ivanti Neurons

医療IT、生体医学、セキュリティ

医療機器の可視性を高め、セキュリティリスクを軽減するためのガイド

目次

はじめに

コネクテッド医療機器は、医療IT、生体医学、セキュリティを司るすべての部門にとって大きな課題です。医療機器には、本質的にサイバー脅威に対して脆弱という側面があります。サイバー攻撃が恐ろしい結果を招く可能性があるにもかかわらず、従来のサイバーセキュリティ対策では対応が不可能。それどころか、臨床業務に重大な支障をきたす危険性すらあります。

本ガイドでは、医療機器の可視性を高め、セキュリティリスクを低減させるための3つのプロセスをご紹介します。医療機器のサイバーセキュリティを確立することは、複数のステップを必要とする継続的なプロセスです。強固な基盤からスタートし、系統的かつ体系的なアプローチを採用しましょう。

コネクテッド医療機器に関連するサイバーセキュリティのリスクを検出、評価、軽減する方法を習得しておきましょう。本ガイドでご紹介する3つのフェーズは1回限りのプロセスではなく、定期的なサイクルとして取り組むものです。医療機関のITおよびセキュリティチームは、環境調査、リスク評価、日常的に検出されるセキュリティ問題への対処などにおいて、これらのフェーズを継続的に実行する必要があります。

サイバー攻撃に対する医療機器の脆弱性とは?

ネットワークや機器に接続される医療機器の数は増加する一方。これは便利であると同時に、病院や医療関係者に重大なセキュリティ上の脆弱性をもたらすことにつながっています。これらの機器の多くは安全性が十分に確保されておらず、積極的な管理も行われていないため、さまざまなサイバーセキュリティ上の脅威につながっています。

医療機器が脆弱な理由

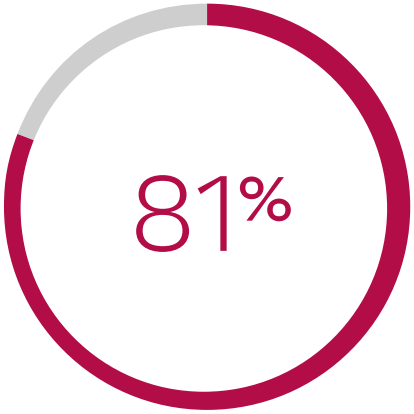
- ソフトウェアコードがセキュリティレビューを受けていない
- 認証が弱い、または存在しない
- 安全性が確認されていないデータ転送チャネルが多く、暗号化もされていない
- 可視性が低く、どの機器がアクティブに使用されているのかわからない
- 機器の使用状況やセキュリティ問題の監視ができない
- 使用中止となった機器が安全に廃棄されていない
- ソフトウェアアップデートがない、またはほとんど導入されていない

環境の理解
所有するIT機器および医療機器を把握して正しく分類し、臨床状況を確認したうえでネットワークのニーズを特定

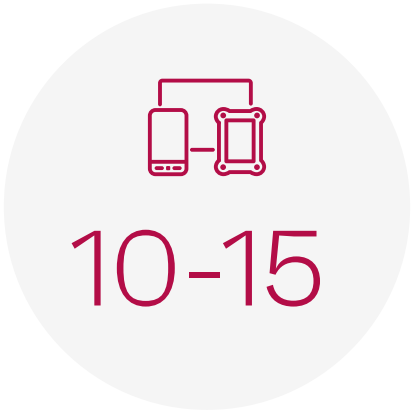
リスク評価
機器の脆弱性とネットワーク関連のリスクを特定し、各機器にリスク指標を割り当て、修復のための推奨事項を提供

