TREND MICRO

POLITECNICO MILANO 1863
DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

産業用ロボットの セキュリティリスク検証からみえること

2018年2月7日
トレンドマイクロ株式会社
上田　勇貴

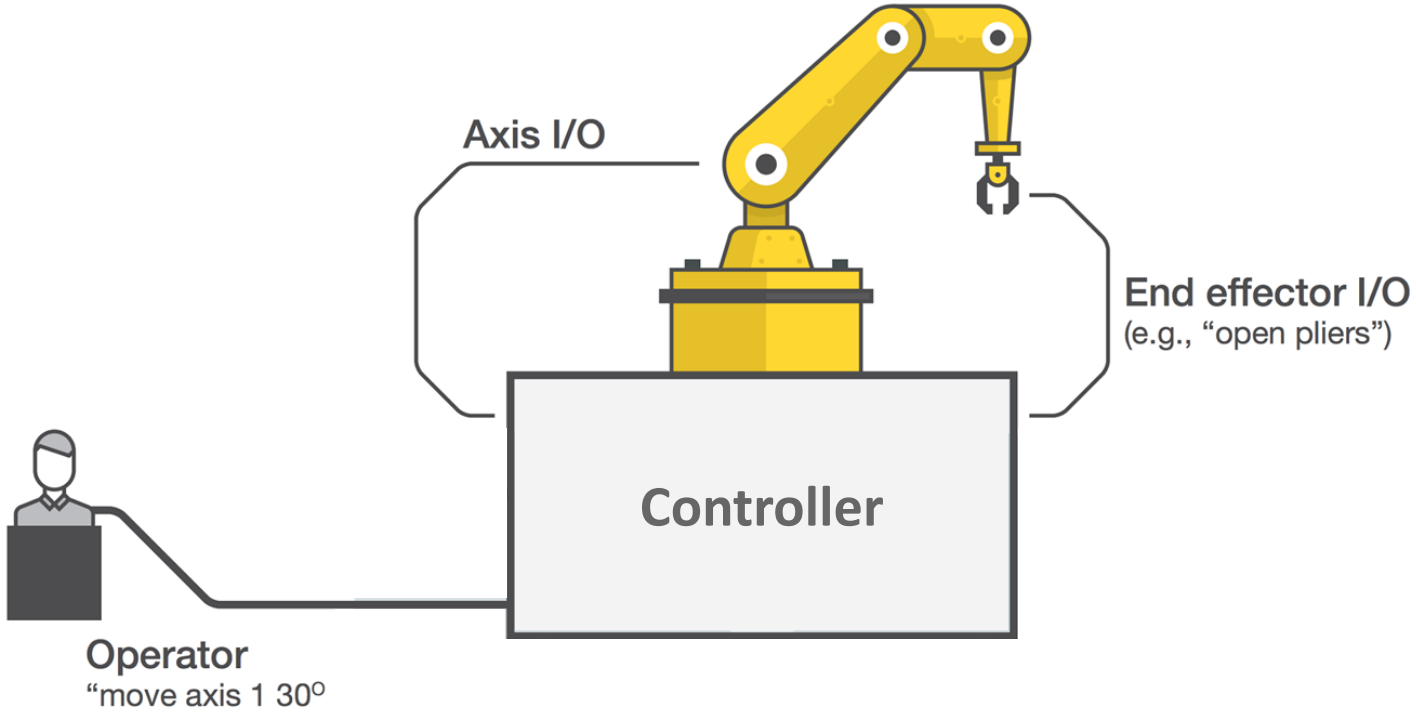
はじめに

- 本セッションの内容は、トレンドマイクロとミラノ工科大学が共同調査を行い、2017年5月に調査レポート、7月にblack hat USA 2017で公表したものです。

