2025年度サイバーセキュリティ月間

供給を受ける側から見たサプライチェーンセキュリティについて

一般社団法人
日本自動車工業会

総合政策委員会 ICT部会
サイバーセキュリティ分科会

2025年3月10日

自己紹介　古田 朋司（ふるた ともじ）

- **日本自動車工業会**

  総合政策委員会 ICT部会 サイバーセキュリティ分科会長

- **トヨタ自動車株式会社**

  情報セキュリティ・トラスト部長

  - ✓ 生産系アプリ開発やグローバルIT戦略を担当
  - ✓ 2017年～現職

目次

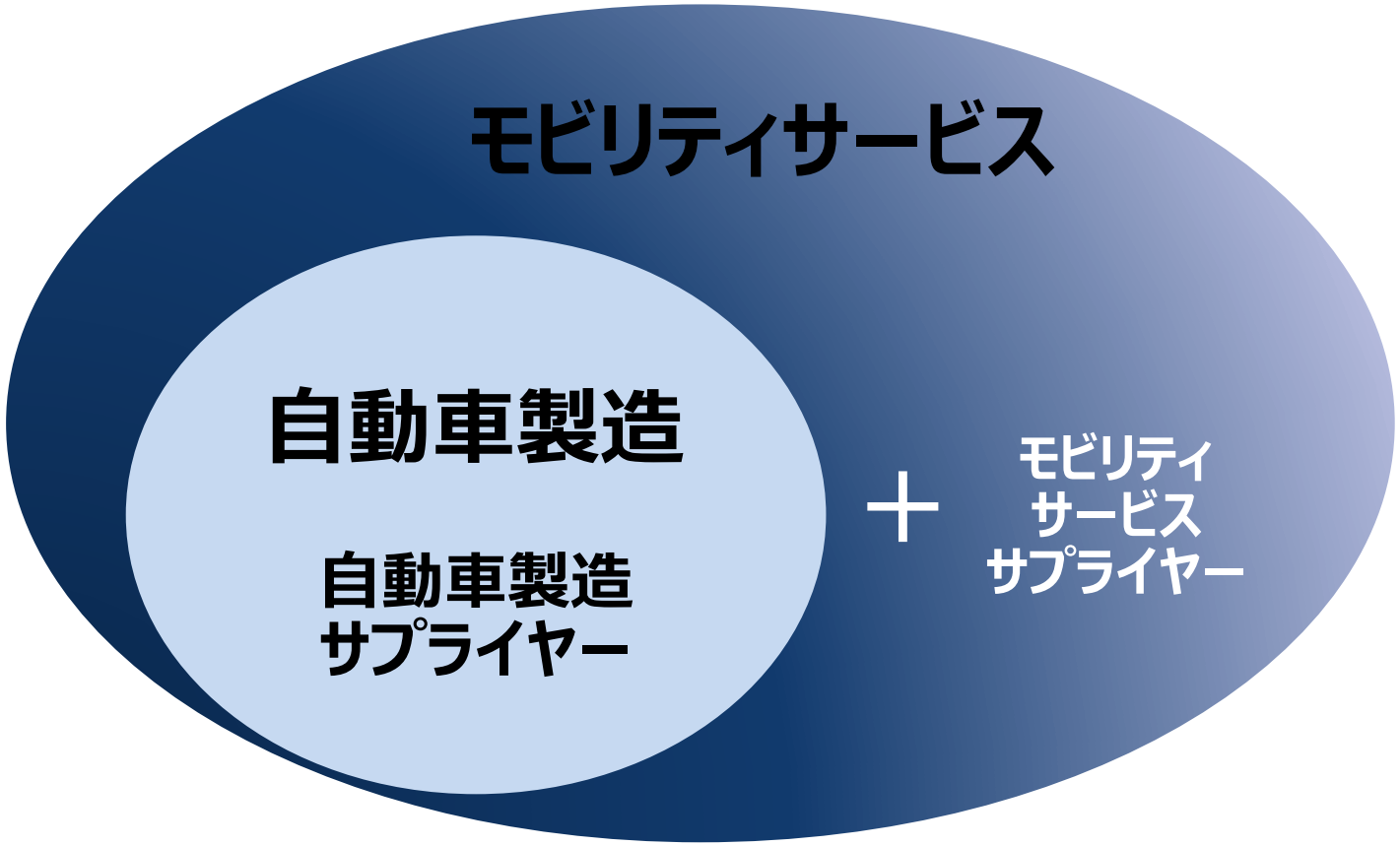
1. 自動車業界の特徴

2. 自動車業界のサプライチェーンセキュリティリスク

3. 自動車業界のサイバーセキュリティへの取組み

1-1. 自動車業界の特徴

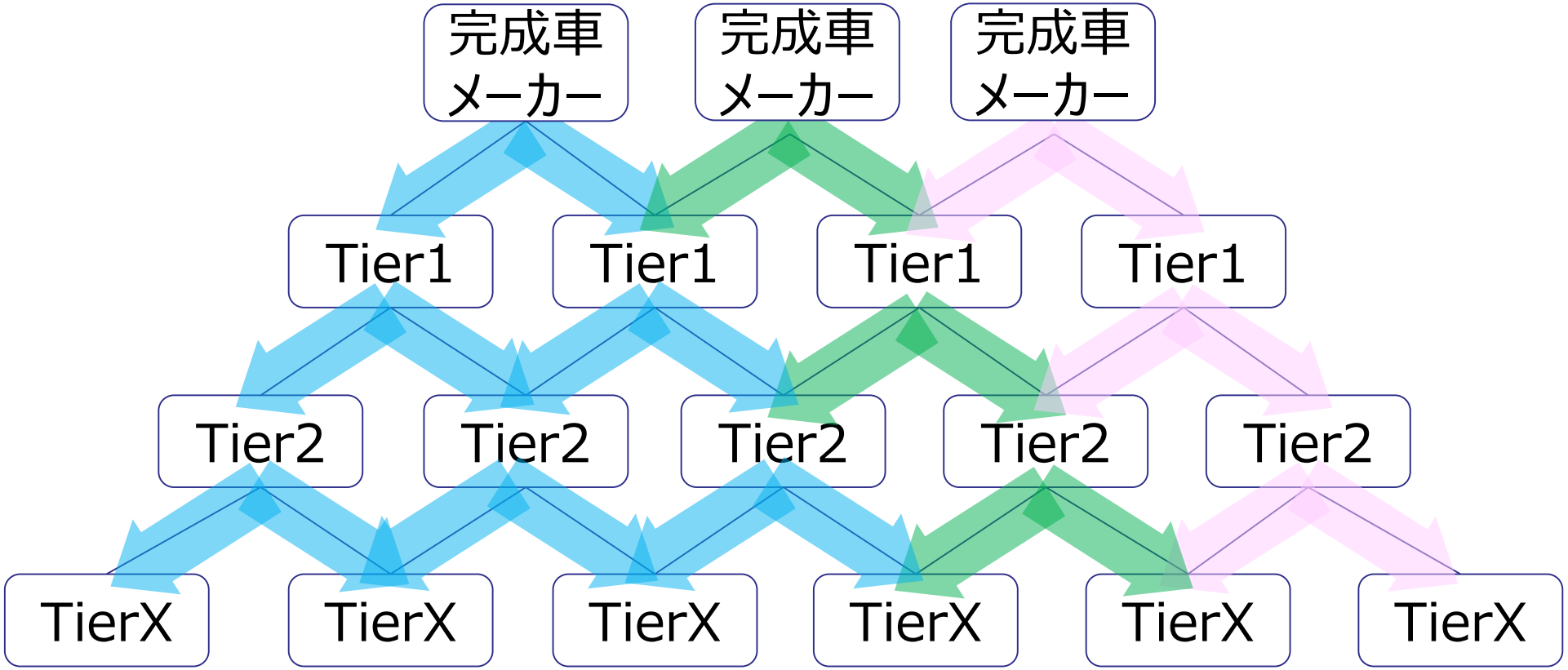
・次世代のモビリティビジネスへの構造変化に伴い、**サプライヤーも拡大** **(モビリティサービスサプライヤー等)**
・取り扱う情報も**機密情報**が多く、**データ量も増加傾向**



