Vol.2014-EIP-63 No.12
2014/2/21

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

久保知裕[†1]　原田要之助[†2]

情報セキュリティ大学院大学原田研究室において実施した情報セキュリティアンケート調査の回答結果から，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の動向を分析した．また，経済産業省等が提供している外部委託時の情報セキュリティ管理に関するガイドラインの利用状況についても調査した．
この調査結果を通して，サプライチェーンの視点からは，国内では独自のセキュリティ管理の考え方が主流であり，海外と相互認証が行える国際的な管理手法が浸透していないことがわかった．サプライチェーンのグローバル展開を考えると，独自基準は貿易障壁になり日本企業の競争力を阻害する可能性がある．

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

TOMOHIRO KUBO[†1]　YONOSUKE HARADA[†2]

Questionnaire survey of information security, executed by Harada lab of IISEC, has provided level of risk recognition and trend of management methodology in supply chain incl. outsourcing as service supply chain. And, the present situation of utilizing the guidelines for information security management published by METI or other authorities has been surveyed.
In this study, it is recognized from the viewpoint of supply chain, that international standards of information security management, enabling to authorize multi-nationally, has not become prevalent in Japan, as domestic or corporates' own standards are more popular. In considering about global expansion of supply chain, unique standards may become trade barrier and impede competitiveness of Japanese companies.

1. はじめに

企業のビジネスモデルは，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のモデルから，自社の得意とする機能を選択集中するモデルに移りつつある[1]．競争力のある外部の機能と自社の得意な機能を組み合わせることで，競争力を高めている．サプライチェーンを例にとると，系列に代表される一社を頂点にしたピラミッド型から，系列を超えて取引を行うメッシュ型や，勝ち残った企業に取引が集中したりするダイヤモンド型等，より複雑化する方向へ変わってきている[2].
また，日本企業の事業活動は，停滞する国内市場から海外市場へ軸足を移しつつある．販売先としての海外だけでなく，原材料・部品・商品の調達，生産や物流，経理や給与計算といった事務作業，ソフトウェア開発やデータセンター運用などの様々な分野で，海外企業との連携や業務の委託が行われるようになっている．
これらの事業活動における情報の伝達や業務処理を支えるのが，IT 基盤である．事業活動のグローバル化や外部との連携を行う上で，インターネットなどの通信ネットワークの活用や IT 基盤の共同利用など IT 利用のモデルも進化してきているが，IT への依存が高まることで，情報セキュリティリスクも高まっている．
IT の効果的な活用，適切な情報セキュリティの維持改善を行う上で，ガバナンスモデルの構築，運用は重要である．しかし，海外を含む企業外部組織との連携を意識した仕組み作りは十分ではないと考えられる．

本研究では，原材料や商品だけでなく，ICT などサービスも含めた他企業との連携を広義のサプライチェーンとしてとらえ，今回は ISMS もしくはプライバシーマーク（以下，P マーク）を取得した企業，大学，官公庁へのアンケートによる現状調査を通して，課題の洗い出しを行った．

2. ガバナンスと認証制度

本稿におけるガバナンス及び認証制度を下記のとおり定義した．

2.1 ガバナンス

企業は営利を目的にして経済活動を行う組織である．2004 年に改訂された OECD の Principles of Corporate Governance[3]によれば，コーポレートガバナンスは，市場ルールや法的な制約の中で企業が経済的な価値創造活動を持続させるための枠組みとプロセスを指す．企業は個々の

†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

独立した組織として経済的な価値を生み出す能力を最大化するために，コーポレートガバナンスの能力を進化させてきた．

企業活動において，情報システムは業務を支援し意思決定を助けるインフラストラクチャであり，業務と不可分である．IT Governance Institute (ITGI) が PWC に託して 2010 年に行った調査[4]では，CEO や CIO など企業経営者の 94%が IT は事業戦略やビジョンの実現のために重要もしくは大変重要だと認識し，特に IT 投資による事業価値の創造，事業戦略の支援に貢献していると考えている．

