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*

森　淳子[1,†]　小山 明美[1]　小川 隆一[1]　竹村 敏彦[2]

概要：多くの企業では，IT システム・サービスに関する業務を委託し，さらにその業務を再委託先等へと連鎖していく IT サプライチェーンが展開されている．一方，IT システム・サービスへの要求は複雑化しており，業務委託契約時に情報セキュリティに係る責任分界点が明確にされないままでシステム構築等が進められることもある．このような状況であれば，セキュリティリスクに直面した際トラブルなどになることも少なくなく，また，セキュリティリスクへの対応や収束の遅延につながることも懸念される．しかしながら，業務委託契約時において情報セキュリティに係る責任範囲を明確化するべき必要性が求められるが，慎重な意見も見受けられる．本研究では，このような背景を踏まえて，2018 年 11 月に独立行政法人情報処理推進機構が実施した「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」の委託先企業を対象とした調査結果を用いて，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の範囲の記載の仕方と企業属性との関係について分析する．分析結果を踏まえて，IT サプライチェーンにおけるセキュリティ対策強化のためには，契約書の雛形を作成することが有効な対策であることを提案する。

キーワード：IT サプライチェーン，順序ロジット回帰分析，業務委託契約，責任範囲

Proposals for strengthening measures from the viewpoint of the department of the IT supply chain

Junko Mori[1,†]　Akemi Koyama[1]　Ryuichi Ogawa[1]　Toshihiko Takemura[2]

Abstract: Many companies consign work related to IT systems and services, and further chain that work to a subcontractor etc. The IT supply chain is being developed. On the other hand, the demand for IT system services is complicated, and outsourcing contracts in some cases, system construction may be promoted without clarifying the demarcation point for information security. In such a situation, there are many problems such as when you encounter security risks, and security There is also concern that response to the risk and delay in convergence may occur. However, at the time of outsourcing contract there is a need to clarify the scope of responsibility for the security, but some cautious opinions can be seen. With this background in mind, in this study, the Information technology Promotion Agency, Japan implemented the IT Supply Chain in November 2018.Using the results of the survey, When conducting a consignment agreement, the contract analyzes the relationship between the scope of responsibility for information security requirements and the company's attributes. Based on the results of the analysis, we propose that it is effective to create a template for contracts in order to strengthen security measures in the IT supply chain.

Keywords: IT Supply chain, Order logit regression analysis, Business consignment contract, Area of responsibility

1. はじめに

近年，多くの企業における 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，ますます複雑化の様相を呈している．また，企業固有の仕様が有り汎用的な製品・サービスを利用できない分野では，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プロジェクトがスタートし，IT システム・サービスの本番稼働後に，情報セキュリティインシデントが発生することも少なくない[1][2]．さらに，IT システム・サービスにおいて，設計・開発・製造・運用・保守・廃棄に至るまでの一連のプロセスにわたり，業務の一部を系列企業やビジネスパートナー等に外部委託し，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は一般的となっている（このような外部委託者が関与する供給の連鎖は「IT サプライチェーン」と呼ばれる）．通常，委託元企業は委託先企業に対して情報セキュリティに関する多種多様なリスクの管理に関する直接的な統制（ガバナンス）を行うことが容易ではない．そのため，委託関係が重層的に連鎖する場合は，より一層ガバナンスを効かすことが困難である．

これらの状況に対して，欧米では，企業がセキュリティ対策を実施することに加えて，その対策が定められた基準

* 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
† j-mori@ipa.go.jp

を満たしていることを証明することが求められるようになっている．具体的に，米国では 2017 年にサイバーセキュリティフレームワーク（NIST（National Institute of Standards and Technology）策定のガイドライン）の中にサイバーサプライチェーンリスクマネジメント（SCRM; Supply Chain Risk Management）が明記されることに至った[3]．また，NIST は，ベストプラクティスとして，不要な機能やサービスの停止，ユーザの権限の制御，ユーザの認証，データやトラフィックの保護などを IT サプライチェーンリスクマネジメント戦略として挙げるとともに，RFP（Request For Proposal）にセキュリティの条件を入れることや，その要件を満たすことが出来ないベンダを排除することなどを調達のリスクのマネジメントとして行うべきことを整理している[4][5].

日本においても，経済産業省・独立行政法人情報処理推進機構（IPA）は 2017 年に改訂した「サイバーセキュリティ経営ガイドライン Ver2.0」において，サイバーセキュリティ経営の重要 10 項目の一つとして「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握＜サプライチェーンセキュリティ対策の推進＞」(監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について，系列企業，サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせることや，システム管理等の委託について，自組織で対応する部分と外部に委託する部分で適切な切り分けをさせることを指示している）が含められることとなった[6].

