Vol.2014-DCC-7 No.13
Vol.2014-EIP-64 No.13
2014/5/15

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

久保知裕[†1]　　原田要之助[†2]

企業におけるサプライチェーンの情報セキュリティガバナンスについて，アンケート調査と企業の開示情報の分析を行った．まず，情報セキュリティアンケート調査では，業務委託等のサービスを含む広義のサプライチェーンに関する情報セキュリティのリスク認識や管理手法に注目した．また，上場企業が有価証券報告書や CSR 報告書などで開示している，サプライチェーンに関する情報セキュリティのリスク情報を分析した．
これらの調査と分析から，中小企業は情報セキュリティ，サプライチェーンのリスクについて，大企業に比べると認識が低い．特に外部からの攻撃についてはリスク意識が低いことから管理手法も不十分だと考えられ，サプライチェーン全体の脆弱性につながっている可能性があることが分かった．

Study of Information Security Governance in the Supply Chain

TOMOHIRO KUBO[†1]　YONOSUKE HARADA[†2]

Information security governance of the supply chain has been researched by questionnaire survey and analysis of disclosure information of listed companies. Questionnaire survey has focused on recognition of information security risk and management measures in supply chain incl. outsourcing as service supply chain. Also, risk information of information security in supply chain, disclosed in annual reports or CSR reports of listed companies, has been analyzed.
Through those survey and analysis, small and medium enterprises have less recognized risk of information security and supply chain, than large enterprises. Especially, risk recognition of attacks from outside is too low to manage effectively. This will lead vulnerability of supply chain.

1. 背景と研究の目的

1.1 背景

企業間の業務連携モデルであるサプライチェーンにおいて，情報セキュリティのリスクは大きくなっている．企業は事業活動全般において情報システムへの依存度が高くなっており，サイバー攻撃，情報システムの障害や誤作動，情報の漏えいなどは，事業継続に直結する問題となっている．
サプライチェーン,特に生産工程における代表例である「カンバン」や「ジャスト・イン・タイム」では，独立した工場内の工程管理だけでなく，部品工場から組み立て工場，それらを担う各企業の情報システムが密に連携して稼働しており，他社の情報システム障害がサプライチェーン全体の事業の停止につながる．すなわち，企業にとっては，自社以外の企業においてリスクが顕在化すると，サプライチェーンを通して自社の顧客に商品やサービスが提供できなくなる．
さらに，標的型攻撃や脆弱性をついた不正アクセス，外部からのサイバー攻撃，内部からの情報流出はサプライチェーンで連携した企業の全体のリスクを高めている．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．
一方で，サプライチェーンモデルは経営環境の変化に対応して進化しているが，リスク認識やリスク管理の進化は追いついていない．日本企業の場合，全ての機能を自社内，自社グループ内に抱え込む垂直統合型の「系列」といわれるビジネスモデルがある．代表する一社を頂点にし，国内の関連企業を裾野にもつピラミッド型を構成していた．気心の知れた取引先と信頼感を醸成し，関係を構築することができた．しかし，海外市場への展開，競争のグローバル化などにより，原材料や部品，サービスの調達を現地で行うようになっていること，資本効率を高めるために企業が得意な分野に特化し系列内だけで調達ができなくなっていること，事業規模を確保するために原材料や部品の生産者が系列を超えて統合し一部の会社に取引が集中することなどから系列が崩壊し，取引関係が複雑化している．これらの新しい現実は,企業間の関係を従来のピラミッド型から,メッシュ型やダイアモンド型[1]に変化させたといわれている．この変化にともないリスクの所在がわかりにくくなっているが，リスクの認識や管理手法はピラミッド型のままで変わっていない．

†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

サプライチェーンおよび情報セキュリティ双方の視点から，新しいモデルにおける有効な管理手法を検討する必要がある．サプライチェーンに関しては，化学物質[2] や紛争鉱物の規制[3] ，児童労働の禁止[4] 等において管理が実施されており，参考にはなるが，これらは国際的な規制という共通の枠組みがあるので，チェーンとして共同で実施しやすいという特徴がある．一方，情報セキュリティにおいてはガバナンスのスコープが個々の企業や企業グループにとどまっているため，サプライチェーン全体に対するフレームワークとしては十分とは言えない．新しいフレームワークが必要となっている．

1.2 研究の目的と進め方

海外においては国際標準や政府レベルで，サプライチェーンの情報セキュリティの脆弱性を改善するための管理手法の検討が進んでいる．NIST[5]，ENISA[6]ではサプライチェーンの情報セキュリティに着目したガイドラインが提示され，ISO/IEC27036[7]も公開された．

このような流れの中で，サプライチェーンにおける情報セキュリティの脆弱性を改善する管理手法を提案することで日本企業の競争力を高める必要がある．

そこで，本稿ではサプライチェーンや情報セキュリティのガバナンスモデル，リスクマネジメントなど関連する研究を参考にしながら，サプライチェーンの情報セキュリティについて企業の認識しているリスクと管理手法について，アンケート調査および企業の開示情報を利用して分析を行う．

