概要説明資料

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

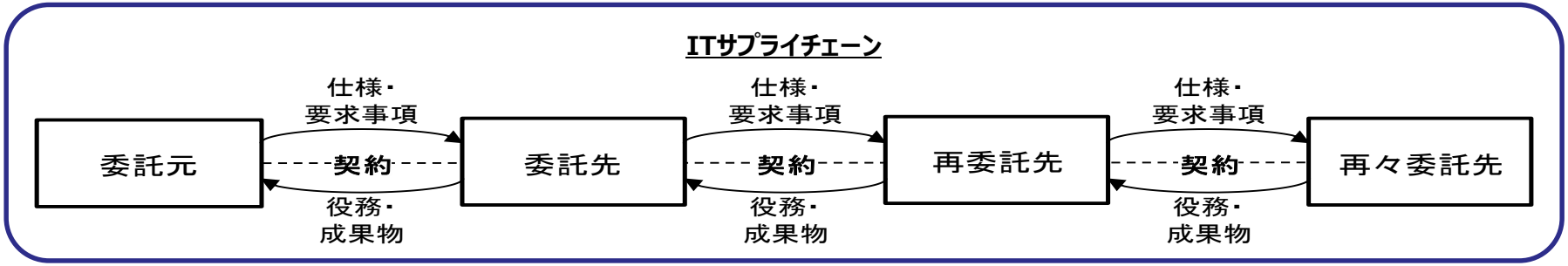
2019年4月

情報処理推進機構
セキュリティセンター
セキュリティ対策推進部
セキュリティ分析グループ

調査の概要

■ 情報セキュリティに係る責任範囲について実態と事例を調査

内容	説明
背景	2017年度の調査において、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確という課題**が明らかになった。
目的	ITサプライチェーンにおける情報セキュリティ上の責任範囲が明確になっていない実態と原因を明らかにし、解決するための対策を導きだす。
調査内容	・ITサプライチェーンリスクマネジメントの実態。 ・IT業務を委託、受託した場合の具体的な事例における情報セキュリティに係る責任の明確化の状況。 ・責任範囲を明確にしている項目。 ・責任範囲が明確ではない項目。 ・責任範囲を明確にできない理由。 ・責任範囲が明確ではないリスクに対する対策。
調査手法	・アンケートによる実態調査。 ・文献調査及びヒアリング調査による事例調査。



※以降のページの「セキュリティ」はすべて「情報セキュリティ」を指します。

調査実績

■ アンケート回収

分類		企業規模*		計
		大企業	中小企業	
委託元**		239	178	417
	製造業	137	91	228
	卸売・小売業	52	50	102
	サービス業	47	35	82
	その他	3	2	5
委託先		165	263	428
合計		404	441	845

＊　企業規模　委託元：大企業（301人以上）、中小企業（300人以下）　委託先：大企業（101人以上）、中小企業（100人以下）

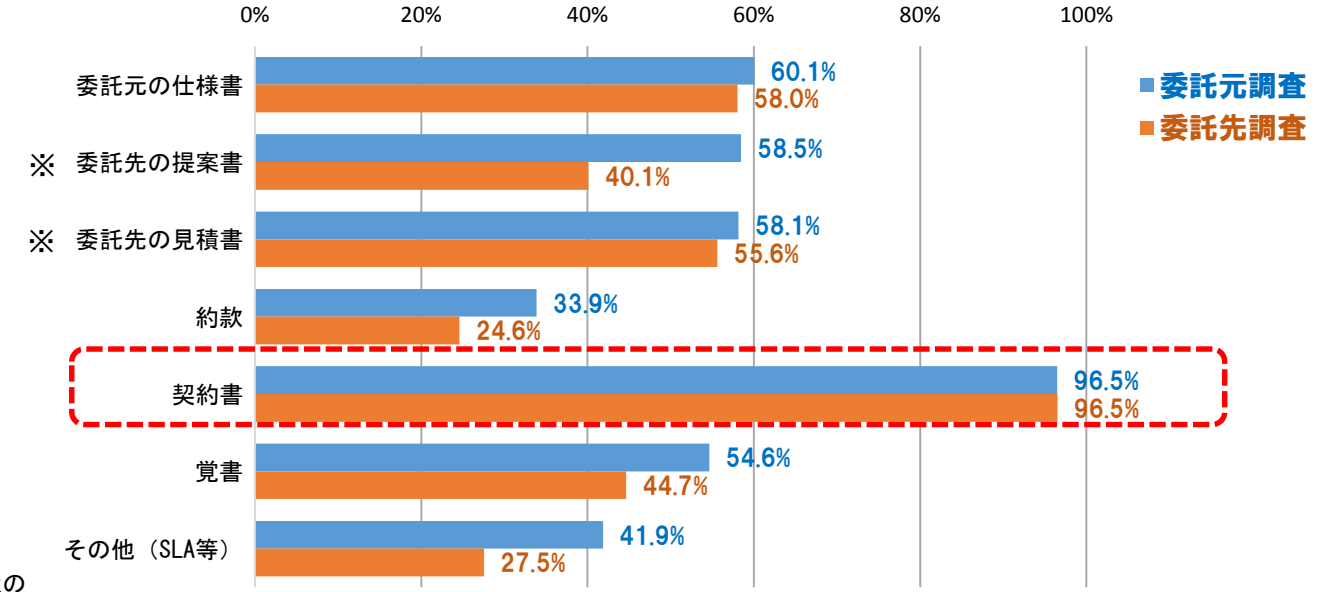
＊＊委託元は、2017年度調査において契約書・仕様書等にセキュリティ要求事項に関する記載をしていると回答した企業の比率が低かった業種（製造業、卸売・小売業、サービス業）に絞って調査を行った。

