

SmartNIC間 軽量暗号ASCON 動作実演

ASCONは、2023年に米国NISTによって次世代の軽量暗号標準として選出された、認証付き暗号（AEAD）アルゴリズムです。従来の標準規格（AES）に比べ、極めて少ない計算リソースで動作するように設計されています。

◆「今」奪われるデータを、未来の脅威から守る

悪意ある第三者が暗号データを事前に収集し、将来量子コンピュータで解読する「Harvest Now, Decrypt Later」の脅威が迫っています。ASCONは設計段階からこの攻撃を想定しており、長期にわたり圧倒的な安全性を維持します。



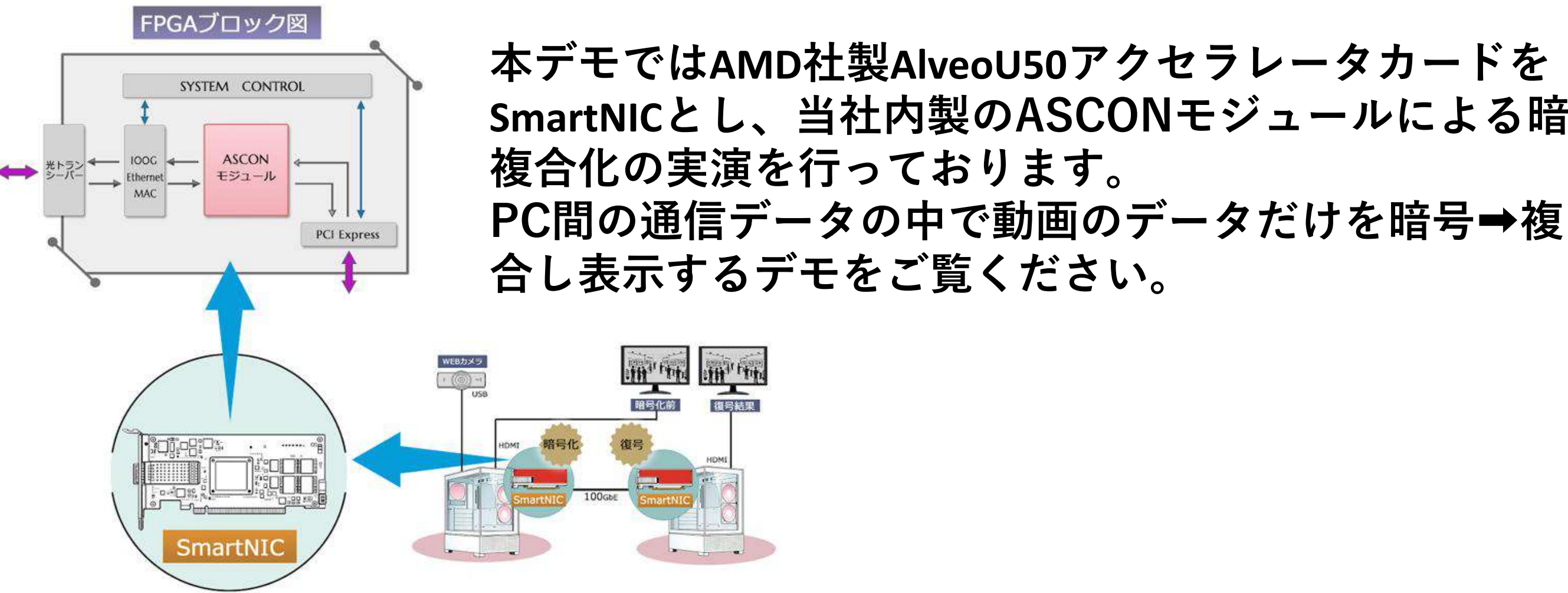
◆宇宙線・発熱を克服する、圧倒的な「軽さ」

暗号化と改ざん検知を1つのアルゴリズムで完結。回路を極限まで小型化し、低消費電力を実現しました。宇宙空間などの過酷な環境下でも、発熱や宇宙線エラーのリスクを最小限に抑えます。

