（情シ　42）
令和 3 年 10 月 22 日

都道府県医師会　担当理事　殿

日　本　医　師　会
常任理事　長島　公之
（公印省略）

「医療情報システムの安全管理に関するガイドライン」に関する
追加資料（チェックリスト、フローチャート）について

平素より本会会務の運営に対しましてご高配を賜り深く感謝申し上げます。

さて今般、厚生労働省医政局研究開発振興課より、本会に対して標記に関する周知方依頼がありました。

本件は、平成 17 年 3 月 31 日「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等の施行等について」（医政発第 0331009 号薬食発第 0331020 号保発第 0331005 号厚生労働省医政局長厚生労働省医薬食品局長厚生労働省保険局長連名通知）の別添として示された「医療情報システムの安全管理に関するガイドライン」の第 5.1 版につきまして、「『医療情報システムの安全管理に関するガイドライン 第 5.1 版』の策定について」（日医発第 1104 号（情シ 53）令和 3 年 2 月 8 日）にてお知らせしたところでありますが、追加資料が策定・発出された旨の通知であります。

「医療機関のサイバーセキュリティ対策チェックリスト」

本チェックリストは、医療機関のサイバーセキュリティ対策の現状を把握することを目的に、そのチェック項目を整理したものであり、幅広くサイバーセキュリティ対策に対応した内容となっております。

チェックリストは、（1）経営層向けチェックリスト、（2）システム管理者向けチェックリスト、（3）医療従事者・一般のシステム利用者向けチェックリスト―の 3 種類から構成されており、医療機関のどの部分に弱みがあるのか把握し優先的に必要な対策を検討する一助となるものです。

「医療情報システム等の障害発生時の対応フローチャート」

本チャートは、医療機関がサイバーセキュリティの体制整備を行うにあたり、平時の備えや障害発生時に各担当者が行う対応について、フローチャートでまとめられております。体制整備や障害発生時の対応の確認を検討する一助となるものです。

つきましては、貴会におかれましても本件についてご了知いただくとともに、貴会管下郡市区医師会及び会員への周知方につき、ご高配賜りますようよろしくお願い申し上げます。

なお、ガイドラインの PDF 形式並びに本追加資料の PDF 形式は下記厚生労働省ホームページにて公開されており、ホームページ内には、医療機関の個別状況に応じて加工可能なようにエクセル形式ファイルも掲載されております。

「医療情報システムの安全管理に関するガイドライン第 5.1 版（令和 3 年 1 月）」
https://www.mhlw.go.jp/stf/shingi/0000516275.html
「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」の項目

以上

【(情シ 42) 添付書類／資料】

■「医療情報システムの安全管理に関するガイドライン」のチェックリスト、フローチャートの策定について（厚生労働省事務連絡／R3.10.20）
・「医療機関のサイバーセキュリティ対策チェックリスト」
・「医療情報システム等の障害発生時の対応フローチャート」

事　務　連　絡
令和３年１０月２０日

公益社団法人日本医師会　殿

厚生労働省医政局研究開発振興課

「医療情報システムの安全管理に関するガイドライン」に関する
「医療機関のサイバーセキュリティ対策チェックリスト」及び
「医療情報システム等の障害発生時の対応フローチャート」について

サイバー攻撃の手法の多様化・巧妙化、クラウドサービス等の普及等、医療情報システムを取り巻く環境の変化に対応するために、「医療情報システムの安全管理に関するガイドライン　第5.1版」を令和3年1月29日に策定したところです。

今般、医療機関におけるサイバーセキュリティ対策に資するために、別紙のとおり「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を策定し、「医療情報システムの安全管理に関するガイドライン　第 5.1 版」の別添としましたので、内容を御了知の上、貴会員等関係者に周知いただきますよう、よろしくお願いいたします。

なお、この「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」については厚生労働省ホームページの「医療情報システムの安全管理に関するガイドライン　第 5.1 版（令和 3 年 1 月）」（https://www.mhlw.go.jp/stf/shingi/0000516275.html）に掲載いたしますので、念のため申し添えます。

医療情報システムの安全管理に関するガイドライン

医療機関のサイバーセキュリティ対策チェックリスト

昨今、医療機関等へのサイバー攻撃が散見されており、医療情報の漏洩や、医療提供体制に影響が生じた事例もある。こうした状況下において、医療機関を中心とした医療分野のサイバーセキュリティ対策の強化は、より一層重要な取組となっている。

本チェックリストは、各医療機関において自院のサイバーセキュリティ対策の現状を把握することを目的に、そのチェック項目を整理したものであり、以下のガイドライン等を参考としているので、詳細は適宜参照されたい。

・医療情報システムの安全管理に関するガイドライン5.1版　本紙
・オンライン診療の適切な実施に関する指針
・電子処方箋の運用ガイドライン
・オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン
・国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンス
・サイバーセキュリティ経営ガイドライン Ver 2.0
・中小企業の情報セキュリティ対策ガイドライン第3版

なお、「医療情報システムの安全管理に関するガイドライン」の内容がe-文書法、個人情報保護法等への対応を行うためのセキュリティ管理なども含めて多岐に渡る一方、本チェックリストは「医療情報システムの安全管理に関するガイドライン」のみを遵守しているかのチェックリストではなく、幅広くサイバーセキュリティ対策に特化した内容となっていることに留意されたい。

全体のチェックリストの構成について

■　チェックリストは、チェックの主体によって、（1）経営層向けチェックリスト　（2）システム管理者向けチェックリスト（3）医療従事者・一般のシステム利用者向けチェックリスト　の3種類から構成されている。

■　各チェック項目は、チェックの主体に加えて、チェックの視点によって、①予防的手続（何か起きないように事前に予防するために必要な手続を指す）、②発見的手続（何か起きたときに迅速に発見するために必要な手続を指す）、③是正的手続（何か起きた後で迅速に現状復帰等をするために必要な手続を指す）に分類されている。

■　全体として医療機関のどの部分（チェックの主体やチェックの視点等）に弱みがあるのか把握し、優先的に必要な対策を検討の上、全体のバランスを取りながらサイバーセキュリティ対策の強化を図ることが重要となる。

経営層向け　サイバーセキュリティ対策チェックリストの使い方

■　経営層が、自らのリーダーシップでセキュリティ対策を進めるために活用することを目的としている。

■　自院のサイバーセキュリティ対策の現状を把握するため、医療情報システム部門の責任者や各部門システムの管理者、各部門の責任者等を招集し、チェックリストに基づいてコミュニケーションを取りながら、セキュリティ対策の強化を検討する。

■　また、定期的（年に数回等）に各責任者とコミュニケーションを取ってセキュリティ対策強化の状況について報告を受け、今後の体制強化や予算等の方針を検討・決定する。

システム管理者向け　サイバーセキュリティ対策チェックリストの使い方

■　医療機関のシステム管理者（他業務と兼務している職員を含む）が、医療機関のサイバーセキュリティ対策を具体的に進めるために活用することを目的としている。

■　チェックリストに基づいて、セキュリティ対策のどの部分（各チェックの主体における予防・発見・是正の視点等）に弱みがあるのか把握の上、必要な対策の優先度を検討し、対策の強化を図る。

■　医療機関の規模や体制により、自らチェックできない場合は、医療情報システムベンダ、サービス事業者等に確認を行いながら、必要なサイバーセキュリティ対策について検討を進める。

