SCIS 2015 The 32nd Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 20- 23, 2015
The Institute of Electronics, Information and Communication Engineers

2014 年情報セキュリティ調査から見えてくる組織(民間企業・官公庁・教育機関)における現状

Present situation on information security management of enterprises and Organizations through the questionnaire survey in 2014

水澤 良平* 原田 要之助* 大賀 麻衣子* 佐々木 崇裕*
Ryohei Mizusawa Yonosuke Harada Maiko Oga Takahiro Sasaki
福島 健二* 伊藤 国浩* 丹木 就之*
Kenji Fukushima Kunihiro Ito Nariyuki Tangi

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研究室(教授：原田要之助)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(民間企業・官公庁・教育機関)を対象に実施している．本年度の調査(2014 年 8 月実施)では，情報セキュリティマネジメントの取組状況，人的要因に関する情報セキュリティへの取組，情報セキュリティの人材育成と教育，個人の行動履歴データの取扱いについて調査した．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，人的要因，人材育成，教育，行動履歴，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 2014 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企業，ISMS 認証取得企業，官公庁，教育機関(以下「組織」という。)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 4，374 組織)である．その結果 437 件(10%)の回答が得られた．なお，本論文においては回答の未記入及び択一問題における重複回答等の無効回答は，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，過去の調査[1][2][3]との比較を行っている．

1　概要

第 1 章では調査概要を示す．組織の業種（図 1-1），年間売上高（図 1-2），全従業員数（図 1-3），回答者の所属（図 1-4）から組織の概要について，図 1-1～1-4 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・官公庁等にあっては予算額）等は，直近又は直近期のものとしている．

業種では，情報通信業が 49%と圧倒的に多い．次に大学が 19%となっている．これは昨年と同様の結果である（図 1-1）．

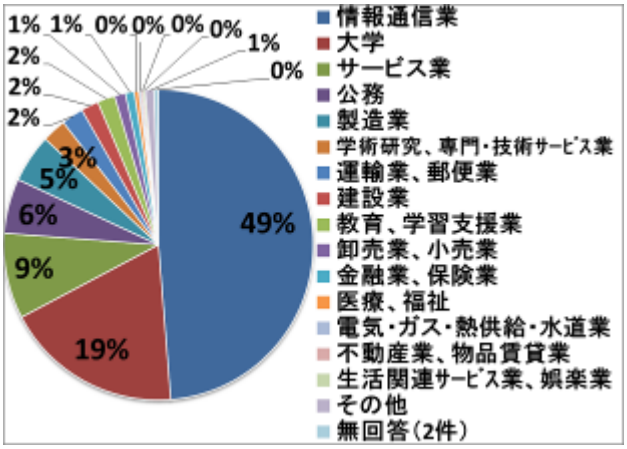

図 1-1 業種(N=437，択一)

* 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

年間売上高では，年間売上高 10 億円～50 億円未満が 27%と一番多く，50 億円未満の組織が 70%を占める．これは昨年度とほぼ同様の結果である（図 1-2）．

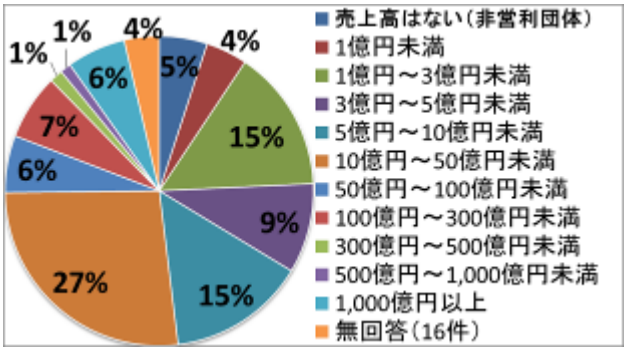

図 1-2 年間売上高(単独)(N=437，択一)

従業員数[1]では，50 人以下の組織が最も多く 30%となっている．また，従業員数 300 人以下の組織で 72%を占める（図 1-3）．

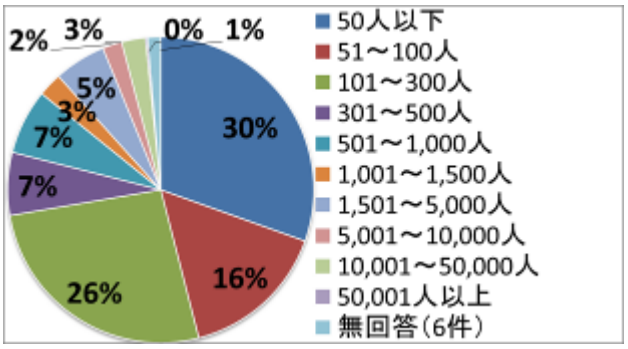

図 1-3 全従業員数(単独)(N=437，択一)

回答者の所属部門は，総務部門が 28%と一番多く，次に情報システム管理部門，三番目が情報セキュリティ担当部門となる．昨年度と同様の順ではあるが，総務部門の割合が減少(31%⇒28%)し，情報セキュリティ担当部門の割合が増加(17%⇒21%)している（図 1-4）．

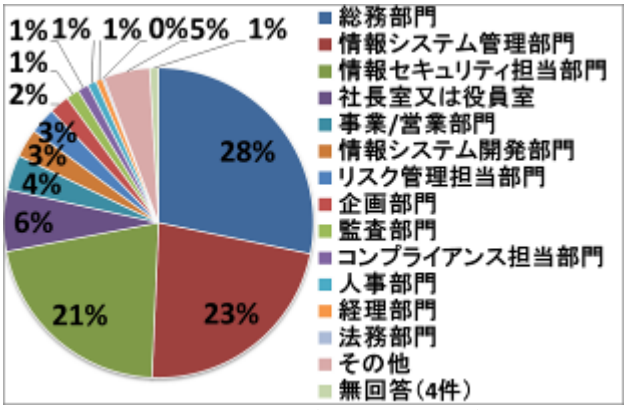

図 1-4 所属(N=437，択一)

