

(2) 【予防】データの暗号化による被害を軽減するための対応策

従来のランサムウェア対策の常套手段であったバックアップは、引き続き有効です。これに加え、2重脅迫ランサムウェアに感染した場合は、組織の機微データや個人情報流出の懸念があることから、「機微データの厳格管理」については、改めて検討する必要があります。

チェックポイント

- 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウェア感染時でもバックアップが保護されるように留意する。例えば、ファイルのコピーを3個取得したうえで、ファイルは異なる2種類の媒体に保存、コピーのうち、1個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する。
- 公開された場合、実際に支障が生じるような機微データや個人情報等に対して、特別なアクセス制御や暗号化を実施する。
- システムの再構築を含む復旧計画が適切に策定できていることを確認する。

(3) 【検知】不正アクセスを迅速に検知するための対応策

不正アクセスを迅速に検知するための対応策が必要です。迅速な検知を実現するためには、オペレーターとマシンによる自動化を検討する必要があります。

チェックポイント

- サーバー、ネットワーク機器、PC等のログの監視を強化する。
- 振る舞い検知、EDR(Endpoint Detection and Response)、CDM(Continuous Diagnostics and Mitigation)等を活用する。

(4) 【対応・復旧】迅速にインシデント対応を行うための対応策

ランサムウェアによる攻撃の被害を受けた場合でも、冷静で適切な対応ができるよう、組織一丸となった対処態勢を構築する必要があります。

チェックポイント

- データの暗号化、公開、インターネット公開サーバーに対するDoS攻撃等を想定した対処態勢、対処方法、業務継続計画等を含むランサムウェアへの対応計画が適切に策定できているか確認する。
- 一部の職員が長期休暇中やテレワーク等であっても、職員がランサムウェア感染の兆候を把握した場合、職員が迅速にシステム管理者に連絡できることを確認する。
- ランサムウェアの感染による被害を受けた場合に、組織内外(業務委託先、関係省庁を含む)に迅速に連絡できるよう、連絡体制を確認する。

参考 URL

- ・ランサムウェアによるサイバー攻撃について【注意喚起】(NISC)
<https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf>
- ・【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について(IPA)
<https://www.ipa.go.jp/security/announce/2020-ransom.html>
- ・CISA and MS-ISAC Release Ransomware Guide(CISA)
<https://us-cert.cisa.gov/ncas/current-activity/2020/09/30/cisa-and-ms-isac-release-ransomware-guide>
- ・大型連休等に伴うセキュリティ上の留意点について(NISC)
<https://www.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf>
- ・最近のサイバー攻撃の状況を踏まえた経営者への注意喚起(経済産業省)
<https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf>
- ・「EMOTET」後のメール脅威状況:「IcedID」および「BazarCall」が3月に急増(トレンドマイクロ)
<https://blog.trendmicro.co.jp/archives/27732>
- ・So Unchill - UNC2198 ICEDIDのランサムウェア・オペレーションへの融解(FireEye)
<https://www.fireeye.com/blog/jp-threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html>
- ・2021年も増加傾向のランサムウェア、被害に関する共通点とは(LAC)
https://www.lac.co.jp/lacwatch/report/20210405_002585.html
- ・UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat(FireEye)
<https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html>

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。

医療機器のサイバーセキュリティの確保に関するガイドンス

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。本ガイドラインでは、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

本ガイドラインの目的は、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ドライン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、本ガイドライン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

本ガイドラインは、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、関連のガイドンス、規格、技術文書、その他の方針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)

薬生機審発 0513 第 1 号
薬生安発 0513 第 1 号
令和 2 年 5 月 13 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)

国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの
原則及び実践に関するガイダンスの公表について（周知依頼）

医療機器のサイバーセキュリティについては、「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)、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、「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」(平成30年7月24日付け薬生機審発0724第1号、薬生安発0724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、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を取りまとめたガイダンスを示し、当該ガイダンスを参考に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きたところです。

今般、医療機器のサイバーセキュリティ確保の重要性や各国のサイバーセキュリティ対策の実情等を踏まえ、国際医療機器規制当局フォーラム(IMDRF)において、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て、「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。）が取りまとめられました。

国際的な規制調和の推進の観点や国境の枠組みを超えて医療機器のサイバーセキュリティに係る安全性を向上させる観点から、我が国においても、今後3年程度を目途に、医療機器製造販売業者に対してIMDRFガイダンスの導入に向けて検討を行っているところです。そのため、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、別添のとおり、国立医薬品食品衛生研究所医療機器部が作成したIMDRFガイダンスの邦訳版を参考として情報提供いたしますので、貴管下の医療機器製造販売業者等に対し、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、IMDRFガイダンスの原文は以下のホームページから入手可能であることを申し添えます。

U R L : <http://www.imdrf.org/documents/documents.asp>

IMDRF/CYBER WG/N60 FINAL:2020



IMDRF International Medical
Device Regulators Forum

最終文書

タイトル： 医療機器サイバーセキュリティの原則及び実践

作成グループ： 医療機器サイバーセキュリティワーキンググループ

日付： 2020年3月18日

Dr Choong May Ling, Mimi, IMDRF 議長

本文書は、国際医療機器規制当局フォーラムによって作成された。本文書の複製又は使用に関する制限はない。ただし、本文書の一部又は全てを他の文書に組み込む場合、並びに本文書を英語以外の言語に翻訳する場合、国際医療機器規制当局フォーラムは、その責任を一切負わない。

Copyright © 2020 by the International Medical Device Regulators Forum

目次

1.0	はじめに.....	5
2.0	適用範囲.....	6
3.0	定義.....	7
4.0	一般原則.....	9
4.1	国際整合	10
4.2	製品ライフサイクルの全体.....	10
4.3	共同責任.....	10
4.4	情報共有	10
5.0	医療機器サイバーセキュリティの市販前考慮事項.....	11
5.1	セキュリティ要求事項及びアーキテクチャ設計	11
5.2	TPLC に関するリスクマネジメント原則	14
5.3	セキュリティ試験.....	17
5.4	TPLC サイバーセキュリティマネジメント計画	17
5.5	ラベリング及び顧客向けセキュリティ文書.....	18
5.5.1	ラベリング	18
5.5.2	顧客向けセキュリティ文書	18
5.6	規制当局への申請に関する文書.....	20
5.6.1	設計文書	20
5.6.2	リスクマネジメント文書	20
5.6.3	セキュリティ試験の文書	20
5.6.4	TPLC サイバーセキュリティマネジメント計画に関する文書.....	21
5.6.5	ラベリング及び顧客向けセキュリティ文書	21
6.0	医療機器サイバーセキュリティの市販後考慮事項.....	21
6.1	意図する使用環境における機器の運用	21
6.1.1	ヘルスケアプロバイダ及び患者	21
6.1.2	医療機器製造業者	23
6.2	情報共有	23
6.2.1	重要原則	23
6.2.2	重要な責任関係者	24

