SCIS 2014 The 31st Symposium on Cryptography and Information Security
Kagoshima, Japan, Jan. 21- 24, 2014
The Institute of Electronics, Information and Communication Engineers

企業・組織における情報セキュリティ調査
Information Security Survey on Organization

佐々木 崇裕* Takahiro Sasaki
原田 要之助* Yonosuke Harada
福島 健二* Kenji Fukushima
河野 翔太* Shota Kono
久保 知裕* Tomohiro Kubo
渡邉 晴方* Harukata Watanabe
佐藤 栄城* Eiki Sato
新原 功一* Koichi Niihara

あらまし 情報システムの安全性・信頼性を確保するための情報セキュリティ対策が非常に重要となっている。情報セキュリティ大学院大学原田要之助研究室では、情報セキュリティマネジメントの研究として「情報セキュリティ調査」を組織・官公庁を対象に実施している。本年は 2013 年 8 月に実施した。テーマとしては、情報セキュリティに関するリスク分析などの定点的な調査項目と、情報セキュリティのマネジメント・人材育成・ガバナンスの取組み状況、営業秘密の管理、クラウドの利用及び認証・公開制度の活用状況、事業継続計画（BCP)の策定状況について調査した。本論文では、調査結果の単純集計とその分析結果について報告する。

キーワード 情報セキュリティ調査, 情報セキュリティマネジメント, 人材育成, 教育, ガバナンス, 営業秘密, クラウド, 事業継続計画 (BCP), セキュリティ用語

序章　調査対象及び回答結果

当研究室では 2013 年 8 月に「情報セキュリティ調査」アンケートを郵送にて実施した。対象は、日本国内のプライバシーマーク取得組織、ISMS 認証取得組織、官公庁、教育機関などから、ランダムに選んだ 4,500 組織(送達確認できたのは 4,378 組織)である。その結果 367 件(8.4%)の回答が得られた。なお、本論文においては重複回答及び記入漏れ等の無効回答は、無回答として計上している。また、比較可能な項目については、昨年の調査[1]及び一昨年の調査[2]との比較を行っている。

1　概要

第 1 章では調査の概要を示す。回答者の所属(図 1-1)、事業者(組織と呼ぶ)の業種(図 1-2)、年間売上高(図 1-3)、全従業員数(図 1-4)から組織の概要について、図 1-1～図 1-4 に示すような結果を得ている。なお、業種については日本産業分類を使用し、従業員数・売上高（大学・公務等にあっては予算額）等は、2013 年 7 月 1 日現在、あるいは直近の決算日のものとしている。

調査結果では、回答して頂いた方の所属部門は、総務部門が 31%と一番多く、次に情報システム管理部門、3 番目が情報セキュリティ担当部門となる。総務部門が多い要因として考えられるのは、情報セキュリティがシステムだけの問題ではなく全社での情報セキュリティへの取り組みへ範囲が拡がっていることが推測される。また、中小の組織(従業員数 300 人以下が 71%。後出.)が多いことから情報セキュリティ専門の組織が無く、総務部門が担当していることが推測される。(図 1-1)

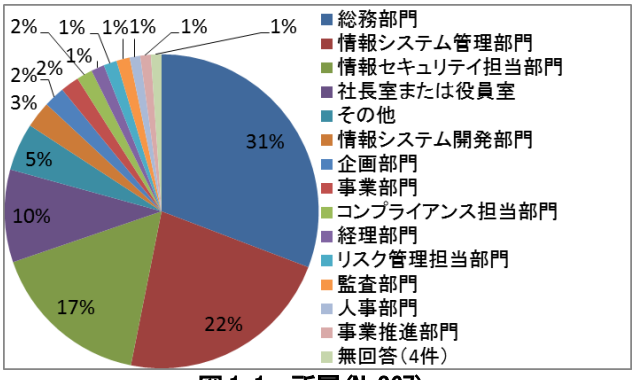

図 1-1　所属 (N=367)

* 情報セキュリティ大学院大学, 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1.
Institute of Information Security, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohasa-shi, Kanagawa, 221-0835 Japan

業種では、情報通信業が 45%と圧倒的に多い。次に大学が 20%となっている。これは昨年の結果とほぼ同様である。情報通信業は昨年の調査と比べると 37.1%から 45%へと 8%程度割合を伸ばしている(図 1-2)。[1]

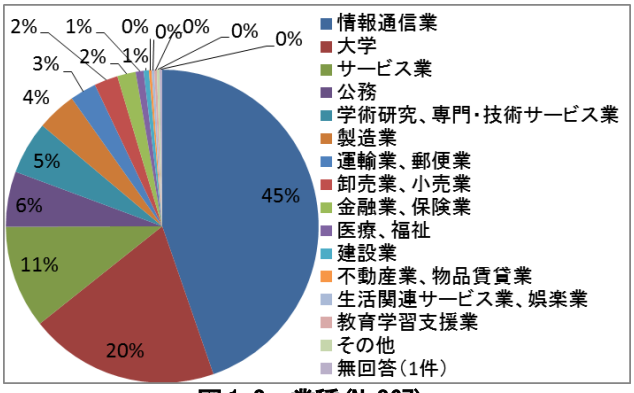

図 1-2　業種(N=367)

年間売上高では、年間売上高 10 億円～50 億円未満が一番多く、50 億円未満の企業が 75%を占める。これは昨年とほぼ同様の結果である。しかし、50 億円以上の企業の割合は昨年同様だが、10 億円未満の企業の割合が減り、10 億円～50 億円の企業の割合が 24%から 32%と増加しており、全体として 10 億円未満の企業が上のランクへ移行している可能性が考えられる(図 1-3)。

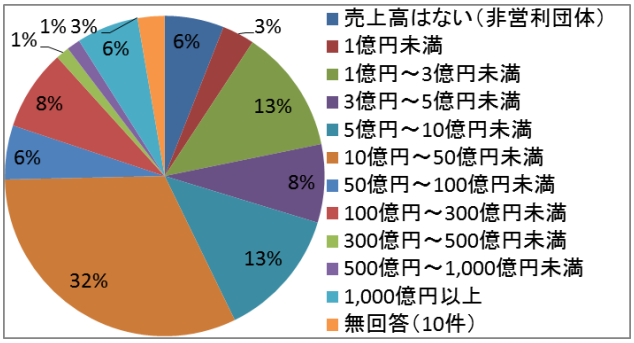

図 1-3　年間売上高(単独)　(N=367)

