情報処理学会論文誌　教育とコンピュータ　Vol.3　No.2　8–19 (June 2017)

研究会推薦ショートペーパー

情報セキュリティ教育教材の改善検討 ——自由記述アンケートの分析から

天野 由貴[1]　隅谷 孝洋[2]　岩沢 和男[2]　西村 浩二[2]

受付日 2015年11月24日，再受付日 2016年6月8日 / 2016年10月30日，
採録日 2017年3月4日

概要：広島大学では，新入生に対し情報セキュリティ・コンプライアンス教育を実施している．本研究では，教材改善に活用するため，学部新入生に対し実施した自由記述アンケートをテキストマイニング手法により分析した．その結果，講習の有効性を評価できることが分かった．分析結果をふまえ，教材改善の内容について検討した．

キーワード：情報セキュリティ教育，教育効果の測定，テキストマイニング

A Discussion on Improving Learning Materials for Information Security ——On the Analysis of Free Description Responses

Yuki Amano[1]　Takahiro Sumiya[2]　Kazuo Iwasawa[2]　Kouji Nishimura[2]

Received: November 24, 2015, Revised: June 8, 2016/October 30, 2016,
Accepted: March 4, 2017

Abstract: The Information Media Center in Hiroshima University has provided the Information Security and Compliance Courses for the all freshmen every year. A text mining method, that allows to analyze the text data in the questionnaires, was used for improving the learning materials of the courses. The result indicates that the courses were effective and there is room for improvement to the materials.

Keywords: Information security education, measurement of educational effect, text mining

1. はじめに

広島大学では，学生を対象とする情報セキュリティおよびコンプライアンス（法令遵守）教育の必要性から，平成23年度より，新入生に対して本学の情報セキュリティポリシに基づく啓発教育を開始した [1]．また，平成24年度には対象を教職員を含む全構成員に拡大した．その結果，平成23年度以降の情報セキュリティインシデント発生件数は，開始以前と比べて大幅に減少している．

広島大学の情報セキュリティ・コンプライアンス教育は，フレッシュマン講習とフォローアップ講習からなる．フレッシュマン講習は，在籍が1年目の学生を受講対象，フォローアップ講習は在籍2年目以降の全構成員を受講対象としている．フレッシュマン講習は，座学（以降，「座学講習」と呼ぶ）とオンライン講座からなるが，本研究では座学講習で使用している教材の改善を目的とする．情報セキュリティ・コンプライアンス教育の全体の概要と座学講習の教材の内容について2章で述べる．

約2,500名の学部新入生のうち約1,500名に対しては，教養教育において開講されている情報科目「情報活用基礎」のなかで座学講習を実施している．

座学講習では学生の聴講態度が向上することを期待して，講習後に自由記述形式のアンケートをとっている．内容は，講習前に知っていたことと，講習後にわかったことを書いてもらうものである．自由記述回答式では，学生が自分の

1　広島大学社会産学連携室情報部情報化推進グループ
Information Promotion Group, Office of Industry-Academia-Government and Community Collaboration, Hiroshima University, Higashi-Hiroshima, Hiroshima 739–8511, Japan
2　広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University, Higashi-Hiroshima, Hiroshima 739–8511, Japan

言葉で表現するため，選択回答式よりも学生の意識について深い調査がおこなえるという利点がある．このアンケートは紙媒体でとっていたが，平成 27 年度より約 1,500 名を対象にオンラインで実施することとした．本研究では，この自由記述式アンケートのテキストデータを活用する．

情報セキュリティ教育の分野では，学生がどれくらい情報セキュリティのことを意識しているかが重要な観点となる．本研究では，講習前から既知であった事柄，講習後に理解した事柄を自由記述アンケートを用いて聞くことにより，その意識の差の確認をおこなう．またこちらが伝えたいと思っている内容について，どれくらい学生が自分自身で理解しているととらえているかの確認をおこなうことにより，講習の効果をある程度計ることができると考える．座学講習の教材は，講師が使用するスライドをそのまま教材としているため，講習の効果 = 教材の効果といってもよい．こうした意識の差や講習の効果を把握することにより，教材の問題点や改善点の気づきを得られると考えた．教材については 2.2 節で詳しく述べる．

情報セキュリティ教育教材について，アンケートをおこなっているものに中村学園大学の研究がある [2], [3], [4]．これはアンケートの中で教材の改善点について自由記述回答式で学生に尋ねているが，実際に教材改善にどう役立ったのかについては述べられていない．また，その自由記述の回答数の母数も少なく 20 名ほどであり，定量的な分析をおこなってはいない．白川ら [5] は情報教育教材をアンケートにより評価しているが，これは 5 件法を使用しており，本研究のような自由記述回答からの分析ではない．

授業に関する自由記述アンケートを，テキストマイニング手法により定量的に分析している先行研究があり [6], [7], [8]，アンケート分析の手法として，テキストマイニングはある程度確立されたものであるといえる．しかし，これらの研究では，その分析方法に主眼が置かれており，それらの結果を用いて，実際に授業内容をどう改善するかまでについては議論されていない．

本研究では，学生のアンケート回答の分析により，情報セキュリティ教育の教材を改善できることを示す．情報セキュリティ教育は，その性質上ほぼ毎年のように内容の更新が必要となってくる．新たな事案をとりいれるだけでなく，学生の実情に照らし不要になった古い事案を削除する必要がある．その目的を達成するため，我々は情報セキュリティ教育の際に自由記述式でアンケート調査を行い，選択式よりも多様な回答を得ている．アンケートをテキストマイニングの手法で分析することで，その結果を教材改善のために活用できることを示すことが，本研究での目的である．

2. 広島大学の情報セキュリティ・コンプライアンス教育

2.1 概要

1 章で述べたように，広島大学の情報セキュリティ・コンプライアンス教育のフレッシュマン講習は，在籍 1 年目の学生を対象に実施している．学部生，大学院生だけでなく，編入生，非正規生（研究生，科目履修生など）も対象としている．

フレッシュマン講習では，その内容を 2 階層に分けている．1 つは，汎用的かつ網羅的な情報セキュリティ知識の習得を目指すものである．もう 1 つは，より緊急度の高い課題を最近の事例を通して学び，またそれらに関連する本学の制度と取り組みを紹介するものである．我々はできるだけ早い時期にできるだけ多くの学生に習得してほしい内容である後者を約 1 時間の座学講習として提供し，前者は学習者のペースで習得できるようオンライン講座として提供している．本研究のアンケートは座学講習を対象として行っている．

学部新入生は基本的に，教養教育の情報科目である「情報活用基礎」「情報活用演習」「情報活用概論」もしくは教養ゼミ内で座学講習を受講する．それ以外の大学院生などおよび情報科目を履修していない学部新入生は，別途開催されている講習会を受講する．

平成 27 年度 4 月は，東広島キャンパスで 8 回（うち英語解説が 1 回，中国語解説が 1 回），霞キャンパスで 2 回，東千田キャンパスで 1 回実施した．また，6 月に補講，秋入学生対象に 10 月に講習，12 月に補講を実施している．どの回も同じ内容で，学生はどこかで 1 回受講すればよい．未受講者に対しては，年に数回督促通知をおこなっている．

平成 23 年度からの受講者数と受講率について，**表 1** に示す．

2.2 座学講習教材

座学講習では，情報セキュリティについて意識し，広島大学の構成員としておこなうべきことを学ぶだけでなく，学生生活の中で実行できるようになることを目的としている．情報セキュリティの重要な事柄は時勢で変化するため，

表 1　座学講習の受講者数と受講率

Table 1　Number of attendees and attendance rate of classroom learning.

