

# IETF101 London ハッカソン報告

鈴木 未央 <[mio@nict.go.jp](mailto:mio@nict.go.jp)>

サイバーセキュリティ研究室 / NICT

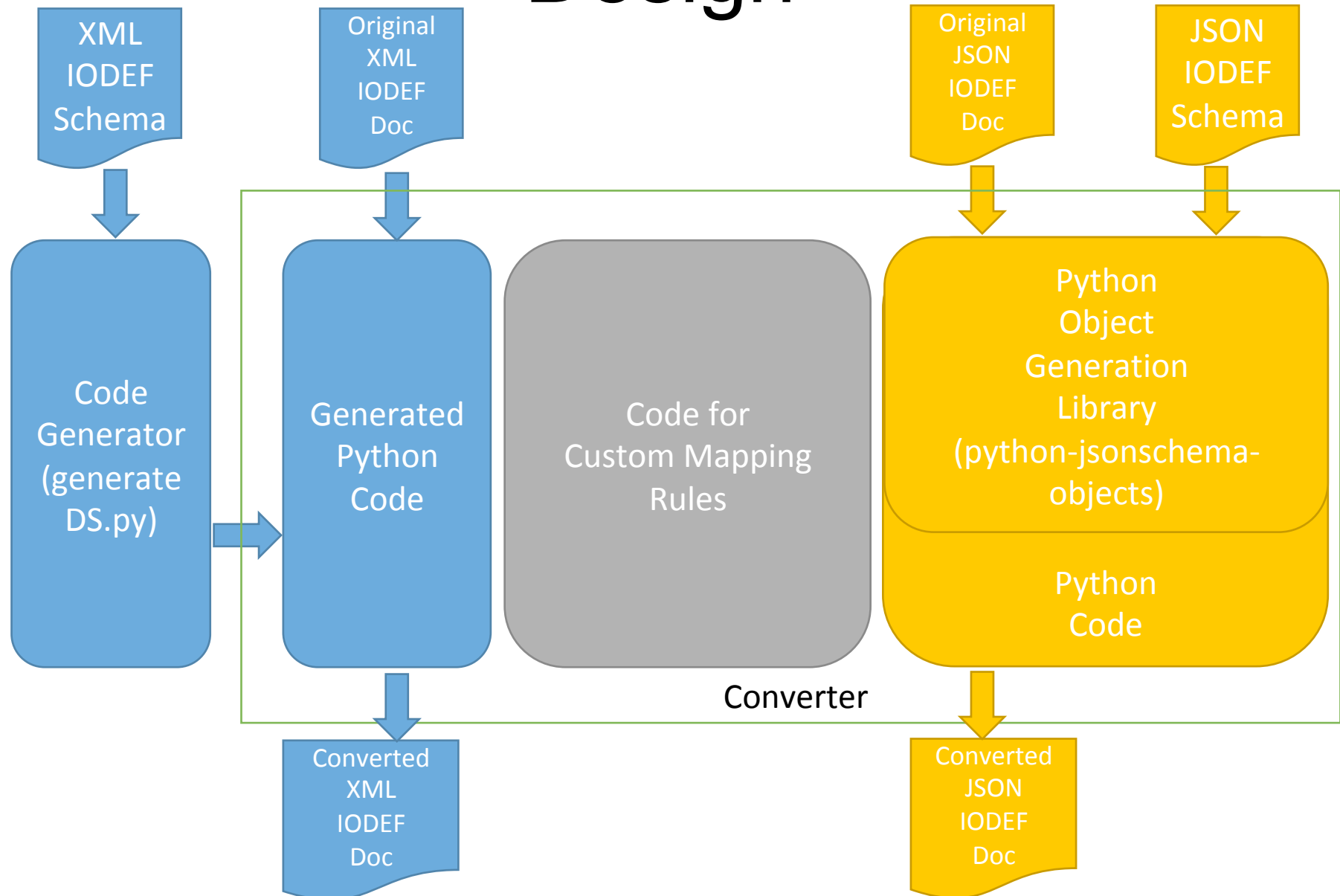
# 自己紹介

- 鈴木 未央 (すずき みお)
- NICT サイバーセキュリティ研究室  
主任研究技術員
- IETF では主にセキュリティ界隈で活動
  - mile(Managed Incident Lightweight Exchange) WG とか
- これまでの活動歴
  - RFC8274 Incident Object Description Exchange Format Usage Guidance
  - draft-ietf-mile-jsoniodef JSON binding of IODEF

# mile Hackathon: Converter Overview

- Aiming to convert from JSON IODEF document to XML IODEF document, and vice versa
- Running code for latest JSON IODEF draft (draft-ietf-mile-jsoniodef-03)
- I'm currently implementing the converter including IETF Hackathon days in London

# mile Hackathon: Converter Design



# mile Hackathon: Problems

- Object generator(python-jsonschema-objects) makes errors caused by self reference recursions
  - On “Contact”, “EventData”, and “IndicatorExpression” in IODEF JSON schema
  - Originated from IODEF XML Schema
  - Problem of implementation of python-jsonschema-objects?
  - It could cause errors on other generators/validators
- Related JSON schema snippet is described below

```
"Contact": {
```

(snip)

```
    "Contact": {  
        "type": "array", "items": {"$ref": "#/definitions/Contact"}},
```

(snip)

