SASEBO クイックスタートガイド

(SASEBO, SASEBO-G, SASEBO-R)

[第1版]

2008 年 10 月 1 日

（独）産業技術総合研究所

情報セキュリティ研究センター

1. 機器の用意

SASEBO の動作テストプログラムには，次の機器を用意します．

1） SASEBO

SASEBO パッケージには，SASEBO 本体，電源ケーブル2本，シャント抵抗数本が梱包されています．

2） 電源

DC 3.3V で 1.0A 以上の容量を持つ電源が必要です．

3） RS-232 メス-メス 9-pin ケーブル，または，USB ケーブル

SASEBO は RS-232 ケーブルでコンピュータと接続します．

SASEBO-R, SASEBO-G は RS-232 と USB のどちらでも接続できます．

4） コンピュータ（Windows）

Windows 2000/XP/Vista を搭載したミドルレンジの性能のコンピュータを用意します．

5） ソフトウェア

Microsoft .Net Framework 3.5 と Xilinx 社 ISE が必要です．

また USB 接続の場合は，FTDI 社の D2XX ドライバと FTD2XX_NET_DLL が必要です．

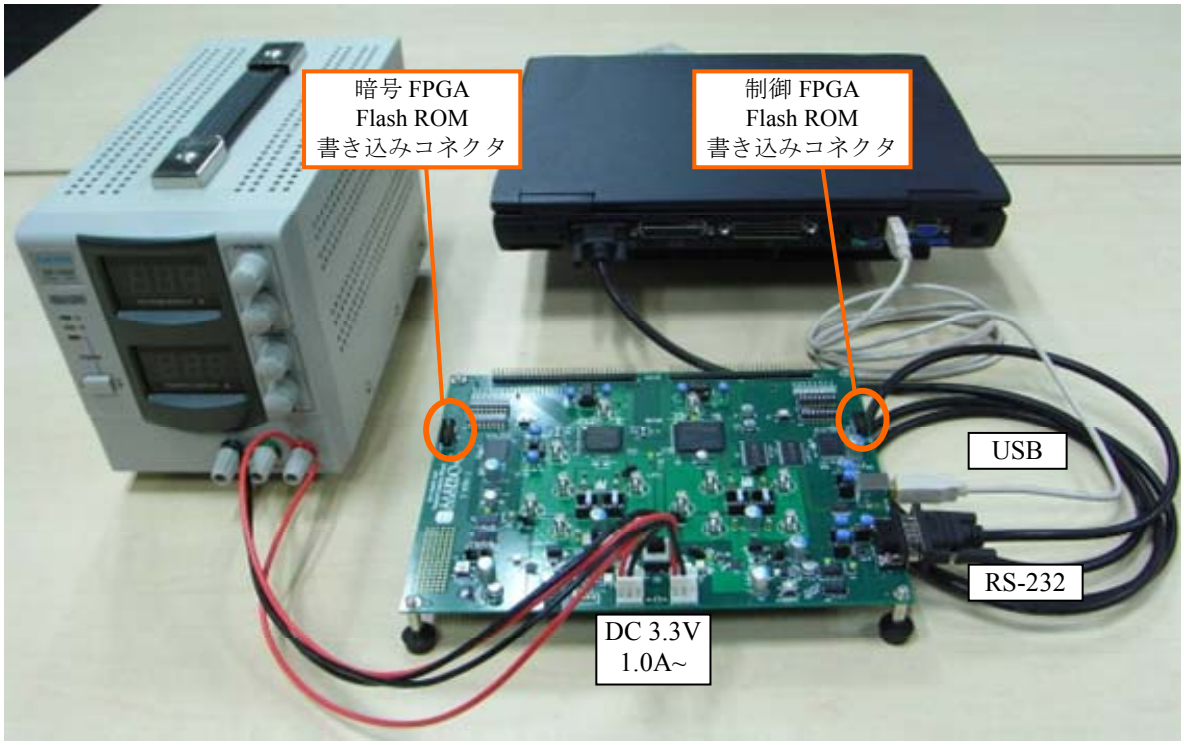
6） FPGA コンフィギュレーションケーブル

制御 FPGA や暗号 FPGA に接続されているフラッシュ ROM を書き換えるためのケーブルです．

Xilinx 社の Platform cable/II, Parallel cable III/IV を用意します．

2. 機器の接続

SASEBO に電源装置を接続し，USB または RS-232 ケーブルでコンピュータと接続します．



3. ソフトウェアのインストール

各々のソフトウェアをダウンロードしてインストールして下さい.

