
**ANSI/NEMA HN 1-2019**

# *American National Standard—*
# *Manufacturer Disclosure Statement for*
# *Medical Device Security*

## *医療機器セキュリティのための製造業者開示説明書*

*発行元*

**National Electrical Manufacturers Association**
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

# 通知及び免責条項

この出版物での情報は、開発当時は、文書の開発及び承認に従事していた人のコンセンサスによって技術的に正常であると考えられた。コンセンサスは、この文書の開発に参加するすべての人による満場一致を必ずしも意味しない。

National Electrical Manufacturers Association（NEMA）規格及びガイドライン出版物は、自発的なコンセンサス規格開発**プロセス**を通じて開発されている。本書もその一つである。この**プロセス**ではボランティアを集め、この出版物の対象となるトピックに関心をもつ人の見解を求めている。NEMA は**プロセス**を処理し、コンセンサスの開発での公平を促進する規則を確立するが、文書の執筆はしない。また、NEMA は、規格とガイドライン出版物に含まれる情報の正確さ若しくは完全性、又は判断の健全性について、独立して試験、評価又は確認を行わない。

NEMA は、特別、間接、必然か補償かにかかわらず、直接的又は間接的にこの出版物、この文書の使用、適用又は依存に起因する身体傷害、財産又は他の損害に対し免責とする。NEMA は、明示か黙示かを問わず、ここに出版された情報の正確さと完全性について免責とし保証はしない。またこの文書中の情報が読者の特定の目的又はニーズを満たすことは免責とし保証はしない。NEMA は、個々の製造業者又は販売業者の製品又は役務の性能を、この規格又はガイドにより保証するものではない。

この文書を出版し利用可能にする際に、NEMA は、個人又は組織のために、又はそれらを代表して専門的その他の役務を与えるものではない。また NEMA は個人又は組織が他の者に対し負う義務を行うものではない。この文書を使用する人は誰でも、自分自身の判断に頼ることが望ましい。又は、適切な場合、所定の状況での合理的な医療行為を決定する際に有能な専門家に対し助言を求めるほうがよい。この出版物の対象のトピックについての情報及び他の規格は、他の情報源から入手できることがある。この出版物の対象でない追加の見解又は情報を求めて、ユーザは他の情報源を調べる必要がある。

# 目次

## 前文

医療機器セキュリティのための製造業者開示説明書（MDS2）は、医療機器内に組み込まれたセキュリティおよびプライバシー対策機能に関する標準化された情報を提供することにより、医療提供組織内のセキュリティリスクマネジメントを支援することを目的としている。MDS2は、業務上のセキュリティ計画へのインプットとして最もよく使用される。すべてのセキュリティ機能がすべての機器に適切でない場合がある。医療機器製造業者及び医療提供者は、基本的な安全性、基本性能、使用する環境及び補完的管理策によるリスクを管理する能力に基づき、各セキュリティ機能の適切性を評価する必要がある。MDS2 は、機器の設計仕様に基づく機能及び能力を開示する。サービスプロセス、サポートコミットメント、またはビジネス契約を通じてより適切に対処されるその他のビジネス活動については説明しない。

MDS2 は、患者ケアの安全かつセキュアな提供が医療機器製造業者と医療提供者間で共有される責任であることを認識した上で、透明性をもって製造業者によって提供される。医療機器製造業者は、市販されている機器に安全かつセキュアな操作を可能にするための業界標準のセキュリティ対策が含まれていることを保証する。医療提供者は、その環境内での業務上のセキュリティに責任を負う。

## まえがき

この文書は、医療機器セキュリティのための製造業者開示説明書（MDS2 書式）及びこの書式の記入方法の説明を示す。MDS2 の目的は、医療機器に関連するサイバーセキュリティリスクの評価を支援する重要な情報を医療提供者に提供することである。この文書は、医療機器に関わるセキュリティリスクアセスメントプロセスの要素にのみ焦点をあてており、組織全体にわたるセキュリティリスクアセスメントのインプットとして利用できる。標準化した書式には次の利点がある。1）製造業者は、製造する医療機器のセキュリティ関連の特徴に関し、医療提供者から大量の情報要求を受けたとき、迅速に回答できる。そして、2）医療提供者は、セキュリティ関連の大量の情報を製造業者から提供されたとき、迅速に検討できる。

製造業者が記入した MDS2 書式は次のようにすることが望ましい：

a. 世界中の医療提供者にとって有用である。記載する情報は、効果的な情報セキュリティのリスクマネジメントプログラムを持ちたいと熱望するすべての医療提供者にとって有用である。

b. 個々の機器モデル及びバージョンの技術的なセキュリティ関連属性に関する機器固有の情報を含んでいる。

c. 医療提供者（機器ユーザ/操作者）が医療機器情報セキュリティ（すなわち機密性、完全性、可用性）のリスクアセスメントを始めるために必要とする、共通で典型的な情報の技術的な機器固有の要素を集める簡単で融通のきく方法を提供する。

**注意事項—MDS2 書式は医療機器調達の唯一の根拠ではないし、かつ根拠としないほうが望ましい。調達仕様書を書くには、セキュリティ環境と医療の使命についてより深く、より広範な知識が必要である。**

医療提供者の学際的な**リスクアセスメント**のチームは、製造業者が MDS2 書式で提供する情報を、ケアデリバリ環境（例：ACCE, American College of Clinical Engineering/ECRI の *Guide for Information Security for Biomedical Technology* を通じて）について集めた情報を一緒に使用し、集積情報を検討して、ローカルのセキュリティマネジメント計画の実行を決定できる。

この書式は、元来 ACCE/ECRI Biomedical Equipment Survey Form に適合し、*Information Security for Biomedical Technology: A HIPAA* Compliance Guide*(ACCE/ECRI,2004)の主要なツールであった。この書式は元々、2004 年に「MDS2 v.1.0(2004-11-01)」として公表され、2008 年に HIMSS/NEMA 合同規格「HIMSS/NEMA Standard HN 1-2008」として公表された。

2010 年には、International Electrotechnical Commission standard IEC 80001-1, *Application of risk management for IT-networks incorporating medical devices* が出版された。**医療機器**の IT-ネットワークへの**リスクマネジメント**の適用を扱い、**リスクマネジメント**のために必要な役割、責任、活動を提供している。2012 年に、IEC 80001 への技術報告書（TR）サプリメントが、IEC / TR 80001-2-2 *Guidance for the communication of medical device security needs, risks and controls* として発表された。このサプリメントでは、**医療機器**の**セキュリティ機能**や IT コンポーネントの 19 のセキュリティ機能が定義されている。19 の高レベルの**セキュリティ機能**は、「ベンダーと購入者または医療機器 IT ネットワークプロジェクトに関わる利害関係者の大きなグループ間での、セキュリティ中心の議論の出発点であることを意図している」。

この目標は密接に MDS2 イニシアチブの第一の目的と一致しているため、NEMA は、IEC/TR 80001-2-2 の 19 セキュリティカテゴリに合わせるために、製造業者が提供する MDS2 情報の拡張と再カテゴリ化を実施している。IEC/TR 80001-2-8 は、各セキュリティ機能に対処し、医療提供者および製造業者による検討のためのセキュリティマネジメントを特定する。

2017 年、NEMA は、文書の機能性をさらに改善し、技術の進歩を取り入れるために、2013 MDS2 の改訂を開始した。また、サイバーセキュリティの知識の改善と、医療提供者のセキュリティリスクマネジメント方法の向上におけるサイバーセキュリティの重要性の増大を把握することも目的とする。

NEMA は MDS2 形式の情報は、各組織のセキュリティコンプライアンスと**リスクアセスメント**の一環として使用されることを推奨している。この規格出版の準備においては、**ユーザ**と他の関係者の意見を求め、評価されている。

質問、コメント、改正提案、改正勧告は、下記宛先の NEMA 製品サブディビジョンに提出して欲しい。

Technical Director, Operations
National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

# セクション1 - 一般

## 1.1 適用範囲

MDS2 書式で提供される情報は、セキュリティのリスクアセスメントプロセスに責任をもつ専門家が、**医療機器**のセキュリティ機能の管理を支援することを目的としている。MDS2 書式で提供される情報は、その他の目的を意図せず、その他の目的には不適切かもしれない。

### 1.1.1 セキュリティマネジメントプロセスにおける医療提供者の役割

医療提供者は、効果的なセキュリティマネジメントを確立することに最終的責任をもつ。

医療情報セキュリティを有効に管理し、関連規制に適合するために、医療提供者は**管理的**、**物理的**、及び**技術的な保護手段**を使用しなければならない—それらは、実際の**機器**にとっては外部的なものが大多数である。

例えば、医療提供者は、セキュリティマネジメントプログラムを作成する際に、以下の活動の一部が含まれる場合がある。

a. 製造業者の機器によって保存/通信するデータの種類を決定する。
b. 製造業者の機器に組み込まれたすべてのセキュリティ関連機能のリストを入手し、どの機能が望ましいか、どのように設定するかを文書化する。
c. 特定の識別タグを含め、製造業者の機器と通信するすべての機器およびアプリケーションを特定し、文書化する。
d. 製造業者の機器を含む、レジリエンスおよび復旧計画を文書化する。

### 1.1.2 セキュリティマネジメントプロセスにおける医療機器製造業者の役割

製造業者が**医療機器**セキュリティに及ぼし得る最大の影響は、効果的なセキュリティプログラムを維持し、関連する規制の要求事項及び/又は規格を満たす医療提供者の努力を容易にするために、**機器**に**技術的保護手段**（すなわちセキュリティ機能）を組み入れることである。**医療機器**製造業界は、有効なセキュリティ機能性を**機器**にもたせることは重要であるとの認識を深めている。製造業者は、医療提供者のニーズ及び要求事項に基づき新しい**機器**を生産するとき、そのようなセキュリティ関連の要求事項を一般には含めている。

**機器**製造業者は、医療提供者がセキュリティマネジメントプログラムを進めるとき、下記情報の提供により医療提供者を支援できる：

a. 製造業者の機器が保存/通信するデータのタイプ；
b. 製造業者の機器がデータを保存/通信する方法；
c. 製造業者の機器に内蔵されるセキュリティ関連の機能。

## 1.2 参考文献

さらなる読解、裏付け資料、及び関連する文献として勧められるものとして以下の参考文献に記載されている。

*Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities,* IEC 80001-1:2010

*Application of risk management...-- Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples,* IEC 80001-2-1:2012

*Application of risk management...-- Part 2-2: Guidance for the communication of medical device security needs, risks and controls,* IEC/TR 80001-2-2:2012

*Application of risk management for IT-networks incorporating medical devices -- Part 2-8: Application guidance -- Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2, IEC/TR 80001-2-8:2016*

*Health Insurance Portability and Accountability Act of 1996* (HIPAA), Pub. L. 104-191 (USA)

*Health Insurance Reform: Security Standards; Final Rule,* 45 CFR pts.160, 162, 164 (USA, 2003).

