サイドチャネル攻撃用標準評価基板
SASEBO-GII 仕様書

Side-channel Attack Standard Evaluation Board
SASEBO-GII Specification

[第 1.02 版]

2012 年 2 月 3 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. 概要 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
2. 暗号 FPGA および制御 FPGA の入出力信号 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4
3. ボード設定 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 11
4. 部品表・回路図・基板レイアウト図 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 16

1. 概要

SASEBO/SASEBO-G/SASEBO-B は，暗号回路単体でのサイドチャネル攻撃実験を目的として開発を行った．しかし，様々な要素技術を組み合わせた暗号システムとしての安全性評価実験や，様々な対策手法が施された大きな回路の実装にも供することができるよう，新たな FPGA ボード SASEBO-GII を開発した．実装評価対象の FPGA には最新の Xilinx Virtex-5 LX30/LX50 を採用しており，SASEBO/SASEBO-G で使用した Xilinx Virtext-II pro xc2vp7 の約 4~7 倍の回路規模を有している．また，回路規模の向上だけでなく，FPGA の再構成機能をユーザが様々な手段でコンフィグレーションできる機構を加えた．さらに，SASEBO/SASEBO-G の実験によって得られた知見をもとに，電力測定用のシャント抵抗の形状変更やクロック源の限定と分離などの改善を行い，1 系統の USB から給電/コンフィギュレーション/データ送受信を可能とすることで，実験環境の大幅な簡略化とユーザインタフェースの向上も図っている．このような機能強化を図る一方で，実装の効率化により基板サイズを従来の 3 分の 1 以下に縮小している．SASEBO-GII の基板の写真と配置図とブロック図を，それぞれ図 1 と図 2 に示す．また SASEBO-G の概要は以下の通りである．

- 基板サイズ 140mm×120mm×1.6mm（板厚），ガラスエポキシ材，6 層構造．
- Xilinx 社製 Virtex-5 シリーズの FPGA XC5VLX30（または LX50）-2FFG324 と XC3S400A-4FTG256（初期バージョンは XC3S50AN-4FT256）を実装し，主に前者を暗号回路用 FPGA，後者を制御回路用 FPGA として使用する．2 つの FPGA 間は，入力と出力共用の 38 ビット汎用バスで接続され，自由に信号をアサインして利用できる．
- 制御用 FPGA に 24MHz クロックを入力，外部クロックによる制御も可能．
- 電源は外部コネクタおよび USB コネクタより直流 5.0V を供給し，基板上のレギュレータが FPGA 用に 3.3V/1.8V/1.2V/1.0V を生成．また，暗号回路用 FPGA のコア電源は外部から直接供給も可能．
- 暗号用 FPGA のコア電源ラインおよびグランドライン上に抵抗を挿入し，電力波形測を観測することが可能．

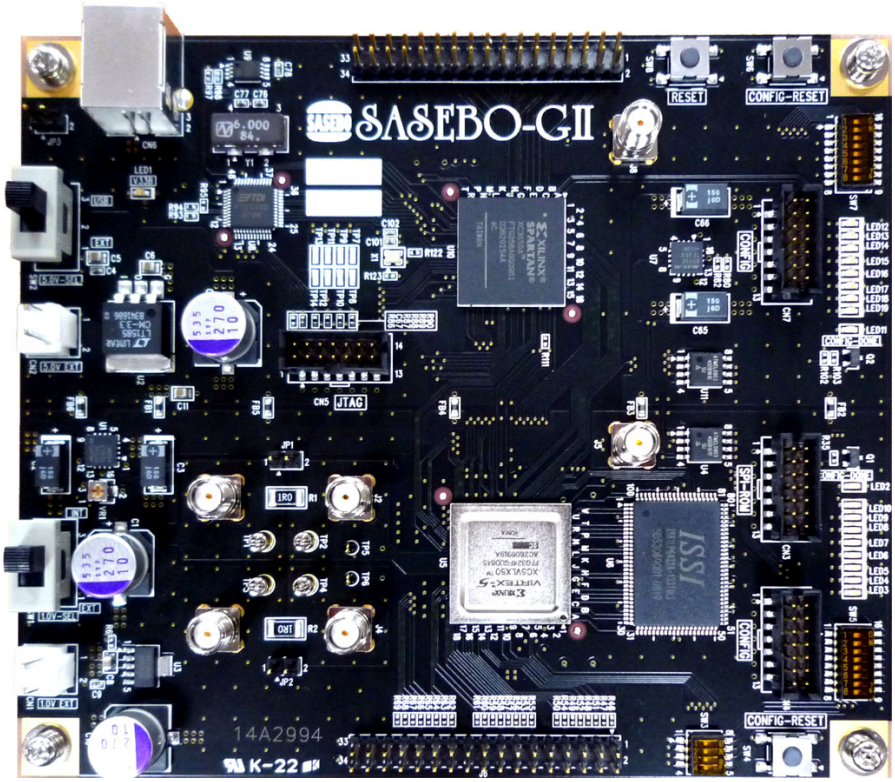


図 1　SASEBO-GII の概観

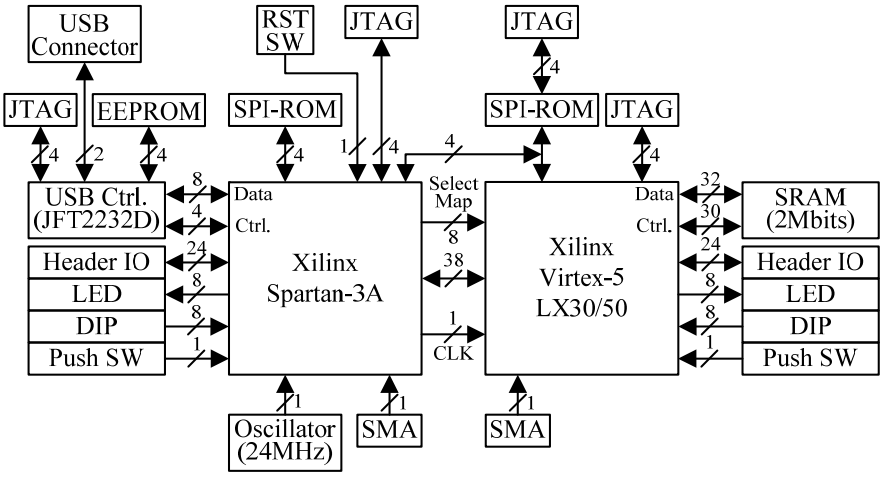


図 2　SASEBO-GII の主コンポーネントのブロック図

ボードの制御は外部に接続した PC から，USB のシリアル I/F を通して行う．メインの回路を実装する Virtex-5 のコンフィギュレーション方式に SPI-ROM，Slave-SelectMap を用意し，制御回路用 FPGA の Spartan-3A から制御する機構を設けることで，動的再構成だけでなく静的な全体・部分再構成も可能となっている．また，Spartan-3A の SPI-ROM からも Virtex-5 のコンフィギュレーションができるように，十分な ROM 容量を確保している．さらに，USB 制御 IC に JTAG 機能が追加された FTDI 社 FT2232D を採用し，特別なケーブルを使用しない JTAG 経由の FPGA コンフィギュレーションもサポートしている．

図 3 および図 4 は SASEBO-GII の給電方式策定のために試作した，SASEBO 用の USB 電源回路図と SASEBO-R に実装した写真である．電力解析実験には安定した電力の供給が特に重要であるが，ボード配布先の研究機関において電源装置によるトラブルがしばしば発生していた．また，市販の安定化電源装置は可搬性が低く，実験環境の簡素化も課題となっていた．そこで，USB から供給される 5V 電源を利用した給電回路を試作するとともに，SASEBO-GII への実装を行った．当初，SASEBO 駆動には 2.0A 以上の安定化電源が必要であったが，詳細な消費電力測定により，電源投入時と FPGA コンフィギュレーション時にのみ大きな突入電力が必要であることが判明した．そこで，その突入電力を供給できるコンデンサを搭載することで，電源装置の容量を大幅に低減することが可能となった．しかし，USB から供給される電源は比較的ノイズ成分が多く，かつ容量も 500mA と決して大きくないという問題があった．そこでいくつかの試作を経て，以下の 3 つの条件を満たす回路構成をとることで，低ノイズの USB 電源供給が行えるようになった．

- ターゲット FPGA に供給する電源は 3.3V および GND 共にインダクタで分離する．
- 出力段に 100uF 以上の容量をもつセラミックコンデンサ，もしくは 330uF 以上の容量を持つ電解コンデンサを実装する．
- 入力段に 0.1uF 以上の容量をもつセラミックコンデンサを実装する．ただしリニアレギュレータの性能に応じて容量を大きくする．

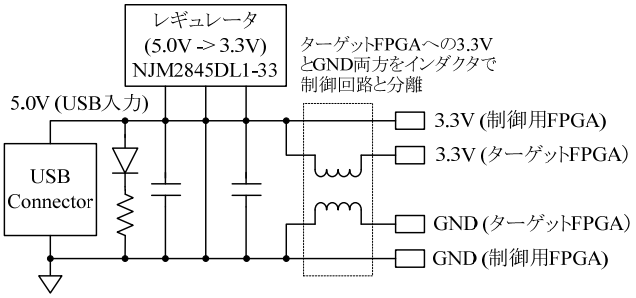


図 3　USB 電源回路図

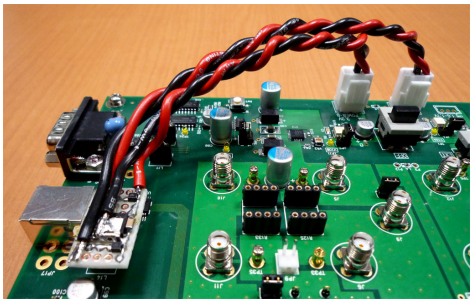
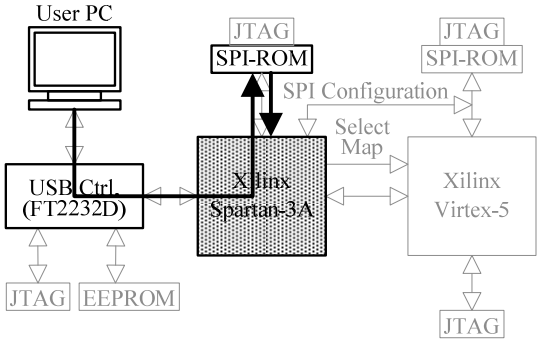


図 4　SASEBO-GII に実装した USB 電源回路

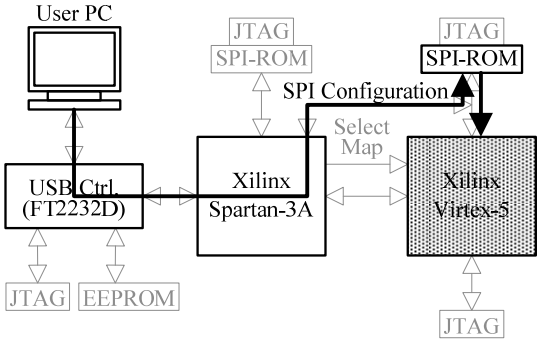
Virtex-5 には組み込みプロセッサの実装やデータ格納用に SRAM を接続しているほか，電源やクロック専用線が追加されたユーザ用 IO を備えており，DAC/ADC やイーサネットコントローラなどソフトウェア無線やネットワークフィルタリングの実験に必要なインタフェースの増設が可能である．Spartan-3A にも同様のユーザ IO を有し，標準のホストコンピュータから制御やデータの送受信は USB インタフェースを通じて行う．FPGA 間のバスや USB 制御用 IC は，従来のボードと互換性を維持しており，これまで開発した制御回路やソフトウェア，解析ツールは変更を加えることなく利用することができる．電力測定機能では SASEBO と同様の測定ポイントを設けた上で，シャント抵抗をラジアルリードからチップ抵抗に，ジャンパ機能をヘッダピンから SMA に変更することで周波数特性の向上も図っている．

SASEBO-GII に備えられている SelectMap，SPI-ROM，JTAG などのコンフィギュレーションの機構は Spartan-3A の回路構成を変更することで，FPGA の再構成機能を利用する各種アプリケーションに合わせた機能の使い分けが可能である．図 5(a)と 5(b)はそれぞれ，Spartan-3 および Virtex-5 の SPI-ROM をユーザ PC から USB 経由で書き換える静的再構成のパスを示している．また．図 5(c)は Virtex-5 を，電源を投入したままユーザ PC から直接，8-bit データ幅の SelectMap により高速に再構成するパスである．図 5(d)の方法では 32-bit バス幅を経由してし，外部 IO を停止することなく Virtex-5 を動的に部分再構成することができる．

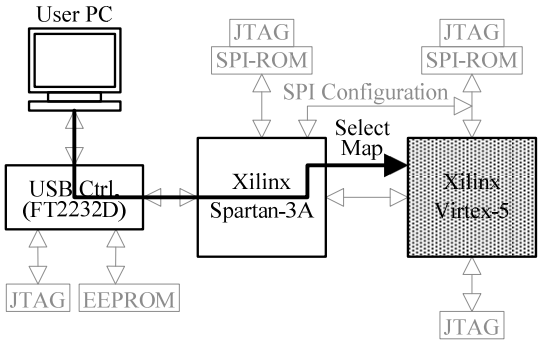
(a) Spartan-3 の ROM からの静的再構成



(b) Virtex-5 の ROM からの静的再構成



(c) Virtex-5 の静的再構成



(d) Virtex-5 の動的部分再構成

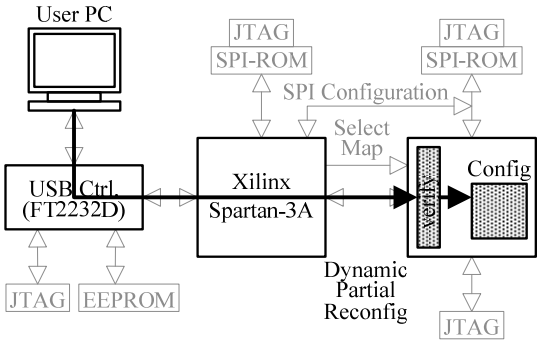


図 5 FPGA のコンフィグレーションパス

2. 暗号 FPGA および制御 FPGA の入出力信号

- 暗号 FPGA(コンポーネント U5)用

表 1　FPGA 設定信号

信号名	端子	入出力	用途･接続先
VIR5_CONFD0	P12	I	Config
VIR5_CONFD1	P13	I	Config
VIR5_CONFD2	M11	I	Config
VIR5_CONFD3	N11	I	Config
VIR5_CONFD4	T13	I	Config
VIR5_CONFD5	T14	I	Config
VIR5_CONFD6	M10	I	Config
VIR5_CONFD7	N10	I	Config
VIR5_BUSY	T6	O	Config
VIR5_INITB	M8	I	Config
VIR5_PROGB	U18	I	Config
VIR5_DONE	P8	O	Config
VIR5_CSB	R16	O	Config
VIR5_RDWRB	P15	IO	Config
VIRT5-CCLK	N8	O	Config
VIRT5-D_IN	R7	O	Config
VIRT5-MOSI	P9	O	Config
VIRT5-FCS_B	P10	O	Config
M0	N12	I	SW3-8
M1	L11	I	SW3-7
M2	N13	I	SW3-6
TCK	M9	--	JTAG
TDI	U5	--	JTAG
TDO	U6	--	JTAG
TMS	V5	--	JTAG
HSWAP_EN	T17	I	PU-R
VBATT	T18	I	PU-R
DXP	L10	NC	NC
DXN	L9	NC	NC
VREFP	K10	--	PU-R
VREFN	J9	--	PU-R
RSVD	P14	NC	NC
RSVD	R14	NC	NC