[1] 本年度の調査から，51～300 人を 51～100 人，101～300 人と分けて実施した．

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，調査を行った．結果を，図 2-1 から図 2-9 に示す．

2.1 情報セキュリティに関するリスク分析

情報セキュリティに関するリスク分析を最後に実施した時期を調査した結果，66%の組織が，1 年未満で実施している．一方，20%の組織がリスク分析を実施していなかった（図 2-1）．

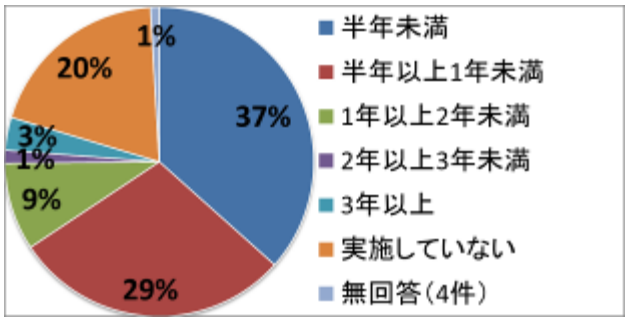

図 2-1 情報セキュリティに関するリスク分析を最後に実施した時期(N=437，択一)

図 2-1 で「実施していない」以外を選択した 352 組織の，リスク分析を実施した理由を調査した結果，ISMS や P マークへの対応が最も多く，情報資産の棚卸，内部規程の改訂が続く結果となった（図 2-2）．

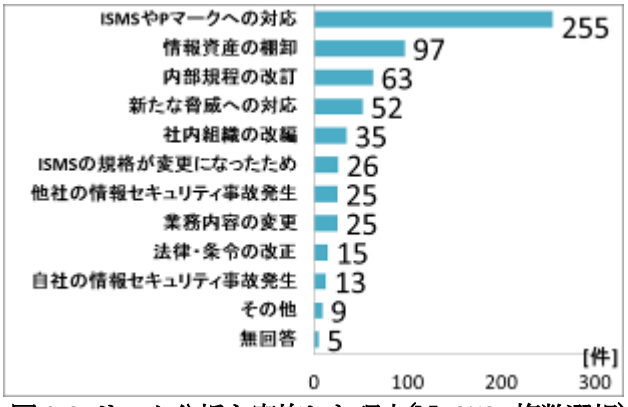

図 2-2 リスク分析を実施した理由(N=352，複数選択)

リスク分析を行う際の問題点について，リスク分析を行っていない場合は実施しない理由を，リスク分析を行っている場合は実施時の問題点を調査した（図 2-3）．「そう思う」と「どちらかと言えばそう思う」を足した割合は，「実施方法が分かる人材が不足している」組織が 81%で一番多く，次いで「通常の業務に比べ，優先度が低い」で 69%であった．

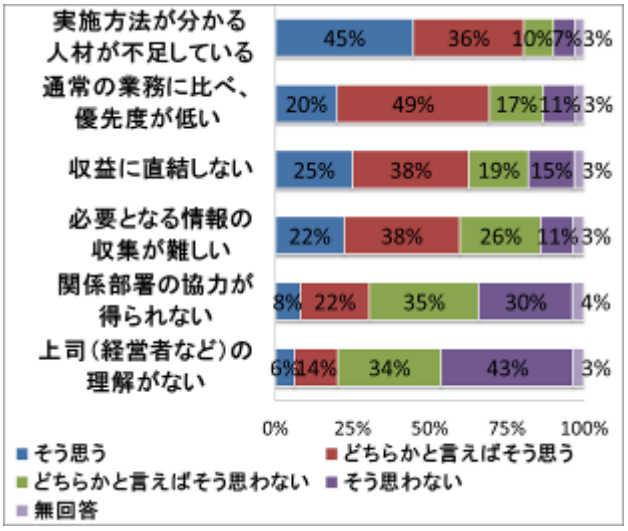

図 2-3 リスク分析を行う際の問題点(N=437, 択一)

2.2 情報セキュリティポリシー

「情報セキュリティポリシー」が示す範囲を，「基本方針・対策基準・実施手順」のうち「基本方針と対策基準」と定義して，以下の調査を行った．

情報セキュリティポリシーを制定しているか，また制定している場合何年経過したか調査した結果，59%の組織が，情報セキュリティポリシー制定から 5 年以上経過している．一方，情報セキュリティポリシーはない，と回答した組織も 10%存在している．また，親会社・親機関の情報セキュリティポリシーに従っていると回答した組織もあった（図 2-4）．

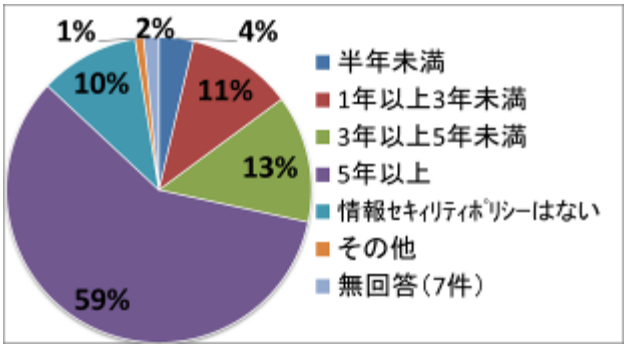

図 2-4 情報セキュリティポリシーを制定した時期 (N=437，択一)