(1) SASEBO テストプログラム sasebo_tester

(2) Microsoft .Net Framework 3.5

（日本語版）

http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6&displaylang=ja

（英語版）

http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6

(3) Xilinx ISE

http://japan.xilinx.com/ise_eval/index.htm

（日本語版）

http://www.xilinx.com/ise_eval/index.htm

（英語版）

(4) FTDI D2XX ドライバ, FTD2XX_NET_DLL

http://www.ftdichip.com/Drivers/D2XX.htm

（D2XX ドライバ）

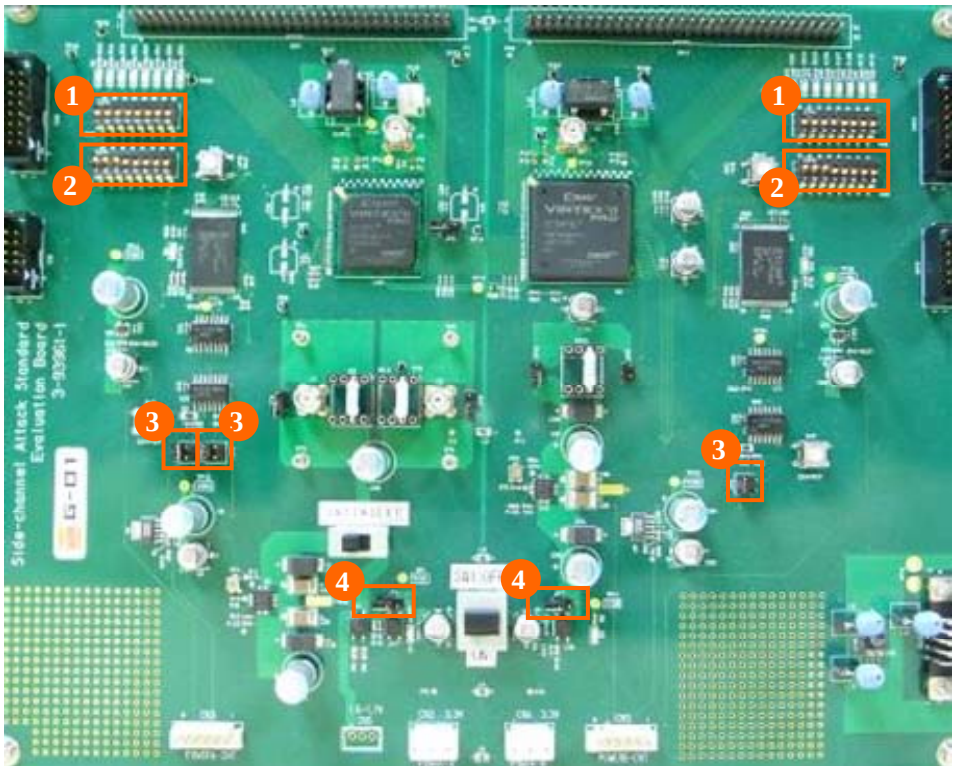
http://www.ftdichip.com/Projects/CodeExamples/CSharp.htm

（FTD2XX_NET_DLL）

FTD2XX_NET_DLL は sasebo_tester のアプリケーションファイルと同じディレクトリにコピーします.

