医療機器メーカーの海外進出とデジタルヘルスケアサービス事業者に求められるサイバーセキュリティ対応

長谷川ちひろ

CONTENTS

要　約

1　医療機器がIT化、ネットワーク化してサイバー攻撃の脅威が高まっていることから、各国・地域は医療機器に販売流通規制を設けている。欧米では、市販前と市販後の製品ライフサイクルにわたり、サイバーセキュリティ対応を行うことを医療機器メーカーに求めている。

2　医療機器メーカーがサイバーセキュリティ関連の要求事項に対応する際には、機能安全面でのセーフティリスクと関連づけて検討することが肝要である。さらに、積極的な海外展開を見据え、要求事項への対応を製品横断的に自社で標準化していくことが望ましい。

3　医療機器のみならず、PHRによる健康増進など、より多面的に「デジタルヘルスケア」としてのサービス普及が予想される。デジタルヘルスケアサービス事業者においても、人々の健康情報を取り扱うという事業の性質上、サイバー攻撃による情報漏洩をはじめとするサイバーセキュリティリスクを整理し、適切な対応を図らなければならない。

4　本論考は医療機器やデジタルヘルスケアを対象とするものであるが、ここで紹介するセーフティとセキュリティリスクの相関やリスクマネジメントの具体的な手法などの内容は、IoTデバイスや個人情報を活用するサービスのセキュリティリスク対応方針・具体策を検討する事業者に向けても有益なヒントとなるだろう。

Ⅰ 医療機器とサイバーセキュリティ

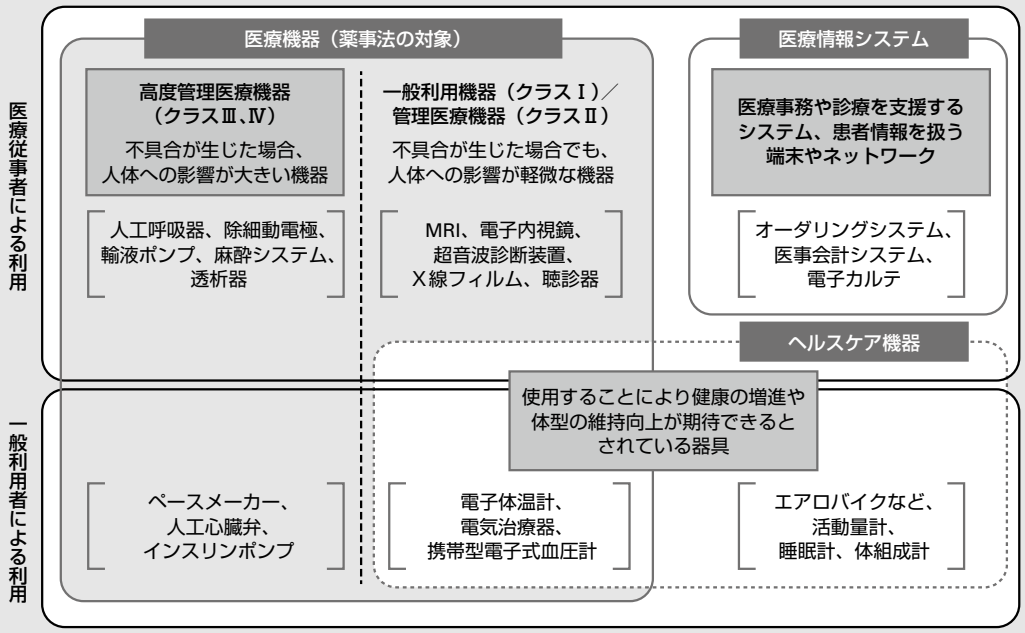
従来のヘルスケアは主に医療従事者による病院内での検査や治療が中心であった。しかし、昨今では医療情報システムにおいて電子カルテなどの医療事務や診療を支援するシステムのみならず、何らかの形で患者の情報を保有するシステムや、遠隔で患者の情報を閲覧・取得するシステム、スマートデバイスなどもその範疇に含まれ[注1]、活用の幅を広げている。

医療情報システムの領域は、近年、急速に拡大・進化している。たとえば、個人の診療情報を生涯にわたって電子媒体に記録し、情報を各医療機関の間で共有・活用するEHR（Electronic Health Record）や日々の体重や血圧などの身体情報や生活習慣を個人が管理するPHR（Personal Health Record）などでは、幅広いシーンでの活用が見込まれ、病院内での検査や治療にとどまらず、病院外での利用により個々人の予防や健康維持まで影響を与えている。

また、医療情報システムと医療機器やヘルスケア機器との連動も活発化している。これまで単体で機能する装置であった医療機器やヘルスケア機器は、近年の技術の進歩により、医療施設の院内ネットワークやインターネットを通じたクラウドサービスなどに接続し、医療情報システムとの連動機能付医療機器やIoTヘルスケア機器などとして広く利用され始めている（図１）。

