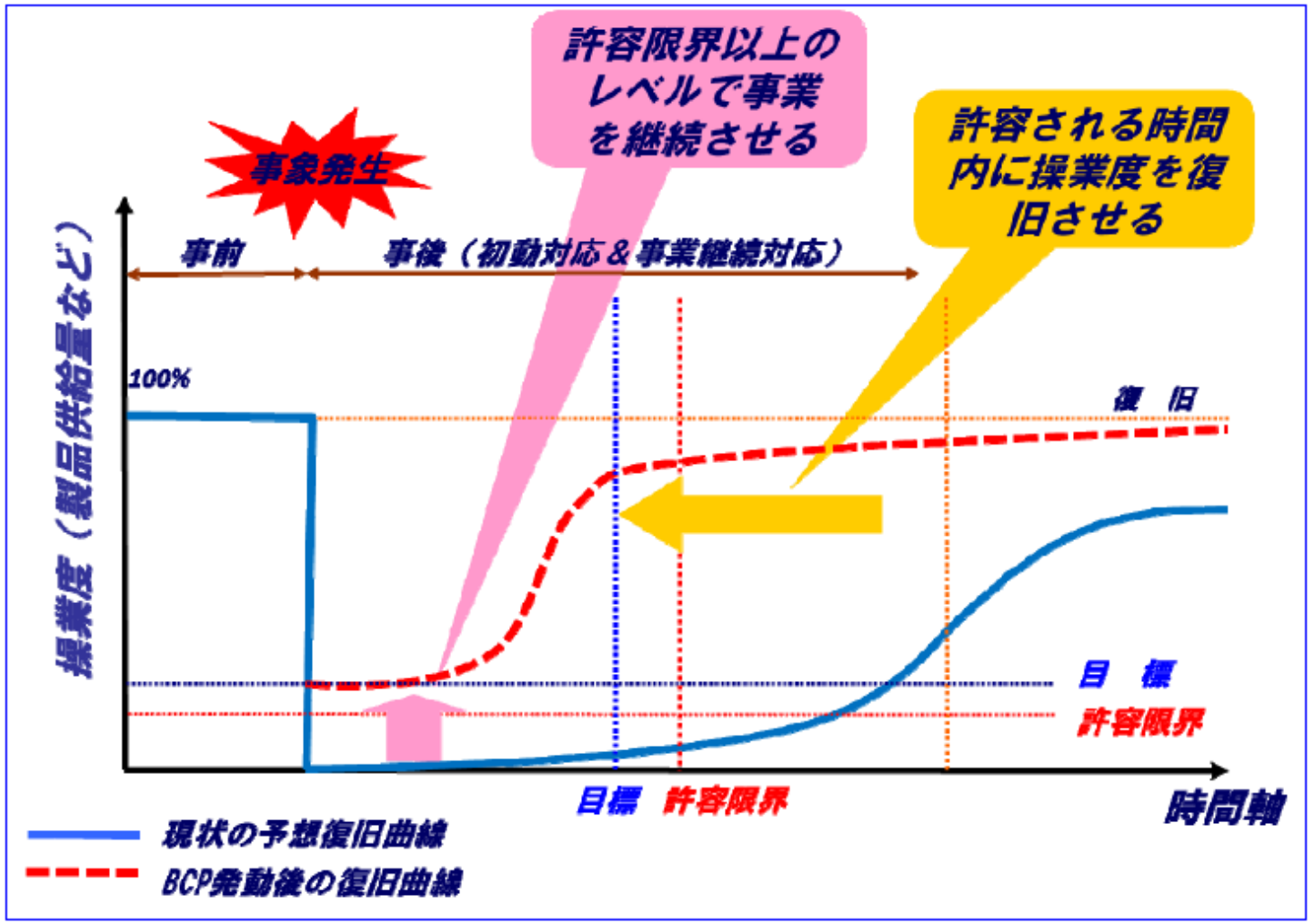


図 1.1-1-1 事業継続計画（BCP）の概念。突発的に被害が発生するリスクの場合[8]

内閣府防災情報. 事業継続ガイドライン

BCP全体におけるIT-BCPの位置付け

BCP=災害・外乱時に診療が提供され続けること

人的な診療が維持される	医療施設設備が維持される	医療IT機能が維持される
・人員が不足しても診療機能が維持される ・疾病者が急増しても診療機能が維持される ・人的組織の一部機能が停滞しても実施可能な代替ワークフローが運用できる	・施設のある装置が不全になっても機能が維持される ・設備によって提供される機能が不全になっても実施可能な代替ワークフローが提供される	・システムのあるITが不全になっても機能が維持される ITによって提供される機能が不全になっても実施可能な代替ワークフローが提供される

鳥飼幸太. サイバー攻撃に備えた医療IT-BCPの策定. 第27回日本医療情報学会春季学術大会, 2023.

サイバー攻撃を想定したIT-BCPについて

（サイバー攻撃）

- 大規模災害、**情報セキュリティインシデント**及び感染症の流行による影響等によって情報システムの運用が中断又は途絶するときに、情報システムを継続又は復旧させることにより、……

- 情報システムの停止を原因として遂行できなくなることを避けるために、必要な計画を事前策定し継続的に維持改善を行うこと、危機的事象発生時に同計画に沿って適切に対処することは、**情報システム担当者の重要な役割の一つ**である

内閣サイバーセキュリティセンター. 政府機関等における情報システム運用継続ガイドライン第3版

サイバー攻撃によるシステム停止は長期間の診療制限につながる…

通常診療まで約2か月かかった

https://www.handa-hospital.jp/

- 自治体の指導による災害拠点病院に対するBCPの策定と訓練は実施されたため、
  病院基幹システムが機能しない状態での事業継続は適切に実践されたが、
  サイバー攻撃によるリスクは想定されていなかった

コンピュータウイルス感染事案有識者会議調査報告書. 徳島県つるぎ町立半田病院, 2022.

サイバー攻撃対応のためのBCPを普及させる必要がある

本日の内容の基礎資料

- 厚生労働省科学研究
  - 群馬大学　鳥飼幸太 先生、　大津赤十字病院　橋本智広 先生　（分担研究）

医療機関におけるサイバー攻撃に対するIT-BCP策定モデル

- NIST CSF / CISA CDMから、備え、インシデント対応、復旧を中心に記述

https://www.ipa.go.jp/security/reports/oversea/nist/about.html

https://www.cisa.gov/cdm

サイバー攻撃を想定したIT-BCPチェックリスト（厚生労働省 2024/6/6）

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

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）

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］

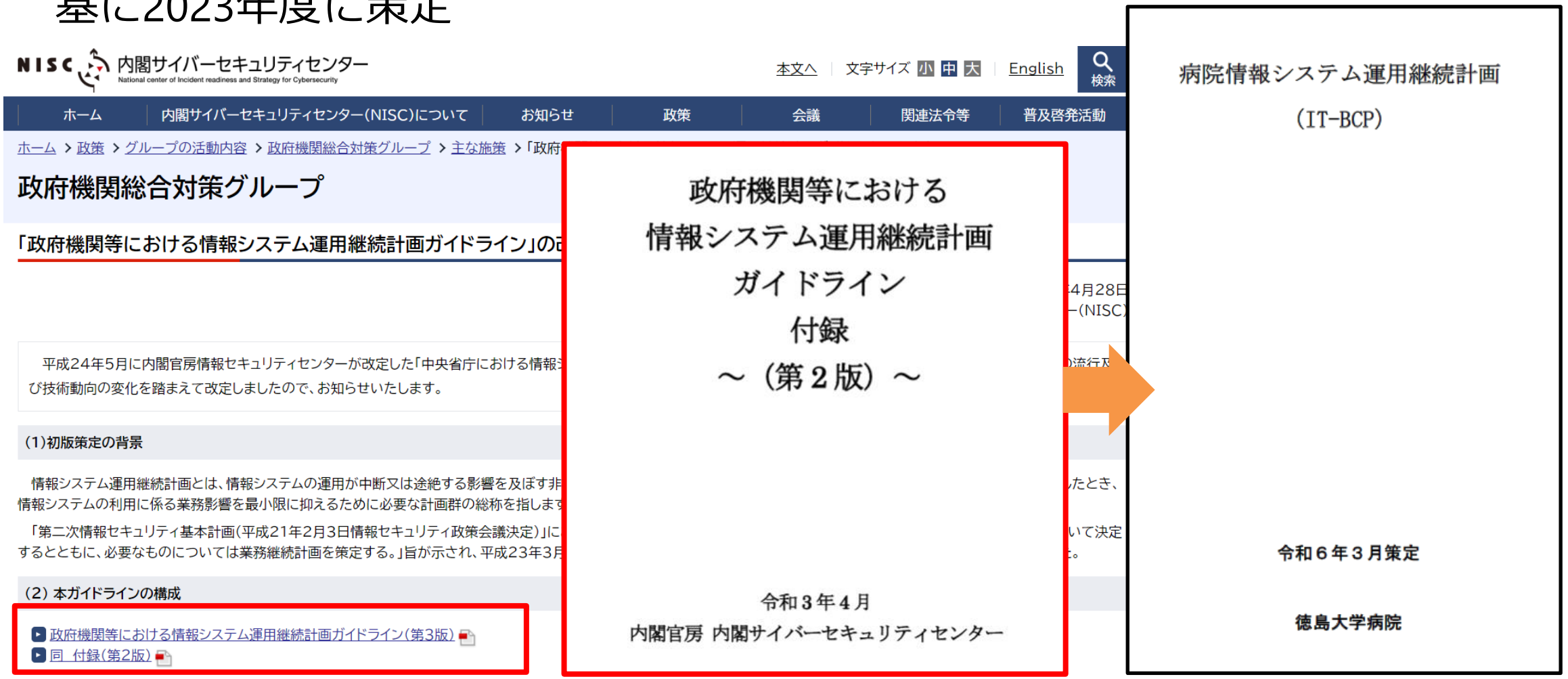
サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※医療機関がBCPを策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです
※BCP策定や見直しの際にご活用ください

項番	大項目	確認項目	確認欄
1	平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）		
1-1	情報機器等の把握と適切な管理、全体構成図の作成	サーバ、端末PC、ネットワーク機器を把握できているか。	
		ネットワーク構成図・システム構成図が整備できているか。	
		システム停止が事業継続に与える影響を把握できているか。	
		サーバ、端末PC、ネットワーク機器の脆弱性への対応ができているか。	
1-2	非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集	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）への連絡体制図が整備できているか。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	
2	検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）		
2-1	システム異常の報告先の把握	異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。	
2-2	システム異常の検知	院内で発生した異常が院内職員によって覚知できるか。	
2-3	CSIRT/経営者によるシステム異常の覚知	院内職員から発出されたサイバー被害情報が組織を通じて速やかにCSIRT（対応者）ならびに意思決定者まで到達するか。	
3	初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）		
3-1	原因調査（必要に応じて事業者に依頼）	原因調査のため、「ネットワーク機器やケーブル等の調査」「電源系統、ブレーカー、ハードウェア、ソフトウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。	
3-2	事業者等への連絡と作業履歴の確認	事業者等への連絡と作業履歴の確認ができるか。	
3-3	被害拡大防止	被害拡大防止に向けた対応ができるか。	
3-4	経営層への報告、経営層による確認と指示、組織内周知と対応	経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。	
3-5	被害状況等調査（フォレンジック調査＋証拠保全）と被害状況等の報告	被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。	
3-6	組織対応方針確認と外部関係機関への報告等の対応	組織対応方針を確認できるか。また、外部関係機関への報告ができるか。	

徳島大学病院におけるIT-BCP策定の取組み

- NISCの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付録を基に2023年度に策定



https://www.nisc.go.jp/policy/group/general/itbcp-guideline.html

IT-BCP策定の
チェックリスト

IT-BCP策定のチェックリスト

1. 平時：　サイバーセキュリティの体制整備
2. 検知：　障害時、早期に医療情報システム部門へ報告し、異常内容を確認
3. 初動対応：　サイバー攻撃による被害拡大の防止や診療影響を最小限に
4. 復旧処理：　医療情報システムの事業者等と協力して復旧
5. 事後対応：　再発防止に向けた検討と再発防止策の周知と実施

1．平時

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表

※医療機関がBCPを策定する際、最低限必要な事項を網羅しているか、確認のために使用するものです

※BCP策定や見直しの際にご活用ください

項番	大項目	確認項目	確認欄
1	平時（平時において、非常時に備え、サイバーセキュリティの体制整備を行う。）		
1-1	情報機器等の把握と適切な管理、全体構成図の作成	サーバ、端末PC、ネットワーク機器を把握できているか。	
		ネットワーク構成図・システム構成図が整備できているか。	
		システム停止が事業継続に与える影響を把握できているか。	
		サーバ、端末PC、ネットワーク機器の脆弱性への対応ができているか。	
1-2	非常時に備えたサイバーセキュリティ体制の整備とリスク検知のための情報収集	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）への連絡体制図が整備できているか。	
		リスク検知のための情報収集体制が整備できているか。	
		教育訓練が実施できているか。	
		バックアップの実施と復旧手順が確認できているか。	

1-1 サーバ、端末PC、ネットワーク機器を把握できているか

- 院内のサーバおよび端末PCのOS、IPアドレス、使用用途、脆弱性対応状況、ウイルス対策ソフトの稼働状況等の一覧を整備しておく
- 各PCにログオンする際に管理者権限でログオンするPCが分かるようにしておく
- 院内設置のすべてのVPN装置、ファイアウォール、ルータ等の所在と、IPアドレス、使用用途等を明記した一覧を作成する

1-1 ネットワーク構成図・システム構成図が整備できているか

- HIS系、インターネット系等の院内LAN、外部接続点（ファイアフォール、VPN、地域連携、オンライン資格確認等）のネットワーク構成が判別できるようにIPアドレスおよびルーティングがわかる構成図を整備しておく

表◯：情報機器台帳（例）

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（出典：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～ ）

