Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

委託契約時における IT システム・サービスのセキュリティ要件検討に関する一考察*

小山明美[1]　森淳子[1]　小川隆一[1]　竹村敏彦[2]

概要：IT システム・サービスに関する業務の委託元企業と委託先企業の間で交わされる契約において，その IT システム・サービスのセキュリティ要件を設定することは必ずしも容易ではない．また，個々のセキュリティ要件事項に係る責任範囲を取り決めておくべきか否か，さらにそれらを契約書類に明記しておくべきか否かなどについての統一的見解も今のところない．この結果，外部委託された IT システム・サービスに係るトラブルが後を絶たないのも事実である．本研究では，2020 年 2 月に独立行政法人情報処理推進機構（IPA）が実施したアンケート調査「IT システム・サービスの業務委託契約書見直しに関する実態調査」の結果などを用いた分析を通じて，委託契約時における IT システム・サービスのセキュリティ要件を検討するに当たって必要なことや望ましいこと（組織体制など）についての考察を行う．

キーワード：IT サプライチェーン，業務委託契約，セキュリティ要件

A Study on Reviewing Security Requirements of IT System/Services in Consignment Contracts

Akemi KOYAMA[†1]　Junko MORI[†1]　Ryuichi OGAWA[†1]
Toshihiko TAKEMURA[†2]

Abstract: When firms make a contract with the outsourcing of IT systems/services, it is not easy to set and agree security requirements of them. It is still now discussed whether they should clarify the responsibilities for information security or write clearly security requirements in contract documents. Unfortunately, we can find many disputes about outsourced IT system/services. In this article, by analyzing data collected from “Survey on the reviewing outsourcing agreement about IT system/service" which IPA conducted in February 2020, we investigate the success factors that we discuss security requirements of IT system/services in consignment contracts.

Keywords: IT supply chain, Outsourcing contract, Security requirements

1. はじめに

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の組織に及ぶため，被害の拡大や（早急な）問題解決が容易ではないことが指摘されている．「サイバーセキュリティ経営ガイドライン Ver2.0」[1]においても，ビジネスパートナーや委託先も含めた IT サプライチェーンに対するセキュリティ対策の必要性が強調され，また米国国立標準研究所（NIST）の「Cyber Security Framework Ver.1.1」[2]でもサプライチェーンリスクマネジメント（SCRM; Supply Chain Risk Management）の項目が大幅に強化されている．これらをはじめとする最近の動向を踏まえると，IT サプライチェーンリスクに対して適切な対応を技術的のみならず，マネジメントの観点からも多くの企業は考えておく必要がある．各種ガイドラインなどでは，広く企業に適用できるような（セキュリティ）要件の汎用化することなどを指摘するものもある．しかしながら，現実問題として，IT サプライチェーン上には，セキュリティ対策状況や組織内で要求されるセキュリティ水準が異なる企業が存在したり，そもそもリスクに対する認識も異なる企業が存在したりすることもあり，セキュリティガバナンスが十分に機能しない可能性がある．IT サプライチェーンリスクへの対応の一つとして，セキュリティ要件（IT システム・サービス毎に必要となる機能要件，非機能要件といった個別要件と，安心して取引を行うための前提ともいえる情報の取り扱いや管理体制，保証・責任範囲，情報セキュリティ対策など）を覚書や仕様書をはじめとする契約書関連文書に記載し，それについて予め合意をとっておくことが挙げられる．

2017 年に IPA が実施した「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」[3]から，回答した約 7 割の企業は委託先が実施すべき情報セキュリティ対策について仕様書等で明記していない実態があることなどを明らかにしている．2018

