発表論文

サプライチェーンの日本企業における情報セキュリティガバナンスの研究

Survey of Information Security Governance in the Supply Chain of Japanese Companies

久保 知裕、原田 要之助
Tomohiro Kubo, Yonosuke Harada
情報セキュリティ大学院大学

要 約

近年、顧客への価値提供は、一組織単独で行われることはない。原材料・部材の調達や生産、物流や事務、IT サービス等の様々な機能を提供する複数の企業によって構成されたサプライチェーンを通して行われるようになっている。サプライチェーンは地理的な広がっていること、取引形態が複雑化していること、調達者と供給者の関係に影響を受けることから、リスクの所在が分かりにくい。そのため、リスク管理は難しさを増している。情報セキュリティの観点からは、取引における情報共有や開示の度合いによってリスクが変わる。本稿では、サプライチェーンのガバナンスモデルや調達・委託業務の種類による違いを踏まえてリスクを整理し、国際標準を利用したセキュリティリスク管理の手法について考察する。

キーワード: サプライチェーン、バリューチェーン、情報セキュリティ、リスク管理、ガバナンス、ISO/IEC27036

1. はじめに

1.1 背景

サプライチェーンは、商品やサービスを最終消費者に提供するまでの一連の業務プロセスや業務活動を指している。通常、複数組織にまたがって行われる。

昨今のサプライチェーンは地理的にも機能的にも複雑化している。まず、海外市場への展開や海外拠点での生産が拡大することで地理的に広がっている（グローバル化）。また、企業は競争力を高めるために自社の得意なコンピテンスに特化するため、機能が細分化・分散化する傾向がある。これらに伴い、サプライチェーンのリスクが変化してきている。タイの大洪水の際に、電機業界や自動車業界におけるグローバルサプライチェーンが機能停止したこと、東日本大震災で特殊な半導体の生産が止まったことで、様々な製品の製造が停止したことなどからも推察できる。ファーストサーバーの障害により EC サイトが停止した事件や、中国に委託した IT サービスからカード情報が漏えいしたアリコ生命の事件など、IT サービスでも同様に推察できる。

また、情報セキュリティリスクをサプライチェーン全体にわたって管理する必要性が高まっている。サプライチェーンは複数の組織間で、設計情報や受発注、在庫等の様々な情報の流通・交換・蓄積・加工を行う仕組みともいえる。そのため、情報の流通が一部の企業で阻害されたり、漏えいしたりするとサプライチェーン全体が機能不全もしくは停止するリスクがある。

1.2 研究の目的と進め方

これまで、情報セキュリティ管理は組織内に向けて、施策が導入され、運用されてきた。サプライチェーンにおいては複数の企業にまたがって、セキュリティレベルを維持管理しなければならない。一方で、サプライチェーンの成果は、取引に関連するコスト全体を最小化することで得られる。取引コストに影響する要素として、取引の形態や企業の力関係等を考慮しなければならない。

サプライチェーンにおける情報セキュリティ管理の手法は、個々の企業における情報セキュリティ管理の手法をサプライチェーンに

拡張しているので、取引の形態や取引コスト、グローバル化における実用性等の点から検討の余地がある。本稿では、サプライチェーンのガバナンスモデルを踏まえ、国際標準を活用したフレームワークを考察する。

2. サプライチェーン情報セキュリティリスク

2.1 サプライチェーン全体のリスク

サプライチェーンに関わるリスクは、過剰在庫や欠品などの財務指標に影響を与えるものや、事故や災害等、事業継続に影響を与えるもの等、多岐にわたる。また、チェーンを構成する場合の供給者[1]や調達者[2]の財務リスクや、取引における地理的、政治的なリスク等もある。

サプライチェーンにおける情報の信頼性に着目した Christopher らは、Mitigating Supply Chain Risk through Improved Confidence[i]で、下記のように述べている。

信頼性が失われることでサプライチェーンに影響を与える事項には、受発注サイクルに費やす時間、受発注の進捗状況、需要計画、供給者の供給能力、生産能力、製品の品質、輸送の信頼性、提供されるサービスがある。

受発注サイクルが長いほど、サプライチェーンの在庫や流通等の状況に関する最新の精度の高い情報がつかめなくなり、情報の信頼性が下がる。結果として、時間的なバッファー（リードタイム）を長くとるようになり、これがさらに受発注のサイクルを伸ばしてしまう。これをリスクスパイラルと呼んだ。

