Power Systems

PowerVM におけるセキュア・ブート

Power Systems

PowerVM におけるセキュア・ブート

お願い

本書および本書で紹介する製品をご使用になる前に、 11 ページの『特記事項』に記載されている情報をお読みください。

本装置は、高調波電流規格 JIS C 61000-3-2 に適合しています。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。本体機器提供後に、追加で電源コード・セットが必要となった場合は、補修用の取扱いとなります。

本書は、IBM AIX バージョン 7.2、IBM AIX バージョン 7.1、IBM AIX バージョン 6.1、 IBM i 7.3 (製品番号 5770-SS1)、IBM Virtual I/O Server バージョン 3.1.0.0、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： Power Systems
Secure boot in PowerVM

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

PowerVM におけるセキュア・ブート

IBM® Power Systems™ サーバーは、高度な機密保護機能を備えたサーバー・プラットフォームを提供します。IBM POWER9™ プロセッサー・ベースのハードウェアおよびファームウェアには、新規の PowerVM® 機能が組み込まれており、クラウド・デプロイメント用にさらにセキュアなプラットフォームを提供します。

POWER9 プロセッサー・ベースのサーバーで使用できる主要な PowerVM 機能には、以下のものがあります。

- セキュアな初期プログラム・ロード (IPL) プロセスまたはセキュア・ブート機能は、適切に署名されたファームウェア・コンポーネントのみがシステム・プロセッサーを実行できるようにします。ファームウェア・スタックの各コンポーネント (ホスト・ブート、POWER ハイパーバイザー (PHYP)、区画ファームウェア (PFW) など) は、プラットフォームの製造元によって署名されており、IPL プロセスの一部として検証済みです。
- ハードウェアの Trusted Platform Module (TPM) を介してシステム・ファームウェア・スタックのリモート構成証明 をサポートするフレームワーク。

セキュア・ブートおよびトラステッド・ブート

本書では、「セキュア・ブート」および「トラステッド・ブート」という用語には特定の意味があります。これらの用語は、明確に区別して使用されていますが、相補的な概念です。

セキュア・ブート
: セキュア・ブート機能は、すべてのファームウェア・コンポーネントのハードウェア保護された検証の実行にデジタル署名を使用することで、システム保全性を保護します。また、この機能は、重要なシステム・メモリー領域へのサービス・プロセッサーとサービス・インターフェースのアクセスを制御することで、ホスト・システムのトラスト・ドメインとフレキシブル・サービス・プロセッサー (FSP) のトラスト・ドメインとの区別も行います。

トラステッド・ブート
: トラステッド・ブート機能は、特定のファームウェア・コンポーネントがシステム上で実行されたことを証明する、強い暗号化で保護されたプラットフォーム測定を作成します。トラステッド・プロトコルを使用して測定を評価ことでシステムの状態を判別し、その情報を使用してセキュリティーに関する決定を行うことができます。

PowerVM におけるセキュア・ブートの新機能

このトピック・コレクションの前回の更新以降に PowerVM におけるセキュア・ブートに関して新しく追加または変更された情報は次のとおりです。

2018 年 8 月

- このトピック・コレクションに対して各種更新が行われました。

用語

この資料で使用される用語について説明します。

アジャンクト
: 別の区画に割り当てられた CPU を使用する子区画。アジャンクトは、システム管理者が容易に使用することができます。アジャンクトを使用して、メイン区画を保守することができます。

変更/表示ユニット **(ADU)**
: メイン・ストレージへのアクセスに使用されるハードウェア・リソース。ADU は、ハードウェアおよびファームウェアのエレメントによって使用されます。

コード・コンテナー
: 検証可能なコード・イメージ。これには、ソース・ブートの接頭部ヘッダーが含まれます。コンテナーは、4K 接頭部ヘッダー (ハードウェア・ヘッダー、接頭部鍵ヘッダー、またはファームウェア・ヘッダー) と、それに続く保護されたペイロード (接頭部ヘッダーにハッシュを持つコード・イメージ)、サーバーに固有の保護されていないペイロード・データから構成されます。

コード署名の権限
: サブジェクト・コードに関する知識がある個人に対して、サーバー機能に署名する権限がある署名者として役割を果たせるように付与される権限レベル。

Core Root of Trust for Measurement (CRTM)
: 優先トラステッド (変更不可能) コード。これは、プラットフォーム資格情報の一部です。静的 RTM モデルでは、サーバーまたは物理ハードウェア環境の電源をオンにする際、あるいはサーバーまたは物理ハードウェア環境をリセットする際に、CRTM コードを最初に実行する必要があります。セキュア・ブート機能のために、CRTM コードは、自己ブート・エンジン/ホスト・ブート (SBE/HB) をベースにしています。 CRTM コードには、自己ブート・エンジンと十分なホスト・ブート・コードが組み込まれており、TPM デバイス・ドライバーを初期化することができます。

