サイバー攻撃の連鎖を断ち切る サプライチェーンのセキュリティ対策

新評価制度に先駆け、今取り組むべき対策とは

中小企業を踏み台にした「サプライチェーン攻撃」が急増し、セキュリティ対策はもはや一企業の問題ではなく、深刻な社会課題となっています。このリスクに対応するため、経済産業省は企業のセキュリティ対策を「可視化」する新制度の導入準備を進めています。本稿では、この新制度の要点と、企業が「今取り組むべき対策」を解説します。

1 あらゆる企業が標的となり得る、サプライチェーン攻撃の脅威

1社のセキュリティ不備で崩壊するサプライチェーン

デジタル化が加速する現代社会において、サイバー攻撃の脅威はかつてないほど深刻化しています。攻撃の標的になるのは、決して大企業だけではありません。信頼関係で結ばれた取引先やグループ会社など、サプライチェーンを構成するあらゆる組織が標的となり得る時代です。

実際に、セキュリティ投資が手薄になりがちな中小企業を踏み台とし、その取引先である大企業を狙う「サプライチェーン攻撃」が急増しています。警察庁の報告からは、ランサムウェア被害において中小企業が狙われる状況が増加傾向にあることがわかります[*1]。また、IPA（情報処理推進機構）の「情報セキュリティ10大脅威 2026」においても、「サプライチェーンや委託先を狙った攻撃」は4年連続で組織向け脅威の第2位に挙げられ[*2]、その影響の大きさがうかがえます。

実際の被害事例

- 病院の給食委託業者への不正侵入が起点となり、病院システムがランサムウェアに感染・暗号化される
- 自動車部品メーカーのマルウェア感染により、大手自動車企業の国内全工場が稼働停止に追い込まれる

1社のセキュリティ不備がサプライチェーン全体の機能を麻痺させかねないこの課題は、もはや個別企業のリスク管理を超えた、社会全体の課題となっています。

サプライチェーンの信頼を可視化する新制度の登場

このような状況下で、取引先を選定する際には、相手のセキュリティ対策が信頼できるかどうかが極めて重要な要件となります。しかし、統一された基準がないために、発注元企業は取引先のセキュリティ対策状況を客観的に判断できず、委託先企業は複数の取引先から個別の対策を要求され対応負荷が増大しているという課題が生じています。

こうした構造的な課題を解決するため、経済産業省は、サプライチェーン全体のセキュリティ水準向上を目的とする「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」（以下、セキュリティ対策評価制度）の導入準備を進めています。

この制度は、これまで不透明だった企業のセキュリティ対策状況を、組織体制から技術的対応、そして運用に至るまで多角的に評価し、可視化するものです。これにより、発注元は客観的な指標に基づいて信頼できる取引先を選定できると共に、委託先は一度の評価で複数の取引先に自社の安全性を証明でき、対応負荷の軽減が可能となります。その結果として、サプライチェーン全体の防御力向上に大きく貢献することが期待されます。

現時点で本制度に法的な拘束力はありませんが、将来的には取引先選定において、セキュリティレベルの提示が標準要件となる可能性が考えられます。また、制度への対応企業を公表する仕組みも予定されているため、事業継続性の確保とブランド価値向上の観点から、早期に対応準備を始めることが推奨されます。

出典：*1 警察庁「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」
*2 独立行政法人情報処理推進機構「情報セキュリティ10大脅威 2026」https://www.ipa.go.jp/security/10threats/10threats2026.html

2 新制度「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」のポイント

セキュリティ対策評価制度の要求事項は多岐にわたり、評価プロセスも厳格に設計されています。経済産業省が公表した「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に関する制度構築方針」から読み解く、本制度のポイントを紹介します。

3段階の評価レベル

本制度は、企業間の取引や契約において、発注元企業が委託先企業に対して、要件に合うセキュリティレベルを提示し、その達成を促すことで、サプライチェーン全体のセキュリティ水準を向上させることを目的としています。

セキュリティレベルは、**★1**～**★5**の5段階で区分されています。このうち**★1**・**★2**はIPAの自己宣言制度「SECURITY ACTION」で既に定義されており、今回のセキュリティ対策評価制度によって新たに**★3**・**★4**・**★5**が設定される予定です。**★3**・**★4**については2026年度下期の本格運用開始を目指し、制度基盤の整備や導入促進といった準備が進んでいます。

表1 段階別評価の概要

成熟度の定義	★3	★4	★5
想定される脅威	● 広く認知された脆弱性等を悪用する**一般的なサイバー攻撃**	● **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	● **未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実施すべき**セキュリティ対策 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等、包括的な対策を実施	サプライチェーン企業等が**さらに目指すべき高度な**対策 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施

※ 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（経済産業省）を基に作成

信頼性を担保する評価の仕組み

制度の高い信頼性を担保するため、評価プロセスはセキュリティレベルに応じて厳格に定められています。例えば、**★3**は自己評価が基本ですが、**★4**以上では第三者評価が原則となる予定です。これにより、評価の客観性が確保される仕組みとなっています。

