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

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

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。

目次

1 章　はじめに 5

1.1. 目的と対象読者 6
1.2. 本書のスコープ 7
1.3. 本書の構成 7

2 章　サプライチェーンにおけるサイバーセキュリティの重要性 9

2.1. サプライチェーンを狙ったサイバー攻撃の増加 9
2.2. サプライチェーンセキュリティインシデント事例 10
2.2.1.　ケース 1　製造業サプライヤーのランサムウェア感染による工場停止 10
2.2.2.　ケース 2　港湾システムのランサムウェア感染によるターミナル操業停止 10
2.2.3.　ケース 3　業務委託先のマルウェア感染による個人情報漏洩 11

3 章　取り組みの流れと期待される効果 13

3.1. サプライチェーンセキュリティの取り組みの流れ 13
3.2. サプライチェーンセキュリティ取り組みの期待効果 14

4 章　サプライチェーンセキュリティの取り組み準備 17

4.1. 方針・計画の策定 17
4.1.1.　基本方針の策定 17
4.1.2.　ロードマップおよび計画の策定 18
4.2. 体制の構築・整備 19
4.2.1.　理想の体制について 19
4.2.2.　体制の構築 20
4.2.3.　社内規定の整備 20

5 章　サプライチェーンの繋がりの整理と評価 25

5.1. サプライチェーンの洗い出しと整理 25
5.1.1.　サプライチェーンの洗い出し 25
5.1.2.　サプライチェーンの繋がりの整理 25
5.1.3.　事業影響度の大きいサプライチェーンの把握 26
5.2. サプライチェーンセキュリティ対策状況の評価 28
5.2.1.　セキュリティ対策の評価手法 28
5.2.2.　セキュリティ対策状況を確認する際の注意点 32

5.2.3. サプライヤーへのヒアリング 32
5.2.4. チェックリスト・ヒアリング結果の整理・分析 33
5.2.5. 分析結果のフィードバック 36
6 章 強固なサプライチェーンの構築 39
6.1. セキュリティ強化のサポート 39
6.1.1. 公的サポートの活用 39
6.1.2. 自社によるサポート 40
6.2. サプライヤーとの契約締結 42
6.2.1. 独占禁止法および下請法の遵守 42
6.2.2. 契約先への事前調整および契約締結 43
6.3. リテラシーの向上 44
6.3.1. 社内教育 44
6.3.2. サプライヤーへの支援 44
6.3.3. 情報共有文化の醸成 44
6.4. レジリエンスの向上 46
6.4.1. インシデント訓練の実施 46
6.4.2. インシデント発生時のコミュニケーション 46
7 章 計画の評価と見直し 49
7.1. 計画の評価と見直し 49
7.1.1. 取り組みの評価と方針・計画の見直し 49
7.1.2. 経営層への報告 51
8 章 まとめ 53

1 章

はじめに

1.1. 目的と対象読者
1.2. 本書の解説範囲
1.3. 本書の構成
1.4. 免責事項

1章　はじめに

近年、サプライチェーンを構成するセキュリティ対策が不十分な中小企業を攻撃対象としたサイバー攻撃の件数が近年増加している。独立行政法人情報処理推進機構（以下、IPA）が毎年発表している「情報セキュリティ 10 大脅威」においても、2019 年から 6 年連続でトップ 10 入りし、サプライチェーンセキュリティの重要性がますます増加していることがうかがえる。

一方、情報セキュリティに関するガイドラインは多数発行されているものの、サプライチェーンセキュリティに関しては、サイバーセキュリティ経営ガイドライン[1]やサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[2]、NIST CSF[3]（日本語約紹介ページ[4]）などでサイバーセキュリティの一部として語られるにすぎない。国外では、米国立標準技術研究所（National Institute of Standards and Technology 以下、NIST）より SP 800-161 rev.1[5]（Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations：システム、および組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス）としてサプライチェーンセキュリティに関する文書が発行されている。しかし、文書の解説範囲は米国政府機関が利用する情報システム、製品、およびサービスの ICT（Information and Communication Technology）サプライチェーンに対するリスクマネジメントの指針と管理策であるため、自社に適用するためには SP 800-161 rev.1 以外の関連文書についても理解を深める必要があり、初学者には学習するハードルが高い。

そこで、IPA が主管する産業サイバーセキュリティセンター[6]（Industrial Cyber Security Center of Excellence，以下、ICSCoE）で実施されている中核人材育成プログラムの 7 期生のうち、サプライチェーンセキュリティに課題や興味を持つ 5 名がサプライチェーンセキュリティに取り組む企業にヒアリングをおこない、中核人材育成プログラムで学んだことをもとに、サプライチェーンセキュリティに携わる担当者がどのように自社のサプライチェーンセキュリティを強化すべきかについての手助けになる手引書を作成した。

各社のサプライチェーンセキュリティの取り組み内容は、業界の特徴、企業の規模、既存のセキュリティ方針や事業継続計画（BCP）の内容などによって異なるが、根本的な考え方などは共通していると我々は考えている。本書では、サプライチェーンセキュリティに関する共通的な考え方や取り組みの流れについて整理をしている。自社のサプライチェーンセキュリティにこれから携わる方や、サプライチェーンセキュリティの推進に悩まれている方の手助けとなる「手引書」として本書をお読みいただき、少しでも参考になれば幸いである。

---

[1] https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

[2] https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html

[3] https://www.nist.gov/cyberframework

[4] https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/nist-csf.html

[5] https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/NIST.SP.800-161r1_JA.pdf

[6] https://www.ipa.go.jp/icscoe/index.html

1.1. 目的と対象読者

本書は、サプライチェーンセキュリティに取り組む際に意識すべき業務の流れや重要なポイントを整理することで、これからサプライチェーンセキュリティに取り組もうと考えていたり、進め方に悩んでいたりするすべてのサプライチェーンセキュリティに携わる実務者のサポートを目的とする。

主に対象とする読者は、図 1-1 に示す通り、企業のサプライチェーンセキュリティの実務者であり、サプライチェーンセキュリティを推進する業務の中核を担う担当者、およびサプライヤーと関係のある部門の担当者を想定している。一方で、サプライチェーンセキュリティは発注元の事業会社のみで完結するものでは無く、サプライチェーンを構成するすべての企業が主体的に取り組む必要があるため、ぜひ一次請以降の実務者にも参考にしていただきたい。

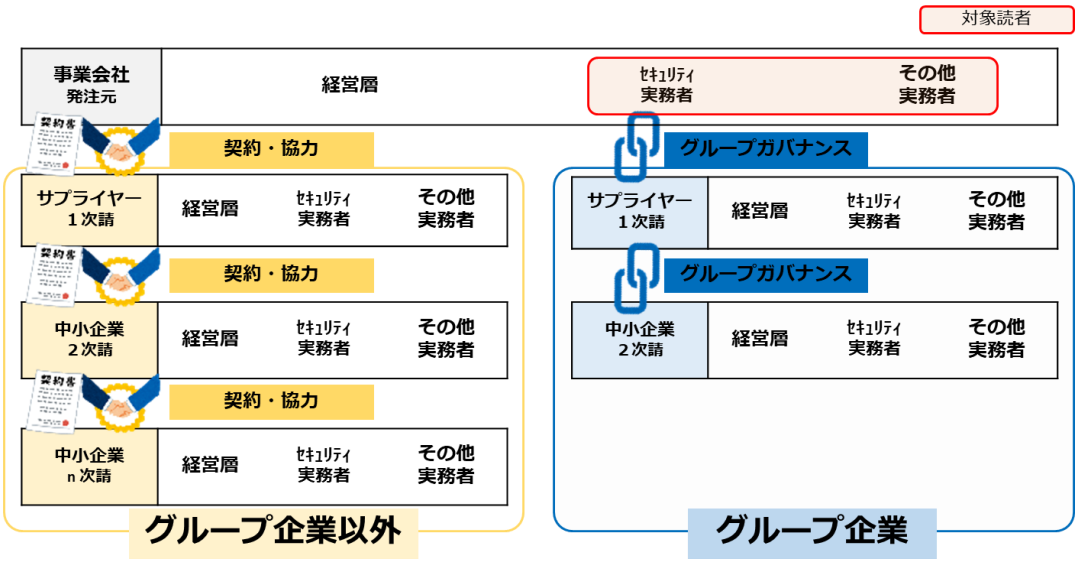


図 1-1 本書の対象読者

1.2. 本書のスコープ

サプライチェーンとは、原材料や部品などの調達、生産、配送、販売、消費までのプロセス全体を指し、商品が最終消費者に届くまでの非常に広範囲な「供給の連鎖」を指す言葉である。
サプライチェーンセキュリティとは、サプライチェーン全体のサイバーセキュリティレベルを評価し、向上をさせる取り組みである。

サプライチェーンは上流から下流まで非常に広範囲にわたるため、本書で取り扱うサプライチェーンセキュリティは、事業会社を起点として主にその上流の調達先（以下、サプライヤー）で構成されるサプライチェーンに焦点を当てている。同様に、サイバーセキュリティについても、広範囲にわたるリスクを対象とする概念であるため、本書で取り扱うリスクを材料や部品などのサプライヤーがサイバー攻撃を受けることにより供給が途絶するリスクに絞り、それらのリスクを低減するために必要な取り組みについて述べる。
なお、ソフトウェアサプライチェーン[7]（ソフトウェア開発ライフサイクルに関係する要素とその相互依存関係の総称）は本書の解説対象外としている。

1.3. 本書の構成

本書は、サプライチェーンセキュリティに初めて従事する実務者が、業務の大枠を把握し、推進できるよう、実際の業務の流れに沿った取り組み内容を記載している。あわせて、サプライチェーンセキュリティの取り組みを円滑に推進するためのアイディアを、企業のヒアリングをもとに紹介している。具体的な取り組みについて解説する 4 章から 7 章では、各節の終わりに、取り組みチェックポイントを記載しているため、節の振り返りや実務でのチェックリストとして活用いただきたい。

また、本書の 4 章から 7 章の具体的な取り組みについて、より分かりやすい形で紹介することを目指し、本書のエッセンスを紹介したガイドブック[8]を作成している。このガイドブックでは、説明内容と関係するステークホルダーや、特に押さえておきたいポイントなどを節単位でシンプルに紹介しており、登山に例えることによって初心者に読みやすい構成としている。本書の参照先も記載してあるため、ぜひご一読いただき、本書と合わせ手元において活用いただきたい。

---

[7] SOMPO CYBER SECURITY サイバーセキュリティお役立ち情報
https://www.sompocybersecurity.com/column/glossary/software-supply-chain
[8] ICSCoE 中核人材育成プログラム 卒業プロジェクト（7 期生）
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/

2 章
サプライチェーンにおける
サイバーセキュリティの重要性

2.1. サプライチェーンを狙ったサイバー攻撃の増加
2.2. サプライチェーンセキュリティインシデント事例

2章　サプライチェーンにおけるサイバーセキュリティの重要性

2.1.　サプライチェーンを狙ったサイバー攻撃の増加

近年、サプライチェーンを標的としたサイバー攻撃が増加しており、IPA が刊行している「情報セキュリティ 10 大脅威[9]」では、2019 年に初登場してから毎年上位にランクインしており 2023 年と 2024 年は 2 位に位置している（表 2-1 参照）。