座　学		H23	H24	H25	H26	H27
対象者（人）	学部生	2,654	2,679	2,670	2,692	2,602
	その他	732	724	680	668	762
受講者（人）	学部生	2,556	2,578	2,627	2,547	2,532
	その他	543	514	464	491	617
受講率（%）		91.5	90.9	92.3	90.4	93.6

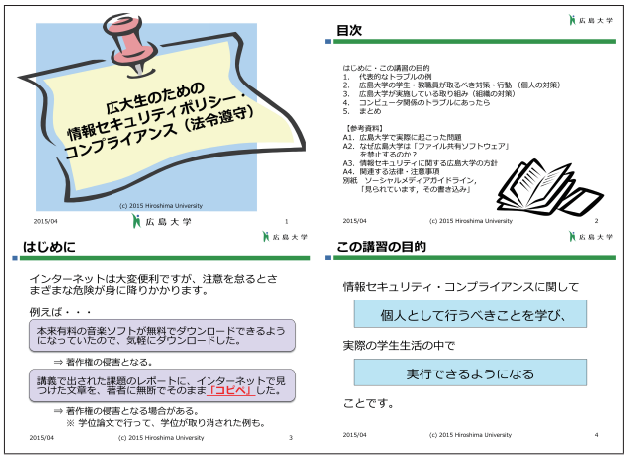

図 1　印刷教材
Fig. 1　Printed material.

教材の内容について毎年度末に見直しをおこない改訂をしている．座学講習は複数教員が講師を担当しているが，同一の教材を使用している．

受講者全員に配布している印刷教材の 1 枚目を**図 1** に示す．講習で使うスライド 66 ページ分に別紙資料 2 枚を添付している構成で，日本語版，英語版，中国語版がある．座学講習では現在 57 ページの【資料】A2 までを講義している．平成 27 年度の教材の各ページについて，以下に内容を示す．

p1　表紙
p2　目次
p3　はじめに
p4　講習の目的
p5　教材内の表記についての説明
p6　1. 代表的なトラブルの例
p7　　トラブル 1：著作物のコピー
p8　　トラブル 2：フィッシングサイト
p9　　トラブル 3：偽ウイルス対策ソフト
p10　2. 広島大学の学生・教職員が取るべき対策・行動（個人の対策）
p11　　対策 1(1)：ファイル共有ソフトを使用しない
p12　　対策 1(2)：広島大学ではファイル共有ソフト使用の禁止
p13　　対策 2(1)：ID，パスワードを適切に管理する
p14　　対策 2(2)：推奨パスワードポリシー
p15　　対策 2(3)：パスワードの変更方法
p16　　対策 2(4)：サービスごとに異なるパスワード
p17　　対策 2(5)：パスワード管理ツールの例
p18　　対策 3：ウイルス対策をおこなう
p19　　対策 4(1)：ソフトウェアをアップデートする
p20　　対策 4(2)：チェックツール（MyJVN）を活用する
p21　　行動 1：利用規約を確認
p22　　行動 2(1)：SNS 利用上の注意
p23　　行動 2(2)：SNS 利用上の注意
p24　　行動 2(3)：広島大学ソーシャルメディアガイドラインの紹介
p25　　行動 3(1)：スマホの取扱いの注意
p26　　行動 3(2)：遠隔操作アプリの注意
p27　　行動 3(3)：不正アプリの注意
p28　　行動 3(4)：写真アプリの位置情報設定の注意
p29　　行動 4：インターネットの匿名性について
p30　3. 広島大学が実施している取り組み（組織の対策）
p31　　取組み 1：利用者認証・身分証の提示
p32　　取組み 2：パスワードの脆弱性診断
p33　　取組み 3：ファイル共有ソフトのネットワーク監視
p34　　取組み 4：ウイルス対策ソフトの提供
p35　　取組み 5：マイクロソフト包括ライセンス
p36　4. コンピュータ関係のトラブルにあったら
p37　　学部・研究科，メディアセンターの連絡先
p38　5. まとめ
p39　　講習の目的の再確認
p40　　オンライン講座の案内
p41　【資料】A1．広島大学で実際に起こった問題
p42　　事例に対する対策・行動・取組み
p43　　事例 1(1)：ファイル共有ソフト使用による著作権侵害行為
p44　　事例 1(2)：著作権侵害行為防止要請文の紹介
p45　　事例 2：個人情報の漏えい（ファイル共有ソフト使用に起因するウイルス感染）
p46　　事例 3：電子ジャーナルの不正利用
p47　　事例 4：友人にパスワードを教える
p48　　事例 5：フィッシングメール
p49　　事例 6：USB メモリを介したウイルス感染
p50　【資料】A2．なぜ広島大学は「ファイル共有ソフトウェア」を禁止するのか？
p52　　国別の主なファイル共有ソフト
p53　　ファイル共有ソフトの違法性
p53　　ファイル共有の仕組み
p54　　ダウンロードによるウイルス感染
p55　　ウイルス感染が原因で重要な情報が流出
p56　　著作権侵害ファイルがいっぱい
p57　　ファイル共有ソフトウェアのまとめ
p58　【資料】A3．情報セキュリティに関する広島大学の方針
p59　　広島大学の情報セキュリティポリシー
p60　　広島大学の情報セキュリティポリシーの体系
p61　【資料】A4．関連する法律・注意事項
p62　　著作権侵害行為に関連する法律
p63　　個人情報の漏えいに関連する法律
p64　　不正アクセスに関連する法律 (1)

p65　　不正アクセスに関連する法律 (2)
p66　　名誉毀損に関連する法律
別紙 1　「見られています，その書き込み」
別紙 2　広島大学ソーシャルメディアガイドライン

3. アンケート分析

3.1 アンケートの概要

2.1 節で述べたように，学部新入生の多くが情報科目内で座学講習を受講している．このうち約 1,500 名が「情報活用基礎」を履修しており，同科目の第 1 回の授業内において，座学講習を受講している．同科目では，第 1 回の授業後，オンラインで 48 項目のアンケートを以前からとっており，クラス分けに活用している．平成 27 年度より，同オンラインアンケートに座学講習アンケートを追加することとした．アンケートは第 1 回めの授業の翌日までに回答することが必須である．

- 対象：「情報活用基礎」受講者　1,478 名（学部 1 年生）
- 時期：2015 年 4 月 9 日～14 日
- 方法：Web 上で，座学講習受講後，翌日までに回答．1 人 1 回

3.1.1 質問の内容

アンケートについては，自由記述回答方式となっている．質問内容は，以下の 2 つである．

(1)「広大生のための情報セキュリティポリシー・コンプライアンス（法令遵守)」（授業の後半 30 分でやった内容です）を聴いてわかったことを 2 つ以上書いてください．

(2)「広大生のための情報セキュリティポリシー・コンプライアンス（法令遵守)」（授業の後半 30 分でやった内容です）を聴く前から知っていたことを 2 つ以上書いてください．

本論文では (1) を【わかったこと】，(2) を【知っていたこと】と記述する．

3.1.2 アンケート対象者と回答数

本研究では，広島大学教養教育科目の情報科目「情報活用基礎」を履修している学部新入生 1,478 名を対象としている．回答者数は以下のとおりである．

【わかったこと】：1,450 名
【知っていたこと】：1,436 名

回答例について付録に示す．誤字脱字などについては，原文のままにしている．

3.2 アンケート集計

3.2.1 集計ツール

アンケートの自由記述回答のような定性的なテキストデータを，恣意性を排除しつつ，かつ少ない労力で分析する手法としてテキストマイニングがある．本研究ではその手法を用いて，アンケートの分析をおこなった．

図 2　TTM
Fig. 2　TinyTextMiner (TTM).

