NIHON KOHDEN

資料４

IoT-SSF 適用実証報告

― 医療機器 ―

日本光電工業株式会社
技術戦略本部 工業会担当
松元恒一郎

2023年 2月 3日：R4
2023年 1月 6日：R3
2022年12月 2日：R2
2022年 7月11日：R1

IoT-SSF の適用の可能性

目的

- 「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）Version 1.0実践に向けたユースケース集」が、医療機器の開発において利用できるか否かを検討し、その差異等を明確にする。
- 医療機器は、CTやMRI等大型となる機器や、弊社で心電計、生体情報モニタ等小型となる機器がある。検討対象は、弊社で開発している心電計、生体情報モニタ、ヘルスソフトウェア、ヘルスITシステムで行う。
- 医療機器の製品寿命の長さを考慮し、利用者区分は事業者、利用環境は製造現場である「Iot-SSFユースケースの2-3-4 化学プラント内の蒸留工程の自動制御」のユースケースとの比較を行う。
- 検討においては、Mitre及びMedical Device Innovation Consortium の「医療機器　脅威モデリング・プレイブック」、FDAの「サイバーセキュリティ市販前ドラフトガイダンス」を参考にする。

IoT-SSF の適用の可能性

医療機器セキュリティのユースケース

医療機器のサイバーセキュリティ

- 医療機器では、まず、**第一に（患者）安全**を目的としてリスクマネジメントを実施する。経済的影響とは異なり、他の分野とは若干異なる。
- 医療機器といっても多種多様であるため、対象の医療機器を特定した上で、脅威モデリングを行う。
  1. 意図する使用及び意図する使用環境を確認する。
     例えば救命救急室で使用する医療機器で認証の階層を複雑にすれば、緊急時の操作が煩雑になり、患者の治療・診療が遅れて、支障をきたすことになる等意図する使用、使用環境を十分考慮する必要がある。
  2. どんな脅威があるかを脅威モデルを使って分析する。
  3. 脅威のシナリオに対策を立てて、リスクが許容できるかどうかを検討する。
  4. 脅威モデルを評価する。
  5. 脅威モデリング後、テストによって検証し、リスクが許容できていることを証明する。

脅威モデリングについては、次ページに紹介する「医療機器 脅威モデリング・プレイブック」に、仮想の医療機器3種に対する事例が紹介されている。

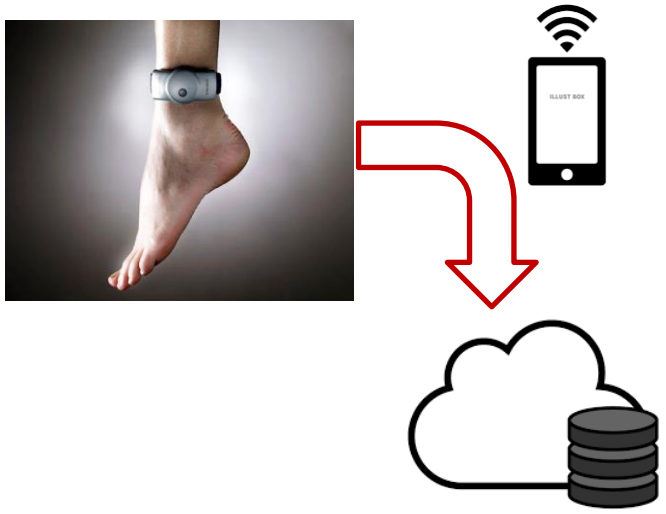
3つの仮想医療機器の脅威モデリングの例

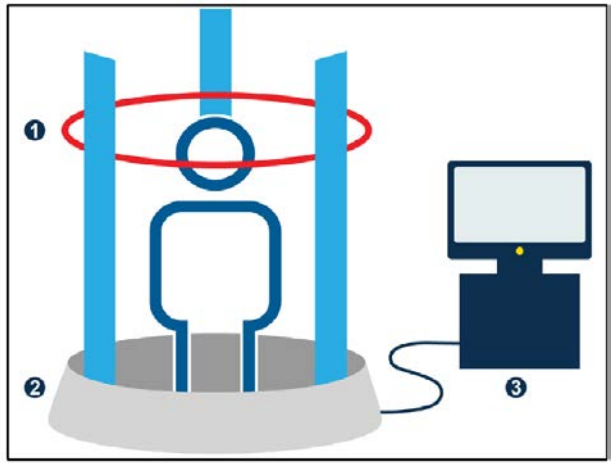
- 医療機器 脅威モデリング・プレイブックでは、脳卒中のリスクがある患者向けの3つの仮想医療機器で脅威モデリングを行っている。

