中小企業が多い

自動車産業におけるセキュリティ向上活動

一般社団法人
日本自動車部品工業会

IT対応委員会　サイバーセキュリティ部会
部会長　後藤 俊二郎

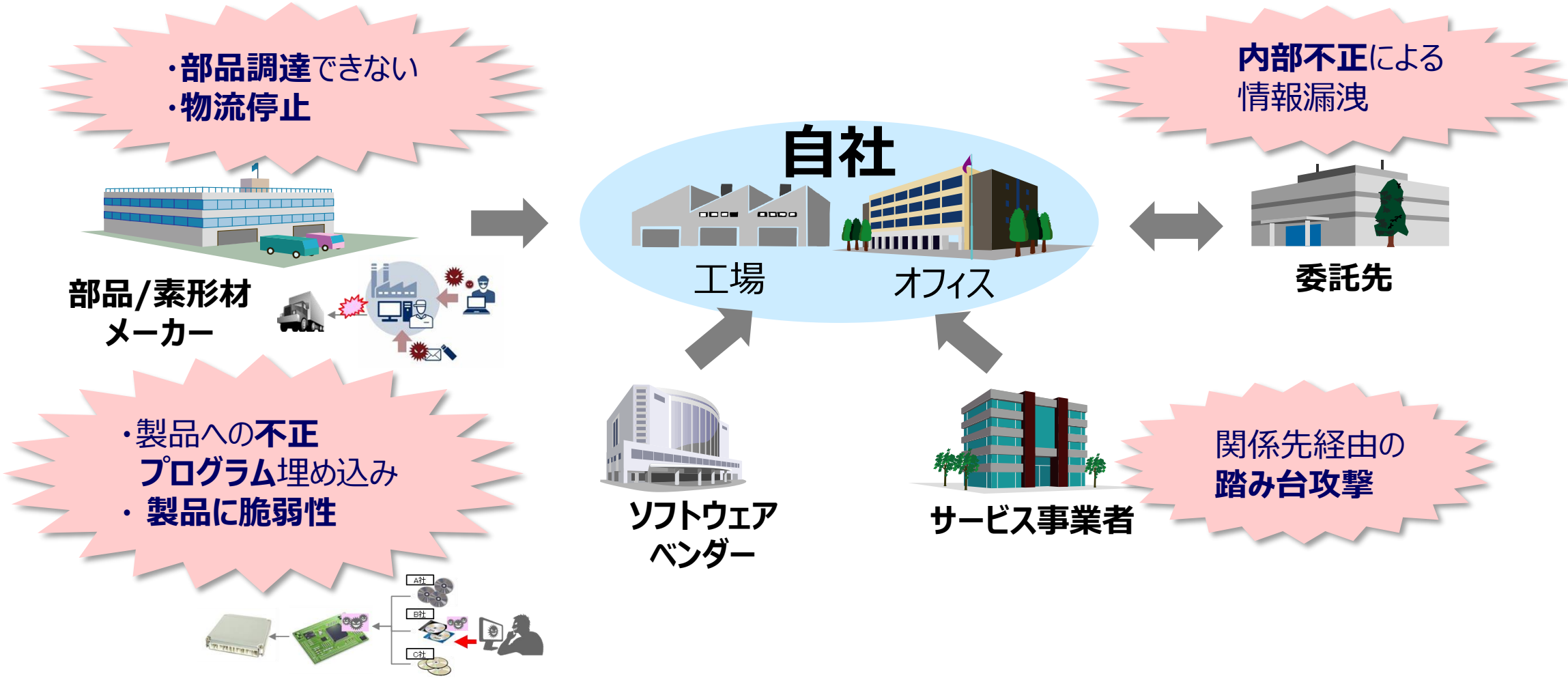
2024年2月

目次

※ 自動車産業サイバーセキュリティガイドラインを、以下のページでは単に【ガイドライン】と記します。

活動の発端：サプライチェーンリスクの増大

自社だけを守っているのでは不十分　　業務で関連する会社のリスク管理が必要



活動の発端：経産省・産業界 連携の動向

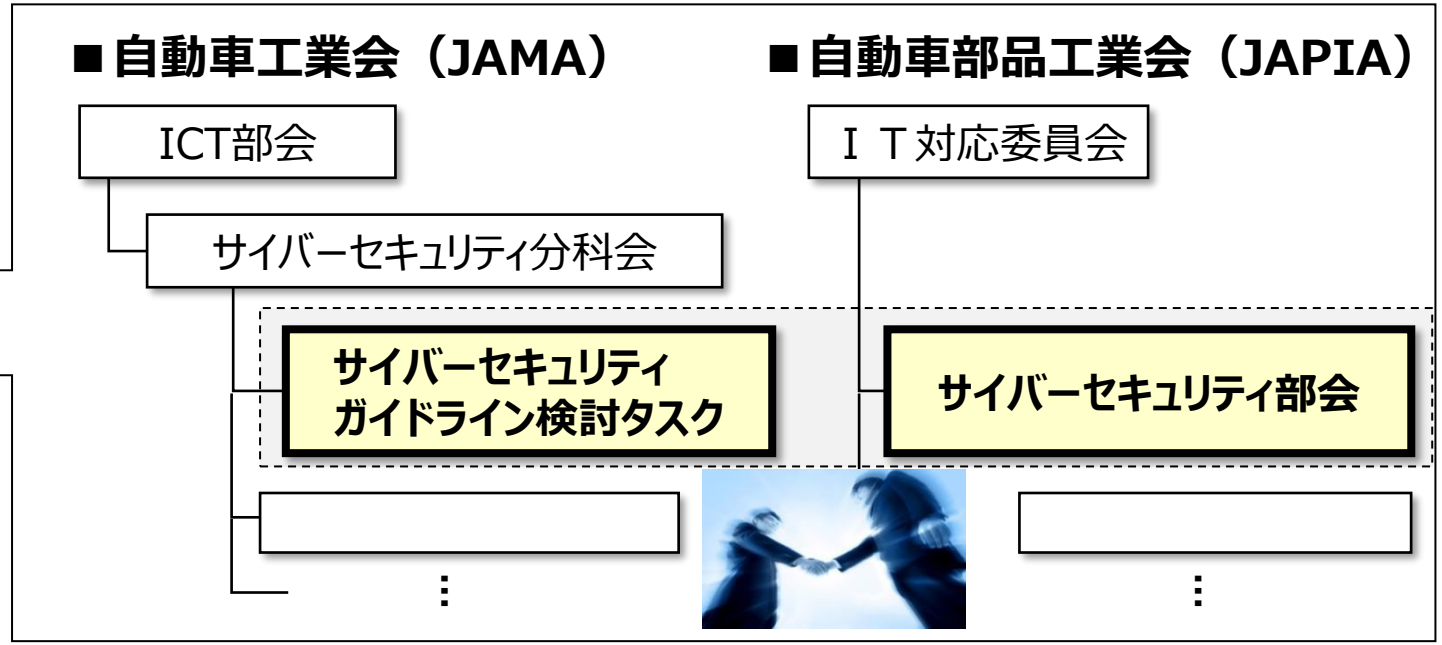
経産省CPSF(2019年発表）をベースに、自動車産業用のガイドライン策定を検討開始

