本学１年生における情報セキュリティの把握傾向に関する考察

増山　一光[*1]
Email: masuyama@kaetsu.ac.jp

*1：嘉悦大学経営経済学部

◎Key Words　　情報セキュリティ，情報セキュリティ対策，計量テキスト分析

1.　はじめに

本学 1 年生に対してデータサイエンス入門という授業を行っており，この授業内で情報セキュリティの導入授業を行った際に，情報セキュリティに関する理解や意識に関する調査を行った。この調査の分析を行うことで，学生の情報セキュリティに対する意識，自身の情報セキュリティへの対策，学習欲求の程度などを示しつつ，これらの調査結果に対してクロス集計を通じて情報セキュリティに対する把握傾向を考察する。

さらに，社会全体として情報セキュリティを高めるため方策についての自由記述から，今後の情報セキュリティ意識の形成に向けた要素について検討する。

2.　アンケートの概要

アンケートは、2025 年 12 月に情報セキュリティの導入授業後に 4 件法で実施し，回答者数は 171 名であった。このアンケートの結果をまとめたものが表 1 である。

アンケートの質問内容は，講義内容の理解，情報セキュリティへの興味関心，企業の情報セキュリティインシデントの対策，自身の情報セキュリティ対策に対する内省，将来の情報セキュリティへの関わり方に分かれている。

表 1 アンケート結果

質問番号	質問	まったく当てはまらない	あまり当てはまらない	やや当てはまる	とても当てはまる
1	これまでの講義の内容で「情報セキュリティ」の意味を理解することができた。	1.2%	5.8%	62.6%	30.4%
2	私は、「情報セキュリティ」に興味・関心がある。	1.2%	10.5%	56.7%	31.6%
3	私は、「情報セキュリティ」を学習したい。	1.8%	16.4%	53.2%	28.7%
4	現在の企業では、情報セキュリティ対策が不足していると思う。		15.8%	59.1%	25.1%
5	私生活において、「情報セキュリティ」を意識して対策をしている。	8.2%	39.2%	37.4%	15.2%
6	自分の個人情報を流出させないような具体的な対策をしている。	6.4%	29.8%	46.2%	17.5%
7	情報セキュリティに関わる仕事をしたいと思いますか。	8.2%	42.7%	40.4%	8.8%

情報セキュリティに関する基礎的な内容の理解については，概ね良好であった。これを踏まえて，情報セキュリティへの興味や関心が高いことが挙げられる。加えて，今後の情報セキュリティに対する学習意欲も高い割合となっている。この背景には，昨今のランサムウェアによる企業に対する被害(1)(2)などの報道と相まって，関心の高まっているようである。さらに，こうした情報セキュリティインシデントがなぜ発生してしまうのかという疑問を感じているようであった。

企業の情報セキュリティの対策については，かなり厳しい結果になっている。これは，前述のようにランサムウェアによるインシデントが影響しているとともに，様々な要因による個人情報漏えいに関する事件が多く発生していることで不信感が募っているようである。このことについては，後述する自由記述から把握することができた。

個人の情報セキュリティ対策に対しては，「あまり当てはまらない」と「まったく当てはまらない」を加えて，47.4%となっており対策していない学生が多くみられる。しかし，個人情報に対する対策に限定すると 1 割程度は向上している。

これまで情報セキュリティ人材は不足しているという現状(3)があり，様々な対策が取られている。こうした状況のなかで，情報セキュリティの仕事をしたいと回答している学生が半数近くいるのは特筆すべきことである。本学が経営経済学科ということもあり，情報セキュリティの技術的な側面よりも，経営管理的な側面からから関わろうとしている。

3.　クロス集計による分析

本章では，前章でのアンケート集計の結果を用いてクロス集計をすることで，回答者の詳細を分析する。集計をするにあたって，4 が「とても当てはまる」，3 が「やや当てはまる」，2 が「あまり当てはまらない」，1 が「まったく当てはまらない」となっている。

表 2 質問番号 2 と 3 のクロス集計

		私は、「情報セキュリティ」を学習したい。				
		1	2	3	4	総計
私は、「情報セキュリティ」に興味・関心がある。	1	1	1			2
	2	1	10	6	1	18
	3	1	17	67	12	97
	4			18	36	54
	総計	3	28	91	49	171

表2は，表1における質問番号2と3をクロス集計したものである。ここでは，情報セキュリティに興味・関心を持っている学生は，学習したいと思っていることがわかる。特に，両者とも肯定的な回答をしている学生が133名となっており多くなっている。なお，相関係数はr=0.62である。

表3 質問番号2と5のクロス集計

		私生活において、「情報セキュリティ」を意識して対策をしている。				
		1	2	3	4	総計
私は、「情報セキュリティ」に興味・関心がある。	1	2				2
	2	3	8	5	2	18
	3	7	40	39	11	97
	4	2	19	20	13	54
	総計	14	67	64	26	171

