HIMSS/NEMA規格HN 1-2013

Manufacturer Disclosure Statement for Medical Device Security

医療機器セキュリティのための製造者開示説明書

発行元

National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
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。

THE HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY（HIMSS）も NEMA も、この文書の内容への適合を監視又は強制する権限も責任もない。HIMSS も NEMA も安全又は健康の目的のために、製品、設計又は設置の認証、試験、若しくは検査を行うものではない。この文書に記載の健康又は安全関連情報への適合の認証若しくは他の言明は、そのいずれに対しても HIMSS 又は NEMA は免責とし、認証した者又は言明した者が全責任を負う。

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者開示説明書（MDS^{2}書式）及びこの書式の記入方法の指示書から構成されている。医療提供者は、医療機器及びシステムによって送信、又は保持される個人情報の保護に関連する脆弱性及びリスクを査定する必要があるが、MDS^{2}書式の意図は、この査定を支援する重要情報を医療提供者に提供することである。セキュリティのリスクアセスメントは組織全体に及ぶので、この文書が重視するのは個人情報を保持又は送信する医療機器に関するセキュリティリスクアセスメントプロセスの要素に限るものとする。標準化した書式には次の利点がある。1）製造者は、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者から提供されたとき、迅速に検討できる。

製造者が記入したMDS^{2}書式は次のようにすることが望ましい：

(1) 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、有効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。

(2) 個々の機器モデルの技術的なセキュリティ関連属性に取り組む機器固有の情報を含んでいる。

(3) 医療提供者組織（機器ユーザ／オペレータ）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。この情報要素は必要である。

注意事項—MDS^{2}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。調達仕様書を書くためには、セキュリティに関するより深い広い知識（個々の施設／医療提供者の状況を考慮して）及び医療の使命が必要である。

医療提供者の学際的なリスクアセスメントのチームは、製造者がMDS^{2}書式で提供する情報を、ケアデリバリ環境（例えば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管理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「MDS^2 v. 1.0 (2004-11-01)」として公表され、2008年にHIMSS/NEME合同規格「HIMSS/NEMA Standard HN 1-2008」として公表された。

*Health Insurance Portability and Accountability Act.

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管理のアプリケーションを扱い、リスク管理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 80001-2-2Guidance 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部品の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MDS^{2}イニシアチブの第一の目的と一致しているため、HIMSSとNEMAは、IEC/TR 80001-2-2の19セキュリティカテゴリに合わせするために、製造業者が提供するMDS^{2}情報の拡張と再カテゴリー化を実施している。

HIMSSとNEMAはMDS^{2}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評価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、ユーザー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。

Vice President, Engineering
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209

MDS²2008 年版からの変更点

１）MDS² を International Electrotechnical Commission（IEC ）規格 80001−1 のサプリメント IEC / TR 80001-2-2 、*Guidance for the communication of medical device security needs, risks and controls* に合せる。

a）(2008)MDS² の質問の順番と番号が変更され、質問は現在 MANAGEMENT OF PRIVATE DATA か MDS² フォームの SECURITY CAPABILITIES の 19 のカテゴリーのいずれかに該当する見出しの下のどちらかに配置されている。

b）デバイス製造業者に要求される MDS² データの量は IEC / TR 80001-2-2 の 19 のセキュリティ機能により適切に対処するために増加している。

c）MDS² 用語の定義は、適用可能な IEC 80001 で使用した定義と一致するように追加または更新されている。

旧 MDS² 版の MDS² セキュリティ関連の質問のすべては変更なく（あるいはわずかな変更で）、この最新版に残っている。2008 MDS² の質問と 2013 MDS² の質問の対比は、Annex で示されている。

２）非ローカライズ

いくつかの地域固有のリファレンス及び標準は、削除されている、又はより汎用的/地域の固有性が低いリファレンスに置き換えられている。米国 HIPAA 法で定義されている「保護された健康情報」（PHI）という用語は、この MDS² 改訂版ではより IEC80001 で定義されている「個人情報」に置き換えられている。

セクション 1

一般

1.1. 適用範囲

MDS^2 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問題を管理することを支援するために意図されている。MDS^2 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. セキュリティ管理プロセスにおける医療提供者の役割

医療提供者組織は、有効なセキュリティ管理を提供することに最終的責任をもつ。機器製造者は、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：

- 製造者の機器が保持/送信するデータのタイプ；
- 製造者の機器がデータを保持/送信する方法；
- 製造者の機器に内蔵されるセキュリティ関連の特徴。

医学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—それらの大部分は実際の機器にとって外部的である。

1.1.2. セキュリティ管理プロセスにおける医療機器製造者の役割

製造者が医療機器セキュリティに及ぼし得る最大の影響は、有効なセキュリティプログラムを保持し、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。医療機器製造産業は、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。

1.2. 参考文献

次の参考文献は、推薦図書、裏付け資料、関連の出版物である。

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

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).

EC Data Protection Directive, 95/46/EC (EU 95/46), 1995.

個人情報の保護に関する法律（2003年成立、法律第57号、日本）

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

Guide for Information Security for Biomedical Technology: A HIPAA Compliance Guide, May 2004, American College of Clinical Engineering (ACCE)/ECRI.

1.3. 定義

管理的保護手段： 個人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、管理的な行為、方針及び手続き。

アンチマルウェア：　アンチウイルスソフトウェアを参照すること。
アンチウイルスソフトウェア：　全ての主要なタイプのマルウェアを認識し、マルウェアインシデントを抑止することでコンピュータやネットワークを監視するプログラム。 ウイルススキャナを参照すること。

監査証跡： セキュリティ監査を容易にするために集められ潜在的に使用されるデータ

生データ： 個人の身体的な特徴又は反復可能な行動（例えば掌紋、網膜走査、虹彩走査、指紋パターン、顔の特徴、DNA 塩基配列特性、声紋、手書きの署名）の測定から人間を識別する。

機器： ハードウェア、ファームウェア、及び/又は（単なる）ソフトウェアなどを含む製品/システム。この MDS^2 文書では、文脈上異なることが明確である場合を除いて、「機器」は MDS^2 書式で製造者が対応する、医療機器（製造者の製品）を指す。「医療機器」を参照。

電子媒体： （1）電子記憶媒体。例えばコンピュータ内のメモリデバイス（ハードディスクドライブ）及び着脱／搬送可能なディジタルメモリ媒体、例えば磁気テープ又は磁気ディスク、光ディスク、又はディジタルメモリーカード。（2）既に電子媒体内にある情報を交換するために用いられる送信媒体。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（関係者だけにアクセスできる情報を用いてビジネスをリンクするインターネット技術を使用する）、賃貸された回線、ダイアルアップ回線及び構内網、並びに着脱／搬送可能な電子記憶媒体の物理的な移動。一部の送信、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、電子媒体による送信ではない。なぜならば交換される情報が送信前には電子媒体の形で存在していないからである。
保護された電子健康情報**（ePHI）：** [米国 HIPAA 法、45 CFR Part 160.103 で定義されている個人]特定できる健康情報（IIHI）であって、（1）電子媒体を用いて送信されるか又は（2）電子媒体の中に記憶されるもの。