4. SASEBO のセットアップ

■SASEBO のディップスイッチ設定



(1) SW5, SW9

すべて OFF

(2) SW4, SW8

1,2,3 番を ON

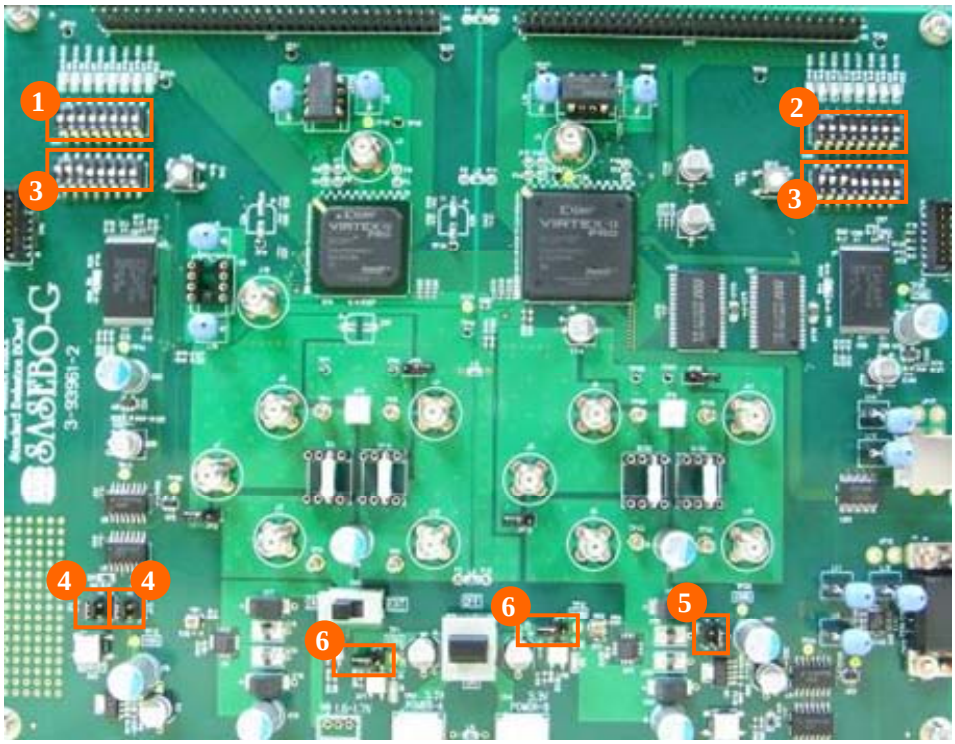
(3) JP1, JP2, JP6

左側をジャンパする

(4) JP4, JP7

開放する

■SASEBO-G のディップスイッチ設定



(1) SW5

すべて OFF

(2) SW9

RS-232 接続のときすべて OFF, USB 接続のとき 1 番を ON

(3) SW4, SW8

1,2,3 番を ON

(4) JP1, JP2


左側(1,2)をジャンパする

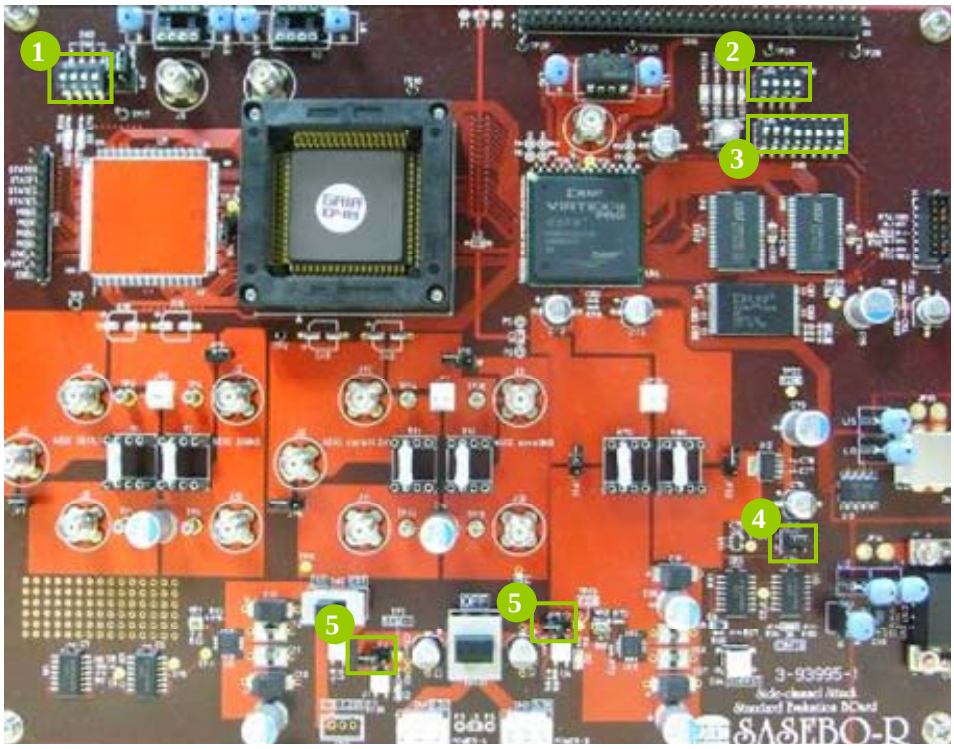
(5) JP6


右側(1,2)をジャンパする

(6) JP4, JP7


開放する

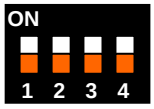
■SASEBO-G のディップスイッチ設定



(1) SW3

すべて OFF

(2) SW6



RS-232 接続のときすべて OFF，USB 接続のとき 1 番を ON

(3) SW5

1,2,3 番を ON

(4) JP10


上側(1,2)をジャンパする

(5) JP4, JP5


開放する

■FPGA のコンフィギュレーション

制御 FPGA のフラッシュ ROM（XCF16P）を配布 mcs ファイルで書き換えます．SASEBO と SASEBO-G は sasebo_v2p30_ctrl_fpga.mcs，SASEBO-R は sasebo_v2p30ctrl_lsi.mcs を用います．コンフィギュレーションケーブルは，SASEBO と SASEBO-G は CN10，SASEBO-R は CN5 へ接続します．コンフィギュレーションでは Impact のデバイスプロパティで Verify と Erase Before Programming はチェック，Parallel Mode はアンチェックに設定して下さい．

SASEBO と SASEBO-G の場合は，暗号 FPGA のフラッシュ ROM（XCF8P）も配布 mcs ファイル sasebo_v2p7_aes_comp.mcs で書き換えます．コンフィギュレーションケーブルは CN6 に接続し，制御 FPGA のときと同様の設定で書き換えを行います．

