

医療機器のサイバーセキュリティ管理のための 市販前申請内容

業界および米国食品医薬品局 スタッフ向けガイダンス

文書発行日：2014年10月2日

本文書のドラフト版は2013年6月14日に発行された。

本文書に関する質問があれば、Office of Device Evaluation（電話 301-796-5550）または Office of Communication, Outreach and Development（CBER）（電話 1-800-835-4709 または 240-402-7800）に連絡のこと。



米国保健福祉省（U.S. Department of Health and Human Services）

食品医薬品局（Food and Drug Administration）

医療機器・放射線保健センター（Center for Devices and Radiological Health）

医療機器審査室（Office of Device Evaluation）

体外診断製品・放射線保健室（Office of In Vitro Diagnostics and Radiological Health）

生物学的製剤評価研究センター（Center for Biologics Evaluation and Research）

はじめに

パブリックコメント

電子媒体によるコメントおよび提案はいつでも当局 (<http://www.regulations.gov>) に提出することができ、当局において検討される。書面によるコメントは、米国食品医薬品局、Division of Dockets Management（ドケット管理部門）（5630 Fishers Lane, rm. 1061, (HFA-305), Rockville, MD, 20852）に提出のこと。すべてのコメントは docket number（ドケット番号）FDA-2013-D-0616-0001 で識別する。当該文書の次回改定または更新時まで当局はコメントに対する意思決定を実行しない。

追加コピー

追加コピーはインターネットから入手できる。また、CDRH-Guidance@fda.hhs.gov宛てに電子メールを送信すれば、ガイダンスのコピーを請求することもできる。請求したいガイダンスを特定するため、ドキュメント番号 1825 を使用すること。

生物学的製剤評価研究センター（Center for Biologics Evaluation and Research : CBER）に請求すれば（住所：Office of Communication, Outreach and Development 10903 New Hampshire Avenue, Bldg. 71, Rm. 3128, Silver Spring, MD 20993-0002、電話番号：1-800-835-4709 または 240-402-7800、電子メール：ocod@fda.hhs.gov）、本ガイダンス文書の追加コピーを入手することができる。また、インターネット

（<http://www.fda.gov/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/default.htm>）でも入手可能である。

医療機器のサイバーセキュリティ管理のための 市販前申請内容

業界および米国食品医薬品局 スタッフ向けガイダンス

本ガイダンスは、本案件に対する米国食品医薬品局 (FDA) の最新の見解を示すものである。本ガイダンスは、いかなる人物にいかなる権利を作り与えるものでもなければ、FDA や公衆に対して拘束力を発動するものでもない。代替アプローチが適用される法規と規制の要件を満たすのであれば、代替アプローチを用いてもよい。代替アプローチについて検討したいのであれば、本ガイダンスの実施責任者である FDA スタッフに問い合わせること。担当の FDA スタッフがわからない場合には、本ガイダンスの標題ページに明記されている当該の電話番号に連絡すること。

1. 序文

ワイヤレス、インターネットおよびネットワーク接続医療機器の利用が増加し、医療機器関連の健康情報を電子媒体で交換する頻度が増えたため、医療機器の機能性と安全性を保証するための有効なサイバーセキュリティの必要性がますます重要視されるようになった。FDA が策定した本ガイダンスは、製造業者が自社医療機器の設計・開発において考慮し、当該医療機器の市販前申請書類を作成する際にも考慮すべきサイバーセキュリティ関連の検討課題を特定することによって業界を支援することを目的としている。本ガイダンス文書に記載されている勧告は、FDA の「医療機器に含まれるソフトウェアの市販前申請内容に関するガイダンス “Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices”」 (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm>) および「業界向けガイダンス：既製品 (Off-the-Shelf : OTS) ソフトウェアを含むネットワーク接続医療機器に対するサイバーセキュリティ “Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software”」 (<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm>) を補完することを意図している。

FDA ガイダンス文書は、本ガイダンスを含め、法的強制力のある義務を定めるものではない。むしろ、ガイダンスにはある案件に関する当局の最新見解が記載されており、特定の規制要件や法定要件が引用されていない限り、提言とみなすにとどめるのが望ましい。当局のガイダンスにおいて *should* (～すること) という文言が使用されている場合には、提案または推奨事項を意味しており、要求を意味しているのではない。

