

IoTデバイスへの攻撃予兆を監視するための IoTセキュリティ国際標準の策定

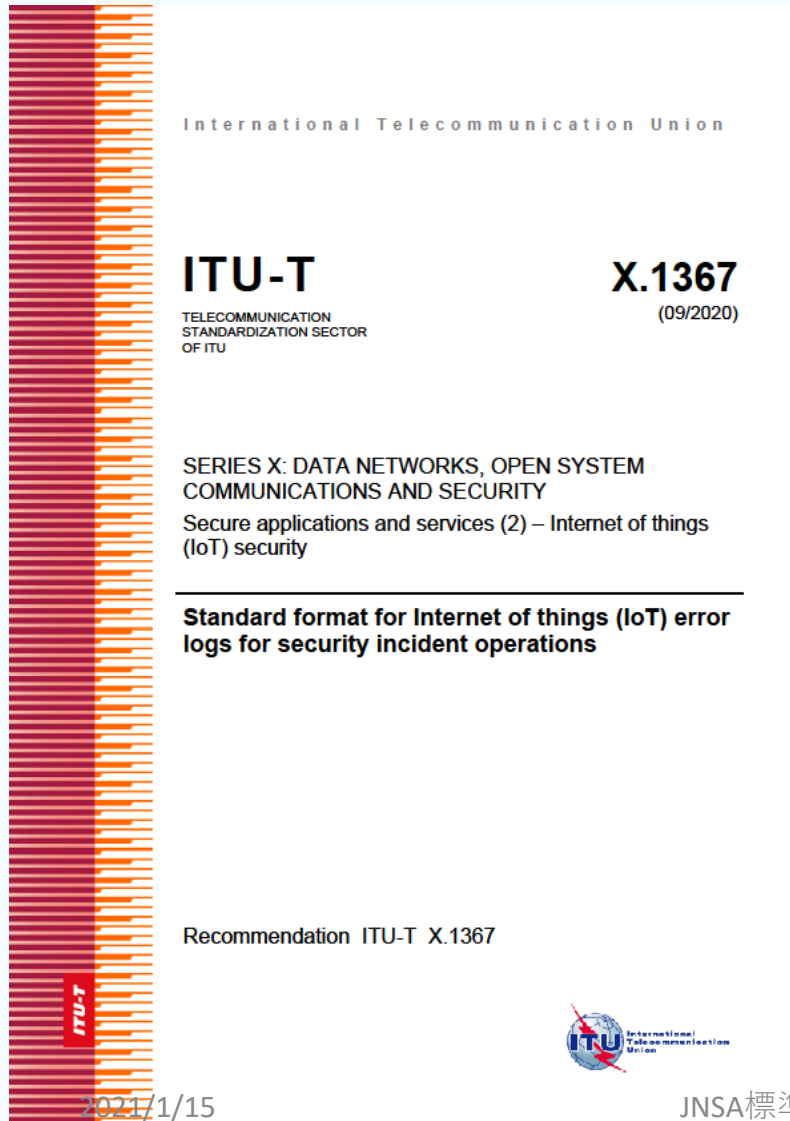
2021年1月15日

(旧)標準化部会IoT機器セキュリティログ検討WG

合同会社もっけ技研

渥美 清隆

祝！X.1367(X.elf-iot)発行



<https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14263>



- X.1367 (X.elf-iot) の概要
- なぜ標準化が必要なのか？
- 期待される利用例
- 発行までの経緯と今後について

- X.1367 (X.elf-iot) の概要
- なぜ標準化が必要なのか？
- 期待される利用例
- 発行までの経緯と今後について

- 以下の2点を定義
 - IoTエッジデバイス用の標準化されたエラーコード
 - Logサーバに送信するためのJSON形式のエラーレコード
- 想定される利用例の提示

X.1367 (X.elf-iot) の概要

標準化されたエラーコード

Table A.1 – Error code and error message

Code	Message	Description
	No Error (0x00-0x0F)	
0x00	No Error	No error occurs.
	Communication (0x10-0x1F)	
0x10	No Response	No response even though the request requires any responses.
0x11	Communication Failed	Some problems for failing communication.
0x12	Link Down	A network interface link is down.
0x1E	Extended Reasons	Prefix code for extended reasons.
0x1F	Other Communication Reasons	Other reasons related to communication.
	Security (0x20-0x2F)	
0x20	Authentication Failed	Some problems of the authentication.
0x21	Certification Failed	Some problems of the certification.
0x22	Encryption Failed	Some problems of the encryption.
0x23	Authorization Failed	Some problems of the authorization.