表 2-1　情報セキュリティ 10 大脅威の順位変動

順位	2021 年	2022 年	2023 年	2024 年
1 位	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害	ランサムウェアによる被害
2 位	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃
3 位	テレワーク等のニューノーマルな働き方を狙った攻撃	サプライチェーンの弱点を悪用した攻撃	標的型攻撃による機密情報の窃取	内部不正による情報漏洩等の被害
4 位	サプライチェーンの弱点を悪用した攻撃	テレワーク等のニューノーマルな働き方を狙った攻撃	内部不正による情報漏洩等の被害	標的型攻撃による機密情報の窃取
5 位	ビジネスメール詐欺による金銭被害	内部不正による情報漏洩等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

サプライチェーン攻撃は大企業を標的とした攻撃者が、サプライチェーンを通じて対象企業へ社会的・経済的な損失を与えようと考え、中小企業を足掛かりに攻撃を行うものである。攻撃が増加する背景として、大企業のセキュリティ対策の成熟が進む一方で、中小企業は費用や人員の余裕が乏しいことが原因で、セキュリティ対策が不十分なままとなり、セキュリティが脆弱な箇所を攻撃者に狙われるという状況なっていることが考えられる。

[9] 情報セキュリティ 10 大脅威：https://www.ipa.go.jp/security/10threats/index.html

2.2. サプライチェーンセキュリティインシデント事例

本節では、国内で発生したサプライチェーンの弱点を標的とした攻撃事例の中から 3 点紹介する。いずれの攻撃事例においてもサプライヤーを起点としており、被害は事業会社の事業停止まで波及している例もあることに留意してほしい。

2.2.1. ケース 1　製造業サプライヤーのランサムウェア感染による工場停止

① 概要

部品製造会社のサーバー群がランサムウェア（感染後、PC のロックやファイルの暗号化により使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求するサイバー攻撃の一種）に感染し暗号化されたことで、事業が停止し部品製造ができなくなった。製造が停止したことで、取引先の事業会社へ部品の納入ができなくなり、最終製品を製造する事業会社の全工場が 1 日稼働停止した。

② 原因

部品製造会社の子会社が特定外部企業との専用通信に使用していたリモート接続機器の脆弱性を突かれ、内部ネットワークを侵害された。

③ 被害規模

工場停止に伴う推定被害金額　500 億円

2.2.2. ケース 2　港湾システムのランサムウェア感染によるターミナル操業停止

① 概要

港湾システムがランサムウェアに感染したことにより、コンテナの搬入・搬出業務に遅延が生じ、国内の物流に影響を与えた。37 隻の船舶の荷役スケジュールに影響が生じ、最大 24 時間程度の遅延が発生した。影響を受けたコンテナは約 2 万本と推計され、完全な復旧までには 3 日を要した。

② 原因

サーバー内のデータすべてがランサムウェアにより暗号化されておりログ解析が困難なため、侵入経路は断定できていないが、以下いずれかの脆弱な箇所が原因と考えられている。

1. 脆弱性対応が不十分な VPN 機器からの侵入
2. 外部記憶媒体（USB メモリ）からの持ち込み
3. 港湾システムと外部の港湾運送事業者間が連携しているネットワークからの侵入

③ 被害規模

荷役スケジュールに影響が生じた船舶　37 隻

搬入・搬出に影響があったコンテナ　　約 2 万本

2.2.3. ケース 3 業務委託先のマルウェア感染による個人情報漏洩

① 概要

IT インフラの運用・メンテナンス業務を委託していた二次請け会社がマルウェア（PC やその利用者に被害をもたらすことを目的とした悪意のあるソフトウェア）に感染したことを契機として、一次請け企業、発注元企業のシステムまで不正アクセスされた結果、発注元企業の保有する個人情報が流出した。二次請けの業務委託先では、業務端末が最初にマルウェアに感染し、さらに Active Directory サーバー（Windows Server の 1 つ。ネットワーク上の管理する資産や利用者情報、権限などを一元管理するサーバー）に侵入されたことで、管理者権限が奪取されるとともに、認証情報等も悪用された。

② 原因

一次請け、二次請けのサイバーセキュリティ対策に不備があり、外部からのマルウェア感染を許した。業務委託契約に、定期的な評価や基準遵守に関する取り決めが存在しておらず、適切な業務委託先の管理監督が実施されていなかった。

③ 被害規模

流出した情報　約 52 万件

特定者間のやり取りなど“通信の秘密”に該当する情報　2 万 2239 件

3章
取り組みの流れと
期待される効果

3.1. サプライチェーンセキュリティ取り組みの流れ
3.2. サプライチェーンセキュリティ取り組みの期待効果

3章　取り組みの流れと期待される効果

3.1.　サプライチェーンセキュリティの取り組みの流れ

本節では、サプライチェーンセキュリティの取り組みの流れと、本書での解説箇所を示す。

サプライチェーンセキュリティを向上させるためには、継続的な取組が必要であり、PDCA サイクルに当てはめて考えると理解しやすい。図 3-1　サプライチェーンセキュリティの PDCA サイクルに本書で整理したサプライチェーンセキュリティの取り組みの流れを示す。

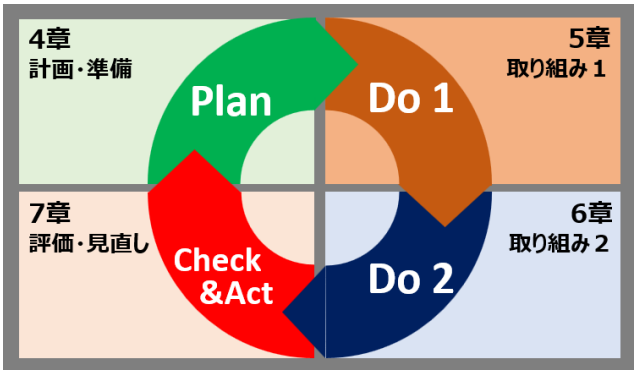


図 3-1　サプライチェーンセキュリティの PDCA サイクル

4 章では、PDCA サイクルの Plan に相当する内容を記載している。「サプライチェーンセキュリティにおける方針・計画、および体制の構築」について述べており、サプライチェーンセキュリティに取り組む際のポイントとして、強力に推進するための体制づくりや協力者として巻き込むべき部門や役職について記述している。

5 章と 6 章では、PDCA サイクルの Do に相当する内容を記載している。

5 章では、サプライチェーンの繋がりの整理と評価について述べており、自社のサプライチェーンを整理し、正しくサプライチェーンリスクを評価することについて解説している。

6 章では、強固なサプライチェーン体制の構築の手法について述べている。サプライチェーンセキュリティの取り組みはセキュリティ部門のみで完結することはできず、サプライヤーと関連の深い部門やサプライヤーとの協力が必要不可欠であることを述べており、強固なサプライチェーン体制を構築する手法はどのようなアプローチがあるかなどについて解説している。

7 章では、PDCA サイクルの Check と Act に相当する内容を記述している。評価方法、および経営層への報告方法などについて述べており、次のサイクルに向けてどのような評価手法があるか、評価結果を経営層へどのように報告すべきかについて解説している。サプライチェーンセキュリティは継続的に取り組み、改善し続けていくことが重要であるため、実現するためのポイントや実現方法について抑えていただきたい。

3.2. サプライチェーンセキュリティ取り組みの期待効果

3.1 に記載した PDCA サイクルを継続して行うことにより、サプライチェーン全体のセキュリティを向上させることが可能である。サプライチェーン全体のセキュリティが向上することにより、サプライチェーンの繋がりが強固になり、サプライチェーンの末端までセキュリティの取り組みを浸透させることができる。

一般的にサプライチェーンセキュリティに取り組んでいない企業は、サプライチェーンを“繋がり”として捉えられていない。その状態を図 3-2 サプライチェーンセキュリティ取り組み前に示す。この図では、一次請けの企業は把握しているものの二次請け以降の繋がりを意識できていない。そのため、サプライチェーンのリスクを正確に把握することができず、セキュリティ施策を行ったとしてもその効果や有効性を評価することができない。

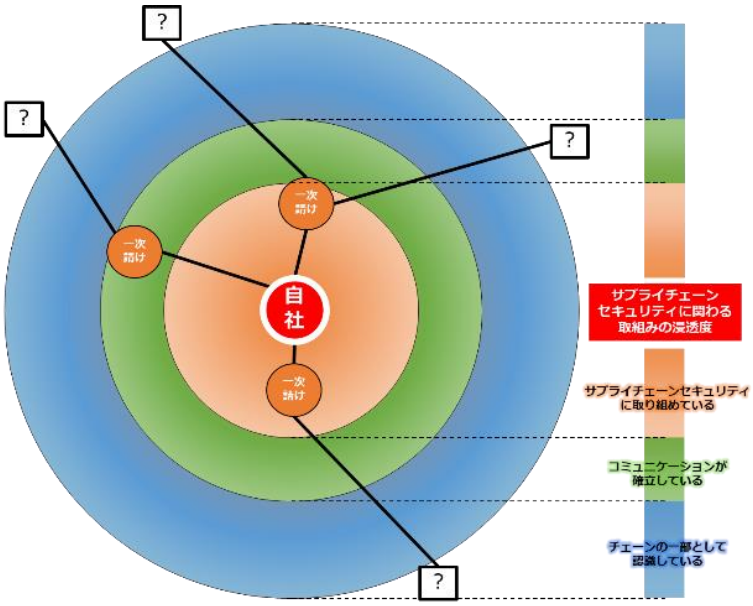


図 3-2 サプライチェーンセキュリティ取り組み前

そこで、5 章サプライチェーンの繋がりの整理と評価の内容を実践することにより、図 3-3 サプライチェーンセキュリティ取り組み後の状態へ移行することができる。今までの状態では、一次請けまでしか認識することができていなかったが、この状態では、二次請け以降のサプライヤーの繋がりも把握できている。サプライチェーンの繋がりとセキュリティ対策状況が把握できるようになることで、サプライチェーンのセキュリティ的な“急所”となる企業を知ることができ、より具体的な対策を講じることが可能となる。