宇宙品質のセキュリティを、あなたのデバイスに
量子コンピュータ時代を見据えた、超軽量・高安全暗号「ASCON」

■ ASCONの特徴（量子暗号/AESとの比較）

特徴	量子暗号	AES (Advanced Encryption Standard)	ASCON (Lightweight Cryptography)
主な用途	究極の鍵交換・配信(地上拠点間や衛星-地上間の鍵共有)	通信の暗号化（SSL/TLS）、VPN、ストレージ暗号化、PC/サーバー	IoTデバイス、センサー、組み込みシステム、RFIDタグ
設計思想	物理学（量子力学）に基づく安全性。盗聴が検知可能	高い処理速度、安全性、標準規格（デファクトスタンダード）	最新・軽量（少ないハードウェアリソース）、省電力、耐タンパー性
処理負荷	極めて高い（光子検出や専用デバイスが必要）	高い（CPU負荷が比較的大きい）	低い（メモリ・電力消費が少ない）
安全性	理論上「解除不可能」	共に高い	
規格の背景	ITU-T等で標準化進行中。次世代の国家機密通信向け	米国政府の標準（FIPS 197）	米国NISTによる軽量暗号の標準

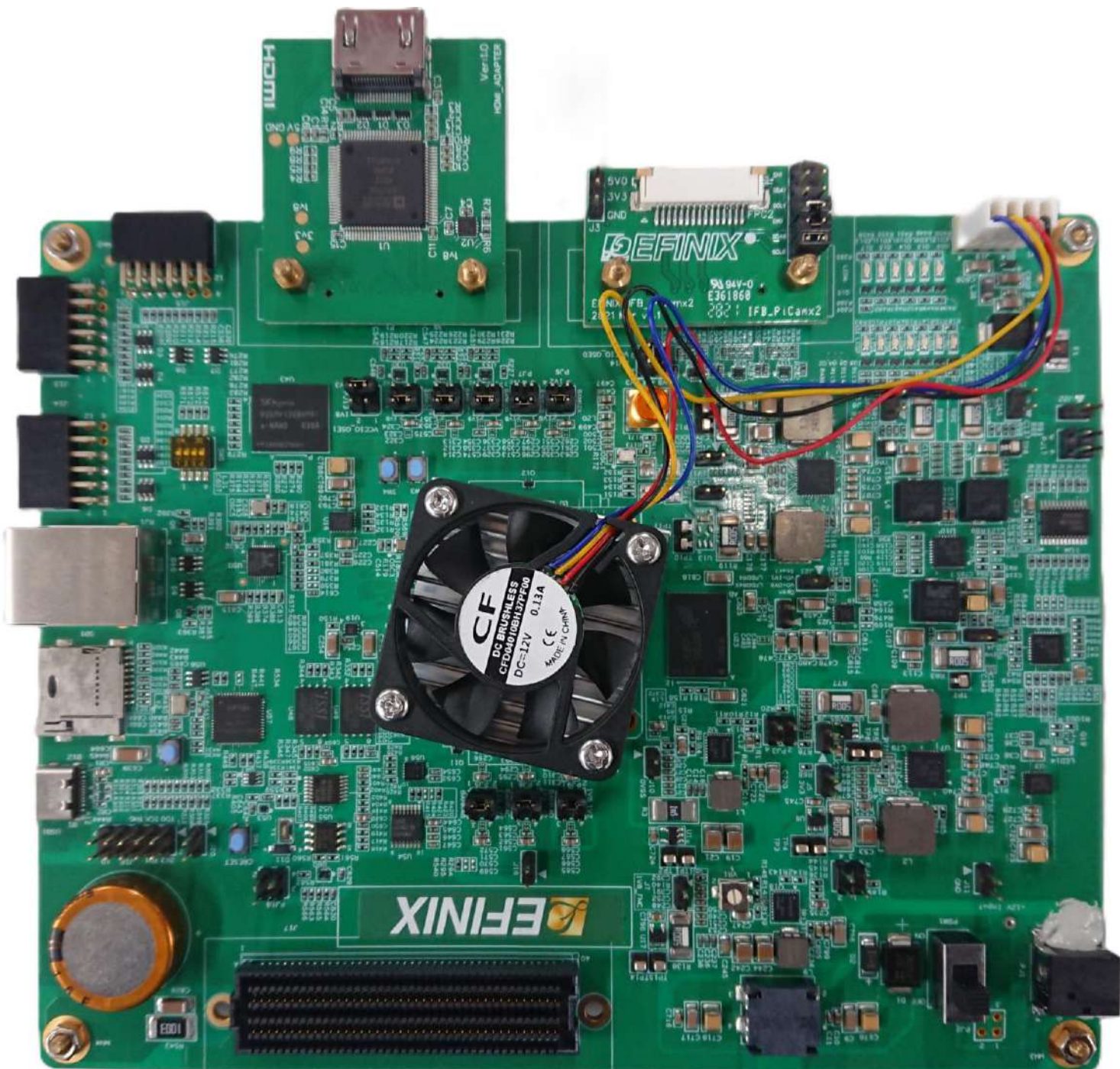


■ ASCONの宇宙関連事業への応用例

衛星間通信	省電力でセキュリティを担保しつつ低遅延での通信を可能にできる。
超小型衛星への応用	CubeSatなど超小型で低消費電力を求められるシステムへ容易に組み込み可能。
高信頼性	月面や火星で、複数のローバー（探査車）や着陸船、ドローンにIoTデバイスとして実装しそれぞれの連携をセキュアで低遅延なものとして組み込み可能。