緊急アクセス：　装置の持っているアクセスコントロール機能を回避して、装置ユーザが緊急(非常)の状況で個人のデータに速く容易にアクセスすることができるプロセスかメカニズム。

個人特定可能な健康情報（IIHI）： 個人特定できる健康情報とは健康情報の部分集合である。例えば個人から集められた個人基本情報を含む情報である。そして：（1）医療提供者、保健計画、雇用者又は医療情報センターによって作成されるか受け取られる情報；及び（2）次のことに関する情報である。個人の過去、現在、又は将来の身体的・精神的な状態；個人への医療の提供；又は個人の医療提供に対する過去、現在又は将来の支払；及び（i）個人を特定するもの；又は（ii）個人識別に使用し得ると考える妥当な根拠があるもの。

使用目的： 製造者が提供している仕様、指示、及び情報に従って、意図されている製品、プロセス、又はサービスの用途。
[ISO 14971: 2007, definition 2.5]

マルウェア：　悪意のあるソフトウェア。システムに、通常は隠れて挿入されるプログラムで、犠牲となるデータ、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、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)*
医療機器： 計器、装置、道具、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、資料、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者によって意図されているもの：

- 疾病の診断、予防、監視、処置、又は緩和、
- 負傷の診断、監視、処置、緩和又は補償

- 解剖学又は生物学的過程の検査、代替、変更、又は支援
- 生命の維持や支援
- 受胎の調整
- 医療機器の殺菌
- 人体から得た試料の体外検査により、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、薬理学、免疫学、或いは代謝の手段によってもたらさないが、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。

操作者： 機器を取り扱う人。

暗証番号（PIN）： 個人に割当てて、同一性を立証するため使用される数字又は記号。

個人情報： 一意に特定された、又は特定できる人に関する情報。

物理的な保護手段： 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。

プライベートデータ： 特定された、又は特定可能な人に関連する情報。

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。

遠隔サービス： 支援活動（例えば試験、診断ルーチン、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（例えばモデム、ネットワーク、インターネットを介する遠隔アクセス）。

着脱可能な媒体： 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媒体。

リスクアセスメント： **プライベートデータの整合性、可用性、機密性への潜在的なリスクや脆弱性の正確かつ徹底的な分析を行う。**
リスクマネジメント： （1）リスクを査定し、容認可能な水準までリスクを減らす手段を講じ、そのリスクの水準を維持するための継続的プロセス。（2）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。

セキュリティ機能： データ及びシステムの信頼性、整合性、可用性、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。

技術的な保護手段： 「個人情報」を保護し、その情報へのアクセスを制御する技術、方針及び手続き。

トークン： ユーザが携行する物理的な認証機器（例えばスマートカード、SecureID^{tm}、など）。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、多くの場合、PIN と組み合わされる二要素認証方式。

ユーザ：「操作者」を参照。

ウイルス：「マルウェア」を参照。

ウイルススキャナ：ウイルスコンピュータプログラム、又は他の種類の不正ソフトウェア（例えばワーム及びトロイの木馬）を検出し、その存在を警告し、それが保護コンピュータに影響することを防ぐコンピュータプ

ログラム（「アンチウイルスソフトウエア」）。不正ソフトウェアは、しばしば、ユーザの想定外の望まれない副作用を起こす。

脆弱性：機器の手続き、設計、実施､内部制御の欠点又は弱さを指し、実行される（偶然に起こるか意図的に実行される）と、その結果セキュリティ違反又は機器のセキュリティ方針の違反になるもの。

1.4. 略語

CD Compact Disk
CF Compact Flash
COTS Commercial Off-The-Shelf
DVD Digital Versatile Disk
IP Internet Protocol
LAN Local Area Network
OS Operating System
ROM Read Only Memory
SD Secure Digital
USB Universal Serial Bus
VPN Virtual Private Network
WAN Wide Area Network
WiFi Wireless Fidelity

Section 2
MDS² 書式の入手、使用、記入の指示

2.1. MDS² 書式の入手（医療提供者）

多くの機器の記入済みの MDS² 書式は、機器製造者（例えば製造者ウェブサイト）から直接入手できる。

注－製造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 書式の最上部の適切な欄に製造者とモデル情報を記入し、この書式と指示書を製造者の法令順守担当部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. セクション 1

最初の二つのセクションは機器を特定するため及び、機器の保持／送信するデータのタイプ、データの保持／送信の方法などを説明するために使用されている。

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「はい」の答え）は、これは暗黙か明示かを問わず、製造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。

2.2.2. 解説

製造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。

2.2.3. セクション 2

MDS2 (SECURITY CAPABILITIES)の最終セクションには、機器の特定のセキュリティ関連の機能に関する情報が含まれる。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る。

2.3. MDS² 書式の記入（製造者）

2.3.1. 一般

製造者は、MDS² 書式で要求される機器の保持／送信するデータのタイプ、データの保持／送信の方法、機器に組み入れられた他のセキュリティ関連の特徴に関する必要な記述的情報などすべての情報を、適切な要求組織に適宜提供しなければならない。

2.3.2. MDS² 書式記入のガイダンス

機器の説明に関するセクション：

機器カテゴリ：これは文章を自由に記入する欄である。製造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して欲しい。

