サプライチェーンでの重要情報漏えい防止を重視する２つの新制度の比較と実務ポイントの解説

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）

本資料では、次の２つの制度・ガイドラインを対象として、その要求事項の比較や、要求事項等から知りうる重要情報漏えい防止の実務ポイントについて解説します。

- 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
  ※以後、「サプライチェーン対策評価制度」という

- 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
  ※以後、「自工会・部工会ガイドライン」という

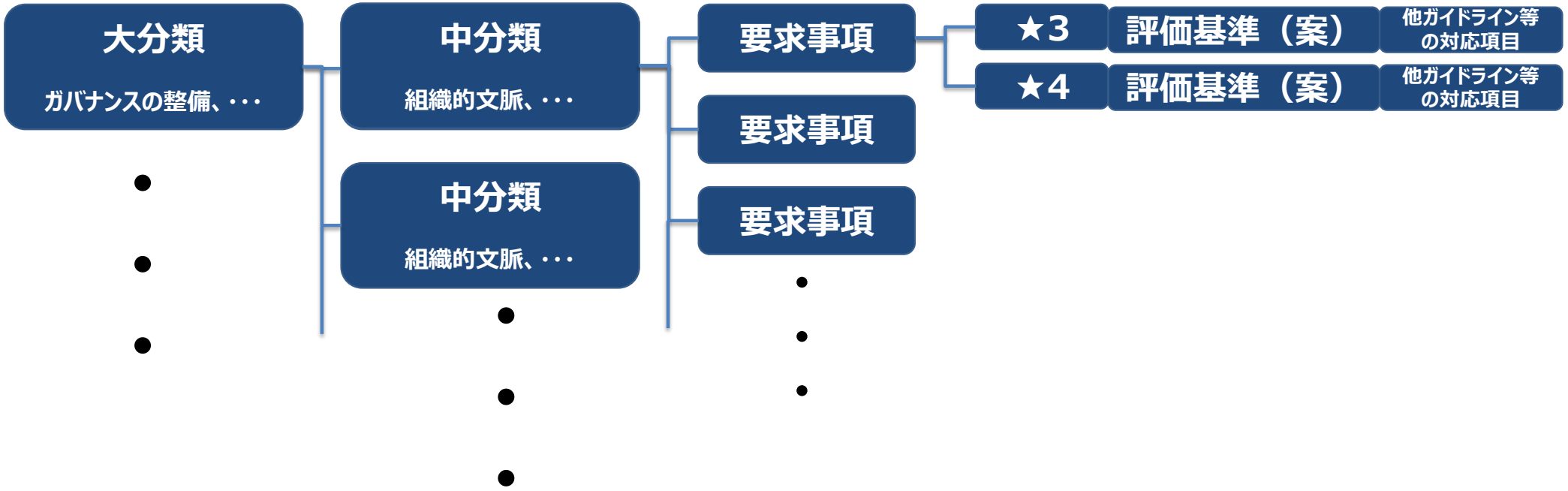
目次

APPTraS
営業秘密保護推進研究会

１．要求事項と達成／評価基準の記載方法について

サプライチェーン対策評価制度の要求事項と評価基準の記載方法

サプライチェーン対策評価制度では、要求事項は**「大分類」と「中分類」で整理**されている。
各要求事項には１つまたは複数の評価基準（案）が割り当てられ、それぞれに対して**達成レベル（★3、★4）が定められている**。
また、評価基準（案）毎に、自工会ガイドライン、ISO/IEC27001等の他のガイドライン等の対応項目が「参考文献」としてマッピングされている。



（参考）サプライチェーン対策評価制度の記載例

APPTraS 営業秘密保護推進研究会

【参考資料1】 ★3・★4要求事項・評価基準案一覧

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、運用を委託している事業者等に実施させることが一般的に想定されるもの)	技術検証 (英国CEを参考に、技術検証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、契約等に規定された事項を考慮し、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 ・上記事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) 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、従業員、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(社外要員除く) ・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)**		
	ポリシー	3	5	自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。	★3	・自社のセキュリティ対応方針を策定し、文書化すること ・セキュリティ対応方針(ポリシー)を役員、従業員、社外要員(派遣社員等)から容易に確認できる状態にすること ・定常的に、かつ、セキュリティ対応方針の改正時に役員、従業員、社外要員(派遣社員等)へと周知すること	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和5年度版) 2.1.3(2) **自動車GL No.1,3 (LV1)**		

自工会・部工会ガイドラインの要求事項と評価基準の記載方法

自工会・部工会ガイドラインでは、整理軸として**14個のラベル**が用意され、**それぞれに目的**が規定されている。
要求事項はラベル毎に整理されており、**各要求事項に対して１つ又は複数の達成条件とその達成基準**が定められている（達成条件毎に付番）。
さらに、**達成条件毎に達成レベル**（Lv1、Lv2、Lv3）を定めている。

自工会・部工会ガイドラインの記載例

APPTraS 営業秘密保護推進研究会

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
13 取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	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	70	Lv1	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している	【規則】 ・一覧表には取引に伴い授受／使用される情報資産とその取り扱いを記載し、取引先と相互に把握すること 【対象】 ・重要な情報資産（No.54 で定められた機密レベルが高い情報資産など）を共有する取引先 【頻度】 ・取引開始時／取り交わす情報・手段の変更時
			71	Lv3	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)の一覧を定期的、または必要に応じて、見直ししている	【頻度】 ・1 回/年 以上
		IT 機器調達における情報セキュリティリスクを管理すること	72	Lv3	IT 機器調達に対するセキュリティ要求事項が決められており、社内に周知されていること	【規則】 ・機器調達に対するセキュリティ要求事項を一覧化していること ・機器調達時に、セキュリティ要求事項を容易に確認できる状態にすること 【対象】 ［機器］ ・社内ネットワークに接続する IT 機器 ［周知］ ・役員、従業員、社外要員（派遣社員等） 【頻度】 ・定常的に、かつ、機器調達時のセキュリティ要求事項の改正時に周知すること
			73	Lv3	IT 機器調達に対するセキュリティ要求事項を購入先と共有しており、購入時の評価結果を記録し保管している	【規則】 ・セキュリティ要求事項が購買契約等に明記されていること ・機器調達時に、セキュリティ要求事項の評価を実施し、結果が保管されていること ・定期的に確認結果が保管されていることを確認する 【対象】 ・社内ネットワークに接続する IT 機器 【保管状態の確認頻度】 ・1 回以上/年