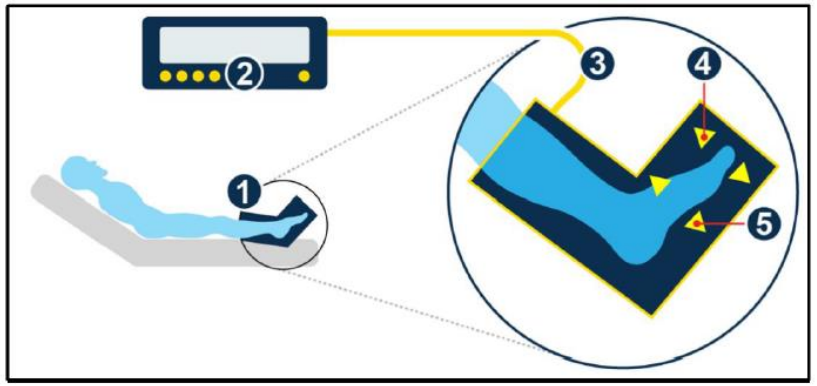
AMPS(Ankle Monitor Predictor Stroke)
夜間や休憩中に脳卒中のリスクがある患者のくるぶしに取り付けて使用する家庭用医療機器。1～3ヶ月装着。医療の専門家が後に分析できるように医療計測値を収集する。

SNAP(Stroke Nerve-Affective Photography)
脳卒中のリスクがある患者や脳卒中からの回復途上の患者が使用する医療用診断装置。

SKATE(Stroke Kinematic Ankle and Toe Exerciser)
脳卒中のリスクがある患者や脳卒中からの回復途上の患者が使用する治療用医療機器。



