Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

情報セキュリティ意識向上のための方策の一考察 −セキュリティに関する教育（研修）に着目して−

大賀　麻衣子[†1]　　原田要之助[†2]

近年,ISMS やＰマークなどの情報セキュリティ認証を取得する組織は大きく増加した.情報セキュリティに関するルールを制定したり,教育（研修）を実施したりする情報セキュリティ対策基盤を作る段階を終え,今後の方向性を模索している組織も多いと考える.情報セキュリティ対策をより効果的に推進するためにはひとりひとりのセキュリティ意識を向上させることが必要であると考え,その効果的な方策を模索した.
本稿では,その方策の一つとして考えうる「セキュリティに関する教育（研修）」に焦点をあてて調査を行った.

Study of measures for information security awareness improvement -focus on education (or the training) -

MAIKO OGA[†1]　　YONOSUKE HARADA[†2]

In the recent years, the organizations, which have acquired the third party certification about the information security, such as ISMS or Privacy mark, have increased. Through establishing rules of the information security and being carried out education (or the training), a stage to make the base of information security measures was over, there are many organizations groping for future directionality to advance to the next stage. The improvement of security awareness of the individual is a key factor to enhance information security effectively, and grope for effective ways of that purpose.
This report focuses on education or training of information security as one of the measures for individual awareness.

1. はじめに

ISO/IEC27000 シリーズが 2013 年に大きく改訂された.情報セキュリティのガイドラインである ISO/IEC27002 についても例外ではない.人的資源のセキュリティの重要なテーマとして「7.2.2 情報セキュリティの意識向上,教育および訓練」の項目については記述が改訂前（2005 年版）の 2 倍以上となり,内容についても,情報セキュリティの教育および訓練に盛り込むべき内容,対象者やタイミング,理解度の確認について触れるなど,より詳細まで踏み込んだ内容となっている[1][2][3].改訂前のものでは,教育・訓練の概念的なことしか書かれていなかったため管理策として不十分であり,具体的に何をやってよいのかわからないという声が多かったことが関係している.一方,近年,ISMS や P マークなどの情報セキュリティ認証を取得する組織は大きく増加した[4][5].ISO/IEC27000 シリーズの改訂の要望が出てきたのは,それまで組織(企業)が「情報セキュリティ」を意識することがほとんどなかった段階から,一段階進んだとも考えられる.つまり,個人情報保護法の制定や情報セキュリティリスクの高まりに伴い,ISMS やＰマークといった情報セキュリティ認証を取得する組織が増えた.また,情報セキュリティのルール制定や教育（研修）の実施などにより基盤が整備されたと考え,さらに向上させる方へ意識が向いたとも考えられる.

情報セキュリティ対策を効果的に実施するには,形式的ではなく実務的なルールの導入や,従業員のやらされ感の解消が必要である.そのためには,対策の検討プロセスは,トップダウンだけではなくボトムアップも必要なのではないか.従業員の個々の意識付け（気づき）が,ボトムアップの重要な要素である.そのため,本稿においては,意識向上の方策の一つとして考えうる「セキュリティに関する教育（研修）」に焦点をあてて調査を行った.まず,本稿においては企業や組織におけるセキュリティ教育の現状を理解するために,公表されている情報セキュリティ教育のガイドライン,公開情報による企業における実践例の分析,情報セキュリティのアンケートによる調査を行った.さらに,情報の利活用教育が初等・中等教育に広がる中で,学校における情報セキュリティ教育の現状についても,指導要領の改定内容の分析を通して調査した.

2. セキュリティ教育（研修）のためのガイドライン類

2.1 総務省「国民のための情報セキュリティサイト」ー企業・組織の対策ー

†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

Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

総務省は利用方法に応じた情報セキュリティ対策を講じるための情報提供の場として「国民のための情報セキュリティサイト」を公開している.「基礎知識」「一般利用者の対策」「企業・組織の対策」から構成されており,そのうち「企業・組織の対策」は,「組織幹部のための情報セキュリティ対策」,「社員・職員全般の情報セキュリティ対策」,「情報管理担当者の情報セキュリティ対策」と,企業・組織における階層・役割別の構成で記述されている.

また,「情報セキュリティポリシーの導入と運用」[6]には,「情報管理担当者として十分留意すること」が述べられている.その一つとして「情報セキュリティポリシーの導入に際しては,社員や職員の教育,啓発の実施方法を十分に考慮する」との記載があり,下記の項目が挙げられている.

・情報セキュリティポリシーを積極的に社員や職員に普及させ支援する.
・情報セキュリティポリシーが遵守され,有効に機能しているか,業務の妨げなどになっていないかなどを日常的にモニタリングする.
・情報セキュリティ対策の評価を行い,経営幹部へ報告を行うなど,情報セキュリティポリシーの導入だけでなく継続的に運用を行う.

