厚生労働行政推進調査事業費補助金

厚生労働科学特別研究事業

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

令和5年度　総括研究報告書

研究代表者　鳥飼　幸太

令和 5（2024）年　5 月

目　　次

厚生労働行政推進調査事業費補助金

厚生労働科学特別研究事業

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

令和5年度　総括研究報告書

研究代表者　鳥飼　幸太

令和６（2024）年　５月

目　　次

厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）
（総括）研究報告書

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

研究代表者　鳥飼　幸太　《国立大学法人 群馬大学 医学部附属病院システム統合センター》

研究要旨

．研究目的
国内におけるサイバー攻撃の被害が増加しており、医療分野におけるサイバーセキュリティ能力の向上は医療能力の安定提供を通じ国民福祉に貢献する。これまで医療機関におけるサイバー攻撃対策ならびに同攻撃被害時における医療ITの事業継続計画(Business Continuing Plan: BCP)(以下IT-BCP)の策定ならびに実施については各医療機関における自主的な取り組みが進められてきた。一方、人為的サイバー攻撃に対し、NIST CSF(CyberSecurity Framework)における用語の意味での「検知」(Detection)や「対応」(Response)といったアクティブディフェンスを行うために際しては、サイバー攻撃対処の技能習得ならびに実施に際して高度な技術能力が必要である。このため、本研究では医療機関が基本的に備えるべき共通のIT-BCP対策の内容について調査検討し、実施可能なチェックリスト案を作成することを目標とする。

Ｂ．研究方法
本研究では、研究代表者所属機関（群馬大学医学部附属病院）、研究分担者所属機関（徳島大学医学部附属病院、大津赤十字病院）におけるサイバーセキュリティ対策のうち、IT-BCPとして捉えられる内容を調査した。次に、IT-BCP対策の参照資料である「医療情報システムにおける安全管理に関するガイドライン第6.0版」を精査し、IT-BCPが備えるべき特徴のカテゴリについて検討を行い案を作成した。作成にあたっては、米国NIST CSFならびに米国CISA CDM(Continuous Diagnostics and Mitigation)の分類を参考とした。その後、作成したIT-BCPカテゴリを参考としながらIT-BCPが備えるべき項目について検討し、実施可能な記述内容であることを確認しながらチェックリスト（IT-BCPチェックリスト）の作成を行った。

（倫理面への配慮）
本研究では患者および個人に関する情報を扱わないため、倫理面での問題は生じない。

Ｃ．研究結果
1.医療情報システムにおける安全管理に関するガイドライン6.0版におけるCSF/CDM/BCP分類の作成
本研究ではIT-BCPを検討する基礎として、今後遵守の対象となっている医療情報システムにおける安全管理に関するガイドライン第6.0版について、多角的な考察を行う目的で、CSF/CDM/BCP分類のどのカテゴリに相当した内容であるかについて調査を行った。調査の結果、図1に示すように、CSF分類としては識別/防御に関する対策が充実していることが分かった。一方、BCP対策における１次対応に相当するアクティブディフェンス能力である検知/対応については相対的に項目が少ないことがわかった。また、BCPにおいて重要な指標である復旧についても、同様に相対的に項目が少ないことがわかった。本調査項目については別添資料にて記載する。

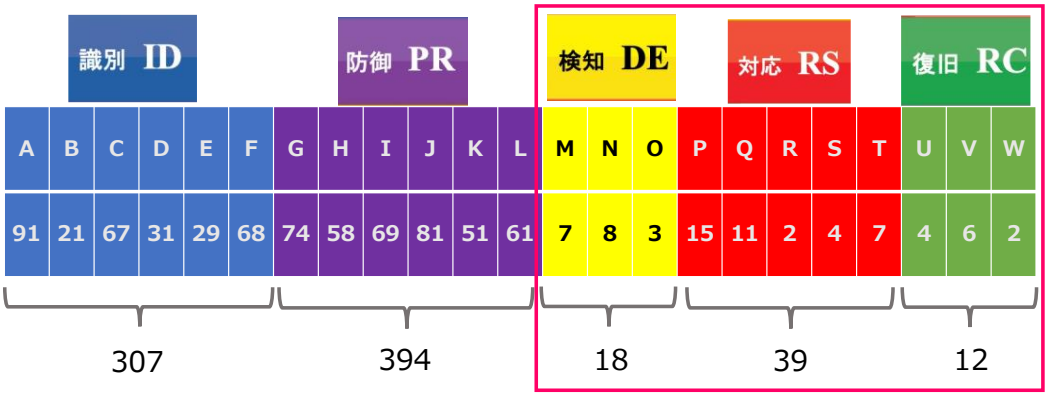


図１医療情報システムにおける安全管理に関するガイドラインのCSFカテゴリ分類

2.医療サイバーセキュリティに関するIT-BCPチェックリストの作成
研究班員はすべて自医療機関（500床以上）での病院情報システム全体更新を主導した経験を有し、またシステムトラブル対処経験を有する。過去にシステムトラブルから復旧した際に必要とした能力や知識について議論を行い、医療機関における事業継続を達成するためには、CSFに示されたサイバー攻撃のみに関する準備のみでは不十分であり、またCDMに示されたサイバー攻撃に備えた防御策のみでも不十分であるとの認識に至った。そこで、サイバー攻撃への対処の中で、システムトラブルと同様の対処が必要な内容を追加し、病院ITのBCPとしてのカテゴリとして以下の５項目を選定した。

１・通常時の備え、
２・サイバー攻撃を覚知できる能力、
３・覚知したサイバー攻撃に対し、自組織の活動停止を回避し、患者生命を保全しつつ攻撃に対処する能力、
４・攻撃の脅威から免れたのち、通常診療のレベルまで速やかに状態を復旧できる能力、
５・復旧後、インシデントに対する振り返りができ能力ならびに善後策を講じる能力

以上の項目より、細目について、CSF/CDMの各5分類からカバーすべき内容に偏りが生じないように内容を選定し記載した。本チェックリストの記載に当たっては、すべての医療機関において使用されるが、特に診療録管理体制加算が充実した200床以上の病院に対して適用できることを考慮して記載した。チェックリストの実施者としては、医療機関におけるシステム管理者のほか、サイバーセキュリティに熟達していない事務職員等においても把握できるよう記載の用語や内容について確認を行った。

D．考察
サイバーセキュリティの実装においては、これまでサイバーセキュリティの専門家のみでの監修が多く、把握すべき資料はインターネットから取得可能ではあるが分量が多いことが理解の妨げになっていたと推測される。また、サイバーセキュリティの用語については、日常用語または医療用語からかけ離れた特有の呼称が多く存在し、サイバーセキュリティの概念の独自性とあわせて理解が困難な側面が存在した。今回、医療機関でのワークフローと連成した資料を作成することにより、医療機関側でセルフチェックが可能になる様式を整備できたと考えられる。これは厚生労働省が目指す均霑化の目的に合致するものと考えられる。また、ガイドライン6.0版のCSF/CDMチェックを事前に行うことにより、各章立てに基づく内容の分割から、その効果に基づく内容の分割を検討でき、BCPとして備えるべき項目に対する根拠づけを行うことができた。

E．結論
本研究は単年度事業であり、研究成果として、医療情報システムにおける安全管理に関する

ガイドライン第6.0版を踏まえた、幅広い医療機関で活用されることを目的としたIT-BCPチェックリスト作成を実施した。

Ｆ．健康危険情報
本研究では生物由来資料、検体、医療機関における診療行為などを調査対象として含まないため、本研究に基づく健康危険は生じないと考えられる。

Ｇ．研究発表
1.　論文発表
鳥飼幸太、　医療機関におけるサイバー攻撃対応のための事業継続計画(BCP)の普及に向けた研究、第43回日本医療情報学会抄録集、2023年11月

2.　学会発表
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・シンポジウム（大会企画セッション3）、2023年7月
鳥飼幸太、　医療機関におけるサイバー攻撃対応のための事業継続計画(BCP)の普及に向けた研究、第43回日本医療情報学会シンポジウム、2023年11月

Ｈ．知的財産権の出願・登録状況
（予定を含む。）
1．特許取得
なし
2．実用新案登録
なし
3.その他
なし

厚生労働行政推進調査事業費補助金（厚生労働科学特別研究事業）
（総括・分担）研究報告書

医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

研究分担者　橋本　智広　«大津赤十字病院　事務部　医療情報課»

研究要旨

本研究では、医療機関が自機関における BCP の策定に向けて、支援するためのツールの作成を行った。具体的には、医療機関における医療情報システムの安定稼働に対する日常的な業務の経験と、前述したサイバー攻撃被害事例を踏まえて、BCP 策定に必要と考えられる要素を整理した。整理した結果を踏まえて、医療機関の BCP 策定を支援するツール（「BCP 策定のための確認表」「確認表の手引き」「ひな形」）を作成した。

A．研究目的

近年、日本国内の医療機関に対するサイバー攻撃により、診療業務の継続が困難となり診療に多大なる影響を及ぼした事例が相次いでいる。具体的には、徳島県つるぎ町立半田病院（被害年月：令和 3 年 10 月）、大阪急性期・総合医療センター（被害年月：令和 4 年 10 月）の遭遇したランサムウェア被害は国内に広く報道された。これらの事案は、数か月にわたり通常診療の継続が困難な状況に陥った。このことから、医療機関は自施設の情報セキュリティ対策を見直す契機となったことはいうまでもない。この状況下で、医療法施行規則の改定（令和 5 年 4 月 1 日施行）において、医療機関の管理者がサイバーセキュリティへの対応が求められる旨が追加された。また、「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）」（以下、ガイドラインと略す）が公開されたことで、医療機関はさらなる情報セキュリティ対策が求められるようになった。さらに、医療法に基づく立入検査では、サイバーセキュリティに関する検査項目が追加され、「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」に基づく対応が求められている。各医療機関はこれまで経験したことのないサイバー攻撃による被害に対して、診療継続を含む医療サービスの提供を継続することを目的として事業継続計画（以下、BCP と略す）の策定が求められている。これまで自然災害においては災害拠点病院等を中心に BCP が作成されている現状はあるものの、サイバー攻撃を想定した BCP はその策定にセキュリティに関する知識や技術的対策に対する考慮が必要となるため必要十分な BCP が作成できないことが想像される。

本研究では、医療機関が自機関における BCP の策定に向けて、支援するためのツールの作成を行う。具体的には、医療機関における医療情報システムの安定稼働に対する日常的な業務の経験と、前述したサイバー攻撃被害事例を踏まえて、BCP 策定に必要と考えられる要素を整理する。整理した結果を踏まえて、医療機関の BCP 策定を支援するツール（「BCP 策定のための確認表」「確認表の手引き」「ひな形」）を作成する。

B．研究方法

本研究は、3 名の研究者により役割分担した上で推進した。具体的には、研究者の所属機関を含むこれまでの教育経験、業務経験から、事実に基づく研究成果が達成できるように務めた。

1. サイバー攻撃の被害に遭遇した医療機関に対する調査および文献調査

前述したサイバー攻撃の被害に遭遇した 2 つの医療機関に対して、当該医療機関の担当者から得られた情報と、一般公開されている報告書から、BCP に必要と想定されることを検討した。具体的には、「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（https://www.handa-hospital.jp/topics/2022/0616/index.html）」「大阪急性期・総合医療センター情報セキュリティインシデント調査委員会調査報告書（https://www.gh.opho.jp/important/785.html）」から情報収集を行った。

2. 調査結果に基づくガイドラインをベースとした BCP 策定に必要な要素整理

項番１の調査から得られた結果を踏まえて、医療機関に求められる安全管理対策が記載されているガイドラインに含まれる「遵守事項」をリストアップし、表１に示す分類のどれに該当するかを全ての項目に対してチェックした。なお、本分類は、「NIST-SP800 シリーズ」に記された CDM（Continuous Diagnostics and Mitigation）および「NIST」の CSF(Cybersecurity Framework)をベースに、医療サービス提供において考慮すべき事象を踏まえて設定した。

表1：分類一覧

分類番号	分類名
1	医療装置・直接
2	医療装置・間接
3	関連装置・間接
4	物理インフラ・間接
5	基幹情報サーバ・間接
6	情報サービス・間接
7	診療データ運用・間接
8	不法対策・間接
9	BCP意思決定
10	BCP必要条件

3. 医療機関の BCP 策定を支援するツールの作成

項番２の結果を踏まえて、医療機関が自機関で BCP 策定に向けた取り組みが実行できるように「BCP 策定のための確認表」「確認表の手引き」「ひな形」を作成した。

4. ガイドラインの遵守事項に対する不足する項目の洗い出しと追加すべき項目の検討

ガイドラインには、情報セキュリティ対策として必要最低限の対策として遵守事項が示されているが、CDM および CSF の観点と、医療機関での医療情報システムに対する実運用を踏まえて不足している点が発見された。具体的には、CSF に含まれる「検知」「復旧」のフェーズに関連する項目が不足しているとして、追加すべき項目の検討を行った。

（倫理面への配慮）
本研究においては、医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究として、人を直接の対象とした研究には該当しない。

C．研究結果

ガイドラインに含まれる「遵守事項」において、表1に示す分類のどれに該当するかを全ての項目に対してチェックした結果を表2に示す。結果として、いずれの分類にも該当しないものが16件確認された。本研究で設定した分類は、医療サービス提供において考慮すべき事象を踏まえてあらかじめ設定したものであった。結果として、遵守事項にも各分類において件数に差はあるものの、比較的網羅されていることが明らかとなった。

表2：分類別の件数

分類番号	分類名	件数
1	医療装置・直接	52
2	医療装置・間接	52
3	関連装置・間接	56
4	物理インフラ・間接	141
5	基幹情報サーバ・間接	137
6	情報サービス・間接	198
7	診療データ運用・間接	121
8	不法対策・間接	168
9	BCP意思決定	54
10	BCP必要条件	135

表2の結果を踏まえて、「BCP策定のための確認表」「確認表の手引き」「ひな形」を作成した。「BCP策定のための確認表」においては、次の5項目を大項目として用意し、各項目に含まれる小項目を設定した。

⑴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。
⑵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。
⑶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。
⑷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。
⑸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。

さらに、ガイドラインの遵守事項に対する不足する項目の洗い出しと追加すべき項目の検討として、検知（12項目）、復旧（17項目）、要検討（6項目）を新規追加案として列挙した。

D．考察

医療機関において、診療提供体制が機関ごとに異なることから、医療情報システムや医療機器等の資産は、医療サービスの提供に必要となるものを保有する現状がある。その中で、各機関は独自にBCPを作成する必要がある。医療機関の多くは、前述したとおりサイバー攻

撃の被害に遭遇した施設は多くないため、被害が発生した際の対応として必要な対策がBCPにもれなく含めることができないかもしれない。本研究の支援ツールを用いて作成されたBCPを各機関から収集することで、BCPの比較や診療提供体制ごとベンチマーク、さらには第三者による評価を行うことで、各機関に対するさらなる提言が可能になると考える。

E．結語

本研究では、医療機関が自機関におけるBCPの策定に向けて、支援するためのツールの作成を行った。医療機関におけるサイバーセキュリティへの対応は、今後さらに高度な対策を求められると考える。その中で、医療機関がサイバー攻撃により診療業務の継続が困難になった場合、医療機関の規模問わず地域医療に与える影響は計り知れない。そのためにも、医療機関は医療サービスの提供に向けたBCPの策定が急務となる。将来的には、各機関において、策定されたBCPが適宜改版され、PDCAサイクルに基づくBCP維持が実践されることを期待する。あわせて、サイバー攻撃に対するBCPと、自然災害、感染等を目的とした既存のBCPを統合した「オールハザード型BCP」の策定が今後必要になると考える。

F．健康危険情報

G．研究発表

1. 論文発表

なし

2. 学会発表

・鳥飼幸太, 田木真和, 橋本智広. IT-BCPをどう実現するか. 第43回医療情報学連合大会, 2023年11月.

・鳥飼幸太, 田木真和, 橋本智広. 医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究. 第43回医療情報学連合大会, 2023年11月.

H．知的財産権の出願・登録状況

1. 特許取得

なし

2. 実用新案登録

なし

3.その他

なし

刊行物一覧

研究報告書（本文）

サイバー攻撃から診療記録を守るために何をすべきか？The Journal of JAHMC 2023 年 10 月号

IT-BCP をどのように実現するか（日本医療情報学会シンポジウム発表資料）

CSF/CDM/BCP 分類資料

以上

寄稿

サイバー攻撃から診療記録を守るために何をすべきか？

鳥飼　幸太　群馬大学医学部附属病院システム統合センター 副センター長／准教授

「サイバー攻撃」とは

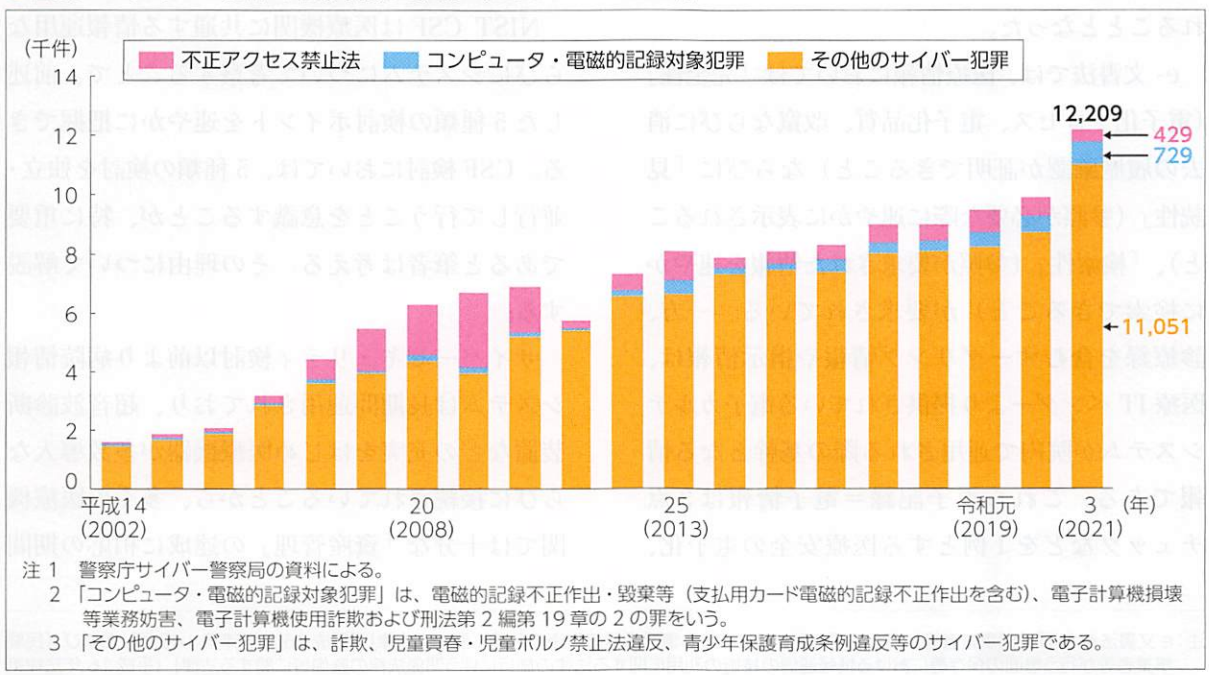
本稿は、医療機関において「サイバー攻撃から診療記録を守る」ために必要な知識背景と行動につき、解説ならびに提案することを目的とする。

まず、「サイバー攻撃」というキーワードの背景について考察する。

サイバー攻撃は犯罪行為の1つであり（図表1）、「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」（サイバー刑法）により、コンピュータ・ウイルス作成罪などの罰則ならびに情報技術（Information Technology：IT）の発展に対応できる操作手続きの整備が定められている[1]。サイバー空間はいわゆる「インターネット空間」であり、自身のパソコンやスマートフォンを通じ、今ではサイバー空間に常時接続された状態に置かれている。サイバー攻撃は「貧者の兵器」と呼ばれ、医療機関において法律ならびに施行規則によって保存が規定されている診療上の記録は、「「診療録等の保存を行う場所について」の一部改正について」（平成25年3月25日付医政発0325第15号・薬食発0325第9号・保発0325第5号厚生労働省医政局長・医薬食品局長・保険局長連名通知）に記載されている[2]。

サイバー攻撃のうち、特定の個人、あるいは組織を狙って行われる攻撃、標的に対して持続的に行われる攻撃（APT〈Advanced Persistent Threat〉攻撃）の実施者は国際的サイバー犯罪

●図表1　サイバー犯罪の検挙件数の推移（2002～2021年）



注1　警察庁サイバー警察局の資料による。
2　「コンピュータ・電磁的記録対象犯罪」は、電磁的記録不正作出・毀棄等（支払用カード電磁的記録不正作出を含む）、電子計算機損壊等業務妨害、電子計算機使用詐欺および刑法第2編第19章の2の罪をいう。
3　「その他のサイバー犯罪」は、詐欺、児童買春・児童ポルノ禁止法違反、青少年保護育成条例違反等のサイバー犯罪である。

出所：法務省『令和4年版犯罪白書』、p.194

組織を含む。このためサイバー攻撃により医療機関が被害を受けた際、重要インフラとしての被害が大きい[3]半面、犯罪者の特定、検挙ならびに賠償請求を行える確率が低いと想定されることがサイバー犯罪対処の困難さとして挙げられる。サイバー攻撃者の特定には、サイバー攻撃被害が発生した際、診療の復旧と相まって、犯罪立証のための電磁的記録の解析技術およびその手続き（サイバーフォレンジック〈Forensics〉）作業を並行することが求められる。

診療情報の電子化・保全は不可欠

次に、「診療記録を守る」というキーワードの背景について考察する。

診療録を中心とする診療記録については、サイバー攻撃対策の是非にかかわらず、すべての医療機関において定められた年限の保管が義務付けられている。診療情報の電子化過渡期においては、処方箋などを原紙で保管するなどで対処されてきたが、2005年4月に施行されたe-文書法[注]によって、各種法令で書面（紙媒体）での保存が義務付けられている文書について、電磁的記録（電子データ）による保存が容認されることとなった。

e-文書法では、医療情報においては「完全性」（電子化プロセス、電子化品質、改竄ならびに消去の履歴確認が証明できること）ならびに「見読性」（参照が必要な際に速やかに表示されること）、「検索性」（参照が要求された情報を速やかに検索できること）が要求されている。一方、診療録を含むオーダリング情報や指示情報は、医療ITベンダーより提供されている電子カルテシステムが院内で運用される際の基幹となる情報である。これら電子記録＝電子情報は3点チェックなどを1例とする医療安全の電子化、ならびに診療記録の共有、適切な診療報酬の算定支援などに不可欠であり、医療機関は法的要請の有無にかかわらず、診療情報の電子化ならびにその保全が不可欠である。

セキュリティ強化に有用なNIST CSF

医療機関がサイバー攻撃から診療記録を守るための調査ならびに検討事項として、サイバー攻撃の侵攻手順、ならびにこの侵攻手順が病院情報システムならびに診療プロセスのどのポイントに該当するかを把握する必要がある。この課題に関しては米国国立標準技術研究所（National Institute of Standards and Technology：NIST）が公開しているサイバーセキュリティフレームワーク（Cybersecurity Framework：以下CSF）に基づく検討が広く知られている[4,5]。CSFは、①識別（Identification：ID）、②防御（Protection：PR）、③検知（Detection：DE）、④対応（Response：RS）、⑤復旧（Recovery：RC）の項目に沿って自施設のサイバーセキュリティ整備・運用状況を整理し、不足箇所の認識ならびにサイバーセキュリティ強化の着手箇所を検討するために有用である（図表2）。

NIST CSFは医療機関に共通する情報運用ならびにシステムについて考察することで、前述した5種類の検討ポイントを速やかに把握できる。CSF検討においては、5種類の検討を独立・並行して行うことを意識することが、特に重要であると筆者は考える。その理由について解説する。

サイバーセキュリティ検討以前より病院情報システムは長期間運用されており、超音波診断装置などの充実をはじめ医療機器が多数導入ならびに接続されていることから、多くの医療機関では十分な「資産管理」の達成に相応の期間

注：e文書法とは、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）および「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（平成16年法律第150号）の総称。

●図表 2　NIST サイバーセキュリティフレームワークにおける機能の 5 分類

出所：米国国立標準技術研究所：重要インフラのサイバーセキュリティを改善するためのフレームワーク，独立行政法人情報処理推進機構翻訳監修，p.6，2018 年 4 月

●図表 3　医療機関における NIST CSF に基づく検討と対策の一例

フレームワーク機能	検討箇所の例	対策ツールの例	対策運用の例
識別 Identification (ID)	病院情報システム全体の接続機器･IP アドレス、セグメンテーション、接続経路、脆弱性等の把握	ネットワーク可視化ツール、脆弱性把握ツール	資産管理手順に沿った調査（リストアップ）、脆弱性情報の迅速把握
防御 Protection (PR)	外部保守接続箇所（放射線診断･治療装置、PACS/ 電子カルテ等）、DMZ 端末、診療録サーバ	VPN、ランサム対策ストレージ	情報漏洩を起こさない院内情報運用研修、診療情報アクセス制御設定、ファイヤウォール設定、セキュリティ保守契約の充実、バックアップ手段と階層、運用の策定と実装
検知 Detection (DE)	電子カルテ端末挙動、ネットワークトラフィック監視、ストレージ / CPU 負荷変動	IDS、EDR（D）、NDR（D）	日常のシステムパフォーマンスモニタにおけるトレンド把握と差異の知覚、対策ツールが提供するダッシュボード機能による監視
対応 Response (RS)	不特定多数や多数のスタッフがアクセスできる機器、電子カルテにアクセスできる端末またはサーバとポート、攻撃検知時のカルテデータバックアップ経路	IPS、EPP、EDR（R）、NDR（R）	インシデント時連絡先の把握と役割分担の検討、医療安全と情報保全、診療継続を両立する対策方法やツール挙動設定の検討、インシデント対応訓練への参加
復旧 Recovery (RC)	電子カルテサーバを中心とする保存義務を有する情報サーバ、診療継続に不可欠な情報端末の運用	バックアップ復元ツール、情報サーバ仮想化インフラ	復元手順の BCP への記載、復元テスト、環境設定を伴った包括的サーババックアップの実施、バックアップ周期の短縮化

略語：PACS（Picture Archive and Communication System）、VPN（Virtual Private Network）、DMZ（Demilitarized Zone）、IDS（Intrusion Detection System）、IPS（Intrusion Prevention System）、EDR（Endpoint Detection and Response）、NDR（Network Detection and Response）、EPP（Endpoint Protection）

とマンパワーを必要とする。一方、近年の急激な国際情勢の変化に伴うサイバー攻撃に対しては、迅速に整備対策を進める必要があり、資産管理を待たずに着手可能な手段を、逐次実施することが必要だからである。

図表 3 に、医療機関における NIST CSF に基づく検討と対策の一例を示し、着手すべき順等を考察する。まず、診療記録を守る上で不可欠な対策は電子化診療録の実運用サーバがサイバー攻撃に対し、情報ならびに機能を失わない

ことである。これに該当するサーバは電子カルテサーバである。実施対策としては②PRならびに⑤RCの機能について調査し、不足であれば該当箇所を強化する手法の検討ならびに実施を速やかに行う。次に、病院経営の継続が病院収入を維持する必要条件であり、診療継続に不可欠な情報サーバならびに端末がサイバー攻撃を受けたとしても、情報ならびに機能を失わないことを考える。これに該当するサーバは、オーダリングサーバのほか、患者受付機能を提供するサーバ、会計算定機能を提供するサーバ等が該当する。診療ワークフロー上では、検体検査、画像検査が停滞することで外来ならびに入院患者の診療継続に多大な支障が生じることから、これらの機能を提供するために不可欠なサーバならびに端末を特定し、サイバー攻撃耐性を高める手当てを実施することが肝要である。また一例として、当該機能を提供しているサーバは、物理サーバと仮想サーバの別により、データ保全や機能保全の具体的手法が異なるなど、サイバーセキュリティ対策においてはシステム構成情報に基づき実施することが必要である。

多要素の認証プロセスを導入し パスワードの定期的変更を確実に

サイバーセキュリティ対策においては、過去に一度有効性が疑われて主運用から外された技術が、セキュリティ環境全体の変化に伴い、再び必要な対策として見直されるケースが存在する。一例として、ユーザー名とパスワードの運用について取り上げる。

The Hacker Newsは「It's a Zero-day? It's Malware? No! It's Username and Password」において、攻撃者の武器で最も強力な武器は盗んだユーザー名とパスワードだとして、その深刻さと課題、Active Directory環境の保護の重要性について報じている。これは、サイバー攻撃の検出が電子情報処理プロセスやネットワークトラフィック、ユーザーの行動など様々なアクティビティの異常を特定することに依存しているため、攻撃者が正常に認証されてしまうと、その後の攻撃を検出することが難しくなることに起因している。

このような状況で診療記録を守るための活動として、認証プロセスにおいて複数の独立したデバイス（パソコンとスマートフォンなど）を操作するよう求められる多要素認証の適用箇所を増加させるとともに、ユーザー名やパスワードの漏洩が起きている可能性があることを前提とし、パスワードを定期的に変更する運用の確実な実施が効果的であると考えられる。サイバーセキュリティの最適解は情勢によって変化することから、その対策の有効性や効果についても適宜見直しができることが望ましい。

責を負うのは経営者 検討では「数値として」決定する

医療機関の経営者視点でサイバーセキュリティを見た場合、その向上対策を「診療報酬に結びつかない固定費」と捉えがちである。しかしながら、経営において誤ったリスク評価に基づく損害の責を負うのは経営者であることが、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版に明記された[6]。

本検討における「リスク」とは、サイバー被害について「被害発生確率×被害額」によって計算される量である。一般にリスク評価においては、リスクについて年間被害額の計算を行い、これを低減する対策実施に必要な適正支出額を算出する、と説明されている。しかしながらこの計算方法にのみ依存すると、長期的に効果の高いリスク低減手法である「ITネットワークインフラの再構成」が提案された場合に、一過性の支出が大きいことのみを理由として申請が否定される傾向にあることが複数医療機関との議論から把握されている。特に、中規模以上の総合病院においてはITインフラを構成する機器ならびにネットワーク要素が多いため、再構

成の見通しを得るために必要な労力を割り当てられないこともその素因を構成していると考えられる。

経営者視点でサイバーセキュリティ対策を考える上では、最も厳しい検討条件として「当該事業所は、サイバー攻撃を含む諸般の外乱により診療停止を行わざるを得ない場合、破綻に至らない停止期間は何日間までだろうか」という問いを設定し、「数値として」決定することが肝要である。その上で、この数値を下回るように情報システムの稼働信頼性を確保するよう検討する。診療において運用している病院情報システムについては、医療 IT ベンダーの担当者と担保すべきシステム稼働信頼性について協議し、Service Level Assurance（SLA）として保守契約を定めることが有効である。SLA では、サイバー攻撃を含むシステム停止が生じた場合の駆けつけまたは対応開始までの時間、手段や条件、障害内容の切り分けならびにフォレンジック作業の受け入れ、診療継続状態維持のための 1 次手当ての方針策定と実施、正常診療状態への復旧等について項目を設け、医療機関側で実施担保する内容と医療 IT ベンダー側で実施担保する内容を分界する（責任分界点の設定）を明確化することで、リスク低減対策に対する支出を決定する。

医療サイバーセキュリティ人材は医療人と同様の登用と配置を

長期的なリスク低減を行う上では、経費の上でも対応の迅速さ確保の上でも、外注と比較してセキュリティ部門の組織化とセキュリティ運用の内製化を段階的に行い、CSF の全体レベルを向上させるための長期戦略を策定して、計画的に実施する能力を涵養することが望ましい。この点においては、社会全体におけるスキルを有する IT 人材が慢性的に不足している実情があり、採用公募のみで適切な人材を確保することが難しいと考えられる。（一社）医療情報学会ならびに医療情報技師育成部会では、医療情報技師能力検定等を定め、高度な医療 IT スキルを有する人材の輩出に努めている。また、（一社）医療サイバーセキュリティ協議会では、医療機関、医療 IT ベンダー、政府機関など立場の異なる役職により、医療サプライチェーンのセキュリティを俯瞰できる教育の提供ならびにユーザー間での ISAC 機能を提供している[7]。

医療 IT 運用は、医療人の育成と同じく「現場から学ぶ」On the Job Training（OJT）の要素が強いと筆者は考えており、読者諸賢においては、素質のある人材を定着させ、育成の視点を踏まえた医療サイバーセキュリティ人材の登用と配置についてご検討、ご配慮いただけたらと願う[8]。

[参考文献]
1) 法務省：いわゆるサイバー刑法に関する Q&A，https://www.moj.go.jp/content/001267488.pdf［2023.9.19 確認］
2) セコム医療システムウェブサイト：電子カルテの保存期間と医療機関における文書保管について、https://medical.secom.co.jp/it/karte/column/post-5.html［2023.9.19 確認］
3) サイバー攻撃で「核の大惨事」の恐れも、米露の元軍指揮官ら警告，AFP 通信 2015 年 5 月 2 日号，https://www.afpbb.com/articles/-/3047155［2023.9.19 確認］
4) 米国国立標準技術研究所：連邦政府の情報および情報システムに対する最低限のセキュリティ要求事項　Minimum Security Requirements for Federal Information and Information Systems，独立行政法人情報処理推進機構翻訳監修，2006 年 3 月，https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025322.pdf［2023.9.19 確認］
5) 米国国立標準技術研究所：重要インフラのサイバーセキュリティを改善するためのフレームワーク，独立行政法人情報処理推進機構翻訳監修，2018 年 4 月，https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000071204.pdf［2023.9.19 確認］
6) 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第 6.0 版，2023 年 5 月
7) 松山征嗣：医療機関におけるサイバーセキュリティ対策，病院，82 (9)，2023.
8) 鳥飼幸太：医療現場の BCP としてのサイバーセキュリティ対策，病院，82 (9)，2023.