医療従事者・一般のシステム利用者向けサイバーセキュリティ対策チェックリストの使い方

■　医療従事者・一般のシステム利用者が普段の業務において何に気を付ければいいのか理解し、日常的にセキュリティ対策に取り組むために活用することを目的としている。

■　医療機関のシステム管理者が全職員に配布・回収し、セキュリティ対策の不十分な部分を把握するとともに、定期的な職員のセキュリティ意識の確認、職員の教育等に活用する。

■　特定の部門の職員や職種等においてセキュリティ対策の不十分な部分が見受けられる場合は、部門の管理者等と情報共有し、組織的にセキュリティ強化を図る。

経営層向け　サイバーセキュリティ対策チェックリスト

記入者	日付

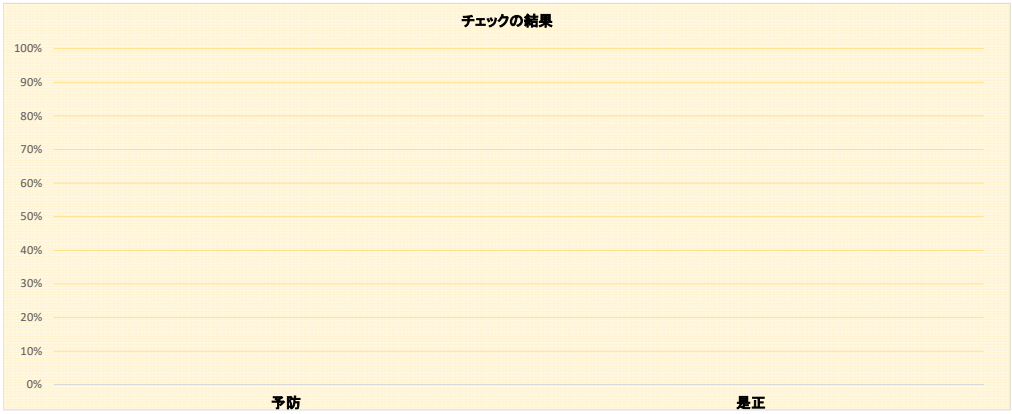
NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	予防	運用管理規程等において次の内容を定めているか ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合はその情報端末等の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	
3	予防	経営者がサイバーセキュリティリスク(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃により損害を被るリスク)を経営リスクの1つとして認識しているか	
4	予防	サイバー攻撃により医療情報が暗号化され、復元のための身代金を請求された医療機関等、公表されているサイバー攻撃の情報を定期的、必要時に確認しているか	
5	予防	サイバーセキュリティ(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)にかかる監査を実施しているか	
6	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為や取組状況)を外部に公開しているか	
7	予防	ウェブサイトの運営において、サーバやネットワーク機器、ウェブアプリケーションに対する脆弱性検査（診断）、監査を実施しているか	
8	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)の現状を調査しているか	
9	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)の現状に基づいて、医療機関で可能な対策を実施しているか	
10	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)を進めるための予算や人材を医療機関で確保しているか	
11	予防	サイバーセキュリティ対策(コンピューターへの不正侵入やウイルス感染、情報漏洩、データの改ざんや破壊といったサイバー攻撃から、情報データを防御する行為の対応状況)について医療機関内部で講じることが難しい場合、外部の組織への相談等を検討しているか	
12	予防	不正防止の観点から、担当者間、部門間等で相互に情報管理に関して、運用状況の点検を実施し、相互牽制（各病棟間、外来部門、医事課事務部門間等）を働かせているか	
13	予防	サイバーセキュリティに関する取組方針を常日頃から従業員や外部委託先等に伝えてコミュニケーションを取っているか	
14	予防	法令上の守秘義務のある者以外の者を従業員として採用するにあたって雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施しているか	
15	予防	従業者の退職後の個人情報保護規程を定めているか	
16	是正	インシデント対応の専門チーム（CSIRT等）を設置しているか	
17	是正	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めているか	
18	是正	医療機関等において、コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合は、直ちに医療情報システムの保守会社等に連絡の上、医療情報システムに障害が発生し、個人情報の漏洩や医療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した場合には、厚生労働省医政局研究開発振興課医療情報技術推進室に連絡することに決めているか	

予防・・・何か起きないように事前に予防するために必要な手続を指す。
発見・・・何か起きたときに迅速に発見するために必要な手続きを指す。
是正・・・何か起きた後で迅速に現状復帰等をするために必要な手続を指す。

チェックの結果

全体として医療機関のどの部分に弱みがあるのか把握し、優先的に必要な対策を実施の上、
全体のバランスを取りながらサイバーセキュリティ対策を強化するため、ご活用ください。

分類	割合	項目数
予防	0.0%	0/15
発見	-	0/0
是正	0.0%	0/3



システム管理者向け　サイバーセキュリティ対策チェックリスト

記入者	日付

NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムで扱う情報を全てリストアップし、リストアップした情報資産に対してリスク分析を実施しているか （医療情報システムの安全管理に関するガイドラインの他、適宜、中小企業の情報セキュリティ対策ガイドライン第3版「（6）詳細リスク分析の実施方法」、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（5. 安全管理のためのリスクマネジメントプロセス）等を参考にすること）	
2	予防	医療情報システムベンダ及びサービス事業者から、役割分担や医療情報システムの安全管理に関する評価、リスクアセスメントの結果、リスクに応じた技術的対策、運用管理規定等の情報を収集しているか	
3	予防	リスク分析の結果に対して、医療情報システムの安全管理に関するガイドライン第5.1版 6.3章～6.12章に示す対策等を実施しているか	
4	予防	個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めているか	
5	予防	医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか	
6	予防	個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めているか	
7	予防	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）の収集を実施しているか	
8	予防	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関の他の情報システムへの影響を確認した上で、従業員に対応方法について指示をしているか	
9	予防	セキュリティに関する脅威や対策等について、収集した情報を他の医療機関等と共有しているか	
10	予防	セキュリティ専門知識を持つ者等と協力して脆弱性検査を実施し、既知の脆弱性の有無を点検しているか	
11	予防	情報機器の設置場所や記録媒体の保存場所について、施錠管理、入室権限、盗難・紛失防止対策を行っているか	
12	予防	医療情報システムへのアクセスにおける利用者の識別・認証を行っているか	
13	予防	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しているか	
14	予防	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ときを想定し、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しているか	
15	予防	利用者の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行っているか。また人事異動等による利用者の担当業務の変更等に合わせて、アクセス権限の変更を行うことを、運用管理規程で定めているか。	
16	予防	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しているか	
17	予防	アクセスログの記録に用いる時刻情報は、日本標準時等の信頼できるものを利用しているか。また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っているか	
18	予防	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、コンピュータウイルス等の不正なソフトウェアが混入していないか確認しているか。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しているか	
19	予防	常時コンピュータウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとっているか。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）を行っているか	
20	予防	医療機関が管理する外部媒体は、ウイルスチェック機能やパスワードロック機能、生体認証等のセキュリティ対策機能を具備したものになっているか	
21	予防	メールサーバーにフィルタリング機能を設定し、迷惑メール等のブロックをしているか	
22	予防	URLフィルタリング機能等を持つ機器を導入し、職員が業務に関係がないウェブサイトの閲覧をしようとした場合に停止や警告等を行っているか	
23	予防	令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行っているか	
24	予防	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しているか 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、適切な手法で管理・運用しているか。また、利用者識別にICカード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めているか	
25	予防	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しているか。 利用者のパスワードの失念や、パスワード漏えい流出のおそれなどにより、医療情報システムの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等のコピーを添付）しているか。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知しているか。なお、パスワード漏えい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ているか	
26	予防	パスワードを利用者認証に使用する場合、以下のいずれかを要件としているか。 a. 英数字、記号を混在させた13 文字以上の推定困難な文字列 b. 英数字、記号を混在させた8 文字以上の推定困難な文字列を定期的に変更させる（最長でも2 ヶ月以内） c. 二要素以上の認証の場合、英数字、記号を混在させた8 文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用にPIN 等が設定されている場合には、この限りではない。 いずれのパスワードを設定した場合でも、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏えい対策が講じられていることを確認しているか	
27	予防	無線LAN を利用する場合、次に掲げる対策を実施しているか。 適切な利用者以外に無線LAN を利用されないようにANY接続拒否等の対策を実施しているか	
28	予防	無線LAN を利用する場合、次に掲げる対策を実施しているか。 少なくともMAC アドレスによるアクセス制限等の不正アクセス対策を実施しているか	
29	予防	無線LAN を利用する場合、次に掲げる対策を実施しているか。 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しているか	
30	予防	無線LAN を利用する場合、次に掲げる対策を実施しているか。 電波を発する機器（携帯ゲーム機等）による電波干渉に留意しているか	
31	予防	IoT機器を利用する場合、次に掲げる対策を実施しているか。 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ているか	
32	予防	IoT機器を利用する場合、次に掲げる対策を実施しているか。 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は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ているか。また、機器に異常や不都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、患者等に情報提供をしているか	
33	予防	IoT機器を利用する場合、次に掲げる対策を実施しているか。 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、運用しているか	
34	予防	IoT機器を利用する場合、次に掲げる対策を実施しているか。 使用が終了した又は不具合のために使用を停止している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外部から接続されるリスクがあるため、対策しているか	