* 本研究の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

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

2 城西大学
Josai University

Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

年に IPA が実施した「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」[4]では，回答企業の多くが委託元企業の知識・スキル不足や継続契約のため責任範囲を見直す機会がないことなどを理由として責任範囲を明確にできないことを指摘している．また，責任範囲を明確化することは契約関連文書の見直しが委託元企業と委託先企業双方にとって有効になる一方で，コストや契約のあり方などの委託元企業と委託先企業ともに克服しなければならない問題があることもあわせて指摘されている．これらの複雑な問題があるがゆえに，IT システム・サービスの契約に関する統一的かつ明確な見解はいまのところない．

本研究では，これらの調査に引き続き、IPA が 2020 年 2 月に実施した「IT システム・サービスの業務委託契約書見直しに関する実態調査」[5]を用いて，委託契約時における IT システム・サービスのセキュリティ要件を検討するに当たって必要なことや望ましいこと（組織体制など）についての考察を行う．

2. 関連研究

本研究で取り上げる IT システム･サービスにおける業務の委託元・委託先に対するサイバー攻撃，調達したソフトウェアの未知の脆弱性，システム運用委託先における操作ミスなどによるシステム停止・情報流出・不正アクセスなどに関する課題に対して，様々な分野から研究アプローチが試みられ始めている．

技術面からアプローチしている研究として，文献[6]は製品に組み込まれるソフトウェア部品に注目して，不正な機能が混入する脅威を既存のセキュリティ技術を用いることで緩和できるか否かを検証している．その結果，単一の技術では全ての脅威のパターンに対応できず，複数の技術の組み合わせなければならないことなどを明らかにしている．また，文献[7]は，製品設計品質の可視化手法である Goal Structuring Notation と，テンプレートをもとに計算機リソースを自動構築する Infrastructure as Code の機能を活用したパブリッククラウド上に構築するシステムがセキュリティ要件を満たすことを確認・合意するための手法を提案している．このように技術面から IT システム・サービスの事業継続計画（BCP）をサポートする研究がここ数年進められている．

IT サプライチェーンは企業間での取り決めに基づき業務が遂行されるものであり，その取り決めは契約により法的に効力を持つこととなる．そのため，法律・契約面から法務・訴訟リスクについての研究が進められている[8-11]．いずれも，システム開発の特殊性を説明した上で，契約成立に関わる論点や債務不履行・瑕疵に関わる論点などを解説して，システム開発紛争にならないための対応策などを紹介している．また，2017 年 5 月に成立した民法の一部を改正する法律（平成 29 年法律第 44 号）が 2020 年 4 月より施行されたことにより，企業において契約内容の見直しを行う契機となった．しかしながら，2020 年 2 月時点でドラスティックに多くの企業で契約書などの見直しが進んだとは言いがたいという調査結果も報告されている[5].

マネジメント面からこれらのリスクにアプローチしている研究として，文献[12]は，IT システム・サービスにおけるサプライチェーンに関する問題点などを俯瞰した上で，複数の企業などが連携する組織形態において組織ごとに異なる IT ガバナンスを統合する仕組みの必要性を指摘している．また，文献[13]は業務委託の連鎖におけるリスク認識について現状の整理を行い，そのリスクを防止・低減するための提案を試みている．

さらに，アンケート調査の実施・その調査結果を用いた実証分析を行っている研究として，文献[14-16]がある．文献[14]は，IT システム・サービスに係る業務委託契約において扱う情報資産のセキュリティリスクの認識が委託元企業と委託先企業の間で異なるか否かなどについて分析を行っている．その結果，両者の間で IT システム・サービスの内容について，委託元企業と委託先企業の間には理解の不一致（認識の齟齬）が存在しがちであること，この認識のギャップを埋めるために綿密にリスクコミュニケーションをとることの必要性などを指摘している．文献[15]では，業務委託契約を行う際に契約書で情報セキュリティに係る要求事項に対する責任範囲の記載の仕方と企業属性などとの関係性についてデータ分析を行い，契約等における責任範囲を明確化させることにつながる要因を明らかにしている．また，文献[16]では，IT システム・サービスにおける情報セキュリティ要求事項に関する責任範囲の取り決めに対する考え方などについて分析を行い、委託元企業と委託先企業グループ間で情報セキュリティ要求事項の責任範囲の取り決めに対する考え方に差異があること，また，両者を比較すると，前者よりも後者の方が情報セキュリティ要求事項の責任範囲の取り決めに対する考え方の水準が高いことを明らかにしている．

