Vol.2013-EIP-62 No.11
2013/11/21

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

原田 要之助[†1]

近年、さまざまな情報セキュリティに関する事件/事故が起きている。また、情報システムの進歩が早く、これに合わせた情報セキュリティに関する技術の開発の速度も速い。そのため、情報セキュリティについての用語のキーワードは、日進月歩で大きく変化している。情報セキュリティ関係者は、これらの動向を十分に把握して、変化に対応する必要がある。情報セキュリティ大学院大学では、キーワードの認知度を組織の情報セキュリティのアウェアネスと考えられるとの仮説を立てて、アンケート調査により、調査を実施した。キーワードの抽出にあたっては、できる限り、該当年度の情報セキュリティの動向を正しく示すものを文献や Web サイトなどから収集した。これらのキーワードについて調査したところ、情報セキュリティの事故/事例や用語のキーワードの認知について、我々情報セキュリティ大学院側が予測していたレベルを大きく下回っていたことであった。そのため、複数年度で調査を継続したが、傾向は変わらなかった。本稿では、これらの調査を分析した結果について示し、今後、情報セキュリティ関係者は、一般誌だけではなく、専門的なものから新しいキーワードを学ぶ必要性について述べる。

A study on the awareness of information security practitioners based on related keyword analysis

YONOSUKE HARADA[†1]

Recently, many information security incidents have occurred and hence many new incident keywords are created. This is because progresses of IT and IT security have accelerated. Now, most of SMEs (Small and Medium size Enterprise) use IT and Database to enhance productivity and efficiency. Hence, the number of keywords for information security is increasing and has changed rapidly. Information Security Personnel should know these keywords. This paper surveyed the awareness of Information Security Personnel by two consecutive questioners in 2011 and 2012) and found that result of awareness is lower than expected. This paper shows the survey, result and analysis of this phenomenon. Keywords are selected from several sources such as IPA, JNSA survey, and web site. This paper proposes that awareness training for information security is necessary regardless of size. Also, this paper concludes information acquisition by information security personnel should be not only by general newspapers but also by information security specialized magazines.

1. はじめに

情報セキュリティ関係者は、自分の管理する情報システムやネットワークを運用して、問題が見つかれば即応する必要がある。昨今は、ほとんどの情報システムがインターネットなどのオープンなネットワークに接続されており、外部からの侵入、中でもサイバー攻撃に晒されている。サイバー攻撃では、世界中の犯罪者や愉快犯が日夜、新しい攻撃方法を開発している。また、企業で広く使われている OS やアプリケーションソフトの脆弱性のパッチについては、緊急性と合わせて報告されている。そのため、管理者は、このような外部の情報に敏感でなければならない。

情報セキュリティ大学院大学の原田研究室では、情報セキュリティのマネジメントに関する調査を実施しており、2010 年からは、企業、官公庁、大学などの教育機関を対象に情報セキュリティするさまざまな調査を実施してきた。とくに、2011 年からは、組織における情報セキュリティのキーワードを通じた Awareness（以下では、認知という）について調査している。この調査においては、企業などの組織において、その時点において、情報セキュリティ管理者が知っておいてほしいキーワードや情報セキュリティに関する事件・事故を抽出し、アンケートで聞く方法をとっている。本稿では、2011 年における調査[1]、2012 年における調査［2］をベースに分析する。

2. キーワード解析について

2.1 キーワード分析

キーワード分析は、先行研究[3]、[4]では、以下の分析を行うことをいう。

・Web サイトなどで、あるキーワードが検索された回数
・文書、記事、文献などで、あるキーワードが出現した回数
・SNS やブログなどで、ユーザがタグ付けした件数

まず、キーワードの検討では、検索エンジン関連分野の研究が進んでいる。例えば、Google などでは、検索エンジンでキーワード分析を実施して、よく検索されているキーワードを検索の Suggestion につなげている。これは、検索のサブメニューでキーワードに関連したものをリストとして提供するものであり、キーワードの組み合わせで構成されている。また、検索の結果では、過去のキーワードで検索された項目のうちアクセスの頻度の高い順番にリストで提供される。そのため、Web を利用したオンラインショッピングでは、キーワード検索結果の上位に入れ込むことで、より多くの露出を高めようという誘因がわく。そこで、人海戦術でアクセスして、検索リストの上位に出現するような方法がとられる。当然、Google もこれに対抗して同一のドメインからのアクセスを頻度に加えないような工夫をするなどしている。このように、キーワードは知識の一部として、きわめて重要な役割を持っている。
また、Google では Google Analytics を提供して、web サイトへの訪問者の行動を分析して、サイト内容の改善につなげている。ここでは、キーワードのデータとアクセスとの関係を分析して、キーワードを精査して、費用対効果の高い広告につなげることを提供している。このように、キーワードは、web サイトのみならず、文献などの内容を構成する要素とみなすことができる。すなわち、キーワードを用いて、その分野の技術内容を表現できるともいえよう。