管理コンソール **(MC)**
: システム管理者およびサービス担当員が、システムのハードウェア、区画化、保守の各側面に関するタスクを表示および実行するためのインターフェース。

マスター・プロセッサー
: NOR (NOT-OR) 型フラッシュ・メモリーに物理的に接続されている、ノード内のプロセッサー。

PCR 拡張
: TPM プラットフォーム構成レジスター (PCR) 上で実行される操作。これにより、レジスター値が更新され、拡張されたメッセージの履歴がレジスターに記録されます。 PCR 拡張操作では、PCR に対して直接書き込み操作を実行するのではなく、PCR 内の元の値を取得し、その値に新規メッセージを連結し、ハッシュを取得して更新されたレジスター値を生成します。拡張されたメッセージの履歴およびエクステントの順序は、対応する TPM イベント・ログと後で比較することができます。

プラットフォーム証明書
: TPM 内に存在する証明書。この証明書は、TPM 関連プラットフォームが、CRTM コードを持つ IBM プラットフォームであることを証明します。この証明書は、プラットフォーム・モデルに依存しません。

PNOR
: プロセッサー NOT-OR (PNOR)。フラッシュとも呼ばれます。

接頭部ヘッダー
: セキュア・ブート・コード・コンテナーの署名付きコード・イメージの接頭部となる 4 KB の構造。

コード署名の秘密鍵
: 公開鍵暗号方式に使用される公開鍵/秘密鍵のペアの秘密部分。非対称鍵アルゴリズムを使用します。

保護レジスター
: フレキシブル・サービス・プロセッサー (FSP) がスキャン通信 (SCOM) を使用した場合は読み取り専用ですが、トラステッド・コードを使用した場合は読み取り/書き込みが可能なレジスター。ほとんどの場合、これらのレジスターは初期化時にスキャンされた値とは無関係で、デフォルトで既知の値に設定されます。

コード署名の公開鍵
: 公開鍵暗号方式に使用される公開鍵/秘密鍵のペアの公開部分。非対称鍵アルゴリズムを使用します。

リモート構成証明
: リモート・コンピューター上で実行されているソフトウェアをチェックします。構成証明は、情報の正確度を検証するプロセスです。リモート構成証明により、許可されたステークホルダーは、TPM とその TPM が存在するプラットフォームの両方の状況を確認することで、ユーザーのコンピューターに対する変更を判別することができます。

自己ブート・エンジン **(SBE)**
: プロセッサー・チップを初期化してホスト・ブート・プロシージャーを実行するために使用される、パワーオン・リセット・エンジン。

シグニチャー
: メッセージの真正性を示します。シグニチャーは、公開鍵/秘密鍵のペアの片方で暗号化されたサブジェクト・メッセージのハッシュから構成されます。

Static Root of Trust for Measurement (SRTM)
: 常に信頼できると見なされるファームウェア・コードの変更不可能な部分からのシステム・ブート。ブート・アクションは、測定プロセスを開始します。このプロセスでは、各コンポーネントがチェーン内の次のコンポーネントを測定します。

Trusted Building Blocks (TBB)
: 保護されたロケーションや保護された機能がない、Root of Trust Measurement (RTM) の部分が含まれます。 TBB には、CRTM、CRTM ストレージからシステム・ボードへの接続、TPM からシステム・ボードへの接続、ユーザーの物理プレゼンスを判別するメカニズムが含まれます。

トラステッド・コード
: 事前指定された IBM ハードウェアおよびファームウェアの権限によって許可されたファームウェア。コードのソースが認証され、イメージの保全性が検査されます。

Trusted Computing Group (TCG)
: Trusted Computing Group は、ベンダー中立のオープンなグローバル業界標準を開発、定義、およびプロモートするために結成された非営利団体であり、相互運用可能な信頼できるコンピューティング・プラットフォームを実現するために、ハードウェア・ベースの Root of Trust Measurement (RTM) を支援しています。

トラステッド・メモリー
: トラステッド・コードのみがアクセス (読み取りおよび書き込み) 可能なメモリー領域。システムがセキュア・モードでブートする場合、トラステッド・メモリーへのアクセスは、ハードウェア分離メカニズムによってブロックされます。トラステッド・メモリー領域の外部にある、メモリーの

小さいセクションは、非トラステッド・メモリー と呼ばれます。このセクションには、サービス・インターフェースを使用して容易にアクセスし、読み取りおよび書き込み操作を実行することができます。

Trusted Platform Module (TPM)
スマート・カードのような低パフォーマンスの暗号化コプロセッサー。TPM は、ブート・シーケンスのハッシュを一連のプラットフォーム構成レジスター (PCR) に保管することができます。

