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（報告用）
（医療機関確認用）

サイバーセキュリティを確保するための対策等が適切に実施されているかを点検するためのチェックリストです。
自己点検欄に、次の区分で該当する記号を記入してください。
（チェックリスト記入要領）
記号 摘要
○ 適正に実施している。
× 不適：一部は実施しているが、不十分な場合を含む。
－ 該当なし（2（2）、2（3）及び（7）で確認不要であるとき以外に使用することは不可。）

・×が付いた項目については、目標日を記入してください。
・「医療機関確認用」は「事業者確認用」の結果を踏まえて、医療機関全体の状況を報告するものであるため、医療情報システムが導入されている場合は、すべての項目に○か×を記入する必要があります。（2（2）及び2（3）で確認不要である場合を除く。）
・医療機関が事業者と契約していなければ「事業者確認用」は不要です。
・(7)セキュリティパッチの適用について、導入システムにより確認が難しい等の場合は、「-」該当無とし、その旨理由を添えてください。
また、システム上、セキュリティパッチ以外の方法でセキュリティ確保をしている場合も「-」該当無とし、どのような方法・理由であるかを添えてください。
・各項目の考え方や確認方法については、「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～」をご覧ください。

参考　厚生労働省ホームページ（医療分野のサイバーセキュリティ対策について）
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

	番号	チェック項目	自己点検	目標日（例:R7.3.31）	調査結果	備考・参考
医療情報システムを導入、運用している。（はい：○、いいえ：×）（「いいえ」の場合、以下のすべての項目は確認不要）						
1 体制構築						
	(1)	医療情報システム安全管理責任者を設置している。				
2 医療情報システムの管理・運用						
	A	医療情報システム全般について、以下を実施している。				
	(1)	サーバ、端末PC、ネットワーク機器の台帳管理を行っている。				
	(2)	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。（事業者と契約していない場合は不要。）				
	(3)	事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。（事業者と契約していない場合は不要。）				
	B	サーバについて、以下を実施している。				
	(4)	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。				
	(5)	退職者や使用していないアカウント等、不要なアカウントを削除している。				
	(6)	アクセスログを管理している。				
	※(7)	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。				
	※(9)	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。				
	C	ネットワーク機器について、以下を実施している。				
	(7)	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。				
	(8)	接続元制限を実施している。				
	D	端末PCについて、以下を実施している。				
	※(4)	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。				
	※(5)	退職者や使用していないアカウント等、不要なアカウントを削除している。				
	※(7)	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。				
	※(9)	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。				
3 インシデント発生に備えた対応						
	(1)	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）への連絡体制図がある。				
	※(2)	インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。				
	※(3)	サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。				

医療機関名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

名古屋市