2019 年度 AMED（医薬品等規制調和・評価 研究事業）
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

# 製造販売業者が行っている
# 医療機器のサイバーセキュリティ対策に関する実態調査
# 調査結果概要

2020 年 3 月

研究代表者
公益財団法人医療機器センター　専務理事　中野壮陛

製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査
調査結果概要

目　次

**調査結果概要** ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1

**調査結果【全回答編】** ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3

**調査結果【対象品目あり編】** ・・・・・・・・・・・・・・・・・・・・・・・・・・・ 43

**調査協力依頼文書** ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 81

**実施状況とりまとめ用紙** ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 85

※本文中のページには下線が付いています

製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査

# 【調査結果概要】

## 調査のスケジュール・概要等

- 送付先：全国の製造販売業者（2722社）
- 発送日：2019年12月17日
- 締切日：2020年1月24日
- 回収数：757件（回収率27.8%）

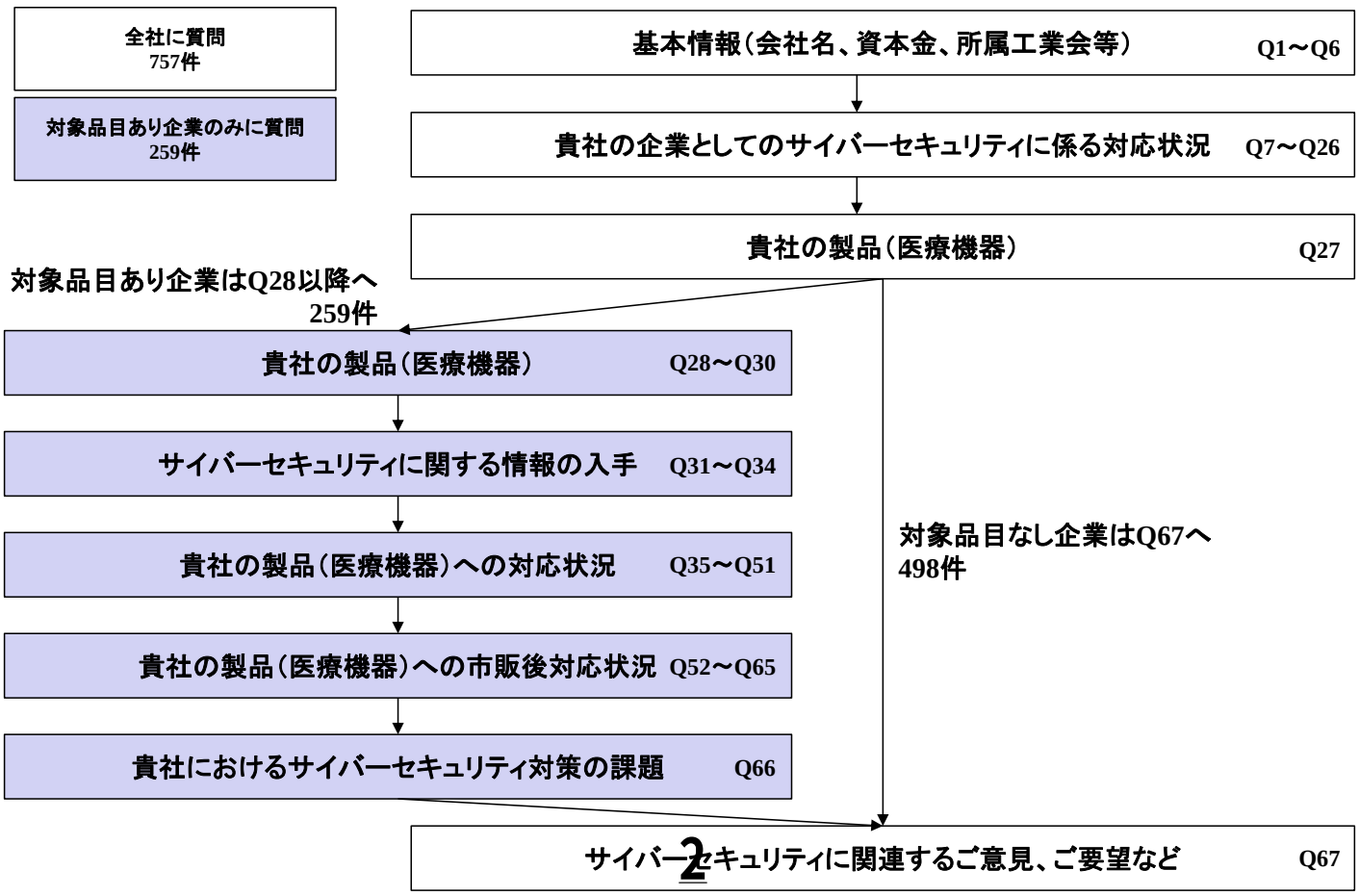
上記のうち、対象品目あり企業数：259件（回収数の34.2%）

## 調査項目の概要

| 全社/特定社 | 項　目 | 質問番号 |
|---|---|---|
| 全社 | 基本情報（会社名、資本金、所属工業会等） | Q1～Q6 |
| 全社 | 貴社の企業としてのサイバーセキュリティに係る対応状況 | Q7～Q26 |
| 全社/特定社 | **貴社の製品（医療機器）** | **Q27**～Q30<br>※Q28から個社 |
| 特定社 | サイバーセキュリティに関する情報の入手 | Q31～Q34 |
| 特定社 | 貴社の製品（医療機器）への対応状況 | Q35～Q51 |
| 特定社 | 貴社の製品（医療機器）への市販後対応状況 | Q52～Q65 |
| 特定社 | 貴社におけるサイバーセキュリティ対策の課題 | Q66 |
| 全社 | サイバーセキュリティに関連するご意見、ご要望など | Q67 |



## 回答フロー



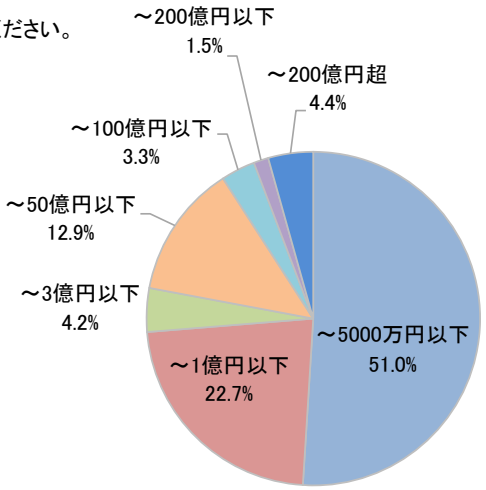
# 調査結果【全回答編】

【全回答】

空白ページ

# 【全回答】

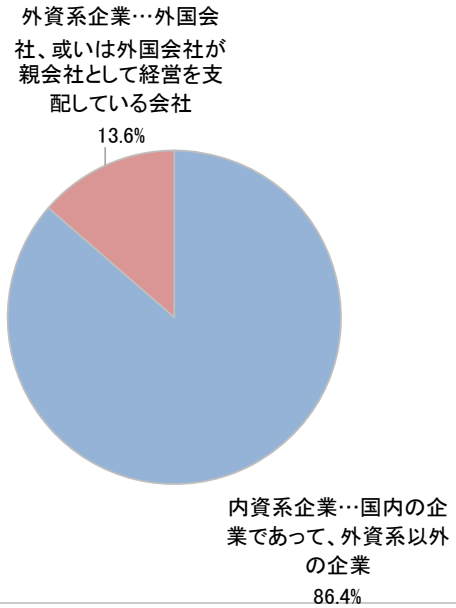
[Q2]資本金についてお答えください。
(n=757)




3

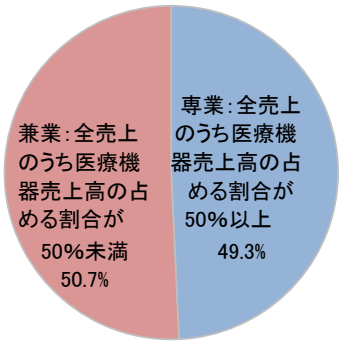
# 【全回答】

[Q3]資本上の区分についてお答えください。
(n=757)



【全回答】

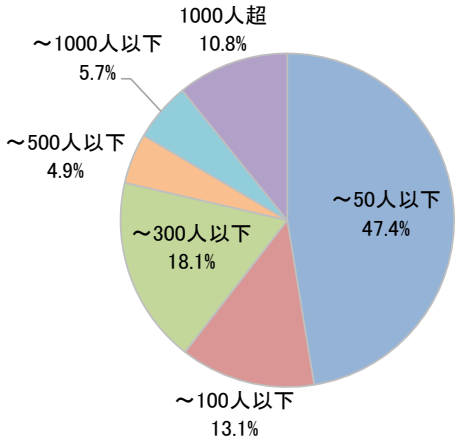
[Q4]専業・兼業の区分についてお答えください。
(n=757)




5

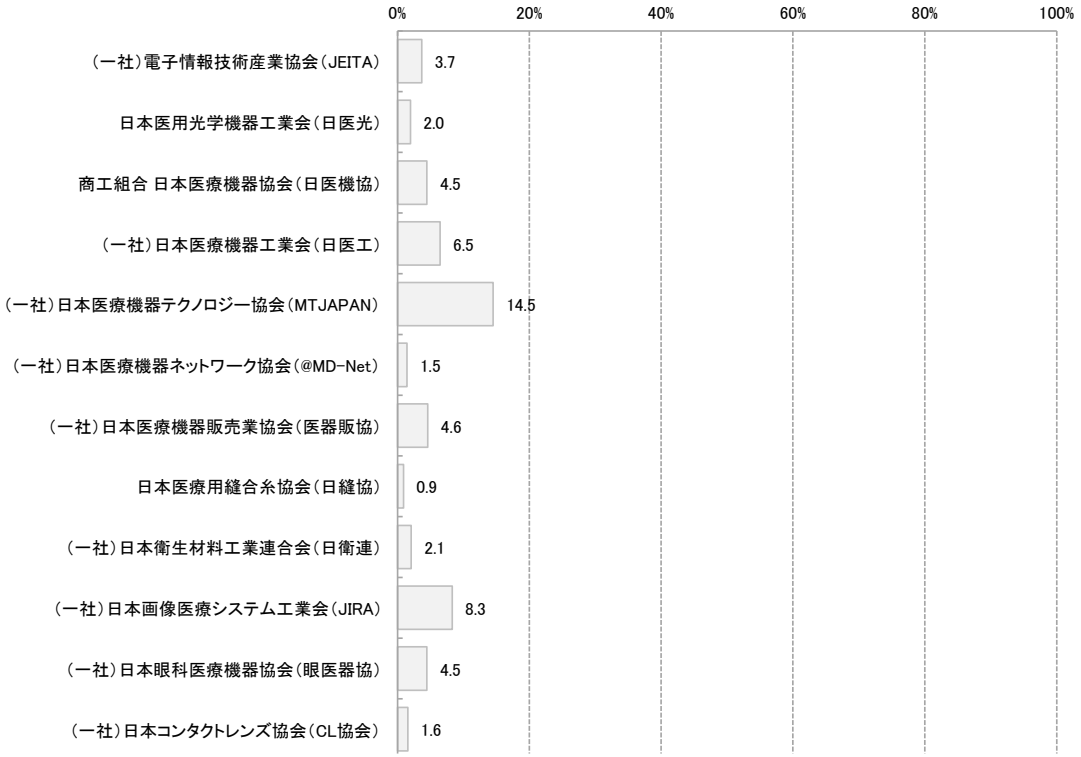
【全回答】

[Q5]全社員数についてお答えください。
(n=757)



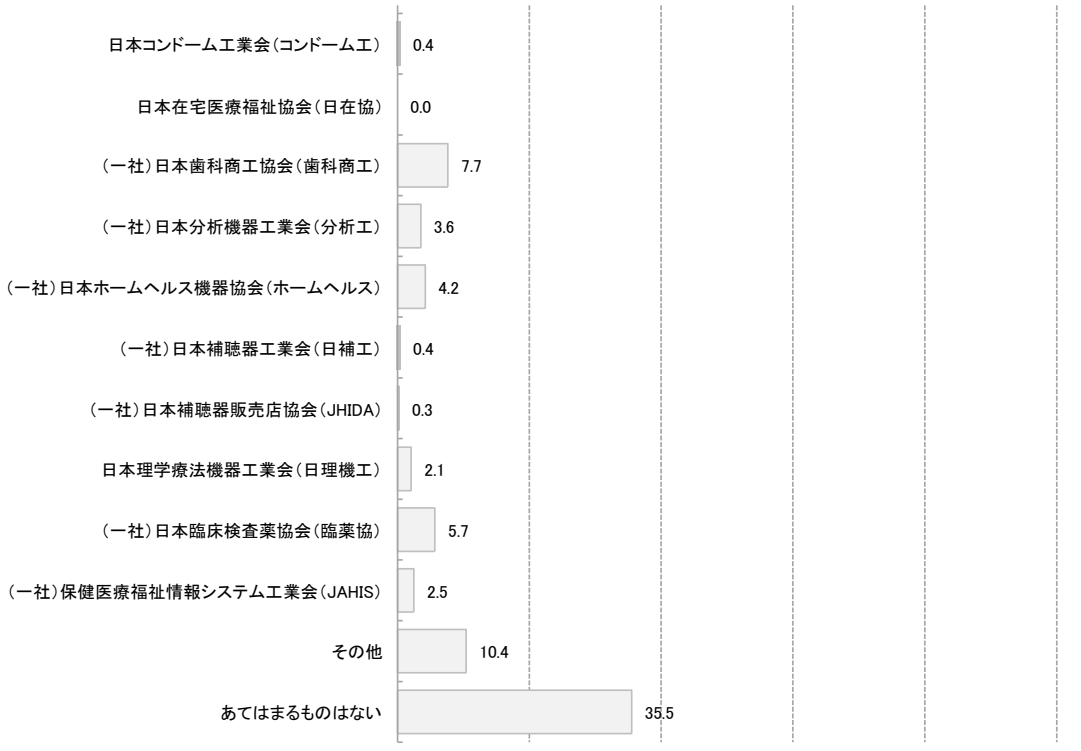
【全回答】

[Q6]主な加盟団体についてお答えください。
(n=757)




7

【全回答】

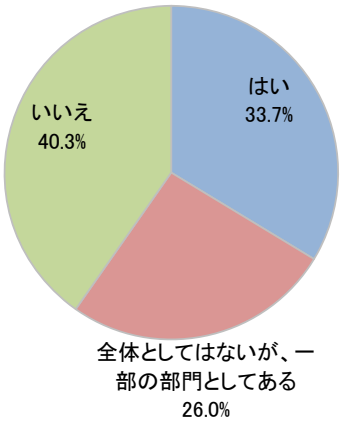





8

【全回答】

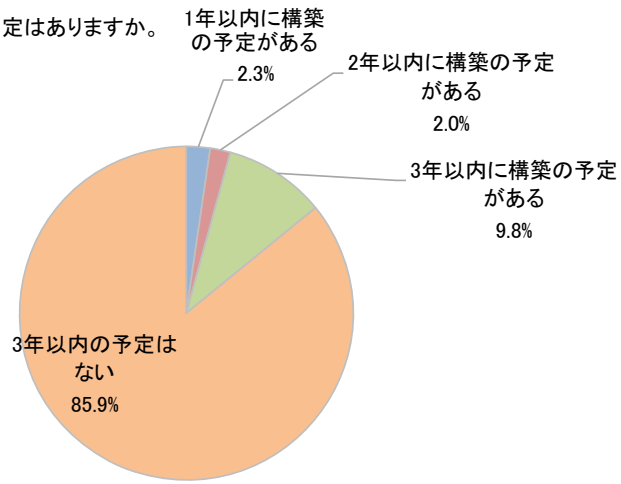
[Q7]会社全体のサイバーセキュリティ対応を行う組織体制がありますか。
(n=757)




9

【全回答】

[Q8]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=305)

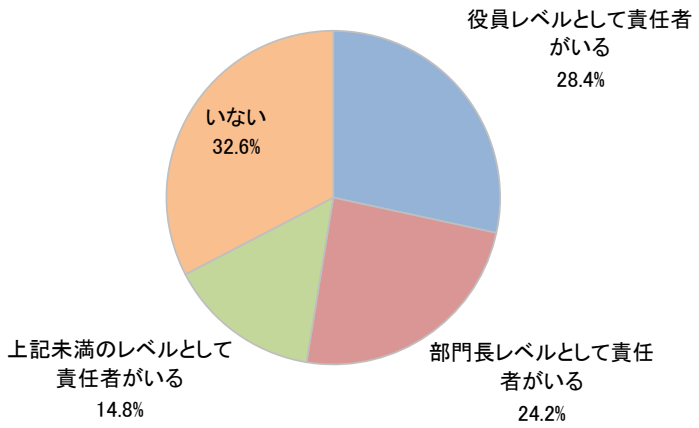





10

【全回答】

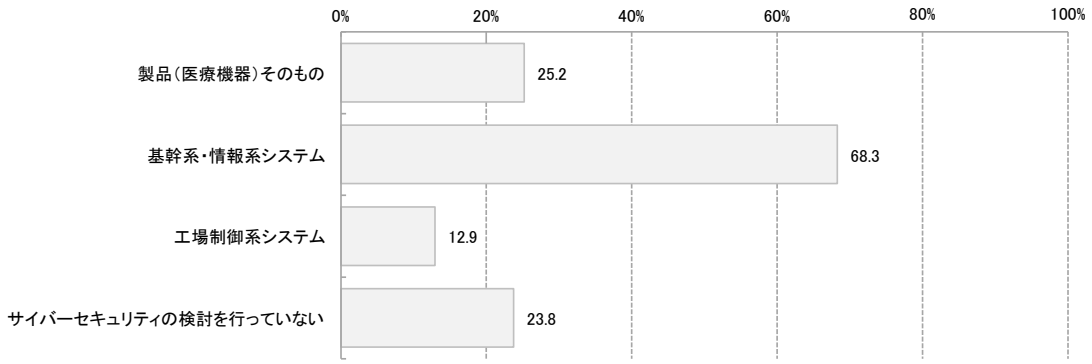
[Q9]サイバーセキュリティに関して統括する立場の責任者はいますか。
(n=757)




11

【全回答】

[Q10]サイバーセキュリティの検討にあたって、次のいずれの範囲を対象としていますか。
(n=757)

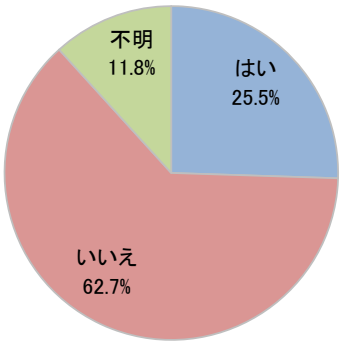





12

【全回答】

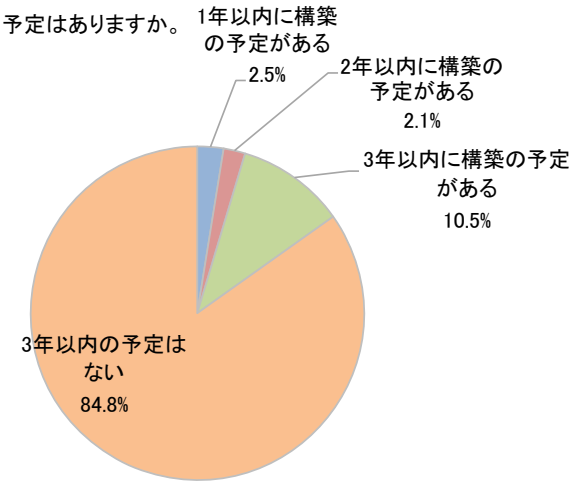
[Q11]コンピュータセキュリティにかかるインシデントに対処するための組織となるCSIRT（Computer Security Incident Response Team）がありますか。
(n=757)




13

【全回答】

[Q12]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=475)

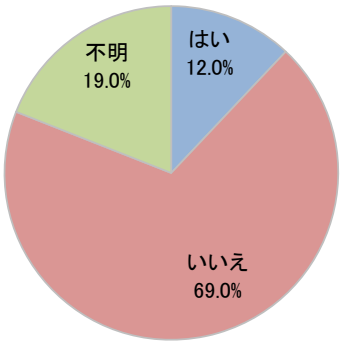





14

【全回答】

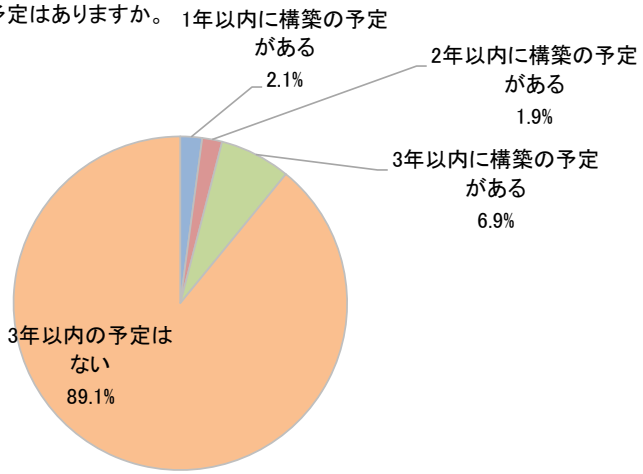
[Q13]組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能としてPSIRT（Product Security Incident Response Team）がありますか。
(n=757)



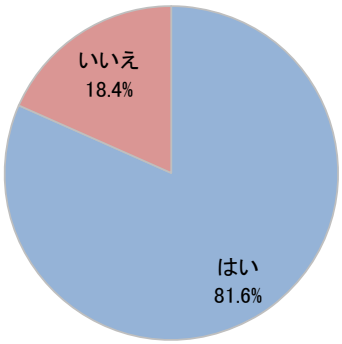

15

【全回答】

[Q14]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=522)



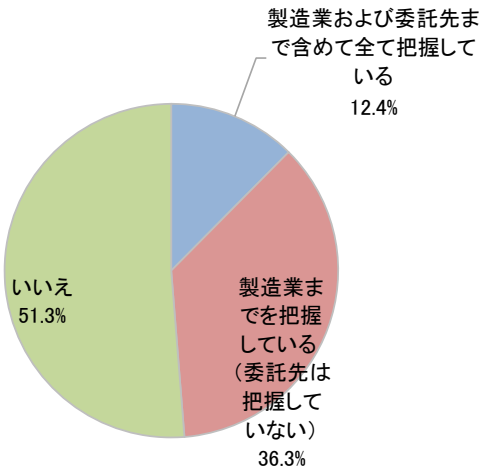
[Q15]QMS対象業務（設計、製造、アウトソーシング先等、関係する全てを含む）で使用しているIT機器について、ウイルス対策やセキュリティ対策に関する対応は行っていますか。
（n=757）





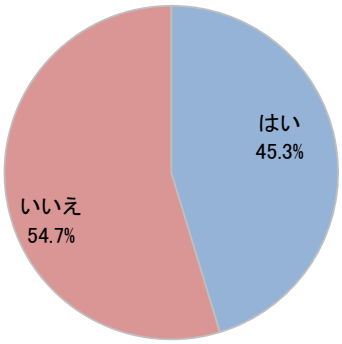



[Q16]製造販売業としてのQMS対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。
（n=757）



【全回答】

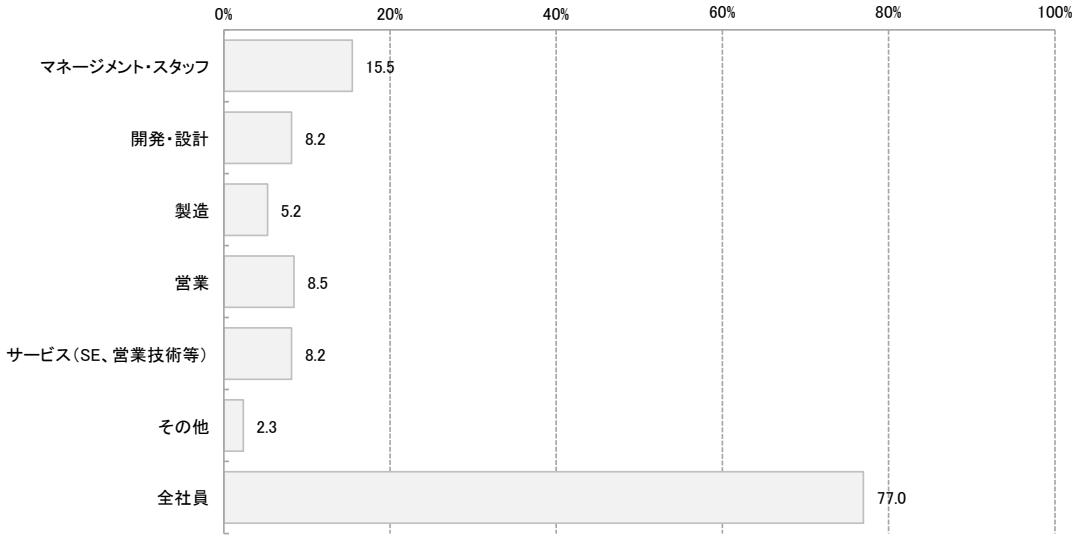
[Q17]サイバーセキュリティに関する社員教育を行っていますか。
(n=757)




19

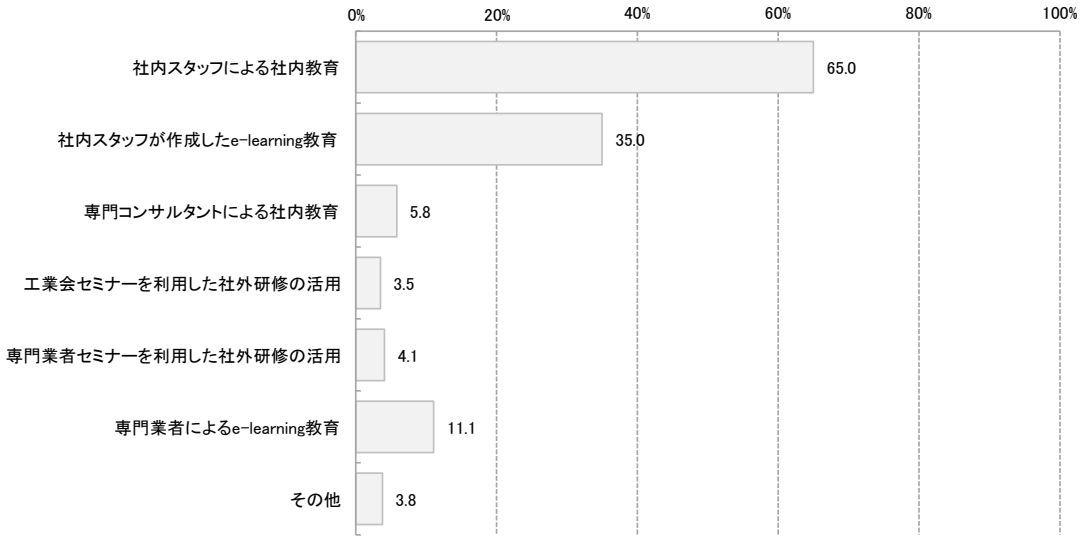
【全回答】

[Q18]「はい」の場合は、誰に対して教育を行っていますか。
(n=343)



# 【全回答】

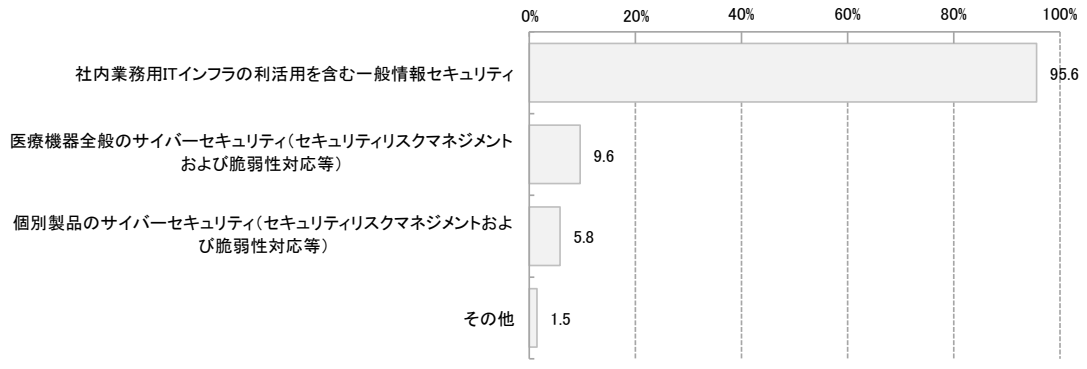
[Q19]「はい」の場合は、どのように行っていますか。
(n=343)




21

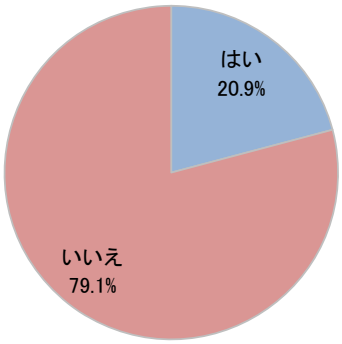
# 【全回答】

[Q20]「はい」の場合は、どのような内容の教育を行っていますか。
(n=343)



【全回答】

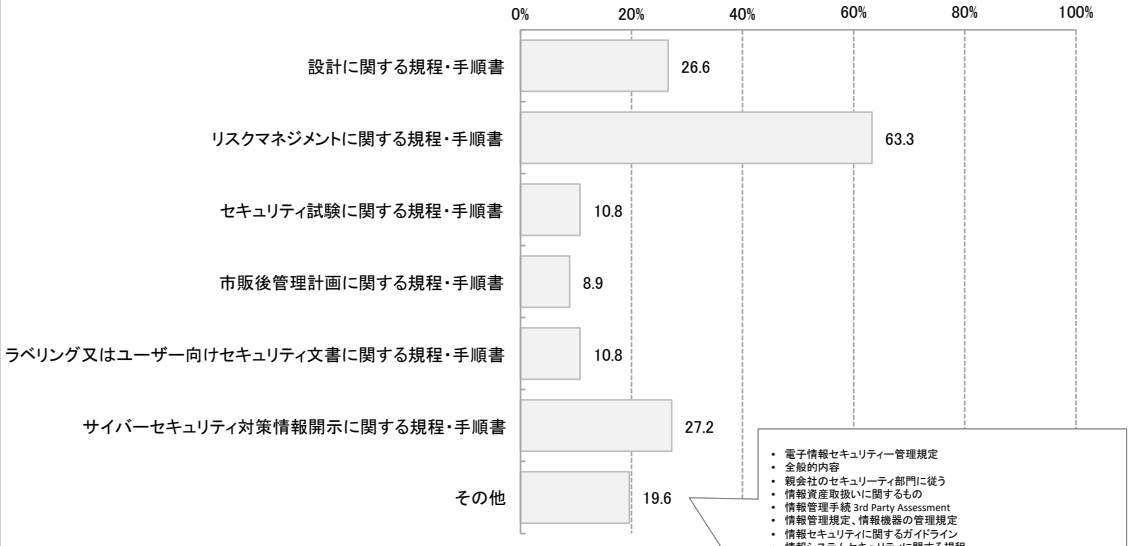
[Q21]サイバーセキュリティに対応するため追加・修正した規程・手順書などがありますか。
(n=757)




23

【全回答】

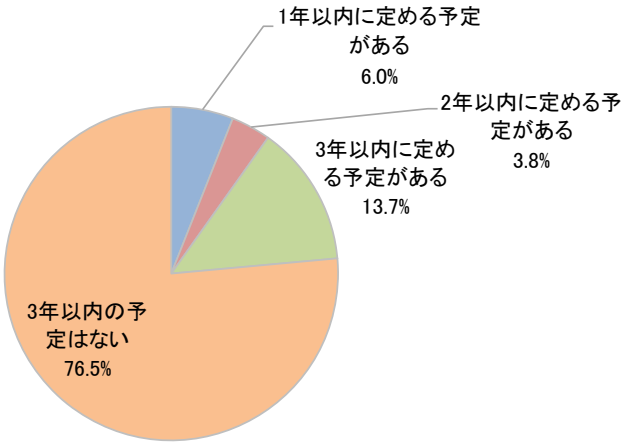
[Q22]「はい」の場合、どのような内容の規定・手順書を追加・修正しましたか。
(n=158)