テキストマイニングを行うソフトウェアとしては，KH Coder [9]，WordMiner [10]，Knowledgeocean [11] など様々なものがあるが，本研究ではフリーソフトウェアである TinyTextMiner（TTM）[12]（**図 2**）を使用した．TTM は，日本語文章から使用されている語を切り出し，頻度の集計をおこなうソフトウェアである．基本的な機能しか持っていないが，煩雑な設定の必要なく集計がおこなえることから採用した．

日本語は分かち書きされていないため，テキストマイニングをおこなうには，まず語（形態素）を切り出す必要がある．本研究では，1 行に 1 人分の自由記述回答が記載されている CSV ファイルを作成した．TTM ではその CSV ファイルを形態素解析器である MeCab [13] を用いて形態素解析後，集計データを作成する．

3.2.2 集計方法

形態素解析の結果を集計する前に，以下のことに注意して語の選択，統合などの整理をおこなった．

(1)　不要語の除外
「こと」「もの」などその語自体に意味はないが多数出てくる語を，集計対象から外した．このことにより，頻度集計をする際に意味のない語が上位に出てきてしまうのを防止するができる．設定した語は「こと」「いつ」「ところ」「もの」「ある」「なる」「思う」「する」「それ」「これ」である．

(2)　表記ゆれの多い語を，1 つの語に集約
「ファイル交換ソフト」「ファイル共用ソフト」「ファイル共有ソフト」など表記ゆれの多かったなどを 1 つの語として設定した．このことにより，頻度集計の際に分散する数値をまとめることが可能となる．集約した内容について**表 2** に示す．

(3)　キーワードを設定
また，教材の中で取り扱われている下記の語をキーワードとして設定した．このことにより，下記の語は，

表 2　表記ゆれの整理
Table 2　Aggregation of keywords.

集計に使用する語	表記ゆれの語
ファイル共有ソフト	ファイル共有，共有ソフト，ファイル交換，ファイル共用，ファイル共有サイト，ファイル共有システム，共有ファイル，共用ファイル，ファイル共用ソフト
パスワード	password
KeePass	キーパス，keepass
漏洩	漏えい，漏れる
ウィルス対策	ウィルス対策ソフト，ウィルスソフト
コンピュータ	パソコン，pc，PC
広島大学	広大
USB メモリ	USB，usb
使用	使う
危険	危険性
スマホ	スマートフォン
ソフトウェア	ソフト

表 3　文字数と単語数
Table 3　Number of characters and words.

		文字数		単語数	
	人数	平均	S.D.†	平均	S.D.†
【わかったこと】	1450	55.0	30.8	7.00	3.73
【知っていたこと】	1436	44.1	24.8	5.92	3.43

† 標準偏差

1 つの語として集計されるようになる．「情報セキュリティ」のような語も連続して記述されている場合には「情報」と「セキュリティ」には分かれない．

ファイル共有ソフト，広島大学，漏洩，パスワード，個人情報，情報セキュリティ，著作権侵害，ネットワーク，SNS，法律，アプリ，ウイルス感染，ダウンロード，使用禁止，名誉毀損，アカウント，アップデート，位置情報，ウイルス対策，遠隔操作アプリ，コンピュータ，コンプライアンス，サービスごと，情報セキュリティポリシー，ソーシャルメディアガイドライン，ソフトウェア，著作権，パスワード管理，フィッシング，不正アクセス，変更，迷惑メール，利用規約，ID，USB メモリ，インターネット，オンライン講座，コピー，写真，スマホ，脆弱性診断，電子ジャーナル，匿名性，なりすまし，偽ウィルス対策ソフト，バージョン，パスワード管理ツール，パスワードポリシー，不正アプリ，マイクロソフト包括ライセンス

これらの整理をおこなった結果，学生 1 人につき，およそどれくらいの量の文章で回答を記述しているかについて，文字数と単語数の平均を**表 3** に示し，単語の度数分布図を**図 3**，**図 4** に示す．なお，本研究では名詞のみを分析対象としているため，ここにあげた単語数には名詞以外は含まれていない．

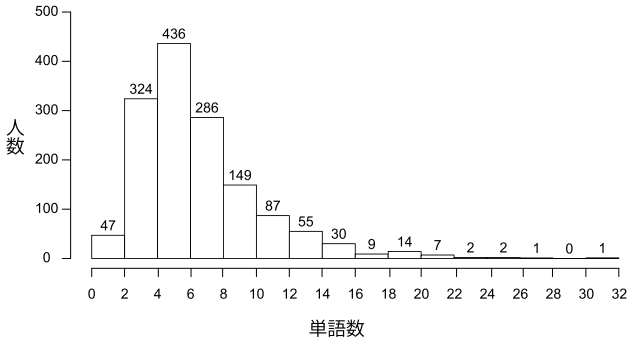

図 3　【わかったこと】の単語数の分布
Fig. 3　Distribution of word numbers in “Things you learned”.

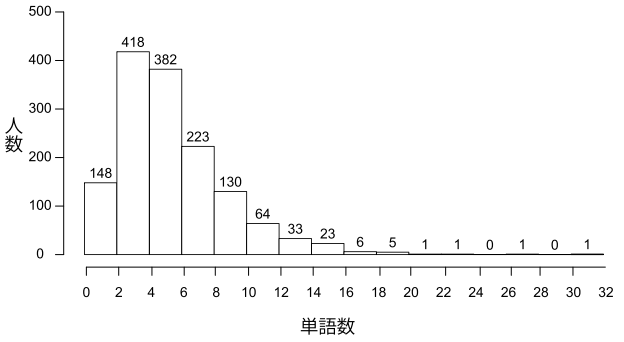

図 4　【知っていたこと】の単語数の分布
Fig. 4　Distribution of word numbers “Things you had already known”.

