令和7年度医療情報セキュリティ研修 及び
サイバーセキュリティインシデント発生時初動対応支援・調査等事業

【システム・セキュリティ管理者向け研修】
医療機器の安全確保コース

医療機器のサイバーセキュリティと運用の実践対応

2025年9月11日
一般社団法人ソフトウェア協会

目的

- 医療機器を取り巻くサイバーセキュリティリスクを理解する
- 医療機器のセキュリティに関する制度的枠組みを把握する
- ソフトウェアのEOSや脆弱性管理など、医療機器の技術的セキュリティ対策の要点を理解し、実践に活かす方法を学ぶ
- インシデント発生時の対応フローと安全確認手順を習得する
- 院内での役割分担と継続的なセキュリティ対策の重要性を認識する

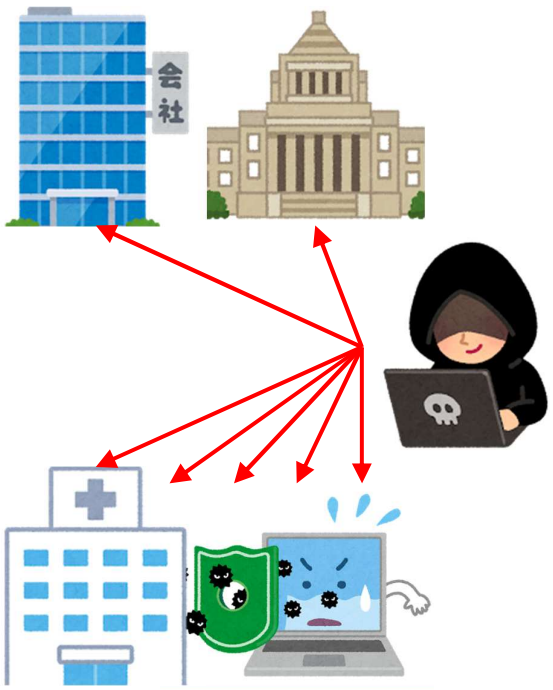
目次

- 医療機関を取り巻くサイバー脅威
- 制度から読み解く医療機器セキュリティの重要性
- 医療機器の技術的対策と脆弱性対応の実践
- サイバーインシデント発生時の医療機器安全確認手順
- 院内で求められる役割分担と継続的対策

医療機関を取り巻くサイバー脅威

医療機関が狙われる背景

大病院や大企業、政府機関など、
規模の大きい組織



組織の規模や業種に関係なく、
セキュリティ対策が手薄な組織

国内の医療機関におけるサイバー攻撃事例

大阪急性期・総合医療センター

【概要】
2022年10月31日、ランサムウェアの攻撃により
電子カルテシステムを含む基幹システムが停止

【被害状況】
・基幹システムサーバーの大部分が暗号化被害
・外来診療の制限、救急受入の停止、予定手術の延期、紙カルテ運用への切替
・約2,200台のPCに不正アクセスの痕跡
→クリーンインストールの実施
・電子カルテシステムの再稼働まで約2ヶ月間
診療機能の全面復旧まで73日間
・調査・復旧費用で数億円
診療制限による逸失利益は数十億円

【出展元】
大阪急性期・総合医療センター
情報セキュリティインシデント調査委員会報告書
https://www.gh.opho.jp/pdf/report_v01.pdf

岡山県精神科医療センター

【概要】
2024年5月19日、ランサムウェアの攻撃により
電子カルテシステムを含む基幹システムが停止

【被害状況】
・最大約4万人分の個人情報の漏洩の可能性
・本院だけでなく東古松サンクト診療所も被害
・紙カルテ運用での診療継続
・約30台のサーバーと244台のPCが暗号化被害
→すべてのPCを完全初期化、もしくは新品へ
・ストレージのデータ全喪失
・電子カルテシステムの完全復旧まで約3ヶ月
・試算では約65人月の復旧工数

【出展元】
岡山県精神科医療センター　ランサムウェア事案調査報告書
https://www.okayama-pmc.jp/wp-content/uploads/2025/02/24bb9b94f7eb10eff58b605c01c384ad.pdf