国立情報学研究所の西澤らは、論文誌や科研費の申請書にどのようなキーワードが出現するかを用いた分析を行って、研究組織の研究内容や他の研究機関との関係を可視化している。この概念をベースに実際のシステム化にも取り組んでいる。この研究では、論文などに出現するキーワードが技術内容を示す重要な役割を演じていると述べている[3]。さらに、西澤は、一般報道と学術論文におけるキーワードを比較することで、学術が一般の影響を受けていること、すなわち、学術分野は、新規性や研究に対する説明責任を示すために、一般に使われているキーワードに対して敏感であることを示した[4]。キーワードはこのように概念との関係性を把握するうえで役立つ。

2.2 情報セキュリティ分野でのキーワードによる分析

岩崎らは、キーワードに着目して、情報セキュリティ分野における概念の普及度合いを分析している[5]。サイバー攻撃の「advanced persistent threat」（以下では、APT という）に着目して、Google Insights for Search を利用して、キーワード検索がどのように変化したかについて分析している。具体的には、Google Trend におけるニュース参照数の動向を図 2.1 に示す。なお、岩崎らが指摘しているように、Google Trend 及び Google Insights for Search で示される結果は、キーワードに対する世間一般における時系列での関心度の遷移を把握することに、適している。

図 2.1　Google Insights for Search における APT のキーワード検索分析結果［5］

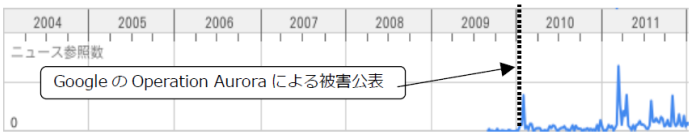

図 2.2　Google Trend における APT の分析結果［5］

岩崎らは、図 2.1 から、Operation Aurora による被害が公表される 2010 年 1 月までは、APT が検索される割合は非常に低く、図 2.2 が示す結果からは、2010 年 1 月までは APT に関連するニュースの Web サイトへの掲載はなかったと述べている。さらに、2010 年 1 月以降においては、図 2.1、図 2.2 が示すように APT の検索ボリュームやニュース参照数は、一定程度の頻度を維持し続けてきている。すなわち、2010 年 1 月以降 APT は、一般的に使用される用語に変わった。とくに、2010 年 1 月に、Google が Operation Aurora と呼ばれる一連のサイバー攻撃による被害を公表した頃から、各セキュリティベンダーが APT をサイバー攻撃の説明に用いるようになり、情報セキュリティ関係者が関心を持つようになったと述べている。

以上のような経緯からは、情報セキュリティ分野においても、キーワード分析が情報セキュリティのアウェアネスとの関係が深いことが分かる。

3.情報セキュリティ調査について

情報セキュリティ大学院大学の原田では、情報セキュリティのマネジメントに関する調査を実施しており、2010 年からは、企業、官公庁、大学などの教育機関を対象に情報セキュリティに関するさまざまな調査を実施してきた。以下に調査の概要について示す。

3.1 2011 年度アンケート調査

2011 年 7 月～8 月に、ランダムに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、教育機関などから、4,500 の組織を選び、情報セキュリティ担当者に「情報セキュリティ調査」を郵送して回答を求めた。その結果、407 件の回答が得られた。なお、回答数には、重複回答及び記入漏れ等が存在するため、回答総数にはバラツキがある。回答者の所属を図 3.1.1 に、事業者の業種を

図 3.1.2 に、全従業員数を図 3.1.3 に示す。また、情報セキュリティ監査の実施について図 3.1.4 に示す。図 3.1.1 からは、所属部内は、「総務部門」、「情報セキュリティ担当部門」、「情報システム管理部門」が多く、図 3.1.2 から、業種では、「情報通信業」が 4 割程度と最も多い。従業員数では「51 人～300 人」が、最も多い。

