AI の脅威やリスクの認識に違いはあるのか*
ー「AI 利用時のセキュリティ脅威・リスク調査」結果の分析ー

小山 明美[1]　竹村 敏彦[1,2]

概要：近年，生成 AI の新サービスの登場により，業務における AI 利用の機会が増加している．しかしながら，AI 利用に伴う脅威やリスクについては十分な検討がなされているとはいえず，悪用や誤用によるサイバー攻撃やインシデントの発生が懸念される．現状を把握するために，独立行政法人情報処理推進機構は 2024 年に企業・組織の IT 実務担当者を対象に実施した「AI 利用時のセキュリティ脅威・リスク調査」を実施した．本研究では，この調査結果を簡単に紹介するとともに，これらの個票データを用いて，業務における AI サービスの利用状況およびセキュリティ上の脅威・リスクの認識や対策の取り組み状況等に関する属性分析を試みる．そして，この分析結果を踏まえて，AI 利活用を促進するために必要な施策や計画への示唆を示す．

キーワード：AI　セキュリティ

Do We Have Differences in Perceptions of AI Threats and Risks? Analysis of Survey on Security Threats and Risk in Using AI

KOYAMA, AKEMIHI[1]　TAKEMURA, TOSHIHIKO[1,2]

Abstract: In recent years, opportunities to use AI in business have been increasing due to the emergence of new services of generative AI. However, the threats and risks associated with the use of AI have not been sufficiently studied, and there are concerns about the occurrence of cyber attacks and incidents due to misuse and abuse.

Keywords: AI　Security

1. はじめに

2022 年秋に ChatGPT3.5 がリリースされ，それまで直接 AI に触れる機会が無かった人々も容易に利用できるようになった．操作方法の容易さもあり，その利用範囲は個人だけでなく，会社・組織などにおいて業務でも活用が広がった．そして，利活用の拡大とともに AI な問題が指摘され，安全な利用のための議論が活発になってきた．本研究では，特にセキュリティに着目して AI の利用における脅威やリスクについて，調査し，分析を行った．

AI の利用にまつわるセキュリティ的な問題の一つに，AI の誤用と悪用がある．意図せず機密情報を入力してしまったことによる情報漏えい，学習に用いられたオリジナルの著作物に類似，あるいはそのまま引用されているのを生成されたものと考え利用してしまう著作権侵害，ハルシネーション（AI が事実と異なる情報を生成）に気づかずにその情報を業務に利用して誤判断や経済損失を与えてしまうといった問題が挙げられている．これらは，AI の仕組みやその脅威・リスクが十分理解されないうちに，生成 AI の利用が広がってしまったために起きている可能性が高く，利用における誤用に相当する．また，偽画像，偽動画を生成し，SNS 等で拡散させたり，偽音声，偽メールなどで誰かを騙そうとしたり，情報かく乱や詐欺等を目的に意図的に AI を悪用することが懸念されている．

今や DX(デジタルトランスフォーメーション)により，ビジネスにおけるデータの利活用，業務の自動化・効率化などにおいてデジタル技術の導入が進んでいる．AI もその新しい IT 基盤の一つとして効果が期待されている．したがって，先に挙げたような様々な問題・課題を踏まえて，自らの AI 利用における脅威やリスクを検討して，対策を行ったうえで利用をすることが望ましい．

独立行政法人情報処理推進機構（IPA）では，AI を利用する際，企業・組織ではセキュリティの脅威やリスクをどのように認識しているのか，対策が検討されているのか，実態を把握するため，2024 年 3 月に「AI 利用時のセキュリティ脅威、リスク調査」（IPA 調査）を行った．

調査概要は以下の通りである．

調査期間　２０２４年３月１８日～２１日
調査方法　ウェブアンケート
回収数　事前調査　企業・組織で従事する人　4941 人
　　本調査　予備調査の回答者の中で
　　AI を業務で利用している人　1000 人

* 本稿の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

1 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan (IPA)
2 城西大学
Josai University

© 2024 Information Processing Society of Japan

This paper is work in progress and not peer-reviewed.

「あなたの所属する組織で，業務での AI 利用、あるいは、職員の業務での AI 利用許可をしていますか？」と質問した結果を以下の図 1-1 に示す.

