2026年度 経営層＋担当者説明会

「自動車産業サイバーセキュリティガイドライン」
自己評価の実施･展開のお願い

一般社団法人
日本自動車工業会

総合政策委員会　ICT部会
サプライチェーン委員会　調達部会

一般社団法人
日本自動車部品工業会

DX対応委員会　サイバーセキュリティ部会
総務委員会　サプライチェーン部会

2026年９月、１０月

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

1-1. 本日の説明会について

✓ 本日は、昨今増加の一途を辿っているセキュリティ事故被害の世間動向をご確認していただき、
以下2点についてお願いする趣旨となります。

①「自動車産業サイバーセキュリティガイドライン」を活用した自社のセキュリティレベル把握と向上

②自社の取引先の巻き込み（サプライチェーン全体でのレベル向上）

✓ 本説明会では、実際の被害事例を基に、サプライチェーン全体でのレベル向上が重要であることを理解いただき、
経営層および担当者の皆様のセキュリティ対策に関する知識を深めていただくとともに、自動車産業
サイバーセキュリティガイドラインを使った**自己評価結果の提出方法**について説明いたします。

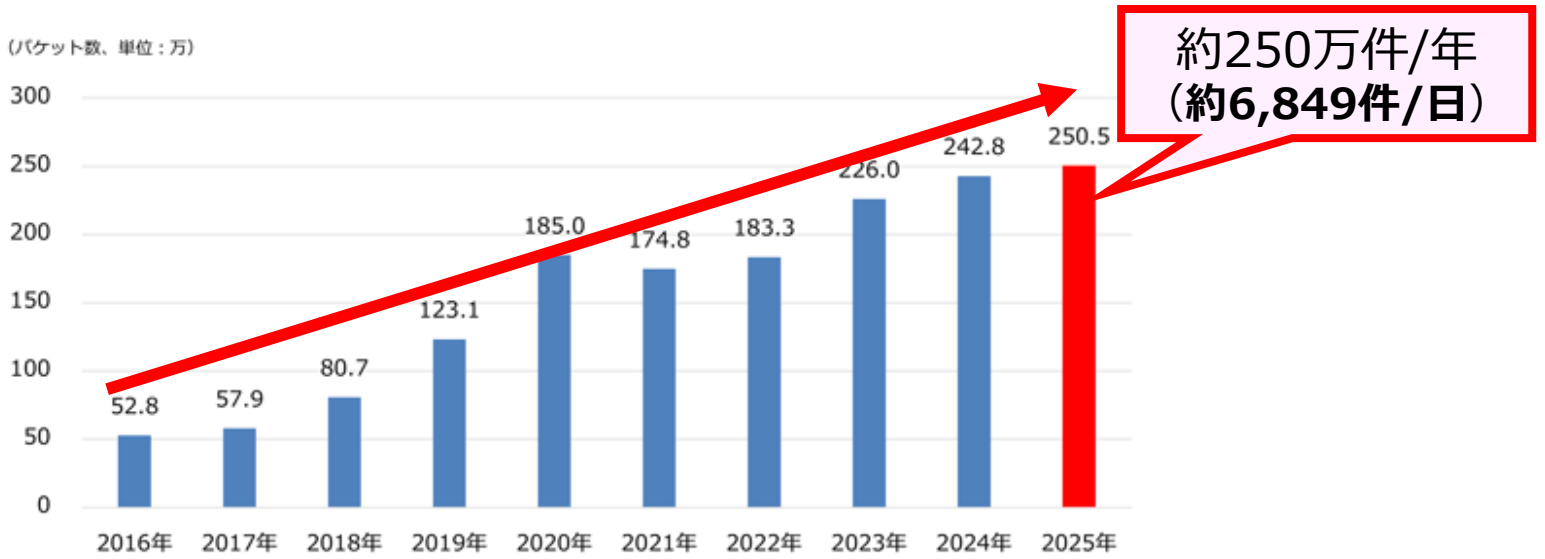
✓ 本説明会の中では、スペシャルコンテンツ*として、**中小企業のサイバー攻撃事例**もご紹介させていただきます。
＊本スペシャルコンテンツは、説明会参加者の方のみの特典となります。

✓ 本説明会が、本日ご参加頂いております各社様に、少しでもお役立て頂けますと幸いです。

1-2. 世の中の状況

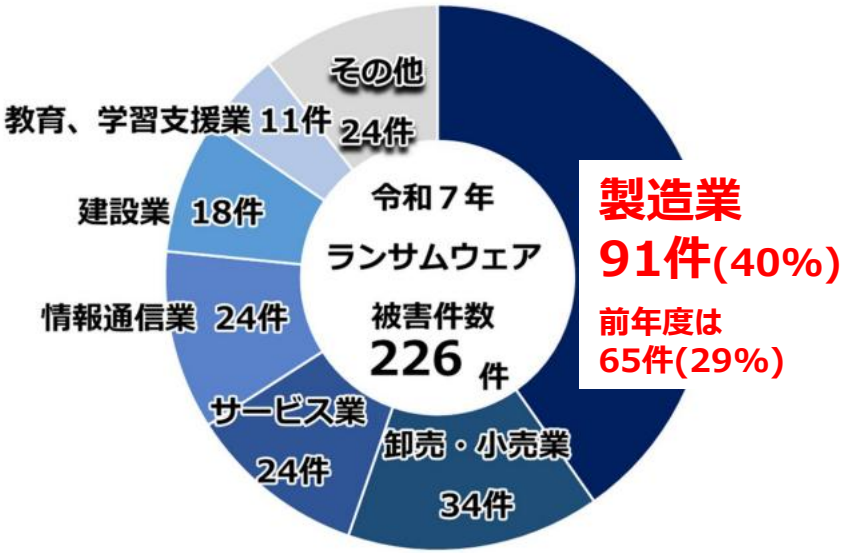
インターネットに接続されている端末は、台当たりに換算すると**毎日7,000件近いサイバー攻撃**を受けており、**年々、攻撃は複雑化、巧妙化しており、今後も更なる増加が予想されている。**
又、**引き続き業種別の割合で見ると製造業が最も多く**、被害件数40%を占めており、**全業種の中で最も標的にされている。**
もはや、**対岸の火事ではなく**、今日狙われる可能性もあり、**自分事と捉えた行動が必要**。

