ザイリンクス Zynq-7000 All Programmable SoC での ARM TrustZone アーキテクチャのプログラミング

ユーザー ガイド

UG1019 (v1.0) 2014 年 5 月 6 日

XILINX®

本資料は英語版 (v1.0) を翻訳したもので、内容に相違が生じる場合には原文を優先します。
資料によっては英語版の更新に対応していないものがあります。
日本語版は参考用としてご使用の上、最新情報につきましては、必ず最新英語版をご参照ください。

この資料に関するフィードバックおよびリンクなどの問題につきましては、jpn_trans_feedback@xilinx.com までお知らせください。いただきましたご意見を参考に早急に対応させていただきます。なお、このメール アドレスへのお問い合わせは受け付けておりません。あらかじめご了承ください。

改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2014 年 5 月 6 日	1.0	初版

目次

ザイリンクス Zynq-7000 All Programmable SoC での ARM TrustZone アーキテクチャのプログラム

ARM TrustZone アーキテクチャの概要

ARM TrustZone® アーキテクチャは、システム オン チップ (SoC) 全体からハードウェア サブセットを分離 (区分け) するソリューションを提供します。

セキュアまたは非セキュア ハードウェアとしての動作を可能とするために、このアーキテクチャが定義する対象は、プロセッサ、ペリフェラル、メモリ アドレス、さらに L2 キャッシュの領域に及びます。

ARM TrustZone テクノロジを採用する SoC では、わずか数クロック サイクルの遅延で、セキュア ソフトウェアが SoC 全体を使用できるようにしたり、通常のソフトウェアが SoC のサブセットを使用できるようにしたりする、動的な切り替えが可能です (図 1 参照)。

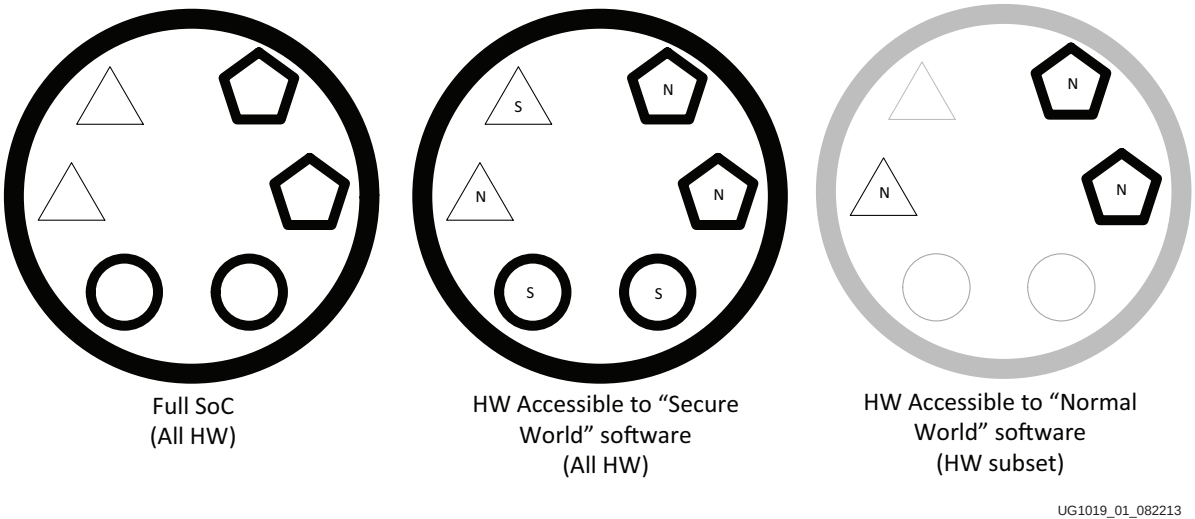

図 1 : ARM TrustZone テクノロジ

通常領域

TrustZone が構築し、管理する「通常領域」(非セキュア領域) は、通常 SoC 内に固定的に定義されたハードウェア サブセットです。TrustZone は、非セキュアなプロセッサまたはマスターが非セキュア (NS) デバイスにのみアクセスし、非セキュア割り込みのみを受け付けるようにします。通常領域のハードウェア サブセットとして、UART、イーサネット、USB インターフェイスなどがありますが、CAN コントローラーのアクセスは含まれません。CAN はむしろセキュア領域専用に使用されます。この領域では、通常領域のソフトウェア スタックに関係なく、CAN トラフィックの管理という目的のためだけに独立した RTOS またはアプリケーションが動作します。

通常領域で動作するソフトウェアは、安全性およびセキュリティ面で不備があると考えられます。つまり、この通常領域のソフトウェアには、機密性の高い情報または機能を暴露する可能性のある、バグ、エクスプロイト、ハッキング、欠陥、不正が含まれているとされます。このような背景で、機密性の高いデータ ストレージや機能を管理する隣接した処理領域 (セキュア領域) を、不備のある通常領域のソフトウェアから分離できる TrustZone 機能の有用性が高くなります。

セキュア領域

通常領域のソフトウェアがハードウェア サブセット上で動作するのとは異なり、セキュア領域のソフトウェアは、Zynq®-7000 All Programmable SoC (AP SoC) の全ハードウェアにアクセスできます。したがって、セキュアなソフトウェアを実行する観点からは、システムが TrustZone のないプロセッサ上で動作している場合と、ほとんど変わりません。これは、セキュアなソフトウェアが、セキュアおよび通常領域の両方に関連するすべてのリソースにアクセスできることを意味します。

信頼できるソフトウェアとは、セキュア領域内で動作するソフトウェアを指す言葉です。

ARM TrustZone アーキテクチャは、通常領域のソフトウェアがセキュア領域のリソースにアクセスするのを防ぐことで、システム全体のセキュリティを向上させます。TrustZone は、通常領域のソフトウェアによるセキュア領域への無用のアクセスを防止しますが、セキュア領域内で動作するソフトウェアの安全性やセキュリティの向上にはほとんど効果がないことにも注意が必要です。したがって、ソフトウェアが信頼できるかどうかは通常、徹底した開発プロセス、テスト、認証を実施したうえで開発者が判断します。

信頼できるシステムを構築できるのは、ソフトウェアにエラーやエクスプロイトがないと判明している (信頼できるソフトウェアとして検証されている) 場合のみであり、コードが小規模なほど安全性やセキュリティの要件に対する認証が容易になることから、通常、信頼できるソフトウェアは最小限の機能とデバイス インターフェイスしか備えていません。たとえば、信頼できるソフトウェアが TCP/IP スタックまたは USB デバイスを備えていなければ、TCP/IP や USB を動作させるデバイス ドライバーや悪用される可能性のあるソフトウェアも存在しないため、これらを介した攻撃に対するセキュリティが確保されます。ARM がセキュア領域内で動作可能としているアプリケーションを確認するには、ARM TrustZone ウェブサイトの「システム アーキテクチャ」タブに記載されているブロック図を参照してください。

信頼できるソフトウェアは根本的な完全性を備えるという前提から、ARM TrustZone にはセキュア領域内で汎用オペレーティング システムをサポートしようという意図はありません。標準オペレーティング システム (10 万～ 数百万行のコード) が信頼できるソフトウェアとして動作することを認証するのはきわめて困難だからです。

信頼できる実行環境

信頼できる実行環境 (TEE : Trusted Execution Environment) とは、セキュア領域内で動作するソフトウェア スタックと、セキュア ソフトウェアが通常領域のソフトウェアと対話できるようにする通信を指します。TEE ソフトウェアは通常、小規模なオペレーティング システムとそのアプリケーション、セキュア ソフトウェアとより大きなユーザー中心のソフトウェア (Android、Linux など) との通信を可能にする API から構成されます。

現在、Zynq デバイスは 2 つのオープン ソース TEE によってサポートされています。1 つはオープン ソース ライセンス供与の RTOS/GPOS 環境とも呼ばれる、名古屋大学の TOPPERS-SafeG です。もう 1 つは、POSIX と GlobalPlatform API をサポートする Sierraware 社の Sierra TEE です。これらの TEE は GPL および商用ライセンス許諾を得て入手できます。

GlobalPlatform は、エンベデッド アプリケーションのセキュアで相互運用性のある展開と管理を促進するための仕様を策定する団体で、複数の業界の企業が参加してます。これらの仕様の 1 つは、「典型的な RTOS」といわれる API と機能、並びに追加機能や TEE 使用事例に適した API を提供する TEE を定義します。

ザイリンクスの TrustZone 関連資料

TrustZone はシステムに関連するトピックであるため、ソリューションを完全に理解するには各種資料を参考にする必要があります。この入門ガイドに加えて、次のリソースを参照することを推奨します。

『Zynq-7000 All Programmable SoC における TrustZone テクノロジのサポート』(WP429)

この資料は、Zynq-7000 での TrustZone サポートをプログラマブル ロジック内の IP コアに拡張する方法について解説しています。

WP429 の守秘条件はこのガイドと同じであり、ウェブサイトからすぐに入手できます。これらの資料の入手方法の詳細は、http://japan.xilinx.com/support/answers/54835.htm を参照してください。

『Zynq-7000 All Programmable SoC テクニカル リファレンス マニュアル』

このユーザー ガイド (UG1019) は、Zynq-7000 AP SoC ファミリの TrustZone 関連レジスタの詳細と使用法を示し、『Zynq-7000 All Programmable SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] の主要技術情報を補足するものです。

サードパーティ IP の資料

Zynq-7000 デバイス ファミリには、ARM、ザイリンクス、サードパーティが提供する IP コアが多数含まれ、そのほとんどが TrustZone アーキテクチャをサポートしています。このユーザー ガイドでは、サードパーティ提供の情報が明らかに必要となることはありませんが、ザイリンクスのウェブサイト (http://japan.xilinx.com/products/zynq-7000/third-party-documentation.htm) にリンクが掲載されている資料は参考になる場合があります。

Zynq-7000 All Programmable SoC 内の ARM TrustZone アーキテクチャ

ARM アーキテクチャは、アプリケーション レベルで異なる保護レベルを提供する、複数の動作モード (スーパバイザー、システム、ユーザーの各モード) をサポートします。TrustZone テクノロジ対応のアーキテクチャにより、アプリケーションを実行し、その内容を保護するセキュアな環境の構築が容易になります。ARM CPU プロセッサおよび多くのペリフェラルに組み込まれた TrustZone は、キー、プライベート データ、暗号化された情報を処理すると共に、これらの機密情報が信頼できないプログラムまたはユーザーに漏えいすることを防ぐ、セキュアなシステムを実現できます。表 1 に、TrustZone セキュリティをまとめます。