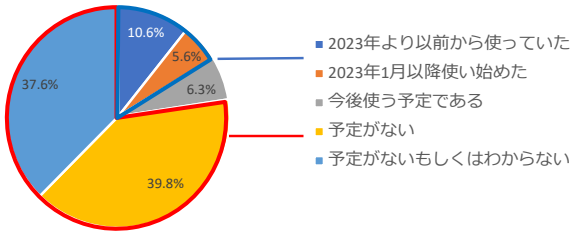


図 1 -1　AI サービスの利用結果

結果，業務で AI を利用/許可しているのは 16.2%，予定ありを合わせても 22.5%（回答者 4,941 人中 1,114 人）とまだ十分浸透はしていない.

AI を利用していない/許可していない，予定もないと回答した 3,827 人に「あなたの組織が AI サービスを利用/許可しておらず、導入予定もない理由は何ですか？」と質問したところ以下の図 1-2 に示す回答を得た.

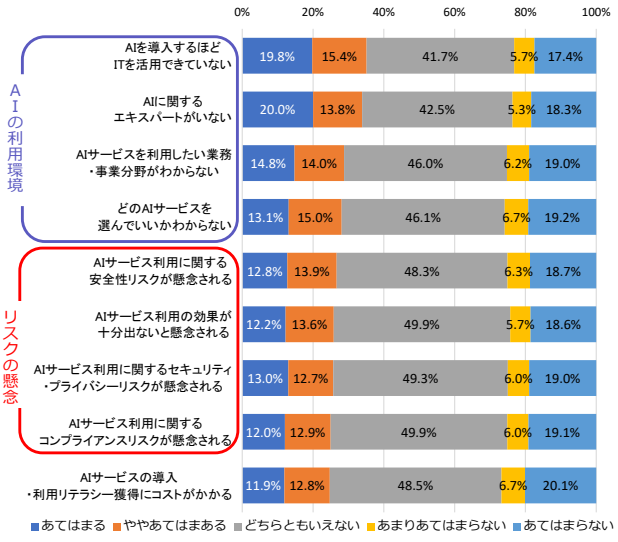


図 1-2　業務に AI を利用しない理由

「あてはまる」「ややあてはまる」を合わせて最も多かったのは「AI を導入するほど IT を活用できていない」続いて「AI に関するエキスパートがいない」「AI サービスを利用したい業務・事業分野がわからない」と続く．セキュリティや安全に対するリスクを懸念するとの回答が 4 分の 1 程度あったが，AI を利用する環境が整っていないことが，利用/許可しないことの一番の要因であることが分かった.

2.　AI のセキュリティ・リスク

AI のセキュリティにまつわるリスクについては，各国，機関が検討を行っている段階である．IPA が発行した情報セキュリティ白書 2024 では，サイバーセキュリティリスクの詳細な分析を以下の三つの類型に分けた。

① AI の悪用

代表例としては、無制限な軍事利用、暴力・犯罪・サイバー攻撃への悪用、フェイクコンテンツ拡散による権利侵害・対立扇動、悪意のボット・ウイルス生成等がある。

② AI の機能特性による誤判断・誤用

代表例としては、誤判断による自動走行事故、生成 AI の不適切な学習やプロンプト処理による差別的回答・情報漏えい・誤情報拡散等がある。

③ AI の機能特性を突いた攻撃脅威

AI モデルの特性により、特定のデータやパターンを含む入力に対して間違った予測・分類結果が出力される場合がある。こうした AI を間違えさせる入力は「敵対的サンプル（Adversarial example）」と呼ばれ、AI モデルの特性を調べる手段となっているが、これを逆手に取った多くの攻撃手法が存在する。一方、学習時点において学習データにノイズを混入させ、AI モデルの性能を劣化させる、あるいは意図的な誤判定を誘導する攻撃（データポイズニング）もよく知られている。

本研究では，これらのリスクのいくつかについて具体的に脅威を感じているのか，課題と認識しているかを AI 利用者に調査した.

3.　仮説

本研究では，以下の 2 つの仮説を立てた.

仮説 1：「生成 AI のセキュリティに関する脅威」の評価は回答者属性（企業属性・個人属性）の違いによって異なる.

仮説 2：「生成 AI の利用・普及における課題」の感じ方は回答者属性（企業属性・個人属性）の違いによって異なる.