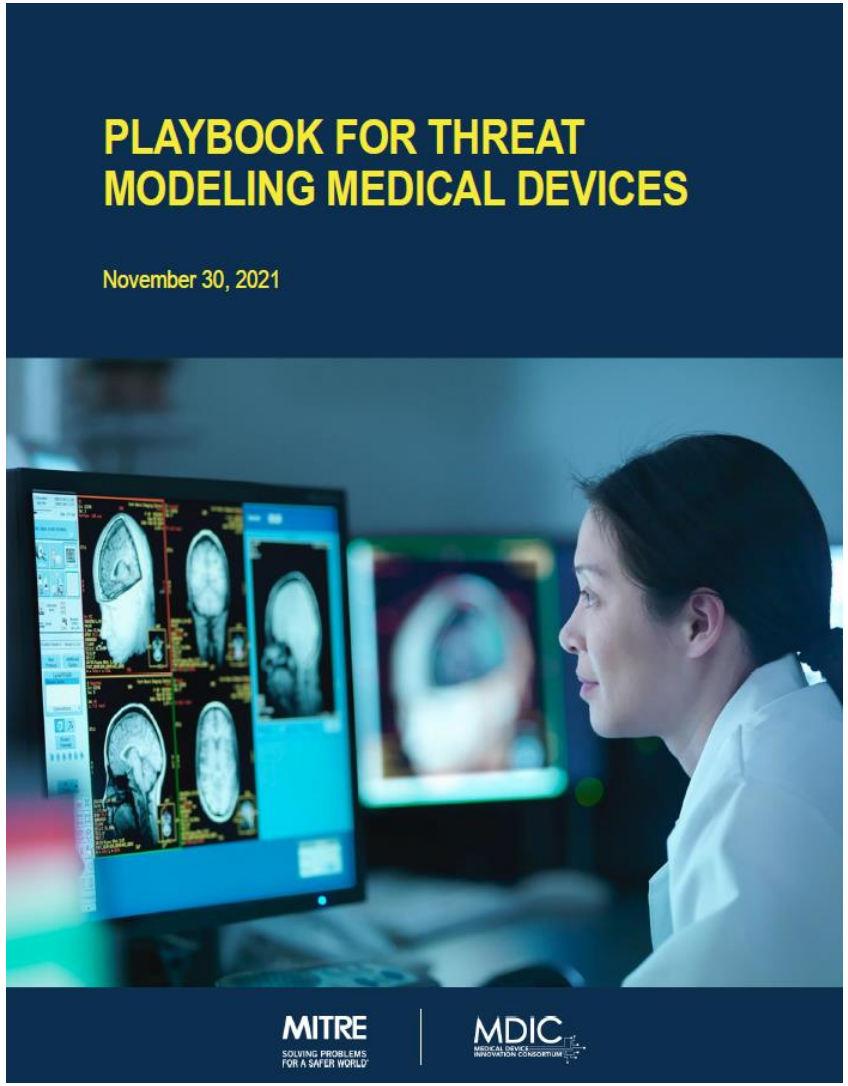




なぜ、脅威モデリングが必要なのか？

- **脅威モデルがないと、具体的にどんな脅威があるのか分からない。（リスク分析を深められない）**
  - 悪意の可能性は無限にあるので、システムやサービスを理解し、どんな脅威の可能性があるのかシナリオを想定する必要がある。
  - あらゆる状況に当てはまる万能のアプローチ（セキュリティ対策）は存在しないため、有効な対策をするために脅威モデルがいる。
- **脅威モデリングによって、システムがどのように機能するかを表し、リスク対策が正当であることを示しながら、システムに対する残りの脅威を識別して、どのような脅威の軽減が行われているかと説明する。**
  - 医療機器の安全性や有効性が保たれることを規制当局やユーザに理解・納得してもらうためには、医療機器製造業者が想定した脅威モデルを使って説明し、テストによって検証されたことを示す。
- **脅威モデリングは市販開発段階だけでなく、市販後保守段階でも利用される。**
  - 市販後に発見された脆弱性や実際に発生したセキュリティインシデントを評価する際にも脅威モデルは使用される。