2017 年に情報処理推進機構（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」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確認され，また契約等において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を明らかにしている[7]．また，この調査報告書では IT サプライチェーンリスクマネジメントのあるべき姿やベストプラクティスの考察が行われている. 2018 年には, この調査結果を受けて，IPA は「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」を実施している[8][a]．この調査から，特に新たな脅威（脆弱性等）について文書で責任範囲を明確にできていないこと等が明らかにしている．また，責任範囲が明確にできない理由として（多くの企業が）委託元の知識・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多くの企業が挙げている．さらに，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・委託先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・委託先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．

本研究では，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試み，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する．そのために，「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」の委託先企業を対象とした調査結果を用いる．この分析結果を踏まえて，IT サプライチェーンにおけるセキュリティ対策強化のための提案を行う．

2. 関連研究

サプライチェーンとは，ある商品の原材料が調達されてから，その商品が最終的に消費者までに届くまでの生産・流通のビジネスプロセスのことを指し，このプロセスにはいくつもの企業が携わっている．それゆえに，このサプライチェーン上で何らかのトラブルが生じれば，ビジネスが止まってしまう危険性があり，事業継続性の観点から様々な研究が行われている[9][10]．サプライチェーン上に存在するリスク（サプライチェーンリスク）は相互依存性（interdependency）を持っているがゆえに，単独でリスクに対する対策を講じるだけでは不十分なものとなってしまう可能性が容易に想像できる．その意味において，サプライチェーンリスクへの対策は喫緊かつ深刻な課題であるといえる．とりわけ，本研究で取り上げる IT サービス・システムにおける情報セキュリティに係るリスク（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）は，上述したように，既に顕在化しており，時としてこれを契機に裁判にまで発展することもある．

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，原田・久保[11]や小山他[12]などがある．原田・久保[11]は，IT サービス・システム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，小山他[12]は，IT サービス・システムに係る業務委託（受託）業務で扱う情報資産のセキュリティリスクの認識にユーザ企業（委託元）とベンダ企業（委託先）の間でギャップがあるかどうか，また委託元・委託先の属性別に見たリスク認識の違いを，アンケート調査結果[7]の統計分析を通じて検証を試み，両者の間で情報セキュリティリスク認識にズレがあることや企業属性によりユーザ企業間やベンダ企業間でも情報セキュリティリスク認識に差異がある[8].

a 「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」とす

ことなどを明らかにしている．そして，情報セキュリティリスク認識のギャップを埋められるよう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を指摘している．

また，技術面からアプローチしている研究として，佐々木[13]や長谷・松浦[14]などがある．佐々木 [13]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た結果，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．長谷・松浦[14]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．

これらの関連研究からもわかるように，サプライチェーンリスクに関する研究蓄積は必ずしも十分な水準にあるとは言えない．今後，これらの研究蓄積が国内外ともに進むことが期待される．

3. IT サプライチェーンにおける責任範囲に関する環境の変化

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．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が，ユーザ企業とベンダ企業の間に存在する情報の非対称性やコミュニケーションの不足から，責任範囲が明確にならず，紛争に発展することもある．

法律・契約面から法務・訴訟リスクについてアプローチしている伊藤他[15]，難波他[16]，飯田・田中[17]，松島・伊藤[18]の研究がある．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，IT システム・サービスの内容について，両者の間には（深刻な）理解の不一致（認識の齟齬）が存在しがちであることなどもあわせて指摘されている．2017 年 6 月 2 日に「民法の一部を改正する法律」（法律第 44 号）が公布され，2020 年 4 月から施行される．改正される民法では，請負契約の瑕疵担保責任の規定が削除され，契約不適合責任に代わる．これに伴い契約目的の明確化や責任追及期間が延びることへの対応など，ユーザ，ベンダ双方で対応が必要である．

日本の商慣行において，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散見されている[7]．また，何か問題が起きたときは話し合いによって十分に解決できるという考え方がまだ根強く残っている．これは，当事者間の信頼関係が築かれていることを意味していると考えると良いことかもしれない．しかしながら，常にサイバー攻撃や未知の脆弱性が存在することやシステム開発の特殊性に加えて，ユーザ企業とベンダ企業の認識の齟齬などが散見されることを考えると，契約にて両者の「責任範囲」を明確化しておくことが必要であると考えられる．本研究のように，データ分析を通じて契約などにおける責任範囲の明確化につながる要因を明らかにする試みは国内外ともに珍しいものであり， IT サプライチェーンリスクマネジメントに関して学術的にも実務的にも大きく寄与することが期待される．