4.　アンケート調査

4.1　調査概要

IPA は，2024 年 3 月 18 日から 21 日の間に「AI 利用時のセキュリティ脅威・リスク調査」（以下，「本調査」と称す）[1]を実施した．「本調査」は，新しい技術として AI が業務利用されつつある状況の中，AI のセキュリティ・リスクの認識や安全な利用のための組織内の規程や体制がどこまで進んでいるのかの実態を把握する目的で実施され，取りまとめられたものである.

「本調査」は，スクリーニング調査にて，回答者の基本情報に関わる質問とともに，AI の利用状況，AI 利用上の

© 2024 Information Processing Society of Japan

立場，最重要 AI，AI を利用／許可しない理由，担当業務，AI 理解度等に関する質問を行い，この中で，AI を業務に利用／許可している（予定も含む）回答者（実際に何らかの AI を業務に利用している企業・組織の実務担当者）を対象者としている．最終的な有効回答者数は 1,000 人である．調査内容としては，AI の業務利用時の検討項目と重要度，AI 利用における管理コストの負担，AI 利用に関する組織の対応手順や体制，AI のセキュリティに関する脅威，生成 AI の利用・評価における課題や生成 AI で生成したコンテンツの課題に関する質問等がある．

以下，本研究と関連する質問項目に関する回答結果の概況を紹介する[a]．これらの質問項目以外については文献[1]を参照されたい．

4.2 質問項目と概況

(1) 回答者属性（企業属性も含む）

表 1 には，「本調査」の回答者の基本属性をまとめたものである．

表 1　回答者属性

Table 1　Respondents' Attributes.

		#			#
年齢	20～29才	103	従業員数	20人以下	82
	30～39才	220		21～50人	84
	40～49才	221		51～100人	84
	50～59才	221		101～300人	161
	60～69才	124		301～500人	82
	70～79才	111		501～1000人	109
職業	会社・団体の経営者・役員	118		1001～5000人	187
	会社員（契約・派遣社員含む）	831		5001～10000人	72
	公務員	51		10001人以上	139
部門	経営層	94	業種	製造業	221
	IT部門	167		卸売業・小売業	90
	リスクマネジメント部門	230		情報通信業	145
	事業部門	204		サービス業	136
	その他	305		その他	408

(2) 生成 AI のセキュリティに関する脅威

「本調査」には，回答者の組織にとって，以下のような生成 AI のセキュリティがどの程度の脅威であるかを問う質問がある．

（脅威 1）生成 AI の誤用によるプロンプト（質問）入力不備に起因する情報漏えい

（脅威 2）生成 AI の誤用による文書チェック・検証不備に起因する事業トラブル

（脅威 3）生成 AI の誤用によるソフトウェア開発コードの不備に起因するシステム障害・サイバー攻撃（脆弱性をつかれる，等）

（脅威 4）職員が自宅で生成 AI を不用意に使うことによる営業秘密漏えい（生成 AI に学習させてしまう，など）

これらの内容に対して，回答者に「全く脅威ではない」「あまり脅威ではない」「どちらともいえない」「やや脅威である」「重大な脅威である」といった 5 つの選択肢の中から最も考えに近いものを選択してもらっている[b]．

図 2 はこれらの 4 つの脅威に対する回答の分布を表したものである．図 2 から 6 割近い回答者が 4 つの事柄に対して脅威に感じていることがわかる．

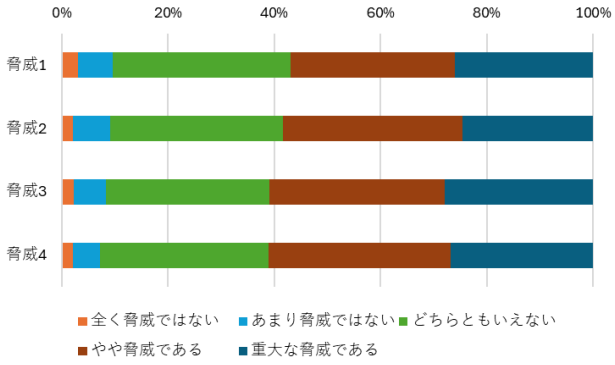


図 2　生成 AI のセキュリティに関する脅威

Figure 2　Threats to the Security of Generative AI.

