ICSCoE TLP:WHITE

実務者のための サプライチェーン セキュリティ手引書

-【別冊】チェックポイント集-

Ver1.0

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター（ICSCoE）
中核人材育成プログラム　７期生

実務者のためのサプライチェーンセキュリティプロジェクト

実務者のためのサプライチェーンセキュリティ手引書-【別冊チェックポイント集】-

2024 年 7 月 31 日　　初版発行

-----免責事項-----

- 本書は単に情報として提供され、内容は予告なしに変更される場合がある。
- 本書に誤りがないことの保証や、商品性または特定目的への適合性の黙示的な保証や条件を含め明示的または黙示的な保証や条件は一切ないものとする。
- 本書に記載の内容は、独立行政法人情報処理推進機構および産業サイバーセキュリティセンターの意見を代表するものではなく、著者の見解に基づいている。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとする。
- 本書の有効期限は、発行日から 2 年間とする。

4章　サプライチェーンセキュリティの取り組み準備

4.1.　方針・計画の策定

- □　経営層にサプライチェーンセキュリティを説明し、経営リスクとして理解してもらえているか
- □　サプライチェーンセキュリティの具体的な目標や方針・計画、およびロードマップが策定されているか
- □　立案した方針・計画は自社の経営方針やセキュリティ方針に合致し、経営層と合意しているか
- □　ロードマップはサプライチェーンセキュリティ推進の道筋を示せているか
- □　ロードマップやスケジュールは関係部門と共有して合意しているか

4.2.　体制の構築・整備

- □　早い段階で必要となる人員の規模や専任メンバーの要否を検討し、担当役員へ伝達しているか
- □　各担当者の役割を明確にし、マネジメント層の承認を得ているか
- □　経営層やサプライヤーと密に関わりがある部門が体制に含まれているか
- □　体制の責任と役割は、既存の BCP やサプライチェーンマネジメントなどの内部統制に整合しているか

5章　サプライチェーンの繋がりの整理と評価

5.1.　サプライチェーンの洗い出しと整理

- □　事業部門や調達部門と協力して、サプライチェーンの繋がりを整理・可視化しているか
- □　BCP 部門と協力し、既存の BCP を踏まえて取り組めているか
- □　サプライヤーの事業影響度を評価し、対応の優先順位を決定しているか
- □　必要に応じて、影響度評価を見直しているか

5.2.　サプライチェーンセキュリティ対策状況の評価

- □　サプライヤーにヒアリングの目的を説明したか
- □　ヒアリングに購買部門や事業部門など関係する部門は同行できているか
- □　チェックリストやヒアリング結果をもとに、セキュリティ対策状況の評価と分析を行い、サプライヤーの事業影響度やセキュリティ成熟度に基づいて分類・対策を整理しているか
- □　評価の結果をサプライヤーにフィードバックしたか

6章　強固なサプライチェーンの構築

6.1.　セキュリティ強化のサポート

- □　支援策は利益供与に該当しないか確認が取れているか
- □　サプライヤー向けの相談窓口の設置など、各サプライヤーに応じたセキュリティ強化のサポートを提供しているか
- □　紹介する支援策などはサプライヤーのセキュリティ成熟度に合致しているか
- □　個社訪問によるサプライヤー支援を実施し、個別の事情に応じた解決策を提供しているか

6.2.　サプライヤーとの契約締結

- □　サプライヤーに特定のセキュリティ製品の購入を強制したり、サイバーセキュリティ対策の有無を理由に不当な価格要求をおこなったりしていないか
- □　独占禁止法や下請法以外に、自社が注意すべき法令を確認したか
- □　契約書にサイバーセキュリティに関する具体的な取り組み内容を明記し、責任範囲を明確にしているか
- □　契約書に抽象的な記載がある場合、その内容について取引先と認識を共有し、誤解を防ぐための措置を取っているか
- □　契約書だけでなく、その他の取引書類にもサイバーセキュリティに関する項目を記載し、担当者の意識を高めているか
- □　業界ごとに作成される法令や規制について確認し、契約がそれらに準拠しているかを確認しているか

6.3.　リテラシーの向上

- □　セキュリティ教育にサプライチェーンに関する内容を含めているか
- □　サプライチェーンセキュリティに関する教育や情報発信が定期的に行われているか
- □　サプライヤーと脆弱性情報やサイバー攻撃に関する情報の共有がおこなえる環境を整えられているか

6.4.　レジリエンスの向上

- □　インシデント発生時の連絡手順、体制はサプライヤーと共有できているか
- □　インシデント発生時の関係各社への共有事項が事前整理されているか
- □　サプライヤーを含めて、サプライチェーン攻撃を想定したインシデント対応訓練を実施しているか
- □　訓練には社内外の報告ルートの確認やサプライヤーのサポート体制の確認が含まれているか
- □　インシデント対応計画が関係者間で定期的に検証されているか

7章　計画の評価と見直し

7.1.　計画の評価と見直し

- □　サプライチェーンセキュリティの取り組みが継続的に評価され、次の取り組みサイクルに反映されているか
- □　取り組みの目標を実効的なものに設定できているか
- □　計画の評価と見直しは定期的に行われ、取り組みが現状に適合しているかどうかが確認されているか
- □　評価方法が適切に構築されており、取り組みの効果を十分に把握することができているか
- □　方針・計画の見直しは国や業界のセキュリティ動向と取り組み評価結果の両面から行われているか
- □　サプライチェーンセキュリティの施策ごとの進捗や成果が定期的に経営層に適切に報告されているか