NO	視点	チェック項目	チェック欄（○or×）
35	予防	従業者に対し個人情報の安全管理に関する教育訓練を定期的に実施しているか	
36	予防	医療機関等の管理者は、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は、個人情報保護のため、次に掲げる対策を実施しているか。 a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。 b 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認すること。 c 清掃等の直接医療情報システムにアクセスしない作業の場合でも、作業結果を定期的に確認すること。 d 受託する事業者が再委託を行うか否かを明確にすること。受託する事業者が再委託を行う場合は、受託する事業者と同等の個人情報保護に関する対策及び契約がなされることを条件とすること。	
37	予防	再委託が行われる場合は、再委託を受ける事業者に対しても、委託会社と同等の義務を課しているか	
38	予防	医療情報等の機密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しているか	
39	予防	情報機器に対して起動パスワード等を設定しているか。また設定に当たっては推定しやすいパスワード等の利用を避けるとともに、定期的なパスワードの変更等の対策を実施しているか	
40	予防	持ち出した情報機器を外部のネットワークに接続したり、他の外部媒体に接続する場合には、コンピューターウイルス対策ソフトやパーソナルファイアーウォールの導入等により、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施しているか なお、ネットワークに接続する場合は医療情報システムの安全管理に関するガイドライン醍5.1版 6.11 章の規定を遵守しているか。特に、公衆無線LAN は基本的に利用してはならず、公衆無線LAN しか利用できない環境である場合に限り、利用を認めているか。（利用する場合は医療情報システムの安全管理に関するガイドライン第5.1版 6.11 章で述べている基準を満たした通信手段を選択する必要がある。）	
41	予防	持ち出した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し、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又は停止するか、業務に対して影響がないことを確認しているか	
42	予防	盗難、紛失時の対応を従業者等に対して周知徹底し、教育を実施しているか	
43	予防	医療サービスを提供し続けるためのBCP（Business Continuity Plan：事業継続計画）の一環として、“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めているか	
44	予防	非常時における対応及び医療情報システムの障害時の対応に関する教育及び訓練を従業者に対して行っているか	
45	予防	非常時の医療情報システムの運用として、「非常時のユーザアカウントや非常時用機能」の管理手順を整備しているか	
46	予防	非常時の医療情報システムの運用として、非常時機能が定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しているか。	
47	予防	ネットワーク経路でのメッセージ挿入、コンピューターウイルス混入等の改ざん又は中間者攻撃等を防止する対策を実施しているか	
48	予防	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対策を実施しているか	
49	予防	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 クライアント認証を実施しているか。（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性水準の高い「高セキュリティ型」に準じた適切な設定を行っているか またソフトウェア型のIPsec 又はTLS1.2 以上により接続する場合、セッション間の回り込み（正規のルートでは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しているか。	
50	予防	SSLVPNは偽サーバへの対策が不十分なものが多いため、原則として使用していないか	
51	予防	クローズドなネットワークで接続する場合でも、コンピュータウイルス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しているか	
52	予防	電子署名に用いる秘密鍵の管理は、認証局が定める「証明書ポリシー」（CP）等で定める鍵管理の要件を満たして行っているか	
53	予防	医療機関等の間の情報通信において、医療機関、電子通信事業者、システムインテグレーター、運用を受託する事業者、遠隔保守を行う機器保守会社等、関連組織で、次に掲げる事項について責任分界点、責任の所在を契約書等で明確にしているか ・診療録等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通の場合又は著しい遅延が発生している場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処	
54	予防	医療機関等内において、次に掲げる事項を契約や運用管理規程等で定めているか ・通信機器、暗号化装置、認証装置等の管理責任（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・患者等に対する説明責任 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置 ・交換した医療情報等に対する管理責任及び事後責任（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項）	
55	予防	ルーター等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶVPNの間で送受信ができないように経路を設定しているか。	
56	予防	ネットワークを通じて医療機関等の外部に医療情報を保存する場合、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っているか	
57	予防	システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするため、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意しているか	
58	予防	医療機関等に医療情報を保存する場合、コンピュータウイルスを含む不適切なソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理しているか	
59	予防	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に医療情報を保存する場合、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、少なくとも契約期間において毎年報告を受けているか	
60	予防	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に医療情報を保存する場合、外部保存を受託する事業者の選定に当たっては、事業者のセキュリティ対策状況を示す資料を確認しているか	
61	予防	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に医療情報を保存する場合、保存された情報を格納する機器等が、国内法の適用を受けることを確認しているか	