(3) 生成 AI の利用・普及における課題

「本調査」あなたの組織にとって，には，回答者の組織にとって，以下のような生成 AI で生成したコンテンツの普及で生じうる課題についての評価を問う質問がある．

（課題 1）業務で扱う情報に生成 AI コンテンツと通常のコンテンツが混在し，どれが生成 AI 由来であるかわからなくなる

（課題 2）業務で作成した生成 AI 由来の文書の誤りが検知できず，事業に支障が出る

（課題 3）業務で扱った生成 AI コンテンツに倫理上の問題があり，事業に支障が出る（利用した生成ＡＩの学習に問題が発覚，等）

（課題 4）業務で扱った生成 AI コンテンツに知財権上の問題があり，事業に支障が出る（利用した生成 AI の学習に問題が発覚，等）

（課題 5）悪意の生成 AI コンテンツを含む詐欺攻撃を受け，金銭・情報を窃取される（フェイク画像・音声による詐欺，巧妙なフィッシングメール等）

これらの内容に対して，回答者に「全く課題であると思わない」「あまり課題であると思わない」「どちらともいえない」「やや課題だと思う」「非常に大きな課題だと思う」といった 5 つの選択肢の中から最も考えに近いものを選択してもらっている．

図 3 はこれらの 5 つの課題に対する回答の分布を表したものである．図 2 から 6 割を超える回答者が 4 つの事柄に

a なお，「本調査」は当時の状況を表しているものであり，現在では状況が変わっている可能性があることを断っておく．

b 選択肢の中には，「わからないもしくはつかわない」もあるが，本研究においては，脅威の大きさを評価できていないと捉えて，これを「どちらともいえない」とまとめていることを断っておく．課題に関しても同様に「わからない」を「どちらともいえない」とまとめている．

© 2024 Information Processing Society of Japan

対して課題に思っていることがわかる．

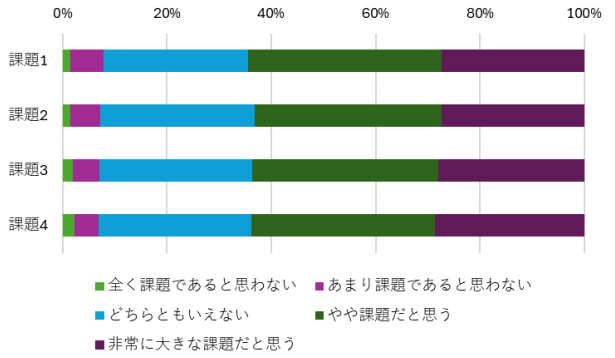


図 3　生成 AI の利用・普及における課題

Figure 3　Issues in the Use and Diffusion of Generative AI.

(4)　AI に関する知識（理解）

「本調査」には，AI に関する知識を問うクイズ（11 問）が含まれている．それぞれのクイズの正答数をもって AI に関する知識の水準を表すものと考える[2,3]．また，見方を変えるとこの知識水準は AI への理解であるともいえる．

この得点の分布を表したものが図 4 である．なお，AI に関する知識の平均値は 6.301 点，中央値は 7 点となっている．また AI に関する知識の最頻値は 6 点である．

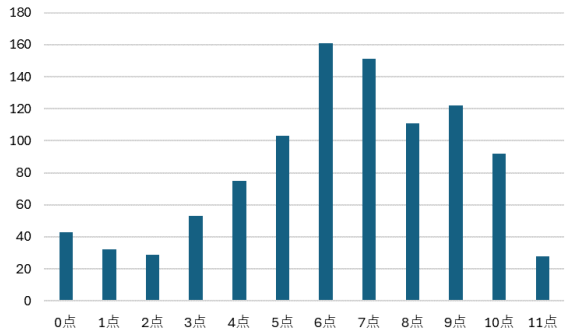


図 4　AI に関する知識（理解）

Figure 4　AI Knowledge.

5.　分析

5.1　分析手法とデータ加工

第 4.2 節で見たように，「生成 AI のセキュリティに関する脅威」と「生成 AI の利用・普及における課題」の評価はいずれも 5 件法でもって測定しているため，第 3 節で示した仮説をノンパラメトリックな手法による多重比較を行って検証する必要がある．本研究では，多重比較には Steel-Dwass 法（Tukey 法のノンパラメトリック版）を採用する．Steel-Dwass 法は，平均値ではなく中央値が有意にグループ毎に異なるか否かを統計的に検定するための手法である[4].