6.2.3 情報の種類	25
6.2.4 信頼できるコミュニケーション	26
6.3 協調的な脆弱性の開示	26
6.3.1 医療機器製造業者	26
6.3.2 規制当局	28
6.3.3 脆弱性の発見者(セキュリティ研究者及びその他の脆弱性発見者を含む).....	28
6.4 脆弱性の修正	28
6.4.1 医療機器製造業者	28
6.4.2 ヘルスケアプロバイダ及び患者	31
6.4.3 規制当局	34
6.5 インシデントへの対応	36
6.5.1 医療機器製造業者	36
6.5.2 ヘルスケアプロバイダ	37
6.5.3 規制当局	38
6.6 レガシー医療機器	38
6.6.1 医療機器製造業者	40
6.6.2 ヘルスケアプロバイダ	42
7.0 参考文献	43
7.1 IMDRF 文書	43
7.2 規格	43
7.3 規制当局のガイダンス	44
7.4 その他の資料及び参考文献	45
8.0 附属書	47
8.1 附属書 A: インシデント対応の役割(ISO/IEC 27035 から引用)	48
8.2 附属書 B: 協調的な脆弱性の開示に関する各地域のリソース	50

序文

本文書は、世界各国の医療機器規制当局の団体である国際医療機器規制当局フォーラム (International Medical Device Regulators Forum: IMDRF)が協議の上、作成されたものである。本文書は、自由に複製、配布、使用して構わない。

ただし、本文書の一部又は全てを他の文書に組み込む場合、並びに本文書を英語以外の言語に翻訳する場合、IMDRFは、その責任を一切負わない。

1.0 はじめに

無線、インターネット及びネットワーク接続機器の使用の増加に伴い、医療機器の機能及び安全性を確保するために有効なサイバーセキュリティの重要性が増している。サイバーセキュリティのインシデントは、医療機器及び病院ネットワークを使用不能にすると共に、ヘルスケア施設における患者ケアの提供を中断させてきた経緯がある。これらのインシデントは、診断及び治療介入の遅延、誤診断又は不適切な治療介入等の発生により、患者危害に至る可能性がある。

ヘルスケア製品の製造業者、ヘルスケアプロバイダ、ユーザ、並びに規制当局及び脆弱性報告者を含む全ての関係者は、医療機器のサイバーセキュリティに関して共同責任を有する。本ガイダンスは、全関係者へ向けて、サイバーセキュリティを積極的に支援するための役割に関する理解を促し、将来起こり得るサイバー攻撃、問題又は事象を予測して、医療機器を保護してセキュアにするための情報を提供することを意図している。

ヘルスケアのサイバーセキュリティの原則及び実践に関する国際整合は、患者安全及び医療機器の性能を確実に維持するために必要である。しかし、現時点における医療機器のサイバーセキュリティに係る規制は国毎に異なっており、国際整合に至っていない。

本 IMDRF ガイダンスは、医療機器のサイバーセキュリティに関する国際整合を図るために一般原則とベストプラクティスを提供することを目的とする。本文書では、適用範囲及び用語をそれぞれ 2 項及び 3 項において定義する。4 項では、医療機器のサイバーセキュリティの一般原則について概説し、5 項及び 6 項では、医療機器のサイバーセキュリティに関する市販前管理及び市販後管理におけるベストプラクティスについて多くの推奨事項を責任関係者に提供する。市販前管理については、主に医療機器製造業者に言及する。市販後管理については、全ての責任関係者に向けた推奨事項を記載する。

本文書は、IMDRF が作成した医療機器のサイバーセキュリティに特化した最初のガイドであるが、セキュリティについて幅広く検討する上で参考すべき IMDRF 文書として「IMDRF/GRRP WG/N47 FINAL: 2018」が挙げられる。当該文書は、医療機器及び体外診断用（In Vitro Diagnostic : IVD）医療機器¹の設計及び製造において充足すべき基本要件基準を提供している。これらの基本要件基準は、医療機器の全ライフサイクル（Total Product Life Cycle : TPLC）に渡って、本ガイドと共に参照することが望ましい。その他の関連文書である「IMDRF/SaMD WG/N12 FINAL: 2014」の 9.3 項では、安全を考慮する際の情報セキュリティの重要性について記載されており、医療機器ソフトウェア（Software as Medical Device : SaMD）の情報セキュリティに影響する幾つかの要因がまとめられている。

¹ N47 の 5.8 項には、不正アクセスからの保護等、情報セキュリティ及びサイバーセキュリティの重要な要求事項が記載されており、医療機器の全ライフサイクルに渡って、本ガイドと共に参照することが望ましい。

2.0 適用範囲

本文書は、全ての責任関係者に向けて、医療機器（IVD 医療機器を含む）のサイバーセキュリティに対する一般原則に係る基本的考え方と検討事項、並びに推奨されるベストプラクティスを提供することを目的として作成された。本文書では、製造業者、ヘルスケアプロバイダ、規制当局及びユーザに向けて、意図する目的に対して医療機器を使用する際に起こり得るサイバーセキュリティリスクを最小化することにより、医療機器の安全性及び性能を維持し、継続使用を確保するための具体的な推奨事項を取りまとめている。本ガイダンスで述べるヘルスケアプロバイダには、医療機関が含まれる。

