IP Lock ライタ [IPL-003WR]取扱い説明書 [Ver2.0]

目次

はじめに

この度は AES 暗号処理方式・IP セキュリティシステム「IP Lock ライタ[IPL-003WR]」をご採用頂き誠にありがとうございます。本 IPL-003WR (以下、IP Lock ライタセットとします)は、信頼性の極めて高い AES 暗号処理技術を採用した FPGA ロジックセキュリティです。IP Lock コアを FPGA に組み込み、IP Lock ライタで任意の ID を書き込んだ暗号処理コントローラチップ(以下、暗号処理チップ)と接続するだけで、お客様の重要な FPGA 内の IP 資産をプロテクトします。

本 IP Lock ライタセットは、ブランクの暗号処理チップにお客様任意のユーザ ID を書き込むためのものですので、別途ブランクの暗号処理チップ(IPL-CHP)をご購入する必要があります。尚、本製品にはユーザ ID 未書き込みのブランク暗号処理チップが 3 個付属しております。

パッケージ内容

IP Lock ライタセットのパッケージ内容は下記のとおりです。

- IP Lock ライタ　1 個
- 暗号処理チップ　3 個 (ユーザ ID 未書き込み)
- USB ケーブル　1 個
- CD-ROM　1 枚
  - IP Lock ソフトウェア/デバイスドライバインストーラ(setup.exe)
  - Altera 社製 FPGA 用 IP Lock コア (TopIPLock.vhd, iplock.vhd)
  - Xilinx 社製 FPGA 用 IP Lock コア (TopIPLock.vhd, iplock.ngc , iplockex.ngo)
  - VHDL デザイン例ソースコード (Counter.vhd, Counter32Bits.vhd)
  - IP Lock 取扱説明書 (IPL-WR-MAN-Vx.xJ.pdf、本ファイル)

システム環境

IP Lock ライタセットご使用にあたり、下記の環境を用意してください。

- PentiumIII 互換 CPU 以上搭載の Windows PC (対応 OS: XP, Vista, 7)
- USB ポート
- FPGA デザインツール。Xilinx ISE 7.1 以降(Xilinx) あるいは Quartus II 4.1 以降(Altera)

使用上の注意事項

IP Lock の使用時は以下の注意事項を厳守してください。

[1] 本 IP Lock ライタセット付属の暗号処理チップは、出荷時に ID があらかじめ書き込まれておりませんので、IP Lock ライタを使用して ID を書き込んでください。

[2] IP Lock ライタにはユニークのライタ ID が埋め込まれており、ユーザ ID を暗号処理チップに書き込む際共に書き込まれます。したがって、異なる IP Lock ライタで同一ユーザ ID を書き込んだ場合は ID 不一致とみなされ、回路は動作しません。必ず IP Lock ライタと同一パッケージに付属の IP Lock コアを組み込んでください。

[3] 暗号処理チップの基板への実装の際は取り付け方向にご注意ください。

[4] 暗号処理チップの基板への実装の際は静電気にご注意ください。静電気はデバイスを破損する恐れがあります。

[5] 暗号処理チップの電圧範囲は 2.5 あるいは 3.3V です。電源の誤使用によるモジュール破損は保証/交換の対象とはなりませんのでご注意ください。

[6] Altera 社製 FPGA をご使用する場合には別途弊社にライセンスファイルを申請する必要があります。登録に必要な事項を弊社 IP Lock サポート(iplock@design-gateway.com)までメールにてお知らせください。

[個人情報の取り扱いについて]

お知らせ頂く情報はライセンスファイル発行の必要情報として厳重に管理されます。ほかの目的に利用されたり第三者に譲渡されることはありません。

システム概要

IP Lock コアはユーザ鍵(ID)を確認しながら暗号処理チップと通信します。ID と一致すれば IP Lock コアはイネーブル信号(1)を出力します。一致しない場合はディセーブル(0)となります。このイネーブル信号をユーザロジックに対して出力させることにより、ID が一致するときのみユーザロジックを動作可能にさせることができます。 図 1 に IP Lock システムのブロック図を示します。FPGA と暗号処理チップは、DC0 および DD0 の 2 本の信号線で接続します。IP Lock コア自体の動作クロックとして、SC0 をユーザロジックより供給する必要があります。この SC0 の周波数は 1-25MHz の範囲となるクロックを供給してください。

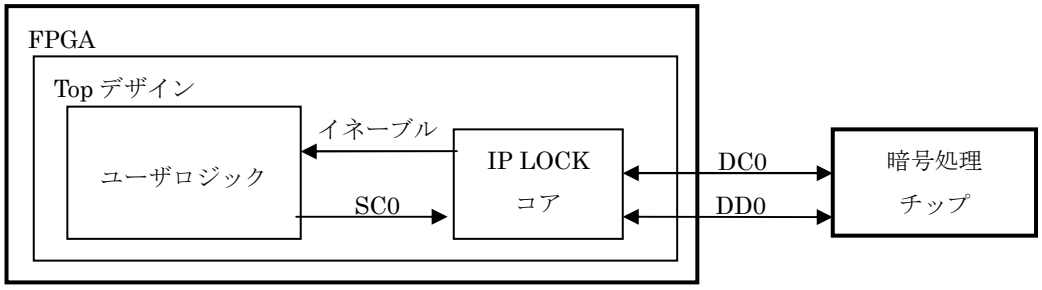

図 1 IP Lock システムブロック図

IP Lock コアからのイネーブル信号は SC0 に同期して出力されますが、ユーザロジック側のシステムクロックが SC0 と異なる場合、イネーブル信号を同期化する必要があります。この場合、下図 2 のように D フリップフロップをユーザロジック内に追加し、必ずユーザクロックと同期させた後のイネーブル信号を使ってください。