これらの技術の進歩は、医療の質の向上や業務の効率化などのメリットをもたらす一方で、サイバー攻撃などの新たな脅威に対応する必要性を生じさせている。

図1　医療機器およびヘルスケア機器、医療情報システム



出所）独立法人 情報処理推進機構「医療機器における情報セキュリティに関する調査」より作成

医療情報を狙った攻撃として、2018年にシンガポール政府の医療データベースがサイバー攻撃を受け、首相含む150万人の医療情報が盗まれる事件が起こった[注2]。また、20年にはドイツのデュッセルドルフ大学病院でランサムウエア攻撃が発生し、救急患者の受け入れ停止を余儀なくされた。当病院で救命処置を受ける予定であった患者は約32km離れた工業都市ヴッパータールの大学病院へ搬送されたが、その後死亡したと報道された[注3]。11年には、通信技術を持つ医療機器への脅威も報じられている。患者の体内とつながるインスリンポンプに対し、悪意のある攻撃者が無線通信経由で誤った命令を実行することで、患者の体内に注入するインスリンの量を故意的に調整できる脆弱性が発見された[注4]。

このような新たな脅威はなぜ顕在化してしまったのか、医療機器の事例を解説する。従来、単体で動作していた医療機器および検査室や手術室内に閉じていた医療機器の通信が、病院内ネットワークもしくはインターネットに接続されることにより、サイバー攻撃を受ける可能性が高まっていることが要因の一つである。また、開発の効率化や機能追加時の利便性などの理由から、WindowsやLinuxなどの汎用OSを用いて開発を行うケースも増加傾向にあり、OSやソフトウエアの脆弱性を突かれたサイバー攻撃を受ける可能性が生じることも要因となっている。昨今のヘルスケアの技術利活用やその波及に伴って、これまで医療機器の性質上考慮する必要のなかった脅威が、ほかのインターネット接続デバイスと同等に顕在化している状況にあるといえる。

各国・地域は、ヘルスケアに関連するこれらの患者情報の漏洩リスクや患者へ被害を及ぼす可能性を最小化するために、医療機器メーカーが販売する医療機器のサイバーセキュリティレベルが担保され、継続的に維持・向上されるように促す仕組みの構築を目指し、法律や規則によって統制・整合を図っている。現在、医療機器メーカーに求められるサイバーセキュリティ関連の要求事項は国・地域ごとに制定されていることから、海外展開が進んでいるわが国のメーカーにおいては、製品の仕向け地ごとに要求事項を確認し、対策を適用する必要がある。

以降、医療機器の市場として規模が大きく、法規制や申請制度の整備・運用が進んでいる欧州と米国に焦点を当て、医療機器メーカーに求められるサイバーセキュリティ関連の要求事項や対応例を述べる。

Ⅱ 欧州・米国における医療機器流通規制

1 欧州で適用される流通規制とは

従来、欧州で流通する医療機器およびその付属品に適用される三つのEU指令が定められていた。これらのEU指令が2017年に二つのEU規則に移行し、規則化されたことで強制力が強まり、適合のためにより踏み込んだ対応が求められるようになった。

医療機器メーカーは欧州で販売を行う際に、対象の医療機器がこれらのEU規則に適合しているとの承認（CEマーキング）を得ることが必要となる。

EU規則の医療機器規則（以降MDR）と体外診断用医療機器規則（以降IVDR）の対象差分は、医療機器が人体に触れるか否かであ

表1　欧州で適用される流通規制

EU指令 原則として、加盟国内で直接適用されるわけではない	EU規則 加盟国内で直接適用	対象
• 医療機器指令（**MDD**） （Medical Device Directive 93/42/EEC） • 能動埋込医療機器指令（**AIMDD**） （Active Implantable Medical Devices Directive 90/385/EEC）	• 医療機器規則（以降**MDR**） （Medical Device Regulation EU 2017/745）	人体に触れる機器
移行		
• 体外診断用医療機器指令（以降**IVD**） （In Vitro Diagnostic Medical Device Directive 98/79/EC）	• 体外診断用医療機器規則（以降**IVDR**） （In Vitro Diagnostic Regulation EU 2017/746）	人体から取り出した検体を検査する機器

る。また、医療機器のクラスによって求められる要求事項が異なるため、医療機器メーカーが欧州で製品販売を行う際には、該当製品がMDRとIDVRどちらに属するのかを含めクラス分類を確認し、それぞれで求められる要求事項に対応し適合の承認を得なければならない（表1）。

2　欧州販売申請のサイバーセキュリティ要求であるMDCGガイダンス

MDR、IVDRの主な要求事項は医療機器の品質マネジメントシステム（QMS）を含む機能安全（以降「セーフティ」）に関する内容であるが、その土台にはリスクマネジメントという切り口からサイバーセキュリティの要求事項が加わっている。MDRとIVDRの付録Ⅰにおいてセーフティの観点からリスクマネジメントプロセスの実行を求めているが、これに紐づく形でサイバーセキュリティに関連する内容を提供しているのが「MDCG 2019-16 Guidance on Cybersecurity for medical devices」（以降「MDCGガイダンス」）である。

