強制実行型情報セキュリティ教育システムの開発と評価
Development and Evaluation of System forcing Information Security Education

坂上博俊† 森山真光† 上田翔太‡
Hirotoshi Sakaue† Masamitsu Moriyama† Shota Ueda‡
†近畿大学大学院　総合理工学研究科
‡株式会社ベレーザコーポレーション　システム事業部
† Graduate School of Science and Engineering, Kindai Univ.
‡ Systems Division, Beleza Corporation.

要旨
情報分野の発達によって企業の情報化が進む中，情報漏洩など人に起因する問題が増えてきたことによって e ラーニングによる情報セキュリティ教育が注目を浴びている．しかし，従来のシステムではユーザ自らがログインし教育を受けるなど，自主的に学ぶシステムであるため確実に教育が行われないという問題点がある．よって本研究では，強制的に情報セキュリティ教育を行うシステムを開発し評価を行う．

1. はじめに

近年，企業の情報分野においてニーズが高まっているものに「情報セキュリティ」がある．ひとたび情報漏洩が発生した場合，企業の損失は計り知れないものになると考えられる．しかし，十分な資金のない中小企業において情報セキュリティを担保するコストは生産性向上に寄与されないとネガティブに考えられており，無視されがちである[1].

情報セキュリティ対策の側面には制限や監視等の機械的管理と，経営者と社員の教育による人間的管理がある．前者の場合，機器やソフトウエアの導入によりオートメーションでのコントロールが可能であるが悪意を持った者によるリスク低減が期待される．後者の場合，俗人的で多くの人的，金銭的コストを要するが，悪意を持った者のみでなく，過失におけるリスク低減も期待される．しかし，後者の人間的管理を実施しようにも，日々の業務に追われている状況で定期的に全員が時間を割いて行うことは困難であると考えられる．また，ISO27001 や P マークでは PDCA サイクルが用いられており，実行した教育には成果を求め，その成果からさらなる改善を計画しなければならない．その際，教育の成果は証拠書類として残さなければならず，時間や人員に余裕のない中小企業においてはより困難なものになってきている[2][3]．また，従来のクラウド教育システムは各人が能動的に時間を割いて実行する必要があるため，情報セキュリティに無関心な社員や非協力的な社員が実行する保証はない．しかし，減俸や懲罰等の圧力的な制度を設けてしまうと，良心の欠如が発生し，情報セキュリティレベルの向上が阻害されてしまう可能性がある．よって建設的な観点から人間的管理の教育を行うべきであるが，属人的で多くの人的・金銭的コストがかかるため，我々がヒアリングを行った企業の多くで何の対策もなされていないという現状がある．そこで本研究では，教育実施者・対象者への負担が少なく，情報セキュリティ教育を 1 日 1 回確実に行うことによる単純接触効果[1][4]を狙った効果的な強制実行型情報セキュリティ教育システムの開発を行う．その後，一定期間試験運用を行い，解答ログの集計と被験者にアンケートを実施することで評価を行う．

2. 関連手法

教育システムを教育対象者に実行させる手法として特開 2008-210411[5]や ELSEC[6]が挙げられる．これらのシステムは教育が実行されなかった場合において画面上に教育が実行されていない旨の刻印を表示したり，わかりやすいように教育内容にアニメーションを利用したりなど，利用者が自発的に所定の処理を実行するように利用者の意志や意識に働きかける機能を実現・提供するというものである．しか

[1] 繰り返し接すると好意度や印象が高まるという効果.