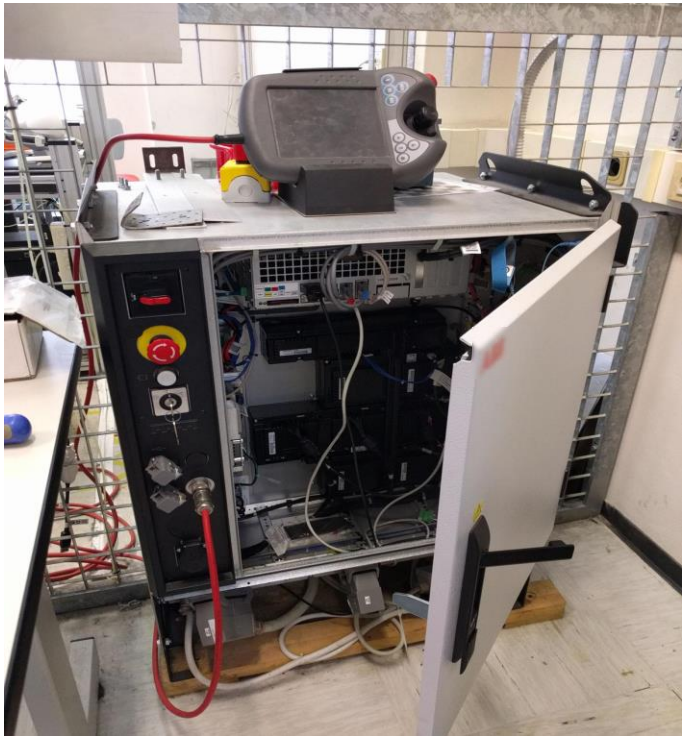
- 発見された脆弱性情報については、製造元に報告し適切に対処されています。

- 全ての産業用ロボットで同一の問題を抱えている、相対的に産業用ロボットのセキュリティリスクが高い、と主張するものではありません。

産業用ロボット



調査対象

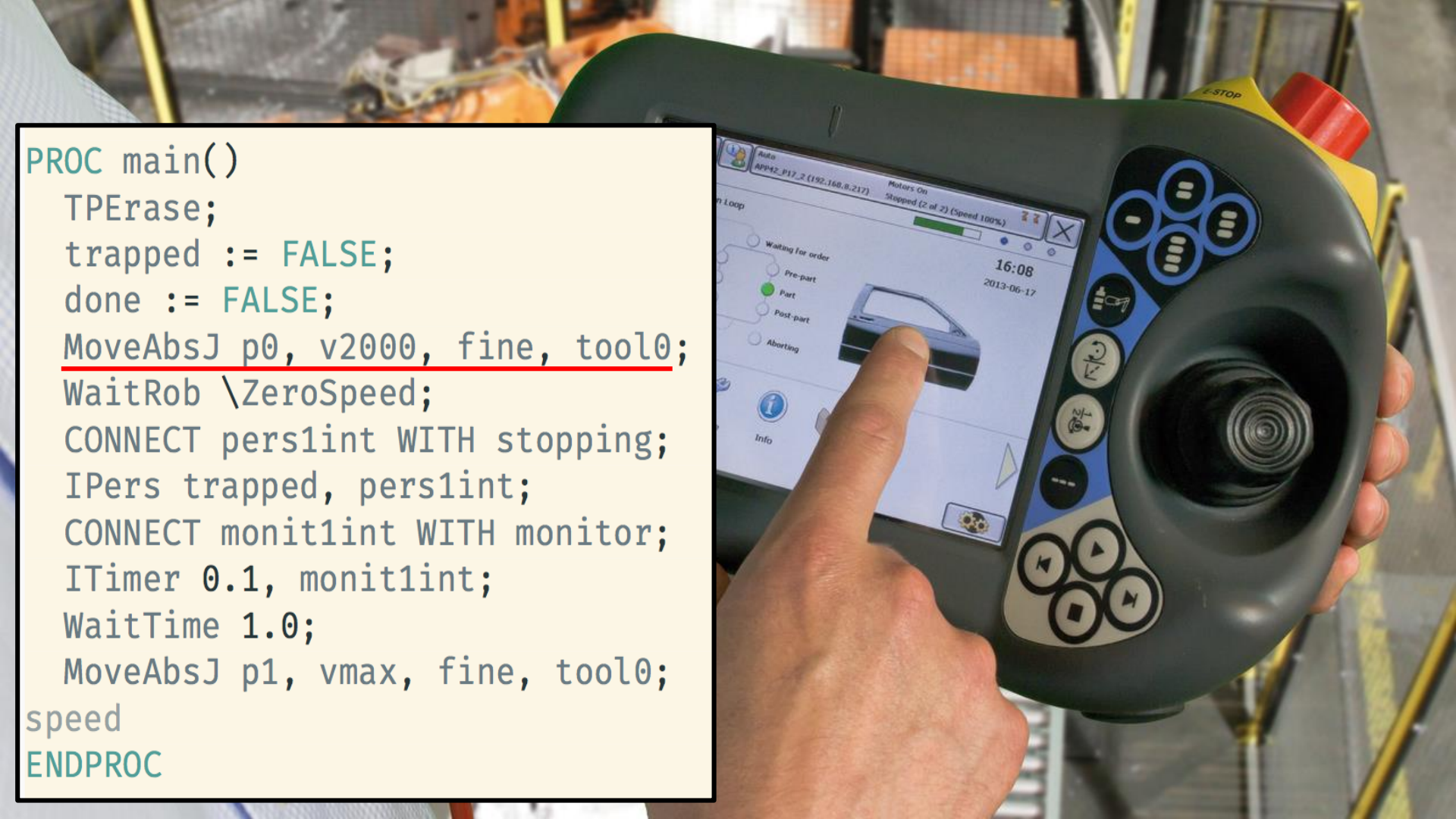


産業用ロボットの特徴

柔軟性のあるプログラミング

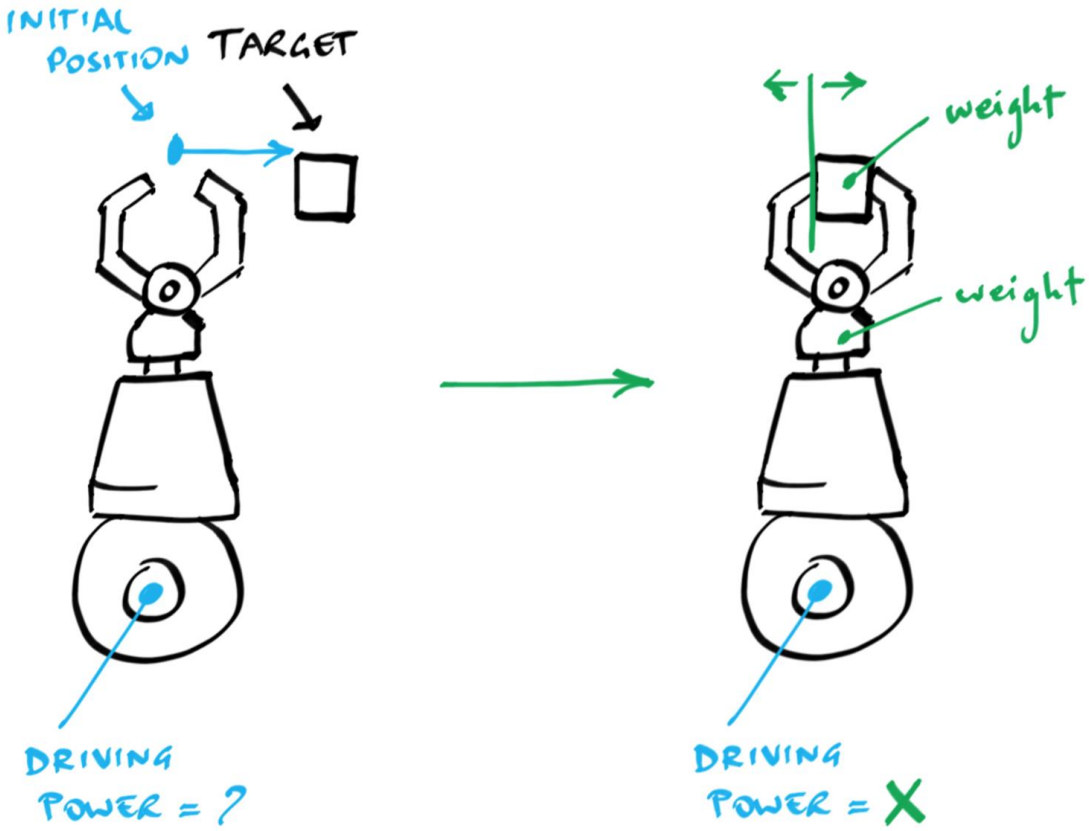
汎用システム

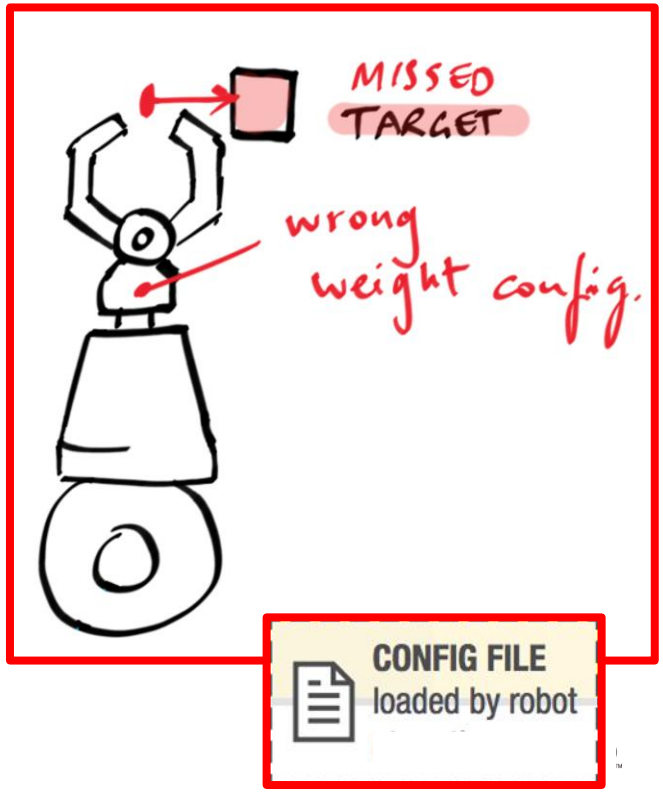
外部接続



```
PROC main()
  TPErase;
  trapped := FALSE;
  done := FALSE;
  MoveAbsJ p0, v2000, fine, tool0;
  WaitRob \ZeroSpeed;
  CONNECT pers1int WITH stopping;
  IPers trapped, pers1int;
  CONNECT monit1int WITH monitor;
  ITimer 0.1, monit1int;
  WaitTime 1.0;
  MoveAbsJ p1, vmax, fine, tool0;
speed
ENDPROC
```

“パラメータ”の存在


INITIAL POSITION
TARGET
DRIVING POWER = ?
weight
weight
DRIVING POWER = X


MISSED TARGET
wrong weight config.
CONFIG FILE
loaded by robot

産業用ロボットの特徴

柔軟性のあるプログラミング

汎用システム

外部接続

End Effector

SMB

IRB 140

contactor unit

drive unit

enable/speed/...

RS-485

axis computer (AXC)

VxWorks 5.x RTOS (PPC)

panel board

RS-485

status LEDs

24V DS

e-stop

24V DS

motors on/off

24V DS

auto / manual

24V digital signal

I/O board

DeviceNet

main computer (MC)

RS-485

FTP, RobAPI, ...

