

第2回 産業サイバーセキュリティ研究会 WG1 工場SWG

医療機器における サイバーセキュリティ対応の取り組み

2022年2月28日

一般社団法人 日本医療機器産業連合会

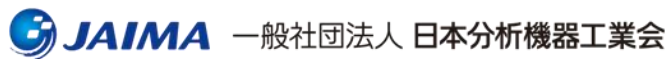
医機連みらい戦略会議 サイバーセキュリティTF

連絡調整会議 医療機器サイバーセキュリティ対応WG

□ (一社)日本医療機器産業連合会の概要

日本医療機器産業連合会（医機連）

創設 : 1984年
加盟団体 : 20（企業約4,280社）
就業者 : 約12万人
賛助会員 : 約160



多様な医療機器（約30万種）



1. 医療機器におけるサイバーセキュリティ対応 (1/2)

(1) 医療分野と医療機器

医療分野における情報化・ネットワーク化が進展し、それに伴い医療機関におけるサイバーセキュリティ対応がますます重要になっている。特に医療機関で使用される医療機器は医療安全(*1)に直接つながるため、医療機器のサイバーセキュリティ対応は今後の重要な課題となっており、医療機関、医療機器企業(*2)、及び他の全てのステークホルダーが連携して対応することが必須となっている。[資料4 参照]

(2) 国の施策

医療機器企業等に向けたサイバーセキュリティ対応に関する多くの通知等が発出されており、医療機器規制の国際調和を目指すIMDRF(*3)から発行された「医療機器サイバーセキュリティガイダンス (IMDRFガイダンス)」を薬機法(*4)による医療機器の規制に取り入れ、2023年を目途に本格運用するとの方針が示されている。

[資料2 参照]

また、医療機関等向け「安全管理ガイドライン(*5)」では「医療機関のサイバーセキュリティ対策チェックリスト」等が示されている。

(*1) 医療安全：ここでは患者安全を中心に、使用者、医療従事者等の安全も含めます。

(*2) 医療機器企業：ここでは製造販売業者、製造業者、販売業者、貸与業者、修理業者、等を指します。

(*3) IMDRF：International Medical Device Regulators Forum：国際医療機器規制当局フォーラム

(*4) 薬機法：医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律

(*5) 安全管理ガイドライン：医療情報システムの安全管理に関するガイドライン

1. 医療機器におけるサイバーセキュリティ対応 (2/2)

(3) 行政と工業会の取り組み

厚労省：

- ・「医療機器のサイバーセキュリティの確保及び徹底に係る手引書について」の通知が発出され、別添として「製造販売業向け手引書(*6)」が公開された。
(2021年12月24日)
- ・医療機器のサイバーセキュリティ対応では国際整合が重要であり、「製品のライフサイクル全体を通じて、システムの再現性、信頼性及び性能を発揮できるよう、設計及び**製造**されなければならない」との趣旨が基本要件基準に盛り込まれる方向。
(2023年を目途)

医機連：[資料1 参照]

- ・今後、SBOMの扱いレガシー機器の扱い、市販後安全対策の検討を進め、製造販売業向け手引書の追補を予定。
- ・AMED研究班(*7)に参画し「医療機関向け手引書(*8)」を策定中。
- ・医療機器企業に対して、周知・啓発活動を推進している。

(*6) 製造販売業向け手引書：「医療機器のサイバーセキュリティ導入に関する手引書」

(*7) AMED研究班：令和3年度医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究

(*8) 医療機関向け手引書：医療機関における医療機器のサイバーセキュリティ確保のための手引書（仮）

2. 医療機器の役割りと課題

(1) 医療安全の確保への寄与

- ・サイバーセキュリティ対応された製品の提供、及びサービス体制構築。
 - ・医療現場でサイバーセキュリティ対応が確実に実施されることへの貢献。
- ⇒医療機器企業は薬機法、及び関係省令等に沿って事業を行っている。

(2) 医療機器の安定供給

- ・重要インフラである医療に対して、必要な医療機器を製造して安定供給すること。
- ⇒BCP（事業継続計画）を策定。
- ・研究開発/製造/サービス等の各工程、及びサプライチェーン全体のサイバーセキュリティ対応が重要。
 - ・部品調達の確保、及び組立・調整・検査の人材確保も必要。