- 電子情報セキュリティー管理規定
- 全般的内容
- 親会社のセキュリーティ部門に従う
- 情報資産取扱いに関するもの
- 情報管理手続 3rd Party Assessment
- 情報管理規定、情報機器の管理規定
- 情報セキュリティに関するガイドライン
- 情報システムセキュリティに関する規程
- 社内の情報セキュリティ管理の基本規程
- 社内システムに関する規定
- 社内インフラ規定
- 社内IT用作業手順書を新規作成
- 社内IT機器に関する規定
- 個人情報保護法に関する規定
- 管理文書全般に関する規程
- 患者安全に関するサイバーセキュリティの手順書を設定
- 一般向け情報セキュリティ
- マルウェア対策
- セキュリティ対策の規定など
- セキュリティハンドブック
- システム管理規定
- グローバルで共通の規定
- グループ標準情報システム規程・規則類
- クラウドサービスの非常用サーバ運用・メンテナンス手順書
- インシデント入手時の社内報告体制
- Web系システムに対するもの
- Q20の印同様
- Pマーク
- ITポリシー

【全回答】

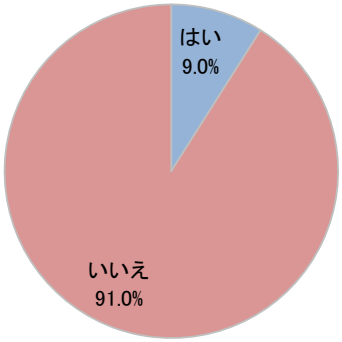
[Q23]「いいえ」の場合、3年以内に追加・修正する予定はありますか。
(n=599)




25

【全回答】

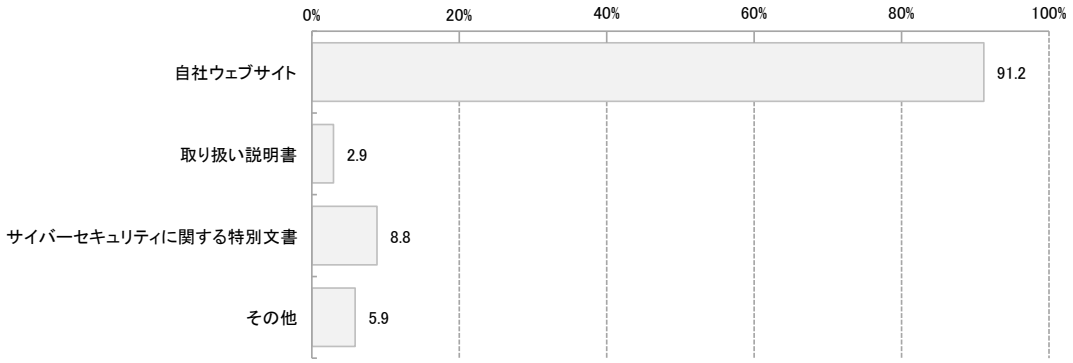
[Q24]サイバーセキュリティに関するポリシーを社外に公開していますか。
(n=757)






26

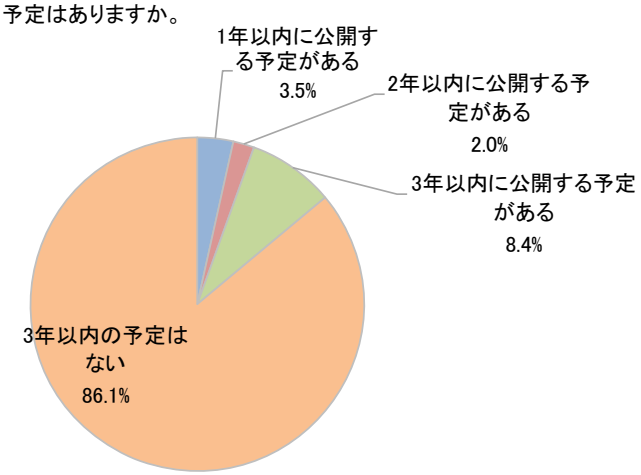
[Q25]「はい」の場合は、どのような方法で公開していますか。
(n=68)



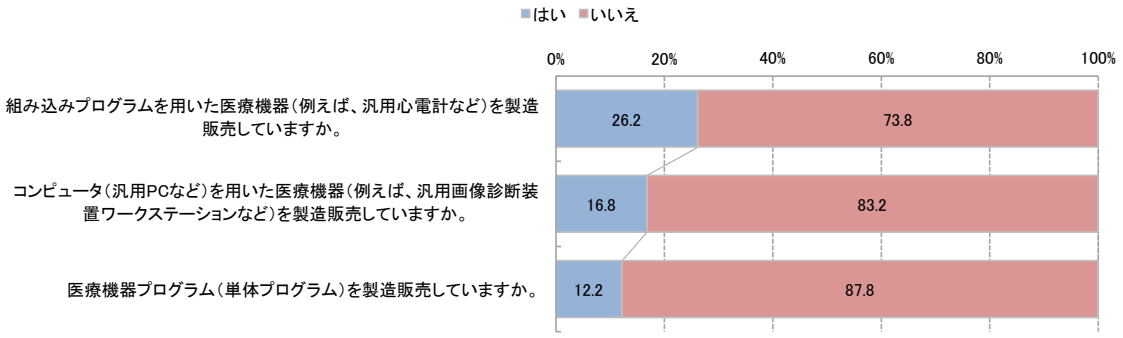





[Q26]「いいえ」の場合、3年以内に公開の予定はありますか。
(n=689)



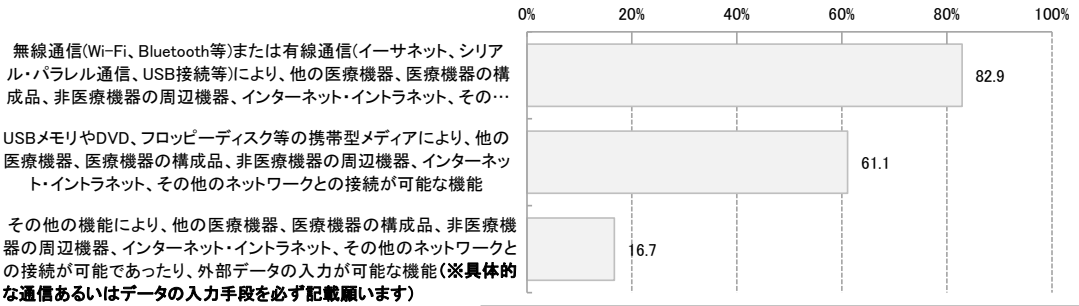
[Q27]製造販売している医療機器についてお伺いします。







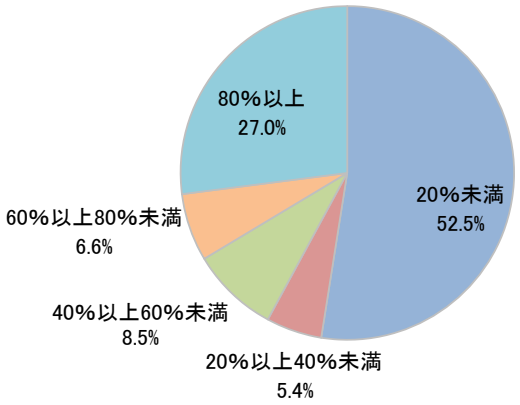

[Q28]それらは、次の機能を有しますか。
(n=234)




- **通信機能は無し**
- **対象外**
- 他の医療機器に画像データを送信
- 他の医療機器、非医療機器の周辺機器との通信
- 測定結果と依頼情報のやり取り
- **組み込みプログラムを有しているが、これらの機能は有していない。（未記入だとえらーが出たため記載しました）**
- 専用機器による接続
- 製造又はサービスの際に、PCを接続することがある。
- 検査（輸血）システムからのオーダー情報
- **機能なし**
- **該当なし（ネットワーク接続等の機能を持たない単なるプログラム内蔵の医療機器のため）**
- **外部データを入力する手段無し**
- リレー接点
- **マイコンの組込プログラムの書換用のコネクタが基板に実装有り。但し、分解しないと接続できない。**
- マイコン
- **プログラムを有するが、接続機能は無い。**
- **ネットワーク接続及び外部データの入力不可**
- **なし**
- トリガー信号、映像信号
- シリアル通信
- **いずれの機能も有しない**
- イーサネットによるネットワーク接続により、外部ホストコンピュータから検査依頼を入力として受付け、医療機器側からは測定結果を出力する
- web上からソフトウェアをダウンロードする
- webブラウザーを介して医療機器実行サイトにLog inし情報を入力する。
- USBメモリーにてデータ入力
- USB バーコードリーダー
- USB
- SDカード
- RS232Cシリアル通信
- RS-232C
- RS232C
- RC232Cポートから他の医療機器及びPCとの接続が可能
- PCより当該機器ソフトの書き換えを行う
- LAN(イーサーネット)
- Hub
- HL-7
- FM
- DICOM規格による通信

17

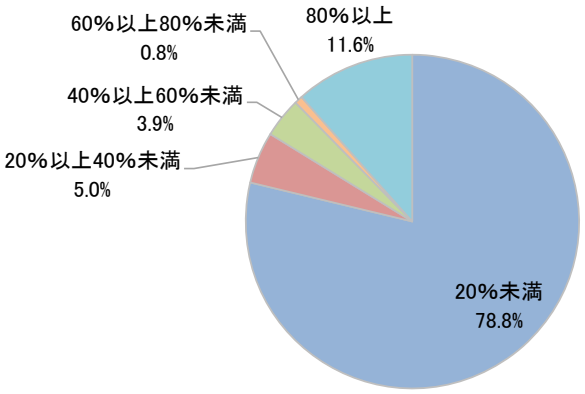
[Q29]貴社の全製品（医療機器）のうち、（現在の対応状況の如何を問わず）サイバーセキュリティ対応を検討しなければならない医療機器の割合はおおよそどの程度ですか。
（n=259）





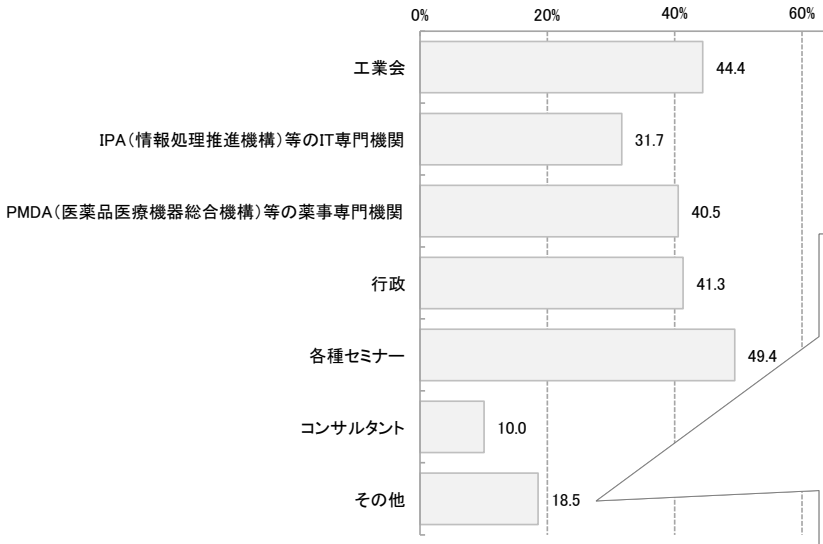



[Q30]前問（Q29）のサイバーセキュリティ対応を検討しなければならない医療機器のうち、既に市販済みの製品であって、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器であり、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できないと考えられる医療機器（Legacy Medical Device）の割合はおおよそどの程度ですか。
（n=259）



【全回答】

[Q31]サイバーセキュリティに関する情報をどこから入手していますか。
(n=259)

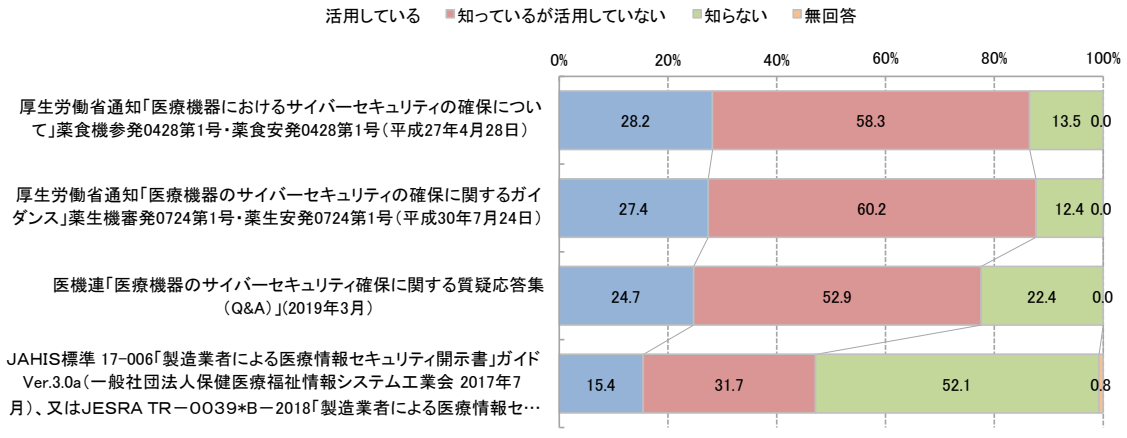



- 米国ISAO
- 米NVD, 米ICS-CERT, 米FDA, 各ソフトウェアベンダの公告
- 認証機関、コンサル会社のメルマガ
- 日本歯科器械工業協同組合
- 日経BPのメール配信サービス
- 担当部署
- 組込みプログラムはクローズタイプ
- 製品製造元
- 製造元
- 製造元
- 製造元
- 親会社セキュリティチーム
- 親会社
- 親会社
- 親会社
- 社内担当部署(海外含む)
- 社内
- 各種メディアや、WEBより
- 外部システム会社
- 外国本社のIT部門
- 海外本社
- 海外本社
- 海外製造元(グループ会社本社)
- 海外製造元
- 海外製造元
- 海外製造元
- 海外親会社より
- 海外親会社
- メール等
- マスコミ
- ベンダー
- セキュリティ関連のWEBサイト
- セキュリティセンタからの通知
- スイス本社
- グループ会社
- インターネット
- web
- Web
- JPCERT,USCERT
- JAHIS
- IT専門ウェブサイト
- FDA、MedISAO
- FDA
- CERTS, NCSC, NISC
- Anti Virus site

33

【全回答】

[Q32]国内の通知、ガイドライン、ガイダンス等を把握・活用していますか。

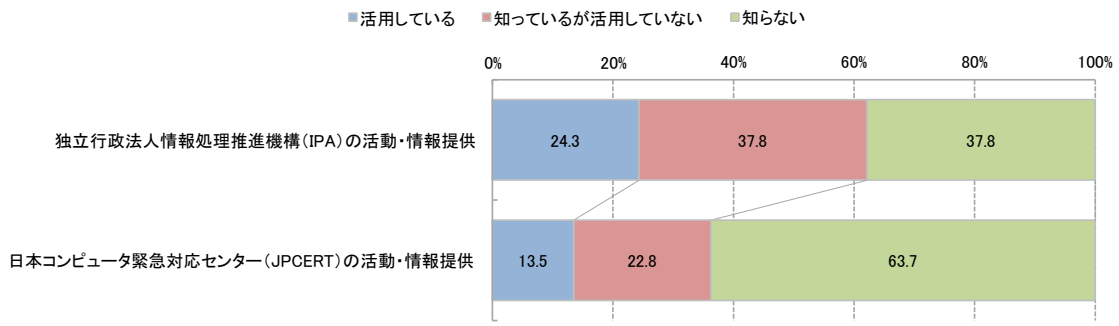





34

【全回答】

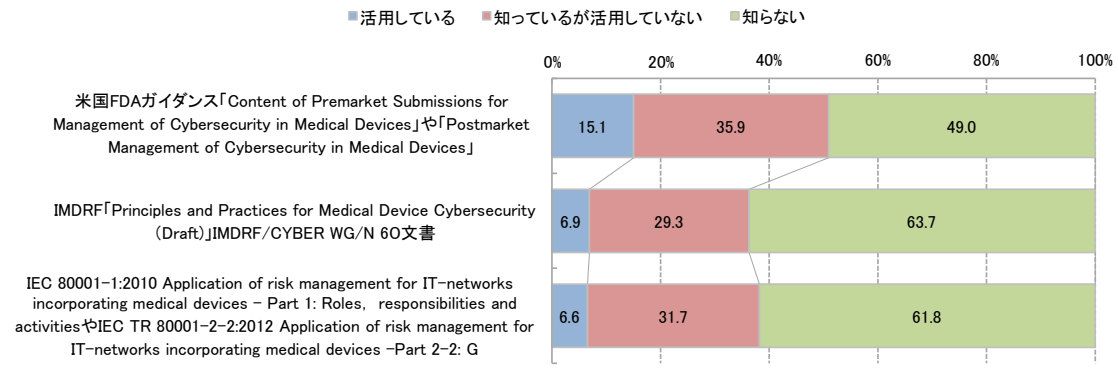
[Q33]サイバーセキュリティ関連組織・活動を把握・活用していますか。



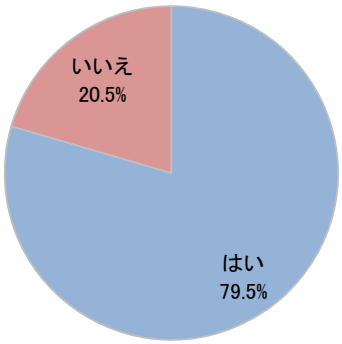

35

【全回答】

[Q34]海外のガイダンスやガイドライン等を把握・活用していますか。



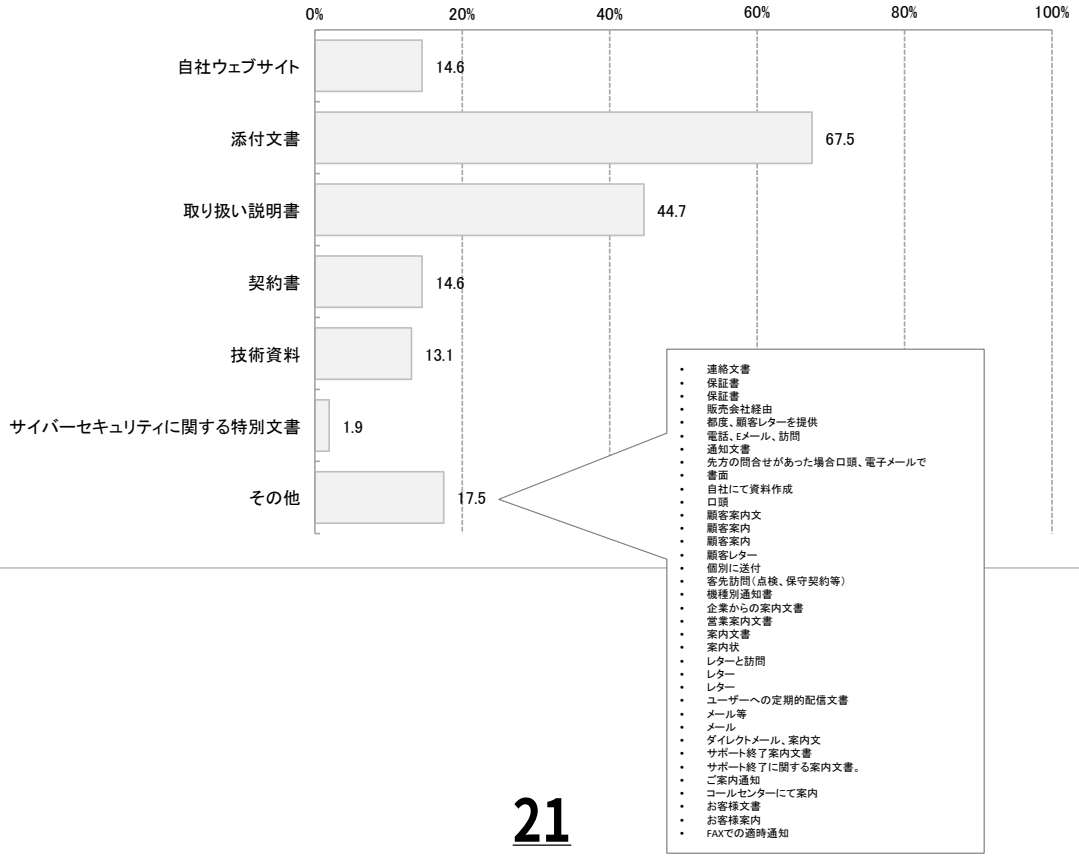
[Q35]貴社の製品（医療機器）の寿命や使用期限、企業からのサポート終了時期について規定し、ユーザーに伝えていますか。
(n=259)





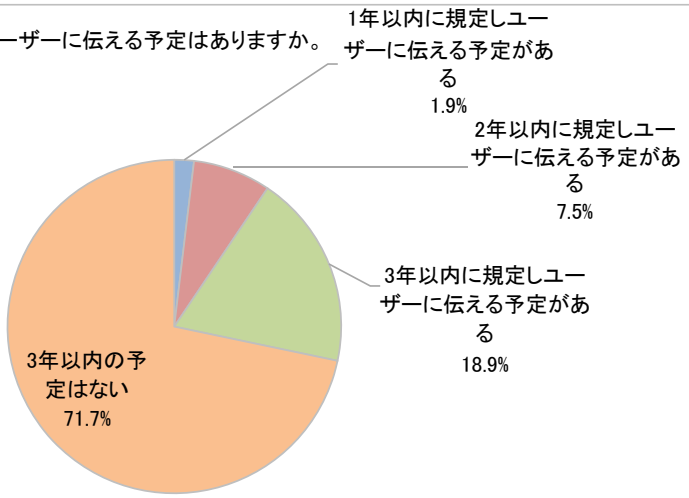



[Q36]「はい」の場合、ユーザーにはどのような媒体で伝えていますか。
(n=206)



# 【全回答】

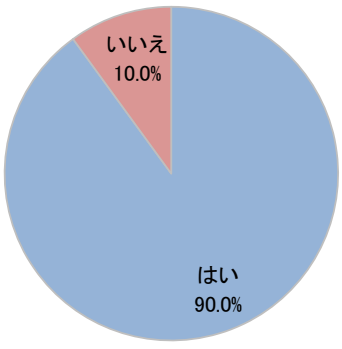
[Q37]「いいえ」の場合、3年以内に規定しユーザーに伝える予定はありますか。
(n=53)




39

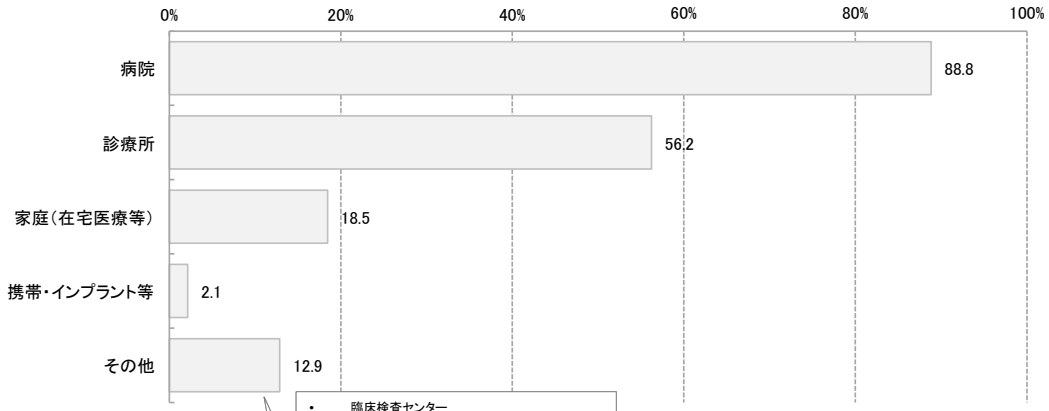
# 【全回答】

[Q38]サイバーリスクが懸念される医療機器について、製品(医療機器)が使用されている主な場所を把握していますか。
(n=259)



# 【全回答】

[Q39]「はい」の場合、具体的にはどのような場所ですか。
(n=233)

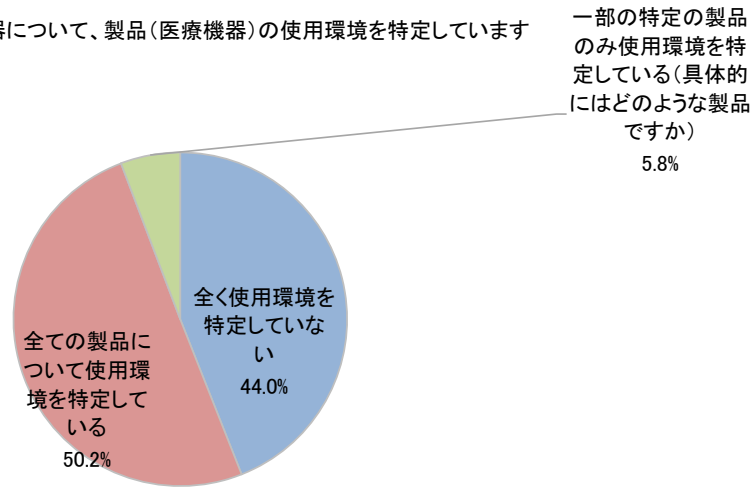



- 臨床検査センター
- 薬局
- 大学、研究機関、トレーニング施設
- 大学、研究機関
- 接骨院整骨院
- 消防等
- 歯科技工所
- 歯科技工所
- 歯科技工所
- 歯科技工所
- 歯科技工所
- 歯科医院
- 検査センター等
- 検査センター等
- 検査センター
- 検査センター
- 検査センター
- 検査センター
- 検査センター
- 検査センター
- 検査センター
- 検査センター
- 血液センター
- 技工所
- 技工所
- 介護施設
- 介護施設
- 一般企業

41

# 【全回答】

[Q40]サイバーリスクが懸念される医療機器について、製品(医療機器)の使用環境を特定していますか。
(n=259)

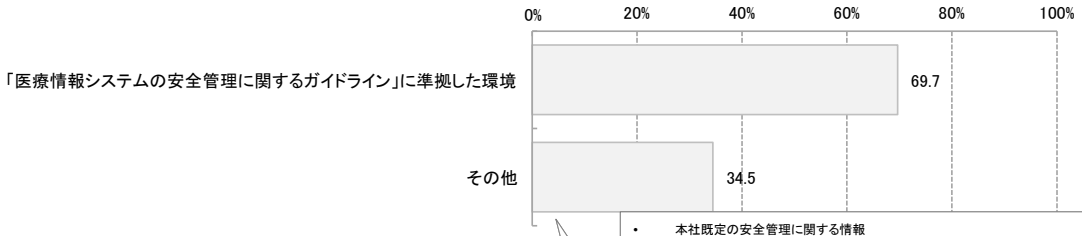





42

# 【全回答】

[Q41]「全て」、「一部」の場合、どのように特定していますか。
(n=145)

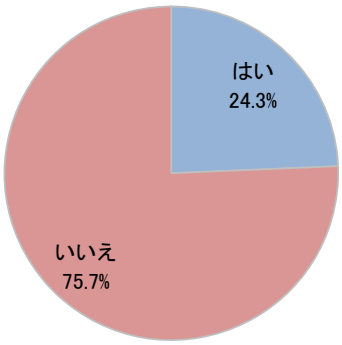



- 本社既定の安全管理に関する情報
- 納品文書
- 添付文書や取扱説明書で使用環境を特定。
- 添付文書/取扱説明書/現場確認
- 添付文書、取扱説明書等で使用方法を規定
- 添付文書、取扱説明書、社内基準
- 添付文書
- 送信のみである
- 全てCDからのダウンロードである
- 設置場所が特定されている。
- 設置時に特定できる
- 設置管理医療機器であるため
- 設計開発を行った製造元の規定
- 製造元のリスク分析
- 周辺温度、湿度
- 取説、添付文書、仕様書、リスクマネジメント等
- 社内設置手順に基づいた状況かどうか
- 社内で規定した環境
- 自主規定
- 自主基準
- 自社判断
- 自社設定基準
- 自社基準
- 使用エリアのみを特定
- 顧客による報告
- 顧客(医療機関)の要件に準拠した環境
- 各機関設定のセキュリティーポリシー
- 海外親会社から提供されるマニュアル
- 一般的な記載（水・埃に注意など）
- リスクマネジメント
- ほとんどが設置管理機器であることから、及び営業の設置情報により。
- セキュリティの確保されていない環境に接続しない事等を指示。
- セキュリティの確保された病院内のネットワークに接続して使用することと特定している。
- インターネットに接続させない。
- PC動作環境
- ISMSの構築
- IEC60601-1, FDA Guidance Postmarket Management of Cybersecurity in Medical Devices
- AAMI TIR57:2016

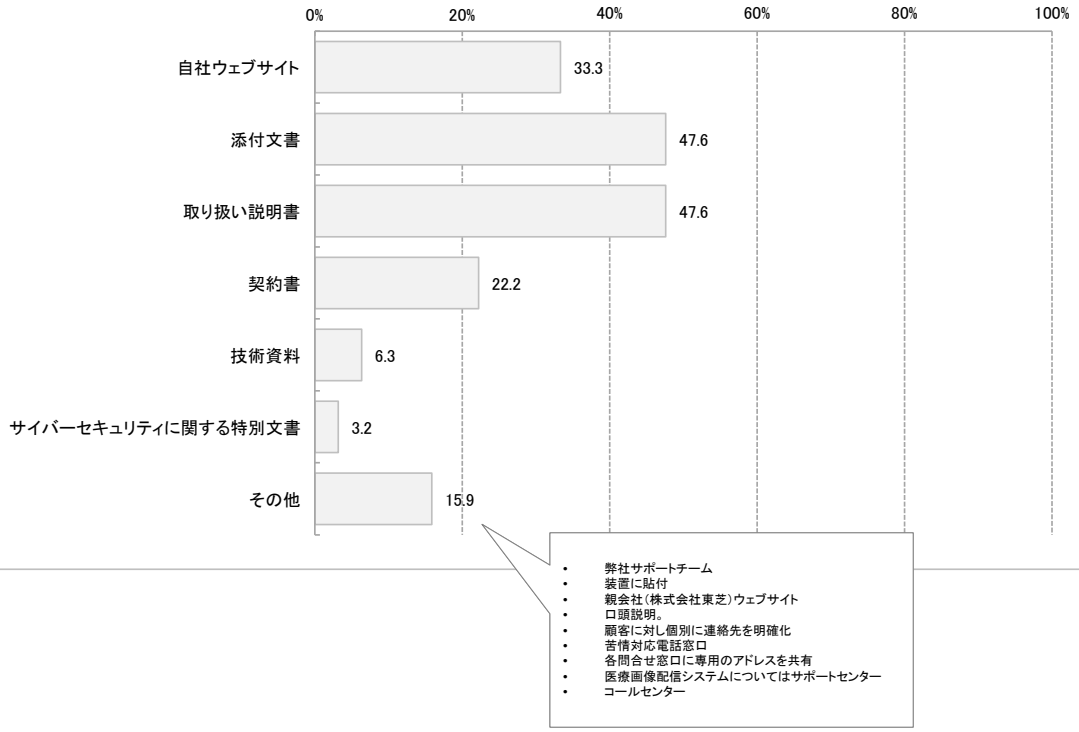
43

# 【全回答】

[Q42]サイバーセキュリティに関する問い合わせ先を明確にしていますか。
(n=259)



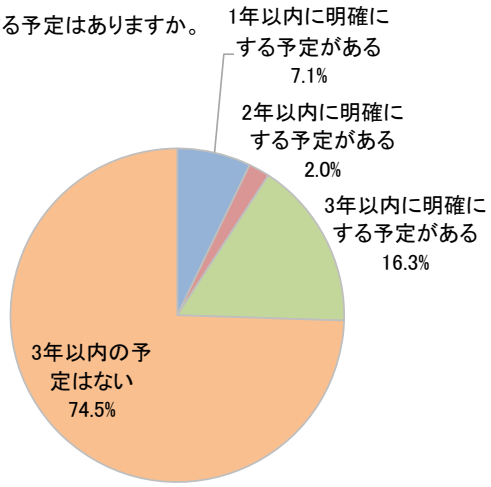
[Q43]「はい」の場合は、どのような方法で明確にしていますか。
(n=63)