*General Data Protection Regulation (GDPR) (EU) 2016/679*

*個人情報保護法改正（日本、第 2 版、2016 年 12 月）*

*Personal Information Protection and Electronic Documents Act* (PIPEDA), Statutes of Canada, 2000.

*Deciding When to Submit a 510(k) for a Change to an Existing Device,* US FDA, 2017*The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)],* US FDA, 2014

*ISO-19770-2 Information technology -- Software asset management -- Part 2: Software identification tag*

*NISTIR 8060, Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*

*NIST Special Publication 800-121, Guide to Bluetooth Security*

*ISO/IEC 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices*

*NIST SP 800-53 Rev 4*

*ISO 27002:2013*

*ISO/TR 11633-1:2009 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 1: Requirements and risk analysis*

*ISO/TR 11633-2:2009 Health informatics -- Information security management for remote maintenance of medical devices and medical information systems -- Part 2: Implementation of an information security management system (ISMS)*

### 1.3 定義

これらの定義は本文書内でのみ使用する。法的定義は、地域の管轄権によって異なる場合がある。用語が元資料と同一である場合、又は元資料から変更されている場合、これらの情報源を特定する。

1.3.1 **管理上の保護手段**： 個人識別可能情報を保護するためのセキュリティ手段の選択、開発、実施及び維持を管理し、並びにその情報の保護に関する組織の行動を管理する、管理措置、方針及び手続き。（出典：HIPAA セキュリティ規定より抜粋）

1.3.2 **マルウェア対策ソフトウェア**： IT システムおよび個々のコンピュータ機器上の悪意のあるソフトウェア（マルウェア）を予防、検出、または削除するために設計されたソフトウェアプログラムの一種。（出典：techtarget.com）。

1.3.3 **アプリケーションのホワイトリスト**：アプリケーションホワイトリストとは、明確に定義されたベースライン（出典：NIST SP800-167）に従ってホストに存在する、またはアクティブであることが許可されているアプリケーションおよびアプリケーションコンポーネント（ライブラリ、設定ファイルなど）のリスト。

1.3.4 **監査**： データセキュリティ及びデータ完全性手順の妥当性及び有効性を試験し、確立された方針及び業務手順の遵守を保証し、必要な変更を勧告するために、システム記録及び業務の独立したレビュー及び検討を実施すること。（出典：IEC62351-2,ed.1.0）

1.3.5 **監査ログ**： システムへのアクセス及び一定期間に実施された操作の記録を含むシステム活動の時系列記録。（出典：Indian Health Manual ; https://www.ihs.gov/ihm/）

1.3.6 **認可**： システムリソースにアクセスするためにシステムエンティティに付与される権限または許可。（出典：IEC62351-2,ed.1.0）

1.3.7 **認証**： 多くの場合、情報システム内のリソースへのアクセスを許可するための前提条件として、ユーザ、プロセス、または機器の識別情報を検証する。（出典：IEC62351-2,ed.1.0）

1.3.8 **生体データ**：個人の身体的な特徴又は反復可能な行動（例：掌紋、網膜スキャン、虹彩スキャン、指紋パターン、顔の特徴、DNA シーケンス特性、声紋、手書きの署名）の測定から人間を識別する。（出典： MDS2-2013）

1.3.9 **補完的管理策**： サイバーセキュリティの補完的管理策とは、機器の製造業者によって設計された対策の代わりに、または対策がない状態で作成される保護手段または対策である。これらの対策は、現場で設定可能な機器設計の外部であり、ユーザが使用し、医療機器の補足的または同等のサイバー保護を提供する。（出典：FDA 市販後ガイダンス 2016）

1.3.10 **クレデンシャル**：ユーザ名やパスワードなど、ユーザを認証するために提供される入力。（出典：カスタム定義）。

1.3.11 **データおよびシステムセキュリティ**：情報資産（データおよびシステム）が機密性、完全性、可用性の劣化から合理的に保護される医療 IT ネットワークの運用状態（出典：IEC80001-1:2010,definition 2.5.）

1.3.12 **非識別化**： 一連の識別データとデータ対象者との関係を削除するプロセスの総称。（出典：ISO/TS25237:2017）

1.3.13 **機器**： ハードウェア、ファームウェア及び/又はソフトウェア（のみ）等を含む製品/システム。本 MDS2 文書での「機器」は、文脈から他の明確な意味の場合を除き、MDS2 書式において製造業者が対応する医療機器（製造業者の製品）を指す。医療機器も参照のこと。（出典：カスタム定義）

1.3.14 **動的アプリケーションセキュリティ試験（DAST）**： 潜在的なソフトウェア脆弱性を検出するためのアプリケーションセキュリティのテストを可能にするプラットフォームオプション。（出典：カスタム定義）

1.3.15 **電子メディア**： コンピュータ内の記憶装置（ハードドライブ）および磁気テープやディスク、光学ディスク、デジタルメモリカードなどのリムーバブル/移動可能なデジタル記憶メディアを含む電子記憶メディア;例えばインターネット（ワイドオープン）、エクストラネット（インターネット技術を使用して、ビジネスと協力関係者のみがアクセスできる情報とをリンクさせる）、専用回線、ダイアルアップライン、プライベートネットワークなど、すでに電子記憶メディアにある情報を交換するために使用される伝送メディア、およびリムーバブル/伝送可能な電子記憶

メディアの物理的移動。特定の通信、例えばファクシミリによる紙及び電話による音声の伝送は、電子メディアによる通信とはみなされない。なぜならば交換される情報が通信前には電子メディアの形で存在していないからである。（出典：HIPAA より抜粋）

1.3.16 **保護対象電子医療情報（ePHI）**：電子形式で提供される保護医療情報（PHI）。（出典：カスタム定義）

1.3.17 **緊急アクセス**： 緊急時または救急時に機器ユーザが意図した機能に迅速かつ容易にアクセスできるプロセスまたはメカニズムで、確立されたアクセスコントロールを迂回する;医療機器への即時アクセスを必要とする緊急事態が発生した場合に、機器ユーザが意図した機能にアクセスする能力。（出典：AAMI TIR57:2016）

1.3.18 **危害**： 人の身体的傷害もしくは健康被害、または、財産もしくは環境の損害、または、有効性の低下、もしくはデータおよびシステムセキュリティの侵害。（出典：IEC80001-1：2010、定義 2.8） 注記： *この定義は、一部の規制上の定義よりも拡張的である。*

1.3.19 **意図する使用**： 製造業者が提供する仕様書、説明書及び情報に従って製品、工程又はサービスが意図されている使用。（出典：ISO14971:2007, *Application of risk management to medical devices,* definition 2.5）。

1.3.20 **マルウェア**： システムに、通常は隠れて挿入されるプログラムで、データ、アプリケーション、オペレーティングシステムの機密性、完全性、可用性を危険にさらす、又はそれらの動作を妨害する、または邪魔することを目的とする。（出典：NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*）

1.3.21 **医療機器**： 計器、器械、用具、機械、器具、インプラント、体外診断薬又は測定器、ソフトウェア、物品、その他これらに類するもの又は関連するもので以下に該当するもの：

a. 以下の特定の目的の 1 つ又は複数のために人体に対して単独で、又は組み合わせて使用することが製造業者によって意図されているもの：
    1. 疾病の診断、予防、監視、治療、又は緩和、
    2. 負傷の診断、監視、治療、緩和又は補助
    3. 解剖学的又は生物学的なプロセスの検査、代替、修復、又は支援
    4. 生命支援又は維持
    5. 受胎調整
    6. 医療機器の消毒
    7. 人体から得た検体の体外検査により、医療又は診断目的の情報を提供する
b. 人体の体表及び体内への主な作用を、薬学、免疫学、或いは代謝の手段によって主機能を達成することはないが、これらの手段により一定の補助的作用をもたらすことができるもの。
   （出典：Global Harmonization Task Force、Definition of the terms medical device and In Vitro Diagnostic (IVD) device）。

1.3.22 **操作者**： 意図された目的のために医療機器を使用する者。（出典：カスタム定義）。

1.3.23 **パッチタグ：** 特定のパッチの識別子。（出典：NIST IR 8060: Guidelines for the Creation of Interoperable Software ID (SWID) Tags）

1.3.24 **個人識別番号（PIN）：**個人に割り当てられ、同一性の検証を提供するために使用される番号またはコード。（出典：カスタム定義）。

1.3.25 **保護健康情報（PHI）：**電子メディアで通信される個人を特定できる健康情報（IIHI）;電子メディアで保持;または、他の形式またはメディアで通信または保持される。（出典：45CFR Section 160 から抜粋）*注記：　これはPII のサブセットである。*

1.3.26 **保護個人情報（PPI）：** 公開から保護されるべき個人に関する情報。これには、健康、財務、その他の種類の情報が含まれる場合がある。患者だけでなく、すべての人に該当する。MDS2 では、これは個人識別可能情報と呼ばれ、IEC TR80001-2-2:2012 の用語である（出典：カスタム定義）。

1.3.27 **物理的保護手段：**組織の電子情報システム及び関連の建物及び設備を、自然・環境の危険及び無許可の侵入から保護する物理的な手段、方針及び手続き。（出典：MDS2-2013）

1.3.28 **個人識別可能情報（PII）：** 機関によって維持される個人に関する情報.で以下を含む。(1) 個人の身元を識別または追跡するために使用できる情報を。および (2) 医療、教育、財務、雇用情報など、個人とリンクまたはリンク可能なその他の情報（出典：NIST800-122）。*注記：　ローカルの法は、PII のローカルにおける法的定義を提供することができ、警告なく変更することができる。*

1.3.29 **プロセス：** 入力を出力に変換する相互関係のある、又は相互に作用する一連の活動。（出典：ISO 9001）

1.3.30 **リモートサービス：** サポートサービス（例えば検査、診断、ソフトウェアのアップグレード）で機器に物理的に直接接続されていないもの（例：モデム、ネットワーク、インターネットを介するリモートアクセス）。（出典： HIMSS Dictionary of Healthcare Terms）