2．要求事項一覧

サプライチェーン対策評価制度の要求事項一覧

APPTraS 営業秘密保護推進研究会

経営の責任

サプライチェーンも含めた組織ガバナンスの整備、**資産管理**（取引先等とのネットワーク接続管理等）、インシデント対応、**事業継続**が求められている。

大分類	中分類	要求事項
ガバナンスの整備	組織的文脈	セキュリティに関する法令や、契約等に規定された事項を考慮し、社内ルールを策定、教育・周知すること
	役割／責任／権限	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
		サイバーセキュリティや予兆を監視・分析する体制を整備すること
		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
	ポリシー	自社のセキュリティ対応方針（ポリシー）を策定し、周知すること
	監督	セキュリティ対策状況を定期的に棚卸し、見直しを行うこと
		定期的に経営層へ対策実態に関する報告を行い、結果を対策の推進に反映すること
リスクの特定	資産管理	ハードウェア、OS、ソフトウェアの情報に関する一覧を作成すること
		ネットワークの情報に関する一覧を作成すること
		取引先等とのネットワーク接続を管理すること
		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
	リスクアセスメント	脆弱性の管理体制、管理プロセスを定めること
インシデントへの対応	インシデントマネジメント	あらかじめ定めた手順に沿ってセキュリティインシデントに対応すること
インシデントからの復旧	インシデント復旧計画の実行	事業上重要なシステムについて、**事業継続の要件に沿う復旧に必要な準備を行うこと**

サプライチェーン対策評価制度の要求事項一覧

APPTraS 営業秘密保護推進研究会

サプライチェーンの防御

取引先管理は、サプライチェーンセキュリティ対策においてキモとなるところである。

取引先との間のビジネス／システム上の関係を把握した上で、これ**を踏まえて**、**機密情報の取扱い方法の明確化**、機密情報等を取扱う取引先の**セキュリティ対策状況の把握**、**インシデント発生時の役割と責任の分担の明確化**、**取引終了時の機密情報・アクセス権等の回収・破棄**を行うことを求めている。

大分類	中分類	要求事項
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	**取引先と自社とのビジネス又はシステム上の関係を把握すること**
		他社との間で、機密情報の取扱い方法を明確にすること
		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
		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
		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

サプライチェーン対策評価制度の要求事項一覧

APPTraS 営業秘密保護推進研究会

IT基盤の防御

攻撃等の防御に関する要求事項は、**概ねサプライチェーンに特化したものではない**。

大分類	中分類	要求事項
攻撃等の防御	アイデンティティ管理とアクセス制御	ユーザID の発行・変更・削除の手続きを定めること
		管理者IDの発行・変更・削除の手続きを定めること
		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
		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
		パスワード設定に関するルールを定め、周知すること
		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。
		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
		可搬媒体の持込み・持出しを制限すること
	意識向上及びトレーニング	経営陣を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること
		IT又はセキュリティを担当する部署の職員に対して、最新の知識とスキルを維持するための教育・研修を実施すること
・・・次ページに続く		セキュリティインシデント発生時の対応に関する教育・訓練を行うこと

サプライチェーン対策評価制度の要求事項一覧

APPTraS 営業秘密保護推進研究会

IT基盤の防御

データセキュリティについては、**取引先等との情報共有／情報送信に関するルールを定めて周知する等、一部サプライチェーンに関する要求事項が存在**している。

大分類	中分類	要求事項
攻撃等の防御	データセキュリティ	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
		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
		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
		適切なバックアップを行うこと
	プラットフォームセキュリティ	ハードウェア・ソフトウェア等の安全な構成を確立し、維持すること
		サポート期限の切れたハードウェア・ソフトウェアの利用停止や更改を実施すること
		情報機器、情報システムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと
		ハードウェア・ソフトウェア等へのセキュリティパッチやアップデートの適用に係る手続等を策定し、実行すること
		システムをマルウェア感染から保護すること
	技術インフラのレジリエンス	内外のネットワークを適切に分離し、境界部分を防護すること
		社内から社外への不正な通信を遮断する対策を実施すること

サプライチェーン対策評価制度の要求事項一覧

IT基盤の防御

攻撃等の検知に関する要求事項は、**概ねサプライチェーンに特化したものではない**。

大分類	中分類	要求事項
攻撃等の検知	継続的モニタリング	ネットワーク上の適切な場所でネットワーク接続やデータ転送を監視すること
		ハードウェアやソフトウェアの状態や挙動を監視すること
	有害イベントの分析	セキュリティインシデントとして扱う対象範囲を明確にし、運用していること

自工会・部工会ガイドラインの要求事項一覧

自工会・部工会ガイドラインの要求事項には、**一部、サプライチェーンに特化したものが組み入れられている**。
ここではラベル８で、**サプライチェーン上で発生する情報セキュリティ要件の明確化**を求めている。

ラベル	要求事項
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機密情報を扱うルール	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
３法令順守	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リスクを管理する体制を整備し、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	自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること
	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
	自組織内あるいは組織を跨いで影響する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・訓練を行なっていること
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

自工会・部工会ガイドラインの要求事項一覧

APPTraS 営業秘密保護推進研究会

業務委託に係る情報セキュリティ対策、**取引で交わされる情報資産とその手段**の把握、**IT機器調達における情報セキュリティリスク**の管理、**外部への接続状況**の把握・管理及び**他組織との連携・データ交換の監視**が求められている。

ラベル	要求事項
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なっていること
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**
	IT機器調達における情報セキュリティリスクを管理すること
14 外部への接続状況の把握	**関係組織（サプライヤー等含む）との関係において、自組織の通信ネットワーク構成を把握し、他組織との連携状態やデータの流れを監視すること**
	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
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なっていること
	リモートワークの環境において、セキュリティ事故（主に情報漏えい、なりすまし）を抑制する対策を行なっていること
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なっていること
	社内への入退室において、セキュリティ事故（主に不正侵入、不正持ち出し、情報漏えい、不審行動）を抑制する対策を行なっていること
	持込み・持出し物の制限を行なっていること
	社内の撮影・録音において、セキュリティ事故（主に情報漏えい）を抑制する対策を行なっていること
	脆弱性が発見された際の対策対象の把握や外部記憶媒体を用いた情報漏えい等を抑制する対策が行えていること
	重要情報を格納・利用するシステムにおいて、人為的設定ミスによる被害を最小化する対策を実施していること

自工会・部工会ガイドラインの要求事項一覧

APPTraS 営業秘密保護推進研究会

21 オフィスツール関係では、メールシステムや、ファイル送信Webアプリケーション（クラウドサービスを含む）等が対象になる。これらのシステム／サービスでは、**関係会社やパートナー会社とファイル共有する際の利用ルール*を定めて周知**することが求められている。　*意図した送信だけでなく、誤送信にも気を配る必要がある

