TLP:CLEAR

2023 年度
第 4 四半期レポート

2024 年 4 月 26 日

一般社団法人　Japan Automotive ISAC

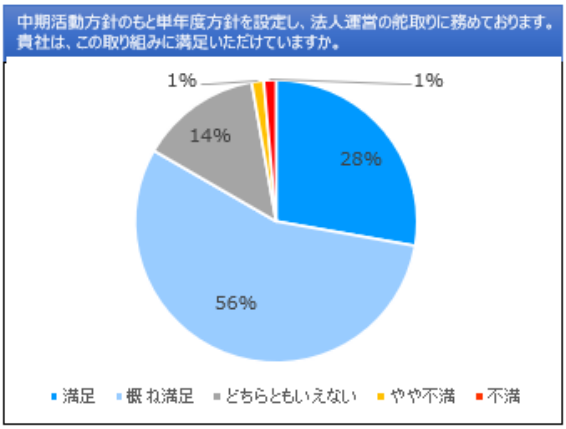
目　次

【第 1 章】運営委員会からの活動報告

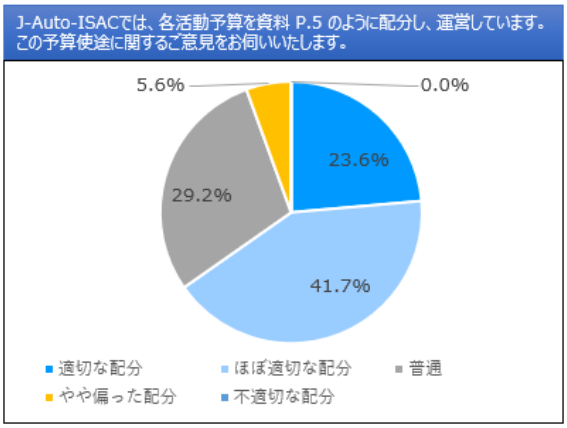
1. 2023 年度運営委員会アンケート結果

72 社の会員の皆様から運営委員会アンケートに回答いただきました。ご協力ありがとうございました。22 年度アンケートと比較すると全体的には改善が進んできた結果となりましたが、まだまだ、足りない点、ご心配かけている点など再確認できました。ここでは各活動への満足度と代表的な意見を共有します。

①



②



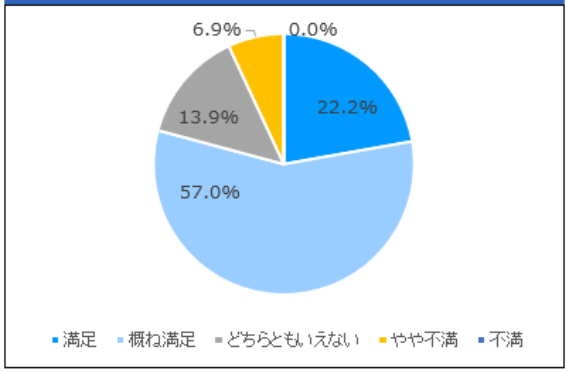
①活動方針に関する満足度と主な意見： 80%以上が満足・概ね満足と回答（22 年度：83%）

・今後の展望についての方向性が見えづらい。
・日本自動車工業会、自動車技術会は'50 年までのロードマップを描いている為、他団体と同期したかたちで更新して欲しい。
・今後の在り方についてみなさんと一緒に議論を深める場があればいいと思います。
・TF 活動など、脆弱な組織ですと全てに対応しきれないのが実情。負荷を下げることも検討して欲しい。

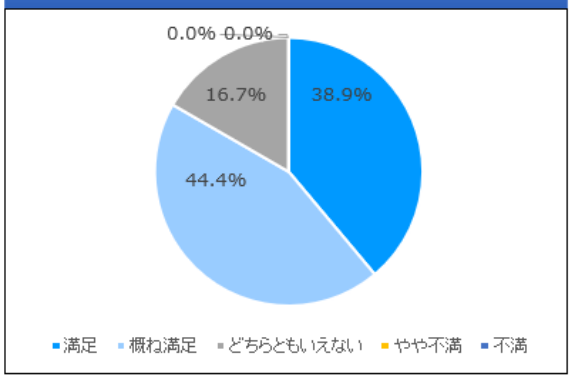
②予算配分に関する満足度と主な意見： 適切・ほぼ適切と 65%が回答（22 年度：74%）

・会員ランクによる会費の違いと運営費との対比がわかりづらい。
・予算の割合や額などについて判断が出来ないが、どのように費用削減に努めているかを教えてほしい。
・何が起こるかわからないリスク対応で予備費はあったほうが良いと考える。
・予算の不足への対処は、物価上昇など加味して判断いただければと思いました。
・SOC が主な支出先というのは理解できますし、範囲も広がってきてきると思います。今後の予算増加に対しての向き合い方を明確にしてほしいと思います。

