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 調査レポート

1. 制度推進の背景

近年、企業のサプライチェーンを狙ったサイバー攻撃が深刻化し、大企業自体ではなく防御の手薄な取引先（中小企業など）が踏み台にされて機密情報漏えいやシステム停止といった被害に直結するケースが増えています[1] [2]。実際に、委託先の PC がマルウェア感染して第三者から不正アクセスを受けたり、部品サプライヤーがランサムウェア攻撃に遭い全工場の稼働が停止した例も報告されており、自社だけでなく取引先や委託先も含めたセキュリティ対策の強化が急務となっています[3]。IPA（情報処理推進機構）の「情報セキュリティ 10 大脅威 2025（組織向け）」でも「サプライチェーンの弱点を悪用した攻撃」が 2019 年に初登場して以降連続でランクインし、2023 年から 3 年連続で第 2 位に挙げられるなど、サプライチェーンにおけるサイバーリスクの深刻さが裏付けられています[4]。

一方、従来は各発注企業が取引先に独自のセキュリティチェックシート等で対策状況を確認してきましたが、取引先側は取引先ごとに基準や様式の異なる多数の質問票に回答する必要があり、大きな負担となっていました[5]。発注側も回答内容を客観

---

[1] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[2] https://secure-navi.jp/blog/000252

[3] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[4] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[5] https://secure-navi.jp/blog/000252

的に比較しづらく、外部から取引先のセキュリティ水準を評価することが難しいという課題があります[6]。このような状況から、**サプライチェーン全体で統一された評価軸を設けてセキュリティ対策状況を「見える化」し、発注・受注の双方の負担軽減と安全性向上を図る必要性**が高まっていました[7]。

以上を受け、経済産業省と内閣サイバーセキュリティセンター（NISC）は**サプライチェーン全体のリスク低減**を目的として企業のセキュリティ対策状況を可視化・評価する新たな制度の検討を進めました[8]。この「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」（通称：**SCS 評価制度**）により、発注企業が取引先に必要なセキュリティ水準を提示し、受注企業がそれを客観的に証明できる共通基盤を整えることで、サプライチェーン全体のセキュリティレベル底上げを図ることが狙いです[9] [10]。

2. 制度の方向性（概要・評価枠組み）

制度の概要と目的: 本制度は企業間取引において**統一基準で各社のセキュリティ対策状況を評価（格付け）し可視化する仕組み**です[11]。単に企業の優劣を競うものではなく、サプライチェーン上での重要度やリスクに応じて適切な対策が実施されているか確認することを目指す「安全性の保証」制度に位置付けられています[12]。発注企業はこの制度を取引先選定や要求水準提示に活用し、受注企業は自社のセキュリ

---

[6] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[7] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[8] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[9] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[10] https://secure-navi.jp/blog/000252

[11] https://secure-navi.jp/blog/000252

[12] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

ティ水準を客観的に示す証明として活用する想定です[13] [14]。結果として、自社のみならず委託先・調達先も含めた包括的なサイバー防御体制の構築を促進し、サプライチェーン全体の情報漏えいリスクや事業停止リスクを低減することが制度の目的となっています[15] [16]。

評価の枠組み: 評価は★（星）の数で表される **3 段階（★3〜★5）で行われます**[17]。**★1 および★2 については既に IPA が運用する「SECURITY ACTION」制度（一つ星・二つ星の自己宣言制度）に対応づけられており、本制度では★3（3 つ星）以上**が評価対象となります[18] [19]。各段階の位置づけと要求水準の概要は以下の通りです[20]。

上記のように、**★3** は業種・規模を問わず「すべての企業が最低限実施すべき」基本的なセキュリティ対策水準、**★4** は★3 を土台に「標準的に目指すべき」より発展的な対策水準、**★5** は最も高度で各社が**到達目標**とするレベルです[21]。※★1・★2

---

[13] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[14] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[15] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[16] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[17] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[18] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[19] https://secure-navi.jp/blog/000252

[20] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[21] https://secure-navi.jp/blog/000252

は IPA の「SECURITY ACTION」（一つ星＝情報セキュリティ 5 か条の自己宣言、二つ星＝基本方針策定の自己宣言）に相当し、本制度では扱いません[22]。