2. 適用範囲

本ガイダンスは、検討していただきたい提言および有効なサイバーセキュリティ管理に関して FDA 医療機器市販前申請書類に盛り込む情報を提供するものである。有効なサイバーセキュリティ管理は、サイバーセキュリティの不備によって医療機器の機能が意図的または非意図的に損なわれる可能性を減少させることにより、患者へのリスクを低減させることを意図している。

本ガイダンス文書は、ソフトウェア（ファームウェアを含む）またはプログラマブル論理を含む医療機器ならびに医療機器に該当するソフトウェアを含む機器に関する以下の市販前申請書類に適用される：¹

- 市販前届出（510(k)）、従来式申請、特別申請および簡略申請を含む。
- *De novo* 申請
- 市販前承認申請（PMA）
- 製品開発プロトコール（PDP）
- 人道機器適用免除（HDE）申請

3. 定義

資産（Asset）²—個人または団体にとって価値のあるもの。

認証（Authentication）—機器、機器データ、情報またはシステムへのアクセスを許可する必要条件として、ユーザ、プロセスまたは機器の身元を確認する行為。

権限付与（Authorization）—機器リソースへのアクセスを許される権利または許可。

¹ 適切な場合には、製造業者は本ガイダンスに記載されているサイバーセキュリティ原則を治験用医療機器に対する適用免除（Investigational Device Exemption）申請および機器の市販前審査免除に適用するよう考慮してもよい。

² ISO/ICE 27032:2012(E) Information technology — Security techniques — Guidelines for cybersecurity (ISO/ICE 27032:2012(E) インフォメーションテクノロジー — セキュリティ技術 — サイバーセキュリティのためのガイダンス) の定義に従う。

利用可能性 (Availability) –期待される手法で適時にアクセス可能かつ利用可能なデータ、情報および情報システム(すなわち、必要なときに情報を利用できることが保証されていること)。

機密保持 (Confidentiality) –データ、情報またはシステム構成が権限付与された人物や実体のみアクセス許可され、権限付与された時点で権限付与された手法によって処理されることにより、データとシステムのセキュリティを保証する一助とすること。機密保持によって、権限のないユーザがデータ、情報またはシステム構成にアクセスすることがないよう保証する(すなわち、信頼できるユーザ (trusted user) のみアクセスできる)。

サイバーセキュリティ (Cybersecurity) –保存されている情報、アクセスされた情報または医療機器から外部受信者に転送された情報への不正アクセス、修正変更、悪用や利用拒否または不正使用を防止するためのプロセス。

暗号化 (Encryption) –データを暗号変換してデータの本来の意味を秘匿し、理解または使用できないようにすること。

損害 (Harm)³ –ヒトの健康状態に対する損傷やダメージまたは所有物や環境に対するダメージと定義される。

完全性 (Integrity) –本文書における完全性 (Integrity) は、データ、情報およびソフトウェアが正確かつ完全であり、不適切な修正変更が行われていないことを意味する。

ライフサイクル (Life-cycle) 2 –初期構想から最終的な廃棄処分まで、医療機器が寿命を全うするまでの全フェーズ。

マルウェア (Malware) –正常機能の破壊、機密情報の収集、その他の接続システムへのアクセスを目的として、悪意をもって意図的に設計されたソフトウェア。

特権ユーザ (Privileged User) 3 –一般ユーザには実行許可が与えられていないセキュリティ関連の機能を実行できる権限を与えられている(したがって、信頼できるユーザ (trusted user) に指定されている) ユーザ。

リスク (Risk) 2 –損害の発生確率と損害の重大性の組み合わせ。

リスク解析 (Risk Analysis) 2 –危険要因を特定し、リスクを推定するために入手可能な情報を体系的に利用すること。

³ ANSI/AAMI/ISO 14971:2007 Medical devices – Application of risk management to medical devices (ANSI/AAMI/ISO 14971:2007 医療機器 – 医療機器へのリスクマネジメントの適用) の定義に従う。

4. 一般原則

製造業者は一連のサイバーセキュリティ制御システムを開発し、医療機器のサイバーセキュリティを保証するとともに、医療機器の機能性と安全性を保持すること。

医療機器のセキュリティはステークホルダー（医療機関、患者、医療提供者を含む）と医療機器製造業者との間で共同責任を負うものであると FDA は認識している。サイバーセキュリティを維持できない場合、医療機器の機能性が損なわれる、（医療または個人）データの利用可能性または完全性の喪失、ほかの接続機器やネットワークがセキュリティの脅威にさらされることにつながる可能性がある。これがさらに患者の病態悪化、受傷または死亡をまねく可能性がある。

