参考資料3

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 ～概要説明資料～

2018年3月

産業サイバーセキュリティ研究会
ワーキンググループ1（制度・技術・標準化）
第2回会合　参考資料

Ver.1.0+

調査概要

背景・目的

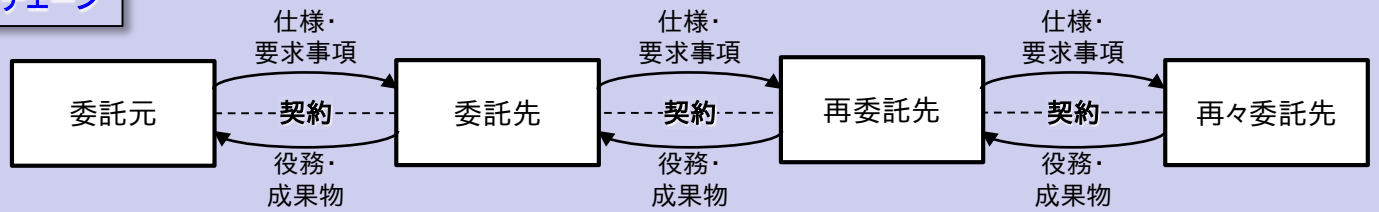
◆ITサプライチェーン上の組織における
インシデントの影響は、関係する複数組織に
及び、被害が拡大したり、問題解決が困難に
なる可能性がある。
◆2016年度の調査において、委託元としてIT
サプライチェーンリスクへの意識は高いものの、
再委託先以降の情報セキュリティ状況の
把握は難しいこと等の課題が挙げられ、
企業においてITサプライチェーンリスクの
把握とその対策が十分にできていないことが
示唆された。
◆ITサプライチェーン上のインシデント事例や
委託元、委託先それぞれが行っている
ITサプライチェーンリスクマネジメントの実態
を調査・分析し、課題を明らかにする。

2017年度調査の内容

◇ITサプライチェーンの委託元・委託先・再委託先・
再々委託先と連鎖的に続く委託形態に注目し、
インシデント事例や情報セキュリティ上のリスク、並
びに当該リスクの防止・低減のための委託元、委
託先の企業での対策の実態を調査

- **文献調査（国内外）**
  - ✓ ITサプライチェーン上の**インシデント事例調査**
  - ✓ ITサプライチェーンリスクマネジメントに関する
    基準、ガイドライン及び規格等に対する調査
- **アンケート調査（国内の委託元、委託先の企業）**
  - ✓ **委託元・委託先**の両方の視点から、
    企業の取組み内容と現状の課題を調査
- **インタビュー調査（国内の企業、有識者）**
  - ✓ ITシステム・サービスの業務委託での
    インシデントの経験と対策の見直し
  - ✓ ITサプライチェーンリスクマネジメントに関する
    企業の取組みと課題意識

ITサプライチェーン



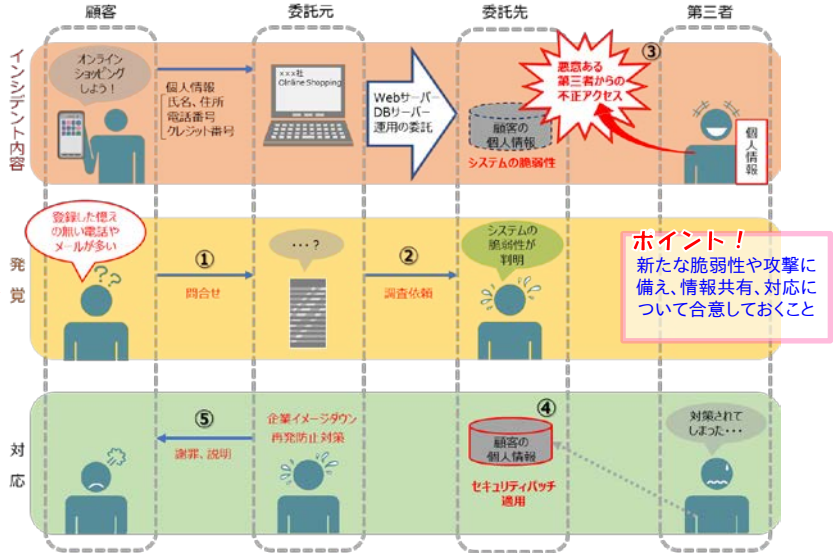
文献調査結果1:

インシデント事例調査と典型パターン

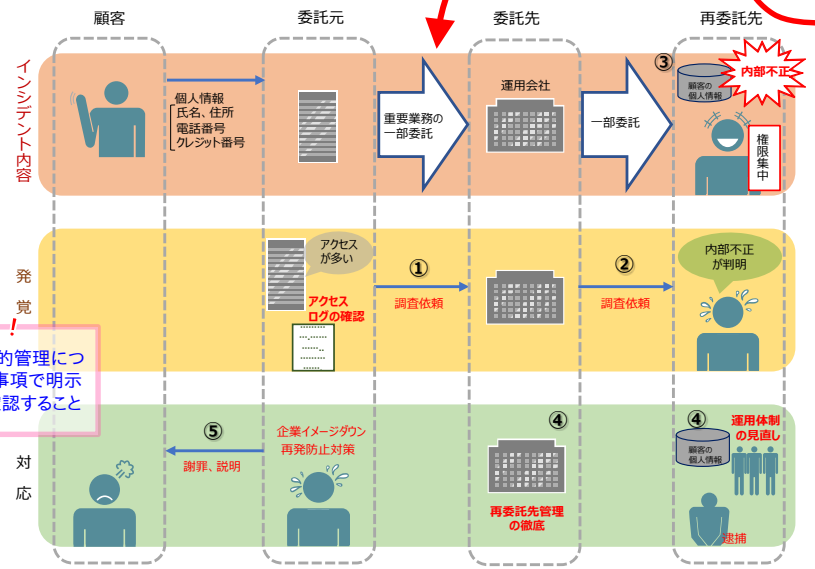
過去5年以内に、ITサプライチェーン上で発生した
国内外の主なインシデント事例を公開情報から
収集し、傾向を分析し、典型パターンを整理した。

