自工会／部工会
サイバーセキュリティガイドラインについて

一般社団法人
日本自動車工業会

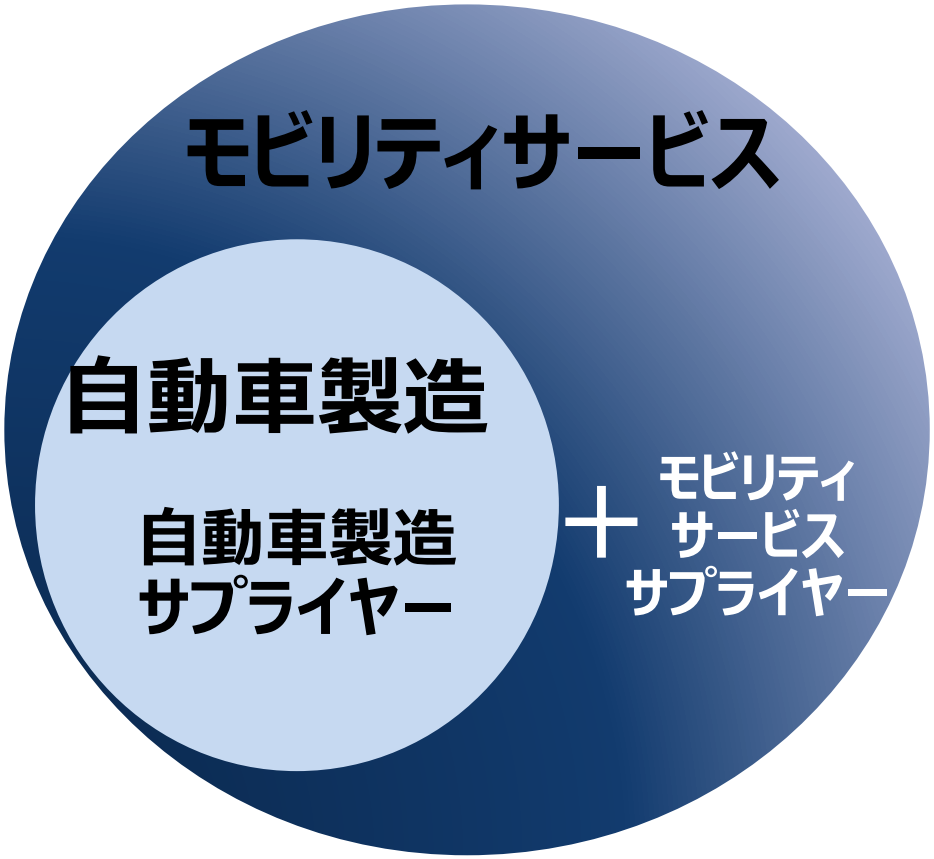
総合政策委員会 ICT部会
サイバーセキュリティ分科会

2024年12月6日

目次

1-1. 自動車業界の特徴

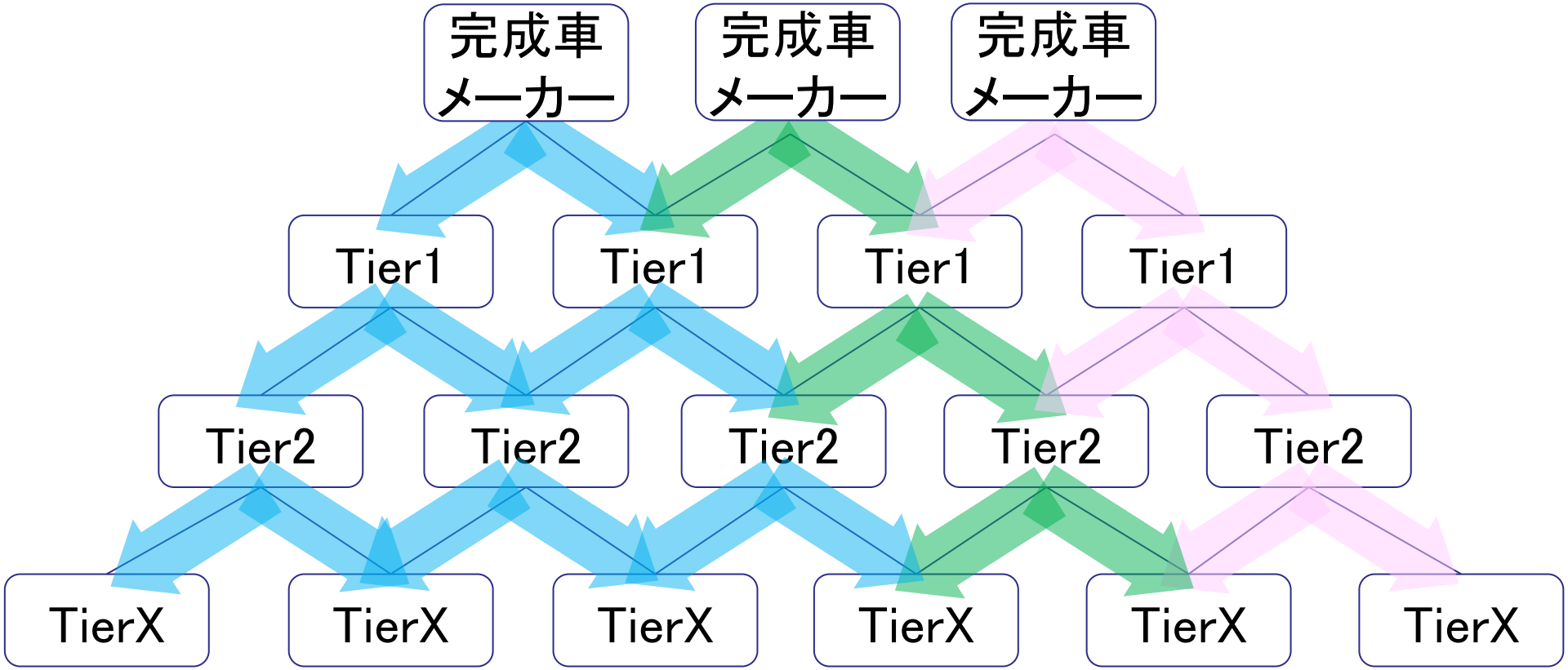
・次世代のモビリティビジネスへの構造変化に伴い、**サプライヤーも拡大**
(モビリティサービスサプライヤー)
・取り扱う情報も**機密情報**が多く、**データ量も増加傾向**