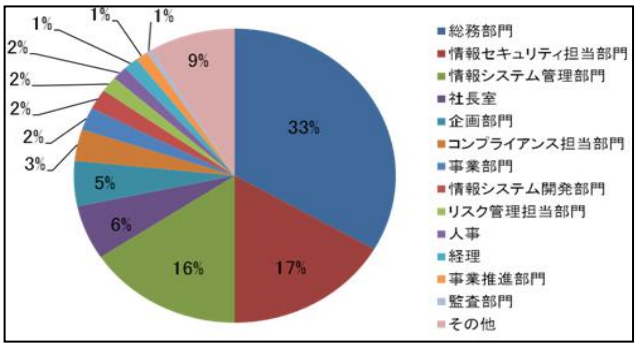

図 3.1.1　所属（N=405）[1]より

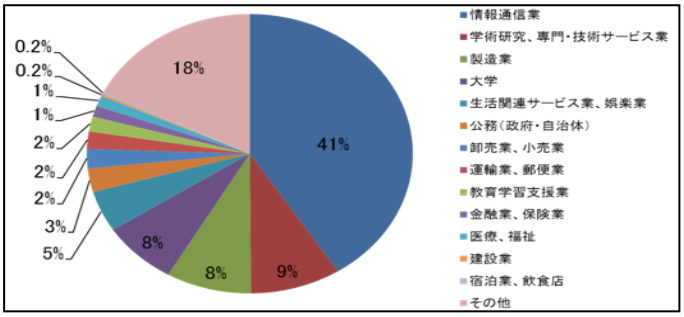

図 3.1.2　業種（N=405）[1]より

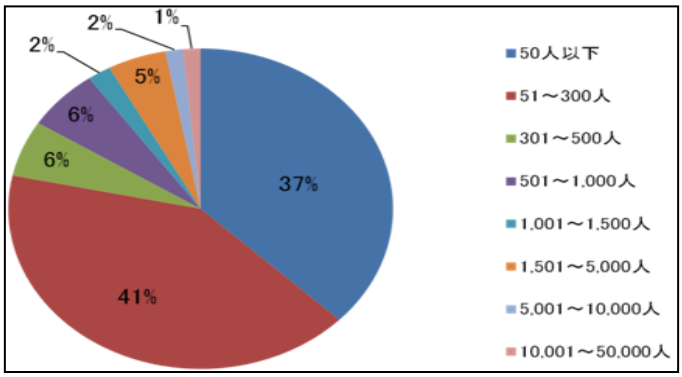

図 3.1.3　全従業員数（N=405）[1]より

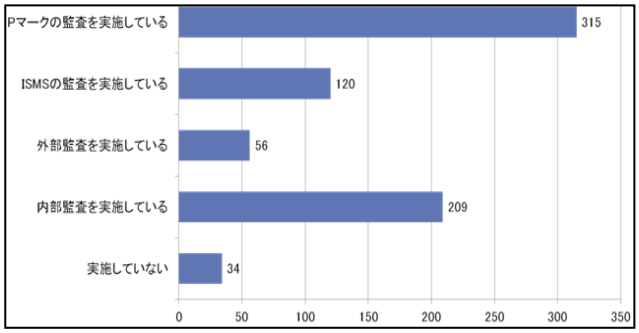

図 3.1.4　情報セキュリティ監査の実施（N=405）

図 3.1.4 からは、「P マークの監査を実施している」事業者が多く、情報セキュリティについては、それなりの理解があることが分かる。

3.2　2012 年度アンケート調査

2012 年 7 月～8 月に、ランダムに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、教育機関などから、4,500 の組織を選び（送達確認できた組織は 4,229）、情報セキュリティ担当者に「情報セキュリティ調査」を郵送して回答を求めた。その結果 335 件の回答（7.9%）が得られた。なお、回答数値には、重複回答及び記入漏れ等が存在するため、質問項目毎の回答総数には多少のバラツキがある。以下に調査結果の概要を示す。

回答者の所属を図 3.2.1、事業者（組織と呼ぶ）の業種を図 3.2.2、全従業員数を図 3.2.3 に示す。

所属部門では、「情報システム管理部門」「総務部門」、「情報セキュリティ担当部門」が多く（図 1-1）、業種では、「情報通信業」が 4 割近くと最も多いが、大学の割合が昨年（8%）より増え、2 割を超えている（図 1-2）。