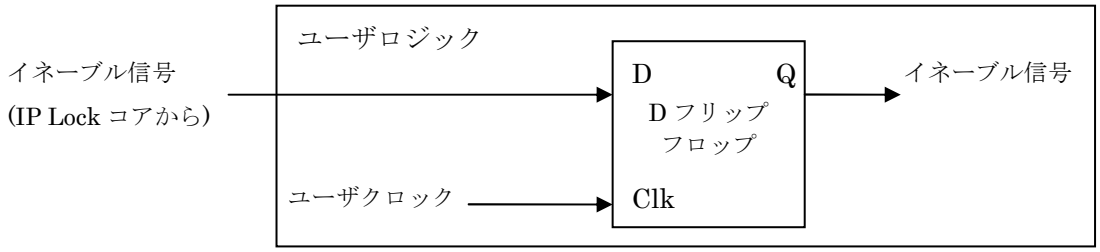

図 2 イネーブル信号の同期

IP Lock コア

図 3 に IP Lock コアのトップレベルのブロック図を示します。

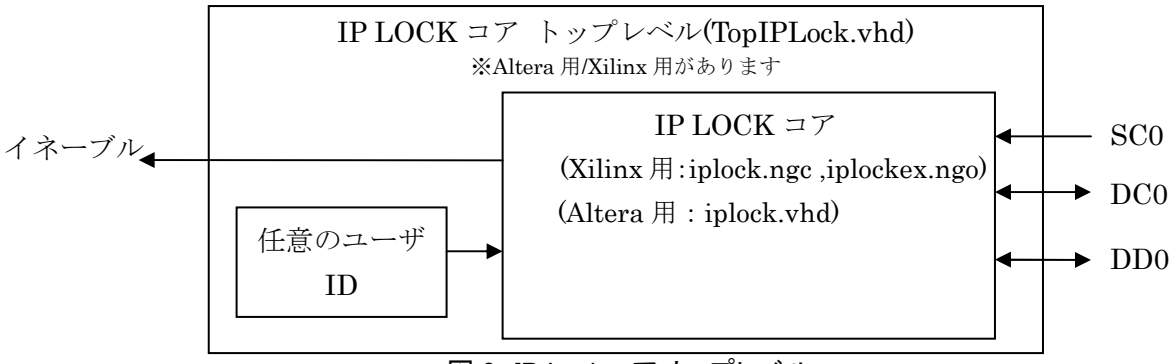

図 3 IP Lock コア トップレベル

IP Lock コア(Xilinx 用:ipLock.ngc, ipLockex.ngo / Altera 用:iplock.vhd)は ID を確認するため暗号処理チップと通信します。ID が一致した時のみ、イネーブル信号を出力します。

ユーザ ID の値はブランクチップに書き込む値と同じ値を設定してください。

■**Xilinx ユーザ**:

ipLock.ngc, ipLockex.ngo 両ファイルを Xilinx プロジェクトフォルダにコピーし、HDL コードを合成・インプリメントしてください。

■**Altera ユーザ**:

Altera 用 IP Lock コアは暗号化されているため HDL コードを合成・インプリメントする前に、IP Lock ライセンスを QuartusII ライセンスに追加する必要があります。

IP Lock のライセンスファイルは、弊社 IP Lock サポートにメールにて登録頂くことにより発行致します。登録に必要な事項を弊社 IP Lock サポート(iplock@design-gateway.com)までメールにてお知らせください。

Altera ユーザ用 IP Lock ライセンス取得の流れ:

1. デザイン・ゲートウェイ IP Lock サポートに下記情報をメールにて通知してください。
   宛先のメールアドレスは、iplock@design-gateway.comです。

氏名：.....
会社名：.....
IP Lock シリアル番号: (ケースおよびCD-ROMに記載).....
ボリュームシリアル番号：.....
住所：.....
Tel /Fax： .....

図 4 ライセンスファイル発行 登録事項

Windows のインストールされているドライブのボリュームシリアル番号をお知らせください。ボリュームシリアル番号は、DOS プロンプトの"dir"コマンドで知ることができます。表示方法を図 5 に示します。

```
C:¥>dir
ドライブ C のボリュームラベルがありません。
ボリューム シリアル番号は A035-6978 です

C:¥ のディレクトリ
2005/06/01210:33              0 AUTOEXEC.BAT
2005/06/01210:33              0 CONFIG.SYS
```

図 5 ボリュームシリアル番号の表示

2. デザイン・ゲートウェイは IP Lock ライセンスを発行し、2 営業日以内にお客様へメールにて返送します。
3. Quartus II のライセンスファイルをノートパッド等で開き、受け取った IP Lock ライセンスを図 6 のように追加してください。