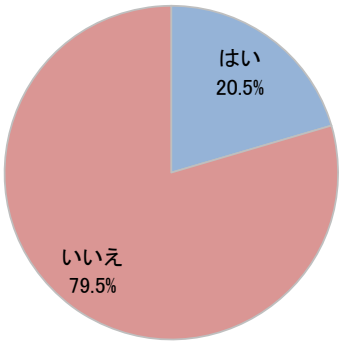





[Q44]「いいえ」の場合、3年以内に明確にする予定はありますか。
(n=196)



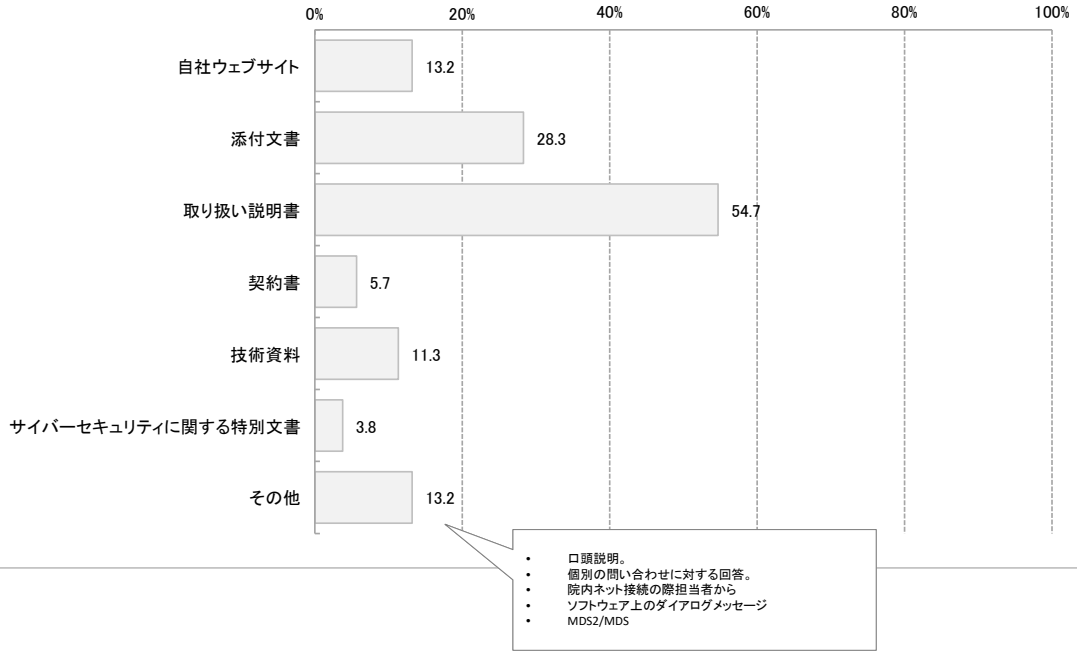
[Q45]製造販売時におけるサイバーセキュリティに関する情報を使用者に対して提供していますか。
(n=259)



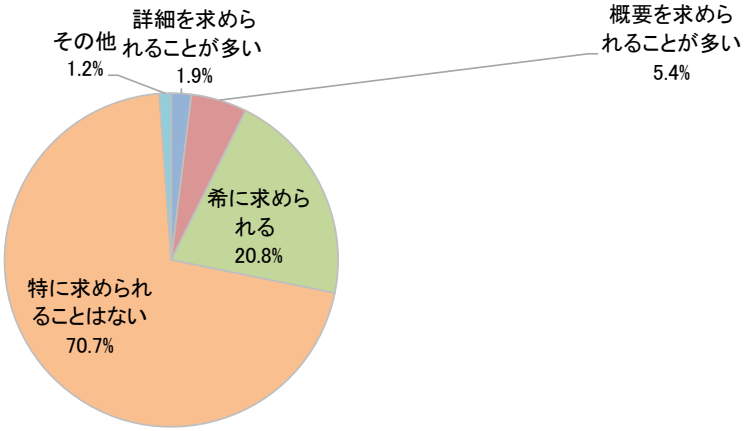





[Q46]「はい」の場合、どのような方法で提供していますか。
(n=53)



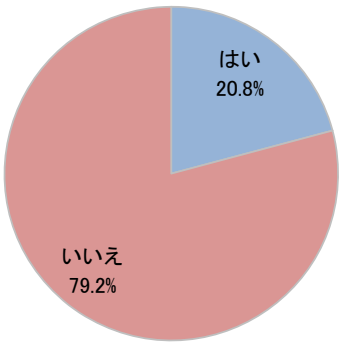
[Q47]売買の引合いや契約等の際に、医療機関等からサイバーセキュリティに関する情報提供を求められますか。
(n=259)



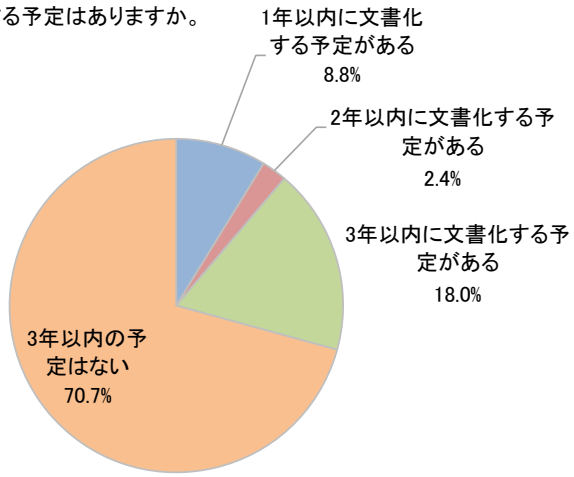





[Q48]サイバーセキュリティに関するインシデント発生時の国内届け出先や手順などを文書化していますか。
(n=259)



[Q49]「いいえ」の場合、3年以内に文書化する予定はありますか。
(n=205)



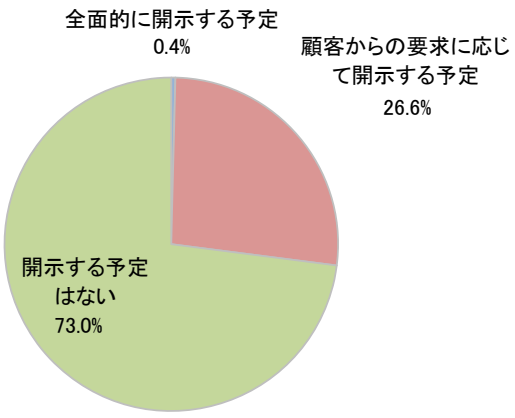





[Q50]貴社は、製品(医療機器)に関するソフトウェア部品表・構成表(SBOM)(注)を医療機関などの顧客に対し、開示することを今後3年以内に予定していますか。

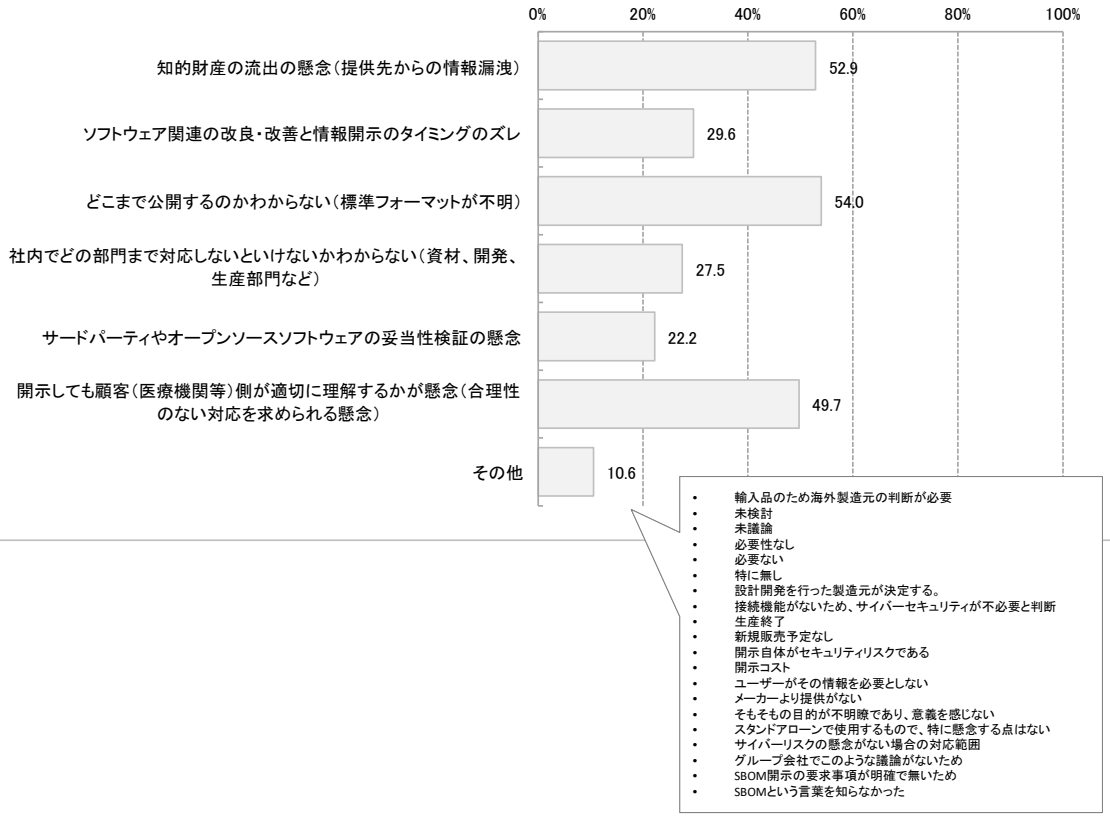
(注) 医療機器に使用されているソフトウェアの透明性を確保するため、製造販売業者は医療機関などの顧客に対してソフトウェア部品表・構成表 (software Bill of Materials: SBOM) を提供して顧客が医療機器のライフサイクルに影響を与えるソフトウェアコンポーネントをよりよく理解できるようにすることが、今後のサイバーセキュリティ対策には必要であるとの議論が国際的になされています。

(n=259)



【全回答】

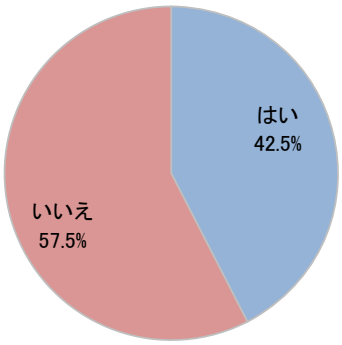
[Q51]「開示する予定はない」の場合、ソフトウェア部品表・構成表（SBOM）の開示には何か課題があると考えられますか。
（n=189）




53

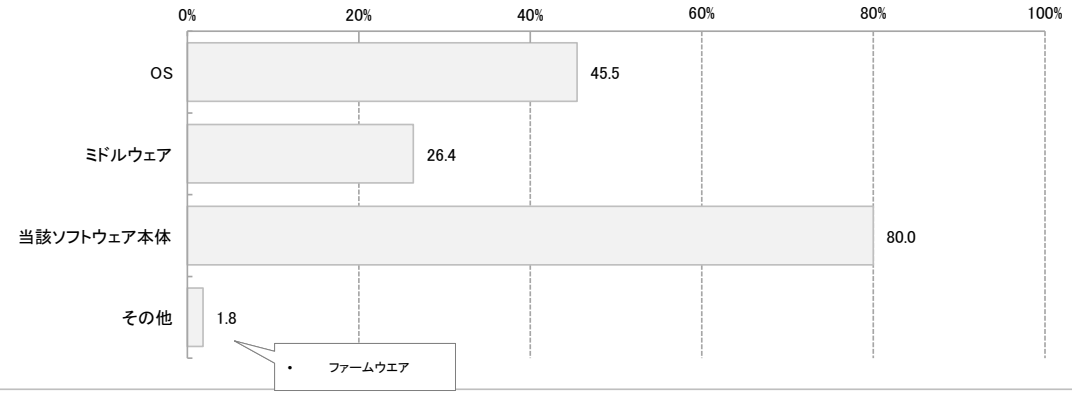
【全回答】

[Q52]市販後に脆弱性の改善に関係するプログラム（ソフトウェア）のアップデートを行っていますか。
（n=259）



【全回答】

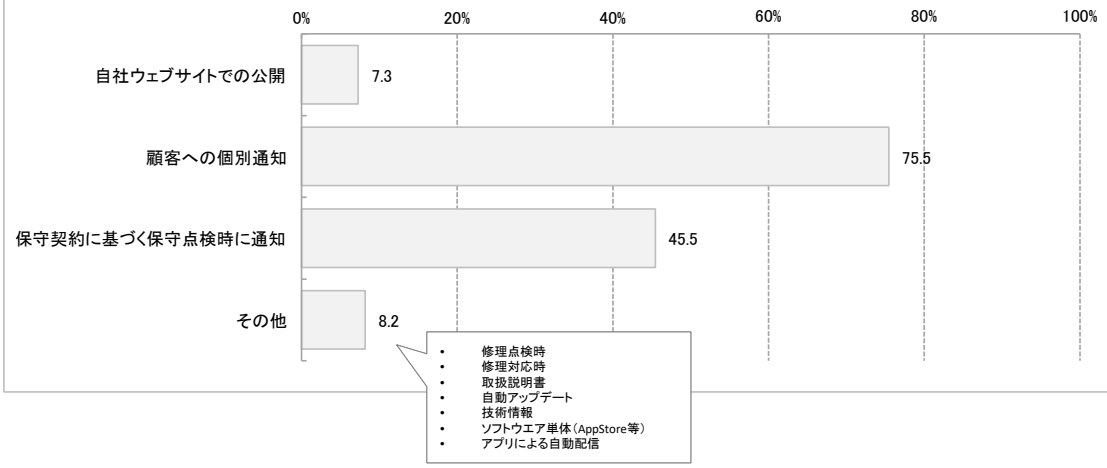
[Q53]「はい」の場合、アップデートする対象をお答えください。
(n=110)



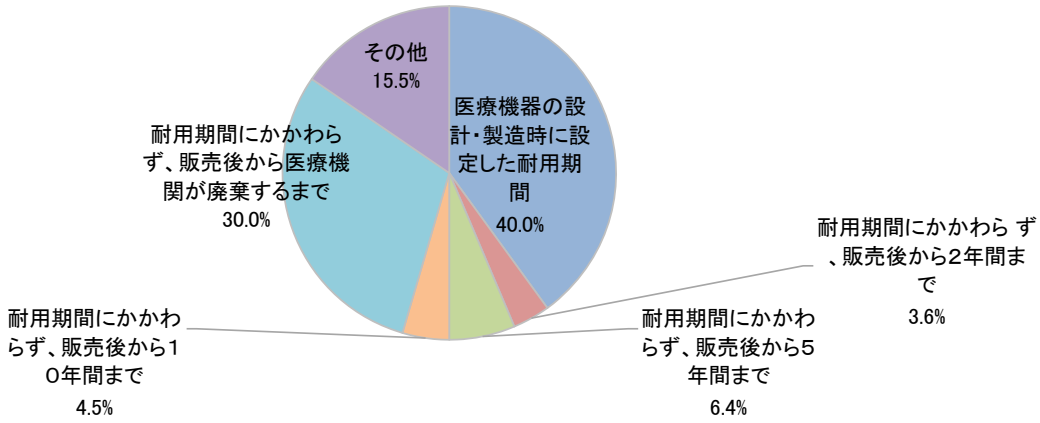

55

【全回答】

[Q54]「はい」の場合、アップデートに関する情報提供の方法をお答えください。
(n=110)



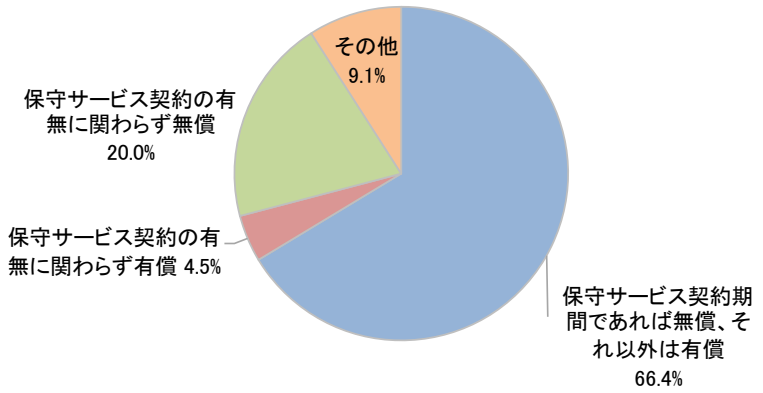
[Q55]「はい」の場合、アップデートを行う期間について、社内の考え方として最も一般的なものをお答えください。
(n=110)





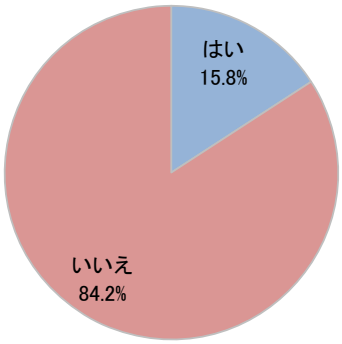



[Q56]「はい」の場合、アップデートを行う際の費用について、社内の考え方として最も一般的なものをお答えください。
(n=110)



【全回答】

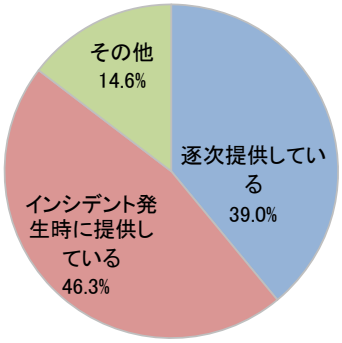
[Q57]市販後においてサイバーセキュリティに関する情報を使用者に対して提供していますか。
(n=259)




59

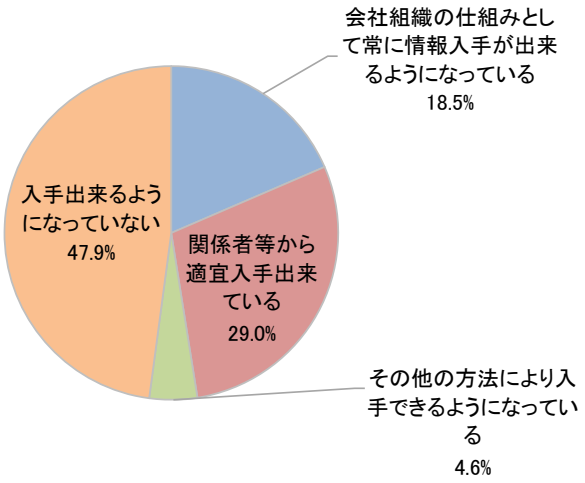
【全回答】

[Q58]「はい」の場合、どのタイミングで提供していますか。
(n=41)



【全回答】

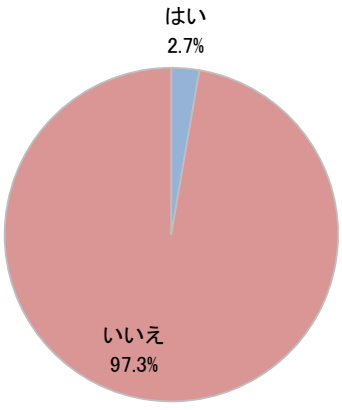
[Q59]使用現場（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。
(n=259)




61

【全回答】

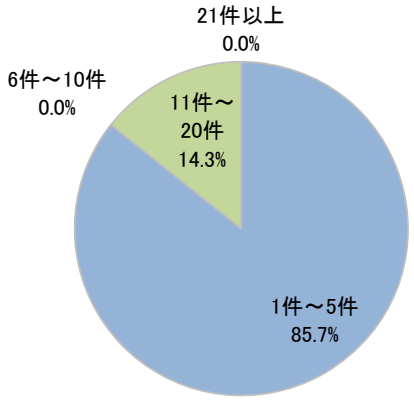
[Q60]貴社の製品（医療機器）に関連して、医療機関から報告を受けたサイバーセキュリティに関連したインシデント事例が3年以内にありましたか。
(n=259)






62

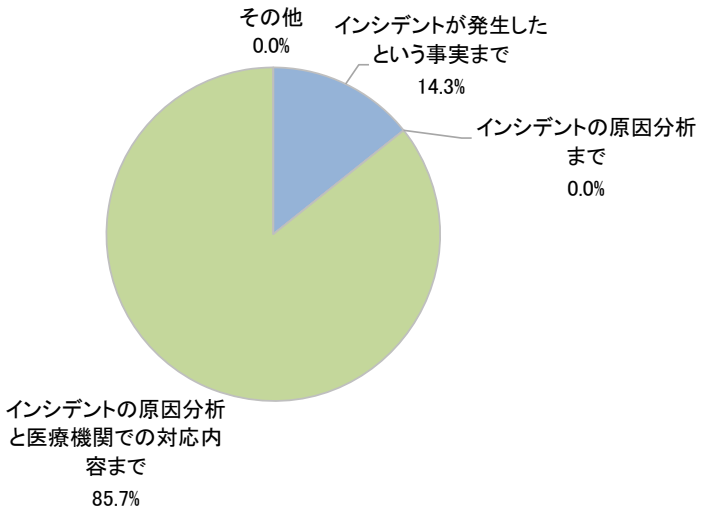
[Q61]「はい」の場合、どの程度の件数でしたか。
(n=7)



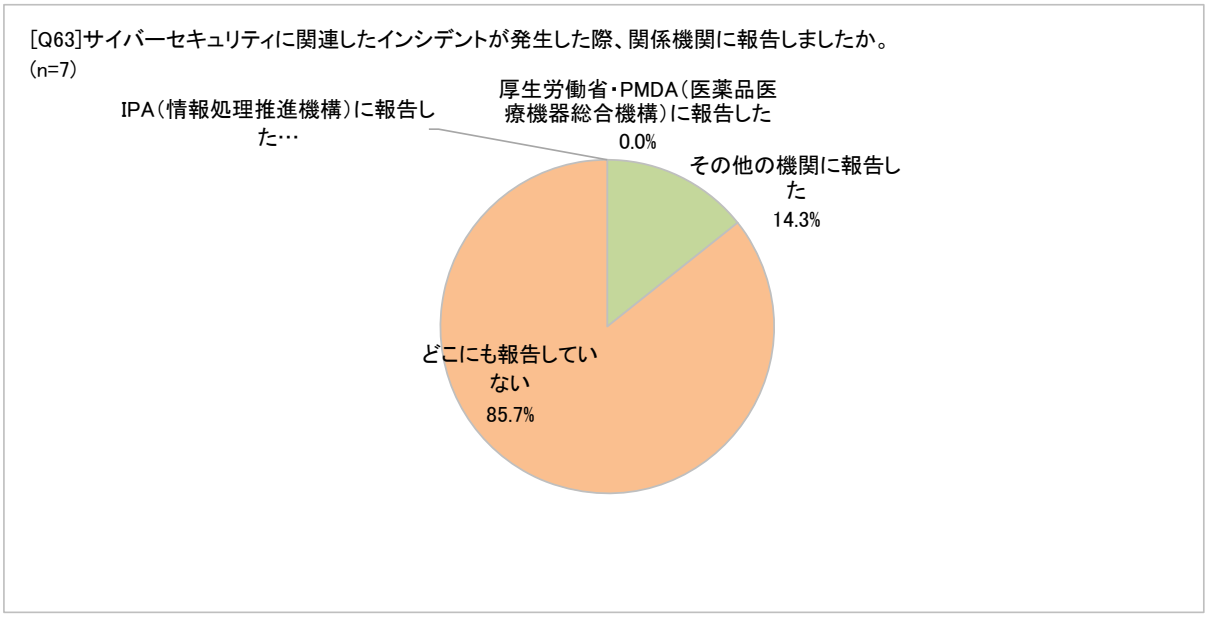





[Q62]「はい」の場合、どのレベルの情報まで情報を入手出来ていますか。
(n=7)



【全回答】



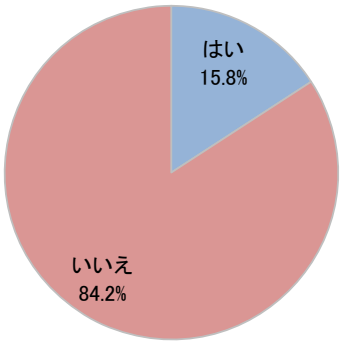



【全回答】

## [Q64]使用現場からの情報入手について、課題や要望等がありますか。

- 品質マニュアルのSOPにより情報が入手できる体制が構築されているので、課題はないと思います。
- 大手が販売する高リスク高額な医療用機器と、中小(零細)の販売する低リスクの家庭用機器を同列に扱わないで欲しい。
- 全国の医療機関において、院内ネットワークやソフトウェアの導入状況、院外往診や検診等で外部LANの使用状況等、使用場所ごとの主要な使用環境についての情報が欲しい。
- 施設によりセキュリティポリシーが異なるため、画一的な対応は不可能である。まずは施設のセキュリティ対策を明確に実施してほしい。また、他社のサイレントアップデート(特に電子カルテ)時の不具合が散見される。
- 使用者環境が千差万別であるため、自社製品に関連するインシデントかどうかを判断するのが難しく、どこまで医療機関に協力を依頼すべきかが課題。
- 使用現場から直接情報を入手する仕組みをどこまで構築するべきかの明確化が必要
- 使用環境での実際の運用が見えない
- 国内に米国のH-ISACのようなISAOが欲しい
- 現場の知識(専門用語など)レベルの問題がある。口頭での伝達が難しいケースがあり、書面でもらうか連絡先を聞き社内担当が直接やり取りするケースが多い。日々変化するセキュリティー環境の中で現場への落とし込みは非常に難しい。
- 技工所も医療情報システムの安全管理に関するガイドラインで指定されている医療機関等に該当するのか？
- 各機関でのセキュリティポリシー、規定を知る必要はあるが実施していない。
- 家庭向けの場合は、情報収集は困難である
- 医療機関において、何がサイバーセキュリティに関連したインシデントなのか理解されていないと思われるので、ほぼ情報収集ができないのではないかと考える。医療機関でもサイバーセキュリティに関する教育を充実れ瀬、適切な対応が行えるようにしてもらいたい。
- ユーザーがネット接続や他の機器(PC含む)に接続する医療機器ではない(スタンドアロン製品です)。
- メーカーが情報を収集するのではなく公的機関がまとめて収集をして欲しい
- どのような場合が情報入手対象になるのか設定が難しい。情報入手と対応のタイミングの設定をどうするか。
- どこまで聞いていいか分からない
- サイバーセキュリティに関する情報がすべて上がっているか判断できない。
- サイバーセキュリティに該当するかどうか不明なケースがある。
- インターネットのセキュリティ情報サイトからでないと、インシデント情報が入ってこない
- インシデント発生時の再現性が課題。特に自社以外の接続機器のセキュリティ対策状況が不明瞭のため、適切な対策を講じにくい。

[Q65]販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導等を行っていますか。
(n=259)



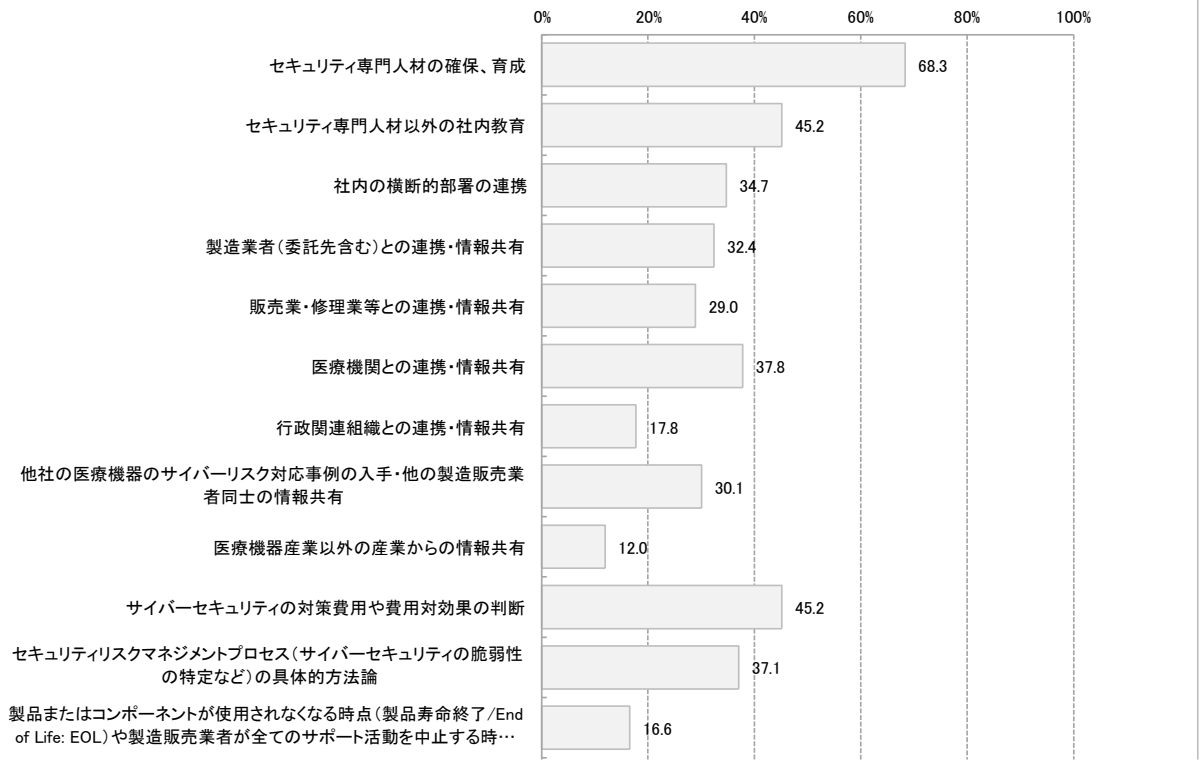





空白ページ

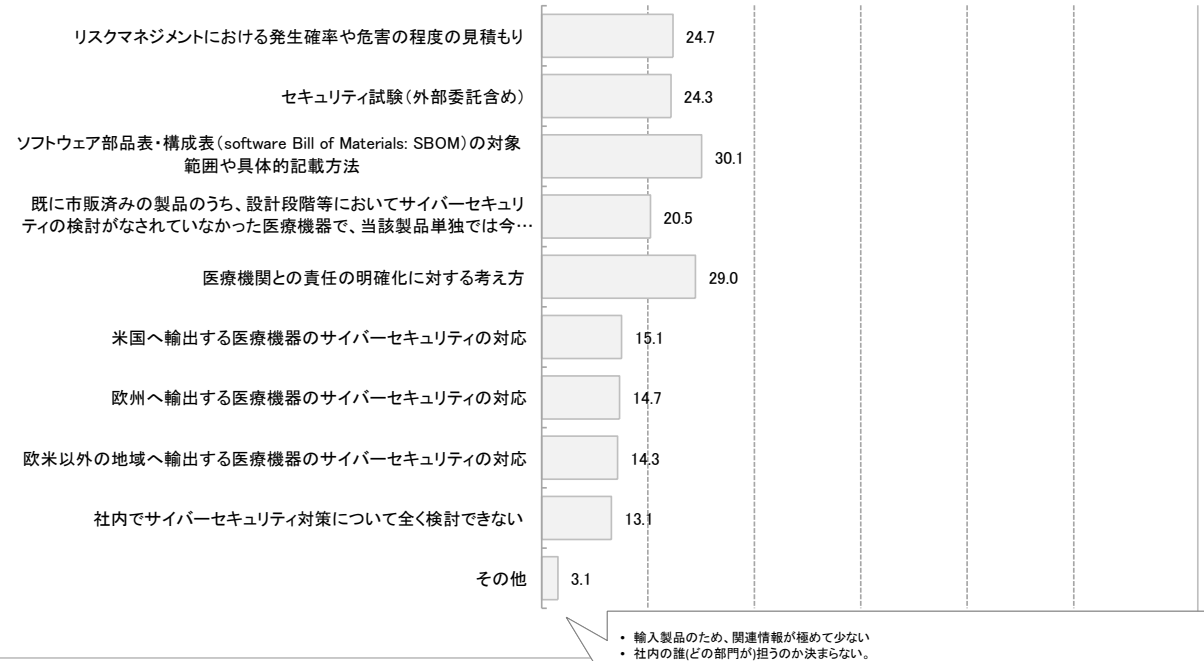
【全回答】

[Q66]貴社におけるサイバーセキュリティ対策の課題についてお答えください。
(n=259)