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



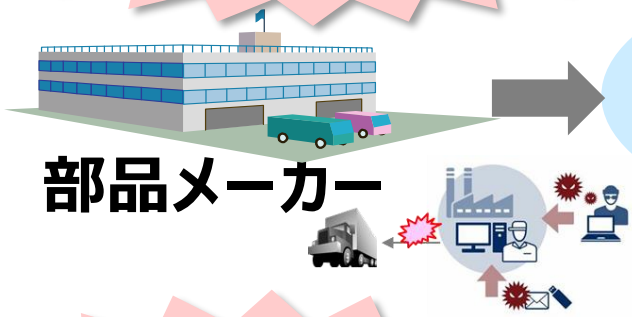
1-3. 自動車業界のサプライチェーンセキュリティリスク

・**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**

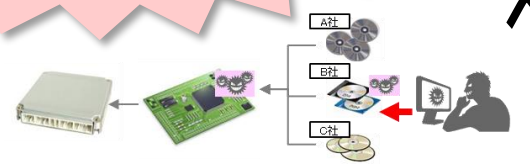
内部不正による
情報漏洩



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

1-4. 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）

1-4. サイバー攻撃によるリスク②：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**

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

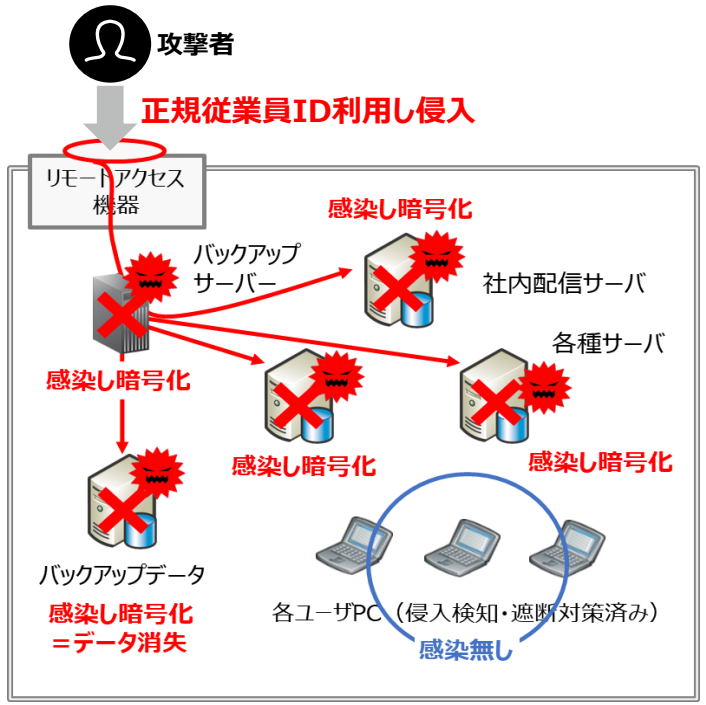
■社内全サーバー停止及び、社内ネットワーク停止

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

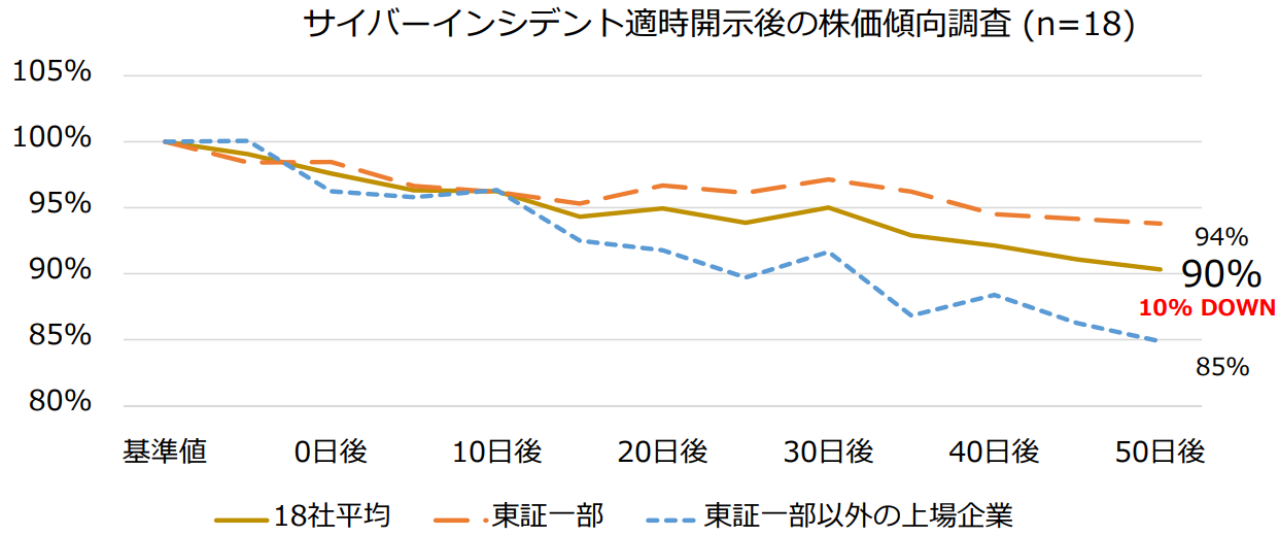


1-4.サイバー攻撃によるリスク③：株価リスク

