# 令和 6 年度　サイバーセキュリティ対策の対応状況に関する
# アンケート調査結果要約

【調査の目的】

サイバー攻撃により社会インフラに多大な影響をもたらす事例が多数発生しており、防護するためのサイバーセキュリティ対策（以下「CS 対策」という。）の重要性は高まっている。医療機器については、令和 5 年 3 月 9 日付け厚生労働省告示第 67 号「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 41 条第 3 項の規定により厚生労働大臣が定める医療機器の基準の一部を改正する件」により、医療機器の基本要件基準第 12 条第 3 項に CS 対策に関する要求事項が明確化され、令和 6 年 4 月 1 日より適用されている。

本研究班では、医療機器全般の CS 対策に関連する制度として、現在の制度での対応が十分か検討し、制度上の手当ての必要性を含めて議論を進めている。本調査は、医療機器全般の CS 対策の現状を把握し、問題点、課題等の情報を収集分析し、その結果をより適切な制度設計の提言案にまとめることを目的に実施する。

- 2024 年 10 月 7 日から 11 月 15 日までの期間、全国の医療機器の製造販売業者、製造業者等を対象に資料に示すアンケート調査を行った（資料１：サイバーセキュリティ対策の対応状況アンケート（設問・選択肢））
- 全 441 社の医療機器の製造販売業者、製造業者等からの回答を得た。アンケート調査の実施にあたっては、一般社団法人日本画像医療システム工業会が所有する WEB アンケートシステムを利用した。アンケート結果の集計、解析作業は、独立行政法人医薬品医療機器総合機構医療機器調査部登録認証機関監督課にて実施した。

【アンケート結果（要約）】（資料２：サイバーセキュリティ対策の対応状況アンケート結果（グラフ））

- アンケート回答者について
  - ✓ 第一種医療機器製造販売業許可取得者が最も多く全体の 52%を占めており、次いで第二種医療機器製造販売業許可取得者が 24%、第三種医療機器製造販売業許可取得者が 12%、製造業登録者が 6%であった（設問 1 及び 3）。
  - ✓ 製造販売業許可取得者については、製造販売業の範囲に含まれる構成員の人数として、21～51 名の会社が最も多く、次いで 1～10 名、201 名以上と会社の規模にはバラツキが大きいと推察された（設問 2）。
  - ✓ 製造販売業許可取得者における設計開発部門の構成員の人数については、設計開発部門を有しない会社が最も多く全体の 36%であった。特に第一種医療機器製造販売業許可取得者のうち、43%の会社では設計開発部門を有していなかった。また、設計開発部門の構成員の人数としては、1～5

名の会社が多く全体の 24%であった（設問 4)。

- ✓ 製造販売業許可取得者における国内製造と外国からの輸入の割合については、国内製造が全体の 43%と最も多かった。特に第二種医療機器製造販売業許可取得者のうち、71%の会社は国内製造のみであった。また、第一種医療機器製造販売業許可取得者では、外国から輸入した医療機器のみを扱う会社が 33%であった（設問 5)。

- CS 対策の対応状況について
  - ✓ 医療機器の製造販売業者、製造業者等において、CS 対策を要する製品が全体の 57%であった。外国製造医療機器特例承認取得者（選任製造販売業者を含む)、第一種医療機器製造販売業許可取得者及び第二種医療機器製造販売業許可取得者において、CS 対策を要する製品が多い傾向であった（設問 6)。
  - ✓ CS 対策を検討しなければならない医療機器のうち、全体の 48%の製品については対応が実施できているとのことであった。一方で、全体の 15%の製品については、対応状況が 0～20%と低く、特に第三種医療機器製造販売業許可取得者では 19%と高い傾向であった（設問 11)。
  - ✓ リスクマネジメント活動に従事できる力量を有する構成員の人数については、11 名以上と回答した会社が最も多く全体の 33%であった。一方で、1～3 名と回答した会社も全体の 31%と多く、特に第三種医療機器製造販売業許可取得者では 50%であり、リスクマネジメントの実施やサイバーセキュリティ対策を実施するにあたり、力量を有する実務者のリソース不足が懸念された（設問 12)。
  - ✓ 社内体制に関する手順書の整備については、全体の 74%の会社で完了しており、全体の 23%の会社で準備中であることから、手順書の整備は順調に進められていると考えられた。サイバーセキュリティ情報の評価体制の整備については、全体の 56%の会社で完了しており、全体の 39%の会社で準備中であることから、評価体制の整備についても概ね順調に進められていると考えられた。しかしながら、第三種医療機器製造販売業許可取得者においては、手順書の整備、評価体制の整備ともに、約 14%の会社で未着手とのことで、対応に遅れが生じていることが示唆された。（設問 13 及び 14)
  - ✓ サイバーセキュリティに関する必要な力量の明確化、教育訓練の実施及び力量の維持については、全体の 49%の会社で完了しており、全体の 36%の会社で準備中であることから、対応は概ね順調に進められていると考えられた。しかしながら、第三種医療機器製造販売業許可取得者においては、30%の会社で未着手とのことで、対応に遅れが生じていることが示唆された（設問 17)。
  - ✓ 製造販売中の製品に関する SBOM の作成状況については、全体の 90%の会社で作成完了又は準備中であり、概ね作成が進められていると考えられ

た。一方で、全体の 9%の会社で未着手であったことから、実務者のリソース不足に起因していることが示唆された（設問 15)。また、製造販売が終了した保守対象製品に関する SBOM の作成状況については、全体の 62%の会社で作成完了又は準備中であったが、全体の 39%の会社で未着手とのことで、製造販売中の製品に関する SBOM 作成に注力していることが示唆された（設問 16)。

- ✓ セキュリティリスクに関する情報収集、分析、修正等、一連の市販後対応の仕組みについては、全体の 63%の会社で完了し、30%の会社で準備中であった（設問 18)。第三者から製品の脆弱性に関する報告を受けることを想定して社内体制を整備している確認したところ、全体の 67%の会社で体制整備を完了しているとのことであった（設問 20)。一方で使用者から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るか確認したところ、全体の 43%の会社で入手していないとのことであった（設問 21)。既知の脆弱性に対する製品の影響を評価する仕組みについては、全体の 20%の会社で確立されていないとのことであった（設問 19)。セキュリティリスクに情報収集する体制は確立されつつも、受動的な情報収集の体制であり、能動的に情報収集するまでには至っておらず、また、製品への影響を評価する仕組みの整備に遅れが生じている可能性が示唆された。
- ✓ 脆弱性等に関する報告（IPA)、セキュリティリスク等に関連する不具合等報告に該当する仕組みについては、全体の 59%の会社で確立されており、28%の会社で準備中であった。しかしながら、第三種医療機器製造販売業許可取得者においては、26%の会社で未着手とのことで、対応に遅れが生じていることが示唆された（設問 22)。
- ✓ 製品の EOL/EOS の設定状況については、製造販売中の製品の全体の 35%の会社で設定済みであり、42%の会社は準備中で、22%の会社が未着手の状況であった（設問 25)。一方、製造販売の終了した保守対象製品は、全体の 42%の会社は設定済みであり、28%の会社は準備中で、30%の会社は未着手の状況であった（設問 26)。
- ✓ サイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みについては、全体の 58%の会社で確立済みであり、29%の会社で準備中、13%の会社で未着手の状況であった（設問 27)。特に、第三種医療機器製造販売業許可取得者においては、22%の会社で未着手とのことで、対応に遅れが生じていることが示唆された。
- ✓ セキュリティポリシーについては、全体の 59%の会社で定めており、25%の会社で準備中、16%の会社で未着手であった（設問 28)。また、セキュリティポリシーの使用者への開示については、全体の 44%の会社で開示に関する仕組みを確立しており、33%の会社で準備中、24%の会社で未着手の状況であった（設問 29)。セキュリティポリシーの設定は進んでいるものの、セキュリティポリシーの使用者への開示に関する仕組みの確

立は若干遅れ気味であることが示唆された。

- ✓ 開発段階で製品ソフトウェアの保守計画を作成する手順を確立しているかについては、全体の 57%の会社で確立済みであり、25%の会社で準備中、18%の会社で未着手の状況であった（設問 31）。製品ソフトウェアの保守計画の使用者への提示については、全体の 23%の会社で提示しており、32%の会社で準備であったが、45%の会社で未着手の状況であった（設問 32）。製品ソフトウェアの保守計画を開発段階で作成する意識は高いが、その保守計画を使用者に提示している会社は少ないことが示唆された。
- ✓ 製造販売中の製品に対する使用者への情報提供体制の整備については、全体の 63%の会社で完了しており、27%の会社で準備中、10%の会社で未着手であった（設問 33）。製造販売が終了した保守対象製品に対する使用者への情報提供体制の整備については、全体の 46%の会社で完了しており、25%の会社で準備中、29%の会社で未着手であった（設問 33）。製造販売業者として、製造販売中の製品への対応を優先しており、製造販売が終了した保守対象製品への対応が遅れていることが示唆された。
- ✓ 脆弱性等に関する使用者への情報提供に関して、PSIRT 等の製品セキュリティインシデント対応組織の設置については、全他の 40%の会社で設置しており、28%の会社で準備中、33%の会社で未設置の状況であった（設問 38）。脆弱性等に関するアドバイザリー情報の使用者への提供については、全体の 26%の会社で提供しており、30%の会社で準備中、44%の会社で未提供の状況であった（設問 37）。一方で、使用者から脆弱性等に対する対応状況の問合せやマルウェアによる感染確認等の依頼は、全体の 72%の会社で受けたことがなかった（設問 42）。また、問合せを受けた場合であっても、全体の 94%の会社で十分な対応ができたとの結果であった（設問 47）。製品セキュリティインシデント対応組織の設置は進められているが、使用者に対する脆弱性等に関するアドバイザリー情報の提供は遅れているものの、使用者からと問合せはアンケート実施時点において多くなく、問い合わせがあった場合でも十分な対応が図られていることが示唆された。
- ✓ 製品の納品時にネットワークに接続して使用することについて、全体の 73%の会社が使用者に確認していた（設問 53）。また、ネットワークに接続する場合は、サイバーセキュリティ確保のための対応が必要であることを、全体の 63%の会社が使用者へ通知していた（設問 54）。
- ✓ 使用者のネットワーク構成図の把握については、全体の 23%の会社で使用者側から開示されない等の理由により把握したいが把握できない状況であり、53%の会社が把握していない状況であった（設問 55）。また、医療機器サイバーセキュリティに関する保守契約を使用者と締結しているのは、全体の 17%の会社にとどまっており、83%の会社は保守契約を締結していなかった（設問 73）。医療機器の製造販売業者等と使用者（医療機関）がサイバーセキュリティに関する認識を合わせて、相互に連携、

情報共有を図り取り組んでいくことが重要ではないかと考えられた。

- ✓ 医療機器のサイバーセキュリティ対策についての課題としては、専門家の確保（全体の 28%）、専門家以外の教育（全体の 21%）、対策費用等（全体の 19%）、医療機関との連携・情報共有（全体の 18%）、リスクマネジメントの具体的方法（全体の 14%）の順で挙げられた（設問 76）。専門家の確保、教育訓練の実施等は、対策費用等につながることであり、製品のサイバーセキュリティに関するリスクに応じた対応が必要だと考えられた。また、上述したとおり、医療機器の製造販売業者等と使用者（医療機関）がサイバーセキュリティに関する認識を合わせて、相互に連携、情報共有を図り取り組んでいくことが重要ではないかと考えられた。

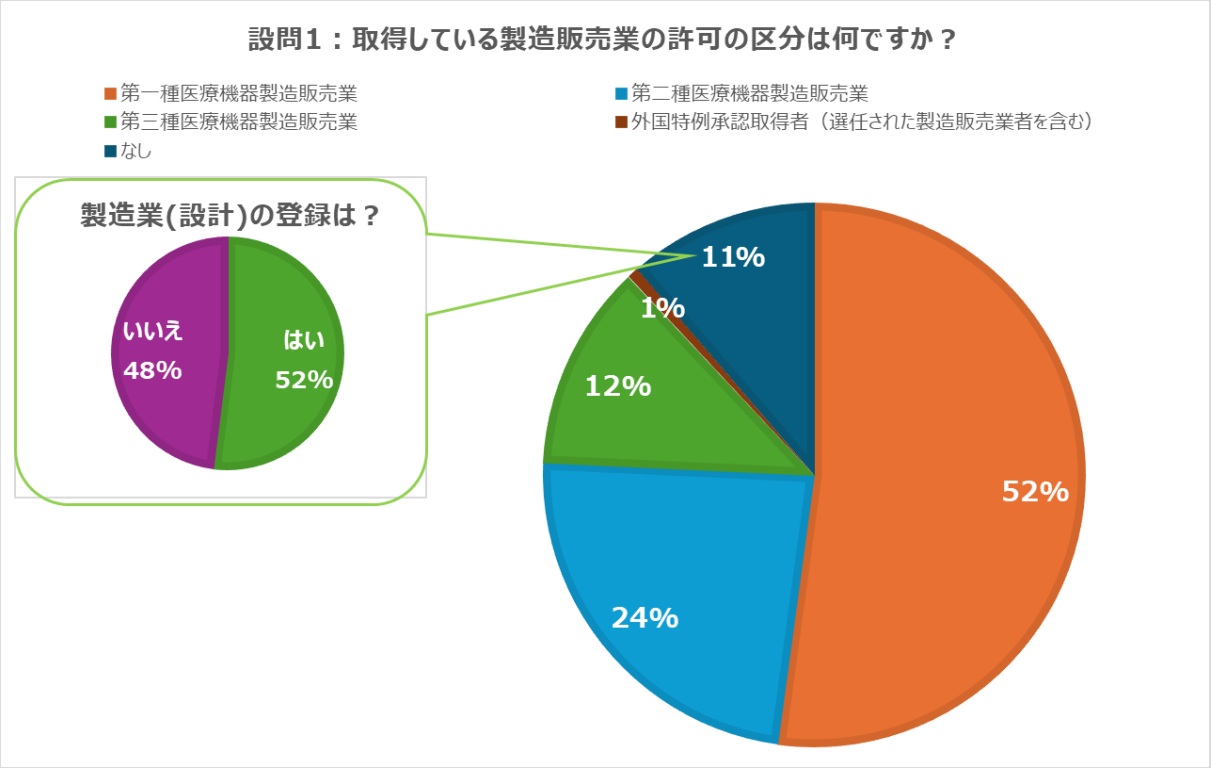
以上

**設問１：取得している製造販売業の許可の区分は何ですか？**

| 選択肢 | 回答数 |
|---|---|
| 第一種医療機器製造販売業 | 230 |
| 第二種医療機器製造販売業 | 104 |
| 第三種医療機器製造販売業 | 54 |
| 外国特例承認取得者（選任された製造販売業者を含む） | 3 |
| なし | 50 |
| 合計 | 441 |

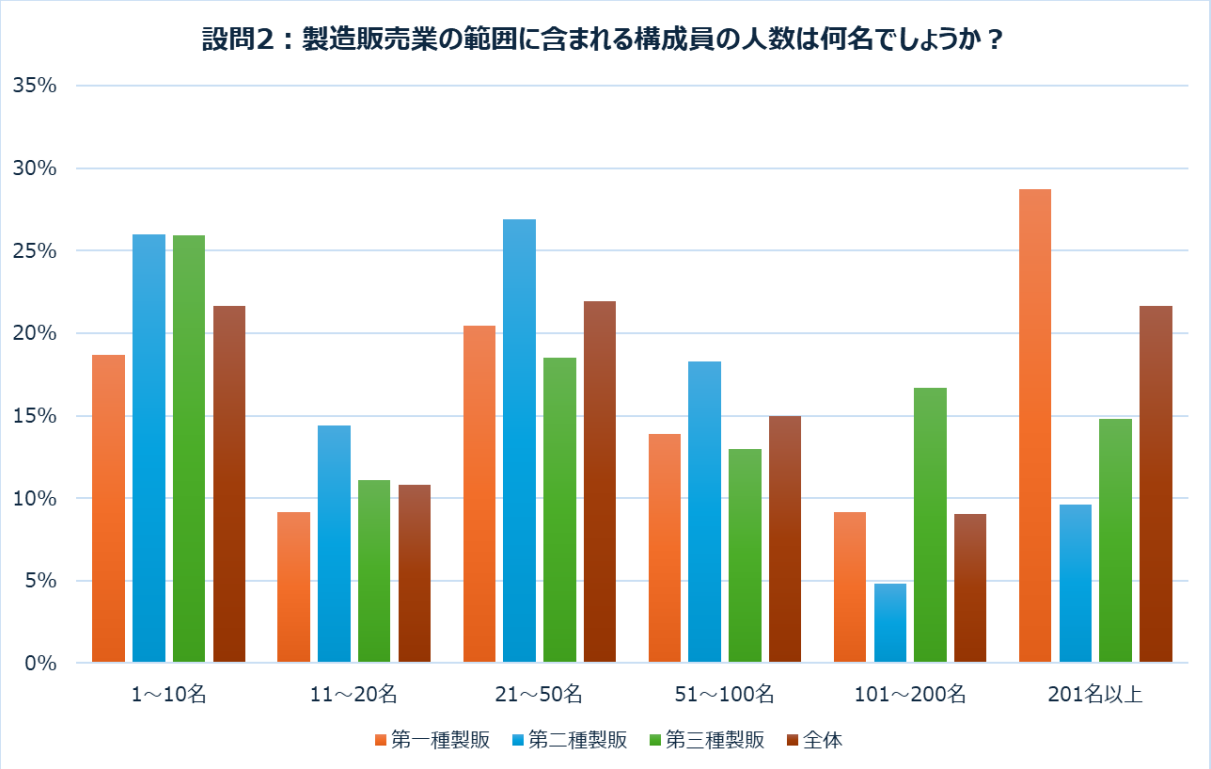
**設問３：設問１ で「なし」を選択された方にお尋ねします。製造業（設計）の登録は行っておられますか？**

| 選択肢 | 回答数 |
|---|---|
| はい | 26 |
| いいえ | 24 |
| | 50 |



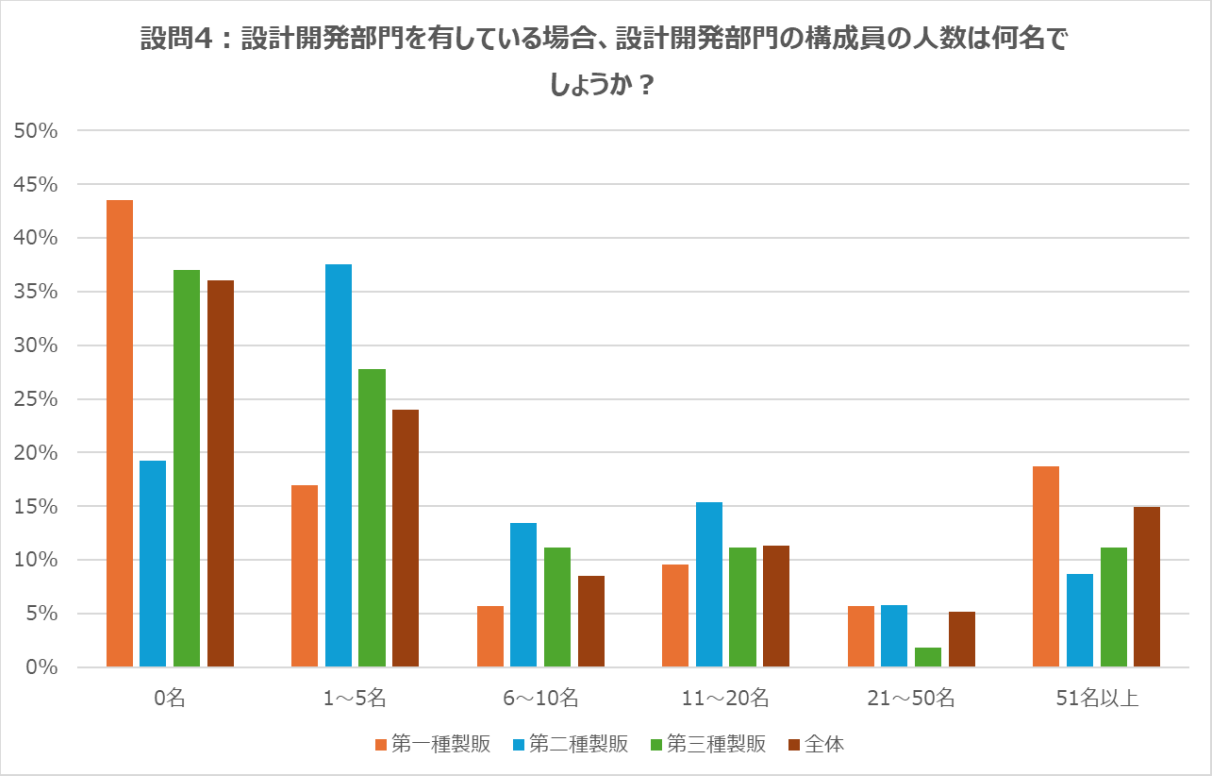
**設問 2：製造販売業の範囲に含まれる構成員の人数は何名でしょうか？**

| 選択肢 | 1～10 名 | 11～20 名 | 21～50 名 | 51 ～ 100 名 | 101～200 名 | 201 名以上 |
|---|---|---|---|---|---|---|
| 第一種製販 | 43 | 21 | 47 | 32 | 21 | 66 |
| 第二種製販 | 27 | 15 | 28 | 19 | 5 | 10 |
| 第三種製販 | 14 | 6 | 10 | 7 | 9 | 8 |
| 全体 | 84 | 42 | 85 | 58 | 35 | 84 |



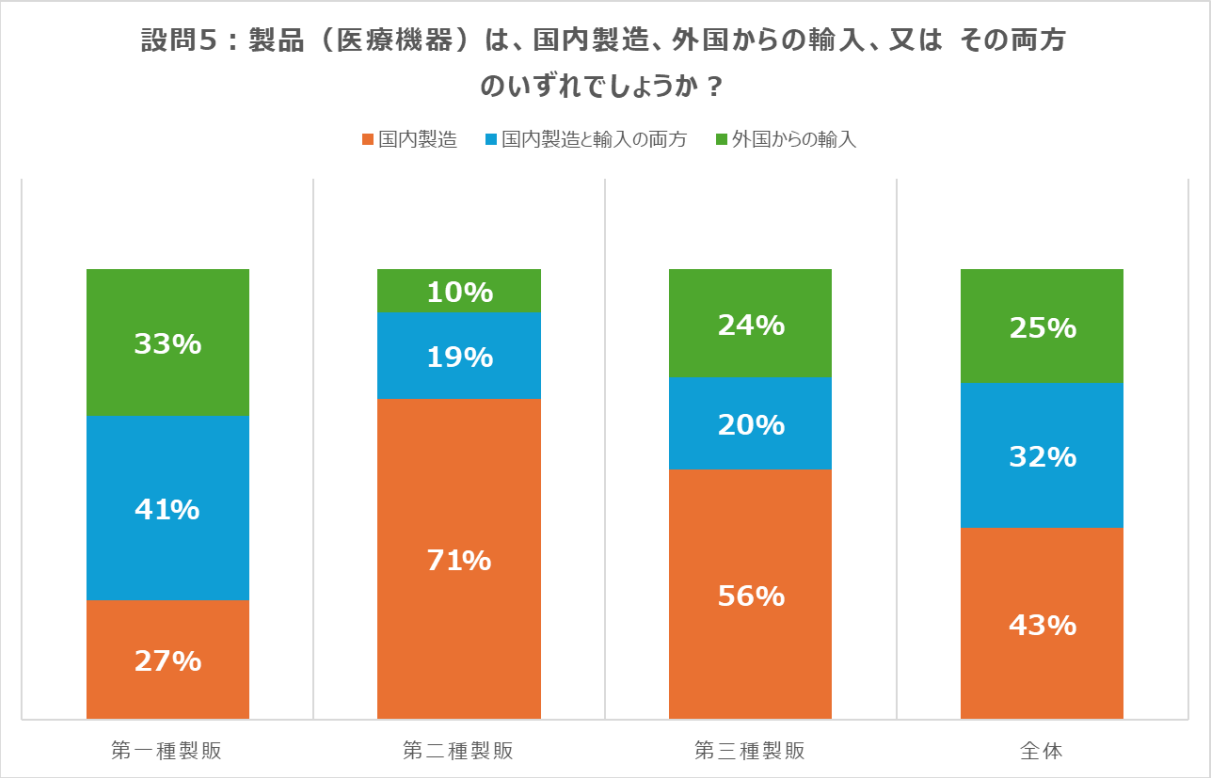
**設問 4：設計開発部門を有している場合、設計開発部門の構成員の人数は何名でしょうか？**

| 選択肢 | 設計開発部門なし（0 名） | 1～5 名 | 6～10 名 | 11 ～ 20 名 | 21 ～ 50 名 | 51 名以上 |
|---|---|---|---|---|---|---|
| 第一種製販 | 100 | 39 | 13 | 22 | 13 | 43 |
| 第二種製販 | 20 | 39 | 14 | 16 | 6 | 9 |
| 第三種製販 | 20 | 15 | 6 | 6 | 1 | 6 |
| 全体 | 140 | 93 | 33 | 44 | 20 | 58 |



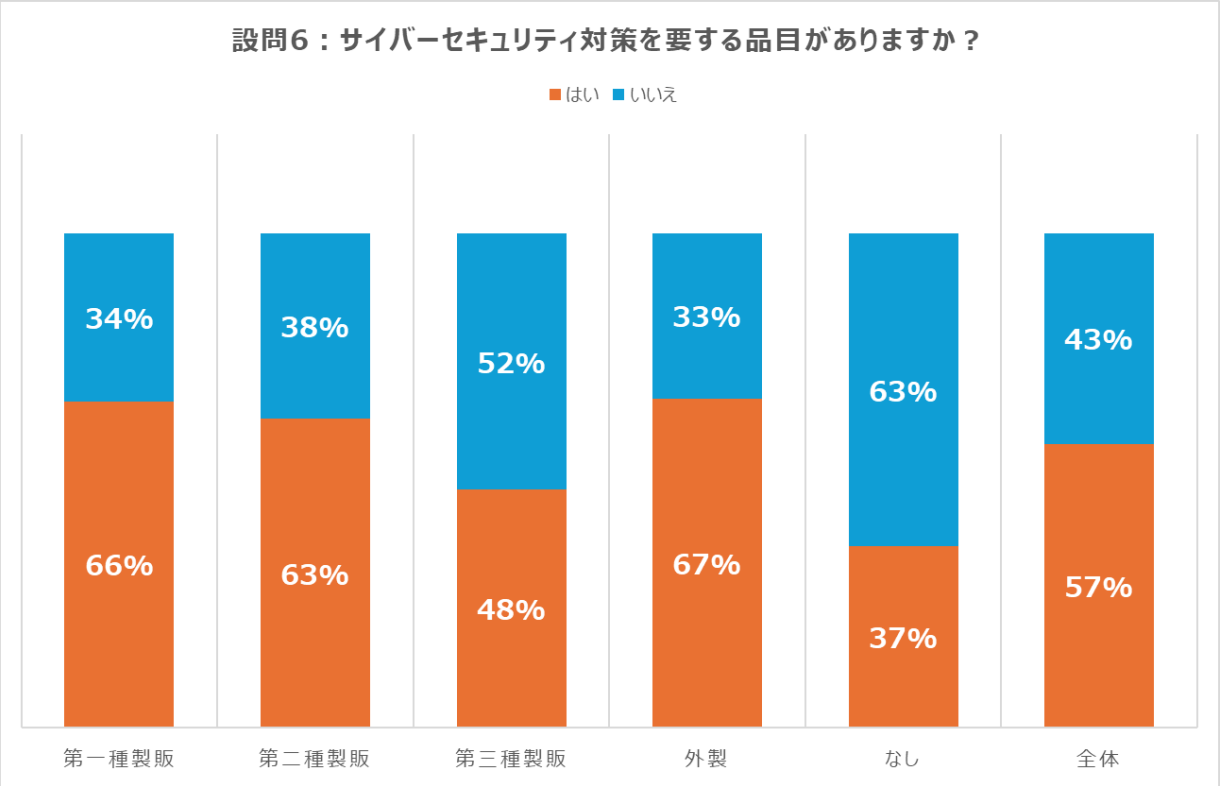
**設問５：製品（医療機器）は、国内製造、外国からの輸入、又は その両方 のいずれでしょうか？**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 |
|---|---|---|---|
| 国内製造 | 61 | 74 | 30 |
| 国内製造と輸入の両方 | 94 | 20 | 11 |
| 外国からの輸入 | 75 | 10 | 13 |
| 全体 | 230 | 104 | 54 |