情報機器の一覧を作ることではなく把握することが目的

- 情報機器の外部接続点に関する確認事項

I. 院内ネットワークへ接続する場合

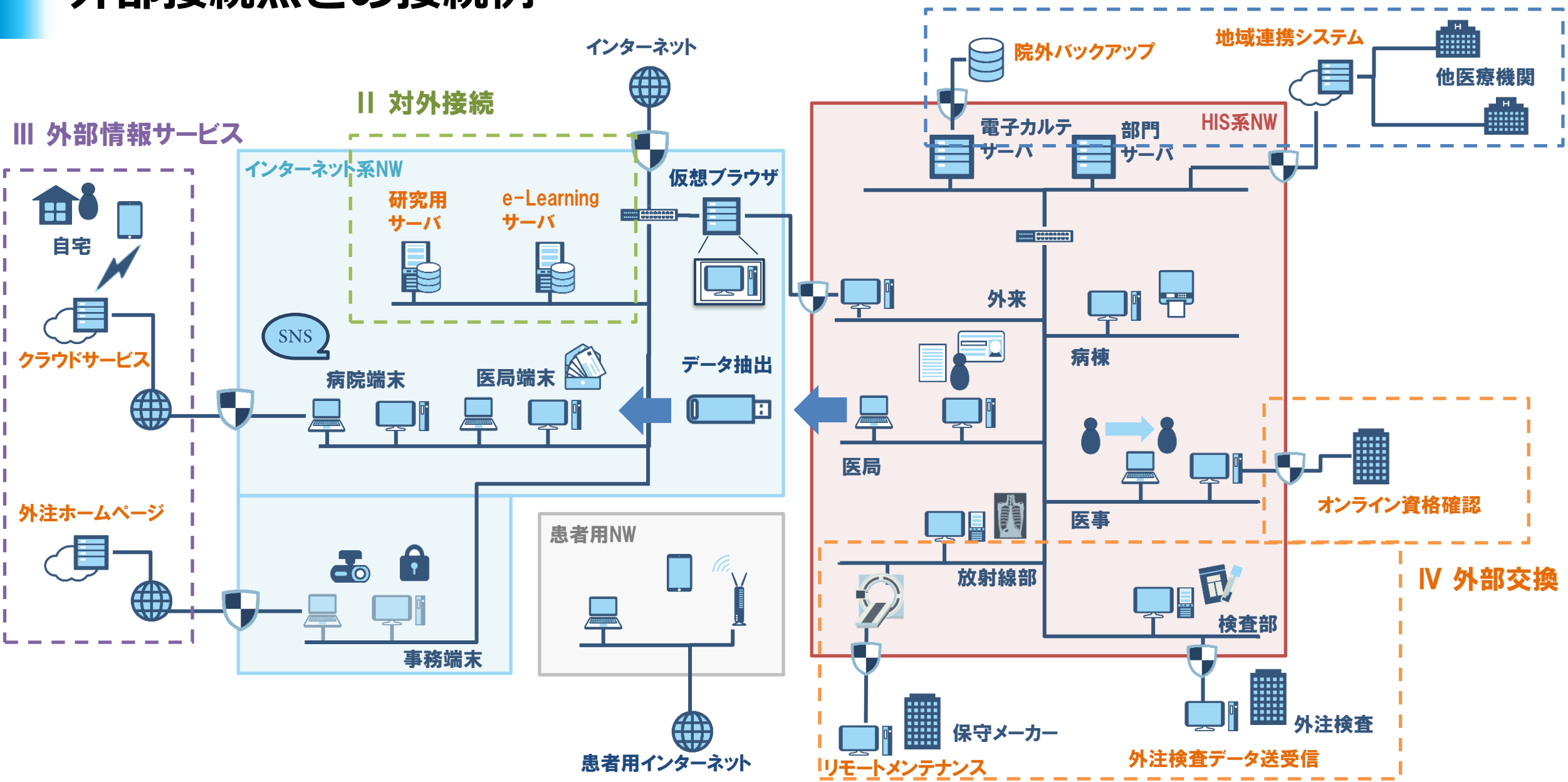
II. 対外接続ネットワークへさらに接続する場合

III. 外部情報サービスを利用する場合

IV. システムで医療情報の外部交換をする場合

V. 医療情報の外部保存をする場合

外部接続点との接続例


V 外部保存
院外バックアップ
地域連携システム
他医療機関
インターネット
II 対外接続
III 外部情報サービス
電子カルテ
サーバ
部門
サーバ
HIS系NW
インターネット系NW
研究用
サーバ
e-Learning
サーバ
仮想ブラウザ
自宅
外来
SNS
病棟
クラウドサービス
病院端末
医局端末
データ抽出
医局
外注ホームページ
オンライン資格確認
医事
患者用NW
放射線部
検査部
IV 外部交換
事務端末
保守メーカー
外注検査
患者用インターネット
リモートメンテナンス
外注検査データ送受信

情報機器のネットワーク接続に関する確認事項

1-1 システム停止が事業継続に与える影響を把握できているか

- 各システムが利用できなくなると、どの業務が継続できなくなるか（検査部門システムの場合、検査の受付と検査結果の電子カルテ送信ができなくなる等）といった被害を想定し、代替運用の手順を作成しておく

- 代替運用サーバ、参照サーバ、バックアップデータの保持といった非常時対策状況を確認しておく

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生直前のデータを保全している。	4
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。	
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。	
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。	

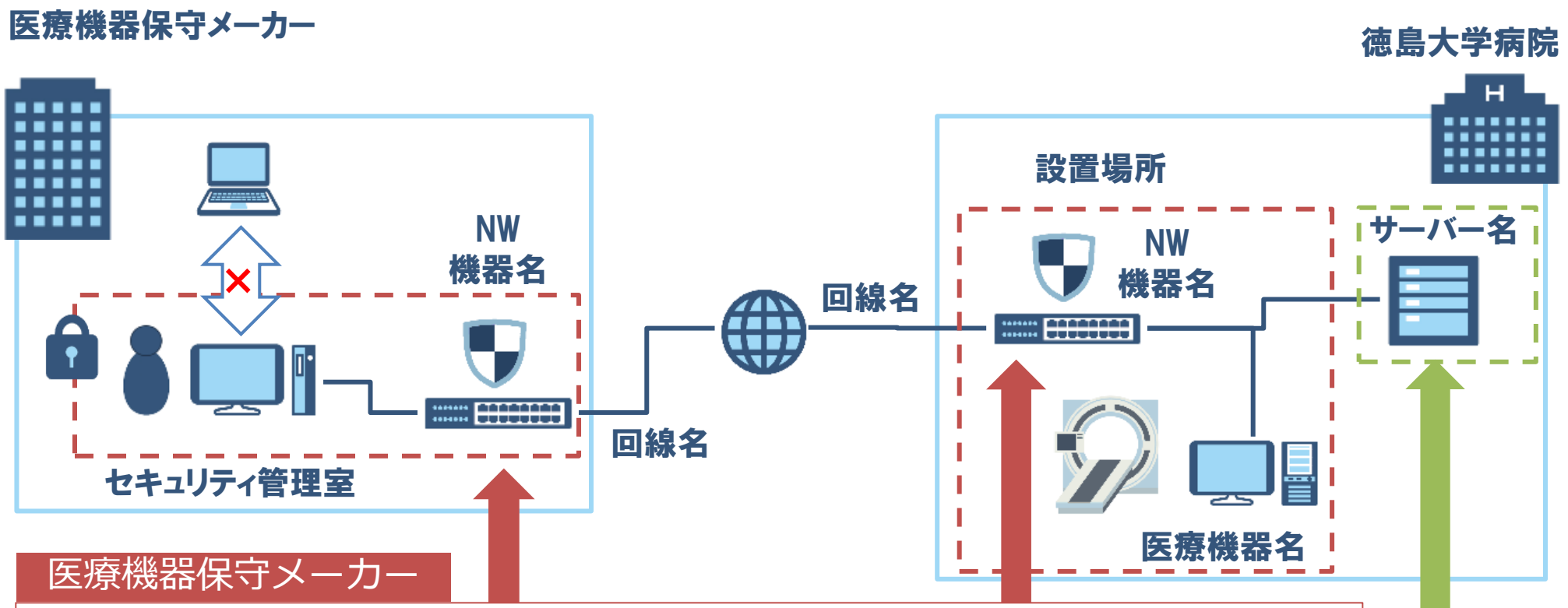
表 5.4-2 病院情報システムの復旧優先度に対応する対策目標

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）	1

1-1 サーバ、端末PC、ネットワーク機器の脆弱性への対応ができているか

- サーバ、端末PC、ネットワーク機器について、病院が管理する機器と、事業者が管理する機器を明確化し、脆弱性情報の収集、脆弱性対応プログラムの適用基準等を定めておく

脆弱性プログラム更新と責任分界点の把握



医療機器保守メーカー

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について

最終更新: 2020-11-27

システム保守メーカー

Netlogon の特権の昇格の脆弱性 (CVE-2020-1472) への早急な対応を

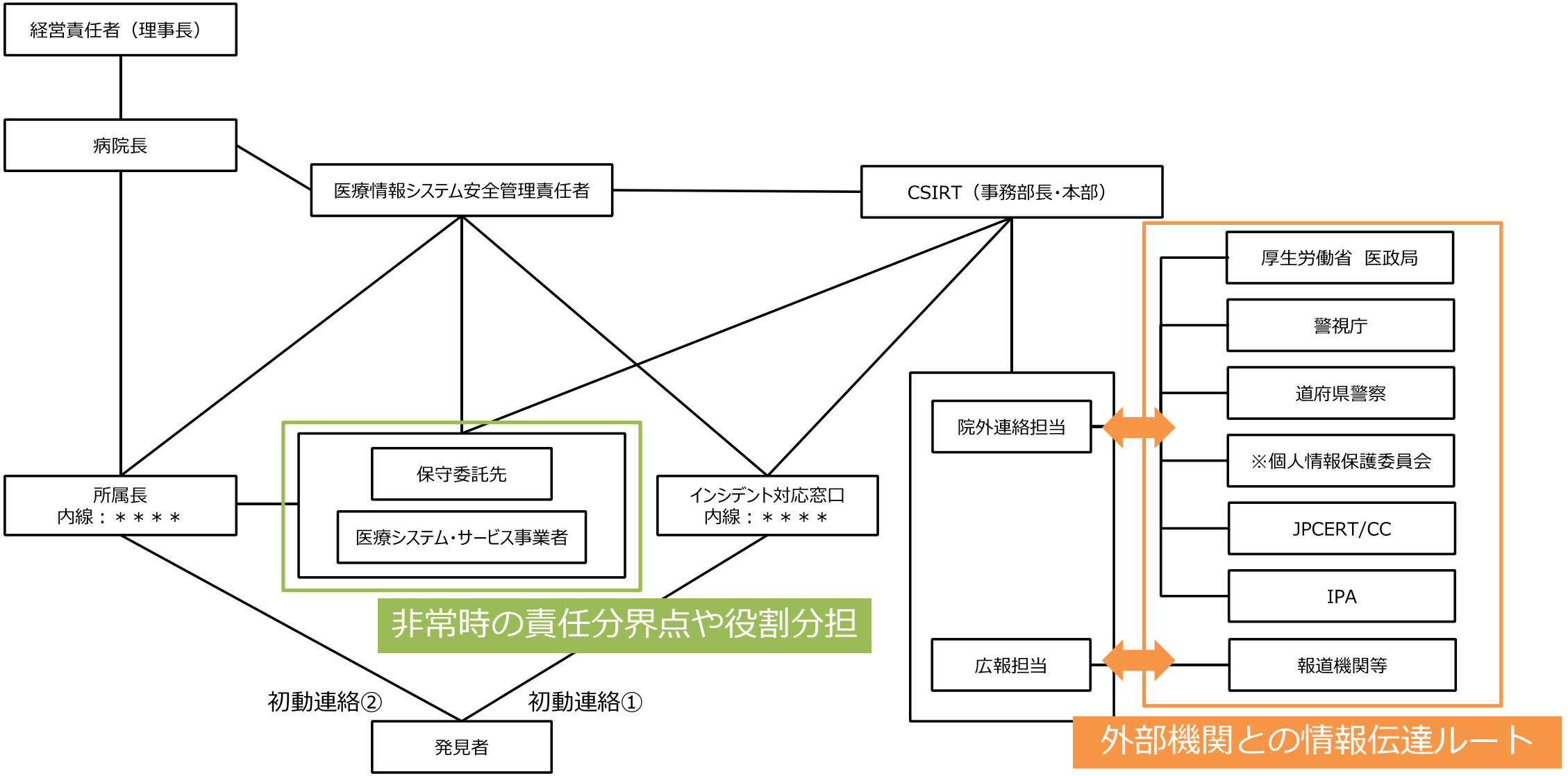
最終更新: 2020-09-25

1-2 インシデント発生時における組織内と外部関係機関への連絡体制図が整備できているか

- 非常時の役割や手順を定め、医療機関の内部や外部関係機関との緊急連絡先や情報伝達ルートを整備し関係者へ周知しておく

- 契約書やサービス・レベル合意書(SLA）により、非常時の責任分界点や役割分担について事業者等との明示的な合意内容を確認しておく

医療機関の内部や外部関係機関との情報伝達ルート



※ 個人情報の漏洩が疑われる場合

1-2 リスク検知のための情報収集体制が整備できているか

- 自医療機関に重要な脆弱性情報が事業者から報告されるスキーム（保守契約等）を確立しておく

- ファイアウォール、VPN等外部接続点のアクセスログを定期的に確認する体制を整備しておく

サイバーセキュリティに関する情報共有の仕組み

- CISSMED

大会企画シンポジウム２　6月15日（土）9：00～　第1会場
医療機関のサイバー防御態勢強化に向けた情報共有
～どのような情報を我々は知り、そして発信すべきか

1-2 教育訓練が実施できているか

- 策定したBCPが迅速かつ適切に利用できるように、教育訓練を定期的に実施する
- システムが利用できなくなることを想定して、障害時マニュアルや伝票運用マニュアルを準備しておく
- 教育訓練の結果、必要に応じて改善計画を作成する。

