Vol.2014-DPS-161 No.3
Vol.2014-EIP-65 No.3
2014/9/18

# サプライチェーンにおける情報セキュリティの研究

久保知裕[†1]　　原田要之助[†2]

企業間連携の代表的な事業モデルであるサプライチェーンは，各企業の得意分野の分業化による効率性を目指す．サプライチェーンの効率性を決める重要な要素の一つが「情報」である．複数の企業をまたがった情報の流通，交換，加工，蓄積の可視化や効率化がサプライチェーンの価値に影響を与える．昨今は，グローバル化や従来以上の分業化，構造の複雑化のために，チェーン上の情報の可視化が難しくなっている．一方で，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つながるリスクが増大している．しかし，日本企業はリスク変化に対応した効果的な施策をとれていないことが，アンケート調査や開示情報を分析することで分かった．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行ったサプライチェーンのリスク管理に関する取組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た．クラウドや国際標準を活用することで，リスクの変化を考慮した対応を行うことができる．

# Study of Information Security in the Supply Chain

TOMOHIRO KUBO[†1]　YONOSUKE HARADA[†2]

Supply Chain is a major business model of enterprise collaboration, which aims to achieve superiority in operational efficiency by optimizing individual competences of enterprises. One of important elements to determine efficiency of supply chain is an “information”. Visualization and efficiency of information distribution, exchange, editing or storing across multiple enterprises influence on the value of supply chain. In these days, visualization of information in the chain becomes more difficult, as the chain becomes more globalized, fragmented and complicated. On the other hand, risk of breakdown caused by information security vulnerability in one of enterprises in the chain increases. However, it was found that Japanese enterprises couldn’t apply effective approach to control such risks, by analysis of questionnaire survey and disclosure information of listed enterprises.
Based on the result of survey of present risk management methodology from the other aspects, such as chemical materials, human rights, so on, as well as information security, it is proposed that the framework to manage information risk in the supply chain, in consideration about governance and characteristics of the supply chain. Solution to use cloud computing or international standards will be effective in the situation where risk is changing.

## 1. 背景と研究の目的

### 1.1 背景

近年，企業などの組織が行う事業活動は，単独の組織で完遂することは難しい．サプライチェーンのように複数の組織にまたがって業務活動が行われ，最終消費者に商品やサービスといった価値を提供することが一般的になっている．企業間の連携活動においては，プロセスの連携，情報伝達や共有が重要であり，情報システムはその基盤となる．企業が所有する情報システムだけでなく，IoT（Internet of Things）等，様々な機器がインターネットを介して結びつけられ，クラウド上におかれた情報システムで制御される環境も生まれつつある．一方で，システムやネットワークの障害，内部不正やサイバー攻撃等による情報流出や改ざん等のリスクも顕在化している．また，外部に依存しているが故，サプライチェーン構成企業のシステム停止やネットワーク障害が，連携するプロセスを阻害してサプライチェーン自体に影響を与える．誤ったデータがプロセスに投入されたり，改ざんされたりすることでサプライチェーン全体が誤動作するリスクもある．さらに，金銭目的であれば，サプライチェーン自体の脆弱性やセキュリティ管理の弱い企業を狙って攻撃することで，弱い企業のみならずチェーン上の全ての企業の株価に影響を与えるシナリオも成り立つ．

単独の企業が独立したシステムを構築・運用・利用していた時代に比べると，複数の企業が連携して事業活動を行う場合の情報セキュリティリスクは，問題の発生可能性，影響の大きさともに高まっている．

しかし，IT 活用ができているとは言い難い日本企業においては，情報セキュリティリスクの認識は薄く，管理施策も不十分であると推察される．現状の課題を踏まえ，日本企業の国際競争力強化につなげられる企業連携における情報セキュリティの枠組みを検討した．

### 1.2 研究の進め方

今回の研究においては，次の手順で検討を行った．まず，関連する先行研究を調査した．その結果を踏まえて，企業や官公庁などに対するアンケート調査や，有価証券報告書，CSR 報告書などの企業の開示情報の分析を行った．さらに，国内外のサプライチェーンにおける情報セキュリティリス

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

Vol.2014-DPS-161 No.3
Vol.2014-EIP-65 No.3
2014/9/18

ク管理状況の調査を行った．これらの調査から抽出された課題に対して，今後に向けた提言をまとめた．

## 2. サプライチェーン

本研究に関連する研究として，サプライチェーンのガバナンスモデル，サプライチェーンのリスク，サプライチェーンの情報セキュリティリスクの分野を取り上げた．

### 2.1 サプライチェーンガバナンスモデル

Gereffi らによる研究［1］よれば，サプライチェーンには市場型や垂直統合型など，いくつかのモデルが示されている．取引の形態や力関係によって決まるモデルに対してガバナンスの形態が異なり，リスクの所在も変化することが述べられている．ガバナンスモデルには以下の 5 類型がある．これを図 1 に示す．