**設問 6：サイバーセキュリティ対策を要する品目（製造販売している又は製造販売は終了したが、使用が継続している）がありますか？**

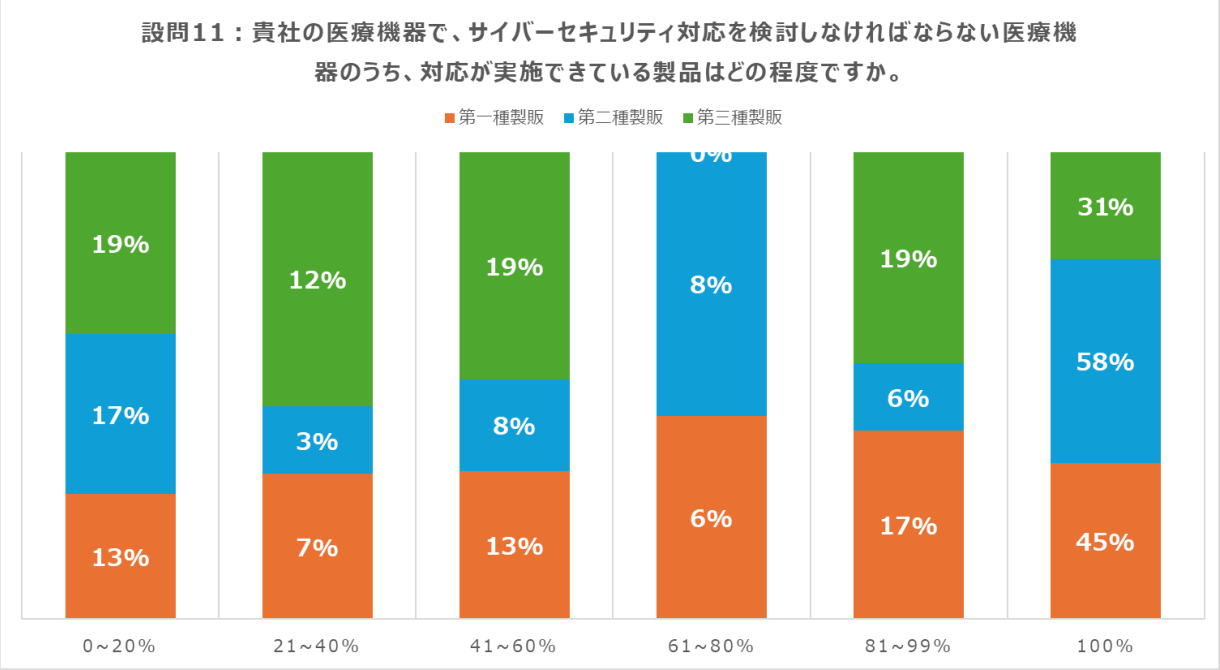
| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 外製 | なし |
|---|---|---|---|---|---|
| はい | 152 | 65 | 26 | 2 | 11 |
| いいえ | 78 | 39 | 28 | 1 | 19 |



**設問 11：貴社の全製品（医療機器）のうち、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、対応が実施できている製品はどの程度ですか。**

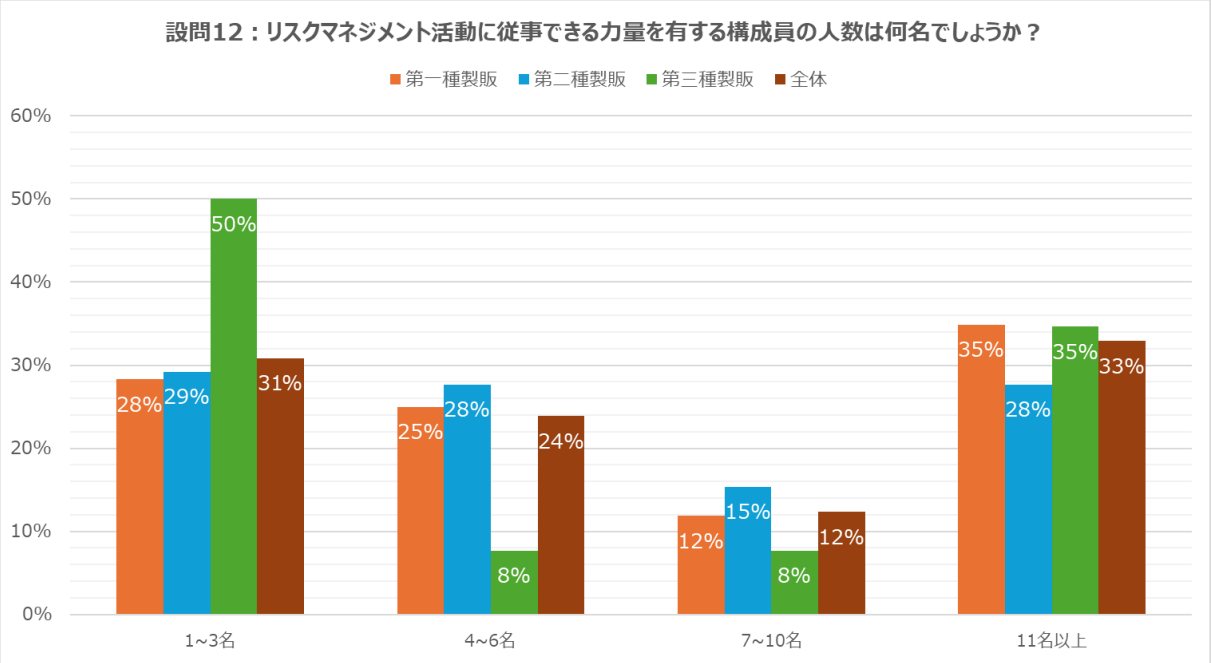
| 選択肢 | 0~20% | 21~40% | 41~60% | 61~80% | 81~99% | 100% |
|---|---|---|---|---|---|---|
| 第一種製販 | 20 | 10 | 19 | 6 | 21 | 49 |
| 第二種製販 | 5 | 2 | 4 | 5 | 4 | 29 |
| 第三種製販 | 4 | 3 | 1 | 0 | 4 | 7 |
| 外製・選任製販 | 0 | 0 | 1 | 0 | 0 | 1 |
| なし | 1 | 0 | 0 | 0 | 0 | 2 |

※　サンプルサイズが 5 件のため、外製・選任製販及びなしについては、設問 12 以降の集計から除いた。



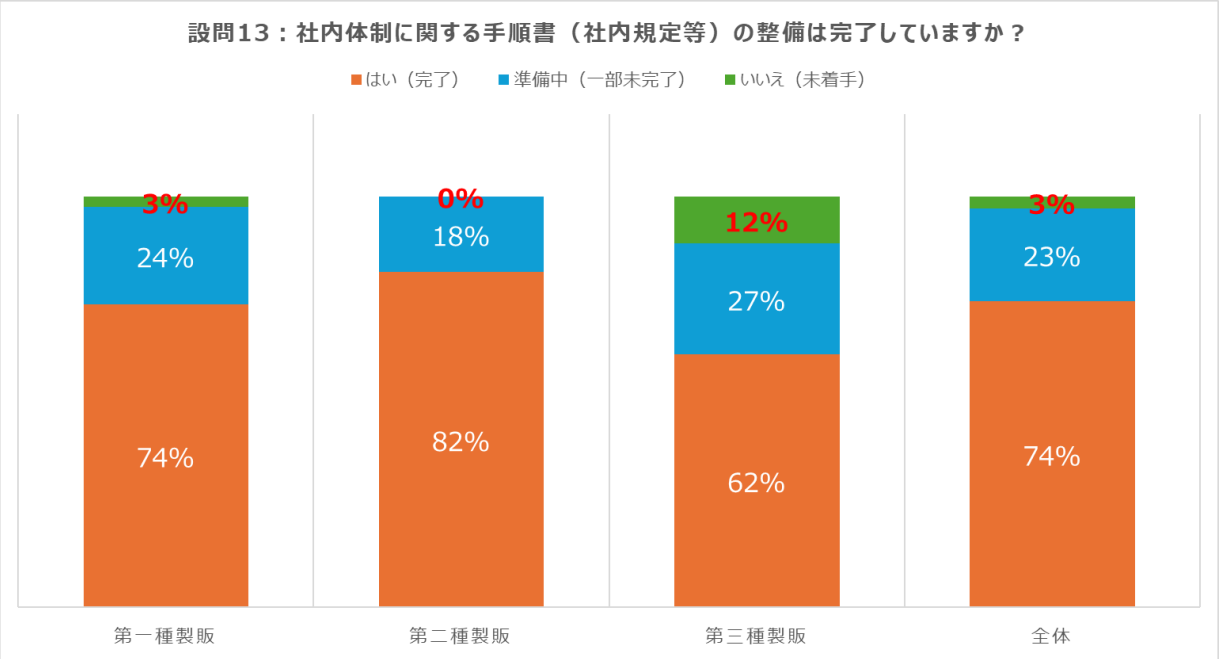
**設問 12：リスクマネジメント活動に従事できる力量を有する構成員の人数は何名でしょうか？**

| 選択肢 | 1~3 名 | 4~6 名 | 7~10 名 | 11 名以上 | 全体 |
|---|---|---|---|---|---|
| 第一種製販 | 43 | 38 | 18 | 53 | 152 |
| 第二種製販 | 19 | 18 | 10 | 18 | 65 |
| 第三種製販 | 13 | 2 | 2 | 9 | 26 |



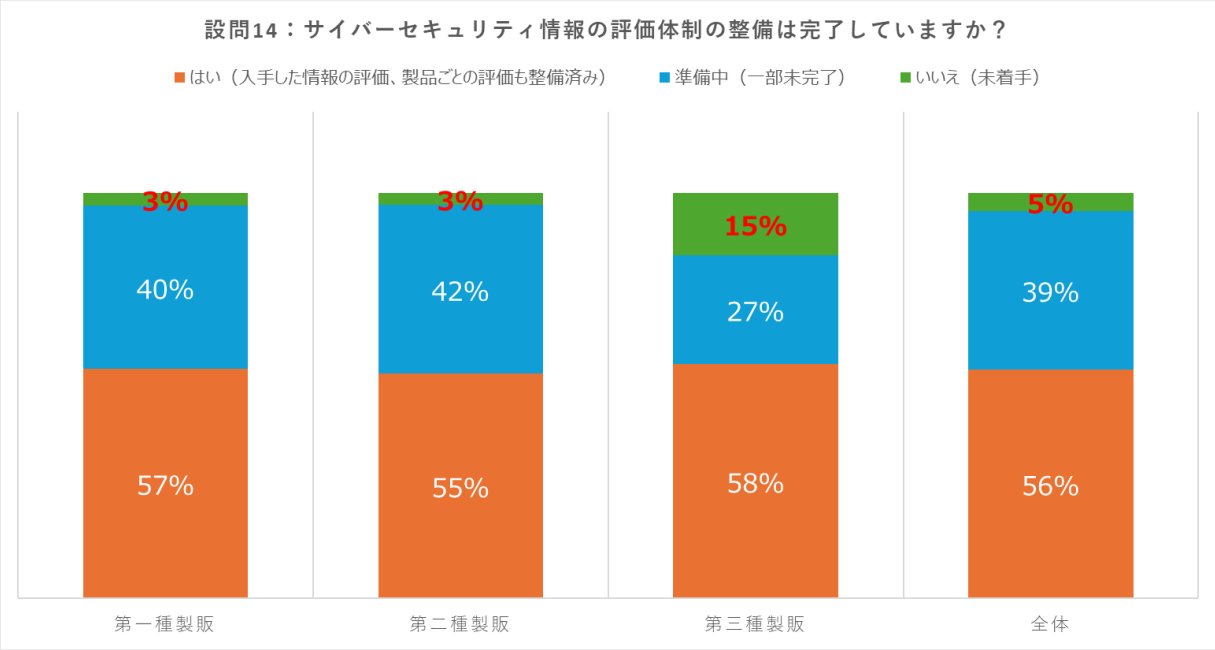
**設問 13：社内体制に関する手順書（社内規定等）の整備は完了していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 112 | 36 | 4 |
| 第二種製販 | 53 | 12 | 0 |
| 第三種製販 | 16 | 7 | 3 |
| 全体 | 181 | 55 | 7 |



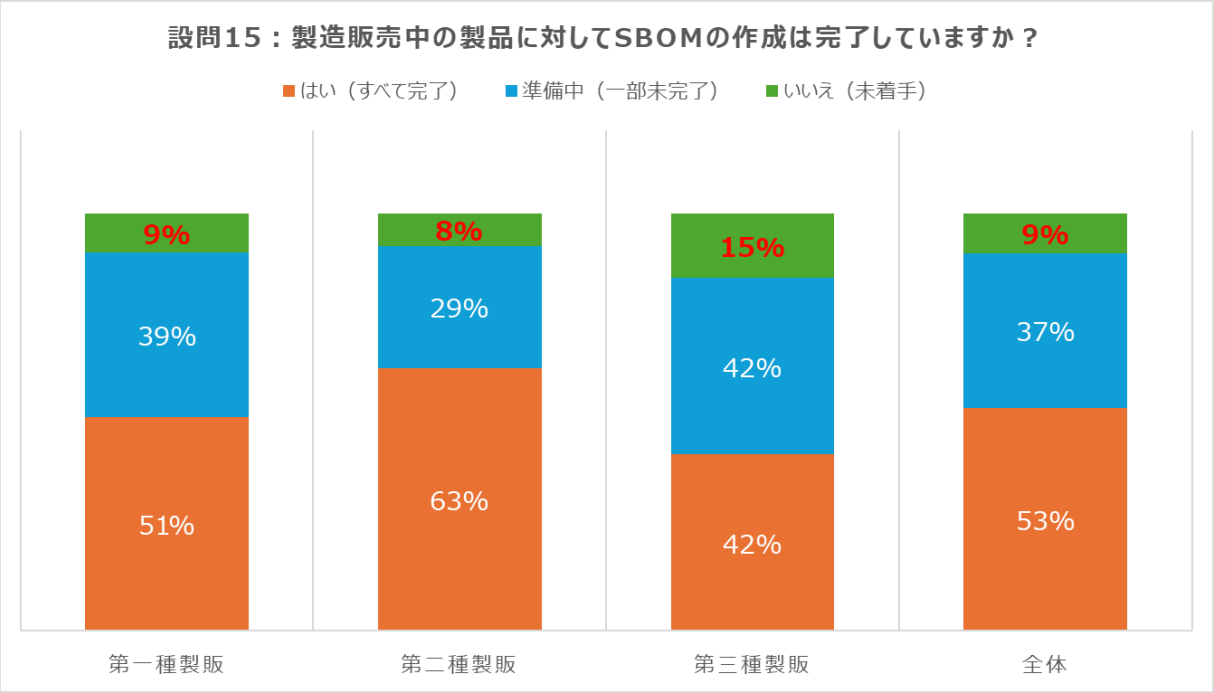
**設問 14：サイバーセキュリティ情報の評価体制の整備は完了していますか？**

| 選択肢 | はい（入手した情報の評価、製品ごとの評価も整備済み） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 86 | 61 | 5 |
| 第二種製販 | 36 | 27 | 2 |
| 第三種製販 | 15 | 7 | 4 |
| 全体 | 137 | 95 | 11 |



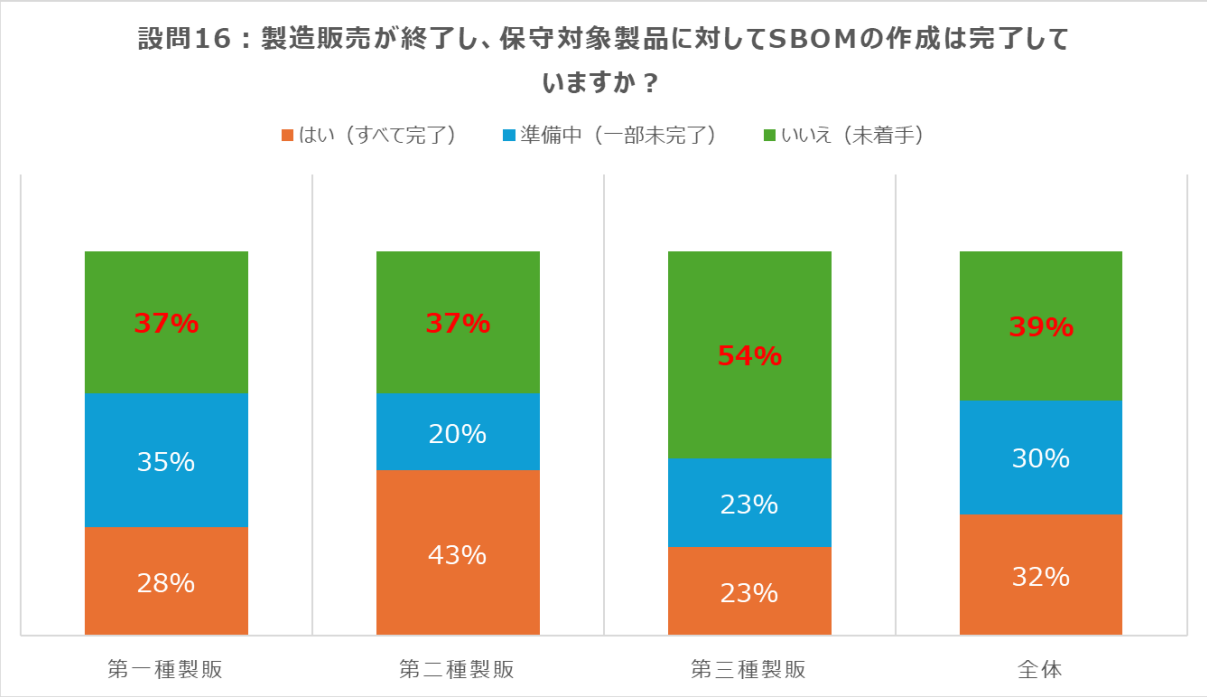
**設問 15：製造販売中の製品に対して SBOM の作成は完了していますか？**

| 選択肢 | はい（すべて完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 78 | 60 | 14 |
| 第二種製販 | 41 | 19 | 5 |
| 第三種製販 | 11 | 11 | 4 |
| 全体 | 130 | 90 | 23 |



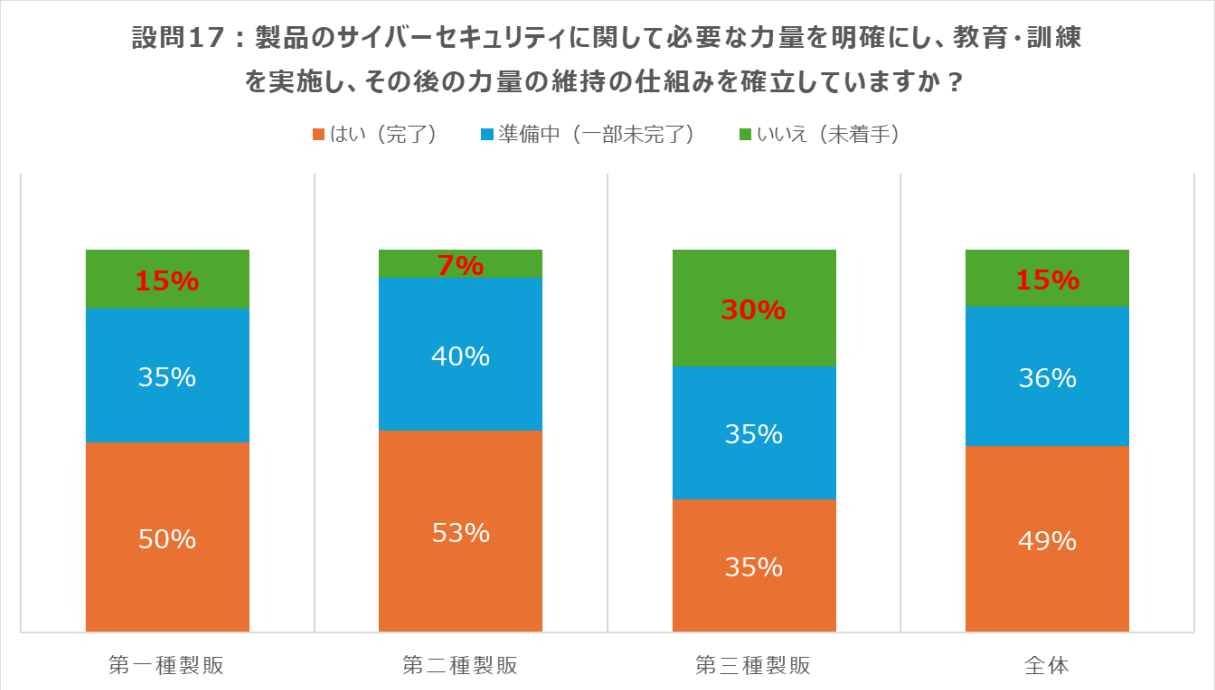
**設問 16：製造販売が終了し、保守対象製品に対して SBOM の作成は完了していますか？**

| 選択肢 | はい（すべて完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 43 | 53 | 56 |
| 第二種製販 | 28 | 13 | 24 |
| 第三種製販 | 6 | 6 | 14 |
| 全体 | 77 | 72 | 94 |



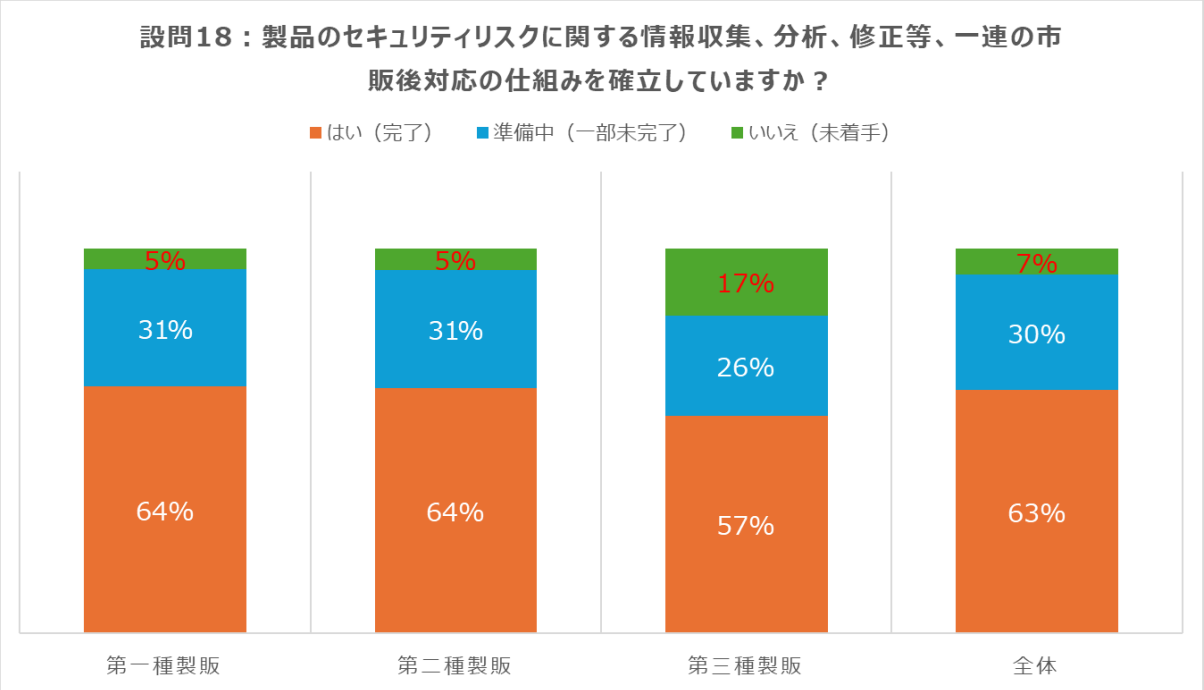
**設問 17：製品のサイバーセキュリティに関して必要な力量を明確にし、教育・訓練を実施し、その後の力量の維持の仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 65 | 46 | 20 |
| 第二種製販 | 29 | 22 | 4 |
| 第三種製販 | 8 | 8 | 7 |
| 全体 | 102 | 76 | 31 |



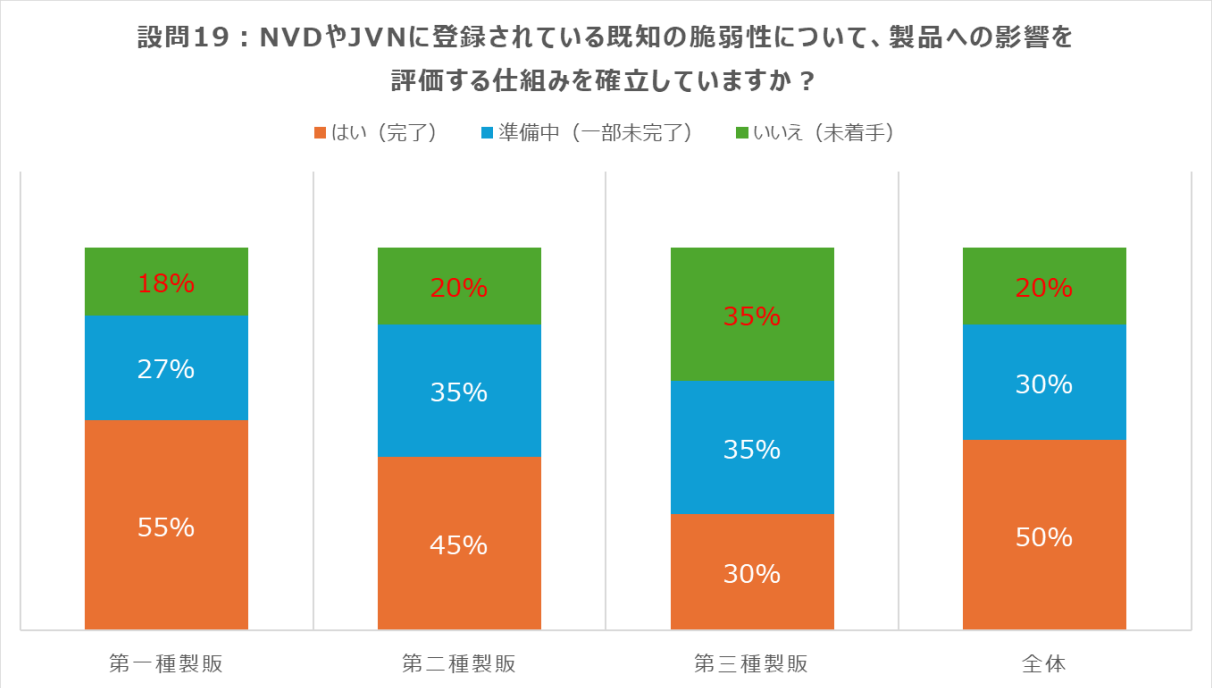
**設問 18：製品のセキュリティリスクに関する情報収集、分析、修正等、一連の市販後対応の仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 84 | 40 | 7 |
| 第二種製販 | 35 | 17 | 3 |
| 第三種製販 | 13 | 6 | 4 |
| 全体 | 132 | 63 | 14 |



