中小企業を含むサプライチェーンにおける
情報セキュリティ対策状況等の調査
－ 調査報告書 －

2022年5月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. 調査の背景・目的

近年、中小企業においても IT 化が進み、業務の効率化、サービスレベルの向上が図られている。その一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害も確認されている。また、情報セキュリティ対策が強固とはいえない中小企業を対象としたサイバー攻撃や、それに起因する大企業等の被害も顕在化してきており、大企業のみならずサプライチェーンを構成する中小企業においてもサイバー攻撃の脅威にさらされている実情が明らかになっている。

このような背景のもとで、独立行政法人情報処理推進機構（以下「IPA」という。）が事務局を務める「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（以下「SC3」という。）[1]」内の「SC3 中小企業対策強化 WG」においても、サプライチェーンを構成する中小企業におけるセキュリティ対策強化を目的に「各業界のセキュリティ対策取組共有」「発注元企業として取組むべき課題」等についての議論が開始されているところである。

そこで、「SC3 中小企業対策強化 WG」におけるこれら議論に供するとともに、今後の中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策促進に向けた施策の検討に用いることを目的として、中小企業を含むサプライチェーンを構成する各業界において、どのような情報セキュリティ対策・取組が採られており、どのような課題に直面しているのか、ヒアリング調査を通じて情報収集・分析する「中小企業を含むサプライチェーンにおける情報セキュリティ対策状況等の調査」（以下「本調査」という。）を実施した。

本調査報告書は、本調査の調査結果を取りまとめたものである。

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

2. 調査概要

業界団体等においては、中小企業を含む業界全体でのセキュリティ対策強化に向けた各種取組を実施しているところもある。これらセキュリティ対策強化に向けた各種取組内容、及び取組を行うにあたって抱えている課題等について、ヒアリング調査を行った。

2.1 概要

本調査における、調査概要は以下のとおりである。

表 2-1 調査概要

調査手法	ヒアリング調査 （リモート形式）
調査対象	SC3 会員を中心とした業界団体（及び発注元企業）
調査件数	11 業界（発注元企業:延べ 18 社）
調査時期	2021 年 10 月～2022 年 1 月

2.2 調査対象

調査対象として SC3 会員を中心に 11 分野の業界団体や ISAC[2]等の団体を選定し、ヒアリングを実施した。また、団体へのヒアリングの中で、個別の発注元企業の立場からも意見を聴取した。

調査対象の詳細は以下のとおりである。なお、調査した団体については、特定されないよう匿名化を行っている。

表 2-2 調査対象

No.	分野	対象団体数	業界構造（調査対象団体が属する業界の特性）
1	製造 A	2 団体	大企業から中堅企業、小規模企業も多く含むピラミッド構造。
2	製造 B	1 団体	大企業から中小企業、顧客や取引先が様々なフラットな構造。
3	製造 C	2 団体	大企業と中小企業が双方同程度の割合含まれる構造。
4	インフラ A	1 団体	供給元は大企業、販売を担う企業は大企業系列企業～中小企業。

[2] Information Sharing and Analysis Center の略。情報共有組織

5	インフラ B	2 団体	供給元は大企業、販売元は大企業系列企業～中小企業。
6	インフラ C	1 団体	主要供給元は大企業で約 1 割、残り 8～9 割は中小企業も多く含む。
7	防衛	1 団体	防衛装備機器メーカーは大企業、発注先には多くの中小企業を含む。
8	情報通信	1 団体	製品製造を行う発注元企業、部品等を納品する取引先企業から成るピラミッド構造。
9	金融	1 団体	銀行・生保・損保・クレジットカード等は大企業、信金や地銀等の中小規模は一部。
10	製薬	1 団体	医薬品製造業者は大企業、取引先企業には中小企業も含む。
11	運輸	1 団体	大都市圏鉄道事業者は大企業、地方には中小企業も含まれる。

調査対象は、製造業と非製造業をいずれも含み、製造業は産業向け及びコンシューマ向け製品のいずれも含む。

いずれの業界においても業界のサプライチェーン全体には中小企業が含まれるが、調査対象とした団体が直接中小企業を含む場合もあれば、団体に所属するのは発注元企業となる大企業が中心で、その取引先に中小企業を含む場合がある。

2.3 調査手法

リモート形式のヒアリング調査を 1 団体あたり 1～2 時間で実施した。

2.4 調査スケジュール

調査対象のうち、2 分野を先行してヒアリング調査を実施し、情報収集内容・収集方法・結果・考察をまとめた中間報告資料を作成した後、SC3 中小企業対策強化 WG 内タスクフォースにて報告を実施した。中間報告で得られた意見をヒアリング内容に反映し、残りの調査を実施した。

調査スケジュールの詳細は以下のとおりである。

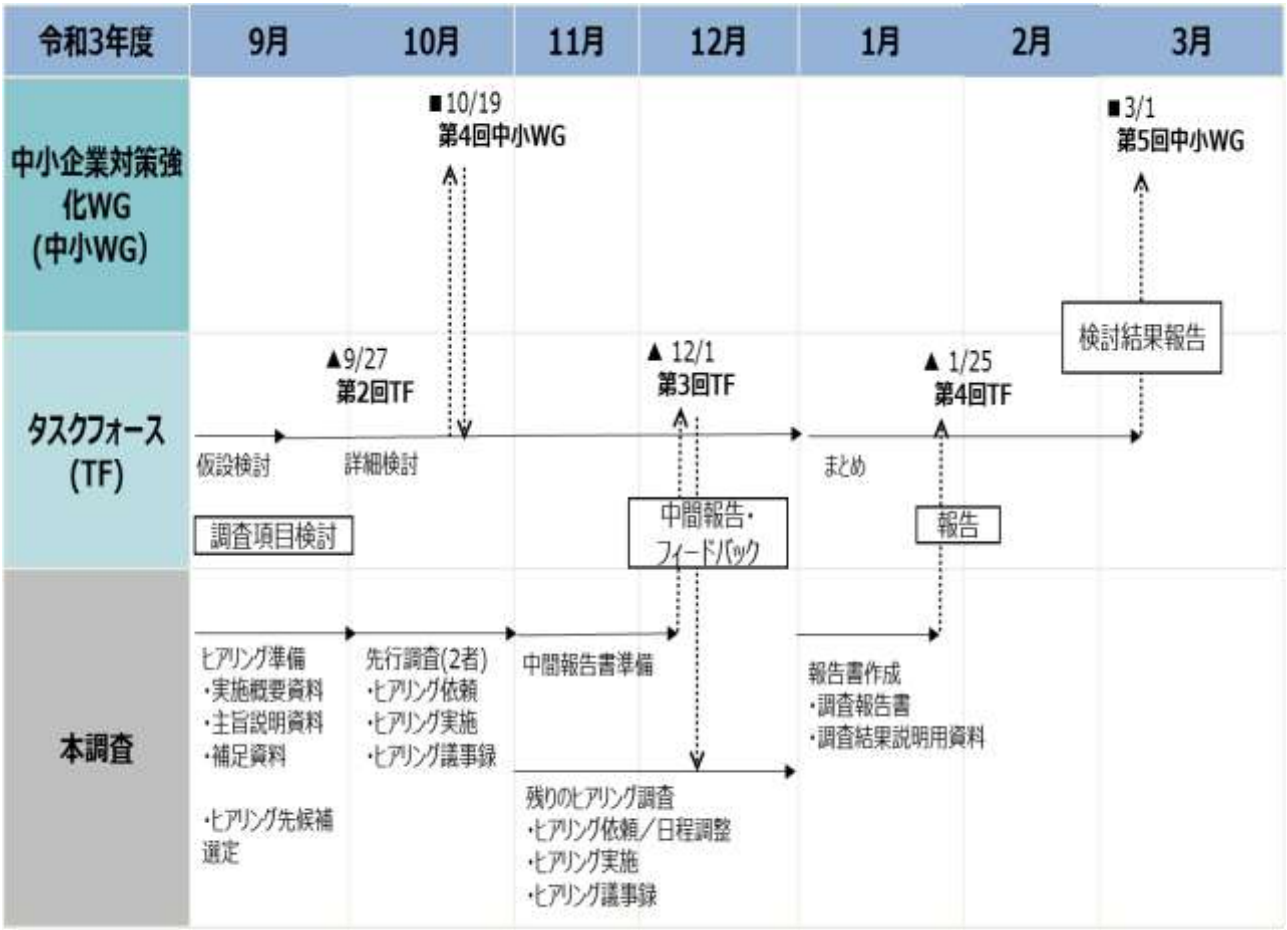

図 2-1 調査スケジュール

2.5 調査仮説

調査にあたって、以下の仮説を設定した。中小企業を含むサプライチェーンにおいて情報セキュリティ対策を推進するにあたり、これらの仮説を検証するため、各業界においてどのような情報セキュリティ対策・取組が採られており、どのような課題に直面しているのかを確認した。

表 2-3 調査仮説

No.	仮説	調査内容
1	業界におけるセキュリティ対策の必要性は認識して検討は行っているものの、参考となる情報が少ないため、セキュリティ対策の取組が進展していないのではないか。（又は、参考となる情報が多すぎてどれが良いかわからない）	各業界の情報セキュリティ対策の取組 ➢ セキュリティガイドラインの策定状況 ➢ インシデント発生時の報告 ➢ 情報セキュリティ対策強化に向けた取組 ➢ 業界横断的に情報共有が望まれる内容 ➢ 抱えている課題
2	取引先中小企業に「セキュリティ対策」を要請したいが自社に明確なセキュリティ選定基準（セキュリティ要件）がないため、要請できないのではないか。	➢ 取引先選定におけるセキュリティに関する選定基準（セキュリティ要件）の有無、またその内容 ➢ 取引先選定にて抱えている課題の有無、またその内容
3	セキュリティ条項の必要性が理解できていないため、契約書に「セキュリティ条項」がないのではないか。	➢ 契約書のセキュリティ条項の記載の有無・またその内容 ➢ 契約に関して抱えている課題の有無、またその内容
4	把握方法が分からないため、取引先の情報セキュリティ対策の実施状況の把握を行っていないのではないか。	➢ 情報セキュリティ対策の実施状況把握のための取組の有無、またその内容、 ➢ 上記取組を行うにあたって抱えている課題の有無、またその内容
5	委託管理のためのガイドラインがないため、再委託の状況を把握できていないのではないか。	➢ 委託管理のためのガイドライン等の有無 ➢ 上記取組を行うにあたって抱えている課題の有無、またその内容 ➢ 再委託管理の取組の有無・内容
6	SECURITY ACTION 制度[3]（一つ星、二つ星）は実施状況の確認を求めていないため、入札条件や取引先選定基準として活用されていないのではないか。	➢ 取引入札条件の活用の可能性

[3] https://www.ipa.go.jp/security/security-action/

2.6 調査項目

調査仮説に基づき、以下のとおり調査項目を設定した。

表 2-4 調査項目

No.	調査項目
1. 回答者（業界）属性	
1.1	属性
2. 各業界の情報セキュリティ対策の取組と問題意識	
2.1	– 各業界における情報セキュリティガイドライン（情報セキュリティに関する基本ルール）の有無、またその内容、参考とした基準、ガイドライン、フレームワーク等
2.2	– 各業界における情報セキュリティ対策強化に向けた取組の有無、またその内容
2.3	– 事故（インシデント）が発生した場合の各業界における報告等の有無、インシデント対応規程の有無、またその内容
2.4	– 業界横断的に情報共有が望まれる内容、及び方法
3. 発注元企業の抱える問題意識	
3.1	– 発注元企業の情報セキュリティ対策の取組
3.2	– 取引先選定に関する問題意識
3.3	– 契約締結に関する問題意識
3.4	– セキュリティ対策の実施状況の把握に関する問題意識
3.5	– 再委託に関する問題意識
4. 既存の取組・制度の認知度、活用意向	
4.1	– 既存の取組・制度の認知度、活用可能性

調査項目について、団体と発注元企業に分けてヒアリング項目を設定した。

具体的な内容を以下に示す。

表 2-5 調査項目の詳細

No.	調査項目	調査対象	ヒアリング項目
1.回答者（業界）属性			
1.1	属性	団体	① 業界の市場規模、団体の所属企業数・各社規模、業界におけるサプライチェーンの構造 等
2.各業界の情報セキュリティ対策の取組と問題意識			
2.1	各業界における情報セキュリティガイドライン（情報セキュリティに関する基本ルール）の有無、またその内容、参考とした基準、ガイドライン、フレームワーク等	団体	① 業界における情報セキュリティガイドライン（情報セキュリティに関する基本ルール）等の有無、またその内容 ② 有り、検討中の場合 ➢ 情報セキュリティガイドラインを策定において直面した・抱えている課題の有無、またその内容 ➢ 情報セキュリティガイドラインを策定するにあたり、参考とした基準、ガイドライン、フレームワーク等の有無
		発注元企業	① 発注元企業が把握している情報セキュリティガイドライン（情報セキュリティに関する基本ルール）等の有無、またその内容 ② 有りの場合 ➢ 情報セキュリティガイドラインの中身の充足度 ➢ 取引先の情報セキュリティ対策状況レベルの認識 ➢ 抱えている課題の有無、またその内容
2.2	各業界における情報セキュリティ対策強化に向けた取組の有無、またその内容	団体	① 業界における情報セキュリティ対策強化に向けた取組の有無、またその内容 ② 業界におけるサプライチェーンのセキュリティ確保に向けた取組の有無、またその内容 ③ 取組において直面した・抱えている課題の有無、またその内容
		発注元企業	① 発注元企業における情報セキュリティ対策強化に向けた取組の有無、またその内容 ② 取組において直面した・抱えている課題の有無、またその内容 ③ 取引先企業の情報セキュリティ対策状況の把握、対策状況のレベルの認識
2.3	事故（インシデント）が発生した場合の各業界における報告等の有無、インシデント対応規程の有無、またその内容	団体	① 事故（インシデント）が発生した場合の報告等の有無 ② 事故（インシデント）が発生した場合の対応規程（対応手順、チェックリスト等）の有無、またその内容（「情報の共有、報告、公表」の観点等） ③ ①②共に無しの場合 ➢ 事故（インシデント）が発生した場合、どのような対応を行うことを想定しているか（監督官庁への報告等）
		発注元企業	① 事故（インシデント）が発生した場合の報告等の有無 ② 事故（インシデント）が発生した場合の対応規程（対応手順、チェックリスト等）の有無、またその内容（「情報の共有、報告、公表」の観点等） ③ 取引先企業側でのインシデント発生時の取組状況 ④ 上記取組状況に対する評価（十分、適切、不十分） ⑤ 取組において直面した・抱えている課題の有無、またその内容

