

サプライチェーン攻撃とは？企業がSCS評価制度への対応を求められる背景

サプライチェーン攻撃とは、攻撃者が標的企業を直接狙うのではなく、取引先、委託先、ソフトウェア、クラウドサービスなど、事業を支える「つながり」の中にある比較的弱い箇所を足掛かりに侵入・妨害する攻撃です。自社のセキュリティ対策が一定水準に達していても、取引先側の認証情報、VPN機器、開発環境、更新プログラムなどを経由して影響を受ける可能性があります。

この問題を背景に整備が進められているのが、「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）」です。SCS評価制度は、企業が実施しているセキュリティ対策を共通の基準で可視化し、取引先間で確認しやすくすることを目的としています。★3・★4は2027年3月頃の運用開始が予定されています。

経営者や管理部門が押さえるべき結論は明確です。サプライチェーン攻撃への対応は、情報システム部門だけの技術課題ではなく、取引継続、事業継続、信用、調達・委託管理に関わる経営課題です。SCS評価制度への対応も、申請直前に資料を整える作業ではなく、取引先から求められても説明できる状態を平時からつくる取り組みとして捉える必要があります。

この記事で分かること

- サプライチェーン攻撃の意味と、なぜ取引先・委託先が狙われるのか
- サプライチェーン攻撃が経営・事業継続・取引関係に与える影響
- SCS評価制度が作られた背景と★3・★4の位置づけ
- 従業員100～1,000名規模の企業が準備しておくべき実務事項
- 脆弱性診断やペネトレーションテストをどこで活用すべきか
- SCS評価制度対応を外部支援会社へ相談する際の確認ポイント

サプライチェーン攻撃とは

サプライチェーンとは、製品・サービスが顧客へ届くまでに関係する企業、システム、物流、委託先、外部サービスなどの連鎖を指します。IT分野では、システム開発会社、運用保守会社、クラウドサービス、SaaS、ソフトウェアライブラリ、更新サーバー、認証基盤なども含まれます。

IPAは「情報セキュリティ10大脅威 2026」で、「サプライチェーンや委託先を狙った攻撃」を組織向け脅威の第2位に挙げています。サプライチェーンの中でセキュリティ対策が相対的に弱い箇所を攻撃の足掛かりにし、間接的・段階的に本来の標的組織へ侵入することが代表的な構図です。

代表的な4つの攻撃パターン

実務上は、サプライチェーン攻撃を「どの経路が悪用されるか」で整理すると対策を考えやすくなります。代表的には次の4パターンがあります。

攻撃経路	具体例	企業側で確認したい点
取引先・委託先経由	委託先のVPNやリモート接続用アカウントが侵害され、接続先の自社ネットワークへ侵入される	外部接続方式、権限、MFA、委託終了時のID削除、ログ確認
ソフトウェア経由	正規の更新プログラムやライブラリに不正コードが混入し、利用企業へ広がる	SBOM、更新元確認、署名検証、依存関係管理、脆弱性情報の収集
クラウド・SaaS経由	外部サービスのアカウント侵害や設定不備から機密情報へアクセスされる	SSO/MFA、管理者権限、監査ログ、委託先の責任分界、データ保管場所
業務停止の波及	部品・物流・決済・認証などの重要委託先が止まり、自社サービスも停止する	代替手段、BCP、復旧優先順位、連絡網、重要委託先の選定基準

取引先の障害が自社の事業停止につながる

サプライチェーンリスクの特徴は、侵害を受けた企業と実際に大きな事業影響を受ける企業が一致しない場合があります。2022年3月には、トヨタ自動車国内仕入先のシステム障害の影響を受け、国内14工場28ラインの稼働を一時停止しました。トヨタ自動車の公式発表では、翌日に全工場の稼働を再開しています。これは、重要な取引先のIT障害が自社の生産継続に直接波及し得ることを示す事例です。