製造業者は、医療機器の設計および開発段階でサイバーセキュリティに取り組むこと。これにより、患者のリスクを堅牢かつ効率的に軽減することができる。製造業者は、サイバーセキュリティ関連機器に関する設計インプット（design inputs）を確立するとともに、21 CFR 820.30(g)⁴に規定されているソフトウェアバリデーションとリスク解析の一環として、サイバーセキュリティの脆弱性と管理に取り組むアプローチを確立すること。このアプローチでは、以下の要素に適切に対処すること：

- 資産、脅威的存在および脆弱性の特定。
- 脅威的存在と脆弱性が機器の機能性とエンドユーザ／患者に与える影響度の評価。
- 脅威的存在と脆弱性が悪用される尤度の評価。
- リスクレベルと適切な緩和戦略の決定。
- 残存リスクとリスク許容基準の評価。

5. サイバーセキュリティ機能

医療機器製造業者がサイバーセキュリティのフレームワークを構成する以下のコア機能を検討し、サイバーセキュリティ活動の指針とするよう当局は推奨する。特定（Identify）、保護（Protect）、検出（Detect）、応答（Respond）、回復（Recover）⁵。

⁴ 21 CFR Part 820 – Quality Systems Regulations: 21 CFR 820.30 Subpart C – Design Controls of the Quality System Regulation (21 CFR Part 820 – 品質システム規制：21 CFR 820.30 Subpart C – 品質システム規制の設計管理)

⁵ 米国国立標準技術研究所(National Institute of Standards and Technology)。Framework for Improving Critical Infrastructure Cybersecurity (重要インフラストラクチャーとしてのサイバーセキュリティを改善するための枠組み)。以下のサイトで入手可能：

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

特定 (Identify) および保護 (Protect)

ほかの機器、インターネットその他のネットワークまたはポータブルメディア (USB や CD など) に (ワイヤレスまたはハードワイヤ配線による) 接続可能な医療機器は、接続できない機器に比べてサイバーセキュリティの脅威に対する脆弱性が高い。セキュリティコントロールを要する程度は、機器の用途、電子データインターフェースの有無と意図、意図されている使用環境、実在するサイバーセキュリティの脆弱性のタイプ、(意図的または非意図的を問わず) 脆弱性が悪用される尤度およびサイバーセキュリティの侵害によって患者が損害を被る推定リスクに応じて異なる。

製造業者は、サイバーセキュリティ保護と意図されている使用環境 (例: 自宅で使用するのか、あるいは医療機関で使用するのか) における当該機器のユーザビリティとのバランスを慎重に検討し、セキュリティコントロールが対象ユーザにとって適切なものであるよう保証すること。たとえば、緊急事態が発生した場合に使用することになっている機器へのアクセスをセキュリティコントロールによって不当に妨げるべきではない。

医療機器製造業者は自社医療機器のために選択したセキュリティ機能について、市販前申請書類に妥当性を裏づける根拠を記載するよう当局は推奨する。

医療機器を保護するために検討すべきセキュリティ機能の具体例を以下に挙げるが、これらに限定されるわけではない。

信頼できるユーザ (Trusted User) にのみアクセス制限する

- ユーザの認証 (例: ユーザ ID やパスワード、スマートカード、バイオメトリック [生体認証]) により機器へのアクセスを制限する。
- 利用環境において適切な場合には、システム内のセッションを終了させるよう自動的に時間制限を設ける。
- 適切な場合には、ユーザの役割 (例: 介護者、システム管理者など) または機器の役割に基づく特権を区別することにより、階層化した権限付与モデルを採用する。
- 適切な認証方式を使用する (例: システム管理者、サービス技術者、保守管理者の機器への特権的アクセスを許可する多要素認証方式など)。
- 「ハードコード」されたパスワードや共通パスワード (各機器に対して同一のパスワードが使用されており、変更が困難であり、公開に対して脆弱なパスワード) を避けてパスワード保護を強化し、機器への特権的アクセスに使用するパスワードへのパブリックアクセスを制限する。
- 適切な場合には、機器とそのコミュニケーションポートを物理的にロックし、改ざんを最小限に抑える。
- ソフトウェアまたはファームウェアの更新を許可する前にユーザ認証そののしかるべきコントロール対策を要求する。このなかには、オペレーションシステム、ア

