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

－ 調査報告書 －

2017年3月30日

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

This page is intentionally left blank

目次

1. 調査の背景と目的

近年における IT システムや提供する製品・サービスにおいて、設計・開発・製造・運用・保守・廃棄に至るまでの一連のプロセスにわたり、業務の一部を系列企業やビジネスパートナー等へ外部委託することは一般的となっている。このような外部委託者が関与する供給の連鎖を本報告書では「サプライチェーン」という。事業の IT 化やグローバル化等の事業環境の急激な変化に伴い、サプライチェーンはより一層多様化することが見込まれる。

外部委託した業務の一部が別の組織に再委託されるなど委託関係が重層的に連鎖する可能性を考慮すると、委託先の情報セキュリティ対策状況の把握・評価や、委託先で発生する情報セキュリティに関するリスクの管理、委託元から要求される情報セキュリティに関するリスクの管理等の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（以下「情報セキュリティに関する SCRM※1」という。）の重要性が高まることとなる。

しかしながら、通常は、委託先には委託元組織の直接のガバナンスは及びにくいため、情報セキュリティに関する多種多様なリスク※2 の管理は困難であり、委託関係が重層的に連鎖する場合は、さらに困難さを増すことになる。

そこで、情報セキュリティに関する SCRM が扱うべきリスクや課題を整理するため、我が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、本調査を執り行うものとする。

なお、企業における委託関係やサプライチェーンにはさまざまな形態があり、本調査だけで上記の目的を全て充足することには自ずと限界があることから、本調査はあくまで上記の目的実現に向けた調査実施の第一段階として位置付けるものとし、情報セキュリティに関する SCRM の全体概要を把握し、論点を明らかにすることを目指す。

※1　SCRM：Supply Chain Risk Management

※2　本調査においては、これらのリスクについて、例えば、サイバー攻撃による機密情報の窃取（漏えい）、IT システム関連機器に対する不正改造、ソフトウェアへの不正なプログラムの埋め込み、設計不備・開発製造不備・運用不備による脆弱性混入、クラウド事業者の BCP 対策不足に起因するサイバー攻撃で停止した IT システムの復旧不備、クラウドサービス利用終了時のデータ消去不徹底による機密情報の漏えい等の情報セキュリティ上のリスクを前提とする。

2. 調査の概要

2.1. 調査の全体像と各調査の概要

本調査は、文献調査、アンケート調査、ヒアリング調査の 3 部構成で実施した。

各調査の流れを図表 2-1 に示す。また、実施概要について以下に記載する。

調査全体の流れとしては、初めに文献調査によって国内外の情報セキュリティに関する SCRM の現状認識や取り組み、更に情報セキュリティに関する SCRM におけるリスクや課題を整理し、文献調査の結果を踏まえて国内企業の情報セキュリティに関する SCRM の取り組み向上に資するような情報を得るために調査仮説を構築した。

次に、構築した調査仮説を検証するために、国内企業のセキュリティ部門担当者や調達部門担当者等を対象にしたアンケート調査を実施した。アンケート調査では、調査仮説に関連した設問を作り、アンケートの集計結果から仮説検証を実施した。

また、文献調査とアンケート調査結果をもとに、日米の情報セキュリティに関する SCRM へ積極的に取り組む組織に対しヒアリング調査を実施した。調査項目は、企業が情報セキュリティに関する SCRM に取り組み始めた経緯や認識しているサプライチェーン上のリスク（脅威）、リスクの課題認識、課題解決の手法などの先進的な取り組み事例等とした。

図表 2-1 調査の全体像

(1) 文献調査	✓ 政府及び民間企業が発行した情報セキュリティに関する SCRM に関する研究報告、先進的な活動に関する文献、ガイドライン・規格等を抽出・関連情報を調査
(2) アンケート調査	✓ 国内の企業に対するアンケート調査を実施 ✓ 企業の再委託状況や企業内の内部統制関係における現状認識、取組み状況等と業界や組織規模の違いを分析
(3) ヒアリング調査	✓ 日米の有識者や企業関係者に対するヒアリングを実施 ✓ IT システム並びに自社製品の設計・構築・運用等のサプライチェーンにおけるリスクや課題認識、先進的な取組み事例等を分析

2.1.1. 文献調査の実施概要

政府及び企業が発行する情報セキュリティに関する SCRM に関する文献の調査を実施し、情報セキュリティに関する SCRM が扱うべきリスクや課題等を整理した上で、アンケート調査の項目とすべき事項を抽出する。

本調査における情報セキュリティに関する SCRM の対象範囲は、①自組織における IT シ

ステム設計・開発・運用に関わるサプライチェーン、並びに②提供する製品やサービスの設計・開発・運用に関わるサプライチェーンとする。調査対象組織は、本対象範囲における情報セキュリティに関する SCRM に積極的な取り組みが見える企業及び団体と定めており、グローバルに事業を展開している企業及び団体、対象範囲に関連する文献を中心に参照している。

調査対象とする文献については、図表 2-2 に示した 12 文献に加え民間企業が公開している関連分野の文献を調査するとともに、アンケート調査を実施するにあたり調査仮説の検討を実施した。

図表 2-2 文献調査リスト

1	NIST[1]: NIST SP 800-161[2] “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”(2015 年 4 月)
2	NIST: NIST IR 7622[3]“Notional Supply Chain Risk Management Practices for Federal Information Systems”(2012 年 10 月)
3	NIST: The Memo from Interview "BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT"(2015 年)
4	NIST: “Improving Critical Infrastructure Cybersecurity” (2014 年 2 月)
5	Coverity: "Coverity Scan Open Source Report 2014“(2014 年)
6	内閣官房 内閣サイバーセキュリティセンター:「政府機関の情報セキュリティ対策のための統一基準群（平成 26 年度版）について」(2016 年 8 月 31 日)
7	内閣官房 内閣サイバーセキュリティセンター:「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」(2016 年 8 月 31 日)
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」(2016 年)
9	情報セキュリティ政策会議:「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」(2014 年 5 月 19 日)
10	経済産業省:「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」(2013 年)
11	文部科学省:「実践クラウドセキュリティ」(2016 年 3 月)
12	財団法人未来工学研究所:「情報システムのサプライチェーンにおける情報セキュリティに関する調査」(2011 年 3 月)

[1] ここで言う NIST とは、National Institute of Standards and Technology（米国国立標準技術研究所）の略称。
[2] ここで言う NIST SP 800-161 とは、NIST Special Publication 800-161 の略称。
[3] ここで言う NIST IR 7622 とは、NIST Interagency Report 7622 の略称。

2.1.2. アンケート調査の実施概要

我が国企業の情報セキュリティに関する SCRM に対する現状認識や取組みの概要を把握するため、委託元からみたサプライチェーンに関連する企業を対象にアンケート調査を実施した。

アンケートの調査手法は、ウェブベースで回答を収集する方法とした。

アンケート調査の回答者は、アンケート対象企業の属性（大企業（従業員数 301 人以上）／中小企業（従業員数 300 人以下)）、職種（「セキュリティ部門担当者・管理者」、「調達部門担当者・管理者」、「リスク管理部門担当者・管理者」、「開発製造部門担当者・管理者」）を設定した。また、回答者の属性（大企業、中小企業）については、それぞれ 500 サンプル以上を回収した。

調査目的や調査対象等の内容を含めたアンケートの調査実施概要を図表 2-3 に示す。

図表 2-3 アンケート調査の概要

調査目的	情報セキュリティに関する SCRM に対する現状認識や取り組み状況を把握するために情報セキュリティに従事する関係者を対象にアンケート調査を実施する。その結果を分析することで我が国企業の情報セキュリティに関する SCRM に対する取り組みレベルの向上に資するデータを取得する。
調査主体	独立行政法人情報処理推進機構（IPA） （アンケート調査は IPA の委託により株式会社野村総合研究所が実施）
調査対象	委託先を有する委託元の立場で、「セキュリティ部門担当者・管理者」「調達部門担当者・管理者」「リスク管理部門担当者・管理者」「開発製造部門担当者・管理者」のいずれかに従事する会社員・公務員
調査時期	2017 年 1 月 20 日～2017 年 1 月 26 日
調査方法	ウェブアンケート調査
有効回答数	1249 件
主な設問	✓ 委託先又は再委託先以降における情報セキュリティ対策の把握状況 ✓ 委託先を選定する際に重要視する条件 ✓ 再委託の許可を与える場合の情報セキュリティ条件　　等

2.1.3. ヒアリング調査の実施概要

文献調査、アンケート調査及び公開情報をもとに、日米の情報セキュリティに関するSCRMへ積極的に取り組む者（組織）に対しヒアリング調査を実施した。ヒアリング調査対象は、ITシステム設計・開発・運用に関わるサプライチェーン、若しくは対象企業が提供する製品またはサービスの設計・開発・運用に関わるサプライチェーンを有し、情報セキュリティに関するSCRMに対して積極的な取り組む企業及び団体を中心に選定した。日米のヒアリング対象企業及び団体の選定理由は図表2-4に示す。

図表 2-4 日米のヒアリング対象企業及び団体と選定理由

対象国	対象企業・団体	選定理由
日本	ITベンダー　A社	自社ではサプライチェーンに関する基本方針を示し、取引先向けのサプライチェーンに関するガイドライン等を策定し、グループ全体で情報セキュリティに関するSCRMに取り組んでいる。
	ITベンダー　B社	海外支社に対し、情報セキュリティ管理システムを活用することでグローバルでのセキュリティ対策に取り組んでいる。
	自動車メーカー C社	グローバルで事業を展開し、複数の子会社のある大規模なサプライチェーンに対しリスクマネジメントへ取り組んでいる。
米国	自動車メーカー D社	評価ツールを活用しており、新規に契約を結ぶ際にこの評価ツールを活用し、評価することで適切なパートナー選定に取り組んでいる。
	製薬メーカー E社	複数のパートナーを持つため、各パートナーにおける情報セキュリティの評価に取り組んでいる。各パートナーの品質を標準化するためにガイドラインを策定し、主要国毎のバージョンを用意している。
	NIST（米国国立標準技術研究所）	「NIST SP 800-161」や「NIST IR 7622」等、米国においてSCRMに関するガイドラインの策定に取り組んでいる。

2.2. 調査仮説の構築とその考え方

文献調査の結果を踏まえ、調査仮説を一覧としてとりまとめた（図表 2-5）。それぞれの調査仮説を構築する際に活用した資料を検討内容とあわせて記載する。

図表 2-5 調査仮説一覧

No	大項目	中項目	調査仮説
1	距離・把握	統制力と距離の関係	委託元は、直接の委託先についてはセキュリティの対策状況を把握できているが、再委託先（孫請負以降）までは把握しきれていない。
2	リスクの認識	業種別の必要度合い	情報セキュリティに関するSCRMの必要性に対する委託元の認識は、大手企業（重要インフラ関係者）、大手企業（非重要インフラ関係者）、中堅・中小企業の順でサプライチェーンリスクマネジメントへの必要性の認識が高い。
3	リスクの認識	再委託管理	委託元は、委託先に対し、再委託を許可する場合は、一定の条件を課している。
4	ルール	ルール・基準	委託元は、情報セキュリティに関するSCRMの全社統一ルールはない。
5	ルール	遵守方法	委託元は、委託先又は再委託先などに対し、ルールを徹底していない。
6	対象	保護対象の特定	委託元は、委託する際にセキュリティの保護対象を特定していない。
7	手段	外部ITシステム利用選定時の確認	委託元は、クラウド選定時にセキュリティ要件を十分に確認していない。
8	手段	開発納品物の確認	委託元は、納品物に使用されるオープンソースの脆弱性について確認していない。
9	手段	開発納品物の確認	委託元は、納品物の不正動作（マルウェアの混入等）について確認していない。

調査仮説 1：委託元は、直接の委託先についてはセキュリティの対策状況を把握できているが、再委託先（孫請負以降）までは把握しきれていない。

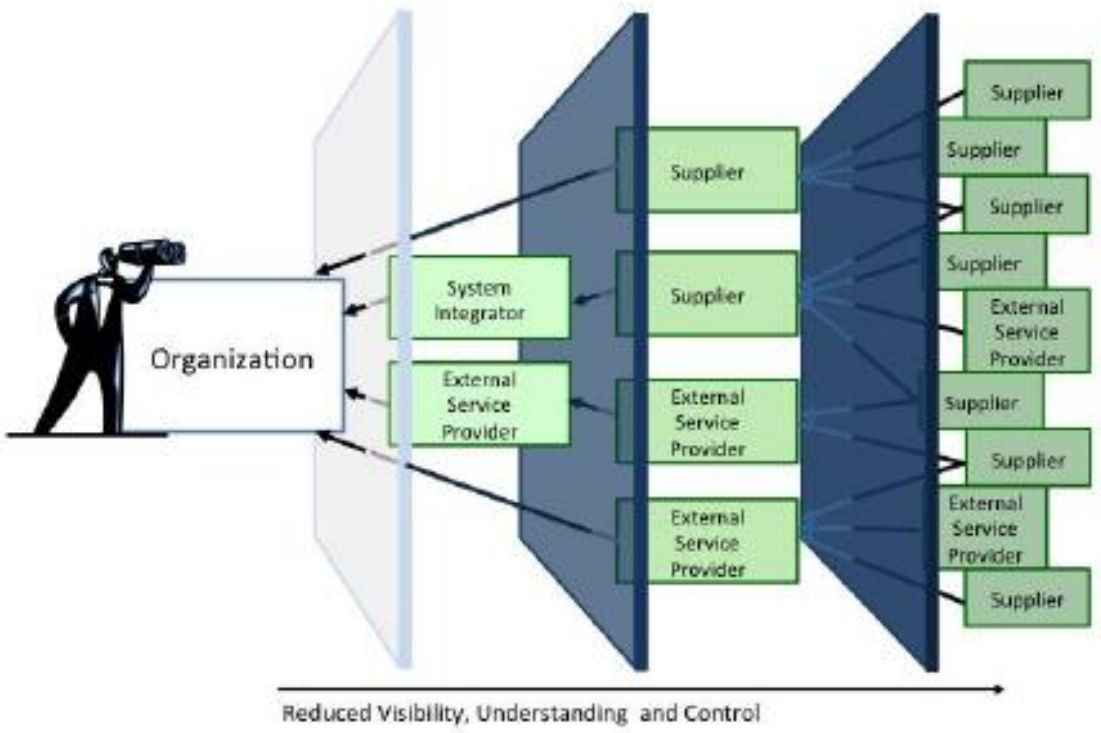
近年では、IT システムや提供する製品・サービスの設計・開発・運用において国内外を含め、業務の一部を外部の企業に委託するケースが増えている。業務の外部委託は、一企業に限らず複数の企業に対して行われることもあり、委託元から業務を引き受けた委託先が更に業務の一部を委託する再委託を行うケースも多く存在する。

米国国立標準技術研究所（以下、「NIST」という。）では、IT サプライチェーンの構造を図表 2-6 で示している。この図表では、企業の委託先や再委託先が増えるにしたがって、委託元の情報セキュリティ管理者等が監視・コントロール出来る範囲が限定的になることを示している。

上記の様な情報を踏まえ、一般的に委託先の情報セキュリティの対策状況はチェック

リスト等による自己評価の提出や現地立ち入り監査等の取組みにより把握しているケースが考えられるものの、再委託先までは把握できていないのではないかという調査仮説を導いた。

図表 2-6 米国における IT サプライチェーン構造



（出典） NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”

調査仮説 2 : 情報セキュリティに関する SCRM の必要性に対する委託元の認識は、大手企業（重要インフラ[4]企業）、大手企業（非重要インフラ企業）、中堅・中小企業の順で低くなる。

内閣サイバーセキュリティセンターは、国民生活や経済活動の基盤であり、機能が停止することで多大な影響を及ぼす恐れのある 13 分野の社会サービスを重要インフラとして定めている。重要インフラのリスクマネジメントの重要性については「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」で示しており、与える影響が大きいため強固なリスクマネジメントが必要であると述べている。

[4]ここで言う重要インフラ企業とは、内閣サイバーセキュリティセンターが定義する 13 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油）に関わる企業を指す。

同様に米国でも重要インフラに対するサイバーセキュリティ対策が取り組まれており、NIST が発行している“Improving Critical Infrastructure Cybersecurity”では、米国の重要インフラにおけるサイバーセキュリティ対策の重要性やサイバー攻撃から防護するためのサイバーセキュリティフレームワークを紹介している。

以上の内容を踏まえて、重要インフラ企業は非重要インフラ企業と比べた際に、情報セキュリティに関する SCRM の必要性に対する認識が高いのではないかと考えられる。また、情報セキュリティに関する SCRM の必要性に対する認識は、企業規模によっても異なると考えられる。

故に、情報セキュリティに関する SCRM の必要性に対する委託元の認識は、大手企業（重要インフラ企業)、大手企業（非重要インフラ企業)、中堅・中小企業の順で低くなるのではないかという調査仮説を立てた。

調査仮説 3：委託元は、委託先に対し、再委託を許可する場合は、一定の条件を課している。

内閣サイバーセキュリティセンターが公表している「府省庁対策基準策定のためのガイドライン」では、「府省庁外の者に、情報システムの開発、アプリケーションプログラムの開発等を委託する際に、行政事務従事者が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において府省庁対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある」としている。また「再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保」し、その「再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を府省庁に提供し、府省庁の承認を受ける」ことなどが示されている（図表 2-7)。

更にグローバルに事業を展開し複数の委託先を抱えている民間企業が公開しているセキュリティ報告書によると、委託先が再委託を行うことに対して、書面による事前承諾を行わせている。

以上を踏まえ、委託元は委託先に対し、再委託を許可する場合は、一定の条件を課しているのではないかという調査仮説を立てた。なお、アンケート調査では調査仮説 3 検証に伴い、具体的にどのような条件を課しているかも合わせて検証を実施した。

図表 2-7 外部委託(再委託含む)に関する遵守事項

遵守事項

(2) 外部委託に係る契約

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを**委託先の選定条件とし、仕様内容にも含める**こと。

(ア) **委託先に提供する情報の委託先における目的外利用の禁止**

(イ) 委託先における情報セキュリティ対策の実施内容及び管理体制

(ウ) 委託事業の実施に当たり、委託先企業又はその従業員、再委託先、若しくはその他の者による**意図せざる変更が加えられないための管理体制**

(エ) **委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供**

(オ) **情報セキュリティインシデントへの対処方法**

(カ) **情報セキュリティ対策その他の契約の履行状況の確認方法**

(キ) **情報セキュリティ対策の履行が不十分な場合の対処方法**

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託する業務において**取り扱う情報の格付等を勘案し、必要に応じて以下の内容を仕様に含めること**。

(ア) 情報セキュリティ監査の受入れ

(イ) サービスレベルの保証

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先がその役務内容を一部**再委託**する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(a)(b)の措置の実施を委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を府省庁に提供し、府省庁の承認を受けるよう、仕様内容に含めること。

（出典）内閣サイバーセキュリティセンター「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」

調査仮説 4：委託元は、情報セキュリティに関する SCRM の全社統一ルールはない。
調査仮説 5：委託元は、委託先又は再委託先などに対し、ルールを徹底していない。

一般的に、企業が情報セキュリティに関する SCRM を行う場合、社外へ業務を委託または再委託することで生じる脅威（リスク）、またその脅威に対し情報セキュリティ対

策が十分であるかを把握する必要がある。この場合、自社内で情報セキュリティに関する SCRM のルールを策定することが考えられる。情報セキュリティに関する SCRM のルール策定において企業は、①費用対効果の観点から全社で統一のルールを策定しているのか、②自社の情報セキュリティへの取り組みを中心に行っている、若しくは特定の委託先にのみルールを策定しているのか、以上の 2 点を文献調査の段階で検証した。

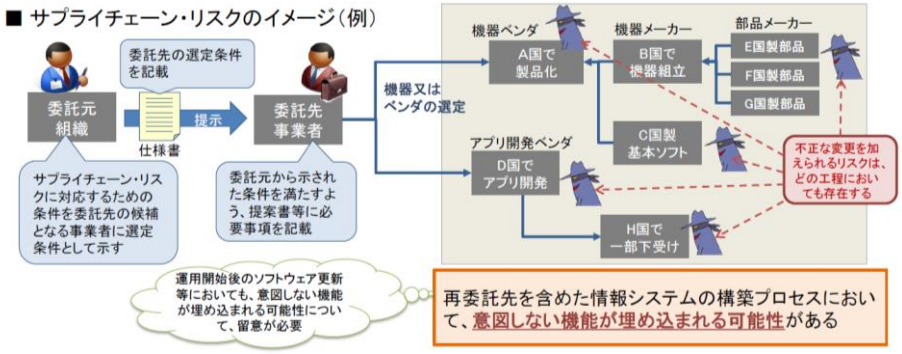
図表 2-8 は、内閣官房内閣サイバーセキュリティセンターがサプライチェーンリスクのイメージを図表で示したものである。具体的には、委託元組織から委託先事業者が業務を受託する場合、機器ベンダやアプリ開発ベンダに再委託する場合のサプライチェーンの構造を図表で示すとともに、そこに介在する不正が行われるリスクを示している。図表で示しているように複数の企業が業務に関わることで高まるリスクを避けるためにも、委託元は情報セキュリティに関する SCRM の統一ルールを設けることで、委託先や再委託先を一定基準の下に管理する必要がある。しかし、我が国では情報セキュリティに関する SCRM に対する認知度が低いこともあり、情報セキュリティに関する SCRM への取り組み対する意識は薄いと考えられる。故に、企業は情報セキュリティの取り組みを行っているが、情報セキュリティに関する SCRM のルールの策定は考慮していない企業が多いものと推察される。

以上の内容を踏まえて、委託元は全社に情報セキュリティに関する SCRM の統一ルールはないといった調査仮説と同様に委託元は、委託先又は再委託先などに対し、ルールを徹底していないといった調査仮説を立てた。

調査仮説 6：委託元は、委託する際にセキュリティの保護対象を特定していない。

また、企業は情報セキュリティ対策を講じる場合、保護すべき対象範囲を定め、その範囲にある資産及び特性（機密性、完全性、可用性など）を特定しそれらの脅威を把握する必要がある。これらの対象範囲・資産を予め定めなければ、資産を守るための効果的な情報セキュリティルールの策定や具体的な対策が難しくなるためである。企業は情報セキュリティポリシーにて、自社 IT システム及び自社が提供するサービス・製品における保護対象となる範囲や資産を特定しているケースもある。しかし、委託先企業に対しては複数の企業にまたがり、想定・対応すべき情報セキュリティリスクの種類が多いため、サービス・製品別に保護対象を設定することは難しいと考えられる。そこで、委託元は委託する際にセキュリティの保護対象を特定していないといった調査仮説を立てた。

図表 2-8 サプライチェーンリスクのイメージ



（出典）内閣官房内閣サイバーセキュリティセンター「政府機関の情報セキュリティ対策のための統一基準群（平成 26 年度）について」より抜粋

調査仮説 7：委託元は、クラウド選定時にセキュリティ要件を十分に確認していない。

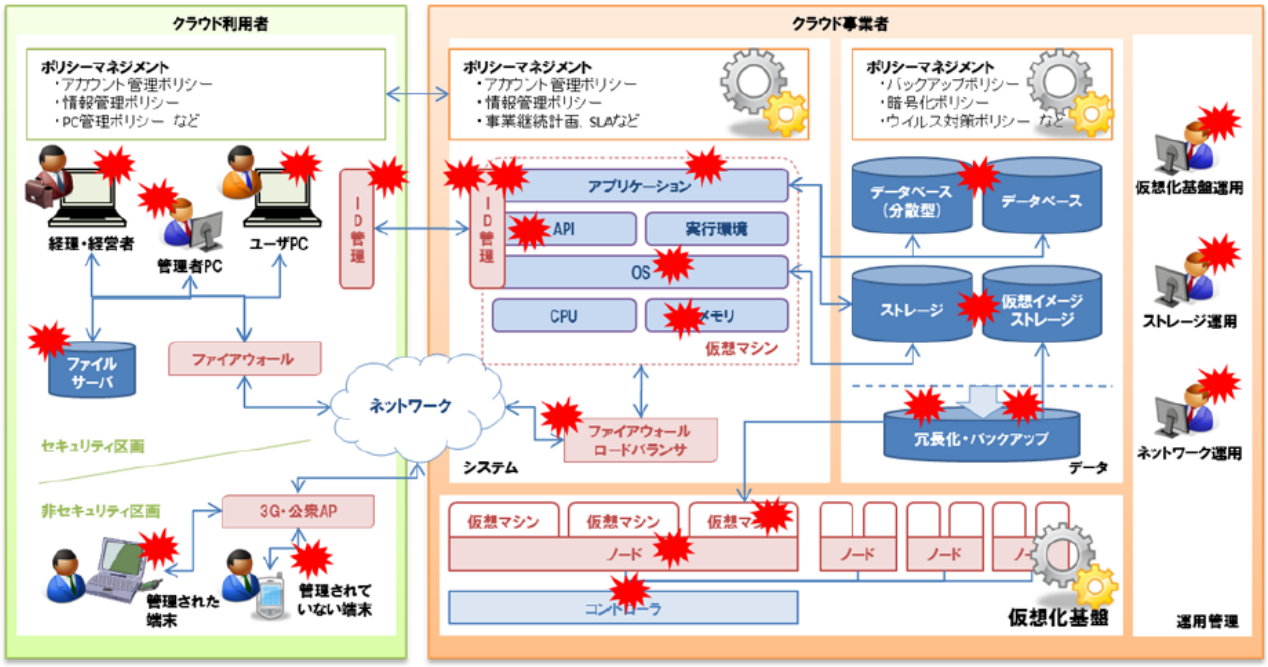
近年、クラウドサービスの普及に伴い、クラウドを利用する企業が増えている。クラウドにより利便性が向上する一方、容易に利用できることからクラウド事業者自体のセキュリティ状況や設定するセキュリティ要件を十分に確認しないままサービスの利用を開始している企業も多いことが想定される。

オンプレミスでは、自社内に閉じたネットワーク環境下でシステム構築・運用できるためクラウドに比べてネットワークセキュリティは高いと言われている。一方で、オンプレミスでは一極集中型で情報資産を保管している場合、自然災害等によってデータの修復が不可能になるリスクが存在する。

また、クラウドでは、図表 2-9 に示したように自社のセキュリティ対策だけでなく、クラウド運用企業側のセキュリティ対策もリスクマネジメントを行う上で重要になってくる。クラウドではリスクの発生可能性が自社のセキュリティ対策次第であったオンプレミスと異なり、図表 2-10 に上げられているリスクのようにクラウド運用企業側のセキュリティ対策次第でリスクが発生するので、セキュリティ要件を十分に確認する必要があるといえる。しかし、図表 2-10 と同様に文部科学省が発行する文献では、セキュリティ要件の検討方法は機能、維持、運用管理、利用、開発・変更工程等の様々な項目から検討する必要があると示しているが、クラウドの利用の容易さから各企業がセキュリティ要件を十分に確認しているとは考えにくいと推察される。

以上の内容を踏まえて、委託元はクラウド選定時にセキュリティ要件を十分に確認していないといった調査仮説を立てた。

図表 2-9 クラウドサービス利用にかかわるリスク



（出典）経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

図表 2-10 クラウドサービスにおける代表的なリスク一覧

番号	リスクの識別名
H01	リソース・インフラの高集約によるインシデントの影響の拡大
H02	仮想／物理の設計・運用の不整合
H03	他の共同利用者の行為による信頼の喪失
H04	リソースの枯渇（リソース割当の過不足）
H05	隔離の失敗
H06	サービスエンジンの侵害
M07	クラウドプロバイダでの内部不正－特権の悪用
M08	管理用インターフェースの悪用（操作、インフラストラクチャアクセス）
M09	データ転送途上における攻撃、データ漏えい （アップロード時、ダウンロード時、クラウド間転送）
M10	セキュリティが確保されていない、または不完全なデータ削除
M11	クラウド内 DDoS/DoS 攻撃
L12	ロックインによるユーザの忌避
L13	ガバナンスの喪失
L14	サプライチェーンにおける障害
L15	EDoS 攻撃（経済的な損失を狙ったサービス運用妨害攻撃）

（出典）文部科学省「実践クラウドセキュリティ」

調査仮説 8：委託元は、納品物に使用されるオープンソースの脆弱性について確認していない。

調査仮説 9：委託元は、納品物の不正動作（マルウェアの混入等）について確認していない。

米国国土安全保障省と協同でオープンソースの品質の向上を支援している Coverity が発行しているレポートでは、オープンソースと商用ソフトウェアの脆弱性を比較した結果を報告している。調査結果レポートによれば、オープンソースの脆弱性は商用ソフトウェアの約 16 倍といった結果になっている。このことから、オープンソースの脆弱性の検査は商用ソフトウェア以上に入念に行う必要があるといえる。

民間企業の大手 IT ベンダーでは保守工程の一環として、オープンソースの脆弱性対応システムを構築していたが、多くの企業が同様に納品物に使用されるオープンソースの脆弱性や不正動作までは確認できているとは考えにくい。その理由として、委託先事業者が増えれば、多種多様なオープンソースやソフトウェアを組み合わせて活用することになり、脆弱性や不正動作の検査を行うにしても人手が掛かり、多くのコストが発生し企業負担が増加することが考えられる。更に、オープンソースやソフトウェア情報も全て公開しているわけではなく、ブラックボックス化している部分も納品物に含まれる場合もあり、サービス・製品の全ての部分を検査することは難しいと考えられる。

以上の内容を踏まえて、委託元は、納品物に使用されるオープンソースの脆弱性について確認していない。更に、納品物の不正動作（マルウェアの混入等）について確認していないといった調査仮説を立てた。

3. 調査結果から得られた示唆

「2. 調査の概要」で前述したアンケート調査とヒアリング調査の 2 つの調査結果により把握された企業における情報セキュリティに関する SCRM の全体概要から、今後、検討が必要になると考えられる論点を分析し、調査結果から得られた示唆として整理した。

なお、アンケート調査とヒアリング調査の詳細な調査結果については、巻末の参考資料に記載している。

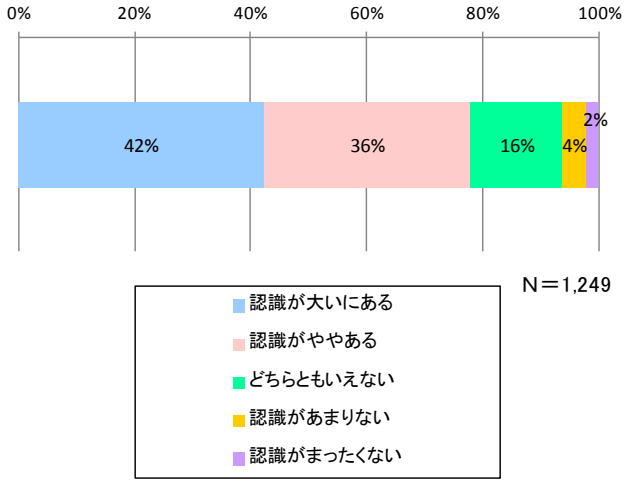
3.1. 情報セキュリティに関する SCRM の重要性に対する経営層の認識

経済産業省が IPA とともに策定した「サイバーセキュリティ経営ガイドライン」においては、企業が委託先または再委託先等に対する情報セキュリティ管理の強化・徹底に努めていくことが必要とされ、そのような観点が、サイバー攻撃から企業を守る上で経営者が認識する必要のある「3 原則」や、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」の中で取りまとめられている。

その一方で、アンケート調査結果をみると、委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する認識は、企業の経営者において、必ずしも十分高まっているとは言えない状況である。「認識が大いにある」と回答した企業の割合は、全体の 40%強と比較的低調である。

また、同割合と「認識がややある」と回答した企業等の割合を合わせると、委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する認識のある企業の割合は、80%弱まで上昇する。この結果は、本調査タイトルや、回答者の所属部署の絞り込みにより、情報セキュリティに関する SCRM について比較的リテラシーの高い属性の回答者が多数派を占めたことが影響しているものと予想される。

