2024年度 経営層向け説明会

「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

2024年８月、9月、10月

本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

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頂き

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）

をお願いする趣旨となります。

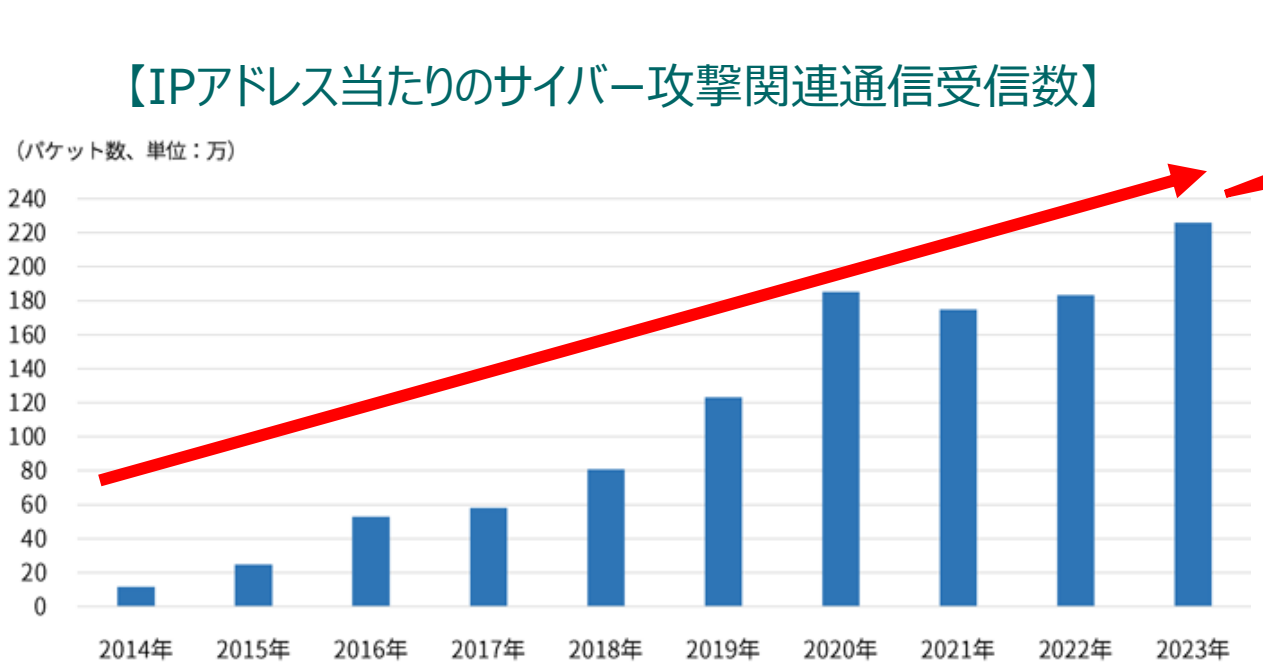
✓　本説明会の中では、**経済産業省様からご寄稿頂いた本活動へのメッセージ**もご紹介させて頂きます。

✓　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。

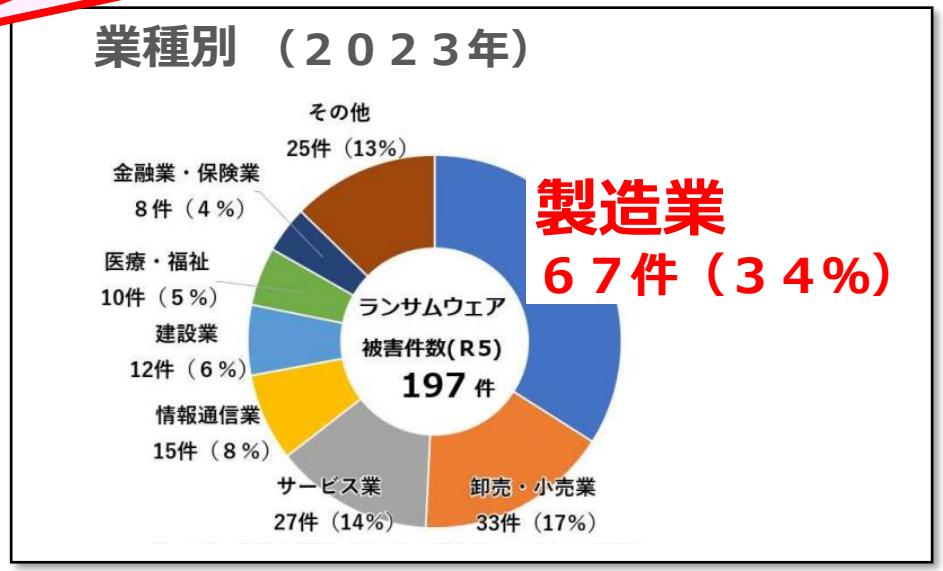
1-2. 世の中の状況

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6,000件のサイバー攻撃**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、**業種別の割合で見ると製造業が最も多く**、被害件数の34%を占めている。
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】



出展：NICTER(国立研究開発法人情報通信研究機構)観測レポート2023

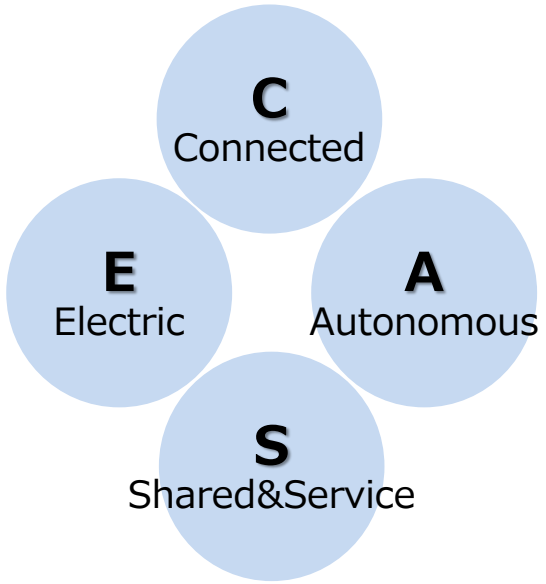


（出典）「ランサムウェア被害報告件数の推移」 ＜警察庁＞

1-3. 自動車業界の環境変化：扱うデータの変化

自動車業界は、CASEをはじめとして100年に一度の大変革期を迎えており、**業界全体がモビリティ社会の実現に向けてIT利活用を促進している。**このIT利活用促進に伴い、**取り扱う情報もデータ量も増加傾向にある。**

