取引先のセキュリティは「自社のリスク」である
サプライチェーン攻撃時代の経営判断


橋中義典


中木聖也

CONTENTS

Ⅰ なぜ取引先のセキュリティ問題が自社の経営課題になるのか
Ⅱ 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とは何か
Ⅲ 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への向き合い方
Ⅳ 制度への対応に向けた実務上の課題
Ⅴ 情報セキュリティ対策の意思決定者に今求められる判断

要 約

1 今日、取引先などを経由して自社の情報システムが狙われる「サプライチェーン攻撃」の脅威が急増している。1社への侵害が連鎖的な事業停止などを招くため、その対策は特定部門の枠を超えた経営リスク管理の最重要課題の一つといえる。

2 この事態を受け、国は発注者（委託元）・受注者（委託先）双方の負担を軽減しつつ、サプライチェーン全体の情報セキュリティ対策水準を可視化し底上げする「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」の具体化を進めている。

3 本制度のうち、2026年度末に運用開始予定の★3・★4という評価段階では、自己評価と第三者評価を経て、認定を受けた後にも年次の更新や自己点検が求められる。対応に向けて情報資産などの組織横断的な把握が共通課題となるが、経営層は、本制度の活用を単なる形式的な認定取得ではなく「事業防衛の投資」と位置づけるべきである。

4 経営層が今すぐ下すべき決断は「制度を見据えた対応方針の明確化」である。加えて、制度開始を待つことなく、重要委託先の把握、ネットワーク棚卸し、バックアップの復旧確認の徹底に直ちに着手することが望ましい。これらを後回しにすることは事業停止リスクの放置にほかならない。

Ⅰ なぜ取引先のセキュリティ問題が自社の経営課題になるのか

1 サプライチェーン攻撃はなぜ「自社だけの問題」ではないのか

今日、業務を遂行するうえで、自社の情報をまったく他社に預けないという企業は極めて少数である。給与計算・人事管理・会計処理・顧客管理といった基幹業務はもちろん、個人情報・健康保険データ・知的財産・取引先との機密契約情報まで、多くの企業が外部のサービスやシステムに委託している。

これは利便性と効率化のための合理的な選択といえる。しかし同時に、自社の情報が他社のセキュリティ対策に依存しているという実態でもある。受注者（委託先）側でセキュリティインシデントが発生した場合、預託していた自社情報の流出や自社業務の停止といったリスクは、発注者（委託元）にとっても決して無視できない問題である。

一方で、受注者の立場で見れば、発注者から預かった重要情報を保護する責任を負っている。自社のセキュリティ対策が不十分であれば、それが原因で発注者に損害を与える可能性がある。受注者側の企業の経営者は、自社がサイバー攻撃の被害者となるリスクだけでなく、サプライチェーンにおけるインシデントの媒介者となり、取引先に損害を波及させるリスク（供給責任や損害賠償責任）を負い得ることを認識しておく必要がある。

サイバー攻撃の脅威は、もはや情報システム部門が管理する技術的な問題にとどまらない。自社の不備がグループ全体、あるいは取引先すべての事業を停止させる経営リスクとして認識すべき根拠がここにある。

