令和７年度　第１回大阪府薬事審議会医療機器等基準評価検討部会　議事録

日時：令和７年８月６日（水）午後２時から午後４時まで
場所：大阪赤十字会館　４０２会議室

１．参加者

委　員：岡本剛、菅原充史、長澤良樹、能勢明、一橋俊司、芳田豊司
講　師：中里俊章
事務局：井上和幸（薬務課長）、中嶋覚子、長野優里、安清準、蓮井良美（以上、薬務課製造調査グループ）

２．配付資料

・次第
・名簿、配席図
・資料１：令和７年度第１回大阪府薬事審議会医療機器等基準評価検討部会 事業概要
・資料２：医療機器のサイバーセキュリティに関する課題
・資料３：意見交換について
・参考１：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第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準
・参考２：【令和６年度 総括･分担研究報告書】医療機関における医療機器のサイバーセキュリティの確保等のために必要な取組の研究

３．議事

【事務局】

定刻となりましたので、ただいまより令和 7 年度第 1 回大阪府薬事審議会医療機器等基準評価検討部会を開催いたします。私は本日司会を務めさせていただきます、大阪府健康医療部生活衛生室薬務課の長野です。委員の皆様方には、お忙しい中、ご出席いただきましてありがとうございます。本日は全ての委員の皆様にご出席いただいておりますので、大阪府薬事審議会部会設置規程第５条第２項により、本部会は有効に成立しておりますことをご報告申し上げます。当部会は、大阪府情報公開条例第 33 条に基づき、原則公開で行うこととなっておりますので、ご了承ください。ただし、議事進行の途中におきまして、その内容が公開にふさわしくないと考えられる場合には、委員協議の上、非公開とすることができますことを申し添えます。それでは、開会にあたりまして、大阪府健康医療部生活衛生室薬務課長の井上よりご挨拶申し上げます。

【事務局】

大阪府薬務課の井上でございます。本日は業務ご多忙の中、本部会にご出席いただき、厚く御礼申し上げます。また、日頃より、本府の薬務行政の取り組みにご理解、ご協力をいただいておりま

すこと、この場をお借りして、御礼申し上げます。
　さて、社会の IT 化が進み、様々な場面でデジタルツールが活用される中、令和 4 年 10 月には府内医療機関でランサムウェアを用いたサイバー攻撃を受けて、電子カルテが使用不能となった事例がございました。医療の提供に支障をきたす事態が発生したということで、大きな社会的な話題にもなっております。医療機器におきましても、様々な機器にプログラムが組み込まれており、インターネット等と接続するようになって、医療機器に対する不正アクセス、サイバー攻撃を防ぐための対策が求められております。令和 5 年 4 月には、薬機法第 41 条第 3 項の規定による医療機器の基準、いわゆる基本要件基準が改正されまして、サイバーセキュリティに係る危険性の特定や評価、低減するための管理が必要となり、今年の 5 月には能動的サイバー防御に係る法律が制定されております。このように、プログラムを用いた医療機器の製造販売において、高度化するサイバー攻撃への対応が喫緊の課題であり、早急な対応が求められていることから、府としてもサイバーセキュリティ対策への理解促進のための取り組みを、２ヵ年計画で検討したいと考えております。第 1 回目となります本日は、事例やガイドラインの紹介とともに、一般社団法人日本画像医療システム工業会より、中里俊章様をお招きして、現状や課題をご説明いただきます。中里様は、民間企業において、ソフトウェアの設計・開発に従事されたご経験をお持ちであり、その後、第三者機関や PMDA に在籍された期間を通じて、医療機器に関する多角的な考察と実務経験を積まれてきました。さらに、IMDRF のガイダンス策定にも関与されておりまして、現在では様々な部会や委員会に参加されながら、国際基準及び日本産業規格の策定にも携わっておられます。本日の部会により、サイバーセキュリティ対策への理解が深まり、今後の円滑かつ効果的な検討を期待しておりますので、皆様には忌憚のないご意見を賜りますようお願いしまして、簡単ではございますが、開会の挨拶とさせていただきます。
【事務局】
　続きまして、本日ご出席の委員を五十音順にご紹介させていただきます。（各委員紹介）
　また、本日は、医療機器のサイバーセキュリティの現状や課題について、専門的な観点からご講演いただくため、一般社団法人日本画像医療システム工業会産業戦略室シニアリサーチャーの中里俊章様にご参加いただいております。
　続きまして、事務局より自己紹介させていただきます。（事務局自己紹介）
　また、本日は傍聴者がお一人いらっしゃいますので報告いたします。
　次に、配付資料の確認をさせていただきます。（配布資料確認）
　それでは、これからの議事進行は部会の設置規程により部会長にお願いしたいと思います。
【芳田部会長】
　芳田でございます。本日はお忙しい中、当部会にご出席いただきありがとうございます。また、中里様におかれましては、ご多忙のところ、遠方よりご出席いただき、誠にありがとうございます。さて、本年度より、医療機器等製造販売業者の皆様の一助となるよう、サイバーセキュリティ対策への理解促進を目的とした取り組みについて、２ヵ年計画で進めてまいります。本日はその第一回目として、現状の課題等を共有し、今後の方向性について、皆様のお知恵をお借りできればと考え

ております。本日ご参加いただいている委員の皆様の業務の中で、ソフトウェア搭載機器の扱いやサイバーセキュリティへの関わり方には、それぞれ違いがあるかと存じます。そのため、今日は専門性の有無にかかわらず、サイバーセキュリティ対策についての素朴な疑問や、日頃感じておられることをざっくばらんに意見交換できる場にしたいと思っております。それでは、早速ですが、議題に入らせていただきます。本部会のテーマである「医療機器のサイバーセキュリティ対策への理解促進に向けた検討」の事業概要について、事務局よりご説明をお願いいたします。

【事務局】

本日は、まずは薬務課より事業概要を説明させていただき、その後中里様から「医療機器のサイバーセキュリティに関する課題」についてご講演いただきます。講演が終了しましたら、意見交換を実施し、現在懸念されている点や苦慮している点などを挙げていただきます。それでは、本部会の事業概要について、ご説明いたします。

まず、医療機器ネットワーク化の進展とその影響についてお話しします。近年、医療機器の高度化とともに、ネットワーク接続が標準化されつつあります。これは、医療現場における診療の質と効率を大きく向上させる一方で、新たなリスクも生じています。利点として、例えば「リアルタイムなデータ共有」、「遠隔モニタリングと遠隔診療の実現」、「機器の稼働状況の監視と保守の効率化」などを挙げることができます。リアルタイムなデータ共有については、患者のバイタル情報や検査結果を即座に医療従事者間で共有でき、迅速な診断・治療が可能になります。遠隔モニタリングと遠隔診療の実現については、在宅医療や地域医療において、医師が遠隔から患者の状態を把握できる体制が整います。機器の稼働状況の監視と保守の効率化については、ネットワークを通じて機器の状態を常時監視し、故障予兆の検知やメンテナンスの自動化が可能になります。

