「IT システム・サービスの業務委託契約書見直しに関する調査」
～インタビュー結果（取り組み事例）～

2020 年 3 月発行

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

目次

はじめに

「IT システム・サービスの業務委託契約書見直しに関する調査」では、アンケート調査だけでなく、インタビュー調査も行った。

アンケート調査では、企業・組織の対策・取り組みの傾向や従事する人々の意識等から全体的な実態を知ることが可能であるが、個別の企業・組織が何をしているのか、どうしてそうすることにしたのかといった活動の詳細やなぜそのようになったのか背景を知ることが困難である。そのため、アンケートの回答者から、契約に関連する業務経験があり、自社の取組みについて紹介いただける方に協力いただき、インタビューを行った。そのインタビューの中から、契約やセキュリティのマネジメントについて参考となる知見をいくつか事例としてまとめた。なお、企業が特定できる情報は公開しないことを条件に協力いただいたため、一部表現や用語については加筆・修正を行っている。

インタビュー調査概要

<table>
<tr><td>調査方法</td><td colspan="4">個別インタビュー</td></tr>
<tr><td>調査対象</td><td colspan="4">東京都、神奈川県、埼玉県、千葉県にお住まいで、IT システム・サービスの業務委託、受託において契約実務[1]、契約推進[2]、監督・監査[3]、相談[4]に 3 年以上携わった経験のある、主任以上の役職者。</td></tr>
<tr><td>調査期間</td><td colspan="4">2020 年 2 月 16 日～2020 年 2 月 27 日</td></tr>
<tr><td rowspan="4">実施人数</td><td colspan="4">9 人</td></tr>
<tr><td colspan="2">委託元(発注企業)</td><td colspan="2">委託先(受注企業及び受発注企業)</td></tr>
<tr><td>大規模
(301 人以上)</td><td>中小規模
(300 人以下)</td><td>大規模
(101 人以上)</td><td>中小規模
(100 人以下)</td></tr>
<tr><td>3 人</td><td>2 人</td><td>2 人</td><td>2 人</td></tr>
</table>

記載上の注意

「見直し」には「点検」すること、点検した結果「改訂」することの両方の使われ方があるため、本取り組み事例の中では、なにがしかの点検を行うことを「点検」、点検の結果、変更や修正を行ったことを「改訂」と記載している。

---

[1] 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・事務処理等。

[2] 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・啓発等。

[3] 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等。

[4] 組織内からの契約に関する相談、契約に関するトラブル、訴訟の対応等。

1. 業務委託契約に関する組織の連携、知識、情報の共有について

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」（以下「2018 年度調査」とする）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実施できないという組織も多いことが分かった[5]。同調査では、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として、個人情報保護法改正、GDPR[6]の施行、「 AI ・データの利用に関する契約ガイドライン[7]」の公表、そして民法改正を挙げていた。これらのような法規制への対応は、情報システム部門、情報セキュリティ部門だけでなく、法律の専門知識を保有する部門や担当との連携が不可欠であり、協力体制の構築と知識・情報の共有が求められる。

以下に協力体制の構築や知識・情報の共有に関する取り組みの事例を示す。

事例 1	民法改正をきっかけとした勉強会の実施
プロフィール	委託元企業　大規模　製造業
情報システム部内で契約担当者を中心に、法務部門と連携した勉強会を実施している。管理職以上が参加しており毎月テーマを決めて、法務部員と顧問弁護士の先生に参加いただき、民法改正の内容について 2~3 時間の意見交換を行っている。 勉強会で学んだ内容は、管理職から各担当者に周知。業務委託契約の決裁は各課長から法務部門にまわる手順であるが、法務部に提出される前に課長が気づき、担当者に差し戻す事ができている。また、担当者に不明点があっても法務部門に確認する前に情報システム部門の管理職に聞けば回答が得られる状況になってきており、勉強会の内容が実務に活かされている。 民法改正をきっかけに、法務部門が古い基本契約書全ての点検を実施したところ、現状にそぐわない契約内容が残っていることを見つける事ができた。勉強会をきっかけに、情報システム部門からも意見を出したことで、より現状に即した内容に改訂できた。この機会に基本契約書全体を点検し、改訂する事ができたのは、良い影響であった。	

[5] 「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」報告書について https://www.ipa.go.jp/security/fy30/reports/scrm/index.html
[6] EU 一般データ保護規則（General Data Protection Regulation）
[7] 「AI・データの利用に関する契約ガイドライン 1.1 版」を策定しました https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html