ノンパラメトリックな手法による多重比較を行うためには，第 4.2 節で紹介した表 1 の回答者の属性のうち（「(所属している企業の）従業員数」ならびに「(回答者自身の）AI に関する知識水準」）をグループ変数として加工する必要がある（なお，「(所属している企業の）業種」と「(所属している企業の）部門」は表 1 の通り 5 つのグループとして分析に用いる）．

まず，（所属している企業の）従業員数は，「100 人以下（小規模）」「101 人以上 1,000 人以下（中規模）」「1001 人以上（大規模）」の 3 つのグループとする（多重比較における組合せ数が膨大になるのを避けるため）．

次に，図 4 にあるように AI に関する知識水準は 0 点から 11 点の範囲をとり，3 点以下であれば「知識低」，4 点以上 7 点以下でれば「知識中」，8 点以上であれば「知識高」の 3 グループとする．なお，表 2 は属性毎の回答者数をまとめたものである．

表 2　属性ごとの回答者数

Table 2　Number of Respondents per Individual Attribute.

		#			#
部門	経営層	94	業種	製造業	221
	IT部門	167		卸売業・小売業	90
	リスクマネジメント部門	230		情報通信業	145
	事業部門	204		サービス業	136
	その他	305		その他	408
従業員数	100人以下（小規模）	250	AIに関する知識水準	知識高	353
	101人以上1,000人以下（中規模）	398		知識中	490
	1,001人以上（大規模）	352		知識低	157

5.2　分析結果

表 2 に示した回答者の属性に基づいて，「生成 AI のセキュリティに関する脅威」と「生成 AI の利用・普及における課題」の評価のノンパラメトリックな手法による多重比較を行った結果，まず「業種」に関してはいずれのグループの組合せにおいて，いずれも統計的に有意差は確認できなかった．そのため、紙面の都合上，多重比較の結果は省略した．

表 3　分析結果 1-1

Table 3　Result 1-1.

	Comparison		脅威		課題	
			Estimator	Statistic	Estimator	Statistic
1	小規模	大規模	0.551 *	2.283	0.499	-0.053
	小規模	中規模	0.576 ***	3.343	0.529	1.254
	大規模	中規模	0.526	1.266	0.531	1.556
2	小規模	大規模	0.543	1.900	0.479	-0.946
	小規模	中規模	0.544	1.911	0.534	1.479
	大規模	中規模	0.502	0.110	0.556 ***	2.822
3	小規模	大規模	0.561 **	2.742	0.483	-0.776
	小規模	中規模	0.579 ***	3.493	0.514	0.604
	大規模	中規模	0.519	0.934	0.532	1.570
4	小規模	大規模	0.541	1.822	0.498	-0.104
	小規模	中規模	0.552 *	2.293	0.509	0.381
	大規模	中規模	0.512	0.574	0.511	0.545
5	小規模	大規模			0.496	-0.168
	小規模	中規模			0.517	0.743
	大規模	中規模			0.521	1.064

***: 1%, **:5%, *:10%

表 4　分析結果 2

Table 4　Result 2.