また,「情報セキュリティ教育の実施」については情報セキュリティ教育を実施するうえで心がけるべきポイントが以下のように記載されている.

・策定した情報セキュリティポリシーに関しては,組織幹部も含め全社員や職員に情報セキュリティ教育を実施して遵守することを徹底しなければならない.
・分厚い資料を渡したり,形だけの方針や指針を伝えたりするだけではなく情報セキュリティポリシーを意識させる仕組みが必要.
・すべての社員や職員が遵守するからこそ,情報セキュリティポリシーに意味があり,情報セキュリティ対策が効果的になる.
・情報セキュリティに対する意識を社員や職員一人一人に啓発することが,企業や組織における大切な情報セキュリティ対策のひとつ.

2.2 IPA（情報処理推進機構）「情報セキュリティ対策実践情報」

IPA では,総務省の「ガイドライン」よりも詳しく,セキュリティの目標について「サービスの提供 VS セキュリティ」「操作性 VS セキュリティ」「セキュリティのコスト VS 損失のリスク」などの相反する要素を考慮することが述べられている[7].

更に,図 1 に示すように,IT 利用の度合いや役割に応じて説明を分けて記載している.同じ IT ユーザでも,情報システム部門責任者とエンドユーザ・ホームユーザ[a]では求められるセキュリティ対策の内容やレベルが異なるし,ネットワークサービス事業者や IT ベンダもまた,求められるセキュリティ対策の内容が異なるためである.これを組織内に置き換えて考えてみると,部署によって状況が異なるため,それぞれに合わせた課題・リスクの認識と対策の実践が必要になる.

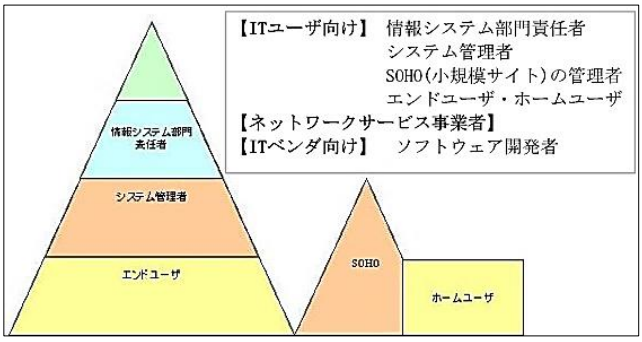

図 1：IPA が想定する「情報セキュリティ対策実践情報」利用者（出典：IPA[7] に追記）

3. 企業・組織の実施例

3.1 RICOH 社の例

RICOH 社では,「情報セキュリティ教育の組織学習の状況」を Web サイト上に公開している.「グループ ISMS の情報セキュリティレベルを継続的に向上させていくためには,全員参加による多面的な情報セキュリティ教育が有効」[8]として,さまざまな教育プログラムを通じて組織学習を実施している.

図 2 に示すように階層別教育においては,全従業者向け教育（e ラーニング）,管理者向け,経営者向け教育に分かれているだけでなく,全従業者向けには基礎編と実践編,管理者向けには初級編と実践編のレベル別の教育プログラムがあるところが特徴的である.

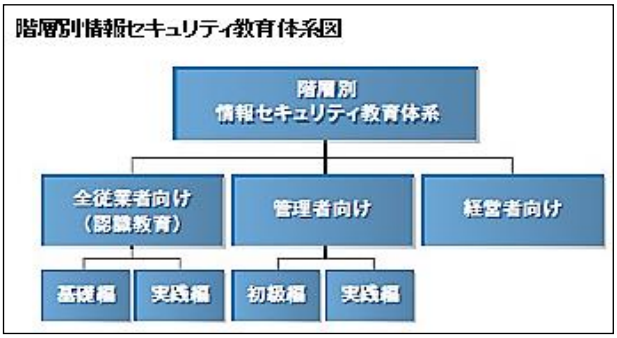

図 2：階層別情報セキュリティ教育体系図
（出典：RICOH 社[8]）

更に,階層別教育とは別に ISMS 推進者や内部監査員を対象にした役割別の教育プログラムがある.この役割別教育では,最初に学習する「基礎教育」と 2 年目以降に学習する「フォローアップ教育」で構成され,習熟度に応じた教育が行えるように工夫されている.

a) IPA では組織において情報システムを利用するエンドユーザ,家庭でコンピュータを利用するホームユーザという区別をしている[7].

Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

3.2 情報セキュリティ報告書にみるセキュリティ教育実施例

近年, 企業は CSR 報告書において, 情報セキュリティ対策の方針や実施状況を取り上げる事例も出てきている. 経済産業省[9][10]では, CSR 報告書等の一部として情報セキュリティへの取り組みを情報開示するよりも「情報セキュリティ報告書」単体として発行する方が効果的として「情報セキュリティ報告書モデル」を提示している. このモデルは, 昨年, ISO/IEC27014 情報ガバナンスにも取り上げられて国際規格となっている. 現時点では「情報セキュリティ報告書」単体として報告している企業はまだ少ないが, 調査した 9 社[b]においては全社員向けのみならず階層別・役割別の教育(研修) を行っているところが多い. 標的型攻撃に対する教育 (訓練) やセキュリティ人材の育成についての記述も多くの報告書に共通して見られた. 今後は, 年度による特徴の変化にも視点を向けて調査・分析を継続する.