本文書では、ファームウェア及びプログラマブルロジックコントローラ等のソフトウェアを有する医療機器（例：ペースメーカー、輸液ポンプ）、又はソフトウェア単独で存在する医療機器（例：SaMD）に関するサイバーセキュリティについて概説されている。ほとんどの規制当局は、その権限が医療機器の安全性及び性能に限定されているため、本文書の適用範囲は、患者への危害が発生する可能性に関する検討に限定されていることに留意する必要がある。例えば、医療機器の性能に影響を与える、臨床活動に悪影響を及ぼす、若しくは誤った診断又は治療に繋がるサイバーセキュリティリスクは、本文書の適用範囲とみなされる。データプライバシーの侵害等、その他の危害も重要であるが、本文書では適用範囲から除外する。さらに、本文書では、製造業者の企業活動に関するサイバーセキュリティを適用範囲から除外する。製造業者の企業活動のセキュリティに関するベストプラクティスについては、米国国立標準技術研究所（National Institute of Standard and Technology : NIST）のサイバーセキュリティフレームワークが情報源としての重要な役割を果たしている。

本文書は以下の事項を意図している。

- 医療機器の設計及び開発に適切なサイバーセキュリティ対応を組み込むために、リスクベースアプローチを採用する。
- 医療機器及び接続されるヘルスケアインフラの安全性、性能及びセキュリティを確保する。
- サイバーセキュリティは、製造業者、ヘルスケアプロバイダ、ユーザ、規制当局及び脆弱性発見者等を含む全ての関係者の共同責任であることを認識する。
- それらの関係者に対して、製品ライフサイクルの全体に渡り、患者危害のリスクを最小化するために有益な推奨事項を提供する。
- 用語を定義すると共に、医療機器のサイバーセキュリティを確保するため、現時点のベストプラクティスを記載する。

- サイバーセキュリティのインシデント、脅威及び脆弱性について、透明性を向上させ対応を強化するために幅広い情報共有のポリシーを促進する。

なお、医療機器の種類や各国の規制に応じて、追加の検討事項が必要となり得ることに留意する必要がある。

3.0 定義

本文書で用いる用語及び定義は、以下に示した各規格、並びに IMDRF/GRRP WG/N47 FINAL: 2018 に準ずる。

- 3.1 資産 (Asset) : 個人、組織又は政府にとって価値のある、物理的又はデジタル形式のエンティティ (ISO/IEC JTC 1/SC 41 N0317, 2017-11-12)
 - 3.2 攻撃 (Attack) : 資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み (ISO/IEC 27000:2018)
 - 3.3 認証 (Authentication) : エンティティの特性の正当性に関する保証の提供 (ISO/IEC 27000:2018)
 - 3.4 真正性 (Authenticity) : エンティティの信憑性 (ISO/IEC 27000:2018)
 - 3.5 権限付与 (Authorization) : 特権の付与。データ及び機能にアクセスするための特権を付与することを含む。 (ISO 27789:2013)
- 注記 : ISO 7498-2 の定義 (権利の付与。アクセス権に基づきアクセスの権利を付与することを含める) に由来する。
- 3.6 可用性 (Availability) : 要求するエンティティへのアクセス及び使用の可能性 (ISO/IEC 27000:2018)
 - 3.7 補完的リスクコントロール手段 (補完的手段) (Compensating Risk Control Measure (Compensating Control)) : 機器設計の一部として実施されるリスクコントロール手段の代替として、又はそれが実施されない場合に適用される特定のリスクコントロール手段 (AAMI TIR97:2019)
- 注記: 補完的リスクコントロール手段としては、製造業者が提供するアップデート等、永続的又は一時的な対応があり得る。

- 3.8 機密性 (Confidentiality) : 認可されていない個人、エンティティ又はプロセスに対して、情報を開示せず、使用させない特性 (ISO/IEC 27000:2018)

- 3.9 協調的な脆弱性の開示 (Coordinated Vulnerability Disclosure : CVD) : 研究者及びその他の責任関係者が、脆弱性の開示に関するリスクを低減するための解決策を見つけるために製造業者と協力して行うプロセス (AAMI TIR97:2019)

注記:このプロセスには、脆弱性とその解決策に関する情報の報告、調整、開示等の作業が含まれる。

- 3.10 サイバーセキュリティ : 情報及びシステムが不正な活動 (不正なアクセス、使用、開示、中断、改変、破壊等) から保護されており、機密性、完全性、可用性に関するリスクがライフサイクル全体に渡って受容可能なレベルに維持されている状態。 (ISO 81001-1)

- 3.11 製品寿命終了 (End of Life : EOL) : 製品のライフサイクルにおいて、製造業者の定義に基づき有効期間を超えた製品の販売を終了する時点。EOL を迎えた製品については、正式な EOL プロセス (ユーザへの通知等) が実施される。

- 3.12 サポート終了 (End of Support : EOS) : 製品のライフサイクルにおいて、製造業者が全てのサポート活動を中止する時点。サービスサポートは、この時点を超えない。

- 3.13 基本性能 : 基礎安全に関連する以外の臨床機能の性能において、製造業者の指定した限界を超えた低下又は欠如が生じた時に受容できないリスクを生じる性能 (IEC 60601-1:2005+AMD1:2012)

- 3.14 悪用 (Exploit) : 脆弱性を通じて情報システムのセキュリティを侵害するための明確な方法 (ISO/IEC 27039:2015)

- 3.15 完全性 (Integrity) : データが作成、送信又は保存された後、不正な方法により変更されていない特性 (ISO/IEC 29167-19:2016)

- 3.16 レガシー医療機器 (レガシー機器) (Legacy Medical Device (Legacy Device)) : 現在のサイバーセキュリティの脅威に対して合理的に保護できない医療機器

- 3.17 否認防止 (Non-Repudiation) : 発生した事象又は行動、並びにそれらを引き起こしたエンティティを証明する能力 (ISO/IEC 27000:2018)

- 3.18 患者危害 (Patient Harm) : 患者の受けた身体的傷害又は健康障害 (ISO/IEC Guide 51:2014 を一部変更)

- 3.19 プライバシー (Privacy) : 個人に関するデータの過度又は違法な収集及び使用に起因する私生活又は個人的事柄に対する侵入がないこと (ISO/TS 27799:2009)

3.20 脅威 (Threat) : セキュリティを侵害し、危害を引き起こし得る状況、能力、行動又は事象が存在する際のセキュリティ違反の可能性 (ISO/IEC Guide 120)