3.3　分析方法

【わかったこと】と【知っていたこと】のそれぞれに対して，総出現語数に対する各語の出現頻度の割合を出現率とする．**図 5** は，【わかったこと】【知っていたこと】のどちらかに出現率 0.5%以上を持つ語を一覧したものである．「差異」は「【わかったこと】における出現率–【知っていたこと】における出現率」を表しており，語は差異の降順に並べてある．すなわち，グラフで左に行けば行くほど【知っていたこと】に比べて【わかったこと】の出現率が高い語，右に行けば行くほど【わかったこと】に比べて【知っていたこと】の出現率が高い語となっている．

「パスワード」は【わかったこと】【知っていたこと】の両方において多数出現している．また，「可能性」「存在」などそれだけでは意味の分からない語がどういう文脈で出現するのかは，出現率のグラフだけでは分からない．そのため，各語の出現パターンをもとにして，クラスタ分析をおこなった．分析方法については，TTM 開発者である松村らの分析方法 [14] を参考にし，フリーソフトウェアの R [15] を使用しておこなった．回答者と語の出現率をクロス集計したデータを用い，出現率 0.5%以上の語を対象に主成分分析をおこなった．すなわち，頻出する語を，どの

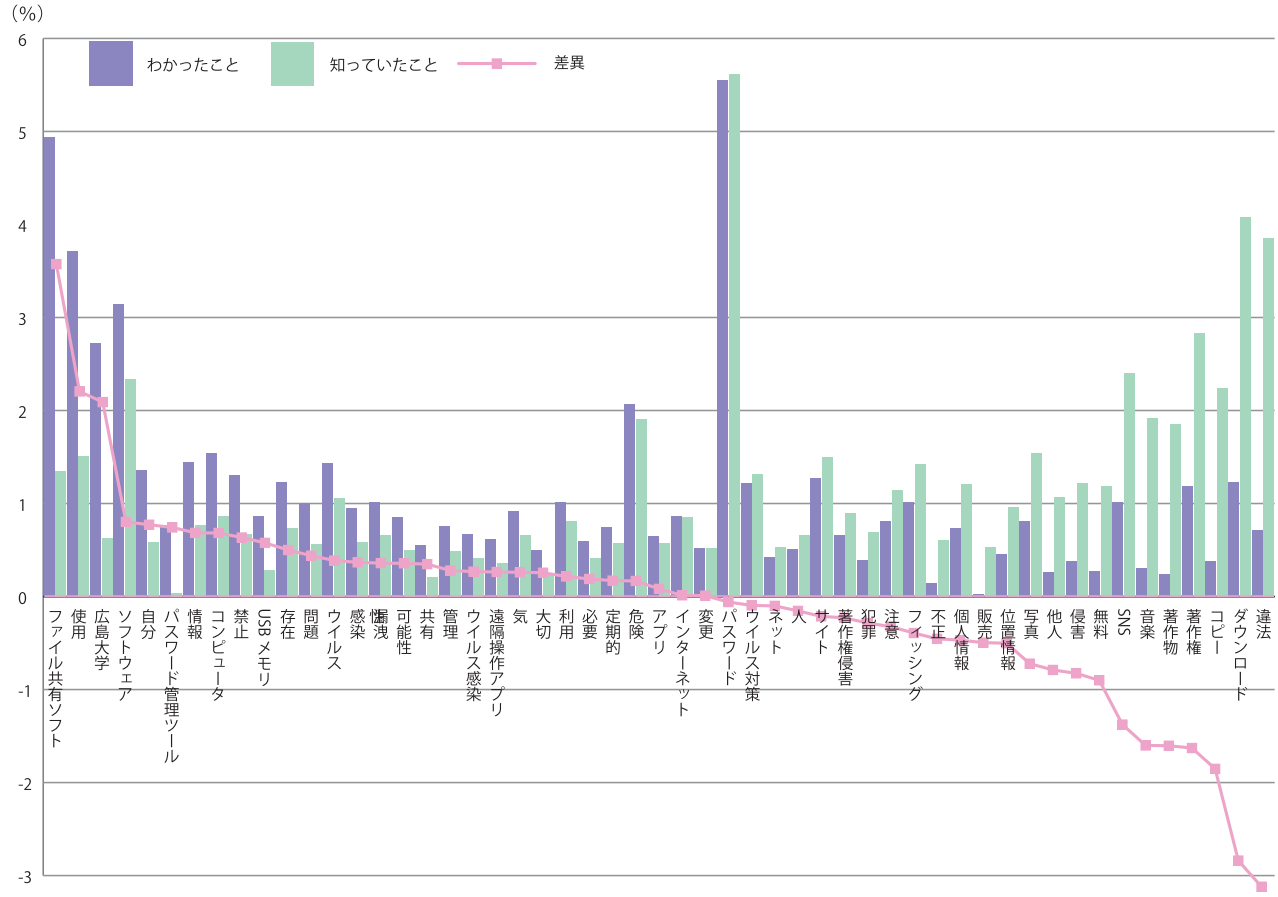

図 5　【わかったこと】と【知っていたこと】のいずれかで頻出した語の出現率とその差異
Fig. 5　Appearance rates and their difference of “Things you learned” and “Things you had already known”.

回答者が使っているのかといった出現パターンに注目していることになる．

算出された主成分得点を用いて，各語間の距離を求め，それをもとにクラスタ分析（Ward 法）を行った．その結果をデンドログラムに表したものを**図 6**，**図 7** に示す．これらの図では，Height の低い位置で線が結ばれているものほど距離が近い，すなわち出現パターンがより近い語となっている．本研究では距離が 1.5 以下の位置でグループを形成している組合せを，「出現パターンが似ている」と定義する．図 6，図 7 では破線よりも下にある組合せになる．

3.4　分析結果

出現頻度が変化したもしくは出現パターンが変化した語には，何らかの教育効果があったと考えられるので，それらの両方もしくはいずれかにあてはまる語に注目して結果を示す．

3.4.1　出現パターンの似た語

下記の (1) から (7) の語については，【わかったこと】【知っていたこと】の両方において，出現パターンが似ていることが分かる．クラスタ分析では数量は把握できないが，各語の関係性を推測することができる．講習・教材で説明されている内容をそれぞれ記した．

(1)「写真」「位置情報」
　位置情報を埋め込まれた写真などの投稿の危険性の説明
(2)「フィッシング」「サイト」
　フィッシングサイトの危険性の紹介
(3)「ウイルス対策」「ソフトウェア」
　広島大学でウイルス対策ソフトウェアの提供をしていること
　偽ウイルス対策ソフトウェアの事例
　ウイルス対策が必要なこと
(4)「USB メモリ」「ウイルス感染」
　USB メモリからのウイルス感染の事例
(5)「音楽」「無料」「違法」「ダウンロード」
　音楽ファイルなどの著作物を無料で配布，不正コピーと知りながらダウンロードすることは違法であること
(6)「広島大学」「禁止」「ファイル共有ソフト」「使用」
　広島大学ではファイル共有ソフトの使用を禁止していること
(7)「SNS」「注意」「必要」「利用」
　SNS の利用上の注意点についての説明