表 2　制御 FPGA I/F

信号名	端子	入出力	接続先(U10)
VIR5-UD0	N17	IO	F13
VIR5-UD1	P17	IO	E14
VIR5-UD2	M16	IO	D15
VIR5-UD3	M18	IO	D16
VIR5-UD4	V16	IO	D14
VIR5-UD5	P18	IO	E13
VIR5-UD6	N18	IO	C15
VIR5-UD7	U16	IO	C13
VIR5-UD8	V18	IO	D13
VIR5-UD9	T16	IO	B14
VIR5-UD10	V17	IO	B15
VIR5-UD11	U15	IO	D11
VIR5-UD12	V15	IO	C12

VIR5-UD13	M15	IO	A13
VIR5-UD14	N16	IO	A14
VIR5-UD15	R17	IO	A11
VIR5-UD16	U14	IO	C11
VIR5-UD17	R15	IO	A10
VIR5-UD18	N15	IO	B10
VIR5-UD19	V13	IO	D9
VIR5-UD20	M14	IO	A9
VIR5-UD21	U13	IO	C9
VIR5-UD22	V12	IO	D8
VIR5-UD23	T12	IO	C8
VIR5-UD24	V11	IO	B8
VIR5-UD25	M13	IO	A8
VIR5-UD26	V10	IO	B6
VIR5-UD27	U10	IO	A6
VIR5-UD28	T9	IO	C6
VIR5-UD29	R12	IO	D7
VIR5-UD30	T8	IO	C5
VIR5-UD31	U9	IO	A5
VIR5-UD32	U8	IO	B4
VIR5-UD33	V8	IO	A4
VIR5-UD34	V6	IO	B3
VIR5-UD35	V7	IO	A3
VIR5-UD36	R9	IO	D5
VIR5-UD37	T7	IO	C4
SP3-VIR5_24MCLK	U11	I	C16

表 3　モニタ信号

信号名	端子	入出力	用途･接続先
LED0	F11	OUT	LED3
LED1	G11	OUT	LED4
LED2	G10	OUT	LED5
LED3	F9	OUT	LED6
LED4	E12	OUT	LED7
LED5	D12	OUT	LED8
LED6	F8	OUT	LED9
LED7	G9	OUT	LED10
DIPSW1	A8	IN	SW5-1
DIPSW2	A9	IN	SW5-2
DIPSW3	B9	IN	SW5-3
DIPSW4	B10	IN	SW5-4
DIPSW5	E9	IN	SW5-5
DIPSW6	D9	IN	SW5-6
DIPSW7	E10	IN	SW5-7
DIPSW8	E11	IN	SW5-8
RESET-CONFIG	U18	IN	SW4

表 4　汎用モニタピン

信号名	端子	入出力	用途･接続先
EXT-D0	A13	IO	J6-1
EXT-D1	B13	IO	J6-2
EXT-D2	A14	IO	J6-3
EXT-D3	B14	IO	J6-4
EXT-D4	B15	IO	J6-5
EXT-D5	A16	IO	J6-6

EXT-D6	B16	IO	J6-7
EXT-D7	A17	IO	J6-8
EXT-D8	A18	IO	J6-11
EXT-D9	B18	IO	J6-12
EXT-D10	C17	IO	J6-13
EXT-D11	C18	IO	J6-14
EXT-D12	D17	IO	J6-15
EXT-D13	D18	IO	J6-16
EXT-D14	E17	IO	J6-17
EXT-D15	E16	IO	J6-18
EXT-D16	F18	IO	J6-21
EXT-D17	F17	IO	J6-22
EXT-D18	C15	IO	J6-23
EXT-D19	C16	IO	J6-24
EXT-D20	D15	IO	J6-25
EXT-D21	D14	IO	J6-26
EXT-D22	E15	IO	J6-27
EXT-D23	E14	IO	J6-28
EXTPORT-CLKP	A6	IO	J6-31
EXTPORT-CLKN	A7	IO	J6-32

表 5　Memory I/F

信号名	端子	入出力	接続先(U6)
SRAM-A0	F1	OUT	37
SRAM-A1	F3	OUT	36
SRAM-A2	G1	OUT	35
SRAM-A3	G4	OUT	34
SRAM-A4	H1	OUT	33
SRAM-A5	H3	OUT	32
SRAM-A6	V1	OUT	100
SRAM-A7	T4	OUT	99
SRAM-A8	K1	OUT	82
SRAM-A9	J2	OUT	81
SRAM-A10	B5	OUT	44
SRAM-A11	B4	OUT	45
SRAM-A12	C3	OUT	46
SRAM-A13	D3	OUT	47
SRAM-A14	E4	OUT	48
SRAM-A15	E1	OUT	49
SRAM-ADSC_N	L2	IO	85
SRAM-ADSP_N	L1	IO	84
SRAM-ADV_N	K2	IO	83
SRAM-BW1_N	M1	IO	93
SRAM-BW2_N	M3	IO	94
SRAM-BW3_N	N1	IO	95
SRAM-BW4_N	N3	IO	96
SRAM-BWE_N	V3	IO	87
SRAM-CE_N	T1	IO	98
SRAM-CE2	P3	IO	97
SRAM-CLK	V2	IO	89
SRAM-DQA0	A2	IO	52
SRAM-DQA1	A1	IO	53
SRAM-DQA2	B1	IO	56
SRAM-DQA3	C2	IO	57
SRAM-DQA4	C1	IO	58

SRAM-DQA5	D4	IO	59
SRAM-DQA6	E5	IO	62
SRAM-DQA7	F4	IO	63
SRAM-DQB0	J4	IO	68
SRAM-DQB1	J3	IO	69
SRAM-DQB2	L3	IO	72
SRAM-DQB3	M5	IO	73
SRAM-DQB4	N5	IO	74
SRAM-DQB5	P4	IO	75
SRAM-DQB6	R4	IO	78
SRAM-DQB7	T3	IO	79
SRAM-DQC0	U1	IO	2
SRAM-DQC1	T2	IO	3
SRAM-DQC2	R2	IO	6
SRAM-DQC3	P2	IO	7
SRAM-DQC4	N2	IO	8
SRAM-DQC5	M4	IO	9
SRAM-DQC6	L4	IO	12
SRAM-DQC7	K4	IO	13
SRAM-DQD0	H2	IO	18
SRAM-DQD1	G3	IO	19
SRAM-DQD2	F2	IO	22
SRAM-DQD3	E2	IO	23
SRAM-DQD4	D2	IO	24
SRAM-DQD5	C5	IO	25
SRAM-DQD6	B3	IO	28
SRAM-DQD7	A3	IO	29
SRAM-GW_N	U3	IO	88
SRAM-MODE	A4	IO	31
SRAM-OE_N	U4	IO	86
SRAM-ZZ	G5	IO	64

- 制御 FPGA(U10)用信号

表 6 FPGA 設定信号

信号名	端子	入出力	用途･接続先
D0/MISO	T14	IO	SPI-ROM
CCLK	R14	IO	SPI-ROM
MOSI/CSIB	P10	IO	SPI-ROM
CSOB	T2	IO	SPI-ROM
GCLK2	R9	IO	CLOCK
VIR5_CONFD0	K15	O	Config
VIR5_CONFD1	K14	O	Config
VIR5_CONFD2	K16	O	Config
VIR5_CONFD3	J16	O	Config
VIR5_CONFD4	J14	O	Config
VIR5_CONFD5	H14	O	Config
VIR5_CONFD6	H15	O	Config
VIR5_CONFD7	H16	O	Config
VIR5_BUSY	K12	I	Config
VIR5_INITB	N16	O	Config
VIR5_PROGB	T13	O	Config
VIR5_DONE	P16	I	Config
VIR5_CSB	J13	I	Config
VIR5_RDWRB	J12	IO	Config

VIRT5_CCLK	N13	I	Config
VIRT5-D_IN	N14	I	Config
VIRT5-MOSI	P15	I	Config
VIRT5-FCS_B	R15	I	Config
PROG_B	A2	--	Config
DONE	T15	--	Config
M0	P4	IN	PU-R
M1	N4	IN	PD-R
M2	R2	IN	PD-R
TCK	A15	--	JTAG
TDI	B1	--	JTAG
TDO	B16	--	JTAG
TMS	B2	--	JTAG
VS0	P5	IN	PU-R
VS1	N6	IN	PD-R
VS2	T3	IN	PU-R

表 7 暗号 FPGA I/F

信号名	端子	入出力	接続先(U5)
VIR5-UD0	F13	IO	N17
VIR5-UD1	E14	IO	P17
VIR5-UD2	D15	IO	M16
VIR5-UD3	D16	IO	M18
VIR5-UD4	D14	IO	V16
VIR5-UD5	E13	IO	P18
VIR5-UD6	C15	IO	N18
VIR5-UD7	C13	IO	U16
VIR5-UD8	D13	IO	V18
VIR5-UD9	B14	IO	T16
VIR5-UD10	B15	IO	V17
VIR5-UD11	D11	IO	U15
VIR5-UD12	C12	IO	V15
VIR5-UD13	A13	IO	M15
VIR5-UD14	A14	IO	N16
VIR5-UD15	A11	IO	R17
VIR5-UD16	C11	IO	U14
VIR5-UD17	A10	IO	R15
VIR5-UD18	B10	IO	N15
VIR5-UD19	D9	IO	V13
VIR5-UD20	A9	IO	M14
VIR5-UD21	C9	IO	U13
VIR5-UD22	D8	IO	V12
VIR5-UD23	C8	IO	T12
VIR5-UD24	B8	IO	V11
VIR5-UD25	A8	IO	M13
VIR5-UD26	B6	IO	V10
VIR5-UD27	A6	IO	U10
VIR5-UD28	C6	IO	T9
VIR5-UD29	D7	IO	R12
VIR5-UD30	C5	IO	T8
VIR5-UD31	A5	IO	U9
VIR5-UD32	B4	IO	U8
VIR5-UD33	A4	IO	V8
VIR5-UD34	B3	IO	V6
VIR5-UD35	A3	IO	V7

VIR5-UD36	D5	IO	R9
VIR5-UD37	C4	IO	T7
SP3-VIR5_24MCLK	C16	O	U11

表 8　モニタ信号

信号名	端子	入出力	接続先
LED0	U10.T10	OUT	LED12
LED1	U10.R11	OUT	LED13
LED2	U10.T11	OUT	LED14
LED3	U10.N11	OUT	LED15
LED4	U10.P11	OUT	LED16
LED5	U10.P12	OUT	LED17
LED6	U10.T12	OUT	LED18
LED7	U10.R13	OUT	LED19
DIPSW1	U10.F4	IN	SW7.16
DIPSW2	U10.E4	IN	SW7.15
DIPSW3	U10.J7	IN	SW7.14
DIPSW4	U10.H7	IN	SW7.13
DIPSW5	U10.K6	IN	SW7.12
DIPSW6	U10.K5	IN	SW7.11
DIPSW7	U10.L6	IN	SW7.10
DIPSW8	U10.L5	IN	SW7.9
PUSH	N10.L7	IN	SW8

表 9　汎用モニタピン

信号名	端子	入出力	用途･接続先
FPGAB-D0	U10.C1	IO	J9-1
FPGAB-D1	U10.C2	IO	J9-2
FPGAB-D2	U10.D3	IO	J9-3
FPGAB-D3	U10.D4	IO	J9-4
FPGAB-D4	U10.E1	IO	J9-5
FPGAB-D5	U10.D1	IO	J9-6
FPGAB-D6	U10.G1	IO	J9-7
FPGAB-D7	U10.F1	IO	J9-8
GND		IO	J9-9
GND		IO	J9-10
FPGAB-D8	U10.H1	IO	J9-11
FPGAB-D9	U10.G2	IO	J9-12
FPGAB-D10	U10.J3	IO	J9-13
FPGAB-D11	U10.H3	IO	J9-14
FPGAB-D12	U10.J1	IO	J9-15
FPGAB-D13	U10.J2	IO	J9-16
FPGAB-D14	U10.K1	IO	J9-17
FPGAB-D15	U10.K3	IO	J9-18
GND		IO	J9-19
GND		IO	J9-20
FPGAB-D16	U10.L2	IO	J9-21
FPGAB-D17	U10.L1	IO	J9-22
FPGAB-D18	U10.J6	IO	J9-23
FPGAB-D19	U10.J4	IO	J9-24
FPGAB-D20	U10.L3	IO	J9-25
FPGAB-D21	U10.K4	IO	J9-26
FPGAB-D22	U10.L4	IO	J9-27
FPGAB-D23	U10.M3	IO	J9-28
GND		IO	J9-29
GND		IO	J9-30
FPGAB-XCLKN	U10.P9	IO	J9-31

FPGAB-XCLKP	U10.N9	IO	J9-32
V33B		IO	J9-33
V33B		IO	J9-34

表 10 USB I/F

信号名	端子	入出力	接続先
USBBDBUS0	U10.R3	IO	U8.40
USBBDBUS1	U10.R5	IO	U8.39
USBBDBUS2	U10.T4	IO	U8.38
USBBDBUS3	U10.T6	IO	U8.37
USBBDBUS4	U10.T5	IO	U8.36
USBBDBUS5	U10.N8	IO	U8.35
USBBDBUS6	U10.P7	IO	U8.33
USBBDBUS7	U10.T8	IO	U8.32
USBBCBUS0	U10.P2	IO	U8.30
USBBCBUS1	U10.R1	IO	U8.29
USBBCBUS2	U10.M4	IO	U8.28
USBBCBUS3	U10.N3	IO	U8.27
V33B	--	--	U8.26