【全回答】




- 輸入製品のため、関連情報が極めて少ない
- 社内の誰(どの部門が)担うのか決まらない。
- 基幹業務としてのサイバーセキュリティ体制は構築されています。また、製品については、簡単なソフトウェアを組み込んだものであり、サイバーセキュリティの問題とはなじみ難いように考えられます(バグの問題の方が大きい・・・)。
- 海外本社からの情報
- 海外主導で対策しており、国内の通知等を適宜情報提供することにより対応している。翻訳までの時差が短縮できると良い。
- 医療機器を操作するPCのサイバーセキュリティ上の取り扱いの明確化
- リスクと利益に対して対策費用が見合わない
- コスト

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【行政に対するご意見・ご要望①】

【全回答】

- 弊社のような弱小零細企業は、慢性的に資金がない。新たな試みに対して資金がなく、資金繰りの圧迫が懸念される。補助金等の資金面の手当てがなければ、現実的ではない。これが零細企業のリアル。
- 輸入業者（製販）として必要な具体的対策の提示をお願いしたい。
- 毎年度1回位定期的に無料のセミナを希望します。お願いします。
- 本件に関しましては、本格的に参入しておりませんので、現時点ではございません。
- 防衛だけで無く発信源の摘発率向上、厳罰化を望む。匿名性・非現実感に醸成される犯罪は、詐欺等に肥大し、国民の勤勉性を消滅させる危機的状況にある。
- 複数省庁にまたがっているガイドライン等の統合
- 認知度を上げてほしい
- 日本発の医療機器の海外展開を容易にするため、日本独自のセキュリティ要件は最小限にしていただきたい。
- 特になし。（決まれば従う）
- 動向やセミナー情報を入手したい。
- 当社は主に防衛医療に関する製品も開発しているので、防衛省関係（関係企業、団体）の情報もフィードバックしてほしい。今後、重要と考えられます。
- 電子カルテのソフトに結合するものを供給しますが、統一規格が必要性がありますが、現状を理解していません。
- 対応の指標として、医療機器の基準（認証基準又は基本要件基準）にIEC 80001-1やIEC/TR 80001-2-2、行政通知等への適合性を要求するなど明確にして欲しい。PMDA・総務省と合同で研修会や講習会を行い、国内外の状況や具体的な対応について解説して欲しい。
- 他国・外部からの侵入は、犯罪となることを知らしめる制度を確立させてほしい。
- 説明会
- 製造販売品目に応じた指標を希望します。
- 初心者を対象とした講習会等の開催をしてほしい。
- 主に医療情報システム向けとしてガイダンスが発行されていることもあり、医療機器個別でどこまで対策すべきかの判断が難しい。
- 自社製品や自社設計ならともかく、海外製品を輸入する場合、ハードウェア的に穴を作られればどうしようも無い。行政としても、すべての機器に全品チェックをすることは不可能なので、そう言う通信機器の不正な挙動を見つけた者に懸賞金を出すなど広く一般の力を利用すべきと思う。
- 講習会を開催して、有効なセキュリティ対策実施の現状についてご指導いただきたい。
- 講習会の開催を希望します。
- "行政は行動の指針を発表し、年度ごとに細かく改定や見直しを進めていただきたい。
- また、サイバー攻撃を行う国は長年ずっと同じなのでAIなどで攻撃を受けた際に自動で反撃・または特定の国のアクセスを遮断するシステム構築をするべき。また、そのシステムは海外にも販売できると思う。"
- 行政として、サイバーセキュリティに関する要求事項を明確にしてほしい。要求事項が曖昧なため、過不足が懸念されます。
- 行政ガイドライン例に必ずしも一致しないケースがあるが病院はガイドラインへの適合を求めてくるケースが多く対応に苦慮している。



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【行政に対するご意見・ご要望②】

【全回答】

- 公教育での基本的なIT教育を欧米並みにやって欲しい。まずはそこから。
- 個人情報保護も含めて、医療機器製造販売に関わるサイバーセキュリティの具体的は手順書の見本等も整備して欲しい。
- 現状は、基幹業務以外では特に問題はないと存じますが、今後、より高度な製品を製造販売する際には、ご指導、ご協力の程、お願い申し上げます。
- 具体的な対策例などの開示があれば有難い。
- 具体的な事例に基づくガイダンスを提供してほしい
- 具体的な資料の作製やセミナーを開催して頂けるとありがたいです。
- 規制・対応内容の明確化、窓口の一本化
- 機器は内容によってこうした問題の対象となるものとならないものがあるのに、すべてひとくくりで施政するのはやめてほしい
- 基準を設けて、それを守るようなガイドラインがあると良いのでは
- 各社の承認申請内容の関して情報漏洩などが無いように万全を期してほしい
- 海外諸国規制との整合性を取って欲しい。
- 何をもって自社のサイバーセキュリティ対策とするか、定義不明。医療機器側で対応できない状況にあるのではないか。
- 横断的な情報共有取り組みの強化（経済産業省、総務省、厚生労働省間含め、各種業界）を希望する。
- 医療機器業界のISAO設立を希望します
- 医療機器のサイバーセキュリティに係る課題についての検討結果を公表して頂きたい。
- 医療機器のサイバーセキュリティに関する情報をメール等で提供して欲しい。
- 医療機器にまつわるインシデントをご紹介ください。
- 医療機関でのサイバーセキュリティ管理に係る費用（専用スタッフ、外部委託）については、診療報酬で評価するなど、医療機関が主体的に動ける仕組みを導入いただきたい。
- 医療システムは国家の重要インフラであり、サイバー攻撃による医療機器等の誤作動等による健康被害の防止、又医療機関が扱う患者の要配慮個人情報の観点から、特に小規模の医療機関の現状把握の上、継続的な財源の担保について一刻も早い対応を望みます
- よく分かりません。
- ユーザ、医療施設側への教育、啓蒙を、通知、ガイドラインのアップデートなどで、継続的に行ってもらいたい。
- もう少し具体的に検討をしてほしい。
- もう少し具体的でわかりやすいサイバーセキュリティ対策のガイドラインを作成していただきたい。
- メーカ、医療機関それぞれに対して、具体的な対策レベル感がわかるような対応指針を示していただけるとありがたい。医療機器メーカに対して医療機関毎に異なる対策を要求されても対応できないので、一定の対応基準が求められる。
- セミナーを実施して頂きたい
- サイバー攻撃に対する罰則強化

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【行政に対するご意見・ご要望③】

【全回答】

- サイバーセキュリティ人材の育成支援
- サイバーセキュリティへの対応は医療機器メーカーだけでは対応できないため、医療機関（特に中小病院や個人クリニック、歯科医院）も積極的に対応してもらえる取り組みを実施してほしい。また、中堅企業がサイバーセキュリティへの対応が行うための補助金等が申請できるような体制を検討していただきたい。
- サイバーセキュリティの担当者が居ないため、将来的にネットワーク非接続の医療機器取扱い業者に対しても情報セキュリティなどの規制要求事項等が発出される際には、素人にも分かりやすい言葉で具体的なご指示を発出して頂けると助かります。
- サイバーセキュリティの重要性は増していると思うので対策についてアドバイスがあればほしい。
- サイバーセキュリティの具体的な評価・方法が知りたいです。チェックリスト等があると参考になります。
- サイバーセキュリティに対する指針を明確にしてほしい。
- サイバーセキュリティに関連する情報展開をしてほしい
- サイバーセキュリティに関連する講習会の実施
- サイバーセキュリティに関する知見が乏しい。セミナー、講演会を開いてほしい。
- サイバーセキュリティについて関連するガイドラインや規定等があれば把握していきたい。
- ｻｲﾊﾞｰｾｷｭﾘﾃｨについても法令化する場合は、ｸﾞﾚｰﾄﾞやｸﾗｽに分類して管理体制の差別化を図って欲しい。
- サイバーセキュリティについては、プラットフォームとなるOSやCPUの提供メーカーの意向に大きく左右されるため、それら大手企業からの情報提供の量と質をもっと向上させるよう、折衝を行ってほしい。
- サイバーセキュリティー対策のための補助金を使いやすくしてほしい。中小企業にとっては汎用のセキュリティーソフトの購入などから始めたいところだが「汎用」は対象外である現状がある。
- サイバーセキュリティーに関するポータルサイト的な総合サイトが欲しい。公表されている通知、ガイドライン、Q&Aなど、厚労省、経産省、内閣（NISC）、総務省、FDA、EC(MDCG)などの枠にとらわれないもの。
- ガイダンス以外に早期にSpecific Requirementを明確にしていただきたい
- インシデント発生時の情報等を開示していただきたい
- Windows7、XPのサポート終了に伴い、顧客、企業共に大きな負担となっている。行政からWindows7の交換に対する助成金や、起業でのセキュリティー対策（IT、現地で修理する人員）の助成等を検討して欲しい
- Securityに係わる法整備が必要です。 ・ハッカーにに対する刑事罰等 ・医療機器に対するNetworkへの接続規制 ・認証基準にSecurity項目の追加 ・法整備の国際協調または事件に対する国際協調 ・GuidanceからRegulationへ移行 ・業許可の要件にSecurity項目を追加
- Q&A等の事務連絡を発出してほしい。
- OSプロトコールレベルの話を一企業に対応求められても実質対応不可能。
- ISO13485+ISO27000シリーズのJIS化等により、対策方法の指南書を制定して欲しい。
- FDA適応に追従して欲しい



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【行政に対するご意見・ご要望④】

【全回答】

- 1.サイバーセキュリティに関する講習会の開催 2.コンサルタントの無償提供派遣
- 1、医療機関におけるサーバーセキュリティの大きな課題の一つとして、対策費用の捻出がある。これは他国でも同様。特に保健医療制度による収入のキャップ、人材不足、働き方改革など、労務費負担増の傾向などがサイバーセキュリティ対策の足かせとなっていると推測される。行政として、この費用面に対する解決の検討をお願いしたい。2、各国のサイバーセキュリティ対応の要求は現在同じ方向性で制定され集約されつつある状況にある。一方で日本は国独自の細かい部分が多々あり他国との歩調が合っていない。よって、世界の流れに沿ったガイドラインなどの策定を希望する。3、厚労省の医療機器に対するガイドラインの中でライフサイクルサポートとサポート期間の指針が示されているが、世間のソフト、ハードのサイバーセキュリティサポート期間を考慮すると実現が甚だ困難であり、サポートする側、される側、サービスを購入する側の三者の実情を考慮した内容となるよう継続検討していただきたい。
- ・厚労省：安全管理ガイドラインの教育活動を促進して欲しい ・現在5版の改定作業進めていると思いますが、医療機関と製造販売業者との連携が重要であることはもっと通知して欲しい ・IMDRF文書N60のパブコメが出ていますが、これが公開になった後、行政としてどう規制に盛り込むのか迅速な対応を期待しています

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【業界団体（工業会等）に対するご意見・ご要望①】

【全回答】

- 例えばPCの積極的活用。最新のツール（iPad等）の活用を促して欲しい。まずそこから啓蒙して頂きたい。
- 理解を進めるために定期的な講習会開催
- 輸入業者（製販）として必要な具体的対策の提示をお願いしたい。
- 明確なガイドラインの策定と責任範囲の明確化
- 平成30年7月24日通知「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」（薬生機審発0724第1号薬生安発0724第1号）における、「サイバーリスクに伴う医療機器の不具合等の情報」について、業界団体で情報提供・共有いただける仕組みがありましたら幸甚です。
- 被害事例の紹介やワーストシナリオの紹介などを含め、全ての企業が適切なレベルの危機感を持つことができるよう、サイバーセキュリティに関する情報提供の場を積極的に設けて頂くことを望みます。
- 特になし。。（決まれば従う）
- 添付文書テンプレートにサイバーセキュリティに関する文言が欲しい。
- 適時、情報開示。サイバーセキュリティに関する対応・対策等の参考例の紹介
- 抽象的なガイダンス、ガイドラインではIoT、サイバー、フィジカル空間の連携として統一性に欠ける。可能な限り具体的な指針を定め、各社共通の対応ができる体制にしてほしい。
- 中小企業にも無料での団体加盟の方法を検討して門戸を広げて欲しい。
- 大手企業保護ではなく、全企業保護の企業目線で検討してほしい。
- 製品数によって割引がある工業化に参加したい。 製品数によって割引があれば、加入したい。
- 製品の特質を考慮したカテゴリー分けを行いRequirementを明確にする必要があると思います。WG等を活用し取り組みをお願いいたします。
- 製販側の対応ガイドラインなどの作成、アップデート。継続的な教育、啓蒙の実施。
- 製造販売業者として何をどのようにするかの具体的な対策に関して講習会等を希望する
- 上記の政府からの指針提示が困難な場合、業界団体が示すことで補うことも現実的な対応になり得る。
- 上記と同じですが、理解化していません。
- 上記が達成されれば業界団体は、それに従うことになる。
- 上記、行政に対する意見・要望への対応に同じ。
- 初心者を対象とした講習会等の開催をしてほしい。
- 実例とその対応内容などを紹介していただけたらと思います。
- 今後とも、適正なルールの策定と普及に努めて頂ければと存じます。
- 講習会開催
- 講習会の開催等を希望します。
- 講習会の開催を希望します。
- 講習会の開催



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【業界団体（工業会等）に対するご意見・ご要望②】

【全回答】

- 講習・セミナーの充実
- 講演会を実施してほしい。
- 具体的な対策例などの開示があれば有難い。
- 具体的な事例を提示してほしい
- 業界団体はJIS規格やISOなどでプログラムやITに関連する製品を製造する際の指針や規約などを定めてもらいたい。
- 業界として、対応していただきたい、対応したい。
- 機器を含まない単体プログラムのみを扱う製販としてやっておくべき対策（事例）を具体的に示してほしい。
- 各団体での認識および見解の統一を図って欲しい
- 各製造業者への啓発活動のほか、医療機関側の主体的な活動の推進と、行政・医療機器に理解を求める動きをしていただきたい。
- 引き続きセミナーで情報を展開して欲しい
- 一般的管理状況の講演会などで方向性や対応を教示して欲しい。
- 医療機器製造販売に関するサイバーセキュリティ―の講習会、セミナー等を実施して欲しい。
- 医療機器のサイバーセキュリティに係る課題への対応について講習会等実施して頂きたい
- 医療機器のサイバーセキュリティに関する情報をメール等で提供して欲しい。
- 医療機器のクラス分類などによる、セキュリティ対策は考慮するべきであり、一律の対策では、メーカーへの負担が大きくなる場合もある
- 医療機器にもスマホアプリやクラウドサービスなどを使うものが出てきているので、そのようなITサービスを行う事業者との連携も含めてサイバーセキュリティ対策を考えていく必要があるのではないでしょうか。
- 医療機器にまつわるインシデントをご紹介ください。
- 医療機器におけるサイバーリスク対応事例の紹介、対応に関連する情報の展開、講習会などの開催
- 医機連傘下の団体の中にも委員会を設置し、各団体で取り纏めや報告会開催を推進してほしい。
- より現実に近い体制構築事例等を紹介していただけるとありがたい。
- よく分かりません。
- セミナーを実施して頂きたい
- セミナーの企画
- セキュリティプログラムの評価を会員間で共有出来る取り組みを検討して欲しい。
- すでに実施されているが、各工業界特有の問題を扱ったセミナーの開催など。
- サイバーセキュリティ対応を行っている（できている）企業の具体的な対応方法や、現時点で最善と考えられる取り組み事例の紹介、医療機関向け（特にサイバーセキュリティ対応が十分でないと考えられる中小病院や個人クリニック、歯科医院等）の注意喚起リーフレット等を作成してほしい。
- サイバーセキュリティに関する教育

**40**

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【業界団体（工業会等）に対するご意見・ご要望③】

【全回答】

- ガイドラインは提示されるが、具体的にどうすれば？で話が止まってしまう
- インシデント発生時の情報等を開示していただきたい
- ・承認、認証におけるsecurityに対する試験方法の確立 ・Incidentに対する情報の協調 ・Security強化によるコストアップの抑制 ・会員各社にSecurity教育の啓蒙
- ・院内機器ネットワークの共通化を進めてほしい ・ネットワークへの接続費などの問題を解決してほしい(接続費の目安の規定など)
- ・もっと医機連主体でサイバーセキュリティ対応の事例紹介など含めた対応セミナーを開催して欲しい ・IMDRF文書N60のパブコメが出ていますが、これが公開になった後、行政の対応を受けて、セミナーなどいち早く開催して欲しい

77

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【医療機関に対するご意見・ご要望】

【全回答】

- 弊社の製品は家庭用であり、医療機関様で使用されることはないと存じます。
- 弊社が製造販売する医療機器に関しては直接サイバー攻撃の対象にならない製品ですが、弊社が構築した社内基幹システムなどは強固なセキュリティで守られており、それが当たり前ですが この時代でもまだまだ対策を殆どしていない企業が多いので継続して啓蒙していただきたい。
- 病院ごとにサイバーセキュリティーに対する見識の相違が大きく、メーカーとして対応しきれない場合が多い為、見識を統一して欲しい
- 認知度を上げる
- 適時、情報開示。サイバーセキュリティに関する対応・対策等の参考例の紹介
- 現時点で特にございません
- 患者の個人情報を守る制度が必要です。
- 学会でのワークショップの開催
- 各医療関連協会、団体等で周知されていると思われるが、「医療情報システムの安全管理に関するガイドライン」は、ボリュームがあり、わかりやすい冊子やQ&Aなどがあれば、より理解が進むのではないか？
- 外部接続の完全シャットアウトの緩和
- 医療機器にまつわるインシデントをご紹介ください。
- 医療機関は、サイバーセキュリティ管理において、医療機器（メーカ）側への依存が高いので主体的な活動を計画いただく必要がある。
- 医療機関に関してはどの程度のネットワーク使用環境が確保されているのか、それが適正な状態か評価基準が判りにくい。 病院機能評価を受審している医療機関が多いと思うので、評価項目にサイバーセキュリティ面の審査を追加し、サイバーセキュリティ対策の積極的強化を促して欲しい。
- 意識の低い医療機関が多い
- ユーザー側で各自にセキュリティ対策が必要であることを認識してほしい。
- セミナーを実施して頂きたい
- セキュリティ、危機管理意識を持ってほしい
- サイバーセキュリティは医療機器メーカーだけが対応するものではなく、基本的には医療機関のシステムがベースになっているということをもっと自覚してもらい、医師会や学会と連携してもっとサイバーセキュリティへの取り組みを積極的に行ってもらいたい。
- サイバーセキュリティー/病院ポリシーを理由に話を聞かずにNGを出す機関が多数見受けられる。（現場ではなく医療情報課等のIT管理部門側にて）
- カルテの個人情報流出を防止して欲しい。
- インシデント発生時の状況（人と物の流れ）、使用環境（他社製品含む）の明確化（テンプレート化）を希望する。
- ITに伴うIot・AIの普及は拡大しており、医療機関におけるIT安全対策の在り方がわかるように願いたい（確認時だけでも）
- ・サイバーセキュリティは共同責任（Shared Responsibility）であることを認識してもらった上で、相互に協力することで対応して欲しい ・ネットワーク構成など製造販売業者との情報交換、相互協力をもっと進めて欲しい
- ・Hardwareを含めた医療機関専用のNetworkを構築してはどうか。 ・Incidentに対する情報の協調



78

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【その他のご意見・ご要望①】

【全回答】

- 有意義な調査だと思います。ありがとうございます。
- 弊社現状医療機器製造販売は行っておらず、販売終了製品の保守のみ行っているのでサイバーセキュリティーについて無体策である。将来製造販売が復活したときは考慮したい。
- 弊社は本社が外国医療機器メーカーの日本法人であり、設計製造は全て本社である為、本社の組織体系を前提とし、回答させて頂きました。
- 弊社はクラス1でQMSが適用されない鋼製小物を製造販売しています。製品にはサイバーセキュリティ対策は実施していませんが、設計や管理用のシステムには親会社（100%出資）のシステム部門がサイバーセキュリティ対策を実施しています。
- 弊社は、製造販売業のみで製造業を取得していなく、医療機器の製造販売業に関する業務に係るIT機器は、書類作成等を行うPCのみとなっている。その場合、サイバーセキュリティ管理はどこまで必要か指針を作成していただきたい。
- 弊社の医療機器は電子系を含まないものなので、本アンケートの内容にそぐわない部分がありました
- 弊社のようにIoTに関わらない医療機器のみ製造販売し、社員数も少なく特に社内に電算システムすらもたない企業では、個々のPCのウイルス対策ソフト導入以外何が必要か皆目見当がつきません。そういう最低レベルに該当するサイバーセキュリティの施策もご検討して頂きたいと思います。
- 日々の技術の進歩、陳腐化に追いついていないと感じる。より柔軟で早急な対応が取れるための施策が必要と感じる
- 当社所在地域外の地方で行われる医療機器等のセミナー、展示会等のDMが増えたように思う。
- 当社は外資企業で、海外本社主導により、全世界の社員に近年サイバーセキュリティに関するe-learningの分量、頻度とも、大幅に増えています。
- 当社は、検査に対する消耗品の製造であるためサイバーセキュリティの対策の必要は特にないと思われます。
- 単体の医療機器プログラムではなく、ソフトウェアを用いて外部アクセス可能な機器はすべて対策が必要であることを、周知するうえで、このアンケートは有用であったと思います。
- 体制や規定がないことに対する、3年以内での対応はない、しないという回答は、現時点では整備時期が明確に答えられない、分かっていない、判断・決定していない、という意味。
- 申し訳御座いませんが、現時点では、サイバーセキュリティを考えなければならない製品がありませんので、大変、答え難い質問が散見されました。尚、取引先でのサイバーセキュリティの件は、今後の課題かと思いました。気づかせて頂き、有難う御座いました。
- 使用しているパソコンはウィルス対策はしているが、サイバーセキュリティに対する知識が不足している為、どのような対策が必要かわからない状態です。
- 現段階であまり実感が無く対応が遅れています。
- 具体的な対策事例等を提示頂けると参考になり、自社に取り込みやすいかもしれない。
- 具体的な対応を考える部門・担当者がいないのと、対応法の想定が不明なため、実際にどのように動けばいいのか検討に至っていない。
- 機器の販売ができていないため、並行してサイバーセキュリティに対する知見を収集中です。
- 一部の大手企業を除いたほぼすべての企業（具体的には従業員数が1000人未満、資本金が10億円未満等の企業）で、サイバーセキュリティ対応が求められる製品を製造販売しているが、対応できる人材が十分に確保できていない企業や、個人診療所・中小規模の病院等でネット環境が十分に整備されていなかったり、専門スタッフが配置できない医療機関がサイバーリスクの危険が大きい。そういった企業や医療機関向けに、対応マニュアル、指針（具体的なポリシーの記載事例や考え方等）、リーフレット等が示せるように行政、業界、医療機関が連携して確実に対応できるような体制（システム）を構築していただきたいと思います。
- メーカ側として課題意識はあるものの、積極的に対応できているとは言えない状況です。行政主導で方針、指針を示していただけると動きやすくなると思われます。
- まだ、取組み姿勢は弱いのですが、抽象でも取組みやすい指針のようなものがあれば、参考に出来ると考えています。

79

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。
## 【その他のご意見・ご要望②】

【全回答】

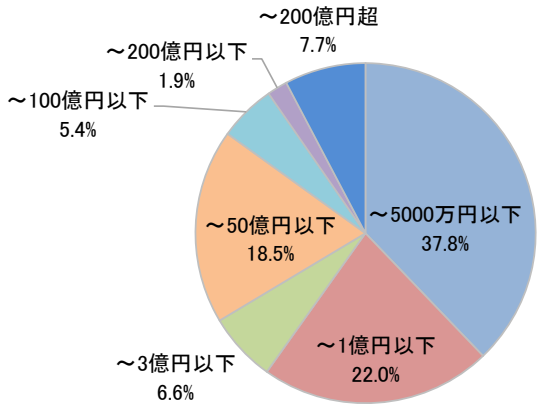
- ネットワークにつなげない製品はサイバーセキュリティーに関係ないと思っていますが、違うのでしょうか。また、製品内のマイコンの組込プログラムも同じ考えですが、どの部分でサイバーセキュリティーが必要なのか分かりません。
- セキュリティ診断に関しては、現状外部サービス利用して行っています。今後、どのような組織体制を構築し、取り組みをしていくかは現在検討段階です。
- サイバー犯罪者の罰則を厳しくして欲しい。
- サイバーセキュリティに求められる最低限の対策構築基準（ソフト及びハード面）の提示があると対応し易いと思います。
- サイバーセキュリティに関する規格(ISO,IEC)の制定、JIS化、規定化をして海外と歩調をあわせてほしい。
- サイバーセキュリティーに該当する製品の製造は現時点で行っていません。
- これまでの通知文書などから「医療機関側が行うこと」という認識がある。そもそも誰が何をどうするのか、明確になっているのだろうか？何から手をつけるべきか要領を得ないのは弊社だけか？
- ウィルス対策ソフト等は、有償のものから無償のものまであるが、ソフト毎の信頼性について何かしらの根拠となるもの（例えば規格や認証など）を示していただけると、ソフトの選定時に参考とさせていただきます。
- アンケート対象の医療機器サイバーセキュリティのほか、医療情報システムやクラウド医療機器プログラムに関係する「3省3ガイドライン」対応も難しいのでわかりやすい実例に即した具体的なガイダンスが提供されることを希望します。
- Windows OSレベルでのセキュリティー対策は業者に頼んで対応しているが、どこまでの対応が求めているのか分からない。
- ・本年製造販売業を取得し、単体プログラムの製品を開発中です。現在は臨床試験中であり、実際に製造販売している製品が無いため、首記のような回答となっております。
- ・ホワイトハッカーの養成は喫緊の課題 ・生命、健康に直結するようなアプリとそうでないアプリとレベルを分けて管理でしょうか。 ・Cyber Securityは医療機器のみで検討も必要と思いますが、自動車業界とか銀行業界とか他業界との協調も必要と思われます。
- ・サイバーセキュリティは避けて通ることの出来ないもので、どこまで対応すればよいかもなかなか判断が難しい。随時、適宜ホームページなどで情報をアップしていただけると対応の一助となるので、よろしくお願いします。
- （本調査回答に関する補足）当社で業務に使用するIT機器は、親会社のセキュリティシステムの下で管理されており、サイバーセキュリティへの対策もとられています。本調査では、当社単独での対応はできていないとの観点から回答を行っておりますので、その点をご理解ください。

# 調査結果【対象品目あり編】

【対象品目あり】

空白ページ

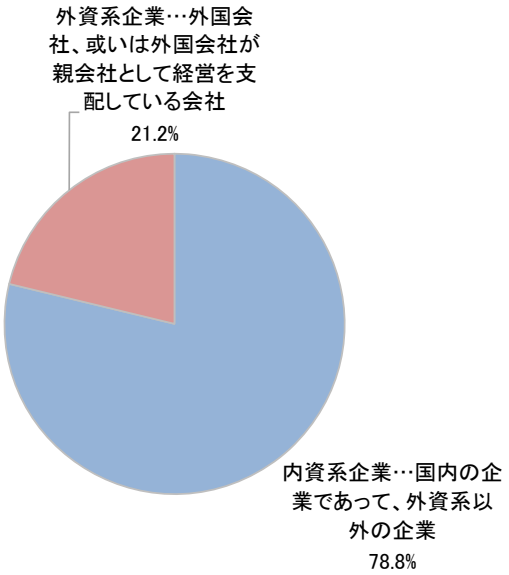
[Q2]資本金についてお答えください。
(n=259)



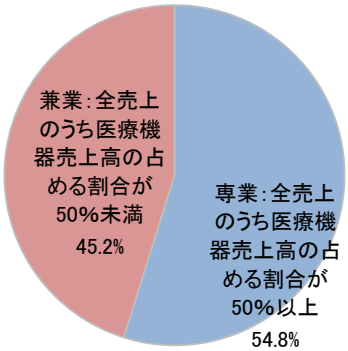





[Q3]資本上の区分についてお答えください。
(n=259)



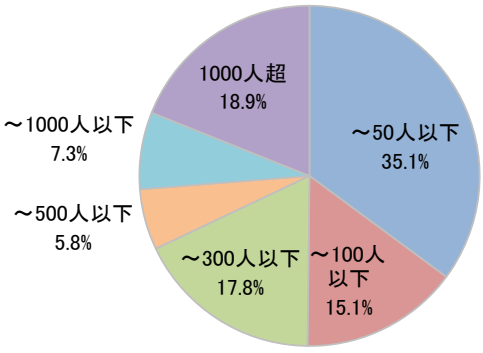
[Q4]専業・兼業の区分についてお答えください。
(n=259)




5



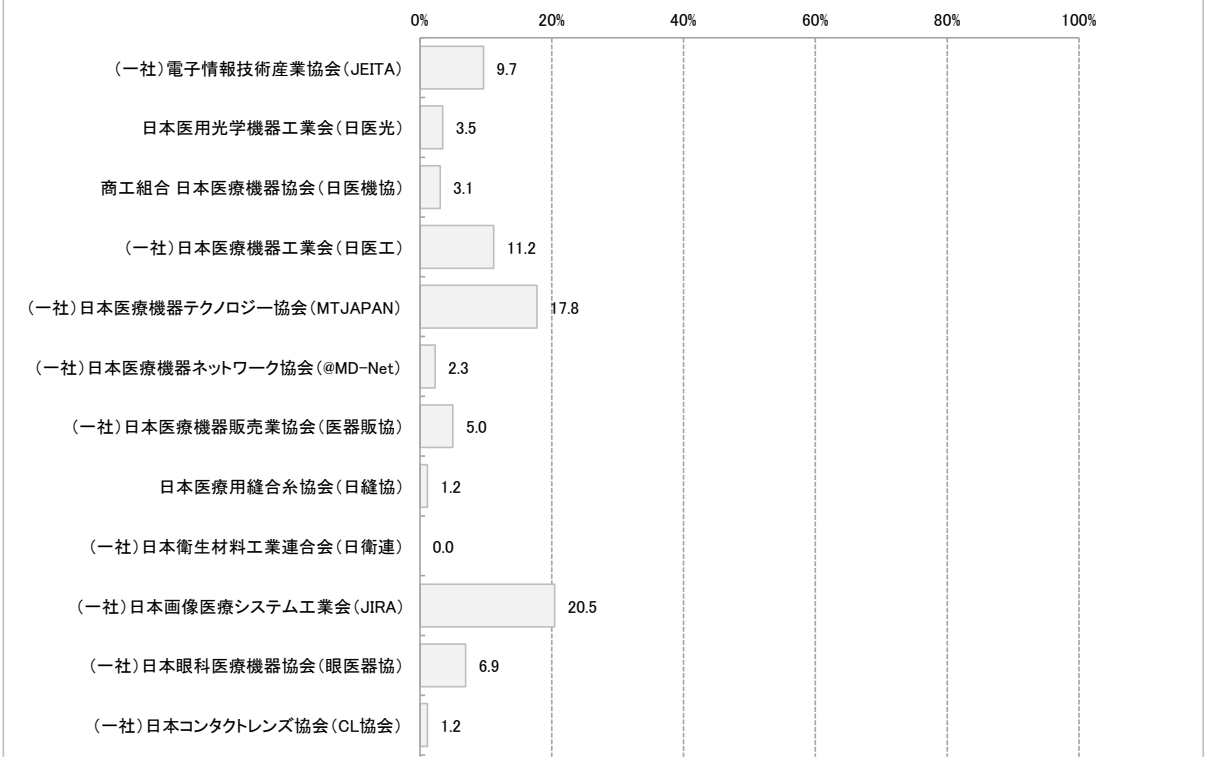
[Q5]全社員数についてお答えください。
(n=259)