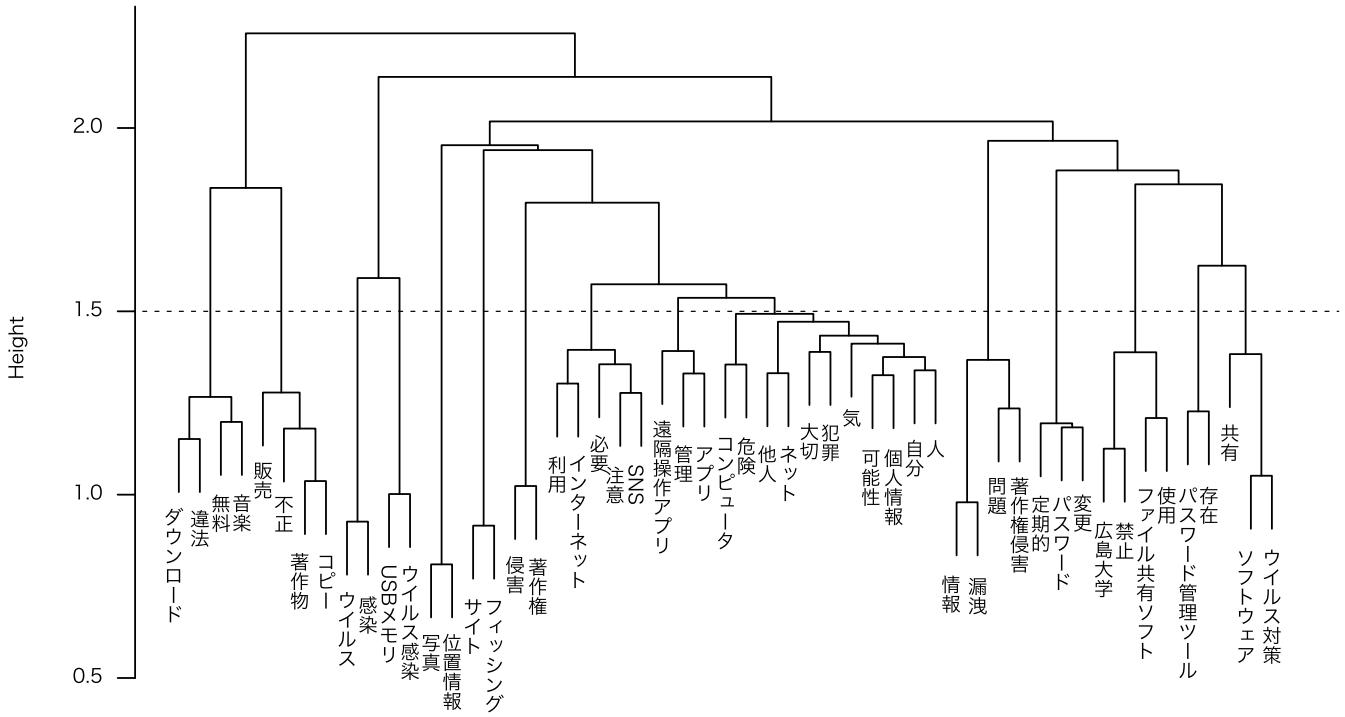

図 6　【わかったこと】のクラスタ分析

Fig. 6　Result of cluster analysis for “Things you learned”.

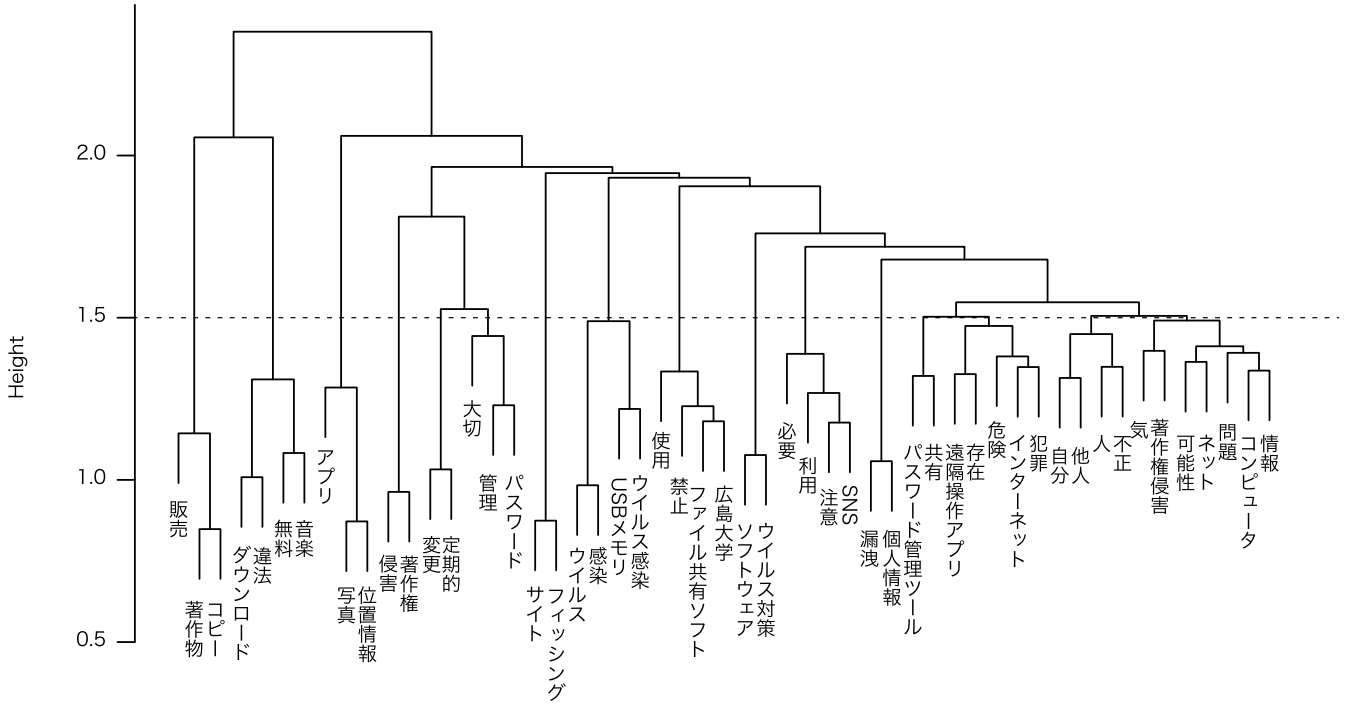

図 7　【知っていたこと】のクラスタ分析

Fig. 7　Result of cluster analysis for “Things you had already known”.