SASEBO にはコンフィギュレーションケーブルとコネクタの形式を変換するアダプタが付いています．

フラッシュ ROM を書き換えても，まだ FPGA は書き換わっていないので，一旦電源を切ってください．

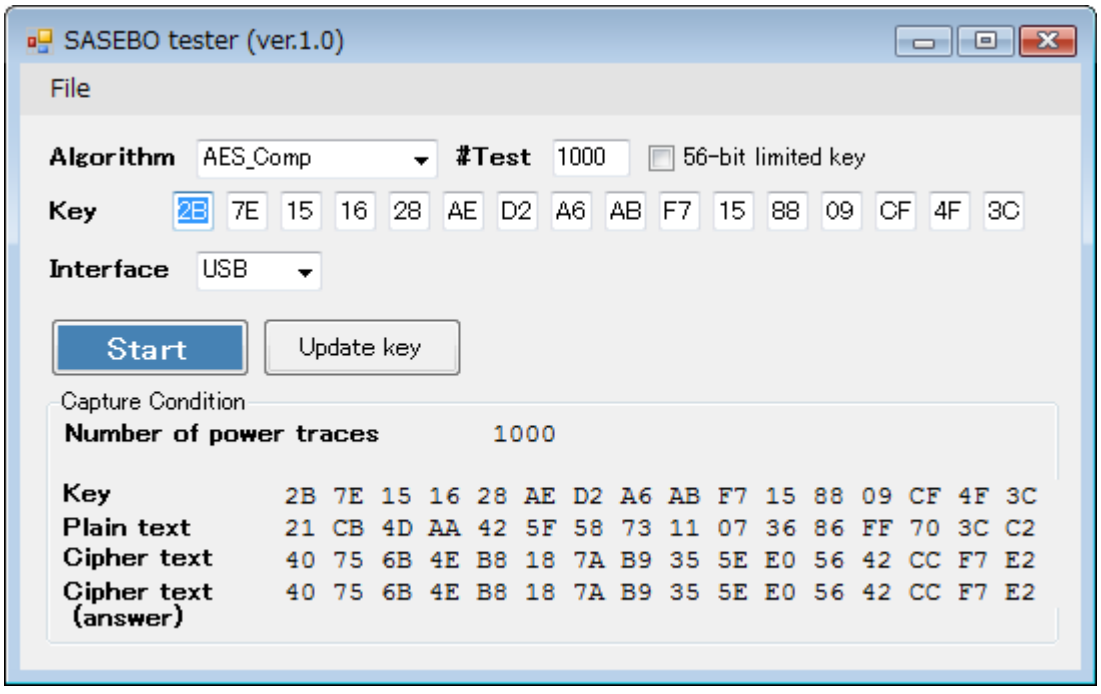
5. 暗号化させてみる

SASEBO の電源を投入すると，LED D1, D3, D4, D14（SASEBO-R は D1,D2,D6）が点灯します．

D1,D3（D1,D2）が点灯しない場合は電源に問題があり，D4,D14（D6）が点灯しない場合は電源，SASEBO の設定，フラッシュ ROM の書き換え失敗に問題があると考えられます．

動作確認後，sasebo_tester プログラムを起動します．

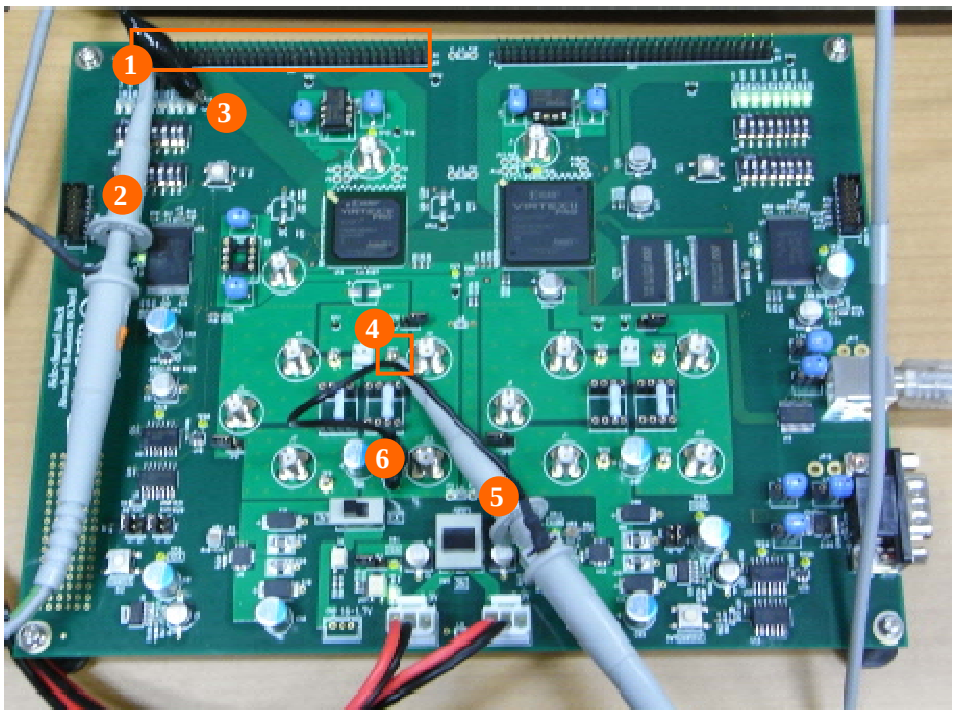
正しく動作すると，SASEBO 上の回路に送信した平文が正しく暗号化されていることを確認できます．



6. 消費電力を測定するには

消費電力の測定にはオシロスコープとプローブ2本を使用します.