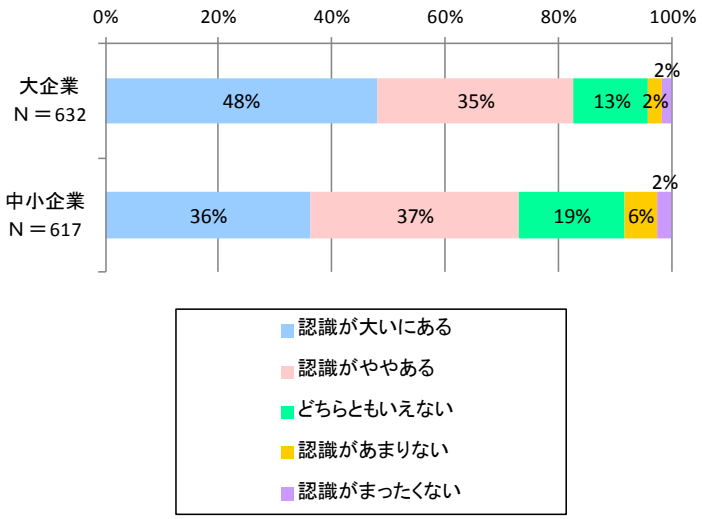
図表 3-1　委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する企業の経営層の認識（単回答）



一方、従業員数からみた組織規模の違いによる意識の差についてみると、「認識が大いにある」、「認識がややある」のいずれかに回答した企業等の割合は、大企業で約 83%、中小企業で約 73%であり、双方に 10 ポイントの大きな開きがあることが分かった。

大企業を中心とする企業ヒアリングでは、日系企業の中に、セキュリティを強みにしたビジネスの拡大に伴い、経営層への意識の浸透が進んできていると見ている企業もあり、アンケート調査結果は、こうした評価とも概ね一致する。

図表 3-2　委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する企業の経営層の認識（大企業、中小企業の比較）（単回答）

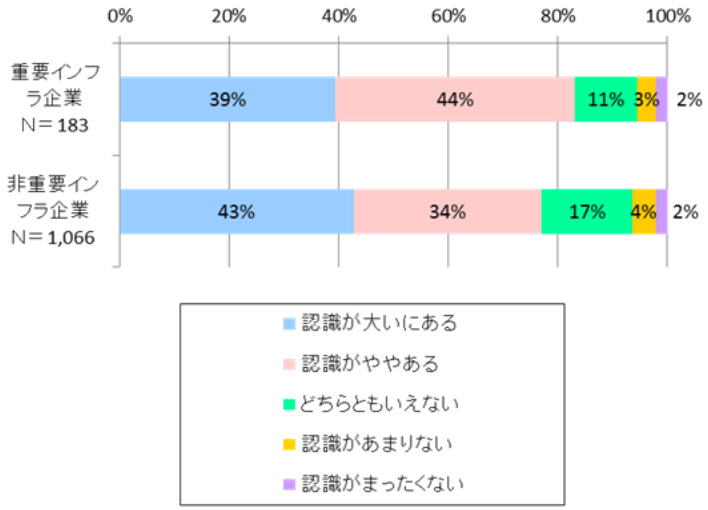


図表 3-3 情報セキュリティに関する SCRM の取組みの達成レベルに関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● セキュリティ強化を起点としたビジネスの拡大、サイバーセキュリティ基本法の施行、IoT セキュリティ分野における取組みの活発化を背景に、情報セキュリティに関するリスクマネジメントに対する経営層の意識も高まってきている。

他方、重要インフラ企業と非重要インフラ企業の間の意識の差についてみると、「認識が大いにある」、「認識がややある」のいずれかに回答した企業等の割合は、重要インフラ企業で約 83%、非重要インフラ企業で約 77%であり、大企業、中小企業の結果と比べると、その差は幾分縮まる。

図表 3-4 委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する企業の経営層の認識（重要インフラ企業、非重要インフラ企業の比較）（単回答）



また、企業ヒアリングによると、各社とも、重大なインシデントの発生や、IoT やシステム連携など ICT 利活用の進展に伴う情報セキュリティリスクの増大を契機として、情報セキュリティに関する SCRM への取り組みを本格的に推進していることが分かった。

図表 3-5 情報セキュリティに関する SCRM の取組みの経緯に関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 2006 年にファイル共有ソフト Winny が流行り、情報漏洩が多発した。Winny に関連した当社の取引先を起因とする事故が 30%以上あったので、2008 年から情報セキュリティのトップマネジメントを行い、セキュリティ推進を行うワーキンググループを構築し、取引先のセキュリティ強化を始めた。
IT ベンダー	● 当社では、2004 年に情報セキュリティ推進組織を設立した。脆弱性のあるソフトウェアの混入という当社が起こした重大なインシデントが、設立のきっかけとなった。このインシデントを契機として、情報セキュリティ施策の決定権をどの部門に置くか、またどの部門が委託管理を担当するかといった観点から、当社内の情報セキュリティの見直しが行われた。
自動車メーカー	● 車載システムのセキュリティについて注目したのは 3 年前である。当時、インパネを外して不正な機器を CAN に繋いだり、故障診断ポート経由でマルウェアが混入されるなど、CAN に対するセキュリティ問題に関わる報告が行われていた。米国の JEEP のハッキング実証実験が公表される前から、自動車工業会や JASPAR、自動車技術会といった国内業界団体では、車載システムのセキュリティ問題を業界共通の問題として認識していた。 ● これがきっかけで、2014 年に社内に車載システムのセキュリティ担当者が置かれ、対策部品の開発・実装を担うようになった。
自動車メーカー	● 2010 年に、カリフォルニア大学サンディエゴ校のカール・コッシャー氏とワシントン大学の教授が、GM の自動車に対するハッキングの実証に関する研究論文を発表し、これに対し、GM 側がハッキングに悪用された脆弱性に対処したことが契機となって、米国自動車業界全体が、GM のリスク対応の動きに追随するようになった。 ● 加えて、2015 年に、Jeep に対し、ハッキングを可能とする脆弱性が公表されたことを契機に、製品セキュリティの必要性が、自社の経営陣に受け入れられるようになった。
製薬メーカー	● 製造ライン自動化を担う制御システムには、エアコンの動力供給システム、液体調剤システム、錠剤の圧縮システムなど、さまざまなシステムが相互接続されているが、過去に、サプライヤーから納入されたコンピュータシステムにおいて、製造段階に、ソフトウェア開発ライブラリのコードの中に悪意のあるコードが仕掛けられたことがあった。 ● このため、製造ライン自動化を担う制御システムは、社内のすべてのシステムから切り離し可能とし、かつ相互のシステム間にはファイアウォールを設置し、認められたごく僅かのトラフィックしか通過できないようにホワイトリストを用いたフィルタリングを実施している。

こうしたインシデントの発生や情報セキュリティリスクの増大等の状況は、企業の経営者の意識変革や情報セキュリティに関する SCRM 推進の取組みの本格化に少なからぬ影響を与えているが、一方で中小企業など、こうした流れから取り残される企業も出てくるものと

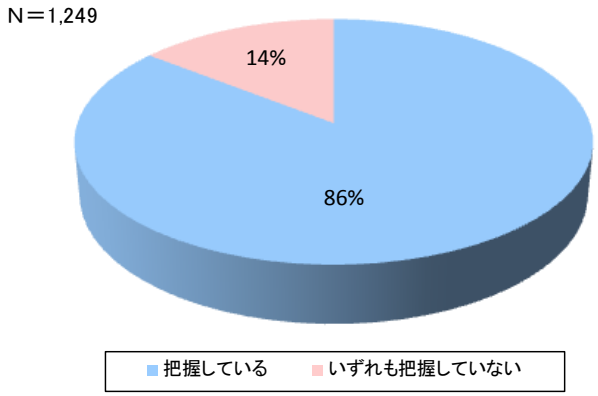
考えられるため、企業の経営者の意識を啓発していくことが重要である。

3.2. 委託先または再委託先等に対するセキュリティ対策状況の把握

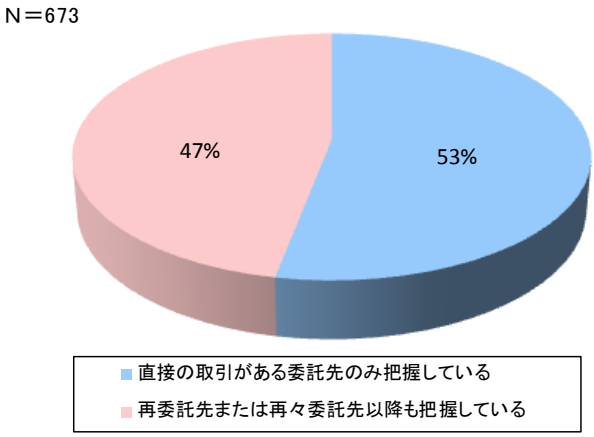
委託先または再委託先等のいずれについても、セキュリティ対策状況を把握している企業は約 86%を占めた。しかしながら、再委託先または再々委託先以降までのサプライチェーンを有する企業（再委託先等があるかどうか分からない企業を除く）のうち、セキュリティ対策状況を把握している範囲が直接取引のある委託先までである企業の割合は約 53%、再委託先または再々委託先以降までである企業の割合は約 47%である。

このように委託元は、直接取引のある委託先についてはセキュリティの対策状況を把握できているが、再委託先以降まで把握できている組織は少ないことが分かった。

図表 3-6 委託先または再委託先等に対するセキュリティ対策状況の把握の有無（単回答）



図表 3-7 再委託先または再々委託先以降のサプライチェーンを有する企業における
セキュリティ対策状況の把握範囲（単回答）



また、企業ヒアリングにおいても、各社とも、情報セキュリティに関する SCRM の取組

みの対象範囲は直接取引のある委託先であると考えていることが明らかになった。

図表 3-8 情報セキュリティに関する SCRM の取組みの対象範囲に関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 委託先には、工事系の企業も含まれ、工事系の企業では、再委託の重層的な連鎖構造が 5 次～6 次まで及ぶ場合もある。再委託先のセキュリティ管理は当社で直接行うことができないため、委託先にセキュリティ管理を一任せざるを得ないのが実情である。
自動車メーカー	● Tier1 サプライヤー[5]に対して、SOW（Statement of Work、作業範囲記述書[6]）に基づく納品物のセキュリティチェックを実施している。SOW においては、セキュリティ上の問題が発生し、当社が設計書や図面等の開示要請を行った場合に、当該要請に応じなくてはならない義務や、第三者によるセキュリティ診断テストの実施の義務等を規定している。また、Tier1 サプライヤーの開発拠点や製造拠点の現地調査も実施している。 ● Tier2 サプライヤー以降に対しては、直接的にサプライチェーンリスクマネジメントの取り組みを実施することはない。
自動車メーカー	● サプライチェーンが重層的な構造になる中で、Tier3 サプライヤーや Tier4 サプライヤーといった川下の企業に対して直接連絡を取るようなことはない。委託元がこのような企業に対してセキュリティ管理を行うことはほぼ不可能であるため、標準化が極めて重要となる。
製薬メーカー	● 契約書上で Tier1 サプライヤーには、Tier2 サプライヤー以降のセキュリティを管理する責任はないが、現実的には Tier1 サプライヤーが自発的に Tier2 サプライヤー以降のセキュリティ管理を行っている。 ● 5 年間のサイバーセキュリティ保険に加入している。保険対象には、サプライチェーンにおける主要サプライヤーで重大なインシデントが発生する可能性を考慮して、主要サプライヤー数社を新たに含めた。保険に加入するためには、主要な Tier1 サプライヤー数社から必要なデータを取得し、保険会社に提出する必要があった。このようなサプライヤーのデータは、保険会社において、リスクコントロール基準に応じたスコアリングに活用されることを期待している。

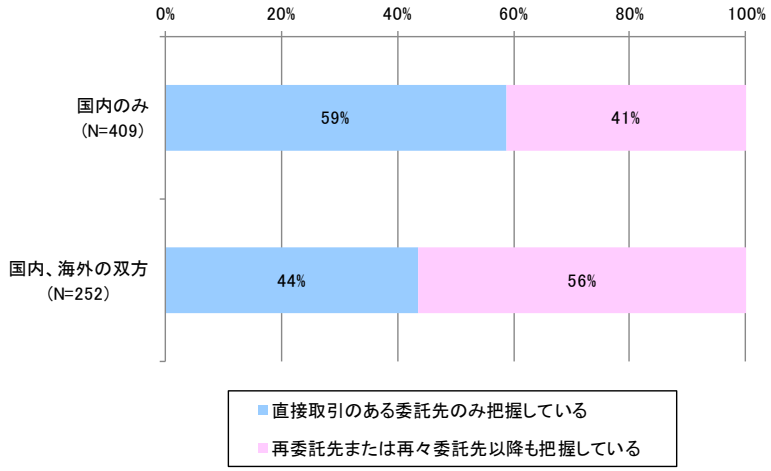
再委託先または再々委託先以降までのサプライチェーンを有する企業（再委託先等があるかどうか分からない企業を除く）においては、委託先がグローバルに分散し広範に及ぶ場合や委託先の数が多い場合など、セキュリティ対策状況の把握にあたっての条件が厳しくなればなるほど、再委託先以降のセキュリティ対策状況を把握している企業の割合が高くなることが分かった。これは、委託先がグローバルに分散し広範に及び、数も多い大企業を中心と

[5]ここで言う Tier1 サプライヤーとは、メーカーに直接部品を納入する一次請けの企業を指す。Tier2 サプライヤーは、二次請けの企業となる。

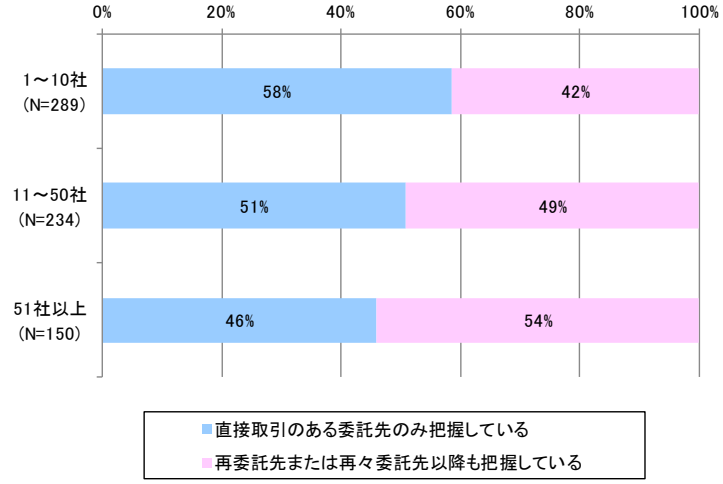
[6]ここで言う作業範囲記述書とは、システム開発などの契約を行う際に、目標や成果物の取り決め、スケジュール、作業内容、参加主体の役割分担、権限などの作業の範囲を定義した文書を指す。

して、企業における情報セキュリティに関するサプライチェーンリスクに対する問題意識が高まってきていることの表れであり、課題を解決することで良い方向に向かう可能性を秘めていると考えられる。

図表 3-9　再委託先または再々委託先以降のサプライチェーンを有する企業における
セキュリティ対策状況の把握範囲（委託先の所在地別）（単回答）



図表 3-10　再委託先または再々委託先以降のサプライチェーンを有する企業における
セキュリティ対策状況の把握範囲（委託先の数別）（単回答）



3.3.　委託先に対して再委託を許可する際の情報セキュリティ管理の条件

再委託先または再々委託先以降までのサプライチェーンを有する企業（再委託先等があるかどうか分からない企業を除く）のうち、委託先に対して再委託の許可を与える場合に、情報セキュリティ管理の条件を特に何も課していない企業の割合は僅か約 2%にとどまっており、企業の多くが何らかの一定の条件を課していることが分かった。再委託に対する企業の不安意識の高さを反映する結果となっている。

再委託の情報セキュリティ管理のために課される条件としては、委託元から事前の了解を得たり、委託先に適用している情報セキュリティ管理に関する規定に適合していることを示す証跡を再委託先に提出させるケースが多い。

他方、委託先に対して再委託先の管理責任を明確にしたり、委託先と同一のセキュリティルールを再委託先に遵守させるなど、情報セキュリティガバナンス体制の確立に向けて厳しい姿勢で臨む企業も多数派ではないが、大企業を中心に存在する。そのような状況のもとで、委託先、再委託先または再々委託先以降の情報セキュリティ管理については、実効性をどのように担保するのかという問題、均質な管理が可能であるか等克服すべき課題が多いと考えられる。

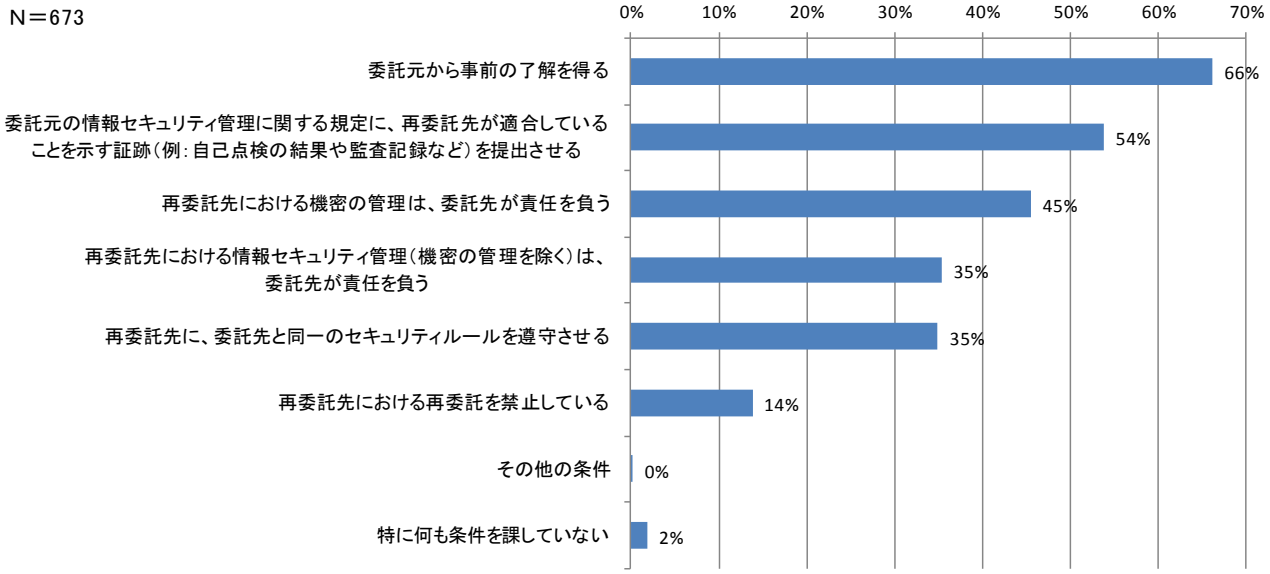
企業ヒアリングにおいても、①委託先の情報セキュリティ管理を担う委託元に関わる課題、②再委託先または再々委託先以降の情報セキュリティ管理を担う委託先に関わる課題の 2 つの課題が浮き彫りになっている。

上記①の課題については、委託先に対し、セキュリティレベル向上に向けた取組みへの協力を得るのが難しいこと、コスト負担の制約があり、一律の取組みの強要が難しいこと、委託先への監査体制や情報伝達体制が脆弱であることなど、多岐にわたることが明らかになっている。また、委託先における資本関係の有無や、委託先の重要度（主要な委託先であるかどうか)、委託先の所在地（国内の委託先であるか、海外の委託先であるか）の違いによって管理レベルが異なる場合があり、十分な情報セキュリティ管理が出来ていない委託先が存在することも明らかになった。

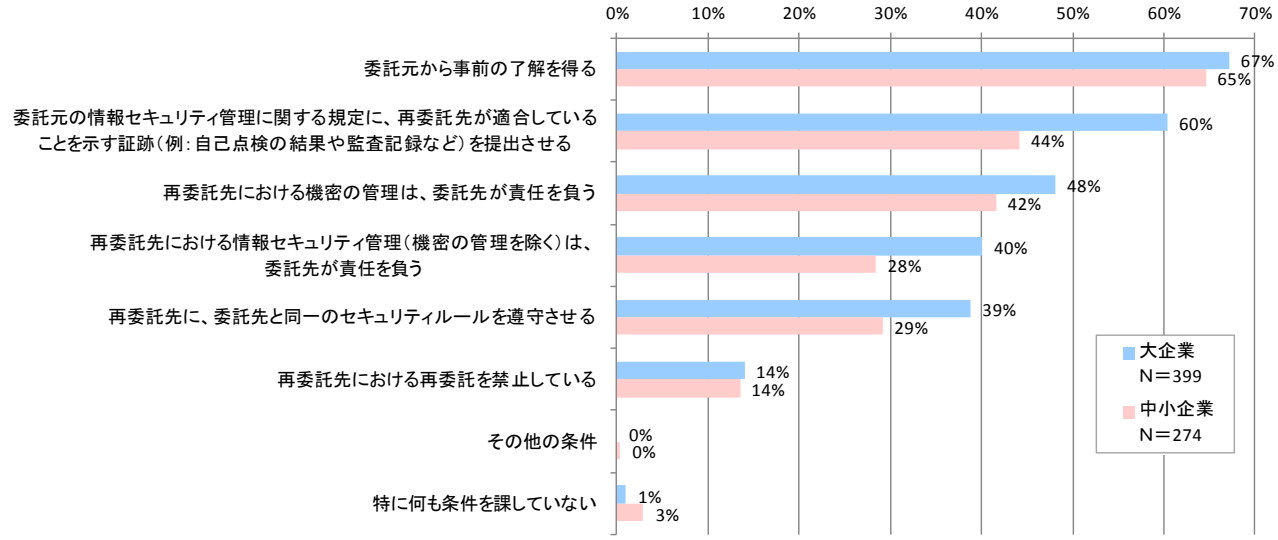
他方、上記②の課題については、再委託先の情報セキュリティ管理は、契約関係がなく委託元が直接行うことができないため、委託先に管理を一任せざるを得ない状況になっている場合が多いことが明らかになった。

このような制約が存在するなか、委託先、再委託先または再々委託先以降の情報セキュリティ管理を総合的に行う仕組みを構築していくことは、今後の重要な課題の一つと言えよう。

図表 3-11　委託先に対して再委託の許可を与える場合に遵守を求める情報セキュリティ管理の条件（複数回答）



図表 3-12　委託先に対して再委託の許可を与える場合に遵守を求める情報セキュリティ管理の条件（大企業、中小企業の比較）（複数回答）



図表 3-13　情報セキュリティに関する SCRM の取組み上の課題に関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 国内における情報セキュリティに関する SCRM の取組み上の課題は 2 つある。 ● 1 つ目は、情報セキュリティ対策に前向きでない企業を中心に、セキュリティレベル向上に関する取り組みが少ない取引先企業をどのように改善していくかが課題である。特に、当社と取引先との力関係からみて、取引先が当社から仕事を得られ、優位な立場にある場合、当社が推進するセキュリティ強化の取り組みに対して前向き取り組んでくれない場合がある。

	● 2 つ目は、異なる企業規模を持つ委託先に対して、共通的に一律のセキュリティレベルの対策を強要するのが難しいことが課題である。特に、技術的な対策に関しては、中小規模の委託先においては、コスト面の制約が大きくなりがちであり、前向き取り組んでくれない場合がある。 ● その結果として、個々のプロジェクトに応じて、情報セキュリティ対策の取組みに温度差が生じるため、全体としての最適化を図っていくことが必要になる。 ● 海外では、委託先のセキュリティ管理を担う海外現地法人の担当者とのコミュニケーションを円滑に行うことができるかが課題である。日本語で会話できる人材の確保難や、契約・交渉にかかる商慣習の違いがコミュニケーションの障壁になりやすい。 ● グローバルの委託先管理においては、中国の現地法人の調達部門が積極的に取り組んでくれている。中国の現地法人では、日本語が話せる人材を積極的に採用しているのでコミュニケーションを取り易い。一方、インドでは日本語を話せない人がほとんどであるので、英語でやり取りする必要があることや文化面で違いがあることといった部分で障壁になるケースが多々あり、コミュニケーションが取り辛い。
IT ベンダー	● 資本関係の有無によらず、すべての委託先に対して、網羅的にセキュリティ管理を行うのは時間面の大きな制約もあり、困難である。委託先に対して実施する現地調査についても、是正が必要な委託先のみに対象を限定している。現地調査においては、均質なレベルで監査の実施が求められるが、このような監査に対応可能な人材が不足し、体制が脆弱であることが課題である。 ● 委託先がセキュリティ事故を起こさないようにするためには、安全な開発環境を構築する必要があるが、コスト負担の問題を伴うため、このような環境の構築が進んでおらず、十分な統制を効かすことができない。
自動車 メーカー	● セキュリティ分野は、社内に経験者が少ないため、外部の知見を活用するしかない。スキルやリソースが足りていないのが大きな課題である。契約書において、委託先に義務付けるセキュリティチェックの項目を記載することが難しいレベルである。

3.4. 委託を行う際のセキュリティ保護資産の特定

委託を行う際にセキュリティ保護資産を特定し指定していない企業の割合が約 16%を占めており、このような企業では、保護すべき資産を明確にし、リスク評価や対策の実施に繋げていくという意識が希薄である。

また、企業の約 83%が、委託を行う際にセキュリティ保護資産を特定し指定しているが、その内訳についてみると、委託契約上でセキュリティ保護資産を個別に指定するよりも、包括的に指定する方が多数派である。この傾向は、中小企業よりも大企業の方が顕著である。

それを見る限りは、委託で扱う製品や IT システムの対象範囲が広範で複雑な大企業になればなるほど、想定・対応すべき情報セキュリティリスクの種類も多くなるため、セキュリティ保護資産の特定のために多大な時間や労力をかけなくて済む包括的な指定を選択しが

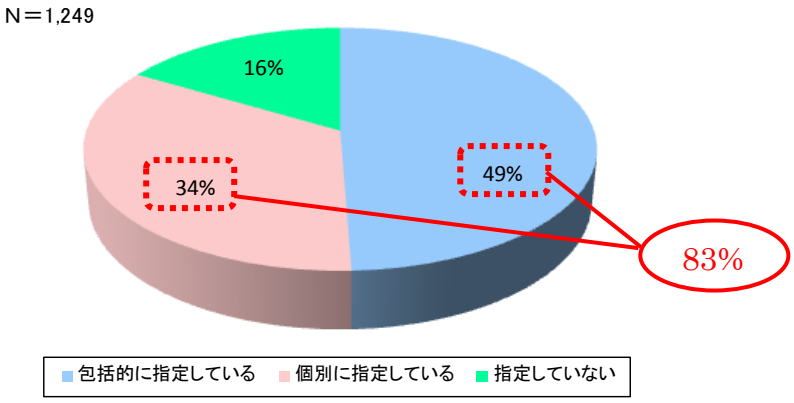
ちであると考えられる。

顧客に製品を提供する製造メーカーでは、顧客の安全性確保やプライバシー保護を、委託を行う際のセキュリティ保護対象として指定している場合がある。他方、ＩＴベンダーでは、顧客の情報資産を、委託を行う際のセキュリティ保護対象として指定している場合がある。

IT システムにおいては、仕様の異なる多様な製品を扱い、想定・対応すべき情報セキュリティリスクの種類も多くなりがちであることから、IT ベンダーは、セキュリティ事故を起こさないとしながらも、確認できる領域の限界を考慮して、納品物に対して、最低限のセキュリティの担保を徹底することを優先させている。

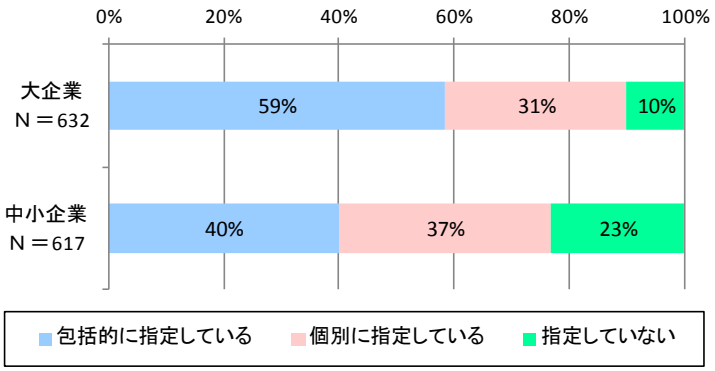
このように対応に苦慮する状況を考慮すると、委託元が委託を行う際にセキュリティ保護資産の対象を具体的に特定していない理由としては、意識が希薄である場合とそのような意識があっても対応に苦慮している場合の 2 つの理由が存在するものと考えられる。

図表 3-14　委託を行う際のセキュリティ保護資産の指定の有無・状況（単回答）



注）数値については、四捨五入して表記しており、100%にならない場合がある。

図表 3-15　委託を行う際のセキュリティ保護資産の指定の有無・状況（大企業と中小企業の比較）（単回答）



図表 3-16 委託を行う際のセキュリティ上のリスクの認識やセキュリティ保護の考え方に関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 委託先でセキュリティ事故が発生した場合は、当社グループの管理不備が問われ、最終的には委託元が責任を負うことになる。このため、当社グループ全体が、委託先と一体となって情報セキュリティ強化に取り組むことにより、顧客からの信頼を得ることが大切であると考えている。 ● 取引先に対し、顧客のデータを預かっており、CIA の中でも Confidentiality（機密性）を一番重視している。 ● 納品物に関しては、委託先に対して事前に脆弱性をチェックするよう依頼している。また、セキュアな開発環境下で開発に取り組んでいる。しかしながら、脆弱性を確認できる領域には限界があるため、最低限のセキュリティ担保で製品・サービスを提供できるように取組んでいる。
IT ベンダー	● 情報セキュリティに関するリスクマネジメントに取り組む目的は、①当社が顧客と共に事業を行ううえでセキュリティ事故を起こさないようにすること、②当社の納品物に対する最低限のセキュリティ担保を徹底できるようにすることである。
自動車メーカー	● 万が一、車両のセキュリティ事故を起こした場合には、企業イメージのダウンに繋がり、販売部門に迷惑がかかってしまう。また、リコールサービスキャンペーンが必要となるため、膨大なコストが発生する。 ● セキュリティ事故の内容次第ではあるが、例えば、車両のメーターが攻撃されて、表示不能となった場合には、車両に関する法規制を遵守できなくなる。このような事態は避けなければならない。
自動車メーカー	● 製品のセキュリティリスクとして、①製品の安全性、②プライバシーの保護、③製品の信頼性の 3 つのリスクを扱っている。自動車同士が繋がっているシステムでは、製品に対する攻撃の影響が、同システムの基盤を介して、販売管理システム等の企業の基幹システムにまで波及する可能性がある。自社が構築するサプライチェーン以外の外部ベンダーの部品を使用できるようになっている場合は、その部品が、製品やシステムに対して悪意のある何らかの行動を起こし、攻撃の機会となるリスクが増す。
製薬メーカー	● セキュリティ保護対象は、患者の安全性、患者のデータ(職員・顧客のデータ)、自社の知的財産、並びに法令であり、優先順位はこの順に従う。 ● セキュリティ保護対象が、どのように保護されるかは、何を委託するかによって決まる。例えば、部品製造の委託を行う際には、少なくとも当社の製造環境でのセキュリティ管理と同等のレベルのセキュリティ管理を担保できるようにする必要がある。

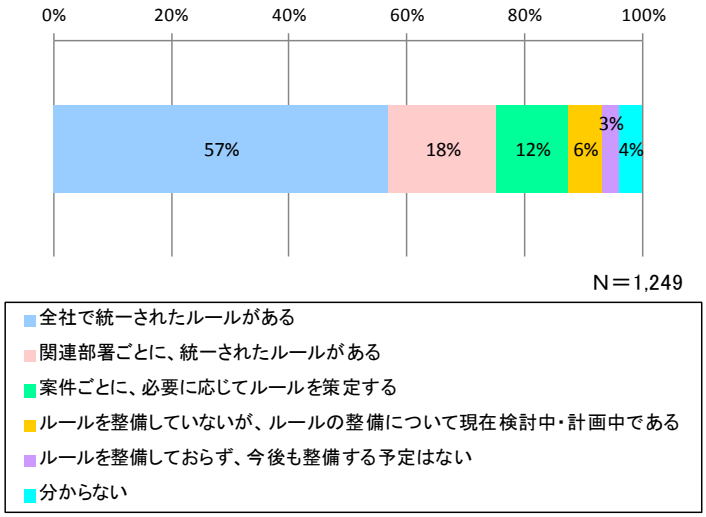
3.5. 情報セキュリティに関する SCRM の全社統一ルールの策定

委託先または再委託先等に対する情報セキュリティ管理については、前述したセキュリテ

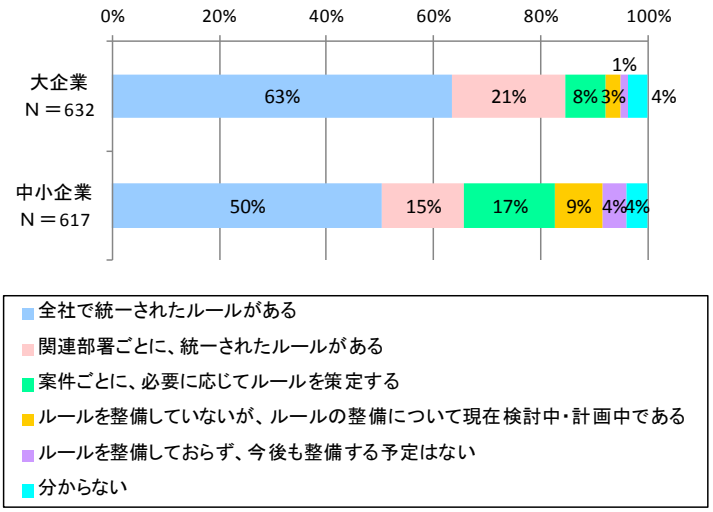
ィ対策状況の把握とともに、委託先が遵守すべき情報セキュリティ管理を定めたルールの適用によりガバナンスを効かせるという企業の意識が顕著である。委託先が遵守すべき情報セキュリティ管理を定めたルールについては、企業の約 87%が策定している。