急速な技術革新

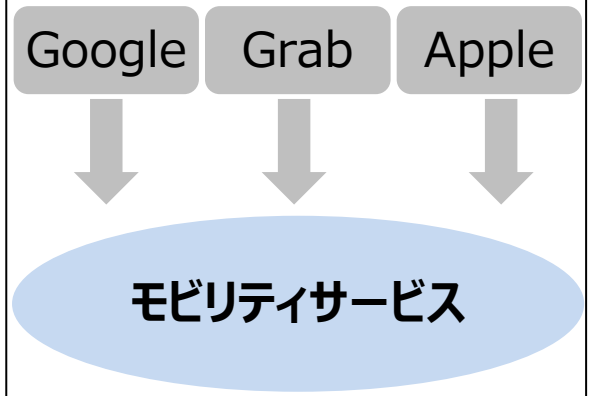


「コネクティッド」、「自動化」、「シェアリング」、「電動化」4つの革新が同時に発生(**CASE革命**)

競争領域の拡大

自動車製造からモビリティサービスへ
産業全体のドメインが大きく変化

競合企業の変化



電動化によりH/Wの重要性が低下、
自動運転/ｺﾈｸﾃｨｯﾄﾞ/ｼｪｱﾘﾝｸﾞ等
S/Wを主戦場とするﾌﾟﾚｰﾔｰが競合に

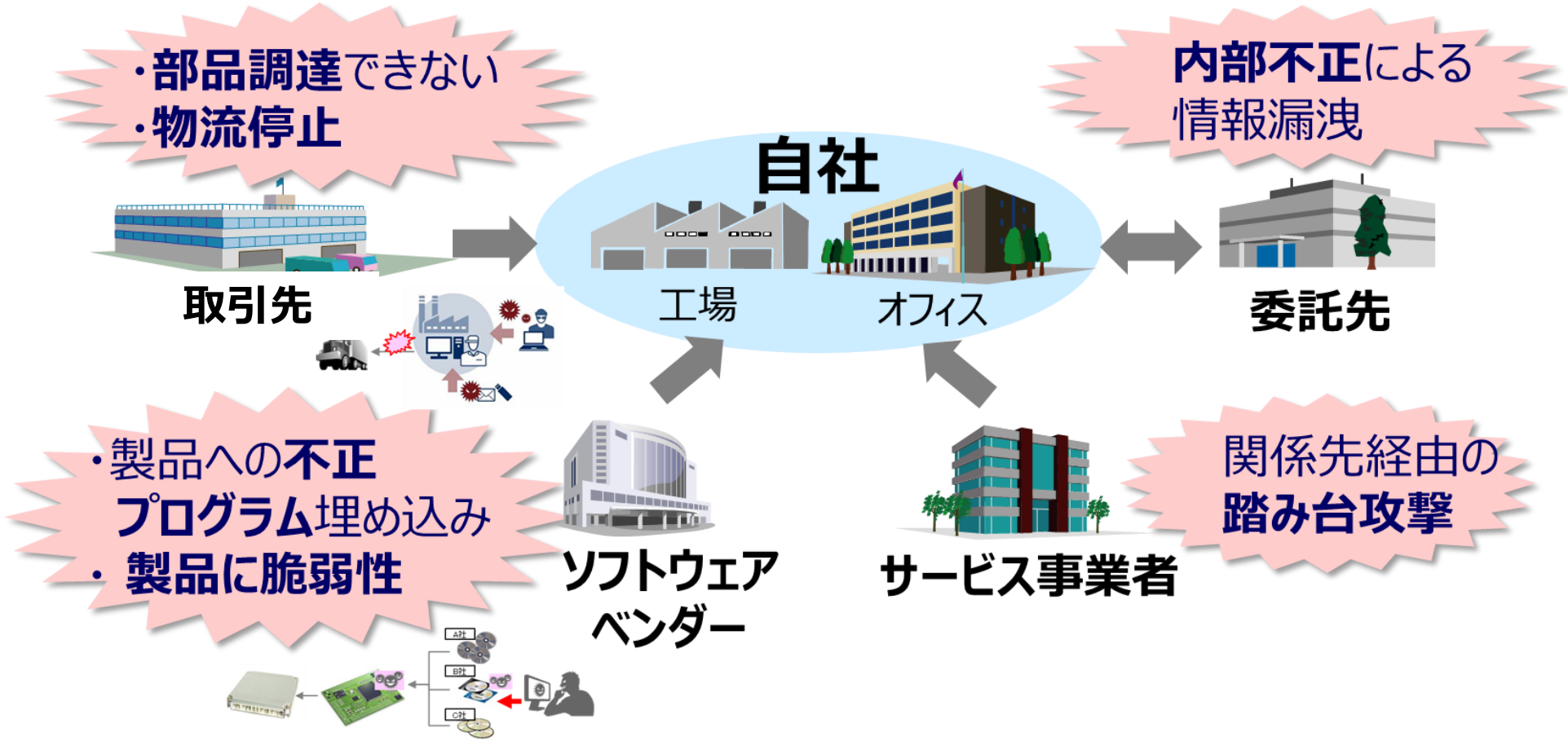
取り扱う情報の増加

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 ・開発情報 ・デザイン　など
プライバシー情報	・個人情報 ・金融情報 ・所有車情報　など