3.3 原田研究室アンケート調査にみる組織における情報セキュリティ教育の実態

情報セキュリティ大学院大学の原田研究室は毎年, 日本国内の P 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, ランダムに選んだ 4,500 の情報セキュリティ担当者を対象とした「情報セキュリティ調査」を実施している. 2013 年は 4500 通に対し有効回答数は 367 であった[20]. 「従業員の教育」についての調査結果では, 年間「1 回」というところが一番多く, 続いて, 「2 回」, 「実施していない」と回答した組織が多かった.

「教育の効果の確認」に関しては, 図 3 に示すようにテストを実施しているという回答が圧倒的に多いが, 「特に実施していない」という回答数が多いことも目を引く.

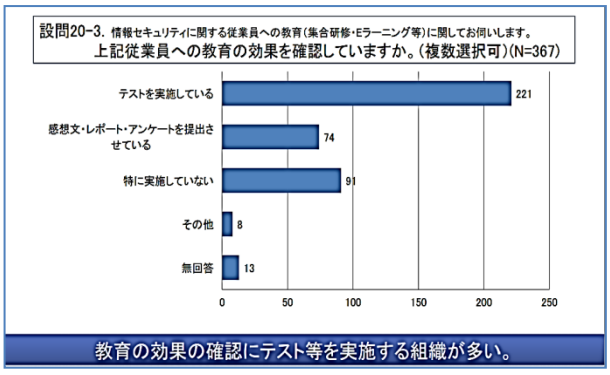

図 3：従業員への情報セキュリティ教育の効果確認
(出典:2013 年情報セキュリティ アンケート調査結果[20])

階層別や年次別の研修と比較して, 全従業員をホールに集めて行うような集合型の研修の場合は, テストの実施や感想文・レポート・アンケートの集計を行うのが難しいという実態があるのかもしれない.

2014 年度の「情報セキュリティ調査」においては, 「全従業員向け」に加えて「全従業員以外の特定の従業員」に対する教育に関する設問を設定した. 特定の従業員といえば, システム部門など特定の部門向けに行われることが想定される. しかし, 特定のタイミング (異動・昇進・昇職時や特定年次など), や派遣・委託先社員などの教育については今まで調査が行われていなかったため, 項目に追加した.

現在までに得られた回答からサンプルとして 50 回答を分析した結果, 82%の組織から「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とした情報セキュリティ教育を行っている」ことがわかった. その教育の対象となるのは, 図 4 に示すように, 新入社員や転入社員(新たに企業(組織)に所属した従業員)が多いが, その他派遣社員や委託先社員に対して情報セキュリティ教育を行っている組織も少なからずあることがわかった.

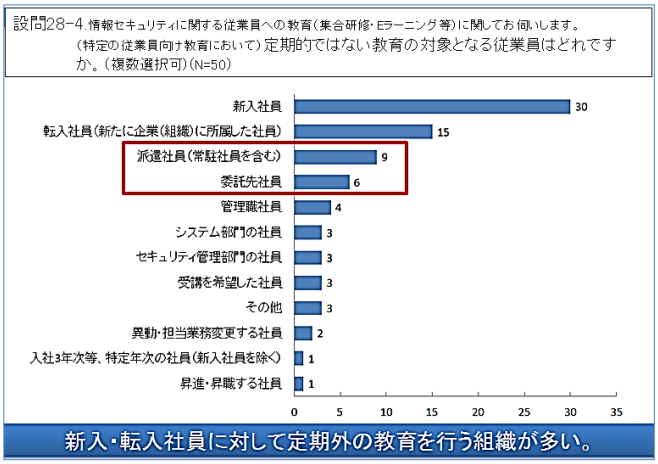

図 4：特定の情報セキュリティ教育の対象となる従業員
(2014 年度情報セキュリティ調査より作成)

教育の効果の確認に関しては, 図 5 に示すように, 全従業員向けの定期的な教育と同程度のテストを実施している組織が一番多い. より詳細なテストや感想文・レポート・アンケートを提出させている組織も存在する. しかし「特に実施していない」の割合は全従業員向けのとき (10%) よりも大きく (20%) なった.