2. 関連研究

本研究に関連する研究として，次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

Greffi らによる，The governance of global value chain model[8]の研究によれば，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．この論文では，サプライチェーンの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．また，Nadvi による Global standards, global governance and the organizational of global value chain[9]では，アジアにおける NIKE の生産委託工場で，禁止されている児童労働が発覚した事件を取り上げ，グローバルガバナンスと国際標準の関係について述べている．

2.2 サプライチェーンリスクマネジメント

サプライチェーンのリスク管理は財務的リスクやオペレーショナルリスクなど様々な側面から取り上げられている．Manuj らによる Global supply chain risk management strategies[10]ではサプライチェーンに関わるリスクと対応策を整理した．Christopher らによる Mitigating Supply Chain Risk Through improved confidence[11]では，サプライチェーン全体の可視化によってリスクが緩和されることや，正確な情報を利用して PDCA を回すことによりサプライチェーン全体の信頼性が高まると述べている．

2.3 情報セキュリティガバナンス

情報セキュリティガバナンスでは，セキュリティリスク管理の観点で様々な検討が行われている．

原田による「情報セキュリティガバナンスと説明責任」[12]ではビジネス価値を高めるための IT ガバナンスと防御的な情報セキュリティガバナンスを区別したうえで，いくつかの制度の中から社会的合意方式による情報セキュリティ監査制度が優れていると述べている．Brotby の Information Security Governance[13]によれば，情報セキュリティガバナンスの戦略策定から導入，運用の過程を示すとともに，効果的な管理のためには尺度を決めて，日ごろから改善を進めることが重要であると述べている．また，Gelbstein による Strengthening Information Security Governance[14]では，情報セキュリティガバナンスの弱い組織はサイバー攻撃に対して脆弱であると指摘し，弱さの兆候を 10 の項目にまとめている．

多田による「情報セキュリティへの取組と企業の社会的責任」[15]や林らによる「企業と情報セキュリティガバナンス」[16]では，企業の社会的責任（CSR）の視点から情報セキュリティガバナンスの重要性を指摘している．

板倉らによる「P マーク審査から見た中堅企業の情報セキュリティ・ガバナンス」[17]では，事業規模の小さな企業の取組としてプライバシーマーク（以下，P マーク）を利用した情報セキュリティ管理の事例を調査している．

3. アンケート調査

3.1 アンケートの概要

情報セキュリティ大学院大学，原田研究室では毎年，情報セキュリティ対策に関するアンケートを行っている．2013 年は情報セキュリティマネジメントの取組み状況，情報セキュリティへの管理体制と人材育成，情報セキュリティのガバナンス，営業秘密の管理，クラウド・コンピューティング，事業継続計画等の調査を行った．調査の概要は次のとおりである．

- 実施期間　2013 年 7 月から 8 月
- 対象組織　ISMS もしくは P マークの取得企業および，大学と官公庁
- アンケート発送数　4500，回答数　367 件
- 調査方法　郵送によるアンケートの送付と回収
- 設問数　50 問

本研究に関しては 12 の設問を通して，組織の調達活動や業務委託，受託に関して情報セキュリティ上のリスク認識や管理手法について調査 した[18].

Vol.2014-DCC-7 No.13
Vol.2014-EIP-64 No.13
2014/5/15

3.2 回答事業体のプロファイル

回答のあった 367 件の事業体について，図 1 に業種，図 2 に事業規模と取得している認証の状況を示す．

図 1 で示すとおり，最も多いのは 45%の情報通信業でソフトウェア開発やデータ処理などの IT サービスや広告業などを含む．次いで大学が 20%，11%が人材派遣などのサービス業となった．

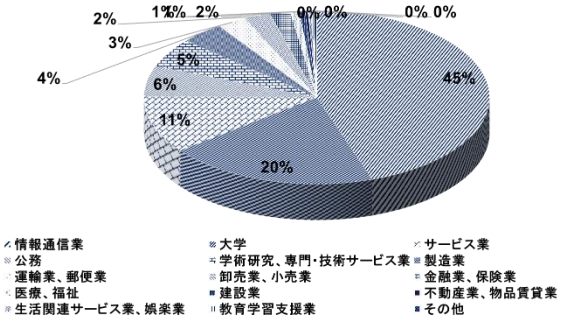

図 1　回答事業体の業種（N=367）

図 2 では回答事業体の規模（企業は売上，大学と官公庁は予算）と取得している認証を示す．最も多いのは 10 億円以上 50 億円未満であり，全体の 33%であった．次いで，5 億円以上 10 億円未満が 14%，1 億円以上 3 億円未満が 13%となっている．また，50 億円以下の事業体が 75%以上を占める．