以後の本章の調査では，図 2-4 の「情報セキュリティポリシーはない」と回答した組織を除いた，391 組織を対象とした．

過去 3 年で情報セキュリティポリシー（全体）を見直した理由を調査した結果，監査などの指摘事項やモバイルコードの利用拡大への対応が 25%以上で多かった．3 年間は管理策の見直しがない組織が 21%で次に多い結果となった（図 2-5）．

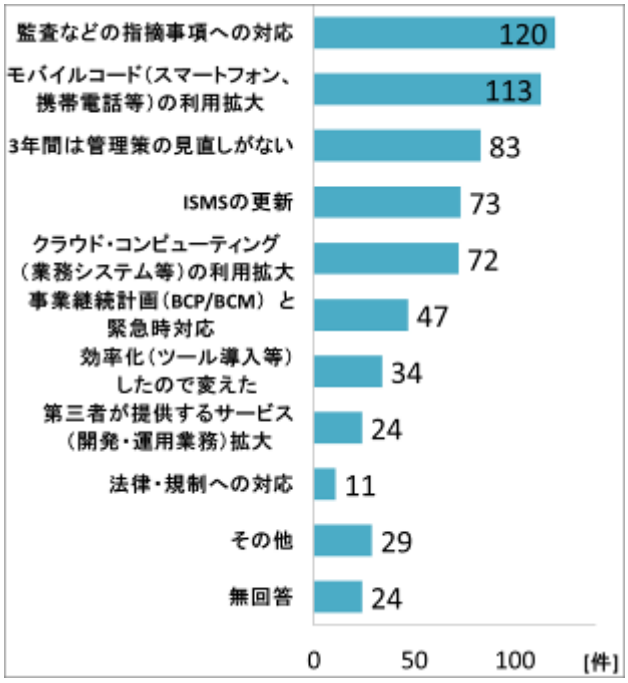

図 2-5 過去 3 年で情報セキュリティポリシー（全体）を見直した理由(N=391，複数選択)

2013 年秋に ISMS の基本基準である ISO/IEC27001 および 27002 が改定されたが，組織の情報セキュリティポリシーに対する影響を，どのように考えているか調査した結果，25%の組織では改定されたことを知らなかった．22%の組織において改定内容を 1 年以内に反映する予定．6%の組織では改定内容を検討中，5%の組織ではすでに改定内容を反映させている．（図 2-6）．

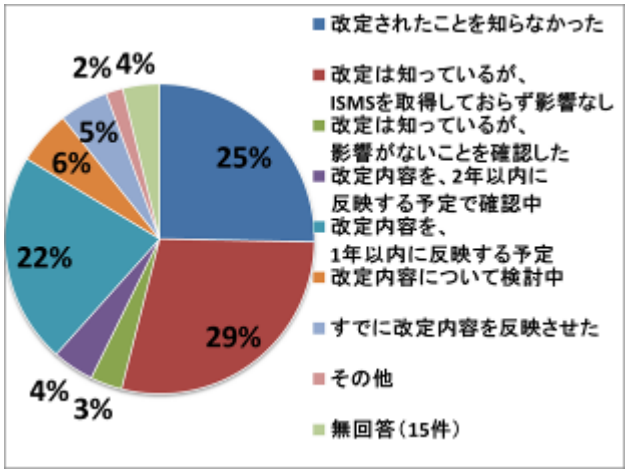

図 2-6 ISO/IEC27001 および 27002 の改定の影響 (N=391，択一)

情報セキュリティポリシーが従業員に定着していると思うか調査した結果，全体的に定着していると考えている組織が多い結果となった（図 2-7）．

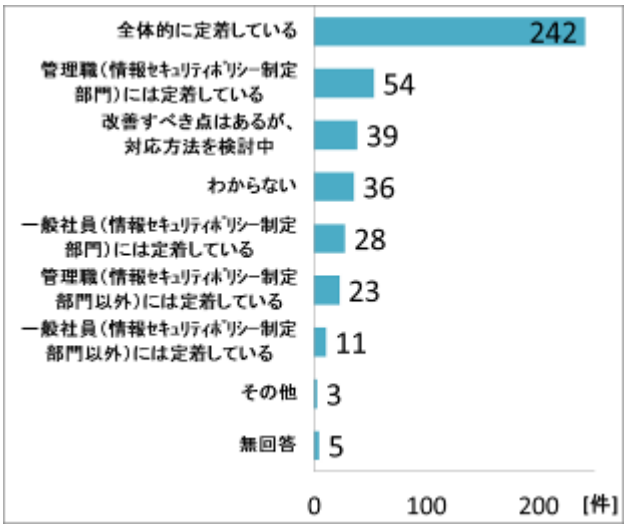

図 2-7 情報セキュリティポリシーは従業員に定着していると思うか(N=391，複数選択)

図 2-7 において，何らかの形で定着していると回答した 359 組織を対象に，定着した理由は何だと思うか調査した結果，「教育・研修等による周知徹底の効果」が出ていると考えている組織が多かった．また，「社内 Web に掲載，ハンドブックの配布など情報セキュリティポリシーの内容を確認しやすくする」，「定期的に定着度チェック（テスト，キャンペーンなど）を実施している」など，情報セキュリティポリシーを意識しやすい環境づくりを効果的と回答する組織も多い結果となった（図 2-8）