収集したインシデント事例(52件)における
事業分野ごとのインシデントの原因に関する傾向

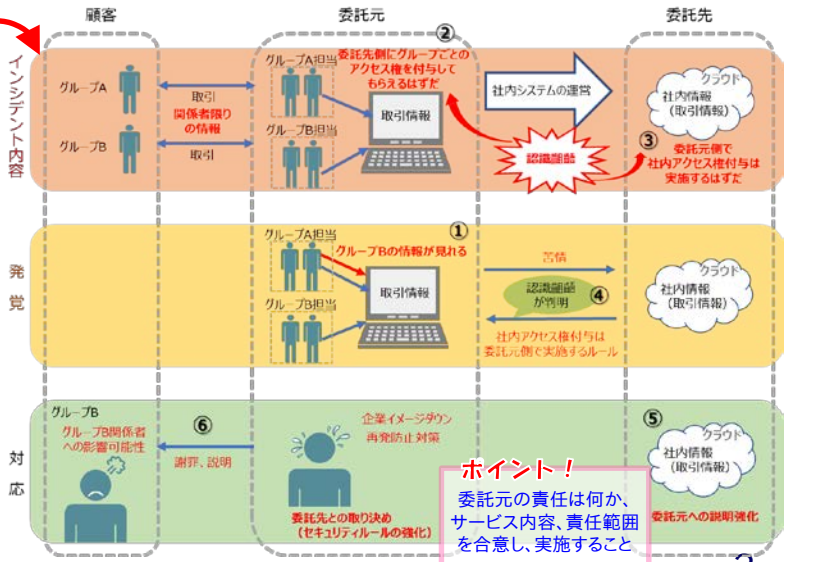
事業分野	原因区分					
	不正アクセス	ウイルス	SWのバグ	内部不正	人的ミス	盗難・紛失
インターネットビジネス	28	2	3		3	1
ITソリューション	1	1		4	5	3
IoTソリューション					1	



ポイント！
新たな脆弱性や攻撃に備え、情報共有、対応について合意しておくこと



ポイント！
委託先の人的管理についても要求事項で明示し、状況を確認すること

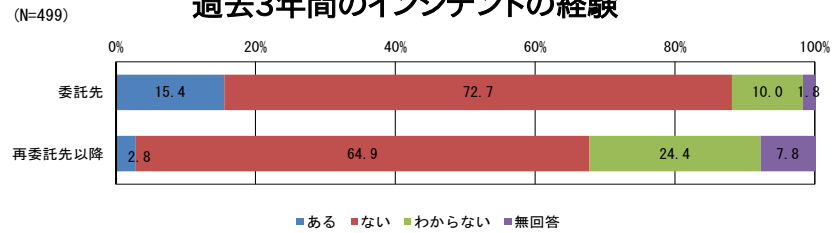


ポイント！
委託元の責任は何か、サービス内容、責任範囲を合意し、実施すること

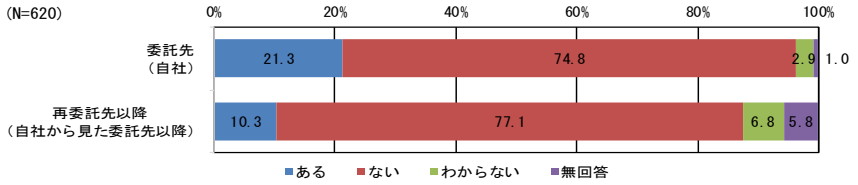
参考）業務委託における インシデントの経験（アンケート調査結果）

- 委託元の15.4%で委託先におけるインシデントを経験している。再委託先以降におけるインシデントは、ある（ 2.8% ）、わからない（ 24.4%）で十分把握できていない可能性がある。
- 委託先では21.3%がインシデントを経験しており、10.3%で再委託先以降におけるインシデントを経験している。（委託先は再委託先が起こしたインシデントを委託元に報告していない可能性がある。）
- インシデントの内容としては「システム・サービスの障害・遅延・停止」（委託元74.4%、委託先52.4%）が最も多い。「情報漏えい、暴露」と「データ毀損、消滅」と続き、委託元、委託先が同じ傾向を示している。