4. アンケート調査

4.1 調査概要

本研究では，IPA が 2018 年 11 月から 2019 年 2 月にかけて，国内の IT システム・サービスのユーザ企業およびベンダ企業を対象に実施した「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によって収集された調査結果のうち，ベンダ（委託先）企業を対象としたもの」（以下，SC 調査と称す）を用いて分析を行う．SC 調査は，SC 調査では，IT システム・サービスに関する受託業務における情報セキュリティ対策などの現状を把握するとともに，2017 年度以降における IT システム・サービスに関する受託業務に関する契約の個別事例（以下，当該事例と称す）について情報セキュリティ要件の明確化の状況等を中心に質問を行っている．なお，SC 調査では 428 社から回答を得ている．割付や調査手法，単純集計の結果などの詳細は「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[8]を参照されたい．

4.2 質問項目と概況

以下，簡単ではあるが，本研究の分析で用いた質問項目と回答結果の概況を紹介する．

(1) 当該事例における責任範囲の明確化の程度

「SC 調査」では，当該事例における契約関連文書に情報セキュリティに係る要求事項をどのような形で記載されているかについて質問している．なお，情報セキュリティに係る要求事項としては「インシデントが発生した場合の対応」「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」「再委託の禁止または制限」「契約終了後の情報資産の扱い（返却，消去，廃棄等）」などがある．また，契約関連文書としては「契約書」「約款」「委託元の仕様書」「覚書」などがあるが，本研究では「契約書」のみを取り上げる．この質問に対して，「1. 契約書は使用していない」「2. 契約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」「3. 当該項目の記載があるが，委託先（貴社）が責任を負うべき範囲が明示されていない（「都度調整」等）」「4. 当該項目について，委託先

（貴社）が責任を負うべき範囲が明示されている」の中から 1 つだけをそれぞれの情報セキュリティに係る要求事項に対して，回答者に選んでもらっている[b]．

図 1 に責任範囲の明確化の程度の分布を表す（#=398）．図 1 を見てわかるように，「契約書は使用していない」と回答した企業の割合は 1 割程度であり，多くの企業では「契約書」により，取り決めを行っている．しかし，「委託先が責任を負うべき範囲が明示されている（取り決められている）」という回答にはバラつきがある（18.3～57%）．

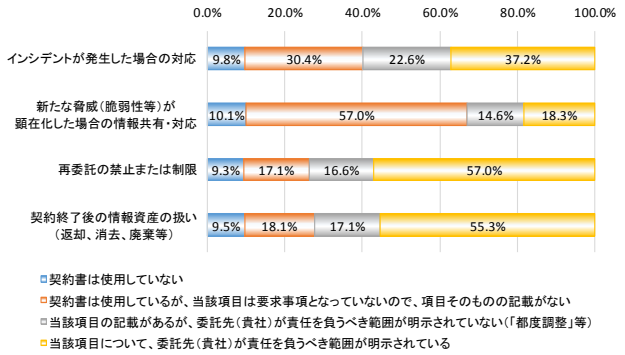

図 1　責任範囲の明確化

Figure 1　Clarification of department.

(2)　当該事例における委託元企業の業種

図 2 に，当該事例における委託元企業の業種の分布を示す（#=407）．委託元企業の業種は情報通信業で最も多く 123 件（30.2%）である．これは，二次請け以降の委託先の場合，委託元はベンダ企業（情報通信業）が多いためである．続いて製造業が 74 件（18.2%）と他の業種に比べて多い．

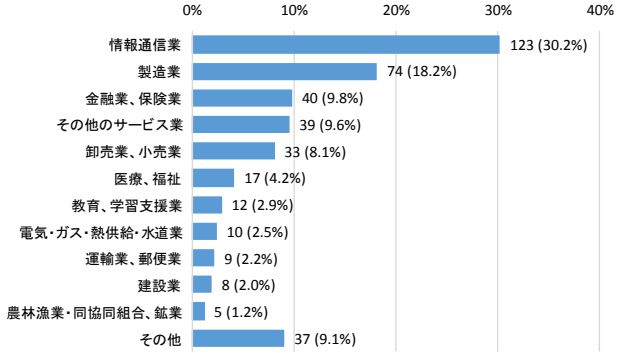

図 2　ユーザ企業の業種

Figure 2　Industry sectors of Users.