*AMD Alveo™ は、米国およびその他の各国における Advanced Micro Devices, Inc. の商標または登録商標です。

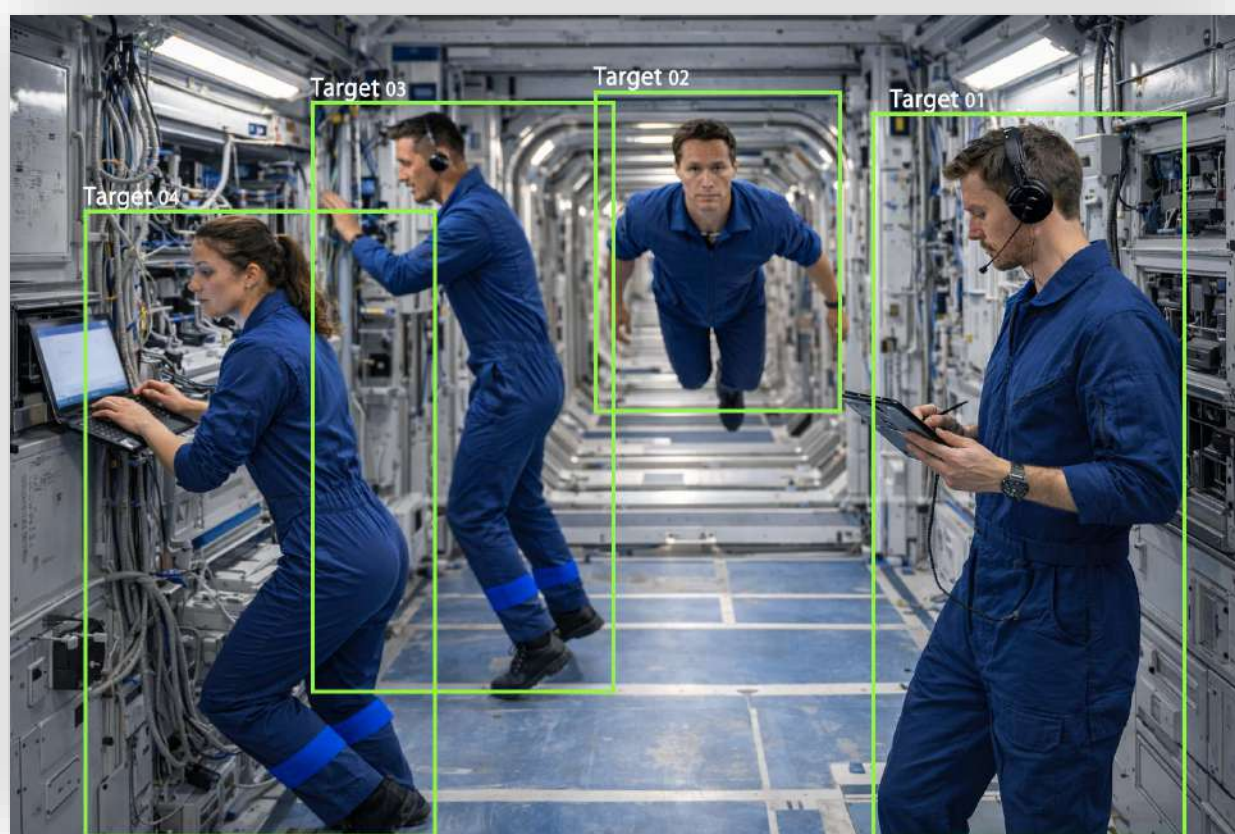
産業用エッジAIボード(Efinix)