3.4.2　出現パターンの異なる語

「可能性」「存在は」出現パターンの似た語が【わかったこと】と【知っていたこと】で異なる．「可能性」の結果は以下のとおり．

・【わかったこと】「個人情報」「自分」「人」「気」「犯罪」「大切」「ネット」「他人」「危険」「コンピュータ」

・【知っていたこと】「ネット」「問題」「情報」「コンピュータ」「気」「著作権侵害」

既知のこととしては，著作権侵害の可能性などをあげており，【わかったこと】では，個人情報の大切さや自分や他人が犯罪に巻き込まれる可能性などをあげていると考えられる（関連した回答例：付録 A1-1，6，付録 A2-5，8，19）．

「存在」の結果は以下のとおり．

・【わかったこと】「パスワード管理ツール」
・【知っていたこと】「遠隔操作アプリ」「インターネット」「犯罪」「危険」

講習でパスワード管理ツールの存在を知ったと考えられる．既知のこととしては，遠隔操作アプリの存在，インターネットには犯罪の危険性があることなどをあげていると解釈できる（関連した回答例：付録 A1-2，10，14，17，付録 A2-21，22）．

3.4.3　前後で変化があった語

【知っていたこと】から【わかったこと】で変化があったものは下記のとおりである．

・「著作物」「コピー」「販売」:【わかったこと】では「不正」が追加
・「パスワード」:【知っていたこと】では「管理」「大切」，【わかったこと】では「変更」「定期的」
・「漏洩」:【知っていたこと】では「個人情報」，【わかったこと】では「情報」

著作物をコピーすることについて，講習後には不正であることを意識できるようになったと考えられる（関連した回答例：付録 A1-1，6，付録 A2-5，7，16，17）．

パスワードについては，適切な管理の大切さは既知のことであったが，定期的に変更したほうがよいことが講習後に伝わったと推測できる（関連した回答例：付録 A1-6，10，21，22，付録 A2-5，6，7，15，16，17）．

3.4.4　出現が片方に寄っている語

図 5 の【わかったこと】で「ファイル共有ソフト」が多く，【知っていたこと】では少ない．このため多くの学生が既知の情報ではなかったと考えられる．また，出現パターンは，図 6 において「使用」「広島大学」が似ている．広島大学がファイル共有ソフトを禁止していることを教材の中で説明しているため，このことが講習の中で多くの学生に伝わったと考えられる（関連した回答例：付録 A1-5，7，12，13，16，18，20）．

図 5 の【わかったこと】の上位にある「パスワード管理ツール」は教材「対策 2(5)：パスワード管理ツールの例」で紹介しており，図 6 で「存在」とも出現パターンが似ているため，講習によりその存在を知ったと考えられる（関連した回答例：付録 A1-2，10，14，17）．

「USB メモリ」は，講習では「事例 6：USB メモリを介したウイルス感染」のページでのみ出てくる語であり，【わかったこと】で多く【知っていたこと】の出現頻度が少ないため，講習を通じて新規に理解した項目といえる（関連した回答例：付録 A1-1，4，9，11）．

図 5 の【知っていたこと】では「違法」「ダウンロード」「コピー」「音楽」「著作権」などが上位にあがっており，図 7 での出現パターンも似ているため，教材の「はじめに」「トラブル 1：著作物のコピー」で紹介している，音楽ファイルの違法ダウンロードやコピーが著作権的に問題がある，ということが既知の事柄であったことが分かる（関連した回答例：付録 A2-2，4，8，9）．

また「SNS」も同様である（関連した回答例：付録 A2-1，16）．

3.5　考察と改善案

3.5.1　考察

3.4 節の分析結果により，教材の内容について下記のことが推測できる．

＜講習で特に印象に残った箇所＞
・「ファイル共有ソフト」の箇所
・「パスワード変更」の箇所
・ 対策 2(5)：パスワード管理ツールの例
・ 事例 6：USB メモリを介したウイルス感染

＜講習前から既知であった箇所＞
・ はじめに
・ トラブル 1：著作物のコピー
・「SNS」の箇所
・「パスワード管理」の箇所

「ファイル共有ソフト」については，【知っていたこと】で少なく【わかったこと】で多く，最も差異のある語になっており，講習の効果があったことが分かる．これまで「ファイル共有ソフト」について存在を知らなかったか，もしくはあまりセキュリティの観点としては意識していなかったが，講習で意識できるようになったものと思われる．教材でも一番多くの 13 ページを割いている内容であり，広島大学としては利用禁止としているため，注意喚起に重きを置いている事柄である．

パスワードの変更方法や管理の方法については，講習の中で大学の取り組みやセキュリティポリシーなど 6 ページにわたって説明している．既知のこととしてもパスワード管理があがっているが，【わかったこと】の頻度数も多く，変更方法や管理ツールなど記述もより具体的になっており，意識すべきことが伝わったと考えられる．

既知の事柄では，「SNS」は学部新入生にとって身近な問題であることは認識していたが，「音楽ファイルのコピー，違法ダウンロード」に関しても数が多かった．現在の教材では「はじめに」の箇所でまずふれている事柄だが，言及する内容については今後検討をおこなう必要があると考えられる．「トラブル 1：著作物のコピー」でも説明している内容のため「はじめに」は別の事柄とするか，もしくはよく知られている事柄を講習のつかみとして利用し，「トラブル 1：著作物のコピー」の箇所では音楽ファイルではない事案を説明するなどの改善案が考えられる．

以上は，出現頻度が高い語に関する考察であるが，逆に

表 4 【わかったこと】で出現頻度 10 以下のキーワード
Table 4 Keywords which the number of appearance are lower than 10 in “Things you learned”.

キーワード	頻度
電子ジャーナル	10
アカウント	9
偽ウィルス対策ソフト	8
不正アクセス	5
迷惑メール	5
脆弱性診断	5
パスワードポリシ	5
名誉毀損	3
オンライン講座	2
バージョン	2
マイクロソフト包括ライセンス	1
情報セキュリティポリシー	0
ソーシャルメディアガイドライン	0
なりすまし	0

頻度の低いほう，すなわち「わかっていないこと」についても検討する必要がある．しかし，自由記述アンケートでは「わかってないこと」がキーワードとして回答に出現することがないため，出現した単語を対象とする出現頻度の差やクラスタ分析によってはこれを扱うことができない．そこで，事前に設定したキーワードの中で出現頻度が低かったものを抽出した．**表 4** は，3.2.2 項であげたキーワードのうち，【わかったこと】で出現頻度が 10 以下であったものを示している．

「電子ジャーナル」は，入学したての学部新入生はほぼ利用していないと思われることから，意識付けが低かったと考えられる．「偽ウィルス対策ソフト」は，【わかったこと】の「ウイルス対策」「ソフトウェア」と「存在」が近いことから，「偽ウイルス対策ソフト」という語は集計できなかったものの，「偽物のウイルス対策ソフトの存在を知った」などのような記載があったため，実質数は少なくなかった．「不正アクセス」と「情報セキュリティポリシー」については，座学講習内でふれておらず，印刷教材の記載のみとなっているため，印象に残りにくかったと推測できる．「マイクロソフト包括ライセンス」と「ソーシャルメディアガイドライン」については，用語が長いため記入がなかった可能性もあるが，教材としては座学講習でもふれているにもかかわらず印象が少なかったことになるので，教材の改善が必要と考えられる．

3.5.2 改善案

以上の分析結果から検討すべき改善案を，**表 5** に示す．ページ数については，2.2 節で示したものを使用している．

【わかったこと】−【知っていたこと】が大きい学習項目は教材から削減し，こちらが伝えたいと思っている内容で【わかったこと】の出現率の低い学習項目は教材で拡充することで教材を改善する．

表 5 教材改善案
Table 5 Improvement plan of the material.