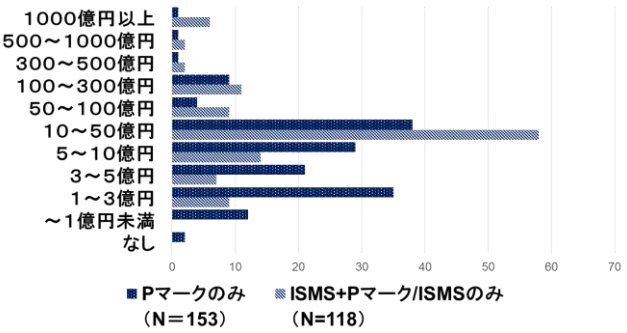

図 2　回答事業体の規模（売上・予算）と認証（N=367）

次に，取得している認証について調べたところ，P マークを取得している事業体は 269 件で企業である．153 件は P マークのみ取得している企業（以下，P マークのみ取得企業）である．116 件は ISMS も併せて取得している企業（以下，ISMS+P マーク取得企業）である．ISMS のみ取得しているのは，2 件の大学であった．P マークのみ取得企業は比較的小規模であった．

3.3 サプライチェーンにおける情報セキュリティ管理

回答事業体のサプライチェーンに関する情報セキュリティガバナンスについて，調べた結果を次に示す．

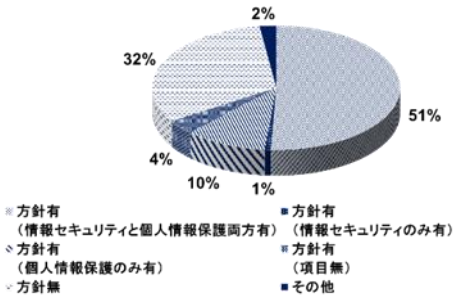

図 3　調達・購買方針と情報セキュリティの項目（N=367）

図 3 は，事業体の調達・購買方針に情報セキュリティの項目が含まれているかどうかを示したもので，半数以上の事業体は情報セキュリティと個人情報保護の双方の項目を記載している．どちらかしか記載していない事業体の場合は個人情報の記載が多い．

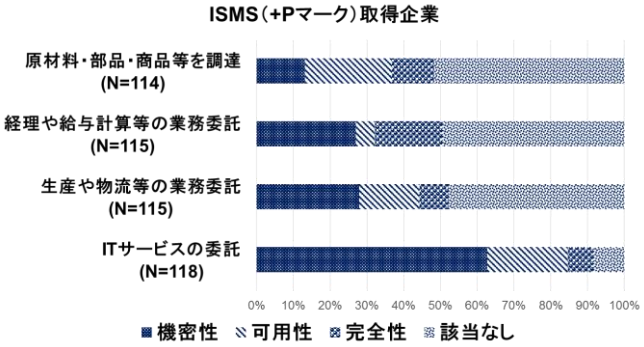

図 4　業務委託先に対する情報セキュリティリスク（ISMS（＋P マーク）取得企業）

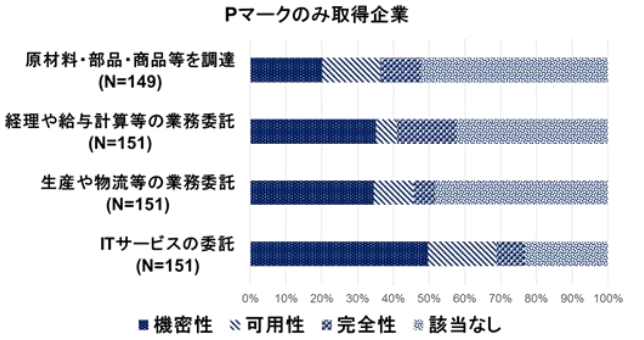

図 5　業務委託先に対する情報セキュリティリスク（P マークのみ取得企業）

図 4 および図 5 は業務委託先に対して重視する情報セキュリティリスクについて，ISMS 取得企業と P マークのみ取得企業に分けて示した．図 4 と図 5 からは業務委託の種類に関わらず機密性を重視する傾向がある．特に P マークのみ取得企業に顕著である．生産や物流などの業務委託や原料・部品・商品などの調達では可用性，経理や給与計算などの業務委託では完全性を重視していることが分かる．

