公益財団法人
医療機器センター

MDSI 医療機器産業研究所
Medical Device Strategy Institute

2023 AAMI exchange 参加報告書

2023 年 7 月

本田 大輔

（公益財団法人医療機器センター附属医療機器産業研究所 主任研究員）

1.　はじめに

AAMI（Association for the Advancement of Medical Instrumentation；エイミーとも呼ぶ）は 1967 年に設立された非営利団体であり、安全で効果的な医療技術の開発、管理、使用という 1 つの重要な使命を掲げ 10,000 人を超える専門家（臨床工学技士、生物医学機器技術者、メーカー、滅菌処理専門家、研究者、品質保証および規制業務の専門家、医療技術管理専門家等）が所属している。具体的な活動としては、医療機器の安全管理や使用、滅菌などの実務に関する情報、サポート、ガイダンスの提供を行っている。この AAMI では毎年学術集会を開催しており、医療機器の保守点検やサイバーセキュリティ、滅菌などに関する内容のシンポジウムや教育セッション、医療機器の展示会などが実施されている。今年は 2023 年 6 月 16 日（金）～6 月 19 日（月）に米国のカリフォルニア州ロングビーチにて「2023 AAMI exchange」がオンサイトで開催された（図 1）。今回、現地に参加して展示会場の視察、教育セッションやシンポジウムを聴講し、視察して感じたことや個人的に注目した講演内容を詳細にまとめたので報告する。

図 1　2023 AAMI exchange のオープニング

2.　学会の様子

学会は 6 月 16 日（金）のオープニングから 6 月 19 日（月）までの最終日まで全ての日程で参加をした。この 4 日間で展示会場の視察、複数の教育セッションを聴講、さらには日本医療機器学会の先生方の講演、AAMI's Annual Business Meeting への参加などもあり大変充実したものであった。この中で教育セッションについては後述することとし、展示会場の視察と日本の先生方の講演の様子について報告する。

2.1.　展示会場の視察

展示会場は 163 社の企業が出展し、医療機器、滅菌機器、医療機器の点検治具などの展示、医療機器保守点検（あるいは修理）サービスの紹介がなされており、中には医療機器の修理を迅速に対応するための特殊車両を展示している企業もあった。展示会場を視察して感じたことは、日本の医療機器に関連する学会での展示会場と比べて修理サービスや医療

機器の点検治具の展示が非常に多いことである（図 2)。これは本学会が医療機器の保守点検等の知見を得ることがメインであり、それに相応する医療従事者が本学会に集まることが理由の一つとして考えられるが、これと同時に米国の医療従事者（主に臨床工学技士）が医療機器の保守点検を専門領域として従事している割合が多いことも考えられた。また、米国の臨床工学技士が医療機器の保守点検を専門性が高いことは、日本の医療機器に関連する学会と比較しても感じるところである。例えば、医療機器の保守点検を業務の一つとする臨床工学技士の学術集会では点検治具等よりも医療機器が多くを占めており、日本の臨床工学技士は臨床業務（生命維持管理装置等を使用した業務）と医療機器の保守点検業務を兼務している割合が高く、米国よりもジェネラルに展開していることの違いと考えられた。このように学会の展示物の違いからも日米の臨床工学技士の業務の専門性の違いを感じられた。

図 2　展示会場の様子

2.2.　日本の先生方の講演

今回、本学会の教育セッションにおいて一般社団法人日本医療機器学会の先生方から 2 つの講演が行われた（図 3)。一つは東京大学医学部付属病院の深柄 和彦先生、千船病院の水谷 光先生、越谷市立病院の酒井 大志先生らによる「Standards for Sterilization in a Healthcare Setting」である。講演内容は日本医療機器学会から発行されている「医療現場における滅菌保証のガイドライン 2021」を紹介し、日本の医療現場における滅菌の標準化への取り組みについて解説するものであった。もう一つは東京工科大学の笠井 亮佑先生による「Application of VR and AR in Learning Support for Medical Devices - Presented by JSMI」である。講演内容は AR/VR を活用した医療教育に関する講演であり、東京工科大学で実施された AR/VR を活用した人工心肺教育についてその効果について発表したものであった。日本からの講演を目の当たりにし、このような大舞台で講演を行うことは世界に日本の活動を示すために重要な取り組みであると感じるとともに自身にとっても大変刺激になるものであった。