3. 医療機器の製造について

(1) 医療機器の特徴

- ・医薬品、医療機器等取り扱いの基本は薬機法(*5)
- ・臨床現場でのニーズに基づき改善改良が繰り返される
- ・多種多様であり、多品種・少量生産
ー 鋼製小物・コンタクトレンズ・カテーテル・生体モニター・内視鏡・画像診断システム、等々

(2) 医療機器の製造

- ・薬機法、QMS省令(*9)等の要件を満たす必要が有る。[資料3 参照]
- ・多品種少量生産 ⇒ 多くの場合、大量生産を前提としたFAシステムは馴染まない。
- ・生産管理や検査工程などでIT化は進められており、医療機器製造においても工場の特性に留意したセキュリティ対策が必要であることは、他の製造業一般と同じ。

(3) 工場SWGの取り組みに対する医療機器の現在の認識

- ・医療機器製造業に特化したガイドラインというものは想定しにくい（多種多様な製造現場があり、類型化が困難であるため）
 - ・一般的な工場向けガイドラインがあれば、医療機器製造現場にとっても有用である。
- ⇒工場SWGの取り組みを理解し、参考にさせていただきたい。

(*9) QMS省令：医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令

4. まとめ（医療機器）

- 医療機器・医療現場におけるサイバーセキュリティ対応の必要性が高まっている
- 国際整合の一環としてIMDRFガイダンスの内容を薬機法規制に取り入れる方向
- 医療機器は多種多様であり、多品種・少量生産
⇒多くの場合、大量生産を前提としたFAシステムには馴染まない
- 工場の特性に留意したセキュリティ対策が必要（他の製造業と同様）
⇒工場SWGの取り組みに注目し、「工場セキュリティガイドライン」等に期待

[資料 1 - 1] 医機連のサイバーセキュリティ対応強化の取り組み

医機連産業ビジョン（2018年10月制定）

- ・新たに取り組むべき重点テーマの一つ：「サイバーセキュリティ強化の推進」
- ・ベースラインの活動としてIMDRF※1) サイバーセキュリティガイダンスへの意見発出

■ 第16回内閣官房健康・医療戦略参与会合

- 医機連会長より「サイバーセキュリティ対応の提言」
（2019年5月）



■ 医機連みらい戦略会議に「サイバーセキュリティTF」 を立ち上げて活動開始（2019年8月）

- サイバーセキュリティに関する業界全体の意識向上
- AMED研究班活動への業界意見の反映と研究成果の共有
- 政策提言による業界の活性化
- 企業、医療機関の実態把握
- 情報共有の体制検討