3. ボード設定

● 電源回路

図 6 に電源回路ブロックの構成を，表 10 に入力電源の設定を示す．また図 7 は電源投入時の各電源ラインの立ち上がり方を示している．USB から全ての電源を供給する場合は，電源切り替えスイッチ SW1 および SW2 をそれぞれ INT に設定する．USB から電源供給を行わない場合は，SW2 を EXT とし，CN2 に直流 5.0V を入力する．また暗号 FPGA のコア電源を外部から直接供給する場合は，SW1 を EXT とし，CN1 に直流 1.0V を入力する．SW1 および SW2 の切り替えは電源投入前に行っておくこと．USB(CN6)または外部電源(CN2)から 5V が供給されるトと，LED1 が点灯する．

表 11　入力電源の設定

選択 SW	SW2		SW1	
	INT	EXT	INT	EXT
電源	USB (CN6) : 5V	CN2 : 5V	Regulator U1 : 1V	CN1 : 1V
説明	制御/暗号 FPGA 用 USB 電源	制御/暗号 FPGA 用 外部電源	暗号 FPGA コア用 内部シリーズ電源	暗号 FPGA コア用 外部電源

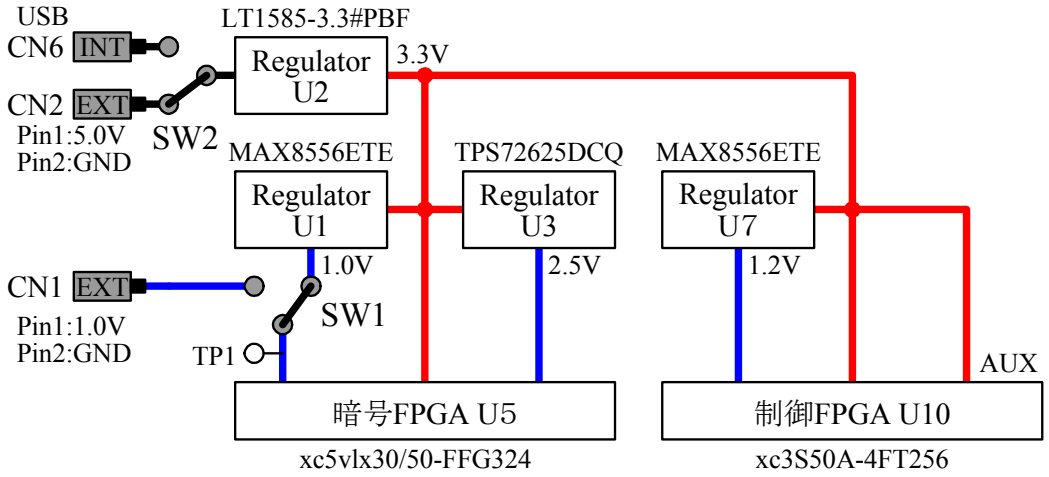


図 6　電源回路ブロックの構成

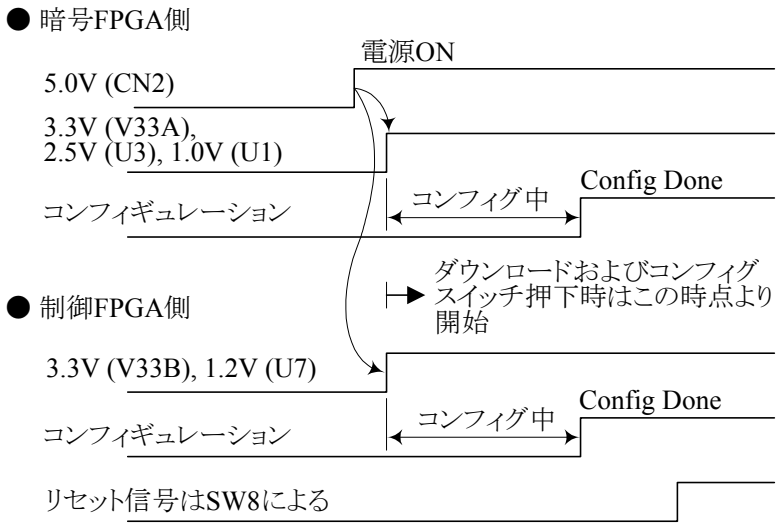


図 7　電源シーケンス

- ジャンパー設定

表 12 ジャンパー設定

用途	ピン番号	設定	説明
USB-CASE の選択	JP3	Short	USB コネクタのケースが GND に接続。
		Open	USB コネクタのケースがいずれにも接続されない。
電力波形測定設定	JP1	Short	暗号 FPGA のコア電源側シャント抵抗 R1 をバイパス
		Open	暗号 FPGA のコア電源側シャント抵抗 R1 を使用
	JP2	Short	制御 FPGA のコア電源側シャント抵抗 R2 をバイパス
		Open	制御 FPGA のコア電源側シャント抵抗 R2 を使用

- コンフィギュレーション

図 8 に JTAG チェーンの接続関係を示す. 暗号 FPGA(U5)と制御 FPGA(U10)それぞれ独立に FPGA 書き込み用コネクタ CN3 と CN7, SPI-ROM U4 と U11 を有している. 表 13 に JTAG コネクタのピンアサインを, 表 14 にコンフィギュレーションモードの指定を行う DIP スイッチ(暗号 FPGA 用は SW3, 制御 FPGA 用は SPI モード固定)の設定を示す. それぞれの FPGA において, PC または SPI-ROM からのコンフィギュレーションが成功すると, 発光ダイオード LED2 および LED11 が点灯する. また, プッシュスイッチ SW4 または SW8 の押下によって, それぞれの SPI-ROM からの再コンフィギュレーションが開始される.

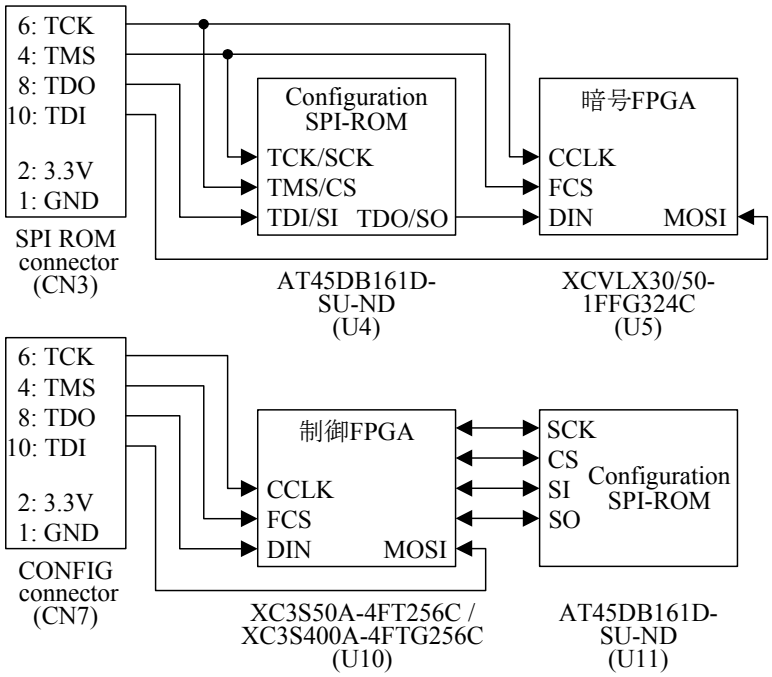


図 8 JTAG チェーン

表 13 JTAG/CONFIG コネクタのピンアサイン

Pin1	GND	Pin2	3.3V
Pin3	GND	Pin4	TMS
Pin5	GND	Pin6	TCK
Pin7	GND	Pin8	TDO
Pin9	GND	Pin10	TDI
Pin11	GND	Pin12	NC
Pin13	GND	Pin14	NC

表 14 モード切替 DIP スイッチ SW3 の Mode 設定

Dip1	M0	ON
Dip2	M1	ON
Dip3	M2	ON
Dip4	NC	OFF

- クロック系統

図9にSASEBO-GIIのクロック系統図を示す. 制御FPGAは， 24MHzのクロック源X1を有し、内部を通して暗号FPGAへ接続いる. また，各クロックは，SMAコネクタJ3，J4を通して，それぞれ独立に外部から供給することも可能である.

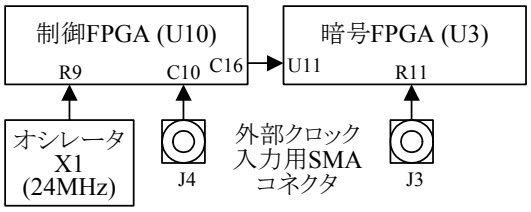


図 9　クロック系統図

- インタフェース部

SASEBO-G は外部 PC との通信用に， USB シリアルインタフェースを有している. 表 15 に, USB のコネクタから FPGA までの信号線の接続関係を示す. USB インタフェース IC には FTDI(Future Technology Device International Ltd.)社の FT2232D を使用しており，デバイスドライバは http://www.ftdichip.com/Products/FT2232.htm からダウンロードすることができる.

表 15 USB インタフェースの信号線

信号	CN6 (XM7B-0442)	U8 (FT2232D)	U10 (XC3S50A-FT256 / XC3S400A-FTG256)
USBDM	2 pin	8 pin	-
USBDP	3 pin	7 pin	-
USBBDBUS0	-	40 pin	U10.R3
USBBDBUS1	-	39 pin	U10.R5
USBBDBUS2	-	38 pin	U10.T4
USBBDBUS3	-	37 pin	U10.T6
USBBDBUS4	-	36 pin	U10.T5
USBBDBUS5	-	35 pin	U10.N8
USBBDBUS6	-	33 pin	U10.P7
USBBDBUS7	-	32 pin	U10.T8
USBBCBUS0	-	30 pin	U10.P2
USBBCBUS1	-	29 pin	U10.R1
USBBCBUS2	-	28 pin	U10.M4
USBBCBUS3	-	27 pin	U10.N3
FT2232-TCK	-	24 pin	-
FT2232-TDI	-	23 pin	-
FT2232-TDO	-	22 pin	-
FT2232-TMS	-	21 pin	-
FT2232-GPIOH0	-	15 pin	-
FT2232-GPIOH1	-	13 pin	-
FT2232-GPIOH2	-	12 pin	-
FT2232-GPIOH3	-	11 pin	-
FT2232-GPIOL0	-	20 pin	-
FT2232-GPIOL1	-	19 pin	-
FT2232-GPIOL2	-	17 pin	-
FT2232-GPIOL3	-	16 pin	-

4. 部品表・回路図・基板レイアウト図

表 16 部品表

品名	型名	メーカ	数量	部品番号
積層セラC (チップ)	GRM155B11A104K	ムラタ	54	C4,C9,C53,C54,C55,C56, C57,C58,C59,C60,C61,C62, C63,C64,C67,C69,C70,C71, C72,C73,C75,C78,C79,C80, C81,C82,C83,C84,C85,C86, C87,C88,C89,C90,C91,C93, C94,C95,C96,C97,C98,C99, C100,C101,C103,C104,C105, C106,C107,C108,C109,C110, C111,C112
積層セラC (チップ)	GRM219B31A106K	ムラタ	9	C5,C6,C8,C11,C39,C40,C41, C68,C92
積層セラ C (チップ)	GRM155B11A104K	ムラタ	38	C12,C13,C14,C15,C16,C17, C18,C19,C20,C21,C22,C23, C24,C25,C26,C27,C28,C29, C30,C31,C32,C33,C34,C35, C36,C37,C38,C42,C43,C44, C45,C46,C47,C48,C49,C50, C51,C52
積層セラ C (チップ)	C3216JB0J336M	TDK	1	C74
積層セラ C (チップ)	GRM1552C1H270JZ01D	ムラタ	2	C76,C77
積層セラ C (チップ)	GRM155B31A105KE15D	ムラタ	1	C102
OS コンデンサ	10SVP270M	SANYO	3	C1,C7,C10
電解コンデンサ	&6TB150M	SANYO	4	C2,C3,C65,C66
発光ダイオード (チップ)	SML-310MTT86	ROHM	19	LED1,LED2,LED3,LED4,LED5, LED6,LED7,LED8,LED9, LED10,LED11,LED12,LED13, LED14,LED15,LED16,LED17, LED18,LED19
フェライトビーズ	MPZ1608S600A	TDK	6	FB1,FB2,FB3,FB4,FB5,FB6
レギュレータ IC	LT1585CM-3.3#PBF	LTC	1	U2
レギュレータ IC	TPS72625DCQ	TI	1	U3
レギュレータ IC	MAX8556ETE+	マキシム	2	U1,U7
FPGA	XC5VLX30-1FFG324	ザイリンクス	1	U5
FPGA	XC3S400A-4FT256	ザイリンクス	1	U10
ROM	AT45DB161D-SU-ND	ATMEL	2	U4,U11
SRAM	IS61LP6432A-133TQ-ND	ISSI	1	U6
USB IC	FT2232D	FTDI	1	U8
SROM	93LC46B_IST	MICROCHIP	1	U9
水晶発振器	ECS	ECS	1	X1
水晶発振子	NX1255GB	NDK	1	Y1
コネクタ	B2P	日本圧着端子	2	CN1,CN2
コネクタ	87832	MOLEX	4	CN3,CN4,CN5,CN7