表 1 : Zynq-7000 AP AP SoC の TrustZone セキュリティのまとめ

PS7 エンティティ	TrustZone セキュリティ	備考
ARM CPU システム		
ARM A9 コア	両方	
L1 キャッシュ コントローラー	セキュア	
L1 キャッシュ	両方	
メモリ管理装置 (MMU)	セキュア	
SCU	セキュア	
L2 キャッシュ コントローラー	セキュア	
SLCR	セキュア	
トリプル タイマー カウンター 0	セキュア	
トリプル タイマー カウンター 1	設定可能	SLCR による設定
ウォッチドッグ	セキュア	
SoC CoreSight デバッグ	セキュア	
OCM	セキュアおよび非セキュア	256KB の RAM は 4KB のセキュア ドメインに分割可能
DDR メモリ	セキュアおよび非セキュア	64MB のセキュア ドメインに分割。AxPROTECT 信号は通過させる
IOU デバイス	設定可能	I2C、GPIO、SPI、イーサネット、SDIO、CAN、USB、UART、Quad-SPI、NOR

Zynq APU 内の TrustZone サポート

システムがパワーオン リセットから安定した状態へ遷移する際に、セキュアおよび非セキュア アプリケーションが同時に動作する場合、システムは図 2 に示す順でブートします。

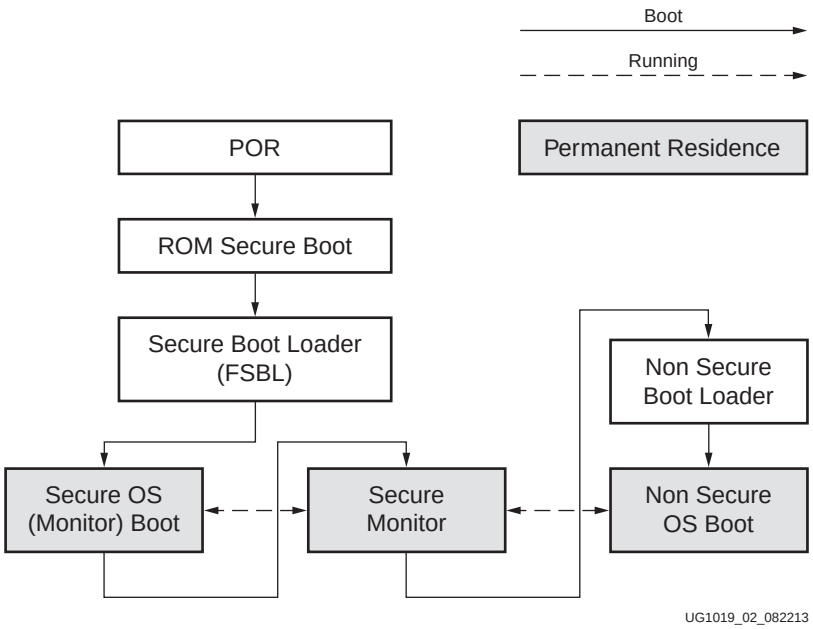

図 2 : TrustZone のブート シーケンス

図 2 では、Zynq のセキュア ブート シーケンスの使用を前提としています。ただし、これは TrustZone セキュア ブートの必須要件ではありません。この図の実線は、ブート フローを示し、点線はシステムが動作状態になった後の処理の遷移を示しています。網掛けのブロックは、システムのブート後も動作を続けるソフトウェアの機能ブロックです。TrustZone のブート フローでは、最初にセキュア OS がブートし、セキュアおよび非セキュア OS 間の確実なゲートウェイとして機能するセキュア モニターを起動します。起動したセキュア モニターは、非セキュア ブート ローダーを起動でき、次にこの非セキュア ブート ローダーが非セキュア OS を起動します。非セキュア OS の起動前に、セキュア OS は、非セキュア OS からセキュア モニターへ強制的に遷移させる、一連のイベントを定義します。これらのイベントには、SMC 命令、IRQ、FIQ、外部データ アボート、外部プリフェッチ アボート例外などがあります。

CPU セキュリティの遷移

セキュア モニター コール (SMC) は、特権モードでのみ使用可能なセキュア モニター例外を発生します。この命令をユーザー モードで実行しようとすると、未定義命令の例外が発生します。

SMC によるモニター モードへの移行以外にも、セキュア モニターを介してセキュア領域と非セキュア領域を切り替える方法はいくつかあります。この場合、セキュア モニターはこれら 2 つの領域間のゲート キーパーの役割を果たします。モニター モードへ遷移させる方法は次のとおりです。

- 外部アボート ハンドラー
- FIQ ハンドラー
- IRQ ハンドラー

詳細は、『Zynq-7000 All Programmable SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] を参照してください。

セキュア モニター モードの場合、プロセッサは SCR.NS ビットの設定にかかわらず、常にセキュア状態です。

通常領域ソフトウェアによる Cortex-A9 TrustZone 違反が原因となり、セキュア領域で誤った非同期アボートが発生することがあります。たとえば、SCR.NS = 1 かつ CPSR.A = 1 (非同期アボート ビットのマスク) の状態で、セキュア ハイパーバイザーが何らかのコードを実行します。この非セキュア コードはセキュア専用とされたメモリに対して読み書きを実行しようとするため、AXI DECERR を受信します。この時点では、CPSR.A = 1 と設定されて例外がマスクされているため、例外は発生しません。セキュア モードに再度遷移すると、ハイパーバイザーがほかのコードに切り換わり、DSB/ISB を実行して CPSR.A を 0 にクリアします。この場合、Cortex-A9 プロセッサは保留中の非同期外部アボートをまだ記憶しているため、CPSR.A = 0 になった時点で例外を発生します。さらに、非セキュア コードがセキュア メモリにマルチワードを格納したことにより、L1 キャッシュのデータが変更された可能性があります。このデータがやがてキャストアウトされると、セキュア モードで非同期外部アボートが発生する可能性があります。

以上のような Cortex-A9 の動作に対処するために、通常領域からセキュア領域に切り替える前に、ソフトウェアによってデータ アボート ステータス レジスタ (『ARM アーキテクチャ リファレンス マニュアル』[参照 2] 参照) の状態を確認します。

保留中のデータ アボートがなければ、切り替えを実行できます。

データ アボートが保留中の場合、次の実行を推奨します。

1. CPSR.A を有効にする (0 に設定する) - セキュア領域に遷移する前に、保留中のアボートが非セキュア領域でただちに発生します。
2. 通常領域では CPSR.A を無視して、セキュア領域ソフトウェアで処理する - この方法では、通常領域のソフトウェアがセキュア アドレス領域へのアクセスを試みたことを、セキュア ソフトウェアが確実に把握できます。

CPSR.A はデフォルトでは通常領域 (非セキュア) ソフトウェアからアクセス可能であり、ユーザー固有の使用事例やシステム デザインは、CPSR.A の処理方法しか決定しません。このレジスタをセキュア レジスタに指定するには、『ARM アーキテクチャ リファレンス マニュアル』[参照 2] のセクション B1.8.7 を参照してください。書き込み許可を無効にすることで非セキュア ソフトウェアによる CPSR.A の使用を禁止する、SCR.AW の使用方法を解説しています。

CP15 レジスタのアクセス制御

セキュアおよび非セキュア機能をサポートするために、Zynq-7000 AP SoC には CP15 の下にバンク化されたレジスタのグループがあります。これは、1 つのレジスタがセキュアおよび非セキュア モード用に 2 つの物理的コピーを持つことを意味します。物理レジスタは、システムがセキュア モニター モードでない場合、SCR.NS ビットに基づいて自動的に選択されます。セキュア モニター モードの場合は、常にセキュアなバージョンが選択されます。表 2 に CP15 レジスタの一部を示します (レジスタの全リストは『ARM アーキテクチャ リファレンス マニュアル』[参照 2] を参照)。

表 2 : 代表的な CP15 レジスタ

CP15 レジスタ	バンク化されたレジスタ	許可されるアクセス
c0	CSSELR、キャッシュ サイズ選択レジスタ	特権モードの場合のみ読み出し/書き込み
c1	SCTLR、システム制御レジスタ	特権モードの場合のみ読み出し/書き込み
	ACTLR、補助制御レジスタ	特権モードの場合のみ読み出し/書き込み
c2	TTBR0、変換テーブル ベース 0	特権モードの場合のみ読み出し/書き込み
	TTBR0、変換テーブル ベース 1	特権モードの場合のみ読み出し/書き込み
	TTBCR、変換テーブル ベース制御	特権モードの場合のみ読み出し/書き込み
c3	DACR、ドメイン アクセス制御レジスタ	特権モードの場合のみ読み出し/書き込み
c5	DFSR、データ フォルト ステータス レジスタ	特権モードの場合のみ読み出し/書き込み
	IFSR、命令フォルト ステータス レジスタ	特権モードの場合のみ読み出し/書き込み
	ADFSR、補助データ フォルト ステータス レジスタ	特権モードの場合のみ読み出し/書き込み
	AIFSR、補助命令フォルト ステータス レジスタ	特権モードの場合のみ読み出し/書き込み

表 2 : 代表的な CP15 レジスタ (続き)

CP15 レジスタ	バンク化されたレジスタ	許可されるアクセス
c6	DFAR、データ フォルト アドレス レジスタ	特権モードの場合のみ読み出し/書き込み
	IFAR、命令フォルト アドレス レジスタ	特権モードの場合のみ読み出し/書き込み
c7	PAR、物理アドレス レジスタ (VA から PA への変換)	特権モードの場合のみ読み出し/書き込み
c10	PRRR、プライマリ領域リマップ レジスタ	特権モードの場合のみ読み出し/書き込み
	NMRR、通常メモリ リマップ レジスタ	特権モードの場合のみ読み出し/書き込み
c12	VBAR、ベクター ベース アドレス レジスタ	特権モードの場合のみ読み出し/書き込み

表 3 に、その他の CP15 制御レジスタと、セキュアおよび非セキュア状態のアクセス制御を示します。

表 3 : その他の CP15 制御レジスタとセキュア/非セキュア状態のアクセス制御

CP15 レジスタ	バンク化されたレジスタ	許可されるアクセス
c1	NSACR、非セキュア アクセス制御レジスタ	特権モードの場合のみ読み出し/書き込み 非セキュア特権モードの場合は読み出し専用
	SCR、セキュア コンフィギュレーション レジスタ	特権モードの場合のみ読み出し/書き込み
	SDER、セキュア デバッグ イネーブル レジスタ	特権モードの場合のみ読み出し/書き込み
c12	MVBAR、モニター ベクター ベース アドレス レジスタ	特権モードの場合のみ読み出し/書き込み