2013 年 6 月 14 日に閣議決定された第二次安倍内閣による「世界最先端 IT 国家創造宣言」[5]の中では，目指すべき社会・姿を実現する取り組みの中で政府による IT ガバナンスの強化を挙げ，戦略的な IT 投資管理，IT 人材育成を進めるとしている．

IT ガバナンスは組織が IT を有効に活用して価値創造を行うためのフレームワークである．COBIT5[6]によれば，“情報と関連技術が，事業体の戦略と目標達成をサポートし，確実に実現できるようにするための，ガバナンスの観点．IT 能力が効率的および効果的に提供されるようにすることなどの，機能的 IT ガバナンスも含まれる”と定義している．また，原田によれば、企業に求められる IT ガバナンスの新しいモデル[7]では，価値創造という攻めの目的に加え，価値保全という守りの目的もあるとしてリスク管理の最適化プロセスを提案している．

攻めのモデルを IT ガバナンス，守りのモデルを情報セキュリティガバナンスとしてとらえ，本稿では ISO/IEC 38500 を参照して作成された JIS 案[8] および ISO/IEC27014 の JIS 案[9]を元に次のように定義した．

IT ガバナンスは情報を取得，加工，保存及び普及するために必要な資源（IT）を対象とし，組織における利用を指示，管理する仕組みを指す．すなわち，IT 戦略を実現化するための制度やプロセスを管理する仕組みや組織能力のことである．（ISO/IEC38500：2008）

情報セキュリティガバナンスは情報の機密性，完全性，可用性を対象とし，組織の情報セキュリティ活動を指導し管理する仕組みのことを言う．法令，規制，契約を順守しながら情報セキュリティの目的と戦略を事業の目的及び戦略と整合性を取っていかなければならない．（ISO/IEC27014：2013）

2.2 認証制度

今回実施したアンケートでは，回答対象として，大学および官公庁と並び，代表的な情報セキュリティの認証である ISMS もしくは P マークを取得している企業から抽出している．データ分類の属性の一つとして利用することから，代表的な特徴について表 1 のとおり整理しておく．

表 1　ISMS と P マーク†3

制　度	ISO27001／ISMS	プライバシーマーク
規　格	国際標準規格 ISO/IEC27001:2013 日本工業規格 JISQ27001:2014	日本工業規格 JISQ15001:2006
対　象	適用範囲内の全ての情報 （ハードやソフト、個人情報も含まれる）	企業内のすべての個人情報 （従業員の個人情報も含まれる）
	事業所単位、部門単位、事業単位も可	企業全体
要　求	情報の機密性・完全性・可用性の維持 （情報資産の重要性、リスクに応じた適切な情報セキュリティ）	適切な個人情報の取り扱い（個人情報の取得、利用、共同利用、委託、提供、安全管理（情報セキュリティ）、開示等要求対応、苦情対応など）
更　新	3年毎、および、毎年の継続審査	2年毎
相互認証	IAF加盟の数十カ国の認定機関間で相互認証	・中国・大連市のソフトウェア産業協会「PIPA制度」と相互認証（2008年6月より） ・韓国情報通信産業協会
セキュリティ対策	133項目の詳細管理策	合理的な安全対策
費用 （取得＋三年間の維持更新）	381万円 （想定：社員30名程度、Webサイト数1、部門数4 全社をISMS認証範囲として取得を想定した場合の金額）	105万円 （右と同様の企業規模：従業員数6～100名、資本金5000万円以下、サービス業）
取得費用	172万円	60万円
維持更新費用	維持審査　48万円/年 更新審査　65万円/3年	付与登録審査　45万円/2年

ISMS は，個別の問題毎の技術対策の他に，組織のマネジメントとして，自らのリスクアセスメントにより 必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを運用する．組織が保護すべき情報について，機密性，完全性，可用性をバランス良く維持し改善することが 情報セキュリティマネジメントシステム(ISMS)の基本コンセプトである[10].