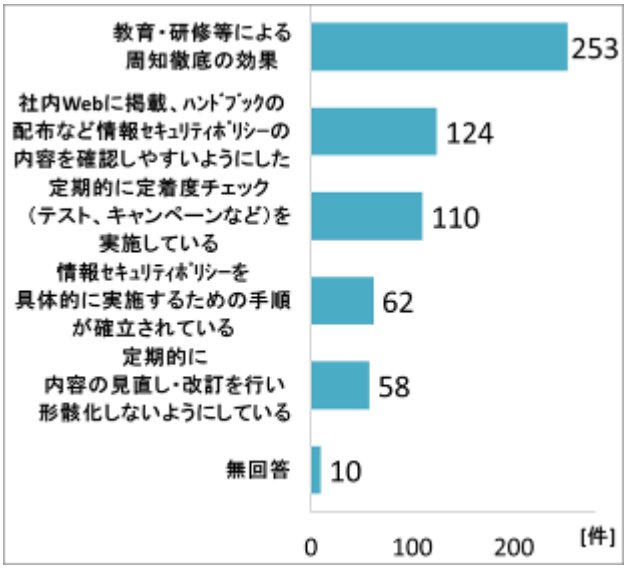

図 2-8 情報セキュリティポリシーが定着している理由（上位５つのみ掲載）(N=359，複数選択)

また，図 2-4 の「情報セキュリティポリシーはない」と回答した組織を除いた 391 組織に，情報セキュリティポリシーを守らなかった場合の罰則規定があるか調査した結果，56%の組織に，情報セキュリティポリシーを守らなかった場合の罰則規定があり，12%の組織では，罰則規定はないが，報告書（始末書）を書かせている．罰則規定導入の予定がないのは 19%のみであった．

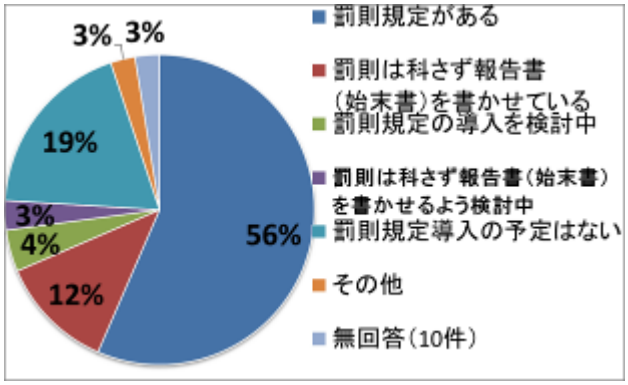

図 2-9 情報セキュリティポリシー違反に対する択一罰則規定の有無(N=391，択一)

3　人的要因に関する情報セキュリティへの取組み

第 3 章では，人的要因によりどのような情報セキュリティに関連する事故・トラブルが発生しているのか．また，内部不正についてはどのような対策が行われているのかを調査した．さらに，自組織内の情報セキュリティに関する人的ミスの情報収集状況及びその情報を外部に公開・提供することについて組織はどのように考えているかを調査した．調査では，図 3-1～図 3-3 に示す回答が得られた．

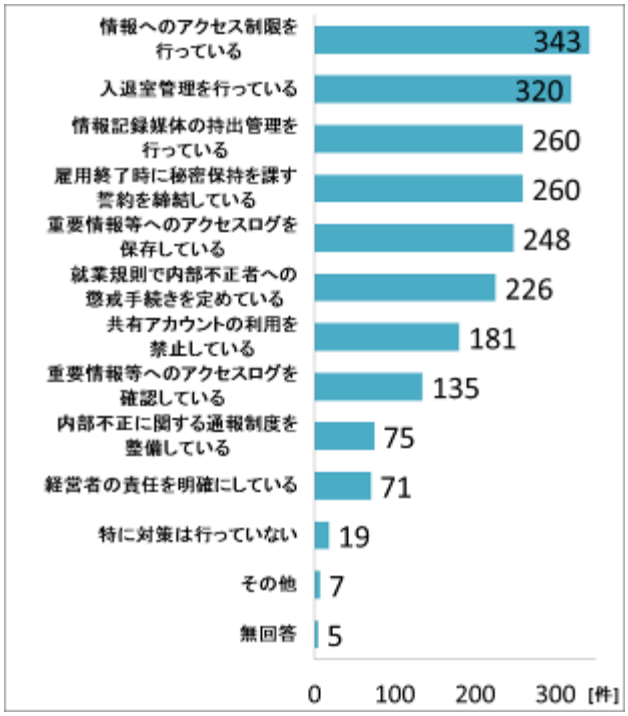

図 3-1 不正行為防止のための対策状況 (N=437，複数選択)

社員・派遣社員などによる情報セキュリティに関連する不正行為を防ぐためにどのような対策を講じているのかを調査した．組織が行っている対策で多いのは，情報へのアクセス制限，入退室管理であり 70%を超える組織が行っている．また，重要情報へのアクセスログを保存している組織は 57%（248 件）あるが，それを確認し

ている組織は 31%（135 件）であった．共有アカウントの利用を禁止している組織は，約 41%であった（図 3-1）．

自組織内において，どのような場合に人的ミスによる事故・トラブルの情報を集めているか調査した結果，内容が誤操作，紛失・置き忘れの場合は，40%強の組織が情報を収集していた．一方，人的ミスだけが原因の場合には情報の収集を行わないとした組織は約 20%存在した（図 3-2）．