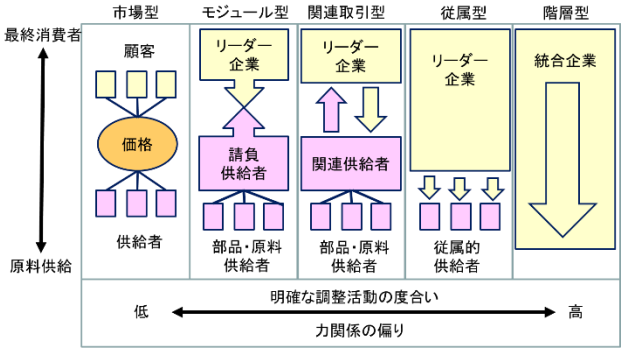


図 1. 5 つのグローバルバリューチェーンガバナンス（Gereffi ら）

- 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．
- 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 1 に示している調整活動は，企業間の情報提供と統制の関係を示している．統合企業のように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重要となる．一方，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 の間で対等の関係が成り立つため，市場型と同様，調整活動は少ない．

すなわち，ガバナンスモデルによって情報の外部への開示の程度や統制活動に違いがあることが分かる．また，業界の特性でも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．

### 2.2 サプライチェーンのリスク

サプライチェーンにおいては，企業が組織内に保持していたリスクを外部に移転したように見える．一方では，チェーン全体にリスクが広がったともいえる．

サプライチェーンに関するリスクは，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 や調達者 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．

IBM が 2009 年に行った Global Chief Supply Chain Officer Study［2］では，400 社のサプライチェーン担当役員への調査では，サプライチェーンオペレーションのグローバル化や相互依存関係の進展によってリスクが高まっており，また，管理自体も困難になっていると述べている．効果的なリスク管理を阻む主な障害としては，標準化されたプロセスの欠如，不十分なデータ，不適切なテクノロジーの利用が挙がっている．PWC のグループ会社である PRMT によれば，2010 年に行った同様の調査［3］で，サプライチェーンリスクは end to end のプロセス全体として考える必要があり，顧客や外部サプライヤと連携したリスク管理の必要性を述べている．

### 2.3 サプライチェーンの情報セキュリティリスク

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［4］で，次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には，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．

Christopher らの研究では，このような状況に陥らないために，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参考になる．

また，IT のアーキテクチャの視点から，自組織のみを守る情報セキュリティ対策だけでなく ICT チェーン全体の情報セキュリティを守るための仕組みについても提案がなされている．長内らは ICT に参加する企業共通のセキュリティ基盤の構築を提案した［5］．これにより標準化された情報セキュリティに関する指標や情報の共有，分析の自動化や継続的なモニタリングする仕組みを提案している．この仕組みにより，日々変化する脆弱性に対して効率的な対応を進められるとしている．

## 3. 情報セキュリティリスクの現状調査

### 3.1 これまでの調査

(1) アンケート調査

情報セキュリティ大学院大学原田研究室でアンケート調査を実施した．2013 年 7～8 月にかけて，ISMS もしくはプライバシーマーク（P マーク）の取得企業，官公庁，大学の 4500 団体に情報セキュリティに関するアンケートを送付し，有効回答 367 を得た［6］．

回答の結果から，アウトソーシングを含むサプライチェーンについては個人情報保護，機密性を重視する傾向があること，委託先に対しては国内基準・企業独自基準を要求する傾向があること，管理手法に関する政府関連のガイドラインの普及施策が進んでいないことがわかった．

(2) 有価証券報告書の分析

上場企業は，経営に影響を与える可能性がある主要なリスクを「事業等のリスク」として有価証券報告書に記載する義務がある．「事業等のリスク」に述べられている情報セキュリティリスクに関連した記載内容を分析することで，企業のリスク認識について調査した．この調査により次のような結果が得られた［7］．

大企業に比べ中小企業は情報セキュリティに関する意識が低く，特に外部からの攻撃に対する認識が低い．すなわちサプライチェーンの中心になる大企業では，セキュリティ対策がとられていても，サプライチェーンを支える中小企業には脆弱性が残っている可能性がある．中小企業であっても，情報セキュリティ対策が不十分な企業が破たんするとサプライチェーン全体が影響を受けて事業全体が停止し，関連する全企業に多大な影響を与える可能性がある．