一方，P マーク（プライバシーマーク）制度は，日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して，個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して，その旨を示すプライバシーマークを付与し，事業活動に関してプライバシーマークの使用を認める制度である[11].

代表的な相違点を次に挙げる．

ISMS は ISO/IEC27001 に基づいた国際規格であるが，P マークは JISQ15001 に基づく国内規格である．そのため，ISMS は IAF(International Accreditation Forum：国際認定機関フォーラム)に加盟する 62 か国の認証機関と相互認証が可能であるが，P マークは，事務作業のアウトソーシング先として利用される大連など 2 機関のみと相互認証できるにすぎない．

また，ISMS がハードウェア，ソフトウェア，データなどを含む組織内の特定な事業（範囲）における情報資産全般を対象とし，情報の機密性，完全性，可用性を要求するものであるのに対し，P マークは全社の個人情報を対象とし，利用者の同意や安全管理等を要求するものである．

取得および維持の費用も異なる．表 1 の費用を用いて試算

†3 参照情報
下記 WEB サイト　2013 年 11 月 25 日閲覧
ISMS と P マーク比較　oficeta.com
http://www.pangkal.com/isms/index2.html
プライバシーマーク制度　相互認証
http://privacymark.jp/links/index_sougo.html
ISIM 取得・維持費用　アーチ株式会社
http://privacymark.co.jp/isms_get/index.html
P マーク取得・維持費用　アーチ株式会社
http://privacymark.co.jp/privacymark_get/index_1.html
http://privacymark.co.jp/privacymark_update/index_1.html

すると，社員数 30 名程度で WEB サイト数 1，部門数 4 の企業が全社を対象にした ISMS を取得，三年間維持する費用は 381 万円と推定される．一方，同規模の企業，P マークの分類で従業員 6 から 100 名程度で資本金 5000 万円以下のサービス業が P マークを取得, 三年間維持する費用は 105 万円となり，おおよそ四倍近い費用差となる．

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

3.2 本稿に関する調査内容（質問）

本稿に関連する質問について表 2 に示す．

表 2　情報セキュリティのガバナンス設問

[Q26]	顧客の立場として，購買方針や調達方針（IT 委託，業務委託を含む）が策定されていますか．策定されている場合，個人情報保護および情報セキュリティに関する項目が含まれていますか．
[Q27]	顧客の立場として委託先・調達先を選定する際，情報セキュリティの観点から最も重要な項目はどれですか．
[Q28]	顧客の立場として委託先を選定する際に，情報セキュリティのリスク対応として要求している事項はどれですか．
[Q30]	受託者・供給者の立場として，顧客から情報セキュリティのリスク対応を要求されていますか．
[Q32]	外部との委託先・調達先に対する情報セキュリティガバナンスに関する下記のガイドライン，ツールについてご存知ですか．

4. 調査結果

4.1 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（売上規模），図 3 に事業規模と取得している認証の状況を示す．

図 1 では，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．

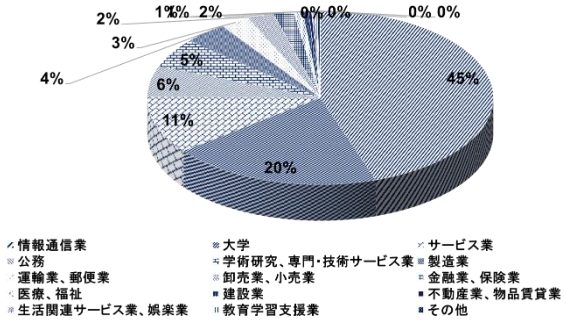

図 1　回答事業体の業種（N=367）

図 2 の事業規模（企業は売上，大学と官公庁は予算）では，10 億円以上 50 億円未満が 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．