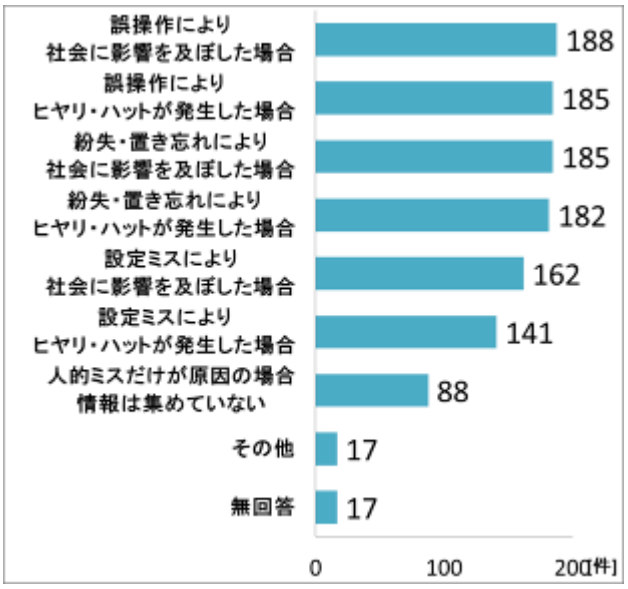

図 3-2 組織内における人的ミスによる事故・トラブルの収集状況(N=437，複数選択)

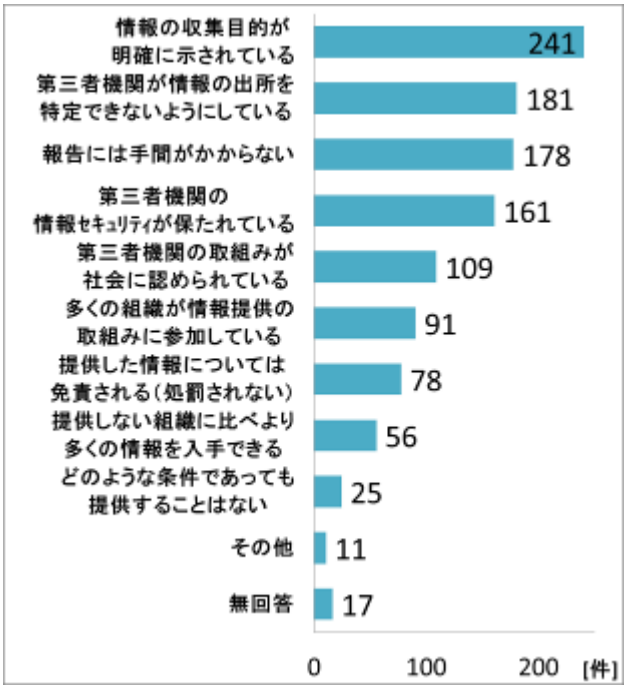

図 3-3 第三者機関へのヒヤリ・ハット事例情報提供の条件(N=437，3 つ選択)

国などによりガイドラインが示され，ヒヤリ・ハット事例情報の収集・分析・公表を担当する公平・中立的で独立した第三者機関が設立されたと仮定した場合，どのような条件があれば自組織内における情報セキュリティについてのヒヤリ・ハット事例情報を第三者機関に提供することができるかを調査した（図 3-3）．結果は，多い順に情報の収集目的が明確に示されている，情報の出所を特定できないようにしている，報告には手間がかからない，であった．また，どのような条件であっても提供することはないとした組織は約 6%であった．

4　情報セキュリティの人材育成と教育

第 4 章では情報セキュリティの人材育成に関してどのような制度があるのか，従業員への教育に関して対象となる従業員や頻度，教育の効果の確認方法について調査を行った．

情報セキュリティの推進者の人材育成に関してどのような制度等があるか調査した結果，外部研修会・セミナーに積極的に参加させている組織が 40%超で一番多いが，特に定めていない組織も 40%近くと多く存在した（図 4-1）．

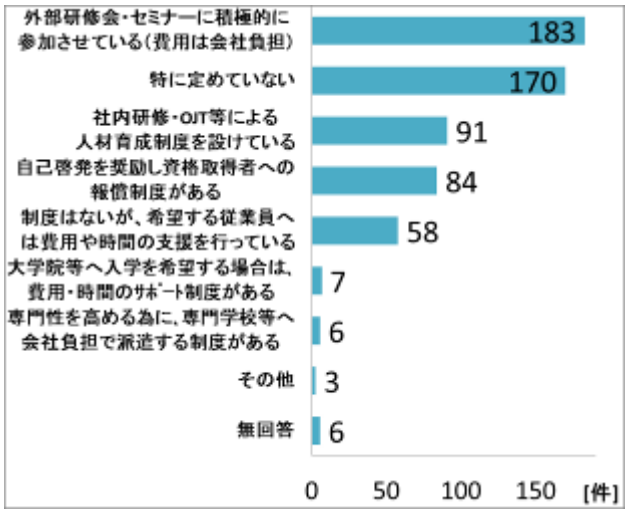

図 4-1 情報セキュリティの推進者の人材育成に関する制度(N=437，複数選択)

情報セキュリティに関する従業員への教育(集合研修・e ラーニング等)について，全従業員向けの教育を年間何回位実施しているか調査した結果，76%の組織が年 1 回以上全従業員向けの定期的な教育を実施しており，9%の組織は教育を実施していないという結果となった（図 4-2）．

