【導入解説】

◯「経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度（検討中）」と「自工会／部工会・サイバーセキュリティガイドライン」の概要

◯基礎としてのガバナンス／マネジメント及びリテラシー構築のあり方　等

2025年11月14日

合同会社三笠ポリシーアドバイザリ　代表社員　三笠 武則
（営業秘密保護推進研究会 事務局長）

APPTraS

目次

APPTraS
営業秘密保護推進研究会

1. 第21回連続セミナー（Part 1 & Part 2）で対象とする制度・ガイドラインのご紹介
   - ●一覧と照会先
   - ●それぞれの位置付けと関係をどのように捉えているか
2. 「経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度（検討中）」と「自工会／部工会・サイバーセキュリティガイドライン」の概要
3. 弊研究会独自の取組　～秘密保護のガバナンス／マネジメント及びリテラシー構築への意識を高める

１．第21回連続セミナー（Part １ & Part 2）で対象とする制度・ガイドラインのご紹介

- 一覧と照会先
- それぞれの位置付けと関係をどのように捉えているか

本セミナーで対象とする制度・ガイドラインの一覧と照会先(URL)

APPTraS 営業秘密保護推進研究会

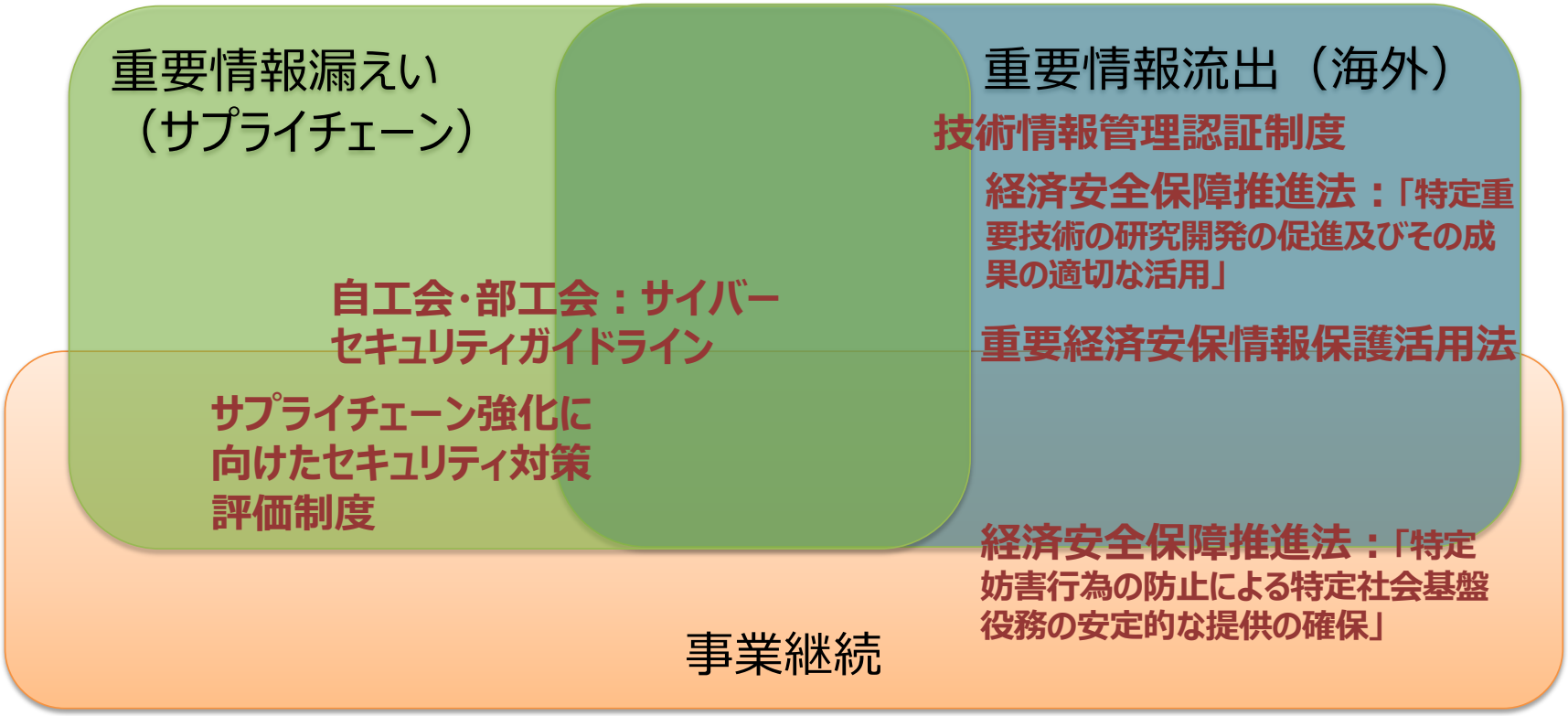
本セミナーでは下記の制度・ガイドラインを取り上げます。管理策にも言及して、できるだけ具体的に解説します。

- 経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度（2026.10公開に向けて検討中）
  https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20250414_report.html
- 自工会・部工会：サイバーセキュリティガイドライン
  https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html
- 経済産業省：技術情報管理認証制度
  https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/
- 内閣府：経済安全保障推進法
  - 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保　届出事項
    https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html
  - 特定重要技術の研究開発の促進及びその成果の適切な活用　協議会情報管理規程（雛形）
    https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/technology/doc/3_kyogikai_mkiyaku.pdf
    ※（参考）研究インテグリティ、研究セキュリティに関する政策がこれに関連
    https://www.mext.go.jp/a_menu/kagaku/integrity/index.html
- 重要経済安保情報保護活用法　質問票（適性評価）、認定申請書（適合事業者の認定）、その他ガイドライン・運用基準等
  https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html
  https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/download/download.html
- 弊研究会：重要な秘密の漏えい／他社の秘密の侵害に対する「組織アウェアネス」向上のためのチェックリストβ版（β試行開始間近）

対象とする制度・ガイドラインの位置取り（大枠の世界観）

本セミナーでは、重点ポイントとして、サプライチェーンからの重要情報漏えい、重要情報の海外流出、事業継続（基幹インフラ、サプライチェーン）のいずれかに焦点を当てた制度・ガイドラインを対象としています。

３つの重点ポイントの関わりと各制度・ガイドラインの位置付けについては、下図のように整理しています。



サプライチェーンに重点を置いた制度・ガイドラインが掲げている目的とは？

「サプライチェーン強化に向けたセキュリティ対策評価制度」「自工会・部工会：サイバーセキュリティガイドライン」がこれに該当。両者ともサプライチェーンからの重要情報漏えい防止を重視。事業継続については、前者は明確にこれを重視している点が特徴だが、後者はシステム継続稼働に焦点を絞っている。