MDCGガイダンスは、欧州委員会（EC）が議長を務める医療機器調整グループ（MDCG: Medical Device Coordination Group）によって策定された。MDRの第105条では「規則全体の実施確保を目的とするためのガイダンスはMDCGが提供する」と位置づけられており、医療機器メーカーがMDR、IVDRに適合するために必要なサイバーセキュリティに関連する要求事項はMDCGガイダンスを参照する必要がある。

3　米国で適用される流通規制とは

医療機器をアメリカで販売する際、法律（FD&C法）にのっとり米国食品医薬品局（以降FDA：Food and Drug Administration）へ申請し承認を得る必要があるが、サイバーセキュリティに関するFDAからの要求事項は以下の二つの文書（以降「FDAガイダンス」）に記されている。

- Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff（2022年4月）

- Postmarket Management of Cybersecurity in Medical Devices（2016年12月）

欧州でMDRとIVDRどちらに属するかクラス分類を確認する必要があるように、FDAへの販売申請の際にもクラス分類を確認する必要がある。ただし、欧州では体内に触れるか否かで区別可能なクラス分類であるのと異なり、FDAでは使用目的やサイバーセキュリティに関連する患者へのリスクに応じてクラス分類を行う必要がある。

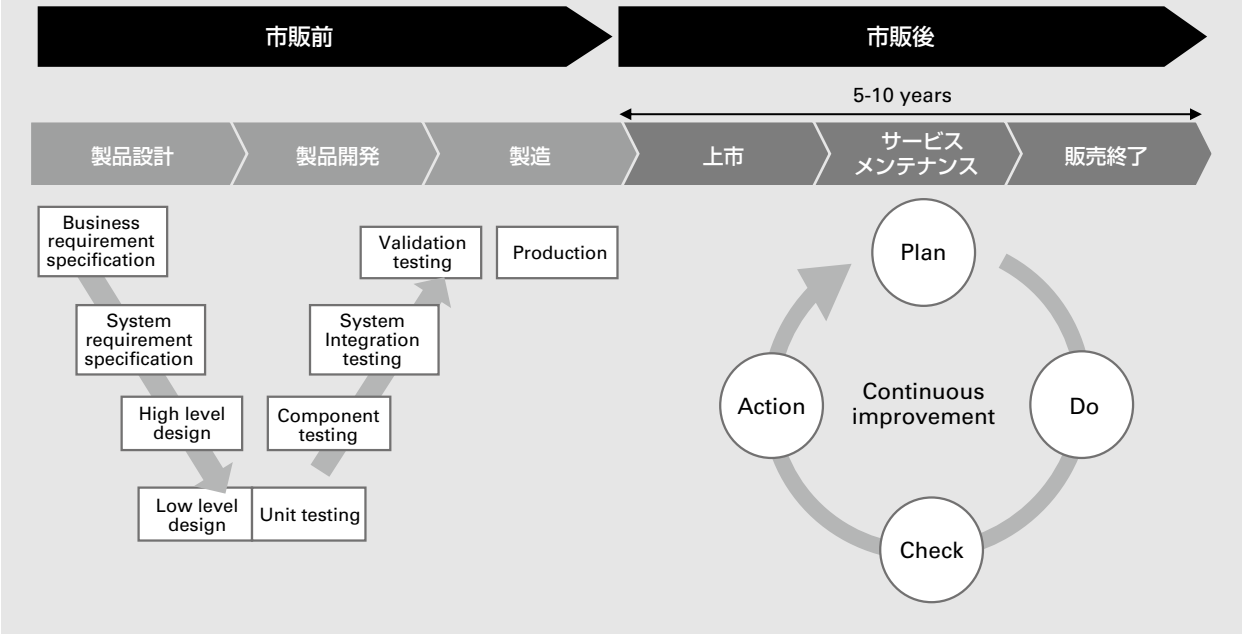
FDAガイダンスではサイバーセキュリティに関してTier1／Tier2の二層に分類されており、Tier1は高いサイバーセキュリティリスクがあるもの、Tier2は標準的なサイバーセキュリティリスクがあるもの、とされている。Tier1／Tier2で要求される事項が異なるため、まずは申請対象となる医療機器がどの分類に位置づけられるのかを整理することが必要である。

4 米国販売申請のサイバーセキュリティ要求である市販前・市販後FDAガイダンス

FDAではサイバーセキュリティに関して市販前と市販後のガイダンスを発表している。市販前には設計段階からサイバーセキュリティについて考慮し、設計プロセスにサイバーセキュリティの観点を組み込むことが求められる。また、市販前にFDAへの提出を推奨する項目が記載されており、主に、設計要件、ラベリング要件、設計機能に関する文書、リスクマネジメント文書について対応する必要がある。

市販後には、製品のライフサイクルにわたりサイバーセキュリティについて考慮することが求められる。たとえば脆弱性管理やソフトウエアのアップデートについて、医療機器の一般的な寿命である５～10年を想定して対応する仕組みを構築し、脆弱性や攻撃動向を

図2　市販前・市販後のサイバーセキュリティ対応



継続的にモニタリングした上で対処する必要があるとされている。市販前のみならず市販後も、継続的・長期的にサイバーセキュリティについて対応することが求められている（図２）。

