この翻訳版ドキュメントのメンテナンスは終了しております。

この文書には、古いコンテンツや商標が含まれている場合があります。

最新情報につきましては、次のリンクから英語版の最新資料をご確認ください。

https://www.intel.com/content/www/us/en/programmable/documentation/lit-index.html

Please take note that this document is no longer being maintained. It may contain legacy content and trademarks which may be outdated.

Please refer to English version for latest update at
https://www.intel.com/content/www/us/en/programmable/documentation/lit-index.html

14. Stratix III デバイスのデザイン・セキュリティ

SIII51014-1.0

はじめに

この章では、デザイン・セキュリティ機能と設計者がこれらの新機能をデザインで利用するための高度暗号化規格（Advanced Encryption Standard、略称 : AES）および Stratix III デバイスのセキュリティ・モードを使用した Stratix® III デバイスへの実装の概要を示します。

Stratix III デバイスは、競争の激しい一般用および軍用環境におけるより大規模かつ条件の厳しいデザインで、その役割を果たし始めており、複製、リバース・エンジニアリング、および改ざんからデザインを保護することがますます重要になっています。

Stratix III デバイスはこれらの問題に対処しており、揮発性および不揮発性の両方のセキュリティ機能をサポートした、業界で唯一の高集積、高性能デバイスです。Stratix III デバイスは、FIPS-197 認定済みの業界標準の暗号化アルゴリズムである AES アルゴリズムを使用して、コンフィギュレーション・ビットストリームを復号化する機能を備えています。Stratix III デバイスは、256 ビットのセキュリティ・キーを利用したデザイン・セキュリティ機能を備えています。

アルテラの Stratix III デバイスは、デバイスの動作中にスタティック・ランダム・アクセス・メモリ (SRAM) コンフィギュレーション・セルに、コンフィギュレーション・データを格納します。SRAM メモリは揮発性のため、デバイスに電源を投入するたびにコンフィギュレーション・データを SRAM セルにロードする必要があります。コンフィギュレーション・データがメモリ・ソース（Flash メモリまたはコンフィギュレーション・デバイス）からデバイスに転送されているときに、それを傍受することができます。傍受されたコンフィギュレーション・データは、別のデバイスをコンフィギュレーションするのに使用できます。

Stratix III のデザイン・セキュリティ機能を使用しているとき、セキュリティ・キーは Stratix III デバイスに格納されます。Stratix III デバイスは、セキュリティ・モードに応じて、同じキーで暗号化されたコンフィギュレーション・ファイル、またはボード・テストの場合は通常のコンフィギュレーション・ファイルを使用してコンフィギュレーションすることができます。

デザイン・セキュリティ機能は、外部ホスト（MAX® II デバイスやマイクロプロセッサ）でファースト・パッシブ・パラレル（FPP）コンフィギュレーション・モードを使用して、Stratix III FPGA をコンフィギュレーションするとき、あるいはファースト・アクティブ・シリアル（AS）

またはパッシブ・シリアル (PS) コンフィギュレーション手法を使用するときに使用できます。デザイン・セキュリティ機能は、ファースト AS コンフィギュレーション・モードでのリモート・アップデートのときにも使用できます。FPP をエンハンスド・コンフィギュレーション・デバイス、または JTAG（Joint Test Action Group）ベースのコンフィギュレーションと一緒に使用して、Stratix III デバイスをコンフィギュレーションする場合、デザイン・セキュリティ機能は使用できません。詳しくは、14–7 ページの「サポートされている コンフィギュレーション 手法」を参照してください。

最大規模のシリアル・コンフィギュレーション・デバイスは、現在、64 M ビットのコンフィギュレーション・ビットストリームをサポートしています。EP3SE260 や EP3SL340 などの大規模な Stratix III デバイス向けのシリアル・コンフィギュレーション・デバイス・サポートについて詳しくは、アルテラのテクニカル・サポートにお問い合わせください。

Stratix III のセキュリティ保護

Stratix III デバイスのデザインは、コンフィギュレーション・ビットストリーム暗号化機能により、複製、リバース・エンジニアリング、および改ざんから保護されています。