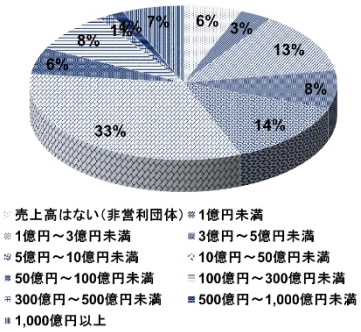

図 2　回答事業体の規模（売上規模）（N=367）

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 件で全て企業である．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．図 3 から，ISMS+P マーク取得企業，P マークのみ取得企業のどちらも 10 億円以上 50 億円未満が最も多い．また，P マークのみ取得企業は約 8 割の企業が 1 億円以上 50 億円未満の範囲に属し，ISMS+P マーク取得企業では約 8 割が 5 億円以上 300 億円未満の範囲に属している．すなわち，P マークのみ取得企業の方が小規模である．

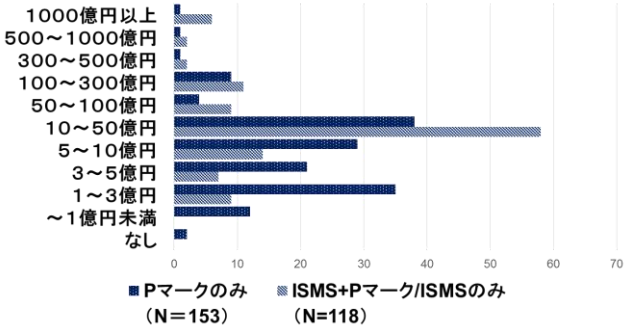

図 3　事業規模と取得認証

4.2 業務委託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のセキュリティガバナンスについて，図 4 に調達・購買方針と情報セキュリティの関係（Q26），図 5 と図 6 に業務委託先に対する情報セキュリティリスクの認識度（Q27），図 7 と図 8 に委託・受託業務の種類と管理手法（Q28 と Q30），図 9 にガイドラインの認知度を示す（Q32）.

図 4 から，個人情報保護と情報セキュリティ，両方の項目を含めている企業は半数を超えている．また，個人情報保護の項目は情報セキュリティの項目よりも考慮されている.

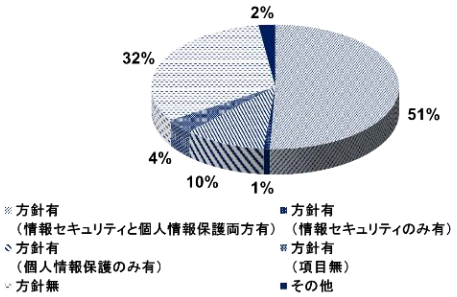

図 4　調達・購買方針と情報セキュリティの項目（N=367）

図 5 と図 6 では，業務委託の種類を IT サービス，生産や物流等，経理や給与計算等，原材料・部品・商品の調達の四つに分け，それぞれについて機密性，可用性，完全性のどれを重要視するかの回答を示した．図 5 は ISMS+P マーク取得企業を対象，図 6 は P マークのみ取得企業を対象としている．ISMS+P マーク取得企業の原材料・部品・商品の調達を除き，他全てについて機密性が重視されている．その傾向は P マークのみ取得企業で顕著である．また，二番目に多い項目を見ると，業務によって異なり，IT サービス，生産・物流等の委託，原材料・部品・商品の調達では可用性，経理・給与計算では完全性が重視されている.