こうした利点がある一方で、ネットワーク化に伴うリスクもあります。例えば「サイバー攻撃による機器の停止や誤作動」、「患者情報の漏洩・改ざん」などを挙げることができます。サイバー攻撃による機器の停止や誤作動については、ランサムウェア（身代金要求型ウイルス）やマルウェアにより、医療機器が操作不能となる事例が国内外で報告されています。医療機器が外部からの攻撃を受けた場合、機器の機能に支障が生じ、患者の安全性に重大な影響を及ぼす可能性があります。製造販売業者としては、こうしたサイバーセキュリティ上の危険性を適切に特定及び評価し、ライフサイクル全体を通じてリスクを低減する管理を行う必要があります。患者情報の漏洩・改ざんについては、ネットワークを介した不正アクセスにより、個人情報が外部に流出するリスクがあります。医療における患者情報は取扱いに注意が必要な情報であり、漏洩や改ざんが起きた場合、患者の信頼を損なうだけでなく、製造販売業者としても情報の取扱いやセキュリティ対応について薬機法に基づく責任を問われる可能性があります。医療機器のネットワーク化は、医療の質を高める大きな可能性を秘めています。しかし、その利点を最大限に活かすためには、サイバーセキュリティ対策を同時に強化することが不可欠です。利点が多くとも、リスクの重大性を踏まえた体制整備と、サイバーセキュリティ対策を講じることが必須です。

続きまして、サイバー攻撃の脅威についてご説明します。近年、医療機関を標的としたサイバー攻撃は急増しており、診療の停止や個人情報の漏洩といった深刻な被害が、国内外で報告されてい

ます。主な脅威として、１つ目は「ランサムウェア攻撃」です。医療機関のネットワークが暗号化され、復旧と引き換えに金銭を要求されるもので、電子カルテや医療機器の操作ができなくなり、診療が停止するケースもあります。２つ目は「医療機器への不正アクセス」です。ネットワークに接続された医療機器に侵入されることで、設定が改ざんされたり、誤作動が引き起こされたりするリスクがあり、患者の生命に関わる可能性もあります。３ つ目は「サプライチェーン攻撃」です。医療機器メーカーやソフトウェアベンダーを経由して、マルウェアが医療機関に持ち込まれるケースです。そして４つ目が「内部要因による情報漏洩」です。職員によるUSB メモリの誤使用やパスワード管理の不備など、人的ミスによって情報が漏洩する事例もあります。こうした脅威に対して、国内外では医療機器のサイバーセキュリティに関する法規制やガイドラインが整備されつつあります。

次に、医療機器のサイバーセキュリティに関する主要な法規制とガイドラインについてご紹介します。これらの法規制やガイドラインは、医療機器の設計・製造・運用のすべての段階で、セキュリティを確保するための重要な指針となっています。国内では、基本要件基準第 12 条第３項において「プログラムを用いた医療機器に対する配慮」が規定されており、令和５年厚生労働省告示第67 号により改正され、令和５年４月１日から適用されています。また、JIST81001-5-1 は、医療機器のソフトウェアに対して、製品ライフサイクル全体でのセキュリティを確保するための国際的な基準として位置づけられています。国際的には、国際医療機器規制当局フォーラム（IMDRF）が、医療機器のサイバーセキュリティ強化を目的として、３つのガイダンス文書を策定しています。これらの文書では、医療機器の安全性と信頼性を保つために、製造業者、医療機関、規制当局など、それぞれの立場で果たすべき役割と責任が示されています。さらに、IMDRF ガイダンスの発行など、国際的な枠組みでの活動を踏まえ、医療機器へのサイバー攻撃に対する耐性基準等の技術要件を導入して整備することを目的として、医療機器製造販売業者向けに「医療機器のサイバーセキュリティ導入に関する手引書」が取りまとめられており、現在は第２版が公開されています。これらのガイドライン等を活用し、組織的かつ継続的なセキュリティ対策を実践していくことが求められます。しかしながら、こうした整備が進んでいるにもかかわらず、現場では依然としてサイバー攻撃による被害が発生しています。

次に、実際に報告されているサイバー攻撃の具体的な事例をご紹介します。国内外における医療機関へのサイバー攻撃事例を紹介します。まずは国内についてです。国内のサイバー攻撃事例の多くは、医療機器そのものへの直接攻撃ではなく、医療機関の情報システムやネットワーク全体を標的とした攻撃です。徳島県つるぎ町立半田病院においては、ランサムウェアに感染し、患者の診察記録を預かる電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用できない被害が生じました。ランサムウェア感染の発覚後は、ネットワークの遮断や端末の停止などを行い、救急や新規患者の受け入れを中止し、手術も可能な限り延期にするなど、病院としての機能は事実上、停止する状態に陥り、通常診療の再開に約２ヵ月を要しました。大阪急性期・総合医療センターは、給食センターのサーバーから病院が管理するサーバーへリモートアクセスが行われ、電子カルテシステムを始め様々な部門システムにランサムウェアを感染させる攻撃が行われ、シス

テムを使用停止せざるを得ない事態に陥りました。病院は医療継続のために、紙カルテ運用の開始、外来診療の制限、救急受入の停止、予定手術の停止などを判断しました。オフラインバックアップデータを参照可能にするシステム、基幹システム並びに部門システムを段階的に構築・接続し、通常診療の再開まで約２ヵ月を要しました。岡山県精神科医療センターでは、ランサムウェアに感染し、サーバーや端末の情報窃取、ウイルス対策ソフトの停止・削除、電子カルテシステムの暗号化などの被害が発生し、完全復旧まで約３ヵ月を要しました。原因は、管理者パスワードの使い回しや、端末ユーザーへの管理者権限の付与によるセキュリティ対策の不備であり、徳島県つるぎ町立半田病院、大阪急性期・総合医療センターの事例と同様に脆弱性が要因です。一方、福島県立医科大学附属病院では、放射線撮影装置の不具合により画像の再撮影が必要となった事例があり、院内調査の結果、ウイルス感染の可能性が判明しました。院内ネットワークはインターネット非接続であったため、既に感染していた端末を院内に接続したことが原因と推定されています。情報流出や身代金要求は確認されていませんが、インターネットに接続されていない環境でも、内部要因による感染リスクが存在することが示された事例です。

次に、海外での事例です。イギリスに所在するシノビス社は、血液検査や病理検査サービスを提供する企業です。検査結果は電子的に医療機器や電子カルテと連携され、診断・治療に活用されます。本件は、シノビス社のシステムに侵入、患者データを暗号化され、検査結果の取得・連携が不能となり、患者情報も意図せず公開されました。停止されたシステムの復旧に約５ヵ月を要しましたが、現在も公開されたデータについて調査中とのことです。その他、サイバー攻撃の事例は複数存在しており、医療機器の製造販売業者にとって、サイバーセキュリティ対策は不可欠です。

最後にプログラム医療機器におけるサイバーセキュリティに関する改修の事例を紹介します。昨年 11 月に改修がありました「汎用画像診断装置ワークステーション」についてです。当該医療機器は診療のために画像を提供する装置であり、多くの医療機関で使用されているかと存じます。セキュリティの潜在的な脆弱性が存在し、この問題によって悪意のある第三者がシステムにアクセスして患者データが操作されてしまう可能性があることが判明し、改修に至りました。危惧される点としては、ソフトウェアの脆弱性が悪用された場合、不適切な診断または治療につながる可能性があります。続いての事例は、心不全時の補助循環に使用される機器であり、当該機器はサイバーセキュリティ対策が必要な製品でした。特定のソフトウェアバージョンがインストールされた製品において、サイバーセキュリティに脆弱性が認められ、これら脆弱性のいずれかが悪用された場合、イーサネット通信が失われ、本製品から病院情報システム・臨床情報システムに治療及び波形データが送信できなくなるおそれがあることから改修となりました。万が一当該不具合が発生し、機器が緊急停止した場合、患者に直接的な健康被害が生じることとなります。このような改修事例からも分かるように、医療機器のサイバーセキュリティ対策は、製造販売業者にとって重要な取り組みです。脆弱性が見つかった際には速やかに対応することが求められます。また、今後も設計から運用までの各段階で、セキュリティを考慮した対応を継続していくことが重要です。