・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

■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**



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」

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

2-1. 大規模サプライチェーン リスク事例

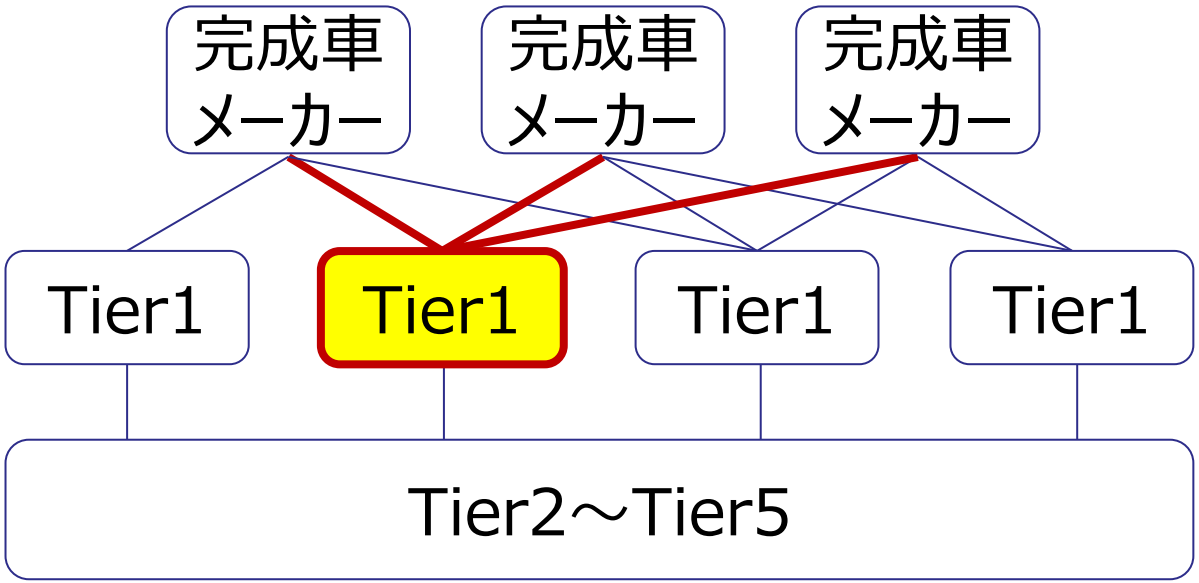
・サプライヤーの業務が停止した場合に、自動車業界への影響は大

・**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**



2007/07/19 09:29

ニュース

【新潟県中越沖地震】トヨタ、日産など自動車大手がライン停止、部品メーカーの工場被災で

市嶋 洋平＝日経コンピュータ　日経コンピュータ

トヨタ自動車、日産自動車など大手各社は、中越沖地震の影響で完成車の製造を7月19日以降に一時停止する。自動車部品メーカー、○○○会社 が被災し部品の納入が止まるためだ。

不足する主な部品は、エンジンを構成する「ピストンリング」と変速機を構成する「シール材」である。トヨタは両部品、日産はシール材、本田技研工業はピストンリングが足りていないという。