図 3　AAMI で講演する先生方（左から深柄先生、水谷先生、酒井先生、笠井先生）

3.　教育セッション等の聴講

本学会の教育セッション等は医療機器の保守点検、修理、規制などをテーマとして各分野の専門家による講演である。学会が開催されている 4 日間で計 81 の講演が実施された。

本年度は医療機器の保守点検、IOT や AI、サイバーセキュリティなどの講演がなされ、この中で本邦でも重要性が増している医療機器のサイバーセキュリティに注目し、医療機関に対するサイバー攻撃の懸念が高まる中における米国での取り組みについて情報収集をしてきたので報告する。講演は全部で 4 講演を聴講し、一つ目は Cynerio 社の Chad Holmes 氏により自社から発行されたサイバー攻撃の報告書をベースにしたサイバー攻撃の患者への影響、二つ目は First Health Advisory 社の Andy Ulvenes 氏らによるサイバーセキュリティ・プログラムを推進する理由、三つ目は TRIMEDX 社の Scott Trevino 氏によるサイバーセキュリティ関連の最近の法律の紹介、四つ目は Health-ISAC の Phil Englert 氏らによる医療機関のサイバーセキュリティ対策の実施主体に関する講演である。以下に各講演内容の詳細を報告する。

3.1.　Clarifying Healthcare Cyberattacks: Insight and Actions to Protect Patients

【概要】

Cynerio 社は医療機器のサイバー攻撃に対するセキュリティ対策のサービス（サイバー攻撃の検出、脆弱性管理、CMMS データリスク分析など）を提供する企業であり、演者の Chad Holmes 氏は Cybersecurity Evangelist として活躍されている方である。本講演では、Cynerio 社と Ponemon Institute から共同でリリースされた「The Insecurity of Connected Devices in Healthcare」（以下、報告書）からサイバー攻撃による財務面の影響や患者ケアの危険性などの紹介、サイバー攻撃の対策を実施するためのアプローチ方法ついて講演された。

【講演内容】

最初にアメリカにおける医療分野のサイバー攻撃の被害状況について取り上げられた。報告書によれば、調査した 517 の医療機関の約 90%の施設がサイバー攻撃を受け、45%は患者に悪影響を及ぼしたとされた。また、43%はランサムウェア攻撃を受け、47%が復旧のために身代金を支払ったとされた。さらに患者への影響について詳しく見てみると、悪影響を受けた 45%の患者のうち、その中から 56%で入院期間が延長し、53%で死亡率が上昇されたと報告している。すなわち、調査した医療機関の全体の 25%で入院期間の延長、24%で死亡率が上昇されたと報告している。他方、国が公開しているデータに着目すると、HHS（Health and Human Services、米国保健福祉省）では「Wall of Shame」が公開されており、500 人以上に影響を及ぼしたデータ侵害のインシデントのリストが公開されている。当該リストによると 2022 年は医療分野においてハッキングなどの IT 関連のインシデントで約 4,300 万件の患者記録が流出しており、これは全データ侵害の約 85%に相当し、米国人の 8 人に 1 人の計算でデータ流出した計算となる。また、5 年間の推移を見てみるとハッキングなどの IT 関連のインシデントは＋269%、データ侵害は＋1333%となっている（図 2）。