以上より、本部会のテーマとして、医療機器のサイバーセキュリティ対策への理解促進に向けた検討をしていきたいと存じます。こちらは参考になりますが、厚労省や PMDA のホームページに

おいて、通知の掲載やサイバーセキュリティについての動画も公開されています。また、厚生労働科学特別研究事業（厚労科研）におけるアンケート調査の研究報告書も公開されております。以上です。

【芳田部会長】

ありがとうございました。ただいま事務局から本部会の事業概要についてご説明いただいたところです。サイバーセキュリティが必要であることは認識していますが、今日改めて、事業概要をお聞きしますと、重要性と対応する必要性を改めて感じるところでございます。本日は、中里様のご講演の後まとめてご質問等を伺いたいと思います。続いて、中里様より医療機器のサイバーセキュリティに関する課題をご講演いただきます。中里様、よろしくお願いします。

【中里様】

本日は少し厳しいお話もしなければならないと考えております。また、多くの方が勘違いされていることや、混在して考えていらっしゃる部分もあるので、その辺も整理していければと思います。

今日は「課題」をテーマとして話させていただきます。一つ目の課題は「医療機関との連携」です。厚労科研の方では、昨年までは医療機器そのものに関する課題に取り組んでいましたが、今は、次の段階として、医療機器を医療機関に導入するときの、「医療機関側との連携における課題」に取り組んでいます。この「医療機関との連携に関する課題」の中で、多くの部分で勘違いされていると考えています。先ほどもインシデントの話がありましたが、岡山の件については、大阪急性期や半田病院に比べれば、はるかに短期間で対処ができています。なぜそこにたどりつけたかと言いますと、大阪急性期の事例で多くのポイントや課題が明らかになったからだと思っています。報告書についても、大阪急性期の報告書がベースとなり、整理された形で岡山の報告書が出ています。

一番のポイントは、「閉領域であればセキュア（安全）」という考え方は誤っているということです。重要インフラの中で一番サイバーセキュリティの対応が遅れているのが医療分野だと言われています。なぜかというと、インターネットから医療機関のシステムに入り、医療情報システム・病院情報システムがあり、そこから内側は閉領域だと多くの人が思っているからです。特に医療情報の中で医療機器が接続されているシステムになると顕著で、医療機器の取扱説明書に「医療機器はセキュアな状態、セキュアな空間に設置して使うことが前提である」という旨が書かかれているケースがありますが、これは国際的には全く理解できないと言われています。実際 OS のサポートが終了した Windows７の機器が 2020 年の段階で販売されています。世間的には売ってはいけないようなものが医療機器では売られているわけです。「閉領域だから安全であり、何を売っても、どういう状態で運用しても構わない」という考え方があるからそのような事態が起こっています。販売業がそう考えるのは、製販業がそう考えているからと思われても仕方ないです。この「閉領域だから安全」という考え方を改めない限り、医療機器・医療機関におけるサイバーセキュリティ、セキュアな状態を保つことはできません。

特に最近の設置管理医療機器では、リモートメンテナンスがあります。リモートメンテナンスは他の分野でもありますが、医療分野では他の分野に比べて 10 倍あるという調査結果があります。技術的な問題や内部のセキュリティに関わる問題、脆弱性はどの分野でもあることですが、大阪急

性期のレポートで、医療機器の契約の問題について言及されています。情報システム系は最近、保守の契約を結んでいく傾向にありますが、医療機器に至っては、責任の所在を示す契約はほとんど結んでいません。全体的に見ても 10%にも満たないです。何の契約もなく設置しており、リモートメンテに関してはほとんど無契約です。リモートメンテの機材に関しては、ほとんどがメーカー側の資産である機材が使用されています。令和７年の医療監視において、リモートメンテナンスの確認が求められているにも関わらず、医療機関側からはリモートメンテの機材の中身が見えず、アップデートされているかどうかもわからない状況です。この状況に正しく対応していかなければなりません。そもそも契約が結ばれていない理由はリモートメンテナンスで使用する機材が医療機器ではないというスタンスがあるからです。

サイバーセキュリティ関係の団体から「経産省のガイドラインは大阪急性期のインシデントを最悪のケースとして作られている。それぐらいひどかった」と言われています。あのインシデントは、たまたま給食システムから侵入されましたが、医療機器から侵入されてもおかしくないぐらい、医療機器はひどい状況であるという調査結果が経産省のワーキングで報告されています。このような状況をいつまでも放置できないということを最初にお話する必要があると思っています。閉領域だから安全ということを意識してはいけません。このインシデントへの対応は医療機器については未だに十分にできてないということです。

もう一つ、勘違いしてはいけないのは、組織のリスクマネジメントと医療機器のリスクマネジメントは違うということです。製販業側も医療機関側も混同して考えているところがあるので、そこは分けようと、厚労科研の中で考えています。「USB をコントロールしましょう」や「勝手に持ってきた PC は繋げないようにしましょう」などは組織のリスクマネジメントであり、例えば ISMS（ISO/IEC27001 など）に基づく情報システム系のリスクマネジメントです。一方で医療機器は患者の生命・安全に関わるもので、ISO14971（医療機器のリスクマネジメント）で対策を講じる必要があります。相互にオーバラップするところもあり、患者への影響があるところは ISO14971 ですが、それを組織で守るという ISMS のリスクマネジメントもかぶさってきます。特に CT や MRI などの設置管理機器等は、海外に輸出する場合、ISO14971 の対策が必要ですが、ISMS の認証書の提出を求められるケースが非常に増えています。今、両方のリスクマネジメントができているかという見方をされており、混同してしまうと、医療機器としての適切な対策も打てなくなります。

次に、医療機関の医療監視におけるチェックリストのことですが、令和 7 年より二要素認証が追加されています。これは一般の情報システムのことだから医療機器には関係ないと思っている方もいらっしゃるかもしれませんが、情報システム系に接続される医療機器も対象となります。１段目としては、例えば管理区域に置いているものはまずカバーされるという考え方があります。ただ、その後の２段目ですが、装置側でログイン機能を持っていなければいけません。例えば手袋した人が指紋認証できない時には、カード認証を持ち込むなどの対策を打てばいいだけの話です。海外ではそうなっていますが、日本はまだ甘いので何も見てないですね。サイバーセキュリティ対策において「できない」ということは許されません。そのためにユーザビリティとサイバーセキュリティ