以下、0xFFまで続く

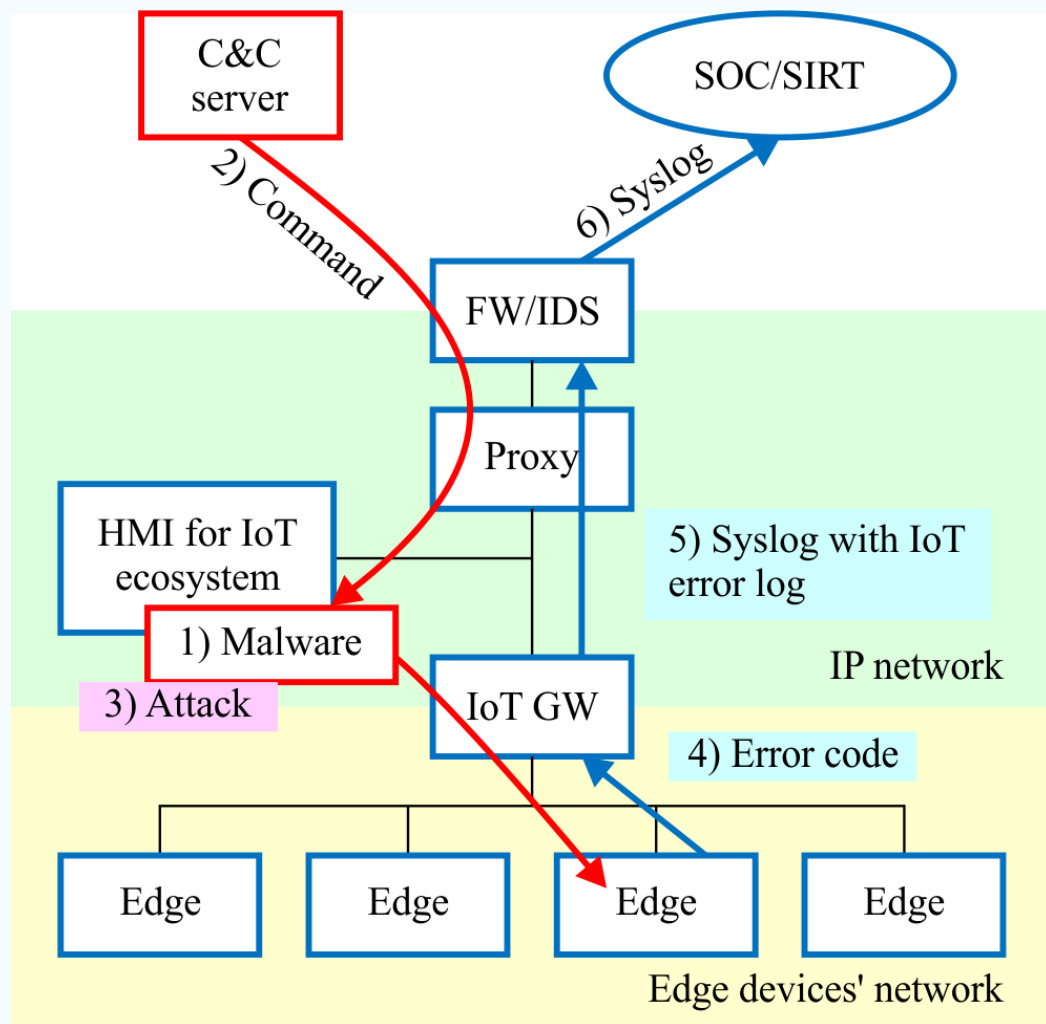
X.1367 (X.elf-iot) の概要

JSON形式のエラーレコード

- 基本構造
- この他に装置識別子の表現を定義

```
{
  "Timestamp":
    "^[0-9]{4})-(1[0-2]|0[1-9])-(3[01]|0[1-9]|12)[0-9])T
      (2[0-3]|01)[0-9]):([0-5][0-9]):([0-5][0-9])(¥.[0-9]{+})Z$",
  "Reporter": {},
  "Protocol": String,
  "Requester": {},
  "Responder": {},
  "Error Code": "/^[0-9A-F]^{+}$/",
  "Error Message": String,
  "Description": String | {},
}
```

X.1367 (X.elf-iot) の概要 利用例



以下のことが記載されている。

- どのような状況が改善されるか
- どのように機能するか

- X.1367 (X.elf-iot) の概要
- なぜ標準化が必要なのか？
- 期待される利用例
- 発行までの経緯と今後について

なぜ標準化が必要なのか？

- SOC/SIRTはログを分析し、攻撃兆候を検知する。
- ログにないイベントからは攻撃を検知できない。
 - IoTエコシステムの管理とネットワークがバラバラ
 - 自社SOCなら監視可能も、委託SOCは困難
 - IoTエッジデバイスの通信はIPとは限らず
 - IPアドレス以外の識別子
 - エッジデバイスの識別困難
 - エラー発生コンテキストが不明
- エラーコードの意味が不明、製品間のエラーコードが互換性なし
 - 数バイト程度の製品固有のエラーコード
 - 同一メーカーでも製品間のエラーコードの互換性保証なし