NO	視点	チェック項目	チェック欄（○or×）
62	予防	医療機関等が外部の事業者との契約に基づいて確保した安全な場所に医療情報を保存する場合、外部保存を受託する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しているか 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 b 医療情報等の安全管理に係る実施体制の整備状況 c 実績等に基づく個人データ安全管理に関する信用度 d 財務諸表等に基づく経営の健全性 e JIS Q 15001、JIS Q 27001 の認証の有無 f「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。 ・JASA クラウドセキュリティ推進協議会CS ゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7 号） ・AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会 IT2 号） 上記認証等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しているか。 ・システム監査技術者 ・Certified Information Systems Auditor ISACA 認定 g 医療情報を保存する機器が設置されている場所(地域、国) h 受託事業者に対する国外法の適用可能性	
63	予防	可搬媒体の授受及び保存状況を確実に記録し、事故、紛失や窃盗を防止しているか。また、他の保存文書等との区別を行うことにより、混同を防止しているか	
64	予防	システム等の潜在的セキュリティリスクを特定するためのセキュリティ文書（例：SBOM（ソフトウェア部品表）など）を入手してサイバーセキュリティ対策の必要性の検討をしているか	
65	予防	サイバーセキュリティに関するサポート対象外の医療機器を把握し、業者によるサポートを受けられる医療機器等への置換の計画を作成して実行しているか	
66	予防	ウェブサイトの構築前に情報セキュリティが継続的に維持され、最新の脅威に対し対策するために、組織の状況に応じた運営形態（例・オンプレミス、レンタルサーバー・クラウドサービス、モール・ASP）を選定しているか	
67	予防	ウェブサイトの安全を維持するために、サーバーOSやソフトウェアに対して脆弱性修正パッチの適用や安全な設定を維持しているか	
68	予防	ウェブサイトで公開すべきでないファイルは公開していないか	
69	予防	ウェブサイトの運営において、不要になったページやウェブサイトは公開していないか	
70	予防	IPA（独立行政法人 情報処理推進機構）が「安全なウェブサイトの作り方」に取り上げている脆弱性を確認し、対策をしているか	
71	予防	ウェブアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしているか	
72	予防	ウェブサイトの運営において、攻撃者に余計な情報を与えないために、ウェブサイトの閲覧者へのエラーメッセージは不要又は必要最低限にしているか。	
73	予防	ウェブサイトの運営において、事故や故障、不正アクセス等の不審な動きがあった際に、原因を追究するための重要な情報源として、必要に応じてウェブアプリケーションのログを保管し、定期的に確認をしているか	
74	予防	ウェブサイトの運営において、OSやサーバソフトウェア、ミドルウェアについて、修正プログラムが公表された際は適用し、脆弱性を解消しているか。（なお、ソフトウェアをバージョンアップした場合、今まで動作していたウェブアプリケーションが正常に動作しなくなる場合があるため、事前の検証の必要がある。）	
75	予防	ウェブサーバ上で不要なサービスが起動している場合、そのサービスが悪用されることがあるため、最低限必要なもの以外は、停止しているか。また、古いバージョンのアプリケーションの脆弱性を攻撃される恐れがあるため、不要になったアプリケーションも削除しているか。	
76	予防	ウェブサーバやウェブサーバを管理する端末に不要なアカウントが登録されている場合、悪用される恐れが高まるため、アカウントの一覧を見直して、最低限必要なものを除き、削除しているか。（特に、開発工程やテスト環境で使用したアカウントが残っているケースがあり、確認することが重要である）	
77	予防	ウェブサイトの運営において、推測されにくい複雑なパスワードを設定・使用しているか。（特に管理者権限を持ったアカウントやリモート管理ソフトなどのアプリケーションの場合、悪用される可能性が高いため、安易なパスワードが設定されていないか、確認する必要がある）	
78	予防	ウェブサーバ上のファイル、ディレクトリに適切なアクセス制御をしているか。（アクセス制御をしていない場合、第三者に非公開のファイルを見られたり、プログラムが実行されたりする可能性がある）	
79	予防	ウェブサーバのログを保管し、定期的に確認しているか。（ウェブサーバ上では各種ログファイル（「システムログ」「アプリケーションログ」「アクセスログ」「データベース操作ログ」など）があり、これらのログファイルを確認することにより、事故や故障、不審な動き（不正アクセス）があったことに気づくきっかけになることがある）	
80	予防	ウェブサイトの運営において、境界ルータなどのネットワーク機器を使用して、外部から内部ネットワークへの不要な通信は遮断しているか。（運用上、外部から内部ネットワークへに通信が必要な場合は、情報を秘匿するためVPN 等を利用することを検討しているか）	
81	予防	ウェブサイトの運営において、ファイアウォールを設置し、「どのサーバ」の「どのサービス」に「どこから」のアクセスを許可するのかを把握し、適切にフィルタリングをしているか。	
82	予防	ウェブサイトに脆弱性が発見された場合、ウェブアプリケーションを速やかに修正できないことがあるため、修正されるまでの間、攻撃による影響を低減する対策としてIDSやIPSおよびWAFを導入してウェブアプリケーションを保護し、不正な通信を検知または遮断しているか	
83	予防	ウェブサイトの運営において、事故や故障、不正アクセス等の不審な動きがあった際に、原因を追究するための重要な情報源として、必要に応じてネットワーク機器のログを保管し、定期的に確認をしているか	
84	予防	ウェブサイトの運営において、セキュリティ対策をサービス事業者側が提供していることがあるため、クラウドなどのサービスを利用する場合は、サービス事業者側の作業範囲とセキュリティ対策を把握した上で、不足する対策は自組織で対応することを検討しているか	

NO	視点	チェック項目	チェック欄（○or×）
85	発見	リストアップした情報資産は医療情報システム安全管理責任者が必要に応じて速やかに確認できる状態で管理しているか	
86	発見	アクセスログを記録するとともに、定期的にログを確認しているか。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しているか。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、操作内容等を記録しているか	
87	発見	情報処理機器自体を破棄する場合、必ず専門的な知識を有する者が行い、破棄終了後に、残存し、読み出し可能な情報がないこと及び確実に情報が廃棄されたことを確認しているか	
88	発見	外部保存を受託する事業者等に破棄を委託した場合は、医療情報システムの安全管理に関するガイドライン第5.1版 6.6 章C.2(事務取扱受託業者の監督及び守秘義務契約）に準じ、委託契約書等に明記するとともに、確実に情報が破棄されたことを確認しているか	
89	発見	メンテナンスを実施するためにサーバに保守会社の作業員（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させているか。（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）	
90	発見	リモートメンテナンス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、当該作業の終了後速やかに医療機関等の責任者が確認しているか	
91	発見	電子化した処方箋を修正する場合、修正前と修正後の処方箋が2重にならないために、修正後の処方箋と修正前のものを区分し、かつ修正責任者を明確にしているか	
92	是正	非常時の医療情報システムの運用として、医療情報システムがコンピュータウイルス等に感染した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備しているか	

予防・・・何か起きないように事前に予防するために必要な手続を指す。
発見・・・何か起きたときに迅速に発見するために必要な手続きを指す。
是正・・・何か起きた後で迅速に現状復帰等をするために必要な手続を指す。

チェックの結果

全体として医療機関のどの部分に弱みがあるのか把握し、優先的に必要な対策を実施の上、
全体のバランスを取りながらサイバーセキュリティ対策を強化するため、ご活用ください。

分類	割合	項目数
予防	0.0%	0/84
発見	0.0%	0/7
是正	0.0%	0/1

以下の項目について、「オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システム」を実施している場合のみチェックしてください