複製に対するセキュリティ

セキュリティ・キーは Stratix III デバイスに安全に格納され、いかなるインタフェースを介してもこれを読み出すことはできません。さらに、Stratix III デバイスではコンフィギュレーション・ファイルのリード・バックはサポートされていないので、デザイン情報を複製することはできません。

リバース・エンジニアリングに対するセキュリティ

Stratix III のコンフィギュレーション・ファイル・フォーマットは独自のものであり、ファイルには特定の復号化を必要とする数百万ビットが収められているので、暗号化されたコンフィギュレーション・ファイルからのリバース・エンジニアリングは非常に困難で長時間を要します。Stratix III デバイスのリバース・エンジニアリングも同様に困難です。これは、このデバイスが最先端の 65 nm プロセス・テクノロジに基づいて製造されているためです。

改ざんに対するセキュリティ

不揮発性キーはワンタイム・プログラマブルです。Quartus® II ソフトウェアで生成されるキー・プログラミング・ファイルに改ざん保護ビットが一度セットされると、同じキーで暗号化されたコンフィギュレーション・ファイルを使用しない限り、Stratix III デバイスをコンフィギュレーションすることはできません。

この機能がセキュリティ保護されている理由について詳しくは、「Stratix III デザイン・セキュリティ ホワイトペーパー」を参照してください。

AES 復号化ブロック

AES 復号化ブロックの主な目的は、圧縮データの復元またはコンフィギュレーションが開始される前に、コンフィギュレーション・ビットストリームを復号化することです。

暗号化されたデータを受信する前に、256 ビットのセキュリティ・キーをデバイス内に入力および格納しなければなりません。不揮発性セキュリティ・キーと、バッテリ・バックアップ付き揮発性セキュリティ・キーのいずれかを選択することができます。

それぞれのキーをプログラムするためのステップは、今後提供される「Stratix III デザイン・セキュリティ・アプリケーション・ノート」に記載される予定です。

セキュリティ・キーはスクランブルしてからキー・ストレージに格納されるので、格納されたキーをデバイスの開封を行って読み出すことが一層困難になります。

柔軟性の高いセキュリティ・キー・ストレージ

Stratix III デバイスは、揮発性キーと不揮発性キーの 2 種類のセキュリティ・キーのプログラミングをサポートしています。表 14–1 に、揮発性キーと不揮発性キーの相違点を示します。

表 14–1. セキュリティ・キーのオプション （1 / 2）

オプション	揮発性キー	不揮発性キー
キーのプログラマビリティ	再プログラム可能かつ消去可能	ワンタイム・プログラマブル
外部バッテリ	必要	不要
キーのプログラミングの方法 (1)	オンボード	オンボードおよびオフボード

表 14–1. セキュリティ・キーのオプション （2 / 2）		
オプション	揮発性キー	不揮発性キー
デザインの保護	複製およびリバース・エンジニアリングに対するセキュリティ保護	複製、リバース・エンジニアリング、および改ざんに対するセキュリティ保護

表 14–1 の注 :
(1) キーのプログラミングは JTAG インタフェースを介して実行されます。

不揮発性キーは、外部バッテリなしで Stratix III デバイスにプログラムすることができます。また、Stratix III の電源に追加の要件はありません。

V_{CCBAT} は揮発性キー・ストレージ専用の電源で、V_{CCIO} や V_{CC} など、その他のオンチップ電源とは共有されません。V_{CCBAT} は、オンチップ電源の状態に関係なく、揮発性レジスタに電源を供給し続けます。この電源の標準電圧は 2.5 V で、その有効動作範囲は 1.0 ～ 3.0 V です。揮発性セキュリティ・キーを使用しない場合は、V_{CCBAT} をグランドまたは 2.5 V 電源のいずれかに接続することができます。

☞ 電源投入後、V_{CCBAT} が確実にその最大レール電圧で安定するように、100 ms (PORSEL = 0) または 12 ms (PORSEL = 1) 待機してからキーのプログラミングを開始する必要があります。

