不正アクセスによる漏えい等の事案を踏まえた対応について

２０２６年１０月９日
内閣官房国家サイバー統括室

国家サイバー統括室では、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害、堅牢さを欠くデータ管理などにより、大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案を複数確認しております。

こうした状況を踏まえ、特に、大量の個人情報を取り扱う事業者や機微な情報を取り扱う事業者等におかれましては、以下にお示しする主な対策のポイントをご参照いただき、より一層の対策の徹底を速やかに検討いただくようお願いいたします。

１．ウェブシステム等の適切な管理

ウェブシステムは、企業活動や顧客サービスの基盤として不可欠な存在となっています。一方で、インターネットに公開されているシステムは特に攻撃の対象となりやすいため、「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。

（１）脆弱性の適切な管理

脆弱性情報が公表されると、攻撃者は短期間のうちに悪用を開始する場合があります。修正プログラムの適用を後回しにせず、インターネットに公開されていない内部のサーバ等も含め、リスクを適切に判断し、計画的かつ迅速に対応することが求められます。

- OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する
- サポートが終了している製品・バージョンを利用しない
- 利用していないシステムや機能は停止・削除する
- 定期的に脆弱性診断等を実施する
- 不要なポート、プロトコル、サービス等を無効化する

（２）アカウント管理・認証

適切な認証対策により、不正アクセスのリスクを大幅に低減させることが可能です。

- 多要素認証（MFA）を導入する
- 推測されやすいパスワードの使用を禁止する
- 管理者アカウントの利用者、アクセス権を必要最小限にする
- 退職者、異動者や利用されていないもの等の不要なアカウントを速やかに無効化する

（3）レジリエンスの向上

侵入を完全に防ぐことは困難です。不審な挙動の早期発見と迅速な対応が被害発生及び拡大の防止につながります。

・ログを適切に取得・保管する
・不審な通信や大量のアクセスを監視する
・侵入検知・防御システムを活用し、パターンファイル等を定期的に更新する
・外部からの異常な認証試行を把握する
・事業継続計画等にサイバーセキュリティを組み入れる
・インシデントが起きた場合の対応態勢を整備する

2．サプライチェーンを通じた侵害への対策

サイバー攻撃への対策は、自社システムのみを対象として考えるのではなく、個人情報や業務情報を預ける委託先企業等を含むサプライチェーン全体で安全性を確保する観点で取り組むことが重要です。攻撃者は、比較的防御が弱い委託先企業等を足掛かりとして侵入し、その後、標的となる企業へアクセスを拡大する手口を用いることがあります。そのため、「委託先企業と共に管理する」という認識の下で、適切な安全管理措置を講じることが求められます。

（1）委託先企業等のセキュリティ対策状況の把握

・委託先等の情報セキュリティ方針、管理体制や委託先等との役割分担・責任分界を確認する
・個人情報や業務情報の取扱状況を定期的に点検する
・セキュリティ認証の取得状況や監査結果を確認する
・再委託先を含む管理状況を把握する
・契約締結時だけでなく、継続的に確認を行う

（2）委託契約におけるセキュリティ要件の明確化

・情報の取扱方法を明確に定める
・アクセス権管理やログ管理の実施を求める
・不正アクセスや漏えいが発生した場合の報告義務を規定する
・インシデント発生時の委託先との連携体制を整備する

（3）情報共有範囲の適正化

・委託先へ提供する個人情報や業務情報を必要最小限とする
・業務終了後の委託先でのデータ削除を徹底する
・委託先に付与するアクセス権を適切に管理する

（4）サプライチェーン全体のリスクマネジメント

・重要な取引先や委託先を洗い出す
・サプライチェーンを含めた情報資産の流れを可視化する
・サプライチェーン上の重要な依存関係を把握する
・定期的にリスク評価を実施する

3．データの適切な管理

企業が保有する個人情報や業務情報は、重要な経営資産です。一方で、不必要な情報の保有や、アクセス権限の管理や保管方法が不十分である場合には、不正アクセスを受けた際に被害が大規模化するおそれがあります。また、近年の攻撃者は、窃取した情報を公開すると脅迫したり、不正に売買するなど、情報そのものを標的とする傾向を強めています。そのため、「保有する情報資産を守る」という視点に立った安全管理措置が求められております。

（1）保有する情報資産の適切な管理

どのような情報資産を保有しているのか把握できていなければ、適切な保護措置を講じることはできません。まずは、自社が保有する情報資産の全体像を把握することが重要です。

・個人情報や業務情報の所在や管理者を把握する
・重要な情報資産を分類し、管理対象を明確にする
・利用目的や保存期間を明確にする
・定期的に情報資産の棚卸しを実施する

（2）保有情報の最小化

万が一情報漏えいが発生した場合でも、保有する情報が少なければ被害の拡大を抑えることが可能です。

・利用目的を終えた情報は速やかに削除する
・法令上の保存期間を経過した情報は適切に廃棄する

（3）適切なアカウント管理・アクセス制御

必要以上の権限が付与されている場合、不正アクセス時に大量の情報が一度に取得されるおそれがあります。

・業務上必要な者のみにアクセスを許可する
・閲覧権限と更新権限を適切に分離する
・管理者権限の付与を必要最小限とする
・定期的にアカウントや権限設定を確認する

（4）データ保護の徹底

情報が窃取された場合であっても、適切な保護措置が講じられていれば悪用のリスクを低減することができます。

・保存データを暗号化する
・通信経路を暗号化する
・パスワードや認証情報を平文で保存しない
・外部電磁的記録媒体の利用やデータ保存等に関するルールを整備する
・バックアップデータについても適切に保護する
・クラウドサービスを利用する場合は、サービス仕様を理解し、保存領域やデータベース等の公開設定及びアクセス権限設定をよく確認する

（５）ログ取得・監視・分析の強化

不正アクセスを早期に発見し、被害範囲を迅速に特定するためには、適切な監視・分析体制が不可欠です。また、不正侵入される事案が複数確認されている状況に鑑み、不審な通信や大量のアクセスの痕跡がないか、アクセスログ等の点検・分析を実施することを推奨します。

・個人情報や業務情報へのアクセス記録を取得する
・不審なアクセスや大量データの取得を監視する
・ログを一定期間保管する
・異常を検知した場合の対応態勢を整備する

サイバー攻撃による被害は、もはや情報システム部門だけの問題ではありません。不正アクセスによって個人情報や業務情報が流出した場合、事業停止、顧客対応など、多方面にわたる経営リスクへと発展する可能性があります。AI の悪用を含むサイバー攻撃の手法が高度化・巧妙化する中、経営層の皆様におかれましては、サイバーセキュリティ対策を経営課題と位置づけ、必要な投資や人的体制整備を含む対策の強化をお願いいたします。

また、被害にあわれた組織にあっては、更なる攻撃被害の拡大を防ぐため、サイバー攻撃に関する技術的な情報を、内閣官房国家サイバー統括室や所管省庁、専門機関等に速やかに共有いただけますよう、何卒ご協力をお願いいたします。

（参考資料）

・重要インフラのサイバーセキュリティ対策のための統一基準
・重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン
・サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集
・サイバーセキュリティ人材フレームワーク 2026

以上

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