■ 事例収集

- ヒアリング　10者（委託元3者、委託先3者、有識者4社）
- 文献調査　15件

IT業務委託契約時に責任範囲を記述している文書

■ IT業務委託において訴訟となった場合、争点となるのは契約書や覚書等の文書における委託元と委託先の合意内容である。このような背景から、委託元がどのような文書でセキュリティに係る要求事項（責任範囲）を記載しているかについて調査したところ、「契約書」を使用するという回答が最も多かった。



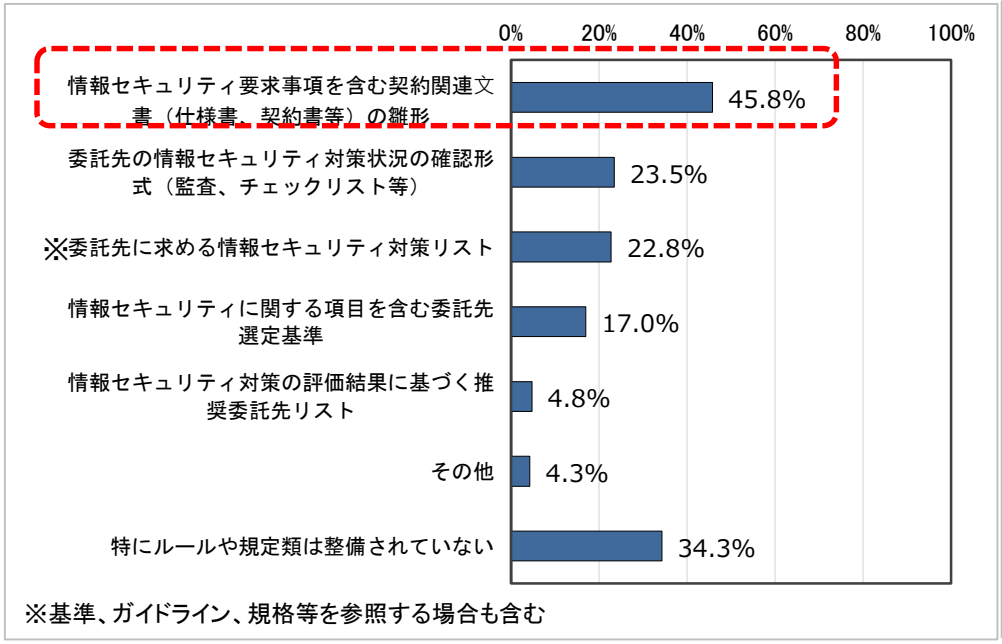
セキュリティに係る要求事項（責任範囲）を記載した文書

※委託先の回答は自社の提案書、見積書を示す。

契約関連文書の雛形の有無と変更の可否（委託元）

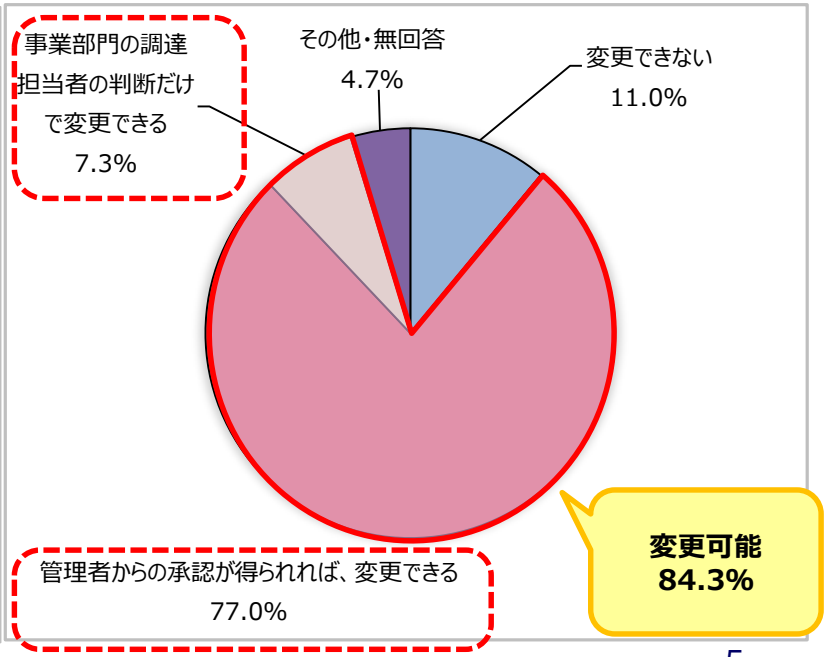
- 委託元の45.8%は、情報セキュリティ要求事項の含まれた契約関連文書（仕様書、契約書等）の雛形を用意していた。
- 雛形を用意している企業のうち84.3%が（業務内容によって異なる）セキュリティ要求事項の追加、条件変更等に合わせた雛形の変更が可能。

