令和６年度　医療機器製造販売業者のサイバーセキュリティ対策周知等事業

医療機関との連携及びPSIRTの実践

一般社団法人　日本医療機器産業連合会
医療機器サイバーセキュリティ対応WG

Ministry of Health, Labour and Welfare of Japan

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

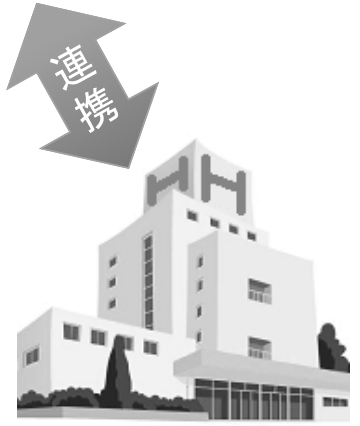
- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について（IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対するJIS T 81001-5-1の適用について

3. 医療機関との連携及びPSIRTの実践

4.「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

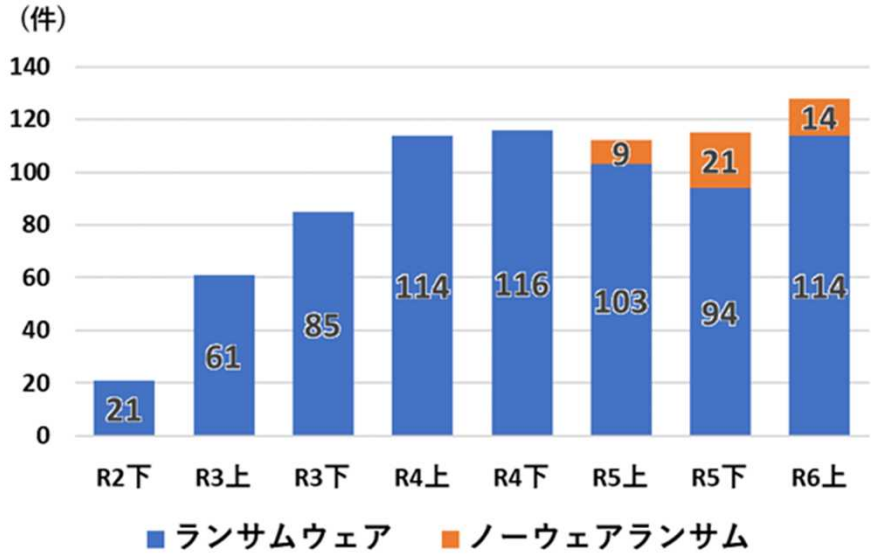


医療機関、
医療情報システム製造業者等

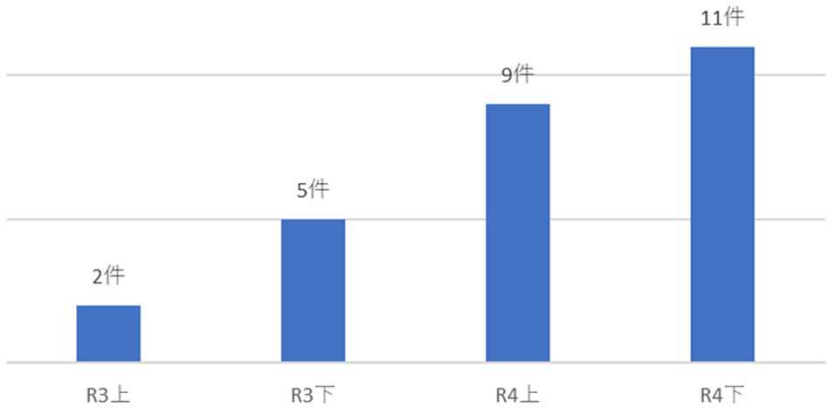
- 医療分野におけるサイバー事案の現状
- 医療機関向けに出ているサイバーセキュリティに係る通知等
- PSIRTの実践

医療分野におけるサイバー事案の現状

- 全体として、ランサムウェアによる被害は増加傾向。
- 医療分野においてもランサムウェア感染は増加。電子カルテシステムが使用不能となり、新規外来患者の受け入れ停止・制限などによる地域医療への影響が生じる事案が発生。



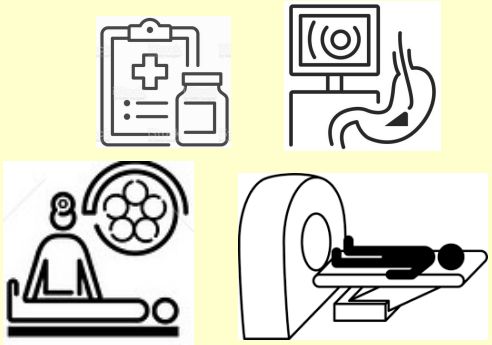
出典：警察庁サイバー警察局 令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

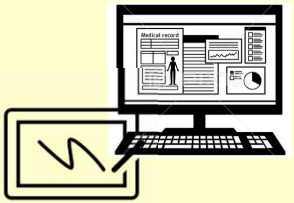


医療・福祉分野におけるランサムウェア被害件数

出典：警察庁サイバー警察局 サイバー事案の被害の潜在化防止に向けた検討会報告書 2023
https://www.npa.go.jp/bureau/cyber/pdf/20230406_2.pdf