＜標準モデル＞ 出典：経産省殿「産業分野におけるサイバーセキュリティ政策」資料

経済産業省:サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

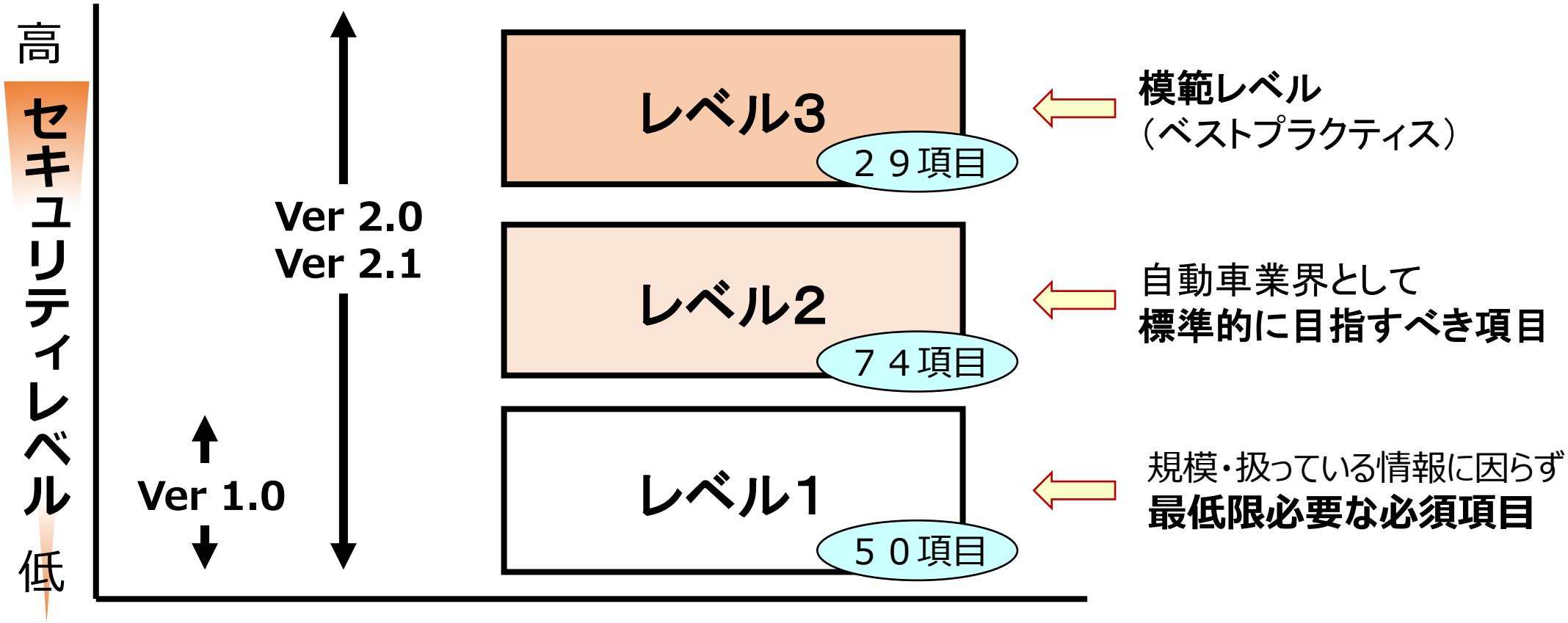
Industry by Industryで検討

自動車工業会（JAMA）・自動車部品工業会（JAPIA）が2019年 連携



活動の経緯：2020年V1.0発行～2023年V2.1発行

① 中小企業が多い自動車産業**全体のレベルアップ**を優先、2020年に**必須項目（Ver 1.0）発行**
② 業界として**標準的に目指すレベルや模範レベル**を定義し、2022年に**レベルアップ版（Ver 2.0）を追加**
③ 自己評価結果の提出**システム化に伴う変更と文言修正**を行い、2023年に**修正版（Ver 2.1）発行**



目次

■活動の発端・活動の経緯

■自動車産業サイバーセキュリティガイドラインの紹介

■2023年度の活動概要

■IPA殿と連携したセキュリティ対策推進支援

※ 自動車産業サイバーセキュリティガイドラインを、以下のページでは単に【ガイドライン】と記します。

ガイドラインの紹介：公開している文書類

cyb_sec_guideline_V02.pdf

読み物的なPDF

JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.1 版

2023 年 9 月 1 日

Japan Automobile Manufacturers Association, Inc.　　Japan Auto Parts Industries Association