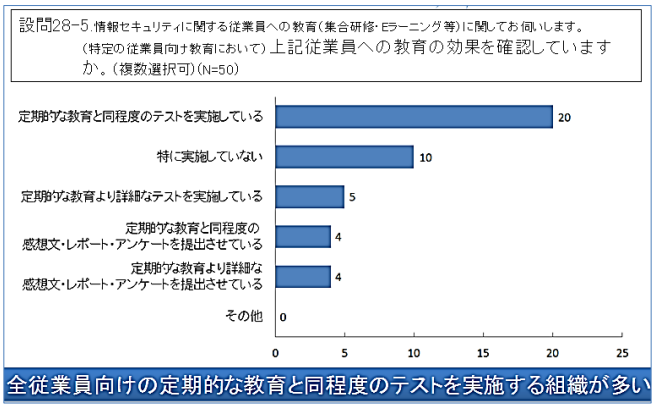

図 5：特定の従業員への情報セキュリティ教育の効果確認
(2014 年度情報セキュリティ調査より作成)

b) NEC [11],NTT データ[12],RICOH [13] (2010 年以降 CSR 報告書に統合),キヤノン[14],サジェコ[15],ジャパンシステム[16],日立[17],富士ゼロックス[18],富士通[19]

Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

今後は,組織の種類や規模により教育手法などの違いも想定されるので,これらの切り口からも分析を行う予定である.

3.4 小学校～高校の指導要領改訂について

企業（組織）に入る前,つまり学生時代にどのような教育を受けたか（あるいは受けなかったか）によっても,入社後に「情報セキュリティ」に対してどのような意識を持つのかに差が出る可能性が高いと考えられる.

高等学校には平成 15 年度に必修科目として普通教科「情報」が新設され,平成 20 年に公示された小中学校の指導要領では「情報を適切に主体的,積極的に活用するための学習活動を充実させること」と明記された[30].小学校には「情報」に関する教科は設置されていないが,総合的な学習や各教科で情報教育を行っている.中学校では,技術・家庭科で情報に関する基礎的な内容が必修化されている.高校では,平成 11 年改訂の高等学校学習指導要領にて「情報 A」「情報 B」「情報 C」という 3 種類の科目が設置され,その中から 1 科目以上を選択して履修するようになった[21].義務教育段階において情報手段の活用経験が浅い生徒でも十分履修できることを想定して「情報 A」を,コンピュータに興味・関心をもつ生徒が履修することを想定して「情報 B」を,情報社会やコミュニケーションに興味・関心をもつ生徒が履修することを想定して「情報 C」を設置した[27].2008 年度の科目実施状況を表 1 に示す.「情報 A」を選択している高校の割合が一番多いのは,生徒によって小中学校での学習内容に差があると想定すると,妥当と言えるだろう.

表 1：2008 年度の埼玉県立高校における科目実施状況

2008 年度の埼玉県立高校における科目実施状況

	目標	実施校数	割合
情報 A	「情報活用の実践力」を養う	133	74.3%
情報 B	「情報の科学的理解」を養う	22	12.3%
情報 C	「情報社会に参画する態度」を養う	24	13.4%

(出典)　埼玉県立高校教育指導課　　平成 21 年度教科「情報」スキルアップ研修会資料

（出典：藤巻[21]）

平成 21 年に改訂された高等学校学習指導要領では,図 6 に示すように,情報手段の活用経験が浅い生徒の履修を想定して設置した「情報 A」を発展的に解消し,「情報 B」と「情報 C」を柱として「社会と情報」（主として情報社会に参画する態度を重視）と「情報の科学 」（主として情報の科学的な理解を重視）が新設された[22].改訂では情報活用の実践力及び情報モラルに関する内容が共通に,かつ,より実践的に行われるように改善が図られている.

また,改訂後の高等学校学習指導要領では,「情報」以外の教科,例えば「地理歴史」「公民」などの教科に関しても,「資料の収集，処理や発表などに当たっては，コンピュータや情報通信ネットワークなどを積極的に活用するとともに,生徒が主体的に情報手段を活用できるようにすること.その際，情報モラルの指導にも留意すること」[23]などと,各教科の「各科目にわたる指導計画の作成と内容の取扱い」に記載がある.「情報」の授業として学ぶだけではなく他の教科の学習においても実践することで,生徒にとってはより理解を深め習得しやすいと考えられる.なお,改訂後の内容は平成 25 年 4 月に高校に入学する生徒から順次適用されている.

