Sereform

IoT機器としてのSoC FPGAを簡単かつセキュアにRemote Reconfigurationするための C/C++/Python 向けライブラリ

室蘭工業大学 灰原 渉

2020/01/23 JANOG45

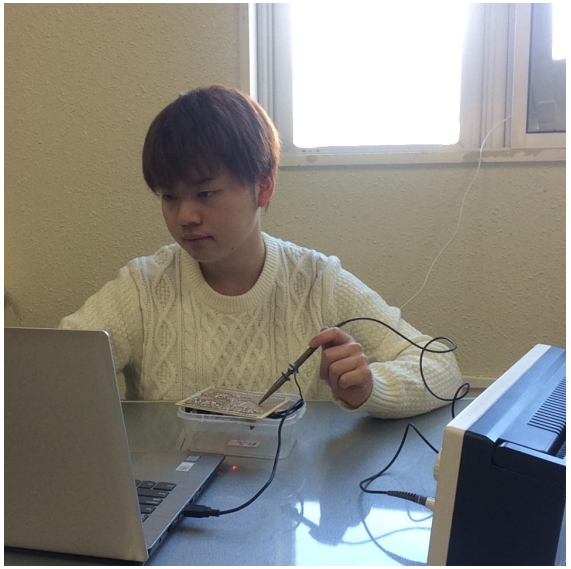
NICT National Institute of Information and Communications Technology

自己紹介

灰原 渉 (Wataru HAIBARA)

- 室蘭工業大学 B2
- 一般社団法人 LOCAL (学生部)
- SecHack365 3期トレーニー

生粋の道産子 && ピチピチの二十歳



Sereform

Secure
Remote Reconfiguration
Plat**form**

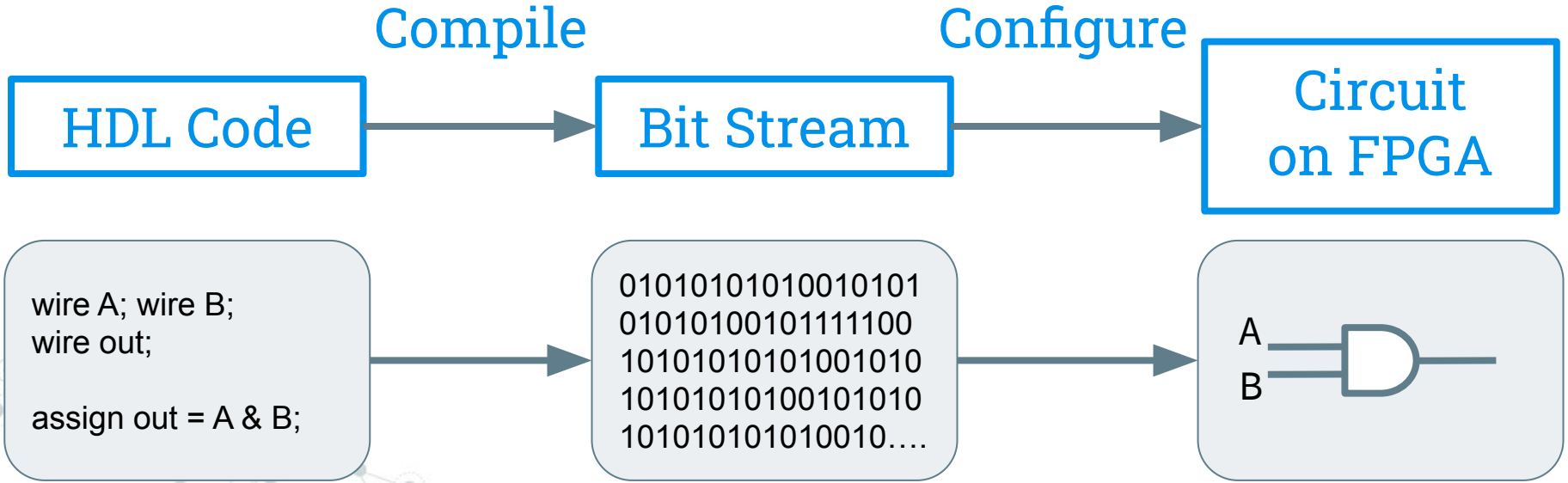
IoT機器としてのSoC FPGAをセキュアに
Remote Reconfigurationするための
プラットフォーム

SecHack365 フィジカルゼミでの取り組み

FPGAとは

Field Programmable Gate Array
内部の論理回路を変更可能な半導体デバイス

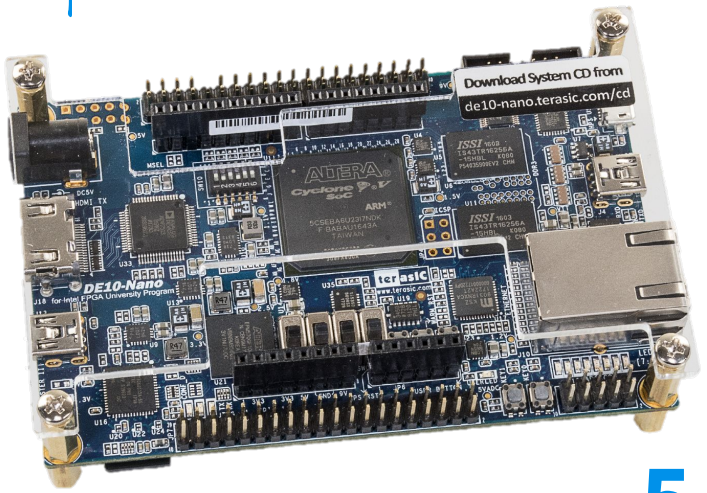
HDL : Hardware Description Language(ハードウェア記述言語)



SoC FPGAとは

プロセッサとFPGAが共にパッケージされたSoC
プロセッサ上のSW と FPGAのHW でデータをやり取り可能
→ プロセッサで通信やその他の汎用的な処理
＋
FPGAで重たいアルゴリズムのアクセラレート