日系企業の情報開示は，米系企業に比べ質量ともに少ない．また，外部からのサイバー攻撃に対するリスク意識は米系企業が日系企業に比べ高いように見える．これらは，米系企業では投資家に対する説明責任を果たすため，リスクを網羅的に記載する傾向にあるためと考えられる．

### 3.2 CSR 報告書および調達方針の調査

有価証券報告書の調査対象とした TOPIX　CORE30 の企業について CSR 報告書及び調達方針から調達における情報セキュリティリスクの認識や管理手法について調査した．

CSR 報告を開示している 29 社のうち，機密情報の保護を中心に 6 割の企業が情報セキュリティを CSR 項目として挙げていた．また，調達方針を開示している 20 社のうち，6 割の企業が情報セキュリティを項目として挙げていた．一方，多段階管理として取引先の取引先について情報セキュリティ管理を求めていた企業は 4 社のみであった．

CSR 報告書から，一部の業界では業界全体として取り組みが行われていることが分かった．代表的な取り組みは，電子業界の国際的行動規範である EICC(電子業界 CSR アライアンス:Electronic Industry Citizenship Coalition)と JEITA（電子情報技術産業協会）である．JEITA は EICC の行動規範［8］を元に，所属企業が引用して自社向けにカスタマイズできるように標準となる CSR 調達ガイドライン［9］を策定している．ガイドラインの中には情報セキュリティに関する項目があり，①コンピュータ・ネットワーク脅威に対する防御，②個人情報の漏えい防止，③顧客・第三者の機密情報漏えい防止について，リスクおよび対応方針について述べている．特に，電機及び通信業界の企業はこのガイドラインに準拠した調達ガイドラインを自主開示している．また，このガイドラインにはチェックシートが添付されておりサプライヤは自己評価を行うことができる．自動車業界では自動車部品工業会がガイドライン［10］を策定しており，コンプライアンス分野の一項目として，機密情報の保護・管理を挙げている． JEITA と同様にチェックシートが添付されておりサプライヤの自己評価を行えるようになっている．

さらに，業界の取り組みに加え個社としてチェックシートや仕様を開示している企業がある．パナソニックでは情報セキュリティに関するチェックシート「お取引様向け情報セキュリティ基準チェックシート（ver2.0c）」［11］を取引先に記入してもらうことを求めている．主な項目は，情報セキュリティの管理体制の確立，情報資産の機密管理，人的な対策，情報セキュリティ事件・事故対応，情報セキュリティマネジメントの実施となっている．また，ソニーは技術マニュアルとして,「製品セキュリティ確保に関する基準（STM-0117 第 10 版 一般用）」［12］を開示している．ソフトウェア製品の納入においては，この仕様に準拠することを求めている．一方，取引先に対するモニタリングは，アンケートなどを用いたセルフチェック，委託先企業の自己監査，委託元企業の立ち入り監査，第三者による監査が行われている．特に第三者による監査については，セブン&アイ・ホールディングス，日立製作所，三菱商事などが

実施している．これらの企業においてはアジアを中心に海外の取引先に監査も行っている．取引先の教育および CSR 実践への支援としては，品質管理を中心としたセブン&アイ・ホールディングスや環境マネジメントを中心にしたコマツのみどり会，日立製作所の新 MMM 倶楽部の活動を挙げることができる．

### 3.3 経団連による CSR 調査

経団連は 2009 年 9 月に企業の CSR の取り組み状況に関するアンケート調査の結果［13］を発表した．

サプライチェーンに関連する設問 5，9，10，11 の回答をまとめると，

- サプライチェーンに関する取り組みが進んでいないこと
- サプライヤの情報セキュリティ管理を重要事項と考えていること，
- サプライヤに対するガイドラインの策定などにくらべ実効性のある教育や監査の取り組みが行われていないこと
- チェーンのグローバル化や多段階化に伴い取り組みの標準化が求められる一方で，画一的な対応が難しいこと

など，企業が抱える問題点を挙げている．

## 4. サプライチェーンにおけるリスク管理の現状調査

サプライチェーンのリスク管理について，情報セキュリティとそれ以外の化学物質管理などに分けて調査を行った．

### 4.1 情報セキュリティのリスク管理

国内外におけるサプライチェーンを対象とする情報セキュリティ管理の施策について次に述べる．

(1) 国内の施策

国内において提案されている施策の課題は，次のとおりである［14］．

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のかどうか疑問である．また，管理手法は標準化を意識しすぎたためか，画一的で，Gereffi 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．さらに，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．チェーン全体のリスク管理を行うために可視化は重要だが，海外に展開した業務や多段階に分割された業務についての言及が不足している．きめ細かな対応は必要であるが，過剰になると取引コストが過剰にかかる可能性がある．これらの点について，さらに検討を行う余地がある．

