IT サプライチェーンにおける
情報セキュリティの責任範囲に関する調査

調査報告書

2019年4月発行

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

改版履歴

年月日	内容
2019年4月19日	発行

目　次

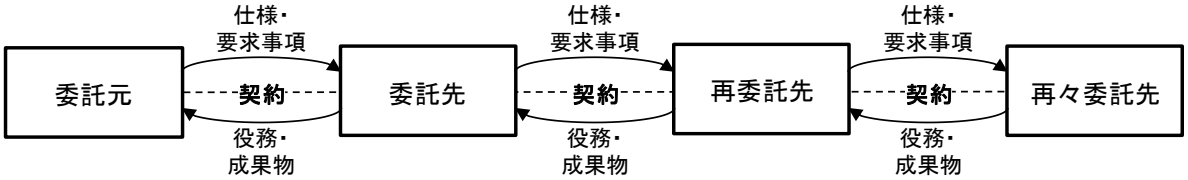
１．はじめに

1.1　調査の背景・目的

現在、多くの企業で基幹系業務のシステム化が済んでおり、IT システム・サービスのニーズは、業務の省力化や効率化を支援するためのものから、事業戦略を策定、推進するためのものへと変化している。そのため、汎用的な製品・サービスを利用できない分野では、IT システム・サービスへの要求はますます複雑化しており、必要な機能や作業のイメージを関係者間で共有できないままスタートしたプロジェクトでは、IT システム・サービスの本番稼働後に、セキュリティインシデント（以下「インシデント」とする。）が発生することも多くなっている。

一方で、IT システム・サービスに関する業務を系列企業やビジネスパートナー等に外部委託し、その業務委託が、委託先の再委託先、再々委託先へと連鎖する委託形態（**図表 1-1**。以下「IT サプライチェーン」とする。）は一般的となっている。IT サプライチェーン上のセキュリティリスクを低減させるためには、委託元と委託先の情報セキュリティに係る責任範囲の明確化が必要であるが、2017 年度に実施した「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」[1]（以下「2017 年度調査」とする。）では、委託元に専門知識が少なかったり、ビジネススピードを優先させるためにリスクを受容しながらも事業を進めたりする状況があり、契約等で情報セキュリティに係る責任範囲を明確にしていない実態があることが分かっている。この調査結果を踏まえ、2017 年度調査の報告書では、「国際規格や既存の基準、ガイドライン及び規格等も参考に、IT サプライチェーンの中で取り扱う情報資産や想定されるリスクを類型化した上で、すべての企業が最低限実施すべき基本的な取組みに関して整理された共通的な指標を整理することが必要と考えられる。」として、「情報セキュリティの取組みに関する共通的な指標の必要性」について言及した。

このような背景から、本調査では、IT システム・サービスに関する業務委託（以下「IT 業務委託」とする）において、情報セキュリティに係る責任範囲として、委託元と委託先の間で明確にしている項目、また、明確にしていない項目については、明確にできない理由や、責任範囲が明確でないリスクに対する対策等、実態を調査・分析した。また、その情報を広く公表することにより、我が国の企業における IT サプライチェーンリスクマネジメント[2]への取組み向上に資することを目的とした。



図表 1-1　IT サプライチェーン

[1] 情報処理推進機構「「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」報告書（2018 年）
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html

[2] IT サプライチェーン上の情報セキュリティリスクを防止・低減するための仕組みや活動のこと。

1.2 調査のスコープ

本調査では、IT システム・サービスの IT 業務委託における、IT サプライチェーンリスクマネジメントの実態や課題を調査、分析すると同時に、実際に業務を委託（委託元の場合）、受託（委託先の場合）した具体的な事例における、情報セキュリティに係る責任範囲の明確化の状況を調査、分析した。

2017 年度調査の報告書で述べたとおり、情報セキュリティに係る責任範囲の議論には、①業務委託の中で、委託先が実施すべき情報セキュリティ対策の範囲、②インシデントが起きた際の委託元と委託先の損害の負担という 2 つの観点がある。この観点を踏まえ、本報告書では、「責任範囲」の定義を、「契約あるいは双方の合意によって定められたセキュリティ面の業務の遂行責任と、それに係る費用負担の取り決め」とした。以降、特に断りが無い限り「責任範囲」は、「情報セキュリティに係る責任範囲」を指すものとする。

また、調査対象とする業務については、IT システムの構築・保守に関連する業務、IT サービスの提供に関連する業務を、次の**図表 1-2** のとおりに整理し、これらの対象業務のいずれか、あるいは、いくつかを組み合わせた業務を委託・受託する場合について調査、分析した。

図表 1-2　調査対象業務

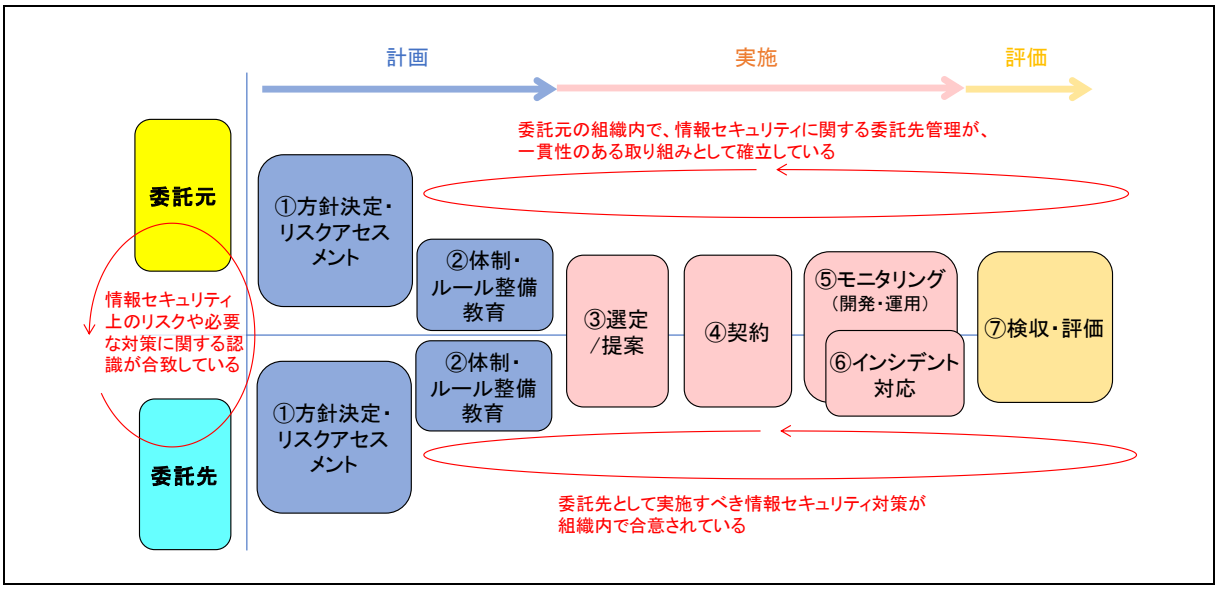
調査対象業務
・ソフトウェア開発[3] ・システム運用・管理 ・アプリケーション保守 ・ソフトウェアサポートサービス[4] ・ハードウェア保守 ・Web サイト構築・運用 ・サービス提供（ASP、SaaS 等） ・インフラ提供（IaaS、ホスティング等） ・データ処理・分析

[3] 本調査では、固有のアプリケーションソフトウェアを開発する業務を指すものとし、パッケージソフトウェアを利用する場合も含めた。

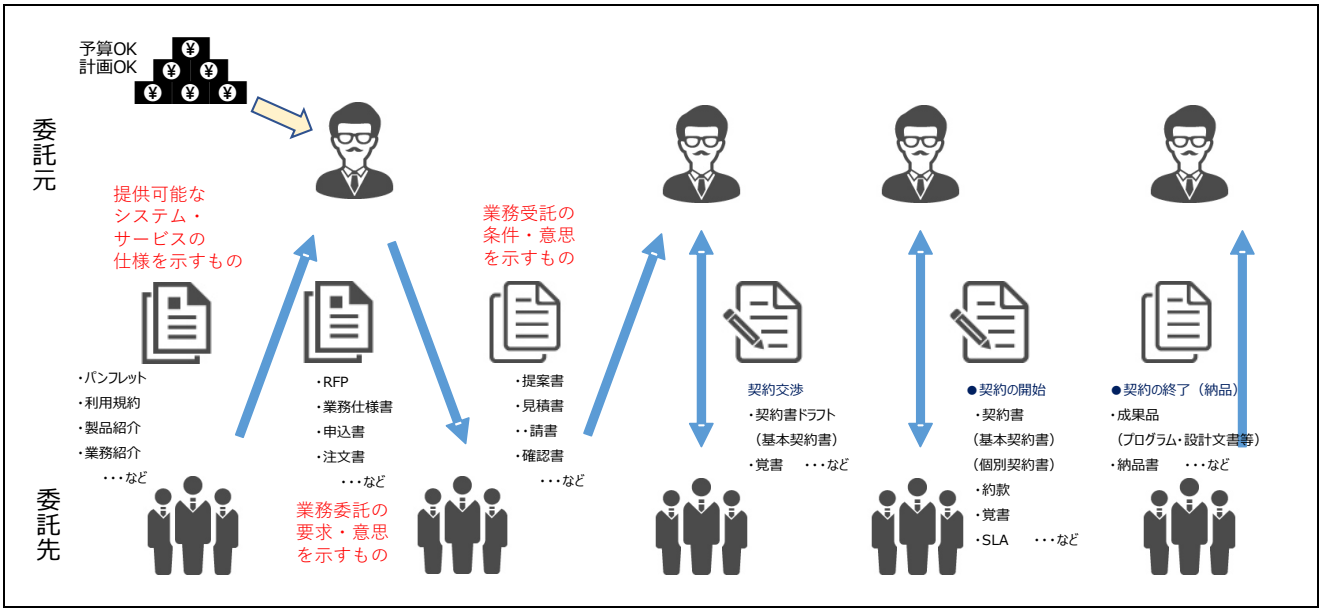
[4] 本調査では、OS やミドルウェア等のソフトウェア製品に関する問い合わせ対応、アップデートモジュールの提供、技術情報や FAQ の提供等によりソフトウェア製品の導入や運用をサポートするサービスを指すものとした。

2017 年度調査では、IT 業務委託のプロセスを、IT サプライチェーンリスクマネジメントの観点から、IT 業務委託の方針決定・リスクアセスメントや委託先管理のルール整備等の「計画段階」、委託先の選定・契約・業務遂行までの「実施段階」、業務の検収、評価等の「評価段階」の 3 つの段階と 7 つの業務委託のプロセスに整理し、次の**図表 1-3** のとおりモデル化した。

また、この**図表 1-3** のプロセスの中で実施する業務委託契約における委託元と委託先の間のやりとりおよび、責任範囲を明確化するための文書を整理したものが、次の**図表 1-4** である。



図表 1-3 業務委託のプロセスにおける IT サプライチェーンリスクマネジメントの取組み



図表 1-4 IT 業務委託において責任範囲を明記・確認することができる文書

図表 1-3 の「①方針決定・リスクアセスメント」において、委託元は業務や情報資産を委託することによるリスクを考慮して対応方針を決定する。その際、委託先から提供可能なシステム・サービスの仕様を示すものを適宜参照する。委託先によっては、システム・サービスが満たしている情報セキュリティのレベルや会社として取り組んでいる情報セキュリティ対策を公開していることもある。

図表 1-3 の「③選定／提案」では、委託元は、既存のシステムの調達やサービスの提供で十分か、それとも、自社の業務要件を元に新規開発やカスタマイズが必要かといったことを検討し、業務委託の要求・意思を示すものを委託先に提示する。既存のシステムやサービスの場合は、委託先の用意した申込書や注文書等で十分であるが、新規開発やカスタマイズを伴う場合は、業務仕様書をまとめたり、提案依頼を行ったりすることにより委託先に要求事項を伝える。取り扱われる情報資産の価値が高かったり、長時間の連続稼働等可用性が求められたり、不特定多数の利用者がアクセスしたりして情報セキュリティリスクが高い場合は、情報セキュリティ対策について提案に含めたり、チェックリストの提出を求めたり、ISMS 等認証取得を条件としたりすることもある。委託先では、委託元からの業務委託の要求・意思表示の内容を確認し、受託可能であるかを検討する。もしも、受託する場合は、業務受託の条件・意思を示すものを委託先から委託元に提示する。この時の手続きは口頭、確認書・請書のような定型の書面の発行、提案書等を用いた説明等、様々である。

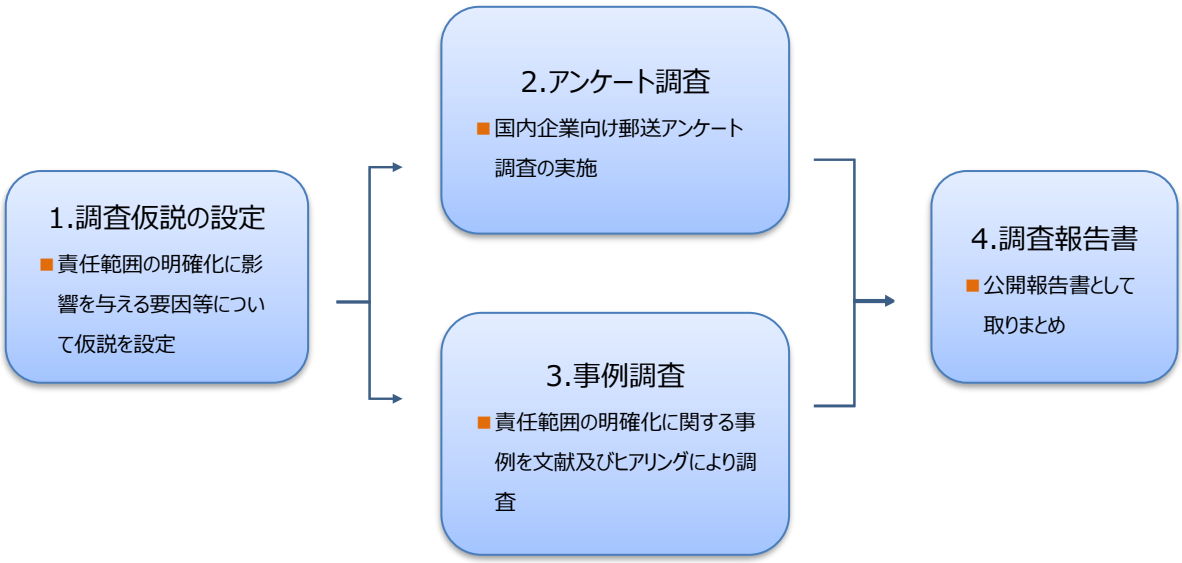
図表 1-4 の後半の活動「契約交渉」、「契約の開始」、「契約の終了」は、図表 1-3 の「④契約」、「④モニタリング、⑤インシデント対応」、「⑦検収、評価」の各プロセスの中で行われる。ソフトウェア開発のように開発工程で徐々に要件が具体化するような業務の場合は、契約締結時は基本的事項のみが合意され、具体的な要件は都度取り決められることが多い。契約書の締結や更新は厳密な手続きが法的に求められるため、覚書や SLA 等を用いられることが多い。本報告書では、委託元と委託先の間で責任範囲について取り決め、記載する文書を総称して「契約関連文書」と呼ぶ。

本調査では、具体的な IT 業務委託の事例について、契約関連文書における責任範囲の明確化の状況を調査、分析した。

1.3 調査の実施概要

1.3.1 調査の実施フロー

本調査では、責任範囲の明確化の状況について、以下の**図表 1-5** に示すフローで調査を行い、その結果を本報告書に取りまとめた。



図表 1-5 調査の実施フロー

1.3.2 調査仮説

本調査では、責任範囲の明確化に影響を与える要因等について、**図表 1-6** の調査仮説とその仮説の調査対象を設定した。

2017 年度調査では、「1.1　調査の背景・目的」で述べたとおり、委託元に専門知識が少なかったり、ビジネススピードを優先させるために責任範囲が曖昧であることのリスクを受容しながらも事業を進めたりする状況があり、契約等で責任範囲を詳細にしていない実態があることが分かっている。

この調査結果を踏まえて、本調査では、IT 業務委託における契約書の雛形とその運用について No.1～No.5 の仮説を、責任範囲が曖昧になる要因について No.6～No.10 の仮説を立てた。

また、責任範囲の曖昧さを解決できない場合のリスクへの備えとして、サイバー保険があるが、サイバー保険の加入状況等について No.11～No.13 の仮説を立てた。

図表1-6 調査仮説と調査対象

No	調査仮説	調査対象	
		委託元	委託先
契約書の雛形とその運用について			
1	委託元の主たる事業が化学製品の生産や販売である場合、情報セキュリティ要求事項の含まれる契約書の雛形を用意している。	○	
2	委託先は、ITシステム・サービスの種類ごとに情報セキュリティ要求事項の含まれる契約書の雛形を用意している。		○
3	委託先は、ITシステム・サービスの種類ごとに情報セキュリティ要求事項の内容を変えている。		○
4	情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形に記載されている情報セキュリティ要求事項の変更は可能である。	○	○
5	大企業は、案件ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けている。	○	○
責任範囲が曖昧になる要因について			
6	委託元は、委託先の責任範囲を限定してしまうと、それ以上のことをしてもらえなくなるので、責任範囲を限定したくない。	○	
7	委託先は、責任範囲を詳細に決めると、コスト高になり、委託元の合意が得られなくなるので、大まかな取り決めでもよいと考えている。		○
8	委託元と委託先の関係に資本関係がある場合、契約関連文書に組織的なセキュリティ対策が明記されることが少ない。	○	○
9	委託元は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなくても委託先が対応すべきだと考えている。	○	
10	委託先は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなければ実施する必要はないと考えている。		○
サイバー保険の加入状況等について			
11	委託元、委託先ともに、サイバー保険に加入している割合は低い。	○	○
12	委託元がサイバー保険に加入している理由は「損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償」が魅力的と思っているからである。	○	

13	委託元がサイバー保険に加入していない理由は「委託先がサイバー保険に入っていればよい」と思っているからである。	○	

以下に、これらの仮説を設定した理由について述べる。

2017 年度調査で、情報セキュリティに関する委託先管理の社内ルール・規定類の整備状況として、最も多かったのが「情報セキュリティ要求事項を含む契約書雛形」であり、従業員数 301 名以上の企業の 47.4%、従業員数 300 名以下の企業の 33.2%という結果であった。契約書雛形があることによって契約書作成を効率よく実施することができるが、反面、雛形と異なる記載がしにくくなったり、雛形に頼り切ってしまい必要な要件が抜け落ちたり、内容が不十分であったりということが懸念される。雛形が情報セキュリティの要件に対して効果的に利用できるようになっているのか、契約の内容が適切であることが確認されているのかを検証するために No.1～No.5 の仮説を立てた。

2017 年度調査で、委託元と委託先の情報セキュリティ上の責任範囲が不明ということが大きな課題として挙げられた。責任範囲が不明となってしまうのはなぜなのか、責任範囲が不明なまま業務が進められることで問題は発生していないのかを検証するため、No.6～No.10 の仮説を立てた。

サイバー攻撃や未知の脆弱性への対応について責任範囲が明確になっていないと、迅速な対応が遅れ、被害の拡大や復旧の遅れに発展する可能性がある。専門性が高いことから委託先が対応することを委託元から期待されることがよくあるが、費用的な負担の調整が後回しとなり、トラブルとなることもある。このような金銭面での負担を軽減する対策として保険を利用することが考えられる。2017 年に改訂された「サイバーセキュリティ経営ガイドライン 」でも、「指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」の中でサイバー保険の活用について触れられている。このような背景から、サイバー保険についてどれくらい認識され、利用されているのか、利用されていないとしたらその原因は何かを検証するため、No.11～No.13 の仮説を立てた。

1.3.3 アンケート調査

（1）調査対象

アンケート調査の調査対象は、次の**図表 1-7** のとおりとし、調査票は委託元用と委託先用の 2 種類を作成した。

図表1-7 アンケート調査の調査対象

分類	定義	回答を依頼した部門
委託元	自社事業のために IT システム・サービス（社内システムや顧客向けシステム）の構築・運用等を委託するユーザ企業	・調達部門（ITシステム・サービスの業務の発注等を行う部門） ・情報システム部門・情報セキュリティ部門（情報システム部門から独立した組織がある場合） ・リスク管理部門 ・法務部門（契約締結/利用規約への同意に責任を持つ部門） ・現場の事業部門（IT業務委託の実施を決定する部門）
委託先	委託元より IT システム・サービスの構築・運用等を受託するまたは当該 IT システム・サービスの構築・運用等の再委託を受けるITベンダ企業	・営業部（IT システム・サービスの業務の受注等を行う部門） ・情報システム部・情報セキュリティ部門（情報システム部門から独立した組織がある場合） ・リスク管理部門 ・法務部門（契約締結/利用規約への同意に責任を持つ部門） ・現場の事業部門（ITシステム・サービスの構築・運用等を実施する部門）

（2）調査票の発送数

①委託元

委託元については、**図表 1-8** のとおり、調査対象業種を製造業、卸売業・小売業、サービス業に絞り込んだ。これは、2017 年度調査の結果から、他の業種よりも「委託先が実施すべき具体的なセキュリティ対策を仕様書等に明記していない」割合が高かった業種である。アンケート調査では、2017 年度調査の調査結果と比較しつつ、調査対象業種の責任範囲の明確化の状況の把握、分析を詳細に行うために、製造業、卸売業・小売業、サービス業の 3 業種のみを調査対象とした。また、企業規模の定義は、2017 年度調査と同様に、中小企業庁[5]の定義を参考に総従業員数 301 名以上を大企業、300 名以下を中小企業とした。調査票の発送数は、2017 年度調査の送付実績と回収実績を参考に、目標とする 300 件の有効標本を得るため、4,091 社とした。

5　中小企業庁　中小企業・小規模企業者の定義
http://www.chusho.meti.go.jp/soshiki/teigi.html

図表 1-8 アンケート調査の対象企業及び調査票発送数（委託元調査）

分類	日本標準産業分類における業種分類 (業種コード)	調査票発送数		
		大企業	中小企業	計
委託元	製造業（E）	1,082	899	1,981
	卸売業・小売業（I）	514	595	1,109
	サービス業 不動産業，物品賃貸業(K) 学術研究，専門・技術サービス業(L) 宿泊業，飲食サービス業(M) 生活関連サービス業，娯楽業(N) 複合サービス事業(Q) サービス業（他に分類されないもの）(R)	419	582	1,001
計		2,015	2,076	4,091

② 委託先

委託先については、**図表 1-9** のとおり、情報通信業を中心としたが、製造業の一部でもソフトウェア開発等を行っている可能性があるため、民生用電気機械器具製造業等の製造業の業種を調査対象に含めた。また、企業規模の定義は、2017 年度調査と同様に、中小企業庁の定義を参考に総従業員数 101 名以上を大企業、100 名以下を中小企業とした。調査票の発送数は 2017 年度調査の送付実績と回収実績を参考に、目標とする 300 件の有効標本を得るため、3,661 社とした。

図表 1-9 アンケート調査の対象企業及び調査票発送数（委託先調査）

分類	日本標準産業分類における業種分類 (業種コード)	調査票発送数		
		大企業	中小企業	計
委託先	情報通信業（G） ソフトウェア業 情報処理サービス業 情報提供サービス業 その他の情報サービス業 国内・国際電気通信業 電気通信に附帯するサービス業 製造業（E） 民生用電気機械器具製造業 電子計算機・同付属装置製造業 工業計器製造業 発電機・電動機・その他の回転電気機械製造業	788	2,873	3,661

（3）調査方法

アンケート調査は、調査対象企業に対し、郵送で調査票を送付する郵送調査法を用いた。回答方法については、郵送による調査票の返送と調査専用 Web サイトによる回答を併用した。調査は 2018 年 11 月から 2019 年 2 月にかけて実施した。

（4）調査票の構成

アンケート調査の調査票は、**図表 1-10** のとおり、3 部構成とした。大項目Ⅰ・Ⅱでは、組織としての責任範囲の明確化の状況を調査した。大項目Ⅲでは、2017 年度以降に実際に業務を委託（委託元の場合）、受託（委託先の場合）した具体的な事例における、責任範囲の明確化の状況を調査した。なお、大項目Ⅲの事例のプロフィールに関する調査項目については、1.3.3 (8) で詳述する。また、調査票は、**付録 2-1（委託元調査）**、**2-2（委託先調査）**に示す。

図表1-10 アンケート調査の調査票の構成

大項目		調査項目
Ⅰ	回答企業・回答者属性	業種、企業規模、回答者の所属等
Ⅱ	IT業務委託の状況	取引数、再委託有無、委託する業務内容等
Ⅲ	IT業務委託の事例における責任範囲の明確化の状況	・事例のプロフィール （当該事例に含まれるITシステム・サービスの種類等） ・委託先の属性 ・契約に使用した文書 ・契約関連文書に記載のあるセキュリティ要求事項

（5）調査対象とする情報セキュリティ要求事項

アンケート調査では、責任範囲の明確化の状況について、次の**図表 1-11** に示す情報セキュリティ要求事項について調査を行った。これは、2017 年度調査の報告書における「表 3.3-6 委託契約に含める項目の例」を参考としたものである。

図表1-11 調査対象とする情報セキュリティ要求事項

項目	内容
秘密保持	委託する業務で扱う秘密情報の扱いを規定する。IPA は「中小企業の情報セキュリティ対策ガイドライン[6]」で、委託契約時の機密保持契約条項のサンプルを提供している。
証跡の提示、監査協力等	情報セキュリティ対策の実施状況の確認方法やそのタイミングについて規定することで、委託先の協力を得ることができる。
情報セキュリティに関する契約内容に違反した場合の措置	損害賠償等についてその要件を規定する。
インシデントが発生した場合の対応	インシデントが発生した際の報告先、報告内容、初動、調査、復旧等の各対応の実施主体、実施方法について規定する。
可用性（稼働率の水準、目標復旧時間等）	クラウドサービス等においては、委託元と委託先間でのサービス内容・範囲・品質等を保証する SLA（Service Level Agreement）に基づくサービス提供が一般的であり、情報セキュリティに関する項目も SLA に含まれている。
新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応	契約時点で想定していない新たな脅威等が顕在化した際に、委託元と委託先の間の情報共有、対応方針決定のスキームについて規定する。
再委託の禁止または制限	再委託の禁止、制限について定める。再委託を認める場合には再委託の実施に必要な手続（事前報告／承認等）委託先から再委託先に示す情報セキュリティ要求事項及びその確認方法等について規定する。
契約終了後の情報資産の扱い（返却、消去、廃棄等）	契約終了後の情報資産の扱い、及びその確認方法について規定する。
組織的な情報セキュリティ対策の実施	委託する業務で実施すべき組織的な情報セキュリティ対策を示す。契約に付随する他の文書で詳細化する形や基準、ガイドライン及び規格等への準拠を求める形もある。

[6] 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第 3.0 版」（2019 年）
付録 5：情報セキュリティ関連規程（サンプル）9-1 業務委託契約に係る機密保持条項
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

(6) 調査対象とする契約関連文書

アンケート調査では、次の**図表 1-12** に示す契約関連文書について、責任範囲の明確化の状況を調査した。これらの文書以外にも SLA 等、業務委託契約に使用される文書は多数あるが、使用頻度が高い文書に絞って調査を行った。

図表1-12 調査対象とする契約関連文書

文書名	内容
約款	不特定多数の利用者との契約を処理するため、あらかじめ定型的に定められた契約条項。クラウドサービス等では約款を使用して契約を結ぶことがある。
提案書	委託元がRFP（Request for proposal）を提示する等して、委託先に提案を求める場合に、委託先から提出される業務提案をまとめた文書。自社の優位性を示すために、実施するセキュリティ対策等と委託先の責任範囲が記載されることがある。
仕様書	主に委託元が作成する業務の仕様をまとめた文書。実施するセキュリティ対策等と委託先の責任範囲が記載されることがある。
見積書	委託先が委託元に提出するIT業務委託の契約に係る費用の見積書。セキュリティ対策はコスト項目であるため、見積りの前提条件として免責事項等が記載されることがある。
契約書	本調査では業務委託契約書を指す。自組織の業務を第三者に委託する際に、業務内容やその条件を書面に記載して合意するための文書。委託する業務で実施すべきセキュリティ対策等と、その作業の役割分担や損害賠償責任が発生した場合の責任分担が記載されることがある。
覚書	前項の契約書に定めのない事項等について別途定めるための文書。契約締結前の機密情報の取り扱い等の当事者間の合意のために使用されることがある。

(7) 責任範囲の明確化の状況に関する調査方法

具体的な IT 業務委託の事例における責任範囲の明確化の状況については、調査対象の情報セキュリティ要求事項（**図表 1-11**）が、調査対象の契約関連文書（**図表 1-12**）において、どのように記載されていたかを、次の 4 つの選択肢から選ぶ方法で調査した。

ⅰ. 当該文書は使用していない
ⅱ. 当該文書は使用しているが、当該項目は要求事項となっていないので、項目そのものの記載がない
ⅲ. 当該項目の記載があるが、委託先が責任を負うべき範囲が明示されていない（「都度調整」等）
ⅳ. 当該項目について、委託先が責任を負うべき範囲が明示されている

（8）IT 業務委託の事例のプロフィールに関する調査項目

IT 業務委託の事例については、次の**図表 1-13** の項目について調査した。なお、より多くの標本を収集するため、請負や準委任といった契約形態は問わないこととした。

図表 1-13 IT 業務委託の事例に関する調査項目

調査項目	調査対象	
	委託元	委託先
事例に含まれる IT システム・サービスの種類	○	○
委託された開発工程（ソフトウェア開発が含まれる場合）		○
IT システム・サービスの障害発生時の社会的影響度	○	○
IT システム・サービスのネットワークの範囲	○	○
IT システム・サービスで扱う情報資産	○	○
IT システム・サービスで扱う情報資産に個人情報が含まれる場合のデータ件数	○	○
契約の際に懸念した情報セキュリティ上のリスク	○	○
委託先の選定方法	○	
再委託先、再々委託先等の有無	○	
委託元の業種		○
委託元の企業規模（総従業員数）		○
委託元と委託先の資本関係	○	○
IT サプライチェーンにおける位置付け		○
使用した契約書の書式	○	○

1.3.4 事例調査

（1）事例調査の概要

事例調査では、**図表 1-14** の整理軸に沿って、責任範囲の明確化の状況等について、文献調査およびヒアリング調査により、情報を収集、分析した。

図表1-14 事例調査の整理軸

分類	内容
責任範囲にまつわるトラブル事例	責任範囲が曖昧であることが要因で訴訟となった事例、訴訟には至らなかったが納期や品質に影響した事例、委託元あるいは委託先が責任を押し付けられた事例等
責任範囲が曖昧な事例	責任範囲が曖昧な事例、責任範囲を明確にできない事例、その理由や曖昧であることのリスク認識等
責任範囲が明確な事例	責任範囲を明確にしている具体的な内容やその合意形成の方法等
責任範囲を明確にするための対策	責任範囲を明確にするための対策、参考となる情報等

（2）文献調査

文献調査では**図表 1-14** の内容を含む事例について記載された書籍、論文、記事、技術資料等を調査した。また、調査対象とする事例は 2013 年度以降に発表されたものとした。なお、調査対象とした文献は、次の**図表 1-15** の整理軸に基づいて、**付録 1 文献調査 調査結果一覧** として一覧表に整理した。本報告書中に示す文献 No はこの一覧表に示す文献 No である。

図表1-15 文献調査の整理軸

項目名	内容
文献No	文献の識別番号
書誌名（記事名）	文献の書誌名（記事名）
分類	文献の分類（書籍、論文、記事、技術資料のいずれか）
著者名	文献の著者名
発行所	文献の発行所
発行年月日	文献の発行年月日（西暦表示）
事例の内容	事例の概略　※分類「責任範囲を明確にするための対策」で契約書の雛形が収録されている場合には雛形の名称を記載。

（3）ヒアリング調査

ヒアリング調査では、委託元・委託先のセキュリティ担当者や法務担当者を対象に、当該企業における責任範囲の明確化の状況についてヒアリングを行った。また、セキュリティや契約関連実務に関する有識者を対象に、国内外における責任範囲の明確化の状況等についてヒアリングを行った。ヒアリングを行った対象者の本報告書内での表記及びプロフィールは、次の**図表 1-16** のとおりである。

なお、委託先においても、再委託する際の委託元としてのコメントがあったため、本報告書では、得られた事例について、委託業務および受託業務に関する事例としてヒアリング結果を整理した。

図表 1-16 ヒアリング調査の対象者

報告書内の表記	ヒアリング対象者のプロフィール
A 社	委託元（製造業・大企業）の情報システム部門責任者
B 社	委託元（製造業・大企業）の情報システム部門責任者
C 社	委託元（サービス業・大企業）のリスクマネジメント部門責任者
D 社	委託元（金融業・大企業）の情報システム部門情報セキュリティ責任者
E 社	委託先（国内 IT 企業・大企業）の品質管理部門責任者及び管理部門法務責任者
F 社	委託先（国内 IT 企業・大企業）の調達部門担当者
G 社	委託先（国内 IT 企業・大企業）の営業担当者
H 社	委託先（IT コンサルタンティング企業）のコンサルタント
I 社	委託先（セキュリティコンサルティング企業）のコンサルタント
J 氏	弁護士