【IPアドレス当たりのサイバー攻撃関連通信受信数】



出典：「NICTER観測レポート2025」<国立研究開発法人情報通信研究機構>

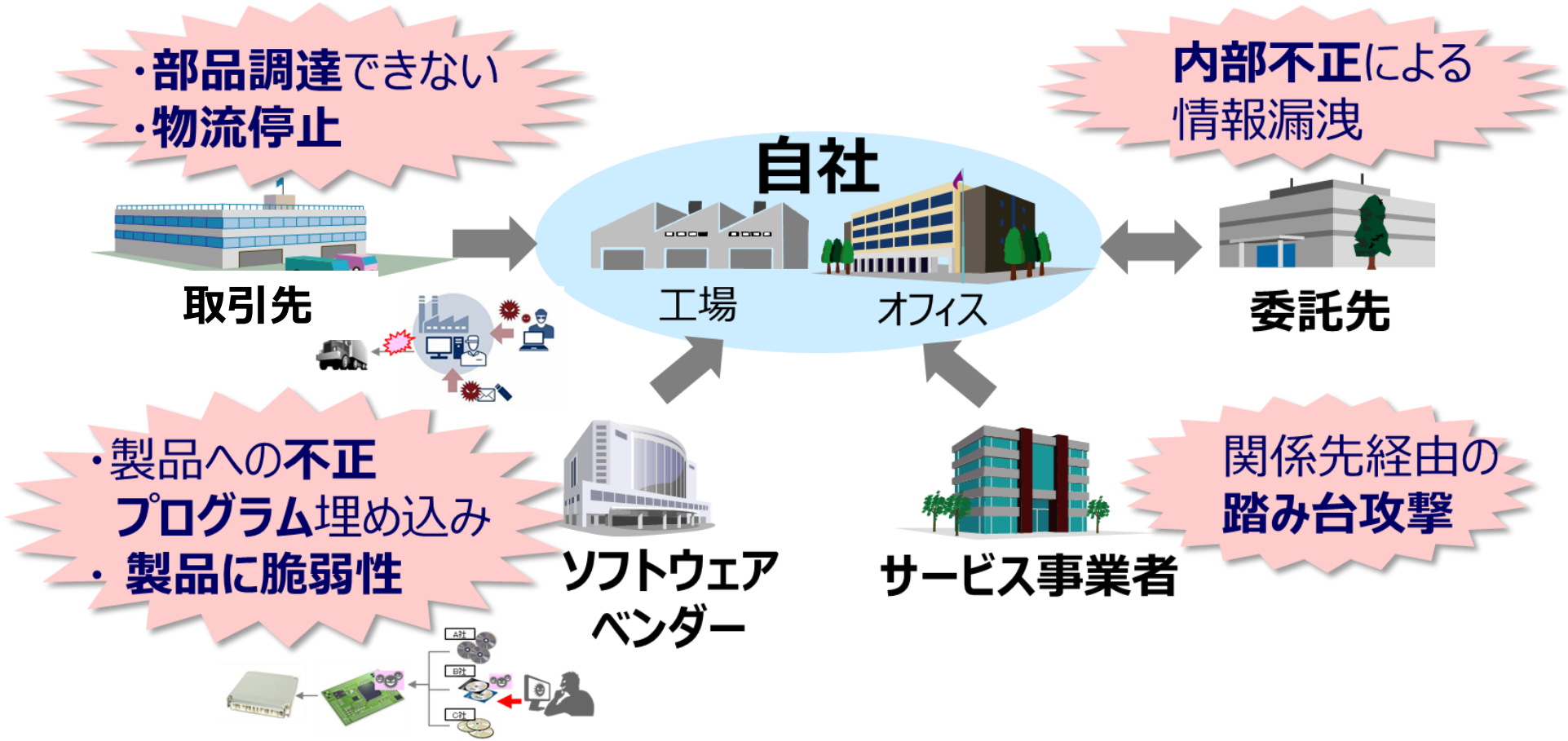
【被害企業・団体等の規模別／業種別報告件数】



出典：「令和7年におけるサイバー空間をめぐる脅威の情勢等について」<警察庁>

1-3. サプライチェーンに於けるセキュリティリスク

業界全体が拡大、扱うデータ量も増加する中で、従来の様に**自社だけを守っていたのでは不十分**。
攻撃者は常に弱い部分を狙っており、**サプライチェーン全体でのリスク管理が必要**となっている。



1-4. 自動車産業サプライチェーンセキュリティ推進活動

国を挙げての全体方針の元、自動車産業として取り組んでいる活動

業界全体のセキュリティレベル底上げを目指し、**業界標準のガイドラインを策定**

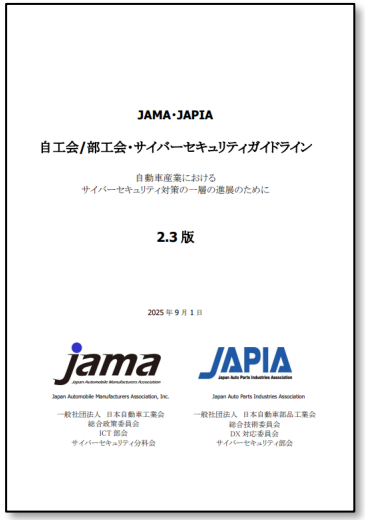
業界内関係各社と連携、協力し、レベルアップ活動を推進中

＜標準モデル＞

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

サプライチェーン対応の
セキュリティガイドラインを策定


JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

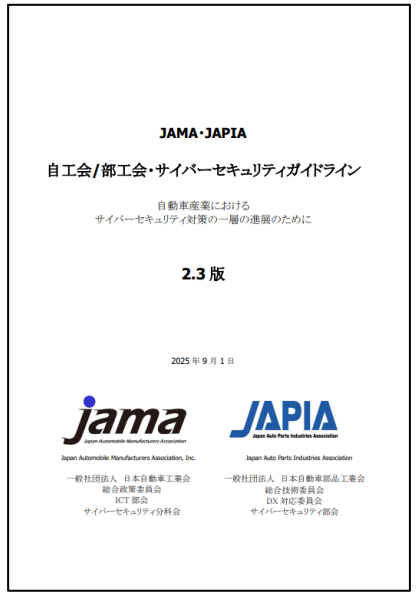
自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.3 版

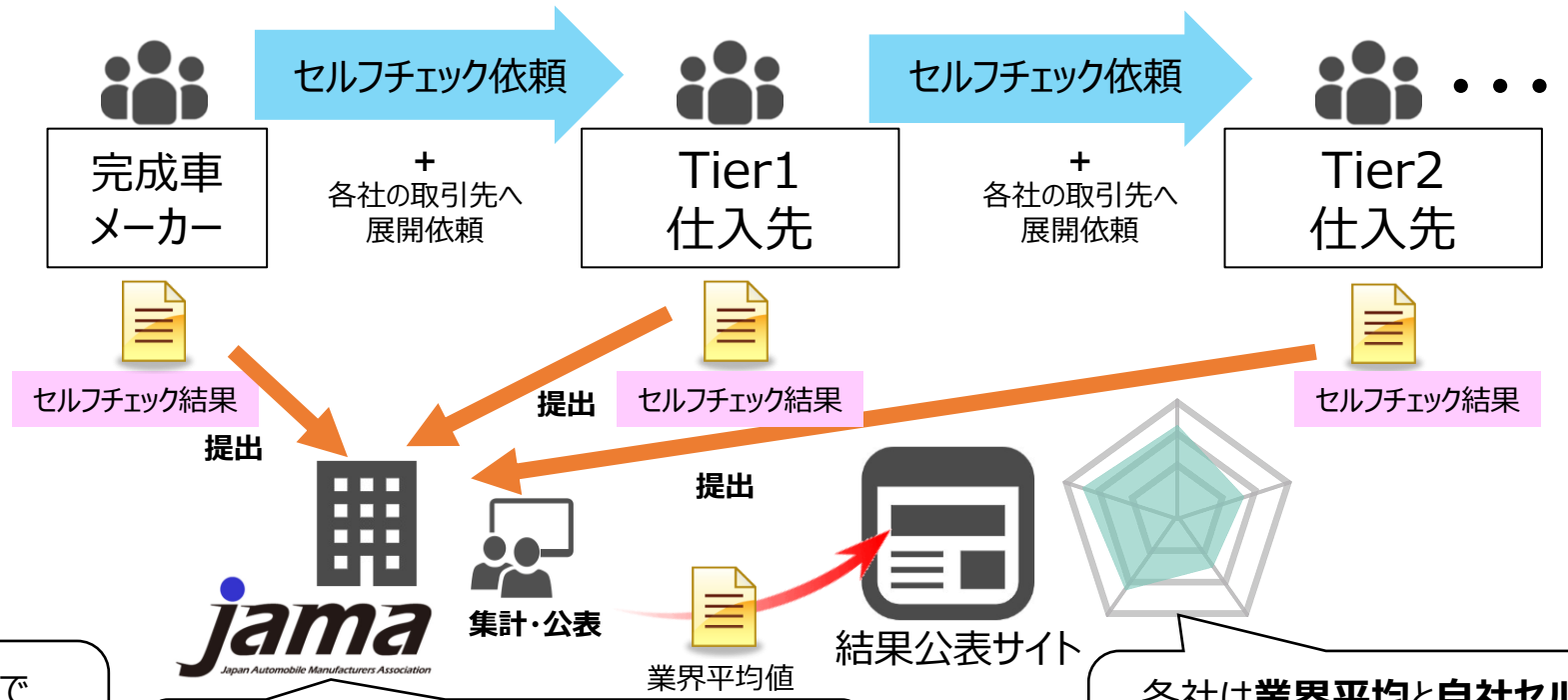
2025 年 9 月 1 日

1-5. 具体的な活動内容

19年度　経産省CPSFを基にした**自工会及び部工会の合同で業界標準ガイドラインを策定**
21年3月から　**業界全体に対して、セキュリティレベルの自己評価及び向上への取り組みを依頼**
→ 自社の自己評価結果に基づき、**重点課題を認識し、対策推進する事でセキュリティレベル向上を図る**



