第3世代AMD EPYCプロセッサーの2つのセキュリティ機能を有効化しても、Dell PowerEdge R6525のOLTPパフォーマンスへの影響は最小限

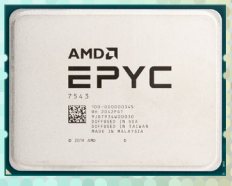
AMD Secure Encrypted Virtualization - Encrypted StateとAMD Secure Memory Encryptionを、AMD EPYC 7543プロセッサー搭載のDell PowerEdge R6525サーバーで有効化しても、オンライントランザクション処理のパフォーマンスはほぼ同等

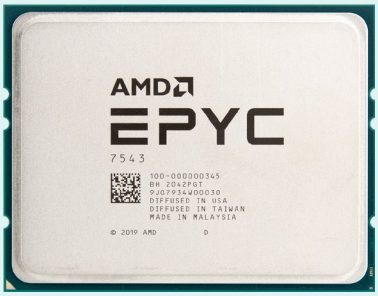
ビジネスの健全性を確実に保ち続け、機密データを保護したいのであれば、ハードウェアレベルでのセキュリティが重要ですが、しばしばコストが問題になります。かつては、CPUセキュリティの強化により、CPU性能が犠牲になることがありました。AMDの2つのセキュリティ機能は、そういった傾向に逆らう潜在能力を秘めています。システムメモリ、ホストメモリ、ゲストCPUレジスタを暗号化しても、OLTPパフォーマンスにはほとんど影響を与えません。

Principled Technologiesでは、AMD Secure Memory Encryption (SME)およびSecure Encrypted Virtualization-Encrypted State (SEV-ES)がパフォーマンスに与える影響を、AMD EPYC 7543プロセッサーを搭載したDell PowerEdge R6525サーバーで測定しました。このサーバーで、SUSE Enterprise LinuxとVMware vSphere 7.0 Update 1ハイパーバイザー上にMicrosoft SQL Server 2019を稼働する仮想化環境を実行し、最初はセキュリティ機能を使い、次にセキュリティ機能を使わずに、業界標準データベースベンチマークを実行しました。セキュリティ機能を有効化したサーバーは、無効化した同じサーバーと同等のOLTPパフォーマンスを示しました。

仮想マシンのセキュリティ強化と暗号化を、最小限のパフォーマンス影響で実現

AMD Secure Memory Encryption (SME)とAMD Secure Encrypted Virtualization-Encrypted State (SEV-ES)を有効化しても、オンライントランザクション処理(OLTP)のパフォーマンス影響はわずか1.7パーセント。





About AMD EPYC 7543 について

このAMD EPYC 7003シリーズの32コアプロセッサーはAMD Infinityアーキテクチャに基づきます。AMDによる最新の第3世代EPYCプロセッサーは、1コア当たり最大32MB L3キャッシュにまで強化したI/Oと、7nmのx86ハイブリッドダイコア、そしてSecure Encrypted Virtualization - Secure Nested Paging (SEV-SNP)、Secure Memory Encryption (SME)、Secure Encrypted Virtualization - Encrypted State (SEV-ES)[1]という新しいセキュリティ機能を装備しています。

セキュリティが重要な理由

WIREDマガジンの2013年の記事によれば、当時のPrivateCore社CTOのStephen Weisが、プロセッサーが急速にIT業界の「新しいセキュリティの競合地域」になりつつあると述べています[2]。ディスクの暗号化は今に至るまで常識となっていますが、機密情報が使用中の場合、つまり、ディスクからシステムメモリに移動したデータにCPUがアクセスしている最中については、そのデータを防御するセキュリティ上の選択肢は、ほとんどありません。Weis氏をはじめ多くの人々が、優秀な攻撃者はセキュリティ上のこのギャップを悪用し、組織のサーバーにある全データにアクセスして、オンラインのアカウントを侵害できるだろうと警告しています。これは、特に不揮発性メモリ技術にとっては不吉なセキュリティ上の欠陥です。攻撃者が、物理的にメモリをシステムから取り外し、暗号化されていない状態の中のデータを保存できてしまうからです。AMD SMEやSEV-ESのようなセキュリティ機能は、コンフィデンシャルコンピューティングを活用して、こういった攻撃を防ぐことを目指しています。

