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報告書（概要説明資料）

2022年5月

独立行政法人情報処理推進機構

目次

1.調査背景・目的 …… 3

2.調査概要 …… 4

3.調査対象 …… 5

4.調査結果 …… 6

- 4.1. 各業界のセキュリティ対策の取組状況と問題意識
- 4.2. 発注元企業の抱える問題意識
- 4.3. 既存の取組・制度の認知度、活用意向

5.まとめ …… 16

- 5.1. 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、先行した取組事例
- 5.2. 発注元企業の抱える問題意識と取組・アプローチ、先行した取組事例
- 5.3. SECURITY ACTION制度、サイバーセキュリティお助け隊サービスの活用可能性

1. 調査背景・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（IPA）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（SC3）の「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の共有」「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・取組が現状採られており、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」を実施した。

2．調査概要

■　調査概要は以下のとおり。

調査手法	ヒアリング調査（リモート形式）
調査対象者	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
調査実施会社	株式会社三菱総合研究所
調査項目	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. 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 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 4. 業界横断的に情報共有が望まれる内容、及び方法 5. 発注元企業の情報セキュリティ対策の取組 6. 取引先選定に関する問題意識 7. 契約締結に関する問題意識 8. セキュリティ対策の実施状況の把握に関する問題意識 9. 再委託に関する問題意識 10. 既存の取組・制度の認知度、活用可能性

3．調査対象

- SC3会員を中心に11分野の業界団体・ISAC※1等の団体にヒアリングを実施した。
- 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。

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。
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。

※1：Information Sharing and Analysis Centerの略。情報共有組織。

4. 調査結果
4.1.各業界のセキュリティ対策の取組状況と問題意識（ガイドラインの策定とセキュリティ対策状況の把握に向けた取組）

■ 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おり、業界団体として所属企業のセキュリティ対策状況の把握に向けた取組を開始しているところもあった。

■業界別ガイドラインの策定状況	
取組状況	• 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**：8分野 ※法律等に基づいて策定されたガイドライン：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：3分野（製造A、金融、製造C）
問題意識	• 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**であり、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、取組例の紹介等を含め別途情報提供しているのが実情。 • 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困難。 • 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**。

■業界別ガイドラインの業界内普及に向けた取組状況	
取組状況	• 業界団体として、業界別ガイドラインをベースに、業界内のサプライチェーンに属するすべての企業に対してガイドラインの実施状況を把握するための取組を行っている：1分野（製造A）
問題意識	• 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おらず、**ガイドラインをどのように業界内に普及、浸透させていくかが課題**。

4. 調査結果
4.1.各業界のセキュリティ対策の取組状況と問題意識（セキュリティ対策強化の取組）

■ その他の各業界における情報セキュリティ対策強化の取組としては、対策促進に向けた啓発コンテンツの作成、訓練／勉強会などを実施している例がある。

■情報セキュリティ対策強化に向けた取組状況	
取組状況	• 業界内でサイバーセキュリティに取組むためのワーキング・グループ（WG）を立ち上げ、**各種ガイドラインやセキュリティ対策促進に資する啓発コンテンツ等を作成し、会員内で共有**している。（金融） • 米国国立標準技術研究所（NIST※2）のサイバーセキュリティフレームワーク（CSF※3）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。（インフラB） • セキュリティ対策強化に向けて**インシデント発生時の報告訓練等の機会を提供**している。（インフラC） • 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。（運輸）
問題意識	• 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、対策を求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意識が低い**場合がある。

※2：National Institute of Standards and Technologyの略。
※3：Cyber Security Frameworkの略。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）」

4. 調査結果
4.1.各業界のセキュリティ対策の取組状況と問題意識（インシデント対応）

■ ヒアリングした業界では、各企業においてインシデント対応規程を策定、情報収集を実施しているところが多い。業界内で情報共有を行うにあたっては、共有範囲をTLP※4で定めて実施している例もあった。