■ 国際政策戦略委員会にサイバーセキュリティWG を立ち上げ（2019年8月）

- IMDRFガイダンスへの意見調整と発出

○厚労省課長通知（2020年5月）

- ・今後3年を目途にIMDRFガイダンスを導入

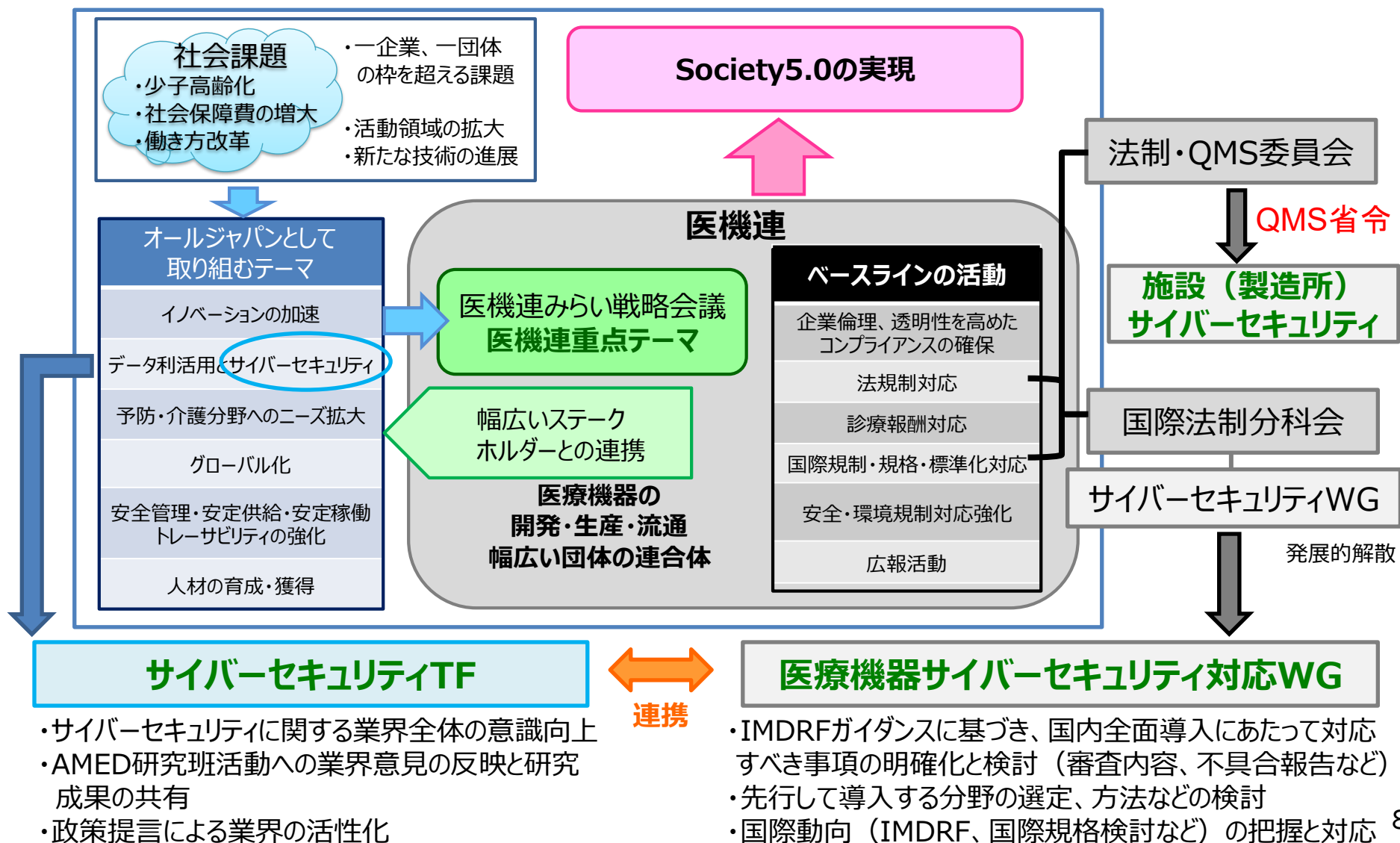


■ サイバーセキュリティWGを発展的に解散し、連絡調整会議に「医療機器サイバーセキュリティ対応WG」 を立ち上げ（2020年7月）

- IMDRFガイダンス国内全面導入への対応
- 実施事項(審査内容、不具合報告等)の明確化
- 先行導入する分野の選定、方法などの検討
- 国際動向(IMDRF、国際規格検討など)の把握

※1) International Medical Device Regulators Forum
国際医療機器規制当局フォーラム

[資料 1 - 2] 医機連のサイバーセキュリティ対応強化の取り組み体制



〔資料 2〕 IMDRFガイダンスの国内導入に向けた検討状況

国際動向

IMDRF Guidance

Sub-Guidance (SBOM and Legacy)

検討体制

AMED研究班調査活動

考え方を反映

2022年春・夏

AMED提言成果物

(医療機関向けにCS導入に向けた考え方を提言)

- 医療機関における医療機器導入時のCS導入の考え方、等

連携

医機連WG活動

(医機連TF活動による
医療業種との連携含む)

2021.12

製販業者向けガイダンス（手引書）にて技術基準等を明確化

初版

(CS対応の基本的
考え方※)

追補

SBoMの扱い
レガシー機器の扱い

追補

(市販後安全対策、
等)

随時、追補を実施

国内運用

課長通知

(2021/12/24)