機器モデル：これは文章を自由に記入する欄である。製造者は、市販される機器の名を記入して欲しい。

文書識別コード：文書識別コードは機器文書化を追跡するために内部で使用される製造者のユニークなタグである。

製造者の連絡情報：この情報は、書式の最終版の責任者に対する連絡方法を指定する。

ネットワーク環境での機器の用途：製造者は、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できる。

個人情報の管理に関するセクション： 製造者はすべての質問に「はい」、「いいえ」、「N/A」（該当なし）、又は「注記を参照」で答えなければならない。

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

A. この装置は個人情報（保護された電子健康情報（ePHI）を含む）を表示、送信、又は保持できるか？

B 装置で保持できる個人情報要素のタイプ：

B.1 患者基本情報（例えば名前、番地、住所、一義的な ID 番号）？

B.2 医療記録（例えば医療記録番号#、会計書番号#、検査又は治療日、装置識別番号）？

B.3 診断/治療（例えば特徴を識別する写真/放射線写真、検査結果又は生理学のデータ）？

B.4 装置ユーザ/操作者によって入力された公開自由文？

B.5 生体データ？

B.6 個人の財務情報（例えばクレジットカードの番号、医療保健の情報、etc）？

C. 個人情報の保持 - 機器で可能なこと：

C.1 揮発性メモリで個人情報を一時的に保持する（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）？

C.2 内部記録媒体に個人情報を確実に格納する？

C.3 個人情報を他のシステムとインポート/エクスポートする？

C.4 停電時に個人情報を保持できる？

D. 個人情報の送信、インポート/エクスポートのための機能：機器は次のことができるか。

D.1 個人情報を表示する（ビデオディスプレイなど）？

D.2 個人情報を含んでいる報告書又は画像を印刷する？

D.3 着脱可能な媒体（ディスク、DVD、CD-ROM、テープ、CF/SD カード、メモリスティックなど）から個人情報を取得する？又はそれらに記録する？

D.4 個人情報の送信/受信又はインポート/エクスポートを専用ケーブルを介して行う？（例えば、IEEE 1073、シリアルポート、USB、FireWire）

D.5 個人情報の送信/受信を有線ネットワーク接続を介して行う？（例えば、LAN、WAN、VPN、イントラネット、インターネット）

D.6 個人情報の送信/受信を統合ワイヤレスネットワーク接続を介して行う？（例えば、WiFi、Bluetooth、赤外線など）

D.7 スキャンを介して個人情報をインポートする？

D.8 その他？

セキュリティ機能に関するセクション:

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、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。

製造者はすべての質問に、「はい」、「いいえ」、「N/A」（該当なし）、又は「注記を参照」のいずれかで答えなければならない。ただし他の答え方を質問が要求している場合を除く。

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

製造者は次のガイダンスに従って質問に答えなければならない。

次の説明、ガイダンスは製造業者が設問に答える際の助けとなるため提供されています。:

注ーこのサブセクション中の番号（下記）は、MDS^{2}書式の質問番号と同じである。

1 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。

1-1 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（例えば、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] 機器は既定で、又は設定によって、常に

- 一定時間操作していない状態が続くと、再認証を強制する、又は
- 一定時間操作していない状態が続くと、ユーザをログオフさせずにユーザアクセスを正しく禁止できるパスワード保護されたスクリーンセーバを起動する

注記セクションを使用して、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/その方法を記載できる（例えば、適切なユーザセキュリティ警告/通知を使ってセッションごとに、又は全体で）。)

1-1.1 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？（注記に時間（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？注記セクションを使用して、調整可能な自動ログオフ/スクリーンロックを備えた機器で以下の設定が可能かどうか示すこと。

- ユーザが決めた時間
- 特定の役割による設定（例えば、管理者、ユーザ）

1-1.2 自動ログオフ/スクリーンロックはユーザが手動で呼び出せるか（例えば、ショートカットキー）？

[ガイダンス] ユーザ/操作者は自動ログオフ/スクリーンロックをショートカットキーの組合せ（CTRL-ALT-DELETE など）で呼び出せるか？

2 監査コントロール（AUDT）: 機器上の活動を正しく監査する機能。

2-1 医療機器は監査証跡を作成できるか？

[ガイダンス] 答えが「いいえ」の場合、2.2.1～2.3.2 の答えは「N/A」とし、セクション 3-1 に進む。もし可能ならば、ログの個人情報イベントに記載されているデータ主体が記されていることを注記に記載してください。

2-2 次のイベントのうち、監査ログに記録されるイベントを示す。

2-2.1 ログイン/ログアウト

2-2.2 データの表示/提示

[ガイダンス] 監査証跡は、表示、印刷、その他データを提示する方法を記録するか？

2-2.3　データの作成/変更/削除

[ガイダンス]「はい」の場合、注記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）を記録するのか示すこと。

2-2.4　着脱可能な媒体からのデータのインポート/エクスポート

[ガイダンス]「はい」の場合、注記でこれらデータ操作のどの形式を記録するのか示すこと。

2-2.5　外部（例えば、ネットワーク）接続を介したデータの受信/送信

[ガイダンス]「はい」の場合、注記でこれらデータ操作のどの形式を記録するのか示すこと。

2-2.5.1 遠隔サービス活動

2-2.6　その他のイベント？（注記セクションで説明）

[ガイダンス]「はい」の場合、注記で他に記録するデータ操作の形式を示すこと。

2-3　監査ログに記録されている各イベントを特定するために使用する情報を示す

2-3.1　ユーザ ID

2-3.2　日時

[ガイダンス]デバイスの時間がどのようにセットされているかについて注記に記載してください。例えば NTP と同期しているなど。

3　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

3-1　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] 機器が許可されていないアクセスを禁止できる場合は、注記にアクセスを禁止するために機器で使用されている物理的もしくは技術的な保護手段を示す（パスワード、バイオメトリックス、キーカードなど）。

3-2　ユーザには、「役割」に基づいてアプリケーション内で異なる権限レベルを割り当てられるか（例えば、ゲスト、標準ユーザ、上級ユーザ、管理者など）？

3-3　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（例えば、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]注記に、機器が複数の権限付きアカウントをサポートしているかどうか示す（例えば、管理者、ルート）。

注記に、製造者が管理者アカウントの使用に関してユーザに何らかの制限を課しているかどうか示す。

4　セキュリティ機能の構成（CNFS）ユーザのニーズを満たすため、デバイスのセキュリティに関する能力を構成／再構成するする能力

4-1　機器の所有者/操作者は製品のセキュリティ機能を再構成できるか？

[ガイダンス]注記に、製造者が製品のセキュリティ機能の再構成に関してユーザに何らかの制約を課しているかどうか示す。

5　サイバーセキュリティ製品のアップグレード（CSUP）セキュリティパッチを保守要員、リモート保守要員、認定された顧客のスタッフがインストールもしくはアップグレードする能力

5-1　関連する OS 及び機器のセキュリティパッチが知られ/利用可能になった時点で機器に適用できるか？

[ガイダンス]製造者が OS 及び機器のセキュリティパッチを適用することをユーザに許可しない場合、又はこの活動に制約を与えている場合は、これら制約の存在を注記に記載すること。

製造者は、注記で直接制約について説明するように選択できるほか、これら制約の説明が記載されている外部文書の参照先を示す、又は単に「製造者の制約/制限に関する情報は要望に応じて提供可能」と記載してもかまわない。

5-1.1 セキュリティパッチ又は他のソフトウェアを遠隔インストールすることができるか？

[ガイダンス]製造者が OS 及び機器のセキュリティパッチ又はその他のソフトウェアをリモートでインストールすることをユーザに許可しない場合、又はこの活動に制約を与えている場合は、これら制約の存在を注記に記載すること。

製造者は、注記で直接制約について説明するように選択できるほか、これら制約の説明が記載されている外部文書の参照先を示す、又は単に「製造者の制約/制限に関する情報は要望に応じて提供可能」と記載してもかまわない。

