薬生機審発０７２４第１号
薬生安発０７２４第１号
平成３０年７月２４日

各都道府県衛生主管部（局）長　殿

厚生労働省医薬・生活衛生局医療機器審査管理課長
（　　公　　印　　省　　略　　）

厚生労働省医薬・生活衛生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の確保に関するガイダンスについて

医療機器のサイバーセキュリティの確保に関しては、「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）、厚生労働省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を確保するために、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を実施し、必要な対応を行うよう、関係事業者等に対する周知を依頼しているところです。

今般、さらに具体的なリスクマネジメント及びサイバーセキュリティ対策について、平成 29 年度日本医療研究開発機構医薬品等規制調和・評価研究事業「医療機器に関する単体プログラムの薬事規制のあり方に関する研究」の研究報告を基に、「医療機器のサイバーセキュリティの確保に関するガイダンス」として別添のとおり取りまとめました。つきましては、医療機器のサイバーセキュリティの確保に当たって、同ガイダンスを参考として、必要な対応を行うよう、貴管下関係事業者等に周知方お願いいたします。

別添

医療機器のサイバーセキュリティの確保に関するガイダンス

背景

「サイバーセキュリティ基本法」(平成 26 年法律第 104 号)に基づき、内閣に「サイバーセキュリティ戦略本部」、内閣官房に「内閣サイバーセキュリティセンター」が平成 27 年 1 月に設置され、「サイバーセキュリティ戦略」が平成 27 年 9 月 4 日に閣議決定された。

「サイバーセキュリティ」は、サイバーセキュリティ基本法第2条において、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていること」と定義されている。またサイバーリスクとは、そうした安全性や信頼性が損なわれ、危害(harm)(※1)が生じるリスクと考えられる。

医療に関するサイバーセキュリティ対応に関しては、医療機関等の医療情報システムについて、平成 17 年3月、厚生労働省から「医療情報システムの安全管理に関するガイドライン」(以下、「安全管理ガイドライン」という。)第 1 版を示し、情勢に応じた随時の改定を経て、平成 29 年 5 月の第 5 版に至っている。

また、医療機器のサイバーセキュリティについては、厚生労働省から「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 号厚生労働大臣官房参事官(医療機器・再生医療等製品審査管理担当)、厚生労働省医薬食品局安全対策課長連名通知。以下、「サイバーセキュリティ通知」という。)にて、医療機器製造販売業者(以下、「製造販売業者」という。)に対し医療機器へのサイバーセキュリティ対応の考え方を示している。

製造販売業者は、有効性及び安全性を確保した医療機器を設計・製造して供給することを責務としており、加えて、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。以下、「GVP 省令」という。)に基づき、販売後の使用における医療機器の有効性、安全性等に関する情報収集・分析、必要に応じた対策等、適切な対応が求められている。このため、製造販売業者は医療機器への悪意を持ったサイバー攻撃に対しても、使用環境を含めた医療機器の特徴に応じて、サイバーセキュリティ対応にも取り組んでいく必要がある。

一般的に、情報セキュリティには、情報の機密性、完全性及び可用性の3つの要素を確保することが求められる。機密性(Confidentiality)とは、正当な権限をもつ限られた者のみ

が、許可された範囲内で情報にアクセスできるよう、保護・管理されていることを指す。完全性(Integrity)とは、データの正当性、正確性及び一貫性が維持され、不適切な変更が行われていないことを意味し、意図された使用方法の下で医療機器の機能や性能が確保され、患者情報や診断結果等の正確性が保たれていることを指す。そして可用性(Availability)とは、必要なときにシステムが正確なサービスを提供できる状態が維持されていることを指す。

これらの要素を満たすべく、サイバーリスクに対するリスクマネジメントを考える際には、従来行われてきた、一次故障や誤操作等をリスク要因として捉えるリスクマネジメントに加えて、悪意を持った攻撃者の存在等もリスク要因として捉えて検討することが必要となる。

(※1　医療機器のリスクマネジメントの規格である JIS T 14971:2012 では、危害(harm)を「人の受ける身体的傷害若しくは健康障害、又は財産若しくは環境の受ける害」と定義している。本ガイダンスでは、患者や医療機器の使用者に対する安全性に係る危害を第一に想定しているが、医療機器の製造販売業者は個人情報の漏洩等の危害についても十分な対応をすることが社会的に求められていることに十分に留意すべきである。)