（2）NIIST, ENISA

海外におけるモデルや施策についても調査した．

NIST はサプライチェーン全体に対するサイバー攻撃のリスクを指摘したうえで，情報システムのライフサイクルを通したリスクの定義と管理策を提唱している．「情報システムセキュリティ」，「調達」，「法律」，「情報システムのオーナーとサービス提供者」の 4 つの柱がサプライチェーンリスクをコントロールする能力を決めるとしている［15］．また，ENISA はサプライチェーン管理の複雑性，サプライチェーン全体に渡る共通したガイドラインや取り組みの欠如，セキュリティ管理のための製品やテクニックの欠如などの問題を指摘している．これらの課題に対応するための施策として，信頼性や整合性を評価するためのフレームワークの必要性を提唱している［16］．

（3）ISO

国際標準の動向として，情報セキュリティ分野では ISO/IEC27002: 2013 が，冗長化等，可用性を重視することと，サプライヤ（供給者）に関連する事項を一つの箇条にまとめるなど，管理施策の見直しが行われた．

ISO/IEC27017 と ISO/IEC27036:2013［17］がサプライヤやアウトソーサー，クラウド事業者等の外部組織の情報セキュリティ施策について独立した標準を構成している．また，情報セキュリティガバナンスについては ISO/IEC27014:2013 が制定されている．

ISO/IEC27036:2013 は 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，「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」，「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」，「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．さらに，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．

### 4.2 規制化学物質のリスク管理

原材料や製品，副資材などにおいて利用される化学物質については，欧州の REACH 規制，日本の化学物質審査規制法等，人体に有害な物質や環境汚染につながる物質の利用規制が法的に定められている．

化学品のサプライチェーンが世界中に張り巡らされていることから，国際化学工業協会協議会 ICCA（International Council of Chemical Association）では，2002 年のヨハネスブルクサミット（WSSD）で設定された 2020 年目標，すなわち「人の健康や環境への重大な悪影響を最小限に抑制できる方法での化学物質の使用と生産」の達成に向けた取り組み［18］を行っている．これは，個社や各国の業界団体

だけの取組ではなく，世界の化学工業会が政府や取引先と連携することで，目的を果たそうとする取り組みである．
規制化学物質の管理において特徴と考えられるのは，関連するステークホルダーとの情報共有，ベストプラクティスの追求を継続的に行っていること，リスクの変化に対応した研究をサポートしていること，中小企業や新興国など急速な対応の難しい事業体への支援プログラムがあること，国際機関と連携しグローバルな視点から考慮されていることである．
さらに，このような動きを踏まえ，日本国内においても中小企業向けのガイドラインが提供されている．平成 24 年度の経済産業省の委託事業として中小企業の製品含有化学物質管理支援推進委員会が作成した「中小企業向け製品含有化学物質管理の手引き」[19]である．公開された JIS Z 7201（製品含有化学物質管理-原則及び指針）にもとづき，サプライチェーンにおける共通の考え方が提示されている．サプライチェーン上の中小企業での対策が進んでない点を課題として挙げ，リスクだけでなくメリットを含めた必要性，取り組むべき事項や範囲，チェックシートやサンプル事例など具体的な管理方法について解説している．

### 4.3 紛争地域鉱物のリスク管理

OECD は「紛争地域および高リスク地域からの鉱物の責任あるサプライチェーンのためのデュー・ディリジェンス・ガイダンス」[20]を 2011 年に発行した．このガイダンスは，中央アフリカの紛争地域で採掘された鉱物，スズ，タングステン，タンタル等のサプライチェーン・マネジメントについて，政府支援のもとで多様な利害関係者が共同で行った取り組みである．目的は企業が人権を尊重すること，また，その鉱物採掘活動を通じて紛争に手を貸してしまうことを回避することである．このガイダンスには法的な拘束力はないが，政治的なコミットメントがあるとされている．国によっては米国における紛争鉱物の開示規制（SEC に対する届け出）[21]のように実質的な拘束力を持つ場合もある．
紛争地域では，反政府勢力が鉱山や流通経路を支配し，徴税やみかじめ料のような形態で資金源とするケースも多い．また，支配の中では強制労働や児童労働，虐待など人権を侵害していることもある．分業化が進む中で，鉱物の採掘や流通，精錬業者，加工業者が，このような問題に知らないうちに手を貸してしまうことを避けるために，サプライチェーン上の関係者がとるべき手段を提供する必要がある．このガイダンスでは，多様な利害関係者が共同で関与し，透明性の高い鉱物サプライチェーンを確保することを求めている．個々の企業の管理システム，チェーン全体のリスク分析，対応する取り組み，独立的な監査，情報の共有といった 5 段階の取組が示されている．さらに，この取り組みを，全ての供給業者や関係者との契約，合意書に盛り込むことが求められている．各国の法制度と国際標準との調和や，関係団体，政府との協力関係の構築が求められている．