受発注サイクルが短く多量の取引がやり取りされる場合や、需要変動が激しい場合は、正確で迅速な情報交換が重要である。サプライチェーンに問題が発生し取引ができなくなった場合の情報セキュリティリスクは高い。

2.2 委託業務と情報セキュリティリスク

情報セキュリティ大学院大学原田研究室では ISMS もしくは P マークの取得企業および、大学と官公庁を対象とした、情報セキュリティ対策のアンケート調査を行っている。2013 年には、この調査の一部としてサプライチェーンの情報セキュリティに関する質問を行い、委託、調達する内容によって情報セキュリティリスクの認識が異なるのかどうか、調査した[ii]。

図 1 から、企業は全般的に機密性を重視する傾向が強い。しかし、原材料・部品・商品の調達や、生産や物流業務の委託では可用性を、給与計算や経理業務の委託では完全性を、機密性と同等、もしくはそれに次いで重視している。すなわち、業務によって重要と認識するリスクが異なることを示している。

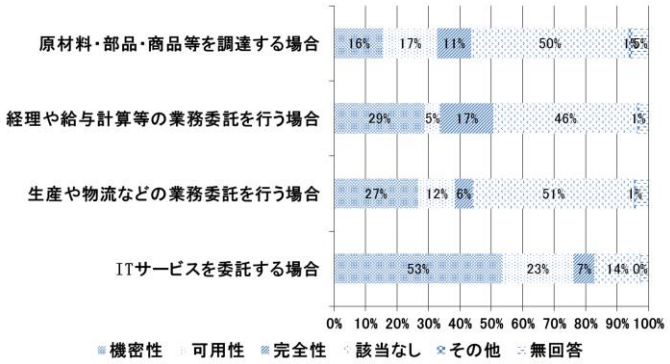

図 1. 業務委託を含む調達における情報セキュリティリスク(N=367)

2.3 ガバナンスモデルと情報セキュリティリスク

サプライチェーンのガバナンスモデルに着目した Gereffi らは、The governance of global value chain[iii]の中で、モデルの違いによって、企業間の力関係が変わること、取引内容の外部開示のレベルが異なることについて述べている。これを図 2 に示す。図 2 のガバナンスモデルには以下の 5 類型がある。

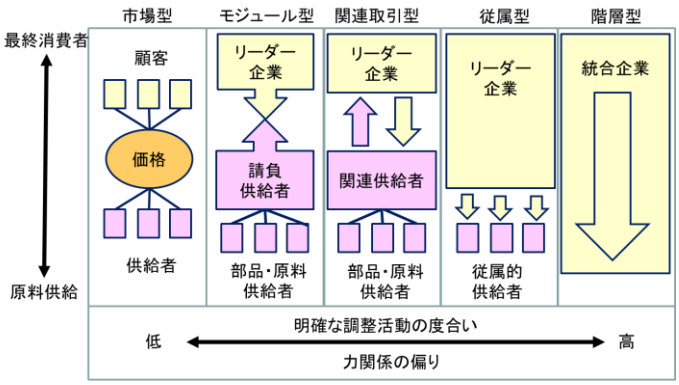

図 2. 5 つのグローバルバリューチェーンガバナンス（Gereffi ら）

- 市場型：スポット市場で、供給側、調達者の切り替えコストは低い。
- モジュール型：多少とも供給者は調達者のニーズに合わせてカスタマイズする。請負納入の場合は、供給者が設備や原料手配などの便宜をはかる。
- 関連取引型：供給者と調達側は特別な設備への投資など依存関係を持つ。地縁や評判、親族などの関係で結びついた取引である。

---

1 供給者：原材料・部品・商品等のモノやサービスの提供者を指す。業務委託先を含む。(Supplier)

2 調達者：原材料・部品・商品等のモノやサービスの購入者を指す。業務委託元を含む。(Acquirer)

- 従属型：大規模な調達者に小規模な供給者が従属した関係である。調達者による、統制やモニタリングが頻繁に行われる。
- 階層型：垂直統合の進んだ形態で、本社と子会社の関係が代表的である。

図２の調整活動は、企業間の情報提供と統制を示している。取引内容の外部開示ができない場合、企業間での調整活動がより重要となる。スポットで調達する市場型では調整活動の重要性は低く、従属型や階層型では重要となる。

