牛島総合法律事務所
情報管理／サイバーセキュリティニューズレター

サプライチェーンのセキュリティ強化に向けた評価制度（中間取りまとめ）について

２０２５年４月１５日

弁護士・情報処理安全確保支援士　小坂光矢

＜目次＞

近年、サプライチェーンを構成する企業の一部がサイバー攻撃を受けることで、取引先企業を巻き込んだ情報漏えいやサービス停止などのインシデントが頻発しています。IPA（独立行政法人情報処理推進機構）が公表する情報セキュリティ 10 大脅威 2025 においても、「サプライチェーンや委託先を狙った攻撃」が 2 位にランクインするとともに、2019 年の初選出以来、7 年連続でランク入りしています。
そうした状況を踏まえ、NISC（内閣サイバーセキュリティーセンター）と経済産業省は、2025 年 4 月 14 日に、サプライチェーン全体のセキュリティ対策を底上げし、企業活動におけるサイバーリスクを軽減することを目的とした「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」（以下「本制度」）の検討に関する中間取りまとめ（以下「中間取りまとめ」）を公表しました（※）。
本ニューズレターでは、本制度の概要や今後の課題・スケジュール、及び実務上の示唆について解説いたします。

※ 本制度の関連資料：
プレスリリース（NISC）
プレスリリース（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（概要）
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構築に向けた中間取りまとめ
【参考資料 1】★3・★4 要求事項案・評価基準案

1. 背景と趣旨

サプライチェーンにおいて想定されるセキュリティリスクは、以下の 3 つに大別されます。

①取引先へのサイバー攻撃等に起因する製品・サービスの提供途絶リスク
②取引先へのサイバー攻撃等に起因する機密情報の漏えい、改ざんリスク
③取引先等を踏み台としたネットワークを通じた不正侵入リスク

もっとも、特に複雑なサプライチェーンにおいては、複数の発注企業それぞれから異なるセキュリティ対策水準

を要求されるため、受注企業側に過度な負担となったり、「どの対策を、どの程度まで導入すべきか」が不透明になりがちであるという課題がありました。また、発注企業側としても、受注企業の対策状況が見えにくいため、サプライチェーン全体として十分な対策が浸透せず、結果的に脆弱性が残ってしまう懸念が指摘されていました。こうした課題に対応するため、本制度では、**主としてサプライチェーン企業（2 社間契約における受注者側）に対して、段階的な指標に対応したセキュリティ対策の実施を促すことを通じて、サプライチェーン全体でのセキュリティ対策水準の向上を図る**ことが意図されています。本制度を通じて、企業が講じているセキュリティ対策が客観的に可視化されることとなるだけでなく、以下のメリットが期待されています。

・受注企業側：自社が講じるべきセキュリティ対策レベルの客観的な把握や、取引先への説明根拠としての活用
・発注企業側：取引先におけるセキュリティ対策の実施状況の把握が容易となり、情報漏えいやサービス停止のリスクを低減できる
・社会全体：経済・社会全体のサイバーレジリエンスが強化されるとともに、サイバー攻撃に適切に備えている企業等が適切に評価される

2. 制度の概要

本制度では、サプライチェーンを構成する企業等の IT 基盤（オンプレミス・クラウド）を評価対象とし、重要度や必要とされる対策レベルに応じて、「★3」「★4」「★5」の三段階のセキュリティ対策が設定される予定です。IoT 機器を評価対象とする JC-STAR 制度（2025 年 3 月開始）とは対象が異なる点に注意が必要です。
各段階の概要は、以下のとおりです。

段階	想定される脅威・リスク	対策の基本的な考え方	評価方法	有効期間
★3	広く知られた脆弱性を突く一般的なサイバー攻撃	**全てのサプライチェーン企業が最低限実装すべき**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）	自己評価	1 年
★4	ビジネス継続や機密情報管理に影響を及ぼす標的型攻撃	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（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）	第三者評価	3 年
★5	より高度で未知の手口のサイバー攻撃	サプライチェーン企業等が**到達点として目指すべき**対策（現時点でのベストプラクティス）	第三者評価（予定）	未定

★3 の自己評価に関しては、**自己評価取得時、及び 1 年ごとの更新時に、社内又は社外の有資格者（情報処理安全確保支援士など）による助言・評価が必要**とされる見込みです。また、★4 の第三者評価に関しては、有効期間は 3 年とされていますが、1 年ごとに自己評価を実施することが求められる予定です。
なお、★5 に関しては、2025 年度以降に、ISMS 適合性評価制度との整合性にも配慮しつつ、また自動車産業におけるセキュリティガイドライン（「自工会/部工会ガイドライン」）等の既存のガイドラインも参照しながら、具体的な要求事項や評価基準、スキーム等についての検討が行われる予定です。

3. セキュリティ対策（要求事項案と評価基準案）の概要

中間取りまとめでは、★3・★4 レベルで要求されるセキュリティ対策を具体化した要求事項や評価基準の案が示されています。ガバナンス、取引先管理、システム防御、インシデント対応などを中心に、★3 については合計 25 個、★4 については合計 44 個の要求事項が挙げられています。概要は以下に列挙するとおりであり、（※）が付された事項は★4 において求められる追加的な要求事項です。評価基準も含めた詳細については、「【参考資料 1】★3・★4 要求事項案・評価基準案」をご確認ください。