1.目的

本ガイダンスの目的は、サイバーセキュリティ通知により示された製造販売業者が行うべきサイバーセキュリティへの取組について、医療機器への開発・設計(市販前)及び市販後の対応をより具体的にするための情報を提供することである。製造販売業者が本ガイダンスを参考に適切な対応を実施することによって、サイバーセキュリティに関するリスクの低減、医療機器本来の有効性及び安全性の確保が図られ、患者へのリスクの低減に繋がる。

なお、サイバーセキュリティの分野は攻撃方法の多様化・巧妙化等の状況の変化が著しいことから、サイバーセキュリティの対策は、本ガイダンスに示したものに限らず、技術動向等を踏まえて適切な対策を取るべきことに十分留意することが必要である。

2.検討が必要となる医療機器及び使用環境の特定

本ガイダンスは、サイバーセキュリティに関するリスクが想定される医療機器を対象とするものであり、医療機器の全てを対象とするものではない。サイバーセキュリティに関する対応が必要な医療機器に該当するかは、機器の特性及びその使用環境等を特定し検討することが必要である。

医療機器におけるサイバーリスクのうち、医療機器を用いた診療を受ける者(患者)及び医療機器の使用者に対する障害に係るリスクは、優先的に対応することが必要である。

2.1 対象となる医療機器

本ガイダンスの対象は、医療機器のうちプログラムを使用したもの（医療機器プログラムを含む。）及び付属品等にプログラムを含むものである。医療機器のクラス分類（Ⅰ～Ⅳ）を問わない。

基本的に、医療機器と接続して使用する又は併用される IT 機器等（単体で医療機器に該当しないもので、プログラム単体の場合を含む。）を医療機器の構成品（付属品等）として提供する場合は、本ガイダンスの対象となる。

2.2 医療機器の使用環境の特定

各医療機器に係るサイバーリスクを想定するためには、当該医療機器の使用環境を特定することが必要となる。また、使用環境だけでなく、医療機器を構成するユニット間又は複数の医療機器で構成されるシステムにおいて、医療機器間でインターネット等（無線等含む）を利用し、制御信号あるいはデータ交換を行う場合についても考慮することが必要となる。

医療機関等においては、「安全管理ガイドライン」を踏まえた安全管理が求められていることに留意すること（例えば、アクセス管理、通信の暗号化等。）。

なお、特定した使用環境に関する情報は、使用者等へ情報提供する必要がある（5. 参照）。

2.2.1 医療機関での使用環境

多くの医療機器は医療機関内で使用されており、また、医療機関の医療情報システムに関しては「安全管理ガイドライン」を踏まえた安全対策及び管理が求められている。したがって、医療機関での使用を意図する医療機器の場合は、「安全管理ガイドライン」で求められる環境での使用を基本とする。

2.2.2 医療機関の管理が及ばない使用環境

例えば、在宅医療で使用される医療機器の場合、医療機関による管理が十分に及ばない環境で使われることに留意する必要がある。

在宅医療で使用する医療機器や家庭用の医療機器の開発においては、当該医療機器の使用環境を明確化し、医療機関の管理が及ばない使用環境での使用を意図した場合は、「安全管理ガイドライン」を踏まえた管理の及ばない環境であることを考慮する必要がある。

2.2.3 その他の使用環境（特定が困難）

体内植込み機器や装着機器等の多くは、患者の移動に伴い様々な場所に移動する。こ

のため、想定される多様な環境での使用時におけるサイバーリスク等を評価し、その危険性等についても留意すること。

2.3 医療機器のネットワーク等への接続

医療機器における通信機能・ネットワークへの接続や USB 等のポートの利用に応じたサイバーリスクの検討が必要となる。

2.3.1 ネットワーク等への接続機器

医療機器が接続されるネットワークを踏まえた検討が必要である。医療機関内に限定され、インターネット回線と分離された環境で使用される機器と、インターネット回線への接続を意図する機器では、使用環境が異なっており、接続環境に応じた対応が必要となる。

ネットワーク通信により医療機器内の情報を送受信したり、操作したりすることが可能な医療機器については、より慎重にサイバーセキュリティ対応を考慮すべきである。なお、ネットワーク接続を利用するリモートメンテナンス等の保守機能を持つ医療機器についても同様である。