を同時に考えていく必要があるということが海外の常識になってきています。

それから、厚労科研のアンケートの結果では、医療機関側は、200 床以上の大病院では施設管理、加算もついてきたこともあり、6～7 割の施設でセキュリティを見る人材がつけられるようになってきました。しかし、医療機器のセキュリティを見る担当の人がほとんどいないというアンケート結果が出てきています。この状況で、医療機器メーカーとしては、情報を分かりやすく伝えていく必要があります。ソフトウェアエンジニアしか分からないような情報をそのまま出すことは、非常識です。脆弱性情報はそもそも非常にわかりにくいので、「この装置にとって何の影響があります」と示すことが必要で、例えば「今 Microsoft から脆弱性の情報が出ているが、パッチを当てるのにどれくらいかかるのか」、「対応する期間がずれると装置にどういう影響が出るのか」、「その間どのような対応が必要か」という情報を出していく必要があり、このことが、国際的には当たり前の話になっています。これがアドバイザリーです。今、法規上で SBOM の作成が求められていますが、SBOM はどんなソフトウェアが入っているかという、ただのリストです。世の中で脆弱性情報が報告された時に、何か関係しているかもしれないと気付くことができますが、この製品にとってどんな関係あるかというのは SBOM だけでは分かりません。だからこそ、重要度や緊急性が高いものに関してはアドバイザリーを出すということが必要です。そうすることで医療機関側はそれに従って対処ができます。だから、SBOM とアドバイザリーは重要な組み合わせになってくるわけです。医療機関側のリスクマネジメントを支援していくというのは、製販業ができることだと思っています。今の状態ですが、実際に医療機関側へ SBOM 等を提供しているのは 3 割で、その中の 4%か 5%ぐらいしか契約書を作ってないというレベルで、改善していくことが必要です。SBOM は法規で求められるため、6～7 割で準備しているかのように見えますが、「求められれば提出できます」というところが多いです。この前も厚労科研で話をしてきましたが、今の製販業は SBOM に限らず全ての情報に対して、求められれば提出するという姿勢です。しかし、医療機関側からすると「何を持っているのか」「何が提出できるのか」が分からないので、何を求めればいいのか分かりません。実は昨年の情報処理学会の秋季大会の時に大学病院の先生が、実際に SBOM を求めたら一社も回答がなかったとおっしゃっていました。求めたときに回答がないのに、「求められれば出す」と答えたこの 7 割のアンケート結果はどういう数字だっていうことですね。さらに言うと、昔の事故はインシデントベースで対応していましたが、サイバーセキュリティの場合は攻撃が起こったら（一度攻撃が成功すれば）一挙に拡散する可能性があるので、予防して動かなければいけません。なので、そこに対してはプッシュで情報を出していき、病院側を防御しないといけません。ISO14971 の 2019 年版にも「プロアクティブに」という言葉が初めて使われており、このことをよく理解した上で、サイバーセキュリティ対策をやっていかなければならないと思っています。

もう一つのポイントは、今、医療機関側から大きなクレームになっているのが「製販業はいろんなプランを持って提供するための情報を作っているのかもしれないが、医療機関側にほとんど情報が来ない」ということです。情報が来たとしても、難解なものばかりです。いずれにしても医療機関側が使えない状況にあるという話がアンケートの結果に出ています。ここの流れをどうするのか

をもう一度点検していただきたいです。

一つは卸さんがほとんど知識がないまま動いているということです。卸は、本来販売が主体で、サービス技術やいろんな製販業者の情報を持っていることは稀だと思います。サイバーセキュリティについても、卸が現場で説明をして、なおかつ情報を提供するということは普通望めないので、必要に応じて製販業者が用意する必要があると思いますので、見直していく必要性があり、このことは手引書でも示されています。今年の骨太の方針では、今までは医療情報のことばかりが取り上げられてきましたが、サイバーセキュリティにおいては医療機器が特出しになってきています。医療機関向けのサイバーセキュリティ対策のチェックリストの中にも「医療機器」という言葉を特出しにして項目を設けようという話も出ており、今後、大きな問い合わせ事項が次々来る可能性もありますので、いよいよ対応が必要となると思っています。

もう一つは、製販業向けのサイバーセキュリティ導入に関する手引書と医療機関向けの手引書についてです。医療機関向けの手引書の第 1 版は、3 つの IMDRF ガイダンスのうち 1 つしか参考にしておらず、更に製販業向けの手引書とリンクしていない状況です。現在、第 2 版の作成が検討されているところです。調整をしている新しい文章に、「2．目的と対象」に「（4）医療情報システムに接続される医療機器の情報セキュリティについて」として、医療機関側がどのように対応すべきか、情報セキュリティ側の視点を加えることを考えています。その下には、具体的に機器のどういうところを優先的にチェックしていくか記載され、この項目がチェックリストにも載ってくると思います。また、生体情報モニター等のアラームシステムに繋がっている機器も追加しています。これらの医療機器をサイバーセキュリティの最優先事項として、有線・無線に関係なく、見ていく必要があります。

続いて侵入路の話です。医療機器に侵入してくる最初の経路というのは非常に重要です。2012 年から 2013 年にかけて最初に言われたのが、保守用のパスワードです。これが保守点検マニュアルにそのまま記載されていたということがあり、FDA が指摘して、世界中で 47 社、100 機種以上にリコールがかかりました。その後も 3 年おきぐらいに、同じことでリコールがかかっています。ROM やソフトウェアコードに記載されていたり、書き直せなかったりする固定パスワードが相変わらずあるということです。これの問題点として、アメリカではサービス関係は第三者に開放する必要があるので、保守用のサービスのパスワードやユーザーID が闇サイトで売られている実態があります。売られていたとしても、定期的にパスワードを変更できる管理ができていれば問題ないので、FDA も変更できるシステムを求めていたわけです。

もうひとつの侵入路はバックドアの問題です。あるメーカーの患者モニターにおいて、購入時点で既に、測定したデータを海外の大学の IP アドレスに送信するソフトが埋め込まれていた事例が確認されています。たまたま、B to B（企業間取引）製品のため、設置時には IP アドレスに対して受け口を立てるようマニュアルに書いてありましたが、データ制御を行っていないとそのまま大学の方にデータが送られてしまいます。実は、有名なメーカーを含めて 60 社ぐらいがこのようなソフトを使っています。外部からの侵入ではなく、内部にそういったソフトが組まれているケースもあるので、サプライチェーンのマネジメントにおいてどんなソフトを組み込んでいるのかを把握

するために、SBOM やサプラインチェーンのマネジメントが非常に重要だと感じています。

国際的な取り組みとして、医療機器の分野に限らず、「セキュア・バイ・デザイン」という考え方があります。設計の段階で対策を講じることは、IMDRF ガイダンスにも書いてあります。ただ、この「セキュア・バイ・デザイン」はさらに厳しく、単体の製品がインターネットに直接つながったとしても、セキュアな状態を保つというのが要求事項です。つまり、先ほどの閉領域なんてありえないわけで、これが国際的な話になっています。もう一つ、先ほどのサプライチェーンについてです。自分で使っている全てのソフトウェアがセキュアな状態になっているかどうかを管理するということです。この２つ取り組みに基づき 13 ヵ国の国際協力の枠組みが今動いています。

あとは 12 条３項についてですが、実際の病院に存在している医療機器で、これに適用している医療機器がどれぐらいあるかというと、通知で期限を切った令和 6 年 3 月 31 日より前に製造販売された医療機器は対策されていないので、2 割にも満たないです。今どうなっているかというと、8 割以上の医療機器は、12 条 3 項を適用していない製品で満たされている状態です。それに対して医療機関側から不満が出ているし、実際インシデントが起こってもおかしくない状態だと言われています。この８割に対して最低限何をしなければいけないかという通知が今年の4月 17 日に出ています。ライフサイクルのどの状況にあるのかを、まず顧客に通知しなさい、打てる対策は全て打ちなさいということです。もちろんサポート終了になっているのであれば、打つ対策はほとんどありませんが、対策がないなら、その状態にあることを通知することがまず求められています。そのコミュニケーションをすることが最大のポイントですが、それすらやってないので、医療機関側は機器の状態が分からないという状況です。このコミュニケーションが努力義務という問題はありますが、通知も出ていますので、改善していかなければいけません。