PROFILE

とりかい　こうた：1979 年福岡県生まれ。2006 年九州大学大学院工学府エネルギー量子工学専攻博士課程修了（工学博士）。医学物理士。2002 年高エネルギー加速器研究機構特別共同利用研究員、2006 年量子科学技術研究開発機構博士研究員、2008 年群馬大学重粒子線医学研究センターを経て現在に至る。2011～2016 年特命病院長補佐（通信・エネルギー）。日本 M テクノロジー学会理事、（一社）医療サイバーセキュリティ協議会常任理事、日本医療情報学会会員、日本加速器学会会員。

令和5年10月1日発行（毎月1回発行） 通巻第407号 第34巻第10号

The Journal of JAHMC

［機関誌 JAHMC（ジャーマック）］
2023 October /vol.34 No.10

2023 10

Japan Association of Healthcare Management Consultants

INTERVIEW **新たな社会基盤としての医療DXを** 小笠原 克彦 氏

REPORT **デジタルヘルスの社会実装**
CASE1 リアルワールドエビデンス（RWE）の創出
CASE2 短縮・迅速化を実現した救急搬送システム
CASE3 モバイルクリニック&ドローンを積極活用

寄稿 **サイバー攻撃から診療記録を守るために何をすべきか？** 鳥飼 幸太

誌上研修 医療DXの新しい潮流 第4回
地域完結型医療をDXで推進
蔭山 裕之

公益社団法人
日本医業経営コンサルタント協会
Japan Association of Healthcare Management Consultants

IT-BCPをどのように実現するか

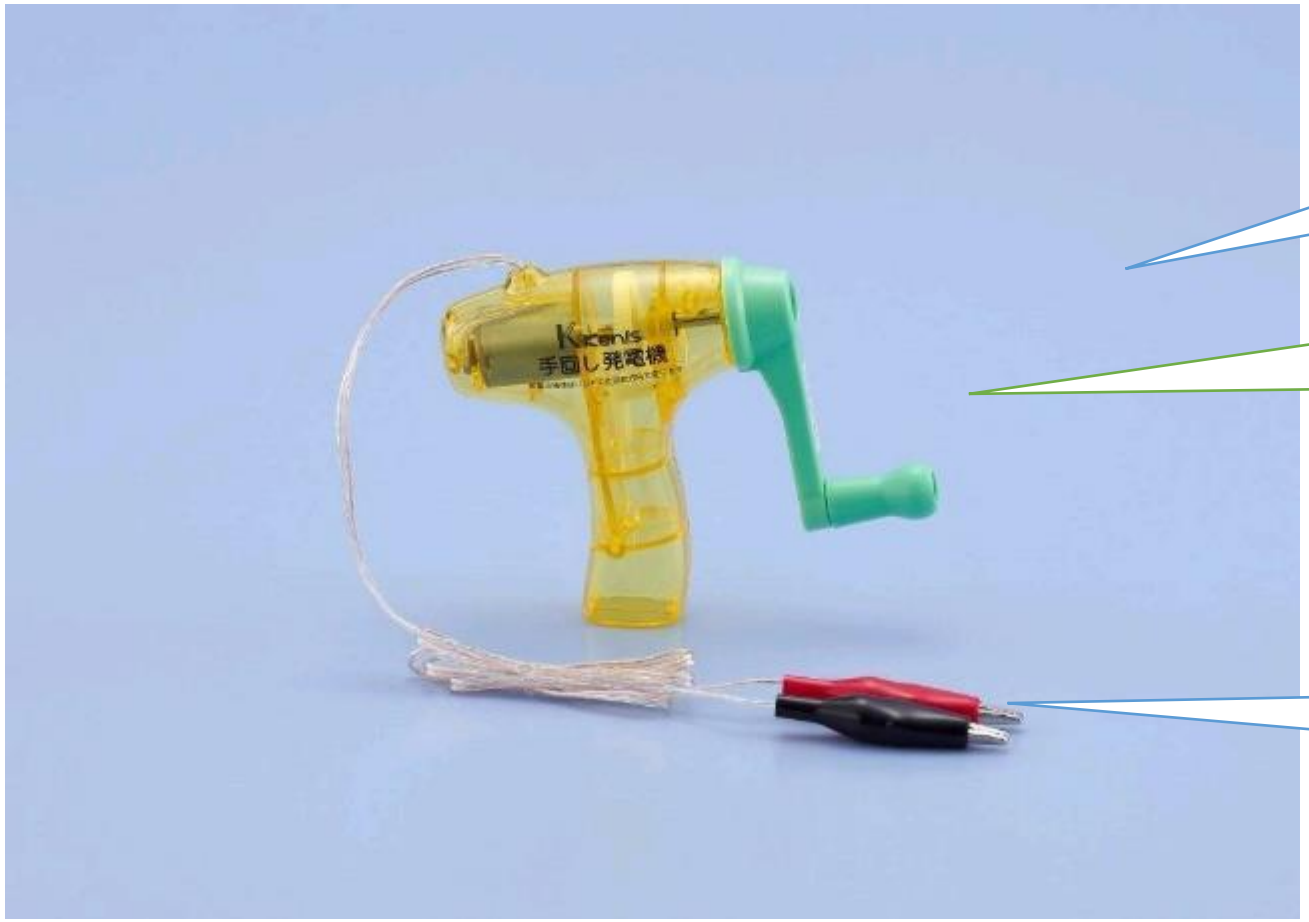
2023/11/23

群馬大学医学部附属病院システム統合センター
防衛医科大学校デジタル化推進本部推進補佐官
鳥飼　幸太

災害対策って、日常生活の役に立ちますか？

http://atasoku.net/2015/10/18/post-10287/

災害対策の維持費は揶揄の対象になっていませんか？



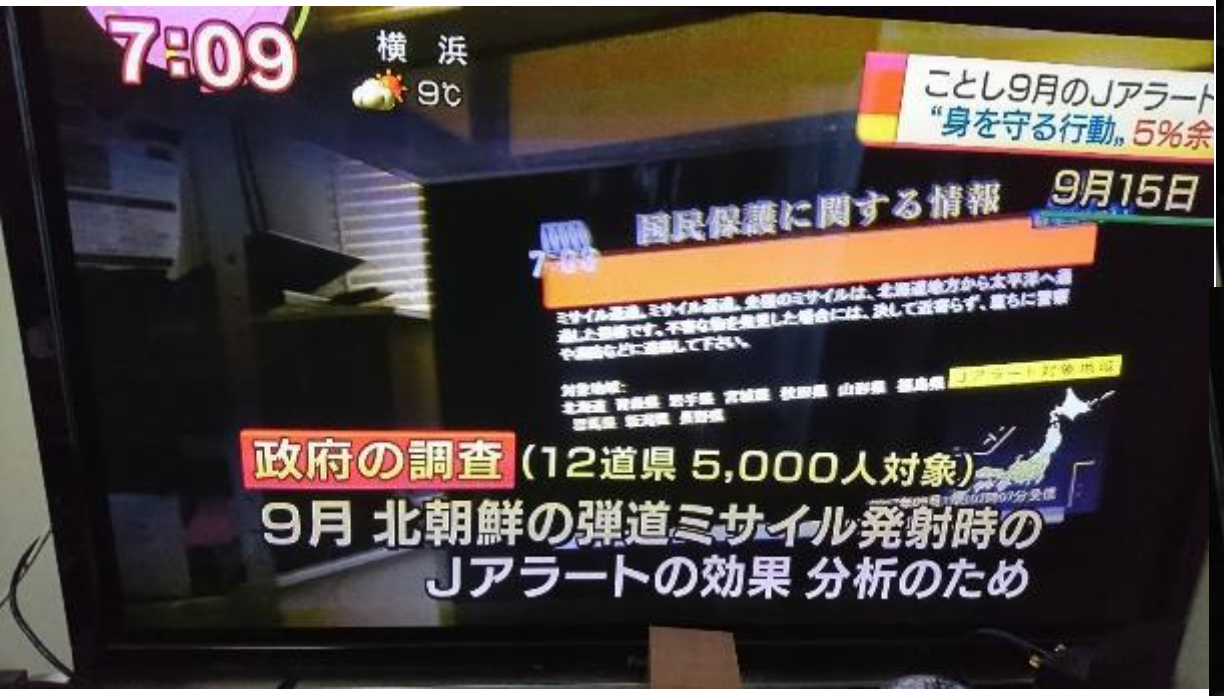
災害なんていつ来るか
分からないじゃない
意味あるの？

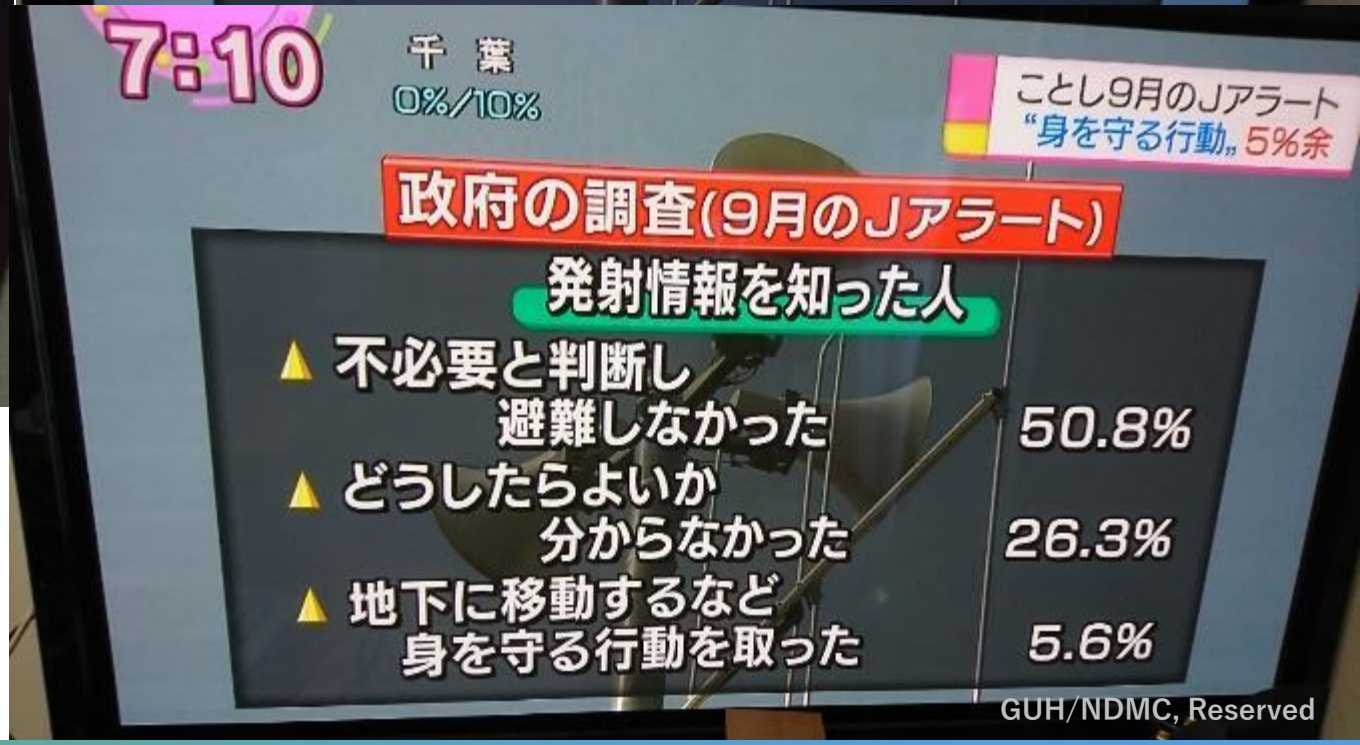
置き場所もかかる
維持費もかかる
起動は年1回の訓練だけ

経営だけだって
大変なのに…

http://science.wao.ne.jp/experiment/recipe.php?contents_no=50616

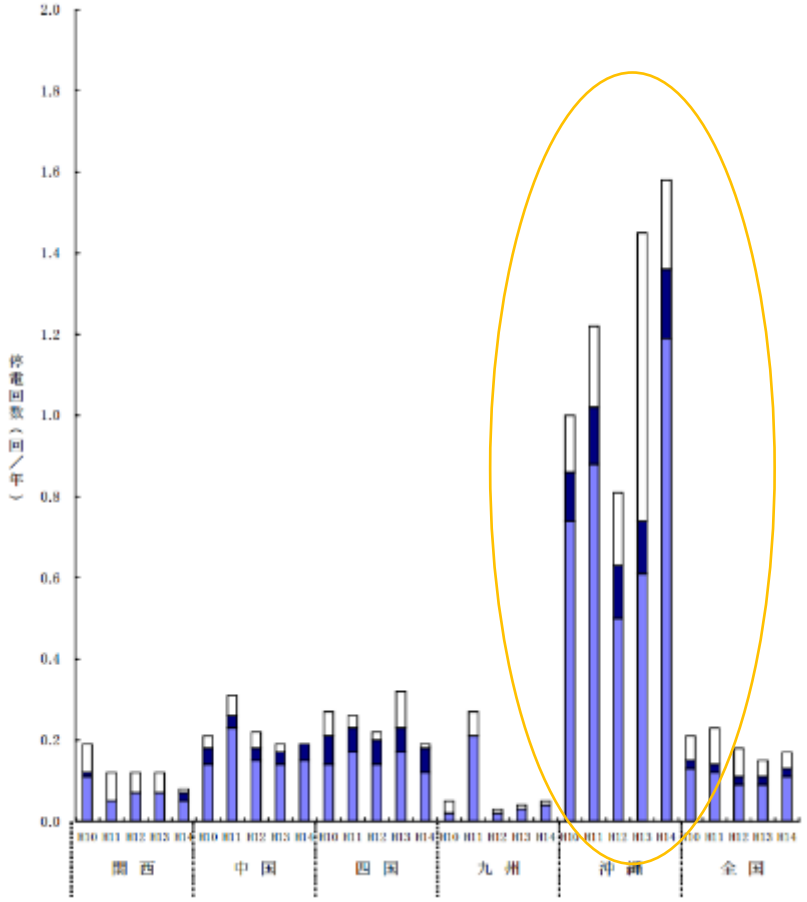
Jアラートと災害訓練



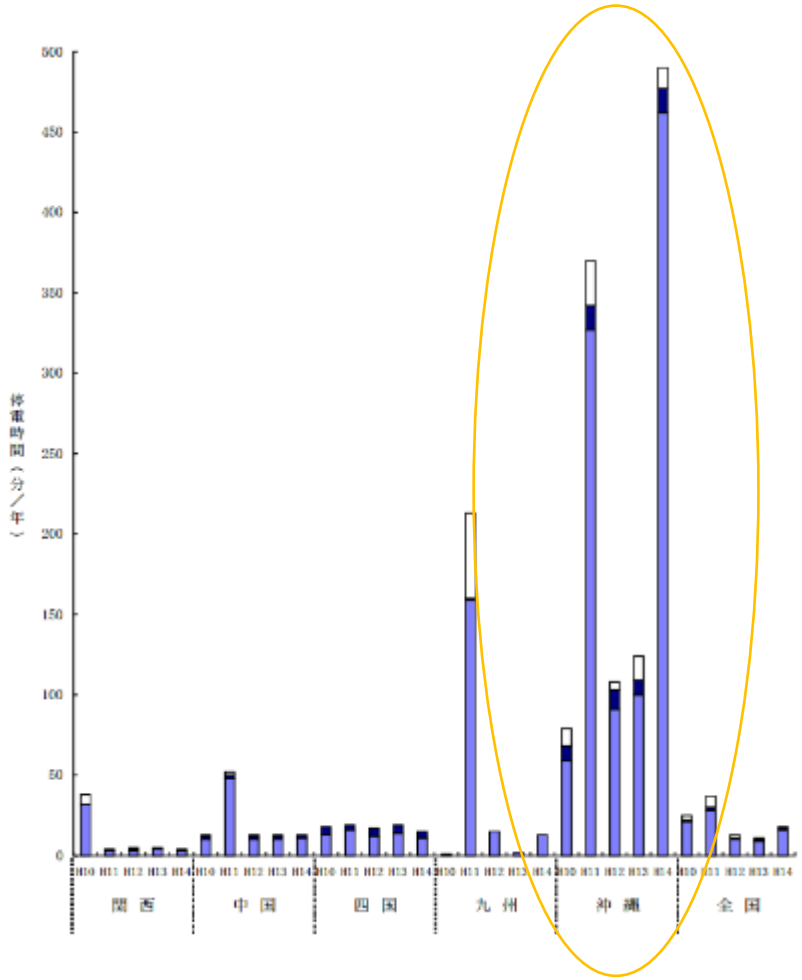


（参考）沖縄県の診療施設における電源無停電化の重要性

- 資源エネルギー庁　電気保安統計 統計表一覧 平成14年度電気保安統計 2　　需要家停電統計より
- 停電時間は病院診療継続に重大な支障を与えるため、病院施設全体の無停電化が必要不可欠である



停電回数



停電時間

頭頸部外科　24（1）：9～14，2014

日常の救急診療においてCT検査（3D画像）が果たす役割
―外傷例での有用性と使用の実際―

北川喜己　　筧　　裕香子

要旨：近年のMulti-detector CTの普及と進歩は，日常の救急診療，特に外傷の分野において大きな変革をもたらしている。Primary Surveyと蘇生処置を終えた後外傷パンスキャンを施行し，緊急処置を必要とする損傷の程度や範囲，活動性出血の有無などの情報をより早く得て，かつ症例によって3D画像での検索を追加し早期の根本治療へとつなげるようになった。3D画像は見落とし検索，骨盤骨折や四肢の脱臼骨折，不全切断，挫滅創などの骨ならびに軟部組織・血管損傷の状況把握，さらに緊急手術
の整備などでその有用性はさらに飛躍的に伸びると考えられる。
キーワード：MDCT，3D画像，外傷パンスキャン，JATEC，FACT

電源側からみたCTの負荷電力は
最大**100kW**

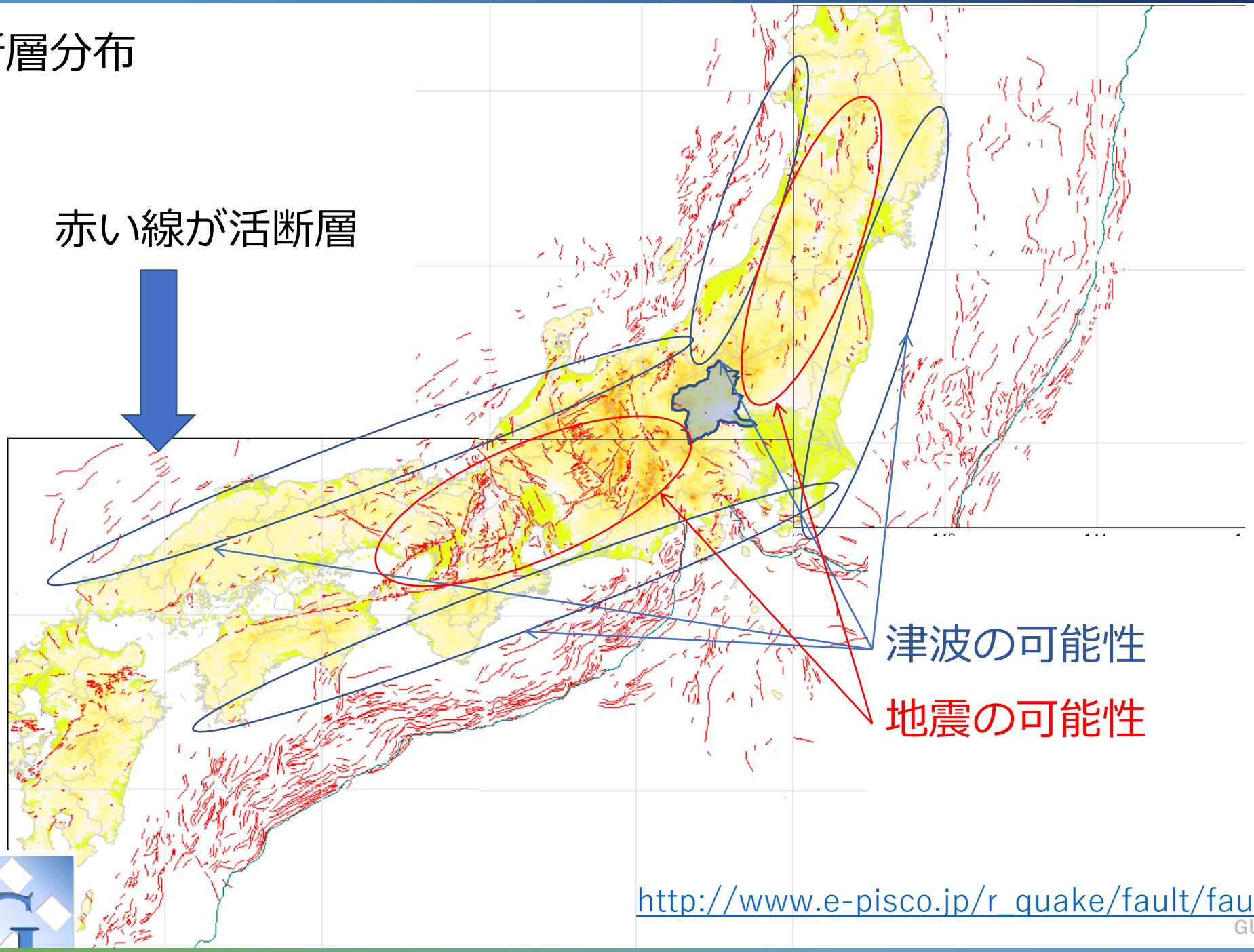
2011.3.12院内損傷点検時

太陽光でお湯が沸く装置

災害・事故における対応

日本の活断層分布

赤い線が活断層



津波の可能性

地震の可能性

http://www.e-pisco.jp/r_quake/fault/fault.html

震災備忘録

石川治　前病院長の記録

2011.3.11～4.1

石川　治　ISHIKAWA OSAMU

群馬大学大学院医学系研究科皮膚科学　教授

http://dermatol-h.dept.med.gunma-u.ac.jp/room_staff_detail.php?no=21

石川治前病院長の手記・ご講演記録より

3月11日（金曜日） 14:46 （M 9.0, 前橋：震度6弱）
地震発生，津波，福島第一原子力発電所全電源喪失

〈病院〉
・地震発生時，4件の手術が行われていたが無事終了．
・病院エレベーターに患者さん1名，付き添い1名が閉じ込められたが1時間後に救出．
・17:00. 昭和キャンパスにはケガ人なく，建物，機器にもほとんど被害がないことを確認．
・高崎を含めて県内で停電地域あり．DMAT派遣要請あるも，県内からの救急患者の受け入れを優先して本日の派遣は見送り．

〈大学〉
・高田学長は国大協の会議で文科省へ出張中．学長に電話連絡できず．メールにより学長，理事（平塚，中島，石川），入試委員会が後期入試の延期を決定して公表した．

～学習～
・今回のような非常時には携帯のメールが役立つ．一度送っておけば，いつかは届く可能性が高い．常に携帯電話の充電器は携行する．

石川治前病院長の手記・ご講演記録より

3月13日（日曜日）

計画停電実施の公表　→　苦難の始まり

・午前10時から県庁で開催の23年度の初期研修ガイダンスへ出席.

