サイドチャネル攻撃用標準評価基板仕様書

Side-channel Attack Standard Evaluation Board Specification

[第1版]

平成 19年 3月30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

目次

	Page
1. SUMMARY ・・・・・・・・・・・・・・・・・・・・・・・・・・・	2
2. I/O Signal ・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
3. ブロック構成図 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	15
4. 基本機能 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	16
4-1 ボード設定 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	16
4-2 クロック系統 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	21
4-3 コンフィギュレーション部 ・・・・・・・・・・・・・・・・・	22
4-4 電源部 ・・・・・・・・・・・・・・・・・・・・・・・	23
4-5 インターフェース部 ・・・・・・・・・・・・・・・・・・・・・・	25
5. 回路図 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	27
6. 部品リスト ・・・・・・・・・・・・・・・・・・・・・・・・・・・	34
7. プリント配線版資料 ・・・・・・・・・・・・・・・・・・・・・・	37
8. 検査仕様 ・・・・・・・・・・・・・・・・・・・・・・・・・・・	43
9. FPGA暗号・制御回路作成上の注意点 ・・・・・・・・・	44
[変更履歴] ・・・・・・・・・・・・・・・・・・・・・・・・・・・	45
[参考文献] ・・・・・・・・・・・・・・・・・・・・・・・・・・・	45

1. Summary

サイドチャネル攻撃標準評価FPGA基板（以下SASEBO（Side-channel Attack Standard Evaluation Board）と呼ぶ）は、暗号モジュールに対する物理解析攻撃法と防御法の性能評価を目的とする。 SASEBOの主な特徴と機能概要を以下に述べる。

＜特徴＞

◎250㎜×200㎜×1.6mm（板厚），ガラスエポキシ材，8層構造

◎周辺回路用FPGA ： Virtex Ⅱ Proシリーズ（Xilinx社製）：2種搭載。

※ 搭載されるFPGA規模は、下記の構成である。

XC2VP7-5FG456C（暗号回路ターゲット用）　　XC2VP30-5FG676C（制御用PowerPC搭載）

◎シリアル・インターフェース搭載。

◎動作クロック最大24MHz。クロックIC搭載。

◎ターゲット側FPGAは、組込み暗号回路に応じて2種類の電源供給を切り替え可能。

（外部供給電源、レギュレータ供給電源）　※FPGAコア電源のみ適用

⇒ ターゲット回路の消費電流を測定する機能をもつ。

◎外部供給基本電源は、3.3Vで構成されている。2.5V、1.8V、1.5V系は内蔵レギュレータで生成。

※但し、ターゲット側外部供給コア電源は直接1.6～1.7V供給する。

＜機能概要＞

◎本ボードの外部制御は、シリアルI/F接続のパーソナルコンピュータ（PC）で行う。

◎ボードには2つのFPGAが搭載され、暗号評価回路用ターゲットFPGAと、その暗号回路を制御する制御用FPGAとに区別されている。また、PCと接続されるFPGAは制御用FPGAのみである。

◎2つのFPGA間は、入出力別々のデータバスDI、DO（16bit）と、アドレスバス（16bit）、制御信号（RD信号、WR信号、RESET信号、CLOCK信号）で構成されている。

◎暗号回路の評価項目の中に、回路の動作消費電流測定があり、ターゲットFPGAの消費電流を測定する機能を持っている。

◎電源供給は、通常外部コネクタよりDC3.3Vが供給され、基板内のレギュレータでFPGA用1.5V、1.8V、2.5Vを生成している。一部、暗号用ターゲット回路には、外部より直接供給することも可能である。

2. FPGA I/O Signal

U14　　電源測定側ターゲットFPGA

信号名	端子	入出力	用途・接続先
CDA0	V17		Config
CDA1	V16		Config
CDA2	W16		Config
CDA3	Y16		Config
CDA4	Y7		Config
CDA5	W7		Config
CDA6	V7		Config
CDA7	V6		Config
BUSY	W18		Config
INIT_B	W17		Config
GCLK	W20		Config
PROG_B	B1		Config
DONE	Y18		Config
M0	Y4		SW4-1
M1	W3		SW4-2
M2	Y2		SW4-3
TCLK	B22		JTAG
TDI	D3		JTAG
TDO	D20		JTAG
TMS	A21		JTAG
PWRDWN_B	Y19		SW4-4
HSWAP_EN	A2		SW4-5
VBATT	C19		P4
DXP	C4		P5
DXN	C5		P6

信号名	端子	入出力	用途・接続先
OSCX	Y12	IN	Clock
RESETA	W8	IN	RESET
CLK	C12	IN	X1
CKK_EXT	D12	IN	CN1

信号名	端子	入出力	用途・接続先
LED0	E7	OUT	D5
LED1	C10	OUT	D6
LED2	D5	OUT	D7
LED3	F9	OUT	D8
LED4	D7	OUT	D9
LED5	B11	OUT	D10
LED6	C8	OUT	D11
LED7	C7	OUT	D12
DIPSW0	E10	IN	SW5-1
DIPSW1	D10	IN	SW5-2
DIPSW2	D11	IN	SW5-3
DIPSW3	C11	IN	SW5-4
DIPSW4	E9	IN	SW5-5
DIPSW5	F10	IN	SW5-6
DIPSW6	F11	IN	SW5-7
DIPSW7	E11	IN	SW5-8
PUSH	D9	IN	SW6

信号名	端子	入出力	用途･接続先
IOA0	L2	IO	CN7-1
IOA1	K1	IO	CN7-2
IOA2	K2	IO	CN7-3
IOA3	J1	IO	CN7-4
IOA4	J2	IO	CN7-5
IOA5	H1	IO	CN7-6
IOA6	H2	IO	CN7-7
IOA7	G1	IO	CN7-8
IOA8	G2	IO	CN7-9
IOA9	F1	IO	CN7-10
IOA10	F2	IO	CN7-11
IOA11	E1	IO	CN7-12
IOA12	E2	IO	CN7-13
IOA13	D1	IO	CN7-14
IOA14	D2	IO	CN7-15
IOA15	C1	IO	CN7-16
IOA16	C2	IO	CN7-17
IOA17	L6	IO	CN7-18
IOA18	K6	IO	CN7-19
IOA19	L3	IO	CN7-20
IOA20	K5	IO	CN7-21
IOA21	K3	IO	CN7-22
IOA22	K4	IO	CN7-23
IOA23	J3	IO	CN7-24
IOA24	H5	IO	CN7-25
IOA25	H3	IO	CN7-26
IOA26	H4	IO	CN7-27
IOA27	G3	IO	CN7-28
IOA28	G4	IO	CN7-29
IOA29	G5	IO	CN7-30
IOA30	E3	IO	CN7-31
IOA31	E4	IO	CN7-32

信号名	端子	入出力	用途・接続先
IOA32	C21	IO	CN7-33
IOA33	C22	IO	CN7-34
IOA34	D21	IO	CN7-35
IOA35	D22	IO	CN7-36
IOA36	E21	IO	CN7-37
IOA37	E22	IO	CN7-38
IOA38	F21	IO	CN7-39
IOA39	F22	IO	CN7-40
IOA40	G21	IO	CN7-41
IOA41	G22	IO	CN7-42
IOA42	H21	IO	CN7-43
IOA43	H22	IO	CN7-44
IOA44	J21	IO	CN7-45
IOA45	J22	IO	CN7-46
IOA46	K21	IO	CN7-47
IOA47	K22	IO	CN7-48
IOA48	L21	IO	CN7-49
IOA49	E19	IO	CN7-50
IOA50	E20	IO	CN7-51
IOA51	G18	IO	CN7-52
IOA52	G19	IO	CN7-53
IOA53	G20	IO	CN7-54
IOA54	H19	IO	CN7-55
IOA55	H20	IO	CN7-56
IOA56	H18	IO	CN7-57
IOA57	J20	IO	CN7-58
IOA58	K19	IO	CN7-59
IOA59	K20	IO	CN7-60
IOA60	K18	IO	CN7-61
IOA61	L20	IO	CN7-62
IOA62	K17	IO	CN7-63
IOA63	L17	IO	CN7-64

信号名	端子	入出力	U5（接続先）
FPGA_DI0	P21	IN	U2
FPGA_DI1	T18	IN	Y4
FPGA_DI2	U19	IN	Y3
FPGA_DI3	U21	IN	Y2
FPGA_DI4	U22	IN	Y1
FPGA_DI5	N21	IN	T2
FPGA_DI6	N22	IN	T1
FPGA_DI7	T21	IN	W2
FPGA_DI8	T22	IN	W1
FPGA_DI9	P20	IN	V6
FPGA_DI10	M21	IN	R2
FPGA_DI11	M19	IN	R1
FPGA_DI12	N19	IN	U3
FPGA_DI13	N20	IN	V4
FPGA_DI14	P19	IN	V3
FPGA_DI15	R21	IN	V2

信号名	端子	入出力	U5（接続先）
FPGA_DO0	R20	OUT	V5
FPGA_DO1	AA22	OUT	AD1
FPGA_DO2	AB21	OUT	AD2
FPGA_DO3	M20	OUT	R4
FPGA_DO4	Y21	OUT	AC2
FPGA_DO5	Y22	OUT	AC1
FPGA_DO6	R22	OUT	V1
FPGA_DO7	T20	OUT	AA5
FPGA_DO8	W21	OUT	AB2
FPGA_DO9	W22	OUT	AB1
FPGA_DO10	T19	OUT	Y5
FPGA_DO11	P22	OUT	U1
FPGA_DO12	V19	OUT	AA4
FPGA_DO13	V20	OUT	AA3
FPGA_DO14	V21	OUT	AA2
FPGA_DO15	V22	OUT	AA1

信号名	端子	入出力	U5（接続先）
FPGA_A0	V3	IN	P25
FPGA_A1	AA1	IN	AE26
FPGA_A2	Y2	IN	T26
FPGA_A3	Y1	IN	AD26
FPGA_A4	W2	IN	R26
FPGA_A5	W1	IN	AC26
FPGA_A6	N2	IN	W25
FPGA_A7	P2	IN	Y25
FPGA_A8	V2	IN	AD25
FPGA_A9	V1	IN	AB26
FPGA_A10	R1	IN	W26
FPGA_A11	M2	IN	V25
FPGA_A12	U2	IN	AC25
FPGA_A13	U1	IN	AA26
FPGA_A14	P1	IN	V26
FPGA_A15	N1	IN	U26

信号名	端子	入出力	U5（接続先）
FPGA_WR	T2	IN	T25
FPGA_RD	T3	IN	AB25
FPGA_RSV0	T1		Y26
FPGA_RSV1	T4		R25
FPGA_RSV2	R3		U25
FPGA_RSV3	R2		AA25

信号名	端子	入出力	
CPUA_TDO	N3		
CPUA_TDI	M3		
CPUA_TCK	M4		
CPUA_TMS	M5		
CPUA_HALT	M6		
CPUA_TRST	N6		

U5　　制御側FPGA

信号名	端子	入出力	用途・接続先
CDB0	AB21		Config
CDB1	AC21		Config
CDB2	Y20		Config
CDB3	AA20		Config
CDB4	AA7		Config
CDB5	Y7		Config
CDB6	AC6		Config
CDB7	AB6		Config
BUSY	AB22		Config
INIT_B	AC22		Config
GCLK	AE24		Config
PROG_B	B1		Config
DONE	AD23		Config
M0	AE3		SW8-1
M1	AF3		SW8-2
M2	AD4		SW8-3
TCLK	B26		JTAG
TDI	D3		JTAG
TDO	D24		JTAG
TMS	B24		JTAG
PWRDWN_B	AF24		SW8-4
HSWAP_EN	B3		SW8-5
VBATT	A24		P13
DXP	A3		P14
DXN	C4		P15

信号名	端子	入出力	用途・接続先
OSCX	AE1	OUT	Clock
RESETB	Y9	IN	RESET
CLK	B13	IN	X2

信号名	端子	入出力	用途・接続先
LED0	C17	OUT	D15
LED1	B19	OUT	D16
LED2	D17	OUT	D17
LED3	A19	OUT	D18
LED4	C20	OUT	D19
LED5	D18	OUT	D20
LED6	E17	OUT	D21
LED7	C18	OUT	D22
DIPSW0	E21	IN	SW9-1
DIPSW1	D20	IN	SW9-2
DIPSW2	E19	IN	SW9-3
DIPSW3	D15	IN	SW9-4
DIPSW4	C15	IN	SW9-5
DIPSW5	B14	IN	SW9-6
DIPSW6	E15	IN	SW9-7
DIPSW7	E16	IN	SW9-8
PUSH	E22	IN	SW10

信号名	端子	入出力	用途・接続先
TX	M25	OUT	シリアルI／F
RX	M26	IN	シリアルI／F
CTS	N25	OUT	シリアルI／F
RTS	L26	IN	シリアルI／F

