BLACK DUCK®

ホワイトペーパー

FDA への申請のための ネットワーク接続型医療機器の セキュリティ保護

医療機器のセキュリティと規制の現状

Internet of Things（IoT）は、消費者に対しても企業に対しても、とてつもない自由、利益、機会をもたらしながら、業界全体を変えつつあります。ただし、ソフトウェアに対する新たなアプリケーション・セキュリティ（AppSec）と、（医療機器をできるだけ早く市販する必要があることによって悪化する）安全上のリスクとをもたらします。医療機器の数と利用が増えた結果、IoT の利点と課題は医療業界において特に顕在化しています。

このホワイトペーパーは、特に米国食品医薬品局（FDA）に関連するセキュリティと規制の現状について調査したもので、FDA の規制の順守を達成および維持しようとする医療機器メーカーと医療提供組織に対するベスト・プラクティスを示しています。

医療機器の相互接続性の向上

ネットワークに接続された医療機器により、患者の治療が改善されています。医療用画像装置、ペースメーカー、輸液ポンプなどは、医療提供者によるバイタル・サインの監視、投薬量の調整、診断の改善、治療の提供を支援し、最終的にはコストを下げながら患者の病状を改善します。

医療機器におけるソフトウェアの使用と高度化は、Vitatron（現在は Medtronic）が最初のデジタル・ペースメーカーを導入した 2000 年代初頭以降、指数関数的に増しています。[1] 当初、ソフトウェアはカスタム・コードでだけで構成されていましたが、まもなくコンポーネント化され、商用ベンダーとオープンソース・コミュニティの両方のコードを利用するようになりました。現在は、需要に対応できるように短期間での開発を可能にしているフレームワーク、ライブラリ、「コピー＆ペースト」されたコードは、依存関係が複雑に絡み合った状態でリンクされているため、開発チームはソフトウェアにおけるすべての依存関係を十分に認識できていません。

ビッグ・データ、人口知能、機械学習などのテクノロジーがますます普及していくのに伴い、ソフトウェアは次世代の延命治療にさらにいっそう欠かせないものになります。これは、COVID-19 のパンデミック中にすでに見られたように、遠隔治療が、利用しやすく便利な、実行可能な治療手段になったからです。遠隔治療の利用は、COVID-19 より前の基準の 38 倍に増えました。[2]

COVID-19 のパンデミックにより、自宅で使用される医療機器の数も増えました。FDA は、患者の監視と治療の可能性を高めるほか、医療提供者の SARS-CoV-2 への暴露を減らすために、特定の患者用ウェアラブル・デバイスの緊急時使用許可を交付しました。[3]

医療機器のセキュリティ・リスク、安全性リスク、規制リスク

非常に多くの個人情報にアクセスするため、医療機器はハッカーやその他の悪意のある行為者にとって一般的で利益を得やすい標的になりました。同時に、複雑性と相互接続性が増したことにより、医療機器は攻撃の影響を受けやすくなりました。不正行為、サプライ・チェーンの途絶、株価操作、ランサムウェア、個人情報の盗難、機密情報、研究開発データはすべて、医療機器上でサイバー攻撃に関連づけられるようになっています。死に至る場合も含め、深刻な健康上の影響を伴う患者の治療中断の恐れがあります。

メーカーや医療提供組織は、医師、患者、政府、社会全体から十分な信頼を得たいのであれば、ネットワーク接続型医療機器のセキュリティ・リスク、安全性リスク、規制リスクに対応する必要があります。

セキュリティ・リスク

前述のとおり、COVID-19 のパンデミックは、CT スキャナ、モニタリングシステム、患者の遠隔計測システム、人工呼吸器などの医療機器の使用の急激な増加をもたらしました。医療機器の使用頻度が増えたため、それらに対する攻撃も増えました。ある報告書によると、パンデミックの最初の年の医療機器に対するハッキング・インシデントは 42%増加しました。[4]

医療機器の脆弱性は、COVID-19 の前にも存在していましたが、2019 年の 1 台の医療機器当たりの脆弱性は平均 6.2 件でした。[5]

ブラック・ダックに依頼された Ponemon Institute によるレポート[6] の内容

- 医療機器メーカーの 60%と医療提供組織の 49%が、病院などでモバイル機器を使用すると、セキュリティ・リスクが大幅に増すと報告
- 医療機器メーカーの 53%が、品質保証と検査手順が不足していると報告
- 医療機器メーカーの 43%が、医療機器を 1 年に 1 回以上検査していないか、1 年に 1 回以上検査しているかどうか定かではない
- 医療機器メーカーの 37%が、自社の医療機器で脆弱性が検出される可能性があると思っている
- 医療機器メーカーの 33%が、IoT 医療機器間の通信を暗号化している。そのうち、暗号化された通信でキー管理システムを使用しているのは 39%のみ

研究・助言会社の Forrester によると[7]、医療機器は次の 4 つの攻撃シナリオに対して脆弱

- サービス妨害（DoS）
- 治療の改竄
- 患者データの盗難
- 資産の損害

ランサムウェア攻撃とセキュリティ侵害

ランサムウェア攻撃は、標的に何かを強要しようとします。それは患者の治療を中断させる可能性があり、クリニックや病院がデータや重要なシステムにアクセスできなければ患者の生命は危険にさらされることになります。その結果、治療の質やレベルが低下するため、医療提供組織には財政的な損害が発生します。

医療における最近のランサムウェア攻撃

- 2021 年 5 月、Scripps Health のネットワークと暗号化された医療機器に対する攻撃により、データの侵害、電子カルテへのアクセスの遮断、外傷患者や脳卒中患者の他の病院への搬送先の変更、集団訴訟などが発生[8]
- 2021 年 5 月、Irish Healthcare Service を不能にする攻撃により、カルテへのアクセスの遮断、COVID-19 関連の検査の遅延、予約のキャンセル、医療画像装置からのスキャンの送受信と比較に対するセキュリティ侵害が発生。攻撃者はビットコインで 2000 万ドルを要求。[9] 同じランサムウェアが米国の少なくとも 16 の医療ネットワークと緊急ネットワークを標的に[10]
- 2021 年 4 月、米国の 42 の医療現場への攻撃により、がんに対する放射線療法の重要な機能に必要なクラウド・サービスが中断[11]

リコール

Ponemon Institute によると、医療機器メーカーの 24%と医療提供組織の 19%が、2017 年 5 月以降、セキュリティ上の脆弱性のために医療機器をリコールしています。[12] それ以来、米国食品医薬品局（FDA）は、何億台もの医療機器に影響を与えるさらに多くのリコールを報告しています。[13]

安全性リスク

患者の生命は、ペースメーカー、インスリン・ポンプ、透析装置のほか、臓器の強化や生命維持に必要な身体機能の管理のためのその他の医療機器に依存していることが多くあります。そのような医療機器の障害は、病気、外傷、身体障害、死亡など、患者に対して深刻な結果をもたらす場合があり、医療機器の性能や機能不全、病院運営の支障、または医療提供の不能に起因することがあります。

サイバー脅威によってもたらされる安全性リスク

- 診断機器上のデータを変更するマルウェア
- 機能を変更する、医療機器に対する再プログラミング
- 医療機器を使用できなくするサービス妨害攻撃
- 他の医療機器を脆弱にする、ネットワークへの不正アクセス
- 管理されていないパスワード