評価項目と基準: 各企業に要求される具体的なセキュリティ対策項目は、国際標準などを参考に策定されています。米国 NIST の「サイバーセキュリティフレームワーク（CSF）」が基盤となり、その 6 つのカテゴリ（識別・防御・検知・対応・復旧・ガバナンス）に「**取引先管理**（サプライチェーン管理）」を加えた **7 分野**で対策項目が整理されています[23] [24]。例えばガバナンス（経営層の関与や方針策定）、取引先管理（委託先のセキュリティ把握）、識別（資産把握・脆弱性管理）、防御（多要素認証やパッチ適用等）、検知（異常監視）、対応（インシデント対応手順）、復旧（復旧計画）といった領域ごとに要件が定義されています[25]。要求項目数は上表の通り★3 で 83 項目、★4 で 157 項目と非常に網羅的で[26] [27]、★5 については今後さらに高度な対策項目が検討されます[28] [29]。

評価の方法: 評価プロセスや認証方法は段階により異なります。**★3** は**「専門家確認付き自己評価」と位置付けられ、各企業が用意されたチェックリストで自己評価を行った後、情報処理安全確保支援士など資格を持つセキュリティ専門家の確認・**

---

[22] https://secure-navi.jp/blog/000252

[23] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[24] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[25] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[26] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[27] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[28] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[29] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

助言を受け、その署名を添えて登録機関に申請する流れが想定されています[30] [31]。第三者機関による審査は不要ですが、専門家のお墨付きと経営層の宣誓をもって信頼性を担保します（有効期間は 1 年間）[32] [33]。★4 は「第三者評価」が必要で、認定を受けた評価機関による書面審査や現地審査に加え、脆弱性診断などの技術的検証を受けて適合性を確認します[34] [35]。★4 は有効期間 3 年間**で、期間内は年次の自己点検も求められる見込みです[36]。★5 も第三者評価になる予定ですが、要求水準や評価方法の詳細は 2026 年度以降に具体化される計画です[37]。★5 では ISO 27001（ISMS 認証）など既存マネジメントシステムの取り組みに加え、製造業ガイドラインのレベル 3 相当の高度な技術対策まで実装していることを証明する枠組みになると想定されています[38]。

対象範囲: 評価の対象となる企業・業界は特定分野に限られません。**すべてのサプライチェーン関連企業（取引の発注側・受注側を問わず）が基本的に対象です[39]。具体的には、製造業などにおける物品・役務の調達に関わる事業者（ビジネスサプライチェーン）や、クラウドサービスや MSP（マネージドサービスプロバイダ）等の IT サービス提供事業者（IT サービスサプライチェーン）まで幅広く含まれます

---

[30] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[31] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[32] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[33] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[34] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[35] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[36] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[37] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[38] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[39] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[40]。**評価の対象となるシステム範囲は各企業の**情報システム基盤全般（オンプレミス環境およびクラウド環境）**であり、生産工場の制御システム（OT）や製品そのもののセキュリティ機能は対象外と整理されています[41]。したがって、委託先であっても開発・製造設備ではなく主に社内 IT 環境のセキュリティ対策状況について評価を受ける形になります。

既存制度との関係: 本制度は既存の他のセキュリティ認証制度等と**競合ではなく相互補完的**な関係を目指しています[42]。例えば、中小企業向けの自主的取組である IPA の「SECURITY ACTION」（★1・★2 に相当）や、産業界別のガイドライン（自動車業界の「JAMA/JAPIA ガイドライン」等）、それに国際規格の ISMS 認証（ISO 27001）などとは整合性を持たせて設計されています[43] [44]。実際、★3 と★4 の要求項目案は自動車業界ガイドラインの内容とかなり対応しており[45]、同ガイドラインに沿って自己評価を行っている企業が本制度を活用できるよう連携が議論されています。また英国の「Cyber Essentials」等、海外の類似制度との将来的な相互認証の可能性も見据えられています[46]。このように本制度は国内外の既存フレームワークを踏まえて策定されており、**日本全体のサプライチェーンにおけるセキュリ**

---

[40] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[41] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[42] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[43] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[44] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[45] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[46] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

ティ水準の底上げ[47] [48]を狙いつつ、企業のこれまでの取組（ISMS 取得や業界ガイドライン対応）が無駄にならないよう配慮されています。

3. スケジュール（策定・導入のタイムライン）

制度策定から導入までの主なマイルストーン: 経済産業省は 2024 年度より有識者や産業界と検討を進め、2026 年度下期の制度開始を目標としています[49]。以下に主なスケジュールをまとめます。

