

# カスタマイズ可能なネットワーク型IDPSをFPGA実装するためのソフトウェア — FPGAのためのアプリケーションと基盤 —

中岡典弘(愛媛大学大学院)

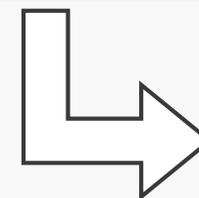
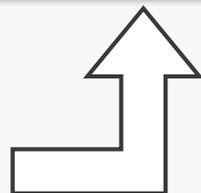
誰かのFPGAを利用したアプリケーションが自分のFPGAボードで再現しようとして容易に再現できなかったという経験がある。

誰かが開発したFPGAアプリケーションを自分のFPGAボードで再現するための基盤としてFCOMPOSE、MANTAを開発した。

また、FPGA本来のリコンフィギュラブル性が伝わるように、本基盤を通してカスタマイズ可能なネットワーク型IDSを提供するFS-NIDSなどのFPGAアプリケーションを開発した。



開発者



利用者

# 誰かが開発したFPGAアプリケーションを自分のFPGAボードで再現する

- FCOMPOSE  
複数FPGAボードに対応・再現しやすい  
FPGAアプリケーションのテンプレートを作成

```
MANTA/apps/blink on master [!] via MANTA via system
→ fcompose apply require.yml
loading require.yml ... OK
project ... blink
target vendor ... xilinx, intel
using module ... LED0, LED1, LED2, LED3
generate template directory ... DONE
generate setup.py, setup.cfg, scripts/blink ... DONE
generate constraints ... xilinx/art7-a7-100, xilinx/zedboard, xilinx/zybo-z7-20, intel/d
e0-cv, intel/de10-nano
generate template topmodule ... blink/xilinx/hdl/blink.v, blink/intel/hdl/blink.v
generate template tcl files ... DONE
generate config.yml for project ... DONE

usage: blink [-h] [--version] {list,apply} ...

blink

positional arguments:
  {list,apply}

optional arguments:
  -h, --help            show this help message and exit
  --version             show program's version number and exit
```

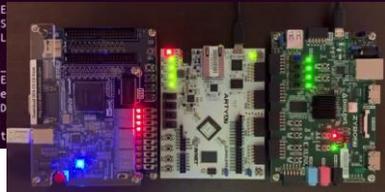
- MANTA  
FPGAアプリ  
ケーションを管理

```
MANTA on master [!] via MANTA via system
→ manta install blink
git clone blink:master...
Installing ./apps/blink...
Adding blink to Pipfile's [packages]...
✓ Installation Succeeded
Pipfile.lock (af015b) out of date, updating to (169f75)...
Locking [main packages] dependencies...
✓ Success!
Locking [packages] dependencies...
✓ Success!
Updated Pipfile.lock (af015b)
Installing dependencies from Pipfile.lock (af015b)...
MANTA on master [!] via MANTA via system took 25s
→ manta list
Name URL Install Status
blink https://github.com/MaineK00n/blink Installed
mitou https://github.com/MaineK00n/mitou
fs-nids https://github.com/MaineK00n/fs-nids
```

- Blink  
Lチカアプリケーション

```
→ blink apply config.yml
***** Vivado v2019.1 (64-bit)
**** SW Build 2552052 on Fri May 24 14:47:09 MDT 2019
**** IP Build 2548770 on Fri May 24 18:01:18 MDT 2019
** Copyright 1986-2019 Xilinx, Inc. All Rights Reserved.

# set_property PROBES.FILE
# set_property FULL_PROBES
# set_property PROGRAM.FILE
link.bit) [get_hw_devices
program_hw_devices [get
INFO: [Labtools 27-3164] E
# refresh_hw_device [line
INFO: [Labtools 27-1434] D
lgn that has no supported
INFO: [Common 17-206] Exit
```



- FS-NIDS  
カスタマイズ可能なネットワーク型IDS

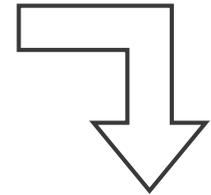
Wireshark

http.request.methodが  
"POST"であるパケットを  
表示

FS-NIDS  
Board: DE10-Nano  
TCPパケットでパケット内に  
"POST"が含まれるものを表示

FS-NIDS  
Board: Zybo Z7-20  
TCPパケットでパケット内に  
"uid=root"か  
"password=password"  
が含まれるものを表示

カスタマイズできる  
シグネチャで  
パケットを検出



Capturing from enp9s0

File Edit View Search Terminal Help

Content-Type: application/x-www-urlencoded.  
Content-Length: 24.  
Origin: http://192.168.11.16/  
Connection: keep-alive.  
Referer: http://192.168.11.16/Index.html.  
Upgrade-Insecure-Requests: 1.  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:72.0) Gecko/20100101 Firefox/72.0

uid=fuga&password=123456

T 192.168.11.26:53296 -> 192.168.11.16:80  
POST /db.php HTTP/1.1.  
Host: 192.168.11.16.  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:72.0) Gecko/20100101 Firefox/72.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8.  
Accept-Encoding: gzip, deflate.  
Content-Type: application/x-www-urlencoded.  
Content-Length: 22.  
Origin: http://192.168.11.16.  
Connection: keep-alive.  
Referer: http://192.168.11.16/Index.html.  
Upgrade-Insecure-Requests: 1.  
uid=root&password=root

File Edit View Search Terminal Help

Interface: Zybo Z7-20  
tcp any any -> 192.168.11.16 80 (content: "uid=root");  
tcp any any -> 192.168.11.16 80 (content: "password=password");

T 192.168.11.26:53296 -> 192.168.11.16:80  
POST /db.php HTTP/1.1.  
Host: 192.168.11.16.  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:72.0) Gecko/20100101 Firefox/72.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8.  
Accept-Language: ja.  
Accept-Encoding: gzip, deflate.  
Content-Type: application/x-www-urlencoded.  
Content-Length: 22.  
Origin: http://192.168.11.16.  
Connection: keep-alive.  
Referer: http://192.168.11.16/Index.html.  
Upgrade-Insecure-Requests: 1.  
uid=root&password=root

Text item (hex), 13 bytes

Packets: 430 - Displayed: 2 (0.5%) Profile: Default