この他にも，経済学の側面から、IT サプライチェーン上でインシデントが発生したとき，そのことがサプライチェーン上の企業の株価のリターンに与える影響について検証を試みる研究もある（文献[17]）．分析結果，インシデントの発生は委託先企業よりも委託元企業の企業価値を低下させてしまうことや，原因が不正アクセスの場合は継続的に企業価値が低下し続けることなどを明らかにしている．

法的側面，マネジメントの側面および経済学的側面からの研究が昨今進んでいるものの，まだその研究蓄積は十分であるとは言えず，未着手の課題がまだ山積している．

本研究では，IPA が 2020 年 2 月に実施した「IT システム・サービスの業務委託契約書見直しに関する実態調査」の調査結果を用いて，日本における IT システム・サービス

Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

の業務委託契約に関する状況を示すとともに，IT システム・サービスのセキュリティ要件を検討するに当たって必要なことや望ましいこと（組織体制など）についての考察を以下の節にて行っていく．

3. アンケート調査

3.1 調査概要

本研究では，IPA が 2020 年 2 月に実施した「IT システム・サービスの業務委託契約書見直しに関する実態調査」（以下，「IPA 調査」と称す）を用いる．この調査はインターネット調査形式で行い，調査対象者は，IT システム・サービスを発注している委託元企業（ユーザ企業），IT システム・サービスを受注している委託先企業（ベンダ企業）に所属している個人としている[a]．

IPA 調査では，企業規模（従業員数）や業種，所属部署などの基本情報に加えて，IT システム・サービスに関する委託・受託業務における役割分担や契約書の雛形の作成・見直し状況，セキュリティ要件を決める上で困っていることなどの実態を中心に質問を行っている．最終的な回答者数は，ユーザ企業所属の個人が 1366 人，ベンダ企業所属の個人が 1351 人である．なお，「IPA 調査」の単純集計などについては文献[5]を参照されたい．

また，ユーザ企業でかつ大企業（従業員数 301 人以上）に所属している個人は 684 人，ユーザ企業でかつ中小企業（従業員数 300 人以下）に所属している個人は 682 人である．同様に，ベンダ企業でかつ大企業（従業員数 101 人以上）に所属している個人は 677 人，ベンダ企業でかつ中小企業（従業員数 100 人以下）に所属している個人は 674 人である[b]．

以下，本研究と関連する質問項目と回答結果の概況を紹介する．

3.2 質問項目と概況

(1) IT システム・サービスに関する委託・受託業務における役割

図 1 は，IT システム・サービスに関する委託・受託業務における 4 つの役割（契約実務・契約推進・監督・監査・相談）の内容をまとめたものである[c]．また，図 2 には役割，図 3 にはその役割を兼務しているかどうかの状況をまとめている．図 2 を見ると，回答者の約 65%が「契約実務」に従事している一方で，「役割なし」と回答している割合が約 16%となっていることがわかる．図 3 から，約 60%の割合の回答者が単独の役割を担い，IT システム・サービスに関する委託・受託業務における役割を果たしている一方で，

契約実務	契約関連文書の作成
	取引先との間での契約内容・条件の調整
	契約関連文書の内容確認
	契約関連文書の承認・事務処理
契約推進	契約推進組織のリソースアサイン・組織化
	契約関連ルールの作成・見直し・承認
	契約関連文書の雛形の作成・見直し
	契約実務に係る人への教育・啓発
監督・監査	内部監査・点検・チェックリストの確認
	委託先監査・点検・チェックリストの確認
相談	組織内からの契約に関する相談
	契約に関するトラブル、訴訟の対応
役割なし	上記のいずれにも関与していない