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								○					

2022年度　重要インフラ分野におけるサイバーセキュリティ体制強化支援

機密性２情報

05.各取組の実施概要

各取組における実施概要を以下に示します。

リスクアセスメントの実施	リスクアセスメントの実施 ✓ リスクアセスメント様式を用いた事業者によるリスクアセスメント実施 ✓ リスクアセスメントの実施を専門家が支援	リスクアセスメント結果の分析 ✓ 事業者のリスクアセスメント結果を評価及び分析 ✓ 事業者に向けたフィードバックレポートを作成	成果・メリット ✓ リスクアセスメントにより、自組織のリスクを把握した上で、改善すべき点を明確化することができます ✓ 専門家からのフィードバックを踏まえた上で、今後のリスク対応計画を検討することができます
インシデント報告・対処体制の整理・可視化	ヒアリングの実施 ✓ 事業者が作成した体制図及び対応フローを参照した上で、事業者へのヒアリング実施	ヒアリング結果の整理 ✓ 事業者のヒアリング結果を整理 ✓ 事業者に向けたフィードバックレポートを作成	成果・メリット ✓ インシデント報告対処状況のヒアリングにより、インシデント発生時における報告先を明確化した上で、対応の迅速化を図ることができます ✓ 専門家からのフィードバックを踏まえた上で、インシデント報告・対処体制を検討することができます
リスクアセスメント結果に基づく実践的な訓練の実施	訓練の実施 ✓ 訓練シナリオに基づく事業者による訓練実施 ✓ 訓練実施を事務局が支援	訓練結果の分析 ✓ 事業者の訓練結果を評価及び分析 ✓ 事業者に向けたフィードバックレポートを作成	成果・メリット ✓ 訓練により、インシデント発生時における対処能力の向上を図ることができます ✓ 専門家からのフィードバックを踏まえた上で、今後のインシデント対処に係る改善に向けた検討ができます

国立大学法人 徳島大学病院　御中

重要インフラ分野におけるサイバーセキュリティ体制強化に係る
フィードバックレポート

第 11 版

厚生労働省　政策統括官付サイバーセキュリティ担当　参事官室

2023 年 3 月 9 日

リスクアセスメントの結果

2.5　リスクアセスメントのフィードバック

2.5.1　総評

徳島大学病院が管理する「電子カルテシステム」では、ネットワーク機器やファイアウォールにより、外部ネットワークやインターネットとの通信を制御していることを確認しました。また、エンドポイントへの対策として、アンチウィルスソフトを各システムの可用性を考慮した上で一部サーバや端末へ導入していることや、ネットワーク機器による通信ログの監視を行っていることを確認しました。また、職員への情報セキュリティ研修の実施や接続可能な USB メモリの限定等、内部不正や事故を未然に防ぐ対策が講じられていることを確認しました

（1）脆弱性管理の不備

【現状】

徳島大学病院における「電子カルテシステム」の運用において、当該システムにおけるサーバ及び管理端末を対象に修正プログラムの適用状況及びバージョンアップの実施状況について定期的に点検していることを確認しました。しかしながら、実態として修正プログラムの適用や最新バージョンへの更新が未対応のサーバ及び管理端末が存在することを確認しました。また、検査機器等で用いる一部端末等において、サポートが終了したソフトウェアを継続利用していることを確認しました。

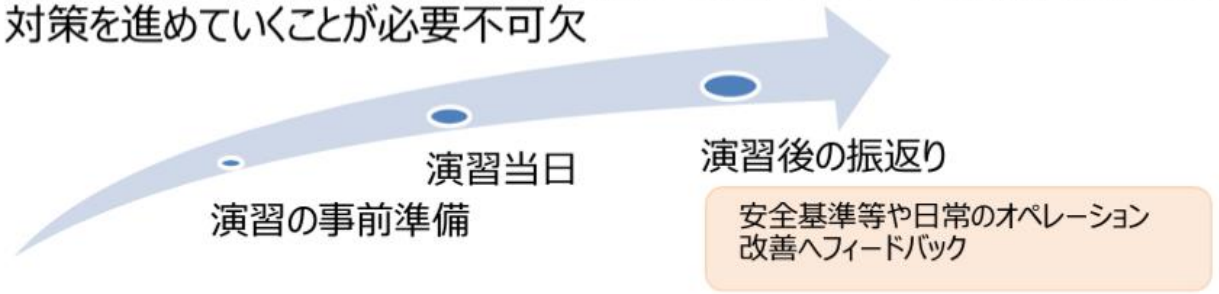
2023年度　分野横断的演習

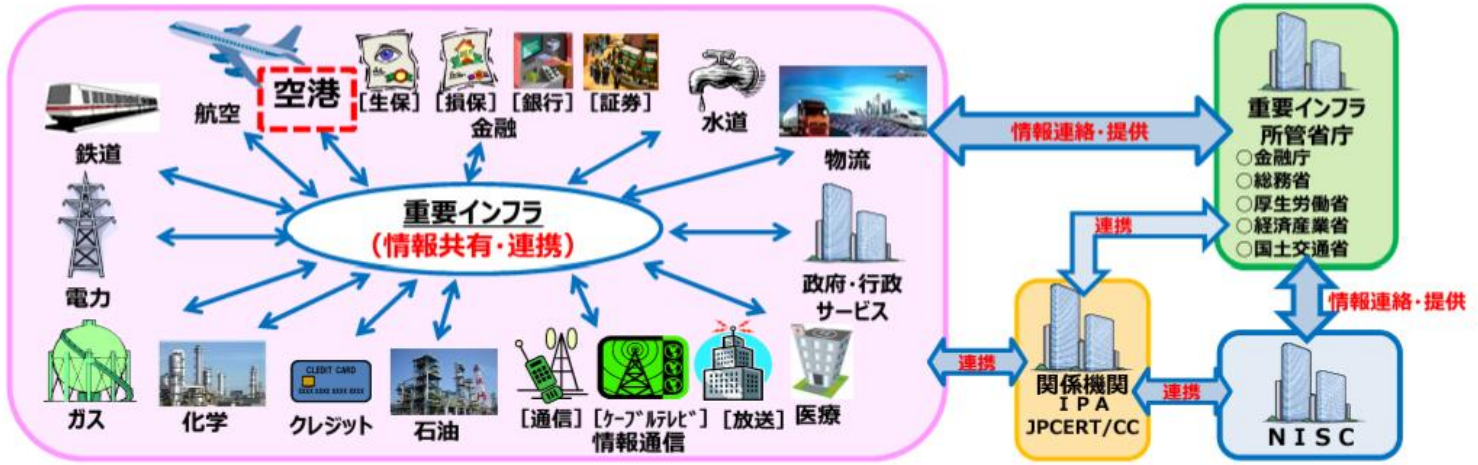
分野横断的演習の基本コンセプトと関係者

NISC

○ 演習当日における対応に加え、事前準備及び事後の振り返りにより構成

→ 演習の事前準備と事後の振返りを通じて、事業者等が365日、対策を進めていくことが必要不可欠





https://www.nisc.go.jp/pdf/council/cs/ciip/dai16/16shiryou06.pdf

演習で洗い出された課題

洗い出された課題	課題が発生した理由
資産管理リストの最新化	脆弱性を含むネットワーク機器を検索しても見つけられなかった
スムーズな連絡方法が存在しない	障害対策委員の招集に時間がかかった
伝票運用における手順が確立されていない	伝票運用の問い合わせが多かった
届出処理に時間を要した	届出様式が煩雑であり、連絡先が複数あった（提出先は統一して欲しい）
関係医療機関へ連絡ができていなかった	連絡網が存在しない
IT-BCPと障害時対策マニュアルで対応フローが重複していた	対応フローが2つあり、どちらを採用するべきか迷った
IT-BCPで想定しているトラブル内容が不十分であった	復旧まで数日かかる場合の運用が決まらなかった
患者向け院内放送とメディア対応の手順がない	患者向け院内放送とメディア対応の運用が決まらなかった
病院全体での訓練が必要と感じた	病院情報センターだけで訓練を実施した

1-2 バックアップの実施と復旧手順が確認できているか

- オフラインバックアップ等サイバー攻撃を想定したデータとシステムのバックアップの実施と復旧手順の確認をしておく

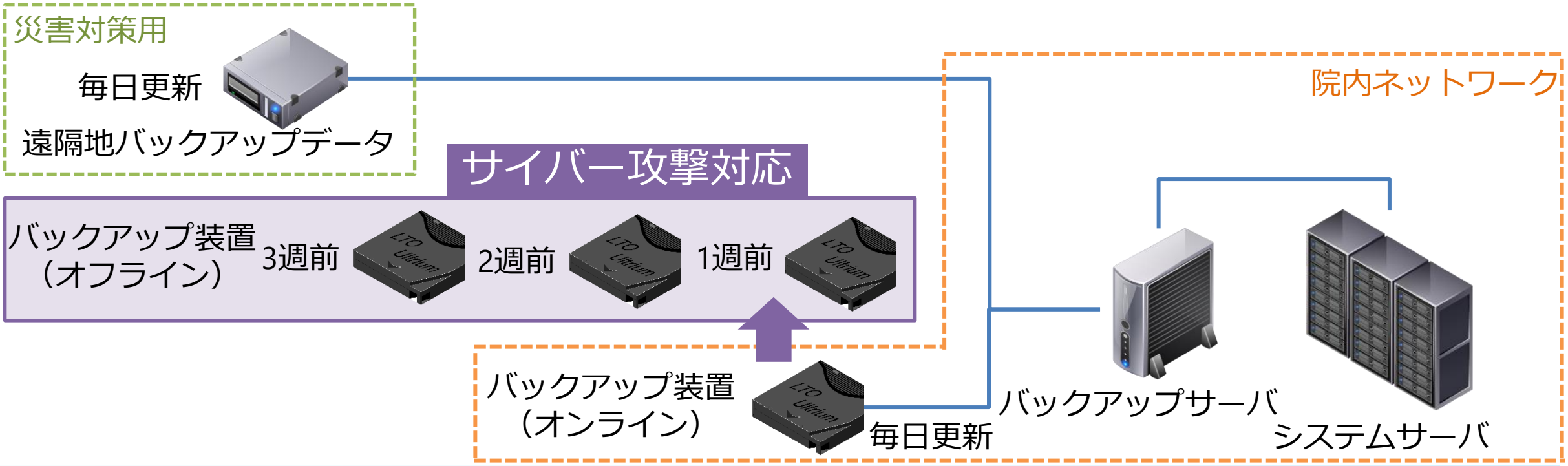
- 復旧手順においては、業務フローを意識して復旧するシステムの優先度（復旧する順序）をあらかじめ設定しておくことが望ましい

オフラインバックアップデータの確保

サイバー攻撃による大規模システム障害を考慮すれば、攻撃を直接受けることのない
オフラインのバックアップを取得しておくことこそが、医療継続の最大の切り札

- システム復旧に向けて、基幹システムのオフラインバックアップ（遠隔地テープ保存）から、電子カルテを参照できる環境を先に構築

情報セキュリティインシデント調査報告書. 大阪府立病院機構大阪急性期・総合医療センター, 2023.



ネットワークから切り離したオフライン保管

問１　「Ａ２０７」診療録管理体制加算の施設基準において、「非常時に備えた医療情報システムのバックアップを複数の方式で確保し、その一部はネットワークから切り離したオフラインで保管していること。」とあるが、厚生労働省「医療情報システムの安全管理に関するガイドライン」の「システム運用編」において「非常時に備えた通常時からの対応」の例として挙げられている「論理的／物理的なネットワークの構成分割」は、ここでいう「ネットワークから」の「切り離し」に該当すると考えてよいか。

（答）よい。なお、ネットワーク全般の安全管理措置については、厚生労働省「医療情報システムの安全管理に関するガイドライン」の「システム運用編」の「13. ネットワークに関する安全管理措置」を参照のこと。

問２　「Ａ２０７」診療録管理体制加算の施設基準において、「非常時に備えた医療情報システムのバックアップを複数の方式で確保し、その一部はネットワークから切り離したオフラインで保管していること。」とあるが、追記不能設定がなされた領域を有するバックアップ用機器又はクラウドサービスを利用し、当該領域にバックアップを保管している場合について、「ネットワークから切り離したオフラインで保管している」ものとみなしてよいか。

（答）当該機器又はクラウドサービスを用いたバックアップの特性も踏まえ、非常時にデータ復旧が可能な状態にある場合には、差し支えない。

なお、その場合、非常時におけるデータ復旧の手段や手順等について、医療情報システム・サービス事業者との契約書等に記載されているか、十分に確認されたい。

疑義解釈資料の送付について（その7）
https://www.mhlw.go.jp/content/12404000/001259608.pdf

システムの復旧優先度

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	
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
56	医事課	DPC ナビ	2	2	A
57	医事課	医学管理サポート	2	2	A
58	医事課	自動精算機システム	2	2	A
75	病院情報センター	資産管理システム	1	1	B
76	病院情報センター	仮想インターネット	1	1	B