重たいアルゴリズムの例
- 暗号アルゴリズム
- ニューラルネット学習
- 画像処理

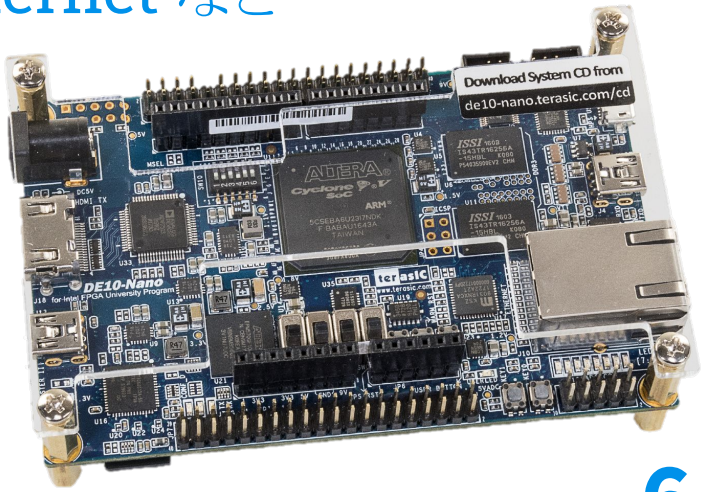


terasic.com DE10-Nano販売ページから引用

使用したSoC FPGAボード

Terasic社 DE10-Nano Kit

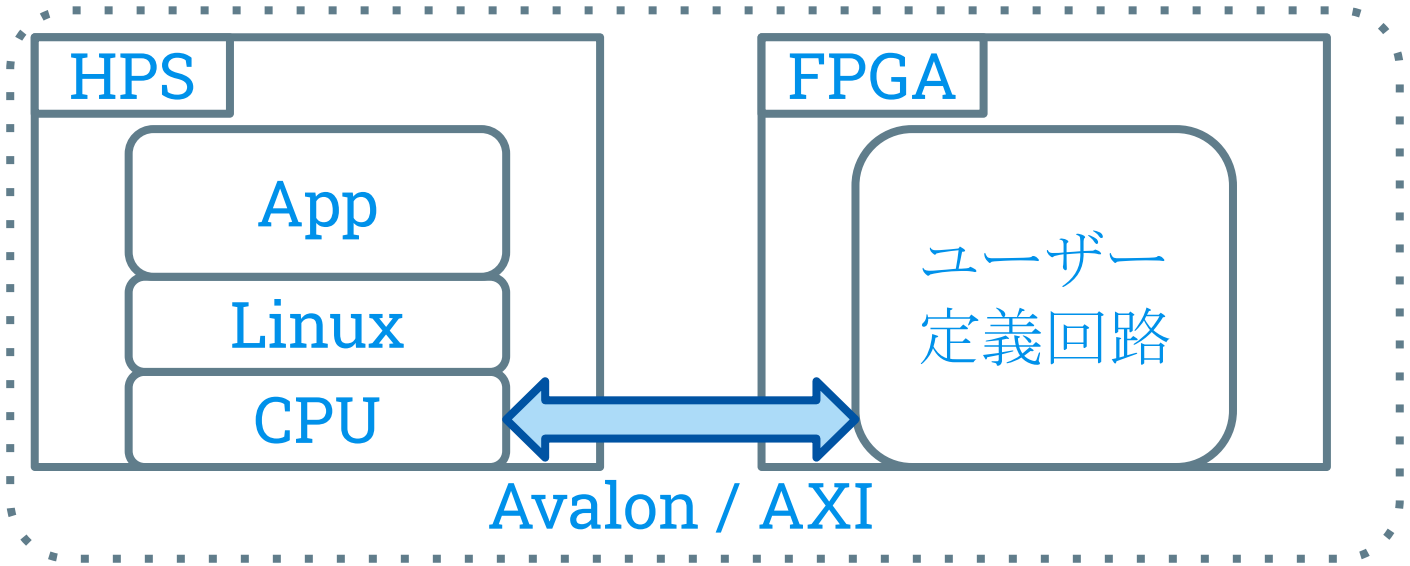
- SoC FPGA：Intel Cyclone® V (ARM Cortex-A9)
- 大きさ:ラズパイより一回り大きい
- 価格:$130
- 周辺機器:GPIO/LED/USB/HDMI/Ethernet など
- SoC FPGAとしてはローエンドな方
  (ハイエンドなボードはPCIeなどで
  サーバーと接続し，データセンター
  等で活躍している)



terasic.com DE10-Nano販売ページから引用

SoC FPGAのアーキテクチャ

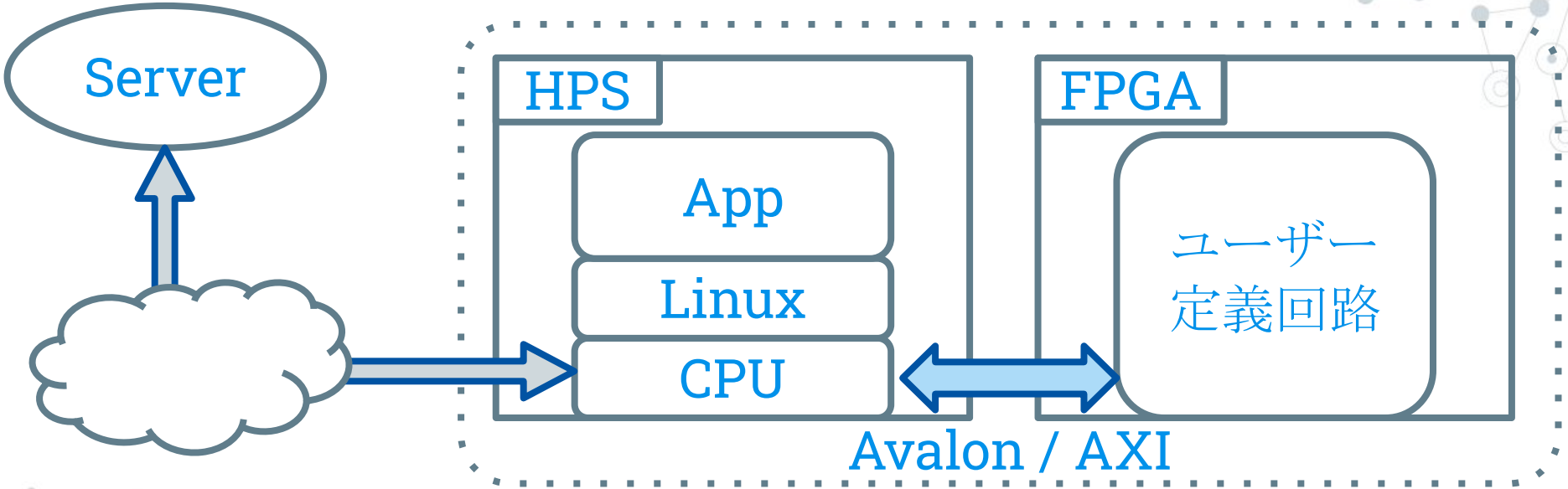
SoC FPGA : HPS + FPGA
HPS : Hard Processor System (CPUとメモリなど周辺システム)