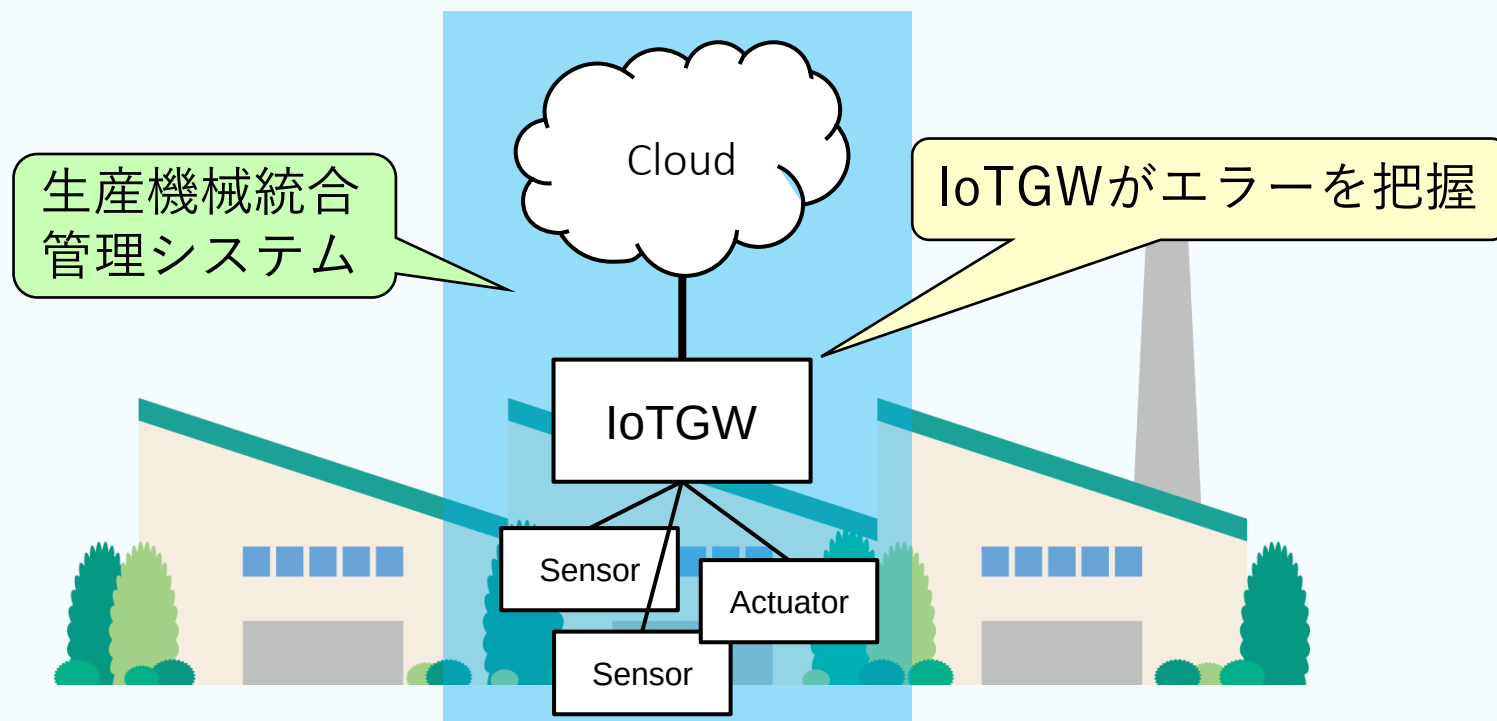
なぜ標準化が必要なのか？ 課題の背景

工場のIoT化の例



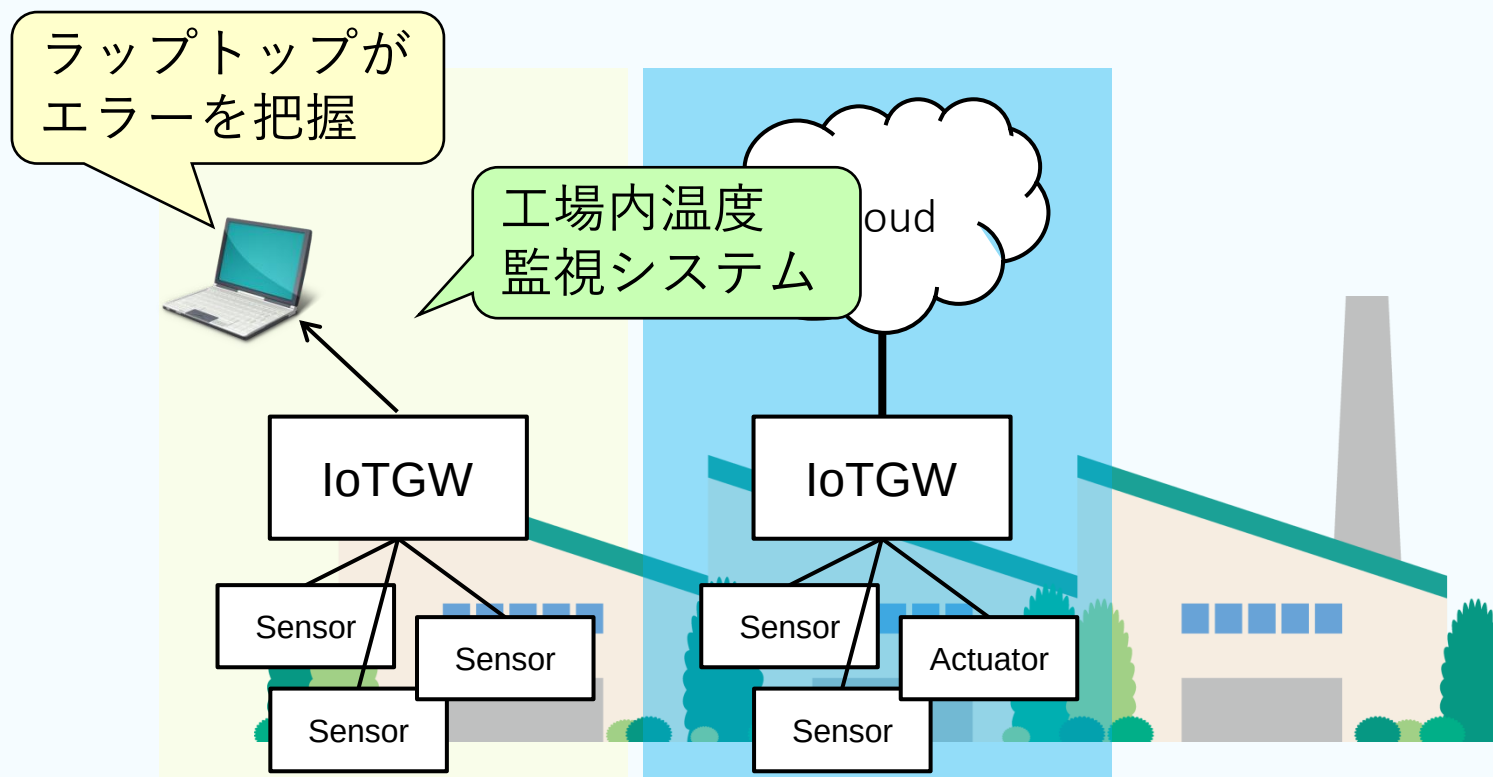
なぜ標準化が必要なのか？ 課題の背景

●A社が1つ目のIoTエコシステム導入



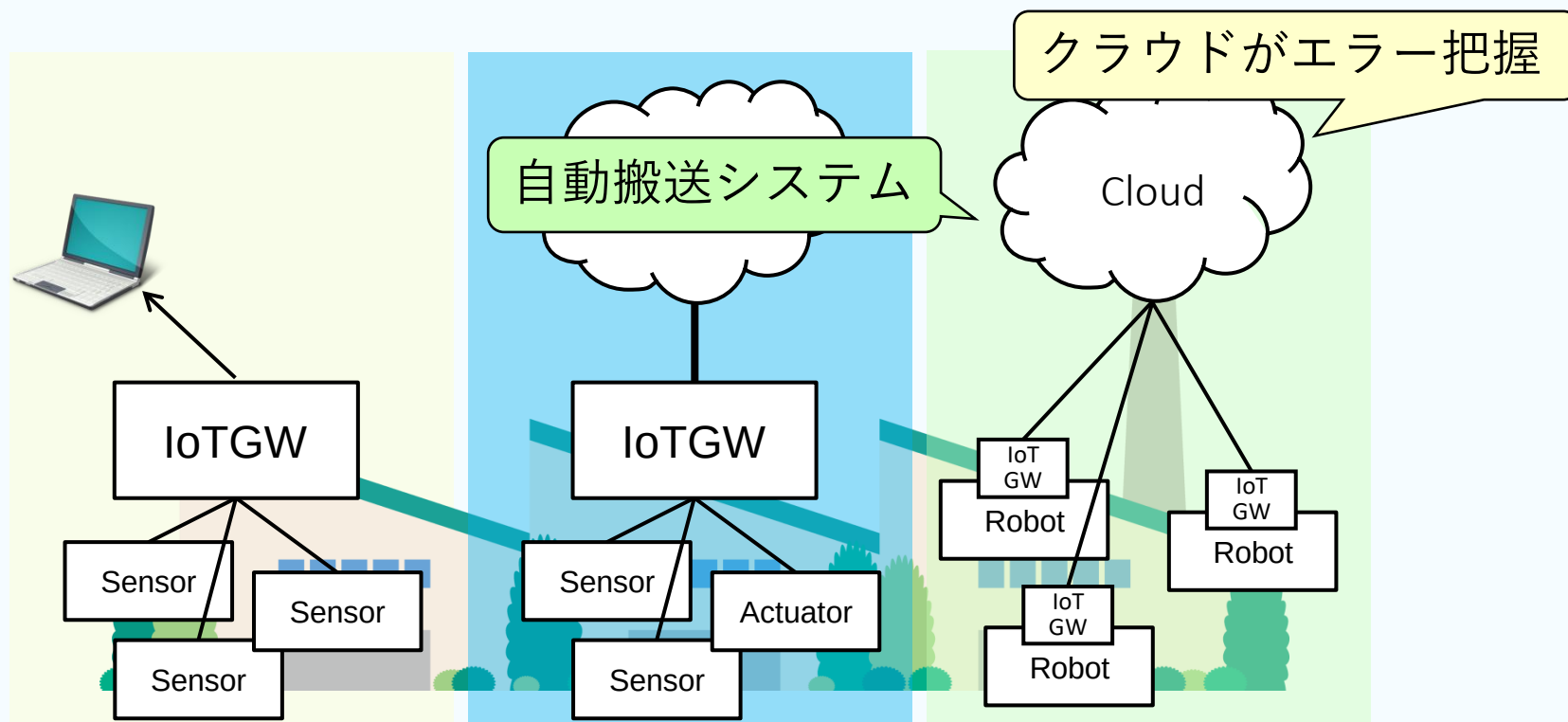
なぜ標準化が必要なのか？ 課題の背景

- A社が1つ目のIoTエコシステム導入
- B社が2つ目のIoTエコシステム導入



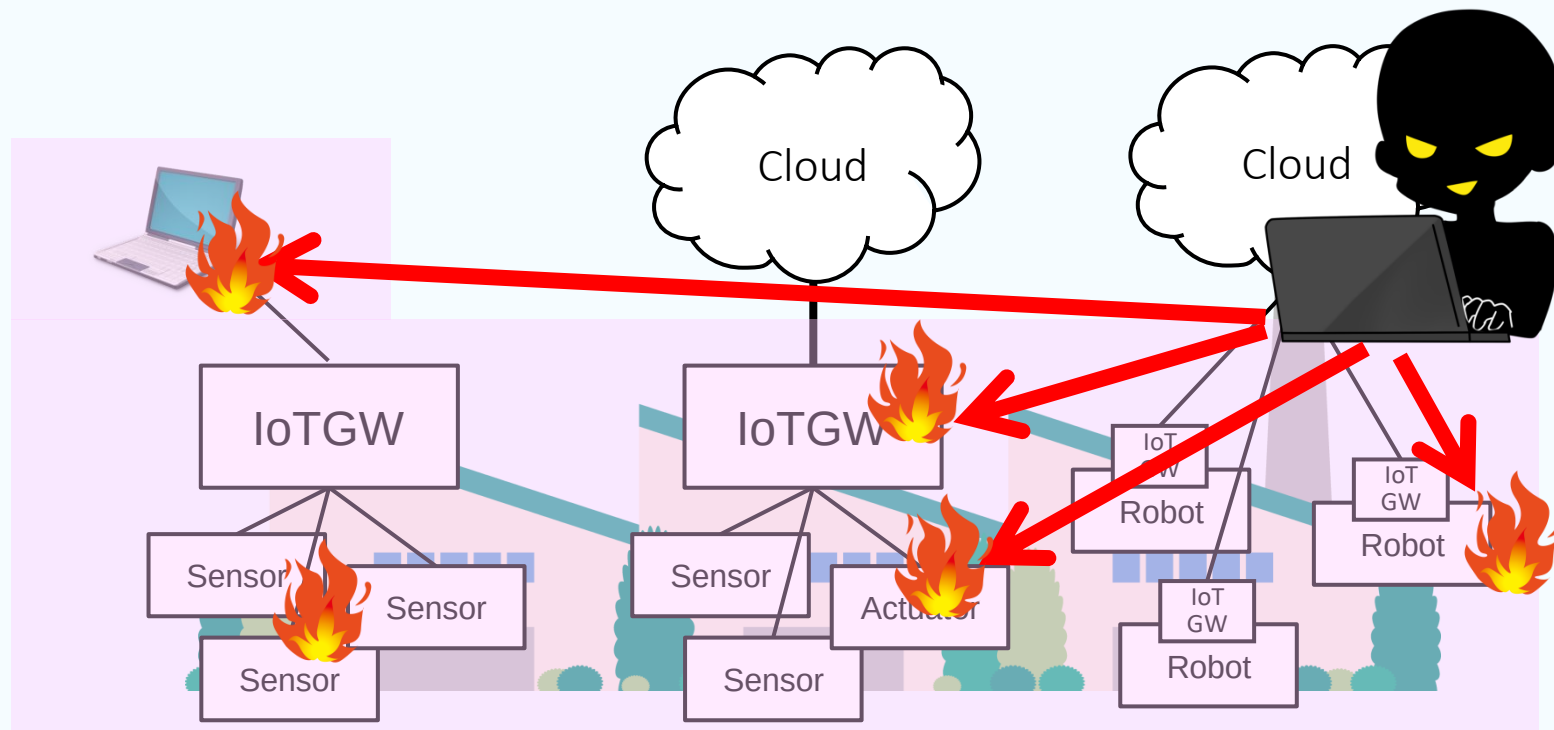
なぜ標準化が必要なのか？ 課題の背景

- A社が1つ目のIoTエコシステム導入
- B社が2つ目のIoTエコシステム導入
- C社が3つ目のIoTエコシステム導入



なぜ標準化が必要なのか？ 課題の背景

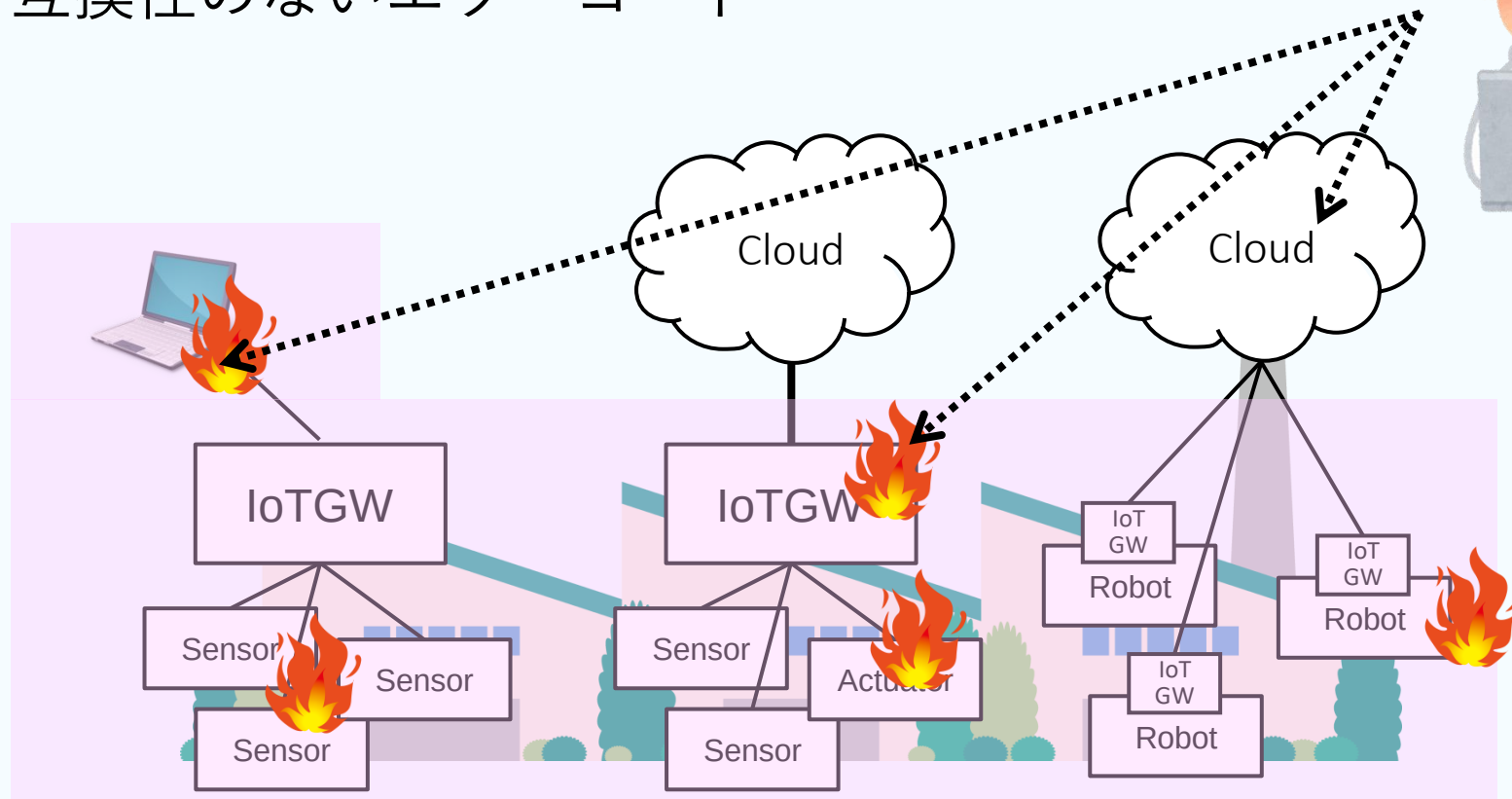
攻撃者は工場内LANから攻撃開始・水平展開



なぜ標準化が必要なのか？ 課題の背景

攻撃の分析が困難

- ばらばらに置かれたログ
- 互換性のないエラーコード



なぜ標準化が必要なのか？

- SOC/SIRTはログを分析し、攻撃兆候を発見する。
- ログにないイベントからは攻撃を検知できない。
 - IoTエコシステムの管理とネットワークがバラバラ
 - 自社SOCなら監視可能も、委託SOCは困難
 - IoTエッジデバイスの通信はIPとは限らず

統合するエラーログ形式の標準化

- エラーコードの意味が不明、製品間のエラーコードが互換性なし
 - エラーコードの抽象化・標準化

なぜ標準化が必要なのか？

標準化されたエラーコード(再掲)

Table A.1 – Error code and error message

Code	Message	Description
	No Error (0x00-0x0F)	
0x00	No Error	No error occurs.
	Communication (0x10-0x1F)	
0x10	No Response	No response even though the request requires any responses.
0x11	Communication Failed	Some problems for failing communication.
0x12	Link Down	A network interface link is down.
0x1E	Extended Reasons	Prefix code for extended reasons.
0x1F	Other Communication Reasons	Other reasons related to communication.
	Security (0x20-0x2F)	
0x20	Authentication Failed	Some problems of the authentication.
0x21	Certification Failed	Some problems of the certification.
0x22	Encryption Failed	Some problems of the encryption.
0x23	Authorization Failed	Some problems of the authorization.