目次

cyb_sec_guideline_CS_v02.xlsx

Excelチェックシート

自動車産業 セキュリティチェックシート(レベルアップ版)　Ver1.9　ドラフト版

会社名	
会社分類	マプルダウンから選択ください
評価範囲	マプルダウンから選択ください
会社従業員数	マプルダウンから選択ください

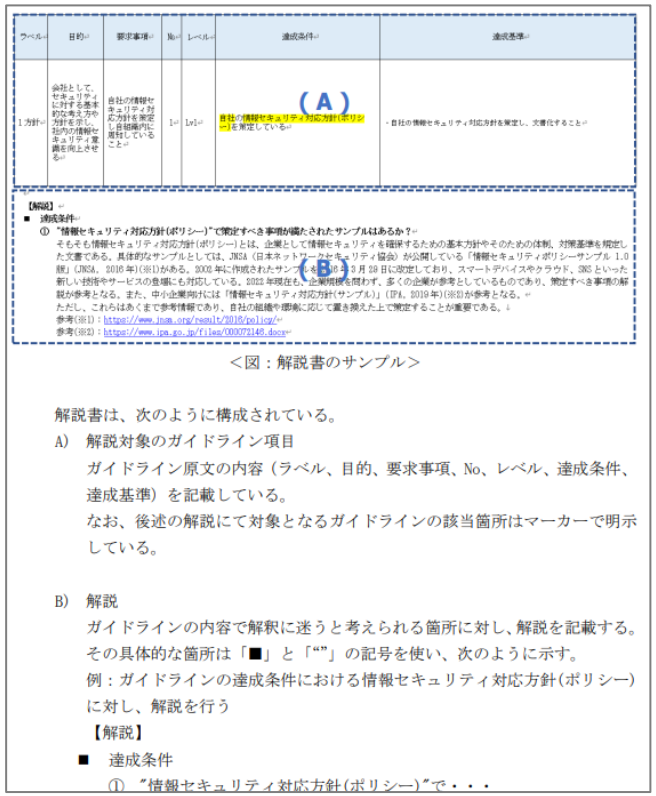
会社情報　分類　対象　担当者

入力

分類	ラベル	目的	要求事項	達成条件	達成基準	他社事例 (参考事例を列記しており、すべての遵守を求めているものではありません)	評価結果 達成条件評価
共通	2機密情報を扱うルール	機密情報を扱うルールを定め、社内へ周知することにより、機密漏えいを防止する	機密情報のセキュリティに関する社内ルールを規定していること	**業務で利用する情報機器の利用ルールを規定し、周知している(個人所有機器(BYOD)含む)**	【規則】 ・情報機器（PC、サーバ、通信機器、記憶媒体、スマートデバイス等）の利用ルールを策定し、この ルールには利用開始時、利用終了時の手続き、利用中の遵守・禁止事項、紛失時の手続きを含むこと ・情報機器の利用ルールを容易に確認できる状態にすること 【対象】 ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定期的に、かつ、ルールの改正時に周知すること	【情報機器の利用ルールの記載事項例】 ・BYODの許可もしくは禁止に関するルール ・社給スマートデバイスではApple Store等は使用禁止とし、業務アプリのみの利用とする 【周知の例】 ・情報機器の利用開始時に利用者に説明 ・役員、従業員、派遣社員等の新規受け入れ時 ・情報機器の利用ルールについて、従業員に年1回e-Learningを受講させている ・社内規則に情報機器を利用する際のルールを明記しており、常時閲覧可能な状態で社内イントラサイトに掲載している ・社内の共通電子申請システムで、情報機器の利用申請を行えるようにしている ・申請書類一式を社内のポータルサイトに掲載している	マプルダウンで評価ください
共通	6事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	**ウイルス感染時の対応手順を定めている**	【規則】 ・ウイルス感染時用の対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、②初動、③調査・対応、④復旧、⑤最終報告	【対応手順の例】 ・クライアントPCにおいて、ウイルス感染や不正アクセスの疑いがある場合、発見後ただちにネットワークから切り離した後に、情報セキュリティ事件・事故時の報告窓口へ連絡する手順書を定義	マプルダウンで評価ください
共通	6事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	**ウイルス感染時の対応手順は、定期的に確認され、必要に応じて、改定していること**	【規則】 ・世間動向や攻撃のトレンドなどをふまえ、教育・訓練内容の見直しをすること 【頻度】 ・1回/年以上	（同上）	マプルダウンで評価ください
共通	7日常の教育	コンピュータウイルスや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意すべきことを教育していること	**標的型メール訓練を実施している**	【規則】 ・標的型メール訓練を実施すること ・万が一開封した時の対応も訓練内容に含めること ・訓練内容や方法を振返り、次回の訓練を改善すること 【対象】 ・電子メールの利用者 【頻度】	【訓練の内容】 ・標的型メールやBEC想定のメールを訓練対象に送る ・経営者向け不審メール訓練を実施している 【訓練項目】 ・メールの例題 ・メール内リンクへのクリック ・リンク先サイトへの情報入力 ・添付ファイルの開封有無 ・社内ヘルプデスクオペレーターのエスカレーション 【訓練後のフォロー】 ・結果および振返りはトップ報告し、次年度の訓練に改善点を反映して	マプルダウンで評価ください

cyb_sec_guideline_manual_v02_01.pdf

解説書



ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
1 方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる。	自社の情報セキュリティ対応方針を策定し、自組織内に周知していること。	1-1	Lv1	(A) 自社の情報セキュリティ対応方針(ポリシー)を策定している。	・自社の情報セキュリティ対応方針を策定し、文書化すること。

【解説】
■ 達成条件
① "情報セキュリティ対応方針(ポリシー)"で策定すべき事項が織たされたサンプルはあるか？
そもそも情報セキュリティ対応方針(ポリシー)とは、企業として情報セキュリティを確保するための基本方針やそのための体制、対策基準を規定した文書である。具体的なサンプルとしては、JNSA（日本ネットワークセキュリティ協会）が公開している「情報セキュリティポリシーサンプル 1.0 版」(JNSA, 2016 年)(※1)がある。2000 年に作成されたサンプルを(B) 3 月 28 日に改定しており、スマートデバイスやクラウド、SNS といった新しい技術やサービスの登場にも対応している。2022 年現在も、企業規模を問わず、多くの企業が参考としているものであり、策定すべき事項の解説が参考となる。また、中小企業向けには「情報セキュリティ対応方針(サンプル)」(IPA, 2019 年)(※2)が参考となる。
ただし、これらはあくまで参考情報であり、自社の組織や環境に応じて置き換えた上で策定することが重要である。
参考(※1)：https://www.jnsa.org/result/2016/policy/
参考(※2)：https://www.ipa.go.jp/files/000072148.docx

＜図：解説書のサンプル＞

解説書は、次のように構成されている。

A) 解説対象のガイドライン項目
ガイドライン原文の内容（ラベル、目的、要求事項、No、レベル、達成条件、達成基準）を記載している。
なお、後述の解説にて対象となるガイドラインの該当箇所はマーカーで明示している。

B) 解説
ガイドラインの内容で解釈に迷うと考えられる箇所に対し、解説を記載する。
その具体的な箇所は「■」と「"」の記号を使い、次のように示す。
例：ガイドラインの達成条件における情報セキュリティ対応方針(ポリシー)に対し、解説を行う