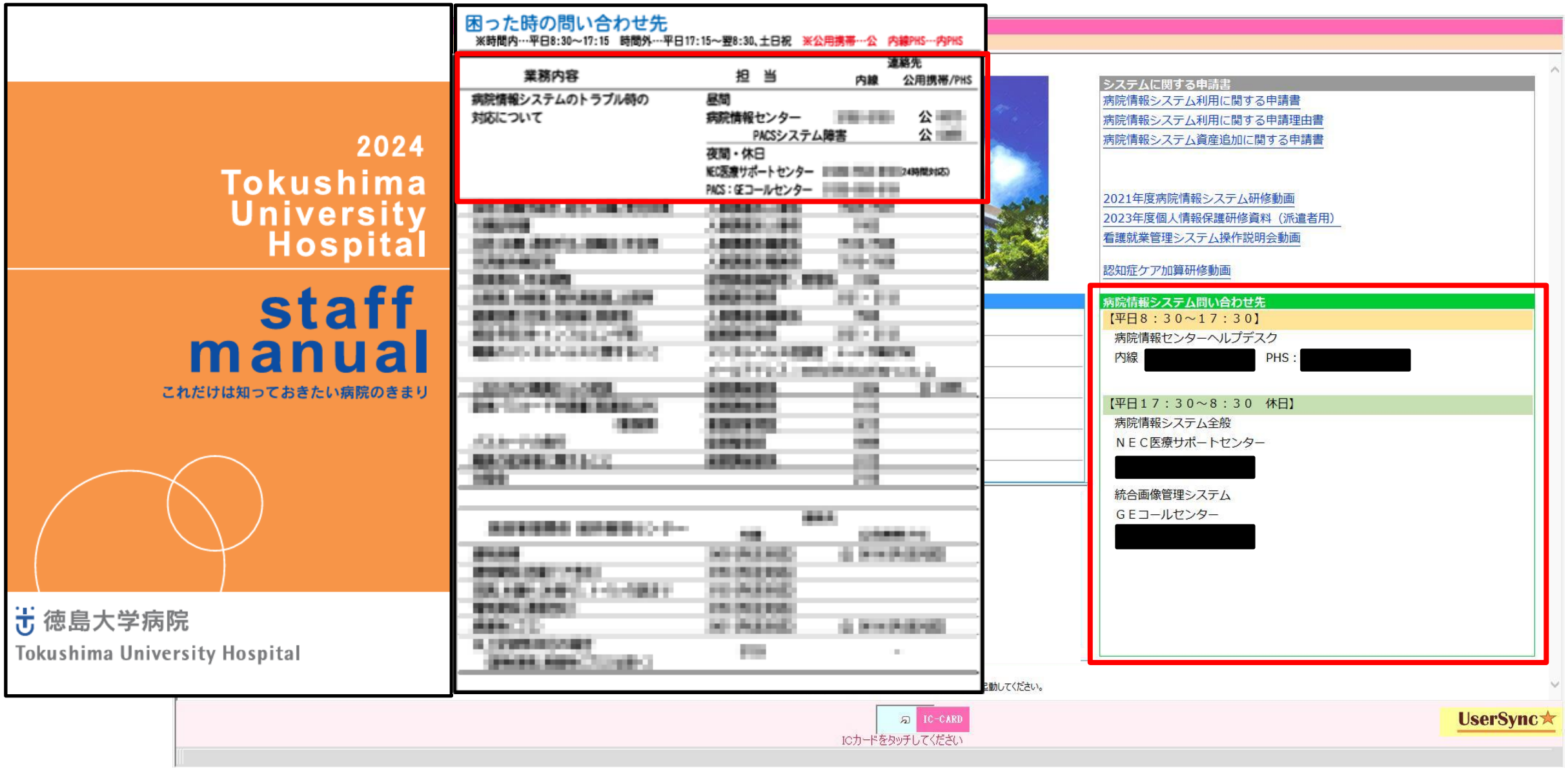
2．検知

2	検知（医療情報システム等の障害が見受けられる場合は、早期に医療情報システム部門へ報告し、異常内容の事実確認を行う。）		
2-1	システム異常の報告先の把握	異常時の連絡体制図が全職員に把握されているか。また、連絡先等を速やかに取得できるか。	
2-2	システム異常の検知	院内で発生した異常が院内職員によって覚知できるか。	
2-3	CSIRT/経営者によるシステム異常の覚知	院内職員から発出されたサイバー被害情報が組織を通じて速やかにCSIRT（対応者）ならびに意思決定者まで到達するか。	

2-1 異常時の連絡体制図が全職員に把握されているか

- 相談窓口の一本化や体系化を組織内で行う
- 連絡先を院内に掲示したり、情報セキュリティマニュアルなどのわかりやすい箇所に明示する

連絡先の掲示


2024
Tokushima University Hospital
staff manual
これだけは知っておきたい病院のきまり
徳島大学病院
Tokushima University Hospital
困った時の問い合わせ先
※時間内…平日8:30～17:15　時間外…平日17:15～翌8:30、土日祝　※公用携帯…公　内線PHS…内PHS
業務内容
担当
連絡先
内線
公用携帯/PHS
病院情報システムのトラブル時の対応について
昼間
病院情報センター
公
PACSシステム障害
公
夜間・休日
NEC医療サポートセンター
PACS：GEコールセンター
システムに関する申請書
病院情報システム利用に関する申請書
病院情報システム利用に関する申請理由書
病院情報システム資産追加に関する申請書
2021年度病院情報システム研修動画
2023年度個人情報保護研修資料（派遣者用）
看護就業管理システム操作説明会動画
認知症ケア加算研修動画
病院情報システム問い合わせ先
【平日８：３０～１７：３０】
病院情報センターヘルプデスク
内線
PHS：
【平日１７：３０～８：３０　休日】
病院情報システム全般
ＮＥＣ医療サポートセンター
統合画像管理システム
ＧＥコールセンター
IC-CARD
ICカードをタッチしてください
UserSync

2-2 院内で発生した異常が院内職員によって覚知できるか

- 発生部署、発生個所、発生日時、連絡者、異常の状態について、口頭、状況の印刷、リモート接続などを用いて正確に伝達する

システムを利用した異常検知

- 例：NDR(Network Detection and Response)

アラート名	検知内容
Concern Index	疑わしいトラフィックを生成
Target Index	疑わしい振る舞いをするトラフィックの標的
Recon	偵察行為
C&C	C&Cサーバとの通信
Exploitation	マルウェアの拡散等の攻撃
DDoS Source	DDoS攻撃の送信元
DDos Target	DDoS攻撃の標的
Data Hoarding	データの大量ダウンロード、内部情報漏えい行動
Exfiltration	外部へのデータ漏えい
Policy Violation	ポリシー違反
Anomaly	その他の動作異常

異常検知の事例

- ICMP Flood
- 端末一覧に存在しないIPアドレスの機器からネットワーク機器へのICMPパケットが多く出ている

問題点の確認

システム管理者が把握できていない新規クライアント端末？が設置？

不明機器はネットワーク作業用でメーカ持ち込み端末、作業終了後は検出されていない

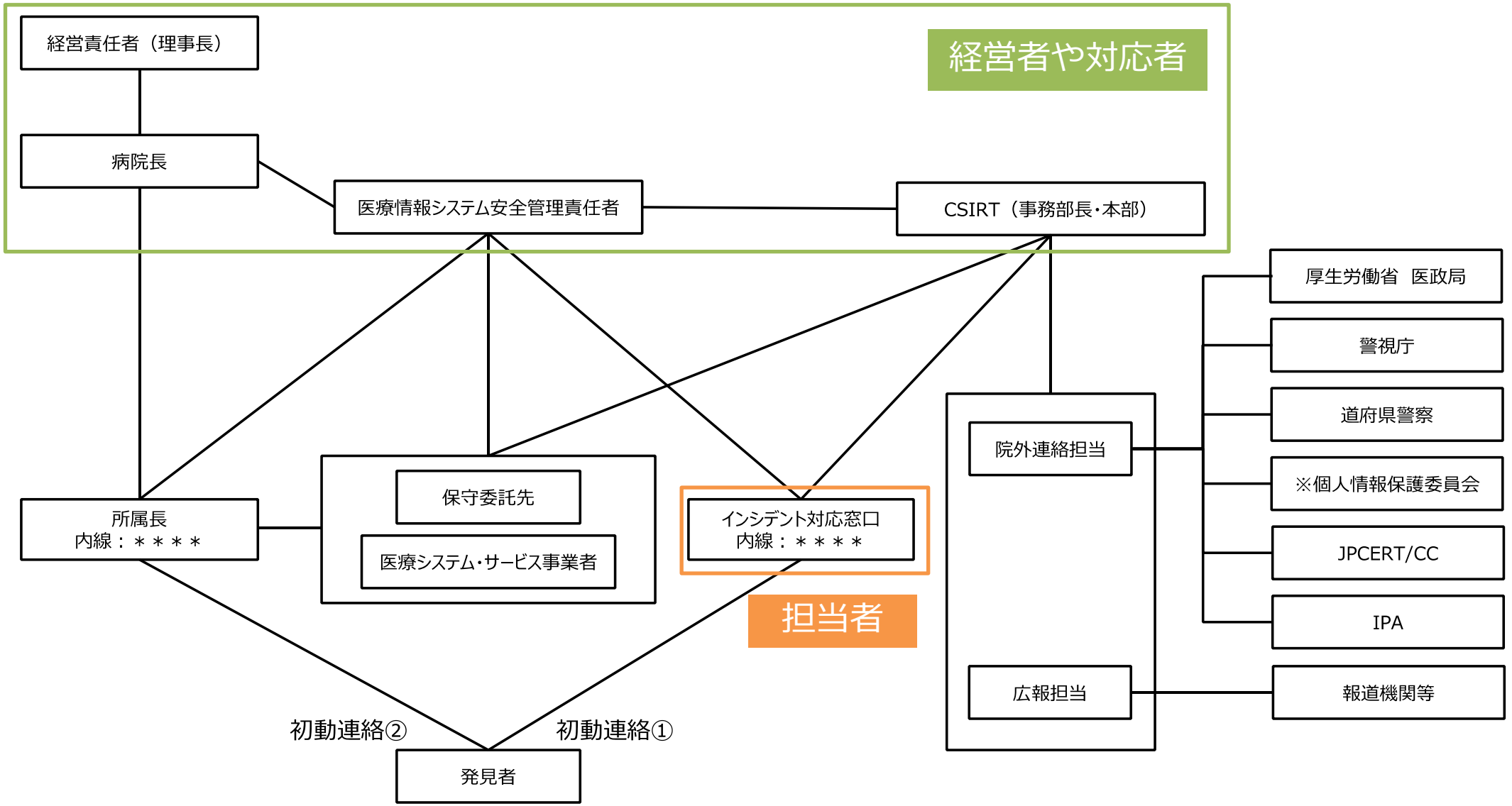
田木真和ら. NetFlowデータを活用した院内通信の可視化と自動解析アラート機能検証によるセキュリティ対策評価. 第39回医療情報学連合大会, 2019.

2-3 被害情報が組織を通じて速やかにCSIRTならびに意思決定者まで到達するか

- 連絡経路を組織化し、院内のどの部署から生じたシステム障害であっても、CSIRT（対応者）と経営者に必ず伝達されるように連絡リレーと担当者を整備する

- 組織変更に応じて適宜最新化し、連絡経路が機能することを担保する

医療機関の内部や外部関係機関との情報伝達ルート



※ 個人情報の漏洩が疑われる場合

病院情報システム障害時のレベル別対応

別紙

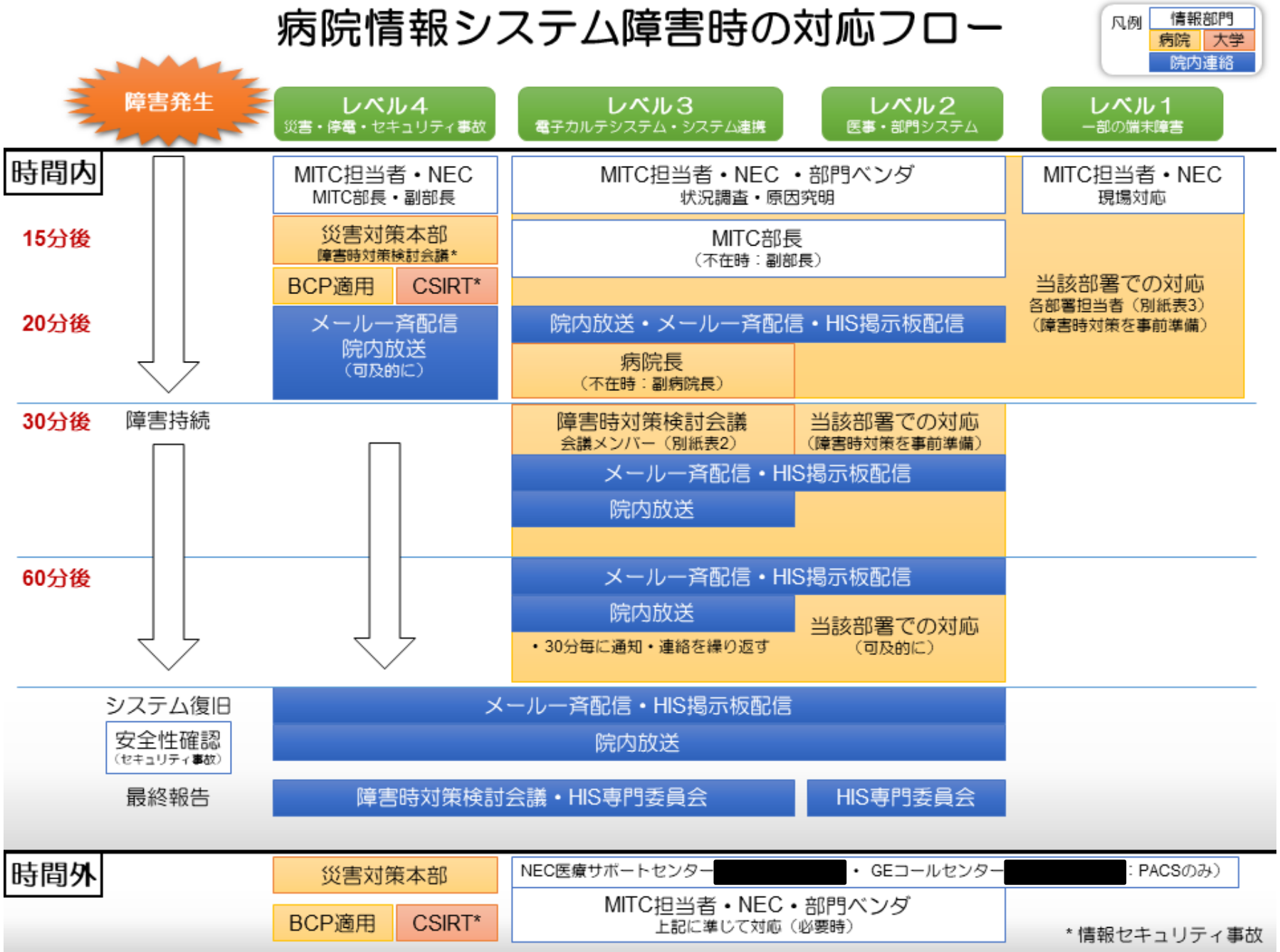
表1．障害レベルと対応

レベル	障害内容	対応
4	システム・ネットワークが全て使用不能 ■ 災害 ■ 院内の給電停止 ■ 情報セキュリティ事故（サイバー攻撃など）*	BCPを適用 CSIRTへ連絡 * 障害対策検討会議を開催 *
3	システム障害・ネットワーク障害（診療継続不能） ■ 電子カルテシステムが起動しない ■ 電子カルテにログインできない ■ システム間連携の障害（HIS端末で結果が確認できない、など）	障害対策検討会議を開催
2	システム障害（診療継続可能） ■ 医事システム障害 ■ 部門システム障害	各部署・MITCで対応
1	HIS端末の障害	各部署で対応