■インシデント対応	
取組状況	• 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（監督省庁や業界団体への報告など）を設けている例がある。：5分野（インフラA、B、C、製造A、金融） • 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。：7分野（インフラA、B、C、製造A、金融、製薬、運輸） • インシデント発生企業が**対応に困っている場合にはサポート**を実施し、質問があれば個別に対応するような共助の取組を実施している。：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。：3分野（金融、製造C、製薬） • 各企業単位でインシデント対応規程を策定、実施している。：11分野（全分野）
問題意識	• 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。

※4：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。

4. 調査結果
4.1.各業界のセキュリティ対策の取組状況と問題意識（業界横断的に情報共有が望まれる内容）

■ 複数の業界間で情報共有を図る取組を実施している例もあった。
業界横断的に情報共有が望まれる内容としては、インシデントへの対処方法などの情報のほか、他業界におけるセキュリティ対策の取組事例等が挙げられた。

■業界横断的に情報共有が望まれる内容	
取組状況	• **複数の関係団体やISACが業界横断的に情報共有する取組を実施している。**：4分野（インフラB、金融、製造C、運輸）
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と考えられる。 • **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。
問題意識	• 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。

4. 調査結果
4.2.発注元企業の抱える問題意識（取引先に求めるセキュリティ対策）

■ 取引先に対して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例もあったが、個別の取引に際してそれぞれセキュリティ対策要請を行うことには取引先選定上の優先度やリソース等で難しい側面がある。

■取引先選定に関するセキュリティ対策取組状況と問題意識	
取組状況	• **取引先に対して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。：４社
問題意識	• 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、といった事情もあるので対応が困難。また、セキュリティ対策を要請しても価格に反映できないので、要請が困難。 • 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い。機密情報の管理など、どちらの基準にも整合的な抽象度の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困難。 • 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、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。

4. 調査結果
4.2.発注元企業の抱える問題意識（契約締結と取引先のセキュリティ対策実施状況把握）

■ 契約書中に具体的なセキュリティ対策に関する条項を含めている例は少なく、特に資本関係のない取引先については実施状況についても把握が困難。

■取引先との契約締結に関するセキュリティ対策取組状況と問題意識	
取組状況	• ヒアリング先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：1社** 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：3社 • 個別のセキュリティ要件については発注仕様書や設計書で示している場合が多い。
問題意識	• 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。 • **どこまで契約書に盛り込むことが可能かわからない。** • 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。 • 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等も課題。
■セキュリティ対策実施状況の把握に関する取組状況と問題意識	
取組状況	• **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**している例があった。 • 取引先を直接訪問し、セキュリティ対策の実施状況を確認している（数年に１回程度）例もある。
問題意識	• **取引先に要請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。** • 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。** • 取引先のセキュリティ対策の実態を確認するリソース、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の要請・確認ができない等、**実施状況把握の実効性の確保が課題。**

4. 調査結果
4.2.発注元企業の抱える問題意識（再委託先のセキュリティ対策）

■ 再委託先からの情報漏えいのおそれがあることは認識されていながらも、対策状況の確認はもちろん、具体的な対策を要請するのが難しいのが実情。

■再委託先に関するセキュリティ対策取組状況と問題意識	
取組状況	• 再委託が行われ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例もあったが、再委託先については管理できないのでセキュリティ対策実施を要請できていないという声もあった。 • 発注元企業として、再委託実施の有無は契約時や判明時に申請してもらうことで把握している。 • 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広く認識されている。
問題意識	• 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。

4. 調査結果
4.3.既存の取組・制度の認知度、活用意向（1/3）

■SECURITY ACTION：認知度・活用意向

- ヒアリング先の発注元企業、業界団体の担当者においては、SECURITY ACTION制度の認知度は高くなかったが、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あった。
- ヒアリング先からは、中小企業も様々なレベルがあるので、そのうち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なるとのコメントがあった。

■個別の企業における取引・入札条件等としての活用可能性

- 調達部門の要求とマッチすれば、活用の可能性はあり得る。
- SECURITY ACTION制度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との感触。
- 既に取引先のセキュリティ対策に関し取組を進めており、新しく本制度を活用する必要性は少ない。