### 4.4 児童労働，労働者の人権のリスク管理

バングラディシュの首都ダッカで 2013 年 4 月に発生した縫製工場の崩落事故では 1000 人を超える犠牲者が出たといわれる．低賃金，長時間労働，劣悪な労働条件での勤務など南アジアを中心とした繊維工業においては労働者の人権問題が指摘されてきた．この事件の結果，工場の経営者にとどまらず，発注元のメーカーが長期にわたる安全対策への支出や労働条件の改善に向けた施策をとることを求められた．このように，サプライチェーンで分業化が進んでも，その管理責任はチェーン全体で負っていかなければならないことを示している．
国連の制定したグローバル・コンパクト 10［22］は人権，労働，環境，腐敗防止の 4 つの分野，10 の原則からなる．グローバルなサプライチェーンを保持する多国籍企業に向けたもので，企業の社会的責任の視点から整理されている．この中で原則 5 が児童労働の実効的排除となっている．地域によるリスクの違いの認識や年齢確認の方法確立などとあわせ，国内法が十分でない場合は国際基準を考慮すること，下請け業者やサプライヤなどその他の関連業者に影響力を駆使すること等が述べられている．
第三者機関による認証制度を持つ国際標準は，企業の倫理的側面に注目した SA8000［23］がある．SA8000 は労働者の人権，雇用環境，児童労働などの項目が含まれている．国内関連法規の遵守に加え，国際的な条約や勧告の原則を考慮し，労働者にとって最も良い条件になるように配慮することを求めている．サプライヤやその下請け業者との取引も可視化し，労働条件が守られていることを管理しなければならない．
海外の大手アパレル企業や新興国のアパレル企業が認証を受けている反面，日本では普及していない．中村の研究[24]の中で日本財団 CANPAN 事務局からの引用として，普及しない理由を三点挙げている．日本の大企業の正規労働者の労働条件はすでに高いレベルにある，ISO など国際規格が多すぎる，日本企業は第三者監査を嫌い経団連でも自主的行動を促している，としている．

### 4.5 その他のイニシアティブ

経団連の企業行動憲章実行の手引き［25］を取り上げる．1996 年に初版が発行された企業行動憲章は，日本企業の社会的な責務に対する取り組みのガイドラインとなる．第三者による認証制度ではなく，自社で率先して取り組むことによる自主規制としての位置づけが高いと考えられる．経営者の責任を含めた 10 の大項目からなる．個人情報・顧客情報の保護やサプライチェーンに対する CSR の働きかけを行うといった具体的な提言が含まれている．情報管理の項目では，高度 ICT 社会の一員として法令遵守にとどまらず自律的な情報セキュリティ対策が強く求められている．

### 4.6 分析

CSR の観点から行われているサプライチェーンのリスク管理の取り組みは国際的なものである．これらの取り組みに共通しているのは次の四点である.「サプライヤ, 取引先, その下請けを含めたサプライチェーン全体の可視化を求めていること」,「政府や国際機関，消費者団体等のステークホルダーとの協調を求めていること」,「国際的な協調を求めていること」,「法的，もしくはそれに準じるような拘束力を持たせるとともに，具体的な施策や基準を示していること」が挙げられている.

海外での取り組みは，内向き志向の強い日本企業では普及しているとは言い難い．品質管理や環境問題に関する取り組みは海外でも評価されていることを考えると，情報セキュリティリスク管理についても，発想を国内の延長線上におくのではなく，グローバルな視点から検討しなければならない．今後，海外企業との分業が当たり前のようになる中で, リスクを普遍的な視点でとらえる経営が必要になる.

## 5. 課題

これまでの調査から，サプライチェーンの情報セキュリティ管理に関する日本企業の課題を 5 つにまとめた.

(1) サプライチェーン全体の可視化ができていない

情報セキュリティだけに限らず，多層化，グローバル化によってサプライチェーン自体の可視化が難しくなっている. 一企業だけの努力ではチェーン全体の情報を収集することは難しい.