6 健康データの匿名化（DIDT）： 人物の識別を可能にする情報を直接削除する機器の機能。

6-1 機器は個人情報を匿名化する完全な機能を提供しているか？

[ガイダンス]匿名化プロセスが特定の匿名化標準/ガイドラインを参照している/従っているかどうかを注記に記載すること。

匿名化手順が設定可能かどうかも記載すること。

7 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、又はソフトウェアの損傷や破壊後に復旧できる機能。

7-1 機器は完全なデータバックアップ能力を持っているか（例えばテープ、ディスクのようなリモートストレージや着脱可能なメディア上へのバックアップ）？

[ガイダンス]これは、リモートストレージや着脱可能な媒体（例えば光ディスク、磁気ディスク、テープなど）上に情報をバックアップする統合された機能やオプションを指す。

該当する場合は、データのバックアップ/災害復旧に関する制限や制約について注記に記載すること。

8 緊急アクセス（EMRG）：保存されている個人情報に即座にアクセスする必要がある緊急事態で、ユーザが個人情報にアクセスできる機器の機能。

8-1 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？

[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。

該当する場合は、セクション 2、（例、質問 2.2.6）緊急アクセス事例を記録する機器の機能について記載すること。

製造者はこれについて、質問 8.1 の注記で記載することもできる：

- 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
- 「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（例えば、許可されたユーザのログインなしで取得されたデータ）

9 健康データの完全性と真正性（IGAU）：機器で処理されたデータが許可されていない方法で改変されていない、又は破壊されていないこと、及び入手先が正しいことを機器で保証する方法。

9-1 機器は、暗黙的・明示的なエラー検出/修正技術により、保存されたデータの完全性を保証しているか？

[ガイダンス]この質問は、保存されているデータの完全性のみを指す。一般に、アプリケーション *プログラム又はシステム*への許可されていない変更を禁止する目的のシステムコントロール

に関する情報は、セクション「システムとアプリケーションの堅牢化（SAHD）」の注記に記載すること。

10　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）を効果的に阻止、検出、及び削除する機器の機能。

10-1　機器はマルウェア対策ソフトウェア[又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？

[ガイダンス]製造者は、注記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/構成）について説明するように選択できるほか、これら制約の説明が記載されている外部文書の参照先を示すことができる。

10-1.1 ユーザはマルウェア対策設定を自分で（再）構成できるか？

10-1.2 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]オプションで、マルウェアの検出時にユーザに通知する方法を注記に記述する。

10-1.3 マルウェアが検出された場合は、製造者が許可した人のみがシステムを修理できるか？

[ガイダンス]オプションで、マルウェアに感染したシステムの修理者として許可する人物、又はしない人物に関する制約を注記に記述し、これらの制約の説明が記載されている外部文書の参照を示すことができる。

10-2　機器の所有者はアンチウイルスソフトウェアの「エンジン」をインストール、又は更新できるか？

[ガイダンス]機器のユーザ/所有者にアンチウイルスソフトウェアをインストール又は更新する「技術的」な能力がある場合は「はい」と答える。ただし、製造者がアンチウイルスソフトウェアをインストール又は更新することをユーザに許可していない場合、又はこの活動に制約を与えている場合は、これら制約の存在を注記に記載すること。

10-3　機器の所有者/操作者は、製造者がインストールしたアンチウイルスソフトウェアでウイルス定義を（技術的/物理的に）更新できるか？

[ガイダンス]システムのユーザ/所有者にウイルス定義/「ウイルス署名ファイル」を更新する「技術的な」能力がある場合は「はい」と答える。ただし、製造者がこれらのウイルス署名ファイルの更新をユーザに*許可*していない場合、又はこの活動に制約を与えている場合は、これら制約の存在を注記に記載すること。ホワイトリストを用いる場合、認証されたアプリケーションのリスト（ホワイトリスト）を修正するための所有者／ユーザの権限を制限するならば注記に示しなさい。

11　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。

11-1　機器は、データの送信側と受信側の両方が相互に認識しており、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？

12　個人の認証（PAUT）：ユーザを認証する機器の機能。

12-1　機器は少なくとも 1 ユーザについて、ユーザ固有の/操作者固有のユーザ名とパスワードをサポートしているか？

[ガイダンス]機器がユーザ名とパスワード以外の識別方法を使用できる場合は、注記に簡潔にそのことを記載すること（例えば、「XYZ安全トークンメカニズムを使用する」）。

12-1.1 機器は複数のユーザに対して一意のユーザ固有の/操作者固有の ID とパスワードをサポートしているか？

12-2　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構成できるか（例えば、MS Active Directory、NDS、LDAP など）**[ガイダンス]「はい」の場合**、注記に可能なメカニズムを記載すること。

12-3　機器は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構成できるか？

[ガイダンス]「はい」の場合、注記に詳細を記載すること。

12-4　既定のパスワードはインストール時に/前に変更できるか？

[ガイダンス]製造者は特定の制約を課している場合、注記に説明すること。

12-5　このシステムでは共有ユーザ ID が使われているか？

[ガイダンス]共有IDを使用するように設計されている場合は、「はい」とする。「はい」の場合、共有IDがサービス及び/又はユーザモード用かどうか指定する。さらに、ID/パスワードが、同じモデルの複数の機器間で共通かどうか記載する。（これには、「緊急」アカウントや「ブレイクグラス」アカウントは含まれない。）

12-6　設定されている（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構成できるか？パスワードの制約に制限がある場合は、注記セクションに記載すること。

[ガイダンス]パスワードの複雑さを設定可能な場合は、「はい」とする。複雑さの要件に関係なく、パスワードの複雑さが設定できない場合は「いいえ」とする。複雑さのルールと制限は注記に記載すること。

12-7　機器はアカウントパスワードが定期的に期限切れになるように構成できるか？

[ガイダンス]「はい」の場合、期限切れになる頻度や管理制御が可能かどうか注記に記載すること。

13　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着脱可能な媒体に保存されている個人情報の**整合性**や信頼性を損なうのを阻止できる。

13-1　個人情報を保持している機器のすべてのコンポーネント（着脱可能な媒体以外）は物理的に安全か（つまり、ツールなしでは動かせない）？

[ガイダンス]この質問は、製造者の機器の一般的な取り付けと構成について尋ねる。

個人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媒体を考える。そのような媒体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「はい」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。

14　機器のライフサイクルにおけるサードパーティ製コンポーネントのロードマップ（RDMP）：機器のライフサイクルでのサードパーティ製コンポーネントのセキュリティサポートに関する製造者の計画。

