事例 1B（*事例 1A からの続き*）　ある企業は、自社の処方薬 *NoFocus* に対し、1 通のメッセージまたはツイートあたりの文字スペースが 140 に制限されている Twitter での販促を検討している。*NoFocus* は、軽度から中程度の記憶障害が適応症である。*NoFocus* の PI には枠組みやその他の警告はなく、既知の致死性または生命を脅かすようなリスクは記載されていない。*NoFocus* に関連する最も重大な使用上の注意は、同製品が発作性疾患のある患者において発作を引き起こす可能性があるという点である。ツイート内にベネフィット情報が提示されているため（事例 1A）、同企業は少なくとも、同じツイートの中で *NoFocus* に伴う最も重大なリスクを伝達することが望ましい。また、同企業は、同じツイートの中に、より完全な *NoFocus* のリスク情報に関する考察にアクセスできる直接のハイパーリンクを組み入れることが望ましい。さらに、利用できるフォーマット化機能を考慮した場合に、リスク情報の視認性は、そのツイートに記載されているベネフィット情報と同等であることが望ましい。

同企業は、ツイートの中に、次に挙げるベネフィット情報とリスク情報を組み入れるよう検討している。

NoFocus－軽度から中程度の記憶障害に。ただし、発作性疾患のある患者では発作を引き起こすおそれがある。www.nofocus.com/risk　[*73/140*]

上記の例では *NoFocus* のベネフィット情報は正確かつ誤解を生じないものであり、ツイートの中で、ベネフィット情報とともに、*NoFocus* に付随する最も重大なリスクが伝達されている。また、同企業は、*NoFocus* についての包括的なリスク情報の提示に充てられている（製品ウェブサイト内の）「安全上重要な注意事項」のウェブページにアクセスする直接のハイパーリンクを組み入れている。さらに、www.nofocus.com/**risk**（強調表示は付け加えたもの）という URL は、ランディングページがリスク情報で構成されていることを表わすものであり、URL に販促を感じさせる意味合いが含まれていない。同企業はこのツイートにおいて、ベネフィット情報と同等の形態でリスク情報を伝達している。このツイートへの *NoFocus* の他の製品情報の組み入れに関するさらに詳しい考慮事項は、本ガイダンス草案の第 VI 節に記載した事例 1C を参照されたい。

事例 2B（*事例 2A の続き*）　ある企業は、自社の処方薬 *Headhurtz* に対し、Google の Sitelinks を用いた販促を検討している。[18]　*Headhurtz* は外傷性脳損傷に伴う重度の頭痛が適応症である。*Headhurtz* の PI には脳腫脹のおそれについての枠組み警告のほか、潜在的に致死性の薬物反応と生命を脅かすおそれのある心拍数の減少についての警告が記載されている。スポンサーリンクフォーマットの中にベネフィット情報が提示されていることから（事例 2A）、同企業は、同じスポンサーリンクフォーマットの中で *Headhurtz* に伴う最も重大なリスクを伝達することが望ましい。また、同企業は、同じスポンサーリンクフォーマットの中に、より完全な *Headhurtz* のリスク情

[18] Google の「Sitelink 拡張子」フォーマットでは、表示されている URL（この例では www.headhurtz.com）に加え、最大で 6 つまで追加リンク（Sitelink）を表示することができる。Google の設定したパラメータでは、個々の Sitelink に対するリンクのテキストは 25 文字以内でなければならない。リンクテキストは、そのリンクのランディングページに記載されている内容に直接の関連性を持ちながら、異なる内容を指摘するものでなければならない。すなわち、どの Sitelink も同じランディングページや同じ内容に連結することはできないことになる。さらに、Sitelink は、リンク先 URL と同じランディングページ（この例では www.headhurtz.com のランディングページ）と直接つながっていてはならない。また、個々の Sitelink のもとで表示するため、最大で二つまで任意の記述行（1 行あたり 35 文字以下）を作成してもよい。これらは 2014 年 1 月 22 日の時点における最新情報である。

報に関する考察にアクセスできる直接のハイパーリンクを組み入れることが望ましい。さらに、利用できるフォーマット化機能を考慮した場合に、リスク情報の視認性は、そのスポンサーリンクフォーマットに記載されているベネフィット情報と同等であることが望ましい。

同企業は、スポンサーリンクフォーマットの中に、次に挙げるベネフィット情報とリスク情報を組み入れるよう検討している。

Headhurtz [*9/25*]
www.headhurtz.com [*17/35*]
外傷性の損傷による重度の頭痛に[*15/70*]
枠組み警告 [*5/25*]
脳腫脹のおそれ [*7/35*]
警告 [*2/25*]
生命に危険のある心拍数の低下[*14/35*]

警告 [*2/25*]
致死のおそれのある薬物反応[*13/35*]
リスク情報 [*5/25*]
安全上重要な注意事項[*10/35*]