(1)　当該事例における提供 IT システム・サービス

図 3 に，当該事例において提供している IT システム・サービスの分布を示す（#=329）．元請け（プライムベンダ）は，ソフトウェア開発だけでなく，保守や運用など他のサービスも合わせて提供できることが多く，当該事例でも複数回答が多かった．

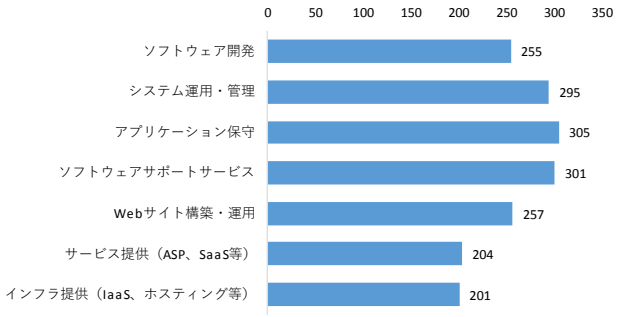

図 3　提供 IT システム・サービス

Figure 3　Supplied IT system/service.

(3)　当該事例におけるサプライチェーンでの位置づけ

「SC調査」では，当該事例のITサプライチェーンにおける，位置付けに関して質問した．委託先企業407社のうち251社（61.7%）が元請け（プライムベンダ），156社（38.3%）が二次請け以降であると回答した．このことから，回答企業の多くがプライムベンダであることがわかる．

(4)　当該事例における情報セキュリティ上のリスクに対する懸念の程度

「SC 調査」では，当該事例の業務で扱う情報資産に関して，契約の際に情報セキュリティ上のリスクをどの程度懸念しているかについて質問し，それに対して「非常に懸念した」「ある程度懸念した」「あまり懸念しなかった」「全く懸念しなかった」「わからない」のいずれか 1 つを回答させた．図 5 は情報セキュリティ上のリスクに対する懸念の程度の分布を表している（#=406）．特徴的なこととして，「人的ミス」「システム障害，停止」に対する懸念は同様の傾向にあることがわかる．また，「内部不正」について懸念を抱いている企業の割合は約 45%にとどまった．

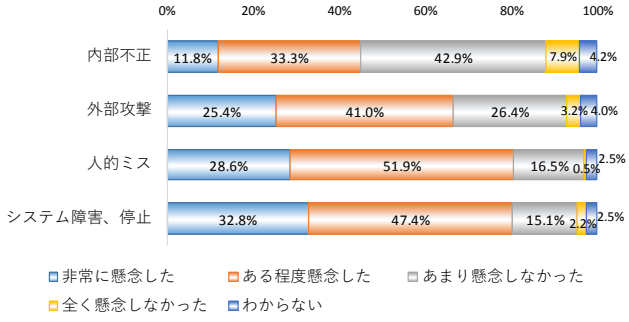

図 5　情報セキュリティ上のリスクに対する懸念

Figure 5　Matters of concern involved the security.

b 注意すべき点として，当該項目を「契約書」に記載されていないとしても，他の「約款」「委託元の仕様書」「覚書」などに記載されていることもあることを断っておく．

(5) 当該事例における契約書の雛形

当該事例において使用した契約書の書式が委託元のものか，委託先のものかについて質問した，その回答分布は図6の通りである（#=393）．6割を超える企業が委託元企業の契約書の書式を採用している．

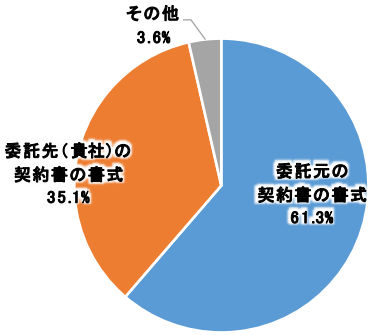

図 6　採用した契約書の書式

Figure 6　Adopted form of contract document.

(6) 情報セキュリティ要求事項を含んだ契約書の雛形の有無

「SC 調査」では，情報セキュリティ要求事項を含んだ契約書の雛形を持っているか否かについて質問した．その回答分布が図 7 である（#=428）．回答企業の約 4 分の 1 が情報セキュリティ要求事項を含んだ契約書の雛形を持っていないことが図 7 より見てとれる．

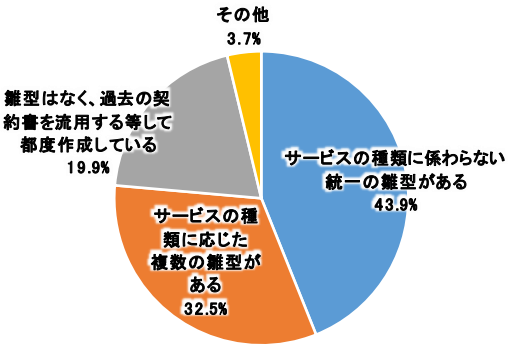

図 7　契約書の雛形の有無

Figure 7　Templates of contract documents.