毎年、FDA は、医療機器に関連する死亡、外傷、機能不全が疑われる数十万の医療機器報告書（MDR）を受け取っています。これらの報告書は、公開データベースの Manufacturer and User Facility Device Experience（MAUDE）において公開されています。さらに、2019 年 6 月、FDA は、1999 年から 2019 年までに発生した医療機器の機能不全に関してメーカーから提出された約 600 万のレポート（MAUDE に含まれていなかったもの）を公開しました。[14]

規制リスク

医療機器メーカーは、医療機器とアプリケーションでの患者の期待に応え、規制順守を徹底する必要があります。規制施行措置の法的影響、特に製品リコールについて理解し、国および国際法、規則、法令、訴訟に関連するリスクと開示について総合的に判断する必要があります。

医療機器のサイバー・セキュリティに対する規制

政府による監督が増加することは、医療機器を含む医療分野での AppSec ソリューションの急速な採用をもたらしています。医療機器のセキュリティ・リスクと安全性リスクに対応する法と規制には、次のものがあります。

- **連邦食品・医薬品・化粧品（FD&C）法（1938 年）：**米国医療機器（21 CFR 807）の第 501(f) 項、第 515 項、第 510(k) 項、1976 年の医療機器修正条項
- **1990 年の医療機器安全法（SMDA）**
- 1996 年の医療保険の相互運用性と説明責任に関する法律
- 2009 年の経済的および臨床的健全性のための医療情報技術（HITECH）に関する法律
- 欧州医療機器規則（MDR）2017/745

さまざまな公共部門組織と民間部門組織（FDA、米国標準技術研究所（NIST）、米国医療機器振興協会（AAMI）、国際電気標準会議（IEC）、米国国家規格協会（ANSI）など）により、医療機器メーカーが適用される法と規制を順守する際に役立つガイダンスと基準が策定されました。

医療機器のセキュリティの一般基準に含まれるもの

- AAMI TIR57：医療機器のセキュリティの原則（リスク管理）
- AAMI TIR97：医療機器のセキュリティの原則（医療機器メーカーの市販後リスク管理）
- AAMI ドラフト標準 SW96：医療機器（医療機器へのセキュリティ・リスク管理の適用）
- IEC 62304：医療機器ソフトウェア（ソフトウェア・ライフサイクルのプロセス）
- IEC/ANSI/ISA 62443-4-1：産業用オートメーションと制御システムのセキュリティ（セキュアな製品開発ライフサイクルの要件）

非常に多くの複雑な規制、基準、推奨事項により、組織がコンプライアンスを維持するのが難しくなっています。例えば、米国で市販されている医療機器の場合、メーカーは、コンプライアンスが必要な特定の基準を満たすことに加えて、FDA の市販前届出 510(k) や市販前承認手続きを行う必要があります。

医療機器メーカーでは、AppSec ソリューションが必要です。AppSec ソリューションにより、自社のソフトウェアのセキュリティ・リスクを特定し、それらのリスクと医療機器の使いやすさおよび入手のしやすさのバランスを取り、規制当局の承認を得ることができ、また承認を維持できます。

FDA のサイバー・セキュリティ・リスク管理における考慮事項

米国政府は、FDA に医療機器が安全かつ効果的であるようにすることを求めていますが、FDA による監督を患者の安全性までに制限し、患者のプライバシーは対象にしていません。2005 年以降、FDA の Center for Devices and Radiological Health（CDRH）は、安全安心な医療機器の設計および開発について、率先してメーカーに助言を行いました。

医療機器の分類レベル

FDA では、使用目的、使用の症状、患者またはユーザーにもたらすリスクに基づいて、医療機器を分類しています。医療機器の使用目的は、単純な体温計から、医療検査、移植、人口器官で役立つ、インターネットに接続された医療機器まで多岐にわたります。ソフトウェアは、ロボット、埋め込み型医療機器、ウェアラブル・デバイス、MRI や CT スキャンなどの装置、診断および監視装置、医療機器専用に設計されたネットワーク装置、モバイル医療アプリケーションなど、さまざまな状況で使用されます。

FDA における医療機器の 3 つのクラス

- **クラス I の医療機器**は、患者の安全性に対するリスクが低く、Bluetooth 対応の歯ブラシ、病院用ベッド、監視機能付き外科用手術器械などです。医療機器のほぼ半分（47%）がこのカテゴリに分類され、そのうち 95%は規制プロセスから除外されます。[15]
- **クラス II の医療機器**は、患者の安全性に対するリスクは中程度で、輸液ポンプ、Apple Watch などのウェアラブル・デバイス、MRI や CT スキャンといった装置などです。医療機器の 43%がこのカテゴリに分類されます。[16]
- **クラス III の医療機器**は、患者の安全性に対するリスクは高くなり、規制当局による厳格な管理に従う必要があります。クラス III の医療機器は、ペースメーカー、小脳刺激装置、侵襲性グルコース・センサーを搭載したインスリン・ポンプやその他の医療ポンプなどです。このカテゴリに分類される医療機器はわずか 10%です。[17]

2018 年、FDA は、医療機器のサイバー・セキュリティ・リスク専用の 2 層分類システムを導入した市販前ガイダンスの草案を作成しました。

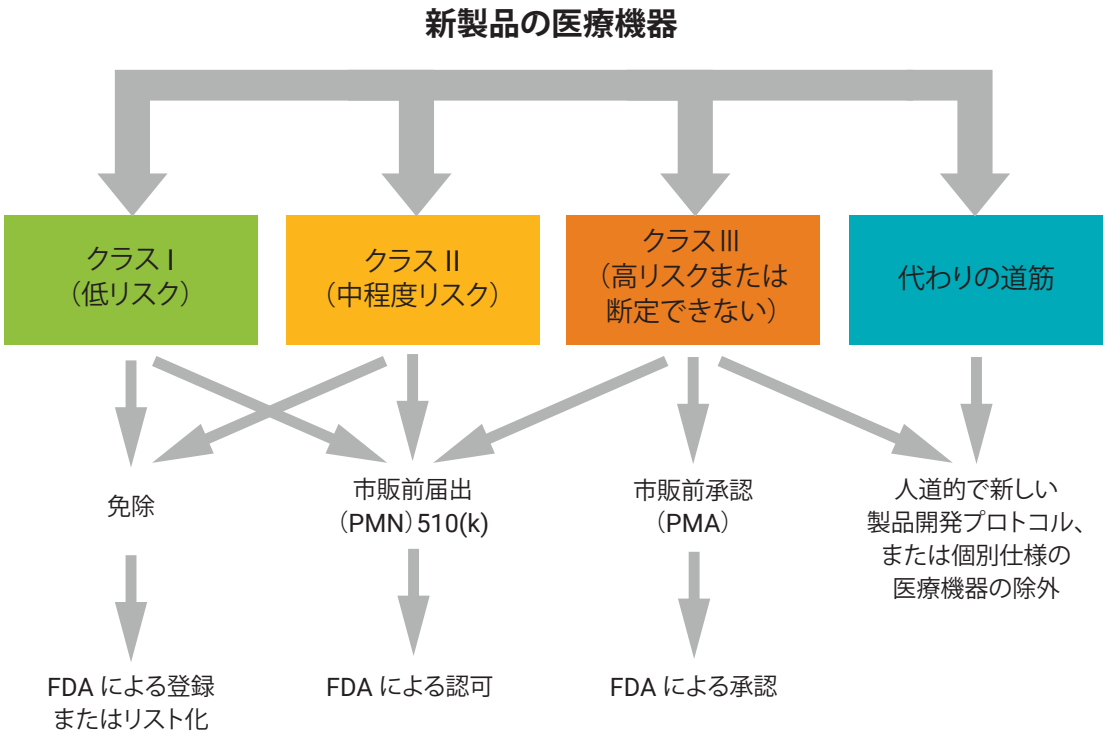
- **Tier 1 の医療機器**は高いサイバー・セキュリティ・リスクをもたらします。
- **Tier 2 の医療機器**は標準的なサイバー・セキュリティ・リスクをもたらします。

