８保医健薬第３２６７号
令和８年１１月１３日

一般社団法人東京都病院薬剤師会
会長　　後藤　一美　様

東京都保健医療局健康安全部長
神永　貴志
（　公　印　省　略　）

サイバー攻撃・不正アクセス等への対策について

平素より、東京都の保健医療行政に御理解と御協力を賜り、厚く御礼申し上げます。昨今、ウェブサイトやシステムのセキュリティ上の脆弱性を悪用した不正アクセスや、システムの運用・保守等を行う委託先を経由したサイバー攻撃などにより、個人情報等が漏えいする事案が、幅広い分野の事業者・団体等で相次いで発生しています。

サイバー攻撃等による被害が生じた場合、事業停止や顧客対応など事業活動に重大な支障を来すほか、悪用による二次被害の拡大など、都民生活に重要な影響を及ぼすおそれがあります。

こうした状況を踏まえ、サイバー攻撃・不正アクセス等による被害の発生及び拡大を防止するため、事業者・団体等において共通して確認が必要となる基本的な取組を、別添１「サイバー攻撃・不正アクセス等への対策のポイント」として取りまとめましたので、お知らせします。必要に応じて、現在講じているセキュリティ対策の点検、対策の実施にお役立てください。

また、本通知の内容について、貴会会員にも周知いただきますよう、併せてお願いいたします。

添付資料
（１）別添１「サイバー攻撃・不正アクセス等への対策のポイント」

【問合せ先】
東京都保健医療局健康安全部薬務課薬務担当
電話番号　０３－５３２０－４５１１

別添１

サイバー攻撃・不正アクセス等への対策のポイント

１　ウェブサイトやシステムの適切な管理

利用している**ソフトウェアやシステム等を最新の状態に保つ**とともに、多要素認証の導入など、**適切な認証及びアカウント管理**を行い、使用していないシステムやアカウントが残っていないか確認することが必要です。

また、サイバー攻撃等によりシステムやデータが利用できなくなった場合に備え、重要なデータのバックアップを適切に管理するとともに、**システム及び業務を復旧・継続するための手順や体制を定めておくことが重要**です。

２　委託先のセキュリティ対策の確認

ウェブサイトやシステム等の管理を委託している場合は、委託先に任せきりにせず、**必要な対策の実施状況や、平時及び事故発生時の役割分担、連絡体制について、あらかじめ確認**しておく必要があります。

３　保有する情報の適切な管理

クラウドサービス等で保管している場合を含め、保有する個人情報や業務上の情報を把握し、**不要な情報が残っていないか、また、情報を利用できる者が業務上必要な範囲に限られているか、定期的に点検することが有効**です。

４　最新のセキュリティ情報の確認及び専門機関等への相談

最新のセキュリティ情報を確認するとともに、対策方法が分からない場合や不正アクセスが疑われる場合には、**早めに専門機関やシステムの保守事業者等に相談**することが重要です。

（参考：セキュリティ情報及び相談窓口）

- 内閣官房国家サイバー統括室「サイバー対応特設サイト」
  https://www.cyber.go.jp/tokusetsu/contactpoint_advisory_hub/index.html
- ＩＰＡ（独立行政法人情報処理推進機構）「重要なセキュリティ情報」
  https://www.ipa.go.jp/security/security-alert/index.html
- ＩＰＡ（独立行政法人情報処理推進機構）「不正アクセス対策特設サイト」
  https://www.ipa.go.jp/security/support/incident-support.html