表2 セキュリティレベルに応じた評価スキーム

分野	★3	★4
評価スキーム	**専門家確認付き自己評価**	**第三者評価**
評価の進め方	**①自己評価** 取得希望組織が★3要求事項に基づき自己評価を記入 **②専門家確認** ①の内容をセキュリティ専門家*3が確認・助言し、署名	**①文書確認** 指定委員会が指定した評価機関が書類を確認 **②実地審査** 評価機関がヒアリング、規定、操作画面等の確認を行う **③技術検証** 技術検証事業者が、VPN装置などインターネットに公開している機器に対して既知脆弱性の悪用等の一般的な攻撃パターンを試行
有効期間	**1年**（毎年の更新が必要）	**3年**（3年ごとの第三者評価および毎年の自己評価の提出が必要）

※ 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（経済産業省）を基に作成

*3 情報処理安全確保支援士（登録セキスペ）やCISSP（Certified Information Systems Security Professional）などの資格を保有し、かつセキュリティ対策評価制度が定める研修を受講した者を「セキュリティ専門家」と定義。

7つのセキュリティ要求事項・評価基準

評価は、以下の7つの分野にわたる要求事項・評価基準に基づいて行われます。各分野においてレベルごとに達成すべき対策が定められており、**★3**では26件、**★4**では43件の要求事項が設定されています。なお、要求事項や評価基準は、最新のサイバーセキュリティ動向を踏まえて定期的に見直される予定です。

要求事項・評価基準案は、NIST（米国国立標準技術研究所）のサイバーセキュリティフレームワークが示す機能に対応しています。サイバー攻撃が高度化し、100%防ぐことは困難と言われる現代において、企業に求められるセキュリティは、単一の対策だけでは成り立ちません。取引先管理を含めたセキュリティガバナンスの確立、そして、攻撃の予防から攻撃された後の対応までを考慮した包括的な防御策が不可欠です。

すでにISO 27001認証を取得されている場合でも、セキュリティ対策評価制度では、より詳細な要求事項・評価基準が設定されているため、個別に評価対応が必要となります。

表3 7つの分野にわたる要求事項・評価基準

分野	★3	★4（★3に加えて）	NISTとの対応
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** ● 自社のセキュリティ担当の明確化 ● セキュリティ対応方針の策定	**継続的改善に資するリスク管理体制の構築** ● 定期的な経営層への報告、不備の是正等	統治 （Govern）
取引先管理	**取引先に課す最低限のルール明確化** ● 他社との機密情報の取扱い明確化 ● 接続している外部情報サービスの把握	**取引先の管理・把握及び取引先との役割・責任の明確化** ● 機密情報共有先の把握 ● 重要な取引先等の対策状況把握 ● インシデント発生時の他社との役割等の明確化	
リスクの特定	**自社IT基盤や資産の現状把握** ● 情報資産やネットワークの把握 ● 外部情報サービスの管理	**脆弱性など最新状況の把握と反映** ● 脆弱性管理体制、管理プロセスの明確化	識別 （Identify）
攻撃等の防御	**不正アクセスに対する基礎的な防御** ● ID管理手続、アクセス制限の設定 ● パスワードの安全な設定及び管理 ● 内外ネットワーク境界の分離・保護 **端末やサーバーの基礎的な保護** ● 適時のアップデート適用、不要ソフトウェアの削除 ● 端末等へのマルウェア対策	**多層防御による侵入リスクの低減** ● 重要な保管データの暗号化 ● ログの収集・定期的な分析の実施 ● 社内システムにおける適切なネットワーク分離 ● 社外への不正通信の遮断（出口対策）	防御 （Protect）
攻撃等の検知	**ネットワーク上の基礎的な監視等** ● ネットワーク接続・データの監視	**迅速な異常の検知** ● 情報機器等の状態、挙動の監視・対応や分析	検知 （Detect）
インシデントへの対応	**インシデント発生に備えた対応手順の整備** ● インシデント対応手順の作成	（★4での追加項目はなし）	対応 （Recover）
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** ● インシデント発生から復旧するための対策の整備	**インシデントからの復旧手順等の整備** ● 復旧ポイント、復旧時間を満たす手順等の整備	復旧 （Respond）

※ 上記は必ずしも全要求事項を網羅しているわけではない点に留意
※ 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（経済産業省）を基に作成

3 富士通が実現する、実践的なサプライチェーンセキュリティ強化

制度開始に先駆けて、お客様のセキュリティ対応状況を可視化

セキュリティ対策評価制度で求められる要求事項は多岐にわたり、一朝一夕での対応は困難です。しかし、日々高度化する攻撃を前に、制度開始まで対応を先送りすることは深刻な経営リスクにつながりかねません。公表されている要求事項・評価基準を基に自社の対策状況を把握し、対策が不足している領域の強化に着手することが、リスクの低減と将来の円滑な制度対応を実現するカギとなります。