アプリケーションおよびマルウェア対策にかかわるものも含まれる。

信頼できるコンテンツ（Trusted Content）を保証する

- ソフトウェアまたはファームウェアの更新を認証コードに限定する。製造業者に検討してもらいたい認証方式の1つとして、コード署名認証が挙げられる。
- 許可ユーザが製造業者からバージョン識別可能なソフトウェアおよびファームウェアをダウンロードするための系統的な手法を用いる。
- 機器との間でセキュリティ保護データを双方向で転送できるように保証し、適切な場合には、暗号化のための手法を用いる。

検出（Detect）、応答（Respond）、回復（Recover）

- 通常使用時に検出、認識、記録、時間制限および実行されるセキュリティ侵害を考慮した機能を実装する。
- サイバーセキュリティ関連の事象が検出された場合に講じる適切な措置に関する情報を策定し、エンドユーザに情報提供する。
- 機器のサイバーセキュリティが侵害された場合であっても、重要な機能性を保護できる機能を機器に実装する。
- 認証された特権ユーザが機器設定を保持および回復させるための手法を提供する。

妥当性を裏づける適切な根拠がある場合、製造業者は別の手法やアプローチを提供することにしてもよい。

6. サイバーセキュリティに関する文書作成

市販前申請において当局が提出するよう推奨している文書のタイプを本セクションに要約する。これらの推奨事項は、設計管理（Design Control）を含めた品質システム規制（Quality System Regulation）を遵守した品質システムの有効な実行と管理が前提となる。

市販前申請において、製造業者は自社医療機器のサイバーセキュリティに関連する以下の情報を提供すること：

1. 自社医療機器に伴う意図的および非意図的なサイバーセキュリティリスクに関するハザード解析、緩和策および設計の考慮事項には、以下の項目が含まれる。
 - 自社医療機器を設計する際に考慮した全サイバーセキュリティリスクについて詳述したリスト。
 - 自社医療機器のために確立したすべてのサイバーセキュリティ制御について詳述したリストと妥当性を裏づける根拠。

2. 実際に行ったサイバーセキュリティ制御と考慮したサイバーセキュリティリスクとを関連づけるトレーサビリティマトリクス。
3. 安全性と有効性を保証し続けるために医療機器のライフサイクル全般を通じて必要とされるバリデーション済みソフトウェアの更新およびパッチを提供するための計画をまとめた要約。通常、FDA はサイバーセキュリティ強化のみを目的として行われた医療機器ソフトウェア変更を審査および承認する必要はない。
4. 開始時点から機器が製造業者の管理を離れる時点まで医療機器ソフトウェアがその完全性（例：マルウェアに感染していない状態の維持など）を維持できるように保証するというコントロール方針をまとめた要約。
5. 意図された使用環境にふさわしい推奨されたサイバーセキュリティ制御（例：ウイルス対策ソフトウェア、ファイアーウォールの使用など）に関連する機器取扱説明書と製品仕様書。

7. 公認基準

インフォメーションテクノロジー（Information Technology：IT）および医療機器セキュリティを扱っている FDA 公認合意基準のリストを以下に列挙する。

1. CLSI, AUTO11-A - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard. (CLSI, AUTO11-A - In Vitro 診断機器およびソフトウェアシステムの IT セキュリティ：承認された基準)
2. IEC, TR 80001-2-2 Edition 1.0 2012-07 - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls. (IEC, TR 80001-2-2 Edition 1.0 2012-07 - IT ネットワーク統合医療機器に対するリスク管理の適用- Part 2-2: 医療機器セキュリティのニーズ、リスクおよびコントロールの開示と伝達に関するガイドライン)
3. AAMI/ANSI/IEC, TIR 80001-2-2:2012, - Application of risk management for IT Networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls. (AAMI/ANSI/IEC, TIR 80001-2-2:2012, - IT ネットワーク統合医療機器に対するリスク管理の適用- Part 2-2: 医療機器セキュリティのニーズ、リスクおよびコントロールの開示と伝達に関するガイドライン)