図 1：IT システム・サービスに関する委託・受託業務における役割

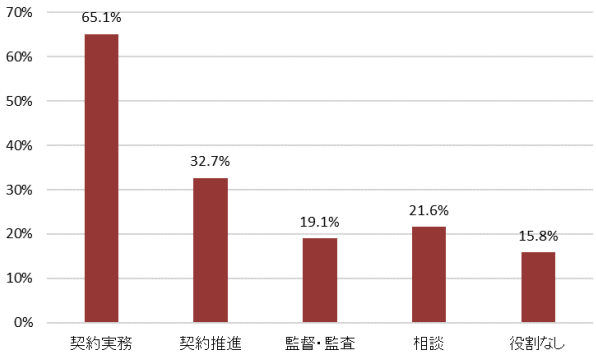

図 2：委託・受託業務における役割の分布

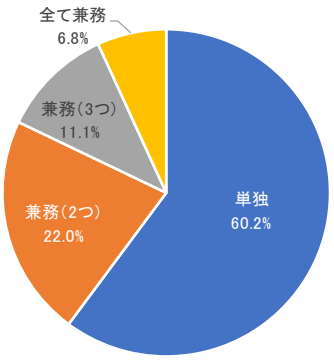

図 3：IT システム・サービスに関する委託・受託業務における役割の兼務状況

残りの割合の回答者が兼務を行っており，全ての役割を担っている回答者の割合が約 7%となっている．なお，2 種類の兼務の場合，「契約実務」と「契約推進」の組合せが一番多く，他の組合せと比較すると突出する結果となっている．

(2) 業務委託契約時にセキュリティ要件の具体的な内容の検討を行う部門（もしくは担当者）

図 4 は，（社内で）業務委託契約時にセキュリティ要件の

a IT サプライチェーンにおける位置づけを考えると，委託先企業は元請け（プライムベンダ），二次請け，それ以降と分けられる．このとき，二次請け以降の委託先企業にとってプライムベンダは委託元と捉えることができる．本研究において，混乱を招かないように，プライムベンダならびに二次請け以降を全てベンダ企業と統一して表現することとする．

b ユーザ企業とベンダ企業の大企業（中小企業）は基準となる従業員数が異なることに注意されたい．

c 「役割なし」とした回答者は本研究では分析の対象から外している．

Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

具体的な内容の検討を行う部門（もしくは担当者）につい

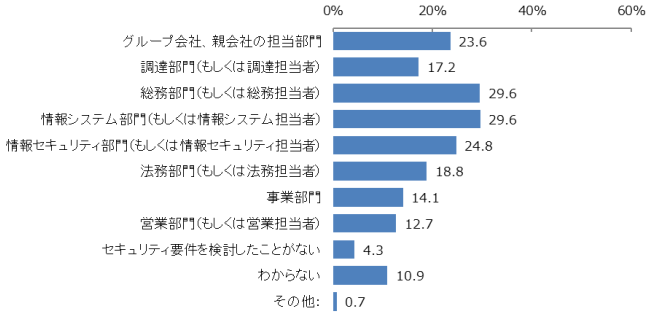

図 4：セキュリティ要件の具体的な内容の検討を行う部門（もしくは担当者）の分布

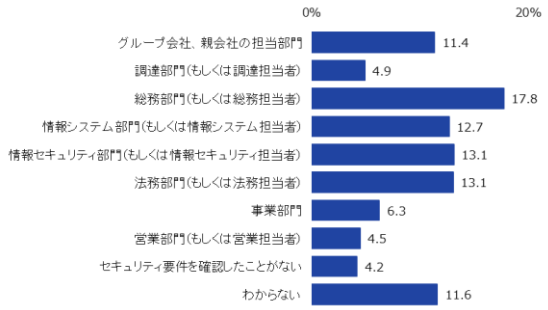

図 5：セキュリティ要件が適切に記載されていることを確認する部門（もしくは担当者）の分布

ての回答の分布である．図 4 から，「総務部門」や「情報システム部門」「情報セキュリティ部門」が IT システム・サービスに関する委託・受託業務契約においてセキュリティ要件の検討に携わっていることがわかる．「セキュリティ要件を検討したことがない」「わからない」を除いた回答者数は 1079 人であり，それらの内，単一の部署（もしくは担当者）でセキュリティ要件の検討を行っていると回答した人数は 595 人（約 55%），またセキュリティ要件の検討を行う部署の平均値は 1.91 となっている．