■評価ボード及び実装AI仕様

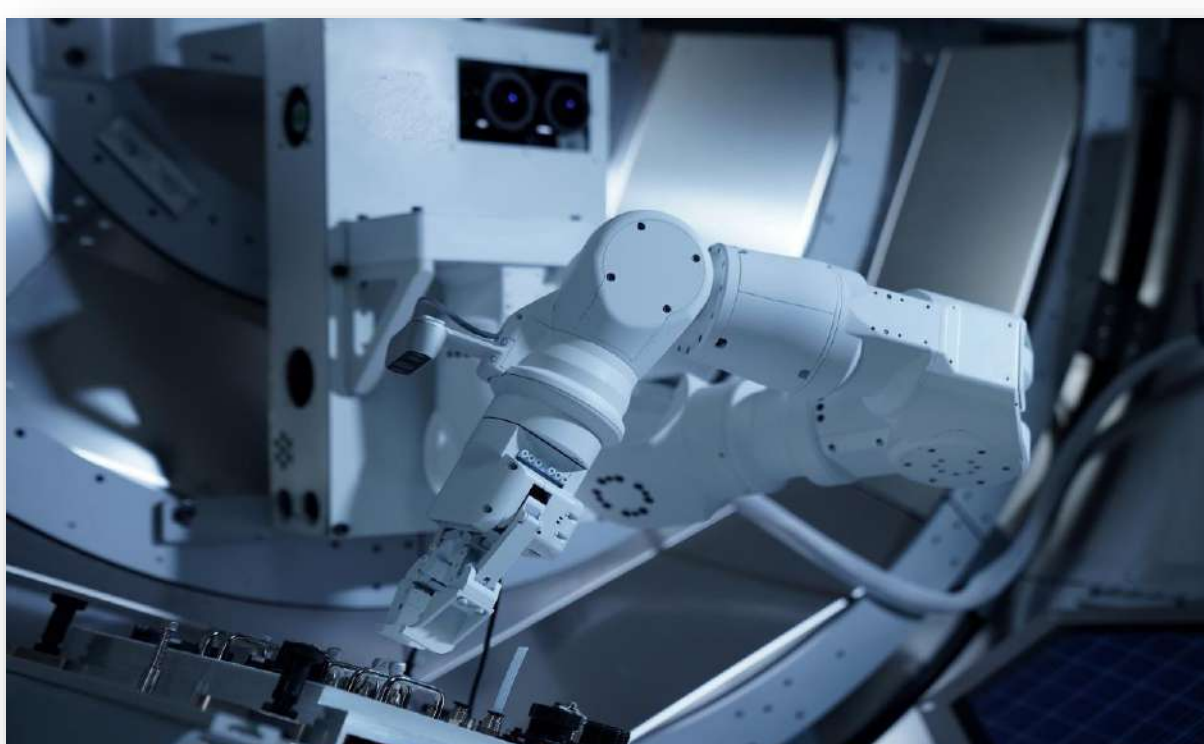
評価ボード仕様	
評価ボード型式	Ti375F524 Titanium_Ti375評価ボード
ベンダー	Efinix,inc. (URL https://www.efinixinc.com/jp/index.html)
HW仕様	Efinix Ti375C529C4(1) FPGA in a 529-ball FineLine BGA package 8 Gbit (256 Mbit x 16 x 2 channels) LPDDR4 or LPDDR4x SDRAM 512 Mbit SPI NOR flash memories 8 GByte eMMC PMODx3 interfaces with extended functionality Gigabit Ethernet interface supporting RGMII standard and complies Micro-SD card slot Supports RTC function
電源	定格入力電圧 DC12V
LED表示	本体PWR(緑),FPGA PowerGood (緑) ユーザーカスタマイズLED 5ヶ (緑)
外形寸法	170mm(W) x mm(D) x mm(H)
AI仕様	
生成モデル	Yolo v8 (人体検知AI)
AI判定速度	1.6TOPS INT8 Perf 64fps
AI推論モデル	eCNN Hardware Accelerator モデル +Tensorflow,Pytorch etc...

当社開発のエッジAIボードは、人物認証に留まらず動き方向を認識して在室カウンターとしての使用や、酸素/二酸化炭素濃度などのセンシング情報から予測値によるコーション/アラート発報など、幅広いニーズにボード単位で対応致します。