3.21 脅威モデリング (Threat Modeling) : データの破壊、漏洩、改ざん又はサービス拒否の形でシステムに危害を及ぼす可能性のある状況又は事象を明らかにするための調査プロセス (ISO/IEC/IEEE 24765-2017 から変更)

3.22 アップデート (Update) : 医療機器ソフトウェアを対象とした修正、予防、適応又は完全化に関する変更

注記 1: ISO/IEC 14764:2006 に規定するソフトウェア保守活動に由来する。

注記 2: アップデートには、パッチ及び設定変更が含まれる。

注記 3: 適応及び完全化に関する変更は設計仕様時になかったソフトウェアの改良である。

3.23 バリデーション (Validation) : 客観的証拠を提示することによって、意図する使用又は適用に関する要求事項が満たされていることを確認すること (ISO 9000:2015)

注記 1: "バリデート済み"とは、バリデーションが完了している状態を示す。

注記 2: バリデーションは、実環境又は模擬環境で実施される。

3.24 検証 (Verification) : 客観的証拠を提示することによって、規定要求事項が満たされていることを確認すること (ISO/IEC Guide 63)

注記 1: 検証のために必要な客観的証拠としては、検査結果のほか、別法による計算又は文書のレビュー等の結果であることがある。

注記 2: 検証のために行われる活動は、適格性プロセスと呼ばれることがある。

注記 3: "検証済み"とは、検証が完了している状態を示す。

3.25 脆弱性 (Vulnerability) : 一つ以上の脅威によって悪用される可能性のある資産又は管理策の弱点 (ISO/IEC 27000:2018)

4.0 一般原則

本項では、医療機器を開発、規制、使用、監視する際に責任関係者が検討すべき、医療機器のサイバーセキュリティに関する一般指針原則を示す。本ガイドラインの全体を通して述べられている当該原則は、医療機器の全体的なサイバーセキュリティを向上させる

ために重要であり、これに従うことで、患者の安全を確保する上で有益な効果を得られることが期待される。

4.1 国際整合

医療機器のサイバーセキュリティは、国際的に注目されている。セキュリティのインシデントは、診断若しくは治療の過失を引き起こす、機器の安全な性能を脅かす、臨床活動に影響を与える、患者の救急救命の利用を妨げること等によって、世界中のヘルスケアシステムの患者安全を脅かす可能性がある。サイバーセキュリティに対する取り組みの国際的整合は、イノベーションを促進し、安全で効果的な医療機器を遅滞なく患者の治療に使用可能とすると共に、患者安全の維持を確保するために必要である。全ての責任関係者は、医療機器の全ライフサイクルに渡ったサイバーセキュリティ対応を国際整合させることが奨励される。これには、製品設計、医療機器の全ライフサイクルを通じたリスクマネジメント、医療機器のラベリング、規制当局への申請に対する要求事項、情報共有、市販後活動に関する整合化が含まれる。

4.2 製品ライフサイクルの全体

サイバーセキュリティの脅威及び脆弱性に関するリスクは、初期構想段階から EOS に至る、医療機器の製品寿命に関する全ての段階を通して検討することが望ましい。サイバーセキュリティの動的特性を効果的に管理するためには、リスクマネジメントを製品の全ライフサイクルに渡って適用し、設計、製造、試験及び市販後監視等の各過程においてサイバーセキュリティリスクを評価及び緩和することが望ましい。

安全性とセキュリティとのバランスを図ることも必要である。製造業者は、サイバーセキュリティのコントロール及び緩和策を組み込む際、医療機器の安全性及び基本性能を維持することが重要である。

4.3 共同責任

医療機器のサイバーセキュリティは、製造業者、ヘルスケアプロバイダ、規制当局及び脆弱性発見者の共同責任である。全ての責任関係者は、医療機器の全ライフサイクルを通して、潜在的なサイバーセキュリティリスク及び脅威を継続的に監視、評価、緩和、情報共有、対応するため、自らの責任を理解し、他の責任関係者と密接に連携する必要がある。

4.4 情報共有

サイバーセキュリティに関する情報の共有は、安全でセキュアな医療機器を実現するための TPLC アプローチの基礎原則である。サイバーセキュリティの情報を共有するため、全ての責任関係者が、市販前及び市販後に積極的に対応することが奨励される。遅滞なく情報が共有されることによって、全ての責任当事者が、脅威を特定し、関連するリスクを評価し、それに適宜対応するための能力が最大化する。その一環として、全ての責任関係者は、医療機器及び接続するヘルスケアインフラの安全性、性能、完全性及びセ

キュリティに影響し得るサイバーセキュリティのインシデント、脅威及び脆弱性に対する協力及びコミュニケーションを強化するため、情報共有分析機関（Information Sharing Analysis Organizations : ISAOs）に積極的に参加することが奨励される。このような取り組みを行うことで、透明性を向上させることができる。ベストプラクティスとして奨励されるもう一つの情報共有手法として、協調的な脆弱性の開示が挙げられる。また、製造業者のみでなくヘルスケアプロバイダ及び医療機器ユーザにも当該ポリシーを適用することは、エコシステムにとっても有益となり得る。規制当局には、患者安全を国際的に保護し、維持するために、海外の規制当局と情報共有することが奨励される。

5.0 医療機器サイバーセキュリティの市販前考慮事項

医療機器のサイバーセキュリティは、製品の全ライフサイクルに渡って検討することが望ましく、製造業者が医療機器の市販前の設計段階及び開発中に対応すべき重要な要素がある。市販前の要素には、1) セキュリティ機能を製品に組み込むこと、2) 受容できるリスクマネジメント手法を適用すること、3) セキュリティ試験、医療機器をセキュアに運用するためのユーザに対する有益な情報提供及び市販後活動のための計画を立案することが含まれる。製造業者は、前述の市販前要素を検討する際、意図したとおりの利用環境に加え、合理的に予見可能な誤使用のシナリオを検討することが望ましい。以下の各項では、これらの概念を概説すると共に、製品ライフサイクルの市販前段階における製造業者への推奨事項を例示する。なお、医療機器ソフトウェアのライフサイクル活動は、IEC 62304:2006/AMD 1:2015 に規定されている。