コンフィデンシャルコンピューティング

コンフィデンシャルコンピューティングは今日のITセキュリティの基本原則の1つで、システムメモリやプロセッサーが機密データを保持する際 (つまり「データの使用中」)に、データを不正な開示や細工から、保護します。IBMによると、コンフィデンシャルコンピューティングは使用中のデータを隔離し、「アクセスできるのは承認を得たプログラムコードのみで、それ以外からは見ることも知ることもできないようにできる」手法です[3]。

コンフィデンシャルコンピューティングでは、CPU が処理中のデータおよび処理予定のデータへのアクセスが承認される、信頼済みのハード、ファーム、ソフトのコンポーネントの数が制限されます。コンフィデンシャルコンピューティングへのAMDのアプローチは、独立したセキュリティ専用プロセッサーを使い、暗号化キーの処理やITセキュリティニーズを満たす様々な機能を提供するものです。システムRAMを暗号化するAMD Secure Memory Encryption (SME)と、仮想マシンのCPUレジスタを暗号化するAMD Secure Encrypted Virtualizationが、該当します。次のセクションでは、後者の2つの機能についての詳細と、それが組織の機密情報の保護にどのように役立つかを見て行きます。

AMD Secure Memory Encryption (SME)

SMEは、メモリ内の機密性の高いデータを防御し、使用中のデータを保護します。

SMEが有効化されているシステムを起動するたびに、AMDプロセッサーの内部にある暗号化エンジンは、ランダムに暗号化キーを作成します。この暗号化キーは、CPUコア上で実行中のソフトウェア自体からは見えません。次に、システムはメモリ内の全情報を暗号化し、CPUのメモリコントローラが暗号化キーを使って、安全に情報にアクセスします。

SMEは、メモリの部分的な暗号化も、完全な暗号化もできます。メモリの完全暗号化は、任意の鍵を用いてメモリ上の全ての情報を暗号化します。これによって、コールドブート攻撃やDRAMインターフェイススヌーピングのような攻撃からも防御できるとAMDは表明しています。また、攻撃者が不揮発性メモリモジュールの内部データを抽出する事態も防ぎます。メモリの部分的な暗号化では、オペレーティングシステムやハイパーバイザー がメモリのサブセットのみを暗号化する選択ができ、機密性の高いデータを保護しながら、それ以外のデータ処理のパフォーマンスを改善します[4]。

Secure Encrypted Virtualization – Encrypted State (SEV-ES)

SEV-ESは、仮想マシン（VM）の暗号化をサポートする技術であるAMD Secure Encrypted Virtualization (SEV)の、拡張機能です。元々のSEV機能は、システムの各VMに一意の暗号化キーを作成し、仮想メモリに保存した情報を保護しつつ、システム全体を円滑に作動させるものです。しかしVMが何らかの理由で実行を停止または中断した場合、使用中だったデータはハイパーバイザーのメモリに保存されます。VM が作動停止した際にもしシステムのハイパーバイザーが侵害されていれば、攻撃者はハイパーバイザー上の暗号化されていない機密データにアクセスして読み出すことができます。システムに不正な変更や改変を行うことすら可能です。 SEV自体は、この手の攻撃は防御できません。

しかし拡張機能のSEV-ESなら、VMが実行を停止しても、全CPUレジスタの内容が暗号化されているので、この種のデータ漏洩を防げます。つまり、SMEとSEVのメモリ暗号化以上のセキュリティの層が追加されるのです。AMDによれば、SEV-ESは「CPUレジスタの状態の悪意による改変も検出」できます[5]。

信頼の基点（Root of Trust）の確立

SMEとSEV-ESは両方とも、入力されるデータの信頼の基点を確立して作動します。暗号化されたシステムでは、信頼の基点が根源にあり、いくつもの検証チェックをパスしているからこそ、常に信頼できるのです。

もしあなたがスパイで、混雑した市場で連絡係に機密情報を手渡す必要がある場合を想像してください。以前その人に実際に会ったことがない場合、どうすれば情報を適切な人物に確実に渡せるでしょうか?解決策のひとつは信頼の基点のような検証を確立することです。例えば連絡係だけが答えを知っている無意味な質問をします。正しい答えが得られたら、その人物を信頼して機密情報を渡します。