サプライチェーン強化に向けたセキュリティ対策評価制度	自工会・部工会：サイバーセキュリティガイドライン
（想定脅威：☆4） • **供給停止等により**サプライチェーンに大きな影響をもたらす企業への攻撃 • **機密情報等、情報漏えいにより**大きな影響をもたらす資産への攻撃 **（目的：☆4）** • 初期侵入の防御に留まらず、内外への被害拡大防止・（攻撃）目的遂行のリスク低減によって取引先のデータやシステム保護に寄与すること • サプライチェーンにおける自社の役割に適合した事業継続を推進していること **（弊研究会の注目点）** 目指すべき達成水準（イメージ）として以下を例示： • **取引先のシステムやデータを含む**内外への被害拡大や攻撃者による目的遂行のリスクを低減する**対策が講じられていること** • 事業継続に向けた取組や取引先の対策状況の把握など、**自社の位置づけに適合したサプライチェーン強靭化策が講じられていること** ☆4は“Standard”と位置付けられており、基本的には、自工会・部工会：サイバーセキュリティガイドラインのレベル２と対比できる。	**（背景）** 昨今、標的の企業を狙うために、攻撃者によるセキュリティ対策を強化中の関係企業や取引先等のネットワークへの不正侵入、企業間ネットワークを経由した攻撃、標的企業が利用するソフトウェアや製品への不正なプログラムの埋め込み等のサプライチェーンを狙ったサイバー攻撃も懸念される。**業界を取り巻くサイバーセキュリティリスクを正確に理解しながら業界全体でサイバーセキュリティリスクに適切な対処を行うことが必要不可欠**である。 **（目的）** 自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、向こう3年の対策フレームワークや業界共通の自己評価基準を明示することで、**自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進**すること。 **（弊研究会の注目点）** 自動車業界として標準的に目指すべき項目を提示し（レベル２）、これを**達成すべき会社**として以下を例示： • **サプライチェーンにおいて社外の機密情報（技術・顧客情報等）を取扱う会社** • **自動車業界として重要な自社技術／情報を有する会社**

出典：制度構築に向けた中間取りまとめ（概要）

出典：サイバーセキュリティガイドライン本文

重要情報の海外流出に重点を置いた制度・ガイドラインが掲げている目的とは？

技術情報管理認証制度は、サプライチェーンのカギとなる軍事転用可能な**重要民生技術を保有する中小企業の技術情報管理を支援し、重要技術情報の海外流出防止を確実にする**ための国の認証制度である。

技術情報管理認証制度

（背景）

- **グローバル化の進展等を背景に、国内外への技術情報流出リスクが増大**している。**民生技術を軍事転用する流れが拡大し、あらゆる先端技術の保有主体が技術獲得のターゲットに**なってきた。技術を通じて自国の勢力を拡大しようとする事例も見受けられる。
- サプライチェーンの**カギとなる技術を保有する中小企業がターゲットと**されるリスクも増大している。
- **技術情報は流出すると回収が難しく**、**経済的に大きな損失を負う**とともに、**取引先からの信頼を失って競争力が大きく棄損**される。
- 中小企業の情報セキュリティ対策は依然として遅れている一方で、セキュリティ対策投資を行う企業の半分が取引を拡大している。
- 業界ごとに情報セキュリティのガイドラインが整備されてきているが、**自己チェックであり、各企業がどこまで満たせているかは不明確**である。

（目的）

- 国の基準を満たすかを客観的に審査・認証し、必要に応じて国が事業者に指導・助言することで**企業の対策を取引先等に示すことを可能とし、取引先からの信頼性を向上**させる。

（弊研究会の注目点）

- 評価対象とするのは、技術情報の管理方法である。従って、**国が示す基準も技術情報の管理基準**である。
- 自工会・部工会：サイバーセキュリティガイドラインのレベル１の要求事項を全て取り込むことで、同ガイドラインとの効果的な共存を目指している。

出典：技術情報管理認証制度（TICS）について

重要情報の海外流出に重点を置いた制度・ガイドラインが掲げている目的とは？

APPTraS 営業秘密保護推進研究会

重要経済安保情報保護活用法は、重要経済基盤に関する**特に秘匿する必要がある情報の海外流出防止**を図る制度である。また、**経済安全保障推進法の「特定重要技術の研究開発の促進及びその成果の適切な活用」**は、**特定重要技術の海外流出対策を強化**する側面を持っている。これに対し、**「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保」は基幹インフラ役務の「事業継続」が主眼**であり、併せてこれを害する**機器脆弱性情報等の海外流出防止にも取り組んでいる**。

重要経済安保情報保護活用法	経済安全保障推進法	
	特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保	**特定重要技術の研究開発の促進及びその成果の適切な活用**
（背景） • 国際情勢の複雑化、社会経済構造の変化等に伴い、**経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大** **（目的）** • **重要経済基盤に関する情報であって我が国の安全保障を確保するために特に秘匿することが必要であるもの**について、これを**適確に保護する体制を確立**した上で収集し、整理し、及び活用すること • **当該情報の保護及び活用に関し**、重要経済安保情報の指定、我が国の安全保障の確保に資する活動を行う事業者への重要経済安保情報の提供、重要経済安保情報の取扱者の制限その他の必要な事項を定めることにより、**その漏えいの防止を図り、もって我が国及び国民の安全の確保に資する**こと	**（背景）** インフラ事業者が利用するICT機器の高度化やそのサプライチェーンの複雑化・グローバル化を背景に、**サプライチェーンの過程で不正機能が埋め込まれる可能性**や、**機器の脆弱性に関する情報がインフラ事業者の意図に反して共有される可能性**等が高まっており、これらは、**我が国の外部から、役務の安定的な提供を妨害する行為の手段として使用されるおそれを増大**させている。 **（目的）** **設備の導入又は維持管理等の委託に関して我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為を未然に防止**するための制度を事業横断的に整備し、**特定社会基盤役務の安定的な提供の確保**を図る。	**（背景）** **主要国は**、感染症の世界的流行、大規模サイバー攻撃、自然災害等も含めた安全保障上の脅威等への有効な対応策として、**先端技術の研究開発・活用を強力に推進**し、鍵となる技術の把握に必要な**情報収集・分析**、**大型研究開発プロジェクトの立ち上げ**、情報共有や成果の社会実装に向けた**官民協力スキームの導入等を進めている。同時に、技術流出問題が顕在化する中、各国とも対策を強化**している。 **（目的）** **特定重要技術を定義**した上で、当該技術に関し、官民連携を通じた伴走支援のための協議会の組織、指定基金協議会の組織等による強力な支援、調査研究業務の委託を整備し、**特定重要技術の研究開発の促進とその成果の適切な活用を図る**。

出典：重要経済安保情報の保護及び活用に関する法律 概要

２．「経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度（検討中）」と「自工会／部工会・サイバーセキュリティガイドライン」の概要

「自工会／部工会・サイバーセキュリティガイドライン」の国内におけるポジション

APPTraS 営業秘密保護推進研究会

「自工会／部工会・サイバーセキュリティガイドライン」は、先行して業界全体で広く実績を積み重ねており、**我が国をリードする好事例としての定評**を得ている。
このため**経済産業省は**、「サプライチェーン強化に向けたセキュリティ対策評価制度」「技術情報管理認証制度」の両方において、当該ガイドラインとの連携を強く意識しており、**具体的な基準レベルでの共通化を進めている**。

経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度

- サプライチェーン対策評価制度（★３/４）は、**先行する自己評価の仕組みである**・・・**「自工会・部工会ガイドライン」**・・・**と相互補完**的な制度として発展することを目指す。
- **★３/4は、自工会・部工会ガイドラインのLv1、Lv2に対応**。
- **自工会・部工会ガイドラインに基づく自己評価結果の本制度での活用などの連携方策**を引き続き検討。・・・