5.1 セキュリティ要求事項及びアーキテクチャ設計

脅威モデリング等、設計段階でサイバーセキュリティに積極的に対応することによって、受動的な市販後活動のみを行うよりも患者危害の可能性をより緩和することが可能である。このような設計インプットは、要求事項の捕捉、設計検証試験又は市販前及び市販後のリスクマネジメント対応等、製品のライフサイクルを通じた様々な段階において実施される。

セキュリティ要求事項も、ライフサイクルの設計プロセスの要求事項取得の段階で特定することが望ましい。セキュリティ要求事項及びセキュリティリスクコントロール手段の情報源としては、AAMI TIR 57:2016、IEC TR 80001-2-2、IEC TR 80001-2-8、ISO 27000 シリーズ、NIST 刊行物（セキュアソフトウェア開発フレームワーク（Secure Software Development Framework : SSDF）等）、OWASP 刊行物（設計原則に基づくセキュリティ等）、ENISA 刊行物、米国ヘルスケア及び公衆衛生分野協調協議会（Healthcare and Public Health Sector Coordinating Council : HS2C）合同サイバーセキュリティワーキンググループ（Joint Cyber Security Working Group : JCWG）の刊行物（合同セキュリティ計画等）等がある。

製造業者が自社製品の設計で考慮することが望ましい設計原則を表 1 に示した。但し、表 1 は完全なリストを意味するものではなく、あくまでも例示である。

設計原則	説明
セキュアな通信	製造業者は、医療機器が併用機器又はネットワークと接続される方式について検討することが望ましい。接続方式には、有線接続及び無線通信が含まれる。接続方式の例としては、Wi-Fi、イーサネット、bluetooth、USB 等が挙げられる。
	製造業者は、外部からの入力のみでなく、全ての入力の検証機能を設計することについて検討し、安全性が低い通信以外サポートされていない医療機器や、家庭内ネットワーク又はレガシー医療機器と接続して通信する等、外部環境と通信する場合を考慮することが望ましい。
	製造業者は、医療機器の送受信データ転送を不正アクセス、不正な改変又は反射攻撃から保護する手法について検討することが望ましい。例えば、製造業者は医療機器/システム間通信の相互認証方法、暗号化の要否、既に送信されたコマンド又はデータの不正再送を防ぐ方法、予め定めた時間設定後に通信を切断する適切性等について検討することが望ましい。
データ保護	製造業者は、医療機器に保存される又は送受信される安全性関連データを暗号化等により保護する要否について検討することが望ましい。例えば、パスワードは暗号化によって保護されたハッシュとして保存することが望ましい。
	製造業者は、通信プロトコルのメッセージ制御、シーケンス領域を保護するため又は暗号鍵材料の内容が漏洩することを防ぐために、機密性に係るリスクコントロール手段の要否について検討することが望ましい。
機器の完全性	製造業者は、データの否認防止を確保できる設計特性の要否を判断するために、監査ログ機能のサポート等、システムレベルのアーキテクチャを評価することが望ましい。
	製造業者は、機器のソフトウェアに対する不正な改変等、医療機器の完全性に関するリスクについて検討することが望ましい。
	製造業者は、ウイルス、スパイウェア、ランサムウェア及び他の悪意のあるコードが医療機器で実行されることを防ぐため、マルウェア対策等のコントロールについて検討することが望ましい。
ユーザの認証	製造業者は、医療機器の使用者の検証、様々なユーザの役割に応じたアクセス権付与又は緊急時のアクセス許可等、ユーザのアクセス制御について検討することが望ましい。また、複数の医療機器や顧客の間で同じ認証情報を共有しないことが望ましい。認証又はアクセス許可の例としては、パスワード、ハードウェアキー、生体認証又は他の医療機器では生成

	できない認証信号等がある。
ソフトウェア保守	製造業者は、定期的なアップデートの実施プロセスと展開プロセスを確立し、その情報を共有することが望ましい。
	製造業者は、オペレーティングシステム、サードパーティ又はオープンソースのソフトウェアのアップデート手法及び管理方法について検討することが望ましい。また、製造業者は、ソフトウェアのアップデートや、安全でないバージョンのオペレーティングシステム上で動作する医療機器ソフトウェア等、管理対象外となった古いオペレーティングシステム環境への対処方法計画を立案することが望ましい。
	製造業者は、新たに発見されたサイバーセキュリティの脆弱性に対してセキュアであるために、医療機器のアップデート手法について検討することが望ましい。例えば、アップデートにおけるユーザ介入の要否、医療機器による自動アップデートの要否、アップデートが医療機器の安全性と性能に悪影響を及ぼさないことを検証する方法等に関する検討が含まれる。
	製造業者は、アップデートを実施するために必要な接続について検討すると共に、コードの署名等の方法を用いて接続又はアップデートの真正性を保証する方法について検討することが望ましい。
物理的アクセス	製造業者は、未許可者による医療機器へのアクセスを防止する手法について検討することが望ましい。例えば、ポートを物理的にロックする、ポートへのアクセスを物理的に制限する又は必要な認証なしに物理ケーブルを用いたアクセスを禁止する等の手法を検討することが望ましい。
信頼性及び可用性	製造業者は、医療機器の基本性能を維持するため、サイバーセキュリティ攻撃を検出、防御、対応及び復旧する設計特性について検討することが望ましい。

表1. 医療機器の設計における検討事項に対する設計原則

セキュアな開発の原則は、セキュアな機器設計にとって必要不可欠である。現在の多くのソフトウェア開発ライフサイクルモデル又は関連規格は、この原則をはじめから組み込んでいるわけではない。医療機器ソフトウェアを開発する製造業者は、自社のソフトウェア開発にセキュリティの原則を組み込むことが重要である。製造業者には、製品の全ライフサイクルを通してリスク及び緩和策を評価することで、製品のサイバーセキュリティに関する全体的な対応が求められる。

5.2 TPLC に関するリスクマネジメント原則

セキュリティと安全性に関する健全なリスクマネジメント原則が、医療機器のライフサイクルを通して組み込まれていることが望ましい。医療機器の安全性と基本性能又は臨床活動に影響を及ぼす、若しくは誤った診断又は治療に繋がるサイバーセキュリティリスクについても、リスクマネジメントプロセスにおいて検討されることが望ましい。製造業者は、ISO 14971:2019 に規定されているリスクマネジメント及び AAMI TIR57:2016 や AAMI TIR97:2019 等で規定されているサイバーセキュリティリスクマネジメントを使用して、リスクマネジメントプロセスの一環として以下のステップを踏むことが望ましい。