ラベル	要求事項
17 通信制御	サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正なWebサイトへの通信制御を行なっていること
18 認証・認可	情報システム・情報機器への認証・認可の対策を行なっていること
19 パッチやアップデート適用	サポート期限が切れた機器、OS、ソフトウェアを利用しないようにしていること
	脆弱性を利用した不正アクセスを防止する施策を実施していること
20 データ保護	情報システム・情報機器のデータ保護を行なっていること
21 オフィスツール関係	**情報システム・情報機器のデータ保護を行なっていること**
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マルウェア対策を行なっていること
23 不正アクセスの検知	ネットワークへの不正アクセスを常時監視する体制を構築すること
	セキュリティ事件・事故が発生した場合に、侵入経路や漏えい経路の調査が行えるよう、ログが取得されていること
	標的型攻撃など、サイバー攻撃を速やかに検知、遮断する対策を行なっていること
24 バックアップ・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とどめる対策を行なっていること
	セキュリティインシデントを想定し事業継続の要件に沿う復旧に必要なデータを準備できていること

３．「サプライチェーン対策評価制度」と「自工会・部工会ガイドライン」の要求事項の比較

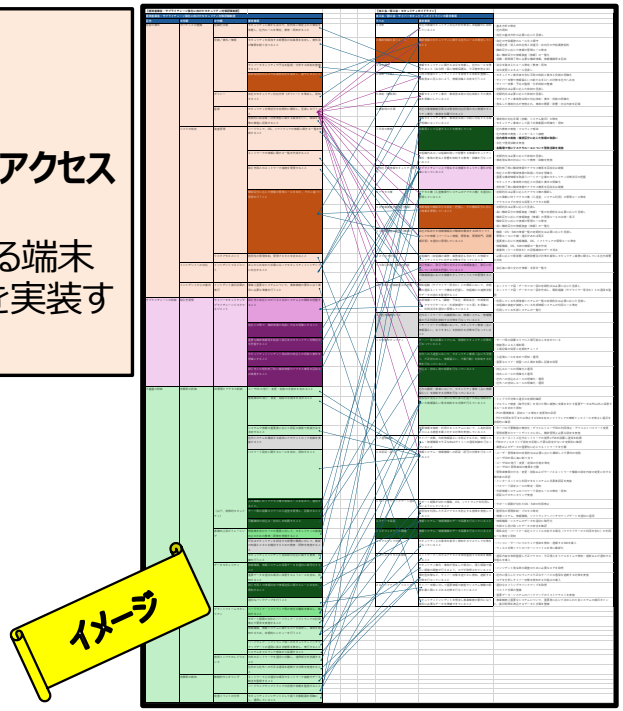
サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項は、構成こそ違えど、内容は相互にほぼ紐付けできることが分かった。両制度のうち一方だけしかカバーしていない要求事項はほとんどない（だからといって両制度が簡単に相互運用できる訳ではないことに注意！）。詳細については、次ページ以降で述べる。

片方の制度だけでしかカバーされていない要求事項

サプライチェーン対策評価制度

- **攻撃等の防護**
  - **アイデンティティ管理とアクセス制御：**
    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

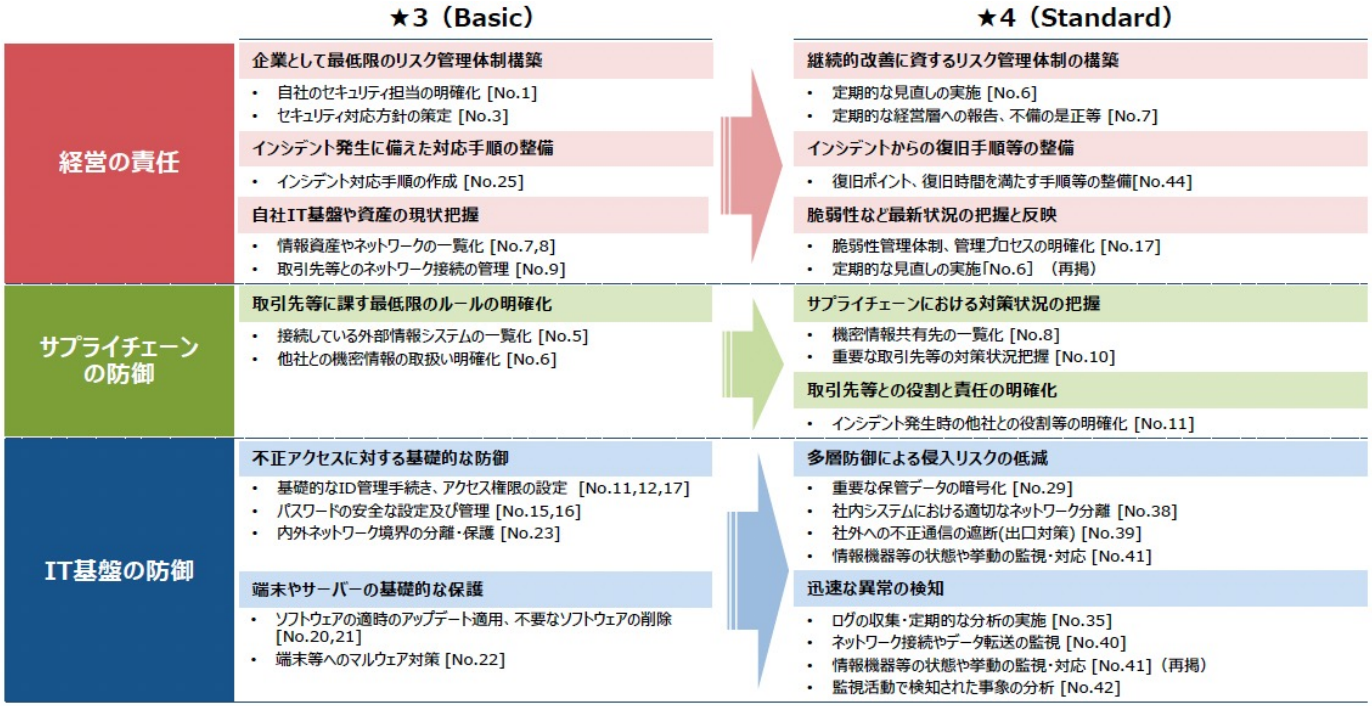


自工会・部工会ガイドライン

- **6 事故時の手順**
  - 自社の事業継続計画又は緊急時対応計画の中に情報セキュリティ事件・事故を位置づけること
- **13 取引内容・手段の把握**
  - IT機器調達における情報セキュリティリスクを管理すること
- **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なっていること
  - リモートワークの環境において、セキュリティ事故（主に情報漏えい、なりすまし）を抑制する対策を行なっていること
- **16 物理的セキュリティ**
  - 社内の撮影・録音において、セキュリティ事故（主に情報漏えい）を抑制する対策を行なっていること

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

サプライチェーン対策評価制度では、レベル毎に**達成すべき「経営の責任」「サプライチェーンの防御」「IT基盤の防御」に資する対策を提示**している。自工会・部工会ガイドラインにはこうしたフレームワークがないので、**当該ガイドラインをこの枠組で整理して、両者を比較**してみた（次ページからの３スライドを参照）。



（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）

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

サプライチェーン対策評価制度と自工会・部工会ガイドラインの両方で、**「経営者の責任」に当たる要求項目**を整理してみた。これを見ると、大枠では、**項目を相互に漏れなくマッピングできることが良くわかる**。