6

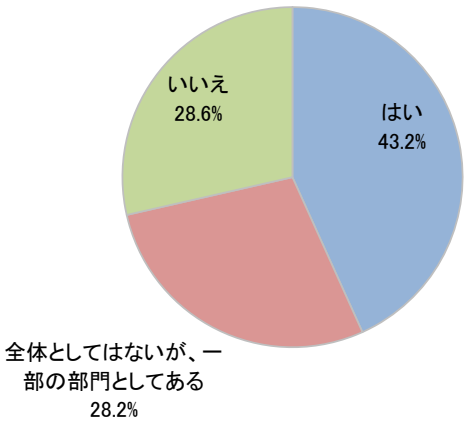
[Q6]主な加盟団体についてお答えください。
(n=259)






【対象品目あり】

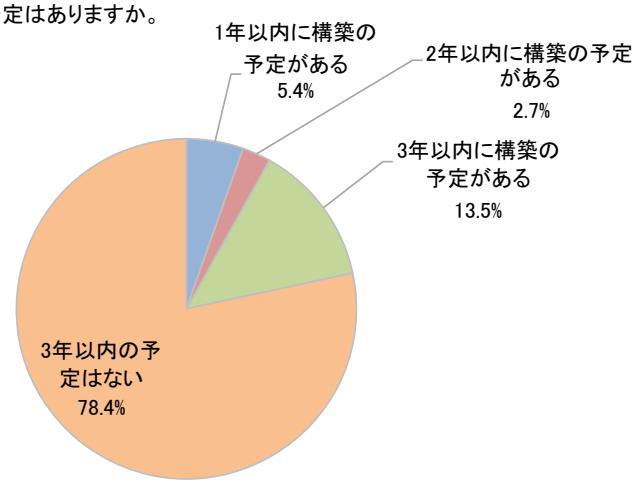
[Q7]会社全体のサイバーセキュリティ対応を行う組織体制がありますか。
(n=259)



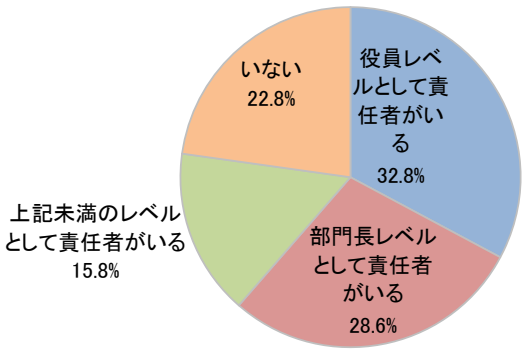





[Q8]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=74)



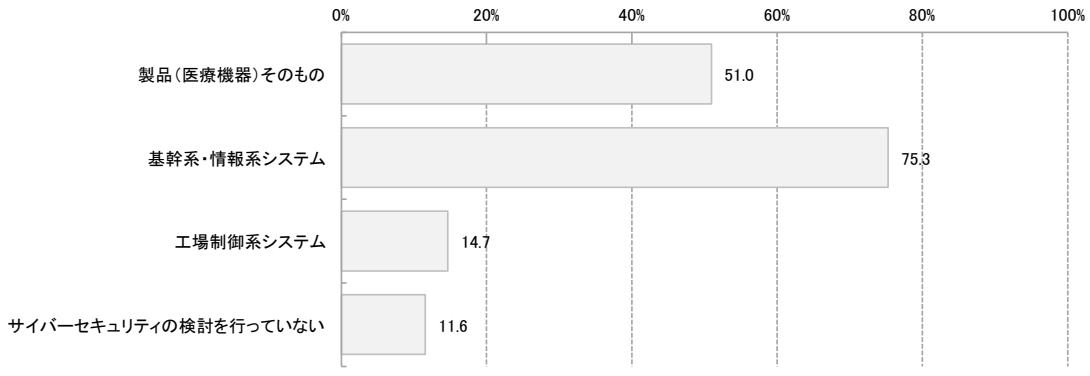
[Q9]サイバーセキュリティに関して統括する立場の責任者はいますか。
(n=259)



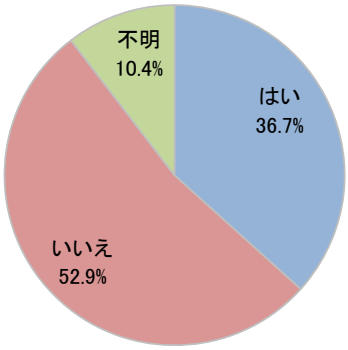





[Q10]サイバーセキュリティの検討にあたって、次のいずれの範囲を対象としていますか。
(n=259)



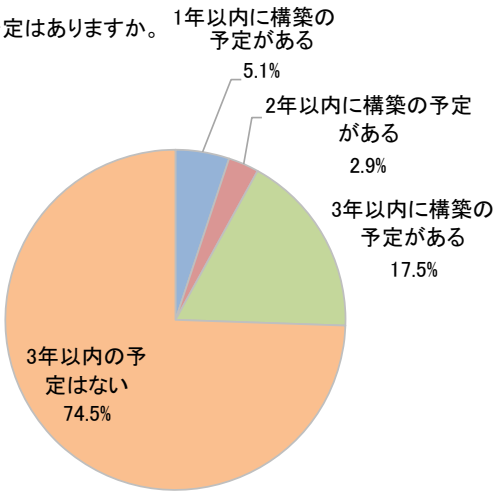
[Q11]コンピュータセキュリティにかかるインシデントに対処するための組織となるCSIRT（Computer Security Incident Response Team）がありますか。
(n=259)



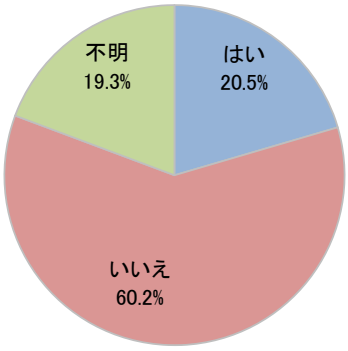





[Q12]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=137)



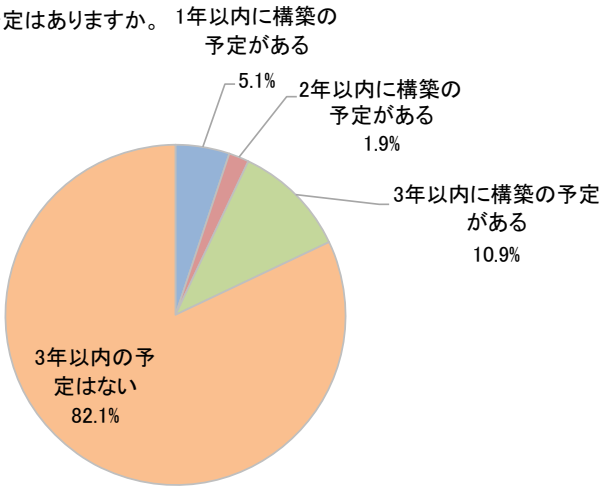
[Q13]組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能としてPSIRT（Product Security Incident Response Team）がありますか。
(n=259)



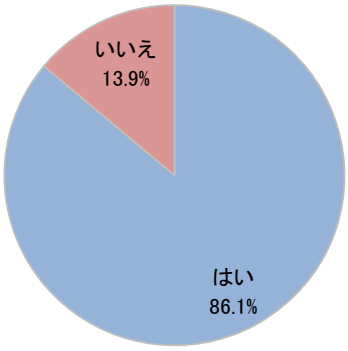





[Q14]「いいえ」の場合、3年以内に構築の予定はありますか。
(n=156)



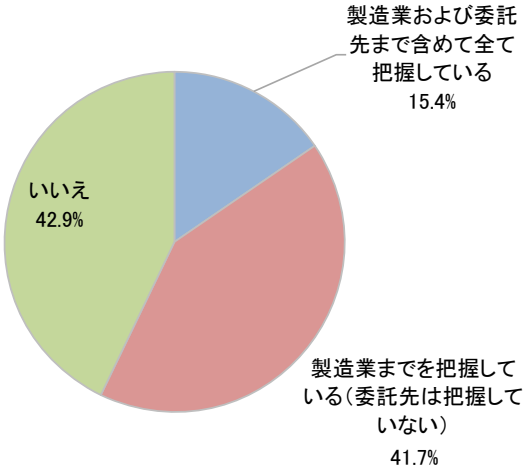
[Q15]QMS対象業務（設計、製造、アウトソーシング先等、関係する全てを含む）で使用しているIT機器について、ウイルス対策やセキュリティ対策に関する対応は行っていますか。
（n=259）



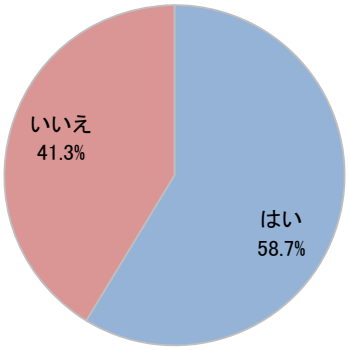





[Q16]製造販売業としてのQMS対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。
（n=259）



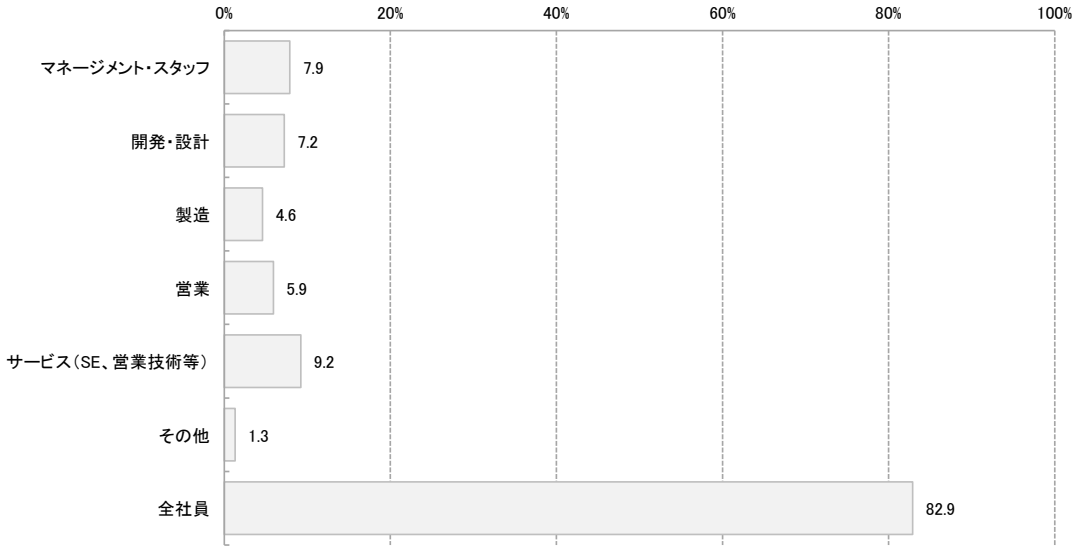
[Q17]サイバーセキュリティに関する社員教育を行っていますか。
(n=259)



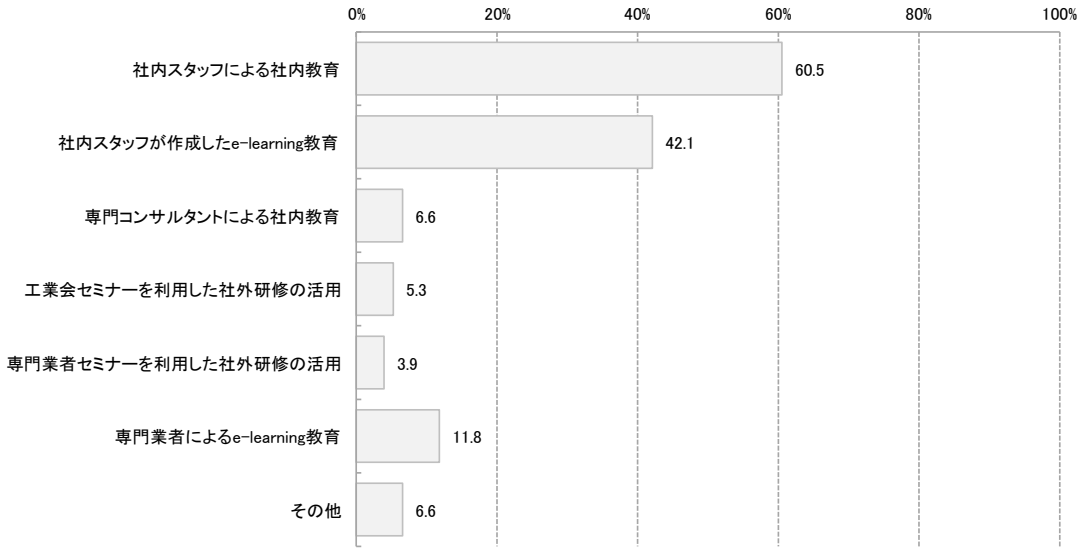

19

【対象品目あり】

[Q18]「はい」の場合は、誰に対して教育を行っていますか。
(n=152)



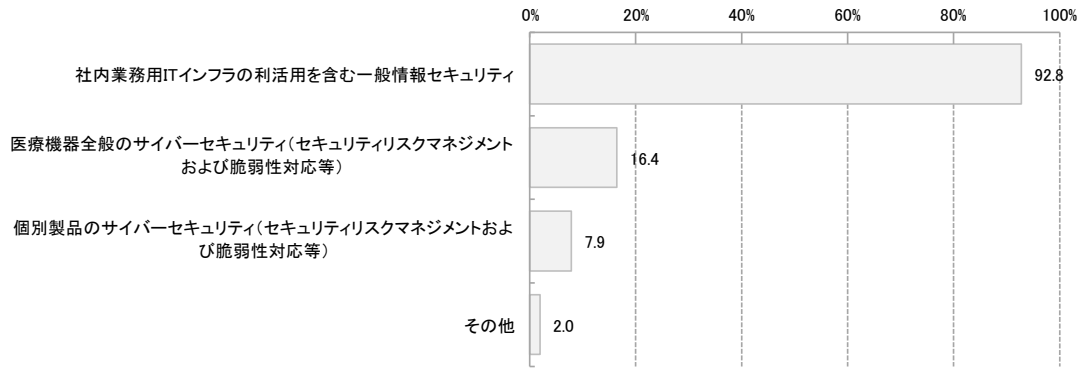
[Q19]「はい」の場合は、どのように行っていますか。
(n=152)



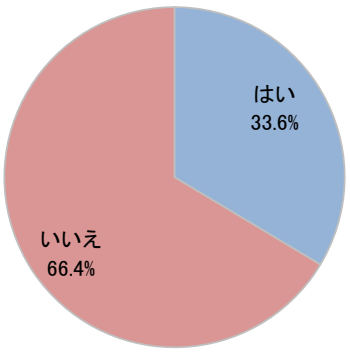





[Q20]「はい」の場合は、どのような内容の教育を行っていますか。
(n=152)



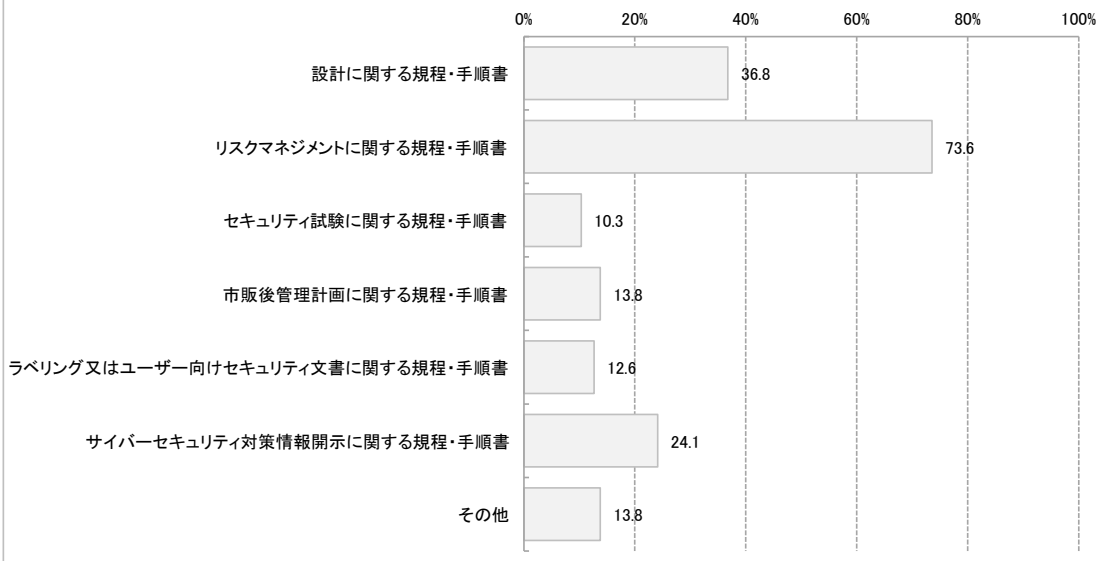
[Q21]サイバーセキュリティに対応するため追加・修正した規程・手順書などがありますか。
(n=259)



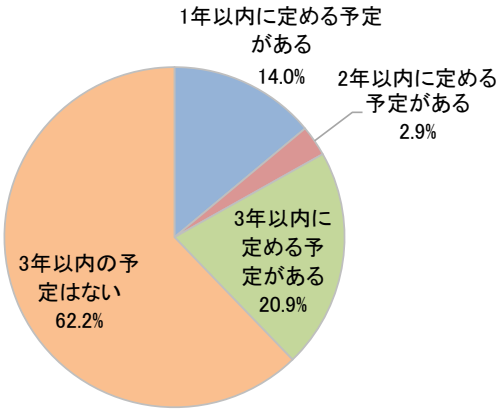





[Q22]「はい」の場合、どのような内容の規定・手順書を追加・修正しましたか。
(n=87)



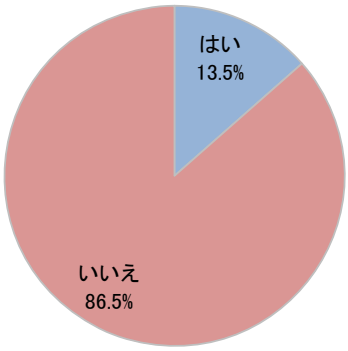
[Q23]「いいえ」の場合、3年以内に追加・修正する予定はありますか。
(n=172)



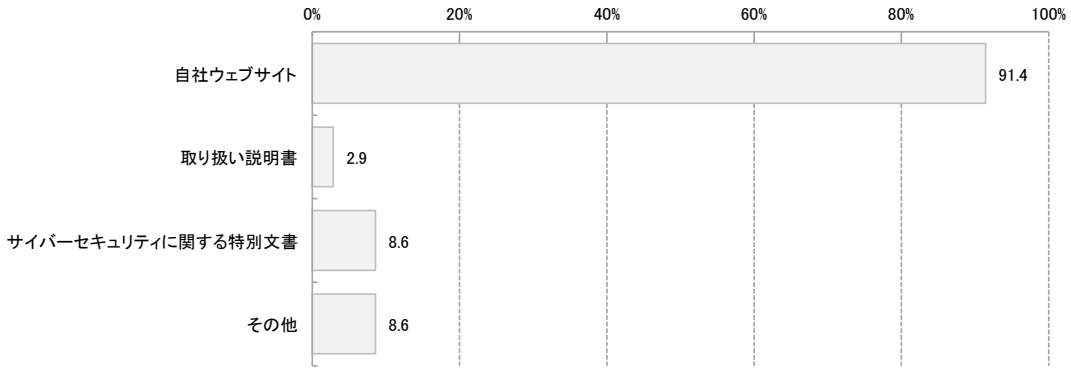





[Q24]サイバーセキュリティに関するポリシーを社外に公開していますか。
(n=259)



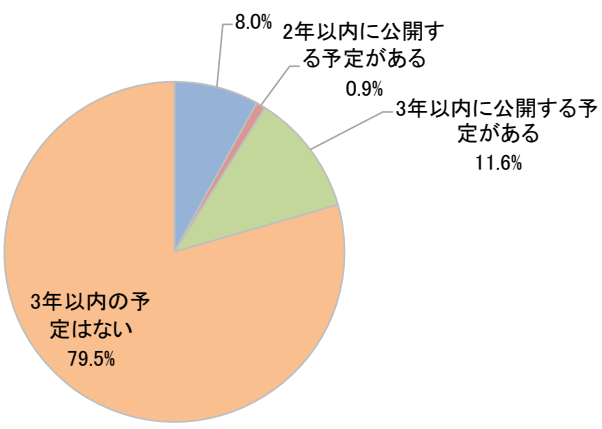
[Q25]「はい」の場合は、どのような方法で公開していますか。
(n=35)



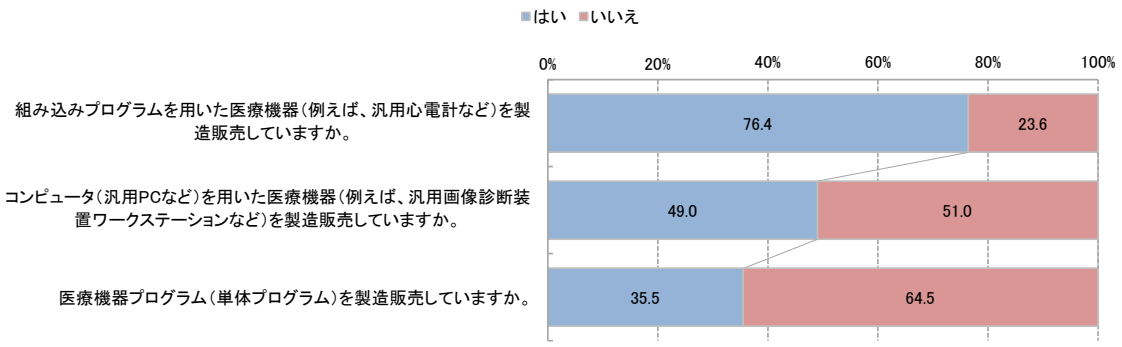





[Q26]「いいえ」の場合、3年以内に公開の予定はありますか。
(n=224)



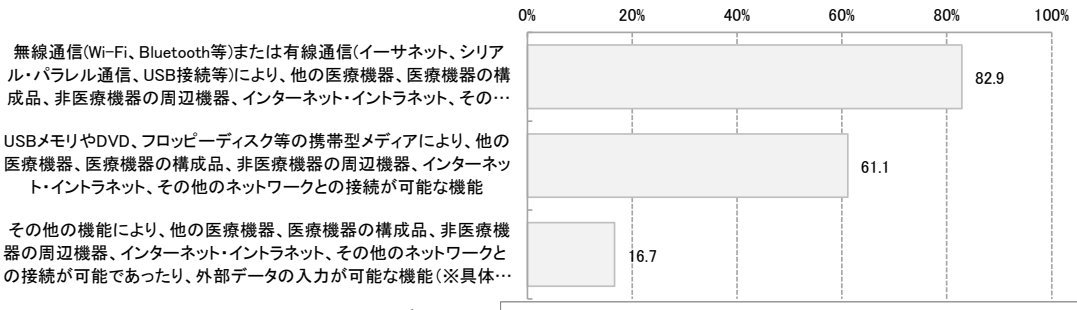
[Q27]製造販売している医療機器についてお伺いします。





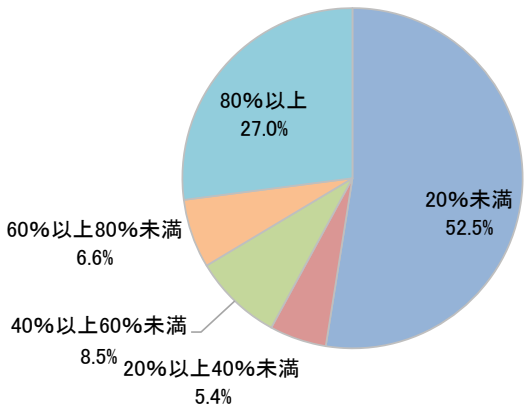

【対象品目あり】

[Q28]それらは、次の機能を有しますか。
(n=234)




- **通信機能は無し**
- **対象外**
- 他の医療機器に画像データを送信
- 他の医療機器、非医療機器の周辺機器との通信
- 測定結果と依頼情報のやり取り
- **組み込みプログラムを有しているが、これらの機能は有していない。（未記入だとえら一が出たため記載しました）**
- 専用機器による接続
- 製造又はサービスの際に、PCを接続することがある。
- 検査（輸血）システムからのオーダー情報
- **機能なし**
- **該当なし（ネットワーク接続等の機能を持たない単なるプログラム内蔵の医療機器のため）**
- **外部データを入力する手段無し**
- リレー接点
- **マイコンの組込プログラムの書換用のコネクタが基板に実装有り。但し、分解しないと接続できない。**
- マイコン
- **プログラムを有するが、接続機能は無い。**
- **ネットワーク接続及び外部データの入力不可**
- **なし**
- トリガー信号、映像信号
- シリアル通信
- **いずれの機能も有しない**
- イーサネットによるネットワーク接続により、外部ホストコンピュータから検査依頼を入力として受付け、医療機器側からは測定結果を出力する
- web上からソフトウェアをダウンロードする
- webブラウザーを介して医療機器実行サイトにLog inし情報を入力する。
- USBメモリーにてデータ入力
- USB バーコードリーダー
- USB
- SDカード
- RS232Cシリアル通信
- RS-232C
- RS232C
- RC232Cポートから他の医療機器及びPCとの接続が可能
- PCより当該機器ソフトの書き換えを行う
- LAN(イーサーネット)
- Hub
- HL-7
- 通信
- COM規格による通信

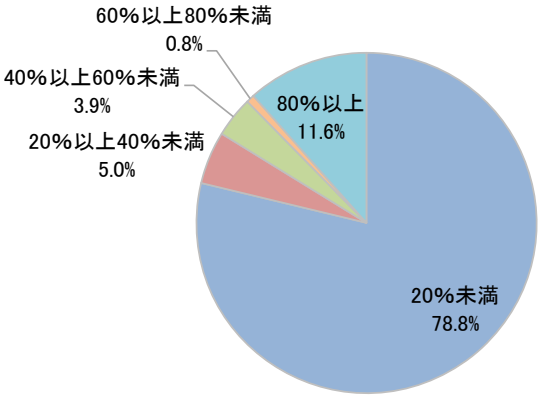
[Q29]貴社の全製品（医療機器）のうち、（現在の対応状況の如何を問わず）サイバーセキュリティ対応を検討しなければならない医療機器の割合はおおよそどの程度ですか。
（n=259）





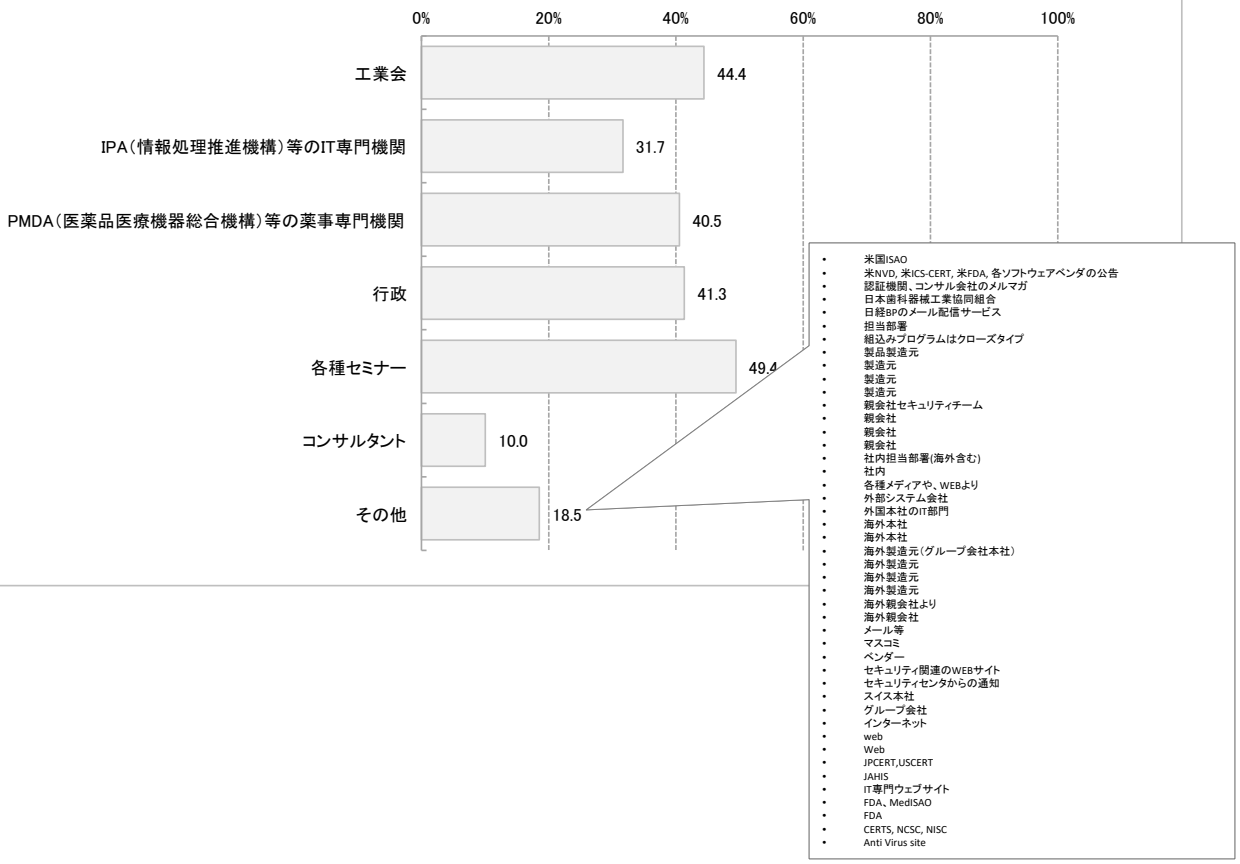



[Q30]前問（Q29）のサイバーセキュリティ対応を検討しなければならない医療機器のうち、既に市販済みの製品であって、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器であり、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できないと考えられる医療機器（Legacy Medical Device）の割合はおおよそどの程度ですか。
（n=259）



【対象品目あり】

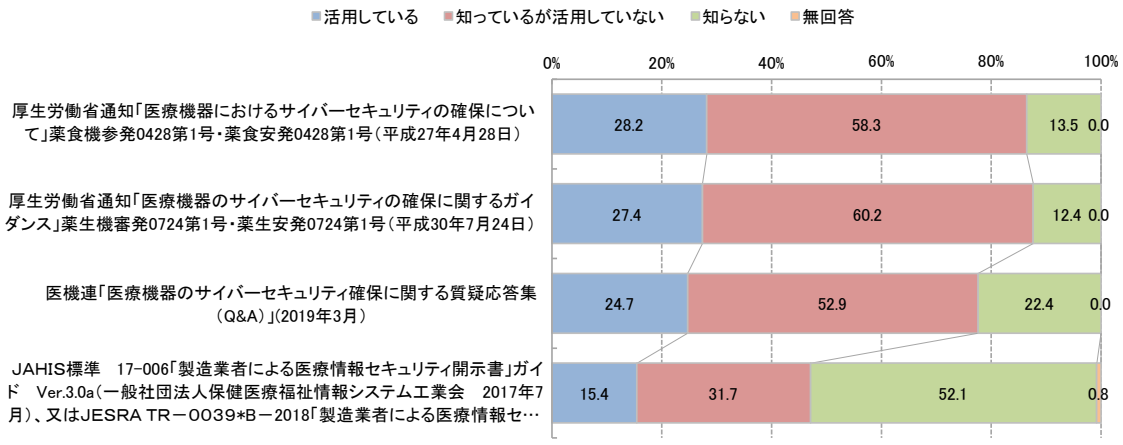
[Q31]サイバーセキュリティに関する情報をどこから入手していますか。
(n=259)