2 サプライチェーン攻撃のメカニズムと実事例

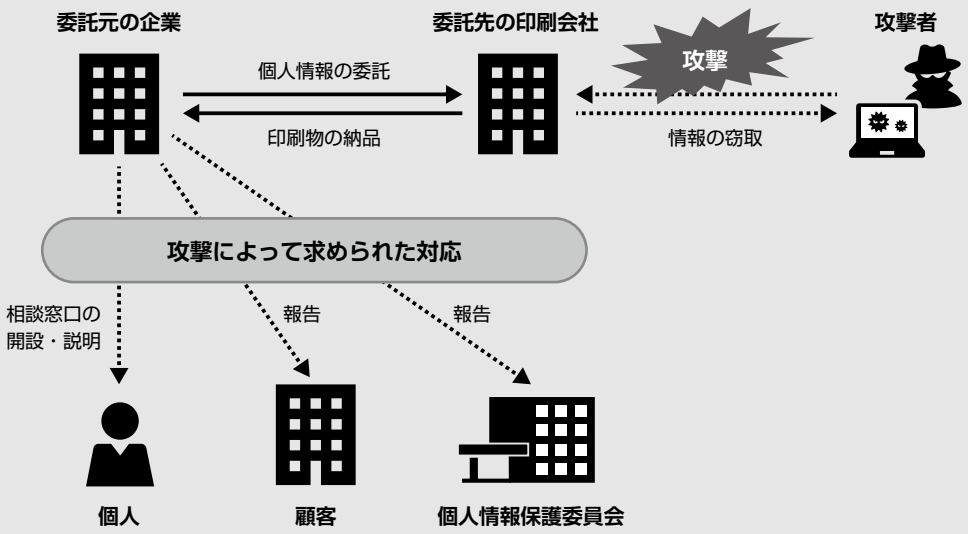
サプライチェーン攻撃では、攻撃者は標的企業ではなく、業務上つながりのある関連企業（委託先、グループ会社など）をはじめに侵害し、そこを経由して標的企業を攻撃する。セキュリティレベルが高い大企業を直接侵害するのは攻撃者にとって困難である。しかし、セキュリティ対策が行き届いていない関連企業を侵害し踏み台とすることで、ネットワークの接続点や標的企業から提供されているアカウントなどを悪用できる。

この構図で最も重要な点は、自社がサイバー攻撃の被害者となるだけでなく、サプライチェーンを通じて他社へ損害を及ぼす媒介者になり得るということである。自社システムの脆弱性を突かれ、預かっていた発注者の顧客情報が流出すれば、発注者のビジネスに重大な損害を与え、ひいては自社の供給責任や賠償責任を問われる当事者となってしまう。

2024年に発生した大手印刷会社へのランサムウエア攻撃は、発注者である各企業に深刻な影響を及ぼした。発注者の企業自体のシステムが堅牢であっても、本件は防げなかった。情報の委託先である印刷会社への不正アクセスが起因していたためである。結果として、図１の下部にあるように、発注者の各企業はそれぞれの顧客などへ情報漏洩にかかる報告や窓口開設などの対応、個人情報保護委員会への報告といった対応に加えて、社会的信用の毀損という連鎖的なダメージを受けることとなった。

また、2025年に発生した大手飲料メーカー

図1　委託先の印刷会社への攻撃によって委託元の企業が求められた対応



や大手流通企業へのランサムウエア攻撃では、顧客の情報漏洩だけでなく、生産／サービス停止といった企業経営への影響、および物流への影響により、取引先や共同配送していた競合他社にまで多大なダメージを及ぼしている。

自社がどれほど堅牢なセキュリティ体制を整えても、サプライチェーン上の１社の脆弱性が自社を危機にさらす恐れがある。これは、自社単独の対策では決して解決できず、サプライチェーン全体で取り組むべき構造的な課題なのである。

加えて、生成AIを悪用した攻撃者による、フィッシングや認証情報の窃取、侵入後の横展開といった手口の高速化・高度化についても、警察庁の報告で言及されている[注1]。サプライチェーン上の１社を起点とした侵害が、より短時間・より広範囲に連鎖するリスクは、今後、さらに高まると見込まれている。

3　発注者から要求されるセキュリティ評価の問題と新制度検討の背景

こうしたリスクへの対応として、発注者が受注者にセキュリティ対策状況の確認を求めるケースが増加している。NRIセキュアテクノロジーズの調査（「NRI Secure Insight 2025」）によると、発注者からのセキュリティ評価に何らかの問題を感じている企業は75.4％に上る。その多くが「発注者ごとに質問内容や書式が異なる」「設問数が多く回答に時間がかかる」「示されるガイドラインやルールが分かりにくい」といった、セキュリティ評価の対応コストの高さに起因する問題を挙げている。