非トラステッド・メモリー
読み取りアクセスおよび書き込みアクセスがオープンなメモリー領域。これには、フレキシブル・サービス・プロセッサー (FSP) や、ホスト・プロセッサーのセキュリティー・ドメインの外部に存在するサービス・インターフェースなどがあります。

検証　署名者の ID を検証します。例えば、コード・コンテナーの検証は、含まれているイメージ内のコードが IBM によってデジタル署名されていること、およびイメージが変更されていないことを検証することを意味します。

検証コード
保護されたコードは、Serial Electrically Erasable Programmable Read-only Memory (SEEPROM) 内に存在し、セキュア・ブート・コード・コンテナーのシグニチャー検証サポートを提供します。検証コードは、セキュア・ブート中の Core Root of Trust for Measurement を構築するために使用される主要なエレメントです。

セキュアな初期プログラム・ロード (IPL) プロセス

セキュア・ブート機能は、システム・プロセッサー上で稼働する無許可のファームウェアを介したカスタマー・データへの不正アクセス、許可されたサービス・プロセッサー・ファームウェア内のセキュリティーの脆弱性を利用したカスタマー・データへの不正アクセス、フレキシブル・サービス・プロセッサー (FSP) 経由でアクセスしたハードウェア・サービス・インターフェースを介したカスタマー・データへの不正アクセスを防止します。

セキュア・ブート機能は、カスタマー・データへの不正アクセスを防止しますが、セキュア・ブート・メカニズムでは、以下の脅威に対する保護は提供されません。

- オペレーティング・システム・ソフトウェア・ベースの攻撃によるカスタマー・データへの不正アクセス。
- システム管理者による不正。
- ハードウェアへの物理攻撃 (例えば、チップの交換やバス・トラフィックの記録など)。

セキュア・ブート機能は、POWER9 プロセッサー・ハードウェアにプロセッサー・ベースの信頼チェーンを実装します。これは、POWER9 ファームウェア・スタックによって有効にされます。セキュア・ブート機能は、信頼できるファームウェア・ベースを提供することで、仮想化環境におけるカスタマー・データの機密性と保全性を強化します。

POWER9 プロセッサー・ベースのサーバーのトラステッド・ブート機能により、システム構成および初期プログラム・ロード (IPL) パス・コードを測定できるようになります。これは、後でシステムの初期 IPL パス構成の構成証明を行う際に証拠として使用することができます。 Core Root of Trust for Measurement (CRTM) を作成するために、セキュア・ブート・フローが使用されます。このフローは、Trusted Platform Module (TPM) との通信が確立されるまで、IPL プロセスの各フェーズに暗号検査を追加します。セキュア・ブート・フローを使用することで、コア・プロセッサーで稼働する必要があるすべて

のファームウェアの保全性が確保され、無許可のファームウェアや悪意を持って変更されたファームウェアが実行されるのを防止できます。いずれかの時点でコードの認証に失敗すると、IPL プロセスは完了できません。

POWER9 システムのセキュア・ブート機能は、プラットフォームのブート・プロセス全体の信頼を確立します。ここでの信頼できる とは、IPL プロセス中に実行されるコードが、そのプラットフォームの製造元から提供されたものであり、プラットフォームの製造元によって署名されており、変更されていないことを意味します。

POWER9 プロセッサー・ベースのサーバーで使用可能なセキュア・モード保護は、FSP およびサービス・インターフェースによるカスタマー・データへの読み取り/書き込みアクセスを防止し、ホスト・プロセッサーでの信頼できないコードの実行を防止し、セキュア・ブート・プロセスのすべてのキーポイントにわたって信頼性を保持することで、信頼性を保持します。

POWER9 のセキュア・ブート機能は、プロセッサー・ベースの信頼チェーンを実装します。このチェーンは、暗黙的に信頼できるコンポーネントから開始されますが、他のコンポーネントは、ホスト・プロセッサー・コアで実行される前に、保全性を確保するために認証および検査されます。 Serial Electrically Erasable Programmable ROM (SEEPROM) 内のロックされたプロセッサーにある検証コードは、初期ファームウェア・ロードを検証します。ファームウェアは、後続のファームウェアが信頼できる必要がある場合、および POWER9 プロセッサー・コアで実行するためにロードされる場合には、そのすべてのファームウェアの暗号シグニチャーを検証します。 POWER9 システムでは、SEEPROM セキュリティー・スイッチは自己ブート・エンジン (SBE) コード内で設定され、システムの製造元 (MFG) の組み立てラインで固定されます。これが、セキュアな IPL フローをハードウェアが実施するための基礎になります。物理的セキュリティー・モードのジャンパーは、システムのバックプレーン で使用可能です。システムに物理的にアクセスすれば、このジャンパーを使用して、プロセッサーのセキュア・モード・スイッチをオーバーライドすることができます。セキュア IPL プロセスは、Power® プラットフォームでのトラステッド・コンピューティングをさらに強化します。