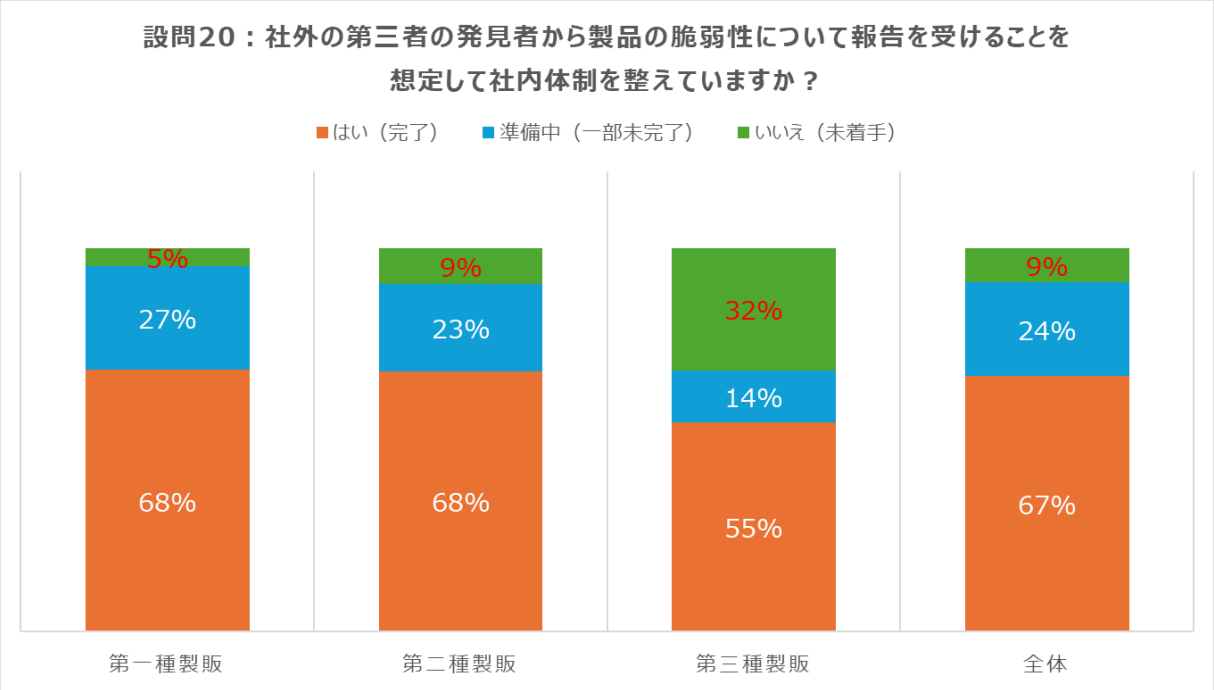
**設問 19：NVD や JVN に登録されている既知の脆弱性について、製品への影響を評価する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 72 | 36 | 23 |
| 第二種製販 | 25 | 19 | 11 |
| 第三種製販 | 7 | 8 | 8 |
| 全体 | 104 | 63 | 42 |



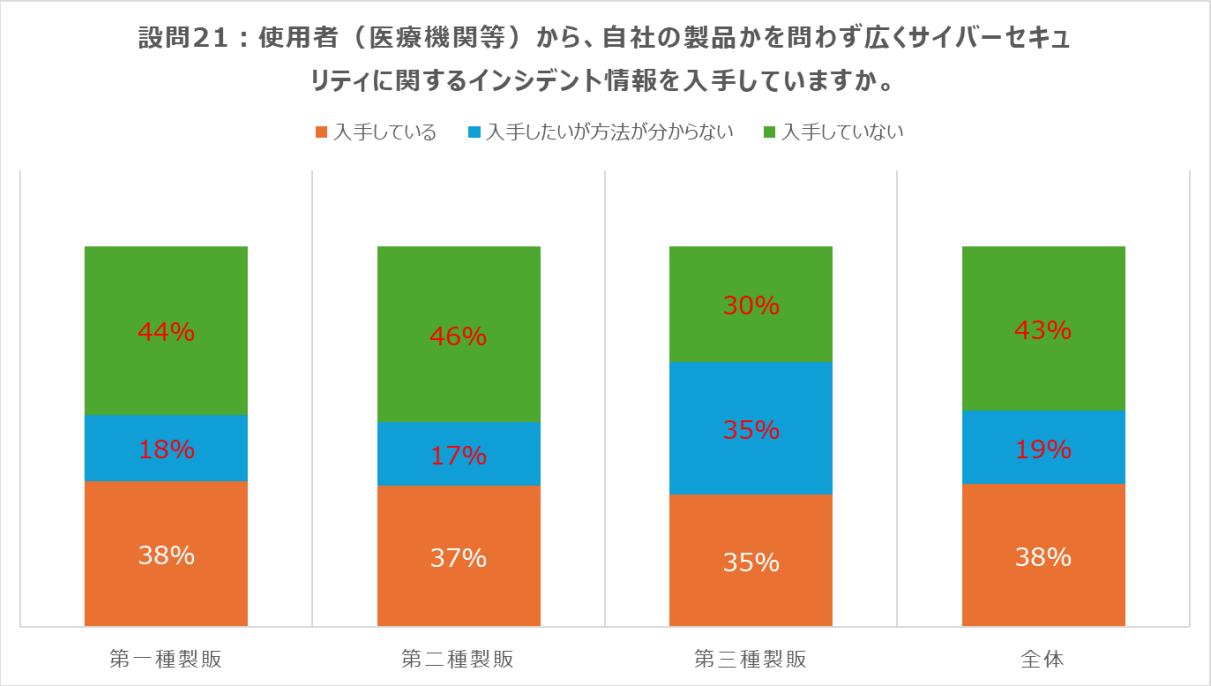
**設問 20：社外の第三者の発見者から製品の脆弱性について報告を受けることを想定して社内体制を整えていますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 86 | 34 | 6 |
| 第二種製販 | 36 | 12 | 5 |
| 第三種製販 | 12 | 3 | 7 |
| 全体 | 134 | 49 | 18 |



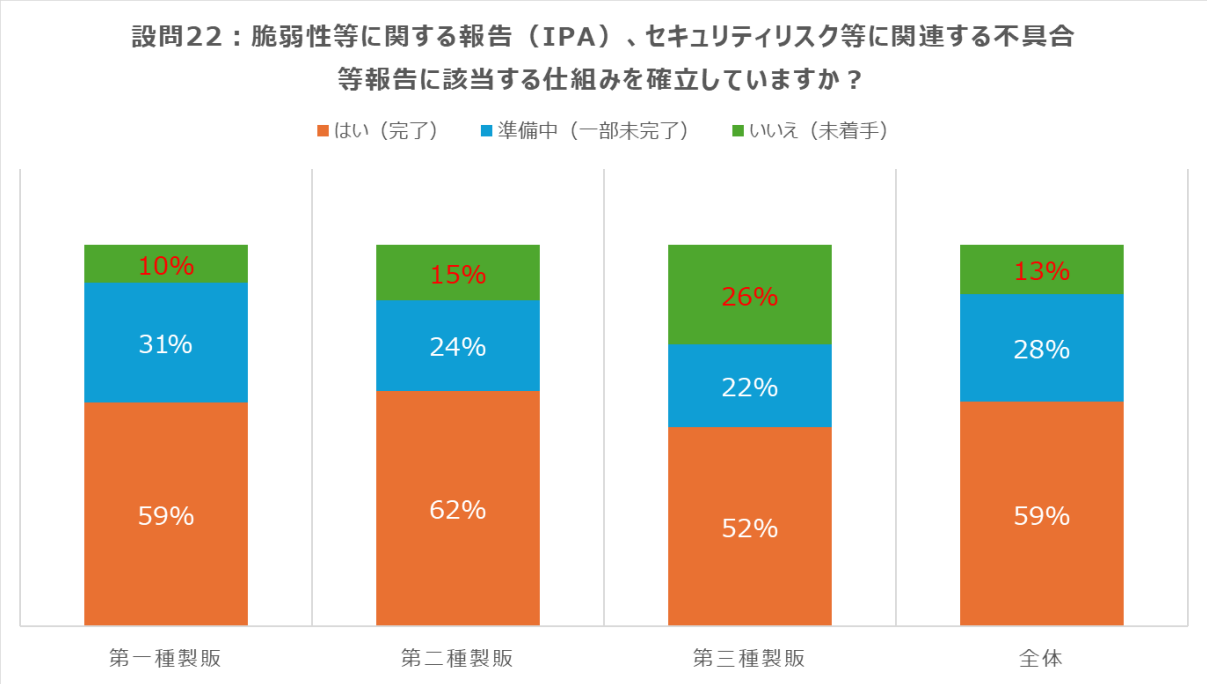
**設問 21：使用者（医療機関等）から、自社の製品かを問わず広くサイバーセキュリティに関するインシデント情報を入手していますか。**

| 選択肢 | 入手している | 入手したいが方法が分からない | 入手していない |
|---|---|---|---|
| 第一種製販 | 50 | 23 | 58 |
| 第二種製販 | 20 | 9 | 25 |
| 第三種製販 | 8 | 8 | 7 |
| 全体 | 78 | 40 | 90 |



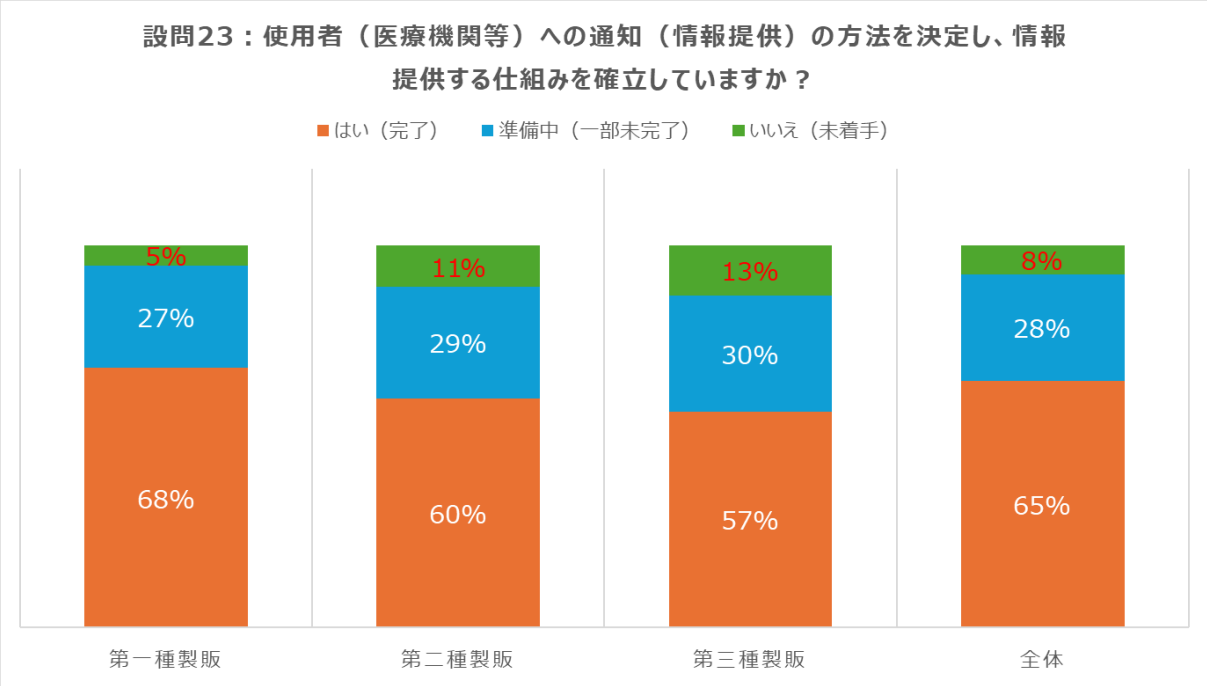
**設問 22：脆弱性等に関する報告（IPA）、セキュリティリスク等に関連する不具合等報告に該当する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 77 | 41 | 13 |
| 第二種製販 | 34 | 13 | 8 |
| 第三種製販 | 12 | 5 | 6 |
| 全体 | 123 | 59 | 27 |



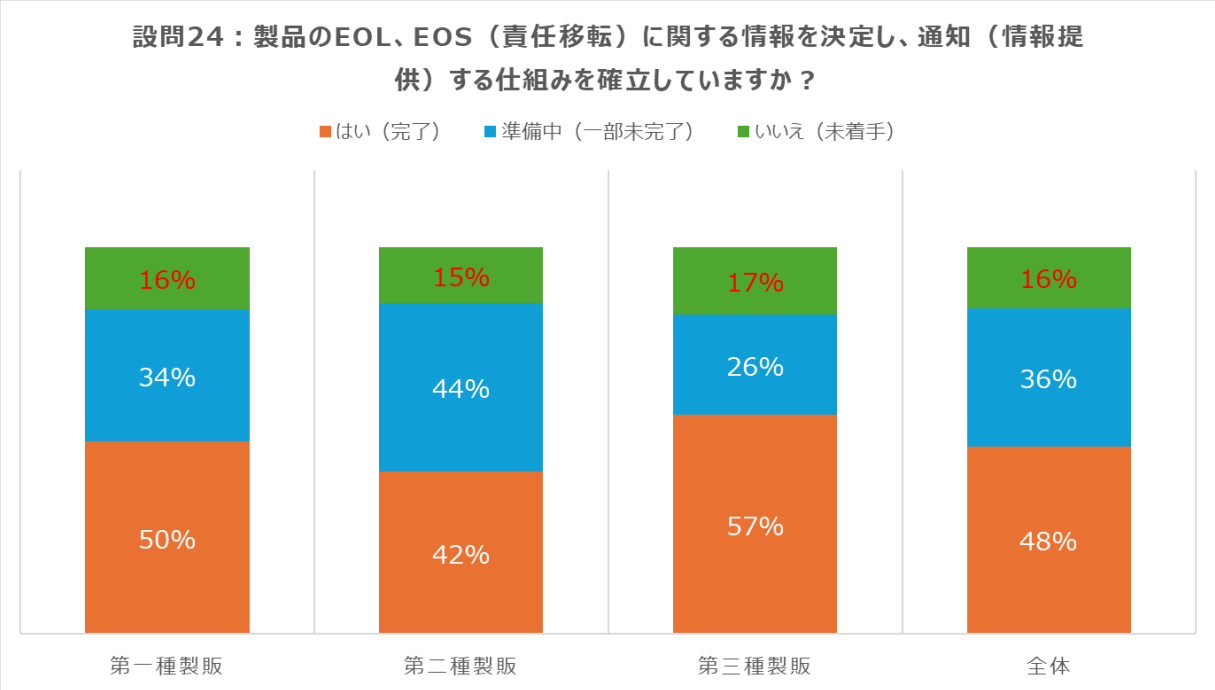
**設問 23：使用者（医療機関等）への通知（情報提供）の方法を決定し、情報提供する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 89 | 35 | 7 |
| 第二種製販 | 33 | 16 | 6 |
| 第三種製販 | 13 | 7 | 3 |
| 全体 | 135 | 58 | 16 |



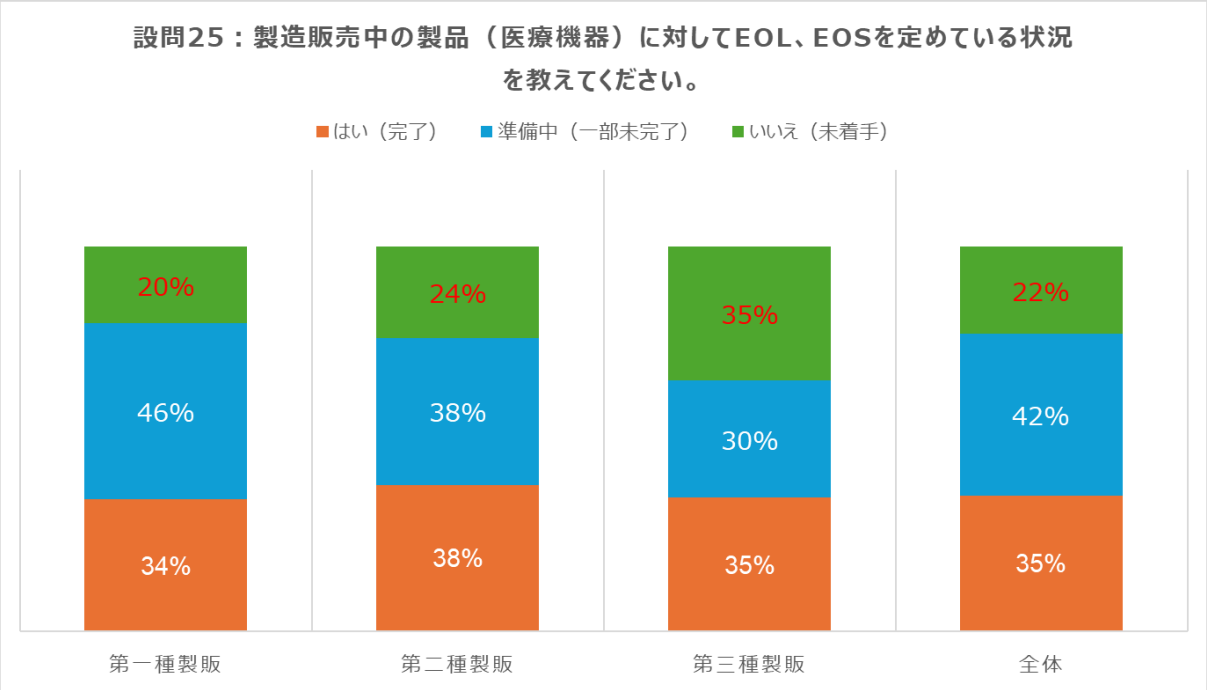
**設問 24：製品の EOL、EOS（責任移転）に関する情報を決定し、通知（情報提供）する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 65 | 45 | 21 |
| 第二種製販 | 23 | 24 | 8 |
| 第三種製販 | 13 | 6 | 4 |
| 全体 | 101 | 75 | 33 |



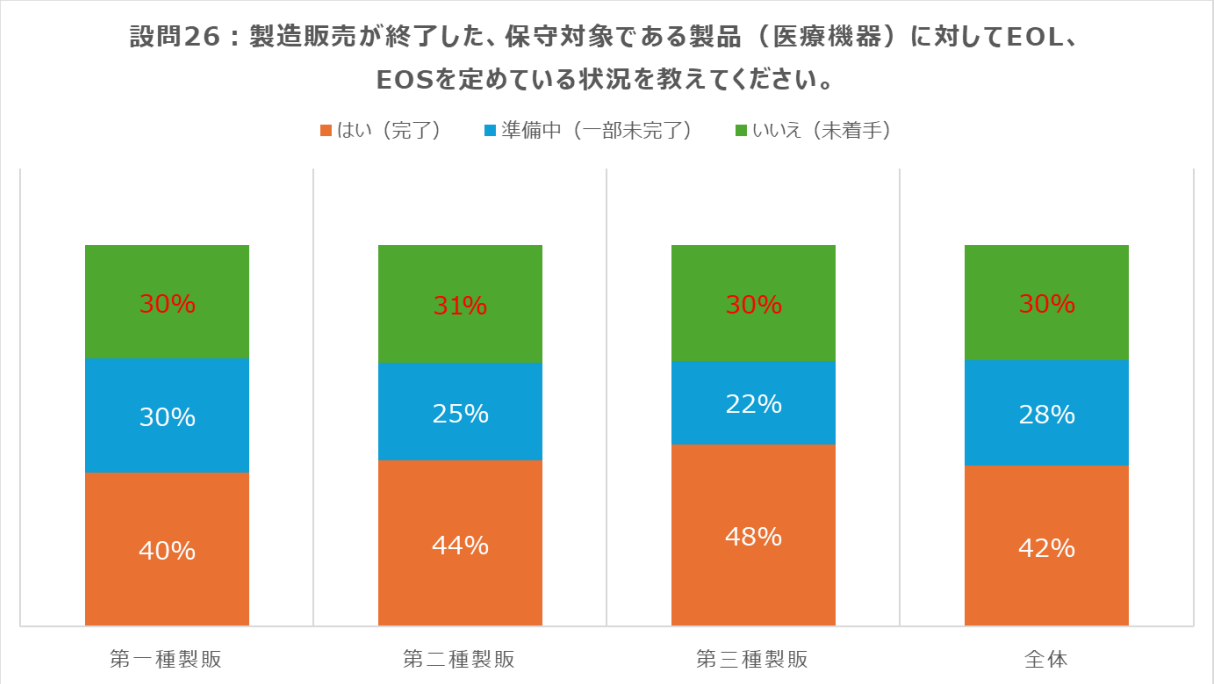
**設問 25：製造販売中の製品（医療機器）に対して EOL、EOS を定めている状況を教えてください。**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 45 | 60 | 26 |
| 第二種製販 | 21 | 21 | 13 |
| 第三種製販 | 8 | 7 | 8 |
| 全体 | 74 | 88 | 47 |



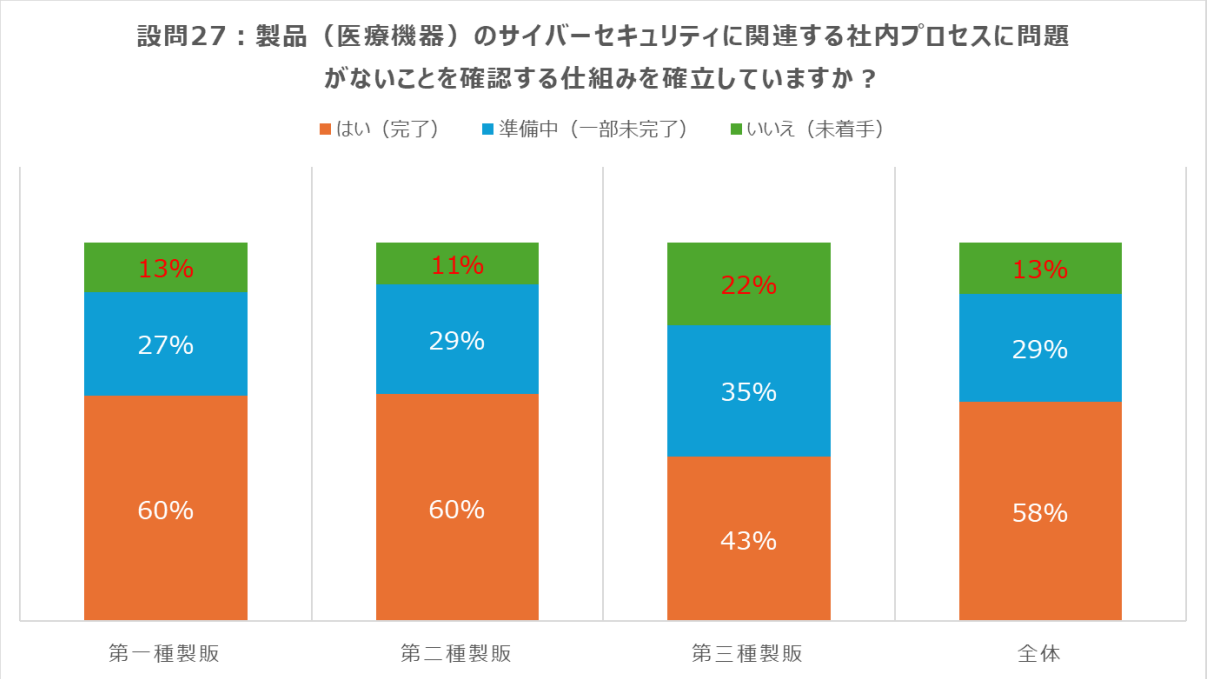
**設問 26：製造販売が終了した、保守対象である製品（医療機器）に対して EOL、EOS を定めている状況を教えてください。**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 53 | 39 | 39 |
| 第二種製販 | 24 | 14 | 17 |
| 第三種製販 | 11 | 5 | 7 |
| 全体 | 88 | 58 | 63 |



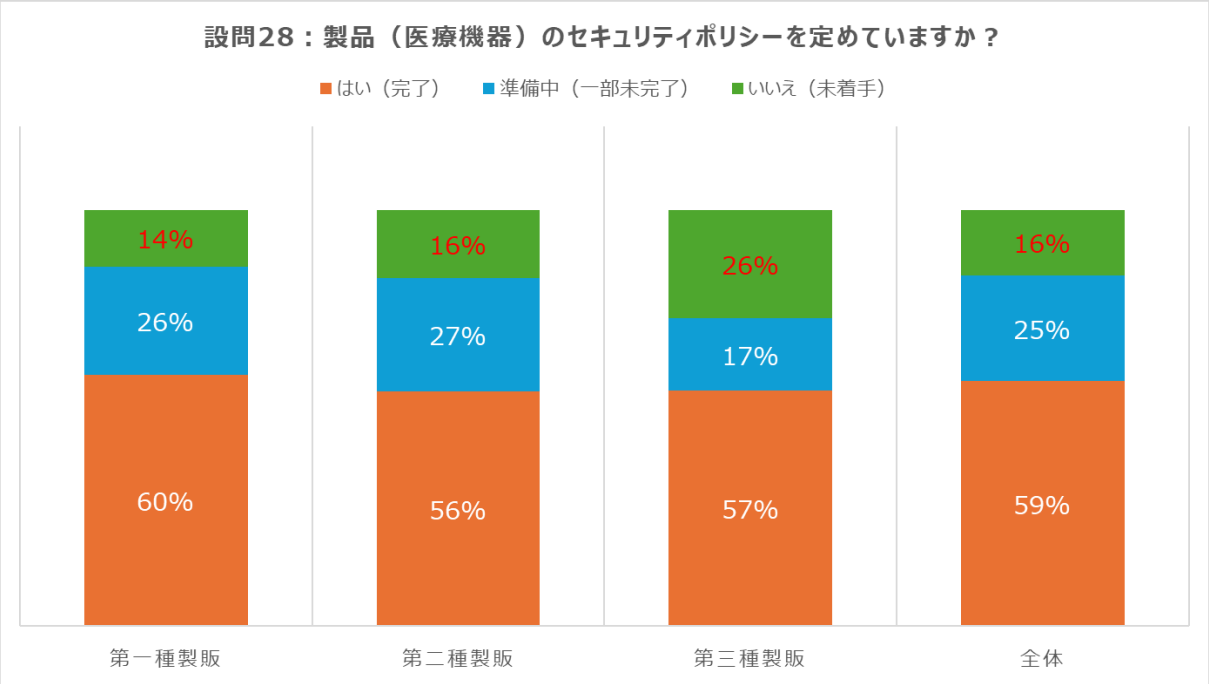
**設問 27：製品（医療機器）のサイバーセキュリティに関連する社内プロセスに問題がないことを確認する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 78 | 36 | 17 |
| 第二種製販 | 33 | 16 | 6 |
| 第三種製販 | 10 | 8 | 5 |
| 全体 | 121 | 60 | 28 |