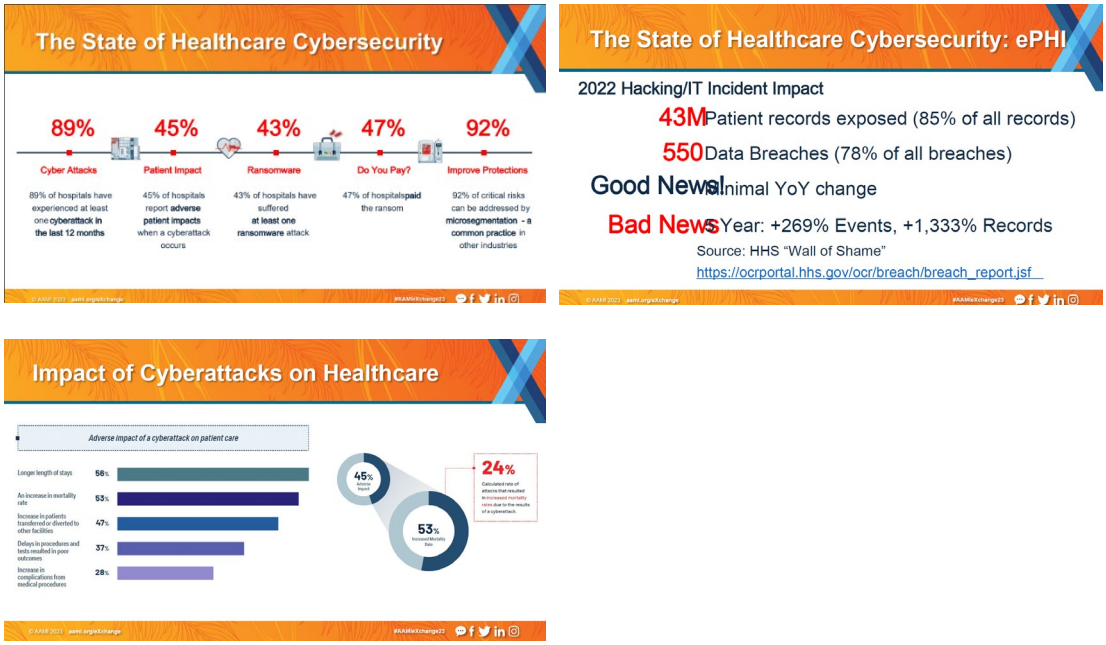

図 4　サイバー攻撃の被害状況

サイバー攻撃のリスクはデバイスリスク、OS リスク、SBOM リスク、Configuration リスクに分けられ、この中でデバイスリスクはリスク全体の氷山の一角である。このため、サイバー攻撃の対策を講じていく上では、デバイスに何か不具合が生じた際には対処が必要なことはもちろんのこと、この他にも OS のバージョンを最新にすること、SBOM を手に入れたら詳細を確認して安全性を確認すること、Configuration（ソフトウェア/ハードウェアの構成や配置、アプリ/プログラムの設定）の確認が重要であり、これらの対策は全ての

医療機関で求められる。これらの対策を実施していくためには、IT の専門的知識を有していない医療機関のみでは対応が難しく、医療機関と企業が協力することが適切である。

また、サイバーセキュリティ対策を講じていく上では、CMMS（Computerized Maintenance Management System、設備保全システム）を活用した保守管理、CISA（Cybersecurity and Infrastructure Security Agency、アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁）からの情報入手が有用であるが、サイバー攻撃対策として先ず実施できることとしては、ネットワークの監視ツールを活用することである。これは Cynerio 社のサービスではあるが、監視ツールを活用することでサイバー攻撃のリスク同定、ePHI（Electronic protected health information、電子保護医療情報）の流出のリスク同定などを通して、ハッカーよりも先に攻撃を阻止し、防御する方法を見つけ出すことができる。また、CMMS Analysis も有用であり、当該システムを使用して保有しているネットワーク接続機器の保守管理を行うことで脆弱性管理を行うことでセキュリティ状態の把握が可能である（図 3）。

図 5　CMMS　Analysis の概要

【考察】

本講演で紹介された報告書では米国のサイバー攻撃の被害状況が報告されていたが、この中でも**調査した医療機関のうち 24%で死亡率が上昇とされる結果**は非常に興味深いものであった。本調査は 517 の医療機関を対象としていることから 24%という数字をどのように解釈するかは意見が分かれるが、実際にサイバー攻撃によって患者の死亡率を上昇させていることの事実はサイバーセキュリティ対策の普及啓発において重要であろう。

患者の安全を守るためにはサイバー攻撃のリスクを知り、サイバーセキュリティ対策を講じることが重要となる。これまで筆者はサイバー攻撃のリスクはデバイスに対するリスクがほとんどを占めると考えていたが、これは氷山の一角であり、**OS、SBOM、Configuration のリスクも多く潜在している**とのことであった。これらを踏まえると、医療機関でサイバーセキュリティ対策を講じていくためには、**サイバーセキュリティに関する専門知識を欠く医療従事者のみでのサイバーセキュリティ対策には限界があり、本講演でも述べられていたように企業との協力は非常に重要**であろう。一方で、企業を介入させてサイバーセキュリティ対策を講じていくためにはその分の予算が必要となる。この**予算をど**