サプライチェーン対策評価制度：経営の責任

ガバナンスの整備	組織的文脈　※ルール整備、教育、法令順守
	役割／責任／権限 ※平時の体制・ルール・責任と権限、秘密保持契約の遵守
	ポリシー
	監督　※PDCAの運用、ルール・台帳等の見直し
リスクの特定	資産管理 ※機密区分に応じた情報管理ルール策定・管理を含む
	リスクアセスメント ※脆弱性管理
インシデントへの対応	インシデントマネジメント
インシデントからの復旧	インシデント復旧計画の実行

自工会・部工会ガイドライン：経営の責任

１方針	２機密を扱うルール	３法令順守
４体制（平時）※責任と役割を含む	５体制（事故時） ※4に同じ	６事故時の手順 ※事故の範囲、計画策定
10 情報資産の管理（情報）※ルール化・一覧化	11情報資産の管理（機器）　※10に同じ	12リスク対応
14外部への接続状況の把握 ※10に同じ	19パッチやアップデート適用 ※体制・プロセス整備	24バックアップ・リストア ※事業継続要件との合致

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

APPTraS 営業秘密保護推進研究会

「サプライチェーンの防御」に関する要求項目についても、大枠では、**相互に漏れなくマッピングできることが良くわかる**。

サプライチェーン対策評価制度：サプライチェーンの防御		**自工会・部工会ガイドライン：サプライチェーンの防御**	
取引先管理 - サイバーセキュリティサプライチェーンリスクマネジメント	取引先と自社とのビジネス又はシステム上の関係を把握	８他社との情報セキュリティ要件 ※機密情報の取扱い／回収・破棄、対策状況の把握、事故時の役割と責任	13取引内容・手段の把握 ※取引で取り交わす情報とその手段
	他社との間で機密情報の取扱い方法を明確化	14外部への接続状況の把握　※外部情報システムの明確化と利用状況の管理	ー
	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の把握		
	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の明確化		
	取引先との契約終了後に機密情報やアクセス権等を回収又は破棄		

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

APPTraS 営業秘密保護推進研究会

「IT基盤の防御」に関する要求項目についても、大枠では、**相互にほぼ漏れなくマッピングできることが良くわかる**。

サプライチェーン対策評価制度：IT基盤の防御		**自工会・部工会ガイドライン：IT基盤の防御**		
攻撃等の防御	アイデンティティ管理とアクセス制御　※異動時のアクセス権管理ルール策定・運用、物理的セキュリティを含む	６事故時の手順　※事故として扱う範囲の明確化	－	－
	意識向上及びトレーニング	７日常の教育　※「自組織を跨ぐ事件・事故抑制の教育」については**マッピング不可**	９アクセス権　※異動時のアクセス権管理ルール、アクセスログ管理	15社内接続ルール ※社内・リモートワークからの接続、**マッピング不可**
	データセキュリティ　※重要データの保管場所、暗号化、バックアップ、取引先との情報共有・送信ルール	16物理的セキュリティ	17通信制御　※境界防御、社内ネットワーク分離	18認証・認可 ※ログ取得とレビューを含む
	プラットフォームセキュリティ ※安全な構成、サポート切れ対応、ログ取得とレビュー、パッチ等の適用、マルウェア感染防止	19パッチやアップデート適用 ※サポート切れ対応を含む	20データ保護 ※データ暗号化	21オフィスツール　※関係先・パートナー企業とのファイル共有ルール
	技術インフラのレジリエンス　※社内ネットワーク分離、社内から社外への不正通信遮断	22マルウェア対策	23不正アクセスの検知 ※常時監視、リアルタイム検知・遮断、通知 ※ログ取得・分析 ※社内に侵入したマルウェアと不正サーバの通信遮断	24バックアップ・リストア ※バックアップ取得・リストア手順のテスト
攻撃等の検知	継続的モニタリング			
	有害イベントの分析　※インシデントの対象範囲の明確化			

【低減するリスクの枠組みについて】

サプライチェーン対策評価制度では：
- 機密情報の漏えい・改ざんリスク（→データ保護）
- 事業・サービス途絶リスク（→事業継続）
- 取引先を踏み台とした不正侵入リスク（→IT基盤への不正アクセス防止）

という**３つのサプライチェーンセキュリティリスクへの対応に焦点**を当てている。

一方で、**自工会・部工会ガイドラインは**、**重視する**サプライチェーンセキュリティリスクの**枠組みを必ずしも前面に打ち出していない**。

今回の連続セミナーの趣旨が「重要情報の漏えい」や「重要情報の海外流出」の防止にあることを考慮し、ここでは上記３つのリスクのうち**「機密情報の漏えい・改ざんリスク」に焦点を絞り、その低減に深く関わる要求事項を抜粋して**、サプライチェーン対策評価制度と自工会・部工会ガイドラインの**比較を試みた**。（次ページ以降参照）

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

APPTraS 営業秘密保護推進研究会

「経営の責任」に関する重要な実務ポイントは**守秘義務、機密区分に応じた情報資産（情報）の一覧化と管理、退職時等の秘密情報等の回収**等であり、両者でこれらの要求事項を共有している。

サプライチェーン対策評価制度：経営の責任

ガバナンスの整備：役割／責任／権限
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

リスクの特定：資産管理
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

自工会・部工会ガイドライン：経営の責任

2 機密を扱うルール：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)(5)(6)自社の守秘義務のルールを規定し、守らせている／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
- (7)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

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
- (54)(55)機密区分に応じた情報の管理ルールを定め、定期的又は必要に応じて見直している
- (56)(57)高い機密区分の情報資産（情報）を一覧化し、定期的又は必要に応じて見直している
- (58)情報資産（情報）は機密区分に応じた管理ルールに沿って管理している

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
- (65)廃棄時(リース終了時含む)は、記憶媒体のデータを消去している

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

「サプライチェーンの防御」に関する重要な実務ポイントは**他社と取り交わす情報資産とその手段**、**他社から入手した情報資産の自社内での取扱い**、**重要な情報を扱うパートナー企業のセキュリティ対策状況等の把握**に加え、**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の明確化**、**取引終了後の情報資産・権限の回収・破棄**等であり、両者でこれらの要求事項を共有している。

サプライチェーン対策評価制度：サプライチェーンの防御

取引先管理：サイバーセキュリティサプライチェーンリスクマネジメント

- 取引先と自社とのビジネス又はシステム上の関係を把握すること
- 他社との間で、機密情報の取扱い方法を明確にすること
- 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
- 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
- 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

自工会・部工会ガイドライン：サプライチェーンの防御

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

- (42)重要な機密情報を取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
- (43)契約終了時に機密情報やアクセス権などを回収または破棄している
- (44)(45)他社との間で、機密情報の取り扱い方法が明確になっており、定期的又は必要に応じて見直ししている
- (46)(47)情報セキュリティ事件・事故時の他社との役割と責任が明確であり、定期的又は必要に応じて見直ししている
- (48)他社から入手した重要機密情報が、自社内でどのように取り扱われているか実状を把握している

