実務者のための
サプライチェーンセキュリティ
ハンドブック

Ver. 1.0

～注意・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ります。
・本書に記載した事項はすべて、記載時点の法律・法令・ガイドライン等に基づいておりますが、今後の変更に対する適合を保証するものではありません。
・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します。
・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ます。
・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します。
・本書で使用している画像（表表紙、裏表紙、各ページの登山に例えたイメージ図）はOpenAI社のChatGPTサービスを用いて作成しています。

はじめに

本書は、「実務者のためのサプライチェーンセキュリティ手引書」のサプライチェーンセキュリティの実務に関わる内容を項目ごとに1ページにまとめたハンドブックです。

サプライチェーンセキュリティに初めて取り組む担当者やサプライヤーとやり取りをする担当者が、サプライチェーンセキュリティの取り組みイメージを持ってもらうことを目的としています。

このハンドブックでは、サプライチェーンセキュリティの一連のプロセスを登山の準備から登頂した後の反省会までそれぞれのフェーズに例えました。
例えば、「サプライチェーンセキュリティ方針・計画の策定」は「登山計画の作成」、「サプライチェーンセキュリティ対策状況の評価」は「登山メンバーの持ち物点検と役割整理」と表現をしました。

本書を手に取っていただいた方が、サプライチェーンセキュリティに取り組む際の概要やポイントを把握でき、サプライチェーンセキュリティの業務に取り組みやすくなるきっかけになると幸いです。

⚠ 本書の内容に、ソフトウェアサプライチェーンは含みません

「サプライチェーンセキュリティとは登山である」

大きな山に挑む時には登山ガイドが役に立つ。

ーさぁ、サプライチェーンセキュリティという山に

私たちと一緒に登りましょう！

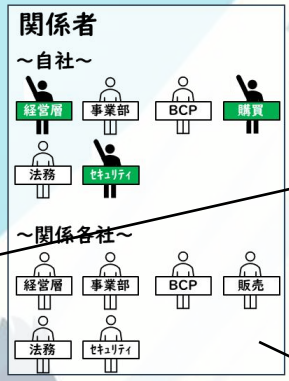
ハンドブックの読み方

サプライチェーンセキュリティハンドブックの読み方について説明します。
各ページは下記の6ブロックで記載しています。

- ①タイトル　：解説項目
- ②登山での例え　：解説項目を登山で例えた際のイメージ
- ③関係者　：関係するステークホルダー
- ④解説　：取り組み内容など
- ⑤チェックポイント　：取り組む際のチェックリスト
- ⑥手引書該当事項：別紙の該当箇所

それぞれのブロックの記載位置や内容は下記の解説を参照してください。

方針・計画の策定



解説

- サプライチェーンセキュリティはステークホルダーが多岐に渡るため、一朝一夕で実現することはできません。基本方針を定めて計画的に実行しましょう。
- はじめに基本方針とスケジュールを定めることで、サプライチェーンセキュリティの取り組みに統一感が生まれ計画的に
- 基本方針を策定する際は、経営層の合意を
社内展開や社外に発信する際の調整コス
力に推進することができます。
- サプライチェーンセキュリティは長期的に取
策定の段階から十分に経営層とコミュニケ
しょう。

チェックポイント!

- □ 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ますか？
- □ 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ますか？
- □ 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ますか？

手引書該当箇所　4.1.1 基本方針の策定
4.1.2 ロードマップおよび計画の策定

①タイトル
解説項目のタイトルを記載しています。

②登山での例え
伝えたいことを登山に例えたキーワードとイラストで表現しています。

③関係者
該当の取り組みに関与すべき関係者を一目で把握することができます。

④解説
該当項目に取り組む理由や取り組み内容、得られる効果、注意点などを示しています。

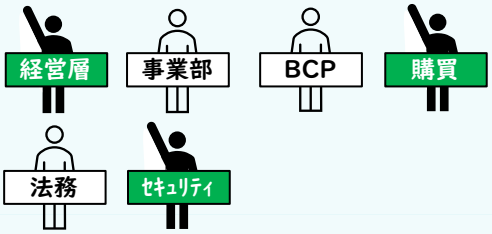
⑤チェックポイント
特に大事な内容をまとめています。
チェックリストとして活用しましょう。