*（現時点の状況：2026 年 1 月現在、本制度は**パブリックコメント実施中**であり、今後 2025 年度内に最終方針が確定される見込みです[50]。その後、制度運営団体の設立や評価機関の認定など運用開始に向けた準備が進められ、**2026 年度下期（令和 8 年度末頃）*からの*評価制度スタートが予定されています*[51] [52]。）

4. 業界の有力企業の取り組み

制度開始を前に、各業界の主要企業や団体もこの新制度を見据えて準備を進めています。その取り組み事例や動向を代表的なものを中心に紹介します。

- **業界ガイドライン策定と制度連携:** 自動車業界では大手完成車メーカーや部品メーカーが加盟する業界団体（日本自動車工業会（JAMA）・日本自動車部品工業会（JAPIA））がいち早くサプライチェーン全体のサイバーセキュリティガイドラインを共同策定しています。この「自工会・部工会サイバーセ

---

[47] https://secure-navi.jp/blog/000252

[48] https://secure-navi.jp/blog/000252

[49] https://www.ey.com/ja_jp/insights/technology-risk/draft-security-measures-evaluation-system-for-strengthening-the-supply-chain

[50] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[51] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[52] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

キュリティガイドライン」は委託先を含めた対策レベルを 3 段階で示したもので、本制度の評価基準にも反映・整合化されました[53] [54]。具体的にはガイドラインの**「レベル 1」が本制度の★3 要求水準に相当し、「レベル 2」**が★4 に対応しています[55]（★5 はガイドライン「レベル 3」に該当する高度な対策を想定）[56]。このように、**業界主導のセキュリティ標準策定**と国の制度設計が連携して進められており、特に自動車など重要産業の大手企業は制度策定段階から深く関与してサプライチェーン全体の安全基盤構築をリードしています。

- **発注企業（大企業）側の対応:** 大手企業や親会社にあたる発注側企業は、取引先に対するセキュリティ要求水準を統一する本制度の趣旨を踏まえ、**調達基準への組み込み準備**を進めています。制度運用開始後は、「当社は★3 以上を取得している企業としか取引しない」等の方針を打ち出し、取引先選定条件として SCS 評価制度の認証取得を求めることが想定されています[57]。実際、経産省も本制度開始後には発注企業による活用を見込んでおり、**「評価段階（★3〜★5）を満たせない企業は取引機会を失うリスクがある」**とも指摘されています[58] [59]。このため多くの大企業は、自社も率先して認証を取得するとともに、サプライヤーに対して準備を促す計画です。また、取引先に高度な対策を求める場合には、その実施コストを適正に価格転嫁できるようにする動きもあります。公正取引委員会とも連携した政府方針により、発

---

[53] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[54] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[55] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[56] https://www.newton-consulting.co.jp/itilnavi/flash/id=8959

[57] https://secure-navi.jp/blog/000252

[58] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[59] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

注側と受注側がセキュリティ対策費用について協議し、製品・サービスの価格に反映させることが推奨されています[60]。例えば「★4 相当の対策」を求めるなら、そのためのシステム導入費や人件費を契約金額に上乗せする交渉は正当とされ、国もパートナーシップの観点からこれを後押ししています[61] [62]。この指針は大企業と中小企業の力関係から生じるコスト負担の不公平を避け、**サプライチェーン全体でセキュリティ強化に取り組むための協力関係構築**を促すものです。

- **受注企業（中堅・中小企業）側の対応:** サプライチェーンの下流を支える中堅・中小企業にとって、本制度は自社のセキュリティ対策レベルを客観的に示すチャンスである一方、対応すべき項目数が多岐にわたるため「何から手を付ければよいかわからない」「人的・予算的リソースが限られている」といった悩みも聞かれます。そこで現在、各種支援策や情報提供が活発化しています。例えば専門団体やコンサル会社による**セミナーや解説資料の提供**が盛んで、2026 年 1 月には認定資格「CISA」を持つコンサルタントが中小企業向けに★3 対応のポイントを解説する無料ウェビナーが開催されるなど、実務者が第一歩を踏み出すための機会が設けられています。また、独立行政法人情報処理推進機構（IPA）は中小企業のセキュリティ自己宣言制度（SECURITY ACTION）を既に運用しており、★1・★2 の達成を支援しています[63]。本制度の★3 取得においても、まずは IPA の二つ星（情報セキュリティ基本方針の策定）まで取り組み済みであることが望ましく、その上で不足する対策を順次実装していくという段階的アプローチが推奨されています。中小企業にとっては、自社の IT 基盤が★3 基準を満たすかを早めに自己診断し、不足部分については自治体や専門家の助言制度なども活用しながら

