資料２－３

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

第16回　健康・医療・介護情報利活用検討会

医療等情報利活用ワーキンググループ

2023（令和５）年３月23日

サイバーセキュリティの確認のためのチェックリスト

医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

サイバーセキュリティの確認のための

【医療機関において確認する項目】

大項目	項番	チェック項目	
1 体制構築	1－1	医療機関に医療情報システム安全管理責任者を配置している。	
2 情報システムの管理	2－1	医療機関において、以下について把握している。	
		①	医療機関で用いる端末の一覧
		②	医療機関で用いるネットワーク機器の一覧
		③	医療機関で用いる記録媒体の一覧
		④	医療機関で用いるサーバーの一覧
	2－2	職員の私物や事業者所有の機器等について、診療に関する業務で使用する場合の許可や管理体制が明確になっている。	
	2－3	医療機関は、既に報告されている脆弱性について、事業者から最新の安全性に関する確認結果の報告を受けている。	
3 情報システムの運用	3－1	退職者のアカウント等、不要なアカウントを削除する管理体制ができている。	
	3－2	利用者の職種・担当業務別の情報区分ごとのアクセス管理機能がある。	
	3－3	ネットワーク機器（※）に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。 （※）VPN機器を含むインターネットとの接続を制御するルータ。	
	3－4	サーバーでアクセス記録（アクセスログ）の管理をしている。	
	3－5	ネットワーク機器にアクセス制限を実施している。	
4 インシデント発生時の対応	4－1	サイバー攻撃を受ける等システムに重大な障害が発生したことを想定した事業継続計画（BCP）を策定済み、又は、令和５年度中に策定予定である。	
	4－2	インシデント発生時に備えて、組織内連絡体制と外部関係機関（事業者、厚生労働省及び警察等）への連絡体制を整えている。	
	4－3	医療機関において、診療継続の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。	

【事業者において確認する項目】

大項目	項番	チェック項目
1 体制構築	1－1	事業者内に、医療情報システムの管理責任者がいる。
2 情報システムの管理	2－1	事業者は、提供するソフトウェア・機器等の脆弱性に関して、医療機関への導入時、以降適時、求められる安全性に関する状況（初期PWの変更、脆弱性の更新状況）を確認し、医療機関にその結果を報告し、対応している。
3 情報システムの運用	3－1	ネットワーク機器（※）に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。 （※）VPN機器を含むインターネットとの接続を制御するルータ。
	3－2	サーバーでアクセス記録（アクセスログ）の管理をしている。
	3－3	ネットワーク機器にアクセス制限を実施している。
4 インシデント発生時の対応	4－1	事業者は、インシデント発生時、事前に明確化している責任分界点に応じて対応できる体制を整えている。
	4－2	事業者は、バックアップについての保管及び取り扱いについて、医療機関に取り扱い説明書等の文書として提供している。