⑥手引書該当箇所
別紙「実務者のためのサプライチェーンセキュリティ手引書」の該当箇所です。
詳細を確認するときに活用しましょう。

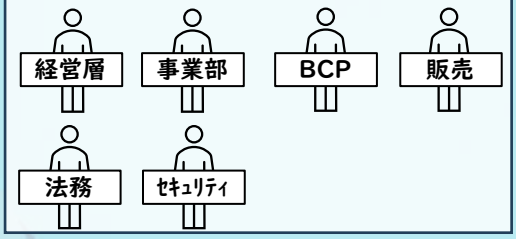
方針・計画の策定

関係者

～自社～



～サプライヤー～



解説

- サプライチェーンセキュリティはステークホルダーが多岐に渡るため、一朝一夕で実現することはできません。基本方針を定めて計画的に実行しましょう。
- はじめに基本方針とスケジュールを定めることで、サプライチェーンセキュリティの取り組みに統一感が生まれ計画的に進めることができます。
- 基本方針を策定する際は、経営層の合意を得て取り組みましょう。
  社内展開や社外に発信する際の調整コストを削減することができ、施策を強力に推進することができます。
- サプライチェーンセキュリティは長期的に取り組む必要があります。基本方針策定の段階から十分に経営層とコミュニケーションを取り、計画的に推進しましょう。

チェックポイント!

- □ 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ますか?
- □ 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ますか?
- □ 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ますか?

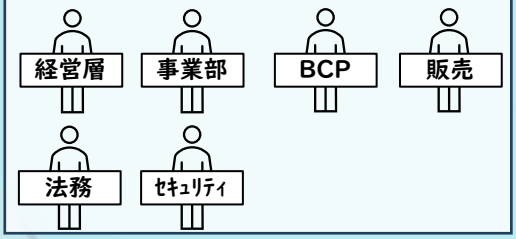
手引書該当箇所　4.1.1 基本方針の策定
4.1.2 ロードマップおよび計画の策定

体制の構築・整備

関係者

～自社～

～サプライヤー～



解説

- 立案した計画を円滑に実施するために、ステークホルダーと目的を共有し、コラボレーションできる実施体制を構築しましょう。
- 例えばサプライヤーとのコミュニケーションは、日頃からやり取りしている購買部門の担当者に役割を持たせるなど、役割と責任を明示し、得意な人が輝ける体制を意識します。
- 部門を横断した体制を機能させるためには、セキュリティ部門のラインに限定せず、購買部門や事業部門の役員など、経営層にも積極的に参加してもらえる体制とすることが大切です。

チェックポイント!

- □ 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ますか？
- □ 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ますか？

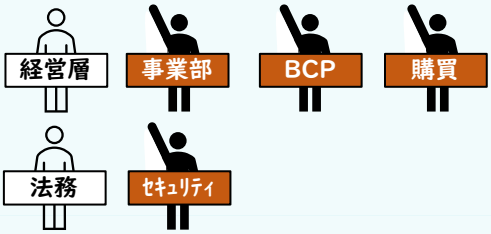
手引書該当箇所

4.2.1 理想の体制について
4.2.2 体制の構築
4.2.3 社内規定の整備

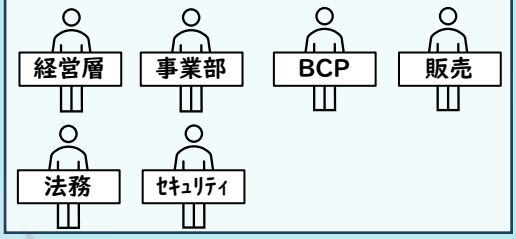
サプライチェーンの洗い出しと整理

関係者

～自社～



～サプライヤー～



解説

- サプライチェーンセキュリティの取り組みは、自社のサプライチェーンを理解するところから始めます。
- 購買部門などを通じ、サプライチェーンを構成する企業をもれなく洗い出し、BCP部門などとともに各サプライチェーン、各サプライヤーの事業影響度を評価します。
- 事業影響の大きなサプライチェーンから優先して対策を講じることで効率的にサプライチェーンのセキュリティ対策を実施できます。
- ビジネスのつながりを評価したうえで、セキュリティを実装することは、事業継続性への貢献を示すことにもなるでしょう。

チェックポイント!

