SASEBO-AES 暗号 FPGA ボード

仕様書

Version 1.3

2007 年 11 月 12 日

東北大学・産業技術総合研究所
暗号ハードウェア開発プロジェクト

目次

1. SASEBO-AES 暗号 FPGA ボード概要

SASEBO-AES は PowerPC プロセッサコアを内蔵した Xilinx 社の 2 つの FPGA (Field Programmable Gate Array) XC2VP7(以下 FPGA1)と XC2VP30(以下 FPGA2)を搭載したサイドチャネル攻撃評価用標準プラットフォームの FPGA ボード Side-channel Attack Standard Evaluation Board (以下 SASEBO)上に，128 ビット共通鍵ブロック暗号 AES (Advanced Encryption Standard)をハードウェア実装し，データの暗号化および復号を行うマルチチップ組込み型の暗号ハードウェアモジュールである．

図 1 に SASEBO-AES の概観を，また図 2 にブロック図を示す．図 2 で灰色に塗られた部分は，SASEBO-AES として未使用のコンポーネントを表している．2 つの FPGA のうち図 1 および 2 の左側のFPGA1 に AES とシリアルインタフェースが実装されており，右側の FPGA2 は RS232C シリアルポートの信号をスルーして FPGA1 に渡している．それぞれの FPGA には電源オン後に，コンフィギュレーション用の EEPROM である EEPROM1 (XCF08P)および EEPROM2 (XCF16P)から，ハードウェア設計情報が自動的にロードされるが，FPGA2 は FPGA1 と RS232C ポート間の結線だけが定義されており，論理回路は一切含まれていない．FPGA1 と FPGA2 では電源系統が左右に分離され，それぞれの電源入力端子に 3.3V を接続し，FPGA1 Power Selector を左側(INT)に，Main Power Switch を下側(ON)にスライドさせることで，レギュレータからそれぞれの FPGA に I/O 用 2.5V，コア用 1.8V の電力が供給される．なお，クロックも両者で独立しており，2 つのオシレータから基板の左右に別々に 24MHz が供給されるが，コンフィグレーション終了後の暗号処理時に FPGA2 はクロックを使用しない．

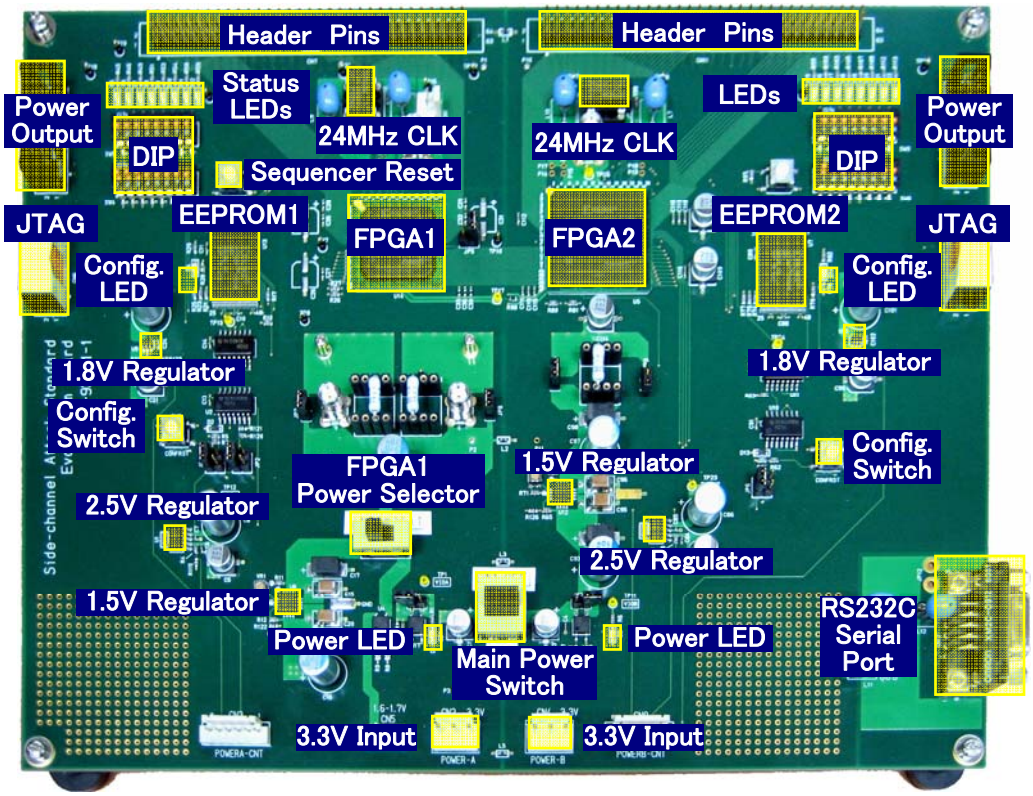

図 1 Side-channel Attack Standard Evaluation Board (SASEBO)の概観

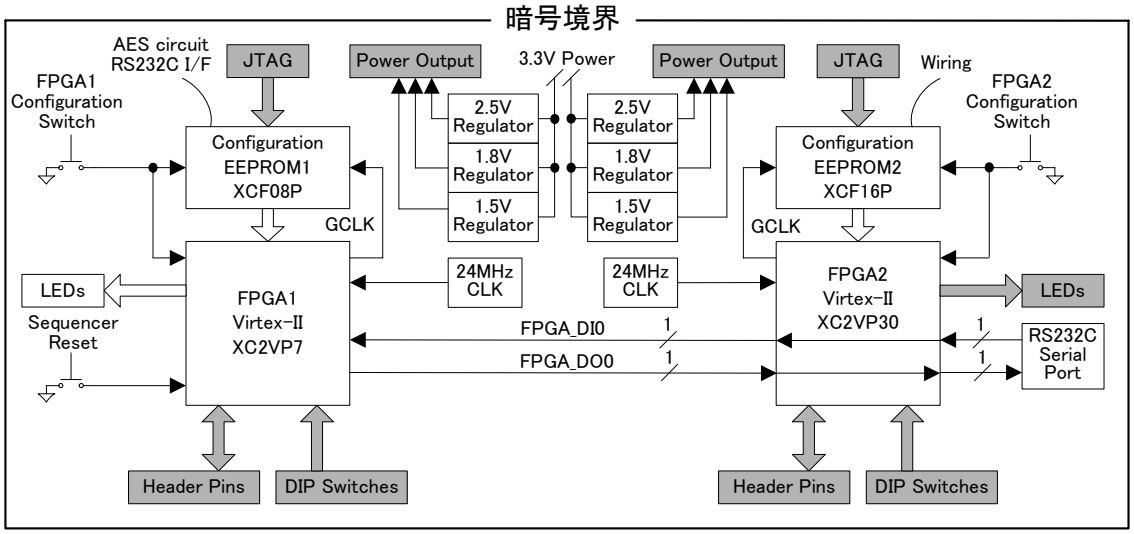

図 2 SASEBO-AES 暗号 FPGA ボードのブロック図

暗号境界は図 1 および図 2 のボード全体で，主要コンポーネントは FPGA1 と AES ハードウェアおよびシリアルインタフェース回路情報を保持する EEPROM1 の 2 つである．SASEBO に含まれる全てのコンポーネントと回路図は別冊の「サイドチャネル攻撃用標準評価基板仕様書」で提供される．

回路情報を保持する EEPROM1 および入出力ポートの結線情報のみを保持する EEPROM2 用の JTAG 端子には，第三者による設計情報の改ざんを防止するために，剥がすと痕跡の残るセキュリティシールが貼られている．FPGA1 と FPGA2 の間は，データ入力(FPGA1←FPGA2)および出力(FPGA1→FPGA2)用として，それぞれ 1 本ずつの信号線で結ばれており，入力線はコマンドおよび秘密鍵・データが，出力線はステータスおよびデータがシリアルに転送される．また外部の PC からは，RS232C ポートを通じて FPGA1 に対してこれらのコマンド/ステータス，鍵/データ入出力制御を行うことができる．FPGA1 に入力された秘密鍵は内部レジスタに保持され，FPGA1 の外部に出力されることはなく，また図1のボードの左側にある 2 つのプッシュスイッチ(Sequencer Reset および Config Switch)のいずれかを押すか，シリアルインタフェースを通じて Reset コマンドを与えるか，あるいは電源をオフにすることでゼロ化される．FPGA1 に接続された LED はエラー状態を示す外部表示装置としての役割を持ち，LED2 に接続された LED は未使用である．詳細は「2．ポート及びインタフェース」を参照のこと．FPGA1 および FPGA2 には他の入出力デバイスとして，電源出力，DIP スイッチ，ヘッダーピンを持つ．SASEBO-AES は様々な回路を後から実装できる汎用の FPGA ボードに AES 暗号回路を実装したものであり，EEPROM1 と EEPROM2 の内容を書き換えて他の用途として用いる場合に，その制御や外部回路を付加するためにこれらの入出力デバイスが用意されている．従って，今回は不要であるこれらのデバイスは SASEBO-AES では使用しておらず，図 2 では灰色のボックスとして示されている．

SASEBO-AES は共通鍵暗号 AES を使用しているので暗号化と復号は同じ 128 ビットの秘密鍵を使用するが，暗号化と復号で回路を分離しかつそれぞれのレジスタに同じ鍵をセットしている．これはレジスタへの鍵設定時に動作エラーが生じると被害が甚大なため，暗号化と復号の両回路で正しく暗号化→復号の処理が行われるかどうかを内部で自動的にテストするためである．

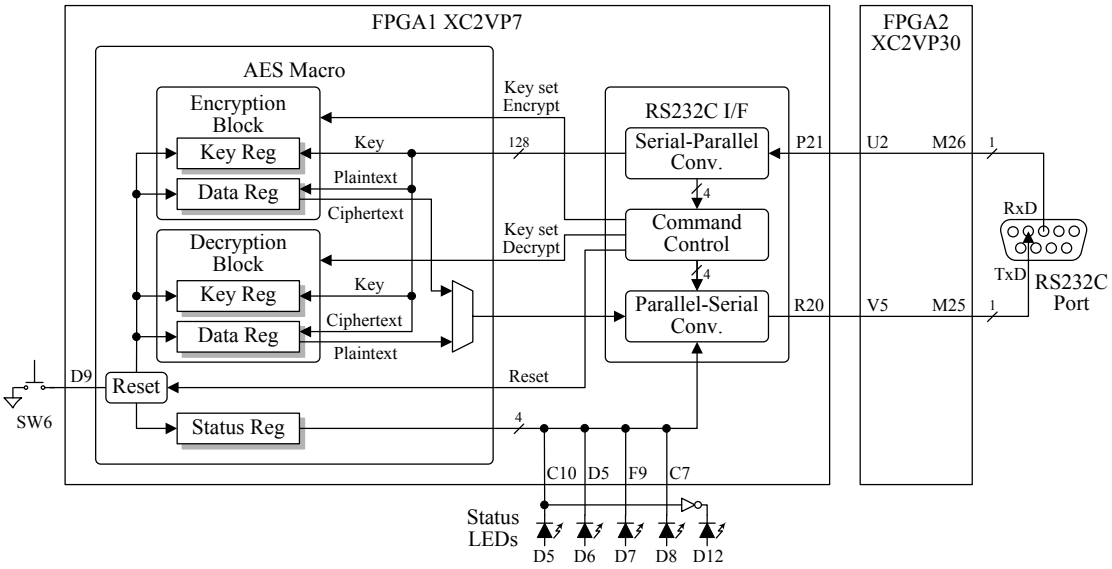

図 3 SASEBO-AES 暗号 FPGA ボードの制御およびデータの流れ

図 3 は，SASEBO-AES において，外部とのデータ入出力，制御入力，ステータス出力が SASEBO-AES においてどのような経路で行われるか，その概略を示したものである．FPGA1 および FPGA2 の入出力線には，それぞれの FPGA で定義されている I/O ピン番号を振ってある．また，リセットスイッチ SW6 とステータス LED の D5～D8,D12 はボード上に印字されている部品番号である．RS232C の RxD ピンには，3 章の「シリアルインタフェース」の図 11 で詳解する入力データフォーマットに従って，コマンド，鍵，平文または暗号文が 1 ビットずつ入力される．この信号は RS232C インタフェース回路のパラレルーシリアル変換回路を通じて，コマンドとデータが分離され，鍵は AES マクロの暗号化ブロックと復号ブロックそれぞれの鍵レジスタへ，また平文は暗号化ブロックのデータレジスタへ，暗号文は復号ブロックのデータレジスタへと書き込まれる．鍵レジスタは暗号化および復号ブロックの内部でのみ使用され，その情報が外部に出力されることはない．また，レジスタの内容はコマンドによるソフトウェアリセット，あるいはスイッチ SW6 の押下によるハードウェアリセットによってゼロ化される．

暗号化のコマンドが発行されると暗号化ブロックで処理が行われ，データレジスタに暗号文が得られた後にパラレルーシリアル変換回路を通り，図 12 の出力データフォーマットに従って RS232C ポートの TxD ピンから 1 ビットずつ出力される．このとき，データの先頭にはコマンドの種類を示す 4 ビットのコマンド情報とエラー状態を示す 4 ビットのステータス情報が付加される．復号時には復号ブロックによる処理が終わるとデータレジスタに平文が得られるので，暗号化と同様，コマンドとステータスと共に RS232C ポートから 1 ビットずつ出力される．なお 4 ビットのステータス情報は図 4 のように D5~D8 の 4 つの LED にも同じものが出力される（ビットが 1 のとき発光）．またエラーがない場合には D12 が発光する．

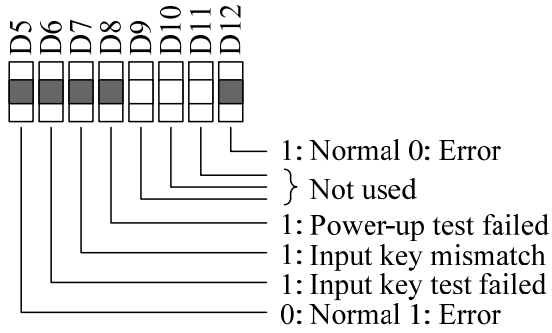

図 4 ステータス LED の意味

2. AES ハードウェアマクロ

本章では SASEBO-AES に実装された AES ハードウェアマクロを詳解する. このマクロは FPGA1 に実装され, データ入出力は同じ FPGA 上に実装された後述のシリアルインタフェースを通して行われる. 本章に示した I/O とタイミングチャートは AES マクロ単体のものであり, シリアルインタフェースでラップされた SASEBO-AES とは制御が異なることに注意されたい.