医療機関内の主要なシステム類（一例）





医療機関内共通
- 電子カルテシステム
- オーダリングシステム
- 医事会計システム

等

部門システム
- 薬剤部門
- **臨床検査部門**
- **放射線部門**
- **手術部門**

等

その他
- 予約システム
- 案内表示システム
- 地域連携システム

等

・・・

経済財政運営と改革の基本方針2023（抄）

第４章 中長期の経済財政運営

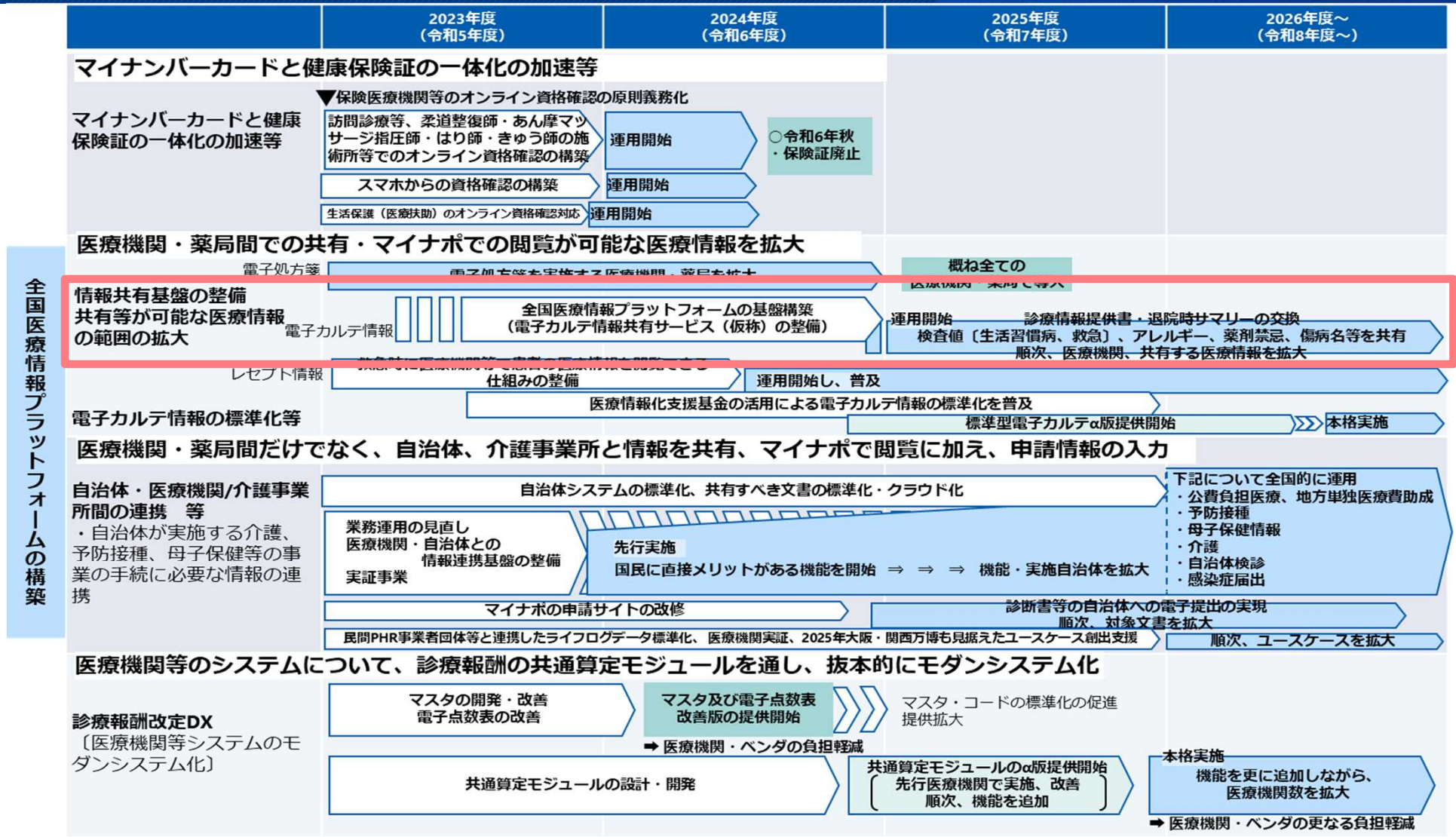
２． 持続可能な社会保障制度の構築

（社会保障分野における経済・財政一体改革の強化・推進）

医療ＤＸ推進本部において策定した工程表に基づき、医療ＤＸの推進に向けた取組について必要な支援を行いつつ政府を挙げて確実に実現する。マイナンバーカードによるオンライン資格確認の用途拡大や正確なデータ登録の取組を進め、2024年秋に健康保険証を廃止する。レセプト・特定健診情報等に加え、介護保険、母子保健、予防接種、電子処方箋、電子カルテ等の医療介護全般にわたる情報を共有・交換できる「全国医療情報プラットフォーム」の創設及び電子カルテ情報の標準化等を進めるとともに、ＰＨＲとして本人が検査結果等を確認し、自らの健康づくりに活用できる仕組みを整備する。その他、新しい医療技術の開発や創薬のための医療情報の二次利活用、「診療報酬改定ＤＸ」による医療機関等の間接コスト等の軽減を進める。その際、医療ＤＸに関連するシステム開発・運用主体の体制整備、電子処方箋の全国的な普及拡大に向けた環境整備、標準型電子カルテの整備、医療機関等におけるサイバーセキュリティ対策等を着実に実施する。

医療DXの推進に関する工程表〔全体像〕

第２回医療ＤＸ推進本部
資料３（令和５年６月２日）一部改変



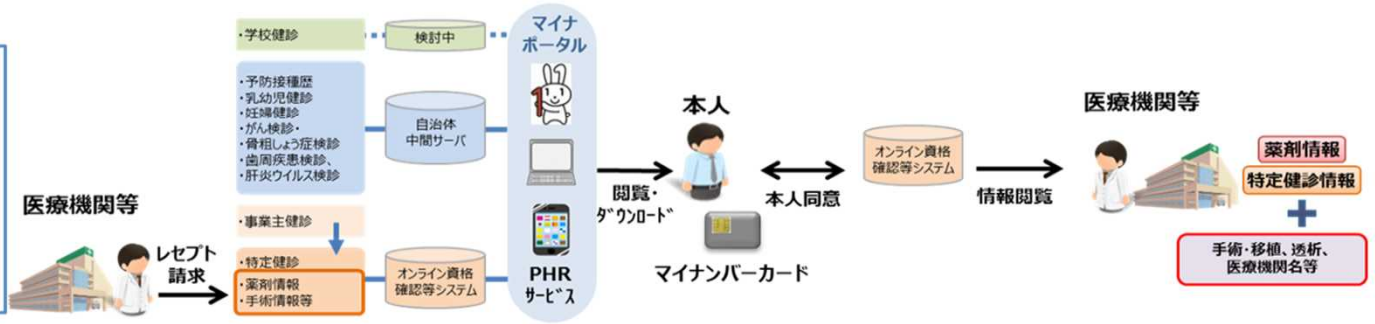
保険医療情報の閲覧の仕組み

第４回健康・医療・介護情報利活用検討会、
第３回医療等情報利活用ＷＧ及び第２回健診等情報利活用ＷＧ
（令和２年10月21日）資料抜粋

保健医療情報の閲覧の仕組みとしては、
① マイナポータル等を通じて、健康診断や予後管理に有用な保健医療情報を本人が閲覧できる仕組み（本人同意の下に、同じ情報が全国の医療機関等でも閲覧可能）
② 患者本人にとって最適な医療を実現するため、医療機関間で電子カルテ情報を相互に閲覧できる仕組み
の二つが存在。

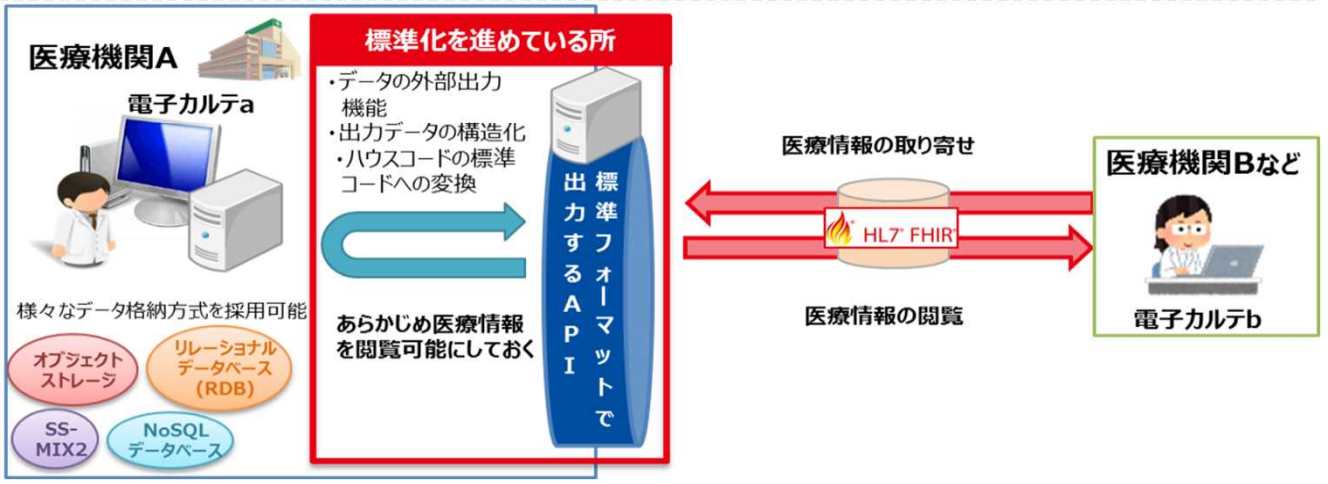
①

患者・国民が閲覧可能な仕組みにより、健康管理や予後管理、災害・救急時に有用な保健医療情報をマイナポータル等を通じて取得できるとともに、患者本人の同意を得た上で、医療機関等が保健医療情報を取得し、適切な医療を実現（災害・救急時は本人確認のみで情報を閲覧）