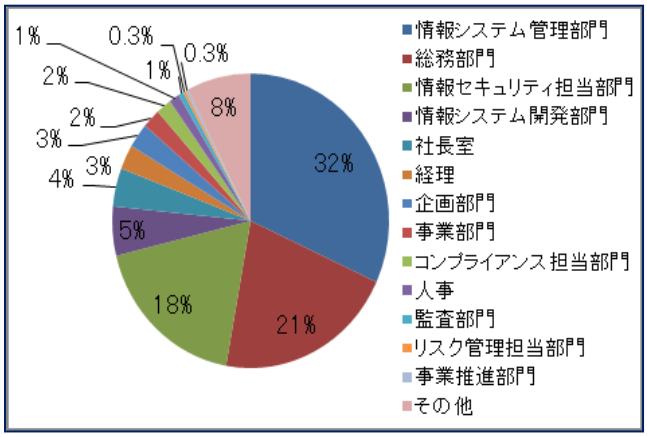

図 3.2.1　所属（N=333）　[2]より

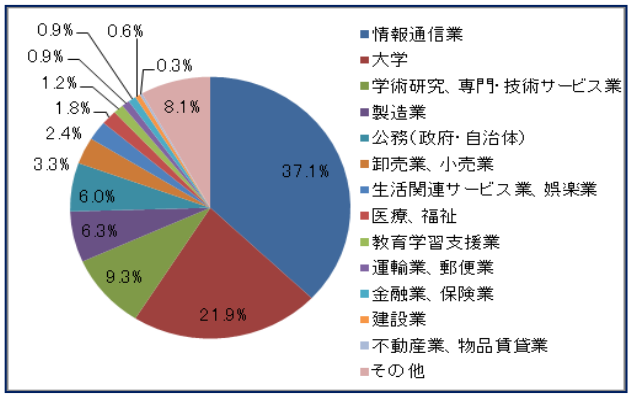

図 3.2.2 業種（N=334）　[2]より

年間売上高では「10 億円～50 億円未満」、従業員数では「51 人～300 人」が最も多く、2011 年と同様の傾向である。

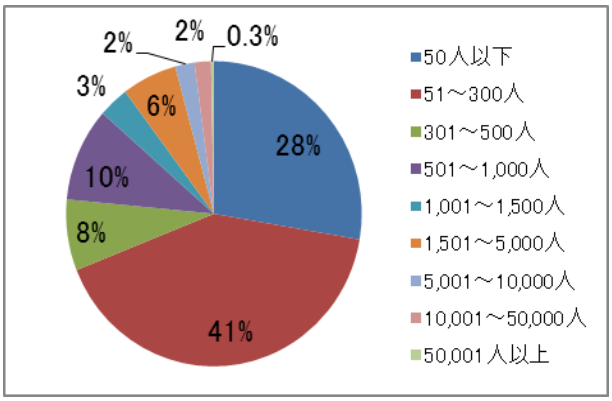

図 3.2.3 全従業員数(単独) (N=332) [2]より

4. 情報セキュリティ分野におけるキーワードによる認知度について

情報セキュリティに関する事件/事故、用語などのキーワードによるアウェアネスの考え方と調査について述べる。

4.1 2011 年度でのキーワード調査

4.1.1 事例/事故のキーワードについて

情報セキュリティの関係者にとって、情報セキュリティに関する過去の事件/事故のキーワードについては、二度と同じことを繰り返さないため専門家の間で共有することが望ましいと考えられている。さらに、リファレンスとなる事例/事故については、マスメディアや専門誌などで取り扱われていることもあるので、これらをキーワードとすることができると考えられる。

表 4.1.1 調査に用いた事例/事件のキーワード (2011 年度)

Sony個人情報流出(2011年)
みずほ銀行システム障害(2011年)
Amazon EC2 障害(2011年)
CLOUD9 障害(2011年)
米ロッキード社へのサイバー攻撃
韓国農協へのサイバー攻撃
サンプル百貨店個人情報流出
三井情報個人情報流出(2010年)
アディダス社員Twitter中傷事件
ヤマト運輸携帯Webサイトの脆弱性
尖閣諸島中国漁船衝突映像流出
大阪地検特捜部証拠改竄事件

2011 年度の調査では、アンケート項目として、JNSA と情報セキュリティ大学院大学の共同研究によるインシデント調査[6]が取り上げている重要な事件/事故を参考に、有名な事例、時事的な事例/事件を、表 4.1.1 に示すような項目を抽出した。

そのほかには、サイバー攻撃や標的型攻撃をベースとした用語を盛り込んだ。さらに、時事的な事件事故についてはマスメディアで取り扱われた情報セキュリティ分野の用語を調査して抽出した。

2011 年度調査における表 4.1.1 をベースとした事例/事故のキーワード分析結果を図 4.1.1 に示す。図 4.1.1 からは、個人情報の情報漏えい関連の事件については、ほとんどが 300 件以上の高い「知っている」との回答を得た。また、有名なサイバー攻撃などの情報セキュリティ事例については 100 件～130 件程度、情報セキュリティ関連のマイナーな事例については、30 件～50 件程度「知っている」との回答を得た。

