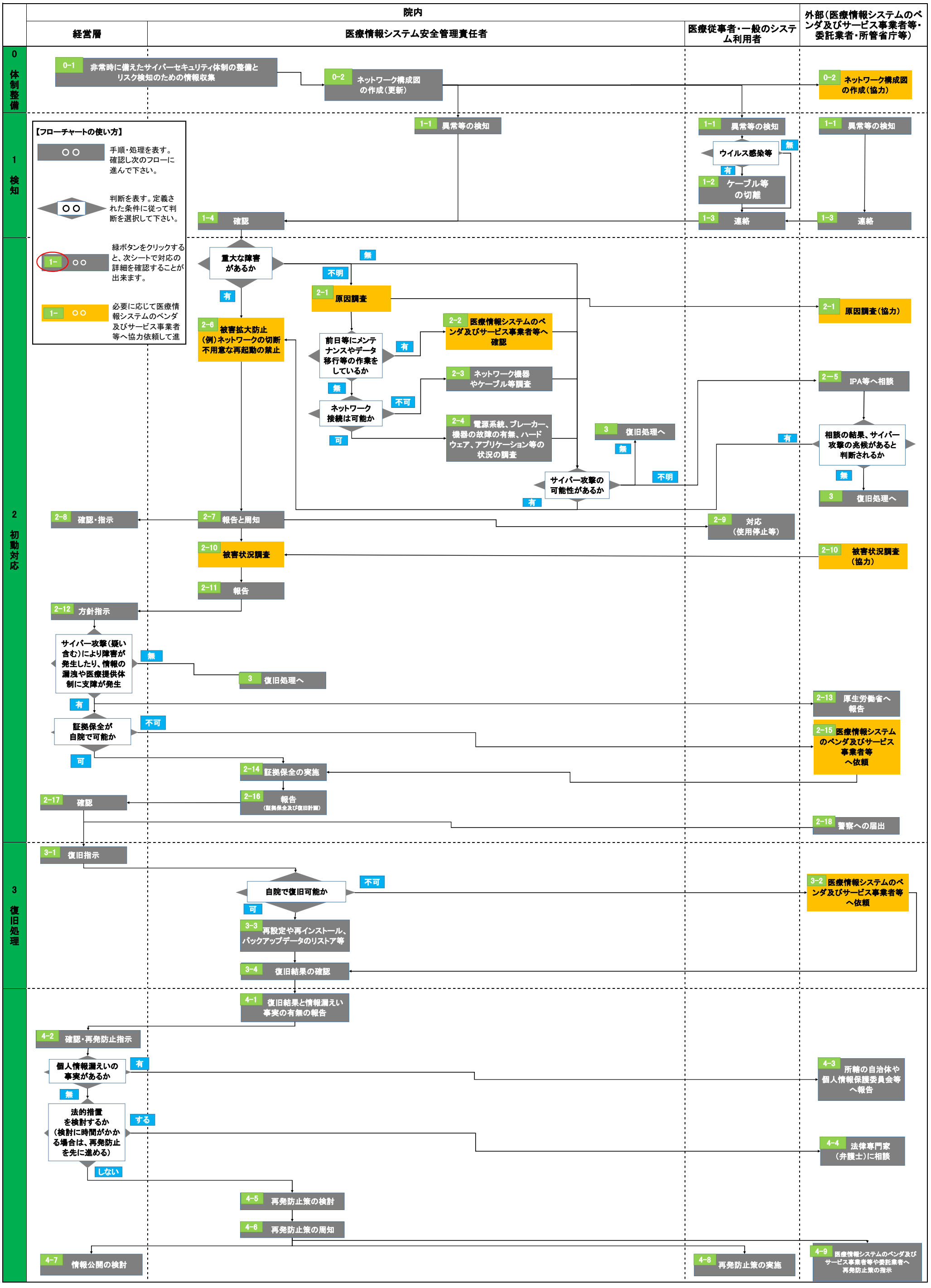
医療情報システムの安全管理に関するガイドライン　医療情報システム等の障害発生時の対応フローチャート