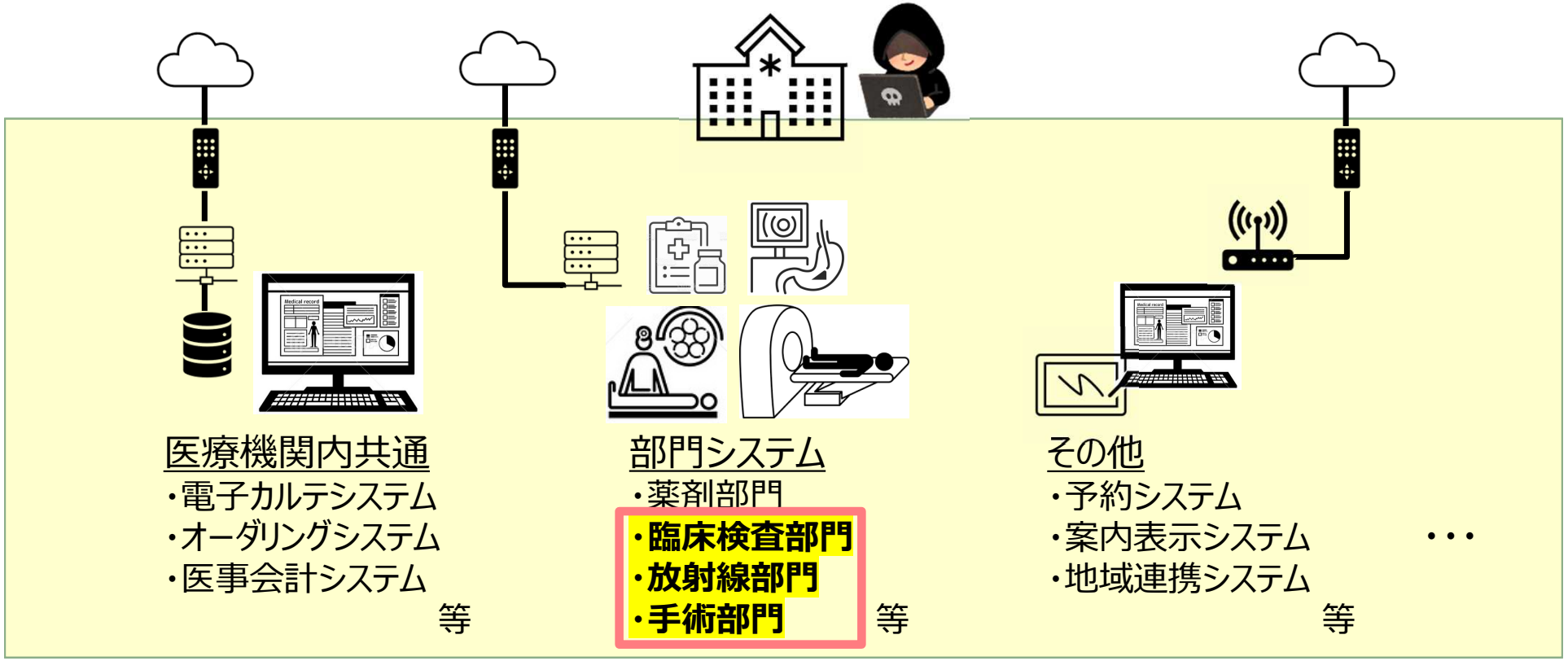
②

医療機関間で閲覧可能な仕組みにより、電子カルテ情報及び交換方式の標準化等を通じた情報の共有を通じて、円滑な紹介（逆紹介）、災害・救急時の利用、医療機器の共同利用等が可能



医療機器のサイバーセキュリティ対応について

- 医療機関には、導入されたシステムに合わせて複数の外部ネットワーク接続点があり、これまでのサイバーセキュリティインシデントの経験などから、厚生労働省通知等によりサイバーセキュリティ対応が求められている。
- 医療機器は、診断、治療若しくは予防に使用、又は構造、機能に影響を及ぼす性質上、サイバーセキュリティ対応を要する製品の医療における機能性と安全性保持のため、**医療機関の取組みへの理解と連携**が重要である。



- 医療分野におけるサイバー事案の現状
- 医療機関向けに出ているサイバーセキュリティに係る通知等
- PSIRTの実践

経済財政運営と改革の基本方針2023（抄）

第４章 中長期の経済財政運営

２． 持続可能な社会保障制度の構築

（社会保障分野における経済・財政一体改革の強化・推進）

医療ＤＸ推進本部において策定した工程表に基づき、医療ＤＸの推進に向けた取組について必要な支援を行いつつ政府を挙げて確実に実現する。マイナンバーカードによるオンライン資格確認の用途拡大や正確なデータ登録の取組を進め、2024年秋に健康保険証を廃止する。レセプト・特定健診情報等に加え、介護保険、母子保健、予防接種、電子処方箋、電子カルテ等の医療介護全般にわたる情報を共有・交換できる「全国医療情報プラットフォーム」の創設及び電子カルテ情報の標準化等を進めるとともに、ＰＨＲとして本人が検査結果等を確認し、自らの健康づくりに活用できる仕組みを整備する。その他、新しい医療技術の開発や創薬のための医療情報の二次利活用、「診療報酬改定ＤＸ」による医療機関等の間接コスト等の軽減を進める。その際、医療ＤＸに関連するシステム開発・運用主体の体制整備、電子処方箋の全国的な普及拡大に向けた環境整備、標準型電子カルテの整備、医療機関等におけるサイバーセキュリティ対策等を着実に実施する。

医療機関におけるサイバーセキュリティ対策の更なる強化策
－ 今後の医療機関におけるサイバーセキュリティ対策の基本方針 －

第12回 健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和４年９月５日）
資料抜粋

（１）短期的な医療機関におけるサイバーセキュリティ対策

１．平時の予防対応

①医療機関向けサイバーセキュリティ対策研修の充実　②脆弱性が指摘されている機器の確実なアップデートの実施
③医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築　④検知機能の強化
⑤G-MIS用いた医療機関への調査実施

２．インシデント発生後の初動対応

①インシデント発生時の駆けつけ機能の確保　②行政機関等への報告の徹底

３．日常診療を取り戻すための復旧対応

①バックアップの作成・管理の徹底　②緊急対応手順の作成と訓練の実施

（２）中・長期的な医療機関におけるサイバーセキュリティ対策

１．バックアップデータの暗号化・秘匿化

２．保健医療分野におけるSOCの構築

医療機関のサイバーセキュリティ対策に係る規制及び関連通知類

医療法　第25条第1項（立入検査）
医療法施行規則　第14条第2項

医療情報システムの安全管理
に関するガイドライン　第6.0版
（令和５年５月31日 産情発 0531 第１号）

医療機関における
サイバーセキュリティ対策チェックリスト
（令和５年６月９日 医政参発 0609 第１号）

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
手引書について
（令和５年３月31日 医政参発0331第1号・
薬生機審発0331第16号・薬生安発0331第8号）

医療機関におけるサイバーセキュリティ
確保事業
（令和6年2月15日 厚労省事務連絡）

医療機関の管理者が遵守するべき事項への位置づけ

第16回 健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和５年３月23日）
資料抜粋

これまでの本WGでの議論を踏まえ、下記の通り、医療機関の管理者が遵守するべき事項に位置づけた。

これまでのWGでの議論

○ 医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきたところ。昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。平時の予防対応として、脆弱性が指摘されている機器の確実なアップデートの実施等が必要。（第11回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和４年５月27日））

○ 医療機関がサイバーセキュリティを確保するための具体的な対策を明示し、ペナルティを課すのではなく、支援・助言を行うための検査になるような進め方が望ましい（（第11回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和４年５月27日））

○ 令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正を行う。（第12回健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和４年９月５日））

改正概要・対応の方向性

○ 医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○ 令和５年３月10日公布、４月１日施行（予定）

○ 「必要な措置」としては、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

○ 安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。

○ また、医療法第25条第１項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

◎医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条 （略）

2 病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

※ 下線部を新設。

医療法に基づく立入検査の概要

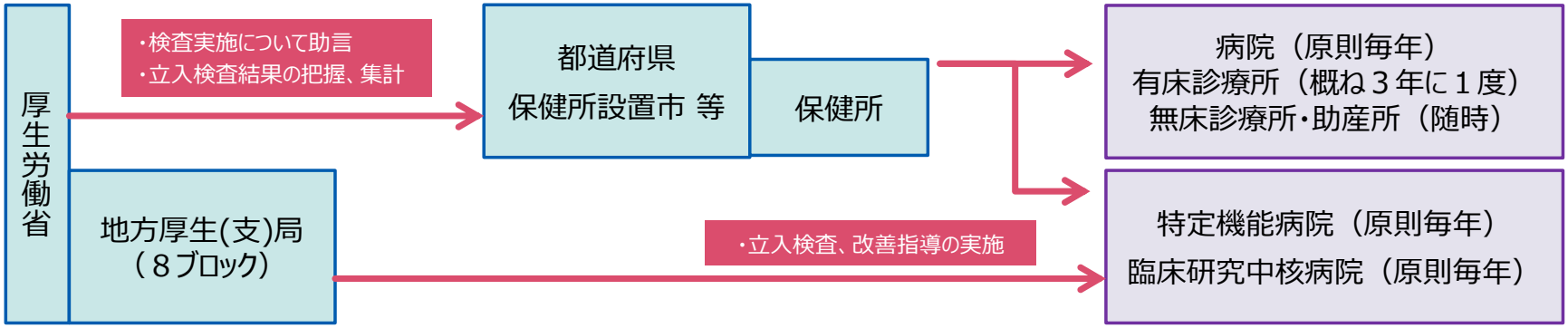
厚生労働省ホームページ

立入検査の目的

・病院、診療所等が法令により規定された人員及び構造設備を有し、かつ、適正な管理を行っているか否かについて検査し、不適正な場合は指導等を通じ改善を図ることにより、病院、診療所等を良質で適正な医療を行う場にふさわしいものとする。

立入検査の実施主体

・**医療法第２５条第１項による立入検査** ・・・ 各病院、診療所等に対し、都道府県等が実施
・**医療法第２５条第３項による立入検査** ・・・ 特定機能病院等に対し、国が実施