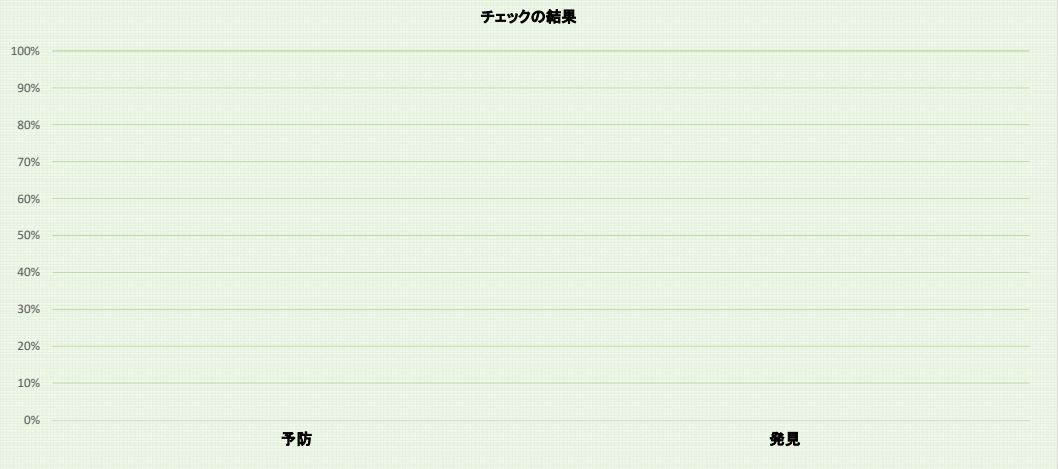
NO	視点	チェック項目	チェック欄（○or×）
1	予防	ネットワークの接続方式については、実施機関が別途認めたサービス事業者によるクローズドな接続方式とするとともに、医療機関等、審査支払機関、医療保険者等及び実施機関間を相互に接続するネットワーク回線において、許可されていない者による盗聴及び漏えいに対する機密性を確保する機能を有しているか	
2	発見	デジタル署名付きデータの送付と受領確認データの返送を確認及びデータの送付に関する受領確認データの相互送信、送信ログ及び受信ログの保管をしているか	

予防・・・何か起きないように事前に予防するために必要な手続を指す。
発見・・・何か起きたときに迅速に発見するために必要な手続きを指す。
是正・・・何か起きた後で迅速に現状復帰等をするために必要な手続を指す。

チェックの結果

全体として医療機関のどの部分に弱みがあるのか把握し、優先的に必要な対策を実施の上、
全体のバランスを取りながらサイバーセキュリティ対策を強化するため、ご活用ください。

分類	割合	項目数
予防	0.0%	0/1
発見	0.0%	0/1
是正	－	－



医療従事者・一般のシステム利用者向け　サイバーセキュリティ対策チェックリスト

記入者	日付

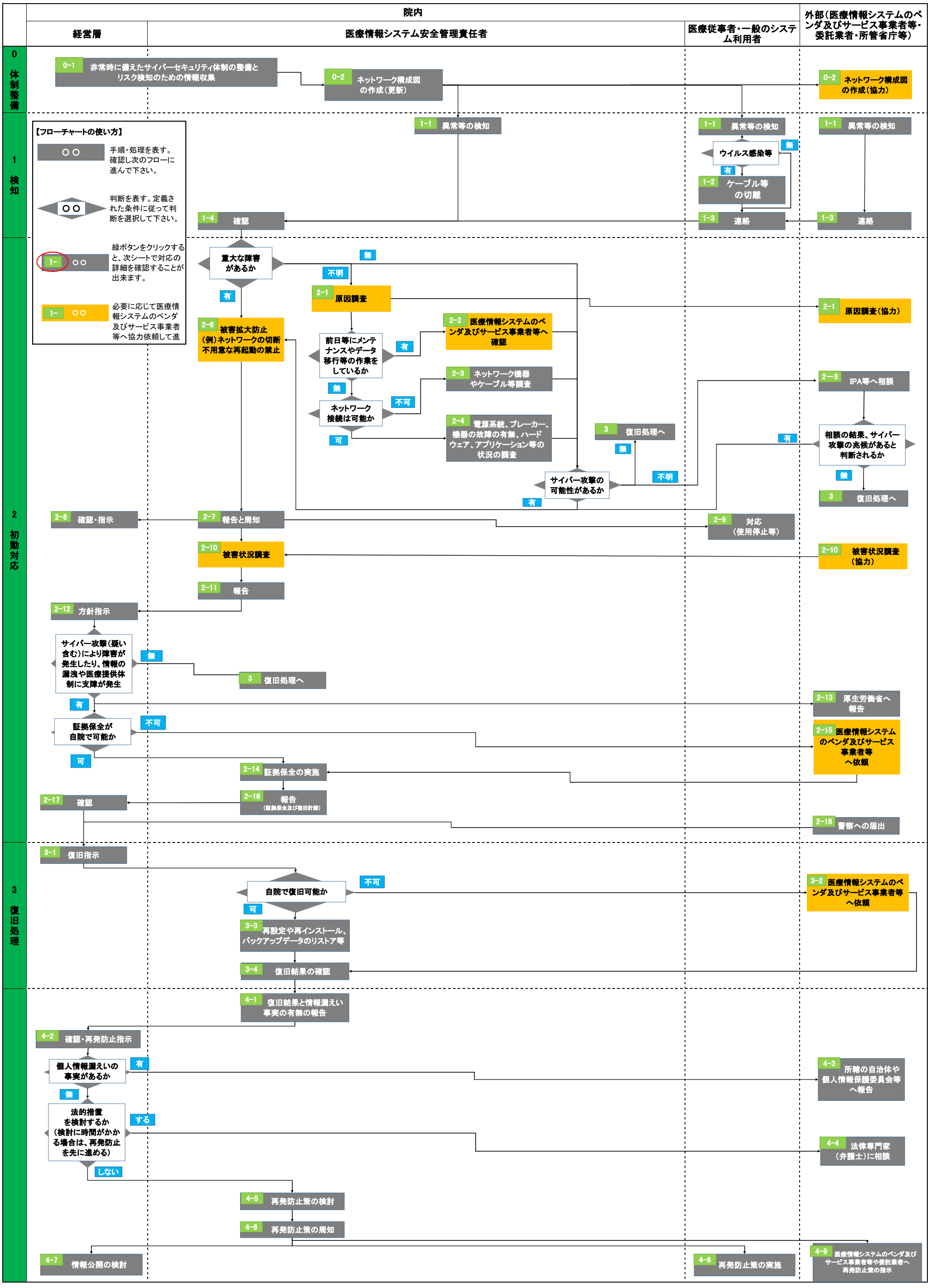
NO	チェック項目	チェック欄（○or×）
1	業務に不要なWEBサイトへのアクセスをしていないか	
2	システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っているか	
3	利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン（画面が他人から見えないようにするために、操作しないまま一定の時間が経つと自動的にパスワード付きスクリーンセーバーが起動するようにしたり、または自動的にログオフするように設定すること）等の対策を実施しているか	
4	従業員個人のUSBメモリ等の外部媒体を使用していないか又は業務上、外部媒体の使用が必要な場合は事前に申請し、医療機関が管理している外部媒体を使用しているか	
5	ソーシャルエンジニアリング（人の心理的・社会的な弱点や盲点をついて入手する手法）について理解し、安易にID・パスワードや個人情報等を外部提供しないようにしているか（本人確認やリンク先やメールアドレスの再確認等をした上で回答する等）	
6	見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意しているか（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）	
7	メール送信前にメール送信確認画面を再度表示し確認したり、メールの遅延送信機能（送信ボタンを押しても、すぐに送信されず、任意の時間の経過後メール送信される機能。メール送信の取消等が可能となり、誤送信の防止に有用となる）等を活用し、メールの誤送信を防止しているか	
8	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護しているか なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと	
9	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関内の情報システム部門または担当者に確認したり、事前に情報システム部門より、対応方法の連絡がある場合は指示に従って処理をしているか	
10	患者の情報について目的外使用をしていないか	