２．責任範囲の明確化の状況（事例調査）

2.1 事例調査の概要

事例調査の調査結果は、次の**図表 2-1** の分類のとおりに整理し、文献調査の結果、ヒアリング調査の結果の順に紹介する。文献から文章を引用する場合については、枠で囲み、**付録 1 文献調査調査結果一覧** の文献 No と文献名を明記した。

図表2-1 調査結果一覧

分類	本書の記載箇所	
	文献調査	ヒアリング調査
責任範囲にまつわるトラブル事例	2.2.1	2.2.2
責任範囲が曖昧な事例	2.3.1 2.3.2	2.3.3
責任範囲が明確な事例	2.4.1	2.4.2
責任範囲を明確にするための対策	2.5.1	2.5.2

2.2 責任範囲にまつわるトラブル事例

2.2.1 文献調査の結果（国内の文献）

(1) トラブル事例１：SQL インジェクション攻撃による情報漏えい事件

この事例は、2017 年度調査の報告書でも紹介しており、非常に多くの文献に取り上げられている紛争事例である。法律的な観点で詳しく解説されている法律雑誌「NBL」の記事を紹介する。

> 情報システムにセキュリティ対策の脆弱性があったために、サイバー攻撃により情報流出が生じたケースでは、情報システムの構築を受託した IT ベンダーのサイバー攻撃により情報流出の被害を受けたユーザー企業に対する法的責任が問題となる。具体的には、セキュリティ対策の脆弱性が債務不履行に当たるのか、債務不履行に当たるとして IT ベンダーの負う損害責任の範囲などが問題となる。
>
> 東京地判平成 26・1・23 判時 2221 号 71 頁は、X 社（ユーザー企業）が Y 社（IT ベンダー）との間で、X のウェブサイトにおける商品の受注システムの設計、保守等の委託契約を締結したところ、Y が開発したソフトウェアにセキュリティ対策の脆弱性があったことにより、ウェブサイトで商品の注文をした顧客のクレジットカード情報が流出し、X は顧客対応等が必要となったために損害を被ったと主張して、Y に対し、委託契約の債務不履行に基づき損害賠償を求めた事案である。
>
> この事案には、①どのような事実があれば情報流失の原因がソフトウェアのセキュリティ対策の脆弱性であると判断することができるか、②IT ベンダーは契約上の債務としてどのようなセキュリティ対策を負う義務があるのか、③IT ベンダーに重過失がある場合に損害賠償責任を制限する規定が適用されるか、④重過失が認められるかなど、実務上興味深い問題が多数含まれている。
>
> （出典）文献 No.5「ソフトウェアのセキュリティ対策の脆弱性により情報流出が生じた事件の判決の実務的検討（論説）（東京地裁平成 26 年 1 月 23 日）」（NBL　No.1055）

この紛争事例の原告 X はインテリア商材の卸小売、通信販売を行う株式会社であり、被告 Y は IT ベンダで、情報処理システムの開発、保守、ネットショップの運営等を行う株式会社であった。この事例では、最も可能性が高い流失原因は SQL インジェクション攻撃であると認定され、「契約書にはセキュリティ対策の具体的内容が規定されていなかったため、IT ベンダがその不正アクセスを防ぐことのできるセキュリティ対策を講じる債務を負っていたか」と「本件システムにカード情報を保存する場合には暗号すべき債務を Y が負っていたか」が争点となった。

この事例の東京地裁判決は、Y に重過失が認められるとして、契約の責任制限規定の適用を否定しながらも、X にもクレジットカード情報の暗号化を怠った責任があるとして、X と Y それぞれの責任の割合を 3 対 7 と判断している。

(2) トラブル事例２：Struts の脆弱性が狙われた情報漏えい事件

この事例は、文献 No.12「日経コンピュータ」（2017 年 4 月 13 日号）に紹介されている事例である。小売業の Z 社が、同社のオンラインショップのシステムに使用されていたミドルウェア「Apache Struts2」（以下「Struts」とする。）の脆弱性を利用されて 4 年間の間に 2 度もシステムに不正に侵入された事案で、1 度目には約 12,000 件のクレジットカード情報が流出した。当該システムに使用されていた Struts が、当時既に脆弱性が指摘されていた古いバージョンのものであったことが原因だった。

Z 社が公開した最終報告書では「ベンダは、すでに脆弱性が指摘されていた Struts の古いバージョンを使用したまま、当社オンラインショップシステムの改修作業を完了しており、本来、システム開発会社として善良なる管理者の義務に基づき瑕疵のないシステム構成を設計すべき義務があるところ、それを看過してシステム構成の設計を行っていた点で責任があると指摘されております。」と、同社が設置した調査委員会の見解を掲載している。

同時に、同報告書では、「当社は、オンラインショップに関するシステムの構築および保守サポート業務をシステム開発業者（「ベンダ」）に対して一括委託をしておりましたが、結果的に後述のとおりベンダにおける情報セキュリティ管理体制の不備が発生していることから、ベンダ選定時の調査・分析、システムの保守サポート業務品質の管理義務が充分になされていなかったという不備が認められると指摘されております。」と、調査委員会の指摘を掲載し、委託元の責任についても認めている。

2.2.2 ヒアリング調査の結果

(1) 契約に関するトラブル事例

以下の**図表 2-2** に示す事例が得られた。

図表 2-2 ヒアリング調査の結果（責任範囲にまつわるトラブル事例）

ヒアリング対象者	ヒアリング内容
F 社：委託先 （国内 IT 企業・大企業）	・システム運用の受託業務で、契約期間中に顧客のシステムがサイバー攻撃を受けた。契約でサイバー攻撃等インシデントが発生した対応方法を明確に取り決めていなかったため、緊急に協議して対応をとらなければならなかった。

2.3 責任範囲が曖昧な事例

2.3.1 文献調査の結果（国内の文献）

(1) ソフトウェア開発に関する事例

ソフトウェアの開発の場合、契約締結時にソフトウェアの詳細な仕様が確定していることは稀であり、更に情報セキュリティ対策の詳細は、契約期間中にソフトウェアの仕様を明確にした上で、その仕様に見合った内容を協議しなくてはならない。また、その情報セキュリティ対策における役割分担や、情報セキュリティ対策が適切に実施されなかった場合に発生した損害の賠償責任については、委託元と委託先の間で協議し、合意した内容を仕様書や覚書等の契約関連文書に記載しなければならない。

法律雑誌「NBL」が企画した IT システム・サービスの契約に関わる企業法務担当者による座談会の記事には、ソフトウェア開発の契約関連文書に関して以下の記載があった。提案書の内容が、当該業務の契約書に明確に参照されていないことが指摘されている。

Ｆ（企業法務担当者） よく提案書の後ろのほうで、体制図の次あたりにいわゆる「星取表」(役割分担表と記載されることもある。) が書いてありますね。ユーザ、ベンダのどちらがどの業務を分担するかが丸や二重丸で記されている。

影島（司会：弁護士） その星取表が、契約書から明確にリファーされていないケースが多いように思います。契約の本文にタイトルが「第〇条（プロジェクトマネジメント義務)」と明記された条文があり、極端に言えば条項中に「提案書第〇章［星取表］に従って、それぞれ役割を果たす」とあるとすると、星取表の内容が契約上の義務であるということを裁判官も重視してくれると思います。ですが、多くのプロジェクトではそうではなくて、パワーポイントの形式で、提案書の後ろのほうに星取表があって、当事者の役割分担が書いてあるだけです。

（出典）文献 No.20「システム開発取引はなぜ紛争が絶えないのか（分析編）（座談会)」（NBL　No.1116）

司会：牛島総合法律事務所／影島広泰弁護士

Ｆ：企業法務担当者（ベンダ側法務経験者）

（2）約款や利用規約等で免責事項が明示されている事例

クラウド等のサービス提供型の業務の場合、責任範囲は、その約款や利用規約等に示されている条件をベースに交渉することになる。この場合、サービスを提供する側の委託先が、自らに有利な形で免責事項を定めることが容易であり、委託元が委託先に責任範囲の見直しを要求するのは難しい。委託元は、サービスを利用することのリスクを十分確認した上で、契約内容を検討する必要がある。

文献 No.31「初めての人のための英文・和文 IT 契約の実務」の中には、そのような業務の例として、「AI プログラムから発生した損害の責任」に関する記述がある。海外企業との契約交渉の難しさもあり、責任範囲を確認する際の課題と考えられる。

> データやプログラムの提供者が米国の大手 IT 企業になると、契約交渉のパワーをどちらが持つかによって、データやプログラムの提供者と相手方との間のサービス契約がどのようになるかが影響を受けることになります。請負など業務委託契約ではなく、ライセンス、（クラウド利用権のような）アクセス権の形態は、基本的には、現状有姿（つまり無保証）で損害賠償責任も負わないとする場合が多くなっています。
>
> そうなると結局は、交渉力を持たないと顧客がすべての損害を負担することにもなりかねないのです。
>
> （出典）文献 No.31「初めての人のための英文・和文 IT 契約の実務」

2.3.2 文献調査の結果（海外の文献）

（1）契約交渉に関する事例

ソフトウェア開発に関しては、日本では、IT ベンダ企業への委託開発が主流だが、米国では、ユーザ企業が自社内で開発する内製が主流であると言われている[7]。しかしながら、IT システム・サービスの多様化に伴い、保守・サポートやクラウド等のサービス利用に関しては、ユーザ企業が IT ベンダ企業とアウトソーシングの契約を結ぶケースも多いようだ。

米国の「Cross Talk 」に掲載されている C. Warren Axelrod 博士の論文「Using Contracts to Reduce Cybersecurity Risks」の「The Importance of Contracts」の節に、米国における IT 業務委託の契約の現状についての記述がみられた。この内容から、米国でも IT ベンダ企業がユーザ企業に対して“take-it-or-leave-it contracts”（契約を結ぶか結ばないかの二者択一で交渉の余地がない契約）を要求することがあることが分かる。

[7] 英繁雄著「揉め事なしのソフトウェア開発契約」日経 BP 社（2017 年 10 月）

Those who negotiate and enforce computer contracts are familiar with the all-too-common vendor statement: “We’ll put this contract in a drawer (or file folder) and never reference it again.” Of course, this is often the case. When contractual terms need to be invoked, however, that statement often indicates an adversarial situation. This is also a ploy to make customers feel more comfortable with boilerplate vendor agreements and not push as vigorously as they might otherwise for stiffer contractual terms and conditions.

However, not standing up for certain contract provisions that are important to your organization is a mistake. This approach is commonly used with take-it-or-leave-it contracts, where vendors are not willing to negotiate at all. The above sentence may be accompanied by this reassurance: “Well, our major customers have already agreed to this.” Such assertions may not necessarily be true and should be verified if possible.

(要約)

コンピュータに関する契約の交渉および締結では、ベンダから「この契約書は引き出しにしまっておいて二度と見ないでいいですよ。」といった、ありがちな発言を聞くことは珍しくない。しかしながら、これは、訴訟などで当事者が対峙したときに引き合いに出される発言でもある。このような発言は、より厳しい条項や条件の契約を結ぶよりも、定型的な文言のベンダの契約書で顧客を満足させようとするベンダの作戦である。

しかしながら、あなたの組織にとって重要な契約書の条項を、確かめようとしないのは誤りである。このような交渉方法は「契約を結ぶか結ばないかの二者択一で交渉の余地がない契約」に使用され、ベンダは少しも交渉をする気がないのだ。上述のような発言は、「ええ、我々の主要な顧客はこの契約書で合意していますよ。」といった顧客を安心させるための言葉を伴うことが多い。このような主張は、必ずしも事実ではないかもしれないので、可能であれば検証すべきものである。

（出典）文献 No.13「Using Contracts to Reduce Cybersecurity Risks」
（Cross Talk　July/August 2017）

2.3.3 ヒアリング調査の結果

(1) 委託先管理に関する事例

責任範囲を明確にできない事例として、以下の**図表 2-3** に示す事例が得られた。

図表 2-3 ヒアリング調査の結果（責任範囲を明確にできない事例・委託先管理）

ヒアリング対象者	ヒアリング内容
B 社：委託元 （製造業・大企業）	・クラウド（SaaS）の場合は、アプリケーションの不具合について運用ベンダに不具合の状況を確認しても、利用者と同じ現象の確認までしかできない。
D 社：委託元 （金融業・大企業）	・委託先の従事者の不正対策が難しい。

(2) サービス提供業務において約款・利用規約に免責事項が明記されている事例

クラウドサービス等のサービス提供型の業務の場合、約款・利用規約に情報セキュリティに関する免責事項が明記されている場合がある。IT システム開発等でそのようなサービスを利用する場合、免責事項が決められている部分については、委託元と委託先の間で責任範囲の交渉ができず、結果として、責任範囲の取り決めに曖昧さが残ることになる。そのような責任範囲を明確にできない事例として、以下の**図表 2-4** に示す事例が得られた。

図表 2-4 ヒアリング調査の結果（責任範囲を明確にできない事例・約款等における免責事項）

ヒアリング対象者	ヒアリング内容
B 社：委託元 （製造業・大企業）	・外資系クラウドベンダとの契約の場合、その多くで外資系ベンダの契約書でないと契約できない。
H 社：委託先 （IT コンサルティング企業）	・クラウドサービスの場合には、オーダーメイド型の役務に対する委託業務契約ではなく、基本的にレディメイド型のサービス提供型の契約である。このような契約形態の場合、契約後に合意形成を諮るような日本的な商慣習は通用せず、約款を前提とした契約リスクの検討を行う必要がある。 ・クラウドサービスを提供する事業者の約款に付帯条件をオンしたいのであれば、サービス利用者側の責任で付帯条件を用意し、追加料金や免責事項、範囲等について、契約前に交渉を重ねなければならない。

（3）受託業務の契約に関する事例

責任範囲を明確にできない事例として、以下の**図表 2-5** に示す事例が得られた。

図表 2-5 ヒアリング調査の結果（責任範囲を明確にできない事例・受託業務の契約）

ヒアリング対象者	ヒアリング内容
F 社：委託先 （国内 IT 企業・大企業）	・当社の契約書の雛形は、情報セキュリティに関して明確な要求がなく、「甲乙で協議する」といったような抽象的な表現となっている。課題を感じてはいるが、契約書の文言を変更するためには全ての関係先と当社との間で合意をとらねばならない。取引先の社数が多いので労力がかかり実行するのは難しい。 ・責任範囲を決めると言っても、何をどう線引きしていいかが分からない。実際にインシデントが発生してみないと分からないことが多い。例えば、保守業務の場合、受注者にどのような役割が求められるのか、必要な作業が何なのかは、平時には予測しづらい。 ・セキュリティにお金をかけることについて、費用対効果が定量的に判断しづらい。インシデントが発生する確率というのは常に変わっていくもので当てにならない。
G 社：委託先 （国内 IT 企業・大企業）	・官公庁の入札案件の場合、詳細な要件を確認できないことがある。 ・発注者の要件が曖昧な場合、リスクぶんのコストを予備費として見積りに上乗せしなければならない。要件が詳細なほうがコストダウンの提案がしやすい。

2.4 責任範囲が明確な事例

2.4.1 文献調査の結果（国内の文献）

（1）役割分担表に関する事例

法律雑誌「NBL」が企画した IT システム・サービスの契約に関わる法務担当者による座談会の記事に以下の記載があった。システム開発業務における委託元と委託先の責任範囲が役割分担表で明確にされている事例である。情報セキュリティに限った内容ではないが参考になる。

D（企業法務担当者）	あるベンダ会社と契約をしたときにそれに近い（役割分担表に関する）契約条項が入っていました。条項から「受託の確認書」という星取表と同様の記載へリファーされ、紐づけられていました。明確に「プロジェクトマネジメント義務」とは書いていませんでしたが、ユーザとしては、仮にベンダがそれどおりにやっていない場合、義務違反を主張する根拠になりますね。
影島（司会：弁護士）	そのような実例があるのなら、発注者（ユーザ側）もそこは契約チェックの段階できちんと確認しないといけませんね。契約書と一体となった付属文書という建付けになるのでしょうから。

（出典）文献 No.20「システム開発取引はなぜ紛争が絶えないのか（分析編）（座談会）」（NBL　No.1116）

司会：牛島総合法律事務所／影島広泰弁護士

D：企業法務担当者（ユーザ側法務経験者）

2.4.2 ヒアリング調査の結果

（1）委託先管理に関する事例

責任範囲を明確にしている事例として、以下の**図表 2-6** に示す事例が得られた。

図表 2-6 ヒアリング調査の結果（責任範囲を明確にしている事例・委託先管理）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・委託先はオフショアを含め、半年に一回、監査（セキュリティチェック）を実施している。委託先の環境（執務環境、ネットワーク、ウィルス対策等）や定期的な情報セキュリティ教育等については、別途委託先チェックシートがあり、基準値がある。
C 社：委託元 （サービス業・大企業）	・契約時に委託先にセキュリティチェックシートを渡し、チェック項目ごとに委託先が実施している内容を記載してもらう。 ・機密性の高い情報を扱う場合は、再委託先や再々委託先までセキュリティ監査を実施する。
E 社：委託先 （国内 IT 企業・大企業）	・委託先には契約時にセキュリティに関するチェックシート（アンケート）に回答していただく。また、機密保持に関する誓約書を委託先の代表者と従事者に提出していただく。
G 社：委託先 （国内 IT 企業・大企業）	・委託先には年 1 回のセキュリティ監査を実施している。現地立入監査とセキュリティチェックシートによる監査を併用している。

（2）委託業務の契約に関する事例

責任範囲を明確にしている事例として、以下の**図表 2-7** に示す事例が得られた。

図表 2-7 ヒアリング調査の結果（責任範囲を明確にしている事例・委託業務の契約）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・海外の大手 IT ベンダは自社の契約書でないと契約しない方針なので、その場合には先方から提示された定型の契約文言に合わせる必要がある。そのため、契約書に付帯条項をつけることを認めてもらう方法をとる。
B 社：委託元 （製造業・大企業）	・基本契約書、発注契約書、仕様書を使用して契約を結んでいる。具体的なセキュリティ要件は、契約書に記載するのではなく、非機能要件の一つとして仕様書に記載している。発注契約書には、委託先の責任範囲とそれに違反した場合にどこまで責任を負うかを記載している。 ・セキュリティ要件は案件のリスクを法務部が判断し、契約書に記載する。リスクの判断が難しい場合は、外部の弁護士に依頼して記載内容を検討する。
C 社：委託元 （サービス業・大企業）	・契約書の文面は「甲乙で協議する」としているが、協議内容は明文化し、委託先と共有している。テスト方法等を細かく指示することがある。
D 社：委託元 （金融業・大企業）	・外資系ベンダは企業間の基本契約は結びたがらず、サービスごとの約款系の契約となるが、その場合は、別途、覚書を交わして、当社の要求する情報セキュリティ要求を反映させる。 ・クラウドサービスを提供する事業者も、事前に情報セキュリティに関する組織体制等を評価した上で契約を結んでいる。 ・年次でシステムのプロフィールを評価し、アセスメントを行って、セキュリティ要件の検討と契約関連文書への記載内容の検討を並行して行う。
J 氏：弁護士	・担当した案件で、契約書に「賠償額は委託費用を上限」とするケースや、「損害賠償額の負担割は〇：〇」とするケースがあった。

（3）受託業務の契約に関する事例

責任範囲を明確にしている事例として、以下の**図表 2-8** に示す事例が得られた。

図表 2-8 ヒアリング調査の結果（責任範囲を明確にしている事例・受託業務の契約）

ヒアリング対象者	ヒアリング内容
E 社：委託先 （国内 IT 企業・大企業）	・ソフトウェア開発の場合、セキュリティ要件については、成果物に日付を入れて協議事項を明記する。例えば、最終納品の際には、納品書にセキュリティパッチのバージョンを記載する。また、上流工程の成果物（外部設計書）も、テスト段階でセキュリティ要件を変更することがあれば、その内容を更新して納品する。
G 社：委託先 （国内 IT 企業・大企業）	・契約書を作成するのは営業担当だが、管理部門のセキュリティ担当に内容の確認を依頼する。業務の内容によっては、セキュリティ担当から「このようにしたほうが良い」と損害賠償や瑕疵担保、データの保存期間等について記載内容を見直すよう助言がある。
I 社：委託先 （セキュリティコンサルティング企業）	・受託業務の契約で、契約書とは別にセキュリティに関するチェックリストがあり、チェック項目に回答して委託元に提出している。

2.5 責任範囲を明確にするための対策等

2.5.1　文献調査の結果（国内の文献）

任範囲を明確化するための方策の一つとして、契約書における記載内容の見直しがある。文献調査で得られた事例の中には、**付録 1 文献調査　調査結果一覧**に記載のとおり、責任範囲を明確にするために有用な、契約交渉の進め方、契約の条件を確認するためのチェックリスト、契約書の雛形や条項の例等があった。

雛形や条項の例には、守秘義務等の一般条項に関するものや、IT システム・サービスの内容ごとのものがあった。一例として、文献 No.16「業務委託契約の基本と書式」に収録されている「漏えい事案等が発生した場合」に関する条項の例を紹介する。

第 17 条（漏えい事案等が発生した場合）

1　甲は、特定個人情報を漏えい、滅失、毀損（以下「漏えい等」という。）することがないよう必要な措置を講ずるものとし、甲の支配が可能な範囲において特定個人情報の漏えい等に関し責任を負う。
2　甲及びその役員・従業員が、本契約に違反して、特定個人情報を本契約に定める業務目的外に利用した場合又は第三者に提供・開示・漏えい等した場には、甲は直ちに乙に報告しなければならない。この場合、甲は、速やかに必要な調査を行うとともに、再発防止策を策定するものとし、乙に対し調査結果及び再発防止策の内容を報告する。
3　特定個人情報の漏えい等に関し、乙の役職員を含む第三者から、訴訟上又は訴訟外において、乙に対する損害賠償請求等の申立てがされた場合、甲は当該申し立ての調査解決等につき乙に合理的な範囲で協力するものとする。
4　特定個人情報の漏えい等に関し、乙の役職員を含む第三者から、訴訟上又は訴訟外において、甲に対する苦情又は損害賠償請求等の申立てがされた場合、甲は、苦情又は申立てを受け、苦情又は申立てがされたことを認識した日から 3 営業日以内に乙に対し、苦情又は申立ての事実及び内容を書面で通知するものとする。
5　本条の定めは本契約終了後も有効とする。

（出典）文献 No.16「業務委託契約の基本と書式」『特定個人情報（マイナンバー）管理委託契約』

また、文献調査で対象としたビジネス法務に関する書籍の中には、契約書の建付け（構成）そのものに関する記述も多かった。IT システム・サービスの種類によって、取引の対象となるものが異なる。例えば、ソフトウェア開発の場合は、最終的な成果物はプログラムや設計書等であり、それが取引の対象となるが、システム運用・管理やハードウェア保守等は、サービス（役務）の提供そのものが取引の対象である。この点についての言及がある文献の一例として、文献 No.31「初めての人のための英文・和文 IT 契約の実務」の記載内容を紹介する。

IT 契約において、最も重要なことは、初期の段階における、契約書の建付け（構成）設計です。すなわち、ズバリ、①契約当事者とその役割、②取引構成（ビジネスモデル）の種類・法的性質、③契約の形態をスポットとするか継続的取引を前提とした基本契約にするか、についての建付け（構成）設計が最も重要といえます。

通常は、いずれかの当事者が用意する（サービス提供当事者が用意するケースが多い）ひな型契約書が提示されて、それをベースに契約条件の交渉が行われることが多いのですが、そのまま、そのひな型をベースに交渉が進められる場合には、最初にひな型が提示された段階で、当事者間の力関係の勝負が決まってしまうことが多いといえます。なぜかというと、そうしたひな型は、ひな型提示当事者に有利なビジネスモデルを前提に当事者間の権利義務が構築・規定されることが多いからです。

（出典）文献 No.31「初めての人のための英文・和文 IT 契約の実務」

2.5.2 ヒアリング調査の結果

責任範囲を明確にするための対策等の事例として、以下の**図表 2-9** に示す事例が得られた。

図表 2-9 ヒアリング調査の結果（責任範囲を明確にするための対策等）

ヒアリング対象者	ヒアリング内容
I 社：委託先 (セキュリティコンサルティング企業)	・セキュリティバイデザイン[8]は理想であるが、そのレベルまでいかなくとも、二要素認証やログ収集等でセキュリティレベルを高くする事ができる。すべてを満たす事を目指さず、優先順位を決めて対応していく事が重要であると考える。
J 氏：弁護士	・現在の日本の標準的な契約書は、委託業務の目的が 3 行程度しか書かれていないが、2017 年の民法改正施行（2020 年 4 月）後は、何のために使用するサービスなのかを明記しないと、例えば「個人情報を使用して〇〇するシステム」等と具体的に記載しないと、情報漏えい等の紛争時に、ベンダの契約不適合責任を追及する委託元の立場は弱くなる。これからは、仕様書を作成する委託元のほうで、より要件を明示しなければならなくなる。 ・契約書の雛形は汎用性があるものにした方がよい。ただ、一つの雛形をあらゆる業務に使おうとするのは難しいので、具体的な要件は仕様書、覚書等に記述し、契約書にはその文書を参照する内容を明記したほうがよい。

[8] 情報セキュリティを企画・設計段階から確保するための方策。

3. 責任範囲の明確化の状況（アンケート調査）

3.1 調査結果の概要

3.1.1 調査票の回収結果

委託元調査における業種別企業規模別の回収状況は、次の**図表 3-1** のとおりである。アンケート調査では、委託元調査については、製造業から 150 件以上（大企業 60 件以上、中小企業 90 件以上）、卸売業・小売業 90 件以上(大企業 40 件以上、中小企業 50 件以上)、サービス業 60 件以上（大企業 30 件以上、中小企業 30 件以上）の有効回答数を得ることを目標としており、結果としてその目標を超える有効回答を得ることができた。

図表 3-1 調査票の回収状況（委託元調査）

分類	業種分類		調査票回収数		
	大分類	中分類	大企業	中小企業	計
委託元	製造業(E)		**137**	**91**	**228**
		飲食料品	17	8	25
		建築材料，鉱物・金属材料	4	6	10
		印刷・印刷関連製品	2	15	17
		化学製品	22	13	35
		電気機械器具、情報通信機械器具	28	6	34
		輸送用機械器具	25	4	29
		その他の製造業	39	39	78
	卸売業・小売業(I)		**52**	**50**	**102**
		繊維・衣服	6	6	12
		飲食料品	10	11	21
		建築材料，鉱物・金属材料	7	4	11
		その他の卸売業・小売業	29	29	58
	サービス業		**47**	**35**	**82**
		不動産業，物品賃貸業(K)	5	2	7
		学術研究，専門・技術サービス業(L)	4	6	10
		宿泊業，飲食サービス業(M)	8	0	8
		生活関連サービス業，娯楽業(N)	2	4	6
		複合サービス事業(Q)	2	5	7
		サービス業（他に分類されないもの）(R)	26	18	44
	その他		**3**	**2**	**5**
計			**239**	**178**	**417**

※企業規模は総従業員数 301 名以上を大企業、300 名以下を中小企業とした。

※（ ）のアルファベットは日本標準産業分類の業種コードである。

委託先調査における業種別企業規模別の回収状況は、次の**図表 3-2** のとおりである。アンケート調査では、委託先調査については、大企業から 150 件以上、中小企業から 150 件以上の有効回答数を得ることを目標としており、結果としてその目標以上の有効回答を得ることができた。なお、委託元の回収企業（**図表 3-1**）と、委託先の回収企業（**図表 3-2**）に重複はない。

図表 3-2 調査票の回収状況（委託先調査）

分類	日本標準産業分類における業種分類(業種コード)	調査票回収数		
		大企業	中小企業	計
委託先	情報通信業（G） 製造業（E）	165	263	428

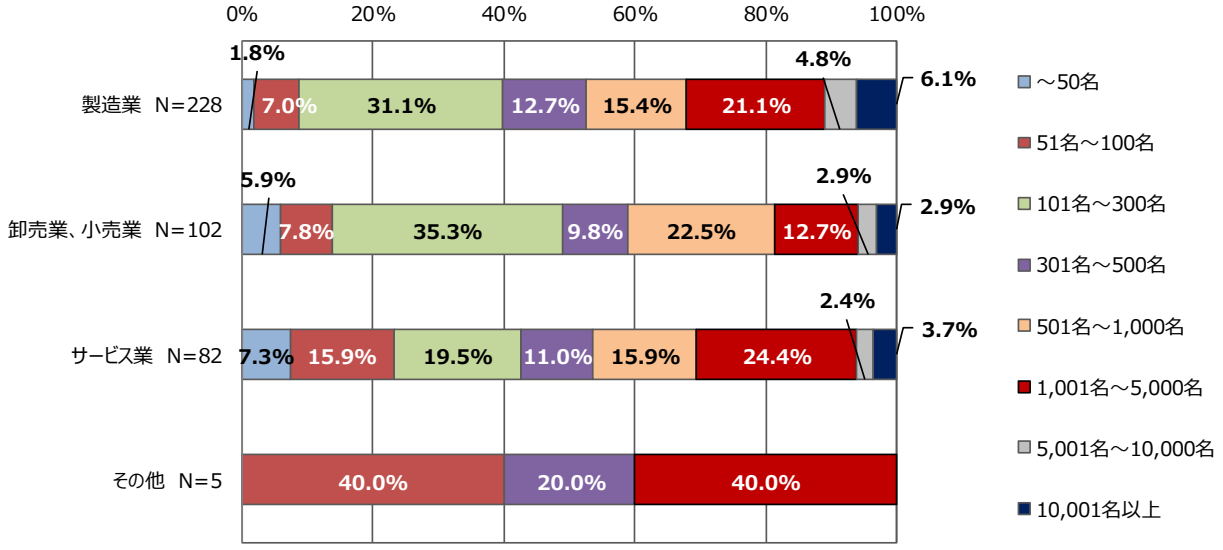
※企業規模は総従業員数 101 名以上を大企業、100 名以下を中小企業とした。

3.1.2 調査仮説の検証方法

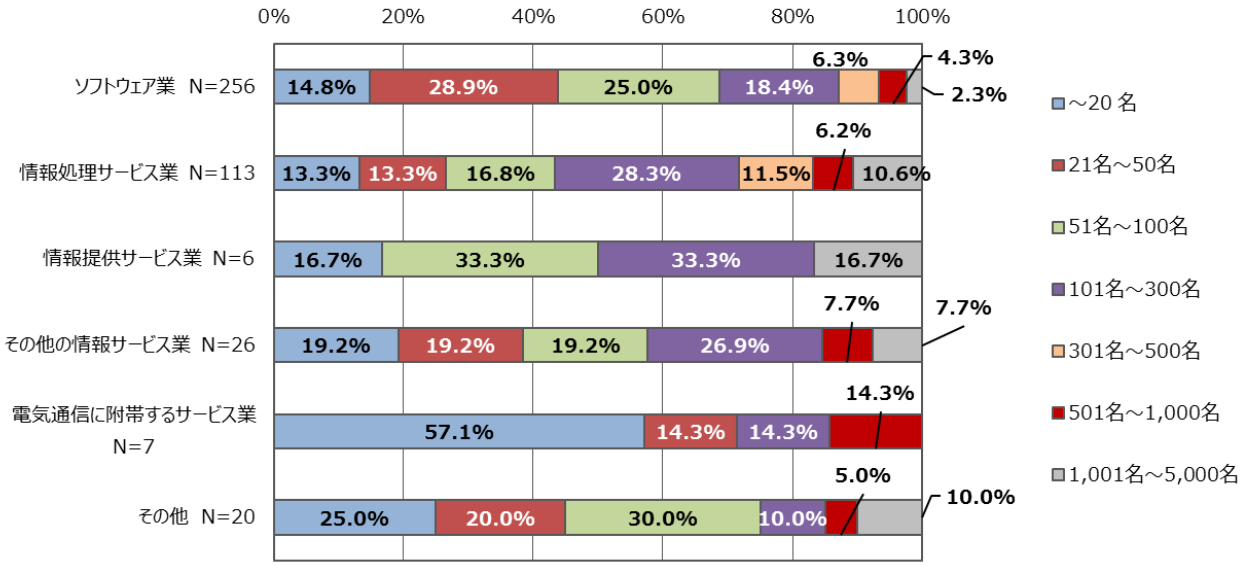
図表 1-6 の調査仮説の検証には、アンケート調査に加えて、事例調査におけるヒアリング調査でも、アンケート調査と同様の質問を行い、分析の材料とした。

3.1.3　回答企業のプロフィール

委託元調査、委託先調査の回答企業の業種と総従業員数は、次の**図表 3-3** と**図表 3-4** のとおりである。委託元調査においては、製造業の大企業からの回答が多く、委託先調査においては、ソフトウェア業の中小企業からの回答が多かった。