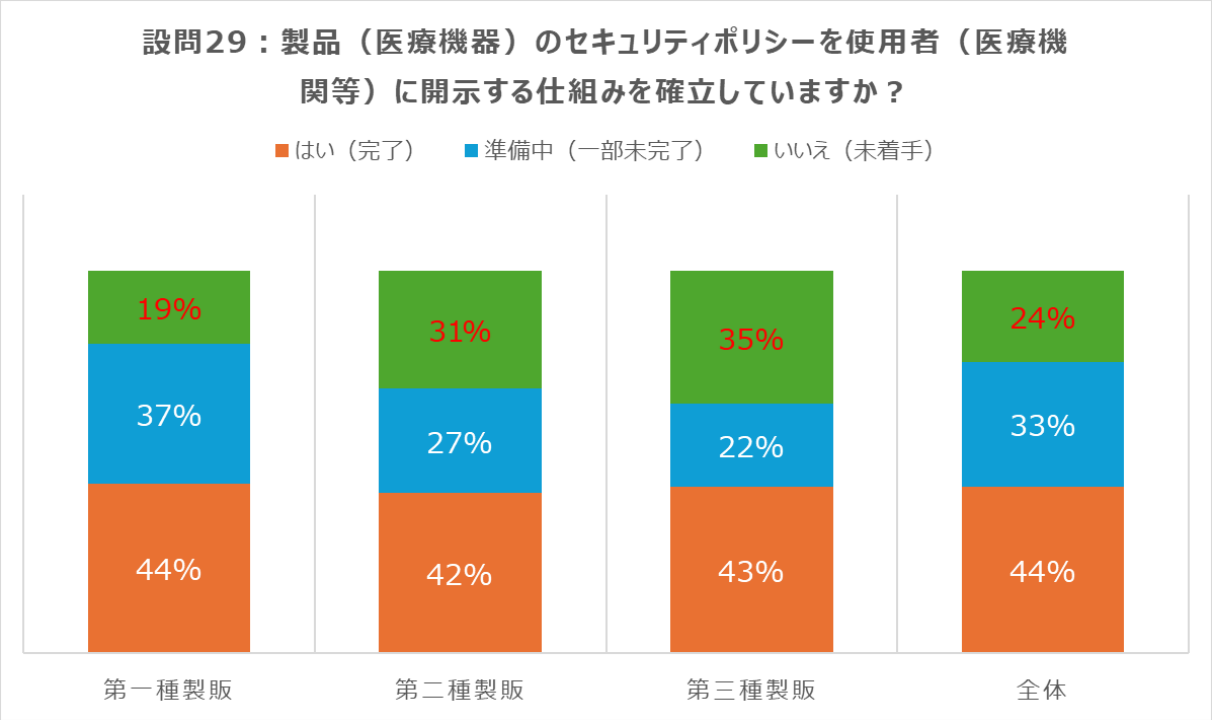
**設問 28：製品（医療機器）のセキュリティポリシーを定めていますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 79 | 34 | 18 |
| 第二種製販 | 31 | 15 | 9 |
| 第三種製販 | 13 | 4 | 6 |
| 全体 | 123 | 53 | 33 |



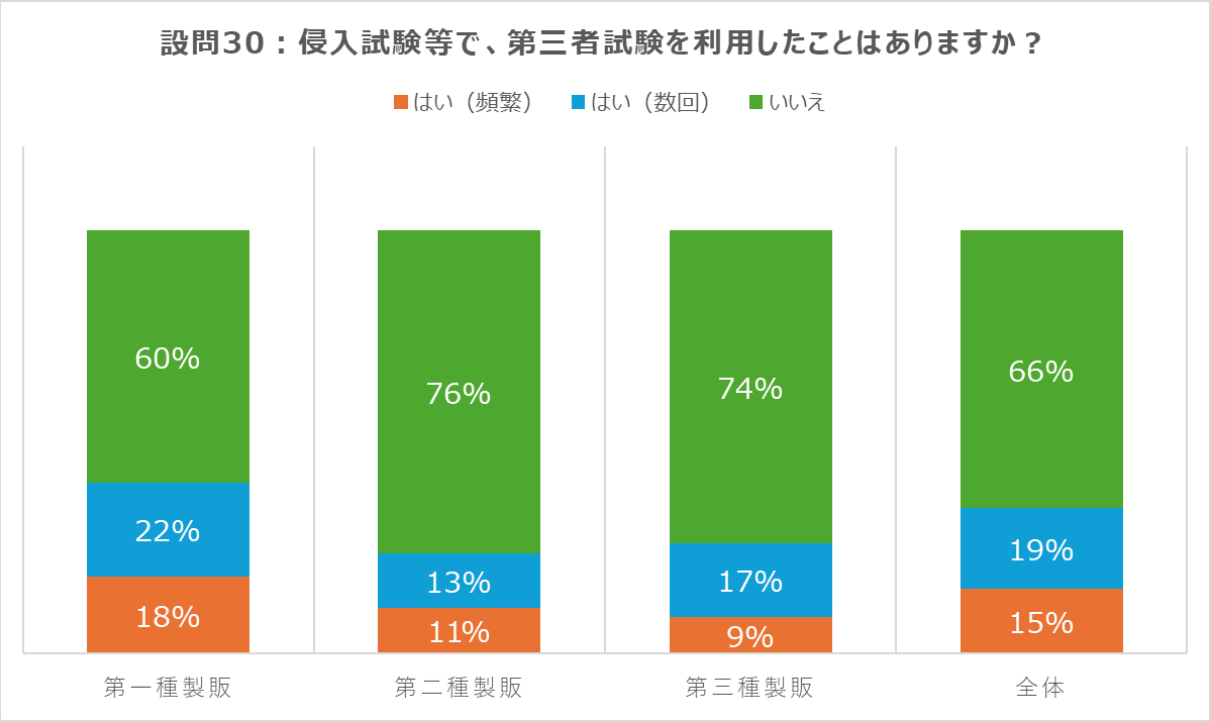
**設問 29：製品（医療機器）のセキュリティポリシーを使用者（医療機関等）に開示する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 58 | 48 | 25 |
| 第二種製販 | 23 | 15 | 17 |
| 第三種製販 | 10 | 5 | 8 |
| 全体 | 91 | 68 | 50 |



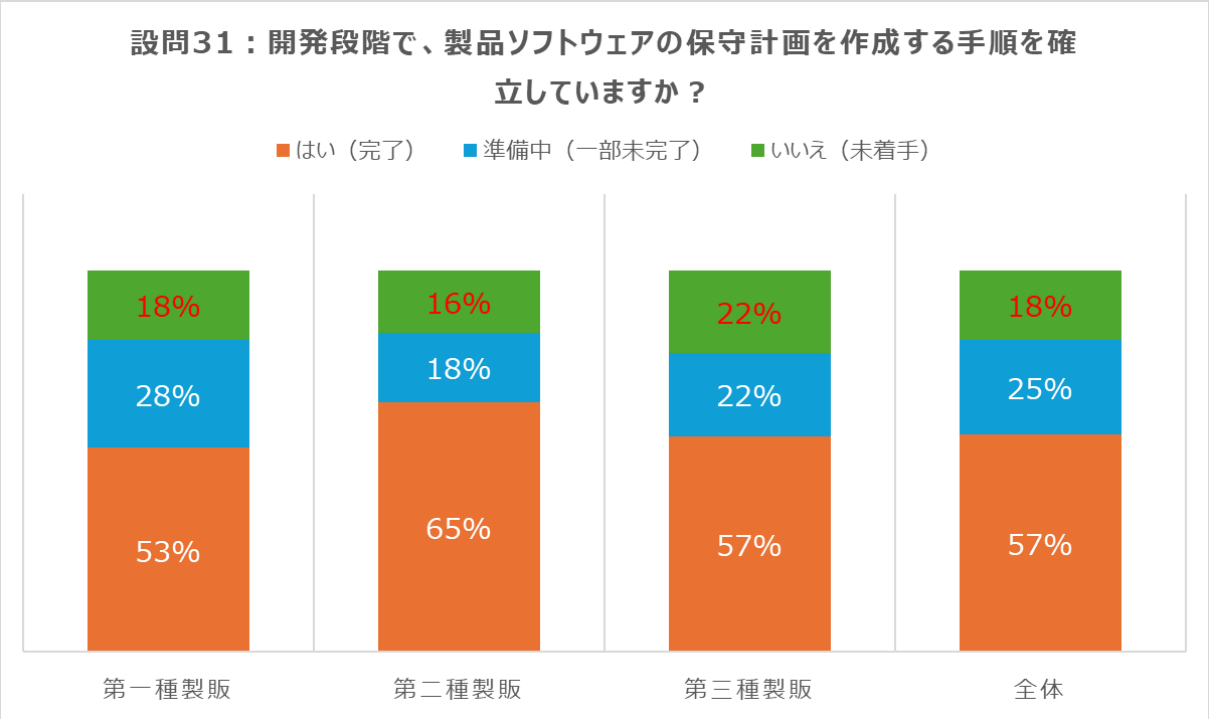
**設問 30：侵入試験等で、第三者試験を利用したことはありますか？**

| 選択肢 | はい（頻繁） | はい（数回） | いいえ |
|---|---|---|---|
| 第一種製販 | 24 | 29 | 78 |
| 第二種製販 | 6 | 7 | 42 |
| 第三種製販 | 2 | 4 | 17 |
| 全体 | 32 | 40 | 137 |



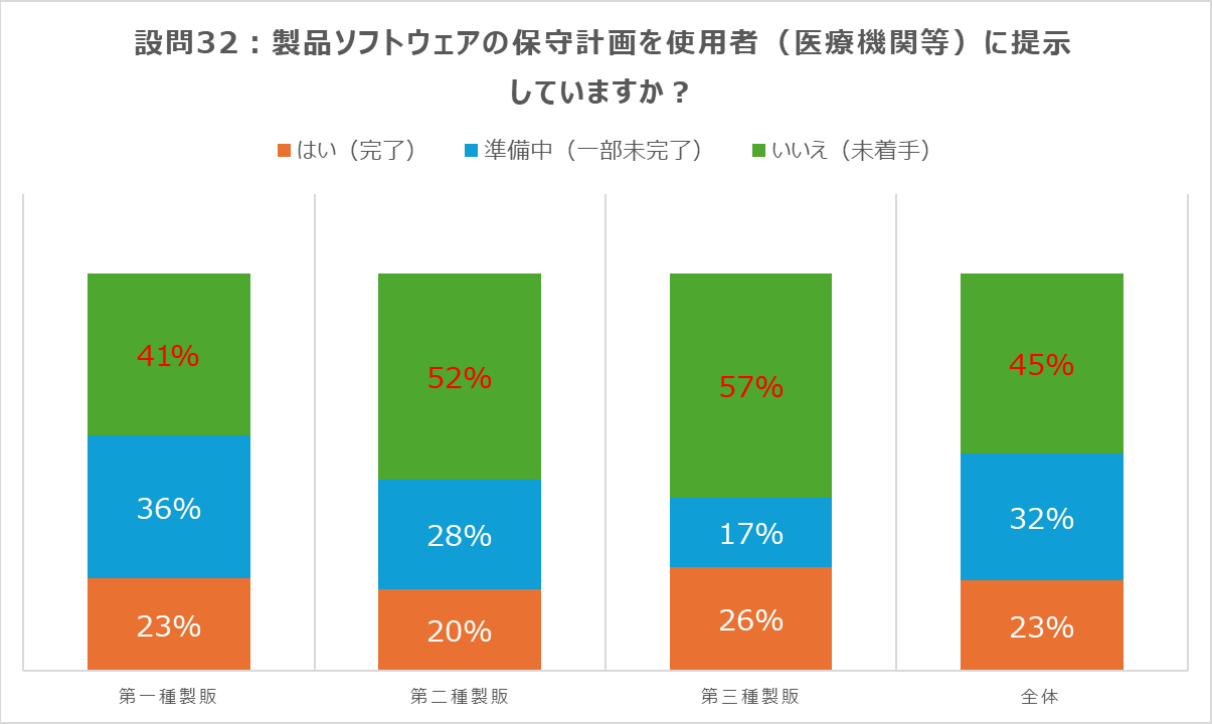
**設問 31：開発段階で、製品ソフトウェアの保守計画を作成する手順を確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 70 | 37 | 24 |
| 第二種製販 | 36 | 10 | 9 |
| 第三種製販 | 13 | 5 | 5 |
| 全体 | 119 | 52 | 38 |



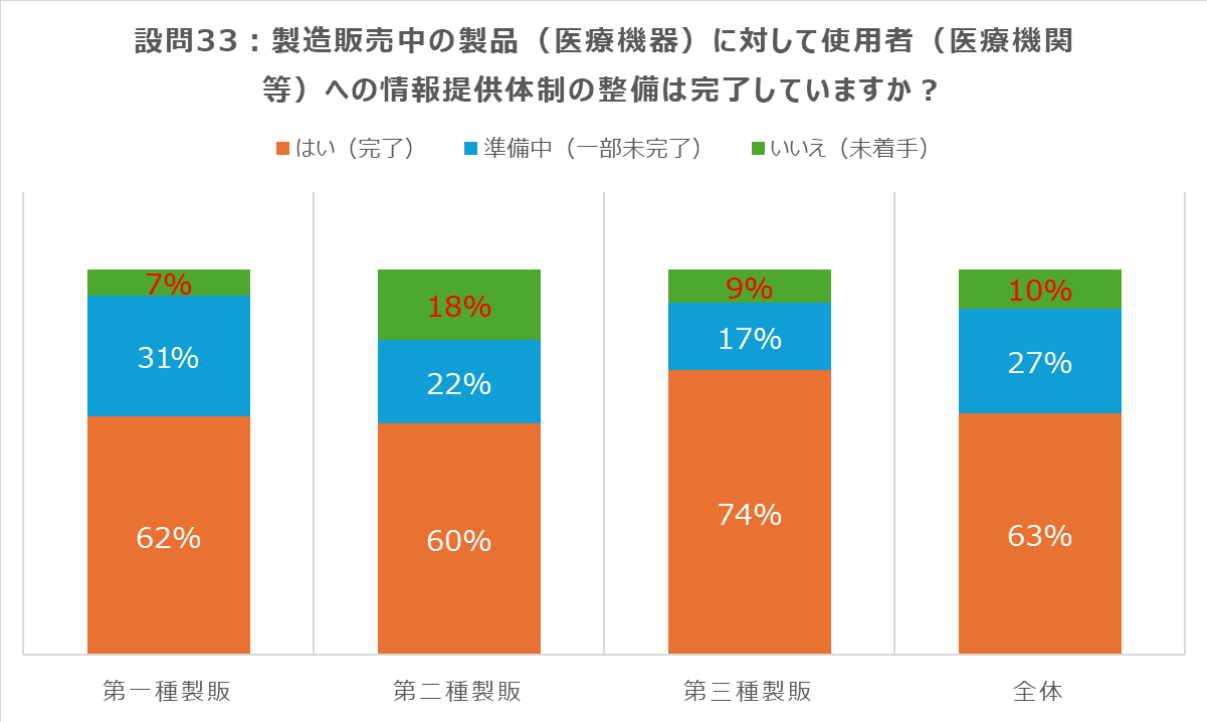
**設問 32：製品ソフトウェアの保守計画を使用者（医療機関等）に提示していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 30 | 47 | 53 |
| 第二種製販 | 11 | 15 | 28 |
| 第三種製販 | 6 | 4 | 13 |
| 全体 | 47 | 66 | 94 |



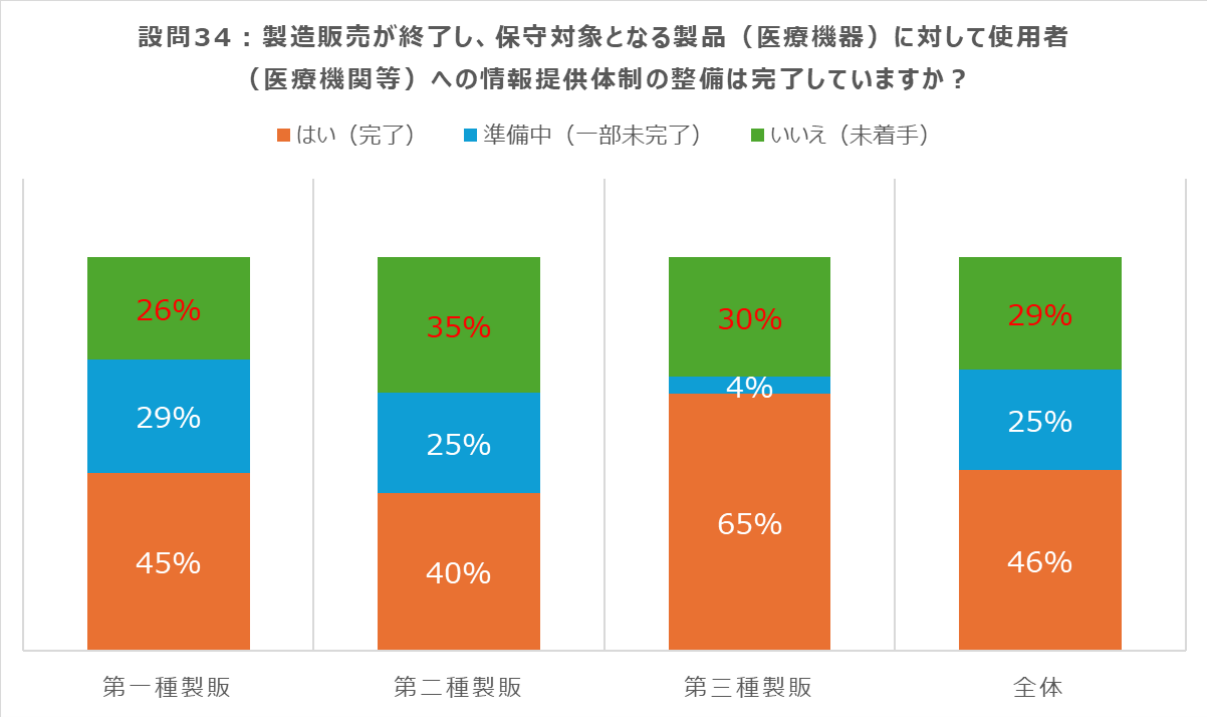
**設問 33：製造販売中の製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 81 | 41 | 9 |
| 第二種製販 | 33 | 12 | 10 |
| 第三種製販 | 17 | 4 | 2 |
| 全体 | 131 | 57 | 21 |



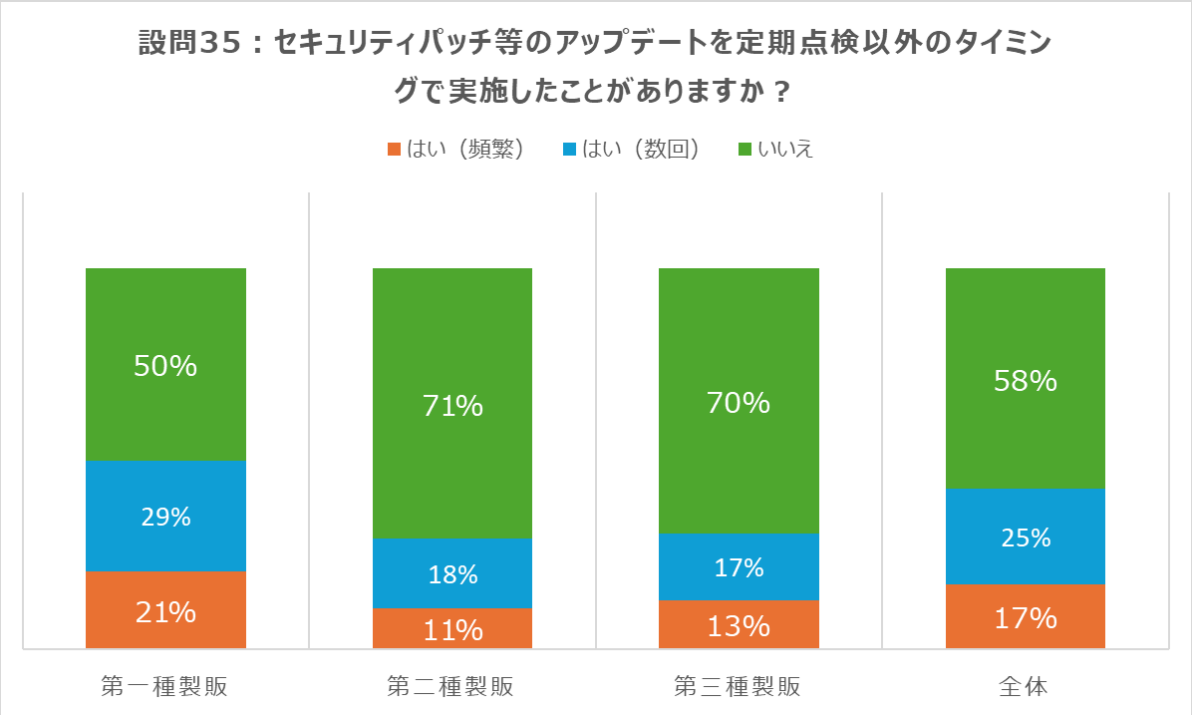
**設問 34：製造販売が終了し、保守対象となる製品（医療機器）に対して使用者（医療機関等）への情報提供体制の整備は完了していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 59 | 38 | 34 |
| 第二種製販 | 22 | 14 | 19 |
| 第三種製販 | 15 | 1 | 7 |
| 全体 | 96 | 53 | 60 |



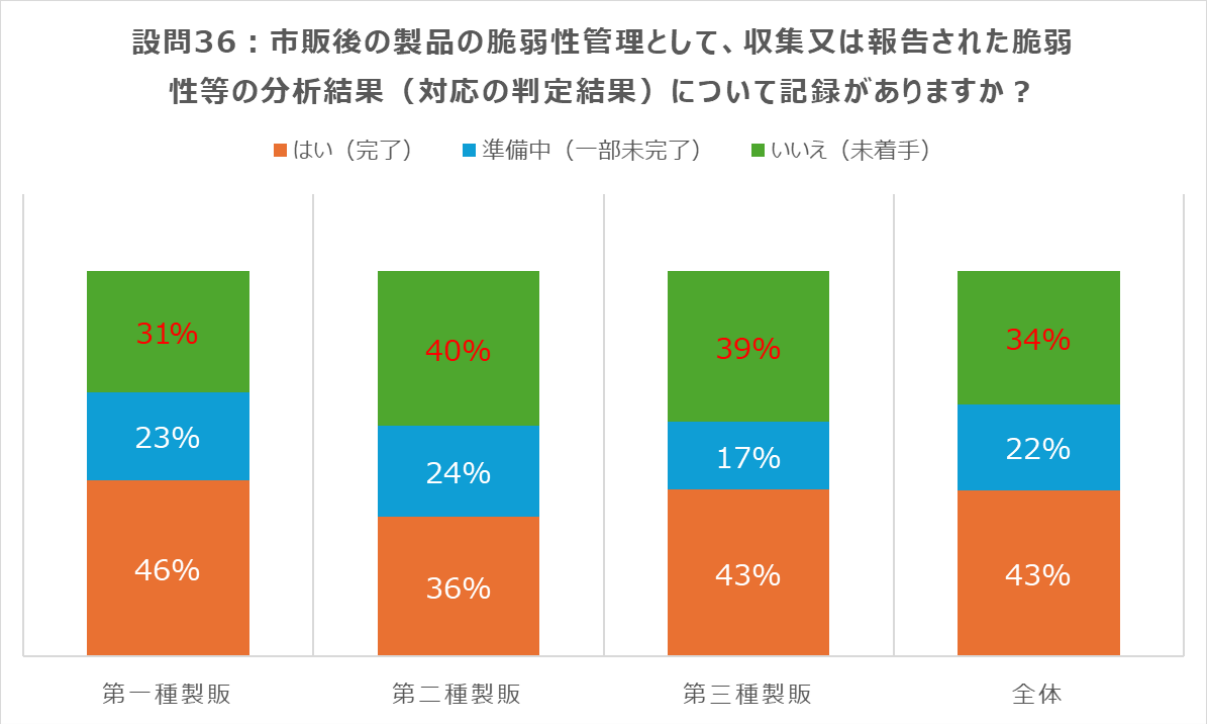
**設問 35：セキュリティパッチ等のアップデートを定期点検以外のタイミングで実施したことがありますか？**

| 選択肢 | はい（頻繁） | はい（数回） | いいえ |
|---|---|---|---|
| 第一種製販 | 27 | 38 | 66 |
| 第二種製販 | 6 | 10 | 39 |
| 第三種製販 | 3 | 4 | 16 |
| 全体 | 36 | 52 | 121 |