機器の保護
機器レベルでのセキュリティに対処し、LANでの機器の隔離、LANまたはWAN上での不要な通信の切断、セキュリティ問題が発生した際の検出戦略を確立

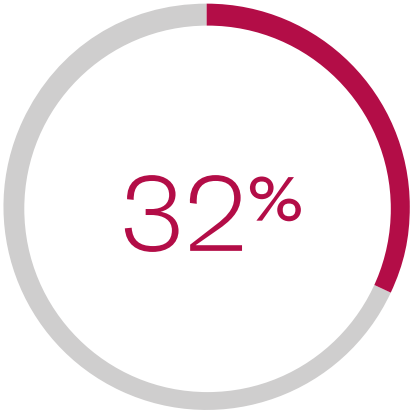
問題はどの程度深刻なのか？



医療機関の81%が過去2年間にサイバー攻撃を受けたことがあると回答



医療機関の32%が、医療機器のセキュリティが最大の懸念事項であると回答



病院のベッドには1台あたり10〜15台の医療機器が接続され、370万台以上が稼働中

出典：KPMG, Wired

医療機器に影響を与える脅威の種類とは?

マルウェア
エンドポイント保護機能を備えていない医療機器が多く、マルウェアに対して特に脆弱

内部脅威
認証が弱いため、悪意ある内部関係者が簡単に不正アクセスをし、機器を勝手に利用する恐れがある

Webアプリケーション攻撃
Webインターフェイスを介して管理可能な医療機器の場合、インジェクション攻撃、クロスサイトスクリプティング(XSS)、パス・トラバーサル攻撃などのサイバーリスクを生む

機器の誤操作
Windows PCで操作されることの多いコネクテッド医療機器は、病院のスタッフが同じデバイスでインターネットを閲覧したり、ソフトウェアをインストールしたりするたびにリスクが高まる

サイバーセキュリティのリスクと攻撃による影響を評価する方法

FDAの医療機器ガイドライン は、機器のリスクレベルに応じてリスクを以下の2種類に区分しています。

ティア1:高度のサイバーセキュリティリスク	ティア2:標準サイバーセキュリティリスク
対象となる医療機器	**対象となる医療機器**
他の医療製品または非医療製品、ネットワーク、インターネットに接続可能 または 機器に影響を及ぼすサイバーセキュリティインシデントにより、複数の患者に直接害を与える可能性がある	他の機器やネットワークに接続可能だが、患者に直接害を与える可能性はない または ネットワークに接続できないが、患者に直接害を与える可能性がある

CVSSリスク計算 のようなフレームワークを使用すると、リスクをより細分化して評価できます。またサイバーセキュリティのリスク評価を行う際は、以下の点に注意しましょう。:

- ソフトウェアの脆弱性
- 患者の安全性
- 認証
- プライバシー
- ネットワーク環境
- 稼働停止

フェーズ 1.
コネクテッド医療機器が置かれている環境を理解

問題解決の最初のステップは、問題の存在を明らかにし、その範囲を把握することです。コネクテッド医療機器の問題は可視性が非常に低く、病院や医療機関のIT、生体医学、セキュリティチームに十分認識されていません。

医療機器はセキュリティチームの盲点

医療機器のセキュリティ対策は、臨床技術部門とIT部門の共通の課題となりつつあります。医療機関には医療機器に関する情報が存在するにもかかわらず、セキュリティチームはそれらに簡単にアクセスできません。

以下のような疑問点は、依然として残されたままです

1. 何台の機器が接続されているのか？
2. どの機器やネットワークと通信しているのか？
3. どんな機器が存在するのか？
4. ネットワークの動作は正常（想定内の動作）なのか、または異常なのか？

コネクテッド医療機器の一覧表示が難しい理由

医療機器は、通常のITネットワークのように、ネットワークスキャンを実行するだけでは特定できません。

- 医療機器は機密性が高い：アクティブなネットワークスキャンを行うと機器の動作に影響を与える恐れがあるため、パッシブな検出を行う必要があります。
- ネットワーク検出ツールでは見つからない：従来の検出ツールでは、ほとんどのコネクテッド医療機器を見つけることができません。単なるWindowsのワークステーションと誤認する可能性もあります。ほとんどの医療機器は、接続中であっても自分からは情報を発信しないため、ネットワーク上で検出するには、アプリケーション層のトラフィックを慎重に分析する必要があります。
- 機器の数と種類が多い：タイプ、ベンダー、バージョンの異なる機器が、数万台存在する可能性があります。
- 状況が常に変化：ネットワークで絶えず追加、交換、削除を繰り返す医療機器は、多くの場合ITが関与する余地がありません。したがって検出とインベントリの作成は継続的に行う必要があります。