発注者の側からすれば、独自の質問票を作成・送付・回収・評価するプロセスは、専門知識なしには評価の精度も担保できず、取引先への負担も大きい。受注者の側からすれば、内容も書式も異なる質問票への回答対応

が積み重なり、実務部門を疲弊させている。

Ⅱ 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とは何か

1 制度が生まれた経緯

前章では、発注者は受注者の情報セキュリティ対策の状況を確認することが難しく、受注者は多数ある発注者に対してそれぞれのフォーマットで情報セキュリティ対策の状況を開示する負担が大きいという二重の問題があることを述べた。

これを解消するために、経済産業省および内閣官房国家サイバー統括室が検討を進めているのが、「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（SCS評価制度）」である。2026年３月に制度構築方針が公表されている。

本制度は、業種横断的な共通基準で自社の対策状況を評価し、取得した★マーク（★３・★４・★５）によってセキュリティ対策水準を客観的に示す仕組みである。評価結果は情報処理推進機構（IPA）で公開され、取引先からも確認可能となる。将来的な国際連携も視野に入れつつ、中小企業を含むサプライチェーン全体の対策の可視化と底上げを目的としている。

制度設計に当たっては、海外の類似制度が参照されている。米国のCMMC（Cybersecurity Maturity Model Certification）や英国のCyber Essentials（サイバーエッセンシャルズ）など、調達条件として活用されている海外制度の設計思想・構造を参考にしながら、日本のサプライチェーンの実態に合わせて設計されている[注2]。

なお、本制度は、何らかの規制を課さない任意の制度として検討が始められた。したがって、★取得は、２社間の取引契約などにおいて参照されることを想定して検討されている。

2 制度の全体像と位置づけ

経済産業省が公開している制度構築方針の内容を取りまとめると、SCS評価制度の狙いは、サプライチェーン全体で通用する共通の評価基準を提供し、取引先のセキュリティ対策状況を客観的・効率的に確認できる仕組みをつくることにある。発注者が独自に作成した質問票ではなく、経済産業省が設計した共通基準に基づく★マークがあれば、この水準の対策が専門家または第三者によって確認されているという事実を、業界・企業規模を問わず共通の言語として使えるようになる。いわば、サプライチェーンセキュリティの共通の評価言語をつくろうという試みである。

本制度は、これまで中小企業を中心に普及してきたIPAの「SECURITY ACTION（★１・★２）」と接続する形で設計されている。こちらは自らの取り組みを自己宣言する制度であるのに対し、SCS評価制度では「専門家確認付き自己評価」もしくは「第三者評価」が必要となっており、評価に客観性を持たせる点が本質的な違いとなっている。

経済産業省が主体となってつくられている制度ではあるが、業界・業種・企業規模を問わず、サプライチェーンを構成するすべての企業で本制度の認証取得が可能である。

本制度では、評価段階を★３・★４・★５の３段階で区分している（★５については

表1　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評価段階（★3 ～★5）の概要

評価軸	SECURITY ACTION		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（SCS評価制度）		
	★1	★2	★3	★4	★5
想定されている脅威	—		広く認知された脆弱性を悪用する**一般的なサイバー攻撃**	機密情報など、情報漏洩により**大きな影響をもたらす資産への攻撃**	未知の攻撃も含めた**高度なサイバー攻撃**
要求項目数	6カ条	25項目	**26項目、81評価基準**	**43項目、153評価基準**	検討中
評価方法	自己評価		**専門家確認付き自己評価**または**第三者評価**	**第三者評価**	**第三者評価**
有効期間	なし		**1年**（毎年更新）	**3年**（年次の自己評価が必要）	検討中
運用開始時期	2017年		**2027年3月予定**	**2027年3月予定**	**未定（2026年度以降）**

