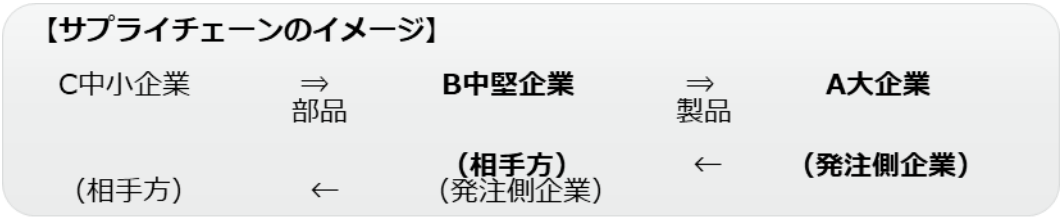
【想定事例】

発注側企業からの「サプライチェーン強化に向けたセキュリティ対策評価制度」４つ星相当の対策の実施要請を踏まえ、発注側企業と取引の相手方とが円満に価格交渉を行うためのプラクティス

（B 中堅企業に対する対象製品の発注側企業は A 大企業のみ）

※　本想定事例は、発注者である大企業や中堅企業と、その取引の相手方となる（中小等の）企業との間でのプラクティスを想定して作成



(1) 大企業からの「４つ星」相当の対策の実施要請

発注側企業である A 大企業は、サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発している近年の状況を踏まえ、供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃などを想定し、取引の相手方である B 中堅企業に対し、

① 製品の仕様とは別途、組織体として、組織ガバナンス・取引先管理、ネットワークやパソコンの不正通信監視や防御といったシステム防御・検知、インシデント対応等包括的な対策を実施すること（＊）、

② B 中堅企業の取引の相手方である C 中小企業に対し、上記①と同様の対策を講ずること、

を要請することとした。

（＊）要請内容は、国において検討中の「サプライチェーン強化に向けたセキュリティ対策評価制度」（サプライチェーン対策評価制度）中の「４つ星」に相当。

(2) 実施要請に当たってのパートナーシップの構築

A 大企業は、サイバーセキュリティ対策の実施要請に当たっては取引の相手方と協力関係を構築することが重要であると考え、B 中堅企業を支援するため以下の取組を実施した。また、C 中小企業も同じサプライチェーンに属するため、支援の対象とした。

① 経営層の関与の下、B 中堅企業及び C 中小企業と良好な関係を構築し、サイバーセキュリティ対策の実施要請と価格交渉を円滑に実施していく上での自社の一般的な対応方針（必要な情報収集をすること、協議を求められた場合の対応、丁寧な対話の実施など）を定めた。

② B 中堅企業及び C 中小企業を含めた取引先に対する説明会を開催し、サイバーセキュリティ対策が自社のみならず取引先にまで影響を及ぼすことを説明した上で、サプラ

イチェーン対策評価制度に基づいて講じるべきサイバーセキュリティ対策を説明した。具体的には、従業員に対する情報セキュリティ教育や情報セキュリティポリシーの策定については、独立行政法人情報処理推進機構（IPA）が提供するコンテンツやひな形を提示して具体的方法を教示した。また、システム防御策については、サイバーセキュリティお助け隊サービスを導入することで必要な対策を最小限の費用で実施できることなどを説明した。加えてC中小企業に対しては、サイバーセキュリティお助け隊サービスの導入に当たりIT導入補助金を活用できることも説明した。

③ その後もサイバーセキュリティ対策の実施や価格交渉の協議を円滑に行うため、年に一度、B中堅企業及びC中小企業とのコミュニケーションの場として説明会を開催することとし、その旨を②の説明会で周知した。