ステップ 1. 機器の検出

医療機器に関するすべてのデータを取得し、データベースを構築します。リスクと脆弱性を正しく判断できるよう、質の高いデータを収集しましょう。特に以下の情報は重要です。

- 機器の種類
- 所属部門と環境
- ベンダー
- モデル
- IPアドレス
- OS
- アプリケーションソフトウェアのバージョン
- 最新のセキュリティパッチ

ステップ 2. ネットワークのマッピングと臨床状況

機器のネットワーク動作を理解することで、その機器が外部または内部の脅威にどの程度さらされているかを把握できます。接続中のそれぞれの機器において、以下の情報を取得してください

- 他の機器との通信状況
- 他の機器、ネットワーク、インターネットへの不要なアクセスの有無
- 機器のネットワーク通信のVLAN上での分離状況
- 使用中のプロトコルの種類
- 保護対象医療情報（PHI）データの送受信の場所と、PHIの種類
- インターネットを経由した外部への通信状況
- 機器がベンダーと継続的に通信する必要性
- 機器の種類に応じたインターネット通信の必要性
- 機器のインターネット通信のVPNトンネルでの分離状況

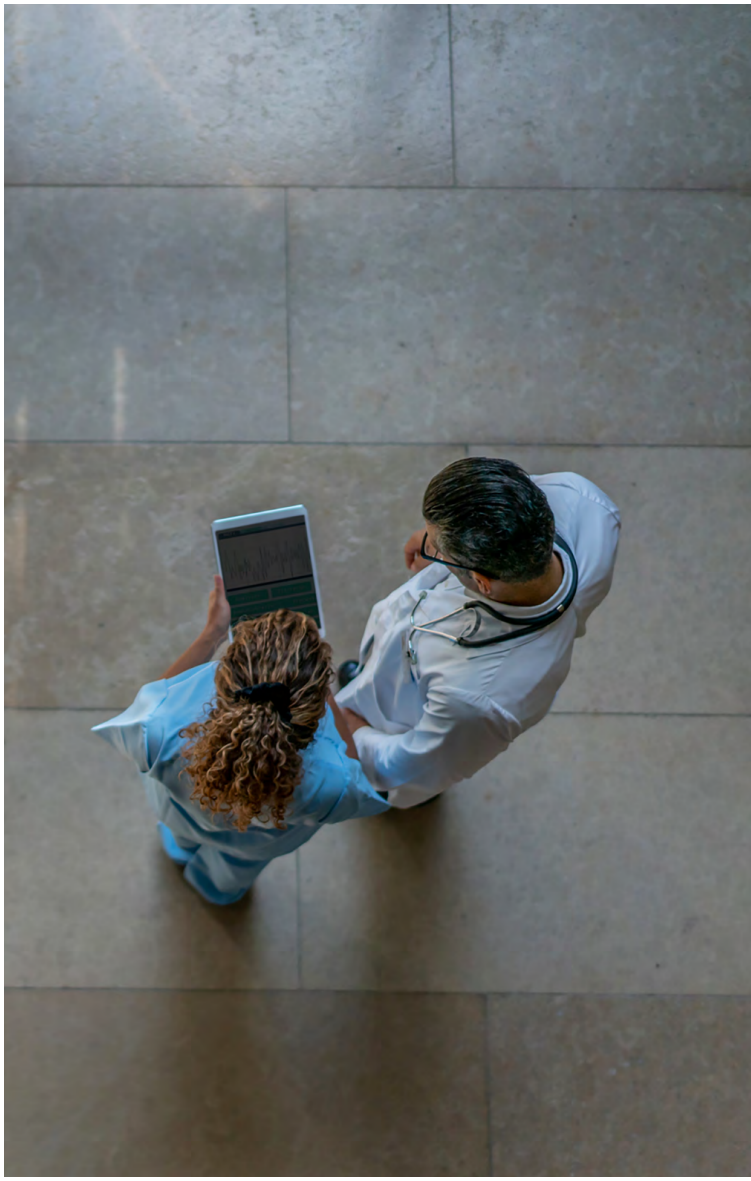
それぞれの機器における臨床用途、拡張性、リスクの度合いを明らかにしましょう。これらのデータを、自動化ツールなしで収集することは非常に困難です。