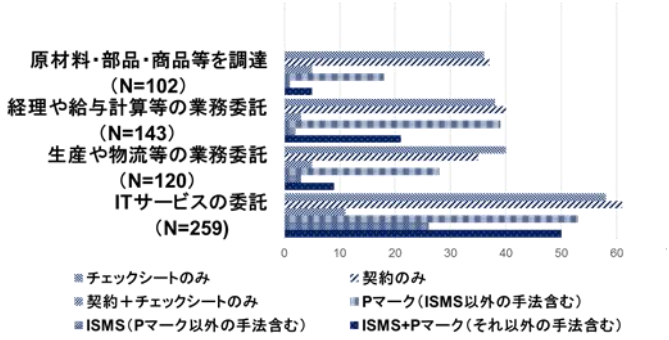

図 6　委託業務の種類と管理手法（委託の場合）

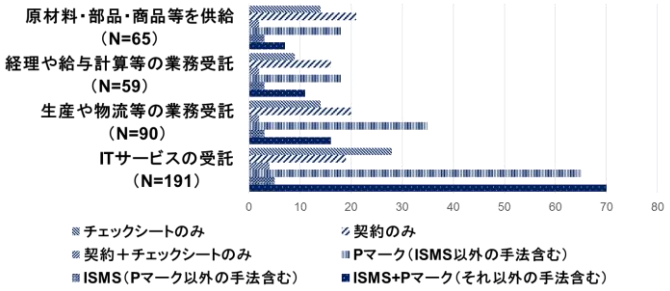

図 7　委託業務の種類と管理手法（受託の場合）

図 6 と図 7 は委託業務の種類によって管理手法が異なるかどうか，委託の場合と受託の場合で調べたものである．

図 6 からは，委託の場合は，チェックシートもしくは契約によって管理することが多く，次いで P マークも利用されることが多い．IT サービス以外の場合，ISMS の利用は少ない．一方，図 7 に示す受託の場合，ISMS＋P マークは IT サービスで最も多く要求されており，次いで P マークとなっている．また，その他の場合は P マークが多く利用されているおり，中小企業が多いことを考えると，板倉らの研究結果と同様の傾向を示している．

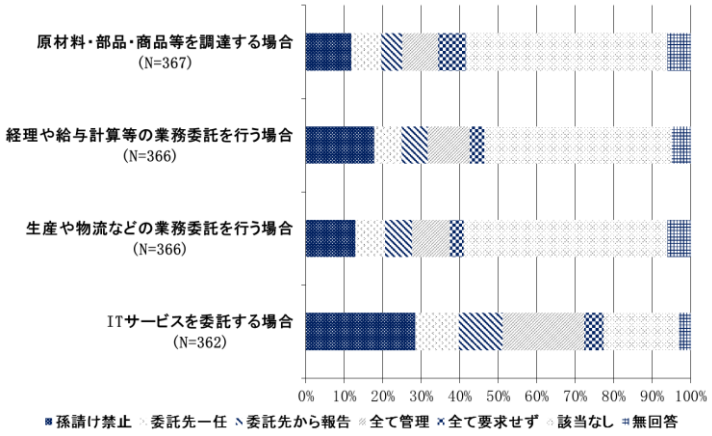

図 8　多段階の委託先管理

図 8 は多段階の委託先管理の状況を示す．図 8 からは，IT サービスの委託においては，孫請け禁止もしくは全て管理しているとの回答が多いが，その他の委託業務については委託先に任せている，また，報告をもらうとの回答も多く，どの委託業務でも，全て要求しないとの回答があった．

3.4 アンケート調査における考察

アンケート調査に回答した企業は，業務委託および調達について機密性のリスクを強く感じており，個人情報保護について関心が高いことが分かった．また，P マークは ISMS に比べ，規模の小さな企業で広く利用されていることが分かった．これは，安価に認証を取得し維持できることが理由だと考えられる．また，企業間の実際の取引においては，契約やチェックシートといった企業特有の条件を要求することが多いことが分かった．すなわち，多段階の取引には向いていない．

サプライチェーンは多段階に渡って取引が広がるが，今回の回答企業の多くはサプライチェーンについてのリスク認識が低いことが分かった．アンケートに回答を寄せた中小規模の企業では取引先の取引先までの管理を行うことは物理的，経済的に難しいかもしれない．

企業では，個人情報などの機密性を重視する中で，法的，経済的な観点から P マークを選択して，情報セキュリティ管理としている実態であることが分かった．しかし，企業が取引において企業固有の要求を優先している実態からは，企業の取引が国内だけにとどまっている間は大きな問題はないと考えられる．しかし，委託先や調達先が海外に広がる場合，すなわちグローバルなサプライチェーンの一部に組み込まれるときには，企業にとって，P マークや自社契約フォームによる情報セキュリティ管理は手法として十分ではなくなる．これには，グローバルな ISMS を活用する余地は大きい．

4. 有価証券報告書などの開示情報の分析

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することができると考えられる．

4.1 対象会社の抽出

本研究では下記に挙げる上場企業（以下，日系企業）を対象に調査を行った．

（1）TOPIX CORE30

流動性が高く時価総額の大きな，日本を代表する企業の株価指標である．別表 1 に示す東京証券取引所の運営する市場第一部（東証一部）の 30 社で構成される．

（2）JASDAQ

東京証券取引所が運営する市場の一つで，一定の事業規模と成長を有する企業群と特色のある技術やビジネスモデルをもって将来の成長性に富んだ企業群で構成されている．

Vol.2014-DCC-7 No.13
Vol.2014-EIP-64 No.13
2014/5/15

いわゆる中堅から中小企業を含み, 2013 年 12 月 31 日現在, 923 社が上場している.

