医薬機審発0328第１号
医薬安発0328第３号
令和６年３月28日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬局医療機器審査管理課長
（　　公　　印　　省　　略　　）
厚生労働省医薬局医薬安全対策課長
（　　公　　印　　省　　略　　）

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

医療機器のサイバーセキュリティの確保については、「医療機器におけるサイバーセキュリティの確保について」（平成27年４月28日付け薬食機参発0428第１号・薬食安発0428第１号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求めています。また、国際医療機器規制当局フォーラム(IMDRF)における、サイバーセキュリティ対策の国際的な調和を図ることを目的とした「Principles and Practices for Medical Device Cybersecurity」（医療機器サイバーセキュリティの原則及び実践。以下「IMDRFガイダンス」という。）の発行等の国際的な枠組みでの活動を踏まえて、医療機器へのサイバー攻撃に対する国際的な耐性基準等の技術要件を我が国へ導入して整備することを目的に、医療機器のサイバーセキュリティに係る必要な開発目標及び技術的要件等を検討し、主に医療機器製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」として取りまとめられたことを「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」（令和３年12月24日付け薬生機審発1224第１号・薬生安発1224第１号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）により、情報提供しています。さらに、IMDRFにおいて追補ガイダンスが発出されたことから、その内容に基づき、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、脆弱性の修正、インシデントの対応等を検

討し、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書」として、「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」（令和５年３月31日付け薬生機審発0331第11号・薬生安発0331第４号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）により、お示ししたところです。

我が国においては、国境を超えて行われる医療機器に対するサイバー攻撃への対策を一層強化して医療現場における安全性を確保するため、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準」（平成17年厚生労働省告示第122号）の改正を行い、許認可において医療機器のサイバーセキュリティ対応を確認することができる体制の構築を進めています。

今般、医療機器のサイバーセキュリティの更なる確保に向けた医療機器製造販売業者等の体制確保を円滑に行えるよう、脆弱性の管理等に関する留意事項を下記のとおりまとめたので、貴管下関係製造販売業者等に対する周知及び体制確保に向けた指導等よろしくお願いします。

なお、本通知の写しを独立行政法人医薬品医療機器総合機構理事長、一般社団法人日本医療機器産業連合会会長、一般社団法人米国医療機器・IVD 工業会会長、欧州ビジネス協会医療機器・IVD 委員会委員長、一般社団法人日本臨床検査薬協会会長及び医薬品医療機器等法登録認証機関協議会代表幹事宛て送付することを申し添えます。

記

１．脆弱性の管理

脆弱性は、システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計、導入又は運用管理における欠陥又は弱みであることから（JIS T 81001-1:2022 3.4.22)、医療機器のサイバーセキュリティを確保するため、医療機器製造販売業者等は、当該医療機器の脆弱性について、特定、評価、開示、修正等を行う必要がある。これら脆弱性の管理について、以下に留意すること。

(1) 脆弱性を特定及び検出するため、医療機器製造販売業者等は医療機関等と連携するとともに、独立行政法人情報処理推進機構（IPA）又は Japan Computer Emergency Response Team Coordination Center（JPCERT/CC）のウェブサイトから適時情報収集に努めること。IPA 又は JPCERT/CC のウェブサイトから適時情報収集するためには、IPA 又は JPCERT/CC の情報提供窓口へメールアドレスを登録する必要があるが、医薬品、医薬部外品、化

粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令（平成 16 年厚生労働省令第 135 号）第 7 条の規定に沿って必要な情報を収集する場合は、この限りではない。

＜IPA＞
以下ウェブサイトを参照の上、メールアドレスを登録すること。
参考：https://www.ipa.go.jp/mailnews.html

＜JPCERT/CC＞
announce-join@jpcert.or.jp へ、件名及び本文を空欄にてメールを送付すること。
参考：https://www.jpcert.or.jp/announce.html

(2) 医療機器製造販売業者等が自社製品に関連する脆弱性と思われる情報を入手した際は、情報の受付、確認及び評価を行い、それに基づき修正策、緩和策又は補完的対策を行うよう手順を確立すること。また、当該製品を使用している医療機関に対して、当該脆弱性に対する自社製品に関する対応について、補完的対策等も含めて情報提供する手順も確立すること。

(3) 医療機器製造販売業者等は、自社製品に関連する脆弱性を確認した場合には、情報セキュリティ早期警戒パートナーシップに記載された手順に基づき対処を行うこと。また、自社における修正策、緩和策又は補完的対策だけでなく、他医療機器製販業者等への影響を考慮した上で、適時かつ適切な範囲に開示すること。

＜IPA＞
以下ウェブサイトを参照の上、情報セキュリティ早期警戒パートナーシップガイドライン 2019 年版第２刷「５．製品開発者の対応」に基づき脆弱性関連情報情報の取り扱いを行うこと。
参考：
https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

なお、情報セキュリティ早期警戒パートナーシップにおいて IPA は脆弱性関連情報の届出の受付機関であり、医療機器製造販売業者等への連絡及び公表に係る調整は調整機関である JPCERT/CC にて実施される。

(4) 前述１.(1)～(3)について、医療機器製造販売業者等の対応内容に係る不明点は、IPA 又は JPCERT/CC のウェブサイト上の FAQ を参照しつつ、必要があれば IPA 又は JPCERT/CC に相談し、一連の脆弱性の管理を適切に実施できる体制を構築するとともに、日常的に適切な対応を行うこと。

＜IPA＞
vuln-inq@ipa.go.jp
参考：https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html

＜JPCERT/CC＞
vultures@jpcert.or.jp
参考：https://www.jpcert.or.jp/reference.html

２．サイバー攻撃への対応

医療機器製造販売業者等は、医療機器のサイバー攻撃に対する耐性が確保されるように設計及び開発を行い、製造販売後においても、意図する使用環境における医療機器の運用、情報共有、脆弱性の管理等を適切に行う必要がある。これらサイバー攻撃への対応について、以下に留意すること。

(1) 医療機関等がサイバー攻撃を受けた（疑いを含む）場合の体制を予め整備するため、医療機器製造販売業者等は製造販売する医療機器に関する必要な情報を医療機関等へ提供し、適時更新すること。

(2) 医療機器製造販売業者等は、医療機関に対し、サイバーセキュリティに関する保守計画、インシデントを処理するためのポリシー及び役割について説明した上で、医療機器を納入すること。

(3) 医療機器が関係するサイバー攻撃を医療機関が受けた場合、医療機器製造販売業者等は、予め整理した内容に基づき医療機関と連携し、医療提供の復旧に協力すること。

(4) 前述２.(3)の内容について、必要に応じて、IPA が提供する情報セキュリティ安心相談窓口、又は JPCERT/CC へ相談出来ることに留意すること。

＜IPA＞
anshin@ipa.go.jp
参考：https://www.ipa.go.jp/security/anshin/about.html

＜JPCERT/CC＞
以下ウェブサイトを参照すること。
参考：https://www.jpcert.or.jp/form/#report

３．その他

医療機器のサイバーセキュリティに関する情報は、以下の厚生労働省ウェブサイトを参照すること。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

以上