AMD PRO テクノロジ

AMD PRO セキュリティと AMD フレームワークによる、安全性、管理性、信頼性の高いビジネス PC

アジャイルで分散化された職場は、絶え間なく進化し続けています。ハイブリッドな事業形態が一般化してきた現在、企業は日常的なワークフローに AI を統合すると同時に、オフィス内での共同作業とリモート ワークのバランスを取ることが求められます。企業は、こうしたトレンドから生じる新しい課題に適応するシステムを導入して、PC フリートを刷新する必要に迫られています。そのため、オンプレミスとクラウドベースの両方の環境に適応しながら、パフォーマンス、セキュリティ、管理性をバランスよく実現するソリューションが求められています。

AMD Ryzen™ PRO プロセッサは、AMD PRO テクノロジにより、最新のビジネス PC を実現します。このテクノロジは、現在の企業の変化し続けるニーズに適応するよう設計および統合された一連のイノベーションを備えています。AMD Ryzen PRO プロセッサを搭載するすべてのシステムには、不可欠な基本コンポーネントが 3 つあります。本レポートでは、その 1 つである AMD PRO テクノロジのセキュリティの柱について説明します。今回はセキュリティに焦点を当てますが、AMD PRO テクノロジには、高度な管理機能とビジネス対応の信頼性も含まれており、これらを組み合わせることで、現代の企業に最適な包括的なソリューションを提供します。

AMD PRO テクノロジの全体像をご理解いただくためにこれら 3 つの柱をご紹介しますが、本レポートでは、進化する脅威から今日のビジネス PC を保護するよう設計された AMD Ryzen PRO プロセッサの次世代セキュリティ機能に特に焦点を当てて説明します。

PRO セキュリティ：現代の企業を守る

AMD PRO テクノロジの基盤となるのは、強固なセキュリティ機能です。完全なメモリ暗号化を実現する AMD メモリ ガード[1]、制御フロー攻撃からの保護を目的とした AMD Shadow Stack、および Microsoft Pluton セキュア暗号プロセッサへの包括的なサポートなど、高度なハードウェア機能により、巧妙な脅威に対する重要な保護を提供します。AMD Ryzen PRO プロセッサは、セキュア ブート[2] と信頼性の高い実行を統合的にサポートすることで、あらゆるレイヤーでデバイスを強化し、エンドポイントからクラウドまで、ユーザー データとアプリケーションを保護します。

本レポートでは最先端のセキュリティ機能に焦点を当てていますが、管理性やビジネス対応の信頼性などを含むより広範な AMD PRO テクノロジ フレームワークも連携して機能し、職場環境の新たなニーズに対応する包括的なソリューションを提供します。

PRO の管理性: IT 運用のシンプル化

多様な PC フリートを管理する作業は、特にハイブリッドな作業環境では複雑で時間のかかるものとなります。AMD PRO の管理性により、クラウドベースのリモート管理とリアルタイムのエンドポイント監視を可能にするオープンスタンダードベースのツールを使用して運用を効率化できます。これらのツールは、リモート システム管理に関して、最高レベルのオープン スタンダード コンプライアンスを提供します。[3] また、AMD PRO の管理性は、Microsoft Endpoint Manager や Windows Autopilot などの業界をリードするツールとの互換性を実現し、一貫性のある効率的な展開プロセスを提供します。

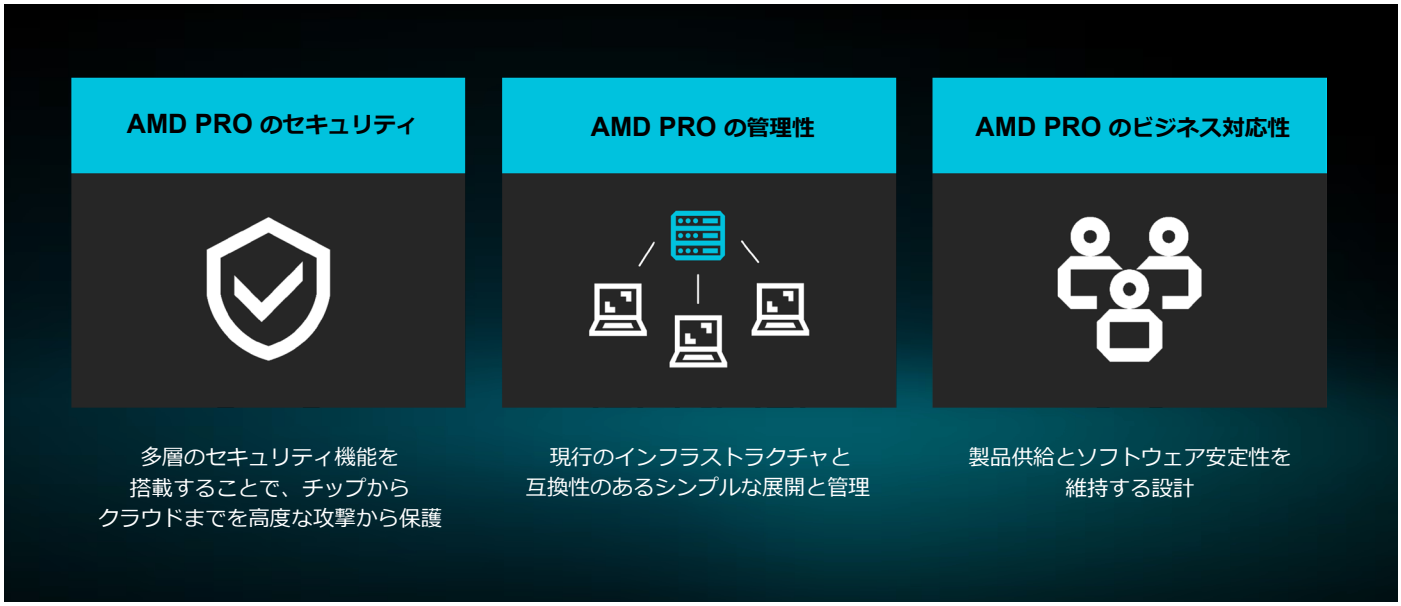
AMD PRO の管理性は、最新の DMTF DASH (Desktop and Mobile Architecture for System Hardware) 仕様をサポートし、最新の暗号化および認証プロトコルである TLS 1.2 および 1.3 などを組み込んでいます。さらに、AMD PRO システムは、TPM 2.0 などのハードウェアベースのセキュリティ コンポーネントを統合し、より安全な暗号化キーの保存と保護を実現します。このようなスタンダードに基づくアプローチは、旧式の独自プロトコルと比較して、より強力な保護と優れたパフォーマンスを実現できます。[4] IT チームは、リモート プロビジョニング、自動パッチ展開、リアルタイム診断などの機能を活用でき、ダウンタイムの削減、エンドポイントの健全性の向上、運用のシンプル化に役立ちます。

