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。	