主な検査項目

○**病院管理状況**
➢カルテ、処方箋等の管理、保存　➢届出、許可事項等法令の遵守　➢患者入院状況、新生児管理等　➢医薬品等の管理、職員の健康管理
➢安全管理の体制確保　等
○**人員配置の状況**
➢医師、看護婦等について標準数と現員との不足をチェック
○**構造設備、清潔の状況**
➢診察室、手術室、検査施設等　➢給水施設、給食施設等　➢院内感染対策、防災対策　➢廃棄物処理、放射線管理　等

令和６年度　医療機関等におけるサイバーセキュリティ対策チェックリスト

第22回 健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和６年６月10日）
資料４抜粋

- 厚生労働省においては、令和５年４月から、医療法に基づく医療機関に対する立入検査に、サイバーセキュリティ対策の項目を位置付けている。
- 立入検査の際に確認する項目については、医療情報システムの安全管理に関するガイドラインから特に取り組むべき重要な項目を抽出し、「医療機関におけるサイバーセキュリティ対策チェックリスト」により示している。
- 令和５年度においては、チェックリストの一部項目について、令和６年度に確認するものを参考項目として位置づけていたが、令和６年度において、すべての項目を確認することとした。
- 令和６年度版「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」（令和６年５月13日付け医政参発0513・第6号医政局特定医薬品開発支援・医療情報担当参事官通知）を発出した。

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

令和５年度版

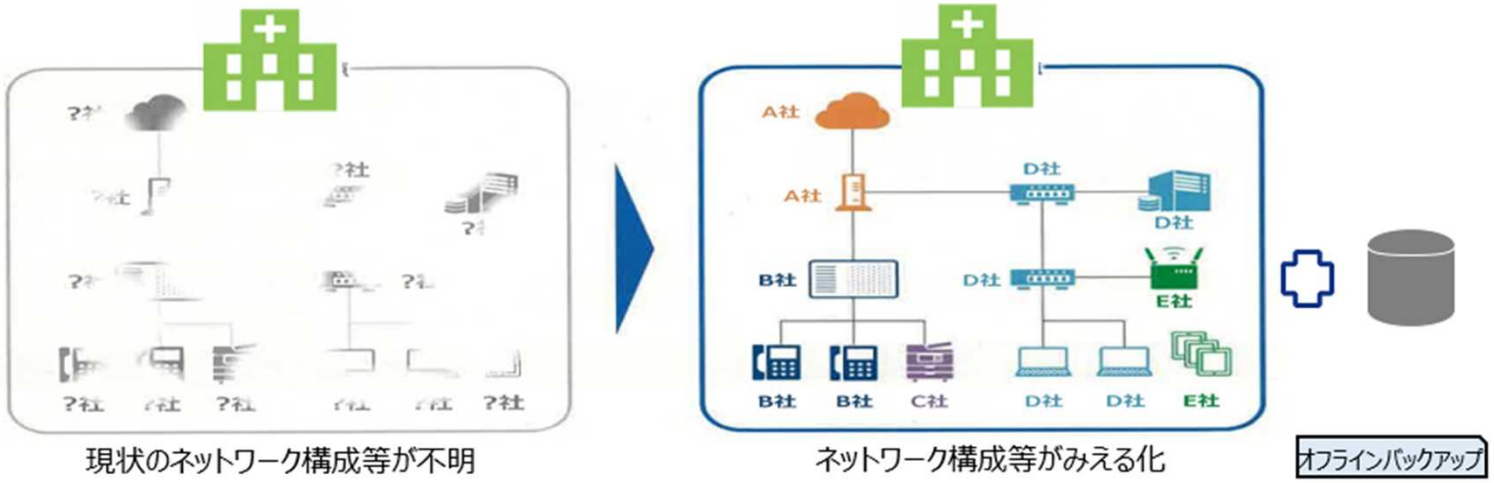
令和６年度版

医療機関におけるサイバーセキュリティ確保事業

令和５年度補正予算　36億円

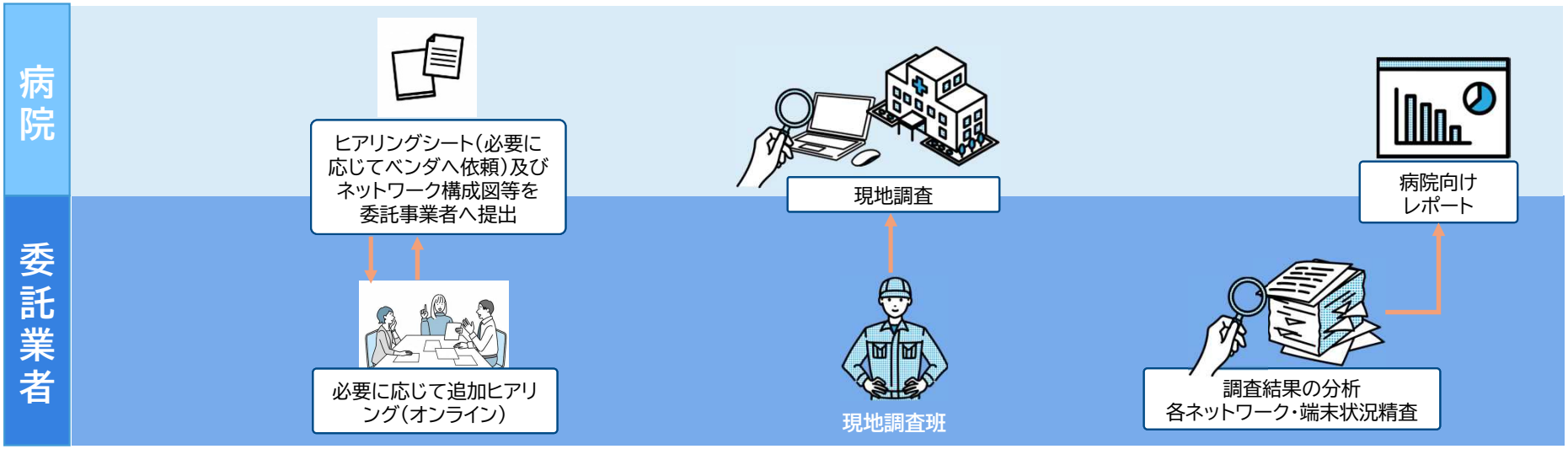
- 医療機関の医療情報システムがランサムウェアに感染すると、診療の一部を長時間休止せざるを得なくなることから、医療機関等におけるサイバーセキュリティ対策の充実は喫緊の課題となっている。
- そのため、医療機関におけるサイバーセキュリティの更なる確保を行う。

- 厚生労働省では、全ての外部ネットワーク接続点を確認することを求めているが、中・大規模病院は多数の部門システムで構成されているため、各システムを提供する事業者と個別に連携しても、全てのネットワーク接続を俯瞰的に把握することは困難である可能性がある。
- また、ランサムウェア対策にはオフライン・バックアップが有効であることを踏まえ、厚生労働省ではオフライン・バックアップ整備を求めている。
- 医療機関におけるサイバーセキュリティの更なる確保のため、外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備を支援する。



外部ネットワーク接続の俯瞰的把握、安全性の検証・調査（進め方）

	①資料収集・ヒアリング	②現地調査・脆弱性診断	③レポート提出
現地調査	病院からネットワーク図、機器・回線一覧、端末情報等、調査に必要な情報をご提供いただく	外部接続拠点とその周辺機器の調査を実施いたします	現地調査報告
脆弱性診断	上記、機器・回線一覧で情報提供いただく	ご提供いただいたIPアドレス等に対して脆弱性診断を実施いたします	脆弱性診断・調査報告