33

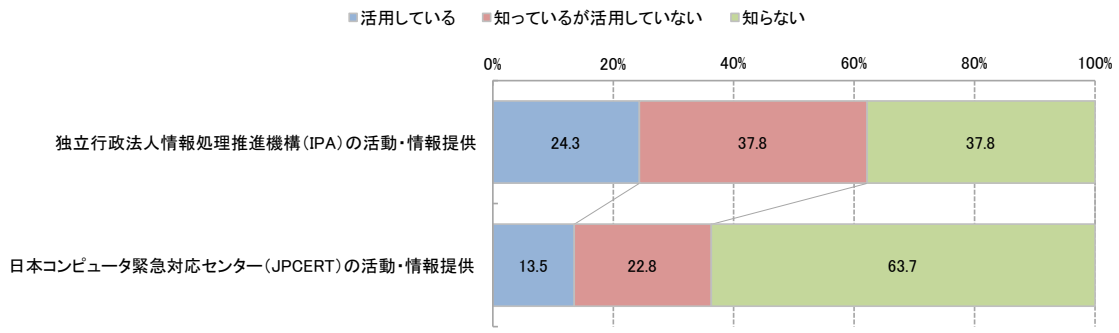
【対象品目あり】

[Q32]国内の通知、ガイドライン、ガイダンス等を把握・活用していますか。



【対象品目あり】

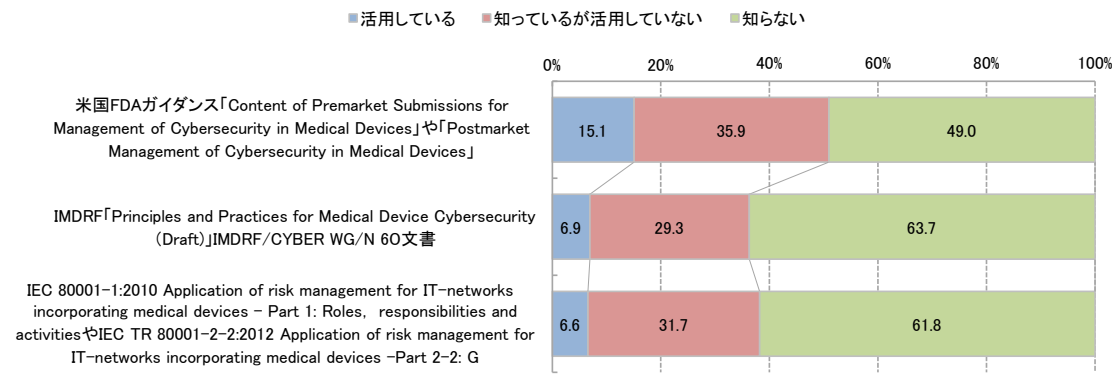
[Q33]サイバーセキュリティ関連組織・活動を把握・活用していますか。



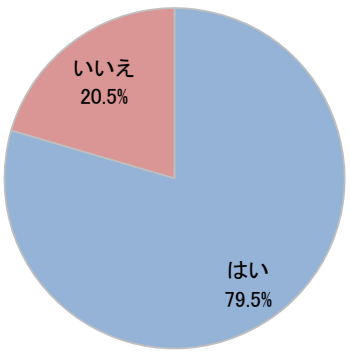

35

【対象品目あり】

[Q34]海外のガイダンスやガイドライン等を把握・活用していますか。



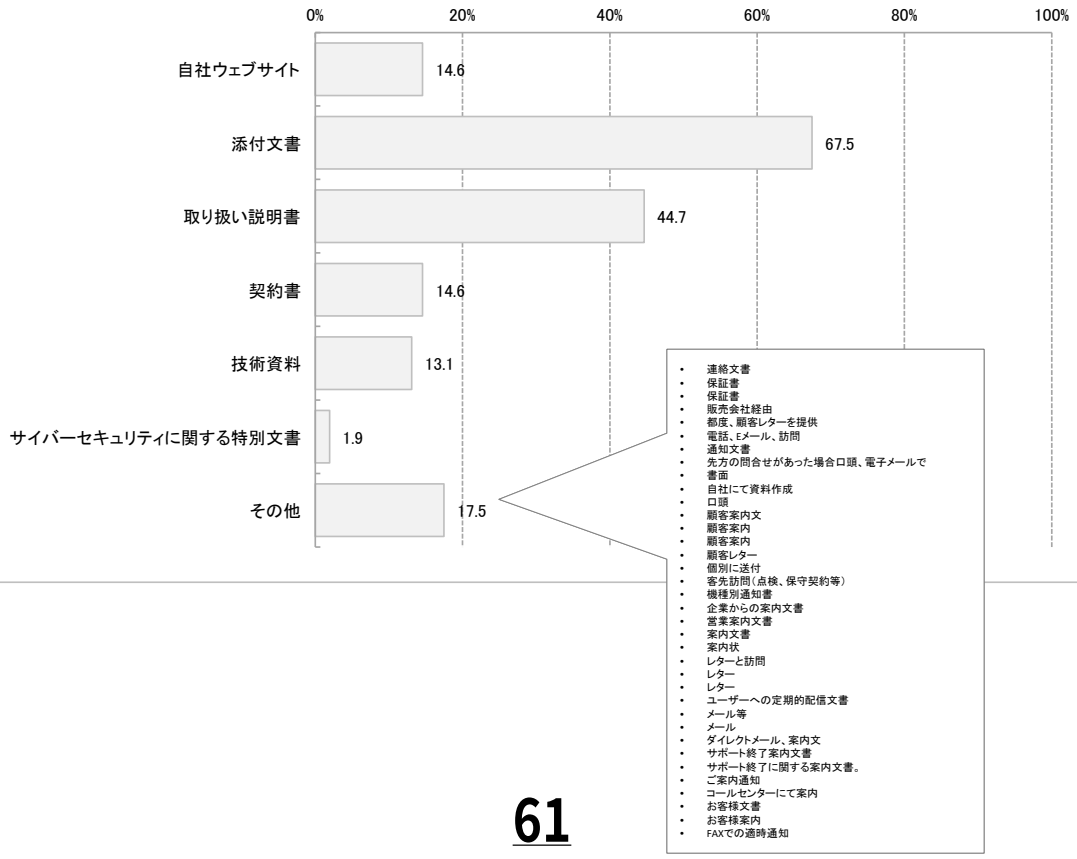
[Q35]貴社の製品（医療機器）の寿命や使用期限、企業からのサポート終了時期について規定し、ユーザーに伝えていますか。
（n=259）



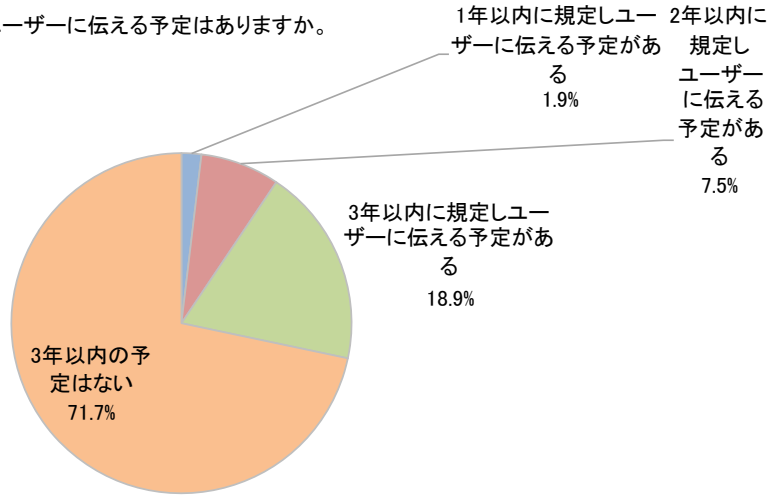





[Q36]「はい」の場合、ユーザーにはどのような媒体で伝えていますか。
（n=206）



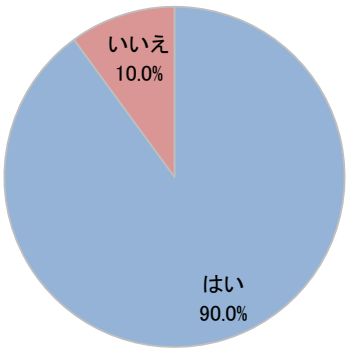
[Q37]「いいえ」の場合、3年以内に規定しユーザーに伝える予定はありますか。
(n=53)



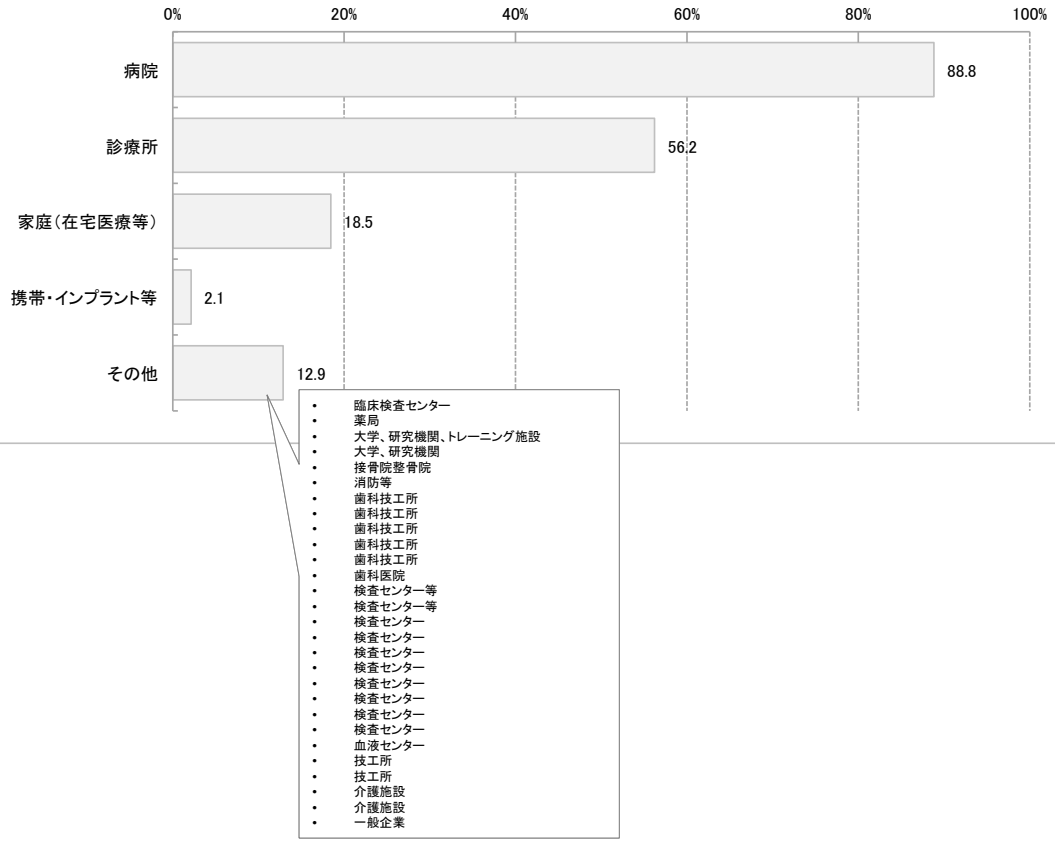





[Q38]サイバーリスクが懸念される医療機器について、製品(医療機器)が使用されている主な場所を把握していますか。
(n=259)



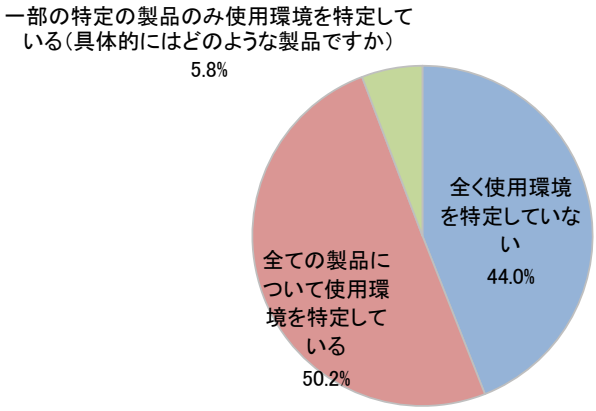
[Q39]「はい」の場合、具体的にはどのような場所ですか。
(n=233)





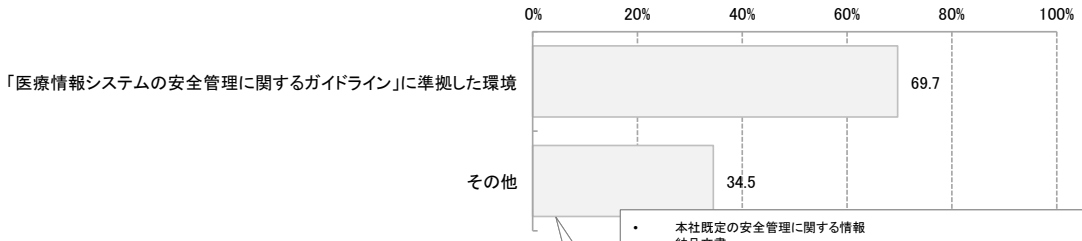



[Q40]サイバーリスクが懸念される医療機器について、製品(医療機器)の使用環境を特定していますか。
(n=259)



【対象品目あり】

[Q41]「全て」、「一部」の場合、どのように特定していますか。
(n=145)

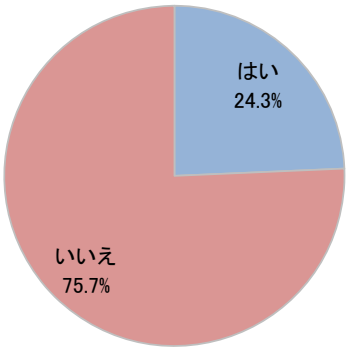



- 本社既定の安全管理に関する情報
- 納品文書
- 添付文書や取扱説明書で使用環境を特定。
- 添付文書/取扱説明書/現場確認
- 添付文書、取扱説明書等で使用方法を規定
- 添付文書、取扱説明書、社内基準
- 添付文書
- 送信のみである
- 全てCDからのダウンロードである
- 設置場所が特定されている。
- 設置時に特定できる
- 設置管理医療機器であるため
- 設計開発を行った製造元の規定
- 製造元のリスク分析
- 周辺温度、湿度
- 取説、添付文書、仕様書、リスクマネジメント等
- 社内設置手順に基づいた状況かどうか
- 社内で規定した環境
- 自主規定
- 自主基準
- 自社判断
- 自社設定基準
- 自社基準
- 使用エリアのみを特定
- 顧客による報告
- 顧客(医療機関)の要件に準拠した環境
- 各機関設定のセキュリティーポリシー
- 海外親会社から提供されるマニュアル
- 一般的な記載（水・埃に注意など）
- リスクマネジメント
- ほとんどが設置管理機器であることから、及び営業の設置情報により。
- セキュリティの確保されていない環境に接続しない事等を指示。
- セキュリティの確保された病院内のネットワークに接続して使用することと特定している。
- インターネットに接続させない。
- PC動作環境
- ISMSの構築
- IEC60601-1, FDA Guidance Postmarket Management of Cybersecurity in Medical Devices
- AAMI TIR57:2016

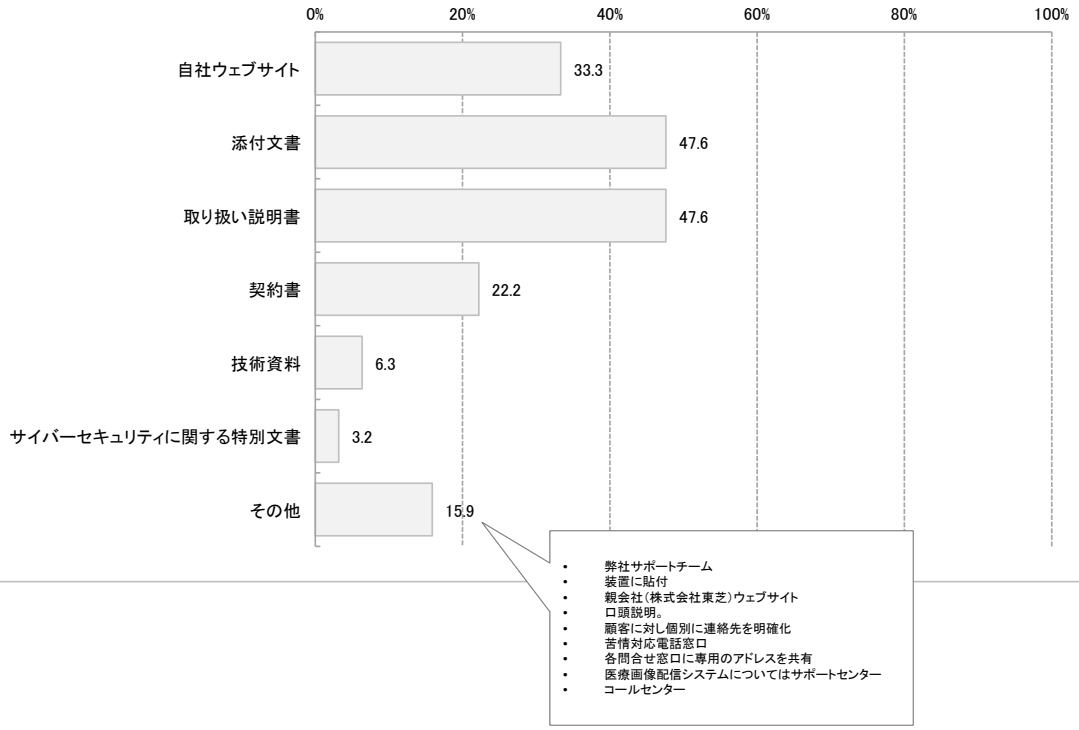


【対象品目あり】

[Q42]サイバーセキュリティに関する問い合わせ先を明確にしていますか。
(n=259)



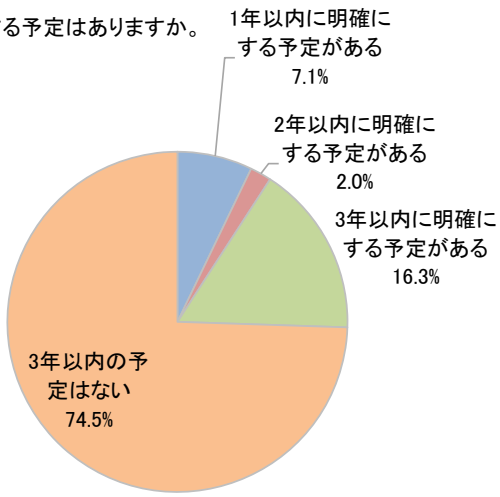
[Q43]「はい」の場合は、どのような方法で明確にしていますか。
(n=63)



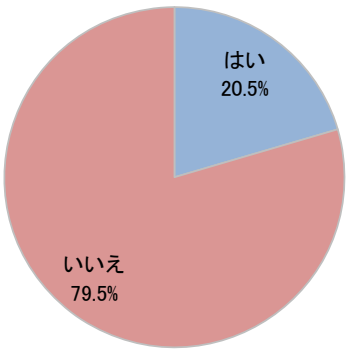





[Q44]「いいえ」の場合、3年以内に明確にする予定はありますか。
(n=196)



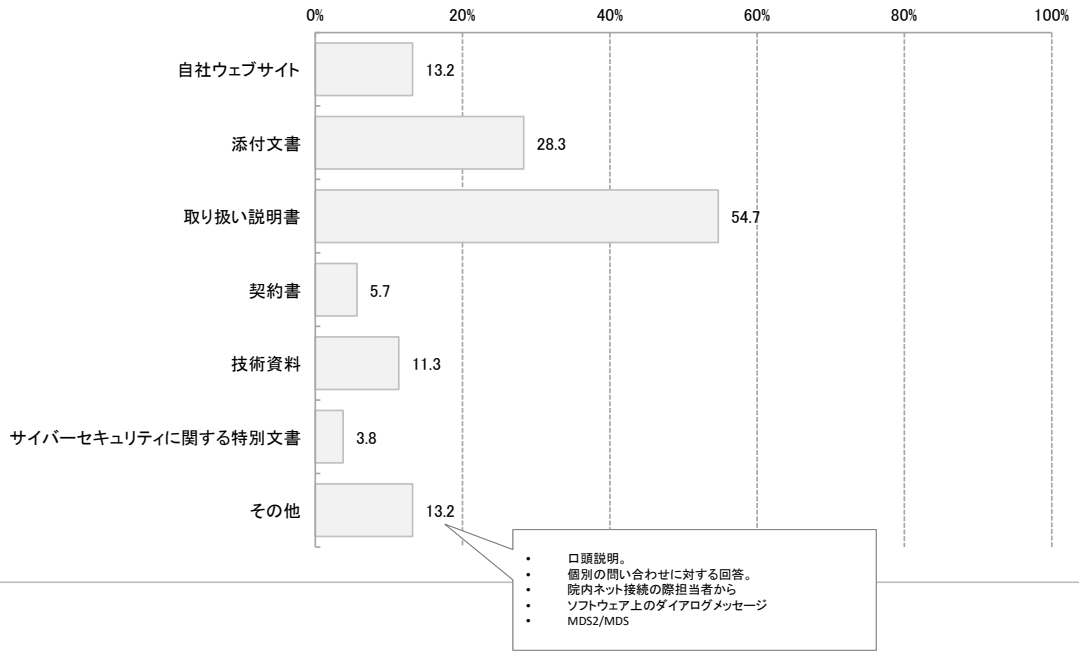
[Q45]製造販売時におけるサイバーセキュリティに関する情報を使用者に対して提供していますか。
(n=259)



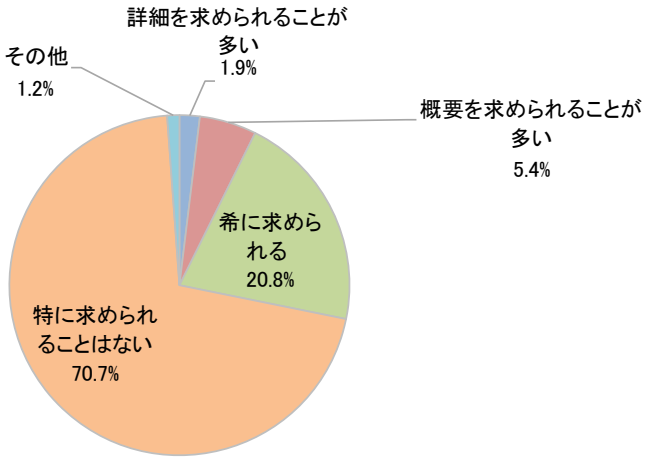





[Q46]「はい」の場合、どのような方法で提供していますか。
(n=53)



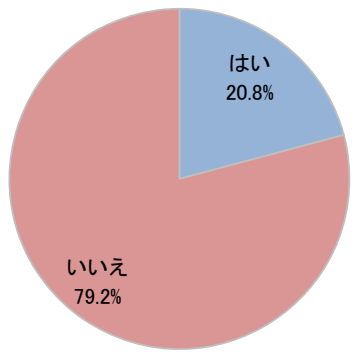
[Q47]売買の引合いや契約等の際に、医療機関等からサイバーセキュリティに関する情報提供を求められますか。
(n=259)



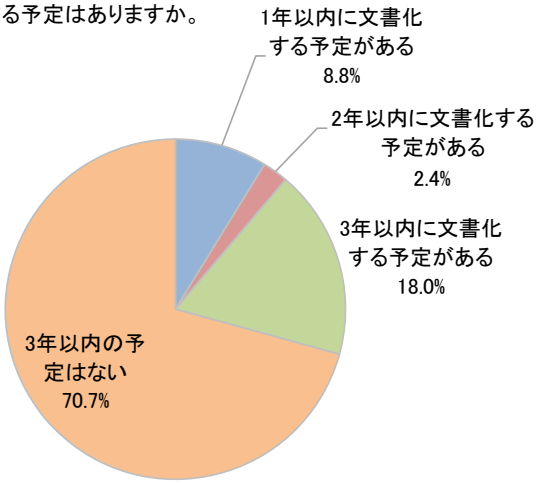





[Q48]サイバーセキュリティに関するインシデント発生時の国内届け出先や手順などを文書化していますか。
(n=259)



[Q49]「いいえ」の場合、3年以内に文書化する予定はありますか。
(n=205)



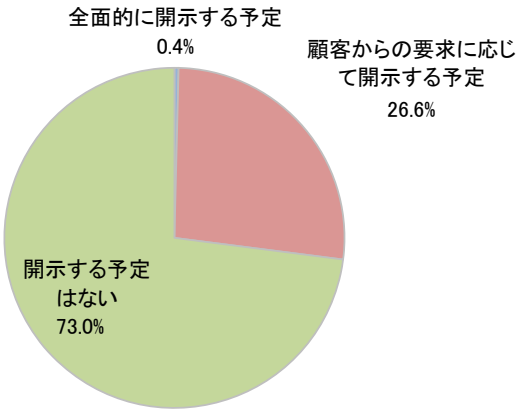




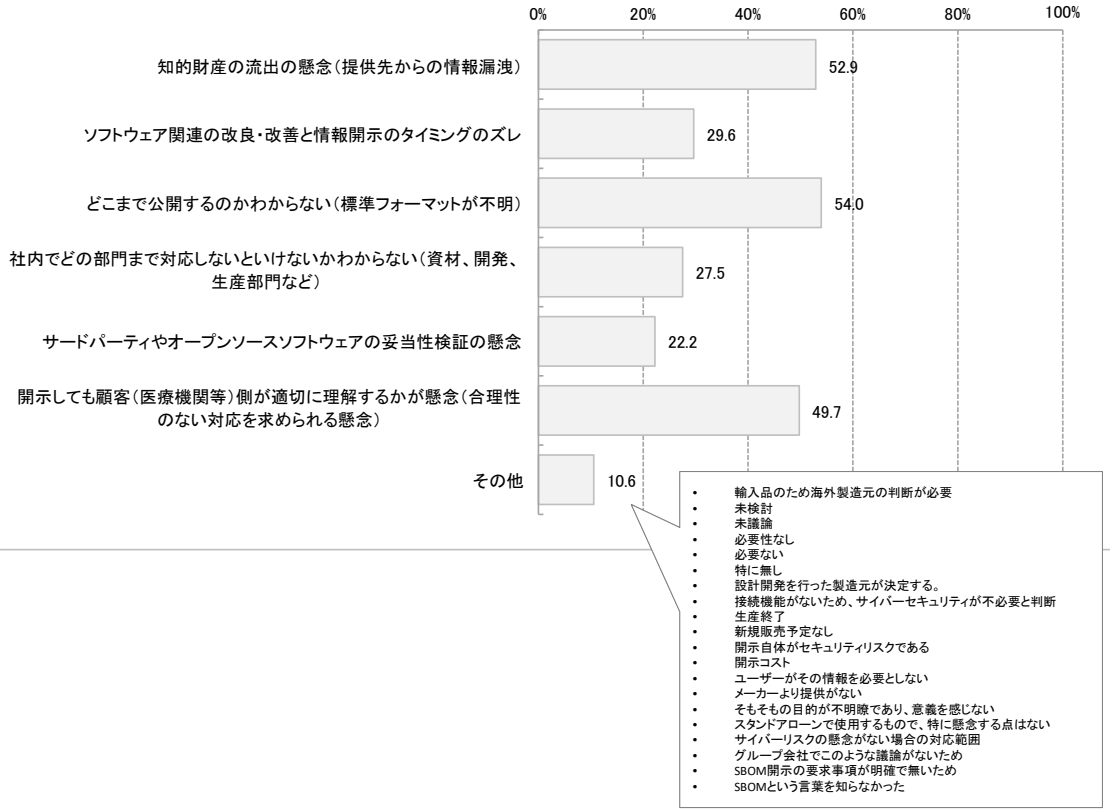

[Q50]貴社は、製品(医療機器)に関するソフトウェア部品表・構成表(SBOM)(注)を医療機関などの顧客に対し、開示することを今後3年以内に予定していますか。

(注) 医療機器に使用されているソフトウェアの透明性を確保するため、製造販売業者は医療機関などの顧客に対してソフトウェア部品表・構成表 (software Bill of Materials: SBOM) を提供して顧客が医療機器のライフサイクルに影響を与えるソフトウェアコンポーネントをよりよく理解できるようにすることが、今後のサイバーセキュリティ対策には必要であるとの議論が国際的になされています。

(n=259)



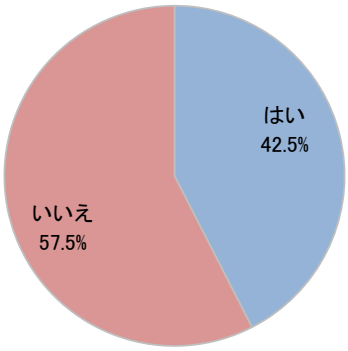
[Q51]「開示する予定はない」の場合、ソフトウェア部品表・構成表（SBOM）の開示には何か課題があると考えられますか。
（n=189）



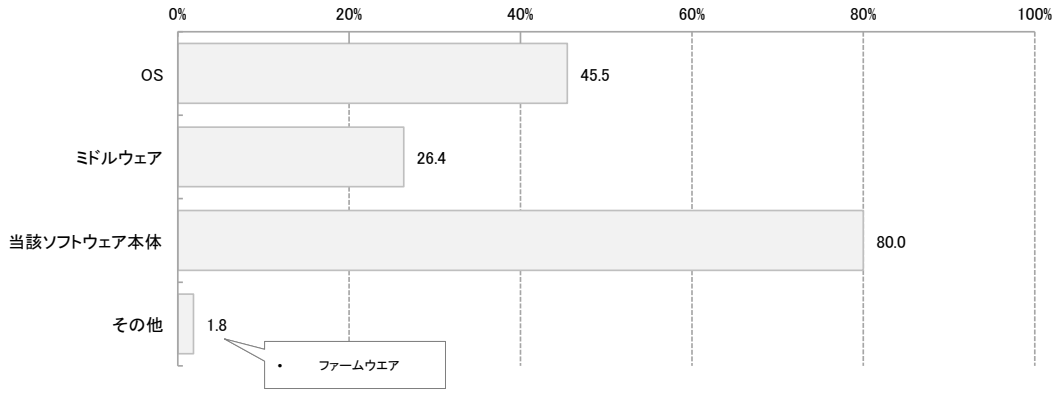





[Q52]市販後に脆弱性の改善に関係するプログラム（ソフトウェア）のアップデートを行っていますか。
（n=259）



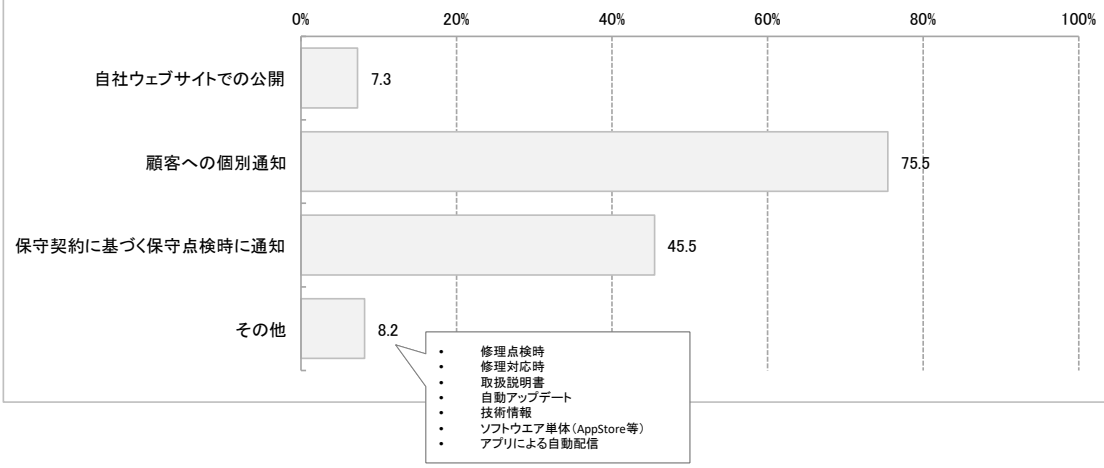
[Q53]「はい」の場合、アップデートする対象をお答えください。
(n=110)



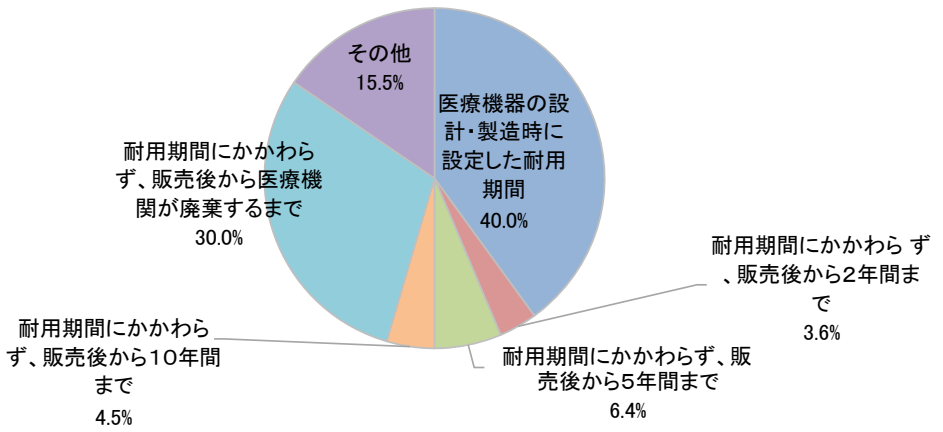





[Q54]「はい」の場合、アップデートに関する情報提供の方法をお答えください。
(n=110)