最近の調査では、AMD PRO の管理性が IT 運用に与える影響が明らかになっており、従来のプロセスと比較して展開時間が最大 41%[5] 短縮され、直感的な統合管理インターフェイスにより実作業の負担が大幅に軽減されることが示されています。企業はこれらの機能を活用することで、従業員の勤務場所を問わずサポートすることが可能となり、複雑な PC エコシステムをよりシンプルかつ迅速に、信頼性の高い方法で管理できるようになります。

PRO のビジネス対応性: あらゆるタスクで信頼性の高いパフォーマンスを発揮

ビジネス対応性を備えた AMD PRO プロセッサは、PC の長寿命化、安定したパフォーマンス、企業向けワークロードの信頼性を実現します。徹底した検証プロセスにより、より高い稼働率が実現し、IT コストの削減に役立ちます。年間を通して全世界で入手可能であるため、企業はオンデマンドでシステムを展開でき、大規模な初期購入の必要性を最小限に抑えることができます。AI 対応アプリケーションや日常的なオフィス業務をサポートする AMD Ryzen™ PRO プロセッサは、企業の成長に欠かせない適応力を提供します。

図 1. AMD PRO テクノロジ。すべての AMD Ryzen™ PRO プロセッサ搭載ビジネス PC を強化。



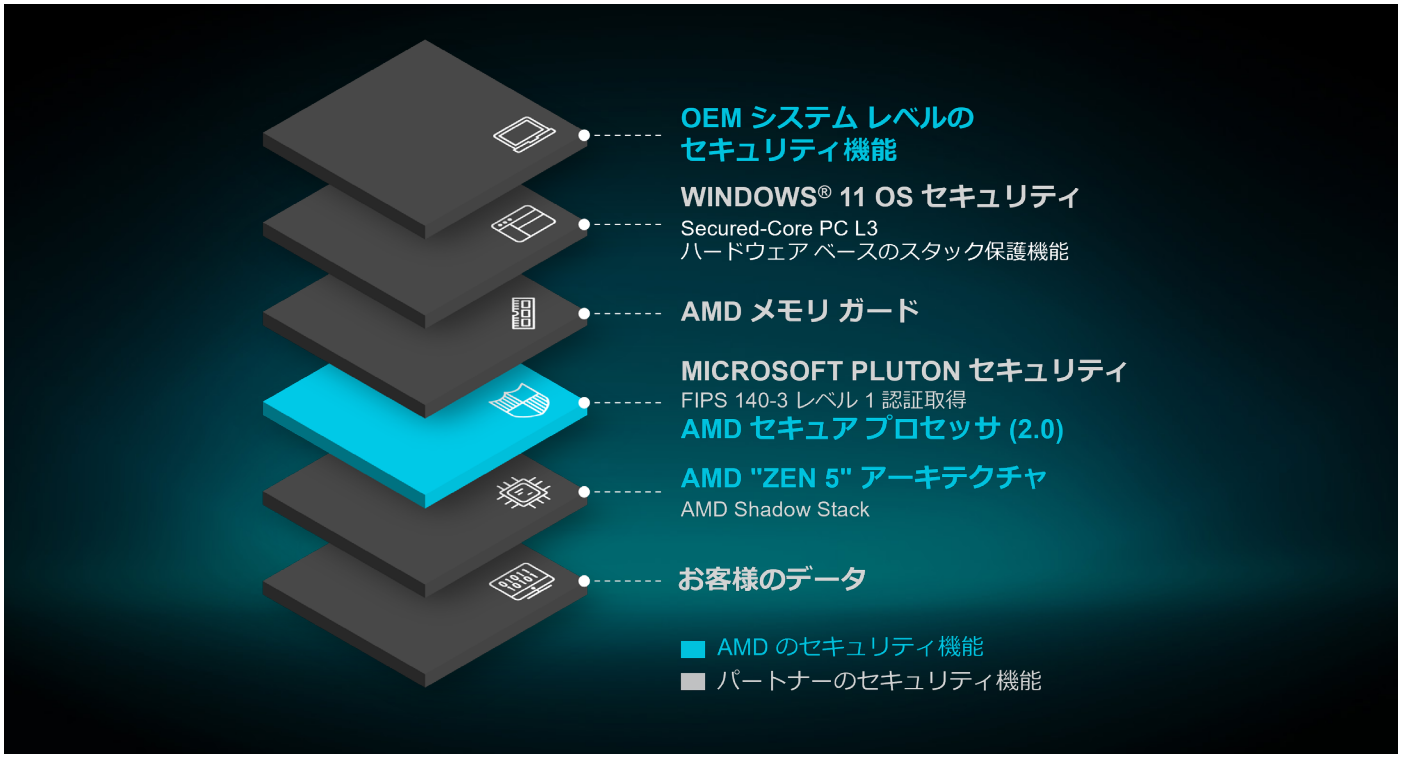
AMD PRO ビジネス対応性テクノロジは、一貫性を長期的に維持することによって信頼性を高めます。これにより、IT 計画がシンプルになり、投資収益率を最大化できます。すべての AMD Ryzen™ PRO プロセッサは、次のようなエンタープライズ級のソリューションを提供します。

- **イメージの安定性:** 18 か月にわたってソフトウェアの安定性を維持します。これにより、IT チームはスムーズな移行でき、安心感を得られます。
- **品質:** 強化されたプラットフォーム検証プロセスにより、要求の厳しいビジネス環境に適したエンタープライズ級の品質を実現します。
- **可用性:** 24 か月にわたって製品供給を維持します。これによってハードウェアの一貫性を保つことができ、安定した企業運営に貢献します。
- **信頼性:** 長期的な安定性と、複数のプロセッサ世代にわたって一貫したユーザー エクスペリエンスを実現するために、継続的にプラットフォームを検証しています。

AMD PRO のビジネス対応性により、ハードウェアとソフトウェアの両面で安定性が確保されます。これによって IT チームは、複雑性を軽減し、企業の長期的な成功のための信頼性の高い基盤を提供します。

企業が新しいワークプレイスのサポートという複雑な課題に臨むにあたり、AMD PRO テクノロジは重要な優位性を提供します。AMD は、最先端のセキュリティ機能、効率的な管理機能、ビジネス対応機能をすべての AMD Ryzen PRO CPU 搭載システムに統合し、業務の保護、IT 管理の合理化、イノベーションの推進に必要なツールを組織に提供します。