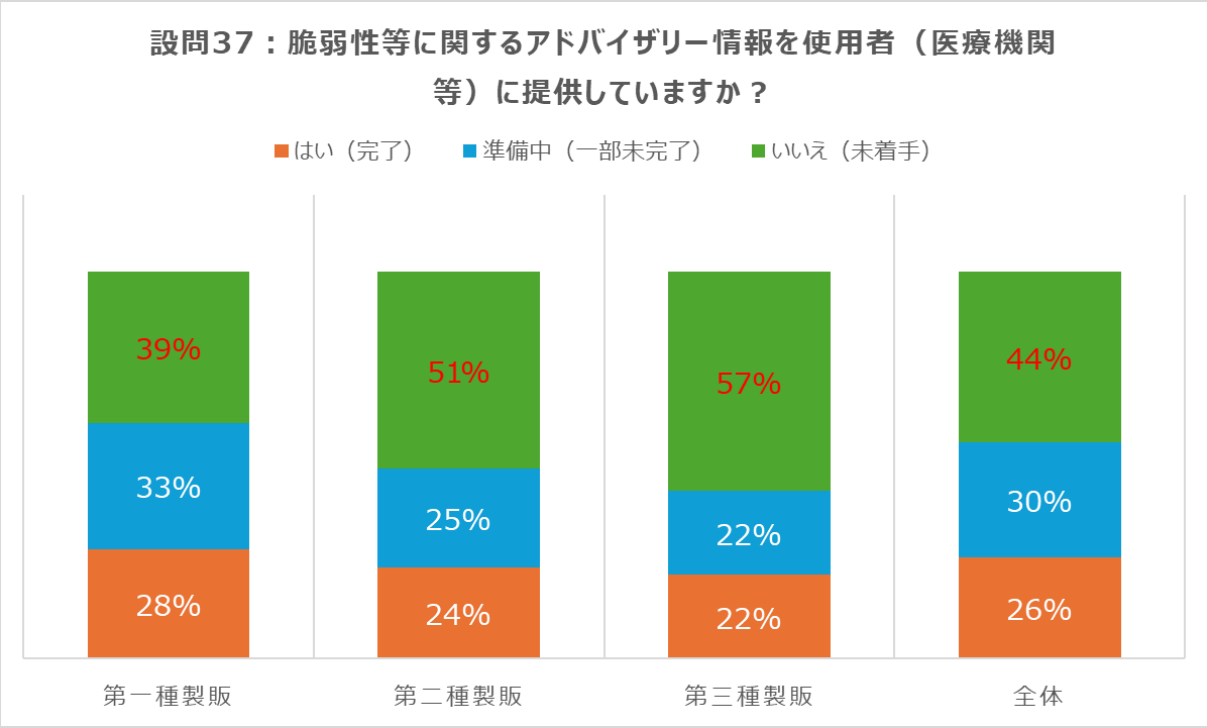
**設問 36：市販後の製品の脆弱性管理として、収集又は報告された脆弱性等の分析結果（対応の判定結果）について記録がありますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 60 | 30 | 41 |
| 第二種製販 | 20 | 13 | 22 |
| 第三種製販 | 10 | 4 | 9 |
| 全体 | 90 | 47 | 72 |



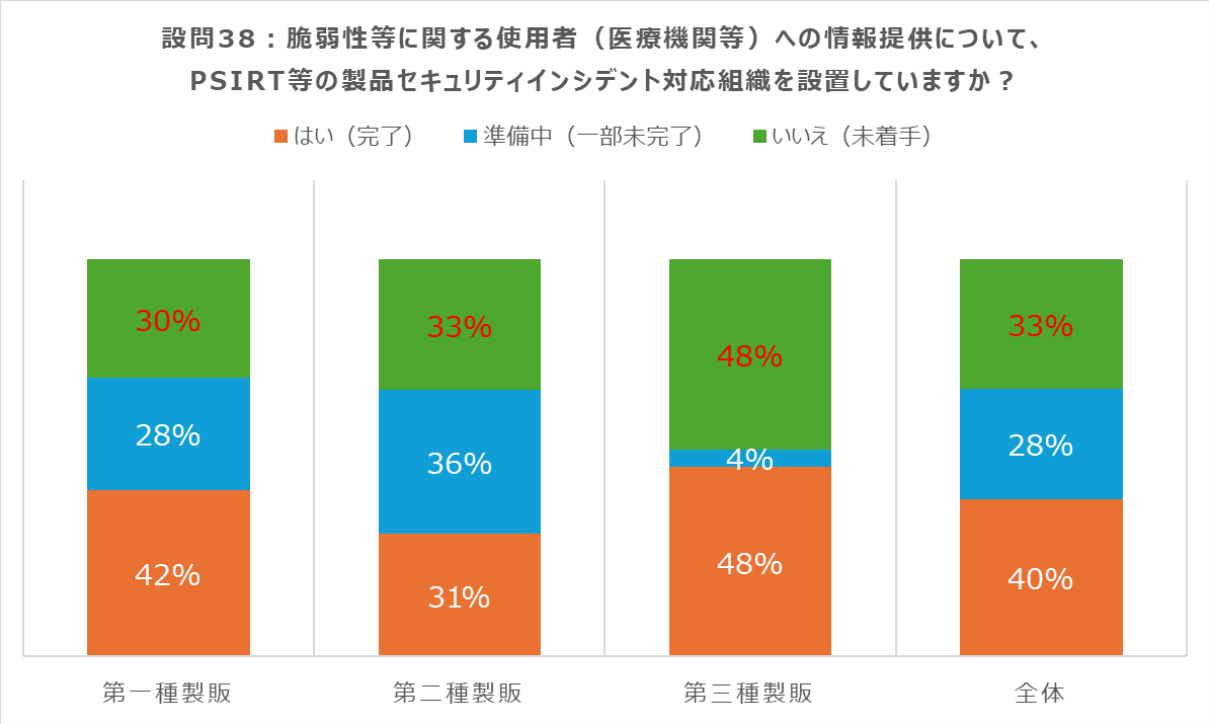
**設問 37：脆弱性等に関するアドバイザリー情報を使用者（医療機関等）に提供していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 37 | 43 | 51 |
| 第二種製販 | 13 | 14 | 28 |
| 第三種製販 | 5 | 5 | 13 |
| 全体 | 55 | 62 | 92 |



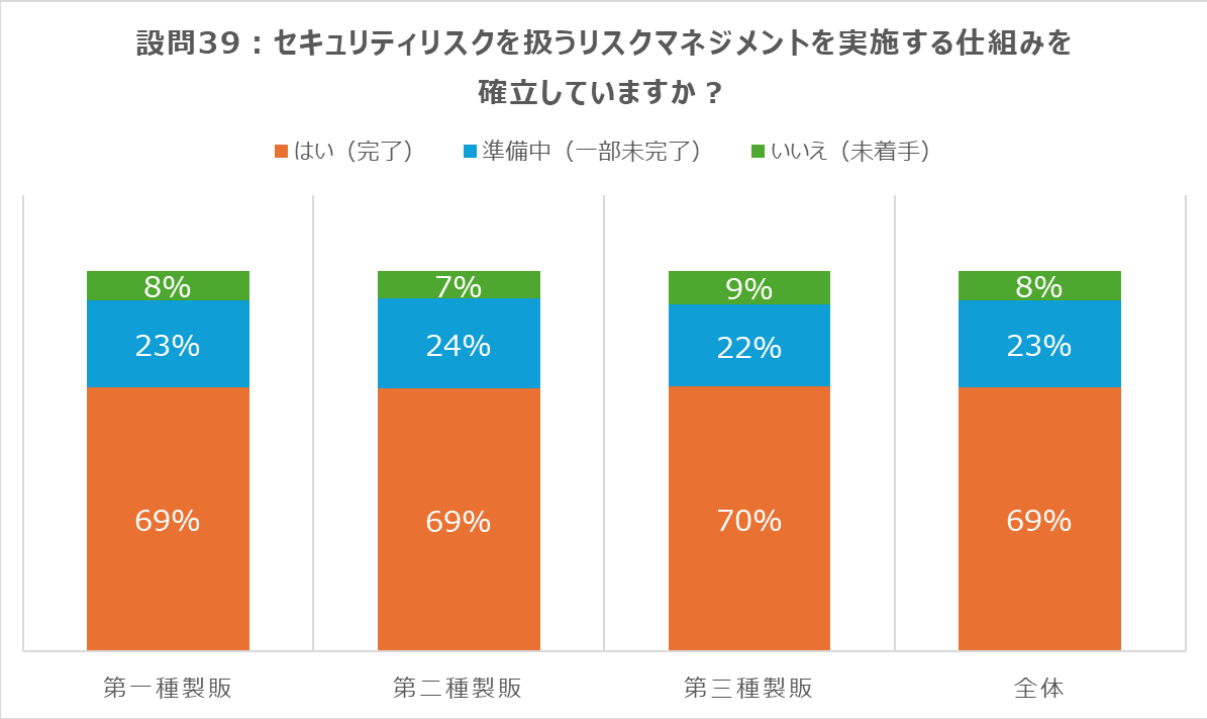
**設問 38：脆弱性等に関する使用者（医療機関等）への情報提供について、PSIRT 等の製品セキュリティインシデント対応組織を設置していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 55 | 37 | 39 |
| 第二種製販 | 17 | 20 | 18 |
| 第三種製販 | 11 | 1 | 11 |
| 全体 | 83 | 58 | 68 |



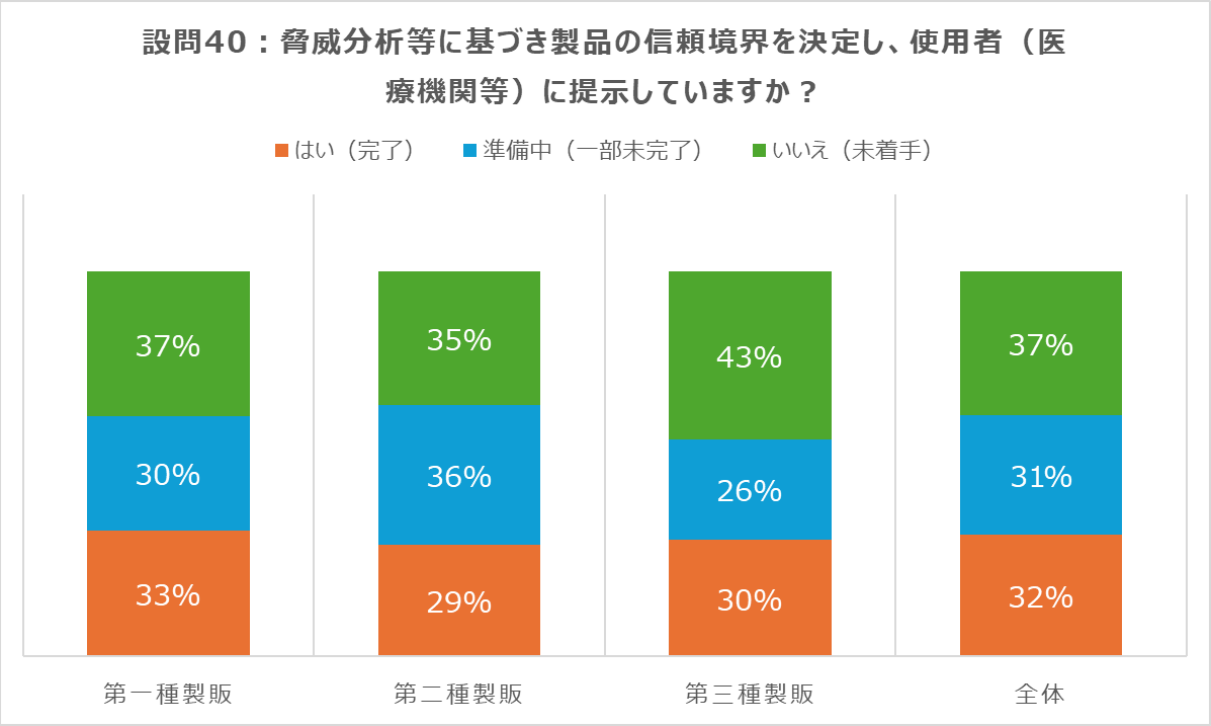
**設問 39：セキュリティリスクを扱うリスクマネジメントを実施する仕組みを確立していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 91 | 30 | 10 |
| 第二種製販 | 38 | 13 | 4 |
| 第三種製販 | 16 | 5 | 2 |
| 全体 | 145 | 48 | 16 |



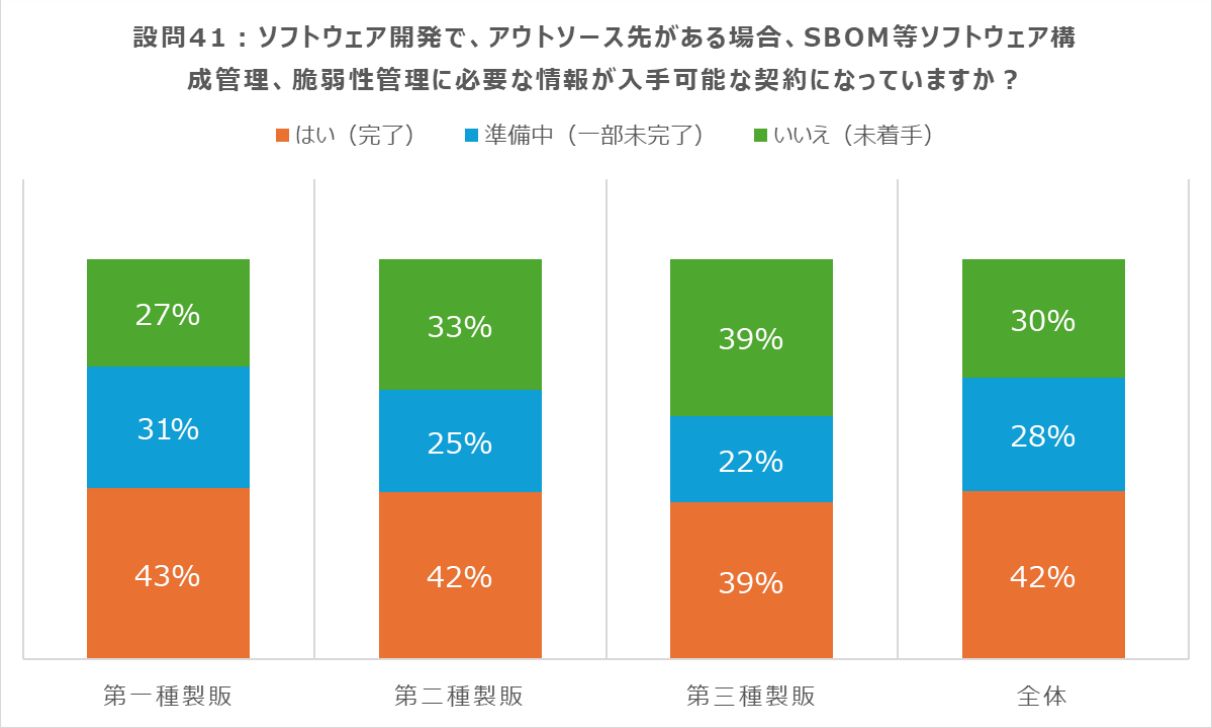
**設問 40：脅威分析等に基づき製品の信頼境界を決定し、使用者（医療機関等）に提示していますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 43 | 39 | 49 |
| 第二種製販 | 16 | 20 | 19 |
| 第三種製販 | 7 | 6 | 10 |
| 全体 | 66 | 65 | 78 |



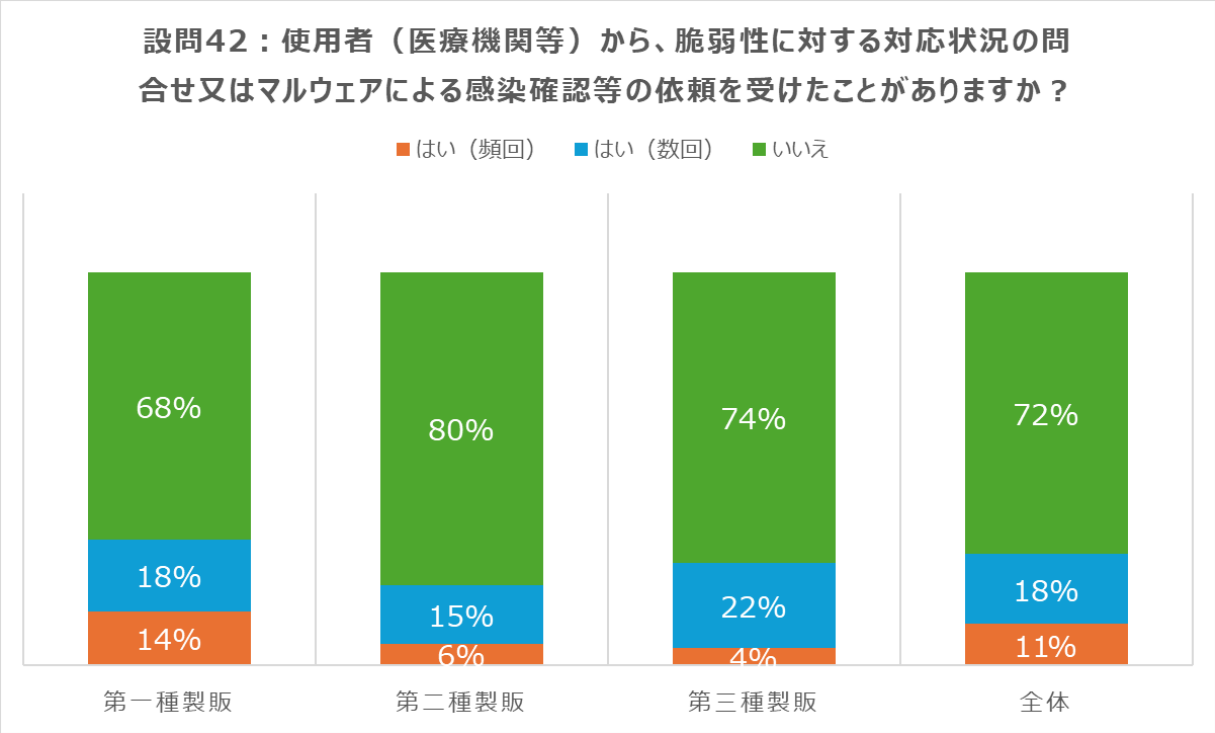
**設問 41：製品のソフトウェア開発では、ソフトウェア構成管理等を含む JIS T 2304 を適用した上で、サイバーリスクを扱うために必要なアクティビティを実施することが求められています。ソフトウェア開発で、アウトソース先がある場合、SBOM 等ソフトウェア構成管理、脆弱性管理に必要な情報が入手可能な契約になっていますか？**

| 選択肢 | はい（完了） | 準備中（一部未完了） | いいえ（未着手） |
|---|---|---|---|
| 第一種製販 | 56 | 40 | 35 |
| 第二種製販 | 23 | 14 | 18 |
| 第三種製販 | 9 | 5 | 9 |
| 全体 | 88 | 59 | 62 |



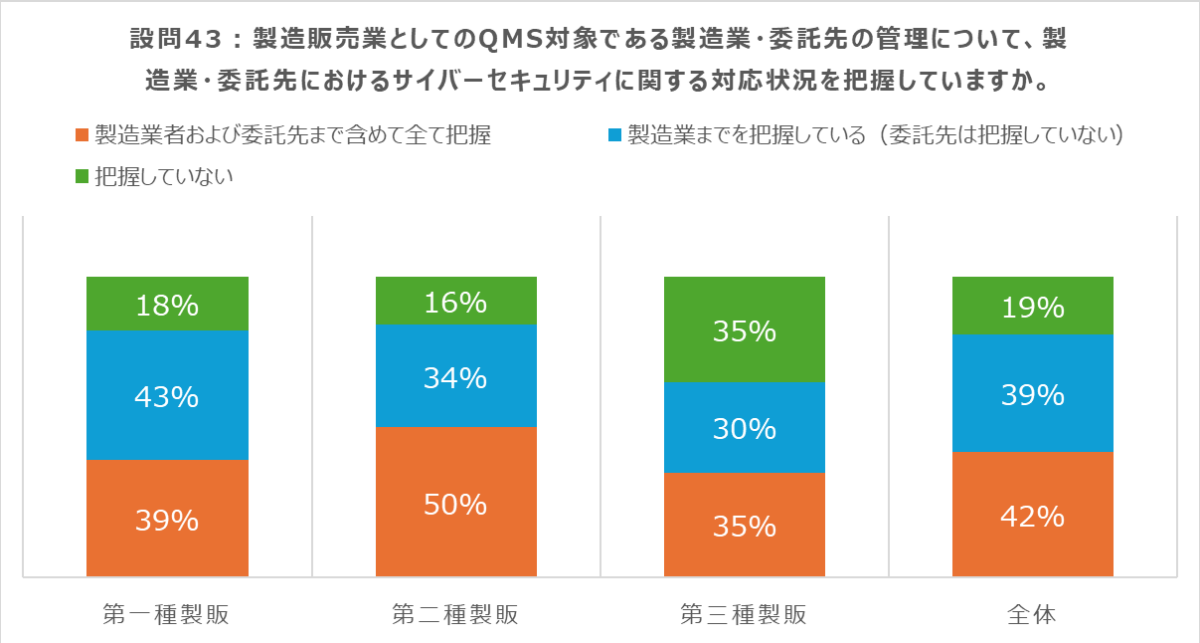
**設問 42：使用者（医療機関等）から、脆弱性に対する対応状況の問合せ又はマルウェアによる感染確認等の依頼を受けたことがありますか？**

| 選択肢 | はい（頻回） | はい（数回） | いいえ |
|---|---|---|---|
| 第一種製販 | 18 | 24 | 89 |
| 第二種製販 | 3 | 8 | 43 |
| 第三種製販 | 1 | 5 | 17 |
| 全体 | 22 | 37 | 149 |



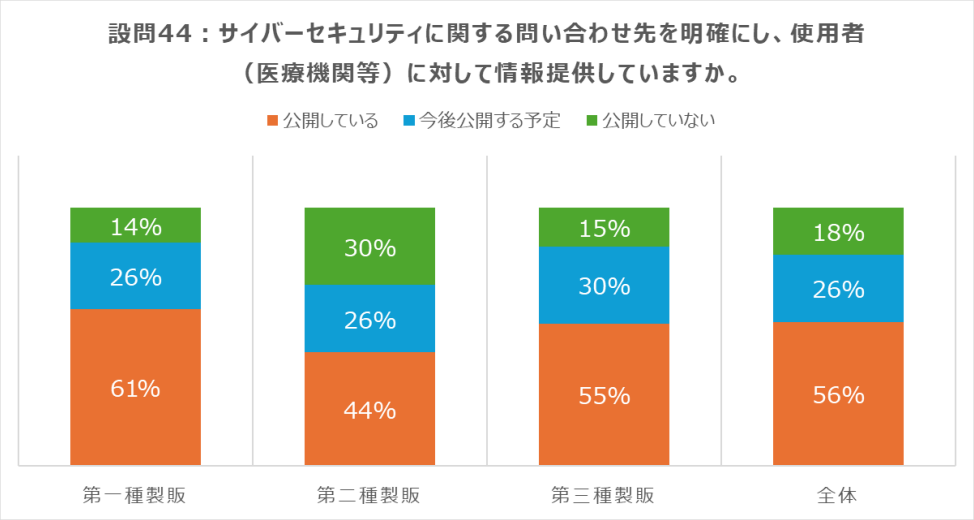
**設問 43：製造販売業としての QMS 対象である製造業・委託先の管理について、製造業・委託先におけるサイバーセキュリティに関する対応状況を把握していますか。**

| 選択肢 | 製造業者および委託先まで含めて全て把握 | 製造業までを把握している（委託先は把握していない） | 把握していない |
|---|---|---|---|
| 第一種製販 | 46 | 50 | 21 |
| 第二種製販 | 25 | 17 | 8 |
| 第三種製販 | 7 | 6 | 7 |
| 全体 | 78 | 73 | 36 |



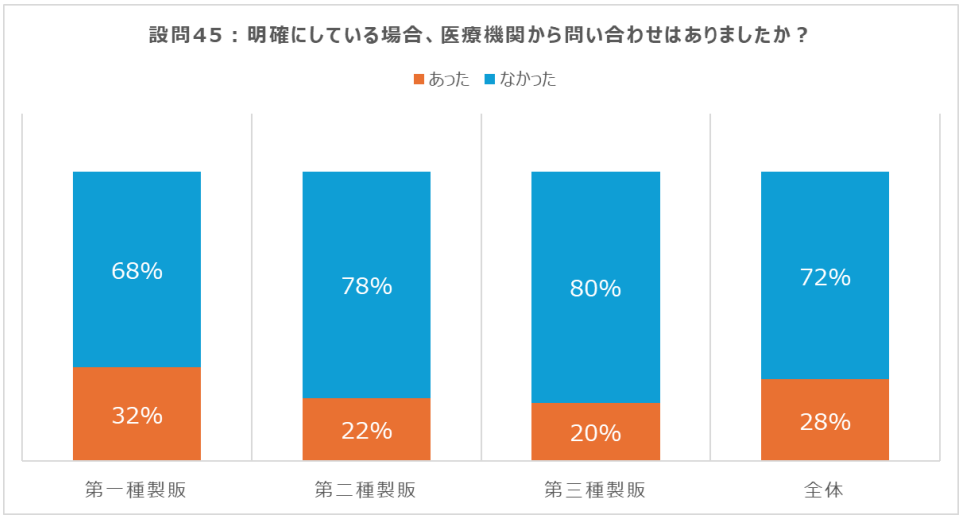
**設問 44：サイバーセキュリティに関する問い合わせ先を明確にし、使用者（医療機関等）に対して情報提供していますか。**

| 選択肢 | 公開している | 今後公開する予定 | 公開していない |
|---|---|---|---|
| 第一種製販 | 71 | 30 | 16 |
| 第二種製販 | 22 | 13 | 15 |
| 第三種製販 | 11 | 6 | 3 |
| 全体 | 104 | 49 | 34 |



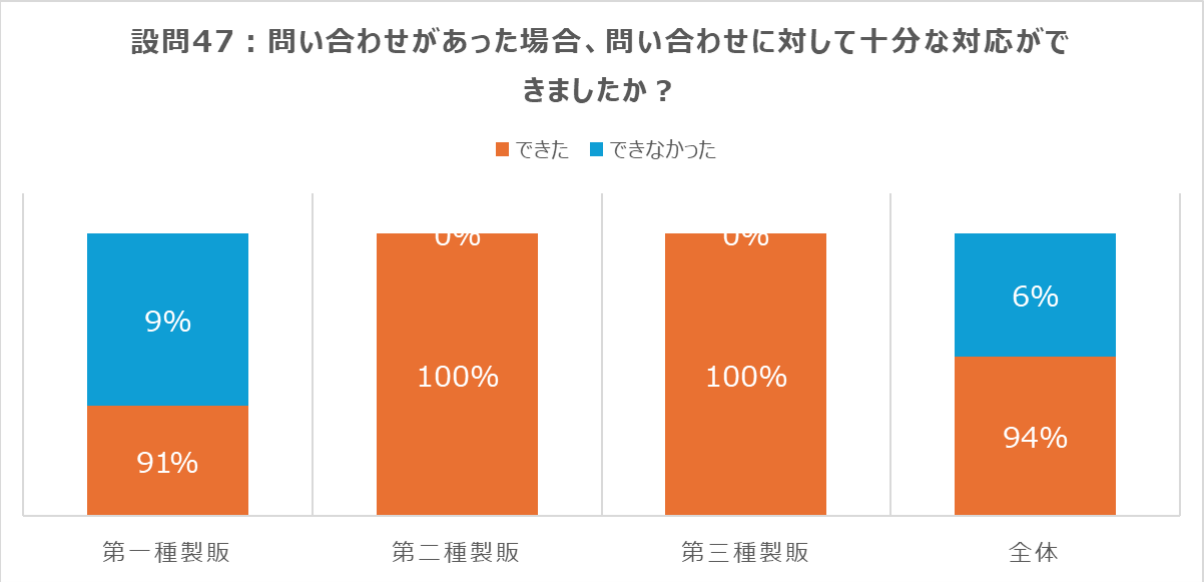

**設問 45：明確にしている場合、医療機関から問い合わせはありましたか？**

| 選択肢 | あった | なかった |
|---|---|---|
| 第一種製販 | 35 | 73 |
| 第二種製販 | 10 | 36 |
| 第三種製販 | 4 | 16 |
| 全体 | 49 | 125 |



