様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　(共通)

科学研究費助成事業　　研究成果報告書

令和　５ 年　６ 月　５ 日現在

機関番号：１０１０１

研究種目：基盤研究(C)（一般）

研究期間：2020～2022

課題番号：２０Ｋ１２５５６

研究課題名（和文）技術流出防止のための、人工知能による新規の該非判定支援システムの開発

研究課題名（英文）Development of Interactive Advisory System for Security Export Control

研究代表者

大林　明彦（OBAYASHI, AKIHIKO）

北海道大学・産学・地域協働推進機構・教授

研究者番号：８０７９８１２４

交付決定額（研究期間全体）：（直接経費）　2,800,000円

研究成果の概要（和文）：研究成果や技術の輸出管理規制への影響を考慮し、学者への助言を目的としたチャットシステムを開発した。しかし、専門家が不足しているため、AI技術を活用して専門家の負担を軽減することが求められている。そこで、輸出管理規制に関する法文を対話的に誘導するシステムを開発した。さらに、論文の分析や同義語、CAS番号、EU法文の番号の検索、外国人研究者のための自動翻訳機能なども実装した。システムの用語集を拡充し、自然言語処理技術を活用することで、専門用語を含まないクエリにも対応できるようにした。実用的なシステムの構築が主な目的であったが、改善点を導入するために様々な実験を行い、その結果を国際会議で発表した。

研究成果の学術的意義や社会的意義
Our system aims to reduce expert workload and enhance researchers' awareness of often overlooked dangers. This is vital as the academic world is susceptible to potential threats to national security. Additionally, we demonstrated the unreliability of relying solely on neural methods.

研究成果の概要（英文）：We have designed a chatbot system to assist academics dealing with research output or technology subject to sensitive export control regulations. Due to a lack of experts in this field, it was crucial to develop AI technology that can ease their burden. Our solution was an interactive chat system that guides users to relevant sections of export control regulatory texts. It incorporates several features: publication uploading, synonym queries, CAS number retrieval, references to EU documents, and automated translation for foreign researchers. By expanding the system's glossary and leveraging natural language processing, it can handle non-technical queries unrelated to legal terms. While our primary objective was to create a functional system, we also conducted experiments, which are detailed in scientific publications.

研究分野：Security Export Control in Academia

キーワード：export control　trade security　expert system　dialog system

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

１．研究開始当初の背景

Recently, export control has been an urging topic not only in industry, but also in academia. Many countries worldwide have been expanding their export control efforts to prevent the transfer of goods, hardware, technologies, and software with military applications to hostile foreign governments or terrorist groups. This increased focus on export controls was triggered by the Toshiba-Kongsberg incident in 1987, where certain member nations of the Coordinating Committee for Multilateral Export Controls violated an agreement by illegally exporting tools to the Soviet Union. In response to this incident, the Japanese government strengthened their restrictions to avoid similar controversies. In 2017, Japan implemented significantly stricter penalties, increasing them by a hundredfold, from 10 million to 1 billion yen (equivalent to USD 96,200 to 9,620,000). Ignoring possible threats of research technology or results have become risky also for academics in Japan.

Our project started by matching common interests of the principal investigator who is a trade security expert and a natural language processing specialists working at the same university. As there is a significant shortage of export control specialists in Japan, inquiries take time, and we felt it would be meaningful to provide a tool which could be used by researchers to get familiar with the regulations before contacting the expert.

２．研究の目的

There is only a single half-automatic method for assisting academics with export control-related issues, namely answering manually prepared yes / no questions (Decision Tree) at the DoResearch site of Stanford University. Such approach has three main flaws: a) it is meant for researchers who have knowledge on the topics of trade security; b) it doesn't allow open questions; c) it is meant for U.S. academics (and created only in English language). To tackle these problems, we decided to join forces in our endeavor of building an interactive assistant AI, which could help Japanese researchers navigate through related legal sources by allowing free input. Except searching for related regulation passages, we decided to provide various functionalities to the proposed system which allow the user to upload publications, to query for synonyms, CAS numbers, numbers of related EU documents, or to automatically translate our system's utterances for foreign researchers working at a university.