従来の情報に加え、電動化、スマート化に伴う**情報が大幅増加**

1-4. 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。



1-5. 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）

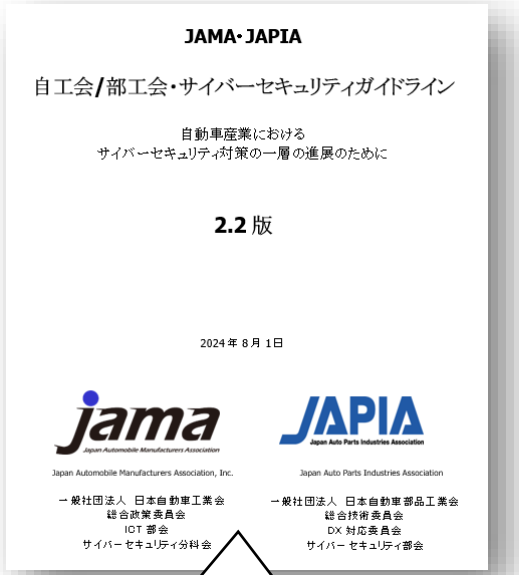
Industry by Industryで検討

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

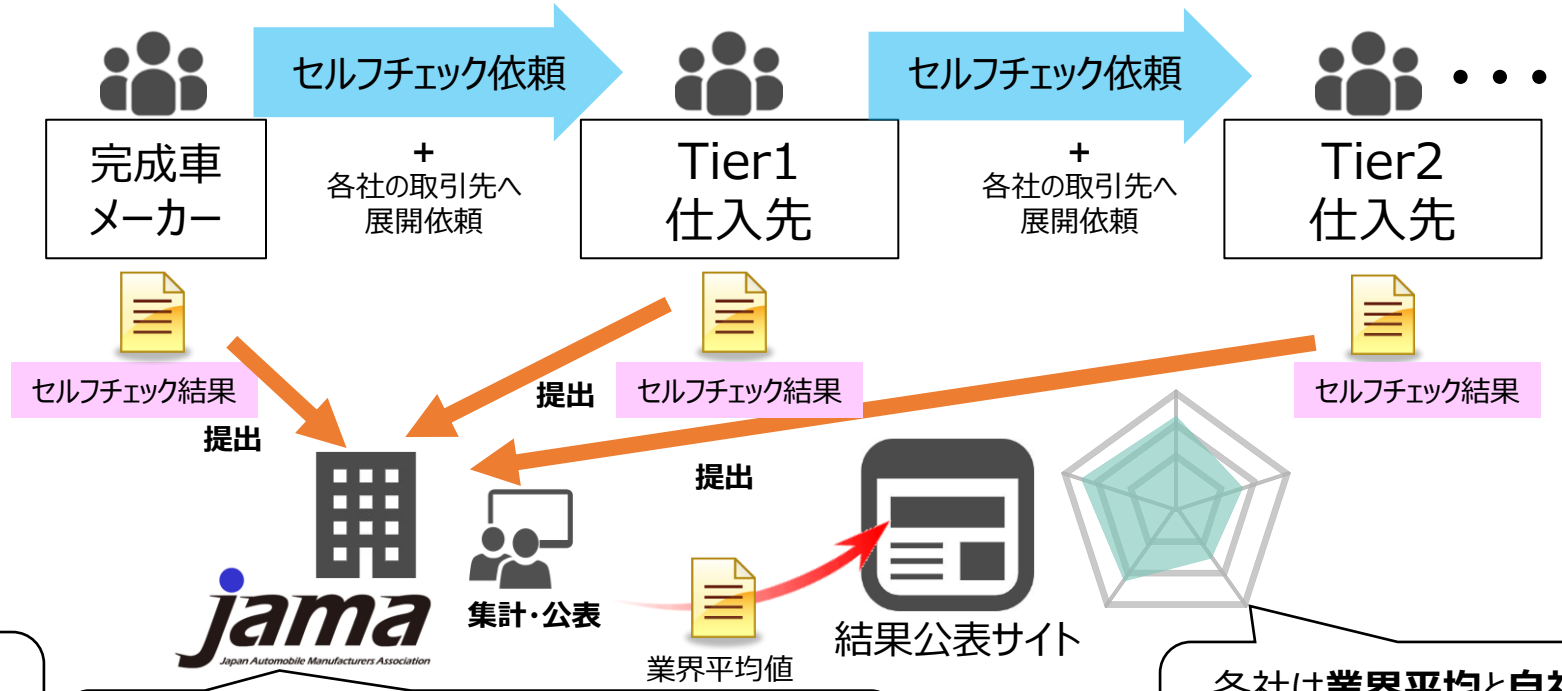
出典：経産省「産業分野におけるサイバーセキュリティ政策」資料

1-6. 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

本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

2-1. 経済産業省/奥家敏和様のご紹介

おくや　　としかず
奥家　敏和　　様

大臣官房審議官
(商務情報政策局担当)

1995年（平成7年）に通商産業省（現経済産業省）入省。マクロ経済分析、科学技術戦略、公務員制度改革、情報システム高信頼など様々な業務を担当した後、2010年より日本貿易振興機構（ジェトロ）New York Centerにて産業調査員を務める。2013年から資源エネルギー庁需給政策室長として日本の第4次エネルギー基本計画の策定等を担当し、2015年より安全保障貿易管理政策に従事。2016年より安全保障貿易管理政策課長として対内直接投資規制等を強化する外為法改正等に取り組んだ。**2017年7月より商務情報政策局サイバーセキュリティ課長、2021年7月より商務情報政策局総務課長、2022年7月より経済産業政策局総務課長、2024年7月より、現職。**

«職歴»

1995年	通商産業省入省
2003年8月	ハーバード大学　研究員
2004年8月	ハーバード大学ケネディスクールミッドキャリア(修士)
2010年7月	日本貿易振興機構出向 JETRO New York Center 産業調査員
2013年6月	資源エネルギー庁　長官官房総合政策課　需給政策室長
	(併　調査広報室長（2014年6月）)
2015年6月	経済産業省　貿易経済協力局　貿易管理部安全保障貿易管理課　課長
2016年6月	同部　安全保障貿易管理政策課　課長
2017年7月	経済産業省　**商務情報政策局　サイバーセキュリティ課　課長**
2021年7月	経済産業省　**商務情報政策局　総務課　課長**
2022年7月	経済産業省　**経済産業政策局　総務課　課長**
2024年7月	現職

2-2. ご寄稿動画

※動画配布権限管理の都合により削除させて頂きました。

2-3. ご寄稿動画へのお礼

- ✓ 経済産業省/奥家敏和様からメッセージをご寄稿頂きました。ありがとうございました。

- ✓ ここからは、実際の事例を踏まえた経営層としての心構えについて解説していきます。
  又、併せて24年度自己評価のお願いについて説明します。

本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

実際の被害事例

3-1. 世の中での被害事例

主なリスク	発生組織	被害の概要	
業務停止	自動車部品製造	• 2022年2月、自社で発生した**ランサムウェア攻撃被害**に起因して、取引先である自動車製造メーカーへ波及、**14工場28ラインが停止**	ランサムウェア サプライチェーン
	名古屋港	• 2023年7月、名古屋港コンテナターミナルで**ランサムウェアによるシステム障害**が発生し、およそ**3日間に渡りターミナルの操業が停止**。最終的に約2万本のコンテナ搬出入に影響があった	ランサムウェア
	関西地方の総合医療センター	• 2022年10月、総合医療センターが**ランサムウェア攻撃**により**緊急以外の手術や外来診療を停止**	ランサムウェア
機密情報・個人情報漏洩	出版	• 2024年6月、グループ会社のデータセンターのサーバーが**サイバー攻撃を**受け、システム障害が発生、**グループ全体の事業に影響**。従業員個人情報の他、取引先との契約書、学校法人の生徒の**個人情報などが漏えい**	ランサムウェア サプライチェーン
	通信サービス	• 2023年11月、サーバーがサイバー攻撃を受け**約44万件の個人情報が流出**。更に2024年2月にも**従業員情報約5万7000件が流出**した可能性あり	ランサムウェア サプライチェーン
	電機製造	• 2020年1月、11月、翌年10月と相次いで**中国現法への不正アクセスを契機とした情報漏洩**が発生。漏洩した情報には**防衛関連情報2万件**が含まれ、**安全保障への影響も懸念**される	標的型攻撃 サプライチェーン