③ 運営委員会では、ホームページ、Teams、総会などを活用し、会員の皆様との情報共有に努めております。貴社は、この取り組みに満足いただけていますか。



④ 貴社は、J-Auto-ISAC事務局が提供する各種会員サポートに満足いただけていますか。（問い合わせに対する回答までの時間、回答の的確さについてなど）



③情報共有に関する満足度と主な意見：　80%弱が満足・概ね満足（22 年度：57%）

・総会の報告内容が定型的、新たに参加しようという意思を生み出しにくいのではないか

・他の ISAC（ICT,医療,等）の取組み状況や連携情報があるとさらに有益になると思う。

・全体の活動状況は見えづらい部分がどうしてもあるため

・運営委員会や理事会に関する情報展開の頻度が少なく感じるため

④事務局サポートへの満足度と主な意見：　80%以上が満足・概ね満足（22 年度：67%）

・当社組織変更に伴うユーザー削除などの依頼に対し、対応期間が長い場合があり、どのタイミングで依頼して良いか分かりにくい。

・困ったときには事務局の方々にタイムリーにサポートいただいております。

・まだ、お問合せさせていただいたケースはありませんが、課題感はありません。

・活動に専念できるような配慮や会員サイト運営など、細かに対応して頂いている。

以上。

皆様からの声を ISAC 運営活動へ取込み、さらなる改善に努めて参ります。

今年度も全体運営の改善に向けたアンケートを行いますので、引き続きご協力いただきますようお願いいたします。

2.　第 4 四半期に入会いただいた新規会員

新規入会会員

・シルバー会員　イーソル株式会社

・賛助会員　パロアルトネットワークス株式会社

・賛助会員　GMO サイバーセキュリティ by イエラエ株式会社

新規会員からの一言（GMO サイバーセキュリティ by イエラエ）

ますます発展が進む自動車の安全安心に少しでも貢献できるよう、ペネトレーションテストやフォレンジック
など培ってきたセキュリティエンジニアの知見を活かして活動に参加したいと思っております。
どうぞ宜しくお願いいたします。

以上

【第 2 章】技術委員会からの活動報告

■はじめに

技術委員会では、23 年度の活動計画に則って WG/SWG の活動を推進してきています。SWG は技術委員会傘下に 12 の活動をしていますが、それぞれの活動を進める中で出てきた課題の解決策と、活動のさらなる充実と拡大に向けた施策を、引き続き「TC 課題検討 TF」で協議しています。

今回は、その施策の一つである第 2 回活動報告会の Part2 を 1 月 16 日（火）に実施していますので、その様子を本章のトピックとして報告します。

現在までの技術委員会活動人員の推移を表 2 に示しています。第 4 四半期時点で、ここまでの会員企業数の増加に伴い参加企業数も増えてきており、技術委員会の延べ参加人数も増加してきました。しかし新年度からの各社組織変更等の影響で 4 月からのメンバー交代や入退会の申し込みが多く来ているため、表 2 では新しい年度になる 4 月 1 日時点の数字を報告します。

表 2　技術委員会活動人数の推移

委員会／WG／SWG	発足時点 (21.6月末)	定期総会 (22.6.24)	臨時総会 (23.1.17)	臨時総会 (24.1.16)	24.4.1 時点	前回比増減
技術委員会 延べ参加人数	258	334	347	355	328	(27)
委員会活動参加企業数／会員企業総数	66／88	78/100	80/107	83/110	86/114	3
情報共有WG	115	128	132	111	106	(5)
インシデント対応事例検証SWG	47	47	50	34	35	1
脆弱性対応SWG	55	65	66	65	57	(8)
グローバル連携SWG	11	12	12	10	12	2
スキルアップWG	88	108	105	102	98	(4)
協同演習SWG	17	18	18	20	20	0
個別研修SWG	20	26	25	20	18	(2)
ベストプラクティス策定SWG	26	32	33	34	32	(2)
セキュリティ人材育成SWG	25	29	27	26	26	0
課題抽出＆解決推進WG	55	78	73	113	97	(16)
サプライチェンリスク対応SWG	33	38	35	32	28	(4)
データベース＆ポータル機能拡張検討SWG	11	14	11	10	廃止	(10)
情報共有プラットフォームSWG	11	13	14	14	13	(1)
フォレンジック検討SWG（'22.4.28発足）	–	11	11	13	13	0
SBOM-SWG	–	–	–	42	41	(1)
用語定義TF（'21.12.3発足）	–	12	13	13	10	(3)
法規動向調査TF（'22.4.21発足）	–	8	8	8	7	(1)
課題検討TF	–	–	6	6	8	2

赤字（　）は減少

技術委員会延べ参加人数は、23 年度にまで増加してきましたが、24 年度からは若干減少し、前年比 27 名減となる見込みです。23 年度 SBOM-SWG が新たに活動を開始し参加人数は増加しましたが、24 年度からはデータベース&ポータル機能拡張検討 SWG が終了すること、いくつかの SWG が成果物を発行して一区切りついたイメージがあることなどから、新たに SWG への参加募集を掛けたものの、各社参加者の整理がなされ全体として減少したものと考えています。

以下に 23 年度の活動計画と実績、トピック報告を記載します。

1. 23 年度活動計画と実績報告

1) 技術委員会活動成果物実績、社外発表等活動実績の報告

表 3 活動成果物一覧（発行成果物と発行予定）

時期	成果物
2023 年 5 月	・技術委員会用語集（正式フォーマットで発行）：用語定義 TF
2023 年 6 月	・インシデント事例分析レポート#1 ・第 2 回協同演習の実施（6 月 29 日）
2023 年 7 月	・脆弱性分析レポート＃ 1
2023 年 8 月	・自動車産業全体で連携して取り組む CS 品質向上活動の必要性（役員向け）動画版公開
2023 年 9 月	・インシデント事例分析レポート#2 ・クルマのサプライチェーンにおけるサイバーセキュリティ取り組みガイド Ver1.01 発行 ・協同演習分析レポート速報
2023 年 10 月	・脆弱性分析レポート＃2
2023 年 11 月	・クルマのサプライチェーンにおけるサイバーセキュリティ取り組みガイド Ver1.05 完成 （知財権確認中） ・インシデント対応ベストプラクティス（概要版）改訂（TLP-CLEAR 化対応中）
2023 年 12 月	・第 2 回法規動向調査 TF 説明会（第 2 回活動報告会の中で説明） ・インシデント事例分析レポート#3 スキルチェックシート Ver2.0（策定中） ・インシデント対応ベストプラクティス（詳細版）改訂（TLP-GREEN 化対応中）
2024 年 1 月	・自動車業界全体で連携して取り組む CS 品質向上活動の必要性(役員向け)動画 の HP での一般公開 ・協同演習分析レポート発行&説明会（第 2 回活動報告会の中で説明）
2024 年 2 月	・インシデント事例分析レポート#4 ・脆弱性分析レポート＃3
2024 年 3 月	－（なし）