以下の図は、セキュア・ブートおよびトラステッド・ブートの IPL プロセスの動作を示しています。

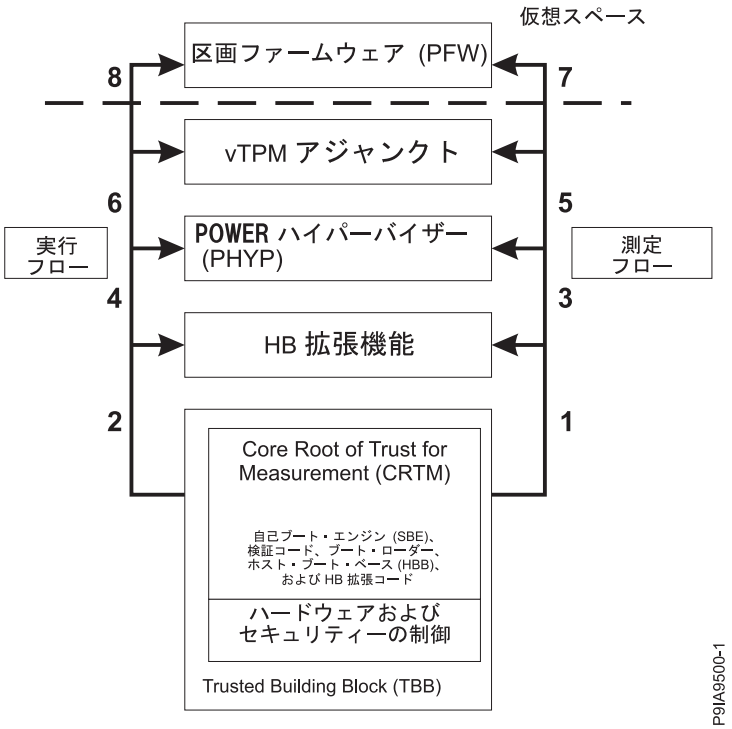

図 *1.* セキュア・ブートおよびトラステッド・ブートのフロー

セキュア・ブート機能は、ロックされた SEEPROM、SBE、およびホスト・ブート・ベース・コード (ホスト・ブート拡張コードの小さい部分を含む) を Core Root of Trust for Measurement (CRTM) として構築し、POWER Hypervisor™ (PHYP)、区画ファームウェア (PFW)、選択されたアジャンクト区画 (物理トラステッド・プラットフォーム・モジュール (pTPM)、仮想トラステッド・プラットフォーム・モジュール (vTPM)、ホスト・ブート・ランタイム、および暗号化アジャンクト)、オンチップ・コントローラー (OCC – 温度管理) を組み込むために信頼チェーンを拡張します。この信頼ドメインとプロセッサー・ハードウェア・セキュリティーのサポートにより、どのようなハードウェアあるいはファームウェアのメカニズムを使用しても、カスタマー・データの表示や変更を行うことができないようにすることができます。

完全なトラステッド・ファームウェア・スタックは、署名されたイメージを使用して認証され、トラステッド・メモリーのロケーションで実行されます。 FSP は、ホスト・サーバーの信頼ドメインの外部にあり、変更/表示ユニット (ADU) レジスター、その他の保護されたレジスター、およびトラステッド・メモリー領域へのアクセスはブロックされます。自己ブート・エンジン (SBE) は、プロセッサー・レジスターの読み取り/書き込みスキャン通信 (SCOM) 機能のブラックリストをフィルタリングすることで、FSP ブロックを実施します。 SCOM 機能は、プロセッサー・チップの SEEPROM 領域にあるセキュア・アクセス・スイッチによって有効にされます。