のように確保するかは課題であり、これには医療機関の経営層のサイバーセキュリティ対策を講じることの理解と国の援助が一つのポイントになるかもしれない。これは日本でも同じ課題と考えられ、米国よりも被害が少ない日本（実際にはサイバー攻撃の発生に気づいていないだけかもしれないが）においてサイバーセキュリティの予算を確保することのハードルは更に高いと考える。このためすぐにサイバーセキュリティ対策を構築する機運を高めることは難しいかもしれないが、先ずは本講演で紹介されたサイバー攻撃による患者への影響などを関連学会で地道に講演していくことが一つの重要な取り組みになると考える。

3.2. From Good to Great How to Accelerate Your Cybersecurity Program

【概要】

本講演では、First Health Advisory 社の Andy Ulvenes 氏、Olin Dillard 氏、UT Health San Antonio の Gene Winfrey 氏から医療機器のサイバーセキュリティ・プログラムを加速する理由、実際の方法についての講演がなされた。First Health Advisory 社は、サイバーセキュリティを構築していくためのコンサルティング、リスク管理などを提供する企業であり、UT Health San Antonio は医療機関である。そして、Gene Winfrey 氏はバイオメディカルエンジニアとして活躍しており、医療機器の修理、医療機器の有効性と安全性を確認するなどの医療機器安全管理の実務を担っている。バイオメディカルエンジニアは日本の臨床工学技士のように臨床業務を実施せず、医療機器の保守点検や修理などを業務としている。

【講演内容】

First Health Advisory 社ではサイバーセキュリティ・プログラムの実装に取り組んできた。サイバーセキュリティ・プログラムとは、First Health Advisory 社のマネージド・サービスフレームワークである。具体的には、サイバーセキュリティ対策を検討するにあたってのよくある落とし穴となる予算不足、対象範囲（IoMT, IoT, OT, IoXT のどこまでを対象とするか)、説明責任（IS と HTM の明確化）などに対して、継続的なリスク管理、インシデントレスポンスとリカバリー、パッチ戦略とセキュアコンフィグレーション、脆弱性管理と改善、予算の確保、アセスメントを提供している。

このようなサイバーセキュリティ・プログラムのサービスについて、医療機関にとっては非常に有益とされている。医療機関ではサイバーセキュリティ対策を実装させようとしてもサイバーセキュリティ対策をどのように実装していいかが難しく、完璧なセキュリティ対策を実装しようとすれば莫大な資金が必要になるなどの課題が多々存在する。このような状況の中で、サイバーセキュリティ・プログラムを導入することは課題解決への道筋を示してくれるものであるとされた。例えば、コンサルティングを受けてサイバーセキュリティ

を講じるには単にスタッフを増員すればよいというわけではなく、脆弱性管理やガバナンス管理から成長させていくことが必要であるということの気づきを与えてくれるとされた。

サイバーセキュリティ対策の実施すべき項目の例としては、アクセス制御とアプリケーション管理、脆弱性管理、リレーションシップ・マネジメントが必要とされた。アクセス制御とアプリケーション管理とは、コンプライアンス管理であり、不正なアクセスを監視することである。脆弱性管理は機器の脆弱性の順位付けを行うことが一つ挙げられ、各機器のリスク要因、重要度、使用者によってリスクの順位付けを行うことができる。そして、もう一つはリスク低減計画を立てることであり、vRAP(Vulnerability Remediation Action Plan、脆弱性改善アクションプラン)を立てて外部および内部ネットワークのリスク低減対策を実施すること、IMHP (IoMT Mitigation & Hardening Profile)により継続的なパッチ管理戦略と安全なデバイス設定によるデバイスのハードニングを実施する。そして、リレーションシップ・マネジメントは HTM(Healthcare Technology Management)※と CIO(Chief Information Officer、情報システム担当役員）とのリレーション構築であり、CIO と HTM でセキュリティ目標およびビジネス目標の共有、コミュニケーションを図ることが重要である（図 4)。