4. IEC, /TS 62443-1-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. (IEC, /TS 62443-1-1 Edition 1.0 2009-07 -業界情報伝達ネットワーク-ネットワークとシステムセキュリティ-Part 1-1 : 専門用語、概念およびモデル)
5. IEC, 62443-2-1 Edition 1.0 2010-11 - Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program (IEC, 62443-2-1 Edition 1.0 2010-11 -業界情報伝達ネットワーク-ネットワークとシステムセキュリティ-Part 2-1 : 工業オートメーションおよびコントロールシステムセキュリティプログラムの確立)
6. IEC, /TR 62443-3-1 Edition 1.0 2009-07 - Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems. (IEC, /TR 62443-3-1 Edition 1.0 2009-07 -業界情報伝達ネットワーク-ネットワークとシステムセキュリティ-Part 3-1 : 工業オートメーションおよびコントロールシステムのためのセキュリティテクノロジー)

FDA 公認合意基準の最新リストに関して、FDA 公認合意基準データベース (FDA Recognized Consensus Standards Database)

(<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm>) を参照するよう当局は勧告する。また、当局公認の IT および医療機器セキュリティ合意基準の最新リストを標題で検索する場合には、検索語に“security”とタイプ入力する。公認合意基準に関する情報は、ガイダンス文書 「Frequently Asked Questions on Recognition of Consensus Standards (合意基準の公認に関するよくある質問)」

(<http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm074973.htm>) を参照のこと。

一般的健康機器： 低リスク機器に関するポリシー

業界および食品医薬品局 スタッフ向け指針

指針草稿

本指針は、コメント投稿用に配布されています。

文書発行日：2015年1月20日

指針草稿がある旨の通知が*Federal Register*（連邦官報）に発表されてから90日以内に、本書に関するコメント及び提案を提出してください。書面によるコメントはDivision of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852に提出してください。電子コメントは<http://www.regulations.gov>に提出してください。全てのコメントに、連邦公報に告示された配布通知に記載の文書番号 (docket number) を明記してください。

この文書に関する質問がある場合は、センター長室 (301-796-5900) までお問い合わせください。

U. S. Department of Health and Human Services (米国保健福祉省)
Food and Drug Administration (食品医薬品局)
Center for Devices and Radiological Health (医療機器・放射線保健センター)

前文

追加コピー

追加コピーはインターネットで入手できます。またはEメールをdsmica@fda.hhs.govに送信してこのガイダンスの電子コピーを受け取るか、またはFax (301-847-8149) で請求してハードコピーを受け取ることもできます。文書番号 (1300013) を用いて請求するガイダンスを特定してください。

目次

I.	緒言	1
II.	低リスクの一般的健康機器に関するポリシー	2
III.	一般的健康機器	3
IV.	低リスク	5
V.	低リスクの一般的健康機器の例	7
	一般的健康機器の決定アルゴリズム.....	9

一般的健康機器： 低リスク機器に関するポリシー

業界および食品医薬品局 スタッフ向け指針

本指針の最終版は、食品医薬品局 (FDA) のこのテーマに関する最新の考えを表すものである。これは何人に対しても如何なる権利を生じるもしくは付与するものではなく、またFDAまたは国民を拘束するために機能するものではない。適用される法的要件・規制要件を満たすものであれば、代替的アプローチを用いても構わない。代替的アプローチについて協議したい場合は、本指針の施行を担当するFDAスタッフに連絡されたい。該当するFDAスタッフが不明の場合は、本ガイダンスの表紙に記載された該当する電話番号に電話されたい。

I. 緒言

米国食品医薬品局 (FDA) は、健康な生活習慣を促進する低リスク製品 (一般的健康機器) に関するCenter for Devices and Radiological Health (医療機器・放射線保健センター、CDRH) のコンプライアンスポリシーについて、業界およびFDAスタッフに対し説明することを目的として、本ガイダンス文書を発行する¹。本ガイダンスは、FDAの他のセンターが規制する製品 (医薬品、生物製剤、栄養補助食品、食品、化粧品など)、またはCDRHが規制する製品²を含む複合製品には適用されない。

本ガイダンスを含めFDAのガイダンス文書は法的に履行を強制できる責務を確立するものではない。むしろ各ガイダンスはあるテーマに対するFDAの現在の考えを述べるものであり、特定の規制要件または法的要件が引用されていない限り、あくまで推奨事項とみなされるべきで

¹ このガイダンスにより、FD&C法または適用規則の諸要件が変わったり撤回されることはない。また、このガイダンスによって、一般的健康機器が消費者製品安全委員会 (CPSC) の権限に基づく消費者製品または機器であるかどうかについて、FDAがCPSCと協議しないわけではない。FDAは、CPSCなどの規制機関および規制当局連携して、製品に対する権限を決定する。製品がFD&C Act法のセクション201(h)の管理下にある機器である場合、通常、消費者製品安全法 (15 U. S. C. § 2052(a)(5)(ii)(H)) の管理下にある「消費者製品」に対するCPSCの権限から除外される。ただし、CPSCおよびFDAがいずれもCPSCが管理する他の法的権限の管理下にある特定の医療機器に対する権限を有する場合がある。