AMD SMEとSEV-ESのセキュリティ機能もそれと同様の手法を使います。システム起動時に、AMDプロセッサー内部で隔離された暗号化エンジンがランダムに暗号化キーを作成し、それがシステムの使用する合言葉となって信頼の基点を確立し、承認されたシステムコンポーネントだけが機密データにアクセスできる仕組みを確保します[6,7]。

Dell PowerEdge R6525サーバーを支えるサイバーレジリエントアーキテクチャ

Dell PowerEdge R6525をiDRAC9と併用すれば、ハードウェアとファームウェアにわたるセキュリティレイヤーを提供し、「サーバーのライフサイクル全体を通して」セキュリティの統合を目指すツールとなります[8]。Dellは、ITセキュリティに対するこの多層化されたアプローチをサイバーレジリエントアーキテクチャと呼び、14Gと15Gの全Dell PowerEdgeサーバーで採用しています。Dellによると、このアーキテクチャには、次の機能が実装されています。

- 半導体ベースのルートオブトラスト
- 暗号化され信頼できる起動
- デジタル署名入りファームウェアパッケージ
- ハードドライブの暗号化とエンタープライズキー管理
- ドリフトの検知
- 動的なシステムロックダウン
- 一貫したイベントログ記録
- 監査ログ記録とアラート
- シャーシへの物理侵入の検知
- 自動化されたBIOSリカバリ
- Rapid OSリカバリ
- ファームウェアのロールバック
- Rapid System Eraseによるストレージメディアからの全データ除去機能

詳細はこちらをご覧ください https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf

当社のテスト結果

安全な、暗号化されたシステムには数々の利点があるにも関わらず、ワークロードのパフォーマンスに悪い影響が出ることを懸念して、オプションのセキュリティ機能の有効化をしぶるIT管理者もいます。実際のところはどうなのか、当社はオンライントランザクション処理(OLTP) データベース環境での、AMD SMEとSEV-ESの影響を判断するテストを実施しました。

ToAMDセキュリティ機能がOLTP のパフォーマンスに与える影響を数値化するため、AMD EPYC 7543プロセッサーを搭載したDell PowerEdge R6525サーバーでDVD Store 3ワークロードを実行し、有効化したセキュリティ機能付き/無しの状態で、サーバーが処理できる1分当たりの命令数の平均値を比較しました。(テスト手法の詳細や、VMware vSphere 7.0 U1環境でAMD SMEとSEV-ESを有効化する手法については、Science behind this report をご覧ください。)

その結果、AMDセキュリティ機能の有効化によるパフォーマンスの低下は、ベースラインからわずか1.7%に留まることが分かりました。これはほぼ無視できる差であると考えます。セキュリティを有効化したサーバーの1分間のオーダー処理数は平均で72,417件、セキュリティ機能を持たないサーバーでは73,636件でした。いずれの場合もこのテストの間、サーバーの平均CPU使用率は80%程度で、この種の業務での実際の使用事例の上限に収まっていると思います。