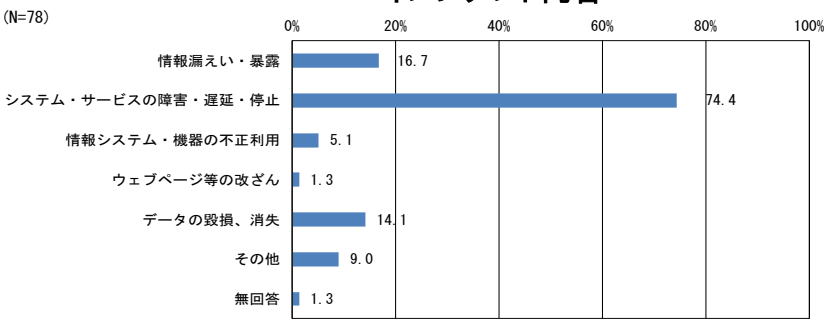
業務委託（委託先または再委託先以降）における過去3年間のインシデントの経験



受託業務（自社や再委託先以降（自社から見た委託先以降））における過去3年間のインシデントの経験

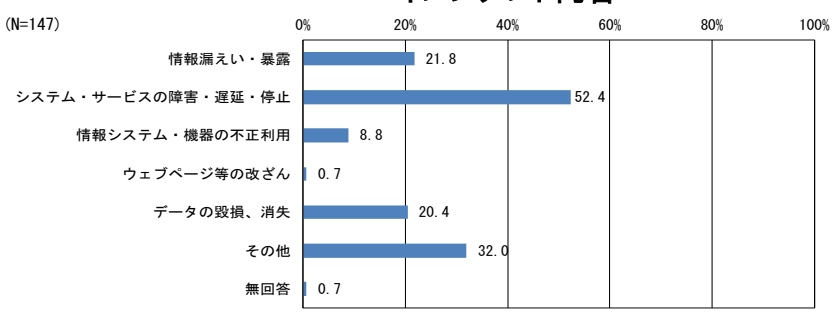


インシデント内容



委託元

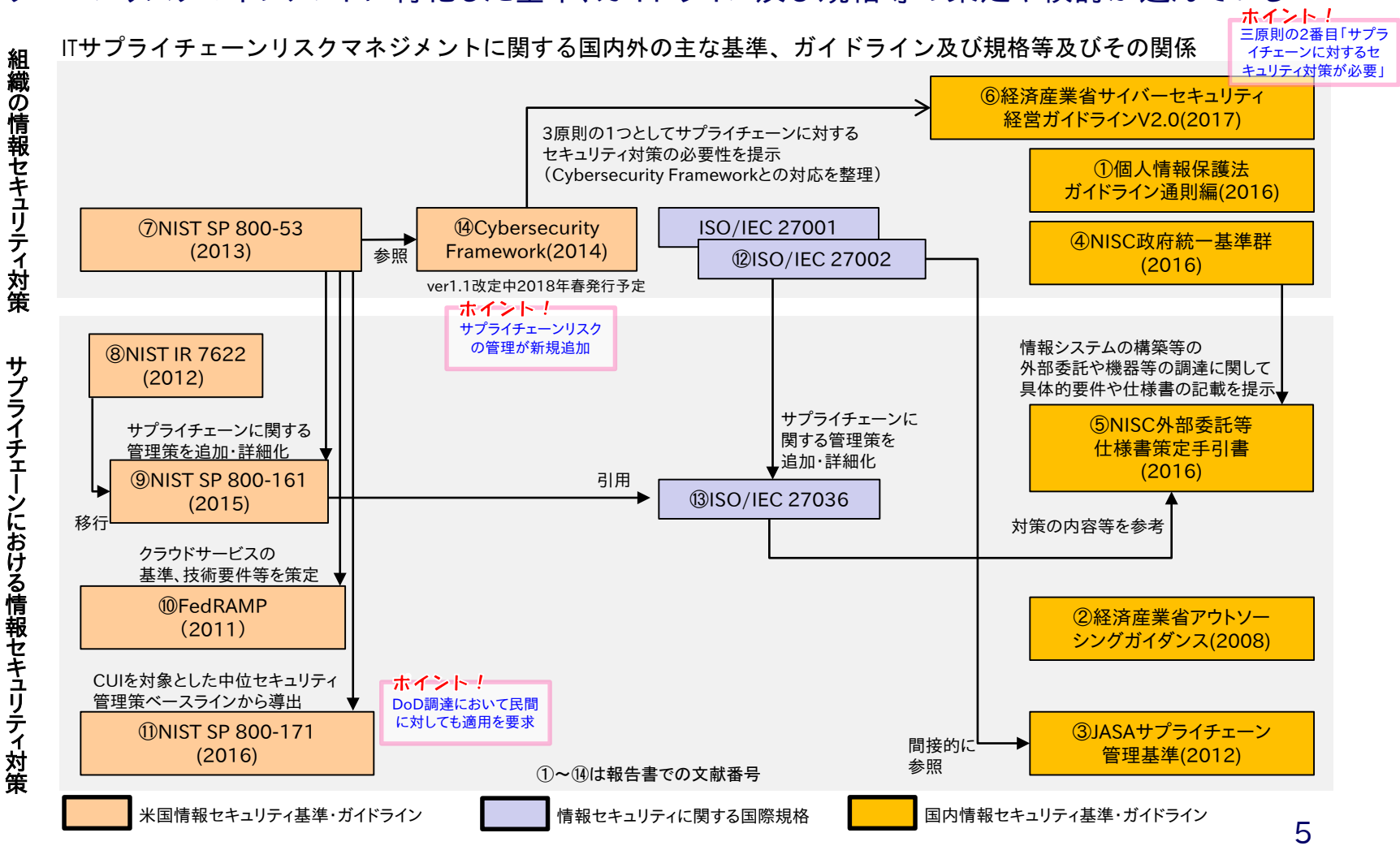
インシデント内容



委託先

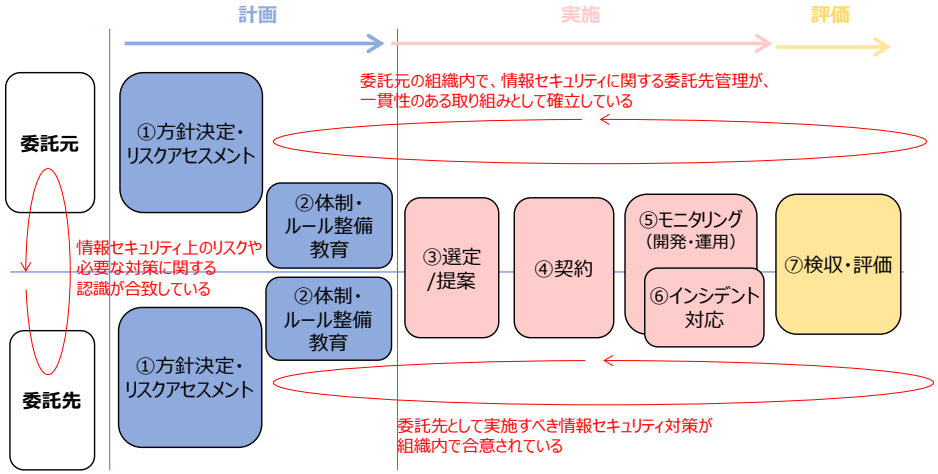
文献調査結果2:
ITサプライチェーンリスクマネジメントの標準

■ ITサプライチェーン全体での情報セキュリティの確保の重要性が認識されてきたことで、ITサプライチェーンリスクマネジメントに特化した基準、ガイドライン及び規格等の策定や検討が進んでいる



アンケート調査及びインタビュー調査の仮説検討

■ インシデント事例及び基準、ガイドライン及び規格等に関する文献調査を基にITサプライチェーンリスクマネジメントに関する企業の取組みを調査仮説を検討し、アンケート調査及びインタビュー調査を通じてこれを検証した。



ITサプライチェーンリスクマネジメントの全体像

段階	プロセス	調査仮説
計画	①方針決定・リスクアセスメント	委託（受託）業務におけるセキュリティ脅威、リスク等について事前に確認していない。
	②体制・ルール整備・教育	業務委託における情報セキュリティの取組みの実施状況は取り扱う情報資産の重要度によって異なる。
実施	③選定／提案 ④契約	委託先の選定において、情報セキュリティ対策の優先順位は高くない。
		委託先で実施する具体的な情報セキュリティ対策について、委託元・委託先間で事前に合意するのは容易ではない。
		委託業務の情報セキュリティ対策において、内部不正対策を含めることは少ない。
		委託元が要求する情報セキュリティ対策に委託先が対応できない場合、同等な代替策を提案させる。
		個々の案件において見積書に計上すべき情報セキュリティ対策について、委託元と委託先の認識にズレがある。
	⑤モニタリング ⑥インシデント対応	契約期間中、あるいは期間後のインシデント発生など新たな脅威に対し、委託元・委託先等のサプライチェーン上のパートナーと情報を共有するための合意がなされていない。
		委託元が委託先・再委託先以降の情報セキュリティ状況を把握したい範囲と確認できる範囲が異なる。

〇アンケート調査

- 国内のITシステム・サービスの委託元及び委託先を対象
- 回収は、委託元499件、委託先620件、計1,119件
- 委託元、委託先とも大企業、中小企業から一定の有効回答を確保*。
  委託元、委託先の抽出方法は以下の通り。
  - 委託元：総務省の「経済センサス」の日本標準産業分類に基づく従業員規模毎・業種毎の企業数分布に則り、層別抽出
  - 委託先：民間企業データベースからITシステムの構築・運用等に該当する業種の企業を抽出