2.1 マクロ概要

本ハードウェアマクロは, FIPS-197 に規定された 128 ビットブロック暗号 Advanced Encryption Standard (AES)の暗号化・復号回路を Verilog-HDL で設計したものである. 鍵長は 128 ビット, またオペレーション・モードは ECB (Electronic Code Book)のみをサポートしている. 128 ビットの入力データバスは鍵と平文・暗号文データに兼用で, 128 ビット出力データバスは平文・暗号文専用である. 一旦マクロ内のレジスタに書き込まれた鍵は読み出すことはできない.

暗号化と復号はそれぞれ 11 サイクルを要し, かつ 11 サイクル毎にデータを供給することができる. 各サイクルで必要な 128 ビット×11 組のラウンド鍵は on-the-fly で入力された鍵から内部生成される. なお, 復号では 11 番目のラウンド鍵を事前に生成しておく必要があるが, これは鍵を入力すると自動的に生成される. マクロは内部に暗号化と復号に異なる 2 つのデータパスを持つ. レジスタも暗号化用と復号の 2 つが用意されており, ユーザはそれぞれに対して同じ秘密鍵を設定する必要がある. 両者は内部で自動的に比較され, まず鍵が誤りなく入力されたかどうかが内部でチェックされる. それに次いで 0 データの暗号化, そしてその暗号文の復号が行われて 0 に戻ることが確認された後に, データを入力待ちとなる.

リセット時にも暗号回路のアルゴリズムテストが行われるが, この時は内部でセットされた鍵が 1 ビットずつ 128 回巡回シフトされ, それぞれの鍵に対して暗号化と復号が行われ, 処理結果の検証が 128 回行われる. この処理には 4,863 サイクルを要する. 鍵入力時とリセット時のテストの結果, エラーが発生した場合はそれに応じてステータスフラグがセットされ, その状況によっては機能を停止する.

表 1 に本 AES マクロの概要を示す.

表 1 AES マクロの概要

アルゴリズム	Advanced Encryption Standard (FIPS-197)
ブロックデータ長	128 ビット
鍵長	128 ビット
利用モード	Electronic Code Book (ECB)
ハードウェア記述言語	Verilog-HDL
スループット	128 bit / 11 clock
ラウンド鍵	On-the-fly 自動生成
鍵テスト	2 回入力された鍵が一致しているかを検証 一致した鍵で暗号化と復号を行いデータがもとに戻ることを検証
アルゴリズムテスト	リセット後に暗号化と復号を繰り返して結果を比較

2.2 AES アルゴリズムとデータパスアーキテクチャ

まず図 5 と図 6 にそれぞれ，128 ビット鍵による AES の暗号と復号のアルゴリズムを示す．暗号処理では，入力された秘密鍵は右側の Key Generator によって 11 組のラウンド鍵に変換される．128 ビットの平文データはまず，4 行×4 列の 16 バイトのマトリクス状に並べられ，4 つの基本関数 SubBytes, ShiftRows, MixColumns そして AddRoundKey が繰返し適用される．復号では，各関数の逆関数，InvSubBytes, InvShiftRows, InvMixColumns そして AddRoundKey（逆関数は同一）が暗号化と逆順に実行される．

SubBytes はバイト単位の非線形変換 S-Box を 16 個集めたもので，ガロア体 GF(2^8)上の乗法逆元演算に続いてアフィン変換を行なう．復号の InvSubBytes では逆アフィン変換の後に逆元演算が行なわれる．AES のガロア体は次の既約多項式によって定義されている．

$$m(x) = x^8 + x^4 + x^3 + x + 1 \qquad (1)$$

ShiftRowsは各4×4バイト行列をバイト単位で行ごとに，あらかじめ決められたオフセット分巡回シフトする．InvShiftRowsは各行を逆方向にシフトする．

MixColumnsでは列方向の4バイトを4項式の各係数と見なして，次の多項式と乗じた後に x^4+1 による剰余を求める．

$$c(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\} \qquad (2)$$

また復号の逆演算InvMixColumnsでは次の多項式との乗算が行なわれる．

$$c^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\} \qquad (3)$$

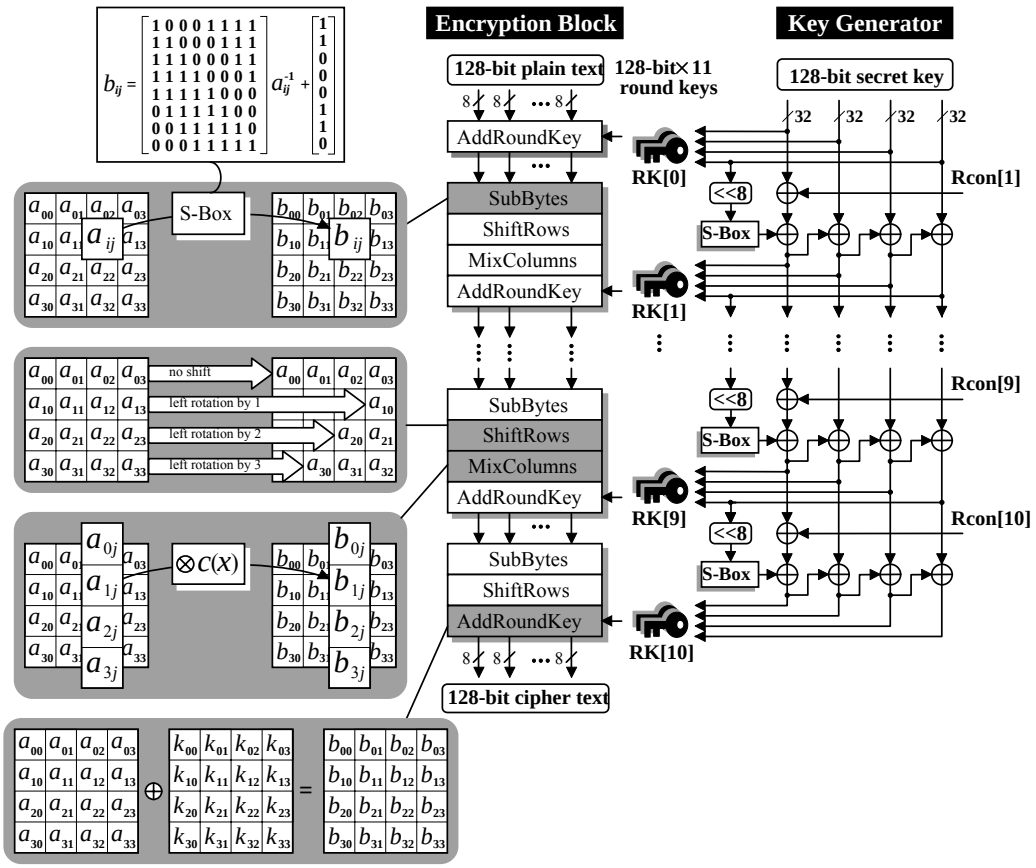

図 5 AES アルゴリズムの暗号化処理

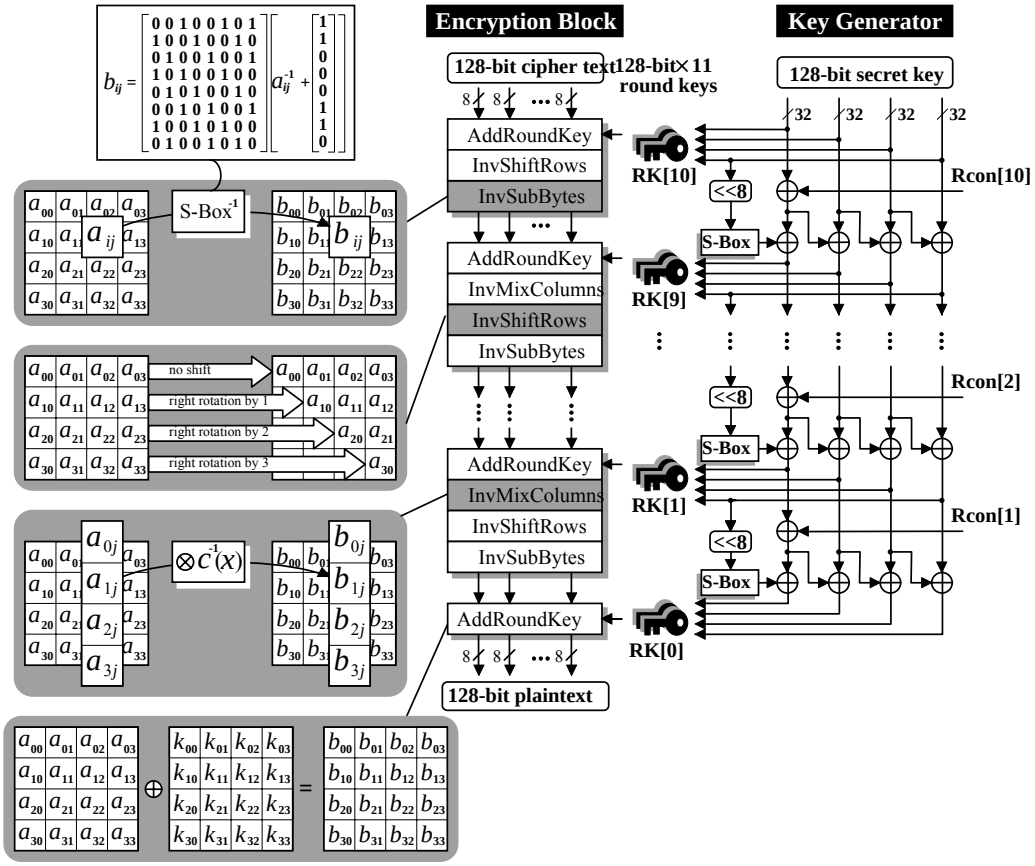

図 6　AES アルゴリズムの復号処理

図 7 と図 8 は本 AES マクロに含まれる，暗号化と復号の回路モジュールのデータパスアーキテクチャを示している．それぞれ 4 つの基本関数，<SubBytes, ShiftRows, MixColumns, AddRoundKey>と<InvSubBytes, InvShiftRows, InvMixColumns, AddRoundKey>の回路ブロックを 1 セット有し，それらのブロックを繰り返し使用して図 5 と図 6 のラウンド処理を実行するループアーキテクチャを採用している．128 ビットの秘密鍵は入力バス Key[127:0]を通じて，右上部の 4 つの 32 ビットレジスタ“Key Registers”にセットされる．秘密鍵は図 5 と 6 に示した 11 組のラウンド鍵 RK[0]~RK[11]に on-the-fly 変換され（RK[0]は秘密鍵と同一），AddRoundKey 関数に渡される．復号ではラウンド鍵を RK[11]~RK[0]の順番で使用するため，図 8 で“Key Registers”に秘密鍵(RK[0])がセットされると，11 サイクルを要して生成した RK[11]を“Key Registers”に再セットする．図 8 の復号回路の鍵スケジューラが，図 7 の暗号回路に比べて複雑なのは，初期設定時に RK[0]→RK[11]の順にラウンド鍵を生成するパスと，復号処理時に RK[11]→RK[0]の順に鍵生成を行うパスの 2 つが必要なためである．なお，図 7 と図 8 では鍵スケジューラのパスにループがあるが，これは図を簡略化したためで，実際のコードにループパスは存在しない．AES マクロのトップモジュールはこの暗号化回路と復号回路を制御して，鍵セット時の動作テストを自動的に行う．