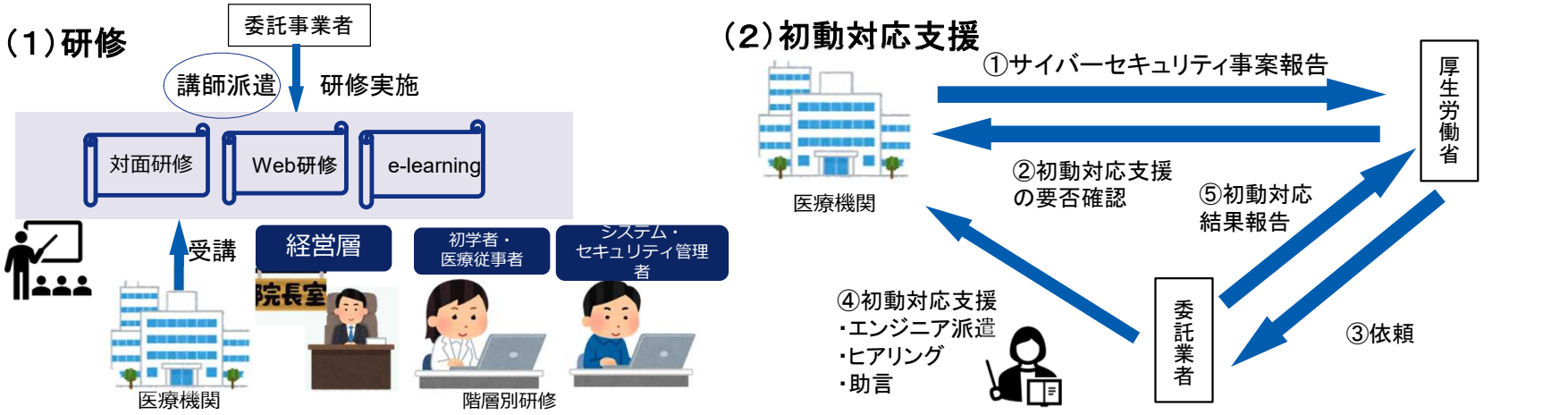


医療分野におけるサイバーセキュリティ対策調査事業

1 事業の目的

○医療機関のセキュリティ対策は、「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきているところである。昨今のサイバー攻撃の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。
○医療機関の医療情報システムがランサムウェアに感染すると、保有するデータ等が暗号化され、電子カルテシステム等が利用できなくなることにより、診療を長時間休止せざるを得なくなることから、医療機関におけるサイバーセキュリティ対策の充実は喫緊の課題となっている。
○医療機関のサイバーセキュリティ対策の徹底を図るべく、**医療従事者や経営層等へのセキュリティ対策研修の実施**、及び医療機関においてサイバーセキュリティインシデントが発生した際の初動対応支援を実施することを目的とする。

2 事業の概要・スキーム



※事業の拡充としては、サイバーセキュリティインシデントに備え、BCPに沿った訓練等の研修の実施とサイバー攻撃の被害が増加している事を踏まえた、初動対応支援可能な医療機関数の増加である。

3 実施主体等

委託先：委託事業（民間事業者）

4 事業実績

◆ 研修受講者数：約9000人（約3500人）
※ 令和５年度実績、　括弧は令和４年度

令和６年度厚生労働省におけるセキュリティ研修の強化と提供について
支援ポータルサイトのご案内

医療機関向け
セキュリティ教育支援ポータルサイト
Medical Information Security Training (MIST)

厚生労働省
厚生労働省委託事業

事業について | 研修内容 | コンテンツ集 | コラム | 講師・技術者リスト | 関連リンク | お問い合わせ | インシデントかも？

令和６年９月より開始
ポータルサイトURL：https://mhlw-training.saj.or.jp/

※医療機関向けのサイトの為、令和6年度は製販企業等は利用できません。

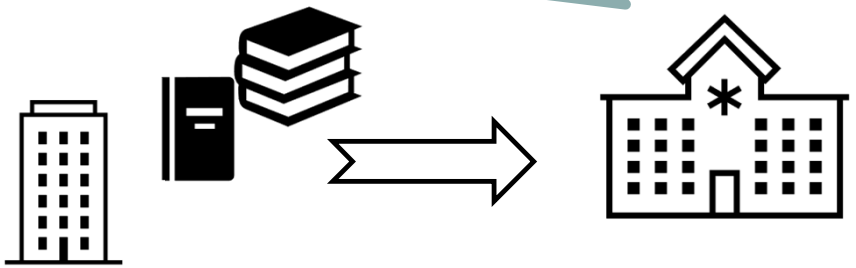
研修種別	コース名	受講対象	実施方法	研修概要
立入検査研修	準備コース	医療機関等保健所関係者	オンライン	医療法に基づく立入検査において、サイバーセキュリティの対応・対策に向けた「医療機関におけるサイバーセキュリティ対策チェックリスト」に基づいた研修 令和6年度に追加された項目等について重点的に解説
	医療機関向けコース	医療機関等保健所関係者		
	保健所向けコース	保健所関係者		
経営者向け研修	ITガバナンスコース	医療機関等の経営に携わる方	オンライン	令和5年度に実施した研修を基にガバナンスの基礎やIT-BCPの基本的な考えや対応方法等について学習
	経営者視点コース			経営者としてサイバーセキュリティを考える重要性を「経営指標」「経営資源の最適配置」など俯瞰した内容でサイバーセキュリティを学習
	IT-BCPコース			過去のインシデント事例を基にIT-BCPの実装、災害BCPの違いなど、ランサムウェア事案を踏まえて学習
システム・セキュリティ管理者向け研修	復習コース ・Windowsセキュリティ編 ・Networkセキュリティ編	医療機関等のシステム・セキュリティ管理する方	オンライン	Windows標準機能を用いた、セキュリティ対策やネットワークセキュリティについて学習
	新規Aコース ・インシデント対応　平時編			インシデント対応「平時」および「初動・封じ込め」について学習
	新規Bコース ・インシデント対応 初動・封じ込め編			
	連携Aコース*	医療機関等のシステム・セキュリティ管理する方 *連携コースは、A・B・Cの3コースで構成していますが、それぞれのコースを単体でご受講可能です。		RFPおよびネットワーク構成図作成に必要な前提スキルとなる、ネットワークの基礎、セキュリティの基礎について学習
	連携Bコース*		ワークショップ	ネットワーク更改に向けて、RFP(提案依頼書)、RFI(情報提供依頼書)に必要な要素について学習
	連携Bコース*		机上演習	インシデントハンドリングに使用できるネットワーク構成図の作成・管理について学習
初学者等向け研修	Aコース ・セキュリティの重要性	医療機関等の中で、サイバーセキュリティの基礎知識を習得したい方	オンライン	一般的なサイバー攻撃の概要および家庭でも役立つ対策について学習
	Bコース ・リスクの理解と対策			医療機関で発生したインシデント事例を中心に、脅威と対策について学習
講師育成研修		自院でIT-BCPの策定等に携わる方	対面	IT-BCPの必要性を正しく認識し、自院でIT-BCPの策定や訓練を実施できるようになるための、座学やワークショップを提供

医療機関とPSIRTの連携（一例）

〇医療法施行規則に基づく立入検査対応のため、下記の資料が欲しい
- ・サイバーセキュリティ対策チェックリスト
- ・MDS/SDS
- ・ネットワーク構成図　等々

〇新たな医療機器の導入にあたり、サイバーセキュリティに関する情報を開示して欲しい
- ・製品仕様情報
- ・保守計画　　等々

〇リスクが高いと思われる既知の脆弱性CVE 2024-xxxx（CVSS値が高いものなど）について、稼働中の医療機器への影響等の情報を開示して欲しい
- ・アドバイザリー情報
- ・セキュリティパッチの適用予定　等々