VxWorks 5.x RTOS (x86)

Teach Pendant

Ethernet

Windows CE (ARM) .NET >=3.5

Ethernet (service port)

(LAN port)

factory LAN

service LAN

Linux...

RS232

PRS

service net (vendor)

Ethernet (WAN)

Service Box

産業用ロボットの特徴

柔軟性のあるプログラミング

汎用システム

外部接続

End Effector
SMB
IRB 140
contactor unit
drive unit
RS-485
enable/speed/...
axis computer (AXC)
panel board
RS-485
status LEDs
24V DS
e-stop
24V DS
motors on/off
24V DS
auto / manual
24V digital signal
Ethernet
RS-485
I/O board
DeviceNet
main computer (MC)
Teach Pendant
Ethernet
Ethernet (LAN port)
Ethernet (service port)
factory LAN
service LAN
無線
RS232
LAN
GPRS
service net (vendor)
Service Box
Ethernet (WAN)

調査で判明した問題点

- **コントローラ**
  - メモリ破壊
  - 設計不備
  - 相手を無条件に信用

- **産業用ルータ**
  - 外部公開
  - 脆弱性

外部公開されている産業用ルータの調査結果

Brand	Exposed Devices	No Authentication
Belden	956	
Eurotech	160	
eWON	6,219	1,160
Digi	1,200	
InHand	883	
Moxa	12,222	2,300
NetModule	886	135
Robustel	4,491	
Sierra Wireless	50,341	220
Virtual Access	209	
Welotec	25	
Westermo	6,081	1,200
TOTAL	83,673	5,105

※出典：https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf
これら全ての産業用ルーターに必ず産業用ロボットが接続されているわけではありません

容易に特定可能な産業用ルータ

- **饒舌な機器**
  - ブランド名、モデル名、バージョン名
- **ベンダのサイトで開示されている技術情報**
  - 技術マニュアル：すべてのベンダ
  - ファームウェア：7/12ベンダ

産業ルーターの脆弱性問題

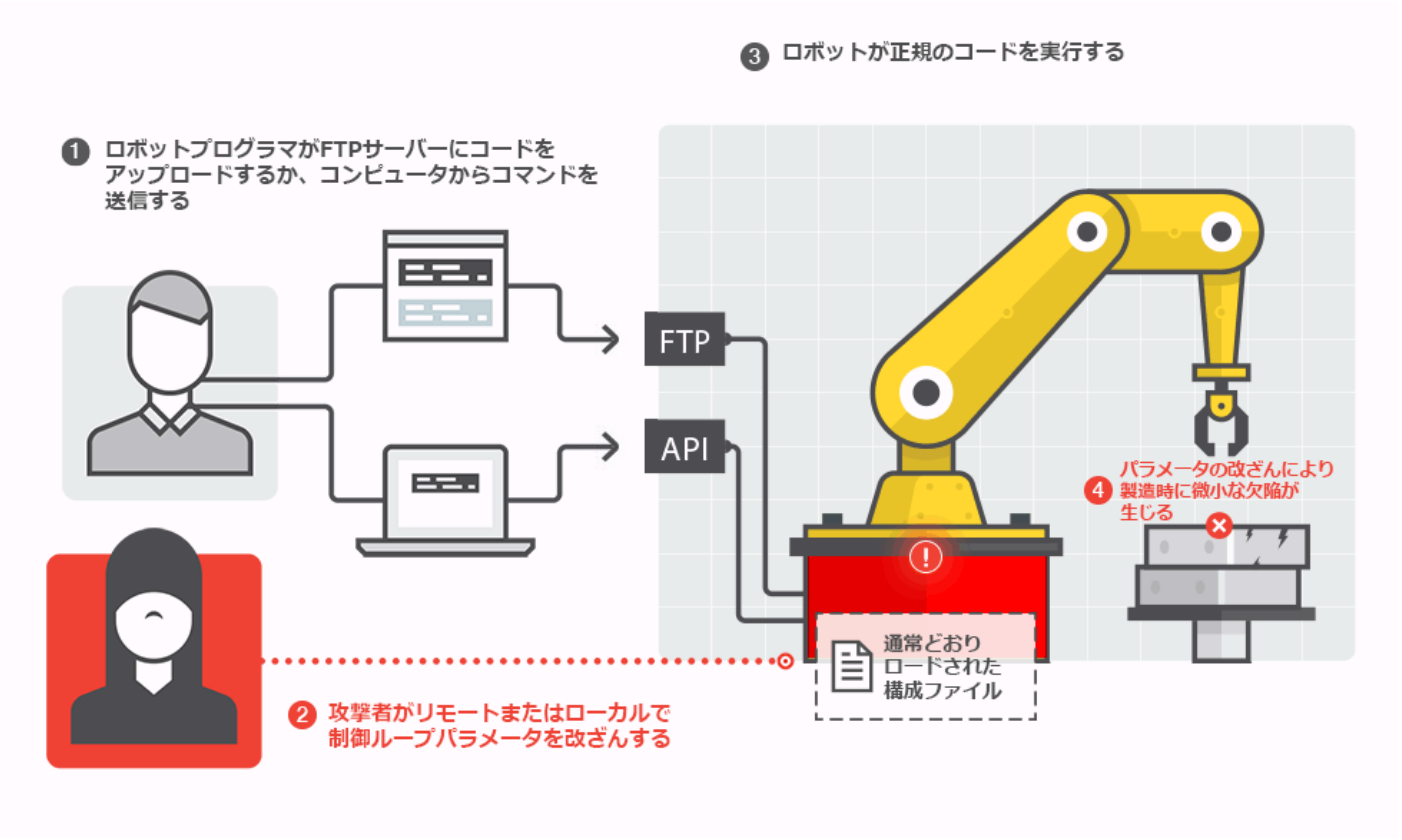
- **アプリケーション**
  - DropBear SSH, BusyBox, etc…
- **ライブラリ**
  - Cypto, etc..
- **カーネル**
- **ベースバンド**
- **コンパイラ**