東日本大震災における計画停電対応

BCP

- **石川治前病院長の手記・ご講演記録より**

- 3/12　計画停電の可能性報道
  在宅酸素療法者への電力確保法伝達
- 3/13　発電機能、情報ネットワークの緊急調査
  自家発電能力を最大3000kWと見積もり
- 3/14　石川治病院長が診療継続を決定
- 緊急被ばくマニュアル配布
- 計画停電予定時間帯での自家発電切り替え運用開始
- 3/15　自家発電時運用マニュアルの作成
- 3/16　最初の計画停電実施
- 3/17　1日最大6時間の停電下で外来・救急機能を維持
- 3/18　病院運用フローの策定

・15:00　病院運営会議を危機対策本部とし，「病院機能の維持を最優先すること」を確認．医療情報部の鳥飼テニュア助教（重粒子線医学研究センター）を対策本部メンバーとして加えた．
・15:20　計画停電実施．

・18:00　全病棟巡視．多くの職員は冷静沈着に対応していた．しかし，「病院周囲の住宅は明かりが点いているのに，なぜ病院は自家発電なのか」という疑問が投げかけられた．この段階では，自分自身も病院への配電システムが周囲住宅とは異なるためだという誤った理解をし，不正確な説明をしていた．
・鳥飼助教は，電力室に詰めて電力消費量をモニタリングしながら，医療サービス課小出課長らと連携して消費電力量が自家発電量（白コンセント用1800kW）を超えないよう指示していた．
　この間に各施設（病棟，外来，中央診療棟，医学部基礎棟および臨床研究棟，保健学科棟，生体調節研究所）の消費電力のデータを収集，分析していた．計画停電の長期化に備え，予定時間より1時間前に各施設の電源を切った大きな理由の1つはここにあった．

大竹英則前技師長（左）

群大病院における電力消費要素と利用限界

No	施設または設備	電　力 [kW]	電力需要特徴
1	病院最低維持電力	1400	常時消費、電子カルテサーバー
2	CT	50	間欠・不定期
3	電灯・暖房	50-100	常時消費
4	MRI	20-40	間欠・不定期
5	CR	＜10	常時消費
6	単純撮影	＜10	間欠・不定期
7	検体検査装置	100	立ち上げ時に　最大電力消費
8	病棟系 HIS 端末／情報機器	＞50	
9	外来 HIS 端末	150	PC100 台、プリンタ 100 台程度
１０	放射線治療装置	50	間欠・不定期
１１	重粒子線装置非常電源系	35	真空維持に限定
１２	臨床研究棟	400	常時消費
１３	医学部基礎棟	400	常時消費
１４	動物実験棟	300	常時消費
１５	生体調節得研究所	250	常時消費
１６	保健学科	150	常時消費

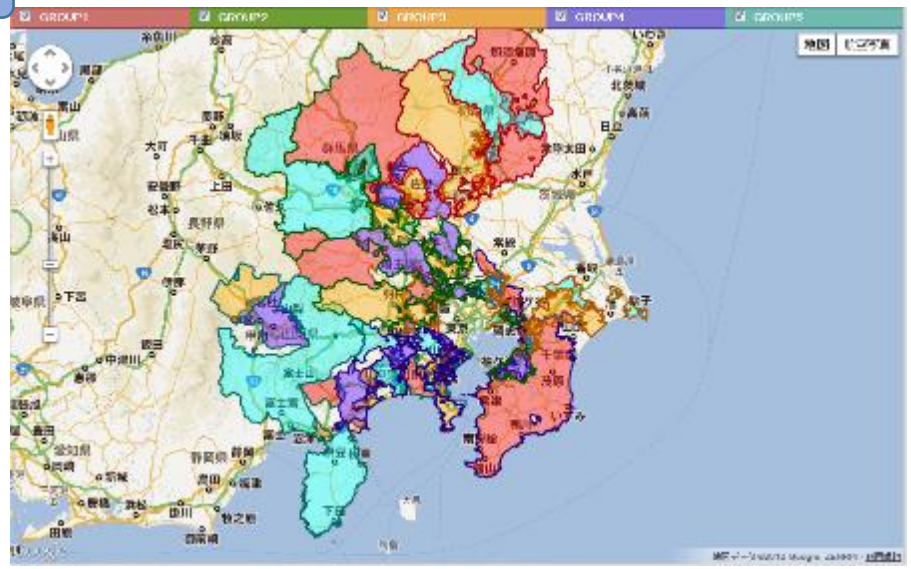
キャンパス内自家発電機で賄えるのは2000kWが限度

貴重な生物系冷凍研究素材を失った

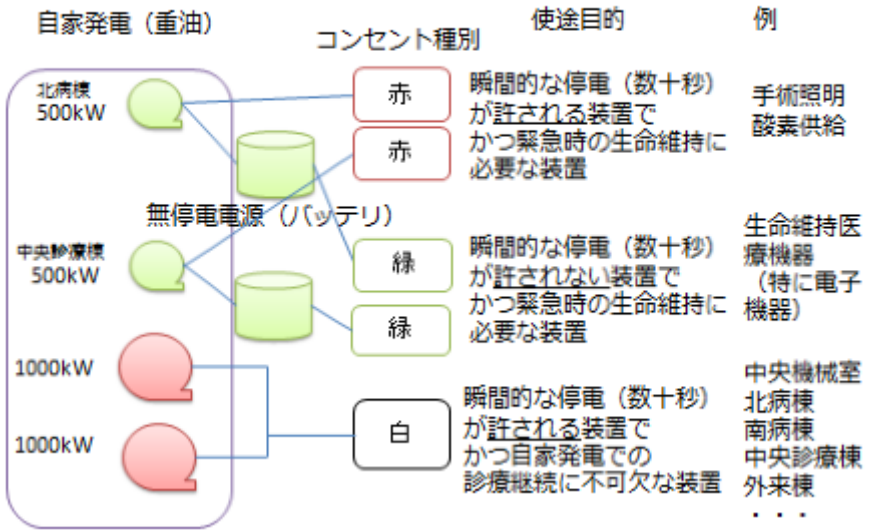
東日本大震災における計画停電対応

BCP

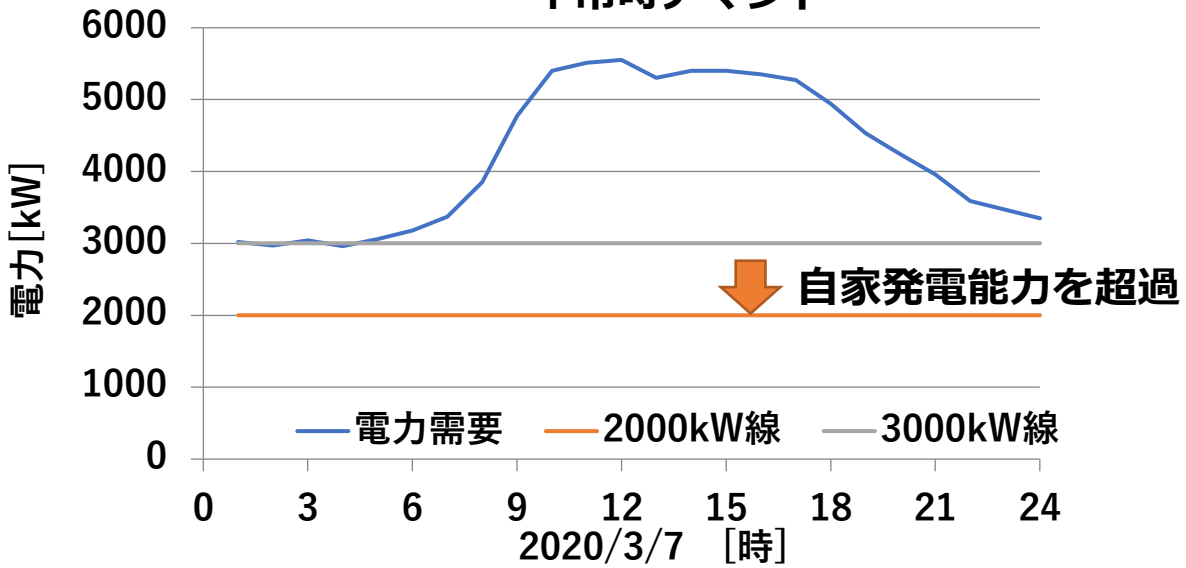
- **計画停電区分**



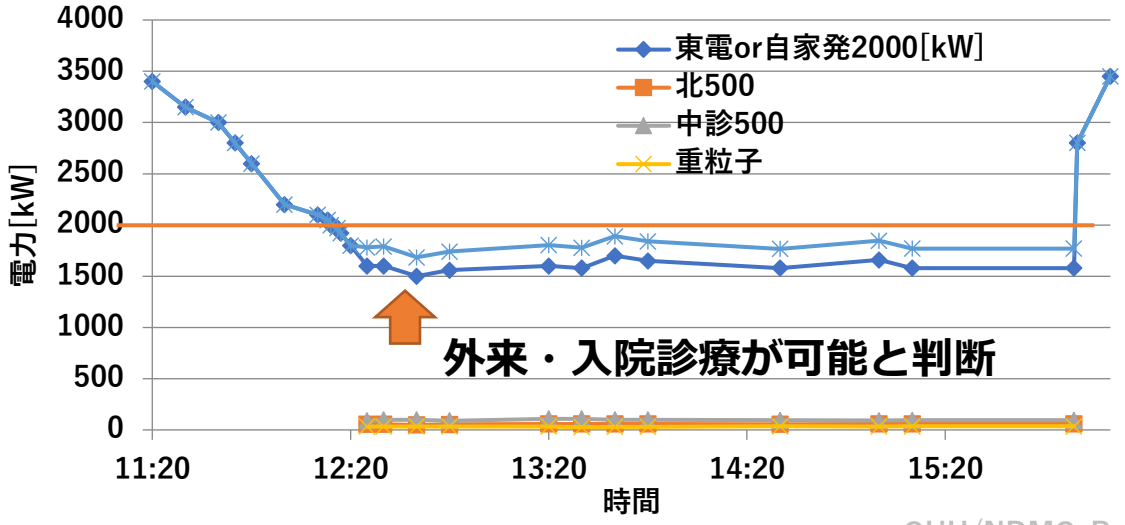
自家発電システムとコンセントの役割



平常時デマンド



緊急減力試験によるフロア別デマンド



石川治前病院長の手記・ご講演記録より

3月23日（水曜日）計画停電実施　18：20～20：00

・18：20．計画停電実施．仕事ができないので帰宅．
トラブル発生
・19：20．**小玉部長**から電話．**1000kW自家発電機のうち1台しか稼働していない**との連絡あり．
・19：40．電力室に到着．2台の発電機が同調しないことが原因．東電の坂口副支社長に携帯電話で事情を直接説明．2回の電話でのやり取り後，20：00に東電より給電あり．周囲住宅の給電は20：20であった．この後，2台の発電機を様々チェックし，発電機自体に問題ないことを確認した．
・明日の計画停電予定15：20～19：であるため，**15時までに終わらない手術は延期ないし中止**と決定．関連各科への連絡を手術部看護師から発信（これが，明朝に生じる問題のもとであった）．
・22：20．帰宅．

～諺どおり～
「**禍は忘れたころにやってくる**」は，本当だった．計画停電への対処もルーチン化されたと思った矢先の発電機トラブルだ．

ネットワーク強靱化・無停電化（棟スイッチ・PoE含めて実施）

平成25年3月 上毛新聞

群大病院が自家発電増強

災害時の機能維持図る

群馬大医学部付属病院（前橋市昭和町）は、計画停電の対象となった東日本大震災の経験を基に、関東地方が災害に見舞われても病院機能を維持できるよう、自家発電装置の整備などに取り組んでいる。今月末には自家発電能力を現在の1・6倍に増強、新年度には燃料となる重油の備蓄量も増やし、「東京電力からの電力供給が完全に止まっても1週間は持ちこたえられる」（野島美久病院長）態勢を整える。

同病院は震災発生直後の2011年3月、全国の国立大付属45病院の中で、山梨大とともに2病院だけ計画停電の対象となった。約3000キロ・ワットの自家発電能力を備えてはいたものの、平時には医学部と合わせて約7000キロ・ワットを使っていた。そのため特命病院長補佐の鳥飼幸太助教（33）らは、計画停電や突発的な大規模停電など状況に応じた対応手順を作成。停電中も診療などを続けるための対応に追われた。

当時は、幸いなことに最も電気使用量の大きい重粒子線医学研究センターがメンテナンス中だった。加えて医学部の研究機能を極力止めたことで、自家発電のみで外来患者の受け入れや入院患者の治療、手術を通常通り行えたという。鳥飼助教は「真夏や重粒子センターの稼働時なら乗り切れなかった」と振り返る。

危機的状況を克服するカギは、病院内で使用する機器の電力使用量を測定してデータ化したことだった。鳥飼助教らは、各機器の電源を順番に切って差分を記録し、電気使用量を測定した。これにより、電気使用量が大きく再起動に時間がかかるコンピューター断層撮影法（CT）装置も確信を持って稼働させられたという。

同年7月には、一部設置されていた停電時にも電気が流れ続けるようにする「無停電装置」を200か所増設。同年夏と秋には突発的な停電が発生したが、病院内は停電が起きたことにすら気付かないほど影響

前橋市城東町の中央前橋駅で

平成29年2月26日 毎日新聞

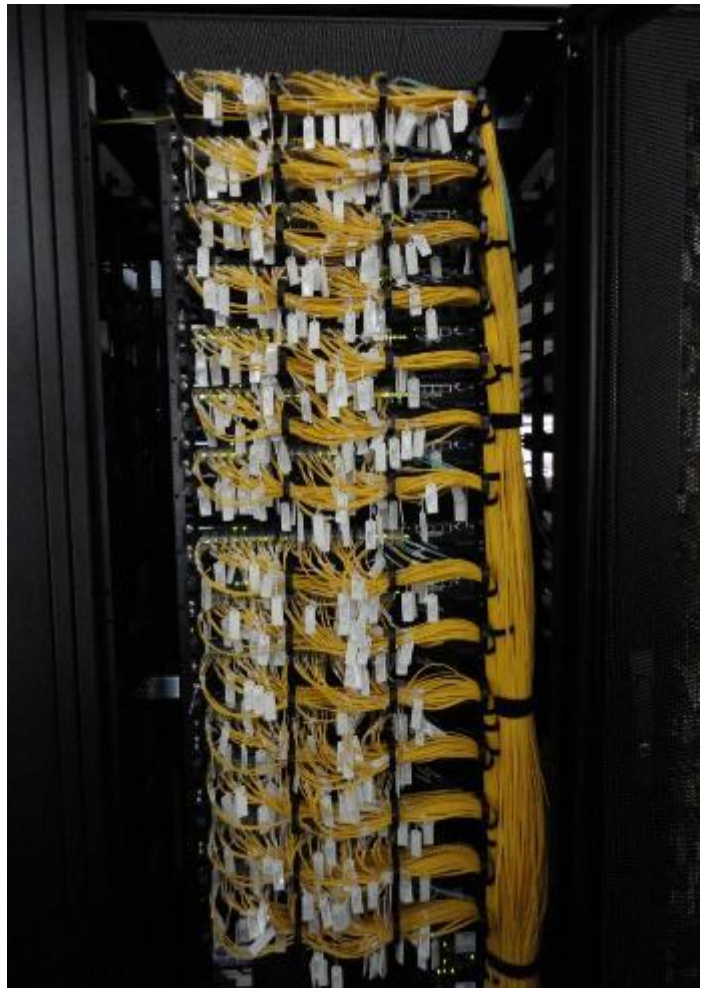
医療支える高速ネット

瞬時にカルテ 患者対応充実

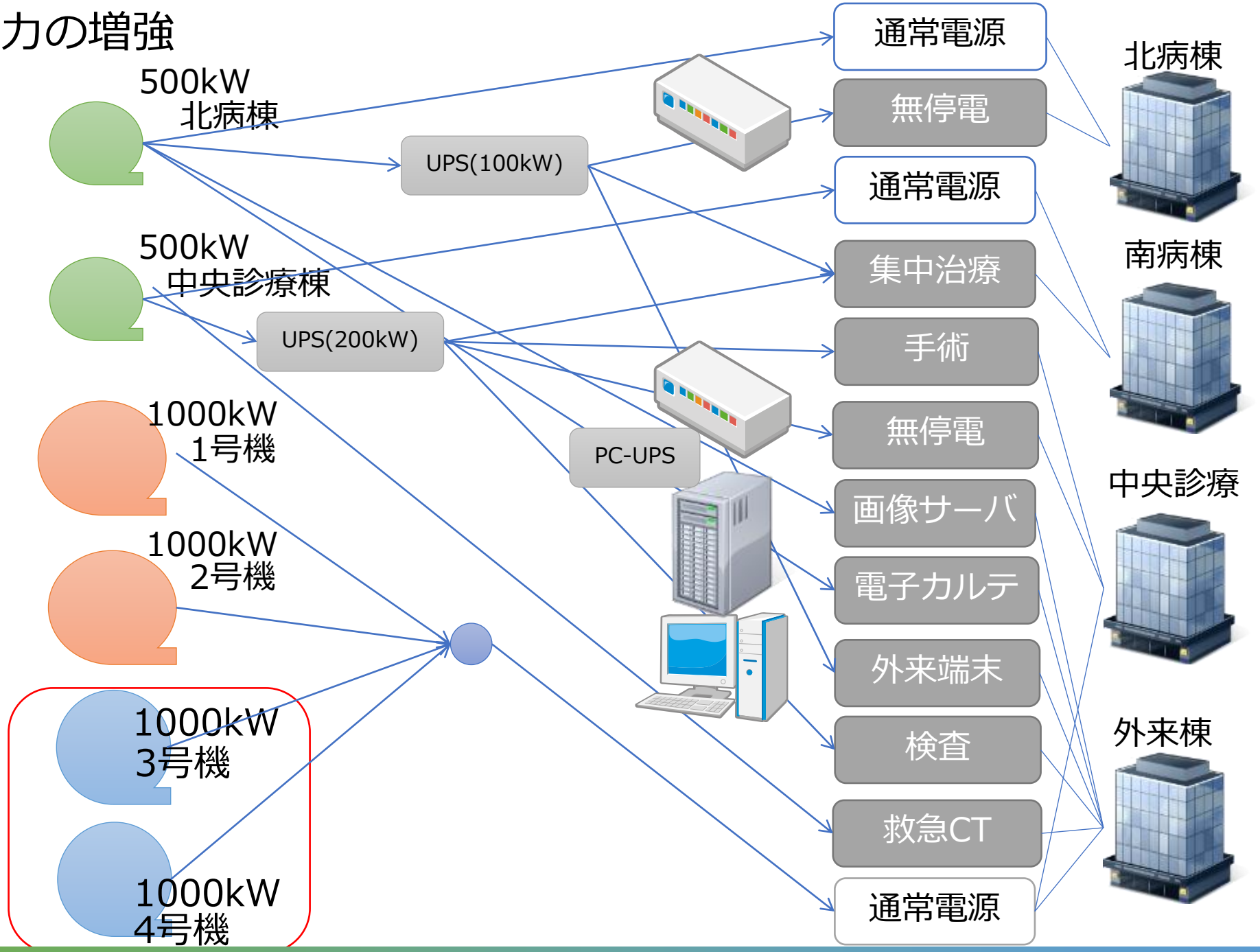
群馬大病院が構築

災害時も迅速回復

FTTD1300本を敷設

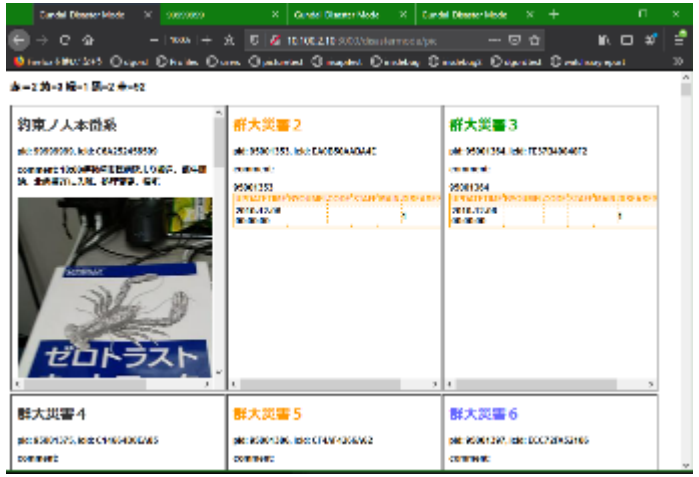


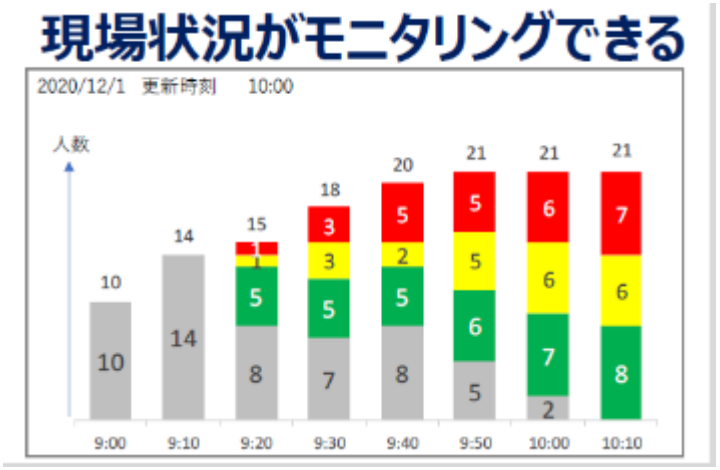
自家発電能力の増強



準災害としてのサイバーセキュリティ訓練・対策の必要性

- 災害トリアージ訓練を2013年より毎年開催
- ICトリアージタグを用いた現場状況のリアルタイム可視化
- 病院全域で動作する無線シンクライアント端末→災害時運用に貢献





医療情報セキュリティと災害BCPは多くの点で共通しています

医療安全　BCP

- **2021年: 千葉大学病院、岡山大学病院**

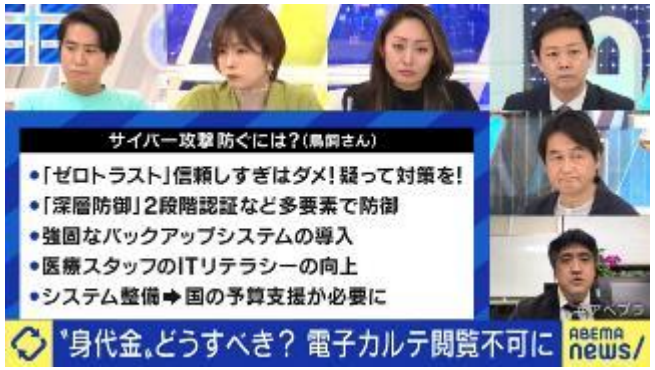
（世界中で）コロナ禍での大量のネット接続

→ハッキングによる
犯罪リスクが急激に増大

知らない間に患者が変死…
電子カルテが開かない！！

Medical Device Cyber Security Council
医療機器サイバーセキュリティ協議会

半田病院サイバー攻撃に関する
速やかな対応提言



2023年電子処方箋試行、さらにリスク増

ドイツ・デュッセルドルフ
手術不能→
緊急搬送患者が死亡
(2020.9)

IT業界全体がサイバー犯罪の
強い危機感を表明

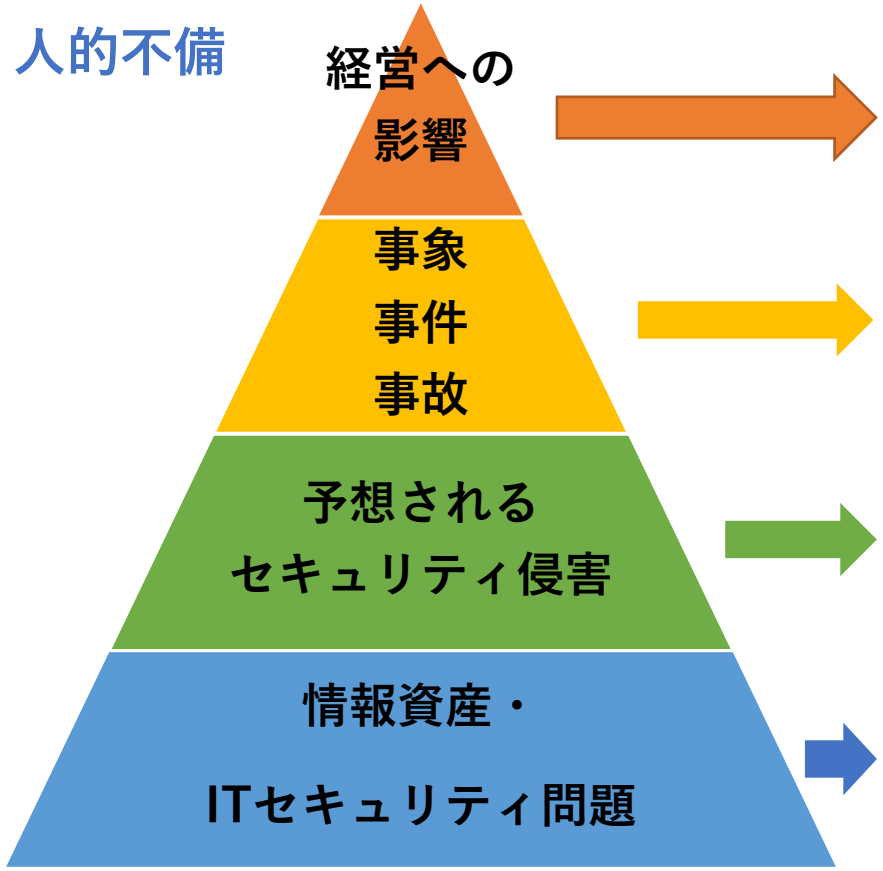
十分にシステム内情を把握
トラブル時の速やかな初動
脆弱ポイントを重点ウォッチ

物的不備、人的不備が病院経営に損害を与えるまで

月刊インナービジョン6月号

A 物的不備

B 人的不備



Confidentiality（機密性）	Integrity（完全性）	Availability（可用性）
社会的信頼の低下、依頼先の変更 損害賠償、依頼獲得の減少 読影業務の停止		
B3 ストーキング 医療情報の暴露 スパイ行為の発生	A5 システム誤作動 偽データの送受信 紛争の誘発	A4 システム稼働停止 病院間通信途絶
B2 利用状況の漏洩 画像・レポートの 漏洩	A3 プログラム改竄 データ改竄	A2 プログラム改竄 データ改竄 通信経路の遮断
A1 ソフトウェア脆弱性 設定不備 プロトコル・暗号強度の不備 ネットワーク・通信の不備	B1 運用上の不備 利用者による改造 認証の不備 ワーム・ウィルス感染	

CISOハンドブック　業務執行として考える情報セキュリティ Ver.1.1β、特定非営利活動法人日本ネットワークセキュリティ協会
社会活動部会 CISO支援ワーキンググループ、2018年6月 p10
図1 ビジネスリスクとセキュリティリスクの関係（コミュニケーションシステム）を参考に改変

診療における病院情報セキュリティの考え方

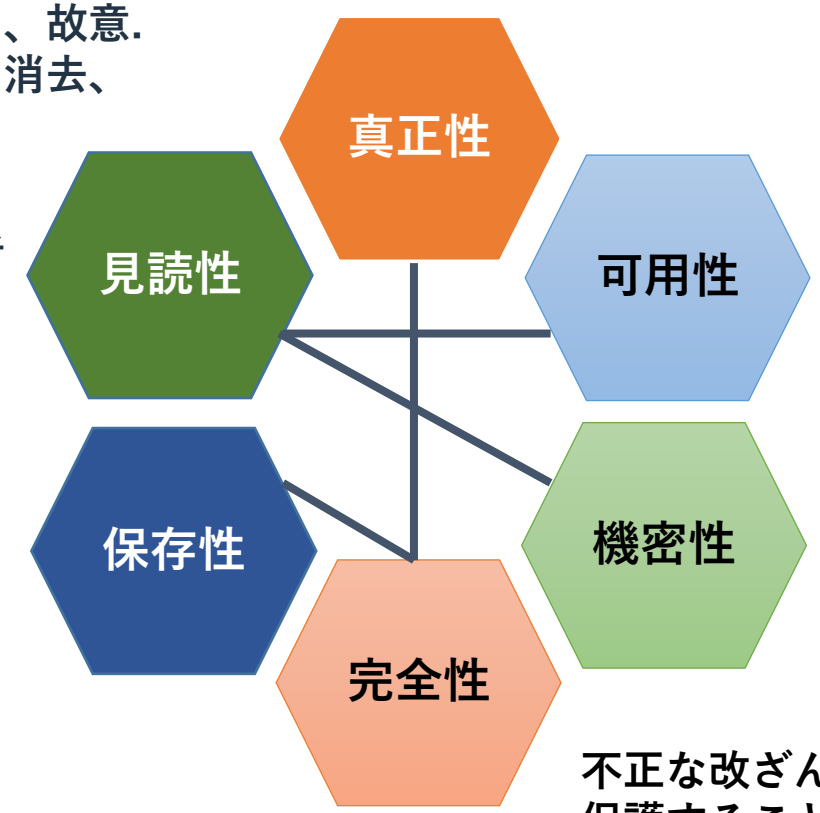
- 電子保存の三原則（真正性、見読性、保存性）
- 情報セキュリティの三原則（可用性、機密性、完全性）

2022.11.8
読売新聞31面全国版13版

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意.または過失による、虚偽入力、書き換え、消去、及び混同が防止されていること

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で.見読可能な状態にできること

記録された情報が法令等で定められた.期間に渡って保存されること



利用者が必要なときに安全に.アクセスできる環境であること

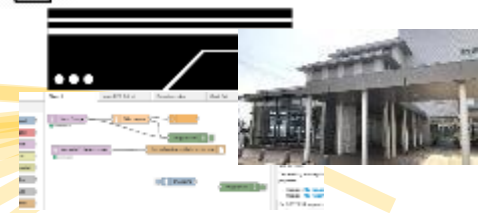
限られた人だけが情報に接触できるように制限をかけること

不正な改ざんなどから.保護すること

スマートホスピタルの機能と医療サイバーリスクの増大

- 診療シーンでの判断や指示・支援が「患者の通院・入院の全期間で、治療目的を達成するように」
- **診療プロセス中にクリティカルなデジタル装置の増加→攻撃ポイント・リスクの増加**

医療ロジック
統合制御サーバ



検査日近くに
事前お知らせ
予約日最適化計算

対話自動文字起こし
推奨検査候補提示

診療計画書作成支援
ベッドコントロール
最適化計算

禁忌・重複
タイミング/量
確認支援

変更迅速同報
AR/MR支援
患者状態AI推定

病棟リハ支援

来院 → 受付 → 問診 → 診察 → 検査 → 入院 → 投薬 → 手術 → リハ → 退院 → 地域

過去病歴・診療歴の
迅速参照

電子化入力
事前スクリーニング

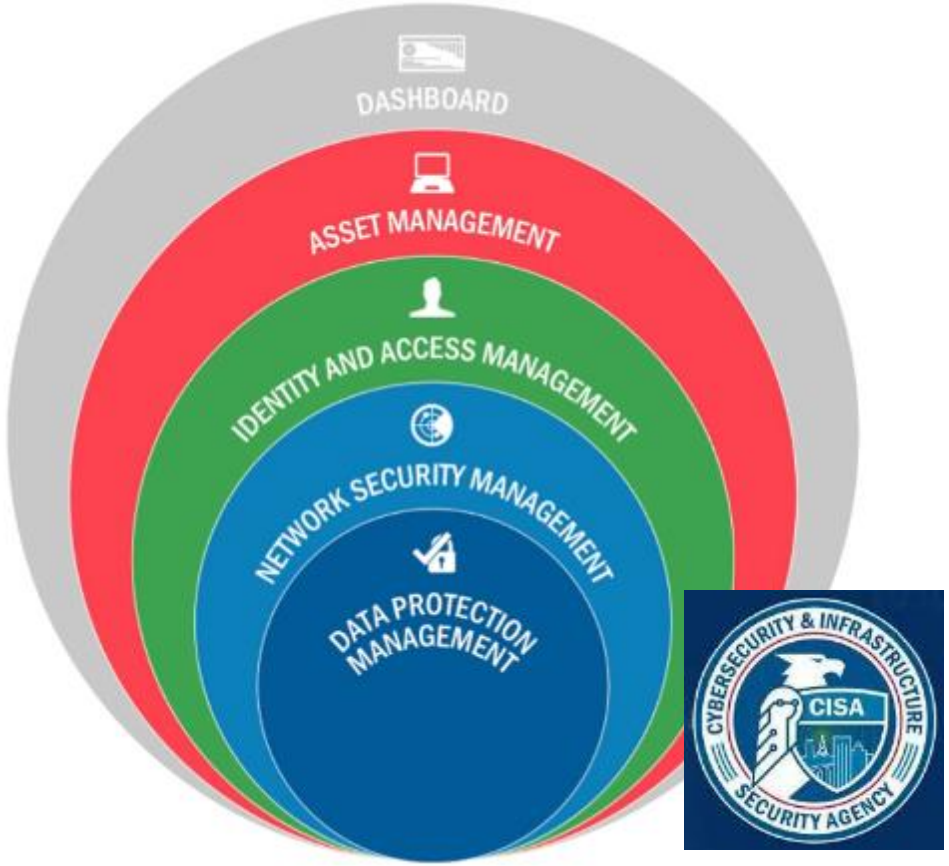
自動同意ステータス
チェック
自動患者照合支援

院内ロジスティクス・オートメーション

NIST CyberSecurity Framework（CSF）
CISA Continuous Diagnostics and Mitigation (CDM)