2.4	業界横断的に情報共有が望まれる内容、及び方法	団体	① 業界における各種取組の中で、他業界においても参考となり得るなど業界横断的に情報共有が望まれる取組、方法の有無、またその内容 ② 同業他社の事例や業界としての対策レベルの紹介等、業界における情報共有の取組の有無
		発注元企業	① 業界横断的に情報共有が望まれる取組、方法の有無、またその内容 ② 情報共有における課題の有無、またその内容
3.発注元企業の抱える問題意識			
3.1	発注元企業の情報セキュリティ対策の取組	発注元企業	① 取引先企業に求める情報セキュリティ対策 ② インシデント対応 ③ 業界横断的に情報共有が望まれる内容
3.2	取引先選定に関する問題意識	発注元企業	① 取引先企業に対して、秘密保持契約（NDA[4]）締結以外で要求している情報セキュリティ対策の有無、またその内容 ② （情報セキュリティ対策を要請していない場合）要請していない理由 ③ 情報セキュリティ対策に関する選定基準（セキュリティ要件）の有無、またその内容 ④ 取引先選定において抱えている課題の有無、またその内容
3.3	契約締結に関する問題意識	発注元企業	① 契約書へのセキュリティ条項記載の有無 ② 無しの場合 ➢ セキュリティ条項を記載しない理由 ➢ 契約書において抱えている課題の有無、またその内容 ③ 契約において抱えている課題の有無、またその内容
3.4	情報セキュリティ対策の実施状況の把握に関する問題意識	発注元企業	① 取引先企業に対して、情報セキュリティ対策の実施状況の把握の有無 ② 有りの場合 ➢ 実施状況把握のための取組 ➢ 上記取組を行うにあたって抱えている課題の有無、またその内容（解決した課題も含む） ③ 無しの場合 ➢ 実施状況を把握しない、把握できない理由（リソース不足、対策状況を確認しきれないなど） ➢ 実施状況を把握できていないことで抱えている課題の有無、またその内容
3.5	再委託に関する問題意識	発注元企業	① 再委託の状況把握の有無（委託先中小企業が再委託されているか、その頻度・割合） ② （再委託されている場合）機密情報の受け渡しの有無 ③ 委託先管理のためのガイドラインの有無 ④ 無しの場合 ➢ 再委託先の情報を把握できていないなど再委託に関する課題の有無、またその内容 ⑤ 再委託管理の取組の有無とその内容 ➢ 再委託管理を行うにあたって抱える課題の有無、またその内容（解決した課題も含む）

[4] Non-Disclosure Agreement の略。取引や交渉に際して相手方から一般に公開されていない秘密の情報を入手した場合、それを公開したり第三者に渡したりしないことを求める契約（秘密保持契約）

4.既存の取組・制度の認知度、活用意向			
4.1	既存の取組・制度の認知度、活用可能性	団体	① SECURITY ACTION の業界としての活用可能性、実現に向けた課題 ② サイバーセキュリティお助け隊サービス[5]の業界としての活用可能性、実現に向けた課題
		発注元企業	① SECURITY ACTION 制度の認知度 ② 中小企業の SECURITY ACTION 制度に対する評価（十分、普通、不十分） ③ 今後期待する SECURITY ACTION 制度の役割、取引先選定への活用可能性（取引先中小企業のセキュリティ対策の可視化、取引先選定基準、専門家による確認、実現に向けた課題など） ④ 自己宣言である SECURITY ACTION の信頼性を高めるための対策 ⑤ サイバーセキュリティお助け隊サービスの認知度 ⑥ 中小企業のサイバーセキュリティお助け隊サービスに対する評価（十分、適切、不十分） ⑦ 今後サイバーセキュリティお助け隊サービスに求める役割、取引先設定への活用可能性（取引先中小企業のインシデント対応可否の確認、実現に向けた課題など）

[5] https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/

3. 調査結果

調査結果について、「各業界の情報セキュリティ対策の取組と問題意識」「発注元企業の抱える問題意識」「既存の取組・制度の認知度、活用意向」として整理した。

3.1 各業界のセキュリティ対策の取組状況と問題意識

各業界のセキュリティ対策の取組状況と問題意識について、業界団体や ISAC 等の団体にヒアリングした内容を「情報セキュリティガイドラインの策定状況と情報セキュリティ対策強化に向けた取組」「インシデント対応」「業界横断的に情報共有が望まれる内容」「業界が抱えている課題」に分けて整理した。

3.1.1 業界別ガイドラインの策定状況

情報セキュリティガイドラインの策定状況として、以下のヒアリング項目を確認した。

① 業界における情報セキュリティガイドライン（情報セキュリティに関する基本ルール）等の有無、またその内容

② 業界における情報セキュリティガイドラインが有り、検討中の場合

- 情報セキュリティガイドラインを策定において直面した・抱えている課題の有無、またその内容
- 情報セキュリティガイドラインを策定するにあたり、参考とした基準、ガイドライン、フレームワーク等の有無

③ 取組において直面した・抱えている課題の有無、またその内容

ヒアリングの結果、業界としてのセキュリティガイドラインを策定している・策定されているのは 8 分野であった。うち、法律等に基づいて策定されたガイドラインは 5 分野（インフラ A、B、C、防衛、運輸）、業界での自主活用を目的としたガイドライン（自分野で製造する製品のセキュリティに関するガイドライン等）は 3 分野（製造 A、金融、製造 C）で策定していた。

政府が定める重要インフラ分野においては、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」において、情報セキュリティ対策の項目及び水準を明示する文書類を「安全基準等」として定めることとなっており、今回の調査対象においても、重要インフラ分野においては全て業界としてのセキュリティガイドラインを策定していた。

また、団体としてサプライチェーンを構成する企業のセキュリティ現状把握の取組を開始している事例が 1 分野（製造 A）見られた。

取組において直面した・抱えている課題として以下が挙げられた。

- 業界スタンダードやガイドライン等のドキュメントの多くは、概要のみで、具体的な対応内容が記載されていない。具体的な対応内容については、団体内で議論したり、会員企業情報を共有したりして定めていく必要がある。
- 企業の実態を把握した上で、業界統一的なガイドラインを策定するのが難しい。
- 業界として統一的なセキュリティ基準となるガイドラインを策定したいが、参考とすべきガイドラインが複数あり、どれを参考にすべきかわからない、ガイドラインを乱立させるとどれに準拠してよいのかわからない。
- 取引先への働きかけには調達部門の協力が不可欠だが、多くの会社では調達部門との調整が困難。
- 業界別ガイドライン普及の前提として、そもそも各企業がネットワーク上でどこまで接続されているか、といった実態の把握ができていない。

表 3-1 業界別ガイドラインの策定状況

No.	分野	ヒアリング結果
1	製造 A	・ 業界として、セキュリティガイドラインを策定している。 ・ 策定にあたっては、CPSF[6]をベースに、NIST[7] SP800[8]や ISO/IEC 27002[9]などの規格や IPA 発行の「5 分でできる！情報セキュリティ自社診断」を参考とした。 ・ 業界内のサプライチェーンに属するすべての会社に策定したガイドラインを適用すべくセルフチェックの実施と結果集約を行っている。1 次サプライヤーの状況は把握しているが、6～7 次サプライヤーとなると状況がわからない。結果を受けて今後検討する。 - 課題は、上記セルフチェックの実施の取組において調達部門との調整が難しい点である。
2	製造 B	・ 業界団体として求める対策は特に無く、各企業でセキュリティ対策を進めている。 ・ 業界のセキュリティガイドラインは無く、各企業でガイドラインを策定している。 ・ 課題は、そもそも各企業がネットワーク上でどこまで接続されているか、といった実態の把握ができていない点である。

[6] CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）：経済産業省が 2019 年 4 月に策定した様々な産業に求められるセキュリティ対策の全体像をまとめたフレームワーク

[7] National Institute of Standards and Technology（米国国立標準技術研究所）の略。

[8] 米国政府機関が定めたセキュリティ基準を示すガイドライン。米国の国防省省と取引する際に準拠が求められるセキュリティ基準。

[9] 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）の要求事項を定めた国際規格群。

3	製造 C	・ 業界にて、制御システムのセキュリティガイドラインや運用ガイドライン、及び副読本としての役割となる機器の現場導入の際のガイドラインを策定している。 ・ ガイドライン策定時の課題は、知識が業界団体として集約できていなかった点である。 ・ 現在は、IEC 62443 を見据え、ガイドラインの改訂する作業を進めている。ガイドラインと IEC 62443 の間で矛盾があると業界に混乱を与えるので、要件のマッチングを進めている。
4	インフラ A	・ 政府の「安全基準等策定指針」を参照して、業界としてガイドラインを策定している。現在、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」の改定が検討されており、改定後に「策定指針」の動向を踏まえて業界のガイドラインも見直すこととなる。 ・ 企業の実態を把握した上で業界統一的なガイドラインを策定するのが難しいことが課題。 ・ ガイドラインにセキュリティ対策について詳細に記載することはリスクになり、また、各社で既に取組んでいる事項もあることから、外部の要請や期待とガイドラインの内容をどのようにすり合わせていくかが難しい。
5	インフラ B	・ 業界では、制御システムや関連システムのセキュリティガイドラインが策定されており、法律で遵守が求められている。法令に紐付かない個別分野のセキュリティガイドラインも策定している。（a 団体） ・ ガイドラインの策定メンバーに業界団体及び主要企業も含まれていたため、法律や社会情勢を踏まえ、ガイドラインへの記載や解釈の合意を図りながら策定した。（a 団体） ・ ガイドライン策定にあたり参考にしたのは、ISO/IEC27000 シリーズなどである。 ・ ISAC では、所管省庁へのインシデント報告、会員間の情報共有のためのガイドラインが策定されている。どのレベルに至ったら報告が必要かなど事業法の事故報告規則、NISC[10]の重要インフラ行動計画、所管省庁からの個別分野への通知文などを元に整備している。事業法ではサービスレベルへの影響が判断軸となるが、NISC の枠組みでは社会への影響度合いも判断軸となる。（b 団体）
6	インフラ C	・ 事業法では、事業者に対して、保安規程を策定するよう義務付けており、サイバーセキュリティについても含めるよう求めている。各事業者は、自社が策定した保安規程に基づき、自主的にセキュリティ対策を実施している。 ・ 業界団体としては、事業者が保安規程に基づき対策を進める参考となるよう、対策の参考例と解説を作成し、会員企業にのみ公開している。
7	防衛	・ 所管省庁が策定している情報セキュリティ基準が、業界におけるセキュリティのガイドラインとなる。発注元となる企業は、本ガイドラインを遵守している。 ・ 本ガイドラインは、2021 度内に改訂される予定である。新しいガイドラインでは、取引において外部に出す情報の保護までが対象となる。NIST SP 800-171 に基づいている。

[10] National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンター

8	情報通信	・ 業界における企業向けの統一的なセキュリティ対策基準となるガイドラインは無く、基本的には、各企業単位でセキュリティ対策に取組まれており、企業独自のガイドラインがある場合がある。 ・ 取引先企業によっては複数の発注元企業から受託することもあり、発注元企業ごとにガイドラインが異なると遵守することが負荷になる可能性もあり、業界として統一的な基準を定めることは意味がある。 ・ 機器として有するセキュリティ要件は国際基準やフレームワーク等が様々あり、どれを参考にすべきかわからない、ガイドラインを乱立させるとどれに準拠してよいのかわからなくなるという意見もあり、ガイドライン策定に対しては慎重な姿勢を取っている。
9	金融	・ 業界として作成しているガイドラインはいくつかあり、会員向けに公開している。例えば、インシデント対応マニュアルは、インシデント発生時の対応をまとめたものであり、BCP[11]、SLA[12]、委託先を含む関係者との連絡体制、訓練・演習、ユーザ対応、所管省庁への報告等を整理している。 ・ ガイドラインは他業界でも活用できる可能性はあるものの、業界特有の規制やシステムの特性の中で多くの実施項目があるため、そのまま活用するのは難しいと思われる。 ・ 所管省庁の指針以外には、NIST サイバーセキュリティ対策フレームワーク、FFIEC CAT[13]、FISC[14]ガイドライン等を参照している。 ・ 課題は、業界スタンダードやガイドライン等のドキュメントは概要のみで、具体的な内容が記載されていない点である。そのため、具体的な対応は、業界団体で議論したり、金融機関同士で情報共有したりして、定めていくことになる。
10	製薬	・ 業界には統一的なガイドラインは存在しない。
11	運輸	・ 業界には、国土交通省が公表しているガイドラインがある。各企業はこのガイドラインや NISC のドキュメント等を踏まえて、自社のガイドラインを作成している。