※Linuxが載らない(載せない)場合もあり
※Xilinx社ではHPSでなくPSという名称

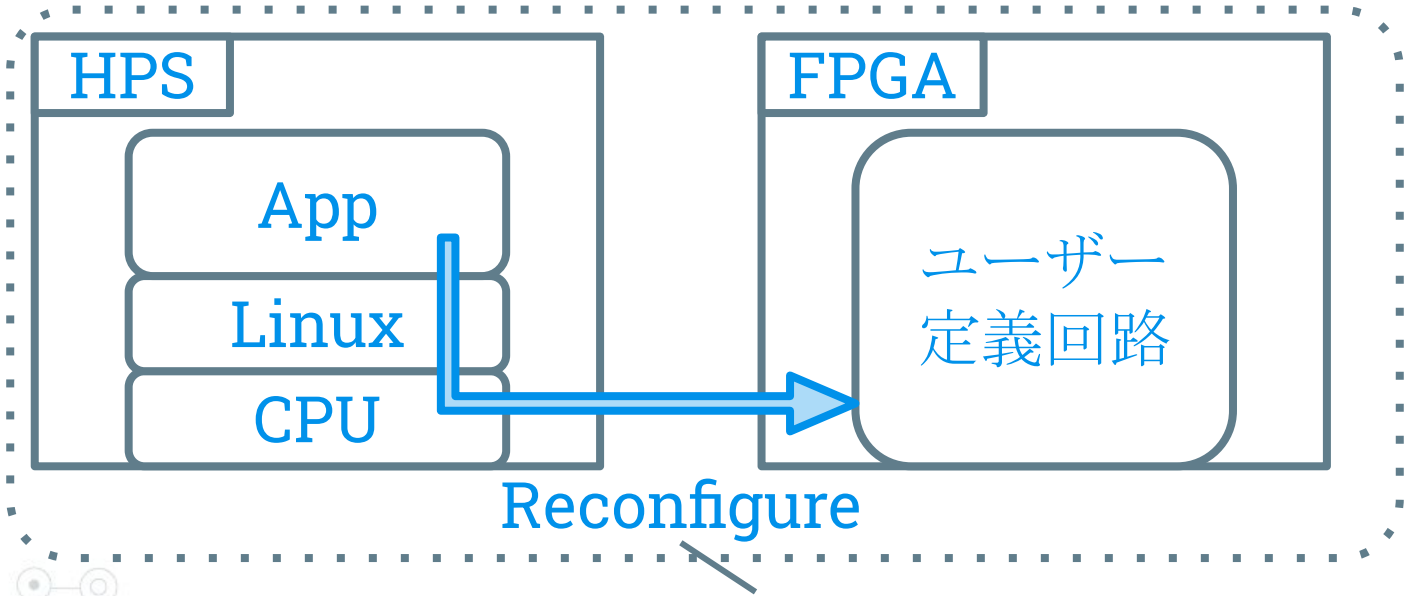
IoT機器としてのSoC FPGA

インターネットに接続し，サーバーと連帯



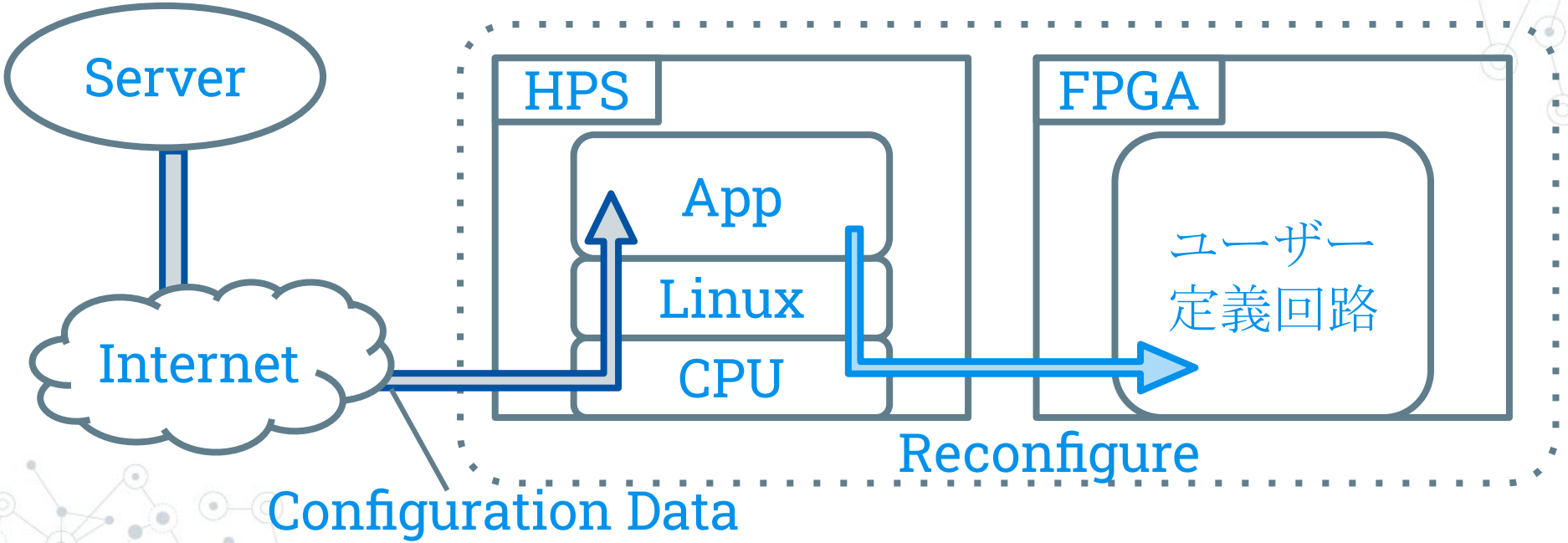
Reconfigurable SystemとしてのSoC FPGA

Linux上のアプリケーションからFPGAをReconfigure
→Linuxからはペリフェラルが置き換わっているように見える