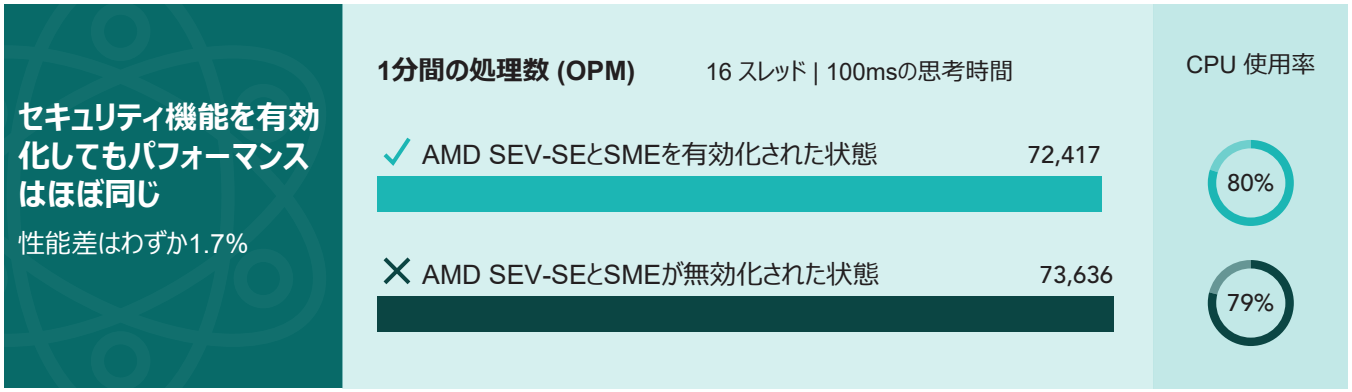


図1: 中央: 1分間当たりの平均オーダー処理数 (OPM)、DVD Store 3ベンチマーク負荷での環境での処理。16スレッドと100ms思考時間を設定。高い程優秀。右: DVD Store 3負荷での環境による平均CPU使用率。当社の仮想化環境はAMD EPYC 7543プロセッサー搭載のDell PowerEdge R6525サーバーで構成。このサーバーはMicrosoft SQL Server 2019をSUSE Enterprise Linux上で実行し、VMware vSphere 7.0 Update 1をハイパーバイザーとして使用。出典: Principled Technologies

現実的な利点

AMD SMEとSEV-ESのセキュリティ機能は、クラウドサービスプロバイダ、プライベートクラウドネットワークを活用する企業、そして複数の顧客の仮想化リソースを同じホスト上に持つ、マルチテナント環境を管理するすべての人に、利点があります。そういったお客様はすでに、顧客やユーザーが互いの仮想マシンにログインできないよう、ロールベースのアクセス制限や2段階認証のような手段を採用したシンプルな対策はしているかもしれません。しかし、そういった手段では、ゲストOSの脆弱性やハードウェアへの不正アクセスにより他のユーザーのデータにアクセスする攻撃者は防げません。SMEとSEV-ESを利用すれば、メモリとCPUレジスタデータが暗号化されるため、VMの中断中や故障中にも、全ての機密情報をハイパーバイザーから防御する手段を確保でき、安心できます。

結論

サーバーのセキュリティを適切に確保できていない場合、もし攻撃者に不正アクセスを行われれば壊滅的な損害を被り、顧客の信頼を失います。それでもやはり、短期的にビジネスのパフォーマンスを低下させるようなセキュリティ機能は誰も実装したいと思いません。

Principled Technologiesで私たちは、AMD EPYC 7543プロセッサー搭載のサーバーでAMD Secure Memory EncryptionおよびSecure Encrypted Virtualization-Encrypted Stateを有効化/無効化して、オンライントランザクション処理のパフォーマンスを比較しました。このセキュリティ機能を利用しても、サーバーの平均オーダー処理率はわずか1.7%下がるだけで、ほとんどパフォーマンスに影響しないことが判明しました。

貴社のビジネスにおいて、パフォーマンス上の高い代償を払わずにサーバーのセキュリティを強化する方法を探しているのであれば、AMD EPYC 7543プロセッサー搭載のDell PowerEdge R6525サーバーで、AMD SEV-ESとSecure Memory Encryptionを活用することをご検討ください。

---

1 "AMD EPYC 7003 processors," accessed March 16, 2021, https://www.amd.com/en/processors/epyc-7003-series

2 Stephen Weiss, "CPU: The New Security Perimeter," accessed March 7, 2021, https://www.wired.com/insights/2013/12/cpu-the-new-security-perimeter/

3 "What is Confidential Computing? | IBM," accessed March 7, 2021, https://www.ibm.com/cloud/learn/confidential-computing

4 David Kaplan, Jeremy Powell, and Tom Woller, " AMD Memory Encryption," accessed March 7, 2021, https://developer.amd.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf

5 David Kaplan, "Protecting VM Register State with SEV-ES," accessed March 7, 2021, https://www.amd.com/system/files/TechDocs/Protecting%20VM%20Register%20State%20with%20SEV-ES.pdf

6 "What is Root of Trust?" accessed March 7, 2021, https://cpl.thalesgroup.com/faq/hardware-security-modules/what-root-trust

7 Jason Landry, "What is Hardware Root of Trust?" accessed March 7, 2021, https://www.delltechnologies.com/en-us/blog/hardware-root-trust/

8 "Technical White Paper: Cyber Resilient Security in Dell EMC PowerEdge Servers," accessed March 16, 2021, https://www.delltechnologies.com/en-my/collaterals/unauth/white-papers/products/servers/cyber-resilient-security-with-poweredge-servers.pdf

Read the science behind this report at http://facts.pt/Gpmoizs ▶

Principled Technologies®

Facts matter.®

This project was commissioned by Dell EMC.