1.3.31 **リムーバブルメディア：** ツールを使用しないでシステムから取り除くことができる電子メディア。（出典： MDS2-2013）

1.3.32 **リスク：** 危害の発生確率とその危害の重大性の組み合わせ（出典：ISO14971）

1.3.33 **リスクアセスメント：**個人識別可能情報またはシステム機能の完全性、可用性、および機密性に対する潜在的リスクおよび脆弱性の正確かつ徹底的な分析の実施。（出典：HIPAA より抜粋）。

1.3.34 **リスクマネジメント：**リスクアセスメントの継続的なプロセス。リスクを受容可能なレベルまで低減し、そのレベルを維持するための措置を講じる。合理的かつ適切なレベルまでリスク及び脆弱性を減らすために十分なセキュリティの手段。（出典：カスタム定義）

1.3.35 **安全性：** 受容できないリスクがないこと（出典：ISO14971）

1.3.36 **セキュリティコントロール：** システムとその情報の機密性、完全性、可用性を保護するために情報システムに規定された管理、運用、技術管理（すなわち、保護手段または対策）。（出典：NIST）。

1.3.37 **セキュリティ機能：** データ及びシステムの機密性、完全性、及び可用性、並びに説明責任のリスクを管理するための技術的、管理的、及び組織的なコントロールを指す幅広いカテゴリ。（出典： MDS2-2013）

1.3.38 **セキュリティ情報イベント管理（SIEM）：** 様々なイベントおよびコンテキストデータソースからのセキュリティイベントのリアルタイム収集および履歴分析を通じて、脅威検知およびセキュリティインシデント対応をサポートする技術。（出典：カスタム定義）。

1.3.39 **医療機器としてのソフトウェア：** ハードウェア医療機器の一部ではなく、これらの目的を実行する 1 つ以上の医療目的に使用することを意図したソフトウェア（出典：IMDRF Software as a Medical Device(SaMD):Key Definitions）

1.3.40 **医療機器**

1.3.41 **ソフトウェア ID タグ：** ソフトウェア製品を特定し、説明する一連のデータ要素。（出典：NIST IR8060:Guidelines for the Creation of Interoperable Software ID (SWID) Tags）。

1.3.42 **技術的保護手段：** 個人識別可能情報を含むデータを保護し、データへのアクセスを管理するための技術、方針、手順。（出典：カスタム定義）

1.3.43 **トークン：** ユーザが携行する物理的な認証機器（例：スマートカード、SecurID[tm]、など）。多くの場合、PIN と組み合わされ、単純なパスワード認証より優れていると一般に考えられる二要素認証方式。（出典：カスタム定義）

1.3.44 **ユーザ：** 操作者を参照。

1.3.45 **ウイルス：** マルウェアを参照。

1.3.46 **脆弱性：** 脅威源によって悪用または誘引される可能性がある機器、情報システム、システムセキュリティ手順、内部管理、または実施における弱点。（出典：NIST SP 800-53 より抜粋）

# セクション2 - MDS2 書式の入手、使用、記入の説明

## 2.1 MDS2 書式の入手（医療提供者）

完成した MDS2s は、**機器**の製造業者（例：製造業者のウェブサイト）から入手できる。このフォームは、機器の仕様の変更を反映するために更新することができる。ユーザは、MDS2 が機器の正しいモデル及び改訂レベルに対応していることを確認しなければならない。製造業者のプロセス及び方針に関する質問は、文書発行日時点の最新の製造業者情報を反映している。

注釈 - 製造業者が該当する**機器**について記入した MDS2 書式をもっていない場合、ブランクの MDS2 書式上部の適切な欄に製造業者とモデル情報を記入し、この書式と説明書を製造業者の法令順守担当部門に提出し記入を依頼すること。

## 2.2 MDS2 書式の使用（医療提供者）

### 2.2.1 機器の説明

MDS2 は、MDS2 機器の説明（DOC-2）及びモデル（DOC-3）に示すように、単一の医療機器に関連するセキュリティ及びプライバシー保護の機能を説明する。

MDS2 書式の最初の二つのセクションは**機器**を特定するため（機器の説明）及び、**機器**の保存/通信するデータのタイプ、データの保存/通信の方法などを説明するために使用されている。（個人識別可能情報の管理）。

**注意事項－リストされた機能を実行する機器の能力の表示（すなわち「Yes」の答え）は、これは暗黙か明示かを問わず、製造業者が機器の構成又はリストされた機能の実行を裏付け又は許可するものではない。**

**能力と許可とを区別することが重要である。示されていない限り、MDS2 書式に含まれる質問は機器能力を指している。通常、許可は MDS2 書式とは別の契約上の問題である。明示的な製造業者による許可なくして機器を変更すると、重大な契約、安全、債務上の問題になることがある。**

## 2.3 MDS2 書式の記入（製造業者）

MDS2 のセクション 2.3（MDS2 書式の記入）には、**機器**の特定のセキュリティ機能に関する情報が記載されている。この情報は、IEC 80001-2-2「*医療機器のセキュリティニーズ、リスク、及びコントロールの伝達に関するガイダンス*」に従ったカテゴリに分類されている。

製造業者が質問に対する答えについて特定の詳細事項を説明するスペースを必要とする場合、MDS2 書式には、解説を記入するスペースがある。

注－製造業者は推奨慣行又は解説のためのスペースを更に追加する必要がある場合は、補足資料を添付してもよい。

### 2.3.1 一般

製造業者は MDS2 で要求される情報を、**機器**によって保存/通信されたデータのタイプ、データの保存/通信方法、**機器**に組み入れられた他のセキュリティ関連の機能に関する必要な記述的情報などすべての情報を含め、要求する組織に適宜提供しなければならない。

この情報は、特定の機器設計、ソフトウェア開発、及び生産特性に基づくべきである。この情報はサイバーセキュリティの目的のために使用され、その目的を念頭に記述する。

この書式の評価および自動化を簡素化するため、製造業者はすべての質問に「Yes」(はい)、「No」(いいえ)、または「N/A」(該当なし) のいずれかで回答しなければならない。追加情報が必要な場合、「See Note X」(注記 X を参照)を追加し、回答をさらに明確にする関連注記を記載する。

この書式は多くのセクションから構成されている。これらのセクションの一部は、特定の機器には適用されない場合がある。すべてのセクションに「No」または「N/A」の回答を適宜記入しなければならない。

答えを適切に解釈するために追加情報が必要な場合、製造業者は解説の欄に情報を記入すること。

インストールされているオプションや付属品によって回答が異なる場合は、回答した個々の質問について添付の「Note」(注記)に説明すること。

広範な回答には、例えばハイパーリンクや文書の識別、文書内の場所の参照など、他の公表された文書をもまた参照することができる。詳細な文書を参照する場合は、簡潔な要約を含めてください。参照文書の入手方法を記載する。

複数の質問に対する回答が Note(注記)を参照している場合、各参考資料は、その質問に回答した Note(注記)の具体的な場所を示すこと。

「アプリ」やプラグインなど、ソフトウェアのみの機器は、該当するセクションに記入し、物理的機器にのみ適用されるセクションには「N/A」と表示する。

注記 -以降のサブセクションの番号は、MDS2 書式の質問番号と相関している

### 2.3.2 機器の説明セクション：

DOC-1 製造業者名： これは文章を自由に記入する欄である。

DOC-2 機器の説明：これは文章を自由に記入する欄である。製造業者は標準的な用語を用いて、主要なモダリティや**機器**の機能性を顧客が分かりやすく区別できるようにすること。製造業者は、FDA が指定した製品コード、ECRI 研究所の機器コード、又はその他の一般的な機器名称に関連する機器名を使用することができる。製造業者は、マーケティング資料、商標名、又は著作権で保護された名称に基づく社内製品名を使用してはならない。

DOC-3 機器モデル：これは文章を自由に記入する欄である。製造業者は、市販される機器のモデルを使用すること。これには、顧客向け銘版に記載されたモデル、機器識別タグに記載されたモデル、又は該当する場合はカタログ ID が含まれる。

DOC-4 文書識別コード：文書識別コードは**機器**文書を追跡するために内部で使用される製造業者のユニークなタグである。

DOC-5 製造業者連絡先：役職または部門の一般的な電子メールおよび代表電話番号を提供する。

DOC-6 ネットワーク環境での機器の用途：製造業者は、顧客のネットワーク環境に接続している場合に、意図している**機器**の機能及び用途、また関連する場合は**機器**に想定される使用方法を説明する。

DOC-7 文書公開日：顧客向け文書公開日（年月日）。

DOC-8 脆弱性開示の協調：製造業者は本機器の脆弱性開示プログラムを有しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

DOC-9 ISAO：製造業者は情報共有分析機関(ISAO)に属しているか?

DOC-10 図表：他のシステムコンポーネントまたは予想される外部リソースへの接続を示すネットワークまたはデータフロー図はあるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

DOC-11 SaMD: 機器は医療機器としてのソフトウェア（すなわち、ハードウェアなしのソフトウェア）か?「No」の場合、このセクションの質問に「N/A」と回答する。

DOC-11.1 SaMD にはオペレーティングシステムが含まれているか?（機器のオペレーティングシステムの詳細については CSUP-2 を参照のこと。）

DOC-11.2 SaMD は所有者/操作者が提供するオペレーティングシステムに依存しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

DOC-11.3 SaMD は製造業者によって運営されているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

DOC-11.4 SaMD は顧客によって運営されているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

MDS2 書式のセキュリティ機能に関するセクションには、**機器**の特定のセキュリティ関連の機能についての質問が含まれている。これらの質問は、適宜 IEC 80001-2-2「**医療機器**のセキュリティニーズ、リスク、及びコントロールの伝達に関するガイダンス」の**セキュリティ機能**カテゴリに分類される。追加のカテゴリも含まれる。

### 2.3.3 個人識別可能情報の管理（MPII）：

機器上または機器によって個人識別可能情報がどのように取り扱われるか。

MPII-1 この**機器**は、**個人識別可能情報**（例：保護対象電子医療情報（ePHI））を表示、通信、保存、または修正できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 機器が保持できる PII 要素（例：患者名、患者 ID、社会保障番号、生体データ）を「Note」に記載するか、完全なリストについて製品文書の参照先を示す。

MPII-2 **機器**は**個人識別可能情報**を保持しているか?

MPII-2.1 **機器**は、**個人識別情報**を一時的に揮発性メモリに保持しているか（つまり、パワーオフ又はリセットによって消去されるまで）?