[11] Business Continuity Plan の略。事業継続計画

[12] Service Level Agreement の略。サービスを提供する事業者が契約者に対し、どの程度のサービス品質を保証するかを提示したもの

[13] Federal Financial Institutions Examination Council Cybersecurity Assessment Tool の略。米国連邦金融機関検査協議会が公表したサイバーセキュリティアセスメントツール

[14] The Center for Financial Industry Information Systems の略。公益財団法人金融情報システムセンター

3.1.2 情報セキュリティ対策強化に向けた取組状況

情報セキュリティ対策強化に向けた取組状況として、以下のヒアリング項目を確認した。

① 業界における情報セキュリティ対策強化に向けた取組の有無、またその内容

② 業界におけるサプライチェーンのセキュリティ確保に向けた取組の有無、またその内容

③ 取組において直面した・抱えている課題の有無、またその内容

ヒアリングの結果、情報セキュリティ対策強化に向けた取組として、セキュリティ対策推進に資するコンテンツの作成、セキュリティ対策強化に向けた訓練の実施、勉強会の開催などの取組を実施されていた。

取組において直面した・抱えている課題として以下が挙げられた。

- 企業によって、セキュリティ対策への温度感や費やせるリソースが異なる点が、対策を進めていく上での課題。
- 中小企業においては、対策の必要性を認識していながらも体制や費用面で実施できない場合と、そもそもセキュリティ対策の必要性に関する認識が低い場合があり、どのようにして、中小企業にセキュリティ対策を促すかは課題。
- クラウド利用時にクラウドそのものが障害を起こして複数の機関が同時にダウンする（集中化リスク）は課題となっている。
- 調達したハードウェアにマルウェアが埋め込まれるリスクは、今後議論する必要がある。
  （米国では、新品で調達したハードウェア機器にマルウェアが埋め込まれている事案が発生した。日本でも同様のリスクは認識されているが、事案として発生していないこともあり、議論はまだ進んでいない。）

表 3-2 情報セキュリティ対策強化に向けた取組状況（業界別）

No.	分野	ヒアリング結果
1	製造 A	・ サプライチェーンにおけるセキュリティ対策状況を把握するために、セルフチェック結果を収集・集計している段階である。 ・ セキュリティガイドラインを軸にしながら、どうすれば○となるのか、各社のセキュリティ対策に関する取組を推進する活動をしていきたい。 ・ 2 次以降のサプライヤーである中小企業では、具体的なセキュリティ対策を理解できていない。（a 団体） ・ セキュリティ対策を求める上での課題は、企業によって、セキュリティ対策への温度感や費やせるリソースが異なる点である。（b 団体）
2	製造 B	・ 業界団体として情報セキュリティに関する情報共有を行っている。 ・ 個社製品に実装するセキュリティ対策は、自社基準に加え、市場の要求水準も考慮している。 ・ 課題は、製品によって求めるレベルが異なり、統一的なセキュリティ基準を設定するのが困難な点である。

3	製造 C	・ セキュリティガイドラインを策定し、現在改訂中である。完成した段階で業界としてアナウンスを行い、会員に見ていただけるよう取組む予定である。 ・ 大手企業は IEC 62443 の遵守に向けて独自に取組んでいるが、中小企業は IEC 62443 への対応は体制や費用面等で困難であるため、中小企業にとってある程度実施しやすいものとしてセキュリティガイドラインを策定した。そのため、中小企業が活用いただけるものと考えている。 ・ ガイドラインの活用状況に関する会員企業へのアンケートでは、あまり活用されていない結果となり、どのようにして、中小企業にセキュリティ対策を促すかは課題である。なお、中小企業がセキュリティ対策を実施していない原因としては、対策の必要性は認識していながらも体制や費用面で実施できない場合と、そもそもセキュリティ対策の意識が低い場合の 2 点が考えられる。
4	インフラ A	・ ガイドライン策定以外のセキュリティ確保の取組については模索中である。加盟企業から共通的な課題が抽出され、業界として共通の取組が必要とあれば実施していくが、現時点ではそのような課題は挙がっていない。 ・ 各企業において、重要インフラであり、供給を止められないという意識を持ち、サイバーセキュリティ対策を積極的に取組んでいる。
5	インフラ B	・ 主要企業のサイバーセキュリティがどうあるべきかを議論する準備として、実態把握が必要と判断し、NIST の CSF[15]を参考にサイバーセキュリティ対策状況の評価を実施した。 ・ 評価結果の中で、評価が低かった項目について業界で取組める改善方法や先進的に取組んでいる活動についての勉強会を実施しようとしている。具体的な項目としては、インシデント対応や復旧計画における役割の確認や文書作成などが挙げられる。
6	インフラ C	・ NISC、J-CSIP[16]、JPCERT/CC[17]などからの情報収集を継続的に実施している。 ・ セキュリティ対策強化に向けて訓練の機会を提供している。例えば、サイバーインシデント発生時の報告訓練では、中小規模の事業者も含めて実施している。より実践的な訓練としては CSSC[18]の演習に参加している。
7	防衛	・ 業界における情報セキュリティ対策強化に向けた取組は特に行っていない。

[15] Cyber Security Framework の略。米国国立標準技術研究所(NIST)が定めたサイバーセキュリティフレームワーク。正式名称は、「Improving Critical Infrastructure Cybersecurity（重要イ ンフラのサイバーセキュリティの向上)」

[16] J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan　IPA を情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組

[17] Japan Computer Emergency Response Team/Coordination Center の略。一般社団法人「JPCERT コーディネーションセンター」の略称。インターネットによる不正アクセスの被害に対応するために設立された情報提供機関

[18] Control System Security Center の略。技術研究組合制御システムセキュリティセンター

8	情報通信	・ 「情報セキュリティ報告書」にて対策を公表している。 ・ セキュリティ推進活動を通して取引先における情報セキュリティは浸透してきており、現時点では課題はないと考えている。
9	金融	・ 業界内にワーキング・グループ(WG)を立ち上げ、各種ガイドラインや対策推進に資するコンテンツ等を作成し、会員内で共有している。 ・ サプライチェーンリスクは各企業が外部委託管理として対応してきたが、クラウド利用時にクラウドそのものが障害を起こして複数の金融機関が同時にダウンする（集中化リスク）については、課題となっている。 ・ 外部委託管理という点では、調達したハードウェアにマルウェアが埋め込まれるリスクは今後議論する必要があると考えている。米国では、新品で調達したハードウェア機器にマルウェアが埋め込まれている事案が発生した。日本でも同様のリスクは認識されているが、事案として発生していないこともあり、議論はまだ進んでいない。
10	製薬	・ 一般的な守秘義務以外に、事案が発生した場合は、再発防止策を追加で要請することはあるが、一律に強化の取組を行ってはいない。
11	運輸	・ 情報セキュリティに関する勉強会や情報共有を実施している。例えば、セキュリティベンダに最新動向を説明してもらう勉強会では、サプライチェーンに関わる情報提供もあった。 ・ 新型コロナウイルスの影響を受け、活動が制限を受けていることもあり、まだ課題を認識するまでの活動になっていない。

3.1.3 インシデント対応

インシデント対応として、以下のヒアリング項目を確認した。

① 事故（インシデント）が発生した場合の報告等の有無

② 事故（インシデント）が発生した場合の対応規程（対応手順、チェックリスト等）の有無、またその内容（「情報の共有、報告、公表」の観点等）

③ ①②共に無しの場合

- 事故（インシデント）が発生した場合、どのような対応を行うことを想定しているか（監督官庁への報告等）
- 国等の行政機関に対しての要望

ヒアリングの結果、業界としてインシデントに関する情報共有を実施する枠組み（監督官庁や団体への報告など）があるのは 5 分野（インフラ A、B、C、製造 A、金融）であった。また、自主的に脆弱性情報やインシデントに関する情報共有を行っているのも 7 分野（インフラ A、B、C、製造 A、金融、製薬、運輸）あった。

うち、インシデントが発生した企業が対応に困っていればサポートをしたり、質問があれば対応したりするような共助の取組を実施している事例が 1 分野（金融）、団体として、インシデント対応に関するガイドラインを策定しているのが 3 分野（金融、制御機器、製薬）であった。

また、11 分野（全分野）において、各企業単位でインシデント対応規程を策定し、情報収集、対応を実施していた。

インシデント対応における課題として以下が挙げられた。

- 共有する情報が機密情報にあたる場合もあり、共有する内容や情報共有のタイミング、方法が課題。
- 共有すべき内容を定めた場合でも、実際に発生したインシデント事象がサイバーセキュリティに起因するものかどうかの判断を含め各社が漏れなく対応できるほどのリソースがあるわけではない。
- 委託先を含め海外にある関係企業とのインシデント情報共有にあたっては、インシデントに対する重要度の認識が異なる等、情報共有における方針やルールの認識合わせが困難。

表 3-3 インシデント対応（業界別）

No.	分野	ヒアリング結果
1	製造 A	【インシデント発生時の情報共有】 ・ 業界団体として、事故（インシデント）発生時に情報を取りまとめて共有する取組はないが、ある業界団体では、事故（インシデント）情報をボランタリーに共有する枠組みがある。（a 団体） 【インシデント対応規程】 ・ 業界としての対応規程はない。（a 団体）
2	製造 B	【インシデント発生時の情報共有】 ・ 業界団体として、インシデント発生時に情報を取りまとめ企業へ共有する取組は行っておらず、各社で対応している。
3	製造 C	【インシデント発生時の情報共有】 ・ インシデントに関して、業界としての取りまとめは無く、各企業の判断に任せている。 【インシデント対応規程】 ・ ガイドラインには、インシデント対応方法がまとめられている。
4	インフラ A	【インシデント発生時の情報共有】 ・ サービス供給に係る何らかの支障が生じた場合、事象に応じて所管省庁に報告を行うこととなる。サイバー関係が原因ということもあり得るが、サイバーに特化した報告義務はない。ただし、サイバー関連インシデントの発生時には企業が所管省庁へ報告し、同時に業界団体とも情報共有することとしている。 【インシデント対応規程】 ・ 正式に規則として位置付けたものではないが、情報共有体制を構築している。個別企業から所管省庁へのインシデント発生の報告を除けば、業界団体が業界内、企業-所管省庁間のハブとなって情報共有を行うことが基本であり、予め連絡先の確認を行っている。
5	インフラ B	【インシデント発生時の情報共有】 ・ インシデント発生時は、事業法の下、企業が直接国へ報告する。また、ISAC のインシデント報告ガイドラインには、国へ報告する際には TLP[19]に応じて、ISAC へも共有する旨が記載されている。 【インシデント対応規程】 ・ ISAC では、各社からの情報の共有に際しては、公開範囲や内容を踏まえ、個社名を伏せ字にするなど情報共有のマニュアルに従い、事務局で精査し展開している。 ・ 情報共有の際には TLP を定めている。インシデント情報はどこの企業か特定できるような情報は伏せて共有する。共有してもらう時点で他社に共有することは合意されているが、出す時点で TLP を決めてもらう。共有範囲も発信元による TLP の指定を踏まえて対応する。
6	インフラ C	【インシデント発生時の情報共有】 ・ サービスの供給停止や人身災害が発生した場合は、事業法に則り、事業者から所管省庁経由で NISC へ報告することとなっている。同様の内容を業界団体へも

[19] Traffic Light Protocol の略。機密情報をいつ、どのように共有するべきかを示した仕組みや基準

		共有するよう依頼している。そこまでの事象に至らずとも、制御システムにサイバー攻撃がなされた場合、業界団体で情報を受けて、所管省庁、NISC に報告する。 ・ 報告事例があれば業界内でも共有していくが、ルールはあるものの、実際に報告事例は発生していない。制御システムはまだスタンドアローンも多く、セキュリティ上の脅威が顕在化するケースは少ない。 ・ 情報系システムへのサイバー攻撃についても、業界団体への任意での情報提供を依頼しているが、実績としてはあまりない。 【インシデント対応規程】 ・ 対応規程は各事業者が策定している。業界団体から何らか提示しているものはない。各事業者は、JPCERT/CC や IPA などのインシデント対応に関するドキュメントを参考にしているのではないか。
7	防衛	【インシデント発生時の情報共有】 ・ 業界として、情報収集を行ったり、とりまとめて報告したりすることは特にない。各企業が契約に応じて所管省庁に報告している。 【インシデント対応規程】 ・ 業界として対応規程を定めていることは特にない。
8	情報通信	【インシデント発生時の情報共有】 ・ 業界団体はインシデント時の報告には関わっていない。各企業において、サービスに影響がある場合は納入先である企業から所管省庁に報告される。機密情報漏えい等の場合の対応は各社が実施しており、業界団体への報告はない。
9	金融	【インシデント発生時の情報共有】 ・ 金融機関から所管省庁へ報告する。 ・ 金融機関から業界団体に情報共有があると、対応をサポートすることがある。インシデントをきっかけに、業界団体で議論に発展することもある。 【インシデント対応規程】 ・ 金融機関から業界団体に共有されたインシデント情報の共有範囲を TLP で定め、これに基づき、共有された情報を適切に取り扱う。
10	製薬	【インシデント発生時の情報共有】 ・ 個人情報漏えいの場合は、業界団体や個人情報保護委員会への報告はある。機密情報の漏えいに関する報告はない。
11	運輸	【インシデント発生時の情報共有】 ・ 業界団体への報告義務はないが、情報共有の取組はある。具体的には、JPCERT/CC が提供する情報共有ツールを活用しながら、不審メールの情報などを自主的に共有している。 【インシデント対応規程】 ・ 報告ルートや報告内容に関するルールは確立している。