し，これはあくまで自発的な実行を促しているに過ぎず，無視してしまえば通常業務に取り掛かることができるので，結果として教育自体が実行されないという問題点がある．

3. 強制実行型情報セキュリティ教育システム

3.1. システムの概要

本研究では情報セキュリティ教育を確実に実行させるシステムを提案する．これは，1 日 1 回強制的に情報セキュリティ教育を実行し，解説に対する問題に解答しなければ通常業務が行えないというものである．図 1 に提案するシステムのアクティビティ図を示す．本システムは PC を立ち上げてから教育対象者にログインさせたのち，1 度起動プロセスを停止し，教育プロセスを実行させてから起動プロセスを再開させてデスクトップ画面を立ち上げる．つまり，教育プロセスを終了させなければ他の一切の動作を受け付けない仕組みを構築することで教育対象者に教育プロセスを強制的に実行させている．

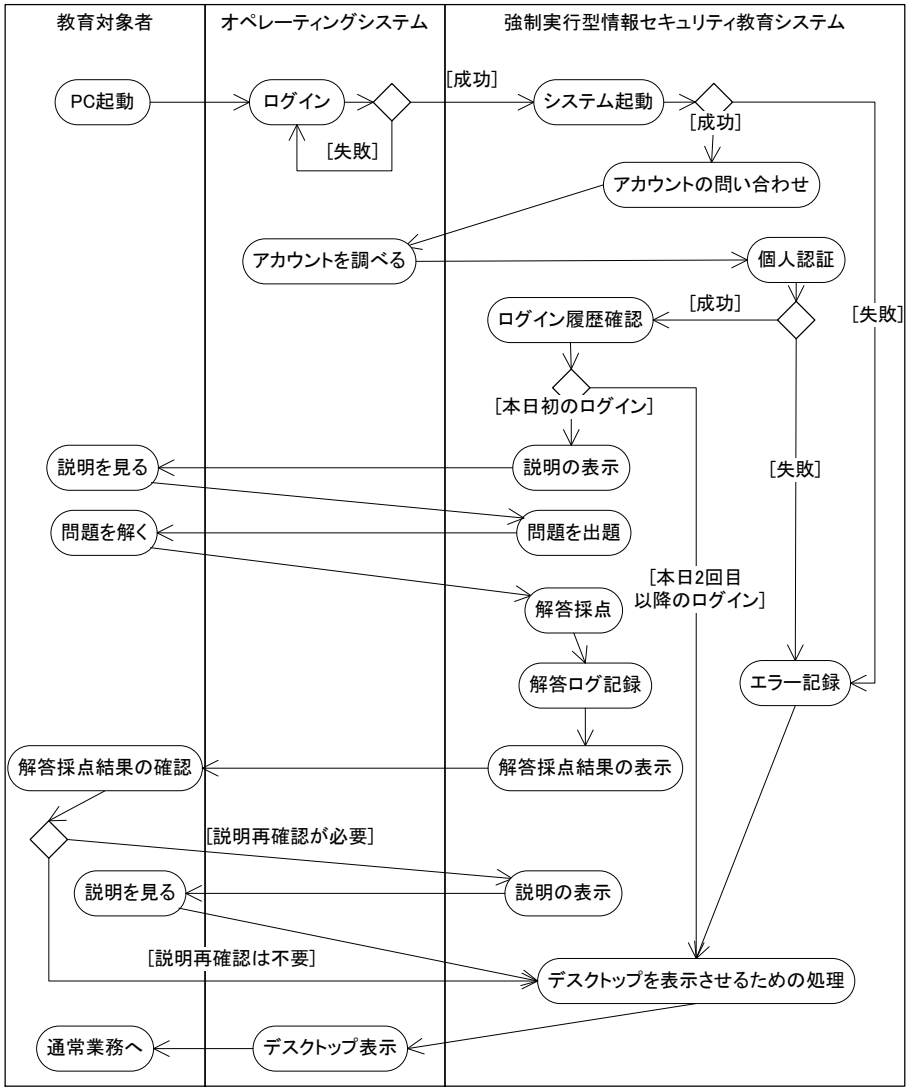

図 1　強制実行型情報セキュリティ教育システムのアクティビティ図

図 2 に教育システムの説明画面の表示例を示す．説明画面では画面上部に情報セキュリティについての説明を文章で表示し，画面下部に図や絵を用いることで説明を補足している．図 3 に問題画面の表示例を示す．問題画面では画面上部に問題文を表示し，画面中央部から下部にかけて 2～4 択の選択肢を表示している．図 4 に結果画面の表示例を示す．結果画面では画面上部に正解であれば丸印，不正解であればバツ印を表示し，画面中央部に正解の選択肢と画面下部に再度説明を確認するかの選択を誘導するボタンを表示している．表示された「はい」ボタンを押すことで再度説明画面が表示され，教育対象者は内容について復習することができる．