大手自動車会社に変速機を納入している大手部品メーカー、ジヤトコやアイシン・エィ・ダブリュ（アイシンAW）の生産状況も影響している。両社とも○○○会社の部品をほぼ100%使っているからだ。ジヤトコは18日夜の段階で生産量を6割減としており、アイシンAWは全国の工場からシール材を集めてなんとか生産を続行している。

トヨタは、19日の夕方から20日中まで全国の工場を停止、日産は20日以降に一部ラインを非稼働としたり主要工場での休日出勤を取りやめるといった、それぞれの措置をとる。本田は19日午後までに対応を決定する。このほか、三菱自動車や富士重工業が生産の一時中止を決めている。

本来であれば事業継続性計画（BCP）の実行を確保するため、自動車や大手部品メーカーは ○○○ 同等部品の調達先を確保しておくべきだが、「高精度な部品であり、○○○会社以外からは調達していないのが実情」（大手部品メーカー）という。サプライチェーンの情報システム整備やバックアップ構築と同時に、調達先の冗長性確保も大きな課題となっていることが浮き彫りとなった。

https://googleads.g.doubleclick.net/pcs/click?xai=AKAOjsuQlvhrhLYrbrhX1JRuZI81gOpm_XHauWHvkOAOUDPvygrQanKBCrchRVc-INvqOt64c

2-1. 大規模サプライチェーン リスク事例

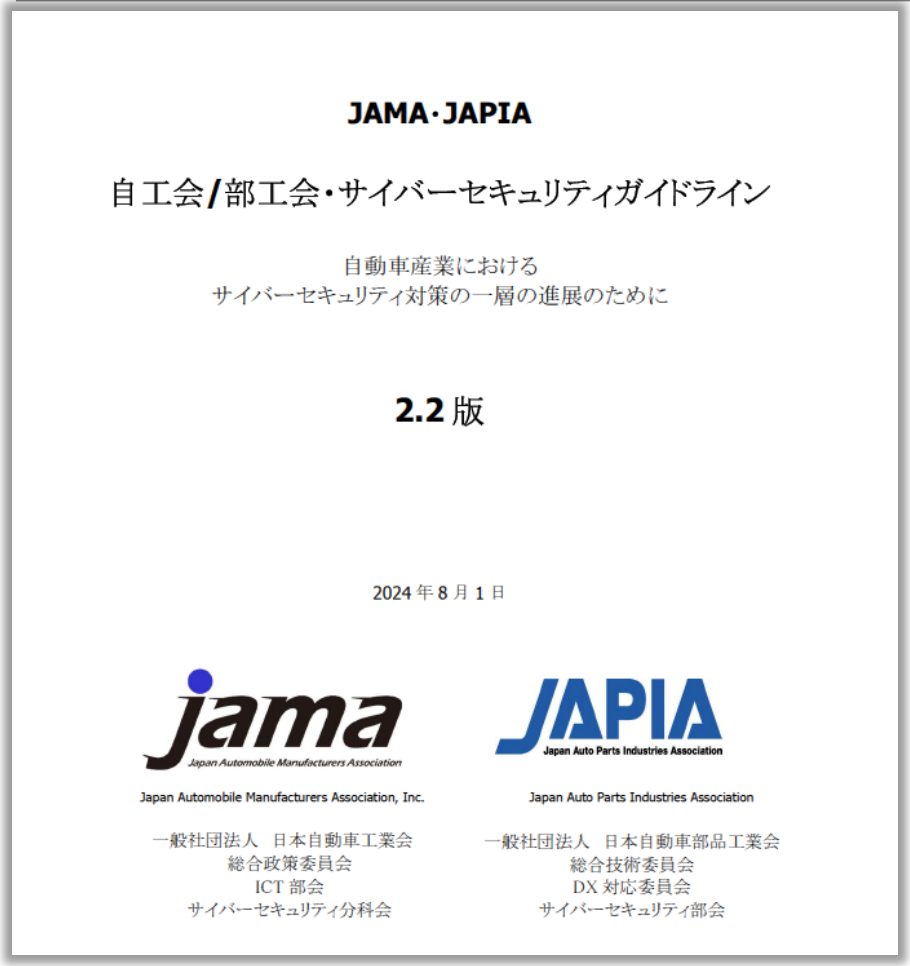
・２０２２年以降、仕入先へのランサム攻撃が多発（海外も多い）
業務に影響のあるケースも多い