上記の例では *Headhurtz* のベネフィット情報は正確かつ誤解を生じないものである。脚注 18 に概略を述べた Google のフォーマット化要件に従い、同企業では 6 つの Sitelink のうち 3 つを利用することにより、枠組み警告と致死性および生命に危険のあるリスクに関する追加の警告を含め、*Headhurtz* に付随する最も重大なリスクを伝達することを選択した。すなわち、スポンサーリンクフォーマットの中で、ベネフィット情報とともに、*Headhurtz* に付随する最も重大なリスクが伝達されている。また、同企業は、*Headhurtz* についての包括的なリスク情報に直接アクセスできる 4 つ目の Sitelink を組み入れている。さらに、脚注 18 に概略を述べた Google のリンク要件に従い、同企業では、それぞれ内容が異なる 4 つのランディングページを作成している。一つ目の Sitelink は脳腫脹のおそれについての枠組み警告に関する詳細な情報の提示に充てられているウェブページへの直接のハイパーリンク、二つ目と三つ目の Sitelink はそれぞれ、これらの Sitelink における記述の中で伝えられる具体的な警告（すなわち、致死のおそれのある薬物反応と生命の危険のある心拍数の低下）についての考察に充てられているウェブページへの直接のハイパーリンクである。さらに、四つ目の Sitelink として、*Headhurtz* についての包括的なリスク情報の提示に充てられている（製品のウェブサイト内の）「安全上重要な注意事項」のウェブページにアクセスする直接のハイパーリンクを組み入れている。同企業はこのスポンサーリンクフォーマットにおいて、ベネフィット情報と同等の形態でリスク情報を伝達している。このスポンサーリンクフォーマットへの *Headhurtz* の他の製品情報の組み入れに関するさらに詳しい考慮事項は、本ガイダンス草案の第 VI 節に記載した事例 2C を参照されたい。

VI. 文字スペースが制限されたインターネット／ソーシャルメディアプラットフォームへの他の製品情報の記載に関する勧告

ガイダンス草案の本節では、文字スペースが制限されたインターネット／ソーシャルメディアプラットフォームへの他の製品情報（適宜、リスク／ベネフィット情報以外に必要になる特定の製品情報など）を組み入れる際の補助的な勧告を提示する。文字スペースの限られた通信へのベネフィット情報とリスク情報の両方の組み入れに加え、該当する他の法律上の要件についても考慮しなければならない場合がある。

文字スペースが制限されたインターネット／ソーシャルメディアプラットフォーム上で製品情報を伝達する際には、企業は次の点について考慮することが望ましい。

- FD&C 法の第 502(e)、(n)、および(r)（21 USC 352(e)、(n)、(r)）は、ラベリングおよび処方薬や制限付き機器の広告では、正式名に添えて商品名または商標名を付記するよう義務付けている。医薬品規制は、商標権のある名称または呼称と正式名を直接併記するよう具体的に規定している（21 CFR 201.10(g)(1)および 202.1(b)(1)）。[19]

- 医薬品規制はまた、広告において、少なくとも一つ以上の具体的な剤形の名称をはっきりと視認できる形で表示するとともに、これらの表示と直接併記する形で、FD&C 法の第 502(n)条で規定されている成分量情報を提示するよう定めている。広告中に他の剤形がリストされている場合は、最もはっきりと認識できるこれらの剤形名のリストと同等の視認性で、これらの剤形に関する成分量情報を直接併記しなければならない（21 CFR 202.1(d)(2)）。

文字スペースに制限のあるインターネット／ソーシャルメディアプラットフォームを使用する場合に定められている上述の規制上の規定について、次に挙げるアプローチが適用されていれば、当局は異議を唱えない意向である。

- 企業は、文字スペースの限られた通信の中で、登録されている名称（商品名または商標名）と（医薬品の）正式名（一般名と呼ばれることが多い）の両方を伝達することが望ましい。製品の一般名は、商標名のすぐ右か、もしくはすぐ下にリストすることが望ましい。

- 文字スペースに制限のある通信に提示した各ハイパーリンクに付随するランディングページでも、前項に勧告したように、企業は商標名と正式名の両方を伝達することが望ましい。また、処方薬について、企業ははっきりと視認できる方法で、少なくとも一つ以上の剤形と成分量情報を商標名および正式名と直接併記することが望ましい。

また、当局は、（科学的なものも医学的なものも含む）一般的な略語や句読点、およびその他の記号は、多くのケースにおいて文字スペースの制約に対処するのに合理的に使用できるものと考えている。以下に、当局が異議を唱えることのないこれらの使用例を提示する。

- 一般的に認識されている言語記号を単語に置き換えて使用してもよい。例えば、「*および*」という単語の代わりにアンパサンド記号（&）を使用することができる。

- 情報を提示しやすくするため、句読点を使用してもよい。例えば、ベネフィット情報とリスク情報を分離しやすいよう、ダッシュを使用することができる。

- 化学成分名を表わすのに、科学的な略語を使用してもよい（例えば塩酸塩には「HCl」、臭化水素酸塩には「HBr」など）。

[19] FDA は、販促における製品名の配置とサイズを扱った個別のガイダンスを作成している。以下のアドレスから入手できる「*広告および販促用ラベリングにおける製品名の配置、サイズ、視認性*」という表題のガイダンス草案を参照のこと。
http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm070076.pdf