【解説】
■ 達成条件
① "情報セキュリティ対応方針(ポリシー)"で・・・

ガイドラインの紹介：Excel チェックシートの構成

■対策完了(2点)
■対策中(1点)
■未実施(0点)
■該当なし

達成条件・達成基準・他社事例に基づき自社を評価し記入（黄色部）

分類	ラベル	目的	要求事項	No.	レベル	達成条件	達成基準	他社事例	達成条件評価	評価の根拠
検知	マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	136	Lv1	パソコン・サーバには、**ウイルス対策ソフト**を導入している	【規則】 ・パソコン、サーバごとに導入 ・適切な範囲と頻度を規定 【対象】 ・NW接続している全端末	【実践例】 ・・・　略　・・・ 【ウイルス対策ソフトが導入できない場合の対応例】 ・・・　略　・・・	▽プルダウンで評価ください	
				138	Lv3	詳細な履歴取得および・・・**行動追跡システム**を導入している	【規則】 ・エンドポイント対策システムを導入すること 【対象】 ・会社支給のクライアントPC ・サーバー	【対策例】 ・EDR（Endpoint Detection and Response）で不審な振舞いをリアルタイム検知・対処をしている ・・・	▽プルダウンで評価ください	
				139	Lv2	・・・、**メールゲートウェイでのマルウェアチェック**を実施している	【規則】 ・メールゲートウェイにマルウェアチェック機能を導入すること	【対策例】 ・外部メールサービスの経路上にマルウェアチェック機能を導入している ・社内にメールセキュリティシステムを導入している ・・・	▽プルダウンで評価ください	

ラベル数24

達成条件No.数153

ガイドライン要求事項一覧(1/4)

＜２４項目のラベル＞

分類	項番	ラベル	主な要求事項
共通	1	方針	自社の情報セキュリティ対応方針を策定し自組織内に周知していること
	2	機密情報ルール	機密情報の取扱いルールを規定し社内へ周知すること
	3	法令遵守	情報セキュリティに関する法令を考慮し、社内ルールを策定すること (法令例：個人情報保護法、不正競争防止法)
	4	体制（平時）	平時の情報セキュリティ対応体制を整備し、 事故発生に至らないよう、情報収集と共有を行うこと
	5	体制（事故時）	情報セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること
	6	事故時の手順	情報セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること
	7	日常の教育	従業員として注意することを教育していること
			情報セキュリティ事件・事故の発生と影響を抑制する教育・訓練を行っていること

ガイドライン要求事項一覧(2/4)

分類	項番	ラベル	要求事項
特定	8	他社との 情報セキュリティ要件	サプライチェーン上で発生する情報セキュリティ要件が明確になっていること
	9	アクセス権	アクセス権(入室権限やシステムのアクセス権)を、適切に管理していること
	１０	情報資産の管理 (情報)	情報資産の機密区分を設定・把握し、その機密区分に応じて情報を管理していること
	１１	情報資産の管理 (機器)	会社が保有する情報機器及び機器を構成するOSやソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を 適切に管理していること
	１２	リスク対応	自組織内(自組織の業務：業務委託も含めて)の情報セキュリティリスクに対する対策を行っていること
	１３	取引内容・ 手段の把握	取引先毎に、取引で取り交わされる情報資産と、取引に利用している手段を把握していること
	１４	外部への 接続状況の把握	外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること
	１５	社内接続ルール	社内ネットワークへの接続時には、情報システム・情報機器の 不正利用を抑制する対策を行っていること

ガイドライン要求事項一覧(3/4)

分類	項番	ラベル	要求事項
防御	１６	物理セキュリティ	サーバー等の設置エリアには、物理的セキュリティ対策を行っていること
	１７	通信制御	インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限していること
	１８	認証・認可	情報システム・情報機器への認証・認可の対策を行っていること
	１９	パッチや アップデート適用	公開されている脆弱性に対する対策を行っていること サポート期限が切れたOS、ソフトウェアを利用しないようにしていること
	２０	データ保護	情報機器、情報システムのデータを適切に暗号化していること
	２１	オフィスツール関連	メール送信による情報漏えいを防止するための対策を実施していること（上司CC等）

ガイドライン要求事項一覧(4/4)

分類	項番	ラベル	要求事項
検知	２２	マルウェア対策	セキュリティ上の異常を素早く検知するウイルス対策を行っていること
	２３	不正アクセスの検知	通信内容を常時監視し、不正アクセスや不正侵入をリアルタイムで検知/遮断および通知する仕組みを導入していること
対応 復旧	２４	バックアップ・ 復元(リストア)	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること （ランサムウエア等に暗号化されないバックアップ）