保有情報	詳細
車両情報	・位置情報 ・速度情報 ・エンジン情報 ・制御系情報　など
技術情報	・図面 ・ＣＡＤデータ ・Ｒ＆Ｄ情報 ・デザイン　など
プライバシー情報	・個人情報 ・家族情報 ・金融情報 ・所有車情報　など

1-2. 自動車業界の特徴

・完成車メーカー,Tier1,Tier2仕入先…と多層で幅広いサプライチェーン



1. 自動車業界の特徴

2. 自動車業界のサプライチェーンセキュリティリスク

3. 自動車業界のサイバーセキュリティへの取組み

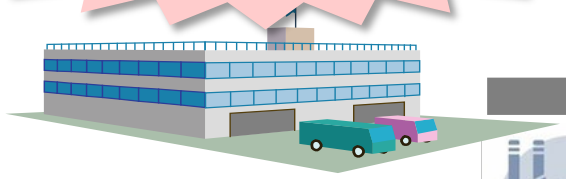
2-1. 自動車業界のサプライチェーンセキュリティリスク

・**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

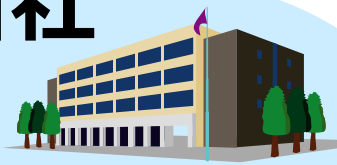
・**部品調達**できない
・**物流停止**

内部不正による
情報漏洩

自社



工場



オフィス

部品メーカー

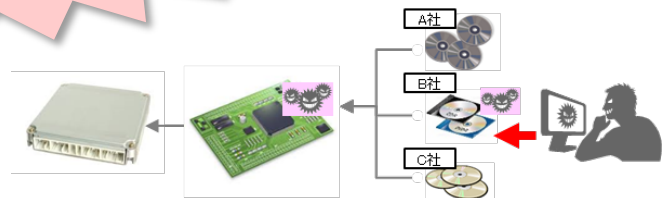
委託先

・製品への**不正プログラム**埋め込み
・**製品に脆弱性**

ソフトウェアベンダー

サービス事業者

関係先経由の
踏み台攻撃



2-2. サイバー攻撃による主なリスク

① 事業停止リスク

サイバー攻撃は事業継続に直接的な影響を及ぼすことが多い（後述）

② 訴訟リスク

セキュリティ対策を怠ると、経営層に対する責任追及に及ぶ場合もあり。

③ 株価下落リスク

情報が流出した場合は、株価が平均でも10%下落。

出典：一般社団法人日本サイバーセキュリティ・イノベーション委員会（略称：JCIC）「サイバーリスクの数値化モデル」

2-3. サイバー攻撃によるリスク①：事業停止リスク

・サプライチェーン攻撃により**完成車の生産操業停止に至った**
→ **サイバー攻撃が事業継続に直接的な影響を及ぼした例**

サプライチェーン攻撃による操業停止の事例

概要

■2022年2月、取引先の部品メーカーでのシステム障害を受け、国内全て(14拠点28ライン)の工場停止を公表した。

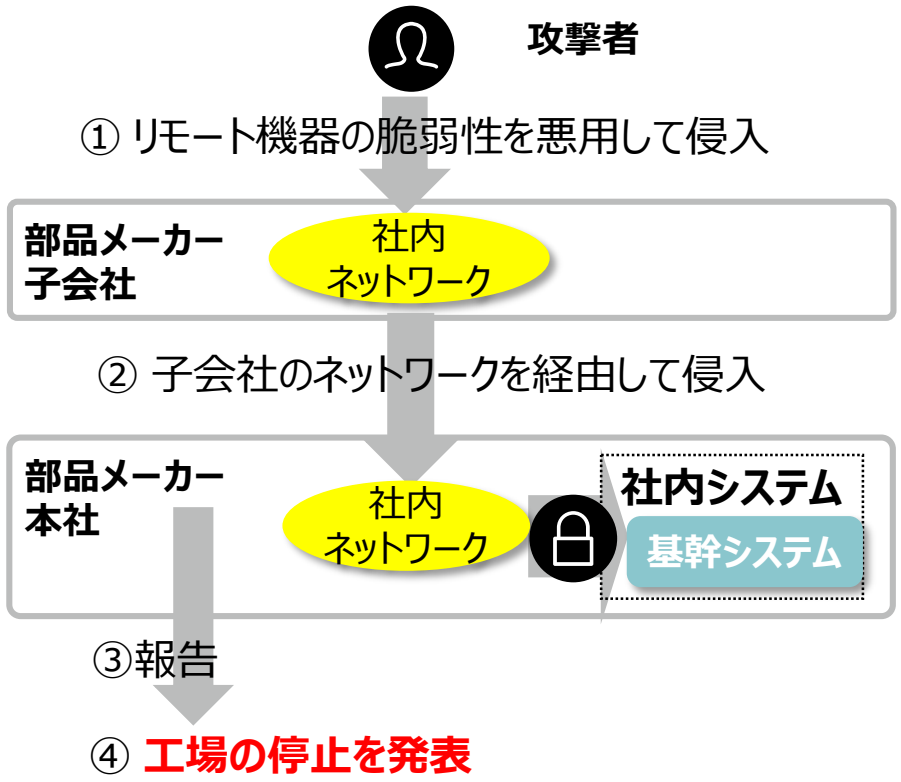
■部品メーカー子会社が利用していたリモート接続機器の脆弱性を悪用し、ネットワークに侵入、更に部品メーカー本社のネットワークに侵入された。