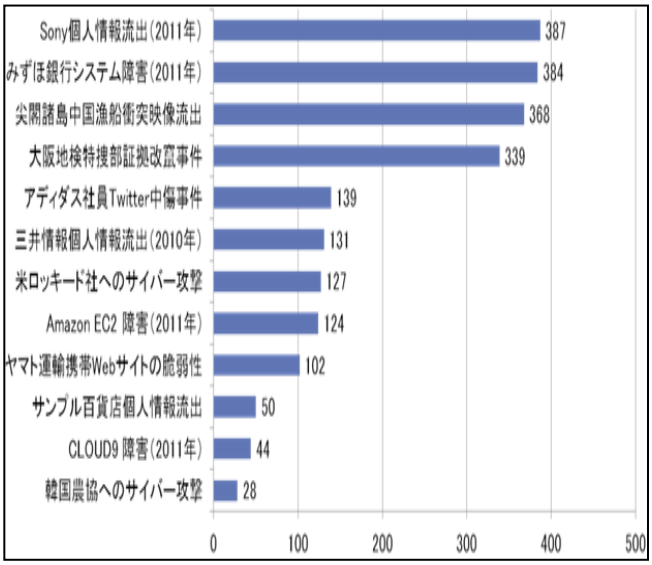

図 4.1.1 事例/事故のキーワード分析結果(N=401) [1]

なお、本調査についてはＰマーク取得事業者が多数含まれていることから、「個人情報流出」についてはマイナーな事例であっても認知が高いと想定したが、結果は、他分野と同程度であった[1]。

4.1.2 用語のキーワードについて

情報セキュリティ用語としてのキーワードは、新しい技術、ぜい弱性、脅威、などを理解する上で必須の知識である。とくに、話題になったキーワードに対する素早い認知は重要である。

2011 年度の調査では、事件/事故のキーワードと整合する用語、インシデント調査[6]で取り上げられている用語、および IPA の十大調査結果[7]をもとに候補を抽出して、検索エンジンでのヒット数や Google Trend などを活用して用語を絞り込み、最終的に決定した。これを、表 4.1.2 に示す。

表 4.1.2 調査に用いた用語のキーワード(2011 年度)

SQL インジェクション
BCP/BCM
インシデントハンドリング
ボットネット/ゾンビ PC
Gumblar(ガンブラー)
SAS70/SSAE16
Android 向けウィルス
マッシュアップコンテンツ悪用型
Stuxnet
Night Dragon
Operation Aurora
マン・イン・ザ・ミドル(中間者)攻撃
Sys Trust
XSS(クロスサイトスクリプティング)
Jailbreak
APT 攻撃
ゼロデイ攻撃
標的型攻撃
短縮 URL
ISAE3402
Spearphishing(スピアフィッシング)

表 4.1.2 の用語のキーワード別の結果を図 4.1.2 に示す。

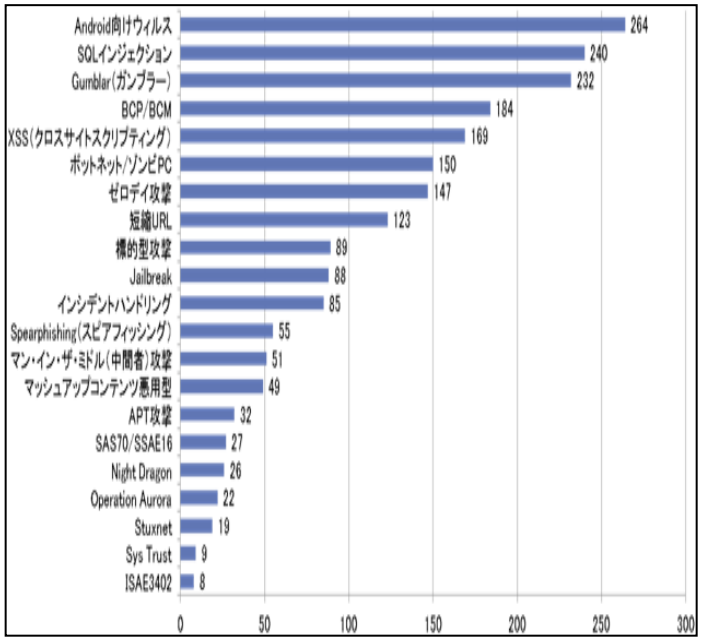

図 4.1.2 用語のキーワード分析結果 (N=347) [1]