MPII-2.2 **機器**は、内部メディアに**個人識別可能情報**を持続的に保存しているか?

MPII-2.3 **個人識別可能情報**は、明示的に消去されるまで、機器の不揮発性メモリに保存されているか?

MPII-2.4 **機器**は、**個人識別可能情報**をデータベースに保存しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

MPII-2.5 **機器**の設定によって、長期ソリューションに保存された後、ローカルの個人識別可能情報を自動的に削除できるようになっているか?

MPII-2.6 **機器**は、**個人識別可能情報**を他のシステムにインポート/エクスポートするか（例：ウェアラブルモニタリング装置は、**個人識別可能情報**をサーバーにエクスポートすることができる）？

MPII-2.7 **機器**は、**個人識別可能情報**をパワーオフまたはパワー中断中も保持しているか?

MPII-2.8 **機器**は、サービス技術者が内部メディアを取り外すことができるようになっているか（例：個別の廃棄または顧客の継続使用のため）？

MPII-2.9 **機器**は、**個人識別可能情報**記録を機器のオペレーティングシステムとは別の場所に保管できるようになっているか（すなわち、二次内部ドライブ、代替ドライブパーティション、またはリモート保管場所）？

MPII-3 **機器**には、**個人識別可能情報**の通信、インポート/エクスポートに使用されるメカニズムがあるか?

ガイダンス： 記載されているメカニズムがオプションであるかどうかを「Note」に示すこと。

MPII-3.1 **機器**は、**個人識別可能情報**を表示するか（例：ビデオ表示等）。

MPII-3.2 **機器**は、**個人識別可能情報**を含むハードコピーのレポート又はイメージを作成するか?

MPII-3.3 **機器**は、**個人識別可能情報**を**リムーバブルメディア**から取得、または**リムーバブルメディア**へ記録するか（例：リムーバブル-HDD、USB メモリ、DVD-R/RW、CD-R/RW、テープ、CF/SD カード、メモリスティックなど）？

MPII-3.4 **機器**は、専用ケーブル接続（例：RS-232、RS-423、USB、FireWire など）を介して**個人識別可能情報**を送信/受信又はインポート/エクスポートするか？

MPII-3.5 **機器**は、有線ネットワーク接続（例：RJ45、光ファイバー等）を介して、**個人識別可能情報**を送信/受信するか？

MPII-3.6 **機器**は、無線ネットワーク接続（例：WiFi、Bluetooth、NFC、赤外線、セルラーなど）を介して**個人識別可能情報**を送信/受信するか？

MPII-3.7 **機器**は、外部ネットワーク（例：インターネット）上で個人識別可能情報を送信/受信するか？

MPII-3.8 **機器**は、文書のスキャンを通じて**個人識別可能情報**をインポートするか?

MPII-3.9 **機器**は、独自のプロトコルを介して**個人識別可能情報**を送信/受信するか?

MPII-3.10 **機器**は、**個人識別可能情報**を通信、インポート、またはエクスポートするために他のメカニズムを使用するか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

### 2.3.4 自動ログオフ（ALOF）

一定時間操作しない場合に、許可されていないユーザの使用や誤用を避けるための機器の機能。

ALOF-1 操作していない時間があらかじめ決めた一定の長さを超えると、ログインしている**ユーザ**の再認証を強制するように**機器**を設定できるか（例：自動ログオフ、セッションロック、パスワードで保護されたスクリーンセーバ）？

ガイダンス： **機器**は、デフォルトでも設定された場合でも常に次のようになっているか：1) 一定の非アクティブ期間の後に再認証を強制する; 2) パスワードで保護されたスクリーンセーバを、事前に選択された非アクティブ期間後に起動し、**ユーザ**をログオフしなくても**ユーザ**アクセスを効果的に防止するか?「Note」セクションは、自動ログオフ又はスクリーンロック機能を無効にできるかどうか/その方法を記載するために使用する。（例：適切な**ユーザ**セキュリティ警告/通知とともに、セッションごとに、又は全体で）

ALOF-2 自動ログオフ/スクリーンロックが実行されるまでの操作しない状態の経過時間は、**ユーザ**又は管理者が設定できるか?「Yes」の場合、「Note」に時間、固定又は設定可能な範囲を示す。

ガイダンス： **ユーザ**又は管理者は自動ログオフ又はスクリーンロックが実行されるまでの経過時間を設定できるか？「Note」セクションは、設定可能な自動ログオフ/スクリーンロックを備えた**機器**が以下を設定できるかどうかを示すために使用します。1) **ユーザ**が指定した時間に設定;2) 特定の役割別（例：管理者、**ユーザ**）。

### 2.3.5 監査コントロール（AUDT）

機器上の活動を確実に監査する機能。

「Note」 - このサブセクションの多くの質問について、監査能力をより詳細に説明する文書がある場合がある。その場合、より詳細な説明文書を参照する「Note」とともに、「Yes」と回答することが適切である。

AUDT-1 **医療機器**は、標準的なオペレーティングシステムログ以外に追加の**監査ログ**や**監査レポート**を作成することができるか?

ガイダンス： 回答が「No」の場合、AUDT-1.1 から AUDT-3.1 までの回答は「N/A」とする。

AUDT-1.1 監査ログにユーザ ID が記録されているか?

ガイダンス：「Yes」の場合、ログ内に**個人識別可能情報**イベントごとにデータ対象者（例：患者）が特定されているかどうかを「Note」に示す。また、**監査証跡**は**個人識別可能情報**の作成・表示・エクスポート等を他のデータと区別できるか、「Note」に記載する。

AUDT-1.2 その他の**個人識別可能情報**は監査証跡に存在するか?

ガイダンス：「Yes」の場合、ログ内に**個人識別可能情報**イベントごとにデータ対象者（例：患者）が特定されているかどうかを「Note」に示

す。また、**監査証跡**は**個人識別可能情報**の作成・表示・エクスポート等を他のデータと区別できるか、「Note」に記載する。

AUDT-2 イベントは監査ログに記録されているか?「Yes」の場合、次のイベントのうち、監査ログに記録されるイベントはどれか：

AUDT-2.1 ログイン/ログアウトの試みに成功したか?

AUDT-2.2 ログイン/ログアウトの試みに失敗したか?

AUDT-2.3 ユーザ権限の変更?

AUDT-2.4 ユーザの作成/変更/削除?

AUDT-2.5 臨床データまたは PII データの提示（例：表示、印刷）?

AUDT-2.6 データの作成/変更/削除?

ガイダンス：「Yes」の場合、「Note」でこれらデータ操作のどの形式（作成及び/又は変更及び/又は削除）が追跡されているのか示すこと。

AUDT-2.7 **リムーバブルメディア**（例：USB ドライブ、外部ハードドライブ、DVD）からデータをインポート/エクスポートするか?

ガイダンス：「Yes」の場合、どの程度の詳細が記録されているかを「Note」に示す（例：患者 ID のみ、文書 ID のリスト）。

AUDT-2.8 ネットワークまたはポイント・ツー・ポイント接続を介したデータまたはコマンドの受信/送信?

ガイダンス：「Yes」の場合、どの程度の詳細が記録されているかを「Note」に示す（例：患者 ID のみ、文書 ID のリスト）。

AUDT-2.8.1 リモートまたはオンサイトのサポート?

ガイダンス：「Yes」 の場合、どのような種類のサービス活動が保存されるかを「Note」に示す。

AUDT-2.8.2 アプリケーションプログラミングインターフェース（API）および同様の活動?

ガイダンス：「Yes」 の場合、HL7 からの FHIR など、機器がログ記録のためにサポートし、監査する独自の、標準的なネットワーク API を「Note」に示す。詳細情報が製品文書に記載されているかどうかを示す。

AUDT-2.9 緊急アクセス（EMRG）

ガイダンス：「Yes」 の場合、「Note」に**緊急アクセス**の事象を記録する**機器**の機能を示す。製造業者は以下を示す場合もある。

a. 監査ログに記録するために、**機器**が（一時的/「緊急」）**ユーザ**名及び/又は病院/診療所 ID 番号の入力を緊急**ユーザ**に求めるかどうか/その方法。

b. 「緊急」セッション時に取得したデータを**機器**が識別する、又は「フラグを付ける」かどうか/その方法（例：許可された**ユーザ**のログインなしで取得されたデータ）

AUDT-2.10 その他のイベント（例：ソフトウェアの更新）?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-2.11 監査能力をより詳細に文書化しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-3 所有者/操作者は、監査ログにどのイベントを記録するか定義または選択できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-4 イベントの監査ログに記録されたデータ属性のリストはあるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 監査ログに記録されたデータ属性を「Note」に示すか、完全なリストについて製品文書の参照先を示す。

AUDT-4.1 監査ログは日付/時刻を記録しているか?

AUDT-4.1.1. 日時はネットワーク時刻プロトコル（NTP）または同等の時刻ソースによって同期できるか?

ガイダンス：NTP を使用していない場合、**機器**の時刻をどのように設定するかを「Note」に示す。

AUDT-5 監査ログの内容をエクスポートできるか?

AUDT-5.1 物理的メディアによるものか?

AUDT-5.2 IHE 監査証跡及びノード認証（ATNA）プロファイルを経由して SIEM へ?

AUDT-5.3 他のコミュニケーション（例：外部サービス機器、モバイルアプリケーション）によるものか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-5.4 監査ログは、転送中または記憶メディア上で暗号化されるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-6 監査ログは所有者/操作者が監視/レビューできるか?「No」 の場合、監査プロセスの詳細または参照を「Note」に記載する。

AUDT-7 監査ログは変更から保護されているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-7.1 監査ログはアクセスから保護されているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUDT-8 監査ログは機器によって分析できるか?該当する場合、「Note」に参照先を記載する。

**2.3.6　認証（AUTH）：**

許可されているユーザかどうかを判断する機器の機能

AUTH-1　**機器**は**ユーザ**ログイン要件又はその他のメカニズムを使って許可されていない**ユーザ**のアクセスを禁止できるか？

ガイダンス：「Yes」の場合、「Note」に許可されていないアクセスを禁止するため**機器**が使用している物理的または**技術的保護手段**（パスワード、バイオメトリックス、キーカードなど）を示す。

AUTH-1.1　機器は、権限付与のためにユーザ認証連携マネジメントを使用するように構成できるか（例：LDAP、OAuth）？「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUTH-1.2　顧客はグループ方針を機器にプッシュすることができるか（例：アクティブディレクトリ）？「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUTH-1.3　特別なグループ、組織単位、グループ方針が必要か?「Yes」 の場合、詳細または参照先を「Note」に記載する。

AUTH-2　**ユーザ**は、「役割 」（例：ユーザ、管理者、サービス等）に基づき、異なる権限レベルを割り当てることができるか?

