Ⅲ　IT-BCP・サイバー BCP

4. 医療機器セキュリティの現実解

松元恒一郎　Koi-HEALTH

医療機関を標的としたランサムウエア被害などの増加に伴い，基幹システムや医療機器への脅威が顕在化している。医療機器特有の脆弱性のあるIT環境が放置されれば，事業継続が困難な状況を作りかねない。わが国でも医療法施行規則の改正や「安全管理ガイドライン」の継続的改訂などに加え，製造販売業者は，サイバーセキュリティに関して，医薬品医療機器等法に紐付く基本要件基準改正および関連する通知への適合によって，医療機器の安全性を確保し，患者の安全の視点からその対応を進めている。この取り組みは，医療機関におけるBCP策定にもつながるところがある。本稿では，製造販売業者の取り組みについて，また，この取り組みを医療機関の視点から説明する。

わが国におけるサイバーセキュリティの現状

現在の医療機器は，有線/無線のネットワークを介したほかの機器やソフトウエアとの連携などによるシステム化や，USBメモリなどの携帯型メディアを介してデータの授受を行いながら相互通信で使用されるものが増加している。ネットワークなどには医療機器以外の電気機器（IoT機器）も接続されており，医療機器の使用環境が常にセキュアであるとは限らない。医療機関を標的としたランサムウエア被害などの増加に伴い，基幹システムや医療機器への脅威が顕在化している。サイバー攻撃が発生した場合には，患者や医療従事者への健康被害につながる可能性もある。このため，医療機器の本来の目的である有効性および安全性を確保するために，サイバーセキュリティ対策の重要性が増している。

わが国においては，医療機器の製造販売を規制する医薬品医療機器等法に紐付く各種基準によってサイバーセキュリティを含むリスクマネジメントが求められ，使用者に対する情報提供や注意喚起を含めて最新の技術水準に立脚して医療機器の安全を確保しなくてはならないこととされている。また，「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）[1]によって，医療機器の使用環境に応じたセキュリティ設計，サイバーリスクに伴う医療機器の不具合などについても「医薬品，医薬部外品，化粧品及び医療機器の製造販売後安全管理の基準に関する省令（GVP省令）」に基づいた情報共有の組織構築が求められている。

2020年4月には，国際医療機器規制当局フォーラム（International Medical Device Regulators Forum：IMDRF）から「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（N60）[2,3]が公表された。さらに，2023年4月には，「レガシー医療機器のサイバーセキュリティの原則及び実践」（N70）[4,5]，「医療機器サイバーセキュリティのためのソフトウェア部品表の原則及び実践」（N73）[6,7]が公表された。

わが国でもN60文書の公表から3年を経た2023年3月末にN70文書，N73文書も考慮した通知として，厚生労働省から「医療機器の基本要件基準第12条第3項の適用について」[8]，「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」[9]が発出された。各医療機器製造販売業者は，この通知を参考にして対策を進めている状況にある。

製品セキュリティ体制

1. 医療機器における製品セキュリティの位置づけ

製造販売業者は，前出の基本要件基準第12条第3項の改正を一つの転機ととらえ，個別対応の積み上げではなく，

〈0913-8919/26/￥300/論文/JCOPY〉