セーフティ設計・セキュリティ設計に関する
実態調査結果

平成 27 年９月１０日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

はじめに

IPA／SEC では、近年の製品・サービス等が相互接続されるシステム構築に伴い発生する課題の解決策として、相互に接続される製品・サービスの信頼性を確認するための仕組みの実現を推進しています。その仕組み構築のために重要な、ハザードに対応するセーフティ設計と脅威に対応するセキュリティ設計及びその設計品質の見える化の取組みについて、産業界の現在の状況を把握するために実施したアンケート結果を報告書として取りまとめました。

本調査は、株式会社ユビテックを請負先として、実施しました。

掲載されている会社名・製品名などは、各社の登録商標または商標です。

「セーフティ設計・セキュリティ設計に関する実態調査結果」

2015 年 9 月 10 日

独立行政法人情報処理推進機構

© Information-technology Promotion Agency, Japan. 2015 All Rights Reserved

目次

図一覧

表一覧

1 概要

1.1 調査目的

平成 25 年度「ソフトウェア開発の取引構造（サプライチェーン）の実態に関わる課題の調査」の結果、今後取り組むべき課題の解決策として、品質基準等が異なる製品間の制御可否判断を行う仕組みや、想定されるリスクや不安な組合せを利用者に知らせるために警告する仕組みの構築等が必要とされていることが明らかになった。また、さまざまな製品にネットワーク機能が普及し、自動車や家電でもパソコン同様に侵入、情報漏えいなどのセキュリティの問題が発生することに加え、新たな機能や製品の登場によってこれまでにない要因による火災やけがなどのセーフティの問題も発生している。

このため、相互に接続される製品・サービスの信頼性を確認するための仕組みを実現するために、ハザードに対応するセーフティ設計と脅威に対応するセキュリティ設計の取組み状況と、アシュアランスケースを使うことによる設計品質の見える化の取組み状況を把握し、産業界（主に中小企業のシステム・サービス・ソフトウェア開発者）にこれらの取組みを広く普及させるための調査を行った。

調査結果は、広く産業界にセーフティ設計とセキュリティ設計を定着させ、かつセーフティとセキュリティの設計品質の見える化の普及を図ることを目的に取りまとめを行い、実態調査結果とガイドブックとしてまとめることとした。

1.2 調査手法

IPA/SEC では平成 18 年、身の回りのシステムの安全性向上のための入門書を「組込みシステムの安全性向上の勧め（機能安全編）」[1]として公表している。本調査では前述の入門書を参考にしながら、「スマート化」が進む消費者向け製品（以下、消費者製品）として自動車、ヘルスケア製品、スマートフォン、スマート家電の 4 分野についてセーフティ設計、セキュリティ設計、アシュアランスケースの利用による設計品質の見える化の取組み状況の実態を調査するアンケートを行った。

これらのアンケート結果をもとに実態調査結果の取りまとめを行い、対策としてガイドブックの編集を行う。ガイドブックについては入門者向けの内容とするため、関連分野の有識者で構成するワーキンググループにおいて検討を進める。

[1] IPA/SEC, “組込みシステムの安全性向上の勧め（機能安全編）,” [オンライン]. Available: http://www.ipa.go.jp/sec/publish/tn05-011.html

1.3　アンケートから判明した事項

以下に、今回のアンケート調査から判明した事項と、それに関連する記載のある項番号を記す。

- すべての回答者が、セーフティ設計またはセキュリティ設計のいずれか、もしくは両方が必要と回答。
  ⇒2.8.1.6
- セーフティ設計またはセキュリティ設計の基本方針を明文化している組織は半数以下である。
  ⇒セーフティ設計　2.8.2.2
  ⇒セキュリティ設計　2.8.2.5
- 基本方針に基づいたセーフティ設計、セキュリティ設計のルールについても明文化率は低くその実施は開発リーダーなどの判断に任されている。
  ⇒セーフティ設計　2.8.3.1、2.8.3.3
  ⇒セキュリティ設計　2.8.3.5、2.8.3.7
- セーフティ・セキュリティの重要な設計上の判断への経営層や品質保証部門等の責任者の関与が少ない。
  ⇒セーフティ設計　2.8.4.6、2.8.4.7
  ⇒セキュリティ設計　2.8.4.13、2.8.4.14
- 回答者のうち約 3 割がセーフティ要件・セキュリティ要件を発注時に受注者側へ提示していない、あるいは受注時に発注者側からセーフティ要件・セキュリティ要件を提示されていないと回答。
  ⇒セーフティ要件　発注時 2.8.6.1、受注時 2.8.6.2
  ⇒セキュリティ要件　発注時 2.8.6.4、受注時 2.8.6.5
- セーフティ設計のハザード分析で利用されている手法・ツールは FMEA、FTA、HAZOP の三大ツールに集中している。一方、セキュリティ設計のリスク分析で利用されている手法・ツールにはばらつきがあるものの、ハザード分析手法である FMEA、FTA、HAZOP の利用が確認された。
  ⇒セーフティ設計　2.8.5.1
  ⇒セキュリティ設計　2.8.5.9
- 設計品質の見える化はあまり進んでいないと想定されるが、回答者の多くは興味を持っている。一部ではグラフィカルな手法である GSN、CAE、D-Case を利用している。
  ⇒セーフティ設計　2.8.5.5、2.8.5.6
  ⇒セキュリティ設計　2.8.5.13、2.8.5.14
- 接続先の製品・ソフトウェアの設計品質やセーフティ・セキュリティ対策レベルを確認して接続制御などに利用する仕組みは検討例があるものの、半数以上が未検討である。
  ⇒セーフティ設計　2.8.7.3
  ⇒セキュリティ設計　2.8.7.7

2 セーフティ設計・セキュリティ設計に関する実態調査のためのアンケート結果詳細

企業･団体等におけるセーフティ設計とセキュリティ設計及び設計品質の見える化の取組み状況を確認し、その実態に即した対策内容をガイドブックに反映することを目的として、アンケート調査を実施した。以下にアンケート調査の結果を示す。

2.1 アンケート結果の概要

セーフティとセキュリティの対策手法に関するアンケート結果からは、セーフティではFTA,FMEA, HAZOPがハザード分析手法として比較的よく利用されており、これらの分析手法がセキュリティにも利用されている例をいくつか確認できた。しかし、こうした実績がある分析手法の結果を､第三者に理解しやすいように構造化した議論の結果として示す手法についてはごく一部での利用があるだけで、ほとんどの場合は知られていない状況がわかった。

これらのアンケート結果は消費者製品の開発に関連する企業・部門のうち、比較的先進的だと考えられる部門に対する調査に基づくものであるため、産業界全体としては今後も、具体的な手法の活用方法などを含めた普及を進める活動が必要だと考えられる。なお、その際は製品のタイプや分野によってセーフティとセキュリティが対応すべき深刻度が異なる状況があるため､必要に応じたムダのない取組みを行う必要があると考えられる。

2.2 アンケートの実施方針

実施方針として、消費者製品の開発におけるセーフティ設計、セキュリティ設計、設計品質の見える化の取組みを先行して実施していると想定される企業の状況を収集することとした｡また､セーフティ設計とセキュリティ設計の対比を行うため､セーフティとセキュリティについて同じ設問項目を用意した。

アンケートの主目的としては設計手法の収集であるため、依頼する先の担当者としては、できるだけ開発部門のリーダーにお願いするようにした。また、設計品質の見える化の取組み状況を確認するため、外部との要件の授受と、外部の製品を連携させるか組込む時の設計品質の確認方法、アシュアランスケースの手法などの設問を設けた。

設問が専門的であるため、アンケート回答者は開発部門でなくても可能としつつ、回答を集計する際に、どのような部門の方の回答であるか目安をつけるため、担当する部門を設問で確認した。

アンケート対象として先行して実施していると想定される企業を選定しているため､統計的に分析を行うと無作為抽出の場合と大幅に異なる結果が予想されるため､統計分析は必要な部分のみとした。ただし、消費者製品の分野について偏りがないように消費者製品の分野を「自動車」「ヘルスケア」「スマート家電」「スマートフォン」に分けて、それぞれ10件以上の有効回答を集めるようにした。各分野については、完成品メーカー、部品メーカー、サービス提供事業者などが含まれる。この4分野以外については「その他分野」としており、その他分野に含まれる業界分野は制御システムと、組込み系の部品・モジュールメーカーなどである。

2.3 アンケート項目の構成

前節の方針を受けて図 2-1 のようにアンケートの設問を構成した。

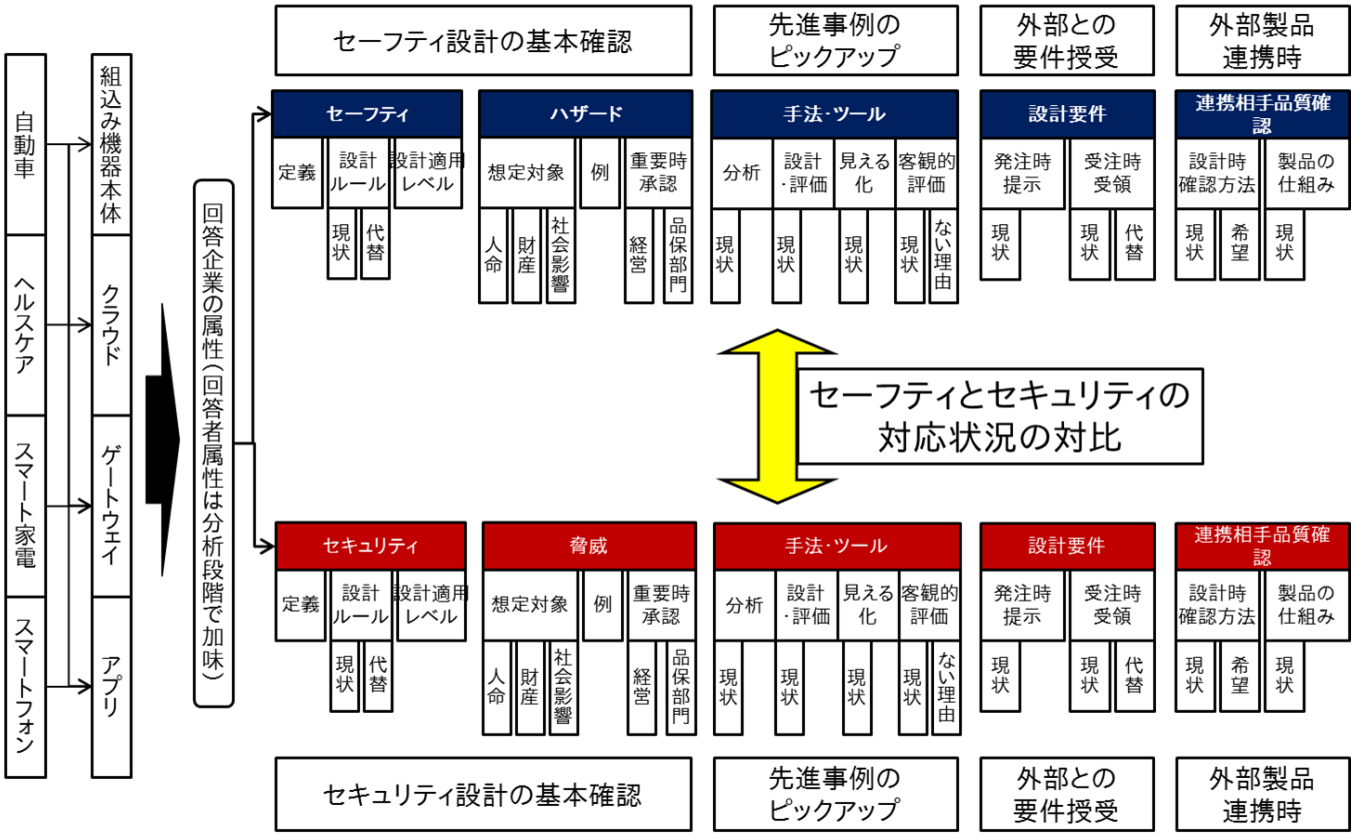


図 2-1 アンケート項目の構成

2.4　アンケート調査票のイメージ

アンケート調査票では、

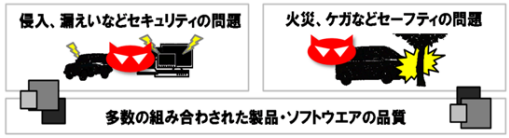
図 2-2 のように、このアンケート調査の趣旨と、セーフティとセキュリティ、設計品質の見える化について、簡単な図入りで説明することで趣旨を理解しやすくした。なお、配布したアンケート調査票は「4 付録 アンケート用紙」にある。

表紙イメージ

独立行政法人 情報処理推進機構 ソフトウェア高信頼化センター(IPA/SEC)
セーフティ・セキュリティ設計の見える化推進のためのアンケート

□自動車　□スマートフォン　□ヘルスケア　□スマート家電 向け

近年、さまざまな製品にネットワーク機能が普及し、パソコン同様に自動車や家電でも侵入、情報漏えいなどのセキュリティが問題になっています。また、新たな機能や製品の登場で、これまでにない要因による火災やけがなどのセーフティの問題も発生しています。しかし、現在のスマート製品を支えるソフトウェアは規模が大きく、他社から調達した部品が多数組合せられているため、セキュリティやセーフティを含めた品質の確保や確認に、課題が多いと指摘されています。



IPA/SEC では、ソフトウェアのセーフティ・セキュリティ設計の普及や設計品質の見える化を推進し、これによりオープンソース、発注先が開発したソフトウェア、市販モジュール等のセーフティ・セキュリティ設計について、採用する企業が容易に設計品質を確認し、安心して利用できる社会を目指しています。今回は、セーフティやセキュリティに関する設計の実態を把握する為にアンケートを実施することになりました。ご協力をお願いいたします。

※アンケートの設問の構成は以下のとおりです。
- ○ご回答者のプロフィール　（設問Ａ～カ）
- ○セーフティ設計について　（設問１～２２）
- ○セキュリティ設計について　（設問２３～４４）
- ○その他　（設問４５、４６）

アンケートのご回答について

※製品企画、システム設計、安全設計、品質保証などの部門のリーダーの方にご回答をお願いいたします。ご回答にかかる時間の目安は 20 分程度です。
※ご回答用紙は同封の封筒かメールにて、9 月 2 日(月)着で ご返送頂けますと幸いです。
※セーフティ設計とセキュリティ設計の設問を別の方が回答される場合には、本回答用紙全体をコピーして、別途ご記入・ご返送ください。

※本アンケートのご回答は統計処理した上でガイドブックと報告書に利用し、個々の企業名などの情報は公開しません。また、個人情報は本調査以外の目的では使用しません。

お問合せ・返送先：(IPA/SEC はアンケート業務を以下の企業に委任しております)

TEL　　E-MAIL:

1

設問シート

B．セーフティ設計の基本方針について

ここでは、貴部門でのセーフティ設計についてお伺いします。

設問１　あなたのご担当部門でいう「製品のセーフティ」には、何が含まれますか？（複数回答）
1．ユーザの命や身体の安全を守るもの　　2．ユーザの財産や利用環境を守るもの
3．関連法令や基準の安全に関わる事項（具体的に：　　）
4．発注者から「セーフティ」として与えられた要件
5．その他（具体的に：　　）
6．製品や開発案件ごとに異なる　　7．特に「セーフティ」は考えていない

設問２　あなたのご担当部門には「製品のセーフティ設計」に関する基本方針がありますか？（最も近いものを一つ）
1．「製品のセーフティ設計」に特化した、明文化された基本方針がある
2．「製品のセーフティ設計」を含む、明文化された基本方針がある
3．明文化された基本方針はない

設問３（設問２で３を選ばれた方へ）　明文化した基本方針の代わりに、何をセーフティ設計の基準にされていますか？（複数回答）
1．社内に暗黙の基本方針がある　　2．過去の開発内容に基づいて判断している
3．機種ごとに検討し、判断している　　4．開発リーダーが判断している
5．その他（具体的に：　　）
6．セーフティ設計の基準は必要ない

C．セーフティ設計の設計ルールについて

ここでは、貴部門でのセーフティ設計の設計ルール（具体的な設計プロセスやレビュー手続きなど）についてお伺いします。

設問４　御社には、セーフティ設計の設計ルールがありますか？（最も近いものを一つ）
1．セーフティ設計に特化した、明文化された設計ルールがある
2．セーフティ設計を一部とする、明文化された設計ルールがある
3．外部の設計ルールを導入している（具体的に：　　）
4．明文化された設計ルールはない

設問５（設問４で４を選ばれた方へ）セーフティ設計ルールの代わりになるものはありますか？（最も近いものを一つ）
1．社内に暗黙の設計ルールや習慣がある
2．リーダーなどの判断に任されている
3．その他（具体的に：　　）
4．セーフティ設計ルールは必要ない

2

図 2-2 アンケート調査票のイメージ

2.5 アンケートの仮説と対応

表 2-1 に、アンケートの仮説と対応を示す。

表 2-1 アンケートの仮説と対応

分類	仮説	アンケートへの反映	仮説検証時の対応
セーフティ・セキュリティ設計の実態	標準化が進んだ分野（自動車）を除けば、独自の手法で対応している企業が多い。	「独自の手法で行っている」という選択肢を設けた。	独自手法を補完、代替しうるものとして、先進的な手法・ツールの有効性を説明。
４分野間の比較	セーフティ・セキュリティ設計の対応が分野間で大きく異なる。	分野に分けて集計できるよう設計した。	進んでいる分野も進んでいない分野も活用できるよう、記述に配慮。
経営の関わり	ハザード・脅威対応の判断に経営が関わっていない企業も多い。	経営の関わりの設問を追加。	経営者にも有効なガイドブックとする。
セーフティ・セキュリティ設計手法・ツール	既存の手法・ツールを使ってみた企業も少なくない。	できるだけ、手法・ツール名を列記し、選択しやすくした。	ガイドブックで取り上げる手法・ツール名の優先度付けに活用。
セーフティ設計とセキュリティ設計の差	セキュリティ設計はセーフティ設計よりも進んでいない（標準化も同様）。	設問を分け、両者を対比できるようにした。	結果に基づいて、セキュリティ設計の説明レベルを調整。
設計品質の見える化	設計品質の見える化は進んでいないが、興味はある。	興味の有無を伺う設問を追加。	ガイドブックの見える化部分のボリュームに反映。
同上	見える化に興味がある企業には、導入していない理由もある。	上記設問に、人手や時間、費用対効果の課題を付加した。	ガイドブックに、課題解決に向けた記載を追記（「トータルでは効率化、コスト削減効果もある」など）
発注元、発注先との要件の授受	発注元、発注先とのセーフティ・セキュリティ要件の授受を行っていない企業も少なくない。	要件の授受の設問を追加。	アンケート結果の分析に活用（設計手法の導入が進んでいない理由となっている可能性があるなど）

2.6　アンケート分析フロー

図 2-3 に、アンケートの仮説に基づく分析フローとガイドへの反映案を示す。

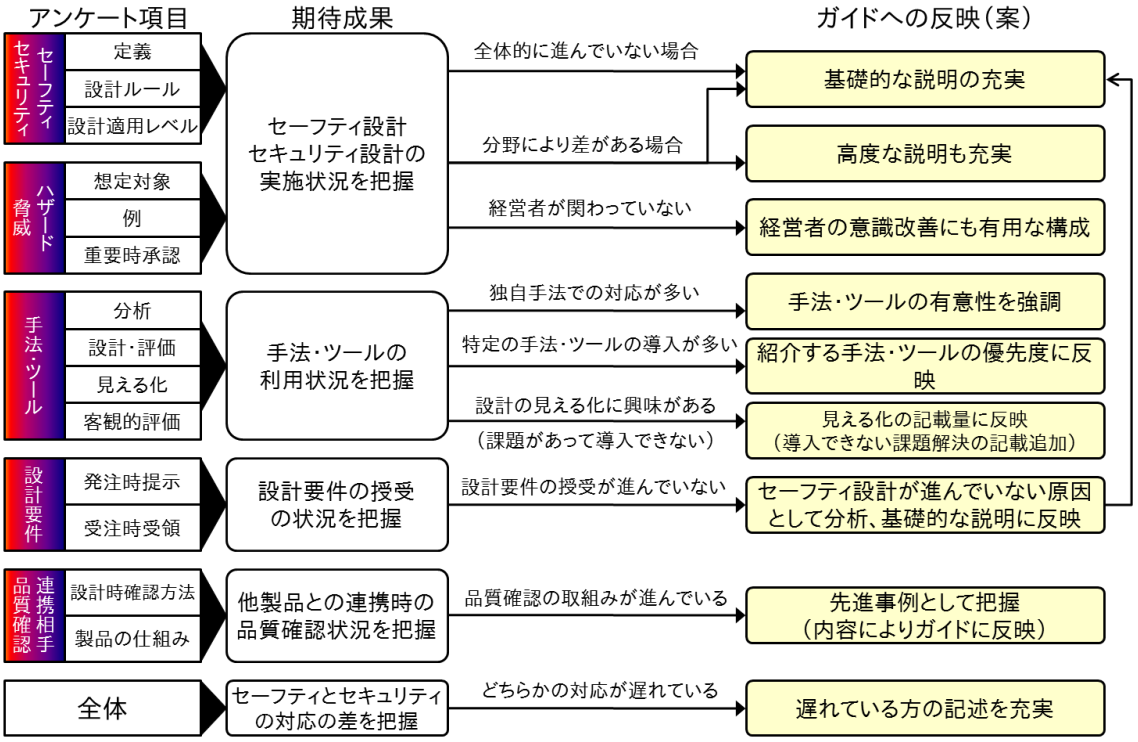


図 2-3 アンケート分析フロー

2.7　アンケート実施状況

以下にアンケート全体の実施状況を示す。

合計配布件数:　320 件

回収件数:　68 件

回収率:　21.3%

以下にアンケート依頼先別の実施状況を示す。

1．自動車、スマートフォン、ヘルスケア及びスマート家電分野でセーフティとセキュリティの対応が進んでいると思われる組織を抽出

配布・回収方法:　郵送とメールで送付

実施期間：　平成 27 年 2 月 12 日～4 月 10 日

配布件数:　89 件

回収件数:　53 件

回収率:　60%

2．関係する団体 1

配布・回収方法: 団体事務局から企業会員向けにメールで配布、調査請負会社に回答

配布期間: 2 月 27 日（金）～ 3 月 16 日（月）

配布件数: 187 件 （団体別の回収数と回答内容数は調査の対象外）

3．関係する団体 2

配布・回収方法: 団体事務局から企業会員向けにメールで配布、事務局が回収し結果のみ調査請負会社に回答

配布期間： 2 月 25 日（水）～3 月 9 日（月）

配布件数: 44 件 （団体別の回収数と回答内容数は調査の対象外）

2.7.1 分野別有効回答数

以下のグラフに分野別有効回答数を示す。N は有効回答数。横軸は回答数。

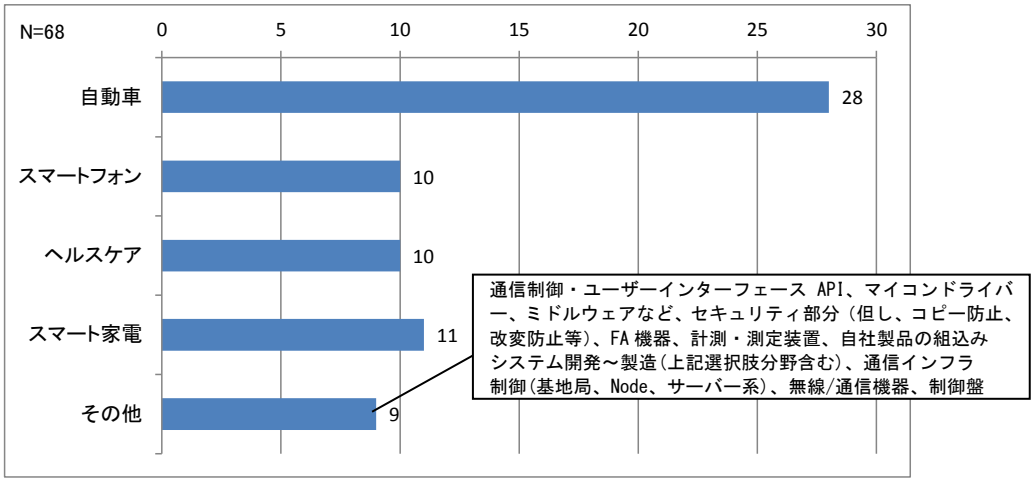


図 2-4 分野別有効回答数

2.8 アンケート結果

以下に、アンケートの集計結果と状況を示す。設問の内容と選択項目の詳細については「4 付録 アンケート用紙」を参照のこと。

2.8.1 回答者プロフィール

2.8.1.1 設問イ)あなたの事業部門が開発されている製品やソフトウェアはどの部分に当たりますか？(複数回答)