以下の図は、セキュア・ブート環境を示しています。

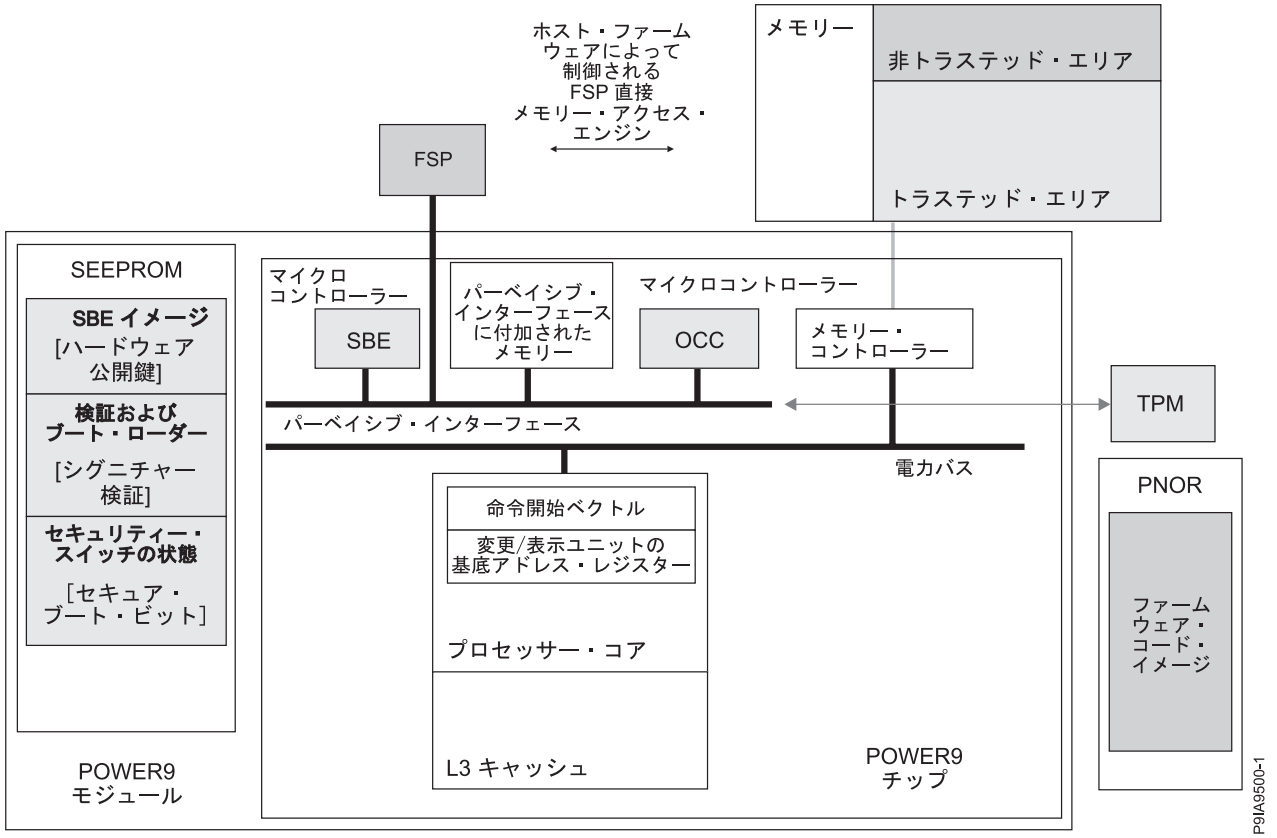

図 2. セキュア・ブート環境

セキュア・ブート・プロセスが開始されると、FSP エレメントは、ブート要求およびブート・タイプに関する詳細をシステム内のプロセッサー・チップに送信します。内部的には、セキュア・ブート・ロジックの状態は、以前に設定された値がクリアされており、適切な既知の状態から開始されます。この状態は、以前に実行されたテンパリング要求もすべてクリアされています。悪意のある攻撃者がこの初期ステップをスキップするのを防止するために、ハードウェア保護メカニズムが実装されています。 FSP から内部チップへのアクセスはロックされ、セキュア・ブート・エンジンが、モジュール上にあるセキュアかつ不揮発性でロックされているメモリーから、初期化コードのフェッチを開始します。このコードは、基本的なチップの初期化を実行し、TPM をリセットします。

ブート・プロセスの初期ステップが完了すると、自己ブート・エンジン(SBE) は SEEPROM からホスト・ブート・ローダーおよび検証コードを、プロセッサー・チップの内部 L3 キャッシュにロードします。その後、プロセッサー・コアが開始され、ブート・ローダーが初期ホスト・ブート・ベース (HBB) コードをプロセッサー NOR (PNOR) フラッシュ・チップからフェッチし、それを L3 キャッシュにロードします。セキュア・モードでは、L3 キャッシュからの検証コードを使用して、トラステッド・キャッシュで使用可能になった HBB イメージが検証されます。初期フラッシュ・コードの検証が完了した後、プロセッサー・コアは引き続きトラステッド・メモリー・スペースからの検証済みコードを実行し、HB 拡張機能 (HBI) をロードして検証します。 HBI が測定され、シグニチャーが検証されてコピーされた後、図セキュア・ブートおよびトラステッド・ブートのフローのステップ **1** に示されているように、有効な認証を示す測定結果 (イメージ・ハッシュ) が TPM に記録されます。この時点で、実行されるすべてのコードが完全に PNOR フラッシュ・チップに入っており、システムにアクセスした他のメカニズムはありません。これは、トラステッド・ブートの境界と呼ばれます。検証に失敗した場合、システムは即時に停止され、ハードウェア保護メカニズムによって保護することで、信頼できないコードや不正なコードが実行されることを防ぎます。