■結果、メール等の社内システム等が稼働できなかった他、部品発注・受注や納品データのやり取りをする**基幹システムが停止。**

影響

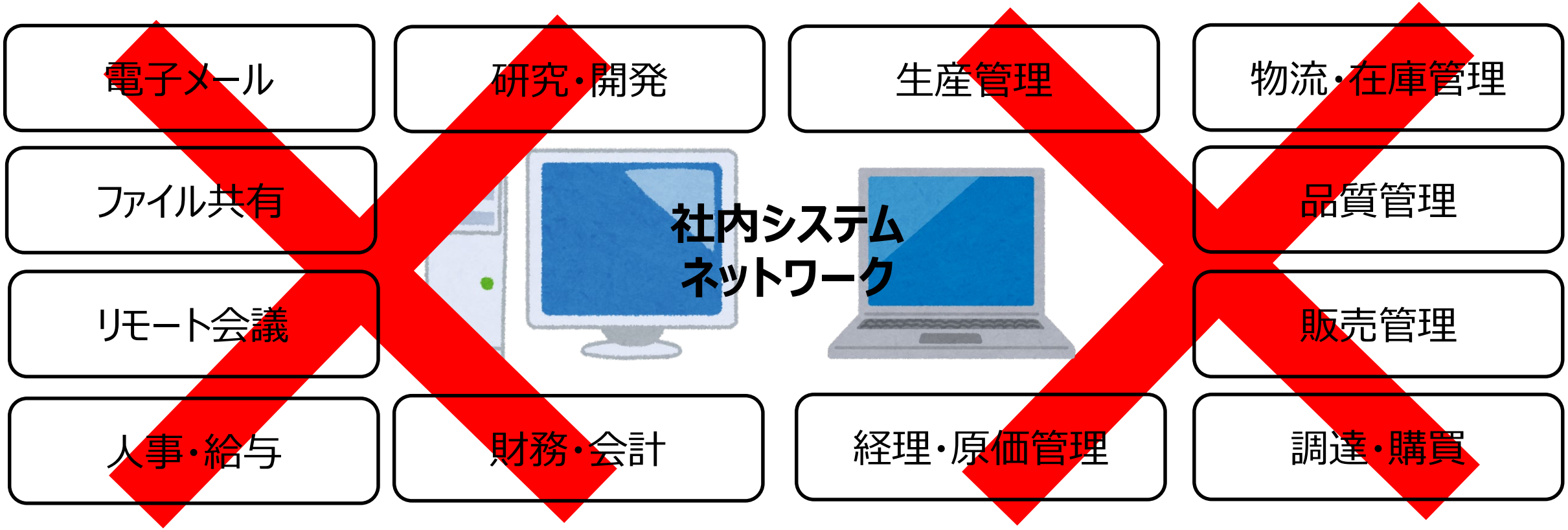
■**国内全ての工場が停止したことで(一日間)、約1万台強の生産に影響**、同年1月の月間生産台数5%に相当するといわれている

事案の全体像（公開情報からの推測）



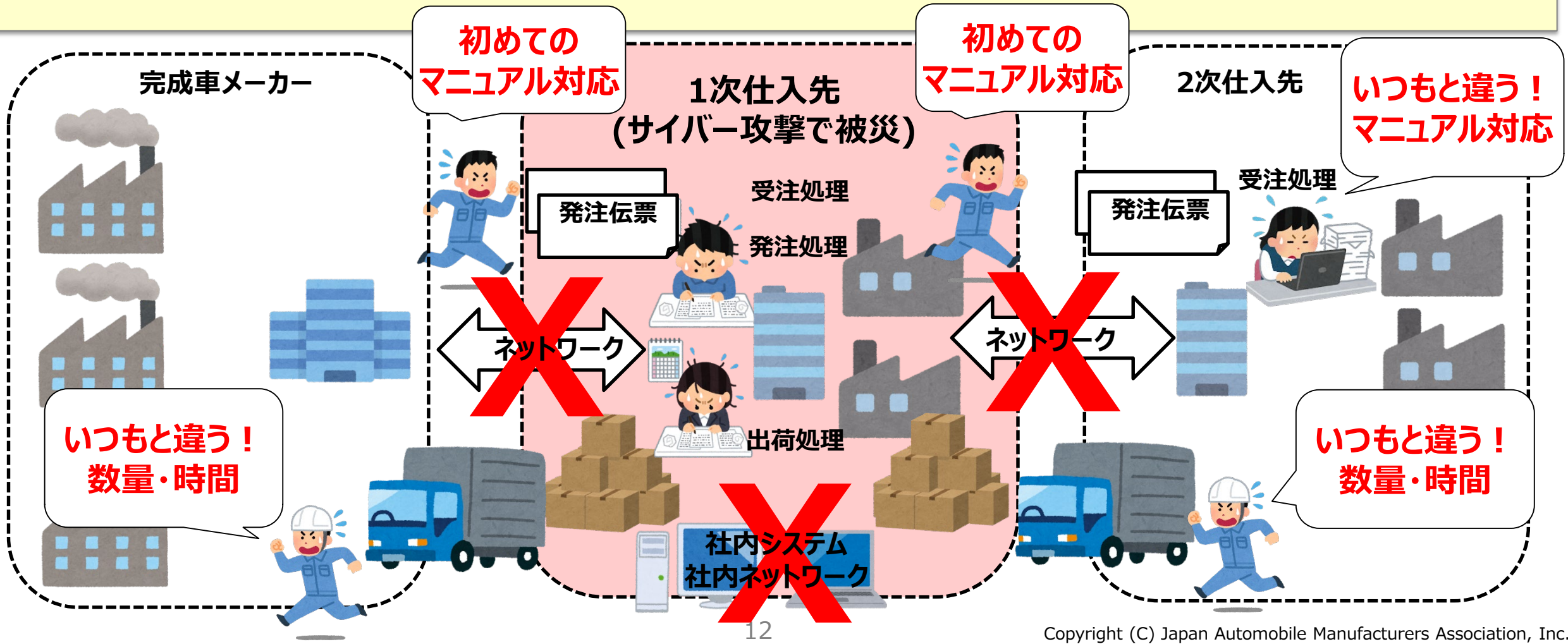
2-4. サイバー攻撃によるリスク①：事業停止リスク　詳細(1)

- 停止システムは、受発注・出荷システムだけに限らず、**全ITシステムが停止**
  →全てをマニュアルで処理しなくてはならない
- **現場の社員の負荷・心理的重圧は非常に高い**



2-4. サイバー攻撃によるリスク①：事業停止リスク　詳細(2)

