学位論文審査の結果の要旨

報告番号	先端科学技術甲第 174 号	氏　名	シュウ　カコウ
論文題目	ニューノーマル時代に備えたマルウェアの分類手法に関する研究		
論文審査委員会	委員（主査）　D○合　寺田　真敏　教授　（情報通信メディア工学専攻） 委員（副査）　D○合　岩井　将行　教授　（情報通信メディア工学専攻） 委員（副査）　D○合　齊藤　泰一　教授　（情報通信メディア工学専攻） 委員（副査）　D○合　八槇　博史　教授　（情報通信メディア工学専攻）		

研究の背景・目的

テレワークなどの新しい働き方が普及するにつれ，これまでのサイバーセキュリティ対策だけでは対応しにくく，見直す必要がでてきている．働き方，勤務環境と管理体制などの急速な変化に乗じた「ニューノーマルな働き方を狙った」サイバー攻撃が増加していることも一因にある．さらに，テレワークとオンライン会議などの利用環境の変化は，テレワーク用ソフトウェアなどに存在する脆弱性を悪用した攻撃の増加という，新たな脆弱性対応問題を顕在化させた．二重脅迫型のランサム攻撃は，暗号化したデータを復元するために金銭を要求する一つ目の脅迫と，金銭の支払いがない場合は窃取した内部情報をWebサイト上で公表する，公表されたくなければ金銭の支払いに応じろという二つ目の脅迫からなるサイバー攻撃である．増えつつある二重脅迫は，ランサムウェアによる攻撃が金銭目当てとするサイバー攻撃としてのビジネス化を定着させたと言える．ニューノーマル時代における情報セキュリティ対策の課題は，マルウェアが関与あるいは起点としたソフトウェアの脆弱性悪用，ランサムウェアによる攻撃であり，対策を講じる必要がある．

研究の内容

ニューノーマル時代に備え，顕在化したマルウェア脅威の特定と被害の低減のために，マルウェアの分類手法を提案している．まず，顕在化したサイバーセキュリティの一つ目の課題である，マルウェアが関与あるいは起点としたソフトウェアの脆弱性悪用状況を明らかにした．次に二つ目の課題であるランサムウェアによる攻撃に対抗するため，ランサムウェア特有の動作パターンに着目したマルウェアの分類手法について言及している．

最後に，ニューノーマル時代に備え，ランサムウェアなど顕在化したマルウェア脅威だけでなく，幅広くマルウェア対策を実現するために，マルウェア全般を対象とした分類手法について，マルウェアが関連する検体データセットを用いた評価実験から，提案手法の有効性を検証している．

本研究では，次の三つの研究を取りまとめている．

- テレワーク製品を狙ったマルウェアが攻撃対象としたソフトウェアの脆弱性を特定する研究
- ランサムウェアによる被害低減のためのファミリーを分類する研究
- ランサムウェアに限らず，マルウェア全般を対象としたファミリーを分類する研究

研究の成果

本論文では，ニューノーマル時代における情報セキュリティ対策に向け，3 つの成果を挙げている．

マルウェアが攻撃対象としたソフトウェアの脆弱性の特定では，マルウェアが攻撃に使用した脆弱性を特定し，さらに，マルウェアファミリーと攻撃に使用した脆弱性との関係性を明らかにし，攻撃アプローチを把握することが可能となった．

ランサムウェアの分類手法は，ランサムウェアがよく使用する API のグループ間の相関性を特徴量とした機械学習による分類手法である．この分類手法により，ランサムウェアの分類だけではなく，ランサムウェアファミリー毎に使用する API の特徴を明らかにしたことでランサムウェア攻撃による被害を抑止することが可能となった．

マルウェア全般を対象とした分類手法は，マルウェアの動作パターンと特徴ある動作とを特徴量とする機械学習による分類手法である．この結果，マルウェア全般を対象とした分類が可能となり，より包括的なマルウェア対策につなげることが可能となった．

この成果は，

［1］ 周家興，廣瀬幸，柿崎淑郎，猪俣敦夫，寺田真敏．“API グループ間の相関性とフォルダ操作頻度に基づくマルウェア分類手法の提案”．情報処理学会論文誌 Vol.61 No.12, pp.1792-1801 (2020)

としてまとめられている．

以上の研究成果は，ニューノーマル時代に備え，顕在化したマルウェア脅威による被害を低減するために，既存のマルウェア分類手法などのマルウェア対策を改善する有効な手段と位置づけることができる．

審査の結果

以上，本論文において著者が検討して得た結論に記された事柄は，ニューノーマル時代における情報セキュリティ対策，特に，マルウェア対策において強化しなければならない技術という点で極めて有用であると判断できることから，本論文の価値は工学的，工業的な観点からも十分に評価できる．よって，本論文は博士（工学）の学位論文として十分な価値を有するものと認められる．