AUTH-3　**機器**の所有者/**操作者**は制限のない管理者権限を取得できるか（例：ローカルルート又は管理者アカウントによるオペレーティングシステム又はアプリケーションへのアクセス）？

ガイダンス：「Yes」の場合、**機器**が複数の特権アカウント（例：管理者、ルート）および管理者アカウントの使用に関する**ユーザ**の制限をサポートしているかどうかを「Note」に示す。

AUTH-4　機器は、**すべての** API アクセス要求を認証または制御しているか?「No」 の場合、詳細または参照先を「Note」に記載する。

AUTH-5　機器は、デフォルトとして、アクセス制限モードあるいは kiosk モード動作するか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

**2.3.7　サイバーセキュリティ製品の更新（CSUP）：**

機器のセキュリティパッチをインストール/更新できるオンサイトのサービス要員、リモートサービス要員、または許可されている顧客要員の能力。医療機器製造業者は、サイバーセキュリティの脆弱性に対処するためのコンピュータソフトウェアの変更を含むソフトウェア設計変更のバリデーションを必要とすることが多い、米国の 21CFR Part820 などの品質システムを規制する適用される機器規則に従うことが求められることに注意すること。

ガイダンス：　CSUP-1、CSUP-2、CSUP-3、CSUP-4、CSUP-5、CSUP-6

セキュリティパッチの適用に関する製造業者の制限を「Note」に示す。「Note」で、これらの制限の説明が記載されている製品文書を参照することができる。

CSUP-1　機器には、機器の製造業者またはソフトウェア/ファームウェアの第三者製造業者のいずれかから、動作寿命中にセキュリティの更新を必要とする可能性のあるソフトウェアまたはファームウェアが含まれているか?「No」の場合、このセクションの質問に「N/A」と回答する。

CSUP-2　機器にはオペレーティングシステムが含まれているか?「Yes」 の場合、2.1〜2.4 を記入する。

CSUP-2.1　機器の文書には、**所有者/操作者**によるパッチのインストールまたはソフトウェアの更新に関する指示が記載されているか?

CSUP-2.2　機器は、パッチまたはソフトウェアの更新をインストールするために**ベンダー**または**ベンダーが承認したサービス**を必要とするか?

CSUP-2.3　機器には、パッチの**リモートインストール**またはソフトウェアの更新を受ける機能があるか?

CSUP-2.4　医療機器の製造業者は、製造業者の承認なしに、第三者製造業者（例：Microsoft）からのセキュリティ更新をインストールすることを許可しているか?

CSUP-3　機器にはドライバーとファームウェアが含まれているか?「Yes」 の場合、3.1~3.4 を記入する。

CSUP-3.1　機器の文書には、**所有者/操作者**によるパッチのインストールまたはソフトウェアの更新に関する指示が記載されているか?

CSUP-3.2　機器は、パッチまたはソフトウェアの更新をインストールするために**ベンダー**または**ベンダーが承認したサービス**を必要とするか?

CSUP-3.3　機器には、パッチの**リモートインストール**またはソフトウェアの更新を受ける機能があるか?

CSUP-3.4　医療機器の製造業者は、製造業者の承認なしに、**第三者製造業者**（例：Microsoft）からのセキュリティ更新をインストールすることを許可しているか?

CSUP-4　機器にはマルウェア対策ソフトウェアが含まれているか?「Yes」 の場合、4.1〜4.4 に記入する。

CSUP-4.1　機器の文書には、**所有者/操作者**によるパッチのインストールまたはソフトウェアの更新に関する指示が記載されているか?

CSUP-4.2　機器は、パッチまたはソフトウェアの更新をインストールするために**ベンダー**または**ベンダーが承認したサービス**を必要とするか?

CSUP-4.3　機器には、パッチの**リモートインストール**またはソフトウェアの更新を受ける機能があるか?

CSUP-4.4　医療機器の製造業者は、製造業者の承認なしに、**第三者製造業者**（例：Microsoft）からのセキュリティ更新をインストールすることを許可しているか?

CSUP-5　機器には非オペレーティングシステムの市販コンポーネントが含まれているか?「Yes」 の場合、5.1～5.4 を記入する。

CSUP-5.1　機器の文書には、**所有者/操作者**によるパッチのインストールまたはソフトウェアの更新に関する指示が記載されているか?

CSUP-5.2　機器は、パッチまたはソフトウェアの更新をインストールするために**ベンダー**または**ベンダーが承認したサービス**を必要とするか?

CSUP-5.3　機器には、パッチの**リモートインストール**またはソフトウェアの更新を受ける機能があるか?

CSUP-5.4　医療機器の製造業者は、製造業者の承認なしに、**第三者製造業者**（例：Microsoft）からのセキュリティ更新をインストールすることを許可しているか?

CSUP-6　機器には他のソフトウェアコンポーネント（例：資産管理ソフト、ライセンス管理等）が含まれているか?「Yes」 の場合、詳細または参照先を「Note」に記載し、6.1～6.4 に記入する。

CSUP-6.1　機器の文書には、**所有者/操作者**によるパッチのインストールまたはソフトウェアの更新に関する指示が記載されているか?

CSUP-6.2　機器は、パッチまたはソフトウェアの更新をインストールするために**ベンダー**または**ベンダーが承認したサービス**を必要とするか?

CSUP-6.3　機器には、パッチの**リモートインストール**またはソフトウェアの更新を受ける機能があるか?

CSUP-6.4　医療機器の製造業者は、製造業者の承認なしに、**第三者製造業者**（例：Microsoft）からのセキュリティ更新をインストールすることを許可しているか?

CSUP-7　製造業者は、インストールするための更新が承認された時点で顧客に通知しているか? その場合、詳細または参照先を「Note」に記載する。

CSUP-8　機器はソフトウェア更新の自動インストールを実行するか?

CSUP-9　製造業者は、機器にインストールできる第三者ソフトウェアの承認済みリストを有しているか? その場合、製造業者が承認した第三者ソフトウェアリストおよび/

または追加の第三者ソフトウェアを承認する要求を管理するための製造業者プロセスを「Note」に記載または参照する。

CSUP-10　所有者/操作者は、製造業者が承認した第三者ソフトウェアを機器自体にインストールできるか?

CSUP-10.1　システムには、未承認ソフトウェアのインストールを防止するためのメカニズムがあるか?

CSUP-11　製造業者は、機器の脆弱性の評価と更新するためのプロセスを整備しているか?

CSUP-11.1　製造業者は、更新のレビューおよび承認状況を顧客に提供しているか?

CSUP-11.2　機器の更新レビューサイクルはあるか? その場合、詳細または参照先を「Note」に記載する。

### 2.3.8　健康データの非識別化（DIDT）：

個人の識別を可能にする情報を直接削除する機器の機能。

DIDT-1　機器は、個人識別可能情報を非識別化するために不可欠な機能を提供しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 非識別化プロセスが HIPAA のセクション 164.514 (b) などの特定の非識別化基準/ガイドラインを参照/遵守しているかどうかを「Note」に示す。非識別化手順が設定可能かどうかも記載する。

DIDT-1.1　機器は、非識別化のための DICOM 規格に適合する非識別化プロファイルをサポートしているか? その場合、詳細または参照先を「Note」に記載する。

ガイダンス：DICOM 規格は一般的に医用画像技術に適用される。

### 2.3.9　データのバックアップと災害復旧（DTBK）：

機器のデータ、ハードウェア、ソフトウェアまたはサイト設定情報の損傷や破壊後に復旧できる機能。

DTBK-1　機器は、個人識別可能情報/患者情報（例：PACS）の長期一次保管を保持しているか?

DTBK-2　機器には、製造業者が提供する元の機器設定を復元するための「工場出荷時リセット」機能があるか?

DTBK-3　**機器**は**リムーバブルメディア**に不可欠なデータのバックアップ機能を備えているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 「Yes」 の場合、データのバックアップ/災害復旧に関する制限または制約を「Note」に示す。これは**リムーバブルメディア**（例：光ディスク、磁気ディスク、テープ等）への情報バックアップをサポートする統合された機能またはオプションを指す。

DTBK-4 **機器**には、**リモート保存**に不可欠なデータのバックアップ機能があるか?「Yes」の場合、詳細または参照先を「Note」に記載する。

ガイダンス： これは**リモート保存**への情報バックアップをサポートする統合機能またはオプションを指す。データのバックアップ/災害復旧に関する制限または制約を「Note」に記載する。該当する場合、個人情報の保護方法を記載する（例：暗号化または省略）。

DTBK-5 **機器**には、システム設定情報、パッチ修復、ソフトウェア修復のバックアップ機能があるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： これは、**ローカル**または**リモート保存**への情報バックアップをサポートする統合された機能またはオプションを指す。データバックアップ/災害復旧に関する制限や制約があれば「Note」に記載する。該当する場合、個人情報の保護方法を記載する（例：暗号化または省略）。

DTBK-6 機器はバックアップの完全性と真正性をチェックする機能を提供するか?

### 2.3.10 緊急アクセス（EMRG）：

医療上の緊急事態が発生し、保管されている個人識別可能情報への即時アクセスを必要とする場合、機器ユーザが個人識別可能情報にアクセスできる機能。

EMRG-1 **機器**には**緊急アクセス**（「ブレイクグラス」）機能が組み込まれているか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： **緊急アクセス**の説明は、「定義」セクションを参照。

### 2.3.11 健康データの完全性と真正性（IGAU）：

機器が完全性を検証し、真正性を検証し、機器に保存された健康データが利用可能であることを保証する方法。機器が健康データを保存しない場合は、本セクションの質問に「N/A」と回答する。

IGAU-1 **機器**は、保存された健康データのデータ完全性チェックメカニズムを提供するか（例：ハッシュまたはデジタル署名）？その場合、詳細または参照先を「Note」に記載する。

IGAU-2 **機器**は、保存されている健康データのエラー/故障の保護および復旧メカニズム（例：RAID-5 など）を提供するか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

### 2.3.12 マルウェアの検出/保護（MLDP）

悪意のあるソフトウェア（マルウェア）を効果的に防御、検出、及び削除する機器の機能。

MLDP-1 実行可能なソフトウェアをホストできるか?

