東北大学 TOHOKU UNIVERSITY

Orchestrating a brighter world NEC

JST

Press Release

2024 年 10 月 11 日

報道機関　各位

国立大学法人東北大学
日本電気株式会社
国立研究開発法人科学技術振興機構（JST）

テラバイトスケールのコンピュータメモリを安全で高効率に暗号化できる新技術を開発

― 遅延 63%抑制、性能低下 44%抑制、攻撃から復旧まで数千倍高速化 安全で快適なクラウド活用に寄与 ―

【発表のポイント】

- コンピュータ上のデータを安全にメモリに格納し、効率的に利活用するための新たなメモリ暗号化機構を開発しました。
- 開発したメモリ暗号化機構の安全性を数学的に証明しました。
- 近年活用されるテラバイトスケールの大容量メモリに対しても、利便性を損なうことなく、高速に暗号化を実現できることを明らかにしました。
- 今後、開発されるコンピュータやメモリシステムの安全性の向上に大きく貢献すると期待されます。

【概要】

普段の生活や社会・経済活動に必要不可欠なパーソナルコンピュータ（PC）やスマートフォンでは、個人情報や機密情報等の情報を処理・格納するメモリデータの機密性、および改ざん検知を実現するメモリセキュリティ（メモリ暗号化）が必要とされています。しかし、近年の大容量化するメモリにおいてデータの安全性、性能、そして利便性を損なわずに暗号化を実現することは特に難しく、安全なコンピュータの実現における大きな障壁となっていました。

東北大学電気通信研究所の本間尚文教授らのグループは、日本電気株式会社（以下、NEC）と共同で、安全性を担保したまま、性能と利便性（レジリエンス性）を飛躍的に向上させたメモリ暗号化機構の新方式を開発しました。本機構は、メモリ暗号化に伴うコンピュータの負荷を大きく削減するとともに、テラバイト級の大容量メモリにも効率的に適用が可能です。またこれまでの方式と比べ、開発した方式は暗号化による遅延を最大約 63%、メモリの性能低下を約 44%抑制でき、偶発的なメモリエラーやメモリ改ざん等のメモリデータへの攻撃検知から復旧までの時間を数千倍高速にできることを明らかにしました。今後、開発した方式により、多様なコンピュータにおいてデータ保護と安全なデータ利活用に貢献することが期待されます。

本成果は 2024 年 10 月 14 日から 18 日に米国計算機学会（ACM）が開催

研究

するコンピュータセキュリティに関する国際会議 ACM SIGSAC Conference on Computer Communications Security（CCS）において発表されます。

【詳細な説明】

研究の背景

現在、個人情報や金融情報といった大切な情報がコンピュータ上で処理され保管されることが一般的となっています。現代のコンピュータのほとんどは、演算処理を行う中央演算装置（CPU）と、データを格納する主記憶装置（メインメモリまたはメモリ）が中心的な役割を担っており（図１）、コンピュータが実行中のプログラムコードや情報処理に必要なデータは通常一時的にメモリに格納されます。一方、メモリに格納されたデータ（メモリデータ）を、データの所有者以外が不正に盗み見る、不正に改ざんするなど攻撃の脅威が報告されています（図 2）。例えば、メモリは CPU の外部に取り外し可能な形で接続されることが多いため、このメモリを取り外して解析する（別のコンピュータに接続し、秘密の情報を盗み見る）攻撃が知られています（注１）。近年では、クラウドサービスなどで遠隔のコンピュータ（計算機サーバ）を利用する機会が増えていますが、このようなクラウドサービスは多数の利用者が同じ CPU やメモリを共有します。利用者に悪意ある攻撃者がいた場合、クラウドサービスにおける共有メモリを介した攻撃（共有されたメモリを介して秘密情報の盗聴や改ざん）が可能なことも報告されています（注２）。このような脅威に対抗するため、メモリデータの機密性と改ざん検知をいかに実現するかについて、暗号と情報セキュリティ分野およびコンピュータ設計分野において世界的に研究開発が進められています。