(7) 企業規模

委託先企業の総従業員数（正社員，準社員等を含む）の分布は図 8 の通りである（#=428）．図 8 を見ると，100 名以下の企業の割合は約 6 割となり，回答企業の多くが中小企業であることがわかる．

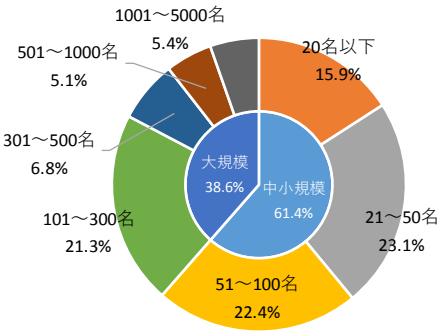

図 8　委託先企業の規模（従業員数）

Figure 8　Company size of venders.

5. フレームワーク

5.1 モデル

本研究では，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」[8] (2019b)において立てられた仮説をもとに，第 4.2 節で紹介した「責任範囲の明確化の程度」に影響を与えると考えられる委託元（ユーザ）企業ならびに委託先（ベンダ）企業の特性との関係を分析する．そのため，心理学や経済学，経営学をはじめ様々な分野で説明変数と被説明変数の関係を捉える分析手法の一つである順序ロジット回帰モデルを採用する（本研究で用いる被説明変数である「責任範囲の明確化の程度」は順序尺度である）．

順序ロジット回帰モデルとは，順序付けした選択肢に対して，対象がどのような選択をしたかという情報を集めることによって，事後的に対象者が順序付けされたそれぞれの選択肢を選ぶ確率を求めて，その選択がある判断から次の判断に変わる閾値を求めることができる（この閾値間の距離によって，選択肢間の親近性などがわかる）ものである．ロジット回帰モデルにおいて確率比であるオッズ比で説明変数の効果を評価するのと同様に，順序ロジット回帰モデルにおいてはオッズ比の相対比（比例オッズ）を用いて説明変数の効果を評価することができる．この順序ロジット回帰モデルにおける係数は最尤法を用いて推定される．なお，順序ロジット回帰分析の詳細については Hosmer, et al. [19]などを参照されたい．

5.2 変数の加工

本研究では，4.2 節で紹介した「責任範囲の明確化の程度」を順序尺度と見なして，被説明変数とする．ここでアサインされる値が大きいほど，責任範囲の明確化が行われていると解釈する．

また，説明変数としては 4.2 節で紹介した「業種」「提供 IT システム・サービス」などを用いる．なお，「業種」に関しては，製造業，情報通信業，金融・保険業に関してダミ

ー変数（当該業種であれば 1，そうでなければ 0 がアサインされる変数）を作成した．同様に，「提供システム・サービス」「サプライチェーンでの位置づけ」もダミー変数として採用している．「情報セキュリティ上のリスクに対する懸念の程度」「企業規模」に関しては，アサインされる値が大きいほど，その変数の程度が大きくなるように加工を行った[c]．

最後に，「契約書の雛形」については当該事例において使用した契約書の書式と委託先（ベンダ）企業が情報セキュリティ要求事項を含んだ契約書の雛形持っているか否の質問を組合せて 3 つのダミー変数を作成した．1 つが委託元（ユーザ）企業が作成した書式の契約書を利用したもの（以下「委託元企業の書式」），もう 1 つが委託先（ベンダ）企業内で統一した情報セキュリティ要求事項を含む契約書の雛形を持ち，それを利用したもの（以下「委託先企業の雛形（統一）」）である．最後が委託先（ベンダ）企業内でサービスごとに複数契約書の情報セキュリティ要求事項を含む雛形を持ち，それを利用したもの（以下「委託先企業の雛形（複数）」）である[d]．

5.3 分析結果

表 1 には，契約書において情報セキュリティに係る要求事項（「インシデントが発生した場合の対応」「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」「再委託の禁止または制限」「契約終了後の情報資産の扱い（返却，消去，廃棄等）」）の「責任範囲の明確化の程度」を被説明変数とするロジット回帰分析の結果をまとめている[e]．欠損値などを除いた結果分析に用いたサンプルサイズは 354 である．

「インシデントが発生した場合の対応」においては，「委託先企業の雛形（複数）」の係数が 1%水準，「委託元企業の書式」「人的ミスへの懸念」の係数が 5%水準，「アプリケーションの保守」「委託先企業の雛形（統一）」「従業員数」の係数が 10%水準で統計的に有意となっている．

「新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応」においては，「金融業・保険業」「委託先企業の雛形（複数）」の係数が 1%水準，「委託元企業の書式」「委託先企業の雛形（統一）」の係数が 5%水準，「システム運用・管理」「従業員数」の係数が 10%水準で統計的に有意となっている．