従業員数では、5 人～300 人以下の企業が最も多く 44%となっており、昨年同様の結果である。また、従業員数 300 人以下の組織で 71%を占める(図 1-4)。

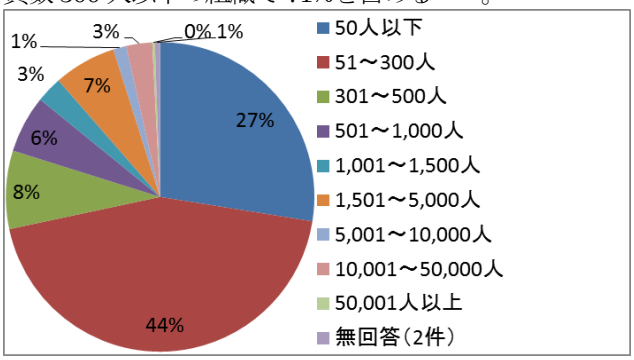

図 1-4　全従業員数(単独)　(N=367)

[1]母数集団の割合においては昨年度のカテゴリから情報通信業へ分類したもの等の調整があるので誤差の範囲と見ている。

2　情報セキュリティマネジメントの取組み状況

第 2 章では、情報セキュリティマネジメントの取組みの現状や阻害要因について示す。調査では、図 2-1～図 2-7 に示す回答結果が得られている。

ISMS を取得している組織は、33%である。そのうち殆どの組織が、P マークも取得している。P マークを取得している組織は 74%であり、昨年の調査の 71%（N=326）と同水準である(図 2-1)。なお、一昨年の調査では 89%(N=404）と高水準であった。

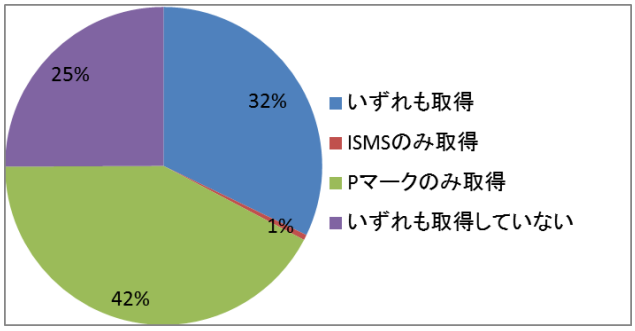

図 2-1　P マークおよび ISMS の取得状況(N=367)

ISMS 取得組織において ISMS を管理している部門を調査した結果、情報セキュリティ担当部門が最も多く、次いで、総務部門、情報システム管理部門、情報システム開発部門となっている(図 2-2)。また、認証を受けた事業部・事業所の部門が管理しているとの回答もあった。

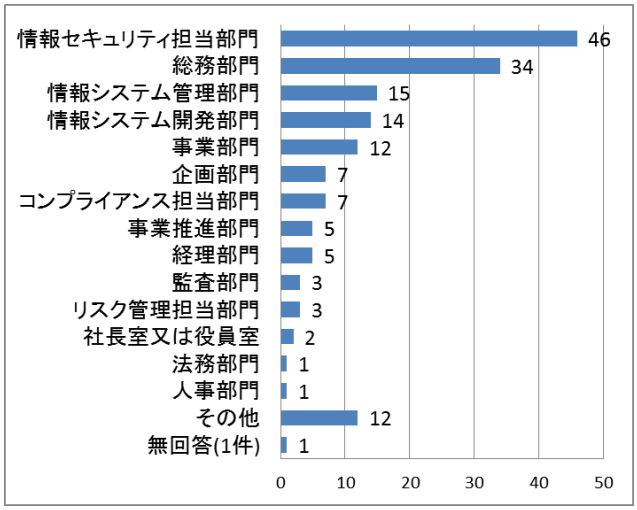

図 2-2　ISMS の管理部門（取得組織のみ）(N=120)

情報セキュリティの脅威のうち、各組織が現時点で重視するものを 3 つまで選択してもらった。その結果、ミスや障害、災害による業務停止に対する意識が高いことが分かった。一方で、近年増加している標的型攻撃については、あまり重視されていない(図 2-3)。従来から存在する脅威について、より重視されていると推測される。

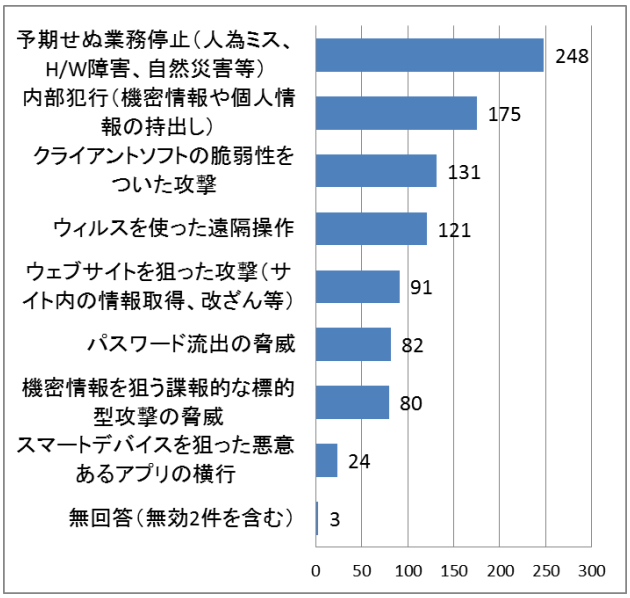

図 2-3　重視する情報セキュリティ上の脅威（N=367）

組織が実施した直近のリスク分析は、70%近くが、1年以内に実施している一方で、実施していない組織が20%弱存在する(図 2-4)。両者とも、昨年の調査と同水準である。

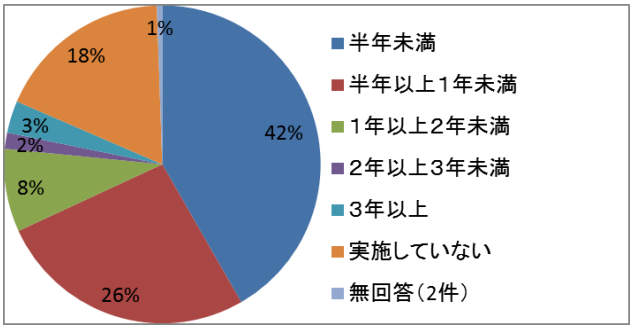

図 2-4　直近のリスク分析（N=367）

リスク分析の問題点としては、人材の不足を感じる組織が、77%と最も多くなっている。また、リスク分析を通常業務に比べ優先度が低いと考える組織が相対的に多い。一方で、上司の理解や関係部署の協力が得られないと感じている組織は少ない(図 2-5)。「必要となる情報の収集がむずかしい」については昨年も調査しており、変化はほぼ認められなかった。