（3）マザーズ

東京証券取引所が運営する市場の一つで，高い成長性を持ち，将来的に市場第一部にステップアップする可能性が高い企業で構成されている．中小の新興企業からなり，2014 年 12 月 31 日現在で，181 社が上場している.

4.2 調査方法

TOPIX CORE30 の各社については, 2012 年度の有価証券報告書 「事業等のリスク」[19]を対象とした.

また, 新興市場である JASDAQ およびマザーズについては, 一般的に事業におけるリスクが大きいため，投資家の信頼を得るには経営戦略の進捗状況やリスク情報等の継続的な情報開示が求められている．2013 年 12 月末時点で上場している企業の有価証券報告書もしくは届出書から一覧として抽出された，東京証券取引所が情報を公開・提供している「JASDAQ 上場会社のリスク情報一覧」[20] ，「マザーズ上場会社のリスク情報一覧」[21] を対象とした.

調査では，統一性の観点から有価証券報告書もしくは届出書のリスク情報に着目し，該当する開示情報の中に，表 1 に示す検索語を含む記述がある場合は，その企業がリスクを認識していると考えることにした．ここではリスクを認識している企業の数を調べた.

表 1　使用した検索語（日系企業）

情報セキュリティリスクに関する検索語
情報セキュリティ
個人情報，プライバシー
システム障害，システムダウン
（情報）漏えい，漏洩
機密情報
サイバー攻撃，サイバーテロ，サイバーアタック
不正アクセス
ハッカー，ハッキング
（コンピューター）ウィルス
マルウェア
サプライチェーンリスクに関する検索語
供給，サプライ
調達
業務委託

4.3 日系企業の調査結果

図 9 には情報セキュリティににについて開示情報などに記載している企業の全体に対する比率を示す.

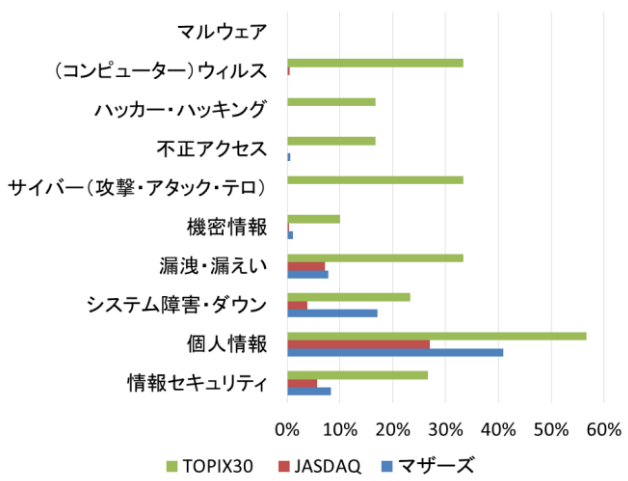

図 9　情報セキュリティリスク記載の日系企業の比率

図 10 には, 同様にサプライチェーンに関するリスクを記載していた企業の全体に対する比率を示す.

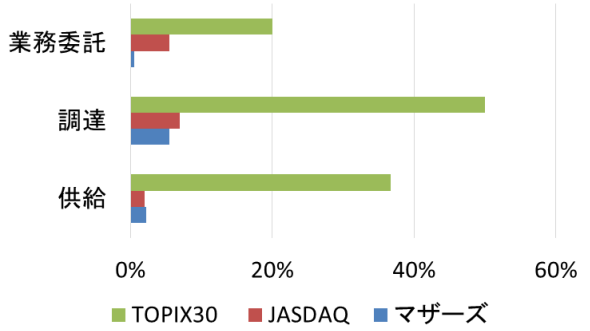

図 10　サプライチェーンリスク記載の日系企業の比率

図 9 と図 10 からは，TOPIX30 に属する大企業は情報セキュリティ，サプライチェーンともにリスク認識が高いことが分かる．情報セキュリティリスクの中では，大企業，中小企業ともに個人情報に関する認識が高い．また，中小企業については外部からの攻撃に対するリスク認識が低い．ただし，マルウェアに対しては企業規模に関わらず記載されていないことが分かった.

4.4 米系企業の調査結果

TOPIX CORE30 に相当するアメリカの大企業として，代表的な株式指標である DOW JONES INDUSTRIAL AVERAGE を構成する 30 社（以下，米系企業）を対象に，アメリカ証券取引委員会の定める年次財務報告書 10K から ITEM1A：Risk factors[22]を対象として 4.3 と同様の比較を行った．その際に利用した検索語を表 2, 対象の企業を別表 2 に示す.