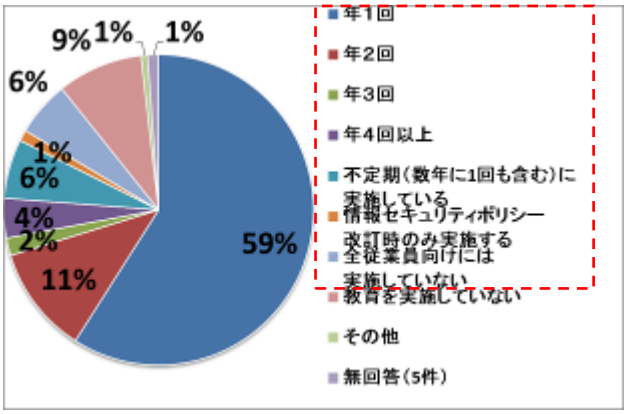

図 4-2 全従業員向けの教育実施回数(N=437，択一)

図 4-2 中において従業員向けの教育を実施していると回答した 398 組織に対し（破線枠内），全従業員向けの定期的な教育以外に特定の従業員を対象にした教育を年間何回位実施しているか調査した．結果は，32%の組織が年 1 回以上全従業員向け以外の特定の従業員向け教育を実施している．不定期（数年に 1 回も含む）や情報セキュリティポリシー改訂時のみ実施する組織も含めると約 71%の組織が特定の従業員向けの教育を実施している（図 4-3）．

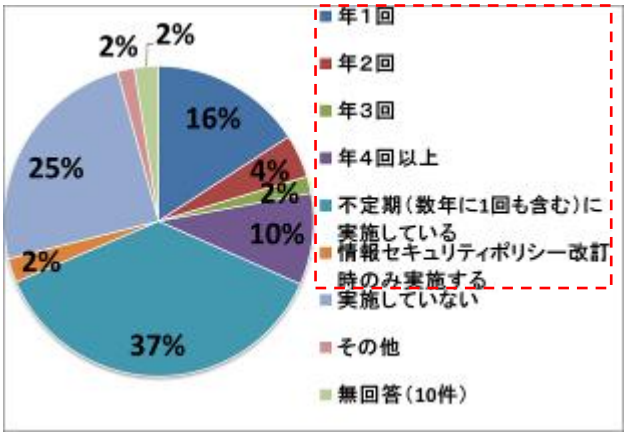

図 4-3 特定の従業員が対象の教育実施回数
(N=398，択一)

図 4-3 で特定の従業員向けの教育を実施していると回答した 283 組織に対し（破線枠内），定期的ではない教育の対象となる従業員を調査した．結果は，全従業員向けの定期的な教育以外の特定の従業員を対象にした教育の対象となるのは，新入社員・転入社員であると回答した組織が多く，次いで，派遣社員・委託先社員であった（図 4-4）．

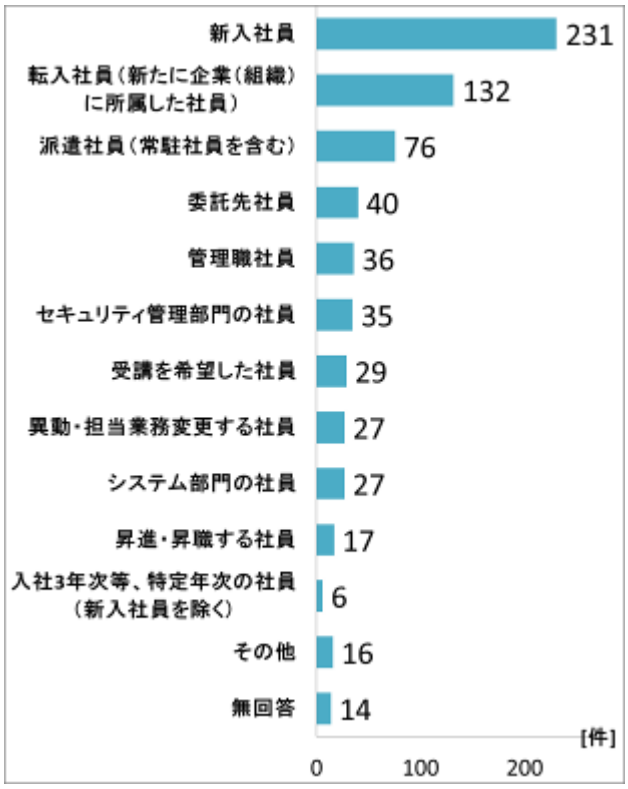

図 4-4 特定の教育の対象となる従業員
(N=283，複数選択)

5 「個人の行動履歴データ」の取扱い

第 5 章では，個人の行動履歴データをどのくらいの組織が取り扱っているのか．また取り扱っている場合には，どのような取り扱いを行い，それが組織にとってどのようなメリットに繋がるかについて調査した．

本章における，「個人の行動履歴データ」の定義は，WEB のアクセス履歴，インターネットショッピング履歴，通信履歴，交通機関利用データ，防犯カメラ映像など，人が入力したデータや，人の活動を記録したデータといった「個人の行動履歴をデータ化したもの」としている．

調査結果を図 5-1～図 5-3 に示す．

「個人の行動履歴データ」を業務で取り扱っているか調査した結果は，個人の行動履歴データを取り扱っている組織が 21%であった（図 5-1）．

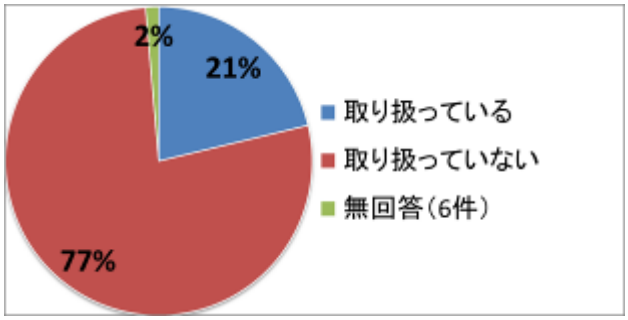

図 5-1 「個人の行動履歴データ」の業務での
取り扱い(N=437，択一)