SoC FPGAのRemote Reconfiguration

遠隔から送られるConfiguration DataをLinux上で待ち受けて
FPGAをReconfigure



IoT機器でFPGAが使えると何が嬉しい？

- (上手くHDLを書けば) HWオフローディングによって
  高速で省電力に演算が可能

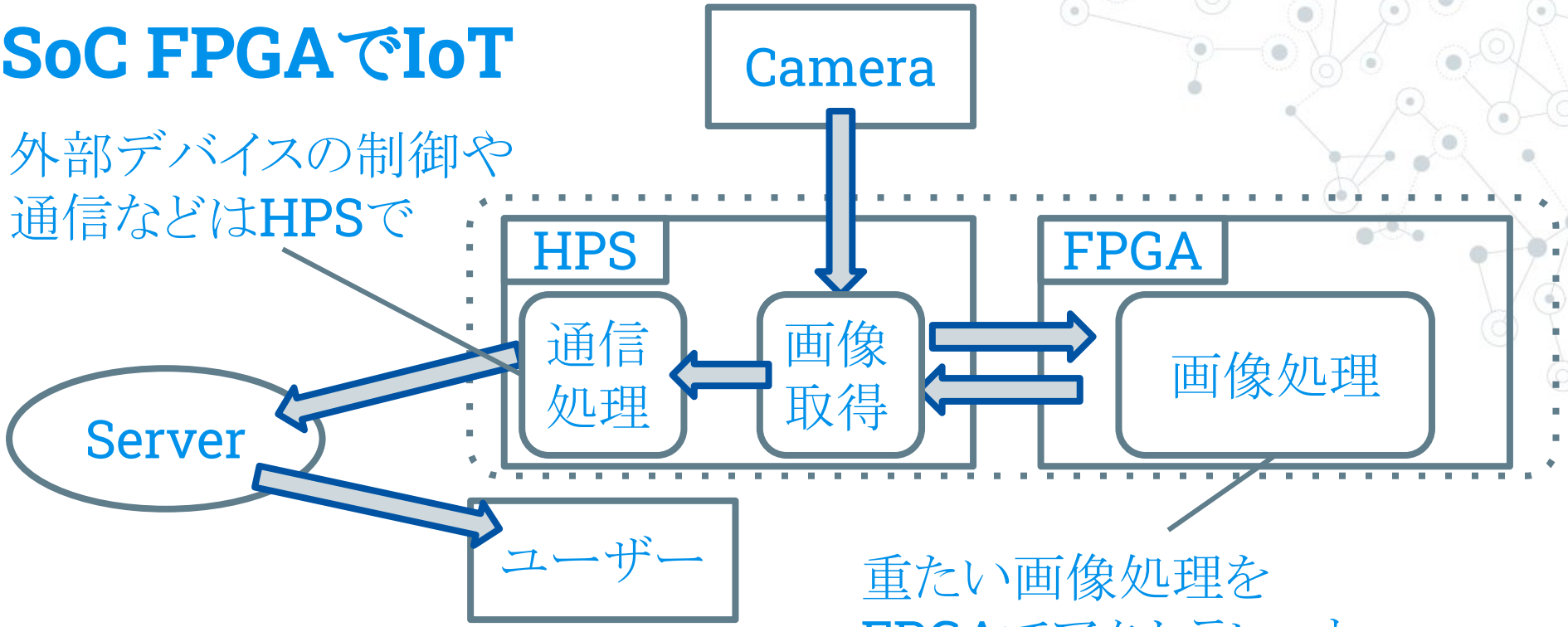
Q. ASIC(専用チップ)でいいんじゃない？
  A. FPGAなら回路が**Reconfigurable！**