（出典）サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ

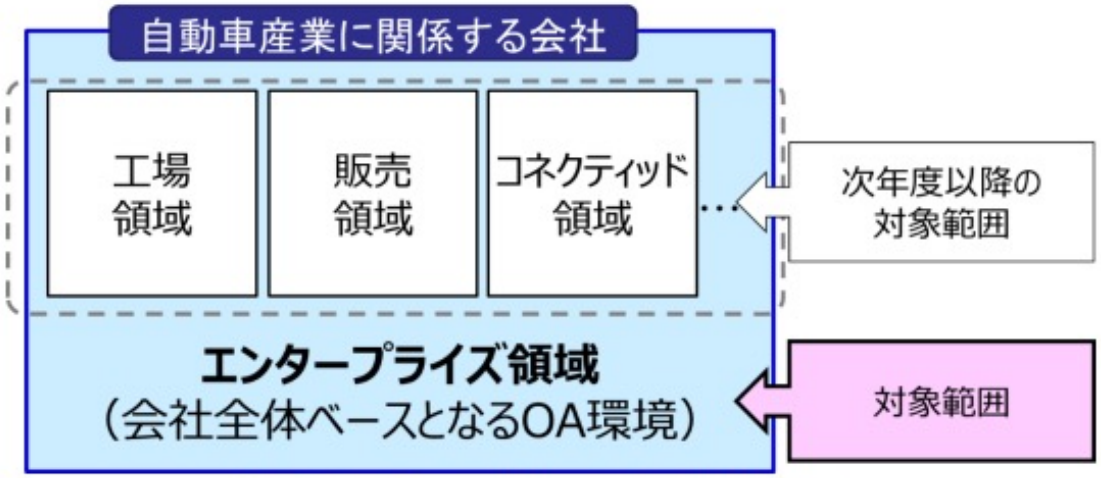
経済産業省：技術情報管理認証制度

- ・・・以下の方針で認証を取得するための基準告知を改正（2024年8月16日施行）
  - ・・・
  - 業界団体の問題意識やニーズを踏まえ、**自工会・部工会ガイドラインのレベル１の項目をカバー**
  - ・・・

（出典）技術情報管理認証制度（TICS）について（2025年10月）

自工会／部工会・サイバーセキュリティガイドラインの対象

自工会／部工会・サイバーセキュリティガイドラインは、**自動車産業に関係する全ての会社のエンタープライズ領域**（会社全体となるOA環境）**を対象範囲**としている。



＜図：自動車産業 CS ガイドラインの対象領域＞

想定読者は、**CISO及びセキュリティ業務に関与する部門**（リスク管理、監査、セキュリティ対応、情報システム開発・運用、データ管理、購買・調達、人事・法務・総務）**の責任者及び担当者**。

（出典）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）

自工会／部工会・サイバーセキュリティガイドラインの達成レベル構成

中小企業を含めた全ての企業がガイドラインを活用できるように、**ベースライン／標準／現時点での最終到達目標という３つのレベルで達成条件／達成基準を設定**している。

レベル３：**現時点で**自動車業界が**到達点**として目指すべき項目
→ 会社規模・技術レベルの観点で**自動車業界を代表し牽引すべき立場の会社**またはそれを目指す会社が対象

レベル２：自動車業界として**標準的に目指すべき**項目
→ **対象は２類型**に整理できる
（類型１：情報漏洩）サプライチェーンにおいて**社外の機密情報（技術、顧客情報等）を取扱う会社**、自動車業界として**重要な自社技術／情報を有する会社**
（類型２：事業継続）相応の規模／シェアを有し、**不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼしうる会社**が対象

レベル１：自動車業界として**最低限、実装すべき**項目
→ 自動車業界に関係する**全ての会社が対象**

（出典）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）

自工会／部工会・サイバーセキュリティガイドラインの統制目標とレベル毎の達成条件／達成基準の記載方法

APPTraS 営業秘密保護推進研究会

統制目標（目的、要求事項）を定め、**その達成レベルごとに達成条件／達成基準を提示**している。達成基準を満たすことのエビデンスを記録することで、レビュー／監査への対応も可能になる。

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
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）
			5	Lv2		【規則】 ・守秘義務の誓約書を提出させること（社外要員除く）
			6	Lv2	派遣社員、受入出向社員について、派遣元、出向元の会社と守秘義務を締結している	【規則】 ・守秘義務には、業務で知り得た情報を外部に漏えいさせない旨の記述があること 【時期】　※守秘義務の締結時期 ・業務開始前
			7	Lv2	退職や期間満了時には必要な機密情報、情報機器などを回収している	【基準】 ・回収物一覧のチェックシートまたは帳票を作成すること ・回収漏れが起こらない手順を整備、運用すること ・手順に従い回収しているかを確認し、必要に応じて手順の是正を行うこと ［回収物］ −情報（印刷物、記憶媒体） −情報機器（PC、スマートデバイス） −アクセス権（ID、鍵） ※上記の他に必要な回収物を各社で判断すること ［回収状況の確認、手順の是正頻度］ −1 回以上/年
			8	Lv1	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、サーバー、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】 ・定常的に、かつ、ルールの改正時に周知すること

- 統制目標（要求事項）37項目
- 達成条件：153項目
  Lv1 50項目
  Lv2 74項目
  Lv3 29項目

（出典）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）

重要情報漏えい防止の観点から見た
自工会／部工会・サイバーセキュリティガイドラインの注目点

設定された統制目標のうちで、**秘密保護の観点から特に重視すべき項目**として、**機密情報を扱うルール整備、日常の教育、他社との情報セキュリティ要件、情報資産の管理（情報）、取引内容・手順の把握、物理セキュリティ、メール誤送信対策（オフィスツール関連の１つ）等**がある。

#	ラベル	秘密保護の観点での着目点	#	ラベル	秘密保護の観点での着目点
1	方針		13	取引内容・手段の把握	◎
2	機密情報を扱うルール	◎	14	外部への接続状況の把握	
3	法令遵守		15	社内接続ルール	○
4	体制（平時）	○	16	物理セキュリティ	◎
5	体制（事故時）		17	通信制御	○
6	事故時の手順		18	認証・認可	○
7	日常の教育	◎	19	パッチやアップデート適用	
8	他社との情報セキュリティ要件	◎	20	データ保護	◎
9	アクセス権	◎	21	オフィスツール関連	◎
10	情報資産の管理（情報）	◎	22	マルウェア対策	
11	情報資産の管理（機器）		23	不正アクセスの検知	
12	リスク対応	○	24	バックアップ・復元（リストア）	

（出典）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）

自工会／部工会・サイバーセキュリティガイドラインの活用において優れている事項

ガイドライン活用のポイントとして、以下に示す点が優れていると考えられる。

- 業界全体での、**共通のガイドラインに基づくセキュリティ実装、評価**。これに基づく**セキュリティ信頼チェーン構築**。
- **自社の評価結果の業界平均との差分**が、基本的なセキュリティ対策の抜け漏れへの気づきを与え、マネジメント（PDCA）によって**定期的に改善する機会を与えている**。
- 自社の評価結果に基づきセキュリティ課題を認識し、**社内での教育・訓練、啓発活動に活用**することが可能。
- **共通のガイドラインに基づく**自社の**評価結果を簡便な手続きでサプライヤから調達元に集約**することが可能。