N は合計回答数。横軸は複数回答の回答数。

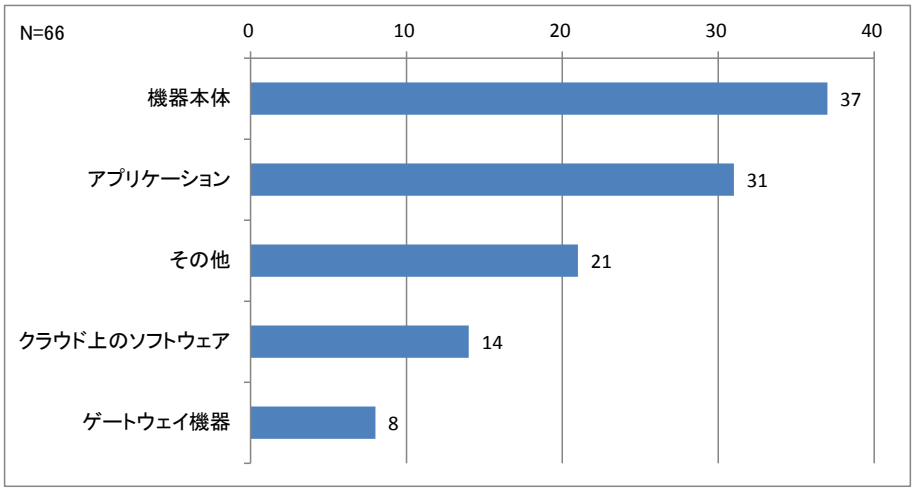


図 2-5 開発している製品

2.8.1.2 設問ウ)あなたが担当されている業務は、何でしょうか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

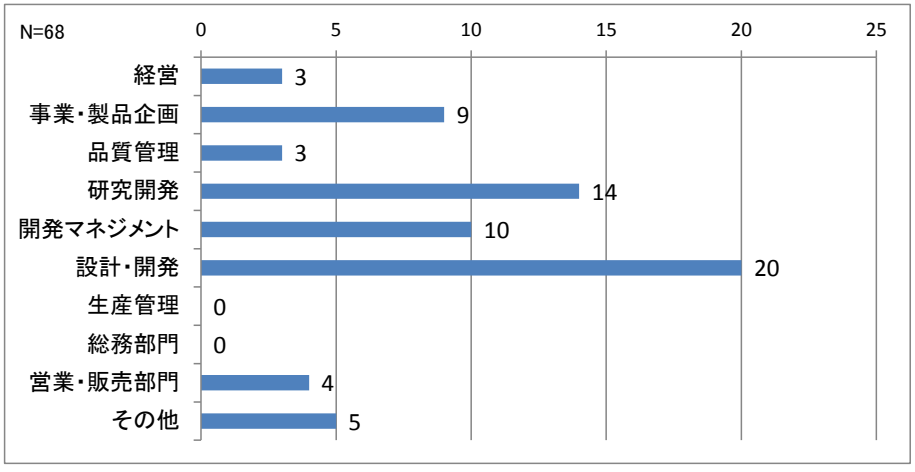


図 2-6 回答者の担当業務

経営から営業まで幅広い層から回答があった。

事業・製品企画担当はセーフティ・セキュリティ設計の詳細を把握していなかったり、設計・開発担当は製品全体のハザード・脅威分析について把握していないなど、担当業務が回答に影響している可能性がある。

2.8.1.3 設問ウ)「分野」×「担当業務」

N は合計回答数。横軸は回答数。

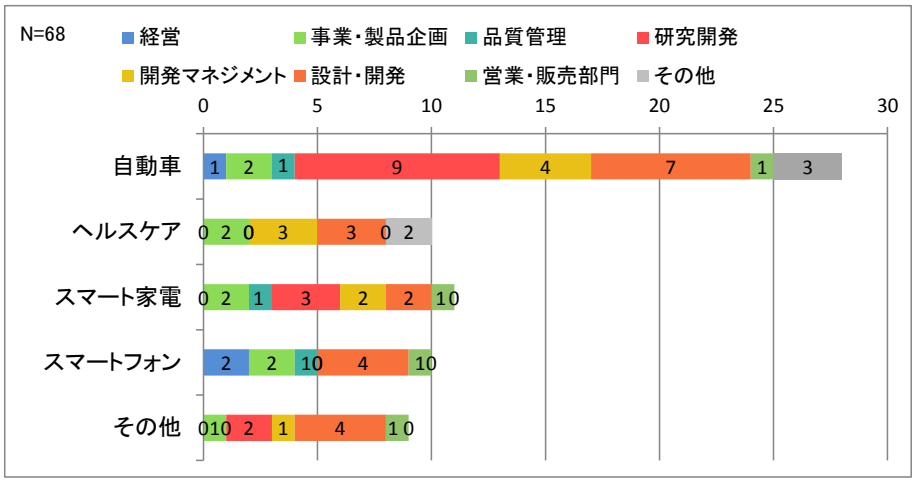


図 2-7 分野別回答者の担当業務

担当業務が分野間で偏りがでた。「研究開発」からの回答は自動車分野では 1/3、スマート家電では 1/4 を占めるが、ヘルスケア、スマートフォンでは 0 人となっている。

分野別の集計を行う場合には、この偏りを考慮する必要がある。

2.8.1.4 設問エ)あなたが担当されている業務の経験年数は何年でしょうか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

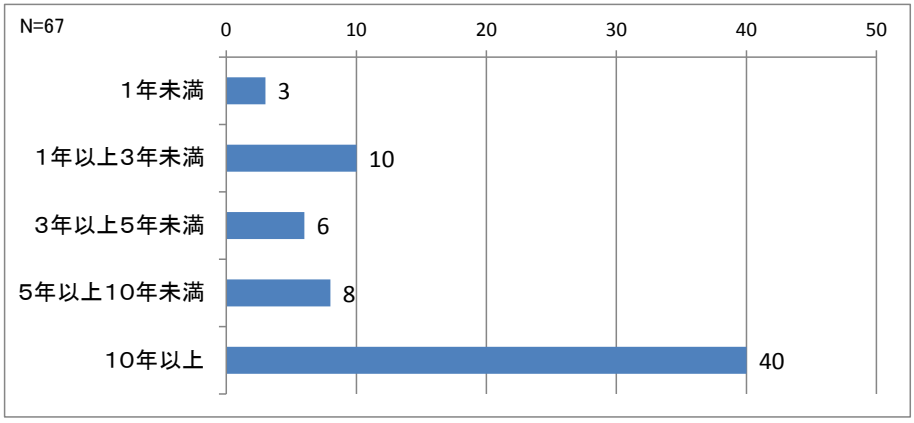


図 2-8 担当者の経験年数

「設計・開発」→「開発マネジメント」のように上流へのシフトにより経験年数がリセットされる場合もあるため、「経験年数が短い」＝「若い」とはならない。

製品サイクルが短い分野の方が業務の経験年数が短くなると想定される。

2.8.1.5 設問エ)「分野」×「業務の経験年数」

N は合計回答数。横軸は回答数。

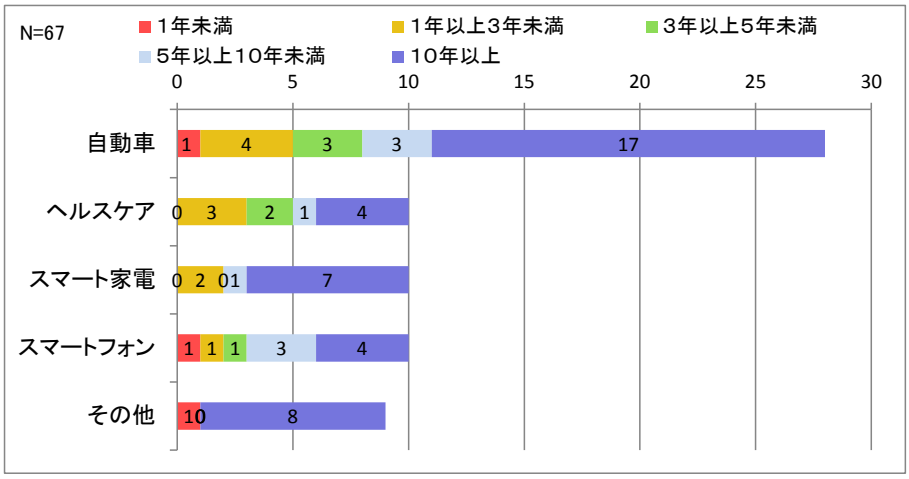


図 2-9 分野別担当者の経験年数

製品のサイクルが長い自動車では経験年数が 10 年以上の回答者が多い。

スマート家電でも同様であるが、テレビやエアコンなど昔からある製品がベースとなっているためと思われる。

2.8.1.6 設問オ)セーフティ設計またはセキュリティ設計の必要性はお感じですか？(どれか一つ)

N は合計回答数。横軸は回答数。

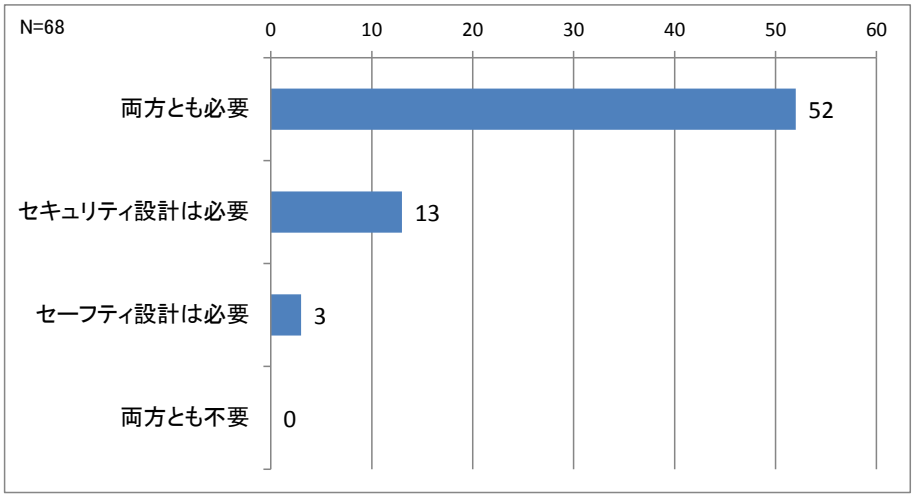


図 2-10 セーフティ･セキュリティの必要性

セーフティ･セキュリティ設計に関心があると想定される企業にアンケートを行ったことは考慮する必要はあるが、すべての回答者がいずれか又は両方を必要と回答した。

2.8.1.7 設問オ)「分野」×「セーフティ・セキュリティ設計の必要性」

N は合計回答数。横軸は回答数。

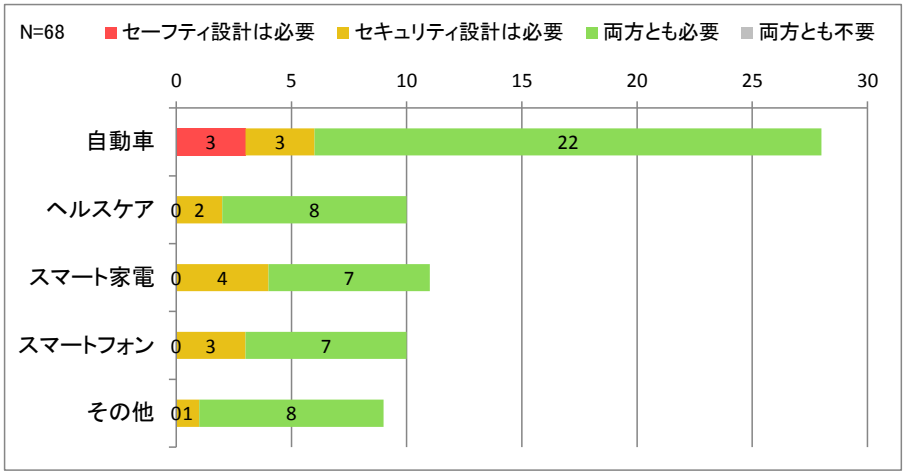


図 2-11 分野別セーフティ・セキュリティの必要性

「セーフティ設計は必要」という回答は自動車のみである。これはセキュリティ意識が低いというよりは、回答者の業務におけるセーフティの比重が高いためではないかと想定される。

自動車分野における「セキュリティ設計は必要」という回答は車載機や ECU ソフトウェア開発ツールのメーカーからの回答であった。

2.8.1.8 設問カ)国際規格で認証を取得されているものがありますか？（複数回答）

N は 1 項目以上回答した回答者数。横軸は複数回答の回答数。

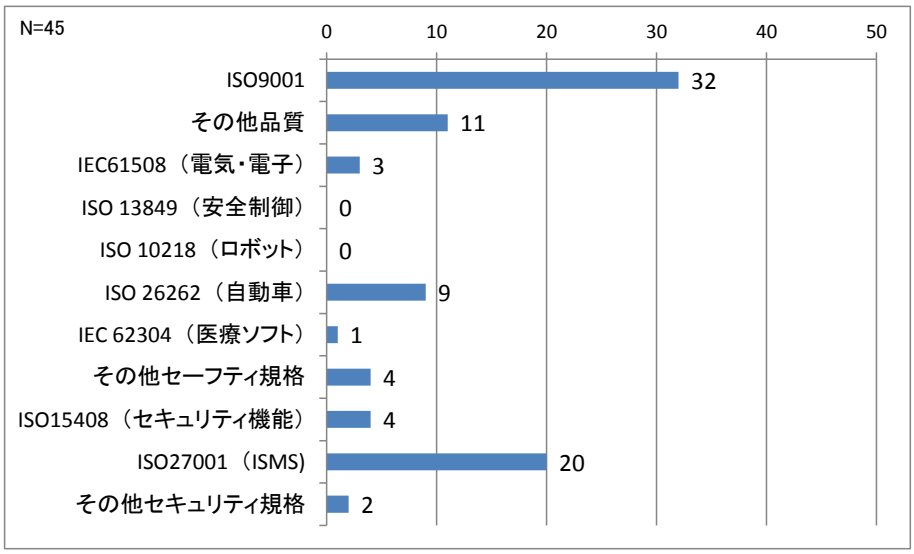


図 2-12 認証取得済みの国際規格

分野によって関連する標準が異なるため、ばらついた結果となっている。

ただし、品質に関する ISO9001 及び組織の情報セキュリティ ISO27001 については、取得している回答者は多い。

2.8.2 設計の基本方針

2.8.2.1 設問１)あなたのご担当部門でいう「製品のセーフティ」には、何が含まれますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

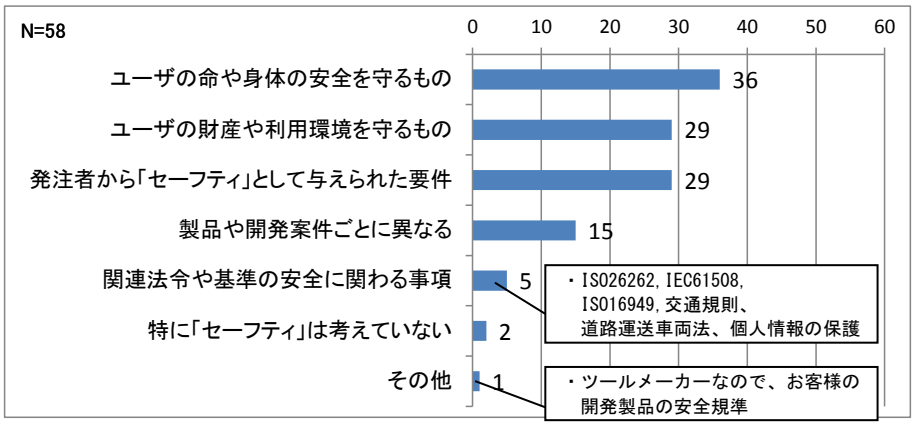


図 2-13 製品のセーフティ

最初の 2 つの選択肢に着目した場合、二つとも選択した回答者がいた一方、いずれか片方を選択した回答者も多かった。 自動車分野はセーフティを重視する結果だった。

- 「ユーザーの命や身体の安全を守るもの」を選択：17 件　例：自動車 10 件
- 「ユーザーの財産や利用環境を守るもの」を選択：10 件　例：自動車　1 件
- 2 つとも選択：　19 件　例：自動車　9 件

- 関連する法令や基準
  - IEC61508
  - ISO16949
  - ISO26262
  - 交通規則、道路運送車両法
  - 個人情報の保護
- その他
  - ツールメーカーなので、お客様の開発製品の安全規準

2.8.2.2 設問２）あなたのご担当部門には「製品のセーフティ設計」に関する基本方針がありますか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

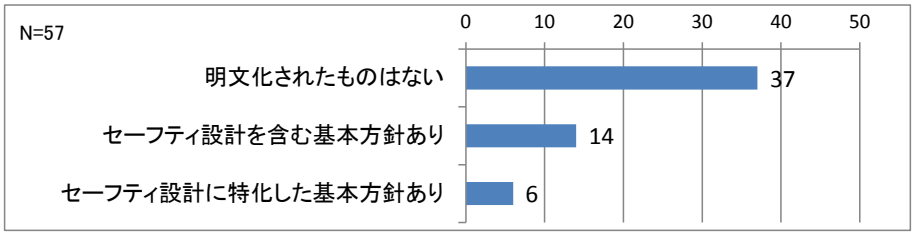


図 2-14 セーフティ設計基本方針

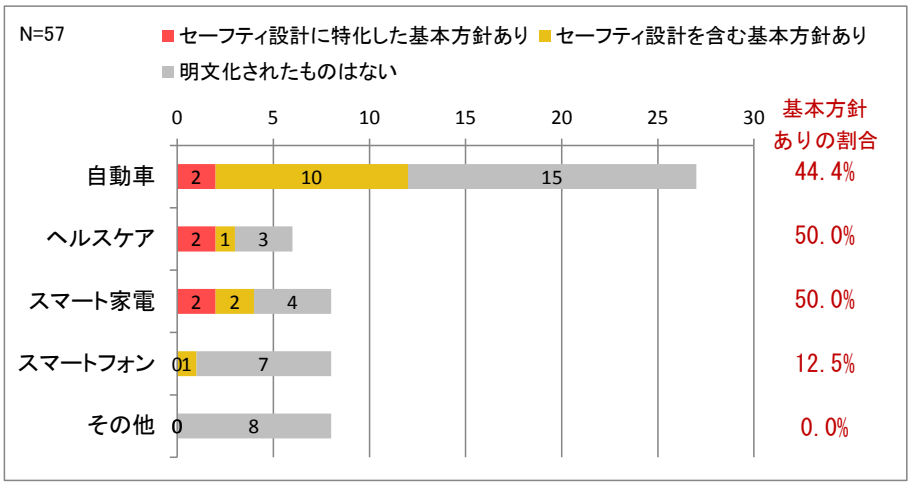


図 2-15 分野別セーフティ設計基本方針

半数以上がセーフティ設計に関する基本方針がないという回答だった。

基本方針があるという回答は自動車分野の比率が高いと予想されたが、分野別に見るとヘルスケア、スマート家電も比率が高い。守るべき対象に違いはあっても、セーフティへの取組み傾向は似ている。

2.8.2.3 設問３)(設問2で3を選ばれた方へ）明文化した基本方針の代わりに、何をセーフティ設計の基準にされていますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

