医薬機審発 0417 第１号
医薬安発 0417 第１号
令和７年４月 17 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対策に関連する情報提供について

「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 41 条第３項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件」（令和５年厚生労働省告示第 67 号）による改正後の「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 41 条第３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。以下「基本要件基準」という。）第 12 条第３項の取扱いについては、「医療機器の基本要件基準第 12 条第３項の適用について」（令和５年３月 31 日付け薬生機審発 0331 第８号。以下「取扱い通知」）等により示しているところです。

取扱い通知４（１）において、追って通知するとしていた令和６年３月 31 日以前に製造販売された医療機器に関する取扱いについて、今般、その一部として、当該医療機器の医療機器製造販売業者、外国製造医療機器等特例承認取得者又は外国指定高度管理医療機器製造等事業者（以下「製造販売業者等」という。）が医療機関等に対して情報提供するべき事項を下記のとおりまとめました。

製造販売業者等は、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（昭和 35 年法律第 145 号。以下「法」という。）第 68 条の２の６第１項に基づき、医療機器の適正な使用のために必要な情報を収集し、及び検討するとともに、これを医療機関等に提供するよう努めなければならないとされていること、法第 68 条の９第１項に基づき必要な措置を講じなければならないとされていることに加え、法第 68 条の 10 第１項に基づき不具合等を厚生労働大臣に報告しなければならないとされているところ、引き続き、本通知における留意事項に基づき、適切な対応を進めるよう、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

令和６年３月 31 日以前に製造販売された医療機器のうち、医療機関等に存在し、「基本要件基準」第 12 条第３項への適合が確認されていない医療機器については、設計及び開発におけるサイバーセキュリティ対応が十分とは限らず、サイバー攻撃に対して脆弱である場合がある。医療現場における患者の安全性を確保するため、医療機器の製造販売業者、外国製造医療機器等特例承認取得者又は外国指定高度管理医療機器製造等事業者（以下「製造販売業者等」という。）は、当該医療機器のサイバーリスクに関する評価を実施し、医療機関等に対し、運用、意図する使用環境におけるサイバーリスク等の情報共有、及び脆弱性の管理等を適切に行う必要がある。従って、令和６年３月 31 日以前に製造販売された医療機器のうち、医療機関等において稼働している可能性のある医療機器のサイバーセキュリティ対応について、以下に留意すること。

(1) 製造販売業者等は、医療現場における患者の安全性を確保するため、当該医療機器のサイバーリスクに関する評価及び対策等を適切に実施し、意図する使用環境におけるサイバーリスクに関する情報を医療機関等に提供すること。また、医療機関等の求めに応じてソフトウェア部品表(SBOM)を提示できるように準備しておくこと。なお、サポート終了（EOS）を過ぎたものと製造販売業者等が判断した医療機器については、納入先である医療機関等に対し、既に EOS などに関する必要な情報提供をしている場合、SBOM の作成及び提示を要しない。

(2) 製造販売業者等は、医療機器のライフサイクルを特定し、製品寿命終了（EOL）及び EOS に関する情報を医療機関等に提供していない場合は、医療機器のライフサイクル（①～③）に応じて医療機関等に提供すること。なお、EOL、EOS を設定する時期については、製品のライフサイクルに応じて各製造販売業者等にて設定されるべきものであるが、EOL、EOS を設定した場合は適宜、医療機関等へ情報提供を行うこと。

①医療機器が EOL を越えていない場合、製造販売業者等は、サポート（適用可能なセキュリティパッチ、セキュリティ確保に必要なアップグレード等）に関する情報を含めて提供すること。
② 医療機器が EOL を越えている場合、製造販売業者等は、EOS までの期間は、限定的サポート（セキュリティパッチ、必要に応じて補完的対策等）に関する情報を含めて提供すること。
③ 医療機器が EOS を越えている場合、製造販売業者等は、補完的対策等の情報を含め、EOS に関する情報を速やかに提供すること。

(3) 製造販売業者等は、医療機器が EOS に達していない（(2)の①又は②）場合、医療機関等に提供したセキュリティパッチ等の情報について、医療機器に適用する計画等を医療機関等へ示し、医療機関等と連携して定期点検等の適切な時期に適用すること。医療機器に適用するセキュリティパッチ等の評価等に時間を要する場合は、ファイアウォール等の補完的対策を先行してリスク緩和策として適用する等の段階的な計画としてもよい。

(4) 製造販売業者等は、医療機器が EOS を越えて使用されている場合においても、有効性及び安全性に関する事項その他製品の適正な使用のために必要なサイバーセキュリティに関する情報を収集し、医療機関等への情報提供を行うこと。また、サイバーセキュリティに関連して医療機器に不具合が発生し、健康被害が発生した又は健康被害の発生のおそれがある場合や、脆弱性に対し外国医療機器の安全確保措置が実施された場合には、不具合等報告の要否を検討し適切な対応をとること。

(5) 製造販売業者等は、中古医療機器を取扱う販売業者等の求めに応じて上記（1）～(4)と同様の対応をすること。