CSF

CDM

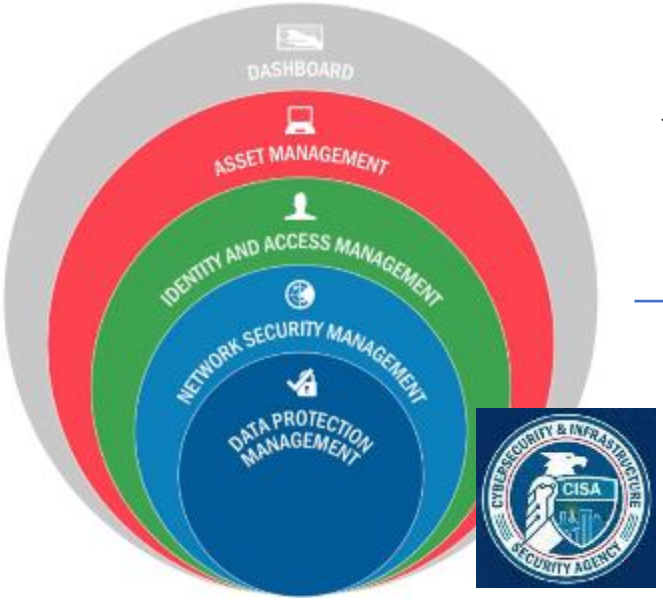


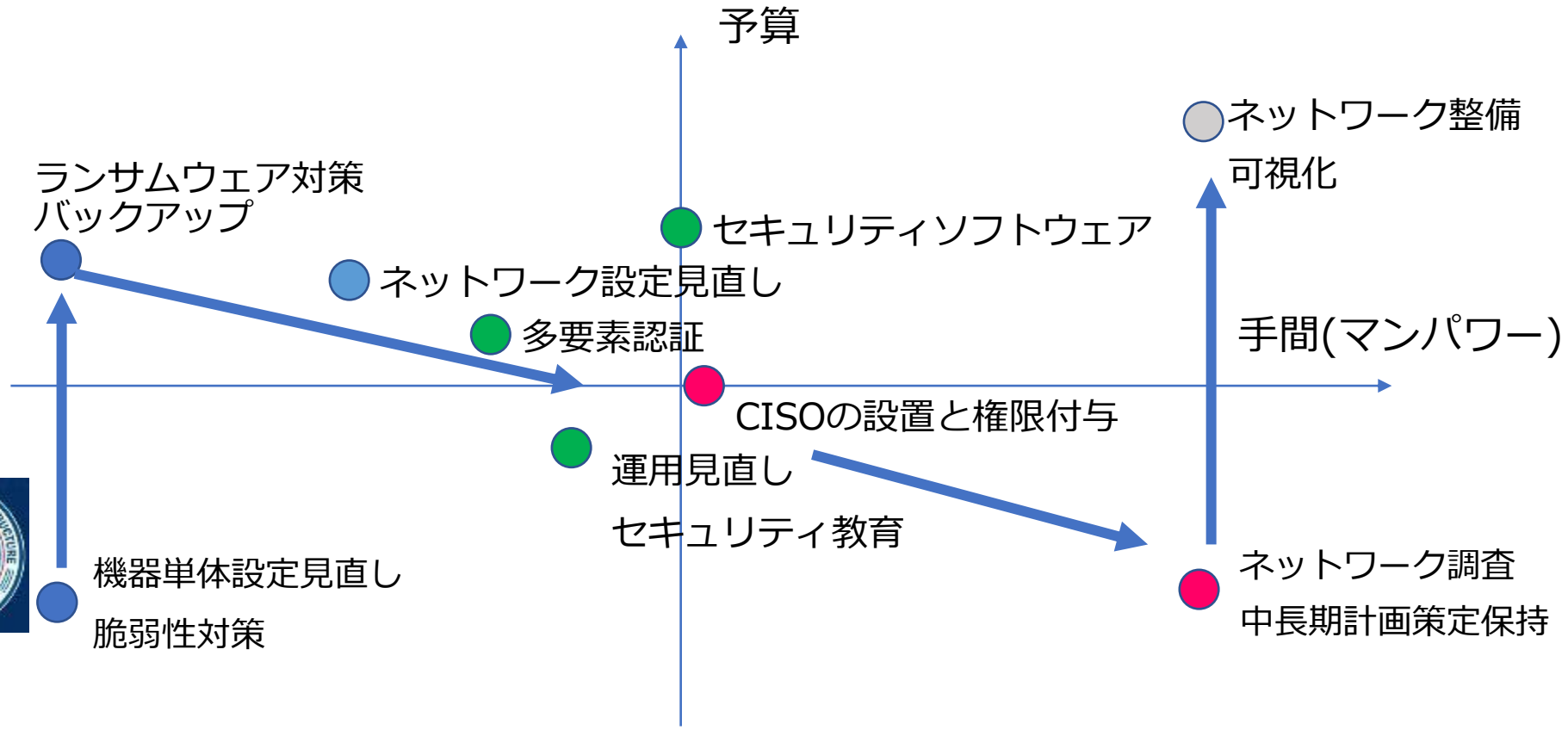
CSFにおける医療機関内情報システム要素の検討・対策箇所

フレームワーク機能	検討箇所の例	対策ツールの例	対策運用の例
識別 ID	病院情報システム全体の接続機器・IPアドレス、セグメンテーション、接続経路、脆弱性等の把握	ネットワーク可視化ツール、脆弱性把握ツール	資産管理手順に沿った調査（リストアップ）、脆弱性情報の迅速把握
防御 PR	外部保守接続箇所（放射線診断・治療装置、PACS/電子カルテ等）、DMZ端末、診療録サーバ	VPN、ランサム対策ストレージ	情報漏洩を起こさない院内情報運用研修、診療情報アクセス制御設定、ファイヤウォール設定、セキュリティ保守契約の充実、バックアップ手段と階層、運用の策定と実装
検知 DE	電子カルテ端末挙動、ネットワークトラフィック監視、ストレージ/CPU負荷変動	IDS、EDR(D)、NDR(D)	日常のシステムパフォーマンスモニタにおけるトレンド把握と差異の知覚、対策ツールが提供するダッシュボード機能による監視
対応 RS	不特定多数や多数のスタッフがアクセスできる機器、電子カルテにアクセスできる端末またはサーバとポート、攻撃検知時のカルテデータバックアップ経路	IPS 、 EPP 、 EDR(R) 、NDR(R)	インシデント時連絡先の把握と役割分担の検討、医療安全と情報保全、診療継続を両立する対策方法やツール挙動設定の検討、インシデント対応訓練への参加
復旧 RC	電子カルテサーバを中心とする保存義務を有する情報サーバ、診療継続に不可欠な情報端末の運用	バックアップ復元ツール、情報サーバ仮想化インフラ	復元手順のBCPへの記載、復元テスト、環境設定を伴った包括的サーババックアップの実施、バックアップ周期の短縮化

CDS＝「できることから始めよう、次第に良くなる計画を立てよう」

- Continuous Diagnostics and Mitigation (継続的なセキュリティ診断とリスク低減)
- いきなり「盤石のセキュリティ」には到達できない（それでも今から始める価値がある）
- 「抑えるべき急所の順序」が存在する
- 対策には「すぐできるもの」と「計画し予算と人手がかかるもの」に分けられる





CSFとCDM：どちらから始めるか？

	Cyber Security Framework (CSF)	Continuous Diagnostics and Mitigation (CDM)
段階の考え方	Tier （分野ごとにレベルを評価）	Core （保護対象の順序を指定）
着手順	攻撃者の侵入経路に沿って	防御者の保護資産に沿って
適した始め方	システム更新の計画開始時	随時
実施時のハードル	資産管理の手間が大きい （調査の支援役務？） シェル型の保護で終わりがち 可用性の確保	より高いレベルでの防御を見込む場合、 資産管理が避けられない 大規模インフラ改修計画を

サイバー攻撃に対してIT-BCPを実現するには

- 「もし、私がサイバー攻撃者で、病院機能を効果的に毀損させる意図があったら」と考えてみる
- 医療機関側は、侵害覚知直後には「全ての被害可能性」を想定し、「攻撃対応」と「診療継続」を両立させる

Aim	人命に直結する装置・手技への攻撃		医療ワークフロー(指示・判断・連携)の混乱・停止への攻撃						
Vector	生命維持・精密静注 誤動作や停止	麻酔装置・手術装置 誤動作や停止	受付・会計・キー検査 部門システム機能停止		オーダ・ステータス 不信頼化・機能停止		系内侵入 漏洩・脅迫		
Target	入院病棟 ICU/SCU	IoTハック 通信切断 電源系攻撃	手術室	IoTハック 通信切断 電源系攻撃	外来・病棟 病院全域	改竄・暗号化 通信切断	外来・病棟 病院全域	改竄・暗号化 通信切断	潜伏活動 DBアクセス 外部送信
IT有BCP	予備医療装置の準備 修理・再稼働手順訓練	参照サーバ・端末の準備 ネットワーク等冗長化 非常時縮退IT運用訓練・高速復旧体制整備							N/A
IT無BCP	手動操作医療器具の準備 緊急時搬送受入先確保				紙運用用紙・運用準備 外部参照系、安全な患者誘導フロー確保				対策マニュアル
	全体BCPとの運用整合（特に、自家発電強化下での電力利用用途優先順位を厳格に定めておく）								
サイバー対策	IPS/ネットワーク監視 脆弱性対策	IPS/ネットワーク監視 制御PCのサイバー保護	5段階防衛の全て 防御/検知/隔離/対応/復旧＋組織訓練						
先進対策	予備装置の地域プール体制		予備サーバの地域プール 冗長化・SaaSミラー						リスク保険
	CSIRT / 医療CISO職配置 / 独立稼働端末指定やサーバの高SLAレベル運用 / CDM戦略の策定と運用								

関連項目：医療セキュリティ責任者/管理者が必要とする能力について

	病院情報セキュリティ責任者	病院情報セキュリティ管理者	病院情報セキュリティ従事者
基本能力	他院のCISO補の指導育成が行える能力を有すること	自立して自院の病院セキュリティを向上できる能力があること	CISO補の指示を受けて、必要な実務作業ができること
攻撃者視点：NIST CSF	CSFの改善方法についてCISO補ならびに他院の経営層にアドバイスできること	自院のCSFについて調査できること	自院のCSFについて理解できること
防御者視点：CISA CDM	CDMの改善方法についてCISO補ならびに他院の経営層にアドバイスできること	自院のCDMについて調査できること	自院のCDMについて理解できること
緊急対応	医療ワークフローならびに医療ITシステムに配慮したサイバーセキュリティデザインが提供できること	自院における長期システム改善計画をセキュリティ、運用改善の両面から検討し、起案できること	自院において策定された長期システム改善計画を理解し、適切なベンダーに対して調査依頼ができること
Security By Design	長期間の診療停止に際してシステム的、医療ワークフロー的に配慮すべき点を復旧段階に応じて適切にアドバイスできること	診療停止を伴わないインシデント（部門システムの停止など）時に、院内状況を適切に把握し、バックアップ保全などの1次的緊急対策を指示できること	提供されている適切な手段に基づき、日常的な脅威を監視できること
保守業務	実務負荷、コスト、長期的視点のバランスが取れた保守計画を提案できること	自院の全体に対してセキュリティ保守業務で調査すべき点を適切に割り出せること	CISO補の立案に基づき、業務負荷の変化について正確な情報を提供できること

関連項目：医療セキュリティ責任者/管理者が必要とする能力について

番号	カテゴリ
1	医療装置・直接
2	医療装置・間接
3	関連装置・間接
4	物理インフラ・間接
5	基幹情報サーバ・間接
6	情報サービス・間接
7	診療データ運用・間接
8	不法対策・間接

カテゴリ1: 医療装置・直接

分野	患者危害リスク	内容	対策項目
医療装置	直接	シリンジポンプ動作不良	ネットワーク通信障害下でも稼働継続する
医療装置	直接	シリンジポンプ動作不良	予備シリンジポンプを有する
医療装置	直接	麻酔装置動作不良	予備麻酔装置を有する
医療装置	直接	酸素吸入器動作不良	電子的制御でない酸素吸入方法が準備されている
医療装置	直接	人工呼吸器動作不良	予備人工呼吸器を有する
医療装置	直接	人工呼吸器動作不良	蘇生バッグでの換気を手技で提供できる
医療装置	直接	人工透析装置動作不良	複数台の人工透析装置を有する
医療装置	直接	ペースメーカー動作不良	代替ペースメーカーの在庫を有する
医療装置	直接	持続血糖測定/管理機器動作不良	別手段による血糖測定/管理手段を有する

カテゴリ2: 医療装置・間接(1/2)

分野	患者危害リスク	内容	対策項目
医療装置	間接	CT装置（本体）動作不良	複数台の当該装置を有する
医療装置	間接	CT装置（本体）動作不良	故障時代替検査手段が運用できる
医療装置	間接	CT装置（制御端末）動作不良	複数台の情報端末を有する
医療装置	間接	MRI装置（本体）動作不良	複数台の当該装置を有する
医療装置	間接	MRI装置（本体）動作不良	故障時代替検査手段が運用できる
医療装置	間接	MRI装置（制御端末）動作不良	複数台の情報端末を有する
医療装置	間接	PET装置（本体）動作不良	複数台の当該装置を有する
医療装置	間接	PET装置（本体）動作不良	故障時代替検査手段が運用できる

カテゴリ2: 関連装置・間接(2/2)

分野	患者危害リスク	内容	対策項目
医療装置	間接	PET装置（制御端末）動作不良	複数台の情報端末を有する
医療装置	間接	放射線治療装置（本体）動作不良	複数台の当該装置を有する
医療装置	間接	放射線治療装置（本体）動作不良	治療引き継ぎ可能な医療機関と連携できる
医療装置	間接	放射線治療装置（制御端末）動作不良	複数台の当該装置を有する
医療装置	間接	手術室内電子/電気機器動作不良	複数の手術室を有する
医療装置	間接	手術室内電子/電気機器動作不良	同手術を代替実施できる連携医療機関が搬送可能な距離に存在する
医療装置	間接	バイタルモニタ動作不良	複数台の当該装置を有する

カテゴリ3: 関連装置・間接

分野	患者危害リスク	内容	対策項目
関連装置	間接	検体検査装置（本体）動作不良	外注サービス先により検査実施が継続できる
関連装置	間接	検体検査装置（情報端末）動作不良	予備の情報端末を有する
関連装置	間接	調剤時使用機器（計量器、分包機等動作不良）	人手によって当該サービスを代替提供できる
関連装置	間接	保温・保冷関連装置の動作不良	装置の保管能力に余裕がある
関連装置	間接	保温・保冷関連装置の動作不良	別手段で冷温調節が持続できる
情報機器	間接	病室モニタ（カメラ）動作不良	別手段/複数台設置等により病室状態の把握が継続できる
情報機器	間接	ナースコール動作不良	故障時病棟運用体制・方法が組織内で合意・整備されている
情報機器	間接	スマートフォン動作不良	固定電話または個人携帯電話にて院内通話を継続できる
情報機器	間接	無線ネットワーク動作体温計の動作不良	非IoT測定機器を備えている

カテゴリ4: 物理インフラ・間接

分野	患者危害リスク	内容	対策項目
物理インフラ	間接	水道ポンプの動作不良	別手段によりサービスを持続できる
物理インフラ	間接	空調制御装置の動作不良	別手段によりサービスを持続できる
物理インフラ	間接	電源供給の不良	別手段によりサービスを持続できる

カテゴリ5: 基幹情報サーバ・間接

分野	患者危害リスク	内容	対策項目
基幹情報サーバ	間接	給食管理システムの動作不良	バックアップ参照システム等を運用して業務が提供できる
基幹情報サーバ	間接	PACSシステムの動作不良	バックアップ参照システム等を運用して業務が提供できる
基幹情報サーバ	間接	医事会計システムの動作不良	バックアップ参照システム等を運用して業務が提供できる
基幹情報サーバ	間接	オーダリングシステムの動作不良	メインサーバと別にオーダ参照システムを有する
基幹情報サーバ	間接	オーダリングシステムの動作不良	紙伝票運用（処方、検査、注射）フォーマットを有する
基幹情報サーバ	間接	電子カルテシステムの動作不良	メインサーバと別にカルテ参照システムを有している
基幹情報サーバ	間接	電子カルテシステムの動作不良	紙診療録運用フォーマットを有する

カテゴリ6: 情報サービス・間接

分野	患者危害リスク	内容	対策項目
情報サービス	間接	患者受付システム動作不良	バックアップシステムでサービスを継続できる
情報サービス	間接	患者認証システム（顔認証等）動作不良	代替手段により診療ワークフローを継続できる
情報サービス	間接	患者受付端末動作不良	代替端末を有しサービスを継続できる
情報サービス	間接	待合呼び出しシステム動作不良	代替手段により診療ワークフローを継続できる
情報サービス	間接	自動会計機動作不良	代替手段により診療ワークフローを継続できる
情報サービス	間接	クレジット支払いシステム動作不良	代替手段により診療ワークフローを継続できる

カテゴリ7: 診療データ運用・間接

分野	患者危害リスク	内容	対策項目
診療データ運用	間接	診療データ自身への真正性の毀損	書き戻し可能なバックアップデータを保存している
診療データ運用	間接	診療データ自身への見読性の毀損	参照可能なバックアップデータを保存している
診療データ運用	間接	診療データ自身への保存性の毀損	バックアップ運用可能な保存機能を有する
診療データ運用	間接	2次的な診療データの誤ったデータ登録	誤ったデータのみを適切に削除可能な手順を整備している

カテゴリ8:不法対策・間接

分野	患者危害リスク	内容	対策項目
不法対策	間接	データ漏洩状況の覚知	組織内連絡先、厚労省等要届出機関一覧が作成されている
不法対策	間接	データ漏洩に関する脅迫行為	組織内連絡先、厚労省等要届出機関一覧が作成されている

End of Document

Seq.No.	編	セクション	表題	項番	内容	CFS	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	管理編	1.1	なし	①	医療情報の安全管理に関する法令等を遵守すること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	管理編	1.1	なし	②	医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。	C.H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	管理編	1.2.1	説明責任	①	医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	管理編	1.2.1	説明責任	②	患者等への説明を適切に行うための窓口の設置等の対策を行うこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	管理編	1.2.1	管理責任	①	医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	管理編	1.2.1	管理責任	②	定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。	C,G	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	管理編	1.2.1	定期的な	①	医療情報システムに関する安全管理を適切に維持するための計画を策定すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	管理編	1.2.1	定期的な	②	医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。	H,J,T,V	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
9	管理編	1.2.2	管理責任	①	情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。	B,O,P,Q,R,S,W	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	0	0
10	管理編	1.2.2	善後策を	①	情報セキュリティインシデントが生じた場合、医療機関内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。	P,R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
11	管理編	1.2.2	善後策を	②	情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。	T,V	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
12	管理編	1.2.2	善後策を	③	①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。	B,F,J	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	管理編	1.3.1	なし	①	医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	管理編	1.3.2	なし	①	業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに役割分担等の責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	管理編	1.4	なし	①	医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	管理編	1.4	なし	②	医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	管理編	2.1	なし	①	取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	管理編	2.1	なし	②	リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	管理編	2.1	なし	③	経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	管理編	2.2.1	なし	①	リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	管理編	2.2.1	なし	②	リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。	D,E,F?	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	管理編	2.2.2	なし	①	リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMSを策定し、実施すること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	管理編	2.2.3	なし	①	医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。	C?	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	管理編	3.1	なし	①	統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を担保するために必要な規程類、管理体制等を整備するとともに、適切に統制が機能しているかを確認すること。	A,C	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	管理編	3.1.2	なし	①	医療機関の規模や組織構成、特性等を踏まえた統制の内容を検討すること。	B,C	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	管理編	3.1.2	なし	②	医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	管理編	3.1.2	なし	③	情報セキュリティに関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。	C,H?	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	管理編	3.1.2	なし	④	情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。	G,H	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	管理編	3.2	なし	①	リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	管理編	3.2	なし	②	情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な範囲で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	管理編	3.2.2	なし	①	整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	管理編	3.3.1	なし	①	医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。	J?	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	管理編	3.3.2	なし	①	医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	管理編	3.3.2	なし	②	内部監査または外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。	T,V ?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
35	管理編	3.4.1	なし	①	情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP等を整備すること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	管理編	3.4.1	なし	②	情報セキュリティインシデントにより、医療機関内の医療情報システムの全部または一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。	B,J,U,V	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
37	管理編	3.4.2	なし	①	情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。	A,C,F,H,Q	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
38	管理編	3.4.3	なし	①	情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。	O,Q?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
39	管理編	3.4.3	なし	②	情報セキュリティインシデントが発生した場合に、厚生労働省等への報告の他に、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	管理編	4.1	なし	①	医療情報システムの安全管理に必要な対策項目（下記参照）の概要を認識した上で、企画管理者やシステム運用者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	管理編	4.1	なし	②	対応ができていない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	管理編	4.2	なし	①	医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	管理編	5.1	なし	①	委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。	A,F,H	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	管理編	5.1	なし	②	委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001またはこれと同様の規格の認証を受けているシステム関連事業者を選定するよう指示すること。	A,F,H	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	管理編	5.2.1	なし	①	委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取り扱い等、医療機関が負う医療情報システムの管理に関して、協働する上で認識の祖語が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	管理編	5.2.2	なし	①	委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	管理編	5.3	なし	①	システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に支持すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	企画管理編	1	なし	①	医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
49	企画管理編	1	なし	②	委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合にも同様の対応をすること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
50	企画管理編	1	なし	③	医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認をとること。また、順守状況に応じて必要な改善措置を講じること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	企画管理編	1	なし	④	医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。	A,B,C,D,E,F?	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	企画管理編	1	なし	⑤	組織における情報セキュリティ方針。医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し。経営層の承認を得ること。	A,B,C,D,E,F?	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
53	企画管理編	1	なし	⑥	⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。	G,H,I,J,K,L?	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	企画管理編	1	なし	⑦	患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
55	企画管理編	2	なし	①	医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
56	企画管理編	2	なし	②	取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
57	企画管理編	2	なし	③	責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。	D,E,F?	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	企画管理編	2	なし	④	委託事業者等と責任分界の取り決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	企画管理編	2	なし	⑤	委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手を特定すること。また、関与する関係者への管理なども責任分界の取り決めに定めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取り決め内容に漏れがないよう留意すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	企画管理編	2	なし	⑥	第三者提供を行う際の責任分界については、技術的な内容と手続き的な部分の役割分担を含めて取り決めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
61	企画管理編	3	なし	①	医療情報システムの安全管理の責任を担う者としての位置づけ、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
62	企画管理編	3	なし	②	情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規定を策定し、経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	企画管理編	3	なし	③	安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	企画管理編	3	なし	④	非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者(CISO)やCSIRTなどの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	B,H,J	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	企画管理編	3	なし	⑤	法律上の対応を含め医療情報の漏洩が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	企画管理編	3	なし	⑥	医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	企画管理編	3	なし	⑦	医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	企画管理編	3	なし	⑧	医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
69	企画管理編	3	なし	⑨	患者等からの相談や苦情への対応を行うための体制を構築すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
70	企画管理編	3	なし	⑩	①～⑨までの対応については、整備した内容を可視化できるようにすること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	企画管理編	4	なし	①	医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	企画管理編	4	なし	②	規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	企画管理編	4	なし	③	医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	企画管理編	4	なし	④	非常時における医療情報の運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	企画管理編	5	なし	①	医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	企画管理編	5	なし	②	証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改竄等を防止する措置を講じること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	企画管理編	5	なし	③	収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	企画管理編	5	なし	④	法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
79	企画管理編	6	なし	①	医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討し、必要な措置を講じること。	C,D,E,F	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	企画管理編	6	なし	②	医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。	A,D,E,F	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81	企画管理編	6	なし	③	医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。	A,D,E,F	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
82	企画管理編	6	なし	④	安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	企画管理編	6	なし	⑤	②～④を踏まえて、リスク分析やリスク評価を担当者と協働して行うこと。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	企画管理編	6	なし	⑥	経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85	企画管理編	6	なし	⑦	リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	企画管理編	6	なし	⑧	リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。	C,D,EF	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	企画管理編	6	なし	⑨	PDCA(Plan-Do-Check-Act)モデルに基づくISMS(Information Security Management System: 情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMSが適切に実施されていることを確認し、経営層にその状況を報告すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	企画管理編	6	なし	⑩	PDCAモデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	企画管理編	7	なし	①	医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	企画管理編	7	なし	②	個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	企画管理編	7	なし	③	医療機関等の事務、運用等を外部の事業者に委託する場合には、委託契約の契約書に守秘・非開示に関する内容を含めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	企画管理編	7	なし	④	③の委託契約の際に、当該委託先事業者の就業規則に①及び②の対応を含めるよう求めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	企画管理編	7	なし	⑤−1	外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94	企画管理編	7	なし	⑤−2	ー保存した医療情報の取扱いについて監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	企画管理編	7	なし	⑤−3	ー医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
96	企画管理編	7	なし	⑤−4	ー総務省・経済産業省の定めた「慰労情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
97	企画管理編	7	なし	⑤−5	ー外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
98	企画管理編	7	なし	⑤−6	ー外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	企画管理編	7	なし	⑤−7	ー保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本稿において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	企画管理編	7	なし	⑤−8	ー保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	企画管理編	7	なし	⑤−9	ー保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	企画管理編	7	なし	⑥	外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	企画管理編	7	なし	⑥−1	a:医療情報等の安全管理に係る基本方針・取扱規程等の整備状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
104	企画管理編	7	なし	⑥−2	b:医療情報等の安全管理に係る実施体制の整備状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	企画管理編	7	なし	⑥−3	c:不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	企画管理編	7	なし	⑥−4	d:実績等に基づく個人データ安全管理に関する信用度		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

107	企画管理編	7	なし	⑥−5	e:財務諸表等に基づく経営の健全性		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
108	企画管理編	7	なし	⑥−6	f:プライバシーマーク認定又はISMS認証の取得	これらは項目に当てはめるのではなく、確認事項として列挙されているので、ひとつずつ対応するものと思われる	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
109	企画管理編	7	なし	⑥−7	g:「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
110	企画管理編	7	なし	⑥−7−1	・政府情報システムのためのセキュリティ評価精度(ISMAP)		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
111	企画管理編	7	なし	⑥−7−2	・JASAクラウドセキュリティ推進協議会CSゴールドマーク		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
112	企画管理編	7	なし	⑥−7−3	・米国FedRAMP		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
113	企画管理編	7	なし	⑥−7−4	・AICPA SOC2（日本公認会計士協会IT7号）		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
114	企画管理編	7	なし	⑥−7−5	・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会IT2号）		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
115	企画管理編	7	なし	⑥−7−6	上記認証が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
116	企画管理編	7	なし	⑥−7−7	・システム監査技術者		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
117	企画管理編	7	なし	⑥−7−8	・Certified Information Systems Auditor ISACA認定		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
118	企画管理編	7	なし	⑥−7−9	h:医療情報を保存する情報機器が設置されている場所（地域、国）		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
119	企画管理編	7	なし	⑥−7−１０	i:委託先事業者に対する国外法の適用可能性		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
120	企画管理編	7	なし	⑦	医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
121	企画管理編	7	なし	⑦−1	ー委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
122	企画管理編	7	なし	⑦−2	ー保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。	委託内容に患者の同意などを含めるもので、項目としては「なし」にあたるかもしれない	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
123	企画管理編	7	なし	⑦−3	ー匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
124	企画管理編	7	なし	⑦−4	ー保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまうまたは患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
125	企画管理編	7	なし	⑦−5	ー情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
126	企画管理編	7	なし	⑧	委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。	F	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
127	企画管理編	7	なし	⑨	委託終了契約に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。	A,C,F,H,J	1	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
128	企画管理編	7	なし	⑩	外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
129	企画管理編	8	なし	①	医療機器等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
130	企画管理編	8	なし	②	医療機関等において保有する医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
131	企画管理編	8	なし	③	医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。	G,I	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
132	企画管理編	8	なし	④	医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。	G,I	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
133	企画管理編	8	なし	⑤	医療機関外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
134	企画管理編	8	なし	⑥	医療機関外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
135	企画管理編	8	なし	⑦	持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
136	企画管理編	8	なし	⑧	医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。	G,I,J,K,L	0	0	0	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
137	企画管理編	8	なし	⑨	患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
138	企画管理編	8	なし	⑩	医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
139	企画管理編	8	なし	⑪	医療情報の破棄に関する手順を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
140	企画管理編	8	なし	⑫	保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業所における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。	J,K,L	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
141	企画管理編	9	なし	①	医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、物理的な資産のほか、医療情報システムが利用するサービス、ライセンスなども含む。）	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
142	企画管理編	9	なし	②	医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
143	企画管理編	9	なし	③	台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
144	企画管理編	9	なし	④	医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。	A,K	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
145	企画管理編	9	なし	⑤	医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。	A,K	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
146	企画管理編	9	なし	⑥	医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えばBYOD(Bring Your Own Device:個人保有の医療機器)の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規定等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
147	企画管理編	9	なし	⑦	医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
148	企画管理編	10	なし	①	医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「5．安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。	J,K	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
149	企画管理編	10	なし	②	医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム・サービスの性格上、報告に基づく確認が難しい場合は、SLAに対する評価等の中で確認すること。	F	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
150	企画管理編	10	なし	③	医療情報システムの取り扱いに関する点検結果を、経営層に報告し、承認を得ること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
151	企画管理編	10	なし	④	医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等の企画管理者や担当者から独立した組織または第三者による監査を実施すること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
152	企画管理編	11	なし	①	医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けて計画を含めること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
153	企画管理編	11	なし	②	医療機関等が定める非常時の定義やBCP(Business Continuity Plan:事業継続計画)との整合性を確認して対応方針を策定すること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
154	企画管理編	11	なし	③	非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
155	企画管理編	11	なし	④	各種規定等に非常時における対応手順・内容も含めること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
156	企画管理編	11	なし	⑤	非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
157	企画管理編	11	なし	⑥	非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。	H,Q,T	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0
158	企画管理編	11	なし	⑦	非常時への対応状況を定期的に確認し、経営層に報告の上、承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
159	企画管理編	11	なし	⑧	非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。	O,P,Q	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0
160	企画管理編	11	なし	⑨	非常時の事象が生じた場合、関係者に対する説明責任を果たすため、報告対応や広報対応を行うこと。	W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
161	企画管理編	11	なし	⑩	非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。	T,V	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
162	企画管理編	12	なし	①	サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
163	企画管理編	12	なし	②	医療機関等において整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
164	企画管理編	12	なし	③	サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
165	企画管理編	12	なし	④	サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認する。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
166	企画管理編	12	なし	⑤	サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。	J,H,Q,T,V	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	0	0	0
167	企画管理編	12	なし	⑥	サイバーセキュリティ事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をあらかじめ整理した上で、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）	P,Q	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
168	企画管理編	12	なし	⑦	サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成30年10月29日付け医政総発1029第1号・医政地発1029第３号・医政研発1029第１号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
169	企画管理編	12	なし	⑧	サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。	P,Q,T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0
170	企画管理編	12	なし	⑨	サイバーセキュリティ事象による非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応とBCP策定」に示す内容を実施すること。	J,P,U	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
171	企画管理編	13	なし	①	リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規定を整備し、管理すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
172	企画管理編	13	なし	②	医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
173	企画管理編	13	なし	③	医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者のID等を付与する等の必要な手順を作成するよう指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
174	企画管理編	13	なし	④	医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規定に応じたものとなっていることが前提となるよう管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
175	企画管理編	13	なし	⑤	医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。医療情報システムの利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じてIDやアクセス権限を付与すること。その具体的な手順については、担当者に作成を指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
176	企画管理編	13	なし	⑥	医療情報システムの管理権限や、医療情報システム、情報機器等で用いるID等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて、利用される管理権限の種類とそのID、利用が認められている者等を管理して一覧化するよう指示すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
177	企画管理編	13	なし	⑦	医療情報システムで利用するID等についての棚卸を定期的に行い、不要なものについては削除すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
178	企画管理編	13	なし	⑧	電子カルテにおける記録の確定に関して、以下の事項を規定等に含めること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
179	企画管理編	13	なし	⑧−1	ー入力者及び確定者の識別・認証	代行入力は医療業界独特の制度と思われる	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
180	企画管理編	13	なし	⑧−2	ー記録の確定手順、識別情報の記録の保存		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
181	企画管理編	13	なし	⑧−3	ー更新履歴の保存		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
182	企画管理編	13	なし	⑧−4	ー代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
183	企画管理編	14	なし	①	法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
184	企画管理編	14	なし	①−1	1．以下の電子証明書を用いて電子署名を施すこと		0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
185	企画管理編	14	なし	①−1−1	（1）「電子署名及び認証業務に関する法律」（平成12年法律第102号）第２条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、。リモート署名、立会人型電子署名の場合も同様である。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
186	企画管理編	14	なし	①−1−2	（2）法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)~(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
187	企画管理編	14	なし	①−1−3	(a)厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす保健医療福祉分野PKI認証局の発行する電子証明書を用いて電子署名を施すこと。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
188	企画管理編	14	なし	①−1−4	ー保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
189	企画管理編	14	なし	①−1−5	ーただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。	電子署名は、アイディ管理とみなしてGと判断	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
190	企画管理編	14	なし	①−1−6	(b)認定認証事業者(電子署名法第２条第３項に定める特定認証業務を行う物として主務大臣の認定を受けた者をいう。以下同じ。）または認定事業者（電子署名法第２条第２項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14.法令で定められた記名・押印のための電子署名」において同じ。）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様。）		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
191	企画管理編	14	なし	①−1−7	(c)「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること。当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証できることが必要である。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192	企画管理編	14	なし	①−2	2．法定保存機関等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること。	G,L	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
193	企画管理編	14	なし	①−2−1	タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認定事業者（タイムビジネスに係る指針等で示されている時刻認定業務の業務に準拠し、一般財団法人日本データ通信協会が認定した時刻認定事業者、以下「認定時刻認証事業者」という。）については、令和4年以降、国による認定制度に順次移行する予定であるから、当面の間、認定時刻認定事業者によるものを使用しても差し支え無い。	タイムスタンプは、ログとみなしてLかなと判断するけれど、趣旨が違うとも感じる。	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
194	企画管理編	14	なし	①−2−2	法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
195	企画管理編	14	なし	①−2−3	タイムスタンプの利用や長期保存に関しては、今後も、関係省庁の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
196	企画管理編	14	なし	①−2−4	タイムスタンプを付与する時点で有効な電子証明書を用いること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
197	企画管理編	14	なし	②	電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」(CP)等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
198	企画管理編	15	なし	①	物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。	A,G,J	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
199	企画管理編	15	なし	②	個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規定等を策定すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
200	企画管理編	15	なし	③	記録媒体及び記録機器の保管及び取扱いについて、運用管理規定を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。	G,H,I	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

