東京電機大学大学院

学位論文内容の要旨

報告番号	先端科学技術甲第 174 号	氏　名	周 家興
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		

本論文は“ニューノーマル時代に備えたマルウェアの分類に関する研究”（Research on Malware Classification Methods for the New Normal Era）と題し，日本語で書かれており，6章よりなる．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の脆弱性問題を顕在化させ、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．

本論文では，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する．顕在化したサイバーセキュリティの課題である，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，ランサムウェアによる攻撃に着目したマルウェアの分類手法を検討した後、ニューノーマル時代に向けたマルウェアの分類手法について、次の三つの研究を取りまとめる．

- 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

「マルウェアが攻撃対象とした脆弱性を特定する研究」では，静的解析を用いてIoTマルウェアが攻撃対象とした脆弱性を特定する．脆弱性を特定する手法については，公開サイトから提供されているマルウェア検体データセットを使って，その有効性を示す．その後，マルウェアファミリーとそれらが攻撃対象とした脆弱性との関係を示す．この手法を用いることにより，マルウェアが攻撃対象とした脆弱性を特定し，さらに攻撃手法と攻撃目的を把握することが可能となる．

「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」では，ランサム

ウェアに呼び出されたAPIから各ファミリーの動作パターンを機械学習しファミリーを特定する手法についてである．複数サイトから提供されているランサムウェアのデータセットを使って特定する手法の有効性を示す．その後，ランサムウェアが攻撃に使用するAPIグループを明らかにすると共に，ランサムウェアファミリー毎に使用するAPIグループの傾向を示す．この手法を用いることにより，ランサムウェアの攻撃手法を特定し、ランサムウェアによる被害を抑止することが可能となる．

最後に，「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」では、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，より汎用性の高いマルウェアファミリーを分類する手法の有効性を示す．ここでは，機械学習を用いて，マルウェアが攻撃で使用した API と操作したフォルダパスから，マルウェアファミリーの動作特性と動作パターンを学習することで分類する．さらに，特徴量寄与度の分析手法を用いて各マルウェアファミリーがよく使用する API と動作目的を示す．この手法を用いることにより，マルウェアのファミリー、攻撃目標と感染経路などを特定し、より包括的なマルウェア対策が可能となる．

論文の構成は以下となる．第 1 章は，“序論”である．ここでは，ニューノーマル時代におけるサイバーセキュリティにある課題を記述してから，本研究の目的を述べ，本論文の構成および得られた成果を述べる．第 2 章は，“ニューノーマル時代のマルウェア脅威”であり，ニューノーマル時代に向け顕在化したマルウェア脅威の状況をまとめてから，本研究で提案するマルウェア対策を概説する．第 3 章は，“マルウェアが攻撃対象とした脆弱性の特定手法”である．この章では，テレワーク製品を狙ったマルウェアに悪用された脆弱性の特定という課題を解決するために，静的解析を用いて，自動的にマルウェアに悪用された脆弱性のエクスプロイトコードを抽出し，脆弱性を特定する手法を提案している．第 4 章は，“ランサムウェアの分類”である．この章では，ランサムウェア攻撃による被害の特定と低減のための分類という課題を解決するために，ランサムウェアに呼び出された API グループ間の相関性を特徴量にして，機械学習でランサムウェアの動作パターンを把握し，ランサムウェアのファミリー、目的と攻撃手段などを特定する手法を提案している．第 5 章は，“マルウェアの分類”である．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の分類手法が必要であるという課題を解決するために，機械学習を用いて，マルウェアに使用された API グループ間の相関性とマルウェアに操作されたフォルダから動作パターンと動作特徴を習得してから，分類手法を提案している．第 6 章は“結論”であり，本論文の内容の総括と今後の課題である．