臨床現場での状況

- どの機器と臨床データの送受信を行っているのか？制御チャネルなどの非臨床通信はどれか？
- 保護対象医療情報（PHI）を転送または保存する機器かどうか？
- 患者の治療に直接関わる機器（患者モニター、輸液ポンプ、ペースメーカーなど）かどうか？FDA Class IIIに該当する機器（生命維持のための機器）かどうか？

対策時の注意点

- セキュリティ対策は、重要なデータフローを妨げないように実施します
- 臨床ワークフローを認識することで、重要な情報の流れに影響を与える可能性のある異常を正確に特定できます
- PHIを保有する機器は、サイバー犯罪者に狙われる可能性が高くなります
- 機器だけでなく、データも保護する必要があります
- 機器は関連する規格や規制に準拠している必要があります
- 患者の治療に直接関わる、または直接危害を加える可能性のある接続中の機器のセキュリティ対策を優先します



フェーズ 2.

リスク評価

接続中の医療機器を詳しく理解し、機器、使用状況、ネットワーク動作のインベントリを作成すると、各機器に関連するリスクと組織への影響を評価できるようになります。

ステップ 1. 機器の脆弱性と修復機会の特定

機器のモデル名、使用中のOS、アプリケーションのバージョンを特定し、それぞれの脆弱性に関するデータを収集します。

同時に、機器の所有者と、セキュリティ問題を解決するためのアクセスレベルを明らかにしておくことも重要です。

ソフトウェアの脆弱性による影響
CVSSリスク計算により、接続中の機器にインストールされたソフトウェアの既知の脆弱性を特定します。

設定ミス
ハードコードされたパスワードやデフォルトのパスワード、パッチが適用されていないOSやソフトウェアなどの、一般的な脆弱性をチェックします。

機器の認証
機器に認証機能があるかどうか、ある場合はその強度、および安全なパスワードが設定されているかどうかを確認します。

管理者の連絡先
臨床技術部門、IT部門、製造業者、外部の請負業者など、機器の管理者を確認します。

アクセスの容易性
セキュリティ管理を実施したり、問題に対処したりする際、セキュリティチームが機器にアクセスしやすいかどうかを確認します。

バックアップ
機器にバックアップや冗長性があるか、また稼働停止した場合の影響度を把握します。

ステップ 2. ネットワークレベルでのリスクの特定

医療機器の脆弱性は、数あるリスクの中での1つの側面にすぎません。ネットワーク接続を分析し、サイバー攻撃者が機器に侵入する経路や手段を特定しましょう。

インターネット接続
機器がインターネット経由で他のシステムに接続しているかどうかを確認します（例：機器がメンテナンスやアップデートの目的でサードパーティや製造元のシステムに接続しているかの確認、など）。

安全性の低い機器への接続
機器が医師のワークステーションなど、安全性の低い機器やエンドポイントに接続する可能性があるかどうかを確認します。また、FTPやSSHなどの管理サービスやデータサービスを公開しているかどうかを確認します。

暗号化
機器が暗号化されていないデータフローを送受信していないか確認します。

安全でないプロトコル
機器が、弱い認証を提供するプロトコル、認証を行わないプロトコル、脆弱性のあるプロトコルを使用していないか確認します。

ステップ 3. リスクの深刻度の特定

医療機器へのサイバー攻撃が成功すると、何が起こるのでしょうか。コネクテッド医療機器に対する攻撃の影響は、医療用ITシステムへの攻撃とは異なり、データのセキュリティやプライバシー問題に限定されません。サイバー攻撃が成功すると、臨床治療が中断され、患者に直接的な危害を加える可能性があります。