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

- (70)(71)会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化し、定期的又は必要に応じて見直ししている

サプライチェーン対策評価制度と自工会・部工会ガイドラインの要求事項の比較

APPTraS 営業秘密保護推進研究会

「IT基盤の防御」については**自工会・部工会ガイドラインの方が少し踏み込んで要求**している。重要な実務ポイントでは**物理セキュリティが重視**され、**パートナー企業とのファイル共有ルール、暗号化、シャドウIT対策、異動時の管理、機密区分に応じた情報の取り扱い等にも配慮**されている。

サプライチェーン対策評価制度：IT基盤の防御

攻撃の防御：アイデンティティ管理とアクセス制御
- 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
- 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
- 可搬媒体の持込み・持出しを制限すること

攻撃の防御：意識向上及びトレーニング
- 経営陣を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること

攻撃の防御：データセキュリティ
- 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
- 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

攻撃の防御：プラットフォームセキュリティ
- ハードウェア・ソフトウェア等の安全な構成を確立し、維持すること

自工会・部工会ガイドライン：IT基盤の防御

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
- (30) 機密区分に応じた情報の取り扱いに関する教育を行なっている
- (32) 各職場で特に重要なリスクやルールについて啓発活動を実施している

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
- (49)(50)人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている

16 物理的セキュリティ：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なっていること
- (84)-(86)入場可能な人を定めている、施錠で入場を制限、入場記録の保管と定期的チェック

社内への入退場において、セキュリティ事故(主に不正侵入、不正持ち出し、情報漏えい、不審行動)を抑制する対策を行っていること
- (88)(89)入退場ルールを定めて周知・運用、重要なエリア・部屋への入場制限と記録保管

持込み・持出し物の制限を行なっていること
- (91)(92)持込み／持出しルール明確化及び運用

脆弱性が発見された際の対策対象の把握や外部記憶媒体を用いた情報漏えい等を抑制する対策がおこなえていること
- (98)PCで利用を許可または禁止するソフトウェアを定め、ソフトウェアの無断インストールを禁止し、違反がないか定期的に確認している

20 データ保護：情報システム・情報機器のデータ保護を行っていること
- (129)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
- (130)外部から受け取ったデータが安全であることを確認している

21 オフィスツール関連：情報システム・情報機器のデータ保護を行っていること
- (131)(132)メール送信による情報漏えい対策、メール誤送信を防止する対策
- (135)関係会社やパートナー企業とファイル共有する場合の利用ルールを定め、周知している（クラウドサービス利用も含む）

４．両制度の要求事項、達成／評価基準を踏まえた重要情報漏えい防止の実務ポイント

実務上のポイントを解説する重要な要求事項の一覧（1/2）

以下では、**機密情報の漏えいリスクを低減するために重要な**、サプライチェーン対策評価制度と自工会・部工会ガイドラインで**相互に連関している要求事項を具体的に取り上げ**、その**達成／評価基準から得られる実務上のポイントを解説**する。

取り上げて解説を加える要求事項は次の7項目（次ページに続く）。

区分	取り上げる要求事項	サプライチェーン対策評価制度の記載	自工会・部工会ガイドラインの記載
経営の責任	**機密区分に応じた**重要情報の管理	リスクの特定：資産管理 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 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
サプライチェーンの防御	**他社との間の**機密情報の取扱方法の**明確化**	取引先管理：サイバーセキュリティサプライチェーンリスクマネジメント 他社との間で、機密情報の取扱い方法を明確にすること	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
	他社から入手した重要機密情報の自社内での**取扱実態把握**	ー	
	会社毎に取り交わす情報・手段の**一覧化**	取引先管理：サイバーセキュリティサプライチェーンリスクマネジメント 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	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

実務上のポイントを解説する重要な要求事項の一覧（2/2）

APPTraS 営業秘密保護推進研究会

取り上げて解説を加える要求事項（続き）：

区分	取り上げる要求事項	サプライチェーン対策評価制度の記載	自工会・部工会ガイドラインの記載
IT基盤の防御	**機密区分に応じた情報の取扱に関する教育**	攻撃等の防御：意識向上及びトレーニング 経営陣を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること	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
	物理的セキュリティの再点検	攻撃等の防御：アイデンティティ管理とアクセス制御 • 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 • 可搬媒体の持込み・持出しを制限すること	16 物理的セキュリティ 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なっていること
	取引先等とのファイル共有／送信時のメール／サービス利用ルールの策定・周知	攻撃等の防御：データセキュリティ 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	21 オフィスツール関係 情報システム・情報機器のデータ保護を行なっていること

機密区分に応じた重要情報の管理

APPTraS 営業秘密保護推進研究会

機密情報の資産管理の充実を！そのためには台帳管理を確実に！また個々の機密情報の管理者の役割がポイント！

- **資産管理はリスク管理**。まずは、機密情報が事業リスクを伴う自社資産であることを、**全職員が改めて認識し直し、全社で危機感を共有することが必要**。
- 管理充実の手筈は、サプライチェーン対策評価制度と自工会・部工会ガイドラインが共通して求める構造：
「機密の特定」ー「機密区分のレベル判定と表示」ー「区分に応じた取扱いー取扱エリアの区分及び制限ー定期的及び必要に応じた管理ルールの見直し」
これに加えて、退職や期間満了時の漏れなき回収が重要。
- 改めて見直していただきたいのは、**事業リスクの程度と機密区分設定のバランス**。
秘密情報の**ほとんどが実態として同じ機密区分**になってしまっていないか？当事者の従業員による機密区分の選択判断が難しく、**「念のため高レベル機密」になってしまっていないか**を点検することが望ましい。
厳格な管理を要する**高レベル機密が多ければ多いほど管理は重くのしかかる**ことになる。
- サプライチェーン対策評価制度も自工会・部工会ガイドラインも、**高い区分の機密情報の一覧管理と定期的又は必要に応じた見直し**を求めている。このためには、基本に戻って機密情報の**台帳管理を確実にする**ことが重要。
- 特に、**高い区分の機密情報を過不足無きように保つことが重要**。すでに述べた通り過大だと管理コストが非現実化する。不足だと高リスクを抱え込んでしまう。これに関連して、**機密区分の適時の上げ下げ**にも力を注ぐべき。
- 高い区分の機密情報の一覧化と資産管理では、サプライチェーン対策評価制度も自工会・部工会ガイドラインも、次の項目の管理を要求：
対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先。
これらの情報を誰が管理するのかがポイント。ここで言う「管理者」が管理するならば、**「管理者」が実効的に実務できる体制の確保**がポイント！
また、この管理項目に**「開示可能範囲」を追加し、管理者が適時に見直す**ことを検討してはいかが？