図 2 説明画面の表示例

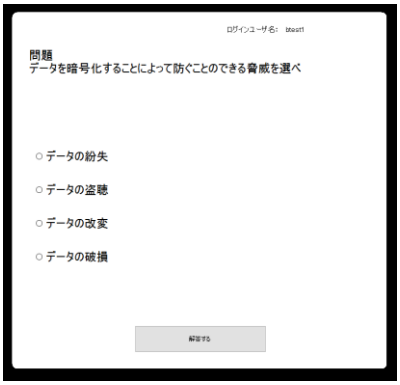

図 3 問題画面の表示例

図 4 結果画面の表示例

3.2. 評価方法

実際に情報セキュリティ教育を必要とする企業内にて評価を行う．初期の計画では本システム導入前後で情報セキュリティに関するテストを行い個人内評価方法にて評価を行う予定であったが，導入前試験で被験者全員が満点をとったためこの評価方法は断念し，代わりにシステム導入後の解答ログとアンケートによる評価を行った. アンケートの各項目については, 運用場面における回答者の負担を考慮し，1〜5 の 5 段階尺度とした．被験者全員の平均が 2（そう思わない）以下もしくは 4（そう思う）以上を閾値として質問内容の拾い上げを行うことで評価を行う．

4. 結果・考察

4.1. 実施結果

本検証においては ISO27001/ISMS の教育資料を参考に作成した説明と 4 択問題を用いて，株式会社ベレーザコーポレーションの社員に対して試験運用を行った．被験者すべての解答ログを試験運用中の全営業日分取得できていることから，システムは問題なく強制実行されたと言える．表 1 に試験運用後に行った 3 名のアンケート回答結果とその平均値及びそれぞれ解答にかかった時間と正答率を示す．被験者 A は事務員であり，情報セキュリティ分野には明るくない．試験運用期間は 2017 年 10 月 5 日から 23 日までの営業日 12 日間である．被験者 B は ISO27001/ISMS（情報セキュリティマネジメントシステム）管理責任者であり，システム部門に 10 年ほど在籍しているので情報セキュリティ分野には明るい．試験運用期間は 2017 年 10 月 3 日から 10 月 23 日までの営業日 14 日間である．被験者 C は営業担当者であり，会社の経営方針から IPA の主催する情報セキュリティマネジメント試験に合格するため 1 か月ほど自分で勉強していると申告があったことから被験者 B と同じく情報セキュリティ分野には明るいと考えられる．試験運用期間は 2017 年 9 月 25 日から 10 月 23 日までの営業日 17 日間である．

表 1　アンケート回答結果とその平均値及び解答時間と正答率

質問内容	A	B	C	平均
A1. 本システムの画面デザインは良かったか	3	2	3	2.7
A2. 本システムの表示画面は印象に残ったか	4	3	3	3.3
A3. 本システムの出題内容は適切であったか	3	3	2	2.7
A4. 本システムには教育の強制力があったか	4	5	4	4.3
A5. 本システムは業務の邪魔になったか	2	2	2	2
A6. 本システムの解説内容はわかりやすかったか	3	3	4	3.3
A7. 本システムの出題内容は適切な難易度だったか	1	3	1	1.7
A8. 本システムの内容は適切な文章量だったか	4	3	3	3.3
A9. 本システムによって情報セキュリティに関する知識が得られたか	4	4	3	3.7
A10. 本システムによって情報セキュリティに関する意識が向上したか	4	4	3	3.7
A11. 本システムは勉強方法として有効であると思うか	4	4	3	3.7