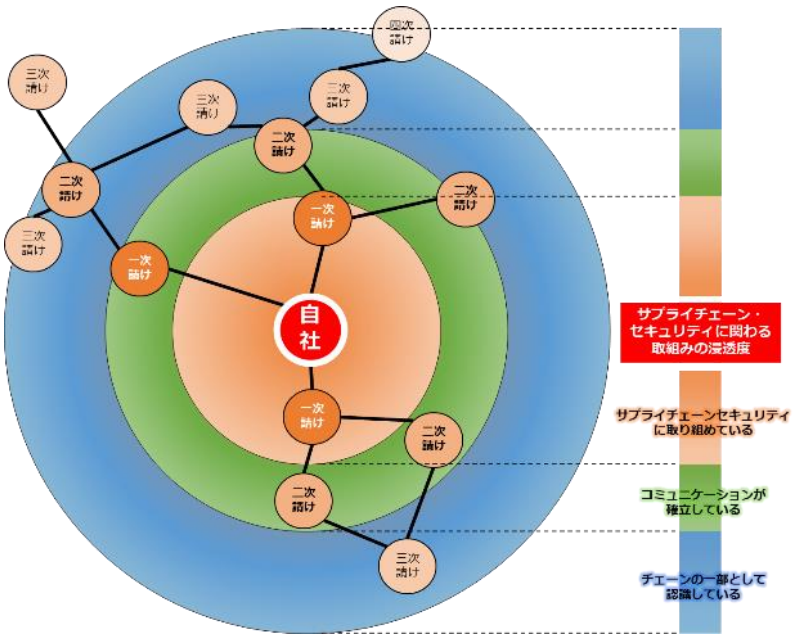


図 3-3 サプライチェーンセキュリティ取り組み後

最後に、6 章強固なサプライチェーンの構築を実践することで、図 3-4 サプライチェーンセキュリティの取り組み浸透後の状態へ移行することができる。6 章を実践する前は、サプライヤーがサプライチェーンセキュリティの取り組み浸透度を表す同心円の中心から離れた場所に位置している（図 3-3）が、実践後は、サプライチェーン全体にセキュリティの取り組みが浸透することで、各サプライヤーが自社の周辺に集まる（図 3-4）。

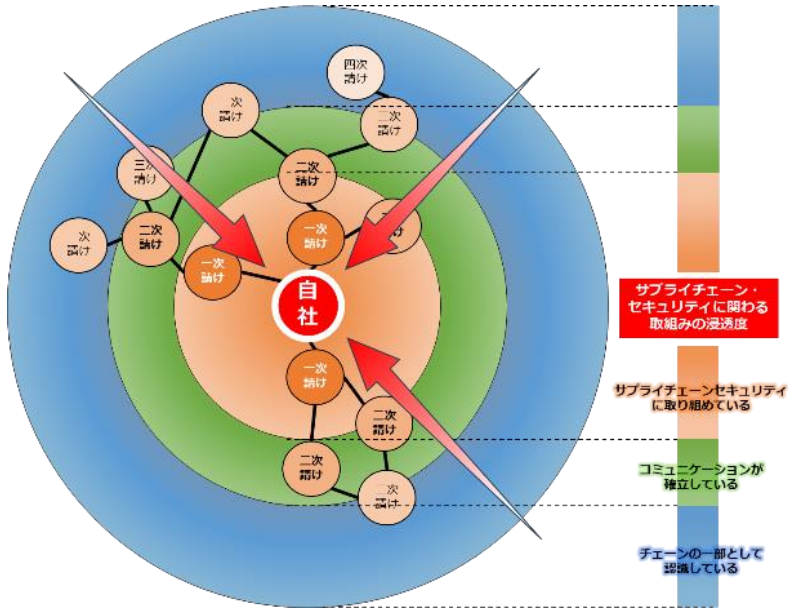


図 3-4 サプライチェーンセキュリティの取り組み浸透後

その後は、継続的にスパイラルアップの取り組みを行うことで、よりよい状態を保つことが期待される。

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
4.2. 体制の構築・整備

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

サプライチェーンセキュリティは一朝一夕で完結するものでは無く、計画から実施・運用まで数年の期間を要すると考えられる。その後も、継続的に評価・修正を行い運用することで、日々進化するサイバー攻撃の脅威からサプライチェーン全体を守ることができる。本節では、長期的な計画を策定し、実施・運用・評価・修正するために必要な基本方針やロードマップの策定について解説を行う。

4.1.1.　基本方針の策定

基本方針を定めることで、サプライチェーンセキュリティの取り組みについて一貫性を維持して推進することができる。基本方針を策定するにあたり重要なポイントは以下の 4 点である。

①　経営層にサプライチェーンセキュリティを経営リスクと認識してもらう

経営層に経営リスクとして認識してもらうことで、サプライチェーンセキュリティ関連の活動に対して投資を得やすくなる効果が見込まれる。さらに、社内で各種調整が必要になった際に心強い味方にすることができる。また、経営層の理解を得ておくことは、サプライヤーへ活動の普及をする際にもメリットがあり、自社とサプライヤーの経営層間で行われるコミュニケーションの中で、サプライチェーンセキュリティが話題に挙がることが期待できる。経営層レベルで話題が共有されることで、サプライヤーにサプライチェーンセキュリティ関連の施策について協力を求める必要が生じた場合にも、サプライヤー側の経営層まで含めた理解を得やすい。

②　サプライチェーンセキュリティの基本方針について経営層の同意を得る

サプライチェーンセキュリティの施策を推進するためには、自部署のみでなく関係部署を巻き込んで取り組む必要がある。そのためには、基本方針について経営層との間で同意を形成しておくことが重要である。それにより、自社内において一定の強制力を持って施策を迅速に展開することができる。詳細は 4.2.1 理想の体制について解説する。

③　既存のセキュリティ方針や BCP の内容と整合している

サプライチェーンセキュリティは強固なセキュリティ体制を構築するための目的の一つである。そのため、既存のセキュリティ方針に整合している必要がある。近年では、東日本大震災を契機に BCP 視点でのサプライチェーンマネジメントが重要視されている。そのサプライチェーンマネジメントの一部にサプライチェーンセキュリティが含まれているため、サプライチェーンセキュリティに取り組む際は BCP 関係部署とも密接に連携することが理想である。

④　サプライヤーに関連する部門と協力して取り組む

サプライチェーンセキュリティはサプライヤーの協力が必要不可欠である。そのため、サプライヤーと関係のある部署と連携をして一体となって取り組むことが重要である。取り組むにあたっての体制などについては、4.2 体制の構築・整備を参考にされたい。

ヒアリングをおこなった企業においては、いずれの企業も、セキュリティ部署のみでサプライチェーンセキュリティを推進することは困難であり、サプライヤーと関係のある部署との連携を、準備段階での重要な取り組みとして挙げている。

4.1.2.　ロードマップおよび計画の策定

サプライチェーンセキュリティの取り組みは短期的に実現するものではないため、ビジョンを示し、具体的な目標とロードマップを策定して、全体像を明確にすることが大切である。

全体像が明確になることで、組織がサプライチェーンセキュリティで実現したいビジョンに向かって一貫した方針で取り組むことが可能となる。また、サプライチェーンセキュリティの取り組みの進捗具合や方向性について、ロードマップに照らし合わせることで、組織が同じ尺度で状況を理解することが可能となる。

サプライチェーンセキュリティに取り組みはじめる際は、スモールスタートにすることを推奨する。スモールスタートにすることで、重要度の大きいサプライヤーや緊急度の高いセキュリティ対策について早期に着手していくことができる。また、取り組み自体の振り返りのサイクルを短くし、素早く評価をフィードバックすることもできる。一定程度取り組みを成熟させてから、対象とするサプライヤーを拡大させていくことで、サプライヤー側の負担を軽減できる可能性もある。

チェックポイント！

- □　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

サプライチェーンセキュリティのステークホルダーは社内にとどまらず、セキュリティ部門のみで運用することはできない。本節では、サプライチェーンセキュリティの取り組みにどの部門・部署と、協力して体制を構築すべきかについて、その背景と共に基本的な考え方を解説する。

4.2.1. 理想の体制について

サプライチェーンセキュリティは、自社のセキュリティ施策と異なり内部統制のような強制力を行使できないため、依頼に基づく取り組みが基本となる。このため、円滑な運用を実現するためには、サプライヤーとセキュリティ意識および目標の共有や日常のコミュニケーションを大切に扱うことが極めて重要である。つまり、サプライチェーンセキュリティの推進体制はセキュリティ関連部門に限定せず、営業部門の担当者や、購買部門の役員など、サプライチェーンに関係する部門を積極的に連携させる形が望ましい。(図 4-1)

取り組みの初期段階においては、セキュリティの専門組織を持たないサプライヤーや、費用の工面に困難が生じるサプライヤーなど、サプライチェーン全体の足並みがそろわないことが想定される。施策を円滑に推進するためには、サプライヤー側の経営層に向けて、取り組みの意義や目的を共有しておくことも有効である。このため、サプライヤーの経営層と対話可能なレベルの社員を任命できるようにしておくことも検討する。

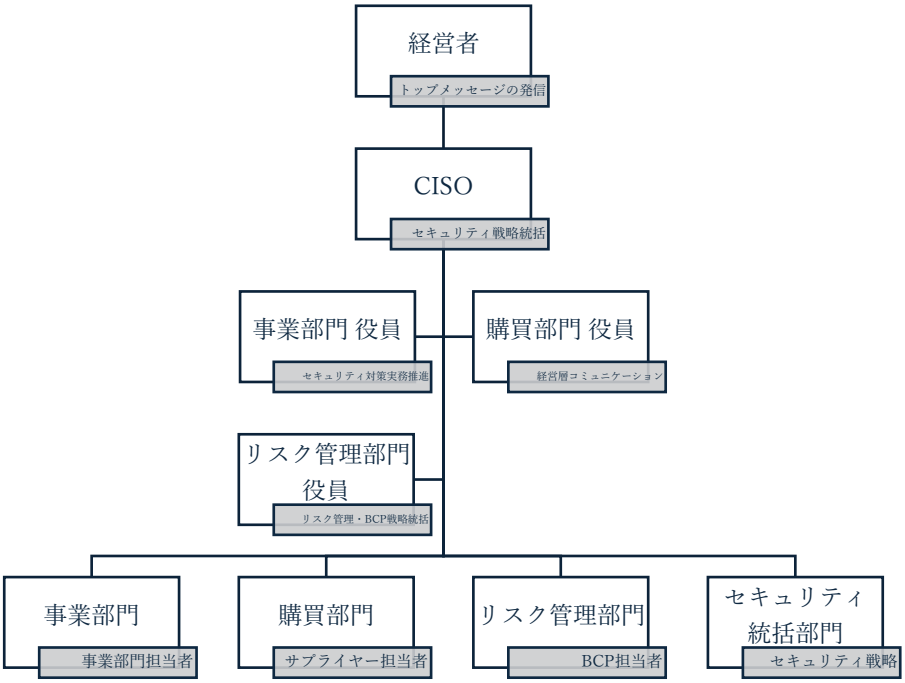


図 4-1 関係部門役員を含めた体制の例

4.2.2. 体制の構築

サプライチェーンセキュリティに取り組むための理想の体制を 4.2.1 で述べた。具体的に社内を横断した体制を構築する際には、社内規定に沿った手続きに着手するより前に、下地作りとなる社内コミュニケーションを実施しておくことが望ましい。

① トップレベルの認識共有

サプライチェーンセキュリティの取り組みでは、通常のプロジェクトと異なり、社外のステークホルダーが多く関与するため、担当者の負荷も相応となることが想定される。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などを検討し、担当役員へ伝達・共有する。役員は経営層レイヤーで組織横断的な意識共有を実施することが望ましい。