---

[60] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[61] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[62] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[63] https://secure-navi.jp/blog/000252

強化を図ることが重要です[64]。実際、**「現時点で自社が★3 と★4 のどちらに近い水準か」を把握する自己チェックを開始する**企業も増えてきています[65]。

- **コンサルティング・支援サービスの活用:** 企業の SCS 評価制度対応を支える**外部サービスも多数登場**しています。例えば大手コンサルティング会社やシステムインテグレータ各社は、制度の動向に即した支援メニューを開発中です。フロンティア・アドバイザリー社は 2026 年 1 月に「SCS 評価制度対応支援サービス」を開始し、受注企業向けには現状セキュリティ対策の棚卸し・ギャップ分析から対策実装、評価取得（自己評価支援・第三者評価模擬審査）まで一貫支援し、発注企業向けにも取引先に求める基準策定やリスク管理プロセスへの組み込みを支援する包括サービスを提供しています[66] [67]。同社は自社でも★4 相当の第三者評価機関となるべく準備中であり[68]、制度開始と同時に評価・認証サービスに対応できる態勢を整えています。このように、専門事業者による**コンサルティングや評価代行のサービス**を活用し、自社では不足するノウハウを補いながら準備を進める企業も多いです。また、委託先管理クラウドなど IT ツールの活用も進んでいます。例えばある企業が提供する「VendorTrustLink」のように、サプライヤーに対するセキュリティチェックシート送付・回収やスコアリングを自動化し、証跡も一元管理できるサービスも登場しています[69]。こうしたツールは、今後本制度に基づく情報提供や証明書管理が必要になる場面で、担当者の負担軽減に寄与すると

---

[64] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[65] https://www.cybersecurity.metro.tokyo.lg.jp/links/706/index.html

[66] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[67] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[68] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[69] https://www.rbbtoday.com/release/prtimes2-today/20260120/1191334.html

期待されています[70]。実際、**サプライチェーン全体でセキュリティ対策状況の確認・説明を求められる機会は今後増える**と見込まれており、企業側でも対応プロセスの効率化ニーズが高まっています[71]。

- **パートナーシップによる取組強化:** 業界横断の連携も進んでおり、産業界と政府が協力してサプライチェーンセキュリティ向上を図る枠組みも整備中です。例えば「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」では業界団体や企業が集まり、情報共有や課題検討を行っています[72]。経済産業省の産業サイバーセキュリティ研究会でも本制度に関するサブワーキンググループが設置され、多様な企業からの意見を制度設計に反映してきました[73]。今後、制度の普及促進に向けた施策（説明会の開催や中小企業支援策）や、評価制度と他の認証制度との相互承認に向けた調整など、官民連携の取り組みが継続して進められる見通しです。大手企業にとっても、サプライチェーン全体の底上げなくして自社の安全は確保できないとの認識が広がっており[74]、取引先とのパートナーシップのもとでセキュリティ強化に取り組む姿勢が鮮明になっています。今後は本制度に基づく認証取得状況が新たな「取引の信用材」として機能し、**セキュリティ対策に優れた企業が競争上も有利になる**環境が整っていくと考えられます[75] [76]。企業はその流れを見据え、攻撃への耐性強化と信用力向上の両面から、自社およびサプライチェーン全体のセキュリティレベル向上に取り組んでいます。

---

[70] https://www.rbbtoday.com/release/prtimes2-today/20260120/1191334.html

[71] https://www.rbbtoday.com/release/prtimes2-today/20260120/1191334.html

[72] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[73] https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

[74] https://secure-navi.jp/blog/000252

[75] https://secure-navi.jp/blog/000252

[76] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

以上、経済産業省が推進中の「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」について、**制度誕生の背景・目的、評価制度の概要と枠組み、導入までのスケジュール、そして業界における主な取り組み状況**を整理しました。サプライチェーン全体の安全確保は企業経営における喫緊の課題であり、本制度はその解決策として 2026 年度からの運用開始に向け具体化が進んでいます。企業側でも制度の趣旨を踏まえた自主的な対応や支援活用が始まっており、**共通の「ものさし」によるサイバーセキュリティ体制強化**が日本産業界に広がりつつあります。[77] [78]

---

[77] https://prtimes.jp/main/html/rd/p/000000012.000121694.html

[78] https://secure-navi.jp/blog/000252