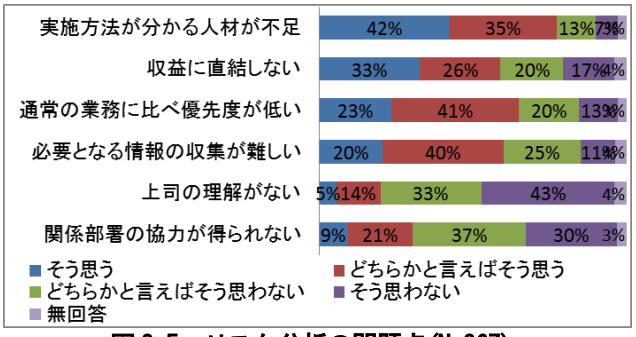

図 2-5　リスク分析の問題点（N=367）

委託先の管理手法は、委託先任せの組織が最も多く、次いで報告書の受領、ヒアリングおよび観察となっている。立入監査や第三者による監査結果の入手を行なっている組織は、極めて少ない。その他の回答には、契約書や社内規程に定める方法、親会社との共同管理などが見られた(図 2-6)。

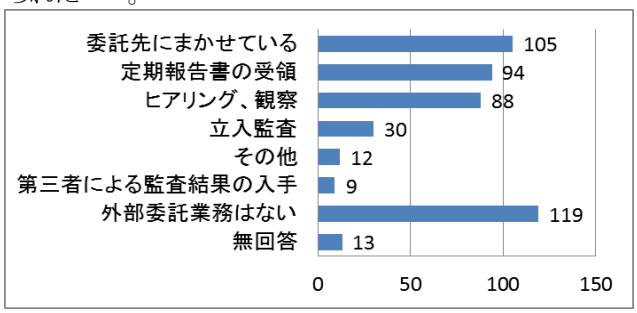

図 2-6　委託先の管理手法（N=367）

システム部門以外への情報セキュリティ教育については、約 80%の組織で、全従業員を対象に実施されている。また、一部を対象に実施している組織も 10%である。しかし、約 10%の組織では現在実施されておらず、その多くで今後も実施が予定されていない(図 2-7)。

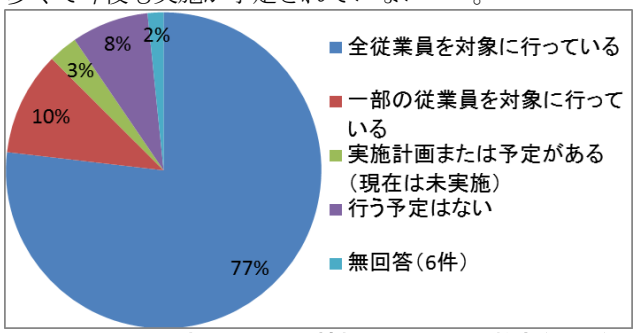

図 2-7　システム部門以外への情報セキュリティ教育（N=367）

3　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

第 3 章では、情報セキュリティ管理体制及び担当者の人材育成について、及び従業員に対する情報セキュリティ教育の実施状況をについて示す。調査では図 3-1～図 3-5 に示す回答が得られている。

情報セキュリティを管理している部署は、情報システム部門が 47%、情報セキュリティ部門が 17%、総務等管理部門の従業員が兼務している組織が 24%存在している(図 3-1)。

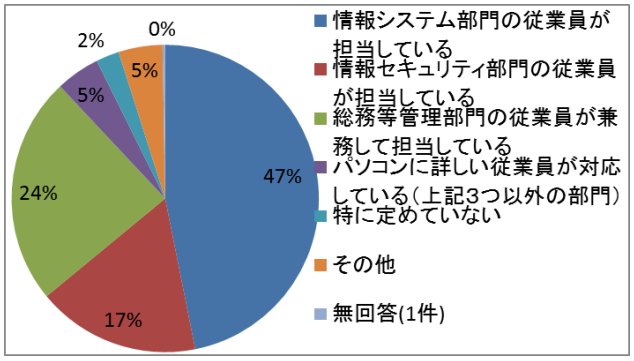

図 3-1　情報セキュリティの管理担当部署（N=367）

約半数の組織が情報セキュリティの推進者の人材育成に関する制度を定めていない。セミナー等の短期間の教育については制度を定めている組織が 1/3 程度ある一方、教育機関への派遣等、長期間の育成に関する制度を定めている組織は少数である(図3-2)。

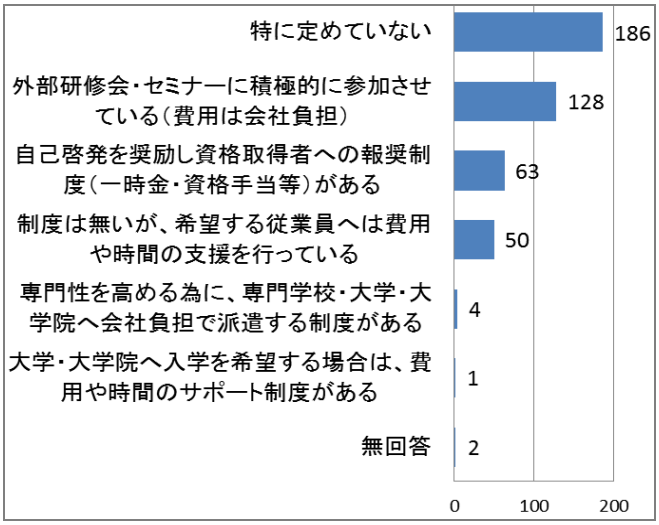

図 3-2　情報セキュリティ人材育成制度の整備状況(N=367)

組織において必要とされる情報セキュリティ関連の資格について調査した結果、マネジメント、運用、技術等組織の実務に関連する資格について必要と考える組織はそれぞれ 35%程度存在するが、審査・監査の関連資格については、約 20%と少ない(図3-3)。監査のみ必要性が低いという傾向は、昨年と同様である。