制度から読み解く
医療機器セキュリティの重要性

サイバーセキュリティに関連する通知等の一覧(1/2)

日付	文書名
平成27年4月28日	医療機器におけるサイバーセキュリティの確保について
平成30年7月24日	医療機器のサイバーセキュリティの確保に関するガイダンスについて
令和2年5月13日	国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）
令和3年6月28日	医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）
令和3年8月23日	医療機器のオペレーティングシステムに係る脆弱性への対応について（注意喚起）
令和3年12月24日	医療機器のサイバーセキュリティの確保及び徹底に係る手引書について
令和4年3月1日	医療機器等に関するサイバーセキュリティ対策の強化について（要請）
令和4年11月10日	医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）
令和5年3月31日	**医療機器の基本要件基準**第12条第3項の適用について
令和5年3月31日	**医療機器のサイバーセキュリティ**導入に関する手引書の改訂について
令和5年3月31日	医療機関における医療機器のサイバーセキュリティ確保のための手引書について

サイバーセキュリティに関連する通知等の一覧(2/2)

日付	文書名
令和5年5月	**医療情報システムの安全管理に関するガイドライン** 第6.0版
令和5年5月23日	医療機器の基本要件基準第12条第3項の適合性の確認について
令和5年7月20日	医療機器の基本要件基準第12条第3項の適用に関する質疑応答集（Q&A）について
令和6年1月15日	医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について
令和6年1月31日	医療機器のサイバーセキュリティに関する質疑応答集（Q&A）について
令和6年3月28日	医療機器のサイバーセキュリティを確保するための脆弱性の管理等について
令和6年4月23日	医療機器のサイバーセキュリティ対策に関連する一部変更に伴う軽微変更手続き等の取扱いについて
令和7年度版	医療機関等におけるサイバーセキュリティ対策チェックリストマニュアル
令和7年4月17日	医療機器のサイバーセキュリティ対策に関連する情報提供について

厚生労働省　医療機器におけるサイバーセキュリティについて
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

医療機器の基本要件基準

医療機器の基本要件基準とは

- 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（薬機法）第41条第3項の規定により厚生労働大臣が定める医療機器の基準
  https://www.mhlw.go.jp/web/t_doc?dataId=81aa6953&dataType=0&pageNo=1
- 患者や使用者、第三者に対して医療機器が安全であり、かつ意図した機能を発揮し、有効性が確保されることを目指す
- GHTF（国際医療機器規制整合化会議）で定められた文書を基にしており、世界的に共通する医療機器の安全確保の考え方を反映
- 「第1章：一般的要求事項」と「第2章：設計及び製造要求事項」で構成され、多岐にわたる要求事項が規定されている

医療機器の基本要件基準の変遷

平成17年 (2005年)	• 基本要件基準制定
平成26年 (2014年)	• 第12条に「プログラムを用いた医療機器に対する配慮」を規定
令和2年 (2020年)	• IMDRF（国際医療機器規制当局フォーラム）による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表 （3年を目途に適用）
令和5年 (2023年)	• IMDRFガイダンスを踏まえ基本要件基準を改正 (第12条第3項の適用)

医療機器の基本要件基準

令和5年（2023年）改正内容

- サイバーセキュリティに関する新たな要件が、第12条第3項として適用
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html
- プログラムを用いた医療機器に対しサイバーセキュリティを確保するための設計及び製造、ライフサイクル活動として、
  ①製品の全ライフサイクルにわたって、サイバーセキュリティを確保する計画を持つこと
  ②サイバーリスクを低減する設計と製造を行うこと
  ③適切な動作環境に必要となる、ハードウェア、ネットワーク、ITセキュリティ対策の最低限の要件を設定すること
  の３つの観点を基本要件基準に盛り込むこととし、基本要件基準を改正

医療機器のサイバーセキュリティに関する通知の変遷

平成27年（2015年）	• 医療機器におけるサイバーセキュリティの確保について
平成30年（2018年）	• 医療機器のサイバーセキュリティの確保に関するガイダンスについて
令和3年（2021年）	• 医療機器のサイバーセキュリティの確保及び徹底に係る手引書について
令和5年（2023年）	• 医療機器のサイバーセキュリティ導入に関する手引書の改訂について