以下の調査では，図 5-1 で，「取り扱っている」とした 93 組織を対象に行った．

対象の 93 組織のうち，「個人の行動履歴データ」取り扱い業務が，売上／利益に影響しているか調査した結果，売上／利益に貢献していると回答した組織が約 25%であった．特に売上／利益に影響はないと回答した組織が一番多く，約 44%であった．個人の行動履歴データの取り扱いが減収／減益に影響したと回答した組織は無かった（図 5-2）．

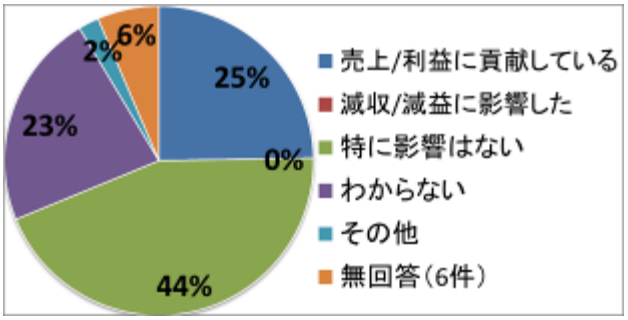

図 5-2「個人の行動履歴データ」取り扱い業務による売上／利益への影響(N=93，択一)

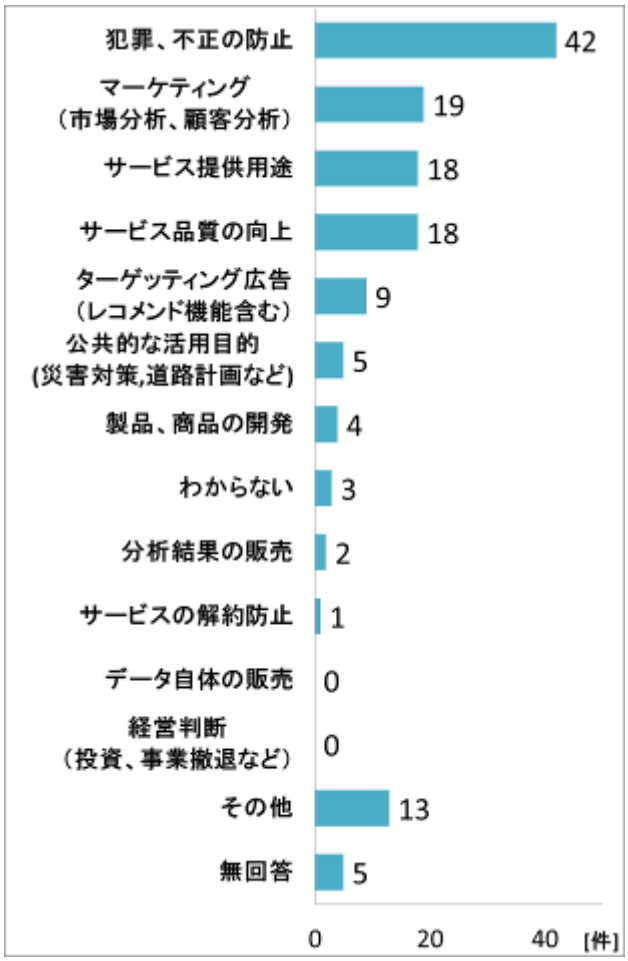

図 5-3「個人の行動履歴データ」を取り扱っている業務の目的(N=93，複数選択)

対象の 93 組織の「個人の行動履歴データ」を取り扱っている業務の目的を調査した結果，1 番多かったのが，犯罪，不正の防止で回答数は 42 件であった．これは総回答数 93 件に対して約 45%の割合となる．次に多かったのが，マーケティング(市場分析，顧客分析)で 19 件の回答数，三番目には同数で，サービス品質の向上とサービス提供用途で 18 件の回答数であった（図 5-3）．