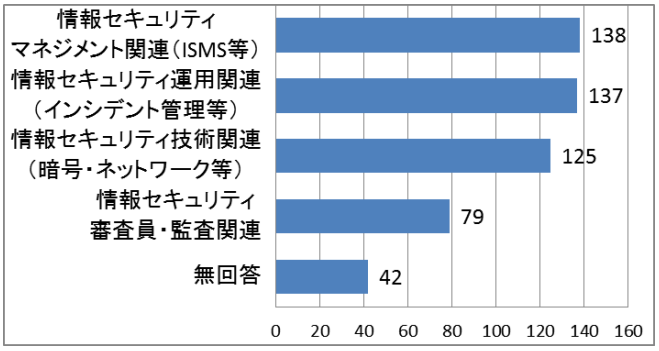

図 3-3　必要とする情報セキュリティ関連資格(N=367)

情報セキュリティ関連資格の活用状況では、多くの組織においては活用できていない。活用できている企業は、対外的アピール、取得奨励に用いている(図3-4)。この傾向は、昨年と同様である。

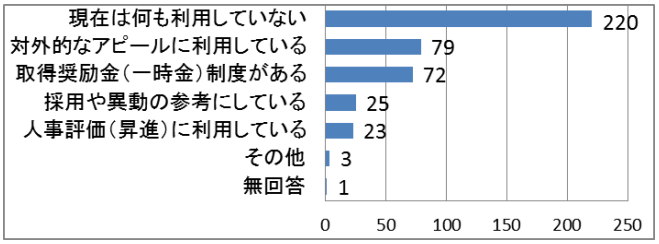

図 3-4　情報セキュリティ関連資格の活用状況(N=367)

従業員への情報セキュリティへの教育では、約 85%の組織が教育を実施している。そのうち約 82%の組織が年間 3 時間未満である(図3-5)。

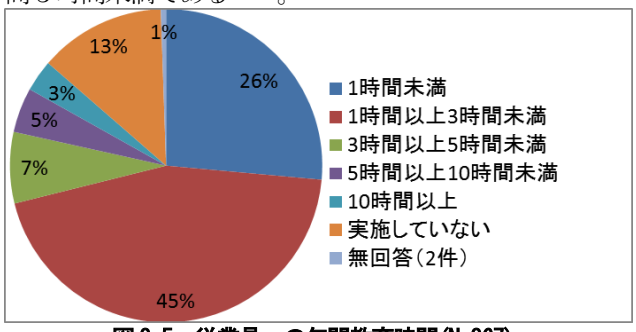

図 3-5　従業員への年間教育時間(N=367)

4　情報セキュリティのガバナンス

第 4 章では、情報セキュリティのガバナンス、セキュリティポリシーの策定・更新の状況について調査した。また、サプライチェーンやアウトソーシング等の外部に組織の重要な機能を依存するビジネスモデルにおけるガバナンス状況についても調査している。調査結果を表 4-1、図 4-1～図 4-5 に示す。

まず、IT ガバナンスの定義について調査した結果、約 1/3 は IT 統制と考えており、IT の管理手続きなどと合わせると半数近い。また、コンプライアンスマネジメント及び一般的な定義の回答がそれぞれ 1/4 あった(表4-1)。

表 4-1　IT ガバナンスの定義(N=367)

選択肢	件数	%
IT ガバナンスは、システムの開発、運用、変更管理やアクセス制御等の手続きをいう	39	10%
IT ガバナンスは、業務上遂行されるプロセスに関して行われる電子承認や電子証跡などの IT の機能をいう	3	1%
IT ガバナンスは、内部統制の一部で IT 全般統制のことをいう	113	31%
IT ガバナンスは、システムの運用管理に関するベストプラクティスを示すフレームワークをいう	6	2%
IT ガバナンスは、システムの開発や運用の仕様に関わる取引先への要求事項をいう	1	0%
IT ガバナンスは、システムの開発や運用の仕様に関わる取引先からの要望事項をいう	3	1%
IT ガバナンスは、システムの開発や運用の仕様に関わる取引先からの要望事項をいう	84	23%
IT ガバナンスは、IT のリスクマネジメントとパフォーマンスマネジメントを実施するにあたっての健全性確保のためのコンプライアンスマネジメントの確立をいう	89	24%
無回答	29	8%

情報セキュリティポリシーの策定・見直し手続きについては、半数以上の組織が情報システム部門、情報セキュリティ部門で策定・見直しをしている。次に、経営層が続いている(図4-1)。

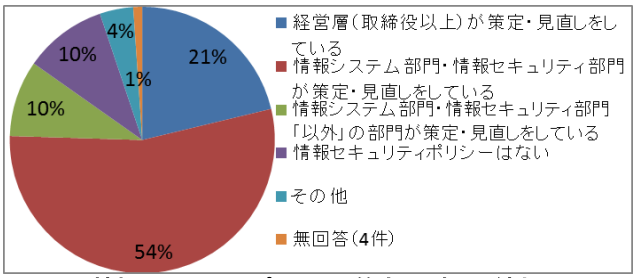

図 4-1　情報セキュリティポリシーの策定・見直し手続き(N=367)

組織が顧客の立場として委託先・調達先を選定する際、委託する業務にかかわらず、機密性を重視している。二番目に重視する項目を含めて比べると、業務委託の種類による違いが鮮明になる(図 4-2)。

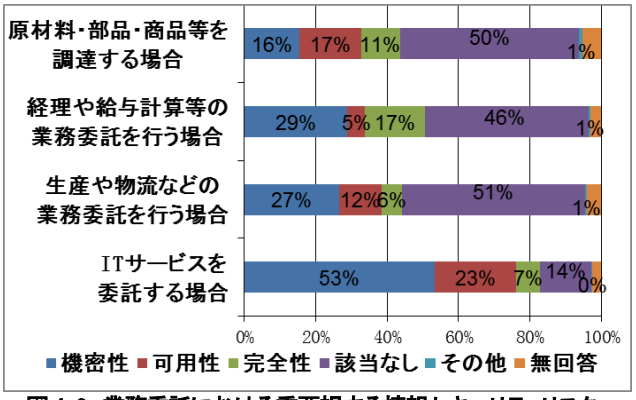

図 4-2　業務委託における重要視する情報セキュリティリスク (N=367)