チェックの結果

全体として医療機関のどの部分に弱みがあるのか把握し、優先的に必要な対策を実施の上、
全体のバランスを取りながらサイバーセキュリティ対策を強化するため、ご活用ください。

割合	項目数
0.0%	0/10

医療情報システムの安全管理に関するガイドライン　医療情報システム等の障害発生時の対応フローチャート



0 体制整備

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。

0-1　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取

【経営層・医療情報システム安全管理責任者(必要に応じて医療従事者・一般のシステム利用者も含む)】
情報セキュリティ事故が発生した場合に迅速に対応するための体制を整備する。

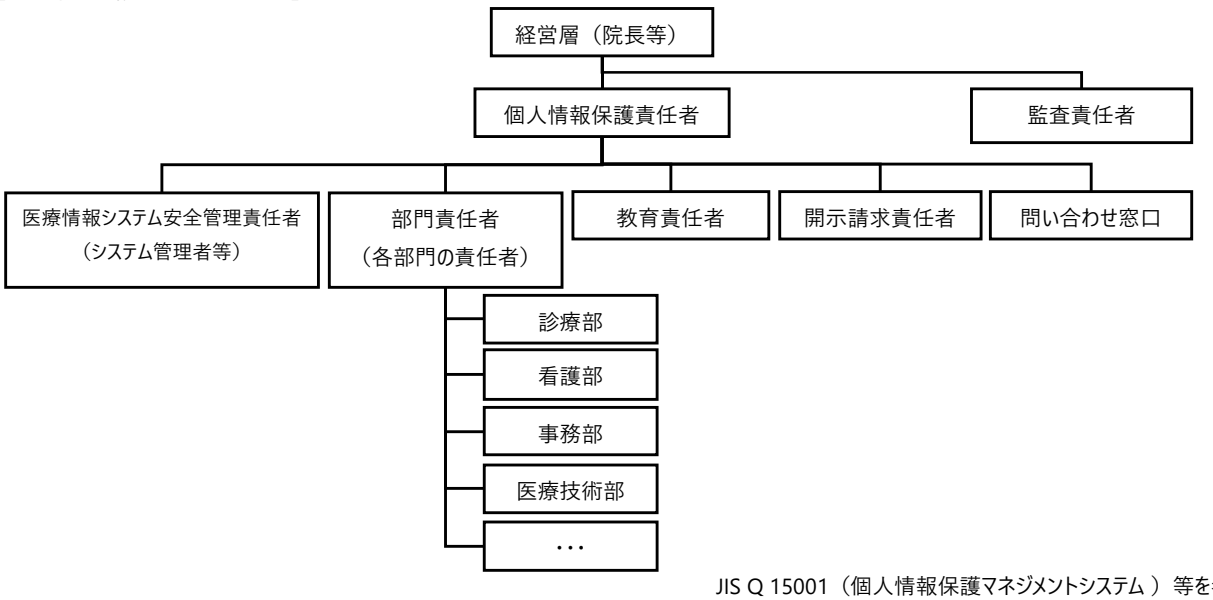
体制整備の例
・非常時において、誰が何をするのか役割や手順を定め、医療機関の内部や外部の医療情報システムのベンダ及びサービス事業者等との緊急の連絡先や情報伝達のルートを整備し、関係者へ周知する。
・非常時を想定した訓練等を実施し、決めた役割や手順通りに動けるかどうか定期的に確認する。
・所管官庁等や委託業者、医療情報システムのベンダ及びサービス事業者等の連絡先や担当窓口等をリスト等にまとめる。(システム等の使用が出来なくなることを想定し、メール以外の連絡手段についても確認してまとめる。)
・他の医療機関等でサイバー攻撃等の事象を発見した場合は、サイバー攻撃の原因や対応方法等に関する情報収集を行い、対策が必要な事項を院内で共有する。

また、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、情報セキュリティ責任者(CISO)等の設置や、緊急連絡体制(CSIRT等)を整備する。

【参考】体制整備の考え方

平時においては、個人情報保護の管理体制を整備し運用するが、サイバー攻撃を受けた時は、サイバーセキュリティ対策のために、医療機関の外部の組織も含めて、サイバーセキュリティの体制に移行することが重要である。

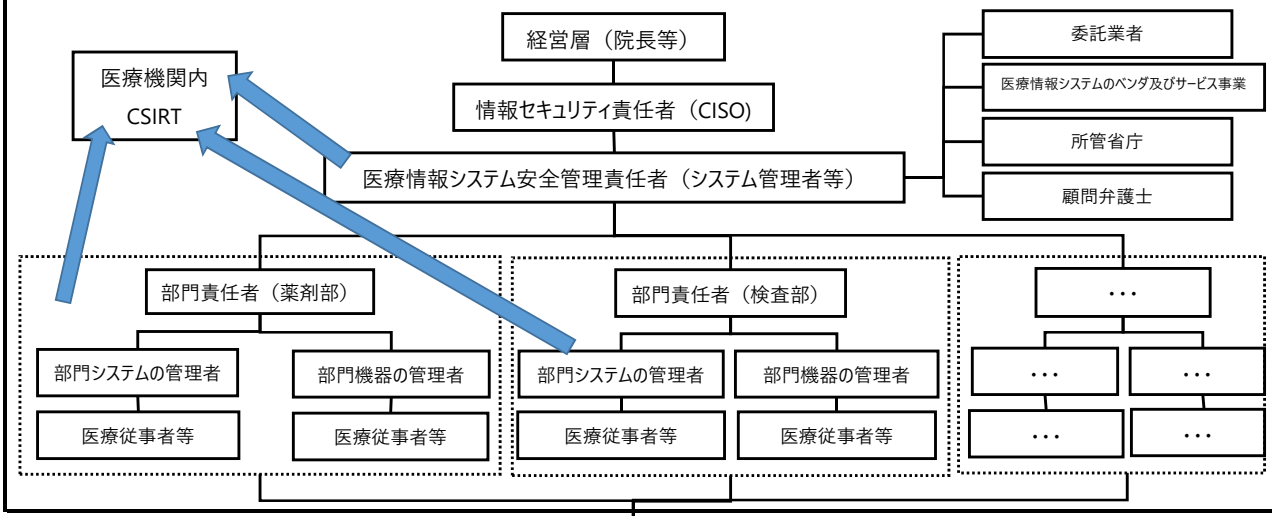
【個人情報保護の管理体制(例)】



JIS Q 15001（個人情報保護マネジメントシステム ）等を参考に作成

サイバー攻撃等の事案発生時は、サイバーセキュリティ体制

【サイバーセキュリティ体制図(例)】



（注）医療情報システムやネットワークの構成によって体制を適宜見直しする

0-2　ネットワーク構成図の作成

【医療情報システム安全管理責任者】
　サイバー攻撃等を受けた場合、自組織の現状を把握して対応するため、かつ医療情報システムのベンダ及びサービス事業者等に相談ができるように、医療機関におけるネットワークの状況を調査し、ネットワーク構成図を作成する。（ネットワーク構成図には、事務系のネットワークも含めるとともに、ネットワーク構成の変更がある都度、ネットワーク構成図の更新を実施する。）
　必要に応じて医療情報システムのベンダ及びサービス事業者等の協力を得ながら、ネットワーク構成図を作成するとともに、ネットワーク構成図を活用し、早期の異常を検知できるように、日常から医療情報システムの稼働状況や負荷状況、ネットワークの状況を監視し、把握しておくことや、侵入検知等の装置や体制を構築する。