時期	被災会社	地域	影響
2月	仕入先A	日本	**社内複数システム、N/W停止**
2月	仕入先B	**北米**	業務への影響なし
3月	仕入先C	**北米**	**社内複数システム、N/W停止**
3月	仕入先D	**欧州**	**社内複数システム、N/W停止**
3月	仕入先E	**北米**	業務への影響なし
4月	仕入先F	**アジア**	業務への影響なし
8月	仕入先G	日本	**社内複数システム、N/W停止**
9月	仕入先H	日本	**社内複数システム、N/W停止**

公開情報より自工会にて調査

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)

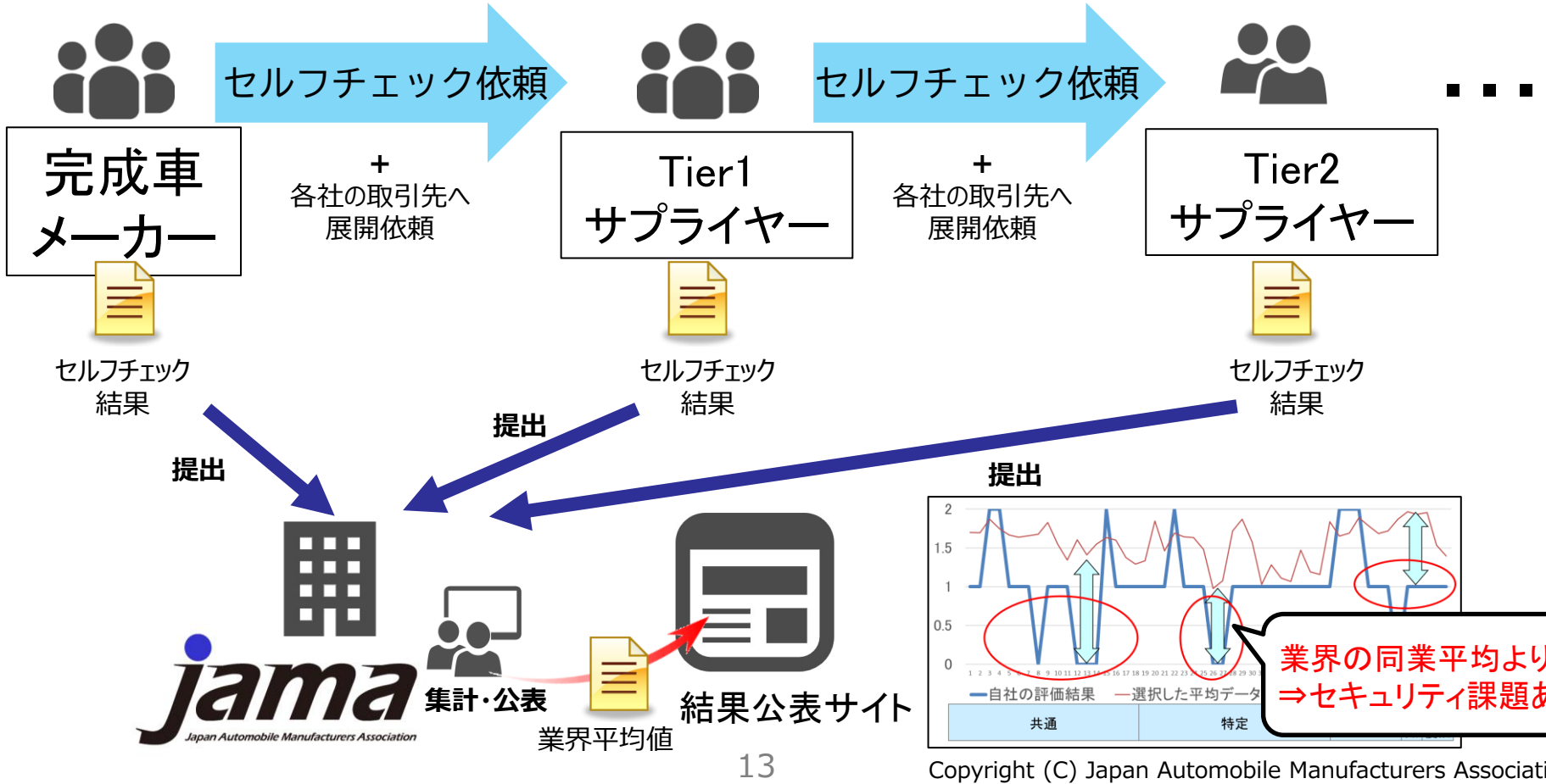
会社名	●●株式会社	評価範囲	▽プルダウンから選択ください	目標レベル	▽プルダウンから選択ください
会社分類	▽プルダウンから選択ください	会社従業員数	▽プルダウンから選択ください		
担当者メールアドレス ※共有先に公開されます		提出済みチェックシートの差し替え、共有先追加の場合は、右のプルダウンから「差し替え」を選択してください。	新規		