（出典）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）

自動車産業サプライチェーンへのガイドラインの優れた推進活動

自工会／部工会が、ガイドラインを自動車産業サプライチェーンに広く普及させるために取り組んでいる推進活動には多くのグッドプラクティスが見られる。

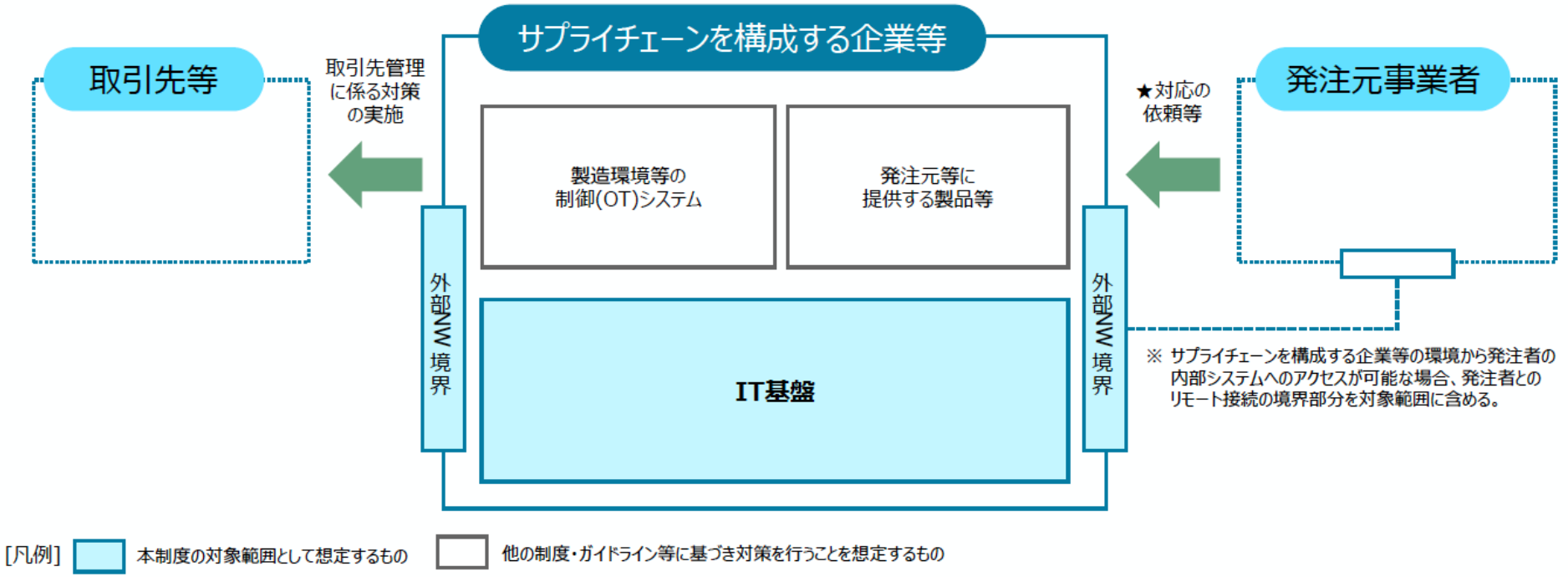
グッドプラクティス	期待される効果
自工会HPで最新チェックシートを常にダウンロード可能	業界全体での共通認識育成とセキュリティ信頼チェーン構築に資する
共通のガイドラインに基づく自己評価結果を業界と調達元に簡便に提出・集約できるIT基盤	● 業界平均を算定・フィードバックすることで、業界各社のセキュリティ改善に具体的な気付きを与えることができる ● 調達元企業がサプライヤのセキュリティ管理を強化・効率化できる
経営者・担当者説明会の継続的な実施	中小企業の場合は経営者の啓発が何より重要。担当者に留まらず中小企業の経営者を直接啓発することができる。
よろず相談会の継続的かつ高頻度な開催	● 各社の自己評価実務担当者が持つ疑問・悩みを持ち寄り、業界他社と情報交換／議論し、解決の道筋に繋がる知見を収集することで、自己評価の質を改善するとともに、実務者のスキル／経験値を高めることができる

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

経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度*の対象

*来年度運用開始を目指して検討中

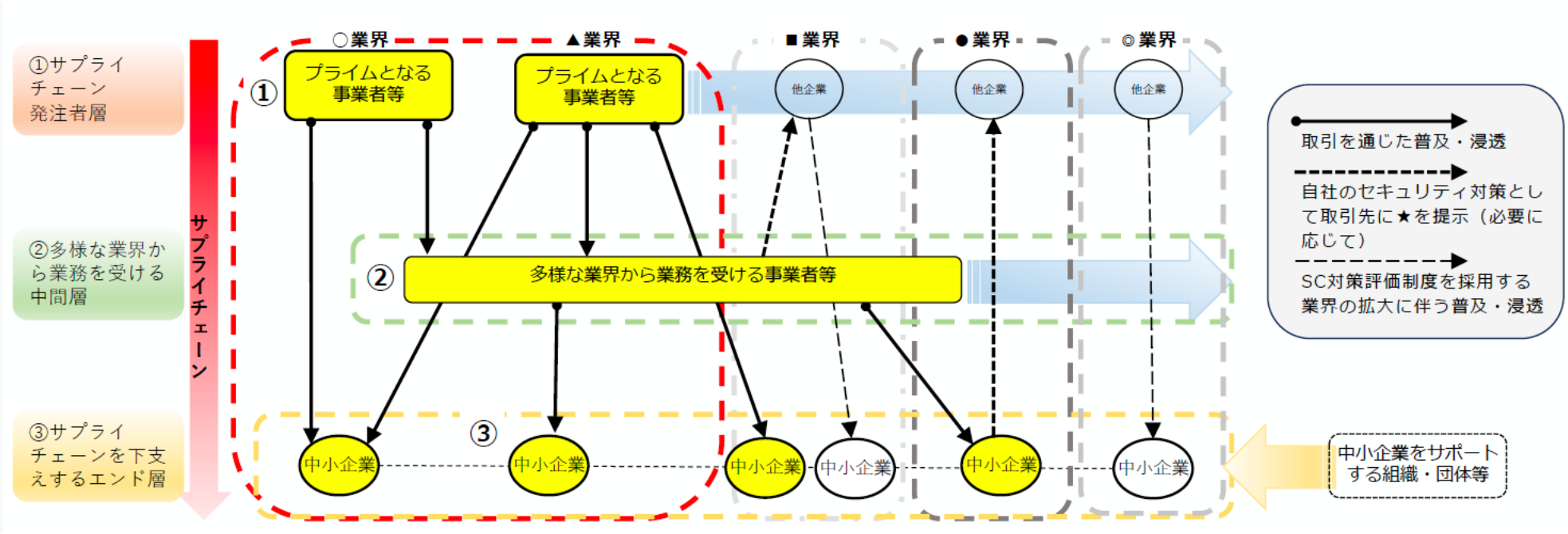
本制度は、**サプライチェーンを構成する企業等のIT基盤**（オンプレミス環境で運用されるものに加え、**クラウド環境で運用するものも含む**）**を対象**としている。発注者とサプライヤ内部システムのリモート接続境界部分も対象範囲に含まれる。他方でOTシステムや中間製品等は対象としていない。 ※基本的には自工会／部工会・セキュリティガイドラインと同様。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度の対象