以下、0xFFまで続く

なぜ標準化が必要なのか？ IoTGW等が持つべきコード変換表

このような変換表をIoTGW等で保持することを期待

メーカー固有 コード	説明	X.1367 エラーコード	説明
01 FF	Communication Timeout.	10	No response
...	...	...	...
03 E0 F2 5E	The certification is out of date.	21	Certification failed
...	...	...	...
5E 31	The command cannot accept in this status.	30	Invalid Command
...	...	...	

なぜ標準化が必要なのか？

JSON形式のエラーレコード(再掲)

- 基本構造。
- この他に装置識別子の表現を定義。

```
{
  "Timestamp":
    "^( [0-9]{4} ) - ( 1[0-2] | 0[1-9] ) - ( 3[01] | 0[1-9] | [12] [0-9] ) T
      ( 2[0-3] | [01] [0-9] ) : ( [0-5] [0-9] ) : ( [0-5] [0-9] ) ( ¥ . [0-9]{+} ) Z $ ",
  "Reporter": {},
  "Protocol": String,
  "Requester": {},
  "Responder": {},
  "Error Code": " / ^ [0-9A-F] ^ {+} $ / ",
  "Error Message": String,
  "Description": String | {},
}
```

なぜ標準化が必要なのか？ 装置の表現

エラーをsyslogで報告する装置

```
"Reporter":{  
  "IP Address":  
    "(^(?:(:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)¥.){3}  
      (?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$)  
    |(^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$)"  
}
```

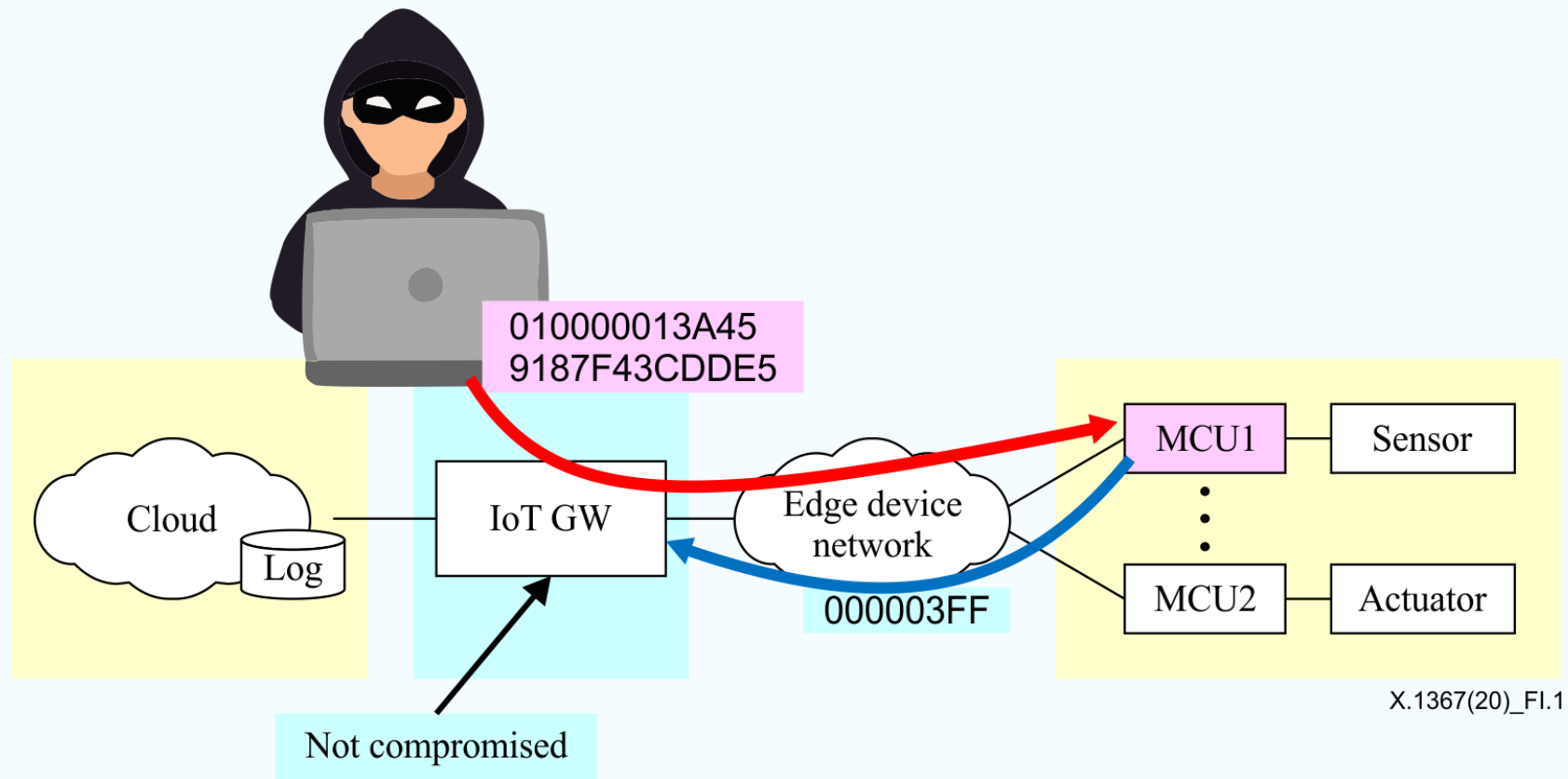
エラーの原因となった通信の送信装置と応答装置

```
"Requester(or Responder)": {  
  "Unique ID": string,  
  "Transmitted Code": "( [0-9A-F])^{\+}"
```