BCP　：事業継続計画
CSIRT：情報セキュリティインシデント対応組織（情報センター）
MITC　：病院情報センター
HIS　：病院情報システム

* 情報セキュリティ事故の場合

病院情報システム障害時の対応フロー



3．初動対応

3	初動対応（迅速に初動対応を進めて、サイバー攻撃による被害拡大の防止や診療への影響を最小限にする。）		
3-1	原因調査（必要に応じて事業者に依頼）	原因調査のため、「ネットワーク機器やケーブル等の調査」 「電源系統、ブレーカー、ハードウェア等の調査」等が実施できるか。また、必要に応じて事業者に依頼できる体制になっているか。	
3-2	事業者等への連絡と作業履歴の確認	事業者等への連絡と作業履歴の確認ができるか。	
3-3	被害拡大防止	被害拡大防止に向けた対応ができるか。	
3-4	経営層への報告、経営層による確認と指示、組織内周知と対応	経営層がサイバー攻撃兆候等を認める際の組織内報告を受け、医療情報システム使用中止等の指示を判断できるか。	
3-5	被害状況等調査（フォレンジック調査＋証拠保全）と被害状況等の報告	被害状況等調査（フォレンジック調査＋証拠保全）と経営層への被害状況等の報告ができるか。	
3-6	組織対応方針確認と外部関係機関への報告等の対応	組織対応方針を確認できるか。	

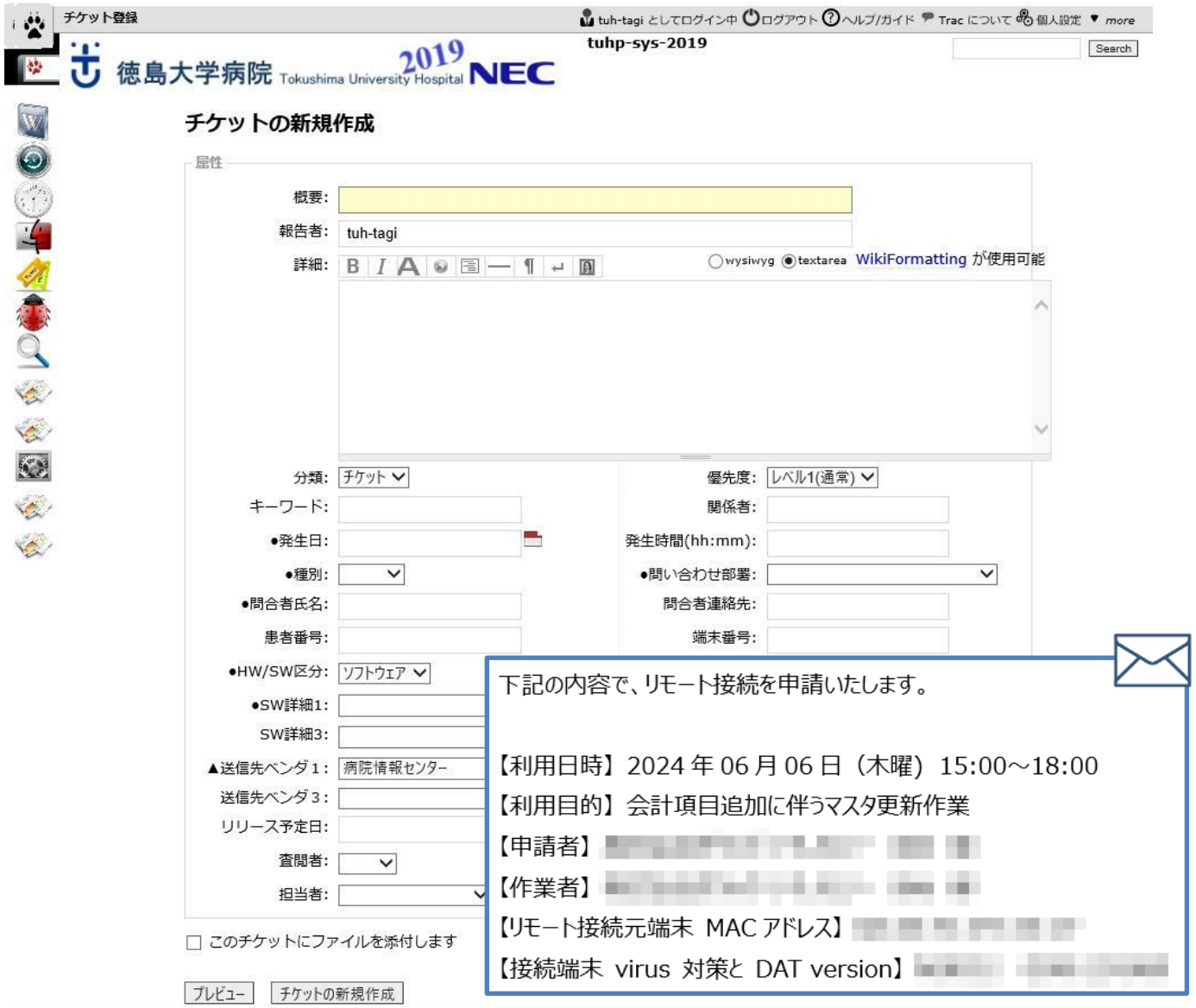
3-1 原因調査等が実施できるか

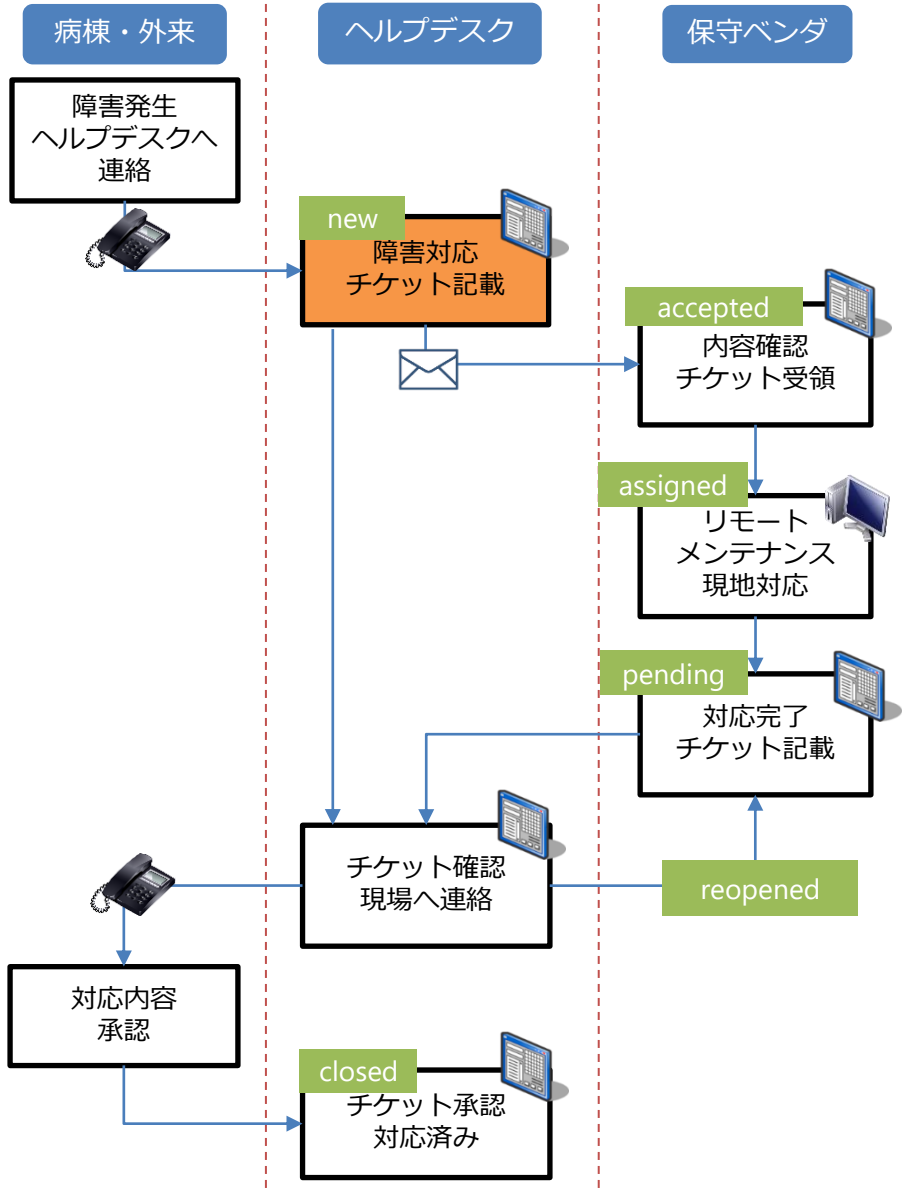
- 障害の原因としてサイバー攻撃の兆候があるか、医療情報システムのメンテナンス等の問題か、医療情報システム自体の問題か、LAN設備やケーブルの問題か、設備の電源系統の問題か等調査を実施する
- 情報漏えいの有無を調査する
- 必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制にする

3-2 事業者等への連絡と作業履歴の確認ができるか

- 障害の前日等に医療情報システムのメンテナンスやデータ移行等の作業の有無を確認し、該当する場合は、当該作業が障害の原因であるかを確認する

医療情報システムのメンテナンス状況の履歴管理





3-3 被害拡大防止に向けた対応ができるか

- 原因調査の結果、サイバー攻撃の兆候がある場合は、ネットワークの遮断により通信を遮断し感染拡大を防止する
- バックドアの無効化、無効にされたセキュリティ機能の復帰、攻撃された脆弱性への対応等の被害拡大防止措置を行う
- 必要に応じて医療情報システム・サービス事業者等に協力を依頼できる体制を整えておく

3-4 経営層が医療情報システム使用中止等の指示を判断できるか

- サイバー攻撃の兆候等がある場合は、経営層に報告し、対象となる医療情報システム等の使用の中止を指示する
- 経営層は、対応チーム設置、及び対象となる医療情報システム等の使用中止に伴う業務運用（診療体制等）方針について検討し、必要に応じて組織内に周知し、対応を求める
- 経営層は診療を継続する観点で「医療施設の災害対応のための事業継続計画」も参考にしながら病院全体の事業継続計画を策定する
- 対象となる医療情報システム等の異常・障害時の、診療体制、及び医療情報システム等を代替した業務運用方法（紙カルテ運用、参照系環境構築等）に関する対処についても定めておく