(3) サイバーセキュリティ対策の実施要請と費用負担の考え方の説明

A大企業は、(2)②及び③の説明を行った上で、B中堅企業に対し(1)のとおり標準的なサイバーセキュリティ対策の実施要請を行った。その際に、費用負担の考え方やセキュリティ対策に要した費用も価格交渉の対象となることを説明し、価格交渉の要請があれば積極的に対応することを周知した。また、サイバーセキュリティ対策の実施要請を受けたB中堅企業は、取引先であるC中小企業に対して、費用負担の考え方やセキュリティ対策に要した費用も価格交渉の対象となることを説明した上で同様の要請を行うとともに、価格交渉についても要請を受けて積極的に対応することを周知した。

(4) 実施要請を受けた取引の相手方の対応

B中堅企業は、サイバーセキュリティ対策の必要性は理解していたものの、要請されたセキュリティ対策のうち、システム防御策については、B中堅企業では従業員が使用するパソコン100台とつながっている業務システムがあり、これまでウイルス対策ソフトは導入していたものの、それ以外の対策は講じていなかった。パソコン100台と業務システムに新たにネットワーク監視機器といったシステム防御策を講じようとすると高額になると思い、導入を躊躇していたが、A大企業からの説明を受けてサイバーセキュリティお助け隊サービス（２類サービス）を導入したところ、初期導入費用、月額運用費用とも安価に抑えることができた。

C中小企業は、これまでサイバーセキュリティ対策を実施しておらず、またサイバーセキュリティに関する知識も乏しかったものの、A大企業やB中堅企業からの説明を受けて理解できたので、要請されたセキュリティ対策のうち、従業員に対する情報セキュリティ教育や情報セキュリティポリシーの策定については、A大企業やB中堅企業からの説明に基づき、IPAホームページで提供されているコンテンツによって従業員に対するセキュリティ教育を実施し、また、IPAホームページで提供されているひな形に基づいて情報セキュリティポリシーの策定を行った。その結果、これらの対策については費用が発生しなかった。一方、システム防御策については、C中小企業では業務システムのほかパソコン30台を導入しているところ、A大企業やB中堅企業からの説明を受けて

サイバーセキュリティお助け隊サービス（１類サービス）を導入したことにより、初期導入費用、月額運用費用とも安価に抑えることができた。また、A 大企業やB 中堅企業からの助言を受けてIT 導入補助金も活用したことにより、最初の２年間分の費用を半額とすることができた。

(5) 価格交渉

B 中堅企業はA 大企業に対し、C 中小企業はB 中堅企業に対し、実施したサイバーセキュリティ対策に要した費用について、A 大企業からの説明に基づいて具体的負担分を検討し、それぞれ価格交渉の要請を行った。**B 中堅企業及びC 中小企業ともに、A 大企業から丁寧な説明を受けていたことにより、サイバーセキュリティ対策の必要性や対策内容について理解が得られており、費用負担も最小限で抑えることができた。双方とも協力関係を構築できたことにより、価格交渉は円満に合意することができ、その結果を双方が書面に記録して保存した。**

(6) 実施要請を行っていないB’中堅企業へのC 中小企業の対応

ところで、C 中小企業には、その取引先としてB 中堅企業以外にもB’中堅企業がいる。

【サプライチェーンのイメージ】

C中小企業　⇒　B中堅企業（発注者）　⇒　A大企業
⇒　B’中堅企業（発注者）*Cに要請していない　⇒　X大企業

C 中小企業は、サイバーセキュリティ対策の実施要請を行っていないB’中堅企業とも価格交渉を行いたいと考えている。そこで、公正取引委員会の相談窓口や、公益財団法人全国中小企業振興機関協会の取引かけこみ寺（中小企業庁の委託事業）を利用して、セキュリティ対策の実施による物件費や人件費の上昇分を、サイバーセキュリティ対策の実施要請を行っていない企業に対して価格交渉するに当たって留意することについて相談し、価格交渉の考え方や、価格交渉に応じてもらえない場合に取ることが望ましい行動（価格交渉をしない理由を書面や電子メール等で回答を求めることなど）について説明を受けた。