医療機器 脅威モデリング・プレイブック

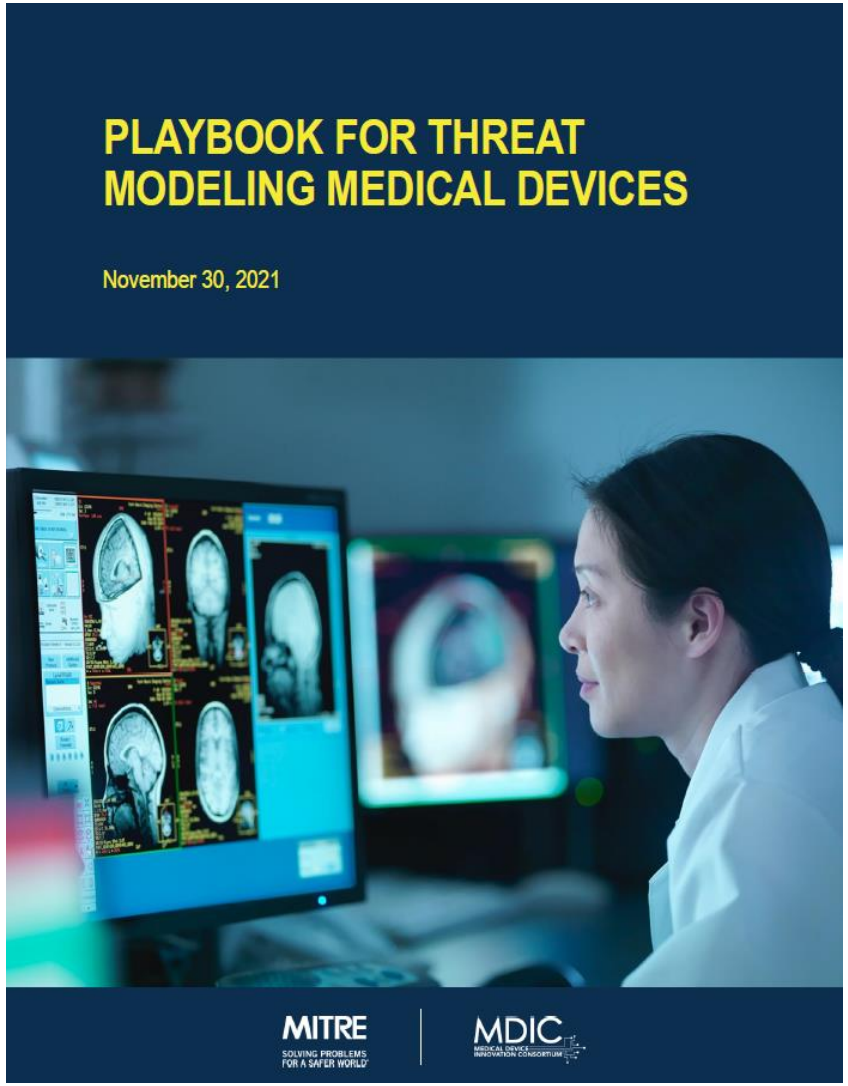


2021年11月30日発行

FDA提供の資金を使い Mitre 及び Medical Device Innovation Consortium が作成した。
Mitre 、MDICだけでなく、FDAや各医療機器メーカのメンバーが脅威モデリングブートキャンプを実施し、ブートキャンプでの収穫を元にしてこのプレイブックが作成された。

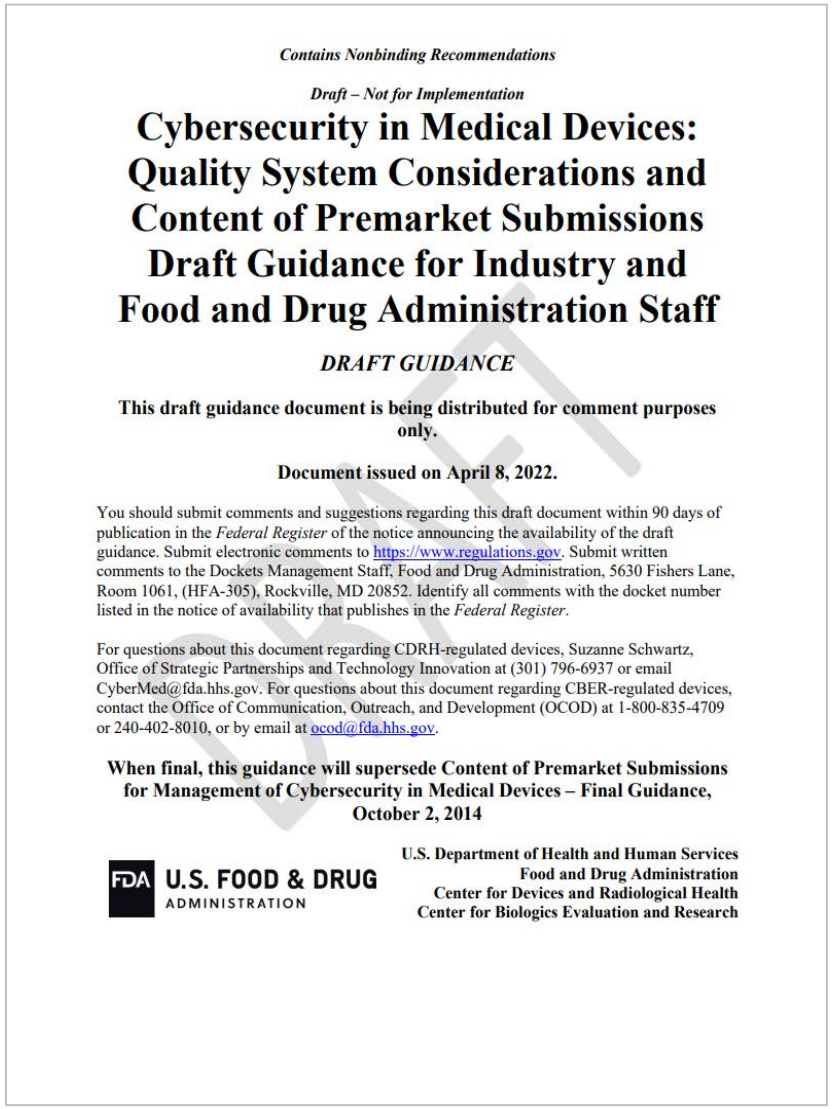
目次

プレイブックは、次のような目的で利用することができる



- 製品開発のマネージャが、脅威モデリングが既存の開発プロセスにどのように適合するかを理解できるようにする。
- システム・エンジニアが、脅威モデリングが設計要件に対してどのように影響するかを理解できるようにする。
- 設計者とアーキテクトが、脅威モデリングが設計にどのように影響するか理解できるようにする。
- 検証及び妥当性確認エンジニアが、テスト戦略において脅威モデルをどのように使えば良いか理解できるようにする。
- レギュレトリ-スペシャリストが、脅威モデルを規制当局にどのように紹介し記述すれば良いかを理解できるようにする。
- 脅威モデリングの経験に少ないメーカーが経験豊富なコンサルタントと契約できるようにする。

FDA サイバーセキュリティ市販前ドラフトガイダンス



Contains Nonbinding Recommendations

Draft – Not for Implementation

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on April 8, 2022.