図表 3-3 委託元の業種と総従業員数　N=417



※国内・国際電気通信業 2 件、電気機械製造業 1 件はその他に含めた

図表 3-4 委託先の業種と総従業員数　N=428

3.2 契約書の雛形とその運用について

3.2.1　主たる事業と情報セキュリティ要求事項の含まれる契約書の雛形の有無

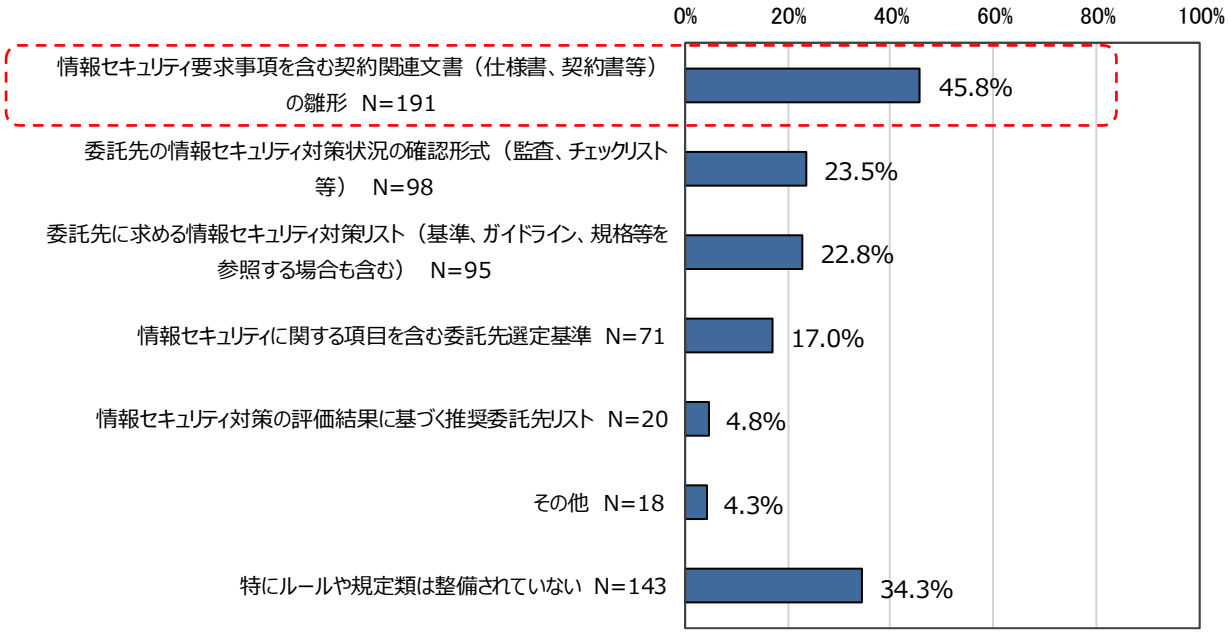
（1）設問の趣旨

委託元調査では、委託先管理において、どのような社内ルール・規定類を整備しているかを調査した。整備対象の社内ルール・規定類については複数の項目をあげ、その一つとして「情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形」を含めた。

また、業種による違いを詳細に比較するため、**図表 3-1** に示した中分類で分析を行った。

（2）調査結果

情報セキュリティに関する委託先管理に関し、整備している社内ルール・規定類を調査した結果、「情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形」を整備している組織は、**図表 3-5** に示すとおり、全体の 45.8%であり、社内ルール・規定類の中では最も多く整備され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委託先管理の社内ルール・規定類の整備状況（委託元調査）
N=417

また、ヒアリング調査でも、次の**図表 3-6** のとおり、記載される項目やその記載の詳細度に違いはあるが、全てのヒアリング調査対象企業で情報セキュリティ要求事項の含まれる契約書の雛形を用意していた。

図表 3-6 ヒアリング調査の結果（委託元調査・情報セキュリティ要求事項の含まれる契約書の雛形の有無）

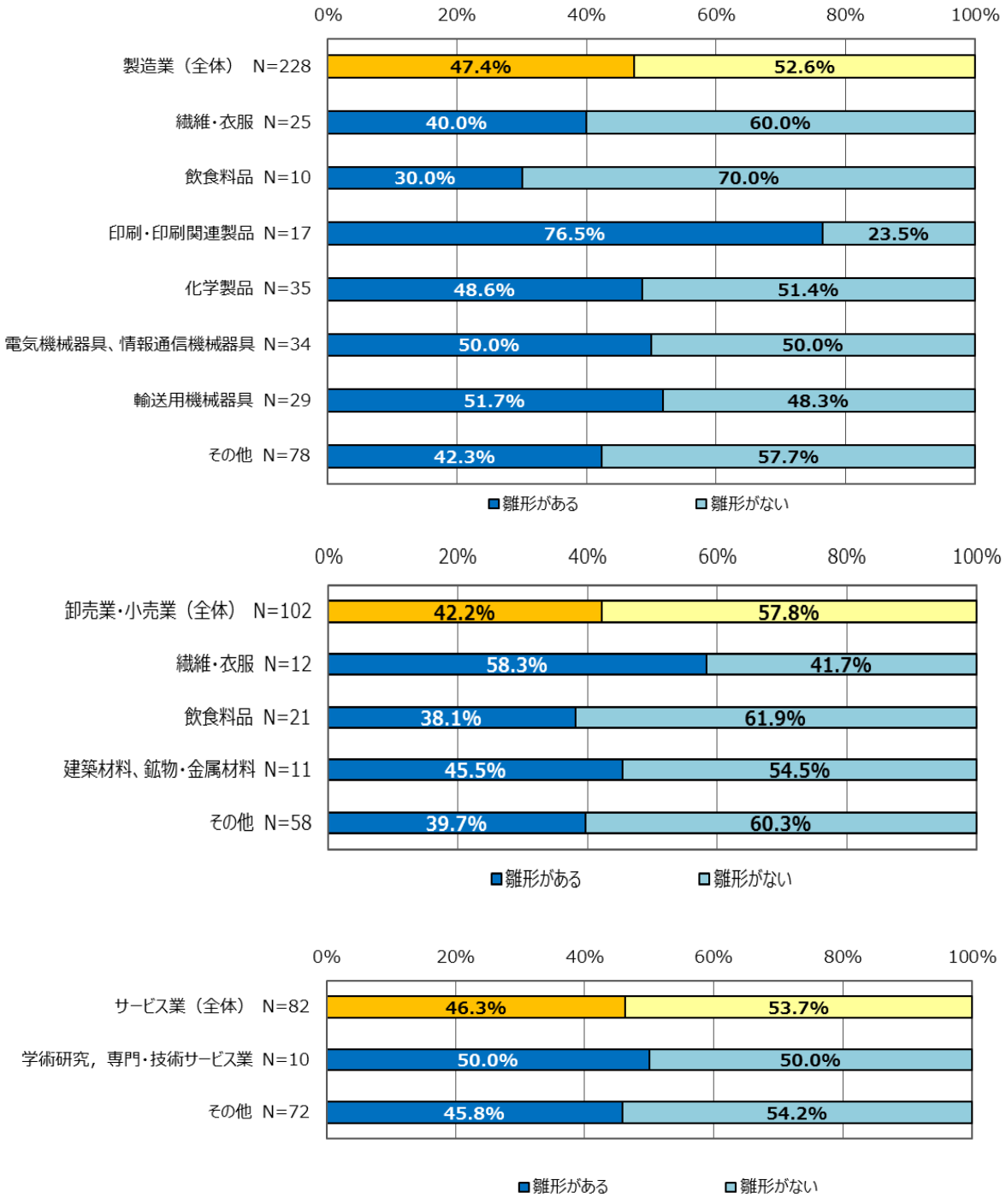
ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・基本契約書の雛形を用意している。情報システム開発の場合は、原則的に基本契約書締結の上、個別契約書を締結している。この個別契約書には、標準的に使用できるテンプレートはない。 ・基本契約書の雛形には、秘密保持や瑕疵担保責任、知的財産権等の条項が記載されている。個人情報を扱う場合には、「個人情報の取り扱いについての覚書」を別途締結する。
B 社：委託元 （製造業・大企業）	・契約書の雛形はあるが、個別のセキュリティ要件については、契約書には書かずに、非機能要件の一つとして仕様書に入れている。契約書についてはあくまでも責任範囲とそれに違反した場合にどこまで責任を負うかを記載している。
C 社：委託元 （サービス業・大企業）	・契約書の雛形があり、機密保持、再委託、監査に関する条項の記載がある。
D 社：委託元 （金融業・大企業）	・契約書の雛形があり、機密情報の管理に関する条項と情報資産の取り扱いに関する条項が記載されている。

また、業種による違いを詳細に比較するため、**図表 3-1** に示した業種（大分類、中分類）ごとに情報セキュリティ要求事項の含まれる契約書の雛形の有無を分析した。その結果を**図表 3-7** に示す。なお、大分類・中分類ともにサンプル数が 10 件以上のものを対象とし、中分類で 9 件以下の業種は「その他」とした。

図表 3-7 のとおり、印刷・印刷関連製品の製造業で、情報セキュリティ要求事項の含まれる契約書の雛形を用意している傾向が強かった。これは、ダイレクトメール等の印刷を請け負う際に個人情報を扱うことが多いことから、企業風土として情報セキュリティに関する意識が高いものと考えられる。

「石油化学製品の製造、加工及び売買」は、政府の指定する重要インフラサービス[9]の一つであることから、情報セキュリティ要求事項の含まれる契約書の雛形を用意しているのではないかと想定し、「委託元の主たる事業が化学製品の生産や販売である場合、情報セキュリティ要求事項の含まれる契約書の雛形を用意している。」とする調査仮説を立てた（**図表 1-6** 調査仮説 No.1）。アンケート調査で得られた結果では、「化学」を主たる事業とする製造業の企業のうち、情報セキュリティ要求事項の含まれる雛形があると回答したのは 48.6%と、他の事業と顕著な差はなく、調査仮説 No.1 を肯定する結果とはならなかった。

9 「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（2018 年 4 月改定）



図表 3-7 主たる事業と情報セキュリティ要求事項の含まれる契約書の雛形の有無（委託元調査）

3.2.2 IT システム・サービスの種類ごとの契約書の雛形の有無

（1）設問の趣旨

IT 業務委託で使用する契約書には、大きく分けて、業務形態やサービスの種類によらない、共通した要求事項を取り決めるための基本契約書と、契約形態やサービスの種類に対する固有の要求を具体的に取り決めるための個別契約書がある（**図表 3-8**）。

共通した要求事項のみの契約書の雛形よりも、サービスの種類に合わせた個別契約書の雛形を用意した方が、責任範囲についてより明確に合意できるのではないかという想定から、調査では、IT システム・サービス種類ごとの契約書の雛形の有無について調査した。これは、**図表 1-6** 調査仮説 No.2 の「委託先は、IT システム・サービスの種類ごとに情報セキュリティ要求事項の含まれる契約書の雛形を用意している。」に関する調査項目である。

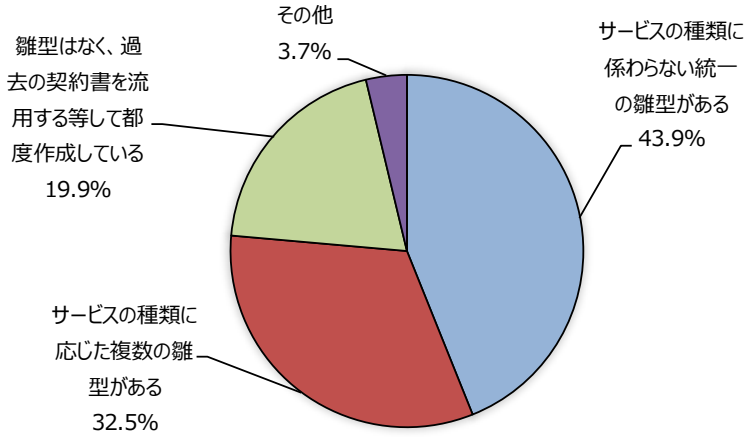
図表 3-8　契約書の雛形の種類（例）

契約書の種類	契約書の概要	内容
基本契約書	契約形態やサービスの種類によらない共通した要求	・秘密保持契約 ・個人情報の取り扱い ・安全管理 ・資産の管理 ・免責事項 ・瑕疵担保責任 ・参考とするガイドライン ・データライフサイクル 等
個別契約書	契約形態やサービスの種類ごとの具体的な要求 契約形態 ・請負 ・準委任（役務提供） サービスの種類 ・開発 ・保守・運用 ・データ処理・分析 ・サービス提供 ・インフラ提供	

（2）調査結果

次の**図表 3-9** のとおり、「サービスの種類に応じた複数の雛形がある」と回答したのは全体の 32.5%、「サービスの種類にかかわらない統一の雛形がある」と回答した企業は全体の 43.9%であった。合わせると、なんらかの情報セキュリティ要求事項が含まれた契約書の雛形を用意している企業は全体の 76.4%となり、委託先企業における情報セキュリティ要求事項の取り決めに対する意識は高い傾向にあると考えられる。

一方、雛形はなく過去の契約書を流用する等して都度作成している企業が 19.9%であった。流用した過去の契約書に、業務に必要な要件が記載されていれば問題ないが、いつも使っているという理由だけで流用している場合、要件の不足や曖昧な契約になっている恐れがある。



図表 3-9 IT システム・サービスの種類ごとの契約書の雛形の有無（委託先調査） N=428

また、**図表 3-10** のとおり、ヒアリング調査の対象とした委託先企業のうち 5 社中 3 社が事業内容別に契約書の雛形を複数用意していた。アンケート調査と同様、調査仮説 No.2「委託先は、IT システム・サービスの種類ごとに情報セキュリティ要求事項の含まれる契約書の雛形を用意している。」が肯定される結果であった。

図表 3-10 ヒアリング調査の結果（委託先調査・IT システム・サービスの種類ごとの契約書の雛形の有無）

ヒアリング対象者	ヒアリング内容
E 社：委託先 （国内 IT 企業・大企業）	・業務の内容によって複数の契約書の雛形がある。基本契約書の雛形には、施設内の安全及びセキュリティのガイドライン、資産管理、瑕疵担保責任等を記載している。
F 社：委託先 （国内 IT 企業・大企業）	・契約書の雛形は業務の内容によって複数あるが、情報セキュリティに関しては明確な要求はなく、「甲乙で協議する」といったような抽象的な表現となっている。
G 社：委託先 （国内 IT 企業・大企業）	・事業内容ごとに複数の契約書の雛形がある。データのライフサイクル管理や個人情報保護に関する条項等を入れている。

3.2.3　IT システム・サービスの種類ごとの情報セキュリティ要求事項の内容

（1）設問の趣旨

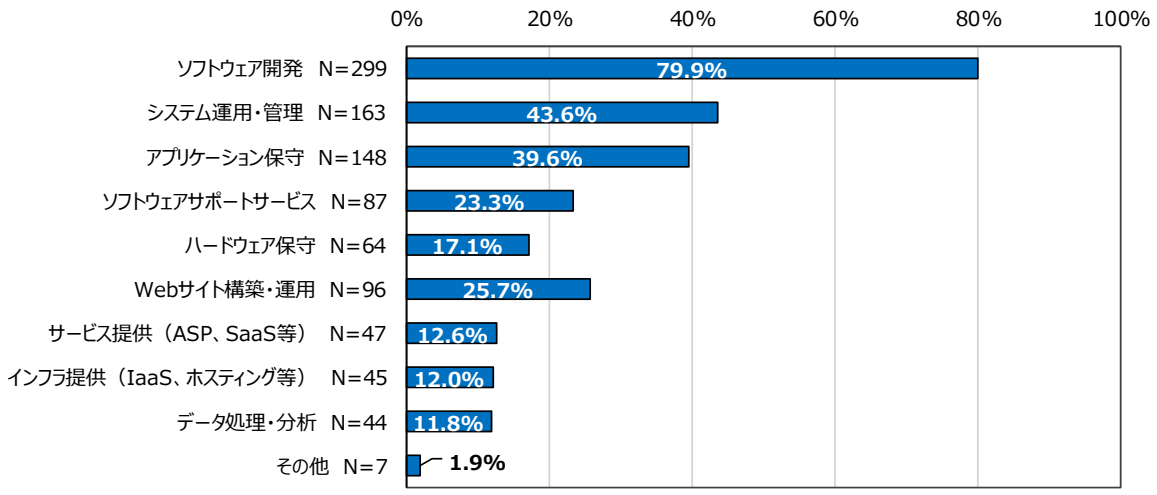
アンケート調査では、具体的な IT 業務委託の事例において、契約書や仕様書等の契約関連文書にどのような情報セキュリティ要求事項を記載していたかを調査した（1.3.3（5）～（8）参照）。これは、**図表 1-6** 調査仮説 No.3「委託先は、IT システム・サービスの種類ごとに情報セキュリティ要求事項の内容を変えている。」に関する調査項目である。

本項では、委託先調査において、調査対象の情報セキュリティ要求事項（**図表 1-11**）が要求の状況を、IT システム・サービスの種類ごと分析する。なお、調査対象の情報セキュリティ要求事項（**図表 1-11**）は 8 項目、調査対象の契約関連文書（**図表 1-12**）は 7 項目有り、組み合わせると 56 項目となるが、分析対象とする事例は、56 項目のいずれかについて、次の選択肢のうちから ii ～ iv の回答があるものとした。この条件で、委託先調査の事例 407 件のうち、分析対象は 374 件となった。

ⅰ. 当該文書は使用していない
ⅱ. 当該文書は使用しているが、当該項目は要求事項となっていないので、項目そのものの記載がない
ⅲ. 当該項目の記載があるが、委託先が責任を負うべき範囲が明示されていない（「都度調整」等）
ⅳ. 当該項目について、委託先が責任を負うべき範囲が明示されている

（2）調査結果

分析対象の事例 374 件における IT システム・サービスの種類（複数選択あり）は、次の**図表 3-11** のとおりである。最も件数が多いのは、ソフトウェア開発を含む事例で 299 件（79.9%）、最も件数が少ないのは、「その他」を除くと、データ処理・分析を含む事例で 44 件（11.8%）である。



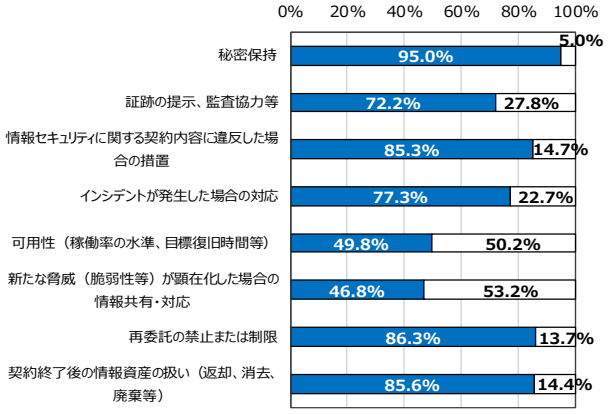
図表 3-11　IT システム・サービスの種類（委託先調査）　N=374

この 374 件の事例を対象に、IT システム・サービスの種類ごとに、情報セキュリティ要求事項の要求の状況を分析した結果は、次の**図表 3-12-1**、**図表 3-12-2** のとおりである。

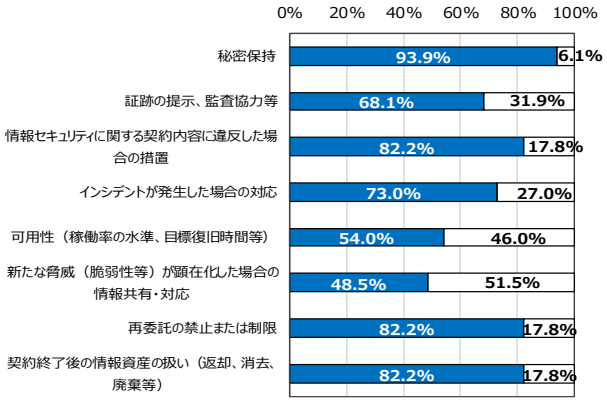
契約書の一般条項に入れられることの多い「秘密保持」は、IT システム・サービスの種類に係わらず、90%以上の比率で要求されている。「証跡の提示、監査協力等」「情報セキュリティに関する契約内容に違反した場合の措置」「インシデントが発生した場合の対応」は、ともにインフラ提供で要求される比率が最も高くなっており、それぞれ 80%以上である。また、「可用性（稼働率の水準、目標復旧時間等）」はハードウェア保守、サービス提供で要求される比率が高い（それぞれ 60%以上）。「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」が要求される比率が高いのは、ソフトウェアサポートサービス、ハードウェア保守、サービス提供、インフラ提供であり、それぞれ 53%前後である。「再委託の禁止または制限」と「契約終了後の情報資産の扱い（返却、消去、廃棄等）」はデータ処理・分析で要求されることが多く、ともに 90%前後となっている。

これらの調査結果から、調査仮説 No.3「委託先は、IT システム・サービスの種類ごとに情報セキュリティ要求事項の内容を変えている。」は、肯定される結果となった。

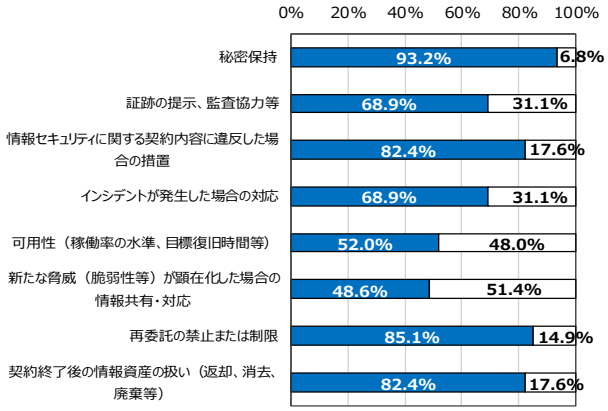
a.ソフトウェア開発を含む事例



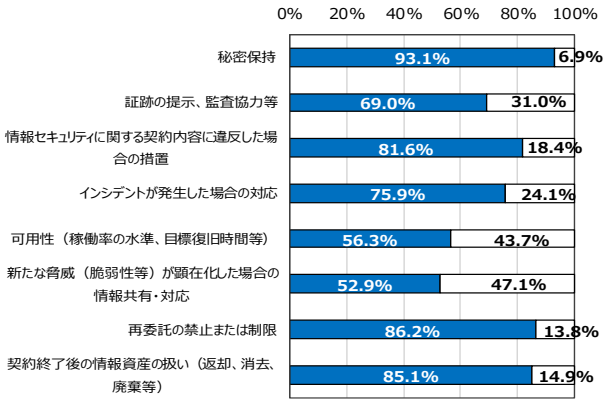
b.システム運用・管理を含む事例

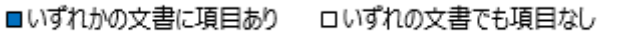


c.アプリケーション保守を含む事例



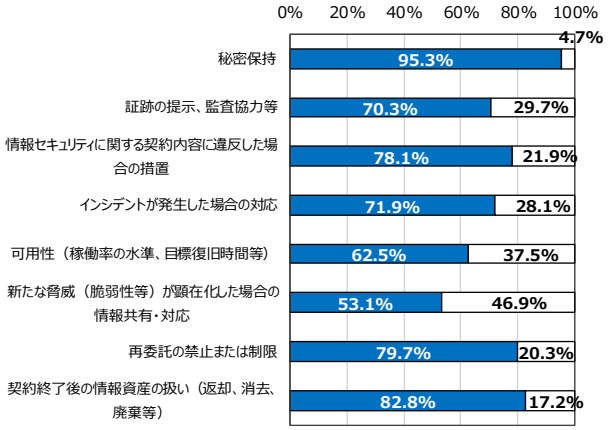
d.ソフトウェアサポートサービスを含む事例



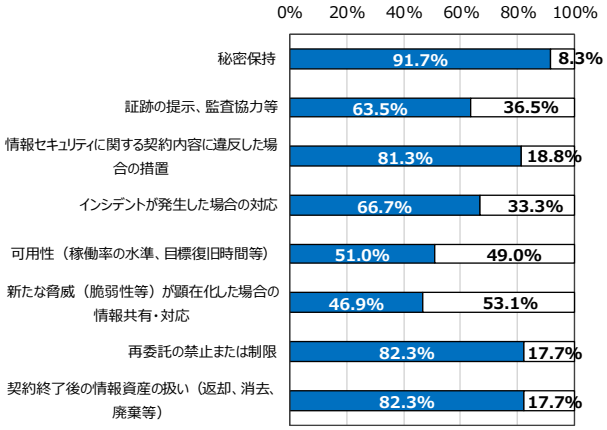


図表 3-12-1　IT システム・サービスの種類ごとの情報セキュリティ要求事項（１）

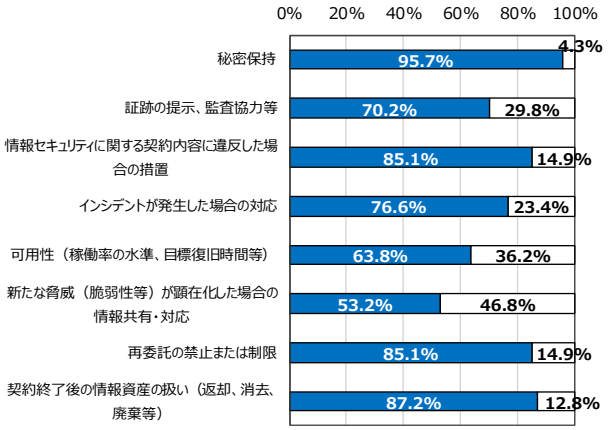
e.ハードウェア保守を含む事例



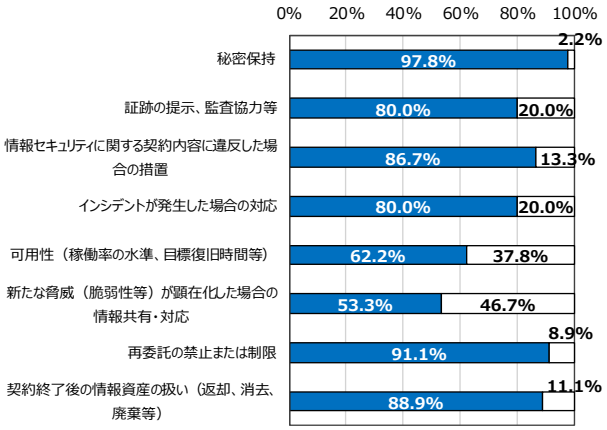
f. Web サイト構築・運用を含む事例



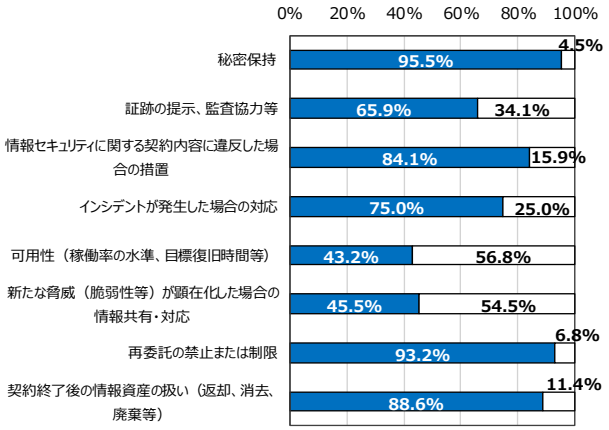
g.サービス提供（ASP . SaaS 等）を含む事例

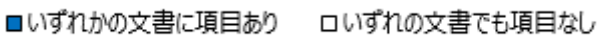


h.インフラ提供（IaaS、ホスティング等）を含む事例



i.データ処理・分析を含む事例





図表 3-12-2　IT システム・サービスの種類ごとの情報セキュリティ要求事項（２）

3.2.4　契約関連文書の雛形における情報セキュリティ要求事項の変更の可否

（1）設問の趣旨

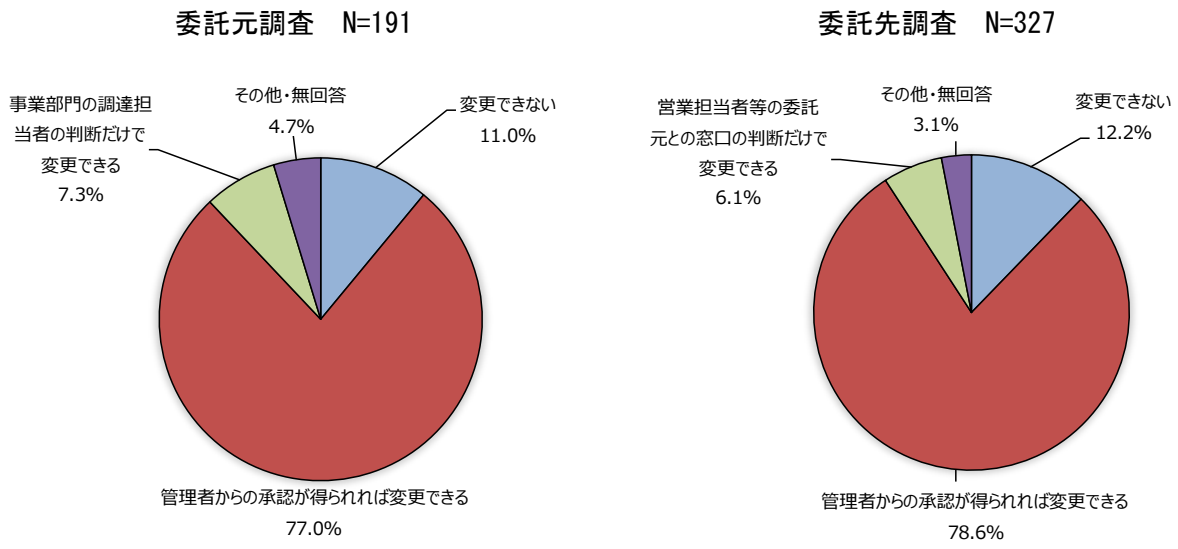
IT システム・サービスはシステム構成や業務内容によって必要なセキュリティ対策が異なり、個々の契約ごとに情報セキュリティ要求事項の追加、条件変更等が発生することが想定される。このような場合、契約書の該当記述を適正に修正することが望ましい。そこで、アンケート調査では、情報セキュリティ要求事項の含まれる契約関連文書（仕様書、契約書等）の雛形があると回答した組織を対象に、契約関連文書の雛形に記載されている情報セキュリティ要求事項の変更が可能であるかを調査した。

これは、**図表 1-6**　調査仮説 No.4 の「情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形に記載されている情報セキュリティ要求事項の変更は可能である。」に関する調査である。

（2）調査結果

調査結果は、次の**図表 3-13** のとおりである。委託元調査、委託先調査ともに「管理者（法務部門や総務部門の担当者等）からの承認が得られれば、情報セキュリティ要求事項の内容は変更できる」の回答が多数を占めている。

ヒアリング調査の結果も、**図表 3-14** のとおり、委託元 4 社、委託先 3 社で、雛形に記載されている情報セキュリティ要求事項の変更が可能であり、調査仮説 No.4「情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形に記載されている情報セキュリティ要求事項の変更は可能である。」は肯定される結果となった。



図表 3-13 契約関連文書の雛形の情報セキュリティ要求事項の変更の可否

図表 3-14 ヒアリング調査の結果（契約関連文書の雛形の情報セキュリティ要求事項の変更の可否）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・主幹部門単独では認められていないが、契約管理部門や情報セキュリティ部門と相談の上、変更はできる。ただし、自社で定めている「セキュリティガイドライン」に反する要求は認められないので、あくまでガイドラインの範囲内になる。
B 社：委託元 （製造業・大企業）	・契約書の内容の変更は可能である。契約を行おうとしている部門から法務部門へ変更要求を出すと検討される。また、契約書の条項を変更する場合は、個別契約書に基本契約書の条項を上書きする変更内容を記載するとともに、その個別契約書に法務担当のサインも入れることになっている。
C 社：委託元 （サービス業・大企業）	・雛形の変更は認められている。リスクマネジメント部門で変更要求の背景確認を行い、承認、否認の判断をする。
D 社：委託元 （金融業・大企業）	・変更可能であるが、契約書の雛形は基本的に高いほうのリスクを想定して情報セキュリティ要求事項を決めてあるので変更は少ない。 ・雛形を変更する場合は、そのリスクを受容できるかどうか、判断根拠を記載して決裁書を起こし、合議をはかる。事業部門でリスク受容できるかどうか判断できない場合は法務部に諮る。
E 社：委託先 （国内 IT 企業・大企業）	・変更は認められている。要求項目を増やしたり減らしたりすることができる。
F 社：委託先 （国内 IT 企業・大企業）	・変更することは可能だが、雛形の記載内容は抽象的なので、個々の要件に応じて内容を変更する必要がない。
G 社：委託先 （国内 IT 企業・大企業）	・各事業部門の管理者から承認が得られれば変更することが可能であり、最終的には管理部門が承認する。