※HTM とは医療機関における医療機器のマネジメントを担当する分野を指しており、医療機器の保守点検、修理、サイバーセキュリティなどが含まれる。

図 6　アクセス制御とアプリケーション管理、脆弱性管理、リレーションシップ・マネジメントの概要

【考察】

本講演ではサイバーセキュリティ対策のサービスを受けている医療機関側の話がなされたが、企業が介入することのメリットを感じるものであった。講演の中であったように、医

療機関側がサイバーセキュリティ対策を講じていくためには、どのようなことから始めればよいかわからないという意見が散見され、企業が介入することで課題解決が進みやすくなると考える。一方で企業の介入はやはり予算の確保が課題となるため、医療機関の規模が大きい施設で予算がある程度確保されている場合には企業の介入を検討することも考えられるかもしれない。

他方、**サイバーセキュリティ対策を実装していくための方法としてアクセス制御とアプリケーション管理、脆弱性管理、リレーションシップ・マネジメントが必要**とされていた。この中でアクセス制御とアプリケーション管理、脆弱性管理に関してはリスク低減が主な目的と考えられ、リスクを限りなく減らすことはサイバーセキュリティ対策として重要と考えられる。しかしながら、これらの対策にはやはり専門的な知識を要することから医療機関に専門家を配置することが必要と思われ、この観点からしても企業の介入は重要と考えられる。一方で**米国の臨床工学技士は医療機器の保守点検の専門性が高く、その守備範囲は電子カルテシステムにも及ぶ**とされている。このため、**ネットワークシステムにも精通する従事者が多く存在していることも考えられ、専門的な知識を要するサイバーセキュリティ対策であってもある程度は実施が可能**と考える。米国のようにある程度のシステム関連の知識が身についていると、例えば、自施設のシステム部門や本講演のようなサイバーセキュリティ対策の企業と議論する際に、医療従事者は臨床現場目線からの議論を、企業等は専門家目線からの議論が可能になると連携がより強固になると考えられる。

3.3. New Legislation and Regulations Are Evolving HTM. Are You Prepared?

【概要】

本講演は TRIMEDX 社の Scott Trevino 氏からサイバーセキュリティの現状やこれに関連する法律、サイバーセキュリティのコンプライアンスと安全性を維持するために必要な方法についての講演であった。Scott Trevino 氏は TRIMEDX 社のサイバーセキュリティ・ソリューションの価値、成長、進化を実現するための戦略を定義する取り組みを指揮している。サイバーセキュリティ、テクノロジーのトレンドを見極め、顧客、市場、業界のニーズの進化を認識・予測し、顧客のニーズを満たし、顧客に価値をもたらす市場をリードするソリューションに変換する責任を担っている。

【講演内容】

米国では医療分野のサイバー攻撃が年々増加しており、2021 年には週平均で 758 件のサイバー攻撃が発生したのに対して、2022 年は 1410 件であり 86%増加した。このような状況の中、米国で医療機器のサイバーセキュリティの課題として挙げられるのは、サイバー攻撃 1 件当たりの被害額の増加、ネットワークに接続される医療機器の増加、現在リリース

されているネットワークに接続される医療機器の半数がサイバー攻撃の重大な脆弱性を有していること、サイバーセキュリティ人材の不足である。また、サイバー保険の保険料増加も課題であり、補償範囲が狭く、適用除外が広いため、どのような攻撃を受けた場合に補償を受けられるかが不明となっている（図 5）。他方、患者への影響についてはサイバー攻撃を受けた医療機関の中で 70%において治療の遅延が発生し、患者の合併症の増加が見受けられたとされた。

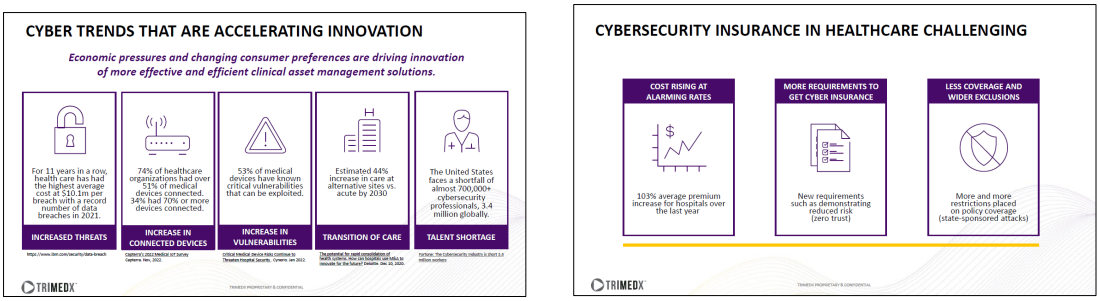

図 7　サイバー攻撃のトレンドとサイバー保険

サイバー攻撃は発生の要因を特定するのに 200 日以上要し、その封じ込めには 70 日を要するとされている。これを踏まえると、サイバー攻撃を特定・検知し、対応・復旧する能力が構築されていないことと捉えられる。