表 2　使用した検索語（米系企業）

情報セキュリティリスクに関する検索語
Information security (Information technology, cyber)

Privacy, Personal information
Disruption, System failure
Breach
Confidential information
Cyber attack, Cyberattack
Unauthorized access
Hack
Computer virus
Malicious, Malware
サプライチェーンリスクに関する検索語
Supply Chain
Purchase
Outsource, Outsourcing

結果を，図 11，図 12 に示す．

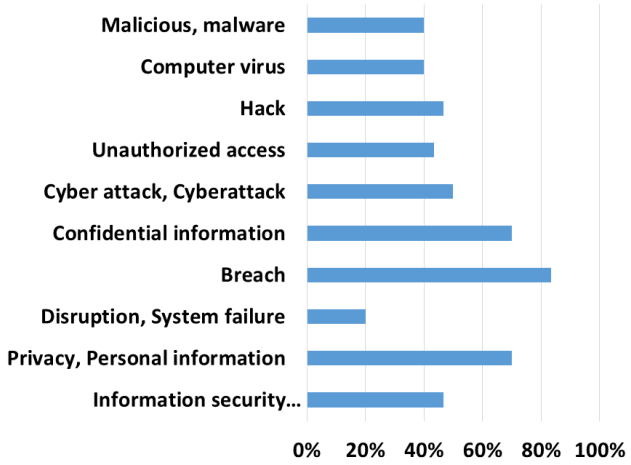

図 11　情報セキュリティリスク記載の米系企業の比率

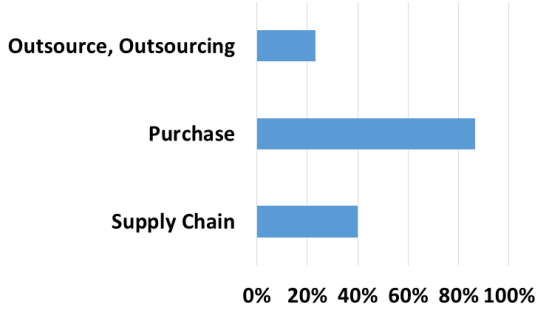

図 12　サプライチェーンリスク記載の米系企業の比率

図 11 と 12 からは，日系企業と米系企業について関連語として定義していないため，直接比較することは難しいが，全般の傾向として，情報セキュリティリスクの認識が高いことが分かる．中でも，個人情報や機密情報といったリスクの認識が高い．また，サプライチェーンリスクに関しても認識が高い．一方，サイバー攻撃等，外部からの脅威についても認識は高いが，悪意のあるプログラムに関するリスク認識については日系企業と米系企業で大きく異なっている．

なお，米系企業の調査で用いた用語“Breach”は情報セキュリティ以外についても使われており，記載数が多い．システム障害に関しては，様々な表現がとられており，“Disruption, system failure”だけでは十分に抽出できなかった可能性がある．

4.5　CSR の観点から見たサプライチェーン管理

エンロンなどの企業不正が相次いだ後，企業の社会的な責任（以下，CSR）が問われ，永続的な発展に向けて努力する姿勢を企業がステークホルダーに対して説明を行うようになった．国連は 2004 年に人権，労働，環境，腐敗防止について 10 の原則を示し，企業が持つべき責任をグローバルコンパクトとしてまとめた．また，2010 年には ISO26000 が策定された．

年次で発行される CSR 報告は企業自体が果たすべき責任に加え，調達や委託といったサプライチェーンに参加する取引先についても要求する内容を述べることがある．また，多くの企業は調達を行う際のガイドライン，例えば調達方針の中で，取引先に要求する項目を示している．情報セキュリティはコンプライアンスやサービス品質の一つとして考えられ，CSR 報告や調達方針の中で，取引先への要求事項に含まれていることも多い．

開示情報の一つとして，TOPIX30 の企業を対象に，CSR 報告書[23]，調達方針[24]の中でサプライチェーンにおける情報セキュリティの記述を通して，リスク認識と管理手法について調査を行った．

図 13 は 30 社の対象企業のうち，情報セキュリティ関連の記述を行った企業の比率を示している．

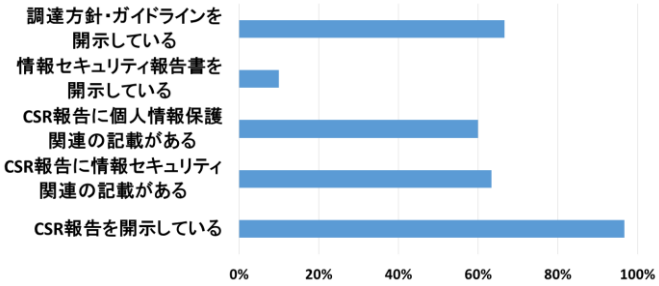

図 13　CSR，調達方針において情報セキュリティに関する記述をしている TOPIX30 企業の比率

調査対象の TOPIX 企業のうち 29 社と，ほぼすべての企業が CSR 報告を開示している．図 13 から，半数以上の企業は CSR 報告書に情報セキュリティ，個人情報保護の項目がある．一方，情報セキュリティの状況を説明した情報セキュリティ報告書については，30 社のうち日立製作所のみ，キヤノン，NTT の関連会社を含めて 3 社が開示しているに過ぎない．また，CSR 報告書以外に，調達方針については製造業を中心に開示していることが多い．