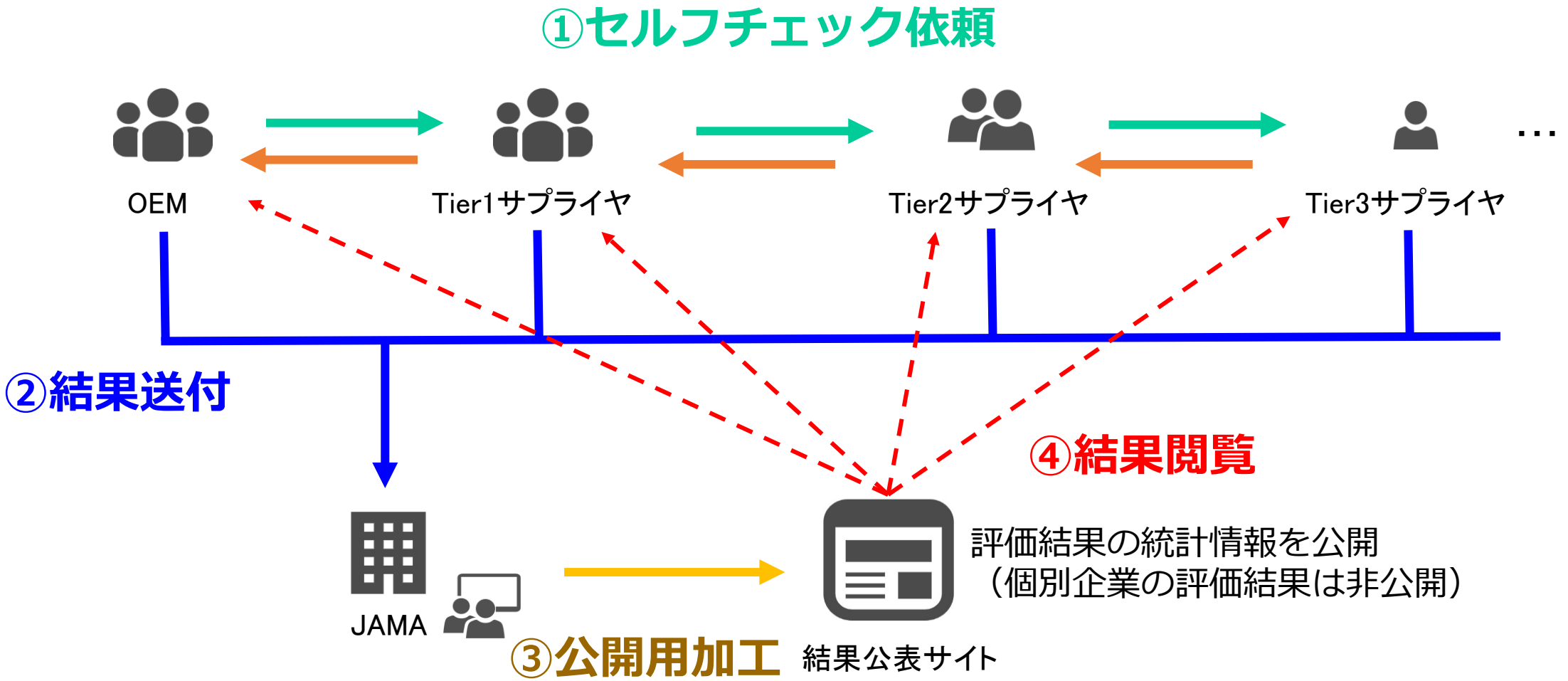
自動車産業ガイド セキュリティ対策マップ

Ver1.0（必須項目）　Ver2.1（追加項目）

	特定（＋共通）		防御			検知	対応・復旧		
技術対策	ガイドライン制定・監査（体制・ルール・啓蒙）	脅威情報収集・分析	メールゲートウェイ	ウェブゲートウェイ	ウイルス対策 多要素認証	セキュリティ監視（SOC）	行動追跡・一時対処 専門家による解析	バックアップ（ランサム対策）	
日常運営	ルール整備/徹底	資産把握・管理	経営層・従業員の教育	通信先精査・棚卸	サポート切れOS対応 セキュリティパッチ適用	対応体制整備（初動対応）	対応体制整備（調査・復旧）	サイバーBCP（生産継続手段）	

チェックシートの展開と回収

お願いレター(チェックシートの入手方法、結果送付方法を含む)を準備し 取引関係を軸に展開



2022年度の自己評価結果紹介（全体サマリ）

21年度→22年度で有効回答総数が増加すると共に レベル１項目の平均点は77%へ向上

年度	回答総数	有効回答総数	平均点
2021	2,300 社	2,296 社	70.97 /100 点 (71.0%)
2022	4,026 社	3,961 社	下表のとおり

（2021 年度は V1.0 のため、レベル 1 項目のみ）

目標レベル	会社数	平均点			
		レベル 1 項目	レベル 2 項目	レベル 3 項目	総合
レベル1	679 社	60.18 /100 点 (60.2%)	－	－	60.18 /100 点 (60.2%)
レベル2	2,166 社	78.14 /100 点 (78.1%)	106.25 /148 点 (71.8%)	－	184.39 /248 点 (74.4%)
レベル3	1,116 社	84.83 /100 点 (84.8%)	118.73 /148 点 (80.2%)	37.35 /58 点 (64.4%)	240.91 /306 点 (78.8%)
	計	76.95 /100 点 (77.0%)	110.49 /148 点 (74.7%)	37.35 /58 点 (64.4%)	－

2022年度の自己評価結果紹介（会社規模毎の達成率）

大規模企業は総じてセキュリティ対策が進んでいる一方で、中小規模企業の底上げが課題

会社規模	目標レベル１		目標レベル2		目標レベル3	
	社数	平均点 (100点満点中)	社数	平均点 (248点満点中)	社数	平均点 (306点満点中)
10,000名超	2社	98.0点 (98.0%)	28社	240.4点 (96.9%)	85社	283.3点 (92.6%)
3,001-10,000名	7社	94.7点 (94.7%)	88社	229.0点 (92.4%)	121社	280.0点 (91.5%)
501-3,000名	45社	83.1点 (83.1%)	468社	213.8点 (86.2%)	307社	262.0点 (85.6%)
101-500名	209社	66.5点 (66.5%)	845社	186.3点 (75.1%)	345社	228.5点 (74.7%)
100名以下	392社	53.9点 (53.9%)	689社	155.0点 (62.5%)	203社	190.9点 (62.4%)

目次

■活動の発端・活動の経緯

■自動車産業サイバーセキュリティガイドラインの紹介

■2023年度の活動概要

■IPA殿と連携したセキュリティ対策推進支援

※ 自動車産業サイバーセキュリティガイドラインを、以下のページでは単に【ガイドライン】と記します。

2023年度（令和５年度）の活動概要

活動名		活動内容
業界活動	入力Webシステム構築	各社の評価結果を入力・保管・分析するWebシステムを構築し運用開始
	業界説明会	主催は業界団体（自工会/部工会）ながら、参加者は広く自動車業界全体に声掛け ガイドラインによる自己評価を依頼する説明会を３回実施
	よろず相談会	中小企業のリアルな実態の把握と実態に則した提案を双方向で行う目的で、 上記説明会から提出期限の間（10～12月）に 全５回実施
	部工会Webセミナー	特に中小企業のセキュリティに対する意識と知識の向上を狙って年４回開催
個社活動	自己評価依頼	各社毎に選定した仕入先委託先にメール等で自己評価を依頼
	取引先の対策支援	会社によっては取引先の対策支援を実施 （達成見込み確認・対策計画収集・訪問現認・困りごと相談・対策支援・監査活動等）

自己評価を依頼した業界説明会の紹介（概要）

サイバーセキュリティの重要性・期待レベル明示・新システム説明・困り事ケアについて説明

アンケート結果：SCセキュリティ重要性/評価提出方法の理解度は95%以上

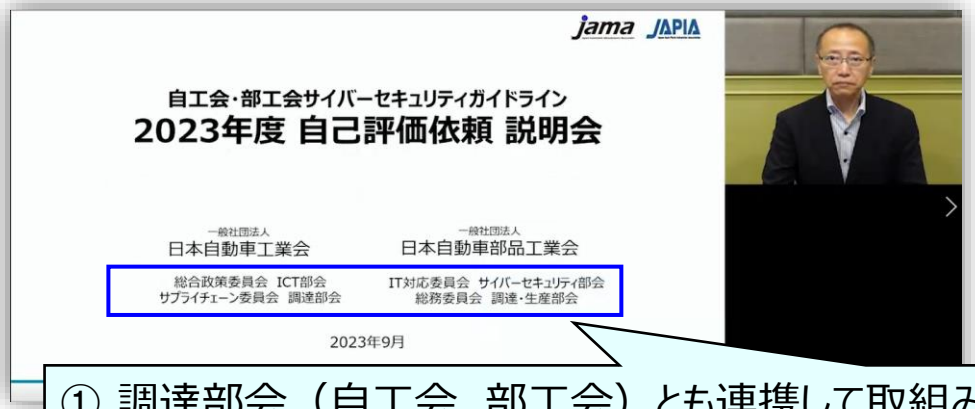
【説明会日程】

第1回	2023 年 09 月 01 日（金）	13:30-15:30	参加者　約2400人
第2回	2023 年 09 月 12 日（火）	10:00-12:00	参加者　約2300人
第3回	2023 年 10 月 10 日（火）	13:30-15:30	参加者　約1500人