図 2. AMD PRO のセキュリティ。最先端デバイスの最新のセキュリティ要件を超越。



AMD 搭載 PC は、あらゆるレベルで最先端のマルチレイヤー セキュリティ設計を採用

AMD は、オペレーティング システム (OS) の開発者や OEM メーカーと緊密に連携して、それらのセキュリティ設計を補完および強化するハードウェア セキュリティ機能を提供しています。

AMD は、シリコンからオペレーティング システムに至るあらゆるレベルで最先端のセキュリティ対策を組み込みます。これによって企業は、最も重要な資産を保護し、ダウンタイムを最小限に抑え、IT の複雑性を軽減できます。

あらゆるレイヤーに組み込まれたセキュリティ

AMD PRO テクノロジは、すべての AMD Ryzen™ PRO プロセッサ搭載デバイスの基盤の柱として、セキュリティを統合しています。現代の企業が抱える課題の変化に対応するよう設計されたこれらのプロセッサは、強固なシリコン基盤から、ファームウェアや OS レベルの防御まで、マルチレイヤーの保護を展開します。

ハードウェアの信頼のルート: 最初から備わっている完全性

AMD のシリコン アーキテクチャは、ハードウェアの信頼のルートを統合しており、セキュア ブート プロセスをサポートします。この信頼のルートを支えるのが AMD セキュア プロセッサ 2.0[6] (ASP 2.0) であり、ファームウェアと OEM BIOS の完全性を検証し、不正な変更や潜在的なファームウェア攻撃から保護します。

メモリ保護の再定義: AMD メモリ ガード[7]

AMD メモリ ガードは、すべてのシステム メモリをリアルタイムで暗号化し、コールド ブートや物理的な攻撃から機密データを保護します。専用のハードウェア暗号化により、デバイスが盗難に遭った場合でも、強固な防御を維持できます。

次世代アーキテクチャ : AMD "ZEN 5" 以降

最新の AMD "Zen 5" コア アーキテクチャでは、強化されたセキュリティ機能が導入されています。独自のプロセッサ ID を活用して、ライフサイクル全体を通じて AMD の正規ハードウェアを安全に追跡できるサプライ チェーン セキュリティもその一つです。こうしたイノベーションにより、巧妙化するサイバー脅威に対するエンドポイントの耐性が強化されています。

業界標準に準拠

AMD PRO プロセッサは、FIPS 140-3 レベル 1 認証などの最新のセキュリティ要件を上回るように設計されています。Microsoft Pluton[8] との統合により、セキュアな認証と暗号化による保護機能が追加され、Windows ベースのシステムの保護がさらに強化されています。

AMD PRO セキュリティ アーキテクチャ

AMD セキュア プロセッサ 2.0:[9] さらに強固な基盤

AMD PRO セキュリティ アーキテクチャの中核となるのは、すべてのシステムオンチップ (SoC) に組み込まれた専用ハードウェア コンポーネントである AMD セキュア プロセッサ 2.0 (ASP 2.0) です。ASP 2.0 はハードウェアの信頼のルートとなり、セキュア ブート フローをサポートし、デバイスの電源投入の瞬間からファームウェアの整合性を検証します。その分離された信頼できる実行環境 (TEE) は、機密性の高い操作が、潜在的な攻撃から保護された状態を維持するのに役立ちます。主なコンポーネントには次のものがあります。

- **暗号化コプロセッサ (CCP):** ハードウェアで鍵生成と暗号化操作を管理する高性能な暗号化エンジンであり、時間的制約のあるセキュリティ タスクに不可欠です。
- **ブート ROM:** 起動初期化に必要な重要なファームウェアを格納したセキュアな読み取り専用メモリ。
- **スタティック ランダムアクセス メモリ (SRAM):** セキュアなプロセスを低電力でサポートします。
- **メモリ管理ユニット (MMU):** ブート ROM と SRAM へのアクセスを管理し、メモリ リソースを厳密に制御します。
- **クラウド ベアメタル復旧:** クラウド経由でデバイスの安全な復旧を促進し、壊滅的な障害が発生した場合でもビジネスの継続を可能にします。
- **サプライ チェーン セキュリティ :** AMD の正規ハードウェアをライフサイクルの各段階で認証し、部品の改ざんや偽造を防止します。
- **ウォッチドッグ タイマー :** ハードウェア レベルで処理の停滞を検知し緩和することで、システムの回復力を強化します。

これらの機能は、出張や在宅勤務、その他のモバイル環境における、機密性の高いビジネス データのリスクの深刻化に包括的に対処します。

Windows セキュリティとのシームレスな統合

AMD PRO セキュリティ アーキテクチャは、セキュア ブートやハードウェアによるスタック保護など、Windows 11 のセキュリティ機能とシームレスに連携し、包括的な多層防御システムを構築します。これにより、エンドポイントを強化して、ファームウェア、BIOS、ドライバー、OS を標的とする攻撃から保護します。

AMD ROM ARMOR

マザーボード上の SPI (Serial Peripheral Interconnect) フラッシュ メモリには、マザーボード UEFI や、セキュア ブートのステータスを含む付加的な構成情報が含まれています。

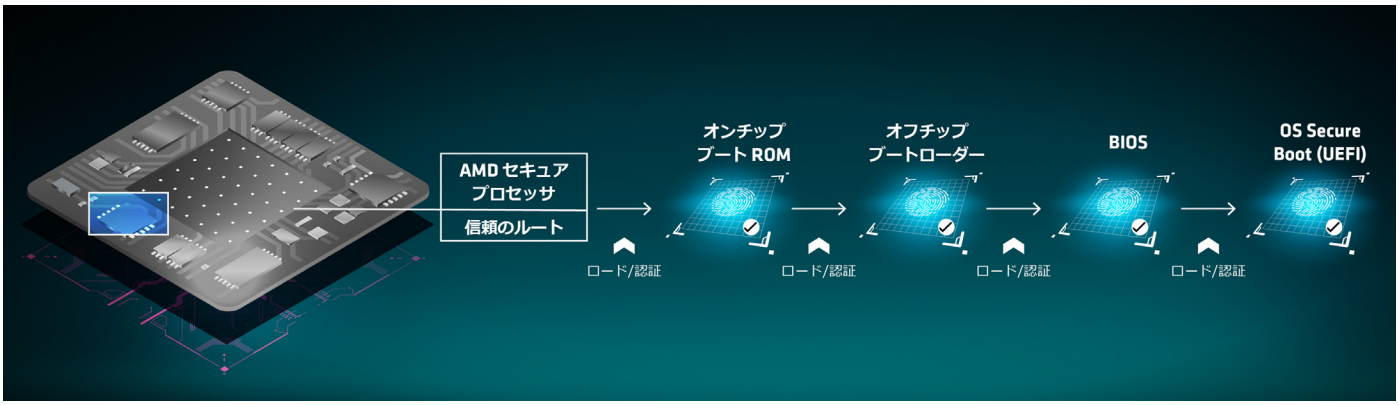
AMD ROM Armor は OS が初期化される前に動作し、SPI フラッシュへの不正な変更から保護します。OS がロードされる前に SPI フラッシュの整合性を確保することで、AMD ROM Armor はシステムの強固な基盤の確立を支援します。AMD ROM Armor が設定され、有効化されると、コンピューターの SPI フラッシュ デバイスは不正な書き込みに対して強化されます。