医療情報システムの安全管理に関するGLの変遷

平成17年（2005年）	• 第1版　医療情報システムのセキュリティ管理を目的として策定
平成19年（2007年）	• 第2版　重要インフラとしての医療情報システムという観点
平成20年（2008年）	• 第3版　個人情報保護施策の議論およびモバイル端末普及
平成21年（2009年）	• 第4版　個人情報保護施策の議論およびモバイル端末普及
平成22年～28年	• 第4.1版～第4.3版　DCにおける外部保存等
平成29年（2017年）	• 第5版　改正個人情報保護法、サイバー攻撃の動向
令和3年～4年	• 第5.1版、第5.2版　認証・パスワード、サイバー攻撃の多様化・巧妙化
令和5年（2023年）	• 第6.0版　全体構成の見直し

制度から読み解く医療機器セキュリティの重要性

医療機器の基本要件基準

- 機器の設計・製造・保守に関する安全性の確保が求められる

医療機関における医療機器のサイバーセキュリティ確保のための手引書

- 導入から運用、廃棄までの各段階での対策が示されている
- 特に、EOS機器のリスク評価や、ベンダーとの連携による脆弱性対応が重要視されている

医療情報システムの安全管理に関するガイドライン第6.0版

- 医療機器を含む情報システム全体の管理体制が求められている

制度面からもセキュリティ対策が必須となっており、適切な対策を講じる必要がある

医療機器の技術的対策と脆弱性対応の実践

ソフトウェアのEOS（End of Support）問題と対策

EOSとは

- ソフトウェアベンダーが、特定の製品バージョンに対するサポートを終了すること
- サポートとは、セキュリティアップデートや、バグ修正、技術サポートなどを含む

対象となるソフトウェア

- Windowsなどのオペレーティングシステム（OS）
- SQL Serverなどのデータベースソフトウェア
- 医療機器独自の組み込みソフトウェアなど

ソフトウェアのEOS（End of Support）問題と対策

EOSがもたらすセキュリティリスク

- 修正されない脆弱性
  EOS後、新たな脆弱性が発見されても、ベンダーから修正パッチが提供されないため、既知の脆弱性が放置されることになる
- サイバー攻撃の標的
  修正されない脆弱性は、サイバー攻撃の格好の標的となり、ランサムウェア感染、情報漏洩、機器の誤動作など、甚大な被害につながる可能性がある
- コンプライアンス違反
  医療情報に関するガイドラインや規制要件を満たせなくなる

ソフトウェアのEOS（End of Support）問題と対策

EOSへの対策

- 基本的な考え方としては、可能な限り「更新」または「廃棄」
  - ソフトウェアのアップグレード
  - 医療機器の更新（買い替え）
  - 医療機器の廃棄

ソフトウェアのEOS（End of Support）問題と対策

EOSへの対策

- 継続使用せざるを得ない場合は、リスク軽減策（緩和策）
  - ネットワーク分離
    ファイアウォールでアクセス元を限定、不要ポートの閉鎖、不要なサービスの停止
  - 厳格なログ監視と異常検知
    医療機器や関連ネットワーク機器のログを継続的に収集・分析
    不正アクセスや異常な挙動を早期に検知する体制を構築

ソフトウェアのEOS（End of Support）問題と対策

対応プロセス

- 棚卸しとリスク評価
  院内のすべての医療機器について、OSやソフトウェアのバージョン、EOSの状況、ネットワーク接続状況などを把握し、患者影響度や情報漏洩リスクを評価
- メーカーとの連携
  EOSの状況、今後のサポート方針、アップグレード計画、代替機器について、積極的にメーカーに問い合わせ、情報共有体制を確立
- 対策計画の策定
  リスク評価に基づき、ソフトウェアアップグレード、緩和策の導入、機器の更新など、具体的な対策とスケジュールを策定
- 実行と継続的な見直し
  計画を実行し、定期的に効果を評価し、新たな脅威や状況変化に応じて見直しを行う