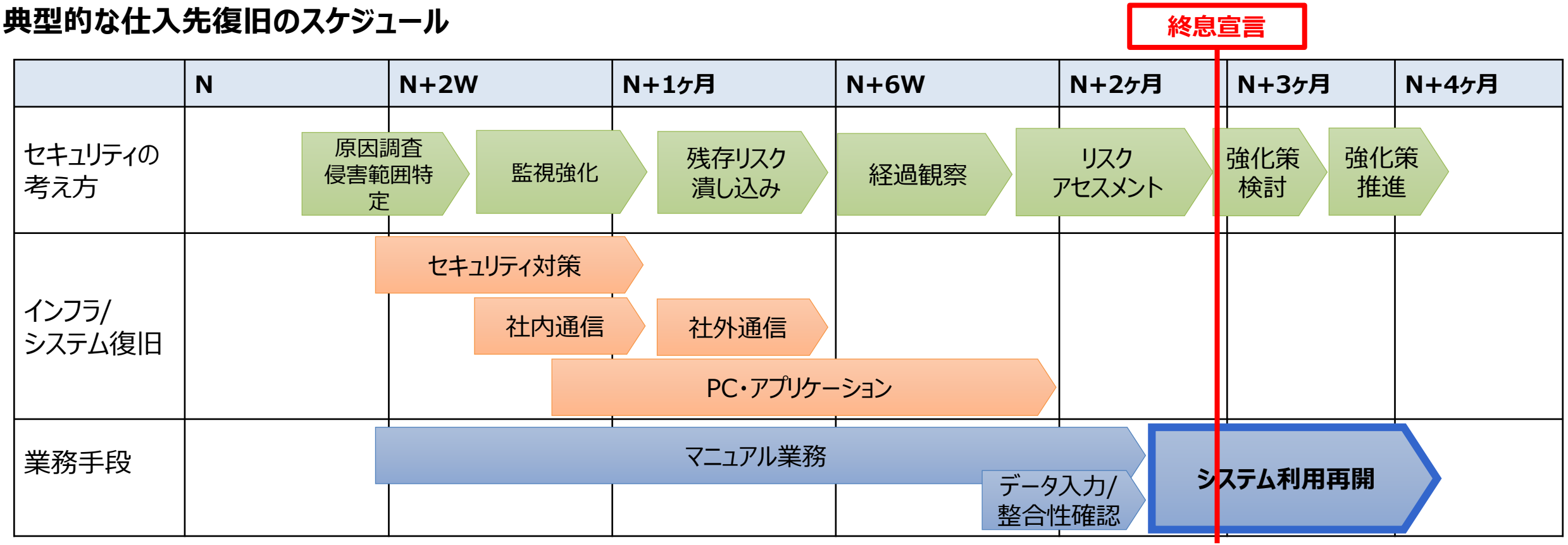
- ネットワークや社内システムを遮断する為、**マニュアルで受発注・出荷等を行い生産を継続**
- **影響は、**自社・納入先・発注先(2次仕入先)・物流など**サプライチェーン全体に広がる**



2-4. サイバー攻撃によるリスク①：事業停止リスク　詳細(3)

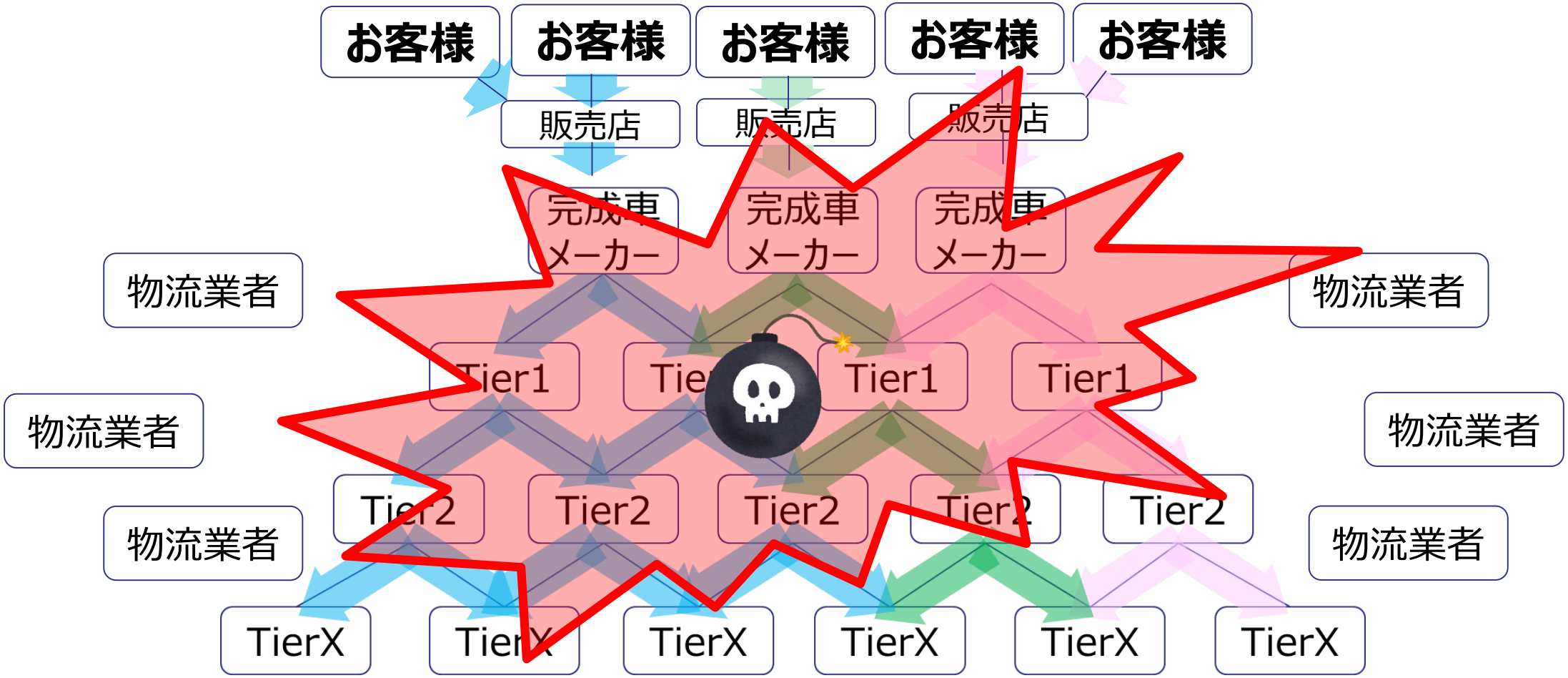
- マニュアル対応で納入先や発注先の業務は継続できても、**自社のシステムや業務オペレーションが元通りになるには数か月かかることが多い**
- 自社への経営インパクト大 ⇒ **セキュリティは全社の経営課題**