自工会、部工会合同で
自動車業界標準の
セキュリティガイドラインを策定



サプライチェーンの各社に展開依頼、
業界全体の評価を自工会で集約

各社は**業界平均**と**自社セルフチェック結果との差異**から
重点課題を認識

＋

＜支援活動＞

- 解説書
- セミナー
  経営層・担当者
- 問合せ対応
  （チャットボット等）
- ＨｏｗＴｏ手引書
  中小企業向け セキュリティ対策
  レベルアップに向けた手引き

今後の展望について
～SCS評価制度～

1-6-1. SCS評価制度　概要（経産省資料より抜粋）

課題

経産省の問題意識	①発注元　：取引先がどの程度対策を行っているのか外部から判断することが難しい ②サプライヤー　：異なる発注元から様々な対策水準を求められ対応に苦慮している

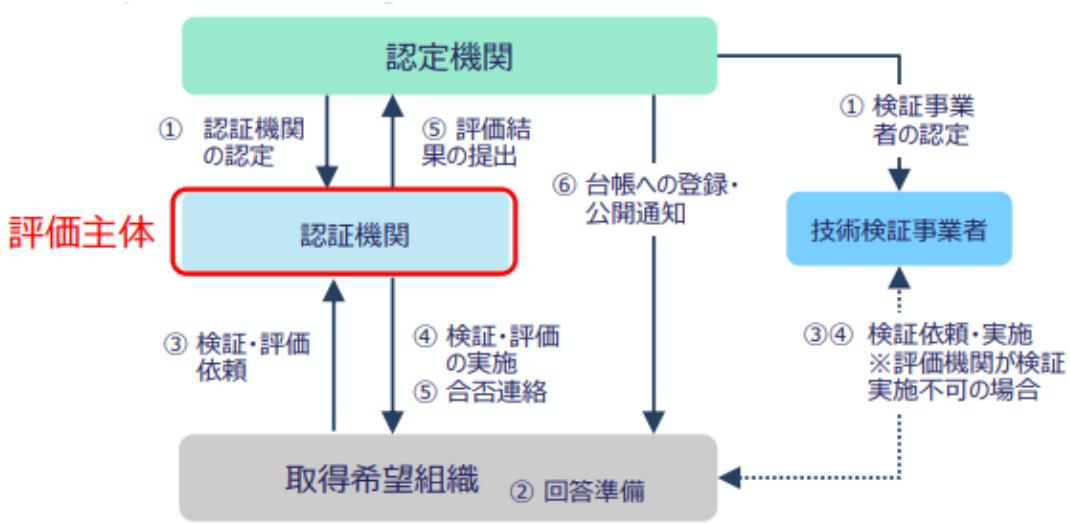
対策

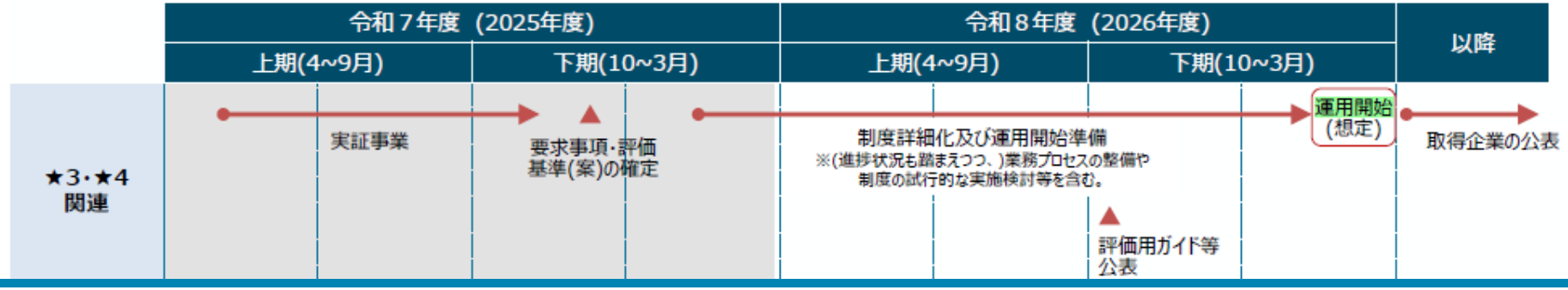
国の評価制度を設け、共通の基準で対策状況を見える化する（★3、★4、★5）

（※ 当制度は法律に基づく義務付けではなく
あくまで企業が自ら行うもの）

・★3、★4の運用開始は令和8年度末頃を予定
・★5の基準、スキームは令和8年度以降、検討

★4の評価スキーム





1-6-2. SCS評価制度への対応方針（自工会・部工会）

「SCS評価制度」について、自工会・部工会として対応方針を整理しましたので、ご報告いたします

●自動車業界として目指す姿

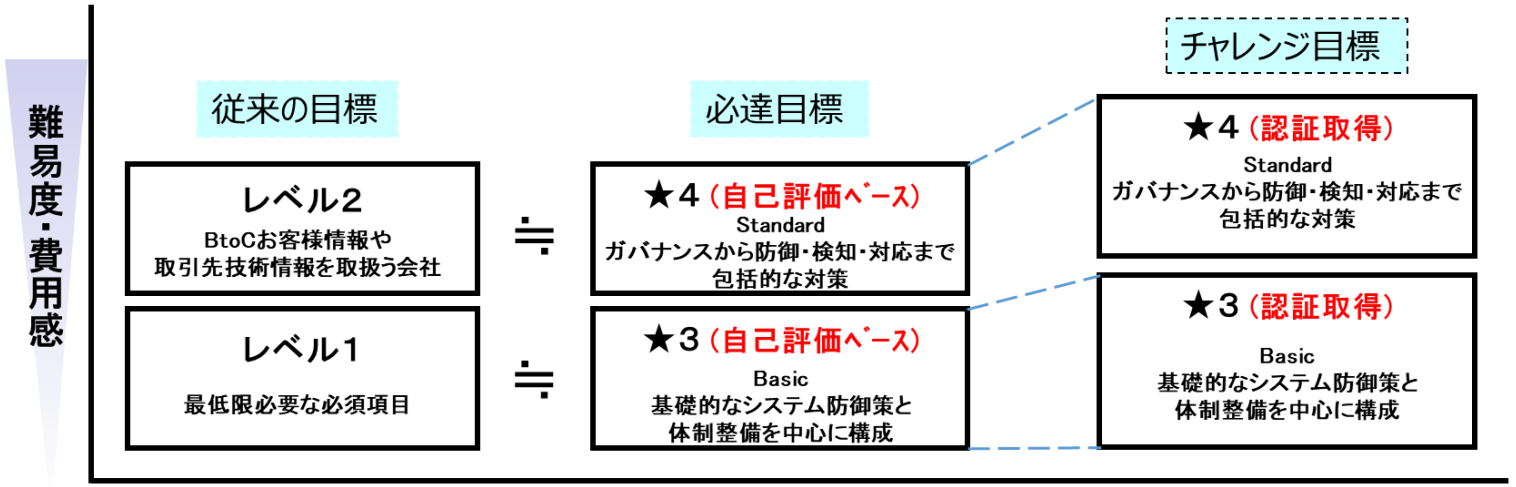
最終的には、国の新制度に一元化すべきと考える（ダブルスタンダードにならないようにする）

●自動車業界としての新制度の活用方法

1）準拠すべきガイドラインは、新制度ガイド１本とする（自動車産業ガイドから、新制度ガイドに乗り換える）

2）新制度ガイドに基づいた「自己評価の実施」と「その結果の提出」を従来同様に各社様にお願いしたい
自工会としての「自己評価結果の集計・分析」と「その結果の公表」も従来同様に継続実施する

3）★３★４の認証取得を必須とはしない（各社の任意とする）



1-6-3. 新制度への切替え大日程（案） *継続検討中

現時点での切替え計画案（＋中間チェックポイントのイメージ）

		’26/1-3	’26年度	’27年度	’28年度	’29年度以降
★3・★4	経産省　大日程	★3,★4運用準備 →		**制度運用開始 (想定)** △		
		先行の国内外制度との調整 →				
	自工会・部工会 大日程	経産省と細部調整（ガイド、運用） →		立上がり状況フォロー →	導入時期・運用方法の決定 △ → 新運用準備・周知 → **新運用開始(仮)** △ → 状況フォロー・改善 →	
★5	経産省　検討中	★5スキーム検討 →		→	運用開始 時期未定 ?	