² 併用製品が医療機器の法的定義を満たすかどうかに関する判断については、Office of Combination Products (combination@fda.gov)に問い合わせること。

ある。FDAのガイダンスにある「should (するものとする)」という言葉は何かを示唆、推奨されているが、義務付けられているのではないことを意味する。

II. 低リスクの一般的健康機器に関するポリシー

CDRHは、低リスクの一般的健康機器がFD&C Act法の意義の範囲内における医療機器³かどうか、その意義の範囲内における医療機器に該当する場合、FD&C Act 法や登録および機器リスト作成ならびに販売前通知の要件 (21 CFR Part 807)、ラベル表示の要件 (21 CFR Part 801 および21 CFR 809.10)、品質システム規制に記載された製造管理および品質管理に関する基準 (21 CFR Part 820)、医療機器に関する報告 (MDR) 義務 (21 CFR Part 803) などの施行規則の規制下にある医療機器の市販前審査及び市販後の規制要件に準拠しているかどうかを確認するためにこれらの機器の検討を意図しているわけではない。

このガイダンスの目的において、CDRHは一般的健康機器を (1) 本ガイドラインに定義されるとおり一般的な健康のみを目的としてのみ使用する、(2) 使用者の安全性に対するリスクが極めて低い製品と定義する。一般的健康機器には、これら2つの条件を満たす運動器具、録音、テレビゲーム、ソフトウェアプログラム⁴で、独占的ではなく小売店 (オンラインの小売店や、ソフトウェアを直接ダウンロードできる販売店を含む) から幅広く購入できる製品が含まれる。

CDRHは定期的に、特定の機器がFD&C Act法が定義する機器であるかどうかに関する問い合わせを受ける。例えば、このガイダンスで検討されている様な特定の一般的健康機器がFD&C Act法のセクション201(h)の医療機器の定義を満たしていないため、FD&C Act法の医療機器の規制要件の影響下でない場合がある。ここでは、医療機器の定義を満たすことを提案するのではなく、これらの製品の例を含めることで、このガイダンスの範囲を示している。

このガイダンスの範囲にある製品が含まれていても、その製品の安全性、有効性、使用目的についての不正商標表示がされていないことが立証されるわけではない。

³ 「機器 (device)」という用語は、FD&C Act法の201(h)において、「・・・何らかのコンポーネント、パーツ、アクセサリを含め、計器、器具、道具、機械、仕掛け、インプラント、in vitro試薬、またはその他類似のものもしくは関連する物品」で、「・・・ヒトにおいて疾患もしくはその他の病態の診断、または疾患の治癒、緩和、治療、予防に使用されることを目的とする」、あるいは、「人体の構造または機能に影響を及ぼす目的のもの・・・」としている。

⁴ 特定のモバイル医療アプリケーションに対するFDAの規制アプローチに関する詳細な検討については、FDAガイダンス：モバイル医療アプリケーション (2013年9月25日発行)

(<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM283366.pdf>) を参照のこと。

III. 一般的健康機器

このガイダンスの目的において、**一般的健康機器**とは、(1) 全体的な健康状態又は健康的な活動の維持または促進に関連する使用目的がある、(2) 使用目的において、健康的な生活習慣の役割と、特定の慢性疾患または慢性的な症状のリスクまたは影響の軽減とを関連付け、健康的な生活習慣を選択することが疾患または症状の健康的な予後における重要な役割を果たす可能性があることが十分に理解され、受け入れられている機器である。

製品の使用目的が、上記の一般的健康機器の使用目的に限定されていない場合、このガイダンスは適用されない。

一般的健康の使用目的の第一の分類には、疾患あるいは症状に一切言及せず、全体的な健康状態に関連する症状および機能の全体的な改善を持続または提供するという表示が含まれる。このガイダンスでは、一般的健康の第一区分は以下に関連する。

- 体重管理
- 体力（レクリエーション的使用の目的を含む）
- リラクゼーションまたはストレス管理
- 知力
- 自己評価（自己評価のみに関連すると表示した、美容機能搭載の機器など）
- 睡眠管理
- 性機能