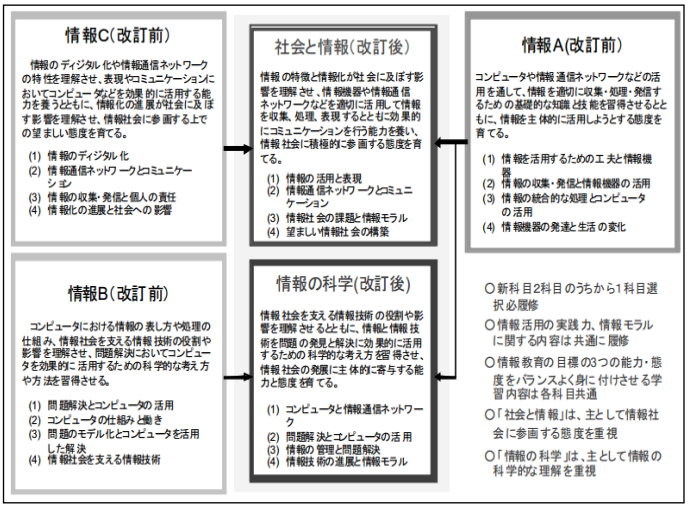

図 6：高等学校学習指導要領の改訂について（出典：文部科学省　高等学校学習指導要領解説　情報編[22]）

指導要領としては小・中・高等学校を通して体系的・系統的に学ばせることを目指している.他方,指導力のある教員の不足や,「情報」が受験に直結しない科目であることから,「情報」の授業の形骸化も懸念されている.東京大学が今年4月に入学した学生3千人を対象に高校での情報の履修状況を調べたところ,15%が「一部もしくは全てが別教科の内容だった」と答えた.「情報の授業内容かどうか分からなかった」との回答も32%に上った[24].

情報処理学会は大学入試センター試験の受験科目に「情報」科目を追加することを目指しており,昨年,情報の全国模擬試験を初めて実施した.情報科目の入試問題を試作し,これを使った模試を実施することでフィードバックを得ながら,適正な範囲・内容・水準を持った試験問題・試験方式の構築を目指す[24].

大学入試における「情報」科目は,専門科目としては大学入試センター試験に「情報関係基礎」[c]として用意されているほか,愛知教育大学などですでに実施されてきた.また,2013年度からは明治大学の情報コミュニケーション学部の定員450名のうち20名[d]について,情報を必須科目の1

c) 専門教育を主とする農業，工業，商業，水産，家庭，看護，情報及び福祉の８教科に設定されている情報に関する基礎的科目が出題範囲.出題科目として指定しない大学も多い[26][27].
d) 従来の A 方式（外国語,国語,地理歴史・公民・数学）とは別に B 方式（外国語,情報総合,数学）を導入した[28].

つとした方式が導入されている.さらに2016年からは慶應義塾大学総合政策学部・環境情報学部でも,入試選択科目の1つとして情報を追加することがアナウンスされている.入試における「情報」科目の追加は,時代背景から今後導入拡大が求められている一方で,多くの大学にとっては実現が難しい面もある.大学にとっても高校にとっても入試科目・受験科目は増やしたくないというのが実情であり,情報入試を選択する受験生が少なければ導入・存続は難しい.すでに情報入試を導入している大学でもこれを選択する受験生はまだ少数[24]である.情報入試研究会[e]は今後,2015年まで毎年5月に模試を実施し,調査・検討を進める.その成果をもとに各大学・学部がそれぞれの方針やレベルに応じて,2016年2月実施の実際の大学入試において情報入試科目を導入できるようにしたい考えだ[24].

4. 先行研究

4.1 実技と講義を融合させた教育の実践

指導要領の改訂を通して,高校までの授業において,積極的にコンピュータや情報通信ネットワークなどを活用する中で情報モラルやセキュリティについても学べるように,という方針で教育が行われていくようになることが期待される.

藤巻[21]は「情報」科目の導入時からの自身の勤務校での実践例を通して考察を行っている.「実技と講義を融合させた教育の実践」としてExcelやPowerPoint等の実習を行うだけではなく,セキュリティ意識の向上を目指すために下記のように様々な工夫をしている.

(1) アカウント管理
- 入学時に,生徒 ID,初期パスワード,メールアカウントを付与し,4月最初の授業で初期パスワードを変更(英数字を混ぜて8文字以上).
- パスワード忘れや紛失時は,パスワードリセット申請書に氏名・理由を書かせて担当者に提出.

(2) アクセス制御
- 課題の配布や提出をすべてアクセス制御されたLAN上で行う.
- 配布フォルダは読み取りのみ,提出フォルダは書き込みのみ許可.

(3) 知的財産権
- 授業の一環としてWebページを作成する際,他人のページの引用や写真等の利用を希望する場合は,希望者本人が直接,自分のメールアカウントで県立学校間ネットワークシステムを利用して利用許可願のメールを送信.使用許可メールの受信,または正式な書類等で手続き完了したもの以外は利用させないことで,電子メールのマナーを覚えさせると共に,人の著作物を守ることの重要さを理解させる.

どれも,日々の学習の中で身につけられるようになっている.藤巻[21]の考察において期末考査は「暗記が問われる設問よりも実習で行った範囲の設問の方が,平均点よりも正解率は高い」結果となった.実技と講義を融合させた教育が効果的であると言える.