（2）サプライヤとの協力関係の構築が難しい

分業化が進むことで，関係するサプライヤの数が増加している．グローバル化に伴って国や地域，文化の多様性を考慮しなければならなくなっている．また，チェーン全体のコスト削減を求める中で，個別のリスク対応はコスト上昇につながる可能性がある.

（3）セキュリティリスクの認識が機密性に偏っている

個人情報保護法を意識しているため，機密性に対する認識は高い．一方で，サービスの種類やガバナンスモデルによってリスクは異なるので, 画一的に機密性を担保できない. また，サイバー攻撃に対する認識が低く，セキュリティ対策が脆弱な企業が存在するチェーンは高いリスクを包含していると言える.

（4）リスク管理において国際標準の利用が進んでいない

チェーンのグローバル化が進む一方で，国内のみの制度である P マークの認証を受けて，これで十分としている企業が多い．また，個社の要件を定める契約だけでセキュリティ要件を示している企業が多い.

(5)セキュリティリスク認識の啓発や対処方法の普及施策が不十分である

情報セキュリティ管理は法的な拘束力がなく，企業任せになっている．チェーン上の化学物質や紛争鉱物の取引，児童労働については法的，もしくは準ずる形態の拘束もしくは義務がある. 情報面では, 個人情報保護法の施行により，日本企業における個人情報へのリスク認識が高まったことを考えると，情報セキュリティ管理に関する取り組みは不十分だと考えられる. グローバル化に対応した啓発活動が，企業単独，業界，政府といったレベルでほとんど行われていない．言語に起因するかもしれないが，国内の取り組みだけに終始しているため，チェーン全体としても不完全であると言える．サプライヤの協力会を通した啓発，教育，改善支援活動が行われているものの，一部の企業に限定されている．海外サプライヤへの働きかけも弱い．これらの問題は，日本企業が系列といわれた同系色の強い企業集団から，海外企業を含むマルチサプライヤ型に変化していく過程で発生している一過性的な状況かもしれない.

## 6. 対応策

企業にとって最も重要なのは，自社がイニシアティブを持ってサプライチェーンをコントロールする意思である．サプライヤなどの取引先にリスク管理を任せてしまうことで, リスクの所在や大きさが分からなくなる．情報セキュリティリスクに係らず，サプライチェーン戦略が対応の基本となる.

また，サプライチェーンの対象となるモノやサービス，業界の構造やガバナンスモデルによって情報セキュリティリスクは異なる．業界固有の問題であれば，一企業だけでなく業界全体の取り組みを行うべきである．先に述べたとおり，規制化学物質の取引においては化学工業に関わる団体や政府，国連関係機関等の様々なステークホルダーが関与してルールを決めている. また, 電子業界における EICC, JEITA の取り組みや自動車業界における調達ガイドラインも同様である．業界で取り組むことにより，業界固有の要件に関するルールの策定，管理手法の標準化，モニタリング手法の共通化など，リスク管理に関するコストの分担，低減を図ることが可能になる.

### 6.1 PDCA サイクル

リスク管理のステップを PDCA サイクルとして，次のようにまとめた.

（1）計画

計画段階では，サプライヤの選択と並行してチェーン全体のスコープの定義，リスク分析，さらに，リスクに応じた施策の策定を行う．この分析においては，情報セキュリティ部門だけでなく，関連部門（例えば，調達部門），サプライヤと共同して行う必要がある.

取引の力関係によって，国際標準の利用を推奨するレベルから，強制的に適用させるレベルまで考えられる．また，支配関係が強ければ，サプライチェーンに属する企業が共

同して利用できるようなコミュニティクラウドを利用するか， FedRAMP ［26］のように一定以上のセキュリティを担保したクラウドを利用させる．FedRAMP は，米政府が官公庁の利用するクラウドサービスに対してセキュリティ評価や認証，モニタリングのための標準手法を提供するプログラムである．これにより，ベースラインとなるセキュリティをサプライチェーンに保証することが可能になる．クラウドの利用により，海外のサプライヤであっても，多段階のサプライヤであっても共通の基盤を利用することでインフラとしてのセキュリティは担保しやすくなる．

（2）構築・導入

セキュリティ施策の構築・導入については，サプライヤとの良好な協力関係が重要である．セキュリティ対策はコスト要因の一つでもあり，契約においては利害が対立する．戦略的な取引関係を長期にわたって継続する場合は，利害関係を緩和するために，サプライヤに対する技術的，人的な導入支援を行うこともあり得る．施策の導入だけではなく，リスクに関する教育・啓発，例えばサイバー攻撃の脅威等，を行う必要がある．例えば，大成建設とトレンドマイクロは共同で簡易セキュリティ診断ツールを開発した．建設業界はサプライチェーンの多段階化が進んでおり，一つの建設現場だけで多くの下請け業者が参加する．設計資料等へアクセスする PC は事前にインターネット経由で診断ツールを使って，セキュリティレベルに該当しているかどうかを確認することができる．この診断を通して，下請け業者のセキュリティ意識を啓発することができたとしている［27］.