Vol.2014-DCC-7 No.13
Vol.2014-EIP-64 No.13
2014/5/15

図 14 には，調達方針に記載されている，取引先に対する CSR に関連する要求項目を示す．

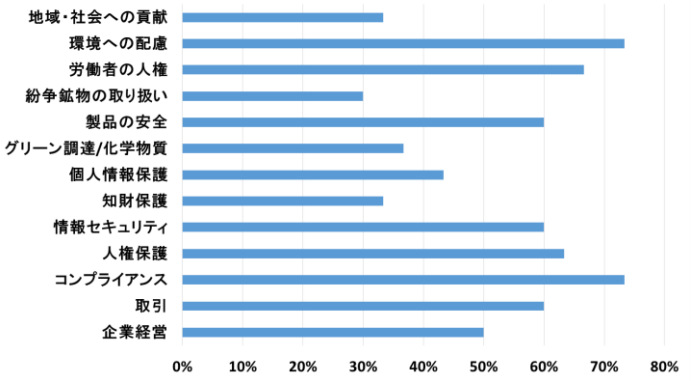

図 14　CSR の主要な項目を調達方針の中で取引先に要求している TOPIX30 企業の比率

図 14 からは，調達方針の開示が 7 割の企業であることから，コンプライアンスと環境に関する項目については，すべての企業が記載していると言えよう．情報セキュリティについては機密情報の保護に関する記述が多く見られる．一方で，個人情報保護についてはコンプライアンスもしくは情報セキュリティに含まれるためか，開示企業の 6 割程度に留まっている．

なお，取引先の取引先まで情報セキュリティ管理を要求していた企業は，トヨタ，NTT，NTT ドコモ，ソフトバンクの 4 社であった．

4.6 開示情報の分析における考察

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．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．

また，日系企業の情報開示は，米系企業に比べ少ない．また，外部からの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．

調達先に機密性を中心とした情報セキュリティ管理を要求する企業は多い．しかし，実効性のある管理手法とあわせた要求かどうかは，詳細を研究する必要がある．

5. まとめ

アンケート調査と開示情報の分析結果から考えると，中小企業は大企業に比べ情報セキュリティやサプライチェーンに関するリスク認識は低い．また，多くの企業は機密性を重視し P マークのように個人情報保護の仕組みを情報セキュリティ管理の手法として利用している．調達先の管理は国際標準を利用する場合が少なく，企業ごとに独自で実施しているといえる．しかし，グローバルなサプライチェーンの広がりを考えると，国際標準を利用して管理を行うことで，調達先の多角化や管理の効率化，製品やサービスの信頼性の担保につなげられる可能性も高いと考える．また，中小企業が導入しやすい仕組みづくり，アメリカにおける政府機関がクラウド事業者を認証する FedRAMP[25]や日本の地方銀行のように共同でシステム基盤を利用するなど，業界団体での標準化の推進や，調達先の組織化などの手法も検討の余地がある．

6. 今後の研究

開示情報の分析については，さらに ISMS や P マークの取得状況を確認するとともに，個々の企業の管理手法について調査を行う．

また，情報セキュリティガバナンスの国際標準である ISO/IEC27014[26]，サプライチェーンの ISO/IEC27036 の分析，NIST や ENISA の提案するガイドラインの分析を行うことで，本稿におけるアンケート調査や開示情報の分析から得られた知見とあわせてグローバルな企業活動における有効な管理手法の提案を行いたい．

謝辞　本研究に関するアンケート調査および開示情報の分析にご協力いただ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．また，アンケートのデータ入力に多大な協力を頂いた神奈川県内特別支援学校の皆様に感謝します．

別表

別表 1　TOPIX CORE30 対象会社
（2012 年 10 月 31 日時点）

社名	業種
日本たばこ産業株式会社	食料品
株式会社セブン＆アイ・ホールディングス	小売業
信越化学工業株式会社	化学
花王株式会社	化学
武田薬品工業株式会社	医薬品
アステラス製薬株式会社	医薬品
新日鐵住金株式会社	鉄鋼
株式会社小松製作所	機械
株式会社日立製作所	電気機器
株式会社東芝	電気機器
パナソニック株式会社	電気機器
ソニー株式会社	電気機器
ファナック株式会社	電気機器