5　市販前と市販後で分離されるサイバーセキュリティ要求

MDCGガイダンスとFDAガイダンスでは共通して市販前と市販後に観点を分け、要求事項を示している。市販前と市販後に分離されている理由は、セーフティとサイバーセキュリティとのリスクの考え方の違いにある。

従来から医療機器で考慮されていたセーフティのリスクにおいては、市販前に安全性を高める要件を機器に適用させることで、市販後においては、経年劣化による緩やかな安全性の低下以外にはリスク増大は考えにくかった。対して、サイバーセキュリティのリスクは、市販前にセキュリティレベルを高める対策を適用したとしても販売後に新たに脆弱性が発見され、リスクが急激に増大する可能性がある。

そのため、医療機器の脆弱性の調査や評価を継続的に行い、サイバーセキュリティを含めた保守体制やインシデント対応体制を維持・運用し続けることが求められる。医療機器メーカーのセキュリティ対応は上市で終了せず、製品のライフサイクル全体を通じて継続することが明確に求められているのである。

Ⅲ　サイバーセキュリティ要件のグローバル統一化動向

医療機器に対するサイバーセキュリティに関する要求事項は、現在、国や地域で各自に設けているという状況である。この状況を踏まえ、国際医療機器規制当局フォーラム（以降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および実践」、以降「IMDRFガイダンス」）が取りまとめられた。

IMDRFガイダンスの内容は、FDAの市販前および市販後ガイダンスを基本としつつ、医療機器のサイバーセキュリティに対する世界的に調和の取れたアプローチを促進するために、医療機器のサイバーセキュリティのガイダンスを提供している。

欧州のMDCGガイダンスでは、インシデント発生時の報告や根本原因のサイバーセキュリティコードに関する整理方法について５章でIMDRFガイダンスを参照するよう紐づけされている。また、６章ではIMDRFのワーキンググループが開発中の「the Medical Device Cybersecurity Guide」（医療機器サイバーセキュリティガイド）を参照することが重要と明記されている。

わが国においても、2020年に厚生労働省が医療機器メーカーに対して、今後三年程度をめどにIMDRFガイダンスの導入するよう検討を行っていると公表している[注5]。

IMDRFガイダンスにはグローバルハーモナイゼーションについてうたっている章もあり、各国の規制機関担当者が執筆に関与していることから、今後、このガイダンスが主要国における医療機器のサイバーセキュリティガイドラインとして統一的に採用されていく可能性も十分に考えられる。しかし、統合は

数年先の見通しとなるため、まずは販売先の国・地域の要求事項について、同書の内容を参考に自社でできるところから対応を進めることが推奨される。

Ⅳ 医療機器メーカーで実施すべき対応

では、欧州・米国のサイバーセキュリティ要求事項に対応するために、医療機器メーカーはどのような取り組みを行うべきか、四つの対応例を示す。

1 自社対策状況とのFit&Gap

前章で紹介した各国・地域の文書で示されているサイバーセキュリティ要件に対して自社が現状どのくらい対応できているのか、各国・地域で販売承認を得るにはどこを強化する必要があるのか、自社の状況を可視化するためにFit&Gapを実施する（図３）。

2 不足事項への対応

Fit&Gapの結果、不足する事項として抽出された要件へ対応を行う。各国・地域が求める要求事項への四つの対応策を例示する。

（1） リスク分析手法例

MDCGガイダンス・FDAガイダンスではサイバーセキュリティの観点でリスクマネジメントプロセスの実行を要求している。リスクマネジメントプロセスの一つであるリスク分析の手順を提供するガイドライン・規格であるNIST SP 800-30とAAMI TIR57を例にとり、二つの文書で示されているリスクモデルおよび脅威指向型アセスメントアプローチを採用した場合のリスク分析手法を紹介する。

