Vol.2020-DPS-184 No.6
Vol.2020-EIP-89 No.6
2020/9/10

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

渡邊　浩平[†1]　　後藤　厚宏[†1]

概要
政府・行政機関が発表している、ガイドライン及び調査の動向が示す通り IT サプライチェーン管理の重要性は今後更に高まっていくと予想される。実際に業務連鎖することが原因で発生しているインシデントも多く、様々な業界が時代の変化の中でビジネスモデルの転換や技術開発に前のめりになっているが、リスクマネジメントの変化は疎かになっていないだろうか。本研究では、委託元・委託先・再委託先と連鎖的に続く委託形態に注目し、業務委託時の情報管理としての情報セキュリティを阻害する要因の検討を行い、その要因から業務委託リスク認識を高める為の研究仮説を設定。先行研究等を分析しリスク認識に作用する要因を洗い出し仮説の裏付けを進め、企業における当該リスクの防止・低減のする為に必要な業務委託リスクの現状を考察していく。

キーワード：IT サプライチェーン，サプライチェーンマネージメント
リスクマネジメント，アウトソーシング，情報セキュリティ

A study on outsourcing risk in IT supply chain

KOHEI WATANABE[†1]　　ATSUHIRO GOTO[†1]

Abstract
It is expected that the importance of IT supply chain management will further increase in the future, as indicated by the guidelines and survey trends announced by governments and government agencies. Many incidents are actually caused by business chains, and various industries are leaning towards business model conversion and technology development due to the changes of the times, but changes in risk management are neglected. Isn't it? In this research, we focus on the consignment form that continues in chain with the consignor, consignee, and subcontractor, and examine the factors that hinder information security as information management during business consignment, and recognize the business consignment risk from that factor. Set research hypothesis to increase. We will analyze the previous studies to identify the factors that affect risk recognition, support the hypothesis, and consider the current status of outsourcing risks necessary for companies to prevent or reduce such risks.

Keyword　:IT supply chain, Supply chain management
Risk management, outsourcing, Information security

1. はじめに

IT サプライチェーンに関するセキュリティ対策は、世の中の動向からも見える様に外すことの出来ない重要事項となっている。しかし、技術対策に特化するあまりリスク管理面、からのアプローチは疎かになっていないだろうか。

「情報セキュリティ 10 大脅威」の「サプライチェーンの弱点を悪用した攻撃の高まり」[1]や、「サイバーセキュリティ経営ガイドライン v2.0」の「ビジネスパートナーや委託先企業も含めたサプライチェーン全体でのセキュリティ対策の必要性」[2]、NIST CSF(サイバーセキュリティフレームワーク)でもサプライチェーンリスクマネジメントの項目が大幅に強化された[3]。この様に政府・行政機関が発表するガイドラインや調査の動向が示す通り、IT サプライチェーン管理の重要性は今後更に高まっていくと予想される。

その中でも、企業における IT システム・サービスに関する業務を系列企業やビジネスパートナーに外部委託し、委託が連鎖する形態はメリット(コスト削減/効率化/本業への集中/組織のスリム化)の多さから一般的となっている。市場平均成長率も年 2.1%で推移し 4 兆円を突破、今後も人材不足やクラウド利用促進により 2022 年度以降の成長率は飛躍的に高まり 5 兆円規模に成長すると予測され

[†1] 情報セキュリティ大学院大学

Vol.2020-DPS-184 No.6
Vol.2020-EIP-89 No.6
2020/9/10

ている[4]。

ビジネスパートナーとの関係は古くて新しい課題でもあり、技術の進化や企業を取り巻く経営環境の変化とともに変容してきたが依然として課題や摩擦を払拭できていない状況が見える。IT 戦略上重要であると多くの企業が認識しているが満足度は低い[5]。さらに、外部委託先を管理する上で感じている課題として、「リスクの可視化が困難」「委託先情報の更新・連絡が大変」等と実に 7 割以上の企業が何らかの課題を感じていることが明らかになっている[6]。