一般的健康機器表示の第一分類の例としては、以下のものがある。

- 健康的な体重を促進または維持、健康的な食事を促進、または体重減量の目標達成を支援すると表示するもの
- リラクゼーションを促進する、または不安障害についての言及あるいは疾患又は症状に関するその他の言及がない場合、ストレスを管理すると表示するもの
- 気の流れを高める、改善する、向上させると表示するもの
- 知力、指示に従うこと、集中力、問題解決、マルチタスク、リソース管理、意思決定、論理的思考、パターン認識、目と手の連携を改善すると表示するもの
- 運動活動の記録、追跡または傾向分析、エアロビクスフィットネスの測定、身体運動の改善、持久力、強度または連携の発達または改善、活力の向上など、体力を促

進すると表示するもの

- 睡眠の傾向を追跡記録するなど、睡眠管理を促進すると表示するもの
- 自己評価を向上させるなど、自己評価を促進すると表示するもの
- 筋肉の大きさまたは体調を強化または改善する、身体または筋肉を調整あるいは安定させる、心臓機能を向上させる、または性的能力を向上または改善するなど、特定の身体構造又は身体機能に対応すると表示するもの
- 全体的な運動機能を改善する、または運動障害があるまたはレクリエーション活動における運動が制限されている個人を支援すると表示するもの
- 心拍を監視する、または不調の頻度又は影響を監視するなど、レクリエーション活動参加の結果をモニタリングして、レクリエーション活動の参加を改善すると表示するもの

一般的健康機器表示の第一分類に含まれないものの例としては、以下のものがある。

- 製品が肥満を治療または診断するという表示
- 食欲不振など、摂食障害を治療するという表示
- 不安症の治療を支援するという表示
- コンピュータゲームにより自閉症を診断または治療するという表示
- 筋萎縮または勃起障害を治療するという表示
- 疾患により障害のある身体構造または身体機能を復元するという表示（四肢切断患者が人工装具によりバスケットボールができるようになるという表示など）⁵

一般的健康の使用目的の第二分類は、以下の小分類に分けられる

- 1) 健康的な生活様式の一環として、特定の慢性疾患または慢性的症状のリスクの軽減を助けると考えられる選択を促進、追跡、および/または奨励する使用目的
- 2) 健康的な生活様式の一環として、特定の慢性疾患または慢性的症状がありながら健康的な生活を支援すると考えられる選択を促進、追跡、および/または奨励する使用目的

疾患に関連した一般的健康機器のいずれの小分類の表示にも、健康的な生活様式を選択する

⁵ 疾患による障害のある身体構造または身体機能の復元を目的とした機器は、個別に分類されたレクリエーション的使用機器または一般的な分類で分類された製品としてFDAによる規制を受ける場合がある。例えば、障害者が走ることができるようにすることを目的とした義肢は、21 CFR 890.3420または21 CFR 890.3500による規制を受ける。

ことにより、慢性疾患または症状のリスクまたは影響が軽減する可能性があるということが十分に理解されているという言及が含まれている必要がある。つまり、健康的な生活様式を選択が健康的な予後において重要な役割を果たすという主張が一般的に受け入れられている必要がある。そのような関連性は通常、論文審査のある専門誌に記載されている。健康的な生活様式がリスクの軽減する、あるいはまたは疾患を有しながら健康的な生活を支援できる様な慢性疾患の例としては、心臓疾患、高血圧、II型糖尿病などがある。

疾患に関連する一般的健康機器表示の第二分類の例としては、以下のものがある。

- 製品Xは、健康的な生活様式の一環として、高血圧のリスクを権限できる可能性がある身体活動を促進する。
- ソフトウェア製品Yは、カロリー摂取量を追跡記録し、健康的な食事プランを管理して健康的な体重とバランスの取れた食生活を維持することができる。健康的な体重とバランスの取れた食生活により、高血圧とII型糖尿病に罹患しながら健康的な生活を送ることができると考えられる。
- 製品Zは睡眠パターンを記録し、健康的な睡眠週間を促進することにより、健康的な生活習慣の一環として、II型糖尿病を発症するリスクを軽減することができると考えられる。

IV. 低リスク

CDRHの一般的健康のポリシーは、使用者の安全性に対する固有のリスクを有するデバイスに拡張されるものではない。

本ガイダンスの目的において機器が低リスクかどうかは、製品が以下に該当するかどうかによって決定される。

- 1) 侵襲的であるかどうか。⁶
- 2) レーザー、放射線の曝露、インプラントによるリスクなど、機器の制御が適用されない場合、使用者の安全性に対しリスクを及ぼす可能性がある介入または技術が含まれるかどうか。
- 3) 使用可能性について新たな問題を引き起こすかどうか。

