02 号
2024 年 10 月
Newsletter issued by
Strategy in Motion Co., Ltd
SiM...Times

医療機器法規制関連　豆知識

医療機器のサイバーセキュリティと品質マネジメントシステム

皆さん、こんにちは。今回のコラムでは、医療機器のサイバーセキュリティについての我が国の規制の枠組みについて、概要を解説するとともに、その要求事項をどのように品質マネジメントシステムに取り入れて運用すれば良いかについても言及したいと思います。

近年、国内外の医療機関を標的とした、ランサムウェアによるサイバー攻撃による被害が増加している [1]ことから、医療機器においてもサイバーセキュリティを適切に確保することの重要性が増していることは皆様ご承知のとおりです。我が国においても、令和 5 年 3 月 9 日付の厚生労働省告示第 67 号の発出により、いわゆる医療機器の「基本要件基準」が改正され、プログラム医療機器に対するサイバーセキュリティの確保について、以下の条項が追加されました。

> ＜プログラムを用いた医療機器に対する配慮＞
>
> 第 12 条 3 項
>
> プログラムを用いた医療機器のうち、他の機器及びネットワーク等と接続して使用する医療機器又は外部からの不正アクセス及び攻撃アクセス等が想定される医療機器については、当該医療機器における動作環境及びネットワークの使用環境等を踏まえて適切な要件を特定し、当該医療機器の機能に支障が生じる又は安全性の懸念が生じるサイバーセキュリティに係る危険性を特定及び評価するとともに、当該危険性が低減する管理が行われていなければならない。また、当該医療機器は、当該医療機器のライフサイクルの全てにおいて、サイバーセキュリティを確保するための計画に基づいて設計及び製造されていなければならない。

この基本要件基準第 12 条 3 項は、①製品の全ライフサイクルにわたって医療機器のサイバーセキュリティを確保する計画を文書化しておくこと、②サイバーリスクを低減する設計及び製造を行うこと、③適切な動作環境に必要となるハードウェア、ネットワーク及び IT セキュリティ対策の最低限の要件を設定することをプログラム医療機器の製造販売業者や製造業者に求めており、経過措置期間終了後の令和 6 年 4 月 1 日から、義務化されています。

ここで、この医療機器についてのサイバーセキュリティの確保に必要な要件をどのように正確に理解し、会社・組織の中でどのように運用していけばよいでしょうか？まず、要件を正確に理解するためには、合わせて発行されている厚生労働省発出の通知などの文書や、グローバルに発出されている各種ガイダンス文書を読み込み、理解することが重要です。次ページの表に、日本を含む世界主要地域で発出している医療機器のサイバーセキュリティに関する主要ガイダンス文書を示します。

厚生労働省発出の「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」では、一般社団法人日本医療機器産業連合会の医療機器サイバーセキュリティ対応ワーキンググループで作成した「医療機器のサイバーセキュリティ導入に関する手引書」（以下、手引書という）を情報提供しており、この手引書は、「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」（以下、薬機法という）のもとで、医療機器の製造販売業者が実施、運用すべき医療機器のサイバーセキュリティに関する要求事項の枠組みが文書化されたものになっています。手引書は、国際的な規制調和の観点から International Medical Device Regulators Forum（国際医療機器規制当局フォーラム、以下 IMDRF という）のサイバーセキュリティに関する各ガイダンス文書をもとに作成されていますので、プログラム医療機器を日本のみならず他地域にも流通させる場合には、IMDRF の各種ガイダンス文書も熟読し、理解しておくことが必要となってきます。

手引書や IMDRF のサイバーセキュリティに係る各種ガイダンスに記載されている各要件については、会社・組織の中に必要な仕組みをゼロから作るのではなく、既に世界主要各国の医療機器の法規制の枠組みの一つとして適用されている ISO13485：2016 医療機器における品質マネジメントシステムの国際規格（以下、QMS という）に基づいて

1)　厚生労働省、事務連絡　医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）、令和 3 年 6 月 28 日

編集後記

暑いそして長い夏も終わり、やっと涼しくなってきた今日この頃ですが、温暖化の影響なのか、ここ最近の日本では、気持ちの良い春や秋がとても短くなっているのを実感しますね。今年も 10 月になって秋を感じることができるようになったと思うと、急に夏日が戻ったり、翌日には 20℃を切るような 11 月くらいの気温になったりと、気温も乱高下しています。ニュースでも衣替えのタイミングを見計らうのが難しいと報道もされており、体調管理も以前にもまして気を遣うようになっている中、このニュースレターをお読みなっている皆様のお身体のご自愛を切に願う次第です。

話は変わりますが、当社は 9 月に第 2 期の決算を無事終了することができました。これも一重に、当社とビジネス上お付き合いいただいているお客様やご協力くださっている関係会社の皆様のおかげであり、この場を借りて御礼申し上げます。第 3 期もお客様や周囲の皆様の声に耳を傾け、様々な取り組みを前向きに実行していく所存ですので引き続きよろしくお願いいたします。