あとのポイントとして、海外で一番厳しいところをお伝えします。米国の政府調達、VA ホスピタル（退役軍人病院）に納める場合は、FISMA という法律に従う必要があります。何が求められるかというと、ATO という資格を取得することが求められています。これには、取得した全ての製品の稼働している全てのバージョンに対して月次で脆弱性の対応状況を報告する義務があります。そこで使用するスキャンツールも指定されており、脆弱性は当然増えるため、実施するチェック項目も 3 ヵ月ごとに更新されます。月次報告は 2013 年から運用されていますが、最近増えたことは、3 ヵ月以内に OS のアップデートが求められるようになりました。脆弱性のチェックだけではなくて、重要だと判断されたものに関しては、実際にパッチを当てる必要性が追加されています。これは何が起こるかというと、何千台、何万台という機器に対して、3 ヵ月ごとにパッチを当てるということです。私立病院でも ATO の証書のコピーが求められるケースが非常に増えており、アメリカでは ATO を使うことが標準であると考えないといけないと思っていますし、最近は FDA の申請時にもこの数字（3ヵ月つまり 90 日）が影響してきています。私が知る限り、申請時に 100 日以上前のサイバーセキュリティに関する試験成績書を提出した場合は、新しく試験した結果を出すように言われます。試験の計画から見直さなければいけない状況になってきています。他にもセキュリティルールが改正されつつあり、年に 2 回の脆弱性のチェックも出てきているので、いろんな意味で厳しくなりつつあると思っています。

それともう一つ、日本ではサイバーセキュリティを QMS では見ないと、厚労科研やいろんなところで言われていますが、FDA の場合は、第 524B 条が市販前ガイダンスに参照されており、設計段階で「セキュア・バイ・デザイン」を組み込むことと、それに必要なプロセスを確立することは必ずペアで動いています。市販前ガイドで確認され、なおかつ QSR 監査の時にもセキュリティのためのプロセスができているかを全部見られます。つまり、国際的に見ても、QMS 的にはそれを見ないと言っているのは、日本ぐらいかと私は感じているところです。

SBOM については、まだまだツールに機能不足があったり、ツール間連携に課題があったりするので、ツールの不足をエンジニアが補いながら使っていかなければいけない部分がかなりあります。また、ツールが年間で最高 3000 万円ぐらいする状況です。厚労科研ではありませんが、今年度の厚労省の予算事業として SBOM をどういうふうに作っていけばよいかのガイダンスを作ろうとしているところです。

ちなみに、サイバーセキュリティの製品ラベルについてですが、制度化の中には含めないという見解が厚労省より出ています。現在、医療機器の制度化の中に含めているのは、シンガポールだけです。以上です。

【芳田部会長】

中里様、ご講演どうもありがとうございました。大変内容の濃いお話をお伺いいたしました。この後、現在の懸念点や、苦慮している点の意見交換を実施したいと思いますが、現時点でご講演の内容を含めて、ご質問等ありましたらお聞きしたいと思いますが、委員の皆さんいかがでしょうか。

試験成績書の話で、FDA に 100 日以上前のサイバーセキュリティに関する成績書を提出した場合は、古いと指摘を受けるとのことですが、これはもう世界中でという理解でしょうか。

【中里様】

期限付きとして扱われるケースが聞こえてきますが、表立って私が把握したのは FDA だけです。まだ欧州の場合は認証機関なので、認証機関がそのように動いているという話は聞いています。

【芳田部会長】

ありがとうございます。QMS の話がでましたが、長澤委員どうでしょう。

【長澤委員】

現状、サイバーセキュリティの要件は、法制化されたところもあるので、QMS として当然取り込む必要はあるし、そこが取り込まれたかということを、例えば「変更していますか」と確認されたり、その上で「そのシステムがありますか」ということを見られたりは、あってしかりかなと思います。医療機器審査管理課では、製品にどんな対策をしているのか、その良し悪しまで QMS 調査で確認しようとする動きがあり、それについては、QMS 調査の範囲としてはやや踏み込みすぎではないかという意見もあります。そうした調査が実施されることについては、制度上の整理が必要ではないかという話が、QMS 委員会でもあります。

【芳田部会長】

菅原委員いかがですか。

【菅原委員】
　非常に難しくて、我々も形だけはできているかもしれませんが、どこまでできているか、今現状の装置や既に販売したものでできているかというと、疑問があります。
【芳田部会長】
　私も同意見です。岡本委員何かございますか。
【岡本委員】
　弊社としましては、体外診断用の医療機器も扱っていますし、このサイバーセキュリティも関係していますので、非常に興味深いです。勉強不足な部分が多い状態です。古い機械が多いので、サイバーセキュリティの対応に苦慮しています。業界団体としては臨床検査薬協会ですので、団体としてあまり関係してこないのかなというところです。
【芳田部会長】
　そうしましたら、意見交換の方に入らせていただきたいと思います。まず事務局よりご説明をお願いできますでしょうか。
【事務局】
　この後の意見交換について、サイバーセキュリティ対策において現在懸念している点や苦慮している点を伺いたいと思っています。その中で、今後の部会での取り組みについてですが、１つにアンケートの実施を考えています。府内の事業者の現状を把握するとともに、医療機器のサイバーセキュリティ対策の重要性を改めて認識いただくきっかけとなるようなアンケートの作成を考えています。
　アンケートについては、昨年度、厚労科研においても実施されましたが、部会で取り組む場合は、今回の意見交換で示された懸念点や実態等も踏まえ、必要に応じて設問数を絞るなど、回答しやすい形式とする工夫も検討してまいります。また、府内全事業者へ直接周知する予定です。アンケートは、来年 2 月から 3 月頃の実施を視野に入れており、来年度の部会にて結果をご報告の上、今後の具体的な方策の検討・決定につなげていくことを想定しております。なお、アンケート以外にも何か良い方法があれば、ご提案いただければ幸いです。以上です。
【芳田部会長】
　ありがとうございます。アンケートということで、大阪府下の全製造販売業者に対してという理解でよろしいでしょうか。中には、先ほどの岡本委員の話でもありましたが、サイバーセキュリティに関係する製品を扱っていない事業者さんもいらっしゃるかと思いますが、そこに対しても実施しますか。
【事務局】
　どの事業者がどの機器を扱っているかということを全て把握しているわけではございませんし、今後サイバーセキュリティに関連する機器等を扱うことも検討されている事業者もいらっしゃるかもしれないので、全製造販売業者に対して実施します。
【芳田部会長】
　それでは医療機器のサイバーセキュリティ対策について、意見交換を実施したいと思います。実

際の現場での悩み、気になる点等あれば、ざっくばらんにお話しいただければと思っております。事務局が提案する今後の予定についてもご意見を伺えればと思っています。製造販売業者として、どういうところに気をつけていかなければならないか、見ていく必要があるかと思うんですけど、何かご意見ございますか。