Q. GPUでいいんじゃない？
  A. (上手くHDLを書けば) GPUよりも**省電力**に実装可能

Q. HDL書ける人少なくない？
  A. FPGAアクセラレータの**研究は盛ん**.
    HDL人口の増加・便利なフレームワークの登場に期待

SoC FPGAでIoT

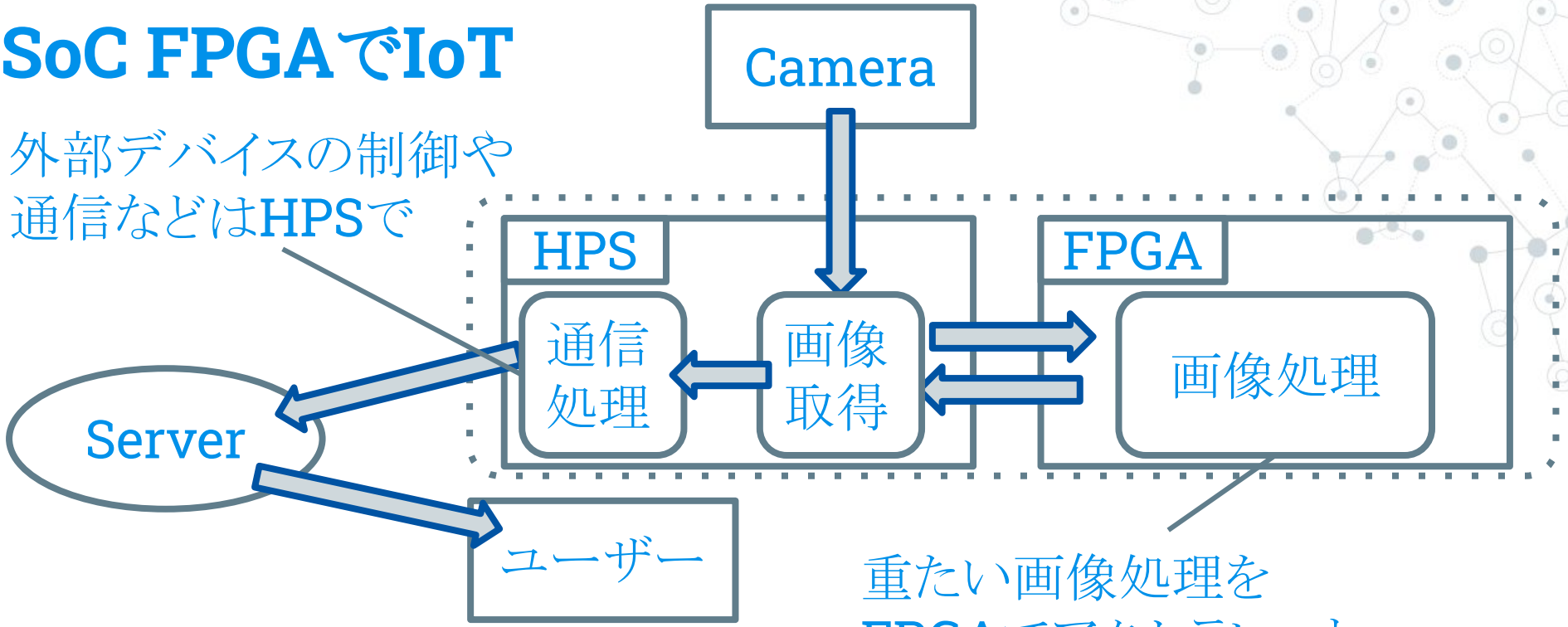
外部デバイスの制御や
通信などはHPSで



重たい画像処理を
FPGAでアクセラレート

SoC FPGAでIoT

外部デバイスの制御や
通信などはHPSで



重たい画像処理を
FPGAでアクセラレート

→高速化・省電力化が見込める
HW化した画像処理部分も更新可能

Remote Reconfigurationに関わる脅威

1. 通信を盗聴され，Configuration Dataを盗まれる.
   → 知的財産権の侵害.

2. 通信が改ざんされ，攻撃者にReconfigureされる.
   → FPGAに任意の回路が実装されるリスク.

Remote Reconfigurationに関わる脅威

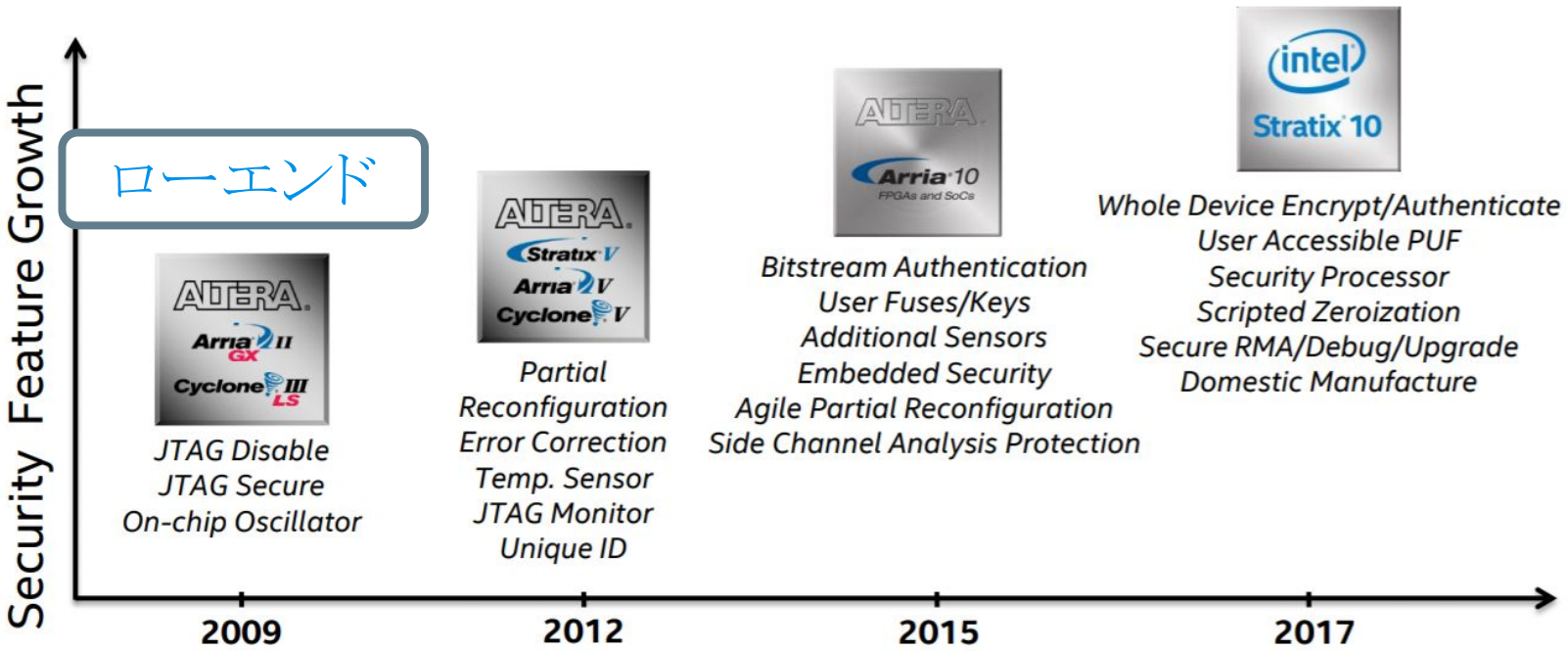
- 既存の対策
  FPGAベンダーごとにセキュリティ機能の提供
  - Intel SoC FPGAの場合
    - デバイスでConfiguration DataをAES復号化
      かつ 復号化したものだけでFPGAをReconfigure
    - コンフィグレーションのリードバックを無効

  など

ベンダーによるセキュリティ機能
(Intel SoC FPGAの場合)

チップによってセキュリティ機能の差が大きい.