このようなルールの運用形態については、①全社で統一されたルールを運用する形態や、②関連部署ごとに統一されたルールを運用する形態、③案件ごとにルールを策定し運用する形態といった多様な形態が存在するが、このうち、上記①の割合は、全体の約 57%を占め、全社の情報セキュリティガバナンスを強化する傾向がみられる。このような傾向は、中小企業よりも大企業の方が強いことが読み取れる。

図表 3-17 委託を行う際の委託先が遵守すべき情報セキュリティ管理を定めたルールの策定の有無・状況（単回答）



図表 3-18 委託を行う際の委託先が遵守すべき情報セキュリティ管理を定めたルールの策定の有無・状況（大企業と中小企業の比較）（単回答）



他方、全社で統一されたルールについては、海外の委託先を含めた適用を促進することが、情報セキュリティガバナンス強化の視点からも求められる。企業ヒアリングによると、日系企業については、海外の委託先を対象とした、情報セキュリティに関する SCRM にかかるルール適用は、各国・地域における法規制や商慣習などの違いもあり、これからの検討課題、あるいは、着手し始めた段階であることが分かった。また、海外の委託先を含むサプライチェーン全体に、日系企業が自社で策定した自主基準のルールや、その中に規定されているセキュリティ管理プロセスをローカライズして適用しようとしているのに対し、米国企業は、業界標準のルールや特定の国・地域の法令による要求基準等に依存しないグローバル化されたセキュリティ管理プロセスを適用しようとしており、その背景として、米国企業が、グローバルに分散し広範に及ぶ委託先に対して自主基準のルールを適用する場合に監査にかかる負担が大きくなると見ていることも分かった。

これまで日系企業の多くが国内の委託関係だけで概ねビジネスを充足できていたため、自社で策定した自主基準のルールの適用が可能であったが、グローバル化の進展によって委託関係が国内、海外を含め複雑かつ広範になり、そのような運用形態が通用しにくくなってきている。日系企業は、今まさに、委託先または再委託先等に対する情報セキュリティ管理を中心として、将来の情報セキュリティガバナンス体制をどのように構築していくのかを決める岐路に立たされていると言うことができる。

図表 3-19 委託関係の重層的な連鎖やグローバル化に対する取組みの実効性に関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 当社グループ全体で情報セキュリティに関する SCRM の統一ルールを整備している。しかし、海外グループ会社へのルールの適用徹底については、各国における法規制や商慣習などの違いもあり、これからの検討課題である。
IT ベンダー	● 情報セキュリティに関する SCRM の取組みは、海外の委託先に対しては、まだ着手し始めたばかりである。資本関係のある海外の委託先に対しては、国内の委託先向けに定めたセキュリティ管理の全社統一ルールをもとに運用する方針である。しかしながら、国・地域ごとに法令遵守事項が異なるため、全社統一ルールに対して、国・地域ごとに細かい変更を加えて運用している。
自動車メーカー	● 自動車部品、バックエンドシステム、工場設備などのセキュリティ管理を包括した委託先向けの全社的なルールは整備されていない。
自動車メーカー	● グローバル企業としての運営を志向するなかで、すべてのプロセスをグローバルスタンダードに基づくプロセスに更新しようとしている。これにより、複数段階において契約合意が必要となるプロセスや、仕様とは異なる製品が開発されるプロセスを不要となるようにする。しかしながら、各国・地域の法規制の違い等から、グローバルスタンダードに基づくプロセスを統一的に運用することが不可能となる場面も生じ得る。 ● また、各国・地域の法規制に対して、解釈を誤って適用するなど遵守が不十分となる場

	合には、罰則等を受けるリスクも起こり得る。 ● このため、全社的な取組みとして、各国・地域の法規制の違いやこれに起因するリスクを追跡し管理できるようにするための専門組織を立ち上げている。
製薬メーカー	● グローバルでの情報セキュリティに関する SCRM の取組みについては、なるべく各国の要求基準等に固執・依存しない最善のセキュリティ管理体制を追求しているが、個人情報の取り扱いのように米国、欧州、ロシア、中国それぞれで法律上の義務化された要求基準等が異なる場合にはローカライズ対応を実施せざるを得ない状況である。
NIST	● 企業の多くが、情報セキュリティに関する SCRM にかかる自社の自主基準を世界中のサプライヤーに課しているが、その場合、当該基準を基に委託先等を監査する必要があり、このことが国際標準規格に準じた第三者による監査と違って、委託先等が当該基準で要求しているものを保護しているかを証明することを難しくしている。 ● そのため、監査の実効性・効率性を高めていくにあたっては、第三者による監査が可能で、かつ広範な分野に適用可能な国際標準規格の策定とそれに基づく認証制度の確立が必要になると考えられる。

3.6. 情報セキュリティに関する SCRM のルール遵守の徹底

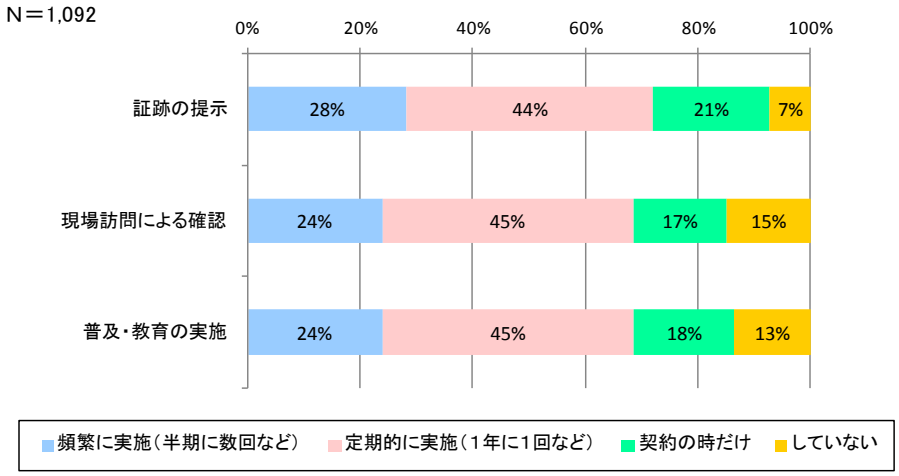
委託先に対する、委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底に向けた取組みについて、アンケート調査では、「証跡の提示」、「現場訪問による確認」、「普及・教育の実施」といった監査の観点からルール遵守の徹底を確認する 3 つの取組みを採り上げている。

「証跡の提示」、「現場訪問による確認」、「普及・教育の実施」のいずれにおいても、契約時のみの徹底や不徹底といった取組み自体に積極的ではない企業が約 30%前後存在する。

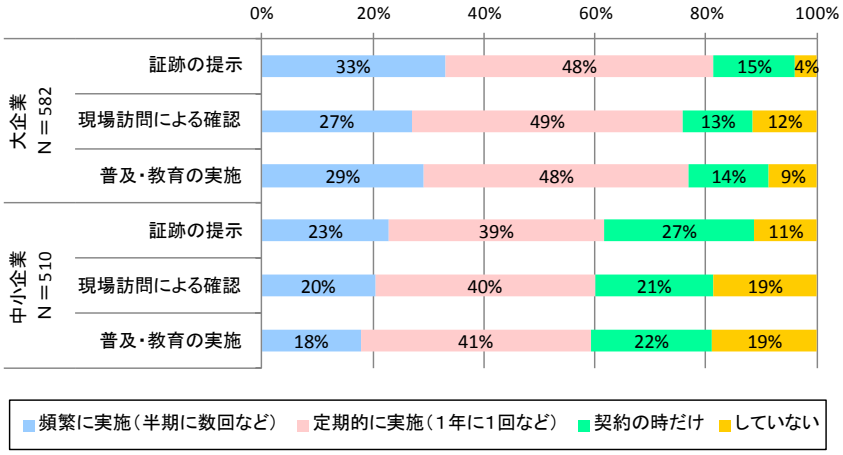
同割合は、大企業では約 20%前後であるのに対し、中小企業では大企業の 2 倍に相当する約 40%前後まで大きく跳ね上がることから、このままでは、中小企業は委託先に対する情報セキュリティ管理に十分に対応できないことが懸念される。

他方、重要インフラ企業においては、「証跡の提示」、「現場訪問による確認」、「普及・教育の実施」といった確認手法のいずれにおいても、「頻繁に実施（半期に数回など）」や「定期的に実施（1 年に 1 回など）」といった取組み自体に積極的である企業が約 70%～80%存在する。重要インフラ企業における、監査の観点からルール遵守徹底を確認する積極的な取組みが約 70%～80%で十分かどうかは議論が分かれるところであるが、取組み自体に積極的ではない企業も約 20%～30%存在することから、ルール遵守の更なる徹底が望まれる。

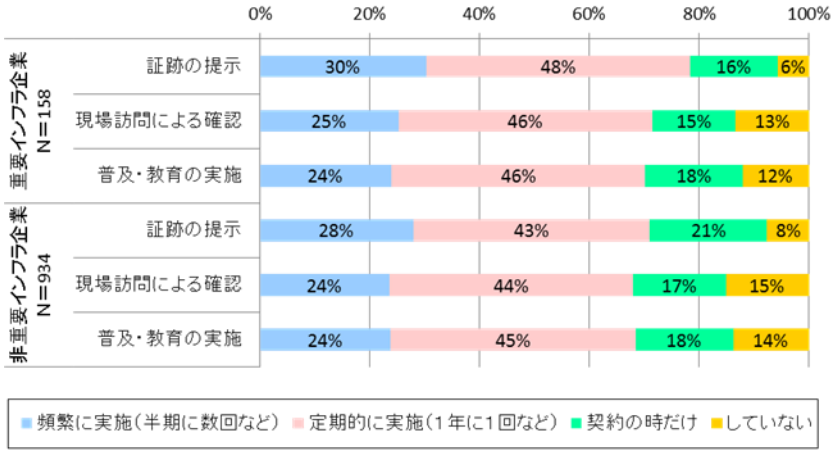
図表 3-20　委託先への委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底（単回答）



図表 3-21　委託先への委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底（大企業と中小企業の比較）（単回答）



図表 3-22　委託先への委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底（重要インフラ企業と非重要インフラ企業の比較）（単回答）



また、委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底において対応が特に難しいのが、委託先における再委託の運用である。企業ヒアリングによると、このような運用の形態には、①原則、再委託を禁止しつつも条件次第で再委託が例外的に容認される形態と、②再委託を容認しつつも条件次第で再委託が禁止される形態の 2 種類の形態が、企業において採られていることが明らかになっている。

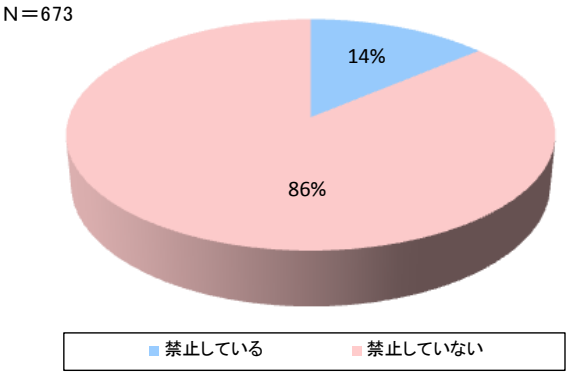
前者の①では、再委託先の社員を委託先に常駐させるという条件と引き換えに、再委託を例外的に容認する場合がある。他方、後者の②では、委託先がセキュリティ対策状況等の必要となる情報を開示しない限り、再委託を容認しない場合がある。

図表 3-23 情報セキュリティに関する SCRM における再委託の取り扱いに関する主なヒアリング調査結果

回答企業	主な発言等
IT ベンダー	● 原則、再委託を禁止する規定を設けている。しかし、当社と取引のある委託先の半分以上は、再委託を行っている。再委託の多くの場合、再委託先の社員に当社に常駐してもらうことにより、情報漏えいを回避する取組みを行っている。 ● 防衛・宇宙産業、金融業、通信業では、顧客が再委託の禁止を要求する場合もある。
IT ベンダー	● 当社では、全社統一ルール上に再委託を禁止する規定を設けていない。ただし、委託先のセキュリティレベル分けを行ったうえで、赤信号の評価が下された委託先に対しては、一定の条件や期間において再委託を禁止している。
自動車メーカー	● 再委託先以降に対しては、直接的にサプライチェーンリスクマネジメントの取り組みを実施することはない。委託先が再委託を行う際には、標準契約書上で当社が委託先に対し、課しているセキュリティ義務と同じ内容を、再委託先にも遵守してもらう。委託先に再委託を行う旨を申告してもらい、委託先が再委託先の情報セキュリティ管理責任を負う形を採っている。
自動車メーカー	● 再委託を禁止する規定は設けていない。下請け業者を使用することは一般的であり、規定の多くはそれを考慮して策定される。その一方で、当社では、下請け業者の情報開示を盛り込んだ規定の改正を検討している。セキュリティリスクへの懸念について対応意識が高まるなか、下請け業者やその開発者の詳細について把握する必要性が高まっている。
製薬メーカー	● 委託先における再委託を禁止する一般条項を設けているが、委託先で本当に再委託が実施されていないかを管理するのは非常に難しい。例えば、当社の委託先であるマーケティング会社が、当社のリスク評価プロセスが適用されていない再委託先に対して、ウェブサイトの設計・開発にかかる業務を再委託する事態が起きている。このようなケースでは、マーケティング会社において、情報セキュリティに関する SCRM の重要性に対する認識が希薄であったことが事態を招いた原因であった。優秀な IT 人材を抱えていないマーケティング会社が委託先となる際には、再委託先が前提となるうえ、セキュリティ管理を行うことも困難であることから、過去には、問題が発生したこともある。

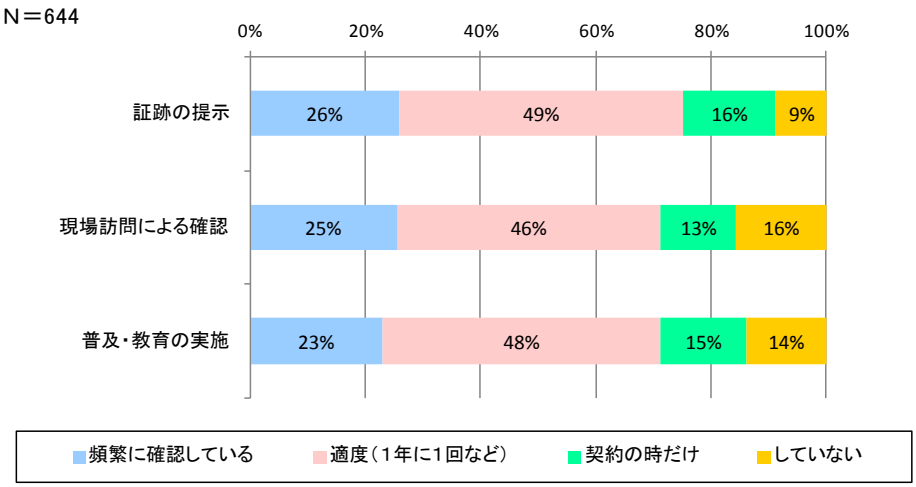
他方、委託先に対して再委託の許可を与える場合に遵守を求める情報セキュリティ管理の条件として、再委託先における再委託を禁止している企業は僅か約 14%にしか過ぎない状況である。委託先のみならず、再委託先における再委託の禁止についても、再委託先に対し、ルール遵守の徹底を求める対応が難しいと見ている企業が多いことを裏付けるような結果が得られている。

図表 3-24 委託先に対して再委託の許可を与える場合に遵守を求める情報セキュリティ管理の条件
～遵守を求める情報セキュリティ管理の条件としての再委託先における再委託の禁止～（単回答）



その一方で、再委託先に対する、監査の観点からルール遵守徹底を確認する取組みは、「証跡の提示」、「現場訪問による確認」、「普及・教育の実施」のいずれにおいても、契約時のみの徹底や不徹底といった取組み自体に積極的ではない企業が約 30%程度存在しており、再委託先に対する情報セキュリティ管理に十分に対応できていない。

図表 3-25 再委託先への委託先が遵守すべき情報セキュリティ管理を定めたルール遵守の徹底（単回答）



このように、証跡の提示や現場訪問を通じてルール遵守を確認する運用とルールを通じ

て再委託を禁止する運用については、委託元が委託先または再委託先に対して、必ずしも十分徹底できていないのが現状である。

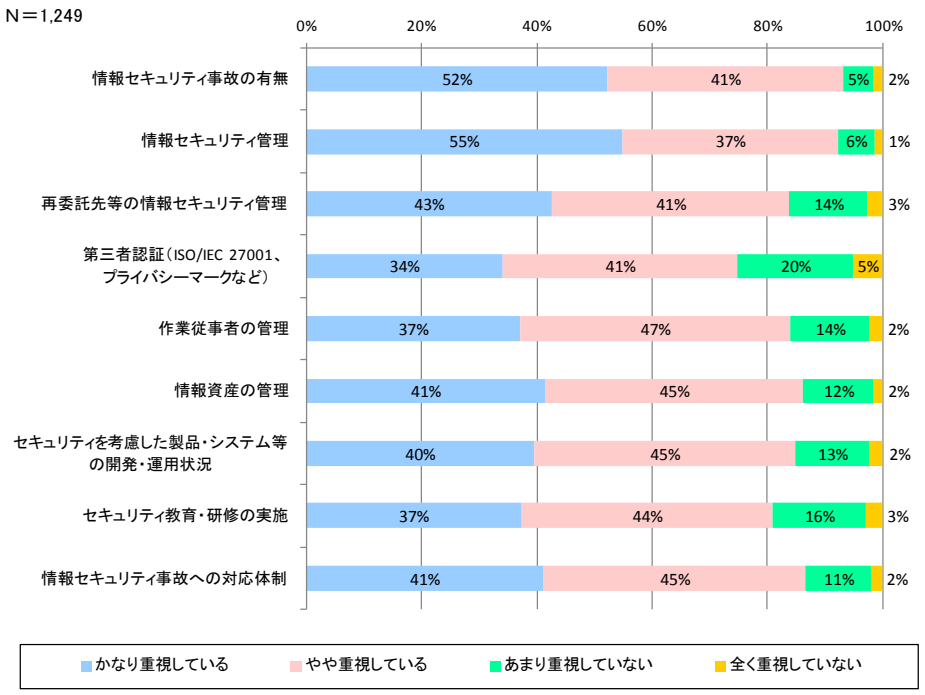
3.7. 委託を行う際のセキュリティ上のリスクの認識

委託先を選定する際に、委託元が重視している情報セキュリティ管理の観点について、「かなり重視している」、「やや重視している」の双方を合わせた割合でみると、情報セキュリティ事故の有無や、情報セキュリティ事故への対応体制が上位を占める。

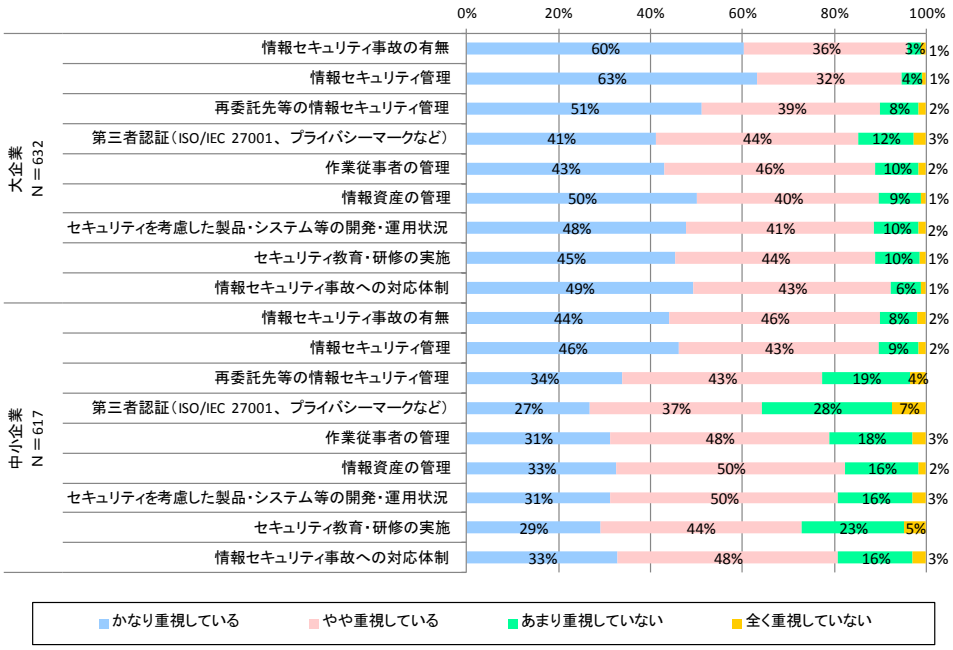
委託元が想定する情報セキュリティリスクの種類については、委託元の IT システム設計・開発・運用に関わるサプライチェーンと委託元が提供する製品またはサービスの設計・開発・運用に関わるサプライチェーンとで異なるものと見られる。

また、この点については、企業ヒアリングにおいても、前者に関わり、顧客と共に事業を行う IT ベンダーでは、顧客から預かったデータの漏洩事故に繋がるリスクを最も警戒しており、他方、後者に関わる製造メーカーでは、顧客に提供する製品の安全性・信頼性の低下に繋がるリスクを最も警戒するなど、業種によって、委託元が想定する情報セキュリティリスクが大きく異なることが明らかになった。

図表 3-26 委託先を選定する際に委託元が重視している情報セキュリティ管理の観点（単回答）



図表 3-27　委託先を選定する際に委託元が重視している情報セキュリティ管理の観点
（大企業と中小企業の比較）（単回答）



図表 3-28　委託を行う際のセキュリティ上のリスクの認識やセキュリティ保護の考え方に関する主なヒアリング調査結果（再掲）

回答企業	主な発言等
IT ベンダー	● 委託先でセキュリティ事故が発生した場合は、当社グループの管理不備が問われ、最終的には委託元が責任を負うことになる。このため、当社グループ全体が、委託先と一体となって情報セキュリティ強化に取り組むことにより、顧客からの信頼を得ることが大切であると考えている。 ● 取引先に対し、顧客のデータを預かっており、CIA の中でも Confidentiality（機密性）を一番重視している。 ● 納品物に関しては、委託先に対して事前に脆弱性をチェックするよう依頼している。また、セキュアな開発環境下で開発に取り組んでいる。しかしながら、脆弱性を確認できる領域には限界があるため、最低限のセキュリティ担保で製品・サービスを提供できるように取組んでいる。
IT ベンダー	● 情報セキュリティに関するリスクマネジメントに取り組む目的は、①当社が顧客と共に事業を行ううえでセキュリティ事故を起こさないようにすること、②当社の納品物に対する最低限のセキュリティ担保を徹底できるようにすることである。
自動車メーカー	● 万が一、車両のセキュリティ事故を起こした場合には、企業イメージのダウンに繋がり、販売部門に迷惑がかかってしまう。また、リコールサービスキャンペーンが必要となるため、膨大なコストが発生する。 ● セキュリティ事故の内容次第ではあるが、例えば、車両のメーターが攻撃されて、表示

	不能となった場合には、車両に関する法規制を遵守できなくなる。このような事態は避けなければならない。
自動車メーカー	● 製品のセキュリティリスクとして、①製品の安全性、②プライバシーの保護、③製品の信頼性の 3 つのリスクを扱っている。自動車同士が繋がっているシステムでは、製品に対する攻撃の影響が、同システムの基盤を介して、販売管理システム等の企業の基幹システムにまで波及する可能性がある。自社が構築するサプライチェーン以外の外部ベンダーの部品を使用できるようになっている場合は、その部品が、製品やシステムに対して悪意のある何らかの行動を起こし、攻撃の機会となるリスクが増す。
製薬メーカー	● セキュリティ保護対象は、患者の安全性、患者のデータ(職員・顧客のデータ)、自社の知的財産、並びに法令であり、優先順位はこの順に従う。 ● セキュリティ保護対象が、どのように保護されるかは、何を委託するかによって決まる。例えば、部品製造の委託を行う際には、少なくとも当社の製造環境でのセキュリティ管理と同等のレベルのセキュリティ管理を担保できるようにする必要がある。

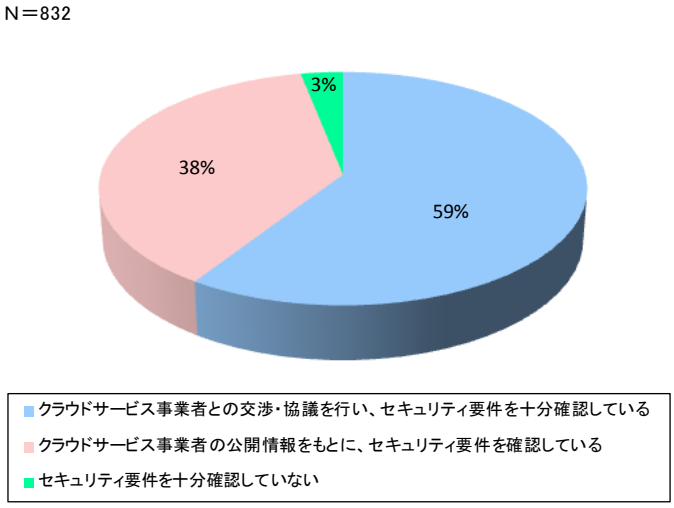
3.7.1. クラウド選定時におけるセキュリティ要件の確認

IT システムの開発・運用や提供する製品またはサービスの開発・運用等でクラウドサービスを使用している企業が、当該サービスの選定時において、どのような方法により当該サービスにおけるセキュリティ要件を確認しているかについては、約 59%の企業が、クラウドサービス事業者との交渉・協議と回答しており、公開情報の約 38%よりも、21 ポイントも高い結果となっている。

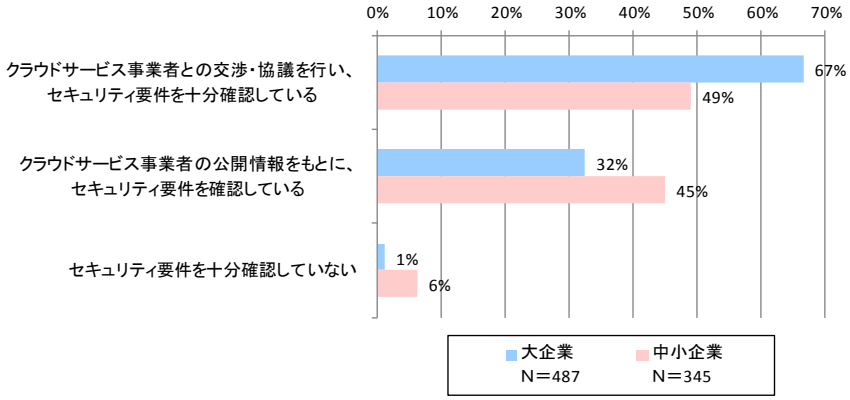
企業が抱えるクラウドに対するセキュリティ面での不安は、公開情報により示されたセキュリティ要件のみでは払拭することが難しいため、クラウドサービス事業者との交渉・協議の場でセキュリティ要件を確認することが必要になってきている。この傾向は、中小企業よりも大企業の方で強まっており、大企業においては、3 社に 2 社がクラウドサービス事業者との交渉・協議を行い、セキュリティ要件を十分に確認している。

顧客から預かったデータの漏洩事故に繋がるリスクに対しては、当該データの保存・管理に使用されるクラウドサービスの選定時において、セキュリティ要件を確認することが特に重要になってきている。

図表 3-29　委託元のクラウド選定時におけるセキュリティ要件の確認（単回答）



図表 3-30　委託元のクラウド選定時におけるセキュリティ要件の確認（大企業と中小企業の比較）（単回答）

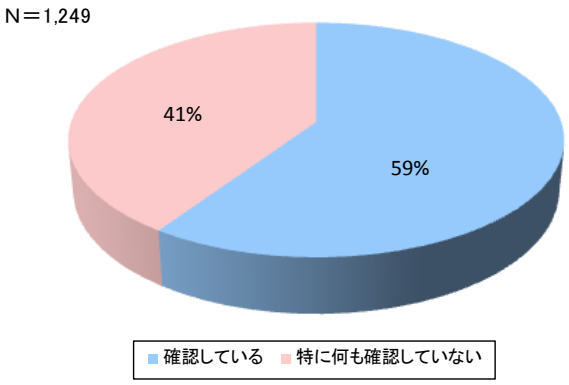


3.7.2.　納品物の不正動作（マルウェアの混入等）の確認

顧客に提供する製品の安全性・信頼性の低下に繋がるリスクに対しては、マルウェアの混入等による不正動作や使用されるソフトウェアやハードウェアの脆弱性といった納品物に対するセキュリティ脅威を確認することが特に重要になってきている。

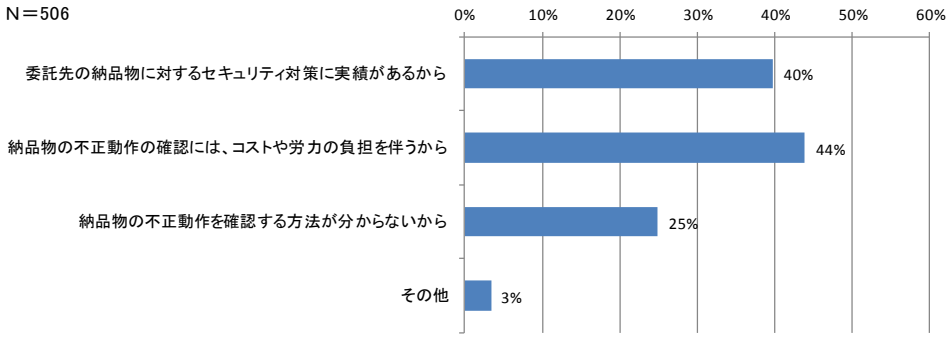
このうち、納品物に対するマルウェアの混入等の不正動作について確認していない企業は約 41%に達している。不正動作については、マルウェアによる外部のＣ＆Ｃサーバーへの通信に代表されるように、IT システムや、IT 活用製品またはサービスの運用を実際に行って初めて分かる場合もあり、納品時における確認だけで全て充足することには自ずと限界があると考えられる。

図表 3-31　納品物の不正動作（マルウェアの混入等）の確認の有無（単回答）



納品物の不正動作を確認していない理由としても、コストや労力の負担を挙げる企業の割合が約 44%と最も高いことから、納品物の不正動作の確認作業にかかる手間を軽減するために、何らかの仕組みを確立することが求められていると言える。

図表 3-32　納品物の不正動作（マルウェアの混入等）を確認していない理由（複数回答）



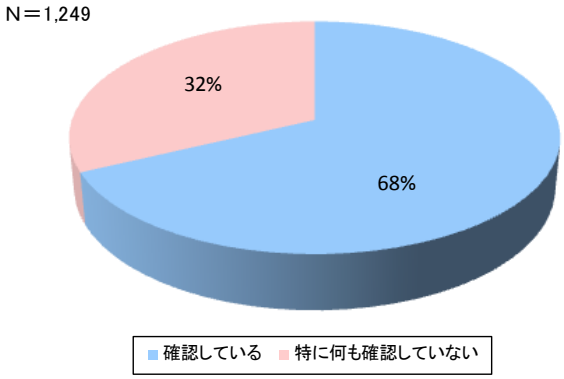
3.7.3.　納品物に使用されるソフトウェア及びハードウェアの脆弱性の確認

納品物で使用されるソフトウェアの脆弱性（OS、プログラム、ソースコード、オープンソース・ソフトウェア等）については、概ね 3 社に 1 社が確認していない。また、納品物で使用されるハードウェア（データ記録・格納媒体、管理・設定機能等）の脆弱性については、概ね 2 社に 1 社が確認していない。