〇インタビュー調査

- ITサプライチェーンにおいてインシデント対応やリスクマネジメントに関する知見を有する企業や有識者を対象にインタビュー調査を実施。実施概要は以下の通り。
  - 委託元（金融業、サービス業各1社）
  - 委託先ー国内IT企業（4社）
  - 委託先ーアジア圏IT企業・有識者（企業1社、有識者1名）
  - 有識者（2名）

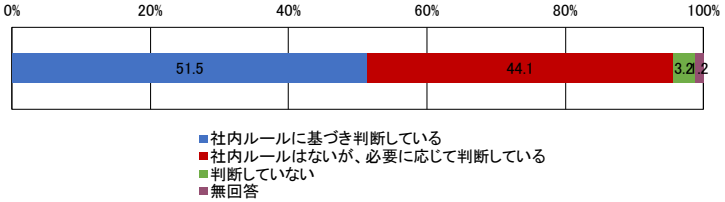
＊委託元は301人以上を大企業、300人以下を中小企業とした。委託先は101人以上を大企業、100人以下を中小企業とした。（中小企業庁の定義ではサービス業は100人以下を中小企業としている。）

社内ルールに基づく対策の判断に委託元と委託先で大きな差がある

- 業務委託で扱う情報資産やリスクに基づく情報セキュリティ対策の判断を、社内ルールに従い実施しているのは委託元で51.5%、委託先79.2%と30ポイント程度違いがある。（アンケート全体で委託先の方が情報セキュリティの脅威・リスクへの認識や対策の実施度が高い傾向がある。）
- 委託元では、情報セキュリティに関する委託先管理を実施する上で社内の人材不足や、すべての業務委託に対する統一的管理体制やルール適用が課題となっている。一方、委託先では委託元毎に様々な種類の受託業務に対応した情報セキュリティ対策を行う個別対応について課題意識がもたれている。

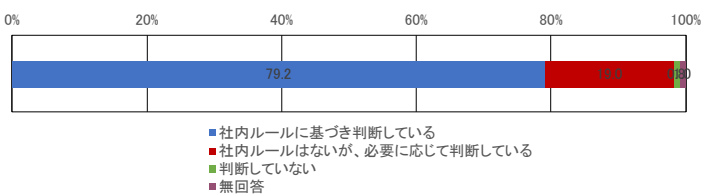
(N=499)

情報資産やリスクに基づく情報セキュリティ対策の判断



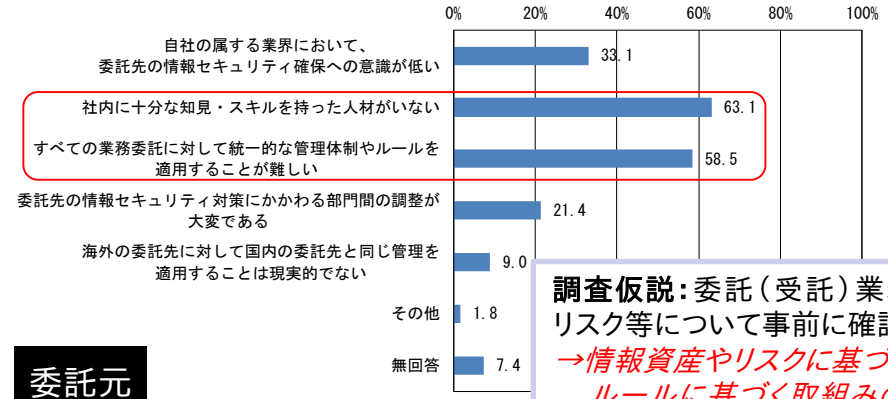
(N=620)

情報資産やリスクに基づく情報セキュリティ対策の判断



情報セキュリティに関する委託先管理の推進の課題

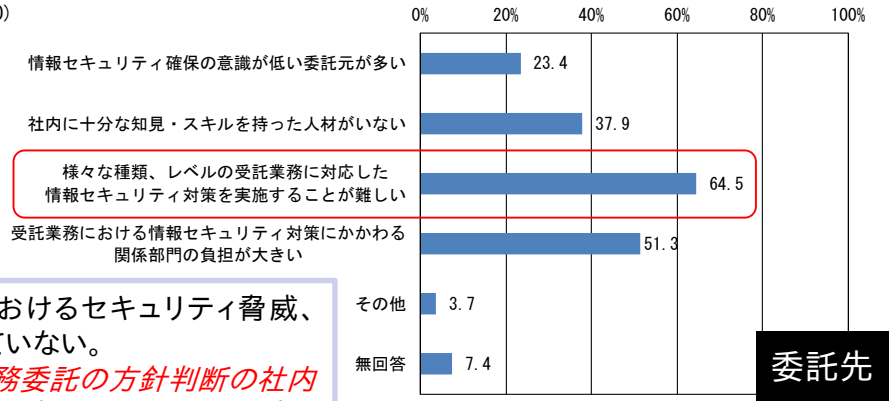
(N=499)



委託元

(N=620)

受託業務における情報セキュリティ対策の課題



委託先

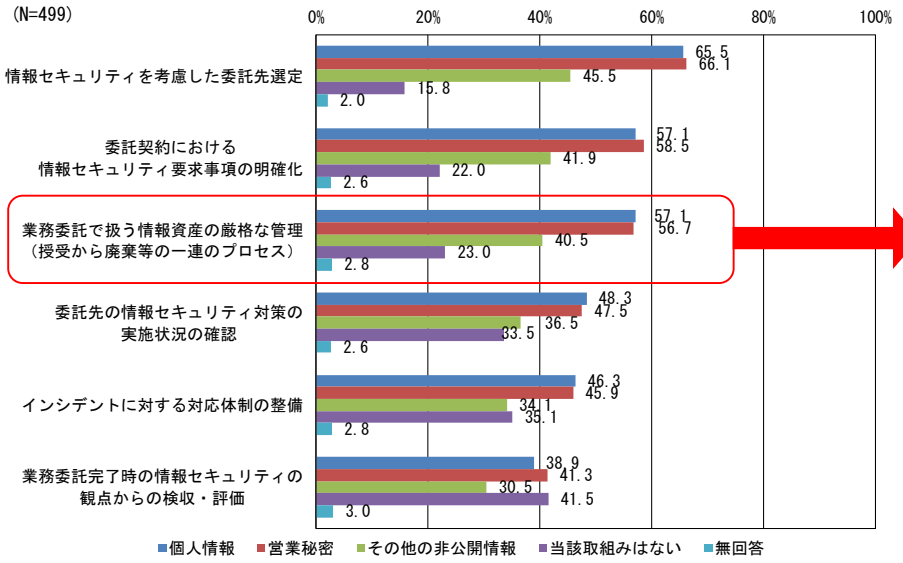
調査仮説：委託（受託）業務におけるセキュリティ脅威、リスク等について事前に確認していない。