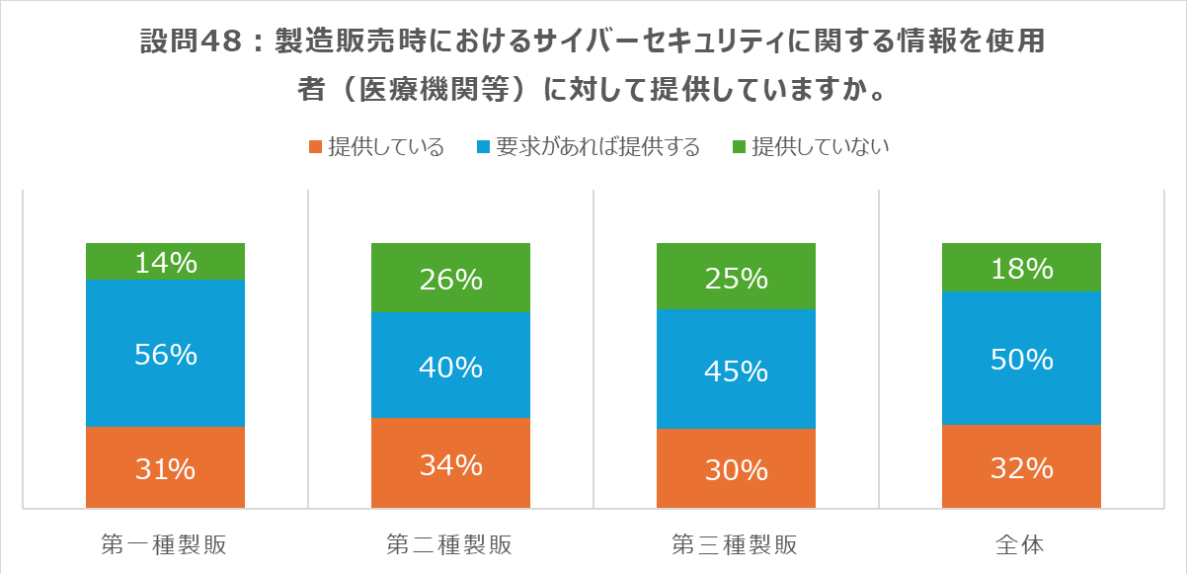
**設問 47：問い合わせがあった場合、問い合わせに対して十分な対応ができましたか？**

| 選択肢 | できた | できなかった |
|---|---|---|
| 第一種製販 | 32 | 3 |
| 第二種製販 | 10 | 0 |
| 第三種製販 | 4 | 0 |
| 全体 | 46 | 3 |



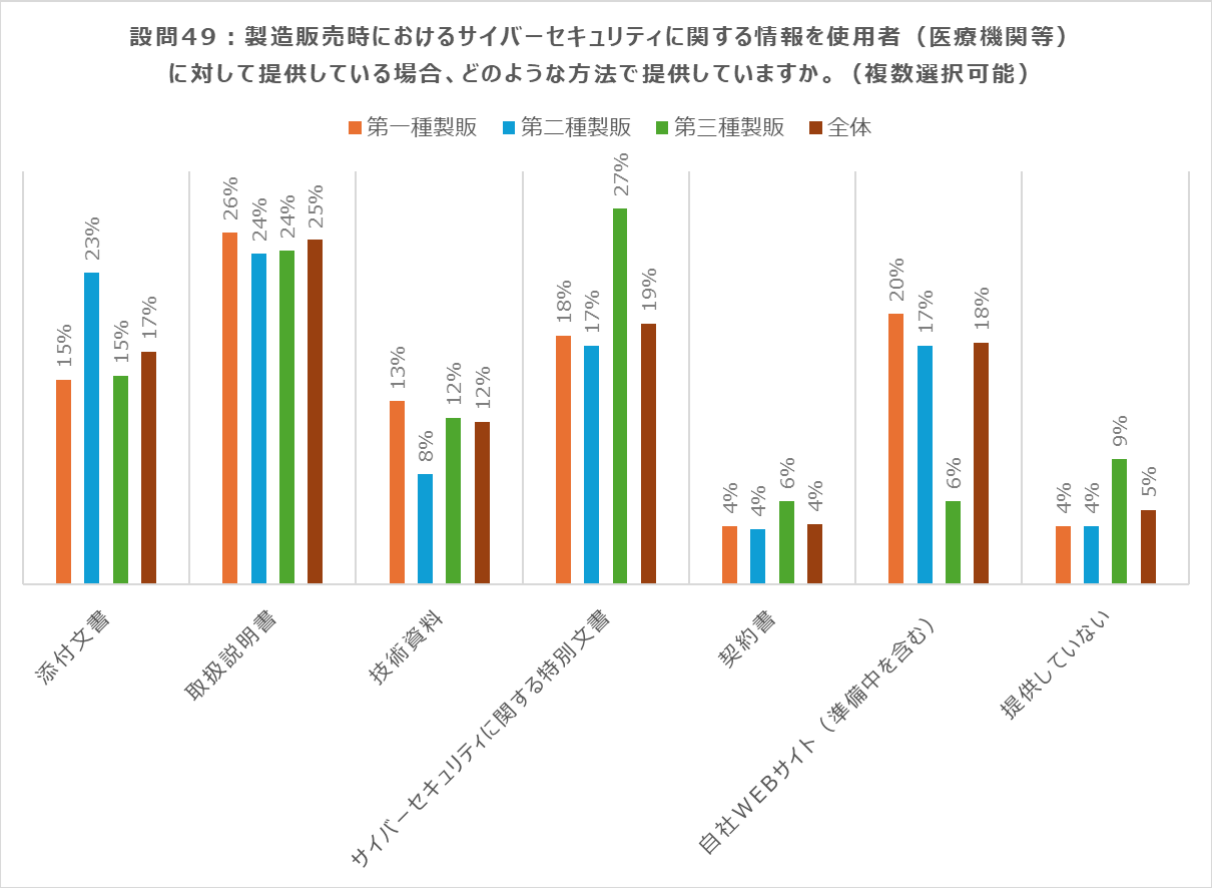
**設問 48：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。**

| 選択肢 | 提供している | 要求があれば提供する | 提供していない |
|---|---|---|---|
| 第一種製販 | 36 | 65 | 16 |
| 第二種製販 | 17 | 20 | 13 |
| 第三種製販 | 6 | 9 | 5 |
| 全体 | 59 | 94 | 34 |



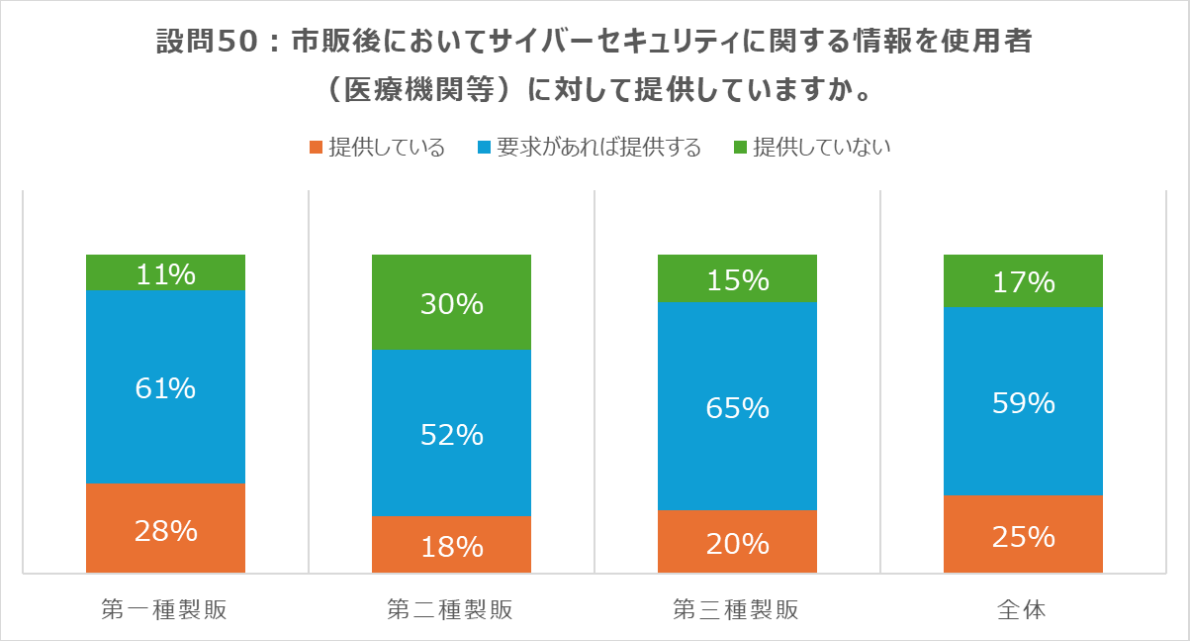
**設問 49：製造販売時におけるサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供している場合、どのような方法で提供していますか。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 添付文書 | 28 | 17 | 5 | 50 |
| 取扱説明書 | 48 | 18 | 8 | 74 |
| 技術資料 | 25 | 6 | 4 | 35 |
| サイバーセキュリティに関する特別文書 | 34 | 13 | 9 | 56 |
| 契約書 | 8 | 3 | 2 | 13 |
| 自社 WEB サイト（準備中を含む） | 37 | 13 | 2 | 52 |
| 提供していない | 8 | 5 | 3 | 16 |



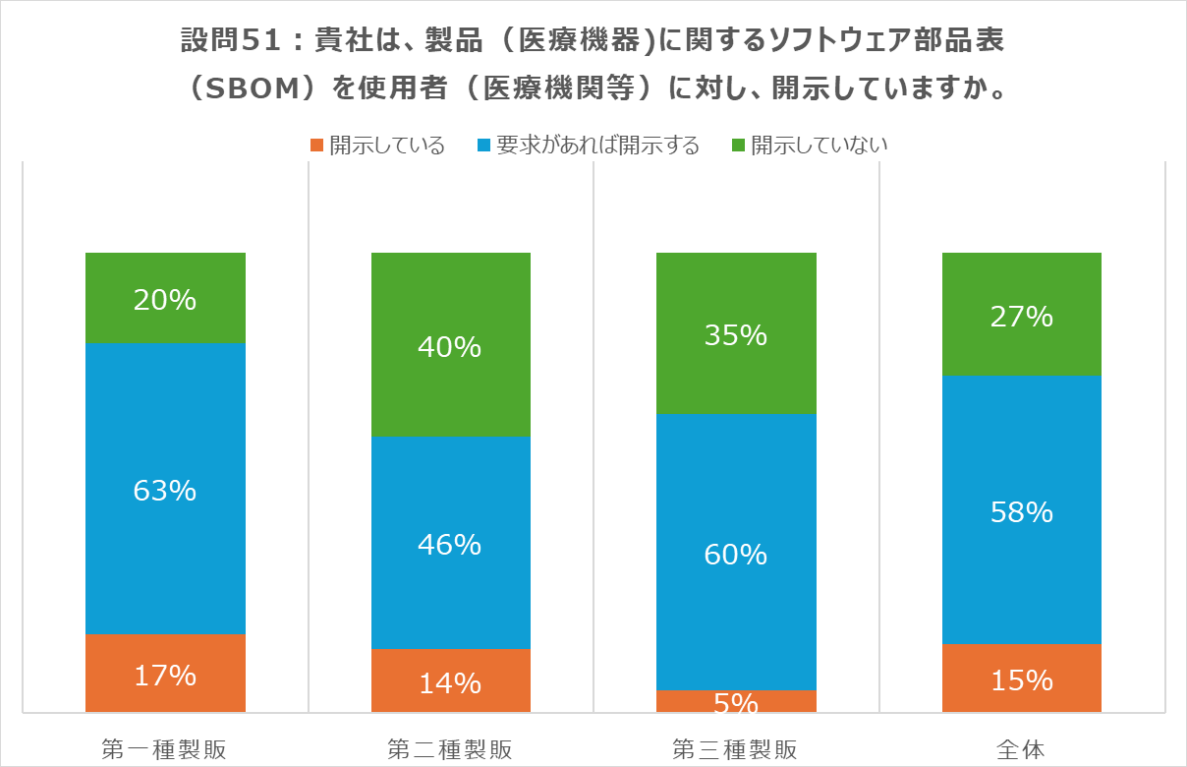
**設問 50：市販後においてサイバーセキュリティに関する情報を使用者（医療機関等）に対して提供していますか。**

| 選択肢 | 提供している | 要求があれば提供する | 提供していない |
|---|---|---|---|
| 第一種製販 | 33 | 71 | 13 |
| 第二種製販 | 9 | 26 | 15 |
| 第三種製販 | 4 | 13 | 3 |
| 全体 | 46 | 110 | 31 |



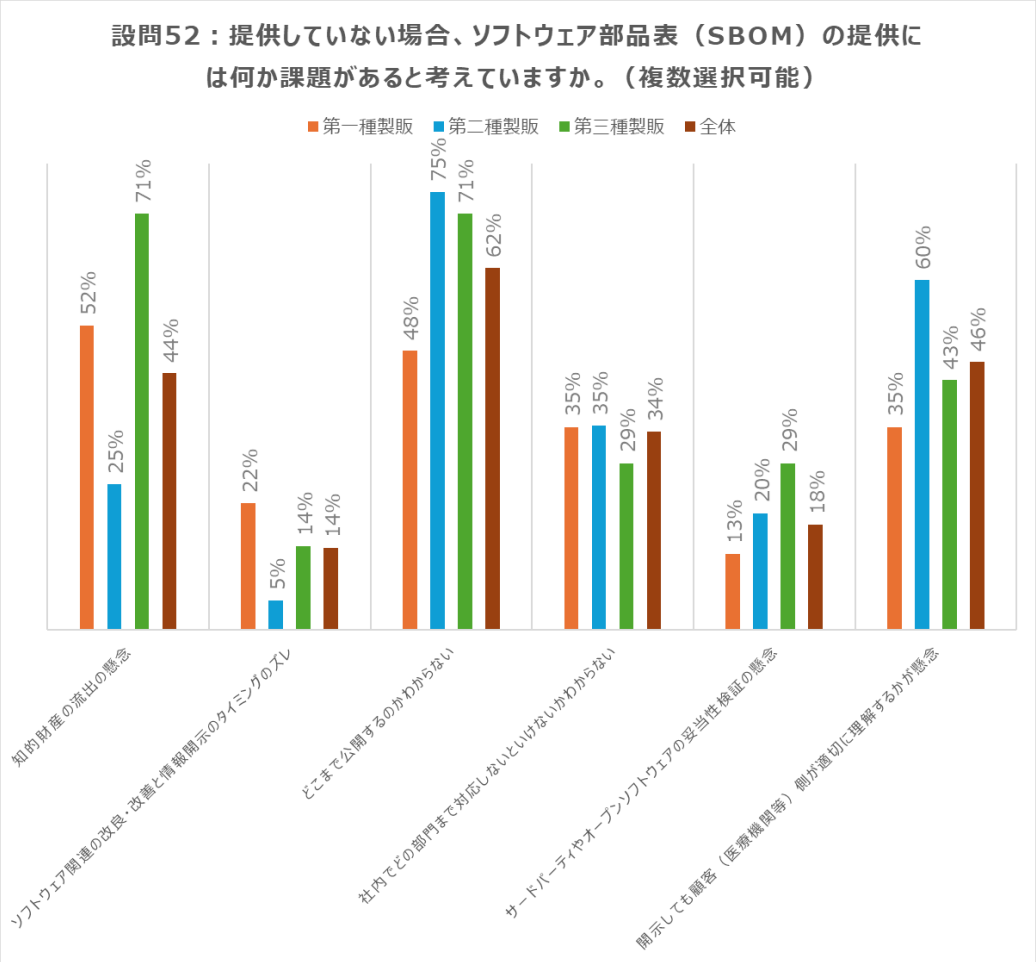
**設問 51：貴社は、製品（医療機器)に関するソフトウェア部品表（SBOM）を使用者（医療機関等）に対し、開示していますか。**

| 選択肢 | 開示している | 要求があれば開示する | 開示していない |
|---|---|---|---|
| 第一種製販 | 20 | 74 | 23 |
| 第二種製販 | 7 | 23 | 20 |
| 第三種製販 | 1 | 12 | 7 |
| 全体 | 28 | 109 | 50 |



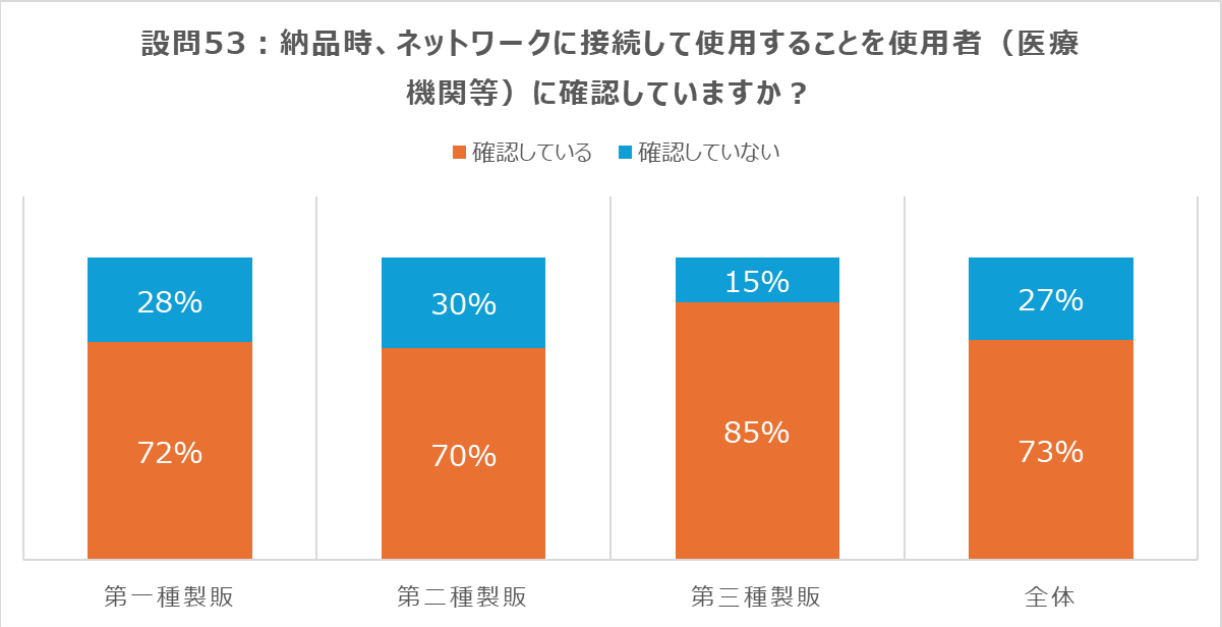
**設問 52：提供していない場合、ソフトウェア部品表（SBOM）の提供には何か課題があると考えていますか。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 知的財産の流出の懸念<br>（提供先からの情報漏洩） | 12 | 5 | 5 | 22 |
| 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 | 5 | 1 | 1 | 7 |
| どこまで公開するのかわからない<br>（標準フォーマットが不明） | 11 | 15 | 5 | 31 |
| 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<br>（資材、開発、生産部門など） | 8 | 7 | 2 | 17 |
| サードパーティやオープンソフトウェアの妥当性検証の懸念 | 3 | 4 | 2 | 9 |
| 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<br>（合理性のない対応を求められる懸念） | 8 | 12 | 3 | 23 |



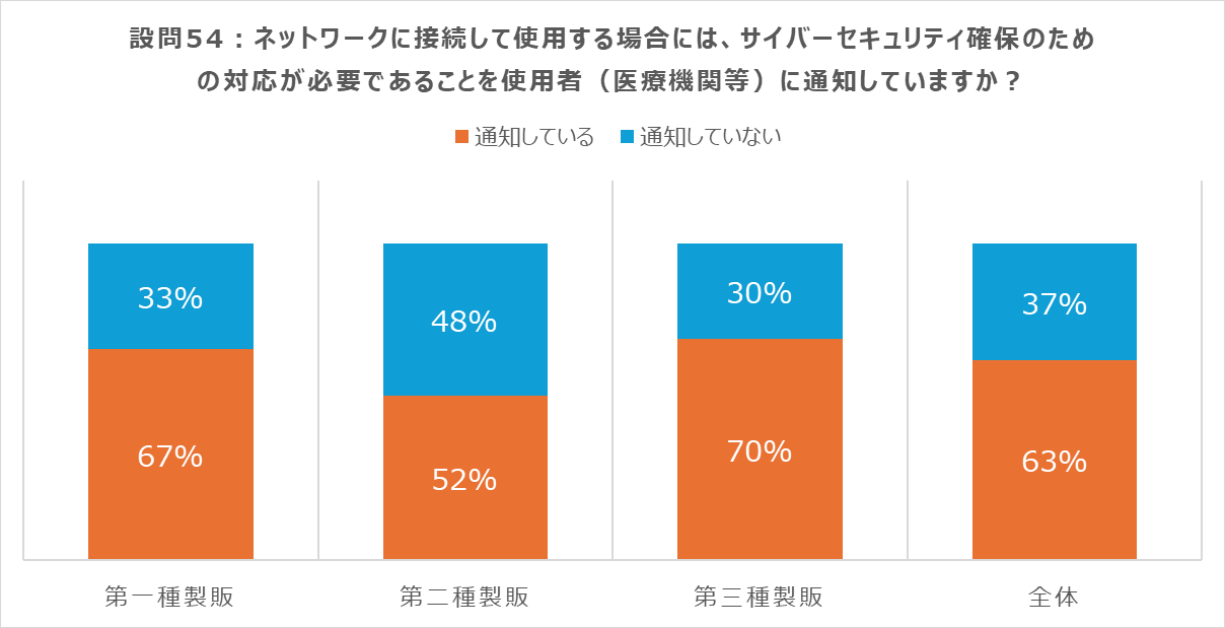
**設問 53：納品時、ネットワークに接続して使用することを使用者（医療機関等）に確認していますか？**

| 選択肢 | 確認している | 確認していない |
|---|---|---|
| 第一種製販 | 84 | 33 |
| 第二種製販 | 35 | 15 |
| 第三種製販 | 17 | 3 |
| 全体 | 136 | 51 |



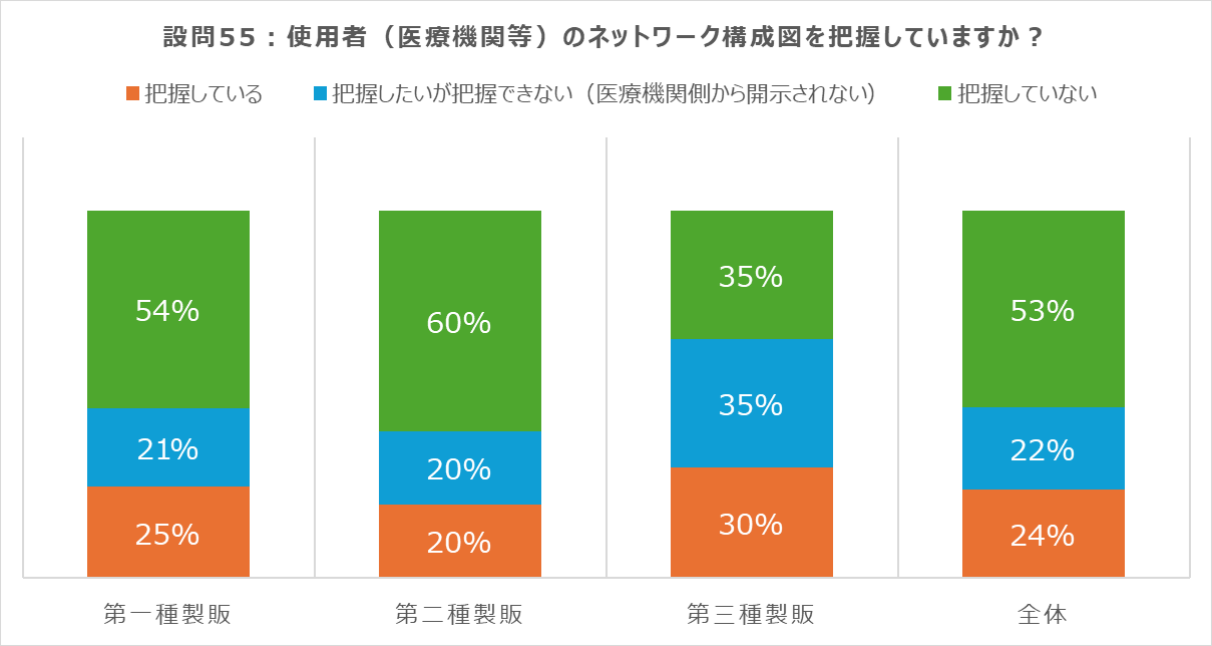
**設問 54：ネットワークに接続して使用する場合には、サイバーセキュリティ確保のための対応が必要であることを使用者（医療機関等）に通知していますか？**

| 選択肢 | 通知している | 通知していない |
|---|---|---|
| 第一種製販 | 78 | 39 |
| 第二種製販 | 26 | 24 |
| 第三種製販 | 14 | 6 |
| 全体 | 118 | 69 |



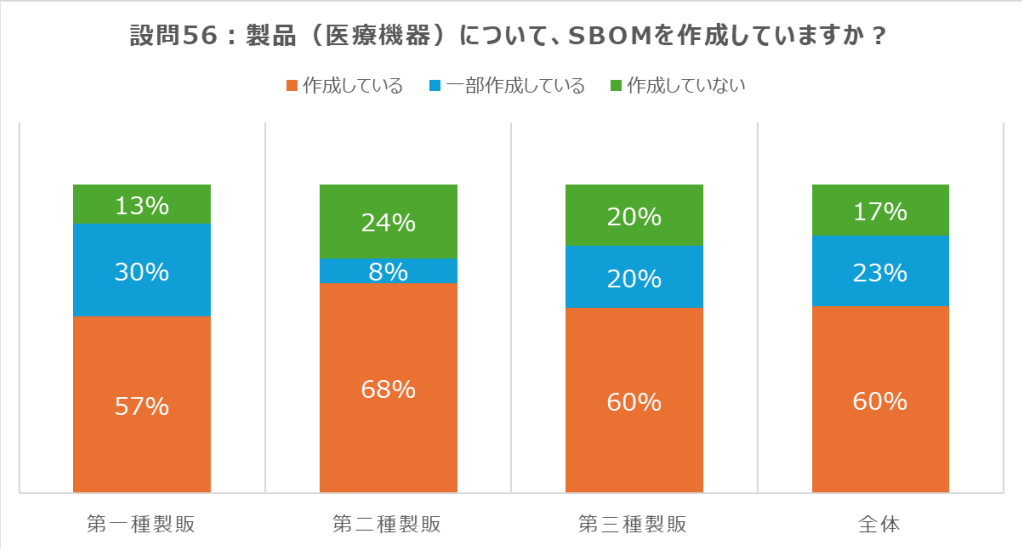
**設問 55：使用者（医療機関等）のネットワーク構成図を把握していますか？**

| 選択肢 | 把握している | 把握したいが把握できない<br>（医療機関側から開示されない） | 把握していない |
|---|---|---|---|
| 第一種製販 | 29 | 25 | 63 |
| 第二種製販 | 10 | 10 | 30 |
| 第三種製販 | 6 | 7 | 7 |
| 全体 | 45 | 42 | 100 |



