氏　　名	葛野　弘樹
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第　　６１８９　　号
学位授与の日付	２０２０年　３月２５日
学位授与の要件	自然科学研究科　　産業創成工学専攻 （学位規則第４条第１項該当）
学位論文の題目	A Study on Kernel Memory Protection and Application Traffic Monitoring for Information Leakage Prevention （カーネルメモリ保護とアプリケーション通信の監視による情報漏洩防止に関する研究）
論文審査委員	准教授　山内　利宏　　教授　谷口　秀夫　　教授　門田　暁人

学位論文内容の要旨

Managing the information assets of public and private organizations is a rapidly growing and important field. Cyberattack is a principal cause of information leakage. Such attacks may be either internal or external. The adversary uses a vulnerability of the software, a missing implementation of the hardware, or a weak user password to intrude on the internal network and its constituent devices. One useful strategy is to employ multiple layers of defense for protection against cyberattack, reduction of damage, and identification of perpetrators. Mutual complementation of multiple layers suppresses risk to an information system. In this dissertation, the focus is on defending the operating system (OS) and the applications. These layers manage and handle information assets on information systems, then detect and prevent information leakage. Moreover, in order to identify information leakage using three detection and prevention methods, these are 1) OS monitoring, to identify kernel memory corruption and illegally overwritten kernel code, and malevolent data in the kernel virtual memory. 2) Application traffic monitoring, to identify information leakage and other traffic from applications requesting excessive permissions. 3) Suspicious application library identification, to use network traffic modeling to identify applications requesting excessive permissions. These elements of a multi-layer defense against information leakage, concentrating on the OS and application layers. To guard the OS against cyberattacks, the kernel memory observer (KMO) virtual memory system is proposed. To guard mobile device users against various forms of information leakage, two new detection methods are developed. The efficacy of these approaches is supported by the observed results. This work should prove valuable to future researchers in the field of information security.

論文審査結果の要旨

企業や個人の情報システムで扱う情報資産の量は，ますます増大している。このため，不正なアクセスにより，情報漏洩が起きた場合は，企業や個人の活動に重大な問題をもたらす。最近は，電子媒体による情報漏洩の割合が増えており，対策が求められている。しかし，情報システムは，大規模になり，かつ複雑化しているため，多層防御が情報漏洩を防止するために重要となっている。多層防御は，外部から内部への攻撃対策（入口対策），内部の振る舞いを制御・監視（内部対策），および内部から外部への情報監視（出口対策）からなる。

論文提出者は，多層防御の内部対策と出口対策に着目し，オペレーティングシステム（OS）とアプリケーションにおける情報漏洩の未然防止や検出を実現する手法を提案している。内部対策として，OSに監視用の仮想記憶空間を導入し，監視用空間からカーネル用の仮想記憶空間のメモリ破壊を検出する手法を提案している。これにより，実際のカーネル脆弱性を用いたメモリ破壊を検出できること，および監視用空間の影響による性能低下を抑制する実現方式を示し，性能評価により，その効果を示している。次に，出口対策として，Androidアプリケーションのトラフィックを収集し，クラスタリングによりシグネチャを生成し，情報漏洩の可能性を検出する手法を提案している。評価では，検出精度が高いことを示している。さらに，アプリケーションの内部対策として，グラフ距離アルゴリズムにより，不審なアプリケーションライブラリの検出手法を提案し，その手法の検出精度が高いことを示している。

以上のように，本論文は，OSとアプリケーションによる多層防御により，情報システムのセキュリティを確保する手法を確立しており，情報工学に寄与するところが大きい。よって，本論文は博士（工学）の学位論文に値すると認める。

なお，論文発表会では，適切な説明が行われ，質疑に対する応答も適切であった。これにより，十分な学力を有すること，及び自立した研究者として活動を行う能力を有することが確認できた。