典型的な仕入先復旧のスケジュール



2-5. サイバー攻撃によるリスクの影響範囲

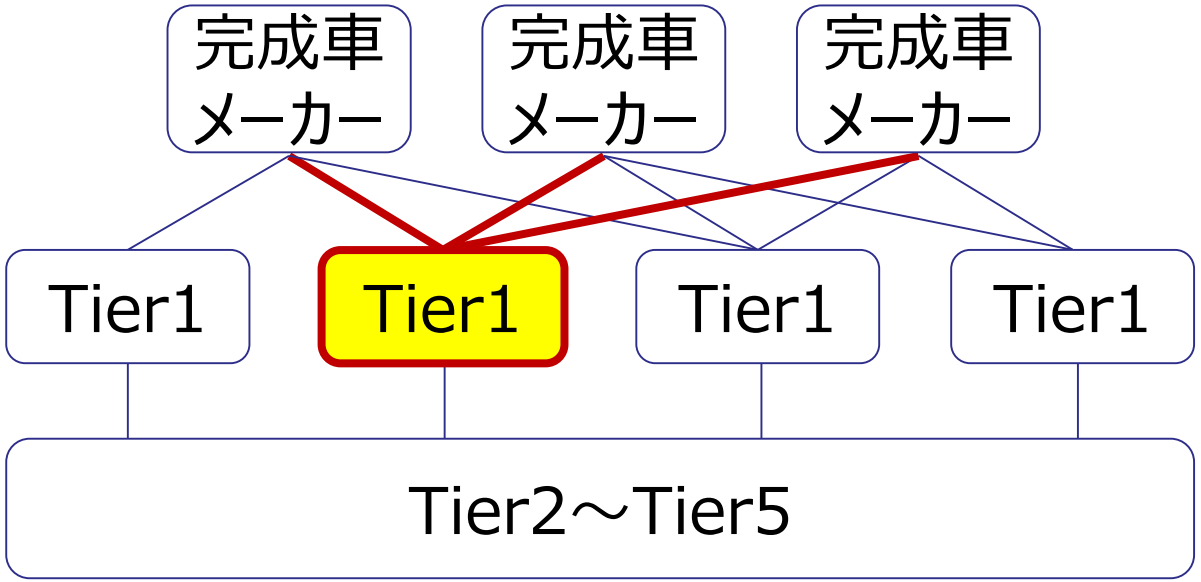
- サプライチェーンは密接に繋がっている
- **自社のリスク ⇒ サプライチェーン全体のリスク ⇒ 消費者であるお客様へのリスク**

