（別紙）

医療機関におけるサイバーセキュリティ確保事業について

１　目的

医療機関の医療情報システムへのサイバー攻撃による診療の休止等を防ぐため、サイバーセキュリティ対策を強化すること。

２　事業の概要

(1) 外部ネットワークとの接続の安全性の検証・検査

厚生労働省が契約するシステム業者（以下、システム業者という。）が、実施対象となった病院にヒアリングや現地訪問を行って、外部ネットワークとの接続点の洗い出しや設置状況、機器情報（設定情報を含む）等の確認を行います。

(2) オフライン・バックアップ体制の整備

ランサムウェア[*1]対策としては、オフライン・バックアップ[*2]（ネットワークとの接続しない状態でバックアップを取ること）が有効であるため、医療機関のネットワークシステムに合わせたバックアップ体制の整備を行います。

[*1] ファイルを暗号化することで利用不可能な状態にした上で、そのファイルを元に戻すことと引き換えに金銭を要求する悪意のあるソフトウェアのこと

[*2] ネットワークとの接続しない状態でバックアップを取ること

３　事業の流れ

(1) 実施医療機関の選定

今回の照会の結果等を元に、対象となる病院を県から厚生労働省に報告します。

病院におかれましては、**令和６年３月８日（金）までに**照会に御回答くださるようお願いします。

(2) 事業の実施

令和６年６月頃より、システム業者より、対象となった病院に直接連絡がありますので、日程調整等を行いながら進めることとなります。

実施にあたり、医療情報システム一覧やネットワーク構成図等、事前質問票への回答等が求められますので、システム業者の依頼に従って御対応をお願いします。

４　その他

- 上記２（1）及び（2）の実施に係る費用（システム業者への委託料）は無料です。ただし、バックアップに係る媒体（クラウドサービスを含む）やソフトウェアに係る費用（40 万円程度と推計）は病院の負担となります。
- 具体的なオフライン・バックアップの方法等はシステムの状況や費用等を勘案し、システム業者とご相談いただきながら進めていただくことが可能です。
- 上記２（1）及び（2）を併せて実施することが推奨されていますが、（1）のみ実施することも可能です。システム業者とご相談ください。

※　厚生労働省医政局作成「医療機関におけるサイバーセキュリティ確保事業について」にはスキーム図等が掲載されていますので、併せて御確認ください。