FDA は、これらの階層が既存の法的な医療機器分類に必ずしも一致していないことは承知しており、メーカーが FDA のコンプライアンスを達成するために抱える課題はさらに複雑になります。

認可と承認

米国で医療機器を市販する前に、申請者は、その医療機器が合法的に市販される医療機器と実質的に同等であると FDA が認めたことが記載されている依頼書の形で FDA から認可を得る必要があります。

医療機器のクラスによって、医療機器を販売するのに必要な FDA による認可の市販前申請の種類が決まります（下図を参照）。クラスに拘わらず、免除されていない医療機器には認可が必要です。クラス III の医療機器および完全な新製品である医療機器には、より厳格な市販前承認（PMA）が必要です。



米国で市販される新製品の医療機器に対する FDA の要件

市販前届出 510(k)

FD&C 法の第 510(k) 条（市販前届出 510(k) または PMN 501(k) と呼ばれることも多い）は、米国で市販前に医療機器が完了する必要のある認可手続きに相当します。その医療機器が合法的に市販されている既存の医療機器と同程度に安全かつ効果的であることを示すために、FDA への申請が必要です。

メーカーは、医療機器を初めて商品流通に投入する場合や大幅に改良した医療機器を再投入する場合、PMN 501(k) を申請する必要があります。

市販前承認

クラス III の医療機器では、FDA による承認を得るために、クラス III の PMN 510(k) に加えて PMA 申請が必要です。クラス III の医療機器が PMA の要件を満たしていない場合、その医療機器は、FDA によって不良医療機器と見なされ、米国で市販することができません。

FDA によるガイダンス

FDA は、規制の監督に加えて、医療機器のサイバー・セキュリティとリスク管理の市販前および市販後のガイダンスを発行しています。このガイダンスは、FDA CDRH による公開文書の形式で発行されます。

FDA によるガイダンスは、拘束力がなく要件でもありませんが、推奨事項の背後には論理的根拠と詳細があり、NIST のサイバー・セキュリティ・フレームワークと合致しています。このガイダンスは法的強制力のあるものではありませんが、一部の組織は、推奨事項を採用し、自発的に要件にしています。それらの組織は、FDA によるガイダンスの文書を参照することにより、どの程度要件を順守しているかを証明する PMN 501(k) または PMA を申請する準備が整っています。

市販前ガイダンス

FDA による市販前ガイダンスは、主に PMN 501(k) や PMA の申請手続きで組織を支援することに重点を置いています。一般に、医療機器メーカーは次のことを行う必要があります。

- サイバー・セキュリティを確保し、医療機器の機能と安全性を維持するための一連の対策の開発
- 医療機器の設計および開発時のサイバー・セキュリティへの対応

潜在的な新しい市販前要件は、FDA、保健福祉省、議会によって大綱が定められます。彼らは組織に対して、医療機器のセキュリティ、ソフトウェアの更新、ソフトウェア部品表（SBOM）に対して措置を講じることを求めています。また、FDA がメーカーに次のことを求めた場合には、医療機器の安全性を高めるように提案します。

- 適宜、医療機器を更新してパッチを適用すること
- FDA への市販前申請に、設計またはアーキテクチャの観点から医療機器の更新とパッチ適用が可能であることを示す証拠を含めること
- サイバー・セキュリティ部品表（CBOM）または SBOM に対して段階的なアプローチを使用すること
- 自社の医療機器の既知のサイバー・セキュリティ上の脆弱性を開示し、顧客にリスクを軽減するための指示を与えること
- サイバー・セキュリティ上の脆弱性への事前対応を改善すること

2018 年、FDA は、前述の提案に対応するように市販前ガイダンスの文書を改訂し、セキュリティが、安全性とともに、医療機器の開発プロセスで設計上の要求となることを推奨しています。さらに、FDA は、2018 年の更新に基づいて、510(k) PMN または PMA を申請することをメーカーに求めています。

FDA は、メーカーを支援するために、更新されたガイダンスで次のことを意図しています。

- 適切なセキュリティ保護によって医療機器の設計および開発にリスクベースのアプローチを採用すること
- 医療機器のライフサイクル全体のリスクと軽減を評価することで、医療機器のサイバー・セキュリティに対して総合的なアプローチを取ること
- 医療機器の重要な安全性と基本性能の維持および継続性を確保すること
- 安全性と効果の継続性を確保するために、信頼性の高い医療機器の開発を推進すること

セキュリティの設計および開発への統合

FDA による市販前ガイダンスでは、プロセスの全ステップでセキュリティに対応するライフサイクルを使用した、信頼性の高い医療機器の設計について記載されています。医療機器の開発においては、次のような設計上の要件を作成することが推奨されています。

- 資産、脅威、脆弱性の特定
- 医療機器の機能とエンド・ユーザーや患者に対する脅威および脆弱性の影響の評価
- 攻撃者が脅威または脆弱性を悪用する可能性の評価
- リスク・レベルおよび適切な軽減戦略の特定
- 残留リスクと許容基準の評価

セキュリティ対策

市販前ガイダンスでは、信頼できるユーザーへのアクセスの制限、信頼できるコンテンツの保証、セキュリティ侵害の検出と対応、セキュリティ侵害からの復旧などのための、セキュリティ対策の例が挙げられています。メーカーは、リスク評価を通してすべてのセキュリティ対策を特定および評価する必要があります。

医療機器の使用目的

FDA は、セキュリティ対策が適切に採用されるように、メーカーがサイバー・セキュリティの保護と目的の環境内の医療機器の使いやすさのバランスを取ることを推奨しています。メーカーは、市販前申請の一環として、使用されているセキュリティ機能（および使用されていないセキュリティ機能）を正当化するために、これらの考慮事項の背後にある論理的根拠を文書化する必要があります。

ラベリング（ラベル表示）の推奨

FDA による市販前ガイダンスには、資産、脅威、責任を特定するために CBOM を提供するという概念が含まれています。 CBOM を用いることで、メーカーは、既存の医療機器に含まれるサードパーティ・ソフトウェアの既知の脆弱性と将来の脆弱性の両方のリスクにさらされていることを理解することができます。ラベリングは、ユーザー、IT 担当者、医療機器の既存のインフラストラクチャへの統合を担当するその他のサポートスタッフを対象としています。

End of Life（EOL、製品寿命終了）の指示は、メーカーが医療機器をサポートしなくなるとリスクが増大することを顧客が理解できるようにするために重要です。

文書

FDA は、メーカーが市販前申請の一環として、討議して文書化する必要があるサイバー・セキュリティの課題のリストを提供しており、設計図、系統図、システムの脅威モデル、リスク管理文書が含まれています。

市販後ガイダンス

医療機器が配置された後のサイバー・セキュリティに目を向けると、FDA による市販後ガイダンスは市販前ガイダンスよりも重要です。市販後、FDA は「メーカーは、医療機器の市販後管理の一環として、サイバー・セキュリティ上の脆弱性とエクスプロイトを監視、特定、対応する必要があることを強調」しています。[18]