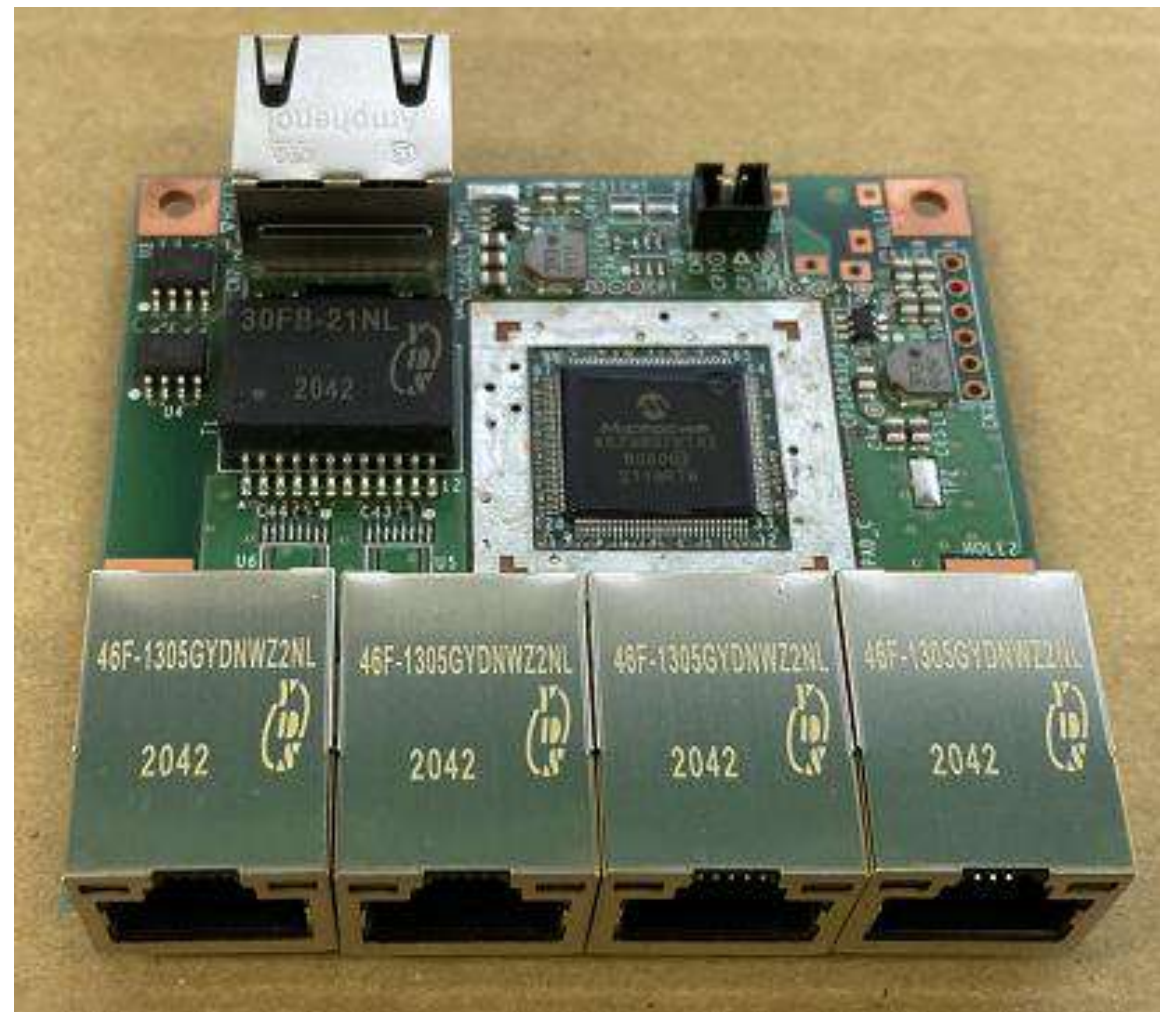
例えば、ISSなどの有人宇宙滞在施設における居住区や実験棟などへの人の出入りや滞在人数の把握などに、施設側のリソースへの負担を軽減し、リアルタイム性を上げる手段として。

例えば、宇宙飛行士の船外活動時のバイタルデータと残存酸素および排出ガスなどから、活動可能時間や活動中止のコーション/アラートを上げて、他クルーの判断、指示の補助として。



例えば、宇宙空間実験装置のセンサーデータから、得られる結果の予測値を返して実験の精度を上げたりロボットアーム遠隔操作時に周囲の障害物の検知からの即時動作補正など、クルーの補助として。

宇宙/航空向け 高信頼性超小型Gigabit L2スイッチ



当社が開発した組込み用の超小型ギガビットLayer2 Switchに、宇宙/航空向けとして耐放射線遮蔽、動作温度範囲拡張などのカスタマイズを実施し、更なる高信頼性を付与したモデルです。
円軌道（高度600km、傾斜角98.0度）5年間耐えられる条件を満たしています。