CVSSリスク計算の3つの影響度指標にしたがい、リスクの深刻度を特定しておくことをおすすめします。

- 機密性：機器に保存されている、または機器から送信される保護対象医療情報（PHI）の漏洩防止対策
- 信頼性：患者の治療に直接使用される機器が患者の安全性を脅かすリスクへの対策
- 可用性：稼働停止リスクへの対策

患者の安全性	プライバシー	S稼働停止
低：FDA Class I 医療機器（患者やユーザーへのリスクが低～中程度	低：PHIを保有しない機器	低：機器が故障しても患者の治療に影響がない
中：FDA Class II 医療機器（患者やユーザーへのリスクが中～高程度）	中：検査や治療の前後といった限られた期間に少量のPHIを保有する機器	中：機器の故障により、患者の治療に影響があるが、重要な医療行為には影響を及ぼさない
高：FDA Class III 医療機器（生命維持装置、体内に埋め込まれている装置、病気や怪我のリスクが高い装置など、患者やユーザーへのリスクが高い機器）	高：複数の検査や治療にわたり大量のPHIを保有する機器	高：機器の故障により、手術、呼吸器、生命維持のための投薬など、重要な医療行為が妨げられる可能性がある

フェーズ 3.

接続中の医療機器を守るために

機器のリスクに応じてそのレベルを分類するには、まずすべての機器を検出して可視化し、リスク評価のための構造化された取り組みが必要です。患者の安全性、プライバシー、稼働停止などのリスクの影響度をスコアとして数値化し、それぞれの機器に割り当てましょう。

組織はこれにより、許容可能なリスクレベルを定義できるようになります。セキュリティチームは、リスクスコアが許容レベルを超えている機器の保護対策に集中でき、それ以外の機器には別途適切なセキュリティ対策を適用できます。

コネクテッド医療機器のセキュリティ対策は、以下の4つのステップで進めることをおすすめします。

1. 機器の保護：パッチの適用、脆弱なサービスの無効化、ベストプラクティスに基づく設定
2. ネットワークの保護：LANレベルでの分離（ローカルネットワーク内での不要な通信を遮断）、WANレベルでの分離（外部エンティティとの通信は既知のもの以外遮断）
3. インシデントの検出：セキュリティ問題が発生した際に、それを検知するための戦略を立てる
4. 指標と分析：セキュリティプログラムの結果を継続的に分析し、調整と改善に取り組む

ステップ 1. 機器のセキュリティを強化

他のコンピュータ機器同様、コネクテッド医療機器にも最新のセキュリティパッチとソフトウェアアップグレードが必要です。また、安全な認証を可能にするための設定を強化する必要もあります。未使用のポートは閉じ、不要な機能を制限するなど、攻撃対象となるような要因を全般的に減らしましょう。

ほとんどの医療機器はWindows OSを搭載していますが、パッチの適用は、ワークステーションやWindowsサーバーのように簡単ではありません。

医療機器のセキュリティ強化の課題

- 機器の製造元によって検証・承認されたWindowsセキュリティパッチを使用する
- 臨床技術部門は、医療機器の機能に影響を与えないパッチおよび更新方法を検証する

ガイドライン

- セキュリティパッチの展開や機器のセキュリティ強化は、必ずしもすべて成功するとは限りません
- リスクスコアの高い機器を優先します
- リスク評価で特定された既知の脆弱性に対処するためのセキュリティパッチや設定変更を優先します

ステップ 2. ネットワーク分離

コネクテッド医療機器のセキュリティを高めるうえで大切なのは、重要性の低い臨床通信から可能な限り機器を分離し、攻撃対象となる範囲をできるだけ狭めることです。これには、次の2つの要素があります。

- ネットワークセグメンテーションを定義する：医療機器の通信先を、臨床プロセスの一部として機能中の機器やシステムのみに限定します
- 外部通信をブロックする：外部との通信を遮断し、医療機器がインターネットに接続することを防ぎます（機器のベンダーや、その他の既知の組織との通信に必要な場合を除く