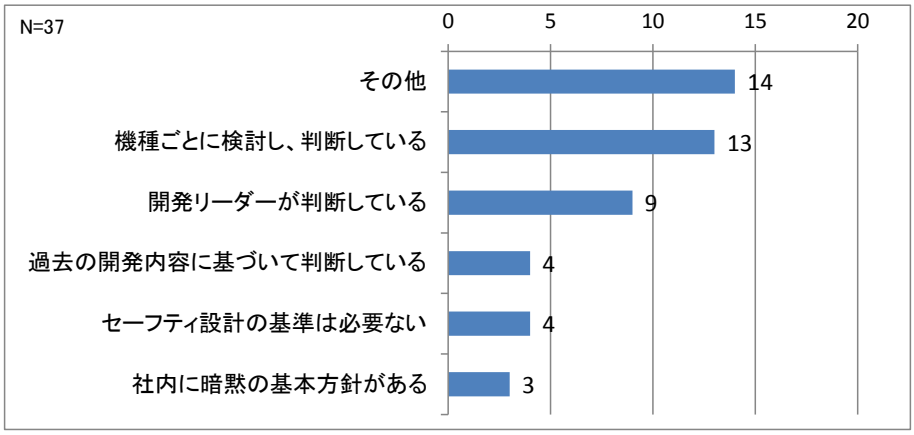


図 2-16 基本方針の代替

設問 2 で「明文化されたものはない 」を選択された方への設問。

「その他」以外では「機種ごとに検討し、判断している」がトップ。

「その他」の自由記述では顧客・発注者の基準という回答が多く見られる。

- その他
  - 顧客・製品ごとに設けられた基準に従う（3 件）
  - 受託開発となる為、顧客提示の基準に従う
  - 顧客の要望に応じた基準設計を行う
  - 要求仕様に従う
  - 発注者と基準を協議
  - ISO や IEC の規約が基準となる
  - 開発プロセスのルールに安全を含むルールがあるので十分と考える
  - 製作所ごとの基準
  - ISO26262 に準拠した社内機能安全規定書
  - FMEA
  - 開発プロジェクト（製品ごとに独自の基準を持っている）
  - 顧客先に従事している

2.8.2.4 設問２３）あなたのご担当部門でいう「製品のセキュリティ」には、何が含まれますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

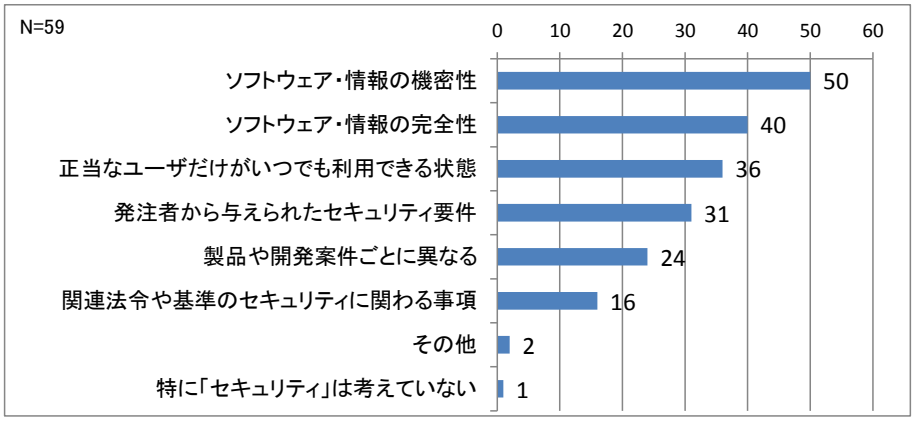


図 2-17 製品のセキュリティ

「ソフトウェア・情報の機密性」は、回答者の 86％が選択している。上位 3 つは CIA（機密性、完全性、可用性）であり、担当者のセキュリティ知識がうかがえる。

- 関連法令や基準
  - クレジット関連国際規格
  - GW のなりすまし、踏み台の回避、Web インジェクションなどの対策
  - IEC62443
  - ISO/IEC15408
  - 各国電波法、規格毎のセキュリティ事項
  - ISO 15408
  - サイバーセキュリティ法
  - 個人情報の保護
  - 企画書に則った実装
  - 個人情報保護法、著作権保護法に加えセーフティに関連する法案
  - PCI DSS、ISO 27001
- その他
  - 現在、JASPER[2]等で論議中
  - 法、規則の定めに合致する

[2]一般社団法人 JASPER, https://www.jaspar.jp/

2.8.2.5 設問24)あなたのご担当部門には「製品のセキュリティ設計」に関する基本方針がありますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

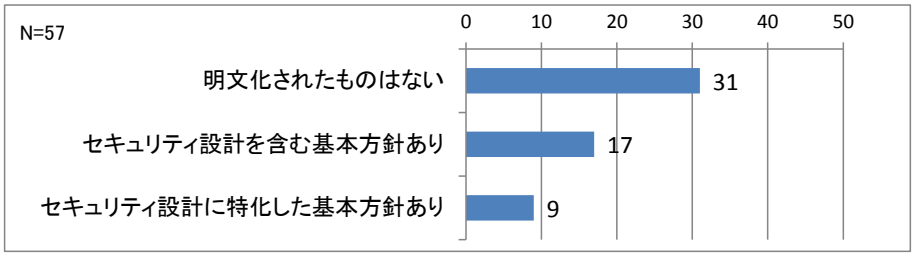


図 2-18 セキュリティ設計基本方針

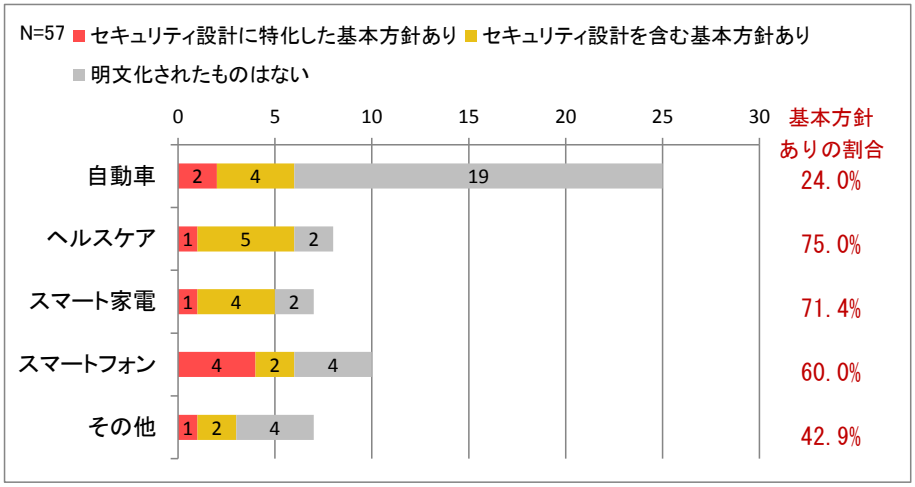


図 2-19 分野別セキュリティ設計基本方針

半数以上がセキュリティ設計に関する基本方針がないという回答だった。

セーフティとは逆に、基本方針があるという回答は自動車分野の比率が低い。

その他の分野は、セーフティと比較して基本方針がある比率が高い。

2.8.2.6 設問２５）（設問２４で３を選ばれた方へ）明文化された基本方針の代わりに、何をセキュリティ設計の基準にされていますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

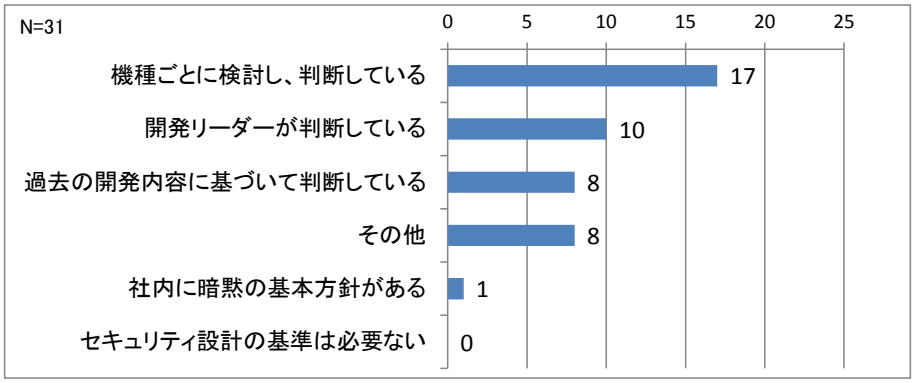


図 2-20 基本方針の代替

設問 24 で「明文化されたものはない 」を選択された方への設問。

セーフティ同様、「機種ごとに検討し、判断している」がトップ。

「その他」は 8 件であり、セーフティと異なり、顧客・発注者の基準という回答は 2 件に留まっている。

2.8.3 設計のルール

2.8.3.1 設問４)御社には、セーフティ設計の設計ルールがありますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

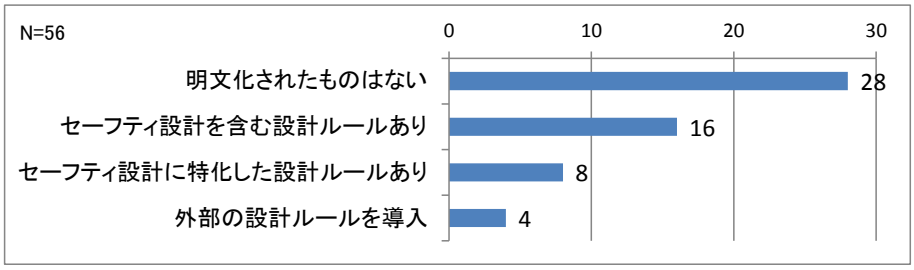


図 2-21 セーフティ設計ルール

2.8.3.2 設問４)「分野」×「セーフティ設計ルール」

N は合計回答数。横軸は回答数。

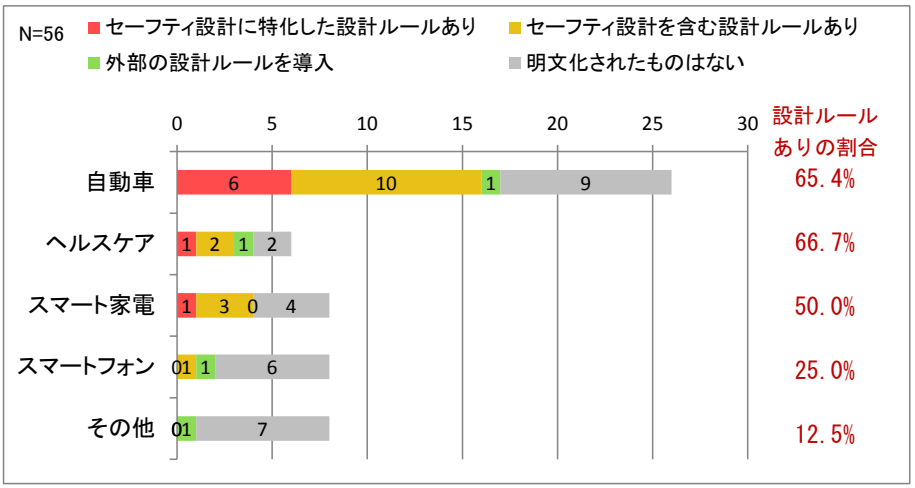


図 2-22 分野別セーフティ設計ルール

セーフティ設計の設計ルールを明文化している組織は半数であった。

分野別に見ると、自動車分野の 6 割以上の回答者が何らの設計ルールがあると回答しており、基本方針の有無よりも大幅に増加している。

2.8.3.3 設問５)(設問４で４を選ばれた方へ)セーフティ設計ルールの代わりになるものはありますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

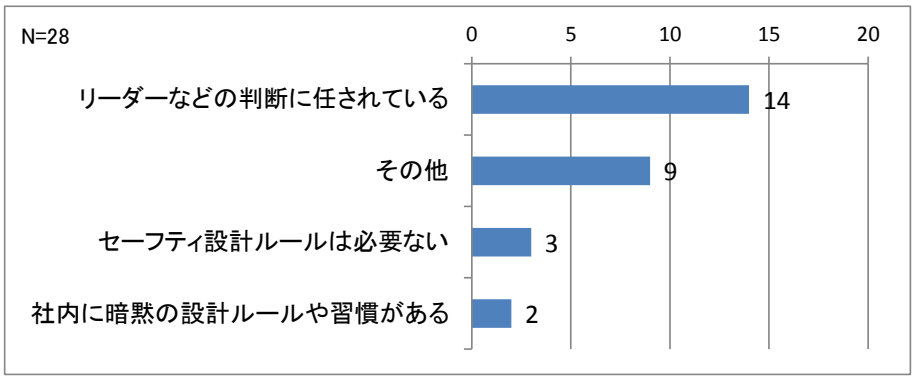


図 2-23 設計ルールの代替

設問 4 で「明文化されたものはない」を選択された方への設問。

「リーダーなどの判断に任されている」がトップ。

「その他」が 2 番目で、自由記述では組織ルールではなく顧客や製品ごとという回答が多く見られる。

- その他（自由記述）
  - 顧客や製品ごとに設けられた設計ポリシーまたはルール（3 件）
  - 受託開発となる為、顧客が規定するルールに従う
  - 要求仕様に従う
  - 発注者から「セーフティ」として与えられた要件
  - 顧客要求に基づきルールを規定する
  - 製作所ごとの基準
  - FMEA

2.8.3.4 設問６)セーフティ設計の適用レベルは、製品や開発案件によって変わりますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

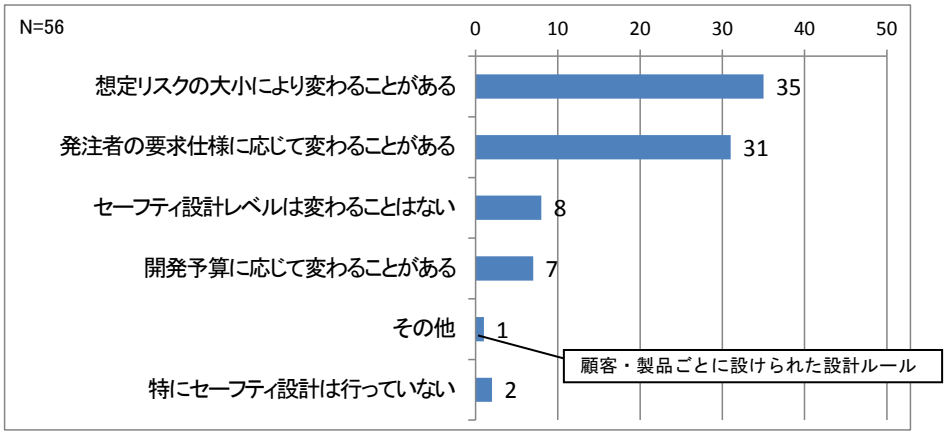


図 2-24 セーフティ設計の適用レベル

「想定リスク・・・」、「開発予算・・・」及び「発注者の要求仕様・・・」はともに多くの回答があると想定していたが、 「開発予算・・・」は大幅に少なかった。

設計に係るコストは開発予算の影響が大きいと想定されるが、セーフティ設計は、予算に関わらず重視されていると想定される。

2.8.3.5 設問２６)御社には、セキュリティ設計の設計ルールがありますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

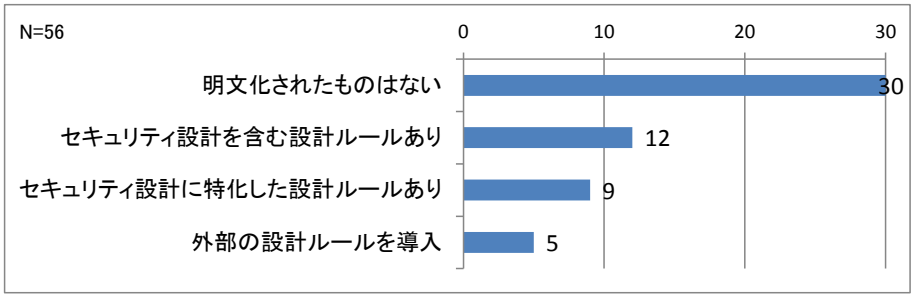


図 2-25 セキュリティ設計ルール

設問 4 のセーフティ設計ルールと比較すると、「明文化されたものはない」が 30 件でほぼ等しい(設問 4 では 28 件)。セキュリティ設計の設計ルールを明文化している組織は半数以下であった。次項で分野別に分析する。

2.8.3.6 設問26)「分野」×「セキュリティ設計ルール」

N は合計回答数。横軸は回答数。

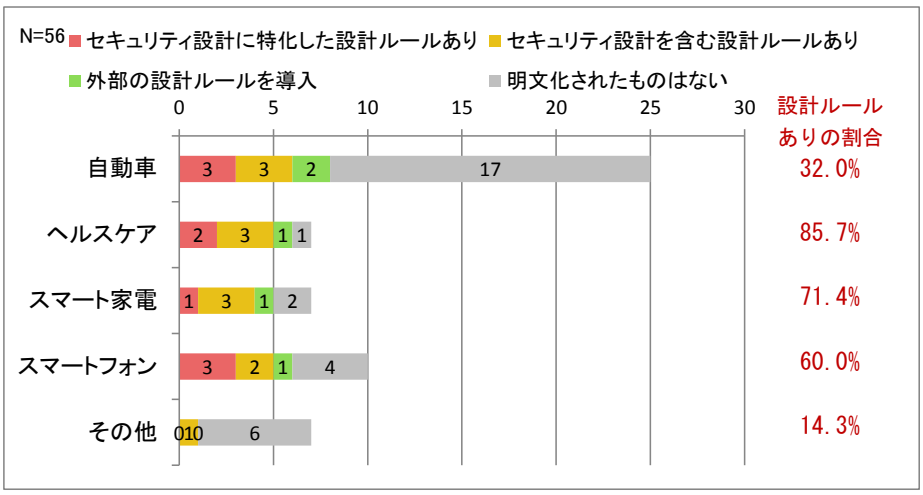


図 2-26 分野別セキュリティ設計ルール

セーフティとは逆に、セキュリティ設計ルールがあるという回答については自動車分野の比率が低い。セーフティ／セキュリティ設計の比重が自動車分野と他の分野で逆であることが分かる。

2.8.3.7 設問27)(設問26で4を選ばれた方へ)セキュリティ設計ルールの代わりになるものはありますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

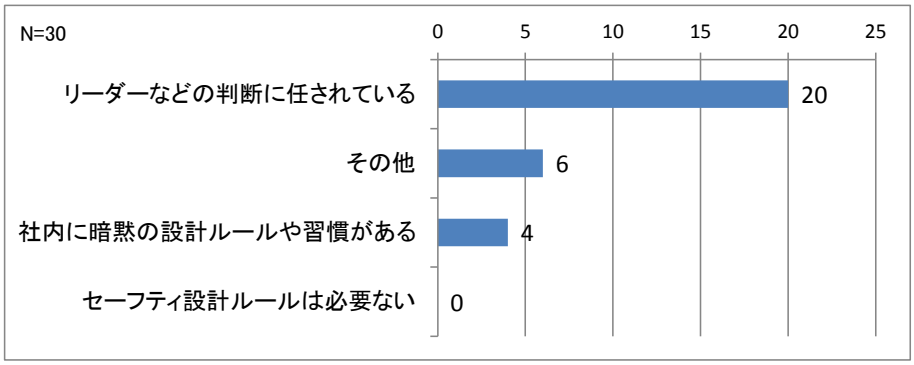


図 2-27 設計ルールの代替

設問 26 で「明文化されたものはない」を選択された方への設問。

セーフティ設計（設問 5）でも同様に「リーダーなどの判断に任されている」が多く、二番目に「その他」が来ており（9 件）、顧客や製品ごとにルールを定めるという自由記述が多かった。これに対してセキュリティ設計の「その他」は 6 件あったが、自由記述の内容には業界の標準や基準に従うという回答があった。

2.8.3.8 設問２８）セキュリティ設計の適用レベルは、製品や開発案件によって変わりますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

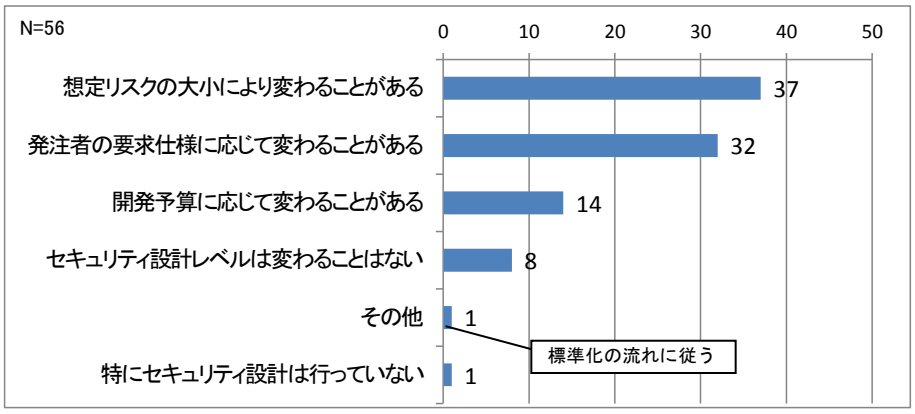


図 2-28 セキュリティ設計の適用レベル

セーフティ設計と似た傾向となっている。ただし、「開発予算に応じて変わることがある」がセーフティの 2 倍の件数となっている点が異なっている。

2.8.4 ハザードと脅威

2.8.4.1 設問７）御社の製品・サービスで想定されるハザードは何でしょうか？（○は各々一つ）

N は各々の項目への合計回答数。横軸は回答数。

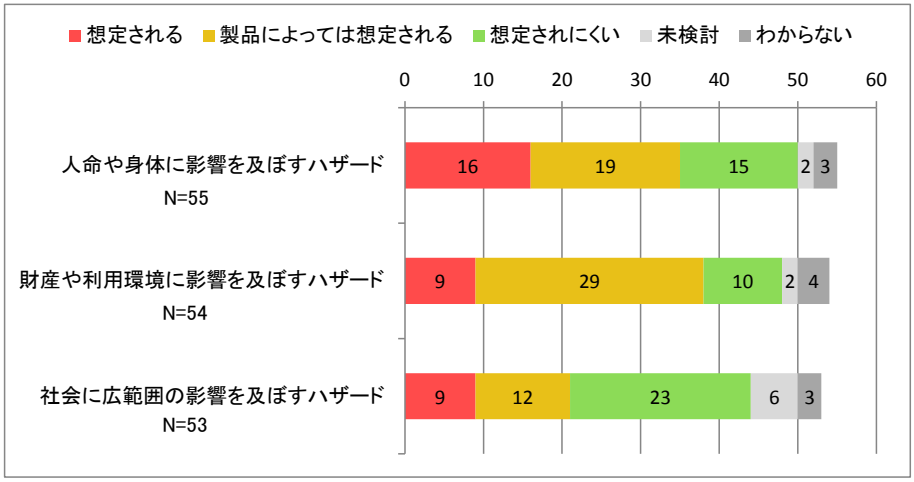


図 2-29 想定されるハザード

「人命や身体・・・」については「想定される」が多いが、「財産や利用環境・・・」については「製品によっては想定される」が大幅に多い。これに関しては、分野による見方の違いが想定される。