信号名	端子	入出力	接続先
IOB0	N3	IO	CN11-1
IOB1	M4	IO	CN11-2
IOB2	L3	IO	CN11-3
IOB3	K3	IO	CN11-4
IOB4	K4	IO	CN11-5
IOB5	G3	IO	CN11-6
IOB6	G4	IO	CN11-7
IOB7	F3	IO	CN11-8
IOB8	F4	IO	CN11-9
IOB9	E4	IO	CN11-10
IOB10	N2	IO	CN11-11
IOB11	M1	IO	CN11-12
IOB12	M2	IO	CN11-13
IOB13	L1	IO	CN11-14
IOB14	L2	IO	CN11-15
IOB15	K1	IO	CN11-16
IOB16	K2	IO	CN11-17
IOB17	J1	IO	CN11-18
IOB18	J2	IO	CN11-19
IOB19	H1	IO	CN11-20
IOB20	H2	IO	CN11-21
IOB21	G1	IO	CN11-22
IOB22	G2	IO	CN11-23
IOB23	F1	IO	CN11-24
IOB24	F2	IO	CN11-25
IOB25	E1	IO	CN11-26
IOB26	E2	IO	CN11-27
IOB27	D1	IO	CN11-28
IOB28	D2	IO	CN11-29
IOB29	C1	IO	CN11-30
IOB30	C2	IO	CN11-31
IOB31	E23	IO	CN11-32

信号名	端子	入出力	接続先
IOB32	F23	IO	CN11-33
IOB33	F24	IO	CN11-34
IOB34	G23	IO	CN11-35
IOB35	G24	IO	CN11-36
IOB36	H22	IO	CN11-37
IOB37	J21	IO	CN11-38
IOB38	J22	IO	CN11-39
IOB39	K23	IO	CN11-40
IOB40	J24	IO	CN11-41
IOB41	L22	IO	CN11-42
IOB42	K24	IO	CN11-43
IOB43	M23	IO	CN11-44
IOB44	M22	IO	CN11-45
IOB45	N24	IO	CN11-46
IOB46	N23	IO	CN11-47
IOB47	C25	IO	CN11-48
IOB48	C26	IO	CN11-49
IOB49	D25	IO	CN11-50
IOB50	D26	IO	CN11-51
IOB51	E25	IO	CN11-52
IOB52	E26	IO	CN11-53
IOB53	F25	IO	CN11-54
IOB54	F26	IO	CN11-55
IOB55	G25	IO	CN11-56
IOB56	G26	IO	CN11-57
IOB57	H25	IO	CN11-58
IOB58	H26	IO	CN11-59
IOB59	J25	IO	CN11-60
IOB60	J26	IO	CN11-61
IOB61	K25	IO	CN11-62
IOB62	K26	IO	CN11-63
IOB63	L25	IO	CN11-64

信号名	端子	入出力	U14
FPGA_DI0	U2	OUT	P21
FPGA_DI1	Y4	OUT	T18
FPGA_DI2	Y3	OUT	U19
FPGA_DI3	Y2	OUT	U21
FPGA_DI4	Y1	OUT	U22
FPGA_DI5	T2	OUT	N21
FPGA_DI6	T1	OUT	N22
FPGA_DI7	W2	OUT	T21
FPGA_DI8	W1	OUT	T22
FPGA_DI9	V6	OUT	P20
FPGA_DI10	R2	OUT	M21
FPGA_DI11	R1	OUT	M19
FPGA_DI12	U3	OUT	N19
FPGA_DI13	V4	OUT	N20
FPGA_DI14	V3	OUT	P19
FPGA_DI15	V2	OUT	R21

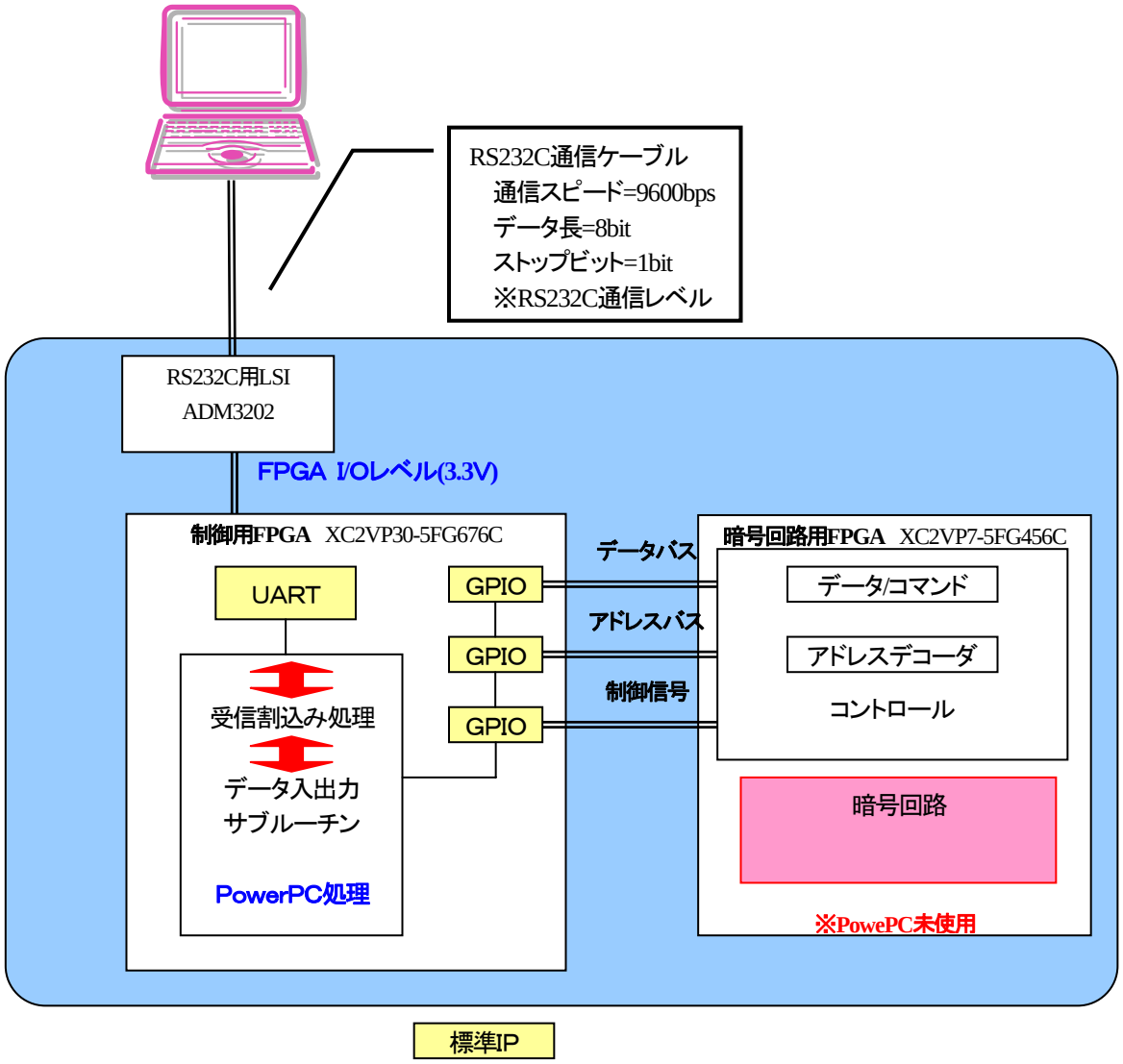
信号名	端子	入出力	U14
FPGA_DO0	V5	IN	R20
FPGA_DO1	AD1	IN	AA22
FPGA_DO2	AD2	IN	AB21
FPGA_DO3	R4	IN	M20
FPGA_DO4	AC2	IN	Y21
FPGA_DO5	AC1	IN	Y22
FPGA_DO6	V1	IN	R22
FPGA_DO7	AA5	IN	T20
FPGA_DO8	AB2	IN	W21
FPGA_DO9	AB1	IN	W22
FPGA_DO10	Y5	IN	T19
FPGA_DO11	U1	IN	P22
FPGA_DO12	AA4	IN	V19
FPGA_DO13	AA3	IN	V20
FPGA_DO14	AA2	IN	V21
FPGA_DO15	AA1	IN	V22

信号名	端子	入出力	U14
FPGA_A0	P25	OUT	V3
FPGA_A1	AE26	OUT	AA1
FPGA_A2	T26	OUT	Y2
FPGA_A3	AD26	OUT	Y1
FPGA_A4	R26	OUT	W2
FPGA_A5	AC26	OUT	W1
FPGA_A6	W25	OUT	N2
FPGA_A7	Y25	OUT	P2
FPGA_A8	AD25	OUT	V2
FPGA_A9	AB26	OUT	V1
FPGA_A10	W26	OUT	R1
FPGA_A11	V25	OUT	M2
FPGA_A12	AC25	OUT	U2
FPGA_A13	AA26	OUT	U1
FPGA_A14	V26	OUT	P1
FPGA_A15	U26	OUT	N1

信号名	端子	入出力	U14
FPGA_WR	T25	OUT	T2
FPGA_RD	AB25	OUT	T3
FPGA_RSV0	Y26		T1
FPGA_RSV1	R25		T4
FPGA_RSV2	U25		R3
FPGA_RSV3	AA25		R2

信号名	端子	入出力	
CPUB_TDO	R23		
CPUB_TDI	P23		
CPUB_TCK	P22		
CPUB_TMS	P24		
CPUB_HALT	P21		
CPUB_TRST	R22		

3. ブロック構成図


RS232C通信ケーブル
通信スピード=9600bps
データ長=8bit
ストップビット=1bit
※RS232C通信レベル
RS232C用LSI
ADM3202
FPGA I/Oレベル(3.3V)
制御用FPGA XC2VP30-5FG676C
UART
GPIO
GPIO
GPIO
受信割込み処理
データ入出力
サブルーチン
PowerPC処理
データバス
アドレスバス
制御信号
暗号回路用FPGA XC2VP7-5FG456C
データ/コマンド
アドレスデコーダ
コントロール
暗号回路
※PowePC未使用
標準IP

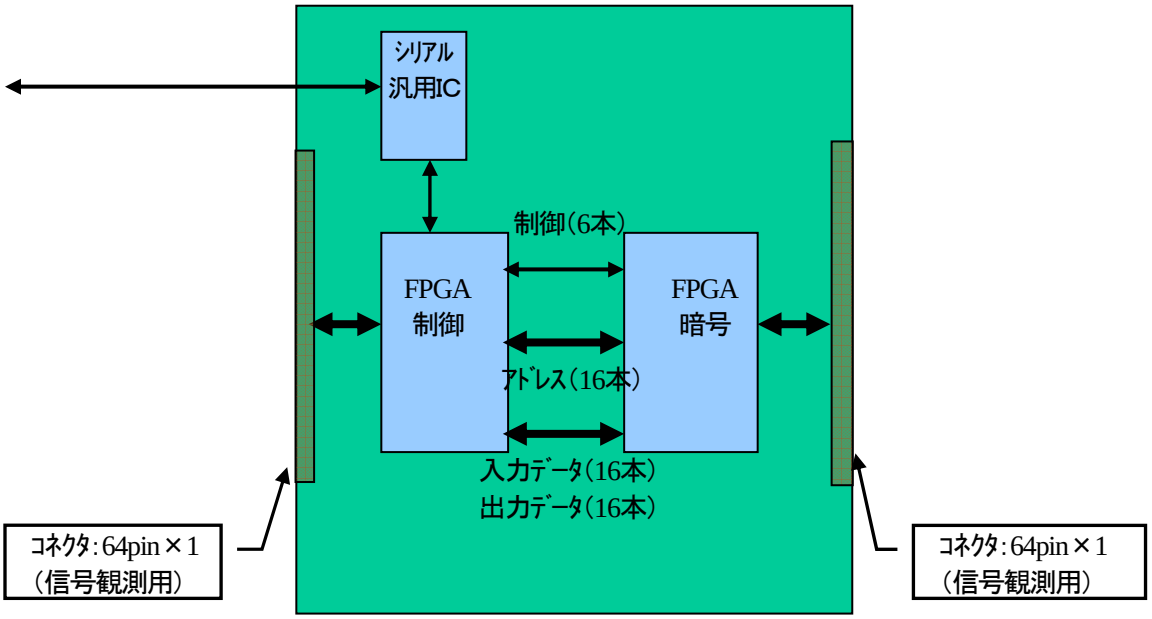
4.　基本機能

4.1 ボード設定

■FPGA 部

メーカ　Xilinx 社製
シリーズ　Virtex Ⅱ Pro
デバイス名　XC2VP30-5FG676C（制御用FPGA）
　　XC2VP7-5FG456C（暗号用FPGA）
パッケージタイプ　FG676、FG456
サイズ　27×27(mm)、23×23(mm)

