

# AES暗号処理方式 IPセキュリティ・システム

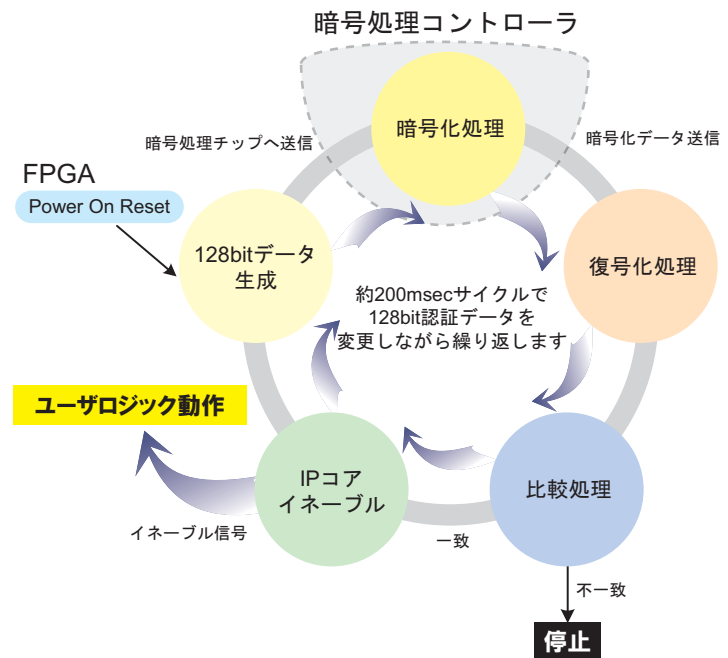
# IP Lock



IP Lock は信頼性の極めて高いAES暗号技術を採用したFPGAロジックセキュリティ・システムです。IP LockをFPGAに組み込み、暗号処理コントローラチップと接続するだけで、お客様の重要なFPGA内のIP資産を不法な複製からプロテクトします。

## 特長

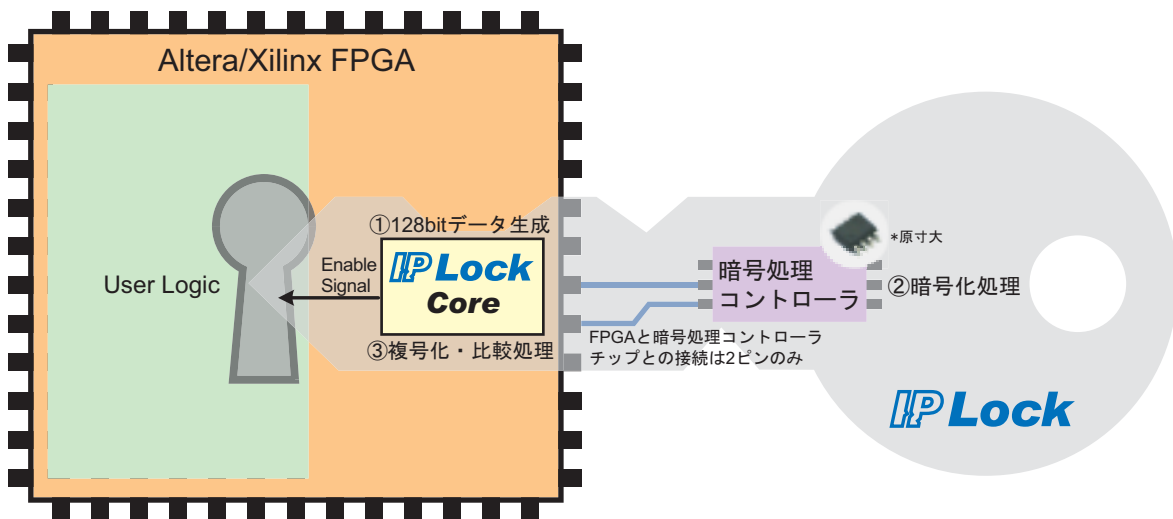
- AES暗号方式による強固なセキュリティ
- 約200msec周期で認証データを変更・暗号化
- 自然乱数発生回路により、真にランダムな認証データの生成を実現
- 暗号処理チップを外すとロジックの一部あるいはすべての機能が停止
- 接続に必要なFPGAのI/Oは2ピンのみ
- IP Lockロジックへのクロック入力不要
- 手軽なラボラトリーズパックとIP Lockライター+ブランクチップをラインナップ