脆弱性管理

脆弱性情報の収集と把握

- IPA（情報処理推進機構）
  重要なセキュリティ情報や脆弱性情報、注意喚起などを公開
- JPCERT/CC（一般社団法人JPCERTコーディネーションセンター）
  セキュリティレポートや注意喚起などの形で情報を提供
- JVN（Japan Vulnerability Notes）
  IPAとJPCERT/CCが共同で運営している脆弱性対策情報データベース
- NVD（National Vulnerability Database）
  米国国立標準技術研究所（NIST）が管理・公開している、脆弱性に関する情報を集約したデータベース
- 医療機器製造販売業者からの通知
- セキュリティベンダーからの情報

医療機器だけでなく、サーバー、ネットワーク機器、関連するソフトウェアの脆弱性情報も収集する

脆弱性管理

脆弱性情報の収集

- JVN (Japan Vulnerability Notes)
  https://jvn.jp/
- PC だけでなく産業機器などの脆弱性も幅広く公表されている

JVN Japan Vulnerability Notes

脆弱性レポート 一覧

最新12ヶ月 | 2024年 | 2023年 | 2022年 | 2021年 | 2020年 | 2019年 | 2018年 | 2017年 | 2016年 | 2015年

2025年

2025/09/08 JVN#75307484:
RICOH Streamline NXにおける操作履歴の改ざんにつながる脆弱性

2025/09/05 JVN#98737186:
RATOC RAID監視マネージャー（Windows用）における引用符で囲まれていないファイルパスの脆弱性

2025/09/05 JVN#41633999:
Obsidian GitHub Copilot Pluginにおける重要情報の平文保存の脆弱性

2025/09/05 JVN#35290164:
Androidアプリ「Yahoo!ショッピング」におけるアクセス制限不備の脆弱性

2025/09/05 JVN#48739895:
Pythonライブラリ「TkEasyGUI」における複数の脆弱性

2025/09/05 JVNVU#90284485:
Honeywell製OneWireless WDMにおける複数の脆弱性

2025/09/03 JVNVU#92183348:
Delta Electronics製EIP BuilderにおけるXML外部エンティティ参照（XXE）の不適切な制限の脆弱性

2025/09/03 JVNVU#91978467:
富士電機製FRENIC-Loader 4における信頼できないデータのデシリアライゼーションの脆弱性

2025/09/03 JVN#65839588:
Web Caster V130におけるクロスサイトリクエストフォージェリの脆弱性

2025/09/02 JVN#47404248:
スマートフォンアプリ「グノシー」における送信データへの機微な情報の挿入の脆弱性

2025/09/01 JVN#22016482:
セイコーソリューションズ製SkyBridge BASIC MB-A130におけるOSコマンドインジェクションの脆弱性

2025/08/29 JVNVU#99831542:
コニカミノルタ製bizhubシリーズにおけるサービス運用妨害（DoS）の脆弱性

2025/08/29 JVN#50585992:
複数のiND製品における複数の脆弱性

2025/08/29 JVNVU#91075142:
複数のSchneider Electric製品における不適切な権限管理の脆弱性

脆弱性管理

脆弱性の評価とリスクアセスメント

- 影響度と緊急度の評価
  - CVSS（共通脆弱性評価システム）を用いて客観的に評価
  - セキュリティベンダーなどが解説している情報
  - 患者安全への影響
  - 医療機関の運用に与える影響
- リスク受容の判断
  脆弱性が悪用される可能性、影響の大きさ、対策コストや難易度を総合的に考慮し、どこまで対策を行うか、あるいはリスクを受け入れるかを判断

脆弱性管理

脆弱性への対応策の検討と実施

- パッチ適用・バージョンアップ
  医療機器のファームウェアやソフトウェアの更新プログラムを製造販売業者から入手し、医療機器の稼働状況や診療への影響を考慮したパッチ適用計画と実施
- 設定変更による緩和策
  - 使用していないポートやプロトコルの無効化、不要なサービスの停止
  - 多要素認証の導入や複雑なパスワードポリシーの適用
  - 最小権限の原則に基づいたユーザーアカウント管理とアクセス制限
- ネットワーク分離
  ファイアウォールによりアクセス元を限定、不要ポートの閉鎖、不要なサービスの停止