14-1　注記に、提供されている、又は必要な（別途購入する及び/又は提供する）オペレーティングシステムをバージョン番号とともに列挙すること。

14-2　**製造業者が提供しているその他サードパーティ製のアプリケーションのリストはあるか？**

[ガイダンス]注記セクションに、機器で使用し、製造者が提供しているその他のサードパーティ製アプリケーションを列挙する。所有権のあるコンポーネントの場合は、販売前に要求に応じてこの情報を入手できるかどうか指定する。

15　システムとアプリケーションの堅牢化（SAHD）：機器は本来、サイバー攻撃やマルウェアに強いものである。

15-1　機器には堅牢化のための方法があるか？

15-2　機器はインストールされているプログラム/アップデートが製造者の許可したプログラムやソフトウェアのアップデートであることを確かめるためのメカニズム（例えば、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？

[ガイダンス]オプションで、アプリケーションプログラム、システム構成、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注記セクションに記述する。

15-3　機器には外部通信機能があるか？（ネットワーク、モデムなど）

[ガイダンス]「はい」の場合、機器が外部接続を開始する必要があるのか、又は接続を受け取るのか注記に記載すること。

15-4　ファイルシステムは、ファイルレベルのアクセス制御の実行を許可しているか？（例えば、MS Windows プラットフォームの New Technology File System（NTFS））

[ガイダンス]注記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（例えば、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）。

15-5　機器の用途に必要のないすべてのアカウントは、ユーザとアプリケーションの両方について無効、又は削除されているか？

[ガイダンス]製造者によってクローズ/無効にされているアカウントがある場合（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アカウントがある場合は、注記に記載すること。

15-6　機器の用途に必要のないすべての共有リソース（例えばファイル共有）は、無効になっているか？

[ガイダンス]製造者によってクローズ/無効にされている共有リソースがある場合（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共有リソースがある場合は、注記に記載すること。

15-7　機器の用途に必要のないすべての通信ポートはクローズ/無効になっているか？

[ガイダンス]製造者によってクローズ/無効にされているポートがある場合（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ポートがある場合は、注記に記載すること。

15-8 機器の用途に必要のないすべてのサービス（例えば、Telnet、ファイル転送プロトコル（FTP）、Internet Information Server（IIS）など）は削除/無効にされているか？

[ガイダンス]製造者によって削除/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、注記に記載すること。

15-9　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、MS Internet Explorer など）は削除/無効にされているか？

[ガイダンス]製造者によって削除/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、注記に記載すること。

15-10　機器は管理されていない、又は着脱可能な媒体（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）から起動できるか？

[ガイダンス]機器で受け入れられる外部媒体を注記に記載すること。

15-11　装置製造者によって認可されないソフトウェア又はハードウェアがツールを使用せずに装置にインストールされ得るか？

[ガイダンス]機器のユーザ/所有者にハードウェアを取り付ける、又はソフトウェアをインストールする「技術的」な能力がある場合は「はい」と答える。ただし、製造者がハードウェアの取り付け、又はソフトウェアのインストールをユーザに許可していない場合、又はこの活動に制約を与えている場合は、これら制約の存在を注記に記載すること。

16　セキュリティガイド（SGUD）：機器の操作者と管理者、及び製造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。

16-1　セキュリティ関連の機能は機器のユーザ用に文書化されているか？

[ガイダンス]製造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、「はい」とする。

16-2　機器/媒体の完全な消去に関する指示は用意されているか？つまり、個人データやその他の機密データを永久に削除する方法の指示など。

[ガイダンス]製造者がユーザ向けの何らかの文書内でそのような指示を用意している場合は、「はい」とする。

17　健康データストレージの機密性（STCF）：不正アクセスによって装置やリムーバルメディアに保存された個人情報の完全性および機密性が危うくされない事を保証する装置の機能

17-1　機器は保存されているデータを暗号化できるか？

[ガイダンス]ネットワーク送信や媒体の書き出し前のデータの暗号化に関する質問はセクション 18 も参照。

18　送信の機密性（TXCF）：送信する個人情報の機密性を保証する機器の機能。

18-1　個人情報は二点間の専用ケーブルでのみ送信できるか？

[ガイダンス]質問の意味の説明：二点間の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）。

18-2　個人情報はネットワーク、又は着脱可能な媒体による送信前に暗号化されるか？（「はい」の場合、注記セクションに暗号化メカニズムが使用する規格を記載する。）

18-3　個人情報の送信は、ネットワーク送信先の固定リストに制限されているか？

[ガイダンス]質問の意味の説明：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。

19　送信の完全性（TXIG）：送信**されるユーザ**の完全性を保証する機器の機能。

19-1　機器は送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をサポートしているか？「はい」の場合、その仕組みを注記セクションに記載すること。

20　その他のセキュリティ考察：その他のセキュリティ考察/医療機器のセキュリティに関する注記

20-1　機器はリモートで保守点検可能か？

[ガイダンス]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。リモートサービスについて製造者が定める制約があれば注記で説明すること。

20-2　機器は特定の機器、ユーザ、ネットワークへ／からのリモートアクセスを制限できるか（例えば、特定の IP アドレス）？

20-2.1 ローカルユーザにリモートアクセスを受け入れる、または開始させるように機器を構成できるか？

医療機器セキュリティのための製造者開示説明書 - MDS²

機器の説明

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

製造者または代理人の連絡先情報	会社名	製造者の連絡情報
	代理人名/役職	

ネットワーク接続環境でのシステムの用途：

個人情報の管理

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
A	この**装置**は**個人情報**（**保護対象電子健康情報（ePHI）**を含む）を表示、送信、または保持できるか？	_____	–
B	**装置**で保持できる**個人情報**要素のタイプ：		
B.1	患者基本情報（例えば名前、番地、住所、一義的な ID 番号）？	_____	—
B.2	医療記録（例えば医療記録番号#、会計書番号#、検査または治療日、装置識別番号）？	_____	—
B.3	診断/治療（例えば特徴を識別する写真/放射線写真、検査結果または生理学のデータ）？	_____	—
B.4	**装置利用者/操作者**によって入力された公開自由文？	_____	—
B.5	**生体データ**？	_____	—
B.6	個人の財務情報？	_____	—
C	**個人情報**の保持 - **機器**で可能なこと：		
C.1	揮発性メモリで**個人情報**を一時的に保持する（つまり、パワーオフまたはリセットによって消去されるまで）？	_____	—
C.2	内部記録媒体に**個人情報**を確実に格納する？	_____	—
C.3	**個人情報**を他のシステムとインポート/エクスポートする？	_____	—
C.4	停電時に**個人情報**を保持できる？	_____	—
D	**個人情報**の送信、インポート/エクスポートのための機能：**機器**は次のことができるか。		
D.1	**個人情報**を表示する（ビデオディスプレイなど）？	_____	—
D.2	**個人情報**を含んでいる報告書または画像を印刷する？	_____	—
D.3	**着脱可能な媒体**（ディスク、DVD、CD-ROM、テープ、CF/SD カード、メモリスティックなど）から**個人情報**を取得する？またはそれらに記録する？	_____	—
D.4	**個人情報**の送信/受信またはインポート/エクスポートを、専用ケーブル接続を介して行う？（例えば、IEEE 1073、シリアルポート、USB、FireWire）	_____	—
D.5	**個人情報**の送信/受信を、有線ネットワーク接続を介して行う？（例えば、LAN、WAN、VPN、イントラネット、インターネット）	_____	—
D.6	**個人情報**の送信/受信を、統合ワイヤレスネットワーク接続を介して行う？（例えば、WiFi、Bluetooth、赤外線など）	_____	—
D.7	スキャンを介して**個人情報**をインポートする？	_____	—
D.8	その他？	_____	—

