protiviti®
Global Business Consulting

医療機器のためのセキュリティ連携 — 機器メーカーと医療提供機関のベストプラクティス

相互に接続された医療機器の普及が進む中で、患者の安全性、データセキュリティ、およびプライバシーに影響を及ぼす新たなサイバーセキュリティリスクが増加しています。これらの課題に対応するためには、医療機器メーカー（MDM）と医療提供機関（HDO）が効果的に協力し、医療機器のセキュリティ（設計、実装、保守を含む）を共通の優先事項として取り扱うことが重要です。HDOとMDMは、米国食品医薬品局（FDA）の指針、米国国立標準技術研究所（NIST）の業界標準、医療保険の相互運用性と説明責任に関する法律（HIPAA）のセキュリティ規則など、主要な規制要件をベストプラクティスとして活用することが推奨されます。

医療システムがデジタル化および相互接続を進める中で、医療機器の可用性、機密性、完全性を守ることは、患者の安全と医療データのセキュリティ、プライバシーを保証するために不可欠です。サイバー攻撃は救命機器の誤作動や患者情報への不正アクセス、さらには医療サービス全体の混乱を引き起こす可能性があります。したがって、これらのリスクを効果的に軽減するためには、MDMとHDOの連携したアプローチが必要です。

端的に言えば、医療機器のセキュリティはチームスポーツであり、MDMとHDOは連携して取り組むべきです。

最近、MDMが医療機器の設計段階でセキュリティ機能を組み込むことが正式に求められるようになりました。これには可能な限り初期設定またはオプションに対してセキュリティ設定（例えば、ドライブの暗号化やユーザー名とパスワード、PINコードなどの安全な認証メカニズム）を備えることが含まれます。同時に、HDOは、組織内で使用する医療機器にセキュリティを実装し、維持する責任を担ってきました（例えば、組み込まれたセキュリティ設定を理解し、適切かつ安全なネットワークセグメントに配置することなど）。しかし、機器やその使用環境が技術的に複雑化するにつれて、安全な状態を実現することはますます難しくなっています。このような状況の中、一部のMDMは、市場における同業他社に対する競争上の優位性として、追加的な医療機器セキュリティに関するガイダンスや協働支援を提供することで成果を上げています。

MDMとHDOは、患者の安全とデータのセキュリティおよびプライバシーを確保するために、以下の戦略を用いて連携することができます。

1. **役割と責任マトリックスの文書化および共有**— MDMとHDOは、製造から廃棄までの各段階において、両者がデバイスセキュリティの設計、導入、維持において重要な役割を果たすことを認識する必要があります。両社が果たす具体的な役割と責任を、サービスレベル合意（SLA）とともに文書化し、将来的に分析するためのバロメーターとして活用します。この文書には少なくとも以下の内容を記載することが推奨されています。

   - 医療機器セキュリティに関する製造者開示文書（MDS2）およびソフトウェア部品表（SBOM）の作成、更新、提出
   - 定期的なリスク評価の実施
   - 潜在的な脆弱性の特定
   - パッチ管理（デバイスソフトウェア、ファームウェア、サーバーなど）
   - デバイスの定期的なメンテナンス

2. **MDS2 フォーム、SBOM およびユーザーマニュアルの活用**— MDMとHDOが重要なデバイスセキュリティ情報を共有する最も簡単な方法の一つは、MDS2フォーム、SBOMおよびデバイスユーザーマニュアルを使用することです。これらの文書は、セキュリティ連携の標準として業界で広く普及しています。

a. **MDS2**：MDS2 フォームテンプレートの最新版には 200 以上のサイバーセキュリティに関する質問と説明が含まれています。

b. **SBOM**：医療機器およびそのプラットフォームを構成するすべてのソフトウェア関連部品、パーツ、コンポーネントの一覧を提供し、HDO が、製品の一部として MDM から明確に開示されていない可能性のあるリスクや脆弱性を特定し、追跡するのに役立ちます。

c. **ユーザーマニュアル**：デバイスの設定方法やデフォルト設定の変更、ユーザー認証の統合などに関する重要な考慮事項が含まれています。これらのマニュアルには、最適な運用の一環として重要なセキュリティ設定を確認するための予防メンテナンスサイクルも記載されています。