2.8.4.2 設問７）「分野」×「人命や身体に影響を及ぼすハザード」

N は合計回答数。横軸は回答数。

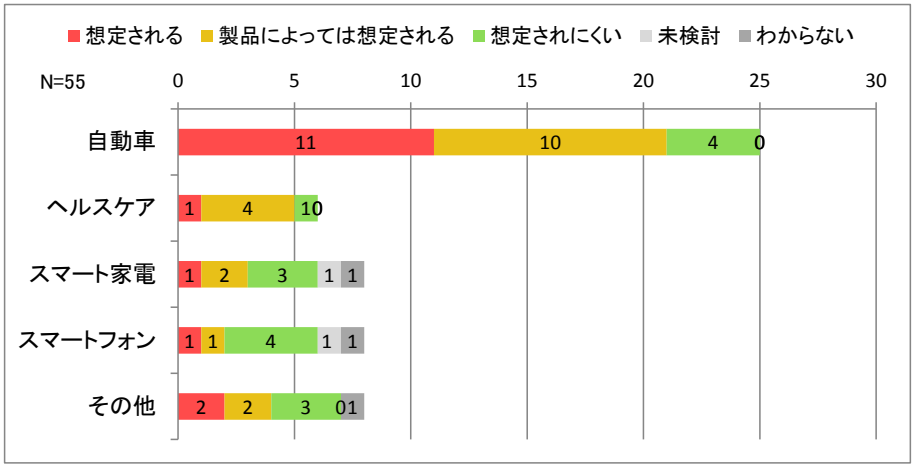


図 2-30 分野別想定されるハザード（人命や身体）

2.8.4.3 設問7)「分野」×「財産や利用環境に影響を及ぼすハザード」

N は合計回答数。横軸は回答数。

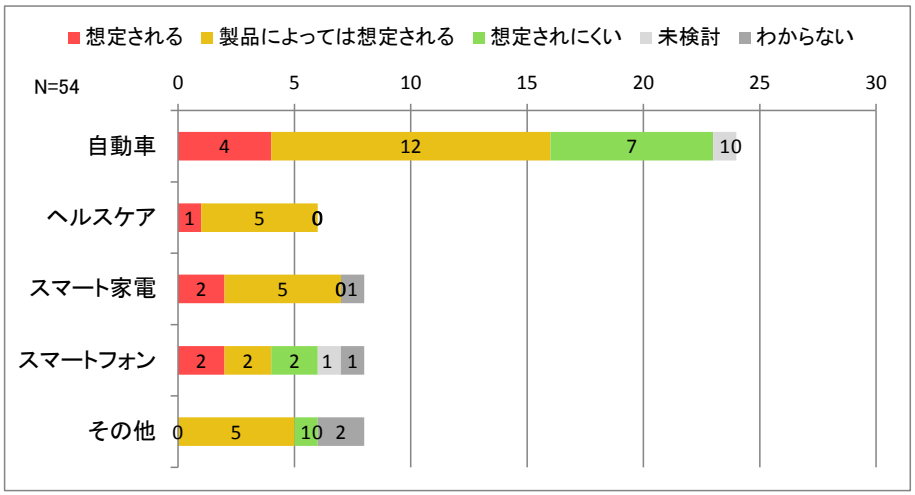


図 2-31 分野別想定されるハザード(財産や利用環境)

「財産や利用環境に影響を及ぼすハザード」について分野別に見ると、自動車において「想定されにくい」の割合が増加、ヘルスケア、スマート家電において「想定される」及び「製品によっては想定される」の比率が増加。

分野によって何をハザードと捉えるかが異なることが分かる。

2.8.4.4 設問7)「分野」×「社会に広範囲の影響を及ぼすハザード」

N は合計回答数。横軸は回答数。

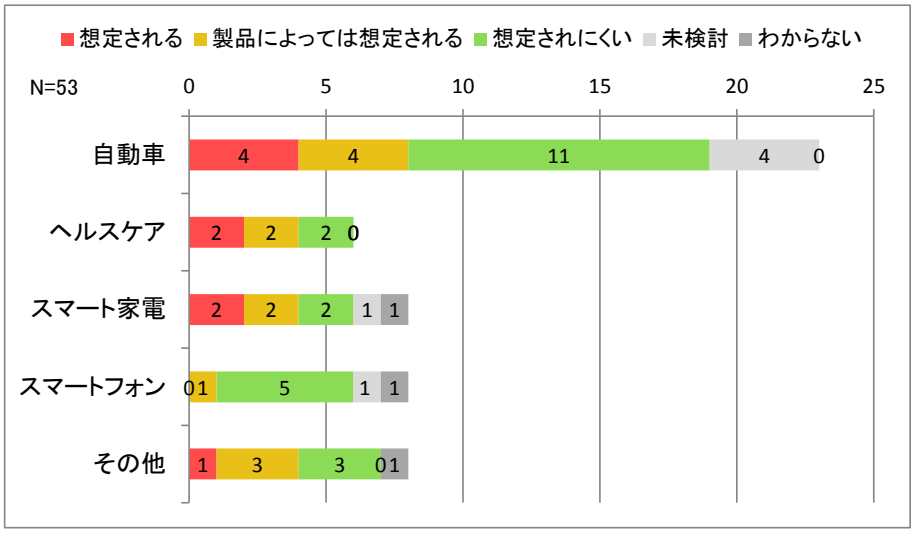


図 2-32 分野別想定されるハザード(社会)

「社会に広範囲の影響を及ぼすハザード」ついて分野別に見ると、全体的に「想定されにくい」が増加している。

セーフティの場合は、機器同士が連携することで波及的に影響が広がるケースが想定しにくいためと思われる。

2.8.4.5 設問８)代表的なハザードの例を記述願います。

「代表的なハザードの例」を分野別に示す。

自動車分野 (13 件)

- 提供したツールの不具合により、お客様の製品が正しい動作をしない可能性はあるが、この防止策についての案内も提供している。
- 自動車のステアリングをアシストする装置の舵が固着する。ステアリング操作が行えず衝突する。
- 適切な取り扱いが行われず、発煙を伴うような故障が発生した場合、火傷等の影響、また接続先である車両への影響。
- パワーウィンドウ挟み込みによる事故。ステアリングロック誤動作による事故。各国電波法違反に伴う事故。
- 製品の不具合により、交通事故を引き起こす。車両の盗難。車両リコール問題。
- 車載用のエンジン制御に関して、急に止まる、暴走するなど。
- ＜車用車速メーターアプリ＞弊社 UI エンジンを利用して、例えば車速メーターを実装した場合を考える。メーターアプリの実装の不具合、あるいは弊社エンジンの不具合により、実際の車速と異なる数値をユーザーに表示してしまった場合、これは人命に影響を及ぼす可能性がある。
- アプリケーションの不具合を起因とする、エンジン・ブレーキ制御などの喪失。
- 車両制御システムの不具合により、乗員及び通行者に危険が及ぶこと。
- リアビューカメラの画像フリーズ（使用者がフリーズに気付かない場合車両後方から接近してくる歩行者等と接触する危険事象を発生させる可能性がある)。
- リモコンエンジンスターターにおける不意なスタート。ドライブレコーダー機能における録画不良。OBD 接続製品における車両への悪影響。
- 電動パーキングブレーキにおいて、意図せずパーキングブレーキが作動し、後続車と衝突し負傷する。
- 人命、身体へのハザード：自動車 ECU の量産ソフト開発など。財産、利用環境のハザード：自販機、ATM のソフト開発など 。

ヘルスケア分野 (6 件)

- 人工心肺の電源系異常の場合、ハード、ソフト、最終的に人力によるバックアップ。
- 製品操作による事故。検体の取り違い。製品障害による利用者の作業遅延。世界標準規格適用不備による違反。
- 投薬量の誤りによる事故。広範囲な通信障害。
- ハードウェアの劣化による誤動作。外部/内部電源が供給されない状態によるシステムダウン。ネットワーク付加増によるデータ転送遅延。
- ソフトウェアの不具合による、自システムの誤動作及びシステムダウン。
- 充電端子、外部接続端子などの接続端子。内蔵電池（リチウムイオン電池)。電波による医用電気機器の作動への影響。

スマート家電分野 (8 件)

- エアコンの on/off 制御のやりすぎによる故障。
- 機械安全の場合：巻き込まれ、挟まれ、切断、押し潰し、感電、火傷。家電の場合：火災、爆発、感電、火傷、巻き込まれ、挟まれ。
- NVM の耐久性。
- 製品の発火・発熱などの物理的ハザード。インフラ機器における大規模通信不可などの障害。
- PL 責任。個人情報の漏えい。
- 人命、身体へのハザード：自動車 ECU の量産ソフト開発など。財産、利用環境のハザード：自販機、ATM のソフト開発など。
- 洗濯機に手を突っ込んでケガをする、電子レンジの電波が漏れ加熱、施錠システムの不具合で開錠となる、など。
- 製品の発火

スマートフォン分野 (3 件)

- スマートフォン等モバイル端末のアプリケーションが暴走等を起こし、バッテリー爆発等による人体への影響が発生する。スマートフォン等モバイル端末の機能が動作しないことにより、生活に影響を与えるなど。
- ヘルスケア機器とクラウドサービスを繋ぐデータ中継の役目として UI を提供。想定されるハザードとしては、機能が正しく動作しないことで、ヘルスケアサービスが正しく受けられずに、健康を害してしまうなどの身体への影響や周辺機器が期待した動作をしないなどが、想定される。
- ネットワーク制御において、通信網が使用できなくなる恐れがあり、課金者にサービス提供ができなくなる。また災害時に、連絡を取る手段がなくなってしまうこともあり得ると想定している。

その他分野 (6 件)

- 対象商品内の個人データ消失、パスワードの漏えいなど。
- 非常停止ボタンがきかない。
- 情報漏えいや、サイバー攻撃による被害を受ける。データの破損や消失による、業務の停止。
- 無人搬送車の暴走→人命に危害。
- 外部機器の制御ミスによる機器の破損。
- 機密データ（クレジットカード番号など）の情報漏洩 →不正利用･国防に関する情報。漏洩 → 脅威 、戦争・原子力などの情報漏洩 → 核の脅威 、テロ。

2.8.4.6 設問９）ハザードを踏まえたセーフティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

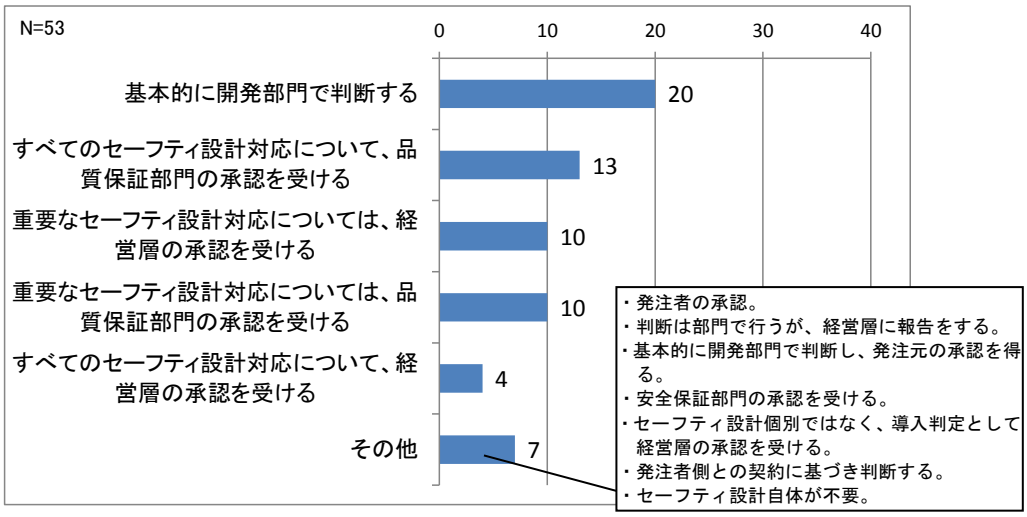


図 2-33 セーフティ設計に対する経営層や品質保証部門の承認

「基本的に開発部門で判断する」がトップ(約 38%)。二番目の「すべてのセーフティ設計対応について、品質保証部門の承認を受ける」については分野別に見てもばらついている状況。その他の半数弱は「発注者」の承認であった。

- その他：発注者の判断や契約が 3 件、別部門や経営者への報告、導入判定などが 3 件となっている。セーフティ設計不要という回答もあった。
  - 発注者の承認。
  - 判断は部門で行うが、経営層に報告をする。
  - 基本的に開発部門で判断し、発注元の承認を得る。
  - 安全保証部門の承認を受ける。
  - セーフティ設計個別ではなく、導入判定として経営層の承認を受ける。
  - 発注者側との契約に基づき判断する。
  - セーフティ設計自体が不要

2.8.4.7 設問９）ハザードを踏まえたセーフティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（単一回答に再集計）

設問９は複数回答の集計のため、経営層の関わりを見るために、複数回答を単一回答に再集計を実施（開発部＋経営層は経営層に分類、開発部＋品質管理は品質管理に分類、開発部＋品質管理＋経営層は経営層と品質管理に分類）。

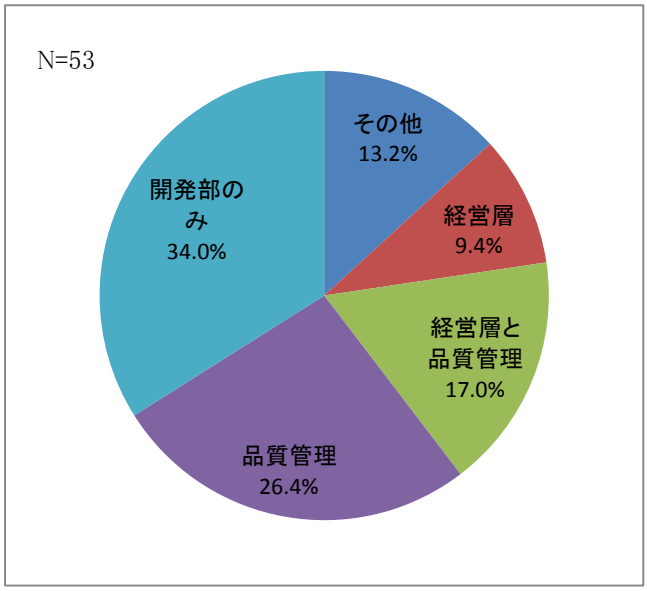


図 2-34 セーフティ設計に対する経営層や品質保証部門の承認（単一回答に再集計）

セーフティ設計の判断への経営層の関与に関しては、経営層が関与していると回答した組織は、26.4%に留まり、開発部門でのみ判断していると言う回答に比べて少ない。

2.8.4.8 設問29）御社の製品・サービスで想定される脅威は何でしょうか？（○は各々一つ）

N は各々の項目の合計回答数。横軸は回答数。

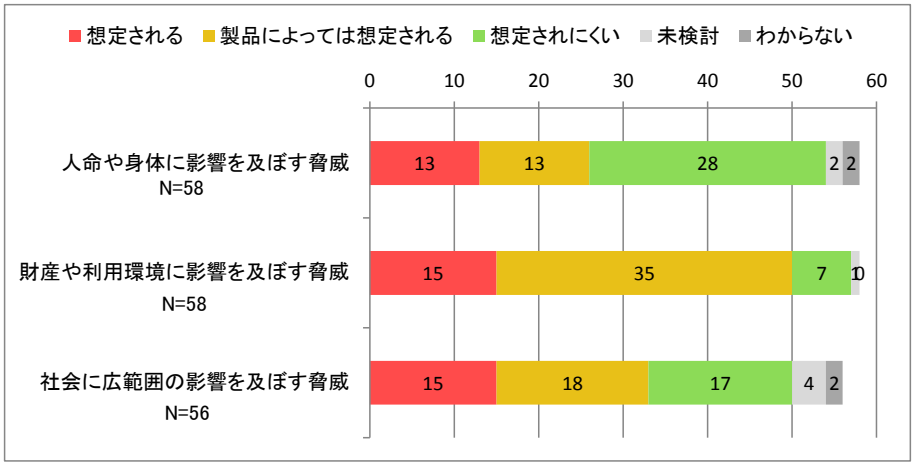


図 2-35 想定される脅威

「想定される」、「製品によっては想定される」の合計をハザードの設問と比較すると、「人命や身体に影響…」については大幅に減少している（ハザードでは 64%、本設問では 45%）。

また、前頁のハザードと比較して「財産や利用環境…」及び「社会に広範囲…」における「想定される」の件数が増加している。これらは、セーフティとセキュリティの性格の違いを示していると想定される。

2.8.4.9 設問29)「分野」×「人命や身体に影響を及ぼす脅威」

N は合計回答数。横軸は回答数。

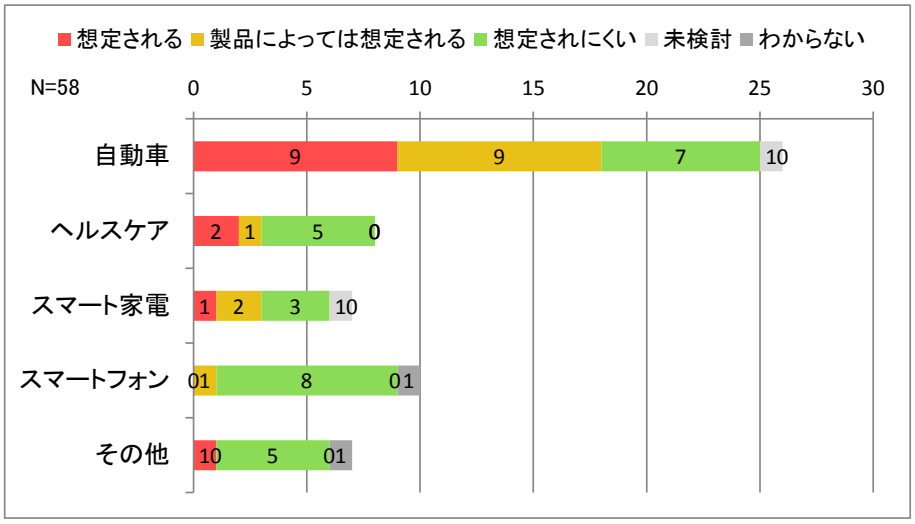


図 2-36 想定される脅威(人命や身体)

「人命や身体に影響を及ぼすハザード」について分野別に見ると、自動車分野において、「想定される」の回答比率が他分野より大幅に多い点はセーフティ（設問 7）と同様である。

2.8.4.10 設問29)「分野」×「財産や利用環境に影響を及ぼす脅威」

N は合計回答数。横軸は回答数。

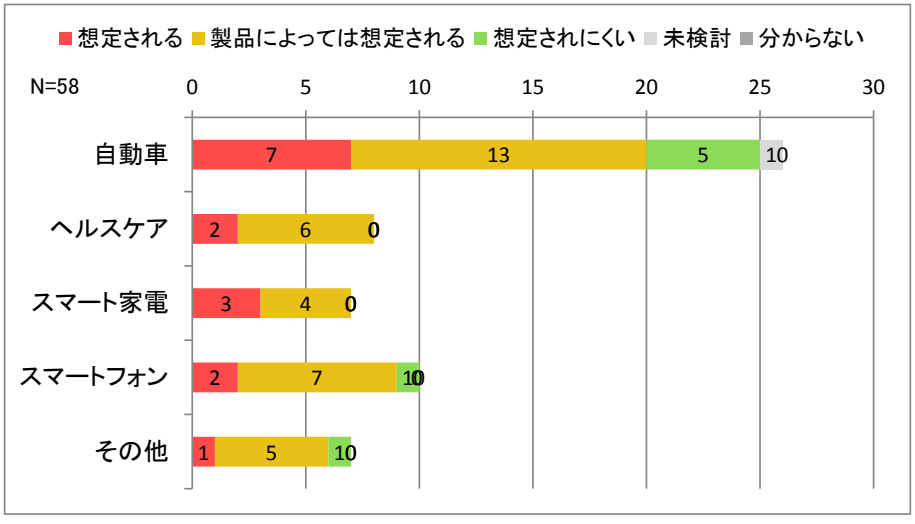


図 2-37 想定される脅威(財産や利用環境)

「財産や利用環境に影響を及ぼすハザード」について分野別に見ると、自動車においては「想定されにくい」が他分野と比較して多いものの、「想定される」、「製品によっては想定される」の件数が多く、セキュリティ意識が高まっていることが見て取れる。

2.8.4.11　　設問29)「分野」×「社会に広範囲の影響を及ぼす脅威」

N は合計回答数。横軸は回答数。

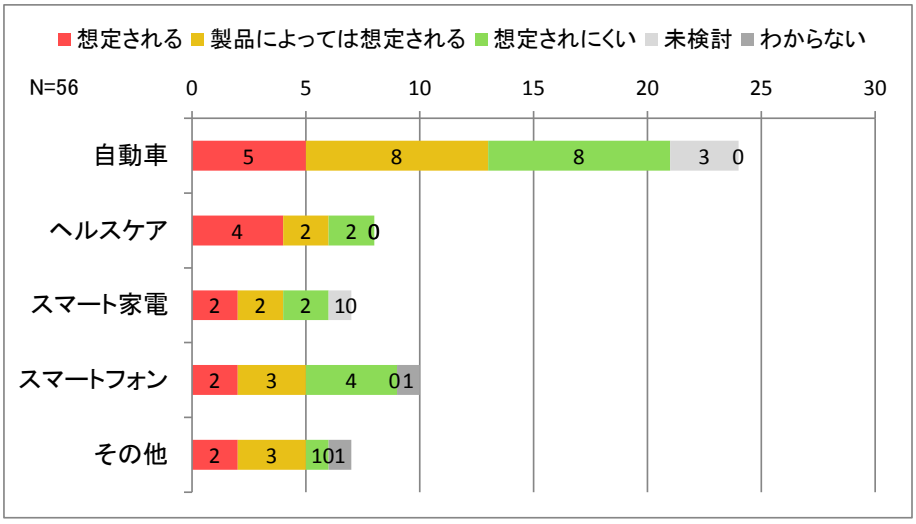


図 2-38 想定される脅威(社会)