MMU のセキュリティ

Cortex-A9 の MMU は、アドレス変換に加えて、アクセス許可チェックを実行する TrustZone 機能によって強化されています。セキュアおよび非セキュアの各領域で、メイン メモリに格納された 1 組の 2 レベル ページ テーブルによって、命令側およびデータ側の変換ルックアサイド バッファー (TLB) の内容が制御されます。仮想アドレスに関連して計算された物理アドレスは、セキュアおよび非セキュアなエントリの共存を可能にする非セキュア テーブル識別子 (NSTID) と共に TLB に格納されます。TLB は CP15 制御レジスタ c1 内の 1 ビットで、セキュアおよび非セキュア領域のそれぞれで有効化され、ソフトウェアに対して 1 アドレスの変換機能と保護機構を提供します。

セキュアおよび非セキュア領域間の遷移が発生したときに、TLB と分岐先アクセス制御 (BTAC) の状態がどのように処理されるかを説明します。

- セキュア状態から実行された分岐予測全無効化 (BPIALL : Branch Predictor Invalidate All) は、非セキュア状態の BTAC エントリを無効化する場合としない場合があります。
- セキュア状態から実行された TLBIALL は、非セキュア状態からの BTAC エントリを無効化しません。
- セキュア状態から CONTEXTIDR に書き込むと、SCR.NS = 1 でも非セキュア状態の BTAC エントリは無効化されます。

すべてのコンテキスト スイッチは CONTEXTIDR への書き込みを実行し、非セキュア状態の BTAC エントリを無効化するため、セキュア状態からの BPIALL は非セキュア BTAC エントリに影響を与えず問題になりません。

L-1 キャッシュのセキュリティ

キャッシュの各ラインにはセキュアまたは非セキュア データが含まれます。データ セキュリティに違反するアクセスはキャッシュ ミスを発生させます。ミスが発生した場合、次に外部メモリへアクセスし、NS 属性がアクセス許可に一致しなければアボートが返されます。

セキュリティ例外制御

例外が発生した場合、プロセッサの実行はその例外のタイプに対応したアドレスに強制的に移動します。これらのアドレスは例外ベクターと呼ばれます。デフォルトの例外ベクターはワード境界に位置合わせされた 8 連続のメモリ アドレスであり、次の例外ベース アドレスから始まります。

Zynq-7000 AP SoC デバイスには、3 つの例外ベース アドレスがあります。

1. 非セキュア例外ベース アドレスは、非セキュア状態で処理されるすべての例外に適用されます。
2. セキュア例外ベース アドレスは、セキュア状態で処理されるすべての例外に適用されます。
3. モニター例外ベース アドレスは、モニター モードで処理されるすべての例外に適用されます。

CPU デバッグにおける TrustZone アクセス制御

CPU のデバッグ ステータスは 4 つの制御信号、DBGEN、NIDEN、SPIDEN、SPNIDEN で制御します。これら 4 つの制御信号は、デバイス コンフィギュレーション インターフェイス モジュール内のセキュアで保護されたレジスタに属します。表 4 にサポートされる最も重要なモードを示します。

表 4 : デバッグ ステータス制御

モード	DBGEN	NIDEN	SPIDEN	SPNIDEN	コメント
デバッグなし	0	0	0	0	CPU デバッグを一切実行しません。
非セキュア 非侵襲性デバッグ	1	1	0	0	トレース、パフォーマンス モニターなどの非侵襲性デバッグを非セキュア モードで実行することを許可します。
非セキュア 侵襲性デバッグ	1	1	0	0	プロセッサ停止などの侵襲性デバッグを非セキュア モードで実行することを許可します。
セキュア 非侵襲性デバッグ	1	1	0	1	セキュア状態で CPU のトレースとプロファイルを許可します。
セキュア 侵襲性デバッグ	1	1	1	1	セキュア モードの侵襲性デバッグを許可します。

SCU レジスタ アクセス制御

SCU 非セキュア アクセス制御レジスタ (SNACR) は、SCU 内の各主要コンポーネントに対するグローバル非セキュア アクセスを制御します。割り込みコントローラーの分配器制御レジスタ (ICDDCR) は、セキュアおよび非セキュア アクセスを制御するためのバンク化されたレジスタです。

L2 キャッシュ内の TrustZone サポート

キャッシュ コントローラーは、L2 キャッシュおよび内部バッファーに格納されるすべてのデータに NS ビットを付加します。非セキュアなトランザクションは、セキュア データにアクセスできません。したがって、コントローラーはセキュアおよび非セキュア データを 2 つの異なるメモリ空間に属するものとして扱います。コントローラーは、L2 キャッシュ内のセキュア データへの非セキュアなアクセスをキャッシュ ミスと見なします。読み出し転送の場合、キャッシュ コントローラーは外部メモリにライン フィル コマンドを送信し、外部メモリからのセキュリティ エラーをすべてプロセッサに伝搬し、L2 内にラインを割り当てません。

次に、L2 内での TrustZone サポートに関する注意事項を示します。

- L2 制御レジスタに対する、L2 キャッシュを有効化または無効化するための書き込みは、セキュア タグの付いているアクセスによってのみ可能です。
- 補助制御レジスタに対する書き込みは、セキュア タグの付いているアクセスによってのみ可能です。補助制御レジスタの Bit[26] は NS ロックダウンの有効化に使用します。このビットを用いて、非セキュア アクセスにロックダウン レジスタの変更を許可するかどうかを設定します。
- 非セキュアなメンテナンス動作は、セキュア データをクリーンまたは無効化しません。
- Zynq L2 キャッシュ コントローラーはデバッグ制御レジスタにアクセスする必要がありません。ただし、NS モードからこのレジスタにアクセスしようとすると、DECERR が発生します。

DDR メモリに対する Zynq TrustZone サポート

Zynq-7000 SoC の TrustZone 機能は、DDR メモリを増分 64MB の独立したセキュアまたは非セキュア領域として設定できます。この設定は、システム レベル制御レジスタによって提供されます。

- ある特定ビットが `0` の場合、その特定メモリ セグメントがセキュア メモリ領域であることを示します。
- ある特定ビットが `1` の場合、その特定メモリ セグメントが非セキュア メモリ領域であることを示します。

セキュア領域に非セキュア アクセスを実行すると、マスターに DECERR 応答が返されます。セキュア領域への書き込みの場合、コントローラーに送信される前に書き込みデータがマスクされ、DRAM への実際の書き込みは発生しません。非セキュア アクセスによってセキュア領域を読み出そうとすると、すべてゼロが返されます。

Zynq-7000 All Programmable SoC 内の TrustZone コンフィギュレーション レジスタ

このセクションでは、Zynq-7000 AP SoC に含まれるペリフェラルを TrustZone 対応のシステム デザインにインスタンシエートするための設定方法を説明します。

ここでいうセキュアなハードウェアとは、セキュア領域でのみ認識されるハードウェアを指します。非セキュアのマークが付いたハードウェアは、通常領域とセキュア領域の両方で認識されます。

モジュールの概要

Zynq-7000 AP SoC には 22 個のレジスタを含む 1 つの TrustZone モジュールがあります。

表 5 : モジュールの概要

モジュール名	モジュール タイプ	ベース アドレス	バージョン	説明
trustzone	TrustZone	`E0200000`、`F8000000`	1.0.0	TrustZone の制御レジスタ

モジュール TrustZone

モジュール名	trustzone
ベース アドレス	E0200000 および F8000000
説明	TrustZone の制御レジスタ
バージョン	1.0.0
ドキュメント バージョン	1.0
ベンダー情報	ザイリンクス

レジスタ アクセス凡例

アクセス タイプ	説明
CLRONRD	読み出し可能。読み出し時に値をクリア。
CLRONWR	読み出し可能。書き込み時に値をクリア。
NSNSRO	非セキュア アクセス時にスレッドが非セキュアな場合、読み出し専用。
NSNSRW	非セキュア アクセス時にスレッドが非セキュアな場合、読み出し/書き込み。
NSNSWO	非セキュア アクセス時にスレッドが非セキュアな場合、書き込み専用。
NSSRAZ	非セキュア アクセス時にスレッドが非セキュアな場合、0 として読み出し。
RAZ	0 として読み出し。
RO	読み出し専用。
RS	w : 影響なし。r : 全ビットをセット。
RUD	未定義読み出し。
RW	通常読み出し/書き込み。
RWSO	読み出し/書き込み。セットのみ。
SRO	セキュア アクセス時、読み出し専用。
SRW	セキュア アクセス時、読み出し/書き込み。
SWO	セキュア アクセス時、書き込み専用。
W0C	w : 1/0 の場合、一致ビットに影響なし/一致ビットをクリア。r : 影響なし。
W0CRS	w : 1/0 の場合、一致ビットに影響なし/一致ビットをクリア。r : 全ビットをセット。
W0S	w : 1/0 の場合、一致ビットに影響なし/一致ビットをセット。r : 影響なし。
W0SRC	w : 1/0 の場合、一致ビットに影響なし/一致ビットをセット。r : 全ビットをクリア。
W0T	w : 1/0 の場合、一致ビットに影響なし/一致ビットをトグル。r : 影響なし。
W1	w : ハード リセット後最初の書き込みは指定どおり、その他の書き込みは影響なし。r : 影響なし。
W1CRS	w : 1/0 の場合、一致ビットをクリア/一致ビットに影響なし。r : 全ビットをセット。
W1SRC	w : 1/0 の場合、一致ビットをセット/一致ビットに影響なし。r : 全ビットをクリア。
W1T	w : 1/0 の場合、一致ビットをトグル/一致ビットに影響なし。r : 影響なし。
WAZ	0 として書き込み。
WCRS	w : 全ビットをクリア。r : 全ビットをセット

アクセス タイプ	説明
WO	書き込み専用。
WO1	w : ハード リセット後最初の書き込みは指定どおり、その他の書き込みは影響なし。r : エラー。
WOC	w : 全ビットをクリア。r : エラー。
WOS	w : 全ビットをセット。r : エラー。
WRC	w : 指定どおり。r : 全ビットをクリア。
WRS	w : 指定どおり。r : 全ビットをセット。
WS	w : 全ビットをセット。r : 影響なし。
WSRC	w : 全ビットをセット。r : 全ビットをクリア。
WTC	読み出し可能。クリアするには 1 を書き込み。
Z	0 としてアクセス (読み出しまたは書き込み)。