このタイミングで切替え可否判断

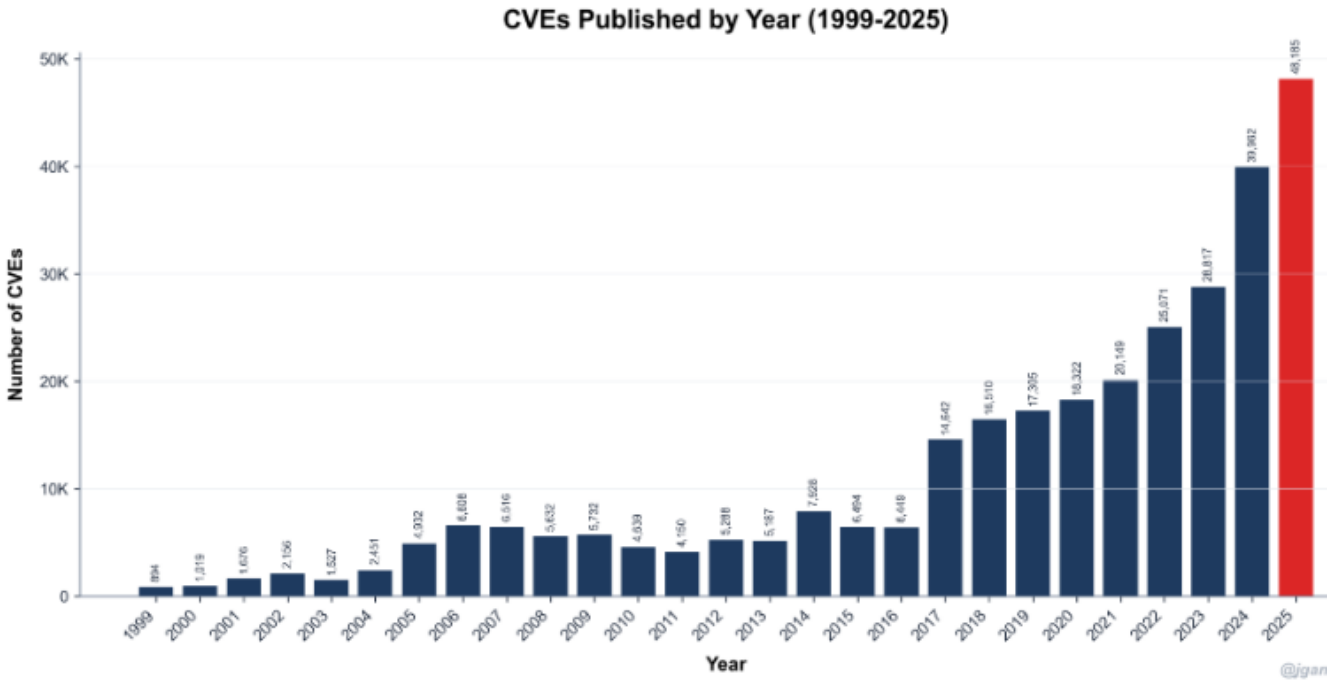
喫緊の課題について

～高性能AIへの対応～

1-7-1. 脅威認識：高性能AIによる脅威の増大

脆弱性の発見や高度な攻撃コードの生成に優れた「高性能AI」の発展に伴い、従来の前提が根本から変容する恐れ

- **量**：これまでの脆弱性の発見
  →既に大量に発見、**急激な増加**が予想

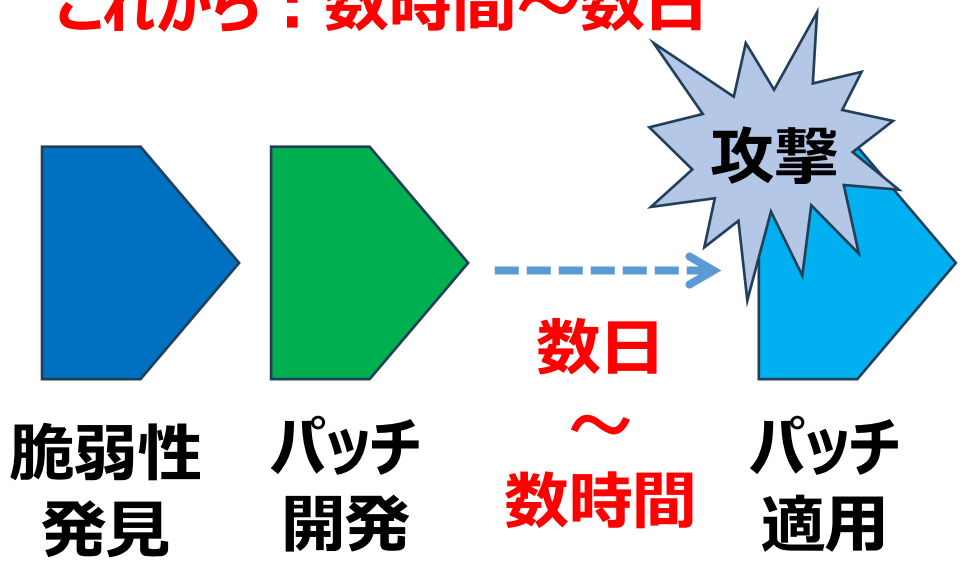


- **時間軸**：超大量を**超短期で**対応が必要

（攻撃までのリードタイム）

これまで：数週間～数か月

これから：数時間～数日



参照元：2025CVEBlog/blog_final.md at main · jgamblin/2025CVEBlog · GitHub

1-7-2. 高性能AIによる脅威増大への備え

・AI技術が急速に進展する中、サイバー攻撃にAIが活用されることで、攻撃のスピード・規模が劇的に加速・拡大する等、サイバーセキュリティを巡る脅威が高まっている

・特に、いわゆる「高性能AI」により、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上が見込まれることを踏まえ、 我々自動車業界も、これに対応する取組が必要不可欠である

◆まずは以下項目について早急な取組みをお願いします（自工会HP掲載「緊急メッセージ」参照）

1）発見された脆弱性に早期に対応してください

積極的に脆弱性関連情報を収集し、脆弱性が発見された場合には、ビジネスに於ける重要度及び発生リスクの重大度による優先度を設定した上で、重要度・重大度に応じた速やかな対応を行ってください（特に、外部公開システムには最優先で修正プログラムの適用をお願いします）

2）組織のトップが主導して取り組んでください

サイバーセキュリティリスクは経営リスクとの認識を持ち、経営陣のリーダーシップの下、必要なリソースの確保と対応を行ってください
（具体例：脆弱性対応に必要な体制・工数・費用の確保、侵入された場合に備えたBCPの策定、等）

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

本事案のサマリ

BtoB通販大手「アスクル社」が、2025年10月にサイバー攻撃を受け、ECサイト・物流が停止

復旧まで約4か月を要し、**お客様情報約74万件が流出**した

自工会/部工会ガイドラインなどを活用し、セキュリティ要件をチェックすることで、

「弱い部分を可視化し、リスクを把握」の上、「リスクに対する対策」を行っておく

サイバー攻撃は、既に「自社でも起こるかもしれない」ではなく「いつ起こるのか」と言った状況

サイバー攻撃を自分事と捉える事が、備えの第一歩

「アスクル株式会社」様について

社名	アスクル株式会社
主な事業	eコマース事業：オフィス用品・日用品等の通販サービスの提供 • 企業向けECサイト「ASKUL」「ソロエルアリーナ」 • 個人向けECサイト「LOHACO」
特徴	• 製造業・建築業向け専門用品、医療品等まで提供 • **物流に係る業務のほとんどを自動化**
サプライチェーン	子会社である「ASKUL LOGIST」が、委託元として **「無印良品」「LOFT」公式ECサイトの物流業務を受託**