脆弱性管理

対応状況の追跡と効果の確認

- 脆弱性管理台帳の作成
  発見された脆弱性、評価結果、対応策、担当者、対応状況、完了日などを記録し一元管理
- 定期的なスキャンと診断
  定期的な脆弱性スキャンやペネトレーションテストで、新たな脆弱性の有無や対策の効果を確認
- ログ監視と監査
  医療機器や関連システムから出力されるログを継続的に監視し、不審な挙動や攻撃の兆候がないかを確認
- プロセス改善
  脆弱性管理サイクル全体を定期的に見直し、より効率的かつ効果的なプロセスへと改善

継続的な技術的対策と脆弱性管理が不可欠

脆弱性管理

項目	記載内容	記載例
管理番号	脆弱性を識別するためのID	VT-2025-001
発見日	脆弱性情報が公表された日、または発見した日	2025年9月11日
機器名	脆弱性が存在する医療機器またはシステム名	CTスキャナー (製品名: Alpha-CT Pro)
機器ID	資産管理台帳と紐づく機器の固有ID	MC-12345
ソフトウェア/OS	脆弱性が存在するソフトウェアやOSのバージョン	Windows 10 (バージョン 22H2)
脆弱性情報	脆弱性情報（CVE-ID、JVN-IDなど）	CVE-2025-XXXXX
深刻度（CVSS）	CVSSスコア（例: 7.5）と評価ベクトル	7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
リスク評価	脆弱性が悪用された場合の、患者安全や運用への影響	重大（機器停止リスク、診療への影響大）
対応方針	脆弱性に対して取るべき対策（修正、緩和策、受容）	緩和策（ネットワーク分離）
対応内容	実際に行った対策の詳細	機器を基幹ネットワークから隔離し、アクセス元を保守専用端末に限定
対応状況	対策が完了したかどうかのステータス	完了
完了予定日	対策の完了を計画している日付	2025年10月31日
完了日	対策が完了した実際の日付	2025年10月31日
備考	特記事項や、メーカーとのやり取りなど	メーカーとの協議の結果、機器の買い替えを検討中

脆弱性管理

脆弱性スキャン

- NMAPとは
  ネットワーク上のホストやサービスを検知する、ネットワーク探査ツール
- 主な機能
  - ホスト発見: 特定ネットワーク内の稼働コンピュータの特定
  - ポートスキャン: ターゲットホストの提供サービス調査のための、開放ポートの確認
  - OS検出: ターゲットホストのオペレーティングシステム（OS）の推測
  - バージョン検出: 稼働中ソフトウェアのバージョンの特定

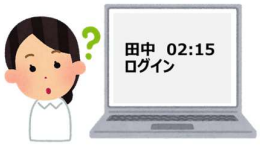
サンプルコマンド　※既知の脆弱性（vulnerabilities）をスキャンします
```
nmap --script vuln x.x.x.x
```

※本ツールは自身の管理外のネットワークやホスト等に使用すると、攻撃行為と判断される場合があります。
不正アクセス禁止法に抵触する恐れもありますので、検証環境や使用が許可されているネットワークの範囲内などで検証してください。