201	企画管理編	15	なし	④	医療情報システムが情報を保管する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規定に定め、その運用を関係者全員に周知徹底すること。	G,H,I,J	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
202	企画管理編	15	なし	⑤	記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規定に定めるとともに、関係者に周知徹底すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
203	企画管理編	15	なし	⑥	システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
204	企画管理編	15	なし	⑦	医療機関等において利用するネットワークについて、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を理解の上、経営層に報告し、承認を得ること。	A,L(M,N)	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
205	企画管理編	15	なし	⑧	保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約やSLA等により管理項目について取り決めを行うこと。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
206	企画管理編	15	なし	⑨	医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規定等に含めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。	I,K	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
207	企画管理編	15	なし	⑩	医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
208	企画管理編	15	なし	⑪	情報機器、ソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
209	企画管理編	15	なし	⑫	システム構成やソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
210	企画管理編	15	なし	⑬	医療情報システムが法令等で求められている要件を満たすように適切に管理すること。特に「施行通知」、「外部保存通知」などで定める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容については、担当者に確認の上、必要な検討を行うよう指示すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
211	企画管理編	15	なし	⑭	①～⑬において、担当者が整備した対策について、関連規定等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を反映の上、経営層に報告し承認を得ること。	A,C	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
212	企画管理編	16	なし	①	紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規定等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
213	企画管理編	16	なし	②	スキャナにより読み取った電子情報と元の文書等から得られる情報と同党であることを担保する情報作成管理者を配置すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
214	企画管理編	16	なし	③	紙媒体で作成した医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りにかかる責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規定等に定めること。なお、電子署名については「14.法令で定められた記名・押印のための電子署名」を参照するこ	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
215	企画管理編	16	なし	④	情報作成管理者に対して、スキャナによる読み取り作業が運用管理規定に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
216	企画管理編	16	なし	⑤	診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてからまたは情報を入手してから一定期間以内にスキャンを行うことを運用管理規定等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
217	企画管理編	16	なし	⑥	過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
218	企画管理編	16	なし	⑥－１	・対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
219	企画管理編	16	なし	⑥－２	・必ず実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
220	企画管理編	16	なし	⑥－２－１	ー運用管理規程の作成と妥当性の検証方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を担保した委員会等で行うこと（倫理委員会を用いることも可））	G?	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
221	企画管理編	16	なし	⑥－２－２	ー作業責任者	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
222	企画管理編	16	なし	⑥－２－３	ー相互監視を含む実施体制	G?　なし？	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
223	企画管理編	16	なし	⑥－２－４	ー実施記録の作成と記録項目（次項の監査に耐えうる記録を作成すること）	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
224	企画管理編	16	なし	⑥－２－５	ー事後の監査人と監査項目	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
225	企画管理編	16	なし	⑥－２－６	ースキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
226	企画管理編	16	なし	⑥－３	・事後の監査は、システム監査技術者やCertified Information Systems Auditor(ISACA認定)等の適切な能力を持つ外部監査人によって実施すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
227	企画管理編	16	なし	⑦	企画管理者は、紙の調剤済み処方箋をスキャナ用で電子化して保存する場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
228	企画管理編	16	なし	⑦－１	・紙の調剤済み処方箋の電子化のタイミングに応じて、⑤または⑥の措置を講じること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
229	企画管理編	16	なし	⑦－２	・「電子化した紙の調剤済み処方箋」を修正する場合、「「元の」電子化した紙の調剤済み処方箋」を電子的に修正し、「「修正後の電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
230	企画管理編	16	なし	⑧	企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
231	企画管理編	16	なし	⑧－１	・情報作成管理者が、スキャナによる読み取り作業が適正な手続きで、確実に実施される措置を講じる旨を運用管理規程等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
232	企画管理編	16	なし	⑧－２	・電子化した後、元の紙媒体やフィルムの安全管理を行うこと。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
233	システム運用	1	なし	①	法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。	C,I,J	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
234	システム運用	2	なし	①	医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
235	システム運用	2	なし	②	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者）を作成し、常に最新の状態を維持すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
236	システム運用	2	なし	③	医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
237	システム運用	2	なし	④	医療情報システムの利用者が常に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。	H?	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
238	システム運用	2	なし	⑤	非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
239	システム運用	3	なし	①	医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
240	システム運用	3	なし	②	事業者と技術的な対応に関する責任分界を調整する際に、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
241	システム運用	3	なし	③	通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、その結果を企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
242	システム運用	3	なし	④	サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
243	システム運用	3	なし	⑤	第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
244	システム運用	4	なし	①	企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。	A,G,I	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
245	システム運用	4	なし	②	事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合会辞書」を利用することが考えられる。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
246	システム運用	5	なし	①	システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
247	システム運用	5	なし	②	マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
248	システム運用	5	なし	③	データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。	G,I,J	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
249	システム運用	5	なし	④	電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態にすること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
250	システム運用	6	なし	①	システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
251	システム運用	6	なし	①－１	ークライアント層		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
252	システム運用	6	なし	①－１－１	・情報の持ち出し・管理・破棄等に関する安全管理措置	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
253	システム運用	6	なし	①－１－２	・利用機器・サービスに関する安全管理措置	A,I,J,L	1	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
254	システム運用	6	なし	①－２	ーサーバ側		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255	システム運用	6	なし	①－２－１	・ソフトウェア・サービスに対する要求事項	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
256	システム運用	6	なし	①－２－２	・事業者による保守対応等に対する安全管理措置	A,C,K?	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
257	システム運用	6	なし	①－２－３	・事業者選定と管理	A,C,F	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
258	システム運用	6	なし	①－２－４	・システム運用管理（通常時・非常時等）	A,B?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
259	システム運用	6	なし	①－３	ーインフラ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
260	システム運用	6	なし	①－３－１	・物理的安全管理装置（サーバールーム等、バックアップ）	A,G,H,I,J？	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
261	システム運用	6	なし	①－３－２	・ネットワークに関する安全管理措置	G,I,J,L	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
262	システム運用	6	なし	①－３－３	・インフラ運用管理（通常時・非常時等）	A,B?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
263	システム運用	6	なし	①－４	ーセキュリティ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
264	システム運用	6	なし	①－４－１	・認証・認可に関する安全管理措置	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
265	システム運用	6	なし	①－４－２	・電子署名、タイムスタンプ	G,L?	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
266	システム運用	6	なし	①－４－３	・証跡のレビュー、システム監査	G,L？	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
267	システム運用	6	なし	①－４－４	・外部からの攻撃に対する安全管理措置	J,L？	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
268	システム運用	7	なし	①	医療情報及び情報機器の持ち出しについて、運用管理規定に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
269	システム運用	7	なし	②	保守業務を行う事業者に対して、原則として個人情報を含むデータの持ち出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。	I,K,L	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
270	システム運用	7	なし	③	医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
271	システム運用	7	なし	④	持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
272	システム運用	7	なし	⑤	持ち出した情報機器等について、公衆無線LANの利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
273	システム運用	7	なし	⑥	持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については、削除または停止するか、業務に対して影響がないことを確認すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
274	システム運用	7	なし	⑦	医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。	A,I,L	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
275	システム運用	7	なし	⑧	セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を 患者等に貸し出す際には、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等に説明し、同意を得ること。また、機器に異常や不具合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
276	システム運用	7	なし	⑨	破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
277	システム運用	7	なし	⑩	情報処理機器自体を破棄する場合、必ず専門的な知識を行うものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
278	システム運用	7	なし	⑪	外部保存を受託する事業者に破棄を委託した場合は、確実に医療機器が破棄されたことを、証憑または事業者の説明により確認すること。	I?	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
279	システム運用	7	なし	⑫	保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。	G,K	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
280	システム運用	7	なし	⑬	利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を担保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
281	システム運用	7	なし	⑭	患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI（Public Key Infrastructure:公開鍵暗号基盤）認証等の対策を実施すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
282	システム運用	7	なし	⑮	医療情報を格納する記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。	G,I,J,L	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
283	システム運用	8	なし	①	システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウィルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。	I,J,L,N	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
284	システム運用	8	なし	②	常時不正なソフトウェアの侵入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	L,M,N	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
285	システム運用	8	なし	③	医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用するこ	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
286	システム運用	8	なし	④	メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
287	システム運用	8	なし	⑤	情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
288	システム運用	8	なし	⑥	IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様であ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
289	システム運用	8	なし	⑥－１	IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
290	システム運用	8	なし	⑥－２	IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用するこ	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
291	システム運用	8	なし	⑥－３	使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。	D,E,G	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
292	システム運用	8	なし	⑦	企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
293	システム運用	8	なし	⑧	BYODの実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
294	システム運用	8	なし	⑨	BYODであっても、医療機関等が管理する情報機器等と同様の対策が講じられるよう、手順を作成すること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
295	システム運用	9	なし	①	システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
296	システム運用	9	なし	②	情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
297	システム運用	9	なし	③	医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
298	システム運用	9	なし	④	医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるような措置を講じること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
299	システム運用	10	なし	①	動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。	G,I,K	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
300	システム運用	10	なし	②	診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。	G,I,K	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
301	システム運用	10	なし	③	保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
302	システム運用	10	なし	④	リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。	G,K,L	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
303	システム運用	10	なし	⑤	リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
304	システム運用	10	なし	⑥	診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関に許可を求めなければならない。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
305	システム運用	11	なし	①	非常時の医療情報システムの運用について、次に掲げる対策を実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
306	システム運用	11	なし	①－１	ー「非常時のユーザアカウントや非常時用機能」の手順を整備すること。	J,P,Q	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
307	システム運用	11	なし	①－２	ー非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。	M,N,P,Q	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0
308	システム運用	11	なし	①－３	ー非常時ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。	J,P,U	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0

							A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W			
309	システム運用	11	なし	①－4	一医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。	J,P,Q	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
310	システム運用	11	なし	①－5	ーサイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
311	システム運用	11	なし	①－6	一重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない方法で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。	J,L,P	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
312	システム運用	11	なし	①－7	医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。	M,N	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
313	システム運用	12	なし	①	医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、**災害**（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。	A,D?	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
314	システム運用	12	なし	②	医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。	G,J	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
315	システム運用	12	なし	③	個人情報が保管されている情報機器等の重要な情報機器には盗難措置を講じること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
316	システム運用	12	なし	④	医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。	J,L	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
317	システム運用	12	なし	⑤	記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能または不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。	J,L	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
318	システム運用	12	なし	⑥	利用者が医療情報を入力・参照する端末から長時間離籍する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
319	システム運用	13	なし	①	ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
320	システム運用	13	なし	②	セッション乗っ取り、IPアドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。	G,I,L,M,N	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
321	システム運用	13	なし	③	オープンなネットワークからオープンでないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。	A,G,L.M.N	1	0	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
322	システム運用	13	なし	④	オープンでないネットワークを利用する場合は、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。	A,G,I,J,L	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
323	システム運用	13	なし	⑤	ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特にVPN接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。	A,G,I,J,L	1	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
324	システム運用	13	なし	⑥	オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSのクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNは利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsecまたはTLS1.2以上により接続する場合、セッション間の回り込み（正規のルートでないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。	A,G？	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
325	システム運用	13	なし	⑦	利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
326	システム運用	13	なし	⑧	医療機関で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
327	システム運用	13	なし	⑨	ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
328	システム運用	13	なし	⑩	施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
329	システム運用	13	なし	⑪	医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。	G,I,L,M,N	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
330	システム運用	13	なし	⑫	医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
331	システム運用	13	なし	⑬	医療情報システムにおいて無線LANを利用する場合、次に掲げる対策を実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
332	システム運用	13	なし	⑬－1	一適切な利用者以外に無線LANを利用されないようにすること。例えば、ANY相互拒否等の対策を実施すること。	A,G,L	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
333	システム運用	13	なし	⑬－2	一不正アクセス対策を実施すること。例えばMACアドレスによるアクセス制限を実施すること。ただし、MACアドレスは詐称可能であることや、最近のモバイル端末においてはプライバシー保護の観点からMACアドレスランダム化が標準搭載されていることから、MACアドレスによるアクセス制限の効果が限定的であることに留意する必要がある。	G,I	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
334	システム運用	13	なし	⑬－3	一不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP等により通信を暗号化すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
335	システム運用	13	なし	⑬－4	一利用する無線LANの電波特性を勘案して、通信を阻害しないものを利用すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
336	システム運用	14	なし	①	医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証法に関する手順等に関して、規則、マニュアル等で文書化すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
337	システム運用	14	なし	②	利用者の識別・認証にユーザIDとパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
338	システム運用	14	なし	③	利用者の識別・認証にICカード等のセキュリティ・デバイスを用いる場合、ICカードの破損等、セキュリティ・デバイスが利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
339	システム運用	14	なし	④	アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
340	システム運用	14	なし	⑤	利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定されている医療情報システムを、今後、新規導入または更新するに際しては、二要素認証を採用するシステムの導入、またはこれに相当する対応を行うこと。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
341	システム運用	14	なし	⑥	パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
342	システム運用	14	なし	⑥-1	一類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。		0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
343	システム運用	14	なし	⑥-2	一医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な方法で官・運用すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
344	システム運用	14	なし	⑥-3	一利用者のパスワードの失念や、パスワード漏洩などのおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知りえない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。	ここはアイディ 管理でG	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
345	システム運用	14	なし	⑥-4	一医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
346	システム運用	14	なし	⑦	医療情報システムにおいて用いるIDについて、台帳管理を行うほか、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
347	システム運用	14	なし	⑧	電子カルテシステムにおける記録の**確定手順**の確立と、識別情報の記録について、以下の機能があることを確認すること。	確定手順は医療	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
348	システム運用	14	なし	⑧－1	一電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
349	システム運用	14	なし	⑧－1－1	a:診療情報の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
350	システム運用	14	なし	⑧－1－2	b:「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
351	システム運用	14	なし	⑧－1－3	c:「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
352	システム運用	14	なし	⑧－1－4	d:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。	確定：なし 時刻源：なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
353	システム運用	14	なし	⑧－1－5	e:一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
354	システム運用	14	なし	⑧－1－6	f:確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規定に定めること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
355	システム運用	14	なし	⑧－2	一臨床検査システム、医用画像ファイリングシステム等、所定の装置又はシステムにより記録が作成される場合		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
356	システム運用	14	なし	⑧－2－1	a:運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。	確定：なし 時刻源：なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
357	システム運用	14	なし	⑧－2－2	b:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
358	システム運用	14	なし	⑧－3	一いったん確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。	J,L	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
359	システム運用	15	なし	①	法令で定められた記名・押印のための電子署名について、企画管理編「14.法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
360	システム運用	16	なし	①	医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
361	システム運用	16	なし	②	運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、緊急に閲覧が必要になったときに迅速に閲覧できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
362	システム運用	17	なし	①	利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
363	システム運用	17	なし	②	アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
364	システム運用	17	なし	③	アクセスログの記録に用いる**時刻情報**は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
365	システム運用	17	なし	④	監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡等の整理等を行い、企画管理者に報告すること。	L	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
366	システム運用	18	なし	①	医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
367	システム運用	18	なし	①－1	一攻撃を受けたサーバ等の遮断や他の医療機関への影響の波及の防止のための外部ネットワークの一時切断	P,S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
368	システム運用	18	なし	①－2	一他の医療情報への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離	P,S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
369	システム運用	18	なし	①－3	一他の医療機器への波及の調査等被害の確認のための業務システムの停止	P,S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0
370	システム運用	18	なし	①－4	一バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）	J,P,U	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
							91	21	67	31	29	68	74	58	69	81	51	61	7	8	3	15	11	2	4	7	4	6	2			
							A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W			
							307						394						18			39					12					

Seq.No.	編	セクション	表題	項番	内容		
1	管理編	1.1	なし	①	医療情報の安全管理に関する法令等を遵守すること。	なし	
2	管理編	1.1	なし	②	医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。	22	
3	管理編	1.2.1	説明責任	①	医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。	なし	
4	管理編	1.2.1	説明責任	②	患者等への説明を適切に行うための窓口の設置等の対策を行うこと。	なし	
5	管理編	1.2.1	管理責任	①	医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。	13？34？	
6	管理編	1.2.1	管理責任	②	定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。	32	
7	管理編	1.2.1	定期的な	①	医療情報システムに関する安全管理を適切に維持するための計画を策定すること。	33，34	
8	管理編	1.2.1	定期的な	②	医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。	33，34	
9	管理編	1.2.2	管理責任	①	情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。	32，44	
10	管理編	1.2.2	善後策を	①	情報セキュリティインシデントが生じた場合、医療機関内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。	32，33，44	
11	管理編	1.2.2	善後策を	②	情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。	33	
12	管理編	1.2.2	善後策を	③	①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。	32，33，44	
13	管理編	1.3.1	なし	①	医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。	21	
14	管理編	1.3.2	なし	①	業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに役割分担等の責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。	21	
15	管理編	1.4	なし	①	医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。	43，44	
16	管理編	1.4	なし	②	医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。	43，44	
17	管理編	2.1	なし	①	取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	33，34	
18	管理編	2.1	なし	②	リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。	33，34	
19	管理編	2.1	なし	③	経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。	33，34	
20	管理編	2.2.1	なし	①	リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。	33，34	
21	管理編	2.2.1	なし	②	リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。	32	
22	管理編	2.2.2	なし	①	リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMSを策定し、実施すること。	32，33，34	
23	管理編	2.2.3	なし	①	医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。	33，34	
24	管理編	3.1	なし	①	統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を担保するために必要な規程類、管理体制等を整備するとともに、適切に統制が機能しているかを確認すること。	13，34	
25	管理編	3.1.2	なし	①	医療機関の規模や組織構成、特性等を踏まえた統制の内容を検討すること。	13，34	
26	管理編	3.1.2	なし	②	医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。	なし	特権と考えるなら24
27	管理編	3.1.2	なし	③	情報セキュリティに関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。	なし	特権と考えるなら24
28	管理編	3.1.2	なし	④	情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。	21，22	
29	管理編	3.2	なし	①	リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。	33	
30	管理編	3.2	なし	②	情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な範囲で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。	phase1	
31	管理編	3.2.2	なし	①	整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。	22	
32	管理編	3.3.1	なし	①	医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。	なし？	22？
33	管理編	3.3.2	なし	①	医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。	32	
34	管理編	3.3.2	なし	②	内部監査または外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。	32，33	
35	管理編	3.4.1	なし	①	情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP等を整備すること。	32，44	
36	管理編	3.4.1	なし	②	情報セキュリティインシデントにより、医療機関内の医療情報システムの全部または一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。	32，44	
37	管理編	3.4.2	なし	①	情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。	43，44	
38	管理編	3.4.3	なし	①	情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。	32	
39	管理編	3.4.3	なし	②	情報セキュリティインシデントが発生した場合に、厚生労働省等への報告の他に、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。	32	
40	管理編	4.1	なし	①	医療情報システムの安全管理に必要な対策項目（下記参照）の概要を認識した上で、企画管理者やシステム運用者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。	phase1	
41	管理編	4.1	なし	②	対応ができていない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。	phase1	
42	管理編	4.2	なし	①	医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。	phase1	
43	管理編	5.1	なし	①	委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。	21	
44	管理編	5.1	なし	②	委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001またはこれと同様の規格の認証を受けているシステム関連事業者を選定するよう指示すること。	21	
45	管理編	5.2.1	なし	①	委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取り扱い等、医療機関が負う医療情報システムの管理に関して、協働する上で認識の祖語が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。	21	22も？
46	管理編	5.2.2	なし	①	委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。	なし？	21？

47	管理編	5.3	なし	①	システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に支持すること。	21	
48	企画管理編	1	なし	①	医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。	21，22	
49	企画管理編	1	なし	②	委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合にも同様の対応をすること。	21，22	
50	企画管理編	1	なし	③	医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認をとること。また、順守状況に応じて必要な改善措置を講じること。	なし？	21？
51	企画管理編	1	なし	④	医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。	phase1	34も？
52	企画管理編	1	なし	⑤	組織における情報セキュリティ方針。医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し。経営層の承認を得ること。	phase1	34も？
53	企画管理編	1	なし	⑥	⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。	phase1	34も？
54	企画管理編	1	なし	⑦	患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。	なし	
55	企画管理編	2	なし	①	医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。	21	
56	企画管理編	2	なし	②	取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。	なし？	
57	企画管理編	2	なし	③	責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。	なし？	
58	企画管理編	2	なし	④	委託事業者等と責任分界の取り決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。	なし？	
59	企画管理編	2	なし	⑤	委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手を特定すること。また、関与する関係者への管理なども責任分界の取り決めに定めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取り決め内容に漏れがないよう留意すること。	なし	
60	企画管理編	2	なし	⑥	第三者提供を行う際の責任分界については、技術的な内容と手続き的な部分の役割分担を含めて取り決めること。	43	
61	企画管理編	3	なし	①	医療情報システムの安全管理の責任を担う者としての位置づけ、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。	24	
62	企画管理編	3	なし	②	情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規定を策定し、経営層の承認を得ること。	24	
63	企画管理編	3	なし	③	安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。	24	
64	企画管理編	3	なし	④	非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者(CISO)やCSIRTなどの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	34	
65	企画管理編	3	なし	⑤	法律上の対応を含め医療情報の漏洩が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	32，44	
66	企画管理編	3	なし	⑥	医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。	22	
67	企画管理編	3	なし	⑦	医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。	21，22	
68	企画管理編	3	なし	⑧	医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。	32	
69	企画管理編	3	なし	⑨	患者等からの相談や苦情への対応を行うための体制を構築すること。	なし	
70	企画管理編	3	なし	⑩	①〜⑨までの対応については、整備した内容を可視化できるようにすること。	なし	
71	企画管理編	4	なし	①	医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。	なし？	phase1？
72	企画管理編	4	なし	②	規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。	なし？	phase1？
73	企画管理編	4	なし	③	医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。	なし？	phase1？
74	企画管理編	4	なし	④	非常時における医療情報の運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。	32	
75	企画管理編	5	なし	①	医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。	41	
76	企画管理編	5	なし	②	証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改竄等を防止する措置を講じること。	41	
77	企画管理編	5	なし	③	収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。	33，41	
78	企画管理編	5	なし	④	法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。	32，33，41	
79	企画管理編	6	なし	①	医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討し、必要な措置を講じること。	33	
80	企画管理編	6	なし	②	医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。	phase1、34	
81	企画管理編	6	なし	③	医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。	phase1、34	
82	企画管理編	6	なし	④	安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。	41	
83	企画管理編	6	なし	⑤	②〜④を踏まえて、リスク分析やリスク評価を担当者と協働して行うこと。	33	
84	企画管理編	6	なし	⑥	経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。	なし？	14？
85	企画管理編	6	なし	⑦	リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。	32	
86	企画管理編	6	なし	⑧	リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。	33，34	
87	企画管理編	6	なし	⑨	PDCA(Plan-Do-Check-Act)モデルに基づくISMS(Information Security Management System: 情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMSが適切に実施されていることを確認し、経営層にその状況を報告すること。	33，34	
88	企画管理編	6	なし	⑩	PDCAモデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。	33，34	
89	企画管理編	7	なし	①	医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。	21	
90	企画管理編	7	なし	②	個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。	22	
91	企画管理編	7	なし	③	医療機関等の事務、運用等を外部の事業者に委託する場合には、委託契約の契約書に守秘・非開示に関する内容を含めること。	21	
92	企画管理編	7	なし	④	③の委託契約の際に、当該委託先事業者の就業規則に①及び②の対応を含めるよう求めること。	21，22	
93	企画管理編	7	なし	⑤−1	外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。	N/A	

94	企画管理編	7	なし	⑤－2	ー保存した医療情報の取扱いについて監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。	21
95	企画管理編	7	なし	⑤－3	ー医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。	21，31
96	企画管理編	7	なし	⑤－4	ー総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。	21
97	企画管理編	7	なし	⑤－5	ー外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。	21
98	企画管理編	7	なし	⑤－6	ー外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。	phase4？
99	企画管理編	7	なし	⑤－7	ー保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本稿において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。	phase4？
100	企画管理編	7	なし	⑤－8	ー保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。	phase4？
101	企画管理編	7	なし	⑤－9	ー保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。	phase4？
102	企画管理編	7	なし	⑥	外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。	なし？
103	企画管理編	7	なし	⑥－1	a:医療情報等の安全管理に係る基本方針・取扱規程等の整備状況	N/A
104	企画管理編	7	なし	⑥－2	b:医療情報等の安全管理に係る実施体制の整備状況	N/A
105	企画管理編	7	なし	⑥－3	c:不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況	N/A
106	企画管理編	7	なし	⑥－4	d:実績等に基づく個人データ安全管理に関する信用度	N/A
107	企画管理編	7	なし	⑥－5	e:財務諸表等に基づく経営の健全性	N/A
108	企画管理編	7	なし	⑥－6	f:プライバシーマーク認定又はISMS認証の取得	N/A
109	企画管理編	7	なし	⑥－7	g:「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無	N/A
110	企画管理編	7	なし	⑥－7ー1	・政府情報システムのためのセキュリティ評価精度(ISMAP)	N/A
111	企画管理編	7	なし	⑥－7ー2	・JASAクラウドセキュリティ推進協議会CSゴールドマーク	N/A
112	企画管理編	7	なし	⑥－7ー3	・米国FedRAMP	N/A
113	企画管理編	7	なし	⑥－7ー4	・AICPA SOC2（日本公認会計士協会IT7号）	N/A
114	企画管理編	7	なし	⑥－7ー5	・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会IT2号）	N/A
115	企画管理編	7	なし	⑥－7ー6	上記認証が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること	N/A
116	企画管理編	7	なし	⑥－7ー7	・システム監査技術者	N/A
117	企画管理編	7	なし	⑥－7ー8	・Certified Information Systems Auditor ISACA認定	N/A
118	企画管理編	7	なし	⑥－7ー9	h:医療情報を保存する情報機器が設置されている場所（地域、国）	N/A
119	企画管理編	7	なし	⑥－7ー10	i:委託先事業者に対する国外法の適用可能性	N/A
120	企画管理編	7	なし	⑦	医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。	N/A
121	企画管理編	7	なし	⑦－1	ー委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。	phase4？
122	企画管理編	7	なし	⑦－2	ー保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。	phase4？
123	企画管理編	7	なし	⑦－3	ー匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。	なし
124	企画管理編	7	なし	⑦－4	ー保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまうまたは患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。	21
125	企画管理編	7	なし	⑦－5	ー情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。	なし
126	企画管理編	7	なし	⑧	委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。	なし？
127	企画管理編	7	なし	⑨	委託終了契約に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。	なし
128	企画管理編	7	なし	⑩	外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。	なし
129	企画管理編	8	なし	①	医療機器等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。	なし
130	企画管理編	8	なし	②	医療機関等において保有する医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。	なし
131	企画管理編	8	なし	③	医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。	13
132	企画管理編	8	なし	④	医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。	43
133	企画管理編	8	なし	⑤	医療機関外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。	31，43，45
134	企画管理編	8	なし	⑥	医療機関外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。	43，44，45
135	企画管理編	8	なし	⑦	持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。	21，23
136	企画管理編	8	なし	⑧	医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。	なし
137	企画管理編	8	なし	⑨	患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。	なし
138	企画管理編	8	なし	⑩	医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。	なし
139	企画管理編	8	なし	⑪	医療情報の破棄に関する手順を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。	なし
140	企画管理編	8	なし	⑫	保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業所における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。	なし
141	企画管理編	9	なし	①	医療情報システムにおいて用いる情報機器等の資産管理を行うために必要な属性その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、物理的な資産のほか。医療情報システムが利用するサービス、ライセンスなども含む。）	phase1
142	企画管理編	9	なし	②	医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。	11
143	企画管理編	9	なし	③	台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。	11