（参考：達成／評価基準の抜粋）機密区分に応じた重要情報の管理

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
リスクの特定	資産管理	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	★3	・情報資産(情報)を対象に、以下の内容等を含む管理ルールを定め、文書化していること - 機密の特定　- 機密区分のレベル判定と表示 - 区分に応じた取り扱い方法　- 取り扱いエリアの区分及び制限 - 機密区分のうち、高い機密区分の情報資産(情報)を一覧化すること - 高い機密区分の情報資産(情報)一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと
			★4	・退職や期間満了時には機密情報、情報機器等を回収すること - 回収物には、情報(印刷物、記憶媒体)、情報機器(パソコン、スマートデバイス)、アクセス権(ID、鍵)を含めること - 回収漏れが起こらない手順(例：回収物一覧のチェックシートの作成等)を整備、運用すること - サーバ、会社支給のパソコン、スマートデバイス、外部記憶媒体の廃棄時(リース終了時含む)はデータを復元できないよう消去すること ※ディスクのフォーマットは、データを復旧される可能性があるため不可 - サーバ、会社支給のパソコン、スマートデバイス、外部記憶媒体の記憶領域の消去を実施した記録又は業者の廃棄証明書を保管すること

（参考：達成／評価基準の抜粋）機密区分に応じた重要情報の管理

APPTraS 営業秘密保護推進研究会

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
10情報資産の管理 (情報)	情報資産を適切に管理し、機密情報の漏洩を防止する	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	54	1	機密区分に応じた情報の管理ルールを定めている	【規則】・以下の内容等を含む管理ルールを定めること 機密の特定、機密区分のレベル判定と表示、区分に応じた取り扱い方法、取り扱いエリアの区分及び制限 【対象】・情報資産（情報）
			55	2	機密区分に応じた情報の管理ルールを 定期的、または必要に応じて見直ししている	【規則】・管理ルールの内容を確認し、必要に応じて改善すること 【頻度】・1回以上 ／年
			56	1	高い機密区分の情報資産(情報)を一覧化している	【規則】・一覧には、対象情報、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと 【対象情報】・No.54で定めた機密区分のうち、高レベルの機密に該当する情報資産
			57	2	高い機密区分の情報資産(情報)の一覧化を 定期的、または必要に応じて見直ししている	【規則】・一覧表の内容を確認し、必要に応じて是正すること 【頻度】・1回以上 ／年
			58	1	情報資産(情報)は機密区分に応じた管理ルールに沿って管理している	【規則】・No.54に定義した管理ルールの順守状況の点検を行い、不備・違反があれば是正を行うこと 【頻度】・1回/年 以上

他社との間の機密情報の取扱方法の明確化

機密情報を取引先と**共有する前に**、まず**機密情報の定義の認識を合わせた上で**、その取扱いルールに係る**契約等を取り交わすこと**！業務開始後は、取扱実態の**定期モニタリングと必要に応じたルール改善**も不可欠！
これらを前提に、**高い区分の機密情報を共有する取引先をしっかりと絞り込み、格別の厳格な取扱いルールを設定**して、協力してこれを順守することが望ましい。

- 取引先との業務開始前（機密情報を取り交わす前）：
  サプライチェーン対策評価制度も自工会・部工会ガイドラインも、機密情報を共有する取引先との間で、業務開始前に**機密情報の取扱いに関するルール決めと（契約等の）取り交わし**を要求。
  まずは、取引先との間で**機密情報の定義や特定に関する認識に齟齬が生じない**ようにすることが「一丁目一番地」。
  その上で、**機密情報の表示・保管方法・複製可否・第三者提供の可否等の取扱ルール**を取り交わす。
- **高い区分の機密情報を共有する取引先にはより厳格な取扱いを求める必要**があり、それが確実に実践できる取引先を**「少数精鋭」で選定**することが望ましい。**相手を格付けしてルールを変える**ことになるが、これを実効的に運用することは**決して容易ではない**ことに注意！
- 取引先との業務開始後は、取扱実態に課題がないかを**定期的に確認し、必要に応じてルールを改定**することが求められる。
- 取引先との業務終了後は、機密情報を確実に回収又は破棄することが必要。

（参考：達成／評価基準の抜粋）他社との間の機密情報の取扱方法の明確化

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	他社との間で、機密情報の取扱い方法を明確にすること。	★3	・機密情報を共有する取引先等との間で、業務開始前に機密情報の取り扱いについて、例えば以下の内容を含む取り交わしを行うこと - 機密情報の定義 - 機密情報の取扱い（表示、保管方法、複製可否、第三者への提供可否等） - 機密情報の返還

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8他社との 情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	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	44	1	他社との間で、機密情報の取り扱い方法が明確になっている	【規則】・業務開始前に機密情報の取り扱いについての取り交わしを行うこと 【対象】・機密情報を共有する会社
			45	3	他社との間で、機密情報の取り扱い方法に課題が無いか定期的に確認され、必要に応じて、改定していること	【頻度】・1回以上/年

他社から入手した重要機密情報の自社内での取扱実態把握

他社から入手した重要機密情報の取扱いについても、自社の重要機密情報と同じように、**組織全体で同じルール・基準に従って統一的に管理**することが望ましい。これが実現できている企業は必ずしも多くないと見られる。
他社の重要機密情報については、**取扱いを許可された当事者の不適切な行為に加えて、許可なき従業員の不正使用にも目を向ける**必要がある。さらに、「コンタミネーション」防止のため、**自社情報ときちんと分けた保管**が望ましい。

- 自工会・部工会ガイドラインは、**他社から入手した重要機密情報が自社内でどのように取り扱われているか実状を把握**しておくことを求めている。この要求事項については、当事者が個別に管理していたとしても、**組織全体で同じルール・基準に従って統一的に管理できている企業は必ずしも多くない**ものと推察される。

- ガイドラインが提示している達成基準から判断すると、**他社の重要機密の、許可された当事者による、許可された目的の範囲内での使用を確実にする**ことを求めているものと解釈できる。
（参考）提示されている達成基準：他社の重要な機密情報を自社で取り扱った履歴を記録・保管すること。（この履歴が）適切に記録・保管されていることを確認し、必要に応じて是正すること。

- **許可された当事者による不適切な行為**としては、①許可のない者（社内外）への**不正又は不注意な開示**、②**不正又は不注意での目的外使用**、③不適切な管理・持ち出し・送信等による**社外への漏えい**（誤って紛失・送信等を含む）がある。
①と関わってくるが、**社内の許可なき者による不正な使用**も防止する必要がある。

- これとは全く異なる観点として、**「コンタミネーション」**がある。**他社の秘密の管理がずさんで自社の秘密と混ざり合ってしまう**と、**許可のあるなしに関わらず、本人が知らないうちに意図することもなく**、不正・不注意な開示・目的外使用・社外漏えいを起こしてしまう恐れが生じる。「コンタミネーション」を防止するためには、**他社の秘密を自社の情報とはっきり分けて保管**することが望ましいと言える。