「社会に広範囲の影響を及ぼすハザード」ついて分野別に見ると、セーフティと比較して、「想定される」が多くなっている。

機器同士が連携することで波及的に影響が広がるケースは、セキュリティの方が想定しやすいためと思われる。

2.8.4.12　　設問30)代表的な脅威の例を記述願います。

自動車分野 (12 件)

- ツールの不正利用等。
- ステアリングロック不正操作による操作不能等。
- ぜい弱性。
- システムのハッキング。乗っとりにより、交通事故を引き起こす。
- 顧客情報の流出、ホストサーバーのダウン。
- インターネットから車載機器（OBD2）アダプタ、ナビなどへ侵入して正常でない動作をさせる。
- 組込みシステムに対する脅威によって、システムが暴走し、人への危害が与えられる。
- アップデート用ファームウェアの改ざんによる不正動作。
- OBD 接続製品におけるファームウェアの不正改ざん。
- 未知のウイルスによるシステムの改ざん。
- CAN データが改ざんされ、パーキングブレーキが解除され、止めていた車が動き出し、車にひかれ負傷する。
- 全運転支援システムにおける、人物・車輌検知ソフトウェアにて、ソフトウェア改ざんによる誤検知または検知できなかったことによる、交通事故の発生など。

ヘルスケア分野 (5 件)

- サービスの主体となるクラウド側に、改ざんされたデータが送信されてしまう脅威。
- 個人情報の漏えい。
- 個人情報等の漏えい。
- 通信内容の傍受等。
- 著作権保護の解除、個人情報・プライバシー情報の漏えい、等。

スマート家電分野 (5 件)

- 個人情報、パスワードの漏えい等。
- イントラネットへのリモート侵入。エアコン/照明などの不正制御。
- HEMS への攻撃による、家電関連の異常制御（異常発熱等含む)、通信自体の妨害。
- 鍵の漏えい、(金銭管理の）データ改ざん。
- パスワードリスト攻撃で顧客の電話番号、住所が盗まれた、ハッキングでブルーレイの映像をコピーされた、ハッキングでエアコンの誤作動を起こされ熱中症になった、など。

スマートフォン分野 (9 件)

- 個人情報の意図しない漏えい、情報収集に関するユーザーからの批判。
- ウイルス検知、不正侵入検知、不正 URL 検知、不正アプリ検知、DDoS[3]攻撃対策。
- 弊社ツールを利用して、ユーザーが独自に作成したデザインリソースが第三者に盗まれてしまう事があると、これは財産に影響を及ぼすと考えられる。
- 著作権保護の解除、個人情報・プライバシー情報の漏えい、等。
- マルウェアや、ウイルスによる感染。情報漏えい。
- 悪意あるハッカー等により、正規利用者の利益を損なうもの。
- 悪意のあるプログラムが入り込むことによる個人情報の流出や誤課金
- スマートフォンで考えられる脅威。例えば、通信路の盗聴、権限昇格、SW 改造、アルゴリズム漏えい、Personal data 漏えい、コンテンツ保護のバイパス、など。
- サイバー攻撃、標的型攻撃、機密情報の漏えい 。

その他の分野 (3 件)

- （制御装置の）プログラム・パラメーター改ざん、不正なリモート操作、トラフィック増大。
- ネットワーク Down。
- 検査画像から顧客の製品情報などが漏えいする。

[3] DDoS (Distributed Denial of Service attack)は、多数の分散されたコンピューターから同時に同じ対象のサービスを利用することで、その対象サービスを停止させる攻撃手法

2.8.4.13 設問31）脅威を踏まえたセキュリティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

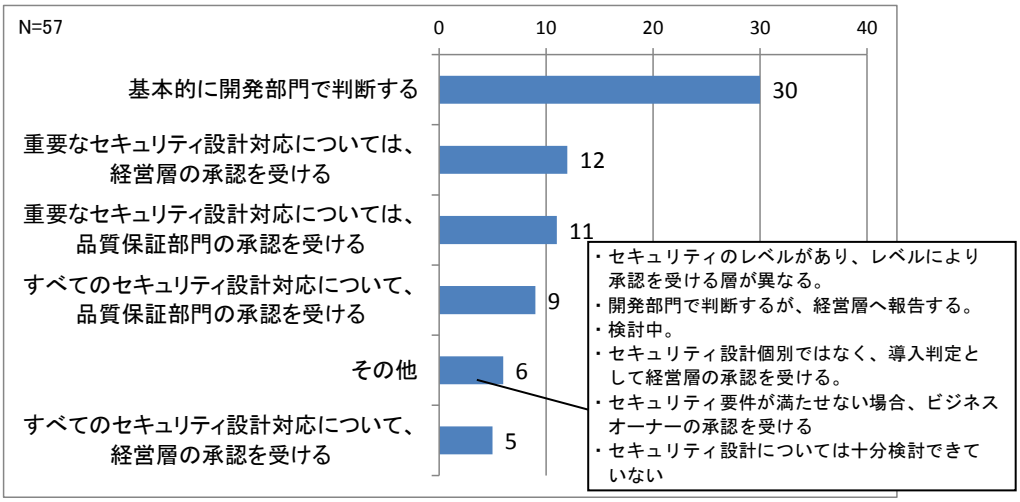


図 2-39 セキュリティ設計に対する経営層や品質保証部門の承認

セーフティ同様、「基本的に開発部門で判断する」がトップであるが、件数はセーフティよりも多く、回答全体の約 50%で、経営層や品質保証部門の承認を得ていないケースが多い。

2.8.4.14 設問31）脅威を踏まえたセーフティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（単一回答に再集計）

設問 31 は複数回答の集計のため、経営層の関わりを見るために、複数回答を単一回答に再集計を実施（開発部＋経営層は経営層に分類、開発部＋品質管理は品質管理に分類、開発部＋品質管理＋経営層は経営層と品質管理に分類）。

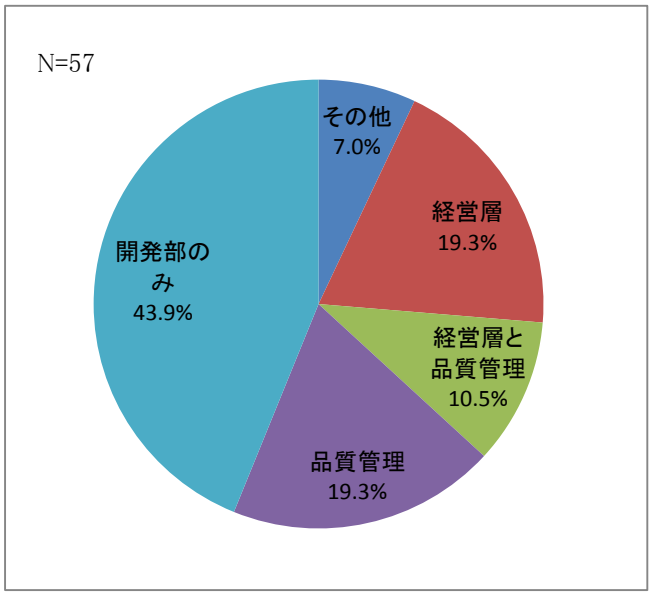


図 2-40 セキュリティ設計に対する経営層や品質保証部門の承認（単一回答に再集計）

セキュリティ設計の判断への経営層の関与に関しては、経営層が関与していると回答した組織は、29.8%に留まり、開発部門でのみ判断していると言う回答に比べて大幅に少ない。

2.8.5 手法とツール

2.8.5.1 設問10)ハザード分析について、手法やツールを利用していますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

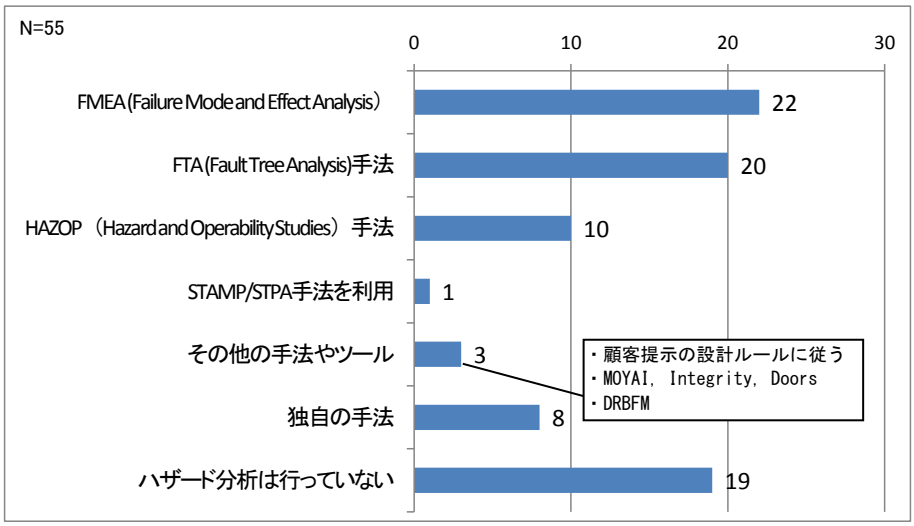


図 2-41 ハザード分析の手法･ツール利用

FMEA、FTA、HAZOP が三大利用ツールである。

「ハザード分析は行っていない」が 19 件あった。

2.8.5.2 設問10)「分野」×「ハザード分析は行っていない」

N は合計回答数。横軸は各分野内での回答割合と回答数。

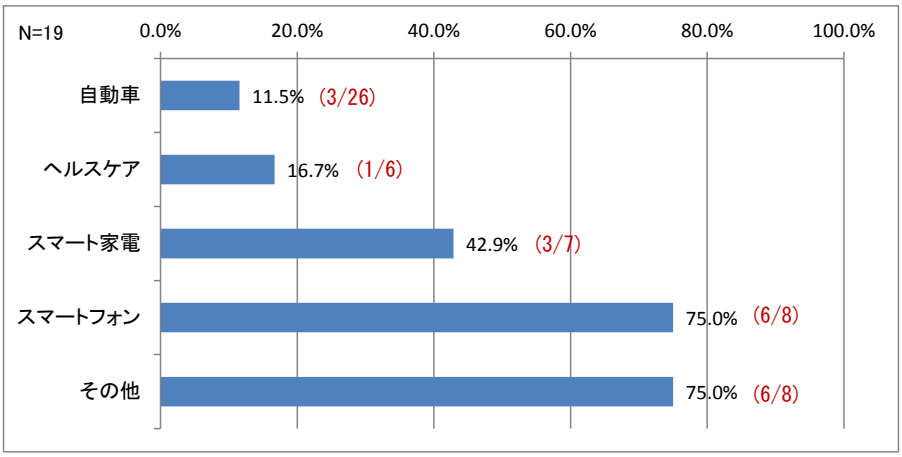


図 2-42 分野別ハザード分析未実施率

「ハザード分析は行っていない」件数を分野別に見ると、スマートフォンはハザード分析を行っていない回答が多く、自動車、ヘルスケア分野は少ない。

2.8.5.3 設問11)ハザードに対するセーフティ設計・評価について、手法やツールを利用していますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

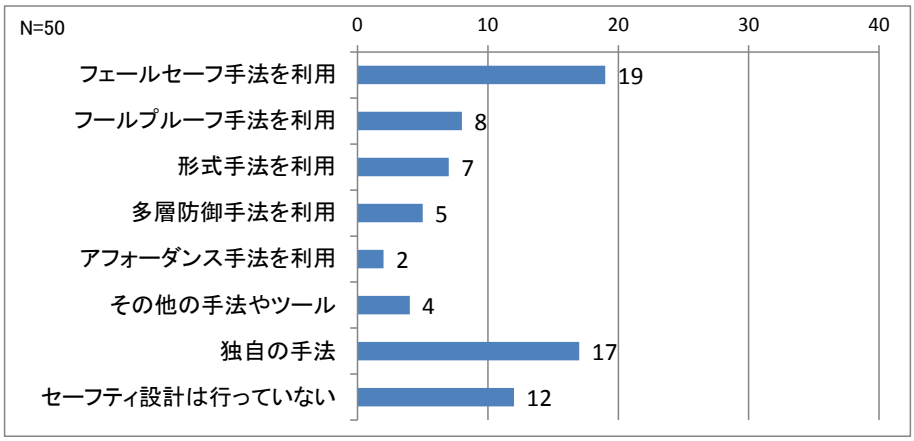


図 2-43 セーフティ設計評価の手法･ツール利用

「フェールセーフ手法」がトップであり、その他の件数は半分以下と差がある。

独自の手法が 17 件と多い。業界や企業独自の手法、経験的な手法が想定されるが、今回のアンケートでは情報が得られなかった。

2.8.5.4 設問11)「分野」×「セーフティ設計は行っていない」

N は合計回答数。横軸は各分野内での回答割合と回答数。

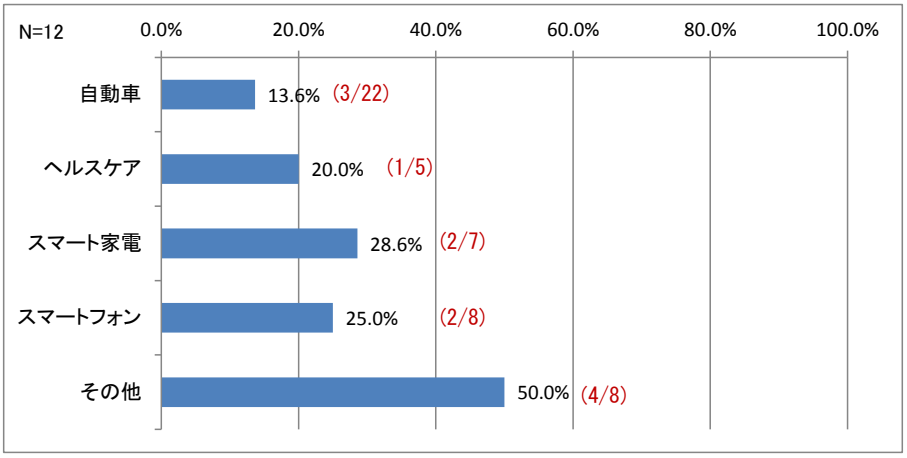


図 2-44 分野別セーフティ設計未実施率

「セーフティ設計は行っていない」件数を分野別に見ると、設問 10 と比較して、スマートフォンの件数が減少している。ハザード分析は行っていないが、セーフティ設計を行っている件数が半数（4 件）を占めており、分析はしなくても設問 11 で回答した手法を利用することが通常の開発の中に組み込まれていることが推測される。

2.8.5.5 設問１２)セーフティ設計品質の見える化について、手法やツールを利用していますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

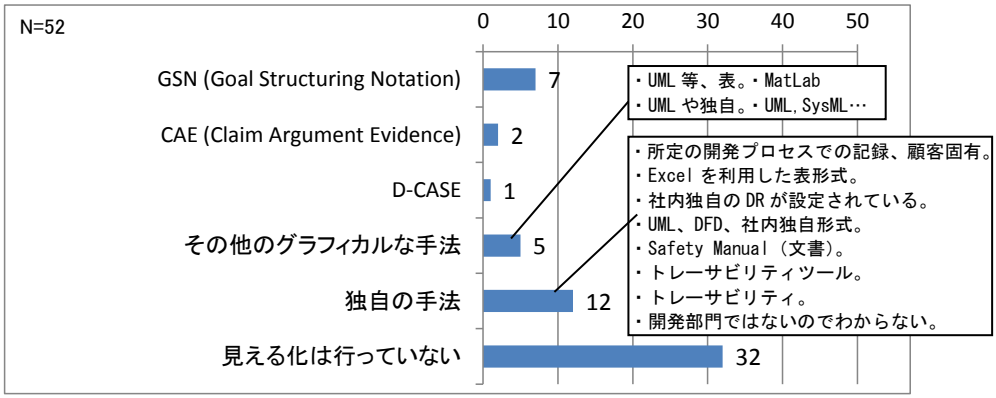


図 2-45 セーフティ設計見える化の手法･ツール利用

今回のアンケート対象は先進的な企業が多いにも関わらず、 「見える化は行っていない」件数が多く、実施例のトップも「独自の手法」である。見える化の手法が一般には普及していないことがうかがえる。 なお、複数回答の重複を除いた、GSN, CAE, D-Case のうちどれかを利用しているという回答数は 8 件だった。

- 設問 12 で、何らかの見える化を行っている回答者
  - 20 件が何らかの見える化を行っている
- 分野別にみると、自動車分野が多い
  - 自動車 13、スマート家電 2、スマートフォン 2、ヘルスケア 1、その他 2 件
- 担当業務別の傾向は見られない
  - 経営 2、事業・製品企画 4、設計・開発 6、研究開発 5、開発マネジメント 2、その他 1 件と多様

2.8.5.6 設問13)(設問12で6を選ばれた方へ)見える化の手法に興味はありますか?(最も近いものを一つ)

N は合計回答数。横軸は回答数。

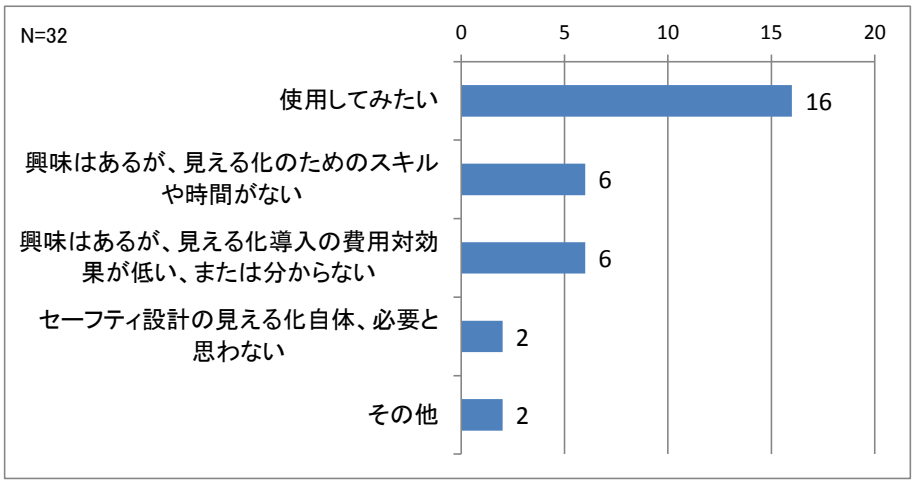


図 2-46 見える化手法への興味

設問 12 で「見える化は行っていない」を選択した方への設問。

「使用してみたい」が多く、「必要と思わない」件数は 2 件と少数。導入するきっかけをうかがっている可能性がある。

2.8.5.7 設問14)セーフティ設計品質をどのように「客観的」に確認していますか?(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

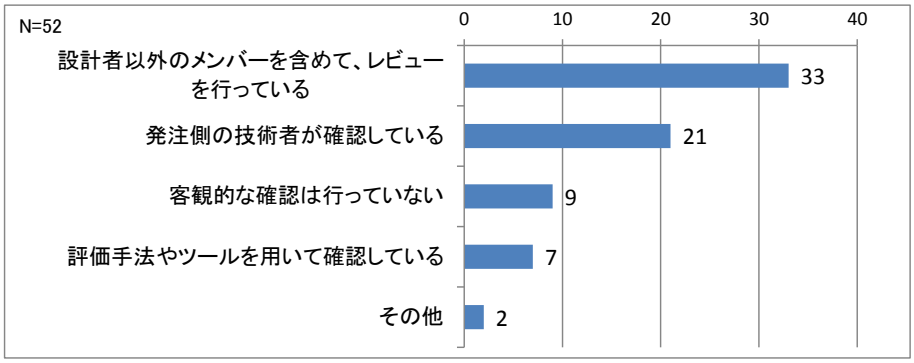


図 2-47 セーフティ設計品質の「客観的」確認

「設計者以外のメンバーを含めて、レビューを行っている」、「発注側の技術者が確認している」が多い。「その他」の回答も、実施に近い内容であり、「客観的な確認を行っていない」は一桁に留まっている。

設問 12 で何らかの見える化を行っている回答者 20 件の回答者の本設問に対する回答では、18 件が「設計者以外のメンバーを含めて、レビューを行っている」、さらにその中の 10 件は「発注側の技術者が確認している」と回答。それに対し、見える化を行っていない回答者 32 件は「設計者以外のメンバーを含めて、レビューを行っている」「発注側の技術者が確認している」を合わせても 22 件で、第三者が参加するレビューのために見える化している可能性がある。

2.8.5.8 設問１５）（設問１４で5を選ばれた方へ）客観的な確認を行っていない理由は何でしょうか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

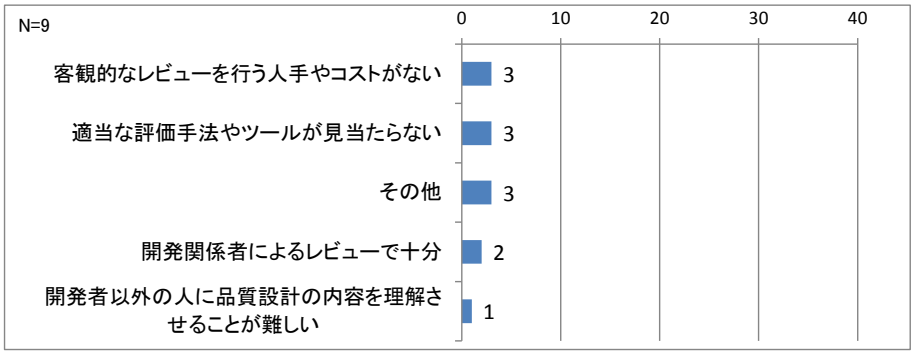


図 2-48「客観的」な確認を行っていない理由

設問 14 で「客観的な確認は行っていない」を選択された方への設問。

本設問については、アンケート設計時に想定した選択肢が数件ずつ選択されており、特に共通的な理由があるわけではなく、各社の事情によるものと想定される。

2.8.5.9 設問３２）セキュリティ上のリスク分析について、手法やツールを利用していますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