2.3.2 無線通信等利用の医療機器

無線通信（医療用無線周波数帯域、Bluetooth、Wi-Fi 等）を利用し、医療機器のユニット間又は医療機器間で制御信号や情報交換をする機能を有する機器に関しては、利用している技術及び使用する機器の種類におけるリスクに応じた配慮が必要となる。

2.3.3 USB 等の外部入出力ポート

USB ポートや CD/DVD ドライブ等を備え、使用可能な状態にある医療機器に関しては、これらを使用した場合のリスクへの対応が必要となる。

3.サイバーセキュリティ対応

医療機器に係るサイバーセキュリティへの対応については、製造販売業者による対応はもちろんのこと、使用者側における当該医療機器の適切な使用、維持管理、「安全管理ガイドライン」に基づく情報システムの維持管理等日常の適切な管理が重要である。

なお、サイバーセキュリティへの対応に当たっては、関連のガイダンス、規格、技術文書、その他の方法等の最新の情報を参考にしながら、医療機器の使用環境を踏まえ実施する必要がある。（巻末の「参考資料等」及び「規格、規格文書等」を参照。）

3.1 製造販売業者によるサイバーセキュリティ対応

製造販売業者は、意図される使用環境におけるサイバーリスクに対するリスクマネジメントを実施し、必要な対策を行い、その結果リスクが受容可能になることを説明できるようにすること。リスクマネジメントを行うに当たっては、医療機器の意図される使用方法、使用者、使用環境等を考慮したベースラインを定めて実施、検証することが望ましい。

特に、医療機器の開発・評価時に使用されるデータベースや、実使用時に利用される OS 等の既製品ソフトウェアについても、医療機器のライフサイクル(※2)を通じ考慮する必要がある。なお、これら既製品ソフトウェアを用いた医療機器のライフサイクルと搭載した当該既製品ソフトウェアのライフサイクルについては、整合させることが望ましいが、困難である場合には、その対応について検討を行い、必要に応じて使用者へ必要な情報を提供する(5項参照)。

なお、製造販売業者は、供給する製品のサイバーセキュリティ対応に関する社内の方針・体制を品質システム等の一部として確立することが求められる。また、サイバーセキュリティに関連する問合せ窓口及びサービスに係る取組について、使用者へ開示することが望ましい。

(※2 ライフサイクルとは、開発から使用を終了し破棄されるまでが本来の期間ではあるが、これとは別に医療機器の設計・製造時には耐用期間が特定されている。各医療機器の耐用期間については、通常、添付文書に「保管方法及び有効期間等」として記載されており、製造販売業者は、少なくともこの期間は、当該医療機器についてサイバーセキュリティへの対応を行うことが必要となる。また、既出荷製品について適切な脆弱性管理ができない場合、製造販売業者は、製品の扱いに関する情報を使用者へ速やかかつ適切に伝えるとともに、使用者と連携して対応することも必要となる。)

3.2 使用者によるサイバーセキュリティ対応

製造販売業者から出荷された医療機器は、販売業者・貸与業者を経て、医療機関等の使用者に納入される。納入後の医療機器のサイバーセキュリティに関する日常の管理は、医療機関等の使用者にて実施する必要があることから、製造販売業者は、必要に応じて医療機関と連携を取り、保守契約等に基づきサイバーセキュリティの確保を支援することが重要である。なお、医療機器から医療機関等の情報システムへ転送されたデータに関するサイバーリスクについては、システムの管理者である医療機関による対応が必要である。

サイバーリスクに伴う医療機器の不具合等の情報も、GVP省令における安全管理情報の一つであるため、製造販売業者は、医療機関と連携を取り、こうした情報を収集する必要がある。

また、独立行政法人情報処理推進機構(IPA)セキュリティセンターでは、「コンピュータウ

イルス対策基準」(平成7年通商産業省告示第 429 号)、「コンピュータ不正アクセス対策基準」(平成8年通商産業省告示第362号)及び「ソフトウェア製品等の脆弱性関連情報に関する取扱規定」(平成 29 年経済産業省告示第 19 号)、に基づき、コンピュータウイルス・不正アクセス・脆弱性情報に関する発見・被害の届出や情報提供を受け付け、提供を受けた情報は、被害の拡大・再発の防止、情報セキュリティ対策の向上に役立てられている。製造販売業者はこれらの情報を参考にするとともに、独立行政法人情報処理推進機構(IPA)セキュリティセンターに対して医療機器のサイバーリスクに関係する情報を適切に提供していくことが望ましい。