- ☐ 事業部門、調達部門と連携して、事業影響を評価していますか?
- ☐ BCP部門と協力し、既存のBCPを踏まえて取り組めていますか?
- ☐ 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ますか?

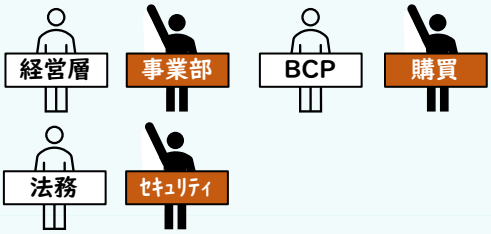
手引書該当箇所

5.1.1 サプライチェーンの洗い出し
5.1.2 サプライチェーンの繋がりの整理
5.1.3 事業影響度の大きなサプライチェーンの把握

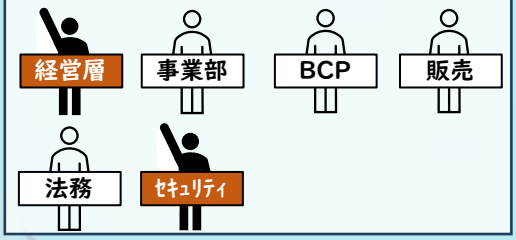
サプライチェーンセキュリティ対策状況の評価

関係者

～自社～



～サプライヤー～



解説

- サプライヤーのセキュリティ対策状況を把握・分析することで、サプライチェーンセキュリティを向上させるための具体策を検討することができます。目標に適したガイドラインやフレームワークを選定し、評価に取り掛かりましょう。
- 評価の目的はサプライチェーン全体のセキュリティ強化であり、評価結果はサプライヤーに不利益を与えるものではないと伝えましょう。
- 評価結果をもとに個別にヒアリングを実施するサプライヤーを選定しましょう。自社の購買部門や事業部門もなるべくヒアリングに出席してもらいましょう。
- 分析した結果をサプライヤーにフィードバックし、今後のセキュリティ対策強化の方針をアドバイスしてあげることで、取り組みの本気度を伝えることができます。

チェックポイント!

- ☐ サプライヤーにヒアリングの目的を説明しましたか？
- ☐ ヒアリングに購買部門や事業部門は同行できていますか？
- ☐ 評価の結果をサプライヤーにフィードバックしましたか？

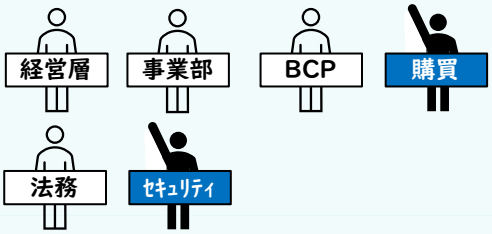
手引書該当箇所

5.2.1 セキュリティ対策の評価手法
5.2.2 セキュリティ対策状況を確認する際の注意点
5.2.3 サプライヤーへのヒアリング
5.2.4 チェックリスト・ヒアリング結果の整理・分析
5.2.5 分析結果のフィードバック