© 2024 Information Processing Society of Japan

	Comparison		脅威 Estimator	脅威 Statistic	課題 Estimator	課題 Statistic
1	IT部門	その他	0.491	-0.335	0.421 **	-3.014
	IT部門	リスクマネジメント部門	0.431	-2.498	0.468	-1.141
	IT部門	経営層	0.447	-1.437	0.506	0.174
	IT部門	事業部門	0.525	0.885	0.488	-0.431
	その他	リスクマネジメント部門	0.442	-2.420	0.547	1.966
	その他	経営層	0.457	-1.297	0.579	2.340
	その他	事業部門	0.533	1.332	0.569 **	2.833
	リスクマネジメント部門	経営層	0.511	0.317	0.535	1.014
	リスクマネジメント部門	事業部門	0.594 ***	3.614	0.520	0.780
	経営層	事業部門	0.576	2.145	0.483	-0.484
2	IT部門	その他	0.471	-1.113	0.428 **	-2.765
	IT部門	リスクマネジメント部門	0.420 **	-2.902	0.437	-2.315
	IT部門	経営層	0.467	-0.921	0.497	-0.069
	IT部門	事業部門	0.500	0.013	0.480	-0.693
	その他	リスクマネジメント部門	0.454	-1.941	0.504	0.146
	その他	経営層	0.495	-0.144	0.562	1.846
	その他	事業部門	0.527	1.091	0.548	1.943
	リスクマネジメント部門	経営層	0.543	1.247	0.556	1.663
	リスクマネジメント部門	事業部門	0.578 **	2.980	0.544	1.656
	経営層	事業部門	0.533	0.945	0.486	-0.398
3	IT部門	その他	0.477	-0.876	0.456	-1.693
	IT部門	リスクマネジメント部門	0.442	-2.072	0.477	-0.834
	IT部門	経営層	0.466	-0.913	0.531	0.839
	IT部門	事業部門	0.517	0.593	0.506	0.212
	その他	リスクマネジメント部門	0.469	-1.304	0.520	0.816
	その他	経営層	0.485	-0.429	0.568	2.012
	その他	事業部門	0.540	1.636	0.547	1.893
	リスクマネジメント部門	経営層	0.516	0.428	0.550	1.451
	リスクマネジメント部門	事業部門	0.575 **	2.884	0.528	1.061
	経営層	事業部門	0.550	1.396	0.478	-0.621
4	IT部門	その他	0.477	-0.904	0.491	-0.351
	IT部門	リスクマネジメント部門	0.432 *	-2.463	0.502	0.079
	IT部門	経営層	0.435	-1.779	0.532	0.853
	IT部門	事業部門	0.487	-0.443	0.525	0.886
	その他	リスクマネジメント部門	0.461	-1.622	0.509	0.377
	その他	経営層	0.458	-1.261	0.536	1.023
	その他	事業部門	0.511	0.464	0.533	1.337
	リスクマネジメント部門	経営層	0.494	-0.158	0.527	0.772
	リスクマネジメント部門	事業部門	0.555	2.084	0.522	0.846
	経営層	事業部門	0.554	1.495	0.493	-0.184
5	IT部門	その他			0.477	-0.882
	IT部門	リスクマネジメント部門			0.448	-1.899
	IT部門	経営層			0.545	1.208
	IT部門	事業部門			0.523	0.800
	その他	リスクマネジメント部門			0.473	-1.128
	その他	経営層			0.557	1.685
	その他	事業部門			0.539	1.561
	リスクマネジメント部門	経営層			0.586 *	2.464
	リスクマネジメント部門	事業部門			0.567 *	2.549
	経営層	事業部門			0.482	-0.518

***: 1%, **:5%, *:10%

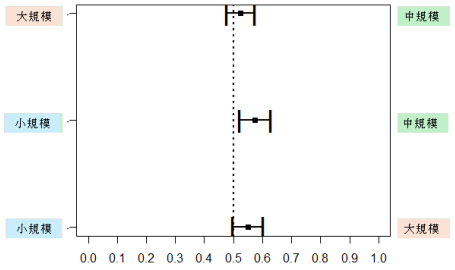
続いて，「従業員数」「部門」「AI に関する知識水準」に関する 4 つの「生成 AI のセキュリティに関する脅威」と 5 つの「生成 AI の利用・普及における課題」の多重比較の結果をまとめたものが表 3 から表 5 である．例えば，表 3 において脅威 1（生成 AI の誤用によるプロンプト入力不備に起因する情報漏えい）の評価は小規模グループと大規模グループ，小規模グループと中規模グループにおいて，それぞれ統計的な差異があることが確認された．しかしながら，大規模グループと中規模グループの間には統計的な差異は確認されなかった．また，課題 1（業務で扱う情報に生成 AI コンテンツと通常のコンテンツが混在し，どれが生成 AI 由来であるかわからなくなる）の感じ方は大規模グループ，中規模グループおよび小規模グループを問わず，これらのグループ間には統計的な差異は確認されなかった．

表 5　分析結果 3-1

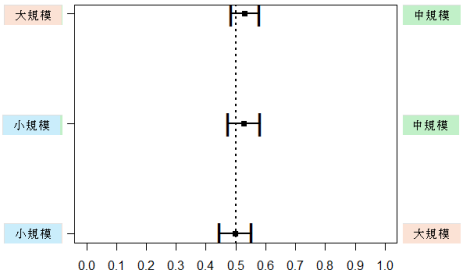
Table 5　Result 3-1.