サイバーセキュリティの法律に着目すると、米国ではサイバーセキュリティに関する多くの法案が出されており、最近の 2 年間では 4 つの法案が可決され法案成立のスピードが加速している。具体的には、2021 年には「The State and Local Government Cybersecurity Act of 2021」が可決され、DHS（United States Department of Homeland Security、アメリカ合衆国国土安全保障省）によるサイバーセキュリティ評価と技術支援の提供、サイバーセキュリティ導入のための補助金プログラムが創設された。2022 年には「Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)」が可決され、重要インフラ事業者と連邦政府機関は、CISA（Cybersecurity and Infrastructure Security Agency、サイバー攻撃をサイバーセキュリティ・インフラ安全保障局）に報告することが義務付けられた。これにより、サイバー攻撃の発生後 72 時間以内に攻撃の報告とランサムウェア攻撃による支払いは 24 時間以内での報告が義務付けられた。さらに、2022 年は「Strengthening American Cybersecurity Act of 2022」が可決され、重要インフラへの脅威に対する対処、連邦政府機関の連携強化、すべての民間機関がすべての攻撃を CISA に報告することを義務付けられた。2023 年は「Consolidated Appropriations Act(Omnibus Bill / FDORA)」が可決され、医療機器の市販前承認プロセスの一環として医療機器のサイバーセキュリティの確保が義務付けられ、さらに FDA から医療機器のサイバーセキュリティ管理のための市販前申請の内容に関するガイダンスを公表すること、機器のサイバーセキュリティ向上に関する公的リソースを提供することなども盛り込まれた。ここでのサイバーセキュリティの確保とは、

SBOM の提供、脆弱性の開示、ファームウェアのパッチやアップデートによる安全性の確保などである。(図 6)

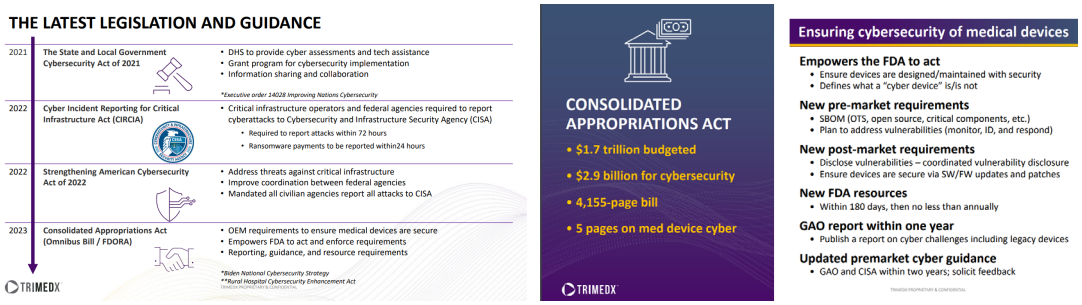

図 8　米国で可決されたサイバーセキュリティに関連する法律

サイバーセキュリティの安全性を高めていくための方法としては、医療機器の台帳管理は非常に重要である。医療機器の台帳管理を行うことで脆弱性の可視性の向上、既知のパッチと改善策の特定、リスク低減活動、戦略、計画の効率的な優先順位付けなどに有用とされている。また、従事者のスキルアップも重要であり、例えば、教育と資格取得の機会に投資すること、臨床工学部門に対して IT やソフトウェア関連のスキルアップを図ることが重要とされた。

【考察】

本講演ではサイバーセキュリティの法律について触れられており、ここ数年の出来事を見ると米国では国が主体となってサイバーセキュリティに対策に注力していることを改めて実感した。特に **2023 年の「Consolidated Appropriations Act(Omnibus Bill / FDORA)」は医療機器のサイバーセキュリティに対する具体的な法律であり、安全な医療機器を流通させるための強固な対策**であると考えられる。他方、サイバーセキュリティの安全性を高める方法としては、臨床工学部門のスキルアップも重要とされた。ただし、本公演内においても具体的な実施方法までの言及はなかったことから、世界的にも議論、検討段階にあると考えられた。そのため、本邦においても世界に遅れをとらないように取り組みを進めるべきである。