図7において，128 ビットの平文データは Din[127:0]を通して入力され，“Key Register”内の RK[0]と XOR の後“Data Register”に保存される．このレジスタにセットされたデータは，ShiftRows→SubBytes→MixColumns→AddRoundKey のパスを 9 回ループした後に，10 ループ目で MixColumns(図では MxCo)をバイパスし，暗号文が Dout[127:0]に出力される．この出力バスは演算途中の内部状態がそのまま出力されてしまうため，この暗号回路を含む図 9 のトップモジュールには最終結果だけをラッチする出力レジスタを用意しており，途中結果が外部に漏れないようにブロックしている．

図 8 の復号回路においても図 7 と同様に，128 ビットの暗号文データはバス Din[127:0]から入力され，ラウンド鍵 RK[10]と XOR された後に“Data Register”にセットされる．レジスタの値は InvMixColumns→InvShiftRows→InvSubBytes→AddRoundKey のパスを 9 回ループして処理され，最後に InvMixColumns（図では $MxCo^{-1}$）をバイパスして平文が Dout[127:0]に出力される．図 7 の暗号回路と同様に，この出力バスには演算途中の内部状態がそのまま現れるため，トップモジュールに含まれる最終結果だけをラッチする出力レジスタが暗号回路とこの復号回路で共有され，途中結果が外部に漏れないようにしている．

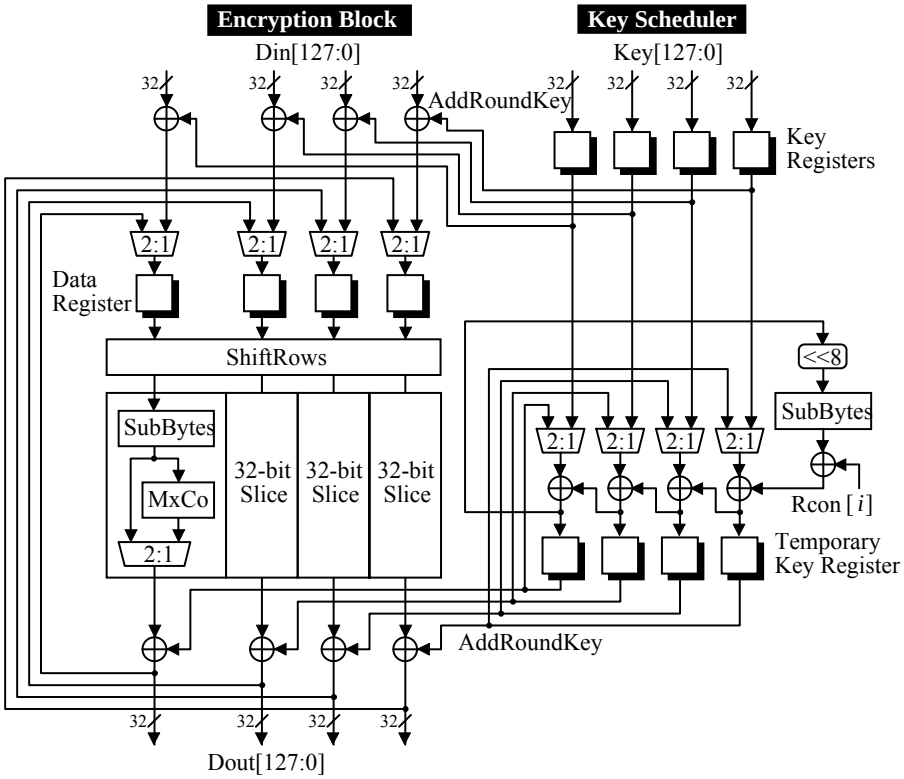

図7 暗号回路モジュールAES_ENCのデータパスアーキテクチャ

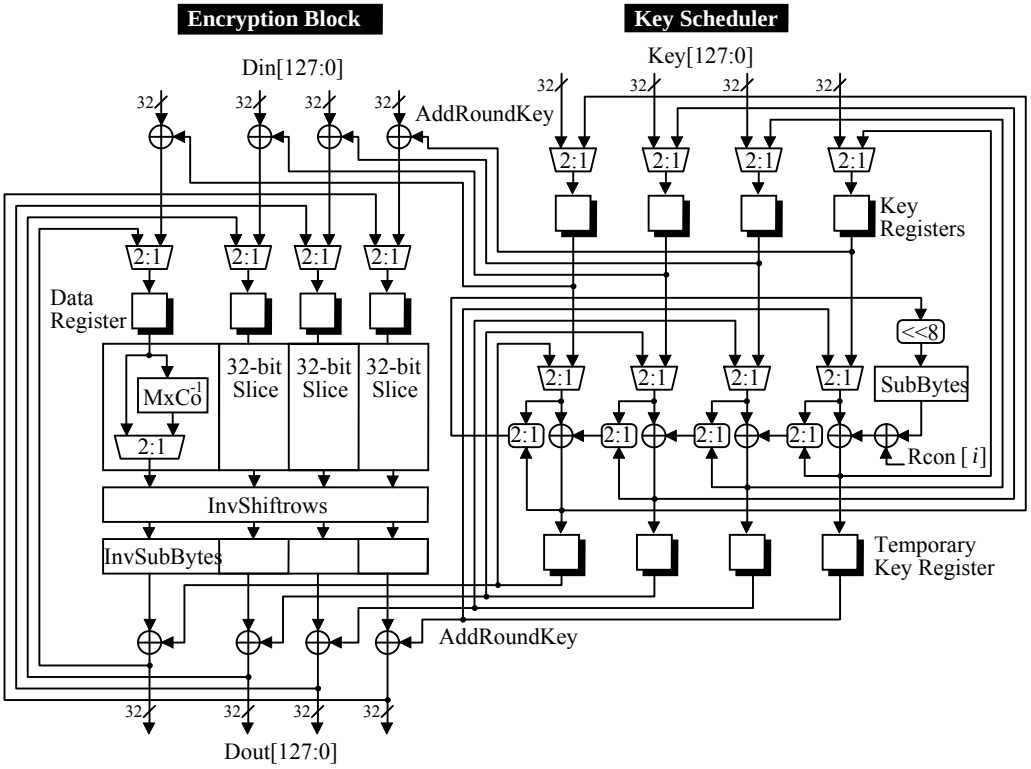

図8 復号回路モジュールAES_DECのデータパスアーキテクチャ

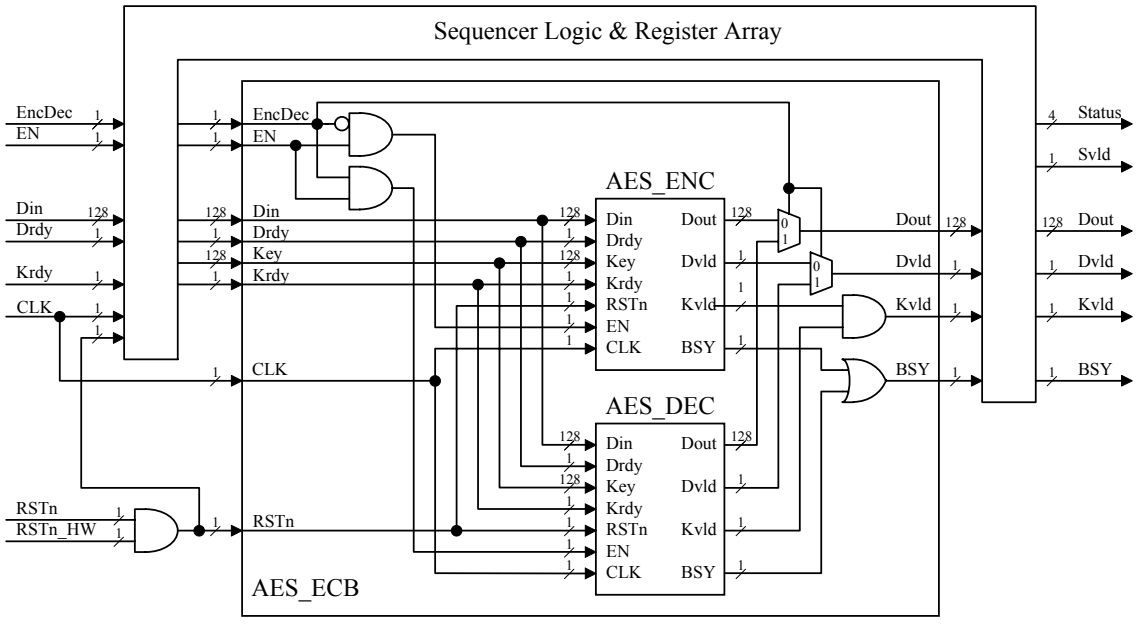

図9 トップモジュールAES_TOPの階層構造

図 9 は図 7 の暗号回路モジュール AES_ENC と図 8 の復号回路モジュール AES_DEC を含む，AES 回路のトップモジュール AES_TOP の階層構造を示している．なお公開されているソースコードに含まれるモジュールは以下の通りである．

SASEBO_AES.v
　モジュール AES_ENC と AES_DEC および，基本関数全て．本実装の SubBytes と InvSubBytes には合成体 GF(((2^2)^2)^2)上の逆元回路を用いているが，Look-up Table や PPRM を用いた関数も用意されている．

SASEBO_AES_TOP.v
　トップモジュール AES_TOP および AES_ECB を含む．

SASEBO_AES_AVS.v.
　NISTが定めた“The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)” (http://csrc.nist.gov/cryptval/aes/AESAVS.pdf)に対応した128ビット鍵のECBモードのテストベンチ．“6.4.1 Monte Carlo Test –ECB”, “Appendix B. GFSbox Know Answer Test Values”, “Appendix C. KeySbox Know Answer Test Values”, “Appendix D. VarTxt Known Answer Test Values”, “Appendix E. VarKey Known Answer Test Values”によってAESモジュールAES_TOPをテストする．

SASEBO_AES_AVS_DATA.txt
　AES_AVS.v から呼び出されるテストデータファイル．

暗号化と復号の ECB モードをサポートするモジュール AES_ECB では，AES_ENC と AES_DEC の入力信号がイネーブル信号 EN を除いて全て共通化されており，また出力信号も切り替えや AND/OR ロジック等によってまとめられている．2 つの暗号モジュールの切り替えは信号 EncDec によって行われ，AES_ECB への入力 EN=1 のときに EncDec=0 で暗号が，EncDec=1 で復号が行われる．2 つのマクロの 128 ビット出力 Dout と有効なデータが出力されていることを示す Dvld も，EncDec の値によって切り替えられる．また鍵が両方のマクロに正しくセットされると AES_ECB からの出力 Kvld=1 となり，いずれかのマクロが動作を始めると BUSY=1 となる．

トップモジュール AES_SASEBO は，リセットあるいは鍵セット時にアルゴリズムテストまたは鍵テストを行い，状況に応じてステータスを出力し，また暗号・復号中の途中結果が外部に漏れないように出力バッファを制御する．Low アクティブの 2 つのリセット信号 RSTn と RSTn_HW を持っているが，前者はコマンドによるソフトウェアリセットに，後者はハードウェアリセットに用いる．このトップモジュールの入出力信号の使用法を以下にまとめておく．

CLK
　システムクロック．出力をよび全ての内部信号はCLKの立ち上がりエッジに同期している．

RSTn
　イネーブル信号 EN の状態とは無関係に，1 クロック以上 0 に落とすことでシーケンサーおよび鍵レジスタをリセットする．またリセット後に RSTn=1 となると，アルゴリズムテストが自動的に始まる．テスト中は BUSY=1 となり，正常に終了するかエラーが検出されると，BUSY=0 となりそれぞれ鍵入力待ちまたは動作停止状態になる．エラーが発生した場合，ステータスレジスタの値は Status[3:0]=1001 となる．

RSTn_HW
　ハードウェア用リセット信号．機能は RSTn と同じ．

EN
　この信号を 1 にすることで，リセット以外の各種コマンドが実行可能となる．また 0 にすることで，リセット以外の処理を一時停止することができる．

BUSY

この信号が 1 のとき暗号モジュールが動作中であり，アルゴリズムテスト中はリセットのみ，それ以外の処理ではリセットとイネーブル信号 EN 以外の制御は無視される．

EncDec

暗号化と復号の切り替えを行う．0 のとき暗号化，1 のとき復号となる．

Din[127:0]