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。

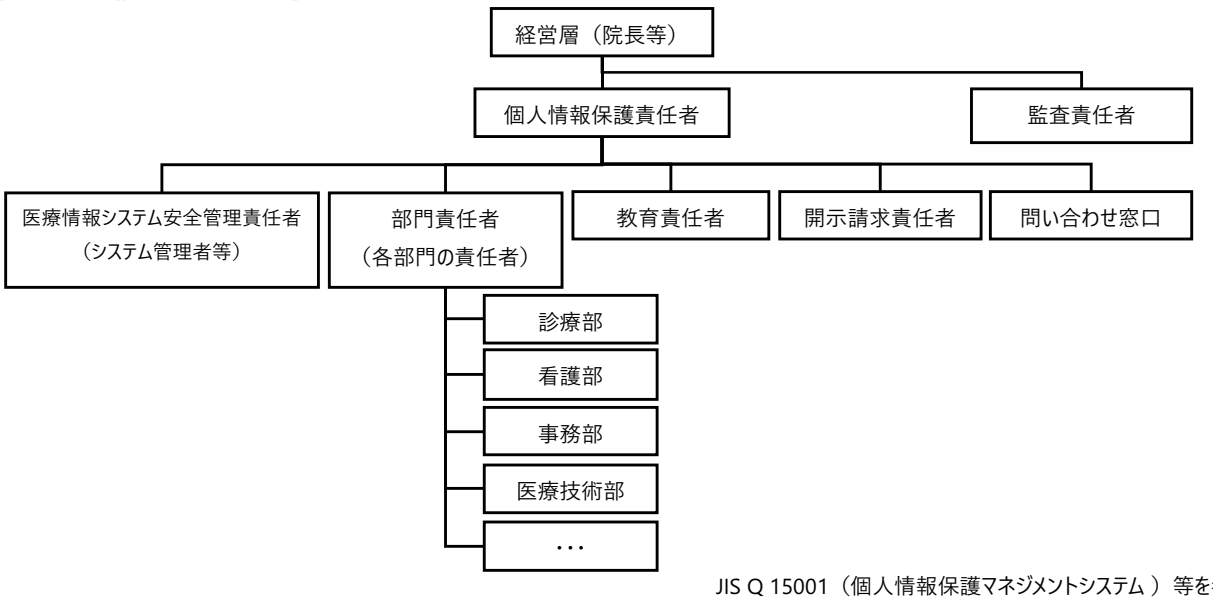
体制整備の例
・非常時において、誰が何をするのか役割や手順を定め、医療機関の内部や外部の医療情報システムのベンダ及びサービス事業者等との緊急の連絡先や情報伝達のルートを整備し、関係者へ周知する。
・非常時を想定した訓練等を実施し、決めた役割や手順通りに動けるかどうか定期的に確認する。
・所管官庁等や委託業者、医療情報システムのベンダ及びサービス事業者等の連絡先や担当窓口等をリスト等にまとめる。(システム等の使用が出来なくなることを想定し、メール以外の連絡手段についても確認してまとめる。)
・他の医療機関等でサイバー攻撃等の事象を発見した場合は、サイバー攻撃の原因や対応方法等に関する情報収集を行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

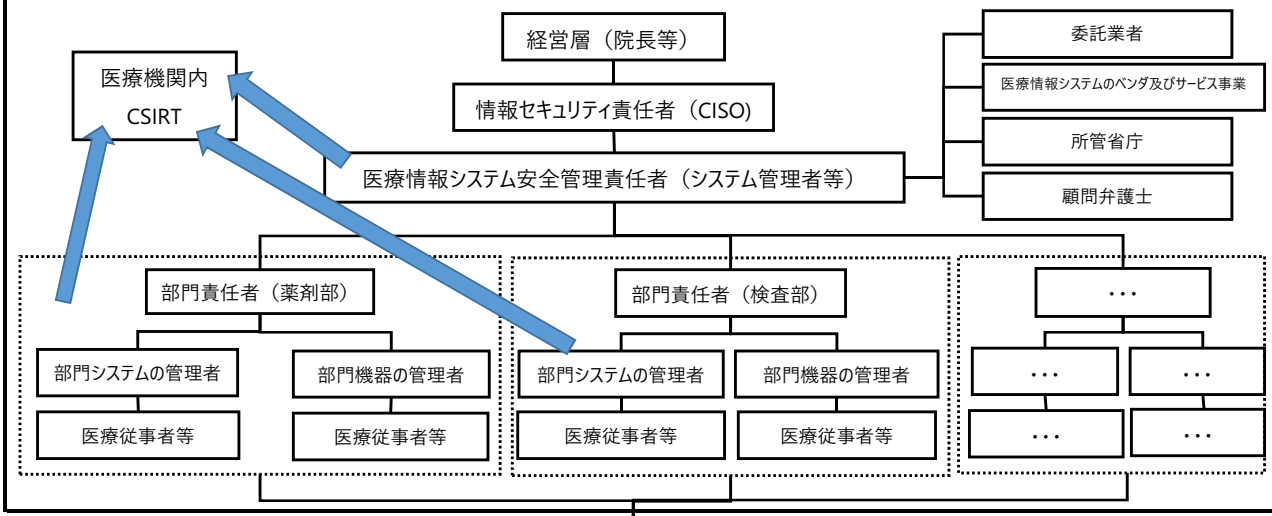
【個人情報保護の管理体制(例)】



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。