3-2. 名古屋港へのサイバー攻撃：概要

名古屋港(貿易額：年間約21兆円　※取り扱い貨物量で日本一)にて、サイバー攻撃被害が発生。
自動車メーカーの稼働停止やアパレルメーカーの入荷遅延等に影響発生した。

概要

- ✓ 2023年7月4日朝に名古屋港統一ターミナルシステム(NUTS)で障害が発生、名古屋港全ターミナルの作業停止
- ✓ **ランサムウェア感染によりシステムが暗号化され障害発生**
- ✓ **復旧を優先し、バックアップからシステムを復旧**、7月6日夕方(**障害発生から約3日**)に**全ターミナルで作業を再開**

影響

- ✓ 荷役スケジュールに影響が生じた船舶37隻
- ✓ 搬入・搬出に影響があったコンテナ約２万本
- ✓ 自動車メーカーの国内複数拠点の稼働停止
- ✓ アパレルメーカーにおける衣類の入荷遅延等
- ✓ **情報漏えいは確認されていない**

【ターミナル停止による影響】

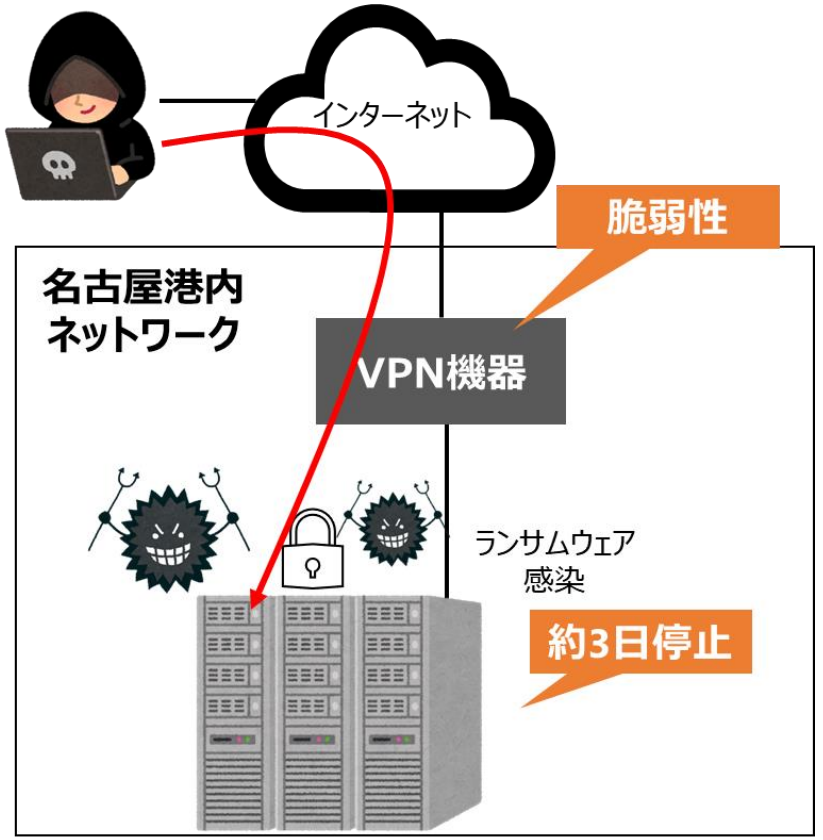
自動車メーカーの稼働停止や
アパレルメーカーの入荷遅延等に影響

3-3. 名古屋港へのサイバー攻撃：状況

保守用に利用していた**VPN装置の脆弱性を突いて不正にアクセスされた**可能性があったが、
復旧を優先させ調査・解析を行わず対応を進めた為、**感染経路の特定は出来ず。**
更には、**バックアップからもマルウェアが検知**され、駆除のために復旧時間が遅延した。

状況

- ✓ 保守用**VPN機器の脆弱性を突いた不正アクセス**の可能性
  ※**復旧を優先させたため、感染経路の特定は出来ず**
- ✓ データセンター内の全ての物理サーバー及び仮想サーバーが感染
- ✓ **データのバックアップを3日分しかとっておらず、バックアップからもマルウェアが検知**され、駆除のために復旧時間が遅延
- ✓ システム専用プリンターから約100枚の脅迫文書が印刷されたが
  脅迫文書に身代金額の記載はなく、攻撃者への連絡は行わず



3-4. 名古屋港へのサイバー攻撃：責任者の声

サイバー攻撃は、大企業向けにアタックをかけてるのかなというイメージがあった。

まさかこんな大がかりな攻撃が、**うちみたいな中小企業団体に襲いかかってくると言う事を、全く想定していなかった。**

出典：NHK： https://www3.nhk.or.jp/news/html/20230905/k10014183621000.html

3-5. 名古屋港へのサイバー攻撃：問題点と学び

問題点

①基本的な対策の不足
- 保守作業用VPNのセキュリティ対策の見落とし
- 不十分なウイルス対策
- インシデント調査に必要なログの保全
- バックアップ取得期間の不足

②インシデントを想定した備えの不足
- システム障害発生時の対応手順が未整備
- 初動時に専門家の意見を聞く場面がなかった
- 復旧時の健全性の確認・評価が十分

学び

①基本的な対策の実装状況を確認し、自社のリスクに応じた対策を継続的に進める

⇒ 自動車産業セキュリティガイドを活用して自社の対策レベルを把握、業界比較を通じ、**継続的な改善**

②事故を防ぐ対策に加えて、事故発生を想定し事前に備えておく

⇒ インシデント発生時の対応・復旧手順や全社的な組織体制・役割分担を明確にした**計画の策定**

⇒ インシデント発生を想定した**継続的な訓練の実施**

サイバーセキュリティ対策は経営課題、加えて強力な推進には経営のリーダーシップが不可欠

経営に与えるリスクの理解、自らの言葉による重要性の浸透、セキュリティ対応組織・体制確立、セキュリティ投資判断、他

経営層としての心構え

3-6. サイバー攻撃によるリスク：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** → **サイバー攻撃は、事業継続に直接的な影響を及ぼす**