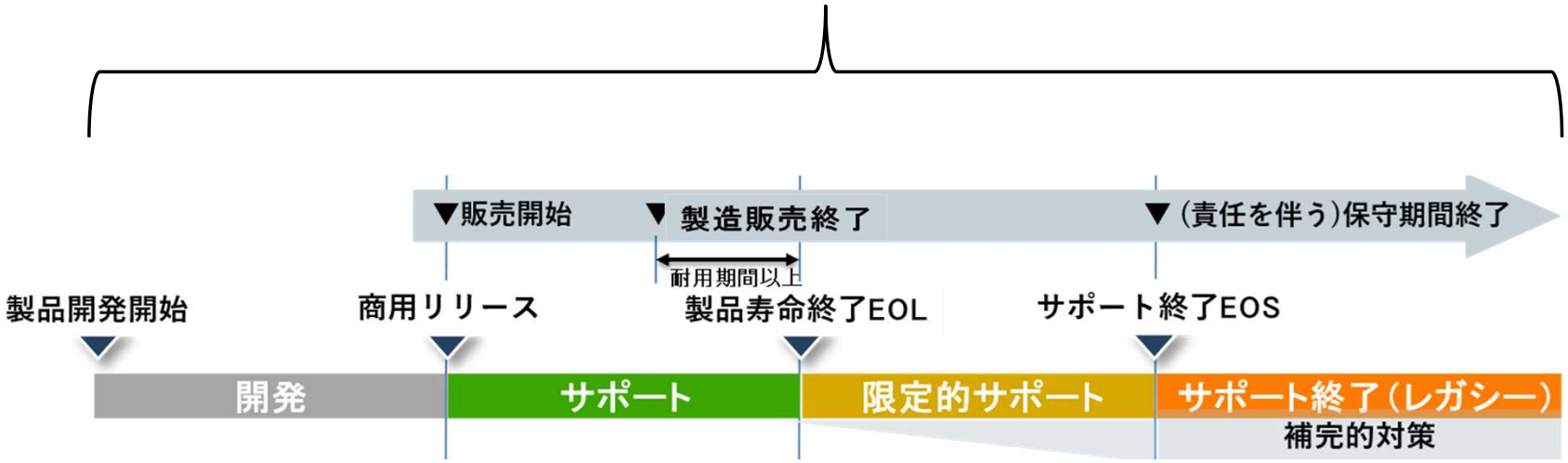


- 医療分野におけるサイバー事案の現状
- 医療機関向けに出ているサイバーセキュリティに係る通知等
- PSIRTの実践

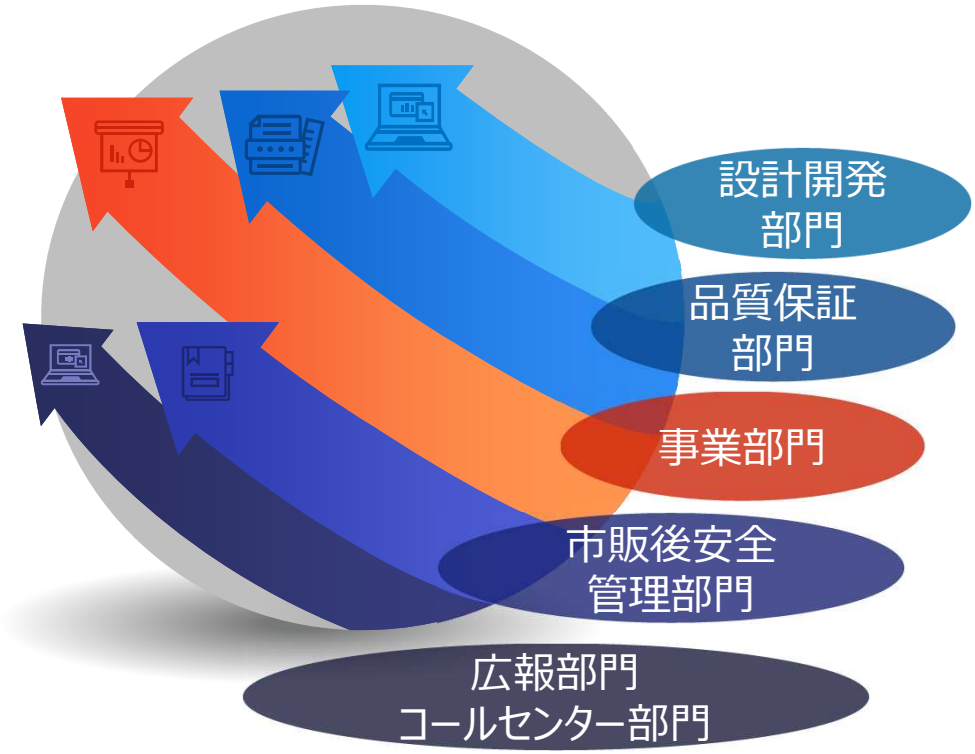
PSIRT「組織」が必要か

製品開発段階～市販後まで、製品ライフサイクルにわたって
「PSIRT機能」を発揮できる「体制」を設けること

※PSIRT：Product Security Incident and Response Team



「PSIRT機能」と体制について



等

- 医療機関等からの問い合わせ・依頼、脆弱性対応、EOL/EOS※1設定・通知等のPSIRT機能を果たすため、製品開発部門・品質保証部門・市販後安全管理部門等の既存組織との連携など、自社に適した体制を構築し運用する。

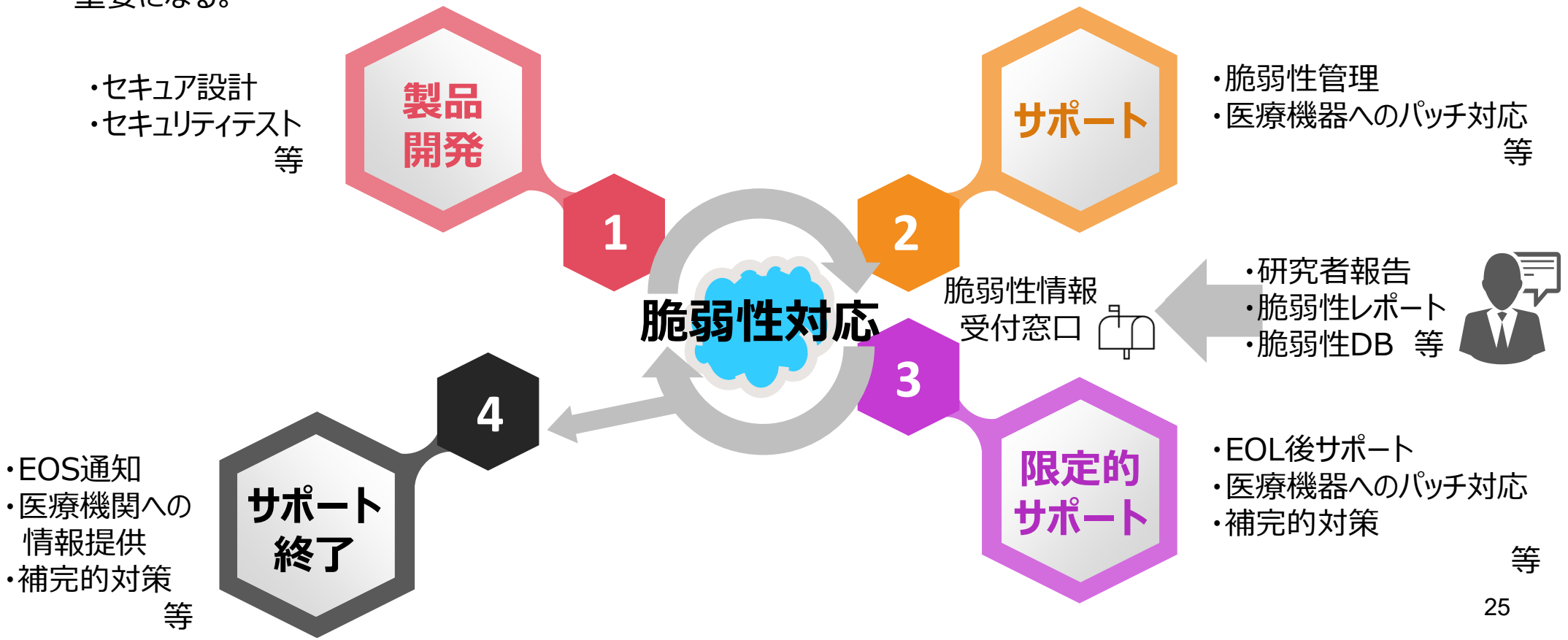
  参考として「PSIRT Services Framework※2」において、いくつかのモデルが示されている。

※1：EOL：End of Life、EOS：End of Service

※2 http://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1_ja.pdf

製品ライフサイクルにわたるPSIRTの取組みについて

- **サプライチェーン管理**の観点から、外部事業者を活用したソフトウェア、OSS（Open Source Software）含むOTS（Off-the-Shelf）ソフトウェア等を活用した製品の場合は、脆弱性対応に関する契約の確認・見直し等が重要になる。



ソフトウェア部品表（SBOM）を用いた脆弱性管理について１/2

構成管理

・SBOM作成
（**サプライチェーンの把握も重要**※）
・統合、承認
・統合管理
・規格遵守確認

情報収集

・**情報収集（窓口設置、周知も行う）**
・SBOMと突合
・継続監視

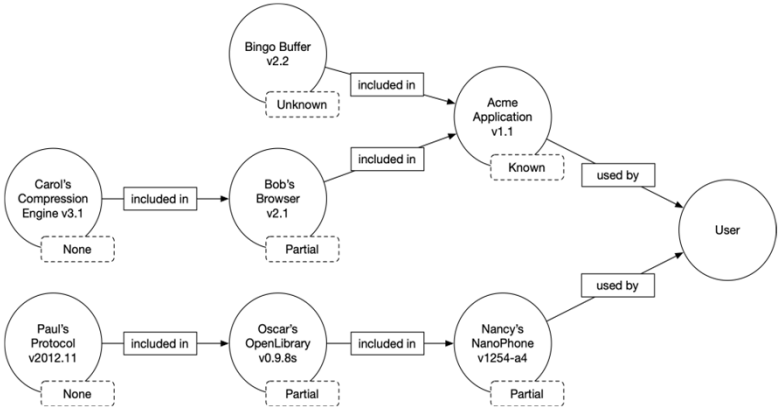
判断

・影響度判定
・トリアージ

対応

・**情報開示**
・**脆弱性対策プログラム公開**
・対応状況記録管理

Component Name	Supplier Name	Version String	Author	Hash	UID	Relationship	Relationship Completeness
NanoPhone	Nancy	v1254-a4	Nancy	0x523	237	Primary	Partial
|--- OpenLibrary	Oscar	0.9.8s	Nancy	0xA23	394	Included in	Partial
|--- Protocol	Paul	2012.11	Nancy	0xB53	934	Included in	None