一方,星野[30]の研究では,図7に示すように教員に対する教育(研修)において「伝達型(集合研修)」と「ファシリテーション型(ワークショップ型)」と比較している。「伝達型(集合研修)」は「一斉に多くの人に教育することができることや,知識を効率よく獲得するためには有効な方法である」が,「研修を受ける対象者が受動的な態度になってしまいがちになることや,個々のおかれた状況とは関係なく研修が行われるため,たとえ意欲があったとしても予備知識が不足している場合には苦痛を強いるだけの研修になりかねない」[30].一方,「ファシリテーション型(ワークショップ型)」は,「参加者が主体的にコミュニケーションを図るために,ファシリテーター(講師)が一方的な関わりではなく,受講者の関わりなども交え,ヒントを与えたりして関与することで,気づきを進めていく」[30].

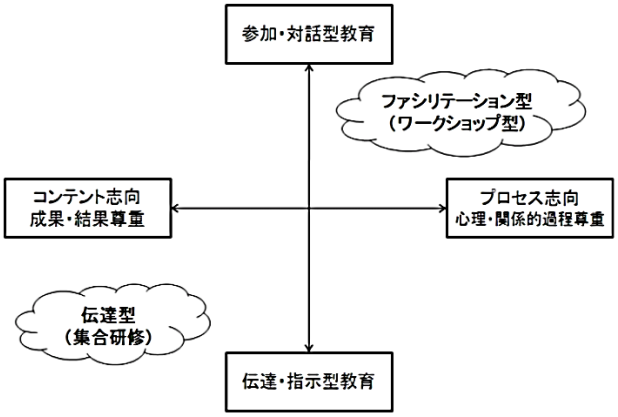

図7:教員に対するセキュリティ教育のタイプ
(出典:星野[30])

このことから,「予備知識のあるなしに関わらず誰でも取り組める環境としてのツールが必須」[30]ではあるものの,参加者間の相互コミュニケーションをもとにして進めていく「ファシリテーション型(ワークショップ型)」の方が望ましいとしている.

原田他[31]の研究においても,SNSを題材にしたケーススタディの教材を開発して,神奈川県内の女子大学の経営学の学習の一部として実証実験を実施している.

学生だけのリスクだけでは無く,学生のリスクが関係者(大学や企業)にとってインパクトがあるようなストーリ

Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

ー[e]を設定し，同時に，大学や企業にとっても SNS のリスクに関係することを併せて理解できるものとなっている．そして，SNS の公開設定，情報の広がり方の認識，問題が発生したときにどのような影響が出るかについて，ケースメソッドの事前と事後での理解度の違いは図 8 に示す通りである．リスクマネジメントで重要となる「情報の広がり方」「問題発生時の影響」の知識はケースを通じた学習で理解が深まることを確認できた．

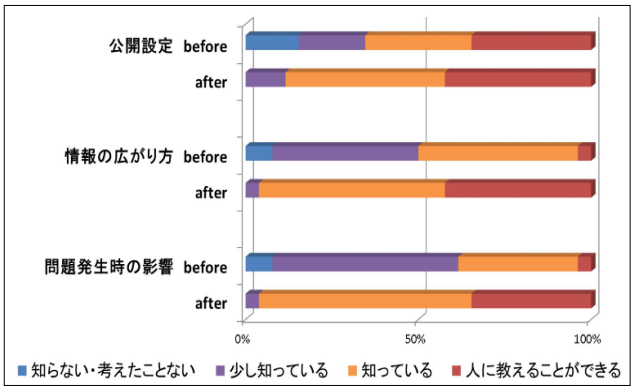

図 8：学習効果について（SNS の設定，情報の拡散，問題についての理解の変化）(出典：原田他[31])

4.2 情報セキュリティの脅威への対応

セキュリティ教育では，実践が重要である．実践を通して従業員一人一人がセキュリティ意識を深め，「気づき」が促されなければならない．ENISA[32]，NIST[33]においては，教育の前段階においてセキュリティ意識を全従業員に根付かせることが必要だとしている．個人（各従業員）が情報セキュリティに関する懸念を認識し，懸念内容に応じた反応をするためである．

また「セキュリティ教育」においては教育対象者（企業であれば従業員）全体の底上げが必要である．Seppo 他[34]によると，不注意な従業員は，情報セキュリティに対する脅威の鍵となる．それ故に，全ての従業員はセキュリティについて認識する必要があるだけではなく，組織の情報セキュリティポリシーと手順に従う必要があり，そのためには，以下のことが必要であると述べている．

(1)情報セキュリティポリシーに迅速にアクセス可能であるだけではなく，従業員が情報セキュリティポリシーから必要とする情報を迅速に見つけられることが重要である．

(2) 情報セキュリティポリシーの情報量が，従業員のニーズに対して十分である必要がある．例えば，情報セキュリティポリシーが長すぎたり短すぎたりしてはいけない．

(3)情報セキュリティポリシーが従業員にとって容易に解釈できるものでなければならない．例えば，情報セキュリティポリシー内で使われる用語は従業員にとって理解しやすいものでなければならない．