	Comparison		脅威 Estimator	脅威 Statistic	課題 Estimator	課題 Statistic
1	知識高	知識低	0.313 ***	0.257	0.374 ***	-4.959
	知識高	知識中	0.452 **	0.407	0.483	-0.884
	知識低	知識中	0.640 ***	0.585	0.621 ***	4.858
2	知識高	知識低	0.339 ***	0.280	0.359 ***	-5.623
	知識高	知識中	0.443 ***	0.398	0.463	-1.961
	知識低	知識中	0.607 ***	0.550	0.602 ***	4.226
3	知識高	知識低	0.319 ***	0.261	0.321 ***	-7.347
	知識高	知識中	0.452 **	0.407	0.465	-1.838
	知識低	知識中	0.640 ***	0.583	0.649 ***	6.311
4	知識高	知識低	0.327 ***	0.271	0.285 ***	-9.348
	知識高	知識中	0.452 **	0.406	0.440 ***	-3.126
	知識低	知識中	0.635 ***	0.580	0.668 ***	7.261
5	知識高	知識低			0.330 ***	-7.098
	知識高	知識中			0.461	-2.018
	知識低	知識中			0.639 ***	5.940

***: 1%, **:5%



(a)　脅威 1



(b)　評価 1

図 5　分析結果 1-2

Figure 5　Result 1-2.

図 5 はこれらの結果（どちらのグループの値の方が大きいか）を可視化したものとなる．表 3 の Estimator の値が 0.5 よりも大きければ，1 つ目のグループよりも 2 つ目のグループの方が脅威の評価（課題と思っている程度）がより大きいことを意味する．図 5 の(a)を見てみると，小規模グループよりも大規模グループ（また，小規模グループよりも大規模グループ）の方が，脅威 1 をより脅威であると評価していることが確認できる．他方，大規模グループと中規模グループの場合，脅威 1 に対する評価の程度に差がないことが確認できる．

表 3 を見ると，脅威も課題も回答者の属している企業属性である「従業員数」（企業規模）においては「脅威 1」と「脅威 3（生成 AI の誤用によるソフトウェア開発コードの不備に起因するシステム障害・サイバー攻撃）」の評価は小規模グループと大規模グループ（中規模グループ）の間に統計的な差異が確認されたが，大規模グループと中規模グループの間には統計的な差異は確認されなかった．また「脅威 2（生成 AI の誤用による文書チェック・検証不備に起因する事業トラブル）」の評価についてはいずれのグループにおいても統計的な差異は確認されなかった．「脅威 4（職員が自宅で生成 AI を不用意に使うことによる営業秘密漏え

© 2024 Information Processing Society of Japan

い)」の評価は小規模グループと中規模グループの間で統計的差異は確認されたが，それ以外のケースにおいては確認されなかった．また，「課題」においては「課題 2（業務で作成した生成 AI 由来の文書の誤りが検知できず，事業に支障が出る)」に関して統計的差異が確認されたのは，大規模グループと中規模グループの間のみであった．

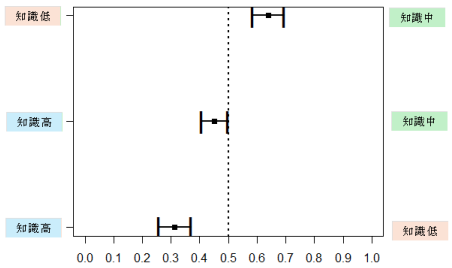
表 4（回答者の所属している企業の部門）に関しては，「脅威」ならびに「課題」においていくつかの組合せでグループ（部門）間で統計的な差異は確認されたが，多くのケースで統計的な差異は確認されなかった．