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。

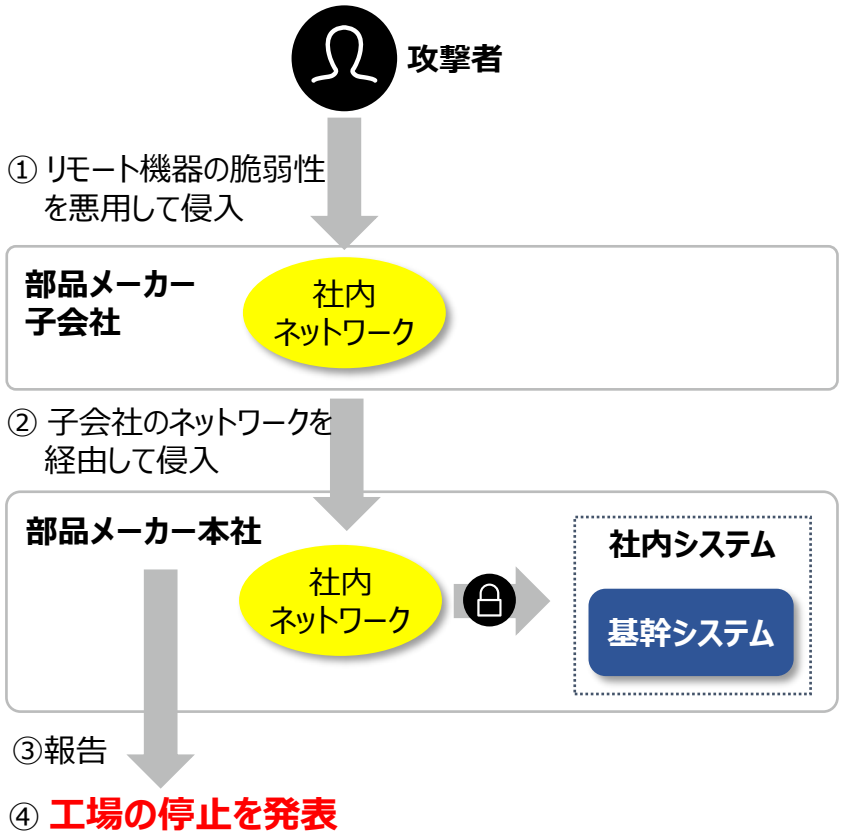
■部品メーカー子会社が利用していたリモート接続機器の脆弱性を悪用し、ネットワークに侵入、更に部品メーカー本社のネットワークに侵入された。