個人情報の管理
注記：

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

セキュリティ機能

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
1	**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。		
1-1	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（例えば、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）？		
1-1.1	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**または管理者が設定できるか？（注記に時間（固定、または設定可能な範囲）を示す	_____	—
1-1.2	自動ログオフ/スクリーンロックは**ユーザ**が手動で呼び出せるか（例えば、ショートカットキー、近接センサ）？	_____	—
		_____	—
ALOF 注記：			
2	**監査コントロール(AUDT)** **機器**上の活動を正しく監査する機能。		
2-1	**医療機器**は**監査証跡**を作成できるか？	_____	—
2-2	次のイベントのうち、監査ログに記録されるイベントを示す。		
2-2.1	ログイン/ログアウト	_____	—
2-2.2	データの表示/提示	_____	—
2-2.3	データの作成/変更/削除	_____	—
2-2.4	**着脱可能な媒体**からのデータのインポート/エクスポート	_____	—
2-2.5	外部（例えば、ネットワーク）接続を介したデータの受信/送信	_____	—
2-2.5.1	**リモートサービス**活動	_____	—
2-2.6	その他のイベント？（注記セクションで説明）	_____	—
2-3	監査ログに記録されている各イベントを特定するために使用する情報を示す：		
2-3.1	**ユーザ** ID	_____	—
2-3.2	日時	_____	—
AUDT 注記：			
3	**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		
3-1	**機器**は**ユーザ**ログイン要件また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？	_____	—
3-2	**ユーザ**には、「役割」に基づいてアプリケーション内で異なる権限レベルを割り当てられるか（例えば、ゲスト、標準**ユーザ**、上級**ユーザ**、管理者など）？	_____	—
3-3	**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（例えば、ローカルルートまたは管理者アカウントによるオペレーティングシステムまたはアプリケーションへのアクセス）？	_____	—
AUTH 注記：			

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
4	**セキュリティ機能の構成（CNFS）** **ユーザ**のニーズに合わせて**機器のセキュリティ機能**を構成/再構成する機能。		
4-1	**機器**の所有者/**操作者**は製品の**セキュリティ機能**を再構成できるか？	_____	__
CNFS 注記：			
5	**サイバーセキュリティ製品のアップグレード（CSUP）** **機器**のセキュリティパッチをインストール/アップグレード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。		
5-1	関連する OS 及び**機器**のセキュリティパッチを利用可能になった時点で**機器**に適用できるか？	_____	__
	5-1.1 セキュリティパッチまたは他のソフトウェアをリモートでインストールすることができるか？	_____	__
CSUP 注記：			
6	**健康データの匿名化（DIDT）** 患者の識別を可能にする情報を直接削除する機器の機能。		
6-1	**機器**は**個人情報**を匿名化する完全な機能を提供しているか？	_____	__
DIDT 注記：			
7	**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、またはソフトウェアの損傷や破壊後に復旧できる機能。		
7-1	**機器**は完全なデータバックアップ能力を持っているか（リモートストレージや、例えばテープ、ディスクのような**着脱可能なメディア**上へのバックアップ）？	_____	__
DTBK 注記：			
8	**緊急アクセス（EMRG）** 保存されている**個人情報**に即座にアクセスする必要がある緊急事態で、**ユーザ**が**個人情報**にアクセスできる**機器**の機能。		
8-1	**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？	_____	__
EMRG 注記：			
9	**健康データの完全性と信頼性（IGAU）** **機器**で処理されたデータが許可されていない方法で改変されていない、または破壊されていないこと、及び入手先が正しいことを**機器**で保証する方法。		
9-1	**機器**は、暗黙的・明示的なエラー検出/修正技術により保存されたデータの完全性を保証しているか？	_____	__
IGAU 注記：			

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
10	**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**）を効果的に阻止、検出、及び削除する**機器**の機能。		
10-1	**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？	_____	__
10-1.1	**ユーザ**は**マルウェア**対策設定を自分で再構成できるか？	_____	__
10-1.2	**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？	_____	__
10-1.3	**マルウェア**が検出された場合は、製造者が許可した人のみがシステムを修理できるか？	_____	__
10-2	**機器**の所有者は**アンチウイルスソフトウェア**をインストール、または更新できるか？	_____	__
10-3	**機器**の所有者/**操作者**は、製造者がインストールしたアンチウイルスソフトウェアでウイルス定義を（技術的/物理的に）更新できるか？	_____	__
MLDP 注記：			
11	**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。		
11-1	関連する OS 及び機器のセキュリティパッチを利用可能になった時点で**機器**に適用できるか？	_____	__
NAUT 注記：			
12	**個人の認証（PAUT）** **ユーザ**を認証する**機器**の機能。		
12-1	**機器**は少なくとも 1 **ユーザ**について、**ユーザ/操作者**固有のユーザ名とパスワードをサポートしているか？	_____	__
12-1.1	**機器**は複数の**ユーザ**に対して一意の**ユーザ/操作者**固有の ID とパスワードをサポートしているか？	_____	__
12-2	**機器**は外部認証サービスを通して**ユーザ**を認証するように構成できるか（例えば、MS Active Directory、NDS、LDAP など）？	_____	__
12-3	**機器**は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構成できるか？	_____	__
12-4	既定のパスワードはインストール時に/前に変更できるか？	_____	__
12-5	このシステムでは共有**ユーザ** ID が使われているか？	_____	__
12-6	設定されている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**を構成できるか？	_____	__
12-7	**機器**はアカウントパスワードが定期的に期限切れになるように構成できるか？	_____	__
PAUT 注記：			
13	**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**着脱可能な媒体**に保存されている**個人情報**の整合性や信頼性を損なうのを阻止できる。		
13-1	**個人情報**を保持している**機器**のすべてのコンポーネント（**着脱可能な媒体**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）？	_____	__
PLOK 注記：			