本研究では IT サプライチェーンの中でも特に、連鎖的に続く委託形態に注目しインシデントや情報セキュリティ上のリスク、企業における当該リスクの防止・低減をする為に必要な業務委託リスク管理の現状を考察していく。

2. IT サプライチェーンリスク

2.1 IT サプライチェーンの概要

IT サプライチェーンとは、IT システムが納入されるまでの設計・開発・製造等の工程や運用・保守・廃棄に至る「一連のプロセス」のことで、外部組織への委託もサプライチェーンの一環に含まれる。ここでいう IT システムとは情報系サービス提供企業のゲートウェイシステム全般のことで、メール・コミュニケーション・ファイル共有等サービス提供するシステムを指す。個々の企業の役割分担にかかわらず、原料の段階から製品やサービスが消費者の手に届くまでの全プロセスの繋がりとも言える。その視点から、IT を活用して効果的な事業構築・運営する経営手法が SCM（サプライチェーンマネージメント）と呼ばれ、大別して「製品セキュリティ」と「情報管理としての情報セキュリティ」が含まれる。

2.2 考慮すべきリスク

IT サプライチェーンリスクには「外部」と「内部」があり、「外部」は関連組織を狙った IT サプライチェーン攻撃で、大企業は対策が進み攻撃しにくい・対策が薄手な委託先を狙う・委託先を経由して大企業へ侵入するといった特徴がある。一方「内部」は、ハード（部品/製品）・ソフトウェア・委託事業者（再/再々委託事業者）・委託元である[7]。内部リスクに関しての事例は後続(*2.3*)で一部紹介。

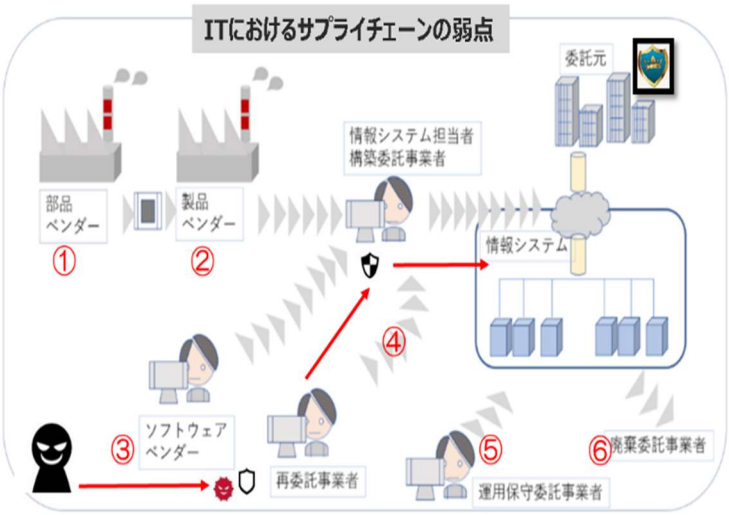

図 1　IT サプライチェーンリスクの図式
組織のセキュリティ対策 McAfee 2018［7]を元に筆者作成

それぞれのリスクポイントを以下に示す。

① 部品ベンダー
委託事業者は、グローバル拠点での生産が多く各部品の品質にはばらつきが生じ、ガバナンスとリテラシーの低さから、異物混入のリスクが高くなる。

② 製品ベンダー
再委託により納期遅延や委託事業者の管理も煩雑になりがちである為異物混入が生じる。

③ ソフトウェアベンダー
不正コード埋め込みのリスクが高まる。

④ 委託先事業者(後続 *2.3 事例一・二*に該当)
セキュリティ対策・連携不足、機密情報搾取、不正機能の組み込みなどのリスクが高まる。(三次委託以降はよりリスクが高まる)