表3は，表1における質問番号2と5をクロス集計したものである。これは，情報セキュリティに興味・関心を持っている学生が，対策をしているかどうかをみるものである。ここからは，情報セキュリティに興味・関心があることにより，情報セキュリティ対策が取られているわけではないことを示している。なお，相関係数はr＝0.24である。

表4 質問番号4と6のクロス集計

		自分の個人情報を流出させないような具体的な対策をしている。				
		1	2	3	4	総計
現在の企業では、情報セキュリティ対策が不足していると思う。	1					
	2	2	12	11	2	27
	3	8	22	55	16	101
	4	1	17	13	12	43
	総計	11	51	79	30	171

表4は，表1における質問番号4と6をクロス集計したものである。ここでは，情報セキュリティ対策が不足していると肯定的に回答している学生が，必ずしも個人情報を流出させない対策をしていると多くはなっていないことがわかる。ここからは，企業の情報セキュリティ対策に対する考え方と，自身の自衛手段として対策を行うことにはあまり関連性がない。なお，相関係数はr=0.12である。

表5 質問番号2と7のクロス集計

		情報セキュリティに関わる仕事をしたいと思いますか。				
		1	2	3	4	総計
私は、「情報セキュリティ」に興味・関心がある。	1	2				2
	2	5	11	2		18
	3	7	48	36	6	97
	4		14	31	9	54
	総計	14	73	69	15	171

表5は，表1における質問番号2と7をクロス集計したものである。ここでは，情報セキュリティに興味・関心の高い回答者が，必ずしも情報セキュリティに関わる仕事をしたいわけでないことを示している。ここからは，情報セキュリティに関わる仕事の内容をあまり認識していないなどの課題はあるが，希望する職業にあまりなっていないのが現状である。なお，相関係数はr=0.46である。

4. 情報セキュリティ対する学習ニーズ分析

今回のアンケートでは，「もし，情報セキュリティを学ぶ機会があったならば，どのようなことを学びたいですか」という問いに対して，学習したい内容について自由記述をさせた。このアンケート結果を用いて情報セキュリティに関する学習ニーズを分析するために，生成AIであるGeminiに記述内容を入力し，記述の多いものから上位の10の内容にまとめるように指示をした。その結果が，表6である。

表6 希望する学習内容の一覧

順位	学習項目（カテゴリ）	主な学習要望・学生の関心内容
1	サイバー攻撃の手口・対策・事例	実際のハッキング手法、最新の攻撃と具体的な防御策、過去の事件のケーススタディ
2	コンピューターウイルス・マルウェア	ウイルス感染の経路・仕組み、ランサムウェア対策、感染時の具体的な対処法
3	個人情報の保護・漏洩対策	情報が流出する経緯やプロセス、個人情報を100%守るための具体的な流出防止策
4	日常生活・身近なセキュリティ	スマホやPCの安全な利用、ネットリテラシーの基本、日常で使える自衛の技術
5	企業のセキュリティ・リスクマネジメント	組織の情報資産を守る仕組み、リスクマネジメント、セキュリティ関連の法律や資格
6	パスワードの作成・管理・認証	強固なパスワードの作り方、使い回しのリスク、二段階認証などの認証技術
7	SNS・ネットサービスの安全利用	投稿からの個人特定プロセス、アカウント乗っ取り・なりすましの対策
8	システム・ネットワーク・プログラミング	不正アクセスの仕組み、ネットワーク防御、保護プログラムやアプリ開発の基礎
9	暗号技術の基礎・仕組み	データの暗号化・復号のプロセス、公開鍵・共通鍵暗号、パスワードのハッシュ化
10	危険なサイト・フィッシング詐欺の見分け方	偽のネット通販サイトや危ないサイトの見抜き方、詐欺メールの識別方法

この表からは，日々発生しているサイバー攻撃をはじめとする情報セキュリティインシデントへの学習意欲が高いことがわかる。これは，今回行った講義の内容も影響しているが，情報セキュリティインシデントに関する報道内容を理解することが難しいことが一因である。特に，ランサムウェアに関連した被害は，システムの暗号化による障害や，個人情報の流出，身代金の支払いの有無など広範囲に渡るため，インシデント自体の把握が難しく全体像を理解しにくい。このため，学習意欲の動向もこうした内容に集中していると思われる。

これ以外の学習傾向は，学生の身近な生活に密着した情報セキュリティに関する内容が多くなっている。その

ため，4 位に日常生活・身近なセキュリティが入っており，これに関連した項目が多数みられる。加えて，本学では多くの学生が経営や経済を学んでいるため，企業のセキュリティやリスクマネジメントへの興味も高くなっており，あわせて関連法律の学習希望の高まりも示されている。

一方で，情報セキュリティに関するテクノロジー分野に対する学習ニーズは低くなっている。これは，やはり文系の学生が多くため，ICT 分野の理系に関連する学習分野であるプログラミング，ネットワーク，暗号等に対するニーズは低くなっている。

