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

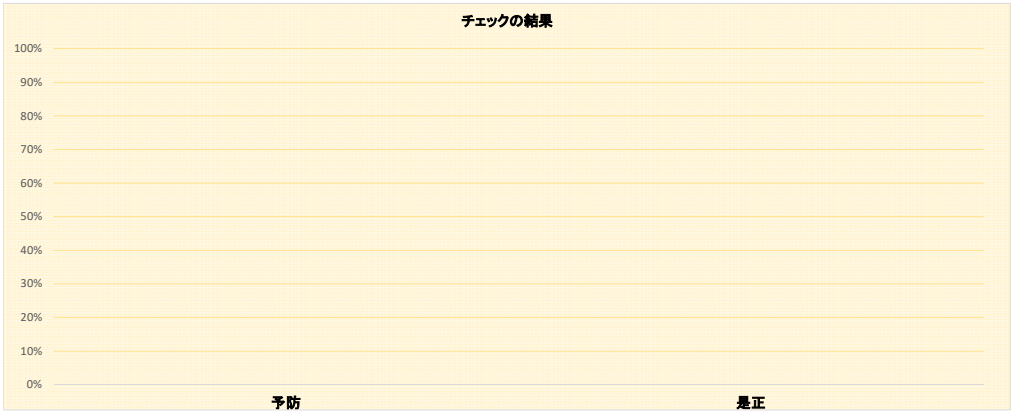
NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口	
2	予防	運用管理規程等において次の内容を定めているか ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 端末等を用いて外部から医療機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

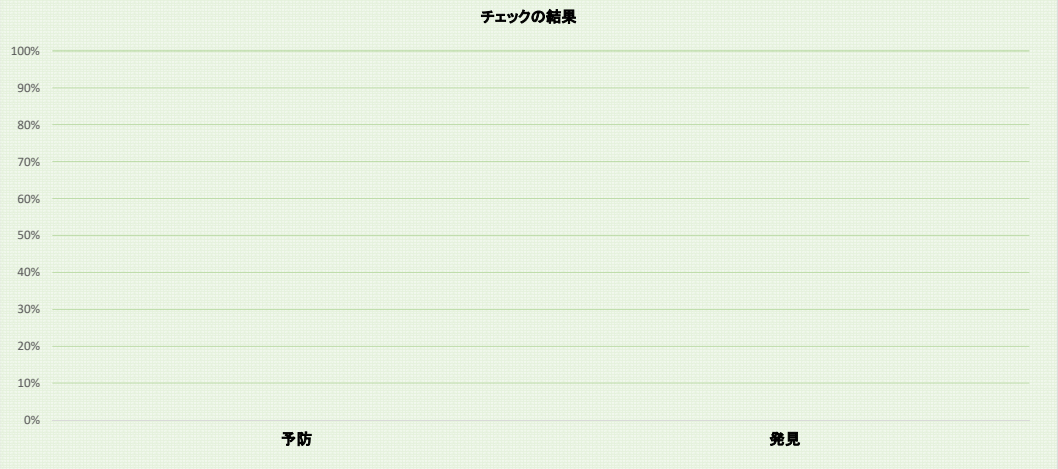
NO	視点	チェック項目	チェック欄（○or×）
1	予防	ネットワークの接続方式については、実施機関が別途認めたサービス事業者によるクローズドな接続方式とするとともに、医療機関等、審査支払機関、医療保険者等及び実施機関間を相互に接続するネットワーク回線において、許可されていない者による盗聴及び漏えいに対する機密性を確保する機能を有しているか	
2	発見	デジタル署名付きデータの送付と受領確認データの返送を確認及びデータの送付に関する受領確認データの相互送信、送信ログ及び受信ログの保管をしているか	

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