図 4.1.2 からは、「Gumblar」「スマートフォン」「BCP/BCM」などの 2009 年以降話題になった用語のキーワードに対する回答数が多い一方で、「APT 攻撃」や「監査」分野の用語に対する回答数が少ない。なお、「APT 攻撃」の認知度が低いことについては、調査が 2011 年の 7 月～8 月に実施されており、国内における「APT 攻撃」が顕在化した 9 月以前の調査であったためである。この結果について、組織の情報セキュリティ関係者がマスメディアによる報道に大きな影響を受けていることが分かる。

4.2 2012 年度でのキーワード調査

4.2.1 事例/事故のキーワードについて

2012年度の「情報セキュリティ調査」における過去の事例/事故のキーワードの認知について調査した。その結果を、図4.2.1 に示す。なお、2012年度の過去の事例/事故の調査にあたっては、2011年度に作成した表4.1.1をベースにして2012年度にマスメディアで大きく報道されるなどした項目を追加し、知名度が減ったものを削除した。

図4.2.1の結果を見ると、2011年度と同様に一般的に有名な出来事件/事故のキーワードについては320の有効回答のうち、200 以上の組織が、知っていると回答している[2]。なお、2012年度に新しく追加した「Google 利用規約/プライバシポリシ統一」については、事件/事故のキーワードとは言えないが、回答者のうち184以上の組織が知っており、認知されていることが分かる。その他の情報セキュリティ関連の事件/事故のキーワードについては50 件～100 件程度であり、その多くは日本で発生もしくは何らかの影響が出たものである。一方、海外で発生した事例/事故のキーワードについては回答数が30以下であり、関心が低い。

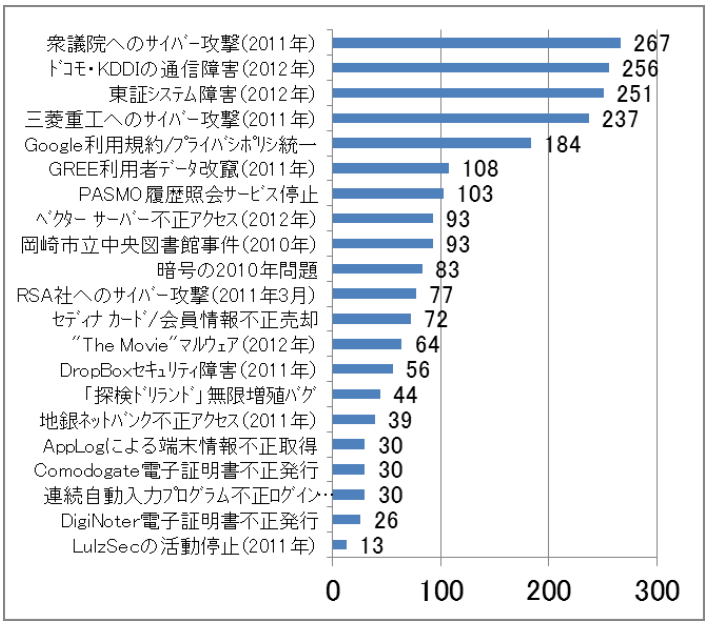

図4.2.1 事例/事故のキーワード分析結果(N=320) [2]

4.2.2 用語のキーワードについて

2012年度においては、2011年度と同じく、2012年度において社会問題となり日本のマスメディアで大きく報じられた用語のキーワードを選んで追加・削除した、「コンプリートガチャ」、「Anonymous」、「スマートフォン向けフィ

ッシングサイト」などは、回答が200を超えている。「シングルサインオン」は、セキュリティ用語として定着している結果と考えられる。一方、私物デバイスを業務に利用するBYOD は79 件であり、マスメディアでは広く取り上げられているにも関わらず、情報セキュリティ関係者には、あまり定着していないようである。

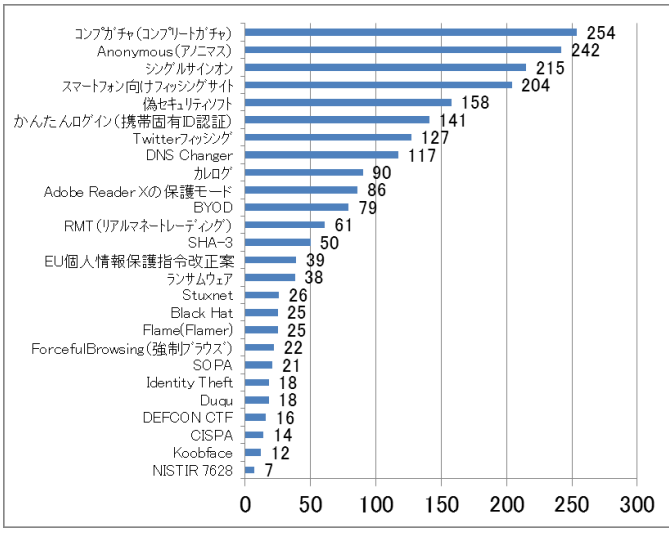

図4.2.2 用語のキーワード分析結果(N=317) [2]