その後、HB コードは新しいトラステッド・イメージを使用して、セキュアな不揮発性メモリーの保留中の更新を管理します。 Core Root of Trust (CRTM) を保護するために、HB コードはセキュア・メモリーをロックすることで、そのメモリーに対する追加の書き込みアクセスを防止します (このアクションは、システムがリブートされると、この信頼できる状態に戻すことを意味します)。その後、HB コードは、オンチップ・メモリー・コントローラーおよび取り付けられたメモリー DIMM (Dual Inline Memory Module) を初期化します。また、HB コードは、メモリー・コヒーレント・インターフェースをシステム内の他のチップに構築する前に、そのコードが実行されるプロセッサーに直接取り付けられた他のチップも初期化します。これらの他のチップも、セキュアで信頼できる状態であることを確認するために検証されます。

その後、上位のファームウェア・スタック・コンポーネントがロード、検証、実行され、その測定結果が TPM に記録されます。このアクションでは、図セキュア・ブートおよびトラステッド・ブートのフローに示されたステップ **2** を実行します。図セキュア・ブートおよびトラステッド・ブートのフローのステップ **3** では、POWER Hypervisor (PHYP) ペイロードがメイン・メモリーにロードされます。その後、コードは暗号で認証され、認証に成功すると PHYP の実行が開始されます。 PHYP コードの認証測定の結果は TPM に記録されます。同様に、図セキュア・ブートおよびトラステッド・ブートのフローに示されたステップ **4** から **8** が実行され、ロックされていないフラッシュ・メモリーからトラステッド・メモリーにコードをロードします。コードが暗号で認証された後、各種アジャンクトと区画ファームウェア (PFW) が実行されます。

セキュア・ブートでの物理 TPM サポート

Trusted Platform Module (TPM) により、稼働中のシステムでのコード・スタックのリモート構成証明が可能になります。トラスト・ファームウェアのチェーンは、ロードされたファームウェアのハッシュを記録し、その記録をプロセッサー TPM のネットワークに保管します。ネットワークは、マスター・プロセッサー当たり 1 つの TPM (ローレンジからミッドレンジのプラットフォームの場合)、あるいはマスター・プロセッサーまたは代替マスター・プロセッサーによる冗長 TPM (マルチノード・エンタープライズ・プラットフォームの場合) で構成することができます。トラスト・ファームウェアのチェーンは、すべてのイベントを TPM イベント・ログにも適切に記録します。

構成証明は、Trusted Computing Group (TCG) 2.0 準拠のトラステッド・ブートをサポートします。 TPM インフラストラクチャーは、IBM によってオープン・ソース化された参照リモート構成証明の実装をサポートします。

ホスト・プロセッサー TPM は、製造業 (MFG) 業界におけるリモート構成証明に対応しており、プロビジョニング・フェーズと初期化フェーズが組み込まれています。 *TPM* プロビジョニング は、システムを組み立てる前に現場交換可能ユニット (FRU) の TPM モジュールに対して実行される、一回限りのプロセスです。 *TPM* プロビジョニング は、TPM が、必要なセキュリティー・サービスをフルスタック・ユーザーに提供するための準備をします。 *TPM* プロビジョニング には、TPM の事前構成値、許可値、およびポリシーの設定、階層のプロビジョニング、TPM 不揮発性 (NV) スペースへの関連する証明書と鍵のインストールが組み込まれており、それらにより、指定された TPM に証明書がバインドされます。このプロセスには、単一ノード・システムの場合にはエンドースメント鍵とプラットフォーム証明書の設定が含まれます。マルチノード・システムの場合にはさらにノード証明書の設定が含まれます。この段階の処理では、システムに IBM 認証局からの証明書が必要です。

TPM 初期化 は、初期プログラム・ロード (IPL) ごとに 1 回、ファームウェアによって実行されます。その後、TPM は、電源オフ状態 (リセットがアサートされた状態、または TPM 電源が投入されていない状態) から初期化された状態に移行します。 *TPM* 初期化 には、Roots of Trust for Measurement のリセ

ット、TPM ファームウェアの検証、TPM インターフェースでコマンドを受け入れる準備が組み込まれています。 TPM は、TPM 自己診断テスト (プラットフォームの始動ポリシーで定義されたエクステント) の完了後に、完全に作動可能なモードに入ります。

TPM 2.0 のプロビジョニング

Trusted Platform Module (TPM) プロビジョニング・プロセスについて説明します。

製造業 (MFG) 業界における *TPM* プロビジョニング・プロセスには、以下の要件があります。

- TPM は、すべての POWER9 プラットフォームで、交換可能なカード上で使用可能でなければなりません。この要件は、*TPM* プロビジョニング の単一制御点を提供します。*TPM* プロビジョニング は、POWER7®/POWER8® 重要プロダクト・データ (VPD)/アンカー・カードのプロセスに基づいて設計されています。
- *TPM* プロビジョニング は、(MFG のボックス組み立てライン・プロセスではなく) オフラインの部分組み立てプロセスで実行される必要があります。
- *TPM* プロビジョニング の後、TPM カードは、引き続きシステム情報や発注固有の情報を持たない汎用カードと見なされます。
- TPM カードは、プロビジョン後に資産保護区分番号 3 (APC3) のパーツ (セキュア・サプライ・チェーン・トラッキングでの定義) になります。
- *TPM* プロビジョニング を行う場合、TPM カードのプロビジョニング中に IBM 認証局との接続が必要です。
- *TPM* プロビジョニング では、フルフィルメントが取り消された場合に TPM カードを出荷可能状態に戻すためのプロセスが必要です。