A12. 本システムで勉強を継続したいと思うか	4	4	3	3.7
A13. 本システムは操作に困らなかったか	4	4	5	4.3
A14. 本システムの文章は見やすかったか	4	2	5	3.7
A15. 本システムの絵や図は見やすかったか	3	2	5	3.3
A16. 本システムの利用中に画面が正しく表示されないことがあったか	1	2	1	1.3
A17. 本システムの利用中に表示が遅れたり止まったりすることがあったか	2	4	1	2.3
平均問題解答時間	56 秒	11 秒	11 秒	
平均正答率	58%	93%	100%	

4.2. 考察

3 名の平均評価が 2 以下もしくは 4 以上の項目を本システムにおける特徴として拾い上げを行った．項目 A4「本システムには教育の強制力があったか」に関しては平均評価が 4.3 となっており，本システムが強制力を持っていると判断できる．項目 A5「本システムは業務の邪魔になったか」に関しては平均評価が 2 となっており，業務に影響なく教育が行えていると判断できる．項目 A7「本システムの出題内容は適切な難易度だったか」に関して平均評価が 1.7 となっており，取り扱う教育内容に問題があることが判明した．項目 A13「本システムは操作に困らなかったか」に関しては平均評価が 4.3 となっており，本システムがわかりやすい UI になっていると判断できる．項目 A16「本システムの利用中に画面が正しく表示されないことがあったか」に関しては平均評価が 1.3 となっており，試験運用において本システムは正しく動作できていたと判断できる．また，単純接触効果の結果を確認する項目 A10「本システムによって情報セキュリティに関する意識が向上したか」に関しては閾値を超えなかった．これは実施期間が短かったため，十分に意識付けされなかったことが考えられる．

本研究によって情報セキュリティの教育対象者に知識のばらつきがあり，取り扱う教育内容においては個々のレベルにあった問題を出題する仕組みが求められていることが判明した．具体的な対策として，項目反応理論を用いて問題の難易度と教育対象者の理解度を計算し，教育対象者の理解度に適した難易度の問題を出題することが考えられる．

5. おわりに

本研究では教育関係者への負担を抑えた人間的管理型の情報セキュリティ教育を確実に行うことを目的として強制実行型情報セキュリティ教育システムの開発を行い，その評価を行った．結果として本システムは，アンケート項目 A5 から通常業務に影響が出ないほど人的負担がないと判断できる．また，解答ログが 100%取得できていたことやアンケート項目 A4 から強制的に教育が実行されていることが分かる．さらに教育を行った証拠書類が作成されていることから情報セキュリティ教育の運用工数が減り，企業の負担を軽減できると判断できる．しかしアンケート項目 A7 から問題内容と出題方法に改善の余地があることが判明した．成果が見られなかった単純接触効果については今後実施期間の延長することによる追加調査を行う予定である．

参考文献

[1] 独立行政法人情報処理推進機構, “2016 年度中小企業における情報セキュリティ対策に関する実態調査”, 2017, pp74-75.
[2] Keller S., Powell A., Horstmann B., Predmore C., Crawford M., “Information Security Threats and Practices in Small Businesses.”, *Information Systems Management*, Vol.22 No.2, 2005, pp.7-19.
[3] 菅野泰子, 寺田真敏, 山田安秀, 鎌倉稔成, 土居範久, “企業の情報セキュリティ対策におけるモチベーションの構造に関する考察”, 情報処理学会論文誌, Vol.50 No.9, 2009, pp.2193-2206.
[4] Zajonc, Robert B., “Attitudinal effects of mere exposure”, *Personality and Social Psychology*, Vol.9, 1968, pp.1-27.
[5] クオリティ株式会社, 情報処理システムおよびプログラム, 特開 2008-210411, 2008.
[6] 川上昌俊, 安田浩, 佐々木良一, “情報セキュリティ教育のための e ラーニング教材作成システム ELSEC の開発と評価”, 情報処理学会論文誌, Vol.52 No.3, 2011, pp.1266-1278.