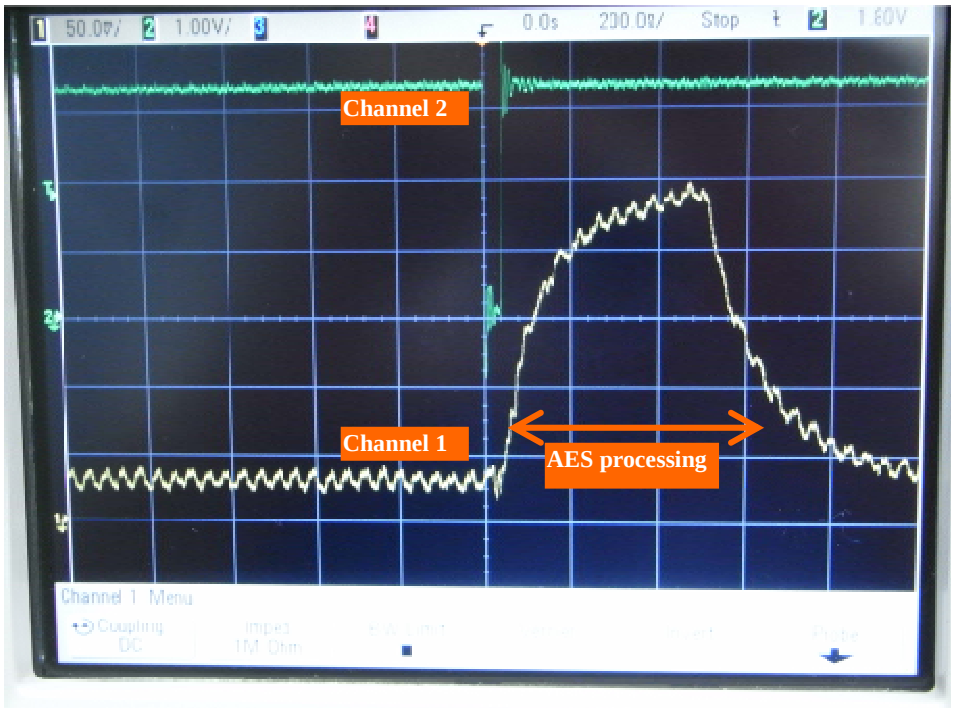
■SASEBO-G の例



CN7(1)の 1-pin に出力されているトリガをチャンネル2(2)で測定します. グランドは TP20(3)に接続します.

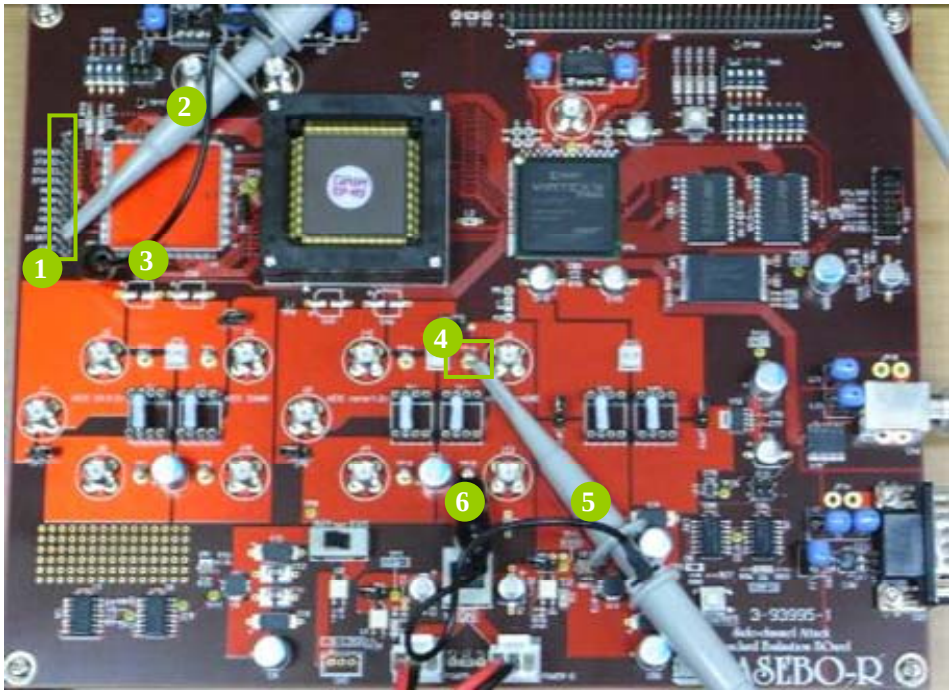
消費電力の波形は TP6(4)にチャンネル1(5)を接続して測定します. グランドは TP5(6)に接続します.