表２－３ 社外発表等の活動実績一覧

時期	外部講演、セミナー関係
2023 年 5 月	第 1 回技術委員会活動報告会
2023 年 6 月	第 5 回 J-auto-ISAC 定時総会 （会員総会）
2023 年 7 月	第 4 回サイバーセキュリティフォーラム （JBpress） 自動車技術会フォーラム 2023（夏季）「自動車 CS 最前線」
2023 年 8 月	JNSA セミナー「日本におけるソフトウェアサプライチェーンのこれから」
2023 年 9 月	自動車技術会 自動車サイバーセキュリティ講座 2023
2023 年 10 月	Auto ISAC Cybersecurity Summit2023
2023 年 12 月 2024 年 1 月	**第 2 回技術委員会活動報告会（Part1：12 月開催／Part2：1 月開催）**
2024 年 2 月	**第 9 回オートモーティブ・ソフトウェア・フロンティア 2024 SDV 時代に求められるセキュリティ保証」講演**
2024 年 3 月	**NCA の課題検討及び脆弱性 WG イベントでの講演+パネルディスカッション登壇 （テーマ：「自動車業界における SBOM の現状」） Security Days Spring2024 で講演**

23 年度各四半期も、ほぼ毎月計画通りに成果物を委員会内で発表が出来ました。
また社外への発信も積み重ね、新たに入会申請をする会社が出てきていることから、J-Auto-ISAC の認知や入会のきっかけにすることも出来たと言えます。

2) 23 年度活動計画の棚卸

23 年度期末で 1 年間の活動を棚卸しました。第 4 四半期の時点で技術委員会としては、23 年度に以下のことが出来たと報告しました。

- 連携先との役割分担の整合・合意と活動のスタート
  北米 Auto-ISAC と包括で MOU を締結し、SBOM で具体的な連携活動開始
- 技術委員会内計画レビューの実施
  通期棚卸を 3 月の運営委員会報告完了し、3 月の技術委員会にて来期の計画策定
- 技術委員会アンケートの実施
  23 年度のアンケート結果を課題検討 TF で分析、対策を立案して来期計画へ反映
  23 年度は自由記述に対して、回答したメンバーからの個別ヒアリングを実施し、コメントの背景まで分析の対象とした
  次回活動報告会にて対応策について整理・報告予定
- 新たな TF 設置と運営等
  課題検討 TF を設置(9 月)して継続活動中
  各 SWG からの新規用語の定義ニーズに基づき用語定義 TF を再開

2. 【トピック報告】第 2 回活動報告会 *Part2*（*'24/1/16* 開催）

1）目的・背景

22 年度実施した技術委員会メンバーへのアンケート結果に基づく課題（他の SWG 活動の成果物、情報の共有）対策を目的に、23 年度に年間 2 回のイベントとして「技術委員会活動報告会」を開催しました。

2 回目となる第 2 回活動報告会は、技術委員会の活動全体像と各 SWG の関係性、成果物に関する詳細説明（成果物発表）、更に各 WG/SWG の活動内容と目標に焦点をあてた構成としました。そのため Part1 と Part2 に分けて以下の日程で開催しています。

第 2 回活動報告会 Part1：2023 年 12 月 6 日（水）10:00～17:20　@品川フロントビル

第 2 回活動報告会 Part2：2024 年 1 月 16 日（火）10:00～12:25　@品川フロントビル

2）内容（Part2：資料については技術委員会内で公開中）

① 協同演習 SWG（23 年度協同演習結果の報告とパネルディスカッション）

② TC 課題検討 TF（第 2 回技術委員会アンケート結果報告）

③ SBOM-SWG（活動概要報告）

3）Part2 実施後のアンケート結果速報と効果

Part2 実施後に取ったアンケートの結果は技術委員会メンバーで 99%、技術委員会不参加の会員で 100%が「他の WG/SWG の活動内容を知ることができた」と言っており、目的はほぼ果たせたと言えます。

活動報告会には見学を希望された J-Auto-ISAC の非会員企業の方々に、オブザーバとして誓約書提出の上参加いただいています。活動報告会後、それら非会員の企業から入会の申し入れがあり、現在も入会審査が続いています。このことから活動報告会での J-Auto-ISAC 活動のアピール効果もあったと考えています。

以上

【第 3 章】サポートセンターからの活動報告

1. 「よろず相談会」 開催

数十社から要望があり、2023 年 10 月より、新たな取り組みとして「個別相談会」を開始し、2024 年 2 月からは「よろず相談会」として月例化しました。さらに「テーマが決まっていると相談しやすい」との声に応えて、2 月以降はテーマを設定して隔週で開催しました。