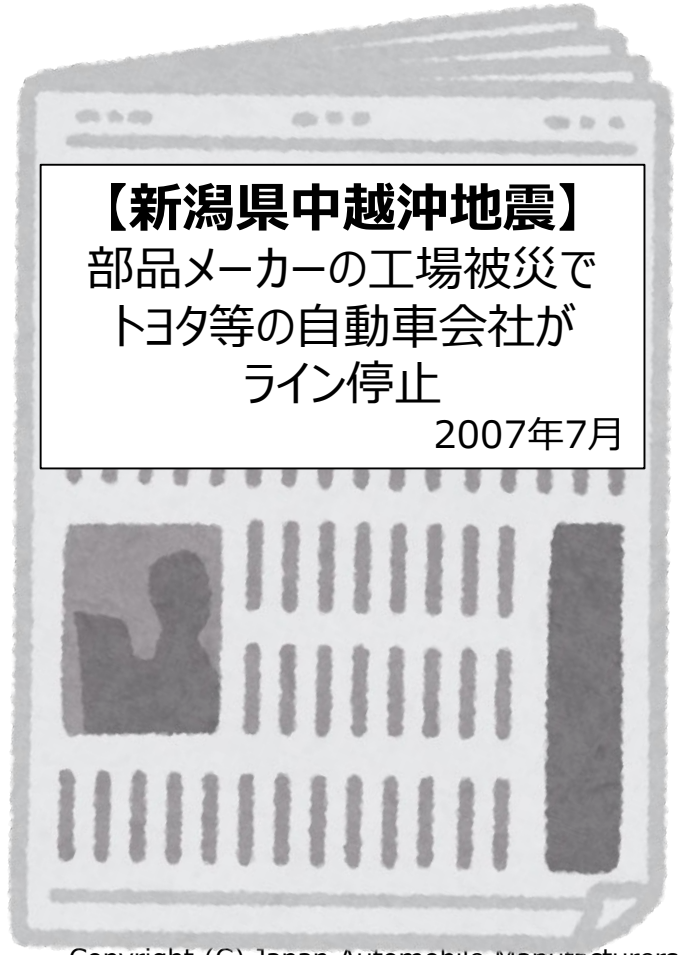


2-6. 大規模サプライチェーン リスク事例

・サプライヤーの業務が停止した場合に、自動車業界への影響は大
・**サイバー攻撃によるサプライヤーの生産停止も同様**の影響が発生

＜自然災害の事例＞
新潟県中越沖地震
⇒**1社の停止が、複数の完成車メーカー製造停止へ**





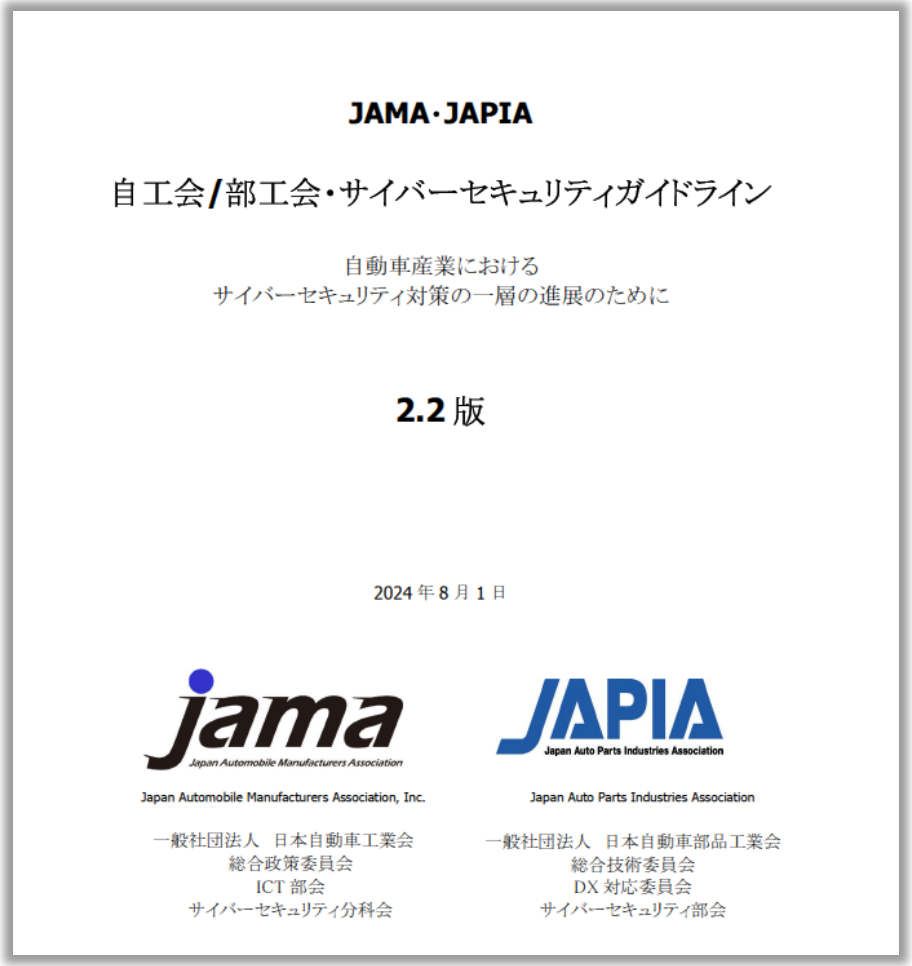
1. 自動車業界の特徴

2. 自動車業界のサプライチェーンセキュリティリスク

3. 自動車業界のサイバーセキュリティへの取組み

3-1. セキュリティガイドラインの概要

- **全６項のガイドライン**と**付録**として自社のセキュリティ対策の取り組み状況をセルフ評価し、対策レベルの効率的な点検を行うための**チェックシートで構成**



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

2.2 版

2024 年 8 月 1 日

Japan Automobile Manufacturers Association, Inc.

一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
総合技術委員会
DX 対応委員会
サイバーセキュリティ部会

目次

3-2. セキュリティガイドラインの概要

・取り扱う情報により、**標準的／最終到達点として目指すべき項目**
２４項目のラベル、３７項目の要求事項、１５３項目の達成条件を記述

自動車産業 セキュリティチェックシート(V2.2)

会社名	●●株式会社	評価範囲	▽プルダウンから選択ください	目標レベル	▽プルダウンから選択ください
会社分類	▽プルダウンから選択ください	会社従業員数	▽プルダウンから選択ください		
担当者メールアドレス ※共有先に公開されます		提出済みチェックシートの差し替え、共有先追加の場合は、右のプルダウンから「差し替え」を選択してください。	新規		

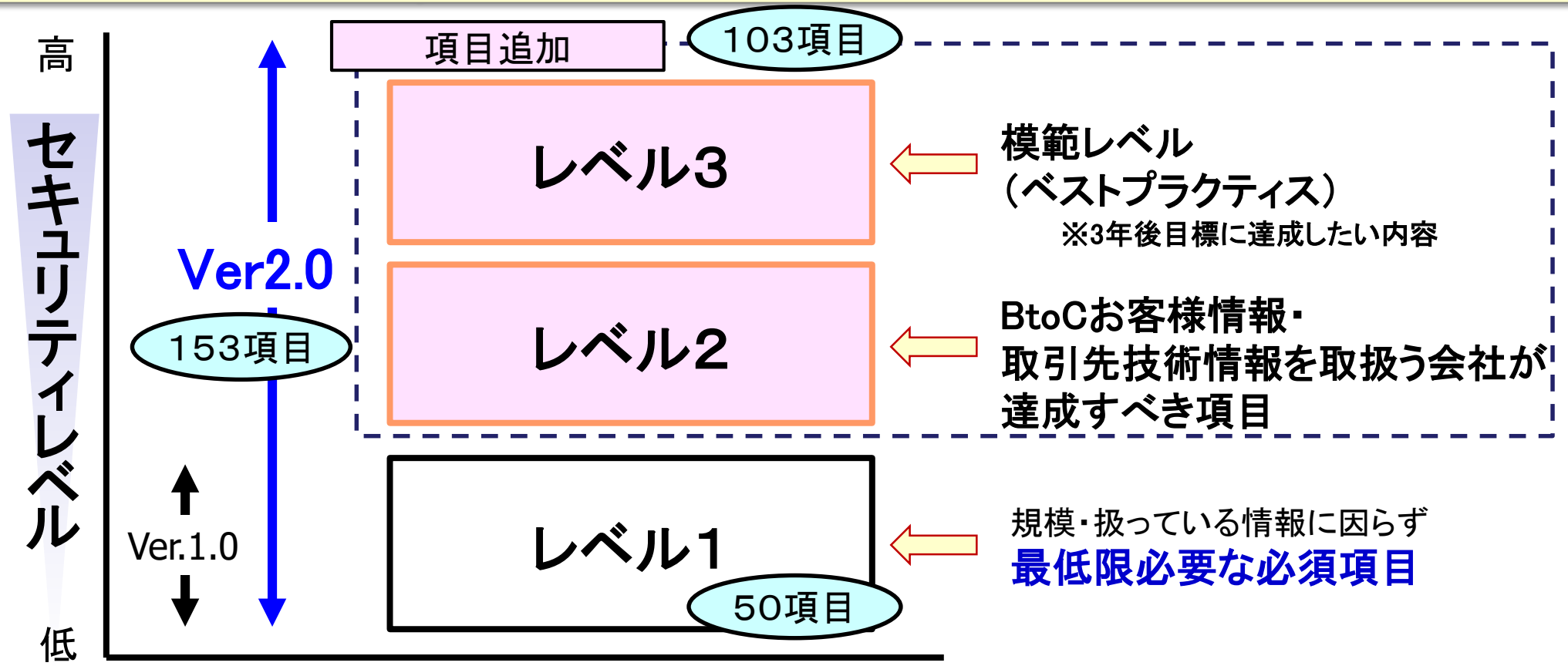
分類	ラベル	目的	要求事項	No.	レベル	達成条件	達成基準	評価結果 達成条件評価	評価結果 評価の根拠記入欄 ■対策完了(2点)：規程名、導入システム/策定・改定・導入年 ■対策中(1点)：現状と完了予定時期 ■未実施(0点)：今後の改善計画 ■該当なし：該当しないと判断した理由
共通	1方針	会社として、セキュリティに対する基本的な考え方や方針を示し、社内の情報セキュリティ意識を向上させる	自社の情報セキュリティ対応方針を策定し自組織内に周知していること	1	Lv1	自社の情報セキュリティ対応方針(ポリシー)を策定している	・自社の情報セキュリティ対応方針を策定し、文書化すること	▽プルダウンで評価ください	
				2	Lv2	自社の情報セキュリティ対応方針(ポリシー)の内容を確認し、必要に応じて見直ししている	【規則】 ・社内外の環境変化を踏まえて、内容を確認し、適宜見直ししていること 【頻度】 ・情報セキュリティ対応方針(ポリシー)の内容を確認、改善 -1回以上/年 ※別途、重大な変化が発生した場合には迅速に対応すること	▽プルダウンで評価ください	
				3	Lv1	情報セキュリティ対応方針(ポリシー)を社内に周知している	【規則】 ・情報セキュリティ対応方針(ポリシー)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】 ・定常的に、かつ、情報セキュリティ対応方針の改正時に周知すること	▽プルダウンで評価ください	
	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	4	Lv1	自社の守秘義務のルールを規定し、守らせている	【規則】 ・自社の守秘義務を策定し、文書化すること ・入社時あるいは社外要員の受け入れ時に守秘義務を説明すること ・退職もしくは期間満了時に会社の機密情報を持ち出さないこと 【対象】 ・役員、従業員、社外要員（派遣社員等）	▽プルダウンで評価ください	