（放射線量分析モデル：SHIELDOSE2）

（※特許取得済み）

■特徴

- ・組込みに特化した設計により、名刺より小型化され装置内への組込み自由度が格段に向上
- ・ODMメーカーとして半世紀を超える歴史を持つ当社開発品のため、長期サポートを実現
- ・産業機器や医療機器への組込みを想定した設計により標準品の段階で高い信頼性を実現
- ・カスタマイズにより高い放射線耐性（特許取得済み）と標準品を大きく超える動作環境温度（-40℃～85℃）を実現
- ・入力電圧の変更やLANコネクタ位置の変更など、カスタマイズ可能

信頼性とコストの相反する高い要求にも、高い信頼性と低コストを実現した本機で応えます。

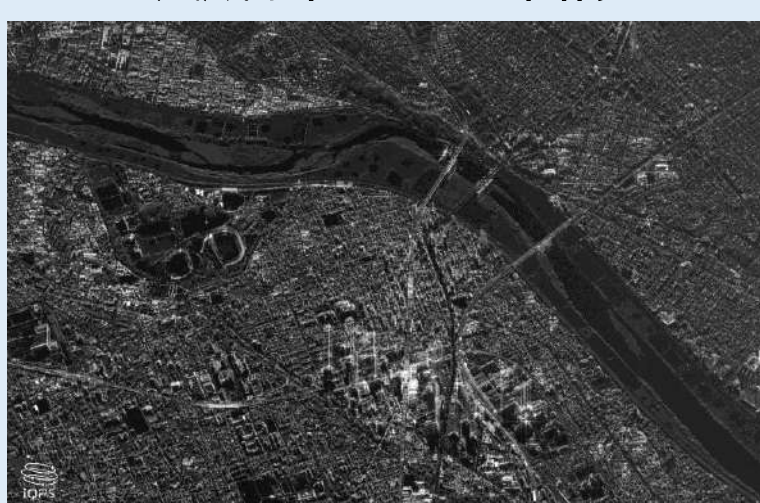
宇宙/航空分野でのCOTSの活用化へ貢献

■実績

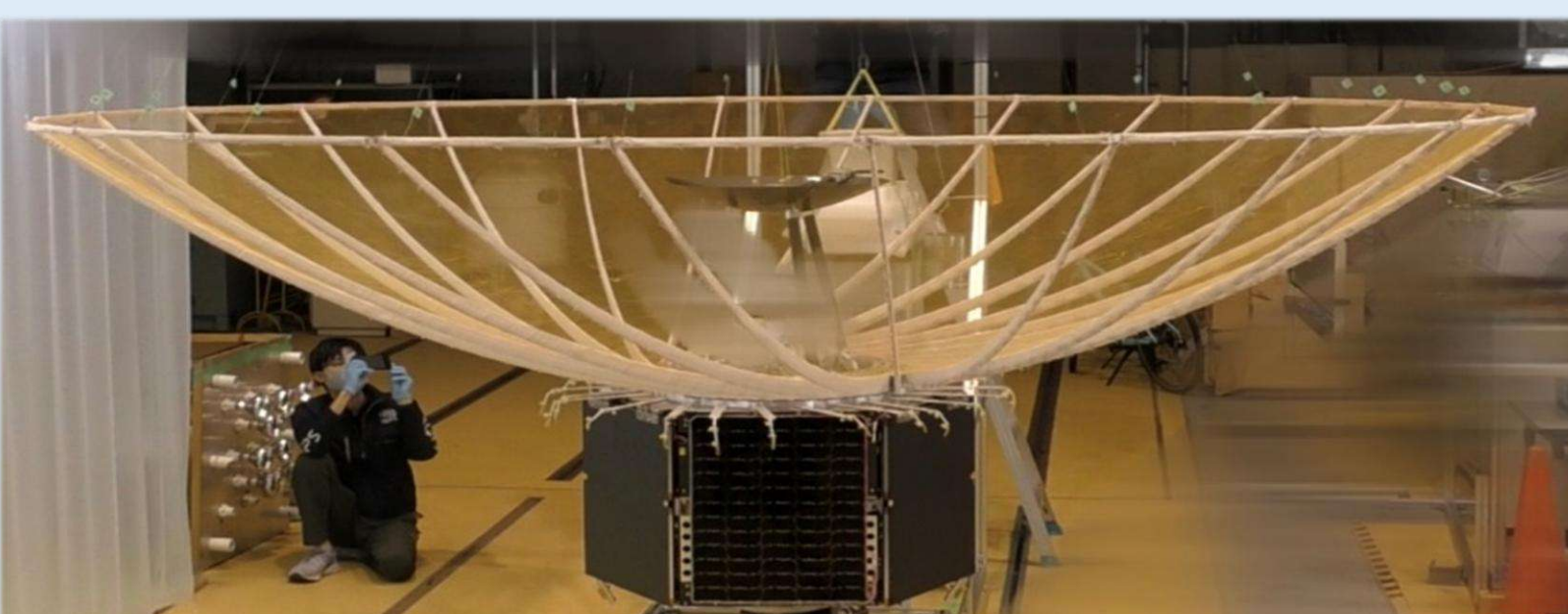
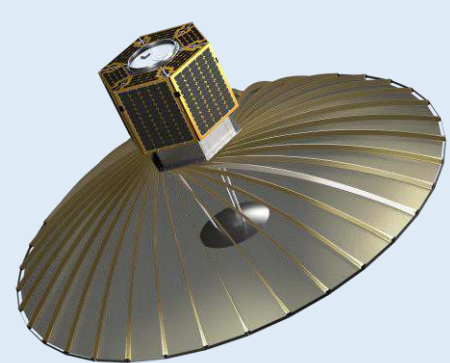
株式会社QPS研究所様の2021年1月25日に打上がった小型高精細SAR衛星QPS-SAR 2号機「イザナミ」以降、同社の衛星内部の通信ユニットとして採用されています。