医療機器を分離する際の注意点s

- 臨床データフローをそれ以外のデータフローから分離する
- 必要不可欠な臨床上の通信以外は、すべてブロックする

ガイドライン

- 厳密なアクセスポリシーとネットワークセグメンテーションを設定し、重要性の低い通信を制限します
- 影響分析で特定されたリスクと脆弱性に対処するための、セグメンテーションポリシーを設定します
- 機器の機能に必要不可欠な場合を除き、機器のインターネット接続をブロックし、接続する場合は既知の組織に接続先を限定します
- 重要なデータフローを中断しないよう、臨床技術部門および医療技術管理（HTM）チームと緊密な連携をとります

ステップ 3. インシデントの検出と対応

コネクテッド医療機器をすべての潜在的脅威から守り切ることは不可能です。なぜなら、交換できず、かつ重要なレガシー機器は常に存在し、完全にパッチを当てたり分離したりすることが不可能だからです。つまり、攻撃対象を制限することはできますが、排除することはできません。さらに、脆弱な機器を残したまま、分離作業だけに長い時間と手間がかかる場合もあります。機器を監視し、異常な動作が発覚した場合は直ちに検知し、警告することが重要なのは、このためです。

セキュリティインシデントを監視する際の注意点

- ネットワークタップやミラーポートなどのパッシブモニタリングを使用して、機器の稼動状態が中断されないよう監視する
- 臨床状況について収集した各機器の情報を活用し、臨床通信の通常時の状態を把握する
- 現在の動作をベンダーの仕様、過去の動作、内部環境および他の組織における同様の機器の動作と比較する

ガイドライン

- リスクスコアの高い機器に特に重点を置きながら、すべての機器を継続的に監視します
- 進行中の通信を通常の臨床通信と比較するための手段を確立させます
- 通常の動作と大きく異なる場合は、セキュリティに異常があることを警告します
- オンデマンドのネットワークセグメンテーションなど、リモートで迅速に修復できるサードパーティと統合します

ステップ 4. 指標と分析

医療機器のサイバーセキュリティ対策は長期にわたるプロセスです。絶えず変化し続ける脅威に対処するには、時間をかけて維持および改善を続ける必要があります。

進捗状況を追跡しながら方向性が正しいかどうかを確認し、取り組みによって状況が改善されていない場合は、適宜修正を加えてください。医療機器のセキュリティ対策プロジェクトを推進しながら、その進捗状況を確認するためのガイドラインを、以下にご紹介します。

- スコアカードを作成する：医療機器のスコアカードを作成し、時間の経過とともにリスクが低減されるよう継続的に管理します
- 効果のあった活動や戦略を特定する：これまでにKPIを改善し、リスク指標を総合的に低減した実績のある取り組みや戦略を特定します
- KPIを設定し、改善状況を監視する：重要な機器のリスクに基づくKPIを設定し、患者の安全性やサービスの可用性などのビジネス目標と関連付けることで、経営幹部の賛同を得やすくなります
- データを収集する：リスク指標と機器の過去の動作に関するデータを収集することで、より精度の高い調達の判断材料として役立てることができます

Ivanti Neurons for Healthcareは、医療機器資産の可視性を高め、セキュリティリスクを低減します

Ivanti® Neurons for Healthcareなら、医療機器の資産を可視化し、セキュリティリスクを軽減することが可能になります。Ivanti Neurons for Healthcareは、医療機器とInternet of Medical Things（IoMT）を検出してインテリジェントにプロファイルを作成し、セキュリティリスクを評価し、脅威を報告し、複数のデータソース間で機器情報を調整するソリューションです。施設内のさまざまな医療機器を分類し、使用状況などの詳細を把握しながら、セキュリティリスクの低減や異常事態への対応に役立てることができます。また、ベンダーのデータを収集して照合することで、すべての機器情報を一元管理することが可能です。

詳しくは こちらをご覧ください。
ivanti.co.jp/products/ivanti-neurons-healthcare

ivanti Neurons

ivanti.co.jp/neurons
+81 (0)3 52265960
contact@ivanti.co.jp