同一システム上に多様なソフトウェアが混在している場合やブラックボックス化したソースコードが使用されている場合、既知の脆弱性情報が多いためテスト項目が多くなる場合などが、納品物における脆弱性の確認を難しくさせていると考えられる。

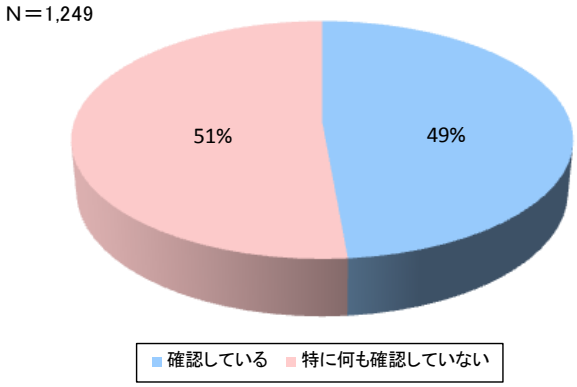
図表 3-33　納品物に使用されるソフトウェアの脆弱性

（OS、プログラム、ソースコード、オープンソース・ソフトウェア等）の確認の有無（単回答）



図表 3-34　納品物に使用されるハードウェアの脆弱性

（データ記録・格納媒体、管理・設定機能等）の確認の有無（単回答）



3.8.　調査仮説の検証と考察

「2.2. 調査仮説の構築とその考え方」で前述した調査仮説について、アンケート調査結果に基づき検証した結果を以下に示す。

検証結果を見る限りは、企業における情報セキュリティに関するSCRMの取組みは当初、調査仮説で想定していた取組みのレベルを上回るレベルで取組みが進んでいることが明らかになった。

しかしながら、情報セキュリティに関するSCRMに積極的に取り組む企業へのインタビュー調査結果によると、長年取り組んでいる企業であっても取組みを委託先等に浸透させることが難しいと認識しており、本調査仮説の検証結果とのギャップが生じている。

ついては本調査仮説の検証結果については、次のようなバイアスが想定される。

①全般的に情報セキュリティ管理に対する意識が高いという回答が得られたものの、今回

のアンケート調査における設問の抽象度が高く、また取組みのレベル感についても設問上で必ずしも十分考慮されていなかったため、少しでも取組みがあれば、全体的に取組みがなされているとポジティブに捉えた回答票が集まったことが考えられる。

②本調査タイトルや、回答者の所属部署の絞り込みにより、情報セキュリティに関する SCRM について比較的リテラシーの高い属性の回答者が多数派となったことが予想される。

全般的な情報セキュリティに関する SCRM において、国内組織のリスクの実態を把握するにはもう少し踏み込んだ調査が必要になると考えられる。これらを踏まえ、以下に調査仮説への検証結果を示す。

図表 3-35 調査仮説の検証結果

調査仮説	検証結果
仮説 1：委託元は、直接の委託先についてはセキュリティの対策状況を把握できているが、再委託先（孫請負以降）までは把握しきれていない。	委託元は、直接の委託先についてはセキュリティの対策状況を把握している企業の割合は約 86%を占めた。再委託先または再々委託先以降のサプライチェーンを有する企業のうち、再委託先または再々委託先以降のセキュリティ対策状況を把握している企業は約 47%である。
仮説 2：情報セキュリティに関する SCRM の必要性に対する委託元の認識は、大手企業（重要インフラ企業）、大手企業（非重要インフラ企業）、中堅・中小企業の順でサプライチェーンリスクマネジメントへの必要性の認識が低くなる。	委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性について、経営層が認識している企業の割合は、大企業で約 83%、中小企業で約 73%である。重要インフラ企業と非重要インフラ企業の認識を比較すると重要インフラ企業の割合は約 83%、非重要インフラ企業の割合は約 77%である。
仮説 3：委託元は、委託先に対し、再委託を許可する場合は、一定の条件を課している。	再委託を行っている企業のうち、委託先に対して再委託の許可を与える場合に情報セキュリティ管理の条件を課している企業の割合は約 98%である。
仮説 4：委託元は、全社に情報セキュリティに関する SCRM の統一ルールはない。	委託を行う際の委託先が遵守すべき情報セキュリティ管理を定めたルールについて、全社で統一されたルールが策定されている企業の割合は約 57%である。
仮説 5：委託元は、委託先又は再委託先などに対し、ルールを徹底していない。	委託先や再委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルー

	ルの遵守については、契約時のみの徹底にとどまる企業や徹底していない企業の割合が、委託先、再委託先ともに約 30%存在する。
仮説 6：委託元は、委託する際にセキュリティの保護対象を特定していない。	委託を行うに際して、セキュリティの保護資産を指定していない企業の割合は約 16%である。
仮説 7：委託元は、クラウド選定時にセキュリティ要件を十分に確認していない。	クラウドを利用している企業のうち、クラウド選定時において、セキュリティ要件を十分に確認していない企業の割合は約 3%である。
仮説 8：委託元は、納品物に使用されるオープンソースの脆弱性について確認していない。	委託を行う際に納品物に使用されるソフトウェアの脆弱性を確認している企業は約 68%である。
仮説 9：委託元は、納品物の不正動作（マルウェアやバックドア混入等）について確認していない。	委託を行う際に納品物の不正動作（マルウェアの混入等）を確認していない企業は約 41%である。

4. 本調査の総括

4.1. 情報セキュリティに関するSCRMの取組み普及・推進時に考えられる制約要因

前述したアンケート調査やヒアリング調査の結果から見えてきた情報セキュリティに関するSCRMの取組みの普及を推進していくうえで制約要因となることが懸念される点としては、以下の3点が挙げられる。

①再委託先以降への情報セキュリティに関するSCRMの取組みの普及については、その推進を直接取引のある委託先に依存せざるを得ない状況となっている点

②委託先等に対して情報セキュリティ管理を定めたルール遵守の徹底を図る委託元の負担が一様ではない点

③納品物のセキュリティ品質保証を委託元による納品時の確認や委託先による事前の確認だけで全て充足することには自ずと限界が生じる点

上記①については、前述の図表3-7に示したとおり、再委託先または再々委託先以降までのサプライチェーンを有する企業のうち、セキュリティ対策状況を把握している範囲が委託先までである企業の割合は約53%、再委託先または再々委託先以降までである企業の割合は約47%となっており、委託元は、直接取引のある委託先についてはセキュリティの対策状況を把握できているが、再委託先以降まで把握できている組織は少ないことが分かった。

これについては、前述の図表3-8に示したとおり、再委託先の情報セキュリティ管理は、契約関係がなく委託元が直接行うことができないため、委託先にその管理を一任せざるを得ない状況になっている場合があることが分かった。

また、その委託先については、前述の図表3-13に示したとおり、情報セキュリティ管理にかかる協力への消極的な姿勢やコスト負担の制約などの課題があり、自らの情報セキュリティ管理であっても十分になされていない場合があることが分かっており、これらの状況が情報セキュリティに関するSCRMの取組みの普及推進の足かせになっていると考えられる。

上記②については、委託関係がグローバルに分散し広範に及ぶ企業とそうではない企業とで、委託元の負担の格差は相当程度ある。前者の企業においては、前述の図表3-19に示したとおり、各国・地域における法規制や商慣習などの違いが、グローバルでの全社統一ルールの適用を難しくさせており、ローカライズ対応が必要となることが分かった。

また、委託を行う際のセキュリティ保護資産の特定についても、前述の図表3-14で示したとおり、セキュリティ保護資産を包括的に指定している企業の割合が約49%、セキュリティ保護資産を個別に指定している企業の割合が約34%となっており、委託で扱う製品やITシステムの対象範囲が広範で複雑になればなるほど、想定・対応すべき情報セキュリティリスクの種類も多くなるため、セキュリティ保護資産の特定のために多大な時間や労力を

かけなくて済む包括的な指定が、委託元に選択されがちであることが分かった。

このように情報セキュリティに関する SCRM の取組みは、委託関係の構造、委託で扱う製品や IT システムの対象範囲、再委託の許可を与える場合に委託先に遵守を求める情報セキュリティ管理の条件など多くの面が作用しており、委託先等に対して情報セキュリティ管理を定めたルール遵守を一律に徹底することが難しいのが現状であると言える。

このため、情報セキュリティに関する SCRM の取組みの普及を推進するにあたっては、情報セキュリティ管理を定めたルール遵守の徹底の負担を、委託元だけでなく、委託先や再委託先、再々委託先以降も含めたサプライチェーン全体で低減していくことが重要な課題になると考えられる。

上記③については、IT システムの設計・開発・運用や、提供する製品またはサービスの設計・開発・運用に関わるサプライチェーンの中で取り扱われる情報セキュリティリスクとして、従来は個人情報の窃取・漏えいなど機密性に支障をきたすリスクが最初に挙げられることが多かった。しかし近年においては、IT システム関連機器に対する不正改造やソフトウェアへの不正な機能の埋め込み、脆弱性の混入など、システム、ソフトウェア、機器などの機能の完全性や可用性に支障をきたすリスクも注視されるようになった。

その一方で、前述の図表 3-31 や図表 3-33、図表 3-34 に示したとおり、納品物の不正動作（マルウェアの混入等）、納品物に使用されるソフトウェアやハードウェアの脆弱性に対して、確認を行っていない委託元企業がそれぞれ約 4 割、約 3 割、約 5 割を占めており、このままでは近年高まる情報セキュリティリスクに十分に対応できないことが懸念される。

完全性や可用性の確保は、重要インフラ企業においては国民生活や経済活動に直接的な影響を与えるため、特に大切であるが、後述の参考図表 2-45 に示したとおり、重要インフラ企業においても同じ傾向が見られる。

また、委託元の中には、委託先に対しては、事前に納品物の脆弱性の確認を行うことを要請している企業も見られるが、前述の図 3-16（再掲のため図 3-28 と同じ）に示したとおり、このような委託先の取組みには限界があると認識している IT ベンダーが存在することも分かった。

これらの状況は、納品物のセキュリティ品質保証を、委託元による納品時の確認や委託先による事前の確認だけで全て充足することには自ずと限界が生じることを裏付けるような結果となっている。

なお、上記①、②及び③が、情報セキュリティに関する SCRM へ取り組む際にどの程度の制約要因になり得るかなど、今後その実態をより詳しく把握することにより、情報セキュリティに関する SCRM の取組みの普及推進のヒントが得られる可能性がある。

4.2. 今後に向けて

今後に向けては、委託元からみた情報セキュリティに関する SCRM の取組みの動向だけでなく、委託先や再委託先以降からみた情報セキュリティに関する SCRM の取組みの動向や、情報セキュリティに関する SCRM の取組みを支援する政府や業界団体等の支援ニーズの動向についても把握することに努めるとともに、これらを踏まえた情報セキュリティに関する SCRM の取組みの普及を推進していくうえでの制約要因の実態、情報セキュリティに関する SCRM の取組みの方向性、及び委託関係を構成する各ステークホルダーの具体的な対応の在り方について、有識者や事業者等のさまざまな意見を聴取しつつ検討を行うことが重要である。

参考資料

参考資料 1 アンケート調査票

IT システムの構築や IT 活用製品の開発製造の業務において、業務の一部が、他の企業に委託・再委託される場合があります。この場合は、委託先の情報セキュリティ対策状況の把握・評価や、情報セキュリティに関するリスク管理を適切に行うことが重要です。本調査では、これを『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』と呼びます。

ここからは、『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』の実態についてお伺いします。

【注意事項（以降アンケートに御回答になられる前に必ずお読みください)】

1. 本調査の対象は、以下の 2 つの範囲になります。対象範囲が、『物流のサプライチェーンではない』ことに留意してください。
   ①貴社の IT システム設計・開発・運用に関わるサプライチェーン
   ②貴社が提供する製品、またはサービスの設計・開発・運用に関わるサプライチェーン

2. アンケートの回答については、あなた自身が勤務・所属する企業・団体において、主にあてはまるものを選んで、御回答いただきますよう御願い申し上げます。

3. 本調査で定義している『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』は、委託先の情報セキュリティ対策状況の把握・評価や、委託先で発生する情報セキュリティに関するリスクの管理、委託元から要求される情報セキュリティに関するリスクの管理等を適切に行うことを指しています。

4. 『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』の取組みにより保護される対象は、必ずしも『情報の機密性』だけではありません。例えば『情報の完全性（データの改ざん)』や、『サービスの可用性や真正性』、『製品の真正性（偽物の納品や、不正プログラムの埋め込み)』なども、本調査における保護の対象とお考えください。

（回答者：本調査対象者全員）
問 1. あなたの勤務先・所属先の企業・団体（以下、貴社と呼ぶ。）において、委託元（貴社へ委託している組織）は存在しますか。（ひとつだけ）【必須】
1. 存在する
2. 存在しない

（回答者：本調査対象者全員）
問 2. 貴社において、直接取引のある委託先の数について、最も近いものをお知らせください。（ひとつだけ）【必須】
1. 1 社～10 社
2. 11 社～50 社
3. 51 社～100 社
4. 101 社以上

（回答者：本調査対象者全員）
問 3. 貴社の委託先の所在地について、次のうち、あてはまるものをお知らせください。（ひとつだけ）【必須】
1. 国内のみ
2. 海外のみ
3. 国内、海外の双方

（回答者：本調査対象者全員）
問 4. 貴社は、委託先等における情報セキュリティ対策状況を把握していますか。（ひとつだけ）【必須】
1. 直接の取引がある委託先のみ把握している
2. 再委託先まで把握している
3. 再々委託先以降も把握している
4. いずれも把握していない

（回答者：問 4. で選択肢 1 と回答した方にうかがう。）
問 5. 貴社からみた、再委託先等の存在について、あてはまるものをお知らせください。（ひとつだけ）【必須】
1. 再委託先はない
2. 再委託先はあり、再々委託先はない
3. 再委託先もあり、再々委託先以降もある
4. 再委託先はあるが、再々委託先があるかどうか分からない
5. 再委託先等があるかどうか分からない

（回答者：問 4. で選択肢 2 および 3 と回答した方、または問 5. で選択肢 2、3 および 4 と回答した方、にうかがう。）

問 6. 貴社は、委託先に対し再委託の許可を与える場合、情報セキュリティ管理に関して条件を課していますか。あてはまるものをお知らせください。（いくつでも）【必須】

1. 貴社から事前の了解を得る
2. 貴社の情報セキュリティ管理に関する規定に、再委託先が適合していることを示す証跡（例：自己点検の結果や監査記録など）を提出させる
3. 再委託先における機密の管理は、委託先が責任を負う
4. 再委託先における情報セキュリティ管理（機密の管理を除く）は、委託先が責任を負う
5. 再委託先に、委託先と同一のセキュリティルールを遵守させる
6. 再委託先における再委託を禁止している
7. その他の条件（具体的に　　）
8. 特に何も条件を課していない（排他選択肢）

（回答者：問 6. で選択肢 8 と回答した方にうかがう。）

問 7. 貴社が、委託先に対し再委託の許可を与える場合に、特に何も条件を課していない理由について、お知らせください。（いくつでも）【必須】

1. 貴社が直接再委託先の管理をするため
2. 委託先が独自に運用している、再委託の管理プロセスの信頼性や安全性が高いため
3. 貴社において、再委託先を管理するための手間やコストを負担できないため
4. 委託先において、再委託先を管理する能力が十分ではないため
5. その他（具体的に　　）

（回答者：本調査対象者全員）

問 8. 委託先又は再委託先等に対する情報セキュリティ管理の強化・徹底が必要になることについて、貴社の経営層は、その重要性をどの程度、認識されていますか。最も近いものをお知らせください。（ひとつだけ）【必須】

1. 認識が大いにある
2. 認識がややある
3. どちらともいえない
4. 認識があまりない
5. 認識がまったくない

（回答者：本調査対象者全員）

問 9. 貴社では、委託を行う際に、委託先が遵守すべき情報セキュリティ管理を定めたルール（規定など）はありますか。（ひとつだけ）【必須】

1. 全社で統一されたルールがある
2. 関連部署ごとに、統一されたルールがある
3. 案件ごとに、必要に応じてルールを策定する
4. ルールを整備していないが、ルールの整備について現在検討中・計画中である
5. ルールを整備しておらず、今後も整備する予定はない
6. 分からない

（回答者：問 9. で選択肢 1～3 と回答された方のみ）

問 10. 貴社は、委託先に対し、問 9. でお答えになられたルールの遵守を、どの程度徹底していますか。（それぞれひとつずつ）【必須】

	頻繁に実施（半期に数回など）	定期的に実施（1 年に 1 回など）	契約の時だけ	していない
1. 証跡の提示※1				
2. 現場訪問による確認				
3. 普及・教育の実施				

※1 証跡…（例：自己点検の結果や監査記録など）

（回答者：問 6 に誘導された方のうち、問 9. で選択肢 1～3 と回答された方のみ）

問 11. 貴社は、再委託先に対し、問 9. でお答えになられたルールの遵守を、どの程度徹底していますか。（それぞれひとつずつ）【必須】

	頻繁に確認している	適度（1 年に 1 回など）	契約の時だけ	していない
1. 証跡の提示※1				
2. 現場訪問による確認				
3. 普及・教育の実施				

※1 証跡…（例：自己点検の結果や監査記録など）

（回答者：本調査対象者全員）

問 12. 貴社は、委託先を選定する際に、情報セキュリティ管理に関するどのような観点を重視していますか。以下に示すそれぞれの重視度合いをお知らせください。（それぞれひとつずつ）【必須】

	かなり重視している	やや重視している	あまり重視していない	全く重視していない
1. 情報セキュリティ事故の有無				
2. 情報セキュリティ管理				
3. 再委託先等の情報セキュリティ管理				
4. 第三者認証（ISO/IEC 27001、プライバシーマークなど）				
5. 作業従事者の管理				
6. 情報資産の管理				
7. セキュリティを考慮した製品・システム等の開発・運用状況				
8. セキュリティ教育・研修の実施				
9. 情報セキュリティ事故への対応体制				

（回答者：本調査対象者全員）

問 13. 貴社は、委託する際にセキュリティの保護資産を指定していますか。以下のうち、最もあてはまるものをお知らせください。（ひとつだけ）【必須】

1. 包括的に指定している
2. 個別に指定している
3. 指定していない

（回答者：本調査対象者全員）

問 14. 貴社では、委託する際に、どのような情報資産の保護を、委託先に求めていますか。（いくつでも）【必須】

1. 貴社独自の企業機密情報（経営・管理、営業、事業・技術・製品・サービス等に関する情報）
2. 貴社独自の個人情報
3. 顧客から預かっている機密情報（経営・管理、営業、事業・技術・製品・サービス等に関する情報）
4. 顧客から預かっている個人情報
5. 委託する際の業務内容全般に関する情報（仕様書、設計図、指示書、会議録等に関する情報）
6. セキュリティの管理・運用に関する情報（アクセス権限、ID・パスワード、重要情報の保管場所・方法、機器等の設定情報、ログ、鍵管理等に関する情報）
7. その他（具体的に　　）

（回答者：本調査対象者全員）
問 15. 貴社では、委託を行う際に、納品物に対し、以下のセキュリティ脅威に関する確認を行っていますか。あてはまるものをお知らせください。（いくつでも）【必須】
1. 不正動作（マルウェアの混入等）
2. 使用されるソフトウェアの脆弱性（OS、プログラム、ソースコード、オープンソース・ソフトウェア等）
3. 使用されるハードウェアの脆弱性（データ記録・格納媒体、管理・設定機能等）
4. その他（具体的に　　）
5. 特に何も確認していない（排他選択肢）

【用語解説】（引用元：IT 用語辞典 e-Words）
マルウェア…コンピュータの正常な利用を妨げるなど、利用者やコンピュータに害を成す不正な動作を行うソフトウェアの総称。

（回答者：問 15. で選択肢 1 と回答していない方にうかがう。）
問 16. 貴社では、納品物の不正動作（マルウェアの混入等）を確認していない理由について、お知らせください。（いくつでも）【必須】
1. 委託先の納品物に対するセキュリティ対策に実績があるから
2. 納品物の不正動作の確認には、コストや労力の負担を伴うから
3. 納品物の不正動作を確認する方法が分からないから
4. その他　（　　）

（回答者：本調査対象者全員）
問 17. 貴社の IT システムの開発・運用や、貴社が提供する製品、またはサービスの開発・運用等において、クラウドを使用していますか。（ひとつだけ）【必須】
1. 使用している
2. 使用していない

（回答者：問 17. で選択肢 1 と回答した方にうかがう。）
問 18. 貴社では、クラウド選定時にセキュリティ要件を確認していますか。（ひとつだけ）【必須】
1. クラウドサービス事業者との交渉・協議を行い、セキュリティ要件を十分確認している
2. クラウドサービス事業者の公開情報をもとに、セキュリティ要件を確認している
3. セキュリティ要件を十分確認していない

（回答者：本調査対象者全員）
問 19. 貴社は、次のうち、どれにあてはまりますか。（ひとつだけ）【必須】
1. 農業・林業・漁業
2. 建設・土木・鉱業
3. 製造業（石油化学）
4. 製造業（石油化学以外）
5. 電気・ガス・熱供給・水道業・エネルギー業
6. 情報通信業（電気通信・放送・ケーブルテレビ）
7. 情報通信業（電気通信・放送・ケーブルテレビ以外）
8. 運輸業・物流業
9. 卸売業・小売業
10. 金融・保険業
11. 不動産・物品賃貸業
12. 学術研究・専門・技術サービス業
13. 宿泊業・飲食サービス業
14. 生活関連サービス業・娯楽業
15. 教育・学習支援業
16. 医療・福祉
17. 複合サービス業（郵便局、協同組合等）
18. その他サービス業
19. 公務
20. その他

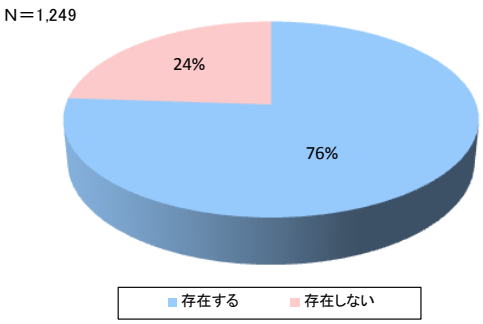
（回答者：本調査対象者全員）
問 20. 貴社の年間売上高は、次のうち、どれにあてはまりますか。（ひとつだけ）【必須】
1. 10 億円未満
2. 10 億円以上 100 億円未満
3. 100 億円以上 1,000 億円未満
4. 1,000 億円以上

参考資料 2　アンケート調査結果

(1)委託元の有無(問 1)

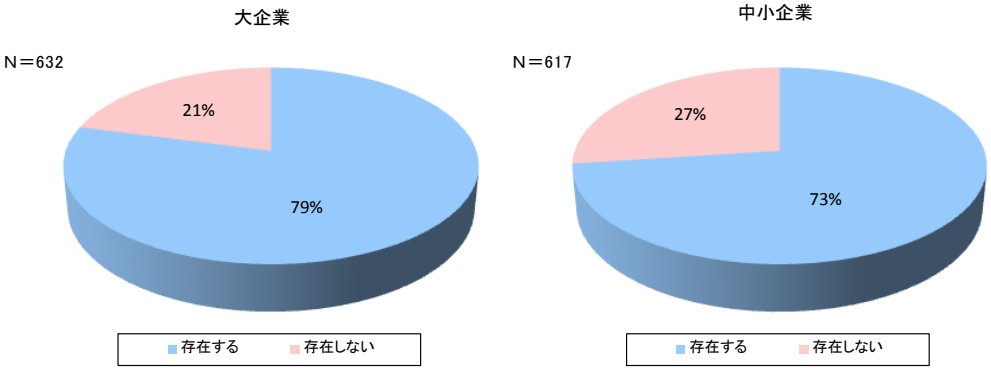
回答企業の約 4 分の 3 は、委託元が存在する。

参考図表 2-1　委託元の有無(問 1)(単回答)



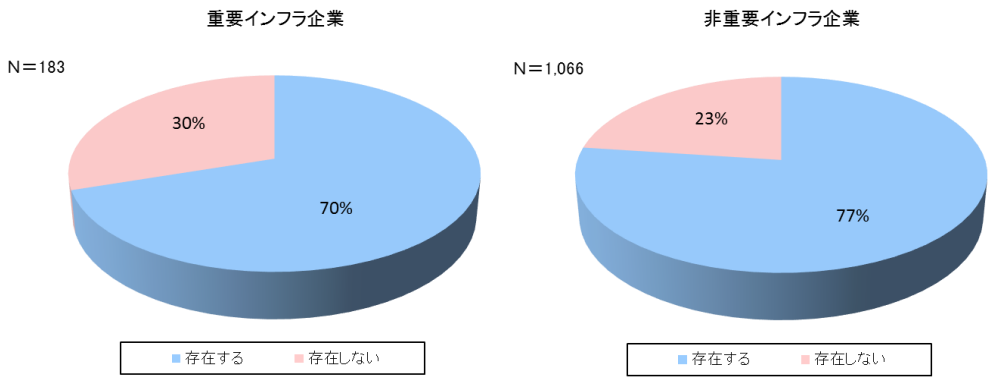
委託元が存在する企業の割合は、大企業が中小企業よりもやや高い。

参考図表 2-2　委託元の有無(大企業と中小企業の比較)(問 1)(単回答)



委託元が存在する企業の割合は、重要インフラ企業が非重要インフラ企業よりもやや低い。

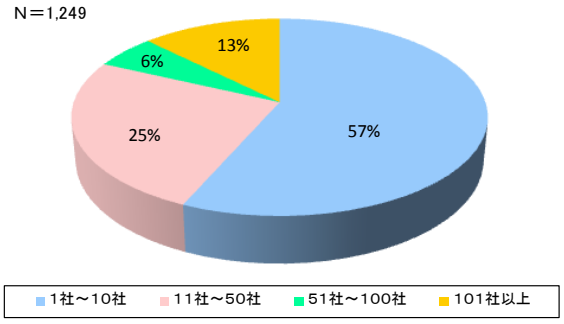
参考図表 2-3　委託元の有無(重要インフラ企業と非重要インフラ企業の比較)(問 1)(単回答)



(2)直接取引のある委託先の数(問 2)

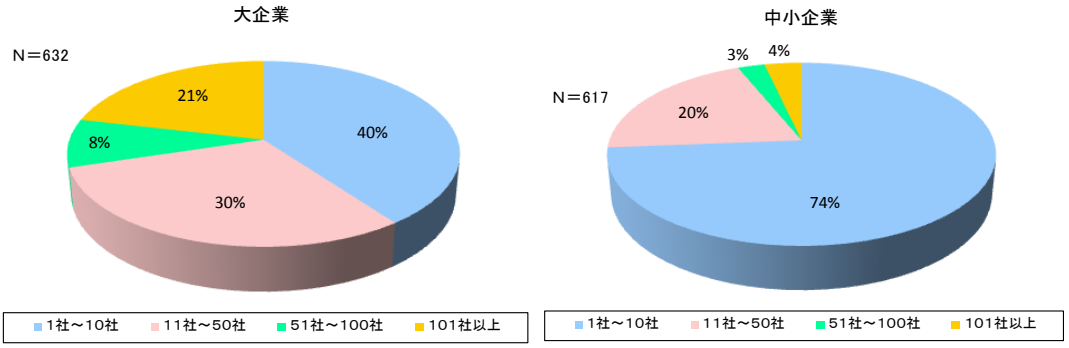
回答企業の約 60%が「直接取引のある委託先を 1～10 社」有しており、回答企業の約 20%が「直接取引のある委託先を 51 社以上」有する。

参考図表 2-4　直接取引のある委託先の数(問 2)(単回答)



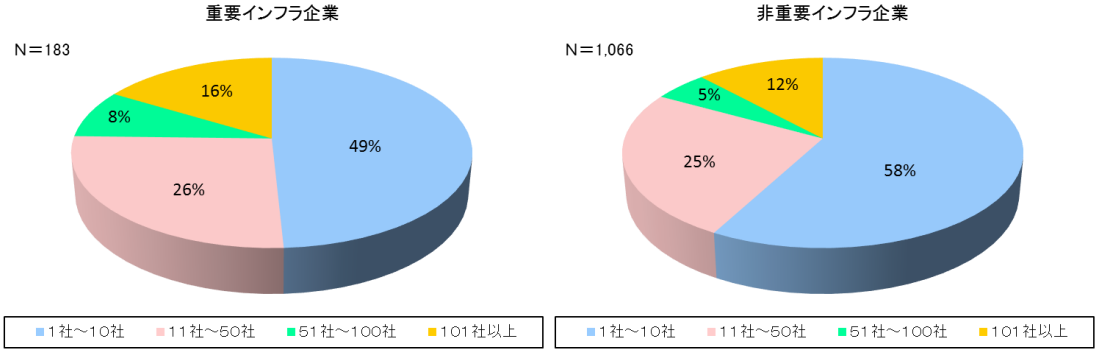
大企業は、「直接取引のある委託先の数が 101 社以上」の企業の割合が約 20%と、中小企業の同項目の約 5 倍である。

参考図表 2-5　直接取引のある委託先の数(大企業と中小企業の比較)(問 2)(単回答)



重要インフラ企業は、直接取引のある委託先の数が、非重要インフラ企業よりも相対的に多い。

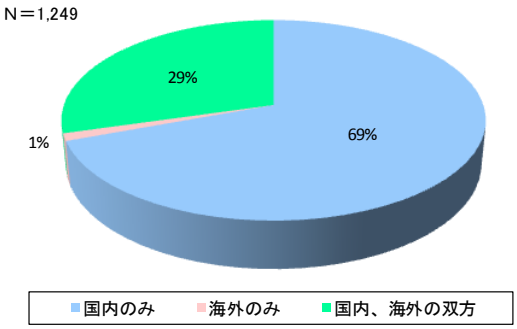
参考図表 2-6　直接取引のある委託先の数（重要インフラ企業と非重要インフラ企業の比較）（問 2）（単回答）



(3)委託先の所在地（問 3）

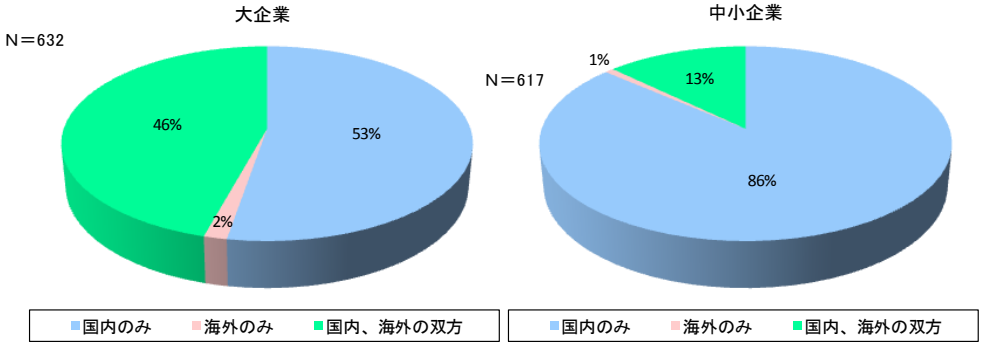
海外の委託先が存在する企業の割合は約 30%である。

参考図表 2-7　委託先の所在地（問 3）（単回答）



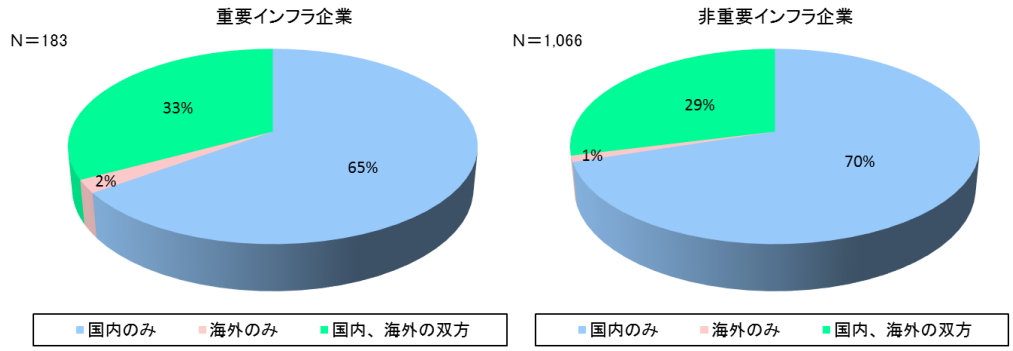
「海外の委託先が存在する」企業の割合は、大企業において約 48%であるのに対し、中小企業は約 14%にとどまる。