144	企画管理編	9	なし	④	医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。	11，12，14		
145	企画管理編	9	なし	⑤	医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。	なし？		14？
146	企画管理編	9	なし	⑥	医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えばBYOD(Bring Your Own Device:個人保有の医療機器)の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規定等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。	11，15		
147	企画管理編	9	なし	⑦	医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。	11		
148	企画管理編	10	なし	①	医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「５．安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。	33		
149	企画管理編	10	なし	②	医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム・サービスの性格上、報告に基づく確認が難しい場合は、SLAに対する評価等の中で確認すること。	21		
150	企画管理編	10	なし	③	医療情報システムの取り扱いに関する点検結果を、経営層に報告し、承認を得ること。	33		
151	企画管理編	10	なし	④	医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等の企画管理者や担当者から独立した組織または第三者による監査を実施すること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。	32		
152	企画管理編	11	なし	①	医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けて計画を含めること。	32，33		
153	企画管理編	11	なし	②	医療機関等が定める非常時の定義やBCP(Business Continuity Plan:事業継続計画)との整合性を確認して対応方針を策定すること。	32		
154	企画管理編	11	なし	③	非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。	32，44		
155	企画管理編	11	なし	④	各種規定等に非常時における対応手順・内容も含めること。	32，33，44		
156	企画管理編	11	なし	⑤	非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。	32，33，44		
157	企画管理編	11	なし	⑥	非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。	22，32，33		
158	企画管理編	11	なし	⑦	非常時への対応状況を定期的に確認し、経営層に報告の上、承認を得ること。	32，33		
159	企画管理編	11	なし	⑧	非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。	44		
160	企画管理編	11	なし	⑨	非常時の事象が生じた場合、関係者に対する説明責任を果たすため、報告対応や広報対応を行うこと。	32，44		
161	企画管理編	11	なし	⑩	非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。	33		
162	企画管理編	12	なし	①	サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。	21，22，32		
163	企画管理編	12	なし	②	医療機関等において整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。	32，33		
164	企画管理編	12	なし	③	サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。	34		
165	企画管理編	12	なし	④	サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認する。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。	33，34		
166	企画管理編	12	なし	⑤	サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。	22，33，34		
167	企画管理編	12	なし	⑥	サイバーセキュリティ事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をあらかじめ整理した上で、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）	21		
168	企画管理編	12	なし	⑦	サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成30年10月29日付け医政総発1029号第1号・医政地発1029第３号・医政研発1029第１号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。	32，44		
169	企画管理編	12	なし	⑧	サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。	44		
170	企画管理編	12	なし	⑨	サイバーセキュリティ事象による非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応とBCP策定」に示す内容を実施すること。	44		
171	企画管理編	13	なし	①	リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規定を整備し、管理すること。	21，23，24		
172	企画管理編	13	なし	②	医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。	21，23，24		
173	企画管理編	13	なし	③	医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者のID等を付与する等の必要な手順を作成するよう指示すること。	21，23，24		
174	企画管理編	13	なし	④	医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規定に応じたものとなっていることが前提となるよう管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。	21，23，24		
175	企画管理編	13	なし	⑤	医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。医療情報システムの利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じてIDやアクセス権限を付与すること。その具体的な手順については、担当者に作成を指示すること。	21，23，24		
176	企画管理編	13	なし	⑥	医療情報システムの管理権限や、医療情報システム、情報機器等で用いるID等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて、利用される管理権限の種類とそのID、利用が認められている者等を管理して一覧化するよう指示すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。	21，23，24		
177	企画管理編	13	なし	⑦	医療情報システムで利用するID等についての棚卸を定期的に行い、不要なものについては削除すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。	21，23，24		
178	企画管理編	13	なし	⑧	電子カルテにおける記録の確定に関して、以下の事項を規定等に含めること。	N/A		
179	企画管理編	13	なし	⑧－１	－入力者及び確定者の識別・認証	21，23，24		
180	企画管理編	13	なし	⑧－２	－記録の確定手順、識別情報の記録の保存	なし？		41？
181	企画管理編	13	なし	⑧－３	－更新履歴の保存	41		
182	企画管理編	13	なし	⑧－４	－代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者	なし？		
183	企画管理編	14	なし	①	法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。	23		

184	企画管理編	14	なし	①－１	１．以下の電子証明書を用いて電子署名を施すこと	N/A	
185	企画管理編	14	なし	①－１－１	（１）「電子署名及び認証業務に関する法律」（平成12年法律第102号）第２条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、。リモート署名、立会人型電子署名の場合も同様である。	N/A	
186	企画管理編	14	なし	①－１－２	（２）法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)~(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いること。	N/A	
187	企画管理編	14	なし	①－１－３	(a)厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす保健医療福祉分野PKI認証局の発行する電子証明書を用いて電子署名を施すこと。	N/A	
188	企画管理編	14	なし	①－１－４	ー保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。	N/A	
189	企画管理編	14	なし	①－１－５	ーただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。	N/A	
190	企画管理編	14	なし	①－１－６	(b)認定認証事業者(電子署名法第２条第３項に定める特定認証業務を行う物として主務大臣の認定を受けた者をいう。以下同じ。）または認定事業者（電子署名法第２条第２項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14.法令で定められた記名・押印のための電子署名」において同じ。）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様。）	N/A	
191	企画管理編	14	なし	①－１－７	(c)「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること。当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証できることが必要である。	N/A	
192	企画管理編	14	なし	①－２	２．法定保存機関等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること。	23，41	
193	企画管理編	14	なし	①－２－１	タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認定事業者（タイムビジネスに係る指針等で示されている時刻認定業務の業務に準拠し、一般財団法人日本データ通信協会が認定した時刻認定事業者、以下「認定時刻認証事業者」という。）については、令和4年以降、国による認定制度に順次移行する予定であるから、当面の間、認定時刻認定事業者によるものを使用しても差し支え無い。	41	
194	企画管理編	14	なし	①－２－２	法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。	41	
195	企画管理編	14	なし	①－２－３	タイムスタンプの利用や長期保存に関しては、今後も、関係省庁の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。	41	
196	企画管理編	14	なし	①－２－４	タイムスタンプを付与する時点で有効な電子証明書を用いること。	23，41	
197	企画管理編	14	なし	②	電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」(CP)等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。	21，23	
198	企画管理編	15	なし	①	物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。	なし？	phase1？
199	企画管理編	15	なし	②	個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規定等を策定すること。	なし	
200	企画管理編	15	なし	③	記録媒体及び記録機器の保管及び取扱いについて、運用管理規定を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。	22，33	
201	企画管理編	15	なし	④	医療情報システムが情報を保管する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規定に定め、その運用を関係者全員に周知徹底すること。	33	
202	企画管理編	15	なし	⑤	記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規定に定めるとともに、関係者に周知徹底すること	なし？	33？
203	企画管理編	15	なし	⑥	システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。	14，33	
204	企画管理編	15	なし	⑦	医療機関等において利用するネットワークについて、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を理解の上、経営層に報告し、承認を得ること。	13，31，33	
205	企画管理編	15	なし	⑧	保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約やSLA等により管理項目について取り決めを行うこと。	なし？	33，34？
206	企画管理編	15	なし	⑨	医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規定等に含めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。	42，43	
207	企画管理編	15	なし	⑩	医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。	33，34	
208	企画管理編	15	なし	⑪	情報機器、ソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	なし？	33，34？
209	企画管理編	15	なし	⑫	システム構成やソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	なし？	33，34？
210	企画管理編	15	なし	⑬	医療情報システムが法令等で求められている要件を満たすように適切に管理すること。特に「施行通知」、「外部保存通知」などで定める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容については、担当者に確認の上、必要な検討を行うよう指示すること。	なし？	
211	企画管理編	15	なし	⑭	①～⑬において、担当者が整備した対策について、関連規定等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を反映の上、経営層に報告し承認を得ること。	33，34	
212	企画管理編	16	なし	①	紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規定等に定めること。	なし	
213	企画管理編	16	なし	②	スキャナにより読み取った電子情報と元の文書等から得られる情報と同究であることを担保する情報作成管理者を配置すること。	なし	
214	企画管理編	16	なし	③	紙媒体で作成した診療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りにかかる責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規定等に定めること。なお、電子署名については「14.法令で定められた記名・押印のための電子署名」を参照すること	なし	23？
215	企画管理編	16	なし	④	情報作成管理者に対して、スキャナによる読み取り作業が運用管理規定に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。	なし	
216	企画管理編	16	なし	⑤	診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてからまたは情報を入手してから一定期間以内にスキャンを行うことを運用管理規定等に定めること。	なし	
217	企画管理編	16	なし	⑥	過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。	N/A	
218	企画管理編	16	なし	⑥－１	・対象となる患者等に、スキャナ等で電子化して保存することを事前に 院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。	なし	
219	企画管理編	16	なし	⑥－２	・必ず実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。	なし	
220	企画管理編	16	なし	⑥－２－１	ー運用管理規程の作成と妥当性の検証方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を担保した委員会等で行うこと（倫理委員会を用いることも可））	なし	
221	企画管理編	16	なし	⑥－２－２	ー作業責任者	なし	

222	企画管理編	16	なし	⑥－２－３	－相互監視を含む実施体制	なし	
223	企画管理編	16	なし	⑥－２－４	－実施記録の作成と記録項目（次項の監査に耐えうる記録を作成すること）	なし	
224	企画管理編	16	なし	⑥－２－５	－事後の監査人と監査項目	なし	32？
225	企画管理編	16	なし	⑥－２－６	－スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法	なし	
226	企画管理編	16	なし	⑥－3	・事後の監査は、システム監査技術者やCertified Information Systems Auditor(ISACA認定)等の適切な能力を持つ外部監査人によって実施すること。	なし	
227	企画管理編	16	なし	⑦	企画管理者は、紙の調剤済み処方箋をスキャナ用で電子化して保存する場合、以下の措置を講じること。	N/A	
228	企画管理編	16	なし	⑦－１	・紙の調剤済み処方箋の電子化のタイミングに応じて、⑤または⑥の措置を講じること。	なし	
229	企画管理編	16	なし	⑦－２	・「電子化した紙の調剤済み処方箋」を修正する場合、「「元の」電子化した紙の調剤済み処方箋」を電子的に修正し、「「修正後の電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。	なし	
230	企画管理編	16	なし	⑧	企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。	なし	
231	企画管理編	16	なし	⑧－１	・情報作成管理者が、スキャナによる読み取り作業が適正な手続きで、確実に実施される措置を講じる旨を運用管理規程等に定めること。	なし	
232	企画管理編	16	なし	⑧－２	・電子化した後、元の紙媒体やフィルムの安全管理を行うこと。	33，34	
233	システム運用編	1	なし	①	法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。	なし	
234	システム運用編	2	なし	①	医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。	なし	
235	システム運用編	2	なし	②	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者）を作成し、常に最新の状態を維持すること。	なし	
236	システム運用編	2	なし	③	医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。	なし	
237	システム運用編	2	なし	④	医療情報システムの利用者が常に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。	なし	
238	システム運用編	2	なし	⑤	非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。	32	
239	システム運用編	3	なし	①	医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。	21	
240	システム運用編	3	なし	②	事業者と技術的な対応に関する責任分界を調整する際に、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。	21	
241	システム運用編	3	なし	③	通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、その結果を企画管理者に報告すること。	21，32	
242	システム運用編	3	なし	④	サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。	21，32	
243	システム運用編	3	なし	⑤	第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。	43？	
244	システム運用編	4	なし	①	企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。	なし	
245	システム運用編	4	なし	②	事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合会辞書」を利用することが考えられる。	なし？	21？
246	システム運用編	5	なし	①	システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。	34	
247	システム運用編	5	なし	②	マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。	34	
248	システム運用編	5	なし	③	データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。	34	
249	システム運用編	5	なし	④	電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態にすること。	42，45	
250	システム運用編	6	なし	①	システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。	N/A	
251	システム運用編	6	なし	①－１	－クライアント層	N/A	
252	システム運用編	6	なし	①－１－１	・情報の持ち出し・管理・破棄等に関する安全管理措置	なし	
253	システム運用編	6	なし	①－１－２	・利用機器・サービスに関する安全管理措置	phase1	
254	システム運用編	6	なし	①－２	－サーバ側	N/A	
255	システム運用編	6	なし	①－２－１	・ソフトウェア・サービスに対する要求事項	phase1	
256	システム運用編	6	なし	①－２－２	・事業者による保守対応等に対する安全管理措置	33,34	
257	システム運用編	6	なし	①－２－３	・事業者選定と管理	21?	
258	システム運用編	6	なし	①－２－４	・システム運用管理（通常時・非常時等）	phase3	
259	システム運用編	6	なし	①－３	－インフラ	N/A	
260	システム運用編	6	なし	①－３－１	・物理的安全管理装置（サーバールーム等、バックアップ）	11?	
261	システム運用編	6	なし	①－３－２	・ネットワークに関する安全管理措置	phase1、31	
262	システム運用編	6	なし	①－３－３	・インフラ運用管理（通常時・非常時等）	32，33	
263	システム運用編	6	なし	①－４	－セキュリティ	N/A	
264	システム運用編	6	なし	①－４－１	・認証・認可に関する安全管理措置	21，23，24	
265	システム運用編	6	なし	①－４－２	・電子署名、タイムスタンプ	23	41？
266	システム運用編	6	なし	①－４－３	・証跡のレビュー、システム監査	32	
267	システム運用編	6	なし	①－４－４	・外部からの攻撃に対する安全管理措置	44	
268	システム運用編	7	なし	①	医療情報及び情報機器の持ち出しについて、運用管理規定に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	なし	
269	システム運用編	7	なし	②	保守業務を行う事業者に対して、原則として個人情報を含むデータの持ち出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。	42	
270	システム運用編	7	なし	③	医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。	42，43	
271	システム運用編	7	なし	④	持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。	13，15，31	
272	システム運用編	7	なし	⑤	持ち出した情報機器等について、公衆無線LANの利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。	13，15，31	
273	システム運用編	7	なし	⑥	持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については、削除または停止するか、業務に対して影響がないことを確認すること。	12，15，31	
274	システム運用編	7	なし	⑦	医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。	15	
275	システム運用編	7	なし	⑧	セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を患者等に貸し出す際には、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等に説明し、同意を得ること。また、機器に異常や不具合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。	なし	

276	システム運用§7	なし	⑨	破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。	なし	
277	システム運用§7	なし	⑩	情報処理機器自体を破棄する場合、必ず専門的な知識を行うものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。	なし	
278	システム運用§7	なし	⑪	外部保存を受託する事業者に破棄を委託した場合は、確実に医療機器が破棄されたことを、証憑または事業者の説明により確認すること。	なし	
279	システム運用§7	なし	⑫	保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。	21，31	
280	システム運用§7	なし	⑬	利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を担保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。	31，43，45	
281	システム運用§7	なし	⑭	患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI（Public Key Infrastructure:公開鍵暗号基盤）認証等の対策を実施すること。	31，43，45	
282	システム運用§7	なし	⑮	医療情報を格納する記録媒体や情報機器の盗難や紛失（ネットワークへの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。	42，43，45	
283	システム運用§8	なし	①	システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウィルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。	12，13，14	31も？
284	システム運用§8	なし	②	常時不正なソフトウェアの侵入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	12，13，14	31も？
285	システム運用§8	なし	③	医療情報とシステムに接続する不正ソフトウェアのリスクなどにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。	14，33，34	
286	システム運用§8	なし	④	メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	31，43	
287	システム運用§8	なし	⑤	情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。	23？	
288	システム運用§8	なし	⑥	IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様であ	N/A	
289	システム運用§8	なし	⑥－1	IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。	15，33	
290	システム運用§8	なし	⑥－2	IoT機器には、製品出荷後にアップデート等に関する脆弱性が発見されることがある。このようなサイバーセキュリティの脅威を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。	14，15，33	
291	システム運用§8	なし	⑥－3	使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。	11，12，15	
292	システム運用§8	なし	⑦	企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。	11，12，13	
293	システム運用§8	なし	⑧	BYODの実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。	15	
294	システム運用§8	なし	⑨	BYODであっても、医療機関等が管理する情報機器等と同様の対策が講じられるよう、手順を作成すること。	15	
295	システム運用§9	なし	①	システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。	11，12，13	
296	システム運用§9	なし	②	情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。	33，34	
297	システム運用§9	なし	③	医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。	33，34	
298	システム運用§9	なし	④	医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるような措置を講じること。	41	
299	システム運用§10	なし	①	動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。	42，43	
300	システム運用§10	なし	②	診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。	42，43	
301	システム運用§10	なし	③	保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。	23，24，42，43	
302	システム運用§10	なし	④	システムによるアクセス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。	23？	31？
303	システム運用§10	なし	⑤	リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	31？	43？
304	システム運用§10	なし	⑥	診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関に許可を求めなければならない。	32，42，43	
305	システム運用§11	なし	①	非常時の医療情報システムの運用について、次に掲げる対策を実施すること。	N/A	
306	システム運用§11	なし	①－1	ー「非常時のユーザアカウントや非常時用機能」の手順を整備すること。	23，32，44	
307	システム運用§11	なし	①－2	ー非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。	32	
308	システム運用§11	なし	①－3	ー非常時ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。	なし	
309	システム運用§11	なし	①－4	ー医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。	32，44	
310	システム運用§11	なし	①－5	ーサイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。	13，31，44	
311	システム運用§11	なし	①－6	ー重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない方法で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。	なし	
312	システム運用§11	なし	①－7	医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。	31，32	
313	システム運用§12	なし	①	医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、**災害**（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。	なし	
314	システム運用§12	なし	②	医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。	なし	
315	システム運用§12	なし	③	個人情報が保管されている情報機器等の重要な情報機器には盗難措置を講じること。	なし	
316	システム運用§12	なし	④	医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。	なし	
317	システム運用§12	なし	⑤	記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能または不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。	なし	
318	システム運用§12	なし	⑥	利用者が医療情報を入力・参照する端末から長時間離籍する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。	なし	
319	システム運用§13	なし	①	ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。	13，31	

320	システム運用編	13	なし	②	セッション乗っ取り、IPアドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。	13，31	
321	システム運用編	13	なし	③	オープンなネットワークからオープンでないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。	31	
322	システム運用編	13	なし	④	オープンでないネットワークを利用する場合は、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。	31	
323	システム運用編	13	なし	⑤	ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特にVPN接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。	31	
324	システム運用編	13	なし	⑥	オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSのクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNは利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsecまたはTLS1.2以上により接続する場合、セッション間の回り込み（正規のルートでないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。	31	
325	システム運用編	13	なし	⑦	利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。	31	
326	システム運用編	13	なし	⑧	医療機関で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。	31	
327	システム運用編	13	なし	⑨	ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。	31	
328	システム運用編	13	なし	⑩	施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。	31	
329	システム運用編	13	なし	⑪	医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。	31	
330	システム運用編	13	なし	⑫	医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。	31	
331	システム運用編	13	なし	⑬	医療情報システムにおいて無線LANを利用する場合、次に掲げる対策を実施すること。	N/A	
332	システム運用編	13	なし	⑬－１	－適切な利用者以外に無線LANを利用されないようにすること。例えば、ANY相互拒否等の対策を実施すること。	31	
333	システム運用編	13	なし	⑬－２	－不正アクセス対策を実施すること。例えばMACアドレスによるアクセス制限を実施すること。ただし、MACアドレスは詐称可能であることや、最近のモバイル端末においてはプライバシー保護の観点からMACアドレスランダム化が標準搭載されていることから、MACアドレスによるアクセス制限の効果が限定的であることに留意する必要がある。	31	23も？
334	システム運用編	13	なし	⑬－３	－不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP等により通信を暗号化すること。	31	
335	システム運用編	13	なし	⑬－４	－利用する無線LANの電波特性を勘案して、通信を阻害しないものを利用すること。	31	
336	システム運用編	14	なし	①	医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証法に関する手順等に関して、規則、マニュアル等で文書化すること。	21，23	
337	システム運用編	14	なし	②	利用者の識別・認証にユーザIDとパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。	23	
338	システム運用編	14	なし	③	利用者の識別・認証にICカード等のセキュリティ・デバイスを用いる場合、ICカードの破損等、セキュリティ・デバイスが利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。	なし	
339	システム運用編	14	なし	④	アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。	23，24	
340	システム運用編	14	なし	⑤	利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定されている医療情報システムを、今後、新規導入または更新するに際しては、二要素認証を採用するシステムの導入、またはこれに相当する対応を行うこと。	23？	
341	システム運用編	14	なし	⑥	パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。	N/A	
342	システム運用編	14	なし	⑥-1	－類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。	なし	
343	システム運用編	14	なし	⑥-2	－医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な方法で官・運用すること。	23	
344	システム運用編	14	なし	⑥-3	－利用者のパスワードの失念や、パスワード漏洩などのおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知りえない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。	23？	
345	システム運用編	14	なし	⑥-4	－医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。	なし	
346	システム運用編	14	なし	⑦	医療情報システムにおいて用いるIDについて、台帳管理を行うほか、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。	21	
347	システム運用編	14	なし	⑧	電子カルテシステムにおける記録の**確定手順**の確立と、識別情報の記録について、以下の機能があることを確認すること。	N/A	
348	システム運用編	14	なし	⑧－１	－電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合	N/A	
349	システム運用編	14	なし	⑧－１－１	a:診療情報の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。	23	
350	システム運用編	14	なし	⑧－１－２	b:「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。	なし	
351	システム運用編	14	なし	⑧－１－３	c:「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。	24？	
352	システム運用編	14	なし	⑧－１－４	d:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。	なし	
353	システム運用編	14	なし	⑧－１－５	e:一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。	なし	
354	システム運用編	14	なし	⑧－１－６	f:確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規定に定めること。	なし	
355	システム運用編	14	なし	⑧－２	－臨床検査システム、医用画像ファイリングシステム等、所定の装置又はシステムにより記録が作成される場合	N/A	
356	システム運用編	14	なし	⑧－２－１	a:運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。	なし	
357	システム運用編	14	なし	⑧－２－２	b:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。	なし	
358	システム運用編	14	なし	⑧－３	－いったん確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。	なし	
359	システム運用編	15	なし	①	法令で定められた記名・押印のための電子署名について、企画管理編「14.法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。	23	

360	システム運用	16	なし	①	医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。	なし
361	システム運用	16	なし	②	運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、緊急に閲覧が必要になったときに迅速に閲覧できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。	なし
362	システム運用	17	なし	①	利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。	41
363	システム運用	17	なし	②	アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。	41
364	システム運用	17	なし	③	アクセスログの記録に用いる**時刻情報**は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。	なし
365	システム運用	17	なし	④	監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡等の整理等を行い、企画管理者に報告するこ	32，33
366	システム運用	18	なし	①	医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。	N/A
367	システム運用	18	なし	①－1	－攻撃を受けたサーバ等の遮断や他の医療機関への影響の波及の防止のための外部ネットワークの一時切断	31，32，44
368	システム運用	18	なし	①－2	－他の医療情報への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離	31，32，44
369	システム運用	18	なし	①－3	－他の医療機器への波及の調査等被害の確認のための業務システムの停止	32，44
370	システム運用	18	なし	①－4	－バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）	なし

「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（遵守事項）」に基づくIT-BCPチェックリスト

Seq.No.	編	セクション	表題	項番	内容	該当なし	カテゴリ1 医療装置・直接	カテゴリ2 医療装置・間接	カテゴリ3 関連装置・間接	カテゴリ4 物理インフラ・間接	カテゴリ5 基幹情報サーバ・間接	カテゴリ6 情報サービス・間接	カテゴリ7 診療データ運用・間接	カテゴリ8 不法対策・間接	カテゴリ9 BCP意思決定	BCP必要条件	備考	CFS
1	管理編	1.1	なし	①	医療情報の安全管理に関する法令等を遵守すること。		1	1	1	1	1	1	1	1	1	1		C
2	管理編	1.1	なし	②	医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。		1	1	1	1	1	1	1	1	1	1		C,H
3	管理編	1.2.1	説明責任	①	医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。		1	1	1	1	1	1	1	1	1	1		A,J
4	管理編	1.2.1	説明責任	②	患者等への説明を適切に行うための窓口の設置等の対策を行うこと。							1						なし
5	管理編	1.2.1	管理責任	①	医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。							1	1	1	1	1		A,B,C,D,E,F
6	管理編	1.2.1	管理責任	②	定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。		1	1	1	1	1	1	1	1	1	1		C,G
7	管理編	1.2.1	定期的な	①	医療情報システムに関する安全管理を適切に維持するための計画を策定すること。										1	1		J
8	管理編	1.2.1	定期的な	②	医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。							1	1		1	1		H,J,T,V
9	管理編	1.2.2	管理責任	①	情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。										1			B,O,P,Q,R,S,W
10	管理編	1.2.2	善後策を	①	情報セキュリティインシデントが生じた場合、医療機関内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。		1	1	1	1	1	1	1	1	1	1		P,R
11	管理編	1.2.2	善後策を	②	情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。		1	1	1	1	1	1	1	1	1	1		T,V
12	管理編	1.2.2	善後策を	③	①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。		1	1	1	1	1	1	1	1	1	1		B,F,J
13	管理編	1.3.1	なし	①	医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。		1	1	1	1	1	1	1	1	1	1		A,C,F,H
14	管理編	1.3.2	なし	①	業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに枠組分担等の責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。							1		1	1	1		A,C,F,H
15	管理編	1.4	なし	①	医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。							1	1	1				I
16	管理編	1.4	なし	②	医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。							1	1	1	1			A
17	管理編	2.1	なし	①	取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。							1	1	1				D,E,F
18	管理編	2.1	なし	②	リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。										1			D,E,F
19	管理編	2.1	なし	③	経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。										1			D,E,F
20	管理編	2.2.1	なし	①	リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。										1			D,E,F
21	管理編	2.2.1	なし	②	リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。							1			1	1		D,E,F?
22	管理編	2.2.2	なし	①	リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関刀における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMSを策定し、実施するこ							1			1		要検討	D,E,F,J
23	管理編	2.2.3	なし	①	医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。										1	1		C?
24	管理編	3.1	なし	①	統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を担保するために必要な規程類、管理体制等を整備するとともに、適切に統制が機能しているかを確認すること。										1	1		A,C
25	管理編	3.1.2	なし	①	医療機関の規模や組織構成、特性等を踏まえた統制の内容を検討すること。										1	1		B,C
26	管理編	3.1.2	なし	②	医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。										1	1		C,H
27	管理編	3.1.2	なし	③	情報セキュリティに関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。									1	1	1		C,H?