☞ 一例として、BR1220 (-30°C ～ +80°C) や BR2477A (-40°C ～ +125°C) などの、揮発性キー・ストレージに使用されるリチウム・コイン電池タイプのバッテリがあります。バッテリの仕様について詳しくは、「Stratix III デバイス・ハンドブック Volume 2」の「Stratix III デバイスの DC & スイッチング特性」の章を参照してください。

Stratix III デザイン・セキュリティ・ソリューション

Stratix III デバイスは SRAM ベースのデバイスです。StratixIII デバイスは、デザイン・セキュリティを提供するために、コンフィギュレーション・ビットストリーム暗号化に 256 ビットのセキュリティ・キーを必要とします。

図 14–1 に示す以下の 3 つのステップに従って、安全なコンフィギュレーションを行うことができます。

1. セキュリティ・キーを Stratix III FPGA 内にプログラムします。

JTAG インタフェースを介して、ユーザ定義の 256 ビット AES キーを Stratix III デバイスにプログラムします。

2. コンフィギュレーション・ファイルを暗号化して外部メモリ内に格納します。

   Stratix III デバイスをプログラムするのに使用するのと同じ 256 ビットのキーで、コンフィギュレーション・ファイルを暗号化します。Quartus II ソフトウェアを使用して、コンフィギュレーション・ファイルの暗号化が行われます。暗号化されたコンフィギュレーション・ファイルは、コンフィギュレーション・デバイスやフラッシュ・デバイスなどの外部メモリ内にロードされます。

3. Stratix III デバイスをコンフィギュレーションします。

   システムのパワーアップ時に、外部メモリ・デバイスから暗号化されたコンフィギュレーション・ファイルが Stratix III デバイスに送られます。

図 14–1. デザイン・セキュリティ 注 (1)

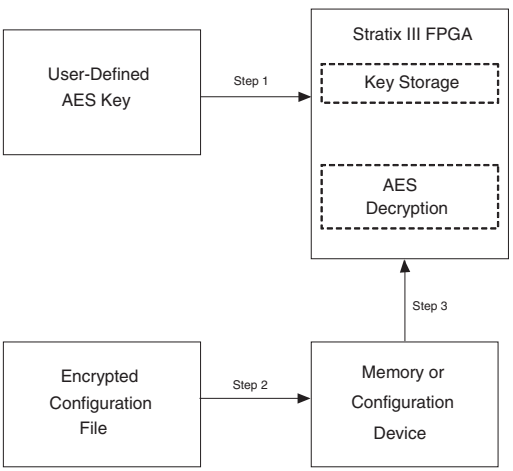

図 14–1 の注 :

(1) ステップ 1、ステップ 2、およびステップ 3 は、「Stratix III デザイン・セキュリティ・ソリューション」の項に詳述した手順に対応します。

使用可能なセキュリティ・モード

Stratix III デバイスで使用できるセキュリティ・モードは、以下に示すとおりいくつかあります。

揮発性キー

プログラムされた揮発性キーと必要な外部バッテリによるセキュリティ保護動作 : このモードでは、暗号化されたコンフィギュレーション・ビットストリームと暗号化されていないコンフィギュレーション・ビットストリームの両方を受け入れます。暗号化されていないコンフィギュレーション・ビットストリームは、ボードレベルのテストにのみ使用します。

不揮発性キー

プログラムされたワンタイム・プログラマブル・セキュリティ・キーによるセキュリティ保護動作:このモードでは、暗号化されたコンフィギュレーション・ビットストリームと暗号化されていないコンフィギュレーション・ビットストリームの両方を受け入れます。暗号化されていないコンフィギュレーション・ビットストリームは、ボードレベルのテストにのみ使用します。

改ざん保護ビットがセットされた不揮発性キー

プログラムされた OTP セキュリティ・キーによる改ざん防止モードでのセキュリティ保護動作 : デバイスのコンフィギュレーションには、暗号化されたコンフィギュレーション・ビットストリームのみ許可されます。