＜雛形の有無＞



※基準、ガイドライン、規格等を参照する場合も含む

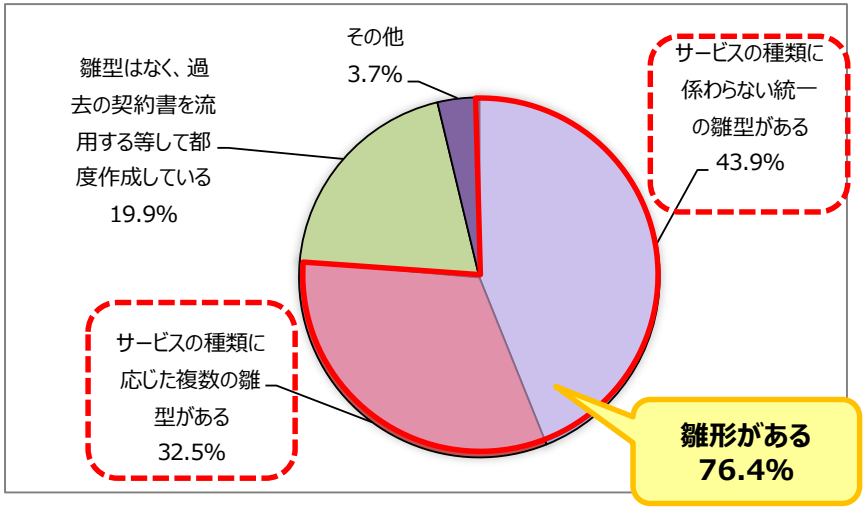
＜変更の可否＞



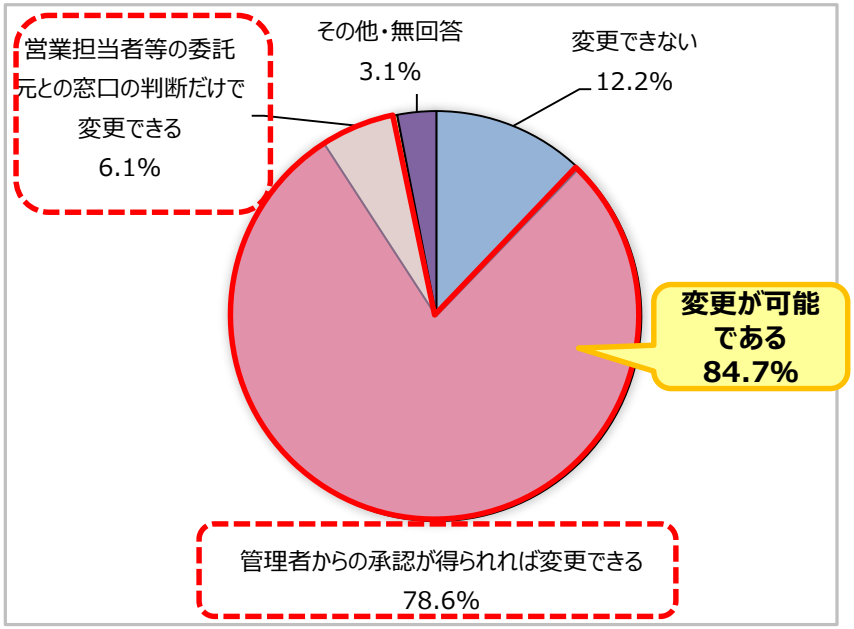
契約関連文書の雛形の有無と変更の可否（委託先）

- 委託先の76.4%は、情報セキュリティ要求事項の含まれた契約関連文書（仕様書、契約書等）の雛形を用意していた。
- 雛形を用意している企業のうち84.7%が業務内容によって異なるセキュリティ要求事項の追加、条件変更等に合わせた雛形の変更が可能。

＜雛形の有無＞



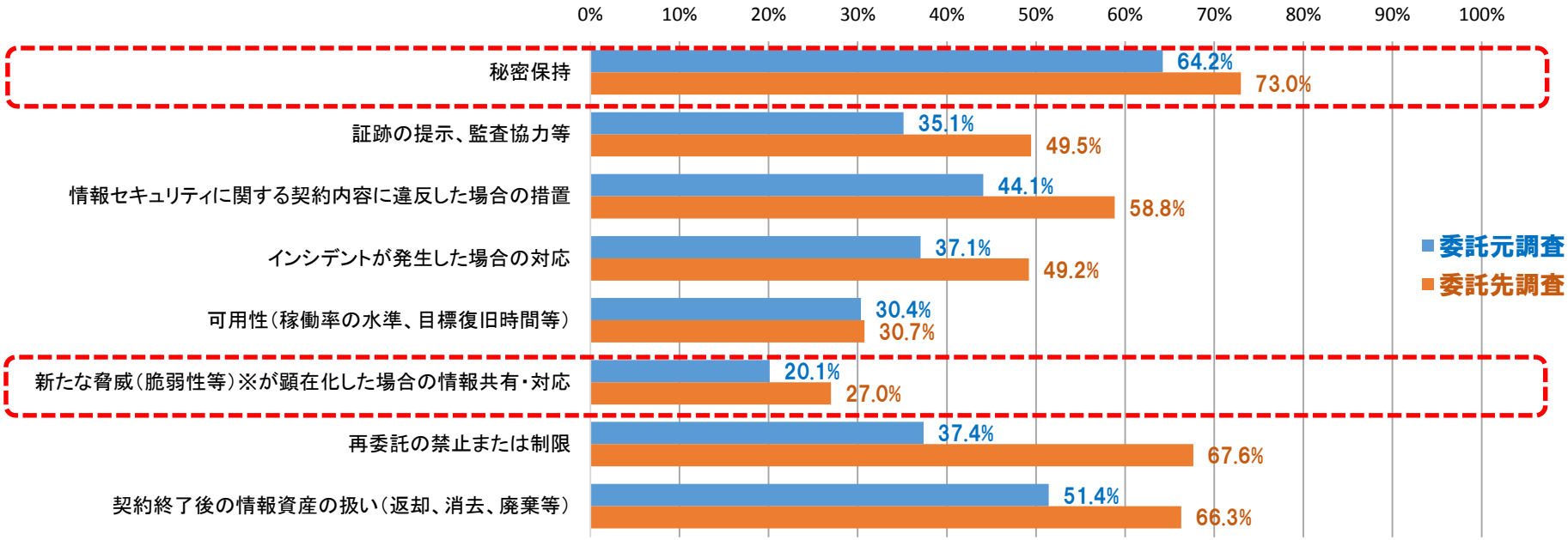
＜変更の可否＞



サービスの種類：ソフトウェア開発、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、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・分析など