コネクタ	XM7B-0442	OMRON	1	CN6
ヘッダー	XG8S-0231	OMRON	3	JP1,JP2,JP3
ジャンパソケット	HIF3GA-2.54SP	HIROSE	1	JS1
SMA ソケット	T124 426 000N		6	J1,J2,J3,J4,J5,J8
ヘッダー	A1-34PA-2.54DSA	HIROSE	2	J6,J9
トランジスタ	2SC2712BL	TOSHIBA	2	Q1,Q2
チップ抵抗	RK73BW2HTTD1R0J	KOA	2	R1,R2
チップ抵抗	RK73B1ETTP472J	KOA	59	R3,R10,R11,R12,R13,R14, R16,R17,R18,R19,R20,R27, R28,R29,R30,R31,R32,R34, R35,R36,R37,R38,R39,R40, R41,R42,R43,R44,R80,R81, R83,R84,R85,R92,R99,R100, R103,R104,R105,R106,R108, R109,R113,R114,R117,R118, R121,R124,R125,R126,R127, R128,R129,R130,R131,R132, R133,R135,R136
チップ抵抗	RK73B1ETTP102J	KOA	2	R4,R6
チップ抵抗	RK73B1JTTD151J	KOA	19	R5,R33,R72,R73,R74,R75, R76,R77,R78,R79,R101, R137,R138,R139,R140,R141, R142,R143,R144
チップ抵抗	RK73H1ETTP1000F	KOA	2	R7,R8
チップ抵抗	RK73B1ETTP220J	KOA	35	R9,R25,R46,R47,R48,R49, R50,R51,R52,R53,R54,R55, R56,R57,R58,R59,R60,R61, R62,R63,R64,R65,R66,R67, R68,R69,R70,R71,R86,R87, R88,R89,R90,R111,R122
チップ抵抗	RK73B1ETTP331J	KOA	2	R15,R102
ジャンパー抵抗	MCR01MZPJ000	ROHM	16	R21,R22,R23,R24,R26,R45, R96,R107,R110,R112,R115, R116,R119,R120,R123,R134
チップ抵抗	RK73B1ETTP332J	ROHM	1	R82
チップ抵抗	RK73B1ETTP471J	ROHM	1	R91
チップ抵抗	RK73B1ETTP270J	ROHM	2	R93,R94
チップ抵抗	RK73B1ETTP152J	ROHM	1	R95
チップ抵抗	RK73B1ETTD103J	ROHM	1	R97
チップ抵抗	RK73H1ETTP2201F	ROHM	1	R98
トリマ	ST-32ETA 2kΩ	コパル	1	VR1
スイッチ	CS-12AAP1	NIKKAI	2	SW1,SW2
DIP スイッチ	CHS-04B	COPAL	1	SW3
タクトスイッチ	B3FS-1000	OMRON	3	SW4,SW6,SW8
DIP スイッチ	CHS-08B	COPAL	2	SW5,SW7
端子	MM-2-1	MAC8	4	TP1,TP2,TP3,TP4
端子	LC-33-G-KURO	MAC8	2	TP5,TP6

図 10 暗号 FPGA 周辺回路 (電源入力回路/コア電源回路)

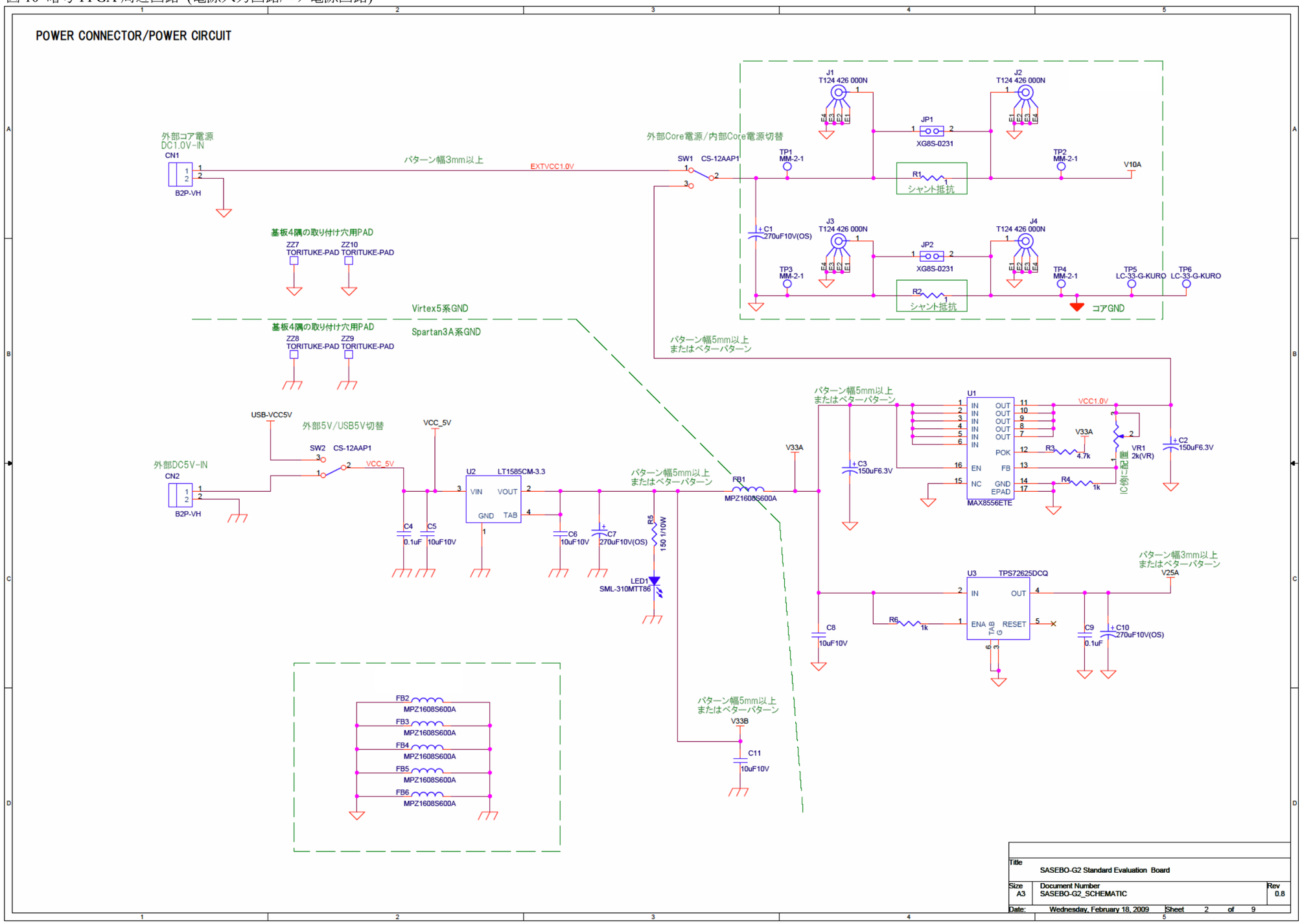


図 11 暗号 FPGA 周辺回路 (FPGA 接続部/電源回路/コンフィギュレーション回路)

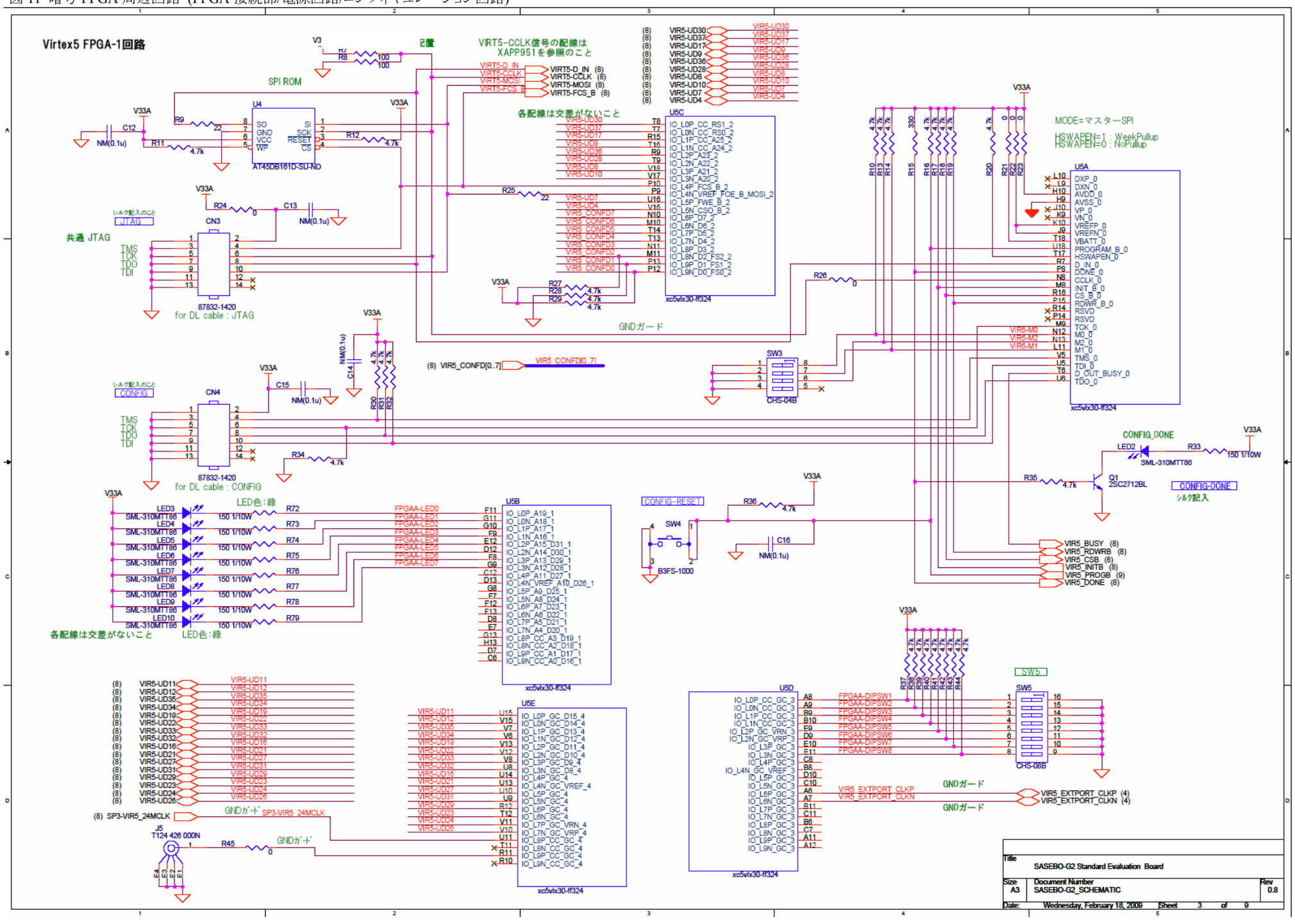


図 12 暗号 FPGA 周辺回路 (FPGA 接続部)

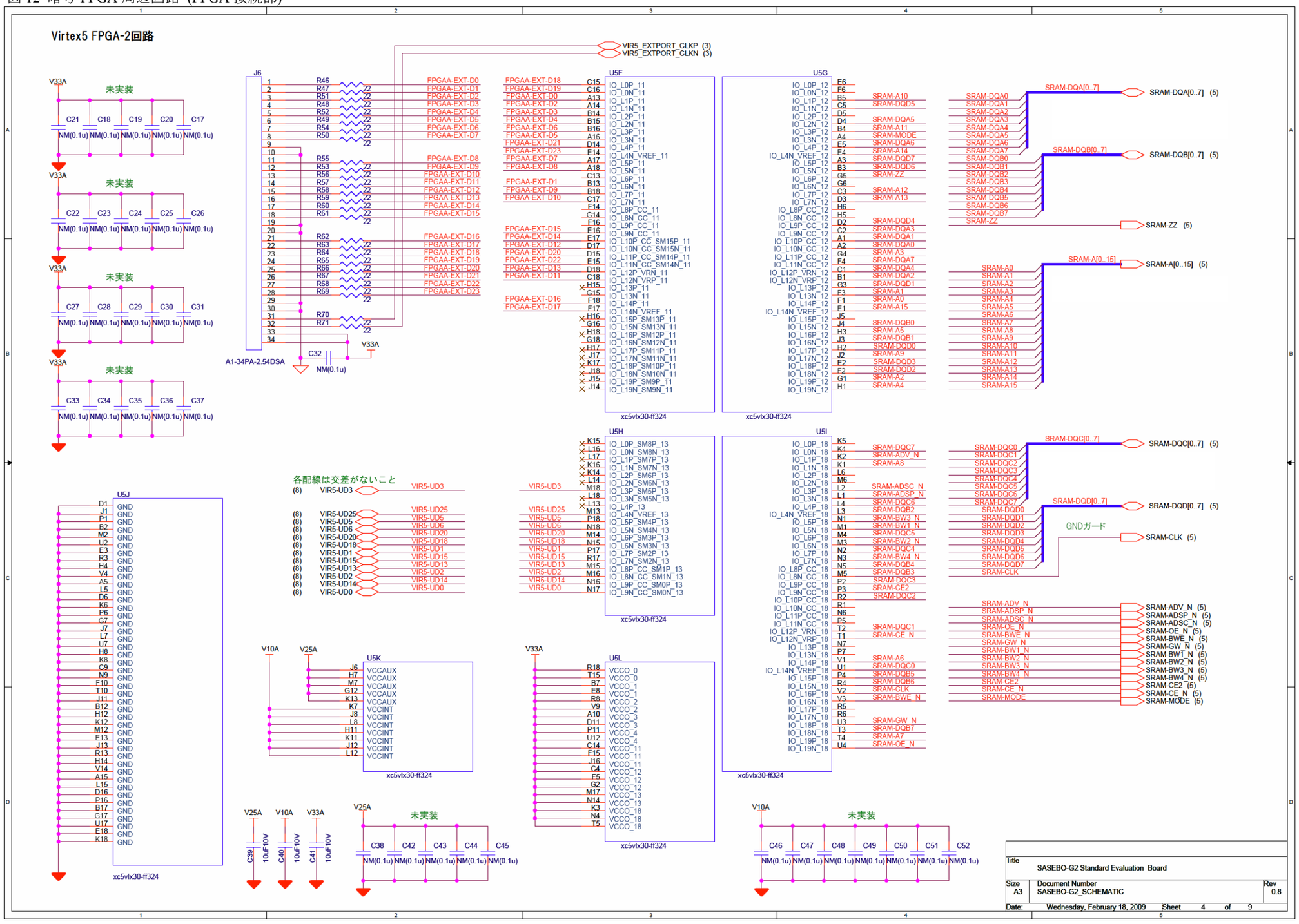


図 13 暗号 FPGA 周辺回路 (SRAM 回路)