デバイス	2VP30	2VP7
FPGAユーザIO数	676	456



4.1.1 パワースイッチ

電源はDC3．3VをCN2、CN4から供給してください。

電源供給時はSW1のメインパワースイッチをOFFにしてください。

CN2側　電流測定用FPGA電源

CN4側　コントローラ側FPGA電源

CN2，CN4	1ピン：DC3．3V
	2ピン：DC0V
	3ピン：未接続

電流測定用FPGAのコア電源を外部から供給する場合は、CN5からDC1．5～1．7Vを供給してください。

CN5	1ピン：DC1．5～1．7V
	2ピン：DC0V
	3ピン：未接続

SW1のメインパワースイッチをONにする前に、SW3の設定を確認してください。

CN5からのDC電源を利用する場合はSW3をEXT側に、利用しない場合はINT側に設定してください。

電源がONになるとD1（電流測定側）、D3（コントローラ側）のLEDが点灯します。

4.1.2 電流測定コア電圧切替えスイッチ

SW3は電流測定用FPGAのコア電圧の選択を行ないます。

スイッチの切替えはSW1のメインパワースイッチをOFFの状態で行なってください。

INT側：基板内で生成したコア電圧を供給します。

EXT側：CN3のコア電圧を供給します。

4.1.3 IO電源選択ジャンパ

JP4：電流測定用FGPA側の電源を直接供給するか、MOSリレーを経由して供給するかを切替えます。

ショート状態：直接供給します。

オープン状態：MOSリレーを経由して供給します。（出荷時設定）

JP7：コントローラ用FGPA側の電源を直接供給するか、MOSリレーを経由して供給するかを切替えます。

ショート状態：直接供給します。

オープン状態：MOSリレーを経由して供給します。（出荷時設定）

JP2：JP7がオープン状態の場合にMOSリレーをONにするタイミングを選択します。

ショート状態：2．5V電源の立ち上がりでONにします。（出荷時設定）

オープン状態：1．5V電源の立ち上がりでONにします。

4.1.4 CONFIGリセット切替えジャンパ

JP1：電流測定用FGPA側の電源ON時のコンフィグスタート用のジャンパーです。

1－2ショート：2．5V電源の立ち上がりでスタートします。（出荷時設定）

3－4ショート：1．5V電源の立ち上がりでスタートします。

JP6：コントローラ側FGPA側の電源ON時のコンフィグスタート用のジャンパーです。

1－2ショート：2．5V電源の立ち上がりでスタートします。（出荷時設定）

3－4ショート：1．5V電源の立ち上がりでスタートします。

4.1.5 電流測定ジャンパ

JP3：電流測定用FPGAの電源側シャント抵抗R2のバイパスに使用します。

ショート状態：シャント抵抗R2を無効にします。

オープン状態：シャント抵抗R2を使用します。（出荷時設定）

JP5：電流測定用FPGAのコア電圧1．5VとGNDをショート状態にします。

ショート状態：コア電圧1．5VをGNDレベルにします。

オープン状態：コア電圧1．5Vを有効にします。（出荷時設定）

JP8：電流測定用FPGAのGND側のシャント抵抗R114をバイパスします。

ショート状態：シャント抵抗R114を無効にします。

オープン状態：シャント抵抗R114を使用します。（出荷時設定）

JP10：コントローラ側FPGAの電源側シャント抵抗R125のバイパスに使用します。

ショート状態：シャント抵抗R125を無効にします。

オープン状態：シャント抵抗R125を使用します。（出荷時設定）

JP11：コントローラ側FPGAのコア電圧1．5VとGNDをショート状態にします。

ショート状態：コア電圧1．5VをGNDレベルにします。

オープン状態：コア電圧1．5Vを有効にします。（出荷時設定）

4.1.6 コンフィグ

PCからのFPGAのコンフィグはCN6，CN10を経由してJTAGで行ないます。
コンフィグが完了するとD4（電流測定側）、D14（コントローラ側）のLEDが点灯します。

電流測定側FPGAはCN6をコントローラ側FPGAはCN10を使用します。
JTAGはそれぞれPROM，FPGAの順にカスケードされています。

1ピン：TCK　　2ピン：GND
3ピン：TDO　　4ピン：3．3V
5ピン：TMS
9ピン：TDI　　10ピン：GND

4.1.7 モード切替DIPスイッチ

SW4：電流測定側FPGAのPROMからのコンフィグモードを指定します。
SW8：コントローラ側FPGAのPROMからのコンフィグモードを指定します。

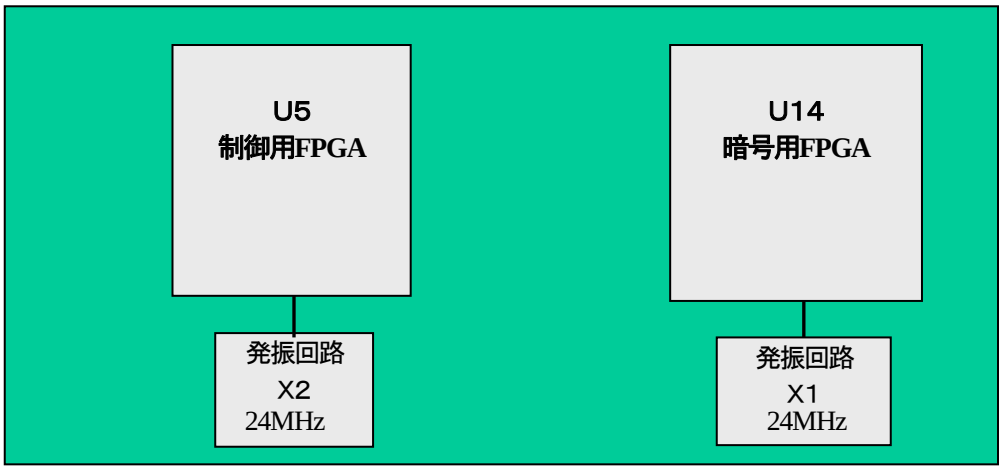
出荷時はMasterSelectMapモードになっています。

1：M0　出荷時設定OFF
2：M1　出荷時設定OFF
3：M2　出荷時設定ON
4：PWRDWN　出荷時設定OFF
5：HSWAP　出荷時設定OFF
6－8は未使用です。

4.1.8 リコンフィグスイッチ

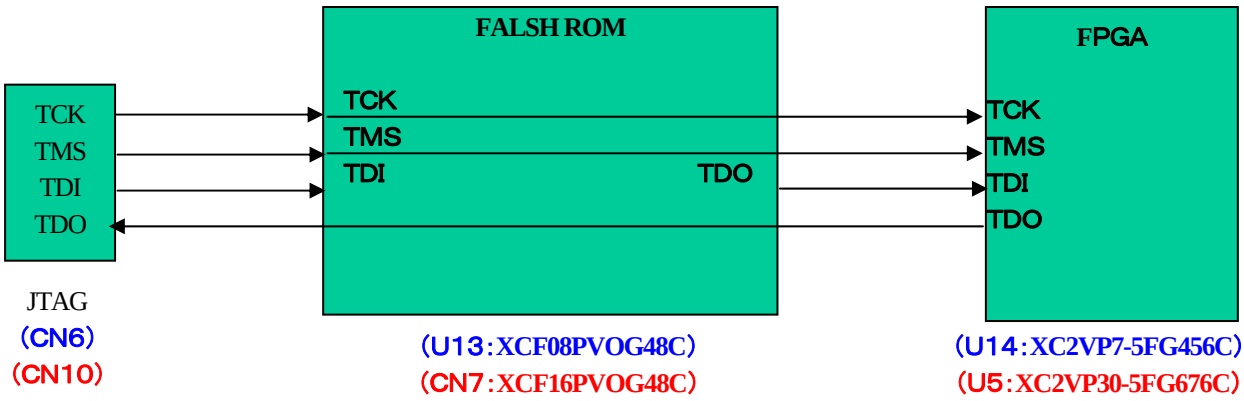
SW2：両方のFPGAをPROMから再コンフィグします。
SW4：コントローラ側のFPGAをPROMから再コンフィグします。

4.2 クロック系統



■ 各FPGAは独立したクロックIC（X1，X2：24MHz）からクロック入力される。
U5（制御用FPGA）・・・X2 （テストポイント：TP26、測定ポイント：J4）
U14（暗号用FPGA）・・・X1 （テストポイント：TP15、測定ポイント：J3）

4.3 コンフィギュレーション部

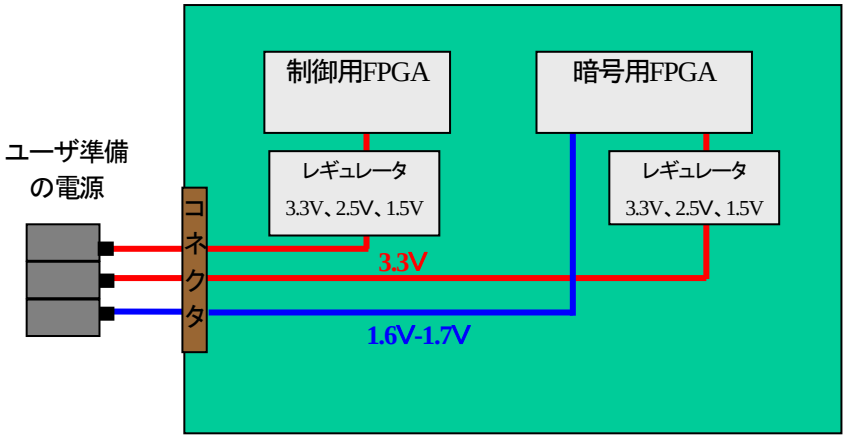


■Xilinx パラレルケーブルⅣ

Xilinx社ダウンロード・ケーブル。今回は、JTAG機能を使いデータ転送を行う。

※2種類のFPGAはそれぞれ独立した、JTAGチェーンで構成され、別々にコンフィギュレーション可能である。

4.4 電源部



○外部電圧(VCC)　・・・　3．3V
供給源　・・・　各FPGA用コネクタより供給する。

暗号回路FPGA用コネクタ
（VCC）　・・・　CN2（1pin）
（GND）　・・・　CN2（2pin）
テストポイント　・・・　TP1

制御回路FPGA用コネクタ
（VCC）　・・・　CN4（1pin）
（GND）　・・・　CN4（2pin）
テストポイント　・・・　TP11

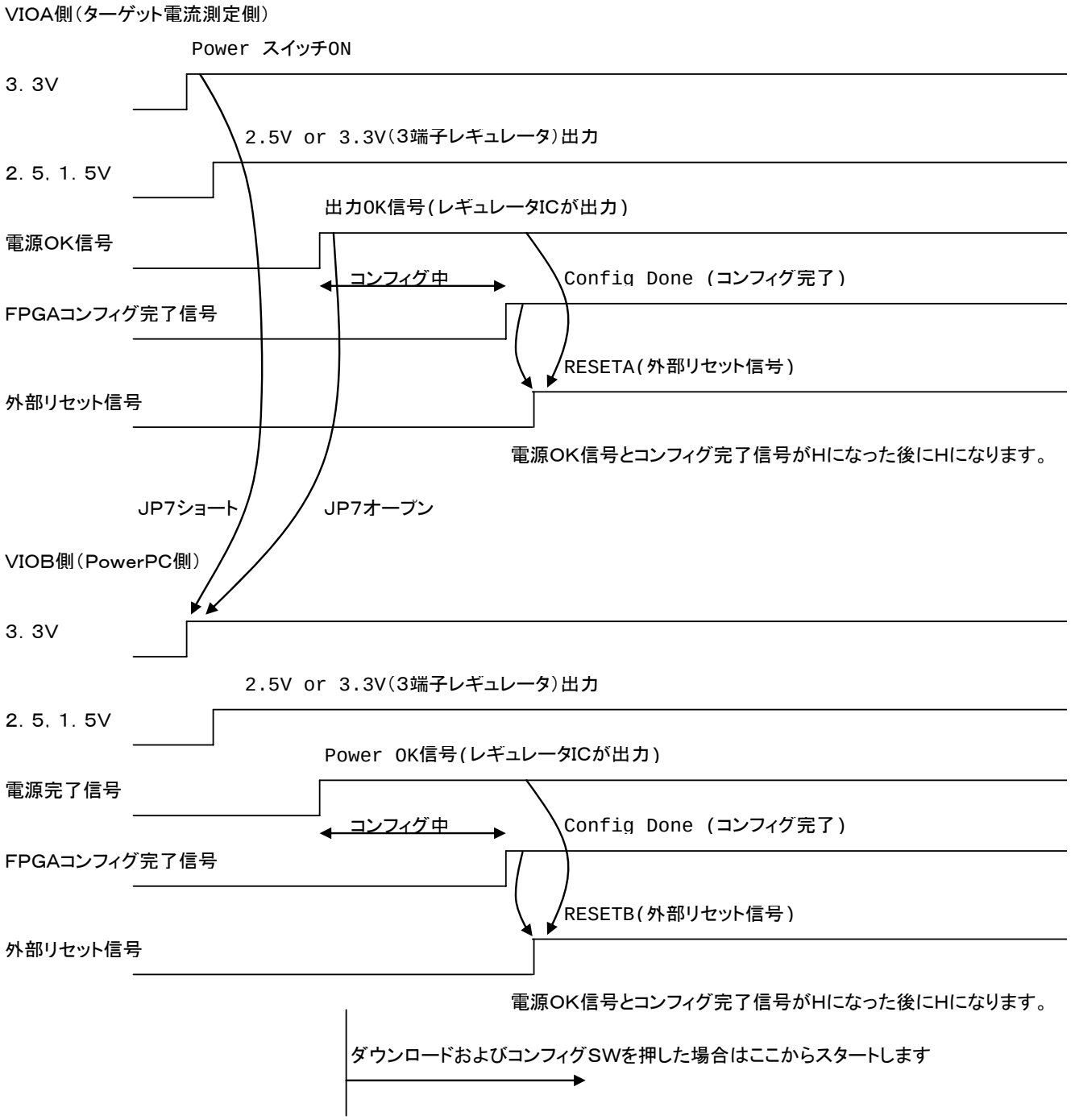
暗号回路外部入力コネクタ
（VCC）　・・・　CN5（1pin）
（GND）　・・・　CN5（2pin）
テストポイント　・・・　TP3、4