IT業務委託契約時に明確にしている責任範囲の内容

■ IT業務委託契約時に、委託元がセキュリティに係る要求事項（責任範囲）について、どのような内容を文書で明確化しているかを調査したところ、委託元、委託先ともに最も多く明確化していたのは「秘密保持」、最も明確化されていないのは「新たな脅威（脆弱性）が顕在化した場合の情報共有・対応」であった。



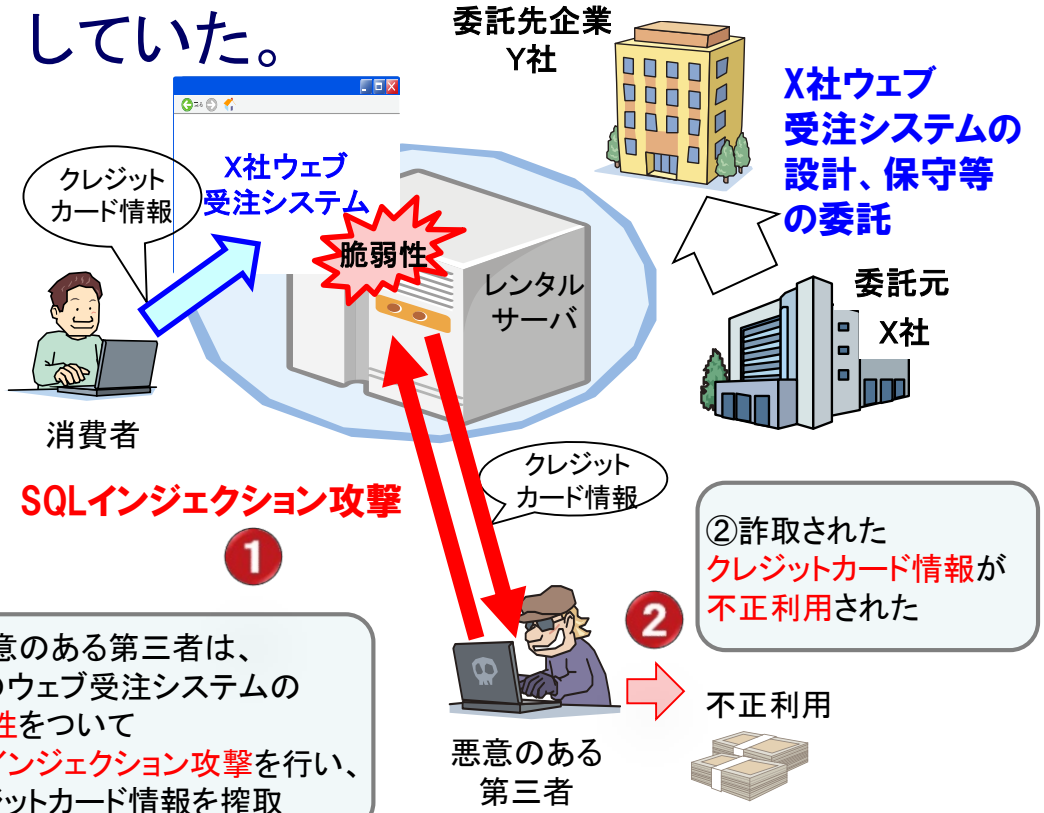
※未知の脆弱性を含む。

IT業務委託時に明確にしている責任範囲の内容

参考：国内インシデント事例：サイバー攻撃に対するIT事業者の責任

a IT事業者にはその当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていた。

b IT事業者はクレジットカード情報の保存による危険性を説明していた。