→情報資産やリスクに基づく業務委託の方針判断の社内ルールに基づく取組みの浸透度は委託元と委託先で差がある

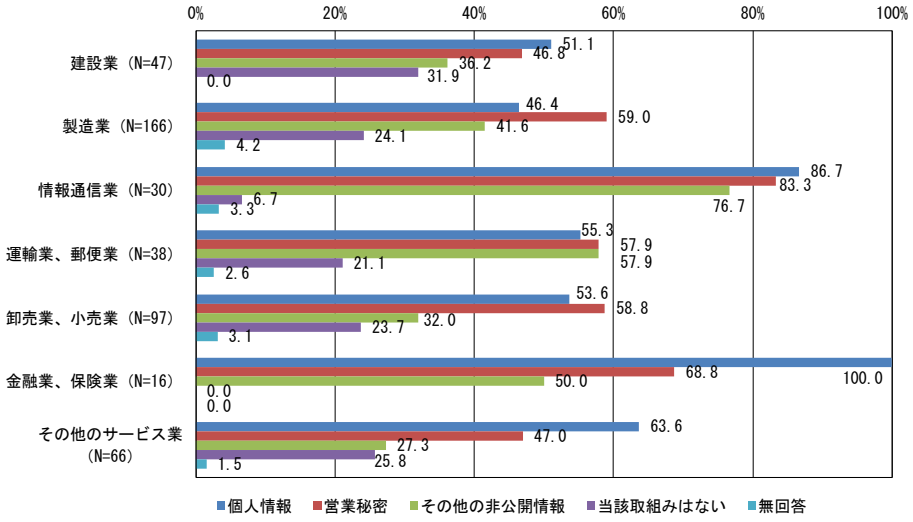
業種により情報セキュリティの取組みに差がある

- 委託元における情報セキュリティの委託先管理の取組みの実施状況は個人情報や営業秘密に対して特に実施率が高くなっている。
- 委託における情報資産の管理について、規制や監督官庁の指導がある業種では、委託先管理の取組みが浸透している。また、業種において重要度が高いと考えられる情報資産に対しては、実施率も高くなる傾向がある。（例：金融業、保険業は個人情報、製造業は営業秘密等）

情報セキュリティに関する委託先管理の取組みの実施状況



委託先管理のうち、「業務委託で扱う情報資産管理」の実施状況（業種別）



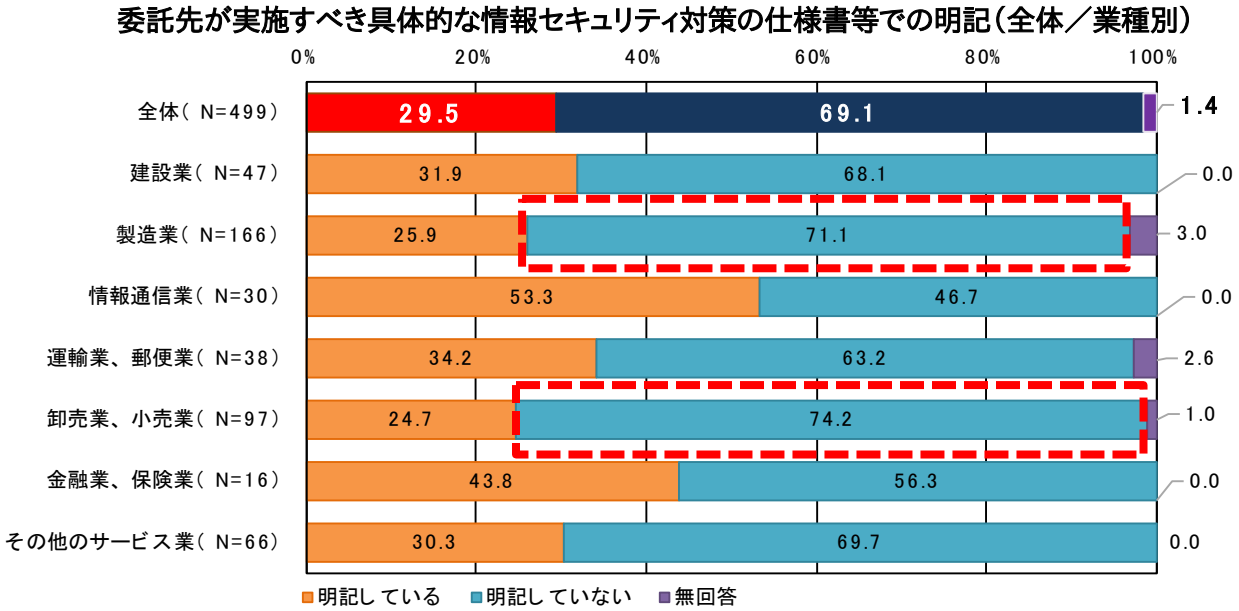
委託元

調査仮説：業務委託における情報セキュリティの取組みの実施状況は取り扱う情報資産の重要度によって異なる。
→情報資産により取組みの実施率が異なり、特に委託元では業種において重要度が高いと考えられる情報資産に対しては、実施率も高くなる

委託元の情報セキュリティに関する要件は仕様書等で委託先に明示できていない

- 委託元の回答企業のうち、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ないのは69.1%であり、全体の実施率は高くない。
- 特に、製造業は71.1%、卸売業、小売業は74.2%が明記しておらず、顕著である。
- 情報セキュリティの委託先管理の取組みが進んでいる情報通信業や金融業、保険業においては、仕様書等へ明記する実施率が高くなっているものの、高いとは言えない。
- 委託先へのインタビュー調査でも、委託元からセキュリティ要件が提示されるかは、業種によって差異があるとの意見があった。