図4.2.2からは、「標的型攻撃」の回答数は多いが、「Stuxnet」、「Duqu」、「Flame(Flamer)」など実際に発生した攻撃や手法への回答数は30 件未満と低い。以上のことから、総称的な用語のキーワードは認知されているが、具体的な内容については理解が不十分なことが推測される。

4.3 情報セキュリティに関する認知率の組織規模別の分析

組織の情報セキュリティに関する認知度を用語への回答数の合計を用いて評価する。ここでの仮設としては、組織が用語を多数知っている場合には、組織の情報セキュリティのアウェアネスのレベルが高いと考えられることに基づいている。

また、本節では、組織規模のパラメータとして、従業員数を用いた。これは、調査に、NPOや官公庁が含まれていて、資本金や売上がないため、これらを用いることができないからである。また、組織の情報セキュリティの教育はすべての従業員を対象とすることからも、従業員数が適していると考えられる。

組織別の全体の用語に対する回答割合を認知率と定義して用いる。この認知率を組織の規模別に分析したものを図4.3.1に示す。図中の0-50人の組織の用語全体に対する組織全体の平均の認知率が、0.19であることを示す。

図4.3.1からは、組織の規模と認知率に比例関係があることが分かる。すなわち、規模の大きい組織ほど、認知率が高い。ただし、5,000～10,000人の規模の組織の認知率が低い。この多くは官公庁であり、官公庁は規模が大きいが、用語についての認知率が低く、今後、高める必要ある。

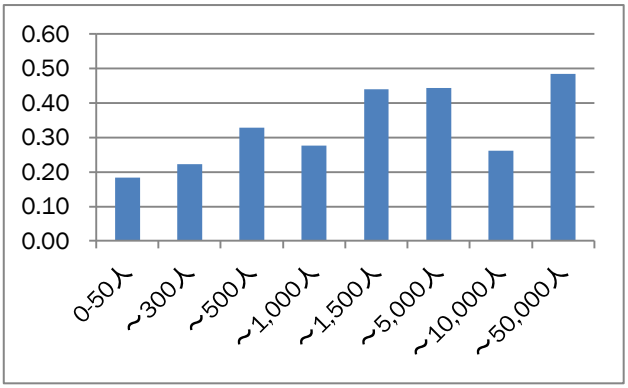

図4.3.1 従業員規模別の認知率 (N=347)

次に、用語別の組織規模別の認知率を表4.3.1に示す。この表では、0.6を超えるものについて色を付けている。この表からは、すべての規模の組織で0.6を超えているものは「Android向けウィルス」のみであり、「Gamblar」がこれに続いている。しかし、多くの技術的な用語については認知率が極めて低い。また、多くの用語で、認知率は組織の規模に関係があり、図4.3.1と同様な傾向が見られる。

表 4.3.1 用語別・組織規模別の認知率 (N=347)

	0-50	300	500	1,000	1,500	5,000	10,000	50,000
SQL インジェクション	0.49	0.59	0.82	0.61	0.88	0.80	0.33	0.67
BCP/BCM	0.23	0.48	0.68	0.65	1.00	0.85	0.50	0.83
インシデントハンドリング	0.15	0.24	0.23	0.26	0.13	0.40	0.00	0.17
ボットネット	0.25	0.32	0.55	0.43	0.88	0.85	0.50	0.67
Gumblar	0.45	0.52	0.91	0.74	1.00	0.85	0.83	0.83
SAS70/SSAE16	0.05	0.06	0.05	0.04	0.13	0.20	0.17	0.33
Android 向けウィルス	0.61	0.63	0.68	0.61	0.88	0.95	0.67	0.83
マッシュアップ	0.11	0.11	0.09	0.13	0.13	0.15	0.00	0.17
Stuxnet	0.03	0.03	0.09	0.04	0.13	0.15	0.00	0.50
Night Dragon	0.05	0.08	0.00	0.09	0.13	0.00	0.00	0.33
Operation Aurora	0.04	0.03	0.05	0.04	0.13	0.15	0.00	0.33
マン・イン・ザ・ミドル	0.08	0.08	0.18	0.13	0.38	0.45	0.17	0.33
Sys Trust	0.02	0.02	0.00	0.00	0.13	0.00	0.00	0.17
XSS	0.29	0.41	0.59	0.57	0.63	0.75	0.33	0.67
Jailbreak	0.13	0.19	0.32	0.22	0.38	0.65	0.17	0.50
APT 攻撃	0.05	0.07	0.18	0.04	0.25	0.05	0.00	0.50
ゼロデイ攻撃	0.25	0.34	0.55	0.39	0.50	0.80	0.33	0.67
標的型攻撃	0.15	0.18	0.36	0.30	0.63	0.40	0.50	0.67
短縮 URL	0.27	0.21	0.45	0.30	0.63	0.55	0.83	0.67
ISAE3402	0.02	0.03	0.00	0.00	0.00	0.00	0.00	0.00
スピアフィッシング	0.12	0.08	0.14	0.22	0.38	0.30	0.17	0.33
平均	0.18	0.22	0.33	0.28	0.44	0.44	0.26	0.48