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document regarding CDRH-regulated devices, Suzanne Schwartz, Office of Strategic Partnerships and Technology Innovation at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

FDA サイバーセキュリティ市販前ドラフトガイダンス
2022年4月8日発行

目次

SPDF：Secure Product Development Framework

FDA サイバーセキュリティ市販前ドラフトガイダンスが求める「脅威モデリング」

- FDA は 市販前申請時に、システムのために実施されたサイバーセキュリティのリスク評価とリスクコントロールが、安全性及び有効性にどのように対処しているのかを実証するために脅威モデリング文書を含めることを推奨する。

1. どのようなシステムなのか。
2. どんな脅威が想定されるのか。
3. それらの脅威に対してどのような対策を取っているのか。
4. 医療機器の安全性や有効性は保たれるか。

脅威モデリングの手順-1

- **意図する使用及び意図する使用環境を確認する。（1. 設計対象は何か？）**
  - 事前に患者危害を想定したリスク分析を実施しているという前提で、基本性能や基礎安全が何なのかを確認しておく。
  - その上で、システムの全体像を描く。（どのようなI/Fを持っているのか。ネットワークに繋がるのか。付帯サービスは何か）
    - システム全体をデータフロー図で記載し、信頼境界がどこにあるのかを記載する。
  - システムの詳細を分析し、図示した上で、状態遷移図やシーケンス図を描いて、機器やシステムがどのように使われるのか、どのようなサービスを提供するのかを説明する。
- **どんな脅威があるかを脅威モデルを使って分析する。（2. どんな脅威があるのか？）**
  - データフロー図の各要素に対してSTRIDEなどを使って、脅威のシナリオを作成する。
  - アタックツリーを描いて、脅威によってどのような危害に至る可能性があるかを分析する。

脅威モデリングの手順-2

- 脅威のシナリオに対策を立てて、リスクが許容できるかどうかを検討する。（3. 発生する脅威に対して何を行うのか。）
- 脅威モデルを評価する。（4. 分析はどの程度うまくいったか？）

脅威モデリング後、テストによって検証し、リスクが許容できていることを証明する

IoT-SSF の適用の可能性

医療機器のユースケース

ユースケース事例（プラント）とヘルスソフトウェアの違い

2-3-4 化学プラント内の蒸留工程の自動制御のユースケースとヘルスソフトウェアの手順の違い

1. L1272 ①対象ソリューションの概要、L1284 ②ステークホルダ関係図、L1321 ③システムを構成する機器の一覧、L1324 ④システム構成図、データフロー図
   - a. 及び b. の一部に相当する。（似ている）
   - a. には守るべき情報資産を定義することが含まれる。（似ていない？）
2. L1340 ⑤リスク基準、L1357 (2)リスクアセスメント
   - e に相当 （リスク評価基準が異なる）
   - ステークホルダは、患者、医療従事者、医療情報システム
     ユースケースが異なるので当然
   - 個人情報保護が重要視される。
3. L1456 B)発生したインシデントの経済的影響の度合い
   - d, e に相当。
   - 医療情報システムに停止は、経済的影響以上に、患者や地域住民に対して社会的信用を低下させる。
   - ISO 14971 では、危害の重大度　× 発生確率（悪用可能性） にて評価するが明確化されている。
4. L1536 表26 想定される脅威
   - 想定される脅威は、脅威モデリングによって分析される。
   - どの脅威が、具体的にどのような危害に至る可能性があるのかを、医療機関や規制当局に脅威モデルを使って説明しなければいけない。

ヘルスソフトウェアにおけるセキュリティマネジメントの手順

a. 意図する使用及び意図する使用環境を確認する。
b. どんな脅威があるかを脅威モデルを使って分析する。
c. 脅威のシナリオに対策を立てて、リスクが許容できるかどうかを検討する。
d. 脅威モデルを評価する。
e. ISO 14971 に基づき リスク分析をする。
f. 脅威モデリング後、テストによって検証し、リスクが許容できていることを証明する。

青字が、2-3-4 のユースケースと類似している点。
赤字が、ヘルスソフトウェアのセキュリティリスクマネジメントの手順と異なる = 似ていないと思われる点。

注：L****は、「04_【資料4】IoTセキュリティ・セーフティ・フレームワークVersion 1.0 実践に向けたユースケース集_set.pdf」の行番号を示す。