組織が顧客の立場として IT サービスの委託先を選定する際には、第三者認証を利用することが多い。利用される認証では P マークが多く、ISMS は少ない。多くの組織が契約においては、チェックシートを併用、単体で使用することが多い。この傾向は、どの種類の業務委託にも共通している(図 4-3)。

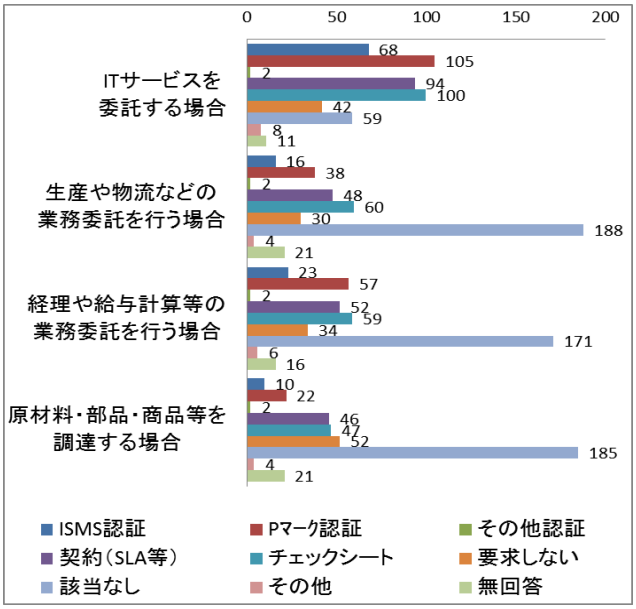

図 4-3　委託業務の種類と管理手法（委託時）(N=367)

組織が受託者・供給者の立場として、顧客から要求される情報セキュリティのリスク対応の調査では、IT サービス受託時には第三者認証が要求されることが多いが、契約やチェックシートといった手法も多い。第三者認証の中では P マークが利用されることが多い(図 4-4)。

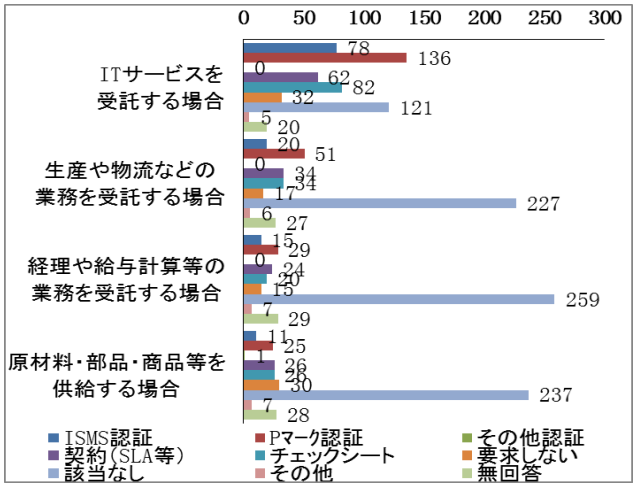

図 4-4　委託業務の種類と管理手法（受託時）(N=367)

組織が受託者・供給者の立場として、顧客に対して調達方針や情報セキュリティ方針において情報セキュリティ上の遵守事項の公開を望むか調査した。業務を受託する際は種類を問わず、常時開示、問い合わせ時には開示してほしいとの要望が多い結果となった(図 4-5)。

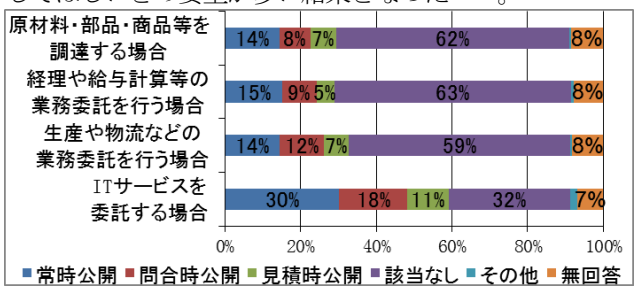

図 4-5　情報セキュリティ遵守事項の開示要求(N=367)

5　営業秘密の管理[3]

第 5 章では、営業秘密の管理について、管理部門、営業秘密とされる情報、秘密性の度合い、情報資産の管理(機密性)との関係の実態を調査している。結果を図 5-1～図 5-4 に示す。

営業秘密を管理している部門では、総務部門が 165 件であり、最も多い結果となった(図 5-1)。

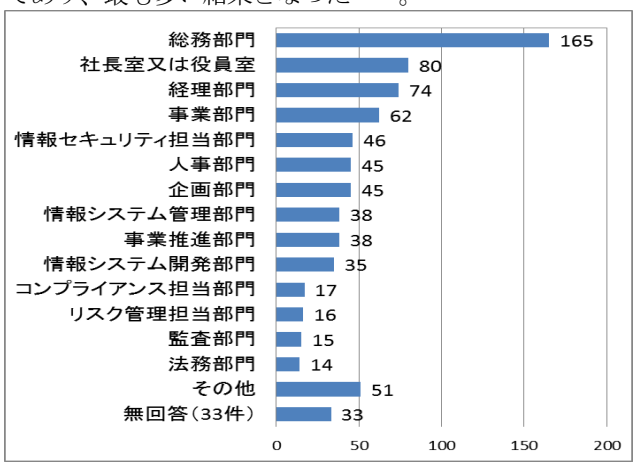

図 5-1　営業秘密の管理部門(N=367)

組織がどのような情報を営業秘密として扱っているかの調査では、仕入先・取引先の情報、従業員情報の回答件数が 200 件を超えた。一方、製造方法や製造図面といった情報は 50 件程度という結果となった(図 5-2)。

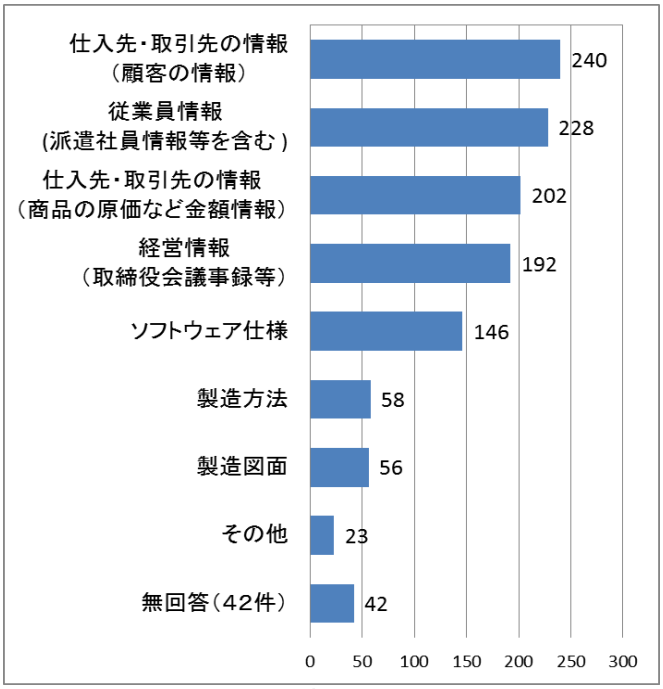

図 5-2　営業秘密の内容(N=367)