レジスタのまとめ

レジスタ名	アドレス	幅	タイプ	リセット値	説明
security2_sdio0	0xE0200008	1	WO	0x00000000	SDIO0 スレーブ セキュリティ設定
security3_sdio1	0xE020000C	1	WO	0x00000000	SDIO1 スレーブ セキュリティ設定
security4_qspi	0xE0200010	1	WO	0x00000000	QSPI スレーブ セキュリティ設定
security6_apb_slaves	0xE0200018	15	WO	0x00000000	APB スレーブ セキュリティ設定
security7_smc	0xE020001C	1	WO	0x00000000	SMC スレーブ セキュリティ設定
DMAC_RST_CTRL	0xF800020C	32	RW	0x00000000	DMA コントローラー SW リセット制御
TZ_OCM_RAM0	0xF8000400	32	RW	0x00000000	OCM RAM TrustZone コンフィギュレーション 0
TZ_OCM_RAM1	0xF8000404	32	RW	0x00000000	OCM RAM TrustZone コンフィギュレーション 1
TZ_OCM	0xF8000408	32	RW	0x00000000	OCM ROM TrustZone コンフィギュレーション
TZ_DDR_RAM	0xF8000430	32	RW	0x00000000	DDR RAM TrustZone コンフィギュレーション
TZ_DMA_NS	0xF8000440	32	RW	0x00000000	DMAC TrustZone コンフィギュレーション
TZ_DMA_IRQ_NS	0xF8000444	32	RW	0x00000000	DMAC TrustZone 割り込みコンフィギュレーション
TZ_DMA_PERIPH_NS	0xF8000448	32	RW	0x00000000	DMAC TrustZone ペリフェラル コンフィギュレーション
TZ_GEM	0xF8000450	32	RW	0x00000000	イーサネット TrustZone コンフィギュレーション
TZ_SDIO	0xF8000454	32	RW	0x00000000	SDIO TrustZone コンフィギュレーション
TZ_USB	0xF8000458	32	RW	0x00000000	USB TrustZone コンフィギュレーション
TZ_FPGA_M	0xF8000484	32	RW	0x00000000	FPGA マスター ポート TrustZone ディスエーブル
TZ_FPGA_AFI	0xF8000488	32	RW	0x00000000	FPGA AFI AXI ポート TrustZone ディスエーブル
security_fssw_s0	0xF890001C	1	WO	0x00000000	M_AXI_GP0 セキュリティ設定
security_fssw_s1	0xF8900020	1	WO	0x00000000	M_AXI_GP1 セキュリティ設定
security_apb	0xF8900028	6	WO	0x00000000	APB ブート セキュア ポート設定

security2_sdio0

レジスタ名	security2_sdio0
相対アドレス	0xE0200008
絶対アドレス	0xE0200008
幅	1 ビット
アクセス タイプ	WO
リセット値	0x00000000
説明	SDIO0 スレーブ セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
	0	WO	0x0	0 : セキュア 1 : 非セキュア

security3_sdio1

レジスタ名	security3_sdio1
相対アドレス	0xE020000C
絶対アドレス	0xE020000C
幅	1 ビット
アクセス タイプ	WO
リセット値	0x00000000
説明	SDIO1 スレーブ セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
	0	WO	0x0	0 : セキュア 1 : 非セキュア

security4_qspi

レジスタ名	security4_qspi
相対アドレス	0xE0200010
絶対アドレス	0xE0200010
幅	1 ビット
アクセス タイプ	WO
リセット値	0x00000000
説明	QSPI スレーブ セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
	0	WO	0x0	0 : セキュア 1 : 非セキュア

この security4_qspi レジスタは、リニア QSPI アドレスへのアクセスがセキュアまたは非セキュアのいずれの機能であるかを定義します。詳細は、『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] の第 12 章を参照してください。

security6_apb_slaves

レジスタ名	security6_apb_slaves
相対アドレス	0xE0200018
絶対アドレス	0xE0200018
幅	15 ビット
アクセス タイプ	WO
リセット値	0x00000000
説明	APB スレーブ セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
usb1_s_apb	14	WO	0x0	0 : セキュア 1 : 非セキュア
usb0_s_apb	13	WO	0x0	0 : セキュア 1 : 非セキュア
gem1_s_apb	12	WO	0x0	0 : セキュア 1 : 非セキュア
gem0_s_apb	11	WO	0x0	0 : セキュア 1 : 非セキュア
smc_s_apb	10	WO	0x0	0 : セキュア 1 : 非セキュア
spi1_s_apb	9	WO	0x0	0 : セキュア 1 : 非セキュア
spi0_s_apb	8	WO	0x0	0 : セキュア 1 : 非セキュア
ua1_s_apb	7	WO	0x0	0 : セキュア 1 : 非セキュア
ua0_s_apb	6	WO	0x0	0 : セキュア 1 : 非セキュア
i2c1_s_apb	5	WO	0x0	0 : セキュア 1 : 非セキュア
i2c0_s_apb	4	WO	0x0	0 : セキュア 1 : 非セキュア
gpio_s_apb	3	WO	0x0	0 : セキュア 1 : 非セキュア
qspi_s_apb	2	WO	0x0	0 : セキュア 1 : 非セキュア
can1_s_apb	1	WO	0x0	0 : セキュア 1 : 非セキュア
can0_s_apb	0	WO	0x0	0 : セキュア 1 : 非セキュア

security7_smc

レジスタ名	security7_smc
相対アドレス	0xE020001C
絶対アドレス	0xE020001C
幅	1 ビット
アクセス タイプ	WO
リセット値	0x00000000
説明	SMC スレーブ セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
	0	WO	0x0	0 : セキュア 1 : 非セキュア

この security7_smc レジスタは、SMC (SRAM または NOR) へのアクセスがセキュアまたは非セキュアのいずれの機能であるかを定義します。詳細は、『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] の第 11 章を参照してください。

DMAC_RST_CTRL

レジスタ名	DMAC_RST_CTRL
相対アドレス	0xF800020C
絶対アドレス	0xF800020C
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	DMA コントローラー SW リセット制御

フィールド名	ビット	タイプ	リセット値	説明
予約	31:1	RW	0x0	予約。書き込みは無視、読み出しデータは 0。
DMAC_RST	0	RW	0x0	DMA コントローラー ソフトウェア リセット信号 • 0 : ディアサート (DMA コントローラーの TrustZone レジスタは読み出し専用) • 1 : アサート (DMA コントローラーの TrustZone レジスタは書き込み可能)

注記 : この DMAC_RST レジスタは常に書き込み可能ですが、DMAC のリセットが解除されるまですべての書き込みは無視されます。したがって、DMAC_RST_CTRL のリセットには、アサート後にディアサートするシーケンスが必要です。

TZ_OCM_RAM0

レジスタ名	TZ_OCM_RAM0
相対アドレス	0xF8000400
絶対アドレス	0xF8000400
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	OCM RAM TrustZone コンフィギュレーション 0

フィールド名	ビット	タイプ	リセット値	説明
TZ_OCM_RAM0	31:0	RW	0x0	各ビットは、4KB ページの TrustZone ステータスを表します。 • 0 : セキュア • 1 : 非セキュア Bit [0] : Page 0 (最初の 4KB) Bit [1] : Page 1 ... Bit [31] : Page 31 (128KB まで)

OCM はセキュアおよび非セキュア動作向けに、実行時に分割できます。OCM にはリセットやクロック状態に基づく厳密な設定要件がないため、このような分割が可能です。新たな TZ 設定に基づいて OCM にアクセスする前に、TZ_OCM_RAM レジスタの内容をリードバックすることを推奨します。

TZ_OCM_RAM1

レジスタ名	TZ_OCM_RAM1
相対アドレス	0xF8000404
絶対アドレス	0xF8000404
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	OCM RAM TrustZone コンフィギュレーション 1

フィールド名	ビット	タイプ	リセット値	説明
TZ_OCM_RAM1	31:0	RW	0x0	各ビットは、4KB ページの TrustZone ステータスを表します。 • 0 : セキュア • 1 : 非セキュア Bit [0] : Page 32 (128KB から開始) Bit [1] : Page 33 ... Bit [31] : Page 63 (256KB まで)

OCM はセキュアおよび非セキュア動作向けに、実行時に簡単に分割できます。OCM にはリセットやクロック状態に基づく厳密な設定要件がないため、このような分割が可能です。新たな TZ 設定に基づいて OCM にアクセスする前に、TZ_OCM_RAM レジスタの内容をリードバックすることを推奨します。

TZ_OCM

レジスタ名	TZ_OCM
相対アドレス	0xF8000408
絶対アドレス	0xF8000408
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	OCM TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
TZ_OCM	31:0	RW	0x0	各ビットは、4KB ページの TrustZone ステータスを表します。 • 0 : セキュア • 1 : 非セキュア Bit [0] : Page 64 (256KB から開始) Bit [1] : Page 65 ... Bit [31] : Page 95 (512KB まで)

TZ_DDR_RAM

レジスタ名	TZ_DDR_RAM
相対アドレス	0xF8000430
絶対アドレス	0xF8000430
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	DDR RAM TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
TZ_DDR_RAM	0	RW	0x0	各ビットは、nMB の位置から始まる 64MB セクション n の TrustZone ステータスを表します。 • 0 : セキュア (リセット値) • 1 : 非セキュア

TZ_DMA_NS

レジスタ名	TZ_DMA_NS
相対アドレス	0xF8000440
絶対アドレス	0xF8000440
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	DMAC TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:1	RW	0x0	0 である必要があります。
DMAC_NS	0	RW	0x0	TZ セキュリティ (DMAC の boot_manager_ns に接続) • 0 : セキュア。DMAC はセキュア状態で動作 • 1 : 非セキュア。DMAC は非セキュア状態で動作

TZ_DMA_IRQ_NS

レジスタ名	TZ_DMA_IRQ_NS
相対アドレス	0xF8000444
絶対アドレス	0xF8000444
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	DMAC TrustZone 割り込みコンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:16	RW	0x0	0 である必要があります。
DMA_IRQ_NS	15:0	RW	0x0	TZ セキュリティ (DMAC の boot_irq_ns に接続) • 0 : セキュア。指定された外部割り込みはセキュア状態で動作 • 1 : 非セキュア。指定された外部割り込みは非セキュア状態で動作

TZ_DMA_PERIPH_NS

レジスタ名	TZ_DMA_PERIPH_NS
相対アドレス	0xF8000448
絶対アドレス	0xF8000448
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	DMAC TrustZone ペリフェラル コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:4	RW	0x0	0 である必要があります。
DMAC_PERIPH_NS	3:0	RW	0x0	TZ セキュリティ (DMAC の boot_periph_ns に接続) • 0 : セキュア。ペリフェラル要求インターフェイスはセキュア状態で動作 • 1 : 非セキュア (リセット値)。ペリフェラル要求インターフェイスは非セキュア状態で動作

TZ_GEM

レジスタ名	TZ_GEM
相対アドレス	0xF8000450
絶対アドレス	0xF8000450
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	イーサネット TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:2	RW	0x0	0 である必要があります。
E1	1	RW	0x0	ギガビット イーサネット MAC 1 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア
E0	0	RW	0x0	ギガビット イーサネット MAC 0 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア

TZ_SDIO

レジスタ名	TZ_SDIO
相対アドレス	0xF8000454
絶対アドレス	0xF8000454
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	SDIO TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:2	RW	0x0	0 である必要があります。
S1	1	RW	0x0	SDIO コントローラー 1 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア
S0	0	RW	0x0	SDIO コントローラー 0 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア

TZ_USB

レジスタ名	TZ_USB
相対アドレス	0xF8000458
絶対アドレス	0xF8000458
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	USB TrustZone コンフィギュレーション

フィールド名	ビット	タイプ	リセット値	説明
予約	31:2	RW	0x0	0 である必要があります。
U1	1	RW	0x0	USB コントローラー 1 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア
U0	0	RW	0x0	USB コントローラー 0 の TrustZone ステータス • 0 : セキュア (リセット値) • 1 : 非セキュア

TZ_FPGA_M

レジスタ名	TZ_FPGA_M
相対アドレス	0xF8000484
絶対アドレス	0xF8000484
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	FPGA マスター ポート TrustZone ディスエーブル

フィールド名	ビット	タイプ	リセット値	説明
予約	31:2	RW	0x0	0 である必要があります。
M1	1	RW	0x0	PL AXI マスター ポート 1 のセキュア ディスエーブル • 0 : マスター ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : マスター ポートは非セキュア アクセスのみ可能
M0	0	RW	0x0	PL AXI マスター ポート 0 のセキュア ディスエーブル • 0 : マスター ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : マスター ポートは非セキュア アクセスのみ可能

TZ_FPGA_AFI

レジスタ名	TZ_FPGA_AFI
相対アドレス	0xF8000488
絶対アドレス	0xF8000488
幅	32 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	FPGA AFI AXI ポート TrustZone ディスエーブル

フィールド名	ビット	タイプ	リセット値	説明
予約	31:4	RW	0x0	0 である必要があります。
P3	3	RW	0x0	PL AXI_HP ポート 3 のセキュア ディスエーブル • 0 : ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : ポートは非セキュア アクセスのみ可能
P2	2	RW	0x0	PL AXI_HP ポート 2 のセキュア ディスエーブル • 0 : ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : ポートは非セキュア アクセスのみ可能

フィールド名	ビット	タイプ	リセット値	説明
P1	1	RW	0x0	PL AXI_HP ポート 1 のセキュア ディスエーブル • 0 : ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : ポートは非セキュア アクセスのみ可能
P0	0	RW	0x0	PL AXI_HP ポート 0 のセキュア ディスエーブル • 0 : ポートはセキュアおよび非セキュア アクセスが可能 (リセット値) • 1 : ポートは非セキュア アクセスのみ可能

security_fssw_s0

レジスタ名	security_fssw_s0
相対アドレス	0xF890001C
絶対アドレス	0xF890001C
幅	1 ビット
アクセス タイプ	RO
リセット値	0x00000000
説明	M_AXI_GP0 セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
fssw_s0	0	RO	0x0	セキュア (S) または非セキュア (NS) 要求をロジックに伝搬するかどうかを定義します。 • 0 : 非セキュア要求をロジックに伝搬しない • 1 : 非セキュアおよびセキュア要求の両方をロジックに伝搬する

security_fssw_s1

レジスタ名	security_fssw_s0
相対アドレス	0xF8900020
絶対アドレス	0xF8900020
幅	1 ビット
アクセス タイプ	RO
リセット値	0x00000000
説明	M_AXI_GP0 セキュリティ設定

フィールド名	ビット	タイプ	リセット値	説明
fssw_s1	0	RO	0x0	セキュア (S) または非セキュア (NS) 要求をロジックに伝搬するかどうかを定義します。 • 0 : 非セキュア要求をロジックに伝搬しない • 1 : 非セキュアおよびセキュア要求の両方をロジックに伝搬する

この資料の「NIC301 PL クロックのアクティブ化とリセットの非アクティブ化」セクションも参照してください。

security_apb

レジスタ名	security_apb
相対アドレス	0xF8900028
絶対アドレス	0xF8900028
幅	6 ビット
アクセス タイプ	RW
リセット値	0x00000000
説明	FPGA AFI AXI ポート TrustZone ディスエーブル

フィールド名	ビット	タイプ	リセット値	説明
ddrc_apb	5	WO	0x0	DDRC に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア
ttc1_apb	4	WO	0x0	TTC1 に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア
afi3_apb	3	WO	0x0	HP3 に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア
afi2_apb	2	WO	0x0	HP2 に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア
afi1_apb	1	WO	0x0	HP1 に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア
afi0_apb	0	WO	0x0	HP0 に対する APB トランザクションを制御します。 • 0 : 常にセキュア • 1 : 常に非セキュア

Zynq-7000 AP SoC 上の TrustZone の設定とプログラミング

このセクションでは、Zynq-7000 デバイス ファミリの TrustZone レジスタをプログラムするために必要なガイドラインを示します。

クロックのアクティブ化とリセットの非アクティブ化

Zynq-7000 デバイスで TrustZone 対応ソリューションを構築するには、AP SoC 内の各種サブシステム固有のレジスタに対する設定が必要です。

重要 : 適切な動作を確保し、レジスタ アクセスによって PS がハングアップすることを防ぐために、適切なクロックがアクティブ化され、リセットがディアサートされていることを確認する必要があります。

PL クロックのアクティブ化とリセットの非アクティブ化

Zynq-7000 デバイスの一部のコンフィギュレーション レジスタは、AXI インターコネクト用の Zynq-7000 GPV レジスタを操作します。次の要件を満たしていなければ、GPV にアクセスを試みた際に PS 全体がハングアップする恐れがあります。

- プログラマブル ロジック内のすべてのクロックをアクティブとして定義する
- GPV 用の PS-PL 間 AXI インターフェイスすべてに含まれる、全リセットをディアサートとして定義する

この要件は、AXI マスター (スレーブ) インターフェイスが内蔵 AXI スレーブ (マスター) に接続されていない場合、およびスレーブに接続する FPGA AXI マスター インターフェイスをリマップ機能を使用して無効化している場合にも適用されます。

詳細は、『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] のセクション 5.6.2「クロックとリセット」を参照してください。

NIC301 PL クロックのアクティブ化とリセットの非アクティブ化

Zynq NIC301 AMBA-AXI インターコネクトには、PL クロックをアクティブにし、対応するリセット信号をディアサートする必要がある、アドレス領域制御レジスタ (nic301_addr_region_ctrl レジスタ) が複数あります。したがって、FPGA_RST_CTL レジスタを、Zynq-7000 AP SoC TRM 推奨事項に従って設定する必要があります (推奨ビット フィールドへの 0 書き込みなど)。『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] のセクション B.21「NIC301 アドレス領域制御」(nic301_addr_region_ctrl レジスタ) および B.28「システム レベル制御レジスタ (slcr)/ レジスタ FPGA_RST_CTRL の詳細」を参照してください。

APB ブート セキュア ポートのリセット

DDRC、TTC1、AFI0、AFI1、AFI2、AFI3 の APB ブート セキュア ポートも、GPV 設定時にリセットをディアサートする必要があります。

PL マスターのセキュリティ

PL マスター IP への TrustZone セキュリティのインプリメンテーションはデザイン固有です。ザイリンクスの AXI Interconnect IP は TrustZone セキュリティ拡張機能をサポートし、これは Vivado IP カタログの IP コンフィギュレーション ウィザードで高度なコンフィギュレーション オプションとして提供されます。詳細は、AXI Interconnect IP のデータシートを参照してください。

AxCACHE = 3 に設定した AXI バス トランザクション

特定の条件の組み合わせで発生する可能性があるメモリ コヒーレンシの問題を避けるため、AXI マスターが発行する AXI バス トランザクションはすべて AxCACHE = 3 として定義する必要があります。

Zynq-7000 DMAC に関する注意事項

Zynq-7000 デバイス ファミリは、DMA をセキュアおよび非セキュア領域で動作するよう設定できる、ARM PL330 DMA コントローラーを使用しています。

DMA 動作の概要は次のとおりです。

1. DMAC がリセットされます。
   - DMAC のセキュリティ状態が読み出されます。
2. DMA チャネルが DMAGO ファンクションで設定されます。
   - DMAC のセキュリティ状態とプログラミング ソフトウェアのセキュリティ状態に注意します。
3. PL330 が、DMAGO が指定する位置から命令をフェッチします。
   - DMA 命令が、PL330 によってキャッシュされます。
4. 特定の DMA チャネルが起動されます。
   - 最後の DMAC 命令に達するまで、チャネル ベースのメモリ動作が実行されます。

以降のセクションでは、DMA アクセスを TrustZone のセキュアおよび非セキュア ソフトウェアに限定する方法について説明します。この情報は、『Corelink DMA-330 テクニカル リファレンス マニュアル』[参照 3] および『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585) [参照 1] のセクション 9.3 「DMA コントローラーのプログラミング ガイド」に掲載された詳細情報を補足するものです。

手順 1 : DMAC セキュリティ状態の設定

Zynq-7000 デバイスの DMAC は、Zynq-7000 AP SoC 内のほかの TrustZone 対応ハードウェアとまったく同様に扱われます。セキュアまたは非セキュア デバイスのいずれかとして定義できます。

重要 : この設定は、DMAC 全体のセキュリティ状態を定義します。DMAC との通信に、非セキュアまたはセキュア コンフィギュレーション ポートのどちらを使用するかは関係ありません。

DMAC のセキュリティは、Zynq-7000 の TZ_DMA_NS ビット (ARM PL330 の資料では boot_manager_ns と呼ばれている) の値に従って設定されます。プログラマーが DMAC コアへのリセットをディアサートする前に、このビットをセキュアまたは非セキュア状態に対応する目標値に設定する必要があります。この TZ_DMA_NS ビットはリセットのディアサートより前に設定されるため、それ以前の DMA チャネル設定はすべてクリアされます。

DMAC をセキュアに設定した場合、非セキュアおよびセキュア DMA チャネルの両方を設定できます。また、DMA チャネル設定を実行しているマスターのセキュリティ状態に応じて、セキュアおよび非セキュア アドレスの両方にアクセスできます。このようなアドレスには、DMAC 命令が格納されているメモリ位置や、実行される AXI チャネル読み込み/格納動作の対象となるメモリ位置が含まれます。

DMAC を非セキュアに設定した場合、各 DMA チャネルを設定している CPU のセキュリティ状態に関係なく、DMAC は非セキュア アドレスにしかアクセスできず、非セキュア DMA チャネルしか生成できません。セキュアおよび非セキュア DMA チャネルの組み合わせが可能なのは、DMAC をセキュアとして定義した場合のみです。

手順 2 : DMA チャネルの設定

各 DMA チャネルは使用前に、「DMAGO」命令を使用して設定する必要があります。命令の構文は次のとおりです。

```
DMAGO <CHANNEL_NUMBER>, <32-bit_immediate>,  [ns]
```