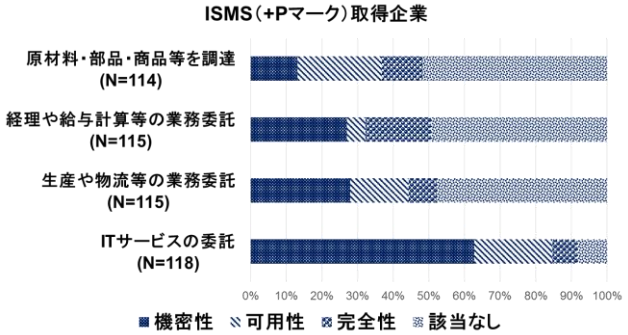

図 5　業務委託先に対する情報セキュリティリスク
ISMS(+P マーク)取得企業

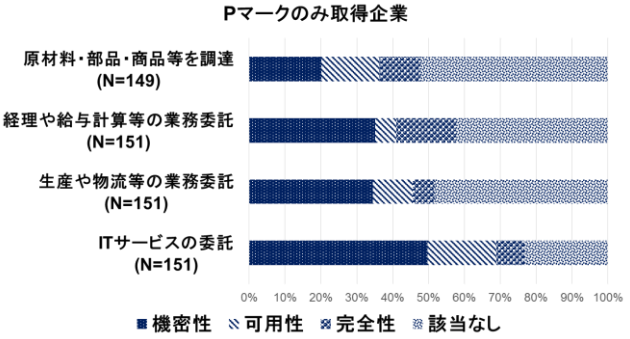

図 6　業務委託先に対する情報セキュリティリスク
P マークのみ取得企業

図 7 と図 8 は，図 5 と図 6 同様に調査した.

業務委託における要求事項は契約のみ，チェックシートのみが，どの業務においても多かった．また，第三者認証としては P マークを利用することが多い. IT サービスの場合，ISMS が利用されているが，P マークとの組み合わせで使われていることも多い.

IT サービスの受託時には，ISMS と P マークに契約やチェックシートを組み合わせる手法，P マークに契約やチェックシートを組み合わせる手法が多いと考えられる．それ以外の業務受託については P マークもしくは契約のみとの回答が多い．また，可用性を重視する生産や物流等の受託でも P マークを利用する回答が多かった.

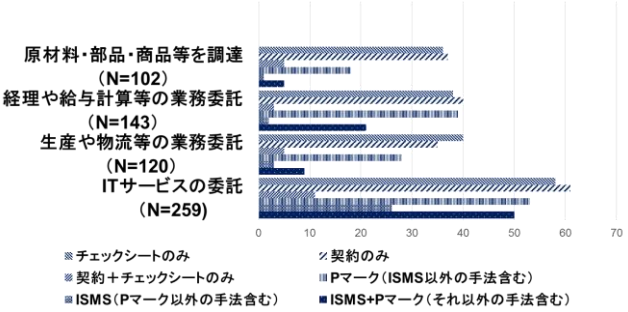

図 7　委託業務の種類と管理手法（委託の場合）

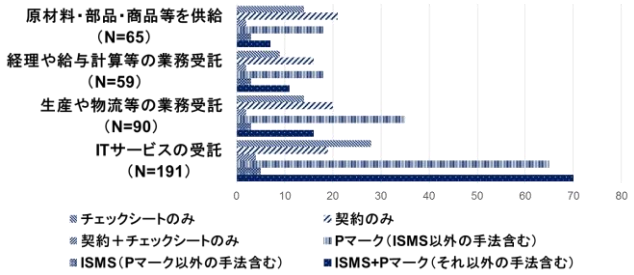

図 8　受託業務の種類と管理手法（受託の場合）

図 9 では，外部委託における経産省等のガイドラインは回答者の 10%前後にしか利用されていない．また，名前しか知らないという回答を含めてもほぼ半数であり，認知度は低い．JASA の提供しているガイドラインは最も認知度が低かった．