出所）経済産業省、国家サイバー統括室「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関する制度構築方針」（2026/3）より作成
https://www.meti.go.jp/files/900017305.pdf

2026年度以降に詳細を検討）。詳細については、制度構築方針[注3]を基に筆者らが情報の追記などをして、表1にまとめている。

★3は、全サプライチェーン企業が最低限実装すべき基礎的な対策を対象としている。本稿執筆時点では26の要求事項（評価基準81項目）について取得希望組織が自己評価し、認定セキュリティ専門家が内容を確認・署名する「専門家確認付き自己評価」方式を採る。この確認には外部専門家への依頼が必要であり、費用が生じる。費用水準は現時点では未公表だが、★4の第三者評価機関と併せて今後示される見通しである。★3の有効期限は1年間であり、定期的な再評価（セキュリティ専門家による確認・助言を経た自己評価の提出）が求められる。

★4は、初期侵入の防御にとどまらず、内部への被害拡大防止・データ保護・委託先管理まで求められる水準である。評価基準153項目について評価機関による第三者評価が必要となる（評価機関は2027年3月の公表が予定されている）。★4の有効期限は3年だが、有効期間内も1年ごとに自己評価を実施して評価機関に提出する必要があり、3年に1回の更新時にはあらためて第三者評価を受ける仕組みになっている。

SCS評価制度の評価内容は、SECURITY ACTIONが「自社でセキュリティ対策に取り組んでいる」という自己宣言にとどまるのとは異なり、取引先のセキュリティ対策状況の把握や、アカウントやネットワーク接続状況の管理・バックアップ取得状況や復旧手順書の確認など、具体的な技術的対策の実施状況を審査するものである。自社で作成したチ

ェックリストを取引先に配付・回収・評価するという従来の方法では、評価の正確性・一貫性・負担の面で限界があった。本制度に基づく★マークであれば、この水準のセキュリティ対策が専門家または第三者によって確認されている根拠として活用できるようになり、評価の正確性・一貫性が担保された評価にスケールメリットがはたらく。

また、SECURITY ACTIONとは異なり、SCS評価制度では継続的な対策の維持・改善が求められる。評価の信頼性の維持が期待される一方で、経営者として中長期的な投資対象として認識しておく必要がある。

Ⅲ 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への向き合い方

第Ⅰ章で述べたように、サプライチェーンを構成する組織の情報セキュリティ対策状況は、無視することができない情勢である。では、前章で解説したSCS評価制度について、企業はどう向き合えばよいのだろうか。本章では、制度に取り組まなかった場合のリスクシナリオとその影響から、求められる対応を論じる。

1 発注者目線でのリスクシナリオ

(1) シナリオ

製造業Ａ社は、長年の取引実績を根拠にＢ社へのセキュリティ対策状況の確認を省略していた。Ｂ社でランサムウエア感染が発生し、Ａ社の設計データが流出したことを踏まえ、Ａ社の株主総会で経営陣が委託先管理の不備を追及された。

(2) 影響

このような事態が発生した場合、Ａ社が被る影響のうち代表的なものを３点挙げる。

まず、信頼毀損である。顧客・株主・取引先からの信頼低下は、ブランド価値や株価に直結し得る。次に法的・費用的負担である。被害を受けた関係者への損害賠償や、事後対応に要する調査・復旧コストは、インシデント規模によっては経営を直撃する水準になり得る。そして、管理体制の再構築コストである。委託先管理の不備が露呈した後は、全取引先を対象とした評価プロセスの整備を迫られ、相当の時間と人員を要する。

(3) 求められる対応

受注者のセキュリティ対策状況を確認しないまま取引を継続することは、こうしたリスクを温存することに等しい。本制度が普及すれば、「★３以上の取得を確認する」という形で委託先評価を効率化しながら、管理責任の観点でも合理的な根拠を持てるようになる。