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. サプライチェーンへの展開の流れ

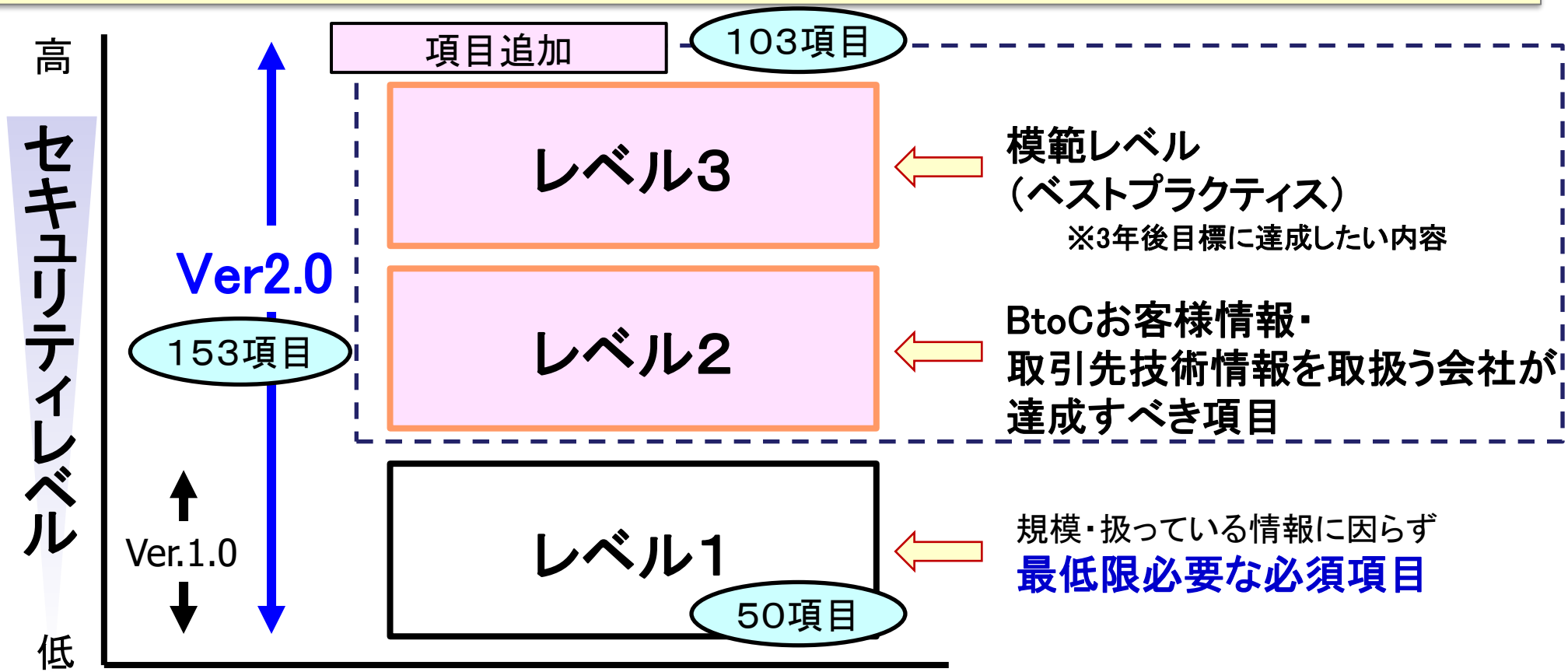
・引き続き24年度も 業界全体に対して、セキュリティレベルのセルフチェックを依頼
・業界平均と自社セルフチェック結果との差異から**重点課題の認識＆レベルアップ**
→ **業界全体のセキュリティレベル向上へ**