組織内で営業秘密を秘密度に応じて区分しているか調査した結果、区分している企業が 51%、区分していない企業が 38%であった(図 5-3)。

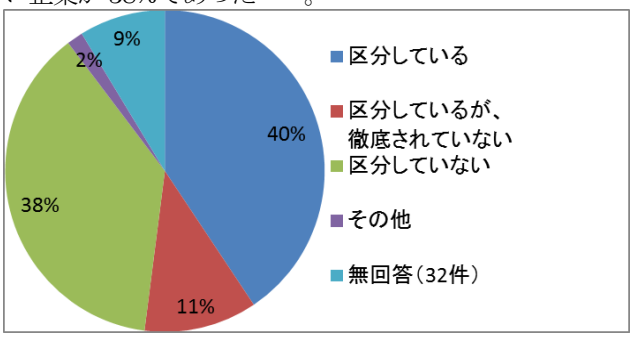

図 5-3　営業秘密における秘密度の区分実態(N=367)

組織が情報資産を機密度に応じて分類しているか調査した結果、機密度に応じて分類している企業は 50%、機密度に応じて分類していない企業が 42%であった(図 5-4)。

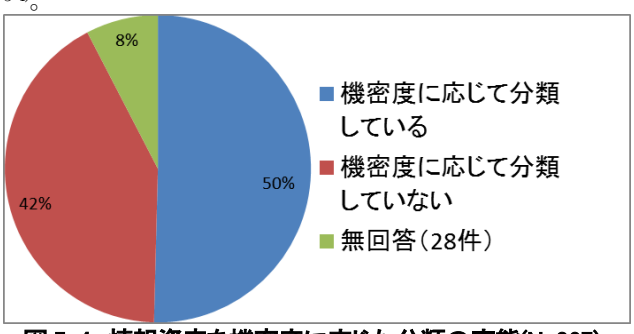

図 5-4　情報資産を機密度に応じた分類の実態(N=367)

6　クラウド・コンピューティング（クラウド）

第 6 章では、クラウドの利用状況と、関連する認証制度・情報公開制度等の認知度・利用状況について示す。調査では、図 6-1、図 6-2 に示す回答結果が得られている。

クラウドの利用状況については、利用する組織の増加傾向が認められる（昨年 34%⇒46%）が、利用する予定がないと答えた組織も微増（昨年 25%⇒29%）している(図 6-1)。クラウドの長所・短所がわかってきたので、様子見の組織が減ってきたと考えられる。

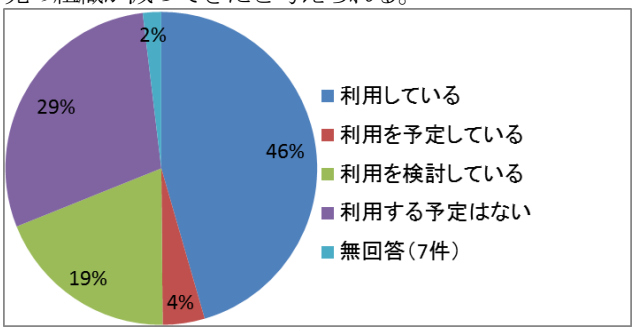

図 6-1　クラウドの利用状況(N=367)

組織のクラウドの認証制度等の利用状況については、ISMS 認証・P マーク認証以外の制度の認知度は低く、利用されていないことが明らかとなった(図 6-2)。

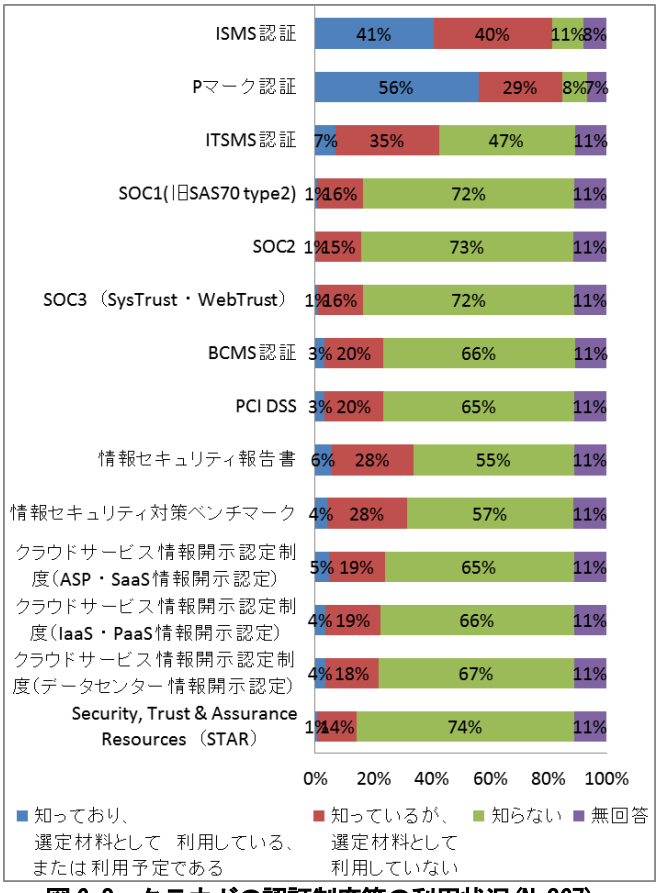

図 6-2　クラウドの認証制度等の利用状況(N=367)

7　事業継続計画について

第 7 章では、組織の事業継続計画の策定状況と想定する脅威について調査している。調査結果を、図 7-1～図 7-4 に示す。事業継続の策定状況では、策定している組織が 41%であった。策定を予定している組織を含めると半数を超えた。一方、策定する予定がない組織も 22%あった。(図 7-1)