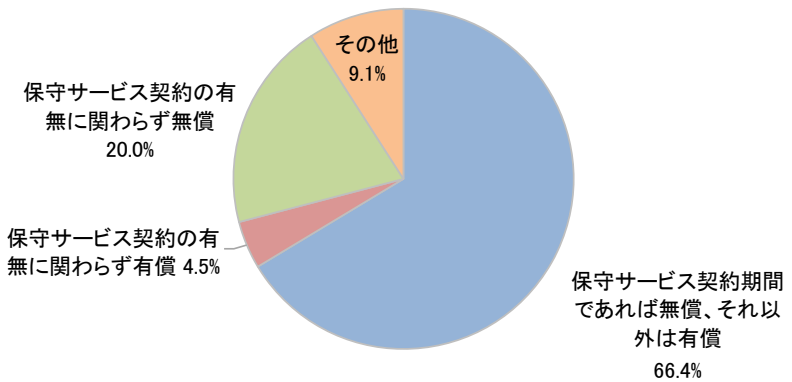
[Q55]「はい」の場合、アップデートを行う期間について、社内の考え方として最も一般的なものをお答えください。
(n=110)



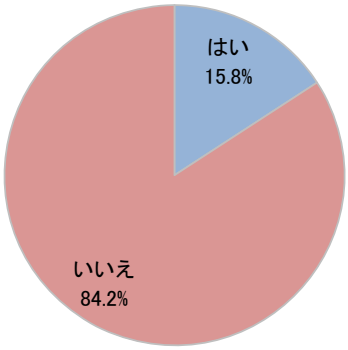





[Q56]「はい」の場合、アップデートを行う際の費用について、社内の考え方として最も一般的なものをお答えください。
(n=110)



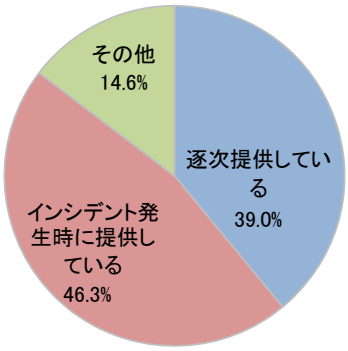
[Q57]市販後においてサイバーセキュリティに関する情報を使用者に対して提供していますか。
(n=259)



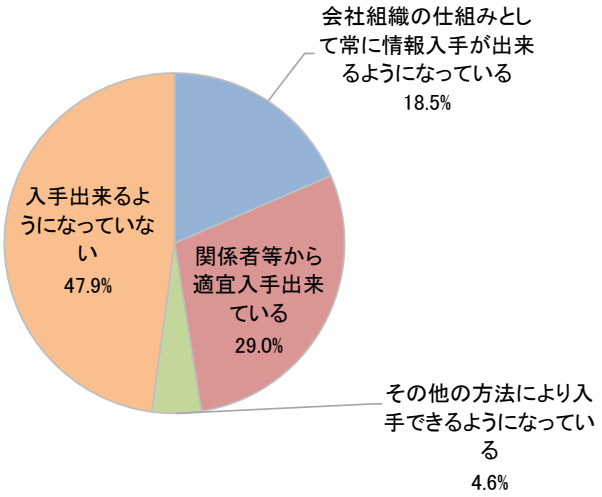





[Q58]「はい」の場合、どのタイミングで提供していますか。
(n=41)



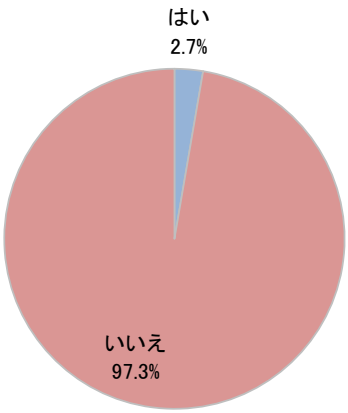
[Q59]使用現場（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。
（n=259）



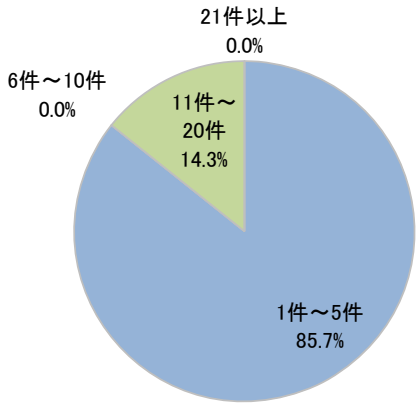





[Q60]貴社の製品（医療機器）に関連して、医療機関から報告を受けたサイバーセキュリティに関連したインシデント事例が3年以内にありましたか。
（n=259）



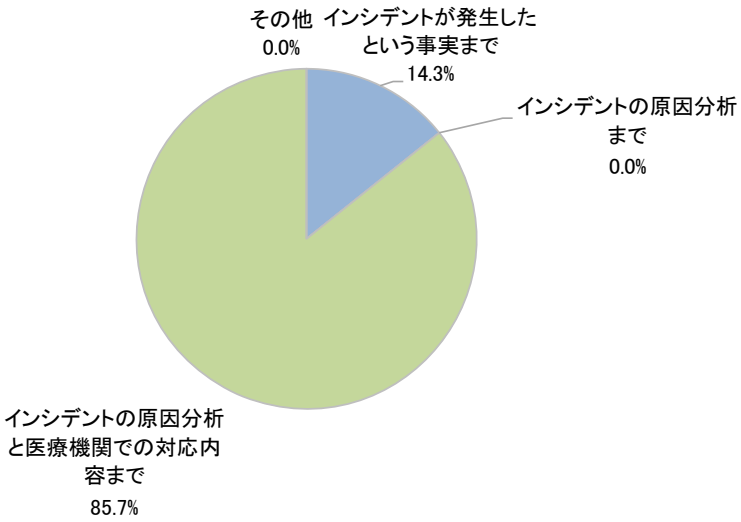
[Q61]「はい」の場合、どの程度の件数でしたか。
(n=7)

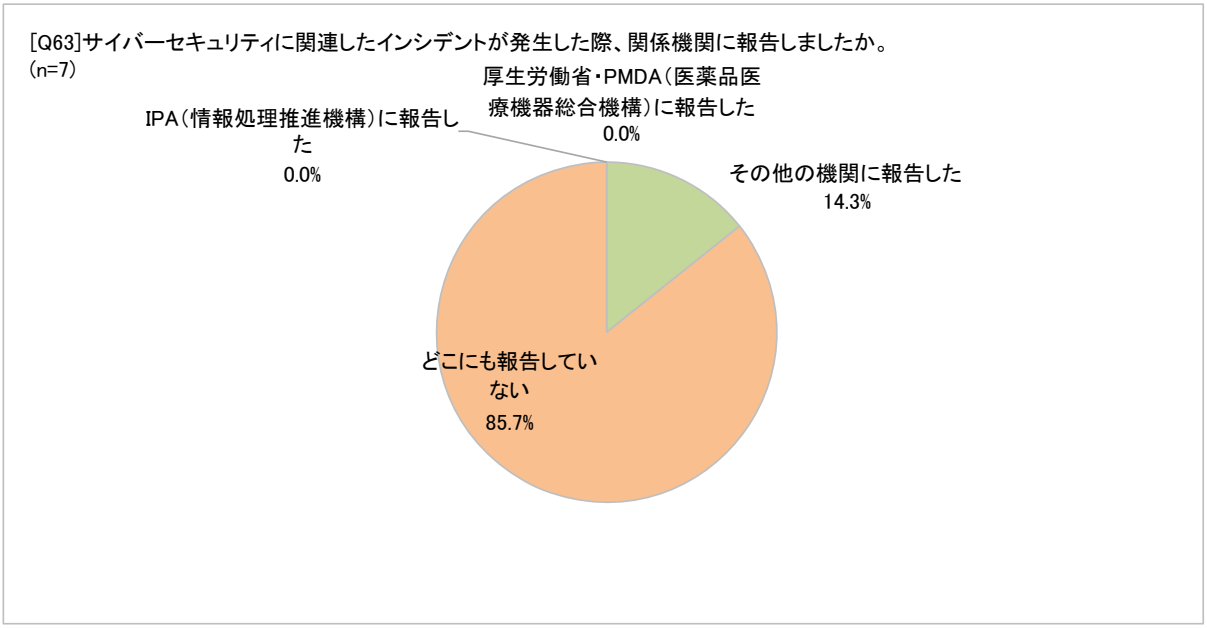







[Q62]「はい」の場合、どのレベルの情報まで情報を入手出来ていますか。
(n=7)





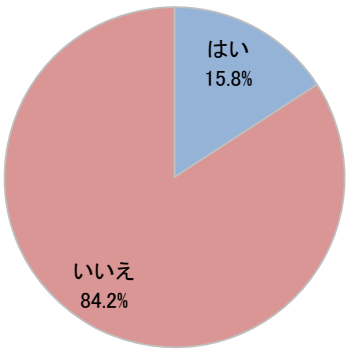





## [Q64]使用現場からの情報入手について、課題や要望等がありますか。

- 品質マニュアルのSOPにより情報が入手できる体制が構築されているので、課題はないと思います。
- 大手が販売する高リスク高額な医療用機器と、中小(零細)の販売する低リスクの家庭用機器を同列に扱わないで欲しい。
- 全国の医療機関において、院内ネットワークやソフトウェアの導入状況、院外往診や検診等で外部LANの使用状況等、使用場所ごとの主要な使用環境についての情報が欲しい。
- 施設によりセキュリティポリシーが異なるため、画一的な対応は不可能である。まずは施設のセキュリティ対策を明確に実施してほしい。また、他社のサイレントアップデート(特に電子カルテ)時の不具合が散見される。
- 使用者環境が千差万別であるため、自社製品に関連するインシデントかどうかを判断するのが難しく、どこまで医療機関に協力を依頼すべきかが課題。
- 使用現場から直接情報を入手する仕組みをどこまで構築するべきかの明確化が必要
- 使用環境での実際の運用が見えない
- 国内に米国のH-ISACのようなISAOが欲しい
- 現場の知識(専門用語など)レベルの問題がある。口頭での伝達が難しいケースがあり、書面でもらうか連絡先を聞き社内担当が直接やり取りするケースが多い。日々変化するセキュリティー環境の中で現場への落とし込みは非常に難しい。
- 技工所も医療情報システムの安全管理に関するガイドラインで指定されている医療機関等に該当するのか？
- 各機関でのセキュリティポリシー、規定を知る必要はあるが実施していない。
- 家庭向けの場合は、情報収集は困難である
- 医療機関において、何がサイバーセキュリティに関連したインシデントなのか理解されていないと思われるので、ほぼ情報収集ができないのではないかと考える。医療機関でもサイバーセキュリティに関する教育を充実れ瀬、適切な対応が行えるようにしてもらいたい。
- ユーザーがネット接続や他の機器(PC含む)に接続する医療機器ではない(スタンドアロン製品です)。
- メーカーが情報を収集するのではなく公的機関がまとめて収集をして欲しい
- どのような場合が情報入手対象になるのか設定が難しい。情報入手と対応のタイミングの設定をどうするか。
- どこまで聞いていいか分からない
- サイバーセキュリティに関する情報がすべて上がっているか判断できない。
- サイバーセキュリティに該当するかどうか不明なケースがある。
- インターネットのセキュリティ情報サイトからでないと、インシデント情報が入ってこない
- インシデント発生時の再現性が課題。特に自社以外の接続機器のセキュリティ対策状況が不明瞭のため、適切な対策を講じにくい。

[Q65]販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導等を行っていますか。
(n=259)

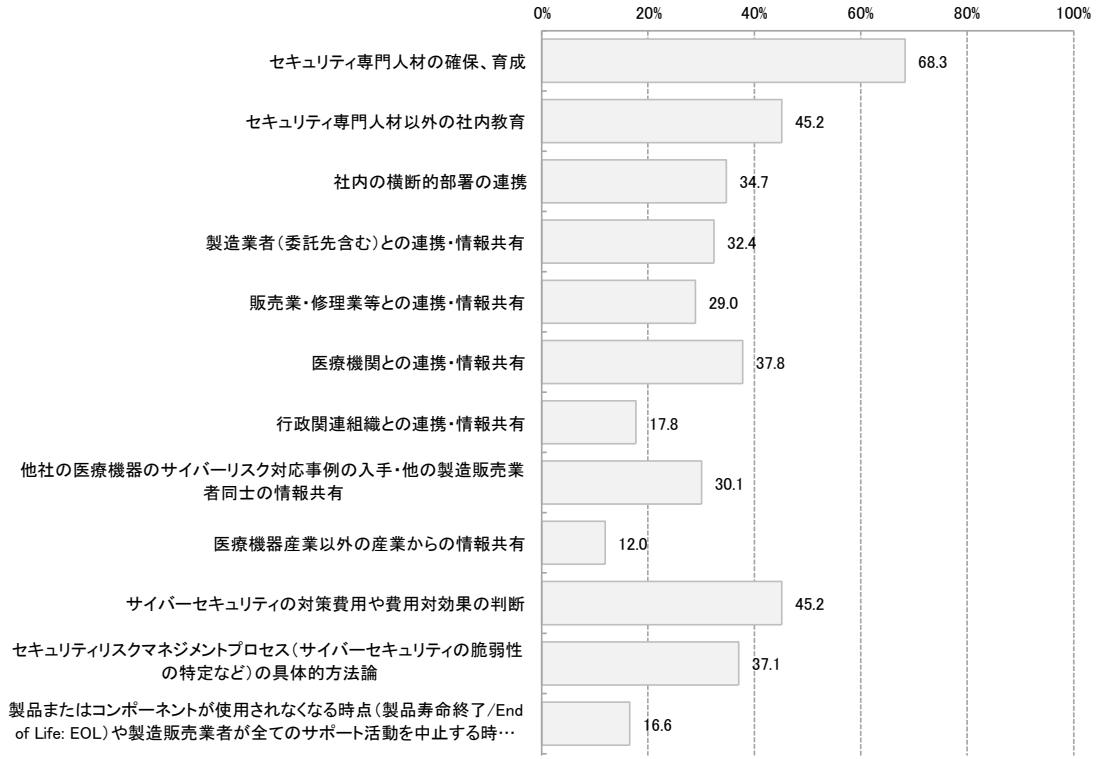






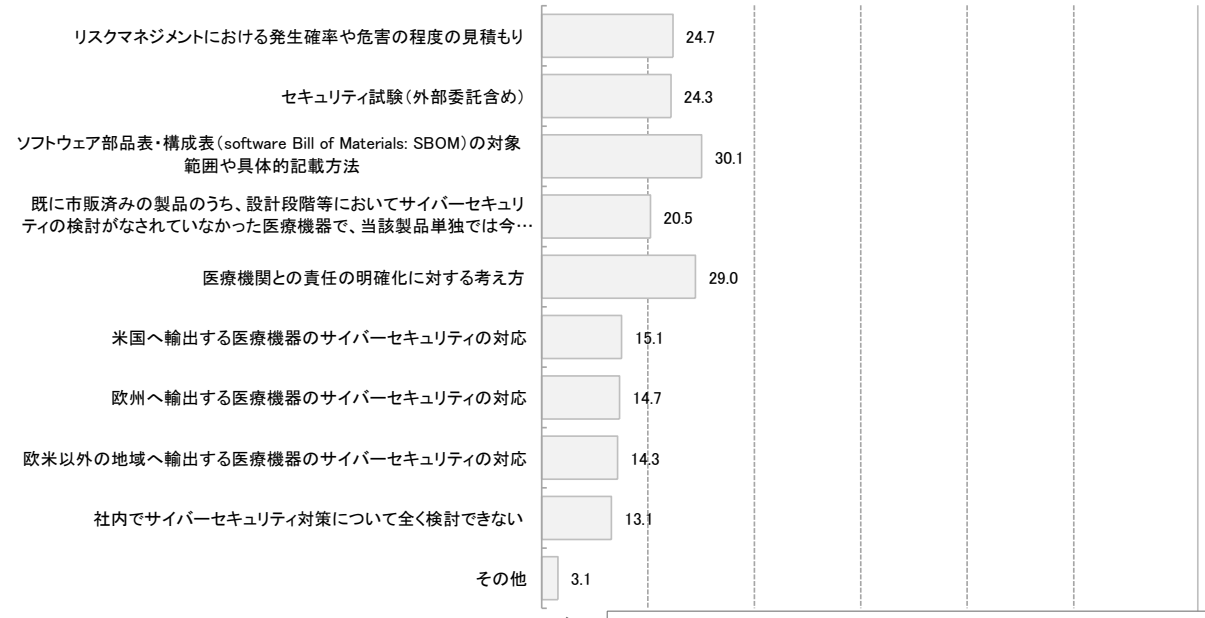

空白ページ

[Q66]貴社におけるサイバーセキュリティ対策の課題についてお答えください。
(n=259)








- 輸入製品のため、関連情報が極めて少ない
- 社内の誰(どの部門が)担うのか決まらない。
- 基幹業務としてのサイバーセキュリティ体制は構築されています。また、製品については、簡単なソフトウェアを組み込んだものであり、サイバーセキュリティの問題とはなじみ難いように考えられます(バグの問題の方が大きい・・・)。
- 海外本社からの情報
- 海外主導で対策しており、国内の通知等を適宜情報提供することにより対応している。翻訳までの時差が短縮できると良い。
- 医療機器を操作するPCのサイバーセキュリティ上の取り扱いの明確化
- リスクと利益に対して対策費用が見合わない
- コスト

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【行政に対するご意見・ご要望①】

【対象品目あり】

- 輸入業者（製販）として必要な具体的対策の提示をお願いしたい。
- 複数省庁にまたがっているガイドライン等の統合
- 認知度を上げてほしい
- 日本発の医療機器の海外展開を容易にするため、日本独自のセキュリティ要件は最小限にしていただきたい。
- "対応の指標として、医療機器の基準（認証基準又は基本要件基準）にIEC 80001-1やIEC/TR 80001-2-2、行政通知等への適合性を要求するなど明確にして欲しい。
- PMDA・総務省と合同で研修会や講習会を行い、国内外の状況や具体的な対応について解説して欲しい。"
- 他国・外部からの侵入は、犯罪となることを知らしめる制度を確立させてほしい。
- 説明会
- 主に医療情報システム向けとしてガイダンスが発行されていることもあり、医療機器個別でどこまで対策すべきかの判断が難しい。
- 行政として、サイバーセキュリティに関する要求事項を明確にしてほしい。要求事項が曖昧なため、過不足が懸念されます。
- 行政ガイドライン例に必ずしも一致しないケースがあるが病院はガイドラインへの適合を求めてくるケースが多く対応に苦慮している。
- 公教育での基本的なIT教育を欧米並みにやって欲しい。まずはそこから。
- 現状は、基幹業務以外では特に問題はないと存じますが、今後、より高度な製品を製造販売する際には、ご指導、ご協力の程、お願い申し上げます。
- 現時点では特にありません。
- 具体的な対策例などの開示があれば有難い。
- 具体的な事例に基づくガイダンスを提供してほしい
- 規制・対応内容の明確化、窓口の一本化
- 何をもって自社のサイバーセキュリティ対策とするか、定義不明。医療機器側で対応できない状況にあるのではないか。
- 横断的な情報共有取り組みの強化（経済産業省、総務省、厚生労働省間含め、各種業界）を希望する。
- 医療機器業界のISAO設立を希望します
- 医療機器にまつわるインシデントをご紹介ください。
- 医療機関でのサイバーセキュリティ管理に係る費用（専用スタッフ、外部委託）については、診療報酬で評価するなど、医療機関が主体的に動ける仕組みを導入いただきたい。
- 医療システムは国家の重要インフラであり、サイバー攻撃による医療機器等の誤作動等による健康被害の防止、又医療機関が扱う患者の要配慮個人情報の観点から、特に小規模の医療機関の現状把握の上、継続的な財源の担保について一刻も早い対応を望みます
- ユーザ、医療施設側への教育、啓蒙を、通知、ガイドラインのアップデートなどで、継続的に行ってもらいたい。
- もう少し具体的に検討をしてほしい。
- もう少し具体的でわかりやすいサイバーセキュリティ対策のガイドラインを作成していただきたい。



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【行政に対するご意見・ご要望②】

【対象品目あり】

- メーカ、医療機関それぞれに対して、具体的な対策レベル感がわかるような対応指針を示していただけるとありがたい。医療機器メーカに対して医療機関毎に異なる対策を要求されても対応できないので、一定の対応基準が求められる。
- サイバー攻撃に対する罰則強化
- サイバーセキュリティへの対応は医療機器メーカーだけでは対応できないため、医療機関（特に中小病院や個人クリニック、歯科医院）も積極的に対応してもらえる取り組みを実施してほしい。また、中堅企業がサイバーセキュリティへの対応が行うための補助金等が申請できるような体制を検討していただきたい。
- サイバーセキュリティの具体的な評価・方法が知りたいです。チェックリスト等があると参考になります。
- サイバーセキュリティについては、プラットフォームとなるOSやCPUの提供メーカーの意向に大きく左右されるため、それら大手企業からの情報提供の量と質をもっと向上させるよう、折衝を行ってほしい。
- サイバーセキュリティーに関するポータルサイト的な総合サイトが欲しい。公表されている通知、ガイドライン、Q&Aなど、厚労省、経産省、内閣（NISC）、総務省、FDA、EC(MDCG)などの枠にとらわれないもの。
- ガイダンス以外に早期にSpecific Requirementを明確にしていただきたい
- Windows7、XPのサポート終了に伴い、顧客、企業共に大きな負担となっている。行政からWindows7の交換に対する助成金や、起業でのセキュリティー対策（IT、現地で修理する人員）の助成等を検討して欲しい
- OSプロトコールレベルの話を一企業に対応求められても実質対応不可能。
- FDA適応に追従して欲しい
- 1、医療機関におけるサーバーセキュリティの大きな課題の一つとして、対策費用の捻出がある。これは他国でも同様。特に保健医療制度による収入のキャップ、人材不足、働き方改革など、労務費負担増の傾向などがサイバーセキュリティ対策の足かせとなっていると推測される。行政として、この費用面に対する解決の検討をお願いしたい。 2、各国のサイバーセキュリティ対応の要求は現在同じ方向性で制定され集約されつつある状況にある。一方で日本は国独自の細かい部分が多々あり他国との歩調が合っていない。よって、世界の流れに沿ったガイドラインなどの策定を希望する。 3、厚労省の医療機器に対するガイドラインの中でライフサイクルサポートとサポート期間の指針が示されているが、世間のソフト、ハードのサイバーセキュリティサポート期間を考慮すると実現が甚だ困難であり、サポートする側、される側、サービスを購入する側の三者の実情を考慮した内容となるよう継続検討していただきたい。
- ・厚労省：安全管理ガイドラインの教育活動を促進して欲しい ・現在5版の改定作業進めていると思いますが、医療機関と製造販売業者との連携が重要であることはもっと通知して欲しい ・IMDRF文書N60のパブコメが出ていますが、これが公開になった後、行政としてどう規制に盛り込むのか迅速な対応を期待しています

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【業界団体（工業会等）に対するご意見・ご要望①】

【対象品目あり】

- 中小企業にも無料での団体加盟の方法を検討して門戸を広げて欲しい。
- 例えばPCの積極的活用。最新のツール（iPad等）の活用を促して欲しい。まずそこから啓蒙して頂きたい。
- 理解を進めるために定期的な講習会開催
- 輸入業者（製販）として必要な具体的対策の提示をお願いしたい。
- 明確なガイドラインの策定と責任範囲の明確化
- 平成30年7月24日通知「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」（薬生機審発0724第1号薬生安発0724第1号）における、「サイバーリスクに伴う医療機器の不具合等の情報」について、業界団体で情報提供・共有いただける仕組みがありましたら幸甚です。
- 添付文書テンプレートにサイバーセキュリティに関する文言が欲しい。
- 適時、情報開示。サイバーセキュリティに関する対応・対策等の参考例の紹介
- 抽象的なガイダンス、ガイドラインではIoT、サイバー、フィジカル空間の連携として統一性に欠ける。可能な限り具体的な指針を定め、各社共通の対応ができる体制にしてほしい。
- 大手企業保護ではなく、全企業保護の企業目線で検討してほしい。
- 製品数によって割引がある工業化に参加したい。製品数によって割引があれば、加入したい。
- 製品の特質を考慮したカテゴリー分けを行いRequirementを明確にする必要があると思います。WG等を活用し取り組みをお願いいたします。
- 製販側の対応ガイドラインなどの作成、アップデート。継続的な教育、啓蒙の実施。
- 製造販売業者として何をどのようにするかの具体的な対策に関して講習会等を希望する
- 上記の政府からの指針提示が困難な場合、業界団体が示すことで補うことも現実的な対応になり得る。
- 上記が達成されれば業界団体は、それに従うことになる。
- 上記、行政に対する意見・要望への対応に同じ。
- 今後とも、適正なルールの策定と普及に努めて頂ければと存じます。
- 講習会の開催
- 講習・セミナーの充実
- 具体的な対策例などの開示があれば有難い。
- 具体的な事例を提示してほしい
- 機器を含まない単体プログラムのみを扱う製販としてやっておくべき対策（事例）を具体的に示してほしい。
- 各団体での認識および見解の統一を図って欲しい
- 各製造業者への啓発活動のほか、医療機関側の主体的な活動の推進と、行政・医療機器に理解を求める動きをしていただきたい。
- 引き続きセミナーで情報を展開して欲しい
- 医療機器のクラス分類などによる、セキュリティ対策は考慮するべきであり、一律の対策では、メーカーへの負担が大きくなる場合もある



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【業界団体（工業会等）に対するご意見・ご要望②】

【対象品目あり】

- 医療機器にまつわるインシデントをご紹介ください。
- 医療機器におけるサイバーリスク対応事例の紹介、対応に関連する情報の展開、講習会などの開催
- より現実に近い体制構築事例等を紹介していただけるとありがたい。
- セミナーの企画
- すでに実施されているが、各工業界特有の問題を扱ったセミナーの開催など。
- サイバーセキュリティ対応を行っている（できている）企業の具体的な対応方法や、現時点で最善と考えられる取り組み事例の紹介、医療機関向け（特にサイバーセキュリティ対応が十分でないと考えられる中小病院や個人クリニック、歯科医院等）の注意喚起リーフレット等を作成してほしい。
- サイバーセキュリティに関する教育
- ガイドラインは提示されるが、具体的にどうすれば？で話が止まってしまう
- ・もっと医機連主体でサイバーセキュリティ対応の事例紹介など含めた対応セミナーを開催して欲しい ・IMDRF文書N60のパブコメが出ていますが、これが公開になった後、行政の対応を受けて、セミナーなどいち早く開催して欲しい

[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【医療機関に対するご意見・ご要望】

【対象品目あり】

- 弊社の製品は家庭用であり、医療機関様で使用されることはないと存じます。
- 病院ごとにサイバーセキュリティーに対する見識の相違が大きく、メーカーとして対応しきれない場合が多い為、見識を統一して欲しい
- 認知度を上げる
- 適時、情報開示。サイバーセキュリティに関する対応・対策等の参考例の紹介
- 現時点で特にございません
- 患者の個人情報を守る制度が必要です。
- 各医療関連協会、団体等で周知されていると思われるが、「医療情報システムの安全管理に関するガイドライン 」は、ボリュームがあり、わかりやすい冊子やQ&Aなどがあれば、より理解が進むのではないか？
- 外部接続の完全シャットアウトの緩和
- 医療機器にまつわるインシデントをご紹介ください。
- 医療機関は、サイバーセキュリティ管理において、医療機器（メーカ）側への依存が高いので主体的な活動を計画いただく必要がある。
- 医療機関に関してはどの程度のネットワーク使用環境が確保されているのか、それが適正な状態か評価基準が判りにくい。病院機能評価を受審している医療機関が多いと思うので、評価項目にサイバーセキュリティ面の審査を追加し、サイバーセキュリティ対策の積極的強化を促して欲しい。
- 意識の低い医療機関が多い
- ユーザー側で各自にセキュリティ対策が必要であることを認識してほしい。
- セキュリティ、危機管理意識を持ってほしい
- サイバーセキュリティは医療機器メーカーだけが対応するものではなく、基本的には医療機関のシステムがベースになっているということをもっと自覚してもらい、医師会や学会と連携してもっとサイバーセキュリティへの取り組みを積極的に行ってもらいたい。
- サイバーセキュリティー/病院ポリシーを理由に話を聞かずにNGを出す機関が多数見受けられる。（現場ではなく医療情報課等のIT管理部門側にて）
- インシデント発生時の状況（人と物の流れ）、使用環境（他社製品含む）の明確化（テンプレート化）を希望する。
- ・サイバーセキュリティは共同責任（Shared Responsibility）であることを認識してもらった上で、相互に協力することで対応して欲しい ・ネットワーク構成など製造販売業者との情報交換、相互協力をもっと進めて欲しい



[Q67]サイバーセキュリティに関連するご意見・ご要望ご意見、ご要望などが有りましたらご自由にお書きください。

## 【その他のご意見・ご要望】

【対象品目あり】

- 弊社は本社が外国医療機器メーカーの日本法人であり、設計製造は全て本社である為、本社の組織体系を前提とし、回答させて頂きました。
- 日々の技術の進歩、陳腐化に追いついていないと感じる。より柔軟で早急な対応が取れるための施策が必要と感じる
- 単体の医療機器プログラムではなく、ソフトウェアを用いて外部アクセス可能な機器はすべて対策が必要であることを、周知するうえで、このアンケートは有用であったと思います。
- 体制や規定がないことに対する、3年以内での対応はない、しないという回答は、現時点では整備時期が明確に答えられない、分かっていない、判断・決定していない、という意味。
- 申し訳御座いませんが、現時点では、サイバーセキュリティを考えなければならない製品がありませんので、大変、答え難い質問が散見されました。尚、取引先でのサイバーセキュリティの件は、今後の課題かと思いました。気づかせて頂き、有難う御座いました。
- 具体的な対策事例等を提示頂けると参考になり、自社に取り込みやすいかもしれない。
- 具体的な対応を考える部門・担当者がいないのと、対応法の想定が不明なため、実際にどのように動けばいいのか検討に至っていない。
- 機器の販売ができていないため、並行してサイバーセキュリティに対する知見を収集中です。
- 一部の大手企業を除いたほぼすべての企業（具体的には従業員数が1000人未満、資本金が10億円未満等の企業）で、サイバーセキュリティ対応が求められる製品を製造販売しているが、対応できる人材が十分に確保できていない企業や、個人診療所・中小規模の病院等でネット環境が十分に整備されていなかったり、専門スタッフが配置できない医療機関がサイバーリスクの危険が大きい。そういった企業や医療機関向けに、対応マニュアル、指針（具体的なポリシーの記載事例や考え方等）、リーフレット等が示せるように行政、業界、医療機関が連携して確実に対応できるような体制（システム）を構築していただきたいと思います。
- メーカ側として課題意識はあるものの、積極的に対応できているとは言えない状況です。行政主導で方針、指針を示していただけると動きやすくなると思われます。
- ネットワークにつなげない製品はサイバーセキュリティーに関係ないと思っていますが、違うのでしょうか。また、製品内のマイコンの組込プログラムも同じ考えですが、どの部分でサイバーセキュリティーが必要なのか分かりません。
- サイバーセキュリティに関する規格(ISO,IEC)の制定、JIS化、規定化をして海外と歩調をあわせてほしい。
- これまでの通知文書などから「医療機関側が行うこと」という認識がある。そもそも誰が何をどうするのか、明確になっているのだろうか？何から手をつけるべきか要領を得ないのは弊社だけか？
- ・サイバーセキュリティは避けて通ることの出来ないもので、どこまで対応すればよいかもなかなか判断が難しい。随時、適宜ホームページなどで情報をアップしていただけると対応の一助となるので、よろしくお願いします。
- （本調査回答に関する補足）当社で業務に使用するIT機器は、親会社のセキュリティシステムの下で管理されており、サイバーセキュリティへの対策もとられています。本調査では、当社単独での対応はできていないとの観点から回答を行っておりますので、その点をご理解ください。