IT事業者は専門的知識を有しており、予見可能で回避策が容易であったのに、しかるべき対策を施さなかった。

SQLインジェクションの注意喚起と対策は委託の2年前にIPAから公開されていた

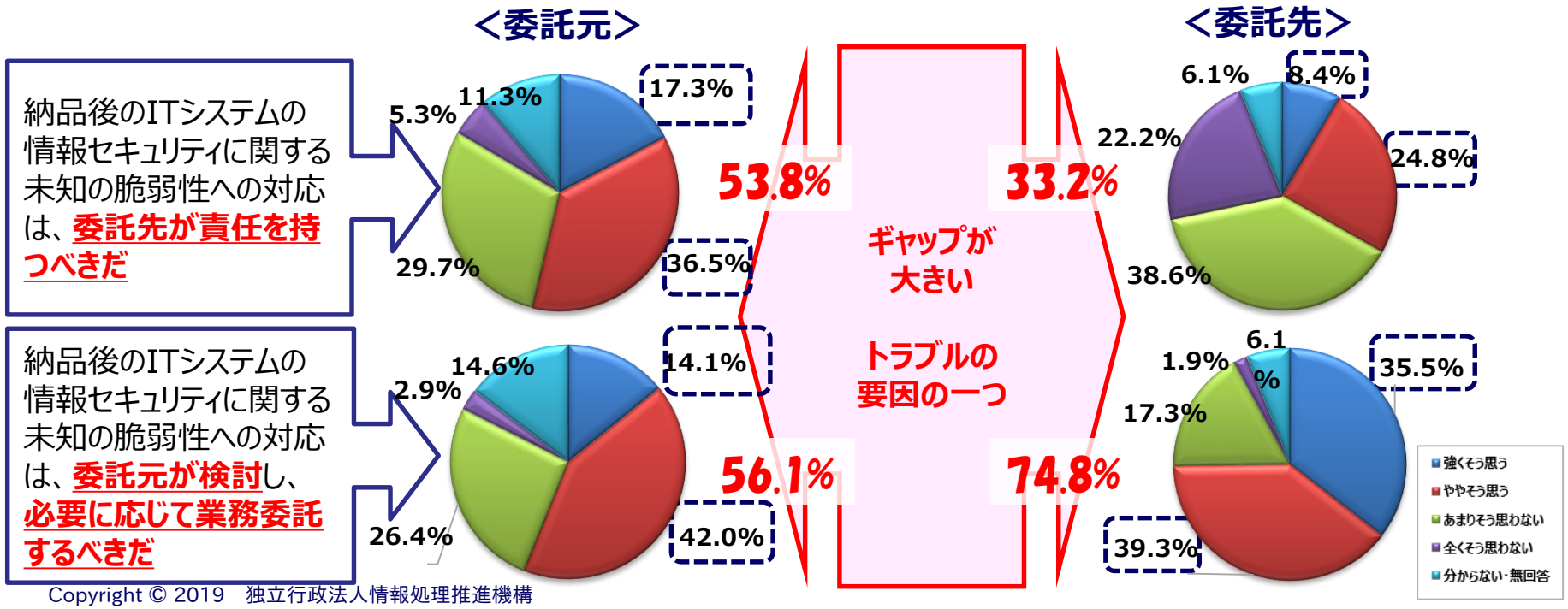
aについて

IT事業者の重過失

bについて、何の返答もしていなかった委託元の過失を認め、過失相殺されたが、重過失により賠償額上限条項は適用されず、賠償金額は委託金額を上回った。

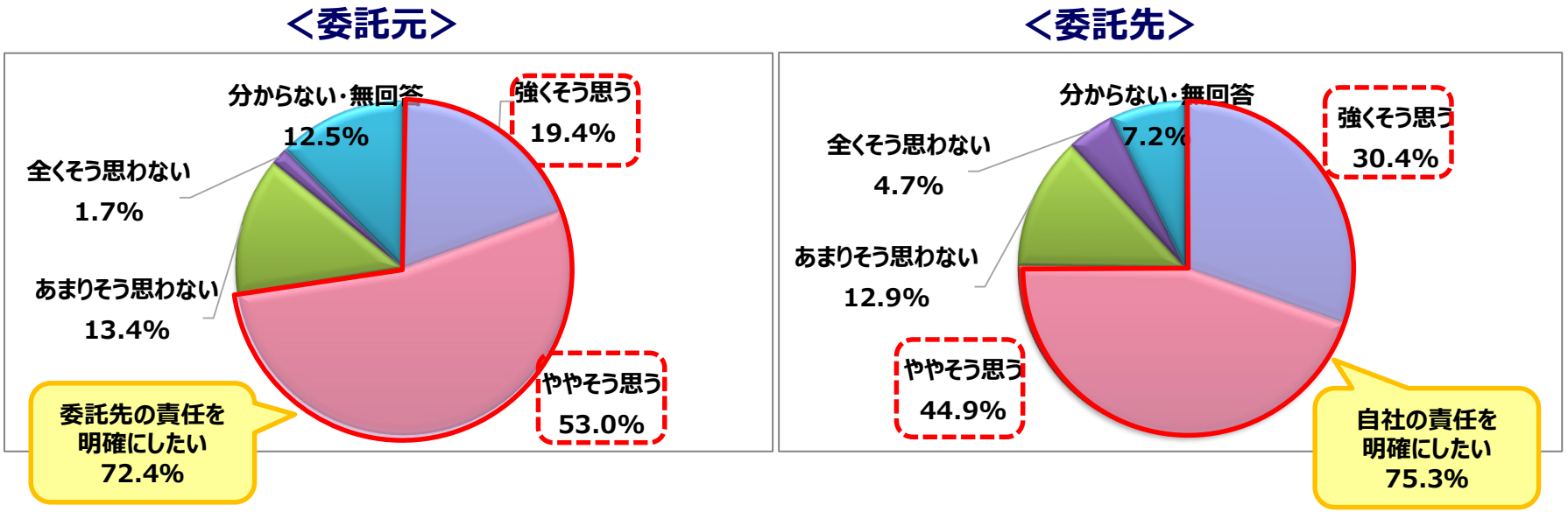
未知の脆弱性に対する考え方

■ 未知の脆弱性について、委託元は納品後も委託先に責任を持って欲しいと考えており、委託先は納品後の責任は委託元に責任をもって欲しい（必要に応じて業務契約をすべき）と考えている傾向があり、委託元と委託先の意識にギャップがあることがわかった。



