

先端科学技術研究科 修士論文要旨

所属研究室 (主指導教員)	サイバーレジリエンス構成学 (門林 雄基 (教授))		
学籍番号	2011257	提出日	令和 4年 1月 21日
学生氏名	増田 祐斗		
論文題目	Intel SGXを用いたクラウドにおけるプロセスの実行時完全性検証に関する研究		
要旨			
<p>クラウドコンピューティングの利用には、ユーザとクラウドプロバイダ間の信頼に関する問題が伴う。クラウドプロバイダが管理する物理的なコンピュータリソースを利用する特性上、ユーザはクラウドに配置したデータやプロセスがクラウドプロバイダによって改ざんされないと信頼する必要がある。Trusted Execution Environment (TEE) は、ハードウェアレベルでの保護を提供し、クラウドプロバイダから保護された環境にデータやプロセスを配置することを可能にする。ユーザはTEEを実現するハードウェアベンダを信頼することで、クラウドプロバイダの信頼性に関係なくクラウドを利用することができる。しかし、TEEにはプロセスのロード時に完全性を証明する機能があるが、プロセスの実行時にその完全性を証明する機能がなく、脆弱性の悪用などによってTEE内のプロセスが改ざんされる可能性がある。プロセスの実行時完全性検証に関する既存技術もあるが、これらの検証手法はクラウドプロバイダに対して保護されない。そこで本研究では、プロセスの実行時完全性検証とTEEの保護機構を組み合わせ、クラウドプロバイダなどの高度権限者から保護されたプロセスの実行時完全性検証を提案する。提案手法の概念実証を実装し、クラウドプロバイダなどの脅威からプロセスの動作が改ざんされたときに、正しく完全性検証ができるかを確認した。また、提案手法が実運用に供するものであるかどうかを確認するためにオーバーヘッドについても確認した。</p>			