AMD PLATFORM SECURE BOOT (PSB)

AMD Platform Secure Boot (PSB) は、デバイスの起動プロセス中に BIOS を含む初期ファームウェアを認証するための、ハードウェアの信頼のルート (RoT) を提供します。システムの電源がオンになると、ASP は ASP 起動 ROM コードを実行し、シリコンとシステム メモリを初期化する前にさまざまな ASP ブートローダー コードを認証します。システム メモリが初期化されると、ASP ブートローダー コードは OEM BIOS コードを検証し、OS が起動する前にほかのファームウェア コンポーネントを認証します。

PSB は、権限のない、または悪性のファームウェアからよりパワフルに防御することでプラットフォームの整合性を強化し、検出時にそれらのアクセスを自動的に拒否します。AMD PSB は、低レベルのファームウェアから OS への移行を保護します。

図 3. AMD Platform Secure Boot。



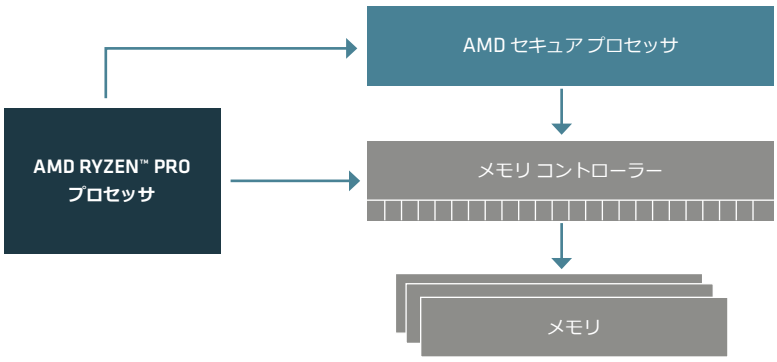
AMD メモリ ガード[3]

AMD メモリ ガードは、物理的な攻撃から顧客データを保護する目的で設計された包括的なメモリ暗号化技術です。AMD メモリ ガードがあれば、ランダム キーですべての DRAM コンテンツを暗号化し、物理的なコールド ブート攻撃、DRAM インターフェイスのスヌーピング、および同様のタイプの攻撃から保護できます。

NVDIMM を搭載したシステムの場合、AMD メモリ ガードはオンダイ メモリ コントローラーの専用ハードウェアに実装されているため、攻撃者がメモリ モジュールを取りはずしてその中身を抽出することを防ぐのにも役立ちます。

- 各コントローラーには、DRAM に書き込むときにデータを暗号化し、読み取るときに復号化するハイパフォーマンスな Advanced Encryption Standard (AES) エンジンが積まれています。
- NIST SP 800-90 準拠のオンダイ ハードウェア乱数ジェネレーターによって生成された 128 ビット キーを使用して実行されます。このモードでは、追加の物理アドレスベースの調整機能で暗号文のブロック移動攻撃から保護します。
- AMD メモリ ガードを搭載した AES エンジンで使用される暗号化キーは、システムをリセットするたびにランダムに生成され、CPU コアで実行されているソフトウェアからは見えません。このキーは AMD セキュア プロセッサ (ASP) によって完全に管理されます。

図 4. AMD メモリ ガード。



AMD SHADOW STACK

ROP (Return-Oriented Programming) は、広まりつつある攻撃ベクトルです。ROP 攻撃は、独自の悪性コードを注入するのではありません。正規のコードの脆弱性を悪用してシステムの制御を奪うことを試みます。

その仕組み

コンピューター プログラミングでは、「ルーチン」によって特定の一連の操作が実行されます。ソフトウェア プログラムが実行すると、それはルーチンと呼ばれます。そのルーチンがジョブを終了すると、リターン アドレスを使用してメイン プログラムに戻ります。このプロセスは「ジャンプ アンド リターン」と呼ばれます。

ROP 攻撃では、攻撃者はジャンプ ルーチンのリターン アドレスを変更します。つまり、メイン プログラムに戻らずに別のルーチンにジャンプして、サブルーチンをつなぎ合わせてシステムに害を及ぼす可能性のある悪性コードを作成します。最も重要なことは、このタイプの攻撃は正当なコードのように見えるため、検出されないことです。

AMD PRO セキュリティ アーキテクチャは、CPU 内の特別なレジスタへのソフトウェア アクセスを提供し、リターン アドレスのコピーを保存可能にすることで、ROP 攻撃を防ぎます。アプリケーションは、「Shadow Stack」と呼ばれる並列スタックを利用して、制御フローを変更しようとするソフトウェア攻撃を防ぐことができます。Shadow Stack は、リターン アドレスのコピーを格納するために専用ハードウェアを使用しており、リターン操作時に通常のプログラム スタックとの照合が実行されます。

内容が異なる場合、例外が生成され、悪性コードがシステムを制御するのを防ぎます。このように、Shadow Stack ハードウェアは最も一般的で悪用されがちないくつかのソフトウェア バグを軽減します。

AMD Shadow Stack は、ROP 攻撃に対する防御力を高めます。リターン アドレスのコピーがハードウェアに保存されているため、悪意あるコードに改ざんすることは非常に困難です。

Microsoft Hardware Enforced Stack Protection は、AMD Shadow Stack を使用する AMD PRO セキュリティ アーキテクチャでサポートされています。

MICROSOFT SECURED-CORE PC

Microsoft Secured-Core PC は、ファームウェアの脆弱性からデバイスを保護し、オペレーティング システムを攻撃から保護し、高度なアクセス制御と認証システムを通じてデバイスとデータへの不正アクセスを防ぎます。

Secured-Core PC は、次のようなさまざまなセキュリティ テクノロジとサービスを使用して、AMD PRO セキュリティ アーキテクチャ プラットフォームで有効になります。

- GMET 機能付き AMD-V™
- AMD Secure Init and Jump with Attestation (SKINIT)
- AMD Secure Loader (SL)
- AMD Dynamic Root of Trust Measurement (DRTM)
- AMD System Management Mode (SMM) Supervisor
- Direct Memory Access (DMA) Protection