未知の脆弱性に対する責任範囲の明確化

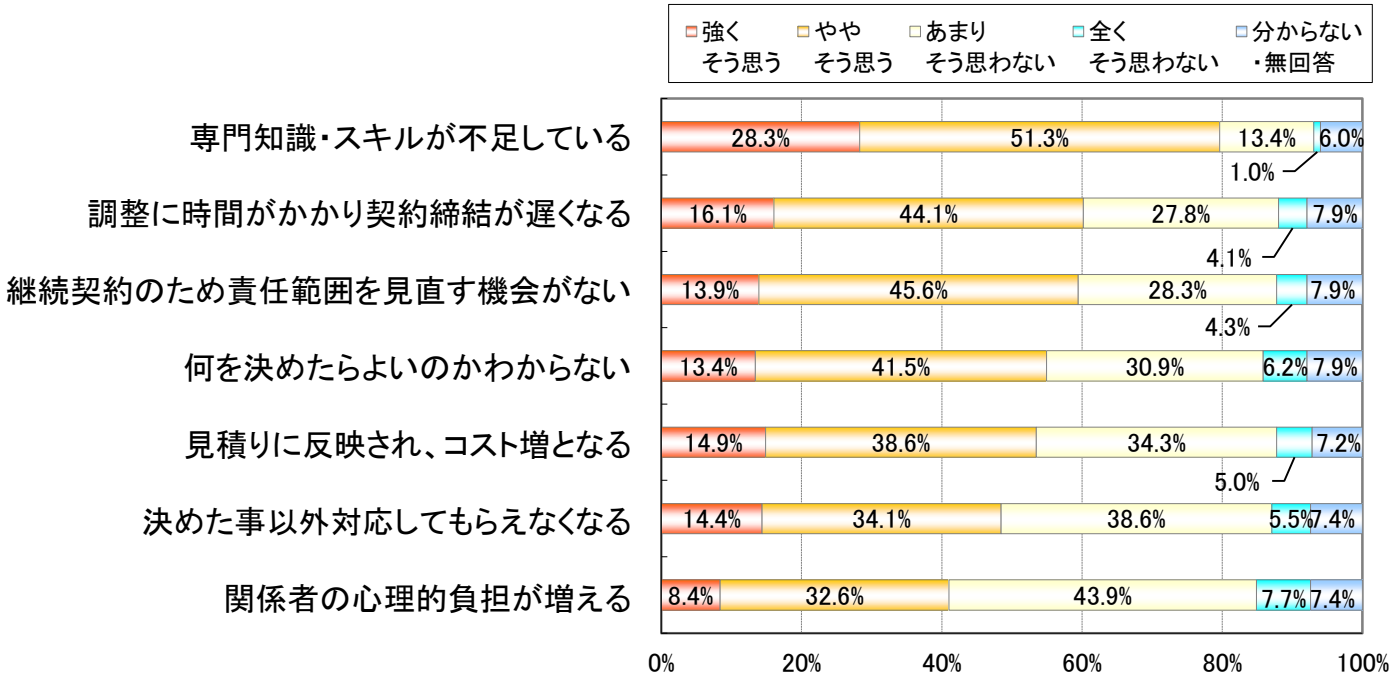
- 未知の脆弱性に対する責任範囲について、委託元と委託先には考え方のギャップがあったため、責任範囲を明確化することについてどのように考えているかを調査したところ、委託元の72.4%、委託先の75.3%が、委託先の責任を明確にしたいと考えていることがわかった。



未知の脆弱性が顕在化した場合の情報共有・対応に対する意識

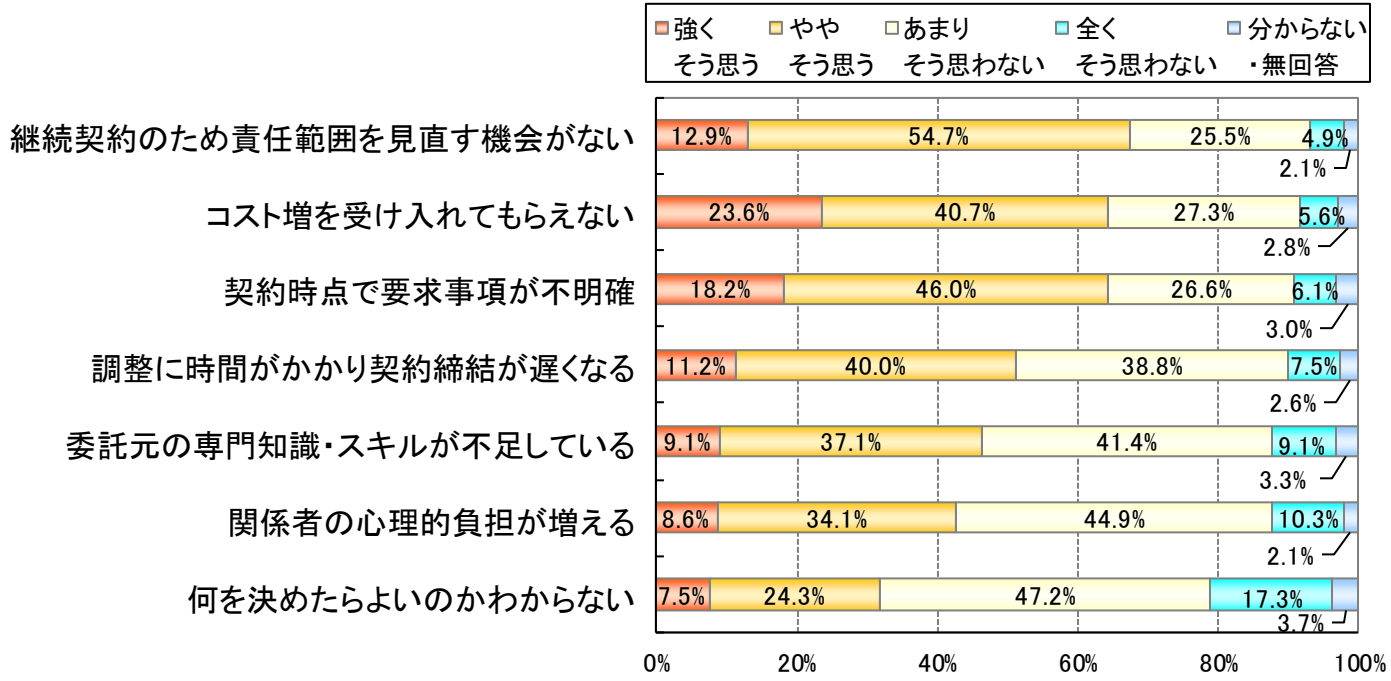
責任範囲を明確にできない理由（委託元）

- 委託元が情報セキュリティに係る要求事項（責任範囲）を明確にできない理由を調査したところ「専門知識・スキル不足」が最も多い回答となったが、その他の理由もほぼ50%程度の回答であり、委託元が責任範囲を明確にできない背景には複数の理由があることがわかった。