紐づけ

関連法令・通知等

「医療機器のサイバーセキュリティの確保に関するガイダンスについて」(平成30年7月24日、薬生機審発0724第1号・薬生安発0724第1号)等

本格運用に向けた周知等

- ・IMDRFガイダンスに基づく本格運用の開始を周知
- ・医機連ガイダンス等の幅広い周知
- ・関連薬事制度の見直し・準備

※企業におけるCS体制構築の考え方、等
2023.夏

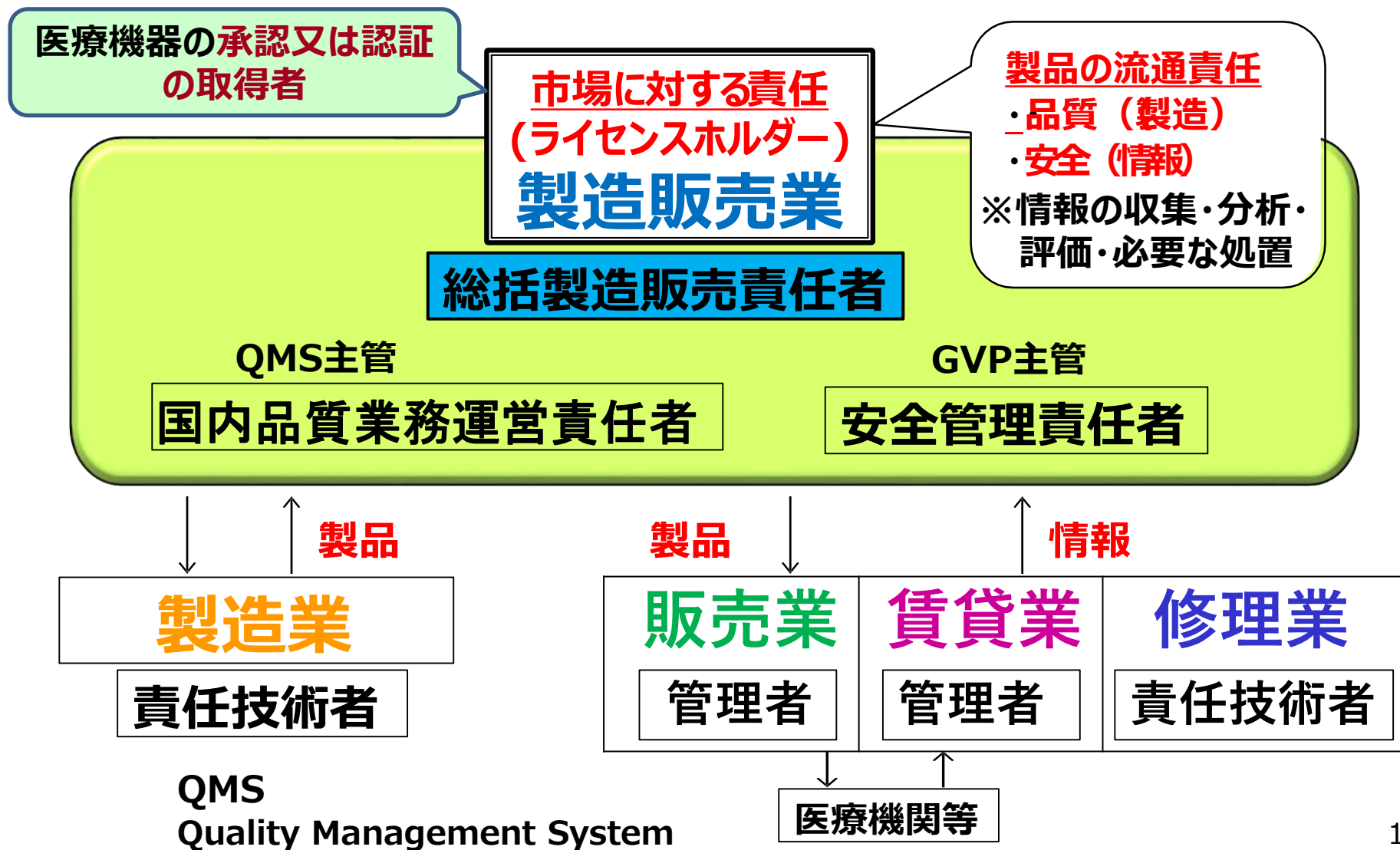
IMDRFガイダンスに基づく国内 対応を本格的に運用

- ・**基本要件基準改正** (CS要求事項を明確化)
- ・関係通知を改訂
- ※国際ガイダンスの改訂に合わせて都度更新

製品のライフサイクル全体を通じて、システムの再現性、信頼性及び性能を発揮できるよう、**設計及び製造**されなければならない。

出典：厚生労働省 医療機器審査管理課資料を基に作成

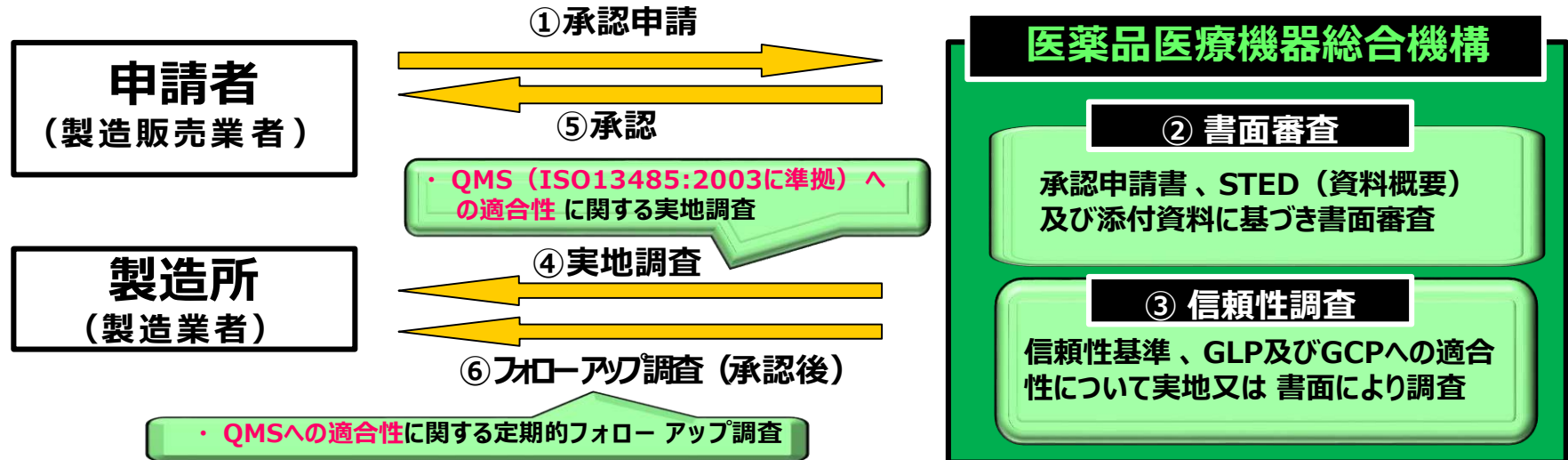
[資料 3 - 1] 薬機法における製造販売業等の業態の関係



PMDA 医療機器の承認申請・審査・製造販売承認より引用 (一部改変)

[資料 3 - 2] 医療機器の承認申請とQMS適合性調査

○ 医療機器の承認申請及び審査の手続き



○ QMSとQMS適合性調査

- ・日本：厚生労働省令第169号（QMS省令）
- ・米国：21CFR Part820（QSR：Quality System Regulation）