力関係を考えると階層型や従属型では、リーダー企業が調整活動を実施することとなる。一方でモジュール型の場合は、リーダー企業と請負供給者[3]の間で対等の関係が成り立つため、市場型のような調整活動は少ない。

Gereffi らの研究から、ガバナンスモデルによって情報の外部へ開示程度や統制活動に違いがあることが分かる。また、業界の特性でモデルが決まること、事業環境の変化によってもモデルが変化することが考えられる。

3. リスク管理手法

3.1 サプライチェーン全体のリスク管理

Christopher らの研究では、リスクスパイラルに陥らないために、サプライチェーン全体の情報の可視化と統制が必要であると述べている。特に、以下の三つの要素を挙げている。

- 情報の正確性、可視化とアクセス
- 統制が効かない状況の警告
- 修正するための対応

これらの仕組みを構築して運用することで、サプライチェーン全体の効率性や統制を維持することができる。この考え方は、情報セキュリティを考える上でも有効である。

3.2 サプライチェーン情報セキュリティ管理基準

日本セキュリティ監査協会が 2011 年に経済産業省の受託事業としてサプライチェーン情報セキュリティ管理[iv]の検討を行った。検討対象となった課題を次に挙げる。

- 社会の標準となる情報セキュリティ管理基準が必要
- 簡易なシステムで参加しやすく、円滑にサプライチェーンの情報セキュリティに関する情報の交換ができること
- 自律的にサプライチェーン全体のセキュリティが向上すること
- 中立的な機関が管理し、適正な情報が開示・参照できること
- 海外においても浸透が可能な仕組みであること

提言においては、社会の標準となる情報セキュリティ管理基準や、自己適合宣誓書を用いた簡易で参加しやすい仕組づくり、自律的なサプライチェーン全体のセキュリティ向上の方法が述べられている。また、委託元と委託先がアクセスできる監査データベース構築への国の支援や中立的な機関による運用、海外展開へ向けた指針が述べられている。

リスク管理すべき情報資産を整理した点や、具体的に記載された管理項目は参考になる。一方で、リーダー企業が日系企業である前提に立って記述されているため、海外企業が主導する場合に利用されるかどうか疑問である。管理の手法は標準化を志向したためか、画一的で、Gerrefi らが指摘したガバナンスモデルの違い等について考慮されていない。供給者の選択や契約といった構築プロセスにおける留意事項については触れられていない。これらの点についてはさらに検討の余地がある。

3.3 情報セキュリティガバナンス導入ガイダンス

三菱総研は 2011 年に「情報セキュリティガバナンス導入ガイダンス補足編～企業グループにおける情報セキュリティガバナンスモデル～[v]」を提言した。この提言では、資本関係のあるグループ会社や、サプライチェーンのような契約関係に基づく取引先に対する情報セキュリティガバナンスのあり方について以下のように述べている。

「調達と供給の契約関係に基づき構成されるサプライチェーンの場合、グループの成り立ちが 一つ一つの契約に依存しているため、強制力を伴う横断的・統一的な統制を実現することは難しい。環境分野では、問題が発生した場合、サプライチェーンに関係する企業全体が連帯責任を担うという考え方がある。そこで、たとえば、当該チェーンのリーダー企業が主導する形で、受委託契約とは別に、情報セキュリティの遵守事項を含むチェーン共通の合意形成を図る取組が考えられる。」

ここで、化学物質管理や紛争鉱物利用規制のようなチェーン全体の責任を明確化すべきだとの指摘は重要である。

一方で、次の点に関しては検討の余地がある。サプライチェーンの場合、可視化することによりチェーン全体のリスク管理を行うことができるが、海外に展開した機能や分散化した機能については可視化が難しい。また、Gerrefi らが述べたように、ガバナンスモデルによっては、リーダー企業が存在しない、もしくは影響力を持たないこともある。すなわち、画一的な取り組みではリスク管理が不足するか、取引コストが過剰にかかる可能性が

---

[3] 半製品を提供する、様々な相手先に合わせて柔軟に生産できる能力を持つ供給者（Turnkey Supplier）

ある。これらの点について、さらに検討を行う余地がある。

3.4 ISO/IEC27036

ISO/IEC27036[vi]は 2013 年に公開された。4 部構成になっており、Part1 は概要、Part2 は一般的なサプライチェーンにおけるフレームワーク、Part3 は ICT サプライチェーン、Part4 はクラウドとなっている。