○内部電圧25　・・・　2．5V
供給源　・・・　三端子レギュレータ(TPS72625DCQ)にて生成する。
テストポイント　・・・　TP12（暗号回路FPGA）
テストポイント　・・・　TP23（制御回路FPGA）

○内部電圧18　・・・　1．8V
供給源　・・・　三端子レギュレータ(PQ1U181M2ZPH)にて生成する。
テストポイント　・・・　TP14（暗号回路FPGA）
テストポイント　・・・　TP25（制御回路FPGA）

○内部電圧15　・・・　1．5V
供給源　・・・　三端子レギュレータ(MAX8556ETE)にて生成、または外部入力する。
テストポイント　・・・　TP3、4（暗号回路FPGA）

■電源シーケンス


VIOA側（ターゲット電流測定側）
Power スイッチON
3．3V
2.5V or 3.3V（3端子レギュレータ）出力
2．5．1．5V
出力OK信号（レギュレータICが出力）
電源OK信号
コンフィグ中
Config Done （コンフィグ完了）
FPGAコンフィグ完了信号
RESETA（外部リセット信号）
外部リセット信号
電源OK信号とコンフィグ完了信号がHになった後にHになります。
JP7ショート
JP7オープン
VIOB側（PowerPC側）
3．3V
2.5V or 3.3V（3端子レギュレータ）出力
2．5．1．5V
Power OK信号（レギュレータICが出力）
電源完了信号
コンフィグ中
Config Done （コンフィグ完了）
FPGAコンフィグ完了信号
RESETB（外部リセット信号）
外部リセット信号
電源OK信号とコンフィグ完了信号がHになった後にHになります。
ダウンロードおよびコンフィグSWを押した場合はここからスタートします

4.5 インターフェース部

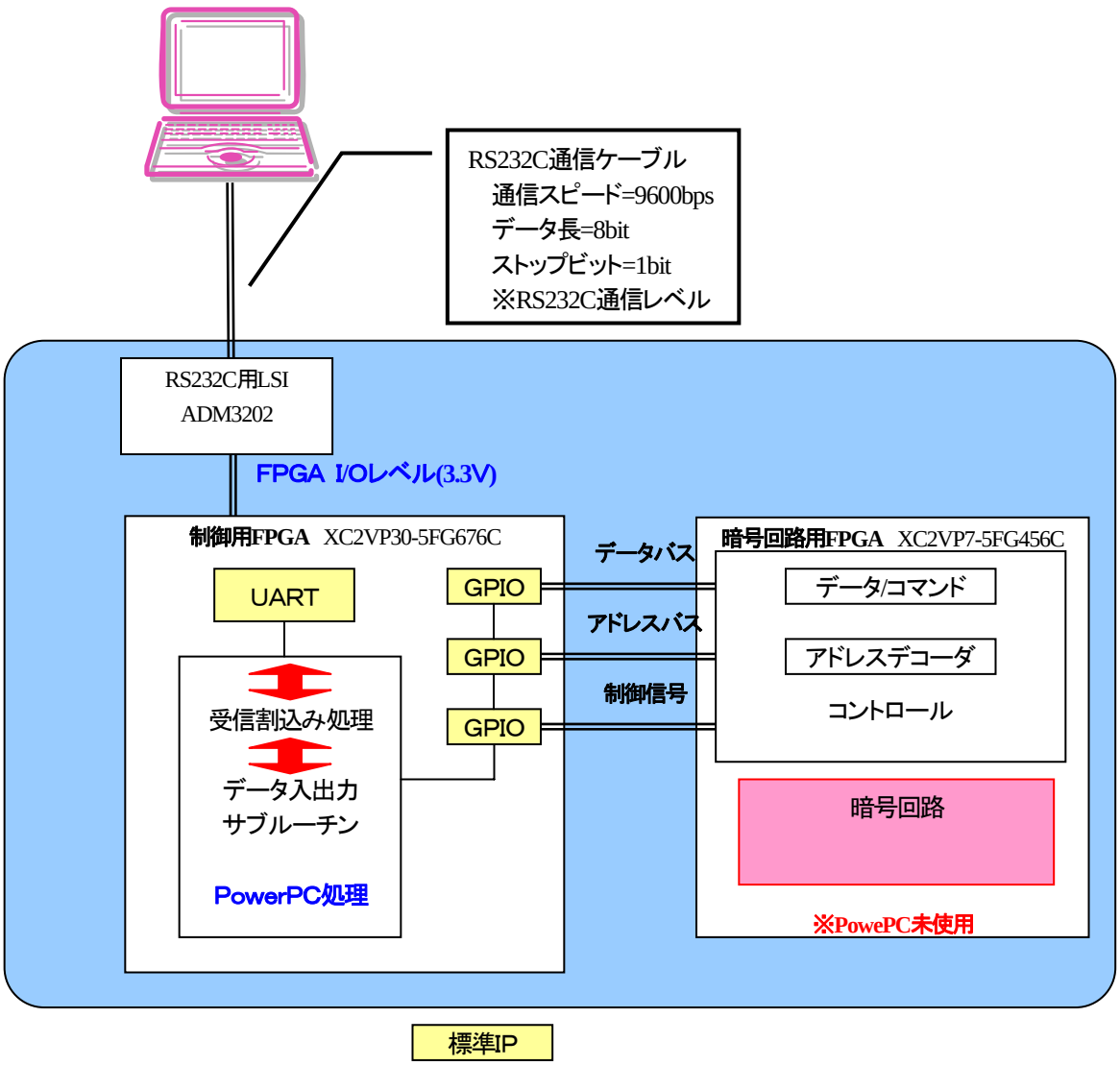
○シリアルインターフェース　　※詳細は、***2. I/O Signal*** を参照下さい。

■CN12（ XM2C-0912-111 ： オムロン製 オス側 ）

信号	CN12 (XM2C-0912-111)	U16 (ADM3202ARN)		U5 (XC2VP30-5FG676C)
TX	2pin	14pin	11pin	M25
RX	3pin	13pin	12pin	M26
CTS	8pin	7pin	10pin	N25
RTS	7pin	8pin	9pin	L26