出典:トヨタ自動車「3/2(水)以降の国内工場における稼働再開について」

<https://global.toyota/jp/newsroom/corporate/36964714.html>

なお、個別事案の原因や攻撃手法は公式発表で確認できる範囲に限って扱う必要があります。一方で、経営上の教訓は普遍的です。重要な業務を支える仕入先・委託先が停止したとき、自社がどこまで事業を継続できるかを把握しておく必要があります。

なぜ今、SCS評価制度への対応が求められているのか

従来、取引先のセキュリティ確認では、発注企業が独自のチェックシートを配布し、委託先が回答する方法が広く使われてきました。しかし、発注側には「回答だけで実態を判断しにくい」、委託側には「取引先ごとに異なる質問へ対応しなければならない」という問題があります。

SCS評価制度は、こうした双方の負担と判断のばらつきを減らし、一定の共通基準で対策状況を可視化するための制度です。IPAは、2社間の取引契約等において、委託元が委託先へ適切な段階(★)を示し、対策を促すとともに実施状況を確認する利用方法を想定しています。

出典:IPA「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)」

<https://www.ipa.go.jp/security/scs/index.html>

SCS評価制度の★3・★4の違い

2026年10月時点で公表されている制度では、★3は一般的なサイバー脅威に対処し得る水準として、基礎的な組織的対策とシステム防御策を中心に求める位置づけです。評価方式は「セキュリティ専門家による確認を経た自己評価」です。

一方、★4は、供給停止や機密情報漏えいなどサプライチェーンへの影響が大きい企業・資産も想定し、組織ガバナンス、取引先管理、防御・検知、インシデント対応などをより包括的に確認します。評価機関による第三者評価に加え、技術検証も行われます。★3を先に取得していなければ★4を申請できないという制度ではありません。

出典:IPA「SCS評価制度の詳細情報」<https://www.ipa.go.jp/security/scs/details.html>

出典:経済産業省「SCS評価制度」<https://www.meti.go.jp/policy/netsecurity/scs.html>

サプライチェーン攻撃の増加が「取引条件の共通化」を促している

発注企業から見ると、重要データやネットワークへアクセスする委託先が十分な対策をしているかは、自社のリスク管理そのものです。そのため、取引開始時のセキュリティ審査、契約条項、定期監査、インシデント報告義務などが強化される傾向にあります。

経済産業省と公正取引委員会は、取引先にSCS評価制度に基づく対策を要請する場面を想定した事例を整理し、セキュリティ対策に伴うコストについて発注側と取引先が協議する考え方も示しています。つまり、SCS評価制度は単なるIT部門のチェック項目ではなく、調達・契約・価格交渉とも接続する制度として位置づけられています。

出典:経済産業省「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」

<https://www.meti.go.jp/policy/netsecurity/partnership2.html>

SCS評価制度への準備をしない場合に起こり得る問題

SCS評価制度は、2026年10月時点で全企業に一律に取得義務を課す制度ではありません。ただし、制度の活用が取引契約の中で想定されている以上、取引先から特定水準への対応を求められる場面は考えておくべきです。

取引開始・更新時の説明に時間がかかる

「対策しています」と回答するだけでは、現在は十分な説明にならないケースが増えています。規程、教育記録、資産台帳、アカウント管理記録、バックアップ結果、ログ監視、脆弱性対応履歴など、実施を裏付ける証跡が必要です。証跡を日常業務で残していなければ、取引先から照会を受けてから短期間で整えるのは困難です。

セキュリティ投資の優先順位が決められない

対策項目を列挙するだけでは、限られた予算をどこへ投じるか決めにくくなります。たとえば、古いVPN装置の更改、EDR導入、バックアップ強化、脆弱性診断、教育、ログ監視を同時に実施できない場合、重要業務と想定攻撃経路を基準に優先順位を決める必要があります。SCS評価制度への準備は、その判断基準を整理する契機になります。

