

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	2111291	提出日	令和 5年 1月 18日
学生氏名	吉村 仁志		
論文題目	高信頼実行環境における安全領域の利用効率を向上したRDBMSの機密データ保護機構の研究		
要旨			
<p>クラウドの普及によって、負荷の高いデータベースサービスもクラウド上で提供されるようになった。しかし、クラウド事業者はクラウドサーバ自体やサーバ上の仮想マシンを管理するハイパーバイザといった、ユーザーが利用可能なアプリケーションよりも下位層にあるコンポーネントを管理するため、VMの管理者がOSやデータベースを堅牢化してもクラウド事業者による機密データの閲覧や漏洩といった脅威が依然として残る。昨今では、Trusted Execution Environment (TEE) と呼ばれる隔離環境 (Secure領域) でプロセスやメモリを保護したままプログラムが実行できるハードウェア支援型のセキュリティ機構がCPUに搭載され、クラウド事業者からのデータやプロセス保護が可能となった。しかし、TEEは通常のOSやプログラムを稼働させるunsecured領域とは独立して確保される資源であり、コンピュータ全体で利用可能な通常のメモリ領域と比較すると、かなり小さい資源である。そのため、高負荷なデータベースで大量のデータや巨大なプロセスを保護する場合には、secure領域のみ過負荷でunsecured領域の資源が大量に残る状況が頻繁に発生して資源利用効率が著しく低下する。そこで本研究では、データベースを構成するコンポーネントのうち、秘匿すべき要素のみをsecure領域にオフロードすることで、secure/unsecured領域の両方の資源を有効活用しながら機密データを保護するRDBMSのデータ保護機構を提案する。本研究の提案システムと、全データをsecure領域に格納して実行するデータベースと比較した結果、提案システムはより高い資源利用効率を実現し、secure領域の過剰利用によるパフォーマンスオーバーヘッドが発生しにくいことを確認できた。</p>			