【アジェンダ】

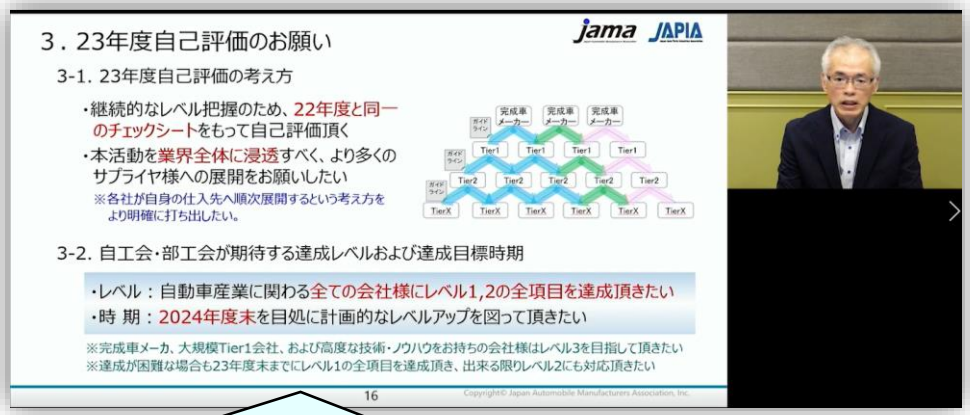
議事１	はじめに	実際のサイバー被害を素材に作ったドキュメント動画も上映して啓発
議事２	22年度自己評価のまとめ	
議事３	23年度自己評価のお願い	レベル1，2の全項目を2024年度末を目処に達成して欲しいという期待値を初めて提示
議事４	自己評価結果提出方法	新しい入力Webシステムの使い方
議事５	今後のセミナー開催スケジュール	よろず相談会（全5回）の予告 **セキュリティ推進上の困り事/悩み、解決の進め方を勉強し合う機会**
議事６	質疑応答	

自己評価を依頼した業界説明会の紹介（風景）



① 調達部会（自工会、部工会）とも連携して取組み

② 実インシデントをドラマ風に仕立てた啓発動画も好評



③ 自社自己評価に加えて商流での広い展開を依頼
自工会部工会が期待する達成レベルも伝えた

④ 約45分間の質疑応答時間を使い切る程 多くの質問を頂いた

よろず相談会の紹介（概要）

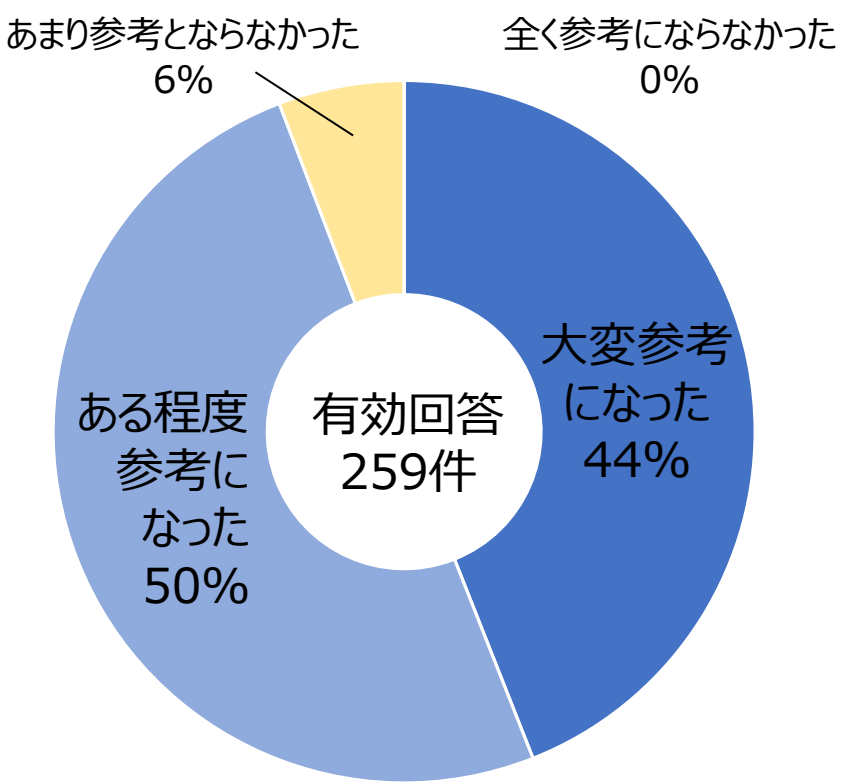
- **中小企業の困り事を少しでも解消**するために、年度途中で実施することを決め、**５回実施**
- 双方向で会話できるように**参加者数は抽選で100名以下**に絞り込み
- 相談会で使った資料と相談会内容を反映したFAQを後日JAMAホームページに掲載

日程	テーマ	参加者数	回答担当	質問のキーワード抜粋 **赤字：特に中小企業に顕著な内容**
23/10/20	ルール・体制	約70名	ホンダ・アイシン スズキ・デンソー	規程作成方法・**専任者不在・必要工数・簡易的方法** 等
23/11/01	技術対策	約80名	ダイハツ・デンソー スバル・三菱	メール訓練・監視＆検知・必要な製品と**価格・コスト感** 等
23/11/17	評価の進め方	約90名	日産・三菱 トヨタ・ホンダ	評価判断レベル・根拠記入欄の書き方・**短期間達成困難** 等
23/12/01	ルール・体制	約70名	トヨタ・マツダ 日産・アステモ	主管部署と体制・社内浸透方法・参考サンプルや事例 等
23/12/15	技術対策	約70名	マツダ・アステモ ダイハツ・アイシン	PC管理＆監視体制・ログの取得と保管・**優先項目** 等

よろず相談会の紹介（事後アンケート結果）

94%が「参考になった」と回答。一方で「現実的には中小企業には難しい」といった声もあった

《参考度》



《自由意見》

記載された125意見を生成AIで要約した結果

肯定的意見

- 他社の事例が参考になった
- 双方向で発信する形式がよかった
- お助け隊やIPAの情報が貴重だった
- 今後も参加したい
- 評価点の付け方の基準が確認できた