インシデント発生時に取引先対応が遅れる

サプライチェーン攻撃では、自社だけで復旧すれば終わりではありません。侵害範囲、取引先データへの影響、外部接続の停止要否、報告先、再開条件などを短時間で判断する必要があります。平時に責任者と連絡経路が決まっていないと、技術調査と顧客説明が同時に進まず、復旧判断が遅れる要因になります。

特に準備を急ぎたい企業・システム・取引場面

従業員100～1,000名規模の企業では、システムや委託先が増えている一方、専任セキュリティ人材が十分でないケースもあります。特に次のような企業は、SCS評価制度の要求事項と自社の現状を早めに照合するメリットがあります。

- 大企業・金融機関・製造業・重要インフラ関連企業などからセキュリティチェックを受けることが多い企業
- 顧客データ、設計情報、ソースコード、認証情報など機密性の高い情報を預かる企業
- 取引先ネットワークへVPN、VDI、保守アカウントなどで接続する企業
- クラウド運用、システム開発、保守、BPO、コールセンターなど外部委託比率が高い企業
- 生産設備、物流、受発注、決済など停止時の影響が大きいシステムを持つ企業
- M&A、IPO、重要取引の開始など、外部から管理体制を精査される局面にある企業

SCS評価制度対応に向けて実施したい7つの準備

1. 適用範囲と重要業務を決める

最初に決めるべきなのは「どこを守るか」です。会社全体を曖昧に対象とするのではなく、重要な製品・サービス、顧客情報、取引先接続、主要拠点、クラウド環境などを整理し、どの範囲を優先するか決めます。対象範囲が不明確なままでは、資産台帳やアクセス権の確認も進みません。

2. IT資産・アカウント・外部接続を棚卸しする

情報システム部門は、サーバー、PC、ネットワーク機器、クラウド、SaaS、業務アプリケーション、特権ID、外部接続アカウントを一覧化します。重要なのは「台帳があるか」ではなく、「現在の状態と一致しているか」です。退職者ID、利用されていないVPNアカウント、管理者権限の過剰付与などは、攻撃者が悪用しやすいポイントになります。

3. 取引先・委託先のリスクを分類する

すべての取引先を同じ強度で管理する必要はありません。自社ネットワークへの接続権限、扱う情報の機密性、代替可能性、停止時の事業影響などで重要度を分けます。重要委託先については、契約時のセキュリティ条件、再委託、インシデント報告、ログ保存、契約終了時のデータ消去などを確認します。

4. 脆弱性を把握し、優先順位を付けて是正する

インターネット公開システムやリモート接続機器は、サプライチェーン攻撃の入口になりやすい領域です。Webアプリケーション診断では、認証・アクセス制御・入力処理などアプリケーション固有の弱点を確認できます。プラットフォーム診断では、OS、ミドルウェア、ネットワーク機器などの既知脆弱性や設定不備を確認します。

より実戦的な検証が必要な場合は、ペネトレーションテストを用いて「複数の弱点を組み合わせると重要資産まで到達できるか」を評価します。なお、★3は文書中心の専門家確認付き自己評価であり、特定の診断サービスを受ければ自動的に取得できる制度ではありません。診断は、要求事項への対応状況を技術面から確認し、是正を進めるための手段として位置づけることが重要です。

5. 検知・インシデント対応・復旧を実際に動かせる状態にする

EDRやログ監視を導入していても、アラート発生時に誰が判断し、誰へ報告し、どの機器を隔離するかが決まっていなければ十分に機能しません。インシデント対応手順、緊急連絡網、証拠保全、外部専門家への連絡条件、経営層への報告基準を整備します。バックアップについては、取得していることだけでなく、復元テストを行い、必要な時間内に業務を戻せるかを確認します。

6. 要求事項を「証跡」で説明できるようにする

SCS評価制度対応では、規程やルールを作るだけでなく、運用されていることを示す証跡が重要です。例として、教育受講記録、パッチ適用記録、棚卸し結果、アクセス権レビュー、インシデント訓練記録、バックアップ復元結果、委託先評価記録などがあります。申請前だけ作るのではなく、定常業務として残る仕組みにすることが効率的です。