事例２	現場からの意見を取り入れた点検
プロフィール	委託先企業　中小規模　ソフトウェア業
業務委託契約書の雛形は定期的ではないが、ソフトウェア開発部門や営業部門などの現場から点検をした方が良いという意見が上がってくるためそのタイミングで点検の有無について検討を実施している。 企業規模が小さく幹部会に営業部門とソフトウェア開発部門の現場担当者が同席することが可能であることから、幹部会の場で現場の声を直接伝えるように配慮し、民法改正における雛形の点検は社内の会議体（幹部会）の中で営業部門、ソフトウェアの開発部門と一緒に検討した。	

事例３	定期的な勉強会の実施と民法改正をきかっけとした点検
プロフィール	委託先企業　中小規模　金融保険業界向け情報システム子会社
業務委託契約書の雛形には点検のルールがあり、法務部門の点検担当者が半年に一回点検をしている。法務部門内で点検の担当者を中心に公務員の上級試験向けのテキストを参考とて民法に関する勉強会を実施している。 勉強会の中で、民法改正をきっかけに以前の契約書に問題はないのかという意見が上がったことから点検に着手した。民法改正をきっかけとして以前の契約書の点検にも着手できた事は良い影響があったと考えている。	

事例４	部門間の情報共有のための定期的な会議の開催
プロフィール	委託元企業　大規模　製造業
会議を半年に一回定期的に開催している。法務部門、情報システム部門、人事部門で部門長から担当者までが出席し、情報システム部門で作成している WEB サイトの著作権の問題や社内コンテンツについて法律や人事的な観点について違法な事がないか議論している。 会議体で部門間の意見交換を行う事を通して、業務内容や専門的な知識、動向などの情報を共有できている。 民法改正に関する契約書の雛形の点検についても本会議体で議論した。	

事例５	有識者の活用による体制構築
プロフィール	委託元企業　中小規模　学術研究、専門・技術サービス業
（契約や業務遂行に関連して）何か問題あった場合、常にプロのアドバイスをうけながら適宜判断している。具体的にはまずは社労士に相談をする。社労士、弁護士、会計事務所が連携しており、社労士に相談をすると他の二者にも伝わり、適切なアドバイスをもらうことができるような体制を構築している。	

幸いにして、今までに大きなセキュリティ事故はないが、トラブルやセキュリティ事故が発生した場合にどのような対応が必要か否か適宜弁護士から情報を収集している。

2. 瑕疵担保責任から契約不適合責任、権利行使期間の変更について

業務委託契約を作成する際、委託先企業または委託元企業の契約書の雛形を用いる場合が多い。どちらの雛形を用いるかについては、業種、業務内容、委託先企業と委託元企業の関係性などにより様々であるが、一般には自社が有利となるような記載内容となっている。民法改正に伴う、瑕疵担保責任[8]から契約不適合責任への変更、権利行使期間の変更[9]についても、契約書の雛形を用いる側の企業が有利となるような内容に変更されているケースが考えられる。過去に業務委託契約を実施した実績がある、継続して業務委託契約を実施しているという場合でも、新規契約、契約更新等の際は業務委託契約書の内容を確認することが望ましい。

以下に民法改正に伴う業務委託契約書の更新や契約についての取り組み事例を示す。

事例６	保守契約の活用による対応
プロフィール	委託先企業　大規模　製造業
システムを運用していく上で瑕疵以外にも問題が発生する可能性がある。基本的な業務に関わるシステムで発生した問題については、影響を最小限にとどめて早期復旧をさせるために保守対応が必須と考えており、保守契約を結んでいる。 瑕疵担保の期間に発見された瑕疵に相当する問題は瑕疵として対応してもらうが、保守契約を結んでいることで瑕疵担保の期間を過ぎて発見された瑕疵に相当する問題についても保守契約の範囲として対応してもらえるケースもあるため、保守契約によるメリットは大きい。 民法改正で権利行使期間が長くなるという理由で業務委託契約の金額を増額するのは社内稟議が通りにくいという事情もあり、保守契約を結ぶ方が稟議を通しやすいというメリットもある。	

[8] 瑕疵（受託者が完成させるべき仕事の欠陥やミス）があった場合に受託者が委託者に対して負う責任。

[9] 民法改正前の瑕疵担保責任は引き渡したときから 1 年以内であったが、民法改正後は発注者が契約不適合を知ったときから 1 年以内に通知、5 年以内に請求、請負人は引渡又は仕事の終了時から最大 10 年は責任を追及されうることに変更。（改正民法第 566 条）