注記 : [ns] を指定できるのは、DMAC がセキュア デバイスとして定義され、セキュア ソフトウェアによってチャネルを設定する場合のみです。DMAC が非セキュア デバイスとして定義されている場合、すべての DMA チャネルは非セキュアとして設定されます。

DMAC をセキュアまたは非セキュア デバイスのいずれに定義したかに応じて (上記参照)、チャネルの設定は、セキュアまたは非セキュア APB ポートのいずれかを用いて実行する必要があります。

非セキュア状態の DMAC

DMAC が非セキュア状態に設定されている場合、コンフィギュレーション ポートは次のように動作します。

非セキュア コンフィギュレーション ポート

DMAC が非セキュア状態の場合、セキュアおよび非セキュア両方の CPU が非セキュア DMA チャネルの設定に非セキュア APB コンフィギュレーション ポートを使用できます。

設定を実行する CPU のセキュリティ状態に関係なく、このポートからの DMA チャネル設定は非セキュア状態で開始されます。このような非セキュア DMA チャネルでは、「手順 3 : DMA チャネル アクセス」に示すセキュリティ上の観点に留意する必要があります。

セキュア コンフィギュレーション ポート

セキュア コンフィギュレーション ポートには、DMAC のセキュアまたは非セキュア状態に関係なく、セキュア CPU のみアクセス可能できます。

DMAC が非セキュア状態の場合、このポートを介して設定されるすべての DMA チャネルは、非セキュア チャネルとして定義されます。セキュア DMA チャネルを作成しようとしても [ns = 0]、NOP が生成されるだけです。このような非セキュア DMA チャネルでは、「手順 3 : DMA チャネル アクセス」に示すセキュリティ上の観点に留意する必要があります。

DMAC チャネル設定のまとめ

表 6 に、DMA チャネルを正常に起動させるために満たすべき条件を示します。関連するアボート状態の詳細は、『Corelink DMA-330 Technical Reference Manual』[参照 3] のセクション 2.8.2 と 2.9 を参照してください。

- S = セキュア
- NS = 非セキュア
- X = Don’t care

表 6 : DMAC チャネル設定のまとめ

マスター (CPU) の S/NS 状態	S/NS APB ポートを介した DMAC アクセス	DMAC S/NS 状態	起動するチャネルに対して要求される S/NS 状態	設定可否	備考
NS	S	X	X	不可	NS CPU はセキュア APB ポートにアクセスできません。
X	NS	S	X	不可	セキュア状態で DMAC が動作している場合、非セキュア コンフィギュレーション ポートへのデータ書き込みはすべてアボートされます。

表 6 : DMAC チャネル設定のまとめ (続き)

マスター (CPU) の S/NS 状態	S/NS APB ポートを介した DMAC アクセス	DMAC S/NS 状態	起動するチャネルに対して要求される S/NS 状態	設定可否	備考
X	X	NS	S	不可	NS DMAC は S チャネルを起動できません。
S	S	S	X	可	
S	X	NS	NS	可	
NS	NS	NS	NS	可	

手順 3 : DMA チャネル アクセス

DMA チャネルの起動後、DMA チャネルおよびアクセス先アドレスのセキュリティ設定に応じて、アクセスが次の 2 つの点で制御されます。

第 1 に、DMAC から DMA 命令コードへのアクセスは、DMAC チャネルのセキュリティ状態と、その DMA 命令コードが格納されたアドレスのセキュリティ状態に基づいて実行されます。DMA チャネルが非セキュアに定義され、命令コードがセキュア アドレスに格納されている場合、AXI インターコネクトから DMAC にアボートが送信されます。DMAC は CPU に対して割り込みで応答します。

第 2 に、DMA チャネルのセキュリティ状態は、DMA 命令コード内で呼び出されるデータ メモリに対して十分なアクセス特権を持っていなければなりません。したがって、DMA チャネルが非セキュアと定義され、その DMA チャネルがアクセスしようとしているアドレスがセキュアな場合、AXI インターコネクトから DMAC にアボートが送信されます。DMAC は CPU に対して割り込みで応答します。

- S = セキュア
- NS = 非セキュア
- X = Don’t care

表 7 : DMA チャネル アクセスのまとめ

アクセスされる DMA チャネルの S/NS 状態	アクセスを試みる命令およびデータ メモリ DMA の S/NS 状態	アクセス可否
S	S	可
S	NS	可
NS	S	不可
NS	NS	可

割り込みおよびペリフェラルの設定

前のセクションでは、DMA チャネルを TrustZone のセキュアおよび通常 (非セキュア) 領域に限定するための PL330 の設定方法について説明しました。PL330 には、外部割り込みおよびペリフェラルがシステムと対話する方法を定義する 2 つの信号もあります。これらの信号は、インターフェイスへのアクセスを定義するのみで、DMA のセキュリティ アクセスには影響を与えません。

TZ_DMA_IRQ_NS [Boot_irq_ns]

boot_irq_ns[] ビットは、外部割り込みの動作を定義し、それらをセキュアまたは非セキュア動作によってトリガーできるかどうかを決定します。また、特定の DMA チャネルが WFI および WFE 命令に応答できるかどうかも制御します。

TZ_DMA_PERIPH_NS [Boot_periph_ns]

boot_periph_ns[] ビットは、ペリフェラル ハンドシェイク インターフェイスに対応します。PL330 は、特定の DMA チャネルと直接ハンドシェイク可能なインターフェイスの数を設定できます。このハンドシェイクにより、ペリフェラル命令のフラッシュ、読み込みと通知など、DMA でペリフェラルを制御できます。PL330 リセットに適用される信号は、これらを非セキュア動作で実行可能か不可 (したがって、boot_manager_ns には接続されない) かを定義します。

セキュアおよび非セキュア DMA チャネル両方に対するシステムの構築

プラットフォームが 2 つのオペレーティング システムを実行する必要があるシナリオを考えます。一方の OS はセキュア領域、もう一方は通常 (非セキュア) 領域で動作します。通常領域の OS は DMA アクセスを必要としていますが、セキュア領域のメモリ空間へのアクセスは禁止する必要があります。このようなシナリオには、それぞれがセキュアおよび非セキュアとして動作する独立した DMA チャネルを起動することで対処できます。ただし、考慮すべき重要なシステム上の注意点がいくつか存在します。

セキュア動作する DMA コントローラーはセキュアおよび非セキュア DMA チャネルの両方を設定、ならびに起動可能です。しかし、非セキュア CPU は DMAC を直接管理できないという点に注意が必要です。つまり、非セキュア DMA チャネルとセキュア DMA チャネルを隣り合わせて作成することはできても、非セキュア チャネルを設定できるのはセキュア CPU のみです。

推奨 : 通常、DMAC は最近のセキュア専用ハードウェア (例 : キャッシュ コントローラー) と同様の方法で取り扱うべきです。

キャッシュ コントローラーなどのセキュア専用デバイスは、セキュア CPU 上で動作するソフトウェアによって直接制御されます。非セキュア CPU がこれらのサービスを使用すると、セキュア CPU に対してセキュア モニター コール (SMC) を呼び出します。通常、SMC は実行を要求されたコマンドと共に、その呼び出しの主要な属性をすべて識別します。

このシナリオの場合、このプロセスに対応可能なカスタム SMC は次の 4 つのみです。

1. 非セキュアからセキュア
    a. DMA チャネルの設定に必要なパラメーターをセキュア領域に渡します。
        i. セキュア領域は非セキュア CPU の代わりに非セキュア DMA チャネルを作成します。
        ii. DMAC は DMAWFE で一時停止し、DMAC 命令コードの実行を開始します。
        iii. この SMC は標準 DMAGO に非常によく似ている場合があります。
2. セキュアから非セキュア
    a. DMA チャネルが使用可能になるとセキュア CPU が非セキュア CPU に通知します。
    b. DMAC は DMAWFE で停止します。
3. 非セキュアからセキュア
    a. 非セキュア CPU は DMA トランザクションを実行することをセキュア CPU に通知します。
4. セキュアから非セキュア
    a. トランザクションの完了時にセキュア CPU が非セキュア CPU に通知します。

Zynq-7000 デバイス PL330 のプログラミング

これまで説明してきた機能に関する情報を補足するために、このセクションでは、DMAC のプログラミング方法の詳細を説明します。

DMAC は TrustZone レジスタを介して設定可能なセキュリティを提供します。これらのレジスタ (TZ_DMA_NS、TZ_DMA_IRQ_NS、TZ_DMA_PERIPH_NS) は、DMAC コアの外部 (SLCR 内) にあり、DMAC のセキュリティ状態を定義します。SLCR レジスタのこれらのビットを設定する場合、次の状態を適切に維持する必要があります。

1. DMAC_RST_CTRL = `1` に設定された場合 (`0xF800020C`)、DMAC コアは常に「RESET」を受信します。DMAC コア レジスタは DMAC_RST_CTRL = `1` に設定された時点ですべて初期化されます。

   注記 : この動作は、TrustZone DMAC レジスタをリセットしません。

2. DMAC コアは、自身のリセットをディアサートする前に、次のインターフェイスがセキュアまたは非セキュア状態に応じた必要な値に設定されているものと仮定します。これは、次の設定 (a、b、c) 向けに `0xF8000440`、`44`、`48` の TrustZone レジスタをプログラムする際、(1) で前述したとおり、DMAC コアをリセット状態に保つ必要があることを意味します。

   a. セキュア DMA チャネル スレッドが必要な場合は、TZ_DMA_NS = `0` に設定します。TZ_DMA_NS = `1` は、非セキュア DMA チャネル スレッドが設定されていることを示します。

      注記 : セットされている場合、DMA マネージャーのセキュリティ状態は一定に保たれます。DMAC 内のレジスタをプログラムしても、DMA マネージャーのセキュリティ状態は変更できません。

   b. セキュア DMA irq が必要な場合は、TZ_DMA_IRQ_NS = `0` に設定します。TZ_DMA_IRQ_NS = `1` は、非セキュア DMAC irq が設定されていることを示します。

      注記 : セットされている場合、irq 信号のセキュリティ状態は一定に保たれます。DMAC 内のレジスタをプログラミングしても、irq のセキュリティ状態は変更できません。

   c. セキュア DMA ペリフェラルが必要な場合は、TZ_DMA_PERIF_NS = `0` に設定します。TZ_DMA_PERIF_NS = `1` は、非セキュア DMAC ペリフェラルが設定されていることを示します。

      注記 : セットされている場合、ペリフェラル要求のセキュリティ状態は一定に保たれます。DMAC 内のレジスタをプログラムしても、ペリフェラル要求のセキュリティ状態は変更できません。