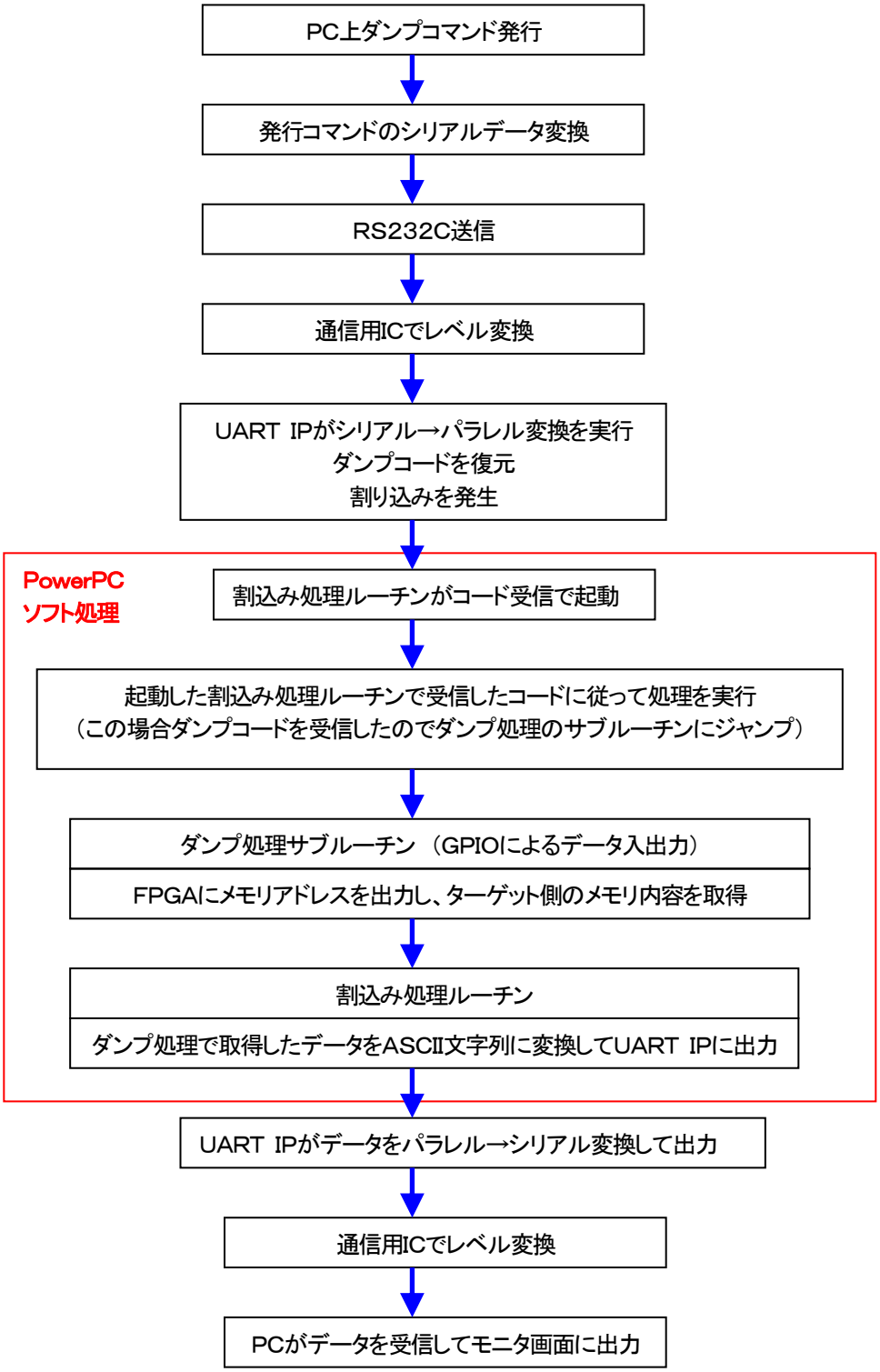
■PCとの接続

シリアル通信ケーブル（ストレート：9pin）で接続する。



■シリアルI/Fプロトコル例

データダンプ・コマンドの場合



5.　回路図

【暗号回路用FPGA周辺】

FPGA接続部, 電源部, コンフィギュレーション部　　・・・・・　28ページ

FPGA接続部　　・・・・・　29ページ

FPGA電源接続部・・・・・　30ページ

【制御回路用FPGA周辺】

FPGA接続部, 電源部, コンフィギュレーション部　　・・・・・　31ページ

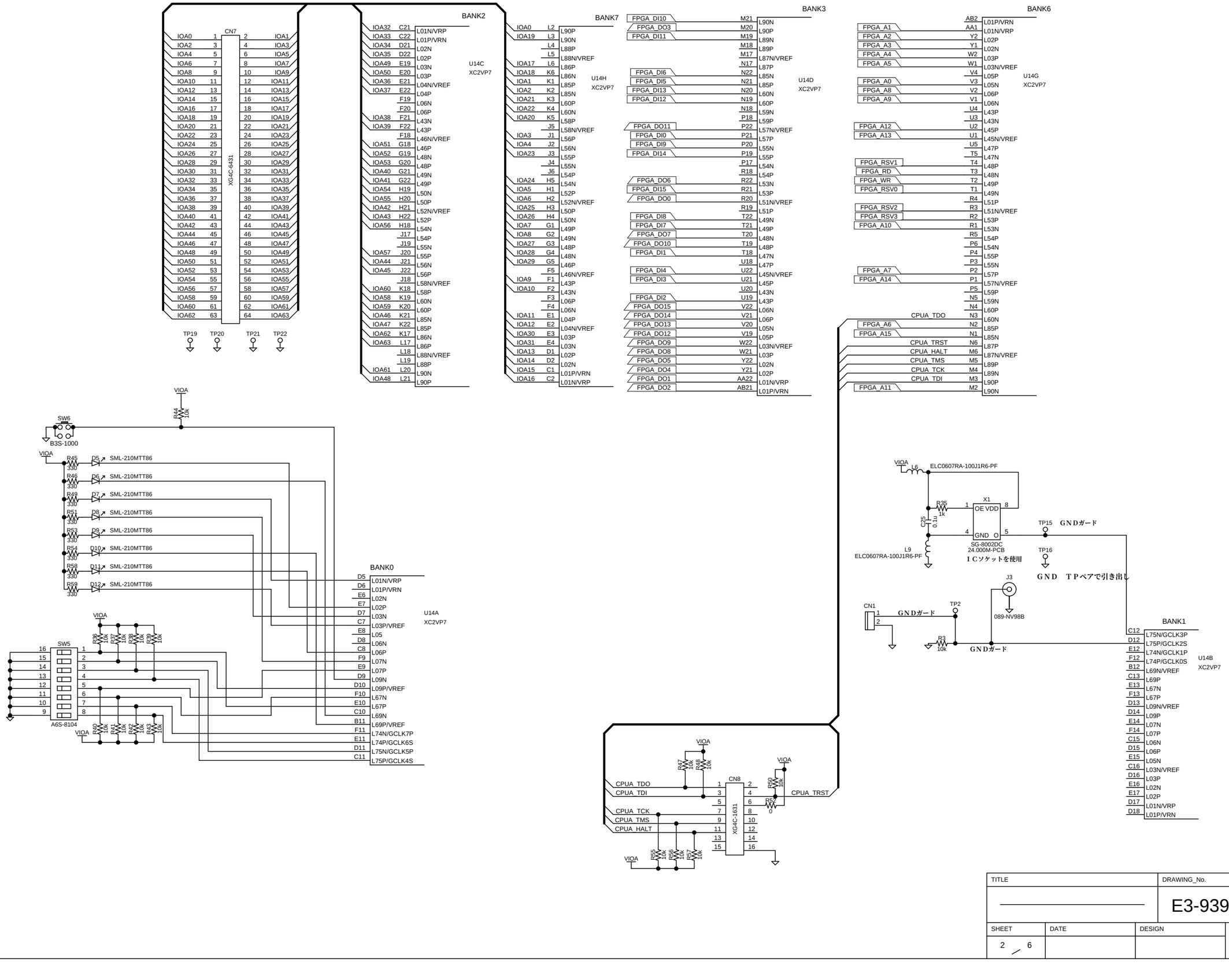
FPGA接続部　　・・・・・　32ページ

FPGA電源接続部・・・・・　33ページ

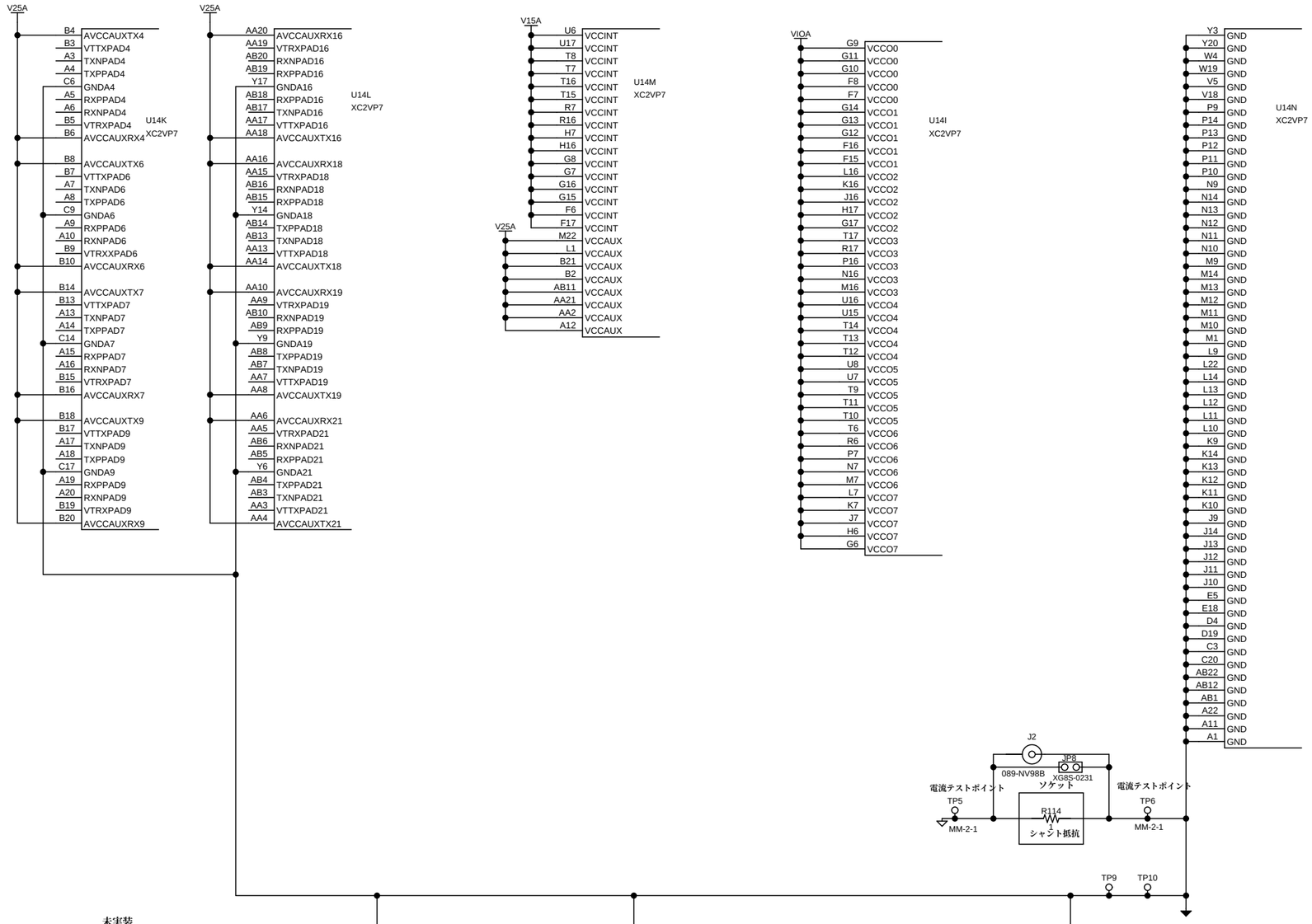
外部入力電源１
3.3V
外部入力電源２
3.3V
外部入力電源３
コア電源　1.6-1.7V
未実装
FPGA１メイン電源
FPGA２メイン電源
電流テストポイント
ソケット
シャント抵抗
CONFRST_BUTTON
RESETA
CONFIG
TCK
TDO
TMS
TDI
GND　TPペアで引き出し
GNDガード
BANK5
BANK4
U14F
XC2VP7
U14E
XC2VP7
U14J
XC2VP7
U13
XCF08PVOG48C
U1 TPS72625DCQ
U6
MAX8556ETE
U8 PQ1U181M2ZP
SW1
SW2
SW3
SW4
M2T-22AAP4
M2T-12AAP1
B3S-1000
B3P-VH
B3P-XH-A
A6S-8104
XG8T-0431
XG4C-1031
089-NV98B
XG8S-0231
SML-210MTT86
74HC14
74HC08
MM-2-1
BLM18AG102SN
POWERA_CNT
CN2
CN3
CN4
CN5
CN6
J1
JP1
JP2
JP3
JP4
JP5
JP7
TP1
TP2
TP3
TP4
TP5
TP6
TP7
TP8
TP9
TP11
TP12
TP13
TP14
TP17
TP18
VR1
SW4
P1
P2
P3
P4
P5
P6
P7
P8
P9
OSCX
GCLK
PROG_B
DONE
M0
M1
M2
TCK
TDI
TDO
TMS
PWRDWN_B
HSWAP_EN
RSVD
VBATT
DXP
DXN
CDA0
CDA1
CDA2
CDA3
CDA4
CDA5
CDA6
CDA7
REV_SEL1
REV_SEL0
EN_EXT_SEL
CONFIG
VIOA
VIOB
V25A
V18A
V15A
270u/16V(OS)
100u/16V
150u/6.3V

TITLE	DRAWING_No.
	E3-93961-1

SHEET	DATE	DESIGN
1 / 6		



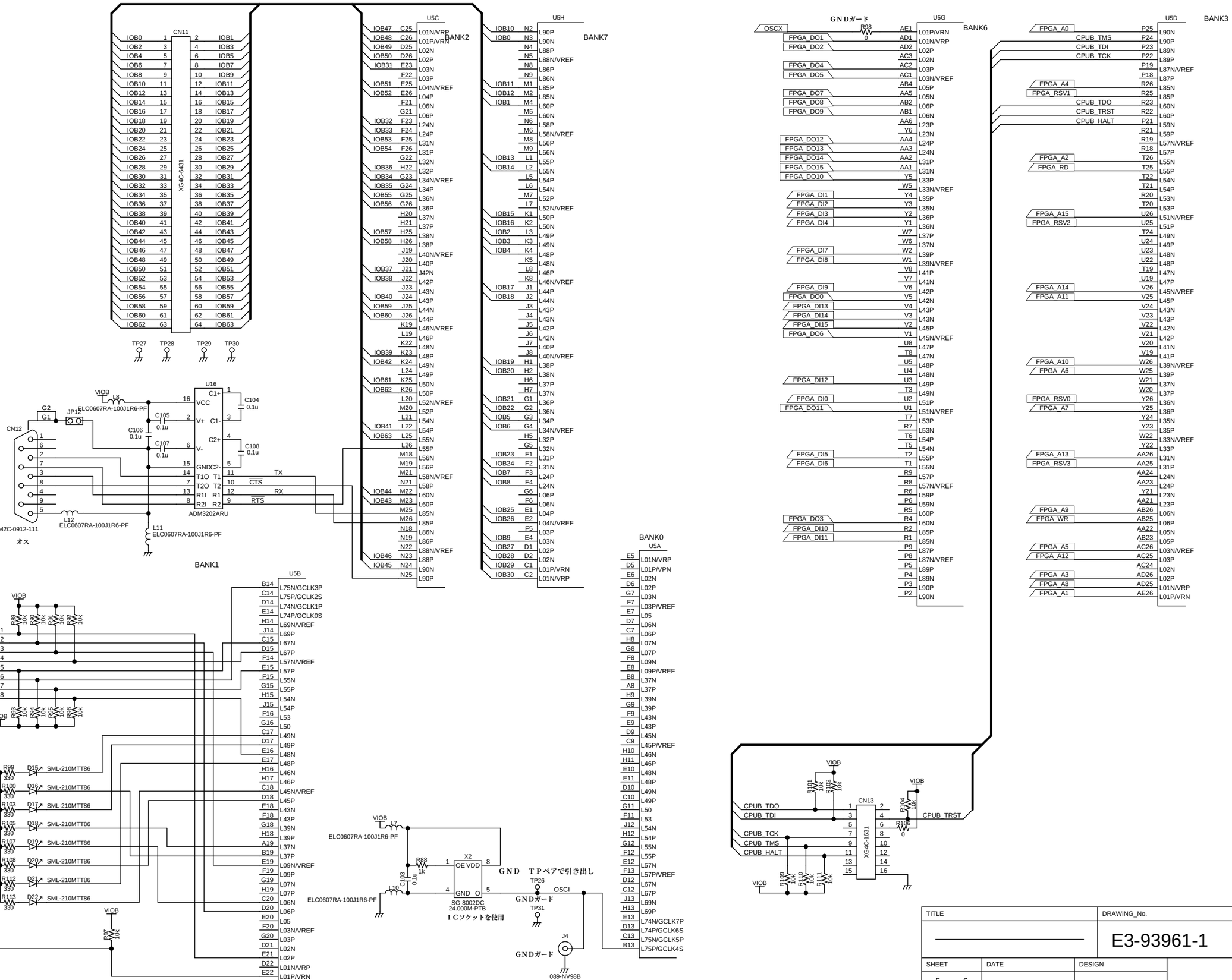
TITLE	DRAWING_No.
	E3-93961-1
SHEET 2 / 6	DATE
DESIGN	