委託元

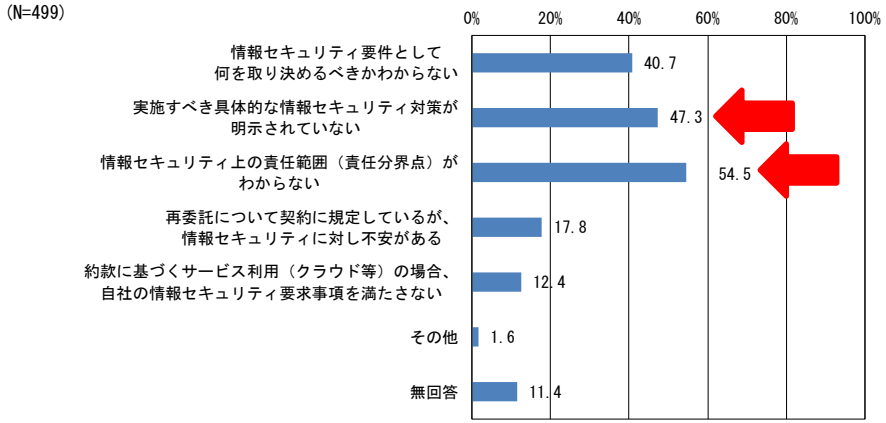


調査仮説: 委託先で実施する具体的な情報セキュリティ対策について、委託元・委託先間で事前に合意するのは容易ではない。
→情報セキュリティの委託先管理の取組みが進んでいる一部の業種を除き、委託元から具体的な情報セキュリティ対策が仕様書等で提示されることはまだ多くない。

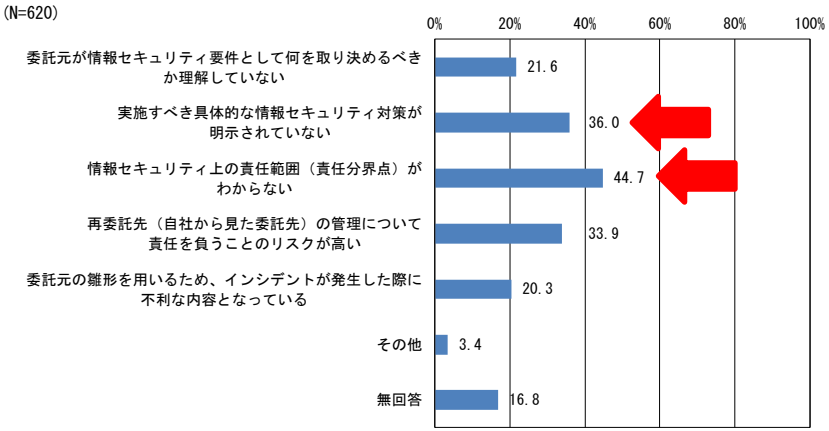
委託元と委託先の責任範囲明確化が課題

- 委託元、委託先とも、契約において情報セキュリティ上の責任範囲がわからない点を契約における課題として認識している。（委託元54.5%、委託先44.7%）
- 続いて、契約において実施すべき具体的な情報セキュリティ対策が明示されていない点が課題として認識されている。（委託元47.3%、委託先36.0% ）
- インタビュー調査からも、契約段階ではセキュリティに関する詳細な要件や責任範囲が定まっておらず、契約締結後の要件定義等の段階ですり合わせが行われているといった実態が聞かれた。

委託先との契約における課題



委託元との契約における課題



委託元

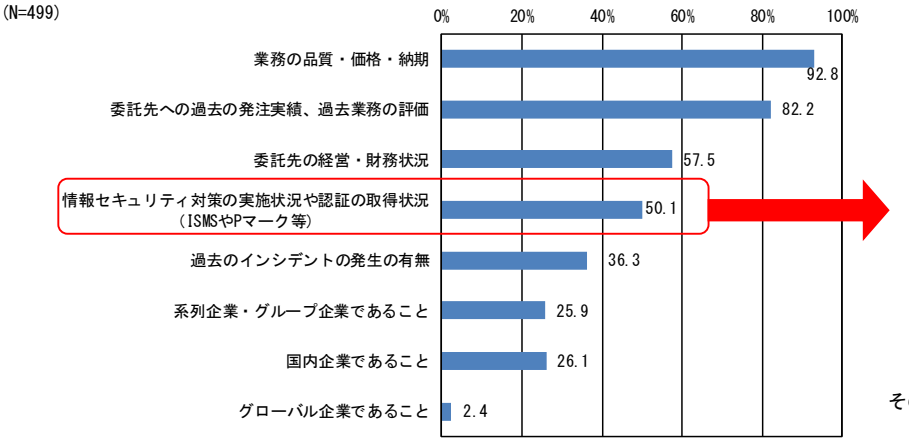
委託先

調査仮説：委託先で実施する具体的なセキュリティ対策について委託元・委託先間で事前に合意するのは容易ではない。
→契約段階で具体的な情報セキュリティ対策や責任範囲について合意することは現実的には難しい場合が多い。
このため、本来必要な情報セキュリティ対策が、抜け落ちてしまう可能性がある。

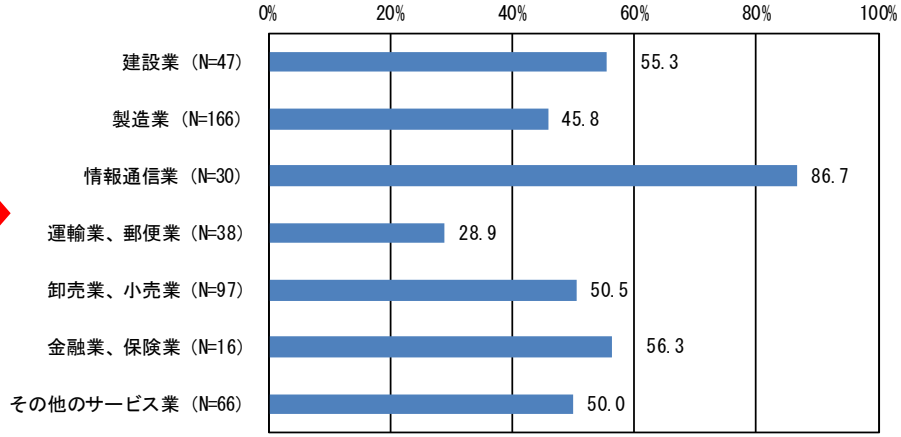
委託先選定において情報セキュリティ対策の優先順位はあまり高くない

- 委託元が、委託先選定において重視する点として、「業務の品質・価格・納期」、「委託先への過去の発注実績、過去業務の評価」、「委託先の経営・財務状況」に次ぎ、「情報セキュリティ対策の実施状況や認証の取得状況（ISMSやPマーク等）」は4番目の優先度である
- 委託元の業種別にみると、情報通信業で情報セキュリティ対策を優先事項として選択する企業が86.7%と高くなっている。情報セキュリティが自社の中核事業に直接かかわる要素であることが委託元の情報通信事業者での、優先順位を高くしていると思われる。