3.1.4 業界横断的に情報共有が望まれる内容

業界横断的に情報共有が望まれる内容として、以下のヒアリング項目を確認した。

① 業界における各種の取組の中で、他業界においても参考となり得るなど業界横断的に情報共有が望まれる取組、方法の有無、またその内容

② 同業他社の事例や業界としての対策レベルの紹介等、業界における情報共有の取組の有無

ヒアリングの結果、複数の関係団体や ISAC で業界横断的に情報共有する取組を実施しているのが 4 分野（インフラ B、金融、製造 C、運輸）であった。

業界横断的に情報共有が望まれる情報として以下が挙げられた。

- 業界に関わらず、インシデント情報やインシデントへの対処方法などが共有されると今後の参考となる。
- 各国の法規制・国際規格への対応等、業界横断的に共通認識を持つのは有効である。
- サプライチェーンのセキュリティ確保に関する取組事例などを共有されると参考になる。

業界横断的に情報共有する取組における課題として以下が挙げられた。

- インシデントとして認識できている件数が多くないため、特に技術的な側面で他の業界に共有できる情報がなかなか蓄積されない。
- 情報共有を実施した場合でも、実際に提供される情報が千差万別であり、情報の受け手側のリソース不足により、情報を取捨選択するのが困難。
- 情報共有における情報提供者のメリットやインセンティブが明確でないと、積極的な情報共有は期待できないのではないか。
- 他業界のセキュリティ対策の取組内容などは、自業界の取組の参考となるが共有されていない。

表 3-4 業界横断的に情報共有が望まれる内容（業界別）

No.	分野	ヒアリング結果
1	製造 A	・ 特に無し
2	製造 B	【業界横断的に情報共有が望まれる内容】 ・ 各国の法規制・国際規格への対応等、業界としての方向性や共通の基準など業界横断的に共通認識を持つことが望ましい。
3	製造 C	【業界における情報共有の取組状況】 ・ 機器ベンダの他、JPCERT/CC、IPA、省庁など、国際標準等を議論する際に重要となる組織が参加する会議体があり、何か取組を進めようとした時に一方的な議論にならない等、情報共有が有効な場となっている。

4	インフラ A	【業界における情報共有の取組状況】 ・ 一部の企業から、実際に提供される情報が千差万別であり、担当者も多くないので、その情報を素早く取捨選択できるかどうかは体制面を考えると難しいという意見が挙がっている。 【業界横断的に情報共有が望まれる内容】 ・ 海外のパイプラインがサイバー攻撃を受けた事例の情報など、企業の取組の参考になる情報があるならば入手したい。
5	インフラ B	【業界横断的に情報共有が望まれる内容】 ・ インシデント情報では、実際に起きていた事実は参考になるのではないか。また、今後はサプライチェーンのセキュリティ確保に関する取組事例などを共有いただけると参考になる。
6	インフラ C	【業界における情報共有の取組状況】 ・ 業界ではインシデントが発生していないため、特に技術面で他の業界へ共有できる情報がなかなか蓄積されない。 ・ セプターカウンシルの中で他業界の取組を勉強することはある。 ・ オリンピック・パラリンピック開催の際には強化期間を設けたなど、業界の取組は適宜発信している。
7	防衛	【業界における情報共有の取組状況】 ・ 情報共有による自社のメリットやインセンティブが明確でないと、積極的な情報共有は期待できないのではないか。
8	情報通信	【業界における情報共有の取組状況】 ・ 過去には、ネットワークや端末で発生したサイバー攻撃の事例を業界団体のウェブページで発表していたこともある。FAX の情報漏えい、ルーター乗っ取りにより攻撃の踏み台にされた等の事例があれば発表するかもしれない。 【業界横断的に情報共有が望まれる内容】 ・ 業界に関わらず、インシデント情報やインシデントへの対処方法などが共有されると今後の参考にできる。
9	金融	【業界における情報共有の取組状況】 ・ 各業界の ISAC が集まる会合が定期的に行われ、インシデントハンドリングにおいて他業界と情報共有を行っている。
10	製薬	・ 特に無し
11	運輸	【業界における情報共有の取組状況】 ・ 他の ISAC とも情報共有を行っている。セキュリティに関する内容だけではなく、加盟企業のために組織として実施すべき取組等について議論を行っている。

3.2 発注元企業の抱える問題意識

発注元企業が抱える課題を把握するため、ヒアリングした内容を「発注元企業の情報セキュリティ対策の取組」「取引先選定に関する問題意識」「契約締結に関する問題意識」「情報セキュリティ対策の実施状況の把握に関する問題意識」「再委託に関する問題意識」に分けて整理した。

3.2.1 発注元企業のセキュリティ対策の取組状況と問題意識

取引先企業に求める情報セキュリティ対策の取組として、以下のヒアリング項目を確認した。

【取引先企業に求める情報セキュリティ対策の取組状況】

① 発注元企業が把握している情報セキュリティガイドライン（情報セキュリティに関する基本ルール）等の有無、またその内容

② 発注元企業が把握している情報セキュリティガイドラインが有りの場合

- 情報セキュリティガイドラインの中身の充足度
- 取引先の情報セキュリティ対策状況レベルの認識
- 抱えている課題の有無、またその内容

③ 発注元企業における情報セキュリティ対策強化に向けた取組の有無、またその内容

④ 取組において直面した・抱えている課題の有無、またその内容

⑤ 取引先企業の情報セキュリティ対策状況の把握、対策状況のレベルの認識

⑥ 取引先企業の情報セキュリティ対策に関して抱えている課題の有無、またその内容

⑦ 今後、取引先企業に求めていきたいセキュリティ対策と求めるにあたっての課題

【インシデント対応の取組状況】

① 事故（インシデント）が発生した場合の報告等の有無

② 事故（インシデント）が発生した場合の対応規程（対応手順、チェックリスト等）の有無、またその内容（「情報の共有、報告、公表」の観点等）

③ 取引先企業側でのインシデント発生時の取組状況

④ 上記取組状況に対する評価（十分、適切、不十分）

⑤ 取組において直面した・抱えている課題の有無、またその内容

【業界横断的に情報共有が望まれる内容】

① 業界横断的に情報共有が望まれる取組、方法の有無、またその内容

② 情報共有における課題の有無、またその内容

表 3-5 発注元企業のセキュリティ対策の取組状況と問題意識

No.	分野	ヒアリング結果
1	製造 A	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 取引先にセキュリティガイドラインを展開し、セルフチェック結果を回収している。セキュリティガイドラインを遵守できない企業については、ウェビナーでの指南や有償で業者とタイアップしてパッケージで支援することもある。なお、セキュリティガイドラインの遵守については、新規取引先における取引要件とすることを検討している。 ・ セキュリティガイドラインの対策を実際に進めるのはサイバーセキュリティ担当者である。取引先企業の担当者が、セキュリティ対策を推進するためには経営者の理解が課題となる。経営者の意識を変えていきたい。 【インシデント対応の取組状況】 ・ 共有した情報が機密情報にあたる場合もあり、共有する内容や情報共有のタイミング、方法が課題である。
2	製造 B	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 自社で製品のセキュリティガイドラインを策定している。ガイドラインには、製品の開発環境に関する要件も含まれる。取引先に対しては、セキュリティガイドラインを遵守するよう要求している。（a 企業） ・ 製品によって求めるレベルが異なり、統一的なセキュリティ基準を設定するのが困難である。（a 企業） ・ 自社内でも商流の違いでセキュリティ基準が統一できない。（支社店や海外開発製品など）（b 企業） 【インシデント対応の取組状況】 ・ 発生した事象がセキュリティ起因かどうかの判断が難しい。（a 企業） ・ 利用者の運用ミスが原因のインシデントでは、調査に専門業者が必要であり、費用負担の整理も必要となる。（b 企業） ・ インシデント発生時は品質保証部門が対応するが、当該部門が品質保証をしていない製品も取り扱う必要がある。（b 企業）
3	製造 C	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 様々な取引があるが、取引先へ要請しているセキュリティ対策は統一しておらず、取引ごとに個別にセキュリティ対策を要請している。（a 企業） ・ システム開発・運用を外部委託する場合、全社統一の社内向け情報セキュリティ規程を活用している。本規程には、外部委託契約に関する項目が含まれ、P マーク・ISMS[20]を取得しているか、過去に違反していないか、再委託する場合は申告しているかなど、委託先の状況を確認している。（a 企業） ・ 委託先にセキュリティ対策を要求するが、その要求が委託先側で適切に実行され、管理されているかを把握することは困難である。現状は、口頭での確認に留ま

[20] Information Security Management System の略。組織内での情報の取り扱いについて、機密性、完全性、可用性を一定の水準で確保するための仕組み

		る。（b 企業） 【インシデント対応の取組状況】 ・ グループ会社であっても、海外企業とのインシデント情報共有は課題がある。海外と日本では、インシデントに対する重要度の認識が異なる等、情報共有における方針やルールの認識合わせは困難と考える。（b 企業） 【業界横断的に情報共有が望まれる内容】 ・ 新しい規格が出たときにどう捉えるか、やらないとどうなるのか等、複数業界が関わっている件で情報共有ができると、意識を合わせていくのに有効と考える。（b 企業）
4	インフラ A	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 複数の企業において、秘密保持契約（NDA）の締結以外にも取引先に対してセキュリティ対策を要請している。内容は発注元企業によって異なるが、例としては以下のとおり。 ➢ 発注元企業の情報が取引先から再委託先にどのように共有されるかの報告を求めている場合がある。 ➢ 多要素認証の実装、ウイルス対策ソフトの導入などを求めている場合がある。 ➢ 自社グループ企業に対するフォローとして取引先に定期的にセキュリティに関するアンケートを採って、高リスクと判断された場合に重点的に改善を推奨する等の取組を行っている企業もある。 ・ セキュリティ対策は各社が自己責任で対応すべきものという考えに基づいて、取引先に対して明確な要請は行っていない企業もある。
5	インフラ B	- 発注元企業へのヒアリングは実施していない
6	インフラ C	- 発注元企業へのヒアリングは実施していない
7	防衛	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 取引先へ発注する際は、製品の仕様書、基本取引契約書等で情報の取り扱いを定めている。 ・ 取引先企業は中小企業が多く、セキュリティ対策を厳しく要求すると、値上げや契約の打ち切りを打診される可能性がある。 ・ 取引先がセキュリティ対策を実施する上での課題は費用面である。
8	情報通信	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ セキュリティ対策は注力して取組んでおり、「情報セキュリティ報告書」を公表している。本文書は毎年発行しており、会社における情報セキュリティの取組をまとめている。取組の中には、基本的な情報セキュリティ対策、情報セキュリティガバナンス、開示可能な範囲での技術的な対策例、取引先のセキュリティ確保に向けた取組などを整理している。（a 企業） ・ サプライチェーンにおける情報セキュリティ対策の取組の概要を公表している。取引先に対しては、インシデント予防対策や再発防止のための教育や監査などを実施している。実施できない場合は、サプライチェーンから外す場合もある。（b 企業）

		・ 取引先に対して情報セキュリティ対策の促進活動を開始した当初、情報セキュリティ対策のチェックリストで評価したところ、満点にならない取引先は多くいた。その後、情報セキュリティの説明会を実施したり、チェックリストで点数の低い項目を分析し、改善施策を提案したりすることで、多くの取引先で満点となっている。このような活動を通して取引先における情報セキュリティ対策は浸透してきており、現時点においては課題はない。
9	金融	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ FISC において様々なガイドラインが策定されており、その中でも安全対策基準を参考に委託先管理を行っている。委託先に対して、セキュリティ状況に関するチェックシートを用意し、ヒアリングを実施している。具体的には、委託先での個人情報の管理方法、ID 管理方法などを確認している。単純な委託なのか、IT に関する委託なのか、業務によってチェック項目は異なる。郵便物配送等個人情報を渡すケース、個人情報をクラウドサービスで保管するケース等、個人情報が含まれるかどうかでチェックシートも異なる。 ・ 現時点で抱えている課題はない。
10	製薬	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ 自社では、情報セキュリティの基本方針と対策基準を策定している。（a 企業） ・ H-ISAC[21]のガイドラインに従っている。他社の状況はわからないが H-ISAC のガイドラインは、ヘルスケア分野のグローバル企業にとっては標準ではないか。（b 企業） ・ セキュリティ対策に対するマインドをどのように変えていくかが課題である。セキュリティに関する情報を外部に出したくない企業もあるが、昨今は、隠すより開示した方がよいという考え方に変わっていると考える。（b 企業） 【インシデント対応の取組状況】 ・ H-ISAC に情報共有を行う枠組みがある。（b 企業） 【業界横断的に情報共有が望まれる内容】 ・ 取引先にセキュリティ対策を要求する場合、契約書でどのように要求している実態があるか、他業界ではここまで要求しているのが一般的か、製薬業のレベルが他業界と比較してどうかがわかると参考となる。（a 企業） ・ セキュリティに関する取組やインシデント情報は業界に閉じる必要はなく、横断的に共有されると参考になるのではないか。（b 企業）
11	運輸	【取引先企業に求める情報セキュリティ対策の取組状況】 ・ システム開発時のセキュリティ要件を定め、取引先に要請している。 ・ 最近、クラウドの利用が増えており、現場で勝手に契約されてしまうケースがある。現時点でインシデントは発生していないが、パブリッククラウドには課題があると考えており、パブリック側の設定が変わってしまって脆弱性を生んでいるケースがある。（a 企業）

[21] Health Information Sharing and Analysis Center の略。災害時の医療供給等の事業継続体制を重視した情報共有組織（ISAC）