製品ライフサイクル全体でのセキュリティの統合

FDA による市販後ガイダンス文書に記述されている主な原則の 1 つは、製品ライフサイクル全体での設計によるセキュリティの実現です。「効果的なサイバー・セキュリティ・リスク管理プログラムは、市販前と市販後の両方のライフ・サイクル・フェーズを組み込み、医療機器の構想から老朽化までの段階でのサイバー・セキュリティに対処する必要があります。」[19]

このガイダンスは、最初からセキュリティを設計および構築し、製品が引退するまで対処し続ける、業界のベスト・プラクティスが反映されています。市販後ガイダンスでは、ライフサイクル全体を通して、メーカーの独自コード、サードパーティのコード、ハードウェアなどにおける脆弱性に対して医療機器を検査することの重要性も強調されています。

FDA による市販後ガイダンスには、脆弱性の影響を評価して患者に対するリスクを見極める（FDA の主要業務）方法が記載されていますが、メーカーの事業、収益、評判などの考慮事項に対するリスクについては触れられていません。

脅威モデリング

FDA は、考えうる脅威の影響を評価する助けとなるように、最新の脅威モデルの重要性を訴えています。また、現在のリスクではなく将来可能性のあるリスクを示している場合でも、メーカーに脆弱性を評価するように提案しています。リスク評価プロセスに一貫性を持たせるために、共通脆弱性評価システムなどのツールの使用も推奨されています。

情報共有

FDA は、サイバー・セキュリティの脆弱性とリスクに対するさまざまな情報源をチェックして、医療機器に対してそれらの脆弱性とリスクを評価するように助言しています。メーカーが自社の開示を評価できるように、メンバーが脆弱性データを共有する情報共有組織への参加も提案されています。そのような組織の 1 つとして、Health Information Sharing and Analysis Center（Health-ISAC または H-ISAC）が具体的に挙げられています。

FDA は、調整された脆弱性開示ポリシーと、組織全体にわたって顧客とともにアクティビティを管理する対策も提案しています。

脆弱性の報告

FDA は、ガイダンスを提供し、報告された脆弱性にいかに素早く対応するかについての改善タイムラインにしきい値を設定しています。推奨される措置として、顧客への伝達、回避策と軽減情報の提供、修正プログラムの開発とデプロイなどがあります。このガイダンスは、メーカーが、業界基準およびベスト・プラクティスに従って脆弱性に素早く対応できなかったことに対処するためのものです。

管理されていないリスク

FDA による市販後ガイダンスでは、医療機器で管理されていないリスクが示されている状況についても記載されています。「修復が為されなければ、患者への被害が管理されていないリスクのある医療機器は、使用または開示の妥当な可能性があると見なされる場合があり、その製品によって健康への深刻な悪影響や死亡がもたらされます。その製品は、FD&C 法に違反していると見なされ、法執行やその他の措置の対象となります。」[20]

FDA のサイバー・セキュリティ・コンプライアンスの課題

FDA によるガイダンスを対策に落とし込むことは、医療機器メーカーにとって進行中の課題です。ガイダンスは全体的な目標の概要を示していますが、技術的なものではなく、実現方法に大きく依存しているものの、目標の実現方法に対する指示はほとんどありません。検査、手続き、ポリシー、手順のチェックリストがあるのが理想的ですが、実際には、テクノロジーと不確定要素が非常に複雑に組み合わさるため、そのようなチェックリストを作成することはできません。

組織的な課題

PMN または PMA の準備をするときに医療機器メーカーが直面する最大の障害として、社内的な障害があります。プロセスを経ていない組織の場合は特にそれが顕著です。

組織的および文化的な障壁として、次のものがあります。

- DevOps プロセスでのセキュリティの欠如
- 対応が遅く受動的なセキュリティ対策
- セキュリティに対する注意不足
- セキュリティに対する説明責任の欠如
- スキルと知識の隔たり
- 予算不足
- 時間的制約
- 非効率的なセキュリティ・テスト対策

これらの領域の問題に対応することは、PMN 501(k) や PMA の手続きでメーカーの助けとなるだけでなく、セキュリティに対するメーカーの心構えを強化します。

規制上の課題

Ponemon Institute によると、ソフトウェアのセキュリティ・リスクを軽減するために FDA によるガイダンスに従っている医療機器メーカーは、わずか 51%です。[21] この数は、絶えず変化および進化する規制環境を乗り切るうえで組織が抱える困難を反映しています。製品とテクノロジーの進歩は FDA や規制機関の規制を作る能力を追い越しているため、それらの機関は常に追いつこうとしています。さらに、サイバー・セキュリティと医療における規制の集合体は、組織の法務、IT、およびその他のリソースに大きな損害を与えています。メーカーは多数の規制を組み込む必要があり、それらの多くはあいまいだったり冗長だったりします。組織がコンプライアンスを実現しても、それは一度で終わってしまうシナリオではありません。組織は、後れを取らないように投資を続ける必要があり、組織が規制機関に対する遅れを取り戻しているときに、FDA や他の規制機関はテクノロジーの進歩に対する遅れを取り戻すという、奇妙な平行状態が生じます。

FDA によるサイバー・セキュリティ・リスクのガイドラインのベスト・プラクティス

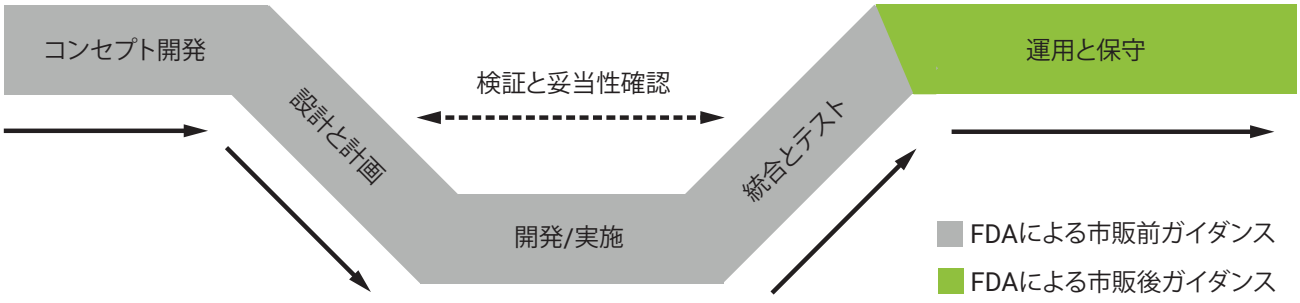
「合理的なセキュリティ」というコンセプトが、FDA の基盤の 1 つです。医療機器メーカーは、開発プロセスにおける対等なステークホルダーとして、品質、スピード、その他の事業の優先順位とともにセキュリティを扱った場合にのみ、合理的なセキュリティを実現することができます。

組織が常にバランスを取る必要があるトレードオフの 1 つに、納期遅れのコストと、一方ではセキュアでないソフトウェアのコスト、他方では潜在的な侵害のコストに対する収益があります。

最適な解決策は、リスク管理プロセスを使用して、セキュリティをすべての開発フェーズに組み込むことです。このやり方を用いれば、セキュリティによって組織は最も費用対効果の高い結果を得ることができます。