MLDP-2 **機器**は**マルウェア対策ソフトウェア**（またはその他の**マルウェア対策**メカニズム）の使用をサポートしているか？詳細または参照先を「Note」に記載する。

ガイダンス： 製造業者は、「Note」で直接**マルウェア**のサポートに関する制約（購入/インストール/設定）について説明、またはこれら制約の説明が記載されている製品文書の参照先を示すことができる。

MLDP-2.1 機器にはデフォルトでマルウェア対策ソフトウェアが含まれているか?

MLDP-2.2 機器にはオプションとしてマルウェア対策ソフトウェアがあるか?

MLDP-2.3 **機器**の文書により、所有者/操作者はマルウェア対策ソフトウェアをインストールまたは更新することができるようになっているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

MLDP-2.4 **機器**の所有者/**操作者**は、**マルウェア対策**の設定を独立して（再-）設定できるか?

MLDP-2.5 **マルウェア検出**の通知が**機器のユーザ**インターフェイスで生じるか？

ガイダンス： 「No」 の場合、**マルウェア**が検出されたときに**ユーザ**に通知する方法を「Note」に示す。

MLDP-2.6 マルウェアが検出された場合は、製造業者が許可した人のみがシステムを修理できるか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

MLDP-2.7 マルウェアの通知はログに書き込まれているか?

MLDP-2.8 マルウェア対策（例：購入、設置、設定、スケジューリング）に関する制限はあるか?

MLDP-3 MLDP-2 への回答が **「No」** であり、マルウェア対策が機器にインストールできない場合、他の補完的管理策が整備されているか、利用可能か?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： MLDP-2 に対する回答が**「Yes」**の場合、MLDP-3 に N/A と回答する。

MLDP-4 機器は、機器上での実行が許可されているソフトウェアおよびサービスを制限するアプリケーションのホワイトリストを使用しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

MLDP-5 機器はホストベースの侵入検知/予防システムを採用しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

MLDP-5.1 ホストベースの侵入検知/予防システムを顧客が設定できるか?

MLDP-5.2 ホストベースの侵入検知/予防システムを顧客がインストールできるか?

**2.3.13 ノードの認証（NAUT）：**

通信パートナー/ノードを認証する機器の機能。

NAUT-1 機器は、データの送信側と受信側の両方が相互に認証しており、転送される情報の受け取りが許可されていることを保証するノード認証の方法を提供/サポートしているか（例：ウエブ APIs、SMTP、SNMP）？「Yes」 の場合、詳細または参照先を「Note」に記載する。

NAUT-2 ネットワークアクセス制御機構はサポートされているか（例：機器に内部ファイアウォールがあるか、ネットワーク接続ホワイトリストを使用しているか）？「Yes」 の場合、詳細または参照先を「Note」に記載する。

NAUT-2.1 ファイアウォールのルールが文書化され、レビューに利用できるか?「Yes」の場合、詳細または参照先を「Note」に記載する。

NAUT-3 証明書ベースのネットワーク接続認証を使用しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 該当する場合、証明書の管理方法を「Note」に説明する。

**2.3.14 接続能力（CONN）**

適切なセキュリティマネジメントを決定する際には、すべてのネットワークおよびリムーバブルメディア接続を検討する必要がある。このセクションでは、機器に存在する可能性のある接続機能を列記する。

CONN-1 機器にはハードウェア接続機能があるか?「Yes」 の場合、機器のハードウェア接続能力を特定する詳細または参照先を示す。「No」の場合、「Note」に「なし」と記載し、このセクションの質問には「N/A」と回答する。

ガイダンス： ネットワークに接続するために機器にインストールされている、又はオプションでインストールされているハードウェア及び基本的なオペレーティングシステムの能力のリストを「Note」に示す。また、機能が購買オプションであるか、無効にできるかを示す。

CONN-1.1 機器は無線接続をサポートしているか?

CONN-1.1.1 機器は Wi-Fi をサポートしているか?「Yes」の場合、「Note」にサポートされている Wi-Fi 認証プロトコル（例：WPA2 EAP-TLS）を記載または参照先を示す。

CONN-1.1.2 機器は Bluetooth をサポートしているか?「Yes」 の場合は、サポートされている Bluetooth セキュリティモードを記載または参照先を示し、それを強制できるかを「Note」に示す。

CONN-1.1.3 機器は他の無線ネットワーク接続（例：LTE、Zigbee、プロプラエタリ）をサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-1.1.4 機器は他の無線接続（例：カスタム RF コントロール、無線検出器）をサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-1.2 機器は物理的接続をサポートしているか?

CONN-1.2.1 機器には RJ45 イーサネットポートがあるか?

CONN-1.2.2 機器には利用可能な USB ポートがあるか?「Yes」 の場合、使用方法およびそれらがどのように保護されているかを示す詳細または参照先を「Note」に記載する。

CONN-1.2.3 機器はリムーバブルなメモリデバイスを必要とするか、使用するか、サポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-1.2.4 機器は他の物理的接続をサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-2 製造業者は、機器に使用される、又は使用される可能性のあるネットワークポート及びプロトコルのリストを提供しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： ネットワーク接続機器にプロトコルが必要かどうかを示す。転送プロトコル（例：IPv4、IPv6）、アプリケーションプロトコル（例：DICOM、IEEE11073、HL7）、その他のサービスプロトコル（例：DHCP、SMB、RDP）、カスタムプロトコルを必ず含めること。該当する場合、バージョンを特定する。

CONN-3 機器は顧客環境内の他のシステムと通信できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-4 機器は、顧客環境以外の他のシステム（例：サービスホスト）と通信できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-5 機器は API コールを作成または受信するか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-6 機器は、その使用目的のためにインターネット接続を必要とするか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-7 機器はトランスポート層セキュリティ（TLS）をサポートしているか?「Yes」の場合、サポートしているまたは使用できない TLS バージョンについて詳細または参照先を「Note」に記載する。

CONN-7.1 TLS は設定可能か?「Yes」 の場合、詳細または参照先を「Note」に記載する。

CONN-8 機器は、別の機器（例：遠隔医療等）から操作者制御機能を提供するか?「Yes」の場合、詳細または参照先を「Note」に記載する。

**2.3.15 個人の認証（PAUT）：**

ユーザを認証するために機器を設定する機能。

PAUT-1 機器は、すべてのユーザおよび役割（サービスアカウントを含む）に固有の ID およびパスワードをサポートし、実施しているか?

PAUT-1.1 機器は、すべてのユーザ及び役割（サービスアカウントを含む）に対して固有の ID 及びパスワードの認証を行っているか?「No」 の場合、詳細または参照先を「Note」に記載する。

PAUT-2 **機器**は外部認証サービスを通して**ユーザ**を認証するように設定できるか（例：MS アクティブディレクトリ、NDS、LDAP、OAuth など）？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： どのメカニズムを使用できるかを「Note」に示す。

PAUT-3 一定回数ログオンに失敗した後ユーザをロックアウトするように機器を設定できるか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： ユーザロックアウト機能の詳細を「Note」に示す。

PAUT-4 すべてのデフォルトアカウント（例：技術者サービスアカウント、管理者アカウント）が文書に記載されているか?「No」 の場合、詳細または参照先を「Note」に記載する。

PAUT-5 すべてのパスワードを変更できるか?「No」 の場合、詳細または参照先を「Note」に記載する。

PAUT-6 確立されている（組織固有の）複雑なルールを満たす**ユーザ**アカウントのパスワードを強制的に作成するように**機器**を設定できるか？ その場合、詳細または参照先を「Note」に記載する。

ガイダンス： パスワードの複雑性を設定できる場合は、「Yes」とする。複雑さの要件に関係なく、パスワードの複雑性が設定できない場合は「No」とする。複雑さのルールと制限は「Note」に記載すること。

PAUT-7 機器は定期的に期限切れとなるアカウントパスワードをサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 期限切れになる頻度や管理的対策が可能かどうか「Note」に記載する。

PAUT-8 多要素認証をサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

PAUT-9 機器はシングルサインオン（SSO）をサポートしているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

PAUT-10 機器上でユーザアカウントを無効化/ロックできるか?

PAUT-11 機器は生体認証をサポートしているか?

PAUT-12 機器は物理的なトークン（例：バッジアクセス）をサポートしているか?

PAUT-13 機器はグループ認証（例：病院チーム）をサポートしているか?

PAUT-14 アプリケーションまたは機器は、認証クレデンシャルを保存または管理しているか?その場合、詳細または参照先を「Note」に記載する。

PAUT-14.1 クレデンシャルはセキュアな方法で保管されているか?その場合、詳細または参照先を「Note」に記載する。

**2.3.16 物理的ロック（PLOK）：**

物理的ロックでは、物理的にアクセスできる許可されていないユーザが機器やリムーバブルなメディアに保存されている個人識別可能情報の完全性や真正性を損なうのを阻止できる。

PLOK-1 機器はソフトウェアのみ? 「Yes」の場合、このセクションの残りの質問に「N/A」と回答してください。

PLOK-2 **個人識別可能情報**を保持している**機器**のすべてのコンポーネント（**リムーバブルメディア**以外）は物理的に安全か（つまり、ツールなしでは取り外せない）？

ガイダンス： この質問は、製造業者の**機器**の一般的な取り付けと設定について尋ねる。**個人識別可能情報**を保持する内蔵データストレージドライブとその他の記憶メディアを検討する。そのようなメディアにツールなしで物理的にアクセスして取り外せない場合は「Yes」とする。この場合、アクセスに必要な物理的な鍵はツールと見なす。

PLOK-3 **個人識別可能情報**（**リムーバブルメディア**以外）を保持するすべての**機器**コンポーネントは、個別に鍵をかけたロック機器の背後に物理的に固定されているか?

PLOK-4 機器には、リムーバブルメディアへのアクセスを制限する物理的ロックを取り付けるオプションが顧客向けにあるか?

**2.3.17 機器のライフサイクルにおける第三者アプリケーションおよびソフトウェアコンポーネントのロードマップ（RDMP）：**

サードパーティーの EOL の管理のような機器のライフサイクル内において、カスタムコンポーネントを含む、サードパーティーアプリケーション及びソフトウェアコンポーネントのセキュリティサポートに関する製造業者の計画。機器に組み込まれるサードパーティーアプリケーションおよびソフトウェアコンポーネントに関する質問については、ソフトウェア部品表（SBOM）、セクション 2.3.18 を参照。

RDMP-1 製品開発中に、ISO/IEC27034 や IEC62304 などの安全なソフトウェア開発プロセスに従ったか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 機器の開発で準拠した安全なソフトウェア開発基準を説明または参照先を示し、使用されたセキュアなソフトウェア開発プロセスを簡単に説明する。

RDMP-2 製造業者は、セキュアな開発業務のために、機器に含まれるサードパーティーアプリケーションおよびソフトウェアコンポーネントを評価しているか?