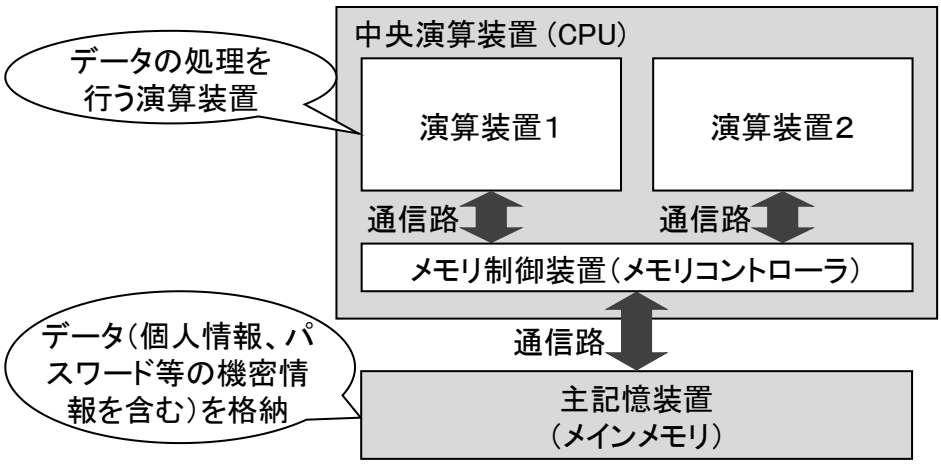
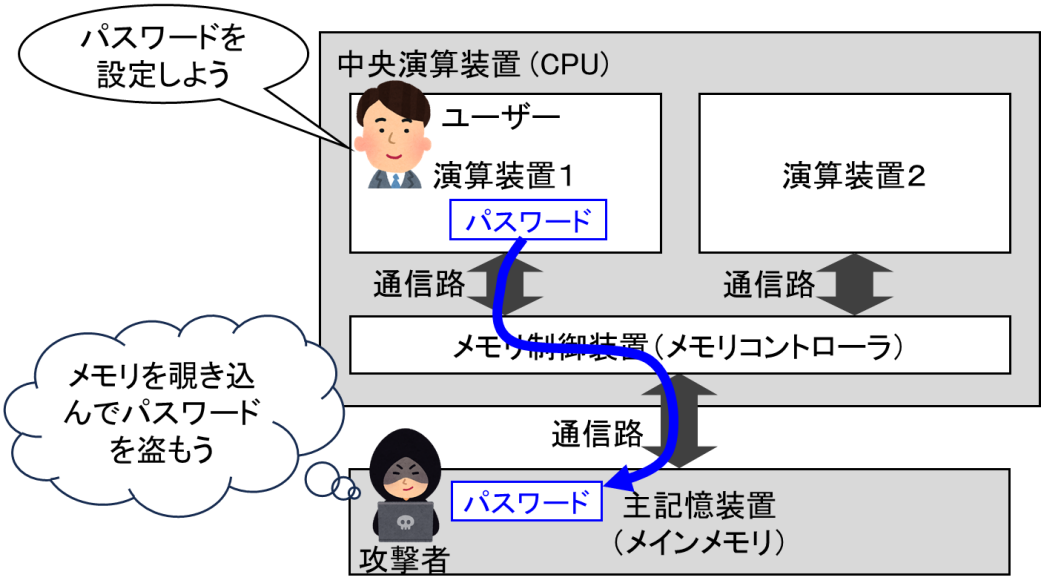
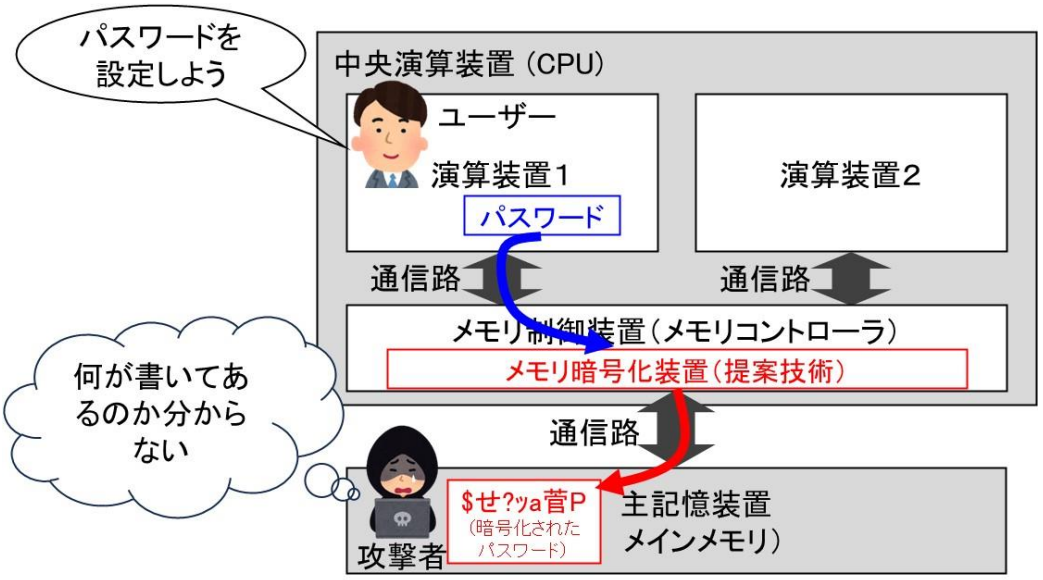