ちなみに、アンケートの内容は今後の部会の中でも検討していくという理解でよろしいですか。

【事務局】

もしアンケートをするのであれば、次回の部会で内容についてご意見いただき、年明けくらいに実施したいと思っています。皆さんがどんな状況でお困りがあるのか、進捗具合等を確認するとともに、気づきとなる質問を入れることも検討しています。アンケート結果から来年度に成果物を作るようなイメージで考えていますが、厚労科研のアンケート結果もあるので一定情報はあると判断し、アンケートはせずに成果物を考えるという、どちらの進め方もあると思っております。

【芳田部会長】

わかりました。当社は、ディスポーザブル（使い捨て）の製品がメインでして、製造販売している機械系は非常に少ないんですけども、その承認申請に携わった薬事担当に苦慮した点を聞いたところ、まず申請前に外部の公的なところで脆弱性の試験をして、申請書を添付する必要があると聞きましたが、いかがですか。

【中里様】

日本の場合は指定されていないです。

【芳田部会長】

分かりました。承認後は、通知に基づくサイバーセキュリティに関する手順書の整備に苦労したと聞いています。そういったところで、ご意見ございますか。

【長澤委員】

当社の場合ですと、ディスポが９割ぐらいのところで、機械系の扱いとなると、製造業者に設計段階から対応いただいていますが、正直なところ、それが十分なのか、どこか漏れがあるのかというレベルは、製造業者さんに大丈夫だと言われたら信じるしかない。製造販売業者がしっかり検証できる状況にはなってないかなと思います。力量のある方の採用や人材を育てていくのが当面の課題と思っています。

【芳田部会長】

製造販売している企業としての職員の意識を高めていくという必要がありますね。

【長澤委員】

その危機感というのは日々あり、そこに対しての手当てというか、早急に対応していかねばというのはあると思います。

【芳田部会長】

本日お集まりの委員の皆様の中で、いわゆる機器系、サイバーセキュリティに関連する装置を製造販売されている会社はありますか。一橋委員いかがですか。

【一橋委員】
自社は無く、多分団体の中でも売っているところはないです。
【菅原委員】
大阪医療機器協会の中では販売業、製造業と製造販売業が混在しています。当然、製造販売業の中でも、当社を含め、ソフトウェアを搭載した機器を扱っている会社はあります。ただ中小企業が大半を占めています。基本的に、ネットワークに接続して使用する装置ではなくても、ソフトウェアを何らかの形で搭載しているものもあります。使用するときにはネットワークに接続しなくても、ソフトウェアのアップデートであったり、製造段階でソフトウェアを流し込む時、ネットワークに接続したり、そうしたところをどこまで管理しないといけないのかというところです。
組織としては、サイバーセキュリティを含めたいろんな対策をしており、社員が使っているパソコンも常にチェックされています。リモートではないですが、パソコンを使ってメンテナンスを行うことも当然あります。実際に悪意のある第三者に対して対策をしないといけない、または工場で接続することがあれば、対策しなければならないということですが、そこをどこまで深く考えていったらいいのかという点が、協会員が迷っている実情です。
【中里様】
今おっしゃられたのは製品ではなく、開発・製造環境のセキュリティですか。
【菅原委員】
開発環境も当然あるとは思いますが、実際に製品が納入されて、その後のメンテナンスを、会社から貸与されているパソコンでチェックすることは当然あるかと思います。その場合に、その装置自体はネットワークの環境では使われなくても、サイバーセキュリティの対策をどこまでしないといけないのか。
【中里様】
全部やらないといけないと思います。基本要件基準第 12 条第 3 項にも書いていますが、「他の機器及びネットワーク」というのはデータのやり取りをするということですので、決して患者情報を扱うことに限定していません。「接続をして使う」「何らかの情報をやり取りする」ということです。なぜかというと、例にもありましたが、その保守用の機器・機材が感染源となって、それを装置に接続したときに、その感染源からまた別の PC に感染し、それで広がっていって、感染を起こしたのが福島県立の病院の事例です。あそこは最初、1 種類のマルウェアだったはずですが、5 年間も保有していて、発見した時には、7 種類に増えていました。いろんなところが混在して、どんどん亜種が増えていく。そういうことになった原因は不完全な保守です。
それから佐世保の病院や熊本の病院で起こった事例のほとんどは、保守が原因でした。あるメーカーが現地で保守をした際にマルウェアを埋め込んだということです。つまり、何の管理もされていないということです。正直に言って、今のところ、医療機器の場合は保守が一番危険であると思っています。保守に使用する装置ですが、「医療機器ではない」という考えがどこかであり、リモートメンテもですが、管理がなされていない。ここは本当に大きな問題だと思っています。

【菅原委員】
装置を接続する場合の PC はかなり我々も気をつけて管理はしています。
【中里様】
手段はいろいろあると思いますので、工夫をしていかなきゃいけないポイントだと思います。
【芳田部会長】
ランサムウェアは、医療機関のターゲットを絞ってやるのか、それとも手当たり次第ですか。
【中里様】
ランサムはターゲットを絞ってやっています。弱いから絞るということもあるし、価値があるから絞るというケースもあります。ただ、日本は比較的少ないですね。それは狙っても価値がないからだと思います。アメリカはいろんな著名人の情報があったり、軍隊があったりという理由から、あれだけの数で事故が起こっています。それから、シンガポールは国王の病院が狙われたので、シンガポールにおいて医療機器の申請は FDA より厳しいです。
【芳田部会長】
日本国内で実際に病院のネットワークに侵入されて、病院のネットワークを通じて、患者さんに使われている医療機器に対して、何か不具合を起こさせるというケースも事例としては出てきているというところですね。
【中里様】
岡山の病院のレポートの中に、「半田病院では医療機器が感染事故を起こしています」、「半田病院で MRI のコンソールが感染事故を起こしてコンソールを交換してます」や「CT も感染してます」と書いています。それはどういうことかというと、まず、医療情報システムの部分で感染事故を起こして、ランサムウェアが波状的に攻撃し、最初の感染から二次攻撃が始まります。何のファイアウォールもなかったと考えられる医療機器が、その二次攻撃を受けてしまって、ネットワークに直接繋がっている MRI や CT のコンソールがダメージを受けたということです。
【芳田部会長】
ほかに何か御意見等ありますか。これは事務局に伺いますが、今後の取り組みたいことであるとかの提案をここの議論で行うということでしょうか。
【事務局】
そうです。あれば教えていただければと思います。
【芳田部会長】
こういうことをやればいいんじゃないか等のアドバイスがあれば教えていただきたいです。
【中里様】
私が最初にサイバーセキュリティを始めたのは 2012 年です。先ほどお話をしました、アメリカの VA ホスピタルのようなところからある日突然電話がかかってきて、確か X 線であったと記憶していますけど、彼らのセキュリティツールがちょうど開発を終えて初めて適用された時期でした。その時に「評価の結果 30 点だったから不適切なんで持って帰って」って、それが我々のサイバーセキュリティとしての初めての指摘でした。そこから、「30 点で持って帰れというのは何だ

ろう」と思って調べてみると、当時の評価項目は 600 項目ぐらいだったんですが、そのうち 30%ぐらいしかできてなかったんです。どんどん評価項目は増えていきますので、彼らは合格点を言わないんですけど、常にその項目をチェックして、どういう状況にあるか、自分たちがどの項目に対策できているのかを、常に更新していく必要があるということです。