回	実施日	テーマ
第1回	10月25日	フリー
第2回	10月27日	フリー
第3回	12月13日	フリー
第4回	12月15日	フリー
第5回	2月14日	SIRT組織について
第6回	2月28日	ランサムウェア攻撃対策
第7回	3月6日	サプライチェーン・セキュリティ（仕入先管理）
第8回	3月27日	規定整備の進め方（情報セキュリティ規定）

＜総 括＞

当初の想定と異なり毎回少人数での開催となったほか、参加者はセキュリティ診断で高い評価を受けている会員が大半でした。結果的には、高い問題意識を持った会員企業の方との踏み込んだ意見交換の場となりました。当センターにとっても、第一線で奮闘されている方の現状を知る良い機会となりました。

2024 年度からは、「お困りごと相談室」に名称を改めて月次開催を継続します。また、会員企業が直面している課題に関して、マンツーマンで個別相談ができる機会を積極的に設けて実施したいと考えています。さらに、サポートセンターからの情報提供に加え、パートナー会員と連携して具体的なサービス紹介も実施します。

主な相談内容	相談会での対応	参加企業のご感想
ISMSとCSMSの重なる部分の取り組みについて、意見交換をしたい	・ワークショップ的に意見交換	・回答者目線での相談ができた ・他の会員と意見交換をすることで理解が深まった ・小グループで相談しやすかった **・今後も継続してほしい** **・定期的な開催を希望** **・マンツーマンで相談できる場もあると良い**
レベル3の項目の妥当性や達成時期を教えてほしい	・意見交換を実施	
設問の解釈や回答内容の妥当性をチェックしたい	・自社でも回答者によってブレる ・取引先の回答のブレを無くしたい →パートナー企業のソリューションを紹介	
自社の判断が正しいか確認したい 設問の理解度、回答の制度を高めたい	・ワークショップ的に意見交換	
脆弱性情報を効率的に分析・仕分けする方法	・ワークショップ的に意見交換	
SIRTを組織する際の責任範囲などSIRT全般に関する意見交換をしたい	・意見交換を実施	

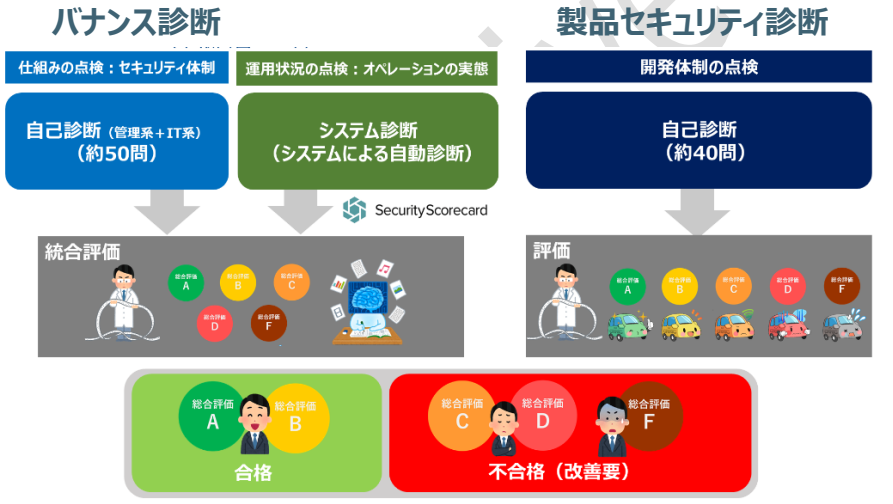
2. 「サイバーセキュリティ診断」について

＜概　要＞

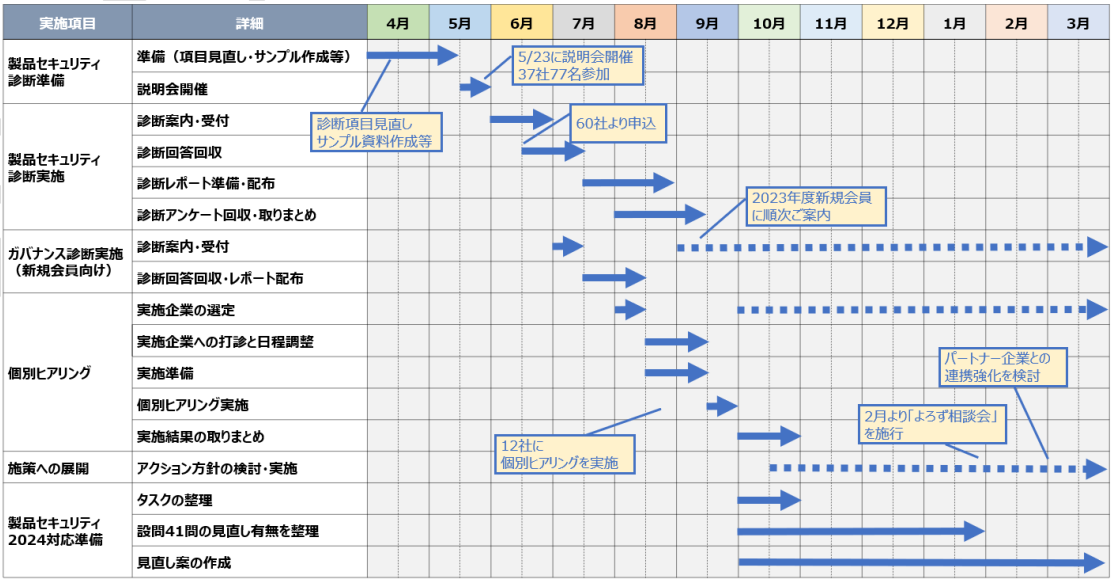
J-Auto-ISAC では、コネクテッドカーに関わるインシデント事例や脅威・脆弱性情報が会員間で共有されます。また活動の中で、他社の機密情報に触れる機会もあります。そこで当センターでは会員が相互に安全に、かつ安心して情報を共有できる"基盤づくり"の一環として「サイバーセキュリティ診断」を実施しています。
（一部の会員種別は除く）

