医療機関におけるサイバーセキュリティの義務化

厚生労働省は、医療機関の管理者に対して、2023 年 4 月 1 日からサイバーセキュリティの確保を義務付けました。医療機関がサイバー攻撃を受けると、患者情報の漏えいやシステム障害だけでなく、診療そのものが停止して地域医療にも大きな影響が及ぶため、サイバーセキュリティ確保が義務化されました。特に、ランサムウェア攻撃や個人情報の流出が問題となっています。

サイバーセキュリティ管理者の設置

病院や診療所の管理者は、医療の提供に著しい支障を及ぼす恐れがないよう、サイバーセキュリティを確保するために必要な措置を講じることが求められています。特に 200 床以上の病院に対しては、専任の管理責任者の配置が必要です。

セキュリティ対策の実施

ウイルス対策ソフトの購入や定期的なシステム更新、不正アクセス対策（ファイアーウォールや侵入検知システムの導入）など、多層防御の考え方を導入する事が求められます。

インシデント対応計画の策定

サイバー攻撃を受けた際の対応マニュアルの作成やバックアップデータの管理、復旧手順の確立が重要視されています。

従業員のセキュリティ教育

フィッシング詐欺や標準型攻撃への対策講習の実施など、従業員への継続的な教育が推奨されています。

- ☐ パスワードを強固なものに変更し、使い回しをしない
- ☐ IoT 機器を含む情報資産の通信制御を確認する 医療機関等のネットワークについて、通信網を正確に把握し、適切に対策が講じられているか、ご確認ください
- ☐ ネットワーク機器の脆弱性に、ファームウェア等の更新を迅速に適用する

医療機関等がサイバー攻撃を受けた際は速やかに厚生労働省に報告を

医療機関等がサイバーインシデント（サイバー攻撃やその疑いを含む）を受けた場合、
以下の連絡先へ、インシデント発生後速やかにご連絡ください。

医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先：医政局・医療情報担当参事官室

TEL: 03-6812-7837

MAIL: igishitsu@mhlw.go.jp

医療機関は、これらの義務化された対策を遵守し、患者の安全と信頼を守るための取り組みを強化する事が求められています。

詳しくはこちらをご確認ください：厚生労働省　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