28	管理編	3.1.2	なし	④	情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。								1	1	1		G,H
29	管理編	3.2	なし	①	リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。								1	1	1		D,E,F,J
30	管理編	3.2	なし	②	情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な範囲で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。									1	1		J
31	管理編	3.2.2	なし	①	整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。							1				1	実施すること、管理者が行うのか？要検討	H
32	管理編	3.3.1	なし	①	医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。									1	1		J?
33	管理編	3.3.2	なし	①	医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。								1	1	1		なし
34	管理編	3.3.2	なし	②	内部監査または外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。								1	1	1		T,V？
35	管理編	3.4.1	なし	①	情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP等を整備すること。									1	1		B,J
36	管理編	3.4.1	なし	②	情報セキュリティインシデントにより、医療機関内の医療情報システムの全部または一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。									1	1		B,J,U,V
37	管理編	3.4.2	なし	①	情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。									1	1		A,C,F,H,Q
38	管理編	3.4.3	なし	①	情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。									1	1		O,Q?
39	管理編	3.4.3	なし	②	情報セキュリティインシデントが発生した場合に、厚生労働省等への報告の他に、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。								1	1	1		なし
40	管理編	4.1	なし	①	医療情報システムの安全管理に必要な対策項目（下記参照）の概要を認識した上で、企画管理者やシステム運用者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。									1	1		I,J,K,L
41	管理編	4.1	なし	②	対応ができていない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。									1	1		I,J,K,L
42	管理編	4.2	なし	①	医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。									1	1		I,J,K,L
43	管理編	5.1	なし	①	委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。									1	1		A,F,H
44	管理編	5.1	なし	②	委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001またはこれと同様の規格の認証を受けているシステム関連事業者を選定するよう指示すること。									1	1	誰に指示するのか？がわからない	A,F,H
45	管理編	5.2.1	なし	①	委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取り扱い等、医療機関が負う医療情報システムの管理に関して、協働する上で認識の祖語が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。									1	1		A,C,F,H,K
46	管理編	5.2.2	なし	①	委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。									1	1		A,C,F,H,K
47	管理編	5.3	なし	①	システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に指示すること。									1	1		A,C,F,H,K

48	企画管理編	1	なし	①	医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。		1	1	1	1	1	1	1	1		1		C
49	企画管理編	1	なし	②	委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合にも同様の対応をすること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
50	企画管理編	1	なし	③	医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認をとること。また、順守状況に応じて必要な改善措置を講じること。		1	1	1	1	1	1	1	1		1		C
51	企画管理編	1	なし	④	医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。		1	1	1	1	1	1	1	1		1		A,B,C,D,E,F?
52	企画管理編	1	なし	⑤	組織における情報セキュリティ方針。医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し。経営層の承認を得ること。											1		A,B,C,D,E,F?
53	企画管理編	1	なし	⑥	⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。		1	1	1	1	1	1	1	1		1		G,H,I,J,K,L?
54	企画管理編	1	なし	⑦	患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。							1						なし
55	企画管理編	2	なし	①	医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
56	企画管理編	2	なし	②	取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。											1		A,C,F,H,K
57	企画管理編	2	なし	③	責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。		1	1	1	1	1	1	1	1		1		D,E,F?
58	企画管理編	2	なし	④	委託事業者等と責任分界の取り決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
59	企画管理編	2	なし	⑤	委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手を特定すること。また、関与する関係者への管理なども責任分界の取り決めに定めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取り決めないように漏れがないよう留意すること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
60	企画管理編	2	なし	⑥	第三者提供を行う際の責任分界については、技術的な内容と手続き的な部分の役割分担を含めて取り決めること。						1	1	1	1				A,C,F,H,K
61	企画管理編	3	なし	①	医療情報システムの安全管理の責任を担う者としての位置づけ、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。									1		1		C,H
62	企画管理編	3	なし	②	情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規定を策定し、経営層の承認を得ること。							1	1	1		1		C,H
63	企画管理編	3	なし	③	安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。											1		C,H
64	企画管理編	3	なし	④	非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者(CISO)やCSIRTなどの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。		1	1	1	1	1	1	1	1		1		B,H,J
65	企画管理編	3	なし	⑤	法律上の対応を含め医療情報の漏洩が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。		1	1	1	1	1	1	1	1		1		B,J
66	企画管理編	3	なし	⑥	医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。							1	1			1		H
67	企画管理編	3	なし	⑦	医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。							1	1			1		A,C,F,H,K
68	企画管理編	3	なし	⑧	医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。		1	1	1	1	1	1	1	1		1		なし
69	企画管理編	3	なし	⑨	患者等からの相談や苦情への対応を行うための体制を構築すること。							1						なし
70	企画管理編	3	なし	⑩	①～⑨までの対応については、整備した内容を可視化できるようにすること。		1	1	1	1	1	1	1	1		1		A,B,C,D,E,F,J
71	企画管理編	4	なし	①	医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。											1		A,B,C,D,E,F,J
72	企画管理編	4	なし	②	規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。											1		A,B,C,D,E,F,J

73	企画管理編	4		なし	③	医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。											1		A,B,C,D,E,F,J
74	企画管理編	4		なし	④	非常時における医療情報の運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。											1		A,B,C,D,E,F,J
75	企画管理編	5		なし	①	医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。		1	1	1	1	1	1	1	1		1		K,L
76	企画管理編	5		なし	②	証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改竄等を防止する措置を講じること。		1	1	1	1	1	1	1	1		1		K,L
77	企画管理編	5		なし	③	収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。		1	1	1	1	1	1	1	1		1		K,L
78	企画管理編	5		なし	④	法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。						1	1	1	1				K,L
79	企画管理編	6		なし	①	医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討し、必要な措置を講じること。		1	1	1	1	1	1	1	1		1		C,D,E,F
80	企画管理編	6		なし	②	医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。		1	1	1	1	1	1	1	1		1		A,D,E,F
81	企画管理編	6		なし	③	医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。		1	1	1	1	1	1	1	1		1		A,D,E,F
82	企画管理編	6		なし	④	安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。						1	1	1	1		1		A,B,C,D,E,F
83	企画管理編	6		なし	⑤	②～④を踏まえて、リスク分析やリスク評価を担当者と協働して行うこと。		1	1	1	1	1	1	1	1		1		D,E,F
84	企画管理編	6		なし	⑥	経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。											1		A,B,C,D,E,F
85	企画管理編	6		なし	⑦	リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。											1		なし
86	企画管理編	6		なし	⑧	リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。		1	1	1	1	1	1	1	1		1		C,D,EF
87	企画管理編	6		なし	⑨	PDCA(Plan-Do-Check-Act)モデルに基づくISMS(Information Security Management System: 情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMSが適切に実施されていることを確認し、経営層にその状況を報告すること。		1	1	1	1	1	1	1	1		1		J
88	企画管理編	6		なし	⑩	PDCAモデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。		1	1	1	1	1	1	1	1		1		J
89	企画管理編	7		なし	①	医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。							1		1		1		C,H
90	企画管理編	7		なし	②	個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。									1		1		C,H
91	企画管理編	7		なし	③	医療機関等の事務、運用等を外部の事業者に委託する場合には、委託契約の契約書に守秘・非開示に関する内容を含めること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
92	企画管理編	7		なし	④	③の委託契約の際に、当該委託先事業者の就業規則に①及び②の対応を含めるよう求めること。		1	1	1	1	1	1	1	1		1		A,C,F,H,K
93	企画管理編	7		なし	⑤－1	外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。											1		A,C,F,H,K
94	企画管理編	7		なし	⑤－2	ー保存した医療情報の取扱いについて監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。									1		1		A,C,F,H,K
95	企画管理編	7		なし	⑤－3	ー医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。						1			1				A,C,F,H,K
96	企画管理編	7		なし	⑤－4	ー総務省・経済産業省の定めた「慰労情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。						1			1				A,C,F,H,K
97	企画管理編	7		なし	⑤－5	ー外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。						1		1		1		1		A,C,F,H,K
98	企画管理編	7		なし	⑤－6	ー外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。						1		1		1		1		A,C,F,H,K

99	企画管理編	7	なし	⑤－7	ー保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本稿において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。							1		1		1		A,C,F,H,K
100	企画管理編	7	なし	⑤－8	ー保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。							1		1		1		A,C,F,H,K
101	企画管理編	7	なし	⑤－9	ー保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。					1	1			1				A,C,F,H,K
102	企画管理編	7	なし	⑥	外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。													A,C,F,H,K
103	企画管理編	7	なし	⑥－1	a:医療情報等の安全管理に係る基本方針・取扱規程等の整備状況							1		1		1		
104	企画管理編	7	なし	⑥－2	b:医療情報等の安全管理に係る実施体制の整備状況					1	1	1	1	1		1		
105	企画管理編	7	なし	⑥－3	c:不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況					1	1	1	1	1		1		
106	企画管理編	7	なし	⑥－4	d:実績等に基づく個人データ安全管理に関する信用度											1		
107	企画管理編	7	なし	⑥－5	e:財務諸表等に基づく経営の健全性											1		
108	企画管理編	7	なし	⑥－6	f:プライバシーマーク認定又はISMS認証の取得									1		1		
109	企画管理編	7	なし	⑥－7	g:「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無					1	1	1		1				これらは項目に当てはめるのではなく、確認事項として列挙されているので、ひとつずつ対応するものと思われる
110	企画管理編	7	なし	⑥－7－1	・政府情報システムのためのセキュリティ評価精度(ISMAP)					1	1	1		1				
111	企画管理編	7	なし	⑥－7－2	・JASAクラウドセキュリティ推進協議会CSゴールドマーク					1	1	1		1				
112	企画管理編	7	なし	⑥－7－3	・米国FedRAMP					1	1	1		1				
113	企画管理編	7	なし	⑥－7－4	・AICPA SOC2（日本公認会計士協会IT7号）					1	1	1		1				
114	企画管理編	7	なし	⑥－7－5	・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会IT2号）					1	1	1		1				
115	企画管理編	7	なし	⑥－7－6	上記認証が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること					1	1	1		1				
116	企画管理編	7	なし	⑥－7－7	・システム監査技術者					1	1	1		1				
117	企画管理編	7	なし	⑥－7－8	・Certified Information Systems Auditor ISACA認定					1	1	1		1				
118	企画管理編	7	なし	⑥－7－9	h:医療情報を保存する情報機器が設置されている場所（地域、国）					1								
119	企画管理編	7	なし	⑥－7－10	i:委託先事業者に対する国外法の適用可能性									1				
120	企画管理編	7	なし	⑦	医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。													A,C,F,H,K
121	企画管理編	7	なし	⑦－1	ー委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。							1		1				
122	企画管理編	7	なし	⑦－2	ー保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。							1		1				
123	企画管理編	7	なし	⑦－3	ー匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。							1		1				委託内容に患者の同意などを含めるもので、項目としては「なし」にあたるかもしれない
124	企画管理編	7	なし	⑦－4	ー保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまうまたは患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。							1	1	1				
125	企画管理編	7	なし	⑦－5	ー情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。							1	1	1				
126	企画管理編	7	なし	⑧	委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。							1	1	1				F
127	企画管理編	7	なし	⑨	委託終了契約に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。							1	1	1				A,C,F,H,J
128	企画管理編	7	なし	⑩	外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。							1	1	1				なし
129	企画管理編	8	なし	①	医療機器等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。					1		1						I,J
130	企画管理編	8	なし	②	医療機関等において保有する医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。									1				C,H

131	企画管理編	8	なし	③	医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。					1			1	1				G,I
132	企画管理編	8	なし	④	医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。					1			1			1		G,I
133	企画管理編	8	なし	⑤	医療機関外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。					1			1					I,J,L
134	企画管理編	8	なし	⑥	医療機関外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。					1			1					I,J,L
135	企画管理編	8	なし	⑦	持ち出した医療情報を格納する（外部からアクセスして格納する場合を含む。）記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。					1			1	1				I,J,L
136	企画管理編	8	なし	⑧	医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。					1	1	1	1	1				G,I,J,K,L
137	企画管理編	8	なし	⑨	患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。						1	1	1					なし
138	企画管理編	8	なし	⑩	医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。					1			1					I,J,L
139	企画管理編	8	なし	⑪	医療情報の破棄に関する手順を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。									1		1		J
140	企画管理編	8	なし	⑫	保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等（格納する記録媒体・情報機器等の破壊含む）を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業所における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。									1		1		J,K,L
141	企画管理編	9	なし	①	医療情報システムにおいて用いる情報機器等の資産管理等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。（なお、情報機器等には、物理的な資産のほか。医療情報システムが利用するサービス、ライセンスなども含む。）					1								A
142	企画管理編	9	なし	②	医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。					1								A
143	企画管理編	9	なし	③	台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。					1								A
144	企画管理編	9	なし	④	医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況（ソフトウェアやファームウェアのアップデートの状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。					1	1	1						A,K
145	企画管理編	9	なし	⑤	医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況（サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等）が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。						1	1		1				A,K
146	企画管理編	9	なし	⑥	医療機関等が管理しない情報機器で、医療情報システムに用いるもの（例えばBYOD(Bring Your Own Device:個人保有の医療機器)の利用による端末）について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規定等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。					1	1		1				信頼度が低いところ（院内関係者でない）に目を向ける	A
147	企画管理編	9	なし	⑦	医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。					1						1		A

148	企画管理編	10	なし	①	医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「5．安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。					1	1	1	1	1				J,K
149	企画管理編	10	なし	②	医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム・サービスの性格上、報告に基づく確認が難しい場合は、SLAに対する評価等の中で確認すること。					1	1	1	1	1				F
150	企画管理編	10	なし	③	医療情報システムの取り扱いに関する点検結果を、経営層に報告し、承認を得ること。											1		C
151	企画管理編	10	なし	④	医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等の企画管理者や担当者から独立した組織または第三者による監査を実施すること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。					1	1	1	1	1				なし
152	企画管理編	11	なし	①	医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けて計画を含めること。											1		B,J
153	企画管理編	11	なし	②	医療機関等が定める非常時の定義やBCP(Business Continuity Plan:事業継続計画)との整合性を確認して対応方針を策定すること。											1		B,J
154	企画管理編	11	なし	③	非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。											1		J
155	企画管理編	11	なし	④	各種規定等に非常時における対応手順・内容も含めること。											1		J
156	企画管理編	11	なし	⑤	非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。											1		J
157	企画管理編	11	なし	⑥	非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。					1	1	1	1			1		H,Q,T
158	企画管理編	11	なし	⑦	非常時への対応状況を定期的に確認し、経営層に報告の上、承認を得ること。					1	1	1	1			1		J
159	企画管理編	11	なし	⑧	非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。		1	1	1	1	1	1	1	1	1	1		O,P,Q
160	企画管理編	11	なし	⑨	非常時の事象が生じた場合、関係者に対する説明責任を果たすため、報告対応や広報対応を行うこと。											1		W
161	企画管理編	11	なし	⑩	非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。		1	1	1	1	1	1	1	1	1	1		T,V
162	企画管理編	12	なし	①	サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。		1	1	1	1	1	1	1	1	1	1		D,E,F,J
163	企画管理編	12	なし	②	医療機関等において整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。		1	1	1	1	1	1	1	1	1	1		J
164	企画管理編	12	なし	③	サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。		1	1	1	1	1	1	1	1	1	1		J
165	企画管理編	12	なし	④	サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認する。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。		1	1	1	1	1	1	1	1	1	1		J
166	企画管理編	12	なし	⑤	サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。		1	1	1	1	1	1	1	1	1	1		J,H,Q,T,V
167	企画管理編	12	なし	⑥	サイバーセキュリティ事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をあらかじめ整理した上で、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）		1	1	1	1	1	1	1	1	1	1		P,Q

168	企画管理編	12	なし	⑦	サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（平成30年10月29日付け医政総発1029号第1号・医政地発1029第３号・医政研発1029第１号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行う		1	1	1	1	1	1	1	1	1	1		なし
169	企画管理編	12	なし	⑧	サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。		1	1	1	1	1	1	1	1	1	1		P,Q,T
170	企画管理編	12	なし	⑨	サイバーセキュリティ事象による非常時としての対応が生じた場合には、「１１．非常時（災害、サイバー攻撃、システム障害）対応とBCP策定」に示す内容を実施すること。		1	1	1	1	1	1	1	1	1	1	要検討、提案必要か？	J,P,U
171	企画管理編	13	なし	①	リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規定を整備し、管理すること。						1	1						G
172	企画管理編	13	なし	②	医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。						1	1						G
173	企画管理編	13	なし	③	医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者のID等を付与する等の必要な手順を作成するよう指示すること。							1				1		G
174	企画管理編	13	なし	④	医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規定に応じたものとなっていることが前提となるよう管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。							1		1				G
175	企画管理編	13	なし	⑤	医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。医療情報システムの利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じてIDやアクセス権限を付与すること。その具体的な手順については、担当者に作成を指示すること。							1					医療者＝利用者、利用のため運用ではない。	G
176	企画管理編	13	なし	⑥	医療情報システムの管理権限や、医療情報システム、情報機器等で用いるID等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて、利用される管理権限の種類とそのID、利用が認められている者等を管理して一覧化するよう指示すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。						1	1	1					G
177	企画管理編	13	なし	⑦	医療情報システムで利用するID等についての棚卸を定期的に行い、不要なものについては削除すること。システム等で用いるID等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。						1	1		1				G
178	企画管理編	13	なし	⑧	電子カルテにおける記録の確定に関して、以下の事項を規定等に含めること。													G
179	企画管理編	13	なし	⑧－１	－入力者及び確定者の識別・認証							1						
180	企画管理編	13	なし	⑧－２	－記録の確定手順、識別情報の記録の保存								1					代行入力は医療業界独特の制度と思われる
181	企画管理編	13	なし	⑧－３	－更新履歴の保存								1					
182	企画管理編	13	なし	⑧－４	－代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者								1					
183	企画管理編	14	なし	①	法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。													G
184	企画管理編	14	なし	①－１	１，以下の電子証明書を用いて電子署名を施すこと													
185	企画管理編	14	なし	①－１－１	（１）「電子署名及び認証業務に関する法律」（平成12年法律第102号）第２条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、。リモート署名、立会人型電子署名の場合も同様である。						1	1	1	1				
186	企画管理編	14	なし	①－１－２	（２）法令で医師等の国家資格を有する者による作成が求められている文書については、以下の(a)~(c)のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いること。							1	1	1				
187	企画管理編	14	なし	①－１－３	(a)厚生労働省「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」において策定された準拠性監査基準を満たす保健医療福祉分野PKI認証局の発行する電子証明書を用いて電子署名を施すこと。							1	1	1				

188	企画管理編	14	なし	①－１－４	ー保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。	1												要検討、提案必要か？	
189	企画管理編	14	なし	①－１－５	ーただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。							1	1	1				電子署名は、ID管理とみなしてGと判断
190	企画管理編	14	なし	①－１－６	(b)認定認証事業者(電子署名法第２条第３項に定める特定認証業務を行う物として主務大臣の認定を受けた者をいう。以下同じ。）または認定事業者（電子署名法第２条第２項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下「14.法令で定められた記名・押印のための電子署名」において同じ。）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様。）							1	1	1					
191	企画管理編	14	なし	①－１－７	(c)「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること。当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証できることが必要である。							1	1	1					
192	企画管理編	14	なし	①－２	２．法定保存機関等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること。							1	1	1				G,L
193	企画管理編	14	なし	①－２－１	タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認定事業者（タイムビジネスに係る指針等で示されている時刻認定業務の業務に準拠し、一般財団法人日本データ通信協会が認定した時刻認定事業者、以下「認定時刻認証事業者」という。）については、令和4年以降、国による認定制度に順次移行する予定であるから、当面の間、認定時刻認定事業者によるものを使用しても差し支え無い。							1	1	1				タイムスタンプは、ログとみなしてLかなと判断するけれど、趣旨が違うとも感じる。
194	企画管理編	14	なし	①－２－２	法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。					1	1	1	1	1				
195	企画管理編	14	なし	①－２－３	タイムスタンプの利用や長期保存に関しては、今後も、関係省庁の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。					1	1	1	1	1				
196	企画管理編	14	なし	①－２－４	タイムスタンプを付与する時点で有効な電子証明書を用いること。							1	1	1				
197	企画管理編	14	なし	②	電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」(CP)等で定める鍵の管理の要件を満たして行われるよう、利用者に指示し、管理すること。							1					1	G
198	企画管理編	15	なし	①	物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。					1	1							A,G,J
199	企画管理編	15	なし	②	個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規定等を策定すること。					1		1		1				G
200	企画管理編	15	なし	③	記録媒体及び記録機器の保管及び取扱いについて、運用管理規定を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。					1	1	1		1				G,H,I
201	企画管理編	15	なし	④	医療情報システムが情報を保管する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規定に定め、その運用を関係者全員に周知徹底すること。					1	1						保管と記録の違いを理解する	G,H,I,J
202	企画管理編	15	なし	⑤	記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規定に定めるとともに、関係者に周知徹底すること。					1	1							I,J,K,L

203	企画管理編	15	なし	⑥	システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。					1	1	1					ITシステム運用	D,E,F,J
204	企画管理編	15	なし	⑦	医療機関等において利用するネットワークについて、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を理解の上、経営層に報告し、承認を得ること。					1	1					1		A,L(M,N)
205	企画管理編	15	なし	⑧	保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約やSLA等により管理項目について取り決めを行うこと。					1	1							A,C,F,H,K
206	企画管理編	15	なし	⑨	医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規定等に含めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。					1	1			1				I,K
207	企画管理編	15	なし	⑩	医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。					1	1	1						A
208	企画管理編	15	なし	⑪	情報機器、ソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。					1	1	1						A
209	企画管理編	15	なし	⑫	システム構成やソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。					1	1	1						A
210	企画管理編	15	なし	⑬	医療情報システムが法令等で求められている要件を満たすように適切に管理すること。特に「施行通知」、「外部保存通知」などで定める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容については、担当者に確認の上、必要な検討を行うよう指示すること。					1	1	1	1					A
211	企画管理編	15	なし	⑭	①～⑬において、担当者が整備した対策について、関連規定等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を反映の上、経営層に報告し承認を得ること。					1	1	1	1					A,C
212	企画管理編	16	なし	①	紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規定等に定めること。					1								I
213	企画管理編	16	なし	②	スキャナにより読み取った電子情報と元の文書等から得られる情報と同等であることを担保する情報作成管理者を配置すること。	1											情報作成管理者を配置する？要検討。5.2にもある	I
214	企画管理編	16	なし	③	紙媒体で作成した医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りにかかる責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規定等に定めること。なお、電子署名については「14.法令で定められた記名・押印のための電子署名」を参照すること。							1	1				情報作成管理者を配置する？要検討。5.2にもある	G
215	企画管理編	16	なし	④	情報作成管理者に対して、スキャナによる読み取り作業が運用管理規定に基づき適正な手続で確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。							1	1					I
216	企画管理編	16	なし	⑤	診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてからまたは情報を入手してから一定期間以内にスキャンを行うことを運用管理規定等に定めること。							1	1					I
217	企画管理編	16	なし	⑥	過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。													
218	企画管理編	16	なし	⑥－１	・対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。	1											表現を検討した方が良いのでは？要検討	なし
219	企画管理編	16	なし	⑥－２	・対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。	1											表現を検討した方が良いのでは？要検討	
220	企画管理編	16	なし	⑥－２－１	ー運用管理規程の作成と妥当性の検証方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を担保した委員会等で行うこと（倫理委員会を用いることも可）））	1												G?
221	企画管理編	16	なし	⑥－２－２	ー作業責任者	1												H
222	企画管理編	16	なし	⑥－２－３	ー相互監視を含む実施体制	1												G? なし？
223	企画管理編	16	なし	⑥－２－４	ー実施記録の作成と記録項目（次項の監査に耐えうる記録を作成すること）	1												なし
224	企画管理編	16	なし	⑥－２－５	ー事後の監査人と監査項目	1												なし

225	企画管理編	16	なし	⑥－２－６	ースキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法	1												I,J
226	企画管理編	16	なし	⑥－２－７	・事後の監査は、システム監査技術者やCertified Information Systems Auditor(ISACA認定)等の適切な能力を持つ外部監査人によって実施すること。	1												なし
227	企画管理編	16	なし	⑦	企画管理者は、紙の調剤済み処方箋をスキャナ用で電子化して保存する場合、以下の措置を講じること。													
228	企画管理編	16	なし	⑦－１	・紙の調剤済み処方箋の電子化のタイミングに応じて、⑤または⑥の措置を講じること。							1		1				I
229	企画管理編	16	なし	⑦－２	・「電子化した紙の調剤済み処方箋」を修正する場合、「「元の」電子化した紙の調剤済み処方箋」を電子的に修正し、「「修正後の電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。							1	1	1				I
230	企画管理編	16	なし	⑧	企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。													
231	企画管理編	16	なし	⑧－１	・情報作成管理者が、スキャナによる読み取り作業が適正な手続きで、確実に実施される措置を講じる旨を運用管理規程等に定めること。							1						I
232	企画管理編	16	なし	⑧－２	・電子化した後、元の紙媒体やフィルムの安全管理を行うこと。					1				1				I
233	システム運用	1	なし	①	法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。					1	1	1						C,I,J
234	システム運用	2	なし	①	医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。					1	1	1						A,J
235	システム運用	2	なし	②	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者）を作成し、常に最新の状態を維持すること。					1	1	1						A
236	システム運用	2	なし	③	医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。					1	1	1						A,J
237	システム運用	2	なし	④	医療情報システムの利用者が常に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。							1						H?
238	システム運用	2	なし	⑤	非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。		1	1	1	1	1	1	1	1				J
239	システム運用	3	なし	①	医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。											1		A,C,F,H
240	システム運用	3	なし	②	事業者と技術的な対応に関する責任分界を調整する際に、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。											1		A,C,F,H
241	システム運用	3	なし	③	通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、その結果を企画管理者に報告すること。											1		A,C,F,H
242	システム運用	3	なし	④	サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。											1	事前	A,C,F,H
243	システム運用	3	なし	⑤	第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。											1		A,C,F,H
244	システム運用	4	なし	①	企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。									1			「要配慮個人情報＝重要度」と位置付けて考える	A,G,I
245	システム運用	4	なし	②	事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」を利用することが考えられる。		1	1	1		1	1					「対策」をBCP対策として考える	A,C,F,H
246	システム運用	5	なし	①	システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。	1												I
247	システム運用	5	なし	②	マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。	1												I
248	システム運用	5	なし	③	データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。	1											過去に向けた対策は該当せず	G,I,J

249	システム運用	5		なし	④	電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態にすること。						1	1						I
250	システム運用	6		なし	①	システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。													
251	システム運用	6		なし	①－１	ークライアント層						1	1						
252	システム運用	6		なし	①－１－１	・情報の持ち出し・管理・破棄等に関する安全管理措置								1	1				I,J,L
253	システム運用	6		なし	①－１－２	・利用機器・サービスに関する安全管理措置						1	1						A,I,J,L
254	システム運用	6		なし	①－２	ーサーバ側						1							
255	システム運用	6		なし	①－２－１	・ソフトウェア・サービスに対する要求事項						1							I,J,L
256	システム運用	6		なし	①－２－２	・事業者による保守対応等に対する安全管理措置						1							A,C,K?
257	システム運用	6		なし	①－２－３	・事業者選定と管理						1							A,C,F
258	システム運用	6		なし	①－２－４	・システム運用管理（通常時・非常時等）						1							A,B?
259	システム運用	6		なし	①－３	ーインフラ					1								
260	システム運用	6		なし	①－３－１	・物理的安全管理装置（サーバールーム等、バックアップ）					1								A,G,H,I,J？
261	システム運用	6		なし	①－３－２	・ネットワークに関する安全管理措置					1								G,I,J,L
262	システム運用	6		なし	①－３－３	・インフラ運用管理（通常時・非常時等）					1								A,B?
263	システム運用	6		なし	①－４	ーセキュリティ													
264	システム運用	6		なし	①－４－１	・認証・認可に関する安全管理措置							1						G
265	システム運用	6		なし	①－４－２	・電子署名、タイムスタンプ							1		1				G,L?
266	システム運用	6		なし	①－４－３	・証跡のレビュー、システム監査							1		1				G,L？
267	システム運用	6		なし	①－４－４	・外部からの攻撃に対する安全管理措置		1	1	1	1	1	1	1	1		1		J,L？
268	システム運用	7		なし	①	医療情報及び情報機器の持ち出しについて、運用管理規定に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。											1		G,I,L
269	システム運用	7		なし	②	保守業務を行う事業者に対して、原則として個人情報を含むデータの持ち出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。							1		1					I,K,L
270	システム運用	7		なし	③	医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。							1		1					I,L
271	システム運用	7		なし	④	持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。							1		1					I,L
272	システム運用	7		なし	⑤	持ち出した情報機器等について、公衆無線LANの利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。							1		1					I,L
273	システム運用	7		なし	⑥	持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については、削除または停止するか、業務に対して影響がないことを確認すること。							1		1					I,L
274	システム運用	7		なし	⑦	医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。						1								A,I,L
275	システム運用	7		なし	⑧	セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を患者等に貸し出す際には、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等に説明し、同意を得ること。また、機器に異常や不具合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。		1	1	1		1								なし
276	システム運用	7		なし	⑨	破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。									1		1			I,J
277	システム運用	7		なし	⑩	情報処理機器自体を破棄する場合、必ず専門的な知識を行うものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。									1		1			I,J
278	システム運用	7		なし	⑪	外部保存を受託する事業者に破棄を委託した場合は、確実に医療機器が破棄されたことを、証憑または事業者の説明により確認すること。									1		1			I?
279	システム運用	7		なし	⑫	保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。		1	1	1	1	1	1						リモートログインできた方が良いケースもあるか？	G,K
280	システム運用	7		なし	⑬	利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を担保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。		1	1	1	1	1	1						リモートログインできた方が良いケースもあるか？	G,I,L

281	システム運用	7		なし	⑭	患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI（Public Key Infrastructure:公開鍵暗号基盤）認証等の対策を実施すること。					1	1	1	1					G,I,L
282	システム運用	7		なし	⑮	医療情報を格納する記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。								1					G,I,J,L
283	システム運用	8		なし	①	システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウィルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。							1	1						I,J,L,N
284	システム運用	8		なし	②	常時不正なソフトウェアの侵入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。					1	1	1						L,M,N
285	システム運用	8		なし	③	医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。					1	1	1						D,E,F
286	システム運用	8		なし	④	メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守党でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。							1	1					医師同士のコンサルをメールで行う等	I,J,K,L
287	システム運用	8		なし	⑤	情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。							1		1					G
288	システム運用	8		なし	⑥	IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。				1								非医療機器をIoTと定義付けた	
289	システム運用	8		なし	⑥－１	IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。				1								非医療機器をIoTと定義付けた	D,E,F
290	システム運用	8		なし	⑥－２	IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。				1								非医療機器をIoTと定義付けた	D,E,F,J
291	システム運用	8		なし	⑥－３	使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。				1								非医療機器をIoTと定義付けた	D,E,G
292	システム運用	8		なし	⑦	企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。											1		A
293	システム運用	8		なし	⑧	BYODの実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。							1						A,G
294	システム運用	8		なし	⑨	BYODであっても、医療機関等が管理する情報機器等と同様の対策が講じられるよう、手順を作成すること。											1		A,G
295	システム運用	9		なし	①	システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。											1		A
296	システム運用	9		なし	②	情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。	1												A,J
297	システム運用	9		なし	③	医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。					1	1	1						A,J
298	システム運用	9		なし	④	医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるような措置を講じること。							1	1					A
299	システム運用	10		なし	①	動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。									1				G,I,K
300	システム運用	10		なし	②	診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。							1	1	1				G,I,K

301	システム運用	10	なし	③	保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。							1		1				保守＝運用と考える	G,I,K,L
302	システム運用	10	なし	④	リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。								1				保守＝運用と考える	G,K,L
303	システム運用	10	なし	⑤	リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。								1					G,I,K,L
304	システム運用	10	なし	⑥	診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関に許可を求めなければならない。								1					G,I,K,L
305	システム運用	11	なし	①	非常時の医療情報システムの運用について、次に掲げる対策を実施すること。													
306	システム運用	11	なし	①－１	ー「非常時のユーザアカウントや非常時用機能」の手順を整備すること。						1	1	1					J,P,Q
307	システム運用	11	なし	①－２	ー非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。						1	1		1				M,N,P,Q
308	システム運用	11	なし	①－３	ー非常時ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。						1	1	1	1				J,P,U
309	システム運用	11	なし	①－４	ー医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。						1	1	1				1	日本語の解釈、次回改版に提案するか？	J,P,Q
310	システム運用	11	なし	①－５	ーサイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。						1							A,J
311	システム運用	11	なし	①－６	ー重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない方法で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。						1	1	1					J,L,P
312	システム運用	11	なし	①－７	医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。						1	1						M,N
313	システム運用	12	なし	①	医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置することなどを考慮すること。						1	1							A,D?
314	システム運用	12	なし	②	医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。						1	1	1	1					G,J
315	システム運用	12	なし	③	個人情報が保管されている情報機器等の重要な情報機器には盗難措置を講じること。						1			1				A,G
316	システム運用	12	なし	④	医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。						1	1						適切に管理する＝機能を意味するためハード側	J,L
317	システム運用	12	なし	⑤	記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能または不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。												1		J,L
318	システム運用	12	なし	⑥	利用者が医療情報を入力・参照する端末から長時間離籍する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。								1	1					G
319	システム運用	13	なし	①	ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。							1	1	1					A
320	システム運用	13	なし	②	セッション乗っ取り、IPアドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。						1								G,I,L,M,N
321	システム運用	13	なし	③	オープンなネットワークからオープンでないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。						1	1							A,G,L.M.N