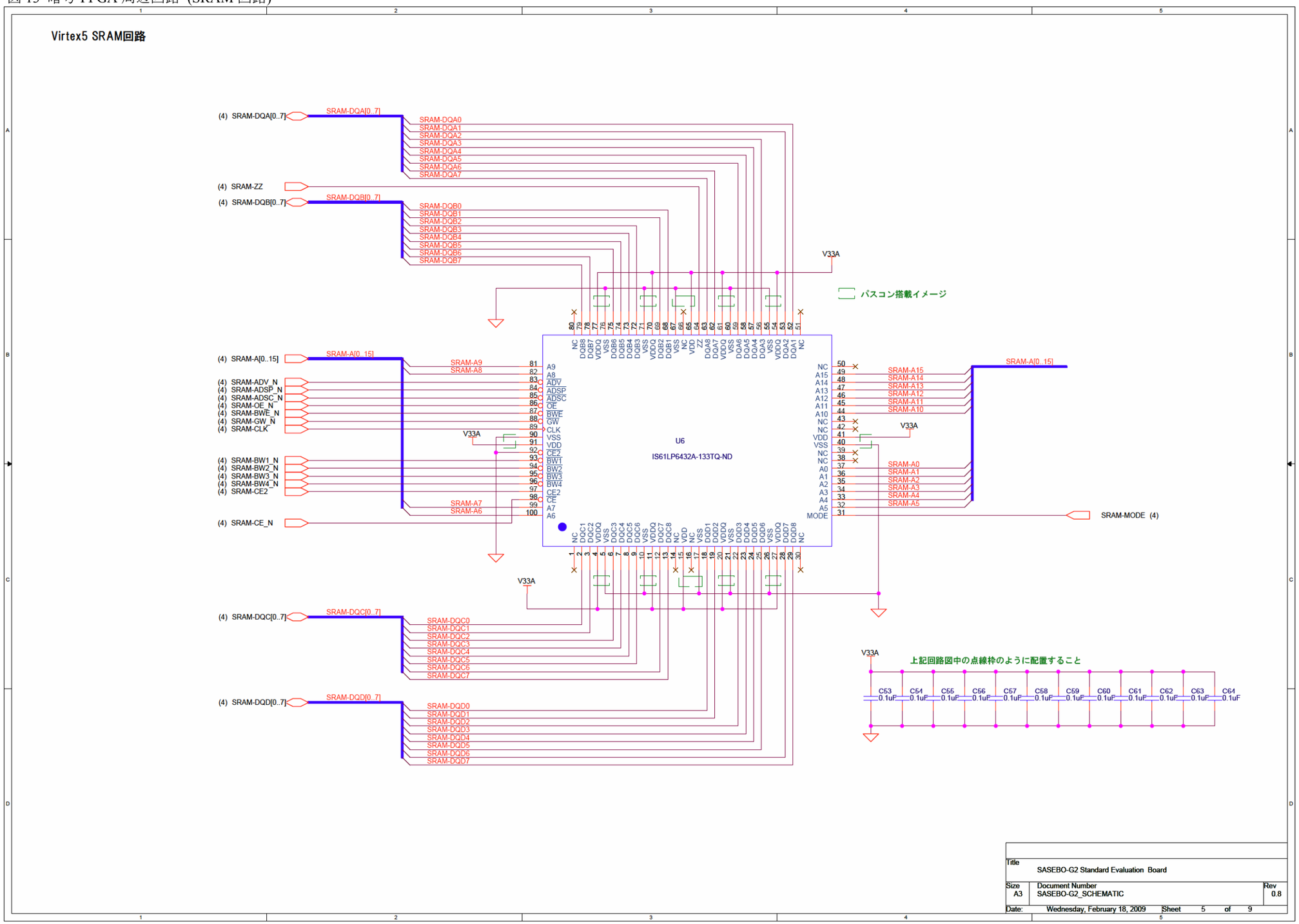


図 14 制御 FPGA 周辺回路 (電源回路/USB 回路)

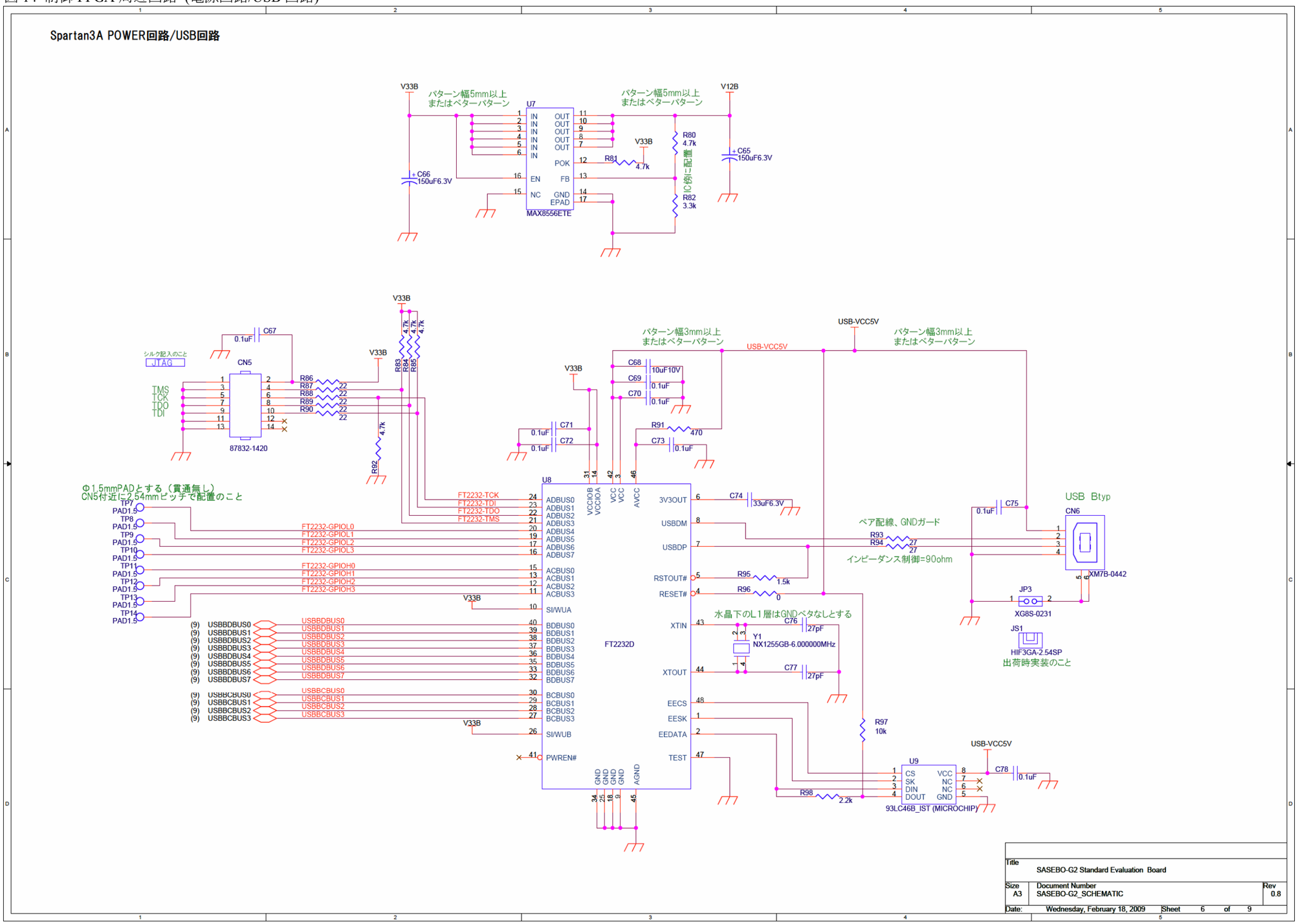


図 15 制御 FPGA 周辺回路 (電源回路/コンフィギュレーション回路)

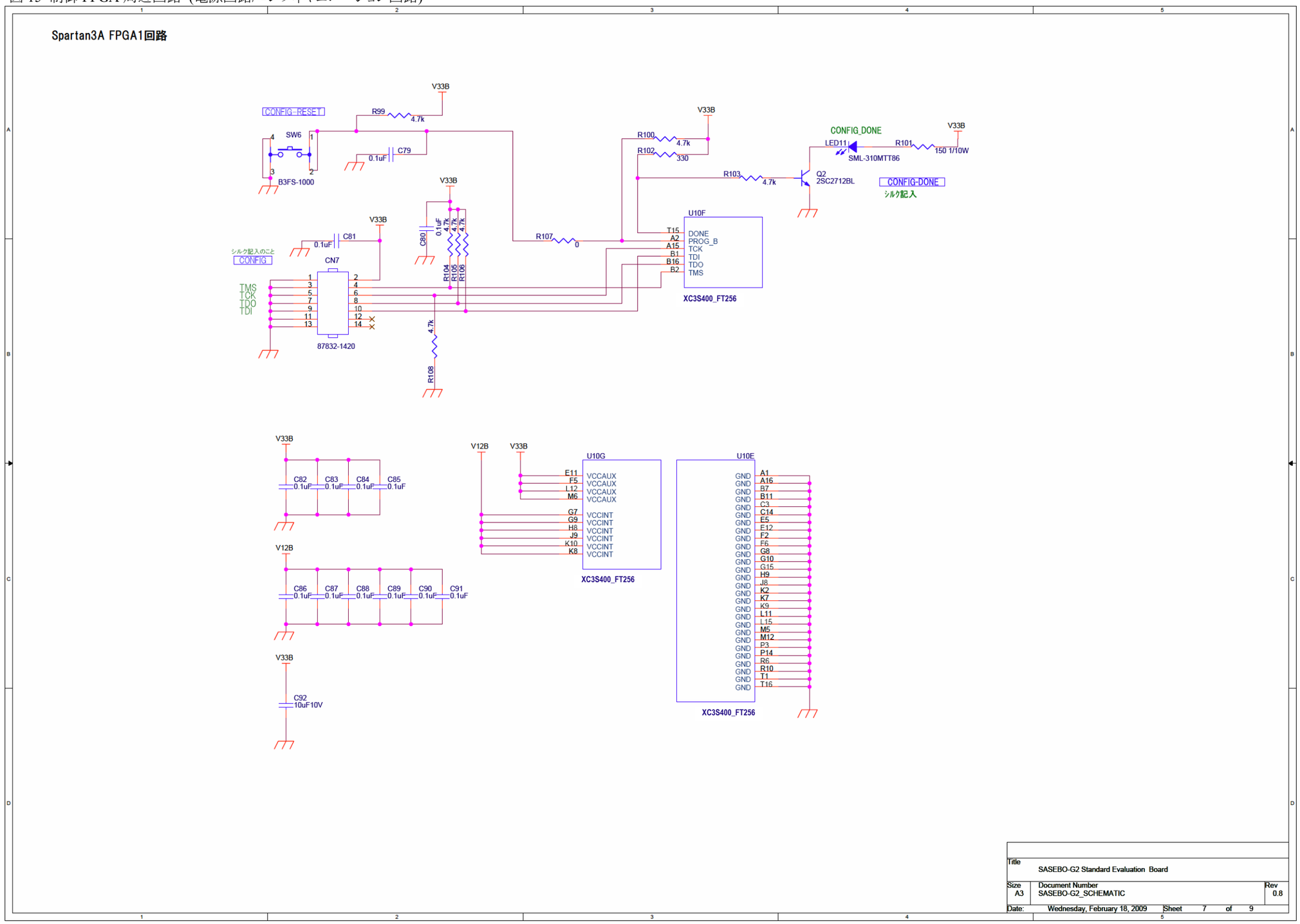


図 16 制御 FPGA 周辺回路 (FPGA 接続部)

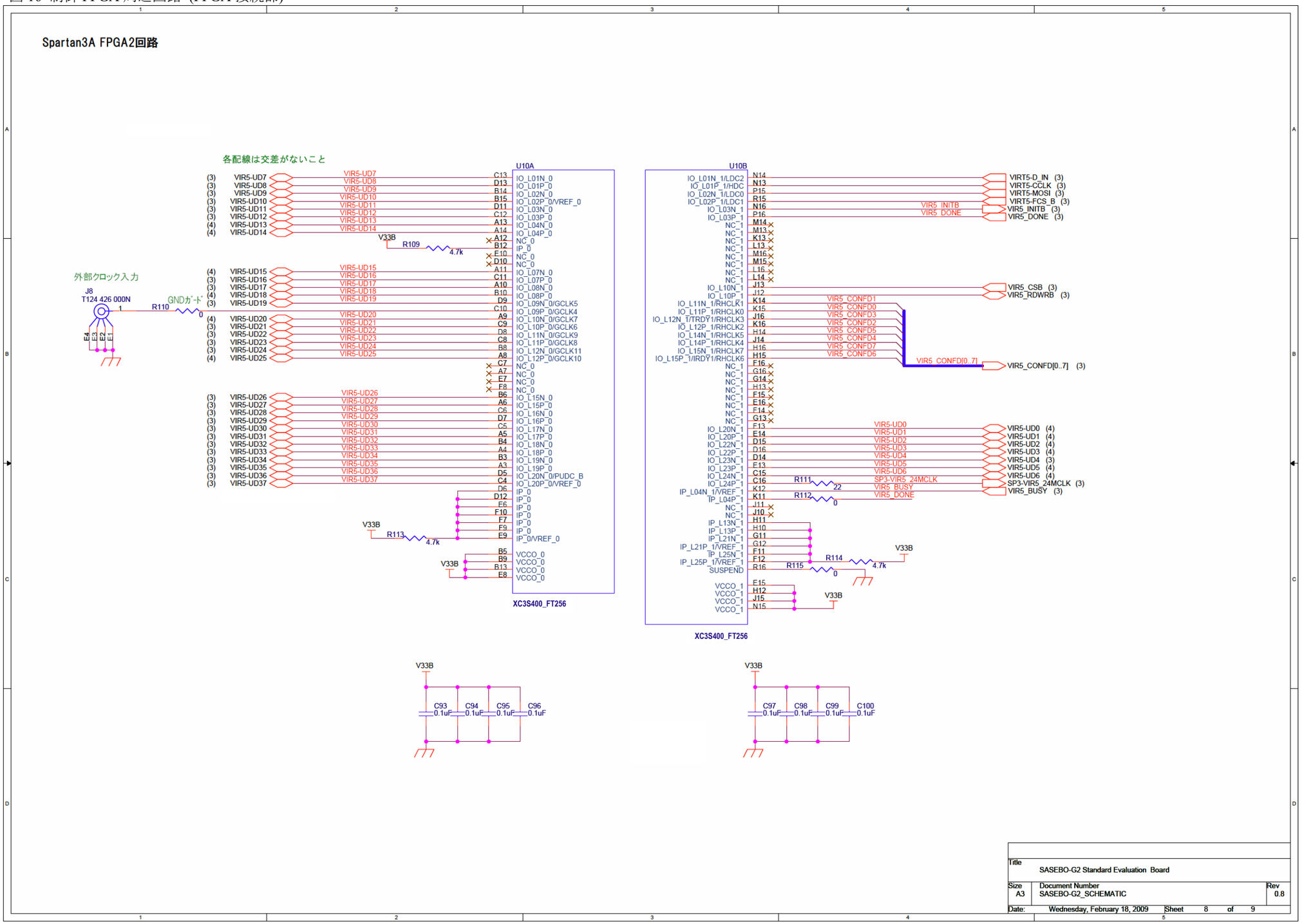


図 17 制御 FPGA 周辺回路 (FPGA 接続部)