5. 共起ネットワークによる分析

さらにアンケートにおいて，「社会全体として情報セキュリティを高めるためにはどのようにしたらよいでしょう」という問いに対して自由記述で回答させている。

この記述内容に対して，KHCoder[4]を用いて計量テキスト分析を行い，Excel の 1 つのセルまたは 1 行を集計単位として，出現数による語の取捨選択における最小出現数を 5，文章数による語の取捨選択における最小文章数を 1 と設定して，図 1 のような共起ネットワーク（一部分を抽出）を作成した。

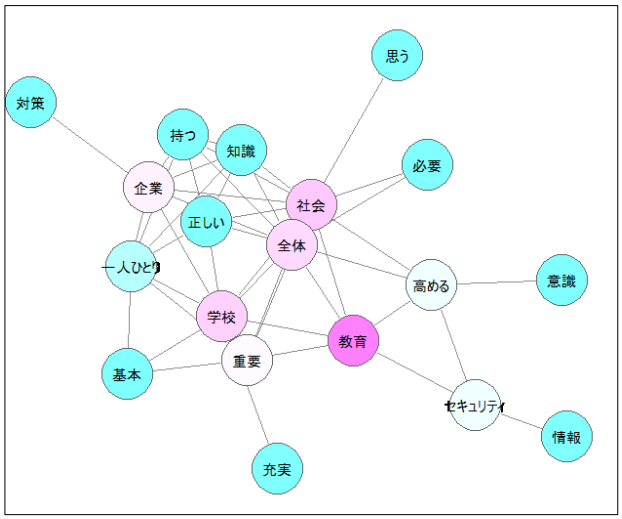

図 1 自由記述の共起ネットワーク

社会全体として情報セキュリティを高める方策という問いに対する回答は，多種多様となる。今回，回答した学生の特徴として，1 年生であり情報セキュリティの初学者であることから，専門的な技術やマネジメントを用いた手法に関する記述はほとんど見られなかった。そのため，本質的な解決策について，何が必要であるかを多く回答していた。

具体的には，情報セキュリティを高めるためには教育の重要性について述べている回答が多いことがわかる。そのため，教育に関連して学校や正しい知識といったキーワードの関連性がみられる。こうしたことから，学校などで情報セキュリティに関する教育を実施して，正しい知識を身に付けることで，社会全体として情報セキュリティを高めることができると考えていることがわかる。

さらに，詳細に自由記述の内容を分析すると，低年齢からの情報セキュリティ教育の必要性を述べている。特に，義務教育段階から情報セキュリティの学習をするべきであるや，学習を通じてリテラシーの向上が重要であるという主張が多くみられた。

6. 考察

今回，実施したアンケートは情報社会において情報セキュリティが必要不可欠なスキルであることから，学生たちの多くが興味・関心を持っていることがわかった。一方で，本学の学生は多様な高校から入学しており，情報セキュリティに関する学習の内容にばらつきがみられるようである。

そのため，自身の情報セキュリティ対策があまりできていないとともに，企業の情報セキュリティ対策への不安を抱いていた。こうした状況の中で，社会全体として情報セキュリティを高めるために，教育や個人のリテラシーの向上が必要であることを示していた。

このようなアンケートの結果から，未就学児からスマートフォンを使用し，小学校に入学以降は GIGA スクール構想によって PC とともに学習を行っており，実効性のある形で発達段階に応じた情報セキュリティ教育の必要性を示唆している。

次期学習指導要領では，小学校の総合的な学習の時間に情報の領域，中学校で情報・技術科の設置が行われ，デジタル学習基盤を前提にしようとしていることからも，児童生徒の情報セキュリティ意識の育成が求められる。

さらに，情報活用能力の抜本的向上に向けて，情報技術の活用，適切な扱い，特性の理解という観点を用いてアプローチすることから，情報セキュリティを基礎とした系統的なデジタルリテラシーを身に付けられるようにしなければならない。

今後は，情報セキュリティ教育が特別な教育ではなく，一般的なリテラシー教育の一環として幅広い年齢層で継続的な実施をしていけるような教育デザインの構築が求められる。

7. おわりに

本稿では，本学 1 年生に行った情報セキュリティに関する理解や意識に関する調査について分析を行うことで，学生の情報セキュリティに対する意識等を明らかにし，社会全体として情報セキュリティを高めるため方策について検討した。

今後は，大学での基礎教育として情報セキュリティ教育を実践し，初等中等教育におけるデジタルリテラシーを高めつつ情報セキュリティを確保できる教育デザインの研究を進めたいと考えている。

参考文献

(1) アサヒグループホールディングス，サイバー攻撃被害の再発防止策とガバナンス体制の強化について，https://www.asahigroup-holdings.com/newsroom/detail/20260218-0101.html（閲覧日：2026.6.14）

(2) ASKUL，アスクルのサイバーセキュリティ，https://www.askul.co.jp/corp/security/（閲覧日：2026.6.14）

(3) (独)情報処理推進機構, 情報セキュリティ白書 2025, pp.141-144，(独)情報処理推進機構(2025)

(4) KH Coder，KH Coder:計量テキスト分析・テキストマイニングのためのソフトウェア，https://khcoder.net/（閲覧日：2026.6.14）