（3）モニタリング

モニタリングには様々な手法が考えられる．リスクの大きさに応じて，簡単なチェックシート，アンケート，サプライヤによる自己監査と宣誓，自社による立ち入り監査，最もコストのかかる第三者監査などが考えられる．セブン&アイ・ホールディングスでは，CSR 調達の一環としてアンケートと立ち入り監査を実施している［28］.食品などを海外から調達するため，取引先の監査は必須である．この監査の一部には情報セキュリティが含まれ，管理状況のモニタリングが行われている．個別要件による立ち入り監査はコストがかかることを考えると，国際標準による認証はより効率的に実施することが可能である．なお，再委託先や海外のサプライヤによる情報の流出事故に伴う委託元の信頼の失墜や，委託先のシステム障害による事業活動の停止などの事件が後を絶たないことから，完全な手法はないかもしれない．しかし，サプライヤとの契約の中で，取引先やその先の取引先に対する抜き打ちの立ち入り監査の権利について明示しておくことにより，ある程度の抑止効果は期待できるのではないだろうか.

（4）改善

サプライチェーンの構造変化に伴うリスクや，サイバー攻撃など情報セキュリティのリスクが変化している中では，継続的な改善活動が重要である．サプライヤ個別の取り組みはコスト等の負荷が大きい．コマツのみどり会や日立製作所の新 MMM 倶楽部のように日本企業では取引先の協力会を持つことも少なくない．協力会はサプライチェーンの効率性向上だけではなく，供給の安定性，品質の向上など事例を共有しながら互いに向上させることを目的としている．情報セキュリティに関しても同様に，是正施策をデータベースや勉強会などの場で共有化することが望ましい．さらに業界全体で共有するケースも考えられる.

### 6.2 国際標準，業界標準，個社要件の考慮

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・調達するモノやサービスによって異なる．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場合，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個別に構築・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 2 のようなフレームワークを提案する.

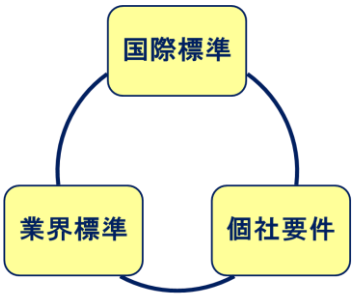


図 2. サプライチェーンにおける情報セキュリティ管理のフレームワーク

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/IEC27036:2013 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 や JEITA 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．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.

### 6.3 普及のための施策

情報セキュリティに関するリスク意識や管理のための施策を普及させるためには，法的な義務を伴うガイドラインも

しくは企業にとって経済的なメリットが提供できる枠組みが必要である．個人情報保護に関しては，法的な整備に伴い遵守することが義務となっている．これは P マークが普及している理由の一つであると考えられる．化学物質の管理や紛争鉱物の取引禁止，児童労働の禁止についても，国際的な取り組みや各国の法律に基づいた規制が，普及要因の一つである．一方で，ISO9000 シリーズの品質マネジメントシステムのように，官公庁や民間企業の入札の条件として要求される場合，企業は取引のために認証制度を利用するようになるであろう．また，問題が発生しても責任を免除されるといった，インセンティブもあわせて考えるべきである．

## 7. まとめ

アンケート調査や文献調査を踏まえた考察の結果，日本企業のリスク認識は不十分で，管理手法についても改善の余地があることが分かった．特に，日本企業の内向性の強さもあり，チェーン全体を見渡した視点が欠けていたり，国際標準の普及が妨げられたりしている可能性があることが分かった．

これからも，為替や労働コスト，地政学的なリスクなどから，グローバルなサプライチェーンはますます発展していくであろう．しかし，サプライチェーンにおける情報セキュリティ管理の在り方についての研究は，海外が先行しているものの，試行錯誤を行っている段階である．日本企業がサプライチェーンを取り巻くリスクを俯瞰して分析すること，業界や個々の企業における協力会のような活動を通して知恵を絞ることで，海外にも通用する管理手法が確立できると考える．個別企業の内部においても，さらに，その中の情報セキュリティ部門においても，内部の殻に閉じこもることなく衆知を集めて，ベストプラクティスを生み出すようにするべきである．