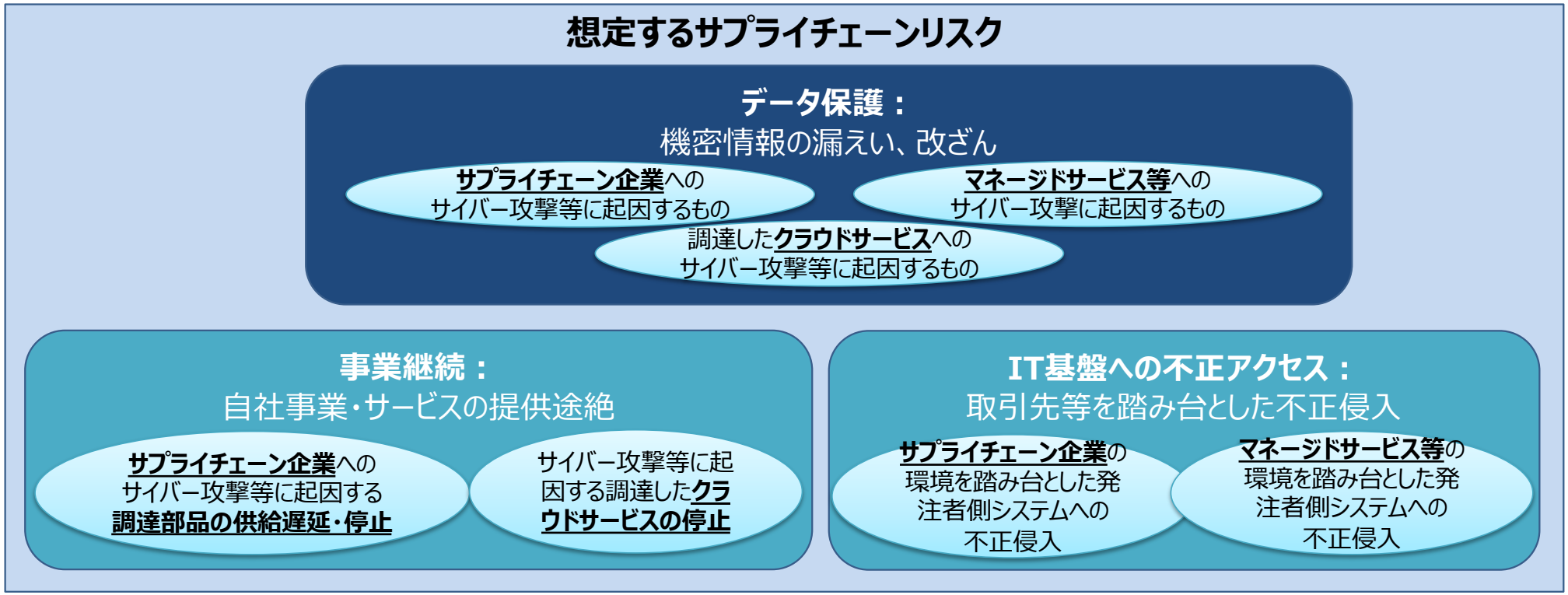
制度の目的を考慮し、**対象を特定の業界に限定していない**。むしろ、多様な業界から業務を受ける中間層の事業者等に幅広く焦点を当てていることが特徴と言える。
また、例えば**従業員数100人未満の中小企業などは「下支えするエンド層」と捉えて、制度の対象**としている。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

サプライチェーン強化に向けたセキュリティ対策評価制度が対象とするリスクの範囲

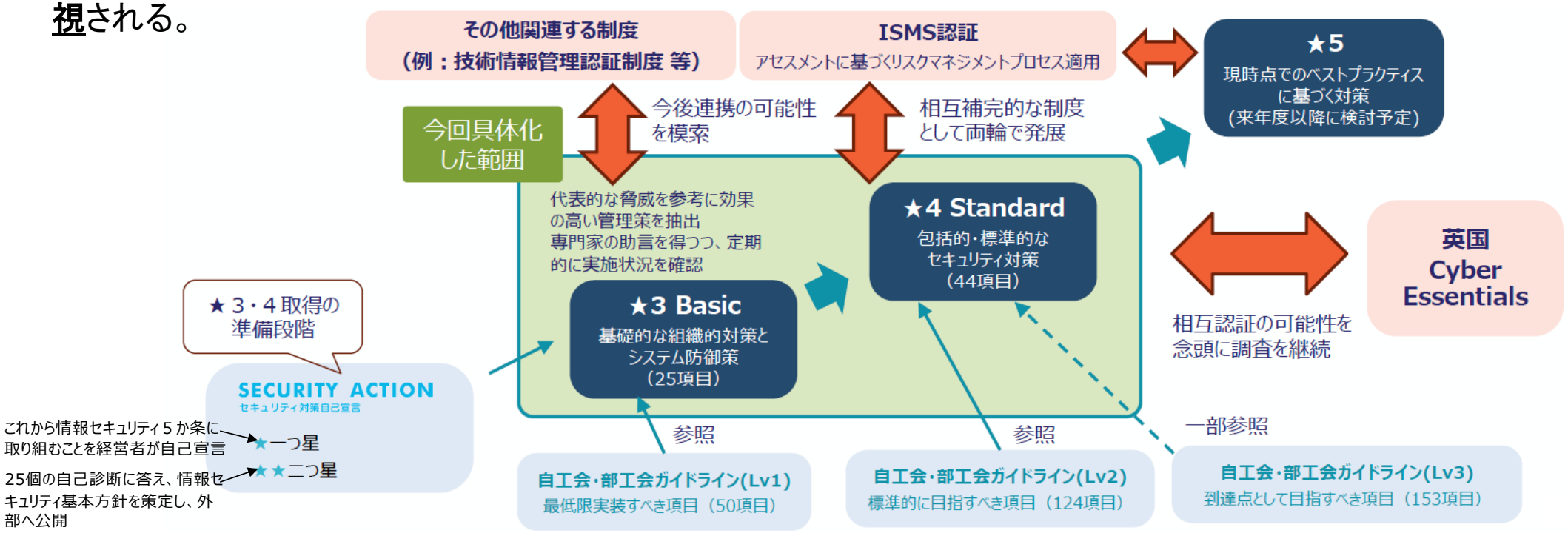
当該制度の主たる特徴として、**機密情報漏えい等リスクと自社事業・サービス提供途絶リスクに焦点**を当てていることが挙げられる。この動きは、経済安保が海外への重要情報流出リスクと基幹インフラのサービス停止リスクに焦点を当てていることと符合している。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