■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）



3-7. サイバー攻撃によるリスク：訴訟リスク

正規従業員IDを使った侵入＝**従業員情報が漏洩していた可能性があり、訴訟リスクの懸念**
→ **対策を怠ると、経営層に対する責任追及にも及ぶ**

訴訟リスクの事例

概要

■2023年6月、大手自動車製造関連会社の北米拠点にてサイバー攻撃被害が発生

■北米拠点にて利用していたリモート接続機器から正規従業員のIDを使って侵入、ネットワークに接続されていた各種サーバーが感染し、暗号化され、システム停止

■生産システム及び、メール等の社内システムは、外部システムを活用し稼働していた為、業務停止無し

影響

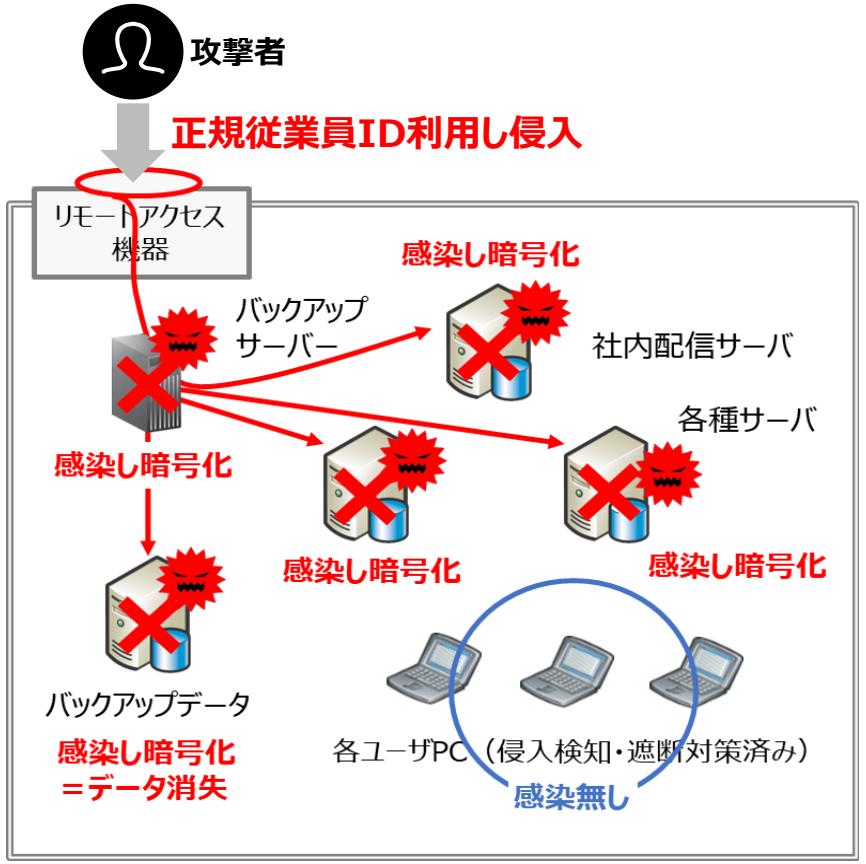
■社内全サーバー停止及び、社内ネットワーク停止

生産への影響は無し

■従業員の情報が漏洩している懸念有り、弁護士に相談

従業員から訴えられる可能性あり

事案の全体像

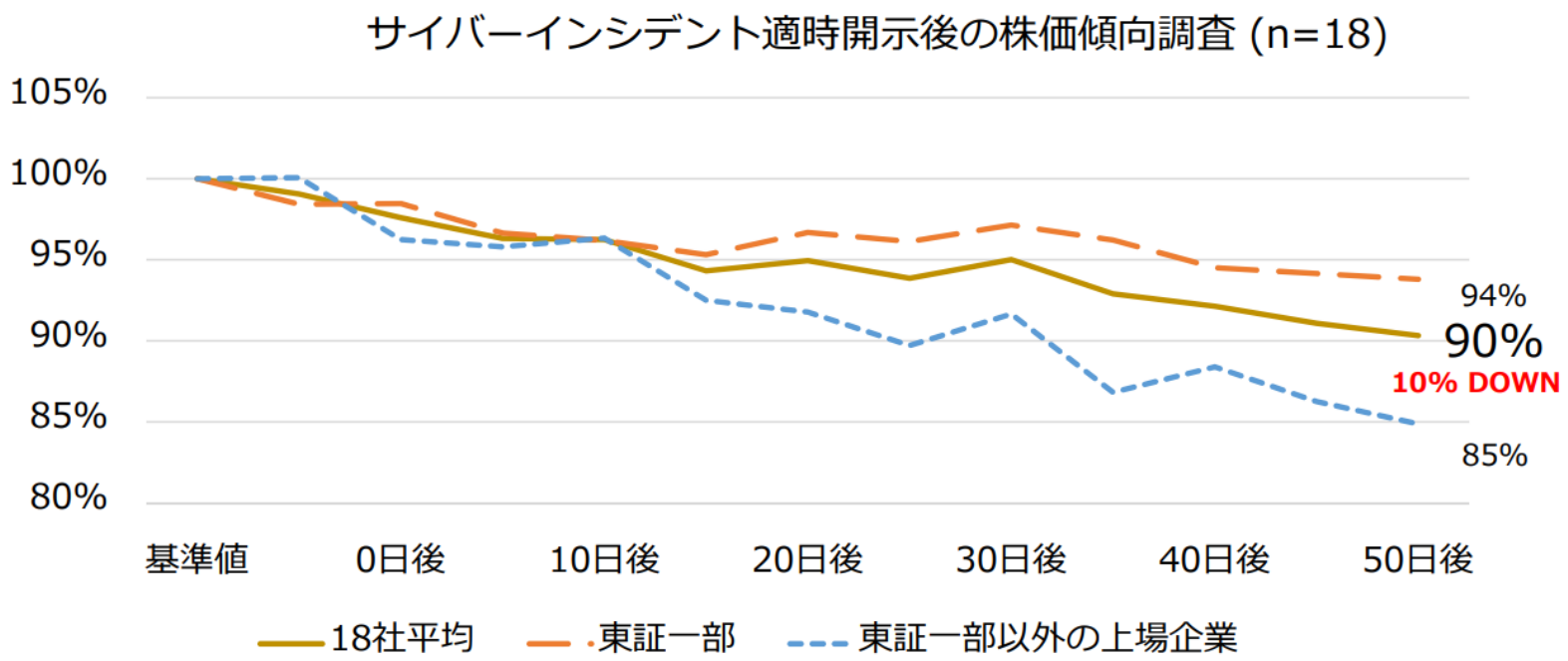


3-8. サイバー攻撃によるリスク：株価リスク

情報が流出した場合、**株価が平均で10%下落** → サイバー攻撃は、**企業価値にも直接的な影響を及ぼす**

サイバー攻撃が与える株価への影響

■日本国内で情報流出等が発生した場合、株価が **平均10%下落**
■特に、東証一部以外の企業は株価が **15%下落**

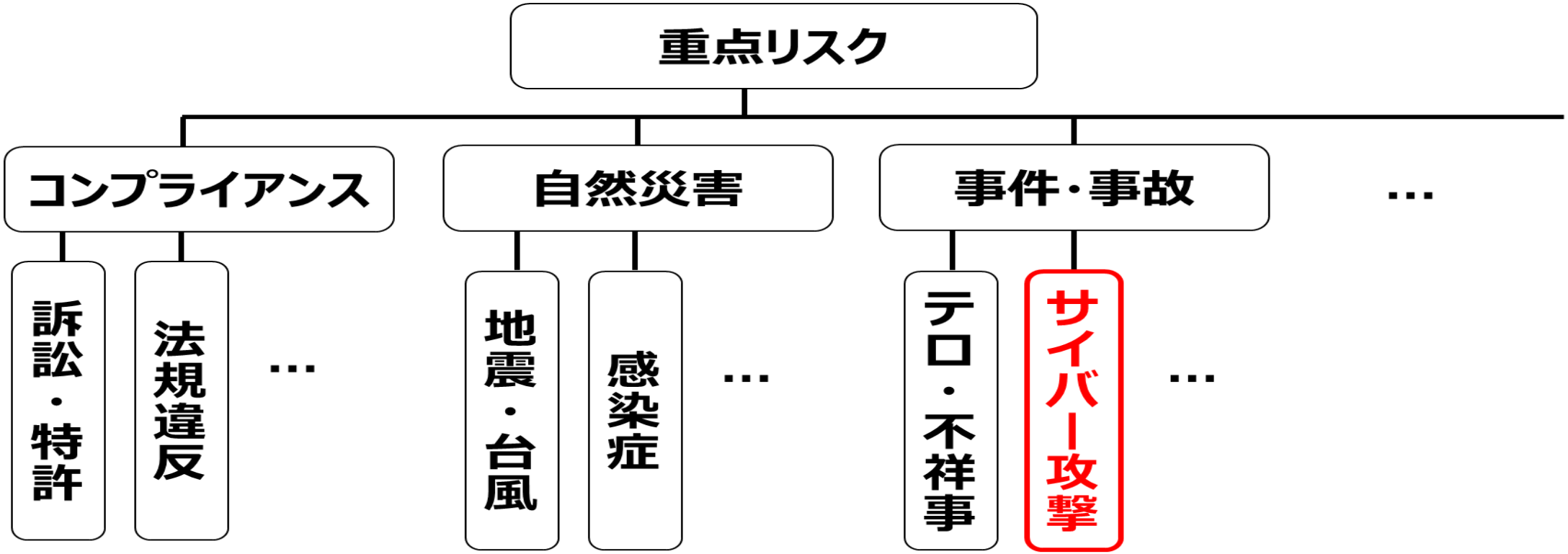


調査手法
- 証券取引所へインシデントの「適時開示」を行った18社
- 2014年7月以降の適時開示企業を対象
- 開示日より10日前を100%（基準値）とした
- 日経平均株価の変動値は調整済み

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」

3-9. 経営層に求められるリーダシップ

サイバー攻撃は、企業の重点管理リスクのひとつ
経営層がリーダーシップをもって動いている姿を、**従業員・現場に対して見せていくことが重要**



3-10. 経営層としての心構え

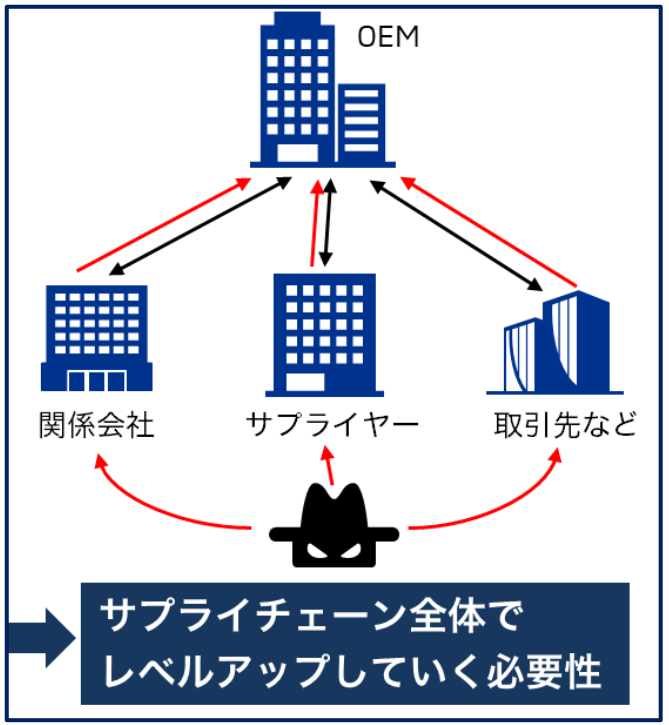
- 経済産業省「サイバーセキュリティ経営ガイドライン」において**経営層がサイバー攻撃から事業を守る為に認識すべき事項**を提唱
- 企業を狙うサイバー攻撃が増加かつ巧妙化するリスク環境において、**経営層が企業戦略としてセキュリティ対策や投資をどの程度行うか判断すること**が必要

◆ガイドラインが提唱する経営者が認識すべき3原則

(1) サイバーセキュリティリスクを認識して**リーダーシップによって対策を進める**

(2) パートナーや委託先も含めた**サプライチェーンに対するセキュリティ対策を実施**

(3) 関係者と平時や緊急時のセキュリティリスクや対策の**コミュニケーションが必要**



Point !