キーなしでの動作

デバイスのコンフィギュレーションには、暗号化されていないコンフィギュレーション・ビットストリームのみ許可されます。

表 14–2 に、各種のセキュリティ・モードと、各モードにサポートされているコンフィギュレーション・ビットストリームの概要を示します。

表 14–2. サポートされるセキュリティ・モード （1 / 2）

モード (1)	機能	コンフィギュレーション・ファイル
揮発性キー	セキュリティ保護	暗号化
	ボード・レベル・テスト	暗号化なし
不揮発性キー	セキュリティ保護	暗号化
	ボード・レベル・テスト	暗号化なし

表 14–2. サポートされるセキュリティ・モード （2 / 2）		
モード (1)	機能	コンフィギュレーション・ファイル
改ざん保護ビットがセットされた不揮発性キー	セキュリティ保護（改ざん防止）(2)	暗号化

表 14–2 の注 :

(1) キーなしでの動作では、暗号化されていないコンフィギュレーション・ファイルのみサポートされます。

(2) 改ざん防止ビットをセットしても、デバイスがリコンフィギュレーションされなくなることはありません。

サポートされているコンフィギュレーション手法

Stratix III デバイスは、暗号化する際に選択したセキュリティ・モードによっては、選択されたコンフィギュレーション手法しかサポートしない場合があります。

図 14–2 に、Stratix III デバイスを暗号化する際の各セキュリティ・モードの制約を示します。

図 14–2. Stratix III のセキュリティ・モード - シーケンスと制約

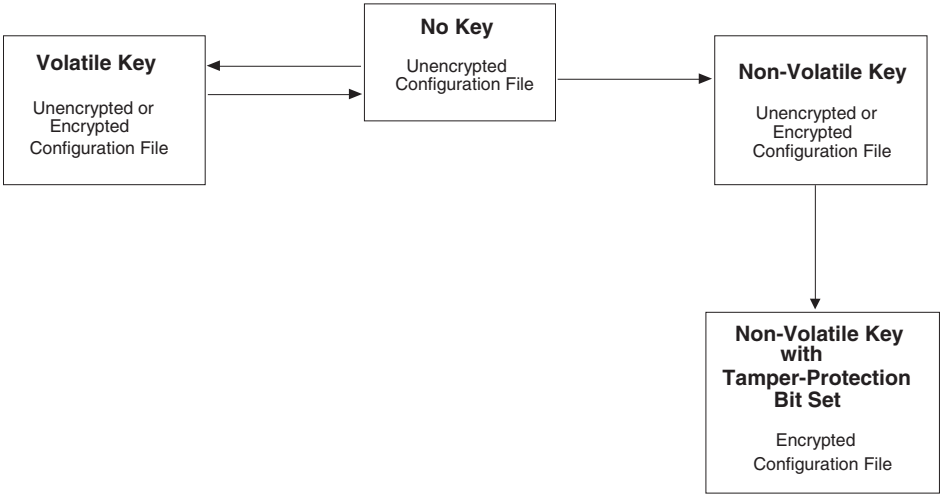

表 14–3 に、各セキュリティ・モードで許可されるコンフィギュレーション・モードを示します。

表 14–3. さまざまなセキュリティ・モードに対して許可されるコンフィギュレーション・モード 注 (1)（1 / 2）

セキュリティ・モード	コンフィギュレーション・ファイル	許可されるコンフィギュレーション・モード
キーなし	暗号化なし	デザイン・セキュリティ機能に関係しないすべてのコンフィギュレーション・モード
揮発性キーによるセキュリティ保護	暗号化	• AES を使用したパッシブ・シリアル（復元あり / なし） • AES を使用したファースト・パッシブ・パラレル（復元あり / なし） • AES を使用したリモート・アップデート・ファースト AS（復元あり / なし） • ファースト AS（復元あり / なし）
揮発性キーを用いたボード・レベル・テスト	暗号化なし	デザイン・セキュリティ機能に関係しないすべてのコンフィギュレーション・モード
不揮発性キーによるセキュリティ保護	暗号化	• AES を使用したパッシブ・シリアル（復元あり / なし） • AES を使用したファースト・パッシブ・パラレル（復元あり / なし） • AES を使用したリモート・アップデート・ファースト AS（復元あり / なし） • ファースト AS（復元あり / なし）
不揮発性キーを用いたボード・レベル・テスト	暗号化なし	デザイン・セキュリティ機能に関係しないすべてのコンフィギュレーション・モード