(4)情報セキュリティポリシーの情報が従業員の仕事と密接な関連性があると認識されること，情報セキュリティポリシーの情報が十分に仕事の現状とあっていることを確実にすることが重要である．

(5)脅威の評価は情報セキュリティポリシーに従うことに対する態度に，大きな影響を与える．従って，情報セキュリティの担当者によって，従業員が情報セキュリティの脅威があることや，脅威の大きさ・広まる速さに気付かされることが重要である．

((1)～(5)は Seppo 他[34]p. 8 を著者にて意訳)

原田研究室における 2014 年度の「情報セキュリティ調査」において，情報セキュリティポリシーを定着させるための工夫や従業員の意識について調査も行っている．今後分析を進めていく中で，Seppo 他[34]や Johnston & Warkentin[35]が言及している「情報セキュリティポリシーを守らせるためには脅威を感じさせることが効果的」という点についても検証を進めていく．

5. まとめ

「セキュリティに対する教育（研修）」を実施することが目的ではなく，受講者が教育（研修）の内容をどのように理解し，実行に移していけるか，ということが重要である．この視点から，今回の調査・分析を踏まえてると，下記の留意点を考慮すべきである．

(1) 全体向けの研修に替えて，もしくは，加えて，役職別，職種別，役割別，理解度別などの個別の研修を実施すると，受講者はより身近なものとして考えられ，気づきが増えるのではないか．

(2) 一方的となる座学だけではなく，受講者が自ら考えたり実践できたりする参加型の研修の方が身につきやすい（但し工夫が必要）．加えて，実践で身につける（＝職場内で）ことを継続することが必要ではないか．

(3) 研修終了後，時間をおいて再度テストを実施すると，より身につきやすいのではないか．研修の内容を暗記していることよりも，思い出したり日常業務に生かせたりすることの方が重要である．そのため，例えば「研修資料や社内 Web で調べてもいいが，受講生内で答えを教え合うのは NG」といったルールにするのがよいのではないか．

(4) 組織所属前（学生時代，前職など）に受けたセキュリティ教育の内容によって個々のセキュリティ意識に差異が出ているのではないか．

(5)「情報セキュリティ意識」を向上させるためには，「脅威」を認識させることが効果的なのではないか．罰則規定は有効なのか．

今後は，海外事例を含む先行研究の調査，海外におけるセキュリティ教育（研修）のためのガイドライン類の調査を継続して行う．原田研究室の 2014 年度

e) 女子大学生が企業にインターンシップで働くというシナリオをベースに，企業で見聞きしたことを SNS でつぶやいたことがきっかけとなって，情報漏えいに繋がる．この情報がネットワークに広まって，企業の戦略に影響を与え機会損失を招く．この結果，女子学生が大学を辞める事になり，大学には賠償請求される[31]というストーリー．

「情報セキュリティ調査」で得られた回答については組織の種類（企業、大学など）や規模による違いについても考慮しながら引き続き分析を実施する．「情報セキュリティ報告書」に対しての考察も引き続き実施し，報告書内で重点的に記載されている内容と社会的に注目されている事案の関係性が年度ごとに変化しているのかについての考察も行う．

謝辞 本研究にご協力いただいた情報セキュリティ大学院大学の教授等関係者，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．また，アンケートへの回答を頂きました企業や団体・組織の皆様，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申し上げます．