End Effector
SMB
IRB 140
contactor unit
drive unit
RS-485
axis computer (AXC)
panel board
enable/speed/...
RS-485
status LEDs
24V DS
e-stop
24V DS
motors on/off
24V DS
auto / manual
24V digital signal
Ethernet
RS-485
I/O board
DeviceNet
main computer (MC)
Teach Pendant
Ethernet
Ethernet (LAN port)
Ethernet (service port)
factory LAN
service LAN
RS232
GPRS
service net (vendor)
Ethernet (WAN)
Service Box

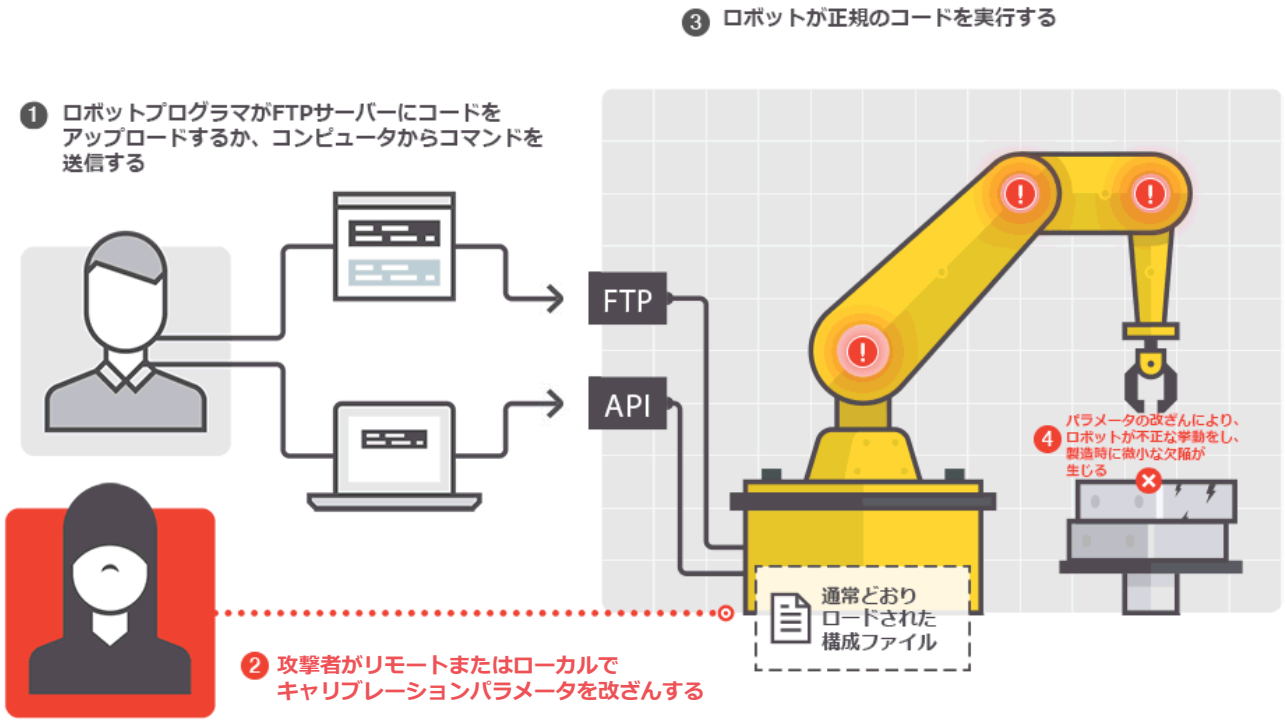
想定される攻撃シナリオ

① コントローラのパラメータ改ざん
② キャリブレーションパラメータの改ざん
③ 生産ロジックの改ざん
④ ロボットのステータス情報の表示を改ざん
⑤ 実際のロボットのステータスを改ざん