表 3 と表 4 ではグループ間で統計的な差異が確認されるケースは少なかったものの，表 5（回答者の AI に関する知識水準）に関して，いずれの「脅威」においても 3 つのグループ間で統計的な差異が確認された。他方，「課題」においては知識高グループと知識低グループ間，ならびに知識低グループと知識中グループ間で統計的な差異が確認され．「課題 4 (業務で扱った生成 AI コンテンツに知財権上の問題があり，事業に支障が出る)」を除き，知識高グループと知識中グループ間には統計的な差異は確認されなかった．図 6 には，「脅威 1」から「脅威 4」までの評価の高低を可視化した結果を示している．図 6 を見てわかるように，いずれの脅威に対する評価も，最も高いのが知識高グループ，続いて知識中グループ，そして最も低いのが知識低グループとなった．つまり，AI に関する知識水準が上がるにしたがって，脅威と評価したり，課題と思う程度が高くなったりする傾向にあることが確認された．また，紙面の都合上，省略したが，「課題」に関しても知識高グループと知識低グループの間に同様の傾向があることが確認された．

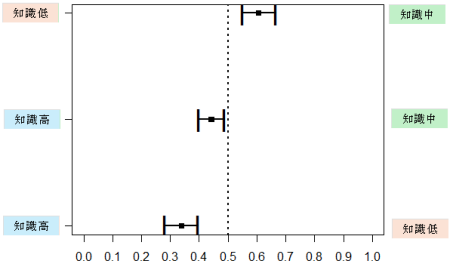
5.3 考察

今回の調査では，企業における生成 AI の利用上想定されるセキュリティ上の脅威やリスクについて，どの程度認識されているのかを調査，分析した．結果，認識の程度は全体として高いが個別の項目ごとの差が小さく，優先すべき課題を明らかにするには，さらなる分析が必要であると考えられた．回答者の属性による差があるかを分析した結果，業種による差は見られなかった，規模による差は，一部に有意な違いを確認できたが，傾向を十分示すものではなかった，さらに AI に関する知識水準で分析を行ったところ，優位な差がみられた．知識水準が高いほど，脅威の評価が高い，課題の認識が高いということが示された．

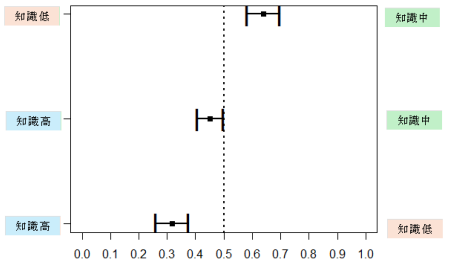
IPA 調査によると利用しない理由は，AI の利用環境が整っていないことの方がリスクの懸念より多かったが，利用環境には AI に関するエキスパートがいないことが含まれており，AI に関する知識水準が高い人材のアサインが AI の利用促進と脅威・リスクを適切に認識し対策することに重要であることが分析結果からも分かった．仮説 1，2 について，今回の調査では企業属性よりも個人属性，特に知識が脅威の評価や課題の感じ方に影響することが分かった．



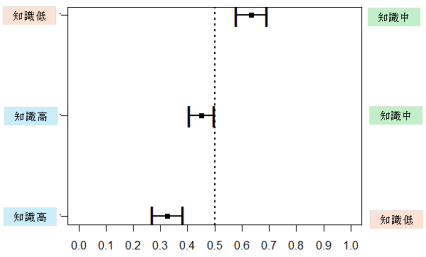
(a) 脅威 1



(b) 脅威 2



(c) 脅威 3



(d) 脅威 4

図 6 分析結果 3-2（脅威）

Figure 6 Result 3-2 (Threats).

参考文献

[1] 情報処理推進機構 : IPA テクニカルウォッチ「AI 利用時のセキュリティ脅威・リスク調査報告書」 https://www.ipa.go.jp/security/reports/technicalwatch/20240704.html

[2] 島成佳，小川隆一，佐川陽一，竹村敏彦．“AI 誤判断による価値損失の定量的評価”．コンピュータセキュリティシンポジウム 2022 論文集, 2022, p.759-766.

[3] 竹村敏彦，島成佳，小川隆一，佐川陽一．AI 誤判断を含むサービスの市場受容に関する定量的評価，コンピュータセキュリティシンポジウム 2023 論文集, 2023, p.950-957

[4] 永田靖・吉田道弘．統計的多重比較法の基礎，サイエンティスト社, 2007

© 2024 Information Processing Society of Japan