別紙１－１

論文審査の結果の要旨および担当者

報告番号	※　甲　第　　号

氏　　名　　MENDSAIKHAN Otgonpurev

論　文　題　目

Effective Application of Natural Language Processing Techniques in Automated Cyber Threat Intelligence
（サイバー脅威情報自動処理における自然言語処理適用に関する研究）

論文審査担当者

主　査　　名古屋大学教授　村瀬　　勉

委　員　　名古屋大学教授　楫　　勇一

委　員　　名古屋大学准教授　嶋田　　創

別紙１－２

論文審査の結果の要旨

Mendsaikhan 氏提出の論文「Effective Application of Natural Language Processing Techniques in Automated Cyber Threat Intelligence」は、情報機器の増加に応じて増えつつある各機器のセキュリティ問題情報に対し、組織のセキュリティ担当者の負荷を減らすため、SNS や議論系 Web サイトから公式情報よりも速くセキュリティ問題情報を得る手法に関する一連の研究をまとめたものであり、全体は 5 章から構成される。

第 1 章は序論であり、近年では公式な脆弱性情報よりも先に SNS 等で話題になる事例があること、自然言語処理を応用してそれらの雑多な情報を収集して脅威情報に整形することができる可能性についての言及、2 章から 4 章の内容をまとめて実現する全体システム、関連研究について述べている。

第 2 章では、議論系 Web サイトから収集したセキュリティ問題情報らしきものを含むデータに対し、真にセキュリティ問題情報のみを抽出するフィルタリングの方法について提案を行っている。Reddit や StackExchange 等の議論系ウェブサイトから取得しラベル付けした約 120 万件のテキストデータに対して Doc2Vec および BERT によるサマライズを適用した結果と、信頼できる情報源から作成したモデルとの比較により、実用的な精度でフィルタリングができることが確認された。

第 3 章では、抽出されたセキュリティ問題情報に対して、機器、OS、アプリケーションのどの問題なのかを解析する処理について提案を行っている。提案では、抽出されたセキュリティ問題情報に対して固有表現抽出による必要情報の抽出と、その結果の既存のナレッジグラフの形式である Cybersecurity Knowledge Graph へのマッピング結果を解析結果としている。評価により、抽出とマッピングを実用的な精度でできることが確認された。

第 4 章では、解析されたセキュリティ問題情報を、広く使われている既存のセキュリティ対応フレームワークである MITRE ATT@CK に対応する形式にマッピングする提案である。マッピングにより、セキュリティ問題からくる脆弱性とそれを利用した攻撃の可能性について、既存の対策ルーチンに落とし込んでの提示を可能とする。解析されたセキュリティ問題情報に対してモデリングと多値分類を適用することにより、実用的な精度でマッピングできることが確認された。

第 5 章は結論であり、本論文の成果のまとめについて述べている。

以上のように、本論文は、自然言語処理の応用により、組織のセキュリティ担当者による早期のセキュリティ問題情報収集を手助けするシステム実現のための一連の提案を行っている。また、収集した実データを用いた評価により、実用的な精度でノイズ情報フィルタリング、セキュリティ情報の形式へのマッピング、セキュリティ対策フレームワークへのマッピングが行えることを確認している。よって、情報科学の学術上・技術上の寄与が大きいと考え、本論文提出者である Mendsaikhan 氏は博士(情報学)の学位を受けるに十分な資格があるものと判定した。