現在までに十数機が打ち上げられ、運用中の全ての衛星において問題なく動作しています。

武蔵小杉レーダー画像



- ・衛星高度：550km～600km
- ・軌道傾斜角：42度（一例）



画像提供：QPS研究所様

■仕様

標準規格	IEEE802.3i(10M) IEEE802.3u(Fast Ethernet) IEEE802.3ab(1000Base-T) IEEE802.3x(フローコントロール)
データ転送速度	10/100/1000Mbps(CSMA/CD)
イーサネットポート	10BASE-T/100BASE-TX/1000BASE-T x5ポート (MDI/MDI-X自動切替) 内1portは背面仕様 Duplex Full/Half ,Auto Negotiation 対応
機能	スイッチングモードストア&フォワード方式 ノンブロッキング・フルワイヤスピード対応スループット 1000M⇄1000M 1,488,000pps(64Byte) 100M⇄100M 148,800pps(64Byte) 10M⇄10M 14,880pps(64Byte) バッファ容量256Kbyte(全Port) Jumbo Frame 最大9,000Byte MACアドレス登録数 4,000エン트리(最大) エージングタイム 300秒
LED表示	本体PWR(緑),ポート(UTP) Link/ACT(Linkup: 緑、ACT: 点滅)
電源	定格入力電圧 DC5V 最大消費電力 3.5W
環境条件	動作温度: -40～85℃、湿度: 10～95%以下(結露無き事) 放射線耐性: <24krad
外形寸法	67mm(W) x 51.6mm(D) x 18mm(H) 突起物含まず