4.市販後の安全性確保について

製造販売業者は、GVP 省令に基づき、医療機器の市販後安全対策として医療機器の不具合情報や文献等を収集・調査し、その情報を分析して、必要に応じて対策を行うことが必要となる。サイバーリスクに基づく不具合等についても、GVP 省令における安全性情報として取り扱い、販売業者・貸与業者や修理業者の協力のもと、医療機関と連携を取り、適切な市販後の安全確保を行う必要がある。

4.1 中古医療機器への対応について

プログラムを使用した医療機器の多くは耐用期間が長く、特定保守管理医療機器に指定されている。これらの医療機器を中古で販売する場合、医療機関から引き取った販売業者及び中古医療機器を医療機関へ販売する販売業者は、医療機器の整備等に関し製造販売業者へ照会し、その指示に基づいて整備を行うことが求められている(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施行規則(昭和 36 年厚生省令第1号)第 170 条)。このため、中古医療機器についても、製造販売業者は当該医療機器の販売業者に対し適切な指示を行い、サイバーリスクへの対応を実施させる必要がある。

また、販売業者は、医療機関に対し、販売する中古医療機器のサイバーリスクへの対応状況等について適切に説明する必要がある。

5.使用者等への情報提供

サイバーリスクが想定される医療機器については、サイバーセキュリティに関する情報を製造販売業者から使用者に提供する事が求められる。体内植込み医療機器等については装着者への提供も必要である。

また、外部との接続がないことが明確である等の理由からサイバーリスクが想定されない

場合であっても、プログラムが使用されていることが明らかな医療機器の場合には、サイバーリスクが想定されない旨の情報を使用者に対し提供を行うことが望ましい。

提供すべき情報としては、次の事項が基本となるが、サイバーリスクの程度に応じて適切に対応すること。なお、公開することにより、サイバーリスクが増大することが想定される情報については、その提供方法についての配慮が必要である。

1） 添付文書への記載事項

- 意図する使用環境
- 使用者側が遵守すべき事項（概要）
- 要求された環境外で使用した場合のリスク（リスクの重要性により必要に応じ記載）

2） 技術資料等

- 技術情報（ネットワーク環境への接続に必要な情報等）

これらの情報は、医療機関等からの求めに応じ提供できること。また、医療機関での使用を意図する医療機器の場合、「安全管理ガイドライン」に沿った情報提供が望ましい。

3） その他

- 医療機器の市販後のライフサイクルに応じた対応の方法
- 製造販売業者としてのサイバーセキュリティ対応への取組み等に関する情報
- サイバーセキュリティに関連する問合せ窓口及びサイバーセキュリティに関連するサービスの照会先

サイバーリスク対応に関する情報提供について、例えば、製造販売業者のホームページ等を利用して提供する旨を添付文書に記載し、必要な時に速やかに情報を入手できるようにすることも一つの方法である。

参考資料等

- 「医療機器プログラムの承認申請に関するガイダンスの公表について」（平成 28 年 3 月 31 日付け厚生労働省医薬・生活衛生局医療機器・再生医療等製品担当参事官室事務連絡）
- 医療情報システムの安全管理に関するガイドライン第 5 版（厚生労働省　平成 29 年 5 月）
- 「医療情報システムの安全管理に関するガイドライン第 5 版」に関するＱ＆Ａ（厚生労働省　平成 29 年 5 月）

- JAHIS標準 17-006 「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a(一般社団法人保健医療福祉情報システム工業会 2017 年 7 月)
- JESRA TR－0039*B－2018 「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a(一般社団法人日本画像医療システム工業会 2018 年 3 月)

規格、技術文書等

- IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities
- IEC TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices -Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- IEC TR 80001-2-8:2016 Application of risk management for IT networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
- NIST SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations

  (NIST: 米国国立標準技術研究所の規格で、多くのセキュリティに関する国際規格から参照されているベストプラクティスによる標準)