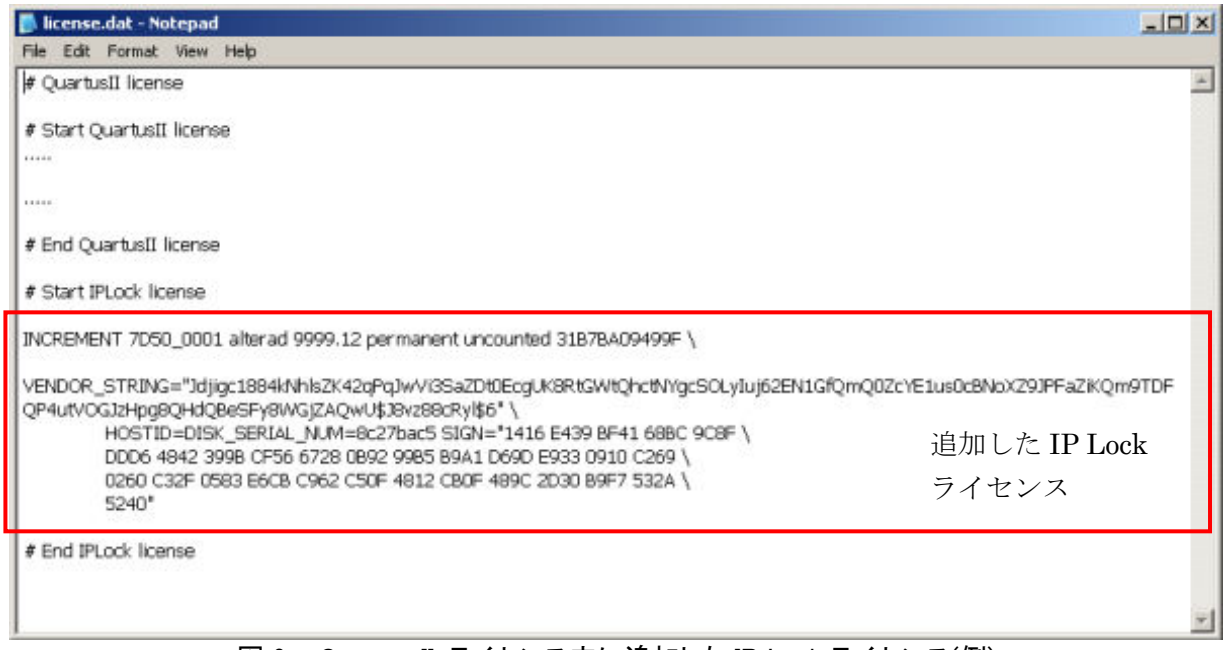

図 6 Quartus II ライセンス内に追加した IP Lock ライセンス(例)

ユーザロジックのユーザ ID 設定/変更方法

ユーザロジックソースコードのユーザ ID を任意の定数で設定/変更することができます。定数は 32 ビットバイナリまたは 8 桁の 16 進数で指定してください。図 7 に 16 進数でユーザ ID を指定した例を示します。

■注記: IP Lock ユーザ ID 書き込み用ソフトウェアソフトウェアは 16 進数(HEX)でユーザ ID を入力する仕様になっておりますので、ここでのユーザ ID の指定も 16 進数で行なうことにより、同一 ID であることの確認が容易になります。

```
-- IP Lock core
Component TopIPLock is
    Port (
      USERID                : in  std_logic_vector(31 downto 0);
      SCO                   : in  std_logic;
      DCO                   : inout  std_logic;
      DDO                   : inout  std_logic;
      ENABLE                : out std_logic
   );
End Component TopIPLock;

-- User's Logic
Component Counter32Bits Is
    Port (
      SysClk                : in  std_logic;
      SysRstB               : in  std_logic;
      Enable                : in  std_logic;
      LED                   : out std_logic_vector(3 downto 0)
   );
End Component Counter32Bits;

------------------------------------------------------------------------------
-------------------------- Constant Declareation -----------------------------
------------------------------------------------------------------------------
constant cUSERID            : std_logic_vector(31 downto 0) := x"00000000";

------------------------------------------------------------------------------
-------------------------- Signal Declareation -------------------------------
------------------------------------------------------------------------------
signal   rEnable              : std_logic;

Begin
------------------------------------------------------------------------------
-------------------------- Component Mapping ---------------------------------
------------------------------------------------------------------------------
```

図 7 ユーザロジックソースコード内のユーザ ID の設定

暗号処理チップ回路図

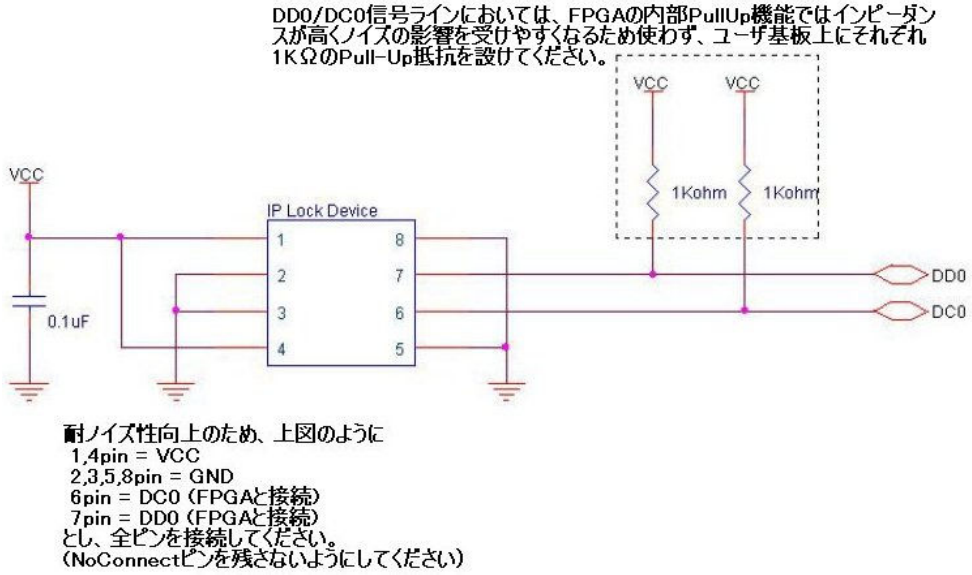

図 8　暗号処理チップ回路例

FPGA と暗号処理チップとの接続には DC0 および DD0 の 2 本の信号線を必要とします。図 8 に暗号処理チップの推奨回路図を示します。

DC0 および DD0 はプルアップし FPGA の I/O ピンと接続し、更に基板上に 1KΩ の PullUp 抵抗を実装してください。FPGA の内蔵 Pull-Up 機能はインピーダンスが高く外来ノイズの影響による誤動作の恐れがありますので使わないでください。 暗号処理チップの適正電圧は 2.5V または 3.3V です。接続する FPGA の I/O ピンと同じレベルの電圧を印加してください。