C 中小企業は、相談窓口や取引かけこみ寺から得られた助言に基づき、価格交渉に必要な積算根拠の資料を収集し、またB 中堅企業との価格交渉で用いた費用負担の考え方を整理して、**B’中堅企業に対し、自ら価格交渉を申し入れ、サイバーセキュリティ対策の必要性や、B’中堅企業との売上高に占める同社との取引割合などを勘案した費用負担の考え方などについて説明した。**

B’中堅企業はC 中小企業の考えを理解し、**価格交渉は円満に合意に達することができ、その結果を双方が書面に記録して保存した。**

（参考）

〇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

上記ページには、ガイドラインのほか、情報セキュリティ関連規程のひな形や、情報セキュリティのハンドブックもあります。

〇サイバーセキュリティお助け隊サービス

https://www.ipa.go.jp/security/otasuketai-pr/

24 時間の見守り・緊急時の駆付け支援・相談窓口をワンパッケージかつ安価（例：初期導入費用 50 万円以内、月額運用費用 1 万円以内など）で提供する、国が認定したセキュリティサービス。上記ページ内の「サービスを比較する」から、サービスを提供する事業者のホームページにアクセスでき、事業者のホームページから問合せや申込みができます。

〇IT 導入補助金

https://it-shien.smrj.go.jp/

「IT 導入補助金セキュリティ対策推進枠」により、サイバーセキュリティお助け隊サービスの導入費用の一部について補助を受けることができます。

〇公正取引委員会の相談窓口

優越的地位の濫用の考え方についての相談 ｜ 公正取引委員会

https://www.jftc.go.jp/soudan/soudan/yuetsutekichii.html

取適法に関する相談窓口 ｜ 公正取引委員会

https://www.jftc.go.jp/soudan/soudan/shitauke.html

〇公益財団法人全国中小企業振興機関協会の取引かけこみ寺

https://www.zenkyo.or.jp/kakekomi/

※取引かけこみ寺は、中小企業庁の委託事業です。

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（令和４年 10 月 28 日　経済産業省・公正取引委員会）を踏まえた想定事例について（解説）

- 発注者側である大企業が取引先である中小企業等に対してサイバーセキュリティ対策の実施要請をするに当たって、一定のサイバーセキュリティ対策を実施していることを取引の条件とすること等については、既に、「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」（令和４年 10 月 28 日　経済産業省・公正取引委員会）において、一定の考え方が示されているところです。

- 他方で、サプライチェーンの弱点を突いたサイバー攻撃が増加しており、その被害が大企業に限らず中小企業等にも及び、中小企業等のセキュリティ対策強化が求められています。そのような中で、発注者側である大企業の要請に基づき取引先である中小企業等が実施したサイバーセキュリティ対策にかかる費用について、どのように価格交渉や費用負担がされるのかについて、独占禁止法や取適法との関係で明確な整理を行うため、今般、【別添】のとおり、想定事例を整理しました。

- この想定事例に関する解説を、本資料において整理しておりますので、御活用いただけますと幸いです。

第１　はじめに

１　パートナーシップ構築に当たって

近年、大企業から中小企業までを含むサプライチェーン上の弱点を狙って、攻撃対象への侵入を図るサイバー攻撃が顕在化・高度化しています。発注者側である大企業（発注側企業）の取引先である中小企業等（取引の相手方）において、サイバー攻撃に対する対策が不十分である場合、サイバー攻撃の影響は、当該取引の相手方の事業活動停止にとどまらず、取引の相手方から製品やサービスを調達している発注側企業の事業活動にまで影響を及ぼすことになります。

そのため、サイバーセキュリティ対策は、自社に限らず、その取引先の安心と安全を守る観点から、サプライチェーン全体として取り組まなければならないものと言えます。このような観点から、発注側企業と取引の相手方がパートナーシップを構築し、サイバーセキュリティ対策を強化していく必要があります。