サプライチェーン強化に向けたセキュリティ対策評価制度が持つ５層構造（★1~★5）

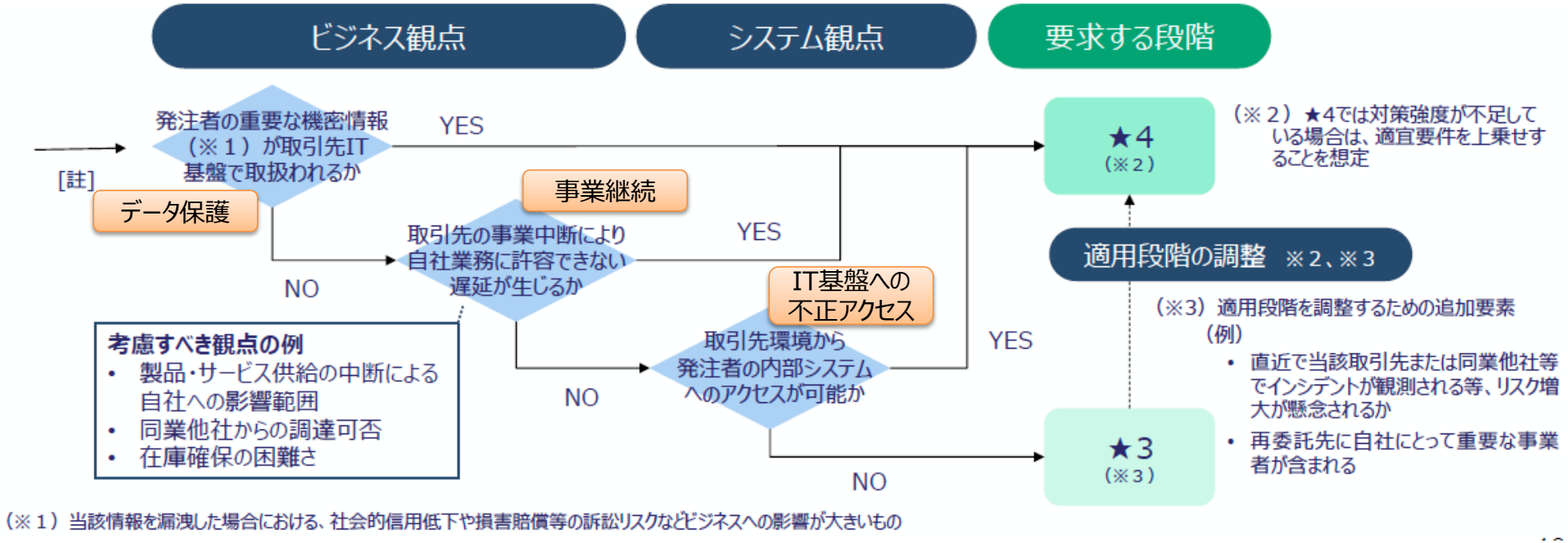
既存制度も取り込むことで、**「経営者の自己宣言(★1)／基本方針公開(★2)」→「自己評価(★3)」→「第三者評価(★4、★5)」とステップアップする複合的な制度**を検討中。幅広い企業を対象とできる反面で、やや複雑な制度と言えなくもない。**★3では実効性が高いシステム防御策に重点**が置かれ、英国Cyber Essentials制度との類似性が高い。他方で**★4では、組織全体の包括的なガバナンス／マネジメント等も重視**される。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

（参考）達成レベル選択の考え方（★3：自己評価と★4：第三者認証のどちらを選ぶか）

サプライヤ企業への適用にあたっては、スライド18の３つのサプライチェーンリスクに照らして適用レベル（★3 or ★4）を判断することを想定している。また、直近のインシデント発生状況を考慮して発注者がレベル調整等を行うことも検討されている。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

サプライチェーン強化に向けたセキュリティ対策評価制度の統制目標とレベル毎の評価基準（達成基準に相当）の記載方法

統制目標（要求事項）を定め、**その達成レベルごとに評価基準（達成基準に相当）を提示**している。達成基準を満たすことのエビデンスを記録することで、レビュー／監査への対応も可能になる。この構造は、自工会／部工会・サイバーセキュリティガイドラインと類似している。
なお、現時点で案出されているのは★3と★4の評価基準であり、★5の評価基準は現在検討中である。

- 統制目標（要求事項）
  44項目
  （技術的・システム的対策を求めるもの：20項目）
- 評価基準（達成基準）
  ★4は全ての統制目標で設定
  ★3は25の統制目標で設定

大分類	中分類	★3 No.	★4 No.	要求事項(案)		評価基準(案)	参照文献	技術的・システム的対策 (技術的・システム的な対策であり、運用を含む) (英国CEを参考に、技術的対策の対象となると考えられる要求事項)	技術検証 (英国CEを参考に、技術的対策の対象となると考えられる要求事項)
ガバナンスの整備	組織的文脈		1	セキュリティに関する法令や、契約等に規定される事項を考慮し、社内ルールを策定、教育・周知すること。	★4	・セキュリティに関連する以下の事項を把握した上で、社内ルールを策定すること - 自社が関連する法令(事業法、個人情報保護法等) - 所管省庁や関係団体における基準等 - 取引先等が提示する制限事項等も含めた、関係者からの要求事項 ・上記4項の改定状況について、年１回以上の頻度又は必要に応じて確認を行い、社内ルールの見直しを行うこと ・策定・見直した社内ルールを教育・周知すること	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和5年度版) 2.1.1(4) **自動車GL No.9, 11 (LV1)**		
	役割/責任/権限	1	2	セキュリティを担当する部署及び従業員を決定し、責任及び権限を割り当てること。	★3	・セキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を明確化すること ・平時のセキュリティ推進活動に必要な連絡先リストを整備すること	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和5年度版) 2.1.1(1)(4)(5)(6) **自動車GL No.13 (LV1)**		
					★4	・セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、情報セキュリティ委員会等の経営判断ができる体制を設置していること	ISO/IEC 27001:2022 4.4, A.5.4 政府統一基準(令和5年度版) 2.1.1(2) **自動車GL No.14 (LV2)**		
			3	サイバー攻撃や予兆を監視・分析をする体制を整備すること。	★4	・サイバー攻撃や脆弱性に関する公開情報、非公開情報を活用する体制を構築すること ・入手した情報やログの相関分析等により、サイバー攻撃の予兆やインシデントの発生の検知を可能とし、適切な対応が導き出せる体制を構築すること ※相関分析： 複合的なログなどで分析してセキュリティインシデントの予兆や痕跡を見つけ出す手法	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和5年度版) 7.1.4 **自動車GL No.16 (LV1), No.17 (LV2)**	○	
		2	4	秘密保持契約又は守秘義務契約を規定し遵守させること。	★3	・役員、正業員、社外要員(派遣社員等)を対象に、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 ・退職時又は期間満了時に会社の機密情報を持ち出させないこと	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**		
					★4	・自社の機密情報を取扱う役員又は従業員に、守秘義務の誓約書を提出させること(社外要員含む) ・派遣社員、受入出向社員について、派遣元、出向元の会社と業務開始前に守秘義務を締結すること ・当該守秘義務では、業務で知り得た情報を外部に漏えいさせない旨の記述を設けること	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.5,6 (LV2)**		