費用負担については、経済産業省・公正取引委員会の想定事例[注4]が参考になる。同文書では、発注者が受注者に対してセキュリティ対策を要請する際に、独占禁止法・下請法との関係で「問題とならない」ケースが示されており、両者がパートナーシップを構築しながら費用負担や価格交渉を協議していく考え方が示されている。その第一歩として、現状の受注者のセキュリティ対策状況を整理し、業務内容や取り扱う情報といった観点から、★マークの取得依頼に向けた計画の立案に着手することが望ましい。

2　受注者目線でのリスクシナリオ

（1）シナリオ

中堅SIのＣ社は複数の大手取引先から異なる形式の質問票を受け取り、対応のたびに情報システム・法務・経理の各部門を動員する状況が続いた。大手Ｄ社が取引先選定で★マークの取得状況を参照するようになったことで、未取得のＣ社は新規案件の引き合いが減少し始めた。

（2）影響

対応コストの増大と機会損失が同時に進行する点が、受注者にとっての本質的なリスクである。質問票対応に要する工数は、複数部門を横断するため見えにくいが、年間で換算すると相当数の工数に上るケースも少なくない。加えて、大手発注者が★マーク取得を取引条件の参考とするようになれば、未取得企業は見積もりや応札段階での比較劣位に置かれるリスクがある。質問票への対応負荷がかかりつつも競争上の優位も得られないという二重の損失構造に陥る可能性がある。

（3）求められる対応

個別対応を有識者による評価や確認による他組織にも共有できる証明という対応に置き換え、工数を集約できる可能性がある。なお、SCS評価制度は★マーク取得を取引先に強制するような制度ではなく、「未取得＝取引停止」という運用は想定されていない。「評価を取得していないと商取引が規制される」といった過度な表現による勧誘には経済産業省らが注意喚起を出しており[注5]、冷静な判断が求められる。

Ⅳ 制度への対応に向けた実務上の課題

本章では、著者らが所属するNRIセキュアテクノロジーズの支援実績や、同社のセキュリティ評価サービス「Secure SketCH」を利用する約1300社のデータを基に、SCS評価制度の★マーク取得に向けた分析を行った。その結果、見えてきた実務上の課題を、「組織規模別の課題（大規模・小規模組織の傾向）」と、規模によらず共通する、「AIの悪用への対策」という２つの側面から整理した。

1　組織規模別の課題

（1）大規模組織における課題

IT専門部隊を持つ大規模な組織であれば、SCS評価制度への対応も比較的スムーズに進むように思われるかもしれない。しかし実際には、情報システム部門に限らず、経営・リスク管理・購買など複数部門にまたがる活動が必要になり、むしろ対策に長期間を要することが考えられる。その根本的な理由は、情報システム部門が把握していない情報資産が、組織内に多数存在する点にある。

たとえば、経理部門が利用しているクラウド会計サービスのアカウント管理、知的財産部門が保管している設計データの取り扱いルール、人事部門が契約している外部の採用管理システムのセキュリティ設定といったものは、情報システム部門が一元的に把握しているとは限らない。本制度の★４では、組織全体の情報資産の棚卸し・機密区分の設定・取引先への預託情報の管理まで求められることから、IT部門が単独で対応することは構造的に難しい。

もう一つの難所が、外部ネットワークとの接続点の洗い出しである。本制度の適用範囲には、インターネット公開サーバやエンドポイント機器（PCやスマートフォンなどの末端端末）に加え、クラウドサービスや親会社のグループ共通ネットワーク、VPN装置など、他社との間でセキュリティ上の責任を共有する領域も含まれる。これらは「責任共有モデル（クラウド事業者と利用企業が、それぞれどこまでセキュリティ責任を負うかという境界線）」の下で管理される。自社側の対策実装、またはサービス提供者の対策状況の確認が求められる。