⑤ 運用保守委託事業者(後続 *2.3 事例一*に該当)
事業者のガバナンスの低さによる、不正な操作や連携・確認不足が多くなる。

⑥ 廃棄委託事業者(後続 *2.3 事例二*に該当)
事業者の不正行為による機密情報搾取が発生。

この様に、IT サプライチェーンは産業構造の中心とも言えるがそこに潜むリスクも多岐に渡っていることが分かる。本稿では、主に④～⑥を研究対象としている。

2.3 発生するインシデント事例

今日、前項のリスクが顕在化し様々なインシデントが発生している。ここでは、本稿の研究対象である業務委託に関連する報道記事にもなった事例を 2 つ紹介する。

＜事例一＞

2018 年市教育委員会 NW システムの公開用サーバ

Vol.2020-DPS-184 No.6
Vol.2020-EIP-89 No.6
2020/9/10

への不正アクセスが確認され、最大５万件の学生データが流出し、委託元先間の訴訟問題へと発展している[8]。本件の直接原因は、公開用サーバの脆弱性放置、FW の設定不備であったが、真因として以下のことが明らかになっている。

委託元[市教育委員会]
・組織としての契約・システム理解不足
・システム管理者は兼業且つ数年で交代
・セキュリティの重要性の認識不足
・情報セキュリティ監査対象外
委託先[大手キャリア]
・市からの通信要件の不明確部分が放置
・再委託先の管理・コミュニケーションが不十分
・重要情報を取り扱う当然の注意が不足していた
[提案書に高セキュリティと記載があった]

これは、前項「2.2 の④や⑤」に該当するリスクが顕在化したと言える。直接原因が発生した理由で最も大きいものは、委託元と委託先の運用面での認識違い(両者ともに相手がやると思い込んでいた)が脆弱性を放置することになってしまった。この事例では委託元が委託先に丸投げし過ぎていたと考えられ、委託先の親切心で対応されていたこともあり、委託元の意識改革(情報セキュリティの重要性と基準の認知)と委託先間との責任範囲を示すものが必要であると考えられる。

＜事例二＞

2019 年県庁のファイルサーバの HDD がオークションで転売されているのが確認され、18 台の HDD 流出[約 50TB]し、委託先は指名停止、再委託社員は逮捕された。直接原因は、再委託社員による HDD 転売であった[9]。真因として以下が明らかになっている。

委託元[県庁]
・行政文書を平文で格納していた
・データ消去完了証明書の受領の欠如
・再委託されていることを未把握
委託先
・データ消去を再委託先に丸投げしていた
・データ消去完了証明書の発行依頼なし
再委託
・消去作業のモニタリングが行われていない
・掲示板等で情報流出が囁かれていたが未把握

これは、前項「2.2 の④や⑥」に該当するリスクが顕在化したと言える。この事例は信用を前提にしていたとも取れ、各組織共に不備があり実質管理しているように見せていただけであると考えられる。この様な組織は日本にまだまだ存在しているのではないだろうか。

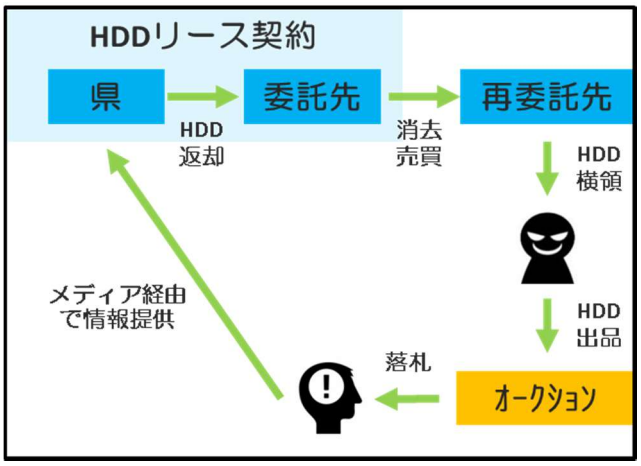

図 2　HDD 流出発覚経緯イメージ

これらの事例は IT サプライチェーン上のリスクが顕在化した例の一部に過ぎず、現在に至っても様々な組織・団体が対策を講じて来たが同様のトラブルは依然として後を絶たない。

3. 研究仮説

2 章までで紹介した、IT サプライチェーンリスクモデルやそこで発生するインシデント事例に関する認識及び先行研究・参考文献、自身の業務経験則に基づき、業務委託時の情報管理としての情報セキュリティを阻害する要因の検討を行い、その要因から業務委託リスク認識を高める為の研究仮説を設定。下図は、仮説の関係性を示したものである。