- X.1367 (X.elf-iot) の概要
- なぜ標準化が必要なのか？
- 期待される利用例
- 発行までの経緯と今後について

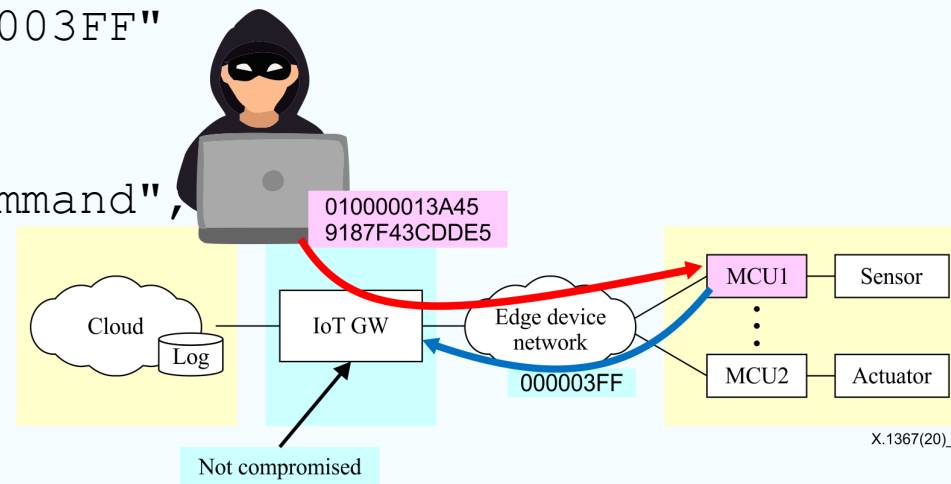
期待される利用例 不正コマンドの送信

- 攻撃者がクラウドからの振りをしてコマンド送信
- どのコマンドが利用可能かを探るためのスキャン



期待される利用例 不正コマンドの送信

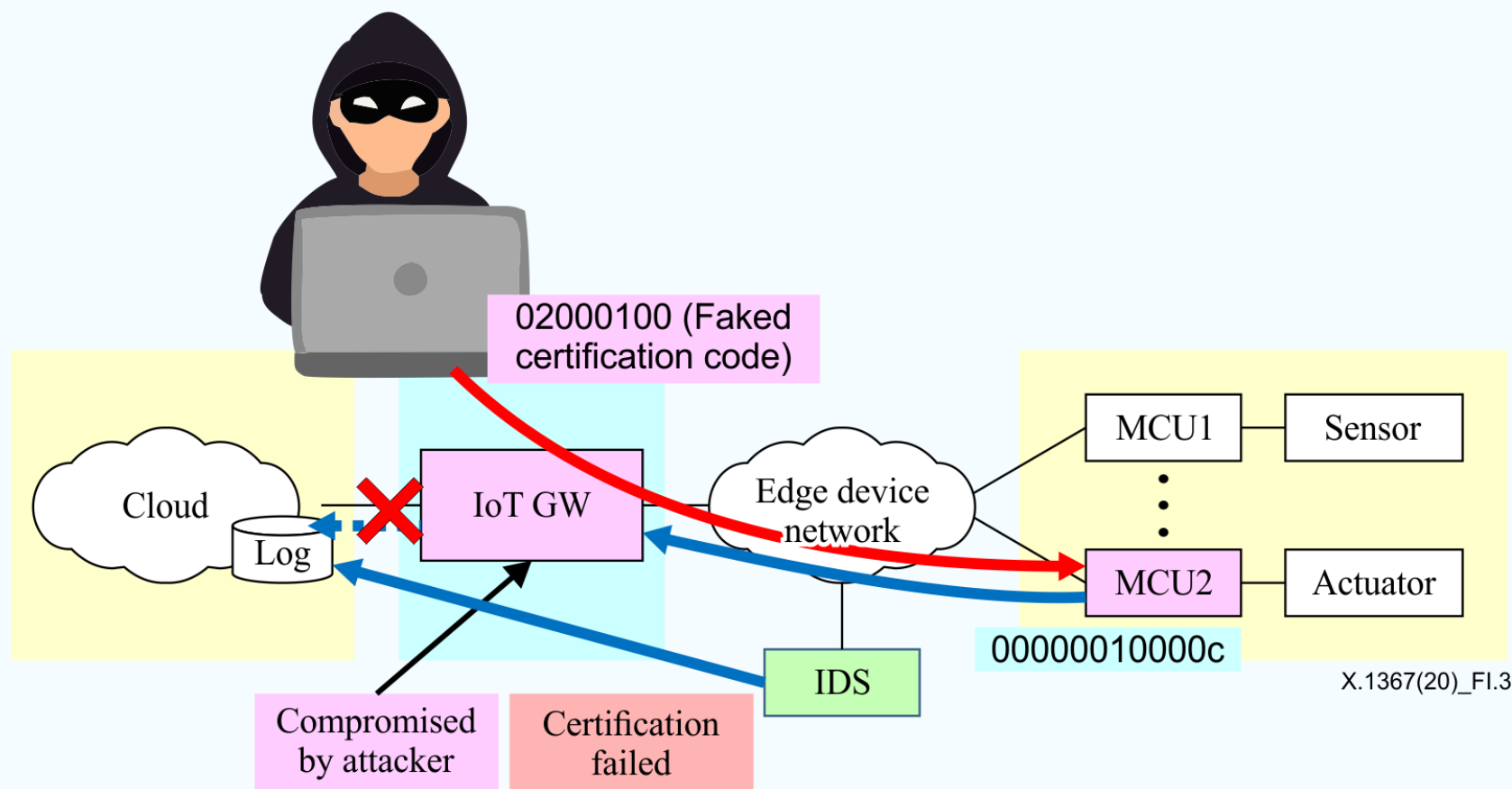
```
{  
  "Timestamp": "2018-08-28T09:34:55.0Z",  
  "Reporter": { "IP Address": "192.168.2.11" },  
  "Protocol": "ABC company protocol",  
  "Requester": {  
    "Unique ID": "0000",  
    "Transmitted Code": "010000013A459187F43CdDE5"  
  },  
  "Responder": {  
    "Unique ID": "0001",  
    "Transmitted Code": "000003FF"  
  },  
  "Error Code": "30",  
  "Error Message": "Invalid Command",  
}
```



X.1367(20)_FI.

IoTGW攻略後に偽証明書の送信

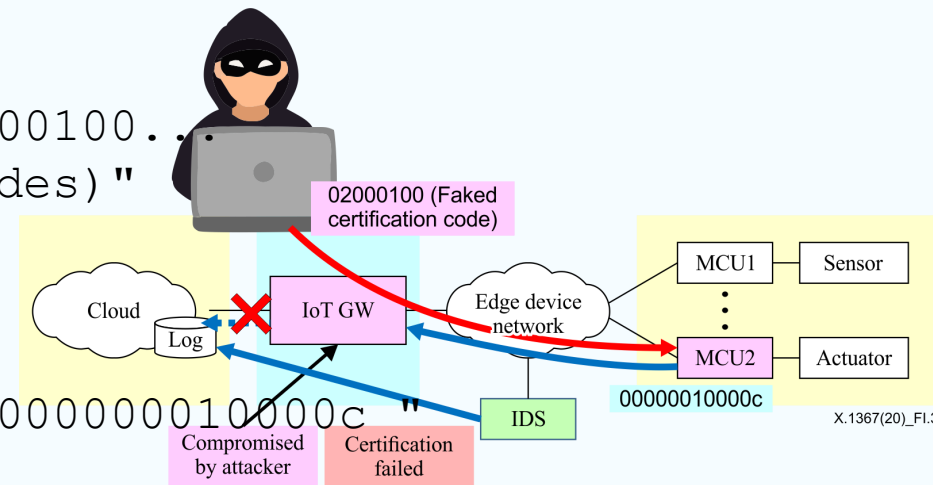
- 最初に攻撃者はIoTGWを攻略
- IoTGWを通じて偽証明書をMCU2に提示
- IoTGWからエラー情報がクラウドに上がるのを阻止



