医療機器製造販売業者等に対する令和6年度アンケート結果に基づく サイバーセキュリティ対策の対応状況に関する課題及び問題点について

2024年10月7日から11月15日までの期間、全国の医療機器の製造販売業者、製造業者等を対象にアンケート調査を行った結果、次の課題及び問題点が示唆された。

1. サイバーセキュリティ対策（以下「CS対策」という。）に関連する活動及びCS対策に関連するリスクマネジメント活動を実施する要員の拡充

医療機器の基本要件基準第12条第3項にCS対策に関する要求事項が明確化され、令和5年4月1日より適用されており、サイバーセキュリティに関する必要な力量の明確化、教育訓練の実施及び力量の維持については、全体の49%の会社で完了しており、全体の36%の会社で準備中であるものの(設問17)、未だ医療機器に関するCS対策を実施するには不十分な面もあり、その途上にあると考えられる。

医療機器製造販売業者等においては、CS対策を実施する要員に必要な力量の明確化、教育訓練の実施及び力量の維持を社内の品質管理監督システム（以下「QMS」という。）等に組入れ、実務者の育成と共に、CS対策に遅れが生じないよう、CS対策に関する業務を適正かつ円滑に遂行しうる必要十分な要員（リソース）を確保する継続的な努力が必要である。

医療機器のサイバーセキュリティ対策についての課題としては、専門家の確保（全体の28%）、専門家以外の教育（全体の21%）、対策費用等（全体の19%）リスクマネジメントの具体的方法(全体の14%)などが挙げられた。(設問76)。専門家の確保、教育訓練の実施等は、事業者によるCS対策の費用負担等につながることであるものの、不十分なCS対策により生じうるビジネスリスクを考慮した場合、リスクに応じた対応を検討することが重要であると考える。

CS対策を実施する要員に対する教育訓練については、医療機器産業界の関係団体と行政が協働で、研修会等の教育訓練の場を提供することもリソースの確保の一助となり得ると考える。

2. 医療機器製造販売業者等における CS 対策の運用の適切性に関する確認方法の検討

セキュリティリスクに関する情報を収集する体制は確立されつつも、自社の製品化を問わず広くサイバーセキュリティに関する脆弱性等の情報を入手できていない会社が半数以上を占めることから、能動的に情報収集できる体制にまでは至っていないこと、また、既知の脆弱性について製品への影響を評価する仕組みの整備に遅れが生じている可能性が示唆された。(設問 18、19、20 及び 21)
医療機器製造販売業者等における CS 対策に関連する体制及びその運用を確認する方法については、現行の「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」(以下「薬機法」という。)では明確に規定されていない。

サイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みについては、全体の 58%の会社で確立済み、29%の会社で準備中であったが、13%の会社で未着手の状況であった。(設問 27)
医療機器等に関するサイバーセキュリティに係る規格である JIS T 81001-5-1:2023 (IEC 81001-5-1:2021)「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」においても、「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」(平成 16 年厚生労働省令第 169 号)(以下「QMS 省令」という。)の元となる ISO 13485 (JIS Q 13485)「医療機器ー品質マネジメントシステムー規制目的のための要求事項」の運用に組入れることを推奨している。

セキュリティポリシーの設定は進んでいるものの、セキュリティポリシーの使用者への開示に関する仕組みの確立は若干遅れ気味であり (設問 28 及び 29)、また、製品セキュリティインシデント対応組織の設置は進められているが、使用者に対する脆弱性等に関するアドバイザリー情報の提供は遅れていることが示唆された。(設問 37 及び 38)
医療機器製造販売業者等から使用者に対してアドバイザリー情報を含むセキュリティリスクに関連する情報が適時的確に提供され、適切な措置がとられることが重要である。

QMS 省令及び ISO 13485 では、サイバーセキュリティに関する要求事項は規定されていない。しかしながら、JIS T 81001-5-1:2023(IEC 81001-5-1:2021)においては、JIS Q 13485:2018 (ISO 13485:2016) の要求事項の一部として実施可能とされている。例えば、品質管理監督システム (品質マネジメント

システム）にサイバーセキュリティに関する要求事項を取込むことは可能であり、QMS 省令第 56 条内部監査の中で CS 対策の運用の適切性を確認することは有用であると考えられた。
なお、個別品目に係る CS 対策の適切性、基本要件基準第 12 条第 3 項に対する適合性については、承認・認証審査の中で確認すべき事項であり、現状の対応のみで十分かについては更なる検討を要すると考える。

3. 医療機器製造販売業者等と使用者である医療機関との連携

使用者のネットワーク構成図の把握については、全体の 23%の会社で使用者側から開示されない等の理由により把握したいが把握できない状況であり、53%の会社が把握していない状況であった（設問 55)。
また、医療機器サイバーセキュリティに関する保守契約を使用者と締結しているのは、全体の 17%の会社にとどまっており、83%の会社は保守契約を締結していなかった（設問 73)。
医療機器のサイバーセキュリティ対策についての課題の一つとして、医療機関との連携・情報共有（全体の 18%）が挙げられた（設問 76)。

医療機器の製造販売業者等と使用者（医療機関）がサイバーセキュリティに関する認識を合わせて、相互に連携、情報共有を図り取り組んでいくことが重要ではないかと考えられるため、連携のための方法を模索する必要があると考える。

4. 第三種医療機器製造販売業許可取得者に対する支援

第三種医療機器製造販売業許可取得者では、CS 対策に関連する社内体制に関する手順書の整備、評価体制の整備、教育訓練の実施及び力量の維持、脆弱性等に関する報告やセキュリティリスク等に関連する不具合等報告の仕組みの確立などの複数の項目（設問 13、14、17、22 及び 27）において、第三種医療機器製造販売業許可取得者における対応が遅れ気味であることが示唆された。

一般医療機器（クラスⅠ）製品については、前述のとおり、サイバーセキュリティに関する要求事項を品質管理監督システム（品質マネジメントシステム）に取込み、QMS 省令第 56 条内部監査の中で CS 対策の運用の適切性を確認することは有用であると考えられた。

以上