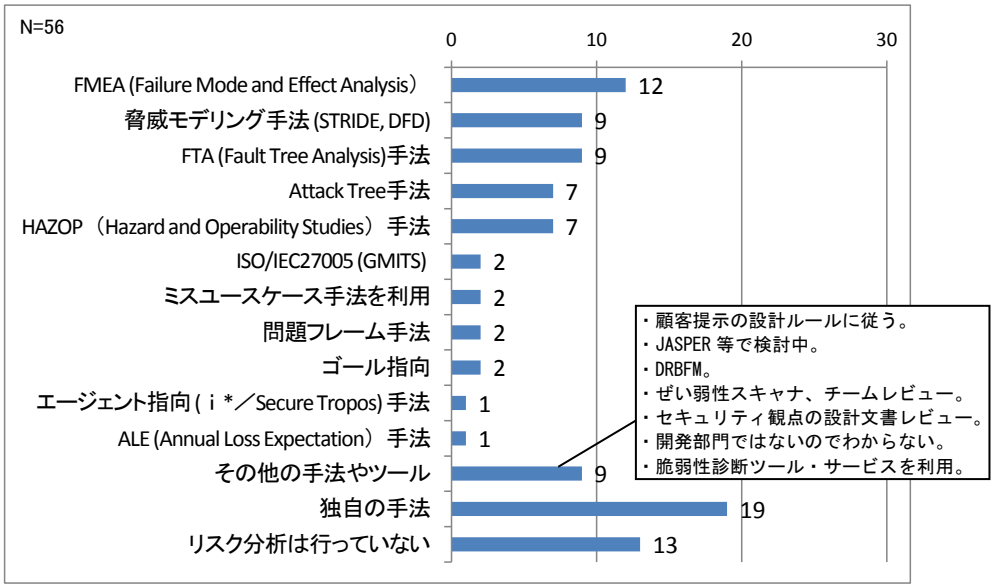


図 2-49 リスク分析の手法･ツール利用

ハザード分析（設問 10）では、回答が 20 件を越える手法が二つあったが、セキュリティでは 10 件を越える手法が一つあるのみで、ばらつきが見られる。

「独自の手法」は 19 件（ハザード分析では 8 件）、「リスク分析を行っていない」は 13 件（ハザード分析では 19 件）。

2.8.5.10 設問32)「分野」×「リスク分析は行っていない」

N は合計回答数。横軸は各分野内での回答割合と回答数。

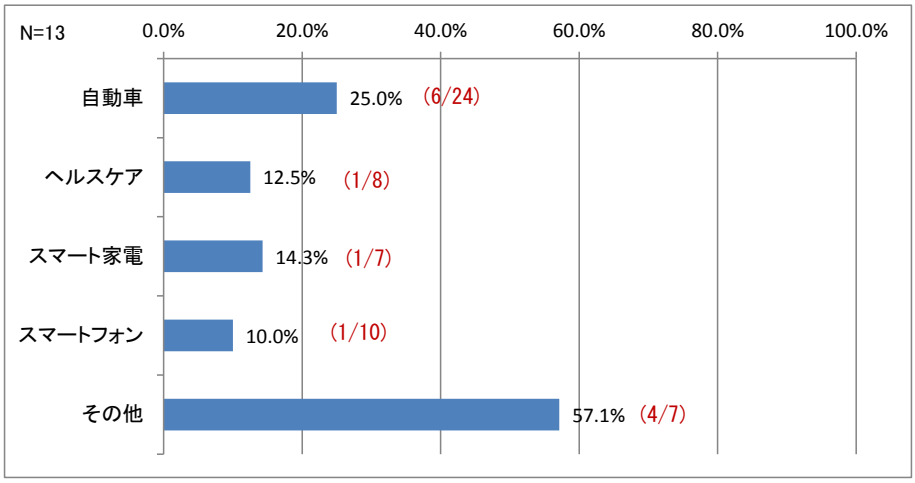


図 2-50 分野別リスク分析未実施率

「リスク分析は行っていない」件数を分野別に見ると、ヘルスケア、スマート家電、スマートフォンは各 1 件で、多くの場合、セキュリティのリスク分析を行っている。

2.8.5.11 設問33)リスクに対するセキュリティ設計・評価について、手法やツールを利用していますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

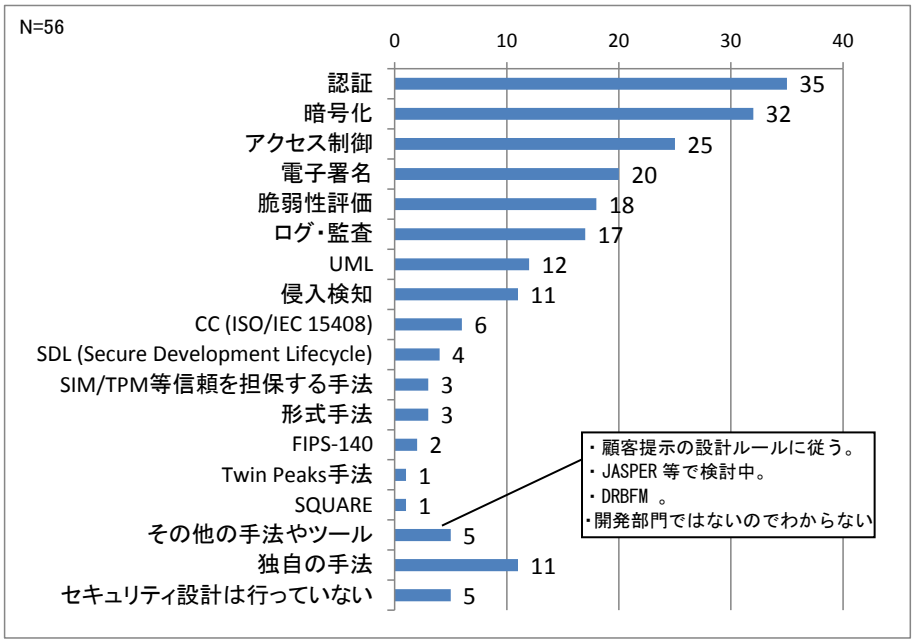


図 2-51 セキュリティ設計評価の手法・ツール利用

「認証」、「暗号化」など 8 項目以上が 10 件以上利用されている。セーフティとの比較は難しいが、セキュリティ技術の普及状況を確認する上では有効と思われる。

2.8.5.12 設問33)「分野」×「セキュリティ設計は行っていない」

N は合計回答数。横軸は各分野内での回答割合と回答数。

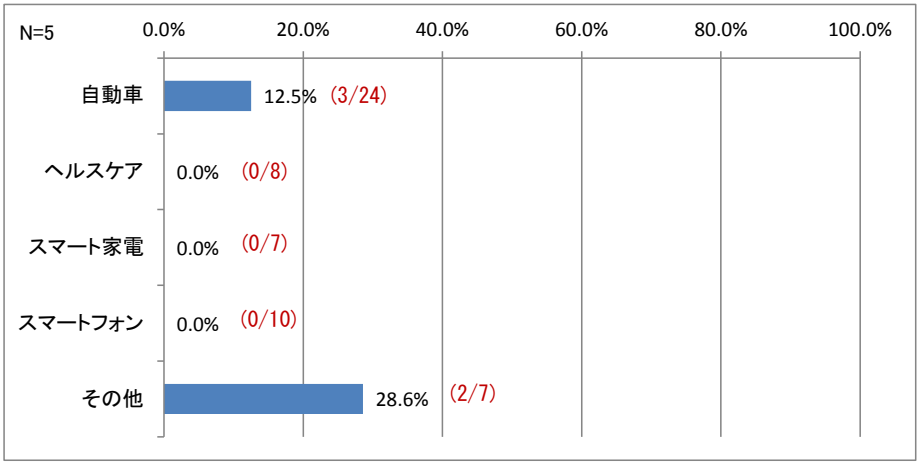


図 2-52 分野別セキュリティ設計未実施率

「セキュリティ設計は行っていない」件数は 5 件であり、「自動車」と「その他」のみであり、ほとんどの回答者が、なんらかのセキュリティ設計に取り組んでいる。設問 32 と比較して各分野とも件数が減少しており、分析はしなくても設問 33 で回答した手法を利用することが通常の開発の中に組み込まれていることが推測される。

2.8.5.13 設問34)セキュリティ設計の見える化について、手法やツールを利用していますか?(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

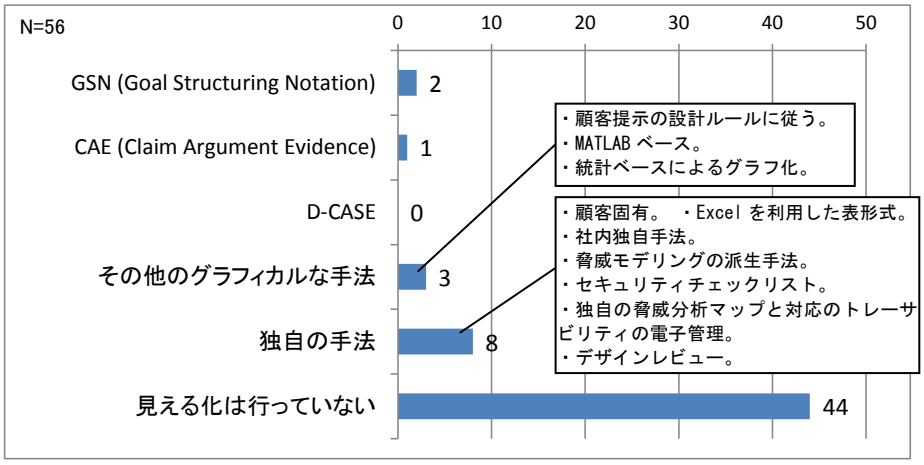


図 2-53 セキュリティ設計見える化の手法･ツール利用

セキュリティ設計に関しては、ほとんど見える化は行われていない状況である。セーフティ、セキュリティとも、見える化を行っている回答者のほとんどは、社内または発注者による客観的なレビューを実施している。 なお、複数回答の重複を除いた、GSN, CAE, D-Case のどれかを利用しているという回答は 2 件だった。

- その他のグラフィカルな手法

- MatLab[4] ベース。
- 統計ベースによるグラフ化 。

- 独自の手法
  - 顧客固有。
  - Excel を利用した表形式。
  - 社内独自手法。
  - 脅威モデリングの派生手法。
  - セキュリティチェックリスト。
  - デザインレビュー。
  - 独自の脅威分析マップと対応のトレーサビリティの電子管理
- 設問 34 で、セキュリティについて何らかの見える化を行っている回答 12 件の内訳
  - 分野
    - セーフティと比較して、各分野から回答がある。
    - 自動車 3 件、ヘルスケア 3 件、スマート家電 3 件、スマートフォン 2 件、その他 1 件
  - 担当業務
    - 経営 1 件、事業・製品企画 3 件、設計・開発 5 件、研究開発 1 件、開発マネジメント 1 件、その他 1 件と多様。

[4] MathWorks, “MATLAB/Simulink,” http://jp.mathworks.com/products/simulink/

2.8.5.14 設問35)(設問34で6を選ばれた方へ)見える化の手法に興味はありますか?(最も近いものを一つ)

N は合計回答数。横軸は回答数。

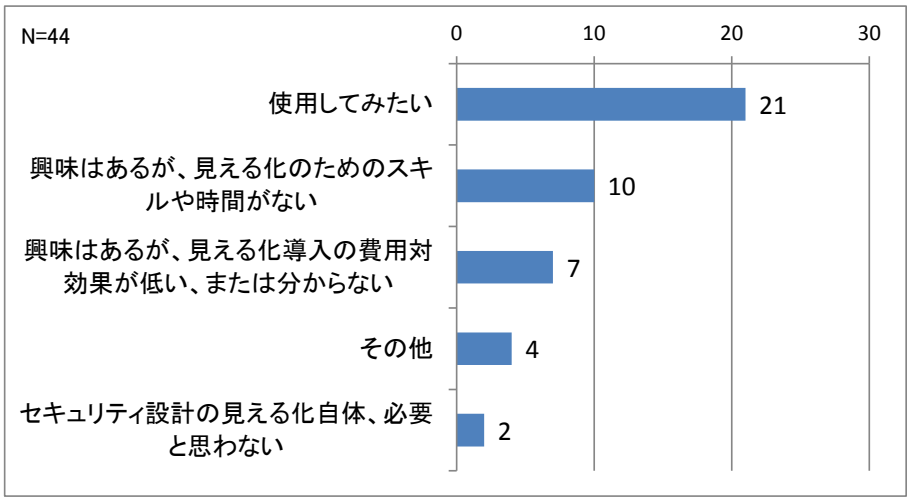


図 2-54 見える化手法への興味

設問 34 で「見える化は行っていない」を選択された方への設問。「使用してみたい」が多く、「必要と思わない」件数は 2 件と少数である。

セーフティ（設問 13）でも記述したとおり、導入するきっかけをうかがっている可能性がある。

2.8.5.15 設問36）セキュリティ設計の品質をどのように「客観的」に確認していますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

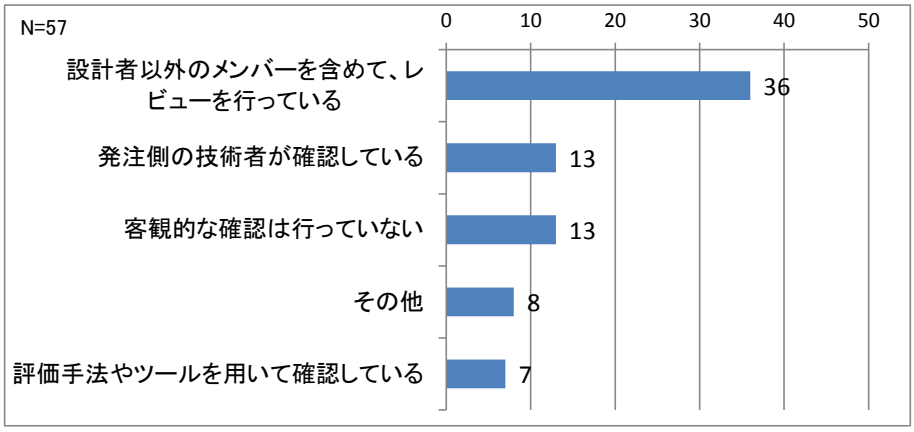


図 2-55 セキュリティ品質の「客観的」確認

「設計者以外のメンバーを含めて、レビューを行っている」が多い。その他の回答も、実施に近い内容（次項参照）。ただし、「客観的な確認を行っていない」も 13 件となっている。

- 評価手法やツールを用いて確認している
  - 脆弱性評価ツール。
  - 独自。
- その他
  - JASPER [1]等で検討中。
  - 脆弱性情報サイトを定期的に閲覧し、対象製品への影響度を調査している。
  - IEC62443。
  - 第三者レビューと評価ツールを検討中。
  - 情報漏れを防ぐ為、特定のメンバーでレビューを行っている。

設問34で何らかの見える化を行っている回答者12件の回答者の本設問に対する回答では、「設計者以外のメンバーを含めて、レビューを行っている」「発注側の技術者が確認している」に合わせて 11 件が回答。残りの 1 件も自由記述で「第三者レビューと評価ツールを検討中」と回答。それに対し、見える化を行っていない回答者 44 件は「設計者以外のメンバーを含めて、レビューを行っている」「発注側の技術者が確認している」を合わせても 29 件で、第三者が参加するレビューのために見える化している可能性がある。

2.8.5.16 設問37)(問36で5を選ばれた方へ)客観的な確認を行っていない理由は何でしょうか?(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

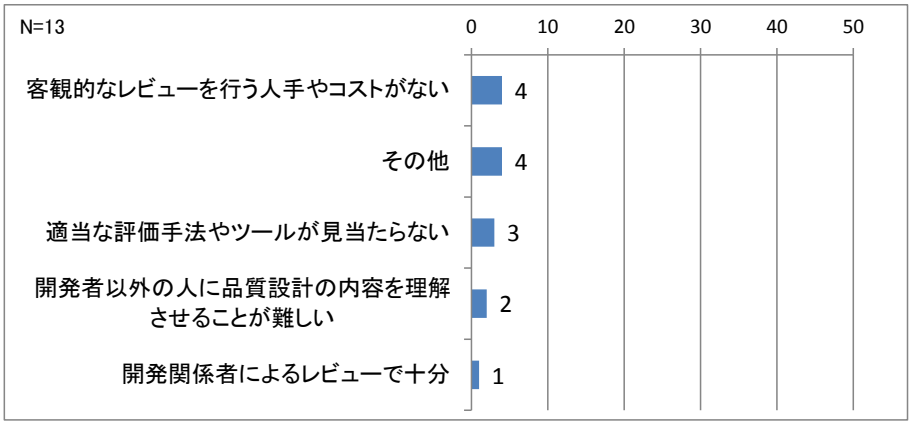


図 2-56「客観的」な確認を行っていない理由

設問 36 で「客観的な確認は行っていない」を選択された方への設問。

本設問については、アンケート設計時に想定した選択肢が数件ずつ選択されており、特に共通的な理由があるわけではなく、各社の事情によるものと想定される。

2.8.6 要件の提示

2.8.6.1 設問16）他社への発注時に、発注先にセーフティ要件を提示していますか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

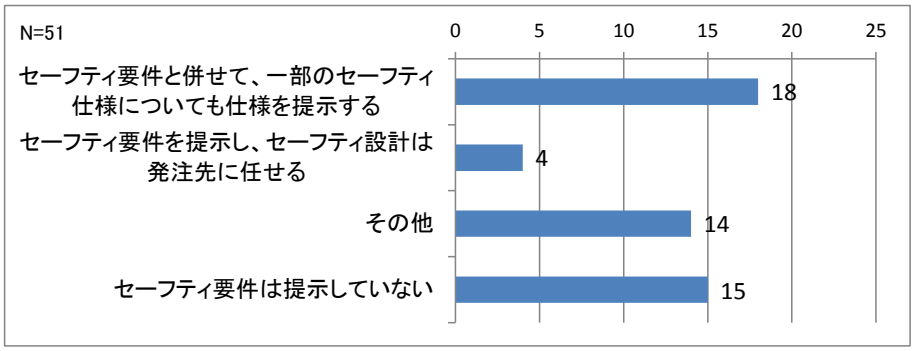


図 2-57 発注先へのセーフティ要件の提示

何らかの形でセーフティ要件を提示している回答が計 22 件、提示していないという回答が 15 件となっている。

「その他」の中に「発注はしない」との回答が多い。 今回は製造業を対象としていたため、外部との受発注を行わない企業は少ないと判断していたが、今後の調査では考慮が必要である。

- その他：「発注していない」の回答以外を下記に記載。
  - 開発プロセス、ドキュメント、レビュー、記録の義務化。
  - 要件の中にセーフティ項目が含まれた形で提示。明示的にセーフティ要件とはなっていない。
  - 関連法令や基準の安全に関わる事項。
  - 案件による。
  - セーフティ要件を含む内容は発注していない。

2.8.6.2 設問17)他社からの受注時に、発注者からセーフティ要件が提示されていますか？(最も近いものを一つ)

N は合計回答数。横軸は回答数。

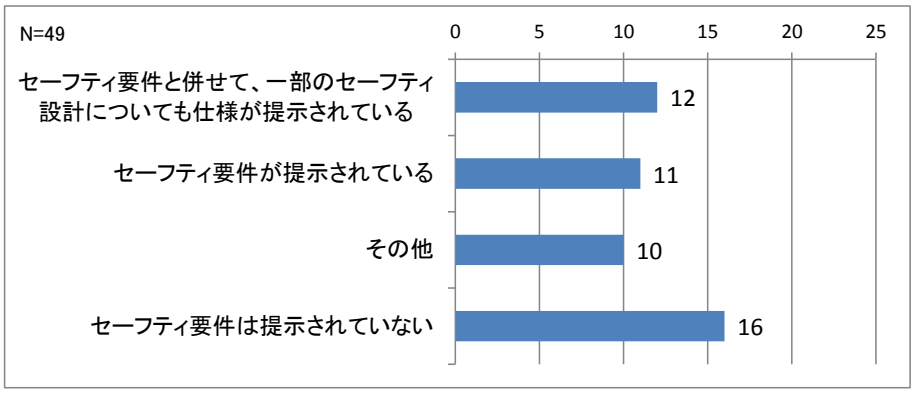


図 2-58 発注者からのセーフティ要件の提示

何らかの形でセーフティ要件を提示されている回答が計 23 件、提示されていないという回答が 16 件となっている。

16 件中 11 件は、設問 16 でセーフティ要件を提示していない回答者である。提示されていない理由として、発注元がセーフティ設計は必要ないと判断している場合もあると想定されるが、その判断の妥当性を検証できないため、本アンケートではこれ以上、深掘りはしていない。

- その他：「受注はない」の回答が多く見られる。それ以外を以下に記載。
  - 要件の中にセーフティ項目が含まれた形で提示。明示的にセーフティ要件とはなっていない。
  - 案件による
  - 開発内容により ISO26262 に準拠の指定がある。

2.8.6.3 設問１８）（設問１７で３を選ばれた方へ）セーフティ要件が提示されない場合、どのように対応しますか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

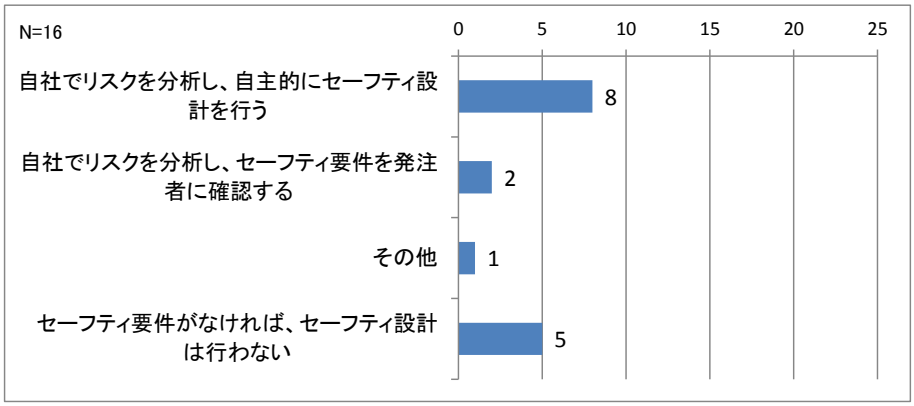


図 2-59 発注者からのセーフティ要件が提示されない場合

設問 17 で「セーフティ要件は提示されていない」を選択された方への設問である。自社でリスク分析を行うという回答が計 10 件あり、「セーフティ要件がなければ、セーフティ設計は行わない」という回答を大幅に上回っている。