② 社内横断的意識共有

構築しようとする体制は、非セキュリティ部門の社員に積極的な関与を求めるものである。これらの部門の管理職・経営層に対し、早い段階で、サプライチェーンセキュリティの取り組みが通常のプロジェクトとは異なる性格であることを伝えておくことが重要である。よくあるプロジェクトのように、IT 部門やセキュリティ部門の指示に対し、受動的に対応する程度の関与を前提としたリソース（人的資源、物的資源、金銭的資源）計画では、体制構築段階から困難が生じると想定される。

③ 強い体制の構築

サプライチェーンセキュリティの取り組みにおいて、強い体制を整えるためには、事前に上長の理解を得ること以上に、担当者がジブンゴトとして積極的に関与し、活躍できる必要がある。具体的には、体制において各担当者がどのような役割を持つのかを明確に示し、マネジメント層の承認をもって活動できるようにする。構築した体制において各担当者が継続的に活躍し続けられるよう、適切な予算を割り当てたうえで、具体的な対策に取り組ませることも有効である。必要に応じて、事前調整された経営層からのトップダウンの指示形態を用いることもできる。

4.2.3. 社内規定の整備

サプライチェーンセキュリティの取り組みを永続化させるためには規定の整備も効果的である。この取り組みは BCP やセキュリティといった既存の管理範囲とも交差するため、既存の規定との競合などが生じないよう、所管する部門と関連する部門それぞれが新しい規程の整備に十分に関与する必要がある。

参考事例

ヒアリングを行った企業では、次の二つの工夫を行ったことで、現場への展開をスムーズに進めることができていた。

① 契約雛形の秘密保持条項の活用

実務において現状に変更を加えることは、困難が伴い、会社間の契約文書の見直しともなれば必然的にタフな仕事となることが想定される。この企業では、既存の契約雛形に記載されている秘密保持契約の条文をそのまま活用していた。

現在の情勢に照らすと標準的なサイバーセキュリティを確保することは、秘密保持契約における善管注意義務の範疇に含まれるとの視点から、この条文に記載されている内容を丁寧に運用することで、契約先にサイバーセキュリティの向上を促した。それに伴い、現場実務者が案件ごとに作成・授受する要件書や仕様書といったドキュメントに明確化することを新たにルール化した。

② 規程の適用開始時、部門別に説明会を実施

セキュリティ部門の担当者は、新たな規定やルールについて、現場担当者への説明会を部門ごとに実施し、当日出席者の疑問に対しても資料を作成して全社へ提供した。社員への意識付けにより、企業全体としての取り組みも順調に滑り出していた。

チェックポイント！

- □ 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

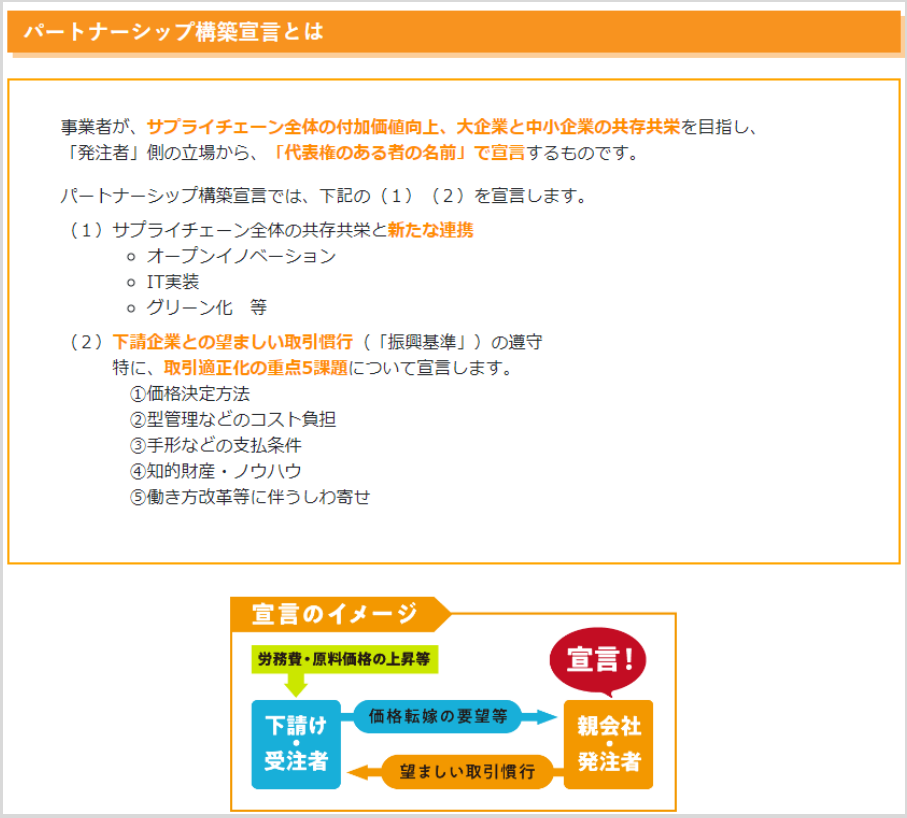
COLUMN　社外への取り組み情報の発信

サプライチェーンセキュリティの取り組み情報を社外に発信することで、サプライヤーへ取り組み内容を広く周知することができる。

本コラムでは、社外へサプライチェーンセキュリティの取り組み情報を発信する手段の１つとして、「パートナーシップ構築宣言[10]」の紹介を行う。

パートナーシップ構築宣言は、「事業者が、サプライチェーン全体の付加価値向上、大企業と中小企業の共存共栄を目指し、「発注者」側の立場から、「代表権のある者の名前」で宣言するもの」である。サプライチェーンセキュリティを強化することは、大企業と中小企業の共存共栄の根幹を強化することにつながるため、パートナーシップ構築宣言の主旨と合致する。また、代表権者の名前で宣言するため、社内におけるサプライチェーンセキュリティの施策の推進への活用や、サプライヤーへ周知する際に取り組みの本気度を示すことができ、サプライチェーン全体にセキュリティ文化を醸成するきっかけになることも期待できる。

パートナーシップ構築宣言の詳細については、パートナーシップ構築宣言を参考にされたい。



（出典）パートナーシップ構築宣言ポータルサイト

図 4-2　パートナーシップ構築宣言とは

[10] パートナーシップ構築宣言：https://www.biz-partnership.jp/

メモ

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
5.2. サプライチェーンセキュリティ対策状況の評価

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

サプライチェーンセキュリティ対策を効果的に実施するためには、自社のサプライチェーンを十分に認識したうえで具体的な対策を検討する必要がある。本節では、サプライチェーンセキュリティの取り組み対象とするサプライヤーを特定する手順を説明する。

5.1.1.　サプライチェーンの洗い出し

①　洗い出し範囲の設定

サプライヤーの範囲については運送やインフラ事業者など、直接的に自社製品・サービスの供給に関連していない事業者まで広く該当するため、あらかじめ洗い出し範囲を定める必要がある。また、各サプライチェーンの深さについても、グローバルな分業化により、サプライチェーンの源流まで把握することが事実上不可能となるため、2 次・3 次までと対象とする範囲を定めて洗い出しを行う。2 次またはそれ以降のサプライヤーについては、通常、自社で情報を保持していないため、調達部門や営業部門の担当者を通じたヒアリング等で調査したり、外部の調査分析サービスを利用したりするが、いずれも時間や費用が必要となる。そのため、以降の取組全体をイメージし、合理的な調査範囲を設定する。

②　洗い出し作業

サプライチェーンセキュリティの担当者がセキュリティ部門の所属であると想定した場合、通常はサプライヤーとの接点を持たないことが多い。4.2 でも触れたが、このようなケースにおける洗い出し作業は事業部門や調達部門の協力を仰ぎ実施するとよい。

また、企業によってはリスク管理部門などで BCP の観点からサプライチェーンの洗い出しや分析を実施し、情報を保持している可能性もあるため、これらの活用についても検討する。

さらに、日本自動車工業会（JAMA）ならびに日本自動車部品工業会（JAPIA）では、業界としてサプライチェーンセキュリティに取り組んでおり、個社で実施する洗い出しよりも強力にサプライチェーンの洗い出しを実施しているため参考にされたい。

実際の洗い出し作業にあたっては、次のような情報を取得するとよい。

・企業情報（法人番号、所属団体）、セキュリティ部門の有無、規模
・取引内容（製品・サービス、取引規模、取引頻度）、代替可能性

5.1.2.　サプライチェーンの繋がりの整理

サプライヤーの洗い出しと併せて、それぞれのサプライヤーの取引先同士のつながりを整理・可

視化する。この際、後続の 5.1.3 で行う事業影響度の大きなサプライチェーンの特定の観点である、ビジネスとしてのつながり（支払いの対価として受け取る原料やサービスなどに着目したつながり）に焦点を当てて整理を行う。

この分析において、自社を中心としたネットワークグラフに表すとサプライヤー相互の接続を可視化することができ全体像の把握に役立てることができる。

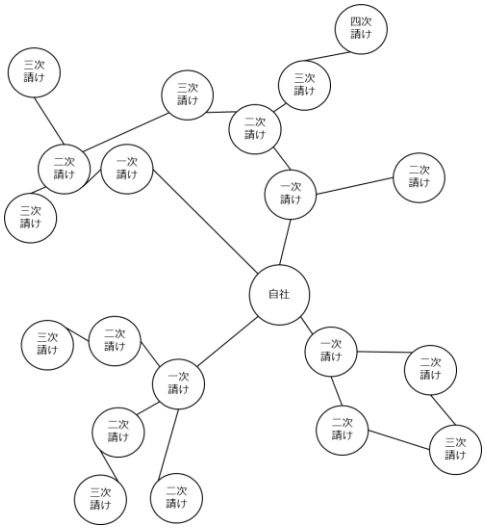


図 5-1 ネットワークグラフの例

サプライヤーごとの観点では、そのサプライヤーから供給される原料やサービスが、自社のビジネスにどのように利用されていくかという観点で供給途絶時の事業影響度を、また、その原料やサービスについて、代替製品や手段がどの程度存在するかという観点で、サプライヤーの重要度を評価することができる。これらの重要度は BCP の一部であるサプライチェーンマネジメントに取り組んでいる場合、すでに評価されていることが考えられるため関係部門と情報共有を密に行うことが重要である。

このほか、サプライチェーンの分析手法は、様々なサプライチェーンマネジメントの解説書にて説明されているため、これらを参照するとよい。

5.1.3. 事業影響度の大きい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の具体的な取り組みは、サプライヤー側での対策が中心となるが、動機付けや効率的な取り組みの支援など、自社からの支援も欠かすことができない。取り組みの実効性を高めるため、事業影響の大きいサプライヤーを特定して、対応の優先順位を決定する。事業影響度の評価は事業部門に協力を仰いで実施することが望ましい。

5.1.1 で述べた BCP 部門による事業影響度の大きいサプライヤーの特定が行われている場合は、その分析が流用できる可能性がある。ただし、影響度評価の前提がサイバーの脅威にも適用できるものであることを確認する。たとえば、大規模震災害を想定脅威とした BCP では、地理的に分散

し相互補完できる工場を持つサプライヤーは、相対的に事業影響リスクを低く評価されている可能性がある。サイバーの脅威は地理的な分散効果が期待できないため、このようなケースであれば評価を見直す必要がある。