期待される利用例

IoTGW攻略後に偽証明書の送信

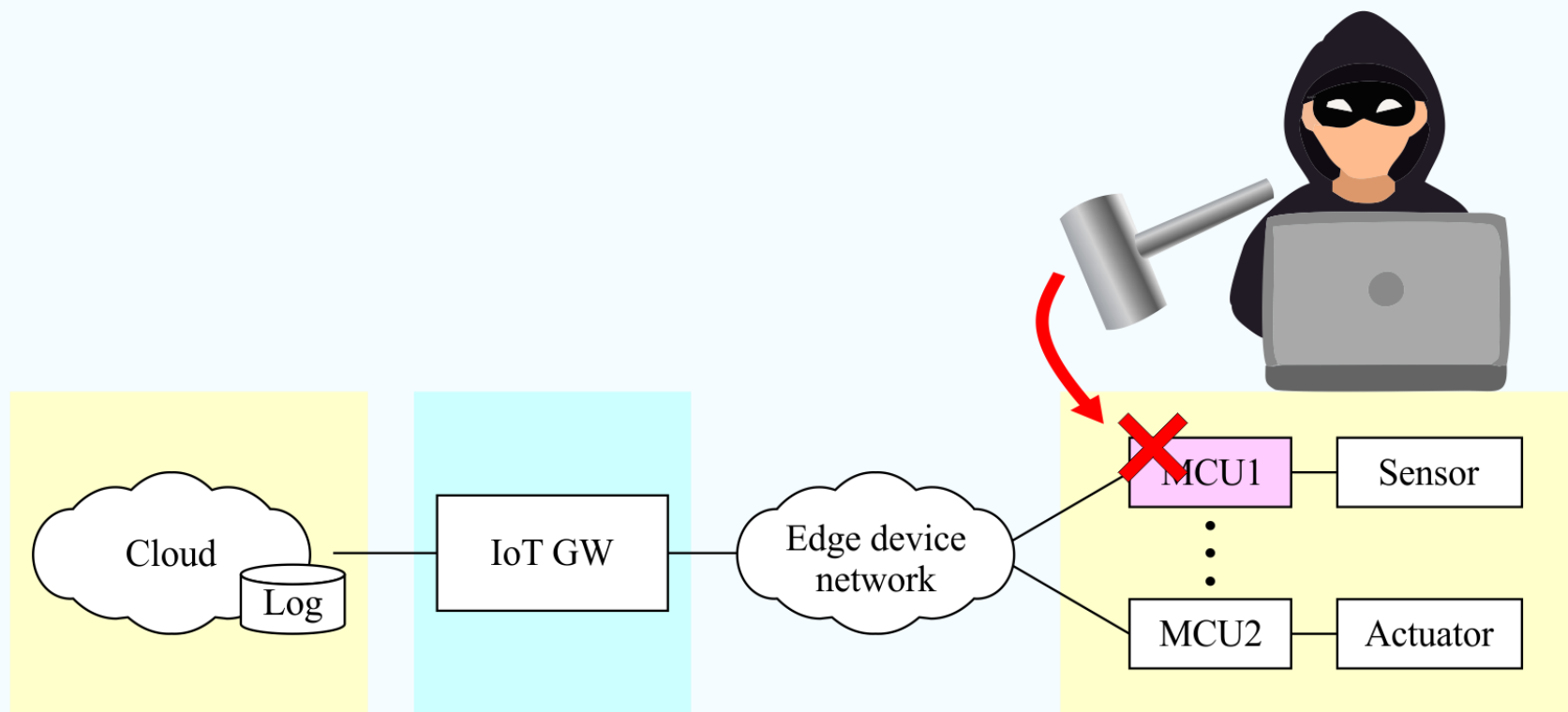
```
{
  "Timestamp": "2018-08-28T09:34:55.0Z",
  "Reporter": { "IP Address": "192.168.100.249" },
  "Protocol": "EEE Company's protocol",
  "Requester": {
    "Unique Name": "0000",
    "Transmitted Code": "02000100...
    (Faked certification codes)"
  },
  },
  "Responder": {
    "Unique Name": "0002",
    "Transmitted Code": "0000000000010000c"
  },
  },
  "Error Code": "21",
  "Error Message": "Certification Failed",
  "Description": {
    "Status": "This message was sent from IDS not IoTGW"
  },
  },
}
```