参考文献

1) 原田要之助, 「情報セキュリティマネジメント規格の改訂と問題点について」,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(10), 1-10, 2014-02-14
2) ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management, 2005 年
3) ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls, 2013 年
4) プライバシーマーク推進センター, （平成 25 年度）「個人情報の取扱いにおける事故報告にみる傾向と注意点」,
http://privacymark.jp/reference/pdf/H25JikoHoukoku_140825.pdf,2014/8/27 アクセス
5) ISMS 認証取得組織数推移,
http://www.isms.jipdec.or.jp/lst/ind/suii.html,2014/8/2 アクセス
6) 総務省,安心してインターネットを使うために 国民のための情報セキュリティサイトー企業・組織の対策ー,
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/index.html,2014/5/8 アクセス
7) IPA,読者層別：情報セキュリティ対策実践情報,
http://www.ipa.go.jp/security/awareness/awareness.html,
2014/5/14 アクセス
8) RICOH,情報セキュリティ教育,
http://www.ricoh.com/ja/security/management/activity/training.html,2014/5/8 アクセス
9) 経済産業省 企業における情報セキュリティガバナンスのあり方に関する研究会-報告書,
http://www.meti.go.jp/report/data/g50331dj.html,
2014/9/10 アクセス
10) 経済産業省 情報セキュリティ報告書モデル（改訂版）
http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf,2014/9/10 アクセス
11) NEC,情報セキュリティ報告書 2014,
http://jpn.nec.com/csr/ja/pdf/isr2014.pdf,2014/9/11 アクセス
12) NTT データ,2014 情報セキュリティ報告書,
http://www.nttdata.com/jp/ja/corporate/csr/security/pdf/2014/rep2014_all.pdf,2014/9/11 アクセス
13) RICOH,リコーグループ企業・IR サイト 2013 年度活動報告と 2014 年度活動計画,
http://www.ricoh.com/ja/security/management/project_report/,2014/9/11 アクセス
14) キヤノン,キヤノンマーケティンググループ情報セキュリティ報告書 2014,
http://cweb.canon.jp/csr/security-report/pdf/security-all2014.pdf,2014/9/11 アクセス
15) サジェコ,平成２５年度 情報セキュリティ報告書 第 1.03 版,
http://www.sajco.jp/sajco/pdf/2013_is_report.pdf,
2014/9/11 アクセス
16) ジャパンシステム,情報セキュリティ報告書,
http://www.japan-systems.co.jp/uploadfile/docs/csrrep121203.pdf,2014/9/11 アクセス
17) 日立,情報セキュリティ報告書,
http://www.hitachi.co.jp/csr/download/pdf/securityreport.pdf,
2014/9/11 アクセス
18) 富士ゼロックス,情報セキュリティ報告書 2014 年度,
http://www.fujixerox.co.jp/company/public/i_security/doc/i_security2014.pdf,2014/9/11 アクセス
19) 富士通,富士通グループ 情報セキュリティ報告書 2014,
http://img.jp.fujitsu.com/downloads/jp/jcsr/csr/management/security/2014/security2014.pdf,
2014/9/11 アクセス
20) 情報セキュリティ大学院大学 原田研究室,2013 年情報セキュリティ アンケート調査結果,
http://lab.iisec.ac.jp/~harada_lab/survey/2013/2013_questionnaire_result.pdf, 2014/7/3 アクセス
21) 藤巻 朗,平成 22 年度情報セキュリティに関する懸賞論文「情報セキュリティ意識を向上させるための教育について 高校における教科「情報」授業実践事例から、今後の PC 教育の在り方へ」,2010 年防衛調達基盤整備協会
22) 文部科学省 高等学校学習指導要領解説 情報編 平成 22 年 1 月,
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2012/01/26/1282000_11.pdf, 2014/7/2 アクセス
23) 文部科学省 高等学校学習指導要領 平成 21 年 3 月,
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2011/03/30/1304427_002.pdf, 2014/7/2 アクセス
24) 「情報」必修は名ばかり,日本経済新聞,2014 年 9 月 17 日（水）朝刊
25) INTERNET Watch,大学入試の「情報」科目、導入校拡大を～5 月 18 日に全国 4 会場で模擬試験,
http://internet.watch.impress.co.jp/docs/news/20130306_590677.html,2014/9/29 アクセス
26) 河合塾, センター試験について理解しよう,
http://www.keinet.ne.jp/basic/1-01-2.html,2014/10/16 アクセス
27) 河合塾,２０１５年度大学入試センター試験出題教科・科目について,
http://www.keinet.ne.jp/topics/13/20130801.pdf,2014/10/16 アクセス
28) 明治大学,【情報コミュニケーション学部】2013 年度入学試験変更点について,
http://www.meiji.ac.jp/infocom/information/2012/6t5h7p00000blvbk.html,2014/10/4 アクセス
29) 情報入試研究会,「情報入試研究会」設立趣意書,
http://jnsg.jp/?page_id=2,2014/10/18 アクセス
30) 星野 進,平成 22 年度情報セキュリティに関する懸賞論文「情報セキュリティ意識を向上させるための教育について 教職員の意識向上のための情報セキュリティ研修に関する一考察」,2010 年防衛調達基盤整備協会
31) 原田 要之助, 久保 知裕, 木村 勇一, 岩渕 琢磨, 笹原 務, 芝原 幸弘,「SNS の利用者意識を高めるケーススタディの一考察-リスク意識の啓発プログラムの開発-」.情報処理学会研究報告. マルチメディア通信と分散処理研究会報告 2014-DPS-161(1), 1-10, 2014-09-11
32) ENISA, The new users' guide_How to raise information security awareness_FINAL.pdf,
https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide, 2014/9/22 アクセス
33) NIST, NIST_Information technology security training requirements, http://nist.gov/customcf/get_pdf.cfm?pub_id=151633, 2014/9/22 アクセス
34) Seppo Pahnilaa, Mikko Siponena and Adam Mahmoodb,

Vol.2014-SPT-12 No.18
Vol.2014-EIP-66 No.18
2014/11/21

Employees' Behavior towards IS Security　Policy Compliance,
Proceedings of the 40th Hawaii International Conference on System Sciences – 2007
35)　FEAR APPEALS AND INFORMATION SECURITY BEHAVIORS: AN EMPIRICAL STUDY1,
Allen C. Johnston,Merrill and Warkentin,
MIS Quarterly Vol. 34 No. 3, pp. 549-566/September 2010