COLUMN　－2nd Tier 問題[11]－

一般に、事業者が直接契約するサプライヤー(1stTier)に対し、いかにセキュリティ管理を行ったとしても、サプライヤーの契約するサプライヤー(2ndTier)やその上流にあるサプライヤーのセキュリティ管理は困難となる。グローバル分業が一般化した現代のサプライチェーンでは 2nd・3rdTier が海外企業であることも珍しくなく、このような企業の場合には法規制・ガイドライン・商習慣などが異なるため、国内で同様の管理を行うこと以上に困難が伴う。このように上流に遡るにつれ、セキュリティ管理は弱くなる現実があり、2ndTier 問題とも呼ばれ、問題視されている。サプライチェーン全体のセキュリティを考える場合、できるだけ上流に遡った管理を検討することが望ましい。

チェックポイント！

- □　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

[11] 出典：製造業のサイバーセキュリティ（p118）　－佐々木弘志 著(日科技連)

5.2. サプライチェーンセキュリティ対策状況の評価

5.1 でサプライチェーンの繋がりを整理し、サプライチェーンに基づいた事業影響度の評価について説明した。本節では、6 章で述べる具体的対策を実施するために必要なサプライヤーのセキュリティ対策状況の評価手法や利用方法について紹介を行う。

5.2.1. セキュリティ対策の評価手法

セキュリティ対策の評価手法については、外部監査による評価や ISMS などの認証取得状況など様々な評価手法が存在するが、本項では、サプライチェーンセキュリティに関するガイドラインやフレームワーク（表 5-1）について紹介を行う。これらを活用することで、サプライチェーンセキュリティについて理解を深めることができ、セキュリティ対策状況を評価手法の検討に大いに力になるため参考にされたい。

利用する際の注意点として、ガイドラインやフレームワークの内容をそのまま適用するのではなく、自社のセキュリティ目標に適合するよう内容を精査し、必要に応じた調整を加えることに留意されたい。

表 5-1　サプライチェーンセキュリティに関連するガイドライン、およびフレームワーク

No.	発行元	資料名/URL	概要
1	経済産業省	サイバー・フィジカル・セキュリティ対策フレームワーク https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html	セキュリティ対策の枠組み（チェックポイント）が開設されている。「添付 C　対策要件に応じたセキュリティ対策例」にセキュリティ対策要件と具体的対策例が記載された一覧表が添付されている
2	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 https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html	中小企業等におけるサイバーセキュリティ対策や、発注側企業の取引先に対するサイバーセキュリティ対策の支援・要請に関する考え方について整理されている
3	独立行政法人 情報処理推進機構	サイバーセキュリティ経営可視化ツール https://www.ipa.go.jp/security/economics/checktool.html	Excel で 40 項目の質問に答えることでサイバーセキュリティ経営ガイドライン Ver3.0 に基づいた対策状況を確認することができる
4	独立行政法人 情報処理推進機構	中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/guide/sme/about.html	情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法についてまとめられている
5	独立行政法人 情報処理推進機構	ＩＴサプライチェーンの業務委託における セキュリティインシデント及びマネジメントに 関する調査報告書 https://warp.ndl.go.jp/info:ndljp/pid/11334363/www.ipa.go.jp/files/000065162.pdf	IT サプライチェーンの委託元・委託先・再委託先・再々委託先と連鎖的に続く委託形態に注目し、インシデントや情報セキュリティ上のリスク、並びに企業における当該リスクの防止・低減のためのマネジメントに関する調査・分析内容が記載されている
6	独立行政法人 情報処理推進機構	情報セキュリティに関する サプライチェーンリスクマネジメント調査 https://warp.ndl.go.jp/info:ndljp/pid/11334363/www.ipa.go.jp/files/000058299.pdf	国企業の情報セキュリティに関する SCRM に対する認識や姿勢、取組みの実態を調査・分析すると共に、日米の先進的な活動を調査し、情報セキュリティに関する SCRM の取組み向上に資することを目的としている
7	内閣官房内閣 サイバーセキュリティセンター	重要インフラのサイバーセキュリティ部門における リスクマネジメント等手引書 https://www.nisc.go.jp/policy/group/cyber/policy.html	リスクの特定・分析・評価などリスクアセスメントの主要なプロセスの解説資料やリスクアセスメントの作業に利用可能な記入様式等が整理されている
8	内閣官房内閣 サイバーセキュリティセンター	外部委託等における情報セキュリティ上のサプライチェーンリスク対応のための仕様書策定手引書 https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf	情報システムの構築やアプリケーション開発を外部委託する場合や機器調達をする場合において、調達元となる府省庁の組織が実施すべき情報セキュリティ上のサプライチェーンリスクへの対応に係る遵守事項を定めている

9	一般社団法人 日本自動車工業会	自工会チェックリスト https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html	「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」を中核に、「NIST Cybersecurity Framework v1.1」、「ISO 27001」、「AIAG Cyber Security 3rd Party Information Security 1st Edition」、「IPA 中小企業の情報セキュリティ対策ガイドライン」をベンチマークにガイドライン、チェクリスト予備チェックリストの解説書が作成されている
10	ISO	ISO/IEC 27000 シリーズ	情報セキュリティマネジメントシステム（ISMS）に関する国際規格で、情報の機密性・完全性・可用性の 3 つをバランスよくマネジメントし、情報を有効活用するための組織の枠組みが示されている
11	NIST（National Institute of Standards and Technology） 米国立標準技術 研究所	NIST CSF （Cybersecurity Framework） https://www.nist.gov/cyberframework 日本語訳　PwC Japan 合同会社 https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/nist-csf.html	米国で主に利用されているフレームワークで、連邦政府機関から民間企業まで、サイバーセキュリティリスクを管理する用途で使用されている
12	NIST（National Institute of Standards and Technology） 米国立標準技術 研究所	NIST SP800-53rev.5 組織と情報システムのためのセキュリティおよびプライバシー管理策 https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final 日本語訳：IPA https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092657.pdf	組織の運営や資産、個人、他の組織、および国家を、敵対的な攻撃、人的エラー、自然災害、構造的欠陥、外国諜報機関、プライバシーリスクなどの多様な脅威とリスクから保護するために、情報システムおよび組織のためのセキュリティおよびプライバシー管理策が記載されている
13	NIST（National Institute of Standards and Technology） 米国立標準技術 研究所	NIST SP800-53B 組織と情報システムのための管理策ベースライン https://csrc.nist.gov/pubs/sp/800/53/b/upd1/final 日本語訳：IPA https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000092658.pdf	連邦政府組織および情報システムのための管理策ベースライン及びテーラリングガイダンスや管理策の選択プロセスをガイドし一連の実用的な前提事項が記載されている

14	NIST（National Institute of Standards and Technology） 米国立標準技術研究所	NIST SP800-161rev1 システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス https://csrc.nist.gov/pubs/sp/800/161/r1/final 日本語訳：IPA https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/NIST.SP.800-161r1_JA.pdf	サプライチェーン全体のサイバーセキュリティリスクの管理を支援するために、組織全体でリスクマネジメントプロセス及び軽減管理策の識別、アセスメント、選択、及び実装を行う方法について記載されている
15	NIST（National Institute of Standards and Technology） 米国立標準技術研究所	NIST SP800-171rev2 非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護 https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final 日本語訳： https://www.eva.aviation.jp/security/nist171/	CUI（Controlled Unclassified Information）の秘匿性を保護するための推奨セキュリティ要件を連邦政府機関に提供すること ※2024/5/14 に rev3 が正式発効
16	NIST（National Institute of Standards and Technology） 米国立標準技術研究所	NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management : Observations from Industry https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf	サイバーサプライチェーンセキュリティマネジメントを実装する際に必要な情報が PDCA サイクルになぞらえて、8 つの観点から解説されている。
17	NERC：North American Electric Reliability Corporation（北米電力信頼性評議会）	NERC CIP-013（Supply Chain Risk Management） https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf	電力事業者が順守すべきサプライチェーンリスクマネジメントに関する要件、要件遵守の証拠例となる方策が記載されている
18	米国 Department of Energy（米国エネルギー省）	ES-C2M2（Electricity Subsector - Cybersecurity Capability Maturity Model Program） https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2	米国電力企業のセキュリティマネジメントの成熟度を測定する自己評価ツール（10 ドメイン×37 目標×312 プラクティスに対して 4 段階で評価）
19	ENISA：The European Network and Information Security Agency（欧州連合サイバーセキュリティ機関）	Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity	加盟国で行われた調査結果とサプライチェーン全体にわたるサイバーセキュリティを強化するための指針を提供。サプライチェーンの各段階で発生し得るリスクを管理し、セキュリティを確保するための具体的な手法やベストプラクティスを紹介している

5.2.2. セキュリティ対策状況を確認する際の注意点

セキュリティ対策状況を確認する手法として、チェックリストによるセキュリティ対策状況の確認や、サプライヤーへのヒアリングが一般的である。いずれの手法においても、セキュリティ対策状況を確認する際に、下記の 2 点について注意すべきである。

① 対策状況を確認する目的を明確に伝える

セキュリティ対策状況を確認する目的が、「サプライチェーンのセキュリティ強化につなげるためであり、個別の企業を評価しサプライヤーに不利益を与えるようなものでは無い」と明確に伝えることで、「セキュリティの取り組みが十分でないと不利益につながるのではないか」といった不安を取り除くことができ、偽りのないセキュリティ対策の現状を知ることができる。また、管理職や経営層名での文書を添えることや、丁寧に対話することでより相手の理解を得ることができるため参考にしてもらいたい。

もし、目的を十分に伝えることができず、セキュリティ対策状況を確認する目的が企業評価のために利用されるとサプライヤーに誤認されてしまうと、セキュリティ対策が不十分な場合でも対策が完了しているなどの偽りの報告を受領する可能性がある。その結果、サプライヤー、およびサプライチェーンの評価を正しく行うことができず、サプライチェーンセキュリティ対策の評価結果と現状が乖離し、実体のないサプライチェーンセキュリティになってしまうため注意が必要である。

② セキュリティに詳しくない企業へのフォロー

中小企業ではセキュリティ専門部門を持たず、セキュリティ業務は他業務と兼務されることが多い。サプライヤーのセキュリティ成熟度を評価する際に、セキュリティ部門の有無など被評価企業の組織の成熟度を考慮しなければ、正しい評価が得られないことも想定される。そのため、相談窓口を設けたり、セキュリティ対策状況を確認する際の補足資料を追加したり、対面でヒアリングを実施しその場で疑問点などを確認し一緒にチェックリストに取り組んだりするようなフォローを提供することが望ましい。

5.2.3. サプライヤーへのヒアリング

対面でのヒアリングによるセキュリティ対策状況確認は、その場で疑問点などについて質疑応答ができるほか、会話を通じて、チェックリストやヒアリング項目にないセキュリティの悩みなどを聞き取ることもできる。ドキュメントだけでのヒアリングに比べ多くのコストを伴うものの、サプライヤーのセキュリティ対策状況の実態を把握できる点で、非常に有効なフォロー手段となる。