「再委託の禁止または制限」においては，「内部不正への懸念」「委託元企業の書式」「委託先企業の雛形（統一）」「委託先企業の雛形（複数）」の係数が 1%水準，「金融業・保険業」「サービス提供」の係数が 5%水準，「従業員数」の係数が 10%水準で統計的に有意となっている．

「契約終了後の情報資産の扱い（返却，消去，廃棄等）」においては，「金融業・保険業」「委託元企業の書式」「委託先企業の雛形（統一）」「委託先企業の雛形（複数）」の係数が 1%水準，「人的ミスへの懸念」の係数が 5%水準，「サービス提供」「従業員数」の係数が 10%水準で統計的に有意となっている．

表 1　分析結果

Table 1　Results of ordered logit regression analysis.

		インシデントが発生した場合の対応				新たな脅威（脆弱性等）が顕在化した場合の情報共有・対応			
		Coef.	S.E.	z	p	Coef.	S.E.	z	p
業種	製造業	−0.081	0.291	−0.280	0.782	0.179	0.307	0.580	0.560
	情報通信業	−0.047	0.270	−0.170	0.861	0.302	0.286	1.060	0.291
	金融業・保険業	0.443	0.367	1.200	0.228	1.159	0.380	3.050	0.002
提供ITシステム・サービス	ソフトウェア開発	0.430	0.287	1.500	0.134	0.046	0.302	0.150	0.880
	システム運用・管理	−0.167	0.250	−0.670	0.503	−0.496	0.267	−1.860	0.063
	アプリケーション保守	−0.479	0.261	−1.830	0.067	−0.058	0.276	−0.210	0.832
	ソフトウェアサポートサービス	0.389	0.272	1.430	0.152	0.440	0.288	1.520	0.127
	Webサイト構築・運用	−0.163	0.269	−0.610	0.545	−0.181	0.286	−0.630	0.526
	サービス提供	−0.476	0.343	−1.390	0.165	−0.516	0.374	−1.380	0.168
	インフラ提供	−0.035	0.357	−0.100	0.923	0.284	0.390	0.730	0.466
サプライチェーンでの位置づけ	プライムベンダー	0.045	0.253	0.180	0.859	0.214	0.264	0.810	0.417
情報セキュリティ上のリスクに対する懸念の程度	内部不正への懸念	−0.004	0.152	−0.020	0.981	0.142	0.162	0.880	0.381
	外部攻撃への懸念	0.083	0.153	0.540	0.588	0.208	0.162	1.280	0.200
	人的ミスへの懸念	0.374	0.185	2.020	0.044	0.093	0.198	0.470	0.637
	システム障害、停止への懸念	0.115	0.160	0.720	0.473	−0.014	0.173	−0.080	0.937
契約書の書式	委託元企業の書式	0.728	0.331	2.200	0.028	0.761	0.367	2.070	0.038
	委託先企業の書式（統一雛形）	0.762	0.403	1.890	0.059	0.999	0.445	2.240	0.025
	委託先企業の書式（複数雛形）	1.270	0.414	3.070	0.002	1.375	0.441	3.120	0.002
企業規模	従業員数	0.124	0.071	1.760	0.078	0.137	0.075	1.830	0.067
閾値	/cut1	0.431	0.695			0.068	0.732		
	/cut2	2.462	0.695			3.315	0.752		
	/cut3	3.511	0.708			4.180	0.764		
	Number of obs	354				354			
	LR chi2(19)	41.340				40.610			
	Prob > chi2	0.002				0.003			
	Pseudo R2	0.046				0.051			
	Log likelihood	−431.726				−380.787			
		再委託の禁止または制限				契約終了後の情報資産の扱い（返却、消去、廃棄等）			
		Coef.	S.E.	z	p	Coef.	S.E.	z	p
業種	製造業	0.216	0.315	0.690	0.493	0.393	0.314	1.250	0.211
	情報通信業	0.233	0.295	0.790	0.429	0.047	0.292	0.160	0.873
	金融業・保険業	0.965	0.430	2.250	0.025	1.338	0.454	2.950	0.003
提供ITシステム・サービス	ソフトウェア開発	−0.077	0.311	−0.250	0.804	−0.175	0.317	−0.550	0.581
	システム運用・管理	−0.398	0.271	−1.470	0.142	−0.405	0.267	−1.520	0.129
	アプリケーション保守	0.328	0.291	1.130	0.260	−0.091	0.286	−0.320	0.751
	ソフトウェアサポートサービス	0.187	0.298	0.630	0.531	0.313	0.292	1.070	0.284
	Webサイト構築・運用	0.129	0.298	0.430	0.664	−0.145	0.287	−0.510	0.613
	サービス提供	−0.702	0.361	−1.950	0.052	−0.652	0.351	−1.860	0.063
	インフラ提供	−0.106	0.387	−0.270	0.785	0.104	0.377	0.280	0.783
サプライチェーンでの位置づけ	プライムベンダー	0.026	0.279	0.090	0.925	−0.185	0.278	−0.670	0.505
情報セキュリティ上のリスクに対する懸念の程度	内部不正への懸念	0.447	0.172	2.600	0.009	0.198	0.170	1.160	0.245
	外部攻撃への懸念	−0.112	0.166	−0.670	0.500	0.021	0.166	0.130	0.898
	人的ミスへの懸念	0.234	0.198	1.180	0.238	0.474	0.197	2.410	0.016
	システム障害、停止への懸念	0.110	0.170	0.650	0.518	−0.013	0.173	−0.080	0.939
契約書の書式	委託元企業の書式	1.217	0.339	3.590	0.000	1.266	0.341	3.720	0.000
	委託先企業の書式（統一雛形）	1.259	0.428	2.940	0.003	1.489	0.436	3.410	0.001
	委託先企業の書式（複数雛形）	1.573	0.441	3.570	0.000	1.676	0.438	3.830	0.000
企業規模	従業員数	0.144	0.081	1.790	0.073	0.138	0.079	1.750	0.080
閾値	/cut1	0.814	0.734			0.649	0.741		
	/cut2	2.277	0.736			2.160	0.742		
	/cut3	3.128	0.746			3.035	0.752		
	Number of obs	354				354			
	LR chi2(19)	56.690				61.110			
	Prob > chi2	0.000				0.000			
	Pseudo R2	0.072				0.076			
	Log likelihood	−365.410				−373.647			