7. 経営層が残余リスクと投資優先順位を承認する

経営層は「すべてのリスクをゼロにする」ことではなく、どのリスクを低減し、どのリスクを許容し、どこに予算を投じるかを判断します。経済産業省の「サイバーセキュリティ経営ガイドライン Ver3.0」でも、経営者が認識すべき原則として、自社のみならずサプライチェーン全体にわたる対策への目配りが示されています。

出典：経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

実施前に用意しておきたい資料

初期診断やギャップ分析を効率よく進めるには、次の資料を可能な範囲で集めておくといでしょう。すべて揃ってなくても問題はありません。むしろ「存在しない資料」が管理上のギャップを示している場合があります。

- 情報セキュリティ基本方針、関連規程、インシデント対応手順、BCP
- 組織図、セキュリティ責任者・担当者・緊急連絡先
- IT資産台帳、ネットワーク構成図、クラウド／SaaS一覧
- アカウント管理・権限レビュー・退職者ID削除の記録
- パッチ適用、脆弱性管理、診断・監査の結果と是正記録
- バックアップ方針、取得状況、復元テストの結果
- 委託先・再委託先一覧、契約上のセキュリティ条項、定期評価結果
- 教育・訓練記録、インシデント対応訓練や標的型メール訓練の結果

対応期間・費用を左右する要因

SCS評価制度対応に必要な期間は、従業員数だけでは決まりません。適用範囲、拠点数、利用システム数、クラウド利用状況、委託先数、既存のISMS等の管理体制、証跡の整備状況、技術的な是正項目の数によって変わります。

既にISMSや内部監査の運用があり、資産台帳・規程・アクセス権レビュー・インシデント手順などが整っている企業では、既存資料を活用できる可能性があります。一方、ルールが担当者の経験に依存している場合は、文書化だけでなく業務プロセスの変更が必要になるため、準備期間が長くなります。

費用も同様です。制度上の申請・登録に関する費用と、ギャップ分析、規程整備、診断、製品導入、ログ監視、教育、専門家確認などの対策費用は分けて考える必要があります。社内稟議では「SCS取得費用」だけでまとめず、制度対応に必要な管理改善費と、既存リスクを低減するためのセキュリティ投資に分けると説明しやすくなります。

社内稟議では何を説明すべきか

経営会議や予算申請では、技術用語を並べるよりも「どの取引・事業を守るための投資か」を示すことが重要です。以下の順番で整理すると、セキュリティ投資を事業課題として説明しやすくなります。

- 背景: 主要顧客・業界で取引先セキュリティ確認が強化されていること
- 事業影響: 重要委託先や自社システム停止時に影響する売上・生産・顧客対応
- 現状ギャップ: SCS要求事項等と比べた不足点
- 優先施策: 短期是正と中期投資を分けた対応計画
- 必要予算: 外部支援、診断、製品、教育、運用工数を分離
- 成果: 取引先説明の迅速化、インシデント耐性向上、監査対応の効率化

SCS評価制度対応を支援する会社の選び方

支援会社を選ぶ際は、制度のチェック項目を埋めるだけでなく、実際の攻撃経路と業務影響を踏まえて改善計画まで設計できるかを確認します。特に、組織面のコンサルティングと技術面の検証を別々の会社へ依頼すると、優先順位が分断されることがあります。両者をつなげて説明できる会社かどうかは重要な選定軸です。

RFP・見積依頼時に確認したい事項

- SCS評価制度の要求事項・評価基準に沿ったギャップ分析が可能か
- 規程整備だけでなく、実際の運用・証跡作成まで支援できるか
- Webアプリケーション診断、プラットフォーム診断、ペネトレーションテスト等を必要に応じて組み合わせられるか
- 指摘事項に重要度・事業影響・対応期限を付けた改善ロードマップを作成できるか
- 経営層向けと実務担当者向けに報告内容を分けられるか
- 機密情報、構成図、アカウント情報、診断データの取扱方法が明確か
- 申請後の継続改善、再診断、教育、監視まで支援可能か