データおよび鍵用 128 ビット入力ポート．BUSY=0 のときに Drdy=1 ならばデータレジスタに，Krdy=1 ならば鍵レジスタにそれぞれ値がセットされる．2 つのレジスタへの同時書き込みはできず，Drdy と Krdy が共に 1 のときは鍵入力が優先される．データ用と鍵用に，暗号化と復号でそれぞれ別々のレジスタを持っており，EncDec=0 のときは平文あるいは鍵が暗号化専用のレジスタに，EncDec=1 では暗号文または鍵が専用のレジスタにセットされる．なお，鍵は必ず暗号化用と復号用の順に同じ値を 2 回セットしなければならない．さらに鍵セットが正しく行われて Kvald=1 となった状態でないと，データレジスタへの入力は受け付けられない．

Drdy

この信号が 1 かつ入力 EN=1，ステータス出力 Status[3:0]＝0000，BUSY=0，Krdy=0,Kvlid=1 のときに内部データレジスタに Din[127:0]の値がセットされる．

Krdy

この信号が 1 かつ入力 EN=1，ステータス出力 Status[3:0]＝0000 or 0010，Krdy=0,Kvlid=1 のときに内部鍵レジスタに Din[127:0]の値がセットされる．ただし，暗号化用の鍵に続いて復号用の鍵（両者は同一）をセットするため，EncDec=0 として暗号化用の鍵をセットした後は EncDec=1 にするまで Krdy は無視される．また，暗号化用の鍵をセットする前に EncDec=1 とした場合も Krdy は無視される．復号用の鍵がセットされると，既にセットされちる暗号化用の鍵と比較され，不一致であると Status[3:0]=0010 となる．これは入力データのミスである可能性があるため，再び暗号化用の鍵入力待ち状態となる．2 つの鍵が一致したならば，11 クロックを要して鍵セットアップ処理が自動的に行なわれる．それに続き 0 データの暗号化，復号が実行されて 0 に戻るかどうかがチェックされる．戻らなかった場合は回路の動作エラーであるため，Status[3:0]=1100 となり動作を停止し，リセット以外は受け付けなくなる．暗号化と復号によって 0 に戻ったならばデータ入力可能な状態となる．

Dout[127:0]

暗号化または復号処理の結果である暗号文または平文が出力される．出力データは，リセット，鍵入力，あるいは次の暗号化または復号処理が終了するまで有効である．

Dvld

リセットによって 0 となった後，暗号化あるいは復号処理が完了するとこの信号が 1 となり，EncDec=0 ならば暗号文が，EncDec=1 ならば平文が Dout[127:0]に出力される．処理が連続して行なわれている場合，有効なデータが Dout[127:0]に出力されているが，新しい出力データとの切り替わりのタイミングがわかるように，その直前の 1 クロックは Dvld=0 としている．

Kvld

リセットによって 0 となった後，暗号化用の鍵に続いて復号用の鍵がセットされると，

復号回路モジュールが鍵セットアップを行い，さらに平文 0 を暗号化と復号で 0 に戻ることが確認されたならばこの信号が 1 となる．2 つの鍵が不一致か，暗号化と復号によってデータが 0 に戻らない場合は 0 をキープする．また新たな鍵が入力されるとこの一連の処理が行われ，その間は 0 となる．

Status[3:0]

ステータスレジスタ．RSTn=0 または RSTn_HW=0 で値が 1000 にセットされ，アルゴリズムテストおよび鍵テストに合格すると 0000 となる．また何らかのエラーが発生すると Status[3]=1 となる．各ビットの意味は以下の通りである．

Status[3] 0:正常 1:エラー発生
Status[2] 0:正常 1:入力鍵の暗号化・復号テスト失敗
Status[1] 0:正常 1:暗号化用と復号用の鍵不一致
Status[0] 0:正常 1:テスト失敗

Svld

リセットによって 0 となった後，アルゴリズムテスト，鍵セット，暗号化・復号等の処理が終了し，ステータスレジスタが読めるようになると 1 にセットされる．

2.3 状態遷移とアルゴリズムテスト

図 10 に AES_TOP の状態遷移図を示す．RSTn=0 または RSTn_HW=0 とすることでマクロにリセットがかかり，「S1 アルゴリズムテスト」に進む．アルゴリズムテスト中にエラーが見つかったならば，電源オフ，リセット以外は受け付けない「8.停止」状態となる．このときエラーの状態を示すステータスフラグが Status[3:0]に立つ．また，鍵テスト時にエラーが発生した場合も，「8.停止」状態となる．図 10 に示されているように，リセットは全ての状態において優先的に受け付けられる．

以下に各状態の説明を記す．

S1. アルゴリズムテスト

リセットによりアルゴリズムテストが開始される．テスト中に期待値と異なるデータが生成されるとエラーとなり，「S8.停止」状態となる．また，テストに合格すると，「S2.コマンド＆データ入力待ち」状態に自動的に遷移する．

S2. コマンド＆データ入力待ち

暗号鍵入力コマンドとともに鍵が入力されると，「S3.復号鍵入力」状態へ，暗号化コマンドとともに平文が入力されると「S6.暗号化」状態へ，復号コマンドとともに暗号文が入力されると「S7.復号」状態へ遷移する．またこの状態にあるとき，ステータスの読み出し，そして暗号化および復号によって暗号文または平文が生成されていれば,それらを読み出すことができる．ユーザには暗号化または復号を行う前に，暗号鍵と復号鍵を正しくセットすることが求められている．リセット後にアルゴリズムテストが終了すると，鍵を入力しなくとも暗号化と復号コマンドを実行することができるが，このときはアルゴリズムテストで使用された鍵が用いられることになる．

S3. 復号鍵入力待ち

AES は共通鍵暗号なので暗号化と復号で同じ秘密鍵を使用する．しかし，秘密鍵が誤って入力されたり，あるいは FPGA 内部の鍵レジスタの故障などにより誤った処理が行われるのを避けるため，秘密鍵を暗号化鍵と復号鍵として 2 度入力し，それらによって正しく暗号化→復号が行われるかどうかをチェックする．この状態にあるとき，復号鍵の入力のみ受け付け，復号回路内の鍵レジスタにセットされる．正しい処理を行うためには，暗号化鍵と同じものが入力さ

れなくてはならないが，ここでは違う値であっても「S4.鍵比較」状態に遷移する．

S4. 鍵比較

「S2.コマンド＆データ入力待ち」状態と「S3.復号鍵入力待ち」状態において入力され，2 つのレジスタにセットされた暗号化鍵と復号鍵が比較され，両者が一致していれば「S5.鍵テスト」へ，異なっていれば「S8. 停止」状態に遷移する．

S5. 鍵テスト

入力された 2 つの鍵が一致したときに，暗号化鍵で 0 データを暗号化し，その暗号文を復号鍵で復号して元の平文 0 に戻るかどうかをチェックする．処理が正しく行われれば「S2.コマンド＆データ入力待ち」状態へ，また平文 0 に戻らなければ「8.停止」状態に遷移する．

S6. 暗号化

暗号化回路が暗号化鍵を用いて平文を処理し，暗号文が生成されると「S2.コマンド＆データ入力待ち」に戻る．

S7. 復号

復号回路が復号鍵を用いて暗号文を処理し，平文が生成されると「S2.コマンド＆データ入力待ち」状態に戻る．

S8. 停止

「S1.アルゴリズムテスト」，「S4.鍵比較」または「S5.鍵テスト」の結果が期待値と一致しない場合に，この状態となる．リセットにより，「S1.アルゴリズムテスト」を再始動することができる．

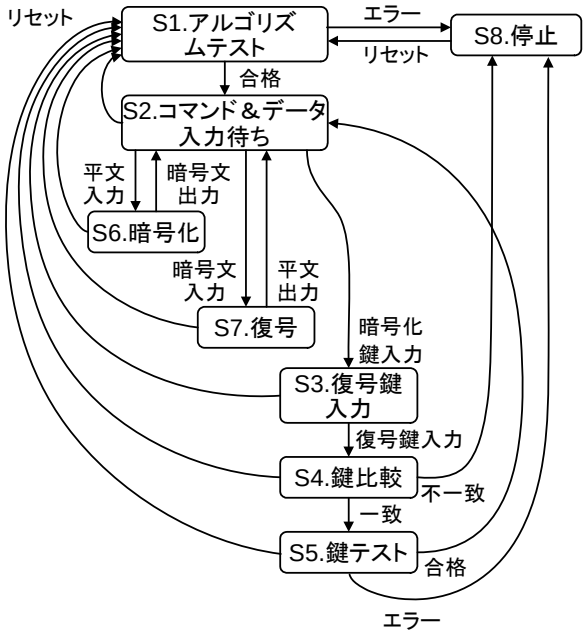

図10 トップモジュールAES_TOPの状態遷移図

2.4 タイミングチャート

ここでは暗号化と復号処理の過程を，図 11 のタイミングチャートを順を追って説明する．全てのレジスタはクロックの立ち上がりエッジに同期しており，説明における各信号の状態はこのエッジでの状態を表している．また，入力信号は全て最短のタイミングで制御しており，リセットは既に行われてアルゴリズムテストは終了しているものとする．

CLK1： EN=1 として AES マクロをアクティベートする．
CLK2： EncDec=0，Krdy=1 として暗号化鍵 KY0 をレジスタにセットする．
CLK3： EncDec=1，Krdy=1 として復号鍵 KY1 をレジスタにセットする．これにより鍵テストが自動的に開始され，次クロックで BSY=1 となる．
CLK15： 復号鍵のスケジューリングが終了し，BSY=0 となる．次クロックから平文 0 の暗号化テストが始まり，その次のクロックで BSY=1 となる．
CLK27： テスト暗号化が終了し，BSY=0 となる．次クロックから復号テストが始まり，その次のクロックで BSY=1 となる．
CLK39： テスト復号が終了し，BSY=0 となる．
CLK40： 鍵テストに合格し Kvld=1 となる．このクロックで EncDec=0，Drdy=1 として，最初の平文 PT0 を入力することができる．
CLK41： 平文 PT0 の暗号化処理が開始され，BSY=1 となる．
CLK51： BSY＝0 に落ち，平文データの入力が可能となる．このクロックで Drdy=1 として新たな平文 PT1 を入力することができる．平文入力の最短の間隔は，ここに示したように 11 クロックである．また平文入力から暗号文出力までは 12 クロックを要する．
CLK52： Dvld=1 となり，PT0 に対する暗号文 CT0 が出力される．また，CLK51 で入力した PT1 に対する暗号化処理が始まり，再び BSY=1 となる．
CLK62： BSY=0 に落ちるので，最短の間隔で処理する場合はこのクロックで次の平文を入れることができる．このクロックで Dvld=0 に落ちるが，次のクロック CLK63 で暗号文 CT1 が出力されるのを告げるためであり，出力バス Dout[127:0]上の暗号文 CT0 は実際には有効である．
CLK63： Dvld=1 となり，PT1 に対する暗号文 CT1 が出力される．Drdy=1 とし，次の平文 PT2 を入力する．
CLK64： PT2 に対する暗号化処理が始まり，BSY=1 となる．
CLK74： PT2 の暗号化が終了し，BSY=0 に落ちる．暗号化を続ける場合は，このクロックで新たに平文を入力することができる．復号処理を行う場合は，次クロック以降で暗号文を入力する．
CLK75： PT2 に対する暗号文 CT2 が出力される．このクロックで EncDec=1，Drdy=1 として暗号文 CT0 を入力し，復号処理を開始することができる．
CLK86： BSY=0 に落ち，暗号文データの入力が可能となる．このクロックで Drdy=1 として新たな暗号文 CT1 を入力することができる．暗号文の入力の最短の間隔は，ここに示したように 11 クロックである．また暗号文入力から平文出力までは 12 クロックを要する．
CLK87： Dvld=1 となり，CT0 に対する平文 PT0 が出力される．また，CLK86 で入力した CT1 の復号処理が始まり，再び BSY=1 となる．
CLK97： CT1 の復号処理が終了し，BSY=0 に落ちる．復号処理を続ける場合は，このクロックで新たな暗号文を入力が可能である．このクロックで Dvld=0 に落ちるが，次のクロック CLK98 で平文 PT1 が出力されるのを告げるためであり，出力バス Dout[127:0]上の平文 PT0 は実際には有効である．
CLK98： Dvld=1 となり，CT1 に対する平文 PT1 が出力される．