不満：理想と現実の差を改めて感じた
中小企業に適した進め方提示が足りていない気がする
自社にそのまま適用できる具体例や事例が足りない

要望：セキュリティ**レベルに応じたクラス分け**
参加者同士の交流や情報共有
業界全体でのセキュリティ**対策の仕組み**

目次

※ 自動車産業サイバーセキュリティガイドラインを、以下のページでは単に【ガイドライン】と記します。

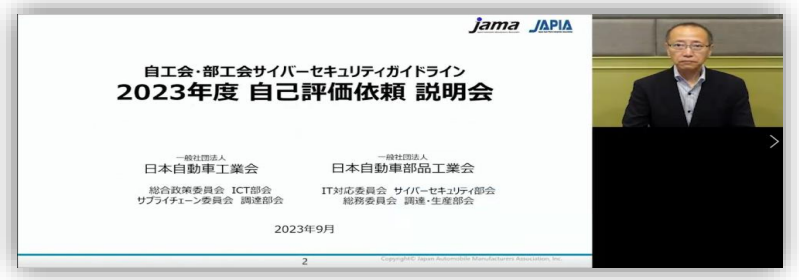
中小企業のレベルアップ活動方針

解説書・セミナー・よろず相談会で公的活動を最大限活用することを促していく

JAMA/JAPIA活動

ガイドライン 本体と解説書

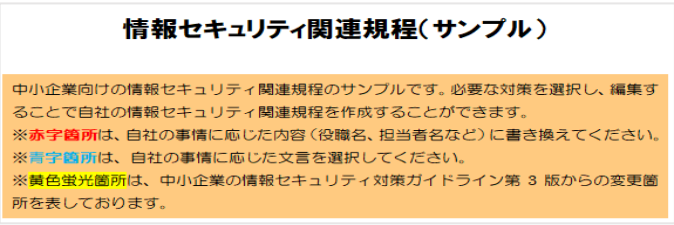
説明会/よろず相談会/セミナー



公的活動（主に経産省＆IPA）

対策手順

規程
ひな形



啓蒙動画

お助け隊

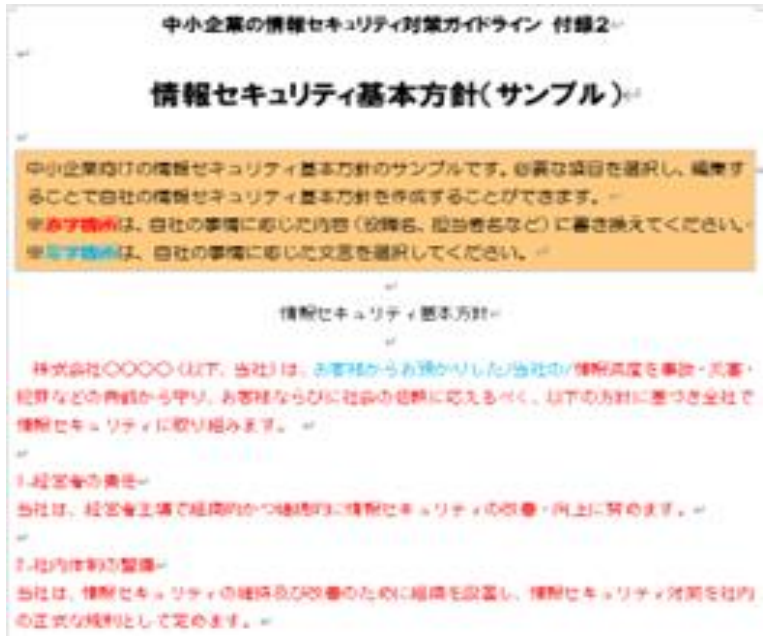
よろず相談会での質問＆回答例①

質問④　23年12月1日 よろず相談会より

規程類は、どの程度のものを作成する必要があるのでしょうか？　サンプルサイトがあれば、ご紹介いただけないでしょうか？

回答：
IPAの「中小企業の情報セキュリティ対策ガイドライン」に、規程のサンプルがありますので活用ください。

また自工会/部工会・サイバーセキュリティガイドラインV2.1解説書（日本語版）にも、記載がありますので、ご活用ください。



中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
[選択肢]は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
[記入例]は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社○○○○（以下、当社）は、お客様からお預かりした当社の情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
6 事故時の手順	情報セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること	24	Lv1	情報セキュリティ事件・事故時の対応手順（初動、システム復旧等）を定めている	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動、③調査・対応、④復旧、⑤最終報告

【解説】

■ **達成条件**

① **“情報セキュリティ事件・事故時の対応手順”にはどのような内容が盛り込まれていればよいか？**

情報セキュリティ事件・事故（マルウェア感染などのサイバー攻撃も含む）の発生時にとるべき対応として、次のような内容が必要に応じて盛り込まれていればよい。（以下例示）

- インシデント報告窓口が設けられて、周知されている
- 発生したインシデントの内容をどこまで情報共有すべきかの判断基準が決められている
- 過去に経験したインシデントを記録し、同じインシデントが発生した際に参照できるようになっている
- 誰に、どの範囲で、どういった手段で告知するか判断する手順が含まれている
- 抑制措置の手段と意思決定者が決められている
- 復旧後にモニタリングする手順が含まれている
- 再発防止策を講じる旨が記載されている

よろず相談会での質問＆回答例②

質問⑬　23年12月15日 よろず相談会より

使えるお金も人員も限られている中、どこからどのように手を付けたらよいのかわからないので、アドバイスいただきたい。

回答：　自工会・部工会としては自動車産業のサプライチェーンに参加される全ての会社様に、その企業規模を問わず、レベル２までの全項目を達成頂くことを希望しております。但し、人員規模・予算上等の問題でそれが困難な会社様におかれましては、**少なくとも23年度中にレベル1の全50項目の達成をお願いしたい**と考えております。その上でレベル２の項目に関しても24年度末に向け、可能な項目から計画的に達成頂ければと存じます。

IPAの対策ガイドライン・規程サンプルを参考にしたり、お助け隊サービスを活用する等も検討頂くと良いと考えます。

24年度末までにレベル２を全件達成することは困難であっても、**出来るところから少しずつでも実行頂くことにより、確実にセキュリティレベルは向上**してまいりますので、よろしくお願い致します。

参考：中小企業の情報セキュリティ対策ガイドライン | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
サイバーセキュリティお助け隊サービス ユーザー向けサイト | IPA