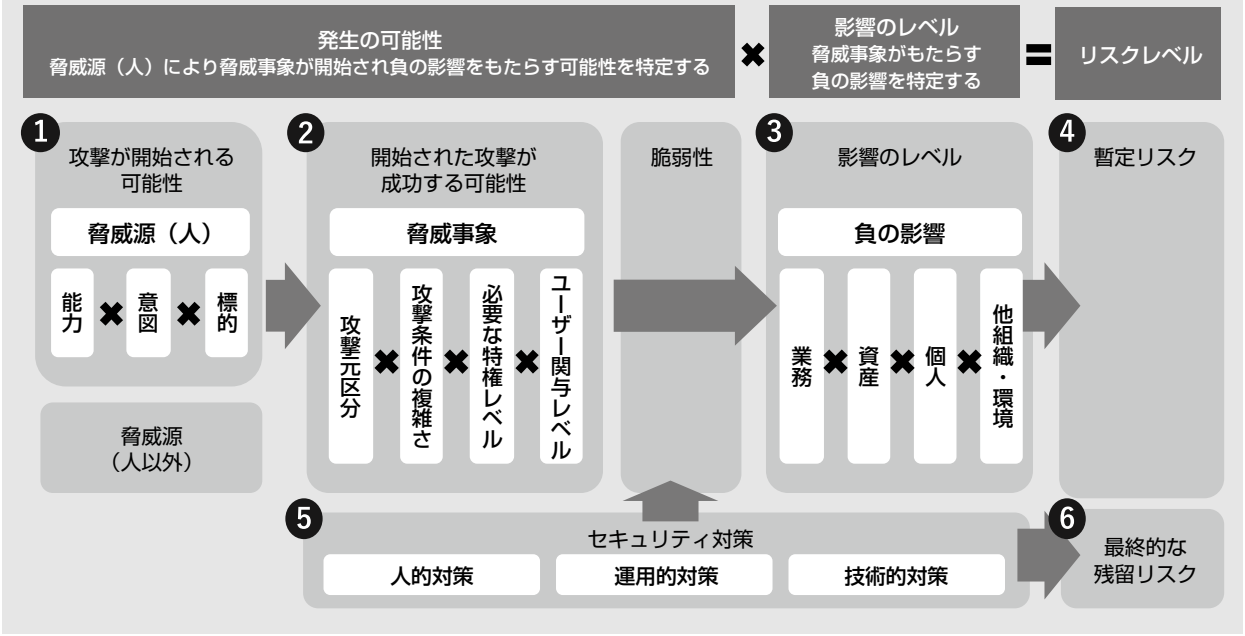
- 製品の使用環境（インターネット接続の有無など）や製品を扱うことのできる人物（医療従事者や悪意のある第三者など）から、脅威源や脅威事象を整理し脅威が発生する可能性を特定する（図４①②）

図3　自社対策状況とのFit&Gap例

各国が求めるサイバーセキュリティ要件 → 自社対策状況

MDCGガイダンスにおける要求事項		FDAガイダンスにおける要求事項			自社対策	
項	要求事項	Pre	Post	要求事項	対応ステータス	文書名
3.1.	製造者は、セキュリティ管理を実施する。製品のライフサイクルを通じて、セキュリティ関連の活動が適切に計画され、文書化され、実行されるようにする		✓	医療機器のサイバーセキュリティに関連する危険を特定して、関連リスクを査定して評価し、それらのリスクを管理し、その効果を監視するため、現在進行中の医療機器ライフサイクルをメーカーは確立し、文書化し、全般通して維持しなければならない	制定済み	・サイバーセキュリティリスクマネジメント規格 ・サイバーセキュリティリスクマネジメントシート

図4　リスク分析手法例



- 製品が保持する情報（患者情報など）や製品の使用方法（体へ機器を挿入するなど）から、脅威がもたらす負の影響を特定する（図4③）
- 脅威が発生する可能性と影響のレベルから暫定リスクを算出し、閾値を参考にサイバーセキュリティ対策の要否を判断する（図4④）
- リスクを低減するためのサイバーセキュリティ対策を選択し、対策実施後の残留リスクを算出する（図4⑤⑥）

残留リスク算出後は、リスク値低減のための対策がきちんと実装されたのか確認できるよう、設計書やテスト結果などとのトレーサビリティを確保する。また、市販後にも新しい脅威が生じていないか、リスク値は閾値を下回っている状態を維持しているか、リスクマネジメント結果を用いて継続的に確認することが求められる。

(2) ソフトウエア要件の整理例

医療機器に実装すべきソフトウエア要件として、たとえばFDAガイダンスでは、認証・暗号化・ログの取得などが求められている。医療機器メーカーは、MDCGガイダンスやFDAガイダンスの示すソフトウエア要件を医療機器に実装する必要がある。しかし、たとえば、パスワードの桁数や試行回数制限数など、医療機器メーカーがどの程度の強度の認証機能を実装すべきなのか、開発設計に参考となり得る具体的な要件はこれまでに述べた文書類では示されていない。パスワードポリシーであれば認証に関するガイドラインである「NIST SP800-63B」、個別のOSのサイバーセキュリティ設定であれば、システムを安全に構築するためのベストプラクティスである「CIS Benchmarks」など、より具体的な要件は関連するガイドライン・ベストプラクティスを参照することが有効な手法である。

（3） 脆弱性の管理例

前述のとおり、５～10年の医療機器のライフサイクルにわたるリスクマネジメントの一環として、サイバーセキュリティの脆弱性や攻撃をモニタリングし、評価し、対処する必要がある。定量的に脆弱性の影響の大きさや深刻度を評価するためにはCVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）などを参考とし、オープンで汎用的な評価を基に脆弱性への対応要否を検討するのも有効な手法の一つである。

（4） 利用者への情報開示例

FDAでは、医療機器の想定使用環境やシステム図、製品仕様を利用者に対して提供することを求めている。そのほかにも、利用者側での実施が推奨されるサイバーセキュリティ対策や、脆弱性またはインシデント検出時における利用者側での対応方法、医療機器のサポート終了に関する情報などの提供を求めている。