日産自動車株式会社	輸送用機器
トヨタ自動車株式会社	輸送用機器
本田技研工業株式会社	輸送用機器
キヤノン株式会社	電気機器
三井物産株式会社	卸売業
三菱商事株式会社	卸売業
三菱 UFJ フィナンシャル・グループ	銀行業
三井住友フィナンシャルグループ	銀行業
みずほフィナンシャルグループ	銀行業
野村ホールディングス株式会社	証券，商品取引業
東京海上ホールディングス株式会社	保険業
三菱地所株式会社	不動産業
東日本旅客鉄道株式会社	鉄道
日本電信電話株式会社	情報・通信業
KDDI 株式会社	情報・通信業
株式会社エヌ・ティ・ティ・ドコモ	情報・通信業
ソフトバンク株式会社	情報・通信業

別表 2　DOW JONES INDUSTRIAL AVERAGE
（2014 年 3 月 2 日現在）

社名	業種
3M Co	Producer Manufacturing
American Express Co	Finance
AT&T Inc	Communications
Boeing Co	Electronic Technology
Caterpillar Inc	Producer Manufacturing
Chevron Corp	Energy Minerals
Cisco Systems Inc	Electronic Technology
E I du Pont de Nemours and Co	Process Industries
Exxon Mobil Corp	Energy Minerals
General Electric Co	Producer Manufacturing
Goldman Sachs Group Inc	Finance
Home Depot Inc	Retail Trade
Intel Corp	Electronic Technology
International Business Machines Co...	Technology Services
Johnson & Johnson	Health Technology
JPMorgan Chase and Co	Finance
McDonald's Corp	Consumer Services
Merck & Co Inc	Health Technology
Microsoft Corp	Technology Services
Nike Inc	Consumer Non-Durables
Pfizer Inc	Health Technology
Procter & Gamble Co	Consumer Durables
The Coca-Cola Co	Consumer Non-Durables
Travelers Companies Inc	Finance
United Technologies Corp	Producer Manufacturing
UnitedHealth Group Inc	Health Services
Verizon Communications Inc	Communications
Visa Inc	Finance
Wal-Mart Stores Inc	Retail Trade
Walt Disney Co	Consumer Services

参考文献

[1] 大塚哲洋他，日本型サプライチェーンをどう評価すべきか，みずほ総研論集 2011 年Ⅲ号，pp.1-9
[2] 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
[3] 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
[4] 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
[5] NIST，NISTIR7622，Notional Supply Chain Risk Management Practices for Federal Information Systems，2012 年 6 月，pp.1-15
[6] ENISA，An overview of the ICT supply chain risks and challenges, and vision for the way forward，pp.19-28
[7] ISO/IEC27036:2013 Information technology – Security techniques – Information security in supplier relationship
[8] Gary Gereffi , John Humphrey, Timothy Sturgeon, The governance of global value chains, Review of International Political Economy 12:1 February 2005, pp.78–104
[9] Khalid Nadvi, Global standards, global governance and the organization of global value chains, Journal of Economic Geography (2008) pp. 1–21
[10] Ila Manuj , John T. Mentzer, Global supply chain risk management strategies: International Journal of Physical Distribution & Logistics Management, Vol. 38 No. 3, 2008：pp. 192-223
[11] 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
[12] 原田 要之助， 情報セキュリティガバナンスと説明責任, InfoCom REVIEW　Vol.49，2009，20-36
[13] Krag Brotby, Information Security Governance, Willey, 2009
[14] Ed Gelbstein, Strengthening Information Security Governance: ISACA JOURNAL VOLUME 2, 2012
[15] 多田 哲, 情報セキュリティへの取り組みと企業の社会的責任, UNISYS TECHNOLOGY REVIEW 第 86 号，AUG. 2005, pp.153-164
[16] 林紘一郎，企業と情報セキュリティガバナンス，セキュリティ経営，2011 年 12 月，79-109
[17] 板倉 征男 , 松田 治男 , 鈴子 学 ,P マーク審査から見た中堅企業の情報セキュリティ・ガバナンス (情報セキュリティ), 情報処理学会研究報告. CSEC, [コンピュータセキュリティ]
[18] 久保知裕，原田要之助，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
[19] 別表 1 に示す企業の 2012 年度有価証券報告書
[20] JASDAQ 上場会社のリスク情報一覧_平成 25 年 12 月末現在, http://jasdaq.tse.or.jp/jasdaq/6014　（2014 年 1 月 10 日閲覧）
[21] マザーズ上場会社のリスク情報一覧_20131231 現在.xls, http://mothers.tse.or.jp/listed_companies/risk_info.html,（2014 年 1 月 10 日閲覧）
[22] 別表 2 に示す企業の 2013 年度 SEC filling 10K (Home Depot, Walmart は 2012 年度)
[23] 別表 1 に示す企業の 2013 年度 CSR 報告，サステナビリティ報告
[24] 別表 1 に示す企業の調達方針，CSR サプライチェーン推進ガイドライン, サプライヤー行動規範（2014 年 3 月 21 日~23 日閲覧）
[25] About FedRAMP　2013 年 12 月 2 日閲覧 http://www.gsa.gov/portal/category/102375
[26] ISO/IEC27014:2013 Information technology -- Security techniques -- Governance of Information Security