3.2.2 取引先選定に関する取組状況と問題意識

取引先選定に関する問題として、以下のヒアリング項目を確認した。

① 取引先企業に対して、秘密保持契約（NDA）締結以外で要求している情報セキュリティ対策の有無、またその内容

② （情報セキュリティ対策を要請していない場合）要請していない理由

③ 情報セキュリティ対策に関する選定基準（セキュリティ要件）の有無、またその内容

④ 取引先選定において抱えている課題の有無、またその内容

ヒアリングの結果、取引先に自社が定めたセキュリティガイドラインの遵守を要請しているのは 4 社であった。

取引先選定における課題として以下が挙げられた。

■要求水準に満たない取引先への対応

・ 要求レベルを満たせない場合であっても、例えば調達できないと製品が成りたたない、業界における取引先が限定されており代替がきかない、といった事情もあり対応が難しい。

・ セキュリティ対策を要求しても価格反映できないため、要請できない。

■統一的、あるいは具体的な要件設定の難しさ

・ 取引先企業においては各々のセキュリティ基準があるため、発注元企業の基準に則って具体的な対策を要請するのは難しく、機密情報を正しく管理するようになど、どちらの基準にも整合的で抽象的な高い要請をもって取引先の選定を行わざるを得ない。

・ 様々な業務の取引があるため、取引先へ要請するセキュリティ対策の内容を統一するのが難しい。

・ セキュリティ対策の要請に際して、例えば、SNS によるコミュニケーションやクラウドサービス利用、テレワーク環境下におけるセキュリティ等、取引先と認識を合わせる必要のある事項が多く、コストが大きい。

■従来から取引関係がある取引先への追加要求

・ 従来から取引関係があり、特にインシデントが発生していない場合には、どのようにセキュリティ対策を追加的に求めていくかが課題という声もあった。

■実態把握の困難さ

・ 取引先に要求したセキュリティ対策が適切に実行されているかを把握することが課題である。

表 3-6 取引先選定に関する取組状況と問題意識

No.	分野	ヒアリング結果
1	製造 A	【取引先選定に関する取組状況】 ・ グループ企業へは、業界ガイドラインの遵守を要請。（a 企業） ・ サプライヤー企業以外には、サプライヤーでの被害事例の共有、標的型メールの注意喚起、二段階認証の要求等を実施。（a 企業） 【取引先選定に関する課題】 ・ 資本関係のない企業に対しては、要請できていない。（b 企業）
2	製造 B	【取引先選定に関する取組状況】 ・ 製品セキュリティガイドラインの遵守を要請。（a 企業） ・ 契約書にセキュリティ要件を明確には盛り込んでいない。ただし、技術部門で必要に応じて取引先とチェックリスト形式でセキュリティ対応状況を確認している。また、製品・運用サービス・ソフトウェア全てを対象に、取引先に対してセキュリティ対策を促す「セキュリティ品質保証ガイドライン」を配布し、セキュリティ対策の意識を持ってもらっている。（b 企業） 【取引先選定に関する課題】 ・ 要求レベルを満たせない場合であっても、調達できないと製品が成り立たないので対応が困難。（a 企業） ・ 製品により要求レベルが異なり、統一的なセキュリティ基準の設定が困難である。今後は製品ごとにレベル分けする予定。（a 企業） ・ 従来より取引関係があり、特にインシデントが発生していない場合には、どのようにセキュリティ対策を追加的に求めていくかが課題である。（b 企業）
3	製造 C	【取引先選定に関する課題】 ・ 委託先にセキュリティ対策を要請するが、その要請が委託先側で適切に管理され、実行されているかを把握することは課題と考える。（a 企業） ・ 取引先には取引先ごとのセキュリティ基準があるため、自社が求めるセキュリティをどのように実行してもらうかが課題である。（b 企業）
4	インフラ A	【取引先選定に関する課題】 ・ 取引先に求める対策の内容や水準をどのように定めるか、実際のセキュリティ対策の実施状況をどこまで確認できるのか、確認手順はどうするかという点が課題である。要求事項が厳しすぎると取引先が過度に限定されてしまうのではないかとの懸念の声もあった。
5	インフラ B	- 発注元企業へのヒアリングは実施していない
6	インフラ C	- 発注元企業へのヒアリングは実施していない
7	防衛	【取引先選定に関する課題】 ・ 取引先企業は中小企業が多く、セキュリティ対策を厳しく要求すると、値上げや契約の打ち切りを打診される可能性がある。
8	情報通信	【取引先選定に関する課題】 ・ 長年、取引先に対して、セキュリティ対策の促進のための取組を進めてきており、改善もされており、課題は特にない。

9	金融	【取引先選定に関する課題】 ・ 取引先のセキュリティ状況の確認に時間を要する点が課題である。
10	製薬	【取引先選定に関する課題】 ・ 取引先候補には、情報セキュリティに関心が高くない企業、こちらが求める情報をコンフィデンシャルということで提示できない企業、セキュリティ対策を何から実施すべきかわからない企業などがある。これらの企業に対して、自社が求めるセキュリティ対策をどのように理解、実施してもらうかが課題である。（a 企業） ・ セキュリティ対策をフルアウトソーシングしている中小企業では、自社のセキュリティ状況を把握できていない場合がある。（b 企業） ・ IT システムの場合、より高いセキュリティを求めた結果、セキュリティ対策を要求した際にコストに影響するのではないかという懸念がある。IT の場合はそれを依頼しないと業務が進まないことがあるため、自社としてどこまでセキュリティへの対策を要求するか、どこまでリスクを許容するかは課題であると考えている。（b 企業）
11	運輸	【取引先選定に関する課題】 ・ 制御システムは、業界構造と今までの運用資産等の関係から、取引先を変更することが難しく、取引先に対応を求めるしかないと考える。（b 企業）

3.2.3 契約締結に関する取組状況と問題意識

契約締結に関する問題として、以下のヒアリング項目を確認した。

① 契約書へのセキュリティ条項記載の有無

② 無しの場合

- セキュリティ条項を記載しない理由
- 契約書において抱えている課題の有無、またその内容

③ 契約において抱えている課題の有無、またその内容

ヒアリングの結果、ヒアリング先の発注元企業において契約書のテンプレートにセキュリティ要件を含めている企業は 1 社で、セキュリティレベルが高い情報等を扱う場合などに限り、特約等でセキュリティ要件を含めている企業は 3 社であった。また、個別のセキュリティ要件を仕様書や設計書で示している場合も多い。

契約にセキュリティ要件を含めるにあたり、以下の課題が挙げられた。

■契約書ひな形の見直しの必要性

・ 契約書は相手先によらず同一のひな形を使用しているため、契約書にはそこまでセキュリティ対策に係る事項について詳しく記載することができない。

■コストアップ分の負担の懸念

・ 発注先にセキュリティ条項を充足してもらうためのコストアップ分の負担が課題となる可能性がある。

■調達部門との調整

・ 発注元企業の調達部門がセキュリティ対策に対する関心度が高くないことが多く、セキュリティ条項を契約書に含めることが難しい。

また、取引先にセキュリティ対策を要求する場合、契約書にどこまで盛り込むことが分からないため、どのように要求している実態があるか、他業界ではここまで要求しているのが分かると参考となるという意見が挙げられた。

表 3-7 契約締結に関する取組状況と問題意識

No.	分野	ヒアリング結果
1	製造 A	【契約締結に関する取組状況】 ・ 取引先との契約では、機密条項に関する要求はあるものの、サイバーセキュリティに関する要求はない。
2	製造 B	【契約締結に関する取組状況】 ・ 調達において、セキュリティ要件を契約書に含めてはいない。（a 企業） 【契約締結に関する課題】 ・ 購買部門は価格優先であり、セキュリティ対策への関心が薄くセキュリティ要件を要求できない。（b 企業）
3	製造 C	【契約締結に関する取組状況】 ・ 契約書には具体的なセキュリティ条項を記載している場合もあるが、記載していない場合は、別途、セキュリティ対策の要請を個別に実施している。
4	インフラ A	【契約締結に関する課題】 ・ 機密保持条項や秘密保持契約（NDA）は定めているが、それ以外の情報セキュリティ条項を契約に含めている発注元企業は 1 社もなかった。その理由として、現状の契約書でこれまで特段に課題になったことがないために機密保持や NDA 以外の内容まで含める必要性を実感できていないことが挙げられている。
5	インフラ B	- 発注元企業へのヒアリングは実施していない
6	インフラ C	- 発注元企業へのヒアリングは実施していない
7	防衛	【契約締結に関する取組状況】 ・ 特約ベースで取引先企業にセキュリティ対策を求めている。
8	情報通信	【契約締結に関する取組状況】 ・ 取引先との契約では、基本契約書に秘密保持が含まれる。セキュリティ要件を含めないと契約できないルールとなっている。特に課題は挙がっていない。（a 企業） 【契約締結に関する課題】 ・ セキュリティを要求したがために見積額が予算を超え、現場で議論になる懸念はある。（b 企業）
9	金融	【契約締結に関する取組状況】 ・ 契約書には、情報の取扱に関して基本的な内容のみ記載されている。契約の前段階で、セキュリティ対策状況を調査し、課題がなければ契約するという流れである。契約の段階で契約書にセキュリティ条項を記載する必要性はあまり無く、その前の取引先選定のところが課題になるのではないか。 ・ 契約書に記載されるのは、個人情報の取り扱いや情報の破棄といった点までである。

10	製薬	【契約締結に関する取組状況】 ・ 現在、契約書のテンプレートにセキュリティ条項の項目があるため、新規で契約する場合は、契約書でセキュリティを要求することは可能である。インシデント報告や監査などの項目は含めている。（a 企業） 【契約締結に関する課題】 ・ 過去に契約締結した取引については、新しい契約書のテンプレートへどのように切り替えるかは課題である。（a 企業） ・ 契約書の締結にあたっては、取引先の法務部門とのやりとりで進めるが、取引先のセキュリティに関するスタンスが異なる場合、合意形成に時間がかかる。（a 企業） ・ 契約書でセキュリティを要求する場合、提供する情報とビジネスの重要性を勘案しその都度契約条項を法務部で審査しているため、一律の契約条項を定めるのは難しいが一定のレベルでは契約できていると思われる。一方で、締結後に契約の水準を満たしているかを定期的に確認できているか状況はわからず、またルールを定めたとしても実効性を確保するのは難しいと思われる。（b 企業） ・ 取引先にセキュリティ対策を要求する場合、契約書でどのように要求している実態があるか、他業界ではここまで要求しているのが一般的か、製薬業のレベルが他業界と比較してどうなのかがわかると参考となる。（a 企業）
11	運輸	【契約締結に関する取組状況】 ・ 契約書へは、具体的なセキュリティ条項を記載していない。業務用の端末と開発保守の端末は分ける、IPS[22]や IDS[23]を必須とするなどの具体的なセキュリティ要件は、仕様書や設計書などに記載される。 【契約締結に関する課題】 ・ システムに詳しい担当者がいれば取引先がきちんとセキュリティ対策に取組んでいるかどうかがわかるが、そうでないとチェックできないという課題はある。

[22] Intrusion Prevention System の略。サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して攻撃を未然に防ぐシステム

[23] Intrusion Detection System の略。サーバやネットワークの外部との通信を監視し、攻撃や侵入の試みなど不正なアクセスを検知して管理者にメールなどで通報するシステム

3.2.4 セキュリティ対策の実施状況の把握に関する取組状況と問題意識

情報セキュリティ対策の実施状況の把握に関する問題として、以下のヒアリング項目を確認した。

① 取引先企業に対して、情報セキュリティ対策の実施状況の把握の有無

② 有りの場合

- 実施状況把握のための取組
- 上記取組を行うにあたって抱えている課題の有無、またその内容（解決した課題も含む）

③ 無しの場合

- 実施状況を把握しない、把握できない理由（リソース不足、取引先が情報セキュリティ対策できない、対策状況を確認しきれないなど）
- 実施状況を把握できていないことで抱えている課題の有無、またその内容

ヒアリングの結果、取引先の情報セキュリティ対策の実施状況の把握については、各社において必要なセキュリティ項目を定め、契約時にセキュリティ対策状況のアンケート形式やセルフチェック結果を回収している企業が多かった。数年に 1 回など、取引先を訪問し実施状況を確認している企業もあった。

セキュリティ対策の実施状況を把握できていない企業からは以下の課題が挙げられた。

■実施状況の確認の難しさ

- 取引先に要求したセキュリティ対策が適切に実行されているか把握することが困難。
- セルフチェックの結果をもとに確認しているが、実際に実施されているかは確認できていない。
- 取引先のセキュリティの実態を確認するリソースや権限がない。
- 資本関係がないところに対してはセキュリティ対策実施状況の把握を徹底することは難しい。

表 3-8 セキュリティ対策の実施状況の把握に関する取組状況と問題意識

No.	分野	ヒアリング結果
1	製造 A	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ 取引先に業界ガイドラインを展開し、セルフチェックにて状況を把握している。（a 企業） ・ 業界ガイドラインを遵守できない企業には支援を実施することもある。（a 企業） 【情報セキュリティ対策の実施状況の把握に関する課題】 ・ 資本関係のない企業に対しては要請ができない。（b 企業）