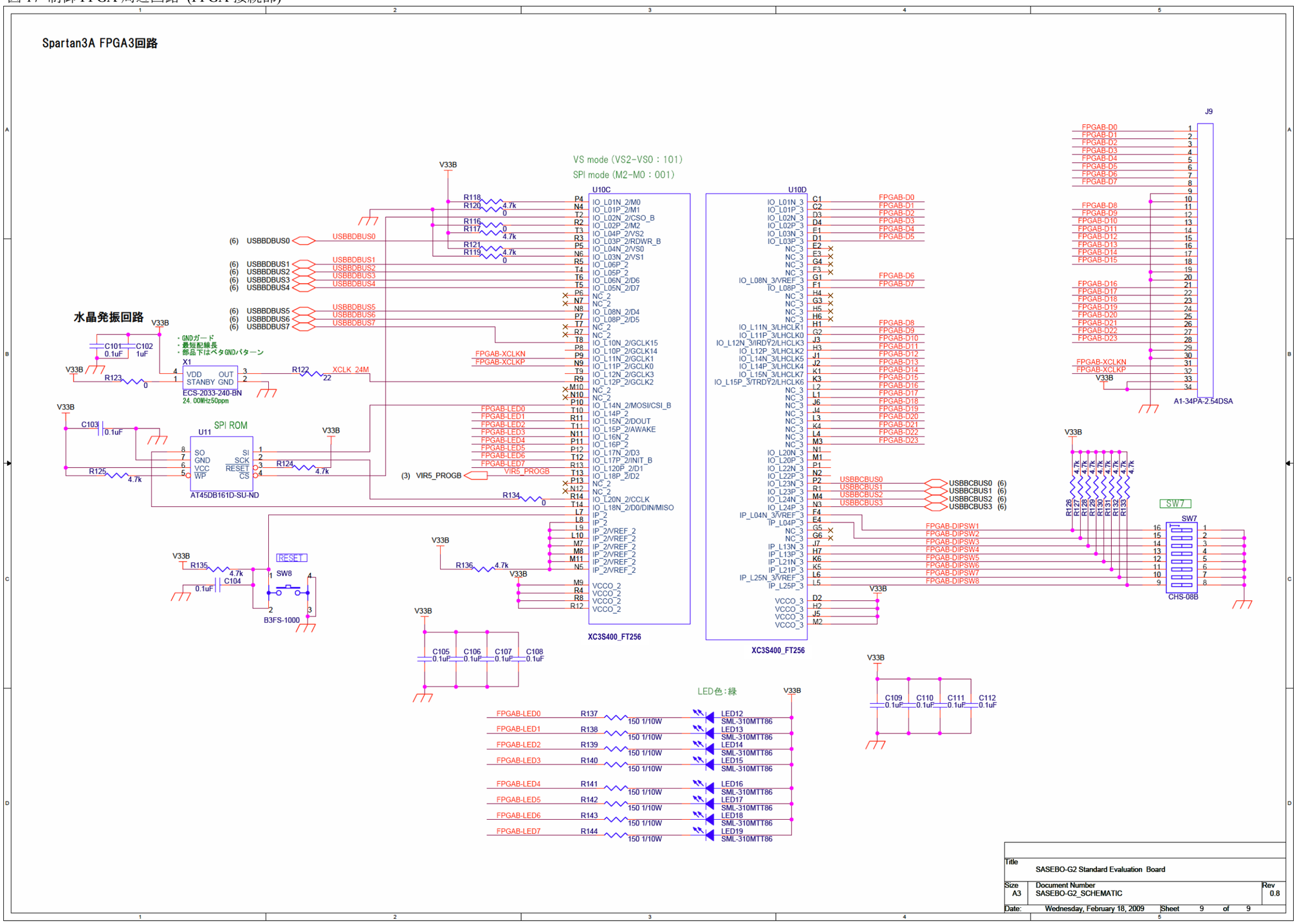


図 18 部品面シルク図/部品面レジスト図(合わせ図)

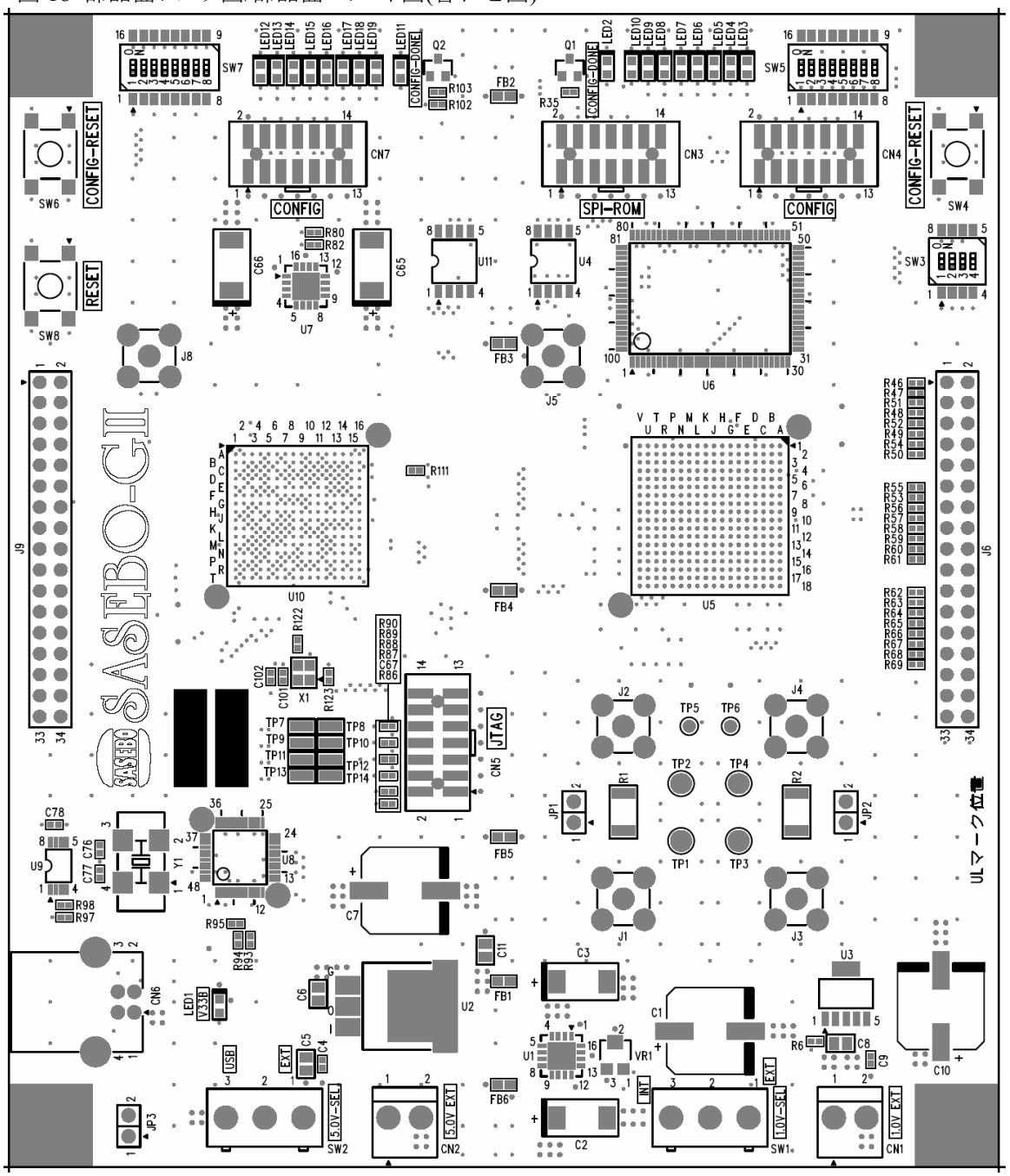


図 19 半田面シルク図(部品面視)/半田面レジスト図(部品面視)(合せ図)

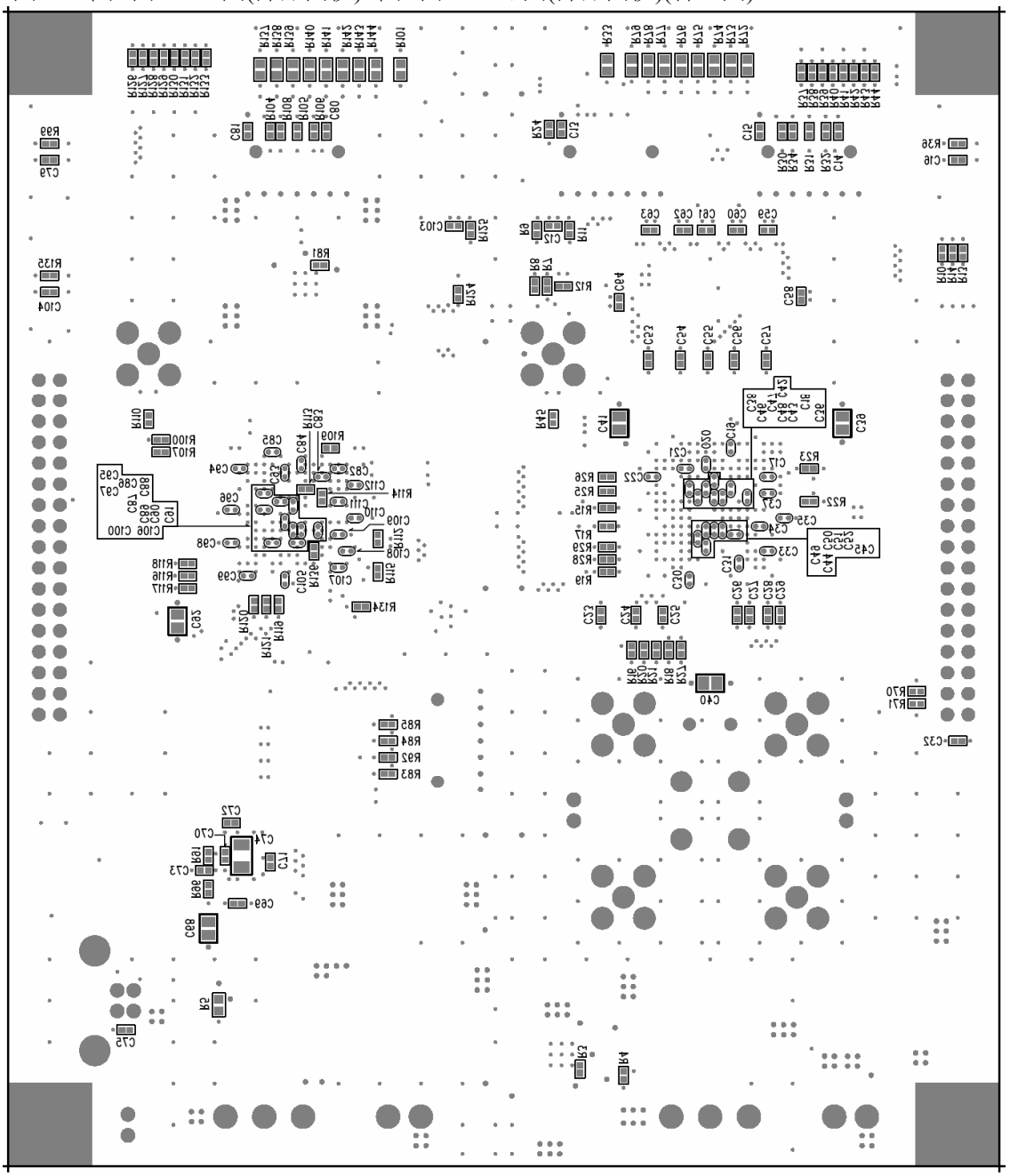


図 20　L1 マスク図(部品面パターン)

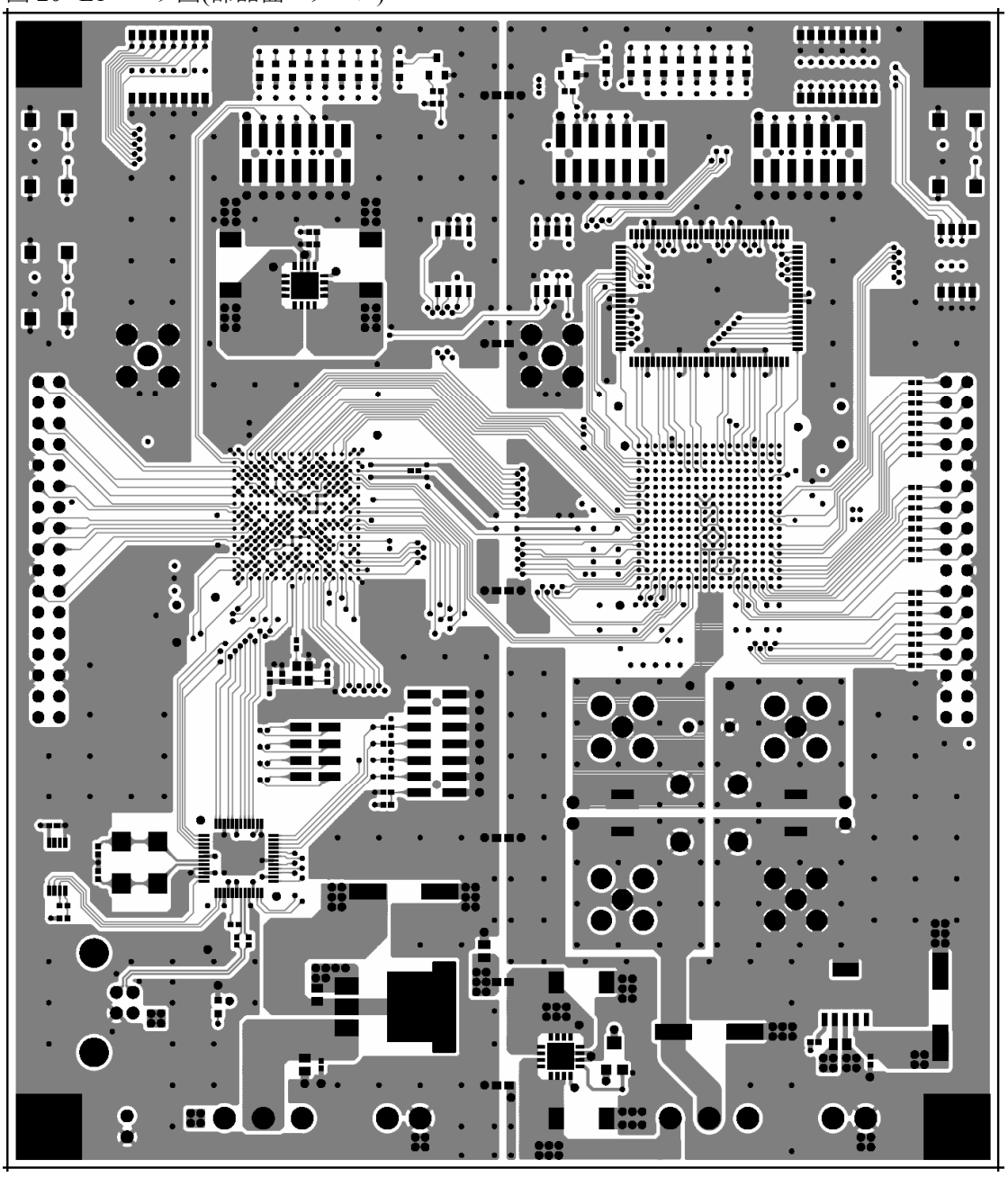


図 21　L2 マスク図(部品面パターン)