２　経営者の責務としてのサイバーセキュリティ対策

パートナーシップ構築に当たり、まず、発注側企業や取引の相手方が認識すべきことは、サイバーセキュリティ対策は経営者が責務として行うものであるということです。

経営者は、サイバーセキュリティ対策が適切でなかったため、組織が保有する情報の漏えいなどにより企業や第三者に損害が生じた場合、善管注意義務や任務懈怠に基づく損害賠償責任を問われ得るなど、法的責任やステークホルダーへの説明責任を負うことになります。

また、サイバーセキュリティ対策は、単なるリスク回避のための手段ではなく、企業価値を高めるための「投資」（将来の事業活動・成長に必須な費用）と位置付けることができます。ここで言う投資とは、これにより直接的な収益を算出できるものではないものの、企業活動におけるリスクや損失を減らすことによって企業の生産性を向上させ、企業の価値を維持・増大していくために必要不可欠なものと言えます。

経営者は、企業の価値を維持・増大していく観点から、サイバーセキュリティリスクを組織の経営リスクの一環として織り込んで把握・評価した上で、自社にとって最適となるサイバーセキュリティ対策を実施する必要があり、これは、企業として果たすべき社会的責任であるとともに、経営者としての責務でもあります。

こうした趣旨は、サイバーセキュリティ基本法において、事業者の責務として、自主的かつ積極的にサイバーセキュリティの確保に努めるものとすること等が規定されていることからも明らかです。

３　サイバーセキュリティ対策の実施要請の背景

「１」で述べたとおり、取引の相手方におけるサイバーセキュリティ対策が不十分である場合、当該企業を踏み台にして発注側企業が攻撃されるおそれがあること

などから、サイバーセキュリティ対策は、サプライチェーンを構成する全ての企業で行う必要があります。

一方で、独立行政法人情報処理推進機構（IPA）が実施した実態調査によれば、中小企業等の中には、サイバーセキュリティ対策について、「必要性を感じていない」との回答が相当数を占めるなど、中小企業等に対するサイバーセキュリティ対策への理解が十分に進んでいない実態があります。

中小企業等においてサイバーセキュリティ対策が実施されるためには、発注側企業が当該対策の必要性や対策の内容を訴えていく必要があり、このような背景から、サイバーセキュリティ対策の実施要請がされています。

第２　想定事例の解説

１　サイバーセキュリティ対策の実施要請と独占禁止法等の関係整理を要する場合

発注側企業から取引の相手方に対してサイバーセキュリティ対策の実施要請をする場合としては、①取引の目的である製品・サービスにおけるサイバーセキュリティ対策を要請する場合、②取引の相手方における組織体としてのサイバーセキュリティ対策を要請する場合があると考えられます。

①の場合、一般的には、要請される具体的なセキュリティ対策の実施内容は製品・サービスに関する仕様書や契約書に明記され、それらを前提として製品・サービスの原価の一部として価格交渉が行われ、負担すべき費用が決定されることになると考えられます。

②の場合、発注側企業から取引の相手方に対し、①の場合に限らず、サプライチェーン全体のリスクを低減させ、付加価値の向上に取り組む観点から、取引の相手方における組織体としてのサイバーセキュリティ対策の実施要請がされることが考えられます。このような場合、発注側企業の要請に基づき取引の相手方に発生したサイバーセキュリティ対策費用についてどのように価格交渉が行われ、価格に転嫁されるのかについて、「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」（令和４年 10 月 28 日　経済産業省・公正取引委員会）では必ずしも明らかにされておらず、発注側企業からは価格交渉のイメージができないといった意見が寄せられていました。

そこで、今般、経済産業省及び公正取引委員会において、サプライチェーン全体のサイバーセキュリティ向上を後押しする観点から、②の場面を対象に、取引当事者間で十分に協議が行われたものと考えられる想定事例を作成することとしました。このような行為を取った場合、通常は私的独占の禁止及び公正取引の確保に関する法律（通称：独占禁止法）及び製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律（通称：取適法）（※）上の問題は生じないと考えられるものです。