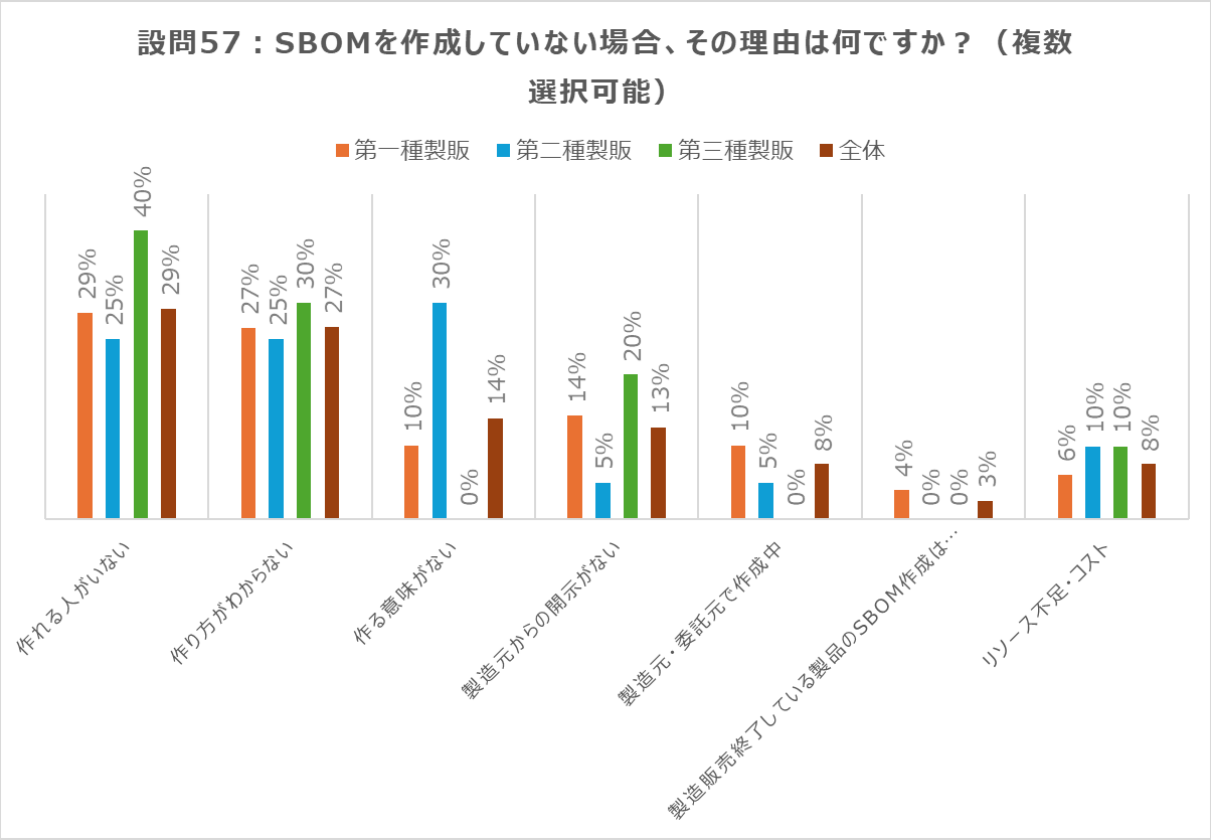
**設問 56：製品（医療機器）について、SBOM を作成していますか？**

| 選択肢 | 作成している | 一部作成している | 作成していない |
|---|---|---|---|
| 第一種製販 | 67 | 35 | 15 |
| 第二種製販 | 34 | 4 | 12 |
| 第三種製販 | 12 | 4 | 4 |
| 全体 | 113 | 43 | 31 |



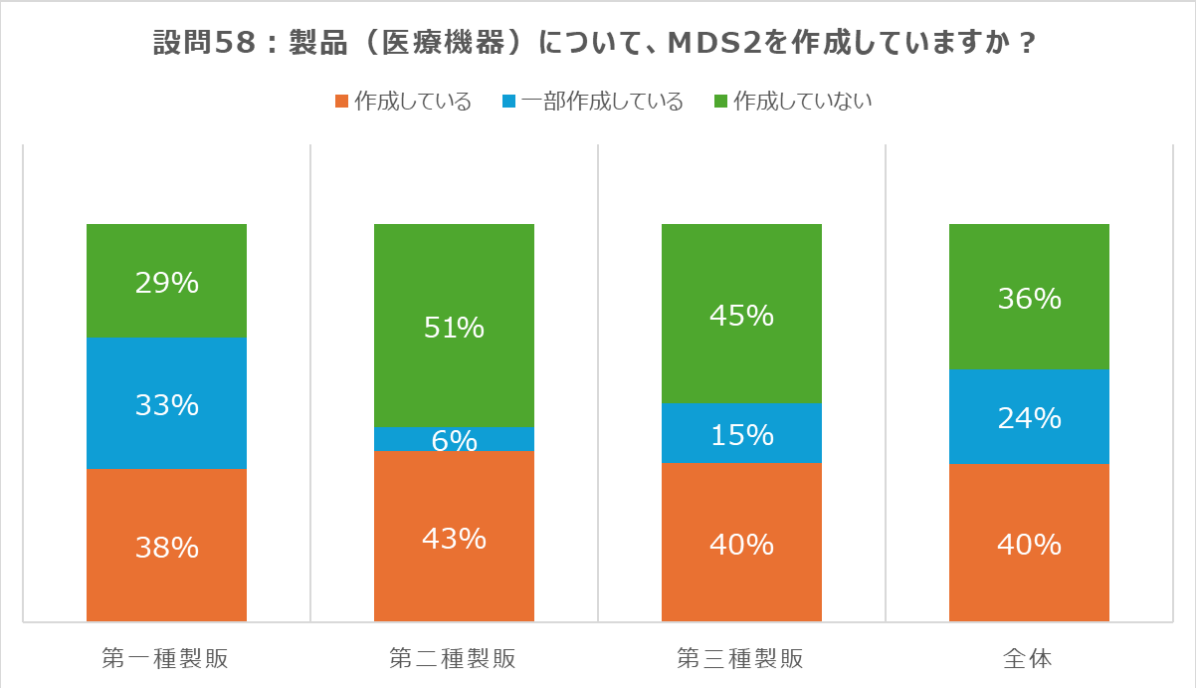
**設問 57：SBOM を作成していない場合、その理由は何ですか？（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 作れる人がいない | 14 | 5 | 4 | 23 |
| 作り方がわからない | 13 | 5 | 3 | 21 |
| 作る意味がない | 5 | 6 | 0 | 11 |
| 製造元からの開示がない | 7 | 1 | 2 | 10 |
| 製造元・委託元で作成中 | 5 | 1 | 0 | 6 |
| 製造販売終了している製品の SBOM 作成は困難 | 2 | 0 | 0 | 2 |
| リソース不足・コスト | 3 | 2 | 1 | 6 |



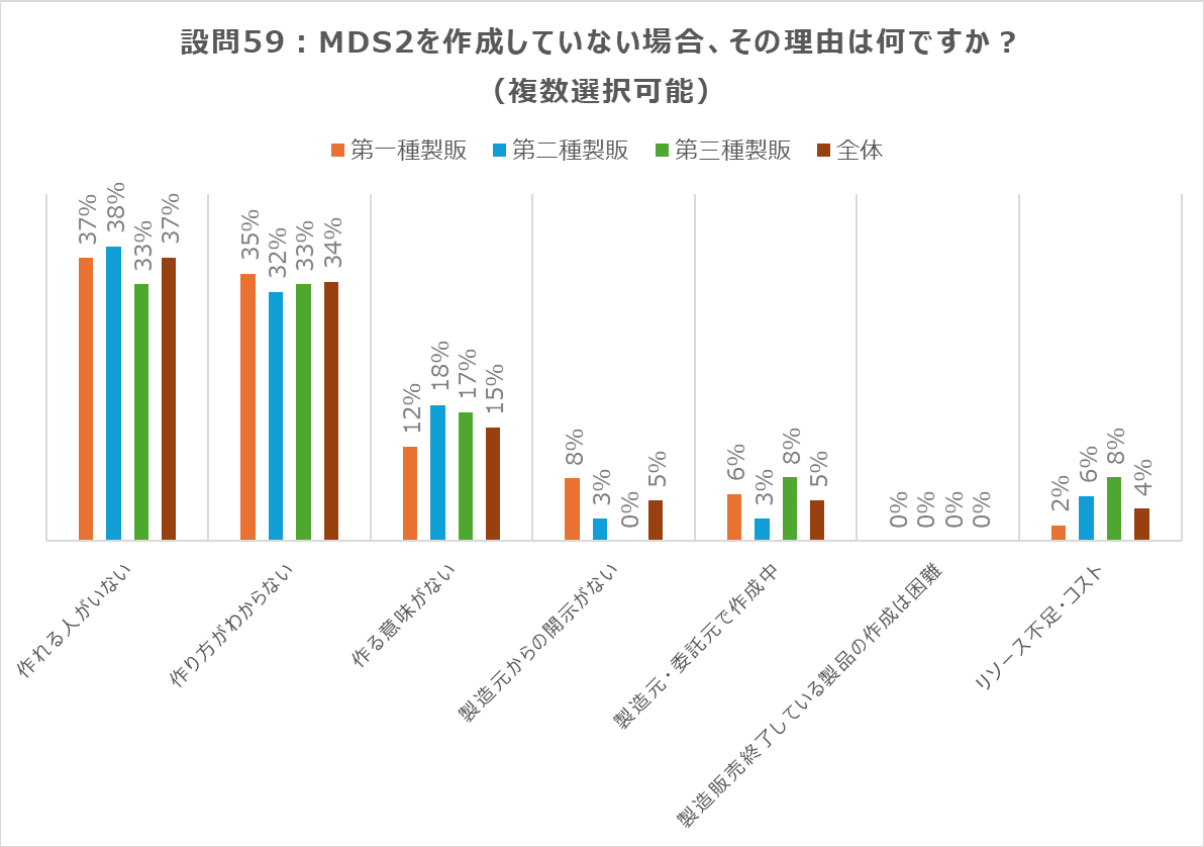
**設問 58：製品（医療機器）について、MDS2 を作成していますか？**

| 選択肢 | 作成している | 一部作成している | 作成していない |
|---|---|---|---|
| 第一種製販 | 43 | 37 | 32 |
| 第二種製販 | 21 | 3 | 25 |
| 第三種製販 | 8 | 3 | 9 |
| 全体 | 72 | 43 | 66 |



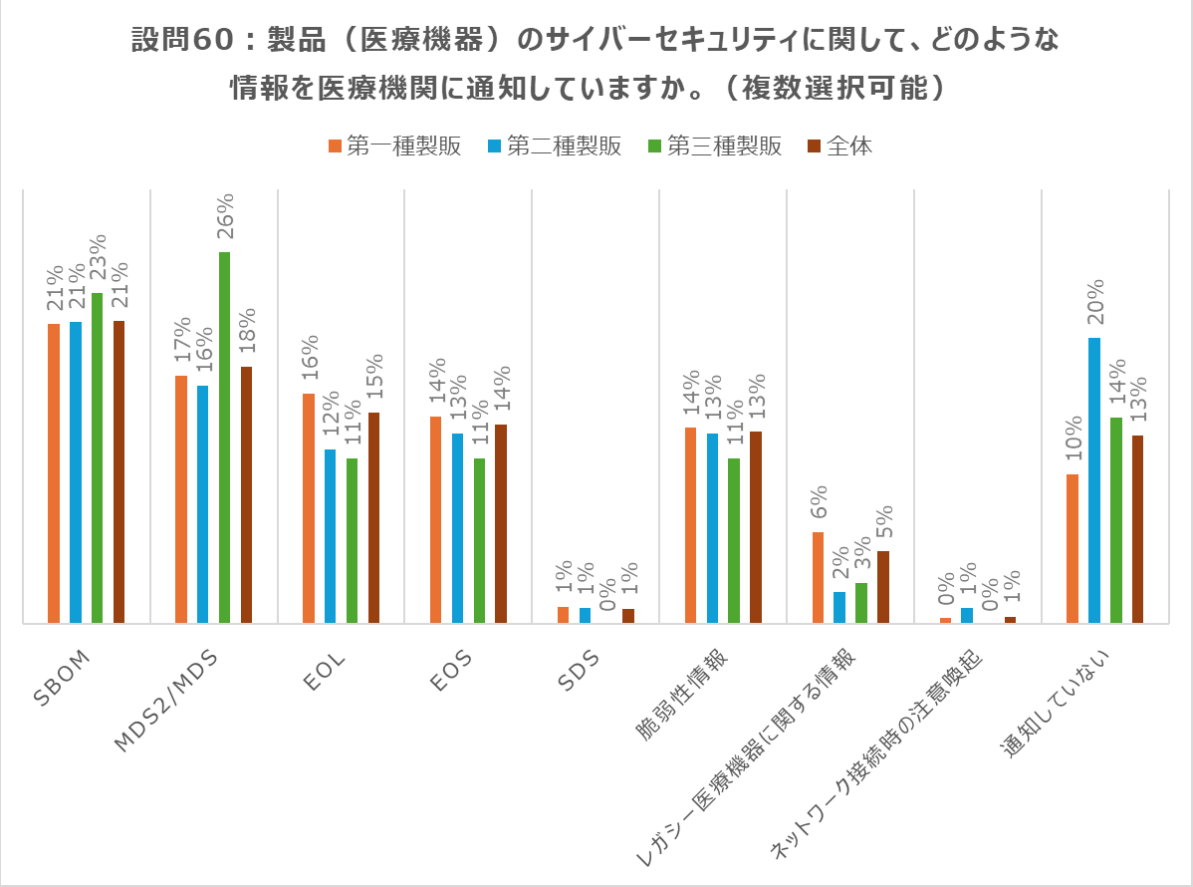
**設問 59：MDS2 を作成していない場合、その理由は何ですか？（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 作れる人がいない | 18 | 13 | 4 | 35 |
| 作り方がわからない | 17 | 11 | 4 | 32 |
| 作る意味がない | 6 | 6 | 2 | 14 |
| 製造元からの開示がない | 4 | 1 | 0 | 5 |
| 製造元・委託元で作成中 | 3 | 1 | 1 | 5 |
| 製造販売終了している製品の SBOM 作成は困難 | 0 | 0 | 0 | 0 |
| リソース不足・コスト | 1 | 2 | 1 | 4 |



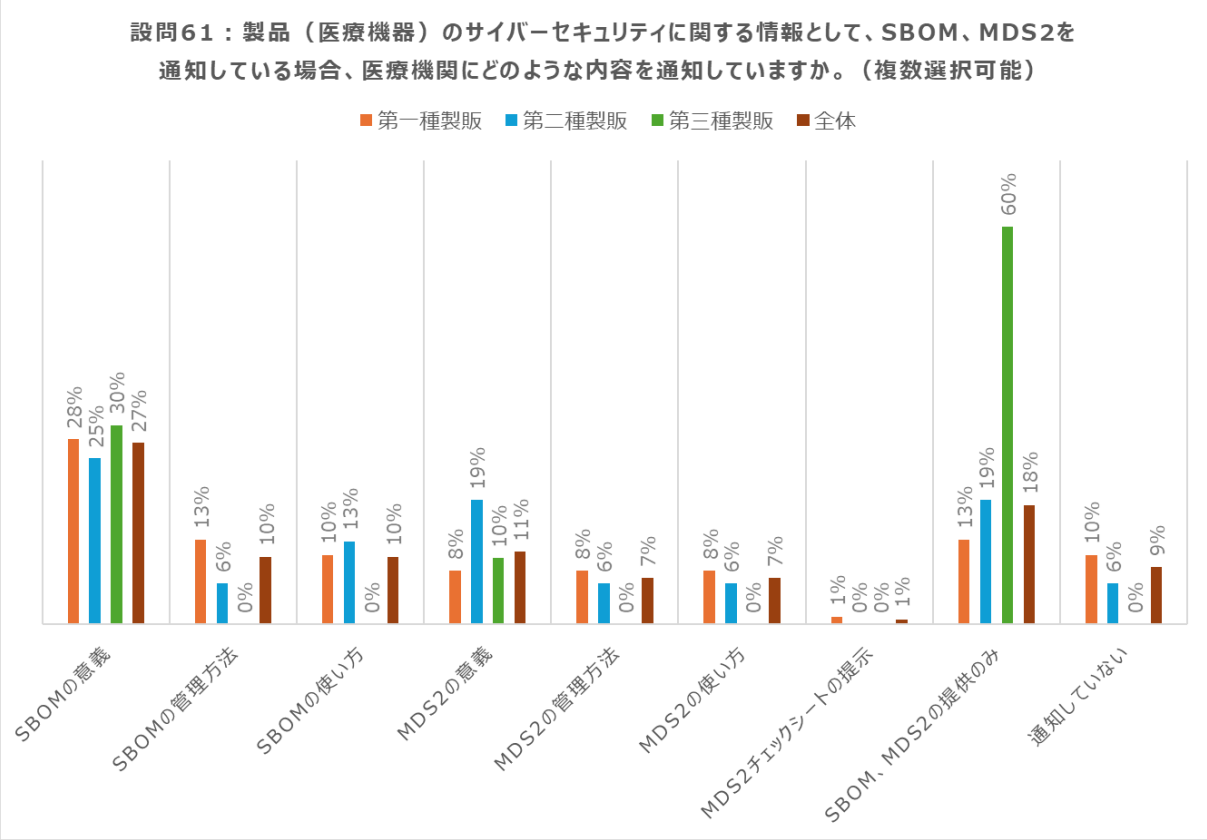
**設問 60：製品（医療機器）のサイバーセキュリティに関して、どのような情報を医療機関に通知していますか。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| SBOM | 52 | 19 | 8 | 79 |
| MDS2/MDS | 43 | 15 | 9 | 67 |
| EOL | 40 | 11 | 4 | 55 |
| EOS | 36 | 12 | 4 | 52 |
| SDS | 3 | 1 | 0 | 4 |
| 脆弱性情報 | 34 | 12 | 4 | 50 |
| レガシー医療機器に関する情報 | 16 | 2 | 1 | 19 |
| ネットワーク接続時の注意喚起 | 1 | 1 | 0 | 2 |
| 通知していない | 26 | 18 | 5 | 49 |



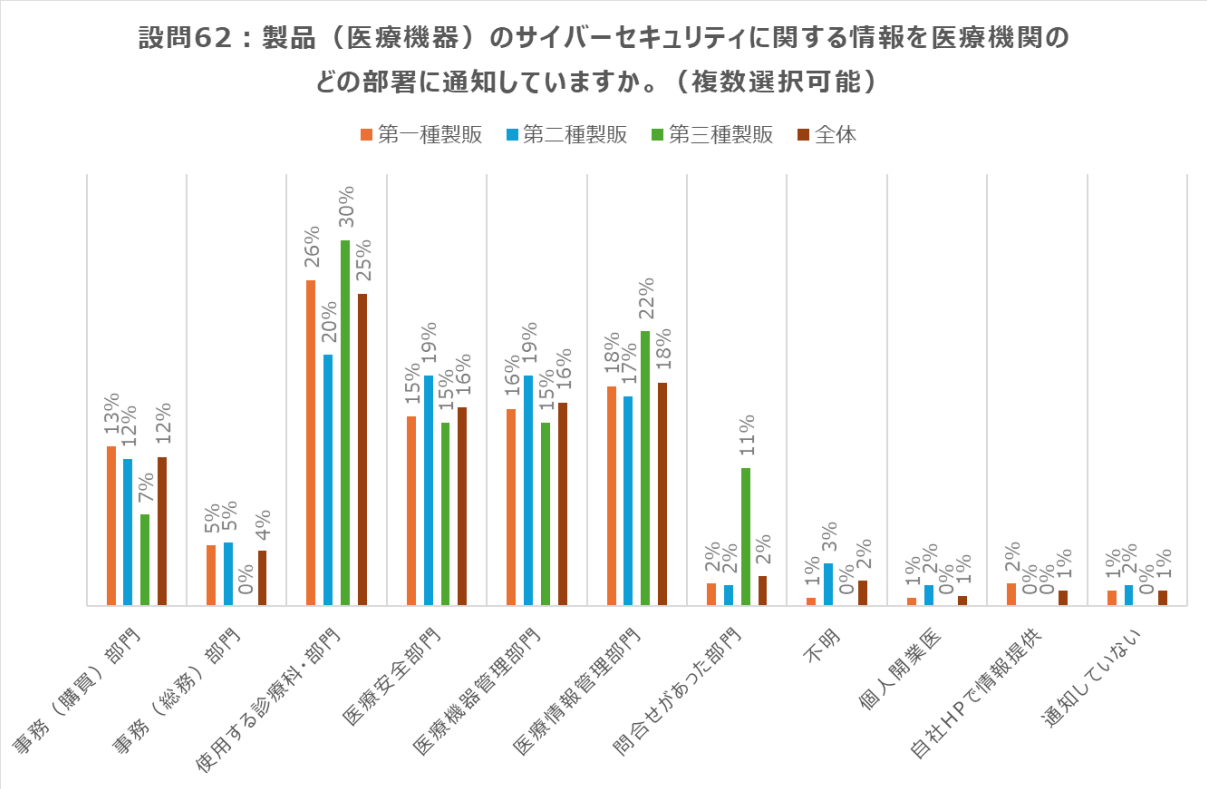
**設問 61：製品（医療機器）のサイバーセキュリティに関する情報として、SBOM、MDS2 を通知している場合、医療機関にどのような内容を通知していますか。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| SBOM の意義 | 24 | 8 | 3 | 35 |
| SBOM の管理方法 | 11 | 2 | 0 | 13 |
| SBOM の使い方 | 9 | 4 | 0 | 13 |
| MDS2 の意義 | 7 | 6 | 1 | 14 |
| MDS2 の管理方法 | 7 | 2 | 0 | 9 |
| MDS2 の使い方 | 7 | 2 | 0 | 9 |
| MDS2 チェックシートの提示 | 1 | 0 | 0 | 1 |
| SBOM、MDS2 の提供のみ | 11 | 6 | 6 | 23 |
| 通知していない | 9 | 2 | 0 | 11 |



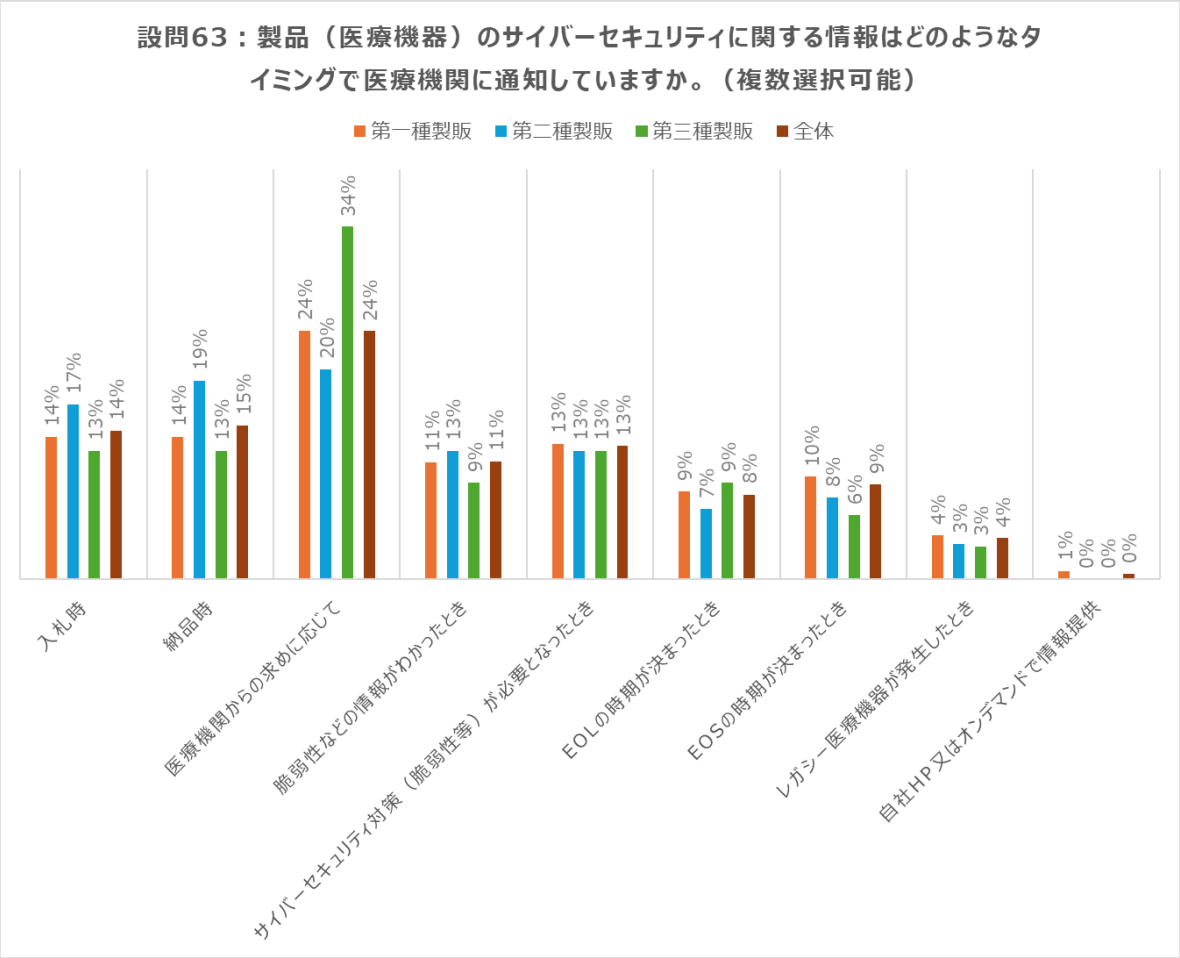
**設問 62：製品（医療機器）のサイバーセキュリティに関する情報を医療機関のどの部署に通知していますか。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 事務（購買）部門 | 21 | 7 | 2 | 30 |
| 事務（総務）部門 | 8 | 3 | 0 | 11 |
| 使用する診療科・部門 | 43 | 12 | 8 | 63 |
| 医療安全部門 | 25 | 11 | 4 | 40 |
| 医療機器管理部門 | 26 | 11 | 4 | 41 |
| 医療情報管理部門 | 29 | 10 | 6 | 45 |
| 問合せがあった部門 | 2 | 1 | 3 | 6 |
| 不明 | 3 | 2 | 0 | 5 |
| 個人開業医 | 1 | 1 | 0 | 2 |
| 自社 HP で情報提供 | 3 | 0 | 0 | 3 |
| 通知していない | 2 | 1 | 0 | 3 |