利用者への情報開示は、市販後のリスクマネジメントの結果で導出されたサイバーセキュリティ対策やソフトウエア要件を市販後の医療機器へ適用させる場合も有効な策となり得る。たとえば、パスワードの定期的な変更をシステム上で強制する対策など、開発段階から組み込むべき技術的な対策は、市販後に医療機器に実装させることが難しい。一度上市した製品に、事後に設計変更などを伴うセキュリティ対策を行うのは多大なコスト・手間が生じる可能性がある。このような対策がリスクマネジメントの結果導出された場合において、残存するリスクや利用者側で行える代替策（定期的な変更を利用者に依頼するなど）を伝え、利用者へ情報開示することは、残存リスクを低減するリスクコントロール策の一つとして医療機器メーカーの方策になり得る。

3 セーフティリスクを考慮したサイバーセキュリティリスクマネジメント

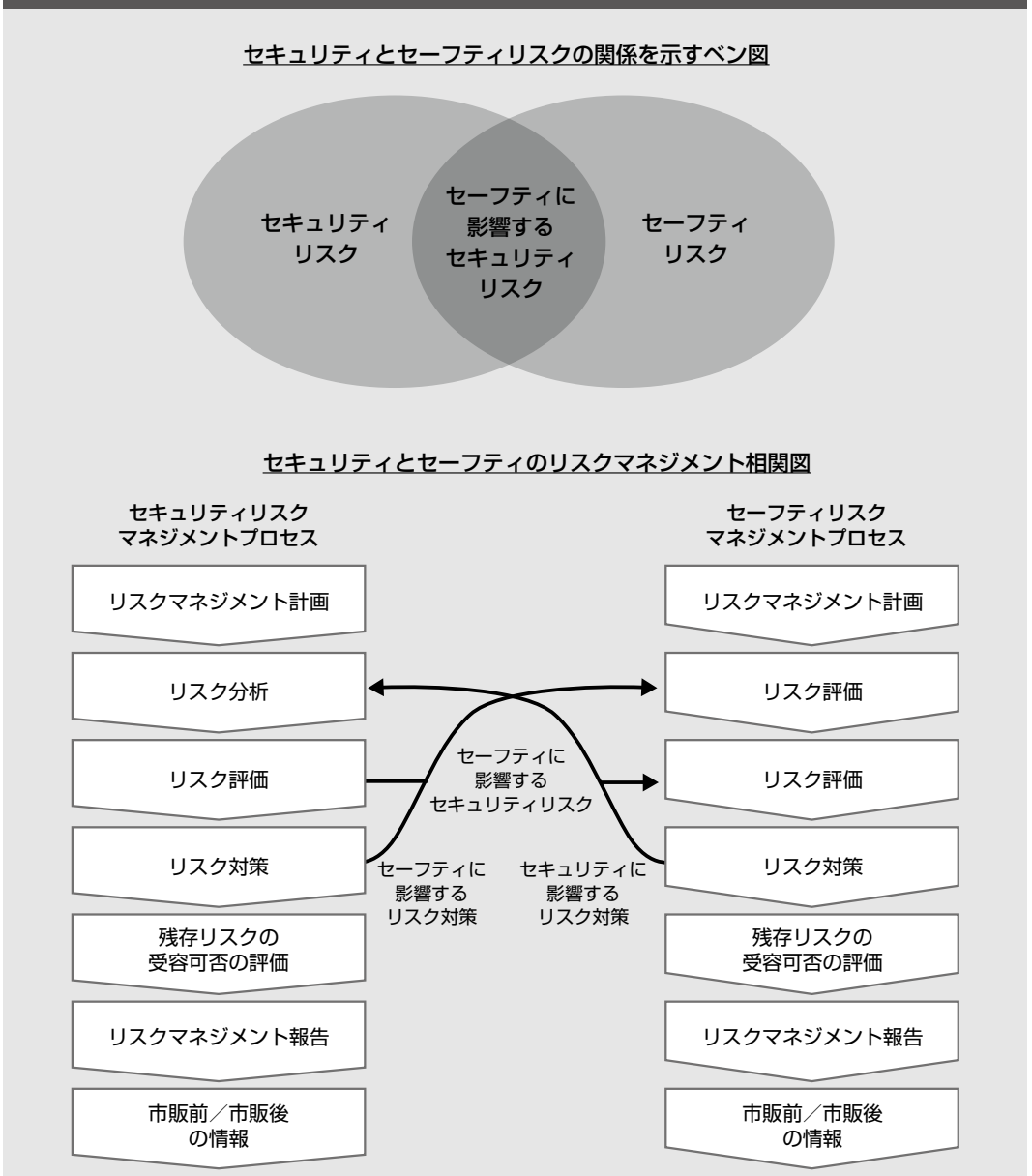
ほとんどの医療機器メーカーでは医療機器リスクマネジメントの国際規格であるISO14971などを根拠として、セーフティの文脈からリスクマネジメントプロセスを構築しているケースが想定される。しかし、各国・地域の文書が求めるサイバーセキュリティ観点からリスクマネジメントを行う医療機器メーカーはいまだ少数であろう。

MDCGガイダンスでは、サイバーセキュリティリスクでありながら、セーフティ側にも影響があり得るリスクの存在やリスクマネジメントプロセスの相関について示している（図５）。このサイバーセキュリティとセーフティの考え方は欧州独自のものではなく、FDAガイダンスが参照する規格であるAAMI TIR57でも同様の図で示されている。