委託先選定において重視する点（合計値）



委託先選定において重視する点：情報セキュリティ対策の実施状況や認証の取得状況（ISMSやPマーク等）（業種別）



N=10以上の業種のみ

注）設問は優先順位順1～4位まで選択の複数回答設問だが、ここでは選択数を合算したグラフとしている（無回答除く）。

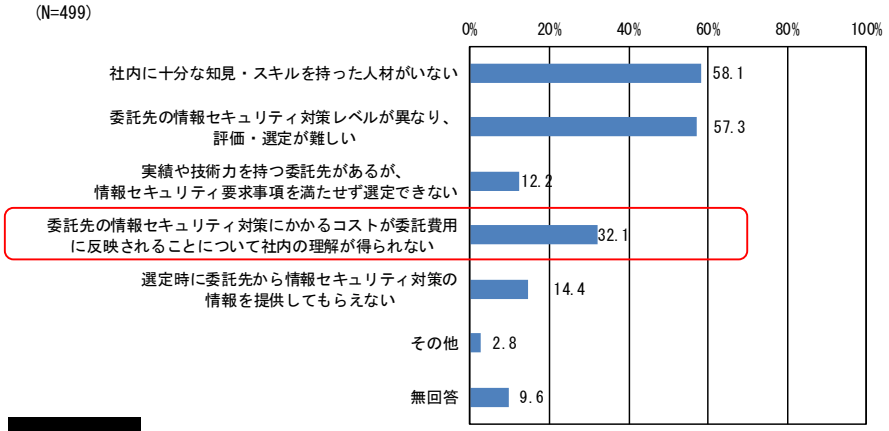
委託元

調査仮説：委託先の選定において、情報セキュリティ対策の優先順位は高くない。
→情報セキュリティが業務の品質・価格・納期、過去の実績、委託先の経営・財務状況といった他の要素に対して、優先されることは多くないのが実態と考えられる。

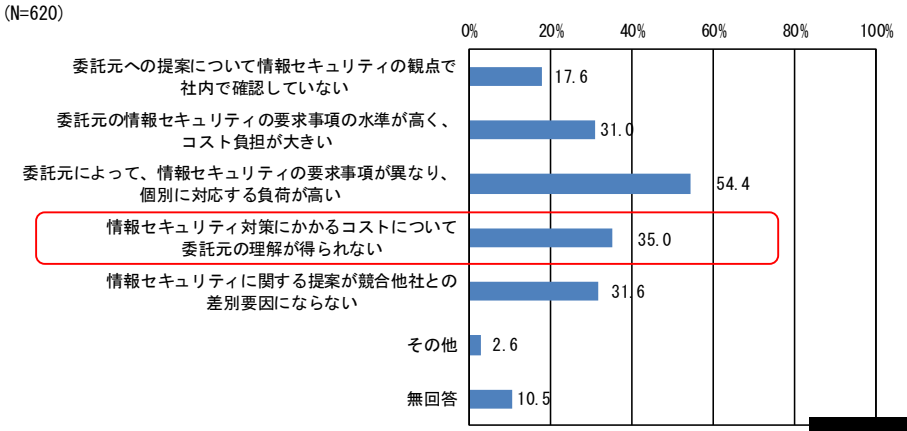
委託先の情報セキュリティ対策コストは委託元の社内で理解を得られにくい

- 委託元の回答企業では「委託先の情報セキュリティ対策にかかるコストが委託費用に反映されることについて社内の理解が得られない」（32.1%）、委託先の回答企業では「情報セキュリティ対策にかかるコストについて委託元の理解が得られない」（35.0%）と、委託先の情報セキュリティ対策のコストについて、同程度の課題意識があった。
- インタビュー調査からは、委託先が委託元への提案に情報セキュリティ対策にかかる費用をどのように計上するかは、委託先での既存の対策や受注戦略にも関係する部分であるが、提案の範囲に含まれない対策が考えられる場合には、提案時に費用見積とともに明示するべきという有識者の指摘があった。

委託先選定における課題



委託元への提案における課題



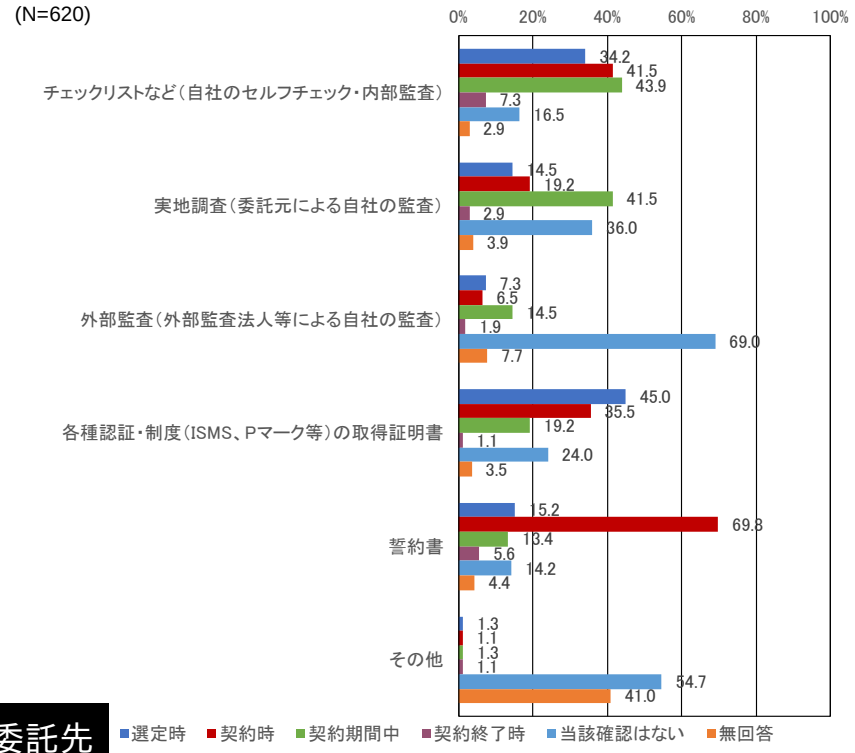
委託元　　委託先

調査仮説：個々の案件において見積書に計上すべき情報セキュリティ対策について、委託元と委託先の認識にズレがある。
→回答結果では、同程度の課題意識があった。しかし、「委託先の情報セキュリティ対策にかかるコストが業務費用に反映されることについて社内の理解が得られない」と委託元で回答されており、委託元の社内に認識の差があるようである。