図 5 は，最終的に，業務委託契約時にセキュリティ要件が適切に記載されていることを確認する部門（もしくは担当者）についての回答の分布である．図 5 を見ると、最も回答が多いのが「総務部門」（約 17.8%），次に「情報セキュリティ部門」「法務部門」（約 13.1%），「情報システム部門」（約 12.7%）という順番になっている．

(3) 契約関連文書の雛形の作成や見直しを行う際のセキュリティ要件の内容を決めることができるか否か

「IPA 調査」では，契約実務担当者および「契約関連文書（仕様書，契約書など）の雛形の作成・見直しの役割」を経験した回答者に対して，契約関連文書の雛形の作成や見直しを行う際のセキュリティ要件の内容（図 6）を決めることができるか否かについて質問をしている．その結果が図 6 である．どのセキュリティ要件の内容でも，最も回答が多かったのは「決めたことはないがセキュリティ有識者

回答方向	決めたことがないので決められない	決めたことはないがセキュリティ有識者のサポートがあれば決められる	決めたことはないが自分で決められる	決めたことがある（セキュリティ有識者のサポートを受けながら決めた）	決めたことがある（自分で決めた）
納品後に公開された脆弱性の対応（未知の脆弱性の対応）	○1	○2	○3	○4	○5
委託先（プライムベンダ）のセキュリティ対策要件	○1	○2	○3	○4	○5
再委託先（二次請け）以降のセキュリティ対策要件	○1	○2	○3	○4	○5
自社のセキュリティ対策要件	○1	○2	○3	○4	○5
委託先のセキュリティ対策要件	○1	○2	○3	○4	○5
納品までに対処する既知の脆弱性の範囲	○1	○2	○3	○4	○5
納品までに対処する事を決めた範囲から納品日までの間に公開された脆弱性の対応	○1	○2	○3	○4	○5
納品後の保守対応	○1	○2	○3	○4	○5
システムの動作環境にかかわる要件（OSのサポート期間など）	○1	○2	○3	○4	○5
セキュリティ事故発生時の対応	○1	○2	○3	○4	○5

図 6：セキュリティ要件の内容

	n	決めたことがないので決められない	決めたことはないがセキュリティ有識者のサポートがあれば決められる	決めたことはないが自分で決められる	決めたことがある（セキュリティ有識者のサポートを受けながら決めた）	決めたことがある（自分で決めた）
1.納品後に公開された脆弱性の対応（未知の脆弱性の対応）	1081	335	423	121	134	68
	100.0	31.0	39.1	11.2	12.4	6.3
2.委託先（プライムベンダ）のセキュリティ対策要件	590	181	221	83	72	33
	100.0	30.7	37.5	14.1	12.2	5.6
3.再委託先（二次請け）以降のセキュリティ対策要件	590	195	209	89	63	34
	100.0	33.1	35.4	15.1	10.7	5.8
4.自社のセキュリティ対策要件	491	142	182	69	61	37
	100.0	28.9	37.1	14.1	12.4	7.5
5.委託先のセキュリティ対策要件	491	146	174	88	53	30
	100.0	29.7	35.4	17.9	10.8	6.1
6.納品までに対処する既知の脆弱性の範囲	1081	322	382	165	147	65
	100.0	29.8	35.3	15.3	13.6	6.0
7.納品までに対処する事を決めた範囲から納品日までの間に公開された脆弱性の対応	1081	325	382	163	136	75
	100.0	30.1	35.3	15.1	12.6	6.9
8.納品後の保守対応	1081	301	367	170	163	80
	100.0	27.8	34.0	15.7	15.1	7.4
9.システムの動作環境にかかわる要件（OSのサポート期間など）	1081	304	391	174	141	71
	100.0	28.1	36.2	16.1	13.0	6.6
10.セキュリティ事故発生時の対応	1081	306	402	158	139	76
	100.0	28.3	37.2	14.6	12.9	7.0