3. **デバイスのホワイトペーパーおよび導入ガイダンスの作成と配布**—多くの MDM は、顧客や患者がデバイスのサイバーセキュリティについてより深く理解できるよう、専門用語を避けて解説したデバイスセキュリティに関するホワイトペーパーを作成し、配布しています。これらのホワイトペーパーは、方向性を示し、幅広い機能を紹介し、セキュリティへの取り組みを伝える役割を果たします。さらに一歩進めて、MDM と HDO が連携してカスタムデバイスの導入ガイダンスを作成することも可能です。このようなガイダンスは、病院システムにデバイスを販売する際に真の競争優位性をもたらします。また、データフローやネットワーク図を作成、維持し、プラットフォーム、アプリケーション、データベース、インフラストラクチャなどの間で、電子的に保護された医療情報（ePHI）が病院やベンダーのネットワーク上でどのように共有されるかを詳細に示すことでさらなる競争優位性を得ることができます。

4. **情報共有コンソーシアムやワーキンググループへの参加**— MDM および HDO は、組織間の透明性を高め、自身の知識向上を図るために、情報共有コンソーシアムやワーキンググループに参加し、積極的に活動することが推奨されます。例えば、医療機器情報共有分析機構(MedISAO)、医療情報共有および分析センター(H-ISAC)、医療情報管理システム協会（HIMSS)、医療機器イノベーションコンソーシアム（MDIC)、アメリカ合衆国保健福祉省（HHS）405(d) プログラム、医療セクター調整協議会(HSCC)サイバーセキュリティワーキンググループ、医療・医療機器サイバーセキュリティのためのアルキメデス・センターなどがあります。これらの組織はそれぞれ異なる視点や目的を持っていますが、MDM と HDO の双方にとって、医療機器のセキュリティに関する知識を集め、共有し、共同で取り組むための素晴らしいプラットフォームを提供しています。

5. **サイバーセキュリティリスクの共同評価の実施**—組織は連携して、NIST のサイバーセキュリティフレームワークのようなツールを活用した定期的な共同リスク評価を実施することで、統合環境に特有の脆弱性を特定できます。このアプローチは、評価対象のデバイスやプラットフォームが技術的に複雑である場合や、医療システム内のベンダーのネットワーク内に設置されている場合に特に有効です。チームは、前述の役割と責任のマトリックスを MDS2 フォームと併せて確認することで、潜在的なセキュリティ構成と実装されたセキュリティ構成の違いを特定することができます。またこのようなプロジェクトにおいて、医療機器セキュリティライフサイクルアセスメントを活用することも可能です。

最新のトップリスク調査結果によると、「サイバー攻撃の脅威」がヘルスケア業界の役員や経営幹部にとって、短期的（2～3年先）および長期的（2035年までの10年間）な最大のリスクとされています。

6. **MDM パートナーとのインシデント対応（IR）および回復力強化計画の調整**— HDO はしばしば単独でインシデント対応計画（IRP）を作成し、他の組織を計画や対応、回復力強化の取り組みに含めないことがあります。しかし、これは誤ったアプローチです。HDO は MDM との関係を活用し、以下のインシデント対応関連活動への支援と協力を依頼するべきです。

- デバイスバックアップ構成の簡易な識別と安全な保管方法の確立
- 大規模な事故発生時に備えた代替機器に関する契約や合意の準備
- インシデント発生時のオンデマンド技術サポートの提供
- IR 計画と調整をテストするための卓上演習への参加

7. **トレーニング、教育、意識向上の活用**—これまで、MDM が医療機器の設計を担当し、HDO の生物医学チームがその機器を導入・使用・保守してきました。そして最近では、HDO のサイバーセキュリティチームがこれらの機器をサイバーリスクや脅威から守る役割を担っています。しかし、これらのチーム間では知識、スキル、経験の共有がほとんど行われていませんでした。今後はこれらのチームが協力し、ベストプラクティスを共有しながら、