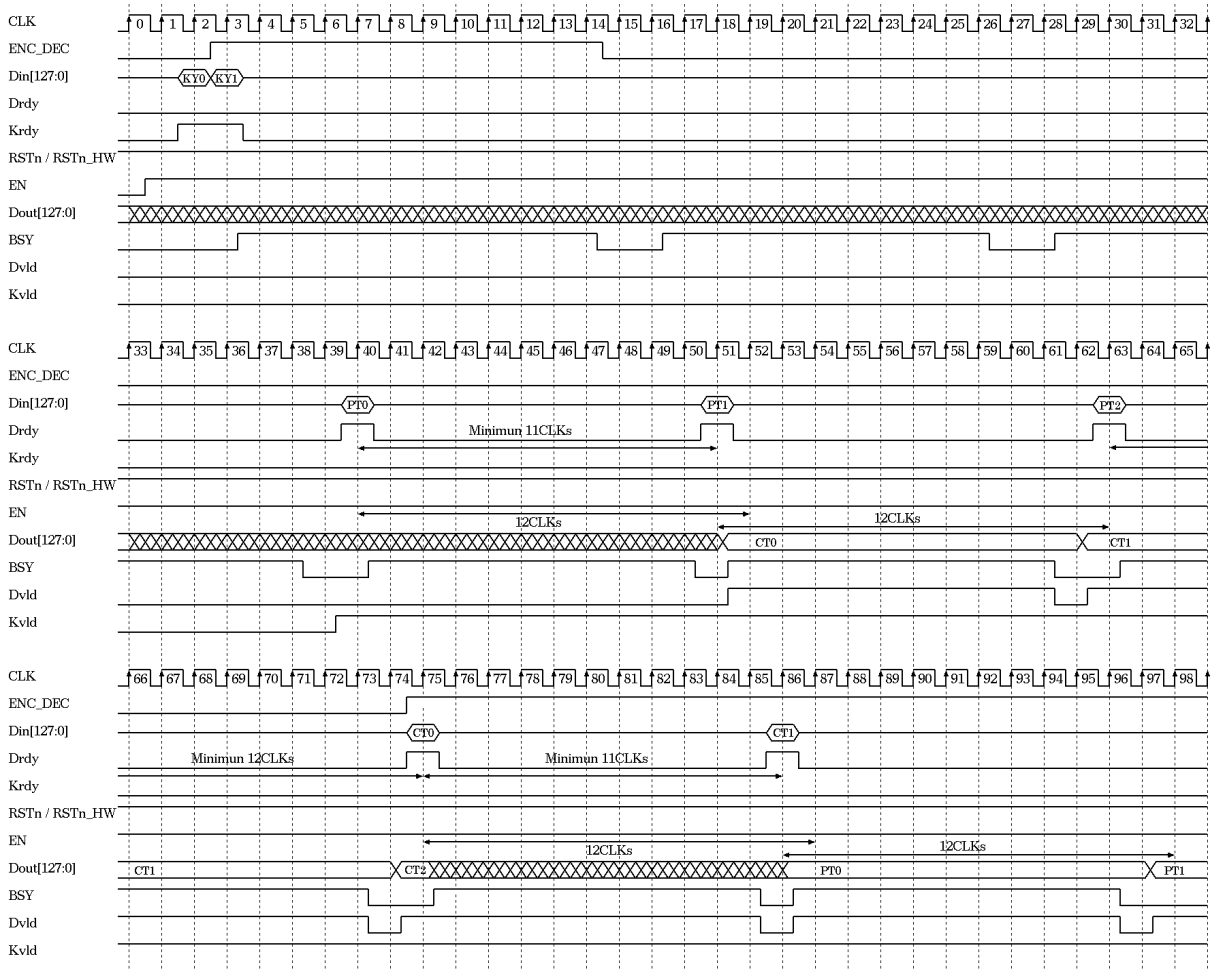

図 11 暗号化・復号処理のタイミングチャート

3. シリアルインタフェース

本章では，SASEBO-AES に実装されたシリアルインタフェース回路の動作を開設する．このインタフェースは FPGA1 に実装される．

3.1 概要

本ハードウェアマクロは，AES 回路とのデータ入出力を RS232C によるシリアルインタフェースを通して行う．表 2 にその概要を，図 12~13 にデータ入出力フォーマットを示す．PC からシーケンシャルに入力されたデータは FPGA2 を介してダイレクトに FPGA1 へ転送される．1 回に入力されるシリアルデータの系列はスタートビット 1 ビット，ストップビット 1 ビットおよびデータ 8 ビットの 10 ビットである．データの処理単位は 136 ビットであり，8 ビットのヘッダと 128 ビットのデータからなる．8 ビットのヘッダはさらに 4 ビットのコマンド（ビット 0~3）と 4 ビットのステータス（ビット 4~7）からなる．コマンドは AES 回路に対するリセット（=1xxx），鍵設定（=01xx），暗号化（=001x）および復号（=0001），ステータス読出し(=0000)の 5 種類である．コマンド発行時にステータスビットは無視される．また，リセットとステータス読み出し時には 128 ビットのデータは不要であるが，全ての入出力データのフォ

ーマットを統一するため，適当な 128 ビットのダミーデータを入力する．

AES による各種処理の後，再び RS232C から PC へと出力される．データの系列長は入力時と同様に 8 ビットのヘッダと 128 ビットのデータからなる 136 ビットである．先頭 4 ビットは直前に処理されたコマンドがそのまま返され，それに続いて必ず 4 ビットのエラー状態を示すステータスが出力される．なお，ステータス読出し時は AES 回路で処理は行われない．リセット，鍵設定，そしてステータス読み出し時は，返すべきデータがないが，データフォーマット統一のため，128 ビットの 0 を出力する．

表 2 シリアルインタフェースの概要

ポート	RS232C 9 ピンシリアルポート
ハードウェア記述言語	Verilog-HDL
通信速度	115.2kbps
通信方式	スタートビット 1 ビット，ストップビット 1 ビット データ 8 ビット，パリティビットなし
送受信データ	136 ビット(コマンド 4 ビット，ステータス 4 ビット，鍵・平文・暗文データ 128 ビット)

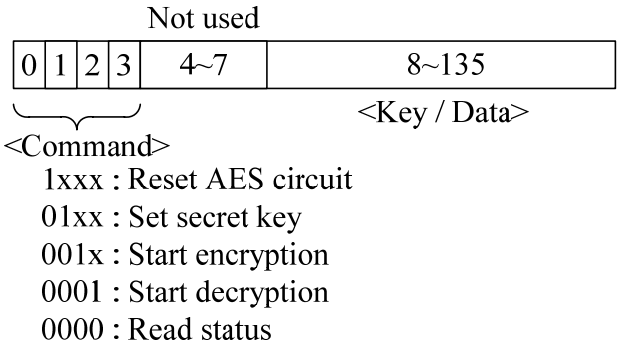

図 12 入力データフォーマット

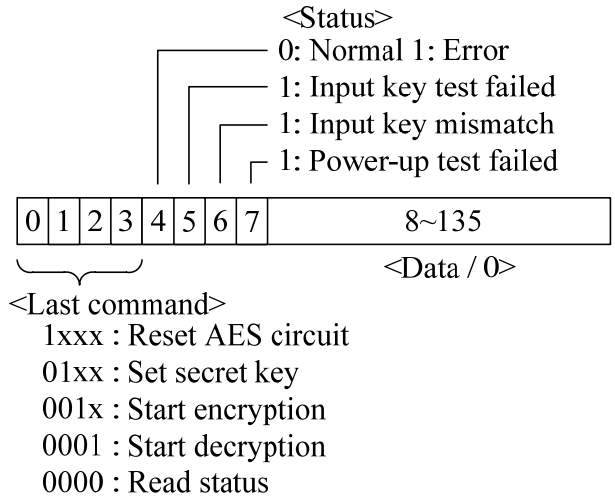

図 13 出力データフォーマット

3.2 アーキテクチャ

図 14 にシリアルインタフェースの回路アーキテクチャを示す．前章で解説した AES マクロへ入力を与えるシリアルーパラレル変換回路（Seri_Para），AES マクロの出力先となるパラレルーシリアル変換回路（Para_Seri）およびそれらで用いるクロック生成回路（Clk_Gen）からなる．

Seri_Para では，PC からのシリアルデータを変換し，AES マクロにパラレルに制御コマンドおよびデータを入力する．シリアルデータは，17 回のデータ通信により 136 ビット単位で入力され，Seri_Para 内部のレジスタにセットされる．データの受け付けは SPstatus の値により決定され，SPstatus=1 のとき受け付け可，SPstatus=0 のとき不可となる．SPstatus の初期値は 1 であり，後述するリセット信号 SPrst により SPstatus=1 となる．また，ハードウェアリセット信号が RSTn_HW=1 となると，直ちに全てのステータス信号がリセットされる．AES マクロへ入力される信号の詳細は 2 章を参照されたい．入力データの先頭 4 ビットのコマンドは出力データの先頭に付加されるため，信号 Cmd[3:0]として Para_Seri へ送られる．136 ビットのデータを受け取ったならば，PSstatus=1 として AES マクロおよび Para_Seri 側に制御を移すと同時に，SPstatus=0 として Seri_Para はデータ入力を受け付けない状態となる．

Para_Seri では，AES マクロからのパラレルデータをシリアルデータに変換して RS232C ポートから PC にデータを出力する．AES マクロによる処理が終了すると，その出力 Dout[127:0]と Status[3:0]に Seri_Para からの 4 ビットのコマンド信号 Cmd[3:0]を加えた 136 ビットをレジスタに格納し，シリアルデータとして 17 回に分けて送信する．データ出力が終了すると，ステータス信号を SPstatus=1 にセットすることで，SPrst＝PSｒｓｔ＝1 となり，各々のステータス信号が初期化（SPstatus=1, PSstatus=0）される．また，Para_Seri はハードウェアリセット信号 RSTn_HW およびソフトウェアリセット信号 RSTn を常に受け付けており，RSTn_HW=0 または RSTn=0 のとき全てのレジスタ・ステータス信号をリセットする．

CLK_GEN では，Seri_Para および Para_Seri で使用するクロック信号 BoudRate16 と BoudRate を生成する．ハードウェアリセット信号 RSTn_HW だけを受け付けており，リセットによってクロック信号を再生成する．

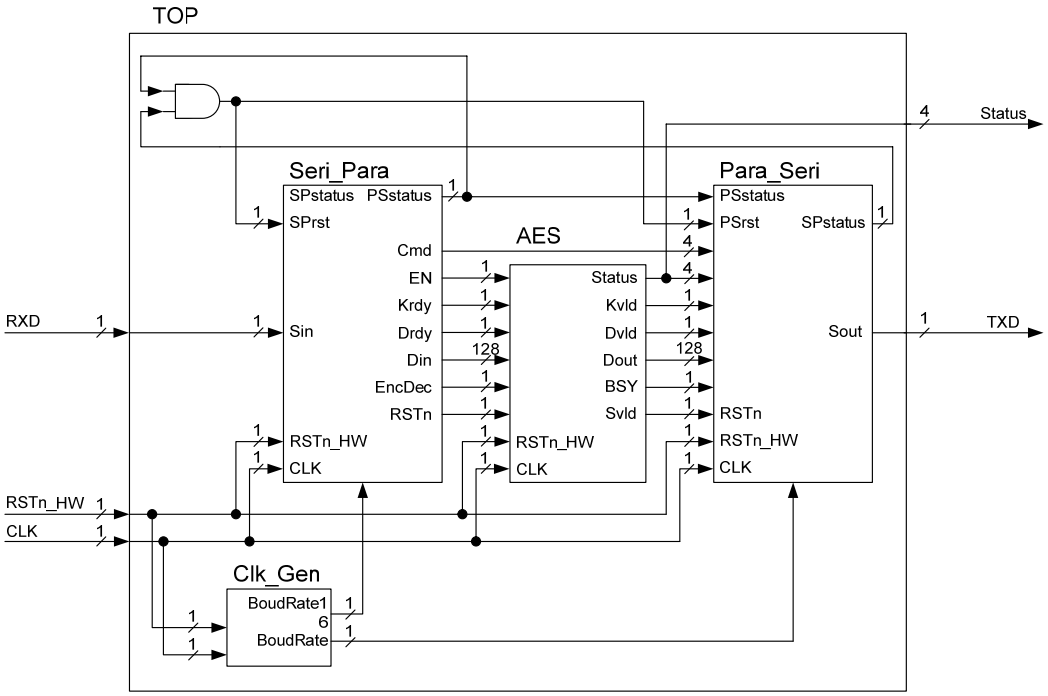

図 14 インタフェースの回路アーキテクチャ

シリアルインタフェース回路として公開されるソースコードは以下の通りで,「2.2 AES アルゴリズムとデータパスアーキテクチャ」に示したソースコードと共に論理合成された回路設計情報が EEPROM1 に保存され, FPGA1 にロードの後に実行される.

SASEBO_TOP.v
本インタフェースのトップモジュール. Para_Seri, Seri_Para, AES_top および Clk_Gen を含む.

SERI_PARA.v
RS232Cからのシリアルデータをパラレルデータに変換する. 入力データをステータス信号 SPstatus=1 のときのみ受け付ける. シリアルデータの系列長は 136 ビットであり, コマンド信号 4 ビットおよびステータス信号 4 ビットを含む. AES 回路への入力データの他に, パラレルーシリアル変換回路へのステータス信号 PSstatus およびコマンド信号 Cmd を出力する.

PARA_SERI.v
AES からのパラレルデータをシリアルデータに変換する. 入力データをステータス信号 PSstatus=1 のときのみ受け付ける. 出力するシリアルデータの系列長は 136 ビットであり, コマンド信号 4 ビットおよびステータス信号 4 ビットを含む. AES 回路からの入力データの他に, シリアルーパラレル変換回路へのステータス信号 SPstatus を出力する.