本項では、初期のドキュメントによる評価において、セキュリティ対策の推進に課題を抱えていることを検出した企業に対面でヒアリングを行う際のアプローチ方法について例示する。

③　パターンＡ：セキュリティ対策を推進できていない理由が不明確な企業

ヒアリングメンバーは、サプライチェーンセキュリティ担当者と日ごろからサプライヤーと関係のある購買部門や事業部門などの担当者で構成することが望ましい。サプライヤーと日ごろから関係のある部門の担当者を同行させる理由は 2 点ある。1 点目は、面識のある人が同席することで、サプライヤーとの最初のコミュニケーションのハードルが下がり、円滑にヒアリングを進めることができることである。2 点目は、自社の購買部門・事業部門担当者がサプライチェーンセキュリティの取り組みや考え方を説明する場に同席することで、副次的にセキュリティ意識向上と教育につながることである。セキュリティ知識が向上することで、サプライチェーンセキュリティの重要性を認識することができ、同行者もまた、今後のサプライチェーンセキュリティの取り組みについての良き理解者となるだろう。

④　パターンＢ：経営層がセキュリティ対策に前向きでない企業

ヒアリングメンバーは、サプライチェーンセキュリティ担当者と日ごろからサプライヤーと関係のある購買部門や事業部門などの担当者に管理職も加えた構成とすることが望ましい。サプライヤーと関連の強い部門の管理職に同席をしてもらうことで、サプライチェーンセキュリティの取り組みへの意識の高さを、サプライヤーにも伝えることができる。また、サプライヤーの上位職にも同席してもらうことで、経営目線での議論も行うことができ、サプライヤーの経営層に対してセキュリティ対策の重要性を訴求することも可能である。

ヒアリングや対話を通じて生まれる人と人との信頼関係は、サプライチェーンセキュリティを強固なものとするためにも有効である。

5.2.4.　チェックリスト・ヒアリング結果の整理・分析

チェックリストとヒアリング結果をもとに、セキュリティ対策状況の評価、および分析をすることで、サプライチェーンの脆弱な箇所や強化すべきポイントを明らかにし、優先的に対応すべきサプライヤーと対策内容を整理することが可能となる。

①　サプライヤーを分類する 2 つの要素

サプライチェーンセキュリティを推進するために重要な分類要素は、事業影響度とセキュリティ成熟度の 2 点である。事業影響度はサプライヤーが自社の事業にどの程度影響するかを表しており、サプライヤーの事業が停止した場合に自社も事業が停止するなど密接に関連する場合は、影響度を大と評価する。セキュリティ成熟度は、サプライヤーのセキュリティ施策の実施状況を表し、各種フレームワークを活用したチェックリストやヒアリング結果をもとに整理するものである。

この 2 要素で分類したグラフを図 5-2 に示す。2 要素のうち、サプライチェーンセキュリティ対策の実施により変化させることができる要素は成熟度であるため、サプライチェーンセキュリティ

施策の目的は、左側に属しているグループを右側の成熟度が高いグループに移行させることである。

一方、事業影響度を低減させるためには、調達先・委託先の冗長化などが該当するが、サプライチェーンリスクマネジメントの領域になるため、サプライチェーンセキュリティの取り組みが影響する範囲の対象外となる。ただし、事業影響度は、サプライチェーンセキュリティに関する具体的な施策を実施するうえで、施策の優先順位などを決定する重要な要素であることに注意したい。

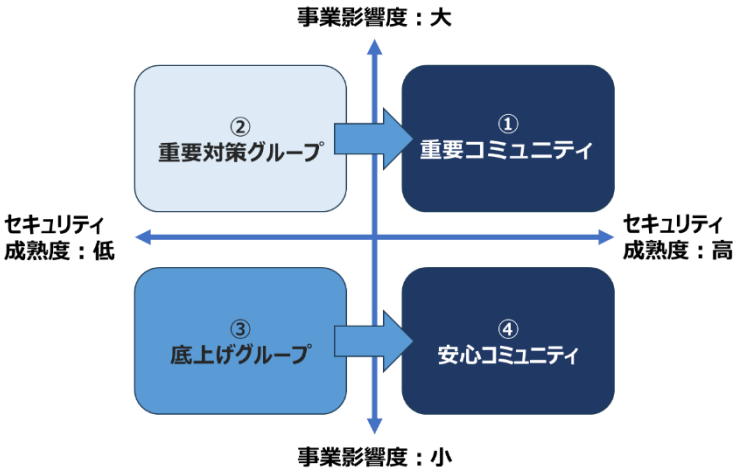


図 5-2　影響度・成熟度分類

②　セキュリティ成熟度による分類

チェックリスト・ヒアリング結果をもとにセキュリティ成熟度毎にグループ分けし、グループ毎に対応することで、効率的なサプライチェーンセキュリティ向上施策を検討することができる。

本手引書では、サプライヤーの成熟度を 3 段階に分類する方法について記載するが、分類方法はこの限りではなく、自社のセキュリティ規定や業界のガイドラインなども参考に検討されたい。

1. 自主的にサイバーセキュリティの向上に取り組めている企業

ガイドラインやフレームワークを自主的に活用しセキュリティ対応ができている企業、または自社で指定する指定する第三者認証機関の認証を取得している企業が該当する

サプライチェーン内では、セキュリティ強化の取り組みとして模範となる企業であるため、コミュニティ内に取り組み内容や知見を共有してもらうような協力を求めるとよいだろう。

2. サイバーセキュリティ対策が一部不足している企業

サイバーセキュリティの取り組みを開始しているものの、開始からの日が浅く成熟が進んでいない企業、または組織、体制、進め方など何らかの課題をかかえ、成熟が進まない

企業が該当する。

サイバーセキュリティの取り組みが開始されている企業については、各種フレームワークを活用したチェックリスト等により評価を行うことができる。個別訪問によるヒアリングやフォローの提供については、事業影響度の評価結果やアンケートによるサプライヤー側からの要望を合わせて検討するとよいだろう。

3. サイバーセキュリティの規定やセキュリティ対策が不足している企業

経営層も担当もセキュリティの重要性を認識しておらず、経営層はセキュリティをコスト源と考えているためセキュリティ対策を推進することができない企業や重要性を認識しているものの、人やコストの面からセキュリティ対策に取り組むことができない企業が該当する。

このような企業には、個別訪問によるヒアリングが効果的であると考えられる。次項に紹介する事業影響度の評価とあわせ、優先順位を定めてフォローを行うとよいだろう。

③　事業影響度による分類

事業影響度を定めることにより、各サプライヤーに優先順位をつけてサプライチェーンセキュリティ対策を実施することができ、限られたリソースで効率的な対応が可能となる。

取引先や委託先が冗長化されているなど事業影響度が低いサプライヤーの場合、必要最低限のセキュリティ対策を実施してもらうことで、リスクを許容することが可能だろう。一方、事業影響度が高いサプライヤーの場合は、自社と同等レベルの高いセキュリティレベルで対策してもらうことで、リスクを許容できる。

④　サプライヤーおよびサプライチェーンの分析

サプライチェーンにおけるセキュリティ対策状況の評価に関しては、5.2.1 に述べたように公開されているガイドラインやフレームワークを参考にして、各社で最適な形を検討するものであるが、ここでは一例としてチェックリストによる数値評価を挙げる。これは、各チェック項目の実現度に応じて、5 段階評価（1:全くできていない～5:十分できている）をつけ、最終的に企業全体の取り組みに点数をつけるものである。チェックリストの結果からセキュリティ対策状況を一律に評価し、サプライヤー全社の平均値やサプライチェーン毎の平均値などを算出することで全体の分析を行う。分析結果を基本方針や計画策定時に設定した目標値と比較することで、サプライチェーンセキュリティ対策全体の評価を行うことが可能であり、今後の具体的取り組み内容などに活用することが可能である。

また、同業種・企業規模・事業影響度別の平均値などを算出し比較することで、業種や企業規模

ごとの特徴などを知り、今後の具体的対策などにつなげることが可能である。

⑤　サプライヤー個社の分析

サプライヤー個社の分析においては、計画時に定めた目標値との評価の他に、サプライヤー全社の平均値や同業種・企業規模・事業影響度別の平均値などと比較することで、取り組み状況を相対的に評価することが可能である。この結果は、次項で述べるフィードバックに活用することで、個社の取り組みを促進することができる。

5.2.5.　分析結果のフィードバック

分析結果をサプライヤーへフィードバックすることで、サプライヤー自身のセキュリティ対策状況と発注元から求められるセキュリティ対策とのギャップなどについて知ることができ、より課題感をもってセキュリティ対策に取り組んでもらうことが期待できる。

また、フィードバックを行う際は評価結果を伝えるだけでなく、セキュリティ対策を実施するためのアプローチ方法についてのアドバイスや評価結果をもとにした今後の方針についても共有することでより効果的なフィードバックになるであろう。

分析結果のフィードバックについては、次のようにいくつかの手法が考えられる。これらを組み合わせ、効果的なフィードバックを検討してほしい。

①　ドキュメントによるフィードバック

サプライチェーン全体のセキュリティ対策状況の総括を評価レポートや小冊子の形にまとめ、郵送やメールにより、サプライチェーンを構成する各社に届ける。あわせて、サプライチェーン全体としての取り組みの方向性や、直近のインシデント事例に基づく短期的な重点施策を解説することで、より具体的な指針を提供することができる。

また、個社のセキュリティ対策状況の回答内容については合計点の偏差値一覧のような指標を示すことで、サプライヤーは、自社の取り組み内容がサプライチェーンの中にで、どの程度の成熟度にあるか自己評価できるようになる。

②　大規模な会議によるフィードバック

発注元や業界団体が主催するセキュリティの勉強会やその他サプライヤーが集まる場（工事が伴う業界などであれば安全懇談会など）でサプライチェーン全体のセキュリティ対策状況の分析結果をサプライヤーに届けることを想定している。①と同様にサプライチェーンセキュリティの取り組みの方向性や、セキュリティ対策状況の分析結果など総括的な内容を共有することで、サプライチェーン全体に同様の課題意識を共有することができる。

また、サプライチェーン内で良い取り組みをできている企業の事例を紹介したり、積極的な取り

組みができているサプライヤーを表彰したりすることで、各社のモチベーション向上に繋げることも可能である。

大規模な会議で議論の内容がサプライチェーン全体のことになると、参加者側からの個別の意見や相談は届きにくくなる。別途、個別に相談を受け付ける窓口の設置なども検討するとよい。

③　グループ毎に実施するフォローアップ

②で説明した大規模な会議と比較して、小規模なグループでのフォローアップミーティングを開催する。グループは、サプライヤーの業種や会社規模など、サイバーセキュリティの取り組み成熟度が近しい企業で構成し、発注元からのフォローアップを中心とした相談会のような形式で実施する。特にサイバーセキュリティの取り組みを開始できていない企業については、相談会よりも、勉強会に近い形となるため、本書や別紙ハンドブックも活用し、実務者に向けたセミナーとすることもできる。