病院情報システム障害時の対応フロー

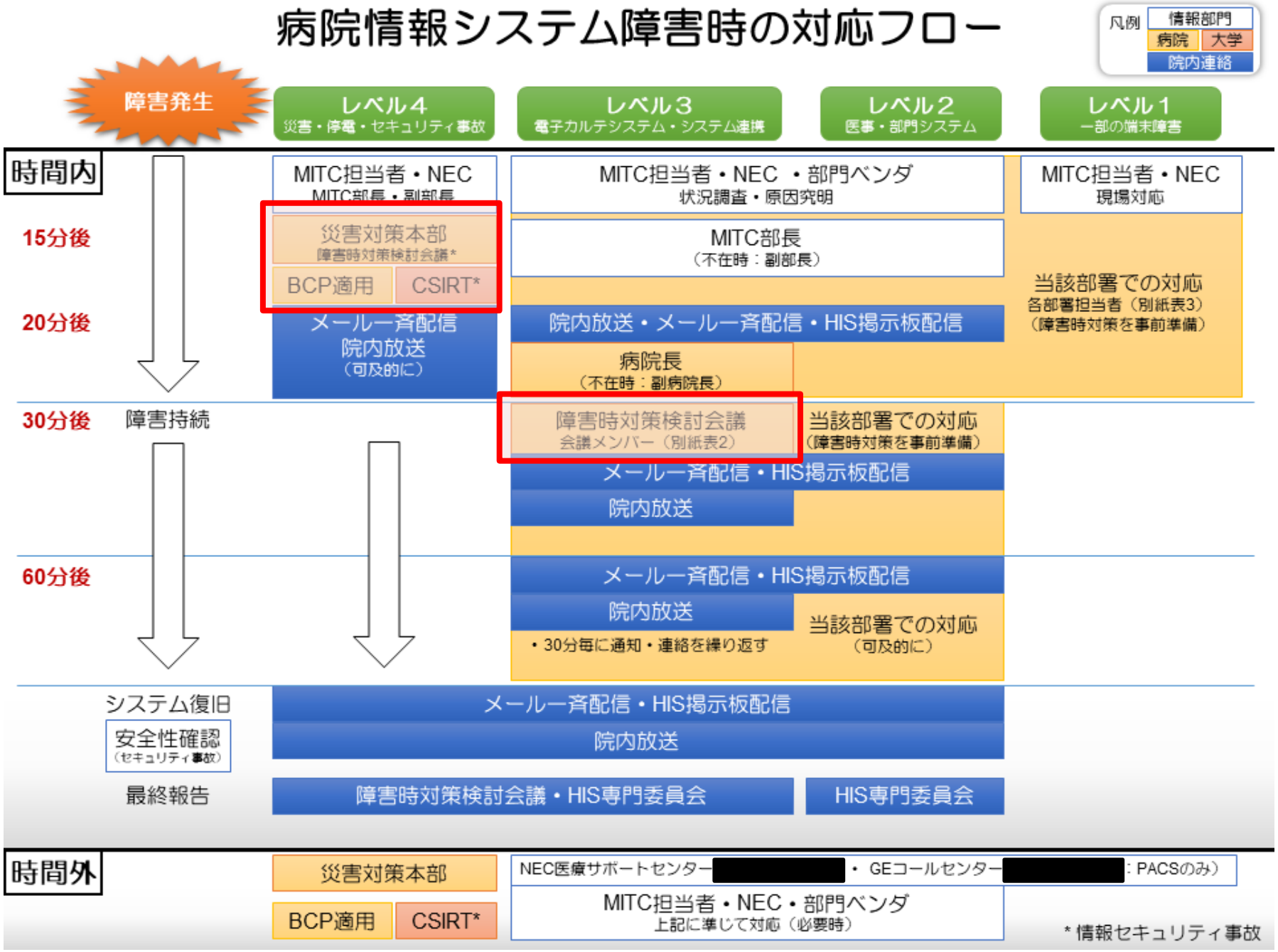
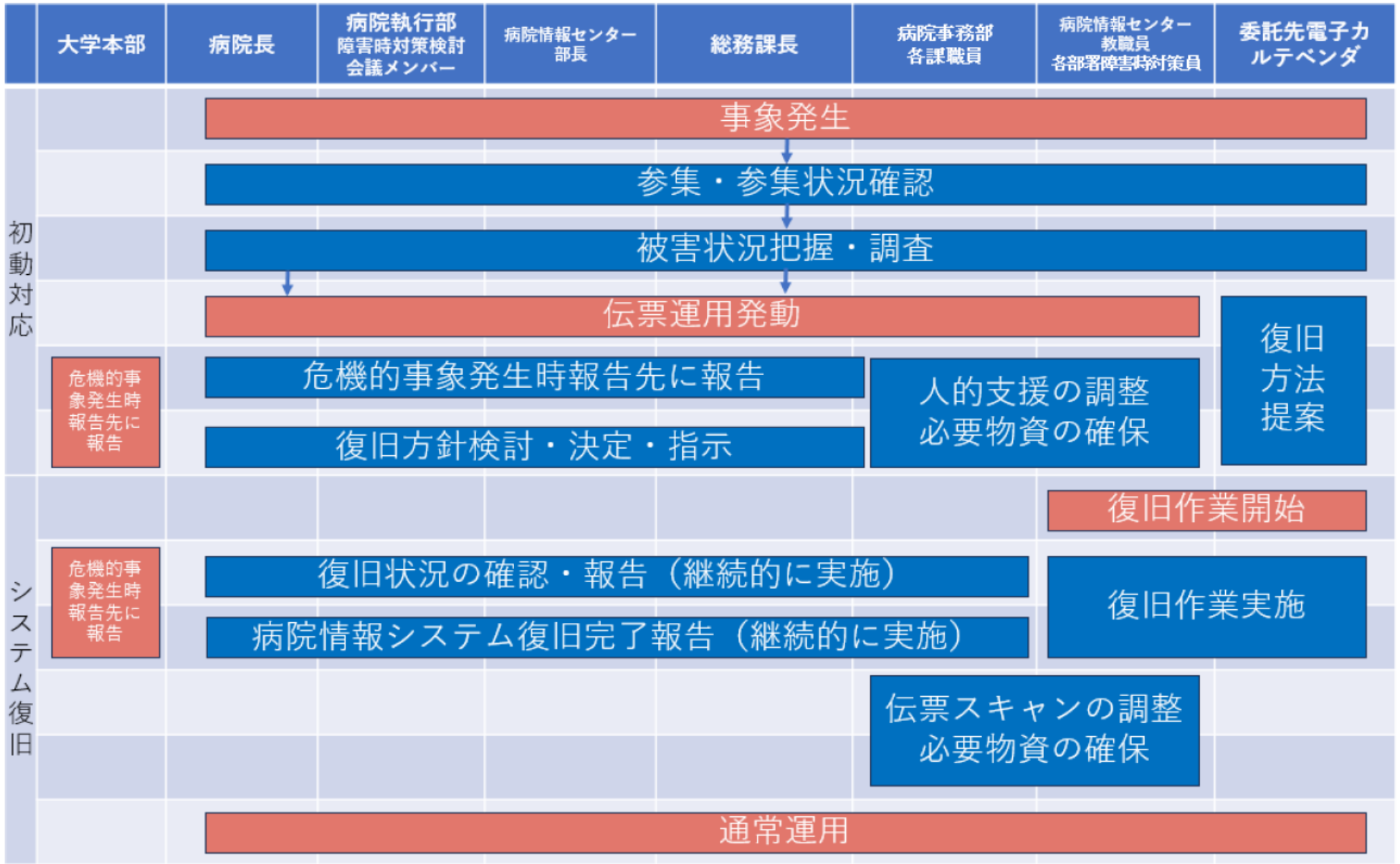


図 2.3-1 情報セキュリティインシデント発生時の全体フロー



医療情報システム等を代替した業務運用方法（伝票運用）

1．サイバー攻撃等に伴うシステム停止時の基本対応

☆本書運用期間　：　システム復旧まで
他院の事例では、数週間から3か月程度の時間を要しています。

☆停止するシステム　：　病院情報システム全般
電子カルテ、オーダリング、医事会計ほか各部門システム

☆システム停止中の基本的な対応

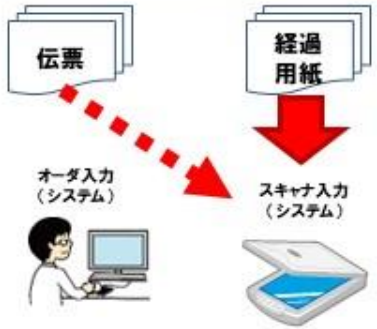
①病棟　：　注射や食事等のオーダ追加および変更は、伝票を使用し、
追加・変更内容を関連部署に電話等で連絡して対応する。
システム復旧後に伝票から画像オーダ等を後追い入力する。
スキャンの必要があるものは、病棟クラークが後日取込する。

②外来　：　受付は、手書きで会計カードを作成（会計伝票を準備）
診察室でのオーダは基本的にすべて伝票処理。（伝票を準備）
システム復旧後に伝票から画像オーダ等を後追い入力する。
スキャンの必要があるものは、外来クラークが後日取込する。

2. システム停止期間中の運用について（概要）

カルテ記載、オーダ入力、各部門の実施入力、医事会計

停止期間中の実施予定オーダを事前入力し、停止期間中の薬品、機材等を準備する。停止期間中の新規オーダとオーダ変更は伝票で運用する。システム復旧後に停止期間中の画像オーダ等を後追い入力する。
医事会計は、システム復旧後に停止期間中の画像オーダ等の取り込みおよび伝票（オーダ未入力）より、料金計算を行う。

	準備物・注意事項	システム停止期間中	システム復旧時
病棟・外来	★準備物 ・経過用紙 ・各種伝票 ・手書き用ラベル ★注意事項 システム停止前にオーダ入力していた項目については、各部門にオーダ伝達状況を確認し、伝票と重複が無いようにする。	 【病棟・外来】診察記事は経過用紙に手書き 【病棟】オーダの追加、変更を伝票に記入 【外来】オーダは、すべて伝票に記入  【病棟・外来】 伝票を各部門に搬送 検査の場合、検体も同時に搬送	 搬送された物品や検査結果で実施（病棟・外来） 【各部門】 伝票により各部門から物品や検査結果を搬送	 **入退院調整・食事の入力完了後、全システム運用再開** 【外来】停止期間中の新患登録を医事課等事務が行う。 【病棟・外来】 伝票を基に画像オーダ・処置（歯科）オーダ・指示コメントを新システムに入力。パスのステップ適用（医師） 経過用紙等は、スキャナ取り込みを行う。
各部門	システム停止までに届いたオーダを確認し、伝票との重複が無いよう注意して実施準備を行う。（病棟分）	システム停止前の入力オーダおよび搬送された伝票に基づき、検査の実施、物品の準備、食事の配膳等を行う（外来・病棟分）	後追い入力されたオーダに基づき、停止期間中のオーダ実施入力を行う。（外来・病棟分） 停止期間中のオーダ取り込みおよび伝票より、料金計算を行う。（医事課）

3-7.【入院】処方オーダの運用

	準備物・注意事項	システム停止期間中	システム復旧時
病棟	処方箋等 【病棟】処方箋の必要部数をSPDに依頼し受け取る。	処方箋等 【医師】処方箋を手書き ※参照端末を利用し、薬の検索が可能。 参照端末を利用して、処方薬の検索が可能	処方箋等 医事課 スキャナ入力 （病棟クラーク、スキャン室） スキャン室に送付 もしくは 補助診療録に貼付 （病棟クラーク）
薬剤部		処方箋等 【薬剤部】「処方箋」を基に対応し、投薬用薬品と院内処方箋の薬袋用を病棟へ	【病棟クラーク、スキャン室】 院内処方箋の薬袋用を、スキャナ入力。 院内処方箋の薬袋用は、補助診療録に貼付。 【医事課】 処方箋等の会計用を、薬剤部に取りに行く。

使用伝票等

（緊急用）院内処方箋

麻薬処方箋

特定生物由来製品・血液製剤処方箋

特定生物由来製品使用説明および同意書

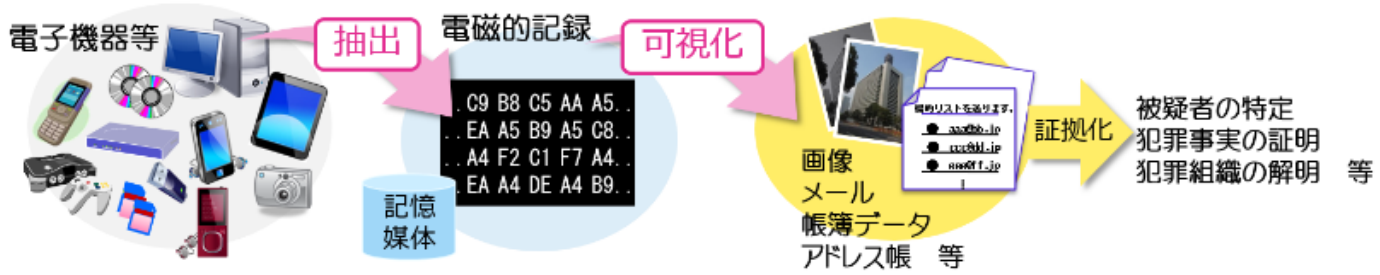
3-5 被害状況等調査と経営層への被害状況等の報告ができるか

- アクセスログの分析や情報の改ざんや暗号化の有無等からサイバー攻撃の範囲、個人情報漏洩の有無等について調査（フォレンジック調査＋証拠保全）し、経営層へ報告する
- 必要に応じて、事業者へ協力を依頼して調査を進める
- 自機関で証拠保全が可能か検討し、困難な場合は事業者等へ依頼する。経営層へ被害状況等を適時報告する
- あらかじめ初動対応の流れについて事業者等と事前に確認しておくこと

デジタル・フォレンジック

電磁的記録は、犯罪捜査において重要な客観証拠となる場合がある一方で、消去、改変等が容易であるため、これを犯罪捜査に活用するためには、適正な手続きにより解析・証拠化することが重要です。警察では、デジタル・フォレンジック（注）を活用し、電子機器等から電磁的記録を抽出したうえで、文字や画像等の人が認識できる形に変換するという電磁的記録の解析を行っています。

注：犯罪の立証のための電磁的記録の解析技術及びその手続き



https://www.npa.go.jp/bureau/cyber/what-we-do/digitalforensics.html

付録資料

A. チェックシート（PCの場合）

No.	確認項目		写真	チェック
1	[事前準備] 複製保存用の HDD/SSD を用意する。事前に、ワイプ処理、HDD/SSD 複製装置がサポートする形式でフォーマットしておく。			□
2	使用する機材の時計を日本標準時刻に合わせる。			□
3	作業開始の前に、作業場所で、立会人と作業員の写真を撮影(ケース番号、当日の新聞をもって撮影)する。		○	□
4	PC のシリアル番号などの固体識別番号を記録、写真撮影する。		○	□
5	電源 ON の場合	OS のシステム時刻を記録する。	○	□
6		(必要に応じて) 画面やプリンタなど出力装置に表示・出力されている情報を記録する。	○	□
7		(必要に応じて) メモリなど揮発性情報を記録・保存する。		□
8		電源を OFF にする。Windows の場合は、電源プラグを抜いて強制的に電源を OFF にする。		□
9	帯電防止リストバンドの使用、帯電防止手袋の着用、帯電防止マットの準備等、静電気による機材の破損が無いように考慮する。			□
10	UPS を用意するなど、電源のトラブルにより HDD/SSD 複製作業に影響が無いように配慮する。			□
11	PC に電源等のケーブルが接続された状態であれば、ケーブルのラベリングをして撮影後、取り外す。		○	□
12	PC 本体から、原本 HDD/SSD の取外しを行う前に、HDD/SSD 自体に暗号化機能がある型番でないか確認する。		○	□

1-4. 想定読者

インシデントが検知されたまたは発覚した現場において、即座に実施する被害拡大等のための対処やコンピュータ等を対象とした電磁的証拠の保全作業にあたる「ファースト・レスポンダ」をはじめとした、デジタル・フォレンジック関連技術を活用するすべての方々が利用可能なものとしている。

本ガイドラインにおける「インシデント」および「ファースト・レスポンダ」の定義は、次のとおりである。

- インシデント：情報の機密性、完全性または可用性を毀損する行為やソフトウェアの脆弱性を攻略する行為や手段(Exploit)による侵害等、デジタル・フォレンジックの対象となる事案のこと。具体的には、コンピュータやネットワーク等の資源および環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為(事象)等を指す。
- ファースト・レスポンダ：「デジタル・フォレンジックに関する専門的な技能や豊富な知識を習得しているとは限らないが、専門事業者または捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」としている。