- ・EU圏：MDR：Medical Device Regulation
IVDR：In-vitro Diagnostics Regulation



世界的にISO13485に係るQMSの要求事項をベースにした
法規制が導入される方向となっている

PMDA「医療機器の承認申請・審査・製造販売承認」を基に作成

〔資料 3 - 3〕 QMS省令

「医療機器及び体外診断用医薬品の製造管理及び品質管理の基準に関する省令」

章	内容	条項	備考
第1章	総則 箇条5.5 外部委託, 5.6 ソフトウェアの使用(バリデーション), 8 文書の管理, 9 記録の管理(セキュリティ)	1～3	製造販売業者等の遵守事項
第2章	医療機器等の製造管理及び品質管理に係る基本的要求事項	4～64	ISO 13485 : 2016 に相当
第3章	医療機器等の製造管理及び品質管理に係る追加的要求事項	66～72の3	文書・記録保管 旧GQP関係等
第4章	生物由来医療機器等の製造管理及び品質管理	73～79	構造設備規則の内容を追加
第5章	放射性体外診断用医薬品の製造管理及び品質管理	80～81	構造設備規則関係
第5章の2	再製造単回使用医療機器の製造管理及び品質管理	81の2～81の2の6	管理に関する要求事項の追加
第6章	医療機器等の製造業者等への準用等 箇条84 製造販売業者等による管理(サプライチェーン)	82～84	輸出用QMS 委託先等QMS