しかし、そもそも「自社の外部接続点がどこか」を網羅的に把握できていない組織は少なくない。情報資産の棚卸しと並行して、外部接続点の一覧化も制度対応の前提作業として位置づける必要がある。

図2は、NRIセキュアテクノロジーズの支援実績およびSecure SketCHの回答データに基づき、SCS評価制度の★マーク取得の要求事項[注6]に対して企業がクリアすべき課題（準拠率が低く、対策が急務となる項目）と、そのボトルネックを抽出し、要求事項を要約するなど加工したものである。

「準拠率が低い要求事項」に多く見られた要素は、ログ管理やインシデント対応であった。全体を俯瞰すると、課題は「専門スキル

図2　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★マーク取得における課題

大分類	準拠率が低い要求事項（筆者らが抽出･加工）	取り組むべき課題
ガバナンスの整備	攻撃予兆・インシデント検知／対応に向けた情報活用やログ相関分析の体制構築を要求	定期的な情報収集・分析体制の確立とインシデント発生時の対応マニュアルなどの整備と人員確保
取引先管理	取引先への預託情報取り扱い、インシデント報告義務、責任分界の明確化を要求	既存契約改訂に向けた法務・取引先との円滑な調整プロセスの構築
	重要度、事業継続性、システム連携有無に基づき、管理対象の取引先の年次評価を要求	評価対象選定スキルの確保と年次評価の負荷軽減、および関連部門・取引先との連携体制の構築
リスクの特定	外部情報システム（クラウド含む）利用時、セキュリティ要件定義とサービス内容の確認を要求	要件設計スキルの確保と都度の利用申請・承認判断プロセスの効率化
攻撃などの防御	役職員へセキュリティインシデント対応教育・訓練を新規受け入れ時と年次で要求	体制・手順および教育・訓練設計スキルの確保と年次実施の運用負荷軽減
	情報機器・システムログの取得と6カ月の保管のほか認証ログの月次点検も要求	ログ要件不適合時の別環境移行・システム化対応と、認証ログ月次点検の運用負荷軽減
攻撃などの検知	ログの統合･単独確認、異常検知、即時アラート・速報、インシデント判断を要求	統合ログ管理や対応自動化機能などの活用によるアラート対応の自動化・効率化



出所）経済産業省「別添★3・★4要求事項及び評価基準」とNRIセキュアテクノロジーズの知見などを基に作成
https://www.meti.go.jp/files/900017306.xlsx

の確保」「運用負荷の軽減」「技術・機能的制約の克服」「円滑な組織間連携の構築」の４つに集約できる。

中でも課題となりやすいのは「取引先管理（契約改訂や年次評価など）」と「攻撃などの防御（ログ取得や教育訓練など）」である。これらは上記４つの課題が複合的に絡み合う領域であり、現場レベルでの対策推進が特に困難となっている。

これらの課題を克服し、制度への確実な対応を進めるには、IT部門のみならず、リスク管理、購買、法務、各事業部門を巻き込んだ全社横断的な体制の構築が不可欠である。この体制構築とリソース配分には、経営層による明確なコミットメントと意思決定が必要となる。

（2） 小規模組織の課題

中小企業を中心に、専任のセキュリティ担当者がいない組織では、課題の性質が異なる。

★３の取得に際しては「認定セキュリティ専門家による確認・署名」が必要であり、社内の情報システムに詳しい担当者がいれば対応できるものではない。情報処理安全確保支援士などの国家資格保有者や、国際的なセキュリティ専門資格（CISSP・CISMなど）を持つスペシャリストのうち、SCS評価制度の所定の研修を受講した者がセキュリティ専門家として認定される予定であり、該当者の確保が課題となる。

経済産業省は、こうした中小企業向けの支援策として、IPAが整備予定の「中小企業向けサイバーセキュリティ対策支援者リスト」や「サイバーセキュリティお助け隊サービス（新類型）」の活用を想定している。後者は★３・★４の取得支援（セキュリティポリシー策定など）を目的としたサービスであり、国が要件を認定する仕組みも整備される予定である。