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
14	**機器のライフサイクルにおけるサードパーティ製コンポーネントのロードマップ（RDMP）** **機器**のライフサイクルでのサードパーティ製コンポーネントのセキュリティサポートに関する製造者の計画。		
14-1	注記に、提供されている、または必要な（別途購入する及び/または提供する）オペレーティングシステムをバージョン番号とともに列挙すること。	_____	—
14-2	製造者が用意している他のサードパーティ製アプリケーションの一覧を入手できるか？	_____	—
RDMP 注記：			
15	**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。		
15-1	**機器**には堅牢化のための方法があるか？業界で認識されている堅牢化標準への適合レベルを注記に記載すること。	_____	—
15-2	**機器**はインストールされているプログラム/アップデートが製造者の許可したプログラムやソフトウェアのアップデートであることを確かめるためのメカニズム（例えば、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？	_____	—
15-3	**機器**には外部通信機能があるか？（ネットワーク、モデムなど）	_____	—
15-4	ファイルシステムは、ファイルレベルのアクセス制御の実行を許可しているか？（例えば、MS Windows プラットフォームの New Technology File System（NTFS））	_____	—
15-5	**機器**の**用途**に必要のないすべてのアカウントは、ユーザとアプリケーションの両方について無効、または削除されているか？	_____	—
15-6	**機器**の**用途**に必要のないすべての共有リソース（例えばファイル共有）は、無効になっているか？	_____	—
15-7	**機器**の**用途**に必要のないすべての通信ポートはクローズ/無効になっているか？	_____	—
15-8	**機器**の**用途**に必要のないすべてのサービス（例えば、Telnet、ファイル転送プロトコル（FTP）、Internet Information Server（IIS）など）は削除/無効にされているか？	_____	—
15-9	**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、MS Internet Explorer など）は削除/無効にされているか？	_____	—
15-10	**機器**は管理されていない、または**着脱可能な媒体**（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）から起動できるか？	_____	—
15-11	装置製造者によって認可されないソフトウェアまたはハードウェアがツールを使用せずに装置にインストールされ得るか？	_____	—
SAHD 注記：			
16	**セキュリティガイダンス（SGUD）** システムの**操作者**と管理者、及び製造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。		
16-1	セキュリティ関連の機能は**機器**の**ユーザ**用に文書化されているか？	_____	—
16-2	**機器**/媒体の完全な消去に関する指示は用意されているか？（つまり、個人データやその他の機密データを永久に削除する方法の指示など）	_____	—
SGUD 注記：			

装置カテゴリー	製造者	文書 ID	文書リリース日時
装置モデル	ソフトウェア・レビジョン	ソフトウェア・リリース日時	

この書式で要求される情報を適切に解釈するには、この標準の 2.3.2 を参照すること。

		はい, いいえ、対象外、注記参照	注記 #
17	**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により、**機器**または**着脱可能な媒体**に保存されている**個人情**報の完全性と機密性が損なわれないようにする機器の機能。		
17-1	**機器**は保存されているデータを暗号化できるか？	_____	—
STCF 注記：			
18	**送信の機密性（TXCF）** 送信する**個人情報**の機密性を保証する**機器**の機能。		
18-1	**個人情報**は二点間の専用ケーブルでのみ送信できるか？	_____	—
18-2	**個人情報**はネットワーク、または**着脱可能な媒体**による送信前に暗号化されるか？（「はい」の場合、注記セクションに使用する暗号化規格を記載する。）	_____	—
18-3	**個人情報**の送信は、ネットワーク送信先の固定リストに制限されているか？	_____	—
TXCF 注記：			
19	**送信の完全性（TXIG）** 送信する**個人情報**の完全性を保証する**機器**の機能。		
19-1	**機器**は送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をサポートしているか？（「はい」の場合、その仕組みを注記セクションに記載すること。）	_____	—
TXIG 注記：			
20	**他のセキュリティ考察（OTHR）** 医療機器のセキュリティに関する追加のセキュリティ考察/注記		
20-1	**機器**はリモートで保守点検可能か？	_____	—
20-2	**機器**は特定の機器、**ユーザ**、ネットワーク位置（例えば、特定の IP アドレス）へ/からのリモートアクセスを制限できるか？	_____	—
	20-2.1 ローカル**ユーザ**にリモートアクセスの受け入れまたは開始を要求するように**機器**を構成できるか？	_____	—
OTHR 注記：			

付録

前回（2008 版）と現在（2013 版）の MDS^2 の内容の比較（参考）

表 A-1

MDS2 質問番号の変更の相互参照:HN 1-2008 vs. HN 1-2013

2013		2008
A	この**装置**は**個人情報**（**保護対象電子健康情報（ePHI）**を含む）を表示、送信、または保持できるか？	1
B	**装置**で保持できる**個人情報**要素のタイプ：	2
B.1	患者基本情報（例えば名前、番地、住所、一義的な ID 番号）？	2a
B.2	医療記録（例えば医療記録番号#、会計書番号#、検査または治療日、装置識別番号）？	2b
B.3	診断/治療（例えば特徴を識別する写真/放射線写真、検査結果または生理学のデータ）？	2c
B.4	**装置利用者/操作者**によって入力された公開自由文？	2d
B.5	**生体データ**？	...
B.6	個人の財務情報？	...
C	**個人情報**の保持 - **機器**で可能なこと：	3
C.1	揮発性メモリで**個人情報**を一時的に保持する（つまり、パワーオフまたはリセットによって消去されるまで）？	3a
C.2	内部記録媒体に**個人情報**を確実に格納する？	3b
C.3	**個人情報**を他のシステムとインポート/エクスポートする？	3c
C.4	停電時に**個人情報**を保持できる？	17
D	**個人情報**の送信、インポート/エクスポートのための機能：**機器**は次のことができるか。	4
D.1	**個人情報**を表示する（ビデオディスプレイなど）？	4a
D.2	**個人情報**を含んでいる報告書または画像を印刷する？	4b
D.3	**着脱可能な媒体**（ディスク、DVD、CD-ROM、テープ、CF/SD カード、メモリスティックなど）から**個人情報**を取得する？またはそれらに記録する？	4c
D.4	**個人情報**の送信/受信またはインポート/エクスポートを、専用ケーブル接続を介して行う？（例えば、IEEE 1073、シリアルポート、USB、FireWire）	4d
D.5	**個人情報**の送信/受信を、有線ネットワーク接続を介して行う？（例えば、LAN、WAN、VPN、イントラネット、インターネット）	4e
D.6	**個人情報**の送信/受信を、統合ワイヤレスネットワーク接続を介して行う？（例えば、WiFi、Bluetooth、赤外線など）	4f
D.7	スキャンを介して**個人情報**をインポートする？	...
D.8	その他？	4g
1-1	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（例えば、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）？	14
1-1.1	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**または管理者が設定できるか？（注記に時間（固定、または設定可能な範囲）を示す	...
1-1.2	自動ログオフ/スクリーンロックは**ユーザ**が手動で呼び出せるか（例えば、ショートカットキー、近接センサ）？	...
2-1	**医療機器**は**監査証跡**を作成できるか？	15
2-2	次のイベントのうち、監査ログに記録されるイベントを示す。	
2-2.1	ログイン/ログアウト	15a