ハイエンド

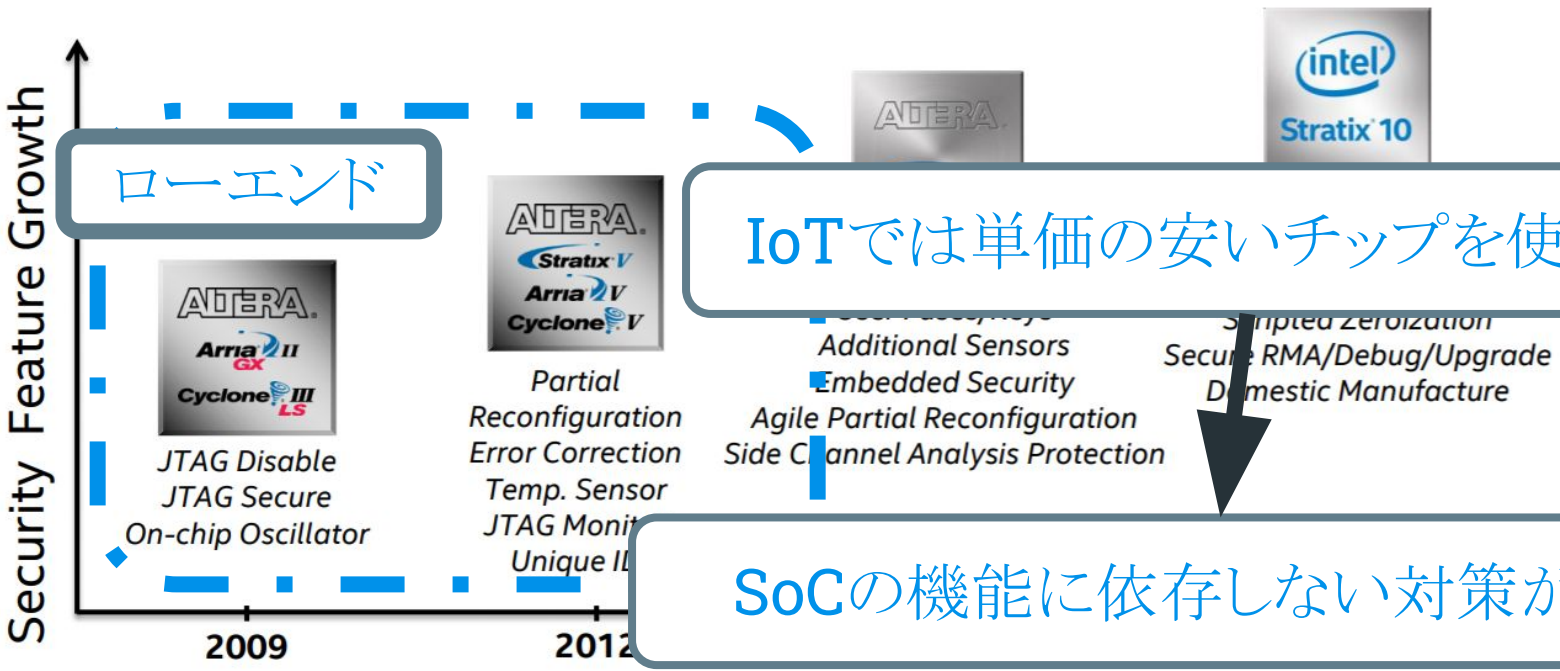


引用: SoC FPGA Hardware Security Requirements and Roadmap Ryan Kenny, Strategic Marketing Intel Programmable Solutions Group

ベンダーによるセキュリティ機能
(Intel SoC FPGAの場合)

チップによってセキュリティ機能の差が大きい.

ハイエンド



IoTでは単価の安いチップを使いたい

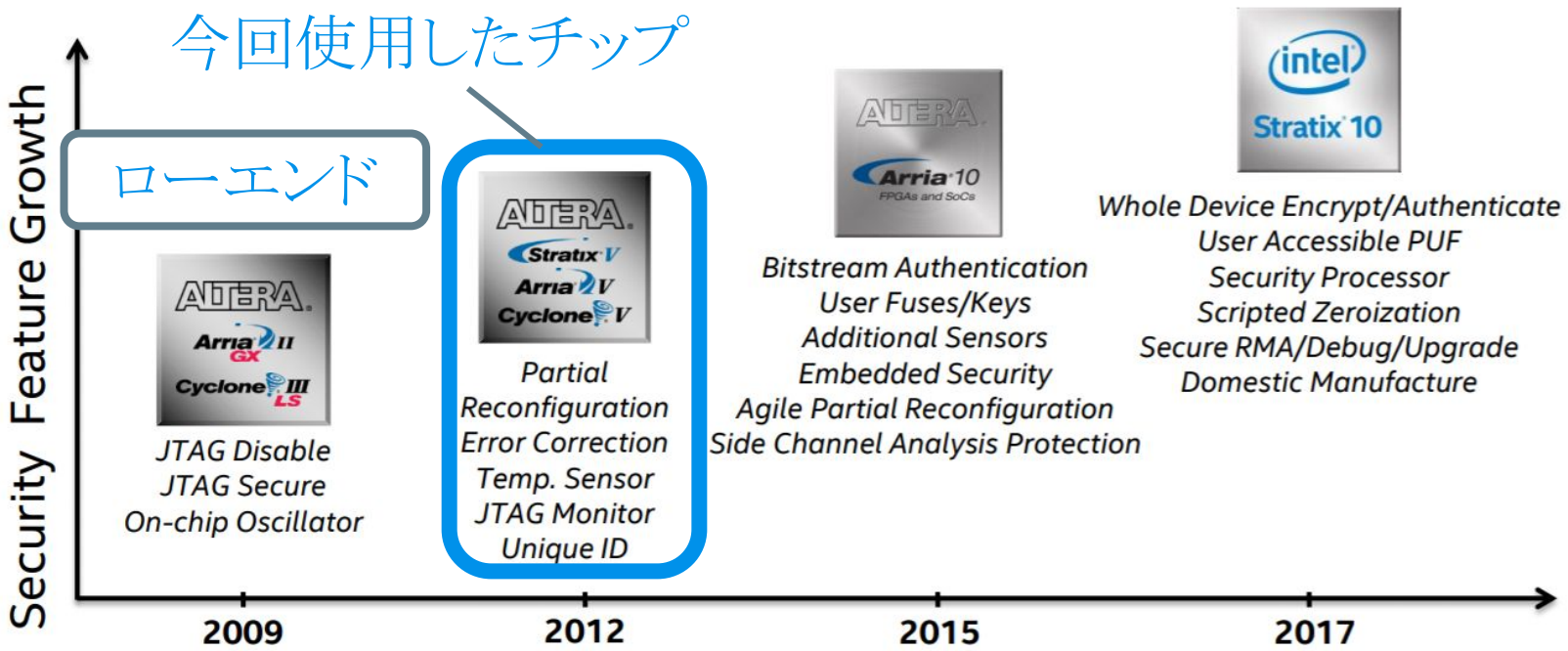
SoCの機能に依存しない対策が必要

引用: SoC FPGA Hardware Security Requirements and Roadmap Ryan Kenny, Strategic Marketing Intel Programmable Solutions Group

ベンダーによるセキュリティ機能
(Intel SoC FPGAの場合)

チップによってセキュリティ機能の差が大きい.