2	製造 B	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ 取引先との契約時には、セキュリティ対策状況をアンケート形式で調査している。ISMS 取得の場合等は調査を省略できる。
3	製造 C	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ 委託先に要求したセキュリティ対策は、対策が実施されているかを確認し、エビデンスを残している。現時点で課題は挙がっていない。（a 企業） ・ 共同でシステムを構築する際の協力会社のセキュリティ状況は年 1 回把握しているが、現時点で、セキュリティ対策の実施状況の把握に関して課題は挙がっていない。（b 企業）
4	インフラ A	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ 一部の企業では、自社グループ企業を対象とするものではあるが、定期的な確認を行っており、独自のセキュリティ基準や確認方法等を定めている。
5	インフラ B	- 発注元企業へのヒアリングは実施していない
6	インフラ C	- 発注元企業へのヒアリングは実施していない
7	防衛	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ 特約でセキュリティ対策を求める場合は、実施状況の確認が必要であるため、確実に実施している。それ以外は、主要な取引先を対象に部分的に確認している。データを暗号化して管理しているか等、具体的な実施状況を確認している。
8	情報通信	【セキュリティ対策の実施状況の把握に関する取組状況】 ・ セキュリティ対策状況は、書類や訪問点検を実施しており、特に課題はない。
9	金融	【情報セキュリティ対策の実施状況の把握に関する課題】 ・ クラウドベンダに対するセキュリティ状況の正確な把握や、中小企業に対するセキュリティ対策の状況確認に時間を要する点が課題である。
10	製薬	【情報セキュリティ対策の実施状況の把握に関する課題】 ・ 現時点で、課題は挙がっていない。
11	運輸	【情報セキュリティ対策の実施状況の把握に関する課題】 ・ セキュリティの実態を確認するリソースや権限がなく、実施状況の把握を徹底することが課題である。（a 企業） ・ システム開発をグループ会社へ委託する場合、年に 1 回、取引先に対するセルフチェック結果をもとに確認しているが、実際に実施されているかは確認できていない。（b 企業）

3.2.5 再委託に関する取組状況と問題意識

再委託に関する問題として、以下のヒアリング項目を確認した。

① 再委託の状況把握の有無（委託先中小企業が再委託されているか、その頻度・割合）

② （再委託されている場合）機密情報の受け渡しの有無

③ 委託先管理のためのガイドラインの有無

④ 無しの場合

- 再委託先の情報を把握できていないなど再委託に関する課題の有無、またその内容

⑤ 再委託管理の取組の有無とその内容

- 再委託管理を行うにあたって抱える課題の有無、またその内容（解決した課題も含む）

ヒアリングの結果、再委託の有無は契約時や判明時に申請をもらうことで把握し、再委託する場合は委託先と同等の内容を再委託先にも求めている企業が多かった。なお、再委託に関して抱える課題についての答えはほとんど得られなかった。一方、再委託先のセキュリティレベルが低い場合に情報漏えいの可能性があり得ることは認識されていた。

再委託に関して課題を抱えている企業からは以下の課題が挙げられた。

■再委託状況の把握の難しさ

- 委託先との契約書には、再委託する場合は委託先に求めるセキュリティ対策と同じ内容を再委託先にも求める旨を記載しているものの、再委託先の実態までは権限もなく把握できない。
- 再委託している場合、機密情報の受け渡しはされているものの、個人情報は別として、どこまで情報のやり取りをしているか正確には把握できていない場合もある。
- 昨今、委託先が海外の場合や発注元が同時に発注先になるなど、様々なケースがあり複雑化している。

表 3-9　再委託に関する取組状況と問題意識

No.	分野	ヒアリング結果
1	製造 A	【再委託に関する取組状況】 ・　基本的には再委託の状況は把握している。（a 企業） ・　高機密情報を扱うすべての取引先に対し、再委託先の運用方針まで把握している。（b 企業） 【再委託に関する課題】 ・　各委託元部署にて再委託状況を把握しているため、全社まとめての状況を十分には把握できていない状況である。（a 企業） ・　一般データを扱う取引先の場合は、全て把握できていない。（b 企業）
2	製造 B	【再委託に関する課題】 ・　顧客や取引先も様々であり、オンラインでどこまで繋がっているか、取引先の把握ができていない。
3	製造 C	【再委託に関する取組状況】 ・　委託先が再委託する場合は、委託先、契約内容等を確認し、取引元と一次取引先の契約と同じ内容で再委託先と契約してほしい旨を伝えている。（a 企業） ・　委託先との契約においては、取引基本契約書を作成し、再委託に関する条項を記載している。再委託条項に記載されている情報セキュリティに関する内容は、再委託する場合も委託先に求める内容と同じ内容を再委託先にも求める旨を記載している。（b 企業） ・　共同でシステム構築を行う協力会社には、定常的に自己点検でセキュリティ対策を求めており、サポート切れ OS がないかどうかなど、社員が訪問または文書レベルでの確認を行っている。再委託先がある場合、そのセキュリティ状況を報告するよう求めている。（b 企業） 【再委託に関する課題】 ・　再委託の管理実態は把握できていない。再委託を制限する場合もある。（a 企業） ・　サプライチェーン全体で、例えば欧州の GAIA-X[24]のように、一元的に情報管理が可能になると、委託先や再委託先といった隔たりがなくなり、標準的な管理ができるようになるのではないか。（a 企業）
4	インフラ A	【再委託に関する取組状況】 ・　再委託がある場合の再委託のセキュリティ対策状況については、約半数の発注元企業において把握している。 ・　再委託先企業と機密情報の受け渡しを行っている発注元企業では、概ね委託先管理のためのガイドラインを持っている。 【再委託に関する課題】 ・　再委託先のセキュリティ体制が脆弱であった場合には自社情報が漏えいする可能性もあるという認識はあるものの、直接の委託先の状況も確認できていない場合もある。
5	インフラ B	- 発注元企業へのヒアリングは実施していない

[24] 2019 年 10 月にドイツ政府とフランス政府が発表した、セキュリティとデータ主権を保護しつつ、データ流通を支援するためのインフラ構想

6	インフラ C	-発注元企業へのヒアリングは実施していない
7	防衛	【再委託に関する取組状況】 ・ 機密情報の受け渡しがある場合、契約上で再委託の制限を設けている。 【再委託に関する課題】 ・ 再委託の状況は、特約が付かない限りは把握しきれていない。委託先管理のためのガイドラインは作成していない。 ・ 経済安全保障面で、サプライチェーン上のリスクが存在する点は課題として認識している。
8	情報通信	【再委託に関する取組状況】 ・ 再委託する際は、事前に再委託される情報や情報管理方法、再委託の業務範囲などを申告してもらっている。 【再委託に関する課題】 ・ 申告内容と実態が合致しているかはわからない。再委託先まで監査はできないが、取引先の監査で委託状況のヒアリングやエビデンスの提出を求めることはできる。直接の取引先までの確認に留まらざるをえず、再委託先の管理までできないのは課題とは言える。
9	金融	【再委託に関する取組状況】 ・ 再委託は事前申請をもらい、契約時に再委託先にも金融機関が求めるセキュリティ水準を満たすことを要求している。しかし、再委託先の状況を直接把握できないため、一次委託先に管理することを求める。 【再委託に関する課題】 ・ 最近は、再委託に関するセキュリティの課題や、再委託先が情報を持ち出した場合にどうするか等の課題感はある。 ・ 米国などであれば再委託もかなり確認してくる。中小企業であっても、海外に納入しているのであれば、グローバルにも意識すべきと考える。
10	製薬	【再委託に関する課題】 ・ 再委託する場合は、委託先を通じて状況を把握し、リスク評価を実施することとなるため、委託先がセキュリティに詳しくない場合や共通言語が英語となる場合は、コミュニケーションに時間を要することがある。（a 企業） ・ 再委託先に対して委託元企業がどこまで要求できるのか、また、要求事項をどのように遵守させるのかは課題である。（b 企業）
11	運輸	【再委託に関する課題】 ・ 情報システム子会社との取引の場合は再委託先の状況を把握しているが、他の取引は把握できていない。その他の委託先であると、契約書に再委託を確認する旨は記載しているが、実態までは把握できない。なお、個人情報の場合は再委託まで把握している。

3.3 既存の取組・制度の認知度、活用意向

3.3.1 SECURITY ACTION

SECURITY ACTION の認知度、活用意向として、以下のヒアリング項目を確認した。

① SECURITY ACTION 制度の認知度

② 中小企業の SECURITY ACTION 制度に対する評価（十分、普通、不十分）

③ 今後期待する SECURITY ACTION 制度の役割、取引先選定への活用可能性（取引先中小企業のセキュリティ対策の可視化、取引先選定基準、専門家による確認、実現に向けた課題など）

④ 自己宣言である SECURITY ACTION の信頼性を高めるための対策

（1） SECURITY ACTION：認知度・活用意向

ヒアリング先の発注元企業、団体の担当者においては、SECURITY ACTION の認知度は高くなかった。

しかし、中小企業といっても様々なレベルがあり、基本的なレベルにおいてセキュリティに注意を払っている（対策意識を有している）というひとつの指標にはなるという意見や、中小企業におけるセキュリティ対策の底上げや普及啓発には有効という意見が得られた。

1） 個社としての活用可能性

個社としての SECURITY ACTION の活用可能性については、調達部門の要求を満たすことができれば、活用の可能性はあり得るのではないかとの意見が得られた。

- 調達部門に対して SECURITY ACTION を持っているから選定すると言いやすい。ただし、活用する場合は、調達部門や情報セキュリティ部門など、全社としての取組が必要である。
- 他の企業も利用しているなど、実績があると推奨しやすい。
- 取組の効果がわかりやすく示せればよい。（どの対策を行っているので、情報漏えいのリスクは低いなど）

しかし、自社の取引先と SECURITY ACTION の対象がマッチしないという意見もあった。

- SECURITY ACTION は中小企業向けであり、自社の取引先にはマッチしないものの二次請け選定等での可能性はある。
- 対策内容としては初歩的な内容であり、啓発や底上げの効果はありながらも、自社の利害に絡む取引条件等として活用するのは難しい。
- 既に取引先のセキュリティ対策に関して取組を進めており、新しく本制度を活用する必要性は少ない。

2） 業界としての活用可能性

加盟企業に対して、普及啓発のために SECURITY ACTION 制度の周知や説明を行うことは可能であるという意見は多かった。また、団体の情報共有を行う場や、中小企業向けの支援方法を議論する場での紹介は可能とのことであった。

一方、本制度の周知は可能であるものの、対策レベル・自己宣言制度であること等を踏まえると積極的に取引先の選定基準として使っていくことが団体として推奨できるかどうかは難しい。という意見もあった。

（2） SECURITY ACTION：制度の在り方についての意見

業界あるいは発注元企業において、本制度を取引条件等に活用するにあたっては、自己宣言企業のセキュリティ対策への取組の確実な実施が担保されるような仕組みや、制度自体が広く普及、高い認知度を獲得していることが重要である。

セキュリティ対策の取組の確実な実施の担保には、第三者機関による評価や監査が有効という意見は多かったが、中小企業の自己宣言を増やすためには、宣言のために工数や金銭負担が増えることは望ましくないという点も認識されており、確実な実施の担保と中小企業の負担のバランスに悩む回答が多かった。

1） SECURITY ACTION 制度に関して

SECURITY ACTION 制度に関して挙げられた意見として、SECURITY ACTION はセキュリティ実施状況の自己申告であり、人によって判断の基準が異なることもあるため、現状では自己宣言企業のセキュリティ対策への取組の確実な実施に不安がある、更新がないため、企業がどれだけセキュリティを継続的に維持・運営できているかどうかがわからない、等の声があった。

第三者機関による評価や監査、もしくは場合によっては非遵守の場合に罰則を設けることもあり得るのではないか、あるいは宣言の根拠となる情報を提示できるかどうか、という意見が挙げられた。

他方で、現状、取引先のセキュリティ実施状況確認は自己申告で判断せざるを得ない状況であるため、自己宣言でも問題ないという声もあった。

2） 制度の普及、取得企業の増加

制度普及のためには、本制度を活用できる中小企業を増やす方が重要ではないかという意見も多かった。普及のために最優先すべきは、中小企業にとって負担が少ないことであり、第三者認証取得等のために中小企業において工数や金銭負担が増えるのは望ましくないという意見もあった。