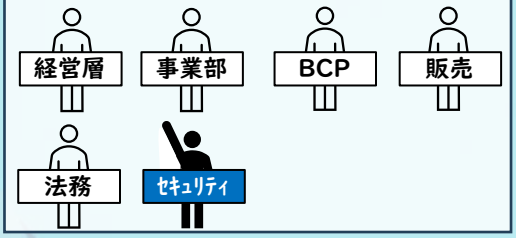
セキュリティ強化のサポート

関係者

～自社～



～サプライヤー～



解説

- サイバーセキュリティは、巧妙化・複雑化するサイバー攻撃に対応しなければならないため、一企業だけで対応することは非常に難しく、経営課題のひとつにもなっています。公的サポートを有効活用することで、自社の負荷なく、サプライヤーのセキュリティレベルを強化することができます。

- サプライチェーンセキュリティを強化するためには、サプライヤーとの連携が重要ですが、利益供与等の問題を生じない範囲でサプライヤーをサポートしましょう。

- サプライヤーからの問い合わせ窓口の設置や体制の準備といった取り組みをおこなうとよいでしょう。

チェックポイント!

- □ 支援策は利益供与に該当しないか確認が取れていますか？
- □ 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ますか？
- □ 紹介する支援策等はサプライヤーのセキュリティ成熟度に合致していますか？

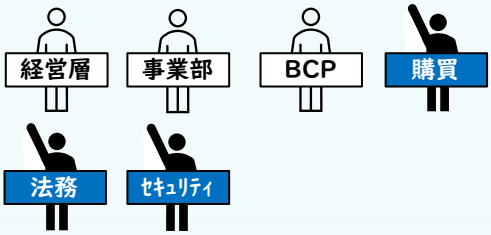
手引書該当箇所　6.1.1 公的サポートの活用
6.1.2 自社によるサポート

サプライヤーとの契約締結

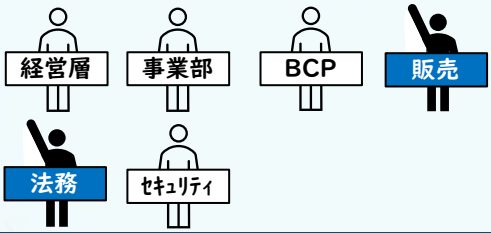
ルールの徹底・再確認

関係者

～自社～



～サプライヤー～



解説

- 継続的にサプライチェーンセキュリティを向上させるためには、法令やコンプライアンスを遵守し、サプライチェーンを構成する企業が一体となって取り組む必要があります。
- サプライヤーとの契約締結時に気を付ける法律として、主に独占禁止法と下請法があります。それ以外に業界ごとの法令なども確認し、法律違反にならないように気を付けましょう。
- 契約書にサイバーセキュリティ対策に関する項目を盛り込むときは、記載内容についてサプライヤーと事前に話し合うようにしましょう。法務部のチェックも忘れずに。

チェックポイント！

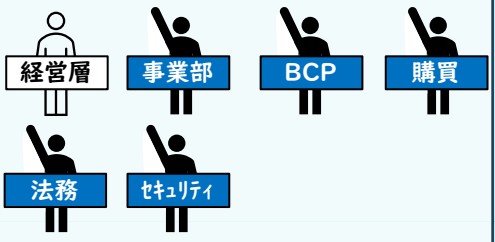
- □ サプライヤーに特定のセキュリティ製品の購入を強制したり、サイバーセキュリティ対策の有無を理由に不当な価格要求を行ったりしていませんか？
- □ 独占禁止法や下請法以外に、自社が注意すべき法令を確認しましたか？

手引書該当箇所　　6.2.1 独占禁止法および下請法の遵守
6.2.2 契約先への事前調整および契約締結

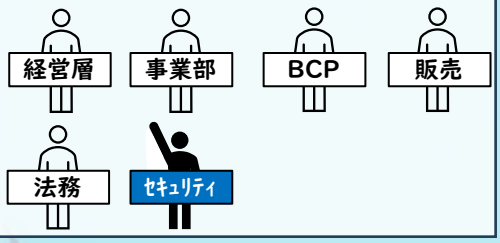
リテラシーの向上

関係者

～自社～



～サプライヤー～



解説

- サプライチェーンセキュリティは特定の担当者や部署が取り組むだけでは達成されません。
- 自社はもちろん、サプライヤーも含めてセキュリティの重要性を理解してもらい、“ジブンゴト”として落とし込んでもらうことで、サプライチェーン全体でセキュリティ強化に取り組むことができます。
- サプライチェーンのコミュニティで情報を共有しましょう。あなたの情報がどこかの会社で起きるサイバーインシデントを防ぐきっかけになるかもしれません。
- 継続的なセキュリティ教育やセキュリティ啓発コンテンツの提供を通じて、セキュリティの重要性を発信していきましょう。

チェックポイント!