GMET 機能付き AMD VIRTUALIZATION (AMD-V™) テクノロジ

AMD-V は、AMD プラットフォームでの仮想化を可能にするハードウェア拡張機能のセットです。Guest Mode Execute Trap (GMET) は、ハイパーバイザーがコードの整合性チェックを効率的に処理しマルウェアから保護するのに役立つ、シリコン内でのパフォーマンス強化です。

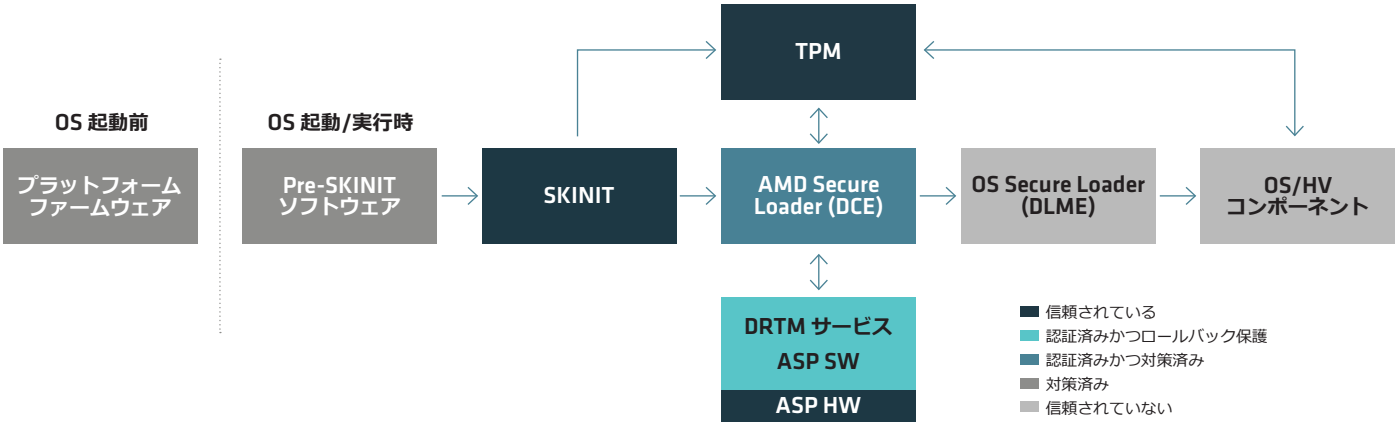
SECURE INIT AND JUMP WITH ATTESTATION (SKINIT)

SKINIT は、信頼性の低い動作モードから開始して、「信頼のルート」を確立する命令です。SKINIT は、プロセッサを再初期化してセキュア ローダー (SL) と呼ばれるソフトウェア コンポーネントの安全な実行環境を強化し、改ざんを防ぐために SL の実行を開始します。SKINIT は、ハードウェア ベースの信頼のルートをセキュア ローダーに拡張します。

AMD SECURE LOADER (SL)

AMD Secure Loader は、AMD セキュア プロセッサが提供する DRTM サービスに構成情報をハードウェアに問い合わせてプラットフォーム構成を検証します。

図 5. DRTM フロー。



システムが OS で起動した後はいつでも、オペレーティング システムは AMD サービス ブロックに値を再測定して証明するよう要求し、その後、さらなる操作を実行します。したがって、OS は起動時から実行時までシステムの整合性を保つことができます。

AMD DYNAMIC ROOT OF TRUST MEASUREMENT (AMD DRTM)

AMD DRTM ブロックは、SKINIT CPU 命令、ASP、および SL で構成されています。このブロックは、ファームウェア間の信頼の鎖を生成、維持する役割を果たします。AMD DRTM は、ファームウェアとブートローダーが保護されていないコードであると想定し、自由にロードできるという概念に基づいて動作します。これは、ハードウェアが低レベルのファームウェアを既知の測定されたコード パスに強制的に変換して、起動後すぐにシステムが信頼できる状態に移行することを念頭に置いています。

AMD DRTM ブロックは、SKINIT CPU 命令、ASP、および SL で構成されています。このブロックは、ファームウェア間の信頼の鎖を生成、維持する役割を果たします。

AMD DRTM は、ファームウェアとブートローダーが保護されていないコードであると想定し、自由にロードできるという概念に基づいて動作します。これは、ハードウェアが低レベルのファームウェアを既知の測定されたコードパスに強制的に変換して、起動後すぐにシステムが信頼できる状態に移行することを念頭に置いています。

DRTM ブロックは、ブートローダーを測定、認証し、OS が使用できるように次のシステム情報 (検証情報や認証情報など) を安全な方法で収集して保存します。

- 物理メモリ マップ
- PCI 設定スペースの場所
- ローカル APIC 設定
- I/O APIC 設定
- IOMMU 設定/TMR 設定
- パワー マネージメント設定

共有ハードウェアの信頼性

これは、ファームウェア コンポーネントが AMD シリコン上の ASP ブロックによって認証および測定され、測定値が安全に保存され、検証情報や認証情報などを含むそれらの測定値を OS がさらに使用できることを意味します。

AMD SMM SUPERVISOR

SMM (System Management Mode) は、x86 マイクロ コントローラーの特別な用途向けの CPU モードであり、パワー マネージメント、ハードウェア コンフィギュレーション、温度監視、その他のデバイス レベルの操作を処理します。これらのシステム操作のいずれかが要求されると、実行時に割り込み (SMI) が呼び出され、BIOS によってインストールされた SMM コードが実行されます。SMM コードは最高の特権レベルで実行され、OS からは見えないため、ハイパーバイザー メモリへのアクセスやハイパーバイザーを変更したりする悪意のあるアクティビティとして利用される可能性があり、それらのターゲットになります。

SMI ハンドラーは通常、オペレーティング システムとは異なるデベロッパーによって提供され、OS/ハイパーバイザーのメモリとリソースにアクセスできます。これは、SMM コードの悪用可能な脆弱性が、Windows OS、ハイパーバイザー (HV) および Virtualization Based Security (VBS) の侵害につながることを意味します。

SMM の分離を支援するために、AMD は AMD SMM スーパーバイザーと呼ばれるセキュリティ モジュールを導入しています。これは、SMI の発生後、制御が SMI ハンドラーに転送される直前に実行されます。AMD SMM スーパーバイザーは AMD DRTM サービス ブロックに常駐し、次の目的で使用されます。

- SMM がハイパーバイザーまたは OS メモリを変更できないようにブロックする。ただし、2 点間の小さな通信バッファーを除く
- SMM が実行時に新しい SMM コードを取り込まないようにする
- SMM がハイパーバイザーまたは OS を危険にさらす可能性のある DMA、I/O、またはレジスタにアクセスするのをブロックする