チャンネル1を 50mV/div, 150mV オフセット, 20 MHz BWL, チャンネル2を 1V/div, 0V オフセットに設定し, トリガ条件をチャンネル2ソースでネガティブエッジに設定します.



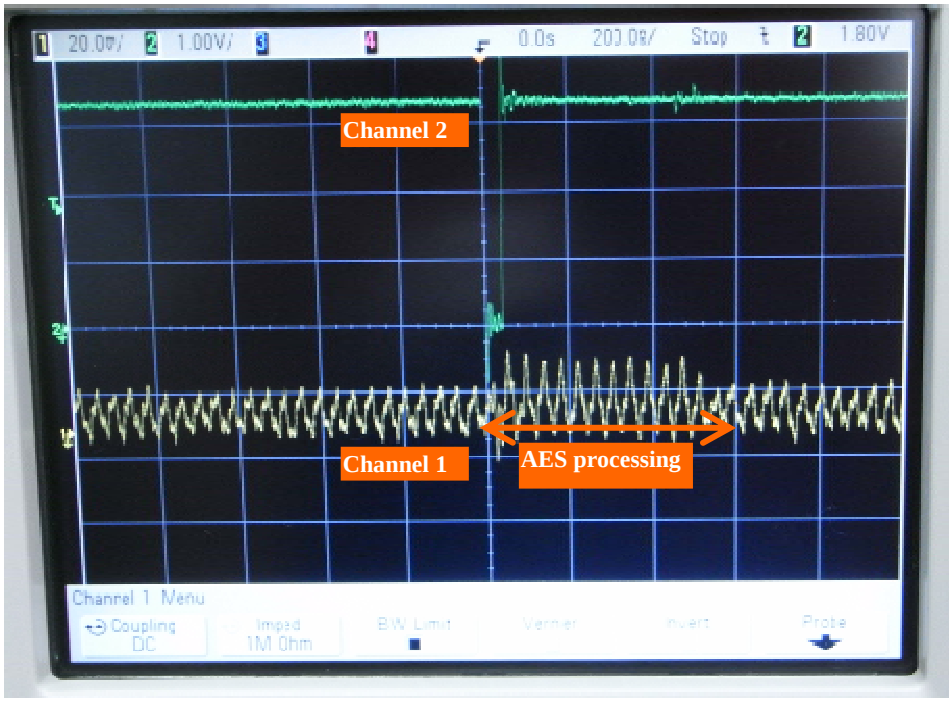
このような消費電力の波形が得られれば成功です.

■SASEBO-G の例



CN4(1)の START_N に出力されている信号をチャンネル2(2)で測定します．グランドは TP5(3)に接続します．
消費電力の波形は TP16(4)にチャンネル1(5)を接続して測定します．グランドは TP15(6)に接続します．

チャンネル1を20mV/div，20mVオフセット，20 MHz BWL，チャンネル2を1V/div，0Vオフセットに設定し，トリガ条件をチャンネル2ソースでネガティブエッジに設定します．



このような消費電力の波形が得られれば成功です．

※1　本ボードの著作権は(独)産業技術総合研究所に，本仕様書の著作権は経済産業省に帰属します．

※2　本ボードおよ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　ボードおよび本仕様書は，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　本ボードの仕様は，将来予告なく変更することがあります．

【問合せ先】

(独) 業技術総合研究所 情報セキュリティ研究センター

〒101-002
東京都千代田区外神田 1-18-13 秋葉原ダイビル 11 階 1102 号室
TEL：03-5298-4722
FAX：03-5298-4522