ハイエンド



引用: SoC FPGA Hardware Security Requirements and Roadmap Ryan Kenny, Strategic Marketing Intel Programmable Solutions Group

ベンダーによるセキュリティ機能
(Intel SoC FPGAの場合)

チップによってサポートされている暗号化モードが固定.

表 2. サポートされている Intel® FPGAでのAESモード

FPGA		AESモード
ローエンド	40 nm	カウンターモード (CTR)
	28 nm	暗号ブロックチェーン (CBC)
ハイエンド	20 nm	CTRおよび鍵付きハッシュメッセージ認証コード (HMAC)

引用: AN556: インテル® FPGAにおけるデザイン・セキュリティー機能の使用

ベンダーによるセキュリティ機能の課題
(Intel SoC FPGAの場合)

- ローエンドなSoCに対する対策が(ハイエンドなものと比べて)少ない.
- 特に, Configuration Dataの暗号化モードが固定

- ベンダーによるセキュリティ機能だけでいいか？
  - 単一障害点になりうる？
  - セキュリティ的にベンダーを全面的に信用していいか？
    - いわゆる「ゼロトラスト」な方が安全ではないか

Sereform 開発で目指したもの

- 簡単にSoC FPGAでIoTできるように
- SoC FPGAをネットワークを介した攻撃から保護する
- ベンダーに依存した機能を使わずにセキュリティを高める
- 認証/暗号モジュールはユーザーが自由に選択・拡張できる.

Sereform 開発で目指したもの

・簡単にSoC FPGAでIoTできるように

→Pythonモジュールとして実装(Cライブラリ+SWIG)

・SoC FPGAをネットワークを介した攻撃から保護する

・ベンダーに依存した機能を使わずにセキュリティを高める

→独自にConfiguration Dataを暗号化(FPGAで高速に)

・認証/暗号モジュールはユーザーが自由に選択・拡張できる

→Sereformでは暗号モジュールを提供せず，

暗号モジュールの呼び出しをする，

Sereform 概要

C/C++ 及びPython向けのライブラリとして提供

- Sereform for Desktop (IoT管理者のPCで使う)

  暗号アルゴリズムの管理, 暗号モジュールへ暗号化の依頼

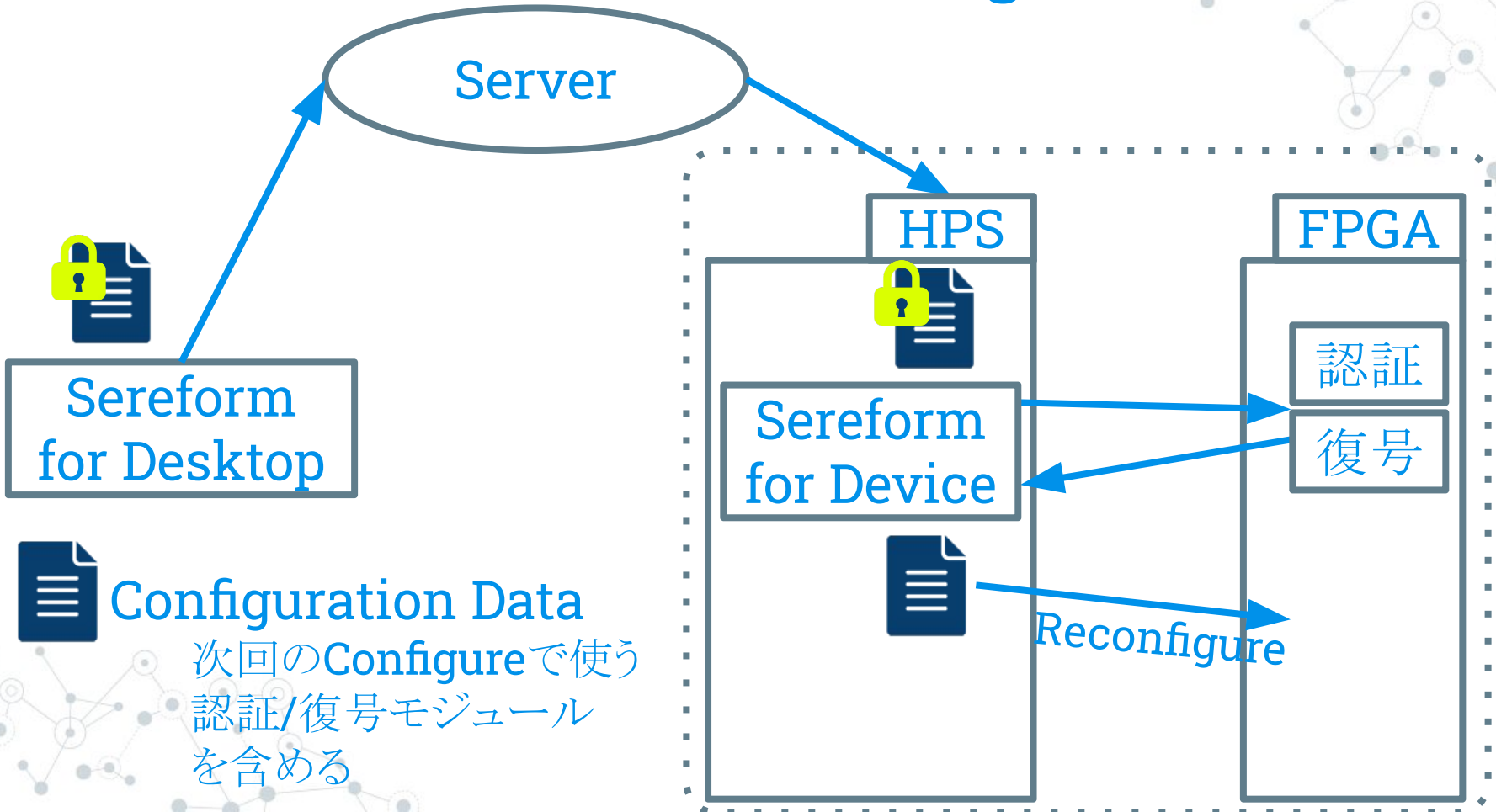
- Sereform for Device (SoC FPGAで使う)