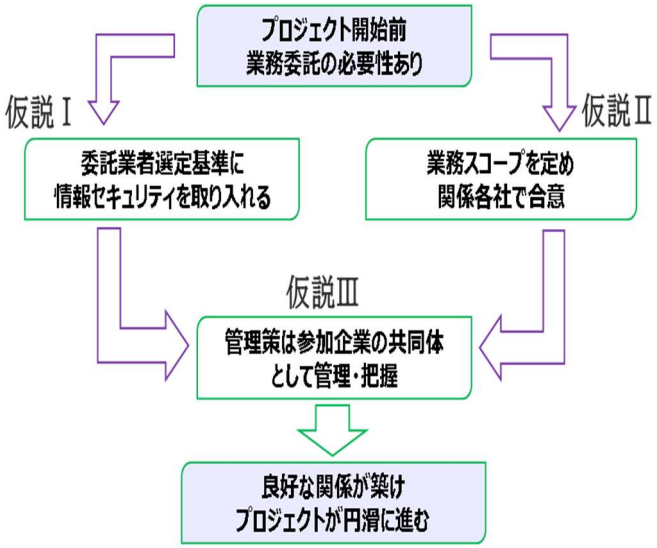

図 3　業務委託リスクを高める仮説

本研究では、IT システムの業務委託時に必要な情報セキュリティ基準や適切な業務範囲を定め管理することで、不要な争いや不公平感を避け良好な関係がプロジェクトの成功に繋がるとの考えの下、

委託元-委託先間、更に連鎖する再委託先以降も対象としている。

【仮説Ⅰ】:委託業者選定を判断する管理者が,金額・技術・慣例だけでなくセキュリティ基準も用いて選定を行えば,組織として業務委託リスク認識を高められる.

連鎖する委託形態の中で、業者選定基準として1番の要素としてセキュリティ基準を挙げる企業は少ないと思われる。しかし、時代の要請の中でセキュリティに対する重要度は益々高まっている為に選定要素の 1 つとして確実に抑えておかなければ、前項「2.3 のインシデント事例一」の様にアカウンタビリティを果たせなくなってしまう。この基準が業務委託リスクとして論じられた例は少ない。

【仮説Ⅱ】: 業務委託契約を行う管理者が,両者が納得する業務スコープを定められれば各社の対応が明確になり迅速な対応が期待される.

契約書の多くは明確に業務責任範囲を示しているとは言い難い状況になっている。それは、責任を曖昧にしておきたい委託元の意識が反映されていることや都度協議とし優位な立場を保ちたいという心理が働くことが考えられ、これは前項「2.3 のインシデント事例一・二」にも当てはまる。
また、インシデント発生時の動きが遅くなることが更に事態を悪化させる要因の 1 つと考えられる。

【仮説Ⅲ】: 業務委託時のリスク管理は,各社任せではなく参加企業全体として管理する等の新たな枠組み・法律での縛りがプロジェクトを円滑に進めることに作用する.

リスクマネジメントを行う際の管理策は様々作成・紹介されているが、コストも掛かる為、導入判断は個社毎に任されている。これは、前項「2.3 のインシデント事例二」の各社共に ISMS 取得や対応策を個社で実施しているが複数社に跨った業務プロセスではあまり意味をなさないことが分かる。実際のプロジェクトでは多くの企業が関わってくる為プロジェクトチーム全体での管理の必要性がある。またそれらを強制する法令(金融庁が示している指針)等と業務委託リスクとの関連を論じた例は少ない。

4. 先行研究と裏付けされた要因

IT サプライチェーンの業務委託リスク認識に関する先行研究を紹介・分析し前項「3 研究仮説」のどの部分が裏付けられ、どの部分が未検証かを洗い出す。

4.1 サプライチェーンにおける情報セキュリティの研究[10]