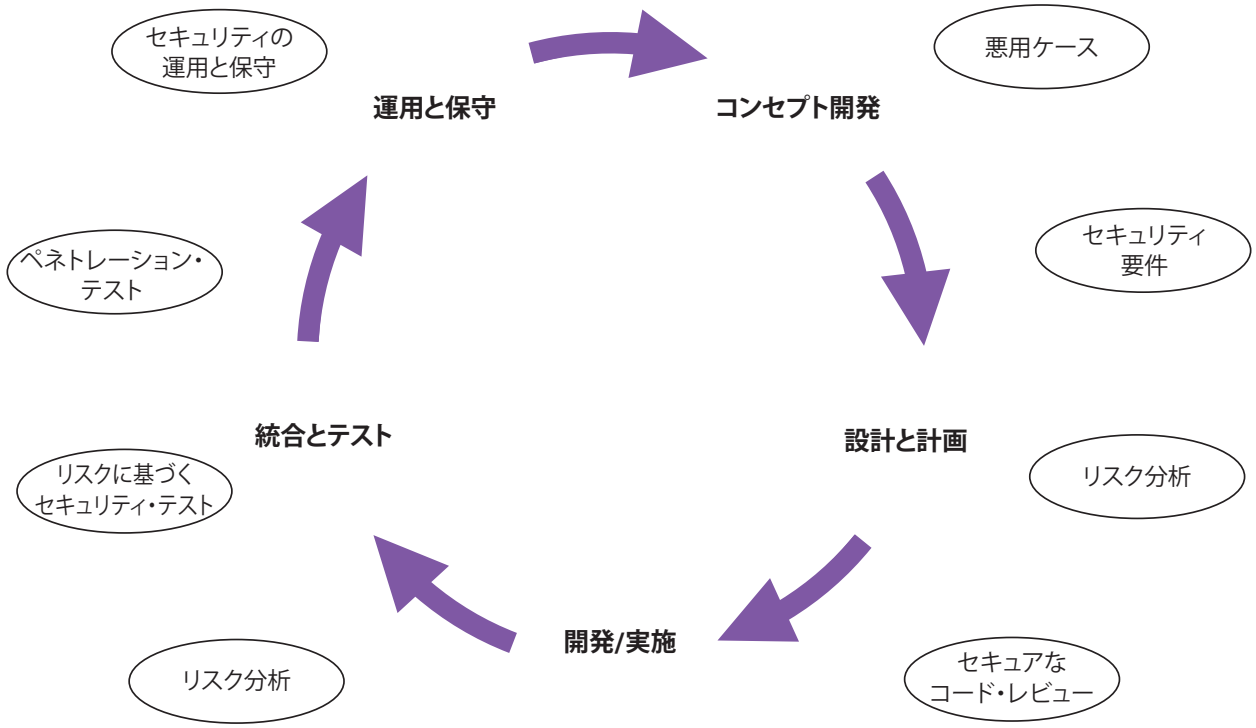
セキュアなシステムまたはソフトウェアの開発ライフサイクル

医療機器には、使用開始から廃棄までのライフサイクル全体を通して、継続的なセキュリティと品質の保守が必要です。システム開発ライフサイクルまたはソフトウェア開発ライフサイクル（SDLC）のフェーズごとの適切なツールと明確なステージ・ゲートにより、医療機器メーカーは、品質、セキュリティ、安全性に対応するセキュアな対策を確立して、FDA によるガイダンスを順守することができます。



システム開発ライフサイクル（システム・エンジニアリングの V モデル）

FDA による市販前および市販後ガイダンスでは、SDLC の一部として、サイバー・セキュリティの脆弱性と不具合の監視、特定、対応が推奨されています。メーカーは、特定のイベントによってトリガーされたチェックポイントで、テスト、分析、検証、証明、妥当性確認などの統合されたセキュリティ・アクティビティを実施する必要があります。チェックポイントは、事業目標を確実に達成しながら効果的なリスク管理を行うガバナンス構造を形成する必要があります。



セキュアな SDLC のためのソフトウェアのセキュリティ・ゲートとタッチポイント

セキュリティ保護の対象

FDA は、医療機器メーカーが IoT のすべての側面に対応するリスク評価を実施することを期待しています。同じ医療機器メーカーのすべての部分に対して簡潔なシステムもあれば、複数の部分および接続に対して複雑なシステムもあります。FDA による規制ガイダンスは、部分ごとに異なる場合があります。FDA による市販前レビューでは、各部分がどのようにシステム全体のリスクの一因となるかが考慮されます。そのため、メーカーは、自社の医療機器のすべての部分がどの程度安全かつ効果的であるかを示すために、システムレベルの追加文書を必要とする場合があります。

一般的なネットワーク接続型医療機器のアーキテクチャまたは設定には、次のものが含まれています。

- 組み込みシステム：専用のコンポーネント
  - オンチップ・メモリ
  - マイクロプロセッサまたはコントローラ
  - ファームウェア
  - Bluetooth、近距離無線通信、その他の有線プロトコルのほか、ユニバーサル・シリアル・バス、セキュアなデジタル・カード、マルチメディア・カードなどのデータ・ポート
  - データ入力 / 出力、センサー、アクチュエータなどの補助装置の周辺ハードウェア
- 臨床医システム
- モバイル・デバイスとモバイル・アプリケーション
- ゲートウェイまたはハブ
- クラウド・サービス
- バックエンド・インフラストラクチャ
- Web サイトと API
- サードパーティの統合

どのように、いつセキュリティを施すか

セキュリティは、状態でも結果でもありません。SDLC 内のタッチポイントを統合した継続的なアクティビティです。

SDLC のフェーズごとの主なアクティビティ

アクティビティ	コンセプト開発	設計と計画	開発 / 実施	統合とテスト	運用と保守
プロセス分析と開発	•	•			
脅威モデリング	•	•			
アーキテクチャ・リスク分析	•	•	•	•	•
静的解析			•		
コンポジション解析			•		•
動的解析			•		
ペネトレーション・テスト				•	•
クラウドおよびコンテナの セキュリティ評価				•	•
モバイル・アプリケーションの セキュリティ・テスト				•	•
ネットワークの セキュリティ・テスト				•	•

悪用ケース

セキュリティの状況は急速に変化します。明日の治療が昨日の脆弱性の対象とならないように、メーカーは攻撃者の脅威や技術に対して遅れを取らないようにすることが重要です。悪用ケースにより、開発チームは、攻撃者の立場で考え、セキュリティをコンセプト開発、設計、計画に統合することができます。攻撃者が既存のセキュリティ対策や欠落しているセキュリティ対策を回避する方法を探すことによって、新しいセキュリティ要件や受容基準を作成することができます。

セキュリティ要件

開発チームは、機能要件や非機能要件とともに、さまざまな規制を満たす要件や FDA ガイダンスやセキュア・コーディング規約のようなガイダンス標準を参照してセキュリティ要件の概要を定義する必要があります。セキュリティ要件はリスク評価全体を通して定義されるのが理想的で、主に設計フェーズや計画フェーズで定義されます。

セキュリティ要件は、事前定義された要素に基づいてチェックリストを使用して特定されますが、開発スタッフとセキュリティ・スタッフの積極的な協力によってソリューション固有の要件も定義する必要があります。プログラムとリスク評価は、セキュリティ要件の推進に役立ちます。

医療機器メーカーは、実行可能なロードマップをセキュリティ・チームと開発チームに提供することによって、AppSec の具体的な課題と目標に対応することができます。このプロセスには、プログラムの目標の実現、計画を成功させるために必要なリソースの特定、成功を判断するためのマイルストーンとメトリクスの導入を行うために、包括的な計画を含める必要があります。