（代表取締役　鷲巣　誠）

株式会社ストラテジー・イン・モーション
神奈川県横浜市西区御所山町 1 番地の 1-601 号

02号
2024年10月
Newsletter issued by
Strategy in Motion Co., Ltd
SiM...Times

表　医療機器のサイバーセキュリティに関する主要ガイダンス文書

ガイダンス文書タイトル	発行元	発行時期
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	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	令和5年3月31日
IMDRF/CYBER WG/N60 **Principles and Practices for Medical Device Cybersecurity**	International Medical Device Regulators Forum	2020年4月20日
IMDRF/CYBER WG/N70 **Principles and Practices for the Cybersecurity of Legacy Medical Devices**	International Medical Device Regulators Forum	2023年4月11日
IMDRF/CYBER WG/N73 **Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity**	International Medical Device Regulators Forum	2023年4月13日

運用されているQMSに必要な要件を取り込んで、既に会社の中で運用しているQMSの各文書類に新たな手順書を追加したり、既存の文書を改訂することで運用することが可能です。ここで、医療機器のサイバーセキュリティの確保に必要な各要素概要とQMS上での運用イメージを下図に示します。

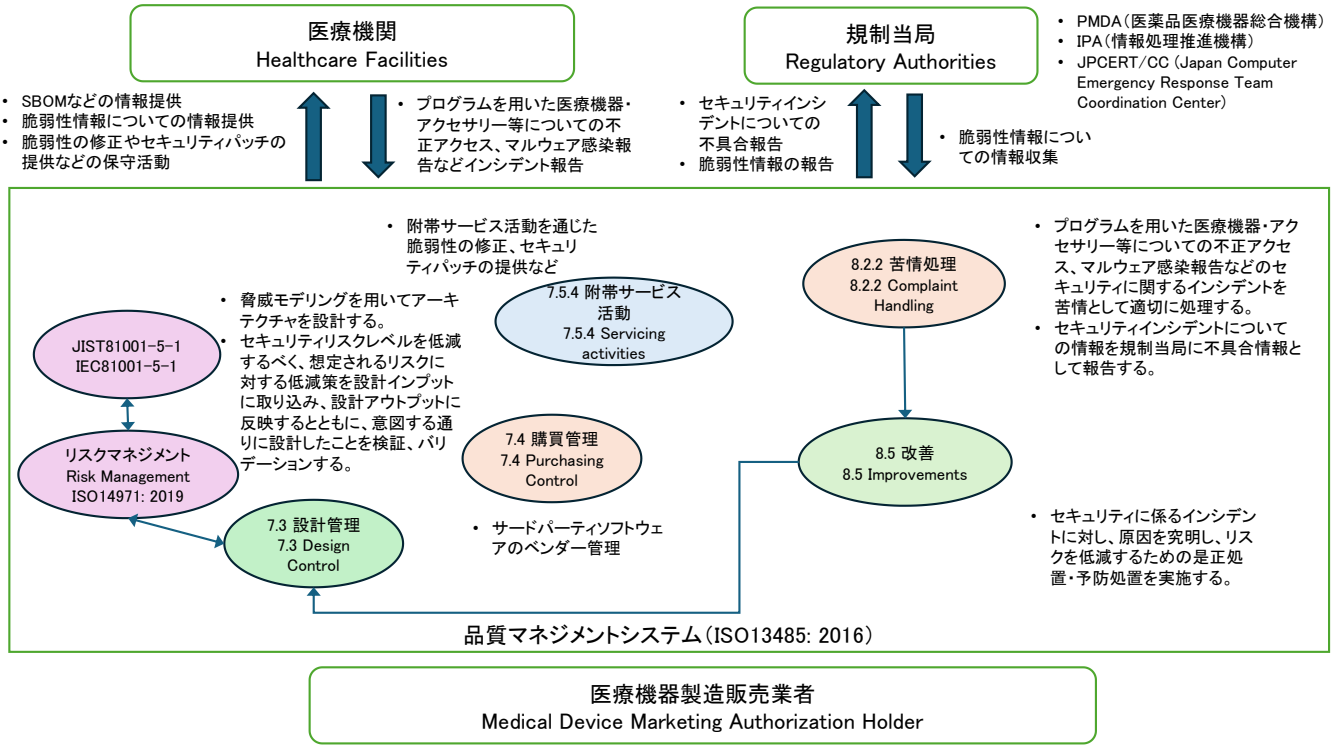

図　医療機器のサイバーセキュリティの確保に必要な各要素概要とQMS上での運用イメージ

SiM...
For Global Medical Device Standard
株式会社ストラテジー・イン・モーション
神奈川県横浜市西区御所山町1番地の1-601号