「ガバナンス診断」では、情報セキュリティに関する規程や推進体制といった仕組みの整備状況を問う"自己診断"に加えて、専用プログラムによる"システム診断"によって総合的に評価して合否判定を実施しています。

また昨年度より、コネクテッドカー開発体制の整備状況を点検する「製品セキュリティ診断」を実施しています。



＜2023 年度の実施スケジュール＞



3. 「ガバナンス診断」について

2023 年度は底上げ活動にリソースを集中するため、新規会員のみを対象に実施し、本年度は計 6 社に対して診断を行いました。なお合格ライン未達の会員企業に対しては、個別に取り組み状況についてヒアリングを実施しました。

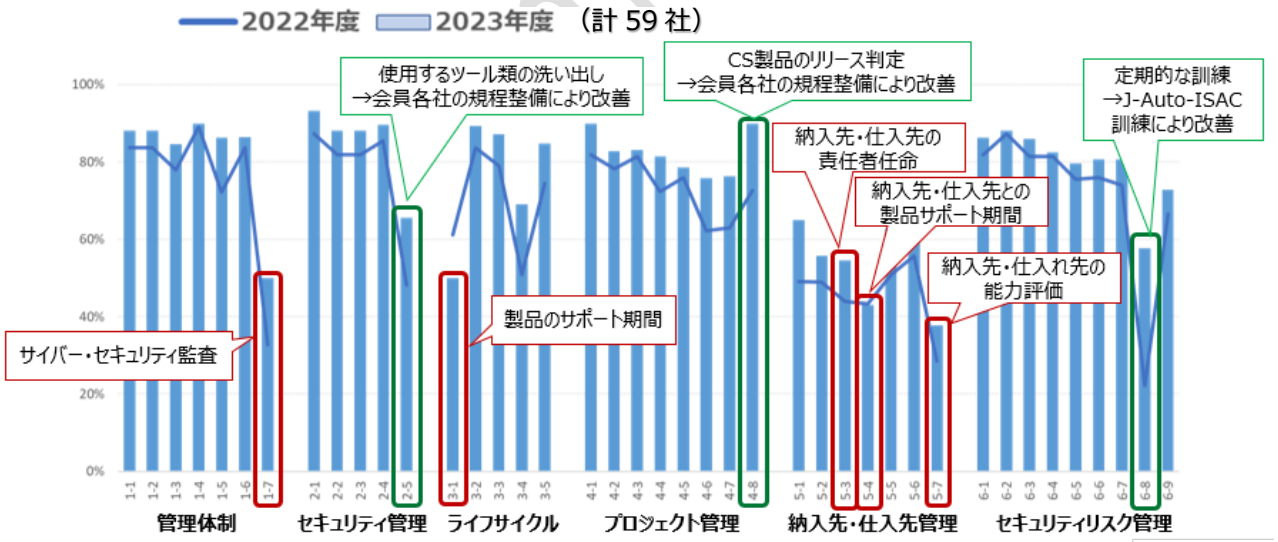
2024 年度は、新規会員企業のガバナンス診断の継続と合わせて、対象となる会員企業に“システム診断”サービスの無償提供を予定しています。

4. 「製品セキュリティ診断」について

2023 年度の診断結果は、2022 年度に比べて各カテゴリでカイゼンが進捗し、診断を実施した会員企業平均で 7 ポイントアップしました。また、カテゴリ別では特に「仕入れ先・納入先管理」「ライフサイクル」に共通課題があるとわかりました。

2024 年度は、これらの共通課題に対して技術委員会やパートナー企業とも連携し、ソリューションとなる支援を検討して行く予定です。

＜設問別の進捗状況＞



以上

【第 4 章】SOC（セキュリティオペレーションセンター）からの活動報告

1. 2023 年度 第 4 四半期の概要

1） 脅威・脆弱性情報の報告件数

2024 年 1 月から 3 月の 91 日間で提供された週次情報レポートの件数は、合計 86 件でした。図 1 に内訳が示されています。脅威・脆弱性情報の報告件数は、第 3 四半期と比較すると、わずかに減少しています。尚、引き続き車両に関連する新たな重大な脅威・脆弱性情報及びインシデントの発生はありませんでした。