24項目 **37項目** **153項目**

3-3.自動車業界が求めるセキュリティレベル

① 自動車業界の多くの会社のレベルアップを優先するため、**企業規模に因らず、最低限必要な必須項目（レベル１）を策定（V1.0）**

② V2.0としてお客様情報・取引先技術情報を扱う会社向けに、
レベルアップ版（レベル２，３）を追加 (22年度発行) ※誤記修正等を行い最新版はV2.2



3-4. セキュリティガイドラインでの優先ポイント

- **基本的な対策に加えて、災害時の備えを推奨**

IPA 様より公表されているセキュリティアクション

情報セキュリティ5か条
①OSやソフトウェアは常に最新の状態にしよう！
②ウイルス対策ソフトを導入しよう！
③パスワードを強化しよう！
④共有設定を見直そう！
⑤脅威や攻撃の手口を知ろう！

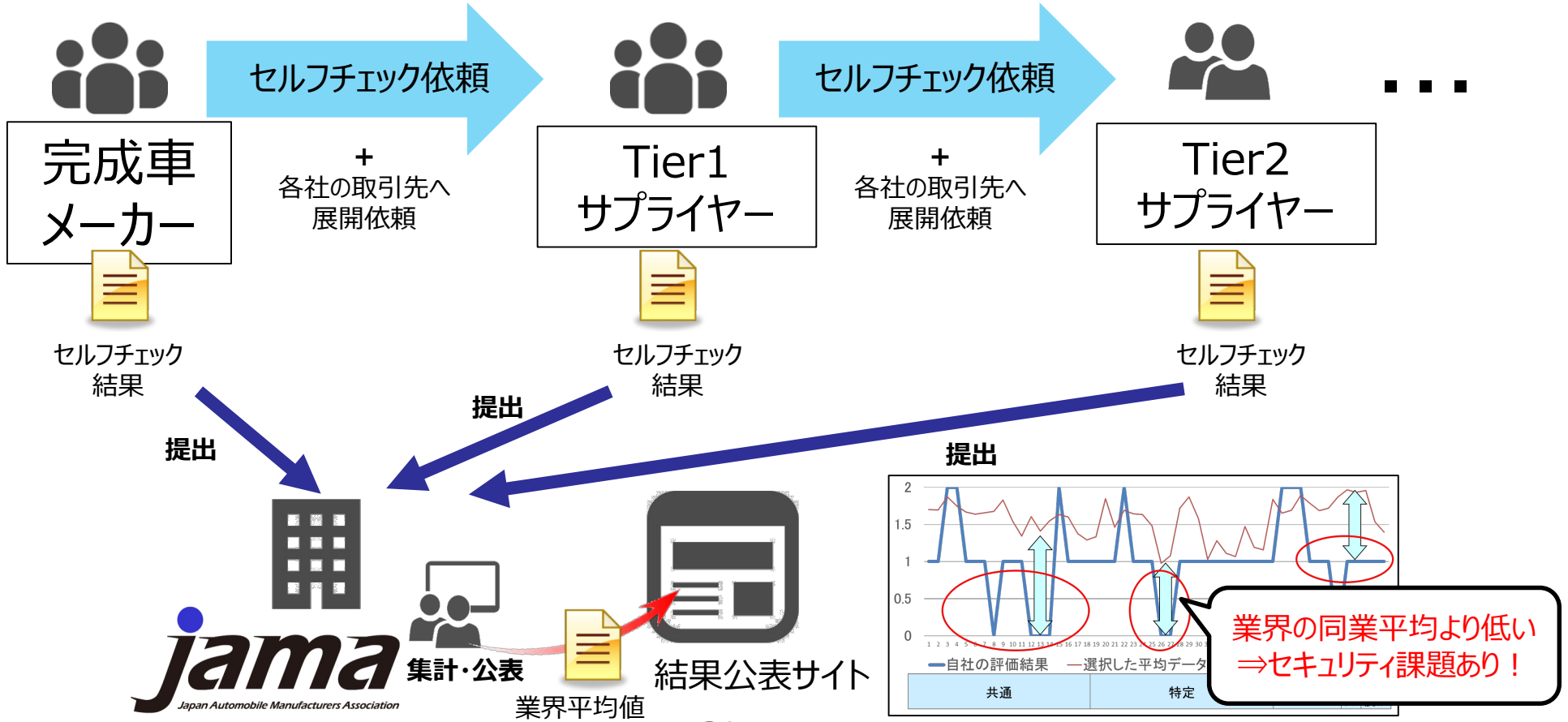
＋

jama 自動車業界での追加3項目 JAPIA

セキュリティ事故災害時の備え
⑥緊急時の対応手順や連絡方法の再確認
⑦ネットワーク外でのバックアップ・データ保管
⑧サーバーダウン時の生産継続方法の検討

3-5. サプライチェーンへの展開の流れ

- 24年度も 業界全体に対して、セキュリティレベルのセルフチェックの依頼を実施
- 業界平均と自社セルフチェック結果との差異から**重点課題の認識＆レベルアップ**
  → **業界全体のセキュリティレベル向上へ**



3-6.自動車業界サプライチェーンでの対応状況

- **2024年度は約３１００社が自己評価を実施**（分析/評価中）
- **2023年度では、全てのレベル項目において、’22年度よりも平均点が向上**
  約20%程の会社では、まだレベル1。レベル2以上へのセキュリティレベル向上が必要

年度	回答総数	有効回答総数	平均点
2023	3,240 社	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%)
2022	4,026 社	3,961 社	ﾚﾍﾞﾙ 1 項目：76.95 /100 点 (77.0%) ﾚﾍﾞﾙ 2 項目：110.49 /148 点 (74.7%) ﾚﾍﾞﾙ 3 項目：37.35 /58 点 (64.4%)
2021	2,300 社	2,296 社	ﾚﾍﾞﾙ 1 項目：70.97 /100 点 (71.0%)