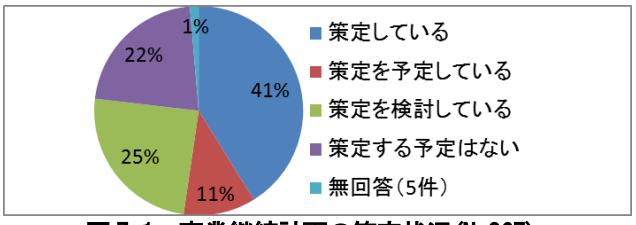

図 7-1　事業継続計画の策定状況 (N=367)

図 7-1 において事業継続計画を「策定している」、「策定を予定している」と答えた組織が想定している脅威は、自然災害（地震、津波、火事等）に係る脅威が上位を占めた。また、情報漏えい事故に係る脅威では、サイバー攻撃よりサイバー攻撃以外による漏えいを脅威とする組織が多かった(図 7-2)。

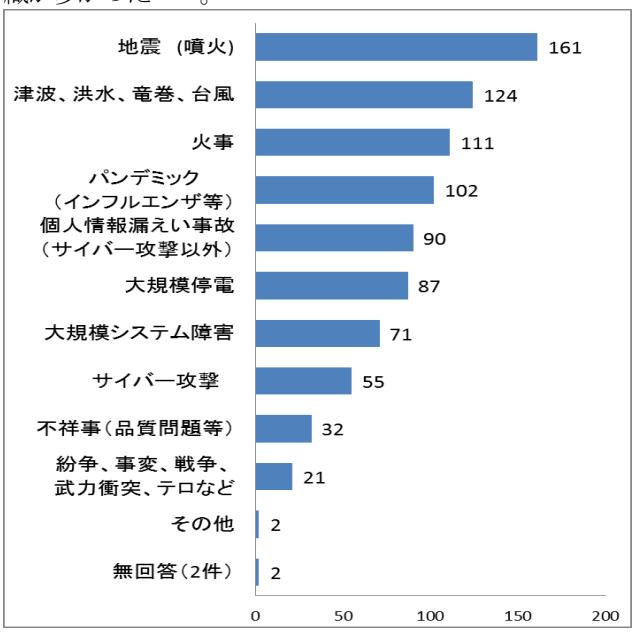

図 7-2　事業継続計画の想定する脅威 (N=192)

IT サービス継続に係る事業継続計画の策定状況については、策定している組織が 25%であった。一方、策定予定が無い組織は 34%であった(図 7-3)。

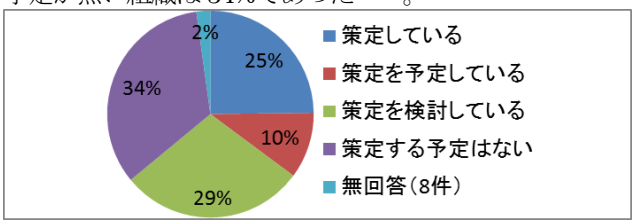

図 7-3　IT サービス継続に係る事業継続計画の策定状況 (N=367)

組織として、IT サービスの停止と個人情報の漏えいとでは、どちらの事業へのインパクトが大きいか調査した結果、IT サービスの停止を選択した組織は 33%であり、個人情報の漏えいを選択した組織は 63%であった(図 7-4)。

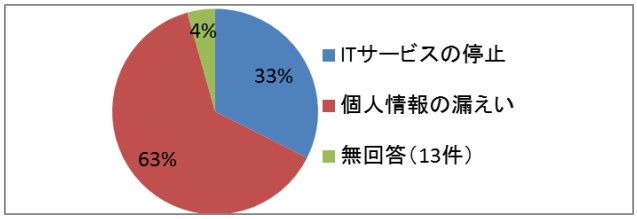

図 7-4　事業インパクトの大きさの比較 (N=367)

8　過去の事例・事故・用語の認知度[4]

第 8 章では、2013 年 6 月までに起きた主要な事件・事故、情報セキュリティに関する用語の認知度について組織の認知度を調査した。結果を、図 8-1、図 8-2 に示す。第 8 章全体の傾向として、過去 3 年間と同様に、マスメディアで取り上げられた事件・事故、用語への関心が高く、専門的なものについては認知度が高くない傾向が見て取れる。なお、Yahoo 事件、遠隔操作ウィルス、スマホアプリによる個人情報漏えい、偽画面によるフィッシングなどはマスメディアで広く取り上げられ、組織内でも検討されたと考えられる。

過去の事例・事故の認知度についてであるが、2012 年のファーストサーバ事件や住基ネットの事件では、システムの可用性の問題についても注目が集まっている(図 8-1)。

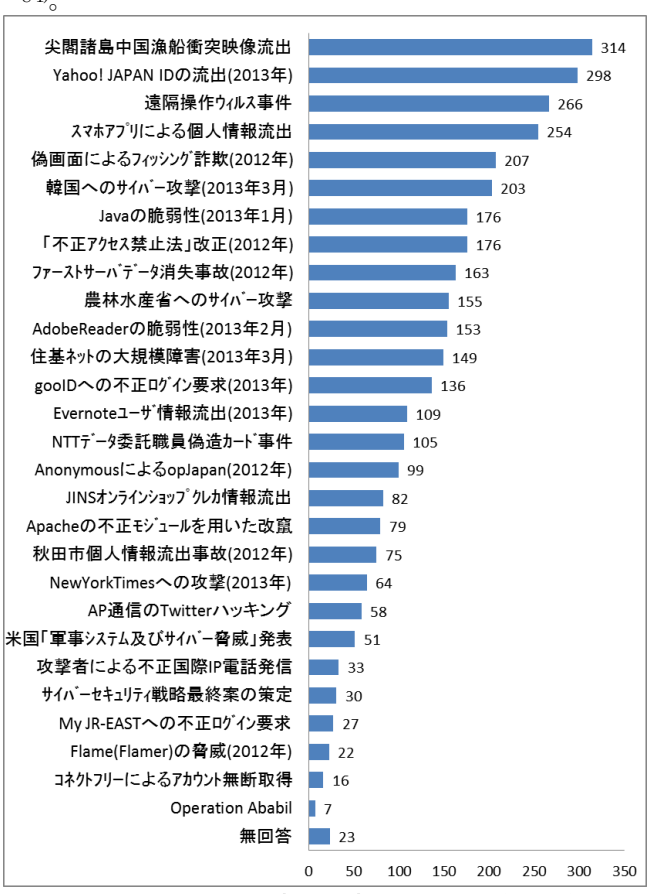

図 8-1　過去の事例・事故の認知度 (N=367)