- サイバーセキュリティの脆弱性を特定する
- 関連するリスクを推定し、評価する
- リスクを受容可能なレベルまでコントロールする
- リスクコントロールの有効性を評価・監視する
- 重要な責任関係者に対する協調的な情報開示を通じて、リスクに関する情報を提供する

セキュリティリスクマネジメントプロセスを図 1 に示した（AAMI TIR57:2016 から引用）。これは、全体的なリスクマネジメントの一部を構成するリスクマネジメントプロセスとして実施できると共に、脆弱性、脅威及びその他のセキュリティ関連用語を対応させて、ISO 14971:2019 のリスクマネジメントプロセスに組み込むこともできる。対応付けについては ISO/TR 24971:2020 の附属書 F を参照すること。

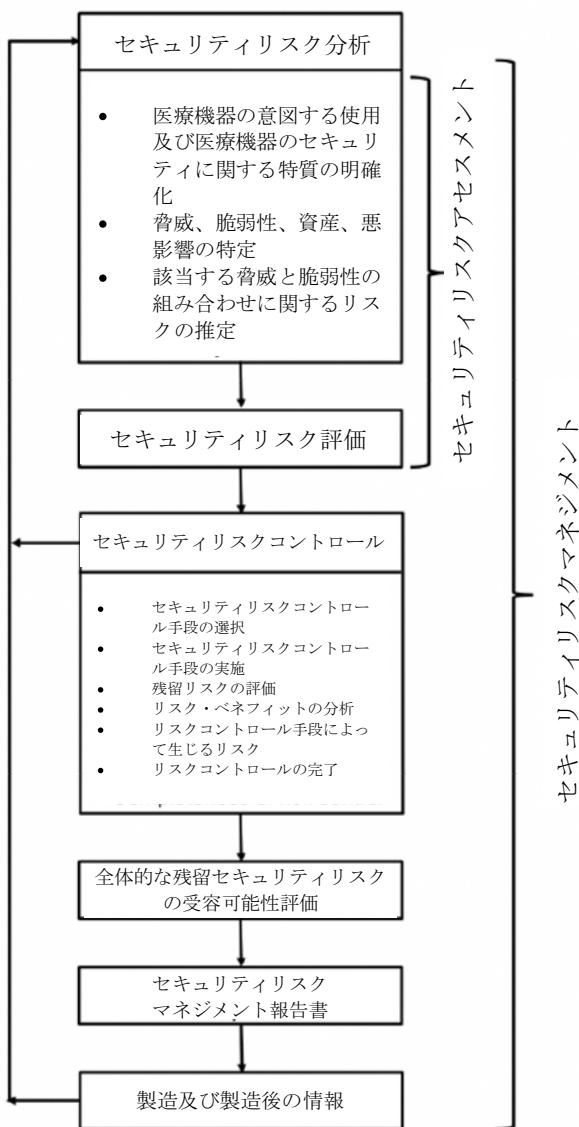


図1. セキュリティリスクマネジメントプロセスの図解
(AAMI TIR57:2016 から許可を得て引用)

医療機器の規制に関するサイバーセキュリティのリスク分析は、サイバーセキュリティの脆弱性の悪用可能性、脆弱性が悪用された場合の患者危害の重大さを考慮して、患者危害のリスク評価に注力することが望ましい。この分析においては、補完的対策及びリスク緩和策についても検討することが望ましい。

リスク評価においては、設計を脅威モデリング、患者危害、緩和策及び検証試験と連結することにより、リスクが適切にマネジメントされるセキュアな設計アーキテクチャを確立することが重要である。この評価では、セキュリティリスク評価、脅威モデリング及び脆弱性スコアリングやその他の手法等、様々なツール及びアプローチが利用できる。

- セキュリティリスクアセスメント：製造業者は、製品の全ライフサイクルを通して、サイバーセキュリティリスク、脅威及び対応について検討することが望ましい。特定されたハザードに対する緩和策の場合、サイバーセキュリティの要求事項は、可能な限り、特定の医療機器のサイバーセキュリティの脅威及び脆弱性と相互参照することが望ましい。
- 脅威モデリング：脅威モデリングは、医療機器やシステムにおける潜在的な脅威によるリスクを特定、列挙、緩和するプロセスである。特に、脅威モデリングには、システムコンポーネント等のサプライチェーンに関連するリスクや、設計、製造、病院環境等への展開、保守に関連するリスク等の検討が含まれる。詳細なシステム設計図の作成は、サイバーセキュリティの設計要素を医療機器に組み込む手法を理解するために有益であると共に、脅威モデリングにとっても有用である。製造業者は、脅威モデルを作成する際、OWASP のガイダンスに基づいて、サイバーセキュリティに関する基本的な 4 つの質問に対する回答について検討することが望ましい。
 - 1) 何を構築しようとしているのか？
 - 2) どのような問題が発生し得るか（どのような攻撃を受ける可能性があるか）？
 - 3) その問題に対してどのように対処するか？
 - 4) 十分な対策を行ったか？
- 必要に応じて、アプリケーションアーキテクチャ、運用データフロー又はより広範囲なシステムレベルの脅威モデリングのコンテキストにおいて、これらの質問を行うこと。医療機器に発生し得る問題を脅威モデリングにおいて判断する場合、製造業者は、ソフトウェア及びハードウェアに対する故意でない誤設定又はインターネットに接続するよう設計されていない医療機器をインターネットに接続する等の悪意のある誤設定を考慮することが望ましい。
- 脆弱性スコアリング：脆弱性スコアリングは、サイバーセキュリティ脆弱性の悪用可能性及び重大さを明確化して評価する方法である。設計開発において特定される既知の一般的脆弱性曝露（Common Vulnerabilities and Exposures : CVE）については、共通脆弱性スコアリングシステム（Common Vulnerability Scoring System : CVSS）又は今後広く採用される可能性が高い脆弱性スコアリングシステム等の一貫性のある脆弱性スコアリングの方法を用いて分析・評価することが望ましい。サイバーセキュリティリスク、脆弱性スコアリング及びコントロール手段は新製品の脅威モデリング及びセキュリティリスクアセスメント、並びに故障モード影響解析（Failure Mode and Effects Analysis : FMEA）等、サイバーセキュリティに特化していない他のリスク評価ツールに対して情報を提供するために使用される可能性がある。