患者の健康と安全、そしてデータ保護を最優先に考えた医療機器の保護方法を決定する必要があります。

医療機器のサイバーセキュリティを強化するには、MDMとHDOの両方が協調して取り組む必要があります。FDAのような規制機関が推奨するベストプラクティスを採用し、国際標準化機構(ISO)やNISTのガイドラインのような国際標準に準拠することで、組織はサイバー攻撃の脅威に対する強固な防御体制を構築することができます。重要なのはコラボレーション(連携)です。責任、知識、戦略を共有することは、より安全な製品だけでなく、患者の健康を最優先とする、より安全な医療提供システムを実現する鍵となります。

医療機器ライフサイクルレビュー

以下に示す医療機器ライフサイクルレビュープログラムは、医療機器のセキュリティに関する効果的な対策を総合的に評価するために開発されました。このプログラムは、米国国立標準技術研究所(NIST)のサイバーセキュリティフレームワーク(CSF)、FDAの事前・事後ガイダンス、そしてHIPAAセキュリティ指針を基盤として構築されています。これにより、医療機器のセキュリティを確保するための主要な管理策が包括的に取り入れられています。

機能	コントロールカテゴリー
戦略とガバナンス	医療機器セキュリティプログラムと戦略
	リスクおよびコントロールフレームワーク／リスク管理プロセス
	方針および手続き
	組織的リーダーシップおよびチーム統合
	調達計画および要件
識別と追跡	資産目録、分類、優先順位付け
	リスク評価および HIPAA リスク分析
	データフローの文書化
プロテクト（保護）	アクセスコントロール、データセキュリティ、ネットワークセグメンテーション
	医療機器セキュリティ（MDS2）に関する製造開示書
	脆弱性およびパッチ管理
	意識向上およびトレーニング
	デバイスの取り扱い手順
検出	セキュリティインシデントの特定、記録、監視
	損失検出および報告
	継続的な在庫監視およびベンダーアラート
対応	インシデント対応計画
	定期的なインシデント対応計画のテスト
	インシデントの追跡および処理
	フォレンジック機能およびプロセス
復旧	障害復旧および事業継続
	改善点／事後分析
	ライフサイクル終了／文書化

NIST、FDA、およびHIPAAに基づく評価

この医療機器ライフサイクルレビュープログラムは、NISTサイバーセキュリティフレームワーク(NIST CSF)を最大限に活用しています。このNIST CSFは、「攻撃に焦点を当てた」構造によって非常に高い評価を受けています。また、FDAの医療機器セキュリティに関する事前／事後ガイダンスもNIST CSFを活用しており、これらの管理フレームワークはHIPAAセキュリティ規則の標準および実装仕様と統合されています。

その他のリソース

1. Cybersecurity | U.S. Food and Drug Administration (FDA)
2. NIST Cybersecurity Framework
3. ISO 14971:2019; Medical devices — Application of risk management to medical devices
4. NEMA - Manufacturer Disclosure Statement for Medical Device Security (MDS2)
5. MedISAO (Medical Information Sharing and Analysis Organization)
6. H-ISAC (Health Information Sharing and Analysis Center)
7. HIMSS (Healthcare Information and Management Systems Society)
8. MDIC (Medical Device Innovation Consortium)
9. HHS 405(d) Program: A collaborative effort between the Health Sector Coordinating Council and the federal government
10. Health Sector Coordinating Council Cybersecurity Working Group
11. Archimedes Center for Medical Device Security
12. Principles and Practices for Medical Device Cybersecurity - IMDRF
13. There's a Culture Shift Happening in Medical Device Manufacturing. Are CISOs Ready?
14. Global Medical Device Company Assembles the Right Team and Microsoft Azure and IoT Solutions to Revolutionize Patient Care
15. Top Security Pitfalls for Medical Devices at Healthcare Providers
16. NIST Securing Internet Connected Medical Devices