3. TrustZone レジスタを目的の値にプログラム後、DMAC_RST_CTRL = `0` (`0xF800020C`) を書き込むことでリセットをディアサートします。

4. TZ_DMA_NS (内部 DMA 信号 boot_manager_ns) が DMAC を動作させるために初期化した際のセキュリティ状態に応じて、適切な APB インターフェイスを使用していることを確認する必要があります。たとえば、DMAC がセキュア状態にある場合、命令はセキュア APB インターフェイスを用いて発行する必要があり、そうしなければ、DMAC は命令を無視します。しかし、DMAC が非セキュア状態にある場合は、DMA チャネルの起動または再起動にセキュアまたは非セキュアいずれの APB インターフェイスも使用できます。

   詳細は、ARM の PL330 仕様書、セクション 2.4 「initializing the DMAC」を参照してください。

実際の TrustZone

以降のセクションでは、Zynq-7000 ベースのソリューションの安全またはセキュリティを向上するために活用できる有用な情報を詳細に示します。

CP15SDISABLE による CPSR のセキュリティ確保

プロセッサは、CP15 システム制御プロセッサ レジスタへの書き込みアクセスを無効にする、プライマリ入力ピン CP15SDISABLE をサポートしています。CP15SDISABLE を 1 に設定した場合、セキュアまたは通常領域のソフトウェアが、NS ビットが 0 のバンク化されたレジスタのセキュア バージョン、または NS ビットが 0 のバンク化されていないレジスタに書き込もうとすると、未定義命令例外が発生します。この信号がセットされていても、セキュアおよび通常領域のソフトウェアによる読み出しアクセスは引き続き可能ですが、各 CPSR ビットのセキュリティ状態に従った制限はそのままです (詳細は、『ARM Cortex-A9 MPCore テクニカル リファレンス マニュアル』[参照 4] を参照)。

この CP15SDISABLE ビットがセットされると、セキュア ソフトウェアであってもパワーオン リセットしない限り変更できません。このため、製品開発中やセキュリティ要件が緩い製品では、システム コンフィギュレーションできるように、このビットをリセットで 0 にできます。

この信号をザイリンクス Zynq-7000 ベースのシステム内で使用することで、特定の種類のハードウェア攻撃を防止できます。それには、ロジックに完全に内包され、外部プローブでアクセスできない外部セキュア ペリフェラル内にこのビットをインプリメントします。

割り込みのセキュリティ確保

ARM Cortex-A9-MP 割り込みコントローラーでは、インプリメントされたすべての割り込みを、個別にセキュアまたは非セキュアとして定義できます。

非セキュア割り込みは、常に Cortex-A9 プロセッサの IRQ メカニズムによって通知されます。

セキュア割り込みは、ICPICR レジスタの FIQen ビットを介して、Cortex-A9 プロセッサの IRQ または FIQ 割り込みメカニズムのいずれを使用するかをプログラムできます。セキュア システム内では FIQ と IRQ の両方は使用できないことに注意してください。どちらか一方を選択する必要があります (詳細は、『ARM Cortex-A9 MPCore Technical Reference Manual』[参照 4] を参照)。

割り込み優先度

Zynq-7000 AP SoC デバイスに搭載されている Cortex-A9 プロセッサには、『ARM Generic Interrupt Controller Architecture Specification』に記載されているフォーマットで、5 ビットの割り込み優先度がインプリメントされています。セキュア領域のソフトウェアは、これら 5 ビットのすべてにアクセスできますが、通常領域のソフトウェアがアクセスできるのは 4 ビットのみです。したがって、通常領域のどの割り込みよりも優先度の高いセキュア割り込みを定義可能です。この方法では、通常領域のソフトウェアが先に優先権を持つリスクなしで、安全またはセキュリティ重視のアプリケーションを必要なときに必要な方法で確実に実行できます。

割り込みコントローラーのセキュリティ確保

割り込みコントローラーには CFGSDISABLE をアサートした場合に、重要なコンフィギュレーション レジスタへの書き込みアクセスを防止する機能があります。この信号は、配分器および Cortex-A9 プロセッサ インターフェイスのセキュア制御レジスタに対する書き込み動作と、割り込みコントローラーのロック可能共有ペリフェラル割り込み (LSPI) を制御します。

CFGSDISABLE が High の場合、割り込みコントローラーは次のレジスタに対する書き込みアクセスを阻止します。

配分器

- ICDDCR のセキュア イネーブル

ICDICTR の LSPI フィールドによって定義されるセキュア割り込み

- 割り込みセキュリティ レジスタ
- 割り込みセット イネーブル レジスタ
- 割り込みクリア イネーブル レジスタ
- 割り込みセット保留レジスタ
- 割り込みクリア保留レジスタ
- 割り込み優先度レジスタ
- ICDIPTR
- 割り込みコンフィギュレーション レジスタ

Cortex-A9 の割り込みインターフェイス

- EnableNS ビットを除く ICCICR

CFGSDISABLE をアサートするとレジスタ ビットが読み出し専用に変更されるため、セキュア領域に実行中の不正コードが存在したとしても、これらのセキュア割り込みの動作は変更されません。いったんセットすると、このレジスタは POR でしかクリアできません。

メモリ アクセスのセキュリティ確保

この資料の冒頭で説明したとおり、ARM TrustZone はセキュア領域と通常領域の概念に従い動作します。セキュア領域はすべてのシステム リソースに無制限にアクセスできます。通常領域は定義されたハードウェア サブセットにのみアクセスできます。

前述のとおり、ザイリンクス Zynq-7000 デバイス ファミリにはコンフィギュレーション レジスタ TZ_DDR_RAM があります。このレジスタによって開発者は DDR 物理アドレス空間の 64MB のセクションを、個別にセキュアまたは非セキュア領域として定義できます。

セキュア領域から通常領域の物理メモリ位置へのアクセスは可能ですが、セキュア領域からは通常領域のページ テーブルの位置、その内容、物理/仮想メモリ位置のデータのメモリ構造がわからないため、アクセスは事実上ブラインド アクセスになります。共有メモリ領域として明確に定義したメモリ領域を除く、通常領域のメモリ データはすべて、セキュア領域ソフトウェアにとっては相関のない `1` および `0` に見えます。セキュア領域ソフトウェアからこれらの詳細を判断することは可能ですが、簡単な作業ではなく、セキュア領域のソフトウェア自体を変更する機能が必要になる可能性があります。

この点から、セキュア領域から通常領域のアドレス位置へのアクセスに伴う注意事項として、セキュア領域が通常領域のメモリ位置を誤って上書きしないようにすることが重要です。

次のセクションでは、セキュア領域から共有メモリ領域にアクセスする場合の注意点を簡単に説明します。

キャッシュ

Zynq-7000 AP SoC に含まれる ARM PL310 はセキュア領域で動作するソフトウェアに役立つ主要な機能を提供します。これには、特定のキャッシュ ラインが通常領域のソフトウェアによってロックされないようにする機能も含まれます。これより、通常領域のソフトウェアが、セキュア領域ソフトウェアに対してある種の DoS 攻撃 (サービス妨害攻撃) を起動することを制限できます。

キャッシュの適切な使用法を理解するには、PL310 インプリメンテーションに関連する次の 2 つの重要なポイントを理解することが大切です。

- PL310 は物理メモリ アドレスに基づいてキャッシュ ラインをロードする
- PL310 はセキュリティ ビットを 33 番目の物理アドレス ビットとして処理する

このインプリメンテーションにより、1 つの一意の DDR メモリ位置が 2 つの異なるキャッシュ ラインを占める可能性が生じます。一方は、セキュア領域ソフトウェアに対応し、もう一方は通常領域ソフトウェアに対応します。このような不明確な状態は、システム設計におけるキャッシュ コヒーレンシの問題を引き起こす可能性があります。しかし、セキュア領域のソフトウェアが必ずそのページ テーブルを変更するようにすることで、このようなコヒーレンシの問題を回避でき、通常領域のソフトウェアも使用するメモリ位置へのアクセスが、すべてセキュア領域からの非セキュア動作として実行されます。

PL へのセキュア アクセスの実現 : ケース スタディ

PL ベースのデザインをセキュア アクセス向けに設定する方法は、26 ページの「Zynq-7000 AP SoC 上の TrustZone の設定とプログラミング」で説明しています。

次のケース スタディでは Zynq-7000 AP SoC のプログラマブル ロジック (PL) に実装したブロック RAM ベースのデザインを取り上げます。クロックは Processing System-7 (PS-7) IP コアの FCLK 出力から供給します。Vivado IP カタログの AXI block RAM controller IP は FCLK のクロック周波数で動作し、PS-7 IP の GP0 マスター ポートを介して PS-7 IP に接続されます。このデザインを動作させるには、表 8 に示すクロックを接続する必要があります。

表 8 : ケース スタディのクロック接続

PS-PL インターフェイス名	ポート名	クロック ソース
GP0/1 AXI マスター	ACLK	ユーザー クロック ソース
GP0/1 AXI スレーブ	ACLK	ユーザー クロック ソース
HP0/1/2 AXI スレーブ	ACLK	ユーザー クロック ソース
ACP ポート	ACLK	ユーザー クロック ソース

ユーザー クロック ソースは FCLK または外部クロック ソースから派生できます。

セキュア/非セキュア アプリケーションでは、GP ポートに対するセキュリティ関連の多数の設定および GP ポートのリセット信号の適切なディアサートにも配慮する必要があります。

制御アプリケーションのソフトウェアは、次を実行する必要があります。

1. SECURITY_FSSW_Sx に `0x1` を書き込み、非セキュア アクセスが GP ポートを介して非セキュア モードで伝搬されるようにします。
2. FPGA_RST_CTRL レジスタを使用して GP ポートのリセットをディアサートします。
3. TZ_DDR_RAM レジスタに書き込むことで DDR メモリ内の非セキュア領域をマークします。
4. 非セキュア アプリケーションを起動します。

レジスタ SECURITY_FSSW_S1、FPGA_RST_CTRL、TZ_DDR_RAM はシステム レベル制御レジスタであり、CPU のセキュア動作モードからしかアクセスできないことに注意してください。

次に非セキュア モードでブロック RAM 制御アプリケーションを実行するために必要な手順を示します。これらの手順はザイリンクスのスタンドアロン OS によって検証済みです。ユーザーの環境によっては、一部の手順が不要な場合があります。

main() :