The biggest challenges of this project were as follows: to disambiguate terms which differ between researchers and legal texts; to match the queries to the system, which can drastically vary in length, with related passages of regulatory texts; and to deploy the system as a working chatbot which would be easily accessible to anyone.

３．研究の方法

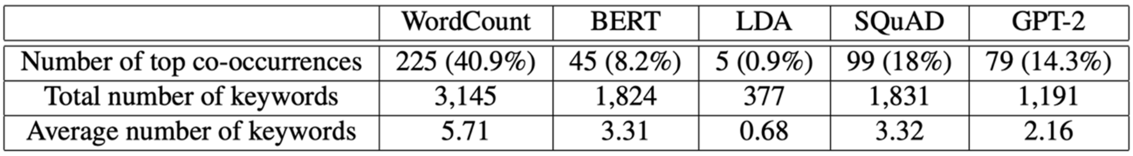
As there is a lack of widely shared knowledge among researchers regarding what can be exported or published according to export control regulations, the first step was to build a classifier capable of recognizing which research topics are closely related to export control (classic methods as Multinomial NB, Linear SVC, Logistic Regression and Random Forest were utilized). We have created a chat system for Slack environment where publications can be uploaded and analyzed on the server bought with the grant funds. But because users want to express their concerns or ask direct questions before writing a paper, sharing data via email or sending samples by mail, the main functionality was based on natural language techniques. Recently, to match users' utterances with regulatory text, the standard approach is to feed the system with big number of samples and let the machine learn how to answer the questions. But the main challenge in using machine learning for this task is the limited amount of data available, as legal documents are relatively short and creating question-answer pairs is difficult. To overcome this limitation, keyword matching became the baseline approach to retrieve relevant passages from legal documents, by using glossary terms and paragraph numbers. However, it was found that 20% of the question set did not contain sufficient keywords or article references. Given the average length and complexity of the questions, we decided to explore the use of neural models with contextual embeddings to refer to specific sentences in the regulatory documents. After obtaining some samples of questions and answers from the Japanese Center for Information on Security Trade Controls (CISTEC), we experimented with GPT-2 and BERT, or tried to utilize Japanese question and answer dataset (SQUAD) dataset to improve question answering capabilities of the system but the tested methods did not overpass results of keyword matching approach. Therefore, in this project we decided to use SentenceBERT for searching related passages which do not contain any terms and concentrated on extending the synonym glossary. After gathering information and suggestions from local specialists and foreign experts (as Prof. Steve Eisner, the Director of Export Compliance at Stanford), we started improving the system by enriching its vocabulary, namely the related (or synonymous) terms. As Prof. Eisner advised us, there are many controlled technologies used in industry under their specific names, for example nicknames of missiles. Hence, we decided to utilize knowledge embedded in Wikipedia by proposing several methods using links with titles and inner-links within articles. We also extended the CISTEC data by creating more questions and answers which are shorter and contain less information as the official FAQ. The most important findings of above-described experiments are given in the next section.

４．研究成果

The classification of publications was tested on two sets of publications on topic of “biological weapons” and “nuclear power” (400 papers in each set). We used 10 main categories out of 15 in the regulatory documents as Export Trade Control Order, the Foreign Exchange Order as well as the *Combined Matrix* (which tabulates these documents and is used by us as the base for the retrieval) and discovered that voting approach (using all outputs) yields the best results. However, results for “biological weapons” (90% accuracy) largely differed from “nuclear power” (58% accuracy) showing that there are research topic and categories that contain vocabulary from different domains.

For matching fuzzy queries from a user, we utilized several algorithms for ranking the most related passages from the regulatory texts and found out that classic methods as LDA and new neural methods (due to the small number of examples) do not work well (see Table 1).