よくある失敗と注意点

チェックシートを埋めること自体を目的にする

最も避けたいのは、「〇を付けられる資料」を作ることが目的になるケースです。実際のアカウント削除、パッチ適用、委託先管理、インシデント対応が動いていなければ、攻撃リスクは下がりません。制度対応と実効性のある改善を同じ計画で進めることが重要です。

SCS対応を情報システム部門だけに任せる

取引先契約、外部委託、教育、BCP、個人情報、危機広報などは、情報システム部門だけでは完結しません。管理部門、法務、調達、事業部門、経営層を含めた役割分担が必要です。

診断を実施したことで安心してしまう

脆弱性診断やペネトレーションテストは重要ですが、それだけでサプライチェーンリスクを網羅できるわけではありません。契約・委託先管理、教育、バックアップ、インシデント対応、ログ監視などの組織的・運用的対策と組み合わせる必要があります。

重要取引先を一律に扱う

取引先数が多い企業ほど、重要度に応じた管理が不可欠です。すべての取引先に同じ要求を出すと、自社の管理工数も相手側の負担も増えます。扱うデータ、接続権限、停止時影響などで分類し、重要度に応じて確認方法を変えます。

Librus株式会社が提供できるSCS評価制度対応支援

Librus株式会社では、SCS評価制度への対応を「申請書類の作成」だけでなく、サプライチェーン攻撃への実効的な耐性を高める取り組みとして支援します。企業ごとの事業内容、取引関係、IT環境、既存の管理体制を確認し、必要な範囲を個別に設計します。

支援では、要求事項とのギャップ分析、対象範囲の整理、規程・証跡の整備、委託先管理、改善ロードマップ策定に加え、必要に応じてWebアプリケーション診断、プラットフォーム診断、ペネトレーションテスト、SOC／CSIRT構築・運用支援、インシデントレスポンス、デジタルフォレンジック、セキュリティ教育、SBOM導入・運用支援まで組み合わせることが可能です。

特徴は、経営・組織・技術を分断せず、一気通貫で整理できる点です。たとえば、診断で見つかった脆弱性を「技術的な危険度」だけでなく、「主要顧客へのサービス停止につながるか」「取引先データへ到達可能か」「SCS対応上での管理策と関係するか」という観点で整理し、経営層と実務担当者が共通認識を持てる形へ落とし込みます。

よくある質問

Q1. サプライチェーン攻撃と通常のサイバー攻撃は何が違いますか？

攻撃経路が異なります。サプライチェーン攻撃では、標的企業を直接攻撃するのではなく、取引先、委託先、ソフトウェア、クラウドサービスなどを経由して侵入・妨害する点が特徴です。ただし、使われる手法自体は脆弱性悪用、認証情報窃取、マルウェアなど一般的な手法と重なることがあります。

Q2. SCS評価制度はすべての企業に義務化されますか？

2026年10月時点で、すべての企業に一律の法的取得義務がある制度ではありません。一方、IPAは取引契約等で委託元が委託先へ適切な段階を示す利用を想定しており、実務上は顧客・発注元から対応を求められる可能性があります。

Q3. ★3と★4はどちらを目指せばよいですか？

取引先からの要求、扱う情報、事業停止時の影響、自社のサプライチェーン上の役割によって判断します。★3は一般的なサイバー脅威への基礎的対策、★4はより重要な企業・資産を想定した包括的対策と第三者評価・技術検証が中心です。

Q4. ISMSを取得していればSCS対応は不要ですか？

不要とは言えません。既存のISMS文書や運用はSCS対応に活用できる可能性があります。SCS評価制度は独自の要求事項・評価基準を持ちます。要求事項ごとに適合状況を確認する必要があります。