参考図表 2-8　委託先の所在地（大企業と中小企業の比較）（問 3）（単回答）



「海外の委託先が存在する企業」の割合は、重要インフラ企業と非重要インフラ企業において有意な差はほとんどない。

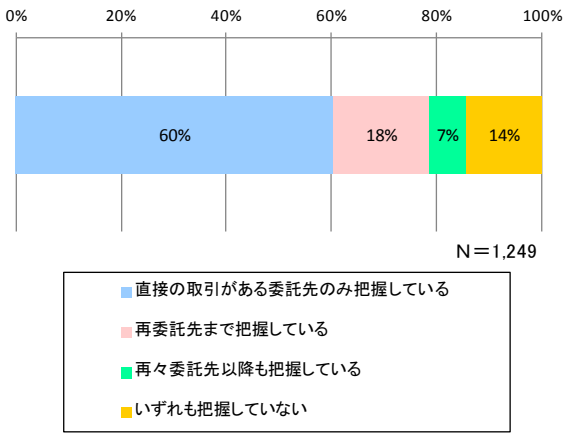
参考図表 2-9　委託先の所在地（重要インフラ企業と非重要インフラ企業の比較）（問 3）（単回答）



(4)委託先等における情報セキュリティ対策の把握状況（問 4）

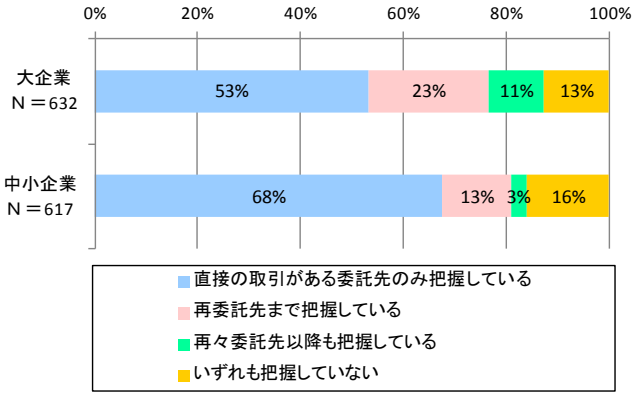
情報セキュリティ対策状況を把握している範囲については、約 60%の企業が、直接の取引がある委託先のみである。また、委託先、再委託先以降のいずれも把握していない企業が約 14%存在する。

参考図表 2-10　委託先等における情報セキュリティ対策の把握状況（問 4）（単回答）



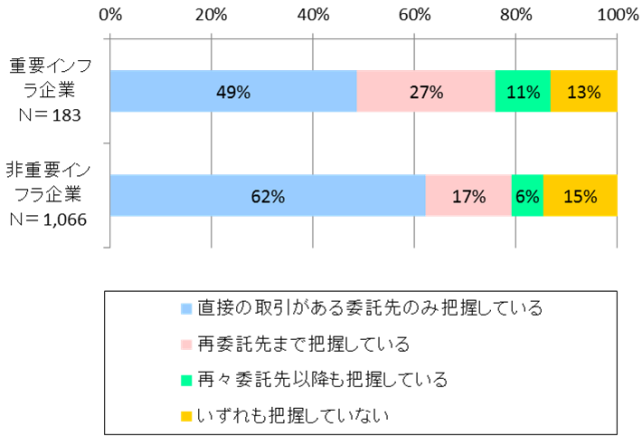
大企業は、取引先の範囲が広いが、約 87%が「委託先の情報セキュリティ対策状況を把握」している。一方、「再委託先までの情報セキュリティ対策状況を把握している」企業の割合は約 23%にとどまる。また、「委託先、再委託先以降のいずれも把握していない」企業が約 13%存在する。

参考図表 2-11　委託先等における情報セキュリティ対策の把握状況（大企業と中小企業の比較）（問 4）（単回答）


0%
20%
40%
60%
80%
100%
大企業
N＝632
53%
23%
11%
13%
中小企業
N＝617
68%
13%
3%
16%
直接の取引がある委託先のみ把握している
再委託先まで把握している
再々委託先以降も把握している
いずれも把握していない

重要インフラ企業では、約 87%が「委託先の情報セキュリティ対策状況を把握」している。一方、「再委託先までの情報セキュリティ対策状況を把握」している企業の割合は約 27%にとどまる。また、「委託先、再委託先以降のいずれも把握」していない企業が約 13%存在する。

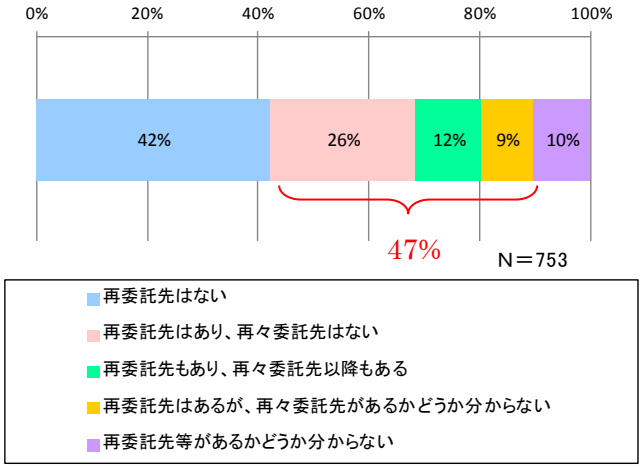
参考図表 2-12　委託先等における情報セキュリティ対策の把握状況
（重要インフラ企業と非重要インフラ企業の比較）（問 4）（単回答）



(5)再委託先、再々委託先等の有無（問 5）

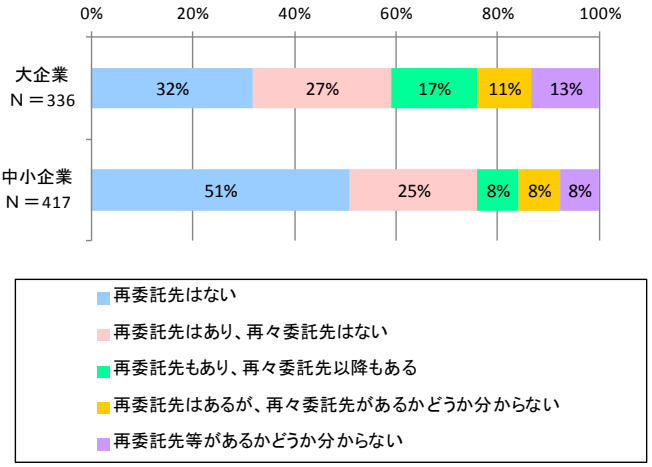
情報セキュリティ対策状況を把握している範囲について、委託先のみと回答している企業のうち、約 47%は「再委託先の情報セキュリティ対策状況を把握していない」。

参考図表 2-13　再委託先、再々委託先等の有無（問 5）（単回答）



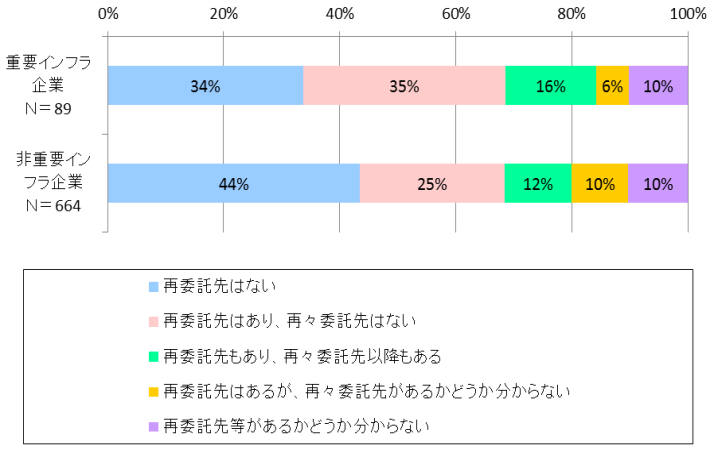
情報セキュリティ対策状況を把握している範囲について、委託先のみと回答している大企業のうち、約 55%は「再委託先の情報セキュリティ対策状況を把握していない」。

参考図表 2-14 再委託先、再々委託先等の有無（大企業と中小企業の比較）（問 5）（単回答）



情報セキュリティ対策状況を把握している範囲について、委託先のみと回答している重要インフラ企業のうち、約 57%は「再委託先の情報セキュリティ対策状況を把握していない」。

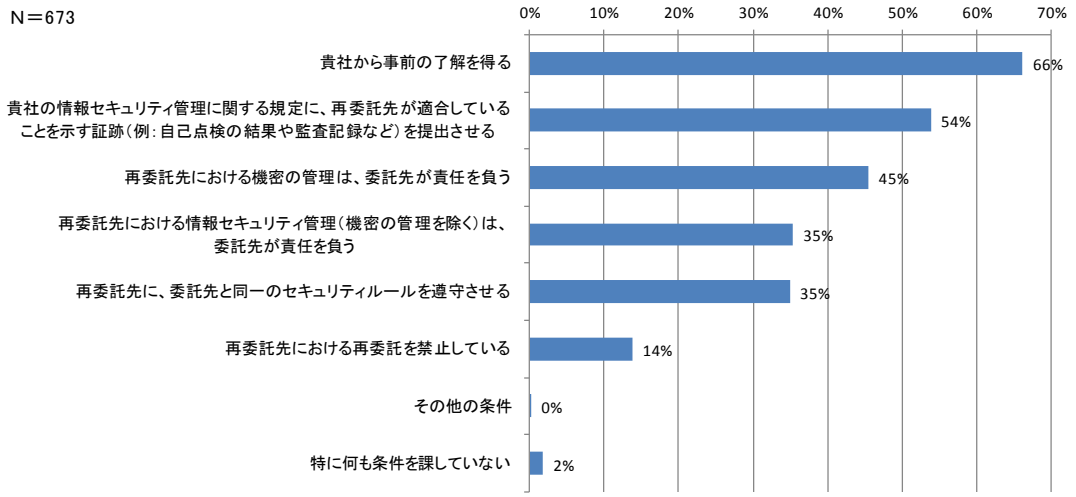
参考図表 2-15 再委託先、再々委託先等の有無（重要インフラ企業と非重要インフラ企業の比較）（問 5）（単回答）



(6)再委託の許可を与える場合に委託先に課している情報セキュリティ条件（問 6）

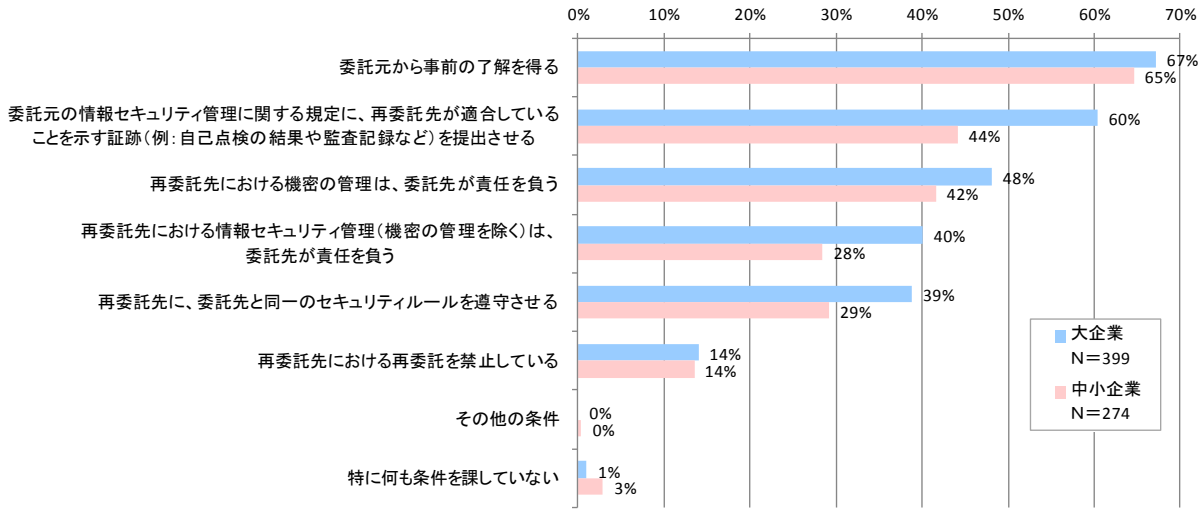
「再委託を行っている企業のうち、再委託先に、委託先と同一のセキュリティルールを遵守させている」企業は約 35%にとどまる。再委託を行っている企業の事前の了解を得たり、再委託を行っている企業の情報セキュリティ管理に関する規定に再委託先が適合していることを示す証跡を提出させることで対応しているケースが多い。

参考図表 2-16　再委託の許可を与える場合に委託先に課している情報セキュリティ条件（問 6）（複数回答）



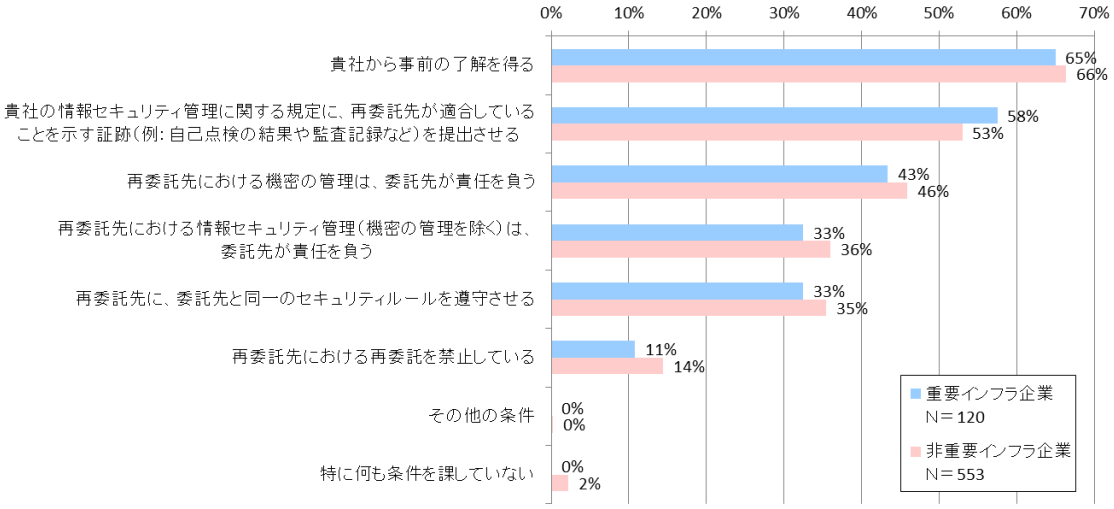
大企業は、再委託の許可を与える場合に、証跡の提出や委託先に対する責任明確化、特に再委託先に対するセキュリティルールの遵守徹底といったセキュリティ条件を委託先に課す傾向にある。

参考図表 2-17　再委託の許可を与える場合に委託先に課している情報セキュリティ条件
（大企業と中小企業の比較）（問 6）（複数回答）



重要インフラ企業と非重要インフラ企業では、再委託の許可を与える場合の、委託先に対する条件に有意な差がほとんど見られない。

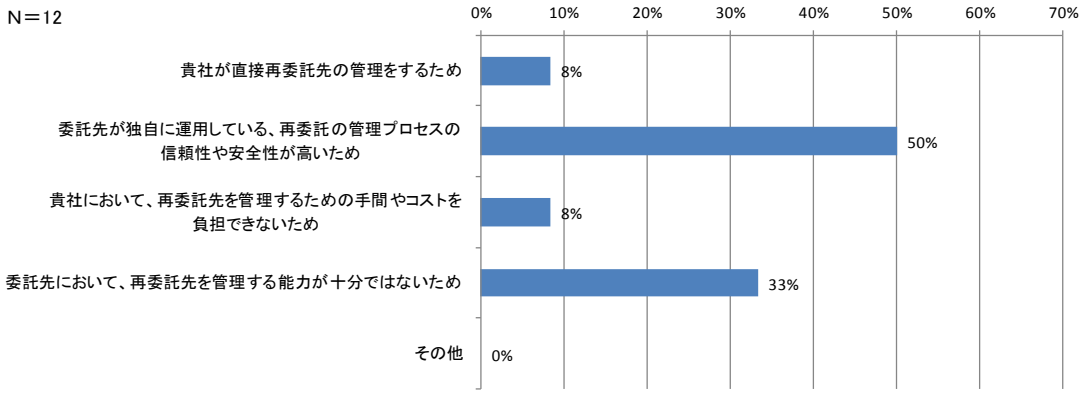
参考図表 2-18 再委託の許可を与える場合に委託先に課している情報セキュリティ条件（重要インフラ企業と非重要インフラ企業の比較）（問 6）（複数回答）



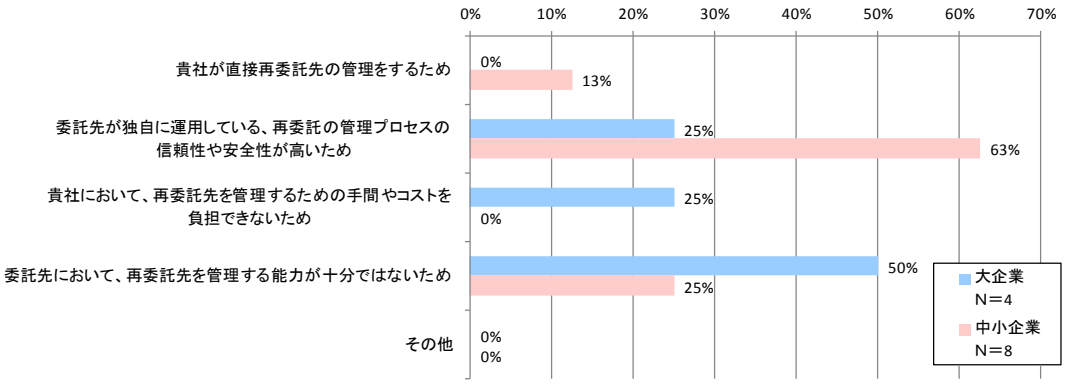
(7)再委託の許可を与える場合に情報セキュリティ条件を課していない理由（問 7）

委託先に対し再委託の許可を与える場合に、「特に何も条件を課していない」企業の割合は低いが、特に何も条件を課していない理由として「委託先が独自に運用している、再委託の管理プロセスの信頼性・安全性が高い」ことを挙げる企業が多い。

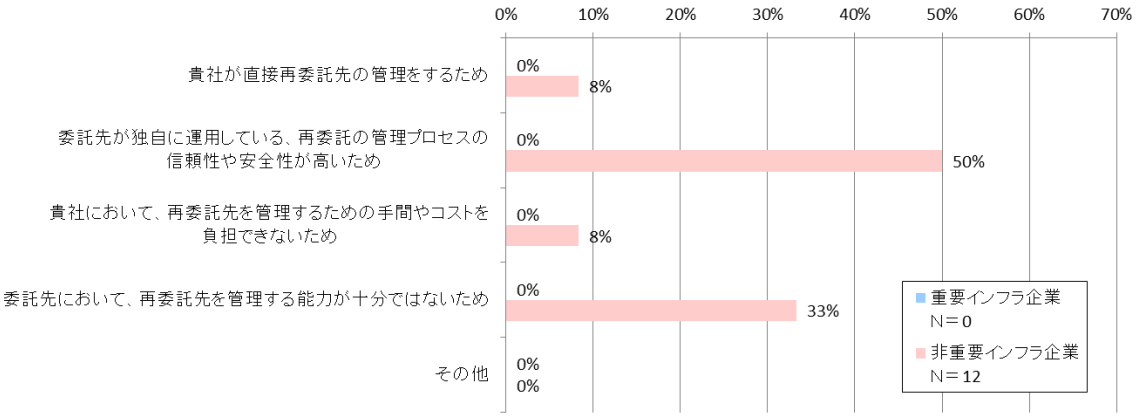
参考図表 2-19 再委託の許可を与える場合に情報セキュリティ条件を課していない理由（問 7）（複数回答）



参考図表 2-20　再委託の許可を与える場合に情報セキュリティ条件を課していない理由
（大企業と中小企業の比較）（問 7）（複数回答）



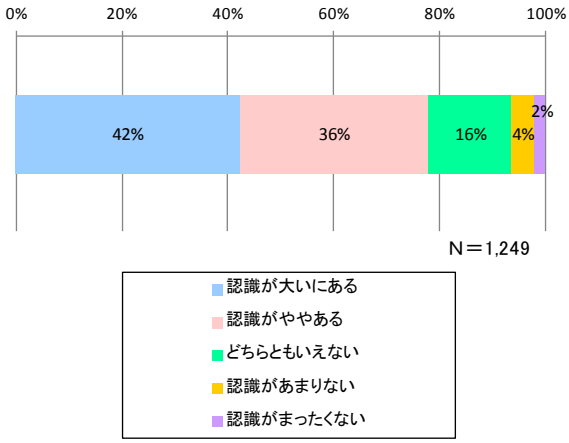
参考図表 2-21　再委託の許可を与える場合に情報セキュリティ条件を課していない理由
（重要インフラ企業と非重要インフラ企業の比較）（問 7）（複数回答）



(8) 委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する経営層の認識（問 8）

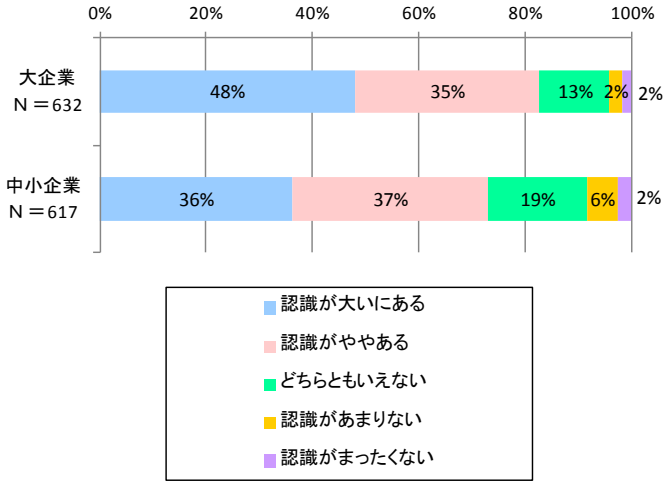
「認識が大いにある」、「認識がややある」を含めると、約 78%の企業の経営層が、情報セキュリティに関する SCRM の重要性に対する認識を持っている。

参考図表 2-22　委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する経営層の認識（問 8）（単回答）



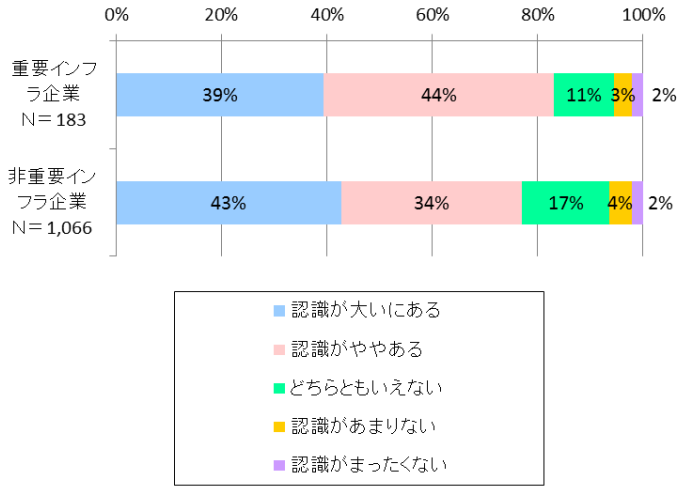
大企業においては、「認識が大いにある」、「認識がややある」を含めると、約 83%の企業の経営層が、情報セキュリティに関する SCRM の重要性に対する認識を持っており、中小企業の経営層よりも 10 ポイント高い。

参考図表 2-23　委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する経営層の認識（大企業と中小企業の比較）（問 8）（単回答）



重要インフラ企業においては、「認識が大いにある」、「認識がややある」を含めると、約 83%の企業の経営層が、情報セキュリティに関する SCRM の重要性に対する認識を持っており、非重要インフラ企業の経営層よりも 6 ポイント高い。

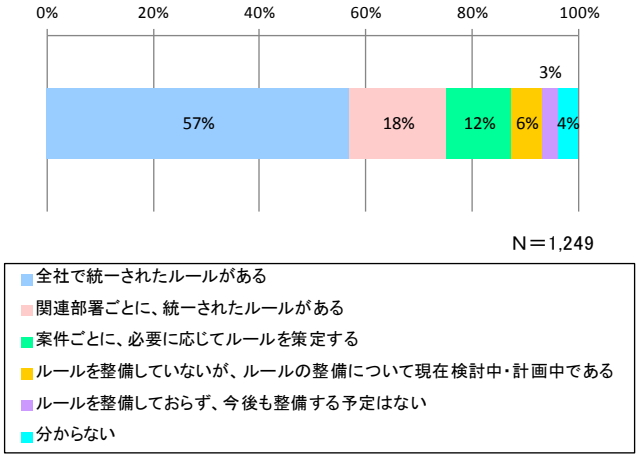
参考図表 2-24　委託先または再委託先等に対する情報セキュリティ管理の強化・徹底の重要性に対する経営層の認識（重要インフラ企業と非重要インフラ企業の比較）（問 8）（単回答）



(9) 委託を行う際に委託先が遵守すべき情報セキュリティ管理を定めたルールの策定状況（問 9）

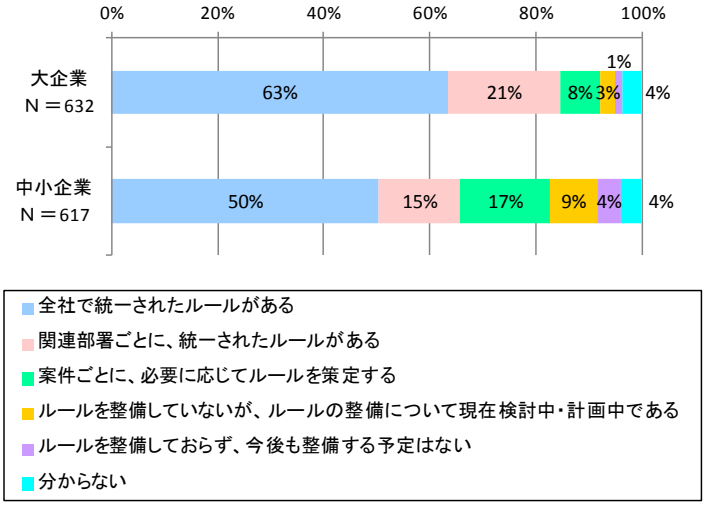
委託先が遵守すべき情報セキュリティ管理を定めたルールについて、「全社で統一されたルールを整備」している企業は約 57%である。他方、「同ルールを整備していない」企業も約 9%存在する。

参考図表 2-25　委託を行う際に委託先が遵守すべき情報セキュリティ管理を定めたルールの策定状況（問 9）（単回答）



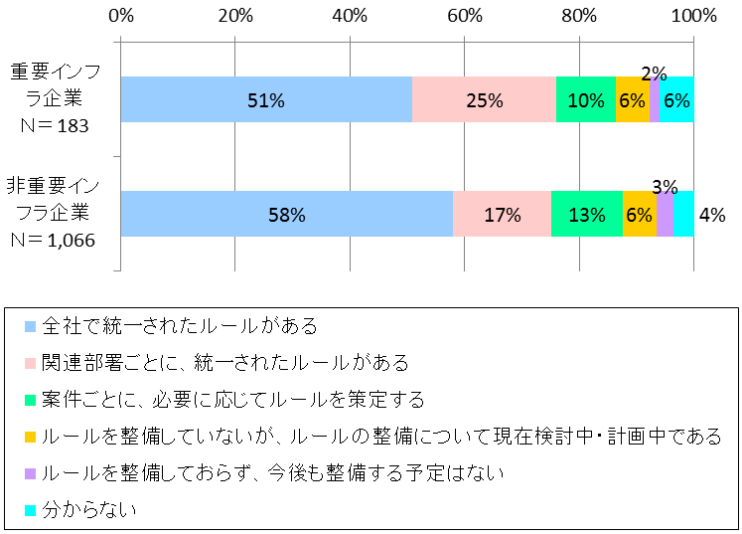
委託先が遵守すべき情報セキュリティ管理を定めたルールについて、「全社で統一されたルールを整備している」企業は、大企業が約 63%であるのに対し、中小企業は約 50%であり、双方に 13 ポイントの開きがある。

参考図表 2-26　委託を行う際に委託先が遵守すべき情報セキュリティ管理を定めたルールの策定状況（大企業と中小企業の比較）（問 9）（単回答）



委託先が遵守すべき情報セキュリティ管理を定めたルールについて、「全社で統一されたルールを整備している」企業の割合は、重要インフラ企業で約 51%と全体の傾向と比べると相対的に低い。一方、関連部署ごとに「統一されたルールを整備している」企業の割合は約 25%と全体の傾向と比べると相対的に高い。

参考図表 2-27　委託を行う際に委託先が遵守すべき情報セキュリティ管理を定めたルールの策定状況（重要インフラ企業と非重要インフラ企業の比較）（問 9）（単回答）

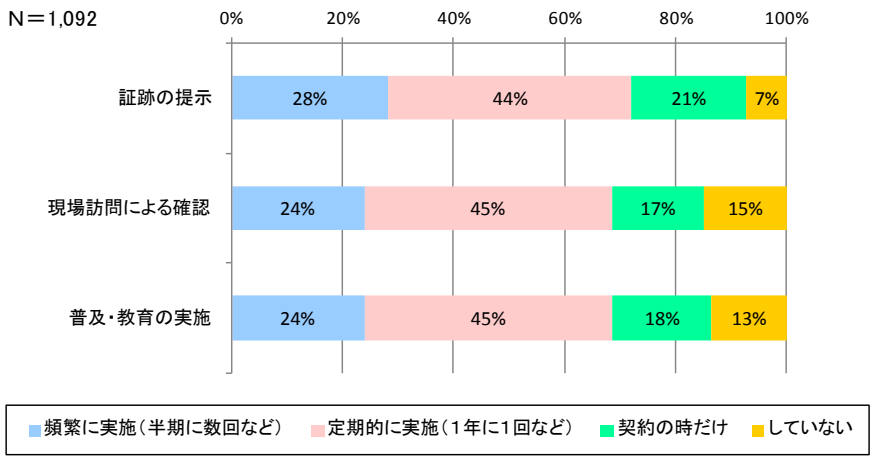


（10）委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（問 10）

委託先における情報セキュリティ管理を定めたルールの徹底状況については、「証跡の提

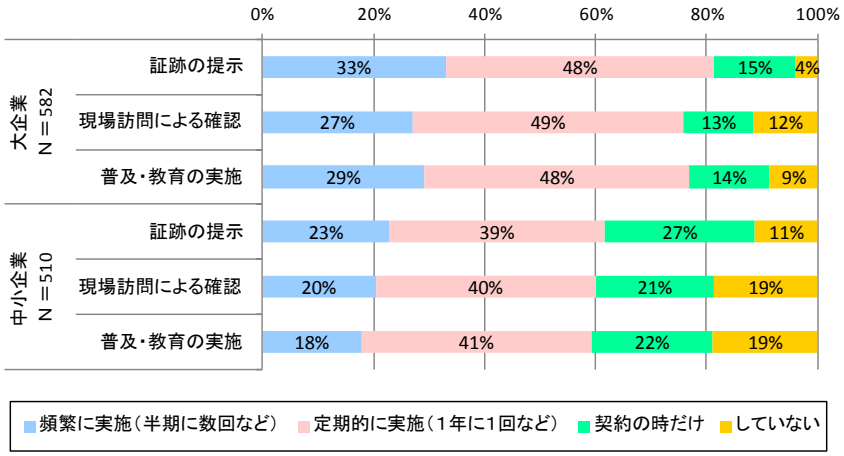
示」、「現場訪問による確認」、「普及・教育の実施」のいずれも、頻繁あるいは定期的に実施している企業の割合は、約 70%前後である。

参考図表 2-28　委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（問 10）（単回答）



委託先における情報セキュリティ管理を定めたルールの徹底状況については、「証跡の提示」、「現場訪問による確認」、「普及・教育の実施」のいずれも、頻繁あるいは定期的に実施している大企業の割合は、約 80%前後であり、中小企業の割合の約 60%前後と比較するとある程度徹底されている。