富士通は、2,500社以上のセキュリティコンサルティングで培った知見を活かし、お客様の制度対応準備をご支援します。まず、①情報セキュリティ対策基準やインシデント対応手順、ネットワーク・システム構成図といった各種資料の確認とヒアリングを通じて、お客様の現状を客観的に把握します。その上で、②Fit&Gap分析により、現状とセキュリティ対策評価制度の要求事項・評価基準との差異を明確にし、準拠性を評価します。③分析結果を基に、リスクと課題を整理し、制度準拠に向けた具体的な対策をご提案します。単なる対策提案に留まらず、ご要望に応じて対策優先度の設定やロードマップの策定まで幅広くご支援することが可能です。

このプロセスを通じて、お客様のセキュリティ強化を図ると共に、制度開始へのスムーズな対応、関係者からの信頼獲得、そして市場における競争優位性の確立までを強力に後押しします。

図1 円滑な制度対応をご支援するプロセス

サプライチェーンセキュリティマネジメントを段階的に強化

サプライチェーンに起因する自社のセキュリティリスクの低減や事業継続性の確保は、すべての企業にとって喫緊の課題です。委託先の適切な監督義務などを果たすべく、取引先やグループ会社、委託先などサプライチェーンを構成する企業のセキュリティ管理・統制の見直しが早急に進められています。しかしながら、複雑化・多様化するサプライチェーンにおいてその管理・統制に課題を抱えるお客様も少なくありません。

富士通では、ISO 27001をはじめとする各種認定取得支援で培った知見に基づき、お客様の改善項目を明確化し、事業に即した実現性の高いセキュリティ管理手順・体制の整備に貢献します。さらに、整備した管理手順などに基づく委託先への説明や、セキュリティ監査の実施まで、実効性のある運用をサポートいたします。

取引先などのセキュリティリスクの可視化と専門家による改善支援

事業継続性を高めるためには、取引先やグループ会社、委託先など、サプライチェーンを構成する各社のセキュリティリスクを把握することも重要です。攻撃者は常に、企業のWebサイトや公開サーバー、ネットワーク機器など、外部からアクセス可能な情報を徹底的に調査し、侵入の足掛かりを探っています。こうした背景から、インターネット上の公開情報を活用し、攻撃者視点で各社がどのように見えているかを客観的に把握することが、対策強化の第一歩となります。

富士通は、セキュリティリスクレイティングサービス「SecurityScorecard」を活用し、各社のセキュリティリスクを定期的に評価。富士通の専門家が取引先様などに評価結果と検知されているリスクを直接説明し、具体的な改善策まで提示します。これにより、お客様の負担を軽減しながらサプライチェーン全体のセキュリティ強化をご支援します。（図2）

本サービスに留まらず、富士通はサプライチェーンセキュリティを強化するための多彩な製品・サービスを取り揃えており、お客様の状況に合わせた最適なご提案が可能です。

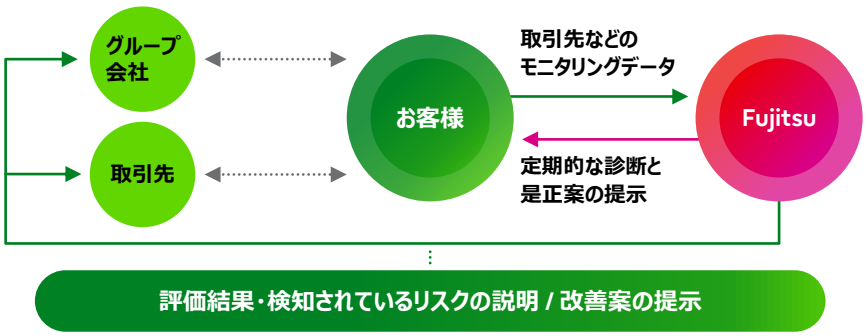

図2 セキュリティリスク評価のイメージ

4 信頼されるデジタル社会の実現に向けて

ひとたびサイバー攻撃を受ければ、その被害は自社に留まらず、サプライチェーン全体、そして社会インフラや個人の生活にまで及びます。誰もが攻撃のターゲットとなり得る今、サプライチェーン全体で攻撃の「予防」から攻撃されたあとの「対応」までを考慮した包括的な対策を講じることが、事業継続、ひいては社会全体の安全を守ることにつながります。

富士通はお客様と共に、真に安心・安全で持続可能な社会の実現を目指します。コンサルティングから具体的なオファリングの導入・運用まで、お客様に寄り添い一気通貫で支援することで、お客様の持続可能な事業活動と、信頼されるデジタル社会の未来を共に築いてまいります。

※ 本資料は、2026年3月時点の情報を基に作成しております。

お問い合わせ先

富士通株式会社

https://contactline.jp.fujitsu.com/contactform/csque04701/821681/