期待される利用例

MCU1の強制停止・破壊

- 攻撃者が定期的にデータ送信するMCU1を強制停止・破壊
- MCU1へのリクエストはない

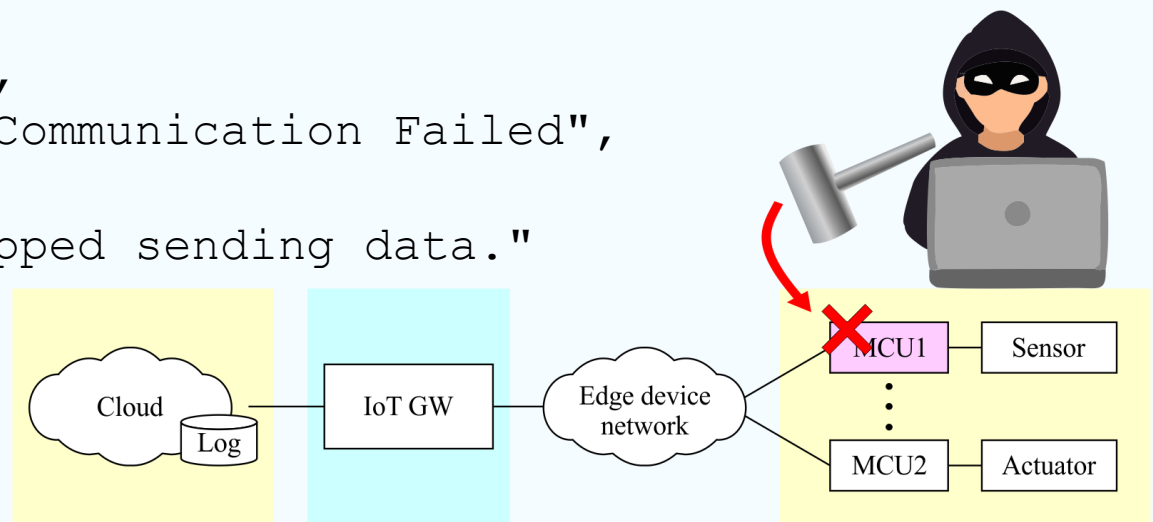


X.1367(20)_FI.5

期待される利用例

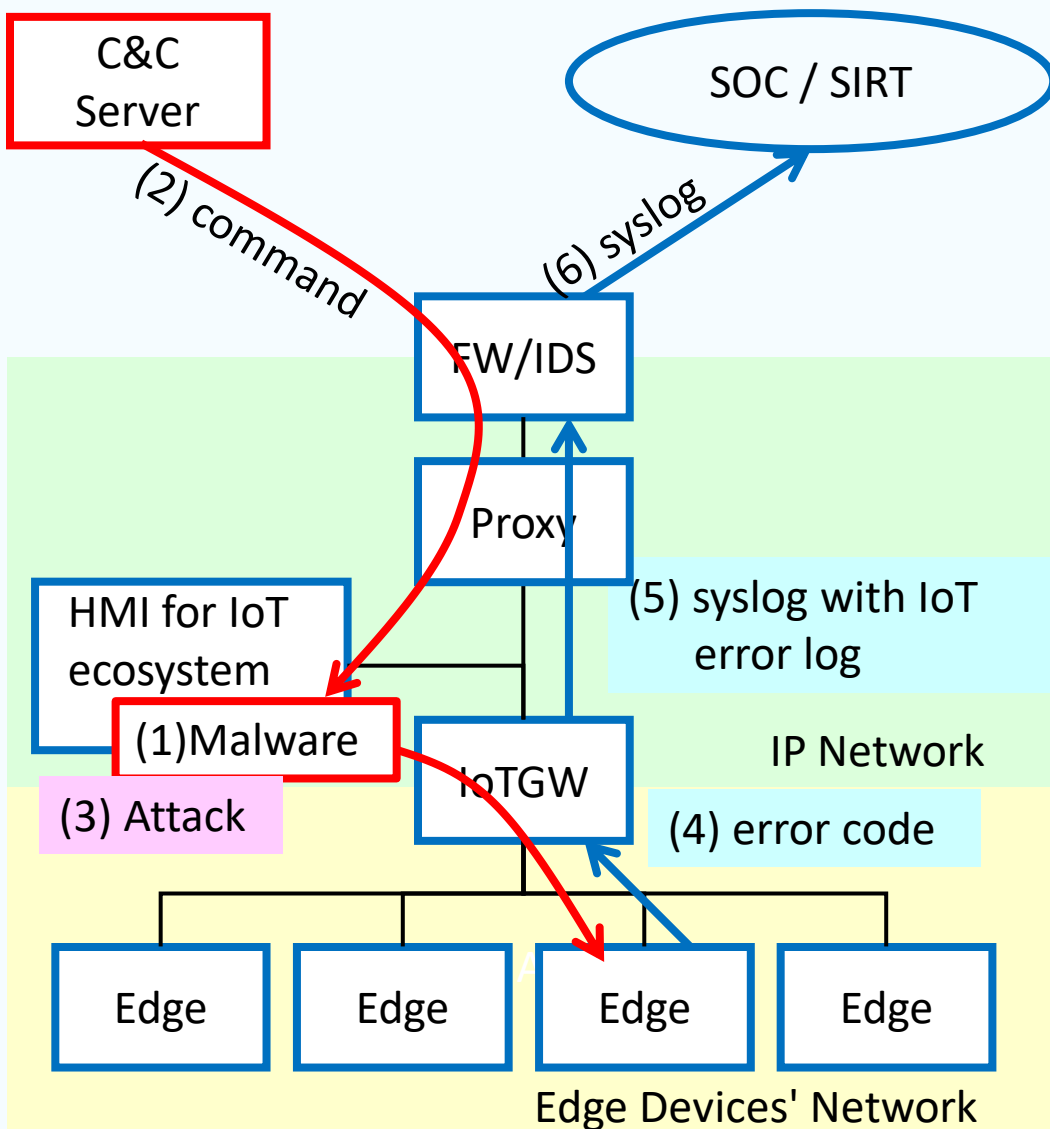
MCU1の強制停止・破壊

```
{  
  "Timestamp": "2018-08-28T09:34:55.0Z",  
  "Reporter": { "IP Address": "192.168.10.254"},  
  "Protocol": "ZZZ Company's protocol",  
  "Requester": {},  
  "Responder": {  
    "Unique Name": "0002",  
    "Transmitted Code": ""  
  },  
  "Error Code": "11",  
  "Error Message": "Communication Failed",  
  "Description": {  
    "Responder stopped sending data."  
  },  
}
```



X.1367(20)_F1.5

期待される利用例 エラーログの流れ(再掲)



1. HMIにマルウェア侵入
2. マルウェアがC&Cサーバからコマンド受信
3. マルウェアがエッジデバイスを攻撃
4. エッジデバイスがエラーコードを送信
5. IoTGWが標準化されたエラーレコードとしてsyslogで送信
6. FW/IDSがC&Cサーバとの通信ログなども集約してSOC/SIRTに送信

- X.1367 (X.elf-iot) の概要
- なぜ標準化が必要なのか？
- 期待される利用例
- 発行までの経緯と今後について

発行までの経緯と今後について 経緯

- 2018年2月：最初の中尾様への提案
- 2018年6月：Q6中間会合(ソウル)にて提案
- 2018年8月：SG17定期会合(ジュネーブ)にて寄書提出・X.elf-iot採番
- 2018年11月～2020年1月：SG17定期会合(ジュネーブ)x2回、Q6中間会合(日本、マレーシア)x2回
- 2020年3月：SG17定期会合(オンライン)・Determined、X.1367採番
- 2020年8月：SG17定期会合(オンライン)・Approved

以下、弊社(もっけ技研)の業務として実施したい

● 実装例の提供

- 本勧告の基本的な機能のライブラリ提供
- RaspberryPiやESP-WROOM-32などで動作するでもシステムの提供
- Echonet-Liteで動作するホーム家電IoT用のデモシステムの提供

● 改訂

- デモシステム運用をフィードバックによるエラーコード表の改訂
- バイナリなどJSON形式以外のエラーログ形式の追加

発行までの経緯と今後について 今後について

皆さんへ

- 標準化活動は皆さんのビジネスのコストを低減させ、市場を開拓、拡大する一つの方策です。
- 実現するための情熱と論理の整った説明ができれば、会議参加者は耳を傾けてくれます。
- 今後も標準化活動への積極的な参加、協力をお願いします。

Any Questions?

エラーコード表(1/2)

Code	Message	Description
No Error (0x00-0x0F)		
0x00	No Error	No error occurs.
Communication (0x10-0x1F)		
0x10	No Response	No response even though the request requires any responses.
0x11	Communication Failed	Some problems for failing communication.
0x12	Link Down	A network interface link is down.
0x1E	Extended Reasons	Prefix code for extended reasons.
0x1F	Other Communication Reasons	Other reasons related to communication.
Security (0x20-0x2F)		
0x20	Authentication Failed	Some problems of the authentication.
0x21	Certification Failed	Some problems of the certification.
0x22	Encryption Failed	Some problems of the encryption.
0x23	Authorization Failed	Some problems of the authorization.
0x2E	Extended Reasons	Prefix code for extended reasons.
0x2F	Other Security Reasons	Other reasons related to the authentication, the certification, the encryption or the authorization.

エラーコード表(2/2)

↵	Command (0x30-0x3F) ↵	
0x30 ↵	Invalid Command↵	The command is undefined or invalid.↵
0x31 ↵	Invalid Argument↵	The argument is out of range or invalid.↵
0x3E ↵	Extended Reasons↵	Prefix code for extended reasons.↵
0x3F ↵	Other Command Reasons↵	Other reasons related to the command.↵
↵	Device (0x40-0x4F) ↵	
0x40 ↵	Device Broken↵	A part of the device has <u>unrecoverably</u> broken.↵
0x41 ↵	Device Failed↵	A part of the device has failed but is recoverable.↵
0x42 ↵	Out of Resources↵	Running out of storage, memory, and any computing resources.↵
0x4E ↵	Extended Reasons↵	Prefix code for extended reasons.↵
0x4F ↵	Other Device Reasons ↵	Other reasons related to the device.↵
↵	Reserved for future extension (0x50-0xDF) ↵	
↵	Reserved for private applications (0xE0-0xEF) ↵	
↵	Others (0xF0-0xFF) ↵	
0xFF ↵	Other Reasons↵	Other reasons except for the above reasons.↵