322	システム運用	13	なし	④	オープンでないネットワークを利用する場合は、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。						1	1							A,G,I,J,L
323	システム運用	13	なし	⑤	ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特にVPN接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。						1								A,G,I,J,L
324	システム運用	13	なし	⑥	オープンなネットワークにおいて、IpsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSのクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNは利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsecまたはTLS1.2以上により接続する場合、セッション間の回り込み（正規のルートでないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。						1	1							A,G？
325	システム運用	13	なし	⑦	利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。						1	1							G,I,L
326	システム運用	13	なし	⑧	医療機関で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。								1		1				G,I,L
327	システム運用	13	なし	⑨	ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。						1	1	1						G,I,L
328	システム運用	13	なし	⑩	施設の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。						1	1			1				G,I,L
329	システム運用	13	なし	⑪	医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。						1	1	1						G,I,L,M,N
330	システム運用	13	なし	⑫	医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。								1	1	1			なりすまし	G
331	システム運用	13	なし	⑬	医療情報システムにおいて無線LANを利用する場合、次に掲げる対策を実施すること。														
332	システム運用	13	なし	⑬－１	－適切な利用者以外に無線LANを利用されないようにすること。例えば、ANY相互拒否等の対策を実施すること。						1								A,G,L
333	システム運用	13	なし	⑬－２	－不正アクセス対策を実施すること。例えばMACアドレスによるアクセス制限を実施すること。ただし、MACアドレスは詐称可能であることや、最近のモバイル端末においてはプライバシー保護の観点からMACアドレスランダム化が標準搭載されていることから、MACアドレスによるアクセス制限の効果が限定的であることに留意する必要がある。						1								G,I
334	システム運用	13	なし	⑬－３	－不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP等により通信を暗号化すること。						1								G,I,L
335	システム運用	13	なし	⑬－４	－利用する無線LANの電波特性を勘案して、通信を阻害しないものを利用すること。						1								G,I,L
336	システム運用	14	なし	①	医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証法に関する手順等に関して、規則、マニュアル等で文書化すること。								1						G
337	システム運用	14	なし	②	利用者の識別・認証にユーザIDとパスワードの組み合わせを用いる場合、それらの譲歩を、本人しか知り得ない状態に保つよう対策を実施すること。								1						G
338	システム運用	14	なし	③	利用者の識別・認証にICカード等のセキュリティ・デバイスを用いる場合、ICカードの破損等、セキュリティ・デバイスが利用できない時を想定し、緊急時の代替手段による一時的なアクセルールを用意すること。						1	1	1						G

339	システム運用	14	なし	④	アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。					1	1	1					医療機器についても物理的なCT装置は医療装置であり、CTのコントローラとしてのPCは物理インフラ・サーバに属すると解釈している。	G
340	システム運用	14	なし	⑤	利用者認証にパスワードを用いる場合には、令和9年度時点で稼働していることが想定されている医療情報システムを、今後、新規導入または更新するに際しては、二要素認証を採用するシステムの導入、またはこれに相当する対応を行うこと。					1	1							G
341	システム運用	14	なし	⑥	パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。							1						G
342	システム運用	14	なし	⑦	ー類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。							1						
343	システム運用	14	なし	⑧	ー医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な方法で管理・運用すること。							1						
344	システム運用	14	なし	⑨	ー利用者のパスワードの失念や、パスワード漏洩などのおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知りえない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。							1						ここはID管理でG
345	システム運用	14	なし	⑩	ー医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。									1				
346	システム運用	14	なし	⑪	医療情報システムにおいて用いるIDについて、台帳管理を行うほか、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。									1		1		G
347	システム運用	14	なし	⑫	電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。													確定手順は医療業界特有かも
348	システム運用	14	なし	⑫－１	ー電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合													
349	システム運用	14	なし	⑫－１－１	a:診療情報の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。						1	1	1					
350	システム運用	14	なし	⑫－１－２	b:「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。							1	1					
351	システム運用	14	なし	⑫－１－３	c:「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。							1		1				
352	システム運用	14	なし	⑫－１－４	d:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、現状回復のための手順を検討しておくこと。					1			1	1				確定：なし 時刻源：なし
353	システム運用	14	なし	⑫－１－５	e:一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。								1	1				
354	システム運用	14	なし	⑫－１－６	f:確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規定に定めること。								1	1				
355	システム運用	14	なし	⑫－２－１	ー臨床検査システム、医用画像ファイリングシステム等、所定の装置又はシステムにより記録が作成される場合													
356	システム運用	14	なし	⑫－２－２	a:運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の指名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。						1	1	1					確定：なし 時刻源：なし
357	システム運用	14	なし	⑫－２－３	b:確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、現状回復のための手順を検討しておくこと。					1			1	1				
358	システム運用	14	なし	⑫－３	ーいったん確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。								1	1				J,L
359	システム運用	15	なし	①	法令で定められた記名・押印のための電子署名について、企画管理編「14.法令で定められた記名・押印のための電子署名」に示す要件を満たすサービスを選択し、医療情報システムにおいて、利用できるように措置を講じること。							1	1	1				G

360	システム運用	16	なし	①	医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。	1													A
361	システム運用	16	なし	②	運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保管を行う場合、緊急に閲覧が必要になったときに迅速に閲覧できるよう、保管している紙媒体等の検索性も必要に応じて維持すること。								1					A
362	システム運用	17	なし	①	利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。						1	1							K,L
363	システム運用	17	なし	②	アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。						1	1							K,L
364	システム運用	17	なし	③	アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。						1	1							なし
365	システム運用	17	なし	④	監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡等の整理等を行い、企画管理者に報告すること。						1	1							L
366	システム運用	18	なし	①	医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。		1	1	1	1	1	1	1	1		1		
367	システム運用	18	なし	①－１	一攻撃を受けたサーバ等の遮断や他の医療機関への影響の波及の防止のための外部ネットワークの一時切断					1								P,S
368	システム運用	18	なし	①－２	一他の医療情報への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離					1	1	1	1	1				P,S
369	システム運用	18	なし	①－３	一他の医療機器への波及の調査等被害の確認のための業務システムの停止		1	1	1			1						P,S
370	システム運用	18	なし	①－４	一バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）					1	1	1	1					J,P,U
						16	52	52	56	141	137	198	121	168	54	135		

サイバー攻撃を想定した事業継続計画（BCP）策定の確認表のための手引き

○ 本手引きは、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」について、サイバー攻撃を想定した BCP 作成の一助となるよう、解説を加えたものです。貴組織において BCP を作成する際の参考として活用してください。

※ サイバー攻撃を想定した BCP 策定時の留意点

- 本手引き及び確認表は最低限必要な事項を記したものです。医療機関の特性に応じて、自機関が主体となり必要な事項を整理し定めてください。
- BCP 策定には先だってリスク分析が重要となります。リスク分析は全過程において自機関だけでなく、事業者、その他の関係者の間で、情報および意見を相互に交換（リスクコミュニケーション）することが必要です。
- BCP は定期的に見直し、必要な項目を更新してください。
- 医療情報システムとは、医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステムを指します。例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定されます。また、患者情報の通信が行われる院内・院外ネットワークも含みます。
- 医療機関の規模により作成する BCP の内容も異なると想定されるため、関係団体等により示されている BCP の手引きについても適宜参照して作成してください。
- 本手引きの各項目の解説の下部には、それぞれの項目に紐づく「医療情報システムの安全管理に関するガイドライン」関連文書の該当箇所を括弧内に示しております。

【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

必要に応じて医療情報システム事業者等の協力を得ながら、自医療機関が保有する情報機器等の全体を網羅する医療情報システムに関する構成図（外部接続点を含むネットワーク構成図等）を作成する。

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。なお、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。また、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。

（企画管理編：9.1、システム運用編：8.4）

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。

（企画管理編：4.4、システム運用編：2、Q&A：概 Q- 6 ）

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。また、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。

（経営管理編：3.4、企画管理編:11）

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、医療機関が管理する機器と、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。

（経営管理編：3.4.2、企画管理編：12）

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。

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。

（経営管理編：3.4.3、企画管理編：2.1、12.3、Q&A：企 Q-16）

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。

（企画管理編：12.2、システム運用編：8.2、17）

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。

（企画管理編：11.⑥）

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。また、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。

（経営管理編：3.4.1、企画管理編：11.2、システム運用編：11）

【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。

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。

（経営管理編：3.4.2）

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。

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、報告様式等を用いて正確に伝達する。

（経営管理編：3.4.3）

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。

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 と経営者に必ず伝達されるように担当者を整備する。また、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。

※CSIRT（Computer Security Incident Response Team）：

コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

【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。

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。また、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

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。

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。

3-1 による原因調査の結果、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。その他、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。

（企画管理編：3.1.5、システム運用編：18.1）

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

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。

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。（サイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性について検討する。）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」も参考にしながら医療機関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。

例）◯紙カルテ運用

・紙伝票の最新化と帳票準備

・運用フローの作成と共有

○ 参照系環境構築

・サーバおよび端末 PC の構築

・プリンタ、印刷用紙、トナー準備

（経営管理編：3.4、企画管理編：11）

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。

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。

＊フォレンジック調査：

サイバー攻撃で消去・改竄されたデータや攻撃活動のログを取得し、攻撃対象、方法、被害範囲などを解明する調査のこと

（企画管理編：11）

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。

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。また、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。

（経営管理編：3.4.3）

【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。

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。特に、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。復旧優先度は、診療継続を意識して定める「重要度」と異なる場合がある。（Q&A：企 Q-42）

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）電子カルテ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。

（企画管理編：11）

４-3) 再設定や再インストール、バックアップデータ復旧等

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。

端末 PC/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。

復旧の際、既知の脆弱性、漏洩した可能性のあるパスワード等に注意する。

（[特集] 医療機関等におけるサイバーセキュリティ:3.3 必要最小限の対策：バックアップ（システム・データ））

４-4) 復旧結果の確認

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。

【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、可能性について、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。

下記を、経営層に報告する（組織内への周知も行う。）。

・異常の内容、原因、被害状況、復旧工数及び費用等について

・復旧結果について

・情報漏えいの有無、範囲について

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。

経営層や対策チームを交え、再発防止策の検討・策定を行う。

（経営管理編：1.2.2、3.4.3、企画管理編：2.1.3、3.1.5）

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。

確定した再発防止策を、関係者等に周知する。

5-4) 再発防止策の実施

再発防止策の実施が行えるか。

定期的なチェック箇所を割り出し、日々の保守業務へのチェック箇所、実施内容、実施者の落とし込みを行う。

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。

策定した再発防止策を事業者へ周知し業務への反映を指示する。指示した再発防止策が実施できているか定期的に確認する。

（企画管理編：2.1.3）

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。

経営層と担当者が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体制を備えておく。関係省庁等外部関係機関への報告とサイバー攻撃の影響・被害状況・影響範囲等を踏まえて、情報公開の必要性および内容について検討し、経営層の意思決定として策定する。

（経営管理編：1.2.2）

医療情報システム部門
事業継続計画（BCP）

〇〇年〇〇月〇〇日　初版

〇〇病院

〇〇部門

目次

第 1 章 総則

1.1　策定目的

本事業継続計画（以下、本 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.　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
III.　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
IV.　平時、非常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.　電子カルテシステム
II.　医事会計システム（レセプト）
III.　医用画像システム
IV.　各種部門システム（検査、処方など）
V.　オーダリングシステム
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. スタッフ間の連絡不能
IV. 情報機器・医療機器の操作不能・誤動作
V. ○○○○○○

また、これらの被害を引き起こすサイバー攻撃の例として以下が挙げられる。

I. 不正アクセス等
II. 標的型メール攻撃
III. マルウェア感染（ランサムウェアを含む）
IV. 分散型サービス妨害（DDoS 攻撃）
V. ○○○○○○
VI. 上記の予兆と思われる現象

1.4 文書の管理および周知

本 BCP は○○部門にて、現状を適切に反映した原本および関連資料の整備ならびに管理を行い、経営層の承認を受けた上で、当院の全職員に開示周知する。

第 2 章 体制整備

2.1 情報機器等の把握と適切な管理

平時において、非常時に備えたサイバーセキュリティの体制整備を以下のとおり行う。

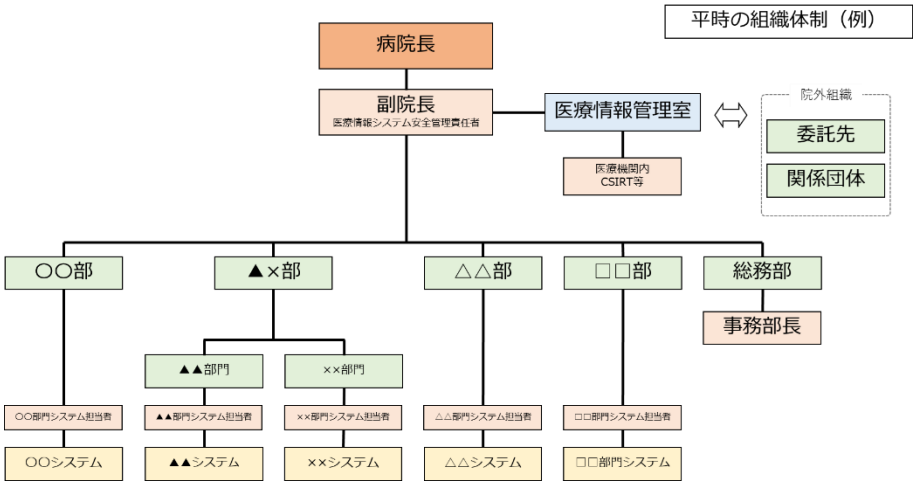
2.1.1 医療情報システム安全管理責任者

〇〇を、医療情報システム安全管理責任者として定める。△△（理事長、病院長）を当院におけるサイバーセキュリティに関する最高責任者とする。

（医療機関の規模・組織等によっては上記が兼務することも想定される。）

2.1.2 組織体制図

診療継続及び医療情報システムの復旧を目的としたサイバーセキュリティの組織体制を以下のとおり定める。担当部署、担当者、役割についても示す。



図〇：平時の組織体制図（例）

表〇：担当者の役割（例）

役割	担当部署・担当者	役割の概要
医療情報システム最高責任者	病院長	診療継続及び医療情報システムの復旧の計画策定を統括し、最終的な責任を負う。
医療情報システム安全管理責任者	〇〇	医療情報システム復旧の計画策定に関する各種検討作業を行う。
病院事務部	〇〇	診療継続の計画策定に関する各種検討作業を行う。
診療部門システム担当者	〇〇課	各診療部門システムの運用継続計画策定に関する各種検討作業を行う。
委託先	〇〇社	医療情報システムの運用保守及び緊急時の状況に関する情報提供・対策調整

2.1.3 情報機器台帳

医療情報システム安全管理責任者は、情報機器の現況を反映した管理台帳を以下（または別紙資料）のとおり整備する。併せて、定期的に棚卸しを行い、機器の所在と稼働状況の確認を行う。

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～ ）

2.1.4 ネットワーク・システム構成図

医療情報システム安全管理責任者は、医療機関等で導入している医療情報システムの全体構成図（ネットワーク図、システム構成図等）を整備する（ネットワークの全体像が分かりやすいものを作成）。併せて、構成、接続等に変更が生じた場合には構成図の更新を行い、常に最新の状態を保つ。

2.1.5 リスク評価・代替運用

各システムが利用できなくなった場合、その業務内容の代替手段を以下のとおり定める。また、代替運用方法については別途、システム停止時の代替運用マニュアル等にて定める。

表◯：業務内容に対する代替手段（例）

業務内容	システム	代替手段
診療録等	電子カルテシステム	紙運用
処方・検査	オーダリングシステム	紙運用（カーボンコピー）
放射線画像診断	PACS	撮影機器ワークステーションにて画像閲覧
会計	医事会計システム	未収扱いを検討
○○○○○○	○○○○○○	○○○○○○

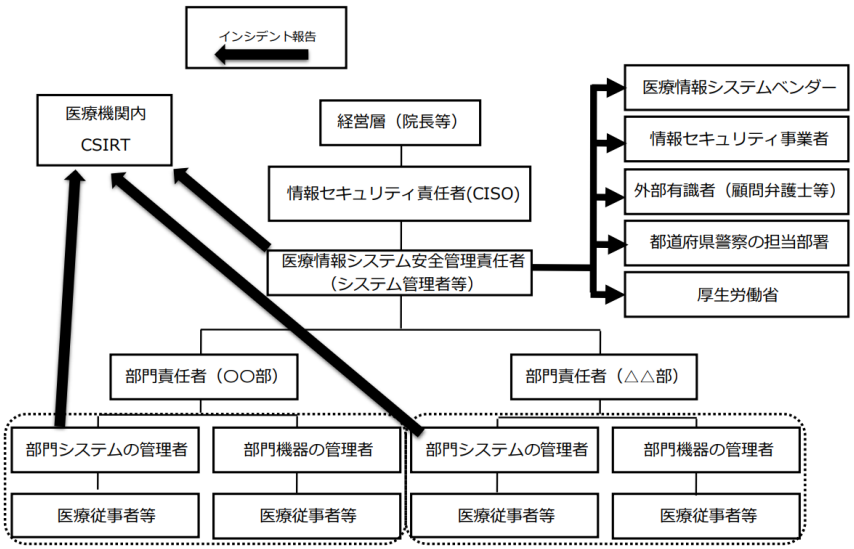
2.1.6 脆弱性に関する対策

医療情報システム安全管理責任者は、契約等で定められた責任分界をもとにサーバ、端末 PC、ネットワーク機器について脆弱性情報の収集を行う。脆弱性が発見された機器について、脆弱性対応プログラムの適応を行う。万が一、適応できない場合の代替手段（隔離運用、隔壁の追加、監視の強化、機器入れ替え等）について事業者等と合意した上で取り決め、実施する。

2.2　非常時に備えたサイバーセキュリティ体制

2.2.1 連絡体制図

診療継続及び医療情報システムの復旧に資するアクションを迅速に行う目的で、サイバーセキュリティの連絡体制（連絡先、担当、メールアドレス、電話番号、連絡目的等）及び外部関係機関の連絡先を以下のとおり定める。



（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～）

図〇：連絡体制図（例）

表〇：外部関係機関の連絡先一覧（例）

外部関係機関	連絡先
厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室	03-6812-7837 igishitsu@mhlw.go.jp
〇〇（都道府県警察の担当部署）	××-××××-××××
〇〇	××-××××-××××
〇〇	××-××××-××××

2.2.2 情報収集体制

当院における各システムの脆弱性情報について事業者等から情報提供を定期的に受け取ることができる体制を以下のとおり構築する。

表◯：事業者等の連絡先（例）

システム	担当	連絡先
電子カルテ	◯◯社	××-××××-×××× ◯◯@◯◯
保守委託先	◯◯社	××-××××-×××× ◯◯@◯◯
放射線撮影機器	◯◯社	××-××××-×××× ◯◯@◯◯
検査機器	◯◯社	××-××××-×××× ◯◯@◯◯
◯◯	◯◯社	××-××××-×××× ◯◯@◯◯

2.2.3 教育体制

本 BCP が迅速かつ適切に利用できるよう、年◯回以上の教育、訓練を実施する。情報セキュリティ責任者（CISO）、医療情報システム安全管理責任者は年間の教育計画に沿った訓練が適切に実施されるように監督する。訓練結果により、事前対策やサイバー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、課題の解決もしくは改善に向けた計画の立案をする。

2.2.4 バックアップ体制

サイバーインシデント発生時に備えた、データとシステムのバックアップの頻度、作成方法及び復旧方法について以下のとおり定める。

表◯：バックアップの作成と復旧方法（例）

システム	頻度	作成方法	復旧方法
電子カルテ	1 日	バックアップサーバにデータベースのバックアップを作成する	データベースを再構築した後に、バックアップサーバのデータを復元する
	7 日	磁気テープ・光学メディア・外付け HDD 等にデータベースとシステムファイルのバックアップを作成する	システムの OS を再構築した後に、磁気テープのシステムファイルとデータベースのデータを復元する
◯◯	◯◯	◯◯	◯◯
◯◯	◯◯	◯◯	◯◯

第３章 サイバーインシデント発生時の対応

3.1　異常発見時の連絡先

異常発見時の連絡経路は 2.2.1 の表◯に示す通りとする。あわせて、各担当部門の連絡先は以下のとおり示す。なお、部門システムの管理者は連絡先が全職員に把握されるように明示して、常に最新版で管理し連絡経路が機能することを担保する。

表◯：部門連絡先一覧（例）

部署名	担当者	連絡先
◯◯部門	◯◯	××-××××-××××
システム管理室	◯◯	××-××××-××××
医療情報システム安全管理責任者	◯◯	××-××××-××××

システム	事業者	担当者	連絡先
電子カルテシステム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××
◯◯◯システム	◯◯	◯◯	××-××××-××××

3.2　システム異常の検知と経営層への情報伝達

システム異常を検知した場合、あらかじめ定めた項目（発生場所、発生箇所、発生日時、連絡者、異常の内容・範囲）について担当部門に報告できるように周知する。なお、口頭による連絡後、「報告様式」を用いて記録を残す。また、院内職員から発出された異常において、医療情報システム安全管理責任者によりサイバー攻撃の可能性が思慮された場合、2.2.1 で作成した連絡体制図を基に、速やかに経営層ならびに関係各所・外部関係機関に共有され、意思決定できるように努める。

3.3　初動対応

サイバーインシデント発生後は、以下のとおり対応する

3.3.1 原因調査

医療情報システム安全管理責任者はサイバーインシデントの原因や被害範囲の特定のために、医療情報システム・サービス事業者へ以下の調査依頼を指示または実施する。

I.　ネットワーク機器やケーブル等の調査
II.　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
III.　情報漏えいの有無に関する調査
IV.　メンテナンスやデータ移行等の作業に関する調査
V.　○○○○○○

3.3.2 被害拡大防止

被害拡大防止のための対応を行う。まずは、バックアップに通ずるネットワークの遮断を行う。次に、外部の通信経路を遮断する。その上で、被害箇所から攻撃範囲および侵入経路の推定を行った上で、セグメンテーション境界において、通信を遮断して感染拡大防止を図る。

3.3.3 経営層への報告

医療情報システム安全管理責任者はサイバーインシデントについて経営層に対して、現在の被害状況を報告するとともにインシデント対応方法と患者安全を担保する運用方針案を提案する。この内容を踏まえて、経営層はシステム停止に伴う診療継続方針（診療体制の確保等）を検討し意思決定する。決定した内容は、速やかに 2.2.1 の連絡体制図で定める組織内ならびに外部関係機関へ周知を行う。

3.4　診療継続

サイバーインシデント対応と診療継続について報告を受けた経営層は以下のとおり対応する。

3.4.1 医療情報システムの縮退運転判断

経営層は医療情報システム安全管理責任者からの提案を受け、医療情報システム等の縮退運転または運転中止を判断する。また、インシデント対応中の診療継続においては、紙カルテの運用等、自然災害時を想定した事業継続計画（もしくはシステムダウン時マニュアル等）に則り運用する。

3.4.2 被害状況等調査（フォレンジック調査＋証拠保全）

医療情報システム安全管理責任者は、証拠保全の作業と診療継続に関する作業を調整しながら両立させる。具体的には、アクセスログの分析や情報の改ざん、暗号化の有無等からサイバー攻撃の範囲、個人情報漏えいの有無等の調査について医療安全を担保しつつ行う。必要に応じて医療情報システム・サービス事業者等へ協力依頼して調査を進める。なお、調査状況は随時経営層に報告する。

3.4.3 組織対応方針の確認と外部関係機関への報告

医療情報システム安全管理責任者の被害状況および調査結果に基づき、経営層は復旧対応方針（復旧に向けた対応、広報への対応）を決定し、その対応を関係者に指示する。また、2.2.1 で定める外部関係機関へ報告を行う。外部関係機関へは被害拡大防止等の観点からできる限り早く連絡する。

3.5 復旧処理

復旧計画に基づいて、以下のとおり対応する。医療情報システム安全管理責任者は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。

3.5.1 復旧指示と復旧作業

医療情報システム安全管理責任者は、経営層からの復旧指示を起点とする復旧対応方針に基づき、システムの復旧作業(システムの再設定、再インストール、バックアップデータからの復元等)並びに検証作業を行う。必要に応じ医療情報システム・サービス事業者に対応を依頼する。あわせて、システム停止中に生じたアナログ情報についてシステムに反映させる選択肢を提示する。経営層は、アナログ情報の反映時期ならびに程度を医療安全の観点を踏まえて意思決定する。

3.5.2 結果の確認

医療情報システム安全管理責任者は、復旧作業により復旧したシステムが安全な状態で正常に稼働したことを確認する。正常に稼働することが確認できた時点で、経営層に報告する。経営層は診療状況を総合的に勘案し、緊急時運用から通常運用への復旧を宣言する。

第 4 章 事後対応

4.1 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、経営層及び組織内に報告する。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。

4.2 再発防止

4.2.1 再発防止策検討・策定

4.1 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、経営層に提案する。経営層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。経営層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。

4.2.2 事業者への指示

経営層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等により、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、医療機関側と誠実に議論し、計画を立てて実施する。

4.3 情報公開

経営層は、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。

サイバー攻撃を想定した事業継続計画（BCP）の作成について

厚生労働省では、令和５年度から、医療法に基づく医療機関に対する立入検査の項目に、サイバーセキュリティ対策を位置付けました。立入検査の際に確認する項目は、「医療情報システムの安全管理に関するガイドライン」から優先的に取り組むべき項目について、「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」（以下「チェックリスト」という。）によりお示ししてきたところです。

昨今の巧妙化したサイバー攻撃の現状において、セキュリティ対策を講じることでリスクを低減させることはもちろん重要ですが、リスクを完全に排除することはできません。

例えば、過去には、

・インシデント発生時の初動対応について十分に協議されておらず、証拠保全が不十分となり、被害範囲の特定ができなかった、
・インシデント発生時に、ネットワーク機器が院内のどこに配置されているかわからず、原因究明に時間を要した、
・ランサムウェアによる攻撃の際に、バックアップが適切に確保できておらず、復旧が難航した、

といった事例が実際に発生しており、このようなケースでは、診療継続を含めた医療機関の機能に重大な影響が生じます。

サイバー攻撃を「どのように防ぐか」だけでなく「発生時にどのように対応するか」という意識で、非常時に診療への影響を最低限に抑えるための対応を、あらかじめ「サイバー攻撃を想定した事業継続計画（BCP）」（以下「BCP」という。）として策定しておくことで、適切な復旧対応等を行うことが可能となります。

こうしたことから、チェックリストの項目としても、医療機関に対して BCP の策定を求めており、今般、BCP の策定に際して参考としていただけるよう、「サイバー攻撃を想定した事業継続計画（BCP）策定の確認表」（以下「確認表」という。）を作成しました。医療機関の特性に応じて必要とされる BCP は様々ですが、今般作成した確認表等や関係団体より発出されている資料等を参考に、貴施設においてもサイバー攻撃を想定した BCP の策定をお願いします。

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。	

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。	
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、可能性について、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。	

令和６年　　３月　　７日

厚生労働大臣
~~（国立医薬品食品衛生研究所長）~~ 殿
~~（国立保健医療科学院長）~~

機関名　国立大学法人群馬大学

所属研究機関長　職　名　学長

氏　名　石崎　泰樹

次の職員の令和５年度厚生労働科学研究費の調査研究における、倫理審査状況及び利益相反等の管理については以下のとおりです。

１．研究事業名　厚生労働科学特別研究事業

２．研究課題名　医療機関におけるサイバー攻撃対応のための事業継続計画（BCP）の普及に向けた研究

３．研究者名　（所属部署・職名）　医学部附属病院・准教授

（氏名・フリガナ）　鳥飼　幸太（トリカイ　コウタ）

４．倫理審査の状況

	該当性の有無	左記で該当がある場合のみ記入（※1）		
	有　無	審査済み	審査した機関	未審査（※2）
人を対象とする生命科学・医学系研究に関する倫理指針（※3）	□　■	□		□
遺伝子治療等臨床研究に関する指針	□　■	□		□
厚生労働省の所管する実施機関における動物実験等の実施に関する基本指針	□　■	□		□
その他、該当する倫理指針があれば記入すること（指針の名称：　　）	□　■	□		□

（※1）当該研究者が当該研究を実施するに当たり遵守すべき倫理指針に関する倫理委員会の審査が済んでいる場合は、「審査済み」にチェックし一部若しくは全部の審査が完了していない場合は、「未審査」にチェックすること。

その他（特記事項）

（※2）未審査に場合は、その理由を記載すること。
（※3）廃止前の「疫学研究に関する倫理指針」、「臨床研究に関する倫理指針」、「ヒトゲノム・遺伝子解析研究に関する倫理指針」、「人を対象とする医学系研究に関する倫理指針」に準拠する場合は、当該項目に記入すること。

５．厚生労働分野の研究活動における不正行為への対応について

研究倫理教育の受講状況	受講 ■　　未受講 □

６．利益相反の管理

当研究機関におけるＣＯＩの管理に関する規定の策定	有 ■　無 □（無の場合はその理由：　　）
当研究機関におけるＣＯＩ委員会設置の有無	有 ■　無 □（無の場合は委託先機関：　　）
当研究に係るＣＯＩについての報告・審査の有無	有 ■　無 □（無の場合はその理由：　　）
当研究に係るＣＯＩについての指導・管理の有無	有 □　無 ■（有の場合はその内容：　　）

（留意事項）　・該当する□にチェックを入れること。
・分担研究者の所属する機関の長も作成すること。