久保は、情報セキュリティ管理の脆弱な企業が原因となって、チェーンの一部の問題が全体の機能停止に繋がるリスクが増大し、また情報セキュリティだけでなく化学物質や人権などの視点でサプライチェーンリスク管理に関する取り組みの調査結果を踏まえ、ガバナンスや特性に合わせた対応策の提言を行っている。クラウドや国際標準を活用することでリスク変化を考慮した対応を行うことが出来るとした。明らかになった事として、多層化・グローバル化によってもはや一企業だけの努力でサプライチェーン全体の可視化は不可能であり、国や地域・文化の多様化によってサプライヤとの関係構築も難しい事、セキュリティリスク認識が機密性に偏っている・国内制度のみに目を向けている為に、セキュリティリスク認識の啓発や対処方法普及施策が不十分と結論付けた。

仮説に対して、国内でも昨今様々な情報セキュリティに関する管理策が登場しているが、各企業が個別で導入判断を行っており、サポートに関しても各企業主体でありとてもサプライチェーン全体といったプロジェクトチームに対した適用が出来ていない。これは【仮説Ⅲ】に関わる前項「2.3 のインシデント事例二」の全体管理の仕組みの不足部分に関して、各種管理策が存在はしているが適用しにくい、法的拘束がなく各企業に任されていると言える。それが競争力と言えばそれまでだが、サプライチェーン上の被害は益々甚大になっているので情報産業にも金融/保険業界の様な遵守しなければならないガイドラインを政府主導で定める時期に来ていると考える。

4.2 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為の提案[11]

森らは、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、IPA のアンケート結果[12]の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した。それは、金融業・保険業、契約書に責任範囲を明示している傾向(金融庁指導が効果的)があること、IT システム・サービスは、特に SaaS は責任範囲を明示していない(約款での取り決めか)ことが分かった。また、「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あり、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、従業員数等によって，責任範囲の明示に傾向があることが分かった。結果として、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と提言しているが具体案の提示は無い。

仮説に対してインシデントが発生しないと責任範囲の明示がされにくい傾向且つオンプレ IT システム・サービスや金融/保険業以外の業種を生業としている企業では管理策が足りていないと言える。また、中小規模ほど、言い換えると委託先が連鎖的に増えるほど責任範囲が不明確になると捉えることも出来る。従って【仮説Ⅱ】に関わる前項「2.3 のインシデント事例一・二」の要件・範囲の不明確さが委託リスクを阻害する要因の一部であると考えられる。また、先行研究で参照している調査文献のアンケート結果からも契約で責任範囲を見直す機会がないこと、セキュリティ対策のコストを受け入れてもらえないこと、心理的不安が増えるということより「対等なパートナー関係」が構築出来ていない要因にも繋がる。

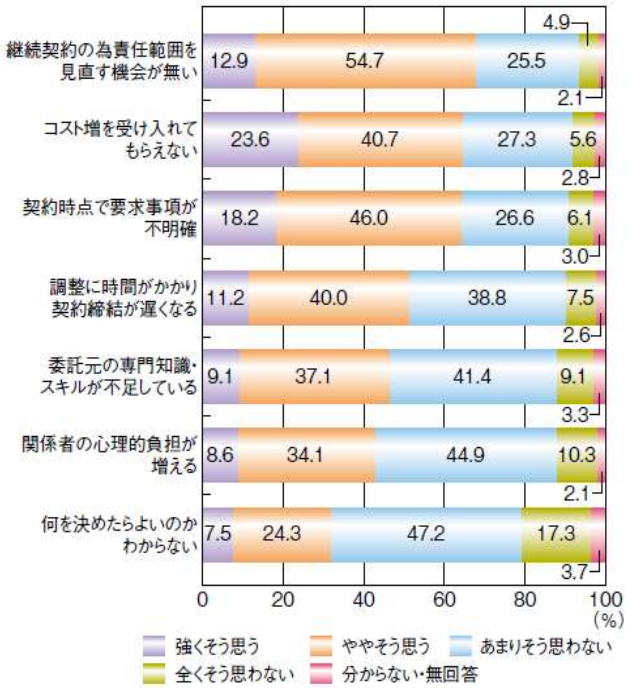

図 4　委託先の責任範囲に対する不安[12]