Q5. 脆弱性診断を受ければSCS★3を取得できますか？

脆弱性診断だけで取得できる制度ではありません。★3は要求事項に基づく自己評価をセキュリティ専門家が確認する方式で、すべての要求事項・評価基準を満たす必要があります。診断は技術対策の実装状況を確認する有効な手段の一つです。

Q6. 取引先・委託先にはどこまで確認すべきですか？

扱う情報、外部接続権限、事業停止時の影響、再委託の有無などで重要度を分類し、重要度に応じて確認方法を変えるのが現実的です。契約条項だけでなく、定期的な評価やインシデント報告方法まで確認します。

Q7. SCS対応はいつから始めるべきですか？

★3・★4は2027年3月頃の運用開始が予定されています。規程や証跡、アカウント整理、委託先契約、脆弱性は正などは短期間では整わないため、取引先から正式に要求される前にギャップ分析から始めることが現実的です。

Q8. 対象範囲が決まっていなくてもコンサルティングを依頼できますか？

可能です。むしろ初期段階では、重要業務・重要資産・取引先との接続関係を整理し、どこを適用範囲とするか決める作業が重要です。対象範囲の整理から外部専門家へ相談する方法があります。

まとめ | サプライチェーン攻撃対策は「取引を守る仕組み」として考える

サプライチェーン攻撃は、取引先、委託先、ソフトウェア、クラウドサービスなど、自社の外側にある弱点を経由して被害が波及する攻撃です。自社だけの境界防御を強化しても、重要な委託先の停止や認証情報の悪用まで防げるとは限りません。

SCS評価制度は、このようなサプライチェーンリスクに対し、企業が必要な対策水準を共通基準で示し、取引先間で確認しやすくする仕組みです。★3・★4は2027年3月頃の運用開始が予定されており、取引契約の中で活用されることも想定されています。

対応の第一歩は、申請書を作ることはありません。重要業務と資産を特定し、取引先・外部接続・脆弱性・アカウント・バックアップ・インシデント対応・証跡を整理し、優先順位をつけて改善することです。結果として、SCS評価制度への準備だけでなく、事業継続や顧客説明、監査対応の質も高めやすくなります。

SCS評価制度対応の進め方が決まっていない段階からご相談いただけます

「自社は★3と★4のどちらを目指すべきか分からない」「要求事項と現状の差が見えない」「どこまで診断や技術対策が必要か判断できない」といった段階でも、Librus株式会社へご相談いただけます。

現状の体制・IT環境・取引関係を整理したうえで、優先して確認すべき範囲、必要な証跡、技術的な検証、改善ロードマップを具体化します。制度対応と実際のセキュリティ強化を別々に進めるのではなく、同じ投資で取引先説明とリスク低減の両方につながる計画を作ることで、不要な重複対応を減らしやすくなります。対象範囲や実施方法がまだ決まっていない場合も、初期整理からご相談ください。

主な公的情報

IPA「SCS評価制度」: <https://www.ipa.go.jp/security/scs/index.html>

IPA「SCS評価制度の詳細情報」: <https://www.ipa.go.jp/security/scs/details.html>

IPA「要求事項・評価基準」: <https://www.ipa.go.jp/security/scs/requirements-criteria.html>

IPA「情報セキュリティ10大脅威 2026」: <https://www.ipa.go.jp/security/10threats/10threats2026.html>

経済産業省「SCS評価制度」: <https://www.meti.go.jp/policy/netsecurity/scs.html>

経済産業省「サイバーセキュリティ経営ガイドライン」:

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経済産業省「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」:<https://www.meti.go.jp/policy/netsecurity/partnership2.html>

監修者

鎌田光一郎: 青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティング合同会社に転籍。金融機関に対するコンサルティング業務に従事。その後、Librus株式会社を設立、代表取締役役に就任。

お問い合わせ先

Librus株式会社(代表取締役 鎌田光一郎)

105-0004 東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F

03-6772-8015

お問い合わせフォーム: <https://librus.co.jp/contact>