3-4.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）**

②V2.0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



4-1.自動車業界サプライチェーンでの対応状況

- ✓2023年度は3240社が自己評価を実施
- ✓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	レベル 1 項目：81.84 /100 点 (81.8%) レベル 2 項目：120.00 /148 点 (81.1%) レベル 3 項目：42.91 /58 点 (74.0%)
2022	4,026 社	3,961 社	レベル 1 項目：76.95 /100 点 (77.0%) レベル 2 項目：110.49 /148 点 (74.7%) レベル 3 項目：37.35 /58 点 (64.4%)
2021	2,300 社	2,296 社	レベル 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

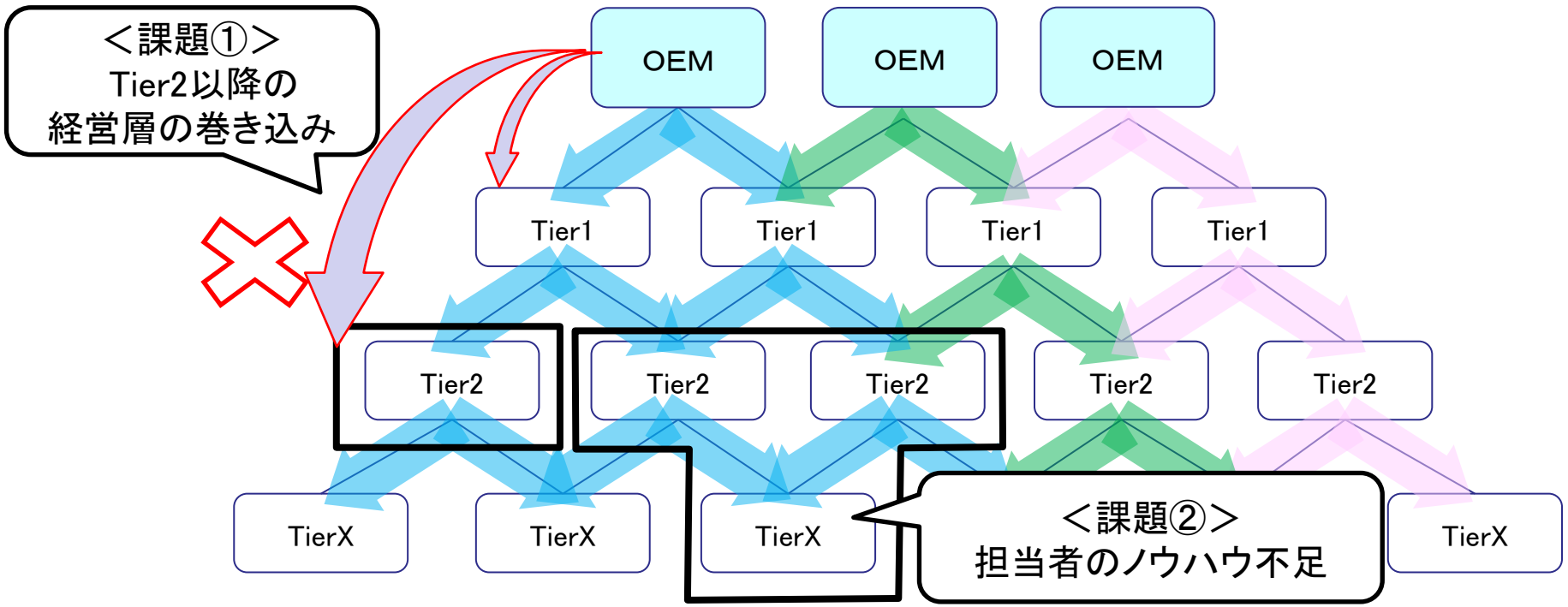
2023 年度平均点詳細

目標レベル	会社数	平均点			
		レベル 1 項目	レベル 2 項目	レベル 3 項目	総合
レベル 1	659 社	62.05 /100 点 (62.1%)	–	–	62.05 /100 点 (62.1%)
レベル 2	1,830 社	85.42 /100 点 (85.4%)	116.84/148 点 (78.9%)	–	197.08 /248 点 (79.5%)
レベル 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. サプライチェーン・セキュリティレベルアップ活動での課題

課題①：取引契約の無い会社への対応が困難（Tier2以降）⇒経営層の巻き込み

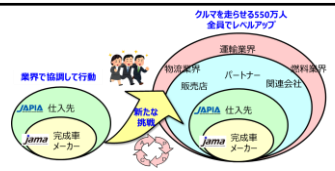
課題②：経営者や担当者にやる気があるが、やり方が分からない⇒担当者のノウハウ不足