RDMP-3 製造業者は、ソフトウェアサポートの日付及び更新に関するウェブページ又はその他の情報源を維持し更新しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

RDMP-4 製造業者は、サードパーティーコンポーネントの EOL を管理するための計画を有しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

### 2.3.18 ソフトウェア部品表（SBOM）

ソフトウェア部品表（SBoM）には、機器に組み込まれるすべてのソフトウェアコンポーネントの一覧で、医療提供者による運用上セキュリティを計画する目的のために記載する。このセクションは、RDMP セクションの管理をサポートする。

MDS2 は、ソフトウェアコンポーネントを説明するための基準又は方法を規定していない。MDS2 は、機器の製造業者に対し、本製品に使用する方法又は基準を説明するよう求めている。コンポーネントを説明するためのその他の基準がある。例として、これらに限定されないが、ISO 19770-2 及び NISTIR 8060 がある。

SBoM に製造業者の方針および慣行に従った機密情報が含まれている場合、その全部または一部を秘密保持契約の対象とすることができる。

SBOM-1　本製品の SBoM はあるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： SBoM をどのように利用できるか、また制限があるかを「Note」に示す（例：機密保持契約）。例えば、SBoM は表として MDS2 書式に直接組み入れることができる。または、外部ハイパーリンクを使用すると、医療提供者がオンライン版に接続することができます。これらの例はすべてを含む包括的なものではない。

SBOM-2　SBoM は、ソフトウェアコンポーネントの説明において標準または共通の方法に従っているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SBOM-2.1　ソフトウェアコンポーネントは特定されているか?

SBOM-2.2　ソフトウェアコンポーネントの開発者/製造業者を特定しているか?

SBOM-2.3.　ソフトウェアコンポーネントのメジャーバージョン番号が特定されているか?

SBOM-2.4　その他の記述的要素が特定されているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス：記述的要素（例：パッチタグ、ソフトウェア ID タグ）に関する追加の詳細は、ISO/IEC 19770-2:2015、ソフトウェアパッケージデータ交換（SPDX）2.1 に記載されている。

SBOM-3　機器には、機器にインストールされたソフトウェアコンポーネントのリストを作成するために利用可能なコマンドまたはプロセス方法が含まれているか? 「Yes」の場合、詳細または参照先を「Note」に記載する。

SBOM-4　SBoM の更新プロセスはあるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

### 2.3.19 システムとアプリケーションの堅牢化（SAHD）：

機器は、サイバー攻撃やマルウェアに強いものである。

SAHD-1 **機器**は業界基準に従って堅牢化しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SAHD-2 機器はサイバーセキュリティの認証を受けているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SAHD-3 機器はソフトウェアの完全性チェックに何らかのメカニズムを使用しているか?

ガイダンス： オプションで、アプリケーションプログラム、システム設定、及び/又は**機器**データの変更を保護するために使われているメカニズムを「Note」セクションに記述する。

SAHD-3.1 **機器**は、インストールされたソフトウェアが製造業者によって認可されていることを確認するための何らかのメカニズム（例：リリース固有のハッシュキー、チェックサム、デジタル署名など）を使用しているか?

SAHD-3.2 **機器**は、ソフトウェア更新は製造業者が許可した更新であることを確認するための何らかのメカニズム（例：リリースごとのハッシュキー、チェックサムなど）を使用しているか?

SAHD-4 所有者/操作者はソフトウェアの完全性チェック（すなわち、システムが変更または改ざんされていないことを確認する）を実施できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 典型的なアウトプットを「Note」に示す。

SAHD-5 システムは、ファイルレベル、患者レベル、またはその他のタイプのアクセス制御を実行できるように設定できるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 「Note」にファイルレベルのアクセス制御の概要を記載すること（例：**ユーザ**アクセスと管理者アクセス、リモートとローカルアクセスなど）。

SAHD-5.1 機器は、役割ベースのアクセス制御を提供しているか?

SAHD-6 製造業者は、システム納入時にシステムまたはユーザアカウントを制限または無効化しているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SAHD-6.1 初期設定後、エンドユーザが設定可能なシステムまたはユーザアカウントはあるか?

SAHD-6.2 これには、サービス技術者などの特定のシステムまたはユーザアカウントを最小特権アクセスに制限することが含まれるか?

SAHD-7 **機器**の**用途**に必要のないすべての共有リソース（例：ファイル共有）は、無効になっているか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 共有リソースがシステム納入時に製造業者によって無効化されているか、または初期設定後にエンドユーザによって設定可能であるかどうかを「Note」に示す。

SAHD-8 **機器**の**用途**に必要のないすべての通信ポート及びプロトコルは無効になっているか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： ポートまたはプロトコルのいずれかが、システム納入時に製造業者によって無効になっているか、または初期設定後にエンドユーザによって設定可能になっているかどうかを「Note」に示す。

SAHD-9 **機器**の**用途**に必要のないすべてのサービス（例：Telnet、ファイル転送プロトコル（FTP）、Internet Information Server（IIS）など）は削除/無効にされていないか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 製造業者によって削除/無効にされている不必要なサービスがある場合（**機器**の設置時、又は設置前）、又はエンド**ユーザ**によって無効にされる予定の不必要なサービスがある場合は、「Note」に記載すること。

SAHD-10 **機器**の**用途**に必要のないすべてのアプリケーション（COTS アプリケーション及び OS 付属のアプリケーション、例えば MS Internet Explorer など）は削除/無効にされていないか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 製造業者によって削除/無効にされている不必要なアプリケーションがある場合（**機器**の設置時、又は設置前）、又はエンド**ユーザ**によって無効にされる予定の不必要なアプリケーションがある場合は、「Note」に記載すること。

SAHD-11 機器は管理されていない、またはリムーバブルメディア（つまり、内蔵ドライブやメモリコンポーネント以外のソース）から起動できないようになっているか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： **機器**で受け入れられる外部メディアを「Note」に記載する。

SAHD-12 物理的ツールを使用せずに、許可されていないソフトウェアやハードウェアを**機器**にインストールすることはできるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 機器のユーザ/所有者によるハードウェアまたはソフトウェアのインストールに関する制限を「Note」に示す。

SAHD-13 製品文書には、ユーザによる運用ネットワークセキュリティスキャンに関する情報が含まれているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SAHD-14 機器はデフォルト設定以上に堅牢化できるか?

SAHD-14.1 堅牢化を強化するためのベンダー指示があるか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

SAHD-15 システムは起動中に BIOS または他のブートローダへのアクセスを防止できるか?

SAHD-16 機器の堅牢化に用いられる 2.3.19 に含まれていない追加の堅牢化方法を持っているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

### 2.3.20 セキュリティガイド（SGUD）：

機器の操作者と管理者、及び製造業者の販売とサービスに関するセキュリティガイダンスの有無。

SGUD-1　機器には所有者/操作者用のセキュリティ文書が含まれているか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 製造業者が専用のセキュリティ文書を用意している、又は**ユーザ**マニュアル、サービスマニュアル、その他の文書内で**ユーザ**に利用できるようにセキュリティ文書を用意している場合は、「Yes」とする。本文書の参照先を「Note」に記載する。

SGUD-2　機器は、機器又はメディアからデータを永続的に削除する機能を有し、その説明を提供するか?「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 製造業者が**ユーザ**向けの何らかの文書内でそのような説明を用意している場合は、「Yes」とする。仕様（例：HMG InfoSec 規格 5、BSI、NIST800-88）を「Note」に記載する。

SGUD-3　すべてのアクセスアカウントを文書化しているか?

SGUD-3.1　所有者/操作者はすべてのアカウントのパスワード管理を実施できるか?

ガイダンス： すべてのリモートアクセスアカウントまたは施設を特定し、そのアクセス管理を文書化しているか（例：リモートデスクトッププロトコル（RDP）およびインテリジェントプラットフォームマネージメントインターフェース（IPMI）などのリモートサービスアクセスプロトコル）？ユーザは、これらのアクセス方法のパスワードを有効化、無効化、管理できるか?

SGUD-4　製品には、機器に推奨される補完的管理策に関する文書が含まれているか?

### 2.3.21 健康データストレージの機密性（STCF）：

許可されていないアクセスを保証する機器の能力は、機器またはリムーバブルメディアに保存された個人識別可能情報およびその他の保護された個人情報（PPI）の完全性および機密性を損なわない。

STCF-1　**機器**は保存されているデータを暗号化できるか？「Yes」 の場合、詳細または参照先を「Note」に記載する。

ガイダンス： 利用可能な暗号化アルゴリズムを「Note」に記載または参照先を記載する。この質問はローカルデータを指す。ネットワーク通信またはメディアエクスポート前のデータの暗号化については、セクション 2.3.22 の質問 TXCF-2 を参照。

STCF-1.1　すべてのデータは暗号化されているか、その他の方法で保護されているか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

ガイダンス： 暗号化が選択的な場合、すべての操作データ（設定、手順、コンフィギュレーション等）または特定の種類のデータ（例：患者記録のみ）のみを網羅しているか?

STCF-1.2　データ暗号化機能はデフォルトで設定されているか?

STCF-1.3　暗号化を設定するための説明は顧客に提供されているか?

STCF-2　暗号化キーを変更または設定できるか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

STCF-3　データは機器にあるデータベースに保存されているか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

STCF-4　データは機器外部のデータベースに保存されているか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

### 2.3.22 通信の機密性（TXCF）：

通信された個人識別可能情報の機密性を保証する機器の機能。

TXCF-1　**個人識別可能情報**は、ポイント・ツー・ポイント専用ケーブルでのみ通信できるか?

ガイダンス： 質問の意味の説明：ポイント・ツー・ポイント専用ケーブル経由とは、一般公衆にアクセスできないケーブルシステムである（すなわち、それが物理的に管理された場所、例えば検査室、通信室又は建物内部にある）。

TXCF-2　ネットワークまたは**リムーバブルメディア**を介して伝送する前に、**個人識別可能情報**を暗号化しているか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

ガイダンス： 該当する規格を「Note」に記載する。

TXCF-2.1　データがデフォルトで暗号化されていない場合、顧客は暗号化オプションを設定できるか?