セキュリティ対策は「コスト」ではなく将来の事業活動や成長に必須な「投資」

セキュリティへの投資は経営層の責務であり経営層の判断が必要不可欠

「鎖は一番弱い輪以上に強くなれない。」
出典：「恐怖の谷」、コナン・ドイル、1914年

"No chain is stronger than its weakest link."
Refer to: "The Valley of Fear", Conan Doyle, 1914.

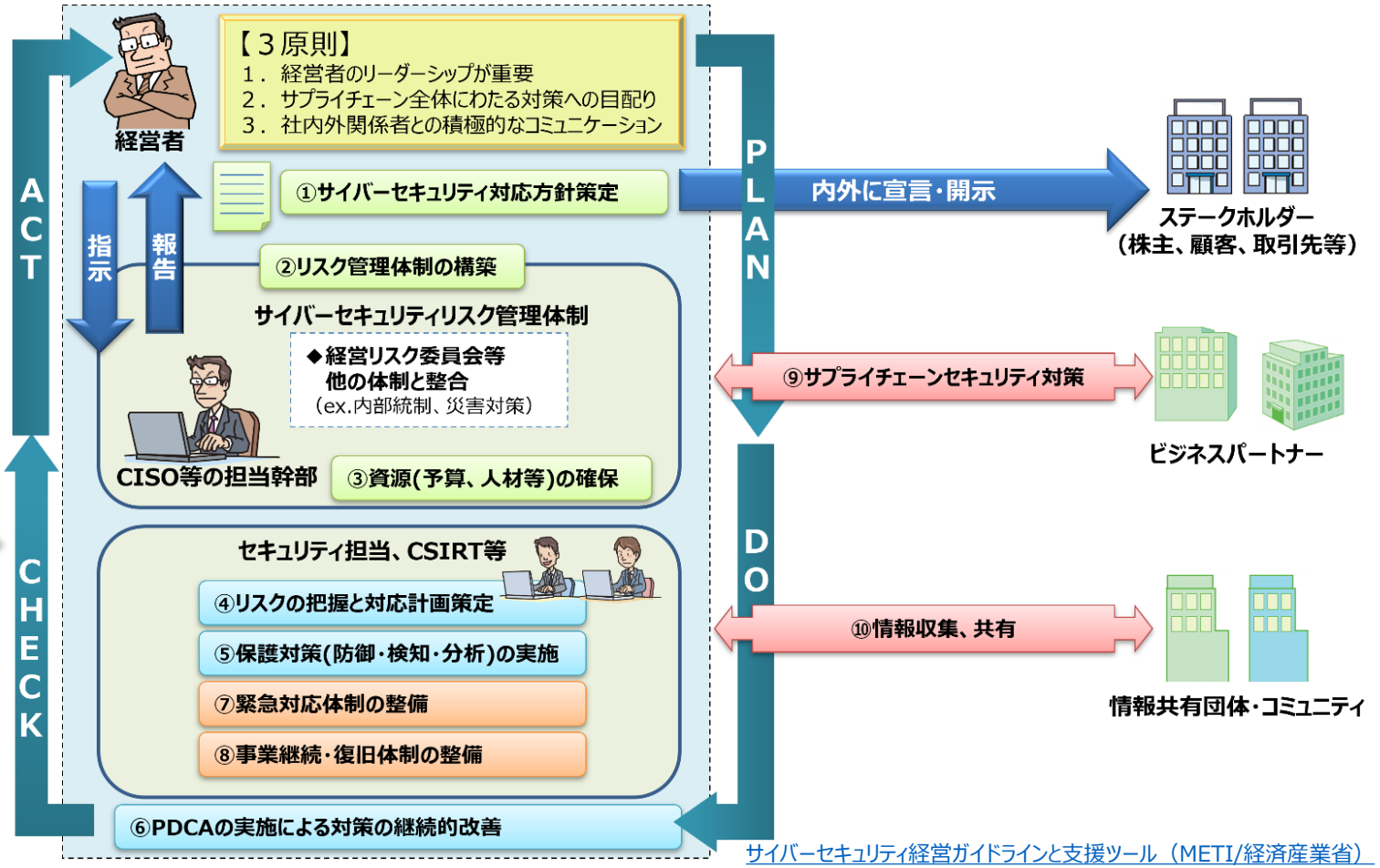
3-11. ご参考：サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドライン＝企業戦略として、経営層が対策に取り組むための指針

サイバーセキュリティ経営ガイドラインの概要

目的	経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため
対象	ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者
発行元	経済産業省
改訂	Ver1.0 :2015年12月 Ver1.1 :2016年12月8日 Ver2.0 :2017年11月16日 Ver3.0 :2023年3月24日
内容	1. はじめに 2. **経営者が認識すべき3原則** 3. **サイバーセキュリティ経営の重要10項目** 付録 A) サイバーセキュリティ経営チェックシート B) サイバーセキュリティ対策に関する参考情報 C) ｻｲﾊﾞｰｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄにそなえるための参考情報 D) 関連する規格・フレームワーク等との関係 E) 用語の定義 F) サイバーセキュリティ体制構築・人材確保の手引き

サイバー攻撃から企業を守る観点で、**経営者が認識する必要のある「3原則」**、及び経営者が情報セキュリティ対策を実施する上での**責任者（CISO等）に指示すべき「重要10項目」**



サイバーセキュリティ経営ガイドラインと支援ツール（METI/経済産業省）

本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

4-1. ’23年度自己評価結果の分析

- ✓ 2023年度は3240社が自己評価を実施（活動内容は1-6. 具体的な活動内容を参照ください）
- ✓ 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の状況。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	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%)	–

4-2. ’24年度のお願い

- ✓ ’継続的なレベル把握のため、’23年度と同様に自己評価頂く
  提出期限：2024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