リスクマネジメントプロセス上の具体的な相関としては、図５で示すとおり、サイバーセキュリティのリスク評価や対策を検討する際、セーフティ側のリスクに影響を及ぼす可能性がないか、影響がある場合はどのくらいなのかを考慮する。セーフティ側でも同様に、機能安全性を高める対策を検討する際に、サイバーセキュリティリスクへの影響を考慮する。

双方の影響を踏まえてリスクマネジメントプロセスを構築することがセキュリティリス

図5　セーフティとセキュリティリスク



出所）「MDCG 2019-16 Guidance on Cybersecurity for medical devices」「AAMI TIR57:2016 ／（R）2019」を基に作成

クマネジメントを行う上で重要な勘所となる。

4　積極的な海外展開のための サイバーセキュリティ対応の 標準化

医療機器メーカーの積極的な海外展開を見据えた際、多くの既存品を抱える医療機器メーカーにとっては、各製品の海外展開の都度、製品ごとに各要求事項を適用することになる。その対応には多大なコスト・手間が生じるため、積極的な海外展開に向けた課題となり得るだろう。

課題解決のための具体策としてはサイバーセキュリティ対応の標準化が考えられる。ルール面では、社内規程の強化やリスクマネジメントプロセスの構築、サイバーセキュリティソフトウエア開発要件の標準化、運用面では脆弱性管理やインシデント対応の製品横断的な体制整備が挙げられる。あらかじめ対応を標準化しておくことで、開発・設計から上市、サポート終了まで各製品のサイバーセキュリティ対策を毎度一から検討・実施せずとも、一定のサイバーセキュリティレベルが複数製品に保たれる仕組みを構築する。

さらに、今後は医療機器の販売の形態として、医療機器単体ではなく、医療機器と医療情報システムを接続させて一連のサービスとしてパッケージ化して販売する形がより普及していくと想定される。医療情報システムにおいてもリスクマネジメントおよびサイバーセキュリティ対応が必要であることから、医療機器リスクマネジメントと医療情報システムリスクマネジメントとの連動・結合も求められる対応となり得る。医療機器のより高度な機能やサービスを積極的に海外展開するには、双方の連動・結合の仕組みも含めて製品横断的に標準化していくことが必要な対応になるといえよう。

V デジタルヘルスケアサービスとサイバーセキュリティリスク

ここからは医療機器のみならずPHRなどを含めたデジタルヘルスケアの広い視点から、医療機器メーカーに限らずデジタルヘルスケアサービス提供事業者に求められるサイバーセキュリティについて述べる。

近年では治療・診療以外の分野、すなわち疾患を予防する分野や、疾患に関係なく自らにとって好ましい健康状態（ウェルビーイング）を目指す分野でもデジタル技術の活用が目立ってきている。また、これまで製薬や医療機器メーカーが中心であった医療業界にGAFA（Google、Amazon、Facebook〈現Meta〉、Apple）をはじめとする大手IT企業からスタートアップまで、幅広い企業が参入している。つまり、デジタルヘルスケアはこれまでヘルスケア関連のサービスを提供してこなかった企業にとっても魅力的な市場と捉えられ始めている。

そういったデジタルヘルスケアも医療機器と同様、技術の利活用と並行してリスクを考慮する必要がある。たとえば、個人が自身の医療情報やデータを記録し、これらを基に企業などがサービスを提供するPHRに関して、

表2　PHRサービスの三つの機能

PHR機能	
① 記録管理・閲覧機能	個人の健康情報などをスマートフォンのアプリなどで記録管理・閲覧できる機能
② リコメンド機能	生活習慣改善に向けたリコメンド（個人に適したサービスや行動などへの提案）が得られる機能
③ 第三者提供機能	記録された個人の健康情報を研究開発などのために第三者に提供する機能

厚生労働省の「国民の健康づくりに向けたPHRの推進に関する検討会」では、民間企業が提供し得るPHRサービスの機能を表2の三つに類型化している。

①の記録管理・閲覧機能とは、たとえば体重や体脂肪率、介護記録などをPHRサービス事業者が利用者から取得し、新たな情報管理サービスとして提供する機能を指す。この機能で利用者が提供するのは自らの健康データであり、中には他人に閲覧されたくない情報も含まれる。また、データに紐づいて位置情報が記録されるケースもあるだろう。したがって、本機能を利用したことによって利用者の個人情報が漏えいした場合、利用者のプライバシー侵害となる可能性がある。このような脅威は、③の第三者提供機能でも発生し得る。

②のリコメンド機能とは、たとえばウエアラブル端末のセンサー機能や①で収集したデータを基に、運動、食事、睡眠などに関する助言を利用者にリコメンドする機能を指す。適切なリコメンドに欠かせないのは収集するデータであるが、このデータを取得するウエアラブル端末などのセンサーが正しく機能しなかったり、あるいは①で収集したデータが、収集後、悪意ある攻撃によって改竄されたりした場合、誤ったデータを基に不適切な情報がリコメンドされる可能性がある。たとえば、血糖値の高い利用者に血糖値が低い利用者向けの食べ物をリコメンドしてしまうことが考えられる。