既存の ISO 14971:2019 リスクマネジメントプロセスにセキュリティリスクマネジメントプロセスを組み込む場合、脅威モデリングや脆弱性スコアリング等のセキュリティ対応を考慮することが望ましい。

5.3 セキュリティ試験

製造業者は、設計開発プロセスの検証及びバリデーションの段階において様々な種類のセキュリティ試験を採用することにより、重大な既知の脆弱性がコードに含まれていないことを証明すると共に、セキュリティコントロールが効果的に実施されていることを証明することが望ましい。当該試験では、医療機器が使用される状況、並びに医療機器がその他の機器又はネットワークに接続される環境を考慮することが望ましい。ソフトウェアの仕様適合性を確保し、異常を最小化するために、ソフトウェアの検証技術を適用することが推奨される。医療機器が、悪用され得る既知の脆弱性に対して検証済みであることを明確化することも重要である。これを行うために、ソフトウェア試験や攻撃シミュレーション等、セキュリティ評価プロセス又は受入確認を対象となる医療機器に適用することが望ましい。セキュリティ試験とは、セキュアな開発フレームワークを構成するコンポーネントの一つである。試験に関する検討事項の詳細は、5.1 項に示す規格及び情報源を参照すると良い。製造業者が考慮すべき上位レベルの考慮事項を以下に例示する。

- 開発時においても、既知の脆弱性又はソフトウェアの弱点について、ソフトウェアコンポーネントとモジュールのターゲット検索を実施する。定期的なセキュリティ試験としては、静的コード解析、動的解析、堅牢性試験、脆弱性スキャン、ソフトウェアコンポジション解析等が挙げられる。
- 侵入テスト等の技術的なセキュリティ分析を実施する。技術的なセキュリティ分析としては、ファズテスト等を用いた未知の脆弱性の特定又は隠しファイル、設定、データストリーム、若しくはハードウェアのレジスタの読み出し等による代替エントリポイントのチェック等が挙げられる。
- 脆弱性評価を行う。脆弱性評価としては、バリアント解析等、自社の他製品に対する脆弱性の影響分析、対抗手段の特定、脆弱性の修正又は緩和等が挙げられる。

5.4 TPLC サイバーセキュリティマネジメント計画

サイバーセキュリティの脅威が継続的に進化している中、製造業者は、製品ライフサイクルの全体を通じたサイバーセキュリティマネジメント計画の一環として、脆弱性及び悪用を積極的に監視、特定、対応することが望ましい。製品開発の市販前段階で計画を作成することが望ましい。また、理想的には、製造業者の組織全体でその計画を維持することが望ましい。この計画では以下に示した項目を取り扱う。

- TPLC を通じた監視：新たに発見されたサイバーセキュリティの脆弱性を積極的に監視・特定すると共に、その脅威を評価して適切に対応するための計画

- 脆弱性の開示：脆弱性発見者からの情報を集約した上で、緩和及び修正策を開発し、脆弱性の存在及び緩和又は修正方法を責任関係者に開示するための正式なプロセス
- アップデート及び脆弱性の修正：医療機器の安全性及び性能を継続的に維持するための、定期的な、若しくは特定された脆弱性に対するソフトウェアのアップデート又は修正作業の実施
- 復旧：製造業者、ユーザのいずれか又は両者が、サイバーセキュリティのインシデント後に、医療機器を通常の運用状態に戻すための復旧計画
- 情報共有：セキュリティの脅威及び脆弱性に関する更新した情報を共有する ISAO 又は情報共有分析センター（Information Sharing and Analysis Centers : ISAC）への参加

5.5 ラベリング及び顧客向けセキュリティ文書

5.5.1 ラベリング

ラベリングは、関連するサイバーセキュリティリスクを考慮して該当するセキュリティ情報をエンドユーザーに伝達するものである。ラベリングには、以下に示した項目を含めることが望ましい。

- アンチマルウェアソフトウェア、ネットワーク接続設定、ファイアウォールの使用等、意図する使用環境に適した推奨されるサイバーセキュリティコントロールに関する医療機器の使用方法及び製品仕様
- 正常な機能を回復するための、バックアップ並びに復元の機能及び手順の説明
- データを送受信するネットワークポート及びその他のインターフェースのリスト、並びにポート機能、着信・発信ポートの説明。但し、未使用ポートは無効化することが望ましいことに留意する。
- エンドユーザー向けの詳細なシステム構成図

5.5.2 顧客向けセキュリティ文書

取扱説明書に加えて、製造業者が提供する医療機器のインストール及び設定に係る技術文書、並びに運用環境のための技術的要件事項は、ユーザが医療機器を安全でセキュアに使用する上で特に重要である。顧客向けセキュリティ文書については、以下に示した項目を含めることが望ましい。