（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

重要情報漏えい防止の観点から見た サプライチェーン強化に向けたセキュリティ対策評価制度の注目点

APPTraS 営業秘密保護推進研究会

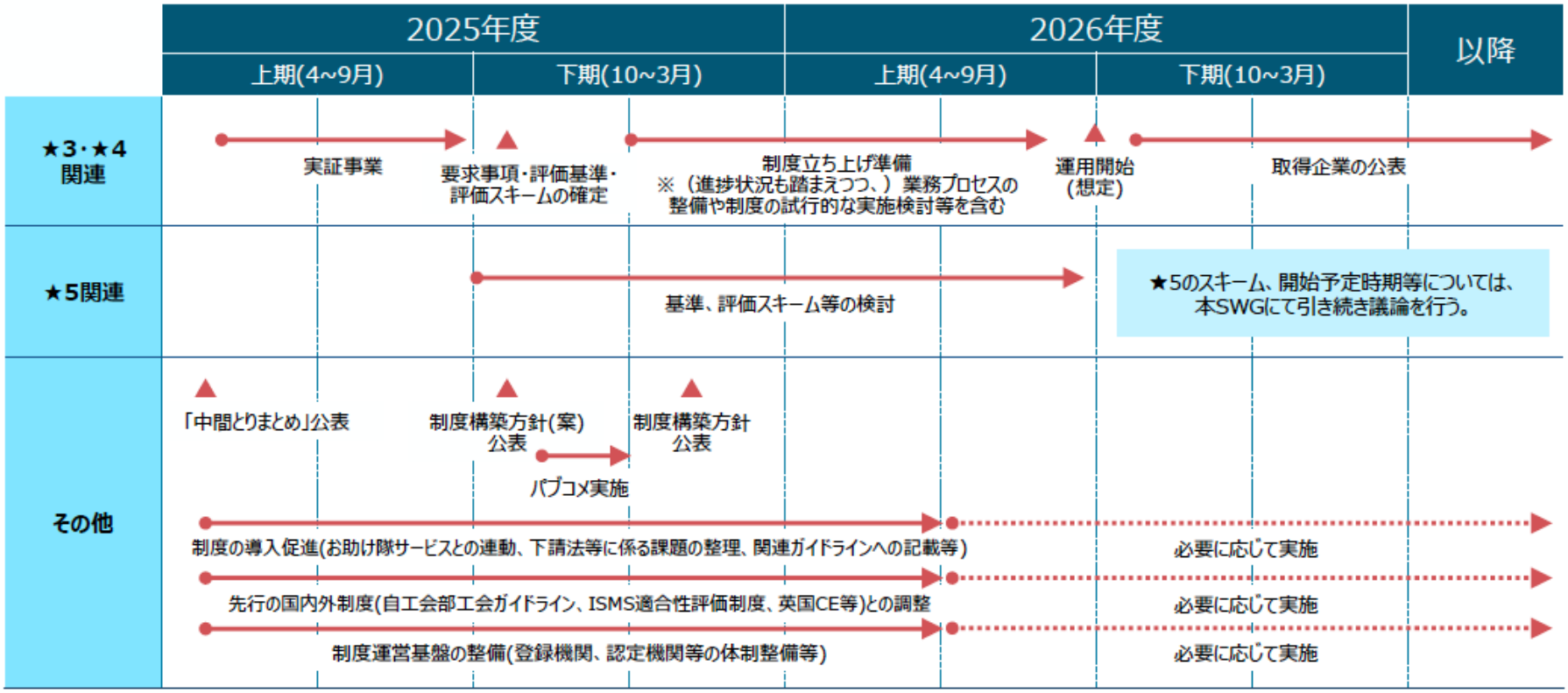
重要情報漏えい防止の観点から注目すべき要求事項を抜粋してみた。

分類	重要情報漏えい防止の観点から注目すべき要求事項（案）	★3の評価基準番号	★4の評価基準番号
経営の責任 ＜対応する大分類＞ ・ガバナンスの整備 ・リスクの特定 ・インシデントへの対応 ・インシデントからの復旧	秘密保持契約又は守秘義務契約を規定し、遵守させること	2	4
	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと	10	16
サプライチェーンの防御 ＜対応する大分類＞ ・取引先管理	取引先と自社のビジネス又はシステム上の関係を把握すること	5	8
	他社との間で、機密情報の取扱い方法を明確にすること	6	9
	重要な機密情報等を取扱う取引先のセキュリティ対策状況を把握すること	–	10
	セキュリティインシデント発生時の他社との役割と責任を明確にすること	–	11
	取引先との契約終了時に機密情報やアクセス権等を回収又は破棄すること	–	12
IT基盤の防御 ＜対応する大分類＞ ・攻撃等の防御 ・攻撃等の検知	システムや情報の重要度に応じて認証の強度や実装方法を決定すること	13	20
	社内システムを構成する端末にアカウントロック制御を実装すること		
	人の異動に伴うアクセス権の管理ルールを定めて運用すること	17	24
	サーバ等の設置エリアへの入退室を管理し、記録すること	–	25
	可搬媒体の持込み・持出しを制限すること	–	26
	情報機器、情報システムの保管データを適切に暗号化すること	–	29
	重要データを適切な場所に保管するようルールを定め、周知すること	–	30
	取引先等との情報共有や情報送信に関するルールを定め、周知すること	–	31

（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）　ved.

サプライチェーン強化に向けたセキュリティ対策評価制度の運用に向けた今後のスケジュール

2026年度の制度開始を目指し、実証事業による制度案の検討と並行して、制度運営基盤の整備や利用促進等を進めていく予定。



（出典）経済産業省：サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（2025年4月14日）

３．弊研究会独自の取組　～秘密保護のガバナンス／マネジメント及びリテラシー構築への意識を高める

弊研究会：
「秘密保護のガバナンス／マネジメント及びリテラシー構築チェックリスト」について

APPTraS 営業秘密保護推進研究会

チェックリスト開発の目的

「重要な秘密」漏えいや「他社の秘密」侵害を防止するための管理と事件発生時の初動対応の実効性を高めるためには、企業・組織の役職員１人ひとりがリスク（項目、内容、影響度等）の重大さをきちんと認識し、リスクを低減する行動の必要性に対する意識を高めて、自ら行動し始めることが重要。

弊研究会では、役職員１人ひとりの「重要な秘密」漏えいや「他社の秘密」侵害に関するアウェアネス（リスクの認識、リスク低減行動の必要性等）を向上させるために、貴社が構築したガバナンスとマネジメントが、現在どの程度充実しているのかを定期的にモニタリングするためのチェックリストを開発してきた。

現時点での進捗状況

現在、βテストに着手する段階。βテストにご協力くださる企業・組織を近々に募集する予定。
ご関心をお持ちの方は office@apptras.org **までご連絡ください。**