- init_platform() プラットフォームの初期化
  - D-cache の有効化 (L1、L2)
- pl_access_setup() 非セキュア モードでの PL アクセスの初期化
  - SLCR レジスタ slcr_unlock のロック解除 (アドレス : `F8000008` を `0xDF0D` に設定)
  - FPGA リセット制御レジスタ FPGA_RST_CTRL の設定 (アドレス `F8000240` を `0x0` に設定)
  - レジスタ security_gp0_axi の設定 (アドレス `F890001C` の Bit0 を `1` に設定)
  - SLCR レジスタ slcr_unlock のロック (アドレス : `F8000004` を `0x767B` に設定)
- configure_secure_world() システムを非セキュア モードに設定
  - board_init
    - TZ_DDR_RAM の初期化
    - TZ_SECURITY_SDIO2 の初期化
    - TZ_SECURITY_SDIO1 の初期化
    - TZ_SECURITY4_QSPI の初期化
    - TZ_SECURITY6_APBSL の初期化
    - TZ_SECURITY5_MIOU の初期化
    - TZ_SECURITY7_SMC の初期化
    - TZ_DMAC_RST_CTRL の初期化
    - TZ_DMA_NS の初期化
    - TZ_DMA_IRQ_NS の初期化
    - TZ_DMA_PERIPH_NS の初期化
    - TZ_GEM の初期化
    - TZ_SDIO の初期化
    - TZ_USB の初期化
    - TZ_FPGA_M の初期化
    - TZ_FPGA_AFI の初期化
    - TZ_OCM_RAM_0 の初期化
    - TZ_OCM_RAM_1 の初期化
    - TZ_OCM_ROM の初期化
  - mpcore_init
    - SCU の初期化
    - GIC IRQ ベクターの初期化
    - GIC CPU ベースの初期化
    - 割り込みの有効化
  - monitor_init
    - モニターの準備 (アセンブリ命令、レジスタ モニター ハンドラー)
    - SMC 命令の起動 (callSMC() ファンクション)

- callSMC
  - 非セキュア アプリケーションのデスティネーション アドレスの設定 (ping、loopback その他)
  - SMC 命令の起動
  - これによって smc_handler を起動
- smc_handler
  - モニターのクリア
  - 非セキュア DDR アクセスを可能にするための TLB の設定
  - 非セキュア DDR アクセスを可能にするための TTBR の設定 (バンク化されたレジスタ)
  - 非セキュア DDR アクセスを可能にするためのドメイン アクセスの設定 (バンク化されたレジスタ)
  - このセキュア モード中にバンク化されたレジスタの内容を読み出す
  - 一時的に非セキュア モードに切り替え
  - TLB を非セキュア モードに設定
  - TTBR を非セキュア モードに設定 (バンク化されたレジスタ)
  - 非セキュア DDR アクセスを可能にするためのドメイン アクセスの設定 (バンク化されたレジスタ)
  - バンク化されたレジスタの内容をセキュア モードから非セキュア モードに更新
  - 非セキュア モードを選択した場合、CPU は非セキュア モードで動作を継続
  - それ以外の場合、CPU をセキュア モードに戻す
  - _custom_boot の起動
- _custom_boot()
  - ベクター テーブルを非セキュア モードに設定
  - 各ベクターに対してスタック領域を設定
  - _cstart の起動 (main () ファンクションの呼び出しと等価)
- _cstart()
  - BSS 領域のクリア
  - 初期スタック フレームの設定
  - グローバル コンストラクターの実行 (アプリケーション起動前の初期スタック フレーム)
  - アプリケーション コードの起動
- application()
  - アプリケーション固有のタスクの実行

PS GEM、SDIO、SDIO、USB コントローラーに対する非セキュア アクセスの実現

GEM

GEM への非セキュア アクセスを可能にするには、GEM に対する非セキュア領域の動作を開始する前に、セキュア領域で次の TrustZone レジスタを設定しておく必要があります。

1. GEM スレーブ セキュリティ設定を 1 にして非セキュア アクセスを可能にします。
   a. security6_apb_slaves .gem0_s_apb = `0x1` // GEM controller 0
   b. security6_apb_slaves .gem1_s_apb = `0x1` // GEM controller 1
2. GEM TrustZone コンフィギュレーション レジスタを非セキュア アクセス モードに設定します。
   a. Slcr.TZ_GEM.E0 = `0x1` //Non-secure access for GEM controller 0
   b. Slcr.TZ_GEM.E1 = `0x1` //Non-secure access for GEM controller 1

上記の設定により、GEM マスターに対する非セキュア メモリ アクセスが可能になります。

上記の設定とは別に、ペリフェラルのクロックおよびハード リセットもセキュア領域からしか設定できません。

GEM クロックを有効/無効にする場合、またはデフォルト クロック設定を変更する場合、セキュア領域で次のレジスタを設定する必要があります。

- SLCR.GEMx_CLK_CTRL
  - CLKACT - クロックの有効化/無効化
  - iSRCSEL - クロック ドメインのソース
  - DIVISOR - GEM コントローラーの第 1 分周比
  - DIVISOR1 - GEM コントローラーの第 2 分周比

GEM コントローラーをハード リセットするには、セキュア領域で次のレジスタを設定する必要があります。

- SLCR.GEM_RST_CTRL

GEM コントローラーのその他の設定および有効化は、すべて非セキュア領域で実行する必要があります。

例

非セキュア領域で GEM コントローラー 0 をデフォルト クロックで有効にするには、セキュア モードで次のレジスタを設定する必要があります。

- security6_apb_slaves .gem0_s_apb
- SLCR.TZ_GEM.E0 = `0x1`
- SLCR.GEM0_CLK_CTRL.CLKACT = `0x1`
- GEM コントローラーのその他の設定 (コンフィギュレーション、有効化、転送トリガー) は、非セキュア モードで実行します。

SDIO

SDIO への非セキュア アクセスを可能にするには、SDIO に対する非セキュア領域の動作を開始する前に、セキュア領域で次の TrustZone レジスタを設定しておく必要があります。

1. SDIO スレーブ セキュリティ設定を `1` にして非セキュア アクセスを可能にします。
   a. gpv_iou_switch.security2_sdio0 = `0x1` // SDIO controller 0
   b. gpv_iou_switch.security3_sdio1 = `0x1` // SDIO controller 1
2. SDIO TrustZone コンフィギュレーション レジスタを非セキュア アクセス モードに設定します。
   a. Slcr.TZ_SDIO.S0 = `0x1` // Non-secure access for SDIO controller 0
   b. Slcr.TZ_SDIO.S1 = `0x1` // Non-secure access for SDIO controller 1

上記の設定により、SDIO マスターに対する非セキュア メモリ アクセスが可能になります。

上記の設定とは別に、ペリフェラルのクロックおよびハード リセットもセキュア領域からしか設定できません。

SDIO クロックを有効/無効にする場合、またはデフォルト クロック設定を変更する場合、セキュア領域で次の SLCR レジスタを設定する必要があります。

- SLCR.SDIO_CLK_CTRL
  - CLKACT - クロックの有効化/無効化
  - SRCSEL - クロック ドメインのソース
  - DIVISOR - SDIO コントローラーの分周比

SDIO コントローラーをハード リセットするには、セキュア領域で次のレジスタを設定する必要があります。

- SLCR.SDIO_RST_CTRL

SDIO コントローラーのその他の設定および有効化は、すべて非セキュア領域で実行する必要があります。

例 :

非セキュア領域で SDIO コントローラー 0 をデフォルト クロックで有効にするには、セキュア モードで次のレジスタを設定する必要があります。

- gpv_iou_switch.security2_sdio0 = `0x1`
- SLCR.TZ_SDIO.S0 = 0x1
- SLCR.SDIO_CLK_CTRL.CLKACT0 = `0x1`
- SDIO コントローラーのその他の設定 (コンフィギュレーション、有効化、転送トリガー) は、非セキュア モードで実行します。

USB コントローラー

USB コントローラーへの非セキュア アクセスを可能にするには、USB に対する非セキュア領域の動作を開始する前に、セキュア領域で次の TrustZone レジスタを設定しておく必要があります。

1. USB スレーブ セキュリティ設定を `1` に設定して非セキュア アクセスを可能にします。
   a. gpv_iou_switch. security6_apb_slaves. usb0_s_apb = `0x1` // USB controller 0
   b. gpv_iou_switch. security6_apb_slaves. usb1_s_apb = `0x1` // USB controller 1

2. USB TrustZone コンフィギュレーション レジスタを非セキュア アクセス モードに設定します。
   a. Slcr.TZ_USB.U0 = `0x1` //Non-secure access for USB controller 0
   b. Slcr.TZ_USB.U1 = `0x1` //Non-secure access for USB controller 1

上記の設定により、USB に対する非セキュア メモリ アクセスが可能になります。

上記の設定とは別に、ペリフェラルのクロックおよびハード リセットもセキュア領域からしか設定できません。

USB クロックを有効/無効にする場合、またはデフォルト クロック設定を変更する場合、セキュア領域で次のレジスタを設定する必要があります。

- SLCR.USBX_CLK_CTRL
  - CLKACT - クロックの有効化/無効化
  - SRCSEL - クロック ドメインのソース
  - DIVISOR0 - USB コントローラーの第 1 分周比
  - DIVISOR1 - USB コントローラーの第 2 分周比

USB コントローラーをハード リセットするには、セキュア領域で次のレジスタを設定する必要があります。

- SLCR.USB_RST_CTRL

USB コントローラーのその他の設定および有効化は、すべて非セキュア領域で実行する必要があります。

例 :

USB コントローラー 0 に対する非セキュア アクセスをデフォルト クロックで有効にするには、セキュア モードで次のレジスタを設定する必要があります。

- gpv_iou_switch. security6_apb_slaves. usb0_s_apb = `0x1`
- SLCR.TZ_USB.U0 = `0x1`
- SLCR.USB0_CLK_CTRL.CLKACT = `0x1`
- USB コントローラーのその他の設定 (コンフィギュレーション、有効化、転送トリガー) は、非セキュア モードで実行する必要があります。

その他のリソース

ザイリンクス リソース

アンサー、資料、ダウンロード、フォーラムなどのサポート リソースを利用するには、ザイリンクス サポート サイトにアクセスしてください。

常に最新情報を受け取るには、マイ プロフィールからアラートにアンサーを追加してください。

用語とその定義については、ザイリンクス用語集を参照してください。

ソリューション センター

デバイス、ソフトウェア ツール、IP のサポートについては、ザイリンクス ソリューション センターを参照してください。デザイン アシスタント、デザイン アドバイザリ、トラブルシュートのヒントなどが含まれます。

参考資料

次の文書/ウェブサイトは、このユーザー ガイドの補足資料として役立ちます。

1. 『Zynq-7000 AP SoC テクニカル リファレンス マニュアル』(UG585)
2. 『ARM アーキテクチャ リファレンス マニュアル』
3. 『CoreLink DMA-330 DMA Controller Technical Reference Manua』
4. 『ARM Cortex-A9 MPCore Technical Reference Manua』
5. Zynq-7000 AP SoC - TrustZone アンサー レコード (AR57835)
6. サードパーティ提供の資料
7. ARM TrustZone のウェブサイト
8. 『ARM アーキテクチャ リファレンス マニュアル』