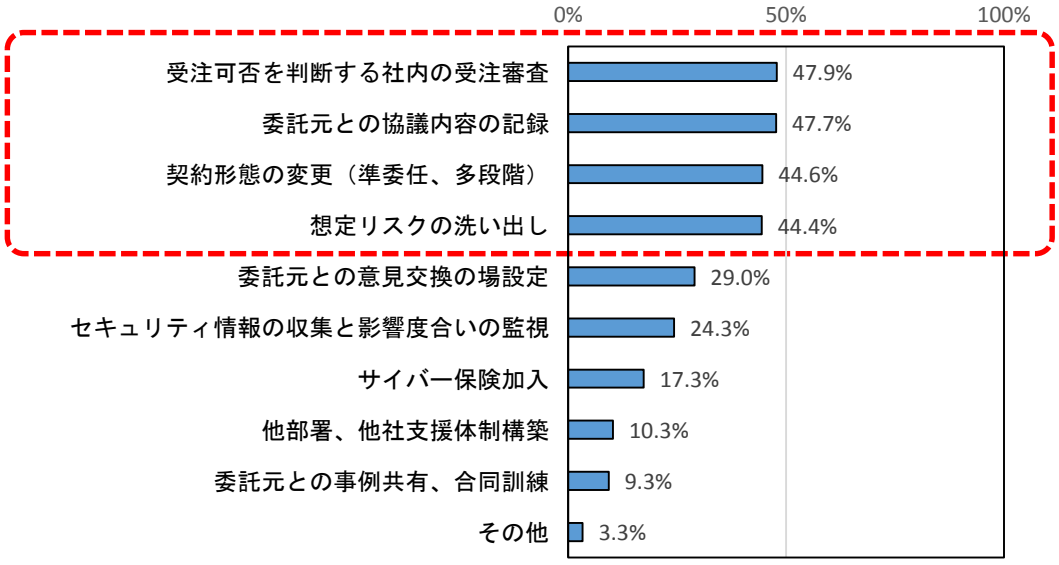
責任範囲を明確にできない理由（委託先）

■「責任範囲を見直す機会が無い」が最も多い回答となったが、「コスト増を受け入れてもらえない」「契約時点で要求事項が不明瞭」「契約締結に時間がかかる」が50%程度の回答であった。委託先が責任範囲を明確にできない背景にも複数の理由があるが、委託元とは理由の傾向が異なることがわかった。



IT業務委託契約時の残存リスク対策（委託先）

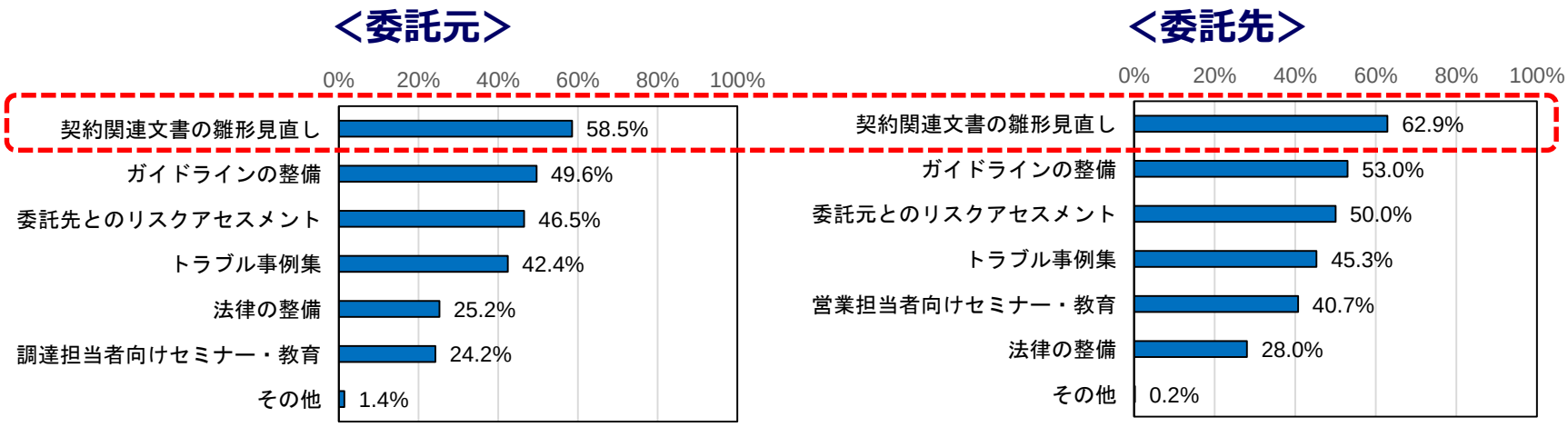
■ IT業務委託契約時に、委託元からのセキュリティに係る要求事項（責任範囲）に不明確な部分が残ってしまう場合に、委託先がなんらかの対策を行っているかを調査したところ、委託先は、主に自組織内でリスクを低減するための対策を実施していた。



IT業務委託契約時に委託先が実施している残存リスク対策（複数選択可）

責任範囲を明確化するために有効な施策

■ 情報セキュリティに係る責任範囲を明確化するために有効な施策について調査した結果、委託元、委託先ともに、契約関連文書（仕様書、契約書等）の雛形の見直しが最も有効な対策と考えられている回答を得た。