リスク分析

医療機器メーカーは、コンセプトと開発の最初のステージから、セキュリティを設計に組み込む必要があります。脅威モデリングやアーキテクチャ・リスク分析などの設計解析技術を採用して、システム・アーキテクチャでセキュリティ上の脆弱性を探す必要があります。設計でセキュリティ上の問題を特に探していない場合、それらのセキュリティ固有の障害モードは見落とされます。セキュリティの障害モードについての理解は、埋め込み型医療機器の生体適合性障害モードについての考慮などと同等に重要です。適切に実行するには、特定の専門知識が必要です。

事業主を含めて、製品開発チームは、リスク分類プロセスを完了することで、プロジェクトの本質的な開発リスクを見極める必要があります。それは、SDLC の後続フェーズで実行する、該当するセキュリティ・アクティビティを特定するためにも役立ちます。また、組織の成熟度が高い場合、セキュリティ・アーキテクトは技術的な設計を脅威モデリングやアーキテクチャ・リスク分析としてレビューします。コーディング・フェーズの後、該当するすべてのセキュリティ・アクティビティが実行されていることを確認するために、再度リスク分析を実行します。

リスク分析は、主に、システムの運用状況に影響を与える可能性のある要因の影響を受けます。例えば、指定された機能またはシステム要素によって規制当局による管理に従う健康上の個人情報が処理されるかどうかは、リスクを見極める要因になります。考慮すべきその他のリスクとして、サプライ・チェーン、患者の安全性、事業関連のリスクなどがあります。

脅威モデル

脅威モデリングでは、悪意ある行為者がどれだけ損害を与えることができるかを確認するために、悪意ある行為者の観点が採用されます。アプリケーションを構築および実行するために医療機器メーカーが依存している外部コンポーネントが、セキュアな設計の侵害、管理の誤設定、セキュリティ対策の抜け、誤用の影響をどれだけ受けるかを調べるため、よく知られているあらかじめ準備された脅威の先が見据えられます。

脅威モデルでは、主なソフトウェア・コンポーネント、資産、脅威エージェント、セキュリティ管理、オブジェクト間の対応する関係を特定することで、システムの攻撃対象領域について記述されています。設計上の要求と規制当局への申請に組み込むトレーサビリティ・マトリクスも作成されます。

脅威モデルには次のものを含める必要があります。

- リスクによって優先順位が付けられた資産
- 可能性によって優先順位が付けられた脅威
- 発生する可能性が最も高い攻撃
- 成功または失敗の可能性がある現在の対策
- 脅威を減らすための改善策

製品チームは、初日からセキュリティについて考え始める必要があります。新製品は発想段階にあり、ホワイトボードにいくつか箱を描いただけでしかなくとも、脅威モデリングを開始する情報は十分であり、うまくいかないわけがありません。システムでインターネットが使用されている場合、それは懸念事項になります。モバイル・アプリケーション、患者の電話、無線通信も同様です。メーカーは、保有情報を使用して、システムのセキュリティに大きな良い影響を与える可能性のある特定のセキュリティ措置を構築することができます。

FDA によると、「脅威モデリングは、医療機器の TPLC [製品ライフサイクル全体] を通してセキュリティを強化するための青写真を提供し、医療製品の安全性と有効性を確実に改善します。脅威モデリングは、科学によって推進されるペネトレーション・テストや、2018 年の市販前ガイダンスの草案で特定された、終了段階でのその他のセキュリティ・テストの基礎を築くのに役立ちます。」[22]

アーキテクチャ・リスク分析

セキュリティ上の問題を引き起こすソフトウェアの欠陥の半分が設計上の欠陥です。そのため、コード行内のセキュリティ上のバグについてのソフトウェアの単純なテスト、またはアプリケーションのペネトレーション・テストでは、システムを攻撃に対して脆弱な状態にする問題の半分は無視されます。

アーキテクチャ・リスク分析は、自動化されたツールが見つけることのできない設計上の欠陥を強調する脅威モデルよりも掘り下げたテストです。個別の欠陥に対する軽減や改善の具体的な助言も行われます。FDA によるガイダンスの草案では、メーカーがサイバー・セキュリティ・リスクを開発プロセスの一部として考慮することが求められています。アーキテクチャ・リスク分析は、サイバー・セキュリティ・リスク管理の必要事項の一歩先を行くステップです。

アーキテクチャ・リスク分析により、医療機器メーカーは、徹底的にリスクを調べ、設計上の根深い欠陥を見つけることができます。これらの評価には、既知の攻撃戦術が使用され、掘り下げた依存関係分析が含まれます。メーカーは、主なコンポーネント、資産、脅威エージェントの間の関係と、アプリケーションの設計におけるシステムの欠陥を見つけることができます。

セキュアなコード・レビュー

設計が実施とテストに着手すると、FDA は、セキュリティに的を絞った解析とテスト技術 (専用コードに対する静的解析、オープンソース・コードに対するコンポジション解析、実行中のアプリケーションに対するファジング・テスト、ペネトレーション・テストなど) の必要性を正式に認めます。2018 年の FDA による市販前ガイダンスの草案と AAMI TIR57 の両方で、静的コード解析、動的コード解析、ペネトレーション・テスト、医療機器のセキュリティ・リスクを管理するその他のテクノロジーについて記載されています。

静的解析

静的コード解析または静的アプリケーション・セキュリティ・テスト (SAST) では、系統的にスキャンが行われ、掘り下げたテストが適用されます。その結果、重要なソフトウェアに共通のソースコードにおけるセキュリティ上の脆弱性が特定および除去されます。当初、SAST は機能障害に対応するために開発されましたが、進化して、セキュリティ上の欠陥、特に、共通脆弱性タイプ (CWE) と呼ばれるソフトウェアの脆弱性タイプを列挙する効果的な方法になりました。

コンポジション解析

サードパーティのソフトウェア・コンポーネントでは、SAST に必要なソースコードに常にアクセスできるとは限りません。2024 年の「オープンソース・セキュリティ & リスク分析」（OSSRA）レポートによると、医療産業、医療技術産業、ライフサイエンス産業における監査済みコードベースの 88%にオープンソース・コードが含まれています。[23]

ソフトウェア・コンポジション解析（SCA）は、チームが、アプリケーションとコンテナにおけるオープンソース・コードとサードパーティ・コードの使用に伴うセキュリティ、品質、ライセンス・コンプライアンスのリスクを管理する際に役立ちます。SAST と SCA を組み合わせると、医療機器メーカーはセキュリティ、品質、ライセンスのリスクを追跡および管理し、FDA による市販前ガイダンスに応えることができます。

NIST、Healthcare Industry Cybersecurity Task Force、FDA では、医療提供組織が影響を受けるかどうかを素早く見極めることができるように、ソフトウェア部品表（SBOM）が推奨されています。SBOM には、医療機器のコンポーネントおよびそれらのコンポーネントに関連する既知のリスクについて記載されています。優れた SCA ツールまたはサービスは、アプリケーションやコンテナの正確な SBOM を提供する必要があります。

セキュリティ・アクティビティ・トップ 10

- 製品のセキュリティ作業グループの結成
- システムレベルのセキュリティ要件の開発
- コンプライアンスとセキュリティ・トレーニングの提供
- 現行の製品サポート機能の拡張
- 設計レベルのリスク評価アクティビティの完了
- セキュリティの文書化の確立
- 適切な自動システム解析ツールの採用
- オープンソースおよびベンダーのリスクの把握
- ベンダー管理の形式化
- システム・エンジニアリングの役割の形式化

