vmware
vCloud Air™ Network

IBM Cloud

VMware on IBM Cloud と Intel® Trusted Execution Technology だからできる

セキュアなクラウド・ワークロード

セキュアなクラウド・ワークロード

パブリック・クラウド内のエンタープライズ・ワークロードを潜在的な脅威から保護します。IBM Cloud のベア・メタル・サーバーと Intel® TXT により、ハードウェアでさらに強化されたセキュアなプラットフォームを構築できます。

特徴的な機能

トラスト・チェーンの構築
ハードウェア・ベースのトラスト・チェーンが、ハードウェアからハイパーバイザーまで起動シーケンス全体に拡張されます。

起動制御ポリシー
ハードウェアと起動前ソフトウェアが入念に検査済みであり、正常な状態であることを検証します。

ロケーションに基づいた制御を提供
コンプライアンスを守るため、仮想マシンのマイグレーション対象サーバーを指定されたポリシーによって制限します。

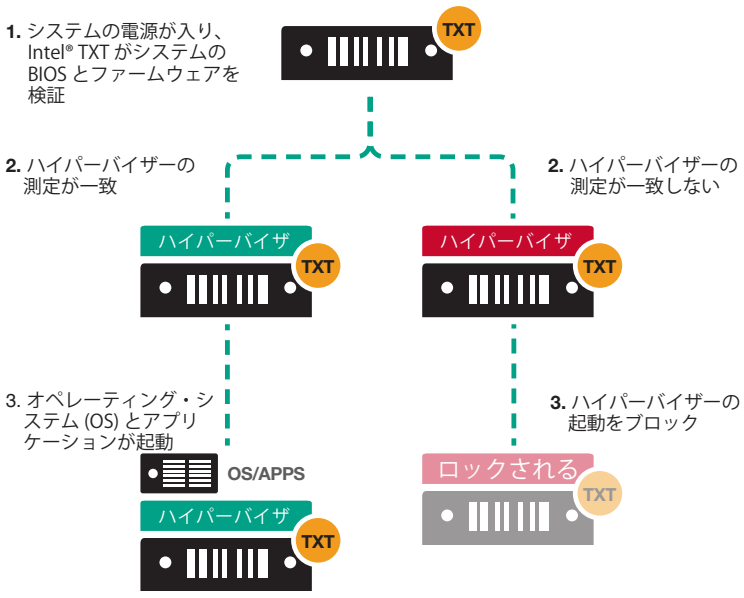
IBM Cloud は、インフラのセキュリティー強化手段として Intel® TXT を提供する初めてのクラウドです。Intel® TXT により、BIOS、ファームウェア、ハイパーバイザーなどのハードウェア・プラットフォームは、確実に正常な状態を保ちます。

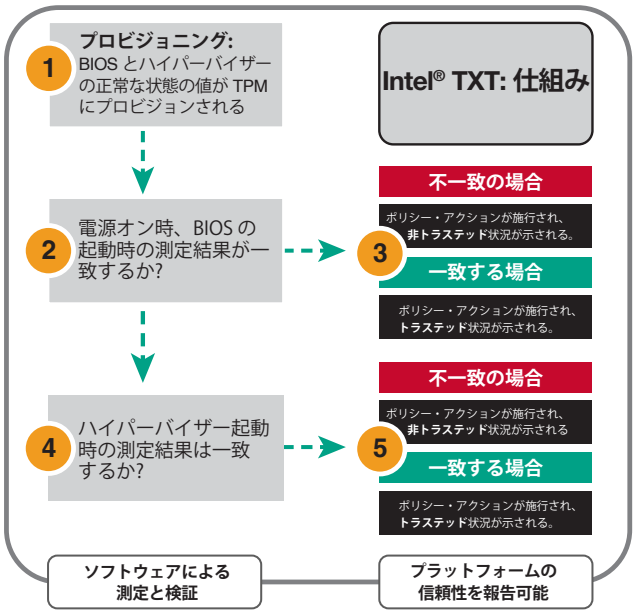
テクノロジー

Intel® TXT は、BIOS からハイパーバイザーまでに至る起動環境のすべての重要要素から構成されるメジャード・ラウンチ環境 (MLE) を作成します。ブート・プロセスの際中、トラステッド・プラットフォーム・モジュール (TPM) は、コンピューターにより生成された暗号化キーを保持します。暗号は基本的に、信頼できるシステムを確立するために繰り返し測定、拡張、検証、実行を行うコードです。実行中のブート環境が正常な状態の構成と一致しない場合、Intel® TXT ハードウェアは起動を阻止し、重要なアプリケーションとサーバーを潜在的な脅威から保護します。

Intel® TXT を使い始めるには

Intel® TXT は、IBM Cloud のベア・メタル・サーバーで利用できます。新しいサーバーをオーダーする際に、ストアで Intel® TXT オプションを選択するか、クラウド・エキスパートに問い合わせてください。





vmware®
vCloud Air™ Network

IBM Cloud