IPA殿による業界活動支援（業界団体向け対策ツール整備）

業界ガイドラインを補完する目的でIPA対策ガイドラインをリファレンスツールとして活用

業界団体
JAMA/JAPIA

中小企業 …

評価（対策事項を明確化）

対策（具体的な方法提供）

業界ガイドライン Lv1(50項目)と
IPA対策ガイドラインを突合

不足点は**付録５**のサンプル規程に追加し、「**自動車産業向けサンプル規程**」を作成

サイバーセキュリティ
セキュリティ対策 S お助け隊
支援制度

IPA殿による業界活動支援（ガイドライン適用マネジメント指導）

実際の中小企業（４社）を選定しガイドライン適用を支援する（23年12月～24年2月）

自動車産業

業界団体
JAMA/JAPIA

中小企業 …

セキュリティ専門家
（情報処理安全確保支援士等）

サイバーセキュリティ
セキュリティ対策 SC お助け隊
支援制度

付録3 5分でできる！情報セキュリティ自社診断

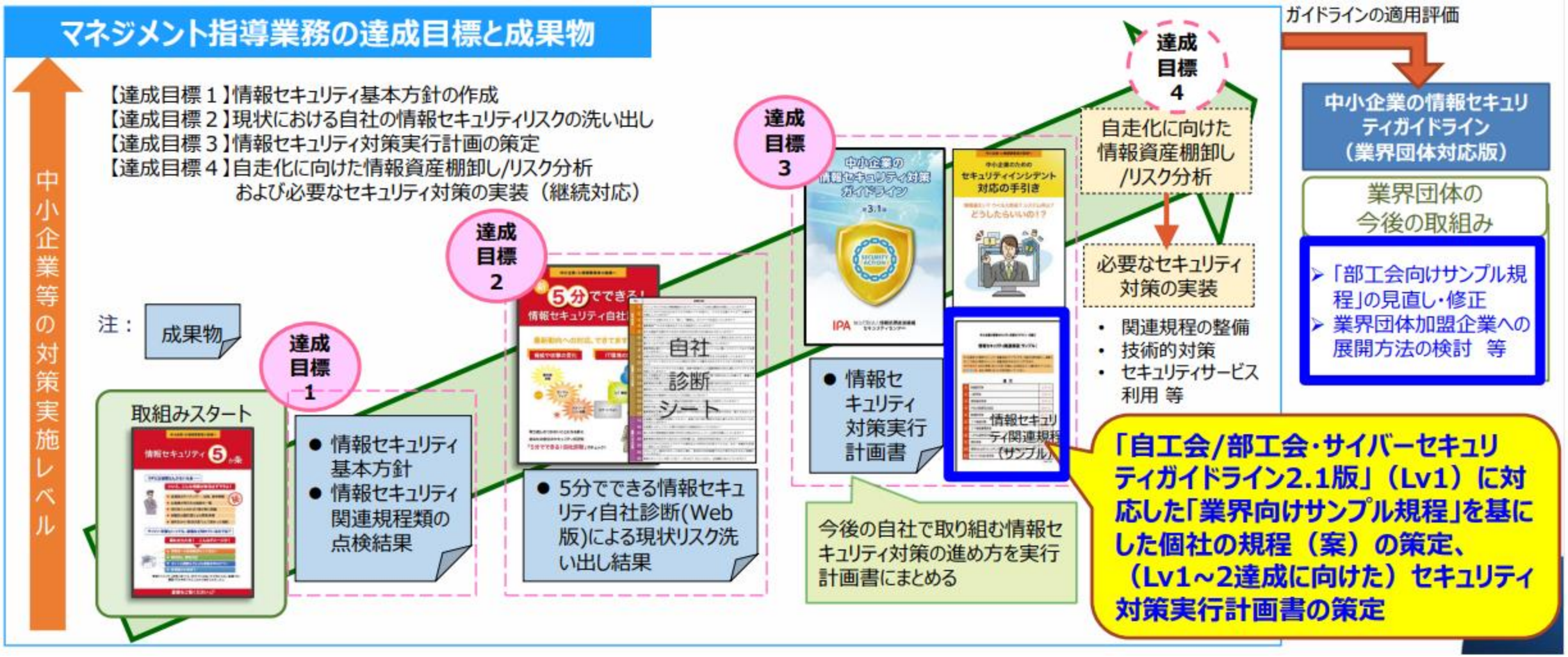
付録5_情報セキュリティ関連規程（サンプル）

付録8_中小企業のためのセキュリティインシデント対応の手引き

中小企業の情報セキュリティ対策ガイドライン第3.1版

情報セキュリティ関連規程の整備
情報資産の洗い出しとリスク分析
対策導入計画策定の支援

ガイドライン適用のマネジメント指導の実施イメージ



IPAマネジメント指導実施結果（速報レベル）

- 自社の**セキュリティ規程が未整備の場合、「自動車産業向けサンプル規程」がそのまま活用可能**。サンプル規程を参照して、自社の規程の見直しを行うことも有効。また、ISO9001など既存のISOの取組みにセキュリティ対策を折り込むと効率的。
- **IT専任者がいない中小企業には、セキュリティ専門家によるマネジメント指導が有効**。例えば、複数工場の担当者が参加したマネジメント指導をOJT的に行い、参加者が実施方法を自分の工場に持ち帰り、横展開する取組みも見受けられた。

企業名	A社	B社	C社	D社
所在地	三重県伊賀市	愛知県名古屋市	岐阜県関市	愛知県犬山市
業種	軸受部品製造	メッキ加工	プレス加工	金属切削加工
業界ガイドライン適用評価＆活用ヒント	• サンプル規程を用いて、自社の**セキュリティ規程を新規に策定**。 • 組織的・人的・物理的対策を優先して実施。 • 技術情報管理は、**ISO 9001の文書管理に基づく対策が効率的**。	• サンプル規程を参照しながら、**既存の規程を見直し改定**。 • **ひとつの工場で規程を見直した後、他の場へ展開**を行う。 • 経営層を巻き込み、体制整備等管理面の対策を推進予定。	• サンプル規程を参照し、**セキュリティ規程を策定中**。 • **ISO 9001に準じ、教育の計画立案、実施手順を作成**。 • 情報資産に対するリスク評価が困難であったが、**マネジメント指導業務を通じて**支援。	• サンプル規程を用いて、自社の**セキュリティ規程を新規に策定**。 • **マネジメント指導業務を通じて**、情報資産のライフサイクルを通じた管理、委託先選定ルール策定、緊急連絡体制等を整備。

今後とも、経産省殿・IPA殿と連携し
業界のセキュリティレベル向上を推進していきます

ご清聴ありがとうございました