TPM イベント・ログ

Trusted Platform Module (TPM) プラットフォーム構成レジスター (PCR) Extend 操作が実行されると、TPM イベント・ログ・ファイルにイベント・ログ項目が記録されます。このログ・ファイルは、リモート構成証明に依存する外部エンティティーによって使用されます。また、マルチノードの同期中にホスト・ファームウェアによって使用されます。これらのログ・ファイルは、PCR 値を再構成し、既知の値に対して検証するために使用されます。イベント・ログ・ファイルは、TPM によって保持されません。したがって、ファームウェアがログ・ファイル用の保管領域を提供し、PCR Extend の実行時にログ・ファイルを更新したり、構成証明のためにログ・ファイルにアクセスしたりするためのインターフェースを提供する必要があります。

初期の *PCR Extend* 操作は、ホスト・ブート (HB) コードによって実行されるため、POWER Hypervisor (PHYP) が開始されると、初期プログラム・ロード (IPL) の実行時の Extend 操作に関連するイベント・ログ情報は、HB コードに保存されます。また、HB コードは、関連するイベント・ログ項目を、ホスト・データ領域 (HDAT) 構造を介して PHYP に通知します。

PHYP は、TPM イベント・ログ情報を物理 TPM (pTPM) アジャンクト状態で保持します。各 TPM ログ・ファイル用に最大 64 MB のストレージ域が割り振られます。並行ファームウェア更新について作成されたログ項目 (無限のログ項目とも呼ばれる) に優先権が付与されます。ローレンジおよびミッドレンジのプラットフォームでは、ノードごとに 1 つの pTPM があります。マルチノード・エンタープライズ・プラットフォームでは、ノードごとに 1 つの追加 (冗長) pTPM があります。

TPM ログ・バッファーがフルの場合、TPM に対する追加の *PCR Extend* 操作が許可されます。ログ・ファイルの切り捨てが記録され、構成証明インターフェースは、配信されたログ・ファイルが切り捨てられたことを示すフラグを受け取ります。

初期プログラム・ロード (IPL) の実行時に、該当するイベント・ログ情報を持つ *PCR Extend* 操作が作成されます。並行ファームウェア更新に関する *PCR Extend* 操作も作成されます。ログ・ファイルには、コード測定の結果、構成、およびプラットフォームの履歴が含まれます。

最初の (コールド) IPL の実行時の現在の見積もりは、単一ノード・システムではノードごとに 50 個のイベント・レコード、4 ノード・システムではノードごとに 200 個のイベント・レコード (イベント・レコード当たり 128 B 換算で、IPL ごとにノード当たり 25 KB) です。

TPM イベント・ログ情報は、リソース・ダンプによって取得することができます。イベント・ログ・ファイルは、物理プラットフォームに関連付けられているため、論理区画と一緒には移行されません。したがって、物理 TPM (pTPM) の TPM 履歴は、論理区画の TPM 履歴と同じではない場合があります。

最初の (コールド) IPL および後続の (ウォーム) IPL の実行時にノード TPM を必要としない TPM 構成設定では、イベント・ログ・ファイルは不要です。ただし、「**TPM 必須 (TPM Required)**」オプションが設定されている場合は、*PCR Extend* 操作および関連するイベント・ログ・ファイルを保持する必要があります。

セキュア・ブートでのシグニチャーおよび鍵

セキュリティー設計では、非対称鍵が使用され、ハードウェア公開鍵のハッシュは Serial Electrically Erasable Programmable ROM (SEEPROM) に保管されます。コード・コンテナー内のファームウェア・コード・イメージのシグニチャーの検証には、SEEPROM からの検証コードとハードウェア公開鍵および追加のソフトウェア公開鍵が使用されます。コア・プロセッサー上で実行する必要がある各ファームウェア・イメージが、必要なセキュリティー情報を含む接頭部ヘッダーとコード・イメージから構成されるコード・コンテナーとして、システム・メモリーにロードされます。コンテナー検証プロセスにより、コードの保全性 (コードが変更されずに保持される) とコード認証 (適切な機関によって署名されている) が確保されます。

コード署名の秘密鍵は、制限されたアクセスと完全な監査制御を備えたファイアウォールによって保護されたセキュア・ハードウェア (例えば、IBM 4767 暗号化コプロセッサー) に保管されます。