事業用品等の物流を担う<u>サプライチェーンの中核企業</u>

事例の概要

ランサムウェア感染により**システムが停止**　その結果、**事業停止**まで被害が及んだ

システムへの影響

- ✓ 物流・社内システムの暗号化
- ✓ バックアップファイルも暗号化
- ✓ 外部クラウドサービス(お問い合わせ管理システム)のアカウントも侵害

事業への影響

- ✓ ASKUL・ソロエルアリーナ・LOHACOの受注／出荷停止
- ✓ 自動倉庫設備・ピッキングシステムが停止
- ✓ 複数物流センターの出荷業務が全面停止

さらに、受注・出荷停止による影響がサプライチェーンにまで波及

ex)株式会社良品計画、株式会社ロフト…

経営への影響

事業停止により決算にも多大な影響が・・・

特別損失(第2Q)

52.2億円

システム障害対応費用
物流基盤維持・調査復旧等

営業損失(第2Q)

▲29.95億円

ピーク月の月次売上
前年同月比 ▲95.1%

個人情報漏えい

約74万件

取引先 約1.5万件を含む

サイバー攻撃対策は事業継続と企業価値を左右する経営課題

時系列

2025/6/5	業務委託先用のアカウントを悪用し、社外より初期侵入
2025/10/19	**ランサムウェアが起動**、ファイルが暗号化、削除、漏えい **「ASKUL」等の受注・出荷業務が停止**
2025/10/20	外部専門機関へ支援要請。詳細調査開始
2025/10/29	FAXを利用した**手動運用による注文受付** (拠点と品目を限定)
2025/11/12	「ASKUL」等、**一部Webサイトで受注再開** 段階的に出荷拠点・受注範囲を拡大
2026/2/13	主要なECサービス機能について、**障害発生前の水準まで復旧**

侵入～被害発覚
約4か月

被害発覚～復旧
約4か月

初動対応 時系列

初動対応では、**ネットワーク遮断、パスワード変更**を中心に迅速な対応を実施

2025/10/19 午前	**ランサムウェアが起動**、ファイルが暗号化、削除、漏えい
2025/10/19	**感染疑いシステムの切り離し・ネットワークの物理的遮断** 全パスワードの変更に着手
2025/10/19 14時	本社内に対策本部を設置
2025/10/19 16時半	**「ASKUL」等の受注・出荷業務が停止**
2025/10/20	外部専門機関へ支援要請。詳細調査開始 意図しないデータ変更・プログラムリリース・タイムスタンプ異常を点検
2025/10/22	**外部クラウドサービスへの不正アクセス発生**
2025/10/23	主要外部クラウドサービスのパスワード変更完了
2025/10/24	**管理アカウントへ多要素認証を適用**、主要アカウントパスワード変更、 EDRシグネチャ更新

本事例におけるポイント　–何が問題だったのか

アスクル社のサイバー攻撃被害における問題点は以下の通り

初期侵入	検知	復旧
委託先アカウントが不正利用	**侵入から4か月被害に気付けず**	**被害発覚から復旧まで4か月**

アスクル社のサイバー攻撃被害は、なぜ発生し、甚大な被害に至ったのか

①初期侵入　–なぜ侵入されたか

侵入経路は、**委託先に付与した管理者アカウントのID・PWの漏えい・不正利用**

問題点①

- ✓ **基本的には多要素認証を導入していたが、当該アカウントについては、例外的に多要素認証が導入されていなかった**

結果

- ✓ **IDとパスワードさえ知っていれば、誰でも正規ユーザーとしてシステムに入れる状態**
- ✓ **攻撃者は2025年6月時点で既に社内ネットワークへの侵入に成功していた**

統一した管理がされておらず、管理が緩い部分が侵入口となった

②検知　–なぜ気づけなかったか

侵入後、攻撃者は**約4か月間かけて**社内ネットワーク**全体のアクセス権限を掌握**

問題点②

- ✓ 侵害が発生したデータセンターでは、サーバに**EDR（脅威検知ソフト）が未導入**
- ✓ 不審な動作を自動検知する仕組みが不足していた

結果

- ✓ **約4か月にわたる**攻撃者の潜伏・拡大を検知できなかった
- ✓ ランサムウェアの実行により、**システムが暗号化されるまで被害に気付けなかった**

EDR未導入サーバが、攻撃者の潜伏を許す**「監視の死角」となった**

③復旧　–なぜ時間を要したのか

ECサービスが障害発生前の水準まで**復旧するまで約4か月**を要した

問題点③

- ✓ バックアップデータは存在したが、その一部が**オンライン（ネットワーク接続状態）で保管されていた**
- ✓ OS更新の過程で被害端末のログが消去、**被害時のログが残っていなかった**

結果

- ✓ 攻撃者はランサムウェア実行前に**バックアップファイルも掌握・暗号化**
- ✓ 侵入経路・被害範囲の特定が困難
- ✓ やむを得ず**システムの再構築（クリーン化）を実施**
- ✓ ECサービスの復旧に**約４か月**を要した

サイバー攻撃を想定した事業継続の備えができていなかった

本事例の問題点と必要な対策①

フェーズ	問題点	必要な対策例	自工会/部工会ガイドラインの例
①初期侵入	**委託先アカウントで多要素認証が未導入**だった ※ID/パスワードさえ分かれば「誰でも」「正規ユーザーとして」ログイン出来る状態	インターネットから利用するシステムや重要データを保管するシステムへの**多要素認証の導入**および設定状況の確認(クラウドサービスやVPN等)	**18 認証・認可 No.120** 「インターネットから利用できるシステムには**多要素認証を実装**している」
		重要な委託先のセキュリティ対策**状況を点検する。** **※サプライチェーン管理/対策**	**8 他社との情報セキュリティ要件 No.42** 「重要な機密情報を取り扱う**パートナー企業のセキュリティ対策状況**を把握している」
②検知	サーバに対して**EDR等の不審な動作を検知する仕組みが未導入**だった	PC・サーバに対して**EDR等の行動追跡システムを導入**する また導入後は、**定期的にEDRのインストール状況のチェックおよびバージョンを最新化**する	**22 マルウェア対策 No.138** 「エンドポイントでの**詳細な履歴取得**及びマルウェア感染後の遠隔対応が可能な**行動追跡システムを導入**している」

本事例の問題点と必要な対策②

フェーズ	問題点	必要な対策例	自工会/部工会ガイドラインの例
③復旧状況	**ネットワークから切り離した環境へのバックアップファイル保存**などの対策が取られていなかった 隔離された環境へのログ保管など、**ログに対する「安全管理」**がなされていなかった	**サイバー攻撃を想定したバックアップを取得**する（3-2-1-1ルール、イミュータブルバックアップ等） **ログ収集専用サーバ等での保管**、当該サーバに対しての**アクセス制御**	**24 バックアップ・復元 No.148** 「**適切なタイミング**でバックアップを取得している」 ※オフラインでの保管を実施するなど **9 アクセス権 No.53** 「アクセスログは、**安全に保管しアクセス制御された状態で管理**されている」