責任範囲を明確化するために有効な対策（複数選択可）

調査結果概要

■ 情報セキュリティに係る責任範囲の明確化の状況

- 委託元、委託先ともに、なにがしかの契約関連文書（主に契約書）を用いて責任範囲を明示しているが、秘密保持以外は明確にしている割合が低い。
- 委託元、委託先ともに見直しのタイミングがない、契約遅延による影響、委託元はスキル不足、委託先は要求事項が曖昧、コスト増などの理由により、明確にすることができていない。
- 委託先は、受注審査や委託元との協議内容の記録、契約形態の変更等により、自組織内で行えるリスク対策を行っている。

■ 責任範囲が明確ではないリスクに対する対策

委託元、委託先ともに責任範囲を明確にしたいと考えており、そのためには契約関連文書（仕様書、契約書等）の雛形の見直しが有効であると考えている。

まとめ

■ 情報セキュリティに係る責任範囲についての実態と事例の調査結果をふまえ、責任範囲の明確化の対策をまとめた。

責任範囲を明確にできない理由		どうすべきか	有効な対策
共通	継続契約で見直しをしていない	契約更新時にセキュリティ要件に不足がないか確認する。	契約書の内容の見直し
共通	契約締結遅延による影響大	基本的なセキュリティ要件を契約書の雛形で明確化しておく。	契約書の雛形の見直し ・専門的な知識がなくても契約で明確化すべきセキュリティ要求事項がわかるような雛形の作成 ・サービスの種類(*)により必要となる基本的なセキュリティ要求事項の雛形の作成
委託元	知識・スキル不足	知識・スキルに依存せずにセキュリティ要件を決められるようにする。	
委託元	何を書けばよいかわからない		
委託先	コスト増	サービスの種類(*)に応じて基本的なセキュリティ要件を契約書で明確化しておく。	
委託先	業務要件自体が未確定	詳細な要件が未確定であっても、委託サービスの種類(*)に応じて決められる要件はあるため、基本的なセキュリティ要件を契約書で明確化しておく。	

(*)サービスの種類:ソフトウェア開発、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、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・分析など

参考） 契約の雛形の見直しと契機

■ 雛形見直しの契機

近年、法律の改正、規則の適応、ガイドラインの公開などがあり、
このようなタイミングで契約書の雛形の見直しを検討することは
責任範囲を明確化するために有効であると考えられる。

■ 民法改正（2020年4月から施行）は見直しの契機として有効

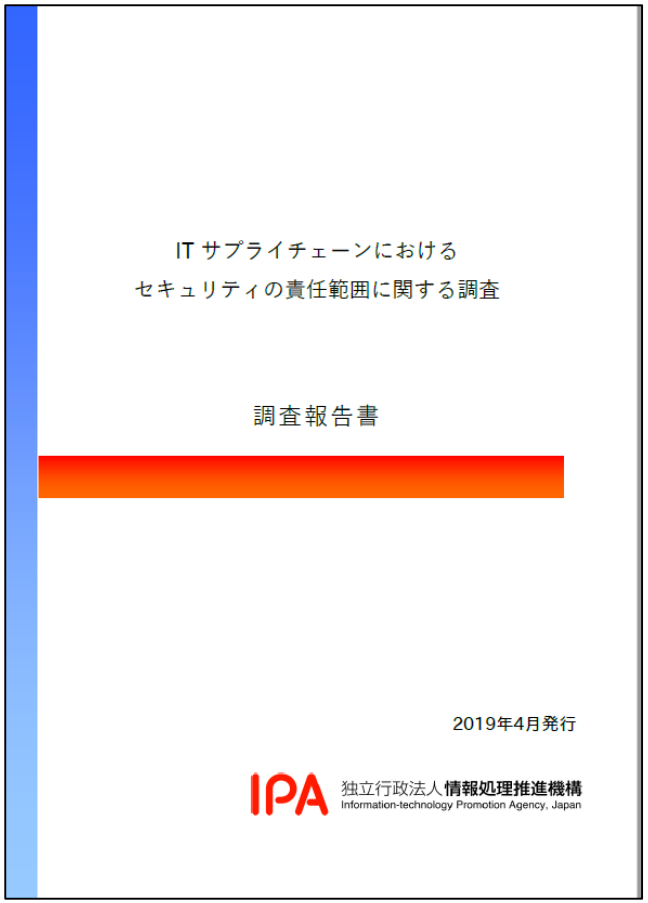
民法改正により、ITシステム・サービス等の業務委託契約における
瑕疵担保責任の考え方、請負や準委任に関する考え方が変更と
なっており、施行後は委託元が以下を明記する必要がある。

- 契約の「目的」を明確にする。（契約不適合責任）
- 契約交渉時に契約関連文書における責任範囲に関する記載（免責事項、瑕疵担保責任等）を確認する。
- 基本となる契約書と、契約に付随する文書の関係を明確にする。

参考） 調査報告書の入手方法

IPAのサイトからダウンロードいただけます。

https://www.ipa.go.jp/about/press/20190419.html



調査報告書目次

1. はじめに
   調査背景・目的、スコープ、実施概要

2. 責任範囲の明確化の状況（事例調査）
   責任範囲にまつわるトラブル事例、明確化の事例、対策等

3. 責任範囲の明確化の状況（アンケート調査）
   契約書の雛形と運用、責任範囲が明確にならない理由等

4. まとめ

付録1　文献調査　調査結果一覧
付録2　アンケート調査票
付録3　アンケート単純集計結果