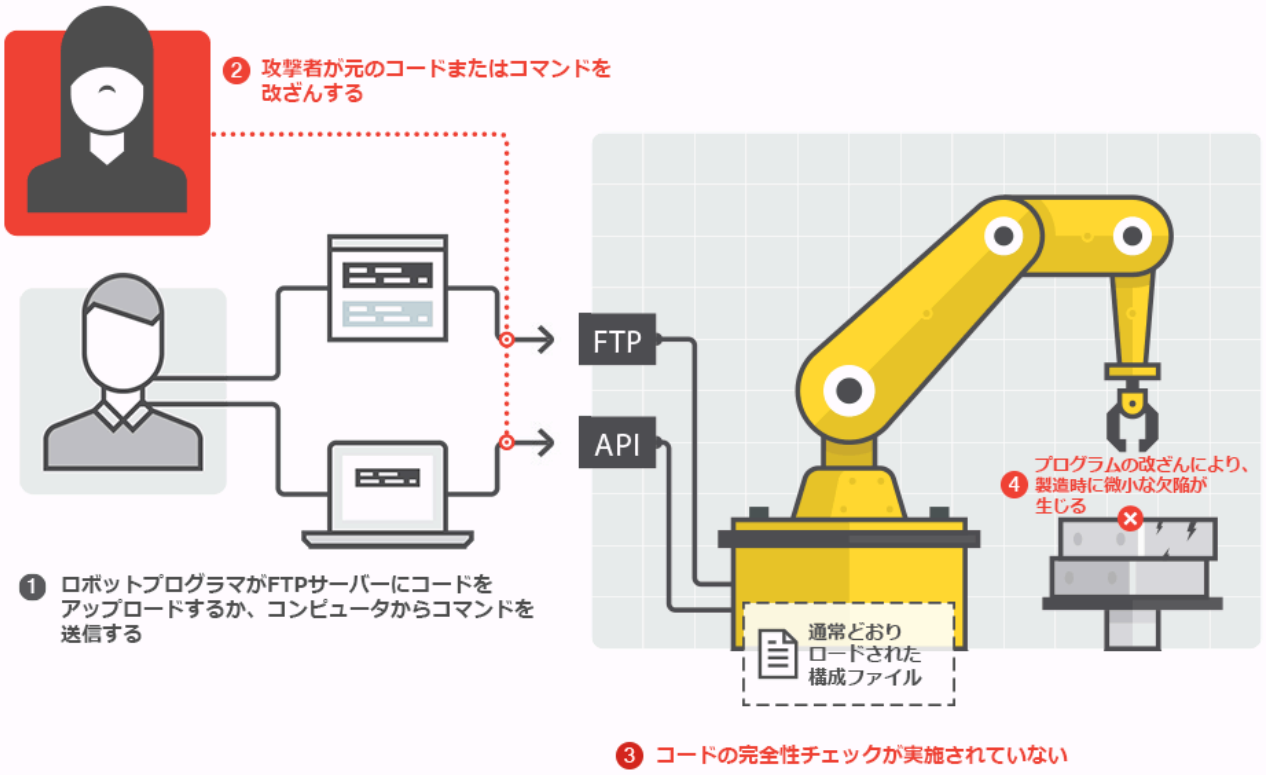
①コントローラのパラメータ改ざん



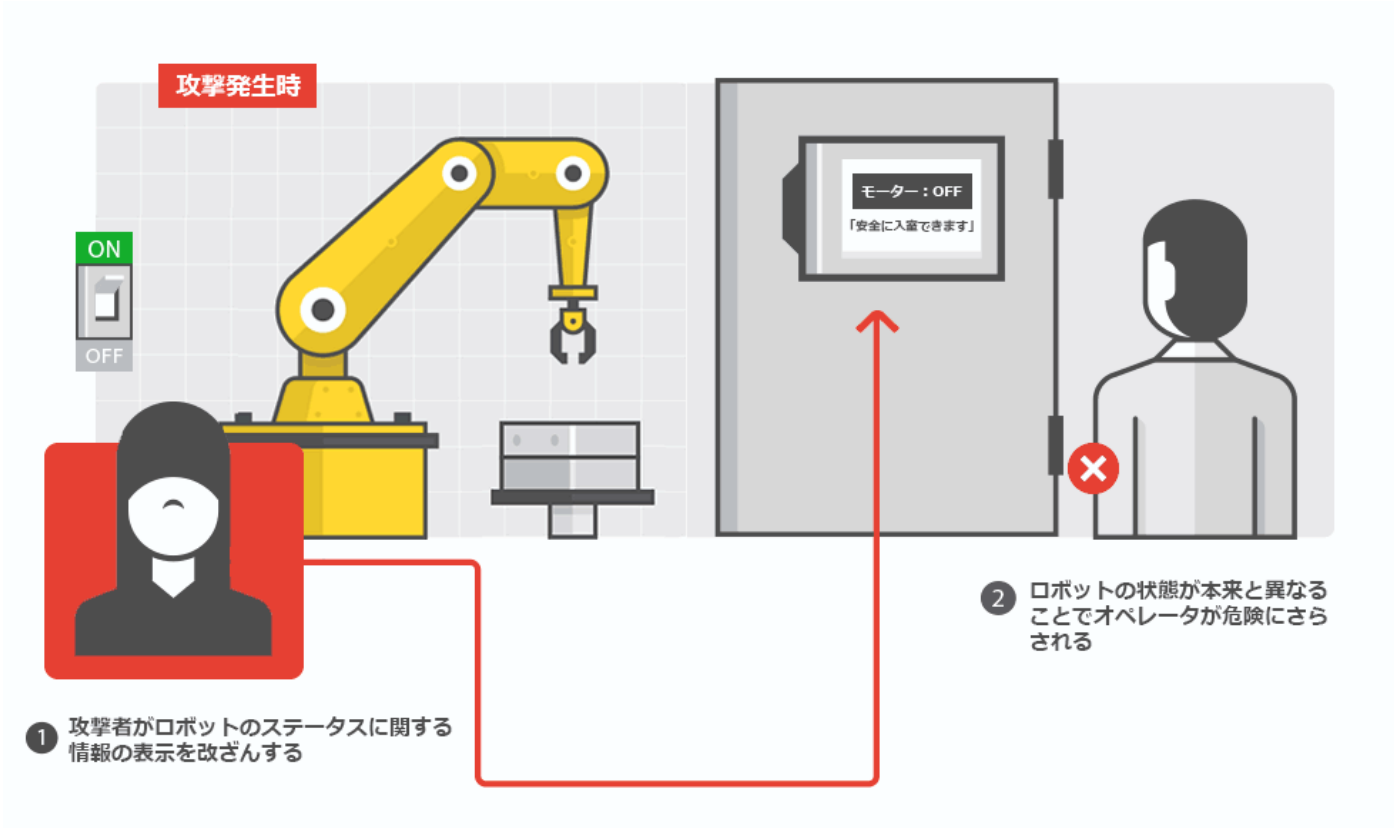
②キャリブレーションパラメータの改ざん



③生産ロジックの改ざん



④ロボットのステータス情報の表示を改ざん

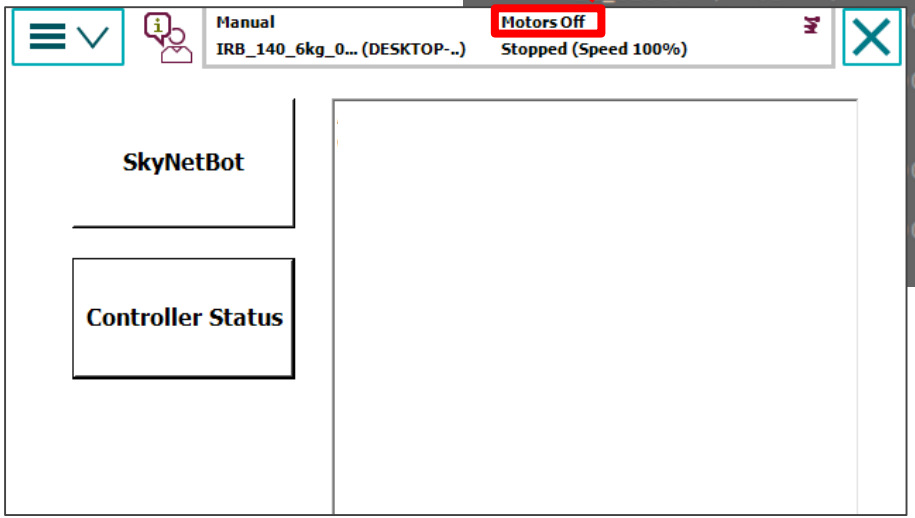


ステータス表示の改ざん 1/2

Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)               */ call       instance string [System.Drawing/*23000
~() /* 0A000028 */
        //IL_0262:  /* 02   |
        ldstr "Motors Off"
        IL_0268:  /* 02   |
        IL_0269:  /* 7B   | (04)0000B2         */ ldfld      class [System.Drawing/*23000007*/]Sys
        IL_026e:  /* 02   |                    */ ldarg.0
                                                 0000B0       */ ldfld      class [System.Drawing/*23000007*/]Sys
                                                              */ ldloca.s   V_1
                                                 000169       */ call       instance int32 [System.Drawing/*23000
                                                              */ conv.r4