3.2.5　契約関連文書の内容を確認する専任担当者の有無

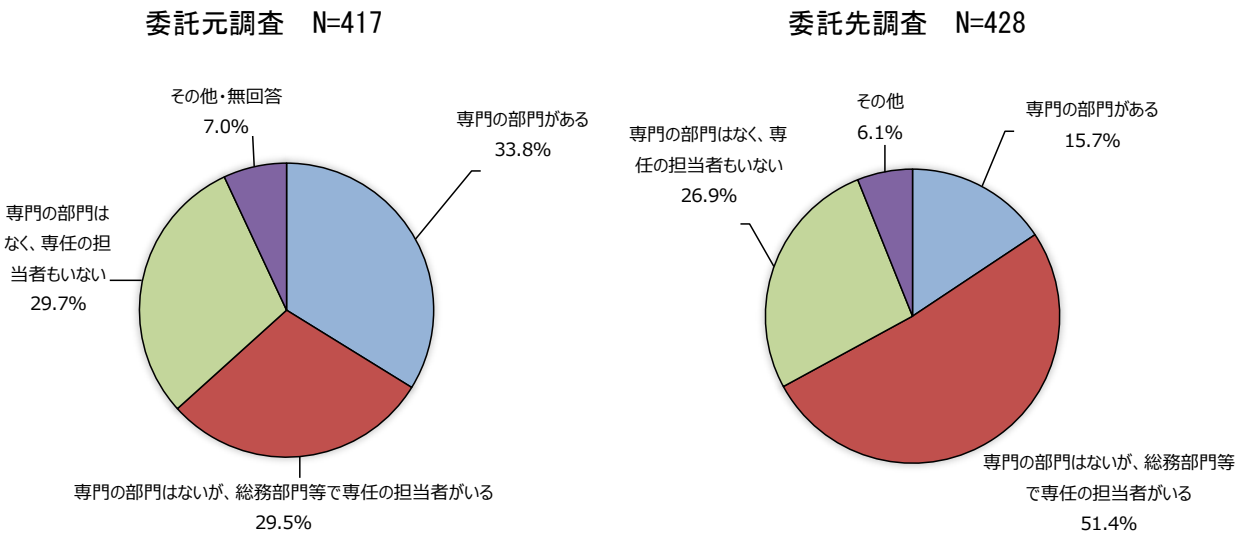
（1）設問の趣旨

アンケート調査では、組織に契約書の内容を確認する専門の部署や専任の担当者がいる場合、契約関連文書における情報セキュリティ要求事項の記載内容が詳細になるのではないかという想定から、委託元調査、委託先調査ともに、契約関連文書の内容を確認する専任担当者の有無を調査した。

これは、**図表 1-6**　調査仮説 No.5 の「大企業は、案件ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けている。」に関する調査である。

（2）調査結果

図表 3-15 に示すとおり、契約関連文書の内容を確認する専門部署または専任担当者を置いておいている割合は、委託元調査では 63.3%、委託先調査では 67.1%であった。

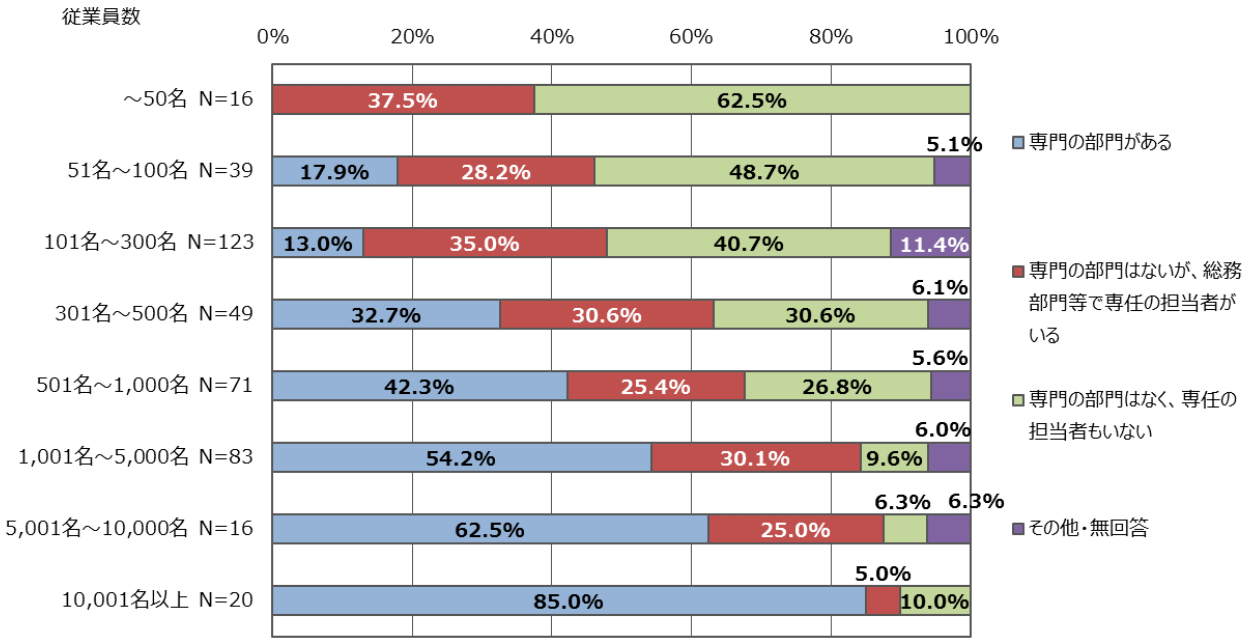


図表 3-15　契約関連文書の内容を確認する専門部署または専任担当者の有無

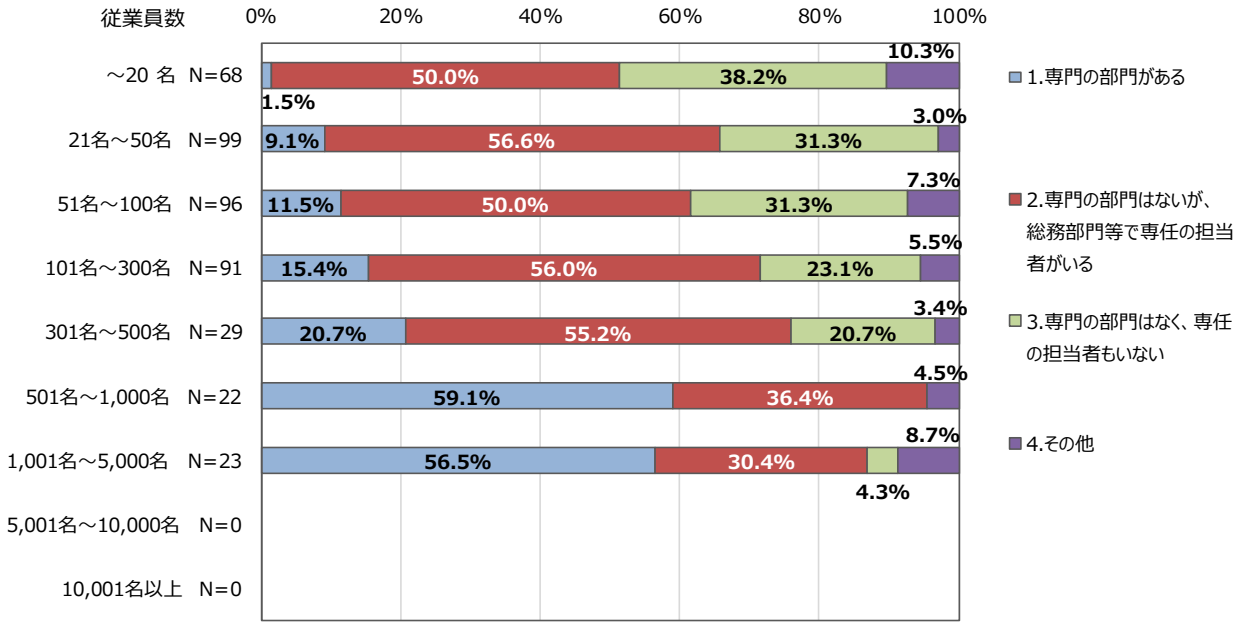
さらに、契約関連文書の内容を確認する専任担当者の有無について、企業規模（総従業員数）ごとの傾向を分析してみた。その結果は、次の**図表 3-16** と**図表 3-17** のとおりである。

委託元調査、委託先調査ともに企業規模が大きくなるにつれ、専門の部署や専任の担当者を置いている傾向が強い。ヒアリング調査の対象とした大企業でも、委託元 4 社、委託先 3 社で専門の部署や専任の担当者を置いていた。

アンケート調査、ヒアリング調査ともに、調査仮説 No.5「大企業は、案件ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けている。」を肯定する調査結果となった。



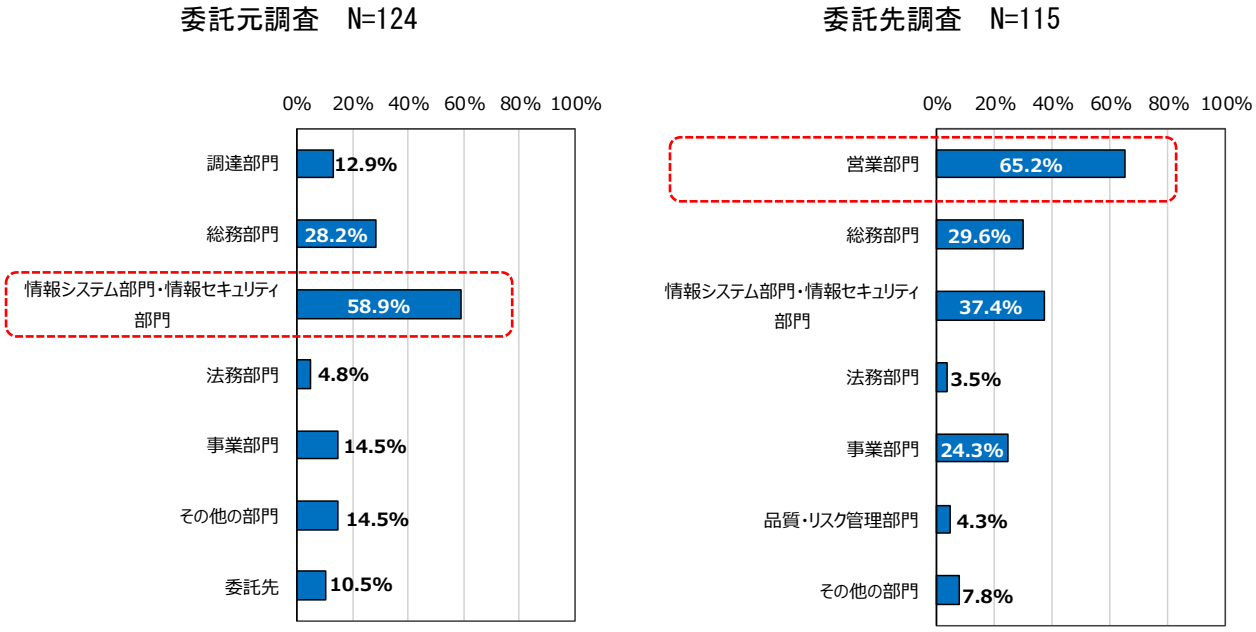
図表 3-16 総従業員数と契約関連文書の内容を確認する専任担当者の有無（委託元調査） N=417



図表 3-17 総従業員数と契約関連文書の内容を確認する専任担当者の有無（委託先調査） N=428

アンケート調査では、業務委託における情報セキュリティ要求事項の明確化について、役割ごとに所管（関与）する部門についても調査した。契約書の内容を確認する専門の部門や専任の担当者がいない場合について、契約書の内容の確認を所管（関与）する部門の回答を集計した結果は、**図表 3-18** のとおりとなる。

契約書の内容を確認する専門の部門や専任の担当者がいない場合、委託元では情報システム部門・情報セキュリティ部門、委託先では営業部門が、契約書の内容を確認していることが多い。



図表 3-18　契約書の内容を確認する部門（専門部門・専任担当者がない場合）

3.3 責任範囲が曖昧になる要因について

3.3.1　責任範囲が明確にならない理由

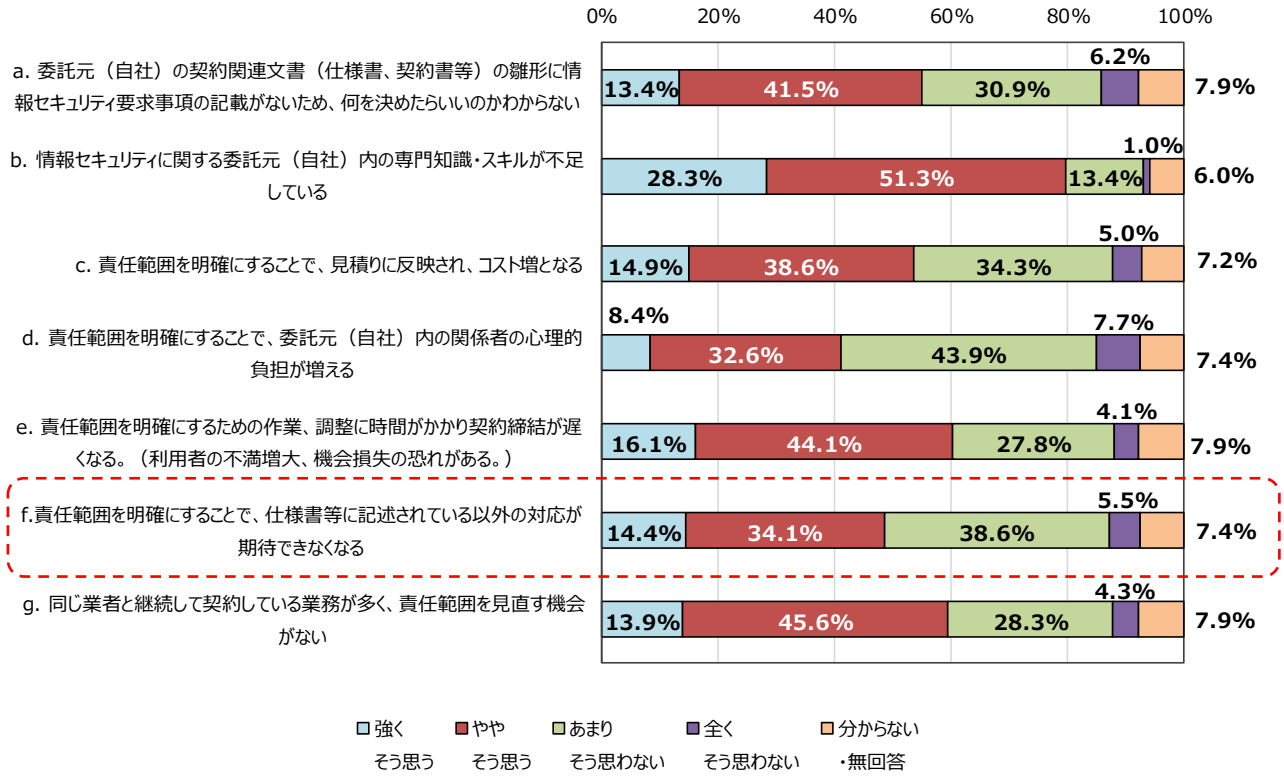
（1）設問の趣旨

2017 年度調査の結果では、委託元調査の回答企業のうち、委託先が実施すべき具体的な情報セキュリティ対策を仕様書等に明記しているのは、全体の 30.9%と低かった。そのため、アンケート調査では、IT 業務委託の契約で責任範囲が明確化にならない理由を調査した。

これは、**図表 1-6** 調査仮説 No.6 の「委託元は、委託先の責任範囲を限定してしまうと、それ以上のことをしてもらえなくなるので、責任範囲を限定したくない。」と調査仮説 No.7 の「委託先は、責任範囲を詳細に決めると、コスト高になり、委託元の合意が得られなくなるので、大まかな取り決めでもよいと考えている。」に関する調査である。

（2）調査結果

委託元の調査結果は、次の**図表 3-19** のとおりである。「f. 責任範囲を明確にすることで、仕様書等に記述されている以外の対応が期待できなくなる」に対する「強くそう思う」と「ややそう思う」の回答を合わせると 48.5%で全体の半数程度となった。調査仮説 No.6 の「委託元は、委託先の責任範囲を限定してしまうと、それ以上のことをしてもらえなくなるので、責任範囲を限定したくない。」は概ね肯定される結果となった。

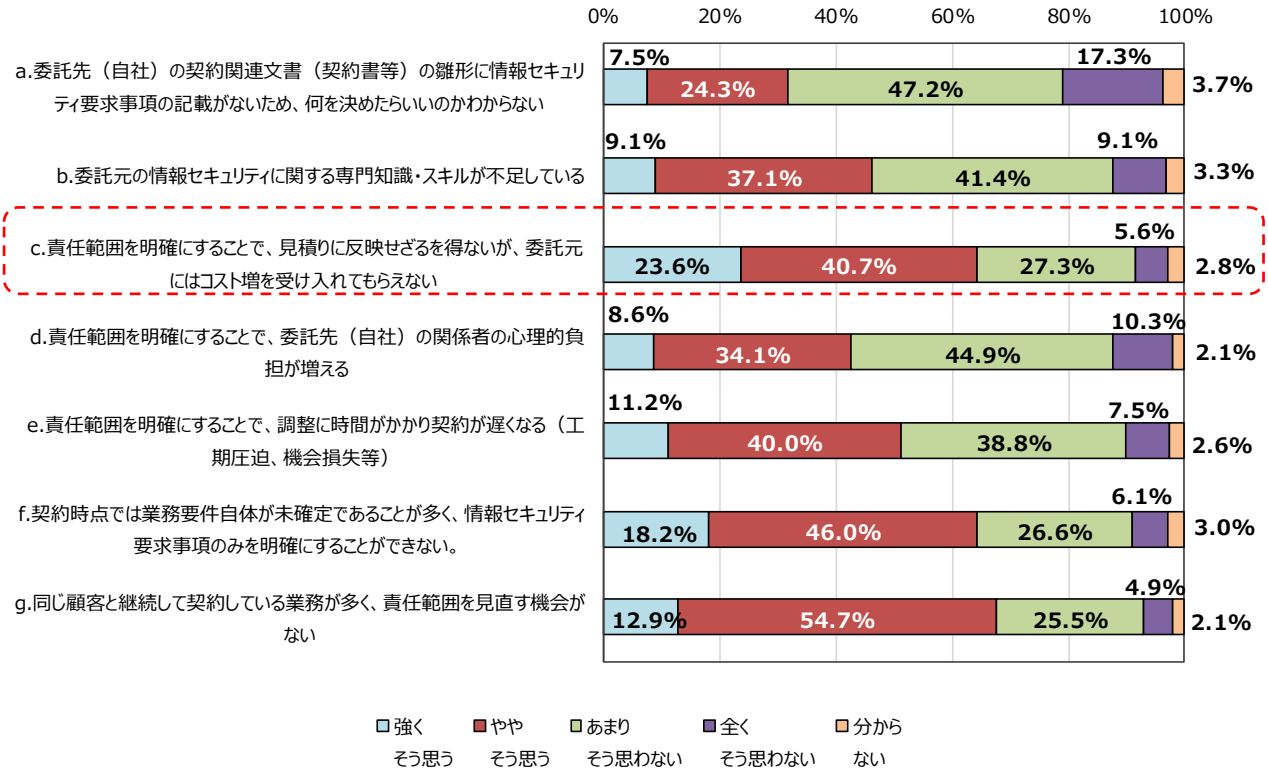


図表 3-19 責任範囲が明確にならない理由（委託元調査）　N=417

また、他の選択肢についても「d. 責任範囲を明確にすることで、自組織内の関係者の心理的負担が増える」以外は全て 50%を超えており、責任範囲を明確にするための課題は多く、中でも「b. 情報セキュリティに関する自組織内の専門知識・スキルが不足している」については 3 割近くが「強くそう思う」と答えており、知識やスキルを補う対策が求められる。

委託先の調査結果は、次の**図表 3-20** のとおりである。「g.同じ顧客と継続して契約している業務が多く、責任範囲を見直す機会がない」に対して「強くそう思う」と「ややそう思う」の回答が最も多く、合わせると 67.6%を占める。次いで多いのが、「c.責任範囲を明確にすることで、見積りに反映せざるを得ないが、委託元にはコスト増を受け入れてもらえない」であり、「強くそう思う」と「ややそう思う」を合わせると 64.3%となる。

調査仮説 No.7 の「委託先は、責任範囲を詳細に決めると、コスト高になり、委託元の合意が得られなくなるので、大まかな取り決めでもよいと考えている。」については、概ね肯定される結果となった。



図表 3-20 責任範囲が明確にならない理由（委託先調査） N=428

3.3.2　資本関係の有無と組織的なセキュリティ対策の要求

（1）設問の趣旨

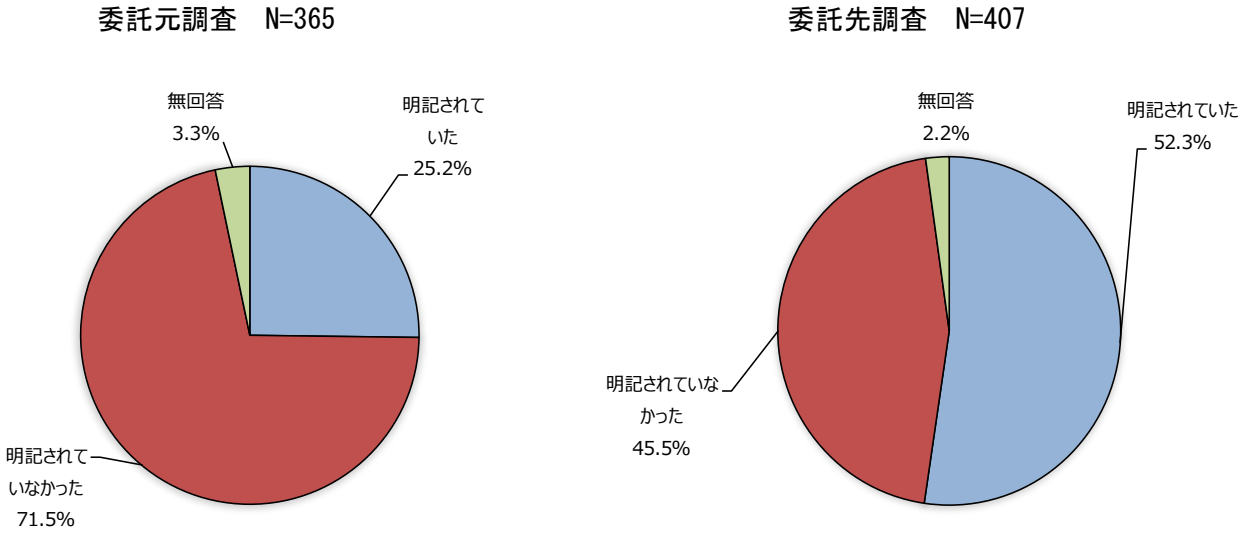
IT システム・サービスの業務委託先の企業が、資本関係のある子会社やグループ企業である場合、お互いのセキュリティポリシー等を理解していることが多いと考えられ、契約関連文書において、組織的なセキュリティ対策を要求することが少ないことが想定される。そのため、アンケート調査では、事例に関する設問の中で、委託元と委託先のあいだに資本関係があるかどうかと、契約書に組織的なセキュリティ対策が明記されているかどうかを調査した。

これは、調査仮説 No.8「委託元と委託先の関係に資本関係がある場合、契約関連文書に組織的なセキュリティ対策が明記されることが少ない。」に関する調査である。

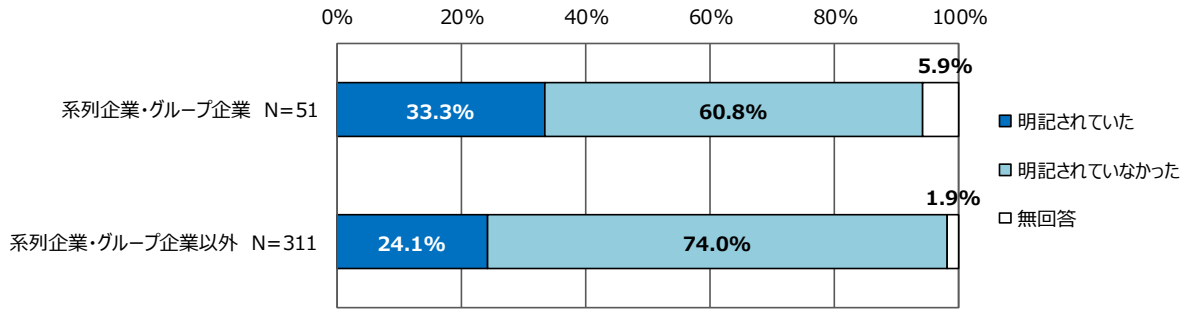
（2）調査結果

契約関連文書における組織的なセキュリティ対策の要求の有無に関する調査結果は、次の**図表 3-21** のとおりである。委託元と委託先で比較すると、委託先のほうが「明記されていた」とする回答が多い。

この調査結果を、さらに、委託元と委託先の資本関係の有無で分析したものが、**図表 3-22** と**図表 3-23** である。委託元調査では、資本関係が有ることで契約関連文書における組織的なセキュリティ対策の要求が強まる傾向にあり、調査仮説 No.8「委託元と委託先の関係に資本関係がある場合、契約関連文書に組織的なセキュリティ対策が明記されることが少ない。」を肯定する調査結果とはならなかった。

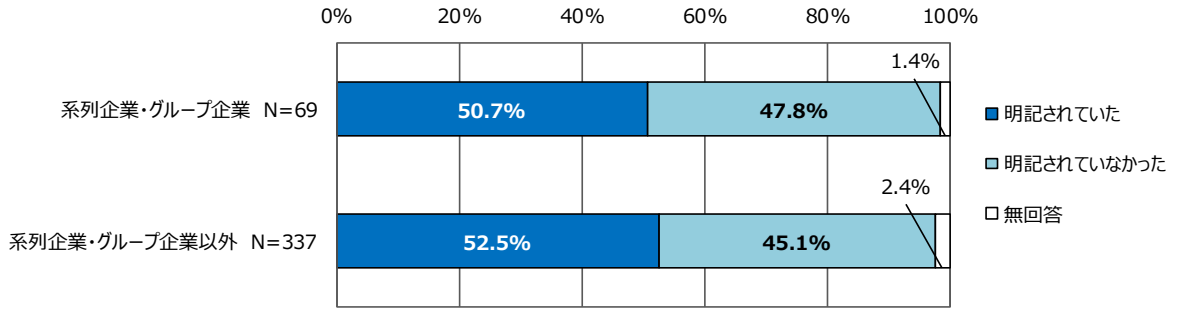


図表 3-21　契約関連文書における組織的なセキュリティ対策の要求



※資本関係の有無について回答のなかったデータ 3 件を集計対象外とした

図表 3-22 資本関係の有無と組織的なセキュリティ対策の要求（委託元調査）　N=362



※資本関係の有無について回答のなかったデータ 1 件を集計対象外とした

図表 3-23 資本関係の有無と組織的なセキュリティ対策の要求（委託先調査）　N=406

3.3.3　未知の脆弱性に関する対応

(1) 設問の趣旨

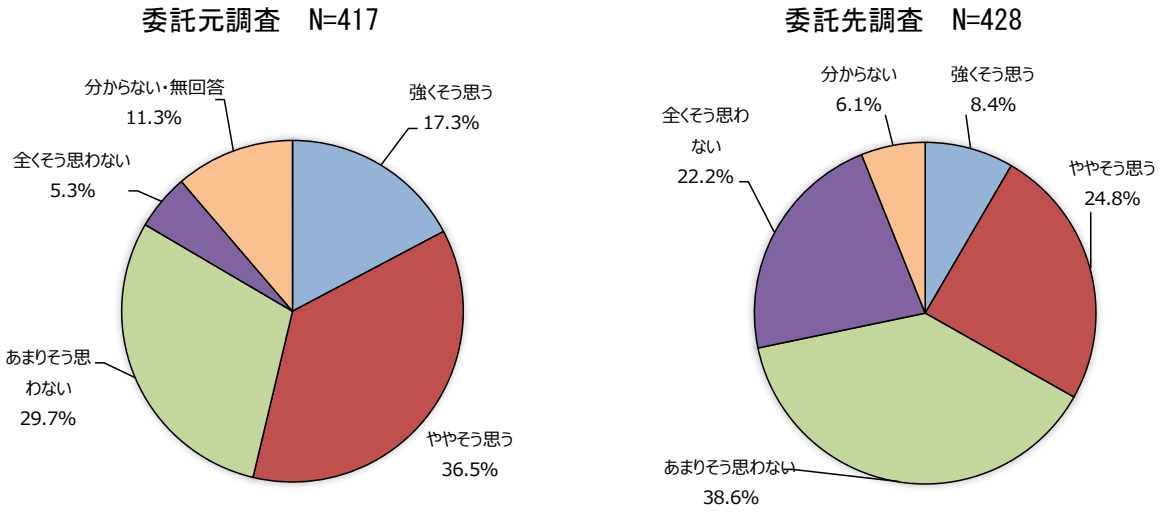
アンケート調査では、ソフトウェア開発等の納品後（契約期間外）に見つかった未知の脆弱性への対応に関して、回答者の考えを尋ねる設問を設けた。これは、**図表 1-6** 調査仮説 No.9「委託元は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなくても委託先が対応すべきだと考えている。」と調査仮説 No.10「委託先は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなければ実施する必要はないと考えている。」に関する調査である。

具体的な設問の内容は次のとおりである。回答方法は、それぞれ「強くそう思う」「ややそう思う」「あまりそう思わない」「全くそう思わない」「分からない」からの択一選択とした。

① 納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ
② 納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ
③ 納品後の IT システムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ

(2) 調査結果 ①

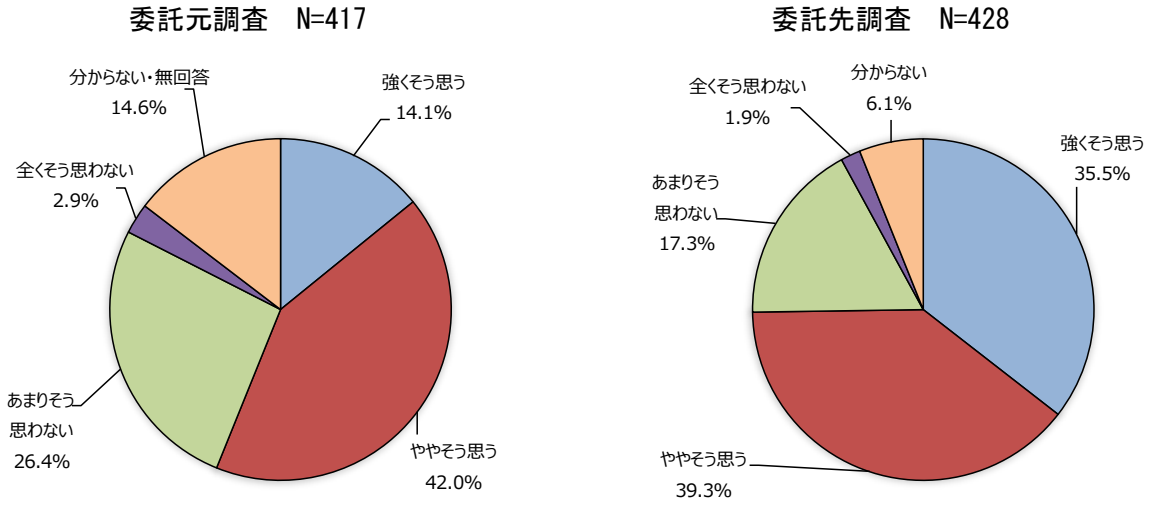
設問①の調査結果は、次の**図表 3-24** のとおりである。「強くそう思う」「ややそう思う」を合わせた割合で見ると、委託元のほうが委託先よりも、大幅に「委託先が責任を持つべきだ」とする回答が多い。



図表 3-24 納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ

(3) 調査結果 ②

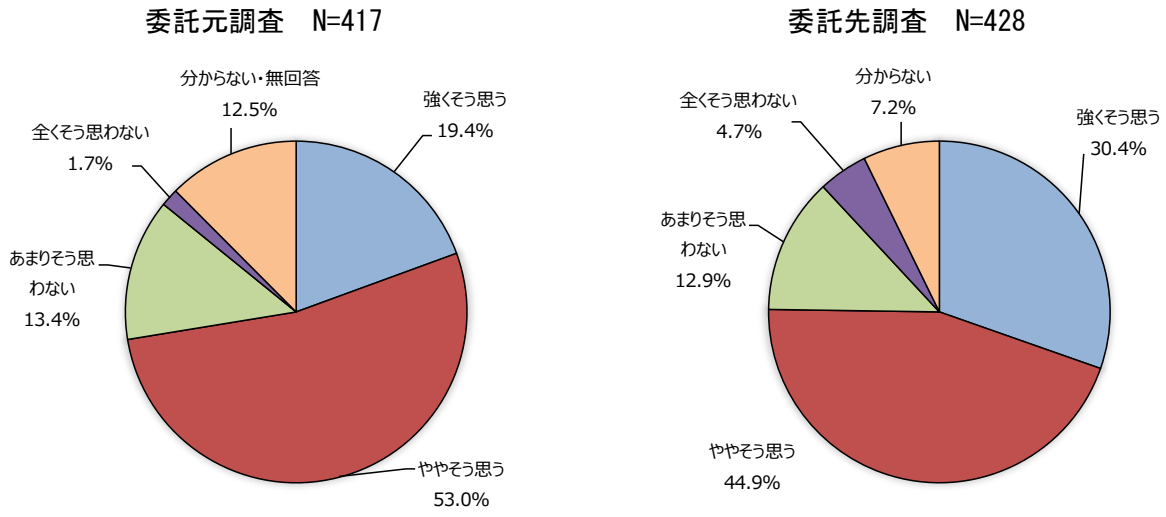
設問②の調査結果は、次の**図表 3-25** のとおりである。「強くそう思う」「ややそう思う」を合わせた割合で見ると、委託先のほうが委託元よりも、大幅に「必要に応じて業務委託するべきだ」とする回答が多い。



図表 3-25 納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ

(4) 調査結果 ③

設問③の調査結果は、次の**図表 3-26** のとおりである。「強くそう思う」「ややそう思う」を合わせた割合で見ると、委託元も委託先も、全体の 4 分の 3 程度が、「契約書等に定めるべきだ」と回答している。