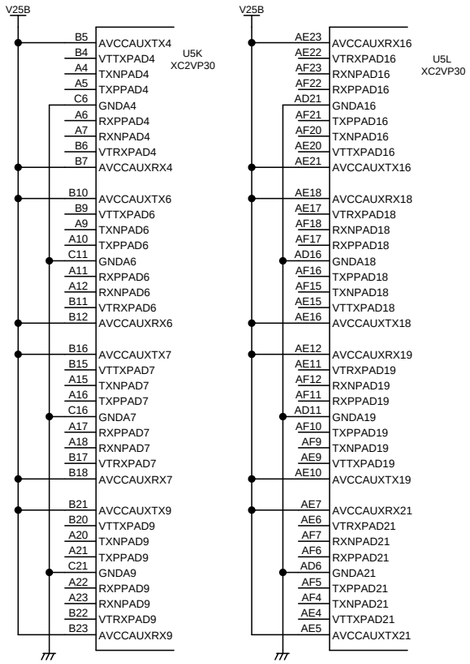
TITLE	DRAWING_No.
	E3-93961-1
SHEET 3 / 6	DATE
DESIGN	

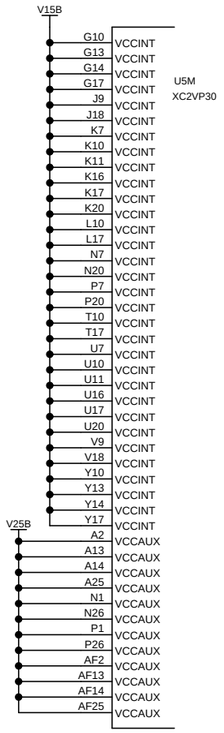
CN9
POWERA_CNT
VIOB
R60 1k
U9 TPS72625DCQ
IN OUT
ENA RESET
TP23
V25B
C83 100u/16V
C84 0.1u
C85 0.1u
C86 270u/16V(OS)
未実装
R124 100
CONFRST_BUTTON
SW7 B3S-1000
R62 1k
R61 10k
D13 1SS352
U10A 74HC14
U10F 74HC14
U11A 74HC08
TP24
RESETB
JP6 XG8T-0431
C91 0.1u
C92 0.1u
R63 1k
U11D 74HC08
C87 0.1u
C88 0.1u
C89 0.1u
C90 0.1u
V18B
U7
C93 150u/6.3V
C94 270u/16V(OS)
C95 47u
U12 MAX8556ETE
IN OUT POK EN FB NC GND
C96 47u
C97 47u
C98 150u/6.3V
R64 2k
R125 シャント抵抗
V15B
JP9 XG8S-0231
JP10 XG8S-0231 ショート
R65 1k
R126 100
未実装
R66 1k
R67 1k
R68 1k
R69 1k
R70 1k
VR2 1k
R71 470
R129 後付 1k
TCK
TDO
TMS
TDI
XG4C-1031
CN10
R72 22
R73 22
R76 22
CDB7
CDB6
CDB5
CDB4
CDB3
CDB2
CDB1
CDB0
R74
R75
R77 4.7k
XCF16PVOG48C
U15 PQ1U181M2ZP
C99 100u/16V
C100 0.1u
C101 270u/16V(OS)
C102 0.01u
R127 100
未実装
R78 470
CONFIG
D14 SML-210MTT86
R82 1k
R80 1k
R81 1k
U5E
U5J XC2VP30
CCLK
PROG_B
DONE
M0
M1
M2
TCK
TDI
TDO
TMS
PWRDWN_B
HSWAP_EN
RSVD
VBATT
DXP
DXN
R83 4.7k
R84 4.7k
R85 4.7k
R86 4.7k
R87 4.7k
SW8 A6S-8104
P10
P11
P12
P13
P14
P15
P16
P17
P18
GND TPペアで引き出し
U11C 74HC08
U11B 74HC08
U10D 74HC14
U10C 74HC14
U10E 74HC14
U10B 74HC14
U5F
BANK5
BANK4
L75N/GCLK7S
L75P/GCLK6P
L74N/GCLK5S
L74P/GCLK4P
L69N/VREF
L69P
L67N
L67P
L57N/VREF
L57P
L55N
L55P
L54N
L54P
L53
L50
L49N
L49P
L48N
L48P
L46N
L46P
L45N
L45P
L43N
L43P
L39N
L39P
L37N
L37P
L09N/VREF
L07N/VREF
L07P
L06N/VRP
L06P/VRN
L05
L03N/D4
L03P/D5
L02N/D6
L02P/D7
L01N/RDWR_B
L01P/CS_B
L01N/BUSY/DOOUT
L01P/INIT_B
L02N/D0/DIN
L02P/D1
L03N/D2
L03P/D3
L05
L06N/VRP
L06P/VRN
L07N
L07P/VREF
L09N
L09P/VREF
L37N
L37P
L39N
L39P
L43N
L43P
L45N
L45P/VREF
L46N
L46P
L48N
L48P
L49N
L49P
L50
L53
L54N
L54P
L55N
L55P
L57N
L57P/VREF
L67N
L67P
L69N
L69P/VREF
L74N/GCLK3S
L74P/GCLK2P
L75N/GCLK1S
L75P/GCLK0P

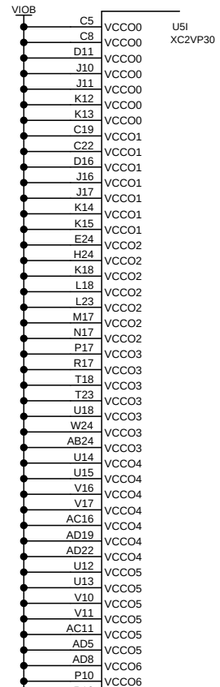
TITLE	DRAWING_No.
	E3-93961-1
SHEET 4 / 6	DATE
DESIGN	

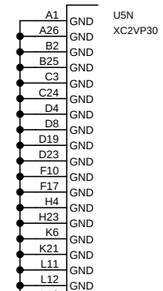


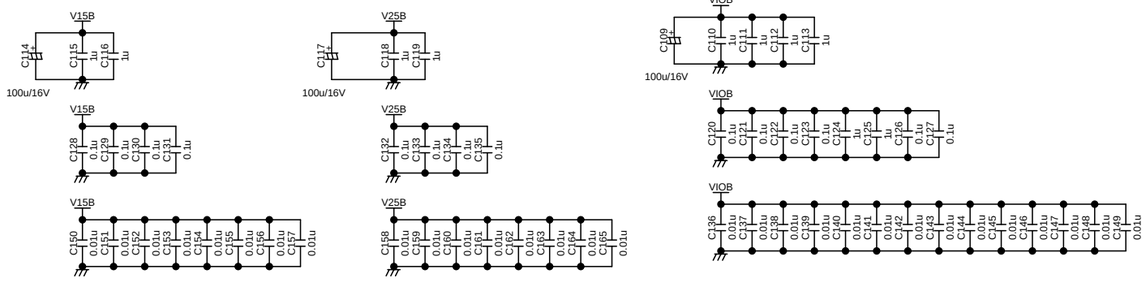
TITLE	DRAWING_No.
	E3-93961-1
SHEET 5 / 6	DATE
DESIGN	











TITLE	DRAWING_No.
	E3-93961-1
SHEET	DATE	DESIGN
6 / 6		

6.　部品リスト

セット名	FPGA暗号評価ボード
基板番号	3-93296-1

品名	型名	メーカ	数量	
積層セラC（チップ）	GRM155F11H103ZA57E	ムラタ	32	C24,C53,C54,C55,C56,C57,C58,C59,C60,C61,C62,C63,C64,C65,C66,C67,C68,C69,C70,C71,C72,C73,C74,C75,C76,C77,C78,C79,C80,C81,C82,C102,C136,C137,C138,C139,C140,C141,C142,C143,C144,C145,C146,C147,C148,C149,C150,C151,C152,C153,C154,C155,C156,C157,C158,C159,C160,C161,C162,C163,C164,C165
積層セラC（チップ）	GRM155F11E104ZA01D	ムラタ	41	C2,C4,C6,C7,C9,C10,C11, C12,C13,C14,C22,C25,C37,C38,C39,C40,C43,C44,C45,C46,C47,C48,C49,C50,C51,C52,C84,C85,C87,C88,C89,C90,C91,C92,C100,C103,C104,C105,C106,C107,C108,C120,C121,C122,C123,C126,C127,C128,C129,C130,C131,C132,C133,C134,C135
積層セラC（チップ）	GRM155F11E105ZE01D	ムラタ	10	C27,C28,C29,C30,C32,C33,C35,C36,C41,C42,C110,C111,C112,C113,C115,C116,C118,C119,C124,C125
積層セラC（チップ）	C4532JF1C476Z	TDK	4	C15,C20,C95,C96　(4532 47u/16V)
アルミ電解（チップ）	EMV-6R3ADA101MF55G	日本ケミコン	9	C1,C3,C5,C21,C26,C31,C34,C83,C99,C109,C114,C117　(100u/6.3V)
OSコンデンサ	EEFUE0J151R	松下	4	C17,C19,C94,C98　(150u/6.3V)
OSコンデンサ	APSA100ELL271MHB5S	日本ケミコン	8	C8,C16,C18,C23,C86,C93,C97,C101
ダイオード（チップ）	1SS352(-TPH3)	東芝	2	D2,D13
フィルタ	BLM18BD182SN1D	村田	5	L1,L2,L3,L4,L5
インダクタ	ELC0607RA-100J1R6-PF	TDK	7	L6,L7,L8,L9,L10,L11,L12 (ELC0607S-100J1R6-PF)
コネクター	DF1-2P-2.5DSA	ヒロセ	1	CN1
コネクター	DF1-6P-2.5DSA	ヒロセ	2	CN3,CN9
レギュレータIC	PQ1U181M2ZPH	シャープ	2	U8,U15
レギュレータIC	TPS72625DCQ	TI	2	U1,U9
レギュレータIC	MAX8556ETE	マキシム	2	U6,U12
FPGA	XC2VP30-5FG676C	ザイリンクス	1	U5
FPGA	XC2VP7-5FG456C	ザイリンクス	1	U14
ROM	XCF08PVOG48C	ザイリンクス	1	U13
ROM	XCF16PVOG48C	ザイリンクス	1	U7
CMOS	SN74HC08NS	TI	2	U3,U11
CMOS	SN74HC14NSE4	TI	2	U2,U10
通信IC	ADM3202ARUZ	Analog device	1	U16

LED	SML-210MTT86	ローム	20	D1,D3,D4,D5,D6,D7,D8,D9,D10,D11,D12,D14,D15,D16,D17,D18,D19,D20,D21,D22
コネクター	XG4C-1031	オムロン	2	CN6,CN10
コネクター	XG4C-1631	オムロン	2	CN8,CN13
ショートポスト	XG8T-0431	オムロン	3	JP1,JP2,JP6
ショートポスト	XG8S-0231	オムロン	7	JP3,JP4,JP5,JP7,JP8,JP9,JP10
MOSリレー	AQY212GS	松下	3	U4,U17,U18
SG-8002DC	24.000M-PCB	エプソン	2	X1,X2 (ICソケット)
チップ抵抗	RK73Z1JTD 0Ω	KOA	3	R52,R98,R106
チップ抵抗	RR0816P-103-D	進工業	32	R3,R5,R36,R37,R38,R39,R40,R41,R42,R43,R47,R48,R50,R55,R56,R57,R61,R89,R90,R91,R92,R93,R94,R95,R96,R101,R102,R104,R109,R110,R111,R120
チップ抵抗	RR0816P-102-D	進工業	30	R4,R7,R10,R12,R13,R14,R15,R16,R17,R22,R26,R27,R28,R29,R35,R60,R62,R63,R65,R66,R67,R68,R69,R70,R79,R80,R81,R82,R88,R128,R129
チップ抵抗	RR0816P-201-D	進工業	2	R8,R9
チップ抵抗	RR0816P-220-D	進工業	6	R19,R20,R24,R72,R73,R76
チップ抵抗	RR0816P-331-D	進工業	18	R1,R6,R45,R46,R49,R51,R53,R54,R58,R59,R99,R100,R103,R105,R107,R108,R112,R113
チップ抵抗	RR0816P-472-D	進工業	18	R21,R23,R25,R30,R31,R32,R33,R34,R44,R74,R75,R77,R83,R84,R85,R86,,R87,R97
チップ抵抗	RR0816P-471-D	進工業	4	R18,R28,R71,R78
チップ抵抗	RR0816P-202-D	進工業	2	R11,R64
チップ抵抗	RR0816P-101-D	進工業	2	R115,R116,R117,R118,R119,R120,R121,R122,R123,R124,R126,R127
トリマ	ST-32EA 1KΩ(13)	コパル	2	VR1,VR2
SMAレセプタクル	089-NV98B	ユウエツ	4	J1,J2,J3,J4
Dサブコネクタ	XM2C-0912-111	オムロン	1	CN12
コネクタ	A1-64PA-2.54DSA(71)	ヒロセ	2	CN7,CN11
コネクタ	B3P-VH(LF)(SN)	日圧	2	CN2,CN4
コネクタ	B3B-XH-A(LF)(SN)	日圧	1	CN5(マスキング)
シャント抵抗	ERX1SJ1R0	松下	3	R2,R114,R125 (ソケット)
DIPスイッチ	A6S-8104	オムロン	4	SW4,SW5,SW8,SW9
タクトスイッチ	B3S-1000	オムロン	4	SW2,SW6,SW7,SW10
スライドスイッチ	CS-12AAP1	日開	1	SW3
スライドスイッチ	CS-22AAP1	日開	1	SW1