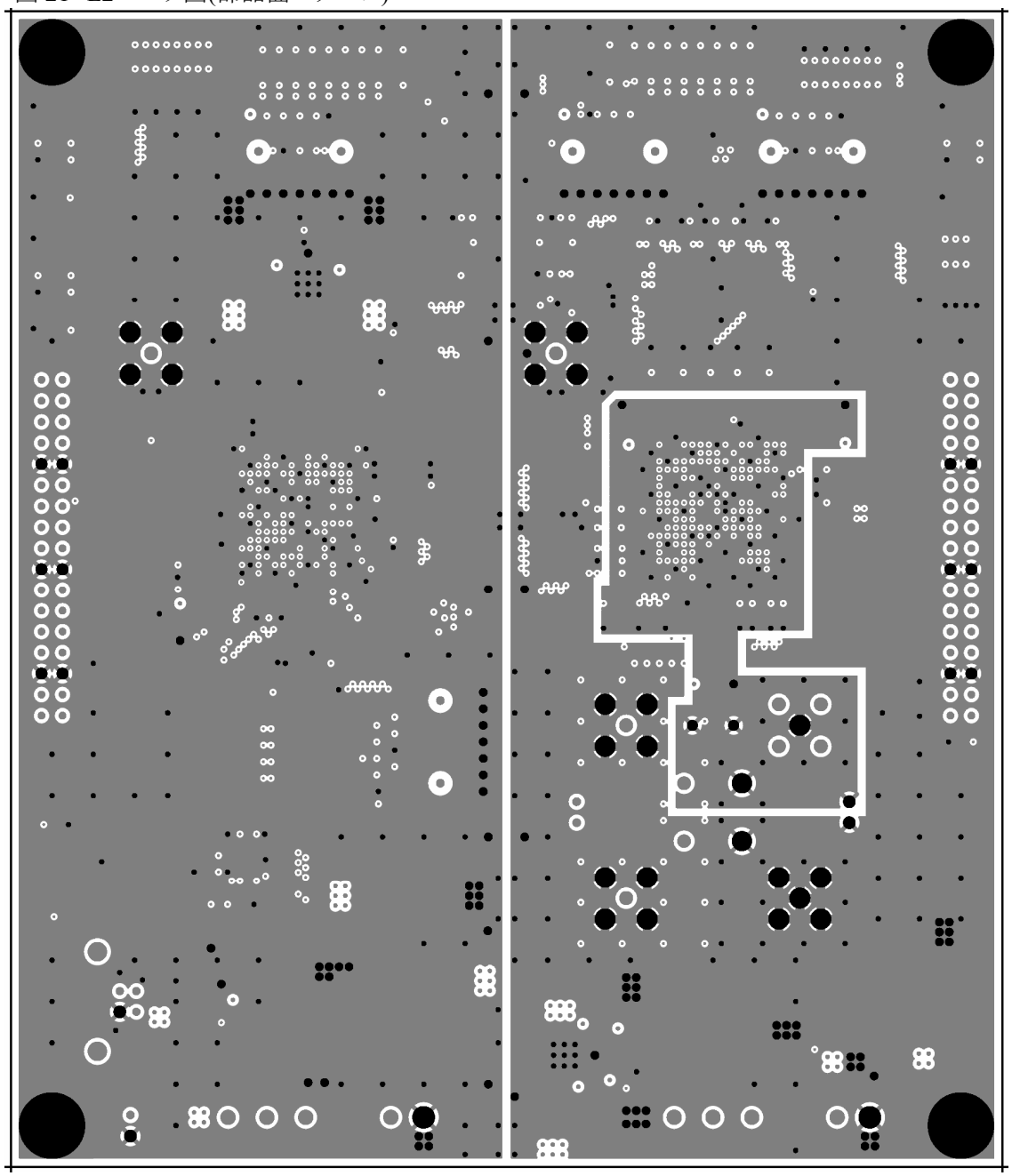


図 22　L3 マスク図(部品面パターン)

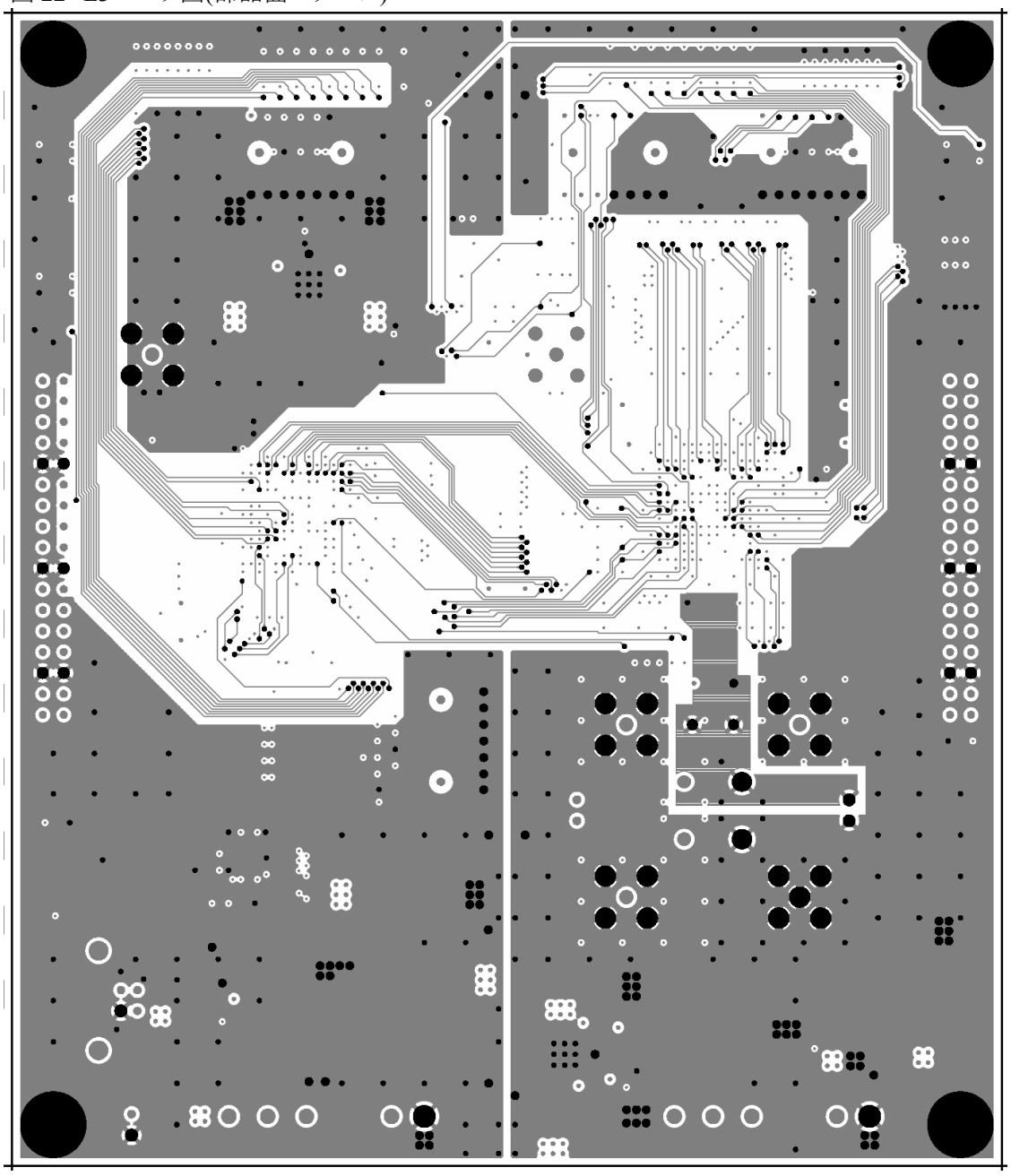


図 23　L4 マスク図(部品面パターン)

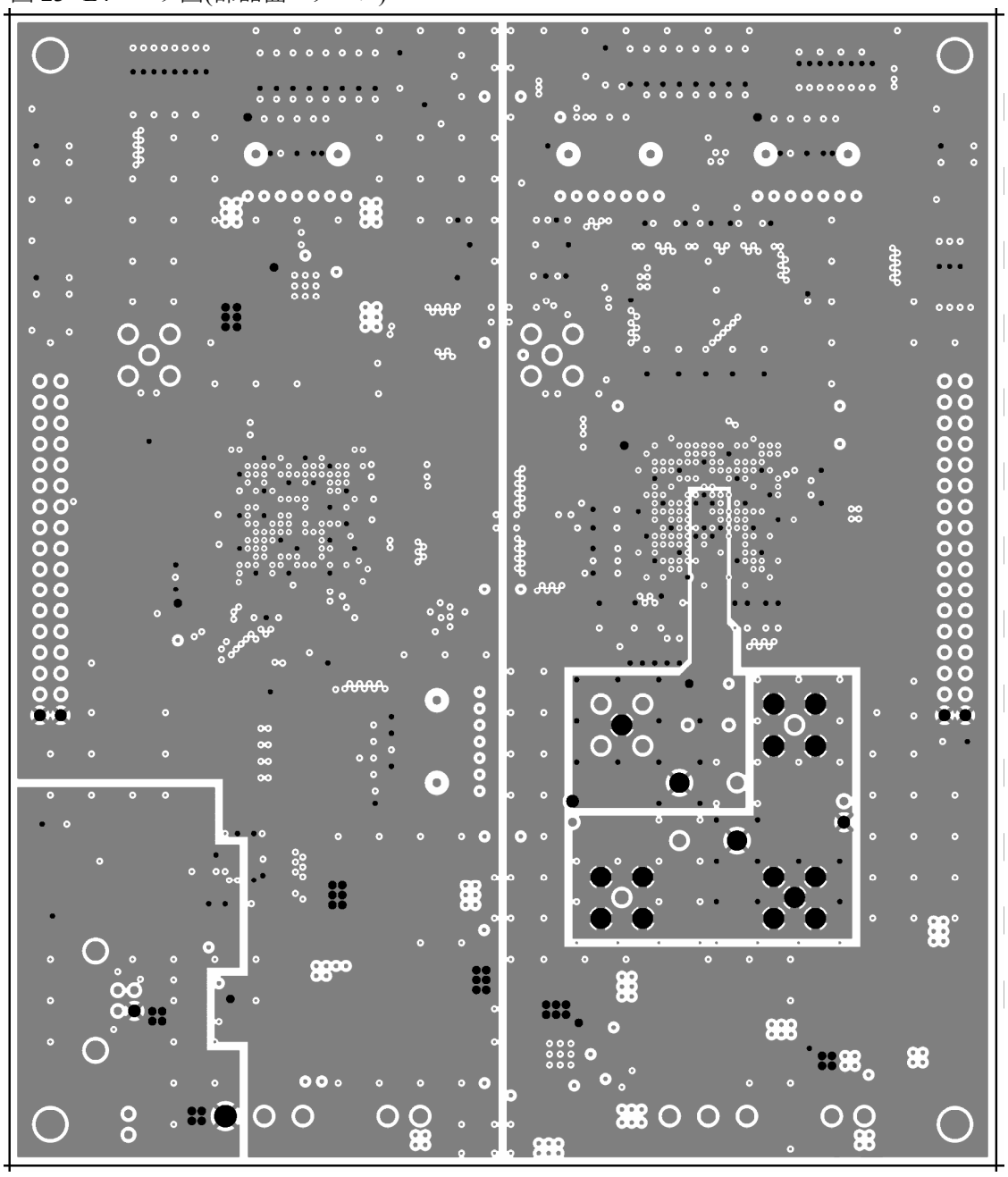


図 24　L5 マスク図(部品面パターン)