Table 1

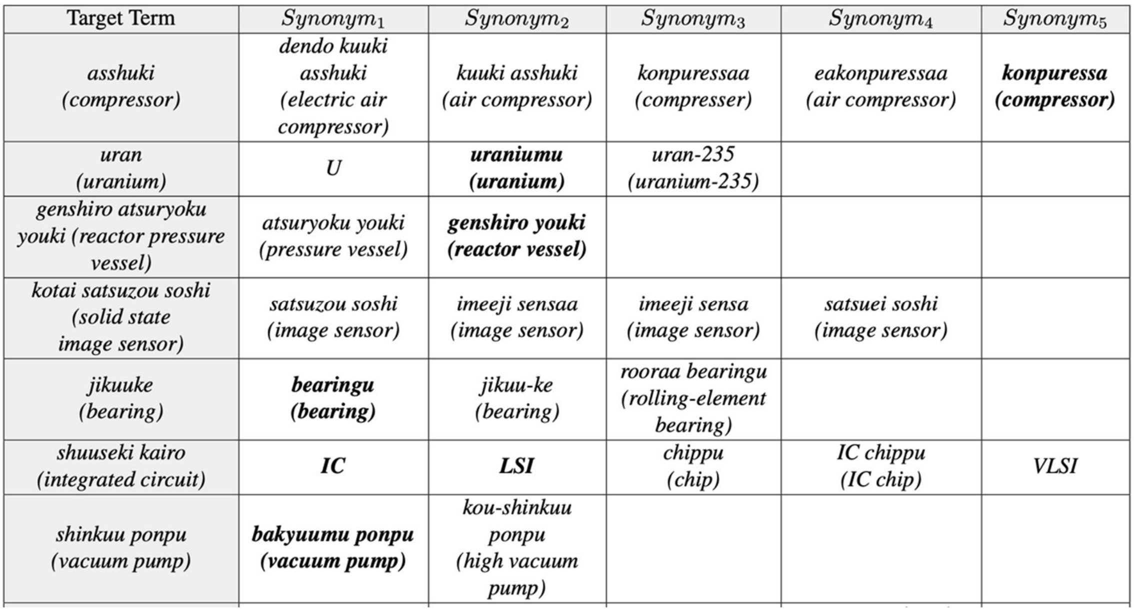


	WordCount	BERT	LDA	SQuAD	GPT-2
Number of top co-occurrences	225 (40.9%)	45 (8.2%)	5 (0.9%)	99 (18%)	79 (14.3%)
Total number of keywords	3,145	1,824	377	1,831	1,191
Average number of keywords	5.71	3.31	0.68	3.32	2.16

The main challenge for this task was the evaluation process. The goal was to determine if machine learning methods can effectively extract relevant passages from regulatory documents. However, this requires expert evaluators who are typically limited to a single person within an organization. While expert assessment is necessary in the long run, we aimed to provide accurate results and save the specialist's valuable time. To accomplish this, we employed a simple initial evaluation approach that measures the co-occurrence of glossary terms and article numbers between human-generated answers in the QA dataset and the top-ranked passages identified by specific models. But the results showed that directly matching glossary terms in regulatory documents outperforms embedding-based methods. This is expected since the terms are carefully selected by human specialists based on their significance. Additionally, we discovered that the classic LDA approach is notably inferior to BERT, indicating that contextualized embeddings contribute to the ranking of answers. The SQuAD-based model, despite using correct answers as context, frequently failed to provide any answer or outputs only a single term. Surprisingly, the GPT-2 generator achieved a relatively high score. However, a high occurrence of keywords did not guarantee a coherent generated answer, which is a common problem of currently popular generative models.

For enriching vocabulary of our dialog system and to increase proper matching capabilities for retrieving related passages for answers, we tested how inner-links and redirect functionality of Wikipedia can help to find synonyms of technical terms regarding export control regulations for the trade security. We discovered that although redirect-based methods yield much better results than inner-links, the expert-made thesaurus used for evaluation has too few overlaps with Wikipedia to achieve satisfactory F-score. However, a small evaluation performed by a single expert suggest that the tested methods have much bigger potential than the scores indicate. Some examples of extended glossary are shown in Table 2.