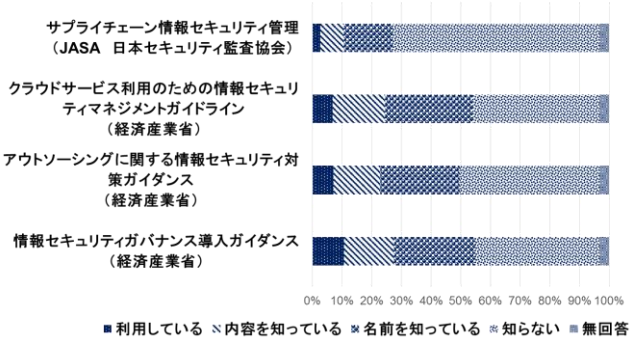

図 9　ガイドラインの認知度（N=367）

5. 考察

5.1 第三者認証の取得と事業体規模

アンケート調査の結果から考えると，第三者認証についてはコストが大きな要素だと考えられる．ISMS の取得・維持費用と P マークの取得・維持費用では，四倍近い開きがある．売上規模の小さな企業にとって ISMS は費用負担が大きい．また，個人情報保護法の存在や，図 4 に示したように購買・調達においても個人情報を重視する傾向があること，図 5 と図 6 で示したように，どんな場合も機密性を重視する傾向があることから，P マークは広範に利用され，特に小規模企業では P マークのみの認証で十分だと考えている可能性がある．

5.2 業務の外部委託に関する情報セキュリティのリスク意識と管理手法

先述のとおり，情報セキュリティリスクについては機密性を重視する傾向がある．IT サービスに関しては，漏えいだけでなくシステム運営の委託なども含まれることから機密性に次いで可用性が重視されている．生産・物流や原材料・部品・商品の調達でも機密性に次いで可用性が重視され，また，給与計算や経理においては完全性が重視されている．これは，システムの停止が操業に与える影響が大きい，また，不完全なデータが業務の混乱を引き起こすためだと考えられる

ISMS+P マーク取得企業と P マークのみ取得企業による傾向の差を見ると，P マーク取得企業のほうがどの業務においても機密性を重視する傾向が強く，ISMS 取得企業は機密性，可用性，完全性の強弱がはっきりしている．個人情報保護を目的とする P マークを運用する企業では機密性に視点が向きやすく，ISMS を運用する企業では他の要素とのバランスを要求されることから傾向に違いがあると考えられる．

委託時と受託時に分けて管理手法の傾向を分析すると，IT サービス受託時の顧客からの要求事項として ISMS+P マークが多かった場合を除き，ISMS を要求されることは少なく，ISMS 以外の管理手法が用いられている．全般には国内独自規格である P マーク，委託時には企業独自の要求を反映する契約，チェックシートが多いことから，ISMS のように国際的に標準化された管理施策が十分に活用されていないと考えられる．

5.3 業務の外部委託に関する情報セキュリティのガイドライン

図 9 に示した通り，経済産業省等から情報セキュリティガバナンスやサプライチェーン，アウトソーシングに関する管理手法についてガイドラインが提供されているが，利用は少ない．内容の認知自体も少ないことを考えると，普及のための啓発活動が足りず，企業での活用を考えて作成されたのか疑問がある．

6. リスクと管理施策の変化

6.1 サプライチェーンリスク

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といえる．

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，サプライチェーン自体に影響を与える．例えば，東日本大震災では，停電による電力供給の途絶などにより，情報システムが停止することで業務が停止するリスクが顕在化した．また，誤った不完全な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作動してしまうリスクもある．サプライチェーンの複雑化により，リスクの所在が見えにくくなっている．

IBM が 2009 年に行った Global Chief Supply Chain Officer Study[12]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の認識の高ま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．
PRMT によれば，2010 年に行った同様の調査[13]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ーと連携したリスク管理の必要性を述べている．