さらに、同じ境遇にある企業が一堂に会すこととなるため、これら企業間に共助の仕組みが生まれることを促すため、懇親会などネットワーキングの場を用意するのもよいアイディアであろう。

④　個社毎に実施するフォローアップ

①～③で説明した内容と異なり、個社ごとの課題や問題点に注目するため、個別に訪問やオンライン会議を行う。個社ごとに実施することで、寄り添う姿勢を示すことができ、セキュリティ対策を推進するうえでの悩みやサプライチェーンセキュリティの取り組みに対する意見などを聞き取ることが可能となる。

全てのサプライヤーに対して個別のフォローアップを行うことは現実的でないため、BCP 上の重要なサプライヤーや、セキュリティ対策について特にフォローが必要なサプライヤーなど、対象を定めたうえで実施するのが良いであろう。

本項で解説する取り組みは一例であるため、上記手法を参考に、各企業の方針や業界の文化などを勘案し、効果的なフィードバックを実施されたい。

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
6.2. サプライヤーとの契約締結
6.3. リテラシーの向上
6.4. レジリエンスの向上

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

サプライヤーのセキュリティ成熟度を評価したのち、各社に目標とする成熟度へ向けたセキュリティの強化を促す。サプライヤーは自助努力によりセキュリティ強化に取り組むことになるが、5.2でも述べたとおりサプライヤー側の事情は個々に異なり、取り組みの開始段階から手厚くサポートが必要となる企業もあれば、相談レベルのサポートで十分な企業もある。ここでは、サプライヤーのセキュリティ強化に活用できる外部のサポートと、企業の実際の取り組み事例を紹介する。

6.1.1.　公的サポートの活用

資本関係のないサプライヤー企業のセキュリティ対策を支援する場合に、会社法における利益供与に抵触しないよう注意する必要がある。公的サポートは、この規則を意識することなく活用することが可能であり、第一の支援策として有効である。

経済産業省、およびIPAでは、中小企業等がサイバーセキュリティ対策を講じることを支援するため次のような施策を提供している。

1. サイバーセキュリティお助け隊サービス（IPA）[12]
2. セキュリティアクション セキュリティ対策自己宣言（IPA）[13]
3. 中小企業の情報セキュリティ対策ガイドライン（IPA）[14]
4. サプライチェーン・サイバーセキュリティ・コンソーシアム[15]

東京都産業労働局では、中小企業向けのサイバーセキュリティ対策コンテンツをより馴染みやすい形で提供する試みとして、サイバーセキュリティ対策の極意ポータルサイト[16]を展開している。外見はライトだが、元にしている情報ソースは確かなものを多く引用しており、こちらはサプライヤー自身で具体的な取り組みを進めていくための参考になるだろう。

---

[12] https://www.ipa.go.jp/security/sme/otasuketai/index.html

[13] https://www.ipa.go.jp/security/security-action/index.html

[14] https://www.ipa.go.jp/security/guide/sme/about.html

[15] https://www.ipa.go.jp/security/sc3/about/

[16] https://www.cybersecurity.metro.tokyo.lg.jp/

6.1.2. 自社によるサポート

本プロジェクトにて、サプライチェーンセキュリティの取り組みを行っている企業へヒアリングをおこなう中で、各社が法令の枠組みに収まる範囲で、それぞれ工夫してサプライヤーをサポートしていることがわかった。以下に事例を紹介する。

① 事例 1 個社訪問による寄り添いサポート

契約の必達条件でなくとも、発注元からの要望には応えたいという意識から、はじめてサイバーセキュリティの取り組みに踏み出すサプライヤー企業も存在する。

このような企業にあっては、担当者との対面でのコミュニケーションを行い、そこから得られた個社事情を踏まえた解決の糸口を提示する。どのように考え、第一歩はどのような形で進められるかといった、知見を提供することで、サプライヤーの第一歩は、自信を伴った力強いものとなるだろう。

② 事例 2 サプライチェーン内の経営層ミーティングにおける講義

サプライヤー企業に形式上のセキュリティ部門や担当者が存在するような場合では、その予算が不十分であるなど、担当者が理解しただけでは取り組みが進まないといったケースも存在する。

このような企業にあっては、経営層がサイバーセキュリティの取り組みに前向きとなることで、予算や人員の都合がつけやすくなり、実務担当者がセキュリティの取り組みに集中することができる。経営層への意識付けのため、発注元とサプライヤー企業の経営層、またはサプライヤー企業同士の経営層が定期的におこなっている会合等に参加し、サプライチェーンセキュリティの取り組みを紹介する。経営層が重要性を理解しているサプライヤーの取り組みは、速度感を伴った実効性のあるものとなるだろう。

③ 事例 3 相談窓口の常設

サプライチェーンセキュリティの取り組みは、基本的に協力依頼の形となるため、サプライヤー企業によっては、依頼のあったタイミングで全社足並みをそろえて、という具合には進まない。

企業それぞれのリソースを活用し、それぞれのスケジュールで取り組みが進められるため、サプライヤー企業における課題も通年それぞれのタイミングで発生する。ちょっとした課題であっても個社で滞留させないよう、サプライヤー企業向けの相談窓口を常設し、早期に課題を解決できるようサポートを提供する。サプライヤー企業のセキュリティ対策を淀みなく進捗させられれば、サプライチェーン全体のセキュリティレベルも持続的に改善していくだろう。

④ 事例 4 講演会の開催

セキュリティの取り組みは、企業個社がそれぞれに行う対策に留まらない。特にサプライチェー

ンは、同業であったり、取引する企業であったり自社と近しい関係の企業の集合体であるため、インシデント発生情報などは、一般に流通する情報より一段と有用な情報である。しかし、インシデントに関連した情報は機微な取り扱いを求める向きも多く、有用な情報共有を実現するためには、企業同士の信頼関係構築が必須である。

サプライチェーンを構成する企業のセキュリティ担当役員や実務者に向け、外部講師を招聘した講演会や勉強会とあわせ、会社を越えた担当者の懇親を深める機会を提供する。セキュリティ知識や目標を共有した担当者たちは、相互の信頼を構築し、情報共有の品質を高め、サプライチェーン全体のセキュリティも強固なものにしていくだろう。

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

会社間の良好なパートナーシップ関係の構築やセキュリティ文化の共有とあわせ、実務では契約でのアプローチも非常に重要である。しかし、前述のサプライヤーへの依頼に基づいた施策と異なり、法律に遵守した施策とする必要がある。本節では日本国内において特に意識すべき法律について説明するとともに契約締結時の留意点を紹介する。

6.2.1. 独占禁止法および下請法の遵守

取引先との契約締結に向けて、関連する法令について確認をおこなう。

考慮が必要な法律として①私的独占の禁止、および公正取引の確保に関する法律（独占禁止法）、②下請代金支払遅延等防止法（下請法）が挙げられる。公正取引委員会はホームページ上で「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[17]」という文書を公開しており、「昨今、サイバーセキュリティ対策の必要性が高まる中、サプライチェーン全体としてのサイバーセキュリティ対策の強化は、サイバー攻撃による被害によってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じないようにするために重要な取組であり、発注側となる事業者が、取引の相手方に対し、サイバーセキュリティ対策の実施を要請すること自体が直ちに独占禁止法上問題となるものではありません。ただし、要請の方法や内容によっては、独占禁止法上の優越的地位の濫用として問題となることもあるため、注意が必要です。」
と記載がある。具体的にどのような行為が独占禁止法や下請法に該当するかといった事例や、個別の相談先窓口が記載されているため、判断に困るときには参考されたい。

① 独占禁止法

取引先に対して、特定の製品の購入を強制することは、優越的地位の濫用と見なされる可能性がある。先ほど紹介した公正取引委員会のホームページに加えて、同じく公正取引委員会が作成された「優越的地位の濫用に関する独占禁止法上の考え方ガイドブック[18]」ではサプライチェーンセキュリティに関わらず、どのような行為が優越的地位の濫用にあたるのかが、事例を交えて解説されている。

② 下請法

取引先の事業規模によっては下請法が適用される。下請法では独占禁止法と同じく特定の製品の購入・利用の強制を行うことは禁じられているため、取引先とサプライチェーンセキュリティの取

[17] https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

[18] https://www.jftc.go.jp/houdou/panfu_files/yuuetsu.pdf

り組みをおこなう際には注意したい。

そのほか考慮する必要のある法令として、業界ごとに作成される法令等が挙げられるため、自身の業界ごとに確認してほしい。

6.2.2. 契約先への事前調整および契約締結

契約書に記載するサイバーセキュリティに関する記述について、理想的には責任範囲を明確にするために具体的なサイバーセキュリティに関する取り組み内容を記載するのが望ましい。それに加えて、業務の再委託に関する条文や秘密保持条項、事故発生時の連絡体制について定義し、契約としてセキュリティを確保していく。場合によってはサプライヤーにヒアリングをおこなう理由付けをするために、セキュリティの取り組みに対して監査をおこなう旨を条文に含める。

具体的な条文については法務部と連携し決めていく。但し、現実的には既存の契約のまま進めたり、抽象的な記載になったりすることも大いに予想されるため、その時には記載内容がどのようなことを意図しているのか取引先とすり合わせ、議事録などに残すことで問題の発生を防ぐようにする。

また、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都度記載することで、担当者の目につく頻度を上げ、意識付けを試みる。

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

自社およびサプライヤーがサプライチェーンセキュリティの重要性を意識できるようにするためには、教育や情報発信といった手段を継続的に実施していくことが求められる。本節では社内へのセキュリティ教育、サプライヤーへのセキュリティ支援、情報共有文化の醸成について取り上げ、それぞれの具体的な方法について紹介する。

6.3.1. 社内教育

サプライチェーンセキュリティは、その業務の担当者や部署だけが取り組めば達成されるようなものではない。会社としてのセキュリティを高めるためには、その会社の全従業員がサプライチェーンセキュリティの理解を深め、ジブンゴトとして取り組むことが必要不可欠である。

その手段の一つとして考えられるのがセキュリティ教育への盛り込みである。例えば、E-Learning 方式であればサプライヤーがサイバー攻撃を受けた場合の影響についての動画視聴や、理解度テストに項目として入れ込むのも一手だろう。対面形式であれば、サイバー攻撃（以下、インシデントとする）発生時のサプライヤーからの報告ルートやサポート体制について確認ができる。IPA のホームページ[19]ではサイバーセキュリティの教育資料が多数掲載されているので、教育資料の参考にするとよい。

6.3.2. サプライヤーへの支援

サプライヤーの中にはセキュリティ教育を含めたセキュリティへの投資に対して、要員や資金を割り当てる余剰がない企業もあることは認識しておくべきである。その場合は、まず 6.3.1 で述べたようなインターネットに公開されている無料の教育資料を使ってもらうのが良いだろう。また、サプライヤーに直接訪問して教育のサポートをする、教育資料を準備してサプライヤーに送付する、などの方法もある。社員全員に認識を持ってもらうことが重要なので、社員全員が受ける安全教育やコンプライアンス教育に内容を盛り込むのも有効である。