- ☐ 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ますか?
- ☐ サプライヤーに対してセキュリティの重要性を発信していますか?
- ☐ サプライヤーと脆弱性情報などの共有が行える環境を整えられていますか?

手引書該当箇所

6.3.1 社内教育
6.3.2 サプライヤーへの支援
6.3.3 情報共有文化の醸成

レジリエンスの向上

事故発生時の対応準備と確認

関係者

～自社～

経営層　事業部　BCP　購買　法務　セキュリティ

～サプライヤー～

経営層　事業部　BCP　販売　法務　セキュリティ

解説

- どれだけ事前に対策しても、サイバー攻撃を完全に防ぐことはできません。「もし攻撃を受けたらどうするか」を考えておくことも大切です。
- サプライヤーがサイバー攻撃を受けた時に備えて、相談窓口を設置しておきましょう。
- 規程やマニュアルに定めていたとしても、実際にサイバー攻撃が起こった時にマニュアルに沿った対応を実行できるとは限りません。インシデント訓練を通じて、自社内やサプライヤーとの連絡ルートを確認しておきましょう。
- サイバー攻撃は、最初からサイバー攻撃かどうか判別できない場合もあります。些細なことでも早めに相談をしてもらえるように、日頃からコミュニケーションをとっておくことが大切です。

チェックポイント!

- □ 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ますか？
- □ 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ますか？
- □ 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ますか？

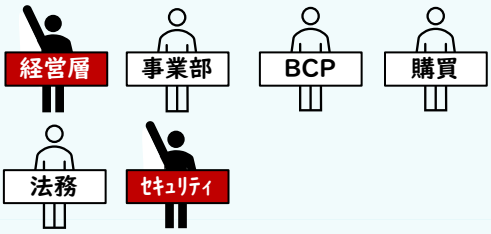
手引書該当箇所　6.4.1 インシデント訓練の実施
6.4.2 インシデント発生時のコミュニケーション

取り組みの評価と方針・計画の見直し

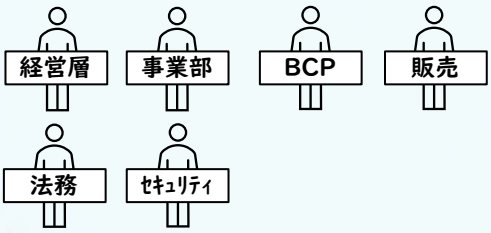
登山後の振り返りと見直し

関係者

～自社～



～サプライヤー～



解説

- サプライチェーンセキュリティの取り組みは段階的・継続的に改善をすることが重要です。
- 定期的にサプライチェーンのセキュリティ対策実施状況を評価し、今後の目標や取り組み内容に反映していくことで、さらなる改善につなげることができます。
- 評価結果・見直し後の取り組み計画ついて、経営層へ報告を行います。経営層のサプライチェーンセキュリティへの関心を高めることで、経営層が強力な味方になってくれることを期待できます。

チェックポイント!

- □ 定期的に方針や計画を見直せていますか？
- □ 取り組みの目標を実効的なものに設定できていますか？
- □ 経営層に対して定期的に進捗報告を行えていますか？

手引書該当箇所　7.1.1 取り組みの評価と方針・計画の見直し
7.1.2 経営層への報告

更新履歴

2024年 7月31日　　初版発行

実務者のためのサプライチェーンセキュリティハンドブック

初版発行　2024年7月

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）
第7期受講者　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