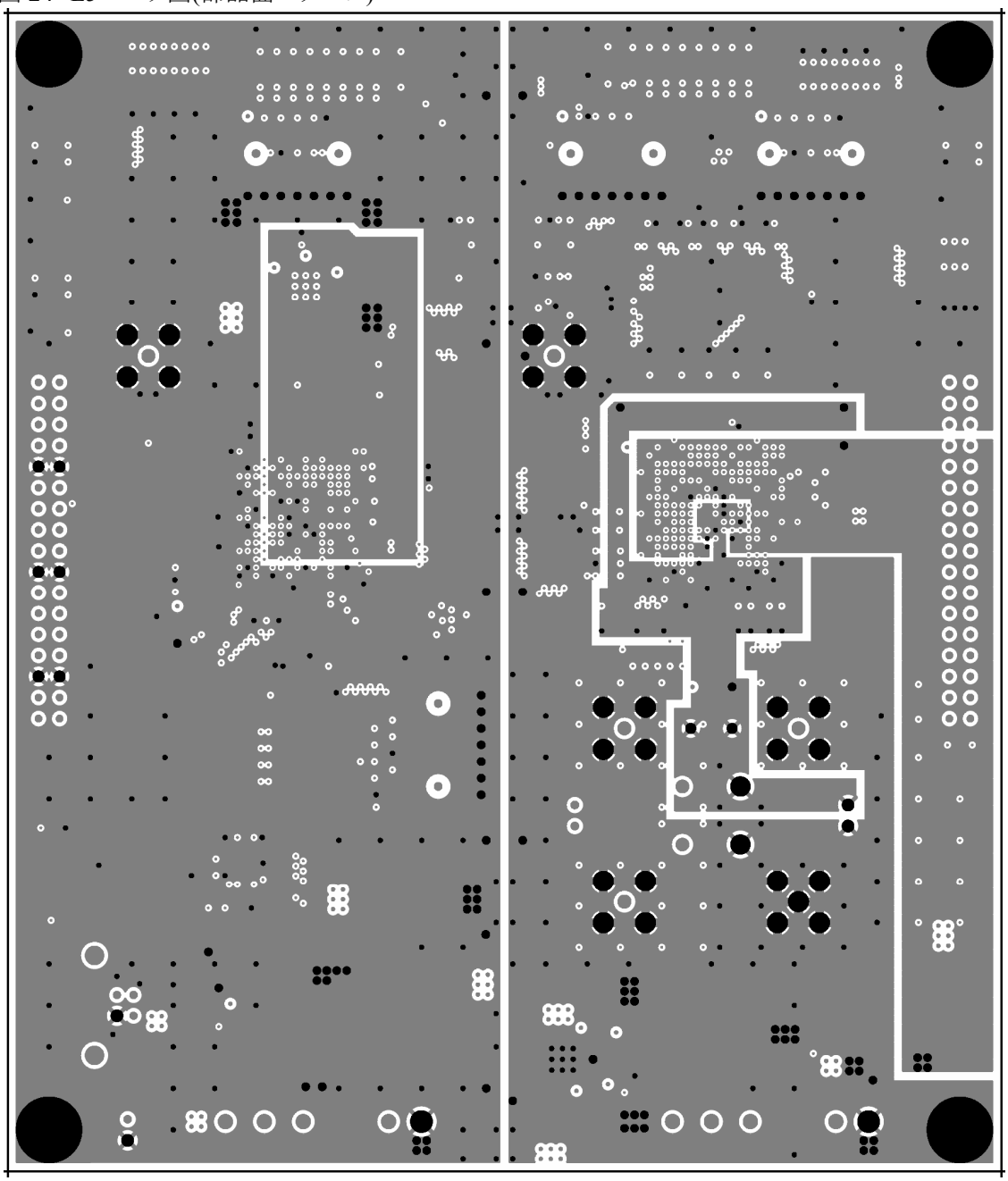


図 25　L6 マスク図(半田面パターン)

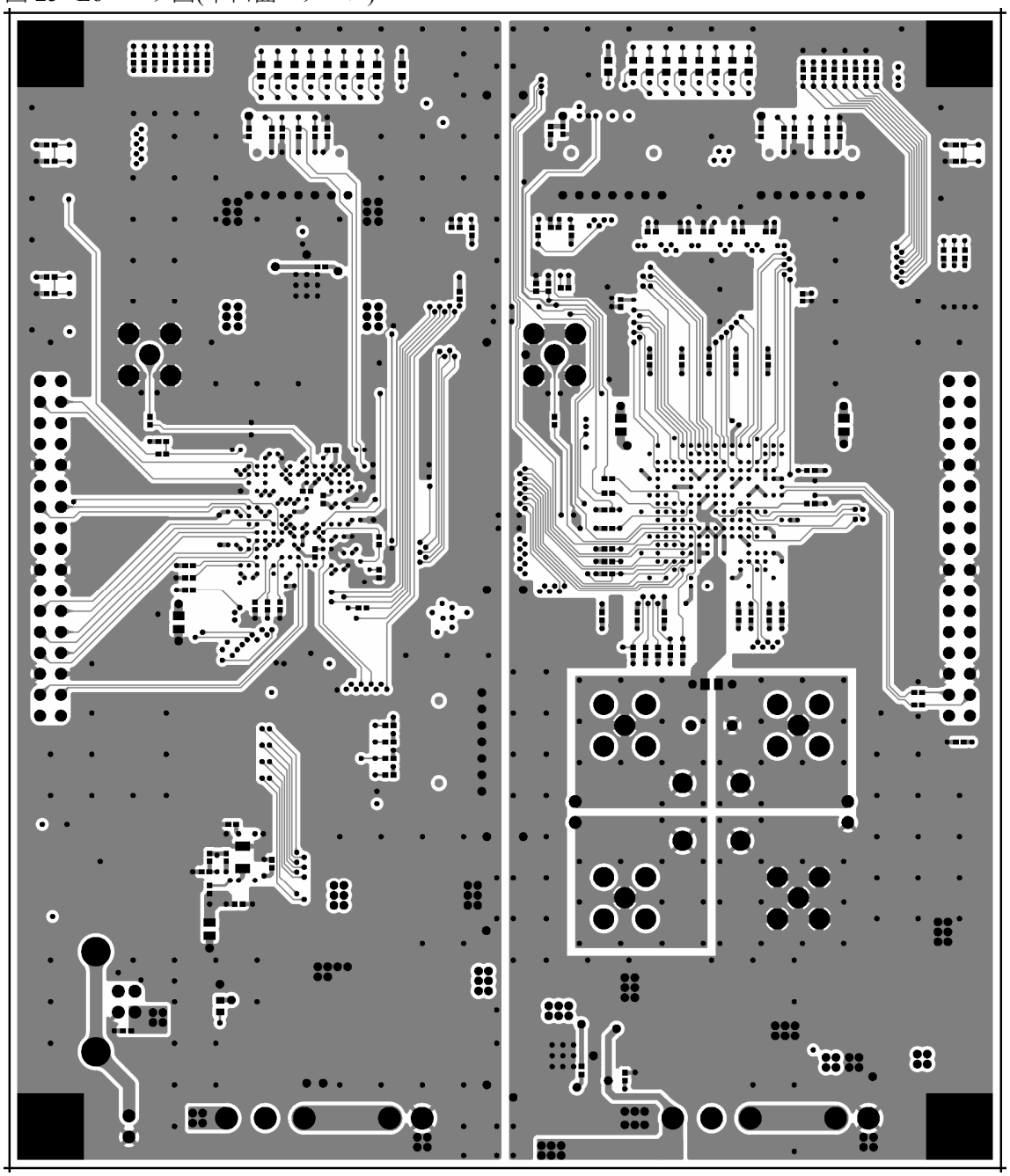


図 26　M1 メタルマスク図(部品面パターン)

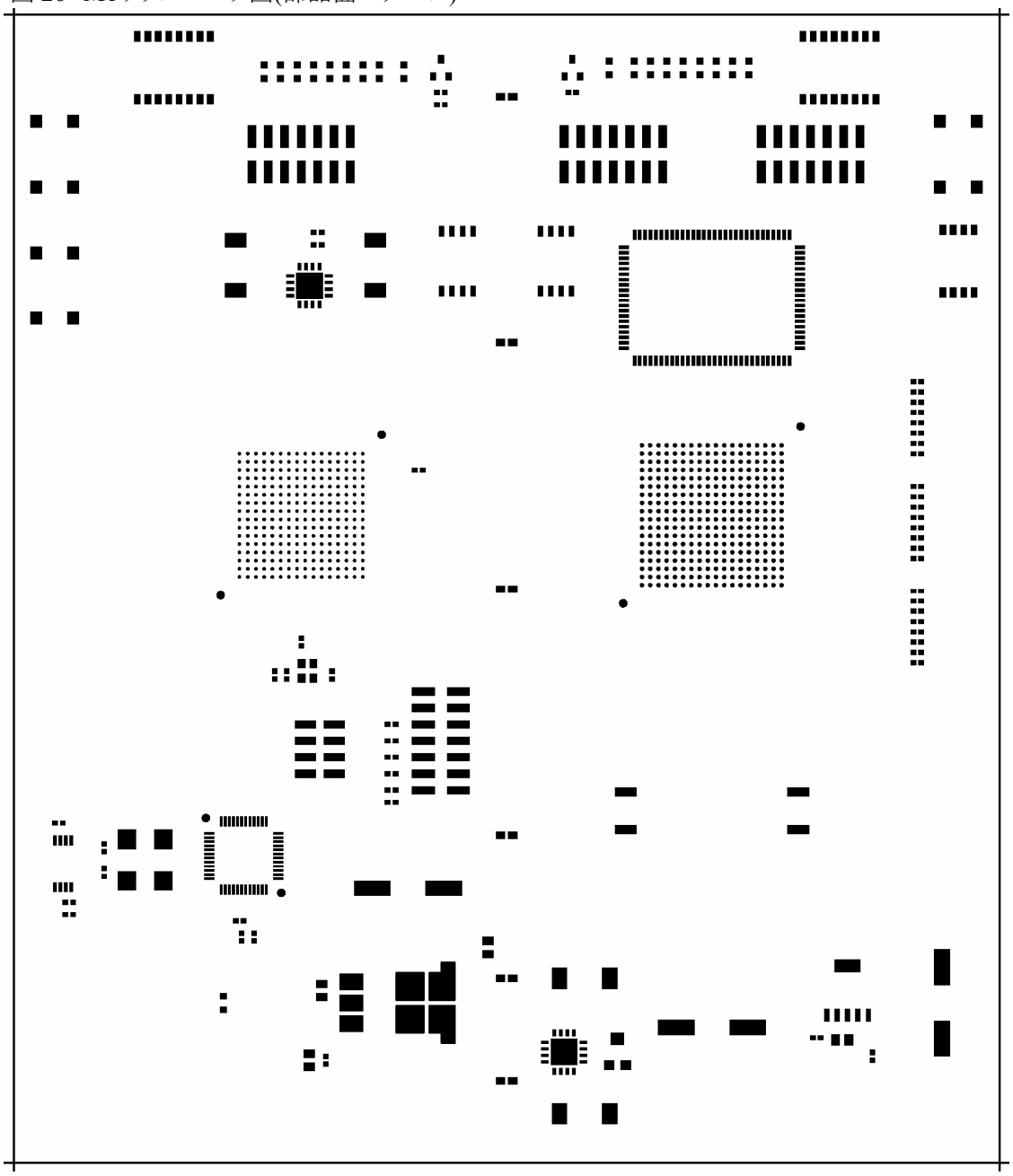
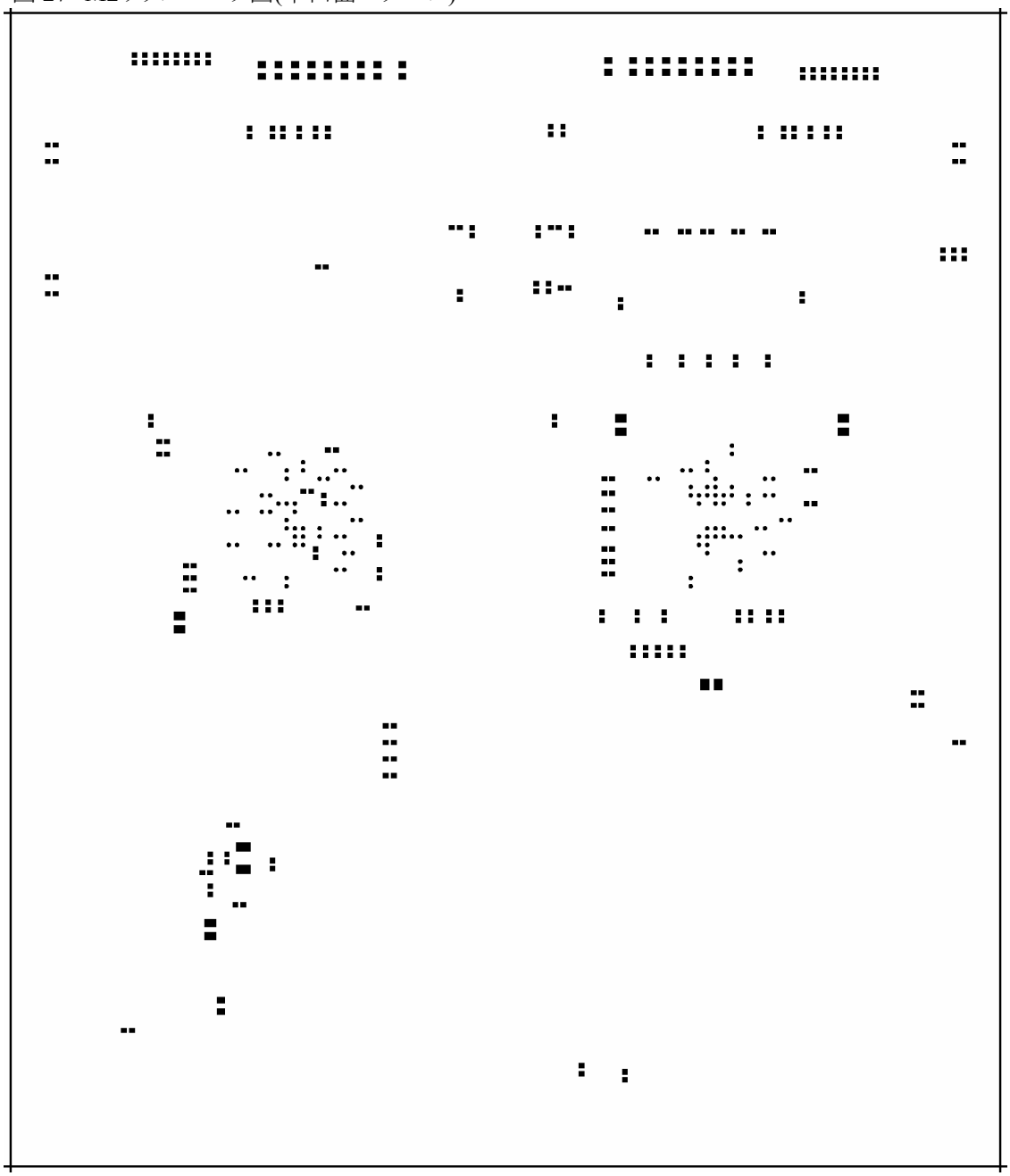


図 27　M2 メタルマスク図(半田面パターン)



SASEBO-GII ボードは経済産業省の委託事業において(独)産業技術総合研究所によって開発されました.

SASEBO-GII board was developed by AIST undertaking projects sponsored by METI (Ministry of Economy, Trade and Industry, Japan)

【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

〒305-8568
茨城県つくば市梅園１－１－１中央第二事業所
TEL：029-861-5284
FAX：029-861-5285