（参考：達成／評価基準の抜粋）
他社から入手した重要機密情報の自社内での取扱実態把握

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
該当なし				

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
8他社との 情報セキュリティ要件	サプライチェーンにおける機密情報の漏洩を防止するとともに、事故発生時の対応を迅速に行えるようにする	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	48	3	他社から入手した重要機密情報が、自社内でどのように取り扱われているか実状を把握している	【規則】 ・他社の重要な機密情報を自社で取扱った履歴を記録、保管すること ・適切に記録、保管されていることを確認し、必要に応じて是正すること 【記録、保管状況の確認、是正頻度】 ・1回以上/年

会社毎に取り交わす情報・手段の一覧化

取引先毎に、取り交わす機密情報とその手段を一覧化し、台帳管理すること！その際に当事者がバラバラに管理するのではなく、**組織全体で統一されたルール・基準に基づき一貫した管理運用を行うことが効果的**。管理負担を現実的な範囲とするため、**管理対象とする機密情報の範囲をしっかり選別**し、**取引先と相互に確認**することが必要。

- サプライチェーンセキュリティ対策評価制度も自工会・部工会ガイドラインも、**取引先毎に**、**取り交わす機密情報とその手段**（受発注の手段、情報のやり取り）**を一覧化**することを求めており、この一覧は定期的又は必要に応じて見直すことが必要になる。この要求事項についても、当事者が個別に管理していたとしても、**組織全体で同じルール・基準に従って統一的に管理できている企業は必ずしも多くない**ものと考えられる。
- サプライチェーン対策評価制度が指摘しているように、上記を実現するためには、**重要な機密情報を共有している取引先の一覧を作成することが前提**になる。
- 取引で取り交わす**機密情報の管理負担を現実的な範囲に抑えるためには**、機密情報の定義や範囲について両社で共通認識を持ち、**しっかりと選別することが重要**であり、これを確実にするためには**組織全体で一貫した運用を行うことが効果的**である。他社から機密情報を受け取る窓口を全社で一本化してしまうといった組織的対応も選択肢となる。
- 会社毎の一覧として**台帳化し、記録すべき項目**として、自工会・部工会ガイドラインは以下を指摘している。また、台帳化した内容は齟齬がないように、取引先と**相互に確認することが求められている**。
  - 対象となる取引先
  - 取引で取り交わす重要な機密情報とその取扱
  - 機密情報を取り交わす手段（受発注の手段等、情報の送受方法等）

（参考：達成／評価基準の抜粋）会社毎に取り交わす情報・手段の一覧化

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	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	★3	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先等)が管理・提供し、自組織の資産が接続している情報システムの一覧を作成していること
			★4	・機密情報を共有している取引先の一覧を作成していること ・会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化していること ・一覧表には取引に伴い授受／使用される情報資産とその取扱いを記載し、取引先と把握すること

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
13取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	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	70	1	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している	【規則】・一覧表には取引に伴い授受／使用される情報資産とその取り扱いを記載し、取引先と相互に把握すること 【対象】・重要な情報資産（№54で定められた機密レベルが高い情報資産など）を共有する取引先 【頻度】・取引開始時／取り交わす情報・手段の変更時
			71	3	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)の一覧を 定期的、または必要に応じて、見直ししている	【頻度】・1回/年 以上

機密区分に応じた情報の取扱に関する教育

職場特有のリスクの理解やルールの遵守が必要な項目として、**経営陣を含む全ての要員**（派遣社員等の社外要員を含む）**に対し**、**機密区分の定義及び取扱いを教育**すること！**特に高い区分の機密の特定が重要**であり、かつ課題も多いので、集合教育等も活用してしっかり教育することが望ましい。

- サプライチェーン対策評価制度も自工会・部工会ガイドラインも、**「機密区分に応じた情報の取扱い（機密区分の定義及び取扱い）」を、職場特有のリスクの理解やルールの遵守が必要な項目として位置付けており**、従業員に対する教育の実施を求めている。
  - **経営陣を含む全ての要員**が教育対象
  - **社外要員（派遣社員等）**も教育対象に含まれる
  - **新規受け入れ時、かつ年1回以上**の教育が求められている
- 教育方法としては次を想定：
  ・教育資料配布・掲示　・eラーニング　・集合教育等
- 教育内容や方法を継続的に見直すことが必要。
- すでに述べたとおり、**機密区分の特定（特に高い区分の機密の特定）が重要であり、かつ課題も多い**ので、**実務上のポイントとしては機密区分の特定をしっかりと教育**することが望ましい。**集合教育に積極的に取り組むのも一案**と考える。

  他方で、区分毎の取扱方法については、各社でそれなりに教育が進んでいるものと推察する。

（参考：達成／評価基準の抜粋）機密区分に応じた情報の取扱に関する教育

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
攻撃	意識向上及びトレーニング	経営陣を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること。	★4	・役員、従業員、社外要員(派遣社員等)を対象に、年１回以上の頻度で、セキュリティの重要性を再認識する機会を設けること ・特に職場特有のリスクの理解やルールの遵守が必要な場合、職場単位で重要なルールやリスクについて、年１回以上の頻度でリマインドすること ・以下のトピックについて、新規受け入れ時、かつ、年１回以上、教育資料配布・掲示、ｅラーニング、集合教育等による教育を実施すること - ・・・ - 機密区分の定義と取り扱い ・上記取組みの実施状況を記録し、保管すること

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
7日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報セキュリティ事件・事故を予防する	従業員として注意することを教育していること	30	1	機密区分に応じた情報の取り扱いに関する教育を行っている	【規則】 ・機密区分の定義と取り扱いについて、教育資料配布・掲示、 eラーニング、集合教育等による教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】・役員、従業員、社外要員（派遣社員等） 【頻度】・新規受け入れ時、かつ、１回／年以上

物理的セキュリティの再点検

物理的セキュリティは古くて新しいテーマと言える。**最近、物理的セキュリティの徹底が話題となることが増えている**と感じている。要求事項は「サーバ等の設置エリアの物理的セキュリティ対策」と「持込み・持出し物の制限」であり、**要求内容に特に目新しさはない**が、**確実に実施する必要があるとの認識が改めて高まっている**ものと考えている。

- サプライチェーン対策評価制度も自工会・部工会ガイドラインも、「サーバ等の設置エリアの物理的セキュリティ対策」と「持込み・持出し物の制限」を求めている。
- 評価／達成基準の内容も伝統的なものであり、特筆すべき変化はない。一方で、サプライチェーン対策評価制度も自工会・部工会ガイドラインも物理的セキュリティについてしっかりと書き込んでいる印象。
- 企業側としては、従来の対策等に漏れや課題がないかを再点検する良い機会であると考えている。