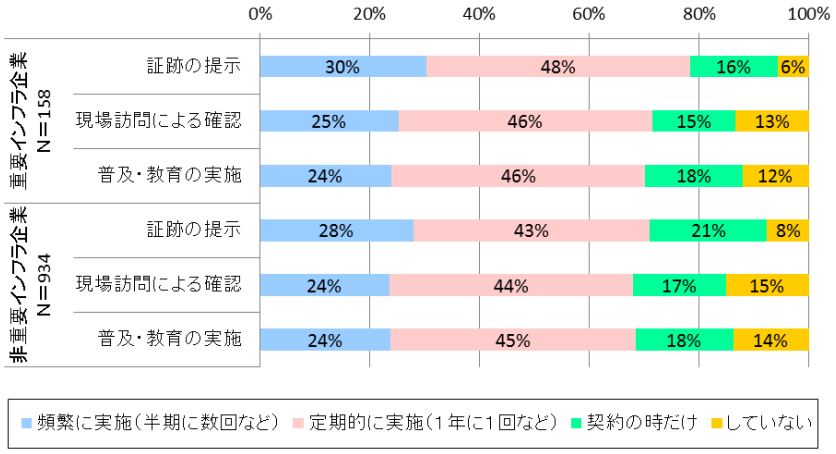
参考図表 2-29　委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（大企業と中小企業の比較）（問 10）（単回答）



委託先における情報セキュリティ管理を定めたルールのうち、「証跡の提示」について頻繁あるいは定期的に実施している重要インフラ企業の割合は、約 78%であり、非重要イン

フラ企業の同項目の約 71%前後と比較するとある程度徹底されている。

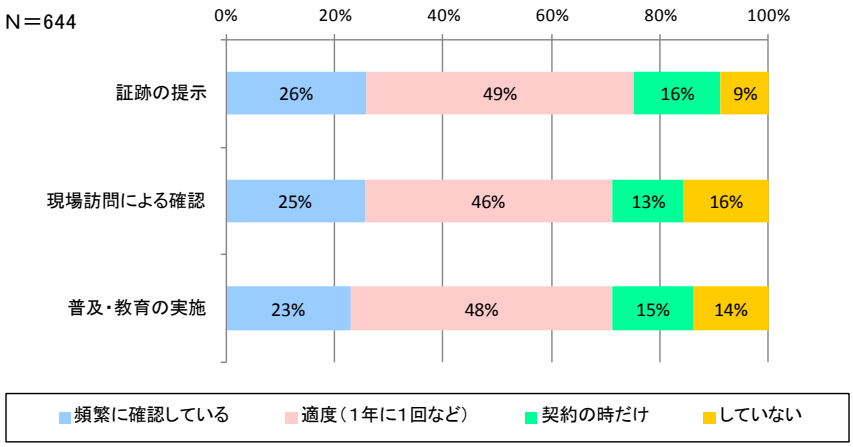
参考図表 2-30　委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（重要インフラ企業と非重要インフラ企業の比較）（問 10）（単回答）



（11）再委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（問 11）

再委託先における情報セキュリティ管理を定めたルールの徹底状況については、「証跡の提示」を頻繁あるいは定期的に実施している企業の割合が約 75%、「現場訪問による確認」や、「普及・教育の実施」を頻繁あるいは定期的に実施している企業の割合が約 71%であり、再委託先までルール遵守が意識されている。

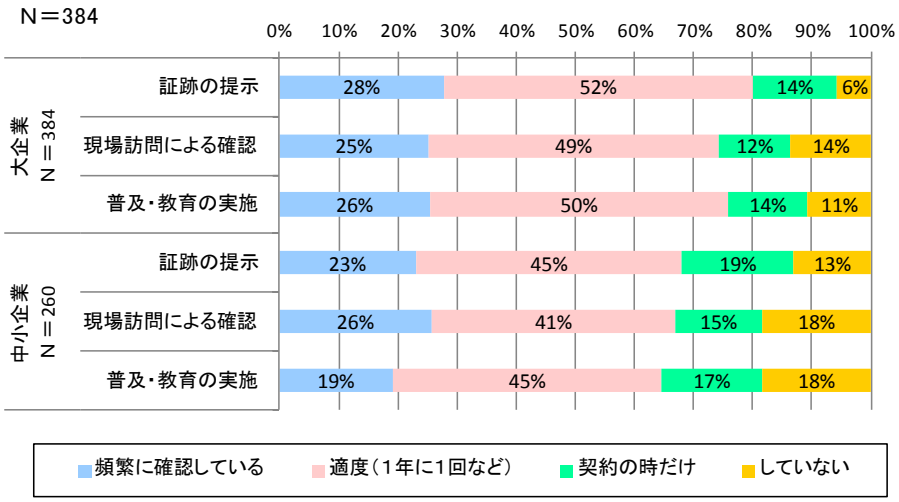
参考図表 2-31　再委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（問 11）（単回答）



再委託先における情報セキュリティ管理を定めたルールの徹底状況については、「証跡の提示」を頻繁あるいは定期的に実施している大企業の割合が約 80%、「現場訪問による確

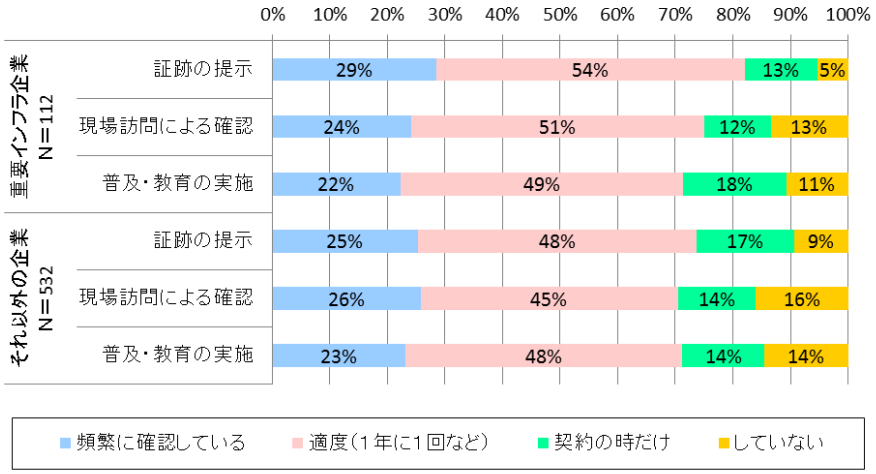
認」や、「普及・教育の実施」を頻繁あるいは定期的に実施している大企業の割合が約75%前後であり、中小企業の同項目と比べて再委託先までルール遵守が意識されている。

参考図表 2-32 再委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（大企業と中小企業の比較）（問 11）（単回答）



再委託先における情報セキュリティ管理を定めたルールの徹底状況については、「証跡の提示」を頻繁あるいは定期的に実施している重要インフラ企業の割合が約 83%、「現場訪問による確認」を頻繁あるいは定期的に実施している重要インフラ企業の割合が約 75%であり、非重要インフラ企業の同項目と比べて再委託先までルール遵守が意識されている。

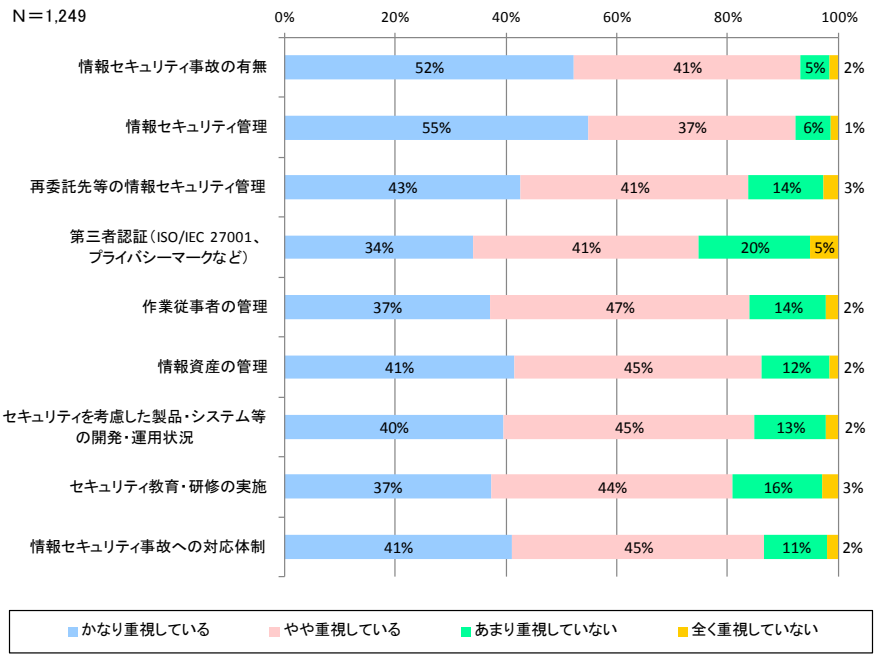
参考図表 2-33 再委託先における、委託先が遵守すべき情報セキュリティ管理を定めたルールの徹底状況（重要インフラ企業と非重要インフラ企業の比較）（問 11）（単回答）



(12)委託先を選定する際に重視している情報セキュリティ管理の観点(問 12)

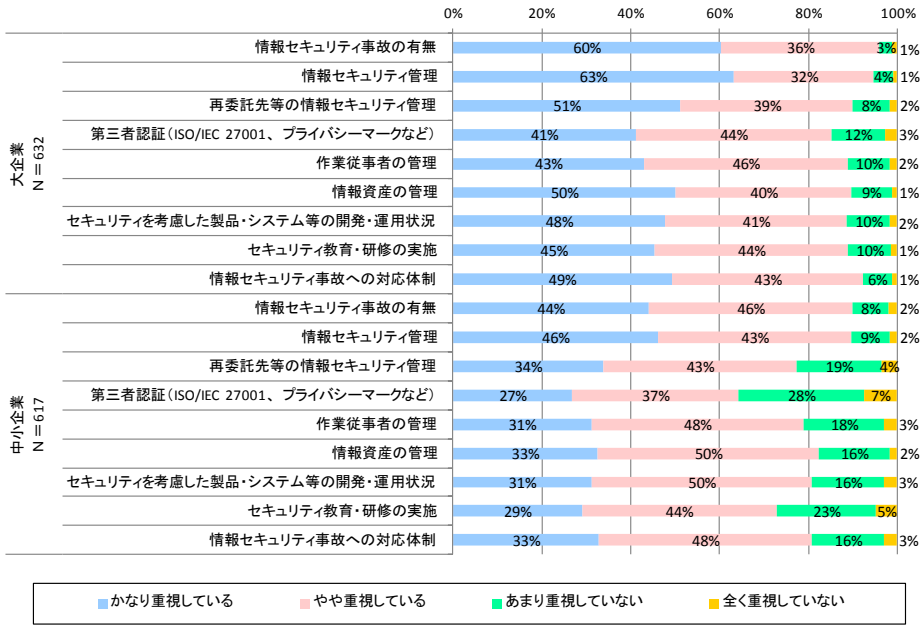
「かなり重視している」、「やや重視している」を含めると、委託先を選定する際に約 93%の企業が「情報セキュリティ事故の有無」、また約 92%の企業が「情報セキュリティ管理」を重視している。

参考図表 2-34 委託先を選定する際に重視している情報セキュリティ管理の観点(問 12)(単回答)



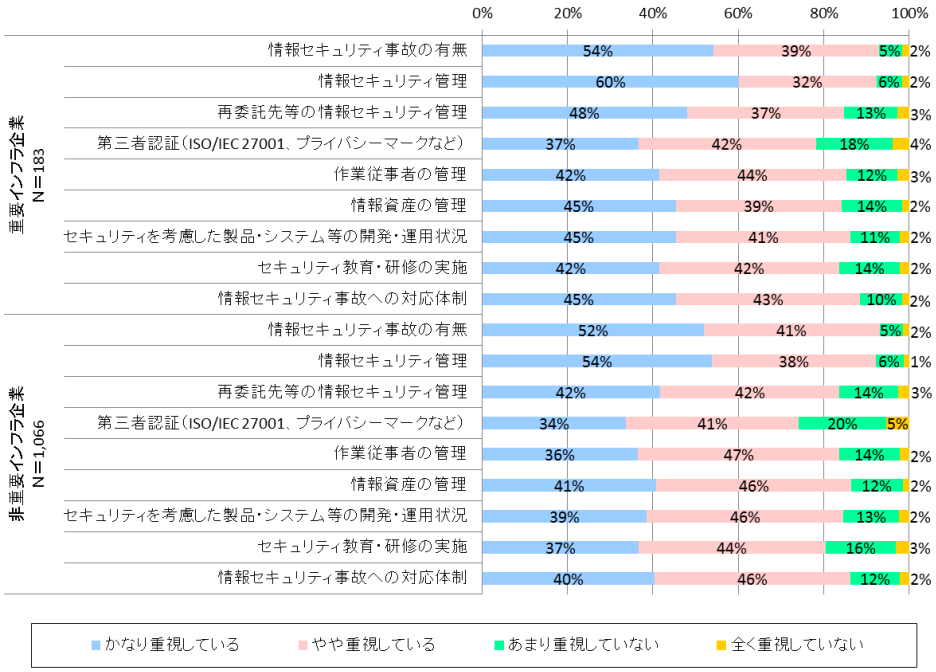
「かなり重視している」、「やや重視している」を含めると、委託先を選定する際に、中小企業では、大企業と比較して、「第三者認証」や「セキュリティ教育・研修」の実施はあまり重視されていない傾向にある。

参考図表 2-35　委託先を選定する際に重視している情報セキュリティ管理の観点（大企業と中小企業の比較）（問 12）（単回答）



「かなり重視している」、「やや重視している」を含めると、委託先を選定する際に、非重要インフラ企業では、重要インフラ企業と比較して、「第三者認証」があまり重視されていない傾向にある。

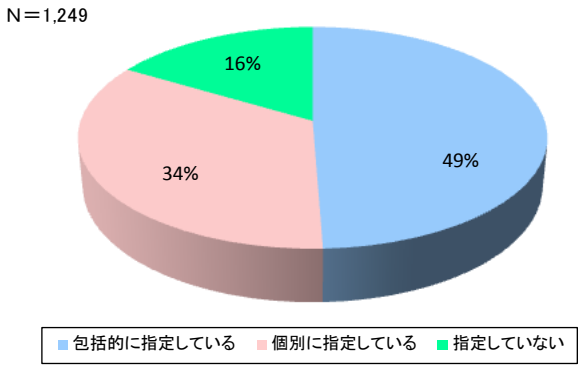
参考図表 2-36　委託先を選定する際に重視している情報セキュリティ管理の観点（重要インフラ企業と非重要インフラ企業の比較）（問 12）（単回答）



(13)委託を行うに際してのセキュリティの保護資産の指定の有無・内容(問 13)

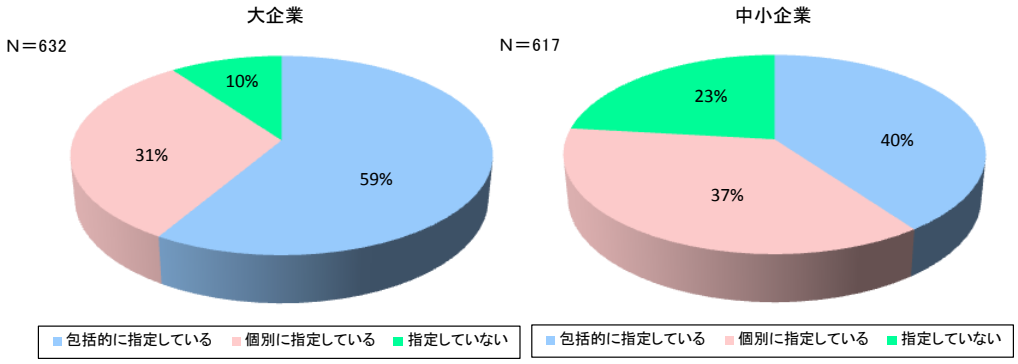
委託を行う際に、企業の約 83%がセキュリティ保護資産を指定している。指定方法としては、「包括的に指定している」場合が「個別に指定している」場合よりも多い。

参考図表 2-37 委託を行うに際してのセキュリティの保護資産の指定の有無・内容(問 13)(単回答)



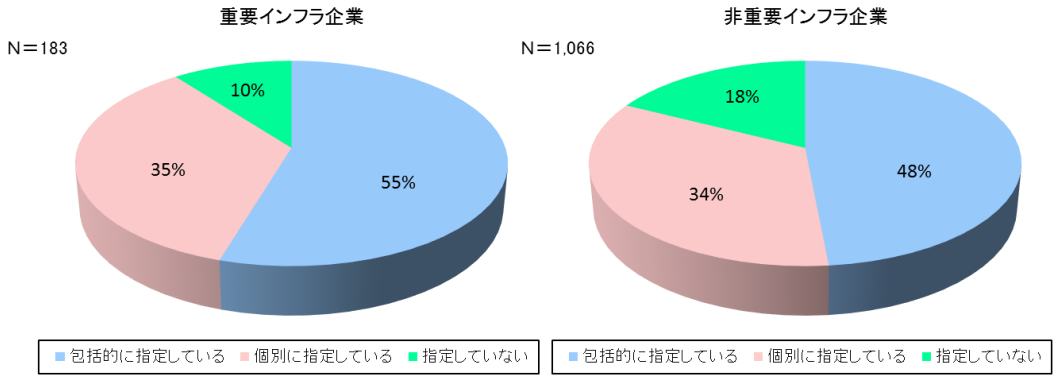
大企業においては、委託を行う際に約 90%が「セキュリティ保護資産を指定」しており、中小企業の同項目と比較すると 13 ポイント高い。また、大企業では、「保護資産を個別に指定する」よりも「包括的に指定する」傾向にある。

参考図表 2-38 委託を行うに際してのセキュリティの保護資産の指定の有無・内容
(大企業と中小企業の比較)(問 13)(単回答)



重要インフラ企業においては、委託を行う際に、約 90%が「セキュリティ保護資産を指定」しており、非重要インフラ企業の同項目と比較すると 8 ポイント高い。また、重要インフラ企業では、「保護資産を個別に指定する」よりも「包括的に指定する」傾向にある。

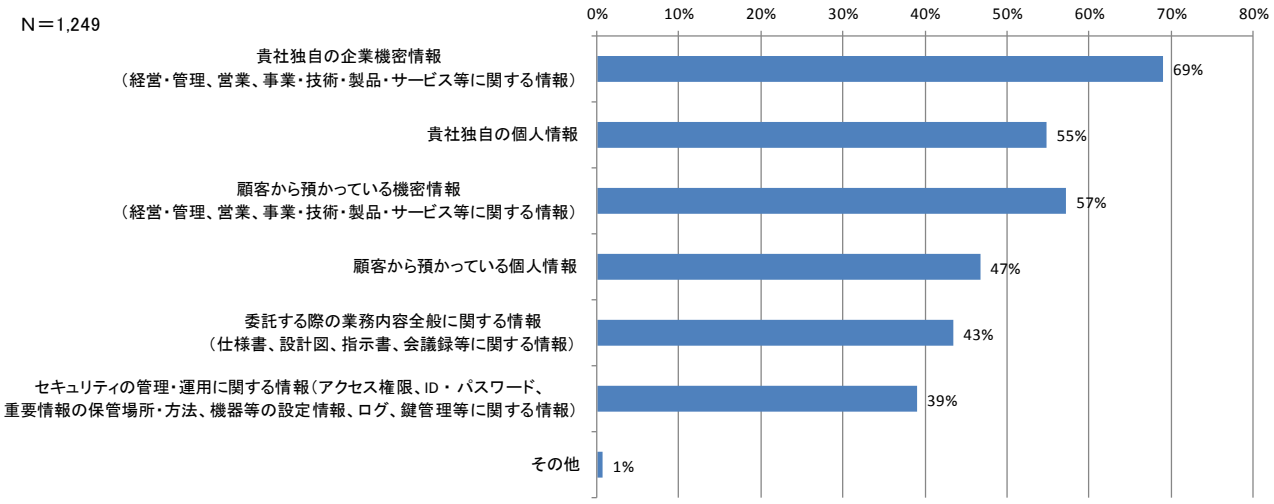
参考図表 2-39　委託を行うに際してのセキュリティの保護資産の指定の有無・内容
（重要インフラ企業と非重要インフラ企業の比較）（問 13）（単回答）



（14）委託先に求める情報資産の保護内容（問 14）

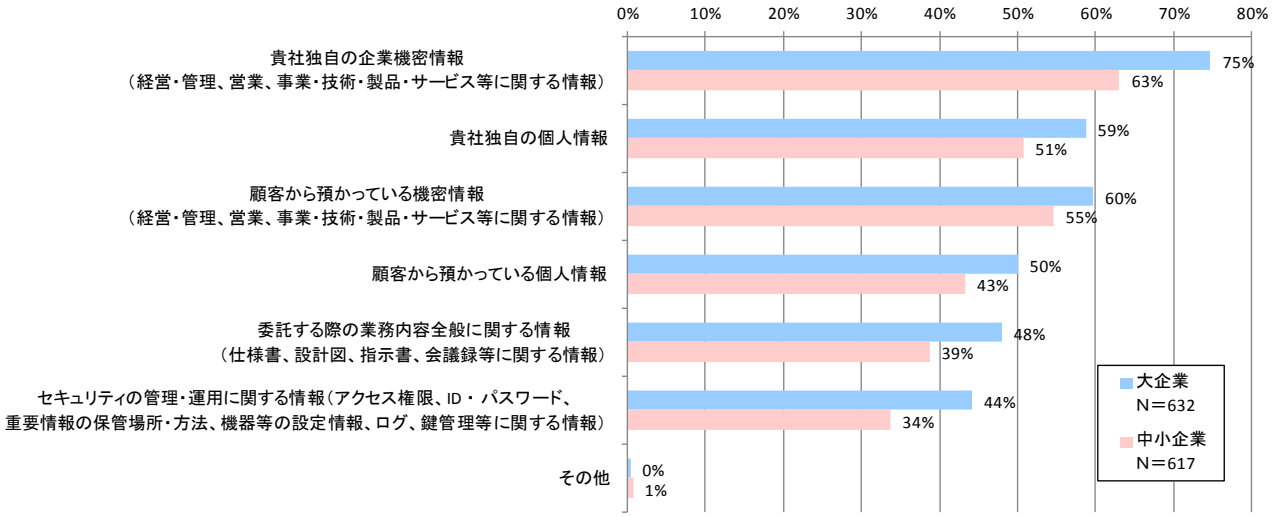
委託先に保護を求める情報資産の種類については、「自社独自の企業機密情報」が最も多く、次いで「顧客から預かっている機密情報」、「自社独自の個人情報」が回答者の半数が選定している。最も低かったのが「セキュリティの管理・運用に関する情報」で 39%であった。

参考図表 2-40　委託先に求める情報資産の保護内容（問 14）（複数回答）



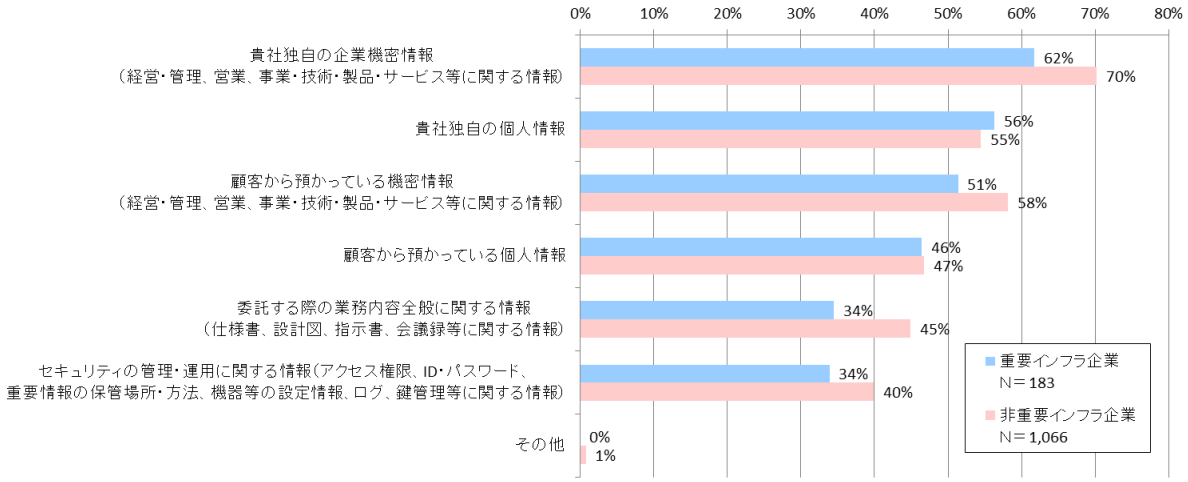
大企業が委託先に保護を求める情報資産の種類については、「自社独自の企業機密情報」が最も多く、次いで「顧客から預かっている機密情報」、「自社独自の個人情報」の順であるが、保護内容はかなり広範に及んでおり、それぞれの保護内容の要求度合いは中小企業と比較して高くなっている。

参考図表 2-41　委託先に求める情報資産の保護内容（大企業と中小企業の比較）（問 14）（複数回答）



重要インフラ企業が委託先に保護を求める情報資産の種類については、「自社独自の企業機密情報」が最も多く、次いで「自社独自の個人情報」、「顧客から預かっている機密情報」の順であるが、このうち、「自社独自の企業機密情報」や「顧客から預かっている機密情報」については、非重要インフラ企業の要求度合いの方が高くなっている。

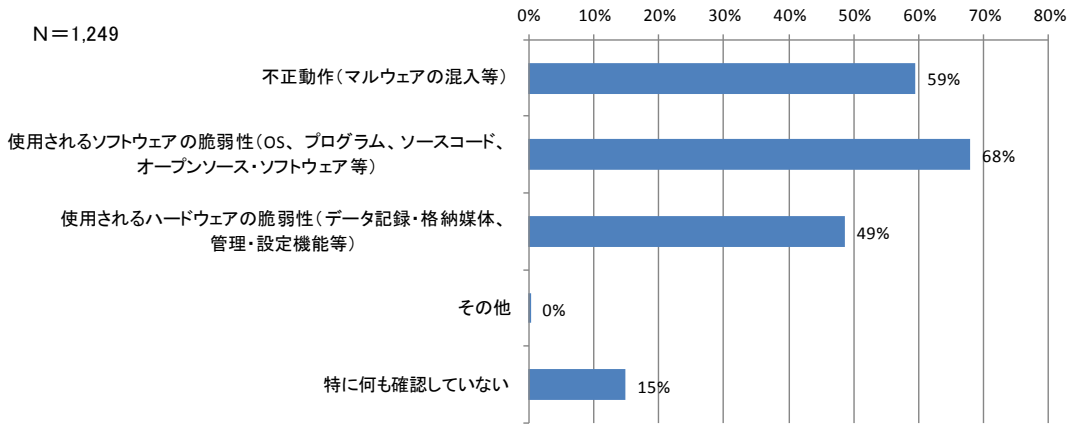
参考図表 2-42　委託先に求める情報資産の保護内容（重要インフラ企業と非重要インフラ企業の比較）（問 14）（複数回答）



（15）委託を行う際の納品物に対するセキュリティ脅威の確認状況（問 15）

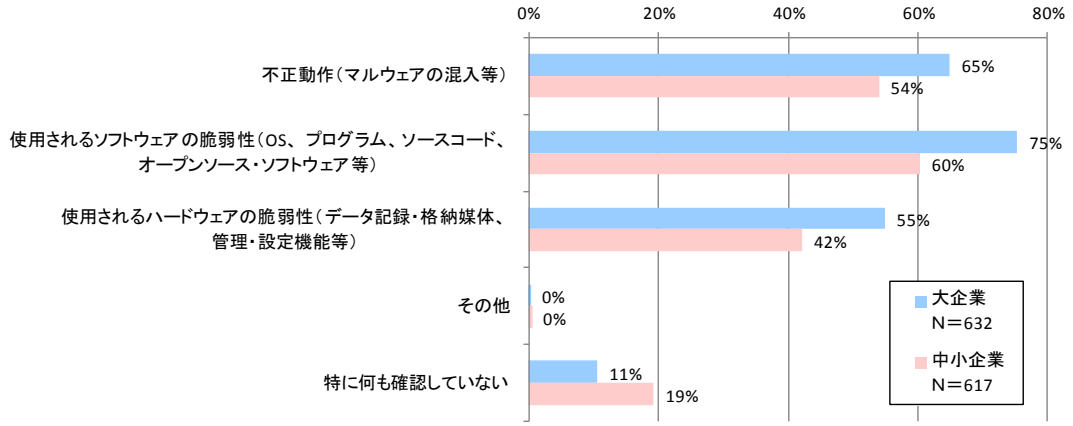
納品物の「不正動作（マルウェアの混入等）」について確認を行っている企業は約 59%で、「使用されるソフトウェアの脆弱性」について確認を行っている企業は約 68%である。納品物に対するセキュリティ脅威について「特に何も確認していない」企業が約 15%も存在する。

参考図表 2-43　委託を行う際の納品物に対するセキュリティ脅威の確認状況（問 15）（複数回答）



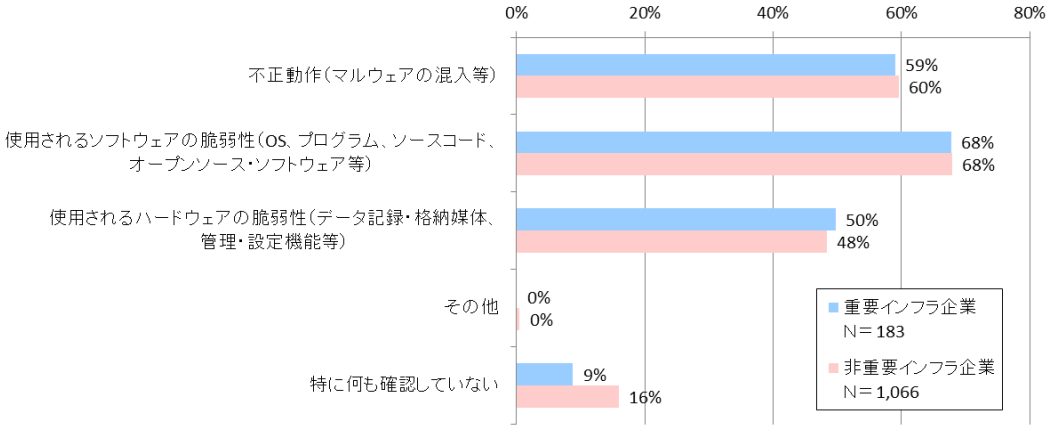
納品物に対するセキュリティ脅威について「特に何も確認していない企業」の割合が、大企業では約 11%であるのに対し、中小企業では約 19%と約 8 ポイントの差がある。

参考図表 2-44　委託を行う際の納品物に対するセキュリティ脅威の確認状況（大企業と中小企業の比較）（問 15）（複数回答）



納品物に対するセキュリティ脅威について「特に何も確認していない」企業の割合が、重要インフラ企業では約 9%であるのに対し、非重要インフラ企業では約 16%と 7 ポイントの差がある。

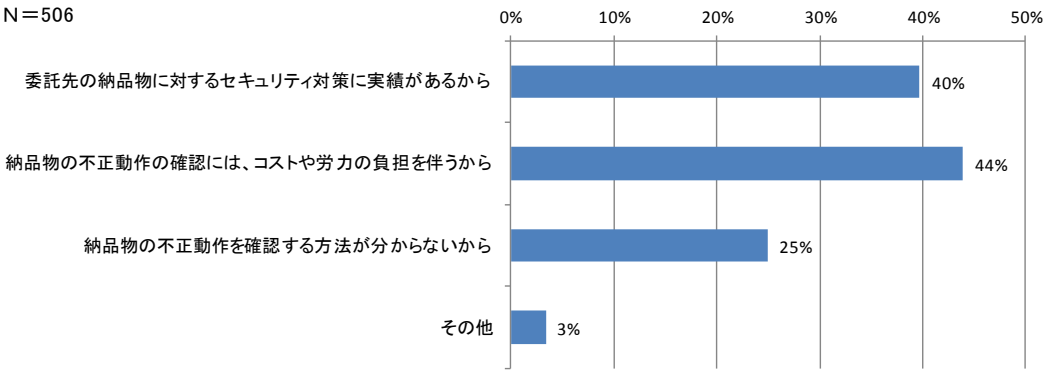
参考図表 2-45　委託を行う際の納品物に対するセキュリティ脅威の確認状況
（重要インフラ企業と非重要インフラ企業の比較）（問 15）（複数回答）