図 7：セキュリティ要件の内容を自身だけで決めることができるか否か

のサポートがあれば決められる」というものであった．また，図 7 からこれまで決めたことがあると回答した割合は 20%を下回っている．もちろん，回答者個人のセキュリティや契約の知識などを有しているか否かということも影響していることは否定できないが，担当者および担当者の所属している部署だけでセキュリティ要件の内容を決めることは必ずしも容易ではないことがうかがえる．

続いて，社内などで業務委託契約に関する契約関連文書の雛形の作成や見直しを行う際にセキュリティ要件について相談，連携ができる部門（もしくは担当者）があるか否かを合わせて質問した結果が図 8 である．図 8 を見てわか

Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

るように,「情報システム部門」と回答している割合が最も

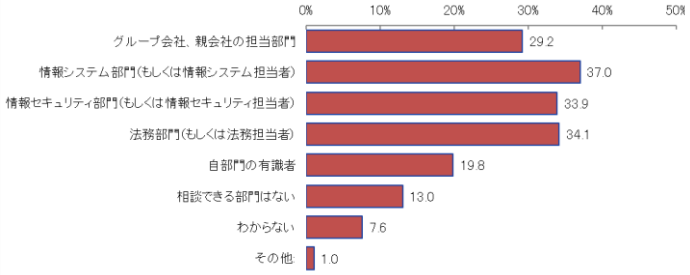

図 8：セキュリティ要件について相談，連携ができる部門（もしくは担当者）の有無

多くて約 37%，続いて「法務部門」（約 34.1%），「情報セキュリティ部門」（約 33.9%）となっている．一方で，「相談できる部門はない」「わからない」と回答している割合もそれぞれ約 13%と 7.6%ということがわかった．これらの割合は少ないものの，業務委託契約に関する契約関連文書の雛形の作成や見直しする際に支障をきたすことにつながる．

図 9 は、回答者の IT システム・サービスに関する委託・受託業務における役割と企業規模などの関係をまとめたものである．図 8 を見ると，どの企業規模であったとしても，また委託元企業でも委託先企業であったとしても，回答者の約 65%が「契約実務」に従事している一方で,「役割なし」と回答している割合が約 16%となっている傾向が変わらないことがわかる．

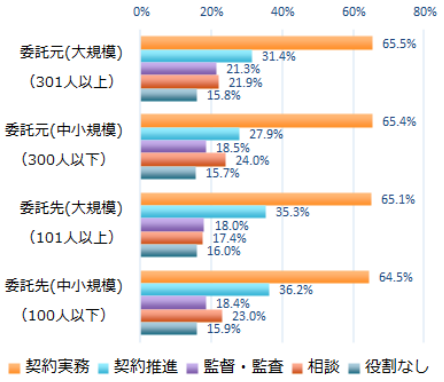

図 9：IT システム・サービスに関する委託・受託業務における役割と企業規模などの関係

図 10 には IT システム・サービスに関する委託・受託業務における役割の種類と企業規模などの関係を示している．図 10 を見ると，単独の役割を担っているケースは，委託元・委託先別ならびに企業規模別ではそれほど大きな違いがないことがわかる．一方で，2 種類以上のケースでは，若干の違いがあることが見てとれる．

また，図 11 には 2 種類以上の役割を担っている個人が所属している部署などをまとめたものである．図 11 を見てみると，最も人数が多い部署は「法務（部門）」であることがわかる．