＊　*令和７年 12 月 31 日までは「下請代金支払遅延等防止法（下請法）」*

２　想定事例の解説

（１）サイバーセキュリティ対策の実施要請の内容（想定事例(1)の解説）（国において検討中のサプライチェーン強化に向けたセキュリティ対策評価制度との関係）

発注側企業と取引の相手方がパートナーシップを構築し、サイバーセキュリティ対策を強化していく必要があること、サイバーセキュリティ対策は経営者が責務として行うものであることは、第１で述べたとおりですが、サイバーセキュリティ対策の実施要請に合理的な必要性がないにもかかわらず対策を強制するものである場合など、要請の方法や内容によっては、優越的地位の濫用として、独占禁止法や取適法上問題となります。

この点、想定事例においては、発注側企業は、国が検討しているサプライチェーン強化に向けたセキュリティ対策評価制度（サプライチェーン対策評価制度）に基づく対策を要請しています。サプライチェーン対策評価制度とは、サプライチェーンにおける、取引先へのサイバー攻撃を起因とした情報流出、製品・サービスの提供途絶及び取引ネットワークを通じた不正侵入等のリスクに対するセキュリティ対策の状況を確認することを目的として、発注側企業が取引の相手方に対し、サイバーセキュリティ対策の適切な段階を提示して実施を促し、取引の相手方が、提示された対策を実施するものであり、サプライチェーン全体としてサイバーセキュリティ対策を可視化することによって、取引の安定化・円滑化を図ろうとするものです。

このような、国において検討中のサプライチェーンにおけるレジリエンス強化のための評価基準に基づいた対策を実施することは、サプライチェーンに属する企業にとって必要性かつ合理性のあるものと考えられますので、取引の相手方に合理的範囲を超えた負担を課しているものではないと考えられます。

（２）価格交渉の前提としてのパートナーシップの構築（想定事例(2)及び(3)の解説）

独占禁止法や取適法をはじめとする取引適正化の観点からも、発注側企業と取引の相手方との間で、適時のタイミングで価格交渉を行えるよう、日頃から十分なコミュニケーションを行っていくことが大切です。

先述のとおり、サイバーセキュリティ対策は、情報漏洩などから生じる経営リスクを回避する観点からも、サプライチェーン全体で取り組まなければならない問題です。しかしながら、中小企業等の中には、第１の３で述べたとおり「必要性を感じていない」と考えている場合もあり、そうした取引の相手方に対しては、一方的な要請をするだけでは十分な理解を得ることが難しい場合も考えられます。

そこで、発注側企業には、取引の相手方に対して、サイバーセキュリティ対策に関する説明会を開催してその必要性を説明して理解を求める、参考事例として具体

的な対策方法を提示する、価格交渉があった際は積極的に応じるなど、単にサイバーセキュリティ対策の実施要請を行うだけでなく、その必要性や具体的な方法、そして価格交渉には積極的に応じる姿勢を示した上で、価格交渉の依頼があった場合には、交渉のテーブルについた上で適切なコミュニケーションを取り、真摯に対応することが大切であると考えられます。また、そうした取引の相手方との対話・協議を適切に行うことを明確に定めた自社の取組方針について、経営トップ自ら、その考え方を示して社内外に周知しておくことも必要です。

なお、想定事例では一般的なパートナーシップ構築の考え方を示すにとどめていますが、要請するサイバーセキュリティ対策の内容や、取引の相手方の対策状況などに応じて、取引の相手方に対する支援を強化するなど、コミュニケーションを一層深めていく必要があります。

（３）サイバーセキュリティ対策実施費用の間接経費への計上と価格交渉（想定事例(5)の解説）

取引の相手方が、組織体としてサイバーセキュリティ対策を実施する場合、一般に、実施する対策の内容が製品・サービスに関する仕様書や契約書に明記されていないことが考えられます。サイバーセキュリティ対策を実施する場合は必ずしも追加費用が発生する訳ではありませんが、例えば、セキュリティ機器やサービスを導入して継続的にシステム監視を行うこととした場合や、セキュリティ専門人材を雇用した場合などは、追加的に費用が発生する場合があります。当該費用は、製品・サービスの直接経費ではなく、労務費や一般管理費といった間接経費として計上されることが想定されます。