事例 1C（事例 1B の続き） ある企業は、自社の処方薬 *NoFocus* に対し、1 通のメッセージまたはツイートあたりの文字スペースが 140 に制限されている Twitter での販促を検討している。*NoFocus* は、軽度から中程度の記憶障害が適応症である。*NoFocus* の PI には枠組みやその他の警告はなく、既知の致死性または生命を脅かすようなリスクは記載されていない。*NoFocus* に関連する最も重大な使用上の注意は、同製品が発作性疾患のある患者において発作を引き起こす可能性があるという点である。FDA が認可した名称は *NoFocus（rememberine hydrochloride）カプセル* であり、*NoFocus* は 200 mg のカプセルとして市販されている。第 IV 節および V 節で詳述したように、文字スペースの限られた通信内でベネフィット情報とリスク情報を伝達するための要素を考慮に入れるだけでなく、同企業はそのツイートにおいて商標名と正式名も伝達することが望ましい。

同企業は、ツイートにおいて、ベネフィット情報およびリスク情報とともに、次に挙げる製品情報を記載するよう検討している。

> 軽度から中程度の記憶障害に NoFocus（rememberine HCl）－発作性疾患のある患者において発作を引き起こすおそれがある。www.nofocus.com/risk [*86/140*]

上記の例では、商標名と正式名がツイートの中で一緒に伝達されている。正式名の提示の中で、企業が*塩酸塩*の代わりに *HCl* という略語を使用している点に留意されたい。また、同企業はダッシュを用いることによって、追加のスペースを使用することなくベネフィット情報とリスク情報を分けている。事例 1B に明記したように、同企業は、*NoFocus* についての包括的なリスク情報の提示に充てられている（製品ウェブサイト内の）「安全上重要な注意事項」のウェブページにアクセスする直接のハイパーリンクを組み入れている。ランディングページの最上部では、「NoFocus（rememberine hydrochloride） 200 mg カプセル」のように、再び商標名と確定名を表記するとともに、剤形と量に関する情報を直接併記している。事例 1A、1B、および 1C において全体的に説明したように、FDA が *NoFocus* に対するこのツイートに異議を唱えることはないものと思われる。

事例 2C（事例 2B の続き） ある企業は、自社の処方薬 *Headhurtz* に対し、Google の Sitelinks を用いた販促を検討している。*Headhurtz* は外傷性脳損傷に伴う重度の頭痛が適応症である。*Headhurtz* の PI には脳腫脹のおそれについての枠組み警告のほか、潜在的に致死性の薬物反応と心拍数の減少が生命を脅かすおそれがあることについての警告が記載されている。FDA が認可した名称は *Headhurtz（ouchafol）錠剤* であり、*Heathurtz* は 200 mg の錠剤として市販されている。第 IV 節および V 節で詳述したように、文字スペースの限られた通信内でベネフィット情報とリスク情報を伝達するための要素を考慮に入れるだけでなく、同企業はそのスポンサーインクフォーマットにおいて商標名と正式名も伝達することが望ましい。

同企業は、スポンサーリンクフォーマットの中に、*Headhurtz* に関するベネフィット情報とリスク情報に加え、次の製品情報を組み入れるよう検討している。

> Headhurtz (ouchafol) [*20/25*]
> www.headhurtz.com [*17/35*]
> 外傷性の損傷による重度の頭痛に [*15/70*]
> 枠組み警告 [*5/25*]　　警告 [*2/25*]
> 脳腫脹のおそれ [*7/35*]　　致死のおそれのある薬物反応 [*13/35*]

警告 [*2/25*]
生命に危険のある心拍数の低下 [*14/35*]

リスク情報 [*5/25*]
安全上重要な注意事項 [*10/35*]

上記の例では、スポンサーリンクフォーマットにおいて、商標名と正式名がともに伝達されている。事例 2B に明記したように、脚注 18 に概略を述べた Google のリンク要件に従い、同企業では、それぞれ内容が異なる 4 つのランディングページを作成し、*Headhurtz* のリスク情報を伝えている。各ランディングページの最上部では、「Headhurtz（ouchafol） 200 mg 錠剤」のように、再び商標名と確定名を表記するとともに、剤形と量に関する情報を直接併記している。事例 2A、2B、および 2C において全体的に説明したように、FDA が *Headhurtz* に対するこのスポンサーリンクフォーマットに異議を唱えることはないものと思われる。

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

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「業界向けガンダンス：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性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にアクセス許可され、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

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ト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

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）」という言葉は何かが示唆、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にない場合がある。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] 特定のモバイルメディカル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：モバイルメディカルアプリケーション（2013年9月25日発行）（http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf）を参照のこと。