                                                              */ ldloca.s   V_1
                                                 0000DF       */ call       instance int32 [System.Drawing/*23000
                                                              */ conv.r4
                                                 0000AD       */ callvirt   instance void [System.Drawing/*230000
```

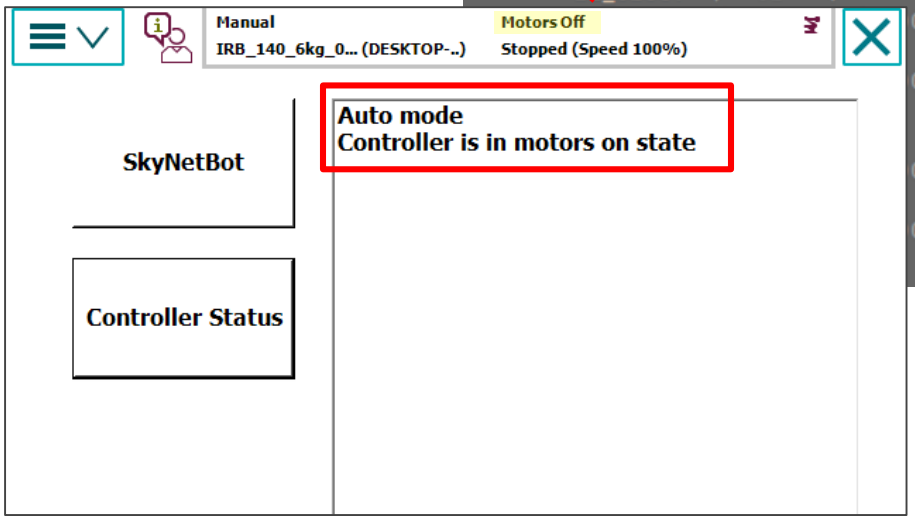


ステータス表示の改ざん 2/2

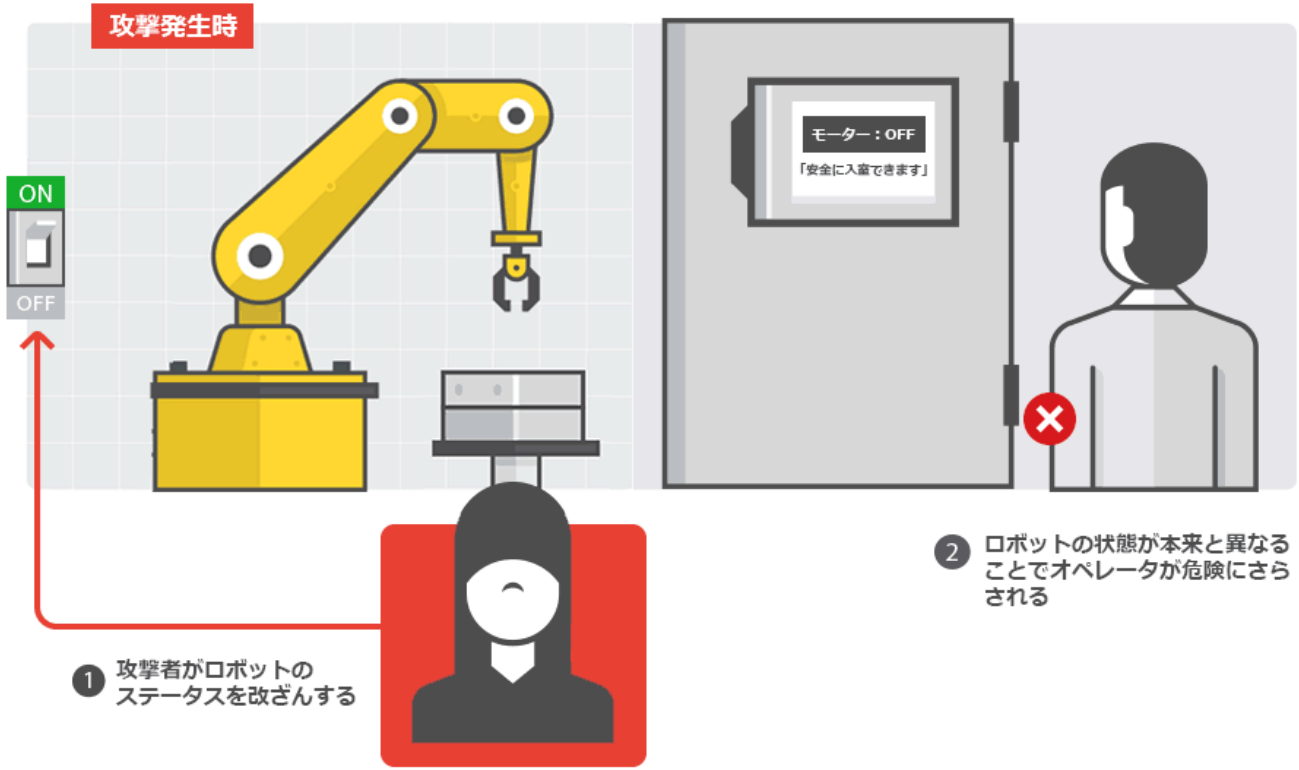
Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)               */ call       instance string [System.Drawing/*23000
~() /* 0A000028 */
        //IL_0262:  /* 02   |
        ldstr "Motors Off"
        IL_0268:  /* 02   |
        IL_0269:  /* 7B   | (04)0000B2         */ ldfld      class [System.Drawing/*23000007*/]Sys
        IL_026e:  /* 02   |                    */ ldarg.0
                                                 */ ldfld      class [System.Drawing/*23000007*/]Sys
                                                 */ ldloca.s   V_1
                                                 */ call       instance int32 [System.Drawing/*23000
                                                 */ conv.r4
                                                 */ ldloca.s   V_1
                                                 */ call       instance int32 [System.Drawing/*23000
                                                 */ conv.r4
                                                 */ callvirt   instance void [System.Drawing/*230000
```



⑤実際のロボットのステータスを改ざん



想定される影響

不良品	設備損傷	人的被害
信用失墜	コスト	情報漏洩

想定される攻撃者の目的

金銭

興味

自己顕示

競合排除

セキュリティ強化に向けて 1/2

- **短期的**
  - パッチの適用、外部接続の見直し、異常検知
- **中期的**
  - ハードニング
- **長期的**
  - 産業用ロボットにおけるサイバーセキュリティの標準化と実装

セキュリティ強化に向けて 2/2

- **ベンダ**
  - 率先した取り組みの継続
- **ユーザ**
  - 工場設備全体を俯瞰した対策の検討

ご案内

- **本調査の技術面を含む説明**
  - black hat USA 2017公演ビデオ
  - https://youtu.be/RKLUWnzIaP4

- **詳細レポートとその抄訳**
  - https://www.trendmicro.com/jp/iot-security/special/20100

ご清聴ありがとうございました。