あなたの会社では、これらの対策を実施できていますか？

サイバー攻撃デモ

事前の備え/対策が出来ていないと、如何に簡単に侵入し、
攻撃を行う事が出来てしまうのか・・・

まとめ

①**サイバー攻撃への対策は、**事業継続と企業価値を左右する**経営課題**と認識する

②**自工会/部工会ガイドライン**などを活用し**「リスク把握」**及び**「リスクに対する対策」**を確実に行う

③侵入及び被害拡大を防ぐためにも、**サイバー攻撃を想定した事前の備え**が重要

サイバー攻撃は、既に**「自社でも起こるかもしれない」**ではなく**「いつ起こるのか」**の状況

サイバー攻撃を自分事と捉える事が、備えの第一歩

最後に…スグにでも取り組むべきこと

① **まず「自社の現在地」を知ること**
自工会/部工会ガイドラインなどを活用し、対策状況を確認することが第一歩

② **不足している対策へのリソースを確保する**
経営層が関与し、人員・予算・体制を確保することではじめて対策が動く

③ **サイバーセキュリティを経営課題として継続的に見直す**
一度やって終わりではない。定期的なチェックシートの見直しと改善を継続する

今日、明日からでも、まずは第一歩を踏み出してください

Appendix – 参考文献、用語解説

参考文献

アスクル株式会社「ランサムウェア攻撃の影響調査結果および安全性強化に向けた取り組みのご報告(ランサムウェア攻撃によるシステム障害関連・第13報)」

https://pdf.irpocket.com/C0032/PDLX/O3bg/N4O3.pdf

(2026-07-22 最終アクセス)

アスクル株式会社「2026年5月期 第2四半期(中間期)決算短信〔日本基準〕(連結)」

https://pdf.irpocket.com/C2678/ikpa/wnGE/HEKP.pdf

(2026-07-22最終アクセス)

用語解説

用語	解説
ランサムウェア	システムやファイルを暗号化し、復旧と引き換えに金銭を要求するマルウェア（悪意あるソフトウェア） 感染するとデータへのアクセスが不可能になり、事業が完全停止するリスクがある
多要素認証 （MFA）	ログイン時にパスワードに加え、スマートフォンへの通知や生体認証など複数の要素で 本人確認を行う仕組み。ID/パスワードが漏えいしても、不正にログインされづらくなる
EDR（Endpoint Detection and Response）	パソコンやサーバ上の不審な動作をリアルタイムで検知・記録し、サイバー攻撃の早期発見と対応を支援するセキュリティソフトウェア
バックアップ	データの消失や破壊に備えて複製を別の装置や媒体に保存しておくこと ネットワークから切り離した環境（外付けHDDや専用ストレージ等）に保管することで、 ランサムウェアによる暗号化被害を防ぐことが可能

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

3-1. 2025年度自己評価結果の分析

✓ 2025年度は4,032社が自己評価を実施（前年度比＋898社）
※過去最高の参加社数
✓ レベル１～３の全てのレベルにおいて、2024年度よりも平均点が向上

年度	有効回答総数	平均点
2025	4,032 社	ﾚﾍﾞﾙ 1 項目:83.13/100 点 (83.1%) ﾚﾍﾞﾙ 2 項目:126.14 /148 点 (85.2%) ﾚﾍﾞﾙ 3 項目:41.24 /58 点 (71.1%)
2024	3,134 社	ﾚﾍﾞﾙ 1 項目:82.80 /100 点 (82.8%) ﾚﾍﾞﾙ 2 項目:123.47 /148 点 (83.4%) ﾚﾍﾞﾙ 3 項目:39.34 /58 点 (67.8%)
2023	3,240 社	ﾚﾍﾞﾙ 1 項目:81.84 /100 点 (81.8%) ﾚﾍﾞﾙ 2 項目:120.00 /148 点 (81.1%) ﾚﾍﾞﾙ 3 項目:42.91 /58 点 (74.0%)

2025 年度平均点詳細

目標ﾚﾍﾞﾙ	会社数	平均点			
		ﾚﾍﾞﾙ 1 項目	ﾚﾍﾞﾙ 2 項目	ﾚﾍﾞﾙ 3 項目	総合
ﾚﾍﾞﾙ1	989 社	63.32 /100 点 (63.3%)	－	－	63.32 /100 点 (63.3%)
ﾚﾍﾞﾙ2	1,704 社	87.25 /100 点 (87.3%)	121.20/148 点 (81.9%)	－	208.45 /248 点 (84.1%)
ﾚﾍﾞﾙ 3	1,339 社	92.52/100 点 (92.5%)	132.43 /148 点 (89.5%)	41.24 /58 点 (71.1%)	266.18 /306 点 (87.0%)
	計	83.13 /100 点 (83.1%)	126.14 /148 点 (85.2%)	41.24 /58 点 (71.1%)	－

3-2. 2026年度のお願い

- ✓ 継続的なレベル把握のため、2025年度と同様に自己評価頂く
  ご提出期日：2026年12月31日
- ✓ 本活動を業界全体に浸透すべく、より多くのサプライヤ様への展開をお願いしたい

1）自社の自己評価及び自工会への提出

2）取引先様へのご依頼
※自己評価及び自工会への提出

3-3. 自工会/部工会が期待する達成レベル及び目標時期

2026年度の目標
自動車業界としては、2025年度末にレベル１，２達成を目標に進めてきました。
2026年度は下記目標にて推進をお願いします。

✓ 既に達成済みの会社様 ➡ 維持及びレベルアップ
※完成車メーカ、大規模Tier1会社、および高度な技術・ノウハウをお持ちの会社様はレベル3を目指して頂きたい

✓ 未達成の会社様及び今から始められる会社様 ➡ 2026年度でのレベル１，２達成
※達成が困難な場合も26年度末までにレベル1の全項目を達成頂き、出来る限りレベル2にも対応頂きたい

＜自動車産業サイバーセキュリティガイドラインのセキュリティレベル定義＞

Lv. 3	⇦	**模範レベル（ベストプラクティス）**
Lv. 2	⇦	**顧客情報・取引先技術情報を取扱う会社が達成すべき項目**
Lv. 1	⇦	規模・扱っている情報に因らず**最低限必要な必須項目**

3-4. 自己評価・提出の要領

下記要領に基づき26年度自動車産業サイバーセキュリティガイドライン自己評価・ご提出をお願いします。

項目		説明
1	自己評価に用いる JAMAチェックシート	• 2025年度とチェック内容は同一です。 • **自工会ホームページの以下のサイトよりチェックシートV2.3を取得しご使用ください。** 自動車産業サイバーセキュリティガイドライン | JAMA - 一般社団法人日本自動車工業会
2	ご提出期限	• **2026年12月31日までにご提出願います。**
3	ご提出方法 （自工会・依頼元）	• 提出方法は１項のHPに掲載されている提出方法をご確認の上、ご提出ください。 **1. １項のHPに掲載されている「2026年度 チェックシート提出用URL申し込み」サイトへ申し込みをする。** **2.メールで送付されたチェックシート提出用URLへ提出する。**
4	補足事項	• 自己評価依頼を受けた会社様は自社の１次仕入先様にも自己評価を要請願います。 その際、順次その１次仕入先様にも展開頂く様、併せて要請ください。

本日のアジェンダ

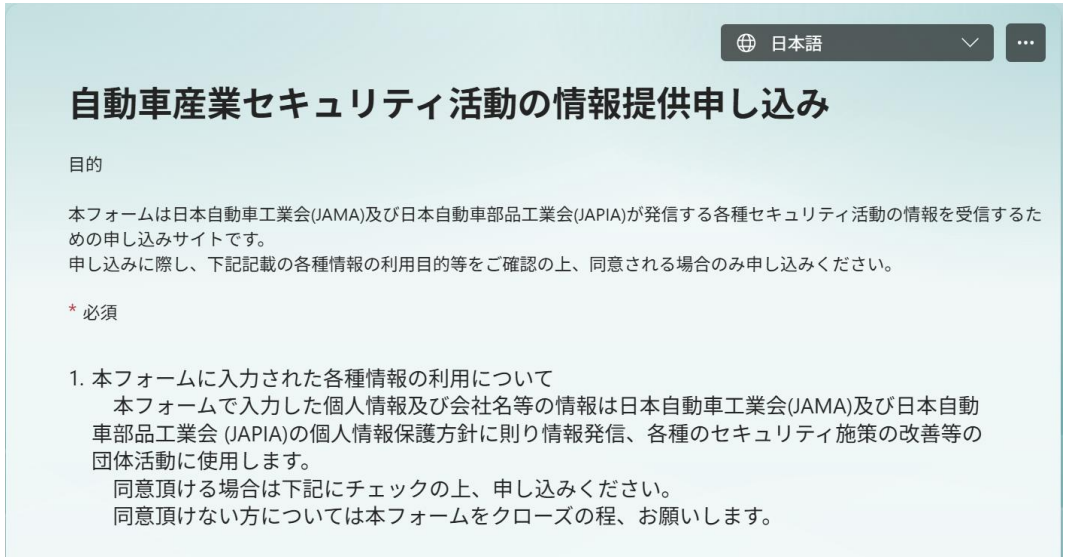
1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