脆弱性管理

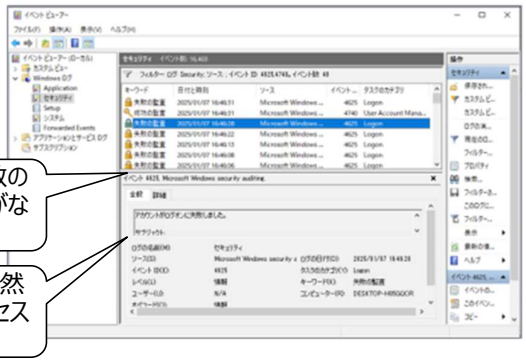
ログ監視と監査

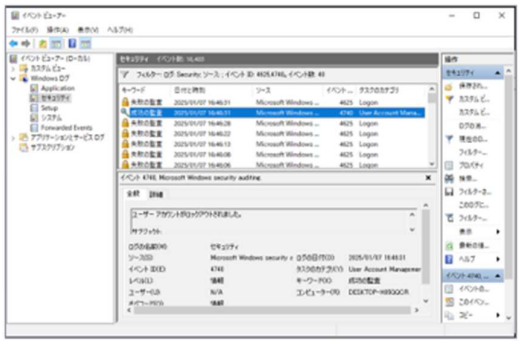
- イベントビューアで確認



短時間で多数のログオン失敗がないか？

深夜など不自然な時間にアクセスがないか？





Event ID	内容	着眼点
4624	ログオン成功	不審なログイン試行、不自然なアクセス時刻、 通常はあり得ないリモートデスクトップ接続
4625	ログオン失敗	
4634	ログオフ	
4776	NTLM認証失敗	NTLMとは、Windowsで利用される認証プロトコルの1つ。現在、より新しい認証プロトコルであるKerberosが主流ですが、場合によっては引き続き使用されています。このイベントは、セキュリティ上の潜在的な問題（不正アクセスやブルートフォース攻撃など）を示している可能性があるため、特に頻繁に発生している場合は注意して調査する必要があります。
4740	アカウントロックアウト	ロックアウト設定を行なっている場合、主要アカウントや同時多発での発生など

サイバーインシデント発生時の医療機器安全確認手順

インシデントの検知と確認

アラートの確認

- ファイアウォールやログ監視システムなどからのアラート、または医療機器の異常動作、ネットワークの遅延、ユーザーからの異常報告などを検知

初期情報の収集

- いつ、どこで、どのような異常が発生しているか（日時、場所、機器名、機種、設置場所など）
- 異常の具体的な内容、症状、発生頻度
- 影響を受けている機器の範囲（単体か、複数か、特定のネットワークセグメントか）
- 異常発生時の状況（電源投入時、特定の操作中、ネットワーク接続時など）
- 異常を検知した人物、その連絡先
- 患者への直接的な影響の可能性（例：治療中の機器、生命維持装置など）

関係者への迅速な連絡と情報共有

インシデント対応チームへの連絡

- 院内情報システム部門、医療機器管理部門、セキュリティ責任者、リスク管理部門など

医療従事者への注意喚起

- 状況と初期対応方法（例：一時的な使用中止、代替機器への切り替え、手動運用への移行など）を速やかに周知し、患者安全を最優先とする行動を促す

関係部署への報告

- 院長、経営層、広報部門などの関係部署にも報告

外部ベンダーへの報告

- 医療機器製造販売業者、セキュリティベンダーなどに連絡をし連携を図る

被害拡大防止のための応急措置

影響範囲の特定と隔離

- 影響を受けている医療機器やシステムを特定し、ネットワークから隔離
- 同じ種類の医療機器や類似の環境にある機器への感染拡大の可能性を評価し、予防的措置を講じる

情報の保全

- インシデント発生時のログ、システムのスナップショット、エラーメッセージなど、後の調査に必要となる可能性のある情報を保全

代替手段の確保

- 影響を受けた医療機器の機能停止に備え、代替機器の使用、手動での運用、診療の継続が可能な体制を検討・確保

サイバーインシデント発生時の医療機器安全確認手順

この安全確認手順は、あくまで一般的なものです。
定期的な訓練（机上演習、シミュレーション）を通じて、個別の医療機関の体制やインシデントの内容に応じて柔軟に調整する必要があります。関係者間の連携を強化し、有事の際に迅速かつ適切に対応できるよう準備しておくことが極めて重要です。

院内で求められる
役割分担と継続的対策

医療機関内の主要部門の役割分担の明確化

情報システム部門、および医療機器安全管理責任者

- ネットワークやシステムのセキュリティ構築・運用
- セキュリティパッチ適用、脆弱性管理の支援
- ログ管理システムの導入・運用
- インシデント発生時の技術的調査と復旧支援