表は次頁へ続く

表 A-1 続き

2013		2008
2-2.2	データの表示/提示	15b
2-2.3	データの作成/変更/削除	15c
2-2.4	**着脱可能な媒体**からのデータのインポート/エクスポート	15d
2-2.5	外部（例えば、ネットワーク）接続を介したデータの受信/送信	
2-2.5.1	**リモートサービス**活動	11b
2-2.6	その他のイベント？（注記セクションで説明）	...
2-3	監査ログに記録されている各イベントを特定するために使用する情報を示す：	...
2-3.1	**ユーザ** ID	...
2-3.2	日時	...
3-1	**機器**は**ユーザ**ログイン要件また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？	...
3-2	**ユーザ**には、「役割」に基づいてアプリケーション内で異なる権限レベルを割り当てられるか（例えば、ゲスト、標準**ユーザ**、上級**ユーザ**、管理者など）？	...
3-3	**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（例えば、ローカルルートまたは管理者アカウントによるオペレーティングシステムまたはアプリケーションへのアクセス）？	12d
4-1	**機器**の所有者/**操作者**は製品の**セキュリティ機能**を再構成できるか？	...
5-1	関連する OS 及び**機器**のセキュリティパッチを利用可能になった時点で**機器**に適用できるか？	12a
5-1.1	セキュリティパッチまたは他のソフトウェアをリモートでインストールすることができるか？	11c
6-1	**機器**は**個人情報**を匿名化する完全な機能を提供しているか？	...
7-1	**機器**は完全なデータバックアップ能力を持っているか（例えばテープ、ディスクのようなリモートストレージや**着脱可能なメディア**上へのバックアップ）？	8
8-1	**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？	16
9-1	**機器**は、暗黙的・明示的なエラー検出/修正技術により保存されたデータの完全性を保証しているか？	19
10-1	**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？	...
10-1.1	**ユーザ**は**マルウェア**対策設定を自分で再構成できるか？	...
10-1.2	**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？	...
10-1.3	**マルウェア**が検出された場合は、製造者が許可した人のみがシステムを修理できるか？	...
10.2	**機器**の所有者は**アンチウイルスソフトウェア**をインストール、または更新できるか？	12b
10-3	**機器**の所有者/**操作者**は、製造者がインストールしたアンチウイルスソフトウェアでウイルス定義を（技術的/物理的に）更新できるか？	12c
11-1	関連する OS 及び機器のセキュリティパッチを利用可能になった時点で**機器**に適用できるか？	11a
12-1	**機器**は少なくとも 1 **ユーザ**について、**ユーザ/操作者**固有のユーザ名とパスワードをサポートしているか？	13
12-1.1	**機器**は複数の**ユーザ**に対して一意の**ユーザ/操作者**固有の ID とパスワードをサポートしているか？	...
12-2	**機器**は外部認証サービスを通して**ユーザ**を認証するように構成できるか（例えば、MS Active Directory、NDS、LDAP など）？	...
12-3	**機器**は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構成できるか？	...
12-4	既定のパスワードはインストール時に/前に変更できるか？	...

表は次頁へ続く

表 A-1 続き

2013		2008
12-5	このシステムでは共有**ユーザ** ID が使われているか？	...
12-6	設定されている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**を構成できるか？	...
12-7	**機器**はアカウントパスワードが定期的に期限切れになるように構成できるか？	...
13-1	**個人情報**を保持している**機器**のすべてのコンポーネント（**着脱可能な媒体**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）？	7
14-1	注記に、提供されている、または必要な（別途購入する及び/または提供する）オペレーティングシステムをバージョン番号とともに列挙すること。	6
14-2	製造者が用意している他のサードパーティ製アプリケーションの一覧を入手できるか？	...
15-1	**機器**には堅牢化のための方法があるか？業界で認識されている堅牢化標準への適合レベルを注記に記載すること。	...
15-2	**機器**はインストールされているプログラム/アップデートが製造者の許可したプログラムやソフトウェアのアップデートであることを確かめるためのメカニズム（例えば、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？	...
15-3	**機器**には外部通信機能があるか？（ネットワーク、モデムなど）	...
15-4	ファイルシステムは、ファイルレベルのアクセス制御の実行を許可しているか？（例えば、MS Windows プラットフォームの New Technology File System（NTFS））	...
15-5	**機器**の**用途**に必要のないすべてのアカウントは、ユーザとアプリケーションの両方について無効、または削除されているか？	...
15-6	**機器**の**用途**に必要のないすべての共有リソース（例えばファイル共有）は、無効になっているか？	...
15-7	**機器**の**用途**に必要のないすべての通信ポートはクローズ/無効になっているか？	...
15-8	**機器**の**用途**に必要のないすべてのサービス（例えば、Telnet、ファイル転送プロトコル（FTP）、Internet Information Server（IIS）など）は削除/無効にされているか？	...
15-9	**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、MS Internet Explorer など）は削除/無効にされているか？	...
15-10	**機器**は管理されていない、または**着脱可能な媒体**（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）から起動できるか？	9
15-11	装置製造者によって認可されないソフトウェアまたはハードウェアがツールを使用せずに装置にインストールされ得るか？	10
16-1	セキュリティ関連の機能は**機器**の**ユーザ**用に文書化されているか？	5
16-2	**機器**/媒体の完全な消去に関する指示は用意されているか？（つまり、個人データやその他の機密データを永久に削除する方法の指示など）	...
17-1	**機器**は保存されているデータを暗号化できるか？	...
18-1	**個人情報**は二点間の専用ケーブルでのみ送信できるか？	18a
18-2	**個人情報**はネットワーク、または**着脱可能な媒体**による送信前に暗号化されるか？（「はい」の場合、注記セクションに使用する暗号化規格を記載する。）	18b
18-3	**個人情報**の送信は、ネットワーク送信先の固定リストに制限されているか？	18c
19-1	**機器**は送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をサポートしているか？（「はい」の場合、その仕組みを注記セクションに記載すること。）	...
20-1	**機器**はリモートで保守点検可能か？	11
20-2	**機器**は特定の機器、**ユーザ**、ネットワーク位置（例えば、特定の IP アドレス）へ/からのリモートアクセスを制限できるか？	11a
20-2.1	ローカル**ユーザ**にリモートアクセスの受け入れまたは開始を要求するように**機器**を構成できるか？	...