暗号処理チップの 1,4 ピンは VCC に、2,3,5,8 ピンは GND に接続してください。

暗号処理チップ寸法、電気的特性

暗号処理チップは SOP8 ピンパッケージです。図 9 にパッケージの外形寸法を示します。

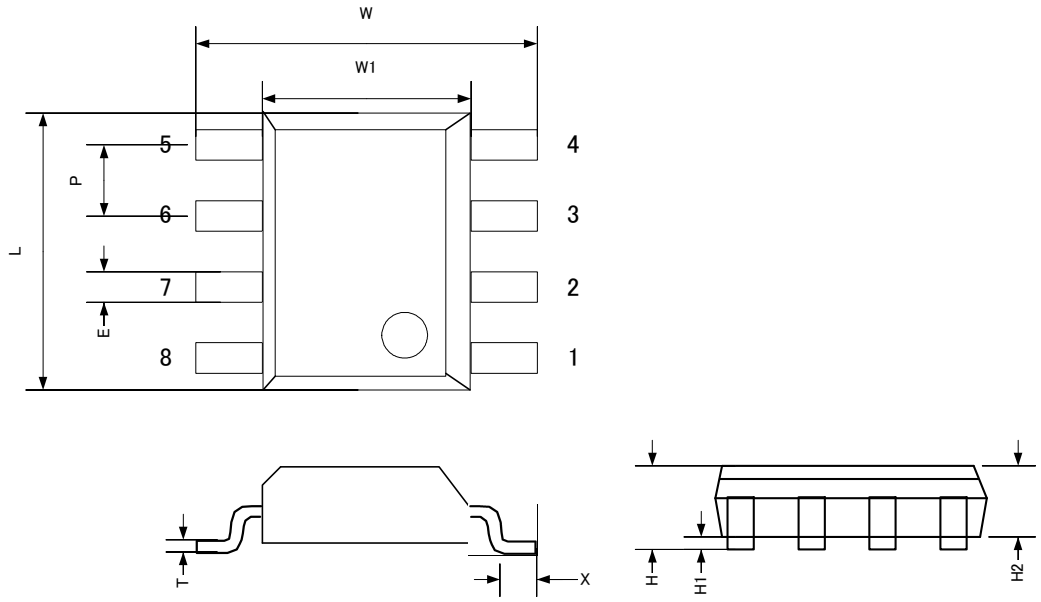

図 9　暗号処理チップ　パッケージ外形寸法図

表　暗号処理チップ　パッケージ各部寸法(単位:mm)

項目	記号	最小	平均	最大
実装時高さ	H	1.35	1.55	1.75
スタンドオフ	H1	0.10	0.18	0.25
パッケージ厚	H2	1.32	1.42	1.55
チップ全体幅	W	5.79	6.02	6.20
パッケージ幅	W1	3.70	3.91	4.00
パッケージ長さ	L	4.80	4.90	5.00
ピンのリード・ピッチ	P		1.27	
ピンのリード幅	E	0.33	0.42	0.51
ピンのリード厚	T	0.20	0.23	0.25
ピンのフット長	X	0.48	0.62	0.76

暗号処理チップの電気特性を下記に示します。

[絶対最大定格]
保存温度:　−40℃～+125℃
動作温度:　−20℃～+85℃
電圧範囲:　−0.3V～+3.3V

[推奨動作条件]
動作温度範囲:　0℃～+70℃
動作電圧範囲:　2.5V 動作時　2.25V～2.75V
　　3.3V 動作時　3.0V～3.6V

暗号処理チップパターン寸法

図 10 に暗号処理チップの推奨フットパターン寸法を示します。

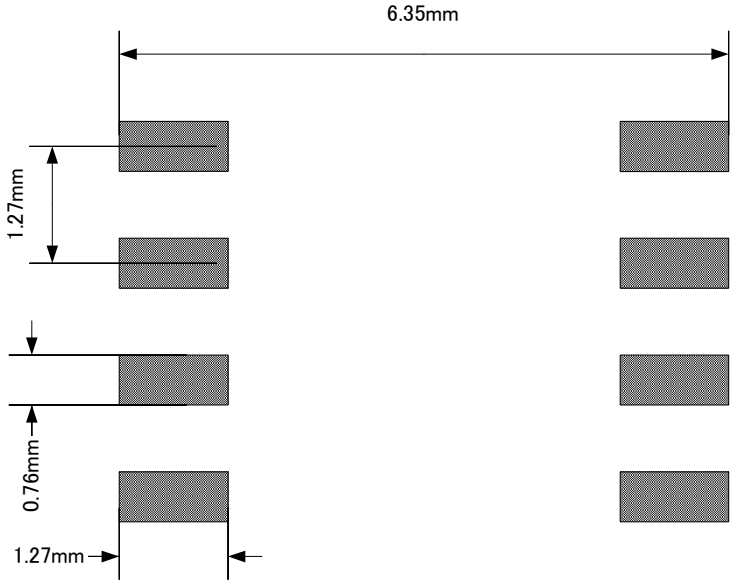

図 10　基板の推奨フットパターン寸法

IP Lock ライタ

IP Lock ライタにより、任意のユーザ ID(キー)をブランクの暗号処理チップ(以下ブランクチップ)に書き込みます。IP Lock ライタは USB Bus パワーより電源が供給されますので、外部からの電源供給は不要です。任意のユーザ ID(キー)を書き込むために、ブランクチップを IP Lock ライタのソケットにマウントしてください。マウント方向は 1 番ピン(マークされています)が IP Lock ライタの “LED status”側になるようにしてください。図 11 に IP Lock ライタを示します。