（16）納品物の不正動作（マルウェアの混入等）を確認していない理由（問 16）

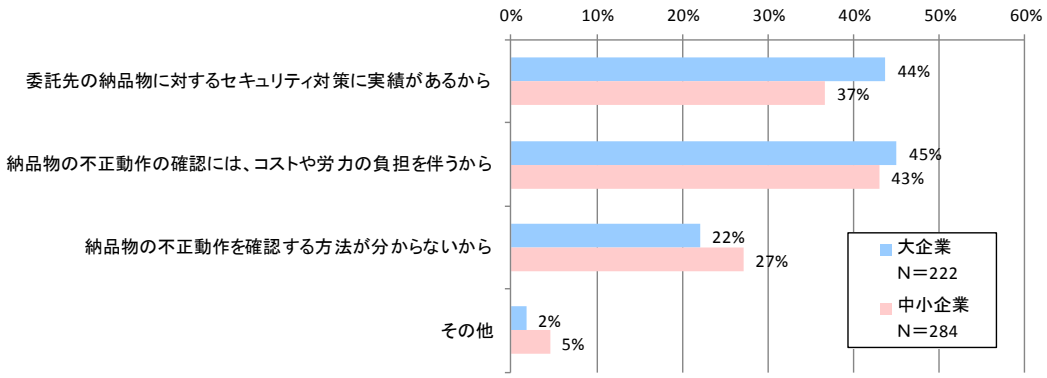
納品物の不正動作を確認していない理由については、「コストや労力の負担」が最も高く約 44%、「委託先の納品物に対するセキュリティ対策の実績がある」を選択した企業は約 40%。また「確認方法が分からない」企業も約 25%存在する。

参考図表 2-46　納品物の不正動作（マルウェアの混入等）を確認していない理由（問 16）（複数回答）



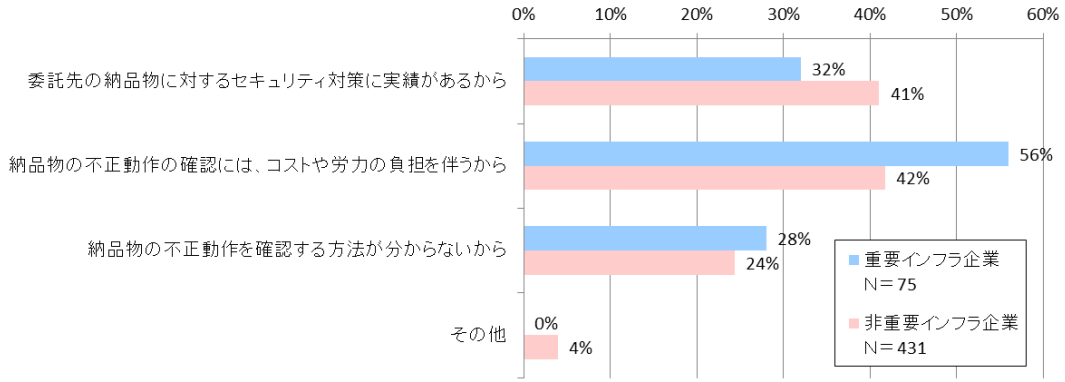
納品物の不正動作を確認していない理由について、「委託先の納品物に対するセキュリティ対策の実績があるから」を選定している企業は、大企業が約 44%であるのに対し、中小企業は約 37%であり、大企業の方が中小企業よりやや委託先への信頼にゆだねている傾向にある。

参考図表 2-47　納品物の不正動作（マルウェアの混入等）を確認していない理由（大企業と中小企業の比較）（問16）（複数回答）



重要インフラ企業では、納品物の不正動作を確認していない理由について、「コストや労力の負担」を挙げている企業が約 56%で、非重要インフラ企業の約 42%より 14 ポイントも差がある。

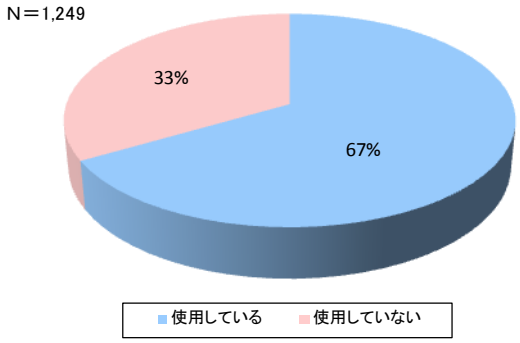
参考図表 2-48　納品物の不正動作（マルウェアの混入等）を確認していない理由
（重要インフラ企業と非重要インフラ企業の比較）（問 16）（複数回答）



（17）IT システムの開発・運用や提供する製品またはサービスの開発・運用等におけるクラウドの活用状況（問 17）

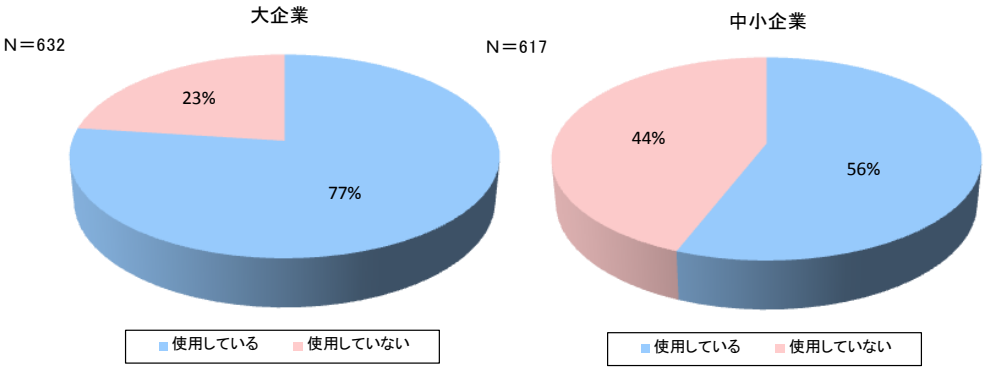
企業の約 67%（3 社に 2 社）が、IT システムの開発・運用や提供する製品またはサービスの開発・運用等において、「クラウドを使用している」。

参考図表 2-49　IT システムの開発・運用や提供する製品またはサービスの開発・運用等における
クラウドの活用状況（問 17）（単回答）



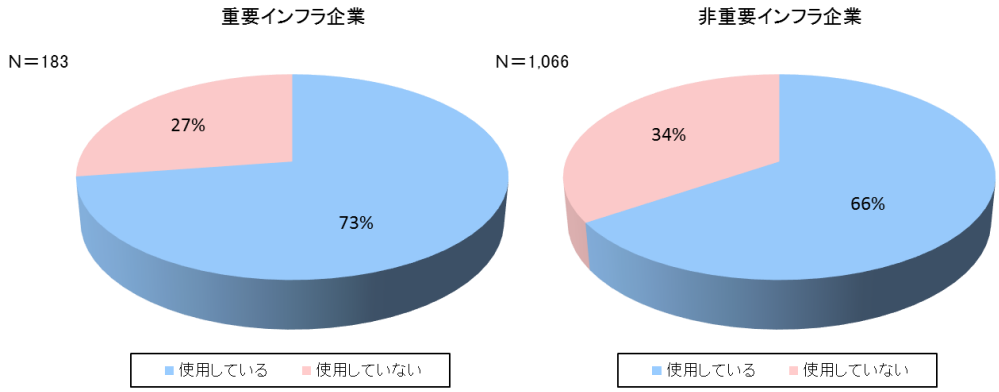
IT システムの開発・運用や提供する製品またはサービスの開発・運用等において、「クラウドを使用している」企業は、大企業で約 77%、中小企業で 56%と、大企業は中小企業よりも、「クラウドを使用している」傾向にある。

参考図表 2-50　IT システムの開発・運用や提供する製品またはサービスの開発・運用等における
クラウドの活用状況（大企業と中小企業の比較）（問 17）（単回答）



IT システムの開発・運用や提供する製品またはサービスの開発・運用等において、「クラウドを使用している」企業は、重要インフラ企業で約 73%、非重要インフラ企業で約 66%と重要インフラ企業は非重要インフラ企業よりもやや「クラウドを使用している」傾向にある。

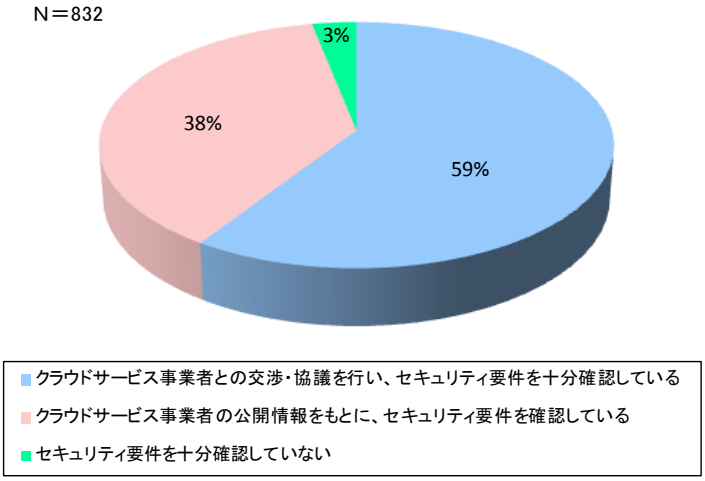
参考図表 2-51　IT システムの開発・運用や提供する製品またはサービスの開発・運用等における
クラウドの活用状況（重要インフラ企業と非重要インフラ企業の比較）（問 17）（単回答）



（18）クラウド選定時におけるセキュリティ要件の確認の有無・方法（問 18）

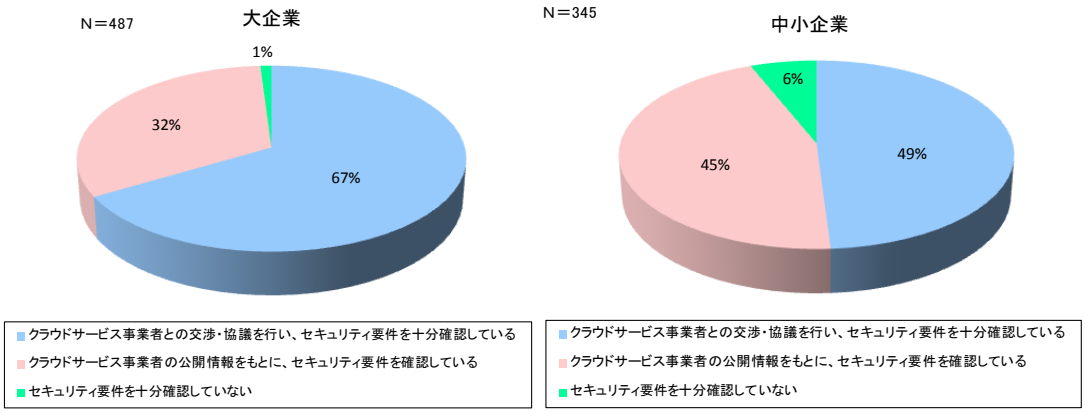
クラウド選定時に、「クラウドサービス事業者との交渉・協議を行い、セキュリティ要件を十分確認している」企業は約 59%、「公開情報をもとにセキュリティ要件を確認している」企業は約 38%、「セキュリティ要件を十分に確認していない」企業は約 3%存在する。

参考図表 2-52　クラウド選定時におけるセキュリティ要件の確認の有無・方法（問 18）（単回答）



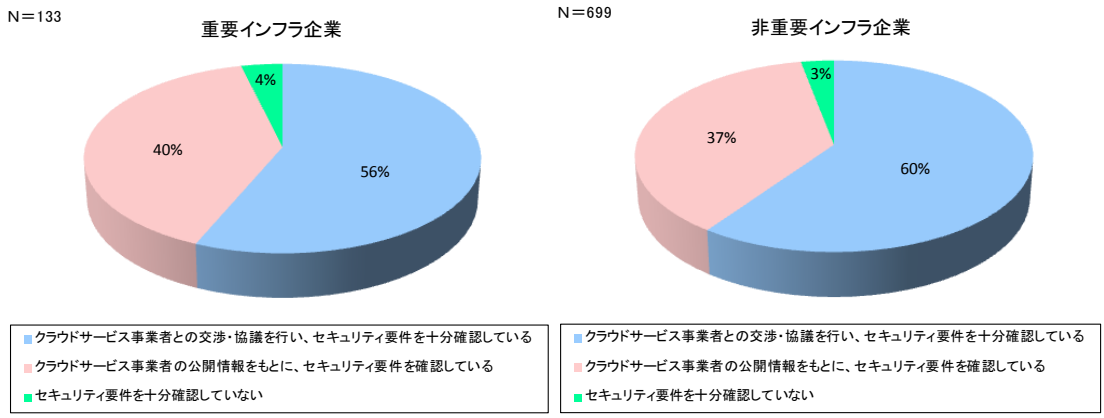
クラウド選定時に「クラウドサービス事業者との交渉・協議を行い、セキュリティ要件を十分確認している」企業は、大企業が約 67%、中小企業が約 49%であり、双方に 18 ポイントの大きな開きがある。

参考図表 2-53 クラウド選定時におけるセキュリティ要件の確認の有無・方法（大企業と中小企業の比較）（問 18）（単回答）



クラウド選定時に、「クラウドサービス事業者との交渉・協議を行い、セキュリティ要件を十分確認している」企業は、重要インフラ企業が約 56%、非重要インフラ企業が約 60%であり、双方に有意な差はほとんど見られない。

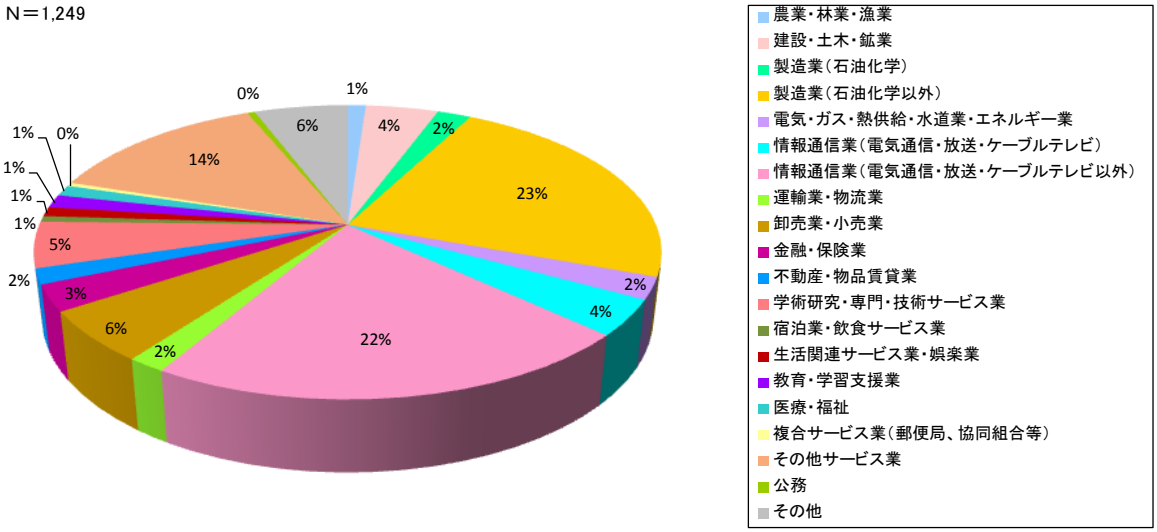
参考図表 2-54 クラウド選定時におけるセキュリティ要件の確認の有無・方法（重要インフラ企業と非重要インフラ企業の比較）（問 18）（単回答）



(19) 業種（問 19）

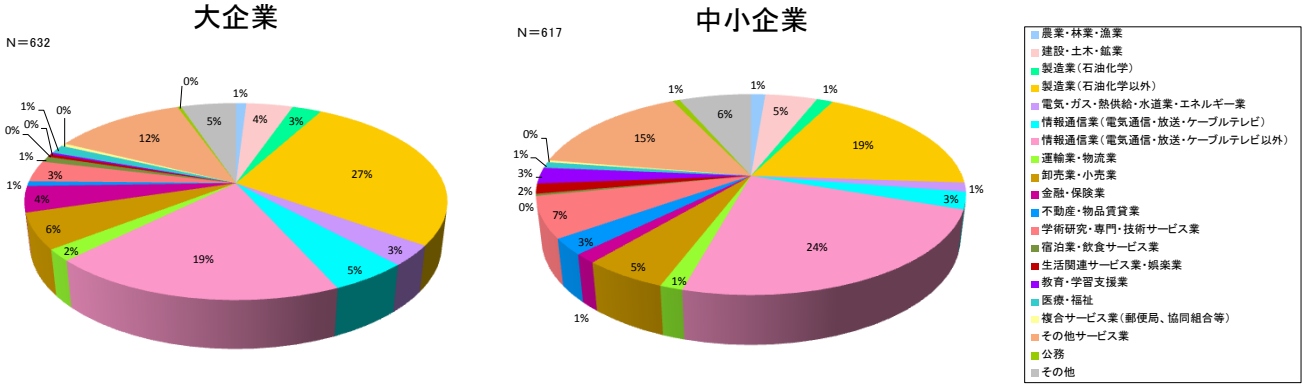
アンケート回答企業の業種をみると、「製造業（石油化学以外）」が約 23%、「情報通信業（電気通信・放送・ケーブルテレビ以外）」が約 22%、「その他サービス業」が 14%と割合が高い。

参考図表 2-55　業種（問 19）（単回答）



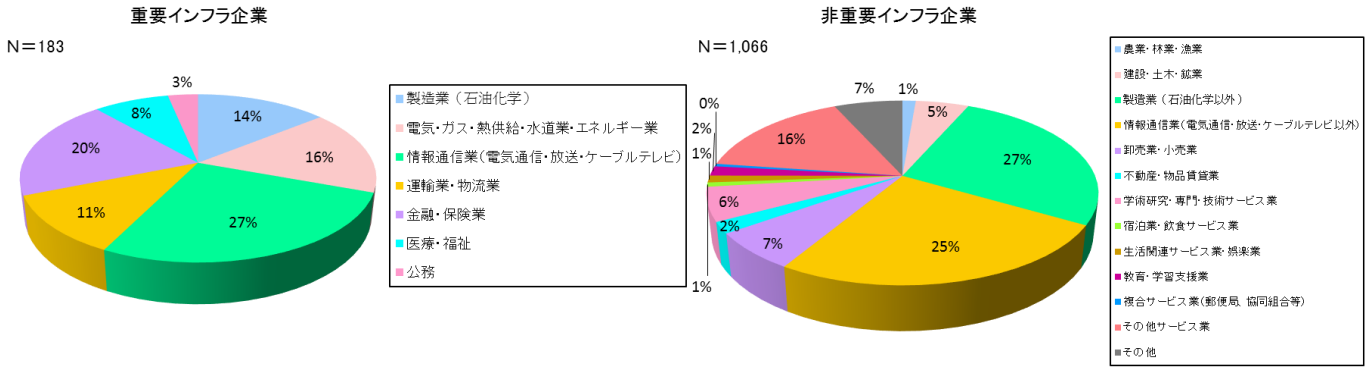
大企業では「製造業（石油化学以外）」の割合が最も高く約 27%で、中小企業では「情報通信業（電気通信・放送・ケーブルテレビ以外）」の割合が最も高く約 24%を占める。

参考図表 2-56　業種（大企業と中小企業の比較）（問 19）（単回答）



重要インフラ企業の中では「情報通信業（電気通信・放送・ケーブルテレビ）」の割合が最も高く約 27%、次に「金融・保険業」、「電気・ガス・熱供給・水道業・エネルギー業」が約 16%を占める。非重要インフラ企業においては、「製造業（石油・化学以外）」の割合が高く約 27%、次に「情報通信業（電気通信・放送・ケーブルテレビ）」が約 25%、「その他サービス業」が約 16%を占める。

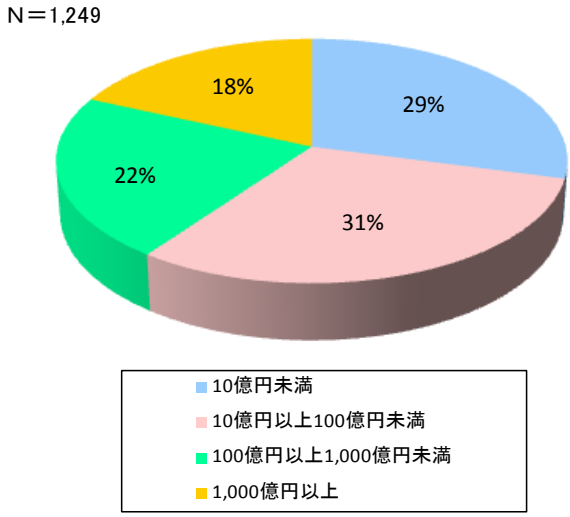
参考図表 2-57　業種（重要インフラ企業と非重要インフラ企業の比較）（問 19）（単回答）



（20）年間売上高（問 20）

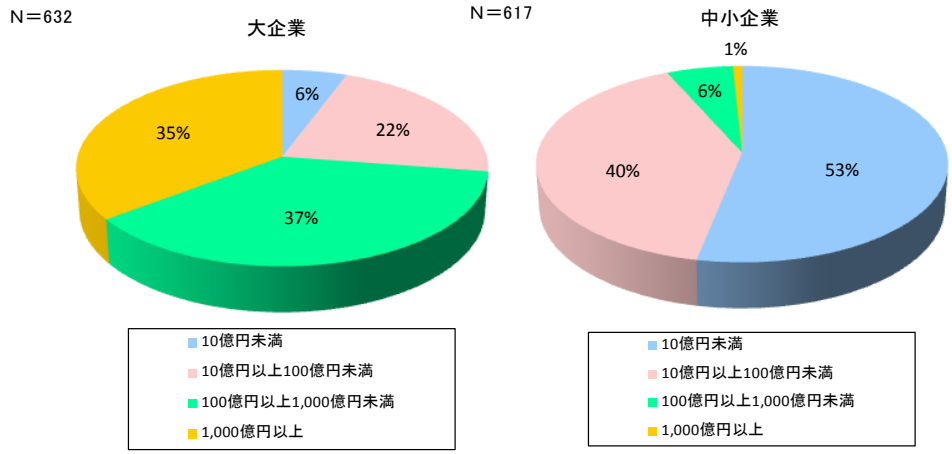
年間売上高をみると、「10 億円以上 100 億円未満」が最も多く約 31%、「10 億円未満」が約 29%、「100 億円以上 1,000 億円未満」が約 22%、「1,000 億円以上」が約 18%である。

参考図表 2-43　年間売上高（問 20）（単回答）



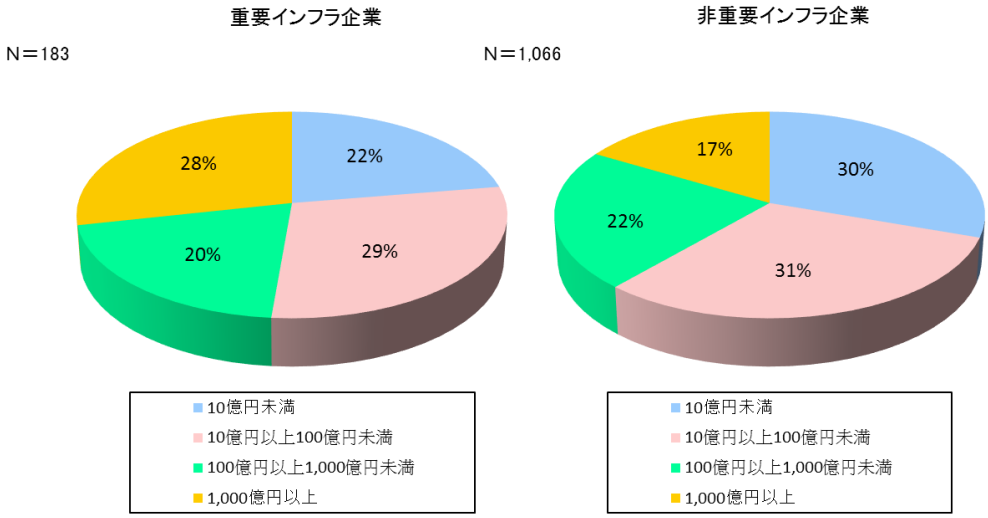
大企業の年間売上高をみると、「100 億円以上 1,000 億円未満」が最も多く約 37%、「1,000 億円以上」が約 35%である。中小企業の年間売上高をみると、「10 億円未満」が約 53%、「10 億円以上 100 億円未満」が約 40%と 100 億円未満の企業が全体の約 93%を占める。

参考図表 2-44　年間売上高（大企業と中小企業の比較）（問 20）（単回答）



重要インフラ企業、非重要インフラ企業の年間売上高をみると、双方ともに「10 億円以上 100 億円未満」の割合が高い。

参考図表 2-45　年間売上高（重要インフラ企業と非重要インフラ企業の比較）（問 20）（単回答）



参考資料 3 ヒアリング項目

日米のヒアリング調査では、IT システム設計・開発・運用に関わるサプライチェーン、若しくは対象企業が提供する製品またはサービスの設計・開発・運用に関わるサプライチェーンを有し、且つ情報セキュリティに関する SCRM へ積極的に取り組む民間企業（IT ベンダー、自動車メーカー、製薬メーカーが含まれる）五社と、米国国立標準技術研究所（以下、NIST）を対象とした。

民間企業に対するヒアリング項目を以下に示す。なお、優先的に聴取した項目を下線で示す。

1. 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に対する意識について

（1）貴社において、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の取組みが始まった経緯や、重要性に対する認識が高まってきている背景や状況について、どのように見ていますか。

ア）いつ頃、何をきっかけに取組みを始めましたか。取組み前の状況はどのようでしたか。実際の脅威がありましたか。

イ）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の取組みを行う目的や狙いについて、どのように考えていますか。

ウ）近年、情報セキュリティ事故低減を図っていくうえで、果たすべき役割や責務が、どのように変わってきていますか。

エ）委託先における情報セキュリティ確保を図っていくうえで、何が課題になりますか。

①マネジメントの課題（ルール策定、監査・確認、ガバナンスの効かせ方等）

②取組みの課題（委託先の情報入手、コスト負担、ツールの有無、その他取組みを阻害する要因等）

オ）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への取組みについては、どのような考え方のもとで実施していますか。

カ）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の取組みにおいて、当初の目的や狙いをどこまで達成できたと考えていますか。

2. 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の具体的な取組みについて

（1）貴社では、グループで統一されたルールを策定していますか。

ア）ルールの全体構成はどのようになっていますか。海外の取引先にも適用されるものですか。

イ）委託先においては、ルール遵守がどの程度徹底されていますか。どのような方法で徹底を図っていますか。

ウ）ルールを策定するにあたり、参照しているガイドライン（NIST のガイドライン、業界のガイドライン等）はありますか。

(2) 貴社では、再委託先の情報セキュリティ管理が、どの程度必要になっていますか。
ア）委託先との基本契約で再委託できない旨を定めていますか。
イ）（定めている場合）例外はどの程度認められますか。例外が認められるには、何が必要になりますか（委託元から書面により再委託の事前承諾を得る、委託先や再委託先に追加の要件を課すなど）。
ウ) 再委託先における情報セキュリティ対策状況をどのような方法により把握していますか。
(3) 委託関係が重層的に連鎖する場合や、グローバルに地理的に分散し広範に及ぶ場合には、どのような取組みが必要であると御考えですか。
ア）情報セキュリティ上の観点からみたリスクのうち、特に問題視しているリスクは何ですか。
イ）上記のリスクに対して、どのようにマネジメントしていますか。
ウ）ルール遵守の確認や検査をどの程度やり切れていますか。
エ) 委託先に対する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への取組みの実効性を高めるために、どのような事項について、モニタリングを実施できていますか。何かツールを導入し活用していますか。
(4) 委託する際に、契約上でセキュリティの保護対象をどのように特定して、保護を求めていますか。それとも包括的な対応を求めていますか。
ア）顧客から預かっている個人情報・機密情報や、自社独自の個人情報・機密情報を漏洩させないようにすることが多いですか。
イ）製品・サービスの安全性に関わる脅威についても、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の取組みの対象になりますか。
ウ) 機密性に関する脅威のほか、改ざんやなりすましなどの完全性に関する脅威や、破壊や障害、DoS 攻撃などの可用性に関する脅威から、情報資産を保護することについて、どの程度考慮していますか。
(5) コストやリソースを考慮すると、委託先の情報セキュリティ管理をすべて賄うことには、自ずと限界が生じると考えられますが、そのような状況の中で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の取組みの効果を最大化するために、どのような取組みを行っていますか。
ア) 主要な事業に係るサプライチェーンリスクマネジメントの範囲を重点的に取り組んでいるなどの工夫はありますか。
(6) 納品物に対する確認・検査や、製品・サービス選定時のセキュリティ要件の確認は、どのような方法で実施していますか。
ア）納品物に使用されるソフトウェア（オープンソース・ソフトウェア等）の脆弱性や、納品物の不正動作（マルウェアやバックドアの混入等）を確認していますか。
イ）クラウド選定時や機器選定時にセキュリティ要件を確認していますか。
ウ）納品物に対する確認・検査や、製品・サービス選定時のセキュリティ要件の確

認は、どのような組織体制で実施していますか。

エ）納品物に対する確認・検査や、製品・サービス選定時のセキュリティ要件の確認において、どのような課題に直面することが多いですか。

オ）コストやリソース、開示情報の制約等を考慮すると、納品物に対する確認・検査等をすべて賄うことには、自ずと限界が生じると考えられますが、そのような状況の中で取組みの効果を最大化するために、どのような取組みを行っていますか。

(7) 貴社では、委託先をどのようにして選定していますか。

ア）委託先における情報セキュリティ対策状況は、どのような方法により把握していますか。

イ）訪問調査や書面調査はどのような方法や頻度で実施していますか。

3. 貴社の委託先等の情報セキュリティ管理体制について

(1) 委託先の情報セキュリティ管理は、どのような組織体制で実施していますか。

ア）委託元の立場である調達関連の部門・部署、開発製造関連の部門・部署と、委託元となる部門・部署を監督する立場である情報セキュリティ関連の部門・部署、リスク管理関連の部門・部署それぞれの役割はどのようになっていますか。

イ）どのような位置づけ・立場の者が、書面調査や直接訪問調査を実施していますか。

また、NIST に対するヒアリング項目を以下に示す。

1. NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”について

(1) 当該ガイドラインは、どのような経緯により策定されましたか。

ア）米国政府機関にどのような問題意識があって、その問題意識が、どのような検討や取組みを経て、 NIST SP 800-161 に形作られていきましたか。（NIST Cybersecurity Framework との整合性や、メリーランド大学の Cybersecurity Framework Risk Assessment Tool の活用との関連性など）。

イ） NIST SP 800-161 の策定に、民間はどのように関わっていますか。

(2) 当該ガイドラインを策定した目的やねらいは何ですか。またどの程度、効果がありましたか。

ア）当該ガイドラインでは、政府機関の調達のさまざまな場面において、必要となるリスクマネジメントプロセスや、ICT サプライチェーンリスクを軽減する管理策の実装について解説することが目的となっているが、現時点において、どれぐらいの米国政府機関等に、当該ガイドラインが活用されていますか。

イ）米国政府機関等において、当該ガイドラインの活用が進むことにより、どのような効果がありましたか（民間（各業界）において当該ガイドラインがどれぐ

らい活用されるようになったか、委託先のリスク管理に関わる問題発生率や業務負担軽減、市場の反応・評価の観点からみた場合にどうか)。

(3) 当該ガイドラインの適用対象について、どのような考え方で設定していますか。

ア) 適用対象が、政府調達から民間調達へと広がることが目指されているが、民間の中でも特に優先的に取り組んでもらいたいと考えている業界はどこですか（重要インフラ分野、IT 分野など)。

イ) 米国内の企業のみならず、グローバル企業にも適用されることが必要になると考えられますが、適用対象をグローバル企業へ広げていくために、どのような工夫がなされていますか。

(4) 当該ガイドラインや、当該ガイドラインを通じて、企業における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への取組みを、どのようにして普及させていますか。

ア) 当該ガイドラインが広く活用されるために、何が障壁になっていて、その障壁を取り除くには、どのような取組みを行っていますか（当該ガイドラインを活用して、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への取組みを実施した企業にとってインセンティブが働くような取組みや、実施していない企業に対してある程度強制力が働くような取組みなど)。