サプライチェーンにおける問題点として、①供給者と調達者のセキュリティコントロールのギャップ、②調達者がセキュリティコントロールを外部に頼らざるを得ないこと、③調達者のコントロールを弱めてしまうコンフリクトを挙げている。それらの要因として、ガバナンスの弱さ、誤った情報伝達、地域・社会・文化といった環境などを挙げている。

サプライチェーンのライフサイクルについて指摘している点は、先に挙げた 2 つの手法と異なる。サプライチェーンの構築時に、計画策定、供給者選定、契約、運用管理、契約を終了までの一連のプロセスを想定して、要求事項を織り込むべきだとしている。この考え方は汎用的に利用することができる。

4. 考察

サプライチェーンにおける情報セキュリティリスクは、業界の構造に依存したガバナンスモデルや委託・調達する業務によって異なる。これまでに提案された管理手法は、標準化を意識し画一化される傾向にある。また、日系のリーダー企業が存在するサプライチェーンを前提としているので、グローバル化や機能の分散化に伴う複雑な環境への応用が難しい。一方で、個社ごとにコントロールを構築・運用する仕組みでは取引コストが増大してしまい、サプライチェーンの効率化を阻害する。このような課題を考慮し、図 3 のようなフレームワークを提案する。

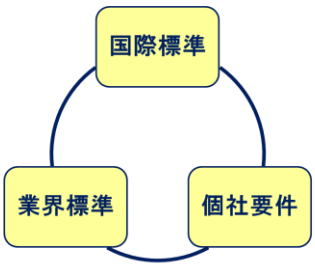

図 3. サプライチェーンにおける
情報セキュリティ管理のフレームワーク

このフレームワークは三つの要素からなる。海外企業からの委託や調達、受託や供給という視点から考えると、国際的な汎用性を持たせるために ISO/IEC27036 のような国際標準の活用が必要である。また、これまで述べてきたように業界の構造に依存するガバナンスモデルの違い、取引関係を考慮した業界共通の考え方も必要である。電機業界では EICC[4] や JEITA[5]からサプライチェーン管理の手法が提案されている。さらに、個社ごとの要求事項が差別化の視点から必要とされる場合がある。例えば、ソニーではソフトウェア納入物に関する独自のセキュリティ仕様書を公開している。しかし、この要求に偏りすぎると取引コストが増大してしまう。サプライチェーンの情報セキュリティ管理を考える上で、これらの要素をバランスよく組み合わせることが必要である。

5. まとめ

本稿では、サプライチェーンに関わる情報セキュリティリスクを検討し、国際標準を活用した管理手法について考察した。

今後は構築や運用、ISMS との関連等の観点から、さらなる検証が必要である。企業の事例研究や、NIST や ENISA 等の海外機関の提言内容の検討、特定化学物質や紛争鉱物の取り扱い規制等との比較を通して、さらに考察を深めたい。

謝辞

本研究に関して、様々な指導や助言を頂いた原田研究室の先輩，同僚の皆様に謹んで感謝の意を表します。

参考文献

[i] Martin Christopher, Hau Lee, Mitigating Supply Chain Risk Through Improved Confidence: International Journal of Physical Distribution & Logistics Management, vol.34, No.5, 2004, pp.388-396

[ii] 情報セキュリティ大学院大学原田研究室、2013 年情報セキュリティアンケート調査結果、スライド 39

[iii] Gary Gereffi , John Humphrey, Timothy Sturgeon, The governance of global value chains, Review of International Political Economy 12:1 February 2005, pp.78–104

[iv] 日本セキュリティ監査協会（JASA）、第五章サプライチェーンの情報セキュリティ管理基準の策定 中間報告、2012 年 2 月 20 日

[v] 三菱総合研究所、情報セキュリティガバナンス導入ガイダンス 補足編～ 企業グループにおける情報セキュリティガバナンスモデル ～、2011 年年 3 月、pp.9-26

[vi] ISO/IEC27036:2013 Information technology – Security techniques – Information security in supplier relationship

4 EICC：Electronic Industry Citizenship Coalition (電子業界 CSR アライアンス)

5 JEITA：電子情報技術産業協会