4-3.課題への取組み（Tier2 以降の経営層の巻き込み）

- 課題への対策として、**対象者を意識した説明会を実施**
  - ✓ 課題①：取引契約の無い会社への対応が困難（Tier2以降）
  - ✓ 課題②：経営者や実務担当者にやる気があるが、やり方が分からない

課題①：経営層向け説明会の実施

	開催案内	セミナー内容（敬称略）
これまで 	・OEMからの商流で案内(OEM→Tier1→Tier2→…) ・自工会内で調達部会の連携［継続］ 連携①	・セキュリティ推進の必要性 ・自動車産業ガイドラインを使った自己評価のお願い
1）裾野を広げる（Tier2以降）	＜広報協力＞ ・IPA ・商工会議所 ・J-Auto-ISAC 連携②	・経産省 寄稿動画 連携③
2）仲間を増やす	＜他業界活動・地域活動との連携＞ ・商工会議所　（日商と相談の上、方法相談） ・自動車他団体連携・他業界	

課題②：実務担当者向けよろず相談会の実施（昨年度より継続）

説明会・情報展開	内容	参加者の声
・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回実施予定）	・他社の**具体的事例**が聞けて参考になった ・評価の**具体的な基準**が確認出来て参考になった ・**費用面、人材面共にハードルが高い**ことが分かった

5-1.工場領域でのこれまでの取組み(1)

既存の「自工会／部工会・サイバーセキュリティガイドライン」（以降**エンタープライズ版**）と独立した工場独自ガイドラインを作成した場合の**利用各社の負担増を避けるため**
エンタープライズ版をベースに活動を進めることを決定

エンタープライズ版の**チェックシート**を**工場領域**に適用する場合の解釈集（**工場領域版「チェックシート」（案）**）を作成 （部工会代表5社と共同）

5-1.工場領域でのこれまでの取組み(2)

自工会・部工会会員各社にチェックシート（案）を提示し意見収集実施

■自工会（7社）、部工会（29社）から回答。

■工場領域版チェックシート策定に際し、特に重要な意見として「①対象領域に関する意見」と「⑥チェックシートの位置づけや目的、構成等に関する意見」が挙げられた。

意見分類	検討ポイント
①対象領域に関する意見	• エンタープライズ領域と工場領域との項目のすみ分け • エンタープライズ領域と工場領域の関連性・整合性
②用語の定義に関する意見	• 用語の定義の記載または見直し（工場、製造現場、製造ライン、機密情報設置エリア、重要機器設置エリア等）
③レベルの定義に関する意見	• レベルと重要度の定義の記載改善
④チェックシートの対象範囲に関する意見	• チェックシートの利用対象範囲の明確化
⑤チェックシートの見方・理解・解釈・表記・体裁に関する意見	• チェックシートの体裁の改善 • チェックシートの見方・評価方法・項目の趣旨等の解説追加 • 専門用語・IT用語の理解が難しいことに関する対応
⑥チェックシートの位置づけや目的、構成等に関する意見	• チェックシートの構成検討 • チェックシートの使用目的や位置づけの明確化
⑦評価・回答方法に関する意見	• 評価時の担当者欄の見直し • 設問の対象者・対象領域の明確化
⑧他基準へ関連性・整合性に関する意見	• 他基準との関連性や整合性の記載に関する改善
⑨対策や対応状況に関する意見	• 対策が難しい又は困難な設問があること
⑩今後の展開に関する意見	• 他領域への展開方法
⑪その他	• その他のご意見

5-2.工場領域での取組み：今後の予定

各社からの意見と以下の残課題を踏まえ、工場領域版「サイバーセキュリティチェックシート」の策定および運用方法の検討
（'25/3メドにチェックシート公表）

- 工場は千差万別であり、工場によって対策可能な内容が変わるため、一律の**達成基準の設定が難しい。**
  ⇒工場領域版については、**自社・自工場のセキュリティ向上のための自己チェック用としての活用**を促すべく、目的・利用方法についての正しい理解を促すことが重要。
- 工場の担当者の役割によっては、工場領域版だけではなく、エンタープライズ版のチェックシートにも対応する場合がある。工場領域版として記載すべき項目や表現方法について留意する必要がある。
- チェックシートの運用方法（エンタープライズ版のように広く展開し集計等を行うか否かなど）についても今後の検討事項。

ご清聴ありがとうございました

4-5. 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	守秘義務	社内機密情報のセキュリティ社内ルールを規定していること
	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

4-5. 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

4-5. 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
特定	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
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ついて、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)

4-5. 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）