```
"EventData": {
```

(snip)

```
    "EventData": {  
        "type": "array", "items": {"$ref": "#/definitions/EventData"}},
```

# 他プロジェクト紹介: DNS

- DoH(DNS over HTTPS) Interop
  - draft-ietf-doh-dns-over-https

## What got done: DoH

Work in Progress: More details in the [DOH branch of the IETF GitHub repo](#)

Language	Code	Client	Server	Who
C	<a href="#">getdns</a>	Y		Willem Toorop
Go	<a href="#">Go DNS</a> <a href="#">CoreDNS</a>	-	-	Miek Gieben
Python/C	<a href="#">github</a>	Y	Y	Stéphane Bortzmeyer
Python	<a href="#">github</a>	Y	Y	Manu Bretelle
nginx + Lua	<a href="#">github</a>		Y	Tony Finch
C + PHP	<a href="#">github</a>	Y	Y	Massimiliano Fantuzzi
Javascript	<a href="#">github</a>	Y		Tom Puseteri
Python	<a href="#">Test System</a>	-	-	Manu Bretelle

[出展: https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/DNS\\_DOH\\_presentation.pdf](https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/DNS_DOH_presentation.pdf)

# 他プロジェクト紹介: SUIT

- SUIT: Software Updates for Internet of Things
- **Input to the recently formed SUIT WG**
- Creating signed manifest
  - Encoded in CBOR
  - COSE signed with ECDSA.
- Manifest & firmware transport to IoT board via UART.
- Bootloader verifies received manifest and installs new firmware.