2.8.6.4 設問38）他社への発注時に、発注先にセキュリティ要件を提示していますか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

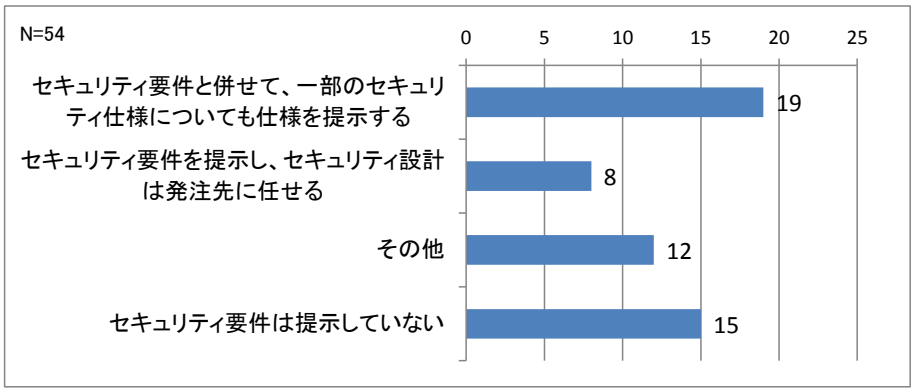


図 2-60 発注先へのセキュリティ要件の提示

何らかの形でセキュリティ要件を提示している回答が計 27 件、提示していないという回答が 15 件となっている。

なお、セーフティ要件、セキュリティ要件とも提示していない回答者は、10 件であった。

「その他」の中には、セーフティ同様、「発注はしない」との回答が多い。

- その他 ：「発注しない」の回答以外を下記に記載。
  - 要件の中にセキュリティ事項が含まれている形で提示。明示的にセキュリティ要件とはなっていない。
  - 案件による
  - Software Development Security Assurance 対応できている S/W 外注がいないので、当方の仕様と開発手順に従ってもらっています。
  - セキュリティ要件は提示していないが、検討中。
  - セキュリティに関係する部分はブラックボックスで提供する。

2.8.6.5 設問３９）他社からの受注時に、発注者からセキュリティ要件が提示されていますか？（最も近いものを一つ）

N は合計回答数。横軸は回答数。

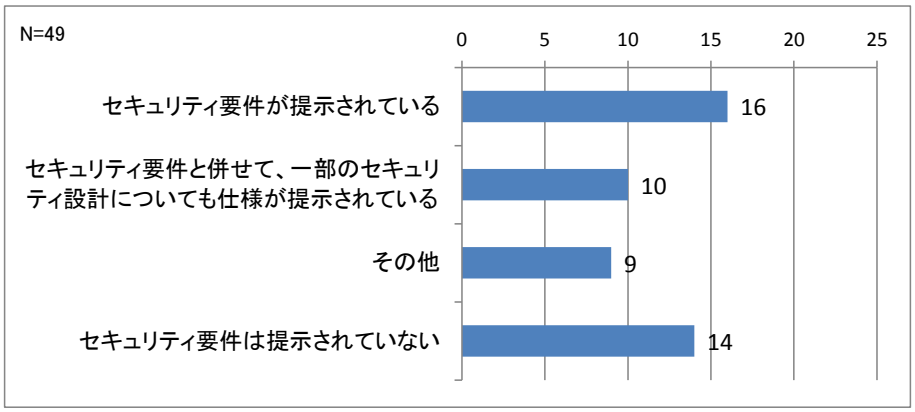


図 2-61 発注者からのセキュリティ要件の提示

何らかの形でセキュリティ要件を提示されている回答が計 26 件、提示されていないという回答が 14 件となっている。ただし、「その他」にも一部提示していると見られる回答がある。

「その他」の中に「受注はない」との回答が見られる。今回は製造業を対象としていたため、外部との受発注を行わない企業は少ないと判断していた。今後の調査では考慮が必要である。

- 「受注はない」との回答が見られる。また「必ずしも提示されない」及び「案件による」は、提示することもあると解釈される。 「受注はない」の回答以外を下記に記載。
  - 要件の中にセキュリティ事項が含まれている形で提示。明示的にセキュリティ要件とはなっていない。
  - 必ずしも提示されない。
  - 案件による。
  - 当社がセキュリティの基準を決めているので、外部からの指示は受けない。

2.8.6.6 設問40)(設問39で3を選ばれた方へ)セキュリティ要件が提示されない場合、どのように対応しますか?(最も近いものを一つ)

N は合計回答数。横軸は回答数。

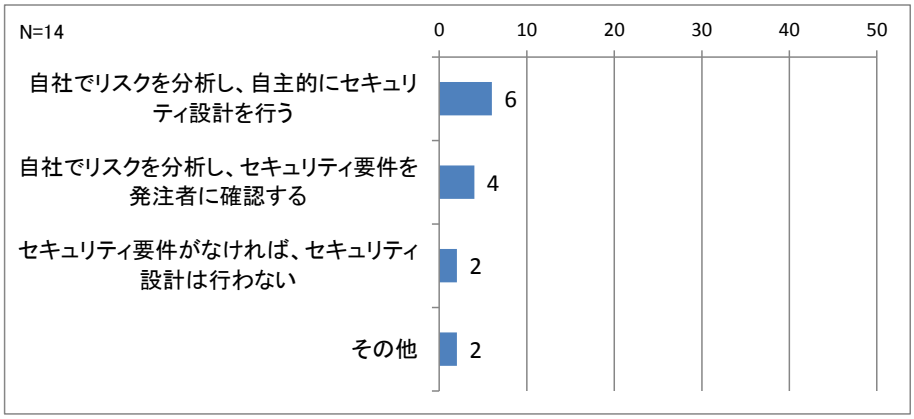


図 2-62 発注者からのセキュリティ要件が提示されない場合

設問 39 で「セキュリティ要件は提示されていない」を選択された方への設問である。自社でリスク分析を行うという回答が計 10 件あり、「セキュリティ設計は行わない」という回答を大幅に上回っている。

2.8.7 他社製品・ソフトウェアの設計品質

2.8.7.1 設問19）他社の製品・ソフトウェアと組合せて開発を行う場合、他社製品・ソフトウェアのセーフティ設計品質の確認はどのように行いますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

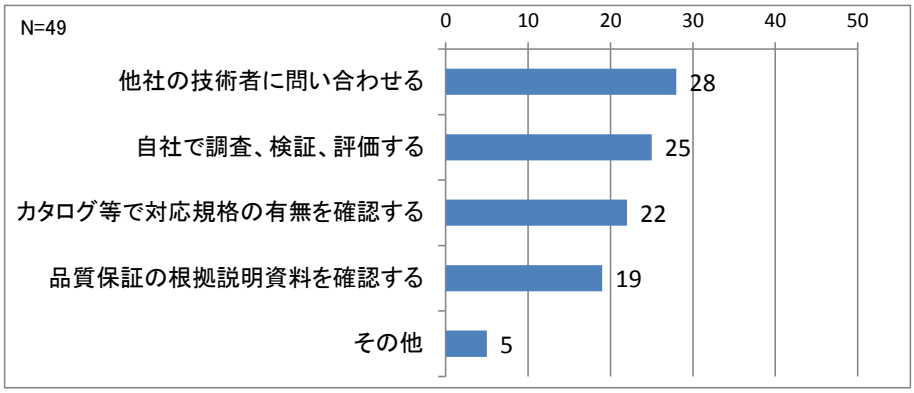


図 2-63 他社製品･ソフトウェアのセーフティ設計品質の確認

アンケート設計時に想定した選択肢に対して、回答者の 4 割から 5 割程度の選択があった。その他は 5 件であり、想定した 4 つの選択肢でセーフティ設計品質確認の手段を網羅していると想定される。

2.8.7.2 設問20）他社製品・ソフトウェアの設計品質の確認のために、何があるとよいと思われますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

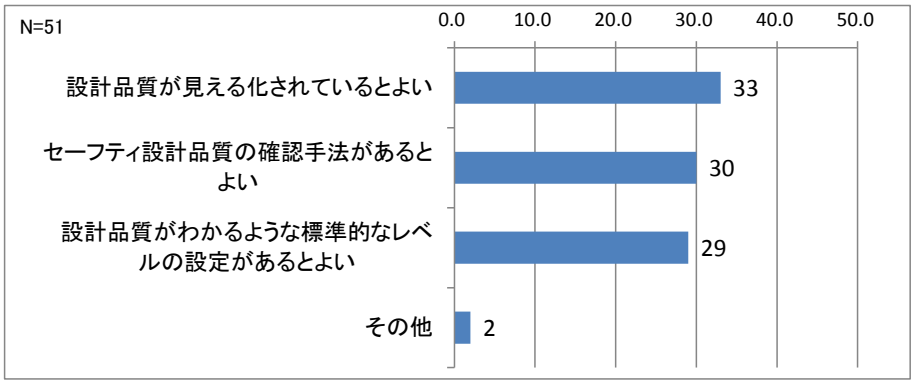


図 2-64 他社製品･ソフトウェアのセーフティ設計品質の確認のためにあるとよいもの

アンケート設計時に想定した選択肢に対して、30 件前後（6 割前後）の選択があった。その他は 2 件であり、選択肢の設定は妥当であったと評価されるが、件数の差が小さいため、ガイドブック反映や今後の施策に対する優先度を付けにくい点が課題。

2.8.7.3 設問21）利用者が自社製品と他社製品を接続させる際に、接続先の製品・ソフトウェアのセーフティ設計品質やレベルを確認して、接続の制御などに利用する仕組みはありますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

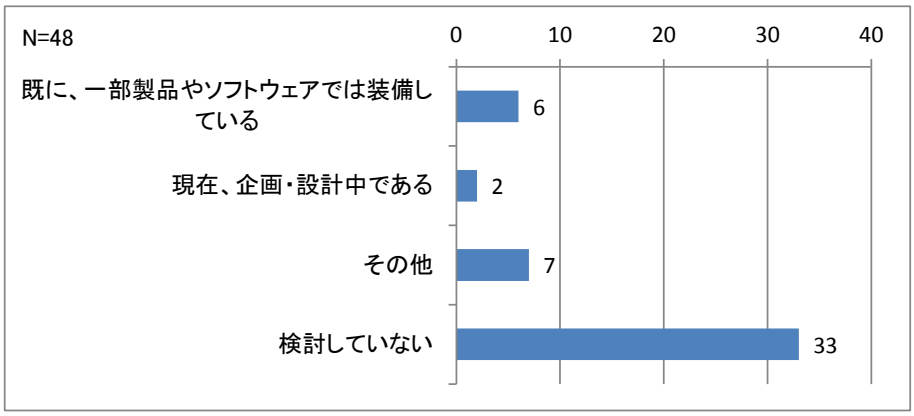


図 2-65 他社製品・ソフトウェアのセーフティ設計品質やレベルを確認する仕組み

「既に、一部製品やソフトウェアでは装備している」が 6 件、「現在、企画・設計中である」が 2 件と、少ないながら該当する回答者がある。内容については、設問 22 参照。

- セーフティに関しては自動車分野が進んでいる
  - 「既に・・・」: 自動車 4 件、ヘルスケア、スマート家電各 1 件
  - 「現在・・・」: 自動車 1 件、スマート家電 1 件
- 担当業務：
  - 「既に・・・」は、研究開発 2 件、設計・開発 2 件、開発マネジメント 2 件
  - 「現在・・・」は、研究開発 1 件、開発マネジメント 1 件
- その他の特徴
  - 全員、何らかのハザード分析手法及びセキュリティ設計手法を利用している。ただし、選択した手法の数はばらけている。

2.8.7.4 設問22）（設問21で1または2を選ばれた方へ）上記の機能はどのような内容でしょうか？（自由記述）

設問 21 で「既に、一部製品やソフトウェアでは装備している」または「現在、企画・設計中である 」を選択された方への設問。

具体的な内容を確認すると、ハードウェア／ソフトウェアによる自動化されたシステムはなく、人による手続き（プロセス）であることが分かる。

- 内容：
  - コンポーネント認定のプロセス。
  - 安全マニュアル等を元に、接続の可否を検証する仕組みがあります。
  - ISO26262 のコンポーネント認定や、外部方策の取扱い方法に準拠する。
  - 予め他社製品の想定リスク分析を行い、そのリスクの再現実験を実施、対策がされているかを確認した上で、組合せて利用する。

2.8.7.5 設問41)他社の製品・ソフトウェアと組合せて開発を行う場合、相手のセキュリティ設計品質の確認はどのように行いますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

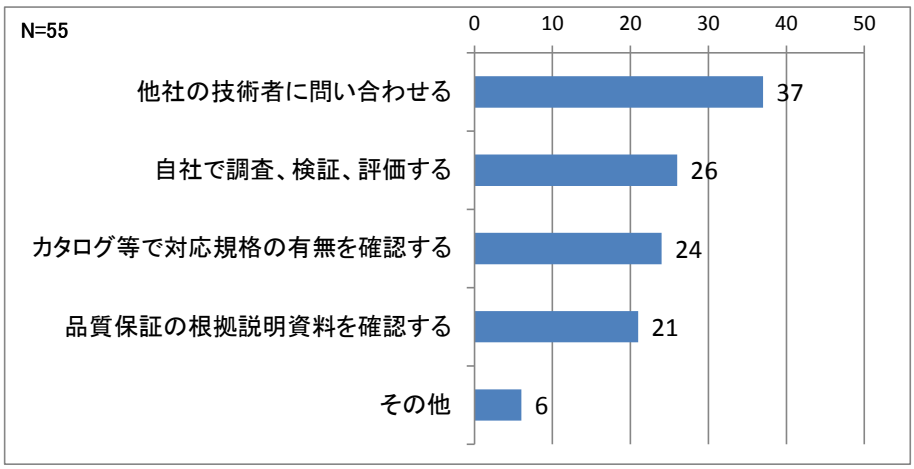


図 2-66 他社製品･ソフトウェアのセキュリティ設計品質の確認

アンケート設計時に想定した選択肢に対して、回答者の 4 割から 6 割程度の選択があった。その他は 6 件であり、想定した 4 つの選択肢でセーフティ設計品質確認の手段を網羅していると想定される。

2.8.7.6 設問42)他社製品・ソフトウェアの設計品質の確認のために、何があるとよいと思われますか？(複数回答)

N は複数回答の合計回答数。横軸は複数回答の回答数。

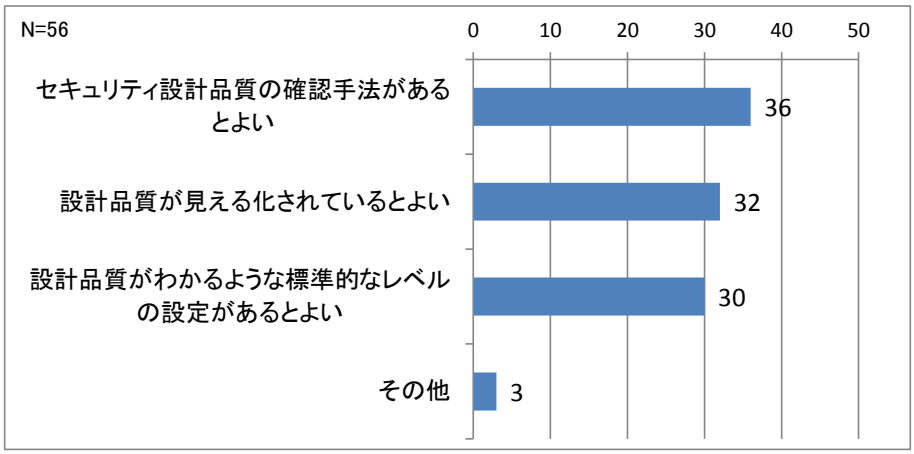


図 2-67 他社製品･ソフトウェアのセキュリティ設計品質の確認のためにあるとよいもの

アンケート設計時に想定した選択肢に対して、30 件前後（6 割前後）の選択があった。その他は 3 件であり、選択肢の設定は妥当であったと評価されるが、件数の差が小さいため、ガイドブック反映や今後の施策に対する優先度を付けにくい点が課題。

2.8.7.7 設問43）利用者が自社製品を他社製品と接続させる際に、接続先の製品・ソフトウェアのセキュリティ設計品質やレベルを確認して、接続の制御などに利用する仕組みはありますか？（複数回答）

N は複数回答の合計回答数。横軸は複数回答の回答数。

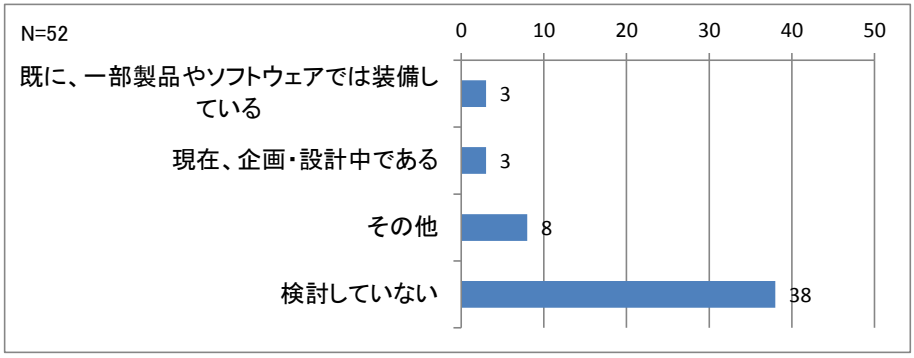


図 2-68 他社製品・ソフトウェアのセキュリティ設計品質やレベルを確認する仕組み

「既に、一部製品やソフトウェアでは装備している」が 3 件、「現在、企画・設計中である」が 3 件と、少ないながら該当する回答者がある。

- 分野
  - 「既に・・・」：自動車 1 件、スマート家電 1 件、スマートフォン 1 件
    - 前 2 件は同じグループ企業
  - 「現在・・・」：自動車 2 件、スマート家電 1 件
- 担当業務
  - 「既に・・・」は、設計・開発 2 件、開発マネジメント 1 件
  - 「現在・・・」は、3 件とも「研究開発」であり、そのために企画内容を知っていたと思われる。
- その他の特徴
  - 利用しているセキュリティ設計手法の数（設問 33）は、「既に・・・」の 3 件は 9～16 個と比較的高いが、 「現在・・・」の 3 件は 0～1 個。

2.8.7.8 設問44）（設問43で1または2を選ばれた方へ）上記の機能はどのような内容でしょうか？

具体的な内容を確認すると、ハードウェア／ソフトウェアによる自動化されたシステムはなく、人による手続き（プロセス）であることが分かる。

- 内容：
  - アクセス制御や受入れソフトの耐タンパー化などケースバイケースではあるが、社内セキュリティ基準に合致するように対応する。

3 おわりに

複数の健康器具を組み合わせたヘルスケアサービスや、スマートフォンで家電を制御するサービスなど、異なる分野の製品やサービスを組み合わせた新たなサービスが始まっており、今後は、さらに様々な製品等による高度なつながるサービスが出現すると見込まれる。このような「つながる世界」においては個々の製品の問題がシステム全体の問題となる。1 つの機器のセキュリティ上の脅威だったものが、つながることによりシステム全体の脅威となり、1 つの機器の安全上のハザードがシステム全体の安全上のハザードになり得る。また、問題が発生したときは迅速な説明責任が求められる。

本調査は「つながる世界」において求められる安全や安心といった観点から、セーフティ設計（設計の段階で安全を作りこむこと）とセキュリティ設計（設計の段階で脆弱性の低減や脅威への対策を考慮に入れること）、及び設計品質の見える化（エビデンスを使って論理的に第三者に分かるように説明すること）が今後必要になるとの考えの下、相互に接続される製品・サービスの信頼性を確認するための仕組みを実現するために、ハザードに対応するセーフティ設計と脅威に対応するセキュリティ設計がどの程度実施されているか、またアシュアランスケース等を使ったこれら見える化の取組みが産業界にどれほど普及しているかについての現状調査を目的に実施した。。

この調査結果から、「1.3 アンケートから判明した事項」 に記載した多くの有用な知見を得ることができた。

調査結果は、広く産業界にセーフティ設計とセキュリティ設計を定着させ、かつセーフティとセキュリティの設計品質の見える化の普及を図ることを目的に活用し、普及のためのガイドブックを作成して公開を行う予定である。

謝辞

本調査にあたり、アンケートによって有用な情報をご提供頂いた皆様、及びアンケート調査のレビューにご協力頂いた「サプライチェーンにおける品質の見える化 WG」の皆様に謝意を表する。

IPA/SEC 関係者一同

4 付録 アンケート用紙

（次ページから）

独立行政法人 情報処理推進機構 ソフトウェア高信頼化センター(IPA/SEC)
セーフティ・セキュリティ設計の見える化推進のためのアンケート

近年、さまざまな製品にネットワーク機能が普及し、パソコン同様に自動車や家電でも侵入、情報漏えいなどのセキュリティが問題になっています。また、新たな機能や製品の登場で、これまでにない要因による火災やけがなどのセーフティの問題も発生しています。しかし、現在のスマート製品を支えるソフトウェアは規模が大きく、他社から調達した部品が多数組合せられているため、セキュリティやセーフティを含めた品質の確保や確認に、課題が多いと指摘されています。

IPA/SEC では、ソフトウェアのセーフティ・セキュリティ設計の普及や設計品質の見える化を推進し、製品・サービスを採用する企業が容易に設計品質を確認し、安心して利用できる社会を目指しています。今回は、セーフティ・セキュリティ設計と品質を見える化する手法を解説するガイドブックを発行するにあたり、実態を把握する為にアンケートを実施しております。ご協力をお願いいたします。

※アンケートの設問の構成は以下のとおりです。

○ご回答者のプロフィール	(設問ア～カ)
○セーフティ設計について	(設問１～２２)
○セキュリティ設計について	(設問２３～４４)
○その他	(設問４５、４７)

アンケートのご回答について

※製品企画、システム設計、安全設計、品質保証などの部門のリーダーの方にご回答をお願いいたします。ご回答にかかる時間の目安は 20 分程度です。

※(締切のご案内は削除)

※セーフティ設計とセキュリティ設計の設問を別の方が回答される場合か、設問イ(1)の異なる分野のご担当が回答なさる場合には、本回答用紙全体をコピーして別途ご記入・ご返送ください。