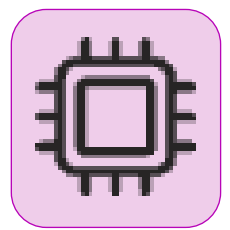
スペースICT推進フォーラム法人会員

会社概要のご紹介



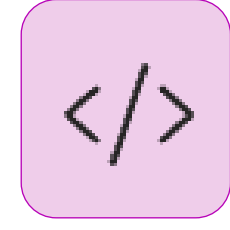
超高速フォトニック
ネットワーク開発推進
協議会 会員

1. ODM [受託設計・製造]のご紹介



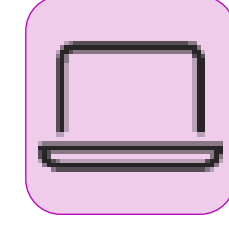
電子回路設計

お客様の要件に基づき、長年の経験とノウハウを活かした高品質な電子回路を設計いたします。



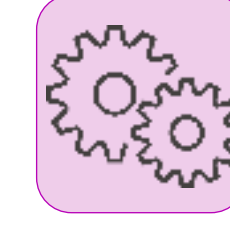
FPGA設計

様々なFPGAデバイスでの設計実績があります。複雑な処理を効率的に実現いたします。



SW設計

ハードウェアと一体となった最適なソフトウェアをご提案し、完成度の高いシステムを構築いたします。



製品製造

設計した回路図から電子基板を製作いたします。また製品の組み立てや配線まで対応可能です。

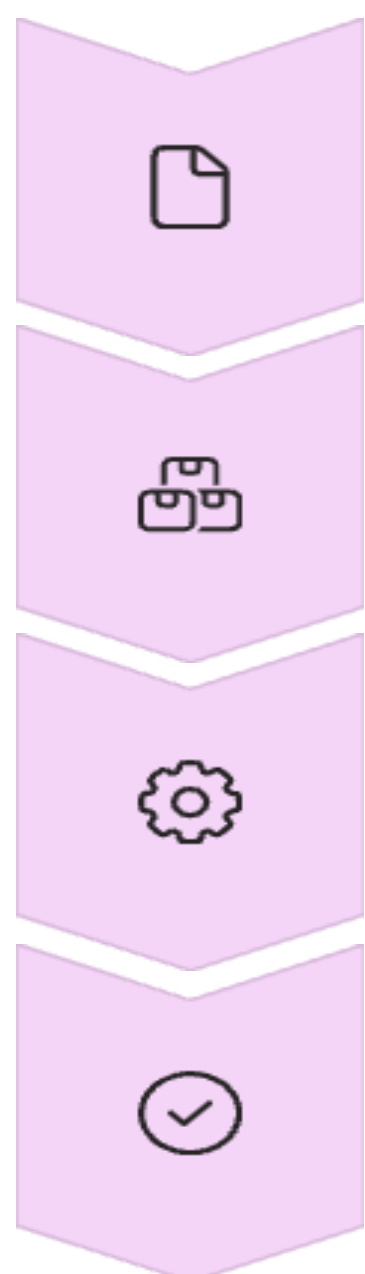
2. FPGAデザインサービスのご紹介



- 2015年 Xilinx社のアライアンス・パートナー・プログラムに加入
- 高速トランシーバ、ZynqSoCの最新デバイスを駆使した最適デザイン
- HDMI, SDI, DisplayPort等の各種映像IFの実装経験
- 200G/400Gb Ethernet システム開発（低遅延伝送 etc）
- ディスコンデバイスのマイグレーション（デバイス置換）対応可能

- 2020年よりEfinix社のデザインパートナー契約
- RISC-V SoC ソリューション、迅速なローカルサポートを提供可能
- RTOSファームウェア開発実績

3. EMSサービスのご紹介



図面確認

部材調達

実装・組立

評価・検査

当社のEMSサービスでは、お客様の設計したシステムをISO9001に則ったプロセスで高品質な形にします。
チップサイズ 0402 の実装が可能であり、大型基板（510mm × 460mm）まで対応可能という柔軟性も強みです。

保有設備

装置名	メーカー	型番
はんだ印刷機	パナソニック	SP18P-L
はんだ印刷検査機	CKD	VP9000L
多機能実装機	パナソニック	AM100
リフロー槽	タムラ製作所	TNV-L7412CR-X
画像検査装置	オムロン	VT-S500
マイクロスコープ	キーエンス	VHX-X1
X線検査装置	アイビット	FX-300tRX2

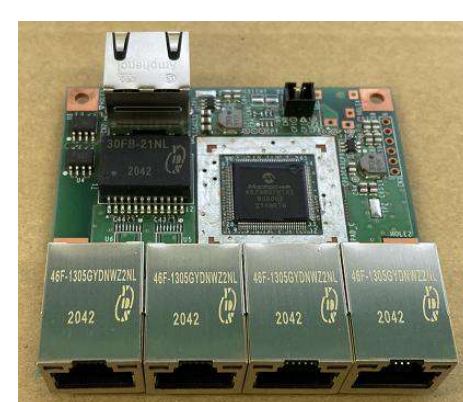
宇宙航空用途向け伝送機器開発

【DWDM】



- Video Interface : ARIB-STD-B58 (MM 850nm×24)
- TRUNK Interface 24Wavelength (ITU-T 100GHz Grid DWDM)
- Transmission distance : ~80km
- Low Latency : 0.33usec
- Size : 450mm(W) x 600mm(D) x 44mm(H)
- Operating Temperature 0 to 40°C

【For AeroSpace HUB】



- 10/100/1000BaseT(X) Ports (RJ45 connector)×5
- Auto negotiation speed Full/Half duplex mode
- Auto MDI/MDI-X connection
- Size : 67mm(W) x 51.6mm(D) x 18mm(H)
- Operating Temperature -40 to 85°C (Custom Ver)
- Ambient Relative Humidity 5 to 95% (non-condensing)

【Optical SW】



- Layer1 Optical Switch
- 1290 - 1330 nm & 1530 - 1570 nm
- 32×32 MEMS
- Interface LC Connector