脆弱性が増えていきますが、対策のベースラインはあるんです。何を最低限やらなきゃいけないかっていうところは、そんなには多くないです。ただ、超音波や内視鏡、CT は、膨大なデータ処理及び画像処理なので CPU の負荷がかかっていて、そこにウイルススキャンやリアルタイムで動くものをかけてしまうと、装置上の性能をキープすることができなくなる。そのことは、FDA 等は全部わかっていて、違うタイプのウイルススキャンを使います。軍も含めてホワイトリスト型のスキャン（起動時に指定されたプログラムだけが動くようにして、それ以外はロックされるタイプ）が指定されているんです。つまり、設計上やらなきゃいけないものもある程度決まっていて、それにプラスして、常に挙がってくる脆弱性に対してパッチを当てていくということなので、本当はサイバーセキュリティって大したことないんです。

ただ、情報システムと違い、長い間記録文書を残さなきゃいけない。毎月 100 件もあるような脆弱性に関する判定や対応記録を残していくことが医療機器に求められている。その記録を残す作業を怠っている方がいるので、そろそろ PMDA に調査で確認してもらいたいと思ってます。おそらくそこに一番負荷がかかりますし、やってないとリコールかかっても追えないので、そこだけは押さえてください。そこの手順さえしっかりしていれば、あとはもうサイバーセキュリティって全然大したことないと思っています。

それから、先ほどの第三者による試験は、侵入試験の部分だけだと思います。例えば、あるパターンで 1 回だけ外部機関にお願いする。大きな機器だと出張して来てもらって、安いところであれば数百万でやってくれると思いますし、FDA 向けのレポートも全部作ってくれるところもあります。やり方やどんなレポートを書くのかさえ覚えてしまえば、自分たちで対応することも可能です。そういうパターンであれば、問題はないと思います。

ただ、事故が頻発しているので、海外では侵入試験のレポートが必要なケースがあります。実は当時の厚労省の通知では、侵入試験は必須ではないと書かれていました。ただ、ここのところ医療機器に対する事故がどうも増えつつある傾向があるのと、医療機器を狙うというダークサイドのキャンペーンが存在しています。そのため、侵入試験のレポートの添付を求める動きが出てきています。なので、近いうちにそれをつけざるを得なくなると思います。

でもそれも手順が定まってしまえば、同じルーチンを繰り返すだけです。いずれにしてもその脆弱性の評価は、レポートや侵入試験に変わるかもしれません。そこの部分が少し GVP とは違うとはいえ、手順的には大したことはないと思います。リソースを食うかどうかという話はあると思いますが、設計については、やるべきことは決まっているので、すぐにやってください。

【芳田部会長】

先ほどの侵入試験ですけども、例えば、その時はオッケーだったとしても、これが半年・1 年経てば、新たな脅威といいますか、侵入してくる方もどんどんレベルが上がってくるのではないので

しょうか。
【中里様】
新たな脆弱性が見つかるというポイントはあるかと思いますが、これは FDA も IMDRF も「最初に脅威分析をしましょう」と言っています。リスクマネジメントのベースがサイバーセキュリティにおいて違う点は、FDA も Q&A の中で述べているように、初めの段階で脅威分析を追加するところです。製品の構成のどこに弱点があるのかを分析して、例えば、侵入経路が弱い場合、最初から対策を打てればいいんですけど、現実的に打てない場所もあるかもしれません。古い装置で設計上触れていない部分があり、ある程度のリスクを負わなければいけないこともあります。そうした判明している「弱み」を全てリスクマネジメントに書き連ねておいて、どう防御するかを検討しておき、ある日突然脆弱性が発表された時に、それがこの脆弱性に関係するものであれば、即座に対応しなければなりません。もし分析していなかったら、放置してしまい、その瞬間に攻撃を受けることになります。だからこそ、まず製品が今どういう状態にあるのかを考えます。新規製品であれば対策を打てばいいですが、古い製品ではある程度リスクを受け入れながら運用する必要があります。それでも、新たなクリティカルな脆弱性が見つかった場合、例えばファイアウォールで防げるのか、どうするのかを検討しなければいけません。場合によっては、「ネットから外してください」と病院に言わなければいけないかもしれません。その覚悟を持ち、コミュニケーションを取ったときに「どのようなダメージを受けるか」、「お客様がどう反応するか」、「そのときはどのように対応するか」等を含めて対応する必要があります。それをまず分析してください、というのが、今年の 4 月 17 日の通知でした。
【芳田部会長】
ありがとうございます。岡本委員なにかございますか。
【岡本委員】
例えば USB ポートがある機械で、USB ポート自体を使用できなくしてしまうというのも一つの対策になるのでしょうか。
【中里様】
ならないです。昔の方は「ポート」という言葉を間違えていたんです。私たちが言っている「ポート」、つまりサイバーセキュリティ用のポートというのは、ソフトウェア上のポート番号です。そのポートを塞ぐ話をしているのですが、間違った人はハードウェアのポート、つまり物理的に塞げばいいと思い、キャップをつけています。そんなものは簡単に取れますし、いくらでも侵入できます。そういう話ではなく、ソフトウェア上でコントロールしてプロテクトしなさいということです。
【岡本委員】
例えばソフト的に USB を使用できないよう、デバイスとして切り離してしまうというか、無効にしてしまうというのはどうなんですか
【中里様】
それをしてくださいっていうことなんです。ただそれは普通できないです。なぜかというと、CPU

から直接ポートにアクセスしているからです。Windows になってからはプラグアンドプレイが導入されているので、USB を挿せばすぐに反応してしまいます。だから通常はその反応を抑えるために、中間に仕組みを入れて、挿しても反応しないようにします。これが先程言った、最初にやらなきゃいけない設計上のことです。会社で使用されている PC は、全てプラグアンドプレイを無効化し、USB を挿しても起動しないように設定し、セキュアな状態にしています。そして、自動のプラグアンドプレイを無効化し、使っていいものだと判断されたものだけを手動で起動するようにしています。不便なんですけど、悪用されないように無効化しているわけです。ところがそのプラグアンドプレイを無効化するということを、なぜか医療機器には適用しておらず、USB や CD を挿すと動いてしまいます。いろんなことがあるので、素のままの OS ではなく、プラグアンドプレイを無効化する、使ってないポートを使えないようにする、塞ぐといった最低限のことは設計上最初にやるべきです。ウイルスプロテクトの部分も、最低限のところをやればいいだけなんですよ。これは私が最初にミシガンでサイバーセキュリティの教育を受けたときに、アメリカでは、「PC を買ったときに最初にやること」として授業でやるそうで、小学生でも知っていますと言われたんです。そういうことすら日本の企業はやってなかったと、軍から指摘されました。

【岡本委員】

ありがとうございます。もう一点、PC との接続以外に RS232C っていうレガシーインターフェースもやっぱり対象になるんでしょうか。

【中里様】

通信方式がなんであれ通信しているので関係ありません。

【岡本委員】

ありがとうございます。

【芳田部会長】

RS232C はいまでも動いているんですか。

【中里様】

動いています。特に計測器、検体検査機器などです。

【事務局】

厚労科研の報告書で第三種医療機器製造販売業者への支援が必要と書かれていましたが、先ほど「製品のリスクマネジメント」と「体制のリスクマネジメント」は分けなくてはいけないということで、内部監査などで見ていくというのは、体制のリスクマネジメントを見ていくということを、一つの提案として書かれていたということでしょうか。