6　過去の事例・事故・用語の認知度

第 6 章では，2014 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．

過去の事例・事故について調査した結果を図 6-1 に示す．

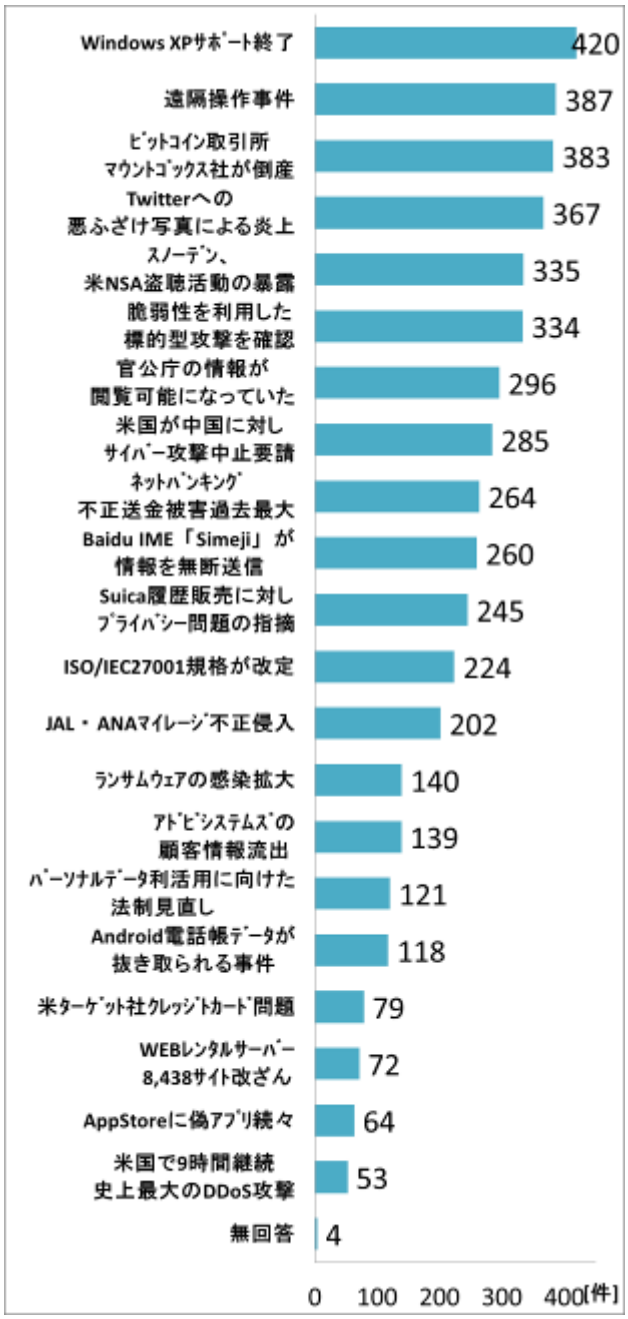

図 6-1 過去の事例・事故の認知度(N=437，複数選択)

例年の傾向通り，マスメディアなどで取り上げられた事例・事故の認知度が高く，専門的なものについては高くない傾向が見て取れる．「ISO/IEC27001 規格が改定」の認知度は 51%である．モバイル端末向けのｱﾌﾟﾘに関する事例についての認知度が低い結果となっている．

なお，本年度は本設問の選択肢を事例・事故名のみから文書形式に変更したため，例年に比べ認知度が高い傾向にある．

用語について調査した結果を図 6-2 に示す．マスメディアで多く取り上げられた用語の認知度が高い結果となった．ワンタイムパスワードについては，認知度が 80%を超え(2013 年度 73%⇒2014 年度 83%)，一般に理解される用語になったと考えられる．攻撃手法の認知度については，専門的なものになるとその認知度が低くなる傾向がある．マイナンバー法案の認知度は 2013 年度が 68%，2014 年度が 73%となった．ランサムウェアについては 2013 年度が 12%，2014 年度が 33%となった．

例年の傾向通り，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傾向が出ている．また，パーソナルデータにあっては，用語の認知度は高かった(79%)が，パーソナルデータの利活用に関する法制の見直しについては低い(28%)という結果となっている．

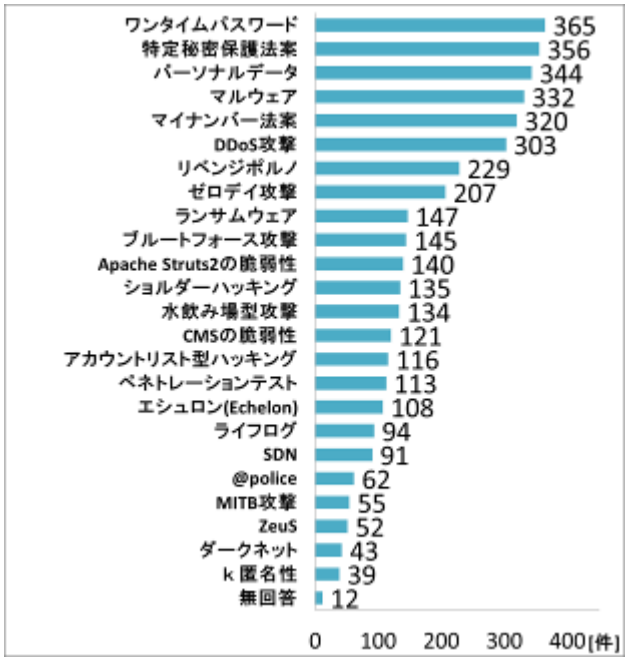

図 6-2 用語の認知度(N=437，複数選択)

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であろう．

7 まとめ及び今後の研究活動

本研究では，2014 年 8 月に「情報セキュリティ調査表」を郵送し，437 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，日本の組織における情報セキュリティの現状を深く理解することが出来た．この結果は，2014 年時点における日本の組織における情報セキュリティの一面を示しており，今後の研究活動の参考に資する．

なお，今回示した調査結果は 2014 年度の「情報セキュリティ調査」の一部であり，全ての調査結果，並びに第 6 章で取り上げた過去の事例・事故及び用語の解説は，情報セキュリティ大学院大学原田研究室の以下のページにおいて公開している．

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

8 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頂いた，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，神奈川県立中原養護学校，神奈川県立横浜ひなたやま支援学校，川崎市立田島養護学校及び他 1 校の神奈川県内の特別支援学校(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，議論頂いた原田研究室の研究員の皆様，郵便の事務にご協力頂いた大学事務の皆様に感謝します．

参考文献

[1] 佐々木崇裕，原田要之助，福島健二，河野翔太， 久保知裕，渡邉晴方，佐藤栄城，新原功一，“企業・組織における情報セキュリティ調査”，2014 年暗号と情報セキュリティシンポジウム講演予稿集，1A1-1.

[2] 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.

[3] 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.

[4] 情報処理推進機構，組織における内部不正防止ガイドライン，<http://www.ipa.go.jp/security/fy24/reports/insider/>，2014 年 11 月 16 日アクセス.

[5] 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.