内容	ページ	改善案
ファイル共有ソフト	11，12，43，50–57	ページ削減
著作物のコピー	7	音楽ファイル以外の事例紹介
ソーシャルメディアガイドライン	24，別紙 2	説明，説明の拡充
マイクロソフト包括ライセンス	35	説明，説明の拡充

4. まとめと今後の課題

本研究では，教材改善に活用するため，学部新入生に対し実施した自由記述アンケートを，テキストマイニング手法により分析した．直接観測することが困難な【わかったこと】や【知っていたこと】を調べるためには，次の 2 点を用いた．

(a) 学習項目に対応するとおぼしき単語の出現頻度
(b) クラスタ分析を用いた得られた単語の共起関係

上記 (a)，(b) から学習者の【わかったこと】や【知っていたこと】を推測する．その結果，学部新入生が (1) 講習において理解できたと思われる内容，(2) 講習前から既知と考えられる内容，(3) (1)，(2) の差，(4) 教材として伝えたい内容にもかかわらずあまり伝わっていないと思われる内容，についておよその把握をおこなうことができた．

情報セキュリティの脅威や対策は刻々と変化するものであることから，座学講習の教材も毎年改訂をおこなっている．我々はテキストマイニング手法に精通していたわけではなかったが，本研究の方法を行うことにより，多様で多量な学生の回答を定量的に分析し，前述の (1)〜(3) をふまえることで，教材改善に活かせることが分かった．今後は継続的にこの方法を活用していきたい．

今後の課題として，以下のことが考えられる．

現在【わかったこと】【知っていたこと】の 2 項目の自由記述回答式としているアンケート項目について，今後自由記述回答式かキーワードによる選択回答式にするかの問題がある．選択回答式にするとより集計が容易におこなえ，【わかったこと】と【知っていたこと】の回答項目数の差などをはかることもできるというメリットがある．しかし，質問者の想定外の回答を得られなくなるという問題もあるため，検討が必要である．

現在は留学生にも英語・中国語のアンケートを紙媒体でとっている．留学生においては日本人とセキュリティ意識に差があることが推測できるため，できれば別途集計を行えるとよいが，データの仕分け，翻訳の手間などが発生するため実施方法について検討が必要である．

今回は「情報活用基礎」のアンケートのみを対象としたが，現在紙媒体で実施している大学院生などのアンケート

のとり方について検討が必要である．大学院生は学部新入生と既知の事柄が違うことが予想される．フレッシュマン講習で受講するオンライン情報セキュリティ講座の中でアンケートをとることも考えられるが，座学講習の内容に関する回答を得るには，質問設定に工夫が必要と考えられる．

「情報活用基礎」のオンラインアンケートでは，コンピュータの利用経験やコンピュータ不安度なども調査している [16]．これらと情報セキュリティ・コンプライアンス講習のアンケートデータをあわせて検討し，コンピュータ不安度などとセキュリティ意識レベルとの関連をはかることができないかと考えている．

謝辞　本研究を実施するにあたり，広島大学の情報科目「情報活用基礎」担当教員に協力をいただいた．また，広島大学大学院工学研究院北村充教授に，アンケートの内容について助言をいただいた．ここに記して感謝の意を表する．

参考文献

[1] 西村浩二，大東俊博，岩沢和男，隅谷孝洋，稲垣知宏，中村純，宮内祐輔，三戸里美，相原玲二：広島大学における情報セキュリティ・コンプライアンス教育の取組み，情報処理学会研究報告インターネットと運用技術（IOT），2012-IOT-18, No.2, pp.1–6 (2012).
[2] 花隈悦子，梶田鈴子：e ラーニング教材を使った情報セキュリティ教育の試みと評価，中村学園大学・中村学園大学短期大学部研究紀要，Vol.42, pp.293–302 (2010).
[3] 花隈悦子：e ラーニング教材を使った情報セキュリティ教育の試みと評価 (2)，中村学園大学・中村学園大学短期大学部研究紀要，Vol.43, pp.223–231 (2011).
[4] 有田真貴子，梶田鈴子：情報セキュリティ教育における e ラーニング教材の学習効果の検証，中村学園大学・中村学園大学短期大学部研究紀要，Vol.45, pp.65–74 (2013).
[5] 白川雄三，神谷善弘，中嶌康二：情報リテラシー教材におけるインストラクショナルデザイン活用の効果測定，教育情報研究，Vol.30, No.3, pp.61–70 (2015).
[6] 石田　崇，後藤正幸，平澤茂一：大学の情報系授業における学生アンケートの分析，コンピュータ&エデュケーション，Vol.18, pp.152–157 (2005).
[7] 武市祥司，ライニアンソン・リー，松石正克：データマイニング手法を用いた学習到達度自己評価のアンケート分析，*Journal of JSEE*, Vol.59, No.4, pp.9–14 (2011).
[8] 阪上辰也：テキストマイニングによる英語授業に関する自由記述回答の内容分析，広島外国語教育研究，Vol.18, pp.55–64 (2015).
[9] 樋口耕一：KH Coder，入手先 ⟨http://khc.sourceforge.net/⟩（参照 2015-11-24）．
[10] 日本電子計算株式会社：WordMiner，入手先 ⟨https://www.jip.co.jp/product/wordminer/⟩（参照 2015-11-24）．
[11] エヌ・ティ・ティ・ソフトウェア株式会社：Knowledge-ocean，入手先 ⟨https://www.ntts.co.jp/products/knowledgeocean/⟩（参照 2015-11-24）．
[12] 松村真宏，三浦麻子：TinyTextMiner，入手先 ⟨http://mtmr.jp/ttm/⟩（参照 2015-11-24）．
[13] 工藤　拓：MeCab，入手先 ⟨http://taku910.github.io/mecab/⟩（参照 2015-11-24）．
[14] 松村真宏，三浦麻子：人文・社会科学のためのテキストマイニング，誠信書房 (2014).
[15] The R Foundation: The R Project for Statistical Computing, available from ⟨https://www.r-project.org/⟩ (accessed 2015-11-24).
[16] 隅谷孝洋，長登　康，稲垣知宏：大学新入生のコンピュータ不安の長期定点観測，情報処理学会研究報告コンピュータと教育（CE），2015-CE-130, No.5, pp.1–5 (2015).

付　　録

A.1 【わかったこと】の回答（一部）

ランダムに 22 件を抽出した．

1. 「著作権」についての問題は他人事ではないということ．USB メモリを介してウイルスに感染することがあるということ．
2. ネット上でのトラブルを防ぐためにファイル共有ソフトを使用しないということ．パスワード管理ツール等を使用する．
3. レポートでコピペはだめ．フィッシングサイトに気をつける．
4. フィッシングサイトのこと．USB メモリを介したウイルス感染．パスワードの変更方法
5. ファイル共有ソフトを使用してはいけないこと．フィッシングサイトというものが存在することは知らなかった．
6. 自分が無料だと思っていたものが本当は有料で著作権の侵害になるという事．偽ウイルスソフトがあるという事．
7. ファイル共有ソフトを使わない．パスワードを他人に教えないパスワードを複雑なものにする
8. フィッシングサイト．パスワードの強度が組み合わせで相当強くなるといこと
9. アカウントとパスワードを教えあってはいけない．USB を介したウイルス感染がある
10. 長時間同じパスワードを使用しないこと．パスワード管理ツールがあること．
11. USB メモリを介したウイルス感染について．遠隔操作アプリについて
12. ファイル共有ソフトを使ってはいけない．SNS 利用上の注意
13. 電子ジャーナルの不正利用について．広島大学がファイル共有ソフトを禁止した理由
14. DVD をリッキング（原文ママ）してコピーするのが禁止になったこと．パスワード管理ツールの有無．
15. 1 つ目　ソフトウェアを定期的にアップデートすること．2 つ目　ウイルス対策を必ず行うこと．
16. 広島大学ではファイル共有ソフト使用が禁止されているということ．文字の種類や桁数が増えるとパスワードの強度が高まるということ．インターネット上にはウイルスがたくさんいるということ