4.3　サプライチェーンと情報セキュリティの研究[13]

金子は、サプライチェーンと情報セキュリティの問題を俯瞰して整理し，実務上の課題について検討している。委託先における情報管理としての情報セキュリティは，委託先に情報セキュリティを要請する必要性と制度上の取組を紹介し情報セキュリティ事故発生時の委託先への責任に対する考え方と解決方法の提案を行ったもの。明らかになった事は、業務上、ある会社にしか頼めない場合などもあるので委託元が情報セキュリティ費用を含めた面倒をみる必要はあるが、コスト削減のために委託しているので出し渋りが起きている。また、保険に頼ることで、責任を共有するのが合理的だが各企業は情報セキュリティ対策の努力を怠ることはないようにする仕組みも必要とし、保険により大きな損害賠償の懸念を払しょくし、安心して情報セキュリティに真摯に取り組んでいることを競争力の一つと出来るようにすることが、世の中の情報セキュリティレベルを上げることに繋がると提言している。

仮説に対して、古くからの企業体質が根強く残っていることもあり、責任を明確化するのは難しい(前項「2.3 のインシデント事例二」にも該当)と論じているが【仮説Ⅱ】を設定するに至った自身が考える阻害要因と同様の課題認識ではある。また【仮説Ⅲ】の「コスト意識」に関する投資が消極的であることが分かる。保険による責任共有提案は興味深いが実例の少なさから実現可能性とスピード感・納得感を考慮した場合に疑問も残る部分はある為、「別の管理策」で効果は小さいかもしれないが先ず取り組む・意識することから段階的に解決するきっかけを与えたいと考える。

4.4　裏付けされた要因と検証項目案

先行研究の調査結果から 3 章で述べた研究仮説のうち、仮説Ⅱの「業務委託契約を行う管理者が，両者が納得する業務スコープを定められれば各社の対応が明確になり迅速な対応が期待される」は裏付けされていると考えられる。これは、業務委託が必要なプロジェクトが立ち上がった場合に、契約段階より明確な責任範囲を示すことで後々不要な争いを避けることにも繋がり、委託先も安心して自身の業務範囲に集中し良好な委託関係がプロジェクトの成功に繋がっていく。

従って、「委託契約時の業務スコープ設定と業務委託リスク認識の関係」は既に検証済であること、一方、仮説Ⅰの「委託業者選定時セキュリティ基準と業務委託リスク認識の関係」・仮説Ⅲ「全体共同管理・法律が業務委託時のリスク管理に与える影響」に関しては未検証部分が多いことが分かった。これらの未検証部分を今後検証していくことで、どのリスク認識の要因が良好な委託関係を構築することに繋がり、プロジェクトの成功に関連しているかが見えてくると考えられる。

図 5 は現状で設定している仮説の検証を行う為の

項目を示したものである。先行研究・調査文献より一部ではあるが業務委託リスク認識に影響する要因と捉えることが出来たもの(グレーアウト箇所)も見えて来た。

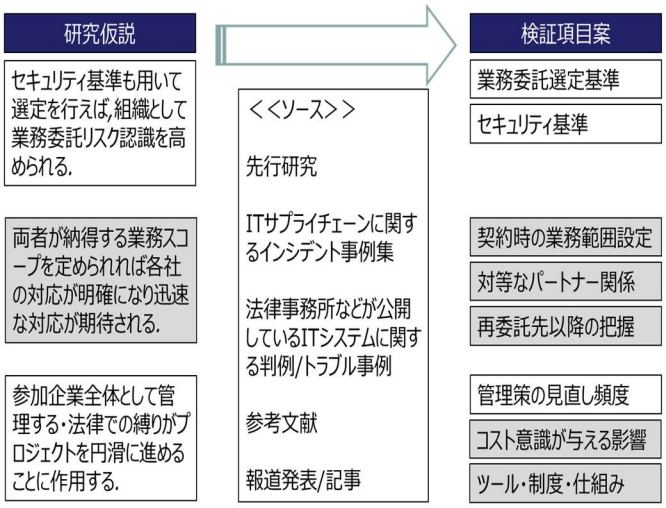

図５　仮説に対する検証項目案

5. まとめと今後の研究

１章及び２章で言及した通り、IT システムの業務委託は今後も活発に行われると予想されている。先行研究では、もはや一企業だけの努力でサプライチェーン全体の可視化は不可能であること、新たな仕組みの必要性も指摘されている。