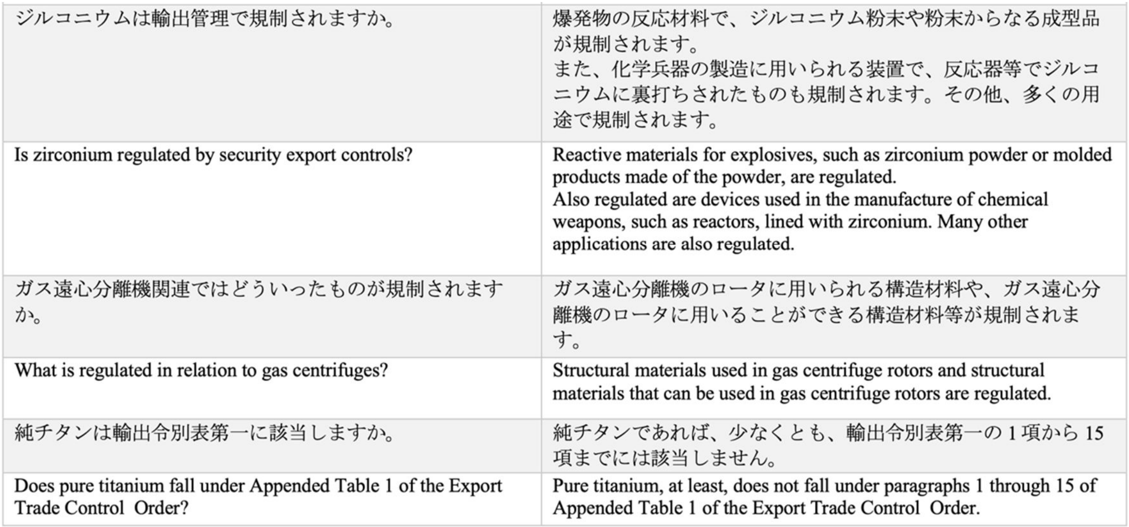
Table 2



Target Term	$Synonym_1$	$Synonym_2$	$Synonym_3$	$Synonym_4$	$Synonym_5$
asshuki (compressor)	*dendo kuuki asshuki (electric air compressor)*	*kuuki asshuki (air compressor)*	*konpuressaa (compresser)*	*eakonpuressaa (air compressor)*	***konpuressa (compressor)***
uran (uranium)	*U*	***uraniumu (uranium)***	*uran-235 (uranium-235)*		
genshiro atsuryoku youki (reactor pressure vessel)	*atsuryoku youki (pressure vessel)*	***genshiro youki (reactor vessel)***			
kotai satsuzou soshi (solid state image sensor)	*satsuzou soshi (image sensor)*	*imeeji sensaa (image sensor)*	*imeeji sensa (image sensor)*	*satsuei soshi (image sensor)*	
jikuuke (bearing)	***bearingu (bearing)***	*jikuu-ke (bearing)*	*rooraa bearingu (rolling-element bearing)*		
shuuseki kairo (integrated circuit)	***IC***	***LSI***	*chippu (chip)*	*IC chippu (IC chip)*	*VLSI*
shinkuu ponpu (vacuum pump)	***bakyuumu ponpu (vacuum pump)***	*kou-shinkuu ponpu (high vacuum pump)*			

Opposed to long questions and answers with many related keywords regarding mostly exceptions, we created an addition to QA dataset that addresses short queries and answers made by the expert according to his work-experience by answering questions from academic researchers (see Table 3). This addition will allow to test our dialog-based expert system and the quantitative effect of adding typical questions and answer will be confirmed in the next phase of our research by using retrieval-based large language models.