医療従事者（医師、看護師など）

- セキュリティポリシーの遵守（USB持ち込み制限、不審メール報告など）
- 医療機器の異常動作、不審な挙動の早期発見と報告
- インシデント発生時の医療機器使用可否判断への協力

医療機関内の主要部門の役割分担の明確化

医療機器管理部門（CE部門/臨床工学技士部門）

- 医療機器の資産管理（台帳整備、ネットワーク接続状況の把握）
- 医療機器のOS・ソフトウェアバージョンの管理とEOS情報の把握
- 医療機器のセキュリティ設定の実施と管理
- 医療機器製造販売業者との連携（セキュリティ情報入手、アップデート適用調整）
- インシデント発生時の医療機器の安全確認と切り分け

経営層・管理者層

- セキュリティ対策への予算・人員の確保
- セキュリティポリシーの策定と順守の推進
- インシデント発生時の最終的な意思決定と対外説明

部門横断的な連携体制の構築

定期的な連携会議の開催

- セキュリティ状況、課題、対策の進捗状況を共有・議論する会議体を設置
- インシデント発生時の情報共有と連携訓練の実施

インシデント対応計画の策定と訓練

- インシデント発生時の具体的な役割、責任、手順を明記し、全員が理解

共同でのリスクアセスメントと対策検討

- 医療機器の導入時や、既存機器の運用において、セキュリティリスクを共同で評価し、最適な対策を検討

インシデント対応計画と訓練

準備フェーズ

- 連絡体制、緊急連絡先リスト、担当者の役割

検知・分析フェーズ

- ログ監視、異常検知の閾値、初期調査手順

封じ込め・復旧フェーズ

- 医療機器の隔離手順、使用中止基準、代替医療機器の準備、データ復旧手順

事後対応フェーズ

- 原因分析、再発防止策、報告書作成、法規制・ガイドラインへの対応

インシデント対応計画と訓練

定期的なインシデント対応訓練の実施

- 机上訓練
  シナリオを用いたロールプレイング
- シミュレーション訓練
  実際に環境を用いて対応手順を確認
- 訓練結果の評価とインシデント対応計画の見直し

職員へのセキュリティ教育と意識向上

全職員向け

- 一般的なサイバーセキュリティの基本
- フィッシング詐欺対策
- パスワード管理の重要性　など

医療従事者向け

- 医療機器の安全な利用方法
- 患者情報保護の重要性　など

システム・セキュリティ管理者向け

- より技術的なセキュリティ知識
- 最新の脅威動向　など

セキュリティ意識向上のための啓発活動

- 定期的な情報発信
  （セキュリティニュース、注意喚起）
- セキュリティに関する疑問や相談を受け付ける体制の構築

サプライヤー（医療機器製造販売業者等）との連携

医療機器のライフサイクルを通じた連携

- 購入前のセキュリティ要件確認
- セキュリティ情報の共有（脆弱性情報、アップデート情報）
- インシデント発生時の共同対応（ベンダーによる分析支援、パッチ提供）
- EOS時のサポート継続や代替策の相談

契約におけるセキュリティ条項の確認

- セキュリティに関する記述
- サポート期間
- セキュリティアップデートの提供体制　など

まとめ(1/2)

リスクの全体像を理解

- 医療機器は、サイバー攻撃の標的になりうる脆弱性を持つ重要な資産
- ランサムウェアなどによる攻撃は、機器の機能停止やデータ改ざんを引き起こし、診療継続に深刻な影響
- 医療機器に関する制度的枠組み（基本要件基準、ガイドライン）を理解し、「安全性」の確保には「セキュリティ」が不可欠

実践的な対策を実施

- ソフトウェアのEOS問題と対策
- 脆弱性管理
- 継続的な技術的対策と脆弱性管理が不可欠

まとめ(2/2)

院内の連携と継続的な運用体制を確立

- サイバーインシデントはいつ発生するか分からない
  いざという時のために、インシデント対応計画を策定し、訓練を実施
- 関係部門が密に連携し、役割分担を明確にすることが重要
- セキュリティ対策に「終わり」はない
  定期的なリスク評価、職員への教育、サプライヤーとの情報共有を通じて継続的な改善を図る