なお，全ての情報セキュリティに係る要求事項において

c 「わからない」と回答しているものについては欠損値として扱って分析を行う．

d いずれにおいてもゼロがアサインされた場合は委託先企業で情報セキュリティ要求事項を含む雛形を持たず，それを利用したものになる．

e 本研究では統計ソフトウェアとして Stata/MP2 15.1 を用いている．

有意となったものは「委託元企業の書式」「委託先企業の雛形（統一)」「委託先企業の雛形（複数)」「従業員数」の係数である.

いずれかの情報セキュリティに係る要求事項において統計的に有意となった「金融業・保険業」「内部不正への懸念」「人的ミスへの懸念」「委託元企業の書式」「委託先企業の雛形（統一)」「委託先企業の雛形（複数)」「従業員数」の係数の符号は正，「システム運用・管理」「アプリケーションの保守」「サービス提供」の係数の符号は負の値をとっている．例えば，「従業員数」の係数が正であることは，委託先企業の従業員数が多いほど，責任範囲の明確化がなされる傾向にあると解釈することができる.

これ以外の係数に関してはいずれも統計的に有意な結果が得られていない．ここで，統計的に有意となっていないことは「責任範囲の明確化にこれらが影響を全く与えないということではなく，比例オッズがちょうど 1 になっていること」を意味しているということに注意しなければならない.

5.4 考察・提案

ここでは，第 5.3 節で示した分析結果についての考察を行う．まず，業種別では，金融業・保険業の場合に，多く責任範囲を明示している傾向がみられた．金融業・保険業は業界としての対策の推奨や金融庁[20]による取組指導によりセキュリティ対策を意識した結果になっているのではないかと考えられる．また提供した IT システム・サービスの種類別では，サービス提供(ASP,SaaS 等）の場合「再委託の禁止または制限」「契約後の情報資産の扱い」の責任範囲を明示していない傾向がみられた．これはサービスの特性上再委託や契約終了時の情報の取り扱いについては契約書ではなく約款で取り決められている事が理由と考えられる.プライムベンダか二次請け以降かによるサプライチェーンの位置づけにおいては傾向の違いはみられなかった．これについては，別の分析手法やさらに深ぼりした分析をすることで傾向の違いが見える可能性も考えられるため、今後の検証課題と考える.情報セキュリティ上のリスクに対する懸念の程度では「人的ミスへの懸念」が高いほど「インシデントが発生した場合の対応」と「契約終了時の情報資産の扱い」の責任範囲を明示している傾向がみられた．これは，ミスが発生すること，ミスによるサービス提供のために利用した情報資産の漏洩などを意識していると考えられる．また「内部不正への懸念」が高いほど「再委託禁止または制限」についての責任範囲を明示している傾向がみられた．これは再委託する事により，管理が行き届かなくなることを意識していると考えられる．契約時に用いた契約書の書式としては、「契約書の雛形がない」場合と「委託先企業の書式」「委託先企業の雛形（統一)」「委託先企業の雛形（複数)」を用いた場合のオッズ比で評価した結果、全ての要件において責任範囲を明示している傾向がみられた.その中でも「委託先企業の雛形（複数)」を用いた場合,より責任範囲を明示している傾向がみられた.これは委託対象となる IT システム・サービスの内容を,委託元より理解している委託先がサービスの種類ごとに作成している雛形には詳細に責任範囲を明確化するための項目が記載されているということが考えられる。企業規模では，従業員数が多いほどセキュリティ要件の責任範囲を取り決めている傾向がみられた．これは従業員数が多いほどセキュリティ対策の専門部署の設置や担当者をアサインする事ができるためであると考えられる.