3.4.　Who Should Lead Medical Device Cybersecurity Management?

【概要】

本講演では、医療機関でサイバーセキュリティを講じていくにあたって、臨床工学部門と IT 部門のそれぞれでイニシアチブをとることの長所と短所について取り上げるものであった。演者は Health-ISAC の Phil Englert 氏であり、臨床工学に精通し、現在は医療機器ライフサイクル管理プログラムに関わっている。もう一人は、Medsec の Jim Keller 氏であり、

患者安全、技術管理、サイバーセキュリティの専門家である。

【講演内容】

昨今では医療機関におけるサイバー攻撃は多く発生しており、サイバー攻撃の事例としては、ドイツのデュッセルドルフ大学病院におけるランサムウェア攻撃、米国のアラバマ州モービルのスプリングヒル・メディカル・センターにおけるランサムウェア攻撃、米国のテネット・ヘルスケアのサイバー攻撃、南オハイオ医療センターのサイバー攻撃などが挙げられる。このような状況の中、FBI と FDA からサイバーセキュリティに関する施策が公表され、FBI はレガシーデバイスに対してサイバーセキュリティ脆弱性に対処するための推奨事項を発表し、FDA からは新たな規制として医療機器の市場投入に際して医療機器が安全性を考慮して設計されていることが求められるようになり SBOM の提出、パッチ適用が義務付けされた。

医療機器のサイバーセキュリティにおける課題としては、医療機器の台帳管理が十分に実施できないこと、パッチ適用がなされていないこと、サイバーセキュリティの役割と責任の不明確さなど 10 の課題が挙げられる。そして、これらの課題に対応していくためには、ベンダーによる管理、台帳管理、サイバー攻撃の継続的な監視、事故報告などを講じていくことが必要となる（図 7)。

図 9　サイバーセキュリティの課題とマネジメント

米国では医療機関におけるサイバーセキュリティ対策の実施主体は、臨床工学部門と IT 部門がリーダーシップをとりながら実施されている。それぞれの部門の特徴としては、臨床工学部門は医療機器技術と臨床現場に関する深い知識、顧客サービス重視、”患者の安全"を原動力とする対応力が備わっている。一方、IT 部門は、ソフトウェア、ネットワークのスキルセットを持ち合わせているものの、臨床的視点に欠けていること、コンセンサス志向でプロセスメトリックスに重点を置いているため、機敏な対応ができないかもしれないという弱みがある。

このように医療機関でサイバーセキュリティ対策を講じるにあたり、臨床工学部門と IT 部門にそれぞれの強みと弱みがあるが、どちらが適しているのか実際の医療機関の現状を把握すべく調査が実施された。本調査には 42 人が回答し、回答者の属性は IT 部門、臨床工学部門、リスクマネジメントなどであった。調査の結果、サイバーセキュリティ担当部署

は、IT 部門と臨床工学部門でおよそ 50%：50%の回答であった。また、医療機器のサイバーセキュリティはどの部門が主導すべきか、という質問に対しては IT 部門と臨床工学部門でおよそ 50%：50%の回答であった。回答者の施設において医療機器のサイバーセキュリティ対策が実施できている項目としては、リスクアセスメント、台帳管理、ネットワーク監視が多く挙げられた。一方、医療機器のサイバーセキュリティ対策が実施できていない項目としては、パッチ管理、脆弱性管理が多く挙げられた。

本調査結果を踏まえたまとめとしては、医療機器のサイバーセキュリティ対策において臨床工学部門と IT 部門はどちらも主要な部署であり、どちらかがイニシアチブを取ってサイバーセキュリティ対策を実施していくことが必要である。どちらの部署が主導していくかは各医療機関でサイバーセキュリティの主導権をどの部署が持つかによって決まる。しかしながら、演者の考えとしては、サイバーセキュリティ対策は臨床工学部門が多くを担うことになり、そのためのリソースを確保することが必要と考えている。