3. セキュリティ要件の取り決めについて

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と回答した委託元企業は 69.1%であった[10]。また、2018 年度調査では、「インシデントが発生した場合の対応について責任範囲の記載がない」と回答した企業は 62.9%であった。セキュリティ要件が曖昧な場合は、都度話し合い等で対応されることが多いが、脆弱性やインシデントの対応は被害最小化、迅速な対応が必要であり、契約段階で基本的な取り決めをしておくことが望ましい。

また、クラウドサービスは、約款・利用規約等に情報セキュリティに関する免責事項が明記されており、利用開始後にセキュリティ対策上の問題に気付いても委託元と委託先の間で責任範囲の交渉ができないことが多い。そのため、選定段階でセキュリティ要件が満たせることを確認の上、利用することが大切である。

以下に責任範囲の取り決めやクラウドサービスベンダを選定するための要件を明確にしている取り組み事例を示す。

事例 7	脆弱性の対応に関するランクと対応期間の取り決め
プロフィール	委託元企業　大規模　情報通信業
脆弱性が判明した場合にリスクを放置して危険な状態が継続することを防ぐため、脆弱性の対応について業務委託契約時に弊社と委託元企業との間での対応を取り決めている。具体的には発見された脆弱性の脅威の度合いによりランクを設け、影響の大きい脆弱性から順番に A から C の 3 つのランクを設け A ランクは 3 日、B ランクは 5 日、C ランクは一週間といった対応期間のルールを取り決めている。	

事例 8	セキュリティ事故発生時の役割の取り決め
プロフィール	委託元企業　中小規模　学術研究、専門・技術サービス業
セキュリティ事故の発生時に、より迅速に対応するため、業務委託契約時に弊社と委託先企業との間でセキュリティに係る事故が発生した場合の対応を取り決めている。具体的には「何時間以内に誰が、どこに、どういう形で連絡をする」「対応の範囲」「処置を何時間以内にする」といった役割と担当を取り決めており、社内訓練も実施している。	

[10] 「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」報告書について
https://www.ipa.go.jp/security/fy29/reports/scrm/index.html

事例 9	クラウドサービス契約時にアセスメントを実施
プロフィール	委託元企業　大規模　製造業
業務効率向上のため、現場からクラウドサービスを使いたいというリクエストが頻繁にある。安全なクラウドサービスを使うため、クラウドサービスの契約はすべて許可制で、許諾を得てから利用する運用としており、クラウドサービスの契約可否を判断するための「クラウドサービス業者選定用のアセスメントシート」を作成している。 クラウドサービスを利用したい場合アセスメントシートをクラウドサービスベンダに記入してもらい、チェックした結果、問題がなければ契約する。 アセスメントシートで確認している内容の一例を以下示す。 ・データが暗号化されているか ・契約終了後にデータが消去されるか ・データをエクスポートできるか ・データセンターの場所が日本であるか	

4. セキュリティ事故発生に対する準備

2018 年度調査で、過去 3 年間の業務委託において発生したセキュリティ事故について、最も多かったのは「システム・サービスの障害・遅延・停止」であり、回答した委託元企業の 37.2%が経験していた。セキュリティ事故がサイバー攻撃によるものと最初から判断できることは少なく、事象としてはシステム・サービスの不調として報告されることも多い。そのため、セキュリティ事故か、それ以外の原因かの早期切り分けと、適切な復旧体制が求められ、日頃からの情報収集、体制の構築が重要である。

以下にセキュリティ事故発生時の体制に関する取り組み事例を示す。

事例１０	保守契約を結んだ上での対応を推奨
プロフィール	委託先企業　中小規模　ソフトウェア業
保守契約していない場合でも、委託元企業から相談や調査を依頼されて断ることは難しいため、まずはお伺いするということはあるが、基本的にはできるだけ保守契約を結んでもらい、その中で対応していくようにしている。	

事例１１	もしもの時のための事前契約
プロフィール	委託元企業　大規模　製造業
セキュリティ事故かもしれない事象があった場合の第一段階の確認は社内で実施しているが、問題があるかもしれない場合は、すぐにベンダに連絡をして調査してもらっている。 セキュリティ事故に関する調査を依頼したい場合、機密保持契約の対応なども必要になり、状況に応じて契約すると時間がかかりすぐ対応してもらえない場合も多いため、もしもの時にすぐに対応してもらえるように事前にセキュリティベンダと契約している。	