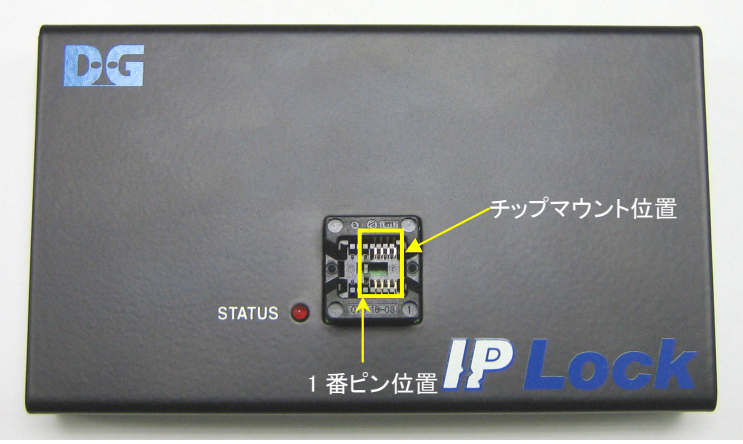

図 11　IP Lockライタ

ソフトウェア/デバイスドライバのインストール

下記の手順でソフトウェアおよびデバイスドライバをインストールしてください。

1. CD-ROM の IPLockSoftware フォルダを開き、setup.exe をクリックしてください。図 12 のようにセットアップ・ウィザードが起動しますので、「Next >」ボタンをクリックして次に進みます。

図 12　IP Lock ライタソフトウェア　セットアップ・ウィザード

1. 図 13 のダイアログでインストール先のフォルダを指定し「Next >」ボタンをクリックします(デフォルトは C:¥Program Files¥DesignGateway¥IPLockWriter)。
図 14 の確認画面で「Next >」ボタンをクリックすると、インストールを開始します。

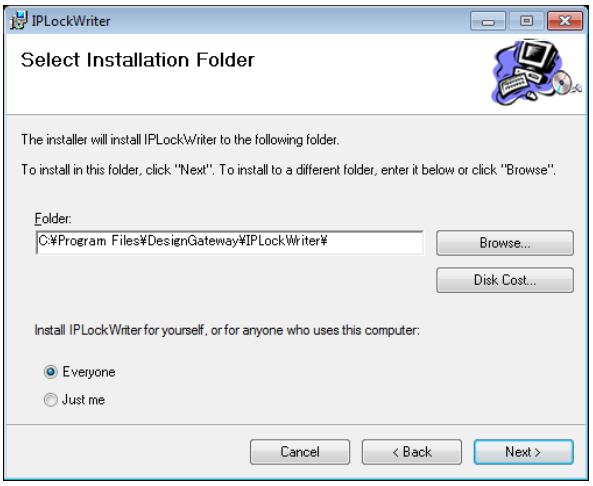

図 13 インストール先フォルダの指定

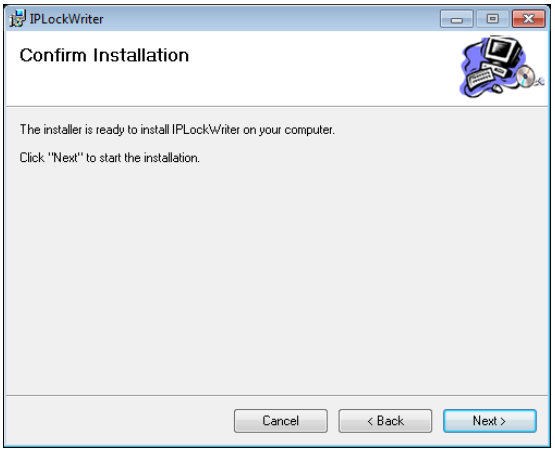

図 14 インストール確認画面

2. インストールが終了すると、図 15 のダイアログが表示されます。「Close」でインストーラを終了します。

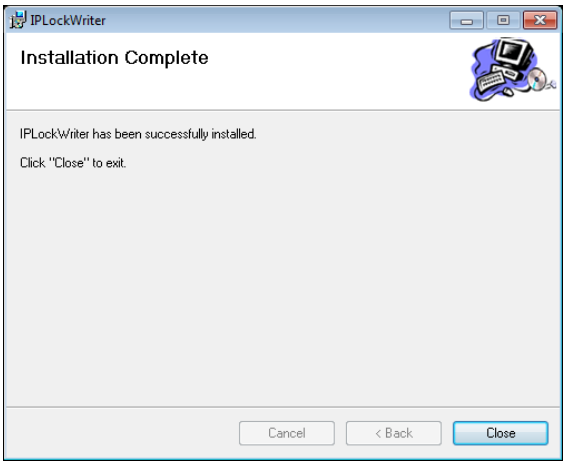

図 15 インストールの終了

3. IP Lock ライタを PC と USB 接続します。デバイスドライバをインストールするために、「Windows スタートボタン」→「コンピュータ(右クリック)」→「管理」→「デバイスマネージャー」を開くと、図 16 のように「ほかのデバイス」に、「IP LOCK WRITER Design Gateway」が検出されます。