本稿では、IT システムの業務委託時に必要な情報セキュリティ基準や適切な業務範囲を定め管理することで、不要な争いや不公平感を避け良好な関係がプロジェクトの成功に繋がるとの考えの下という仮説を示した。

今後は、さらに仮説検証(項目検討精査含む)を進め、IT システムプロジェクトにおけるより前進した委託関係を構築する助けについて提言したい。

参　考　文　献

[1] 情報処理推進機構:情報セキュリティ10大脅威(online), 入手先 <https://www.ipa.go.jp/security/vuln/10threats2020.html> (参照2020.7.9).

[2] 経済産業省:サイバーセキュリティ経営ガイドラインver2.0(online),入手先<https://www.meti.go.jp/policy/netsecurity/mng_guide.html> (参照2020.7.9).

[3] NIST:サイバーセキュリティフレームワーク(online), 入手先<https://www.nist.gov/cyberframework> (参照2020.7.9).

[4] 矢野経済研究所:ITｱｳﾄｿｰｼﾝｸﾞｻｰﾋﾞｽ市場規模推移と予測(online), 入手先<https://www.yano.co.jp/press-release/show/press_id/2005> (参照2020.7.9).

[5] ガートナー :デジタル時代にふさわしいパートナー戦略に関する指針(online), 入手先<https://www.gartner.com/jp/newsroom/press-releases/pr-20190820> (参照2020.7.9).

[6] GRCS:企業の外部委託先管理に関する実態調査(online),入手先<https://www.grcs.co.jp/news/20180927> (参照2020.7.9).

[7] McAfee:組織のセキュリティ対策　2018(online), 入手先<https://blogs.mcafee.jp/scrm-risk-prevention> (参照2020.7.9).

[8] 前橋市教育委員会:(online),入手先<https://www.city.maebashi.gunma.jp/kosodate_kyoiku/3/6/13577.html>(参照2020.7.9).

[9] 神奈川県庁:(online), 入手先<https://www.pref.kanagawa.jp/docs/fz7/cnt/p0273317.html> (参照2020.7.9).

[10] 久保知裕：サプライチェーンにおける情報セキュリティの研究, 情報処理学会研究報告, EIP, [電子化知的財産・社会基盤] 2014-EIP-65(3), (2014).

[11] 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為の提案, コンピュータセキュリティシンポジウム2019論文集 (2019).

[12] 情報処理推進機構:情報セキュリティ白書2019(online),入手先<https://www.ipa.go.jp/security/publications/hakusyo/2019.html> (参照2020.7.10).

[13] 金子啓子：サプライチェーンと情報セキュリティの研究, 情報処理学会研究報告電子化知的 財産・社会基盤 (EIP) (2017).

[14] 長内仁：企業間における情報セキュリティ連携アーキテクチャの検討, 電子情報通信学会技術研究報告, 信学技報,(2013).

[15] 久保木孝明：アウトソーシングと情報セキュリティ問題-プリン業務のマネージドサービスを題材として-, 情報処理学会論文誌,Vol.50,No2,pp.140-149,(2009).

[16] 河野翔太：プロセスアプローチを用いたIT外部委託先管理の研究, 情報処理学会研究報告電子化知的 財産・社会基盤 (EIP) (2014).

[17] 関口和代：アウトソーシング・ビジネスの現状と課題-BPOを中心に-, 東京経大学会誌,経営学(270),143-157,(2011).

[18] 小山明美、森 淳子、小川 隆一、竹村敏彦：企業の民法改正対応への取り組みに関する一考察, 情報処理学会第82全国大会,情報システム・電子化知的財産, 2G-01, (2020).