イ) DHS や DoD などの政府機関と連携して、どのような取組みを行っていますか。

ウ) その他に普及のためにどのような工夫を行っていますか。またどのような障壁を問題視していますか。

エ) 普及状況は業界によって、どのように異なりますか。またその要因は何ですか。

(5) 当該ガイドラインを受けて、米国政府機関等では、政府横断的に、委託先等に対して要求する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への取組みを定めた統一的なルールを策定していますか。

ア) (策定している場合) どの機関から、どのようなルールが策定されていますか。

イ) (策定していない場合) 策定されない理由や障壁について、どのように考えていますか。

(6) 当該ガイドラインについては、どのようなメンテナンス体制を構築することにより、ガイドラインの有効性低下や、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への取組みの陳腐化を防ぐ予定ですか。

ア) 当該ガイドラインの改訂や、PDCA を回すための仕組みについて、どのように考えていますか。

イ) NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”以外で、注目している海外のガイドラインはありますか。どのような点に注目していますか。

(7) 当該ガイドラインでは、必要となるリスクマネジメントプロセスや、ICT サプライチェーンリスクを軽減する管理策を取り決める際に、実効性や効率性について、どの程度考慮していますか。

ア）米国政府機関等における実装・運用にかかる負担を、どのように軽減していますか（リスク回避、リスク低減、リスク保有、リスク移転等による対応を適切に使い分けるなど）。

イ）企業における実装・運用にかかる負担を、どのように軽減していますか（リスク回避、リスク低減、リスク保有、リスク移転等による対応を適切に使い分けるなど）。

ウ）マネジメントするためのシステムを、どのように効率的に構築していますか（シンプルなプロセスや、ステークホルダー間での合理的な連携・分担を可能にするなど）。

(8) 米国政府機関等が、企業に対して要求する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への取組みや、企業の徹底を図るための取組みの更なる充実強化を図るため、今後、米国政府機関において、どのような施策の立案が必要になりますか。

2. NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”に従う企業側の意識や状況について

(1) NIST SP 800-161 が策定された 2015 年 4 月頃と、現時点（2017 年 1 月頃）を比較した場合、企業における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の重要性に対する認識に、どのような変化や違いが見られますか。

ア）（重要性に対する認識が高まってきている場合）どのような背景・理由がありますか（直近に何か重大な問題が発生したり、問題が発生する可能性があるリスクが高まっていますか、敵対国の企業とのグローバル取引の拡大などの米国の特殊事情が作用していますかなど）。

イ）（重要性に対する認識が変わらない場合）どのような背景・理由がありますか（委託関係が重層的に連鎖する場合や、グローバルに地理的な分散し広範に及ぶ場合が増えるなかで、これらに十分に対応し切れないか、買収や協業のダイナミックな動きなどの米国の特殊事情が作用していますかなど）。

(2) 米国政府機関等が、企業に対して要求する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への取組みについて、企業側では、何が課題になっていると認識していますか。

ア）現状の課題は何ですか。今後更に検討が必要となる課題は何ですか。

イ）当該ガイドラインが規定するリスクマネジメントプロセスや、ICT サプライチェーンリスクを軽減する管理策について、あるべき姿としての理想と、企業等が対応できることの現実との間には、どのようなギャップがありますか。

(3) 多くの企業が、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について、必ずしも十分に取り組んでいるとは言えない状況であると想定されるが、こうした状況を生み出す課題や要因に対して、どのような対応策が有効・有用であると考えていますか。

参考資料 4 ヒアリング調査結果

(1)民間企業のヒアリング調査結果

① 情報セキュリティに関する SCRM の取組みの経緯

回答企業	主な発言等
IT ベンダー	● 2006 年にファイル共有ソフト Winny が流行り、情報漏洩が多発した。Winny に関連した当社の取引先を起因とする事故が 30%以上あった。2008 年から情報セキュリティのトップマネジメントを行い、セキュリティ推進を行うワーキンググループを構築し、取引先のセキュリティ強化を始めた。
IT ベンダー	● 当社において発生した、脆弱性のあるソフトウェアの混入というインシデントがきっかけとなり、2004 年に情報セキュリティ推進組織を設立した。このインシデントを契機として、情報セキュリティ施策の決定権をどの部門に置くか、またどの部門が委託管理を担当するかという観点から、当社内の情報セキュリティの見直しが行われた。
自動車メーカー	● 車載システムのセキュリティについて注目したのは 3 年前である。当時、インパネを外して不正な機器を CAN に繋いだり、故障診断ポート経由でマルウェアが混入されるなど、CAN に対するセキュリティ問題に関わる報告が行われていた。米国における JEEP のハッキング実証実験が公表される前から、自動車工業会や JASPAR、自動車技術会といった国内業界団体では、車載システムのセキュリティ問題を業界共通の問題として認識していた。これがきっかけで、2014 年に社内に車載システムのセキュリティ担当者が置かれ、対策部品の開発・実装を担うようになった。
自動車メーカー	● 2010 年に、カリフォルニア大学サンディエゴ校のカール・コッシャー氏とワシントン大学の教授が、GM の自動車に対するハッキングの実証に関する研究論文を発表し、これに対し、GM 側がハッキングに悪用できる脆弱性に対処したことが契機となって、米国自動車業界全体が、GM のリスク対応の動きに追随するようになった。 ● 加えて、2015 年に、Jeep へのハッキングを可能とする脆弱性が公表されたことを契機に、製品セキュリティの必要性が、自社の経営陣に受け入れられるようになった。
製薬メーカー	● 製造ライン自動化を担う制御システムには、エアコンの動力供給システム、液体調剤システム、錠剤の圧縮システムなど、さまざまなシステムが相互接続されているが、過去に、サプライヤーから納入されたコンピュータシステムにおいて、製造段階に、ソフトウェア開発ライブラリのコードの中に悪意のあるコードが仕掛けられたことがあった。 ● このため、製造ライン自動化を担う制御システムは、社内のすべてのシステムから切り離し可能とし、かつ相互のシステム間にはファイアウォールを設置し、認められたごく僅かのトラフィックしか通過できないようにホワイトリストを用いたフィルタリングを実施している。

② 情報セキュリティに関する SCRM の取組みの目的と保護対象

回答企業	主な発言等
IT ベンダー	● 委託先でセキュリティ事故が発生した場合は、当社グループの管理不備が問われ、最終的には委託元が責任を負うことになる。このため、当社グループ全体が、委託先と一体となって情報セキュリティ強化に取り組むことにより、顧客からの信頼を得ることが大切であると考えている。 ● 取引先に対し、顧客のデータを預かっており、CIA の中でも Confidentiality（機密性）を一番重視している。
IT ベンダー	● 情報セキュリティに関するリスクマネジメントに取り組む目的は、①当社が顧客と共に事業を行ううえでセキュリティ事故を起こさないようにすること、②当社の納品物に対する最低限のセキュリティ担保を徹底できるようにすることである。
自動車メーカー	● 万が一、車両のセキュリティ事故を起こした場合には、企業イメージのダウンに繋がり、販売部門に迷惑がかかってしまう。また、リコールサービスキャンペーンが必要となるため、膨大なコストが発生する。 ● セキュリティ事故の内容次第ではあるが、例えば、車両のメーターが攻撃されて、表示不能となった場合には、車両に関する法規制を遵守できなくなる。このような事態は避けなければならない。 ● ナビゲーションユニットで扱われる電話帳や通行履歴などのプライバシー情報がセキュリティ保護対象となる。本人の特定が可能な情報や本人が知られたくない情報をプライバシー性の高い重要データとして指定している。 ● 製品の機能やデータの安全性も保護対象となる。四段階で求める安全度合いのランク付けを実施している。現在、ECU プログラムなどのソフトウェア機能のセキュリティを、不正な書き換え等の攻撃からどう守るかが重要となる。
自動車メーカー	● 製品のセキュリティリスクとして、①製品の安全性、②プライバシーの保護、③製品の信頼性の三つのリスクを扱っている。自動車同士が繋がっているシステムでは、製品に対する攻撃の影響が、同システムの基盤を介して、販売管理システム等の企業の基幹システムにまで波及する可能性がある。自社が構築するサプライチェーン以外の外部ベンダーの部品を使用できるようになっている場合は、その部品が、製品やシステムに対して悪意のある何らかの行動を起こし、攻撃の機会となるリスクが増す。
製薬メーカー	● セキュリティ保護対象は、患者の安全性、患者のデータ(職員・顧客のデータ)、自社の知的財産、並びに法令であり、優先順位はこの順に従う。 ● 薬品業界の最優先事項である患者の安全性を確保するため、製造工程の混乱・停止により、医薬品を必要とする患者に医薬品を渡せなくなる状態や、製造工程で利用されるデータの中に誤りのあるデータが含まれる事態を回避しなければならない。 ● セキュリティ保護対象が、どのように保護されるかは、何を委託するかによって決まる。例えば、部品製造の委託を行う際には、少なくとも当社の製造環境でのセキュリティ管理と同等のレベルのセキュリティ管理を担保する必要がある。

③ 情報セキュリティに関する SCRM の取組みと対象範囲

回答企業	主な発言等
IT ベンダー	● 委託先に対しては、納品前の脆弱性の確認や、セキュアな開発環境下での製品開発に取り組むよう要請している。しかしながら、委託先が確認できる領域には自ずと限界が生じるため、最低限の安全性の担保と考えている。 ● 委託先には、工事系の企業も含まれ、工事系の企業では、再委託の重層的な連鎖構造が 5 次～6 次まで及ぶ場合もある。再委託先のセキュリティ管理は当社で直接行うことができないため、委託先にセキュリティ管理を一任せざるを得ないのが実情である。 ● 納品物に関しては、委託先に対して事前に脆弱性をチェックするよう依頼している。また、セキュアな開発環境下で開発に取り組んでいる。しかしながら、脆弱性を確認できる領域には限界があるため、最低限のセキュリティ担保で製品・サービスを提供できるように取組んでいる。
IT ベンダー	● 委託先に対して、①情報、②組織体制の二つを管理するための取組みを徹底するよう要請している。 ● 系列会社（資本関係のある委託先を含む）に対しては、ISO/IEC 27000 シリーズや経済産業省の情報セキュリティ管理基準をベースに、情報セキュリティ施策推進会議が定めたサイバーセキュリティマネジメントフレームワークに基づいて管理を行っている。 ● 資本関係がない委託先に対しては、当社の理念・行動規範の遵守に加えて、情報管理や情報システムのセキュリティに関する当社が策定した規定の遵守を要求するとともに、契約時にそれらの遵守を約束する誓約書を提出させている。 ● 情報セキュリティに関するリスクマネジメントの全社統一ルールを策定する際には、製品を提供するプロダクト事業や、システム開発事業などの対象事業によって、セキュリティ確保の考え方や管理が必要となるプロセスの範囲が異なり、組織も複数にまたがるため、統一化を図ることが難しい。このため、ルール策定にあたって、経営層からトップダウンで指示が下りてくることが重要となる。 ● 各国・地域によって、系列会社のセキュリティ管理に対する取組みの方法が異なるため、先ずは、海外の系列会社への一律の統制が求められる最低限の範囲を明確にし、その範囲から海外の系列会社に対する統一的なセキュリティ管理を始めることが重要となる。 ● 製品に関するセキュリティ強度の評価基準は、製品仕様ごとに異なり、一律の評価基準をすべての製品に適用できる訳ではない。このため、当社では、技術面の管理以上に、プロセス面の管理に重点的に取り組んでいる。 ● 技術的対策と物理的対策における安全措置の実装は、委託先によるコスト負担を伴うため、実装が必要となる安全措置の範囲を明確に規定していない。このため、安全措置の取組みはあくまで最低限の範囲にとどまる。 ● 納品物に使用されるソフトウェアの脆弱性については、診断ツールを活用して検査を行っており、ほぼ最新の脆弱性情報まで対応可能である。

	● 納品の過程で媒体を介する場合には、媒体のウイルスチェックを適宜実施している。納品後の製品に対するマルウェア監視については、顧客による取組みを前提にしている。 ● ウェブアプリケーションの脆弱性についても、ソースコードレベルでの事前確認と専用の診断ツールを活用した検査を行っている。
自動車メーカー	● Tier1 サプライヤーに対して、SOW（Statement of Work、作業範囲記述書）に基づく納品物のセキュリティチェックを実施している。SOW においては、セキュリティ上の問題が発生し、当社が設計書や図面等の開示要請を行った場合に、当該要請に応じなくてはならない義務や、第三者によるセキュリティ診断テストの実施の義務等を規定している。また、Tier1 サプライヤーの開発拠点や製造拠点の現地調査も実施している。 ● Tier2 サプライヤー以降に対しては、直接的にサプライチェーンリスクマネジメントの取り組みを実施することはない。
自動車メーカー	● 社内には、製品におけるサイバーセキュリティの確保を担当する専門組織が存在する。当該組織は、すべての製品を対象として、製品にサイバーセキュリティ対策を実装するための全社方針を策定するとともに、当該方針への遵守を徹底させる責任を負っている。このような専門部署による取組みにより、現在においては、セキュリティリスクへの対処が徹底された製品が確実に設計・開発されるようになった。多くの OEM が同様の専門部署を設置している。 ● サプライチェーンが重層的な構造になる中で、Tier3 サプライヤーや Tier4 サプライヤーといった川下の企業に対して直接連絡を取れない。委託元がこのような企業に対してセキュリティ管理を行うことはほぼ不可能であるため、標準化が極めて重要となる。 ● 納品された製品をテストし、純正部品のみから構成されていることを確認する。純正部品については、サプライチェーンのより川下になればなるほど、安全性・信頼性確保という本来の目的を実現することが難しくなる場合があるため、純正部品が確実に納品されたことを確認することが重要となる。 ● 納品物で使われているソフトウェアの脆弱性や不正動作については、セルフテストによる確認を行っている。但し、既知の脆弱性や不正動作については、セルフテストによる確認が可能であるが、新しい脆弱性や新しい攻撃手法を用いた不正動作については、確認は不可能である。 ● NIST ガイドラインの枠組みは非常に有用であるが、自動車業界では、遵守義務がなく、ベストプラクティスや推奨規格のガイダンスでしかないと考えられている。
製薬メーカー	● 契約書上で Tier1 サプライヤーには、Tier2 サプライヤー以降のセキュリティを管理する責任はないが、現実的には Tier1 サプライヤーが自発的に Tier2 サプライヤー以降のセキュリティ管理を行っている。 ● 委託先のセキュリティ水準が当社の要求する水準に満たしているかを見極めている。新しい委託先と取引を行う際には、当該委託先のセキュリティコントロールが

	どの程度有効であるかを五段階で算定するリスク評価プロセスを適用している。このプロセスを通じて、委託先のセキュリティコントロールが脆弱であることが判明すれば、委託を見送る可能性がある。また既に取引のある委託先であっても、セキュリティコントロールの質の低下が見られる場合には、それを理由に委託を取りやめる可能性がある。 ● 5 年間のサイバーセキュリティ保険に加入している。保険対象には、サプライチェーンにおける主要サプライヤーで重大なインシデントが発生する可能性を考慮して、主要サプライヤー数社を新たに含めた。保険に加入するためには、主要な Tier1 サプライヤー数社から必要なデータを取得し、保険会社に提出する必要があった。このようなサプライヤーのデータは、保険会社において、リスクコントロール基準に応じたスコアリングに活用されることを期待している。 ● リスク評価プロセスの適用やユーザー行動分析等のモニタリングの積極的な推進を通じて、委託先に対する取引開始時の監査や定期的な監査を実施している。セキュリティチームでは、1 週間の期間においてモニタリングされた 1,000 億件のイベント（ビッグデータ）を分析・処理している。

④ 情報セキュリティに関する SCRM における再委託の取り扱い

回答企業	主な発言等
IT ベンダー	● 原則、再委託を禁止する規定を設けている。しかし、当社と取引のある委託先の半分以上は、再委託を行っている。再委託の多くの場合、再委託先の社員に当社に常駐してもらうことにより、情報漏えいを回避する取組みを行っている。 ● 防衛・宇宙産業、金融業、通信業では、顧客が再委託の禁止を要求する場合もある。また、顧客から提示される調達要件の中に、委託先の国籍提示が求められる場合が増えている。
IT ベンダー	● 全社統一ルール上に再委託を禁止する規定を設けていない。ただし、委託先のセキュリティレベル分けを行ったうえで、赤信号の評価が下された委託先に対しては、一定の条件や期間において再委託を禁止している。
自動車メーカー	● 再委託先以降に対しては、直接的にサプライチェーンリスクマネジメントの取り組みを実施することはない。委託先が再委託を行う際には、標準契約書上で当社が委託先に対し、課しているセキュリティ義務と同じ内容を、再委託先にも遵守してもらう。委託先に再委託を行う旨を申告してもらい、委託先が再委託先の情報セキュリティ管理責任を負う形を採っている。
自動車メーカー	● 再委託を禁止する規定は設けていない。下請け業者を使用することは一般的であり、規定の多くはそれを考慮して策定される。その一方で、当社では、下請け業者の情報開示を盛り込んだ規定の改正を検討している。セキュリティリスクへの懸念について対応意識が高まるなか、下請け業者やその開発者の詳細について把握する必要性が高まっている。
製薬メーカー	● 委託先における再委託を禁止する一般条項を設けているが、委託先で本当に再委託が

	実施されていないかを管理するのは非常に難しい。例えば、当社の委託先であるマーケティング会社が、当社のリスク評価プロセスが適用されていない再委託先に対して、ウェブサイトの設計・開発にかかる業務を再委託する事態が起きている。このようなケースでは、マーケティング会社において、情報セキュリティに関する SCRM の重要性に対する認識が希薄であったことが事態を招いた原因であった。優秀な IT 人材を抱えていないマーケティング会社が委託先となる際には、再委託先が前提となるうえ、セキュリティ管理を行うことも困難であることから、過去には、問題が発生したこともある。

⑤ 情報セキュリティに関する SCRM にかかるグローバル化に対する実効性

回答企業	主な発言等
IT ベンダー	● 当社グループ全体で情報セキュリティに関する SCRM の統一ルールを整備している。しかし、海外グループ会社へのルールの適用徹底については、各国における法規制や商慣習などの違いもあり、これからの検討課題である。
IT ベンダー	● 情報セキュリティに関する SCRM の取組みは、海外の委託先に対しては、まだ着手し始めたばかりである。資本関係のある海外の委託先に対しては、国内の委託先向けに定めたセキュリティ管理の全社統一ルールをもとに運用する方針である。しかしながら、国・地域ごとに法令遵守事項が異なるため、全社統一ルールに対して、国・地域ごとに細かい変更を加えて運用している。 ● 一方、ネットワークと一部のシステム環境を対象としたモニタリングについては、資本関係のある海外の委託先を含め共通の取組みを実施できている。 ● 海外の系列会社のセキュリティ管理における、情報セキュリティ施策推進会議が定めたサイバーセキュリティマネジメントフレームワークの活用については、決定までには至っていない。
自動車メーカー	● グローバル企業としての運営を志向するなかで、すべてのプロセスをグローバルスタンダードに基づくプロセスに更新しようとしている。これにより、複数段階において契約合意が必要となるプロセスや、仕様とは異なる製品が開発されるプロセスを不要となるようにする。しかしながら、各国・地域の法規制の違い等から、グローバルスタンダードに基づくプロセスを統一的に運用することが不可能となる場面も生じ得る。 ● また、各国・地域の法規制に対して、解釈を誤って適用するなど遵守が不十分となる場合には、罰則等を受けるリスクも起こり得る。 ● このため、全社的な取組みとして、各国・地域の法規制の違いやこれに起因するリスクを追跡し管理できるようにするための専門組織を立ち上げている。
製薬メーカー	● 当社のセキュリティチームは 150 名のメンバーにより構成され、米国、シンガポール、チェコ共和国に主要拠点を配置するなどグローバルに展開している。各環境・地域に配備された担当者・チームは、当該環境・地域でのセキュリティコントロールの全てを担う。

	● グローバルでの情報セキュリティに関する SCRM の取組みについては、なるべく各国の要求基準等に固執・依存しない最善のセキュリティ管理体制を追求しているが、個人情報の取り扱いのように米国、欧州、ロシア、中国それぞれで法律上の義務化された要求基準等が異なる場合にはローカライズ対応を実施せざるを得ない状況である。

⑥ 情報セキュリティに関する SCRM の取組みの達成レベル

回答企業	主な発言等
IT ベンダー	● 国内においては、取引先のセキュリティ事故件数は、かなり減少しており、情報セキュリティに関するリスクマネジメントの成果が出ている。 ● 納品物の不正動作については、診断ツールを活用することにより検知できるものもあるが、ブラックボックス化されている部分もあるため、必ずしも十分な確認・検査が実施できている訳ではない。 ● 海外の委託先に対しては、国内の委託先に求めるセキュリティレベルと同等のレベルの取組みを適用できていない。現在は、ソフトウェア開発の委託が中心で売上高が大きく、リスクも高い中国の委託先を対象として、先行的にセキュリティレベルの強化に向けた取組みを行っている。今後、アジアパシフィックの委託先に対しても、順次、同様の取組みを展開していく予定である。 ● ソフトウェア開発の委託をほとんど行っていない北米や欧州の委託先に対しては、中国やアジアパシフィックで推進しているセキュリティレベルの強化に向けた取組みを実施する必要はないと考えている。
IT ベンダー	● 情報セキュリティに関するリスクマネジメントの取組みは効果が上がっており、重大なセキュリティ事故が全く起きていない状態が数年間続いている。 ● セキュリティ強化を売りとしたビジネスの拡大、サイバーセキュリティ基本法の施行、IoT セキュリティ分野における取組みの活発化を背景に、情報セキュリティに関するリスクマネジメントに対する経営層の意識も高まってきている。
自動車メーカー	● Tier1 サプライヤからの納品物のセキュリティチェックはまだまだこれからであると認識している。現在は設計書上の書面チェックやホワイトハッカーによるセキュリティ診断テストの実施により、セキュリティ事故の発生に対して一定の歯止めをかけられているものの、これらの取組みだけで十分とは考えていない。
自動車メーカー	● 技術的対策としては、非純正部品を不正に使用しようとした場合に、製品のハードウェアがそれを検知し、使用を停止できる仕組みを実装しており、一定の成功を収めている。 ● 一方、サプライチェーン全体にわたって、模倣品が部品として使用されていないかどうかを調査したり、各ベンダーからそのような行為を行っていないという報告を受けたりするなどの監査を行うことは現時点では困難である。

	● このような監査の促進に繋げるために、ハードウェアに関する、サイバーセキュリティ・ソリューション向けのシリコンチップの機能の標準化や、サプライチェーン全体で必要となる情報を共有する方法の標準化が必要である。

⑦ 情報セキュリティに関する SCRM の取組み上の課題

回答企業	主な発言等
IT ベンダー	● 国内における情報セキュリティに関する SCRM の取組み上の課題は二つある。 ● 一つ目は、情報セキュリティ対策に前向きでない企業を中心に、セキュリティレベル向上に関する取り組みが少ない取引先企業をどのように改善していくかが課題である。特に、当社と取引先との力関係からみて、取引先が当社から仕事を得られ、優位な立場にある場合、当社が推進するセキュリティ強化の取り組みに対して前向き取り組んでくれない場合がある。 ● 二つ目は、異なる企業規模を持つ委託先に対して、共通的に一律のセキュリティレベルの対策を強要するのが難しいことが課題である。特に、技術的な対策に関しては、中小規模の委託先においては、コスト面の制約が大きくなりがちであり、前向き取り組んでくれない場合がある。 ● その結果として、個々のプロジェクトに応じて、情報セキュリティ対策の取組みに温度差が生じるため、全体としての最適化を図っていくことが必要になる。 ● 海外では、委託先のセキュリティ管理を担う海外現地法人の担当者とのコミュニケーションを円滑に行うことができるかが課題である。日本語で会話できる人材の確保難や、契約・交渉にかかる商慣習の違いがコミュニケーションの障壁になりやすい。 ● グローバルの委託先管理においては、中国の現地法人の調達部門が積極的に取り組んでくれている。中国の現地法人では、日本語が話せる人材を積極的に採用しているのでコミュニケーションを取り易い。一方、インドでは日本語を話せない人がほとんどであるので、英語でやり取りする必要があることや文化面で違いがあることといった部分で障壁になるケースが多々あり、コミュニケーションが取り辛い。
IT ベンダー	● 資本関係の有無によらず、すべての委託先に対して、網羅的にセキュリティ管理を行うのは時間面の大きな制約もあり、困難である。委託先に対して実施する現地調査についても、是正が必要な委託先のみに対象を限定している。現地調査においては、均質なレベルで監査の実施が求められるが、このような監査に対応可能な人材が不足し、体制が脆弱であることが課題である。 ● 委託先がセキュリティ事故を起こさないようにするためには、安全な開発環境を構築する必要があるが、コスト負担の問題を伴うため、このような環境の構築が進んでおらず、十分な統制を効かすことができない。 ● サプライチェーン全体でセキュリティ管理を徹底することは困難であり、当社は委託先までを管理対象とせざるを得ない状況である。再委託先のセキュリティ管理は委託

	先に一任している。
自動車メーカー	● セキュリティ分野は、社内に経験者が少ないため、外部の知見を活用するしかない。スキルやリソースが足りていないのが大きな課題である。契約書において、委託先に義務付けるセキュリティチェックの項目を記載することが難しいレベルである。 ● 自動車部品、バックエンドシステム、工場設備などのセキュリティ管理を包括した委託先向けの全社的なルールは整備されていない。
自動車メーカー	● セキュリティ上の新たな脅威が発見されれば、脅威への対応のために、脅威が備える機能や脅威への対処法に関する情報をサプライチェーン全体で共有することが求められる。その際、如何にしてサプライチェーン全体で必要となる情報を共有する方法を確立できるか、また、脅威に対して、ベンダー同士の協働・協調のもとで、対処法の検討を実施できるかが重要な課題となる。 ● これらを確立・実施していくうえで、重層的な連鎖構造を形成するサプライチェーンを考慮すると、標準化が極めて重要となる。SAE（米国自動車協会）の主導のもと、このような標準化が推進されている。その一つの取組みとして、サイバーセキュリティ・ソリューション向けのシリコンチップの機能の標準化が目指されている。 ● NIST の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の枠組みは、有益であるが、遵守義務がなく、ベストプラクティスの推奨にとどまるため、自動車業界ではあくまでガイダンスとして捉えられている。自動車業界に幅広く受け入れられるためには、SAE 基準にその内容が組み込まれることが必要となる。 ● サプライチェーンの各段階において、納品物が受入可能であるかを確認する標準化された方法が未だ確立されていないことが課題である。各段階では必ずしも OEM と同等のレベルで確認を行っている訳ではないため、人為的なミスの発生により、脆弱性が看過される可能性がある。 ● OEM が脆弱性を検知した場合、実際に是正しようとすると、Tier3、Tier4 まで遡る必要があり、コストや時間を要することから、脆弱性を認識するにとどまっている。取り分け、自動車のサプライチェーンにおいては、開発の最終段階に近づけば近づくほど、検知された脆弱性に対処することは難しくなる。 ● 既知の脆弱性については、セルフテストにより確認できるが、新しい脆弱性や新しい攻撃手法を用いた脅威については確認できない。
製薬メーカー	● 正常な行動からの逸脱が見られるユーザーを検知した場合、委託先と密接に関わる然るべき担当者を通じて、適切なセキュリティ対策を講じることが重要である。その際、当該担当者に対して、正確な情報を適正なタイミングで如何に伝達できるかが最大の課題となる。

(2)NISTのヒアリング調査結果

① NIST SP 800-161 の策定経緯や策定した目的・狙い

- 2008 年より、国家安全保障会議（大統領執務室）が主導する包括的全米サイバーセキュリティイニシアチブ（CNCI）が始まり、その重点分野の一つに ICT における SCRM の分野が位置付けられた。この一環として、当該分野の主要プラクティスに関わるガイドラインの開発が NIST へ委託されたことがきっかけである。
- また、NIST IR 7622 の策定には 4 年間を費やしたが、まだまだ不十分なものであったため、NIST SP 800-161 への移行を目指した。

② NIST SP 800-161 の適用対象設定にあたっての考え方

- 情報セキュリティに関する SCRM の取組みにより、製品へのマルウェアの混入や低品質のソフトウェアの開発、偽造品の開発といった問題を解決しようとした。また、これまで悪意のある攻撃者による意図的な行為に焦点を当ててきたが、偶発的に脆弱性が作り込まれる行為も含め包括的な内容に焦点を当て、解決すべき問題の範囲を拡大してきた。

③ NIST SP 800-161 を通じた企業における情報セキュリティに関する SCRM の取組みの普及状況

- NIST SP 800-161 は民間企業に広範に認識されつつも、必ずしも十分に利用されていないのが現状である。
- その一方で、IT ベンダー向けに供給者関係におけるセキュリティを規定した ISO/IEC 27036 の国際標準規格策定には大きな影響を与えた。2008 年以降、政府機関が情報システムに関する SCRM に関心を持っていることが分かると、民間は独自規格の開発に着手した。これが、ISO/IEC 27036 の国際標準規格策定へと繋がるきっかけとなった。現在では、一部の企業がその認定を受けることに繋がる。
- NIST SP 800-161 には民間に対して遵守を要求する権限はないため、委託関係のグローバル化を考慮すると、ISO/IEC 27036 のような国際標準規格が必要であり、それに基づく認証制度が、情報セキュリティに関する SCRM の取組みを強化するうえで最善の方法と考えている。
- 現在では、情報セキュリティに関する SCRM に関する、金融業界やエネルギー業界において、NIST SP 800-161 を基に独自ガイダンスを策定されている。

④ NIST SP 800-161 に基づく情報セキュリティに関する SCRM の取組みを定めた政府機関統一的なルールの策定状況

- 商務省、司法省、米国国立科学財団（NSF）、および米国航空宇宙局（NASA） において、2015 年より歳出予算法第 516 条に基づいて、NIST SP 800-161 の使用が義務化された。
- また、その後、2016 年に、米国行政管理予算局（以下、OMB）が、政府機関において影響度が「高度」と評価された情報システムを対象に、NIST SP 800-161 の使

用を要求する A130 を発行した。これにより、各機関の監査官は OMB に対して NIST SP 800-161 への遵守状況に関する年 1 回の報告義務が課されている。

⑤ NIST SP 800-161 のメンテナンス

- 現在、連邦政府情報システムへのセキュリティ管理策（以下、NIST SP 800-53）の改訂版を開発中であり、それに合わせて、NIST SP 800-161 の更新を予定している。

⑥ NIST SP 800-161 に基づく情報セキュリティに関する SCRM の取組みの実効性や効率性に対する考慮事項

- NIST SP 800-53 から情報セキュリティに関する SCRM に関する管理策を抜粋し、それらの管理策に対する情報セキュリティに関する SCRM 固有の実施ガイダンスを策定するアプローチは適当ではないと判断した。
- 実効性を高めるためには、既に普及しているリスクマネジメントの内容を土台にした方が効果的である。組織レベルのリスクマネジメントに関わる既存の NIST のガイダンスを基にして、そのうえに情報セキュリティに関する SCRM の側面をガイダンスに組み入れるアプローチが重要であり、NIST SP 800-161 の策定においては、当該アプローチを採用した。

⑦ 米国政府機関等が企業に対して要求する情報システムに関する SCRM の取組みを実施する上での課題

- NIST IR 7622 は、策定当初、セキュリティ強化に伴うビジネス面での追加コストの強制といった観点から各業界から懸念や不信感を持たれ、異論が多かった。
- NIST SP 800-161 への移行を目指すにあたり、各業界との定期的なミーティングの開催や、情報セキュリティに関する SCRM の取組みに関わる裏付け調査の実施などを通じて、各業界との信頼関係の構築に注力してきた。このような活動は、NIST SP 800-161 への懸念や不信感を払しょくするうえで一定の効果を上げた。

⑧ 米国政府機関等が企業に対して要求する情報セキュリティに関する SCRM の取組みの更なる充実強化を図るための必要施策

- 企業の多くが、情報セキュリティに関する SCRM にかかる自社の自主基準を世界中のサプライヤーに課しているが、その場合、当該基準を基に委託先等を監査する必要があり、このことが国際標準規格に準じた第三者による監査と違って、委託先等が当該基準で要求しているものを保護しているかを証明することを難しくしている。
- そのため、監査の実効性・効率性を高めていくにあたっては、第三者による監査が可能で、かつ広範な分野に適用可能な国際標準規格の策定とそれに基づく認証制度の確立が必要になると考えられる。