また、サービスが正常に提供できなくなると、利用者が本来得られる便益を享受できなくなることに加えて、PHRサービス事業者のレピュテーションリスク（ブランドイメージの毀損）につながる恐れもある。

Ⅵ デジタルヘルスケアサービス提供事業者において求められる対応

デジタルヘルスケアを取り扱う、あるいは取り扱う可能性がある事業者は、これまで述べてきたサイバーセキュリティ上の脅威を熟知し、適切なサイバーセキュリティ対応を図らなければならない。その対応には「ベースラインアプローチ」と「リスクベースアプローチ」という二つのアプローチが有効である。

1 ベースラインアプローチ

ベースラインアプローチとは、ガイドラインなどに定められている特定のサイバーセキュリティ対策のリストを自社に適用することでサイバーセキュリティレベルの底上げを図るアプローチである。たとえば、総務省・厚生労働省・経済産業省が2021年4月に公表した「民間PHR事業者による健診等情報の取扱いに関する基本的指針」の別紙には、事業者の情報サイバーセキュリティや個人情報の取り扱いに関するチェックリストがある。その中には、組織的・技術的・人的・物理的サイバーセキュリティ対策が含まれ、中小規模の事業者でも着手しやすい基本的な内容となっている。PHRサービス事業者はこれを参照することで基本的なサイバーセキュリティ対策を実装できる。

2 リスクベースアプローチ

リスクベースアプローチとは、一律の対策

を所与とするのではなく、自らの提供するシステムやサービスに潜在するリスクを詳細に検討し、それぞれのリスクに対応することでサイバーセキュリティレベルを向上させるアプローチである。たとえば、総務省・経済産業省が2020年８月に公表した「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」は、医療情報システムで発生し得る情報の流れ（情報流）を洗い出し、各情報流に紐づくリスクを低減させるためのサイバーセキュリティ対策を導くためのリスクマネジメントの手順が記されている。

この二つのアプローチのどちらを採用するかは、事業者のサイバーセキュリティへの対応の成熟度によって異なる。たとえば、これまでデジタルヘルスケア関連のサイバーセキュリティ対応に取り組んだ経験の少ない事業者は、まず最低限必要と思われる対策をベースラインアプローチによって実装するのが有効である。

一方、既にある程度のサイバーセキュリティ対応を実践してきた事業者は、自らの対応に抜けや漏れがないかを確かめるためにも、リスクベースアプローチに取り組むのが有効である。その際、仮に人命に影響を及ぼすようなシステムやサービスが含まれる場合は、そうしたシステム・サービスのリスクを優先的に洗い出す対策を講じるなど、デジタルヘルスケア特有の工夫も必要である。

人々の健康情報を取り扱うというデジタルヘルスケア事業の性質上、サイバーセキュリティ上の脅威に適切に対応していくことは何よりも優先される。とはいえ、一口に「サイバーセキュリティ対応」といっても、組織的対応から技術的対応までさまざまな方法がある。必要な対応の不足はもちろん避けなければならないが、自らの展開するサービスや事業特性に照らして過剰なサイバーセキュリティ対応にコストとリソースをかけた結果、サービス推進の妨げとなるような事態も避けなければならない。

過不足のないサイバーセキュリティ戦略を立案・実行していくことが、デジタルヘルスケアのさらなる普及にとって重要な課題となる。このような課題解決の一助となるのが、リスクベースアプローチである。自社が展開するサービスに実際に潜在するリスクの実像を把握することで、取るべき対応が自ずと具体化してくる。

たとえば、サイバーセキュリティ対策を新たに導入する場合、ターゲットとするリスクの低減に実効性の高い箇所にのみ導入することで、過剰なサイバーセキュリティ投資を抑えることができる。

厚生労働省が20年に実施したPHRサービス利用者へのアンケートでは、一般消費者の多くが利便性とサイバーセキュリティとのバランスを重視する旨の回答をしている。さらに、自らが利用したことのないサービスについては、利便性よりもむしろサイバーセキュリティを重視する傾向があることも報告された。このような結果を踏まえると、サイバーセキュリティ対応はデジタルヘルスケアのブレーキではなく、むしろアクセルとなる可能性が高い。自社が展開するサービスのリスクの実態を把握して適切なサイバーセキュリティ対応を図る。そうすることで、これらのサービス展開がさらに加速していくことに期待している。

注

1　厚生労働省「医療情報システムを安全に管理するために」2021年1月
2　THE STRAITS TIMES「Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack」2018年7月
3　日本医師会総合政策研究機構「医療機器に関わるサイバーセキュリティの動向」2022年3月
4　独立法人 情報処理推進機構「医療機器における情報サイバーセキュリティに関する調査」2014年4月
5　厚生労働省「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）」2020年5月

著者

長谷川ちひろ（はせがわちひろ）
NRIセキュアテクノロジーズ リスクマネジメントコンサルティング部グローバル&リサーチグループコンサルタント
専門は医療サイバーセキュリティ、サイバーセキュリティ対策状況評価、プライバシー・個人情報保護