IP Lock 暗号/復号化処理フローチャート

## AES暗号方式

AES(Advanced Encryption Standard)は米国標準技術局により選定された共通鍵暗号化方式です。暗号化・復号化が高速、トリプルDESより強固である点が特徴で、DESに代わる次世代の暗号標準として注目されています。現在では金融関係、LANのセキュリティ等で採用されています。

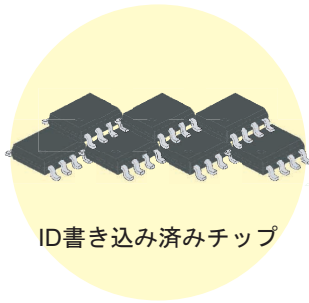


IP Lock ブロック図

## 使用方法

### ラボラトリーズパック

ラボラトリーズパックは出荷時にユーザ専用のIDが暗号処理チップにあらかじめ書き込まれているので、少量使用に最適です。



ID書き込み済みチップ

デザイン・ゲートウェイにて各パックごとにユニークのIDを書き込み済み

### IP Lockライター+ブランクチップ



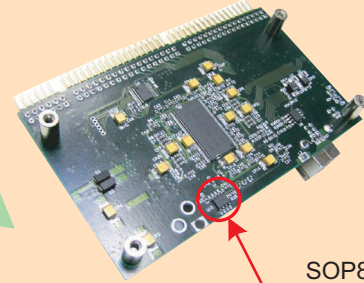
IP Lockライター IPL-003WR

IPL-CHP \*原寸大

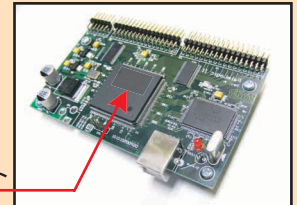
IP Lockライターでブランクチップにお客様任意のIDを書き込み

IP Lockライターでブランクチップに任意のIDを書き込むことができます。IP Lockライターごとに固有のIDを持つため、他のIP Lockライターで同じキーを指定しても、異なるIDが書き込まれます。製品版搭載時や複数製品にIP Lockを搭載する場合に最適です。

### IP Lock実装例



Step1:  
SOP8ピンパッケージ  
暗号処理チップを実装



Step2:  
IP Lock コアを  
FPGAにインプリメント

## 仕様

■名称	IP Lock (アイピーロック)	
■暗号方式	AES-128 暗号方式	
■IP Lockコア消費リソース	約1,200LE / 約24,500メモリビット 約400スライス / 2ブロックRAM	(Altera社FPGA使用時) (Xilinx社FPGA使用時)
■暗号処理コントローラ	SOP8ピンパッケージ FPGAとの接続に2本のI/O使用 クロック入力不要	
■付属品	<ul style="list-style-type: none"> <li>● IP Lock 暗号処理コントローラチップ</li> <li>● IP Lockコア ネットリスト</li> <li>● ユーザマニュアル</li> <li>● ID書き込みソフトウェア(Windows版、IP LockライターIPL-003WRのみ付属)</li> </ul>	
■型番	<ul style="list-style-type: none"> <li>● IP Lock ラボラトリーズパック                             <ul style="list-style-type: none"> <li>IPL-010L IPコアネットリスト + 暗号処理コントローラチップ10個パック</li> <li>IPL-030L IPコアネットリスト + 暗号処理コントローラチップ30個パック</li> </ul> </li> <li>● IP Lockライター                             <ul style="list-style-type: none"> <li>IPL-003WR IP Lockライター (IPL-CHP 3個付属)</li> <li>IPL-CHP IP Lockライター専用ブランクチップ (最低発注数量100個単位)</li> </ul> </li> </ul>	

※記載の会社名、製品名はそれぞれの登録商標または商標です。  
※仕様は予告無く変更される可能性があります。