図表 3-26 納品後の IT システムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ

（5）調査結果（ヒアリング調査）

納品後に見つかった未知の脆弱性への対応については、ヒアリング調査でもヒアリング項目とした。その結果は、**図表 3-27** のとおり「委託元が責任を持つべき」という回答が多く、責任範囲の曖昧さを容認するような発言はなかった。

図表 3-27 ヒアリング調査の結果（納品後に見つかった未知の脆弱性への対応）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・受入検査を行っている以上、納品後は、委託元が最終責任者であると考える。受入検査は、ネットワーク検査、静的検査、動的検査、ペネトレーション検査等、かなり念入りに行っている。 ・受入検査で見つかった問題はベンダに解決してもらう。ただし、開発時の注意義務や、運用・保守の条件によっては委託先の責任もある（フレームワークやミドルウェアの選定、セキュリティパッチの対応、サポート切れによるバージョンアップ対応等）。
B 社：委託元 （製造業・大企業）	・納品物の検収の際に予測できたものかというのが一番大きいのではないか。一生懸命に調べても分からなかったもの、その時点で専門家でも世界的に未知であったものについては、委託先に責任を負わせられない。
C 社：委託元 （サービス業・大企業）	・保守契約中は委託先に対応を依頼することがある。保守契約が終了しているシステムはケースバイケースで都度検討している。
D 社：委託元 （金融業・大企業）	・未知の脆弱性というのは、受入検査のときに分かっていなかったものであるから、その責任を委託先に求めるのには無理があると思う。プログラムの瑕疵であれば、善管注意義務というのを問うこともできるだろうが、未知の脆弱性については、委託先に責任を求めることはできない。
E 社：委託先 （国内 IT 企業・大企業）	・委託元が責任を持って監視すべきで、必要に応じてセキュリティ要件を見直しすべきだと思う。
F 社：委託先 （国内 IT 企業・大企業）	・当社は委託元になることもあり、発注者側としては、受注者側に全部責任を持ってもらいたいと思う。しかしながら、受注者側の立場としては、コスト的に負担になることもあり、全ての責任を負いきれないので、発注者側に責任範囲を限って欲しい。
G 社：委託先 （国内 IT 企業・大企業）	・どちらが作業環境を用意したかによって責任は異なる。当社が用意した環境で発生したものであれば当社の責任。顧客の用意した環境で発生したものであれば顧客の責任だと思う。

(6) まとめ

設問①の調査結果（**図表 3-25**）および設問②の調査結果（**図表 3-26**）はともに委託元と委託先のあいだで回答にギャップがある結果となった。設問①の調査結果（**図表 3-25**）では、委託元のほうが委託先よりも「委託先が責任を持つべきだ」とする回答が多く、設問②の調査結果（**図表 3-26**）では、委託先のほうが委託元よりも「必要に応じて業務委託すべき」とする回答が多かった。委託先は必要に応じて業務委託契約を結んだ上で対応したいと考える企業が多いということになる。

設問①「納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託先が責任を持つべきだ」は、調査仮説 No.9 の「委託元は、稼働後のシステムやサービスのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなくても委託先が対応すべきだと考えている。」に関する調査であった。この設問に対し、委託元の 53.8%は、「強くそう思う」と「ややそう思う」を選択している。一方、委託先で「強くそう思う」と「ややそう思う」を選択しているのは 33.2%にとどまる。ヒアリング調査の対象とした委託元の大企業では、**図表 3-27** のとおり、納品後に見つかった未知の脆弱性については、委託元が責任を持つべきという回答が多かった。また、設問②「納品後の IT システムの情報セキュリティに関する未知の脆弱性への対応は、委託元が検討し、必要に応じて業務委託するべきだ」では、委託元の 56.1%が「強くそう思う」と「ややそう思う」を選択し、委託先ではこれが 74.8%まで割合が高くなる。設問②も考慮したこれらの調査結果より、調査仮説 No.9 は肯定される結果とはならなかった。

設問③「納品後の IT システムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ」の調査結果（**図表 3-27**）は、委託元、委託先ともに、全体の 4 分の 3 程度が、「納品後の IT システムの情報セキュリティに関する未知の脆弱性への責任分担について契約書等に定めるべきだ」と回答していた。この設問は、調査仮説 No.10 の「委託先は、稼働後のシステムやサービスのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなければ実施する必要はないと考えている。」に関する調査であったが、委託先の 75.3%が、未知の脆弱性に対する対応を「契約等で明記すべき」「必要に応じて業務委託すべき」と回答している。委託先は明示的な合意に基づいて対応したいと考えている傾向にあり、調査仮説 No.10 については、概ね肯定される結果となった。

3.4 サイバー保険の加入状況等について

3.4.1　仮説の背景

責任範囲の曖昧さを解決できない場合のリスクへの備えとして、保険により金銭面の補てんをすることが考えられる。2015 年に実施した「企業におけるサイバーリスク管理の実態調査 2015[10]」では、コンピュータの故障に関する保険、情報漏えいに関する保険、サイバー攻撃に関する保険のいずれかに加入している（ＩＴ関連保険の加入者）割合は全体の約 15%であった。

その後、保険各社からサイバー保険が発売され、保障内容が充実してきており、また、サイバー攻撃を完全に防ぐことが困難であることから、早期に検知、被害の最小化、迅速な復旧のための対策強化の重要性が高まってきており、サイバー保険に対する注目度も高まっていることが想定される。

2017 年に改訂された「サイバーセキュリティ経営ガイドライン[11]」 においても、「指示４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」の中でサイバー保険の活用について触れられており、組織的な対策として検討が必要と考えられる。このような背景から、保険の加入状況や加入の阻害要因を調査した。

3.4.2　サイバー保険の加入状況

（1）設問の趣旨

アンケート調査では、委託元調査、委託先調査ともに、サイバー保険の加入状況を尋ねる設問を設けた。これは、**図表 1-6** 調査仮説 No.11 の「委託元、委託先ともに、サイバー保険に加入している割合は低い。」に関する調査である。

（2）調査結果

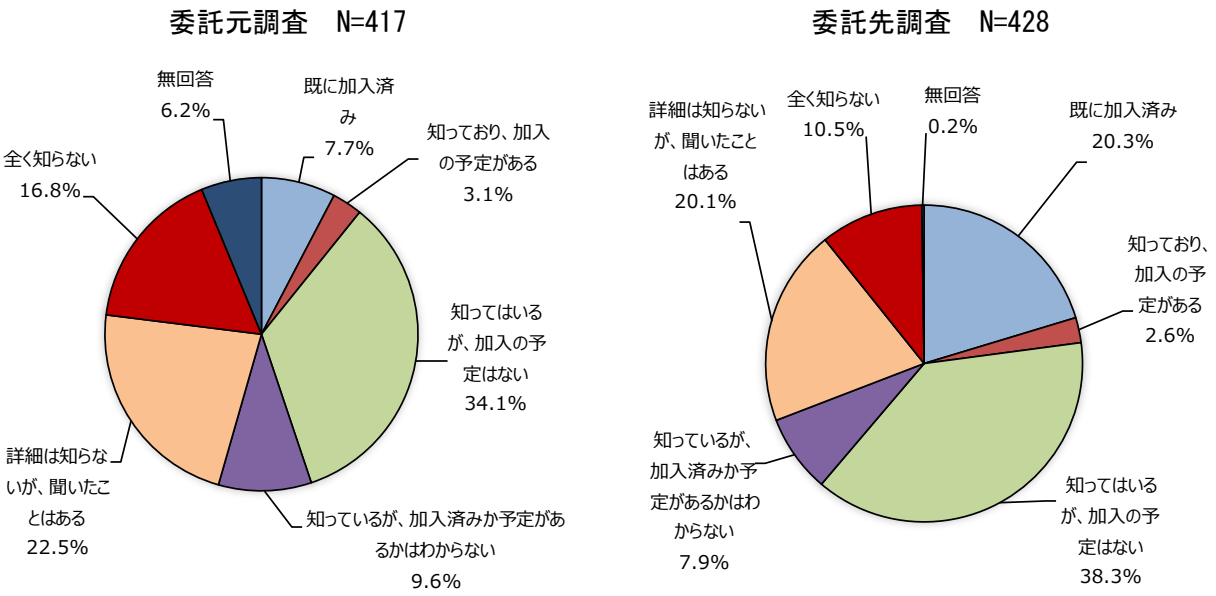
調査結果は、次の**図表 3-28** のとおりである。既にサイバー保険に加入している企業は、委託元が 7.7%、委託先が 20.3%であり、2015 年に実施した調査と比較し、委託先については若干増加していたが、委託元の加入状況はかなり低く、概ね調査仮説 No.11 のとおりの結果となった。

なお、サイバー保険を知ってはいるが加入の予定はないとする企業は、委託元で 34.1%、委託先で 38.3%と、ともに全体の 3 分の 1 以上を占めていた。ヒアリング調査の結果でも、**図表 3-29** のとおりサイバー保険に加入している企業は 7 社中 3 社であった。

---

10 情報処理推進機構「企業におけるサイバーリスク管理の実態調査 2015」報告書について(2015 年)https://www.ipa.go.jp/security/fy27/reports/cyber-ins/index.html

11 経済産業省「サイバーセキュリティ経営ガイドライン」
http://www.meti.go.jp/policy/netsecurity/mng_guide.html



図表 3-28 サイバー保険の加入状況

図表 3-29 ヒアリング調査の結果（サイバー保険の加入状況）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・加入している。サイバー保険単品の契約ではなく、ビジネス保険の特約として加入している。
B 社：委託元 （製造業・大企業）	・国内では加入していない。
C 社：委託元 （サービス業・大企業）	・個人情報漏えい保険には加入しているが、サイバー攻撃に対する補償のものには加入していない。
D 社：委託元 （金融業・大企業）	・加入していない。
E 社：委託先 （国内 IT 企業・大企業）	・現在は個人情報漏洩対策の保険のみ加入済。 ・サイバー保険は、現状は加入していないが、新年度から加入予定である。
F 社：委託先 （国内 IT 企業・大企業）	・加入していない。社内で話題になったこともない。
G 社：委託先 （国内 IT 企業・大企業）	・加入しているようだが、補償内容等詳細は分からない。

3.4.3　サイバー保険に加入している理由

（1）設問の趣旨

アンケート調査では、サイバー保険の代表的な補償内容を 6 点列挙し、回答者が魅力を感じる補償内容について最大 3 つを選択する調査を実施した。

これは、**図表 1-6** 調査仮説 No.12「委託元がサイバー保険に加入している理由は『損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償』が魅力的と思っているからである。」に関する調査である。

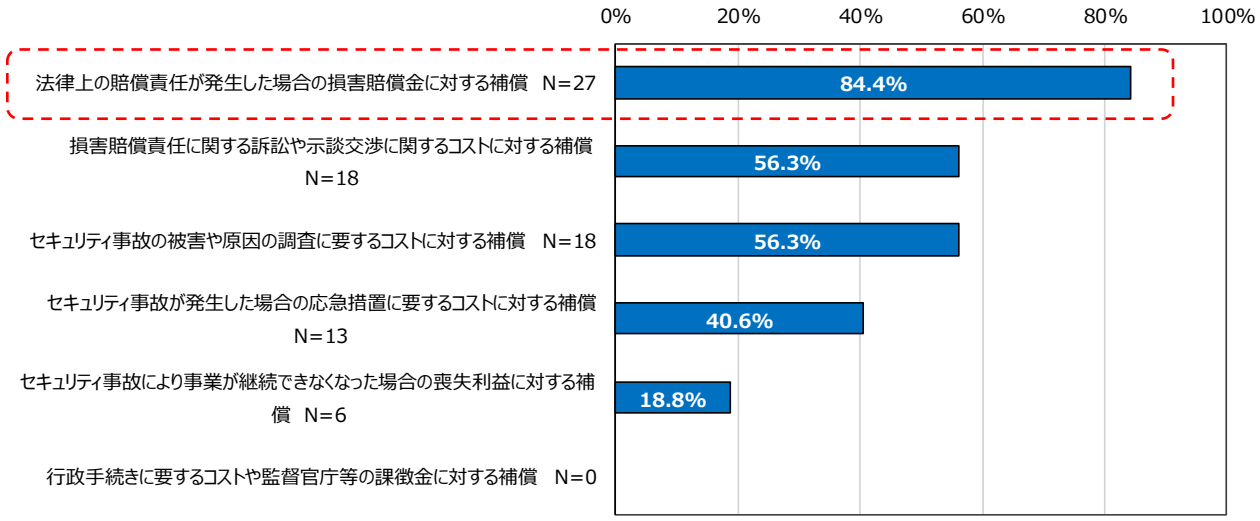
（2）調査結果

前項の調査で「サイバー保険に既に加入済み」と回答した企業を対象に、サイバー保険の補償内容の魅力に関する調査の結果を集計したものが、次の **図表 3-30** と**図表 3-31** である。

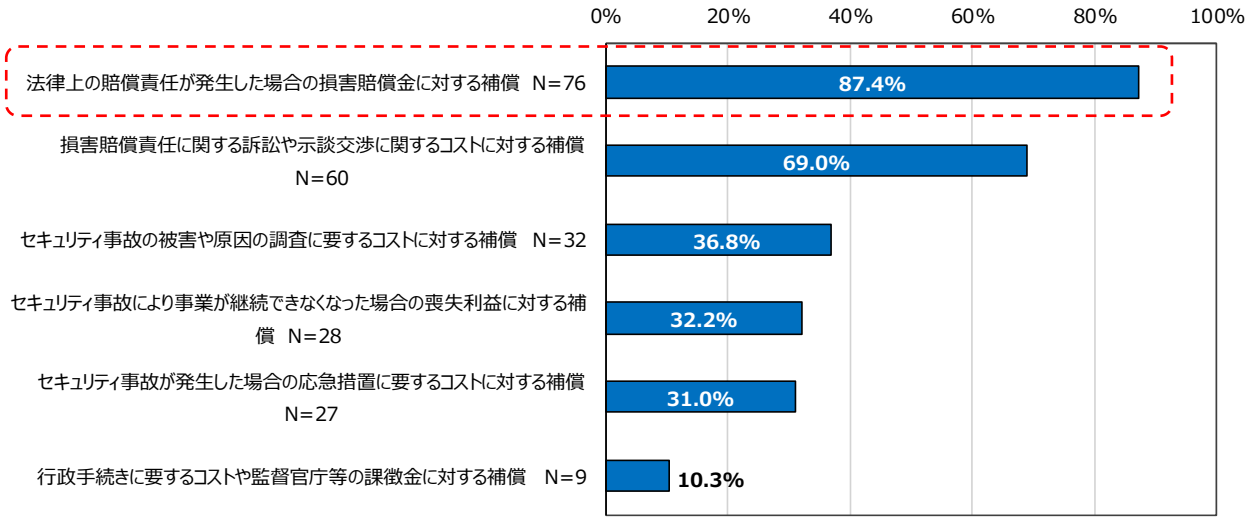
委託元、委託先ともに「法律上の賠償責任が発生した場合の損害賠償金に対する補償」が最も多く、加入している企業の 85.0%前後と高い比率だった。また、次に回答が多かったのは、委託元は「損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償」と「セキュリティ事故の被害や原因の調査に要するコストに対する補償」であり、委託先は「損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償」であった。

なお、ヒアリング調査では、**図表 3-32** のとおり、サイバー保険に加入している企業は「訴訟のリスク」や「情報漏えい時に損害賠償」に対する備えが加入の理由だった。

アンケート調査の結果、ヒアリング調査の結果ともに、調査仮説 No.12「委託元がサイバー保険に加入している理由は『損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償』が魅力的と思っているからである。」を肯定する結果となった。



図表 3-30 サイバー保険に加入している理由（委託元調査・加入済みの場合）　N=32



図表 3-31 サイバー保険に加入している理由（委託先調査・加入済みの場合）　N=87

図表 3-32 ヒアリング調査の結果（サイバー保険に加入している理由）

ヒアリング対象者	ヒアリング内容
A 社：委託元 （製造業・大企業）	・訴訟等のビジネスリスクに備えるためである。
E 社：委託先 （国内 IT 企業・大企業）	・個人情報漏えい時の損害賠償額の補填のためである。

3.4.4　サイバー保険に加入しない理由

（1）設問の趣旨

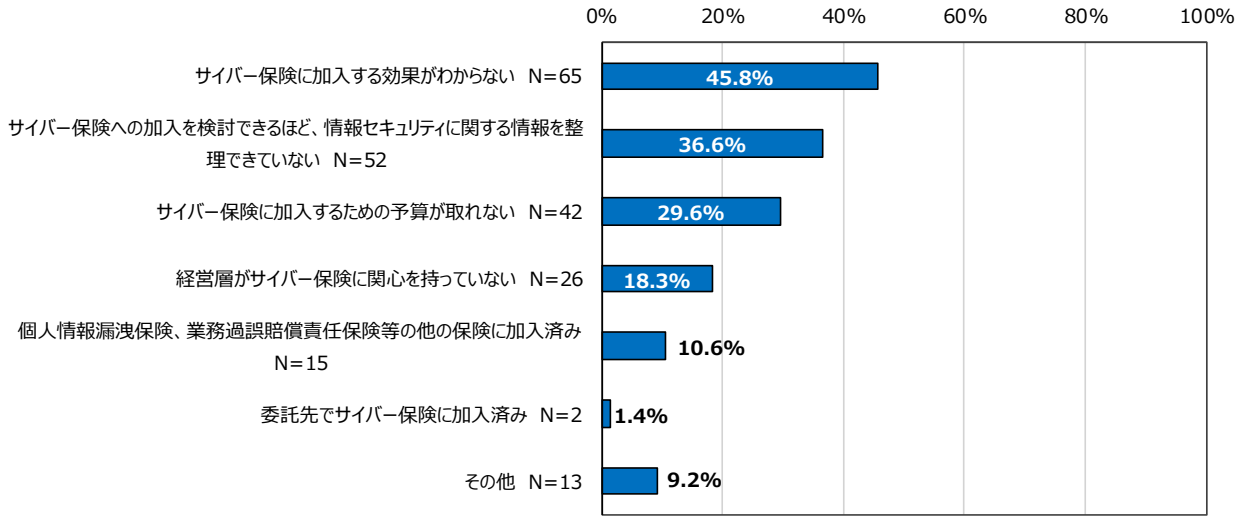
アンケート調査では、3.4.2 の「サイバー保険の加入状況」の設問で「（サイバー保険を）知ってはいるが、加入の予定はない」を選択した委託元の回答者を対象に、サイバー保険に加入しない理由を調査した。調査方法は、代表的な理由を 6 点列挙し、そのなかから該当するものを全て選択する方法とした。

これは、**図表 1-6** 調査仮説 No.13「委託元がサイバー保険に加入していない理由は『委託先がサイバー保険に入っていればよい』と思っているからである。」に関する調査である。

（2）調査結果

アンケート調査の結果は、次の**図表 3-33** のとおりである。サイバー保険に加入しない理由は「サイバー保険に加入する効果がわからない」が最も多く、次いで多いのが「サイバー保険への加入を検討できるほど、情報セキュリティに関する情報を整理できていない」であった。また、ヒアリング調査の結果は、**図表 3-34** のとおりである。大量の顧客情報を扱う大企業では、インシデントが発生した場合の損害賠償金額が高額になることが予想され、現時点のサイバー保険で用意されている補償内容では、その費用を賄えないため加入していないとする回答が多かった。

アンケート調査、ヒアリング調査ともに、仮説 No.13「委託元がサイバー保険に加入していない理由は『委託先がサイバー保険に入っていればよい』と思っているからである。」を肯定する調査結果とはならなかった。



図表 3-33 サイバー保険に加入しない理由（委託元調査・知ってはいるが加入の予定がない場合）
N=142

図表 3-34 ヒアリング調査の結果（サイバー保険に加入しない理由）

ヒアリング対象者	ヒアリング内容
B 社：委託元 （製造業・大企業）	・サイバー保険で補償される金額が実際に必要な金額にマッチしないと考えている。サイバー保険の保険料を支払うくらいなら、セキュリティ対策に投資したい。ただし、保険会社が、業態ごとにビジネスリスクを踏まえた補償のメニューを用意したり、セキュリティアセスメントを行って、組織の状況に応じた保険料を設定したりするサービスを始めるようであれば、検討の余地はあると思う。
D 社：委託元 （金融業・大企業）	・当社に必要な補償額を賄うための保険料は莫大なものになる。その費用があれば、セキュリティ対策に投資する。 ・サイバー保険というのは、基本的に中小企業向けのものだと思っている。例えば、会社を立ち上げて EC ビジネスをはじめたような会社が、情報漏えいを起こしたりすると、賠償で倒産に追い込まれるようなことになる。企業の事業継続性や顧客保護という観点で、中小企業がサイバー保険に加入するというのは有効だと考える。
F 社：委託先 （国内 IT 企業・大企業）	・セキュリティにお金をかけることについて、費用対効果が定量的に判断しづらい。インシデントが発生する確率というのは常に変わっていくもので当てにならない。
H 社：委託先 （IT コンサルティング企業）	・サイバー保険の一般的なメニュー料金は下がったが、ある程度の補償を求めると保険料も上がる。大企業で何かインシデントが起きると補償額が億を超えることがありうる。各保険会社の保険料の計算式に、その補償額を当てはめると保険料が跳ね上がり加入を検討するのは難しい。
I 社：委託先 （セキュリティコンサルティング企業）	・「保険のおかげで助かった」という話を聞くことがなく、効果が見えないので、必要性が感じられないのではないか。

3.5 責任範囲の明確化の状況に関する分析

3.5.1 分析の概要

アンケート調査では、具体的な IT 業務委託の事例において、調査対象の契約関連文書（**図表 1-12**）に、調査対象の情報セキュリティ要求事項（**図表 1-11**）が記載されていたか、また、記載されている項目については、責任範囲が明示されていたかを調査した（1.3.3（5）～（8）参照）。本節では、その調査結果から、事例のプロフィールに関する調査項目（**図表 1-13**）と責任範囲の明確化の状況との関係を分析し、項目間に傾向の差が見られたものについて、分析の概要を示した。

なお、調査対象の情報セキュリティ要求事項は 8 項目、調査対象の契約関連文書は 7 項目有り、組み合わせると 56 項目となるが、分析対象とする事例は、56 項目のいずれかについて、次の選択肢のうちから ii ～ iv の回答があるものとした。この条件で、分析対象の事例は委託元が 313 件、委託先が 374 件となった。

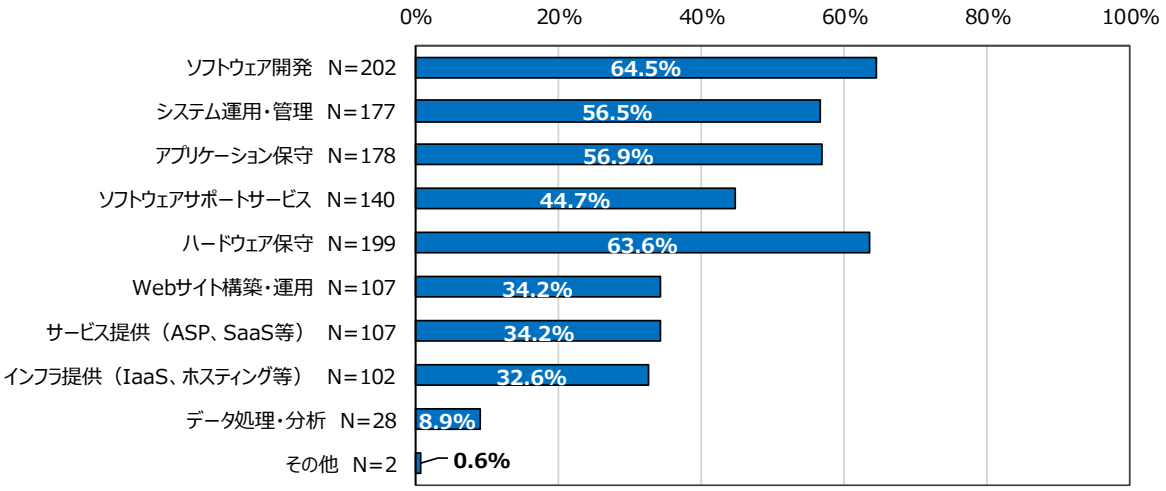
ⅰ. 当該文書は使用していない
ⅱ. 当該文書は使用しているが、当該項目は要求事項となっていないので、項目そのものの記載がない
ⅲ. 当該項目の記載があるが、委託先が責任を負うべき範囲が明示されていない（「都度調整」等）
ⅳ. 当該項目について、委託先が責任を負うべき範囲が明示されている

3.5.2 IT システム・サービスの種類と責任範囲の明確化の状況に関する分析

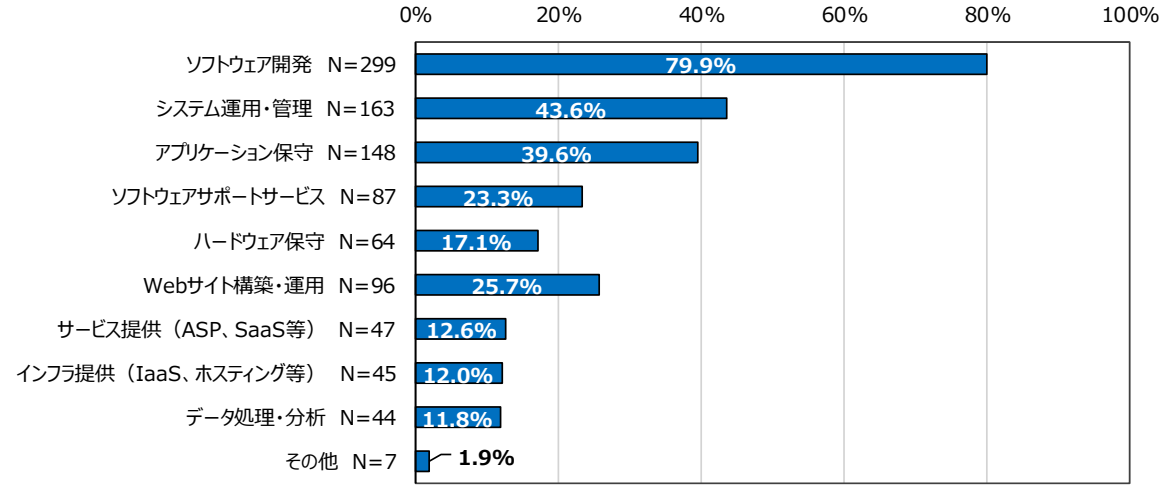
（1）事例に含まれる IT システム・サービスの種類

3.2.3 において、委託先調査では、IT システム・サービスの種類によって情報セキュリティ要求事項の内容に違いがあることが分かった。ここでは、委託元調査、委託先調査の両方の事例を対象に、IT システム・サービスの種類ごとに責任範囲の明確化の状況の関係を分析する。

委託元が業務委託した事例は、**図表 3-35** のとおり、システム運用・管理やアプリケーション保守、ハードウェア保守等が、ソフトウェア開発と同じ程度に多かった。これは、ソフトウェアの新規開発は数年に一度というような企業の場合でも、システムの維持管理は常に必要な作業であり、かつ、その業務を外部委託するケースが多いことによるものと考えらえる。一方、委託先が受託した業務の事例は、**図表 3-36** のとおり、ソフトウェア開発が含まれる事例が多く、次に多いシステム運用・管理に比べても 2 倍近い件数であった。これは、ソフトウェア業専業の企業からの回答が多かったためと思われる。



図表 3-35 IT システム・サービスの種類（委託元調査） N=313

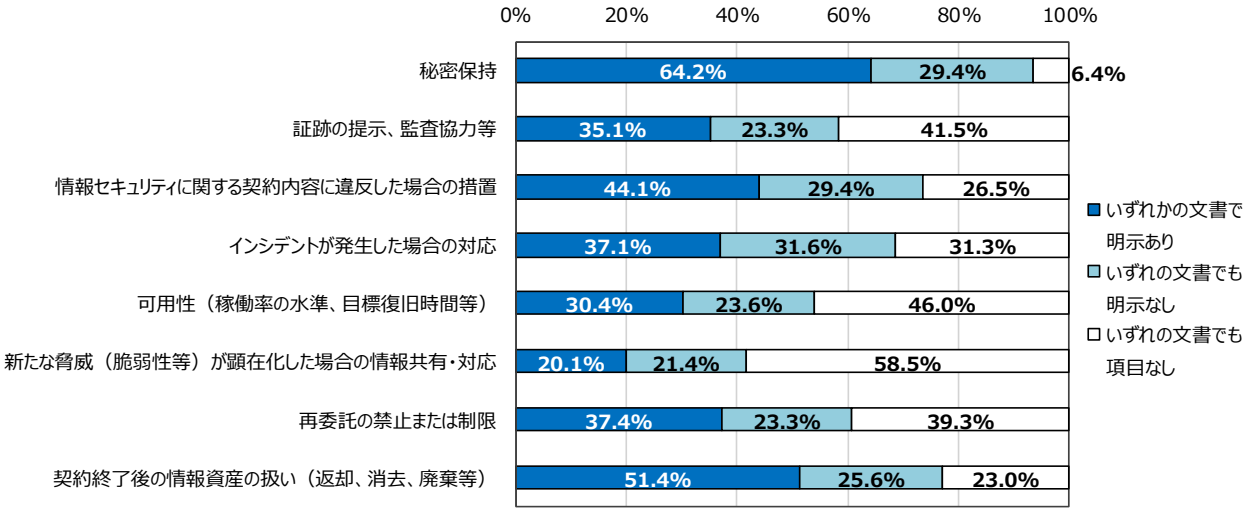


図表 3-36（図表 3-11 再掲） IT システム・サービスの種類（委託先調査） N=374

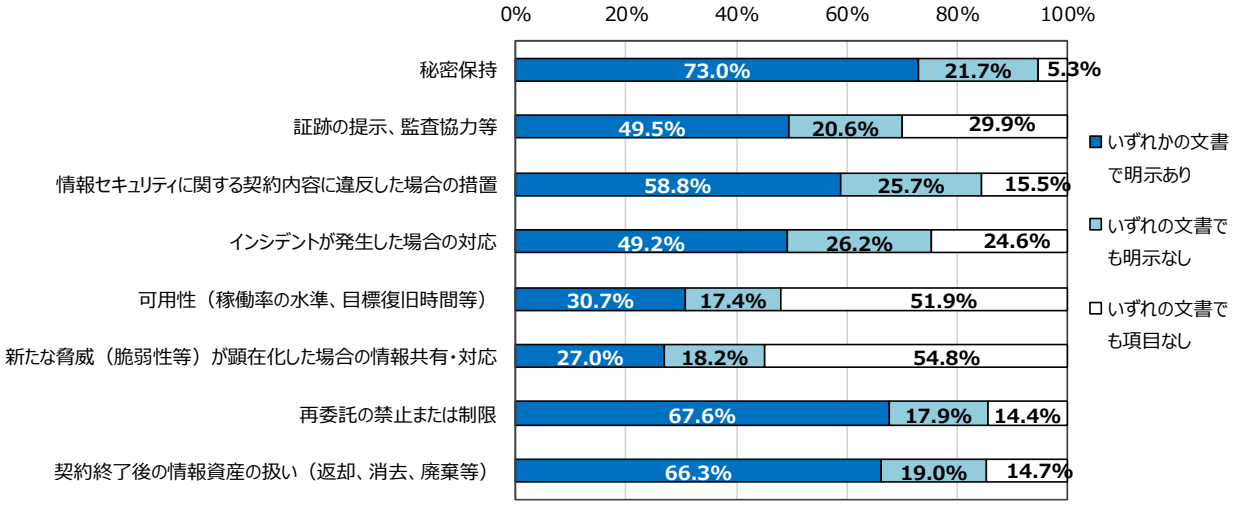
（2）全体の傾向

分析対象の事例、委託元 313 件、委託先 374 件について、契約関連文書における責任範囲の明確化の状況（記載されている文書は問わない。以下同じ。）を分析した結果は、次の**図表 3-37**、**図表 3-38** のとおりである。なお、グラフの凡例は、調査対象の契約関連文書（**図表 1-12**）のいずれかに、調査対象の情報セキュリティ要求事項（**図表 1-11**）の具体的な責任範囲を明示していた場合を「いずれかの文書で明示あり」、項目はあるがその記載は都度調整などで具体的な責任範囲までは明示していた場合を「いずれの文書でも明示なし」、いずれの文書にも項目が無かった場合を「いずれかの文書でも項目なし」とした。

全体の「明示あり」の回答の傾向について、委託元（**図表 3-37**）と委託先（**図表 3-38**）を比較すると、全ての情報セキュリティ要求事項について、委託元よりも委託先のほうが「明示あり」の比率が高い。