システム・ソフトウェアのリモート構成証明

Trusted Platform Module (TPM) により、稼働中のシステムでのコード・スタックのリモート構成証明が可能になります。トラスト・ファームウェアのチェーンは、ロードされたファームウェアのハッシュを記録し、その記録をセキュア・ブート TPM のネットワークに保管します。ネットワークは、POWER9 プロセッサー・ベースのプラットフォーム上のマスター・プロセッサーごとに 1 つの物理 TPM を持つことができます。構成証明は、Trusted Computing Group (TCG) 2.0 準拠のトラステッド・ブートをサポートします。識別された TPM インフラストラクチャーは、それ以降の構成証明スタックをサポートします。

物理構成証明インターフェースを使用することで、信頼できるサード・パーティー・クライアントが、ターゲット PowerVM システムのトラステッド・ブート状態に関する情報を取得できるようになります。このプロセスではシステムの物理 TPM を使用します。これは、TCG 2.0 準拠のデバイスです。これらの TPM は、システム・ファームウェアがブート・プロセス中の測定を拡張するために使用します。

特記事項

本書は米国が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。 実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒*103-8510*
東京都中央区日本橋箱崎町*19*番*21*号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任は適用されないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。 IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述は、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。 記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、類似する個人や企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。 お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。サンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).
このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。
© Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

IBM Power Systems サーバーのアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術コンテンツを快適に使用できるようにサポートします。

概説

IBM Power Systems サーバーには、次の主なアクセシビリティー機能が組み込まれています。

- キーボードのみによる操作
- スクリーン・リーダーを使用する操作

IBM Power Systems サーバーでは、最新の W3C 標準 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) が US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) および Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) に準拠するように使用されています。アクセシビリティー機能を利用するためには、最新リリースのスクリーン・リーダーに加えて、IBM Power Systems サーバーでサポートされている最新の Web ブラウザーを使用してください。

IBM Knowledge Center に用意されている IBM Power Systems サーバーのオンライン製品資料は、アクセシビリティーに対応しています。IBM Knowledge Center のアクセシビリティー機能は、IBM Knowledge Center のヘルプの『アクセシビリティー』セクション (www.ibm.com/support/knowledgecenter/help#accessibility) で説明されています。

キーボード・ナビゲーション

この製品では、標準ナビゲーション・キーが使用されています。

インターフェース情報

IBM Power Systems サーバーのユーザー・インターフェースには、1 秒当たり 2 回から 55 回明滅するコンテンツはありません。

IBM Power Systems サーバーの Web ユーザー・インターフェースは、コンテンツの適切なレンダリング、および使用可能なエクスペリエンスの提供を、カスケード・スタイル・シートに依存しています。アプリケーションは、視覚障害者が、ハイコントラスト・モードを含め、システム表示形式の設定を使用するために同等の仕組みを提供します。フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

IBM Power Systems サーバーの Web ユーザー・インターフェースには、アプリケーションの機能領域に迅速にナビゲートできる WAI-ARIA ナビゲーション・ランドマークが組み込まれています。

ベンダー・ソフトウェア

IBM Power Systems サーバーには、IBM の使用許諾契約書の適用外である特定のベンダー・ソフトウェアが組み込まれています。IBM では、それら製品のアクセシビリティー機能については、何ら保証責任を負いません。ベンダーの製品に関するアクセシビリティー情報については、該当のベンダーにお問い合わせください。

関連したアクセシビリティー情報

標準の IBM ヘルプ・デスクおよびサポートの各 Web サイトに加え、IBM では、聴覚障害を持つユーザーまたは聴覚機能が低下しているユーザーが販売サービスやサポート・サービスにアクセスするのに使用できる TTY 電話サービスを用意しています。

TTY サービス
800-IBM-3383 (800-426-3383)
(北アメリカ内)

アクセシビリティーに対する IBM の取り組みについて詳しくは、IBM アクセシビリティー (www.ibm.com/able) を参照してください。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie をはじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらのCookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

プログラミング・インターフェース情報

この「PowerVM におけるセキュア・ブート」資料は、IBM AIX® バージョン 7.2、IBM AIX バージョン 7.1、IBM AIX バージョン 6.1、IBM i 7.3、および IBM Virtual I/O Server バージョン 3.1.0.0 のサービスを取得するプログラムをお客様が作成できるようにするためのプログラミング・インターフェースについて記述しています。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corp. の商標です。 他の製品名およびサービス名は、IBM または各社の商標です。 現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml の「Copyright and trademark information」をご覧ください。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

適用可能性: これらの条件は、IBM Web サイトのすべてのご利用条件に追加されるものです。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。 ただし、IBM の明示的な承諾を得ずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾を得ずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示したりすることはできません。

権利: ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。 これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21