- 意図したとおりの医療機器の動作を確保するための、支援インフラの要求事項に関するユーザへの具体的なガイダンス

- セキュアな設定を用いた機器の強化あるいは強化可能性に関する説明。セキュアな設定とはマルウェア対策、ファイアウォール/ファイアウォール規則、ホワイトリスト、セキュリティイベントパラメータ、ロギングパラメータ、物理的セキュリティ検出等のエンドポイント保護を含む。
- 必要に応じて、セキュアなネットワーク接続の展開及びサービスを可能にするための技術的指示、並びにサイバーセキュリティ脆弱性又はインシデントが検知された際の対応方法に関するユーザへの指示
- セキュリティ事象が検出された場合に、医療機器又は支援システムがユーザに異常を通知する方法に関する説明。セキュリティ事象の種類としては、設定変更、ネットワーク異常、ログイン試行、未知のエンティティに対する要求送信等の異常トラフィックが挙げられる。
- 認証された特権ユーザが、医療機器の設定を保存し、回復するための方法の説明
- 許可されたユーザが、製造業者からアップデートをダウンロードしてインストールするための体系的な手順の説明。必要に応じて、セキュリティ設定又は使用環境を変更することで生じるセキュリティリスクとその影響についても説明する。
- 医療機器のサイバーセキュリティサポート終了に関する情報（6.6 項「レガシー医療機器」参照）
- 医療機器に実装される商用、オープンソース及び市販のソフトウェア部品のサイバーセキュリティに関する情報及びサポートをオペレータに提供するためのソフトウェア部品表（Software Bill of Materials : SBOM）。名前、作成元、バージョン、ビルド番号によって各ソフトウェア部品が特定されるため、SBOM を使用することで、必要とされる透明性が確保される。SBOM は、患者及びヘルスケアプロバイダを含む医療機器のオペレータが、その資産及び関連するリスクを効果的に管理し、医療機器及び接続されるシステムに対して特定された脆弱性の潜在的影響を理解し、医療機器の安全性及び基本性能を維持するための対応を可能にする。医療機器のオペレータは、SBOM を使用することにより、脆弱性が潜んでいる可能性があるソフトウェアの特定、要件の更新及び適切なセキュリティリスクマネジメントの実施を医療機器製造業者と協力して促進することができる。SBOM を使用することにより、アプリケーションで使用されているコンポーネントを可視化して顧客に提示できると共に、潜在的セキュリティリスクを特定できるため、購入決定に必要な情報を提供することが可能となる。製造業者は、SBOM の展開で使用される形式、構文、マークアップに関する業界のベストプラクティスを活用することが望ましい。SBOM によって医療機器に関する機密情報が公開されるため、信頼できるコミュニケーションチャネルを通じて SBOM を配布することが奨励される。オペレータへの SBOM 配布方法の信頼性は製造業者が決定する。

5.6 規制当局への申請に関する文書

製造業者は、上項に概説した対応に加えて、サイバーセキュリティに関する自社の活動を明確に文書化し、要約することが望ましい。規制当局は、医療機器のクラス分類に応じて、サイバーセキュリティ対応に関する文書を市販前又は市販後の段階で要求する可能性がある。規制当局が市販前承認のためにサイバーセキュリティ文書を要求する場合、製造業者は、サイバーセキュリティに関連して、医療機器の設計機能、リスクマネジメント活動、検証試験、ラベリング及び製品の全ライフサイクルに渡って新たに発生する脅威を監視し、対応するための計画の根拠を明確に記載した文書を提出することが望ましい。これらの詳細については、下項で説明する。

5.6.1 設計文書

全てのインターフェース又は通信経路又はコンポーネント（ハードウェア及びソフトウェア）、患者危害に関するサイバーセキュリティのリスクを緩和するために、アクセスコントロール、暗号化、セキュアなアップデート、ログ機能、物理的セキュリティ等に関する対策を選択した根拠及び推定を中心として、5.1 項で概説した全ての設計機能を記載した文書である。

5.6.2 リスクマネジメント文書

サイバーセキュリティの脅威及び脆弱性、関連するリスクの推定、リスクを緩和するために行うリスクコントロール、並びにリスクコントロールが適切に検証されたことを示す根拠を明確に説明する文書である。製造業者は、その他の安全性に過度な影響を与えることなく、医療機器のサイバーセキュリティを最大化するリスクコントロールについて検討することが望ましい。特に、規制当局に提出するサイバーセキュリティに関するリスクマネジメント文書では、明確な説明を心掛けると共に、リスクマネジメント規格（AAMI TIR57:2016、AAMI TIR97:2019 等）をガイダンスとして利用することが望ましい。この成果文書を全体的なリスクマネジメントの入力として利用できるように、ISO 14971:2019 で規定されている全体的な要件に従って成果文書を作成することが望ましい。サイバーセキュリティに関するリスクマネジメント文書には、以下のような文書がある。

- リスクマネジメント報告書やセキュリティリスクマネジメント報告書等の包括的なリスクマネジメント文書。これらの文書には、脅威モデリング及び特定されたサイバーセキュリティの脅威について記載することが望ましい。
- その他のリスクマネジメントに与えるセキュリティリスク緩和策の影響に関する考察

5.6.3 セキュリティ試験の文書

医療機器のセキュリティ及び全てのセキュリティコントロールの有効性を検証するために実施した全ての試験を要約した試験報告書である。5.3 項に記載したソフトウェアコ

ンポーネント又はサブシステムと既知の脆弱性データベースとの相互参照等、特定の試験に係る詳細のほか、試験報告書には、以下の事項を記載することが望ましい。

- 試験方法、結果及び結論の説明
- セキュリティリスク、セキュリティコントロール、並びにセキュリティコントロールの検証試験のトレーサビリティマトリクス
- 使用した規格及び内部 SOP/文書の参照

5.6.4 TPLC サイバーセキュリティマネジメント計画に関する文書

医療機器の全ライフサイクルを通して安全性及び性能を継続的に保証するための市販後プロセスに係る保守計画の要約である。5.4 項に記載したとおり、このプロセスとしては、TPLC 監視、計画的又は修正のためのアップデート、協調的な脆弱性の開示ポリシー及び情報共有が挙げられる。

5.6.5 ラベリング及び顧客向けセキュリティ文書

5.5 項において概説した医療機器の意図する使用環境下でユーザがリスクを効果的に管理するための関連情報を含む、サイバーセキュリティに関する全ての情報を収載したユーザ文書である。

6.0 医療機器サイバーセキュリティの市販後考慮事項

脆弱性は時間経過に伴って変化するため、市販前の設計段階で実施したセキュリティ対応は、リスクが受容可能な状態を適切に維持できない可能性がある。そのため、様々な責任関係者がそれぞれの役割を果たす市販後のアプローチが必要になる。市販後アプローチは、意図する使用環境における医療機器の運用、情報共有、協調的な脆弱性の開示、脆弱性の修正、インシデントへの対応及びレガシー医療機器等を含む様々な要素に及んでいる。製品のライフサイクルの市販後プロセスに関する全ての責任関係者へ向けた推奨事項として、これらの要素について下項で概説する。

6.1 意図する使用環境における機器の運用

6.1.1 ヘルスケアプロバイダ及び患者

- a. ヘルスケアプロバイダが採用すべきサイバーセキュリティのベストプラクティス

医療機器のサイバーセキュリティは共同責任であり、ヘルスケアプロバイダを含む全ての責任関係者の参画が必要である。ヘルスケアプロバイダは、自身の IT インフラに接続される医療機器の安全性、性能及びサイバーセキュリティに対応するために、リスク