※出典：Framing Software Component Transparency (2024)
https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024

ソフトウェア部品表（SBOM）を用いた脆弱性管理について２/2

JPCERTコーディネーションセンター 及び 情報セキュリティ早期警戒パートナーシップについて

一般社団法人JPCERTコーディネーションセンター

（**J**a**p**an **C**omputer **E**mergency **R**esponse **T**eam / **C**oordination **C**enter）

- コンピューターセキュリティインシデントへの対応、国内外にセンサーをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器等の脆弱性への対応など**国内の「セキュリティ向上を推進する活動」**を行う
- インシデント対応をはじめとする国際連携が必要なオペレーションや情報連携に関する**日本の窓口となる「CSIRT」**
- 主に2つの調整を実施： コンピューターセキュリティインシデント、脆弱性情報の調整

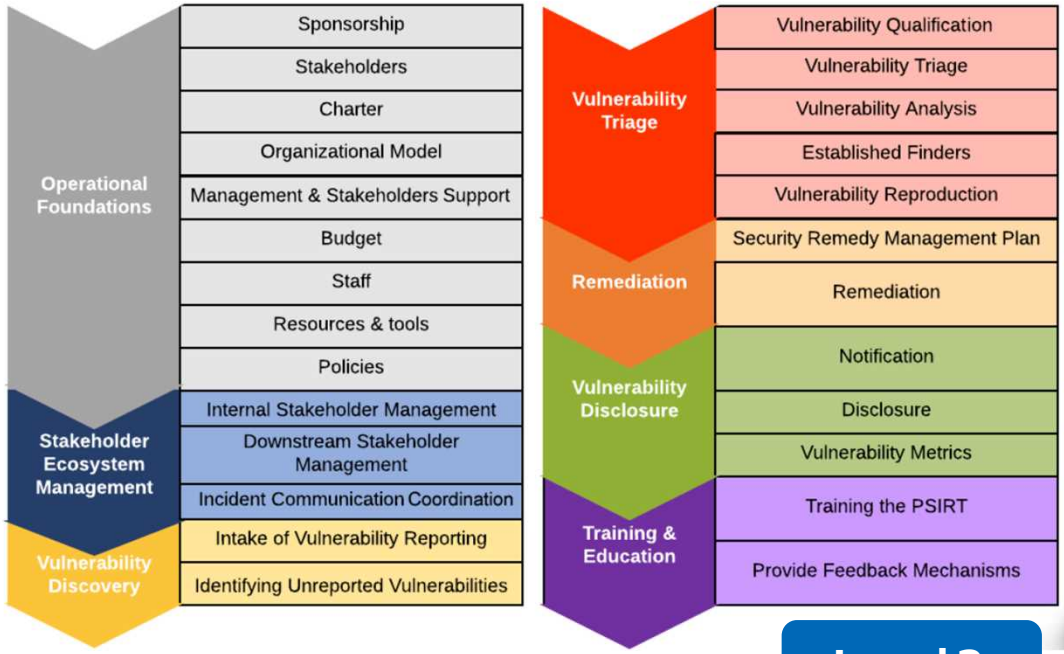
情報セキュリティ早期警戒パートナーシップについて

- 「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（経済産業省告示）に基いて定められた、脆弱性関連情報の円滑な流通、および対策の普及を図るための官民の連携体制として整備された公的ルール
- IPA（独立行政法人情報処理推進機構、受付機関）および JPCERT/CC（調整機関）により共同運営している 情報セキュリティ早期警戒パートナーシップガイドライン
- 最終的に脆弱性情報ポータルサイトJVN（Japan Vulnerability Notes）にて脆弱性情報およびその対策情報を公表し、製品利用者への周知を行う

（参考）PSIRT機能の強化

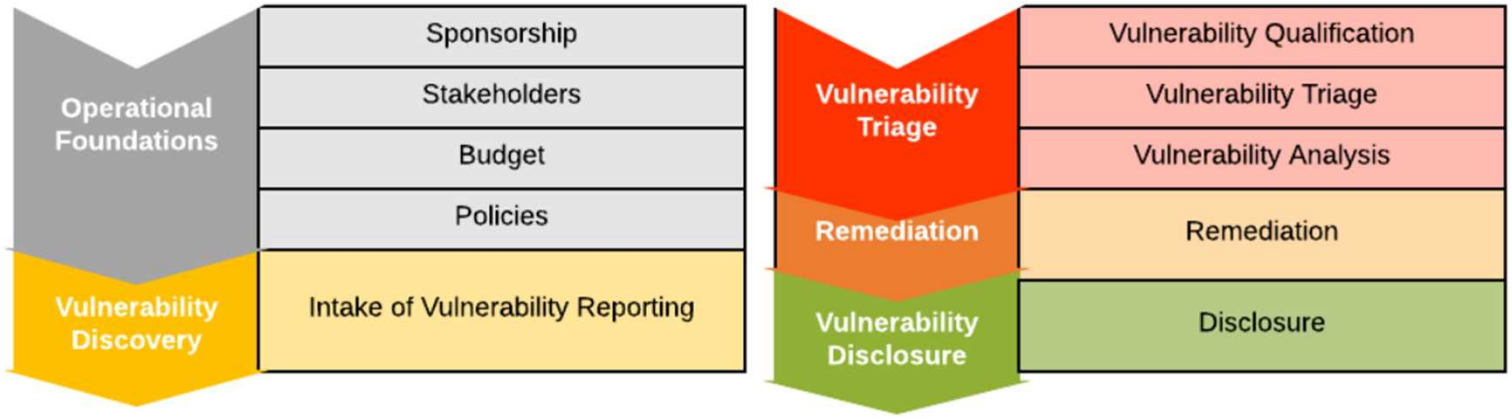
- PSIRT機能の発展モデルとしてFIRST「Product Security Incident Response Team (PSIRT) Maturity Document」には、Level 1 （下図）、Level 2 （右図）、Level 3 が示されている。
- 和訳版が公開されている。

  （日本シーサート協議会と Software ISAC によって翻訳、JPCERT/CC とPanasonic PSIRT とTOSHIBA-SIRT によりレビュー）



Level 2

Level 1



出典:
FIRST「Product Security Incident Response Team （PSIRT) Maturity Document」
https://www.first.org/standards/frameworks/psirts/psirt_maturity_document

医療機器におけるサイバーセキュリティ対応の関連通知は下記サイトにて掲載

厚生労働省

https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html

PMDA

https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について

（医薬安発0115第２号）

医薬安発0115 第２号
令和６年１月15 日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医薬安全対策課長

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方について

医療機器のサイバーセキュリティの確保については、「医療機器におけるサイバーセキュリティの確保について」（平成27 年４月28 日付け薬食機参発0428第１号・薬食安発0428 第１号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求めています。また、医療機器のサイバーセキュリティに関する具体的なリスクマネジメント並びにサイバーセキュリティ対策及び処置の考え方については、「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日付け薬生機審発0724 第１号・薬生安発0724第１号・厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）として取りまとめられており、**製造販売業者は、サイバーリスクに伴う医療機器の不具合等を「医薬品、医薬部外品、化粧品、医療機器及び再生医療等製品の製造販売後安全管理の基準に関する省令」（平成16 年厚生労働省令第135 号）における安全管理情報として取り扱い、適切な製造販売後安全管理を行う必要がある**ことを示しています。

製造販売業者等が行う不具合等の報告については、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（昭和35 年法律第145 号）第68 条の10 第1 項により規定され、その取扱いは「「医薬品等の副作用等の報告について」の一部改正について」（令和３年７月30 日付け薬生発0730 第８号厚生労働省医薬・生活衛生局長通知）により示しているところです。

今般、医療機器に対するサイバーセキュリティの確保を一層強化するため、製造販売業者等が行う不具合等の報告について、「新たな形態の医療機器等をより安全かつ有効に使用するための市販後安全対策のあり方に関する研究」（厚生労働行政推進調査事業費補助金（医薬品・医療機器等レギュラトリーサイエンス政策研究事業）、研究代表者 国立医薬品食品衛生研究所医療機器部 サイバーセキュリティワーキンググループにおいて、**別添のとおり「医療機器サイバーセキュリティに関する不具合等報告の基本的考え方」が取りまとめられましたので、御了知の上、医療機器のサイバーセキュリティの更なる確保に向けた医療機器の製造販売後安全管理が円滑に行えるよう**、貴管下関係製造販売業者等への周知及び指導等よろしくお願いいたします。