17. フィッシングサイトというものがあること．ウイルス対策ソフト自体が危険なことがあること．パスワードを使いまわさないほうがよい．パスワード管理ツールがあること．アップデートは定期的にやっておくべきということ
18. SNS の利用には十分注意すること．ファイル共有ソフトを使用しないことちゃんと定期的にソフトのアップデートを行うこと
19. フィッシングサイトによる被害．チェックツールの活用について
20. ファイル共有ソフトの危険性．パスワードの管理および保護について
21. パスワードを定期的に変える．ウイルス対策ソフトを毎週更新する
22. パスワードは簡単に破られること．パスワードは定期的に変更することが大事

A.2 【知っていたこと】の回答（一部）

ランダムに 22 件を抽出した．

1. 気軽に手を出せる SNS には危険が潜んでいるということ．広島大学での ID には二通り（大文字と小文字）があるということ．
2. 音楽ソフト等の違法なダウンロードは法律で禁止されている．フィッシングサイトの存在．
3. ファイル共有ソフトを使わない．偽ウイルス対策ソフトがあること．
4. 音楽ソフトなどの違法ダウンロード不正アプリのこと
5. 著作権の掛っているものをコピーしてはいけないこと．ID やパスワードを他人に教えてはいけないこと．
6. パスワードは他人には教えてはいけないという事．パスワードは桁数が少ないほどばれやすい
7. 著作権というものがある．ワンクッリク詐欺（原文ママ）というものがある
8. 著作権のコピー（音楽など）．リンクに飛ぶとウィルスに引っかかることがある
9. 無料のコンテンツをダウンロードしてはいけない．フィッシングメール
10. 他人が推測しやすいパスワードはやめておくこと．パスワードをサービスごとに変えること．
11. フィッシングサイトについて．ファイル共有ソフト使用禁止のこと
12. コピペ．ウイルス対策ソフト
13. フィッシングサイト等の現状．ファイル共有ソフトウェアの内容．ウイルスの実態
14. パスワード管理は一つ一つ違うものを設定すること．ファイル共有ソフト原因の犯罪．
15. 1 つ目　パスワードをしっかり管理すること．2 つ目違法行為をしないように気をつけること．
16. コピペしてはいけないということ．パスワードはサービスごとに変えないといけないこと．SNS には誹謗中傷は書き込んではいけないこと．GPS 機能には注意が必要だということ
17. コピペをしてはいけない．広大 ID とパスワードを人に教えてはいけない
18. パスワードを複雑にすること．コピペはしてはいけないこと
19. コピペの著作権侵害．悪徳サイトによるウイルス感染
20. コピペにより作成および提出された論文は発覚次第単位または学位の取り消し対象．フィッシングサイト
21. 遠隔操作アプリが存在すること．著作物のコピーはよく考えて情報を発信すること．
22. コピペをしてはいけないことインターネット上にはたくさんのウイルスが存在ので，ウイルス対策を行う必要があるということ

推薦文

大学における情報セキュリティ教育の重要性は高いが，どのような教育を行えば効果的かということについてはまだまだ課題が多い．本論文では，情報セキュリティ教育の分野で重要視されている，学生がどのくらい情報セキュリティのことを意識しているか，について教養教育の中で行われた講習における自由記述アンケートの記述内容から調査した結果を報告している．本研究で目指していることは，自由記述アンケートを用いて学生に講習前から「知っていたこと」，講習後に「わかったこと」を聞くことによる意識の変化の確認，その差の中で教授者が伝えたいと思っている内容をどれくらい学生が自分自身で理解しているととらえているかの確認，を行うことで講習の効果を測ること，そして，さらにそれを教材の改善に活かすことである．このために，テキストマイニング手法による自由記述アンケートの定量的な分析による情報セキュリティ教育の教材の評価とそれに基づく教材を改善すべき箇所を具体的に示している．本研究で行われている自由記述アンケート分析手法はフリーソフトウェアを利用した，TinyTextMiner（TTM）を利用した形態素解析，その結果を用いた R によるクラスタ分析といった比較的導入しやすいものである．また，提案している教材の改善方針としては，分析結果で得られた「わかったこと」と「知っていたこと」から，その差が大きい学習項目は教材から削減する，教授者が伝えたいと思っている内容で「わかったこと」の出現率の低い学習項目は教材で拡充するという簡潔な形でまとめられている．このように，本論文で示されていることは，情報セキュリティ教育を行っている大学教員，職員の方々にとって，他大学の事例としての教材開発の参考情報になるとともに，自大学での状況を調査する手法の参考になるものである．そして，このような事例を共有していくことで，ド

メインにかかわらずに自由記述アンケートを分析するためのテキストマイニング手法の発展にも貢献できると考えられる．このように事例をまとめたものが本トランザクションを通じて共有され，研究および大学教育の現場の発展に貢献することを期待したい．

（SSS2015 プログラム委員長/論文誌「教育とコンピュータ」編集幹事/教育学習支援情報システム研究会幹事

林　雄介）

天野 由貴

1992 年大阪教育大学教育学部卒業．2016 年熊本大学大学院社会文化科学研究科教授システム学専攻博士課程前期終了．修士（教授システム学）．2008 年より広島大学職員として勤務．2012 年より情報化推進グループに配属となり，情報セキュリティ教育および情報教育支援に従事．情報処理学会，日本教育工学会会員．

隅谷 孝洋

1987 年広島大学総合科学部卒業．1989 年同大学院工学研究科博士課程前期修了．博士（学術）．同大学総合科学部教務員と助手，同大学情報教育研究センター助手を経て，2001 年より同大学情報メディア教育研究センター准教授．学習支援システムの運用と研究に従事．情報処理学会，日本教育工学会，日本計算機統計学会各会員．

岩沢 和男

1984 年筑波大学第一学群自然学類（物理）卒業．1984 年より（株）SRA 勤務．1986 年同退社．1991 年筑波大学大学院物理学研究科博士課程修了（理学博士）．1991 年より東京大学原子核研究所研究員および名古屋商科大学非常勤講師．1996 年より筑波大学文部技官，1999 年より現職，広島大学情報メディア教育研究センター講師．センターサービスの利用者情報管理および情報システム&情報セキュリティに関する研究に従事．ISMS 推進担当．情報処理学会会員．

西村 浩二

1989 年広島大学工学部第二類（電気系）卒業．1991 年広島大学大学院工学研究科博士課程前期修了．1991 年より全日空システム企画（株）勤務．1994 年同退社，広島大学総合情報処理センター助手．2007 年同大学情報メディア教育研究センター准教授を経て，2011 年より同教授．博士（工学）．コンピュータネットワークの運用管理，移動透過通信，情報セキュリティに関する研究に従事．電子情報通信学会，情報処理学会各会員．