4-1. 自動車産業セキュリティ活動の情報提供申し込み

- ✓ 昨年度より、**自動車産業全体のサイバーセキュリティ対策向上**のため、自工会・部工会から情報セキュリティ活動や、自工会・部工会活動に関する情報を適宜発信しています
- ✓ 自工会公式ホームページに掲載の**「自動車産業セキュリティ活動の情報提供申し込み」**ページにて、**「情報提供を希望する」**を選択いただいた方々へ、メールにて送付をさせていただきます

自動車産業サプライヤー向け 各種情報提供 -「申込フォーム」

https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_supply_chain.html



《発信予定情報》

- ✓ 自動車産業サイバーセキュリティガイドライン自己評価関連情報
- ✓ 自己評価依頼説明会案内　等

4-2.メールマガジンの配信について

- ✓ 昨年度より、**自動車産業界全体でのセキュリティ活動活性化を狙いにメールマガジンを配信しています**
- ✓ 自工会公式ホームページに掲載の**「自動車産業セキュリティ活動の情報提供申し込み」**ページにて、**「情報提供を希望する」**を選択いただいた方々へ、**メールにて送付をさせていただきます**
- ✓ **セキュリティに関するTIPSや自工会/部工会の取り組みをご紹介**していきます

■内容

・セキュリティ対策の紹介や注意喚起など：パスワード、ログ管理、暗号化、長期連休に向けた注意喚起、など
・セキュリティニュース(報道された重大事象、サイバー攻撃動向、新しいリスク、流行している攻撃メール等の情報、など)
・セキュリティ脆弱性注意喚起(重大な脆弱性の連絡、対策の簡易説明)
・連絡事項(イベント紹介、自工会からの連絡事項、など)
※配信時のアンケートご意見を参考に選定しております

■配信頻度

昨年度は全３号の配信でしたが、今年度は隔月での全６号の配信を予定しております

4-3. 自動車産業サイバーセキュリティガイドライン問い合わせチャットボット（概要）

自動車産業サイバーセキュリティガイドライン問い合わせチャットボットを開設

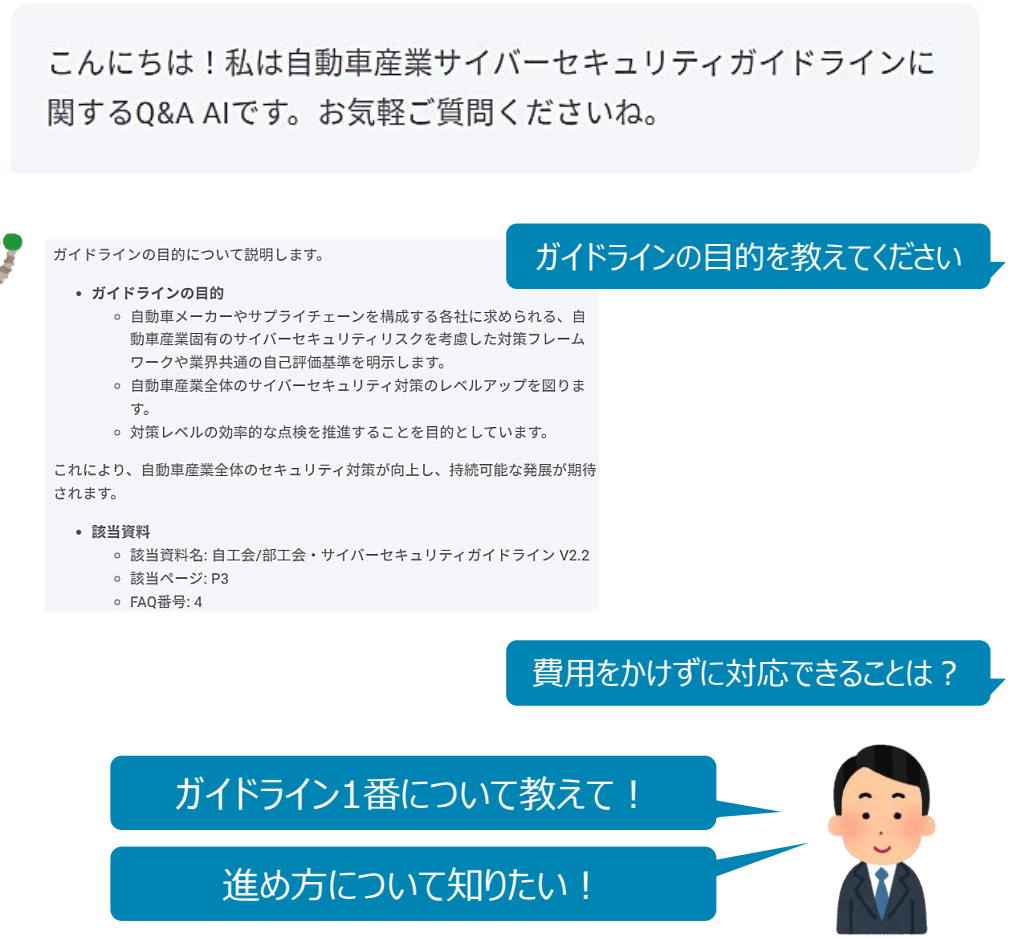
◆ チャットボット設置場所（自工会HP）
チャットボットURL：自動車産業サイバーセキュリティガイドライン問合せチャットボット

◆ 利用可能期間：2026年9月1日~2027年1月15日
※ガイドライン提出期限は2026年12月31日

◆費用：無料

◆用途：自動車産業サイバーセキュリティガイドラインに関するお問い合わせ

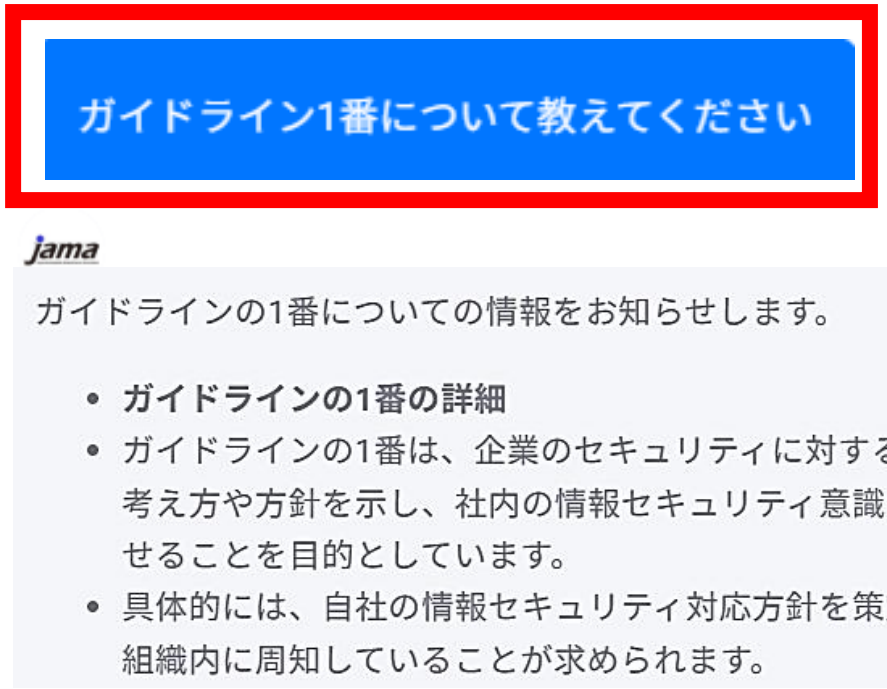
ガイドラインによる自己評価を進める上での困りごとに対し、
過去にお寄せ頂いたお問い合わせ等を
学習したチャットボットが手助けをいたします