特定非営利活動法人デジタル・フォレンジック研究会. 証拠保全ガイドライン第9版

3-6 組織対応方針を確認できるか

- 被害状況（診療継続への影響や個人情報漏洩への有無等）に基づいた経営層による対応方針を確認し、対応する

- 被害状況について所管省庁への報告、法的措置、機密情報漏洩等の対応を確認して報告する

被害状況の確認と方針の決定

4	**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。 ・電子カルテ端末起動画面、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。	青字は日中
5	**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、危機的事象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。	

４．復旧処理

4	復旧処理（復旧計画に基づいて、医療情報システムの事業者及びサービス事業者等と協力して復旧を行う。証拠保存の観点からバックアップデータ等を取得する。）		
4-1	経営層からの復旧指示の確認と実施	復旧指示の確認と実施ができるか。	
4-2	医療情報システム等の事業者等へ復旧対応依頼	医療情報システム等の事業者等への対応依頼ができるか。	
4-3	再設定や再インストール、バックアップデータの復旧等	再設定や再インストール、バックアップデータの復旧等ができるか。	
4-4	復旧結果の確認	復旧結果の確認ができるか。	

4-1 復旧指示の確認と実施ができるか

- 復旧計画、復旧時間、費用等を踏まえて、経営層は復旧計画を指示し、情報システム担当者等は復旧計画の実施を行う

- ワークフローを意識してあらかじめ設定した医療情報システムの「復旧優先度」を基に復旧を行う

復旧指示と復旧作業の実施

6	**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「病院情報システム停止時の伝票運用手順」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
7	**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。	

4-2 医療情報システム等の事業者等への対応依頼ができるか

- 自機関で復旧が困難な場合、事業者等へ復旧作業を依頼する

  例）
  - 情報システム担当者と事業者間で、バックアップ復元手順や対応者を、平時に定めておく
  - 復旧に時間を要する場合、代替として、紙カルテ運用、参照系環境構築を検討する

オフラインバックアップデータ範囲の把握

① 磁気テープ装置によるバックアップ

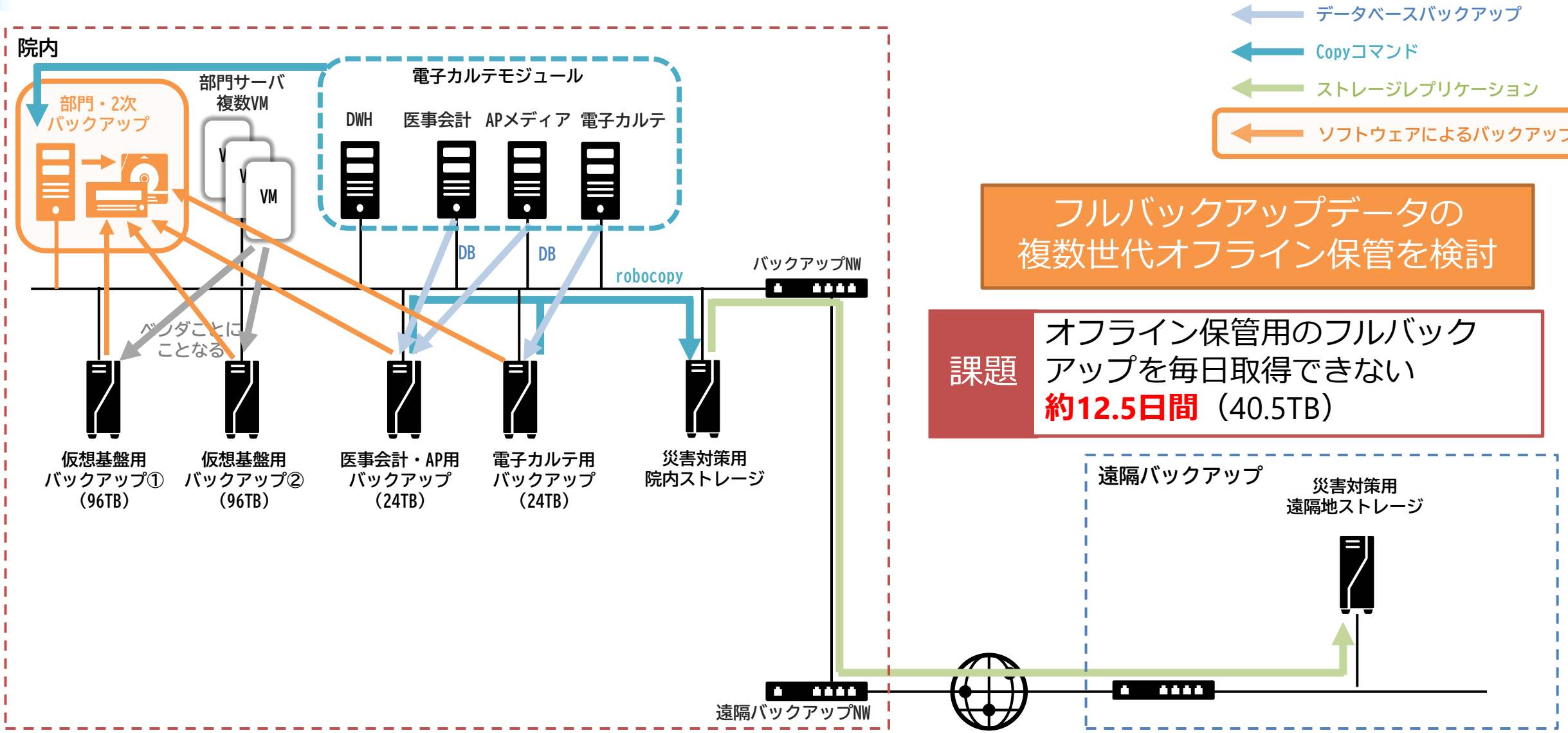
- 基幹システム　＋　部門システム
  - 基幹システム：　電子カルテ、アプリケーションメディア、医事会計、データウェアハウス
- フルバックアップ2世代分（1世代15日間隔）毎にマガジンを交換してオフライン保管
- 6マガジン　12世代（半年前まで）をローテーション保管

② クローンファイルシステムによるバックアップ

システム種別	保存期間	作成間隔	世代数
基幹システム	短期	毎日	60 世代
	長期	2ヶ月	11 世代
部門システム	短期	10 日	6 世代

田木真和ら. ランサムウェアによるサイバー攻撃に備えた病院情報システムのバックアップシステムの構築. 第43回医療情報学連合大会, 2023.

方法①：磁気テープ装置へのフルバックアップ

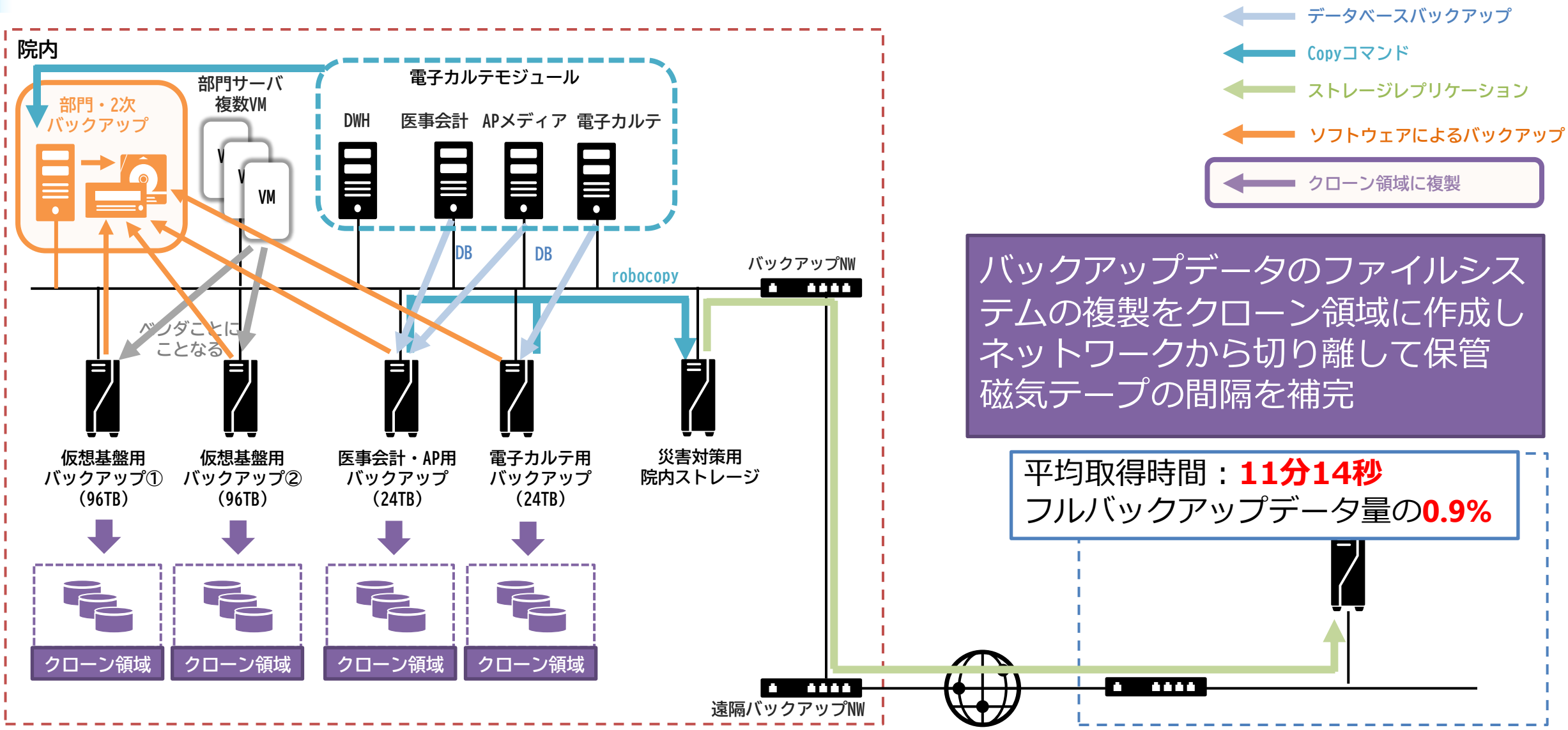


フルバックアップデータの
複数世代オフライン保管を検討

課題 オフライン保管用のフルバックアップを毎日取得できない
約12.5日間（40.5TB）

田木真和ら. ランサムウェアによるサイバー攻撃に備えた病院情報システムのバックアップシステムの構築. 第43回医療情報学連合大会, 2023.

方法②：クローン領域へのファイルシステムバックアップで補完



バックアップデータのファイルシステムの複製をクローン領域に作成しネットワークから切り離して保管
磁気テープの間隔を補完

平均取得時間：**11分14秒**
フルバックアップデータ量の**0.9%**

田木真和ら. ランサムウェアによるサイバー攻撃に備えた病院情報システムのバックアップシステムの構築. 第43回医療情報学連合大会, 2023.

オフラインバックアップデータ範囲の把握

① 磁気テープ装置によるバックアップ

- 基幹システム　＋　部門システム
  - 基幹システム：　電子カルテ、アプリケーションメディア、医事会計、データウェアハウス
- フルバックアップ2世代分（1世代15日間隔）毎にマガジンを交換してオフライン保管
- 6マガジン　12世代（半年前まで）をローテーション保管

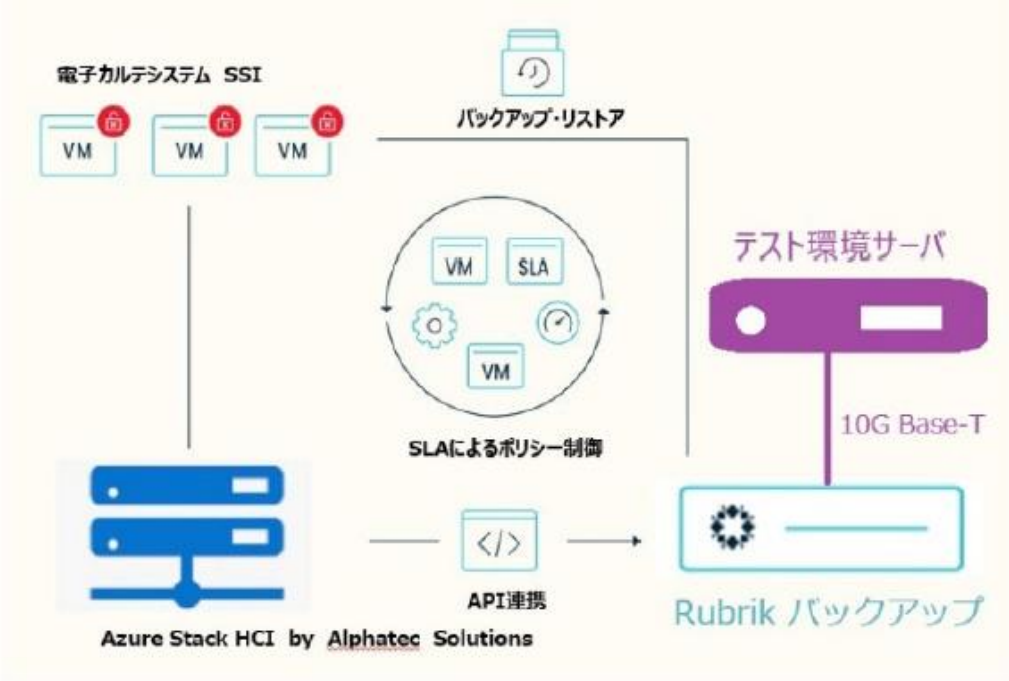
② クローンファイルシステムによるバックアップ

システム種別	保存期間	作成間隔	世代数
基幹システム	短期	毎日	60 世代
	長期	2ヶ月	11 世代
部門システム	短期	10 日	6 世代

田木真和ら. ランサムウェアによるサイバー攻撃に備えた病院情報システムのバックアップシステムの構築. 第43回医療情報学連合大会, 2023.