通知本文：
https://www.mhlw.go.jp/content/11120000/001195155.pdf

医療機器サイバーセキュリティに関する不具合等報告の基本的考え方　　別添

1. はじめに
2. 本文書の対象
3. 用語の解説
4. **製造販売業者における医療機器の不具合等報告**

通知本文：
https://www.mhlw.go.jp/content/11120000/001195155.pdf

(1) 医療機器の不具合等報告の基本的事項
不具合等報告書は、報告期限内に、PMDA医療機器品質管理・安全対策部 医療機器安全対策課に提出する。

(2) サイバーセキュリティに関する不具合等報告
レガシー医療機器において発生した事象についても、同様に不具合等報告の必要性を考慮すること。

(3) 脆弱性に関する対応
当該脆弱性の悪用が原因で、死亡や重篤な健康被害が発生した場合、又は発生するおそれがあると判断した場合には、報告の要否や区分を評価、判断し、医薬品医療機器等法第68条の10第1項の規定により規制当局への不具合等の報告を実施する。

(4) レガシー医療機器に関する対応
EOS 後の継続した使用に関しては、決して推奨できる状態ではないとともに、継続して使用する責任は医療機関にあることは、全ての関係者が理解しておかねばならず、そのために製造販売業者は、積極的な情報提供を行い、顧客との連携、医療機関と認識を共有することが重要である。

5. **情報共有体制について**

製造販売業者は、医療機器のCS に関する不具合や健康被害が発生した場合には、当該医療機器の影響等を評価し、不具合等報告の要否について判断し、必要に応じてPMDA に報告する。その際に、製造販売業者は、医療機関、使用者、規制当局及び脆弱性発見者等と必要な情報共有等を行い、連携したアプローチを実施することが求められる。そのために製造販売業者は、脆弱性に関する情報の収集、評価、報告に関する情報共有体制の構築、維持が必要であり、併せて継続的な人材育成が望まれる。

6. **まとめと今後の展望**

今後は、医療機器のCS に関する情報を入手した際に、関係者間で情報共有等を行い、連携して対処するための具体的な手順の確立が望まれる。

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

（医薬機発0328第１号、医薬安発0328第３号）

医薬機審発0328第１号
医薬安発0328第３号
令和６年３月28日

各都道府県衛生主管部（局）長 殿

厚生労働省医薬局医療機器審査管理課長
厚生労働省医薬局医薬安全対策課長

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

医療機器のサイバーセキュリティの確保については、「医療機器におけるサイバーセキュリティの確保について」（平成 27 年４月 28 日付け薬食機参発 0428 第１号 ・ 薬食安発 0428 第１号厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当）・ 医薬食品局安全対策課長連名通知）において、医療機器の安全な使用の確保のため、医療機器に関するサイバーリスクに対する適切なリスクマネジメントの実施を求めています。また、 国際医療機器規制当局フォーラム におけ る 、 サイバーセキュリティ対策 の 国際的な調和 を図ることを目的とし た「Principles and Practices for Medical Device Cybersecurity 」（ 医療機器サイバーセキュリティの原則及び実践 。以下「IMDRFガイダンス」という。）の発行等の国際的な枠組みでの活動を踏まえて 、医療機器 へのサイバー攻撃に対する国際的な耐性基準等の技術要件を我が国へ導入して整備することを目的に、医療機器 のサイバーセキュリティに係る必要な開発目標及び技術的要件等を検討し、主に医療機器製造販売業者向けの「医療機器のサイバーセキュリティ導入に関する手引書」として取りまとめられたことを「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」（令和３年12 月24 日付け薬生機審発1224第１号・薬生安発1224第１号厚生労働省医薬・生活衛生局医療機器審査管理課長 ・ 医薬安全対策課長連名通知）により、情報提供しています。

さらに、 IMDRFにおいて追補ガイダンスが発出されたことから、その内容に基づき、Software Bill of Materials(SBOM)の取扱いやレガシー医療機器の取扱い、**脆弱性の修正、インシデントの対応等を検討し、改訂版の「医療機器のサイバーセキュリティ導入に関する手引書」として、「医療機器のサイバーセキュリティ導入に関する手引書の改訂について」（令和５年３月31日付け薬生機審発0331第11号・薬生安発0331第４号厚生労働省医薬・生活衛生局医療機器審査管理課長・医薬安全対策課長連名通知）**により、お示ししたところです 。

我が国においては、 国境を超えて行われる医療機器に対するサイバー攻撃への対策を一層強化して 医療現場における安全性を確保するため、「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第四十一条第三項の規定により厚生労働大臣が定める医療機器の基準」（平成 17 年厚生労働省告示第122号 の改正を行い、 許認可において医療機器のサイバーセキュリティ 対応 を確認することができる体制の構築を進めています 。

今般、**医療機器のサイバーセキュリティの更なる確 保に向けた医療機器製造販売業者等 の体制確保を円滑に行えるよう 、 脆弱性の管理等に関する留意事項**を下記のとおりまとめたので 、 貴管下関係製造販売業者等に対する周知及び体制確保に向けた指導等よろしくお願いします。

情報セキュリティ早期警戒パートナーシップガイドライン 2019 年版第２刷※
「５． 製品開発者の対応」
※通知発出時は2019年版のところ、令和６年６月に2024年版へ改訂

https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html

通知本文：
https://www.mhlw.go.jp/content/11120000/001237125.pdf

医療機器のサイバーセキュリティを確保するための脆弱性の管理等について

（医薬機発0328第１号、医薬安発0328第３号）

■ 脆弱性の管理

脆弱性は、システムのセキュリティポリシーを破るために悪用される可能性のある、システムの設計、導入又は運用管理における欠陥又は弱みであることから（JIS T 81001-1:2022 3.4.22）、医療機器のサイバーセキュリティを確保するため、**医療機器製造販売業者等は、当該医療機器の脆弱性について、特定、評価、開示、修正等を行う必要**がある。

- **医療機器に製品固有の脆弱性が見つかった場合**
- **医療機器に汎用の脆弱性の存在及び悪用により受容できないリスクが発生する可能性がある場合**

＜IPA＞
以下ウェブサイトを参照の上、脆弱性関連情報を届出すること。
参考：https://www.ipa.go.jp/security/todokede/vuln/uketsuke.html
なお、IPAは脆弱性関連情報の届出の受付機関であり、医療機器製造販売業者等への連絡及び公表に係る調整はJPCERT/CCにて実施される。

通知本文：
https://www.mhlw.go.jp/content/11120000/001237125.pdf

まとめ

- 医療の高度化、技術の進展に伴い、ネットワークに接続するなどサイバーセキュリティ対応を要する医療機器は、今後も増加すると見込まれる。製造販売業者は、該当品目の機能性や安全性を確保するため、基本要件第12条第３項や関連通知等に沿った継続的な対応が必要である。

- 医療機関は、電子カルテシステムなど数多くのシステムを保有するため、厚生労働省通知等に沿ったサイバーセキュリティ対応が求められている。製造販売業者は、医療機関の連携にあたり、それら取組みへの理解と適切な連携、情報発信、情報提供などが必要となる。

- PSIRT機能の運用にあたっては、継続的な医療機関との連携、脆弱性管理等の活動と並行して、規制動向等に合わせた機能強化等も重要である。

令和6年度医療機器製造販売業者のサイバーセキュリティ対策周知事業

■ 医療機器サイバーセキュリティにおける、医療機関との連携に向けた取組と諸課題

1. 医療機器のサイバーセキュリティに関する国内規制の動向

2. 医療機器サイバーセキュリティの実践

- 医療機器のサイバーセキュリティについて
- サイバーセキュリティに係る規格について
  （IEC 81001-5-1:2021）
- 医療機器のサイバーセキュリティ要件に対する
  JIS T 81001-5-1の適用について
  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000179749_00009.html
  https://www.pmda.go.jp/review-services/drug-reviews/about-reviews/devices/0051.html

3. 医療機関との連携及びPSIRTの実践

4.「製造業者/サービス事業者による医療情報セキュリティ開示書」の概要

5. ソフトウェア部品表（SBOM）の作成と運用

医療機器
製造販売業者等

連携

医療機関、
医療情報システム製造業者等

医療機関との連携及びPSIRTの実践

ご清聴ありがとうございました。