K64F

Firmware + Manifest

←  
Via UART

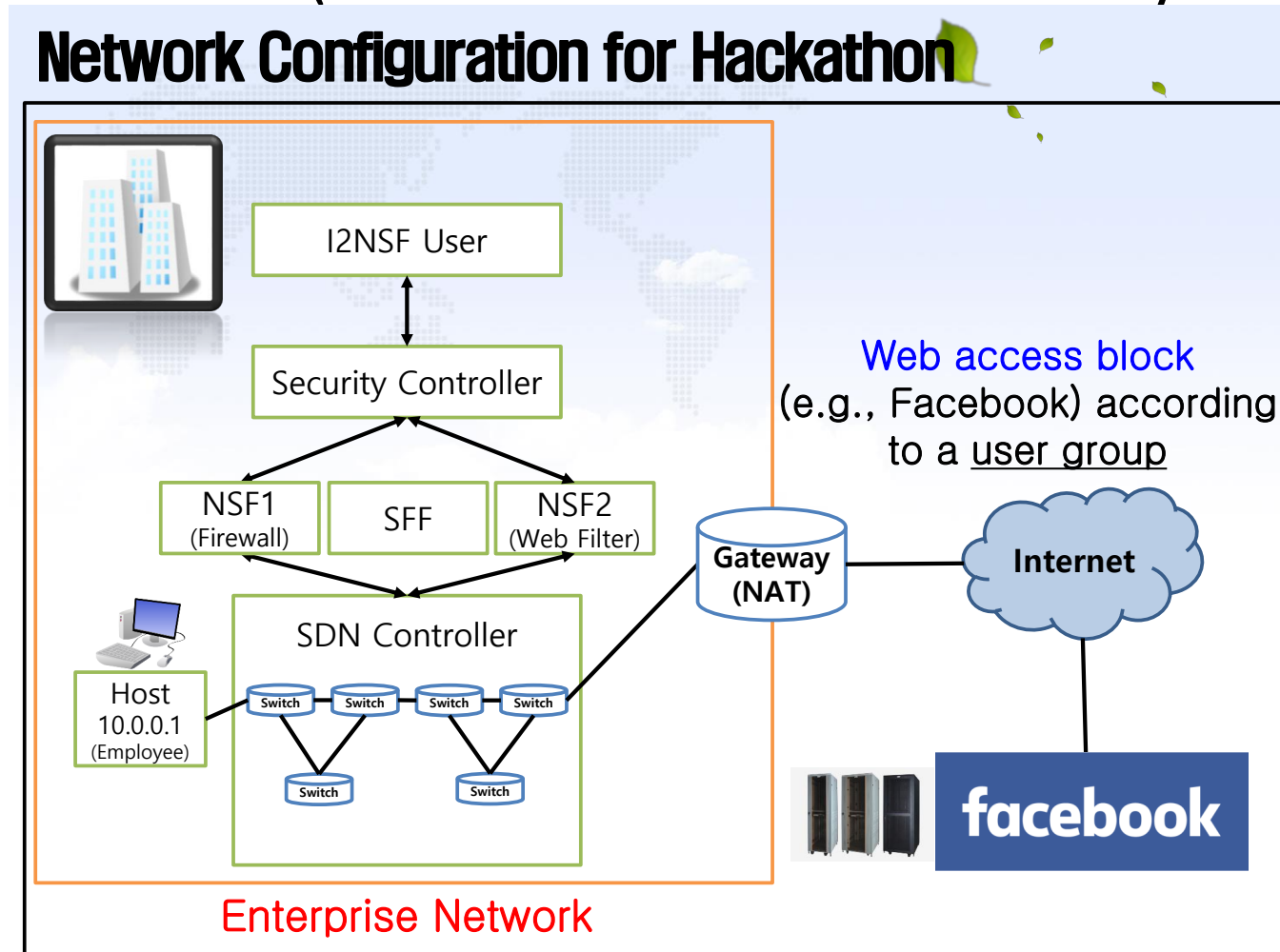
```
|0100 01101000 01100101 00  
|0100 01110101 01110100 01  
|0010 01101001 01100001 01  
)0000 01110100 01101111 00  
)1100 01100101 01100001 01  
)1110 00100000 01100010 01  
)1110 01100001 01110010 01  
)1110 00100000 01010001 00  
)1000 01101111 011  
)0000 01111001 011
```



[出展: https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/IETF101-SUIT-Hackathon.pptx](https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/IETF101-SUIT-Hackathon.pptx)

# 他プロジェクト紹介: I2NFS

- PoC of I2NSF(Interface to Network Security Function)



出展: <https://github.com/IETF-Hackathon/ietf101-project-presentations/blob/master/IETF101-I2NSF-Hackathon.pdf>