事　務　連　絡
令和４年３月１日

各都道府県衛生主管部（局）薬務主管課　御中

厚生労働省医薬・生活衛生局医療機器審査管理課

厚生労働省医薬・生活衛生局医薬安全対策課

医療機器等に関するサイバーセキュリティ対策の強化について（要請）

本日付けで、経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁及び内閣官房内閣サイバーセキュリティセンターより、別添のとおり、政府機関や重要インフラ事業者をはじめとする各企業・団体等において、サイバー攻撃の脅威に対する認識を深めるとともに、リスク低減のための措置等を講じることによりセキュリティ対策の強化に努めていただくよう、注意喚起いたしました。

つきましては、貴管下関係事業者に対して、本注意喚起に基づく適切なセキュリティ対策の実施について周知方御配慮お願いいたします。

令和４年３月１日
経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

１．リスク低減のための措置

○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

２．インシデントの早期検知

○サーバ等における各種ログを確認する。

○通信の監視・分析やアクセスコントロールを再点検する。

３．インシデント発生時の適切な対処・回復

○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。