すなわち、QMS 上で既に運用している設計管理とリスクマネジメント、購買管理、附帯サービス活動、苦情処理、是正処置及び予防処置などの QMS の各プロセス上で、サイバーセキュリティの確保に必要な各要素を取り込んで文書化し、運用すれば良く、各プロセスごとにそのポイントを以下に解説していきます。

- 設計管理とリスクマネジメント；プログラムを用いた医療機器のアーキテクチュア設計に際しては、脅威モデリングを用いるとともに、セキュリティリスクレベルを設計段階から低減すべく、「ISO14971: 2019 医療機器- リスクマネジメントの医療機器への適用」に基づいたリスクマネジメントプロセス」に JIST81001-5-1, IEC81001-5-1「ヘルスソフトウェア及びヘルス IT システムの安全、有効性及びセキュリティー第 5 － 1 部：セキュリティー製品ライフサイクルにおけるアクティビティ」に示される各要素を関連付けることにより、サイバーセキュリティの脆弱性を特定し、その悪用によって生じる脅威や悪影響に伴う想定されるリスクに対する低減策を設計インプットに取り込み、設計アウトプットに反映するとともに、意図する通りに設計したことを設計検証や設計バリデーションの活動の一つとして実証することが求められます。また、医療機器のリスクマネジメントのインプットとして、意図する使用環境だけでなく、合理的に予見可能な実使用環境を考慮した上で、リスク低減のために医療機関や使用者に伝えるべき情報をラベリングのインプットとして特定し、医療機器製品の注意事項等情報、取扱説明書及び顧客向けセキュリティ文書を設計アウトプットの一部として作成、更新します。プログラム医療機器に実装されている自製、オープンソース及び市販のソフトウェア部品（製品コンポーネント）の透明性を確保するために、SBOM（Software Bill of Materials, ソフトウェア部品表）を作成し、医療機関や使用者にどのように提供するかの計画も立案します。
- 購買管理；医療機器の設計に組み込まれるソフトウェアプログラムに、サードパーティベンダーが開発したソフトウェアプログラムが含まれるのであれば、そのベンダーの供給業者評価を行い、承認済み供給業者リスト（Approved Supplier List）に登録し、そのベンダーの提供するソフトウェアプログラムについて、サイバーセキュリティの確保が適切に実施されていることを確認、監視する必要があります。
- 附帯サービス活動；製造販売業者はソフトウェアの保守について、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保守活動に取り込むとともに、そのアップデート情報を医療機関及び使用者へタイムリーに共有する必要があります。また、医療機器の設計に組み込まれているオペレーティングシステム（以下 OS という）やオープンソース等のサードパーティ製ソフトウェアについても脆弱性情報やアップデート情報を常に監視し、市場で流通している医療機器を適切にアップデートすることが求められます。既に流通している医療機器のソフトウェアの修整やアップデートはその内容によっては、薬機法で規定する回収・改修に該当する場合があることにも注意が必要です。
- 苦情処理及び規制当局への報告；プログラムを用いた医療機器・アクセサリー等についての不正アクセス、マルウェア感染などのセキュリティに関するインシデントについての医療機関からの報告を苦情として処理、記録し、収集した当該医療機器の脆弱性に関する情報に対して、有効性及び安全性等に関する影響等を評価し、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する必要があります。規制当局への報告については、医薬品医療機器総合機構（PMDA）に対する薬機法に基づく不具合等報告のみならず、情報処理推進機構（IPA）に対するサイバーセキュリティに関する報告を実施するとともに、医療機器自体の脆弱性に係るインシデントは JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)等の機関に報告する必要があることに留意する必要があります。
- 是正処置及び予防処置；プログラムを用いた医療機器・アクセサリー等について脆弱性に係るリスクが判明した場合、是正処置及び予防処置（CAPA）プロセスに従い、根本原因を究明し、リスクを低減するための脆弱性の修正や取扱説明書の変更・改訂や、医療機関・使用者への脆弱性情報の開示等の必要なアクションを是正処置・予防処置として実施します。

以上、今回のコラムでは、医療機器のサイバーセキュリティについての法規制の枠組みの概要と、サイバーセキュリティの確保に必要な要件をどのように QMS 上の各プロセスに取り込んでいけばよいかを筆者なりの考えを交えてお伝えしました。昨今でも、政府機関や民間企業がサイバー攻撃を受け、重要な情報が流出したり、基幹システムがダウンしたりするなど莫大な被害を受けたというニュースが毎週のように報道されています。医療機器業界においても、サイバーセキュリティは今後益々重要になっていくと思われます。サイバーセキュリティについて、QMS 上でどのような対策を行えば良いか、詳細について、もっと話を聴きたいなどご要望がございましたら、私どもにお問い合わせください。

株式会社ストラテジー・イン・モーション
SiM...
For Global Medical Device Standard
神奈川県横浜市西区御所山町 1 番地の 1-601 号