6.3.3. 情報共有文化の醸成

サプライチェーンセキュリティで重要なのは、そのサプライチェーンに属する会社間の情報連携である。ある会社で起きた不審メールの情報を同サプライチェーンの会社に共有できれば、事前に対策をしてサイバー攻撃を防ぐことができるかもしれない。反対に、その不審メールの情報を共有しなければ、知見のある会社からアドバイスも受けられず、他の会社も含めてサイバー攻撃の対象になるかもしれない。このような事態を防ぐためには日頃からの情報連携が必要である。共通の掲

---

[19] ここからセキュリティ！のうち企業組織向け教育コンテンツ
https://www.ipa.go.jp/security/kokokara/study/company.html

示板やポータルサイトがあればそこに掲載してもよいだろう。ある会社では、サプライヤーが属する組合で情報発信をし、サプライヤー同士での情報交換を促している。

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

セキュリティ対策をどれほど強化したとしても、サイバー攻撃を全く受けない、あるいは 100%防ぐということは難しい。もしサイバー攻撃を受けた場合に備え、「攻撃を受けてもいかに被害を少なくするか」「攻撃を受けたあと、いかに速やかに回復させるか」という観点が重要になる。そのためには、インシデント対応計画を関係者間で定期的に検証し、訓練することが大切である。

6.4.1. インシデント訓練の実施

サプライヤーがサイバー攻撃を受けた時に早期収束が図れるように、事前にインシデント訓練をしておくことが必要である。サプライヤーが攻撃を受けたと想定し、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などを行うとよい。

また、訓練の内容により参加者や規模が大きく異なるため、実施する訓練の目的を明確にすることが重要である。例えば、初めて訓練を実施する場合は、社内のサプライチェーン関係部署の代表者が会議室に集合して模擬連絡訓練を行うような、規模が小さく実施しやすいものから取り組むことを推奨する。以下に他社の取り組み事例と参考文献について紹介を行う。

① 事例 1 動画を用いた仮想インシデント演習（社内）

ある企業では、動画を使った演習を行っている。1 つの会議室に参加者を集め、インシデントの紹介動画を全員で視聴してインシデントの経過を把握しつつ、インシデントの状況が変化するタイミングで自分たちが取るべき対応について議論をするというものだ。この演習により、既存のインシデント対応マニュアルに沿ってただ対応するのではなく、例えば A という行動ができなかった場合はどうするか、B に連絡を取れる体制は会社の中に存在するか、など想定するパターンの幅を広げ、マニュアルの改善や体制の見直しに役立てることができる。社内のサプライチェーンに関する部門を集めて訓練するのもよいが、理想としてはサプライヤーも含めて実施するのがよい。

その他にもインシデント訓練は、関係者をすべて巻き込んだフルスケールの訓練から、規程やマニュアルの読み合わせなどの実施しやすいものまで多くの手法がある。具体的な取り組み内容やそれらの目的については、一般社団法人日本シーサート協議会でサイバー攻撃演習訓練実施マニュアル[20]が整備されているため参考にされたい。

6.4.2. インシデント発生時のコミュニケーション

サプライチェーン内でサイバー攻撃が発生した場合、速やかにその情報を入手し、封じ込めの対策を行うことが重要となる。サプライヤーが攻撃を受けた際、サプライヤーが連絡するべき報告窓

[20] https://www.nca.gr.jp/activity/pub_doc/PDF/nca-cybersecurity-exercise-manual.pdf

口の設置は必須と言える。ただ、異常を発見した時点ではサイバーインシデントかどうか判断がつかないこともあり得るので、一次請けとして日常的にサプライヤーと密接に関係がある部署が窓口になることが妥当と考えられる。報告窓口だけでなく、インシデント発生時にはどのような内容を連絡するべきなのかを一覧にしてサプライヤーに配布している企業もある。

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. 取り組みの評価と方針・計画の見直し
7.2. 経営層への報告

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はその取り組みを継続して行うことによって、サプライチェーン全体のセキュリティレベルを上げ、脆弱な状態を最小限に留めることができる。これを実現するためには、定期的に取り組みの状況を評価し、次の取り組みサイクルに反映し続けることが重要である。本節では、計画の評価、見直し、および経営層の報告について解説を行う。

7.1.1.　取り組みの評価と方針・計画の見直し

①　取り組みの評価

サプライチェーンセキュリティは、4 章から 6 章までに述べたプロセスを、単一のプロジェクトとして完結するものではなく、継続的な取り組みとしてスパイラルアップしていく必要がある。この一連の継続的な取り組みの効果を最大化するためには、定期的に見直しを行うことが重要であり、見直し根拠となる取り組みの評価方法については十分に検討する必要がある。

評価項目や方法について、表 7-1 に例示する。対象とするサプライチェーンの性格や規模によって異なる部分は適宜読みかえて利用されたい。

表 7-1　サプライチェーンセキュリティ施策評価の例

評価項目	評価観点	評価方法	見直すべき点
スケジュール	・ロードマップ通りに進んでいるか	実際のスケジュールと比較する	ロードマップとの乖離がないかを確認し、進捗に遅れがある場合、無理のないスケジュールに見直す
セキュリティ成熟度 （サプライヤー）	・計画通りに成熟度が向上しているか ・目標に無理がないか	サプライヤー各社へ自己チェックシートなどを用いた評価を依頼する	評価結果をもとに次回の目標を定める 進展がない企業については、個別フォローの計画に反映する
社内体制 （自社）	・計画時に想定した役割が機能しているか	担当者へのヒアリングやアンケート	計画通りに活動できていない場合は、阻害要因を調査し、担当管理職を通じた調整を検討する
社内規則の運用実態 （自社）	・意図通りに規程・基準が機能しているか	担当者へのヒアリングやアンケート	意図通り機能していない、または遵守が難しい規程・基準となっていた場合、規則側の見直しを検討する
関係者の理解度 （自社）	・取り組みについて、全社員の理解が定着しているか	e ラーニングと合わせ、テスト形式の効果測定を実施する	部門ごとの目標理解度を著しく達成しない部門などがあった場合は、教育計画の見直しを検討する
インシデント訓練 （自社・サプライヤー）	・インシデント対応訓練を計画通り遂行できるか ・新たな課題や問題点を抽出し解決策を整理できているか	訓練の振り返りを行い、事前に想定した手順や目標とした時間が適切だったか確認する	インシデント対応フローと次回訓練計画の改善、各担当者への教育計画を見直す

②　方針・計画の見直し

方針・計画の見直しは、サプライチェーンセキュリティの取り組み評価結果と国や業界のセキュリティに対する動向の 2 つの観点から行うことが望ましい。国や業界のセキュリティ動向をもとに基本方針を見直しつつ、サプライチェーンセキュリティの取り組み評価結果から具体的な計画や取り組み手法を見直すことになるだろう。

また、サプライチェーンセキュリティは社内外に多くのステークホルダーを有するので、方針・計画を見直す際は事前の調整が重要であることに留意しなければならない。特に対策を強化することで業務に影響が出る場合や費用が発生する場合には、関係個所への事前の調整と連絡を行い、理解を得ることが重要である。

7.1.2. 経営層への報告

サプライチェーンセキュリティの取り組みについて、施策ごとの進捗や成果を経営層に対して報告する。セキュリティの取り組みは直接的な利益といった分かりやすい指標に結びつかないため、取り組みの価値を力強く発信することが大切となる。

経営層報告の意味は大きく二つあり、一つは現在までの進捗を踏まえ、これからの計画の承認を得るための報告。もう一つは、現在までの投資に対し、十分な効果が得られていることを実感し、継続的な投資が妥当であると判断してもらうための報告である。

これら報告の目的は、いずれも未来の活動を定義していくことに直結している点で共通し、現状の成果報告にとどめず、次期以降の見通しを勘案した形で現状を報告することが望ましい。

セキュリティ投資の効果については、前述のとおり、利益以外の指標が求められるため、経営層が納得できる形で価値を発信することが大切になる。例えば、サプライチェーン全体の成熟度を点数評価し、その改善の程度を表すことが該当する。そのほか、個社別にサポートを行ったサプライヤー企業の数や、提供したサポートに対する社外からの評価や要望なども利用することができる。経営層のタイプに違いはあるものの、多くの経営層は、報告内容に対し直接的な事実だけでなく、納得と安心を得られる情報の提供を期待している。このことを理解し、報告対象の経営層の視点に立ち、必要とされる形で情報を提示することが大切である。

チェックポイント！

- □ 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

8章

まとめ

8章　まとめ

4 章～7 章では実務担当者が実施する 1 つ 1 つのタスクについてフォーカスを当て、その内容を記載してきたが、これまでにも述べてきたように、サプライチェーンセキュリティは一朝一夕で完了するものではない。巻き込む社内部署、およびサプライヤーを増やしながら、継続的に実施し、成熟度を高めていくことが必要である。そのためには、4 章～7 章で記述した取り組みと併せて、ステークホルダーとのコミュニケーションの継続も重要な要素である。

サプライチェーンセキュリティに取り組む目的を明確にし、4.1　方針・計画の策定で掲げた方針を社内外問わずステークホルダーに説明し、全員で共通認識を持っておく。さらに、取引先へ定期的にヒアリングをおこない、抱えている課題に共に取り組むことで、良好な関係を築くことができる。取引先企業が加盟する団体を設立し、そこで継続的なコミュニケーションをおこなっている業界もある。勉強会や意見交換にサプライチェーンセキュリティの話題を盛り込み、団体での意識向上を図っており、加盟企業同士での横の繋がりが生まれるという効果も生まれている。このほかにも相談窓口の開設など 6.1　セキュリティ強化のサポートで記すような、適切なサポート体制を構築することも良好な関係の構築に繋がる。

このように、自社内関係部署およびサプライヤーとの信頼関係を構築してそれを維持していくことによって、サプライチェーン全体でセキュリティレベルを底上げしていく環境が整うだろう。最終的に目指すのは、自社にもサプライヤーにも「サプライチェーンセキュリティは大事であり、全員で継続的にセキュリティレベルを高めていくことが重要だ」という“文化”を醸成することなのである。

謝辞

本書の作成にあたりまして、DMG 森精機株式会社　堀様、九州電力株式会社　岩田様、トヨタ自動車株式会社　坂様、北海道電力株式会社　村上様、マツダ株式会社　林様には、貴重なご意見や情報をご提供いただくなど、多大なるご支援・ご尽力を賜りました。お世話になりました皆様にこの場を借りて心より御礼申し上げます。

また、本卒業プロジェクトのメンターを務めていただきました、産業サイバーセキュリティセンター中核人材育成プログラムの講師であられる門林雄基先生、IPA 中山顕様には多くのご指導・ご助言を賜りました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトをともに実施した、下記メンバーの皆様にも感謝を伝えたいと思います。

プロジェクトメンバー

本書は、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中核人材育成プログラムにおける卒業プロジェクト「実務者のためのサプライチェーンセキュリティ」の成果物として作成されました。

【リーダー】
小島 啓史

【サブリーダー】
渋谷 篤

【メンバー】
桑原 大河
竹内 法彦
中角 直毅

実務者のためのサプライチェーンセキュリティ手引書

2024 年 7 月 31 日　　初版発行

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期生受講者　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