図表 3-37 責任範囲の明確化の状況（委託元調査・全体） N=313



図表 3-38 責任範囲の明確化の状況（委託先調査・全体） N=374

(3) IT システム・サービスの種類ごとの傾向

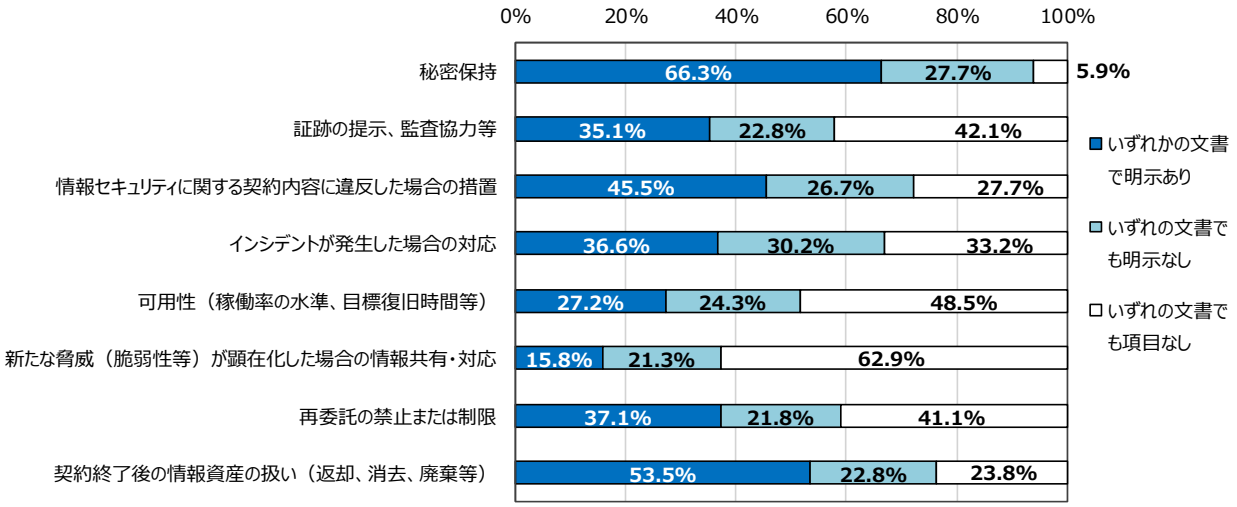
① 分析対象の IT システム・サービスの種類

委託元の事例 313 件のうち、211 件（67.4%）は、システム運用・管理、アプリケーション保守、ソフトウェアサポートサービス、ハードウェア保守の 4 業務の中から 2 業務以上を含んだ業務委託契約の事例であった。また、ソフトウェア開発と他の業務を同時に契約している事例が多く、単独で契約されている比率が高かったのは、システム運用・管理、サービス提供（ASP、SaaS 等）、データ処理・分析だった。他の業務と同時に契約されていることの多い業務を分析した場合、IT システム・サービスの種類ごとの責任範囲の明確化の差は表れにくいと判断し、

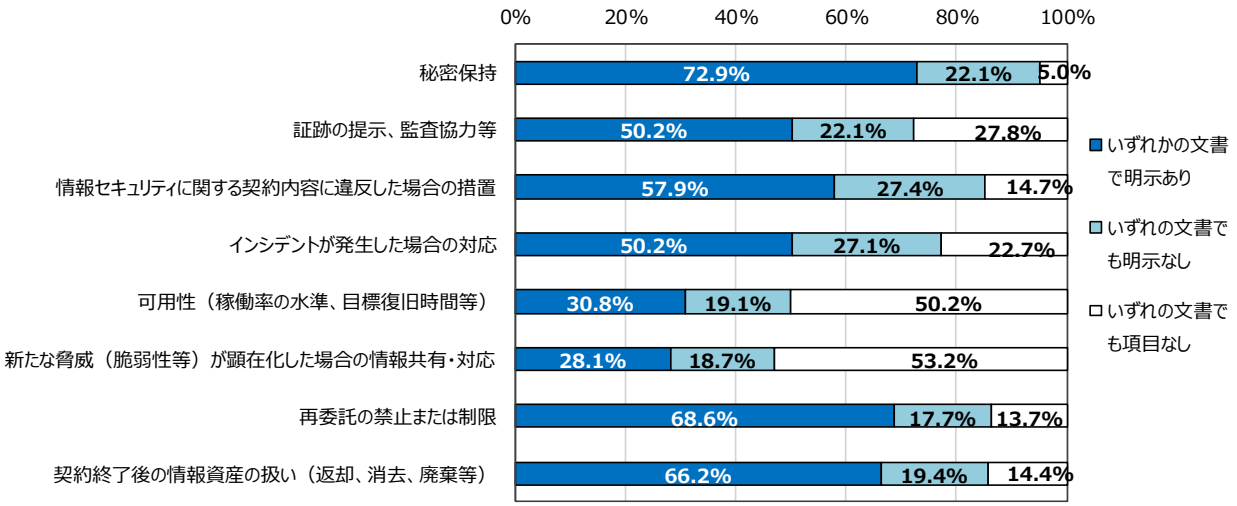
ここでは、委託元、委託先ともに事例件数の多いソフトウェア開発と、ソフトウェア開発と同時に契約される比率の低い、システム運用・管理、サービス提供（ASP、SaaS 等）、データ処理・分析に絞って分析することとした。

② ソフトウェア開発を含む事例

ソフトウェア開発を含む事例で、責任範囲の明確化の状況を分析した結果は、次の**図表 3-39**、**図表 3-40** のとおりである。（2）の全体の傾向と同様、委託先（**図表 3-40**）のほうが委託元（**図表 3-39**）よりも「明示あり」の比率が高い傾向にある。



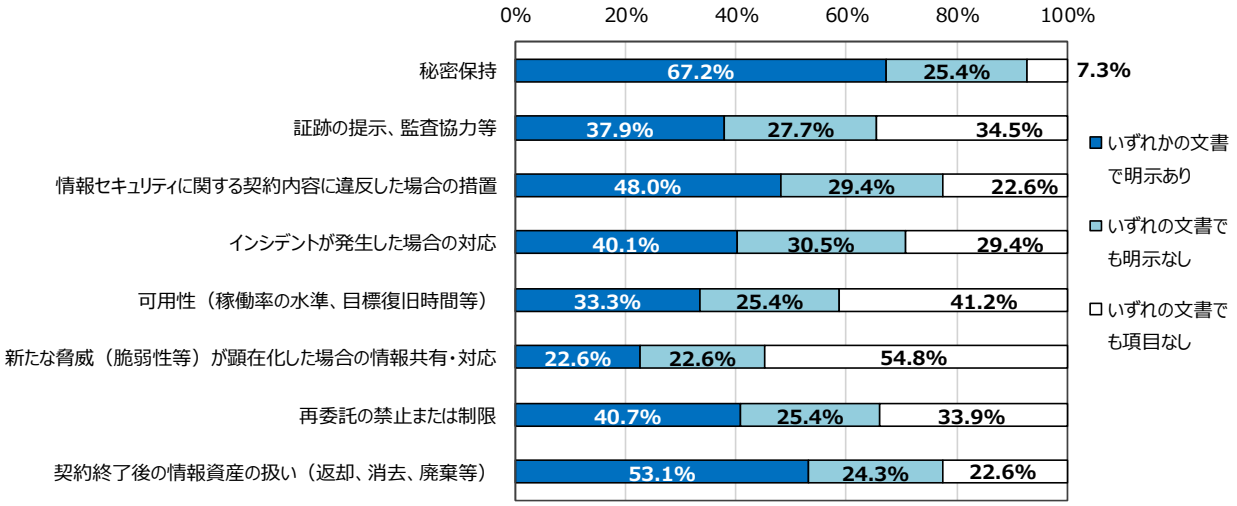
図表 3-39 責任範囲の明確化の状況（委託元調査・ソフトウェア開発） N=202



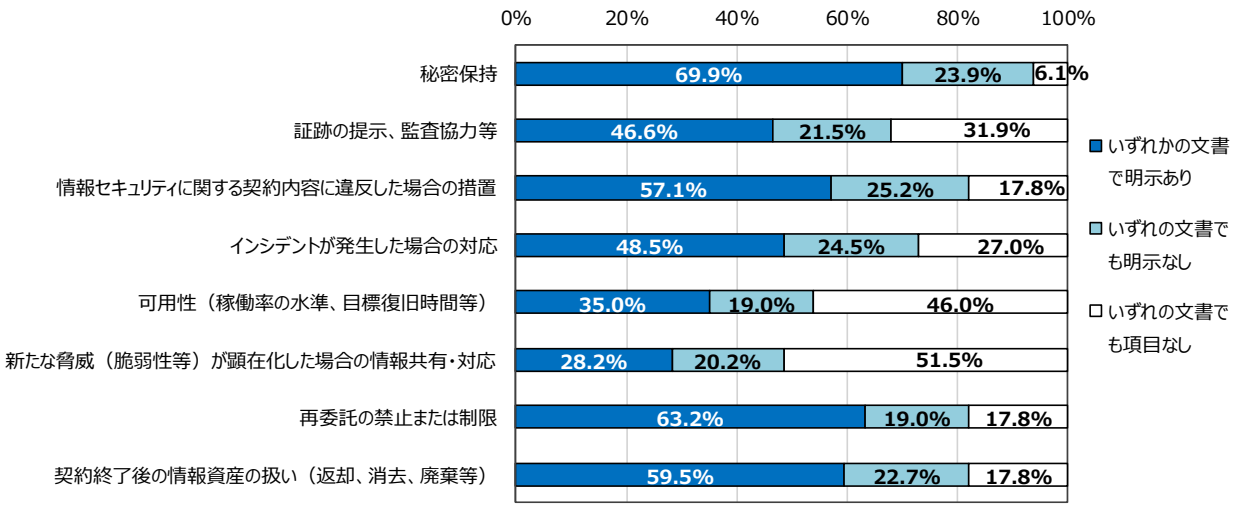
図表 3-40 責任範囲の明確化の状況（委託先調査・ソフトウェア開発） N=299

③ システム運用・管理を含む事例

システム運用・管理を含む事例で、責任範囲の明確化の状況を分析した結果は、次の**図表 3-41**、**図表 3-42** のとおりである。委託元（**図表 3-41**）の分析結果を見ると、「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」の「明示あり」の割合は 22.6%であり、**図表 3-39** のソフトウェア開発の場合（15.8%）よりも 7%程度高かった。



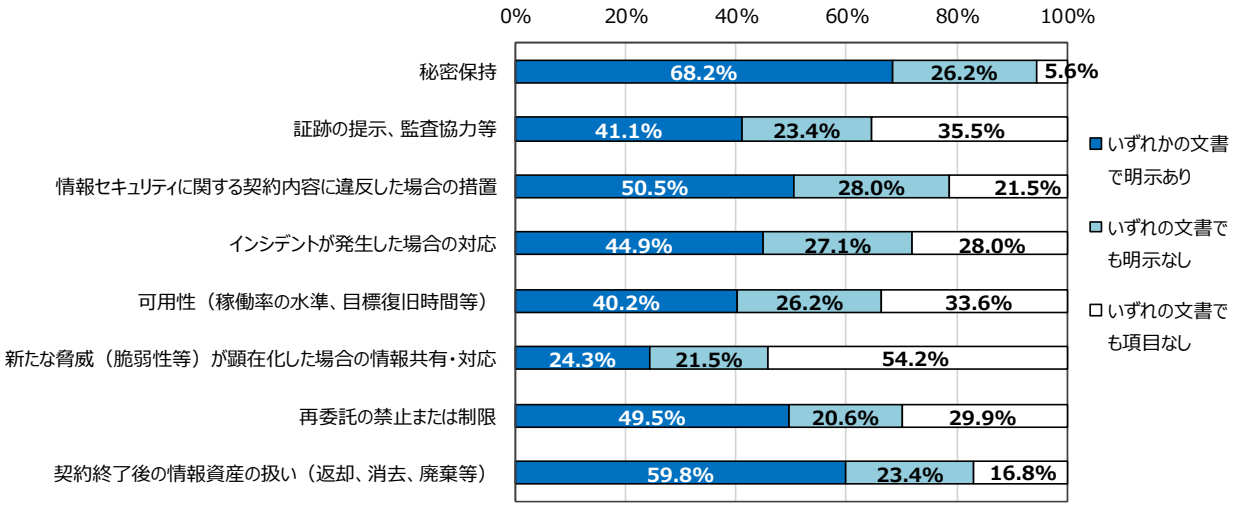
図表 3-41 責任範囲の明確化の状況（委託元調査・システム運用・管理） N=177



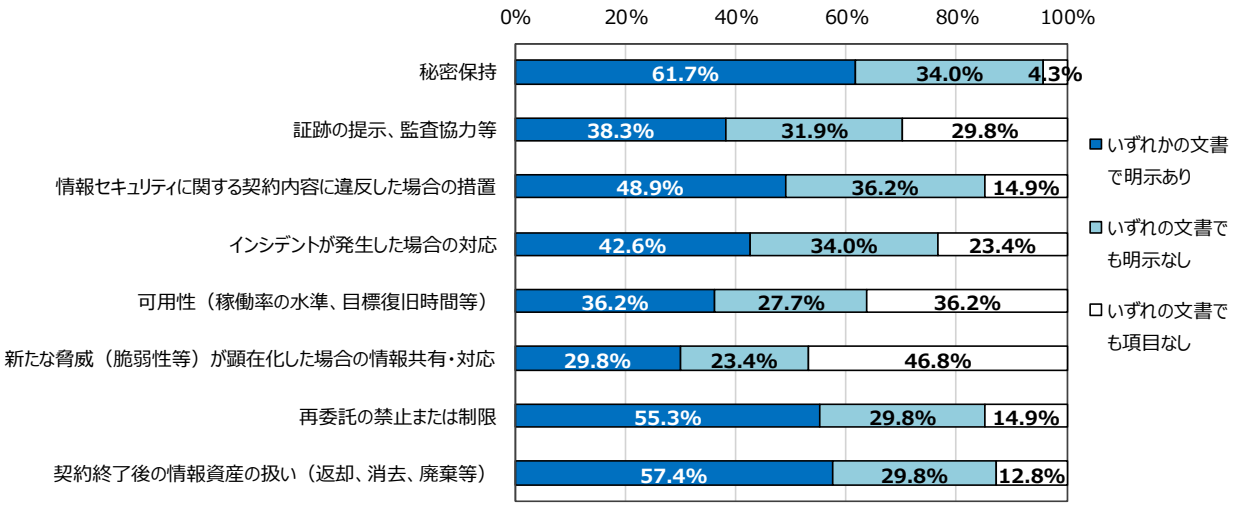
図表 3-42 責任範囲の明確化の状況（委託先調査・システム運用・管理） N=163

④ サービス提供（ASP、SaaS 等）を含む事例

サービス提供（ASP、SaaS 等）を含む事例で、責任範囲の明確化の状況を分析した結果は、次の**図表 3-43**、**図表 3-44** のとおりである。委託元（**図表 3-43**）について「可用性（稼働率の水準、目標復旧時間等）」の責任範囲の明確化の状況をみてみると、「明示あり」の割合は 40.2%で、**図表 3-39** のソフトウェア開発の場合（27.2%）よりも 10%以上高かった。委託先（**図表 3-44**）でも、「可用性（稼働率の水準、目標復旧時間等）」の「明示あり」の割合は 36.2%であり、**図表 3-40** のソフトウェア開発の場合（30.8%）よりも 5%程度高かった。



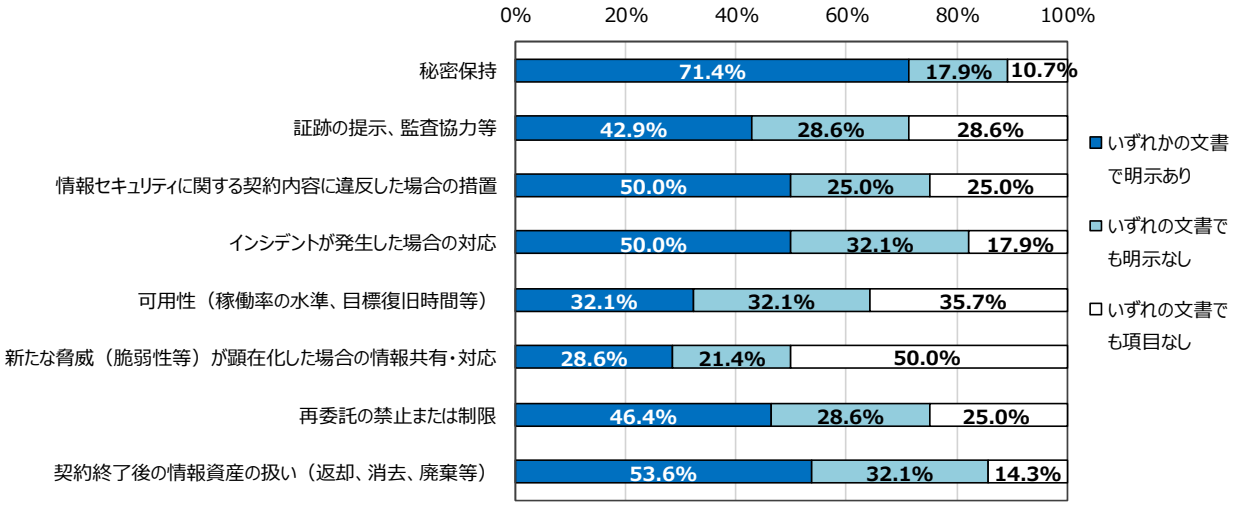
図表 3-43 責任範囲の明確化の状況（委託元調査・サービス提供） N=107



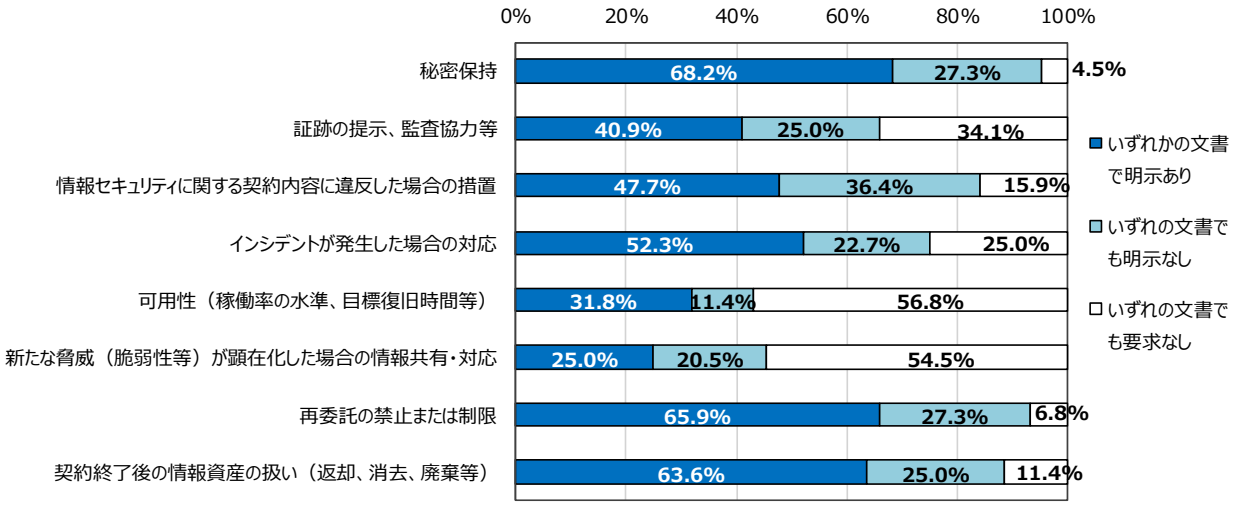
図表 3-44 責任範囲の明確化の状況（委託先調査・サービス提供） N=47

⑤ データ処理・分析を含む事例を含む事例

データ処理・分析を含む事例で、責任範囲の明確化の状況を分析した結果は、次の**図表 3-45**、**図表 3-46** のとおりである。委託元（**図表 3-45**）について「再委託の禁止または制限」の責任範囲の明確化の状況をみてみると、「明示あり」の割合は 46.4%で、**図表 3-39** のソフトウェア開発の場合（37.1%）よりも 10%近く高かった。



図表 3-45 責任範囲の明確化の状況（委託元調査・データ処理・分析） N=28

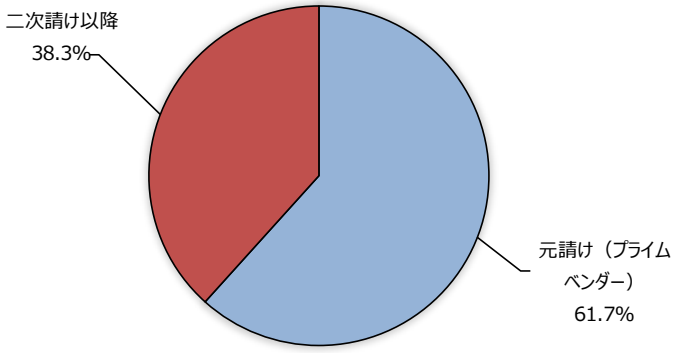


図表 3-46 責任範囲の明確化の状況（委託先調査・データ処理・分析） N=44

3.5.3　委託元の業種と責任範囲と明確化の状況に関する分析（委託先調査）

（1）IT サプライチェーンにおける位置付け

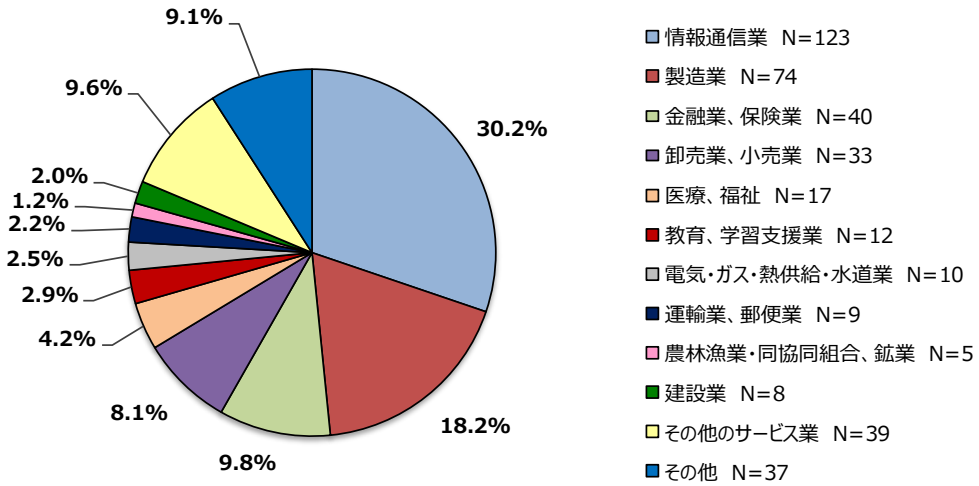
委託先調査では、IT サプライチェーン上の位置づけを調査した。その結果は、**図表 3-47** のとおり、元請け（プライムベンダー）が 61.7%（251 件）、二次請け以降が 38.3%（156 件）であった。



図表 3-47 サプライチェーンにおける位置づけ（委託先調査）　N=407

（2）委託元の業種

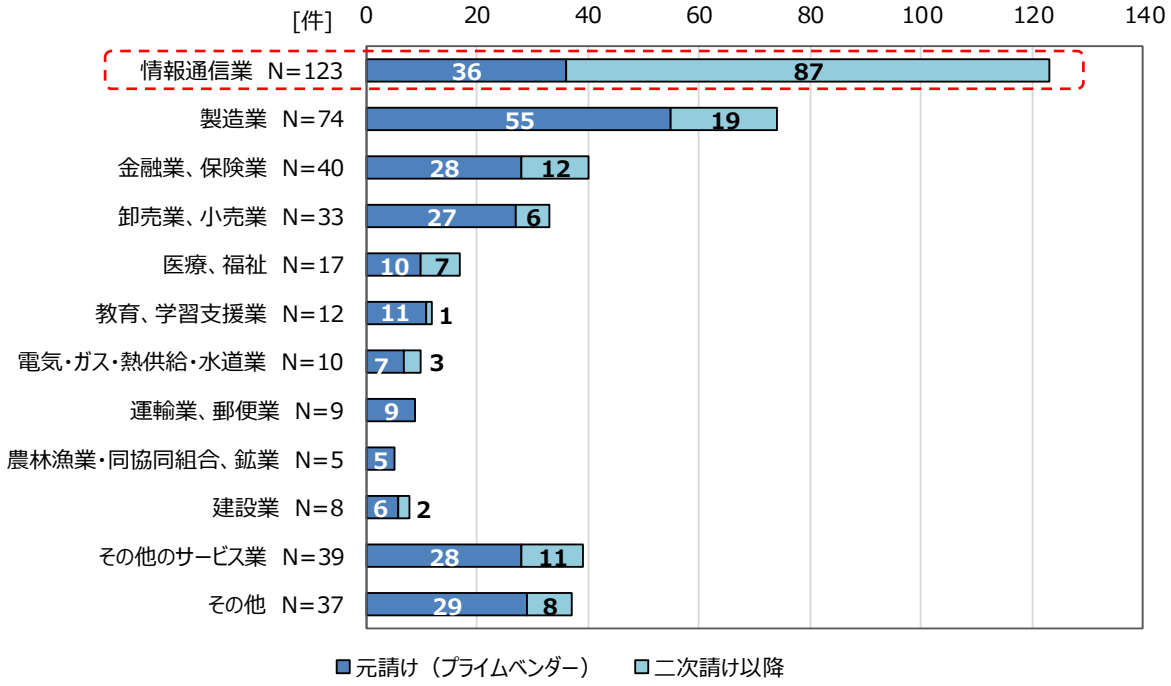
委託先調査では、委託元の業種（以下「委託元業種」とする。）を調査した。その結果は、**図表 3-48** のとおり、407 件のうち情報通信業が 123 件（30.2%）で最も多かった。



図表 3-48 委託元の業種（委託先調査）　N=407

(3) IT サプライチェーン上の位置付けと委託元の業種の関係

委託先調査において、回答企業の IT サプライチェーン上の位置付けと委託元業種の関係を分析した結果は、次の**図表 3-49** のとおりである。**図表 3-49** をみると、委託元業種が情報通信業である事例 123 件のうち 70.7%（87/123 件）が二次請け以降の事例である。他の委託元業種と比較しても、情報通信業が委託元業種である事例は、二次請け以降の占める比率が高いことが分かる。



図表 3-49 IT サプライチェーン上の位置付けと委託元の業種の関係（委託先調査） =407

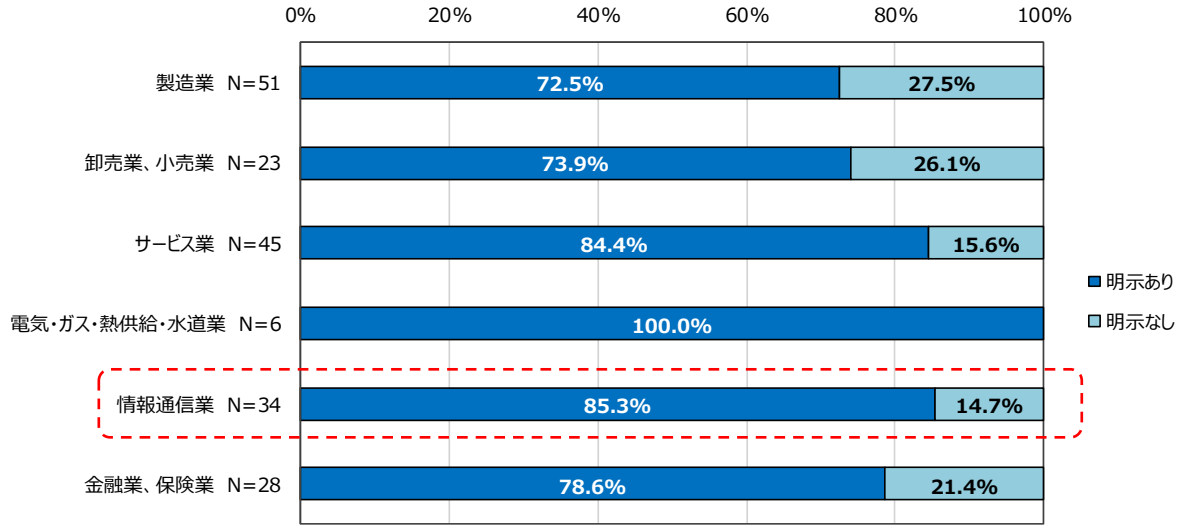
(4) 委託元企業の業種と責任範囲の明確化の状況

3.5.2 の IT システム・サービスごとの責任範囲の明確化の状況の分析では、委託元調査の結果（**図表 3-37**）と委託先調査の結果（**図表 3-38**）を比較した場合に、委託先のほうが「明示あり」とする回答が多い傾向があることを述べた。

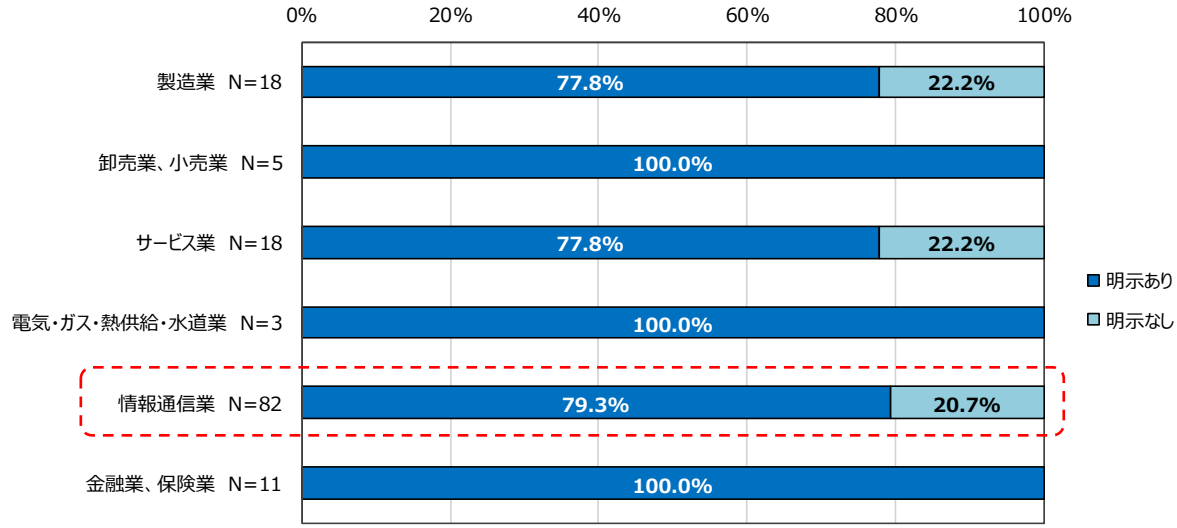
委託元に比べて「明示あり」の回答の比率が高い理由として、委託元業種が情報通信業である事例の比率が高いことが考えられる。2017 年度調査の調査結果では、情報通信業は情報セキュリティ要求が厳しい傾向があることが分かっている。

そこで、委託元の業種と IT サプライチェーン上の位置付けで層別し、責任範囲の明確化の状況（契約関連文書および情報セキュリティ要求事項を問わない）を分析した。分析する業種は、委託元調査で調査対象にした製造業、卸売業・小売業、サービス業の 3 業種と、情報通信業および情報通信業と同様に社会インフラ系の業種である金融業・保険業、電気・ガス・熱供給・水道業とした。

分析の結果は、次の**図表 3-50**、**図表 3-51** のとおりである。



図表 3-50 委託元の業種と責任範囲の明確化の状況（委託先調査・プライムベンダー） N=187



図表 3-51 委託元の業種と責任範囲の明確化の状況（委託先調査・二次請け以降） N=137

情報通信業は、プライムベンダーの場合（**図表 3-50**）は 85.3%、二次請け以降の場合（**図表 3-51**）は 79.3%とともに高い比率で責任範囲を明示していることが分かる。

委託元調査は、調査対象業種を、製造業、卸売業・小売業、サービス業の 3 業種に絞ったが、委託先調査は委託元の業種を絞らずに調査を行ったため、収集した事例のおよそ 3 分の 1 が情報通信業となった。さらに、**図表 3-50**、**図表 3-51** のとおり、委託元業種が情報通信業の場合、プライムベンダーの場合も二次請け以降の場合も高い比率で責任範囲を明示していた。その結果、委託元調査の結果（**図表 3-37**）よりも委託先調査の結果（**図表 3-38**）の方が「明示あり」の回答の比率が高くなったものと考える。

なお、情報通信業以外と同じく社会インフラ系の業種である金融業・保険業、電気・ガス・熱供

給・水道業も、プライムベンダーの場合も二次請け以降の場合も、委託元調査の対象業種（製造業、卸売業・小売業、サービス業）よりも「明示あり」の回答の比率が高い傾向にある。責任範囲の明確化の状況は、社会インフラ系の業種か否かによって傾向が異なると言える。

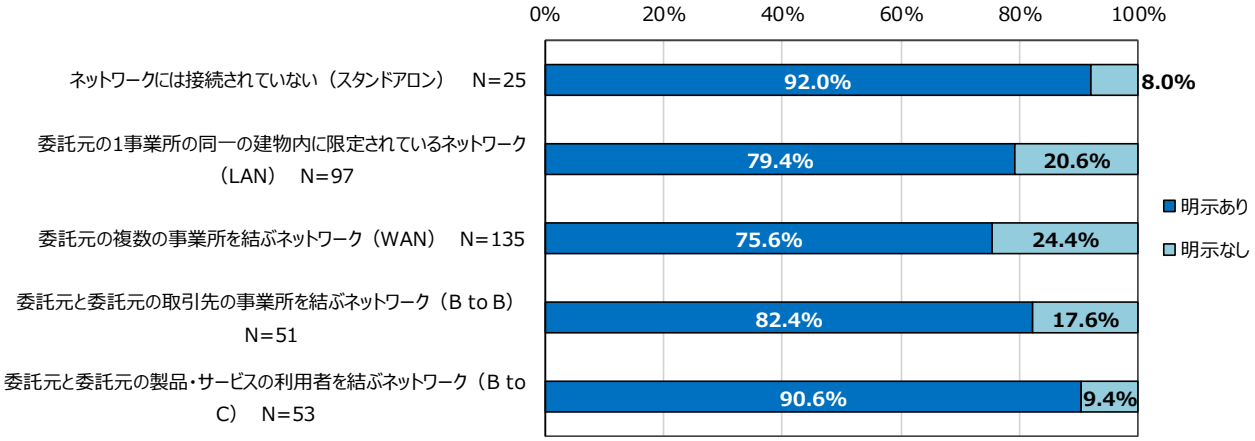
3.5.4　ネットワークの範囲と責任範囲の明確化の状況に関する分析

（1）ネットワークの範囲と責任範囲の明確化の状況

ビジネスにインターネットを使用する目的は、①不特定多数の顧客との商取引の実現、②商取引の機会の拡大（時間的制約、地理的制約の低減）、③事業の効率化によるコスト削減等が考えられるが、EC サイト等でビジネスを行う場合等は特に、情報セキュリティ上のリスクが大きくなる。