※ご回答者でご希望の方にはガイドブックを謹呈いたします。(詳しくは末尾で)

※本アンケートのご回答は統計処理した上でガイドブックと報告書に利用し、個々の企業名などの情報は公開しません。また、個人情報は本調査とガイドブック送付以外の目的では使用しません。

(返送先は削除)

A．ご回答者の部門の開発内容

設問ア　ご回答者(あなた)が所属する御社名と事業部門、御氏名をご記入ください。

御社名［　　］　部署名［　　］御氏名［　　］

設問イ　あなたの事業部門が開発されている製品やソフトウェアについてお伺いします。

1)製品・ソフトウェアの分野は、何でしょうか？(最も近いものを一つ)

1．自動車　2．スマートフォン　3．ヘルスケア　4．スマート家電

5．その他（具体的に：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

2)どの部分を開発されていますか？(複数回答)

1．機器本体　2．ゲートウェイ機器　3．クラウド上のソフトウェア　4．アプリケーション

5．その他（具体的に：　　）

設問ウ　あなたが担当されている業務は、何でしょうか？（最も近いものを一つ）

1．経営　2．事業・製品企画　3．品質管理　4．研究開発　5．開発マネジメント

6．設計・開発　7．生産管理　8．総務部門　9．営業・販売部門

１０．その他（具体的に：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

設問エ　あなたが担当されている業務の経験年数は何年でしょうか（最も近いものを一つ）

1．「1年未満」　2．「1年以上3年未満」　3．「3年以上5年未満」

4．「5年以上１０年未満」　5．「１０年以上」

設問オ　セーフティ設計またはセキュリティ設計の必要性はお感じですか？(どれか一つ)
なお、セーフティ設計とは設計の段階で安全を作りこむこととお考えください。セキュリティ設計とは、設計の段階で脆弱性の低減や脅威への対策を考慮に入れることとお考えください。

1.セーフティ設計の必要性を感じている　2．セキュリティ設計の必要性を感じている

3.セーフティ設計とセキュリティ設計の必要性を感じている　4．どちらも必要と感じていない

設問カ　国際規格で認証を取得されているものがありますか？（○で各々一つ）

○品質マネジメントシステムの国際規格について

1．ISO 9001 を　（　取得している　／　取得していない　）

2．他の品質マネジメントシステムを　（　取得している　／　取得していない　）

↳ 具体的に：＿＿＿＿＿＿

○セーフティ関係の国際規格について

3．IEC 61508（電気・電子・プログラマブル電子）を（　取得している　／　取得していない　）

4．ISO 13849（安全制御システム）を　（　取得している　／　取得していない　）

5．ISO 10218（産業用ロボット）を　（　取得している　／　取得していない　）

6．ISO 26262（自動車用機能安全）を　（　取得している　／　取得していない　）

7．IEC 62304（医療機器ソフトウェア）を　（　取得している　／　取得していない　）

8．他のセーフティ関係の国際規格を　（　取得している　／　取得していない　）

↳具体的に：＿＿＿＿＿＿

○セキュリティ関係の国際規格について

9．ISO 15408(セキュリティ評価・認証) を　（　取得している　／　取得していない　）

１０．ISO 27001（情報セキュリティマネジメントシステム、ISMS）を（　取得している　／　取得していない　）

１１．他のセキュリティ関係の国際規格を　（　取得している　／　取得していない　）

↳ 具体的に：＿＿＿＿＿＿

B．セーフティ設計の基本方針について

ここでは、貴部門でのセーフティ設計についてお伺いします。

設問１　あなたのご担当部門でいう「製品のセーフティ」には、何が含まれますか？（複数回答）

1．ユーザーの命や身体の安全を守るもの　　2．ユーザーの財産や利用環境を守るもの
3．関連法令や基準の安全に関わる事項（具体的に：　　）
4．発注者から「セーフティ」として与えられた要件
5．その他（具体的に：　　）
6．製品や開発案件ごとに異なる　　7．特に「セーフティ」は考えていない

設問２　あなたのご担当部門には「製品のセーフティ設計」に関する基本方針がありますか？（最も近いものを一つ）

1．「製品のセーフティ設計」に特化した、明文化された基本方針がある
2．「製品のセーフティ設計」を含む、明文化された基本方針がある
3．明文化された基本方針はない

設問３（設問２で３を選ばれた方へ） 明文化した基本方針の代わりに、何をセーフティ設計の基準にされていますか？（複数回答）

1．社内に暗黙の基本方針がある　　2．過去の開発内容に基づいて判断している
3．機種ごとに検討し、判断している　　4．開発リーダーが判断している
5．その他（具体的に：　　）
6．セーフティ設計の基準は必要ない

C．セーフティ設計の設計ルールについて

ここでは、貴部門でのセーフティ設計の設計ルール（具体的な設計プロセスやレビュー手続きなど）についてお伺いします。

設問４　御社には、セーフティ設計の設計ルールがありますか？（最も近いものを一つ）

1．セーフティ設計に特化した、明文化された設計ルールがある
2．セーフティ設計を一部とする、明文化された設計ルールがある
3．外部の設計ルールを導入している（具体的に：　　）
4．明文化された設計ルールはない

設問５（設問４で４を選ばれた方へ）セーフティ設計ルールの代わりになるものはありますか？（最も近いものを一つ）

1．社内に暗黙の設計ルールや習慣がある
2．リーダーなどの判断に任されている
3．その他（具体的に：　　）
4．セーフティ設計ルールは必要ない

設問６　セーフティ設計の適用レベルは、製品や開発案件によって変わりますか？（複数回答）

1．想定リスクの大小により、セーフティ設計レベルが変わることがある
2．開発予算に応じて、セーフティ設計レベルが変わることがある
3．発注者の要求仕様に応じて、セーフティ設計レベルが変わることがある
4．セーフティ設計レベルは製品や開発案件によって変わることはない
5．その他（具体的に：　　）
6．特にセーフティ設計は行っていない

D．セーフティ設計の対象となるハザードについて

ここでは、貴部門でのセーフティ設計の対象となるハザード（危害の潜在的な源）についてお伺いします。

設問７　御社の製品・サービスで想定されるハザードは何でしょうか？（〇は各々一つ）

〇人命や身体に影響を及ぼすハザード
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

〇財産や利用環境に影響を及ぼすハザード
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

〇社会に広範囲の影響を及ぼすハザード
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

設問８　代表的なハザードの例を記述願います。

具体的に：

設問９　ハザードを踏まえたセーフティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（複数回答）

1．重要なセーフティ設計対応については、経営層の承認を受ける
2．すべてのセーフティ設計対応について、経営層の承認を受ける
3．重要なセーフティ設計対応については、品質保証部門の承認を受ける
4．すべてのセーフティ設計対応について、品質保証部門の承認を受ける
5．基本的に開発部門で判断する
6．その他（具体的に：　　）

E．セーフティ設計のための手法やツールについて

ここでは、貴部門で利用されているセーフティ設計のための手法やツールについてお伺いします。

設問１０　ハザード分析について、手法やツールを利用していますか？（複数回答）

1．FMEA (Failure Mode and Effect Analysis）を利用　2．FTA (Fault Tree Analysis)手法を利用
3．HAZOP（Hazard and Operability Studies）手法を利用　4．STAMP/STPA 手法を利用
5．その他の手法やツールを利用（具体的に：　　）
6．独自の手法でハザード分析を行っている　7．ハザード分析は行っていない

設問１１　ハザードに対するセーフティ設計・評価について、手法やツールを利用していますか？（複数回答）

1．フールプルーフ手法を利用　2．アフォーダンス手法を利用　3．フェールセーフ手法を利用
4．多層防御手法を利用　5．形式手法を利用
6．その他の手法やツールを利用（具体的に：　　）
7．独自の手法でセーフティ設計・評価を行っている　8．セーフティ設計は行っていない

設問１２　セーフティ設計品質の見える化について手法やツールを利用していますか？（複数回答）

（注）「セーフティ設計品質の見える化」とは、対象システム（製品）の安全性が設計において確保されていることを、エビデンスを使って論理的に第三者に分かるように説明を行うことです。

1．GSN (Goal Structuring Notation)で見える化している
2．CAE (Claim Argument Evidence)で見える化している
3．D-CASE で見える化している(D-CASE を GSN として使用している場合は 1 を選択願います）
4．その他のグラフィカルな手法を利用している（手法名を具体的に：　　）
5．独自の手法で見える化を行っている（手法内容を具体的に：　　）
6．見える化は行っていない

設問１３（設問１２で６を選ばれた方へ）見える化の手法に興味はありますか？（最も近いものを一つ）

1．手軽に使える見える化手法やツールがあるなら、使用してみたい
2．見える化手法やツールに興味はあるが、見える化のためのスキルや時間がない
3．見える化手法やツールに興味はあるが、見える化導入の費用対効果が低い、または分からない
4．セーフティ設計の見える化自体、必要と思わない
5．その他（具体的に：　　）

設問１４　セーフティ設計品質をどのように「客観的」に確認していますか？（複数回答）

1．設計者以外のメンバーを含めて、レビューを行っている
2．評価手法やツールを用いて確認している（評価手法の名称：　　）
3．発注側の技術者が確認している
4．その他（具体的に：　　）
5．客観的な確認は行っていない

設問１５（設問１４で５を選ばれた方へ）客観的な確認を行っていない理由は何でしょうか？（複数回答）

１．開発関係者によるレビューで十分であるため
２．客観的なレビューを行う人手やコストがないため
３．開発者以外の人に品質設計の内容を理解させることが難しいため
４．適当な評価手法やツールが見当たらないため
５．その他（具体的に：　　）

Ｆ．受発注時のセーフティ設計の要件の提示について

ここでは、貴部門で開発の受発注を行う際の「セーフティ要件」（その製品・ソフトウェアにおいてセーフティ上、何を守るかの指定事項）の提示についてお伺いします。

設問１６　他社への発注時に、発注先にセーフティ要件を提示していますか？（最も近いものを一つ）

１．セーフティ要件を提示し、セーフティ設計は発注先に任せる
２．セーフティ要件と併せて、一部のセーフティ仕様についても仕様を提示する
３．セーフティ要件は提示していない
４．その他（具体的に：　　）

設問１７　他社からの受注時に、発注者からセーフティ要件が提示されていますか？（最も近いものを一つ）

１．セーフティ要件が提示されている
２．セーフティ要件と併せて、一部のセーフティ設計についても仕様が提示されている
３．セーフティ要件は提示されていない
４．その他（具体的に：　　）

設問１８（設問１７で３を選ばれた方へ）セーフティ要件が提示されない場合、どのように対応しますか？（最も近いものを一つ）

１．セーフティ要件がなければ、セーフティ設計は行わない
２．自社でリスクを分析し、セーフティ要件を発注者に確認する
３．自社でリスクを分析し、自主的にセーフティ設計を行う
４．その他（具体的に：　　）

Ｇ．他社の製品・ソフトウェアのセーフティ設計品質の確認について

ここでは、貴部門が他社の製品・ソフトウェアと組合せて製品・ソフトウェア開発を行う場合における、セーフティ設計品質の確認についてお伺いします。

設問１９　他社の製品・ソフトウェアと組合せて開発を行う場合、他社製品・ソフトウェアのセーフティ設計品質の確認はどのように行いますか？（複数回答）

１．カタログ等で対応規格の有無を確認する　　２．品質保証の根拠説明資料を確認する
３．他社の技術者に問い合わせる　　４．自社で調査、検証、評価する
５．その他（具体的に：　　）

設問２０　他社製品・ソフトウェアの設計品質の確認のために、何があるとよいと思われますか？（複数回答）

１．他社の製品・ソフトウェアのセーフティ設計品質の確認手法があるとよい
２．他社の製品・ソフトウェアの設計品質が見える化されているとよい
３．他社の製品・ソフトウェアの設計品質がわかるような標準的なレベルの設定があるとよい
４．その他（具体的に：　　）

設問２１　利用者が自社製品と他社製品を接続させる際に、接続先の製品・ソフトウェアのセーフティ設計品質やレベルを確認して、接続の制御などに利用する仕組みはありますか？（複数回答）

１．既に、一部製品やソフトウェアでは装備している
２．現在、企画・設計中である
３．その他（具体的に：　　）
４．検討していない

設問２２（設問２１で１または２を選ばれた方へ）上記の機能はどのような内容でしょうか？

具体的に：

H．セキュリティ設計の基本方針について

ここでは、貴部門でのセキュリティ設計についてお伺いします。

設問２３　あなたのご担当部門でいう「製品のセキュリティ」には、何が含まれますか？（複数回答）

１．ソフトウェア・情報の機密性　　２．ソフトウェア・情報の完全性（改ざんからの保護）
３．正当なユーザーだけがいつでも利用できる状態　　４．発注者から与えられたセキュリティ要件
５．関連法令や基準のセキュリティに関わる事項（具体的に：　　）
６．その他（具体的に：　　）
７．製品や開発案件ごとに異なる　　８．特に「セキュリティ」は考えていない

設問２４　あなたのご担当部門には「製品のセキュリティ設計」に関する基本方針がありますか？（最も近いものを一つ）

１．「製品のセキュリティ設計」に特化した、明文化された基本方針がある
２．「製品のセキュリティ設計」を含む、明文化された基本方針がある
３．明文化された基本方針はない

設問２５（設問２４で３を選ばれた方へ）明文化された基本方針の代わりに、何をセキュリティ設計の基準にされていますか？（複数回答）

１．社内に暗黙の基本方針がある　　２．過去の開発内容に基づいて判断している
３．機種ごとに検討し、判断している　　４．開発リーダーが判断している
５．その他（具体的に：　　）
６．セキュリティ設計の基準は必要ない

Ｉ．セキュリティ設計の設計ルールについて

ここでは、貴部門でのセキュリティ設計の設計ルール（具体的な設計プロセスやレビュー手続きなど）についてお伺いします。

設問２６　御社には、セキュリティ設計の設計ルールがありますか？（最も近いものを一つ）

1．セキュリティ設計に特化した、明文化された設計ルールがある
2．セキュリティ設計を一部とする、明文化された設計ルールがある
3．外部の設計ルールを導入している（具体的に：　　）
4．明文化された設計ルールはない

設問２７（設問２６で４を選ばれた方へ）セキュリティ設計ルールの代わりになるものはありますか？（最も近いものを一つ）

1．社内に暗黙の設計ルールや習慣がある
2．リーダーなどの判断に任されている
3．その他（具体的に：　　）
4．セキュリティ設計ルールは必要ない

設問２８　セキュリティ設計の適用レベルは、製品や開発案件によって変わりますか？（複数回答）

1．想定リスクの大小により、セキュリティ設計レベルが変わることがある
2．開発予算に応じて、セキュリティ設計レベルが変わることがある
3．発注者の要求仕様に応じて、セキュリティ設計レベルが変わることがある
4．セキュリティ設計レベルは製品や開発案件によって変わることはない
5．その他（具体的に：　　）
6．特にセキュリティ設計は行っていない

Ｊ．セキュリティ設計の対象となる脅威について

ここでは､貴部門でのセキュリティ設計の対象となる脅威(損害を与える可能性がある事象の潜在的な原因)についてお伺いします。

設問２９　御社の製品・サービスで想定される脅威は何でしょうか？（○は各々一つ）

○人命や身体に影響を及ぼす脅威
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

○財産や利用環境に影響を及ぼす脅威
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

○社会に広範囲の影響を及ぼす脅威
［ 想定される ／ 製品によっては想定される ／ 想定されにくい ／ 未検討 ／ わからない ］

設問３０　代表的な脅威の例を記述願います。

具体的に：

設問３１　脅威を踏まえたセキュリティ設計上の判断に、経営層や品質保証部門の責任者が関わることはありますか？（複数回答）

1．重要なセキュリティ設計対応については、経営層の承認を受ける
2．すべてのセキュリティ設計対応について、経営層の承認を受ける
3．重要なセキュリティ設計対応については、品質保証部門の承認を受ける
4．すべてのセキュリティ設計対応について、品質保証部門の承認を受ける
5．基本的に開発部門で判断する
6．その他（具体的に：　　）

K. セキュリティ設計のための手法やツールについて

ここでは、貴部門で利用されているセキュリティ設計のための手法やツールについてお伺いします。

設問３２　セキュリティ上のリスク分析について、手法やツールを利用していますか？（複数回答）

1．脅威モデリング手法（STRIDE, DFD）を利用　　2．ISO/IEC27005 (GMITS) を利用
3．ミスユースケース手法を利用　　4．エージェント指向（i *／Secure Tropos）手法を利用
5．問題フレーム手法を利用　　6．ゴール指向を利用　　7．FTA (Fault Tree Analysis)手法を利用
8．FMEA (Failure Mode and Effect Analysis）を利用　　9．Attack Tree 手法を利用
10．ALE (Annual Loss Expectation）手法を利用
11．HAZOP（Hazard and Operability Studies）手法を利用
12．その他の手法やツールを利用（具体的に：　　）
13．独自の手法でリスク分析を行っている　　14．リスク分析は行っていない

設問３３　リスクに対するセキュリティ設計・評価について、手法やツールを利用していますか？（複数回答）

1．CC (ISO/IEC 15408)を利用　　2．FIPS-140 を利用　　3．Twin Peaks 手法を利用
4．SDL (Secure Development Lifecycle) を利用　　5．SQUARE を利用　　6．UML を利用
7．アクセス制御を利用　　8．認証を利用　　9．暗号化を利用　　10．電子署名を利用
11．侵入検知を利用　　12．ログ・監査を利用　　13．脆弱性評価を利用
14．SIM/TPM 等信頼を担保する手法を利用　　15．形式手法を利用
16．その他の手法やツールを利用（具体的に：　　）
17．独自の手法でセキュリティ設計・評価を行っている　　18．セキュリティ設計は行っていない

設問３４セキュリティ設計の見える化について、手法やツールを利用していますか？（複数回答）

（注）「セキュリティ設計品質の見える化」とは、対象システム（製品）のセキュリティが設計において確保されていることを、エビデンスを使って論理的に第三者に分かるように説明を行うことです。

1．GSN (Goal Structuring Notation)で見える化している
2．CAE (Claim Argument Evidence)で見える化している
3．D-CASE で見える化している(D-CASE を GSN として使用している場合は 1 を選択願います)
4．その他のグラフィカルな手法を利用している（手法名を具体的に：　　）
5．独自の手法で見える化を行っている（手法内容を具体的に：　　）
6．見える化は行っていない

設問３５（設問３４で６を選ばれた方へ）見える化の手法に興味はありますか？（最も近いものを一つ）

1．手軽に使える見える化手法やツールがあるなら、使用してみたい
2．見える化手法やツールに興味はあるが、見える化のためのスキルや時間がない
3．見える化手法やツールに興味はあるが、見える化の費用対効果が低い、または分からない
4．セキュリティ設計の見える化自体、必要と思わない
5．その他（具体的に：　　）

設問３６　セキュリティ設計の品質をどのように「客観的」に確認していますか？（複数回答）

1．設計者以外のメンバーを含めて、レビューを行っている
2．評価手法やツールを用いて確認している（評価手法の名称：　　）
3．発注側の技術者が確認している
4．その他（具体的に：　　）
5．客観的な確認は行っていない

設問３７（問３６で５を選ばれた方へ）客観的な確認を行っていない理由は何でしょうか？（複数回答）

1．開発関係者によるレビューで十分であるため
2．客観的なレビューを行う人手やコストがないため
3．開発者以外の人材にレビューを行わせることが難しいため
4．適当な評価手法やツールが見当たらないため
5．その他（具体的に：　　）

Ｌ．受発注時のセキュリティ設計の要件の提示について

ここでは、貴部門で開発の受発注を行う際の「セキュリティ要件」（その製品・ソフトウェアにおいてセキュリティ上、何を守るかの指定事項」の提示についてお伺いします。

設問３８　他社への発注時に、発注先にセキュリティ要件を提示していますか？（最も近いものを一つ）

1．セキュリティ要件を提示し、セキュリティ設計は発注先に任せる
2．セキュリティ要件と併せて、一部のセキュリティ設計についても仕様を提示する
3．セキュリティ要件は提示していない
4．その他（具体的に：　　）

設問３９　他社からの受注時に、発注者からセキュリティ要件が提示されていますか？
（最も近いものを一つ）

1．セキュリティ要件が提示されている
2．セキュリティ要件と併せて、一部のセキュリティ設計についても仕様が提示されている
3．セキュリティ要件は提示されていない
4．その他（具体的に：　　）

設問４０（設問３９で３を選ばれた方へ）セキュリティ要件が提示されない場合、どのように対応しますか？（最も近いものを一つ）

1．セキュリティ要件がないので、セキュリティ設計は行わない
2．自社でリスクを分析し、セキュリティ要件を発注者に確認する
3．自社でリスクを分析し、自主的にセキュリティ設計を行う
4．その他（具体的に：　　）

M. 他社の製品・ソフトウェアのセキュリティ設計品質の確認について

ここでは、貴部門が他社の製品・ソフトウェアと組合せて製品・ソフトウェア開発を行う場合における、セキュリティ設計品質の確認についてお伺いします。

設問４１　他社の製品・ソフトウェアと組合せて開発を行う場合、相手のセキュリティ設計品質の確認はどのように行いますか？（複数回答）

1．カタログ等で対応規格の有無を確認する　　2．品質保証の根拠説明資料を確認する
3．他社の技術者に問い合わせる　　4．自社で調査、検証、評価する
5．その他（具体的に：　　）

設問４２　他社製品・ソフトウェアの設計品質の確認のために、何があるとよいと思われますか？（複数回答）

1．他社の製品・ソフトウェアのセキュリティ設計品質の確認手法があるとよい
2．他社の製品・ソフトウェアの設計品質が見える化されているとよい
3．他社の製品・ソフトウェアの設計品質がわかるような標準的なレベルの設定があるとよい
4．その他（具体的に：　　）

設問４３　利用者が自社製品を他社製品と接続させる際に、接続先の製品・ソフトウェアのセキュリティ設計品質やレベルを確認して、接続の制御などに利用する仕組みはありますか？（複数回答）

1．既に、一部製品やソフトウェアでは装備している
2．現在、企画・設計中である
3．その他（具体的に：　　）
4．検討していない

設問４４（設問４３で１または２を選ばれた方へ）上記の機能はどのような内容でしょうか？

具体的に：

アンケートは以上です。ご協力ありがとうございました。