⁶ 本ガイダンスにおいて、「侵襲的」は、身体の皮膚または粘膜に浸透または貫通することを意味する。

4) 生体適合性についての問題を引き起こすかどうか。

上記のいずれかについて該当する場合、その危機は低リスクの一般的健康機器ではなく、このガイダンスは適用されない。

以下に、ユーザーの安全性に対する固有のリスクがあり、本ガイダンスに記載する「低リスク」の機器とは見なされない製品の例を示す。

- 日焼け目的で販売促進された太陽灯製品の、皮膚がんのリスク上昇を含む（これに限定されない）、紫外線照射により使用者の安全性に対するリスク。
- セルフイメージの改善または性的機能の向上について販売促進されたインプラントの、脱腸やインプラントの材料に対する有害反応などの使用者に対するリスク、移植手順に関連するリスク。
- 皮膚を活性化させることにより使用者の見た目に対する自信を高めると表示されたレーザー製品。皮膚の活性化や使用者の見た目の向上に関する表示は一般的な健康性に関する表示であるが、レーザーの技術には皮膚および眼のやけどの危険性や、ラベル表示およびその他の機器制御で対応することができる有用性の考慮事項がある。

機器が本ガイダンスにおける低リスクであるかどうかを評価する上で、FDAは、CDRHが積極的に上記のような問題の製品と同じタイプの種類の製品を積極的に規制するかどうかについても検討することを推奨している。例えば、CDRHは現在、21 CFR 876.5020に基づき、特別管理による市販前通知が免除されたクラスIIの機器である成功のために十分な陰茎硬度を確立または維持することを目的とした、外付陰茎硬化装置を規制している。これらの機器を特別に管理することにより、組織の損傷、外傷、感染症など（これに限定されない）、これらの機器を使用することにより生じる健康へのリスクに対応している。⁷そのため、こうした種類の機器は、低リスク一般的健康機器とは見なされない。

⁷ FDAガイダンス：クラスII特別管理ガイダンス文書：外部陰茎硬化装置（2004年12月28日発行）を参照（<http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm072098.htm>）

V. 低リスクの一般的健康機器の例

事例1: モバイルアプリケーションが、人を「落ち着かせ、リラックスさせる」、「ストレスと管理する」音楽を再生する。

これらの表示は、リラクゼーション又はストレス管理にのみ関連し、疾患や医学的症状には関連しないため、一般的な健康に関する表示である。また、音楽を再生する技術には、使用者の安全性に対する固有のリスクはない。そのため、この製品は低リスク一般的健康機器の2つの基準を満たす。

事例2: 毎日のエネルギー消費量および心臓血管系のトレーニング活動の監視記録のみを行い、「運動活動を認識し、良好な心臓血管系の健康を維持することができる」モバイルアプリケーション。

この表示は、全体的な健康の関連についてのみ特定の器官に関連しており、疾患または医学的症状については言及していない。また、運動活動の監視または記録にリスクが生じる（不正確な記録など）範囲内において、疾患または医学的症状に関する表示がない場合、使用者の安全性に対するリスクは低い。そのため、この製品は低リスク一般的健康機器の2つの基準を満たす。

事例3: モバイルアプリケーションが食事を監視・記録し、「体重管理のため食事活動を管理し、不健康な食事活動を送る使用者、医療介護提供者、家族に注意喚起する」。

この表示は、食生活の選択および体重管理に関連するため、一般的な健康に関する表示である。また、食事量の監視または記録の技術が使用者の安全性にもたらすリスクは低い。そのため、この製品は低リスク一般的健康機器の2つの基準を満たす。

事例4: 運動や歩行時に使用者の心拍数を監視すると表示する携帯型製品。

この表示は、運動および歩行にのみ関連し、疾患や医学的症状には関連しない。そのため、これは一般的な健康に関する表示である。また、監視するための技術が使用者の安全性にもたらすリスクは低い。そのため、この製品は低リスク一般的健康機器の2つの基準を満たす。

事例5: 顔、手、足の角質を機械により除去し、皮膚を滑らかに柔らかくすることを目的とした製品。

この表示は、自己評価に関連し、特定の疾患や医学的症状について言及していない。