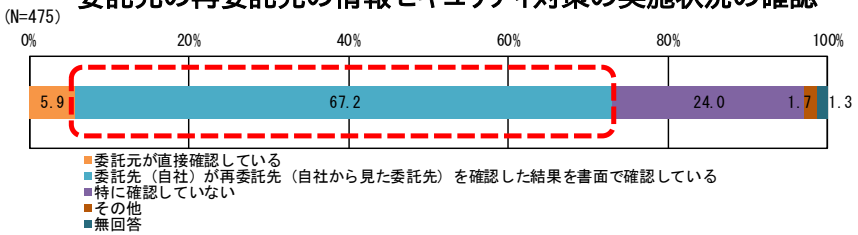
委託元は再委託先の情報セキュリティ対策実施状況を委託先に報告させる

- 委託先では、委託元からの情報セキュリティ対策の実施状況の確認として、様々なタイミングでチェックリストへの回答や実地調査等の対応が発生しているが、委託先からはこうした対応にかかる負担の課題も挙げられている。
- 再委託先がある委託先の67.2%が再委託先の情報セキュリティ対策の確認結果を委託元に報告している。（再委託先に対しては委託元から求められるレベルと同等のセキュリティ対策を要求することが多い）

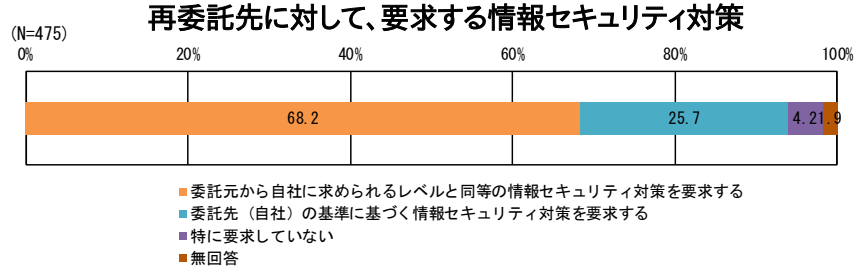
委託元からの情報セキュリティ対策の実施状況の確認方法・タイミング



委託元の再委託先の情報セキュリティ対策の実施状況の確認



再委託先に対して、要求する情報セキュリティ対策



調査仮説：委託元が委託先・再委託先以降の情報セキュリティ状況を把握したい範囲と確認できる範囲が異なる。
→委託元として再委託先を直接確認している企業は限定的であり、また確認を行う場合も基本的には委託先を介した確認となる。

まとめ

(1)委託元の情報セキュリティに関する取組みの強化

- 調査を通じて、委託先では情報セキュリティの取組みがある程度浸透している一方で、委託元では取組みが進んでいるのは情報通信業や金融業、保険業等の特定の業種に限定されている傾向がみられた。
- ITサプライチェーンリスクマネジメントは、委託元と委託先、再委託等のITサプライチェーンの関係者が各々業務を実施する上で適切な情報セキュリティを確保することでより効果的に実現される。本来あるべき姿として、委託元が情報セキュリティの確保を主導できるよう取組みの強化を図っていくことが必要と考えられる。

(2)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

- 調査を通じて、委託先は委託元から要求される情報セキュリティ対策の実施状況に関して、詳細なチェックリストや実地調査等に個別に対応している。また、委託元はそれらの結果の確認や評価に大きな労力を費やしている現状が見えた。
- こうした委託元、委託先の対応を効率化するため、委託先における対策の実施と委託元による対策の確認の両面で利用できる、ITサプライチェーンの情報セキュリティ対策に関する共通的な指標の確立が有効と考えられる。
- 委託先で最低限実施すべき情報セキュリティ対策が共通的に認識されることで、委託元では委託先の情報セキュリティ対策について確認すべき項目や評価方法が明確になるとともに、委託先でも共通的な指標に沿った対策の実施状況を提示することで、委託元ごとに個別の情報提示を行う手間が効率化されることが期待される。

(3)委託元と委託先の責任範囲明確化の必要性

- 調査を通じて、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という点が課題として認識されている。
- 委託元・委託先がリスクを正しく把握した上で必要な情報セキュリティ対策が実施されることを前提に、両者の責任範囲と負担について合意し、損害等の負担についても契約上で明記することが望ましい。

調査報告書等公開URL

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

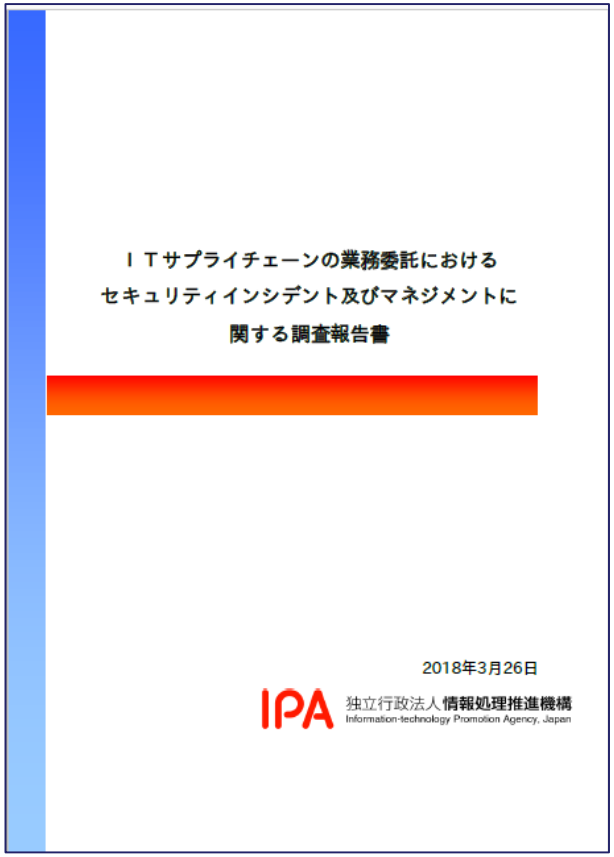
2. ITサプライチェーンにおけるインシデントの状況
   ITサプライチェーンにおけるインシデント事例、紛争の状況

3. ITサプライチェーンリスクマネジメントの標準と考え方
   ITサプライチェーンリスクマネジメントに関する基準、ガイドライン及び規格等、業務委託の全体像と 個別プロセスにおける情報セキュリティ確保の取組み

4. ITサプライチェーンリスクマネジメントに対する企業の取組みの現状
   調査仮説、回答者属性、業務委託の状況、取組み状況

5. まとめ

付録1 ITサプライチェーンで発生したインシデント事例集
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



https://www.ipa.go.jp/about/press/20180326.html