① 脅威・脆弱性情報 ４６件
② 業界動向情報 ４０件

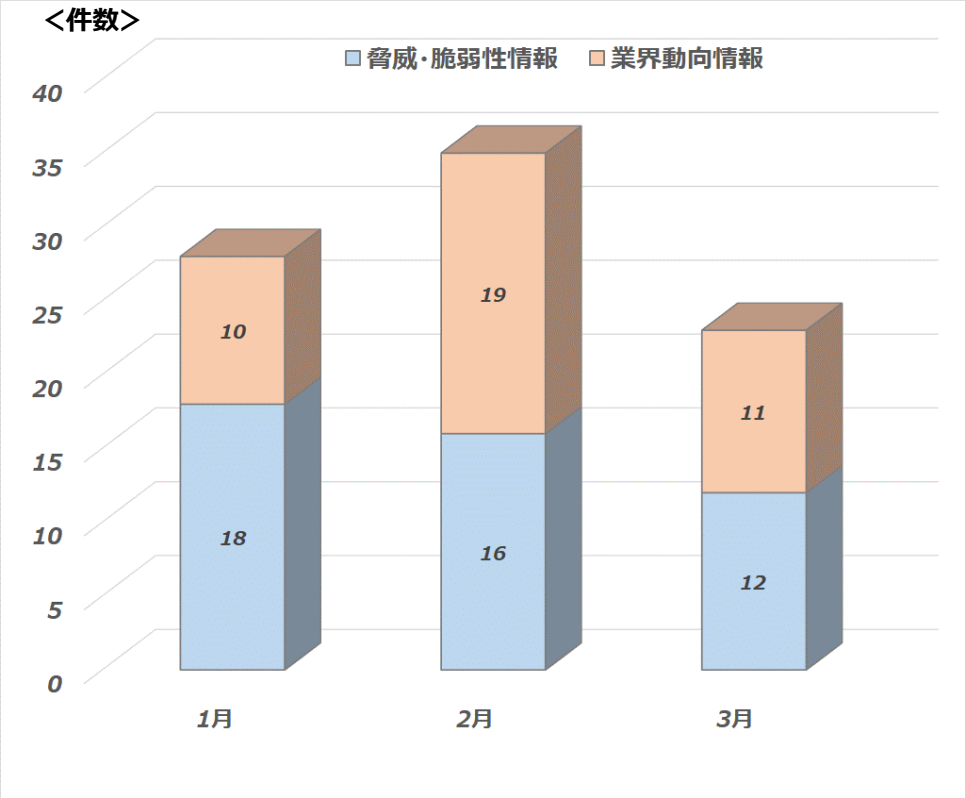


図 1 週次情報レポート 提供件数

※脅威・脆弱性情報件数は、自動車に係わる情報のみであり、かつ同一案件を除く

2） 脅威・脆弱性情報レベル

第 4 四半期における報告した脅威・脆弱性情報を分類すると図 2 のようになります。要注意情報の件数は平均で 8 件/月でしたが、第 3 四半期に比べると減少傾向です。

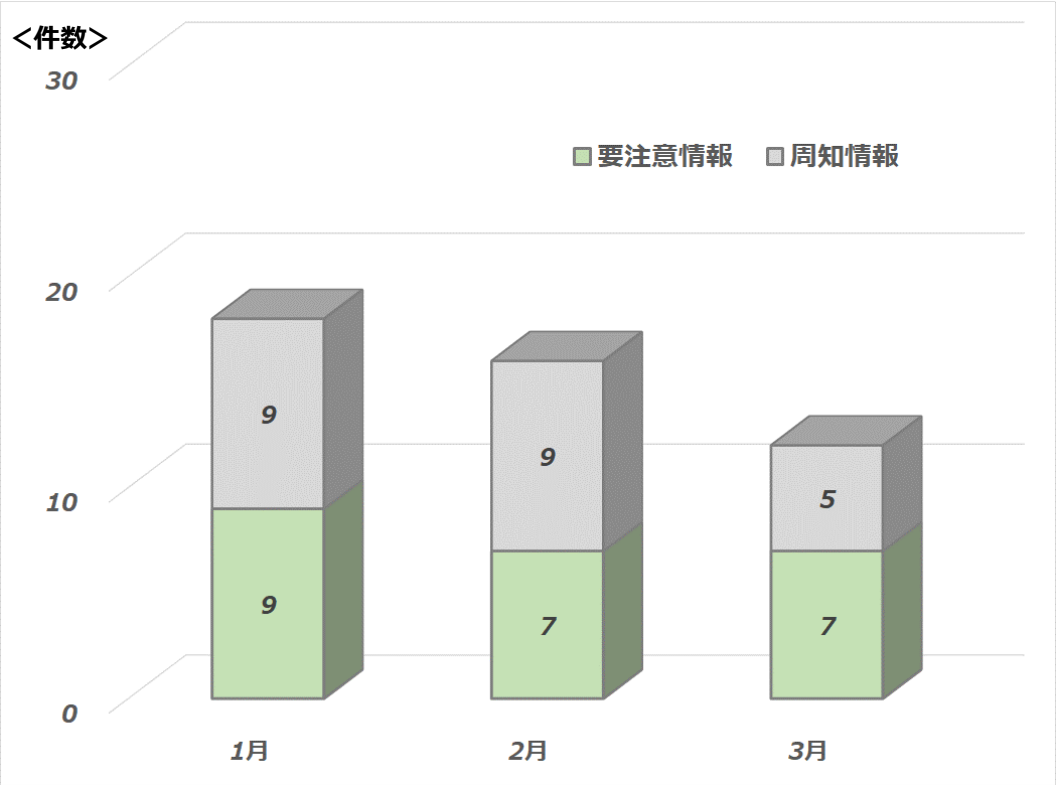


図 2 脅威・脆弱性情報 レベル別件数

<参考>

※1.要注意情報：

自動車への関連性があるが影響度・攻撃可能性が高くない脅威・脆弱性情報

※2.周知情報：

注意すべきセキュリティニュースなど動向として認識すべき情報

※3.重大情報：

自動車への関連性があり、かつ影響度・攻撃可能性が高い脅威・脆弱性情報

2. SOC アンケートのご意見に対する回答と対応案

2023 年度に SOC が配信する各種情報について、その利用状況、必要性妥当性に関する会員の皆様の意見を把握し、今後の SOC 運営の方針検討に活かすためにアンケートを実施させて頂きました。
ご協力を頂きました皆様にはあらためてお礼を申し上げます。