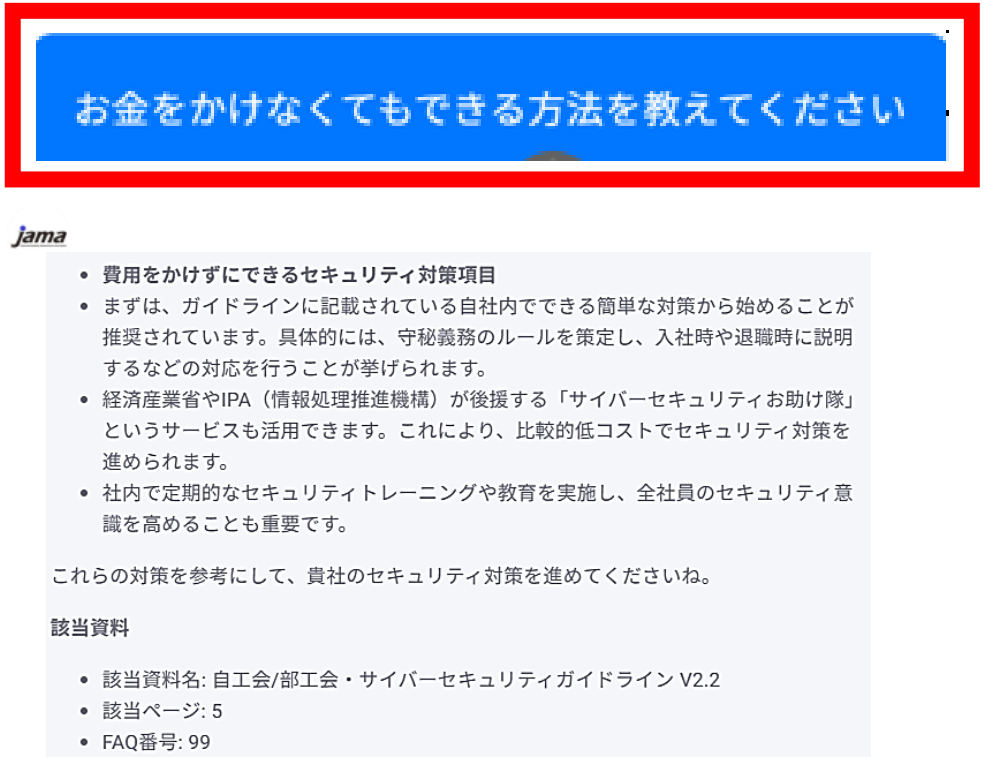
4-4. 相談窓口（ご利用例）

チャットボットに記入頂く質問は具体的でも抽象的でも回答が得られます。

具体的質問の例



抽象的質問の例



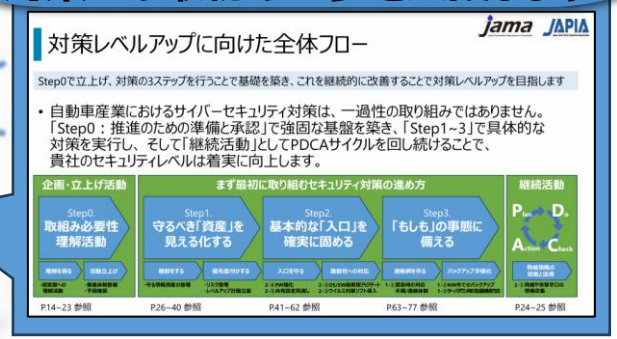
※ チャットボットで回答できる事には限りがありますが、自己評価を進める上での困りごと解決にお役立て頂ければと存じます

4-5. レベルアップ支援活動

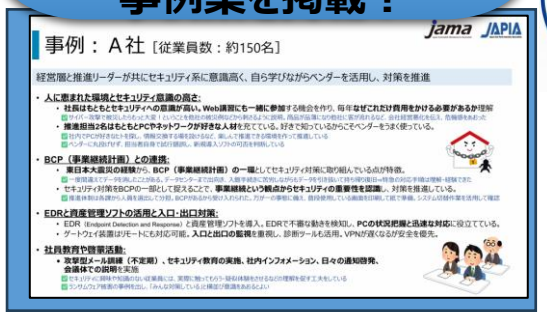
中小企業のセキュリティレベルアップを、この1冊でサポート！

まずは是非読んでみて下さい！

皆様の「困りごと」に寄り添い、対策への最初の一歩を支援します



現場の「生の声」をお届け事例集を掲載！



他社のリアルな取り組みから、自社に合ったヒントが見つかります！

これらの事例は、机上の空論ではなく、
皆様と同じ立場の企業が実践し、成功に至った
確かな道筋です。

セキュリティ対策は、特別なことではありません。

本書は、限られたリソースの中でも「今すぐ取り組めること」から「着実にレベルアップする道筋」までを分かりやすく解説しています。

まずはこの1冊から、できることを始めましょう！

本書はJAMAホームページからダウンロードできます

https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_Security_LevelUp_Handbook.pdf

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

■メッセージ

ある日突然起きた現実。
その経験から得た教訓と変革。

株式会社ミヤキ様が、自動車業界の仲間のために、
実体験とそこから得られた教訓を共有くださいます。
明日、自社で起きてもおかしくない出来事として、ぜひ、自分事としてお聞きください。

■登壇者紹介

株式会社 ミヤキ

経営管理部　執行役員	山本 将之　様
経営管理部経営企画課システム係　主任	鈴木 良宣　様

本日のアジェンダ

1	はじめに
2	サイバーセキュリティ対策の重要性 - 最新事例紹介 -
3	26年度自己評価のお願い
4	今後の活動、セキュリティ情報提供の申し込みについて
5	スペシャルコンテンツ　＊説明会参加者特典
6	まとめ

6-1. 説明会全体のまとめ

【世の中の状況】
- 製造業は被害件数が全業種で最多。もはや「対岸の火事」ではない
- 自社だけの防御では不十分。サプライチェーン全体でのリスク管理が必要

【制度と脅威の動向】
- 経産省／IPAが「SCS制度」を2026年度末までに整備。業界としては2028年度以降ガイドラインを一本化
- AIの悪用にて「より速く・より大規模」に攻撃が拡散。対応スピードが勝負

【最新事例：アスクル様】
- ランサムウェアでEC・物流が停止、復旧に約4か月、個人情報 約74万件が流出
- 多要素認証・EDR・バックアップ等の基本対策の徹底で被害は最小化できた

【自己評価の状況】
- 2025年度は過去最多の4,032社が実施し、平均点も向上
- 継続的なレベル把握のため、2026年度も自己評価の実施をお願い

6-2. 本日のお願い事項

① 自己評価の実施とご提出

・ 自動車産業ガイドラインチェックシートV2.3で自己評価を実施し、2026年12月31日までにご提出ください
（目標はレベル1・2の達成。達成済みの会社様はレベル3を目指してください）

② サプライチェーン全体への展開

・ 自社の1次仕入先様にも自己評価を要請し、順次その先へも展開してください

③ 経営層の主体的な関与

・ セキュリティを経営課題と位置づけ、人・予算・体制をこれまで以上のスピードで確保してください

④ 基本対策の確実な実施

・ 脆弱性の早期対応・パッチ適用・バックアップ整備・多要素認証等の基本対策を徹底してください

6-3. 最後に

まずは「自社の現在地」を知り、第一歩を踏み出してください

① ガイドラインの自己評価で対策状況を確認し、自社のリスクを把握する
② 経営層が関与し、不足している対策に人員・予算・体制を確保する
③ 一度で終わらせず、定期的に見直し、改善を継続する

サプライチェーン全体でのレベル向上を、皆様とともに進めてまいります。本日はありがとうございました。