アンケート調査では、ネットワークの範囲によって情報セキュリティ対策に違いがあることが想定されるため、IT 業務委託の事例に関する調査項目として、当該 IT システム・サービスのネットワークの範囲を尋ねた。

委託先調査におけるネットワークの範囲ごとの責任範囲の明確化の状況の調査結果は、次の**図表 3-52** のとおりである。

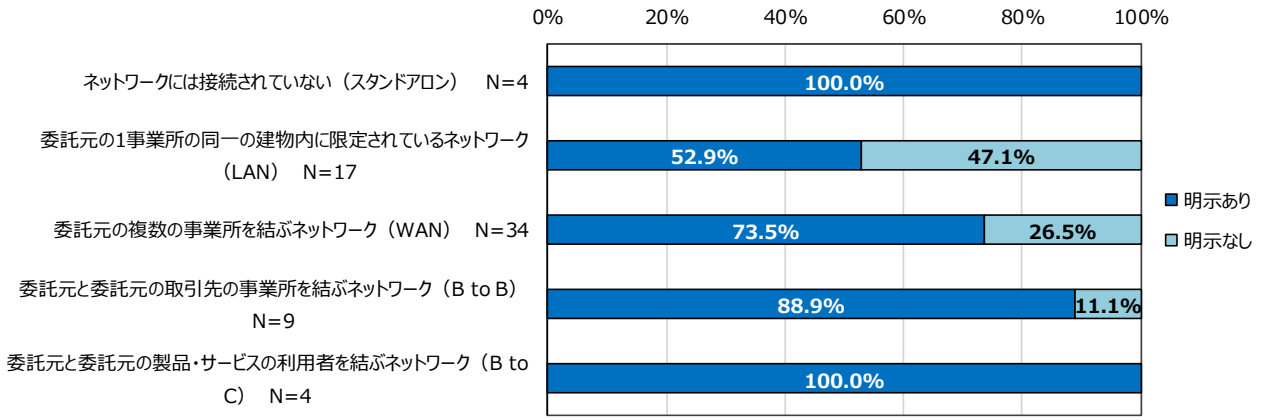


※責任範囲の明示の有無について回答のなかった 46 件を集計から除いている

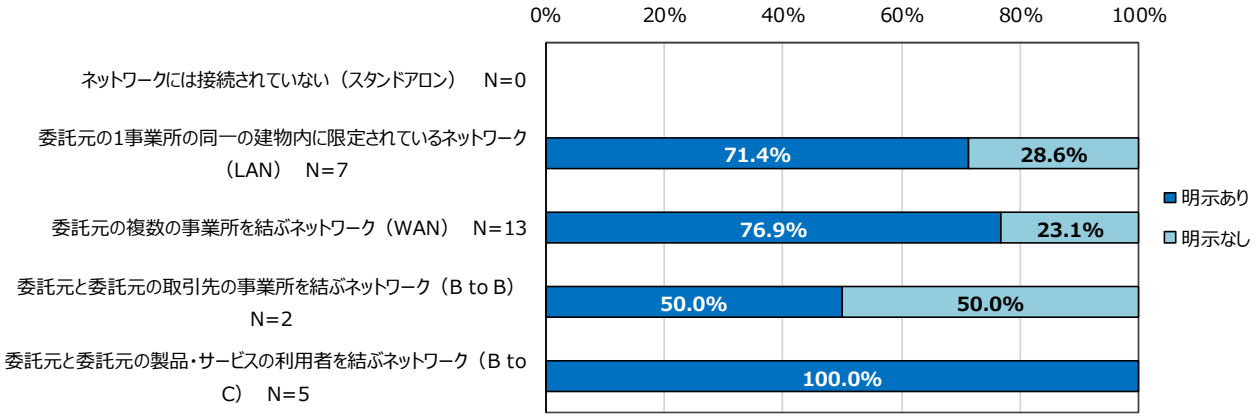
図表 3-52 ネットワークの範囲ごとの責任範囲の明確化の状況（委託先調査）　N=361

（2）業種ごとのネットワークの範囲と責任範囲の明確化の状況

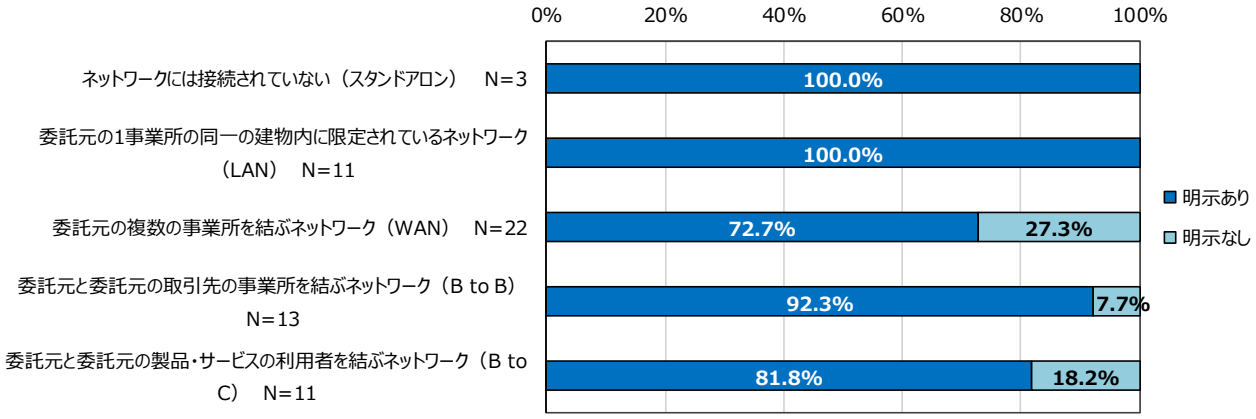
さらに、業種ごとのネットワークの範囲によって、責任範囲の明確化の状況に違いがあるかどうかについて、分析したものが、次の**図表 3-53～3-55** である。製造業（**図表 3-53**）は、業種を絞る前（**図表 3-52**）に比べネットワークの範囲による責任範囲明確化の状況の違いがより顕著であった。



図表 3-53 ネットワークの範囲ごとの責任範囲の明確化の状況（委託先調査・委託元が製造業） N=68



図表 3-54 ネットワークの範囲ごとの責任範囲の明確化の状況（委託先調査・委託元が卸売業、小売業） N=27

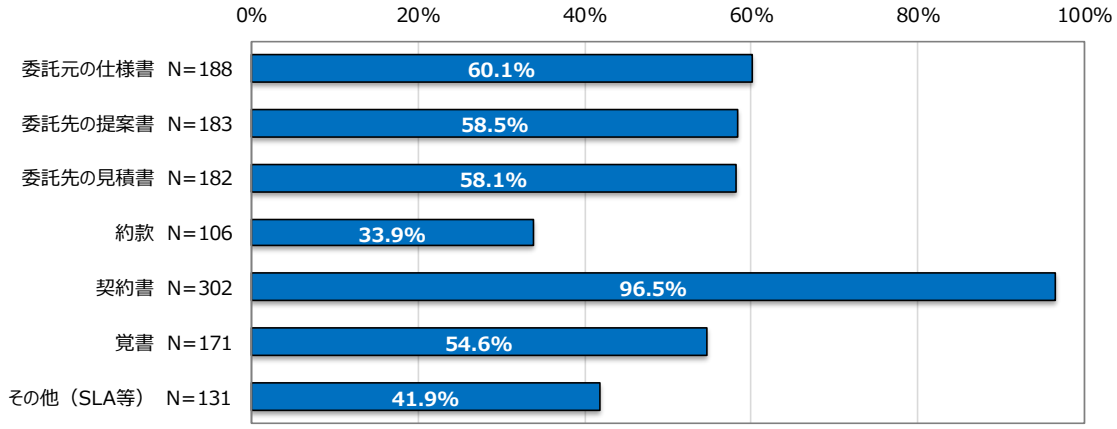


図表 3-55 ネットワークの範囲ごとの責任範囲の明確化の状況（委託先調査・委託元がサービス業） N=60

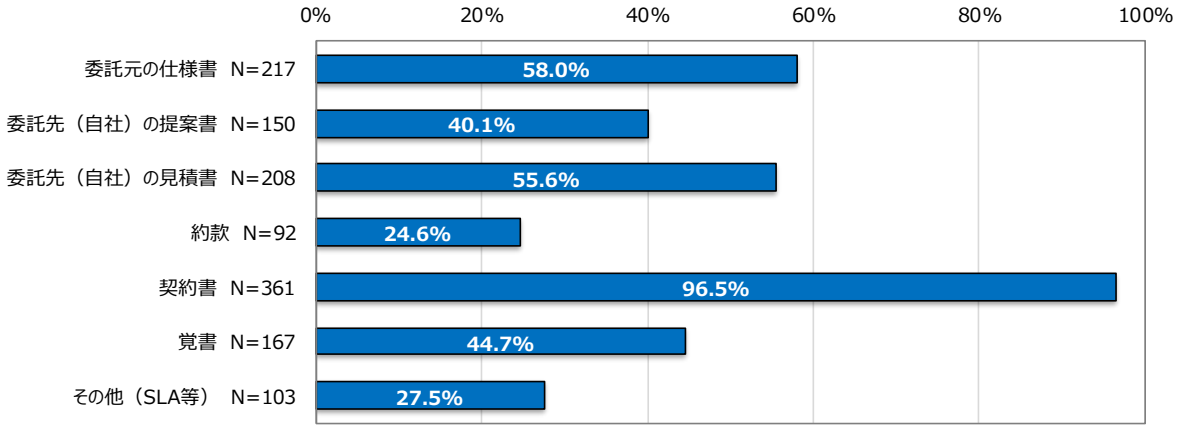
3.5.5　契約書の書式と責任範囲を明確化の状況に関する分析

(1) 契約に使用した文書

契約関連文書の使用状況に関する調査結果は、次の**図表 3-56**、**図表 3-57** のとおりである。使用された契約関連文書は、委託元、委託先ともに契約書が最も多かった。



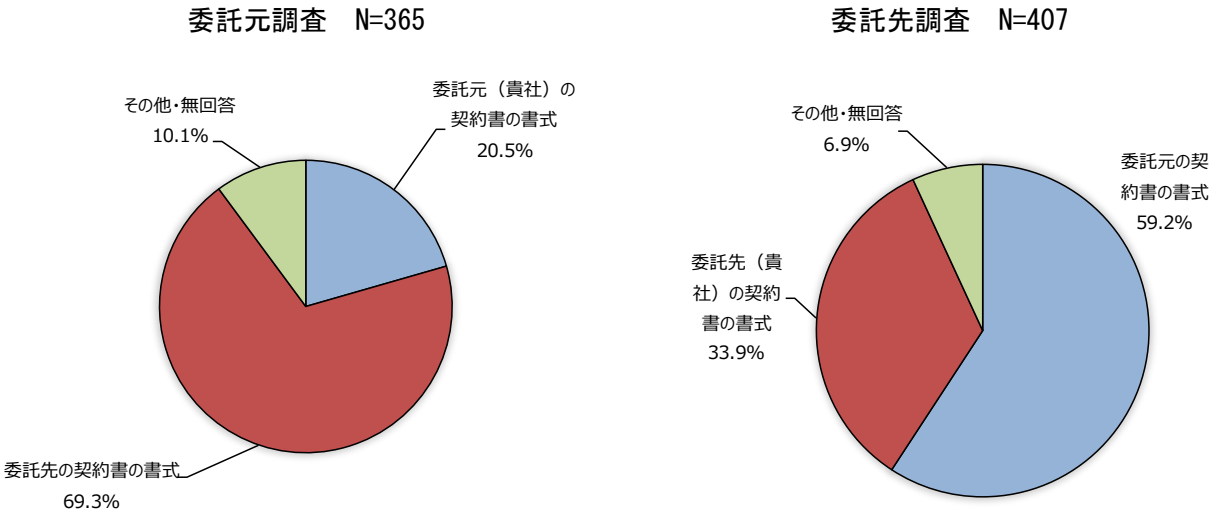
図表 3-56 契約に使用した文書（委託元調査）　N=313



図表 3-57 契約に使用した文書（委託先調査）　N=374

（2）契約に使用した契約書の書式

前述のとおり、業務委託契約の交渉は、ベースとなる契約書の雛形を最初に提示した方に有利に交渉が進んでいくことが多い。事例の調査では、当該事例で仕様した契約書の書式が、委託元のものであるか、委託先のものであるかについても調査した。その調査結果は、次の図表 3-58 のとおりである。委託元は 69.3%が委託先の書式を使用しているのに対し、委託先は 59.2%が委託元の書式を使用しており、全く逆の傾向となった。



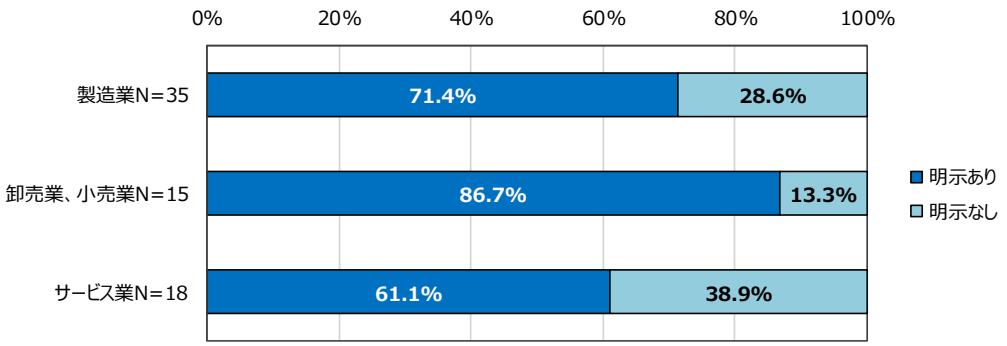
図表 3-58　契約書の書式

（3）契約に使用した契約書の書式ごとの責任範囲の明確化の状況の分析

3.5.3 の分析で、委託元の業種により責任範囲の明確化の状況が異なる傾向があることが分かったため、3.5.3 の分析と同じ業種について、責任範囲の明確化の状況（情報セキュリティ要求事項及び文書は問わない）を、委託元の業種及び使用された契約書が委託元と委託先のどちらの書式であったかで層別して分析した。その結果は、次の**図表 3-59～図表 3-62** のとおりである。

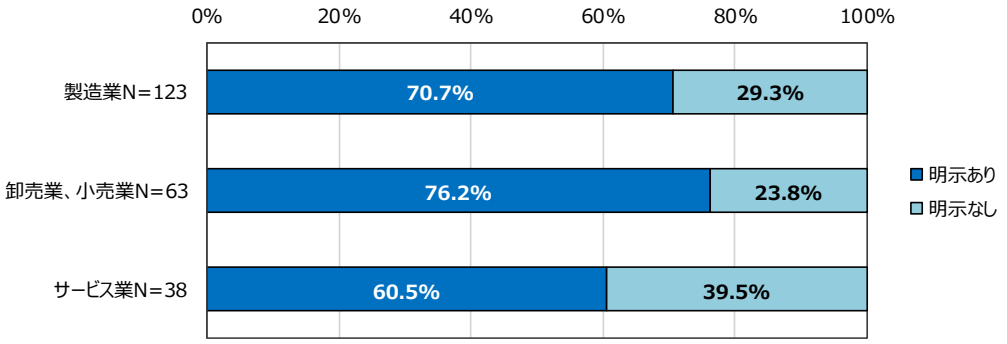
委託元調査の委託元の書式を使用した場合（**図表 3-59**）と委託先の書式を使用した場合（**図表 3-60**）を比較した場合、事例の件数は、3 業種とも委託先の書式を使用した事例のほうが多くなっている。また、責任範囲の明確化の状況は、卸売業・小売業の場合に、委託先の書式を使用したほうが若干「明示あり」の比率が低い傾向が見られるが、他の 2 業種は大きな差はない。

一方、委託先調査の委託元の書式を使用した場合（**図表 3-61**）と委託先の書式を使用した場合（**図表 3-62**）を比較した場合、委託元業種が、製造業、サービス業、情報通信業、金融業・保険業の場合に、委託先の書式を使用したほうが若干「明示あり」の比率が低い傾向が見られる。



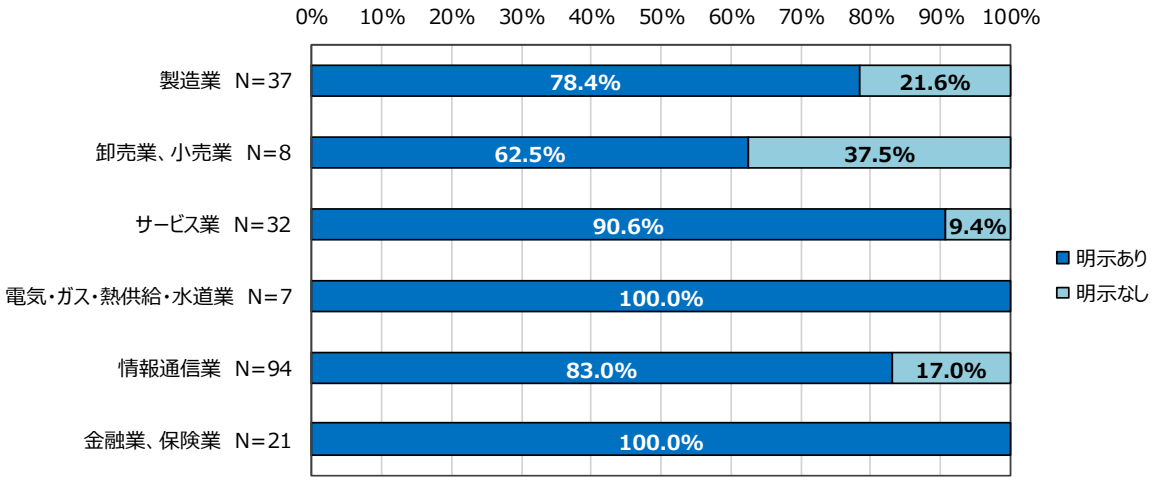
図表 3-59 契約書の書式と責任範囲の明確化の状況（委託元調査・委託元の書式を使用した場合）

N=68



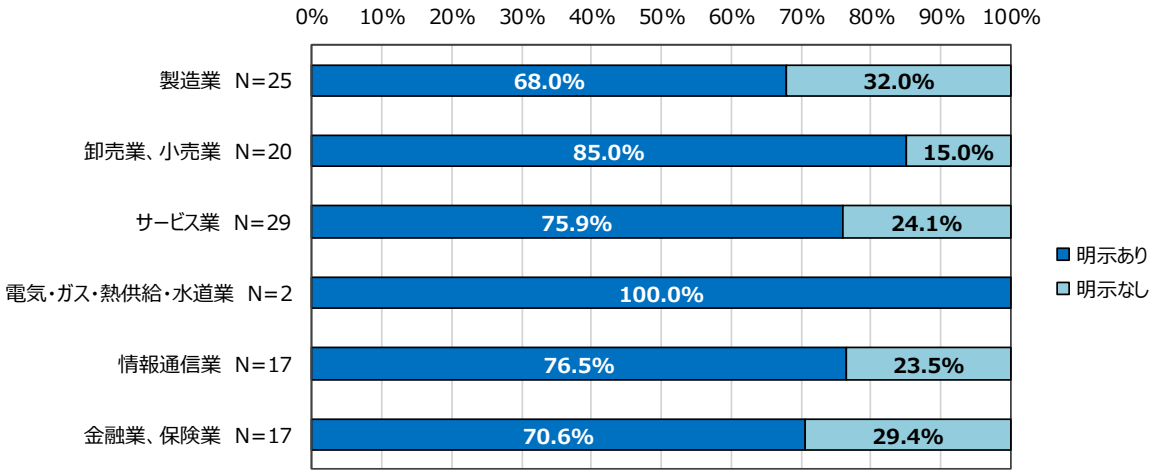
図表 3-60 契約書の書式と責任範囲の明確化の状況（委託元調査・委託先の書式を使用した場合）

N=224



図表 3-61 契約書の書式と責任範囲の明確化の状況（委託先調査・委託元の書式を使用した場合）

N=199

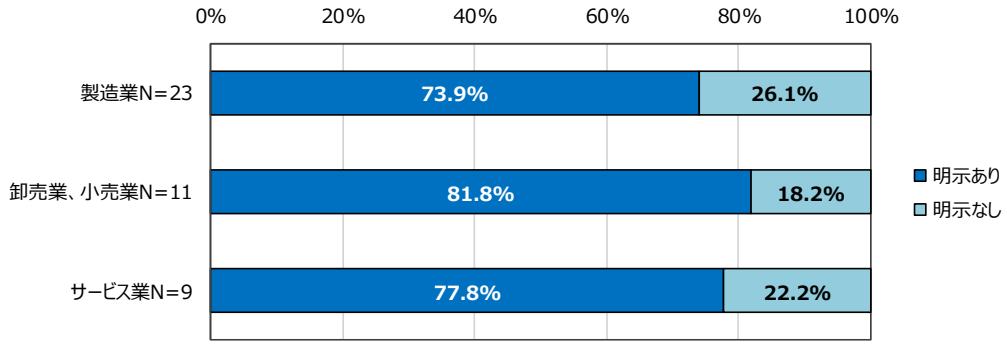


図表 3-62 契約書の書式と責任範囲の明確化の状況（委託先調査・委託先の書式を使用した場合）
N=110

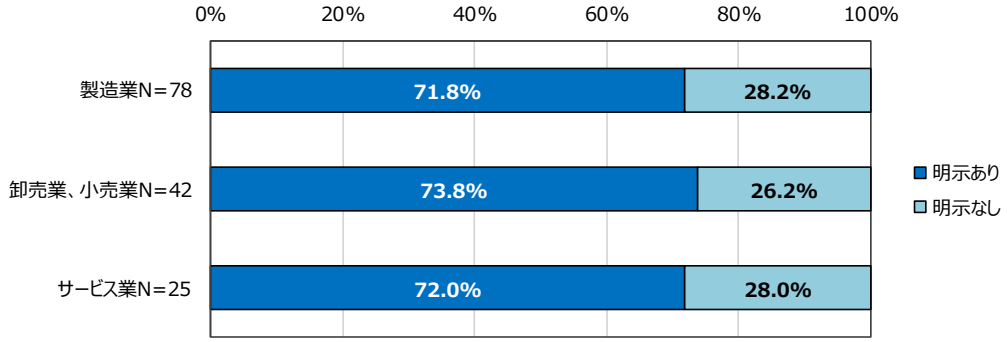
（4）契約に使用した契約書の書式ごとの責任範囲の明確化の状況の分析（ソフトウェア開発を含む事例）

委託先調査の**図表 3-61** と**図表 3-62** を比較すると、委託元業種が製造業、サービス業、情報通信業、金融業・保険業の場合に、委託先の書式を使用したほうが「明示あり」の回答の比率が低かった。委託先調査の事例にソフトウェア開発を含む事例が多いことを考慮すると、ソフトウェア開発を含む事例で委託先の書式を使用して契約を結んだ場合に、責任範囲が明示されていない比率が高いことが推測される。そこで、委託元、委託先ともにソフトウェア開発を含む事例に絞り込んで契約書の書式と責任範囲の明確化の状況を分析した。その分析結果は、**図表 3-63**～**図表 3-66** のとおりである。

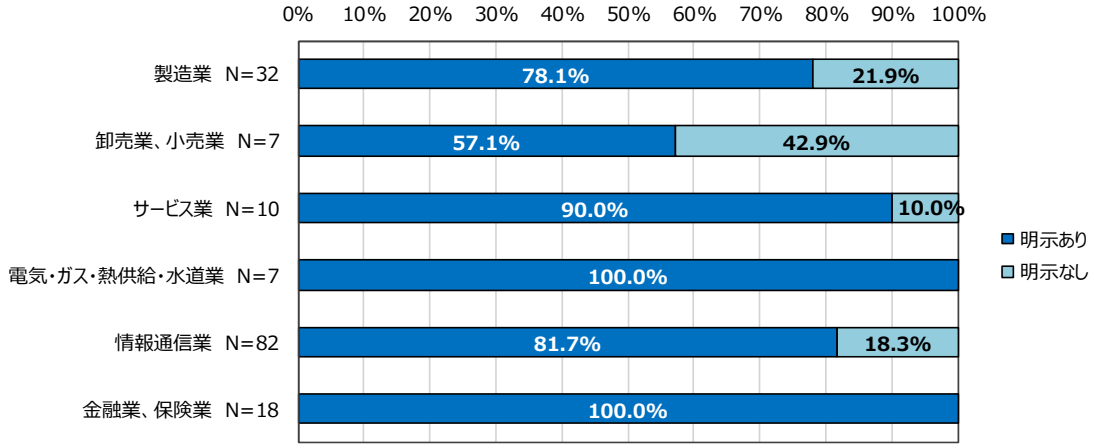
委託元調査の分析結果（**図表 3-63**、**図表 3-64**）は、ソフトウェア開発を含む事例に絞り込む前の**図表 3-59**、**図表 3-60** の場合と同様に、卸売業・小売業の場合に、委託先の書式を使用したほうが「明示あり」の比率が若干低い傾向が見られた。一方、委託先調査の分析結果（**図表 3-65**、**図表 3-66**）は、ソフトウェア開発を含む事例に絞り込む前の**図表 3-61**、**図表 3-62** と比較すると、使用した書式による傾向の違いは大きく変わらなかったが、全般的に委託先の書式を使用したほうが「明示あり」の比率が小さくなっている業種が多かった。



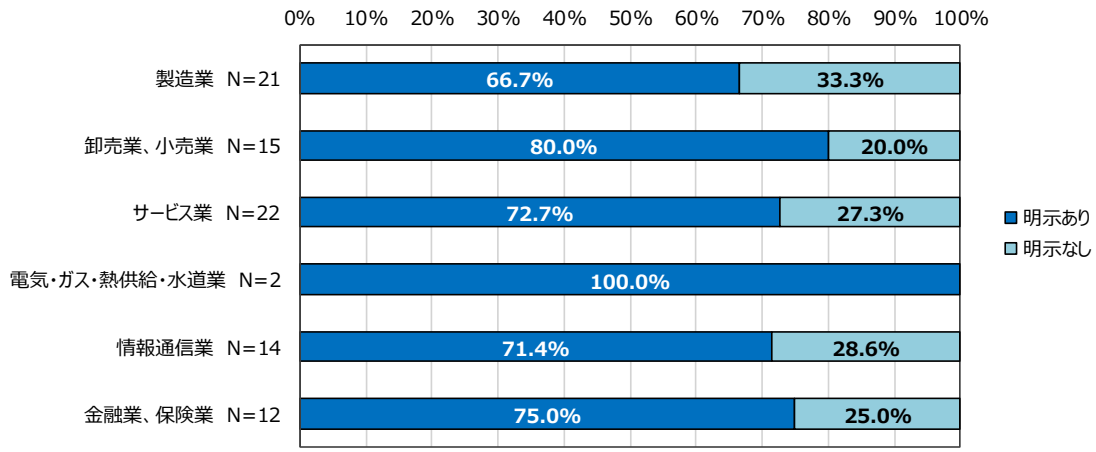
図表 3-63 契約書の書式と責任範囲の明確化の状況（委託元調査・ソフトウェア開発を含む事例で委託元の書式を使用した場合） N=43



図表 3-64 契約書の書式と責任範囲の明確化の状況（委託元調査・ソフトウェア開発を含む事例で委託先の書式を使用した場合） N=145



図表 3-65 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例で委託元の書式を使用した場合） N=156



図表 3-66 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例で委託先の書式を使用した場合） N=86

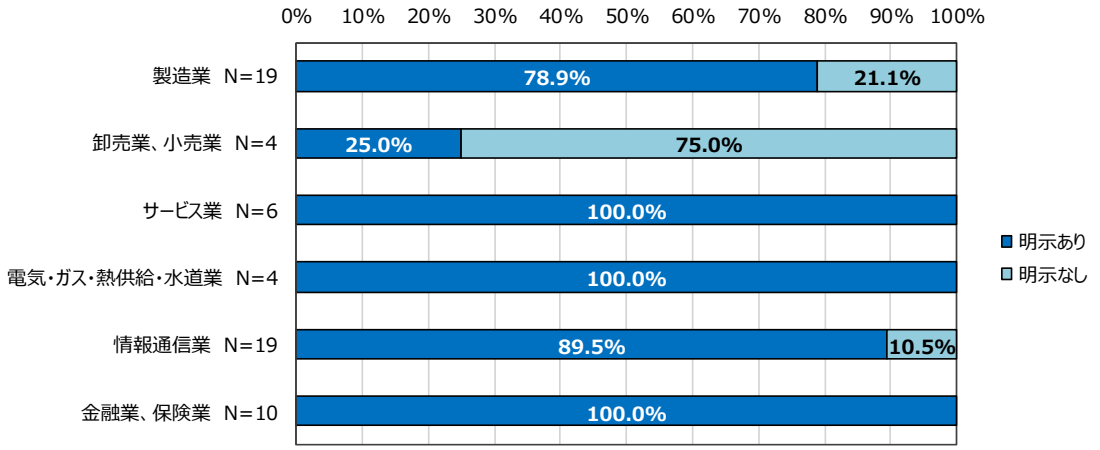
（5）契約に使用した契約書の書式ごとの責任範囲の明確化の状況の分析（ソフトウェア開発を含む事例・プライムベンダー）

3.5.3 の分析では、委託先調査において、委託元業種及び IT サプライチェーン上の位置付けで責任範囲の明確化の状況を分析した。その結果、社会インフラ系の業種である金融業・保険業、電気・ガス・熱供給・水道業の場合に、プライムベンダーの場合も二次請け以降の場合も「明示あり」の回答の比率が高い傾向にあるが分かった。

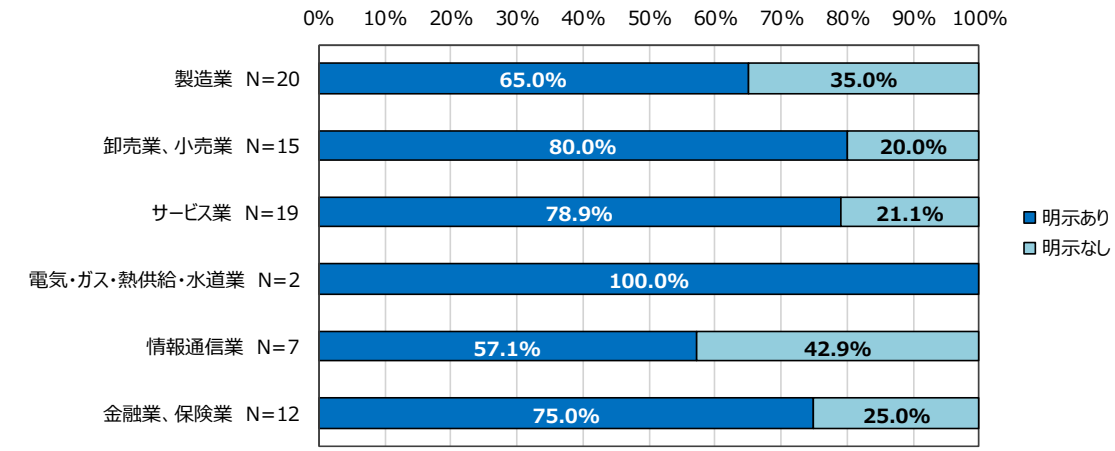
図表 3-65 と**図表 3-66** で業種ごとの事例の件数比率を比較すると、卸売業、小売業、サービス業は、委託先の書式を使用している事例の比率が高く（卸売業、小売業 委託元の書式使用 7/156 = 0.04 委託先の書式使用 15/86 = 0.17、サービス業 委託元の書式使用 10/156 = 0.06 委託先の書式使用 22/86 = 0.26）、一方、情報通信業の場合は、委託元の書式を使用している事例の比率が高くなっているのが分かる（情報通信業 委託元の書式使用 82/156 = 0.53 委託先の書式使用 14/86 = 0.16）。そこで、委託先調査の**図表 3-65** と**図表 3-66** の分析結果を、さらに IT サプライチェーン上の位置付けで層別し、責任範囲の明確化の状況を分析した。

その結果は、次の**図表 3-67～図表 3-70** のとおりである。プライムベンダーの場合、卸売業・小売業を除いて委託元の書式を使用したほうが「明示あり」の比率が高かった。二次請け以降のベンダの場合は、委託先の書式を使用した事例が少なく十分な比較ができないが、サービス業の場合は委託元の書式を使用したほうが「明示あり」の比率が高くなっている。また。二次請け以降のベンダが委託元の書式を使用している事例は 94 件で、分析対象事例 407 件の約 4 分の 1 である。