【中里様】

第三種は特殊な事情です。特にクラスⅠの検体検査装置など、本当は高いリスクがあるのに、クラスⅠだからといって何の対策もされてないケースが日本の企業では非常に多く見られます。第三種の方は、「QMS に関わっていない」「何もしなくていい」と思ってる方がいらっしゃいます。一方、アメリカでは、検体検査装置や病院で使用される検査装置の管理はすごく厳しいです。実際にそれが感染源になって、ウイルスをばらまいたケースがあります。本来、クラス分類は関係あり

ませんが、日本は特に「何もしなくていい」と思っている人たちがそこに集中している傾向があります。

【事務局】

ありがとうございます。

【菅原委員】

大阪医療機器協会の会員からの質問なんですけど、アメリカの機器で、内部ポートで実際に専用のソフトウェアが動いていて、かつ、ネットに接続せずに使う機器なので、サイバーセキュリティの対象外とする連絡が来たということですが、今の話ですとサイバーセキュリティに関係しますよね。そのポート自身を使って、工場でソフトウェアをアップデートしたりするらしいのですが、そこに対する対策はどうなってるんだっていう話を聞いたらしいです。すると対象外だからそこは関係ないというような返事が来たみたいなんですけども。

【中里様】

その話は聞いてます。その話を日本で OK とすると何もしなくなると思います。FDA がそのように言っているのは、全体的に見たときに、サイバーセキュリティに関する概念がきちんとできている国の中で、本当に外と何にも接続せず、リモートメンテなどをしないという条件下だと思います。「内部ポート」という言葉が何かよくわかりませんが、おそらく、「こじ開けないと出てこないようなポート」だと思います。それをもしリモートメンテでやるんだったらアウトだと思います。おそらくそこのところをきちんと説明できてないんじゃないかなと思います。今とにかくリモートメンテはリスクが高いと判断されています。

【芳田部会長】

質問が尽きないところではございますが、時間の方が迫ってきております。能勢委員、いかがでしょうか。

【能勢委員】

質問というより情報共有です。当社は一部輸入品の製販と国内の販売業で商売しております。輸入品の製販なんで、海外のメーカーの方に US、UL、SBOM の依頼をするんですけども、なかなかいただけないという状況があり、困っているということと、あとは国内のメーカーがどうかというと、やっぱりまだまだ「サイバーセキュリティって何」っていう状況で、そういった情報もなかなか入手できない現状でございます。

【芳田部会長】

歯科用の医療機器ということでしょうか。

【能勢委員】

歯科用医療機器です。私どもは海外から何品目かの医療機器を輸入して製販販売しています。古い機械も多いですが、今後のお客様へのアナウンスの際に、そういうものを聞いてもなかなか教えていただけないというメーカーが結構多いです。

【芳田部会長】

海外の製造所からの情報がなかなか取れてないということですか。

【能勢委員】
　国内も含めてです。
【中里様】
　今の件について、ちょうど、ある病院や厚労科研でも確認しているところですが、当然ながらいろんなメーカーにおいて医療機器が製造販売されており、私も常々感じていることです。海外のメーカーから情報が入ってこないということはありましたが、それは大手のメーカーではないのではないでしょうか。
【能勢委員】
　大手ではありません。
【中里様】
　私はサイバーセキュリティに関して、過去にいろんな海外のメーカーや国から教えていただきました。今感じているのは、アメリカのメーカーの場合は、ATO の取得を前提とした環境で育っているところが多いです。そうしたメーカーは、月次での対応がベースであり、自分たちで QMS を確立し、手順を持って、更にはリソースも抱えて、苦しい状況でも運用しているんだと思います。例えば、大きな脆弱性が上がった時に、海外のメーカーからは必ず積極的にレポートが届き、アドバイザリー情報が届きます。日本は、ほとんど何も情報がくることはないです。そういう意味で、やはり海外のベンダーは、大手なのかもしれませんが、確実にアドバイザリーを出し、SBOM も提供しています。
　こうした状況下の格差がついている中で物を買うとすれば、当然ながら情報がもらえるところから買いますよね。そこの格差というのはかなり大きいと思います。要するに何年かの積み上げの中でできている流れであり、技術的なところなので、国内のメーカーには、早く遅れを取り戻していただきたいと思っています。
【芳田部会長】
　ありがとうございます。一橋委員、なにかございますか。
【一橋委員】
　私たちの業界は、ガーゼや脱脂綿など、材料関係なので、機器に関しては全然関係ないのかなと思っています。ただ販売のシステムが乗っ取られて止まってしまうことも聞いたことがあり、製造において古い OS である機材とかもあるので、そういうところはどんどん更新していかないといけないなと感じています。
【中里様】
　先程は触れていませんでしたが、IEC81001-5-1 に、開発環境に関する要求事項があります。製品そのもののサイバーセキュリティだけでなく、開発環境のサイバーセキュリティに関する要求事項もあります。日本では「工場セキュリティ」という言葉になっていますが、開発・製造・サービスも含めて、サイバーセキュリティ確保が要求されています。製品のみではなく、会社の中のシステム自体も狙われることもあります。日本の QMS ではそこを見ないかもしれませんが、米国の QSR はどこでも見れますので、そこも確認されます。特に QSR の場合は工場システムを相当見ま

す。
【長澤委員】
QMS 委員会の中でも企業の QMS や組織に対してのサイバーセキュリティなど、医療機器をきちんと作っていくためのシステムをサイバーセキュリティに絡めて実施することについては避けて通れないという話は出ています。ただ、具体的に何をしようっていうのはまだ全然たどり着けてないところですね。
【芳田部会長】
ありがとうございます。時間が来ておりますのでまとめさせていただきます。幾つかの課題や、やるべきことはあります。ただ、サイバーセキュリティに関しての温度差と言いますか、それが本当に重要であるというところについて、クラスの低い医療機器を扱う第三種製造販売業に関しては、サイバーセキュリティへの対応について、少しおろそかになっているかもしれません。
先ほどお話がありましたように、海外からの製品における情報のやり取りなどの課題がいくつかございますので、アンケート等を交えて、各製造販売業者に対しての意識付けをしていければいいと思っております。本件について事務局で何か気になる点等あればお伺いしたいと思いますが、いかがでしょうか。
【事務局】
ありがとうございます。特にございません。
【芳田部会長】
ありがとうございます。本日の議題は以上となります。事務局にお返ししてよろしいですか。
【事務局】
芳田部会長、議事進行ありがとうございました。また委員の皆様方、中里様、貴重な意見を頂戴いたしましてありがとうございました。今回、製造販売業者の方々に意識付けをしていただきたいというところもありましたので、アンケートで注意喚起も含めたような内容を実施させていただきたいと思っております。こちらのアンケート案を次の部会に向けて作成いたしまして、第 2 回部会で皆様に意見いただきたいと思います。
本日の議事録につきまして、事務局で案を作成いたしまして、また委員の皆様に内容をご確認いただき、最終議事録は作成いたしまして送付させていただきます。また、議事録はホームページにも公表させていただきます。第 2 回部会につきましては、11 月から 12 月ごろの開催を予定しております。また、日程調整のご案内いたしますので、ご協力の方よろしくお願いいたします。
では最後になりましたが、部会長委員の皆様方、中里様、本日は大変お忙しい中、ご審議、ご講義いただきありがとうございました。今後ともよろしくお願いいたします。