テストポイント	LC-3-G(黄)	MAC8	12	TP1,TP2,TP11,TP12,TP13,TP14,TP15,TP17,TP23,TP24,TP25,TP26
テストポイント	LC-3-G(黒)	MAC8	15	TP7,TP8,TP9,TP10,TP16,TP18,TP19,TP20,TP21,TP22,TP27,TP28,TP29,TP30,TP31
電流テストポイント	MM-2-1	MAC8	4	TP3,TP4,TP5,TP6
ショートソケット	XJ8A-0211	オムロン	10	
ICソケット	R110-91-308	プレシディップ	2	
ソケット	PM-3	マックエイト	1	
コネクタソケット	VHR-3N	日圧	2	CN2,CN4
コンタクト	BVH-41T-P1.1	日圧	4	CN2,CN4
ゴム足	BU-692-A	サトーパーツ	4	
スペーサ	ASB320	広杉	4	
ネジ	バインド M3×8		4	
ネジ	Wセムス M3×6		4	
コネクタ	XG4H-1031	オムロン	2	変換基板実装
コネクタ	87832-1420	モレックス	2	変換基板実装
シャント抵抗	ERX1SJ 1R0	松下	2	添付部品
シャント抵抗	ERX1SJ 1R2	松下	2	添付部品
シャント抵抗	ERX1SJ 1R5	松下	2	添付部品
シャント抵抗	ERX1SJ 1R8	松下	2	添付部品
シャント抵抗	ERX1SJ 2R2	松下	2	添付部品
シャント抵抗	ERX1SJ 2R7	松下	2	添付部品
シャント抵抗	ERX1SJ 3R3	松下	2	添付部品
シャント抵抗	ERX1SJ 3R9	松下	2	添付部品
シャント抵抗	ERX1SJ 4R7	松下	2	添付部品
シャント抵抗	ERX1SJ 5R6	松下	2	添付部品
シャント抵抗	ERX1SJ 6R8	松下	2	添付部品
シャント抵抗	ERX1SJ 8R2	松下	2	添付部品

※　赤字は、未実装対応

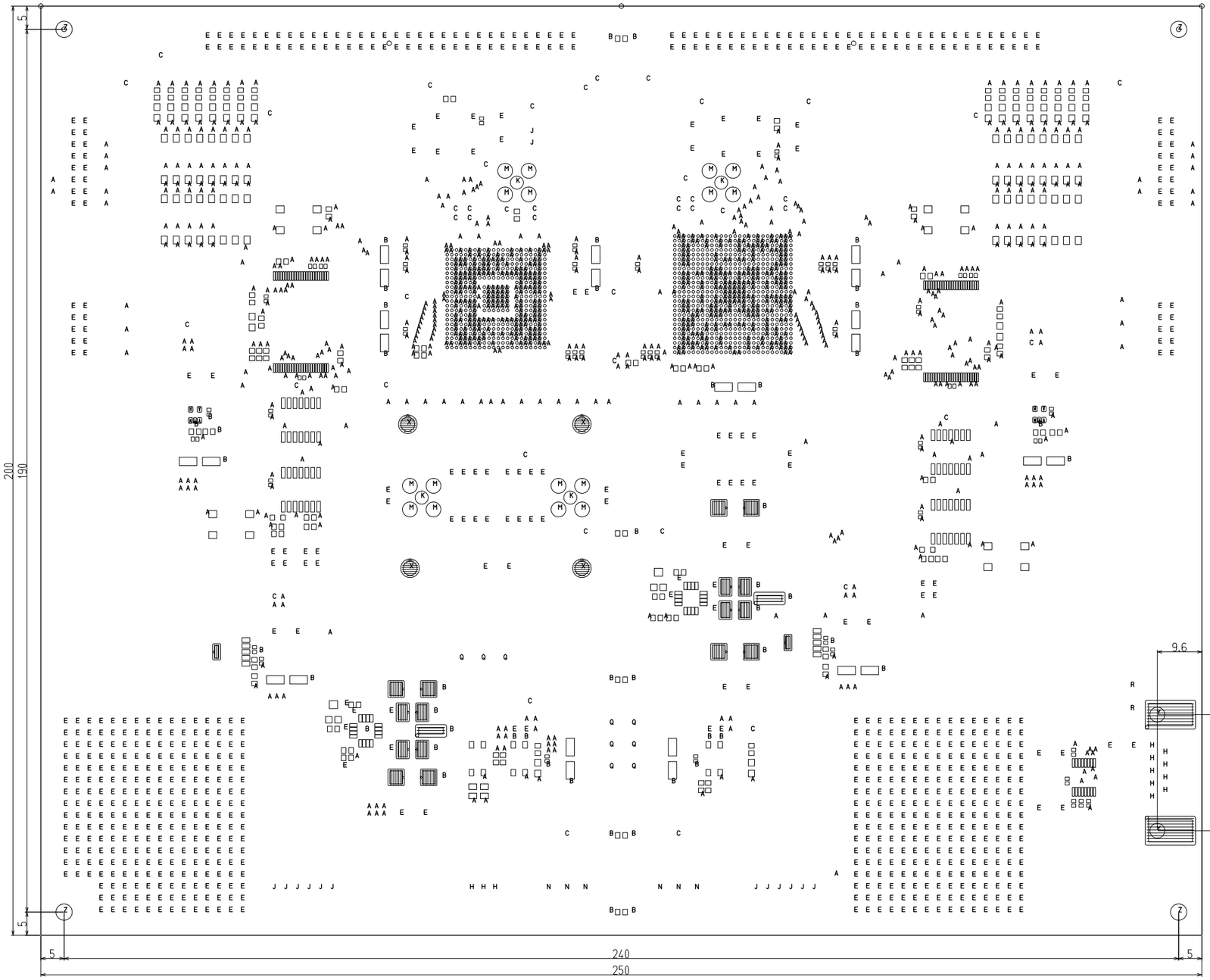
7.　プリント配線版資料

◎基板仕様

寸法　・・・　250×200×1.6[㎜]
層数　・・・　8層
材質　・・・　FR－4

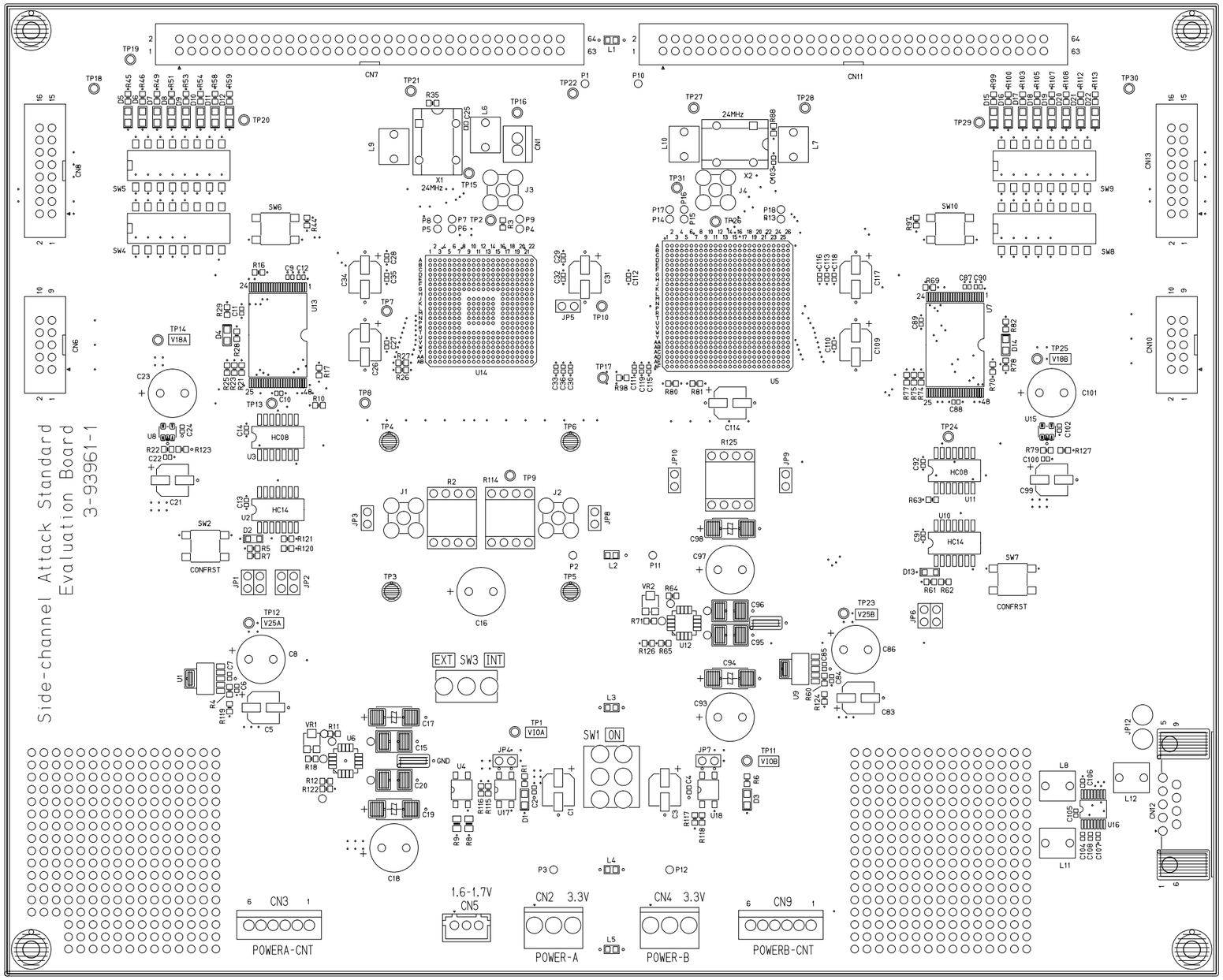
図面

寸法図　・・・・・　38ページ
部品面配置図　・・・・・　39ページ
半田面配置図　・・・・・　40ページ
部品面シルク図　・・・・・　41ページ
半田面シルク図　・・・・・　42ページ



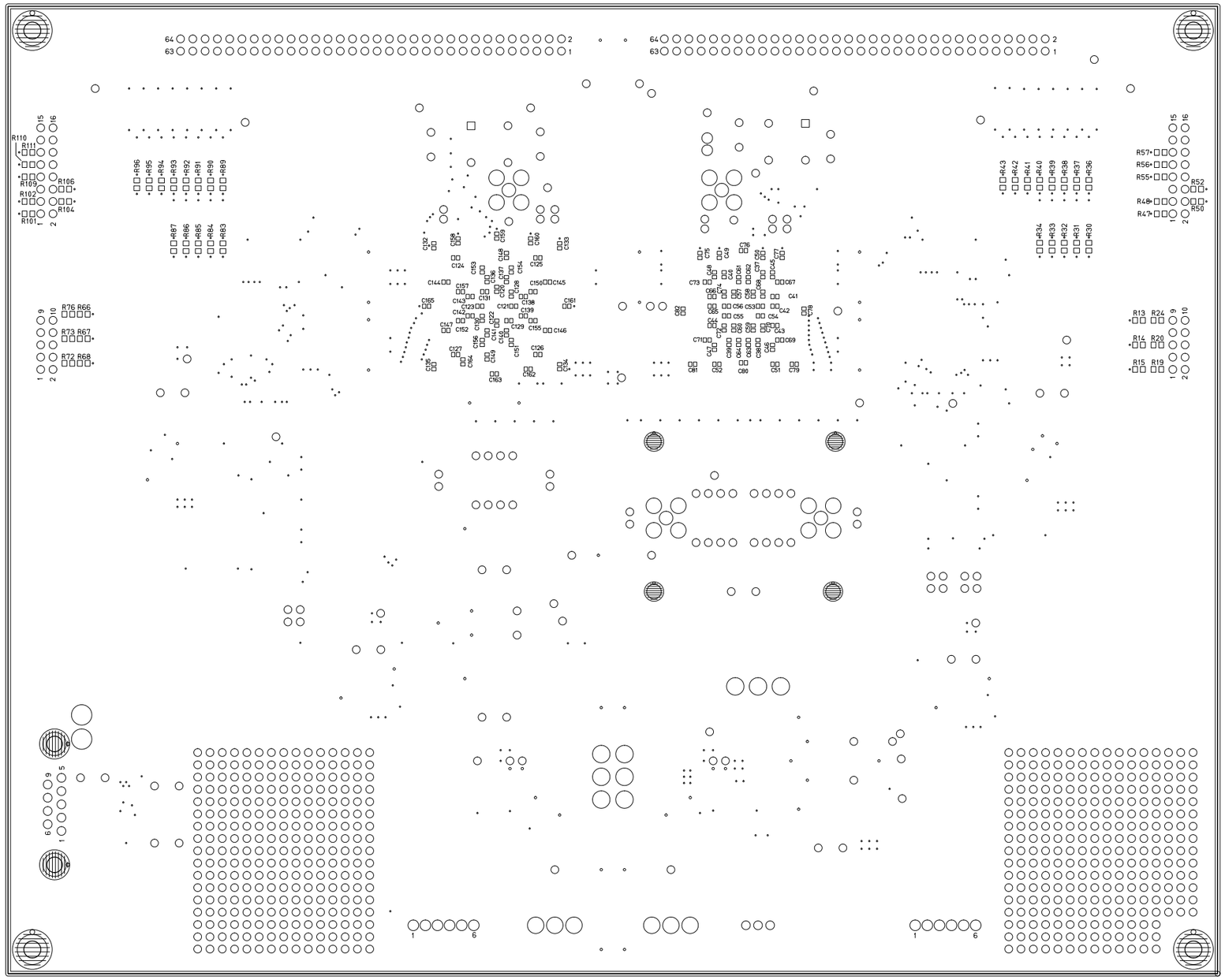
form	diameter	number
X	1.6000	4
Y	3.2000	2
Z	3.5000	4
A	0.3000	1027
B	0.5000	59
C	0.8000	45
E	0.9000	796
H	1.0000	12
J	1.2000	14
K	1.5000	4
M	1.7000	16
N	1.8000	6
Q	1.9000	9
R	2.0000	2

