公益財団法人　セコム科学技術振興財団
研究成果報告書

研究課題名

コンピュータの原理原則に着眼したセキュリティカーネル技術とその応用に関する研究

Research on Security Kernel Technology which is based on the Principles of Computer, and its Application

研究期間

平成 26 年　4 月　～　平成 30 年　3 月

報告年月

平成 30 年　6 月

研究代表者
東京電機大学 サイバー・セキュリティ研究所 副所長
上野 洋一郎

Associate Director, Tokyo Denki University　Cyber Security Laboratories
Yoichiro UENO

概　要

東京電機大学サイバー・セキュリティ研究所は、F.TRON 社と共に、悪意ソフトの後追い対策技術ではなく、コンピュータの原理原則に着眼した、独自のセキュリティカーネル技術を共同研究している。

コンピュータの原理原則として、CPU による動作機構と、権限（Ring 0～3、Ring 0 が最上位）付与による保護機構からなっており、CPU による処理は、与えられた権限レベルにしたがって行われる。現在すべてのアプリケーション動作は Ring 3 レベルで行われており、オペレーティングシステムやドライバーの処理は Ring 0 レベルで行われている。悪意ソフトもアプリケーションであるので、Ring 3 レベルであり、オペレーティングシステムの Ring 0 レベルの処理により駆逐可能であると考えられる。しかしながら、オペレーティングシステムはアプリケーションと様々な通信を行わねばならないと共に、セキュリティホールが残存している。悪意ソフトはセキュリティホールを利用して、オペレーティングシステムと同等の Ring 0 レベルに権限昇格することで、オペレーティングシステムやセキュリティソフトの監視を逃れて、様々な問題を発生させている。したがって、セキュリティソフトは、オペレーティングシステムやアプリケーションから隔離された状態で、オペレーティングシステムやアプリケーション全てを監視することで、悪意ソフトの侵入または動作を阻止すれば、そのコンピュータは悪意ソフトに侵されることはない。

セキュリティカーネル技術は、上記に述べたコンピュータの原理原則に着眼し、上位権限を優先的に確保するために、Ring 0 レベルを確保しながら、オペレーティングシステムよりも先にメモリ内に起動される。その後、セキュリティカーネル技術がオペレーティングシステムを Ring 2 で起動する。このため、セキュリティカーネル技術が存在するコンピュータ内では、セキュリティカーネル技術が Ring 0 レベルを優先的に持つ。このことから、悪意ソフトを含むすべてのソフトの動作を監視・制御できるため、悪意ソフトも作動できず、セキュリティを担保した状態で、コンピュータの処理が可能となる。また、セキュリティカーネル技術はオペレーティングシステムよりも先にメモリ内に起動され、そのメモリ内の存在位置はオペレーティングシステムのアクセス領域外に設定されるため、オペレーティングシステムを介するソフトからはアクセスできず、悪意ソフトからの攻撃はまったく受け付けないために、セキュリティが非常に強化される。

そして、セキュリティカーネル技術を導入したコンピュータのみで構築する安心・安全なオーバーレイネットワークの実現と、オーバーレイネットワーク内のコンピュータからのサービス要求のみ受け付けるセキュア空間を構築することで、安心・安全なネットワークサービスとその基盤を構築することが可能となる。