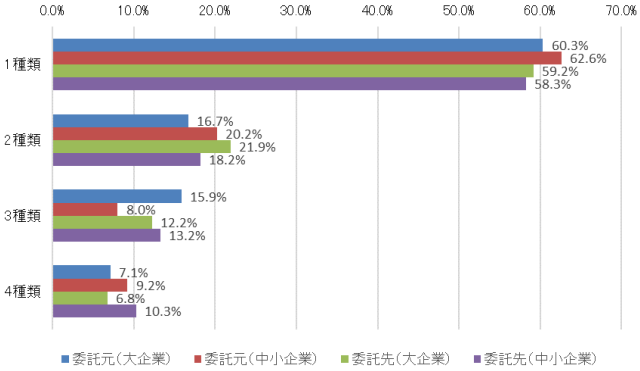

図 10：兼務の種類と企業規模などの関係

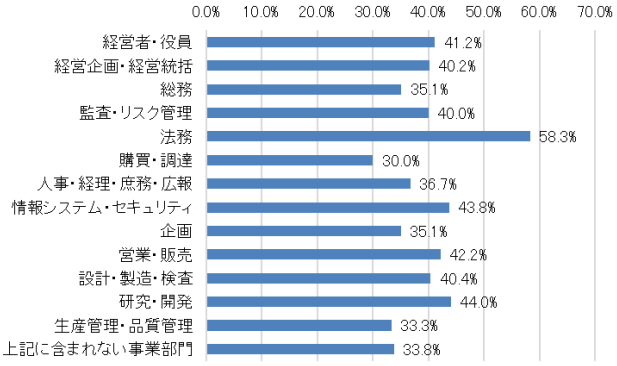

図 11：複数の役割を担っている個人が所属する部署など

4. おわりに

本研究では， IPA が 2020 年 2 月に実施した「IT システム・サービスの業務委託契約書見直しに関する実態調査」を用いて，委託契約時における IT システム・サービスのセキュリティ要件を検討に，どのような部門のどのような役割を担う人がかかわっているのかを，委託元，委託先という立場の違いや，従業員数の違いから確認をした．

その結果，契約に関する役割の中では，契約関連文書の作成や契約内容・条件の調整等の契約実務に携わる人が最も多かった．一人が複数の役割を担うことがあるので，兼務の状況について分析したところ，回答者の 4 割が兼務をしていた．組織の規模により，1 つの役割を単独で担うことができる組織と複数の役割を兼務する組織ができるかクロス集計を行い比較したが，今回の調査結果からは委託元，委託先，大規模，中小規模で大きな違いが無いことが分かった．また，契約について複数の役割を担うと回答した人の所属する部署を確認したところ,「法務部門」が最も多かったが，その他の部署が 40%前後で大きな違いは無かった．

次にセキュリティ要件の検討をどのような組織が行い，セキュリティ要件が適切に記載していることを最終的に確認するのはどの部門かを確認した．セキュリティ要件の最

Vol.2020-CSEC-91 No.30
Vol.2020-SPT-40 No.30
Vol.2020-EIP-90 No.30
2020/11/26

終的な確認は総務部門で実施するという回答が最も多かったが，それ以前の要件の検討については，総務部門，情報システム部門，情報セキュリティ部門がそれぞれ 24.8～29.6%を占めており，セキュリティに詳しい部署が協力して検討を行っていることが分かった．