オフラインバックアップデータの早期復旧

- イミュータブルストレージの活用
  - 簡易な操作かつ早期のシステム復元が可能となる

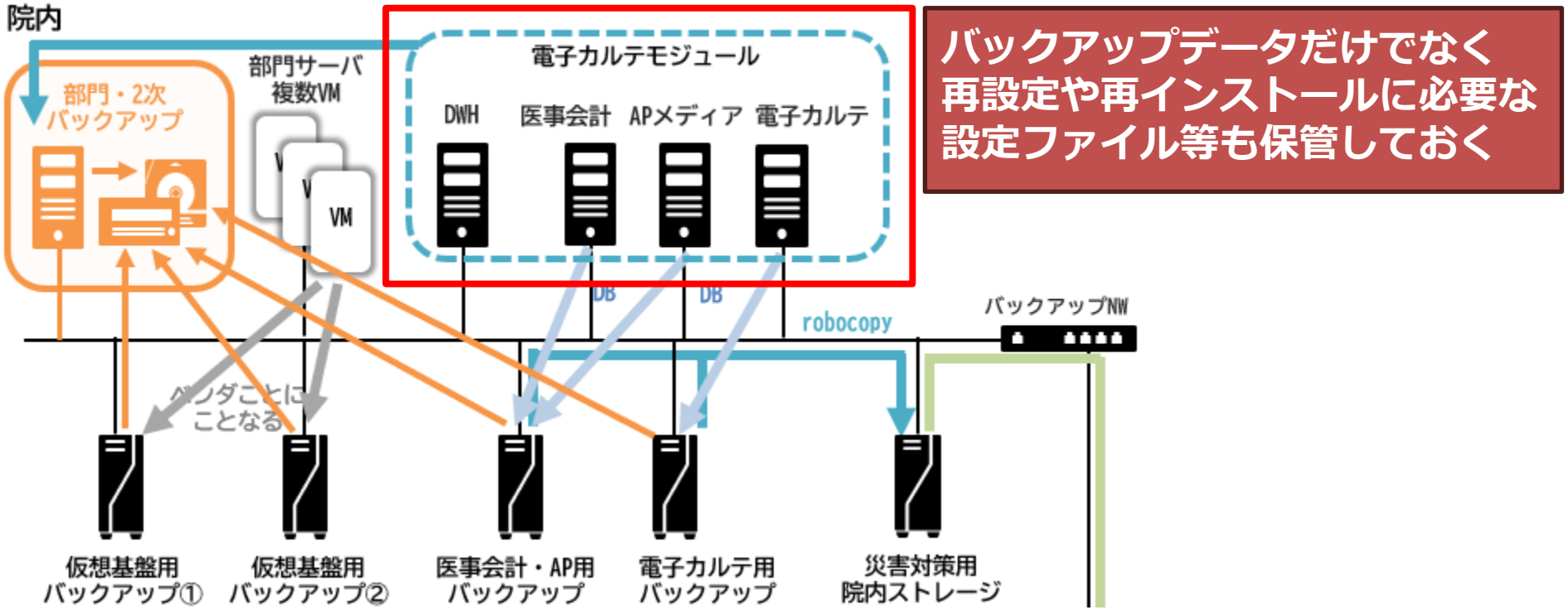


仮想マシン個別復元			
	転送データ量	スループット	復元時間
ドメインコントローラ兼 ファイルサーバ	1181.18GB	4.19Gbps	0:37:43
データベースサーバ	13368.19GB	7.85Gbps	3:47:11
各インターフェースサーバ	107.41GB	1.68Gbps	0:08:39
各インターフェースサーバ	107.41GB	1.73Gbps	0:08:23
各インターフェースサーバ	107.41GB	4.38Gbps	0:03:24
各インターフェースサーバ	107.41GB	4.39Gbps	0:03:24
各インターフェースサーバ	107.41GB	4.38Gbps	0:03:24
検証用クライアント	107.41GB	1.9Gbps	0:07:42
検証用クライアント	107.41GB	2.04Gbps	0:07:10
合計※2023年8月23日時点	15301.24GB	合計	5時07分00秒

吉野絢祐ら.電子カルテシステム復旧用テスト環境構築と目標システム復旧時間の設定について. 第43回医療情報学連合大会, 2023.

4-3 再設定や再インストール、バックアップデータの復旧等ができるか

- 端末PCやサーバ復旧手順について、情報システム担当者、事業者等と連携して事前に定め、それに基づき、再設定や再インストール、バックアップからデータ復旧等を実施する



田木真和ら. ランサムウェアによるサイバー攻撃に備えた病院情報システムのバックアップシステムの構築. 第43回医療情報学連合大会, 2023.

4-4 復旧結果の確認ができるか

- 復旧処理について、医療情報システム等が正常に稼働することを確認する
- 作業者は手順の進捗状況に合わせて経営層に報告を行い、経営層は組織方針に合わせて運用を変更する

被害状況・復旧状況の報告

8	**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、危機的事象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、危機的事象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、危機的事象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。

今回、幸いにも別セグメントにあった診療記録文書統合管理システム（DACS）や医用画像管理システム（PACS）がランサムウェア感染を免れていた。そのため、障害発生翌日の 11 月 1 日から DACS を活用し、予定手術の再開や診療情報提供書の作成などの対応ができた。DACS を参照できる端末も当初の 2 台から最大 20 台まで拡張した。また、11 月 10 日には、バックアップデータを活用した電子カルテの参照端末 20 台の運用も開始。電子カルテの参照端末はその後、高度救命救急センターに 1 台、手術室に 1 台増設できたことから、救急受入の拡充や予定手術の増枠などが実施できた。

情報セキュリティインシデント調査報告書. 大阪府立病院機構大阪急性期・総合医療センター, 2023.

5．事後対応

5	事後対応（復旧結果の報告を受け、再発防止に向けた検討と再発防止策の周知と実施を進める。）		
5-1	復旧結果と情報漏えい事実の有無の報告	復旧結果と情報漏えい事実の有無について、院内での報告を行う方法、報告先、内容を、企画管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-2	再発防止策の検討・策定	再発防止策の検討および策定を進める体制、能力があるか。管理者、システム担当者がそれぞれの分担責任として把握しているか。	
5-3	再発防止策の周知	再発防止策の周知を院内に周知する方法と体制が整備されているか。	
5-4	再発防止策の実施	再発防止策の実施が行えるか。	
5-5	事業者等への再発防止策の指示	事業者に対して再発防止策を具体的に提案し、実施可能かつ有効な方法を策定する能力があるか。	
5-6	外部関係機関への報告と情報公開の検討	情報公開の内容検討を行う体制、連絡先、内容を文書として準備し、必要時に速やかに利用できるか。 経営者と担当者により外部関係機関への報告が行えるか。	

復旧完了報告と復旧作業記録

9	**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、復旧の完了を危機的事象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、危機的事象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。
10	**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。

情報公開

つるぎ町立半田病院

HOME　病院案内図　交通案内　お問い合わせ　サイトマップ　リンク集

外来のご案内 | 入院・面会のご案内 | 人間ドック・健康診断 | 当院について | 医療関係者向け | 採用情報

Home»コンピュータウイルス感染事案有識者会議調査報告書について

- ごあいさつ
- 基本理念
- 概要・沿革
- 歴代病院事業管理者　歴代病院長名

徳島県つるぎ町立半田病院
コンピュータウイルス感染事案有識者会議調査報告書について

令和3年10月31日の未明、つるぎ町立半田病院がサイバー攻撃を受け、電子カルテをはじめとする院内システムがランサムウェアと呼ばれる身代金要求型コンピュータウイルスに感染し、カルテが閲覧できなくなるなどの大きな被害が生じました。令和4年1月4日の通常診療再開までの間、患者さんをはじめ関係者の皆さまには多大なご迷惑とご心配をおかけいたしましたこと、改めて深くお詫び申し上げます。

有識者会議調査報告書ダウンロード

- コンピュータウイルス感染事案有識者会議調査報告書（PDF）
- コンピュータウイルス感染事案有識者会議調査報告書ー技術編ー（PDF）
- 情報システムにおけるセキュリティコントロールガイドライン（PDF）

徳島県つるぎ町立半田病院

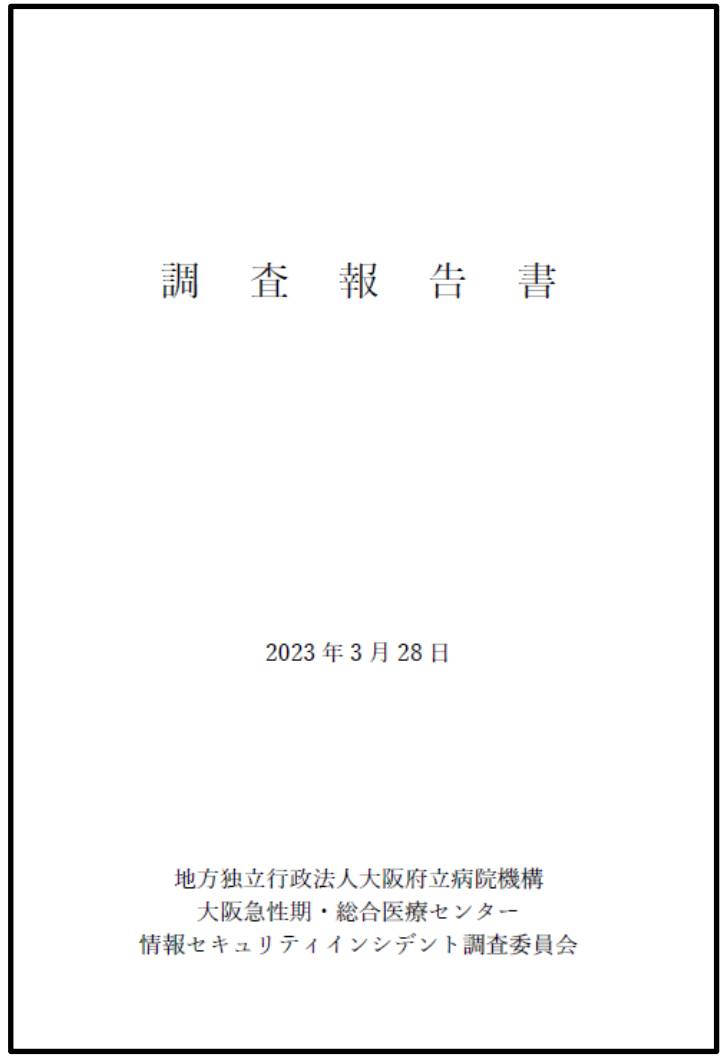
コンピュータウイルス感染事案

有識者会議調査報告書

2022 年 6 月 7 日

https://www.handa-hospital.jp/topics/2022/0616/index.html

情報公開



https://www.gh.opho.jp/incident/1.html

最後に： IT-BCPチェックリストに即したひな形（厚生労働省）

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

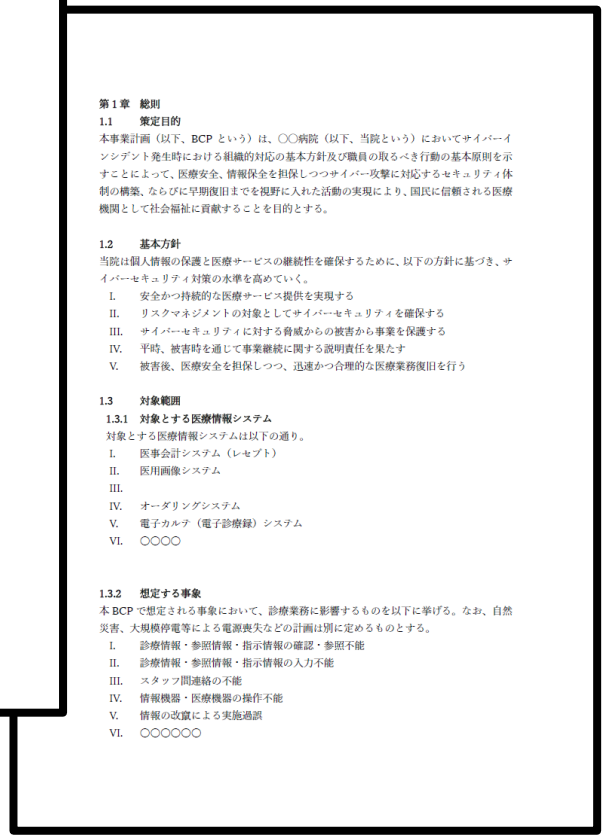

医療情報システム部門

事業継続計画（BCP）

○○年○○月○○日　初版

○○病院

○○部門


第１章　総則

1.1　策定目的

本事業計画（以下、BCP という）は、○○病院（以下、当院という）においてサイバーインシデント発生時における組織的対応の基本方針及び職員の取るべき行動の基本原則を示すことによって、医療安全、情報保全を担保しつつサイバー攻撃に対応するセキュリティ体制の構築、ならびに早期復旧までを視野に入れた活動の実現により、国民に信頼される医療機関として社会福祉に貢献することを目的とする。

1.2　基本方針

当院は個人情報の保護と医療サービスの継続性を確保するために、以下の方針に基づき、サイバーセキュリティ対策の水準を高めていく。

I.　安全かつ持続的な医療サービス提供を実現する
II.　リスクマネジメントの対象としてサイバーセキュリティを確保する
III.　サイバーセキュリティに対する脅威からの被害から事業を保護する
IV.　平時、被害時を通じて事業継続に関する説明責任を果たす
V.　被害後、医療安全を担保しつつ、迅速かつ合理的な医療業務復旧を行う

1.3　対象範囲

1.3.1　対象とする医療情報システム

対象とする医療情報システムは以下の通り。

I.　医事会計システム（レセプト）
II.　医用画像システム
III.
IV.　オーダリングシステム
V.　電子カルテ（電子診療録）システム
VI.　○○○○

1.3.2　想定する事象

本 BCP で想定される事象において、診療業務に影響するものを以下に挙げる。なお、自然災害、大規模停電等による電源喪失などの計画は別に定めるものとする。

I.　診療情報・参照情報・指示情報の確認・参照不能
II.　診療情報・参照情報・指示情報の入力不能
III.　スタッフ間連絡の不能
IV.　情報機器・医療機器の操作不能
V.　情報の改竄による実施過誤
VI.　○○○○○○