図 1. 現代コンピュータの概観。データを処理する中央演算装置（CPU）とデータを格納する主記憶装置（メインメモリ）が主要構成要素。

東北大学電気通信研究所環境調和型セキュア情報システム研究室の本間尚文教授と上野嶺客員准教授（現京都大学大学院情報学研究科准教授）および NEC セキュアシステムプラットフォーム研究所の峯松一彦主席研究員と井上明子主任らの研究グループは、今後の情報通信社会で期待される新たなサービスを安心・安全に利用できるコンピュータの実現を目指し、これまでメモリデータを盗聴や改ざんから守るための専用暗号技術の開発や、暗号技術を現実世界で数学的にも物理的にも安全に実現するための技術開発を行ってきました。



(a) メモリ暗号化がないコンピュータ



(b) メモリ暗号化に基づく安全なコンピュータ

図 2. (a) メモリ暗号化がないコンピュータでは、攻撃者がメモリを不正に読み出すことで秘密情報が漏洩してしまう恐れ。(b) メモリ暗号化によって不正にデータを読み出せる攻撃者に対して秘密情報を守ることができる。

今回の取り組み

今回開発した技術は、メモリデータを暗号化することでその盗聴と改ざんを防ぐ「メモリ暗号化」と呼ばれる機構の新方式です。メモリ暗号化機構では、CPU 上で処理したデータをメモリに保存する際に国際標準暗号 AES（注3）等により暗号化し、メモリに格納されたデータそのものを盗聴されても、もとのデータが何だったか分からなくすることで、データの機密性を確保します。同時に、メモリからデータを読み出すときには、暗号化されたデータを正しく復元できるかを確認することで、データの改ざんを検知します（注4）。

これまでのメモリ暗号化機構は、そうした安全性を達成するためにコンピュータの性能および利便性を大きく損なっていました。すなわち、データのメモリへの書き込みや読み出しに大きな遅延がかかり、追加的なデータを要するためメモリに保存できるデータの最大容量が減ってしまうことで、コンピュータの処理性能を低下させていました。また、メモリ暗号化を施した場合、偶発的なメモリエラー（注5）や電源遮断等の復旧が困難になるという利便性・レジリエンス性の問題もありました。この性能・利便性の低下は、近年利用の進む大容量メモリの保護において特に顕著になります。

今回開発した新方式は、メモリ暗号化機構を備えるコンピュータの性能や利便性を飛躍的に高めるとともに、大容量メモリを効率的に保護することが可能です。この新方式では、メモリ暗号化の高速性とトラブルからの復旧性能を高めるための専用の暗号方式を新たに開発するとともに、それに基づく暗号化メモリのデータ構造およびハードウェア構成を考案しました。数値評価およびシミュレーションの結果から、新方式はメモリ暗号化におけるデータ読み出し・書き込みの遅延を最大 63%削減するとともに、メモリ容量の低下を約 44%削減することが分かりました。また、メモリエラーや改ざん攻撃に対する頑健性を向上するとともに、それが生じた場合からの復旧処理を従来と比べて数千倍高速に完了することを確認しました。さらに、研究グループでは、新方式の安全性を数学的に証明しました。上記の特長から、開発した新方式はテラバイト級の大容量メモリであっても安全かつ効率的にデータの保護を実現します。

今後の展開

今回開発したメモリ暗号化機構は、現代の多くのコンピュータ方式に適合する汎用的な手法です。今後の情報通信社会では、コンピュータの利用形態がますます多様化し、保護すべき価値のあるデータを取り扱う機会の増加が見込ま