CLK_GEN.v.
上記のシリアルーパラレル変換およびパラレルーシリアル変換で用いるクロック信号を生成する.

以下にインタフェース回路で使用される信号について述べる.

CLK
システムクロック. 出力および全ての内部信号は CLK の立ち上がりエッジに同期している.

RSTn
1 クロック以上 0 に落とすことでシーケンサーおよび鍵レジスタをリセットする. またリセット後に RSTn=1 となると, AES 回路でアルゴリズムテストが自動的に始まる.

RSTn_HW
ハードウェア用リセット信号. 機能は RSTn と同じ.

RXD
シリアル入力. 無信号時はハイレベル(以後'1')である. データ入力時は, 1 ビットのスタートビット'0'に続いて, 8 ビット分のデータ列, 1 ビットのストップビット'1'が入力される. データ列後のパリティビットは省略.

TXD
シリアル出力. 1 ビットのスタートビット'0'に続いて, 8 ビット分のデータ列, 1 ビットのストップビット'1'を出力する.

BaudRate
24MHzのクロックを分周して 115.2kHz(=kbps)としたクロック信号. パラレルーシリアル変換においてシリアルデータの 1 ビットの幅となる.

BaudRate16

115.2kHz の 16 倍（＝1.8432MHz）に分周されたクロック信号．シリアルーパラレル変換においてシリアルデータのサンプリングに用いる．

SPstatus

シリアルーパラレル変換回路のステータス信号・初期値は 1 である．1 のときデータを受け付け・データ変換後に 0 となる．0 の間は新たなデータを受け付けない．SPrst 信号が 1 になると 1 に戻る．

PSstatus

パラレルーシリアル変換回路のステータス信号・初期値は 0 である．1 のときデータを受け付ける．0 の間は新たなデータを受け付けない．PSrst 信号が 1 になると 0 に戻る．

SPrst/PSrst

それぞれ SPstatus と PSstatus のリセットに用いる．

Cmd[3:0]

AES 回路へのコマンド信号．初期値およびリセット時は 0000 にセットされる．シリアルーパラレル回路に入力されたコマンドがセットされる．なお，コマンドは 4 種類あり，Cmd=1xxx のときリセット，Cmd=01xx のとき鍵入力，Cmd=001x のとき暗号化，Cmd=0001 のとき復号である．Cmd=0000 の場合はステータス読出しであり，AES 回路では処理は何も行われない．

EN

AES 回路へのイネーブル信号．詳細は 2 章を参照．

EncDec

AES 回路への暗号化と復号の切り替え信号．詳細は2章を参照．

Krdy/Drdy

AES 回路への鍵書き込み信号とデータ平文（もしくは暗文）書き込み信号．詳細は 2 章を参照．

Din[127:0]

AES 回路へのデータおよび鍵用 128 ビット入力．詳細は 2 章を参照．

Status[3:0]

AES 回路のステータス信号．詳細は 2 章を参照．

BUSY

AES 回路のビジー信号．詳細は 2 章を参照．

Dvld

AES 回路の暗号化・復号完了信号．詳細は 2 章を参照．

Kvld

AES 回路の鍵セット完了信号．詳細は 2 章を参照．

Dout[127:0]

AES 回路からの 128 ビット出力．詳細は 2 章を参照．

3.3 タイミングチャート

データの入出力の過程を，図 15~17 のタイミングチャートにより説明する．AES マクロと同様に，全てのレジスタはクロックの立ち上がりエッジに同期しており，説明における各信号の状態はこのエッジでの状態を表している．また，入力信号は全て最短のタイミングで制御しており，リセットは既に行われてアルゴリズムテストは終了しているものとする．

図 15 はシリアルデータ受信時のタイミングチャートであり，データは BoudRate（115.2kbps）のビット間隔で PC より送信される．スタートビット 1 ビット，8 ビット分のデータ，ストップビット 1 ビットの計 10 ビットを送信の単位とする．シリアルーパラレル変換回路 Seri_Para では，BoudRate の 16 倍の周波数を持つ BoudRate16 を用いてデータのサンプリングを行う．ストップビットを受信後，全データ（136 ビット）を受信をしていれば，次の BoudRate の立ち上がりで Para_Seri のステータス信号である PSstatus=1 として，パラレルーシリアル変換回路をデータ待ち状態へと遷移する．

図 16 はシリアルデータ送信時のタイミングチャートである．パラレルーシリアル変換回路 Para_Seri は，PSstatus の立ち上がり後，AES マクロが出力する読出し許可信号が Svld=1 となっていることを確認後，データの外部への出力処理を開始する．まず，データ（136 ビット）の受信，ヘッダの生成，送信データ（8 ビット）の選択に BoudRate で 3 サイクルを要する．その後，スタートビット 1 ビット，データ 8 ビット，ストップビット 1 ビットの計 10 ビット単位でデータを送信する．

図 17 は Seri_Para と Para_Seri のステータス信号 SPstatus と PSstatus をリセットするときのタイミングチャートである．SPstatus=1 のとき Seri_Para はデータを受け付け，SPstatus=0 では受け付けない．また，PSstatus=1 ならば Para_Seri はデータを受け付け，PSstatus=0 のときは受け付けない．BoudRate による最後のビットを送信した 1 サイクル後に Para_Seri は Seri_Para のステータス信号を SPstatus=1 とし，それに伴いステータスのリセット信号 SPrst=1，PSrst=1 となる．その結果，次のサイクルで SPstatus=1，PSstatus=0 となる．

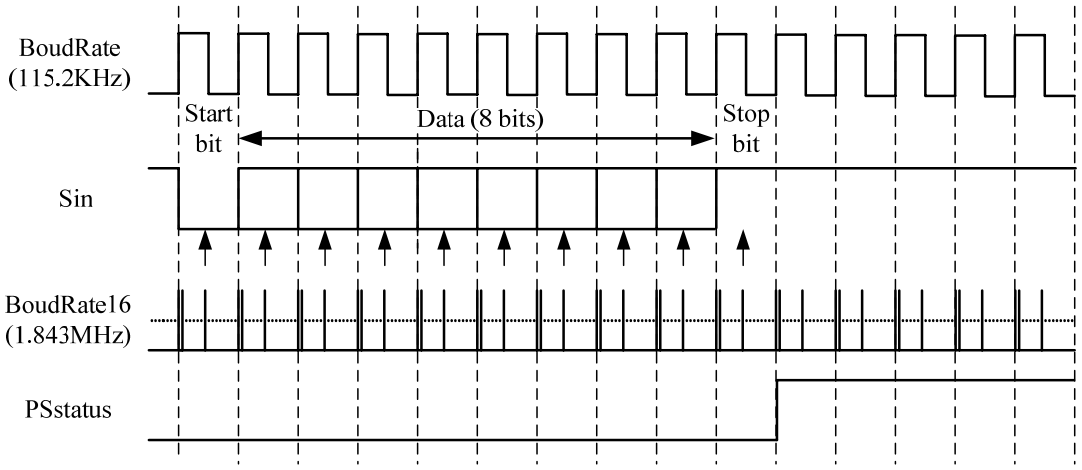

図 15　シリアルデータ受信時のタイミングチャート

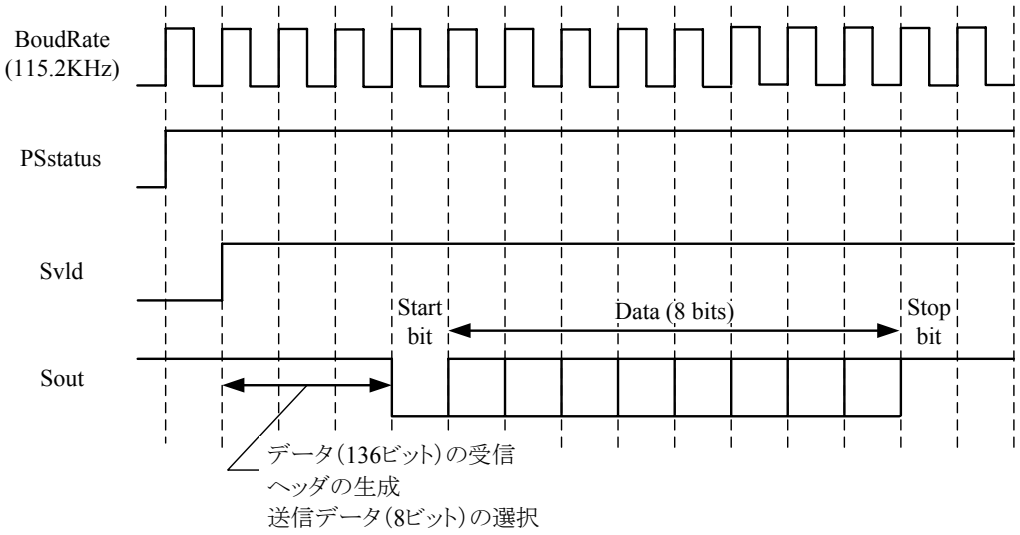

図 16　シリアルデータ送信時のタイミングチャート

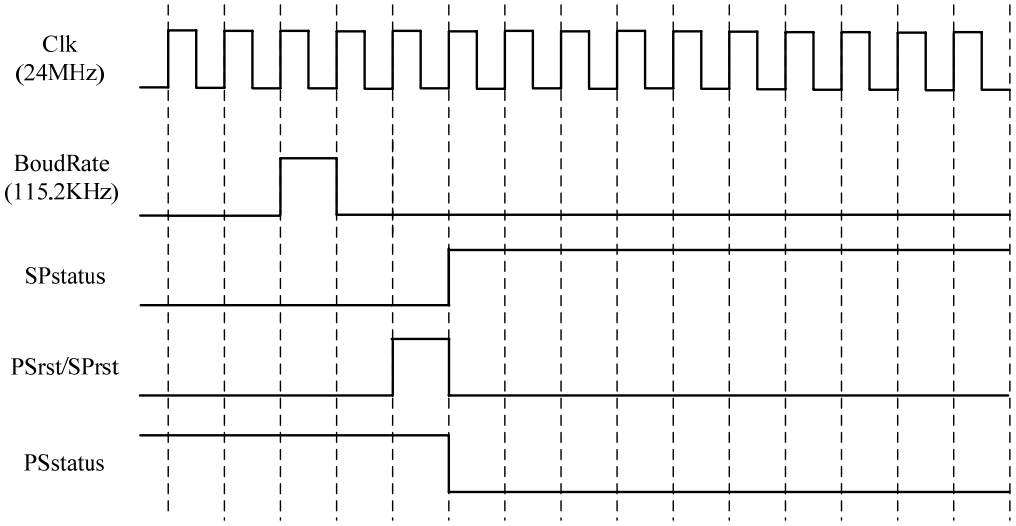

図 17　Para_Seri/Seri_Para のステータス信号リセット時のタイミングチャート

4. SASEBO-AES の運用

本章では，SASEBO-AES のセットアップと Windows 上のサンプル EXCEL ファイルによる動作例を示す．SASEBO-AES は，RS232C シリアルポートにつないだ PC 等の一台の外部端末およびボード上のリセットスイッチによってのみ制御可能で，それらの操作は同時に複数のユーザが行うことはない．したがって，通常は一人のユーザがクリプトオフィサ(管理者)とユーザの役割を担うことを想定している．

4.1　SASEBO-AES のセットアップ

クリプトオフィサは SASEBO-AES を使用可能な状態とするため，以下の手順に従ってセットアップを行う．図 18 は各手順(3.以外)においてボード上でチェックすべき場所を示している．

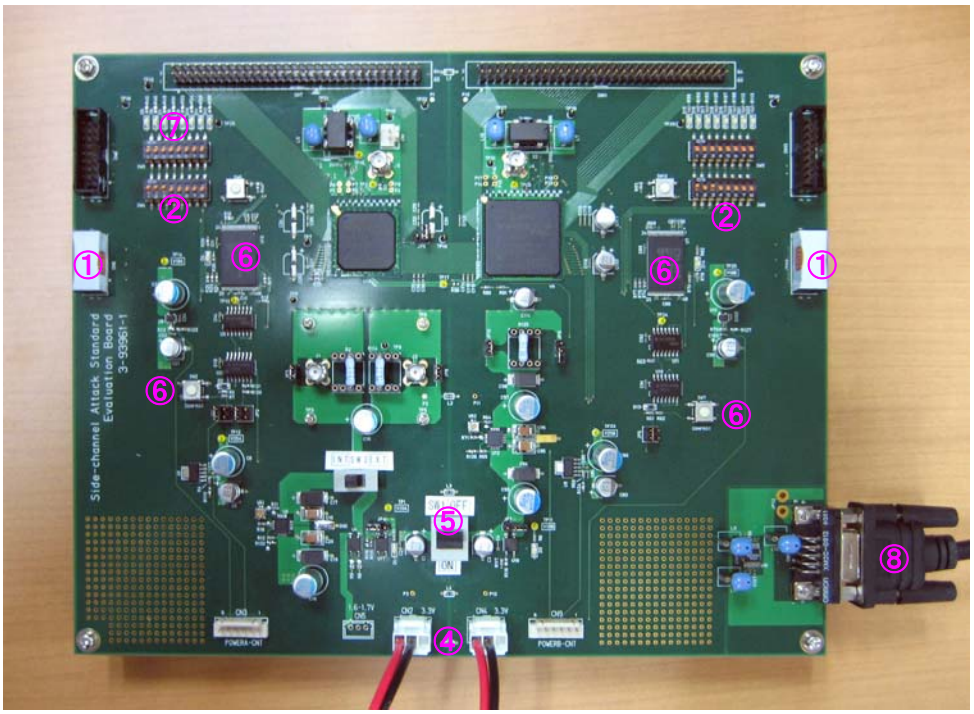

図 18　各手順におけるチェックポイント

①　ボード上の 2 つの EEPROM(XCF08P と XCR16P)の回路設計情報が書き換えられていないことを，改ざん防止シールの状態で確認する．(図 19)