SBOM により、ハードウェア中心の、サードパーティのサイバー・セキュリティ・リスクを適切に管理できるようになります。FDA による 2018 年の市販前ガイダンスの草案では、SBOM に、従来のソフトウェア（ファームウェアを含む）、プログラマブル論理、ハードウェアが含まれている必要があることが強調されています。また組織が商用ソフトウェア、オープンソース・ソフトウェア、脆弱性の影響を受けやすいか受けやすくなる可能性のある既製のソフトウェア・コンポーネントおよびハードウェア・コンポーネントを列挙する方法の概要も記載されています。このガイダンスでは、一貫性と標準化の裏付けとして医療機器の SBOM の特定の主要素が提案されています。[24]

SCA が重要なテスト方法であるにも拘わらず、オープンソースの脆弱性管理プログラムを保有しているのは、2020 年の「セキュア開発成熟度モデル」（BSIMM）レポートで調査された医療組織のわずか 6% でした。[25]

動的解析

動的アプリケーション・セキュリティ・テスト（DAST）では、Web アプリケーションの実行時に、攻撃をシミュレーションし、セキュリティ上の脆弱性を特定することで、ソースコードにアクセスせずに、実際のリスクを見つけることができます。

DAST では、共通の脆弱性（SQL インジェクション、クロスサイト・スクリプティング、セキュリティの誤設定、および Open Web Application Security Project（OWASP）トップ 10 の Web アプリケーション・セキュリティ・リスク、CWE の最も危険なソフトウェア脆弱性トップ 25 などのリストに詳述されているその他の脆弱性など）を特定するために、自動化されたツールを使用できます。

DAST には、認証およびセッション管理、アクセス制御、情報漏洩など、追加設定なしのツールで見つけることができない脆弱性を見つけるために、マニュアル・テストを含めることもできます。マニュアル・レビューでは、偽陽性を特定することもできます。

ファジング・テスト

ファジング・テストは、未知の（ゼロデイ）脆弱性を見つける際に非常に効果的です。ファジング・テストは、外部インターフェースを介して実行中のシステムと相互通信し、不正な動作をトリガーするために不正な形式データを提供します。このタイプのテストの範囲は広く、カスタム・テスト、アーキテクチャまたはソースコード・レビューから駆動されるリスクベースのファジングから、必要に応じて、時間、日、または週に対して入力され実行される、自動化されたファジングにまで至ります。

医療機器では、ゼロデイ脆弱性をもたらす可能性のある、Bluetooth、HL7、DICOM など、さまざまなプロトコルが使用されます。プロトコル・ファジングでは、開発中やテスト中にセキュリティ上の欠陥を先回りして検出できるため、メーカーは現場で侵害や医療機器の障害に対応せずに済みます。

ペネトレーション・テスト

ペネトレーション・テストは、複数のテスト・ツールと掘り下げたマニュアル・テストを使用することで DAST を拡張し、ビジネス・ロジックの脆弱性を見つけ、それらの悪用を試みることができます。現在の既知のセキュリティ・リスクに対するある時点の評価であり、セキュリティの検証および妥当性確認を伴います。ターゲット・システムに対する実際の攻撃をシミュレーションするように設計されているテストの最後の層です。

組み込みソフトウェアのみのシステムに対するペネトレーション・テストは、メーカーがリスクを特定および解決し、それらのリスクが再び発生しないようにするのに役立ちます。メーカーは、SDLC の任意のステージで、組み込みデバイス、モバイル・アプリ、アプリケーションに対して質の高い多重ペネトレーション・テストを実施することや、それを実施するチームを採用することができます。

ペネトレーション・テストの第一の目的は、実際の実施環境で潜在的なセキュリティ上の脆弱性を特定することです。メーカーは、通常、これらのテストを攻撃者の立場から実施し、さまざまな侵入地点からシステムが脅威にさらされていることに注目します。マニュアル・テストでは、ビジネス・ロジックの欠陥も明らかになります。

リスクベースのセキュリティ・テスト

メーカーは、開発後、品質保証フェーズでセキュリティ・テストを実施して、セキュリティ要件の妥当性確認を行う必要があります。マニュアル・テストのアクティビティと自動化されたテストのアクティビティおよびそれらの評価基準は、テスト対象システムのリスク・プロファイルに基づいています。

リスクベースのセキュリティ・テストの実施領域として、クラウドおよびコンテナ、モバイル・アプリケーション、ネットワークがあります。

クラウドおよびコンテナのセキュリティ評価

医療機器メーカーは、自社の環境におけるクラウド・セキュリティ管理の実施方法と、クラウド・アプリケーションにおけるセキュリティ管理のアーキテクチャを評価する必要があります。クラウド・アーキテクチャのリスク分析では、セキュリティ管理が不十分な箇所と、それらを改善する方法の概要が示されます。クラウド設定のレビューにより、クラウド設定によってセキュリティ・チェックが持続されているかどうかが明らかになります。

モバイル・アプリケーション・セキュリティ・テスト

モバイル・アプリケーション・セキュリティ・テスト（MAST）は、静的テスト技術と動的テスト技術を組み合わせて、iOS アプリと Android アプリおよびそれらのバックエンド・コンポーネントの脆弱性を見つけます。MAST は、医療機器メーカーが、ソースコードにアクセスせずに、モバイル・アプリケーションでセキュリティ上の脆弱性を系統的に見つけて修正することができるように、クライアント側コード、サーバー側コード、サードパーティ・ライブラリの解析を迅速に実施できるようにします。

ネットワーク・セキュリティ・テスト

ネットワーク・セキュリティ・テスト（NST）では、手動トリアージを使用した自動スキャンによって、外部ネットワークおよびシステムで共通の重要な脆弱性が検出されます。NST のチェックリストには、暗号化されたトランスポート・プロトコル、SSK 証明書のスコープの問題、管理サービスの使用などのテスト・ケースを含めることができます。

セキュリティの運用と保守

セキュリティの運用は、通常、最初の配置の後およびライフサイクル全体を通して、システムの保護と監視を必要とします。医療機器およびそのアプリケーションの変更、アップグレード、廃棄、交換に関する運用と保守アクティビティには、顧客と現場からのフィードバックの収集、新たな脆弱性についての警告と規制の更新の監視、パッチの適用と改善の実施、規制当局や顧客に対するサイバー・セキュリティ・インシデントと EOL 情報の伝達が含まれます。

サポート・アクティビティ

医療機器メーカーは、セキュリティのタッチポイントの実施をサポートするために、組織的なアクティビティとセキュリティに的を絞ったアクティビティの両方が必要です。

セキュリティ・トレーニング

セキュリティ・トレーニングは、堅牢なシステムのセキュリティ・プログラムを推進するために医療機器メーカーが着手する最も重要なアクティビティの 1 つです。トレーニングは、テスト結果の解釈の改善、より多くの情報に基づく意思決定、組織全体でのセキュリティ文化に寄与します。

トレーニングのトピックには、脅威モデリング、アーキテクチャ分析、ソフトウェアのセキュリティの基本、セキュリティ要件、防衛的プログラミング、セキュアなコード・レビューなどが含まれます。個別の役割や責任に合わせて調整する必要があります。