【医療情報システムのベンダ及びサービス事業者等】
　医療機関からの協力依頼に基づき、ネットワーク構成図の作成の支援を実施する。

1　検知

医療情報システムや医療機器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安全管理責任者へ報告し、異常内容の事実確認を行う。

1-1　異常等の検知

【医療情報システム安全管理責任者】
医療情報システムや機器等の障害を監視し、異常等の検知を行う。（早期の異常を検知できるように、日常から医療情報システムの稼働状況や負荷状況、ネットワークの状況を監視し、把握しておくことや、侵入検知等の装置や体制を構築する。）

【医療従事者・一般のシステム利用者】
医療情報システムや機器等に障害等の異常を感じた場合、ウイルス感染の兆候（HPの改ざんや患者情報の暗号化、データの紛失・消去等）があるかどうか確認する。

【外部（医療情報システムのベンダ及びサービス事業者等・委託業者・所管省庁等）】
医療情報システムや機器等に障害等の異常が発生した場合は、異常内容、影響範囲、講じうる対応策等を調査する。

1-2　ケーブル等の切離

【医療従事者・一般のシステム利用者】
ウイルス感染の兆候（HPの改ざんや患者情報の暗号化、データの紛失・消去等）がある場合は、ケーブル等の切離を実施する。現場で判断が難しい場合は、不用意に電源停止等はしない。

1-3　医療情報システム安全管理責任者へ連絡

【医療従事者・一般のシステム利用者】
医療情報システム安全管理責任者へ異常の内容、発生日等について報告を実施する

【外部（医療情報システムのベンダ及びサービス事業者・委託業者・所管省庁等）】
保守ベンダー等の外部業者は、医療情報システムや機器等に障害等の異常を発見した場合は、医療情報システム安全管理責任者へ異常内容、影響範囲、講じうる対応策等を報告する。

1-4　医療情報システム安全管理責任者による確認

【医療情報システム安全管理責任者】
医療情報システム安全管理責任者は、医療従事者・一般のシステム利用者や外部業者等からの連絡に基づき、異常の事象について確認する

2 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。

2-1　原因調査

【医療情報システム安全管理責任者】
重大な障害がある場合、障害の原因がサイバー攻撃の兆候（HPの改ざんや患者情報の暗号化、データの紛失・消去、外部への通信量の増加、ウイルス対策ソフト等による検知等）があるかどうか、例えば医療情報システムのベンダ及びサービス事業者等によるメンテナンス等の問題なのか、医療情報システム自体の問題なのか、LAN設備やケーブルの問題なのか、設備の電源系統の問題なのか、調査を実施する。また情報漏えいや、情報持ち出しの有無についてもあわせて調査する。必要に応じて医療情報システムのベンダ及びサービス事業者等に協力依頼をして調査を進める。

【医療情報システムのベンダ及びサービス事業者等）】
医療機関からの依頼に基づき、障害の原因調査の支援を実施する。

（参考）兆候の検知や対応方法の例

・医療従事者等から不正メールの受信報告を受けた場合・・・類似メールの受信状況と反応した医療従事者等の把握をし、不正メールの受信停止設定を実施する。

・医療従事者等から不正メールに対応し、IDやパスワード等を入力してしまった報告を受けた場合・・・入力したIDやパスワードの変更と類似メールの受信状況や反応した医療従事者等の把握をし、不正メールの受信停止設定をする。

・医療従事者等より不正メールでウイルスのダウンロードをしてしまった報告を受けた場合・・・端末のネットワークの切断と、ネットワーク上の接続機器のチェックを実施する。類似メールの受信状況と反応した医療従事者等の把握をし、不正メールの受信停止設定を実施する。

・端末の停止や動作が遅い等の動作不良の状態になっている・・・ネットワークやサーバーの負荷状況を確認する。必要に応じて医療情報システムのベンダ及びサービス事業者等に協力依頼をする。

・端末のデータアクセスが不良となっている・・・端末、ネットワーク、サーバーの負荷状況を確認（機器の電源ランプの稼働時の点滅の確認、通信量のチェック、pingによる接続確認を実施する、HDDケーブルの不安定やネットワークループの発生の有無の確認等）を実施する。必要に応じて医療情報システムのベンダ及びサービス事業者等へ協力依頼を実施する。

2-2　医療情報システムのベンダ及びサービス事業者等へ確認

【医療情報システム安全管理責任者】
障害の前日等に、医療情報システムや医療機器等のメンテナンスの実施やデータ移行等の作業実施の有無を確認し、該当する場合は医療情報システムのベンダ及びサービス事業者等に、前日の作業が障害の原因となっていないかどうか確認する

2-3　ネットワーク機器やケーブル等の調査

【医療情報システム安全管理責任者】
医療機関内の他のサーバー等へのアクセスが可能かどうか調査し、ネットワーク機器やケーブル等の問題がどうか調査を実施し、対象の機器やケーブルの絞り込みをする。

2-4　電源系統、ブレーカー、ハードウェア等の調査

【医療情報システム安全管理責任者】
医療情報システムや機器等の起動ができるかどうか確認し、起動ができない場合は電源やブレーカ等の電源系統の確認や機器自体の故障、ハードウェア自体の故障の有無やアプリケーションの状況の調査等を実施する。

2-5　IPA等へ相談

【医療情報システム安全管理責任者】
サイバー攻撃の可能性について、コンピュータウイルスや不正アクセスに関する技術的な相談として、情報処理推進機構（IPA）情報セキュリティ安心相談窓口（03-5978-7509）等に相談する。

2-6　被害拡大防止

【医療情報システム安全管理責任者】
2－1による原因調査の結果、サイバー攻撃の兆候（HPの改ざんや患者情報の暗号化、データの紛失・消去、外部への通信量の増加、ウイルス対策ソフト等による検知等）がある場合は、被害拡大を防止するために、ネットワークの遮断等により通信を遮断し感染拡大を防止する。現場での判断が難しい場合は、不用意な電源停止は行わない。またバックアップ等のデータの退避を実施するとともに、重要な医療情報システム等へのアクセスログを収集する。医療機関内で対応が難しい場合は、医療情報システムのベンダ及びサービス事業者等に協力を依頼する。

（参考）被害拡大防止の例

・医療従事者等から不正メールの受信報告を受けた場合・・・類似メールの受信状況と反応した医療従事者等の把握をし、不正メールの受信停止設定を実施する。

・医療従事者等から不正メールに対応し、IDやパスワード等を入力してしまった報告を受けた場合・・・入力したIDやパスワードの変更と類似メールの受信状況や反応した医療従事者等の把握をし、不正メールの受信停止設定をする。

・医療従事者等より不正メールでウイルスのダウンロードをしてしまった報告を受けた場合・・・端末のネットワークの切断と、ネットワーク上の接続機器のチェックを実施する。類似メールの受信状況と反応した医療従事者等の把握をし、不正メールの受信停止設定を実施する。

・端末の停止や動作が遅い等の動作不良の状態になっている・・・ネットワークやサーバーの負荷状況を確認する。必要に応じて医療情報システムのベンダ及びサービス事業者等に協力依頼をする。