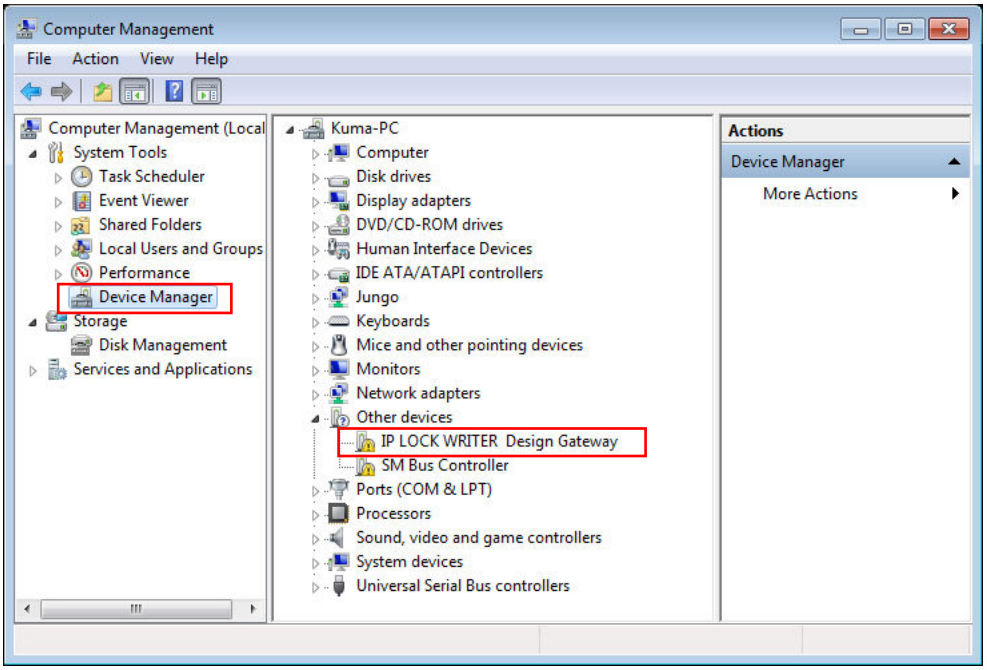

図 15 デバイスマネージャーで「IP LOCK WRITER Design Gateway」を検出

4. 「IP LOCK WRITER Design Gateway」をダブルクリックすると図 16 のようにプロパティが現れるので、「ドライバの更新」をクリックします。

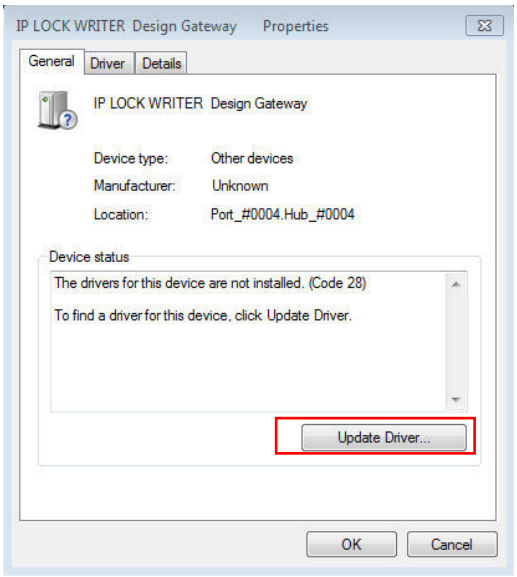

図 16 ドライバの更新

5. 図 17 のような画面が出てきますので、下の「コンピューターを参照してドライバーソフトウェアを検索します」を選択し、ソフトウェアをインストールしたフォルダ（C:¥Program Files¥DesignGateway¥IPLockWriter）を選択します（図 18）。Windows セキュリティの警告が出ることがありますが、インストールを続行してください。