セキュリティ・ライブラリ

医療機器メーカーは、セキュリティ・ライブラリと設計パターンを保守することで、実装におけるばらつきやエラーを減らし、生産性を上げることができます。セキュリティ・ライブラリには、開発者やエンジニア向けに、吟味されたソリューションや共通のセキュリティ機能を含む実装に役立つものが用意されています。

オープンソースのリスク・インテリジェンス

多くのシステムで、アプリケーションやシステムの機能をサポートするオープンソース・ライブラリが使用されています。全体的なリスクに対応するためには、オープンソース・ライブラリがシステムにもたらす可能性のあるリスクについて理解することが重要です。開発者は、オープンソース・コンポーネントを特定および評価し、セキュリティの状態を監視する必要があります。オープンソースのリスク・インテリジェンスは、SCA の出力をサポートするプロセスです。

攻撃インテリジェンスと共有

現在の攻撃パターンと脆弱性についての認識を保守することにより、リスク分析アクティビティを推進することができます。このインテリジェンス（脅威情報の監視、セキュリティのトピックの認識、トレーニング、会議、知識の構築と共有）により、医療機器メーカーは、セキュリティ要件と実装特性を前進させる潜在的な攻撃状況を把握することができます。

メーカーは、医療 ISAC などの情報共有組織に参加する必要があります。それにより、メンバーは、脆弱性データを自社のチームに取り入れ、自社の医療機器がそれらの問題にさらされていることを評価することができます。また、調整された脆弱性開示ポリシーを開発して、組織全体にわたって顧客とともにアクティビティを管理する必要があります。

ポリシーと文書

完全なセキュリティ・プログラムを開発するうえで、医療機器メーカーは、目標の実現においてどのような成果物とプログラムが役立つかを特定するために、社内文化と文書階層を分析する必要があります。事業主とコンプライアンス担当者が維持する社内プロセスの支えがなくなると、セキュリティに対する多くの取り組みは水泡に帰してしまいます。サイバー・セキュリティの文書には、設計図、系統図、システムの脅威モデル、リスク管理文書を含める必要があります。

最後に

妥当なセキュリティに対する FDA の基準を達成するには、セキュリティと規制の現状を乗り切るうえで継続的なサポートが必要です。セキュアな SDLC によって通知および強制されるセキュリティ・プログラムも必要です。それにより、企業は、適切なリスク管理とトレードオフの決定を行うことができます。

医療機器のセキュリティの現状を乗り切ることは困難であるため、医療機器のセキュリティについての知識と技術のあるベンダーを選定することはメーカーにとって特に重要です。

ブラック・ダックは、ソフトウェアのセキュリティにおけるリーダーとして認められています。クライアントがより安全な治療提供システムを構築できるよう、医療業界の取り組みに積極的に関わっています。ブラック・ダックは、主要な政府機関、コンソーシアム、作業グループによって公開された、セキュアな設計ガイダンス文書に対して大きく貢献しています。ブラック・ダックのチームは、AAMI 作業グループを通じて、セキュアな設計ガイダンス文書（『Avoiding the Top 10 Software Security Design Flaws』や『Building Code for Medical Device Software Security by the Institute of Electrical and Electronics Engineers (IEEE) など』を協力して作成しています。また、ミシガン大学のアルキメデス・グループ、IEEE、アメリカ国立科学財団、医療 ISAC、FDA と連携して、医療企業のサイバー犯罪との戦いを支援しています。

ブラック・ダックの顧客には、医療機器メーカートップ 10 と、マネージド・ケア企業トップ 5 のうちの 4 社が含まれています。

さらに、ブラック・ダックのサービス・チームには、医療および医療以外のさまざまな組み込みシステム（埋め込み型医療機器、薬物送達システム、手術用画像システム、ATM、ゲーム機、スマートメーターなど）での評価経験があります。ブラック・ダックと連携したメーカーは、複数の業界のイノベーションの恩恵を受けることができます。

ブラック・ダックは、FDA によるガイダンスを順守したセキュアな医療機器を構築する皆様のお役に立つことができます。

注釈

1 David R. Ramsdale, Archana Rao, Cardiac Pacing and Device Therapy, Springer, 2012

2 Oleg Bestsennyy, Greg Gilbert, Alex Harris, Jennifer Rost, Telehealth: A quarter-trillion-dollar post-COVID-19 reality? McKinsey & Company, July 9, 2021.

3 U.S. Food and Drug Administration, 510(k) Clearances, June 9, 2021.

4 Protenus and DataBreaches.net, 2021 Breach Barometer, Protenus, Inc., 2021.

5 Sara Mitran, Medical Device and Network Security: Coming to terms with the Internet of Medical Things, Frost & Sullivan, 2019.

6 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, BlackDuck, 2017.

7 Chris Sherman, Salvatore Schiano, Best Practices: Medical Device Security. Forrester Research, 2019.

8 Paul Sisson, Scripps ransomware shutdown hits the two-week mark, The San Diego Union-Tribune, May 14, 2021.

9 Nicole Perlroth, Adam Satariano, Irish Hospitals Are Latest to Be Hit by Ransomware Attacks, The New York Times, May 20, 2021.

10 Federal Bureau of Investigation, Cyber Division, FBI TLP White Flash Alert: Conti Ransomware Attacks Impact Healthcare and First Responder Networks. American Hospital Association, May 20, 2021.

11 Ariel Hart, Cyber attack disrupts cancer care, The Atlanta Journal-Constitution, April 27, 2021.

12 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, BlackDuck, 2017.

13 Sedgwick, 2021 Recall Index Report, United States Edition, 2021.

14 Christina Jewett, Hidden FDA Reports Detail Harm Caused By Scores of Medical Devices, KHN.org, March 7, 2019.

15 U.S. Food and Drug Administration, Classify Your Medical Device, 2020.

16 Ibid.

17 Ibid.

18 U.S. Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices, December 28, 2016.

19 Ibid.

20 Ibid.

21 Ponemon Institute, Medical Device Security: An Industry Under Attack and Unprepared to Defend, BlackDuck, 2017.

22 U.S. Food and Drug Administration, FDA CDRH and Medical Device Security: Response to NIST Regarding President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), 2021.

23 BlackDuck, Open Source Security and Risk Analysis, 2021.

24 U.S. Food and Drug Administration, FDA CDRH and Medical Device Security: Response to NIST Regarding President's Executive Order (EO) on Improving the Cybersecurity of the Federal Government (EO 14028), 2021.

25 BlackDuck, Building Security In Maturity Model, 2021.

ブラック・ダックについて

ブラック・ダックは、True Scale Application Security によって、モダン・ソフトウェアの経営レベルのリスクに対応し、規制された、AI を活用した世界におけるソフトウェアの信頼性を保証します。ブラック・ダックのソリューションは、セキュリティ、規制、ライセンスに関するリスクを排除しつつ、組織のスピード、精度、コンプライアンスのトレードオフから解放します。クラウドでもオンプレミスでも、コードが実行されるあらゆる場所でミッション・クリティカルなソフトウェアを保護するには、ブラック・ダックこそが選択肢となるのです。ブラック・ダックを活用することで、セキュリティ・リーダーはよりスマートな意思決定を行い、自信を持ってビジネス・イノベーションを推進することができます。

詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp

©2026 Black Duck Software, Inc. All rights reserved. Black Duck® は Black Duck Software, Inc. の米国およびその他の国における登録商標です。その他の会社名および商品名は各社の商標または登録商標です。2026 年 5 月