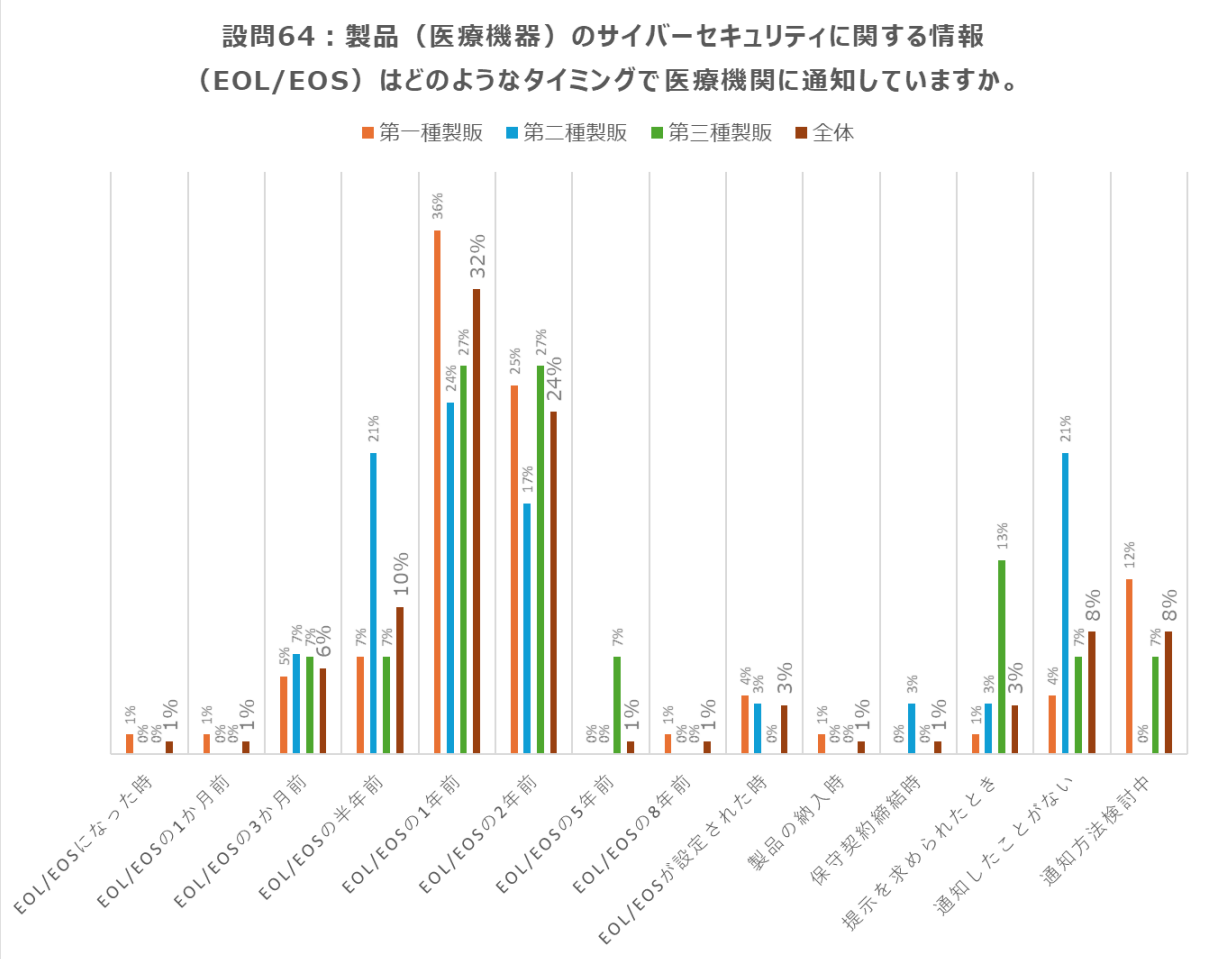
**設問 63：製品（医療機器）のサイバーセキュリティに関する情報はどのようなタイミングで医療機関に通知していますか。（複数選択可能）**

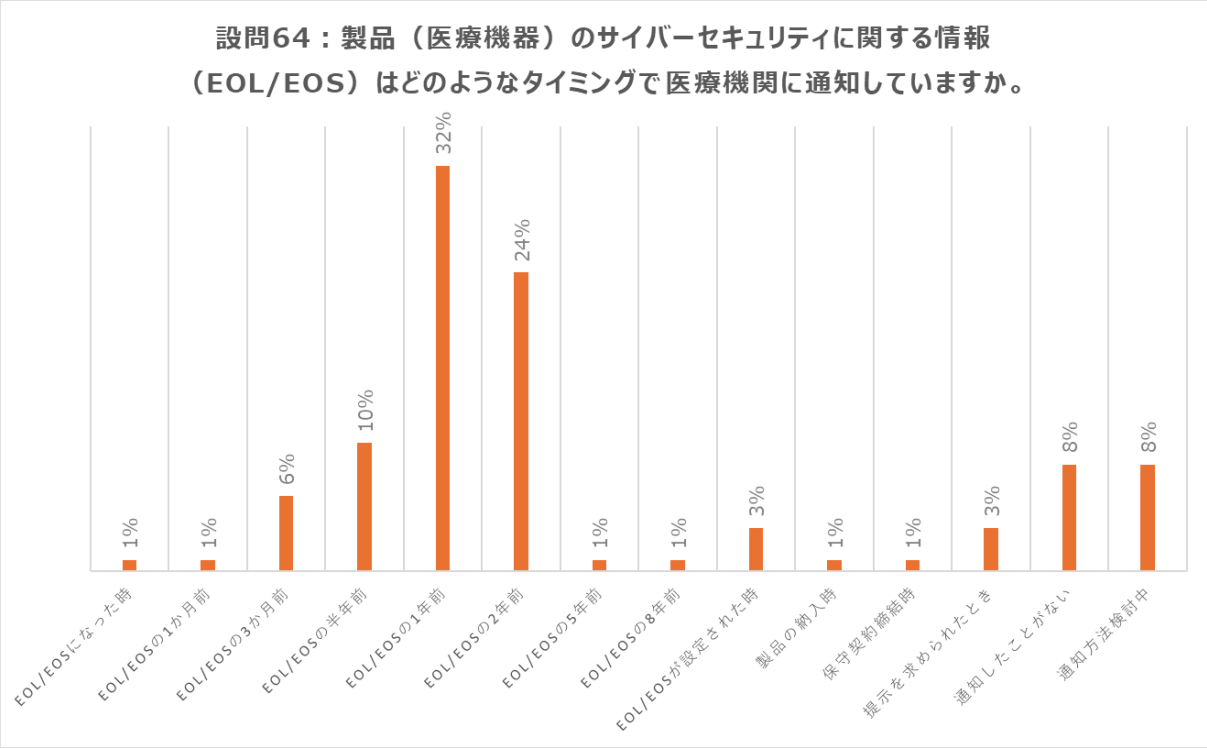
| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 入札時 | 39 | 15 | 4 | 58 |
| 納品時 | 39 | 17 | 4 | 60 |
| 医療機関からの求めに応じて | 68 | 18 | 11 | 97 |
| 脆弱性などの情報がわかったとき | 32 | 11 | 3 | 46 |
| サイバーセキュリティ対策（脆弱性等）が必要となったとき | 37 | 11 | 4 | 52 |
| EOL の時期が決まったとき | 24 | 6 | 3 | 33 |
| EOS の時期が決まったとき | 28 | 7 | 2 | 37 |
| レガシー医療機器が発生したとき | 12 | 3 | 1 | 16 |
| 自社 HP 又はオンデマンドで情報提供 | 2 | 0 | 0 | 2 |



**設問 64：製品（医療機器）のサイバーセキュリティに関する情報（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。**

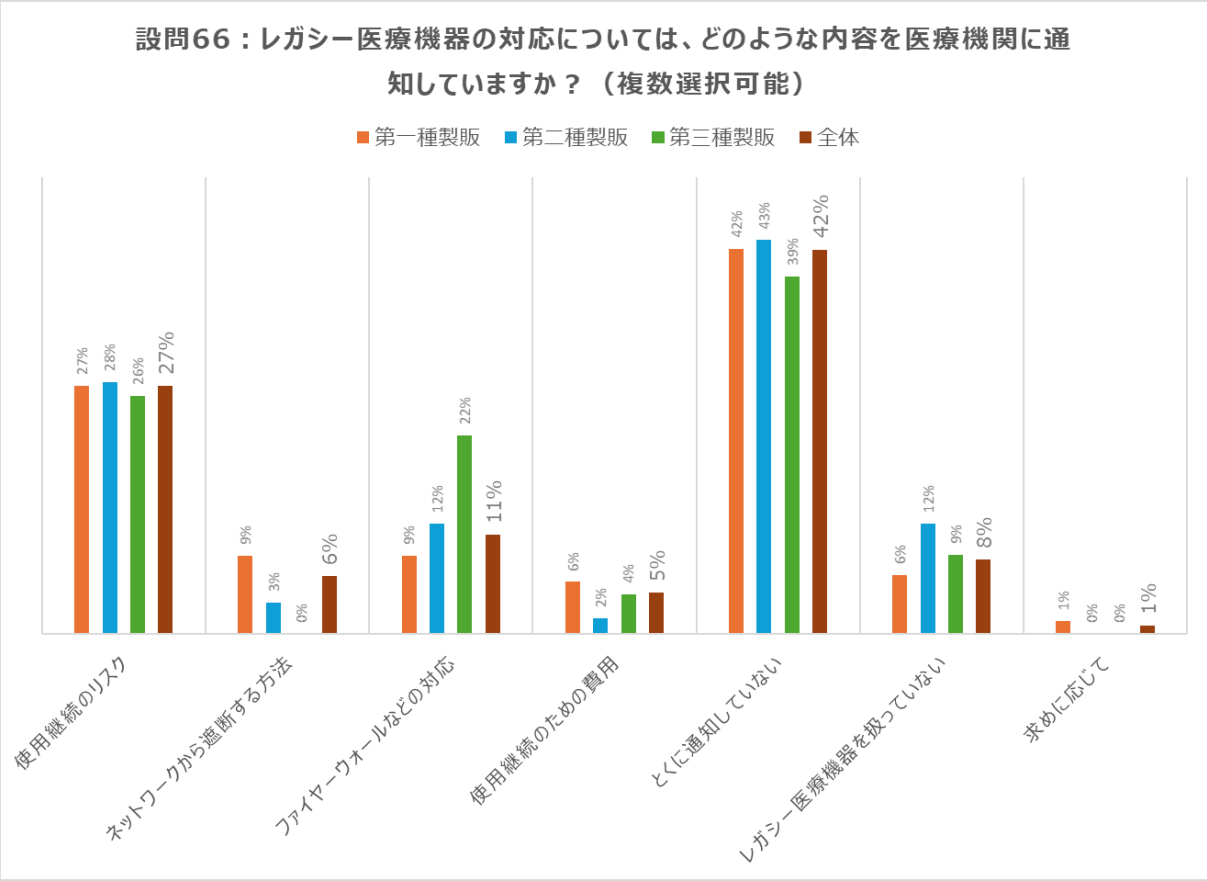
| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| EOL/EOS になった時 | 1 | 0 | 0 | 1 |
| EOL/EOS の 1 か月前 | 1 | 0 | 0 | 1 |
| EOL/EOS の 3 か月前 | 4 | 2 | 1 | 7 |
| EOL/EOS の半年前 | 5 | 6 | 1 | 12 |
| EOL/EOS の 1 年前 | 27 | 7 | 4 | 38 |
| EOL/EOS の 2 年前 | 19 | 5 | 4 | 28 |
| EOL/EOS の 5 年前 | 0 | 0 | 1 | 1 |
| EOL/EOS の 8 年前 | 1 | 0 | 0 | 1 |
| EOL/EOS が設定された時 | 3 | 1 | 0 | 4 |
| 製品の納入時 | 1 | 0 | 0 | 1 |
| 保守契約締結時 | 0 | 1 | 0 | 1 |
| 提示を求められたとき | 1 | 1 | 2 | 4 |
| 通知したことがない | 3 | 6 | 1 | 10 |
| 通知方法検討中 | 9 | 0 | 1 | 10 |




設問64：製品（医療機器）のサイバーセキュリティに関する情報
（EOL/EOS）はどのようなタイミングで医療機関に通知していますか。
1%
1%
6%
10%
32%
24%
1%
1%
3%
1%
1%
3%
8%
8%
EOL/EOSになった時
EOL/EOSの1か月前
EOL/EOSの3か月前
EOL/EOSの半年前
EOL/EOSの1年前
EOL/EOSの2年前
EOL/EOSの5年前
EOL/EOSの8年前
EOL/EOSが設定された時
製品の納入時
保守契約締結時
提示を求められたとき
通知したことがない
通知方法検討中

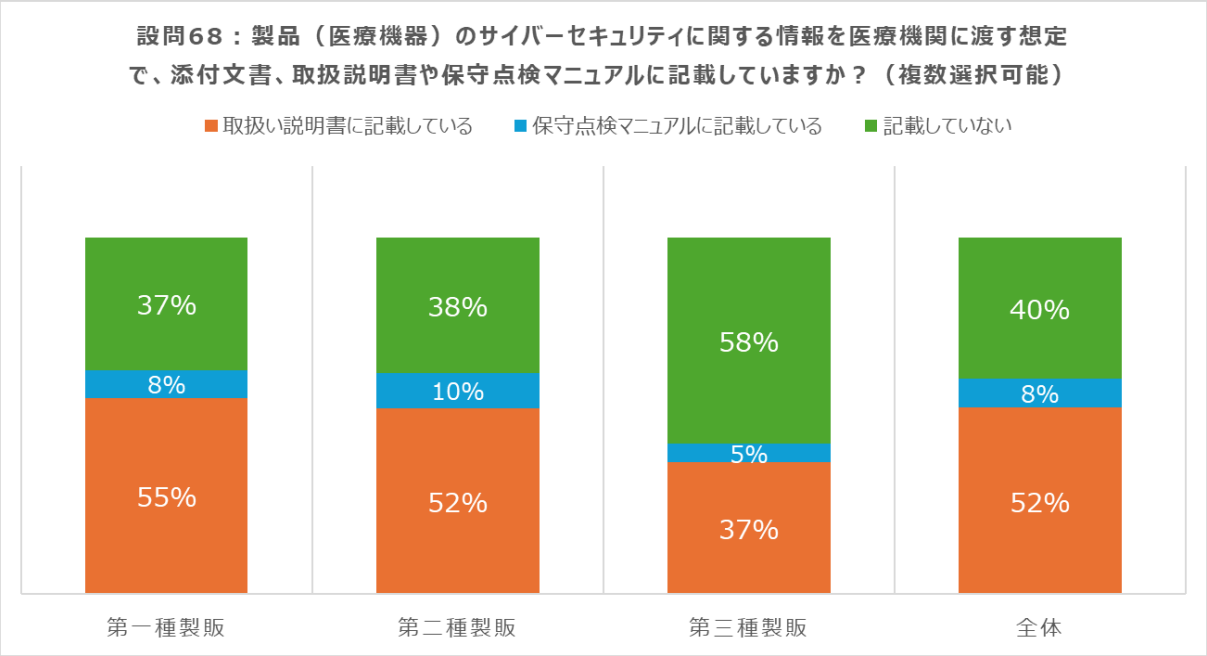
**設問 66：レガシー医療機器の対応については、どのような内容を医療機関に通知していますか？（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 使用継続のリスク | 38 | 16 | 6 | 60 |
| ネットワークから遮断する方法 | 12 | 2 | 0 | 14 |
| ファイヤーウォールなどの対応 | 12 | 7 | 5 | 24 |
| 使用継続のための費用 | 8 | 1 | 1 | 10 |
| とくに通知していない | 59 | 25 | 9 | 93 |
| レガシー医療機器を扱っていない | 9 | 7 | 2 | 18 |
| 求めに応じて | 2 | 0 | 0 | 2 |



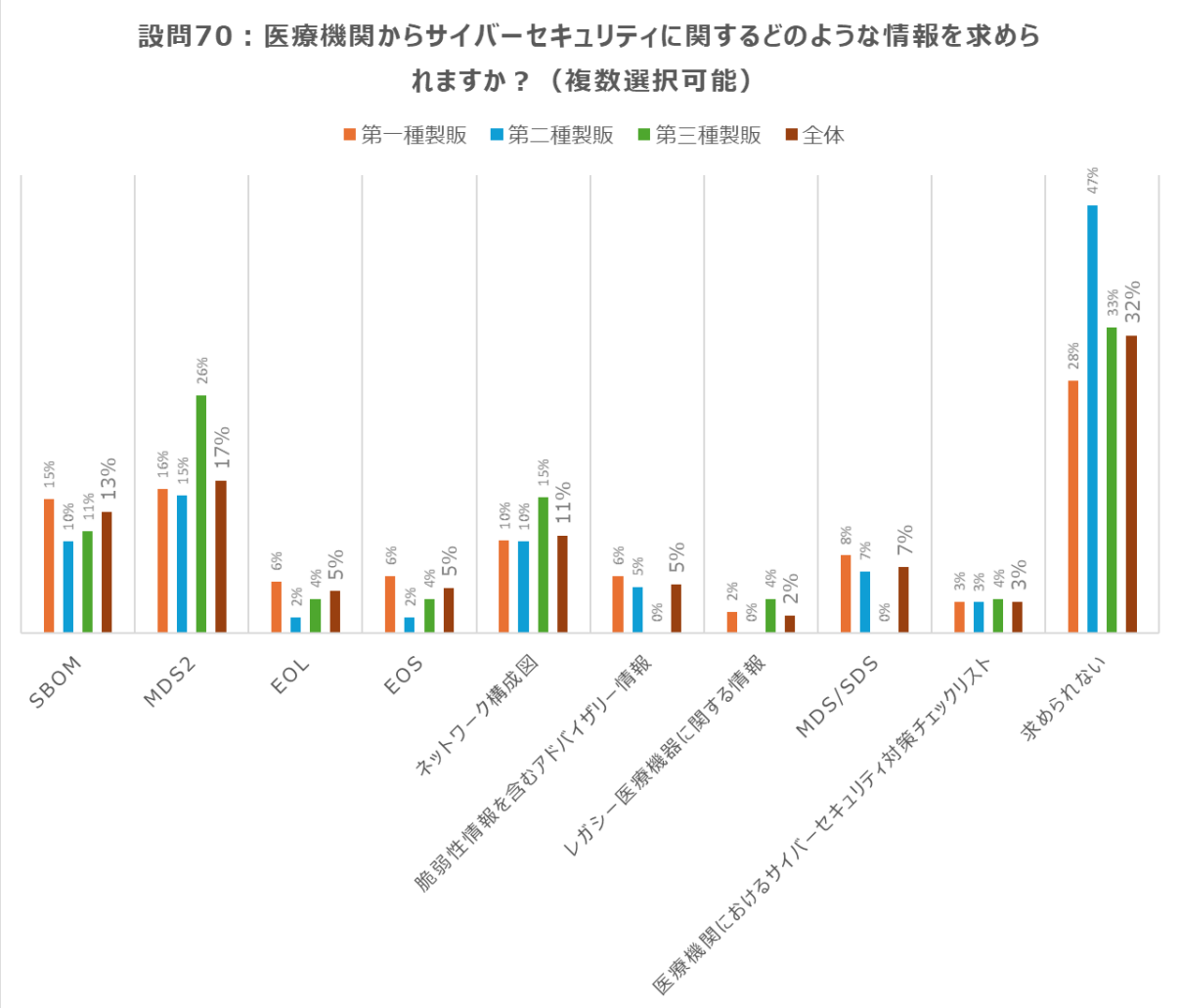
**設問 68：製品（医療機器）のサイバーセキュリティに関する情報を医療機関に渡す想定で、添付文書、取扱説明書や保守点検マニュアルに記載していますか？（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 取扱い説明書に記載している | 62 | 26 | 7 | 95 |
| 保守点検マニュアルに記載している | 9 | 5 | 1 | 15 |
| 記載していない | 42 | 19 | 11 | 72 |



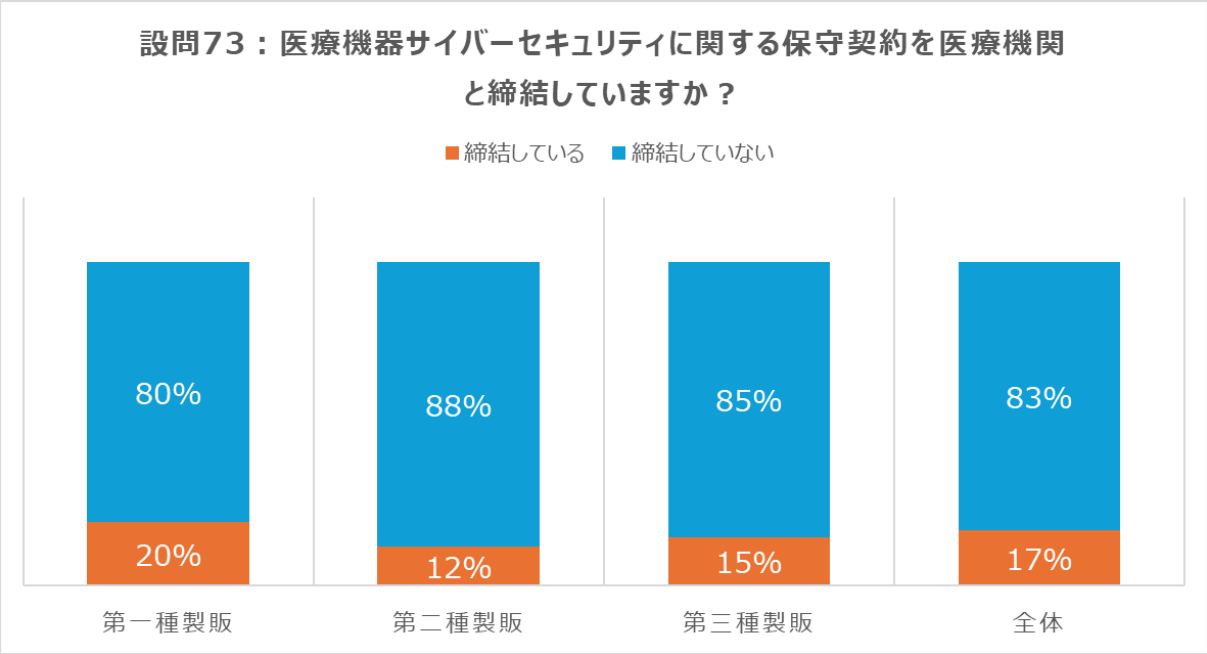
**設問 70：医療機関からサイバーセキュリティに関するどのような情報を求められますか？（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| SBOM | 26 | 6 | 3 | 35 |
| MDS2 | 28 | 9 | 7 | 44 |
| EOL | 10 | 1 | 1 | 12 |
| EOS | 11 | 1 | 1 | 13 |
| ネットワーク構成図 | 18 | 6 | 4 | 28 |
| 脆弱性情報を含むアドバイザリー情報 | 11 | 3 | 0 | 14 |
| レガシー医療機器に関する情報 | 4 | 0 | 1 | 5 |
| MDS/SDS | 15 | 4 | 0 | 19 |
| 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のうち、事業者確認用項目の確認 | 6 | 2 | 1 | 9 |
| 求められない | 49 | 28 | 9 | 86 |



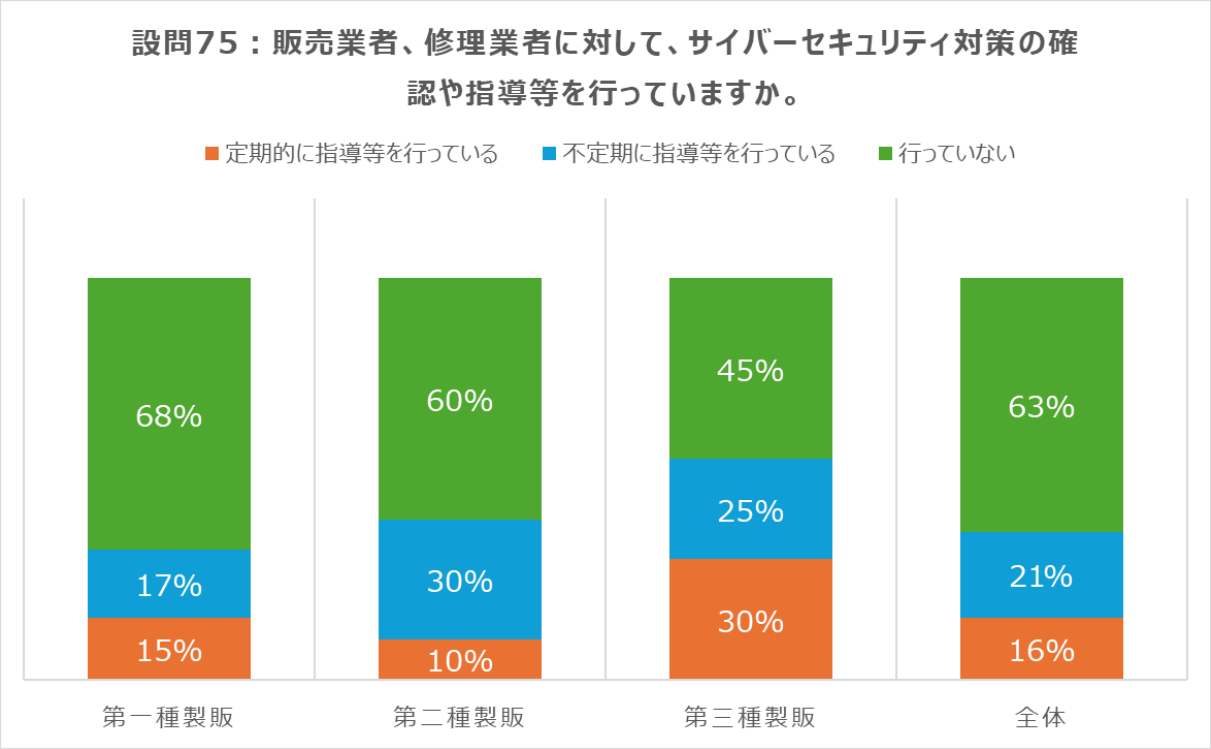
**設問 73：医療機器サイバーセキュリティに関する保守契約を医療機関と締結していますか？**

| 選択肢 | 締結している | 締結していない |
|---|---|---|
| 第一種製販 | 23 | 94 |
| 第二種製販 | 6 | 44 |
| 第三種製販 | 3 | 17 |
| 全体 | 32 | 155 |



**設問 75：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。**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 定期的に指導等を行っている | 18 | 5 | 6 | 29 |
| 不定期に指導等を行っている | 20 | 15 | 5 | 40 |
| 行っていない | 79 | 30 | 9 | 118 |



**設問 76：医療機器のサイバーセキュリティ対策についての課題と感じていることを選択してください。（複数選択可能）**

| 選択肢 | 第一種製販 | 第二種製販 | 第三種製販 | 全体 |
|---|---|---|---|---|
| 専門家の確保 | 93 | 27 | 15 | 135 |
| 専門家以外の教育 | 74 | 15 | 9 | 98 |
| 対策費用等 | 56 | 22 | 11 | 89 |
| 医療機関との連携・情報共有 | 58 | 23 | 7 | 88 |
| リスクマネジメントの具体的方法 | 45 | 13 | 10 | 68 |