その際に各情報提供ベンダー様に対する意見も頂きました。付きましては、各情報提供ベンダー様よりご意見に対する回答及び対応案を頂きました。下記に記載させて頂きます。内容の確認を宜しくお願いします。

1）脅威・脆弱性情報提供ベンダーA 社様：

表１．ご意見と A 社様の回答＆対応案

No	配信元ベンダーのA社様へのご意見	A社様のご回答&対応案
1	いつもお世話になっております。さらに良くするには、 ・エクセルリストの記入内容を充実していただけると助かります。PDFの内容のほうが詳しく、こちらをコピーせざるを得ず、情報を1枚のエクセルに集約するのにかかる時間を節約できると嬉しいです。 ・PDF文章をコピーしようとすると、字と字の間にスペースができたり、変なところで改行されたりで扱いにくいです。各社個別のエクセルリストではなく、「目次」の項目アップデート版に3社分の情報が漏れなく載るようになるとそのまま一覧リストにできるので、助かります。⇒PDFはエクセルを見る前にさっと見て案件をつかむということなら、今のままでいいと思います。	・リストは週次レポート案件の概要を記載しております。詳細の確認は、PDFファイルでお願いしたいと思いますので宜しくお願いします。 ・PDFからコピーでなく、ServiceNowの記事からコピー頂くと書式が崩れずにご利用頂けます。
2	アナリスト説明会への参加は、プラチナ会員以上である必要がある認識です。しかし、アナリスト説明会でお話しいただく内容は、基本的に脅威・脆弱性情報として週単位？月単位でレポートを格納いただいていると思ってます。アナリスト説明会への参加ができない企業さんに対しても、情報としては共有しても良いのかなと思いまして、アナリスト説明会用に資料を作成いただくのではなく、脅威・脆弱性情報として公開いただいている資料を使ってアナリスト説明会で説明いただくことはできますでしょうか？	弊社は、週単位で提供しているレポートの中から月次レポートを作成し、そのレポートをアナリスト説明会の資料とさせて頂いています。
3	各記事の文章での説明はわかりやすく展開する前の解釈に役立っている。たまに、ソースを調べないと不明な文面があった。	分かりやすい（ソースを見なくても概略は理解できる）文章を検討します。
4	セキュリティ専門の担当者ではないこともあるので、もう少しわかりやすく且つ詳細に内容を記載していただきたい。	セキュリティ用語について詳細用語をつけていますが、不足しているとのご意見と捉え、更に語句追加できないか検討します。 <対応案> セキュリティ用語一覧の作成も検討します。
5	マンスリーレポートの頻度を上げて頂きたい。 解説が少ないように感じます。車載製品に関する情報も少ないように思います。レポートのフォームも読みにくく感じます。	・マンスリーレポートの頻度についてはSOC様と調整中です。 ・解説、レポートフォームは、具体的な御指摘をインタビューさせて頂きたいと考えております。 【SOCコメント】費用の関係もあり、頻度を上げることは難しいことをご理解頂ければと思います。 今後、速報の運用改善に関して検討を進めます。
6	・車両に係わる脆弱性をさらに絞ってほしい	さらに絞るためには各社様の製品構成情報等の機密情報が必要であると考えています。J-Auto-ISACでは、現状各社様の機密情報は扱わない方針となっております。よって、絞り込みは各社様にて実施して頂けます様宜しくお願いします。
7	記事の掲載順で、一般／周知情報に属するようなものは最後にして欲しい。脅威・脆弱性情報より先に載せる必要は無い	現在は、検出日の古い順でレポート掲載しています。脅威・脆弱性の先に載せることを検討します。
8	情報は大変役立っております。下記情報ありますと良いかと思います。 ・サイバー攻撃のメカニズム分析、対策分析にもう一歩踏み込んでいただきたいです ・自動車に対する攻撃ツールの出所、関わっている犯罪者などの詳細な情報があると良いです	・サイバー攻撃のメカニズムについては、具体的なことが書かれていないことが多い、また対策分析については設計情報も含む思うので踏み込むのは困難と推定しています。 ・攻撃ツールの出所、犯罪者の情報などは、もう少し詳細に掲載可能か検討します。