Table 3



ジルコニウムは輸出管理で規制されますか。	爆発物の反応材料で、ジルコニウム粉末や粉末からなる成型品が規制されます。 また、化学兵器の製造に用いられる装置で、反応器等でジルコニウムに裏打ちされたものも規制されます。その他、多くの用途で規制されます。
Is zirconium regulated by security export controls?	Reactive materials for explosives, such as zirconium powder or molded products made of the powder, are regulated. Also regulated are devices used in the manufacture of chemical weapons, such as reactors, lined with zirconium. Many other applications are also regulated.
ガス遠心分離機関連ではどういったものが規制されますか。	ガス遠心分離機のロータに用いられる構造材料や、ガス遠心分離機のロータに用いることができる構造材料等が規制されます。
What is regulated in relation to gas centrifuges?	Structural materials used in gas centrifuge rotors and structural materials that can be used in gas centrifuge rotors are regulated.
純チタンは輸出令別表第一に該当しますか。	純チタンであれば、少なくとも、輸出令別表第一の 1 項から 15 項までには該当しません。
Does pure titanium fall under Appended Table 1 of the Export Trade Control Order?	Pure titanium, at least, does not fall under paragraphs 1 through 15 of Appended Table 1 of the Export Trade Control Order.

The datasets and the access to the system (via Slack platform) we have developed is granted to anyone upon request.

参考文献

Akihiko Obayashi and **Rafal Rzepka**, "Annotated Question and Answer Dataset for Security Export Control", Proceedings of The 7th Linguistic and Cognitive Approaches to Dialog Agents (LaCATODA 2021) IJCAI 2021 Workshop, CEUR Workshop Proceedings vol. 2935, Montreal, Canada (2021 年 8 月)

Rafal Rzepka, Daiki Shirafuji, and **Akihiko Obayashi**: "Limits and Challenges of Embedding-based Question

Answering in Export Control Expert System", Proceedings of 25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, September 8-10, Szczecin, Poland. (2021 年 9 月)

Akihiko Obayashi and **Rafal Rzepka**: "Expanding Export Control-related Data for Expert System", Proceedings of 26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, September 5-9, Verona, Italy (2022 年 8 月)

Rafal Rzepka, Shinji Muraji and **Akihiko Obayashi**: "Utilizing Wikipedia for Retrieving Synonyms of Trade Security-related Technical Terms". In the proceedings of the Language Technology Conference (LTC'23), pp. 250-254, Poznan, Poland (2023 年 3 月)

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　4件）

１．発表者名
Rafal Rzepka, Daiki Shirafuji, Akihiko Obayashi

２．発表標題
Limits and Challenges of Embedding-based Question Answering in Export Control Expert System

３．学会等名
Proceedings of 25th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, September 8-10, Szczecin, Poland. 2021年9月（国際学会）

４．発表年
2021年

１．発表者名
Akihiko Obayashi, Rafal Rzepka

２．発表標題
Annotated Question and Answer Dataset for Security Export Control

３．学会等名
Proceedings of Linguistic and Cognitive Approaches to Dialog Agents (LaCATODA 2021) IJCAI 2021 Workshop, CEUR Workshop Proceedings vol. 2935, August, 2021, Montreal, Canada (held online).（国際学会）

４．発表年
2021年

１．発表者名
Rafal Rzepka, Shinji Muraji and Akihiko Obayashi

２．発表標題
Utilizing Wikipedia for Retrieving Synonyms of Trade Security-related Technical Terms

３．学会等名
Proceedings of the Language Technology Conference (LTC’23), pp. 250-254, Poznan, Poland（国際学会）

４．発表年
2023年

１．発表者名
Akihiko Obayashi and Rafal Rzepka

２．発表標題
Expanding Export Control-related Data for Expert System

３．学会等名
Proceedings of 26th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, September 5-9, Verona, Italy（国際学会）

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	ＲＺＥＰＫＡ　Ｒａｆａｌ (RZEPKA Rafal) (80396316)	北海道大学・情報科学研究院・助教 (10101)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関