ISO/TR 80002-2, NIST SP800-171等参照

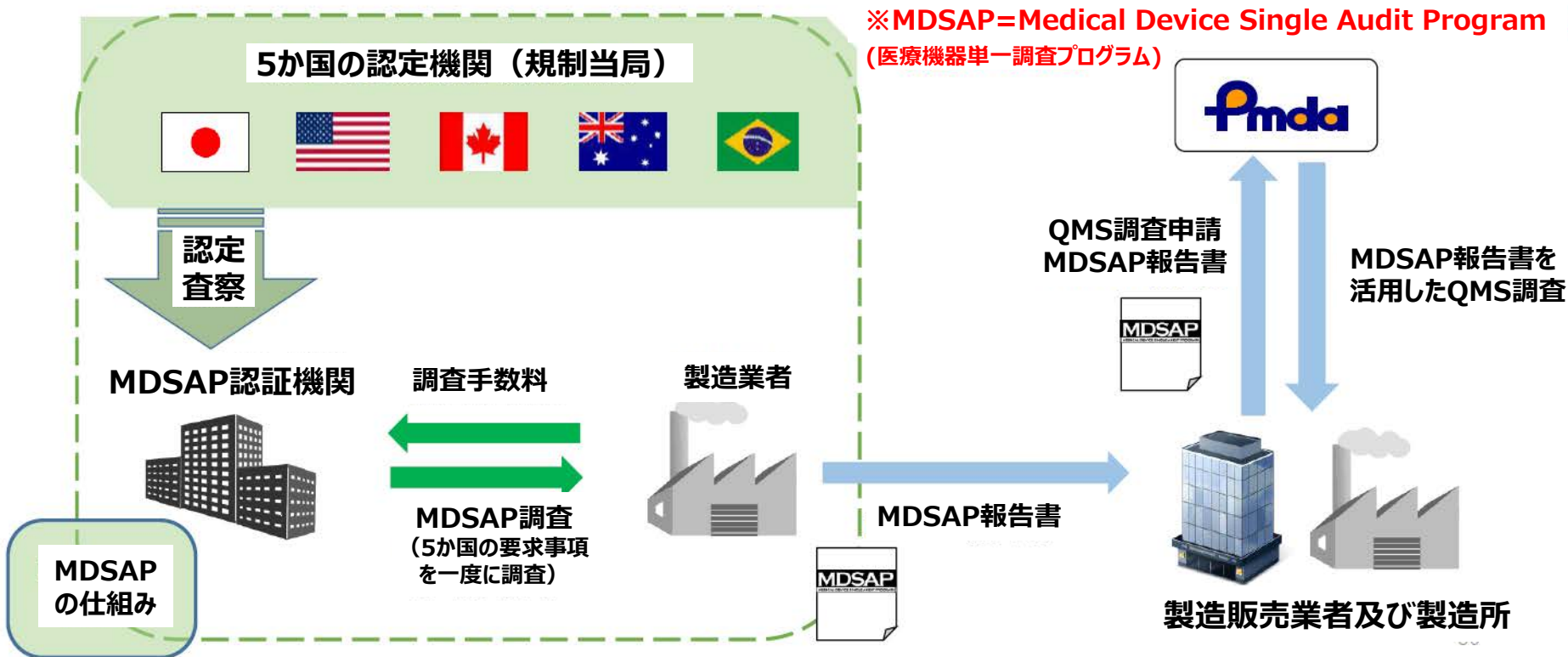
○「…製造販売業者は、供給する製品のサイバーセキュリティ対応に関する社内の方針・体制を品質システム等の一部として確立することが求められる。…」

「医療機器のサイバーセキュリティの確保に関するガイダンスについて」(2018年7月24日厚労省課長通知より)