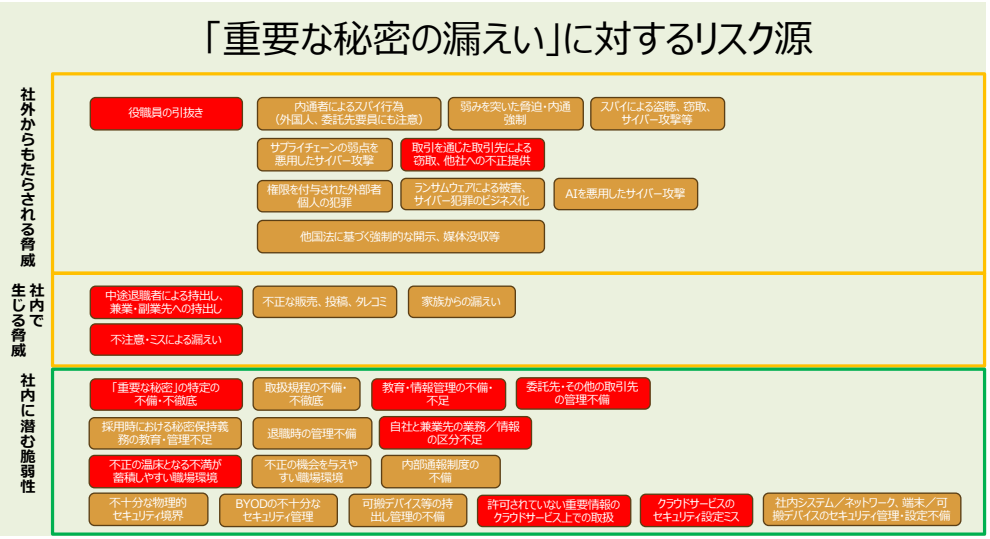
貴社のリスク選好の評価を支援するツールを提供

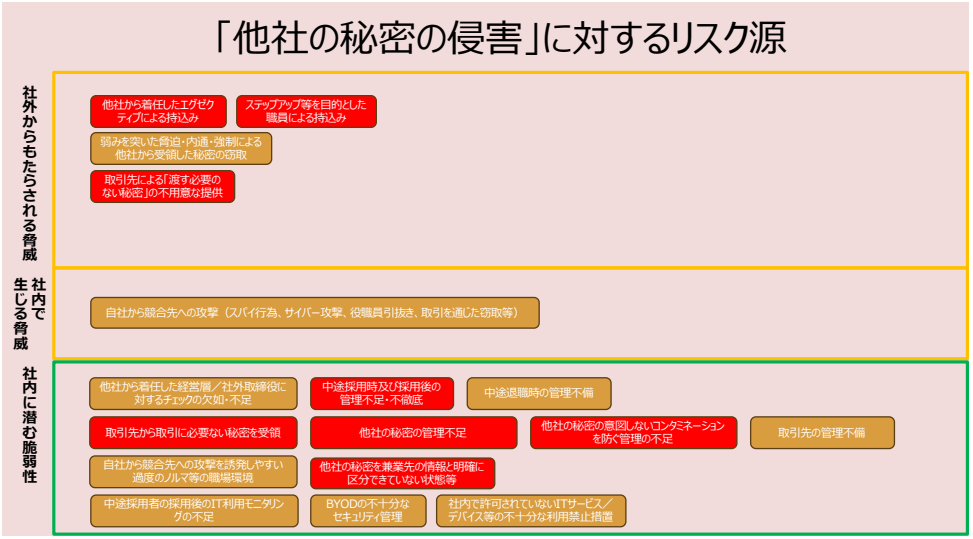
APPTraS 営業秘密保護推進研究会

「重要な秘密の漏えい／他社の秘密の侵害に繋がるリスクの選好」を支援するツール

企業・組織が「秘密保護を脅かすリスク」のどれを重視するかは、その事業内容・環境、経営方針、社会情勢等によってそれぞれ異なる。
そこで、各企業・組織が「秘密保護を脅かすリスク」のどれを重視して社内で共通認識を醸成すれば良いかをランキングできるツールを試作した。

<ランキングの対象とするリスク源（脅威、脆弱性）の例>



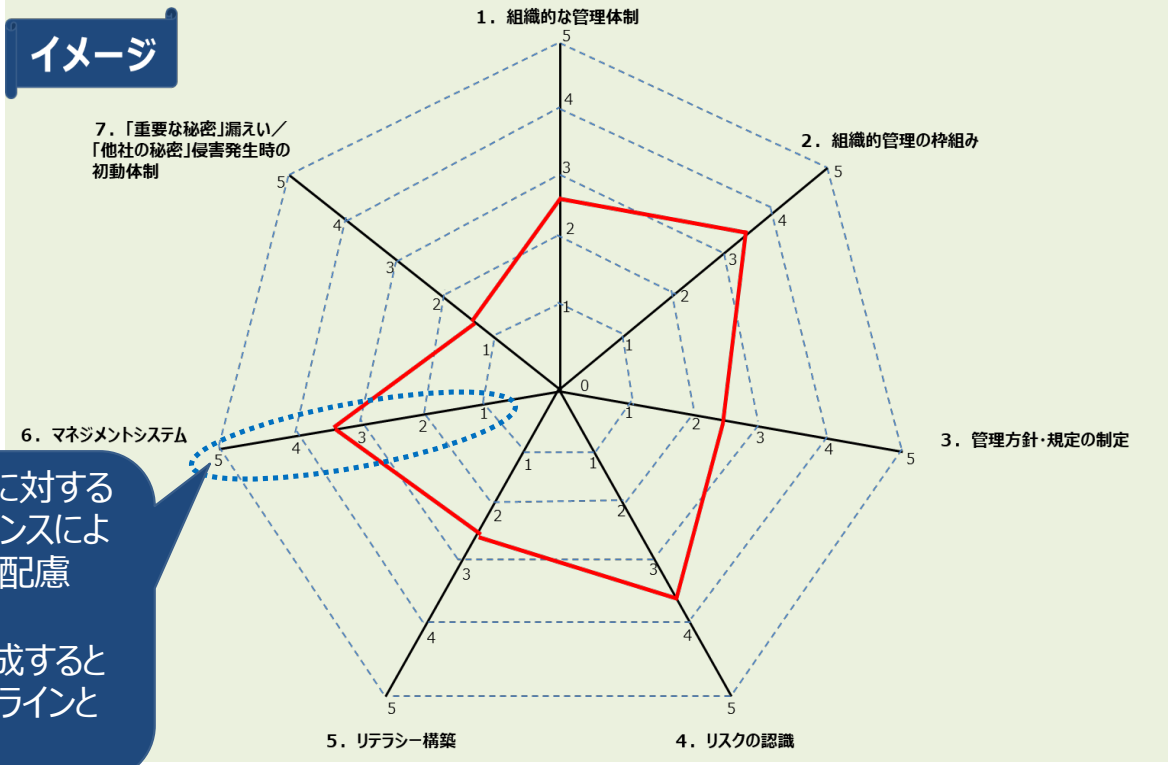


チェックリストによる評価結果のイメージ

このチェックリストでは、秘密の組織的な管理体制、組織的管理の枠組み、管理方針・規定の制定、リスクの認識、リテラシー構築、マネジメントシステム、事案発生時の初動体制の7項目を評価し、レーダーチャートの形にまとめることが可能。

（注）全ての項目で5を取ることは求めていない。

イメージ



チェックリストでは、レベル１から５に対する達成基準を個々に規定し、エビデンスによるレビュー／監査が可能となるよう配慮

なお、全ての項目で同レベルを達成するといった、本日紹介した制度・ガイドラインと同等の運用は想定していない

弊研究会：「秘密保護のガバナンス／マネジメント及びリテラシー構築チェックリスト」について

APPTraS 営業秘密保護推進研究会

チェックリストの評価対象7項目の評価内容について、「重要な秘密漏えい」防止と「他社の秘密侵害」防止を対比して整理した。

#	評価項目	「重要な秘密漏えい」防止のチェック項目	「他社の秘密侵害」防止のチェック項目
1	秘密の組織的な管理体制	情報資産管理への組織的取組み、個々の「重要な秘密」の管理責任者の任命とその管理	情報資産管理への組織的取組み、個々の「他社の秘密」の管理責任者の任命とその管理
2	秘密の組織的管理の枠組み	「重要な秘密」の特定、表示と識別、「重要な秘密」を取扱う業務の管理、共有範囲の指定	「他社の秘密」の受領プロセス、表示と識別、共有範囲の指定・調整、取引先に疑念を生じさせない類似プロジェクト体制の実践、中途転入者の着任時の管理
3	秘密保護に関する規程類の整備	「重要な秘密」の情報管理規程整備、リテラシー構築に関する規程整備	取引先から受領した「他社の秘密」の情報管理規程整備
4	秘密保護に関するリスクの認識	企業全体／各部門で重視するリスク源の共通認識の熟成	企業全体／各部門で重視するリスク源の共通認識の熟成
5	秘密に対するリテラシー構築のための教育	「重要な秘密」の内容と識別・ラベル表示に関するリテラシー構築、リスク認識の共有、管理方針／規程の周知徹底	取引で受領した「他社の秘密」と自社情報の区別・ラベル表示に関するリテラシー構築、リスク認識の共有、管理方針／規程の周知徹底
6	秘密管理のマネジメントシステム	マネジメントシステムの運用、経営者のコミット	マネジメントシステムの運用、経営者のコミット
7	秘密漏えい時の初動体制	初動体制の整備、不審な取扱いに気付いた時の報告の浸透	初動体制の整備、不審な取扱いに気付いた時の報告の浸透

本資料の内容についてのお問い合わせは下記までお願いします。

合同会社三笠ポリシーアドバイザリ　代表社員
営業秘密保護推進研究会 事務局長　三笠 武則

(e-mail) takenori.mikasa@mikasa-pa.jp