DMA 保護

DMA 再マッピング テクノロジにより、AMD プラットフォームは、DMA 再マッピング テクノロジを備えた入出力メモリ管理ユニット (IOMMU) などの AMD セキュア テクノロジを介して、プリブートおよび OS 環境でダイレクト メモリ アクセス (DMA) 保護をサポートします。

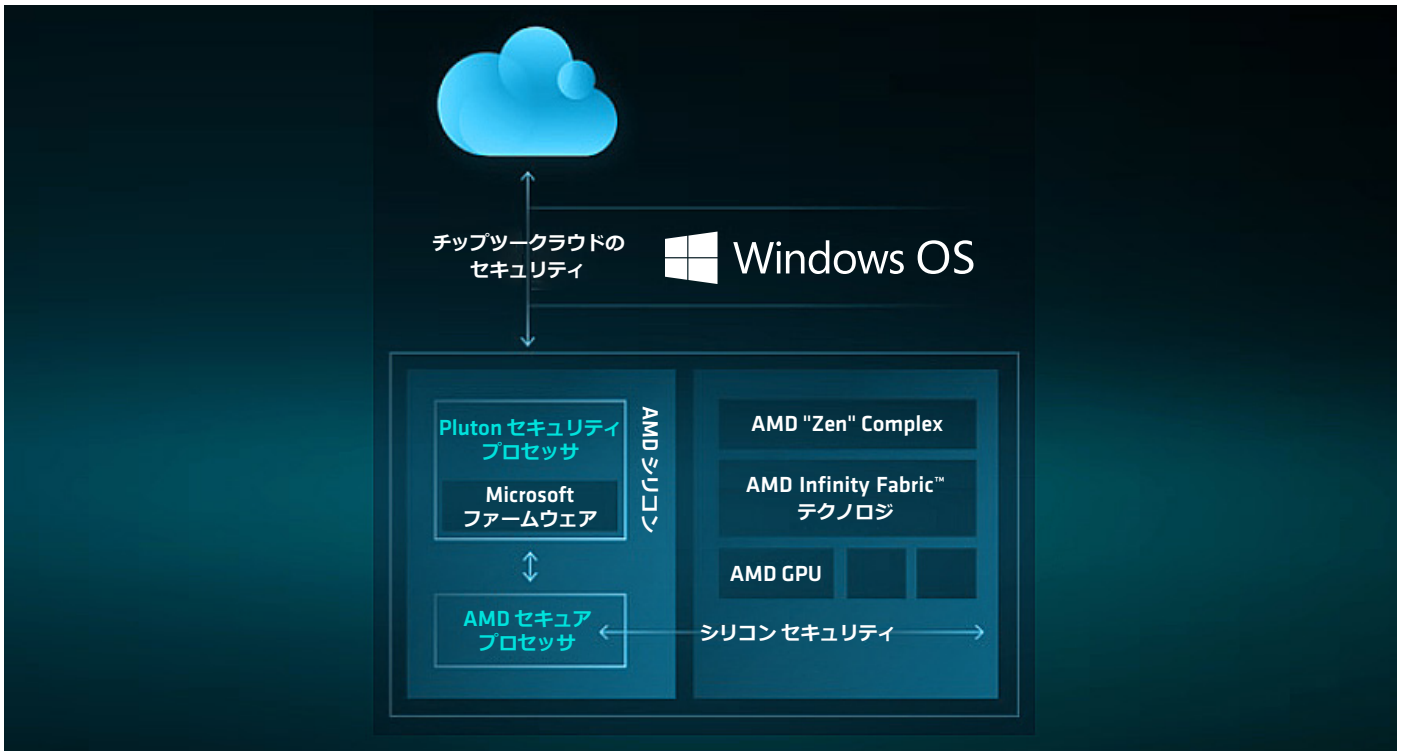
- DMA 保護機能は、接続されたデバイスを使用して攻撃者が DMA を攻撃する、プラットフォーム ファームウェアへの攻撃を防ぎます。
- DMA は、パフォーマンスを向上させるためにデバイスが物理メモリ アドレス空間に直接アクセスできるようにします。ただし、この機能によって悪意のあるソフトウェアがシステムにマルウェアを注入しやすくなり、OS によって検出されない可能性があります。

このような攻撃を防ぐために、AMD は OS 以前のファームウェア レベルで IOMMU を介してデバイスの DMA アクセスを管理/制御するセキュリティ アーキテクチャを設計しました。DMA セキュリティ アーキテクチャは、OS ブートローダーがメモリに構築された後、ファームウェアから OS にシステム メモリ保護設定の責任を引き継ぎます。OS が IOMMU 自体を制御するまで、IOMMU を使用した DMA 保護が各ブートに適用されます。

MICROSOFT PLUTON セキュリティ プロセッサ[8]

Microsoft Pluton は、設計を Microsoft が担当し、シリコン パートナーが製造する、CPU に組み込まれたセキュアな暗号化プロセッサです。Windows Update を通じて Microsoft が提供するアップデートにより、コードの整合性の確認と最新の保護を実現し、コアのセキュリティを強化します。

図 6. Microsoft Pluton セキュリティ アーキテクチャ概要。



Pluton はユーザー認証、ID、個人データ、暗号化キーを保護します。攻撃者がマルウェアをインストールしたり、PC を完全に物理的に占有した場合でも、情報を削除することは非常に困難です。

Microsoft Pluton は、Trusted Platform Module (TPM) の機能を提供し、TPM 2.0 仕様で対応可能な範囲を越えたほかのセキュリティ機能も提供するように設計されています。将来的には、追加の Pluton ファームウェアと OS 機能が Windows Update 経由で配信されるようになります。

AMD セキュア プロセッサ 2.0 (ASP 2.0) と Microsoft Pluton セキュリティ プロセッサは、AMD クライアント シリコン上で共存し、通信を実行してデバイスの整合性を保護します。Microsoft Pluton は、Windows エコシステムの統合型ハードウェアの信頼のルートとして機能することで Windows PC システムの保護を支援します。一方、ASP 2.0 は、シリコン ハードウェアの信頼のルートとして機能することで、プラットフォームにロードされた初期ファームウェアを認証することで整合性の確保を支援します。

プラットフォームのアップデート

AMD PRO プロセッサは、システムにリアルタイムにアクセスしようとする攻撃者に対するセキュリティ防御能力と、堅牢な更新メカニズムを提供します。そのため、企業はプラットフォームを更新し、ハードウェアまたはソフトウェアのバグによってできた脆弱性にパッチを適用できます。