ユースケース事例（プラント）とヘルスソフトウェアの違い

ヘルスソフトウェアにおけるセキュリティマネジメントの手順

a. 意図する使用及び意図する使用環境を確認する。
b. どんな脅威があるかを脅威モデルを使って分析する。
c. 脅威のシナリオに対策を立てて、リスクが許容できるかどうかを検討する。
d. 脅威モデルを評価する。
e. ISO 14971 に基づき リスク分析をする。
f. 脅威モデリング後、テストによって検証し、リスクが許容できていることを証明する。

ISO 14971（JIS T 14971）：
医療機器としてのソフトウェア及び体外診断用医療機器を含む医療機器のリスクマネジメントの用語、原則及びプロセスについて定めており、今回の規格改正 ISO 14971:2019（JIS T 14971:2020）によって、関連するJIS T 0063:2020（ISO/IEC Guide 63:2019）との整合性を図るために用語及び定義を追加し、関連する図を全面的に見直しいる。また、セキュリティなどの新たな技術分野及び医療機器の使用環境などの変化に合わせた改正となっている。

ISO/IEC Guide 63:2019：
医療機器の国際規格への安全側面の開発及び組入れのためのガイド
この文書は、確立されたリスク管理の概念と方法論に基づいて、国際規格に安全性に関連する側面を含めることに関する要件と推奨事項を医療機器規格の作成者に提供する。人、財産の安全性に関連するあらゆる側面に適用できる。

ユースケース事例（プラント）とヘルスソフトウェアの違い

2-3-4 化学プラント内の蒸留工程の自動制御のユースケースとヘルスソフトウェアの手順の違い

1. L1272 ①対象ソリューションの概要、L1284 ②ステークホルダ関係図、L1321 ③システムを構成する機器の一覧、L1324 ④システム構成図、データフロー図
   - a. 及び b. の一部に相当する。（似ている）
   - a. には守るべき情報資産を定義することが含まれる。（似ていない？）
2. L1340 ⑤リスク基準、L1357 (2)リスクアセスメント
   - e に相当 （リスク評価基準が異なる）
   - ステークホルダは、患者、医療従事者、医療情報システム
     ユースケースが異なるので当然
   - 個人情報保護が重要視される。
3. L1456 B)発生したインシデントの経済的影響の度合い
   - d, e に相当。
   - 医療情報システムに停止は、経済的影響以上に、**患者**や地域住民に対して社会的信用を低下させる。
   - ISO 14971 では、危害の重大度　× 発生確率（悪用可能性） にて評価することが明確化されている。
4. L1536 表26 想定される脅威
   - 想定される脅威は、脅威モデリングによって分析される。
   - どの脅威が、具体的にどのような危害に至る可能性があるのかを、医療機関や規制当局に脅威モデルを使って説明しなければいけない。

青字が、2-3-4 のユースケースと類似している点。赤字が、ヘルスソフトウェアのセキュリティリスクマネジメントの手順と異なる = 似ていないと思われる点。

注：L****は、「04_【資料4】IoTセキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集_set.pdf」の行番号を示す。