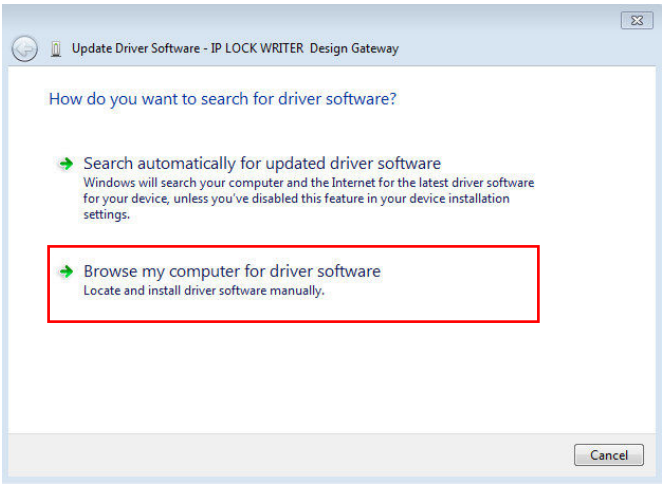

図 17 ドライバの検索

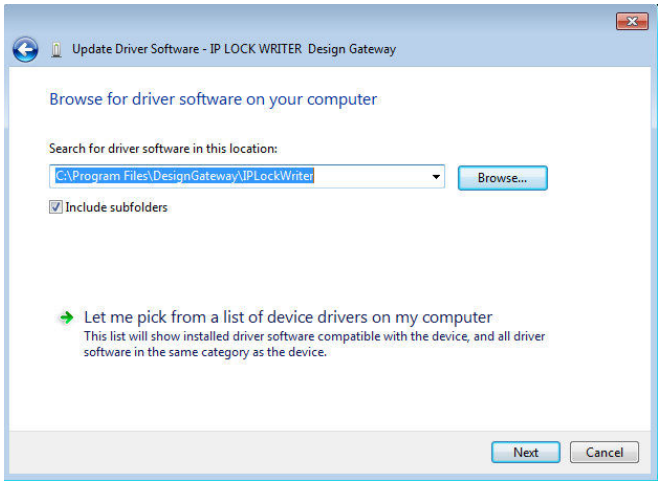

図 18 デバイスドライバ格納先を指定

6. インストールが正常に完了すると、IPLock ライタの赤 LED が消灯します。

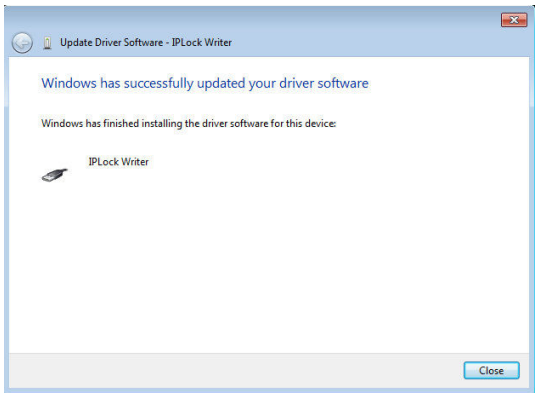

図 21 インストールの完了

IP Lock ユーザ ID 書き込み用ソフトウェア

ブランクチップへの書き込み制御は付属ソフトウェアから実行します。IP Lock 専用ソフトウェアから任意のユーザ ID(キー)とシリアルナンバーを入力し書き込むことができます。ここで書き込むユーザ ID はユーザロジックソースコード内(図 7)で指定した値と一致している必要があります。また、暗号処理チップにはユーザが任意のシリアルナンバーを 16 桁以内の 16 進数で書き込むことができます。このシリアルナンバーは、書き込みをおこなった IP Lock ライタで読み出すことが出来ますので、製品や数量の管理などにお役立てください。ユーザ ID およびシリアルナンバーの書き込みは一度限りですので、書き込む際には十分注意してください。

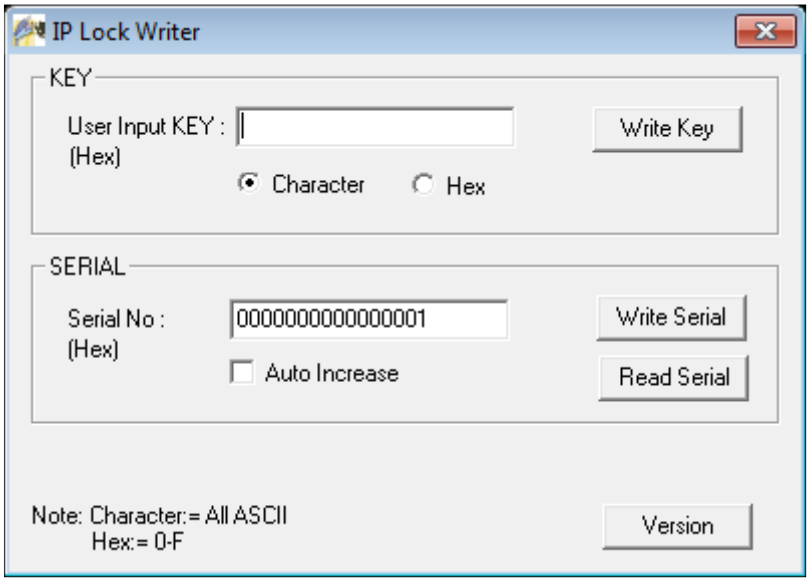

図 22 IP Lock ライタソフトウェア

1. ユーザ ID を入力する

User Input ID のボックスにユーザロジックソースコード(図7)で指定したユーザ ID 値を 8 文字以内の 16 進数(HEX)で入力します。デフォルト値は 0 です。

※8 文字以下の場合は上位桁が 0 の 8 桁として書き込まれます。(例:"1F3"を入力 → "000001F3")

※ ユーザ ID は書き込んだ後の読み出しは出来ません。また、書き込みは一度しか出来ませんので十分ご注意ください。

●「Write Key」ボタンを押すと、ユーザ ID を書き込みます。

2. シリアルナンバーを入力する

Serial No のボックスにシリアルナンバーとして書き込みたい値を入力します。16 桁以内の 16 進数(HEX)で入力します。デフォルト値は 0 です。シリアルナンバーの書き込みは必須ではありません。

「Auto Increase」をチェックすると、シリアルナンバーを書き込む毎に自動的にシリアルナンバーの値が 1 ずつインクリメントされます。

●「Write Serial」ボタンを押すと、シリアルナンバーを書き込みます。

●「Read Serial」ボタンを押すと、シリアルナンバーを読み出すことができます。

4. その他

● 「FW version」ボタンを押すと IP Lock ライタのファームウェアバージョンが表示されます。

VHDL デザイン例

CD-ROM には Counter.vhd と Counter32bits.vhd の 2 つのサンプルソースコードを収録しています。Counter.vhd は、ユーザロジックと IP LOCK コア トップレベル(TopIPLock.vhd)との接続方法を示すデザイン例です。Counter32bits.vhd は、IP Lock コアからのイネーブル信号をユーザロジックで使用するデザイン例です。図 23 に VHDL デザイン例のブロック図を示します。

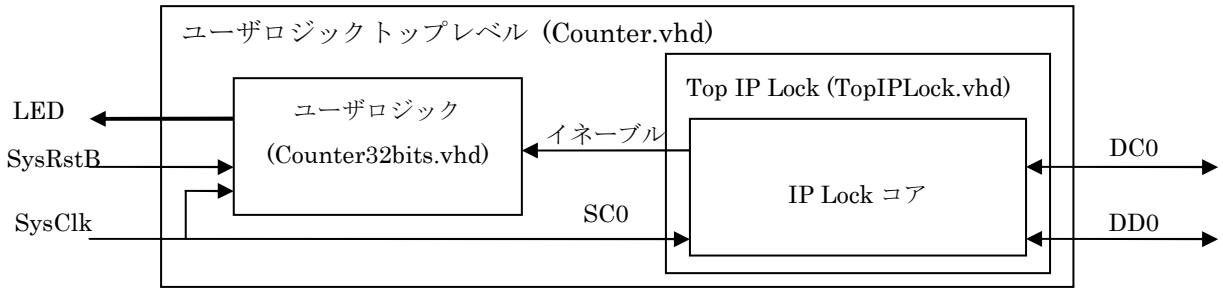

図 23 VHDL デザイン例 ブロック図

図 24、図 25 に VHDL デザイン例ソースファイルのインプリメントの方法を示します。

■**Xilinx ユーザ**:

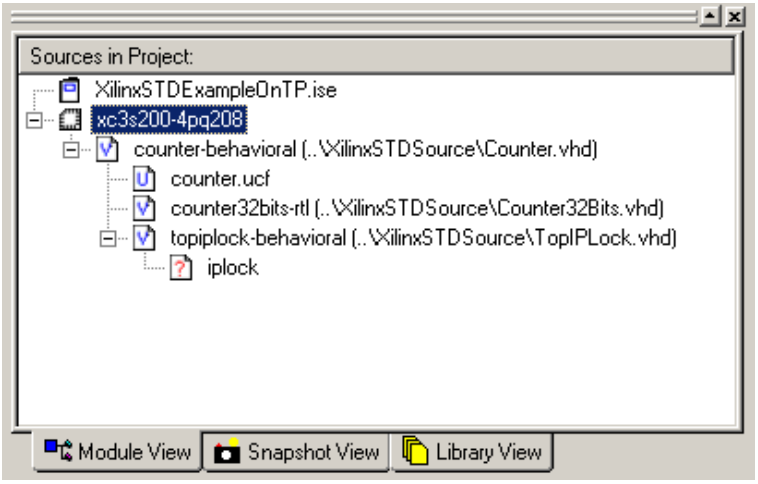

図 24　Xilinx ISE プロジェクトへのインプリメント例

■**Altera ユーザ**:

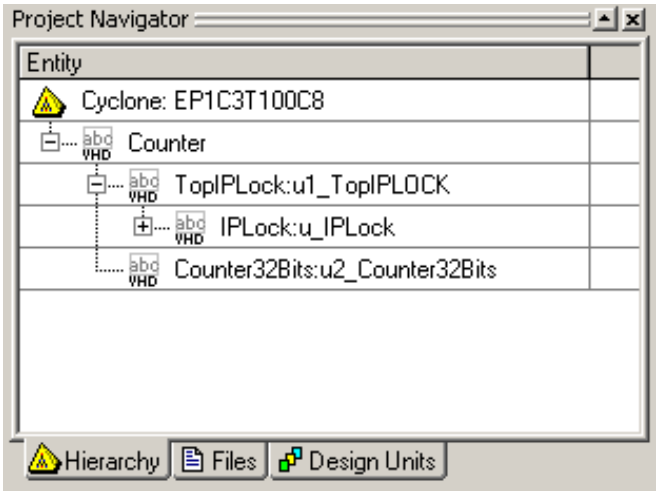

図 25　Quartus II プロジェクトへのインプリメント例

主な仕様

◆暗号方式: AES-128 暗号方式

◆消費リソース: 約 400 スライス/2 ブロック RAM (Xilinx),
約 1200LE/約 24,500 メモリビット(Altera)

◆IP Lock 機能: 暗号処理チップと ID が一致したときのみイネーブル出力、不一致の場合ディセーブル、ユーザロジックの機能(一部あるいはすべて)が停止
約 200msec サイクルで認証データを変更・暗号化

◆対応デバイス: **Xilinx**: Spartan-2, Spartan-2E, Spartan-3, Spartan-3E, Spartan-6
Virtex, Virtex-2/2Pro, Virtex-4, Virtex-5, Virtex-6, Virtex-7, Artix-7, Kintex-7
Altera: Stratix, Stratix2, Stratix3, Stratix4, Stratix5, ArriaGX, Arria2GX/GZ, Arria5
Cyclone, Cyclone2, Cyclone3, Cyclone4, Cyclone5
※2014 年 4 月現在。最新対応デバイスについては、弊社ホームページ IPLock-LIST.pdf をご確認下さい。

◆要求システム環境: Xilinx ISE 7.1 以上の FPGA デザインツール、あるいは
Altera QuartusII 4.1 以上の FPGA デザインツール

◆オプション: 「IP Lock ライタ IPL-003WR」を使用することにより、ブランクの暗号処理チップ(IPL-CHP、別売)に任意の ID を書き込むことができます。

免責事項

IP Lock の使用により生じたユーザ回路基板および基板上のデバイスの損害については免責事項とさせていただきます。また、IP Lock を改造して使用した場合の品質保証は致し兼ねます。

第 3 者によって IP Lock のセキュリティ・システムが逆解析されたことで生じたお客様の損失については免責事項とさせていただきます。

IP Lock のセキュリティ強度につきましては、応用製品を市場に投入される前に、ラボラトリーズパックや評価ボード等で、お客様にて十分なご評価を行っていただく必要があります。

[問い合わせ先]
URL : http://www.dgway.com
Email : info@dgway.com

■ お問い合わせの前に ■

暗号処理チップを FPGA と接続、IP Lock コアとユーザ回路が正常にコンパイルされ、FPGA に正常にダウンロードされたことを確かめた後、IP Lock が動作しない場合、下記の点をご確認ください。

- 暗号処理チップは正しい方向にマウントされていますか? 本取扱説明書「図 8 暗号処理チップ回路例」を確認し、適切な方向にマウントしてください。
- FPGA 内のピンアサインは適正ですか? 本取扱説明書「図 8 暗号処理チップ回路例」を確認し、適切なピンアサインをしてください。
- 暗号処理チップに適正な電圧が印加されていますか? 接続する FPGA の I/O ピンと同じレベルの電圧を印加 してください。尚、暗号処理チップの適正電圧は 2.5 あるいは 3.3V です。
- 暗号処理チップの DD0 と DC0 はプルアップされていますか? またプルアップ抵抗値は 1KΩ でしょうか?
- 暗号処理チップにユーザ ID を書き込んだ IP Lock ライタと同一パッケージに付属の IP Lock コアを使用していますか? IP Lock ライタはユニークのライタ ID を持っております。ユーザ ID を同一に設定しても、異なるセットの IP Lock コアを使用した場合 ID 不一致とみなされ、動作いたしません。
- 以上の点をご確認いただいても IP Lock が動作しない場合は弊社までお問い合わせください。