【考察】

本講演で発表された調査から米国ではサイバーセキュリティのイニシアチブを持つ部署が明確になっていることがわかった。これはサイバーセキュリティ対策の責任がどこにあるかが明確になっているとも捉えられ、これにより具体的なサイバーセキュリティ対策を実施せざる負えないため、具体的な対策が可能になるのではないかと考えられる。例えば、カナダの病院においても Clinical Engineer が主体となってサイバーセキュリティ対応に取組んだ知見が報告されたりもしている。他方、**サイバーセキュリティ対策の実施主体をどこの部署が担うかは重要となるが、さらに重要なのは臨床工学部門と IT 部門が情報共有をすること**と思われる。例えば、臨床工学部門がネットワークに接続される医療機器の台帳管理を作成しているのであればこれを IT 部門と共有して医療機器へのサイバー攻撃のリスクを把握しておくことが必要と思われる。

日本でも米国のようにサイバーセキュリティ対策の実施主体を明確にしておくことが重要と考えるが、日本の医療機関では IT の専門家がいない施設が多い中でどこの部署が担うかは難しい判断と思われる。しかしながら、**臨床工学技士が配置されている医療機関においては保守点検のスペシャリストとして臨床工学技士が先ずは参入していくことが必要**かもしれない。

4. おわりに

教育セッション全体を通したまとめとしては、米国の医療機関におけるサイバーセキュリティ対策は専門的な領域に踏み込んだ対策が求められているが、これはネットワークシステムの知識を持ち合わせた臨床工学技士や IT の専門家が配置されていることが前提にあると思われる。そして、臨床工学技士と IT の専門家は各々でセキュリティ対策を実施する

のではなく、お互いに協力体制を構築し、医療機器の保守点検実務者と院内システムの管理者のお互いの視点を掛け合わせることがセキュリティ強化に重要と考えられる。

一方、**日本においても臨床工学技士がサイバーセキュリティ対策を講じることへの期待が高まっているが、米国のようなサイバーセキュリティ対策を講じていくためには、専従者を配置して専門性を高めることが必要**であり、臨床業務の傍らで実施することは難しいであろう。日本ではタスクシフトにより臨床工学技士の臨床業務の範囲が拡大しつつあるが、将来的に臨床工学技士がサイバーセキュリティ対策を担っていくためには臨床業務と切り離して新たな業務として確立することが重要と考える。

他方、**サイバーセキュリティ対策は、あくまでも各医療機関が独自で実施するリスクマネジメントの一つであり、対策を講じることによる診療報酬のようなインセンティブはないと考えられるが、現場はサイバーセキュリティに対する専門性を高め安全に医療を提供できる基盤の検討が進められていた**。これを踏まえると、米国ではどのような考えの下でサイバーセキュリティ対策の機運を高めているのか、また、米国全体の医療機関がどの程度の割合でサイバーセキュリティ対策を講じているのかは不明である。これらの疑問については今後調査すべきテーマであり引き続き調査を継続していく。

最後に今回 AAMI に参加して海外の医療事情に触れられたこと、日本医療機器学会の先生方からお話を伺えたことは大変貴重な経験となった。AAMI への参加を許可していただいた医療機器センターおよび AAMI に共に参加させていただいた日本医療機器学会の先生方に対して深い感謝を申し上げる。

公益財団法人
医療機器センター

Me＝Medical Equipment（医療機器）はそれぞれの“私”のために。
医療機器は 家庭にまで広がっています。医療機器を“私”の身近なものに感じること、それがさらなる発展の鍵となります。
『企業、研究者、医療者、患者、行政のお互いがそれぞれの“私” を信頼する気持ち、それが明日の医療機器を育てていく。』
という願いを Me にこめました。
“！”は、それぞれの“私”のあらゆる気づき、ひらめきを大切に、当財団の 一人一人が飛躍していきたいという意志を表しています。
ブルーは透明性、技術の高さ、中央の明るい色使いは未来への希望を意味します。

公益財団法人医療機器センター（理事長：菊地眞、東京都文京区本郷）は、医療機器の研究開発等に関する調査研究を行い、その適正な普及及び向上を助長奨励するとともに認証を行い、医療機器産業の健全な発展を図るとともに、臨床工学技士の育成に努め、もって国民の健康増進及び医学の向上に寄与することを目的に 1985 年に設立された公益法人です。