トピックス

デジタルヘルスケアのセキュリティ対応
―医療機器のサイバーセキュリティ対策高度化の課題―

ヘルスケアのデジタル化は、医療の高度化とともにサイバーセキュリティの脅威ももたらす。医療機器メーカーには、既存の品質管理に加えて、セキュリティ面の対処も求められている。セキュリティに関するガイダンスには現状どのようなものがあるのか、また、メーカーとしてはどのような対応を行っていく必要があるのか考察する。

NRIセキュアテクノロジーズ コンサルティング事業本部
ストラテジーコンサルティング部 セキュリティコンサルタント
松本（まつもと） 直毅（なおき）
専門は製造業を中心としたセキュリティに関するコンサルティング全般

医療機器のデジタル化に伴う脅威

ITを活用した新しい技術やサービスにより、あらゆるビジネスのデジタル化が進んでいる。医療業界も例外ではなく、「デジタルヘルスケア」という形で以下の変化が生まれている。

- デバイス（医療機器）へのソフトウェア導入・拡充による機能の高度化
- インターネット接続によるデバイスのコネクテッド化（Internet of Things）
- デバイスから収集される医療データのクラウドへの集約による医療サービスの効率化・高度化

デジタルヘルスケアは、よりよい医療を実現する一方で、サイバーセキュリティ面で脅威に晒されている。ネットワーク接続された医療機器（ペースメーカーやインシュリンポンプ）のソフトウェアの脆弱（ぜいじゃく）性や攻撃手法が日々報告され、実際にサイバーセキュリティに関わるインシデントも発生している。

2018年、シンガポール最大の医療グループSingHealthに対してサイバー攻撃が行われ、医療機関のITシステムに格納された、150万人分の個人情報や16万人分の医療データが流出している（『The Straits Times』2018年7月20日付）。流出したデータには、同国のリー・シェンロン首相のものも含まれていた。

今後は、社会保障番号、病歴などを含む医療データの取引価値がより高まり、攻撃者の標的になっていく（米国保健福祉省「Health Industry Cybersecurity Practices」）。高度化・巧妙化する脅威に対抗するために、セキュリティ対策の高度化が必要とされている。

デジタルヘルスケアといってもさまざまなものが含まれ、その対象は広いが、本稿ではサイバーセキュリティにおける動きが活発で喫緊の対応が求められる医療機器に焦点を当てる。特に、今後、医療機器メーカーに求められる対応を考察する。

セキュリティ対策の現状

サイバーセキュリティ対策の各論に入る前に、一般的なシステムと比べ、医療機器がどのような特徴を持つのかを表1に示す。

まず、医療機器は厚生労働大臣の登録を受けた認証機関の認証（基準適合性認証）を受ける必要があり、設計変更にも届け出が必要である。また、製品のライフサイクルが長い点が挙げられる。特に体内に埋め込む機器の場合は、交換にも手術を必要とするため、メーカーの都合だけで交換やサポートの終了ができない。脆弱性に対する考え方も大きく異なる。一般的なシステムでは、CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）などによって定量的に評価された深刻度を踏まえ、セキュリティパッチの適用などの対応要否を判断する。一方、医療機器においては、CVSSの深刻度が低くても、その脆弱性を突かれると患者の生命に関わる、といったケースもある。従って、CVSSの評価だけで決めるのではなく、攻撃を受けた際の影響の大きさからも評価し、医療機器独特の特徴も踏まえた対策を検討する必要がある。

表1　一般的なITシステムと比較した医療機器の特徴

	一般的なITシステム	医療機器
設計変更に対する考え方	・システムの利用目的から必要と判断されれば、設計変更は可能	・設計変更には届け出が必要であり、簡単には設計変更ができない
ライフサイクル	5年程度	10年以上
脆弱性に対する考え方	・CVSSなどの定量的に評価された深刻度を参照し、一定レベル以下の場合は対応しない、といった指標とする	・患者の生命に影響する機器の場合、CVSSの深刻度による単純な評価だけでは不十分 ・攻撃を受けた場合の影響の大きさも考慮する必要がある

次に、医療機器のサイバーセキュリティ対策を検討する場合の、規制やガイドラインについて述べる。

日本におけるサイバーセキュリティ関連のガイダンスとしては、厚生労働省から2015年4月に「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」、2018年7月には「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」が公表されている。

これらに加え、グローバルにビジネスを行う場合、米国のFDA（Food and Drug Administration：米国食品医薬品局）による、サイバーセキュリティに関するガイダンス（以下、FDAガイダンス）が参考になる。医療機器政策調査研究所「メディカルデバイス2017 医療機器産業の動向」（2018年3月）によると、日本の上場企業20社の近年の海外売上高比率は50～65％と、国内市場と比べて高い。その中でも、医療機器の市場規模として世界最大である米国市場の対応は重要である。また、医療機器に対するサイバーセキュリティ対策において、米国が先行している点も挙げられる。これらの背景から、現時点では厚生労働省の動向を注視しつつ、FDAガイダンスを参照しながらサイバーセキュリティ対策を進めている日系メーカーが多い。

FDAガイダンスは、「ライフサイクルが長い」などの医療機器の特徴を踏まえながら、市販前の設計・開発段階で必要なセキュリティ対策を組み込むとともに、市販後も継続的に対策レベルを維持し続ける対応を求めている点が特徴である。

市販前のガイダンスに当たる「Content of Premarket Submissions for Management of Cybersecurity in Medical Devices」（2014年10月）では、機器の設計・開発段階において、機器の脆弱性や想定される脅威の洗い出し、脅威が発生する可能性や発生した場合の