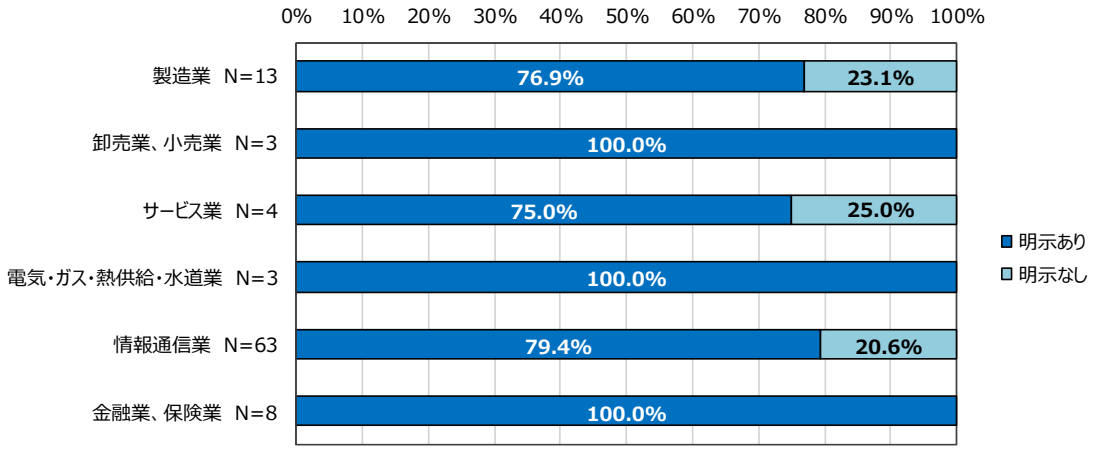
また、**図表 3-58** の契約に使用した書式に関する調査結果で、委託先調査の場合に、委託元の書式が使用されている事例の割合が高いのは、委託先調査の事例に二次請け以降のベンダの事例の割合が高いこと（**図表 3-47**）と、二次請け以降のベンダの場合に委託元の書式を使用することが多いことが要因であると推察する。



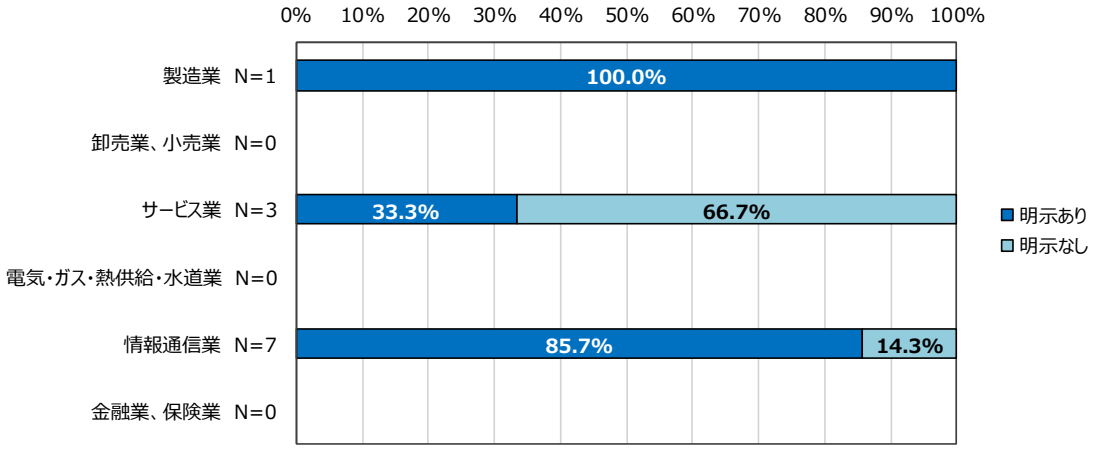
図表 3-67 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例でプライムベンダーが委託元の書式を使用した場合） N=62



図表 3-68 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例でプライムベンダーが委託先の書式を使用した場合） N=75



図表 3-69 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例で二次請け以降のベンダが委託元の書式を使用した場合） N=94



図表 3-70 契約書の書式と責任範囲の明確化の状況（委託先調査・ソフトウェア開発を含む事例でプ二次請け以降のベンダが委託先の書式を使用した場合） N=11

(6) まとめ

委託元調査で最も「明示あり」の比率が最も高いのは、**図表 3-59** のソフトウェア開発を含む事例に絞る前で委託先の書式を使用した場合の卸売業、小売業で 86.7%が「明示あり」であった。また、最も「明示あり」の比率が低いのは、ソフトウェア開発を含む事例に絞る前で委託先の書式を使用した場合を分析した**図表 3-60** のサービス業で 60.5%であった。

委託先調査で最も「明示あり」の比率が高いのは 100%で、**図表 3-65** の電気・ガス・熱供給・水道業など複数あった。一方、「明示あり」の比率が最も低いのは、件数が 4 件と少ないが、**図表 3-67** のソフトウェア開発を含む事例でプライムベンダーが委託元の書式を使用した場合の卸売業・小売業で 25.0%であった。

また、委託元調査の場合、ソフトウェア開発を含む事例に絞り込んだほうが「明示あり」の

比率が高くなり、委託元調査の場合は、ソフトウェア開発を含む事例に絞り込んだほうが「明示あり」の比率が低くなる傾向があった。

3.6 組織的なセキュリティ対策の実施状況

3.6.1 契約関連文書に明記されていた組織的な情報セキュリティ対策

(1) 設問の趣旨

アンケート調査では、IT 業務委託の事例に関して、契約関連文書に委託先が実施すべき組織的な情報セキュリティ対策が明記されていたかどうかを調査した。また、「委託先が実施すべき組織的な情報セキュリティ対策が明記されている」とした回答者に対しては、記載されている項目について調査した。この調査項目は、2017 年度調査では、委託元調査では「委託先（再委託先）が最低限実施すべき情報セキュリティ対策」、委託先調査では「受託業務において最低限実施する情報セキュリティ対策」として調査したものを継承した。

(2) 調査結果

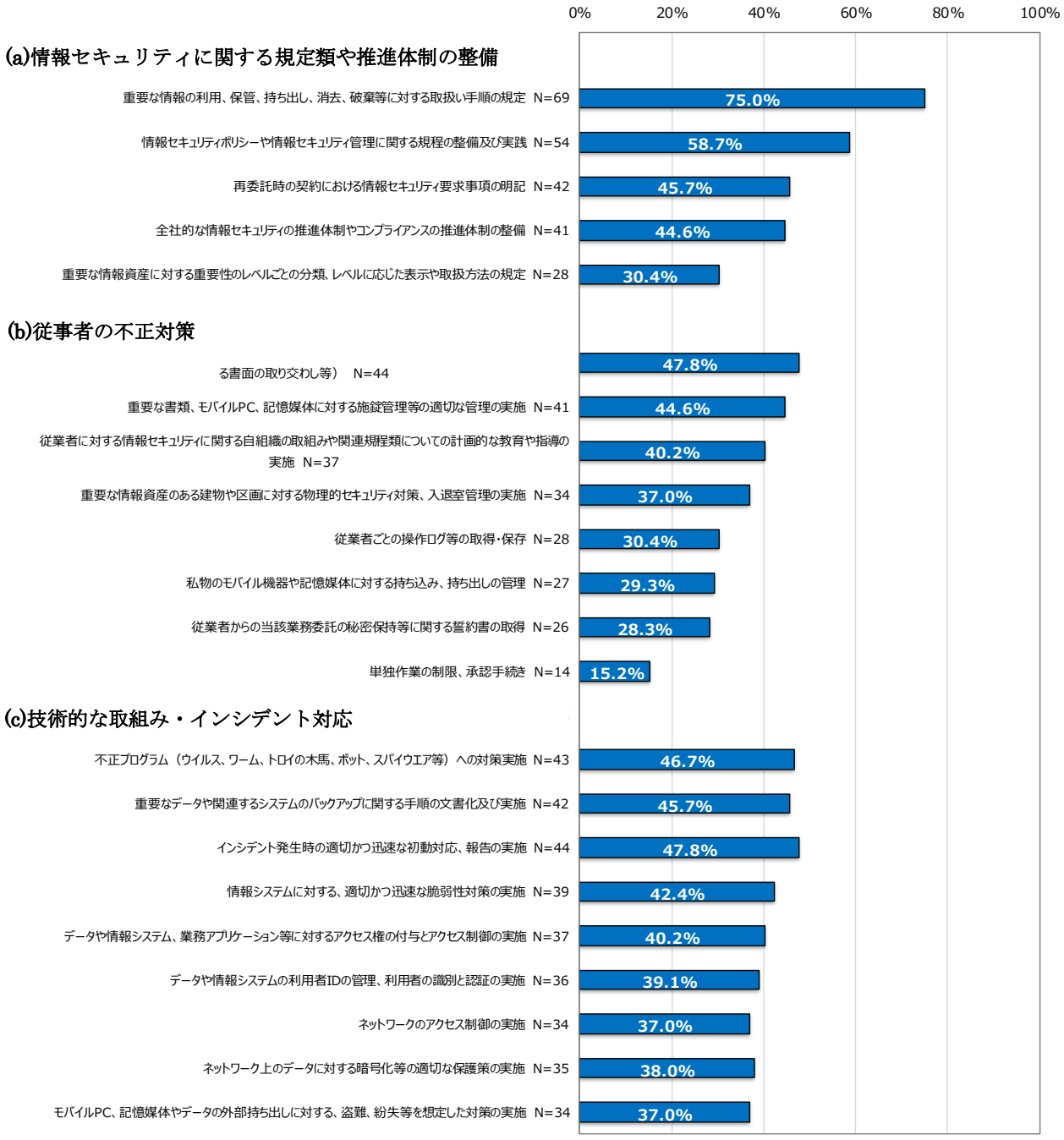
調査結果は、次の**図表 3-71**、**図表 3-72** のとおりである。

まず、(a) 情報セキュリティに関する規程類や推進体制の整備 について見ると、委託元、委託先ともに、「重要な情報の利用、保管、持ち出し、消去、破棄等に対する取扱い手順の規定」を選択する回答者が最も多かった。これは、2017 年度調査においても、選択される割合の高かった項目である。

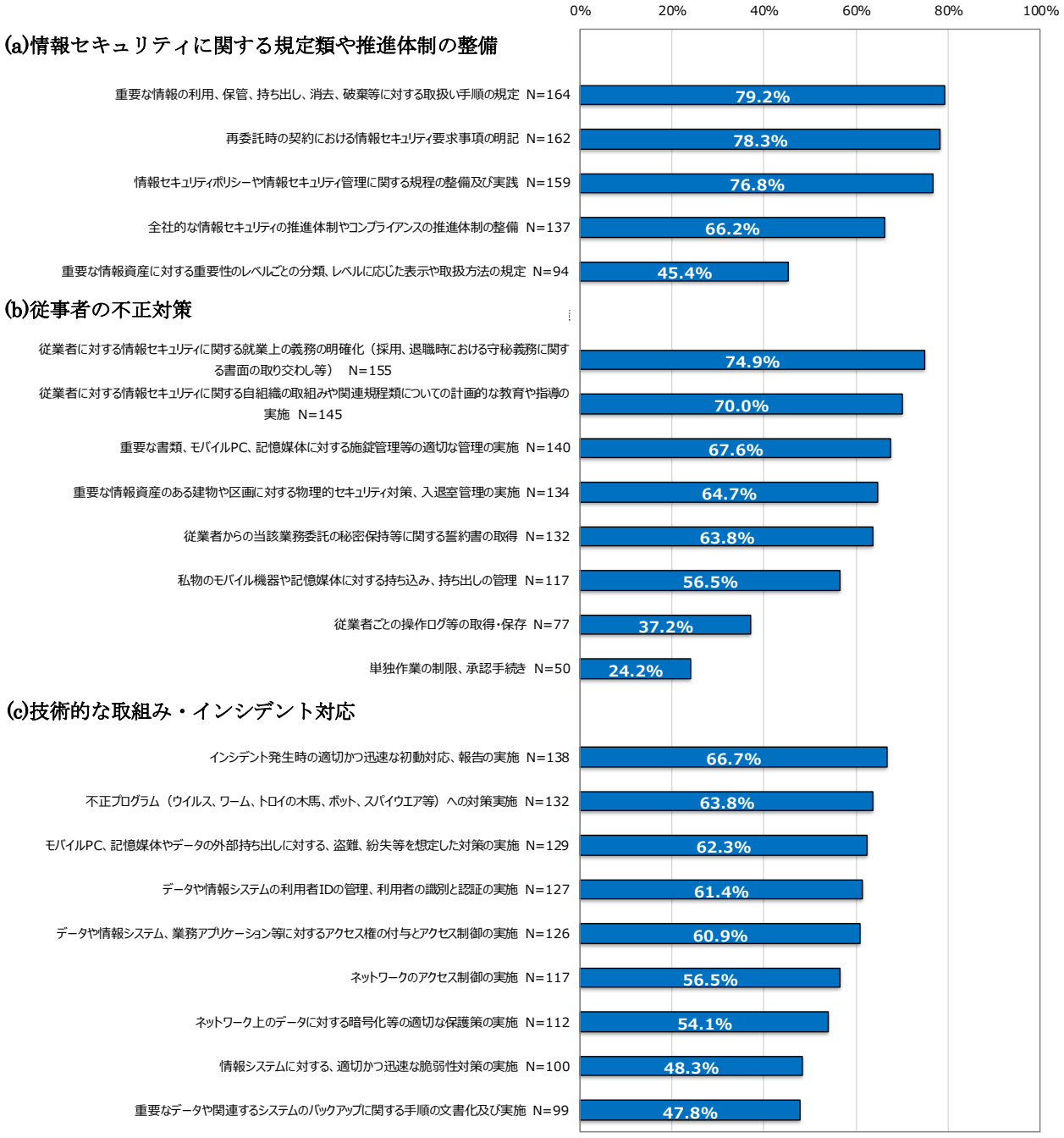
次に、(b) 従事者の不正対策 について見ると、これも、委託元、委託先ともに「従業者に対する情報セキュリティに関する就業上の義務の明確化（採用、退職時における守秘義務に関する書面の取り交わし等）」を選択する回答者が最も多かった。

続いて、(c) 技術的な取組み・インシデント対応 を見ると、委託元で最も回答が多かったのは「不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエア等）への対策実施」であった。一方、委託先で最も回答が多かったのは「インシデント発生時の適切かつ迅速な初動対応、報告の実施」であった。

「再委託時の契約における情報セキュリティ要求事項の明記」は、2017 年度では、18 項目中 2 番目に選択される割合が低かったものだったが、本調査では、委託元では 6 番目に、委託先で 2 番目に多く選択されており、傾向の違いが見られた。



図表 3-71 契約関連文書に明記されていた組織的な情報セキュリティ対策（委託元調査） N=92



図表 3-72 契約関連文書に明記されていた組織的な情報セキュリティ対策（委託先調査） N=207

4. まとめ

4.1 調査仮説の検証結果

4.1.1 契約書の雛形とその運用について

図表 1-6 の調査仮説のうち、契約書の雛形とその運用に関する調査項目の検証結果は次の**図表 4-1** のとおりである。

図表4-1 調査仮説の検証結果（契約書の雛形とその運用）

仮説No	調査仮説	検証結果
1	委託元の主たる事業が化学製品の生産や販売である場合、情報セキュリティ要求事項の含まれる契約書の雛形を用意している。	×：仮説どおりの傾向はみられなかった。
2	委託先は、ITシステム・サービスの種類ごとに情報セキュリティ要求事項の含まれる契約書の雛形を用意している。	○：仮説どおりの傾向がみられた。
3	委託先は、ITシステム・サービスの種類ごとに情報セキュリティ要求事項の内容を変えている。	○：仮説どおりの傾向がみられた。
4	情報セキュリティ要求事項を含む契約関連文書（仕様書、契約書等）の雛形に記載されている情報セキュリティ要求事項の変更は可能である。	○：仮説どおりの傾向がみられた。
5	大企業は、案件ごとに契約関連文書（仕様書、契約書等）の内容を確認する専門の部門（法務部等）や専任の担当者を設けている。	○：仮説どおりの傾向がみられた。

調査仮説 No.1 ついては、調査仮説どおりの傾向はみられなかったが、調査仮説 No.2、調査仮説 No.3、調査仮説 No.4、調査仮説 No.5 については、調査仮説どおりの傾向がみられた。特に仮説 No.3 に関する調査結果からは、ハードウェア保守の場合に「可用性（稼働率の水準、目標）」が要求されることが多かったり、データ処理・分析の場合に「再委託の禁止または制限」や「契約終了後の情報資産の扱い（返却、消去、廃棄等）」が要求されることが多かったりする傾向を把握することができ、IT システム・サービスの種類による情報セキュリティリスクの違いが契約書の内容に反映されていることを確認することができた。

4.1.2　責任範囲が曖昧になる要因について

図表 1-6 の調査仮説のうち、責任範囲が曖昧になる要因に関する調査項目の検証結果は、次の**図表 4-2** のとおりである。

図表4-2 調査仮説の検証結果（責任範囲が曖昧になる要因）

仮説No	調査仮説	検証結果
6	委託元は、委託先の責任範囲を限定してしまうと、それ以上のことをしてもらえなくなるので、責任範囲を限定したくない。	○：仮説どおりの傾向がみられた。
7	委託先は、責任範囲を詳細に決めると、コスト高になり、委託元の合意が得られなくなるので、大まかな取り決めでもよいと考えている。	○：仮説どおりの傾向がみられた。
8	委託元と委託先の関係に資本関係がある場合、契約関連文書に組織的なセキュリティ対策が明記されることが少ない。	×：仮説どおりの傾向はみられなかった。
9	委託元は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなくても委託先が対応すべきだと考えている。	×：仮説どおりの傾向がみられなかった。
10	委託先は、納品後のシステムのセキュリティに関する未知の脆弱性対応は、契約等の明示的な合意がなければ実施する必要はないと考えている。	○：仮説どおりの傾向がみられた。

No.6、No.7 の調査仮説は、ともに責任範囲が明確にならない理由を想定したものである。委託元調査で、「責任範囲を明確にすることで、仕様書等に記述されている以外の対応が期待できなくなる」に対して「強くそう思う」と「ややそう思う」の回答を合わせると 50.8%で過半数を超え、仮説は肯定される結果となった。一方、委託先調査で、責任範囲が明確にならない理由として最も「そう思う」とする回答が多かったのは、「同じ顧客と継続して契約している業務が多く、責任範囲を見直す機会がない」であったが、次いで「責任範囲を明確にすることで、見積りに反映せざるを得ないが、委託元にはコスト増を受け入れてもらえない」であり、調査仮説 No.7 は概ね肯定される結果となった。

また、調査仮説 No.8 は、資本関係のある子会社やグループ企業どうしの契約の場合、お互いのセキュリティポリシー等を理解していることが多いために、契約関連文書に組織的なセキュリティ対策を要求することが少ないのではないかと想定したものであったが、調査結果は仮説を否定するものであった。情報システム子会社等を有する企業は大企業が多いため、内部統制上、情報セキュリティに関しても、資本関係の有無に係わりなく一律の対応をとる傾向が表れているのかもしれない。

No.9 の納品後に見つかった未知の脆弱性に対する対応については、委託元は「委託先が対応すべき」としながらも「必要に応じて業務委託すべき」と考える割合が高く、仮説は肯定される結果とはならなかった。一方、No.10 については、委託先調査の半数以上が未知の脆弱性に対する対応を「契

約等で明記すべき」「必要に応じて業務委託すべき」と回答しており、明示的な合意に基づいて対応したいと考えている傾向がうかがえ、概ね仮説どおりの傾向であった。

4.1.3 サイバー保険の加入状況等について

図表 1-6 の調査仮説のうち、サイバー保険の加入状況等に関する調査項目の検証結果は、次の**図表 4-3** のとおりである。委託元、委託先調査ともに、サイバー保険に加入している割合は低く、No.11 の仮説は肯定される調査結果となった。

また、サイバー保険に加入している委託元がサイバー保険の魅力として選んだもので最も多かったのは、「損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償」であり、No.12 の仮説は肯定される調査結果となった。一方、「委託先がサイバー保険に入っている」を選ぶ企業は少なく、No.13 の仮説は否定される調査結果となった。

図表4-3 調査仮説の検証結果（サイバー保険の加入状況等）

仮説No	調査仮説	検証結果
11	委託元、委託先ともに、サイバー保険に加入している割合は低い。	○：仮説どおりの傾向がみられた。
12	委託元がサイバー保険に加入している理由は「損害賠償責任に関する訴訟や示談交渉に関するコストに対する補償」が魅力的と思っているからである。	○：仮説どおりの傾向がみられた。
13	委託元がサイバー保険に加入していない理由は「委託先がサイバー保険に入っていればよい」と思っているからである。	×：仮説どおりの傾向はみられなかった。

4.2 セキュリティに係る責任範囲の明確化の状況

3.5.2 の分析では、システム運用・管理、サービス提供（ASP、SaaS 等）等のネットワークを利用することの多い業務や、データ処理・分析等の機密情報を扱う業務では、ソフトウェア開発等に比べて、責任範囲を明確にする傾向のある情報セキュリティ要求事項があることが分かった。

また、3.5.3 の分析では、委託元と委託先の比較で、委託先のほうが委託元よりも責任範囲を明確化している傾向が強いのは、本調査で収集した事例に、情報通信業からの委託業務の事例が多いことによることが一因であることが推察された。

3.5.4 のネットワークの範囲に関する分析でも、B to C の場合に、責任範囲を明確化している傾向が強いことが確認できた。また、業種によって、IT 業務委託の事例のネットワークの範囲に傾向の差があることが分かった。

3.5.5 の使用した契約書の書式に関する分析では、委託元が製造業や社会インフラ系の業種である場合、委託元の書式を使用して契約することが多く、委託先の書式を使用するよりも責任範囲が明確になる傾向が見られた。

以上の結果から、契約関連文書における責任範囲の明確化の状況は、委託元の業種や、IT システム・サービスの種類によって、傾向が異なる可能性があると言える。情報セキュリティに関するリスクは、IT システム・サービスの種類によって異なるが、情報漏えい等のリスクが大きい、システム運用・管理、サービス提供（ASP、SaaS 等）、データ処理・分析等の業務分野、およびネットワークの範囲が B to C の場合に、他よりも責任範囲の明確化が進んでいるものと思われる。

また、委託先調査における契約書の書式と責任範囲の明確化の状況に関する分析では、ソフトウェアを含む事例で、プライムベンダーが委託先の書式を使用して契約を結んだ場合に、責任範囲が明示されていない比率が高いことが推察された。ソフトウェア開発は、契約締結時に業務の仕様が明確に決まっていないことが多いため、契約関連文書における記載内容についての調査結果だけでは、責任範囲の明確化の状況を判断することはできないが、事例調査で分析した責任範囲の明確化の対策の一つが契約書における記載の明確化であることを考慮すると、契約締結時に責任範囲を明確化することをあらためて検討すべきであると考える。

4.3 セキュリティに係る責任範囲の明確化に必要な取り組み

4.3.1 契約書の重要性

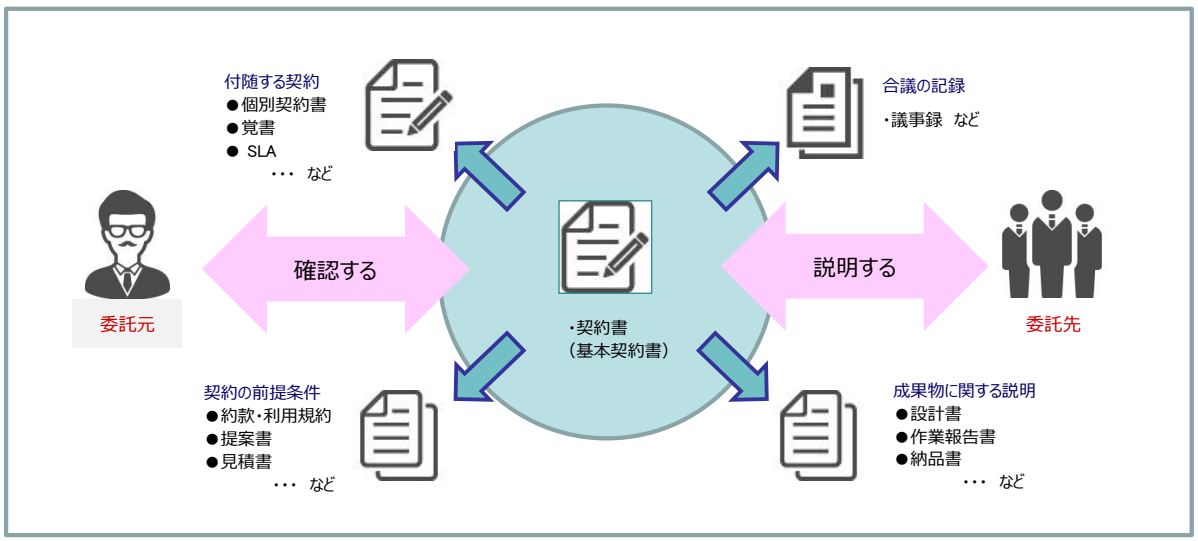
ソフトウェアの開発の場合、委託元が自らの要望に合わせて業務の仕様を決定し、その仕様を委託先に提示して調達を行うことが多い。しかしながら、契約締結時にソフトウェアの詳細な仕様が明確になっていることは少なく、例えば、納品後（運用段階）の責任範囲の詳細は、契約期間中に運用仕様を明確にした上で、その仕様に見合った責任範囲を取り決める事もある。

一方、SaaS のようなクラウドサービスの場合、委託先となるクラウド事業者があらかじめサービスメニューを用意しているのが標準であり、責任範囲はクラウド事業者が約款、利用規約等で提示する条件をベースに交渉することになる。この場合、クラウド事業者（委託先）が、自らに有利な形で免責事項を定めることが容易であり、委託元が委託先に責任範囲の見直しを要求するのは難しい。委託元は、クラウドサービスを利用することのリスクを十分確認した上で、契約内容を検討する必要がある。

IT 業務委託に関して起こったトラブルが法廷に持ち込まれた場合、裁判官が委託元と委託先の責任を判断する根拠とするのは、契約書や覚書等の文書における合意内容である。

事例調査では、責任範囲が曖昧な事例として、契約書と覚書・提案書等の契約期間中に作成される文書との参照関係が曖昧であることが指摘されていることをあげた。ソフトウェア開発の場合、契約締結時に業務の仕様が明確に決まっていることは稀で、多くの場合、運用段階の責任範囲の詳細は契約期間中に合議しなくてはならない。

システム開発に関する訴訟では、委託元の協力義務および委託先のプロジェクト管理義務が問われることが多い。委託元が協力義務を果たしていること、委託先がプロジェクト管理義務を果たしていることを示すためには、契約期間中の議事録や覚書等の文書で、委託元、委託先それぞれの説明内容と合意した内容を記録することが必須であり、同時に、契約書の中で、契約期間中の関連文書の位置付けを明確にする必要があると考える。



図表 4-4 契約書と関連文書の位置付けの明確化（イメージ）

契約関連文書の位置付けを明確にする方法の具体策としては、2.5.2 で紹介した弁護士Ｊ氏のコメント「具体的な要件は仕様書、覚書等に記述し、契約書にはその文書を参照する内容を明記したほうがよい。」という言葉が参考になる。IT システム・サービスの分野は技術革新による環境の変化が大きいため、頻繁に見直しすることが難しい契約書の雛形の中に情報セキュリティに関する条項を設けるよりも、契約期間中に取り交わす覚書等の内容を参照させるように契約書に記述して、具体的な情報セキュリティ要件は、その覚書等に記載したほうが柔軟に対応できると考える。

4.3.2 契約関連文書の雛形の整備・見直し

本調査で行ったアンケート調査では、情報セキュリティ要求事項の含まれた契約関連文書の雛形を用意している企業の割合は、委託先では 76.4%（図表 3-9）と高い水準にあったが、委託元では 45.8%（図表 3-5）と、高いと言える水準ではなかった。また、委託先の調査結果では、雛形が無い場合、過去の契約書を流用して都度作成する、委託元の契約書を使用する等の方法で対応していることも分かった。このような案件ごとの対応では、組織的な情報セキュリティリスク対策との整合性が不十分になる恐れがある。また、事業活動における IT の重要性やサイバー攻撃のリスクの変化は激しく、たとえ雛形が用意されていたとしても、見直しがされていない場合は、リスクに見合わない内容となってしまい、想定していなかった事態が起こった場合に適切に対応できないことも考えられる。円滑な事業運営のためには、自社の事業における情報セキュリティの重要性、想定されるリスク等を考慮した契約関連文書の雛形やガイドラインを整備し、環境の変化に応じて迅速に見直しする体制を準備することが必要である。

しかしながら、本調査で行ったヒアリング調査では、契約関連文書の雛形の見直しは、契約手続きに係る変更は影響範囲が大きく、また、法律や財務的な専門知識も必要とされることから、情報セキュリティの関係部門だけで実施することは困難であり、必要性を感じながらも行動できないという組織も多いことが分かった。

今回の調査では、契約関連文書の雛形の見直しのきっかけとなりそうな環境の変化がいくつかあることが分かった。そのいくつかを以下に示す。

(a) 民法改正

2017 年 5 月に 120 年ぶりの民法改正が国会で可決され、2020 年 4 月から施行されることが決まった。IT システム・サービス等の業務委託契約に関連するところでは、瑕疵担保責任の考え方や、請負や準委任に関する考え方が変更になっている。

(b) 個人情報保護法の改正

民法改正と同時期の 2017 年 5 月に、約 10 年ぶりに改正された「個人情報保護法」が全面施行された。個人情報保護委員会が公表した「個人情報の保護に関する法律についてのガイドライン（通則編）」では、3-3-4 （委託先の監督）において「必要かつ適切な措置」として、①適切な委託先の選定、②委託契約の締結、③委託先における個人データ取扱状況の把握が求められている。

(c) GDPR の施行

2018 年 5 月には、欧州連合（EU）の一般データ保護規則（GDPR）が施行された。日本企業は EU 域内に子会社があるか否かに関わらず、同規則に違反した場合には、巨額な制裁金を課されることとなった。

(d) 「AI・データの利用に関する契約ガイドライン」の公表

2018 年 6 月には、経済産業省から「AI・データの利用に関する契約ガイドライン」が公表された。データ提供型契約およびデータ創出型契約のモデル契約書案が示されているほか、サイバー攻撃によって閲覧できないはずのデータが閲覧できるようになってしまったといった事態が生じた場合、誰に責任があるか、といった具体的なケースについて取り上げ、期待されるセキュリティ対策や免責について示されており、今後、データ利活用がビジネス上重要となる組織であれば参考となる事例が多数示されている。

本調査で行ったヒアリング調査の対象企業の中には、個人情報保護法の改正や GDPR の施行に合わせて、契約書の雛形の見直しを行った企業があった。IT システム・サービスを取り巻く法的な環境の変化は、情報セキュリティ要求事項を含んだ契約関連文書の雛形の作成や見直しを検討する機会である。

例えば、委託先における個人データの取り扱い状況の把握について、実施方法や実施タイミング等を組織のルールに定め、契約関連文書の雛形の中に、証跡の提示、監査協力について明示することは有効だと考える。

また、GDPR にはインシデントが発生した際の報告義務が 72 時間以内に定められている。EU 域内で経済活動を行っている企業においては、IT サプライチェーン上で、この制約に対応可能な機動的な体制を構築する必要がある。

上述の法的環境の変化について、各組織の事業環境に影響の大きいものを契約見直しの契機として取り上げ、関係部署との調整をする中で情報セキュリティについても一緒に検討することは有益なことであると考えられる。

4.3.3 組織的な取り組みの重要性

本調査で実施したヒアリング調査では、責任範囲を明確にしている事例として、契約時に委託先にセキュリティに関するチェックシートへの回答を求める事例や、自社のシステムごとにセキュリティリスクを分析し、当該システムの契約書にそのリスクに対応する条項を入れるようにしている事例等が得られた。

サプライチェーンにおける情報セキュリティリスクは、業界の構造に依存したガバナンスモデルや、委託・調達する業務によって異なることが指摘されており[12]、ビジネスモデルごとにセキュリティリスクを洗い出し、チェックリストを用意する等の対策が必要と思われる。責任範囲の明確化には、組織的な取り組みが必要であり、ビジネスモデルごとの情報セキュリティ対策のガイ

[12] 久保知裕、原田要之助「サプライチェーンの日本企業における情報セキュリティガバナンスの研究」
電子情報通信学会技術研究報告、一般社団法人電子情報通信学会（2014 年 5 月）

ドライン等が整備されることが望まれる。

4.4 参考文献

- □ 松島 淳也・伊藤雅浩 著「新版 システム開発紛争ハンドブック －発注から運用までの実務対応－」第一法規株式会社（2018 年 7 月）
- □ 細川義洋 著「紛争事例に学ぶ、IT ユーザの心得－契約・費用・法律編－」翔泳社（2017 年 9 月）
- □ 上山浩 著「弁護士が教える IT 契約の教科書」日経 BP 社（2017 年 9 月）
- □ 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 10 月）
- □ 独立行政法人 情報処理推進機構「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査報告書」 （2018 年 3 月）