事例１２	セキュリティの組織立ち上げによる情報収集と展開
プロフィール	委託元企業　大規模　製造業
より多くの情報をより早く収集して全社的に対応するため、ベンダからの定期的な情報収集以外にも、CSIRT[11]を立ち上げて情報収集担当を配置することで、最新の脆弱性情報（JVN）を確認して社内に通知している。情報を集める組織の立ち上げにより社内展開が活性化されている。	

[11] CSIRT(Computer Security Incident Response Team)
セキュリティに関連する情報の収集、周知、および社内の情報システムやネットワークでセキュリティ事故（ウイルス感染や不正アクセスなど）やセキュリティ事故の疑いがある現象が発生した際に、被害の拡大防止や再発防止策の策定などの活動を行う組織。

5. セキュリティリスクアセスメント

本調査のアンケート結果では、委託先企業の 78.4%が納品前にセキュリティにかかわる確認テストを実施し、委託元企業の 64.5%が納品時にセキュリティにかかわる受け入れテストを行うと回答した。しかし、攻撃の手口や対策は刻々と変化しており、脅威は高まっている可能性もある。したがって納品前や納品時だけでなく、定期的にアセスメントを行い、新たな脅威の発生や脆弱性の有無、リスクの大きさについて把握することが、対策の検討に有効である。

以下に第三者によるアセスメントの取り組み事例を示す。

事例１３	第三者のアセスメントを実施
プロフィール	委託元企業　大規模　製造業
第三者によるアセスメントを 2 年に 1 回実施。セキュリティベンダまたは大手 SIer に業務委託している。その時に必要があると判断した範囲（システム、業務、拠点等）を決めてアセスメントサービスを発注しており、毎回同じ委託先には発注していない。 外部公開サイトの脆弱性のスキャンも 2 年に 1 回実施しており、こちらは毎回同じ会社に業務委託して差分などを継続的にチェックしている。用途によって業務委託契約するベンダを使い分けている。	

6. まとめ

インタビューの結果、IT システム・サービスの業務委託契約において、民法改正対応およびセキュリティ事故を防止するための対応として企業ごとに様々な工夫をしていることがわかった。

紹介した取り組み事例には大規模企業であるからできる対策、中小規模企業であるからできる対策が含まれており、すべての企業が参考にして同じ対策を実施することは難しいが、部門間の連携、知識の共有、情報の収集、有識者との連携、保守契約の活用等のポイントをご理解いただき、自社の組織体制に合わせた対策を検討する上での参考としていただきたい。

なお、今回の事例には、サイバーセキュリティ経営ガイドライン[12]の指示を実現する具体的な方法として参考となる取り組みが数多く見られたので以下に該当する指示を示す。

業務委託契約に関する組織の連携、知識、情報の共有について

事例		サイバーセキュリティ経営ガイドラインの指示
事例１	民法改正をきっかけとした勉強会の実施	指示 1「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」 法律や業界のガイドライン等の要求事項を把握している。 指示 3「サイバーセキュリティ対策のための資源（予算、人材等）確保」 サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。
事例３	定期的な勉強会の実施と民法改正をきかっけとした点検	
事例２	現場からの意見を取り入れた点検	指示 10「情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供」 社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。
事例４	部門間の情報共有のための定期的な会議の開催	
事例５	有識者の活用による体制構築	指示 2「サイバーセキュリティリスク管理体制の構築」 サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。その際、組織内のその他のリスク管理体制とも整合を取らせる。

[12] サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

セキュリティ要件の取り決めについて

事例		サイバーセキュリティ経営ガイドラインの指示
事例７	脆弱性の対応に関するランクと対応期間の取り決め	指示 9「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」 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、システム管理の委託について、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。
事例８	セキュリティ事故発生時の役割の取り決め	
事例９	クラウドサービス契約時にアセスメントを実施	

セキュリティ事故発生に対する準備

事例		サイバーセキュリティ経営ガイドラインの指示
事例１０	保守契約を結んだ上での対応を推奨	指示 7「インシデント発生時の緊急対応体制の整備」 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制(CSIRT 等)を整備させること。
事例１１	もしもの時のための事前契約	
事例１２	セキュリティの組織立ち上げによる情報収集と展開	

セキュリティリスクアセスメント

事例		サイバーセキュリティ経営ガイドラインの指示
事例１３	第三者のアセスメントを実施	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」 経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させること。