医療機器のセキュリティリスク分析との比較

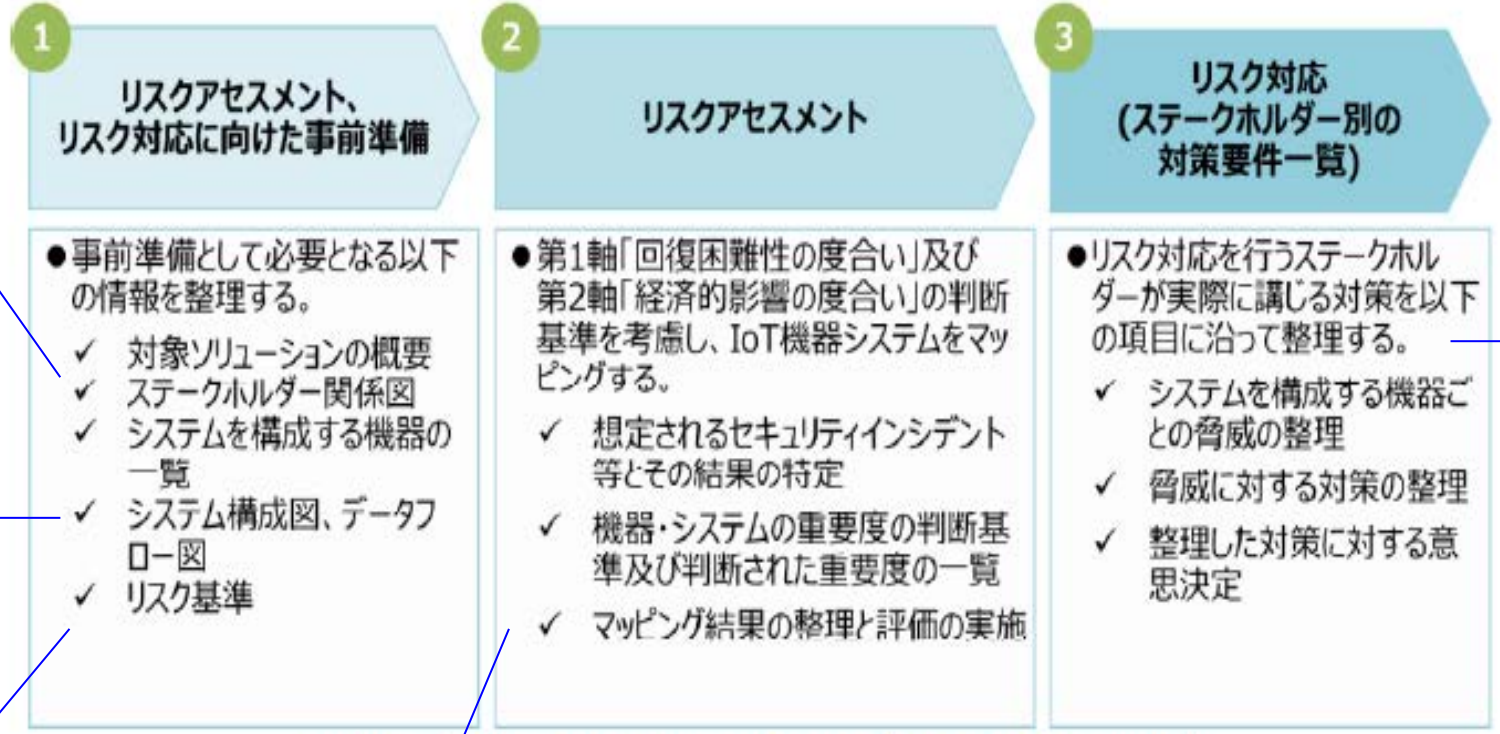
ヘルスソフトウェア、ヘルスITシステムのセキュリティリスク分析は、ISO 24971:2020 Annex F に基づき実施する。

ISO/TR 24971:2020
医療機器ーISO 14971
の適用の指針

ステークホルダは、「患者」「医療従事者」「病院関係者」等に集約される。

脅威モデリングにより、データフロー図、シーケンス図、アタックツリー、状態遷移図等を作成する。データフロー図には信頼境界を記載する。

リスク基準は基本はISO 14971 によって概念が決められている。危害の重大度×危害の発生確率（悪用可能性）



脅威の評価は、リスクアセスメントのプロセスで実施する。脅威に対する対策の是非は、リスクの受容判定にて判断する。

危害の重大度×危害の発生確率を、対策前と後で評価し、リスクを受容できるかどうかを判定する。

IoT-SSF の適用の可能性

まとめ

- 「Iot-SSF）Version 1.0 実践に向けたユースケース集」が、医療機器の開発において利用できるかを検討した。
- その際、Iot-SSFユースケースの2-3-4 化学プラント内の蒸留工程の自動制御のユースケースとで比較を行った。
- 検討の結果、医療機器として第一に考慮する（患者）安全を目的としている点やリスク基準で、主として経済的な影響を考慮している「Iot-SSF）Version 1.0 実践に向けたユースケース集」をそのまま適用することは出来なかった。
- しかし、対象ソリューションの概要、ステークホルダ関連図、システム構成図など各項目においては医療機器の特性を考慮に入れることで利用出来るのではないかと考える。

IoT-SSF の適用の可能性

出典

出典：医療機器 脅威モデリング・プレイブック
https://www.mitre.org/publications/technical-papers/playbook-threat-modeling-medical-devices

参照：FDA サイバーセキュリティ市販前ドラフトガイダンス
https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

22