AMD は OEM と緊密に協力して、ベストプラクティスに準拠し、かつ OEM のプラットフォーム更新ソリューションに統合可能な強化されたプラットフォーム更新アーキテクチャを提供しています。さらに、AMD PRO プロセッサには FAR (Firmware Anti-Rollback) 機能が搭載されており、ハードウェア ベースのポリシーにより、AMD セキュア プロセッサ 2.0 (ASP 2.0) ファームウェアのダウングレードをブロックできます。最後に、AMD PRO プロセッサには、A/B Recovery と呼ばれる安全なリカバリ フレームワークもあります。これは、OEM ソリューションに組み込んで、壊滅的な障害が発生した場合にリカバリを可能にする機能です。

暗号化アクセラレータ

今日の世界では、データと通信を保護するために暗号化操作が重要です。暗号化操作は不可欠ではあるものの、計算量も非常に多くなります。AMD は、シリコンに新しい最適化された命令を組み込むことで、暗号アルゴリズムの計算に関連するコストの削減を支援します。

AMD の "Zen 2" 以降のアーキテクチャでは、256 ビットのベクトル化 AES 暗号 (vAES256) のサポートが追加され、x86 レベルで AES の組み込み関数が統合されたことで、ユーザー アプリケーションが、強化された暗号化のパフォーマンスと効率性を活用できるようになりました。

FIPS 140-3 認証レベル 1

政府機関が IT 機器としてノート PC の購入を検討する場合、政府機関が取り扱うデータの機密性や提供するサービスの重要性を考慮すると、エンドポイントのセキュリティが最優先事項となります。最新のセキュリティ機能を備えていない旧式のハードウェアは、データ損失やサービスの中断という点で、高額なコストが発生する可能性があります。

FIPS (Federal Information Processing Standards) は、米国商務省標準化技術研究所 (NIST) が軍事以外の米国政府機関および請負業者のコンピューター システムで使用するために策定した、一般に公表された一連の規格です。FIPS 規格は、コンピューター セキュリティと相互運用性の要件を定めています。

AMD PRO プロセッサは、業界のセキュリティ認証である **FIPS 140-3 レベル 1** を取得しています。

図 7. AMD Ryzen™ PRO 7000 シリーズ プロセッサ用暗号化アルゴリズム検証プログラム。

Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

Implementation Name	AMD Ryzen PRO 7000 Series PSP Cryptographic CoProcessor (SHA2_RSAPSS_SIGVER)
Description	The AMD PSP Cryptographic CoProcessor provides cryptographic algorithm support for the Ryzen PRO 7000 Series processor. The following cipher implementation is covered: SHA2-384 and RSA-PSS sigver implementation.
Version	bc0c0140FIPS001
Type	HARDWARE
Vendor	Advanced Micro Devices (AMD) 2485 Augustine Drive Santa Clara, CA 95054 USA
Contacts	FIPS Contact FIPS@amd.com +1 408-749-4000

A3018 First Validated: 11/18/2022

Collapsed | Expanded | Aggregated

Operating Environment	Algorithm Capabilities
AMD Ryzen PRO 7330U (100-000000950)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7530U (100-000000949)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7730U (100-000000948)	RSA SigVer (FIPS186-4)
AMD Ryzen PRO 7330U (100-000000950)	SHA2-384
AMD Ryzen PRO 7530U (100-000000949)	SHA2-384
AMD Ryzen PRO 7730U (100-000000948)	SHA2-384

FIPS モジュールは、ハードウェア、ソフトウェア、ファームウェアの組み合わせで、認定されるセキュリティ機能をサポートします。FIPS は連邦政府での使用を目的として開発されたものですが、金融機関やクラウド プロバイダーなど、民間部門でも多くの企業が自主的にこれらの基準を採用しています。さらに、FIPS は北米以外にも拡大しており、ヨーロッパの NATO 加盟国向けのコンピューター プロセッサもその対象となっています。

クラウド ベアメタル復旧

クラウド ベアメタル復旧は、安全にリモートでシステムを復旧するメカニズムを提供し、ハードウェアやソフトウェアの重大な障害が発生した場合のダウンタイムを最小限に抑え、ビジネスの継続をサポートします。この機能は、OS の起動前に起動してクラウド経由でシステム復旧を可能にするため、デバイスを修理に出す必要がなくなります。

AMD PRO セキュリティ アーキテクチャと統合することで、クラウド ベアメタル復旧は、初期化と復旧をハードウェア レベルで強化し、復旧プロセス中の改ざんや悪用から保護します。

サプライ チェーン セキュリティ (デバイス ID)

AMD デバイス ID により実現されるサプライ チェーン セキュリティは、製造から展開、そしてそれ以降のライフサイクル全体を通じて、AMD ハードウェアを認証します。この機能は追跡可能性を提供し、偽造または改ざんされたコンポーネントから保護するため、企業のハードウェアの完全性が担保されます。

AMD デバイス ID によって真正な AMD シリコンの暗号化検証が提供されるため、正規のハードウェアのみが企業システムに統合されます。そのため、展開前にファームウェアやハードウェアが侵害される可能性があるサプライチェーン攻撃から保護できます。

ウォッチドッグ タイマー

ウォッチドッグ タイマーは、ハードウェア レベルで停止または応答不能となったプロセスを検知し、緩和することにより、システムの信頼性を向上させます。この機能により、フォールト トレランスがさらに強化され、システムが正常に動作し続けられるようになり、潜在的な問題からスムーズに回復できるようになります。

AMD PRO セキュリティ アーキテクチャに統合されたウォッチドッグ タイマーは、セキュア ブートやその他の基本機能と連動し、起動前および実行時の動作中に強固な障害検知を提供します。この機能により、ミッションクリティカルな環境におけるシステムのレジリエンスが強化され、ソフトウェアやハードウェアの故障によるダウンタイムのリスクが低減されます。