  FPGAへConfiguration Dataの復号化の依頼,

  FPGAのRemote Reconfigureを行う.

通信処理, 暗号化・復号化処理とは分離して開発

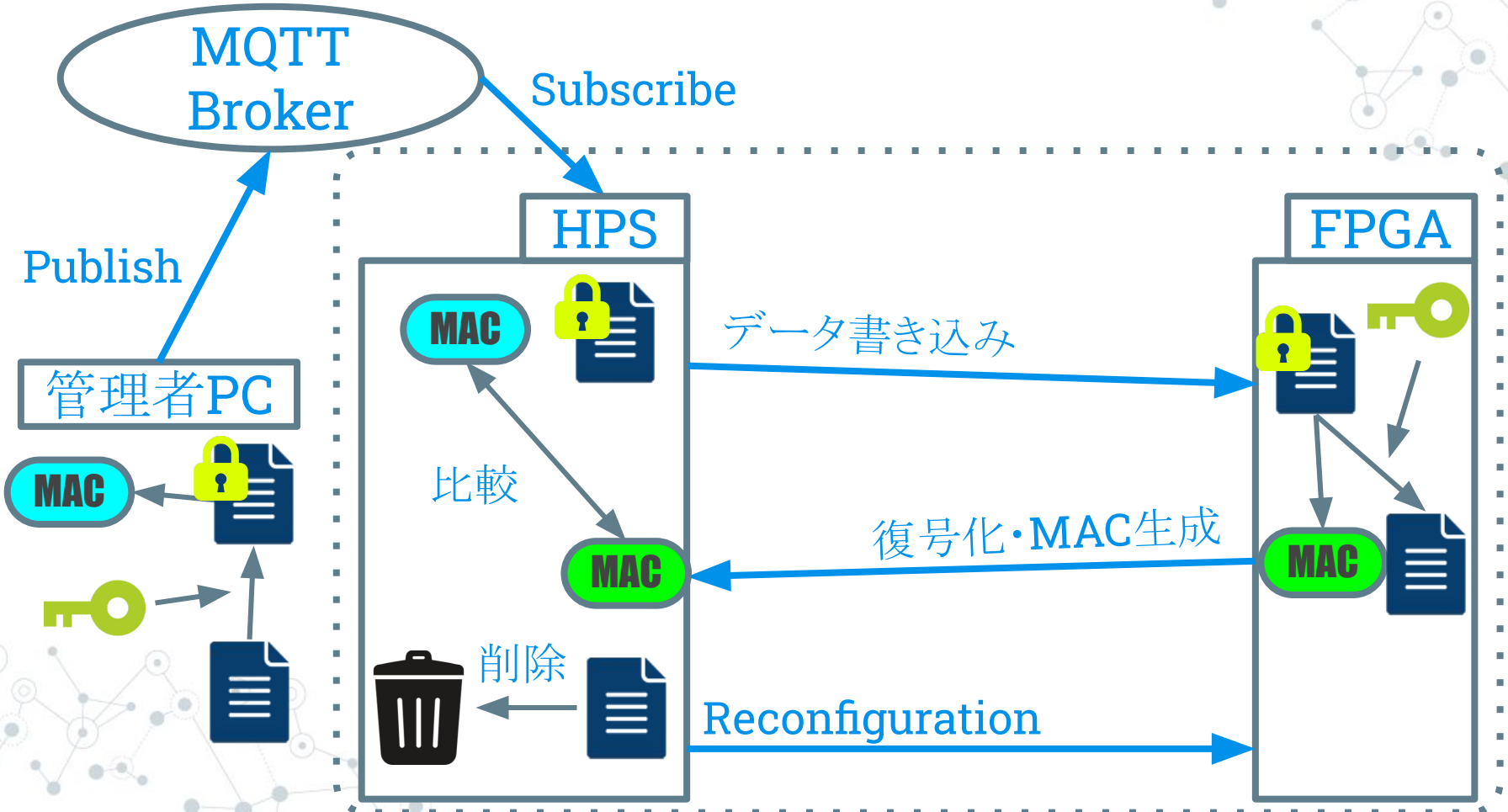
SereformによるRemote Reconfiguration



Configuration Data

次回のConfigureで使う
認証/復号モジュール
を含める

MQTT+AES-GCMでSereformを使う場合



まとめ

- 簡単にセキュアなRemote Reconfigureができる
  C/C++・Pythonライブラリを作成しています.
- 復号化処理をFPGAに実装することで,
  効率的に処理でき, 復号アルゴリズムの更新も可能です
- Sereformはまだまだ開発途中です.

謝辞

今岡工学事務所　今岡 通博さま

情報通信研究機構 / 神戸情報大学院大学　横山 輝明さま

松江高専 情報工学科 4年生　鈴木 豪さま

SecHack365 トレーナー/トレーニー/運営スタッフの皆様

宣伝

3/6に秋葉原にて SecHack365 2019年度成果発表会！！

Sereformの進化にご期待ください！

KAMPPHER

悪意のあるデータ書き換えのハードウェアによる阻止・警報モジュール

↑鈴木くんによるプロジェクトも要チェック！

まとめ

- 簡単にセキュアなRemote Reconfigureができる
  C/C++・Pythonライブラリを作成しています.
- 復号化処理をFPGAに実装することで,
  効率的に処理でき, 復号アルゴリズムの更新も可能です.