6. おわりに

多くの企業では，IT システム・サービスに関する業務を委託し，さらにその業務を再委託先等へと連鎖していく IT サプライチェーンが展開されている．一方，IT システム・サービスへの要求は複雑化しており，業務委託契約時に情報セキュリティに係る責任分界点が明確にされないままでシステム構築等が進められることもある．このような状況であれば，セキュリティリスクに直面した際トラブルなどになることも少なくなく，また，セキュリティリスクへの対応や収束の遅延につながることも懸念される．しかしながら，業務委託契約時において情報セキュリティに係る責任範囲を明確化するべき必要性が求められるが，慎重な意見も見受けられる．本研究では，このような背景を踏まえて，2018 年 11 月に独立行政法人情報処理推進機構が実施した「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」の委託先企業を対象とした調査結果を用いて，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の範囲の記載の仕方と企業属性との関係について分析した．その結果，委託元（ユーザ）企業の業種，業務委託契約した IT システム・サービスの種類，情報セキュリティ上のリスクに対する懸念の程度等によって，責任範囲の明示にいくつかの傾向がある事が確認された.更に,従業員数が多いほどおよび委託先（ベンダ）企業が契約書の雛形を持っている場合，分析の対象としたセキュリティ要件全てにおいて，より責任範囲を明示していることが確認された．従業員数を増やすことで対策する事はできないが，従業員が少ない企業でも，業務委託契約書の雛形を作成することで，責任範囲を明示する事が可能となる．これらの分析結果を踏まえて，IT サプライチェーンにおけるセキュリティ対策強化のためには，契約書の雛形を作成することが有効な対策であることを提案する.

参考文献

[1] 細川義洋，成功するシステム開発裁判に学べ!，技術評論社, 2017,

[2] 情報処理推進機構，情報セキュリティ白書 2019～新しい基盤，巧妙化する攻撃：未知のリスクに対応する力を，情報処理推進機構, 2019,

[3] National Institute of Standards and Technology: NIST ，Cybersecurity Framework Version 1.1，2018, https://www.nist.gov/cyberframework（参照　2019-8-21）

[4] National Institute of Standards and Technology: Best Practices in Cyber Supply Chain Risk Management (Best Practices for Cyber Security SupplyChain Risk Management) , 2017, https://www.nist.gov/sites/default/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf（参照　2019-8-21）

[5] National Institute of Standards and Technology: Best Practices in Cyber Supply Chain Risk Management (Managing Supply Chain Risks End-to-End) , 2017, https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Cisco-Cyber-SCRM-Case-Study.pdf（参照　2019-8-21）

[6] 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　2019-8-21）

[7] 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 2019-8-21）

[8] 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

[9] 苦瀬博仁，サプライチェーン・マネジメント概論：基礎から学ぶ SCM と経営戦略，白桃書房， 2017

[10] 西岡正・目代武史・野村俊郎，サプライチェーンのリスクマネジメントと組織能力～“熊本地震”における「ものづくり企業」の生産復旧に学ぶ，同文館，2018

[11] 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, Vol.2014-EIP-63, No.12, 2014

[12] 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 Proceedings, 4D1-5, 2019

[13] 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 Proceedings, 4D1-3, 2019

[14] 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）, Vol.2019-SPT-32, No.5, 1-6, 2019

[15] 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

[16] 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

[17] 飯田耕一郎・田中浩之，システム開発訴訟，中央経済社, 2018

[18] 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

[19] Hosmer, D.W., Lemeshow, S., Sturdivant, R.X.: Applied Logistic Regression (Wiley Series in Probability and Statistics) 3rd edition, Wiley, 2013

[20] 金融分野におけるサイバーセキュリティ強化に向けた取り組み方針，https://www.fsa.go.jp/news/30/20181019/cyber-policy.pdf(参照　2019-8-21）