過去の調査からセキュリティ要件を取り決めるうえでの課題として人材不足，スキル不足の問題が挙げられている．そのことを確認するため，契約実務担当者及び契約書の雛形の作成・見直しの役割を担う人に，セキュリティ要件を自身だけで決めることができるかを確認したところ，最も回答が多かったのは「決めたことはないがセキュリティ有識者のサポートがあれば決められる」，続いて，「決めたことが無いので決められない」というものだった．セキュリティの知識がある人材の不足はいまだに解決できておらず，セキュリティ有識者を社内に確保することは困難である．このような時にセキュリティの知識を有する委託先が委託元に代わってセキュリティ要件の整理やセキュリティ仕様の作成を行い，委託元がその内容を合意するという方法がしばしば取られている．委託元は委託先の言うなりになるのではなく，検討すべき要件はすべて盛り込まれているのか，リスクに対して十分な対策が取られているのかといったことを確認することが重要であり，また委託先はるどのようなリスクなのか，対策を実施しない場合どれくらいの影響が考えられるのかといった情報を委託元に説明し，対策の要否について合意することが大切である．

本調査では，契約実務，契約推進，監査・監督，相談という役割を担う人がどういう部署にいるのか，セキュリティ要件の検討をどういった部門で連携して実施しているのかを確認した．人材不足，スキル不足という課題を解決するために，どのような役割の人のスキルアップやセキュリティ要件の検討に最適な役割の配置など，さらに調査を行う必要があると考えられる．

参考文献

[1] 経済産業省・情報処理推進機構, サイバーセキュリティ経営ガイドライン Ver2.0, 2017，http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf（参照 20120-10-29）.
[2] National Institute of Standards and Technology: NIST Cybersecurity Framework，Version 1.1，2018，https://www.nist.gov/cyberframework（参照 20120-10-29）
[3] 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, https://www.ipa.go.jp/files/000065162.pdf（参照 2020-10-29）
[4] 情報処理推進機構，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，https://www.ipa.go.jp/security/fy30/reports/scrm/index.html（参照_2020-10-29）
[5] 情報処理推進機構，IT システム・サービスの業務委託契約書見直しに関する実態調査，2020，https://www.ipa.go.jp/security/fy2019/reports/scrm/index.html（参照_2020-10-29）
[6] 佐々木貴之, 既存セキュリティ技術のサプライチェーンへの適用の検討, SCIS2019 予稿集, 4D1-3, 2019
[7] 長谷亮・松浦陽平, パブリッククラウドでの情報システム構築における GSN を活用したセキュリティ要件のトレーサビリティ実現手法，研究報告セキュリティ心理学とトラスト（SPT）, 2019-SPT-32, 5, 1-6, 2019
[8] 伊藤雅浩・久礼美紀子・高瀬亜富, IT ビジネスの契約実務，商事法務, 2017
[9] 難波修一・中谷浩一・松尾剛行・尾城亮輔, 裁判例から考えるシステム開発紛争の法律実務, 商事法務, 2017
[10] 飯田耕一郎・田中浩之, システム開発訴訟，中央経済社，2018
[11] 松島淳也・伊藤雅浩，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, 2018
[12] 久保知裕・原田要之助，日本企業のサプライチェーンにおける情報セキュリティガバナンスに関する研究, IPSJ SIG Technical Report, 2014-EIP-63, 12, 1-6, 2014
[13] 渡邊浩平・後藤厚宏, IT サプライチェーンにおける業務委託リスクに関する考察, IPSJ SIG Technical Report 2020-EIP-89, 6,1-6, 2020
[14] 小山明美・小川隆一・竹村敏彦, IT サプライチェーン上の情報セキュリティリスク認識に関する分析， SCIS2019 予稿集, 4D1-5, 2019
[15] 森淳子・小山明美・小川隆一・竹村敏彦, IT サプライチェーンの責任範囲の実態から見た対策強化のための提案, CSS2019 予稿集, 1B3-5, 2019
[16] 森淳子・小山明美・小川隆一・竹村敏彦，IT サプライチェーンのセキュリティ要求事項に関する分析～責任範囲の取り決めに対する考え方～, SCIS2020 予稿集, 2D3-4, 2020
[17] 竹村敏彦・小山明美・小川隆一, IT サプライチェーン上のセキュリティインシデントが企業価値に与えるインパクト～イベントスタディによる検証～，SCIS2020 予稿集, 2D3-3, 2020