4.4 組織の情報セキュリティのアウェアネス

4.1章～4.3章に述べた結果から、以下のことが分かる。組織の情報セキュリティ関係者は、事故/事例、用語などのキーワードについて、一般誌などで取り上げられた総称的なキーワードについては浸透しているが、事件/事故などに関係する具体的な用語についての認識は十分ではない。この傾向は2011 年度[1]、2012年度で同様である[2]。

情報セキュリティ担当者が、自組織の情報セキュリティレベルを高め、事故や攻撃による被害を未然に防ぐためには、マスメディアで一般に報道されて知るだけではなく、率先して、情報セキュリティに関する事故/事例や新しいキーワードを学び取る取り組みが必要である。

また、小規模な組織ほど情報収集力が不十分であり、用語の認知が低い。今後、中小企業に向けた情報力の強化が必要と考えられる。

5. まとめ及び今後の研究課題について

本研究では、2011年7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、407件の回答が得られたものと、2012 年8 月に「情報セキュリティ調査表」を郵送し、335 件の回答が得られたものをベースに分析した。

過去の事例/事故やマスメディアで大きく報じられたキーワードについての認知度は高いが、具体的な内容を示す用語のキーワードについては認知度が低く、結果として、情報セキュリティの事件/事故や用語についての理解が十分とは言えない。この傾向は、複数年度でほとんど変わらなかった。

自組織の情報セキュリティレベルを高め、事故や攻撃による被害を未然に防ぐためには、組織の情報セキュリティ関係者は自主的に学びとる努力が必要である。一方で、情報セキュリティ研究に関わる我々研究者は、組織の情報セキュリティ対応を具体的に進める為の課題や工夫を出来るだけ判り易く明らかにする必要がある。本研究が、実務担当者の理解と、対策を進める一助になればと考える。

なお、本稿で参照した調査の詳細な結果については、情報セキュリティ大学院大学原田要之助研究室のホームページで公開している。

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

6. 謝辞

本論文の作成にあたっては、2011年、2012年に渡って、アンケートへ回答にご協力を頂きました企業や団体、組織の皆様に感謝いたします。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内の特別支援学校の皆様に感謝いたします。

さらに本研究にあたっては、情報セキュリティ大学院大学の同僚の教授、調査を実施して仮説を設定して分析を遂行してくれた原田研究室の学生・客員研究員、大学事務の皆様に感謝いたします。

7. 参考文献

[1] 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

[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, “組織・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、220

[3] 西澤正己、孫媛、柿沼澄男、日本の論文誌や科研費における研究組織の協力体制や動向の可視化、情報知識学会誌、Vol. 18, No. 2、2008

[4] 西澤正己、孫媛、柿沼澄男、日本の論文誌や科研費における研究組織の協力体制や動向の可視化、情報知識学会誌、Vol. 18, No. 2、2008

[5] 岩崎 正治、原田 要之助、“ＡＰＴを踏まえた情報セキュリティに求められる要素についての考察”、システム監査学会設立25 周年記念第24 回公開シンポジウム講演予稿集、pp. 12-19

[6] 特定非営利活動法人日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ、情報セキュリティ大学院大学_原田研究室_廣松研究室, "2011年情報セキュリティインシデントに関する調査報告書Ver. 1.2"、2011

[7] IPA、2011年版 10大脅威 進化する攻撃、IPAホームページ（調査は毎年実施されている）(http://www.ipa.go.jp/security/vuln/documents/10threats2011.pdf、2011年6月)

付図 用語別・組織規模別の認知率（表 4.3. 1 の図示）