影響度の評価、またそれらに対するリスク低減策の策定などが規定されている。また市販後のガイダンスに当たる「Postmarket Management of Cybersecurity in Medical Devices」（2016年12月）は、リスクの早期検知や特定のための情報収集、特定された脆弱性に対するリスク評価と低減策の策定・導入、そしてそれらの対策状況の情報公開などが規定されている。

メーカーに求められる取り組み

FDAガイダンスを踏まえ、日系メーカーではどのような取り組みが行われているか。市販前のプロセスでは、医療機器の設計・開発において、サイバーセキュリティ要件を組み込むことになり、純粋に負担増となることが懸念される。対応としては、既存のQMS（品質管理システム）やPLM（製品ライフサイクル管理）のプロセスにサイバーセキュリティ要件を組み込んでいくアプローチが有効である。既存の仕組みの上にセキュリティを組み込むことで、製品の品質を損なうことなく、設計・開発プロセス全体に対して網羅的な取り組みが可能となる。

注意すべきは、製品の機能安全に関わるリスクマネジメントのプロセスと、いかに整合性を取ったプロセスとすべきかである。機能安全に関するプロセスは、時間をかけて詳細まで確立されている。しかし、サイバーセキュリティのリスクマネジメントに関する具体的な規格はまだ存在しない。そのため各メーカーはFDAガイダンスを参照し、その要求事項を自社の製品やプロセスに適合する対策に整理し、設計・開発文書に落とし込む必要がある。

次に市販後については、「脆弱性管理」と「（サイバーセキュリティに関する）インシデント管理」について、継続対応が可能なプロセスを確立する必要がある。

「脆弱性管理」は、「準備」「調査」「判断」の3点に集約される。ある脆弱性が自社製品に関連するものかを調査するための準備として、自社製品に格納されるソフトウェア（自社開発、他社からの提供を問わない）の棚卸を行う。一般的に「構成管理」と呼ばれるものである。次に日々公表される脆弱性を定期的に調査し、自社製品に該当する対象を抽出する。該当する脆弱性が特定された場合は、その脆弱性が製品に及ぼす脅威の深刻度を評価し、対策の要否と具体的な実施方針を検討する。

FDAガイダンスにおいては、脆弱性情報の収集についてNIST（National Institute of Standards and Technology：米国国立標準技術研究所）が管理するNVD（National Vulnerability Database：脆弱性情報データベース）の利用などの方法論が推奨されているが、公表される脆弱性情報は膨大である。効率的な運用のため、専任の担当者を「調査（脆弱性情報収集）」に集中させ、脆弱性情報収集の「準備（構成情報の棚卸し）」と「脆弱性への対応をどうするかの判断」は、具体的な製品知識を持つ担当者が行う、というように役割分担すべきである。

また、インシデント発生時の対応についても、プロセスを検討しておく必要がある。一般的に用意されている顧客サポート窓口で

は、サイバーセキュリティの知識は不十分な場合が多い。一次窓口である顧客サポート窓口で、問題がサイバーセキュリティ関連なのか、最低限の切り分けができる手順書を準備し、その上で、該当する問い合わせは製品セキュリティ担当者に報告する、といった運用プロセスを整備する必要がある。

ここまで述べた通り、サイバーセキュリティ対応では、新たなプロセスと役割が生じる。役割を果たすには、製品に対する知識とサイバーセキュリティの知識をバランスよく保持した人材が不可欠となる。

メーカーにおいても、セキュリティに特化したPSIRT（Product Security Incident Response Team）のような組織を立ち上げようと検討が始まっている。

では、これらの取り組みを進めれば、欧米の主要メーカーと比較しても十分といえるだろうか。総務省「サイバーセキュリティ政策推進に関する提言」（2015年5月）によると、米国においては、1998年に、重要インフラ領域における情報共有組織としてのISAC（Information Sharing and Analysis Center）の概念が提唱されており、その後2015年のオバマ政権時には、ISACの機能を補完する機関としてISAOの設置が企図され、官民一体となってサイバーセキュリティに関する脅威情報の交換を行っている）。一方、日本では、情報通信業界における「ICT-ISAC」や「金融ISAC」が活動を始めており、今後は医療業界においても、米国や国内の他の業界に追随した取り組みが進むことが見込まれ、日系メーカーにおいては今後の動向についての情報収集をすべきである。

今後の展望

医療機器のデジタル化は医療の質や利便性向上をもたらす一方で、患者自らが医療機器の脆弱性を利用して、機器の設定を自分の都合のよいように変更するといったケースにもつながる。患者同士で立ち上げたコミュニティで情報交換を行い、そのような利用がされている例がある（『The Atlantic』2019年4月29日付）。本来メーカーにサポート義務はないが、今後はそのような脆弱性が極力発生しない設計・開発を行うとともに、発覚した脆弱性については早期に対応方針を明確にし、一般に公開する必要性が高まっていく。

将来的には、サイバーセキュリティ対策に伴う負荷が課題になる。さらに一部の対策では、高度なセキュリティ知識が求められる。高い専門性を持つ人材を、メーカーが自社に持つことが必ずしも最適とは限らない。新たに必要とされるプロセスを整理した上で、製品知識がいらない定型的な業務や、また高度な専門性を必要とする業務については、外部の専門家と連携することも考えられる。

前述したFDAガイダンスや厚労省ガイダンスは、現在はまだ“推奨事項”に留まっているが、今後は基準適合認証に直結した、より強い拘束力を持つものとして制度化されるのも時間の問題である。EU圏や中国、新興国においても、個別の法規制が適用される。自社におけるサイバーセキュリティ対応を高度化させる取り組みに加えて、販売先国の監督官庁や業界関係者などの外部関係者とも、積極的な情報交換・収集を行うことが求められる。■