専任者がいない組織では、何から手をつければよいかの判断自体が難しいという声も多い。その場合には、第Ⅴ章３節に記載する基本的な確認から始めることが推奨される。

2 組織によらず共通する課題：AIの悪用への対策

本稿で論じてきたサプライチェーンリスクに対し、さらに拍車をかける要因が攻撃者によるAIの悪用である。

AIの悪用が現実的な脅威となった今、基礎的なセキュリティ対策が未成熟な組織への侵害リスクは従来よりもはるかに増大している。これにより、当該組織とネットワーク接続や情報預託といったサプライチェーン上のつながりがある組織への侵害は、より短時間かつ広範囲に連鎖することが見込まれる。

こうした異常を検知し、リスクを可視化するには、前述のログ取得などの対策強化に加え、ネットワーク構成図の作成や機密情報預託先の棚卸しなど、基礎的な情報資産管理の徹底が欠かせない。さらに重要となるのが、サイバー攻撃を前提とした復旧計画の文書化である。具体的には、「どのシステムを、いつまでに、どの状態まで復旧させるか」を明確にしておく必要がある。AIの悪用によって脆弱性の特定が容易になっている今、サービスの中断までを想定した抜本的な備えが必要不可欠である。

こうした課題に光を当て、セキュリティ対

策の水準を測る物差しとなるのが、SCS評価制度の要求事項である。機微情報を他社に委託する組織ほど、本制度を活用した委託先管理を行うことで得られる効果が大きいと考えられる。

機微情報の定義や預託先の管理などのルールを見直す契機となることや、ISMSやプライバシーマークなどほかの認証規格とは異なり、脆弱性への対応状況を技術的に検証する要求事項が含まれていることがその理由の一つである。

なお、AIを活用した攻撃手法は今後も進化し続けることが見込まれる。それ故、特定の技術や製品に依存した対策ではなく、継続的な評価と見直しの仕組みを持つことが、サプライチェーン全体での対策水準の底上げにつながる。

V 情報セキュリティ対策の意思決定者に今求められる判断

前章で明らかになった実務上の課題を乗り越え、SCS評価制度を有効に活用するためには、経営層や意思決定者による早期の判断が不可欠である。本章では、制度開始に向けて今すぐ検討すべき事項を、「発注者」「受注者」「両者に共通する事項」という3つの立場に分けて解説する。

1 発注者として今決めるべきこと

発注者としての経営判断の核心は、「どのような情報資産の取り扱いをどのような相手に委託する際に、どのレベルのセキュリティ対策を求めるか」という方針を定めることである。

この方針を決めるには、まず自社がどの取引先にどのような情報資産を取り扱える状態にしているかの棚卸しが前提となる。しかしこの棚卸し自体が、情報資産をデータや文書に限った場合だけでも、情報の量・機密度・業務上の重要性などの観点から対象を絞り込む必要があり、それだけで相当の作業を要する。取引先の数が多い企業にとって、そのすべてを対象とすることは現実的ではなく、預けている情報の機密度・事業継続上の重要度・システム連携の有無などを基準にした優先順位づけが必要となる。

そのうえで検討すべきことは、主要な取引先に対して本制度の★マーク取得を求めるのか、あるいは独自の質問票による確認を継続するのかという方針の選択である。本制度が普及した段階では、★マーク取得を確認基準として活用することで評価の標準化と双方の負担軽減が期待できる。一方、本制度はまだ運用開始前であり（2026年度末頃の開始予定）、当面は独自の質問票による確認と本制度の併用も現実的な選択肢である。

いずれの方針であっても、サプライチェーンセキュリティをどの水準で保つかの基準とスケジュールを経営レベルで定め、それを取引先管理の方針として組織内に明示することが、今まさに求められている判断である。