表 14–3. さまざまなセキュリティ・モードに対して許可される コンフィギュレーション・モード 注 (1)（2 / 2）

セキュリティ・モード	コンフィギュレーション・ファイル	許可される コンフィギュレーション・モード
改ざん保護ビットがセットされた不揮発性キーを使用した改ざん防止モードでのセキュリティ保護	暗号化	• AES を使用したパッシブ・シリアル（復元あり / なし） • AES を使用したファースト・パッシブ・パラレル（復元あり / なし） • AES を使用したリモート・アップデート・ファースト AS（復元あり / なし） • ファースト AS（復元あり / なし）

図 14–3 の注 :

(1) 暗号化されていないコンフィギュレーション・モードと比較すると、4 倍のデータ・レートの DCLK を必要とする、AES を使用したファースト・パッシブ・パラレル（復元あり / なし）を除き、所要コンフィギュレーション時間に対する影響はありません。

デザイン・セキュリティ機能は、JTAG コンフィギュレーション方法を除く、すべてのコンフィギュレーション方法で使用できます。したがって、デザイン・セキュリティ機能は、FPP モード（MAX II デバイスまたはマイクロプロセッサおよび Flash メモリのような外部コントローラを使用する場合）、またはファースト AS および PS コンフィギュレーション手法で使用できます。

表 14–4 に、揮発性キーおよび不揮発性キー両方のプログラミングのためのデザイン・セキュリティ機能をサポートする、コンフィギュレーション手法の概要を示します。

表 14–4. デザイン・セキュリティ・コンフィギュレーション手法の可用性

コンフィギュレーション手法	コンフィギュレーション方法	デザイン・セキュリティ
FPP	MAX II デバイスまたはマイクロプロセッサおよび Flash メモリ	√ (1)
	エンハンスド・コンフィギュレーション・デバイス	
ファースト AS	シリアル・コンフィギュレーション・デバイス	√
PS	MAX II デバイスまたはマイクロプロセッサおよび Flash メモリ	√
	ダウンロード・ケーブル	√
JTAG	MAX II デバイスまたはマイクロプロセッサおよび Flash メモリ	
	ダウンロード・ケーブル	

表 14–4 の注 :

(1) このモードでは、ホスト・システムは 4 倍のデータ・レートの DCLK を送信する必要があります。

デザイン・セキュリティ機能を、圧縮およびリモート・システム・アップグレード機能などのその他のコンフィギュレーション機能と一緒に使用することができます。デザイン・セキュリティ機能と一緒に圧縮を使用する場合、コンフィギュレーション・ファイルが最初に圧縮され、次に Quartus II ソフトウェアを使用して暗号化されます。コンフィギュレーションの間、Stratix III デバイスは、最初にコンフィギュレーション・ファイルを復号化し、次にそれを復元します。

まとめ

デバイスがグルー・ロジックから条件の厳しいシステム機能の実装に移行するにつれて、デザイン・セキュリティの必要性が高まっています。Stratix III デバイスは、ビルトイン・デザイン・セキュリティを提供することによってこの問題に対処しています。これらのデバイスは、高集積、高性能、かつ最先端の機能を提供して、デザインのニーズに対応するだけでなく、IP の盗用やコンフィギュレーション・ファイルの改ざんからデザインを保護します。

改訂履歴

表 14–5 に、本資料の改訂履歴を示します。

表 14–5. 改訂履歴

日付 & ドキュメント・バージョン	変更内容	概要
2006 年 11 月 v1.0	初版	