12

[資料 3 - 4] 国際的なQMSに関する協働活動（MDSAP※）

MDSAP参加国（日本、米国、カナダ、オーストラリア、ブラジル）がQMS調査機関（MDSAP認証機関）を**共同で評価・認定**し、その質を一定程度に担保するとともに、MDSAP認証機関が実施した**QMS調査結果**（MDSAP調査報告書）の**各国での活用**を目指す。



PMDA 医薬品、医療機器等の製造管理及び品質管理（GMP、QMS等）より引用（一部改変）

[資料4] ヘルスケア業界の現状把握（インシデント等情報）

- Chinese hackers targeted Indian vaccine makers SII, Bharat Biotech
(サイバーセキュリティ企業Cyfirma社によると、**中国政府が支援する攻撃者グループ「APT10」(別名Stone Panda)が、ここ数週間、インドの製薬会社Serum Institute of India (SII)社とBharat Biotech社のITシステムを標的にしている。**SII社は多くの国でAstraZeneca社の新型コロナウイルスのワクチンを製造しており、間もなくNovavax社のワクチンの製造を開始する予定。また、Bharat Biotech社のワクチン「Covaxin」は、ブラジルを含む多くの国に輸出予定。新型コロナウイルスのワクチンにおいて、**インドと中国はライバル関係にあり、インドは世界で販売されているワクチンの60%以上を製造**している。Cyfirma社CEOのKumar Ritesh氏は「攻撃の目的は、知的財産を流出させ、中国がインドの製薬会社に対する競争上の優位性を得ることだ」と語る) 2021/3/2
<https://www.itnews.com.au/news/chinese-hackers-targeted-indian-vaccine-makers-sii-bharat-biotech-561626>
- Oxford University lab with COVID-19 research links targeted by hackers
(**英オックスフォード大学、新型コロナウイルスの研究を行っている構造生物学部門(Strubi)の研究室**でセキュリティインシデントが発生。同研究室への**不正アクセス手段の販売を目論む攻撃者によって、「生化学的調整装置」が侵害**された。同大学によると、臨床研究への影響はなく、患者データや記録に関連するシステムは侵害されていない。同大学は政府通信本部(GCHQ)に報告しており、英国サイバーセキュリティセンター(NCSC)がインシデント調査を実施予定) 2021/2/26
<https://www.zdnet.com/article/oxford-university-biochemical-lab-involved-in-covid-19-research-targeted-by-hackers/>
- House approves cyber funds in relief package as officials press for more
(**米下院、3月10日にCOVID-19 relief bill(COVID-19救済法案)を承認。**本法案で、**サイバーセキュリティと技術の近代化のために約20億ドル(約2,170億円)の資金が割り当てられる。**連邦政府のサイバーセキュリティを強化し、**ハッカーの攻撃を受けている新型コロナウイルスワクチンのサプライチェーンを保護する**ために、サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)には6億5千万ドル(約700億円)が割り当てられるが、**CISAは6億5千万ドルを超えるサイバーセキュリティ資金とリソースの提供**を議会に要請。本法案は、3月12日にバイデン大統領が署名予定) 2021/3/10
<https://www.msn.com/en-us/news/politics/house-approves-cyber-funds-in-relief-package-as-officials-press-for-more/ar-BB1esB1x?ocid=BingNewsSearch>
- Cyberattack on BHG opioid treatment network disrupts patient care
(米国の17州で80以上の外来診療所を運営している**外来オピオイド(麻薬性鎮痛薬)治療企業Behavioral Health Group(BHG)**、**12月第2週にサイバー攻撃を受け、約1週間にわたりITシステムと患者の治療に支障**をきたした。BHGのシステム技術チームは、安全かつ効率的な修復プロセスとシステムの復旧に注力しており、情報セキュリティ専門家とインシデント調査を実施中。BHGは、患者の治療は提供し続けている、としているが、自宅で使用するための治療薬をオピオイド依存の治療患者に提供している一部の診療所で、コンピュータが使用できず処方箋ラベルが印字できなくなったため、治療薬が提供できなかった) 2021/12/14
<https://www.bleepingcomputer.com/news/security/cyberattack-on-bhg-opioid-treatment-network-disrupts-patient-care/>