■業界における取引・入札条件等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。
  （例：業界団体やISAC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。）
- 本制度の周知は可能であるものの、セキュリティ実施状況の自己申告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業界団体として推奨できるかどうかは難しい。

4. 調査結果
4.3.既存の取組・制度の認知度、活用意向（2/3）

■SECURITY ACTION制度の在り方についての意見

- 本制度を取引条件等で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が必要。また、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。

■SECURITY ACTION制度に関して

- 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と言わざるを得ない。
- **更新がない**ので、企業がどれだけセキュリティを継続的に維持・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、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。
- 宣言の根拠となる情報を提示できるかどうか。
- 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もあり、自己宣言でも問題ない。
- SECURITY ACTIONを宣言していることにより、**最低限セキュリティ対策意識のあることが確認できるのであればよい。**

■制度の普及、取得企業の増加に関して

- 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、まず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。
- **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重要。**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。
- 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。

4. 調査結果
4.3.既存の取組・制度の認知度、活用意向（3/3）

■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

- ヒアリング先においては、**お助け隊サービスの認知度は高くなかった**が、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が多かった。
- 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などがあってもよいとの声があった。

【留意点】
- 前提として、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**。
- インシデント発生時に「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良い。

■業界あるいは発注元企業として本サービスを推奨するにあたっての課題

- 業界として本サービス活用を推奨する場合、費用負担をどうするかが問題となり得る。

■サイバーセキュリティお助け隊サービス制度の普及・制度の在り方に関して

- 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するものとなるのではないか。
- 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付けることができれば、各業界の取組とも連携しやすい。
- 発注先企業において、インシデントが発生した際の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。
- 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**ことが重要。

5. まとめ

5.1. 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。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業界横断的に情報発信していくことも有効であると考えられる。

	各業界のセキュリティ対策での問題意識	取組・アプローチのイメージ
業界ガイドライン	• 業界として統一的なセキュリティ対策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。** • **セキュリティガイドラインをどのように業界内に普及、浸透させていくか**が問題。	• **業界ガイドライン等の「共通項」を抽出**、と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。 • **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。
情報共有	• インシデント情報共有の枠組みはあるものの、**内容・タイミング含め方法が難しい。** • **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。	• 効果的なインシデント情報の共有をはじめ、**参考となるような各業界の取組・プラクティスを業界横断的に共有**することが有効と考えられる。

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。
- 情報共有の際にはTLPを定め、企業を特定できるような情報は伏せる形で情報共有を促進。
- 複数の関係団体や、ISACが業界横断的にインシデント情報等を定期的に共有。

5.2. 発注元企業の抱える問題意識と取組・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。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情報発信していくことも有効であると考えられる。

	発注元企業での問題意識	取組・アプローチのイメージ
契約締結	• 取引先にどこまでセキュリティ対策を要請するか、要件を**どこまで契約書に盛り込むことが可能か**わからない。	• **業界ガイドライン等の「共通項」を抽出、業界横断的な対策要件を発信**するとともに**契約書ひな形等を提供**していくことが有効と考えられる。
取引先の実施状況の把握	• 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請・確認ができない等、**実施状況把握の実効性確保**が問題。	• 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、状況把握についての**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。

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関連項目として、インシデント報告や監査等の項目を含めている。 • 提供する情報内容とビジネスの重要性に応じたセキュリティ要件を都度設定し、契約条項を法務部で審査している。 • 再委託先の監査は直接できないものの、取引先の監査の過程で委託状況のヒアリングの実施やエビデンスの提出を求めている。 • グループ企業に対してセキュリティ基準や確認方法等を定め、定期的に確認を行っている。

5. まとめ

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

■ヒアリング結果を踏まえ、例えば以下の点にも留意の上、これら制度について在り方を検討、引き続き普及・活用促進に努める。

- **SECURITY ACTION制度：**
  - 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必要な一方で、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。

- **サイバーセキュリティお助け隊サービス制度：**
  - 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。