（参考：達成／評価基準の抜粋）物理的セキュリティの再点検

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
攻撃等の防御	アイデンティティ管理とアクセス制御	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	★4	・サーバ等の設置するエリアに入場可能な人を定めること。 ・サーバ等の設置エリアを施錠すること。 ・施錠が出来ないエリアにサーバが設置されている場合、サーバを専用ラックに入れて施錠すること。 ・管理者を定めて、施錠管理を行うこと。 ・入退場日時、入場者氏名等を含めて、サーバ等の設置エリアの入退場記録を取得し、少なくとも6 ヶ月間保管すること
		可搬媒体の持込み・持出しを制限すること	★4	・パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器(BYOD)含む)を対象とした社内への持込みルールを定め、文書化すること ・パソコン、スマートデバイス、カメラ、外部記憶媒体(個人所有機器(BYOD)含む)、印刷物(図面等の機密書類)に関する社外への持出しルールを定め、文書化すること

（参考：達成／評価基準の抜粋）物理的セキュリティの再点検

APPTraS 営業秘密保護推進研究会

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
16物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	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	84	1	サーバー等の設置エリアは、入場可能な人を定めている	【規則】・サーバー等の設置するエリアに入場可能な人を定めること
			85	1	サーバー等の設置エリアは、施錠等で入場を制限している	【規則】 ・サーバー等の設置エリアを施錠すること ・施錠が出来ないエリアにサーバーが設置されている場合、サーバーを専用ラックに入れて施錠すること　・管理者を定めて、施錠管理を行うこと
			86	2	サーバー等の設置エリアに入場した記録を保管し、定期的にチェックしている	【規則】・サーバー等の設置エリアの入退場記録を取得し、保管すること 【記録する項目】 ・入退場日時 ・入場者(氏名、所属、連絡先など) ・入場目的 ・承認者 【保管期間】・6ヶ月
		持込み・持出し物の制限を行っていること	91	2	社内への持込みルールを明確にし、運用している	【規則】・社内への持込みルールを定めること ・持込みルールの内容や遵守状況を確認し、必要に応じて是正すること 【対象者】・従業員、派遣社員、受入出向者および社外者 【対象の物品】・パソコン、タブレット、スマートフォン、カメラ、外部記憶媒体 ※上記の他に記録可能な物品があれば各社で判断すること 【持込みルールの内容】・持込み制限の対象とするエリア、物品 ・社内への持込み申請、承認方法 ・持込み記録の保管、管理方法(保管期間:6か月) 【持込みルールの内容や遵守状況の確認、是正頻度】・1回以上/年
			92	2	社外への持出しルールを明確にし、運用している	【規則】・社外への持出しルールを定めること ・持出しルールの内容や遵守状況を確認し、必要に応じて是正すること 【対象】・従業員、派遣社員、受入出向者および社外者 【対象の物品】・パソコン、タブレット、スマートフォン、カメラ、外部記憶媒体、 印刷物(図面などの機密書類) ※上記の他に必要な物品を各社で判断すること 【持出しルールの内容】・社外への持出し申請、承認方法 ・持出し記録の保管、管理方法(保管期間:6か月) 【持出しルールの内容や遵守状況の確認、是正頻度】・1回以上/年

取引先等とのファイル共有／送信時のメール／サービス利用ルールの策定・周知

取引先（関係会社、パートナー企業等）**とのファイル共有・情報送信に関するルールとして**、①**信頼できる相手とのみ共有**すること、②クラウドストレージ、企業向けセキュアファイル転送クラウド等で**社内に送信履歴が残らない手段は禁止**すること、③前記取組みの**実施状況を記録・保管**すること**を定め**、**社内及び取引先に周知**すること！
①については、**取引先の格付けとこれに基づく共有可能な機密区分の策定**も想定される。社外への情報送信のための伝統的な有力ツールである**メールについても、機密情報の漏洩対策や誤送信対策が求められている**。

- サプライチェーン対策評価制度も自工会・部工会ガイドラインも、**取引先（関係会社、パートナー企業等）とのファイル共有・情報送信に関するルールを定め、周知**することを求めている。
  - まず第１ステップとして、社外とファイル共有する場合は**信頼できる相手とのみ共有**することが求められている。
    実務上は、信頼できることを前提として、**機密区分の高さに従って情報を共有できる相手を格付けする**ことも必要になると考えられる。ここまでしっかりできている企業は必ずしも多くないと思われる。
  - 次に第２ステップとして、社外とファイル共有・送信する手段についての要求が提示されている。
    実際によく使われる手段としては、クラウドストレージ、メール添付、企業向けセキュアファイル転送クラウド、取引先専用ポータル、自社開発したセキュアファイル転送システム等がある。このうち、**クラウドストレージ、企業向けセキュアファイル転送クラウド等で、社内に送信履歴が残らない手段は、利用を禁止**することが求められている。
  - さらに、サプライチェーン対策評価制度では、**各ステップの取組みの実施状況を記録し、保管する**ことを求めている。

- 社内に送信履歴が残らない手段が禁じられると、代わりにメールに頼ることも想定される。
  自工会・部工会ガイドラインでは、これを補完する対策として、**機密情報のメール送信に対する情報漏えい対策**と、**社外宛送信メールの誤送信防止対策**の実施も求めている。

（参考：達成／評価基準の抜粋）
取引先等とのファイル共有／送信時のメール／サービス利用ルールの策定・周知

APPTraS 営業秘密保護推進研究会

【サプライチェーン対策評価制度（抜粋）】

大分類	中分類	要求事項（案）	★#	評価基準（案）
攻撃等の防御	データセキュリティ	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	★4	・以下を明文化し、役員、従業員、派遣社員、受入出向者へ周知すること - 社外とファイル共有する場合は、信頼できる相手とのみ共有すること - 送信履歴が残らない方法で、社外へファイル転送することを禁止すること ・上記取組みの実施状況を記録し、記録として保管すること

【自工会・部工会ガイドライン（抜粋）】

ラベル	目的	要求事項	No.	レベル	達成条件	達成基準
21オフィスツール関連	不正アクセスやマルウェア感染のリスクを低減する	情報システム・情報機器のデータ保護を行っていること	131	2	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	【規則】 ・機密情報をメール送信する場合は、情報漏えい対策を実施すること
			132	2	メールの誤送信を防止する対策を実施している	【規則】・メールの誤送信を防止する対策を実施すること 【対象】・社外宛ての送信メール
			135	2	関係会社やパートナー企業とファイル共有する場合の利用ルールを定め、周知している（クラウドサービス利用も含む）	【規則】・下記を明文化し周知すること - 社外とファイル共有する場合は、信頼できる相手とのみ共有すること - 送信履歴が残らない方法で、社外へファイル転送することを禁止すること ※ファイル共有：特定の場所にファイルをアップロードし、特定の相手にファイルのアクセスを許可すること ※ファイル転送：特定の相手にファイルを直接送信すること 【周知対象】・役員、従業員、派遣社員、受入出向者

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