れます。それに伴いコンピュータ上に保存されるデータを攻撃から守るメモリ暗号化機構の重要性はますます高まると予想されます。今後は、開発方式を種々のコンピュータに適用して実証実験をさらに進めます。特に、これまで知られている攻撃を開発方式が搭載されたコンピュータに適用して実機評価することで、その有効性・安全性をさらに明らかにしていきます。これにより、今後開発されるコンピュータのメモリセキュリティ技術の確立に貢献していきます。将来的には、開発方式を活用して、クラウドサービスを提供するデータセンタから、個人利用の PC やスマートフォン、そして組み込み応用まで、様々なコンピュータおよびそれらが繋がる情報通信システム全体の安全性と性能向上に貢献することを目指しています。

【謝辞】

今回の研究成果は、科学技術振興機構（JST）戦略的創造研究推進事業 CREST「Society5.0 を支える革新的コンピューティング技術」研究領域（研究総括：坂井修一）「耐量子計算機性秘匿計算に基づくセキュア情報処理基盤」（研究代表者：本間尚文、グラント番号：JPMJCR19K5）の事業・研究課題の助成により得られました。

【用語説明】

注1. メモリを取り外して解析する攻撃

現代のコンピュータのほとんどは DRAM と呼ばれる揮発メモリ（電源を切るとデータも消えるメモリ）を採用しているが、DRAM は電源を切ってもすぐにデータが消えず一定時間残留するため、DRAM に対してもこのような攻撃は現実的に可能とされる。また、DRAM を冷却すると、電源遮断後のデータの残留時間が伸びる。この現象を使った攻撃は 2009 年に発見され、コールドブート（Cold boot）攻撃と呼ばれる。

注2. クラウドサービスにおける共有メモリを介した攻撃

クラウドサービスでは、図 1 における演算コアを不特定多数の人が利用する一方で、メインメモリは共有される。通常の CPU では、ある利用者が他の利用者のデータを盗聴したり改ざんしたりすることはできないが、キャッシュ攻撃やロウハンマー（Rowhammer）攻撃と呼ばれる特殊な技法を用いることによって、データの盗聴や改ざんが可能なことが報告され

ている。

注3.　AES

Advanced Encryption Standard の略。2001 年に米国国立標準技術研究所（NIST）が連邦標準（FIPS PUB 197）として制定した暗号アルゴリズムで、2005 年に国際標準規格（ISO/IEC18033-3）として採用された。世界で最も広く利用されている暗号アルゴリズムの一つ。Wi-Fi やインターネット通信における代表的な暗号化方式としても知られる。

注4.　暗号技術によるデータ改ざんの検知

暗号化時に、タグと呼ばれる補助データを同時に計算し保管しておくことで、復号時にタグを用いて改ざん検知が可能となる。タグの計算には、メッセージ認証コードや認証暗号と呼ばれる暗号技術が使われる。

注5.　メモリエラー

現代メモリの主流である DRAM では、保存しているデータがときおり変化し得ることが知られている。これは、電磁気的な環境ノイズや、地上に降り注ぐ宇宙線が原因とされる。その他にも、攻撃者が能動的にエラーを誘発させ、データを利用不可にする脅威も存在する。

【論文情報】

タイトル：Crystalor: Recoverable Memory Encryption Mechanism with Optimized Metadata Structure

著者：Rei Ueno, Hiromichi Haneda, Naofumi Homma, Akiko Inoue, Kazuhiko Minematsu

*責任著者：東北大学電気通信研究所　客員准教授　上野嶺

掲載誌：The 31th ACM SIGSAC Conference on Computer and Communications Security (CCS), October 2024

【問い合わせ先】

（研究に関すること）

国立大学法人東北大学電気通信研究所

教授　本間尚文

客員准教授　上野嶺

TEL: 022-217-5506

Email: contact.ecsislab@grp.tohoku.ac.jp

（報道に関すること）

国立大学法人東北大学電気通信研究所　総務係

TEL: 022-217-5420

Email: riec-somu@grp.tohoku.ac.jp

NEC　コーポレートコミュニケーション部　根本

TEL: 090-7246-8179

Email: press@news.jp.nec.com

国立研究開発法人科学技術振興機構（JST）　広報課

TEL: 03-5214-8404

Email: jstkoho@jst.go.jp

（JST 事業に関すること）

国立研究開発法人科学技術振興機構　戦略研究推進部

ICT グループ

前田さち子

TEL: 03-3512-3526

Email: crest@jst.go.jp