・端末のデータアクセスが不良となっている・・・端末、ネットワーク、サーバーの負荷状況を確認（機器の電源ランプの稼働時の点滅の確認、通信量のチェック、pingによる接続確認を実施する、HDDケーブルの不安定やネットワークループの発生の有無の確認等）を実施する。必要に応じて医療情報システムのベンダ及びサービス事業者等へ協力依頼を実施する。

2-7　報告と周知

【医療情報システム安全管理責任者】
サイバー攻撃の兆候がある場合は、経営層へ報告し、その後、医療従事者・一般のシステム利用者へ、感染の疑いがある医療情報システムや機器等の使用の中止を指示する。

2-8　経営層による確認・指示

【経営層】
医療情報システム安全管理責任者からサイバー攻撃を兆候について報告を受けた後、対応チームの組成の必要性を検討すると同時に、被害状況の調査等について医療情報システム安全管理責任者へ指示をする。

2-9　対応（使用停止等）

【医療従事者・一般のシステム利用者】
医療情報システム安全管理責任者の指示に従い、該当する医療情報システムや機器等の使用を停止する。（サイバー攻撃を受けたときを想定して事前に事業継続計画（非常時による紙カルテによる運用等）を立てて、医療従事者・一般のシステム利用者へ教育訓練しておくことが必要である。）

2-10　被害状況等調査

【医療情報システム安全管理責任者】
医療情報システムへの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（ウイルス感染等）の範囲、個人情報の漏洩の有無等について調査し、経営層へ報告を実施する。必要に応じて医療情報システムのベンダ及びサービス事業者等へ協力依頼して調査を進める。

報告事項の例
・異常が発見された日
・異常が発生している箇所や診療への影響
・今後の被害拡大の可能性
・攻撃元（判明する場合）
・攻撃手法（判明する場合）
・被害発生の要因
・講じうる対応策　等

【医療情報システムのベンダ及びサービス事業者等】
医療機関からの協力依頼に基づき、サイバー攻撃による被害状況の調査の支援を実施する。

2-11　被害状況の報告

【医療情報システム安全管理責任者】
経営層へ被害状況の調査結果について報告する。

2-12　方針指示

【経営層】
医療情報システム安全管理責任者から被害状況の報告（診療継続への影響や個人情報や機密情報等の漏えいの有無等）を受け、対応方針（厚生労働省への報告【2－13】、所轄の地方公共団体や個人情報保護委員会への報告【4－3】、法的措置や証拠保全等）について指示をする。（必要に応じて顧問弁護士や医療情報システムのベンダ及びサービス事業者等へ相談する）法的措置の検討に時間を要する場合は、証拠保全や復旧対応を同時に進める。

2-13　厚生労働省へ報告

【経営層】
医療情報システムがサイバー攻撃(サイバー攻撃の可能性を含む)を受けた場合や、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る場合は、厚生労働省医政局研究開発振興課医療情報技術推進室へ連絡する。

2-14　証拠保全の実施

【医療情報システム安全管理責任者】
自院及び委託業者で証拠保全が実施可能か検討し、困難な場合は医療情報システムのベンダ及びサービス事業者等へ依頼する。（日常から複数の医療情報システムのベンダ及びサービス事業者等と危機対応についてコミュニケーションを取っておく。）

2-15　医療情報システムのベンダ及びサービス事業者等への依頼

【医療情報システム安全管理責任者】
証拠保全を依頼した医療情報システムのベンダ及びサービス事業者等から証拠保全の結果やサイバー攻撃元や手法等の報告をうける。また復旧に向けて、具体的な復旧作業や手順、コストの整理を実施する。

2-16　実施結果の報告（証拠保全及び復旧計画）

【医療情報システム安全管理責任者】
経営層へ証拠保全の結果や復旧に向けた計画や工数、費用等について報告を実施する。復旧に時間がかかる可能性がある場合は、紙運用の実施も含めて検討する。

2-17　経営層による確認

【経営層】
医療情報システム安全管理責任者から証拠保全の結果や復旧に向けた計画、必要工数や費用等について確認する。

2-18　警察への届出

【経営層】
被害状況について警察へ届出をする

3 復旧処理

復旧計画に基づいて、医療情報システムのベンダ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。

3-1　復旧指示

【経営層】
復旧に向けた計画、工数、費用等を踏まえて、復旧指示を実施する。必要に応じて予算の手当を実施する。

3-2　医療情報システムのベンダ及びサービス事業者等へ依頼

【医療情報システム安全管理責任者】
自院で復旧が困難な場合は、医療情報システムのベンダ及びサービス事業者等に協力を依頼する。（日常から複数の医療情報システムのベンダ及びサービス事業者と危機対応についてコミュニケーションを取っておく）

3-3　再設定や再インストール、バックアップデータのリストア等

【医療情報システム安全管理責任者】
（医療情報システムのベンダ及びサービス事業者等に）状況を確認し、バックアップを実施する。次にウイルス感染等の場合は、（医療情報システムのベンダ及びサービス事業者等の協力を得て、）可能であればクリーンインストールを実施する。ソフトウェアに問題が生じている場合は、設定変更や再インストールで解決するかどうか（医療情報システムのベンダ及びサービス事業者等へ）確認する。
再インストール後に、ソフトウェアのアップデートやバックアップデータのリストアが必要な場合は実施する。

3-4　復旧結果の確認

【医療情報システム安全管理責任者】
復旧処理について、医療情報システムや機器等が正常に稼働するかどうか確認を実施する。正常に稼働することが確認できたら、医療従事者・一般のシステム利用者へ復旧できたことを連絡する。

4 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。

4-1　復旧結果と情報漏えい事実の有無の報告

【医療情報システム安全管理責任者】
復旧結果について、経営層へ報告する。異常の内容、原因、被害状況、復旧にかかった工数や費用等について報告する。また情報漏えいの事実の有無や範囲について経営層へ報告する。

4-2　確認・再発防止指示

【経営層】
医療情報システム安全管理責任者からの報告を受けて、再発防止策の検討を指示する。

4-3　所轄の地方公共団体や個人情報保護委員会等へ報告

【経営層】
個人情報の漏えい、滅失又は毀損等のおそれがある場合は個人情報保護委員会や所轄の地方公共団体等へ速やかに報告を実施する。

4-4　法律専門家（弁護士）へ相談

【経営層】
法的措置について弁護士等の法律専門家に相談する。証拠保全の結果も踏まえて検討を進める。検討に時間がかかる場合は、再発防止の取組を先に進める。

4-5　再発防止策の検討

【医療情報システム安全管理責任者】
経営層や対応チームのメンバーを交えて、再発防止策の検討や必要となる費用の検討を実施する。

4-6　再発防止策の周知

【医療情報システム安全管理責任者】
検討した再発防止策について、医療従事者・一般のシステム利用者へその内容を周知するとともに、適宜説明等により教育する。

4-7　再発防止策の実施

【医療従事者・一般のシステム利用者】
医療情報システム安全管理責任者から周知された再発防止策について、日常の業務への落とし込みを実施するともに、定期的にチェックをする。

4-8　医療情報システムのベンダ及びサービス事業者等の委託業者への再発防止策の指示

【医療情報システム安全管理責任者】
検討した再発防止策について、医療情報システムのベンダ及びサービス事業者等の委託業者へその内容を周知するとともに、委託業務への反映を指示する。定期的に委託業者の業務をチェックし、指示した再発防止策が実施できているかどうか確認する。

4-9　情報公開の検討

【経営層】
サイバー攻撃の影響や被害状況や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。