TXCF-3　**個人識別可能情報**伝達は、ネットワーク通信先の固定リストに限定されているか?

ガイダンス： 固定リストとは、**機器**ごとに接続と接続の性質を制限する明示的なメカニズム。

TXCF-4　接続は認証されたシステムに限定されているか? 「Yes」 の場合、「Note」に説明するか、参照先を記載する。

ガイダンス： 提供される情報には、制限がどのように達成されるか、さらにアクセス管理がサポートされる場合はどのような方法がサポートされるかを記載する。

TXCF-5　安全な通信方法がサポート/実施されているか（DICOM、HL7、IEEE11073）？「Yes」 の場合、「Note」に説明するか、参照先を記載する。

### 2.3.23 通信の完全性（TXIG）：

通信する個人識別可能情報の完全性を保証する機器の機能。

TXIG-1　**機器**は通信中にデータが変更されないようにする目的で何らかのメカニズム（例：デジタル署名）をサポートしているか？「Yes」 の場合、「Note」に説明するか、参照先を記載する。

TXIG-2　機器には、外部ケーブルで接続された複数のサブコンポーネントが含まれているか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

ガイダンス： 可能であれば、「Note」にシステム図の参照先を記載すること。DOC-10 参照。

### 2.3.24 リモートサービス（RMOT）

リモートサービスとは、機器の保守活動をサービス要員がネットワーク又は他のリモート接続を介して行うことをいう。

RMOT-1　機器は、機器の分析または修理のためのリモートサービス接続を許可するか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

RMOT-1.1　機器は、所有者/操作者が機器の分析や修理のためのリモートサービスセッションを主導できるようにしているか?

RMOT-1.2　リモートセッションが有効、アクティブであるインジケータはあるか?

RMOT-1.3　リモートセッション中に患者データに機器からアクセスまたは閲覧することができるか?

RMOT-2　機器は、予測メンテナンスデータのためにリモートサービス接続を許可または使用するか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

RMOT-3　機器には、リモートアクセス可能なその他の機能（例：ソフトウェアの更新、リモートトレーニング）があるか?「Yes」 の場合、「Note」に説明するか、参照先を記載する。

### 2.3.25 他のセキュリティ考察（OTHR）

このセクションは、本文書の他の場所に分類されていないセキュリティリスクの考慮事項または管理（補完的管理策を含む）を製造業者が入力すること。

# セクション3 - 他の規格との比較

MDS2 における質問は、IEC TR80001-2-2:2012、ISO27000 及び NIST 800-53 の対応するセクションにマッピングされている。このマッピングは情報提供のみを目的としており、製造業者が参照する必要はない。より一般的で非常に有用なクロスウォークは、DHHS 公民権局 （https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf）の「HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework」で見ることができる。

### 3.1 IEC TR80001-2-2:2012

IEC TR80001-2-2:2012 技術報告書は、医療施設ネットワークのリスクマネジメントの一環として重要なセキュリティ機能のリストを特定している。このリストはセクション 5 セキュリティ能力にあり、MDS2[MDS2] の質問カテゴリと密接に整合している。

| IEC TR80001-2-2:2012 セクション | IEC TR80001-2-2 2012 名称 | MDS2 カテゴリ | コメント |
|---|---|---|---|
| 5.1 | ALOF | ALOF | |
| 5.2 | AUDT | AUDT | |
| 5.3 | AUTH | AUTH | |
| 5.4 | CNFS | -- | ユーザ設定の質問を SAHD、SGUD、CSUP、PAUT に移動 |
| 5.5 | CSUP | CSUP | |
| 5.6 | DIDT | DIDT | |
| 5.7 | DTBK | DTBK | |
| 5.8 | EMRG | EMRG | |
| 5.9 | IGAU | IGAU | |
| 5.10 | MLDP | MLDP | |
| 5.11 | NAUT | NAUT | |
| 5.12 | PAUT | PAUT | |
| 5.13 | PLOK | PLOK | |
| 5.14 | SAHD | SAHD | |
| 5.15 | SGUD | SGUD | |
| 5.17 | STCF | STCF | |
| 5.18 | TXCF | TXCF | |
| 5.19 | TXIG | TXIG | |
| -- | -- | RMOT | リモートサービスおよび管理に関する質問を追加 |
| -- | -- | SBOM | ソフトウェア部品表の質問を追加 |
| -- | -- | CONN | 接続能力を追加 |
| -- | -- | RDMP | ソフトウェアロードマップの質問を追加 |

| IEC TR80001-2-2:2012 セクション | IEC TR80001-2-2 2012 名称 | MDS2 カテゴリ | コメント |
|---|---|---|---|
| -- | -- | MPII | 個人識別可能情報に関する質問の管理を追加 |

### 3.2 ISO/IEC 27002:2013

MDS2 の質問と ISO/IEC27002:2013 規格との間のマッピングは、セキュリティ分析における機器製造業者および機器ユーザの補助として提供される。

機器の製造業者が機器の設計及び実施の基礎としてすでに ISO/IEC27002:2013 規格を使用している場合、ISO/IEC27002:2013 規格の関連セクションを、その対象者に関する MDS2 質問に割り当てる。

機器のユーザが、ネットワークを管理するための基盤として ISO/IEC27002:2013 規格ファミリーを使用している場合、ISO/IEC27002:2013 規格の関連セクションをその対象者に関する MDS2 質問に割り当てる。

### 3.3 NIST 800-53 r4

a. MDS2 の質問と NIST 800-53 r4 標準との間のマッピングは、セキュリティ分析における機器製造業者および機器ユーザの補助として提供される。

機器の製造業者がすでに機器の設計及び実施の基礎として NIST800-53 r4 を使用している場合、NIST800-53 r4 の関連セクションを、その対象者に関する MDS2 質問に割り当てる。

機器ユーザがネットワーク管理の基礎として NIST800-53 r4 を使用している場合、NIST800-53 r4 の関連セクションをその対象者に関する MDS2 質問に割り当てる。

# セクション4 - MDS2 2013 と 2019 の相違

MDS2 の 2019 版は、今後 2013 版に取って代わる。

### 4.1 文書体系の変更

文書体系が若干変更された。

a. 質問の番号が変更された。これは現在、IEC TR80001-2-2:2012 規格の番号付けに対応しており、若干の軽微な差異がある。

### 4.2 質問の変更

質問の明確化及び編集上の改訂に加え、質問のセクションに対してより実質的な以下の変更を行った。

**MPII** 用語例を更新し、ウェアラブルのような新しいタイプの機器に対処するために質問を拡大した。

**ALOF** 近接機器などの新しい自動ログオフ技術を追加した。

**AUDT** 1) API アクセスおよびデータアクセスの詳細、2) 時刻同期、3) 監査ファイルのインポート/エクスポートについての質問を追加。リモートサービスを RMOT に移行。

**CNFS** 本セクションを厳格化し、ALOF、AUTH、CVSUP、MLDP、NAUT、PAUT、SAHD、及び SGUD を含む他のカテゴリに含まれる顧客設定管理に関する質問を実施。

**AUTH** 認証タイプの説明を更新。

**CSUP** 本セクションを大幅に改訂。更新の許可および能力に関する詳細を記載。

**DIDT** 利用可能な非識別化標準プロファイルの遵守に関する質問を追加。

**DTBK** 患者情報以外のデータのカテゴリに対応するため、さらに質問を追加。例えば、システム設定情報バックアップが含まれる。

**EMRG** 大きな変化なし

**IGAU** 大きな変化なし

**MLDP** 1) どのような機能を誰が実行できるか、2) どのようにログと通知に対処するか、3) どのようにネットワークプローブに対処するか、4) ホワイトリストがサポートされているかについて質問を追加。

**NAUT**　アクセス制御能力について質問を追加。

**PAUT**　多要素認証機能について質問を追加。

**PLOK**　より多くの種類のロックおよび物理的管理について質問を追加。

**RDMP**　サードパーティーライブラリおよびコンポーネントの使用に関する質問。

**SAHD**　システムの検証、サイトの設定可能性、更新プロセスの詳細に関する質問を追加。

**SGUD**　アクセス制御に関する質問を追加。

**STCF**　質問を改訂し、カテゴリの詳細を追加。

**TXCF**　機器認証に関する質問を追加。

**RMOT**　リモートサービス及び管理能力について質問するため、新たなセクションを追加。

**SBOM**　ソフトウェア部品表について質問するために新しいセクションを追加。

**CONN**　接続能力について尋ねる新しいセクションを追加。

**RDMP**　ソフトウェアロードマップについて質問するために新たなセクションを追加。

**OTHR**　機器の追加製造業者情報のプレースホルダーとして新しいセクションを追加。

### 4.3　MDS2 書式の変更

書式は、紙ベース様式を維持することのないスプレッドシートになっている。作成者とユーザの両方がスプレッドシートプログラムの方にアクセスし、使用することを想定している。

スプレッドシートは、CSV 書式を使用して書式を作成、保存、処理できるように構成されている。これは、MDS2 書式の作成、評価及び保存のためのデータベース、統計解析ツール、ビジネス解析ツール等の使用を可能にするためである。このようなツールの使用は不要である。MDS2 書式は、スプレッドシートプログラムとともに作成し、使用することができる。これにより、MDS2 作成プロセスのさらなる自動化が可能になる。

CSV の構成は以下の通り。

a. すべての説明は列 1 を空欄のままにする。

b. すべての質問には、列 1 に識別タグが付いている。
c. 回答は主に C 列と D 列だが、場合によっては C 列から G 列を使用する。
d. 各質問について、IEC TR80001-2-2:2012、NIST 800-53 および ISO27000 ファミリー規格の関連セクションにクロスウォークを提供する。これらは H 列、I 列、J 列にある。

### 4.4 書式例

完全に現実的ではないが、妥当であると思われる医療機器について、書式例を示す。これは例を修正して使用する人が使いやすいようになっている。

# セクション5 - MDS2 書式

現在の HN1 MDS2 ワークシートにアクセスしてダウンロードするには、ウェブブラウザに以下を入力する。

https://www.nema.org/Standards/ComplimentaryDocuments/MDS2-Worksheet.xlsx

NEMA は、本セクションの書式のコピーを作成し、使用することを許可する。MDS2 文書の全部又は一部を翻訳する場合は、元のセクションラベルを維持すること。