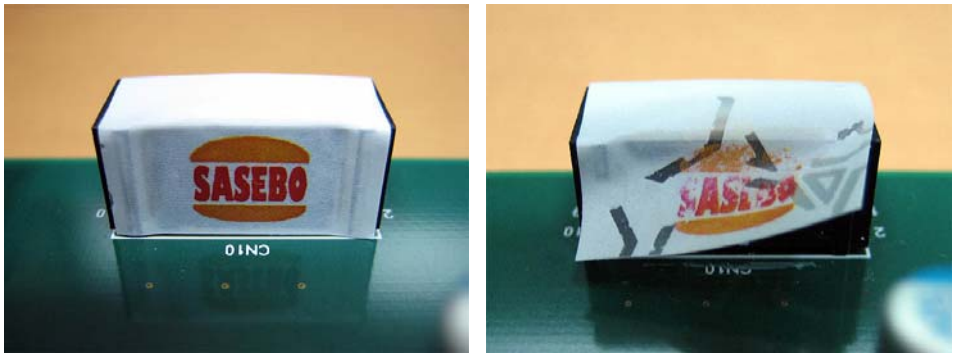

図 19　シールがはがされていないことを確認

②　左右のディップスイッチが図 20 のように設定されていることを確認する．SW4(左)と SW8(右)共に，1~3 が ON で 4~8 が OFF である．また，SW5(左)と SW9(右)は未使用のため設定の確認は不要．

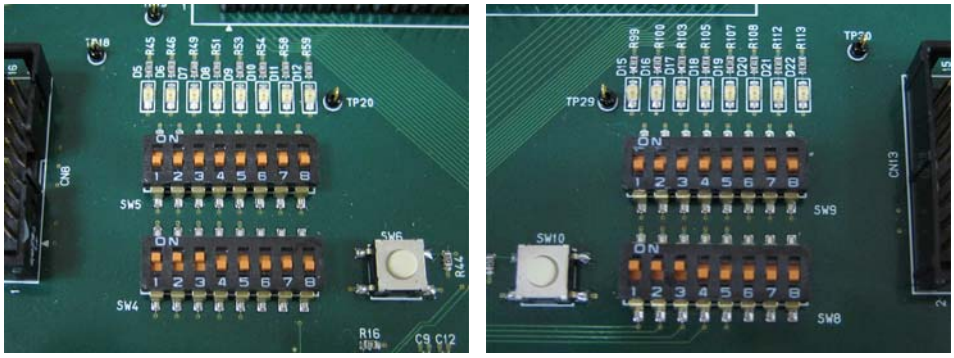

図 20　DIP スイッチの設定

③　　電源とジャンパースイッチの設定が次のようになっていることを確認する. (図 21)

SW1 : OFF　　SW3 : INT
JP1 : SHORT　　JP2 : SHORT　　JP3 : SHORT　　JP4 : OPEN
JP5 : OPEN　　JP6 : SHORT　　JP7 : OPEN　　JP8 : SHORT
JP9 : OPEN　　JP10 : SHORT

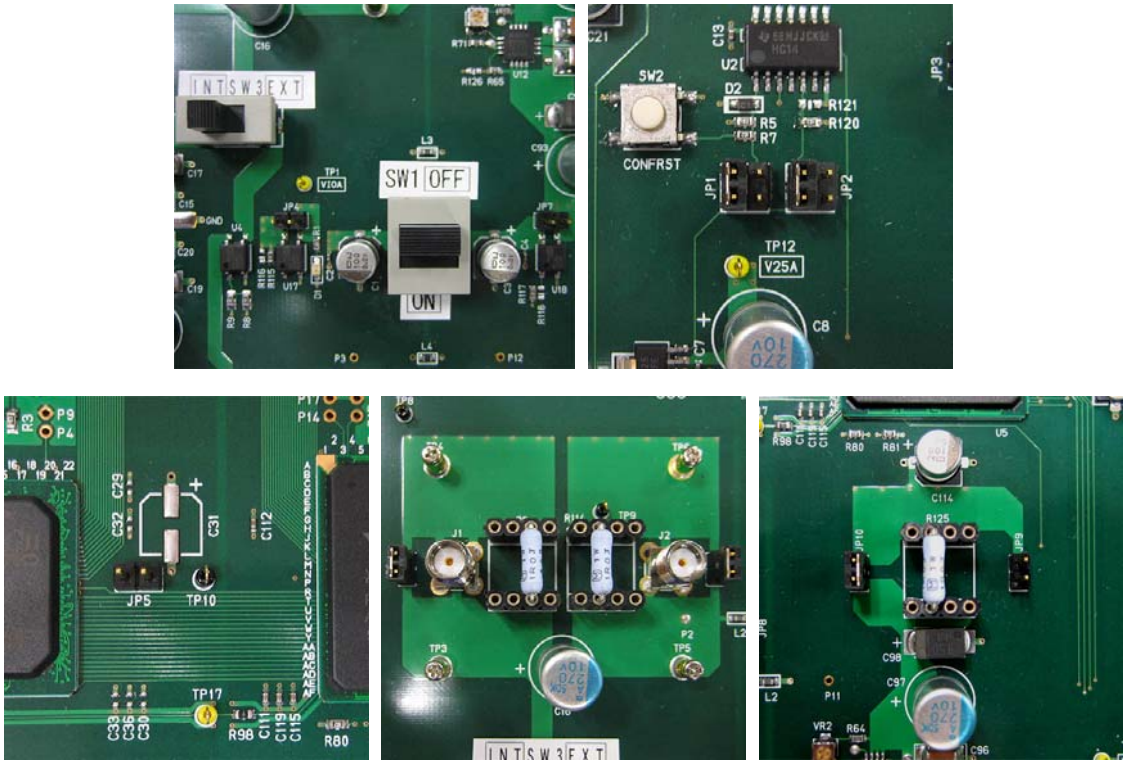

図 21　ジャンパースイッチと電源スイッチの設定

④　　外部電源(直流 3.3V)を SASEBO-AES の 2 つの電源コネクタに接続する.

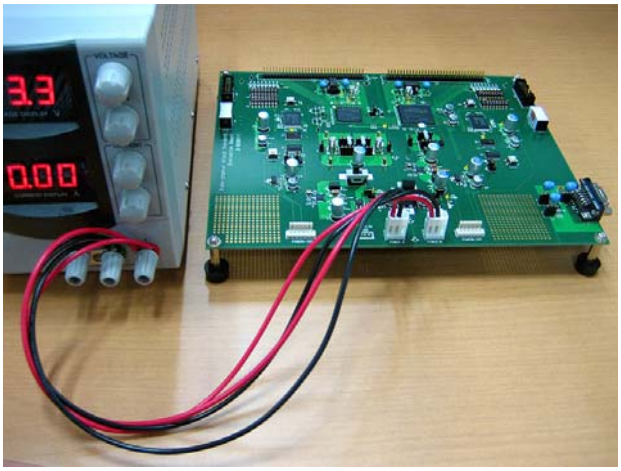

図 22　電源ケーブルを 3.3V 直流電源に接続

⑤　　図 23 のように電源スイッチ SW1を ON にすると，スイッチ両側の 2 つの LED(D1 と D3)が点灯する．点灯しない場合は，電源から電力が供給されていること，電源ケーブルの接続，SW1 と SW3 の状態をチェックする．

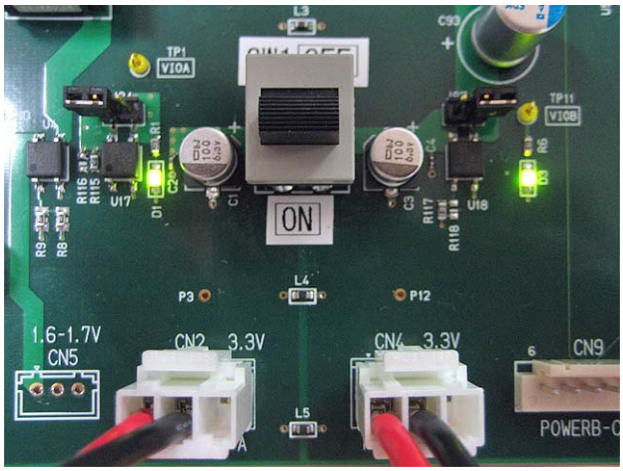

図 23　電源スイッチ SW1 をオン(下)側に倒すと，左右の EEPROM 付近の LED が点灯

⑥　図 24 のように 2 つの EEPROM，XCF08P(左)と XCF16P（右）の横にある核 LED，D4 と D14 が点灯していることを確認する．この LED は各 EEPROM からそれぞれの FPGA（XC2VP7 および XC2VP30）に回路設計情報が正しくコンフィグレーションされたことを示すものである．LED が点灯しない場合は，上記手順 1~5 を再確認し，電源スイッチ SW1 を一旦 OFF した後に再度 ON にするか，図 25 に示した 2 つの再コンフィグレーションスイッチ SW2 と SW7 を順不同で押下する．

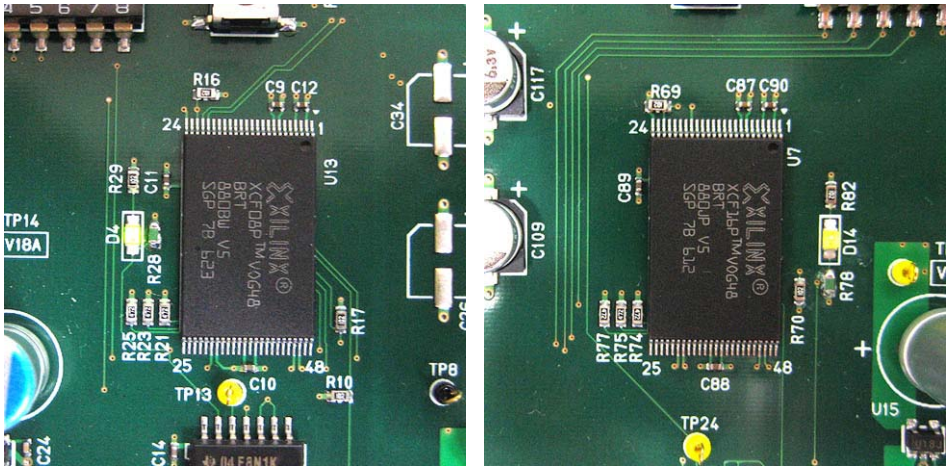

図 24　2 つの EEPROM，XCF08P(左)と XCF16P（右）の LED，D4 と D14 が点灯

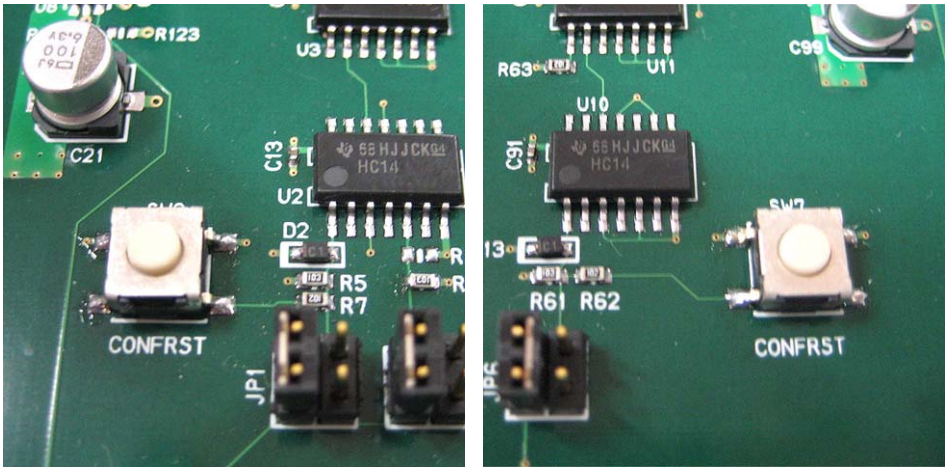

図 25　左右のコンフィグレーションスイッチ SW2 と SW7 をそれぞれ押下

⑦　正しくコンフィギュレーションされたならば，「2.3　状態遷移とアルゴリズムテスト」で説明したテストが自動的に始まり，正常であれば図 10 の「S2.コマンド&データ入力待ち」状態まで進む．その結果，図 26 左のように，ボード左側の FPGA(XC2VP30)に接続された 8 個の LED のうち右端の D12 が点灯する．また，アルゴリズムテストが失敗した場合は，左端の D5(エラー発生)と D8(アルゴリズムテストエラー)の各 LED が点灯する．

