事務連絡
令和８年５月 27 日

各都道府県衛生主管部（局） 御中

厚生労働省医政局医療情報担当参事官室

高性能 AI の悪用リスクを踏まえたサイバーセキュリティ対策の強化について
（医療機関等向け注意喚起）

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピードや規模が劇的に増大するなど、サイバーセキュリティにおける新たな脅威に直面しています。

特に医療分野は、国民の生命・健康を支える重要インフラの一つであり、その機能が停止又は低下した場合には、診療の継続性に重大な支障が生じ、国民生活に深刻な影響を及ぼすおそれがあることから、サイバーセキュリティ対策の一層の強化が求められています。

とりわけ、本年４月に米国 Anthropic 社が公表した Claude Mythos Preview をはじめとするフロンティア AI モデルにより、脆弱性の発見・修正等のサイバーセキュリティ性能が急速に向上していることを踏まえ、こうした技術進展に対応した備えが不可欠です。医療機関においても、電子カルテや医療機器、院内ネットワーク等を含む重要システムの安全性確保の観点から、これらの動向を十分に考慮した対策が必要となります。

こうした状況を踏まえ、内閣官房国家サイバー統括室等より 2026 年５月 18 日付けで発出された「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について （重要インフラ事業者等に対する注意喚起)」（別添１）に基づき、医療機関におけるサイバーセキュリティ対策の重点事項を改めてまとめましたので、管内、管下の医療機関に対し、下記の対策が適切に講じられているか確認を要請するとともに、経営層のリーダーシップの下、医療を担う重要インフラ事業者としての責務を踏まえ、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策を実施するよう注意喚起をお願いします。

医療機関におけるサイバーセキュリティ対策の重点事項

内閣官房国家サイバー統括室等より 2026 年５月 18 日付けで発出された「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について （重要インフラ事業者等に対する注意喚起)」（別添１）においては、
「１．経営層のリーダーシップの下でのサイバーセキュリティ対策」
「２．基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化」
「３．高性能 AI による高速化する脆弱性の発見・修正等への対応」
が強調されております。

これを踏まえ、「医療情報システムの安全管理に関するガイドライン」（参考）の内容を要約し、医療機関等の皆様に改めて優先的にご確認いただきたい事項を以下に整理しましたので、ご参照ください。

1. 経営層の関与とガバナンスの強化

- サイバーセキュリティを経営課題として位置づけ、経営層が主体的に関与すること
- セキュリティ責任者や体制を明確化し、組織的な管理体制を整備すること
- インシデント発生時の意思決定体制・連絡系統を事前に確立すること

2. 医療情報システムの適切なリスク管理

- 電子カルテ、医療機器、院内ネットワーク等の重要システムの把握とリスク評価の実施
- ネットワーク分離やアクセス制御など、システムの重要度に応じた防御対策の導入
- 外部委託・クラウド利用時の責任分担や契約条件の明確化

3. 脆弱性対策と資産管理の徹底

- ソフトウェア・機器の資産管理（棚卸し）を継続的に実施
- セキュリティパッチの適用やアップデートを迅速に行い、既知の脆弱性への対応を遅滞なく実施
- サポートが終了した機器の使用見直し

4. ランサムウェア対策の強化

- バックアップの取得・保管（オフラインを含む）と復旧訓練の実施
- 不審メールや添付ファイルへの対応など、基本的な対策の徹底
- ネットワーク異常や感染兆候の早期検知体制の整備

5. インシデント対応体制の整備

- インシデント発生時の初動対応手順（封じ込め・影響範囲確認等）を明確化
- 厚生労働省、関係機関、ベンダ等への報告・連携体制の確保
- 事後的な原因分析と再発防止策の継続的実施

【医療機関等がサイバー攻撃を受けた場合等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　「×」を「@」に置き換えてください。

※迷惑メール防止のため、メールアドレスの一部を変えています。

6. 人的対策（教育・訓練）の徹底

- 全職員に対する定期的なセキュリティ教育・注意喚起の実施
- フィッシング対策や標的型攻撃を想定した訓練の実施
- 医療従事者と情報部門の連携強化

7. サプライチェーン・医療機器対策

- 医療機器メーカーやベンダとの連携によるセキュリティ情報の共有
- 調達段階からのセキュリティ要件の確認・担保
- 機器の更新・保守におけるセキュリティ対応の徹底

8. 事業継続（BCP）と診療継続体制の確保

- サイバー攻撃を想定した業務継続計画（BCP）の策定・見直し
- システム停止時でも診療を継続するための代替手段（紙運用等）の確保
- 定期的な訓練による実効性の向上

これらの内容を踏まえ、最低限の遵守事項をリスト化したものが、「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」（別添２）です。まずは、本チェックリストを満たしているかをご確認いただき、各医療機関におけるサイバーセキュリティ対策を改めて見直す機会としていただきますようお願いいたします。

（別添１）

・内閣官房国会サイバー統括室・内閣府政策統括官（経済安全保障担当）・警察庁・金融庁・総務省・厚生労働省・経済産業省・国土交通省・防衛省「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフ事業者等に対する注意喚起)」（2026 年５月 18 日）
https://www.mhlw.go.jp/content/10808000/001701517.pdf

（別添２）

・（医療機関確認用）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
（医療機関確認用）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

・（事業者確認用）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
（事業者確認用）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

（参考）

医療情報システムの安全管理に関するガイドラインは、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とともに厚生労働省ホームページにおいて掲載されていますので、ご参照ください。

医療情報システムの安全管理に関するガイドライン　第 6.0 版（令和５年５月）｜厚生労働省

・　医療情報システムの安全管理に関するガイドライン第 6.0 版（概説編）
https://www.mhlw.go.jp/content/10808000/001102570.pdf

・　医療情報システムの安全管理に関するガイドライン第 6.0 版（経営管理編）
https://www.mhlw.go.jp/content/10808000/001102573.pdf

・　医療情報システムの安全管理に関するガイドライン第 6.0 版（企画管理編）
https://www.mhlw.go.jp/content/10808000/001102575.pdf

・　医療情報システムの安全管理に関するガイドライン第 6.0 版（システム運用編）
https://www.mhlw.go.jp/content/10808000/001582980.pdf

・　令和７年度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
https://www.mhlw.go.jp/content/10808000/001490741.pdf