6.2 ガバナンスおよびリスク管理施策の変化

アンケートでは，どのような管理施策が実際にとられているかを調査した．ここでは日本および海外においてどのようなモデルが検討されているかを調査した．
まず，日本においては経済産業省が，2011 年 2 月に情報セキュリティガバナンスの導入ガイダンス補足編として「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」[14]を提案している．その一項目であるサプライチェーンでは，参加企業は共通の目的意識のもとで，必要な情報セキュリティ対策を実施し，グループ全体のリスクを下げる取組が求められる．サプライチェーンに情報セキュリティガバナンスを確立することが重要であると述べる一方で，各社が意識を一つにして情報セキュリティ対策に臨むには状況に差がある各社のために，リーダー企業が何らかの働きかけをしなければならないと述べている．
また，平成 23 年に発表された「サイバーセキュリティと経済研究会の中間報告」[15]においてもサプライチェーンセキュリティの重要性に触れられ，続いて，経済産業省の委託事業として日本セキュリティ監査協会（JASA）が「サプライチェーン情報セキュリティ管理ガイド」[16]を策定した．このガイドでは，委託元と委託先（再委託先含む）の行うべきことが示されている．委託元はサプライヤーの採用基準として情報セキュリティ管理基準を公表し，それに準拠しているか，適切に管理できているかを確認する．一方で，委託先は管理基準を適用し，適切に運用を行っていることを示す．また，中立である情報セキュリティ運営機関がサプライチェーン情報セキュリティポータルを設置運用し，委託先，委託元双方が情報を共有できる仕組みを提案している．
ここ数年で様々な施策が打ち出されていることから，サプライチェーンの急激な進展やそれに伴うリスクの変化を後追いしているといえる．
海外におけるモデルや施策についても調査を行った．米国では NIST の発表した NISTIR7622：National Supply Chain Risk Management Practices for Federal Information Systems[17]の中で，サプライチェーンへの攻撃はチェーン全体のすべてのプロセス，コンピューターシステムのハードウェア，ソフトウェア，サービスについて行われ，重要なデータや技術を盗み出したり，システムを破壊して重要な業務を停止させたりすることでサプライチェーンを攻撃すると述べている．防衛策として，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．
欧州では, ENISA が 2012 年に An overview of the ICT supply chain risks and challenges, and vision for the way forward[18]を発表した．ここでは，７つの挑戦課題として，下記を挙げている．

- グローバルに分散したサプライチェーン（人，プロセス，技術）の複雑性
- ICT サプライチェーンに共通したガイドラインの欠如
- 統計的に信頼できるレベルを測定し, IT エコシステム全体を通して整合性を認証するツール，プロセス，コントロールの欠如
- エンドユーザに提供されるシステムに対する製品評価の手法と技術の欠如
- システムへの偽造や偽装による侵入を検知打破でき幅広く適用できるツール，テクニック，プロセスの欠如
- 生産から利用に至る様々な製品に対して整合性を担保するような協同的アプローチの欠如
- ICT の様々な分野をまたがる互換性の高い整合性の要求欠如

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が提唱されている．
また，国際標準の動向として，情報セキュリティでは ISO/IEC27002 2013 が，冗長化等，可用性を重視することと，サプライヤーに関連する事項をまとめるなど，管理施策の見直しが行われた．
ISO/IEC27017 と ISO/IEC27036 がサプライヤーやアウトソーサー，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 が制定されている．

7. まとめ

アンケート調査においては情報セキュリティに対する意識の比較的高い中小企業を中心に情報セキュリティのガバナンスに関する回答を得ることができた．
これらの企業において，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，管理手法に関するガイドラインの普及施策が弱いことが挙げられる．
しかし，企業活動の観点から考えると，サプライチェーンはグローバルに広がり，構造は複雑になっている．
現在，国際的な課題となっている TPP 等，域内貿易，国際

貿易の自由化を進めるためにはモノやサービスの貿易障壁の除去が必要となる．標準は重要な要素の一つであり，国ごとに異なる標準は非関税障壁にあたる．ウルグアイラウンドのテーマでもあり，標準の世界的統一を進めることは1995年にWTO/TBT協定（貿易の技術的障害に関する協定）[19]で合意された．この協定では，WTO各国は内外無差別原則や手続きの公開が求められている．ISOとの整合性や認証制度における国際標準の採用が求められており，相互承認の推進を通して，各国ごとの独自基準や標準，それに基づく認証制度の制定や運用が貿易障壁にならないようにしなければならない．2010年版通商白書[20]においては“科学技術の進歩に伴うモジュール化，デジタル化，ネットワーク化の進展等により，国際市場での製品等の展開において優位なポジションを獲得・維持するための手段として国際標準の重要性はますます高まっている”と述べられている．