2019 年 12 月

総括製造販売責任者　各位

日本医療研究開発機構研究費（医薬品等規制調和・評価 研究事業）
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（研究代表者）
公益財団法人医療機器センター専務理事 中野壮陛

# 『製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査』へのご協力依頼

当財団では、**厚生労働省医薬・生活衛生局医療機器審査管理課及び医薬安全対策課からの依頼**により、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（日本医療研究開発機構委託研究費（医薬品等規制調和・評価研究事業））を本年度から別添研究班メンバーにより実施することとなりました。

昨今、医療機器のサイバーセキュリティの重要性が指摘され、厚生労働省から行政通知「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）が発出され約 1 年が経過しましたが、この研究班においては、当該ガイダンスを踏まえた**医療機器のサイバーセキュリティ対策の実施状況を把握し、実施上生じる新たな課題などを踏まえ、実効性のあるサイバーセキュリティ対策の具体化や更なる充実化を検討**することを目的としています。

そこで、本研究班では、**『製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査』を実施**することといたしました。

つきましては、裏面の「調査の背景とねらい」をご一読頂き、皆さまにぜひご回答頂きたくお願い申し上げます。**ご回答頂いた方には調査結果概要を後日フィードバックする予定**です。

お忙しい中恐縮ですが、ご理解のうえ、ご協力のほどよろしくお願い致します。

記

提出方法　：　**同封した『実施状況とりまとめ用紙』を活用し関係部署へ確認を行って頂いた後、専用の WEB サイト（https://questant.jp/q/JAAME2019）から提出**

提出期限　：　**2020 年 1 月 24 日（金）**

守秘について

回答頂きました内容については、事務局内で守秘義務を厳守の上、調査のとりまとめを行い、本調査以外には使用致しません。また本調査における個別の回答内容については、事務局内のみでの取り扱いとし、研究班メンバーであっても個別の回答結果を閲覧することはできず、企業名がわからないように加工あるいは一般化された内容のみ閲覧することができる状態とします。また個別の回答内容を行政及び関連機関に報告することもありません。

以上

【事務局】
日本医療研究開発機構研究費（医薬品等規制調和・評価 研究事業）
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班事務局
公益財団法人医療機器センター　中野・鈴木・本田
E-mail：mdsi-cyber@jaame.or.jp　電話：03-3813-8553

調査の背景とねらい

《背景》

近年、「医療の質の向上」と「効率的な医療の提供」という二律背反する課題を克服することがわが国においては喫緊の課題となっています。そのため、医療データを有機的に連結させた ICT インフラを着実に整備していきながら、近年広がる IoT の推進と相まって、医療機器から得られた情報がもたらす新たな価値に期待が集まっています。

このような背景のもと、**医療機器も様々なネットワークに今後ますます接続されていくことが予想**されますが、**国内外においても医療機関に対するサイバー攻撃**は社会的課題となってきており、医療機器においても従来行われてきた一次故障や誤操作等をリスク要因として捉えるリスクマネジメントに加えて、悪意を持った攻撃者の存在等もリスク要因として捉えて検討することが必要となります。

本邦においては、厚生労働省から「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、薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号)、「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、薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号) などが発出されているものの、**ガイダンスは一般的な概要にとどまっている**ことや、医療機器は多種多様で、**個々の製品について必要なサイバーセキュリティ対策が異なる**こと、またサイバーセキュリティは**医療機関における実際の使用環境を含めて考える必要**があること、さらにガイダンス発行から日が浅いことも相まって、**製造販売業者における医療機器のサイバーセキュリティ対策は、課題も多く、解決策に関する情報も不足し、どこまで何をすればよいのかという具体的対策を進めにくい、あるいはそれ故に新たな開発が進めにくいという状況**下に置かれているものと考えられます。

《ねらい》

**これからは、サイバーセキュリティ対策が十分に施された医療機器の開発・供給を行っていくことが国内外で求められます**。本調査は、医療機器のサイバーセキュリティ対策の実施状況を把握し (実態調査)、実施上生じる新たな課題などを踏まえ、**実効性の高いサイバーセキュリティ対策の具体化や充実化を臨産官が一体となって検討**するため**本邦初の大規模調査**として実施するものです。

そのため、**本年は約 2700 社の製造販売業者を対象**として調査を実施し、翌 2020 年には医療機関における医療機器のサイバーセキュリティ対策の調査も実施する予定です。

その後、両者の調査結果を十分踏まえ、**厚生労働省などの行政側が主体となって検討・実施する項目、民間主体にて業界団体が検討・実施する項目、製造販売業者が医療機関などとともに協力しながら進めて行く項目などを整理**し検討することにより、**製造販売業者においてサイバーセキュリティ対策が十分に施された医療機器の開発・供給の体制構築の実現**に寄与することが期待されます。

※本調査は、一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF および各関係団体にご協力頂き実施しています。**ご回答頂いた方には調査結果概要を後日フィードバックする予定**です。

別　添

令和元年度日本医療研究開発機構研究費（医薬品等規制調和・評価 研究事業）
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

研究班メンバー

| | | |
|---|---|---|
| 中野壮陛 | 公益財団法人医療機器センター　専務理事 | ※研究代表者 |
| 長島公之 | 公益社団法人日本医師会　常任理事 | |
| 中村康彦 | 公益社団法人全日本病院協会　副会長（四病協） | |
| 久芳　明 | 一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF リーダー | |
| 古川　浩 | 一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF | |
| 松元恒一郎 | 一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF | |
| 北村正仁 | 一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF | |
| 谷口克巳 | 一般社団法人日本医療機器産業連合会 サイバーセキュリティ TF | |

【オブザーバー】
厚生労働省医薬・生活衛生局医療機器審査管理課
厚生労働省医薬・生活衛生局医薬安全対策課
経済産業省商務情報政策局サイバーセキュリティ課
経済産業省商務・サービスグループヘルスケア産業課医療福祉機器産業室
独立行政法人医薬品医療機器総合機構（PMDA）医療機器審査第一部
独立行政法人医薬品医療機器総合機構（PMDA）医療機器審査第二部
独立行政法人医薬品医療機器総合機構（PMDA）医療機器品質管理・安全対策部
国立研究開発法人日本医療研究開発機構（AMED）創薬戦略部　医薬品等規制科学課

**資料３**

公益財団法人 医療機器センター

製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査

# WEB 回答前の『実施状況とりまとめ用紙』

対 象 者：全国の製造販売業者(約 2700 社)の「総括製造販売責任者」様

調査内容：現時点（記入日）における医療機器のサイバーセキュリティ対策の実施状況

提出方法：**専用の WEB サイト（https://questant.jp/q/JAAME2019）から提出**
**※本用紙は、サイバーセキュリティ対策の実施状況について社内の関連部署への確認などにご活用ください。提出は専用の WEB サイトからのみ**となります。

期　　限：２０２０年１月２４日（金）
社内手続きなどで提出期限以降の提出となることが予め予想される場合は事前にご一報願います。

【特記事項】

- 本調査は、製造販売業者におけるサイバーセキュリティ対策の実施状況の全体像を明らかにするものであり、個別の企業の取組みについて議論をするものではありません。また個別の回答内容を行政及び関連機関に報告することもありません。
- 回答頂きました内容については、事務局内で守秘義務を厳守の上、調査のとりまとめを行い、本調査以外には使用致しません。
- 本調査における個別の回答内容については、事務局内のみでの取り扱いとし、研究班メンバー（別添参照）であっても個別の回答内容を閲覧することはできず、企業名がわからないように加工あるいは一般化された内容のみ閲覧することができる状態とします。
- 回答内容を取りまとめた結果については、報告書として国立研究開発法人日本医療研究開発機構(AMED)に提出し、その一部は AMED 等のウェブサイトで公開されますが、その報告書の内容から個別の企業名や取組み内容について特定できないような記載とします（公知の事実が回答に含まれていた場合については、公知の事実として取り扱う可能性があり、この限りではありません）。
- 回答内容について不明点がある場合には、事務局より個別に確認させていただく場合がございます。その際、ウェブサイトの回答フォームに記入された方の所属部門、氏名、電話番号、メールアドレスを使用しますが、それ以外の用途には使用致しません。
- 「＊」のある設問は、回答が必須の項目です。

日本医療研究開発機構研究費（医薬品等規制調和・評価 研究事業）
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班事務局
公益財団法人医療機器センター　中野・鈴木・本田
E-mail：mdsi-cyber@jaame.or.jp　電話：03-3813-8553

## 【Q1～Q6】
## 貴社について

Q1. 基本情報をお伺いします。

企業名 ＊

製造販売業の許可番号 ＊ （半角英数字）

ウェブサイトの回答フォームに記入される方の氏名 ＊

ウェブサイトの回答フォームに記入される方の所属部門

ウェブサイトの回答フォームに記入される方に連絡の取れる電話番号 ＊ （ハイフンなしの半角数字のみ）

ウェブサイトの回答フォームに記入される方に連絡の取れるメールアドレス ＊

その他連絡事項

※回答頂いた方には調査結果をフィードバックする予定となっております。その際はこちらに記載して頂いたメールアドレスにご連絡致します。

Q2. 資本金についてお答えください。＊

- ○ ～5000 万円以下
- ○ ～1 億円以下
- ○ ～3 億円以下
- ○ ～50 億円以下
- ○ ～100 億円以下
- ○ ～200 億円以下
- ○ ～200 億円超

Q3. 資本上の区分についてお答えください。＊

- ○ 内資系企業…国内の企業であって、外資系以外の企業
- ○ 外資系企業…外国会社、或いは外国会社が親会社として経営を支配している会社

Q4. 専業・兼業の区分についてお答えください。＊

- ○ 専業：全売上のうち医療機器売上高の占める割合が 50%以上
- ○ 兼業：全売上のうち医療機器売上高の占める割合が 50%未満

Q5. 全社員数についてお答えください。＊

- ○ ～50 人以下
- ○ ～100 人以下
- ○ ～300 人以下
- ○ ～500 人以下
- ○ ～1000 人以下
- ○ 1000 人超

Q6. 主な加盟団体についてお答えください。＊（複数選択可）

□　（一社）電子情報技術産業協会（JEITA）
□　日本医用光学機器工業会（日医光）
□　商工組合 日本医療機器協会（日医機協）
□　（一社）日本医療機器工業会（日医工）
□　（一社）日本医療機器テクノロジー協会（MTJAPAN）
□　（一社）日本医療機器ネットワーク協会（@MD-Net）
□　（一社）日本医療機器販売業協会（医器販協）
□　日本医療用縫合糸協会（日縫協）
□　（一社）日本衛生材料工業連合会（日衛連）
□　（一社）日本画像医療システム工業会（JIRA）
□　（一社）日本眼科医療機器協会（眼医器協）
□　（一社）日本コンタクトレンズ協会（CL 協会）
□　日本コンドーム工業会（コンドーム工）
□　日本在宅医療福祉協会（日在協）
□　（一社）日本歯科商工協会（歯科商工）
□　（一社）日本分析機器工業会（分析工）
□　（一社）日本ホームヘルス機器協会（ホームヘルス）
□　（一社）日本補聴器工業会（日補工）
□　（一社）日本補聴器販売店協会（JHIDA）
□　日本理学療法機器工業会（日理機工）
□　（一社）日本臨床検査薬協会（臨薬協）
□　（一社）保健医療福祉情報システム工業会（JAHIS）
□　その他（　　）
□　あてはまるものはない

## 【Q7～Q26】
## 貴社の企業としてのサイバーセキュリティに係る対応状況について

Q7. 会社全体のサイバーセキュリティ対応を行う組織体制がありますか。＊

○ はい　　○ 全体としてはないが、一部の部門としてある　　○ いいえ

※Q7 の回答による
Q8. 「いいえ」の場合、3 年以内に構築の予定はありますか。＊

○ 1 年以内に構築の予定がある
○ 2 年以内に構築の予定がある
○ 3 年以内に構築の予定がある
○ 3 年以内の予定はない

Q9. サイバーセキュリティに関して統括する立場の責任者はいますか。＊

○ 役員レベルとして責任者がいる　　○ 上記未満のレベルとして責任者がいる
○ 部門長レベルとして責任者がいる　　○ いない

Q10. サイバーセキュリティの検討にあたって、次のいずれの範囲を対象としていますか。＊（複数選択可）

□ 製品（医療機器）そのもの
□ 基幹系・情報系システム
□ 工場制御系システム
□ サイバーセキュリティの検討を行っていない

Q11. コンピュータセキュリティにかかるインシデントに対処するための組織となる CSIRT(Computer Security Incident Response Team）がありますか。＊

○ はい　　○ いいえ　　○ 不明

※Q11 の回答による
Q12. 「いいえ」の場合、3 年以内に構築の予定はありますか。＊

○ 1 年以内に構築の予定がある
○ 2 年以内に構築の予定がある
○ 3 年以内に構築の予定がある
○ 3 年以内の予定はない

Q13. 組織が提供する製品の脆弱性に起因するリスクに対応するための組織内機能として PSIRT（Product Security Incident Response Team）がありますか。＊

○ はい　　○ いいえ　　○ 不明

※Q13 の回答による
Q14. 「いいえ」の場合、3 年以内に構築の予定はありますか。＊

○ 1 年以内に構築の予定がある
○ 2 年以内に構築の予定がある
○ 3 年以内に構築の予定がある
○ 3 年以内の予定はない

Q15. QMS 対象業務（設計、製造、アウトソーシング先等、関係する全てを含む）で使用している IT 機器について、ウイルス対策やセキュリティ対策に関する対応は行っていますか。＊

○　はい　　○　いいえ

Q16. 製造販売業としての QMS 対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。＊

○　製造業および委託先まで含めて全て把握している
○　製造業までを把握している（委託先は把握していない）
○　いいえ

Q17. サイバーセキュリティに関する社員教育を行っていますか。＊

○　はい　　○　いいえ

※Q17 の回答による
Q18. 「はい」の場合は、誰に対して教育を行っていますか。＊（複数選択可）

□　全社員
□　マネージメント・スタッフ
□　開発・設計
□　製造
□　営業
□　サービス（SE、営業技術等）
□　その他

※Q17 の回答による
Q19. 「はい」の場合は、どのように行っていますか。＊（複数選択可）

□　社内スタッフによる社内教育
□　社内スタッフが作成した e-learning 教育
□　専門コンサルタントによる社内教育
□　工業会セミナーを利用した社外研修の活用
□　専門業者セミナーを利用した社外研修の活用
□　専門業者による e-learning 教育
□　その他（　　）

※Q17 の回答による
Q20. 「はい」の場合は、どのような内容の教育を行っていますか。＊（複数選択可）

□　社内業務用 IT インフラの利活用を含む一般情報セキュリティ
□　医療機器全般のサイバーセキュリティ（セキュリティリスクマネジメントおよび脆弱性対応等）
□　個別製品のサイバーセキュリティ（セキュリティリスクマネジメントおよび脆弱性対応等）
□　その他（　　）

Q21. サイバーセキュリティに対応するため追加・修正した規程・手順書などがありますか。＊

○　はい　　○　いいえ

※Q21 の回答による
Q22. 「はい」の場合、どのような内容の規定・手順書を追加・修正しましたか。＊(複数選択可)
□　設計に関する規程・手順書
□　リスクマネジメントに関する規程・手順書
□　セキュリティ試験に関する規程・手順書
□　市販後管理計画に関する規程・手順書
□　ラベリング又はユーザー向けセキュリティ文書に関する規程・手順書
□　サイバーセキュリティ対策情報開示に関する規程・手順書
□　その他（　　）

※Q21 の回答による
Q23. 「いいえ」の場合、3 年以内に追加・修正する予定はありますか。＊

○　1 年以内に定める予定がある
○　2 年以内に定める予定がある
○　3 年以内に定める予定がある
○　3 年以内の予定はない

Q24. サイバーセキュリティに関するポリシーを社外に公開していますか。＊

○　はい　　○　いいえ

※Q24 の回答による
Q25. 「はい」の場合は、どのような方法で公開していますか。＊（複数選択可）

□　自社ウェブサイト
□　取り扱い説明書
□　サイバーセキュリティに関する特別文書
□　その他（　　）

※Q24 の回答による
Q26. 「いいえ」の場合、3 年以内に公開の予定はありますか。＊

○　1 年以内に公開する予定がある
○　2 年以内に公開する予定がある
○　3 年以内に公開する予定がある
○　3 年以内の予定はない

## 【Q27～Q30】
## 貴社の製品（医療機器）について

Q27. 製造販売している医療機器についてお伺いします。＊

組み込みプログラムを用いた医療機器（例えば、汎用心電計など）を製造販売していますか。

○　はい　　○　いいえ

コンピュータ（汎用 PC など）を用いた医療機器（例えば、汎用画像診断装置ワークステーションなど）を製造販売していますか。

○　はい　　○　いいえ

医療機器プログラム（単体プログラム）を製造販売していますか。

○　はい　　○　いいえ

※ **上記 3 つの問いに対し、全てが「いいえ」の場合は Q67 へ。**
**いずれか一つでも「はい」がある場合は Q28 以降もお答えください。**

※Q27 の回答において、いずれかに「はい」がある場合のみ
Q28. それらは、次の機能を有しますか。＊（複数選択可）

□　無線通信(Wi-Fi、Bluetooth 等)または有線通信(イーサネット、シリアル・パラレル通信、USB 接続等)により、他の医療機器、医療機器の構成品、非医療機器の周辺機器、インターネット・イントラネット、その他のネットワークとの接続が可能な機能

□　USB メモリや DVD、フロッピーディスク等の携帯型メディアにより、他の医療機器、医療機器の構成品、非医療機器の周辺機器、インターネット・イントラネット、その他のネットワークとの接続が可能な機能

□　その他の機能により、他の医療機器、医療機器の構成品、非医療機器の周辺機器、インターネット・イントラネット、その他のネットワークとの接続が可能であったり、外部データの入力が可能な機能（具体的な通信あるいはデータの入力手段を必ず記載願います：　　）

※Q27 の回答において、いずれかに「はい」がある場合のみ
Q29. 貴社の全製品（医療機器）のうち、（現在の対応状況の如何を問わず）サイバーセキュリティ対応を検討しなければならない医療機器の割合はおおよそどの程度ですか。＊

○　20%未満
○　20%以上 40%未満
○　40%以上 60%未満
○　60%以上 80%未満
○　80%以上

※Q27 の回答において、いずれかに「はい」がある場合のみ

Q30. **前問（Q29）のサイバーセキュリティ対応を検討しなければならない医療機器のうち、**既に市販済みの製品であって、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器であり、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できないと考えられる医療機器（Legacy Medical Device）の割合はおおよそどの程度ですか。＊

- ○ 20%未満
- ○ 20%以上 40%未満
- ○ 40%以上 60%未満
- ○ 60%以上 80%未満
- ○ 80%以上

## ※Q27 の回答において、いずれかに「はい」がある場合のみ【Q31～Q34】
## サイバーセキュリティに関する情報の入手について

Q31. サイバーセキュリティに関する情報をどこから入手していますか。＊（複数選択可）

□　工業会
□　IPA（情報処理推進機構）等の IT 専門機関
□　PMDA（医薬品医療機器総合機構）等の薬事専門機関
□　行政
□　各種セミナー
□　コンサルタント
□　その他（　　）

Q32. 国内の通知、ガイドライン、ガイダンス等を把握・活用していますか。＊

厚生労働省通知「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」薬食機参発 0428 第 1 号・薬食安発 0428 第 1 号（平成 27 年 4 月 28 日）

○　活用している　　○　知っているが活用していない　　○　知らない

厚生労働省通知「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」薬生機審発 0724 第 1 号・薬生安発 0724 第 1 号（平成 30 年 7 月 24 日）

○　活用している　　○　知っているが活用していない　　○　知らない

医機連「医療機器のサイバーセキュリティ確保に関する質疑応答集（Q&A）」（2019 年 3 月）

○　活用している　　○　知っているが活用していない　　○　知らない

JAHIS 標準 17-006「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a（一般社団法人保健医療福祉情報システム工業会　2017 年 7 月）又は JESRA TR-0039*B－2018「製造業者による医療情報セキュリティ開示書」ガイド Ver.3.0a（一般社団法人日本画像医療システム工業会　2018 年 3 月）

○　活用している　　○　知っているが活用していない　　○　知らない

Q33. サイバーセキュリティ関連組織・活動を把握・活用していますか。＊

独立行政法人情報処理推進機構（IPA）の活動・情報提供

○　活用している　　○　知っているが活用していない　　○　知らない

日本コンピュータ緊急対応センター（JPCERT）の活動・情報提供

○　活用している　　○　知っているが活用していない　　○　知らない

Q34. 海外のガイダンスやガイドライン等を把握・活用していますか。＊

米国FDAガイダンス「Content of Premarket Submissions for Management of Cybersecurity in Medical Devices」や「Postmarket Management of Cybersecurity in Medical Devices」

○ 活用している　　○ 知っているが活用していない　　○ 知らない

IMDRF「Principles and Practices for Medical Device Cybersecurity (Draft)」

○ 活用している　　○ 知っているが活用していない　　○ 知らない

IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities やIEC TR 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices -Part 2-2: Guidance for the communication of medical device security needs, risks and controls

○ 活用している　　○ 知っているが活用していない　　○ 知らない

## ※Q27 の回答において、いずれかに「はい」がある場合のみ【Q35～Q51】
## 貴社の製品（医療機器）への対応状況について

Q35. 貴社の製品（医療機器）の寿命や使用期限、企業からのサポート終了時期について規定し、ユーザーに伝えていますか。＊

○ はい　　○ いいえ

※Q35 の回答による
Q36. 「はい」の場合は、ユーザーにはどのような媒体で伝えていますか。＊（複数選択可）

□ 自社ウェブサイト
□ 添付文書
□ 取り扱い説明書
□ 契約書
□ 技術資料
□ サイバーセキュリティに関する特別文書
□ その他（　　）

※Q35 の回答による
Q37. 「いいえ」の場合、3 年以内に規定しユーザーに伝える予定はありますか。＊

○ 1 年以内に規定しユーザーに伝える予定がある
○ 2 年以内に規定しユーザーに伝える予定がある
○ 3 年以内に規定しユーザーに伝える予定がある
○ 3 年以内の予定はない

Q38. サイバーリスクが懸念される医療機器について、製品（医療機器）が使用されている主な場所を把握していますか。＊

○ はい　　○ いいえ

※Q38 の回答による
Q39. 「はい」の場合、具体的にはどのような場所ですか。＊（複数選択可）

□ 病院
□ 診療所
□ 家庭（在宅医療等）
□ 携帯・インプラント等
□ その他（　　）

Q40. サイバーリスクが懸念される医療機器について、製品（医療機器）の使用環境を特定していますか。＊

○ 全く使用環境を特定していない
○ 全ての製品について使用環境を特定している
○ 一部の特定の製品のみ使用環境を特定している（具体的にはどのような製品ですか：　　）

※Q40 の回答による
Q41. 「全て」、「一部」の場合、どのように特定していますか。＊（複数選択可）

□　「医療情報システムの安全管理に関するガイドライン」に準拠した環境
□　その他（　　）

Q42. サイバーセキュリティに関する問い合わせ先を明確にしていますか。＊

○　はい　　○　いいえ

※Q42 の回答による
Q43. 「はい」の場合は、どのような方法で明確にしていますか。＊（複数選択可）

□　自社ウェブサイト
□　添付文書
□　取り扱い説明書
□　契約書
□　技術資料
□　サイバーセキュリティに関する特別文書
□　その他（　　）

※Q42 の回答による
Q44. 「いいえ」の場合、3 年以内に明確にする予定はありますか。＊

○　1 年以内に明確にする予定がある
○　2 年以内に明確にする予定がある
○　3 年以内に明確にする予定がある
○　3 年以内の予定はない

Q45. 製造販売時におけるサイバーセキュリティに関する情報を使用者に対して提供していますか。＊

○　はい　　○　いいえ

※Q45 の回答による
Q46. 「はい」の場合、どのような方法で提供していますか。＊（複数選択可）

□　自社ウェブサイト
□　添付文書
□　取り扱い説明書
□　契約書
□　技術資料
□　サイバーセキュリティに関する特別文書
□　その他（　　）

Q47. 売買の引合いや契約等の際に、医療機関等からサイバーセキュリティに関する情報提供を求められますか。＊

○　詳細を求められることが多い　　○　特に求められることはない
○　概要を求められることが多い　　○　その他（　　）
○　希に求められる

Q48. サイバーセキュリティに関するインシデント発生時の国内届け出先や手順などを文書化していますか。＊

○　はい　　○　いいえ

※Q48 の回答による
Q49. 「いいえ」の場合、3 年以内に文書化する予定はありますか。＊

○　1 年以内に文書化する予定がある
○　2 年以内に文書化する予定がある
○　3 年以内に文書化する予定がある
○　3 年以内の予定はない

Q50. 貴社は、製品（医療機器)に関するソフトウェア部品表・構成表（SBOM）（注）を医療機関などの顧客に対し、開示することを今後 3 年以内に予定していますか。＊

（注）医療機器に使用されているソフトウェアの透明性を確保するため、製造販売業者は医療機関などの顧客に対してソフトウェア部品表・構成表（software Bill of Materials: SBOM）を提供して、顧客が医療機器のライフサイクルに影響を与えるソフトウェアコンポーネントをよりよく理解できるようにすることが、今後のサイバーセキュリティ対策には必要であるとの議論が国際的になされています。

○　全面的に開示する予定　　○　顧客からの要求に応じて開示する予定
○　開示する予定はない

※Q50 の回答による
Q51. 「開示する予定はない」の場合、ソフトウェア部品表・構成表（SBOM）の開示には何か課題があると考えられますか。＊(複数選択可)

□　知的財産の流出の懸念（提供先からの情報漏洩）
□　ソフトウェア関連の改良・改善と情報開示のタイミングのズレ
□　どこまで公開するのかわからない（標準フォーマットが不明）
□　社内でどの部門まで対応しないといけないかわからない（資材、開発、生産部門など）
□　サードパーティやオープンソースソフトウェアの妥当性検証の懸念
□　開示しても顧客（医療機関等）側が適切に理解するかが懸念（合理性のない対応を求められる懸念）
□　その他（　　）

## ※Q27 の回答において、いずれかに「はい」がある場合のみ【Q52～Q65】
## 貴社の製品（医療機器）への市販後対応状況について

Q52. 市販後に脆弱性の改善に関係するプログラム（ソフトウェア）のアップデートを行っていますか。＊

○　はい　　○　いいえ

※Q52 の回答による
Q53. 「はい」の場合、アップデートする対象をお答えください。＊（複数選択可）

□　OS
□　ミドルウェア
□　当該ソフトウェア本体
□　その他（　　）

※Q52 の回答による
Q54. 「はい」の場合、アップデートに関する情報提供の方法をお答えください。＊（複数選択可）

□　自社ウェブサイトでの公開
□　顧客への個別通知
□　保守契約に基づく保守点検時に通知
□　その他（　　）

※Q52 の回答による
Q55. 「はい」の場合、アップデートを行う期間について、社内の考え方として最も一般的なものをお答えください。＊

○　医療機器の設計・製造時に設定した耐用期間
○　耐用期間にかかわらず、販売後から２年間まで
○　耐用期間にかかわらず、販売後から５年間まで
○　耐用期間にかかわらず、販売後から１０年間まで
○　耐用期間にかかわらず、販売後から医療機関が廃棄するまで
○　その他（　　）

※Q52 の回答による
Q56. 「はい」の場合、アップデートを行う際の費用について、社内の考え方として最も一般的なものをお答えください。＊

○　保守サービス契約期間であれば無償、それ以外は有償
○　保守サービス契約の有無に関わらず有償
○　保守サービス契約の有無に関わらず無償
○　その他（　　）

Q57. 市販後においてサイバーセキュリティに関する情報を使用者に対して提供していますか。＊

○　はい　　○　いいえ

※Q57 の回答による
Q58. 「はい」の場合、どのタイミングで提供していますか。＊

○　逐次提供している
○　インシデント発生時に提供している
○　その他（　　）

Q59.使用現場（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。＊

○　会社組織の仕組みとして常に情報入手が可能になっている
○　関係者等から適宜入手出来ている
○　その他の方法により入手できるようになっている（　　）
○　入手出来るようになっていない

Q60. 貴社の製品（医療機器）に関連して、医療機関から報告を受けたサイバーセキュリティに関連したインシデント事例が3年以内にありましたか。＊

○　はい　　○　いいえ

※Q60の回答による
Q61. 「はい」の場合、どの程度の件数でしたか。＊

○　1件～5件
○　6件～10件
○　11件～20件
○　21件以上

※Q60の回答による
Q62. 「はい」の場合、どのレベルの情報まで情報を入手出来ていますか。＊

○　インシデントが発生したという事実まで
○　インシデントの原因分析まで
○　インシデントの原因分析と医療機関での対応内容まで
○　その他（　　）

※Q60の回答による
Q63. 「はい」の場合、サイバーセキュリティに関連したインシデントが発生した際、関係機関に報告しましたか。＊(複数選択可)

□　IPA（情報処理推進機構）に報告した
□　厚生労働省・PMDA（医薬品医療機器総合機構）に報告した
□　その他の機関に報告した（　　）
□　どこにも報告していない

Q64. 使用現場からの情報入手について、課題や要望等がありますか。

Q65. 販売業者、修理業者に対して、サイバーセキュリティ対策の確認や指導等を行っていますか。＊

○　はい　　○　いいえ

## ※Q27 の回答において、いずれかに「はい」がある場合のみ【Q66】
## 貴社におけるサイバーセキュリティ対策の課題について

Q66. 貴社におけるサイバーセキュリティ対策の課題についてお答えください。＊（複数選択可）

- □ セキュリティ専門人材の確保、育成
- □ セキュリティ専門人材以外の社内教育
- □ 社内の横断的部署の連携
- □ 製造業者（委託先含む）との連携・情報共有
- □ 販売業・修理業等との連携・情報共有
- □ 医療機関との連携・情報共有
- □ 行政関連組織との連携・情報共有
- □ 他社の医療機器のサイバーリスク対応事例の入手・他の製造販売業者同士の情報共有
- □ 医療機器産業以外の産業からの情報共有
- □ サイバーセキュリティの対策費用や費用対効果の判断
- □ セキュリティリスクマネジメントプロセス（サイバーセキュリティの脆弱性の特定など）の具体的方法論
- □ 製品またはコンポーネントが使用されなくなる時点（製品寿命終了/End of Life: EOL）や製造販売業者が全てのサポート活動を中止する時点（End of Support: EOS）の設定方法
- □ リスクマネジメントにおける発生確率や危害の程度の見積もり
- □ セキュリティ試験（外部委託含め）
- □ ソフトウェア部品表・構成表（software Bill of Materials: SBOM）の対象範囲や具体的記載方法
- □ 既に市販済みの製品のうち、設計段階等においてサイバーセキュリティの検討がなされていなかった医療機器で、当該製品単独では今後もサイバーセキュリティの脅威に対して合理的に保護できない医療機器（Legacy Medical Device）の取り扱い
- □ 医療機関との責任の明確化に対する考え方
- □ 米国へ輸出する医療機器のサイバーセキュリティの対応
- □ 欧州へ輸出する医療機器のサイバーセキュリティの対応
- □ 欧米以外の地域へ輸出する医療機器のサイバーセキュリティの対応
- □ 社内でサイバーセキュリティ対策について全く検討できない
- □ その他（　　）

## 【Q67】
## サイバーセキュリティに関連するご意見、ご要望などについて

行政に対してのサイバーセキュリティに関連するご意見・ご要望

業界団体（工業会等）に対してのサイバーセキュリティに関連するご意見・ご要望

医療機関に対してのサイバーセキュリティに関連するご意見・ご要望

その他、サイバーセキュリティに関連するご意見・ご要望 等

ご協力ありがとうございます。

製造販売業者が行っている医療機器のサイバーセキュリティ対策に関する実態調査