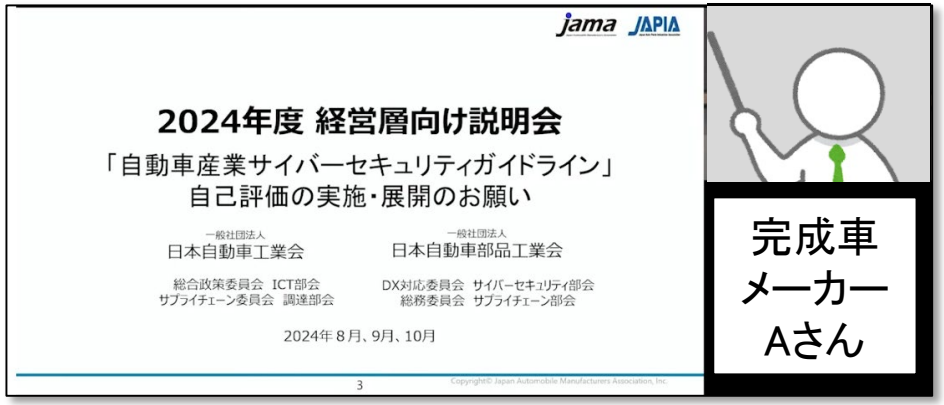
(2021 年度は V1.0 のため、レベル 1 項目のみ)
システム化により同一会社の重複が減少

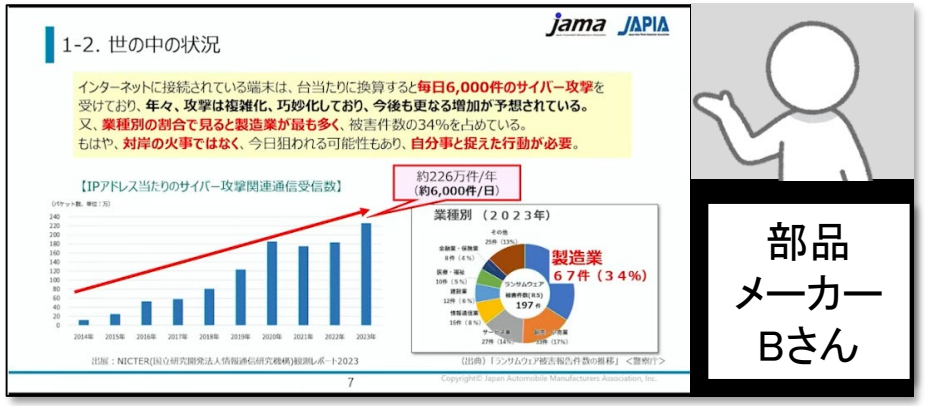
2023 年度平均点詳細

目標レベル	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	659 社	62.05 /100 点 (62.1%)	－	－	62.05 /100 点 (62.1%)
ﾚﾍﾞﾙ 2	1,830 社	85.42 /100 点 (85.4%)	116.84/148 点 (78.9%)	－	197.08 /248 点 (79.5%)
ﾚﾍﾞﾙ 3	751 社	94.46 /100 点 (94.5%)	136.34 /148 点 (92.1%)	42.91 /58 点 (74.0%)	258.03 /306 点 (84.3%)
計		81.84 /100 点 (81.8%)	120.00 /148 点 (81.1%)	42.91 /58 点 (74.0%)	－

3-7. 経営層巻き込みへのチャレンジ(1)

- **仕入先各社の困り事として、“経営層の巻き込み不足” あり**
- **『自動車産業サプライチェーン企業経営層向けサイバーセキュリティ説明会』を実施**
  （自工会・部工会共催で合計４回開催）





参加人数
約4000社、約6000人

＜参加者アンケート＞ 重要と感じた点

①	**経営に与えるリスク**	**[2400]**
②	**セキュリティ投資**	**[1800]**
③	セキュリティ人材育成	[1700]
④	事故を想定した構え	[1600]
⑤	経営層自らの言葉による浸透	[1400]

※複数回答有り

3-7. 経営層巻き込みへのチャレンジ(2)

● **重要性はご理解いただけたが、継続的なコストやリソース面で課題も浮き彫りになった**

分類	参加者の主な声
学び 	• サイバーセキュリティの重要性は良く聞くが、後回しになりがちだった。 **危機感の継続と意識向上につながった** • 従業員・現場に対して　**経営層が取り組んでいる姿を見せることの重要性** • **攻撃を受ける想定で準備が必要**だと強く感じました • 関連企業を巻き込んだ取り組みの大切さを感じた • システム関係者の業務と考えていたが、 **関係者一人ひとりが自分事として取り組めるような環境作りの重要性**を認識できた • セキュリティー対策は、惜しむことなく投資していくことが重要と認識できた （**セキュリティーへの対応はコストではなく投資**）
課題 	• **無料もしくは安価で実行できる**具体的な取り組みの方法も知りたい • 一部社員だけではなく、**全社的にセキュリティ意識を高める**こと • セキュリティには終わりがない、**小企業では継続的な資金面、人材面の対策が厳しい** • 裾野が広く、コストとの兼ね合いもあり**どこまでガバナンスを効かせて対応するのか悩ましい**

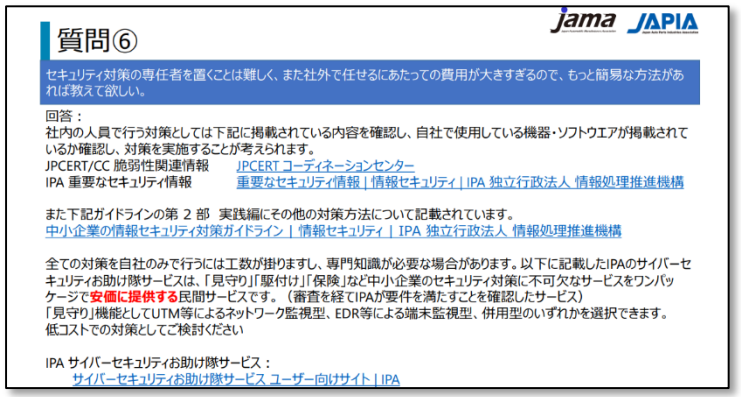
3-8. 仕入先各社でのお困り事への対応

● **自工会・部工会では、よろず相談会で仕入先各社のお困り事に対応**

【相談事例】

レベル１を目指してますが、**何から手を付けていいか分からない**状態です。

費用をかけずに、標的型メール訓練や内部侵入テストを実施したいです。
活用できるサービスや手法などがあれば教えてください。



➢ 詳しくは：

JAMA よろず相談会

５．まとめ

① サイバーセキュリティは経営リスク

② 被害は自社だけでなくサプライチェーン全体に影響が及ぶ場合もあり

③ 対策のやり方は政府（NISC, IPA）自工会・部工会などの情報をご参考

ご清聴ありがとうございました