4-3. 自工会/部工会が期待する達成レベル及び目標時期

✓ 昨年と同様の達成レベルおよび達成時期を継続

⇒ **本年度中（'24年度）の対応を目標に推進いただきたく**

・レベル：自動車産業に関わる全ての会社様にレベル１、2の全項目を達成頂きたい

・時 期：2024年度末を目処に計画的なレベルアップを図って頂きたい

※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

※達成が困難な場合も２４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**

4-4. 自己評価・提出の要領

下記要領に基づき２４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・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	• '23年度とチェック内容は同一ですが、軽微な修正によりチェックシートが変更となっています。 **必ず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V2.2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	提出期限	• **2024年12月末までに提出願います。**
3	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提出ください。 • ガイドラインの提出方法が一部変わります。 **1. １項のHPに掲載されている「自動車産業セキュリティ情報提供申し込み」URLへ申し込みをする。** **2.メールで送付された提出先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	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

5-1. 今後のセミナー開催スケジュール

✓ **自動車業界サプライチェーン全体の強い体質づくりに繋げる**ことを目的に、以下を実施いたします。
- **セキュリティ推進担当者のレベルアップ**を図る情報提供
- **セキュリティ推進上の困りごと**を解決するための相談会（全12回予定）

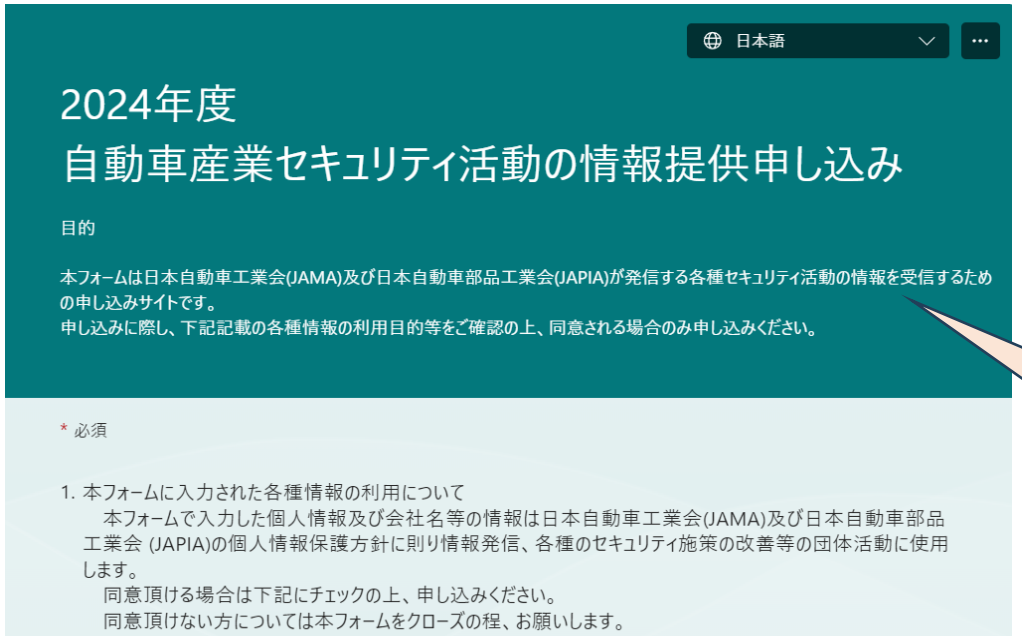
✓ 各**イベント**の情報は、自工会ホームページより展開いたしますので、ご確認お願いいたします。

イベント	内容	開催時期
担当者向け情報展開	**セキュリティ推進担当者向けのレベルアップ** (ガイドライン上の優先度項目の解説)	‘２４年１０月以降
よろず相談会	**セキュリティ推進にあたっての悩み事相談** (全12回予定)	‘２４年１０月～’２５年３月

【ご案内方法】 自工会ホームページ 更新履歴へ告知
<https://www.jama.or.jp/release/latest_update/>

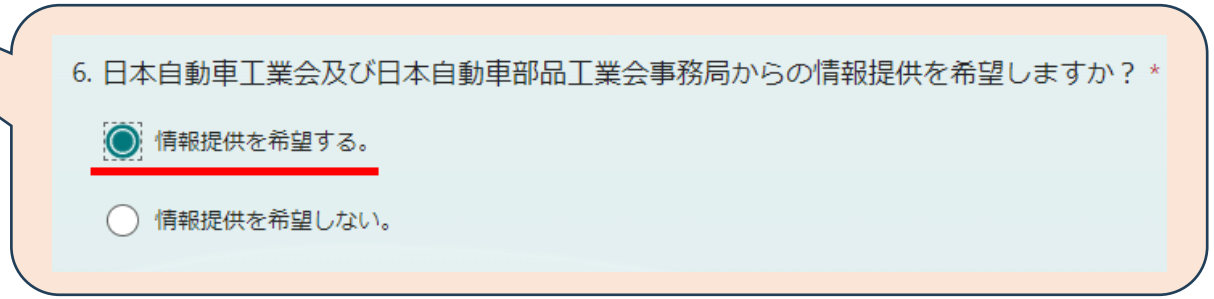
5-2. 自動車産業セキュリティ活動の情報提供申し込み

- ✓ 今年度より、**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きます。
- ✓ 32ページでご紹介した**「自動車産業セキュリティ活動の情報提供申し込みURL」**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。



《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
- ✓ よろず相談会案内　等



本日のアジェンダ

1	はじめに
2	経済産業省様 ご寄稿動画
3	サイバーセキュリティ対策の重要性（名古屋港インシデント事例）
4	’24年度自己評価のお願い
5	今後のイベント、セキュリティ情報提供の申し込みについて
6	まとめ
7	質疑応答

6-1. ご参加頂いている経営層の方へ

①**セキュリティは経営課題**であり、**経営者が取り組まなければいけないリスク対応の一つ**

②**経営層がリーダーシップをもって**セキュリティに対して動いている姿を、**従業員・現場に対して見せていくことが重要**

6-2. 本日のお願い事項

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）

※取引先のセキュリティレベルを把握頂き、**サプライチェーン全体でのレベル向上**

最後に　ー　ご参考まで

まずは「基本のキ」から手を着けてください。
そのうえで、セキュリティ事故に備えたサービスを検討して下さい。

「基本のキ」3つのポイントを周知徹底
- 不用意にメールに添付されたファイルを開かない
- むやみに、怪しいWebサイトを開かない
- 「感染しています、サポートが必要です」の様な、いわゆる“サポート詐欺”に騙されない

更にセキュリティ事故に備えて人材や予算が限られる中小企業でできる対策は？

サイバーセキュリティお助け隊サービス
https://www.ipa.go.jp/security/otasuketai-pr/

下記をワンパッケージで安価に提供するサービス

① 見守り（24 時間監視し挙動や問題のある攻撃を検知）
② 駆付け（問題が発生したときに地域の IT 事業者等が駆付け対応）
③ 保険（簡易サイバー保険で駆付け支援等のサイバー攻撃による被害対応時に突発的に発生する各種コストを補償）

ご清聴ありがとうございました。