2 受注者として今決めるべきこと

受注者としての経営判断の核心は、「SCS評価制度への対応をいつ・どのように進めるか」のスケジュールと優先順位を決めることである。

引き続き個別の質問票への対応を継続するのか、どのタイミングで★マーク取得による

回答の代替として交渉することを目指すのか。この判断を先送りにすると、発注者から求められた際に慌てて対応を検討することになる。これにより、見積もりや応札段階での比較劣位に置かれるリスクが長期化する恐れがある。特に★4は第三者評価機関による審査が必要であり、評価機関の指定・公表が2026年12月頃の予定であることを踏まえると、今から社内の体制整備と要求事項の事前確認を進めておくことが現実的である。

大規模な組織であるほど、どの部署を巻き込む必要があるかの事前調査が重要となる。★4の要求事項には法務・経理・人事・各事業部門にまたがる対応が含まれており、情報システム部門だけでは対応できない。どの部署が何を担うかの役割分担を、準備段階で整理しておく必要がある。

3　立場を問わず、今決めること

第Ⅳ章で示した4つの重点課題のうち、専門スキルや組織間調整を要するものは段階的な対応が必要だが、発注者・受注者いずれの立場であっても、今すぐ着手できる基礎的な確認事項がある。それは、「重要な受注者（委託先）のセキュリティ対策状況の把握」「アカウントやネットワーク接続状況の棚卸し」「バックアップの取得状況とリストア手順の確認」である。

これらはSCS評価制度の★3・★4要求事項および評価基準の中核を成す項目であるが、制度対応とは切り離しても、セキュリティインシデントが発生した際の初動対応や復旧対応など、いずれも事業継続に直結する情報である。「制度のために整備する」という動機よりも、「インシデントに備えた経営の基本として整備する」「インシデントが発生するという前提」という観点での着手が組織内の理解を得やすく、持続的な取り組みにもつながる可能性が高いと考えられる。

情報セキュリティ対策の意思決定者には、これらの基礎的な確認作業の結果を基に、本制度への対応を中期経営計画に組み込むかどうか、いつをめどに★マーク取得や本制度の要求事項を参考にしたサプライチェーンセキュリティの対策を実施するかの判断が求められる。

取引先のセキュリティを「自社のリスク」として捉え、サプライチェーン全体の強靭化を目指すこの新たな挑戦において、本稿が意思決定者の方々の確かな一歩を後押しする一助となれば幸いである。

注

1　警察庁サイバー警察局「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2025/9）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7kami/R07_kami_cyber_jyosei.pdf

2　経済産業省・情報処理推進機構セキュリティセンター「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構築について」（2024/7/12）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/pdf/001_05_00.pdf

3　経済産業省・国家サイバー統括室「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関する制度構築方針」（2026/3）
https://www.meti.go.jp/files/900017305.pdf

4　経済産業省・公正取引委員会「サプライチェー

ン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」（2025/12/26）
https://www.meti.go.jp/policy/netsecurity/partnership2.html

5 経済産業省・内閣官房「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（SCS評価制度）に関する注意喚起」（2026/4/27）
https://www.meti.go.jp/policy/netsecurity/20260427_scs.html

6 ★3・★4要求事項・評価基準
https://www.meti.go.jp/files/900017306.xlsx

著者

橋中義典（はしなかよしのり）
NRIセキュアテクノロジーズ アーキテクチャコンサルティング事業本部 サイバーレジリエンスコンサルティング部 シニアセキュリティコンサルタント
専門はサプライチェーンセキュリティ、ネットワーク運用管理

中木聖也（なかきせいや）
NRIセキュアテクノロジーズ アーキテクチャコンサルティング事業本部 サイバーレジリエンスコンサルティング部 シニアセキュリティコンサルタント
専門は国内外のグループ会社やサプライチェーン全体のリスクアセスメント