ISMSはISO/IEC27000シリーズとして国際的な情報セキュリティ管理標準であり，各国間で相互認証が図れるにもかかわらず活用が十分ではない状況が続くと，グローバルなサプライチェーンを活用した事業機会や効率化機会を失うか，情報セキュリティリスクを管理できないかもしれない．情報セキュリティの標準化において，ガラパゴス化による競争力喪失が起こってしまうと言えるかもしれない．

TPPのような貿易協定が議論される中で，日本の競争優位を確立するためには，認証制度のあるべき姿や展開戦略を策定，実践することが必要である．

8. 今後の研究

本稿では，日本の中小企業を中心にしたアンケート調査の結果を示した．

今後は，アンケート対象に含まれていないと考えられる日本の大企業，例えばTOPIXの指標企業について，有価証券報告書や情報セキュリティ報告書等の開示情報から，サプライチェーンにおける情報セキュリティリスクや管理手法の調査を行う．同様に，比較対象として海外の大企業，例えばダウ30，ユーロネクスト，FTSE，香港ハンセン等の指標企業について開示情報を利用して調査を行う．

さらに，サプライチェーンにおける国内及び海外の認証制度や情報セキュリティ標準の動向について文献と資料による調査を行い，企業の動向と比較する．

これらの調査を通して，外部と連携したビジネスモデルにおける情報セキュリティ管理の課題を確認，分析し，国際標準の動向を踏まえた施策の提言につなげたい．

謝辞 本研究の指導を頂いている情報セキュリティ大学院大学の原田教授，アンケート調査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する．

参考文献

1) ジェイ B, バーニー，企業戦略論（Gaining and Sustaining Competitive Edge）基本編, ダイヤモンド社, 2006年11月, pp.196-198
2) 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
3) OECD, Principles of Corporate Governance, 2004, p.12
4) IT Governance Institute，Global Status Report on the Governance of Enterprise It (Geit)−2011，pp.12-14
5) 高度情報通信ネットワーク社会推進戦略本部（IT戦略本部），世界最先端ＩＴ国家創造宣言, 2013年6月14日閣議決定, pp.19-20
6) ISACA，COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT 日本語版，p.103
7) 原田要之助, 企業に求められるITガバナンスの新しいモデル，InfoCom REVIEW Vol.47，2009，pp.1-15
8) 情報技術－ITのガバナンス　JIS Q38500：2014日本工業規格（案）
9) 情報技術－セキュリティ技術－情報セキュリティのガバナンス　JIS Q27014: 日本工業規格（案）
10) ISMS（情報セキュリティマネジメントシステム）とは，情報マネジメントシステム推進センター，2013年11月27日閲覧，http://www.isms.jipdec.or.jp/isms/index.html
11) プライバシーマーク制度，概要と目的，日本情報経済社会推進協議会（JIPDEC），2013年11月27日閲覧，http://privacymark.jp/privacy_mark/about/outline_and_purpose.html
12) 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
13) PRTM，グローバルサプライチェーントレンド　2010－2012，2010年，p.18
14) 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3月，pp.9-26
15) 経済産業省商務情報政策局情報セキュリティ政策室，サイバーセキュリティと経済研究会報告書中間とりまとめ，2011年8月5日，P.68-69
16) 日本セキュリティ監査協会（JASA），サプライチェーン情報セキュリティ管理ガイド，2012年8月，スライド4-15
17) NIST，NISTIR7622，Notional Supply Chain Risk Management Practices for Federal Information Systems，2012年6月，pp.1-15
18) ENISA，An overview of the ICT supply chain risks and challenges, and vision for the way forward，pp.19-28
19) 日本適合性協会，国際相互承認，2013年11月19日閲覧 http://www.jab.or.jp/accreditation/international_accreditation/
20) 経済産業省，国際標準の重要性の高まり，通商白書2010, pp.395