用語の認知度では、上位 8 位までと、それ以下との認知度の差が大きい。BCP やマイナンバー法案などの時事的なものへの関心が高い。過去の記録と比較すると、BCP の認知度が上がっている。一方、APT、Anonymous の認知度が下がっているのが気になる(図 8-2)。

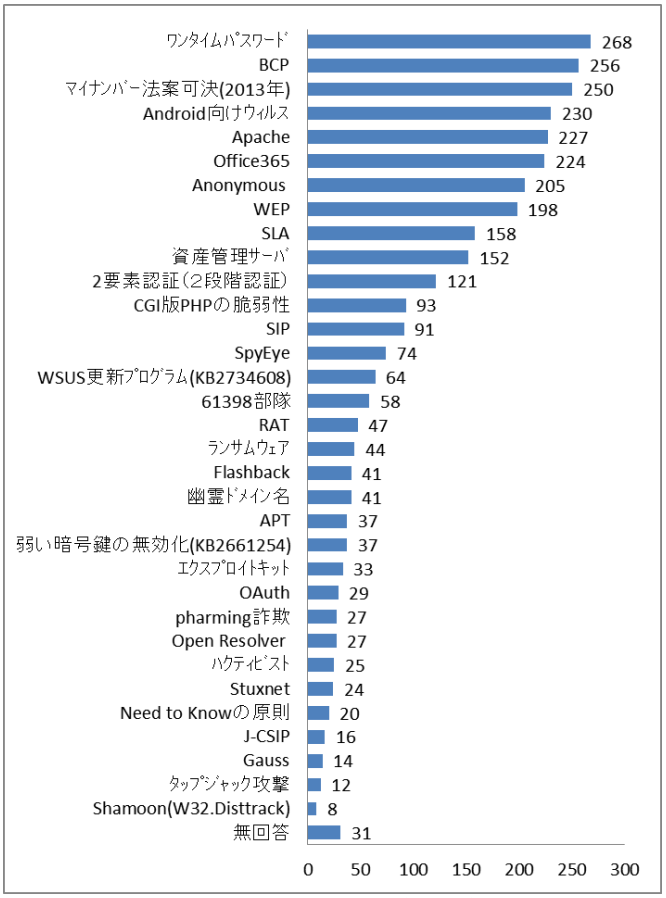

図 8-2　用語の認知度（N=367）

9　まとめ及び今後の研究活動

本研究では、2013 年 8 月に「情報セキュリティ調査表」を郵送し、367 件の回答が得られたものを単純集計して分析している。

今回の分析からは、現状の日本の組織や組織が関わる情報セキュリティの現状をより深く把握することが出来た。この結果は、2013 年の日本の情報セキュリティ一断面であり、今後の調査や研究活動の参考になる。

情報セキュリティマネジメントの取組み状況については、標的型攻撃などの新たな攻撃手法よりも、従来からの脅威を重視する組織が多い。また、リスク分析では人材不足がネックとなっている。

情報セキュリティ管理体制・人材育成及び教育では、約半数の組織が、情報セキュリティの推進者の人材育成に関する制度を定めていない。従業員への情報セキュリティの教育は 80%の組織が年 1 回以上行っている。

情報セキュリティのガバナンスでは、業務の外部委託・受託においては機密性が重視される中で、P マークの利用が多く、また、自組織の要求事項が反映される契約やチェックシートが使われることも多い。国際的な相互認証の可能な ISMS の利用は少なく、コスト面の理由が大きいと考えられる。

営業秘密の管理では、仕入先・取引先の情報、従業員情報を営業秘密として管理している組織が多かった。

クラウドは、利用におけるその長所・短所がわかってきたので、様子見の組織が減ってきたと考えられる。

事業継続計画では、IT サービスの停止と比べ、個人情報の漏えいの方が事業インパクトが大きいとの認識する組織が約 2 倍であった。

過去の事例・事故・用語は、マスメディアで取り上げられた内容については関心が高いが、専門的なものについては高くない。情報セキュリティの担当者や関係者は、継続的に、マスメディアのみならず、専門誌、Web サイトなど幅広く情報を収集して、新しい事象への対応や用語などの理解が必要となる。

なお、本アンケートについては、情報セキュリティ大学院大学原田研究室にて、情報セキュリティ　アンケート調査単純集計結果、及び今回の調査において説明が欲しいとの要望が高かった事件・事故、用語についての解説を公開している。

（http://lab.iisec.ac.jp/~harada_lab/survey.html）

10　謝辞

本調査を実施するにあたり、アンケートへの回答にご協力を頂きました企業や団体、組織の皆様に感謝します。また、アンケートの封入、データ入力に多大な協力をいただいた、神奈川県立麻生養護学校　元石川分教室、神奈川県立高津養護学校　生田東分教室、神奈川県立高津養護学校　川崎北分教室、神奈川県立鶴見養護学校、神奈川県立保土ケ谷養護学校及び川崎市立田島養護学校(五十音順)の皆様に感謝します。さらに温かい指導を頂いた情報セキュリティ大学院の教授の皆様、議論いただいた原田研究室の研究員の皆様、郵便の事務にご協力いただいた大学事務の皆様に感謝いたします。

参考文献

[1] 根岸 秀忠、菅原　尚志、村山　厚、平木　健士、佐藤栄城、原田 要之助, “企業・組織における情報セキュリティ調査,” 2013 年 暗号と情報セキュリティシンポジウム講演予稿集、4E2-2

[2] 堤　健泰、岩崎　正治、鈴子　学、　高梨　智治、橋本　誠、原田　要之助, “企業・組織における情報セキュリティ調査”, 2012 年 暗号と情報セキュリティシンポジウム講演予稿集、2F1-1

[3] 渡邉　晴方、原田　要之助, “情報資産の分類に基づくラベル付けと営業秘密に関する考察,” 研究報告電子化知的財産・社会基盤 (EIP) ,2013-EIP-62(10),1-6

[4] 原田　要之助, “キーワードにみる情報セキュリティ関係者のアウェアネスの現状と課題,” 研究報告電子化知的財産・社会基盤 (EIP), 2013-EIP-62(11), 1-7