2）脅威・脆弱性情報提供ベンダーB 社様：

表２．ご意見と B 社様の回答＆対応案

配信元ベンダーのB社様へのご意見	B社様のご回答＆対応案
いつもお世話になっております。さらに良くするには、 ・もう少し詳しく記載していただけると助かります。チェックレベルでも原文を見ないと分からないことがあるので。	・週次定期レポートの参考ページ（特に公知脆弱性）に関するものと理解しました。 ・真に影響があると考えられるものはダイジェストで詳細化していること、平均して一週20～30件の情報を掲載しているためその全てを詳細化することは難しいことをご理解いただけますと幸いです。
以下の詳細が知りたい レポートする対象情報の選抜ロジック 情報の収集先	・週次定期レポートに対するコメントと理解しました。 ・まず、概要レベルであれば週次定期レポートの末尾の「（参考）今週のダイジェスト監視件数について」と「（参考）脆弱性・脅威情報レベル分けの考え方」に記載してますので、ご確認いただけますと幸いです。 ・その上で、詳細全体に関しては弊社ノウハウとなるためご回答が難しいところがございますが、背景情報をいただいた上で具体的な特定の箇所のご質問であれば回答可能な部分もありますので、それらの点をご連絡いただけますと幸いです。
レポートのヘッダータイトルが、同じもの（今週のダイジェスト）が続くためか、メリハリがなく読むポイントがつかみにくい。ページレイアウトの工夫が欲しい。	<対応案> SOCと改善の検討を進めます。
週次情報レポートと定期配信レポートのファイル名を、以前の様に分けて添付してください。 *現在は、同ファイル名になっています。	<SOCコメント> 改善の検討を進めます。
両社の良いとこ取りでフォーマットを統一してもらえると嬉しい	<SOCコメント> 改善の検討を進めます。
セキュリティ専門の担当者ではないこともあるので、もう少しわかりやすく且つ詳細に内容を記載していただきたい。	レポート作成時に出来るだけ考慮します。
マンスリーレポートの頻度を上げて頂きたい。	<SOCコメント> 費用の関係もあり、頻度を上げることは難しいことをご理解頂ければと思います。 今後、速報の運用改善に関して検討を進めます。
・脆弱性の対象製品、対応状況も記載するようにしてほしい。 ・車両に係わる脆弱性をさらに絞ってほしい	・週次定期レポートの参考ページ（特に公知脆弱性）に関するものと理解しました。 ・真に影響があると考えられるものはダイジェストで詳細化していること、平均して一週20～30件の情報を掲載しているためその全てを詳細化することは難しいことをご理解いただけますと幸いです ・週次定期レポートの参考ページ（特に公知脆弱性）に対するコメントと理解しました。 ・脆弱性の絞り込みですが、脆弱性を含む製品を使用していると想定される車載製品の"分類"の項目を追加させていただき、自社の製品に応じた取捨選択できるようにさせていただければと思います。（対応時期は別途SOC様と調整させていただきます。）
情報は大変役立っております。下記情報ありますと良いかと思います。 ・サイバー攻撃のメカニズム分析、対策分析にもう一歩踏み込んでいただきたいです ・自動車に対する攻撃ツールの出所、関わっている犯罪者などの詳細な情報があると良いです	・月次定期レポートに対するコメントと理解しました。 ・現在も記載させていただいてる認識ですが、可能な範囲でより詳細化を検討します。（ただし、公開情報から取得しているため、難しい点もあることをご理解いただけますと幸いです。）
ベンダー間で配信されるファイル名の日付位置が異なるので可能であれば統一して頂けると助かります。 ①週次レポート＋日付 ②日付＋週次レポート	<SOCコメント> 改善の検討を進めます。
レポート作成時に脆弱性情報とCVEの各情報(CVSS値 / AV / AC等)を見やすく対応付けて欲しい。社内での情報共有の際に概要の説明がしにくい。	・週次定期レポートの参考ページ（特に公知脆弱性）に関するものと理解しました。 ・真に影響があると考えられるものはダイジェストで詳細化していること、平均して一週20～30件の情報を掲載しているためその全てを詳細化することは難しいことをご理解いただけますと幸いです。

3）業界動向情報提供ベンダー：

表４．ご意見とベンダー様の回答＆対応案

No	配信元のベンダー様へのご意見	ベンダー様のご回答＆対応案
1	お世話になっております。さらに良くしていくためには、 ・自動車にどうかかわりがある情報なのかについてはもう少し詳しく記載してあると助かります。たとえば12月13日に配信された「EU、AI包括規制案で大筋合意 対応怠れば巨額制裁金」という記事は、自動車とどう関係があるのか書いてありませんでした。	SOCの活動スコープの中心は自動車業界に関するニュースですが、自動車や他業界のIoTやセキュリティに関するニュースを中心に配信しております。 他業界関連で取り上げているニュースに関しては、必ずしも自動車（車両）固有のものではないため関連性にについて記載することはできません。
2	業界動向の情報に関して、もう少し詳細な情報も加えていただけるとありがたいです。	Weekly配信は速報の位置づけのため詳細な情報を記載しておりません。 Monthly配信において詳細な情報や、続報を取り上げますのでご確認ください。
3	統計的な情報もあると嬉しい。 例：自動車へのサイバー攻撃件数の推移（増加傾向とか、ターゲットの傾向、攻撃手法の傾向　等）	自動車へのサイバー攻撃件数等の統計情報については配信する予定はございません
4	もっと頻繁に情報の配信を実施していただきたい。	<SOCコメント> 費用の関係もあり、頻度をすぐに上げることは難しいことをご理解頂ければと思います。 今後の検討課題とさせて頂きたいと思います。
5	海外の情報がもう少しあってもよいかと思います。	2024年度にSOCで監視ソースの希望に関するアンケートを実施するため、その際に監視してほしい海外サイト・キーワードをご提供ください。
6	記事への関連情報などの付随情報があれば記載願いたい	Weekly配信は速報の位置づけのため詳細な情報を記載しておりません。 Monthly配信において詳細な情報や、続報を取り上げますのでご確認ください。
7	他業界情報について、自動車の法規や電波認証への影響など、自動車業界(製品)への影響も示してもらえると有難い。	サイバーセキュリティと自動車に関する法規については収集・配信いたしますが、セキュリティ以外も含む自動車全般の法規動向については、SOCの活動スコープから外れるため配信する予定はありません。

尚、今回頂きましたご意見に関しては、対応をさらに検討して可能な範囲で対応させて頂きます。
貴重な意見を頂きどうもありがとうございました。引き続きご支援を宜しくお願いします。

以上

一般社団法人 Japan Automotive ISAC

〒108-6028 東京都港区港南 2-15-1 品川インターシティ A 棟 28 階

e-mail：info@j-auto-isac.or.jp

https://j-auto-isac.or.jp/