ソリューションの概要

セキュリティ レイヤー	機能	利点
システム	OEM セキュリティ機能	OEM のエンタープライズ級セキュリティ機能を補完し、有効にすることを目的とした、OS 開発者、ハードウェア ベンダー、OEM パートナー間の緊密な連携。
OS セキュリティ	WINDOWS 11 セキュリティ	Secured-core PC イニシアチブ、ハードウェア ベースのスタック保護機能、Advanced Threat Protection、拡張サインイン、BitLocker などをフル サポート。
ハードウェアおよびファームウェア	AMD セキュア プロセッサ 2.0	専用のセキュリティ プロセッサで実行前にコードを検証し、データとアプリケーションの整合性を確保。
	AMD PLATFORM SECURE BOOT	不正ソフトウェアやマルウェアが重要なシステム機能を乗っ取ることを防止するブート保護。
	AMD メモリ ガード	システム メモリをリアルタイムで暗号化し、ノート PC の紛失や盗難が発生した場合も、物理的攻撃からデータを保護。
	AMD SHADOW STACK	制御フロー攻撃の防御が追加された堅牢なセキュリティ アプローチ。通常のプログラム スタックをハードウェアに保存されたコピーと照合し、Windows 11® セキュリティで Microsoft のハードウェア強制型スタック保護を有効にする。
	Microsoft Pluton セキュリティ プロセッサ	Microsoft が設計、更新するチップツークラウドのセキュリティ テクノロジにより、Windows 11 PC のコア セキュリティを強化し、ユーザーの資格情報、ID、個人データ、暗号化を継続的に保護。
	AMD FIRMWARE TPM	プラットフォームに信頼性を提供し、セキュリティ違反の兆候がないか監視する、ファームウェア バージョン TPM。
	FIPS 140-3 レベル 1 モジュール認証	暗号化ハードウェアのセキュリティを検証するために、民間企業がベスト プラクティスとして政府の標準暗号化規格を採用。
	AMD セキュア プロセッサ 2.0	ハードウェアの信頼のルートとなり、初期ファームウェアを検証し、不正なコードからプラットフォームを保護する。
	クラウド ベアメタル復旧	デバイスを発送することなく、クラウド経由で安全なシステム復旧を可能にする。重大な障害が発生した場合でも、ダウンタイムを最小限に抑えるように設計されている。

要約

AMD PRO テクノロジは、現代の企業の絶えず進化するニーズに対応するための包括的な基盤を提供します。AMD は、強化されたセキュリティ、シームレスな管理性、ビジネス対応の信頼性をすべての AMD Ryzen™ PRO プロセッサに統合することで、企業がデータを保護し、IT 運用を合理化し、さまざまな作業環境で次世代の生産性を実現できるよう支援します。

職場でハイブリッド運用が採用され、AI 主導のワークフローが統合される現在、AMD は引き続きイノベーションの推進に尽力しています。AMD PRO テクノロジは、新しい世代が生まれるたびに、セキュリティ、パフォーマンス、管理性の限界を押し広げており、企業が今日の課題に対応し、明日のチャンスに備えるための装備を充実させています。

免責条項

ここに記載されている情報は、情報提供のみを目的としており、事前通知なしで変更される場合があります。この資料の作成時には確認を重ねているものの、技術的な誤りや欠落、誤記などが含まれる可能性があり、AMD は当該情報の更新または修正の義務を負いません。また、AMD 製品には、公開されている仕様からプロセッサが逸脱する原因となるエラッタが含まれている場合があます。AMD は通知なしにこうした製品のエラッタを特定することがありますが、その義務は負わないものとします。Advanced Micro Devices, Inc. は、この資料の内容の正確性または完全性に関していかなる表明または保証も行わず、ここに記載される AMD ハードウェア、ソフトウェア、その他の製品の操作または使用に関して、非侵害、商品性、特定の目的への適合性の黙示的な保証を含め、いかなる種類の責任も一切負わないものとします。この資料は、黙示的あるいは禁反言で生じるものを含め、いかなる知的財産権へのライセンス付与を行うものではありません。AMD 製品の購入または使用に適用される条件および制限は、当事者間で締結された契約または AMD 標準売買条件に規定されているとおりです。

脚注

1. AMD メモリ ガードによる完全なシステム メモリ暗号化は、AMD Ryzen PRO、AMD Ryzen Threadripper PRO、AMD Athlon PRO プロセッサに含まれ、OEM による有効化が必要です。製品を購入する前に、システム メーカーにお問い合わせください。GD-206。
2. AMD Platform Secure Boot (PSB) 機能を有効にした OEM は、AMD Platform Secure Boot 対応マザーボードを搭載しているプラットフォームでのみ、暗号化された署名付きの BIOS コードを実行できるよう許可できます。プロセッサの OTP (One Time Programmable) ヒューズにより、プロセッサが OEM のファームウェア コード署名キーにバインドされます。この時点で、このプロセッサは、同じコード署名キーを使用しているマザーボード以外では使用できなくなります。GD-192。
3. AMD PRO の管理性は、Intel vPro を上回る DASH Management Initiative のプロファイルを実装し、デスクトップおよびモバイル システムのマルチベンダー管理をサポートします。KRKP-7
4. AMD PRO の管理性は、Intel vPro と比較して、より高いレベルのセキュリティと低いレイテンシ (TLS 1.3 と 1.2 を比較) を実現する TLS (Transport Layer Security) プロトコルの最新バージョンを実装しています。KRKP-8
5. Principled Technologies レポート - https://www.amd.com/content/dam/amd/en/documents/products/processors/technologies/ryzen-7-mixed-cpu-deployment.pdf
6. AMD セキュア プロセッサは、AMD が設計した各システムオンチップ (SoC) および ASIC (特定用途向け集積回路、Application Specific Integrated Circuit) に統合された専用オンチップ セキュリティ プロセッサです。ハードウェアに固定された信頼の基点 (Root of Trust) によるセキュア ブートを可能にし、セキュア ブート フローを介して SoC を初期化し、分離された信頼できる実行環境 (TEE) を確立します。GD-72。
7. AMD メモリ ガードによる完全なシステム メモリ暗号化は、AMD Ryzen PRO、AMD Ryzen Threadripper PRO、AMD Athlon PRO プロセッサに含まれています。OEM による有効化が必要です。製品を購入する前に、システム メーカーにお問い合わせください。GD-206
8. Microsoft Pluton は、Microsoft が所有し、AMD にライセンス供与されたテクノロジです。Microsoft Pluton は、米国およびその他の国における Microsoft Corporation の登録商標です。詳細については、https://www.microsoft.com/security/blog/2020/11/17/meet-the-microsoft-pluton-processor-the-security-chip-designed-for-the-future-of-windows-pcs/ をご覧ください。Microsoft Pluton セキュリティ プロセッサは、OEM による有効化が必要です。製品を購入する前に、OEM メーカーにお問い合わせください。AMD は、第三者の主張を独自に検証していません。GD-202。
9. AMD セキュア プロセッサは、AMD が設計した各システムオンチップ (SoC) および ASIC (特定用途向け集積回路、Application Specific Integrated Circuit) に統合された専用オンチップ セキュリティ プロセッサです。ハードウェアに固定された信頼の基点 (Root of Trust) によるセキュア ブートを可能にし、セキュア ブート フローを介して SoC を初期化し、分離された信頼できる実行環境 (TEE) を確立します。GD-72。