また、本制度を取引条件等で活用するためには、中小企業が取引・入札条件で優遇される等のインセンティ

ブが必要ではないかという意見もあった。

表 3-10　SECURITY ACTION の認知度・活用意向、制度の在り方についてのご意見

ヒアリング結果
【SECURITY ACTION の認知度・活用意向】 ・　ヒアリング参加者は制度を認知していたが、業界としての認知度はそれほど高くない。（製造 A/インフラ A） ・　（個人的な意見だが）SECURITY ACTION 三つ星として、業界ガイドラインと整合性を取り、できていない部分についてお助け隊サービスを活用することができるとよい。（製造 A） ・　自己宣言で、どこまでセキュリティ対策実施状況を担保できるかが課題。（製造 B） ・　セキュリティ対策実施状況の担保には、第三者機関による評価や監査、もしくは場合によっては非遵守の場合に罰則を設けるなど制約を設けることが考えられる。（製造 B） ・　中小企業に第三者認証を求めるのは厳しい。自社が取引先のセキュリティ対策実施状況の確認をする際も自己申告で判断せざるを得ない。（製造 B） ・　調達時に活用されるためにも、SECURITY ACTION を宣言する企業が増えていく必要がある。（製造 B） ・　業界団体が推奨すれば、活用可能性はある。セキュリティ対策実施状況の担保とセットでできればよい制度だと考える。（製造 B） ・　SECURITY ACTION の取引先選定時の活用可能性はあると考える。もし、取引先候補が宣言していた場合、少なくともセキュリティの意識があることの証明となる。また、取引先候補が複数の場合、SECURITY ACTION の星の数が判断材料となる。（製造 C） ・　SECURITY ACTION は、第三者機関による評価や監査があるとセキュリティ対策実施状況の担保になる。しかし、制度普及のためには、まずこの制度を活用できる中小企業を増やす方が重要ではないか。最優先すべきは、宣言にあたって負担が少ないことである。中小企業に体制や費用面で負荷をかけては、SECURITY ACTION 制度は広く活用されないと考える。（製造 C） ・　取引先選定における活用可能性を考えると、自己宣言という点が懸念である。宣言している企業は、セキュリティに関心があることまでは評価できるが、実態としてセキュリティ対策状況が十分かどうかは評価できない。自社との取引の中でも、取引先が申告したセキュリティ状況が実態としては十分でないことがあった。（製造 C） ・　個人的には、専門会社やセキュリティ専門家、IPA などの第三者機関によるお墨付きが付いた方がよい。自己宣言だけでは難しく、宣言する人がよいと思っても、第三者的には問題という場合もあるセキュリティ対策実施状況の担保をどのように高めるかが重要である。（製造 C） ・　将来的に重要性が高まっていく制度だと考える。ただし、取引先に求める基準は各社が判断するものであるし、独禁法の観点もあるため、業界として統一的に制度を活用することは難しい面があるのではないか。（インフラ A） ・　SECURITY ACTION を宣言している企業のセキュリティ対策実施状況の担保には、自社評価レポート等でセキュリティ対策の取組の詳細がわかると良いという意見や、単なる自己宣言にとどまらない仕組み（第三者による確認で虚偽申告を防ぐ、自己宣言ではなく公的認証にする、自治体等が公的な基準として採用する、等）があると良いという意見が挙がった。もちろん、自己宣言という気軽さが制度の特徴であることは理解している。（インフラ A） ・　SECURITY ACTION を宣言する企業は、業界では二次請けや三次請けの企業であり、業界団体の会員企業における取引条件になりづらいのではないか。（インフラ B） ・　発注元企業が取引先の再委託先へ直接セキュリティ対策を要求するのは難しい。（インフラ B） ・　発注元企業が一次請けの取引先企業と契約する際に、再委託先企業に SECURITY ACTION の宣言を要求するのは良い案かもしれない。SECURITY ACTION の記載項目をチェックリストに示すなどでもよい。（インフラ B） ・　ただし、選定条件としたときに、一定水準をクリアしている企業が対策をすべからく実施している訳ではないため、取引の中で優遇することは難しい。（インフラ B） ・　皆で制度を活用しようとなると自業界も乗るのだろうが、宣言企業が増える必要があり、発注側が舵を切るか、ど

ちらが先か次第でもある。（インフラ B）
- 取引先に対策状況を証明するメリットはあるだろうが、業界特性次第ではないか。（インフラ C）
- 各社の判断によるが、事業者が、取引先の評価の参考とする可能性はある。（インフラ C）
- セキュリティ実施状況の自己申告制である同制度のセキュリティ対策実施状況の担保には、宣言の根拠となる情報を提示できるかどうかではないか。根拠を出してもらえるかどうかという課題はある。（インフラ C）
- 業界団体として SECURITY ACTION を推奨することは、事業者としても重く受け止めてしまうため難しいと思う。制度の紹介は可能である。（インフラ C）
- 業界団体の役割としては、制度を加盟企業に周知するに留まるが、加盟していない中小企業の方が多い。加盟企業から中小企業に制度を紹介することになる。（防衛）
- 中小企業がセキュリティ対策を行う場合の課題は費用面である。費用面が政府の制度で補助されると良いと考える。（防衛）
- 取引や入札条件で優遇される等のインセンティブは必要ではないか。調達部門や情報セキュリティ部門など、全社としての取組が必要である。（防衛）
- 発注元企業としては、セキュリティ対策実施のお墨付きは欲しい。中小企業に負担をかけず簡便な形で認証を受けられる、虚偽の申告を防ぐために査察を入れる等の担保が必要と考えられる。（防衛）
- 既に取引先のセキュリティ対策において様々な要件を設定して取組んでいるため、新しい制度に乗り換えるほどではなく、推奨する程度になると考える。（情報通信）
- 直接の取引先が対象とはならないため、再委託先に対して SECURITY ACTION の宣言を推奨する可能性はあるかもしれない。（情報通信）
- 業界としての認知度はそれほど高くない。（金融）
- このような制度の活用を推進するには、金融業界の場合、所管省庁による主導が必要と考える。（サイバーセキュリティお助け隊サービスも同様の意見）（金融）
- 中小企業と一括にするのは避けるべきである。中小企業といっても様々な業種業態、ビジネスの性質、規模があり、同じ括りにして議論することは困難ではないか。（金融）
- 自己宣言で初歩的な内容なので、啓蒙や底上げの効果はあるが、自社の利害に絡めて使うとなると難しい。（製薬）
- SECURITY ACTION に関して、業界団体内で、問合せ窓口を案内したり、会合で制度概要について説明するなど、加盟企業へ周知することは可能である。（運輸）

【SECURITY ACTION 制度の在り方についてのご意見】
- SECURITY ACTION を取引先選定に活用するためには、ISAC などの団体のお墨付きがあるかどうかで信頼できるかが変わる。団体のお墨付きがあれば、取引先のリスク評価において確認項目が少なくなり、短期間で契約まで進められる可能性はある。一方、会社全体で単一のプロセスでリスク評価を行っている関係上、各国または地域固有の制度を取り込むのは現実的には難しい。（製薬）
- ISO のような認証機関による厳格な評価までは求めないものの、第三者機関による評価や監査を求めたい。P マークを取得していても情報漏えいはあるし、それだけで信用できる訳でもないが、目安にはなる。（製薬）
- 一つ星、二つ星は自己宣言なので、三つ星においては、第三者機関等による認証の仕組みがあるとよいと思われる。経済産業省や IPA のガイドラインがあればそれを満たしているかどうかを、認証してもらえると信頼度が増すのではないか。少なくとも、最初の取引先の場合、自己宣言では信用しづらいため、もう少し踏み込んだ形としてほしい。どこまでの第三者認証を求めるのかは検討が必要である。（製薬）
- ISMS、P マークは社内文書を多く作成する必要があるので、中小企業にとって費用をかけるのは難しいだろう。IPA 等が定める基準がありそれを満たしているかがわかる制度で、ある程度は信頼できる、ということであれば有り難い。（製薬）
- 発注元としては、取引先に継続的な対策を求めたく、第三者による評価の方が望ましいのは事実だが、中小企業の負担を考えると難しいと考える。第三者は認証機関でなくとも専門家でもよいと考える。専門家の資質による。（運輸）

- P マークや ISMS は資格取得やそれを維持運用するための努力が要るが、SECURITY ACTION を宣言した企業がどれだけセキュリティを運用できているかどうかがわからない。第三者機関による評価や監査の方が信頼できるのではないか。（運輸）
- 選定する立場では、SECURITY ACTION を持っているから選定すると言いやすい。しかし、それが自己申告であると、セキュリティ対策をしっかり実施している中小企業であっても推せない。セキュリティ対策の取組がわかりやすく示せればよい。SECURITY ACTION を宣言していると、どの対策を実施しているので情報漏えいのリスクは低い、などと説明できるとよい。（運輸）

3.3.2 サイバーセキュリティお助け隊サービス

サイバーセキュリティお助け隊サービスの認知度、活用意向として、以下のヒアリング項目を確認した。

① サイバーセキュリティお助け隊サービスの認知度

② 中小企業のサイバーセキュリティお助け隊サービスに対する評価（十分、適切、不十分）

③ 今後サイバーセキュリティお助け隊サービスに求める役割、取引先設定への活用可能性（取引先中小企業のインシデント対応可否の確認、実現に向けた課題など）

（1） サイバーセキュリティお助け隊サービス：認知度・活用意向

調査した先の発注元企業、団体の担当者においてサイバーセキュリティお助け隊サービスの認知度は高くなかった。

しかし、お助け隊サービスは中小企業のインシデント対応を支援するセキュリティサービスとして評価する意見が得られた。

ただし、お助け隊サービスを推進するためには、以下を考慮する必要があると考えられる。

- お助け隊サービスを導入すればセキュリティ対策が万全というわけではないことを理解する必要がある。「お助け隊サービス」に支援される側に留まらずレベルアップすることが重要である。
- インシデント発生時に「お助け隊サービス」に全て任せるという姿勢ではなく、サービス利用の目的や意義を認識し、自らが取引先に対しても説明できると良い。
- 「お助け隊サービス」はインシデント後の事後対応が中心の印象であり、取引において活用する場合は、お助け隊サービスが実現していることと取引・契約時の要求をすり合わせていくことが必要である。

1） 個社としての活用可能性

個社としてのサイバーセキュリティお助け隊サービスの活用可能性については、取引先の中小企業がインシデントに対処できない状況において本サービスで支援する、中小規模の取引先からセキュリティ対策の相談を受けた際、本サービスを紹介していくという形で、発注元企業として活用できるという意見も得られた。

一方、今回ヒアリングを実施した発注元企業では、取引先に中小企業が少なく、サービスの紹介はできるものの、自社の取引において積極的に利用するのではなく、再委託の際の条件として推奨していく形になるという意見もあった。また、所管省庁からのセキュリティ要求水準が高い業界の場合、本サービスを利用しているレベルでは基準を満たさないのではないかという意見もあった。

本制度の普及にあたっては、業界のサプライチェーンの構造を踏まえ、お助け隊サービスが実現するセキュリティ

対策が適切な中小企業、あるいはこのような中小企業との関係を考慮した上で適切に訴求していく必要があると考えられる。

2） 業界としての活用可能性

業界としてのサイバーセキュリティお助け隊サービス活用可能性については、加盟団体への周知や説明は可能であるという意見は得られたものの、取引時に積極的に本サービス活用を推奨することは難しいという意見が多かった。

（2） サイバーセキュリティお助け隊サービス：制度の在り方についての意見

ヒアリングにおいて、サイバーセキュリティお助け隊サービスを業界あるいは発注元企業として、利用促進を進めていくための課題が挙げられた。

1） 業界あるいは発注元企業としてのサービス推奨の難しさ

業界として有料サービス活用を推奨するとなると、企業に費用負担を求めることとなり、推奨した側にも責任が発生することから、あくまでも制度を周知するに留まる。

発注元企業としても、取引先において既にセキュリティ対策を実施している中、どのサービスを利用するかは各取引先の判断であり、特定のサービスを推奨することは難しい。

2） 制度普及の重要性

中小企業において本サービスはまだ認知度が低いことから、代理店や中小企業に近い団体、地域のセミナー等で説明する機会を設け、制度自体を広めることが重要である。

また、SECURITY ACTION 制度と連携し、自己宣言企業のインシデント発生時の対応支援をお助け隊サービスでサポートすることも有効ではないか。各業界のガイドラインへの対応に繋がるようなサービスを提供するものと位置づけることができれば、各業界の取組とも連携しやすい。発注元企業において、取引先でインシデントが発生した際に窓口が不明であったり、詳細な状況がわからない場合があることから、発注元企業からの問い合わせ窓口としての機能も果たせるとよいのではないか。検知・対応以外のフェーズも含めた更に幅広いサービスに

することで、より総合的なセキュリティレベルアップを提供できるとよい、等の意見も挙がった。

表 3-11 サイバーセキュリティお助け隊サービスの制度の在り方についてのご意見

ヒアリング結果
・ どのように対策を進めるかは各社判断となり、業界として「サイバーセキュリティお助け隊サービス」を推奨するよりは、紹介になると考える。（製造 A）
・ お助け隊サービスの活用の可能性はあると思うが、発注元企業としては、お助け隊サービスに支援される側に留まらずレベルアップすることが重要である。（製造 A）
・ セキュリティの弱点を可視化することが求められるが、そこにお助け隊サービスが適するならばよいと思う。（製造 A）
・ 制度自体は良いものだと思うが、制度を正しく、広く周知させることができていないのではないか。（製造 B）
・ 調達元企業は少なからず、調達先選定に課題を抱えているため、その課題を解決する手段となれば活用される。（製造 B）
・ 代理店や中小企業に近い団体、地域のセミナー等で説明する機会を設けて広めることが大切である。（製造 B）
・ 取引先の中小企業でセキュリティインシデントが発生し、自力で対処できない状況で本サービスに支援されるのであれば、利用は増えると考える。（製造 C）
・ 制御システム業界でサービスを活用するには、サービスメニューに制御システムセキュリティ対応が必要となる。工場のある機器にインシデントが発生した場合、周辺の別のメーカーの機器にも関連することがある。インシデント発生時にメーカーは支援に入るが、メーカーも自身の製品はわかるものの、他の製品はわからない。そのため、複数の機器メーカーの橋渡しのような役割を担うサービスがあると、インシデント対応がスムーズに進められ、エンドユーザは助かるのではないか。（製造 C）
・ 「サイバーセキュリティお助け隊サービス」を活用するには、SECURITY ACTION と連携し、SECURITY ACTION で自己宣言企業のインシデント発生時の対応支援をサイバーセキュリティお助け隊サービスでサポートするという形で展開することがよいと考える。（製造 C）
・ 中小規模の取引先からセキュリティ対策の相談を受けた際にサイバーセキュリティお助け隊サービスを紹介していきたい、活用できるかもしれないという意見が挙がった。（インフラ A）
・ 中小企業が利用しやすい価格帯が重要という意見もあったが、それはすでにサービス基準に取り込まれていると考える。（インフラ A）
・ 取引先と契約するための要件としてセキュリティ体制や防御方法を定めるが、「サイバーセキュリティお助け隊サービス」はインシデントが起きた後の事後対応が中心の印象を受けており、サービスが実現していることと、取引・契約の際に求めることをすり合わせていくことが必要と感じる。（インフラ B）
・ サービスの実用性はあると考える。中小規模の事業者には、担当者に専門知識が不足する場合やそもそも担当がいない場合があり、興味を持つ事業者はいるだろう。特に、インシデント対応支援は、導入を検討する事業者はいるのではないか。保険のような位置づけでの導入も考えられる。費用対効果次第で、導入を判断することとなる。（インフラ C）
・ 業界団体の役割としては、制度を加盟企業に周知するに留まると考える。周知を受けた企業が発注先へ周知して、制度を展開することは可能と考える。まずは、プライムとなる企業に制度を理解してもらうことが重要と考える。（防衛）
・ セキュリティ対策に関心を持っている企業は少ない。セキュリティ対策をこれから開始するような企業にとって良いサービスと感じた。これをきっかけに意識を高めてもらうことが望ましい。（防衛）
・ 有料サービスを業界団体として推奨するのは責任を負うことになるので、業界団体自身が説明を受け、メリットを理解できていないと責任を持って活用の推奨はしづらい。SC3 からの情報として、会員企業に情報提供していくことはできる。（情報通信）
・ 自社の一次取引先は中小企業が多くないため、サービスの紹介はするが、自社の取引において積極的に利用す