ここでハードウェアリセットが正しくかかることを確認するために，リセットボタン SW6 を押下する．ボタンを押し下げたままの状態では，エラーステータスがリセットされて D12 は消灯し，また D5 が一旦点灯する．その後ボタンを離すと，コンフィグレーション時と同様にアルゴリズムテストが実行され，その結果に応じて LED が点灯する．

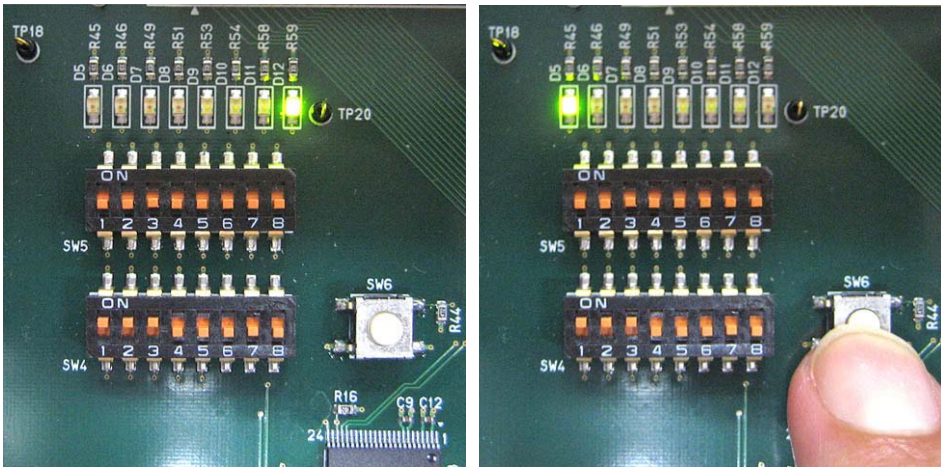

図 26　コンフィグレーション正常終了時とリセットスイッチ押下時のステータス LED の状態

⑧　SASEBO-AES を RS232C シリアルケーブルで外部の PC に接続することで，セットアップが終了する．(図 27)

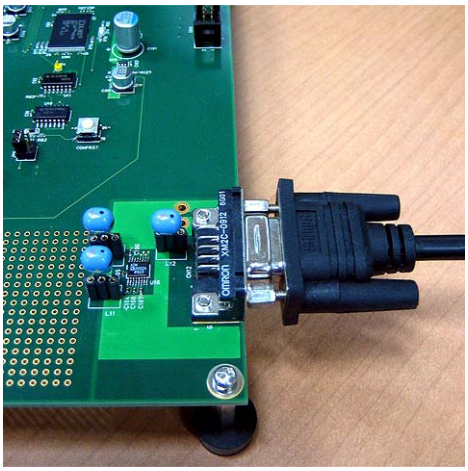

図 27　RS232C ケーブルで SASEBO-AES と PC を接続

4.2　サンプルプログラムの使用法

PC から RS232C を通した SASEBO-AES の制御はユーザ役割であり，そのサンプルプログラムとして，Windows 上で動作するデータ入出力用 EXCEL ファイル SASEBO_AES_TEST.xls を用意している．起動直後のウィンドウは図 28 のようになる．実行手順を以下に示す．

①　使用している PC のシリアルポート番号を調べ，EXCEL ウィンドウ上のセル E2 の COM ポートの欄に記入する．図 27の例におけるポート番号は 7 である．

②　コマンド 4 ビット+ステータス 4 ビットを 16 進で列 A に記入する．ステータス 4 ビットはデータ長を入出力で 4+4+128=136 ビットにそろえるためのダミーであり，この 4 ビットは無視されるので値は何でも構わないが，ここでは 0 としている．コマンドは，リセット，鍵設定，暗号化，復号，ステータス読出しの 5 種類で，シリアルインタフェースの項の図 12 に示したようにそのビット表現は，1xxx, 01xx, 001x, 0001, 0000 である．つまり F~8 がリセット，7~4 が鍵設定，3~2 が暗号

化，1 が復号，0 がステータス読出しであるが，図 28 ではそれぞれ 8，4，2，1，0 としている．

③　列 B にコマンドに応じて 128 ビット(16 進で 32 桁)鍵，平文，暗号文を入力する．リセット 8 とステータス読出し 0 はこの欄のデータ入力は不要であり記入しても無視され，RS232C ポートからは常に 128 ビットの 0 が出力される．複数のコマンドを連続して実行するときには，図のように縦に連続して記入する．途中に空白行があると，そこで処理は停止する．

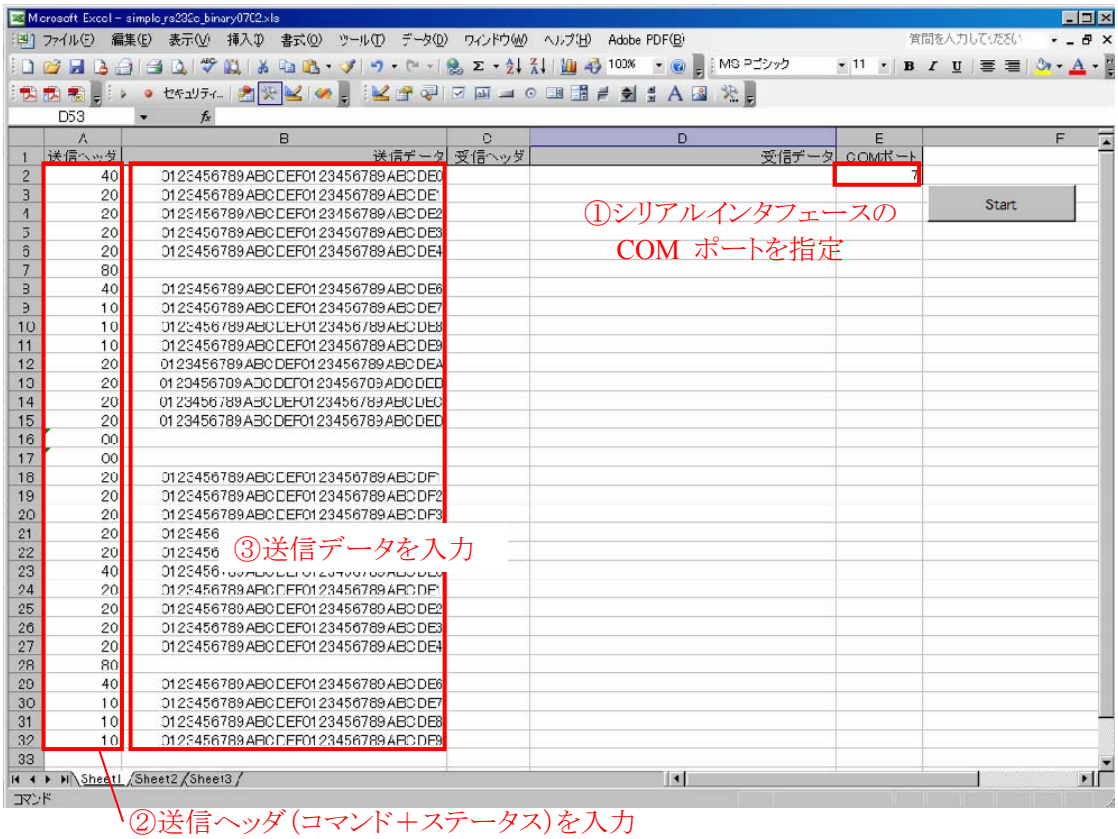

図 28　サンプル EXCEL ファイル起動直後のウィンドウ

④　列 A と B を記入したならば「Start」ボタンをクリックすることでコマンドが連続的に実行され，図 29 のように列 C と D に結果が出力される．

⑤　列 C はその行で実行した 4 ビットのコマンド＋4 ビットのステータス(エラー)情報を示している．この例ではエラーが発生していないので，ステータスは常に 0 である．エラーが発生したときの値は，アルゴリズムテストエラーが C(=1100)，鍵比較エラーが A(=1010)，鍵テストエラーが 9(=1001)である．またそれと同時に，FPGA ボード上のステータスを示す LED の D5 とエラーの種類に応じて D6(アルゴリズムテストエラー)，D7(鍵比較エラー)，D8(鍵テストエラー)が点灯する．

また列 D には処理結果を示しており，データを出力しないリセット，鍵設定，ステータスは 128 ビットの 0 が出力される．

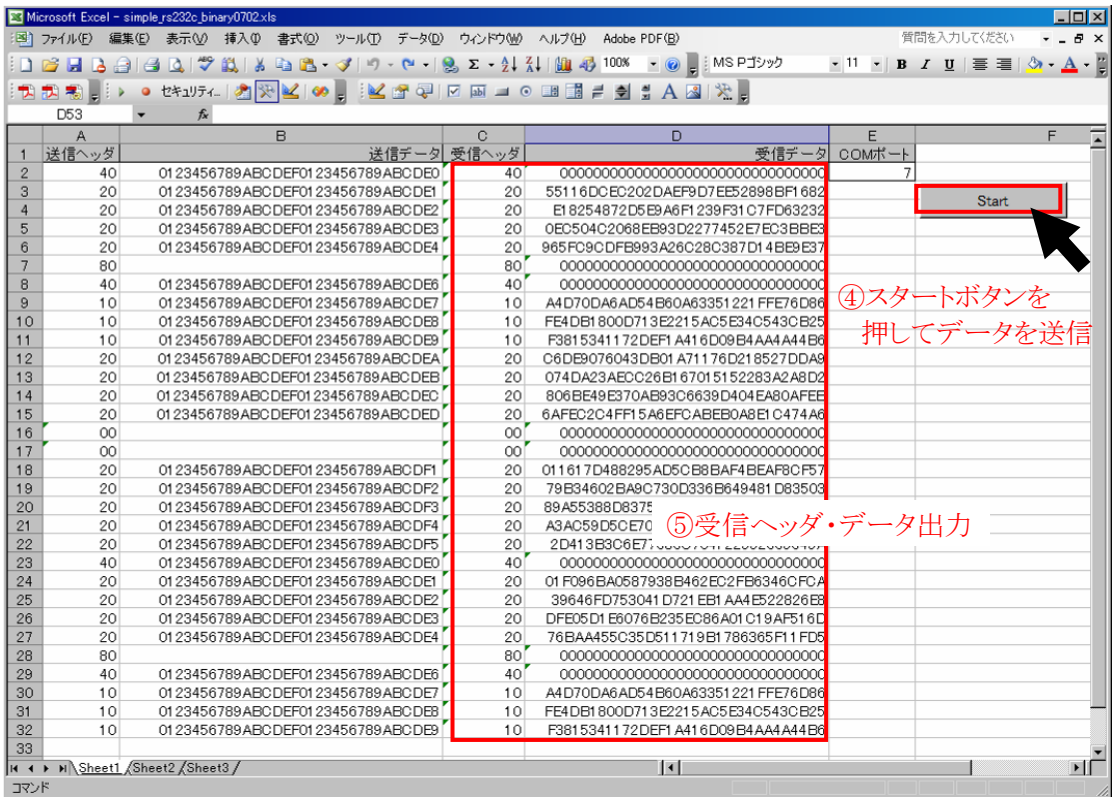

図 29　サンプル EXCEL ファイル実行後のウィンドウ

※1　本製品および本仕様書の著作権は(独)産業技術総合研究所に帰属します.
※2　本製品及び本仕様書の全部または一部を，著作権者に無断で複写，複製することはできません.
※3　本製品及び本マニュアルは，個人として利用するほかは，著作権者に無断で使用することはできません.
※4　本製品は外国為替及び外交貿易管理法の規定により戦略物資等(または役務)に該当しますので，日本国外に輸出する際には，同法に基づき日本国政府の輸出許可が必要です.
※5　本製品の仕様，将来予告なく変更することがあります.

FPGA は，ザイリンクス社の登録商標です.
その他，記載されている社名・製品名は各社の商標および登録商標です.

【製品窓口及び技術的な問合せ先】
(独)産業技術総合研究所
情報セキュリティー研究センター
〒101-0021
東京都千代田区外神田 1-18-13 秋葉原ダイビル 1102 号室
TEL:03-5298-4723　FAX:03-5298-4522