取引の相手方は、この間接経費の増加について、サイバーセキュリティ対策が自社の利益にもつながり得ることや、発注側企業における自社からの仕入割合などを勘案した上で、価格交渉を行うことが考えられます。発注側企業としては、取引の相手方から、製品・サービスの価格への間接経費の転嫁について価格交渉の申出があった場合には、その申出に応じる必要があります。

このため、想定事例においては、このような考え方を念頭に、発注側企業からのサイバーセキュリティ対策の実施要請、当該対策の実施や実施に伴う費用の発生、そして価格交渉の実施及び負担すべき費用の決定について整理し、発注側企業と取引の相手方が結論において円満に合意し、内容について書面などに記録して保存することとしています。

（４）対策実施の要請を行った発注側企業以外の発注側企業に対する価格交渉（想定事例(6)の解説）

特定の製品・サービスを扱うサプライチェーンの中に、サイバーセキュリティ対策の実施要請を行った発注側企業と行っていない発注側企業があり、両企業に共通する取引の相手方がある場合、その取引の相手方としては、サプライチェーン全体

のリスクを低減させ、付加価値の向上に取り組む観点から、当該製品・サービスに関連する費用に鑑みて、サイバーセキュリティ対策の実施要請を行った発注側企業のみならず、行っていない発注側企業に対しても、価格交渉を行う場合があると考えられます。

このような場合、取引の相手方から積極的に価格交渉を申し入れることも必要になります。しかしながら、取引の相手方にとって、要請を行っていない発注側企業に価格交渉の申入れをすることは容易ではありませんので、このような場合には、公的機関や中小企業支援機関に相談することも大切です。公正取引委員会では相談者からの相談に対応する一般相談窓口や事前相談制度等があり、また、公益財団法人全国中小企業振興機関協会では取引の相手方からの相談に無料で対応する取引かけこみ寺（中小企業庁の委託事業）（※）があります。必要に応じて、このような相談先を活用することも大切です。

また、発注側企業は、取引の相手方から価格交渉の申入れがあった場合には、直接的にサイバーセキュリティ対策の実施要請を行っていない場合でも、積極的に交渉に応じる必要があります。

＊　*令和７年 12 月 31 日までは「下請かけこみ寺」*

第３　おわりに

個別の取引や価格交渉に当たり、事業者等がこれから行おうとする行為について独占禁止法や取適法との関係で疑問が生じた場合には、公正取引委員会に相談することができます。

公正取引委員会への相談については、「事業者等の活動に係る事前相談制度」（事前相談制度）による相談と、「事前相談制度」によらない相談（一般相談）の二つの方法があり、事業者等はいずれかを選択することが可能です。

事前相談制度は、公正取引委員会が所管する法律（独占禁止法、取適法又はフリーランス・事業者間取引適正化等法）の運用の透明性を高め、相談制度の一層の充実を図るため、事業者や事業者団体が行おうとする具体的な行為が、公正取引委員会が所管する法律の規定に照らして問題がないかどうかの相談に応じ、書面により回答するものです。相談の際には、申出者名並びに相談及び回答内容が公表されることに同意することが必要となります。

また、公正取引委員会では、相談者の負担軽減、相談者・相談内容の秘匿性等に配慮し、一般相談も受け付けています。一般相談は、電話や E-mail 等で相談内容を説明し、公正取引委員会からの回答は原則として口頭で行われるもので、迅速に対応するとともに、相談内容等については非公表とされています。

なお、これまでの相談事例については公正取引委員会ホームページにおいて「相談事例集」として公表されていますので、必要に応じて参照していただくようお願いします。

サプライチェーン全体としてサイバーセキュリティ対策を強化していくためにも、是非このような制度の積極的な活用をお願いします。