## 謝辞

本研究に関して，様々な指導や助言を頂いた情報セキュリティ大学院大学の教授および原田研究室の先輩，同僚の皆様に謹んで感謝の意を表します．

## 参考文献

1) Gary Gereffi , John Humphrey, Timothy Sturgeon, The governance of global value chains, Review of International Political Economy 12:1 February 2005, pp.78–104
2) IBM, よりスマートな未来のサプライチェーン（GLOBAL CHIEF SUPPLY CHAIN OFFICER STUDY），2009 年，p.18
3) PRTM，グローバルサプライチェーントレンド　2010－2012，2010 年，p.18
4) 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
5) 長内仁，後藤厚宏，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，巻 : 112 号 : 463，pp.699-704
6) 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，情報処理学会研究報告. EIP, [電子化知的財産・社会基盤] 2014-EIP-63(12), pp.1-7
7) 久保知裕，原田要之助，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，電子情報通信学会技術研究報告，巻：114 号：25, pp.75-82
8) EICC 行動基準　Ver4.0
9) 社団法人　電子情報技術産業協会 資材委員会，サプライチェーン CSR 推進ガイドブック【CSR 項目の解説】，平成 18 年 8 月
10) 社団法人　日本自動車部品工業会，CSR ガイドブック，平成 22 年 4 月改訂
11) パナソニック株式会社，お取引先様向け情報セキュリティ基準チェックシート（Ver2.0c）
12) ソニー株式会社ソニー技術標準事務局，製品セキュリティ確保に関する基準（STM-0117 第 10 版 一般用），2013 年 10 月 1 日
13) 社団法人　日本経済団体連合会 企業行動委員会，CSR（企業の社会的責任）に関する アンケート調査結果，2009 年 9 月 15 日
14) 久保知裕，原田要之助，サプライチェーンにおける日本企業の情報セキュリティガバナンスに関する研究，第 28 回研究大会講演要旨，システム監査学会，2014 年 6 月 6 日
15) NIST，NISTIR7622，Notional Supply Chain Risk Management Practices for Federal Information Systems，2012 年 6 月，pp.1-15
16) ENISA，An overview of the ICT supply chain risks and challenges, and vision for the way forward，pp.19-28
17) ISO/IEC27036:2013 Information technology – Security techniques – Information security in supplier relationship
18) 国際化学工業協会協議会 （ICCA），進捗報告書，第 3 回国際化学物質管理会議，2012 年 9 月 17～21 日
19) 中小企業の製品含有化学物質管理支援推進委員会，中小企業向け製品含有化学物質管理の手引き，経済産業省委託事業平成２４年度環境対応技術開発等（製品含有化学物質の情報伝達の実証調査)，2013 年 3 月
20) 経済産業省，OECD 紛争地域および高リスク地域からの鉱物の責任あるサプライチェーンのためのデュー・ディリジェンス・ガイダンス（仮訳），2011 年
21) 経済産業省, 米国の紛争鉱物開示規制, 2013 年 4 月 16 日更新, http://www.meti.go.jp/policy/external_economy/trade/funsou/ (2014 年 6 月 28 日閲覧)
22) グローバル・コンパクト・ネットワーク・ジャパン，『国連グローバル・コンパクト 4 分野 10 原則の解説』の日本語訳（仮訳），http://ungcjn.org/gc/pdf/GC_10.pdf (2014 年 7 月 6 日閲覧)
23) Social Accountability International, SA8000：2008, 株式会社あらたサステナビリティ訳
24) 中村まり，第六章企業の CSR と児童労働，「児童労働根絶に向けた多面的アプローチ：中間報告」調査研究報告書，アジア経済研究所，2011 年
25) 社団法人　日本経済団体連合会，企業行動憲章 実行の手引き（第６版），2010 年 9 月 14 日
26) アメリカ連邦政府，Federation Risk and Authorization Management Program，http://cloud.cio.gov/fedramp (2014 年 7 月 10 日閲覧)
27) トレンドマイクロ株式会社，セキュリティマガジン TREND PARK「大成建設 CIO が語る，ワークスタイル革命への挑戦」，2013 年 1 月 25 日公開，http://www.trendmicro.co.jp/jp/trendpark/talk/taisei/20130820015431.html (2014 年 7 月 10 日閲覧)
28) 株式会社セブン＆アイ・HLDGS，CSR Report 2013， pp.12-13