Evaluation Board
2007/02/13



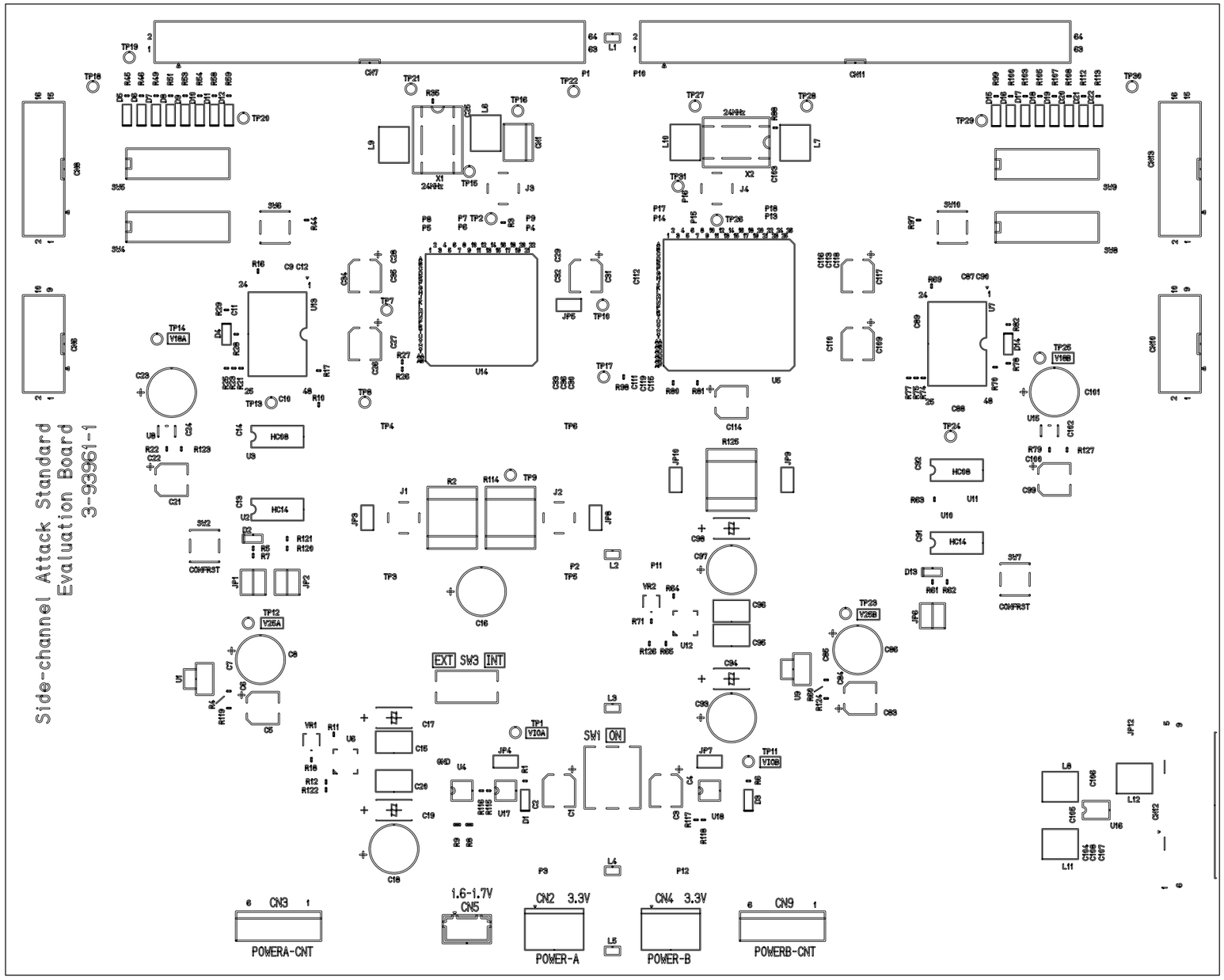
CS

Evaluation Board
2007/02/13



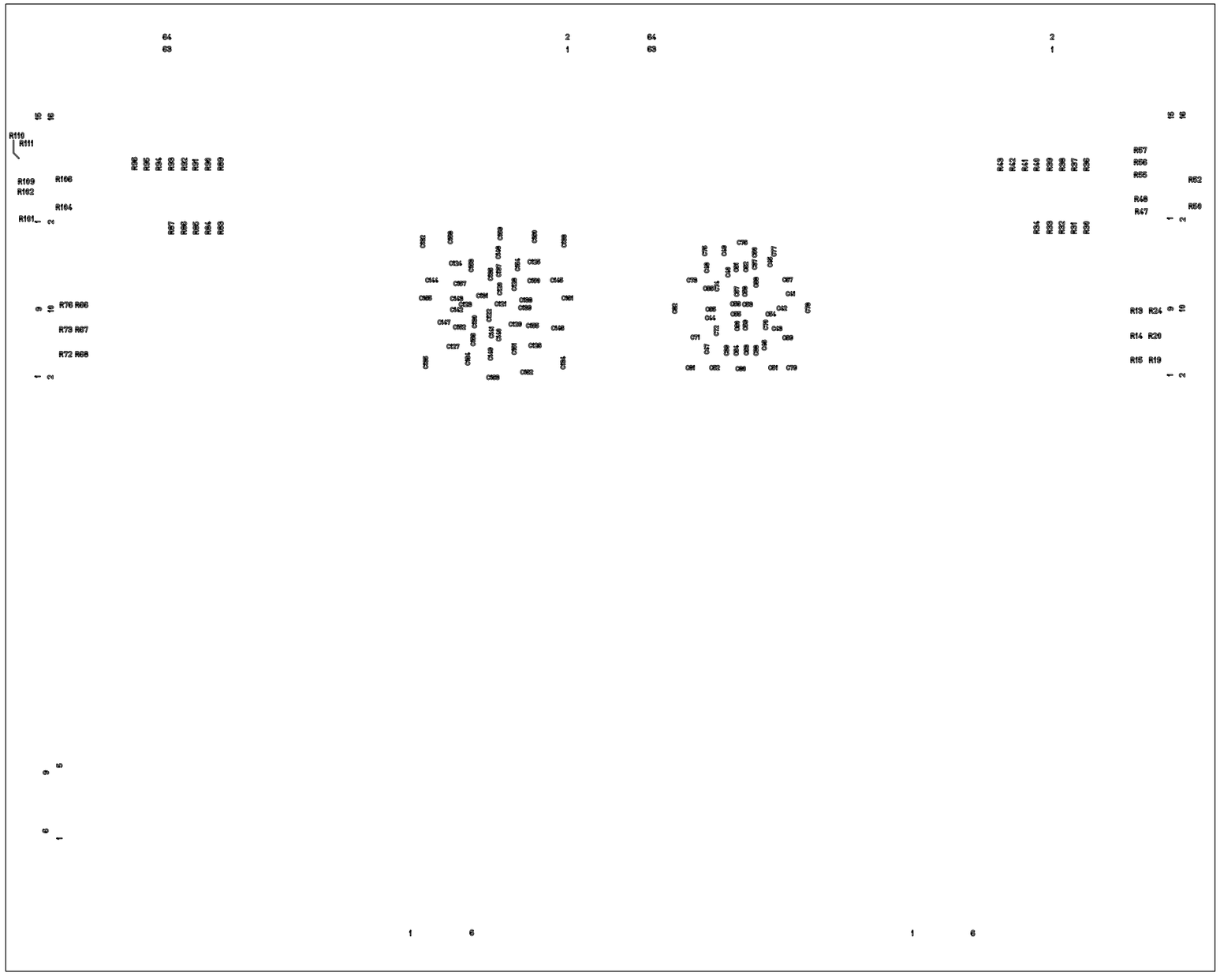
55

Evaluation Board
2007/02/13



CS

Evaluation Board
2007/02/13



Evaluation Board
2007/02/13

8. 検査仕様

検査項目

○検査ボード型式 ・・・ XX07-001A
○ボード番号 ・・・ ボード単位シリアル番号
○検査内容

1. 実装状態	・・・	外観チェック
2. BGA X線解析	・・・	写真撮影 ＋ 写真判定補足チェック
3. 電源ショートチェック	・・・	電源短絡チェック
4. FPGAコンフィギュレーション	・・・	テスト回路のコンフィギュレーション・テスト

9. FPGA暗号・制御回路作成上の注意点

論理合成～配置配線処理をISEで処理する場合、次のポイントに注意しながら回路作成することをすすめる。

（1）Verilog-HDLでRTLを作成する際、各種パラメータはパラメータ・ファイルを作成し、機能記述を読込む前にプロジェクト内に読込むことをすすめる。取込んだパラメータは、ライブラリ化して使用すると扱い易くなる。

（2）機能記述を全て読込んだ後、UCFファイル（PINアサイン情報、タイミング制約、etc）を読込む。

NET "信号名" LOC = "PINロケーション"; （ロケーション指定）
NET "信号名" LOC = "PINロケーション" | IOSTANDARD = LVDCI_33 ; （DCI利用時にDCIタイプ指定）

NET "クロック名" TNM_NET = "クロック名"; （クロック信号名の指定）
TIMESPEC "TS_クロック名" = PERIOD "クロック名" ** ns HIGH 〇〇%;
（**＝周期、〇〇＝Hレベルの時間）

（3）論理合成を行う前に次のオプションをOFFにして実行することをすすめる。
Generate RTL Schematic ＝ OFF
（ONにした場合、処理中の使用メモリが増大する為）

（4）XST（ISEにバンドルされている論理合成ツール）を使用する場合、次の点を考慮の上RTLの作成をすすめる。
・パッケージ1つ、エンティティ2つ、アーキテクチャ2つを1つのファイルに組み込もうとすると、大きなメモリーリソースを消費する。別々のファイルに分割して記述することをすすめる。（VHDL）
・大型のステートマシンを合成する場合、メモリが不足する。中間信号を使用し短い式に区切り構成する。
・コンポーネント/モジュールが何度もインスタンシエートされた場合、大量のメモリが使用される。一旦、コンポーネント/モジュール1つを合成した後、ブラックボックスとしてインスタンシエートすると、使用メモリをおさえることが出来る。
・if文によるネストが深いデザインは、大量のメモリを使用する。＆等を使いif文のネストを改善することをすすめる。

（5）内部メモリを組み込む場合、端子名を予めあわせて記述することをすすめる。また、組み込めるメモリ・タイプを確認の上回路検討する。

（6）未使用の端子は、予めモジュール等にアサインしないことを進める。

（7）モジュール内をスルーするネットが発生しない様な記述を進める。

（8）インスタンシエートされるモジュールに使用するパラメータは、共有パラメータか再度確認する。

（9）ゲーテッド・クロック回路は、ホールドタイミング違反の原因となるため使用しない事をすすめる。
（ISE環境下で上記違反に対する自動改善する機能はありません。）

（10）クロック同期回路をすすめる。

【変更履歴】

版数	作成日	変更内容
第0版	平成19年03月01日	・新規作成
第1版	平成19年03月30日	・誤記修正

【参考文献】

［1］Xilinx:『Virtex－Ⅱ Platform FPGA ハンドブック』

※上記参考文献に関する情報は、予告なく変更されることがあります。

【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11F　1102号室
TEL:03-5298-4722
FAX:03-5298-4522