ることにはならないだろう。（情報通信）

- 会社の直接の取引先に活用するのは難しいという印象であり、再委託の際の条件として推奨というレベル感である。（情報通信）
- 所管省庁から企業に対しては、インシデント発生時に、インシデントの有無や対応方法を適切に判断できるように管理するよう指示されているため、攻撃を受けているかわからない、対処がわからないというレベルでは所管省庁のアセスメントにおいて基準を満たさないと考えられる。（金融）
- 現時点のサービス内容では、セキュリティ対策に意識があるという評価に留まる。（製薬）
- ある特定のサービスを取引先へ要求することはしていない。内部統制も踏まえ、どのサービスを利用するかは各取引先の判断となる。（製薬）
- 現時点のサービス内容では、セキュリティ対策に意識がある企業であるという評価に留まるのではないか。（製薬）
- SECURITY ACTION と同様、周知することは可能であるが、業界として推進するのは難しい。各企業に既にセキュリティ対策の取組があり、情報システム子会社がグループ会社に同じようなサービスを提供している場合もあるので、利用を求めていくのは厳しい。（運輸）
- 費用負担の課題もあり、できれば活用して欲しいという依頼にとどまる。政策として、費用の一部を国が負担するとなれば、導入のハードルが下がる可能性はある。（運輸）
- 「サイバーセキュリティお助け隊サービス」の利用企業には、インシデント発生時にしっかり対処するという印象は持つが、お助け隊サービスに全てお任せという姿勢であると、自分たちで何もできない企業という印象を与えかねない。お助け隊サービスに全てを任せるという姿勢ではなく、サービス利用の目的や意義を認識し、自らが取引先に対しても説明できるとよく、そのための知識が必要である。（運輸）

4. まとめ

調査結果を踏まえ、業界における情報セキュリティ対策強化や取引先のセキュリティ確保に向けて業界横断で抱える問題意識とそれに対する取組・アプローチ、参考となる先行した取組事例、及び SECURITY ACTION、サイバーセキュリティお助け隊サービスの活用可能性について整理を行った。

4.1 各業界のセキュリティ対策における問題意識と取組・アプローチ、参考となり得る取組事例

ヒアリング結果を踏まえ、各業界で抱えている問題意識と、それに対して有効と考えられる取組・アプローチを整理した。また、各業界で実施されていた情報セキュリティ対策のうち、他の業界にとって参考となり得る個別業界における取組事例を参考となり得る取組事例として整理した。

4.1.1 ガイドライン策定

（1） 問題意識

調査した業界の多くは、業界としてのセキュリティガイドラインを策定していたが、そのガイドラインを業界内でどのように普及、浸透させていくかは課題として挙げられていた。また、ガイドラインには抽象度の高いものも多く、個社で具体的な対策を進めるのが難しい場合もあった。

また、業界として統一的なセキュリティ基準となるガイドラインを策定したいが、参考とすべきガイドラインが複数あり、どれを参考にすべきかわからないや団体会員企業の中には、ガイドラインの分量が多すぎて全部確認できないという意見もみられた。

（2） 取組・アプローチ

業界ガイドライン等の「共通項」を抽出、取りまとめて発信することで、ガイドライン未整備の業界における参考とし、業界横断的な共通水準として活用することが有効と考えられる。

また、業界横断的な「共通項」を各業界に普及、浸透させることが効果的である。

（3） 参考となり得る取組事例

- 業界ガイドラインを策定し、サプライチェーンに属するすべての企業においてガイドラインを遵守させるべく、セルフチェック評価の実施と結果の集約を行う取組。
- エンタープライズ領域を対象に、最低限実施すべき 21 項目の要求事項と、50 項目の達成目標を提

示。

- 具体的な取組を進めるための様々なマニュアルやベストプラクティス集を策定し、会員向けに公開。
- セキュリティ対策要領（参考例）と解説を作成し、会員企業に公開。

4.1.2 インシデント情報等の情報共有と業界横断的な情報共有の取組

（1） 問題意識

ヒアリングした業界の多くでは、脆弱性情報やインシデント情報の情報共有の枠組みはあるものの、内容・タイミング含め、情報共有の方法が課題として挙げられた。

特に、製品の情報やサイバー攻撃に対応中の情報等、共有した情報から機微な内容が漏えいすることが懸念されていた。また、一部の企業では、入手する情報が多く、情報を取捨選択することが困難という意見もあった。

業界横断的な情報共有の取組については、実施しているのは一部の業界に限られている。他業界のセキュリティ対策の取組内容などは、業界横断的に共有されると自業界の取組の参考になるという意見が多かった。

（2） 取組・アプローチ

機微な情報が漏えいしないよう、情報共有の内容や共有タイミング、共有方法等を定めることが、業界横断的な情報共有の取組を進めるために有効であると考えられる。

業界横断的な情報共有を望まれる内容としては、インシデント情報や効果的なインシデントへの対応に関する情報が共有されることが望ましい。サプライチェーンのセキュリティ確保に関する取組（取引先への要求事項、契約書への記載内容等）も参考になるという意見もあり、インシデントという非常時の情報共有だけでなく、平時の有効な取組に関しても業界横断的に情報共有する内容として期待される。

製品単位でのセキュリティに関する情報や、各国の法規制・国際規格への対応等、業界横断的に共通認識を持つことが、業界におけるセキュリティ対策を進めるために有効である。

（3） 参考となり得る取組事例

情報共有の際には TLP を定め、どこの企業か特定できるような情報は伏せる形での情報共有を促進している事例が見られた。

複数の関係団体や、ISAC が横断的にインシデント情報等を共有する取組事例が見られた。

制御システム機器に関しては、機器ベンダの他、国際標準等を議論する際の官民の関係組織が参加する会議体があり、取組を進めるための情報共有が有効に働いていた。

業界内の取組では、ISAC においてインシデント情報を共有する仕組があり、インシデントが発生した企業が対応に困っていればサポートをしたり、質問があれば対応したりするような共助の取組を実施している事例も見られた。また、会員にセキュリティの対応状況に関するアンケートを実施し、他の会員の取組の参考となるよう、調査結果を会員に共有している事例も見られた。

オリンピック・パラリンピック開催の際に、強化期間を設けるなどの業界の取組について適宜発信し、関係者や社会に対して安心感を持ってもらうための取組事例もあった。

4.2 発注元企業が抱えている問題意識と取組・アプローチ、参考となり得る取組事例

ヒアリング結果を踏まえ、発注元企業が抱えている問題意識と、それに対して有効と考えられる取組・アプローチを整理した。また、他の企業にとって参考となり得る個別企業における取組事例を「参考となり得る取組事例」として整理した。

4.2.1 取引先選定

（1） 問題意識

要求レベルを満たせない取引先があっても、その取引先から調達できないと製品が成りたたない、業界における取引先が限定されており代替がきかない、といった事情もあり要請できないや、セキュリティ対策を要請しても価格反映できない点などが問題として挙げられた。

また、取引先には各々のセキュリティ基準があり、自社にも様々な業務の取引があることから、取引先選定に参照する統一的、あるいは具体的な要件設定が難しいという問題もあった。既存の契約済の取引先に対して、どのようにセキュリティ対策を求めていくかが課題という意見もあった。

（2） 取組・アプローチ

取引先に対して求めるセキュリティ要件について、業界横断的に共通項を定めていくことで、各業界あるいは各社において取引先に求める要件として活用可能になると考えられる。

（3） 参考となり得る取組事例

業界においてサイバーセキュリティガイドラインを策定しており、グループ企業においてガイドラインの遵守を求める取組が見られる。

4.2.2 契約締結

（1） 問題意識

セキュリティ要件を契約書のテンプレートとして含めている発注元企業は 1 社で、セキュリティレベルが高い情報等を扱う場合などに限り、特約等でセキュリティ要件を含めている企業もあった。また、仕様書や設計書で個別に要求しているケースもあるが、多くの企業では機密保持契約以外のセキュリティ状況をどこまで契約書に含めるかは課題として挙げられていた。

特に、契約書にセキュリティ要件を含めるためには契約書ひな形を変える必要があり、要件が詳しく記載できない。調達部門におけるセキュリティに対する理解と調整が必要となる。場合によっては、セキュリティ対策を求めることによるコストアップ分の負担についても考慮が必要であるという意見が多かった。

（2） 取組・アプローチ

契約書ひな形や、契約書や仕様書等、取引業務内容や調達の実態に応じて、実効性を担保するためのセキュリティ要件を示していくことは有効と考えられる。

（3） 参考となり得る取組事例

契約書のテンプレートにセキュリティ条項の項目として、インシデント報告や監査等の項目を含めている事例や、提供する情報とビジネスの重要性に応じたセキュリティ要件について、都度契約条項を法務部で審査している事例があった。

4.2.3 取引先のセキュリティ対策の実施状況の把握

（1） 問題意識

セキュリティ対策の実施状況の確認は、取引先のセキュリティの実態を確認するリソースや権限がない、資本関係がないところにはセキュリティ対策の要求ができない等、状況把握の難しさが問題として挙げられた。

（2） 取組・アプローチ

取引先からセルフチェックのアンケート形式で実施状況を提出してもらう等、取引先のセキュリティ対策の実施状況の把握について先行した取組を業界横断的に共有していくことが有効と考えられる。

（3） 参考となり得る取組事例

一部の企業では、自社グループ企業を対象に、独自のセキュリティ基準や確認方法等を定め、定期的な確認を行っている事例が見られた。

4.2.4 委託先のセキュリティ確保

（1） 問題意識

再委託先のセキュリティレベルが低い場合の情報漏えいのリスクは認識されており、多くの発注元企業では、再委託の有無は契約前などに申請し、委託先と同等の内容を再委託先にも求めているが、再委託先の実態までは権限もなく把握できない。委託先が海外の場合や発注元が発注先になるなど、複雑化している状況もある。

（2） 取組・アプローチ

取引先の監査にて委託状況のヒアリングやエビデンスの提出を求める等の委託先のセキュリティ確保について先行した取組を業界横断的に共有していくことが有効と考えられる。

（3） 参考となり得る取組事例

再委託先の監査は直接にできないが、取引先の監査で委託状況のヒアリングやエビデンスの提出を求めていた事例があった。

4.3 SECURITY ACTION、サイバーセキュリティお助け隊サービスの活用可能性

SECURITY ACTION 制度については、中小企業のセキュリティ対策の底上げや普及啓発には有効という意見もあった。本制度を取引条件等で活用するにあたっては、第三者機関による評価があると信頼性は向上するものの、制度普及のためには、中小企業にとって負担が少ないことが最も重要である。

サイバーセキュリティお助け隊サービスについては、中小企業のインシデント対応を支援するセキュリティサービスとして評価されていた。しかし、業界や発注元企業において特定のサービスを推奨していくことには難しい部分もある。一層の周知を進めることや、SECURITY ACTION 制度と連携するなど中小企業が利用しやすい仕組みを整えることも有効と考えられる。

4.3.1 SECURITY ACTION

（1） 活用の可能性

セキュリティ実施状況の自己申告では、人によって判断の基準が異なることもあるため、現状では制度の信頼性に不安がある。また、更新がないので、企業がどれだけセキュリティ対策を継続的に維持・運用できているかどうかがわからない。本制度の周知は可能であるものの、対策レベル・自己宣言制度であること等を踏まえると積極的に取引先選定基準として活用は難しい。

（2） 取組・アプローチ

以下の点に留意の上、本制度の在り方について検討、引き続き普及・促進に努める。

- 業界団体の取組を含め、商流に沿った形での普及展開が望まれる。
- 宣言中小企業において、セキュリティ対策意識のあることが確認できる意義がある。
- 入札・取引条件への活用にあたっては、第三者による認証や更新など、自己宣言企業のセキュリティ対策への取組の確実な実施が担保されるような仕組みが求められる一方で、まずは制度自体の普及のために中小企業にとって負担が少ないことも重要。

4.3.2 サイバーセキュリティお助け隊サービス

（1） 活用の可能性

中小企業のインシデント対応を支援するセキュリティサービスとして評価する声は多かったが、お助け隊サービスを導入すればセキュリティ対策が万全になるわけではないことを理解しておく必要がある。「お助け隊サービス」に支援される側に留まらずレベルアップすることが重要である。また、制度の普及を促す場合、本制度の周知することは可能であるものの、特定の有料サービスを推奨することは難しい。制度自体の認知度が高まり、もっと活用する企業が増えないと、制度活用は難しい。

（2） 取組・アプローチ

以下の点に留意の上、本制度の在り方について検討、引き続き普及・促進に努める。

- 業界団体の取組を含め、商流に沿った形での普及展開が望まれる。例えば、各業界ガイドラインへの対応に繋がるようなサービスと位置付けられることが望ましい。
- 業界団体のほか、代理店や中小企業に近い団体組織等を通じた普及が効果的。