① ガバナンスの整備
・セキュリティポリシーの策定と周知
・法令等を踏まえた社内ルールの策定・周知徹底（※）
・セキュリティ担当部署等の決定
・サイバー攻撃や予兆を監視・分析する体制の整備（※）
・従業者等との秘密保持・守秘義務契約の締結
・年１回以上の頻度でのセキュリティ対策状況の棚卸し・見直し

② リスクの特定
・ハードウェア（HW）、OS、ソフトウェア（SW）情報やネットワーク情報に関する一覧の作成
・機密区分に応じた情報の管理ルールの策定と実施
・脆弱性の管理体制、管理プロセスの策定（※）

③ インシデントへの対応及び復旧
・あらかじめ定めた手順に沿ったインシデント対応
・重要システムの事業継続のために必要な復旧準備（※）

④ 取引先管理
・顧客、クラウドサービス提供事業者等の取引先とのビジネス・システム上の関係性の把握
・取引先等との間での機密情報に関する取扱いの明確化
・重要な機密情報等を取り扱う取引先におけるセキュリティ対策状況の把握（※）
・インシデント発生時の取引先等との役割・責任分担（※）
・契約終了時における機密情報やアクセス権等の回収・破棄（※）

⑤ 攻撃等の防御
・アカウント発行・管理プロセスの確立
・パスワードの設定ルールやシステム・情報の重要度に応じた認証強度の決定
・人事異動時の権限管理
・入退室管理（※）、可搬媒体の持込み・持出し制限（※）
・従業者のセキュリティ意識向上と知識・スキルの維持を目的とした教育・研修（※）
・適切なバックアップ、保管データ暗号化（※）、サポート期限の切れた HW／SW の利用停止等（※）
・内外ネットワークの適切な分離と境界部分の防護

⑥ 攻撃等の検知
・ネットワーク接続やデータ転送の監視
・HW／SW の状態や挙動の監視（※）
・インシデントとして扱う範囲の明確化（※）

4. 独占禁止法・下請法との関係

本制度に関しては、特に発注企業が受注企業に対して要求事項等の実施や★取得の推奨等を求める場面において、**独占禁止法上の優越的地位の濫用や下請法違反に注意**が必要であると考えられます。例えば、セキュリティ対策責任者の設置、従業員へのセキュリティ教育の実施、サイバー攻撃による被害発生時における自らが定めた対処フローの遵守など、セキュリティ体制の構築を要請した結果、人件費などのコスト上昇を理由とする取引価格の引上げを求められたにもかかわらず、それに応じない理由を書面、電子メール等で回答することなく従来どおりに取引価格を据え置くことは、優越的地位の濫用に当たり得ます（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」（2022 年 10 月 28 日）参照）。

中間とりまとめによれば、独占禁止法や下請法の論点に関しては、**今後より具体的な法的整理や契約書雛形が示される**予定です。

5. 運用開始に向けたスケジュール

★3・★4 については、2025 年 4 月から 9 月にかけて実証事業を通じた制度案の検討が行われた上で、2025 年 10 月頃から 2026 年 3 月頃にかけて、要求事項・評価基準・評価スキームの確定、制度構築方針（案）の公表、及びパブリックコメント手続等が開始される予定です。その後、**2026 年 10 月頃を目途に制度の運用が開始される**予定です。

なお、★5 については、2025 年度下期以降に評価基準やスキーム、運用開始予定時期等が検討される予定です。

6. おわりに～実務上の示唆

サプライチェーン攻撃は、標的となった企業だけでなく、その取引先や関連企業を経由して被害が拡大し、損害賠償請求や取引停止、風評被害といった二次被害を引き起こす可能性があります。そのため、**今回の中間とりまとめで示された要求事項案や評価基準案を参考として情報セキュリティ体制を点検することは、発注企業・受注企業の双方にとって有益**であると考えられます。

また、本制度に関しては、政府調達の条件とすることや各業界のガイドラインへ組込むことも検討されています。そのため、制度が本格的に始動する頃には、一定レベルの★を取得していることが取引条件とされるといった事態も十分に想定されるところです。

以上を踏まえると、今の段階から、アイデンティティ管理やアクセス制御といった技術的な措置を講じておくだけではなく、以下のような**ガバナンス、取引先管理の観点からの取り組みについても開始しておくことが望ましい**と考えられます。

・個人情報保護法などの情報管理に関係する法令・ガイドラインを踏まえたセキュリティポリシーや情報セキュリティ規程、インシデント対応マニュアル等の整備
・情報の取扱いやセキュリティに関する従業員への教育・研修及び周知徹底
・従業者や取引先との秘密保持契約（NDA）、業務委託契約の再検討

当事務所には、情報処理安全確保支援士の資格を有する弁護士が所属しており、情報セキュリティの視点を含めた法的助言を行うことが可能です。今後の制度導入に向けて「どの程度の準備が必要か」といったご相談がございましたら、ぜひお気軽にご相談ください。

関連記事

・特集記事「業務委託先の情報セキュリティを確保するための実務上のポイント」

以 上