IoTとセキュリティ

長崎県立大学
情報セキュリティ学科
松田　健

IoTの導入事例

https://article.auone.jp/detail/1/2/5/90_5_r_20180808_1533719392286569

線路転落の監視

ホームに設置されているカメラを利用！！

IoTの導入事例

https://japan.cnet.com/article/35093936/

JR東日本のIoT

IoT導入の未来予想図

https://japan.cnet.com/article/35093936/

JR東日本のIoT

IoTとは？

インターネットに接続可能なもの、しているものを活用すること？

⇨ **人の代わり**になるようなことがメイン？

AIとか、ビッグデータとか、ユビキタスとか？？

⇩

ユーザーにとっては、
「自分だけ」
の情報が提供される

IoTのセキュリティの有名な話

DDoS攻撃の実例

ここからは**理想論**

IoTのセキュリティとは？

IPAの資料

https://www.ipa.go.jp/security/iot/iotguide.html

IoTセキュリティの対策

開発者

IPAの資料

事業者連携・業界基準・サービス

IoTセキュリティの対策のキーワード

IPAの資料

IoTのセキュリティ設計

IPAの資料

脅威分析の例1

IPAの資料

Phishingなど

ますます巧妙化

脅威分析の例2

IPAの資料

考慮すべき対策

IPAの資料

考慮すべき対策

IPAの資料

開発側の観点

例題

マイコンで水槽の温度管理がしたいな～

どんな準備が必要？？

例題

マイコンで水槽の温度管理がしたいな～

とりあえずマイコンを探す・・・

例題

マイコンで水槽の温度管理がしたいな～

とりあえずマイコンを探す・・・

Ricardo&Co. 熱帯魚 昆虫 などの温度管理に最適 。 DC12V 汎用 サーモスタット サーモスイッチ 温度調節器 (3.サーモスタット小型)

FUN MARKET By Ricardo&Co.

カスタマーレビューを書きませんか？

現在在庫切れです。 在庫状況について

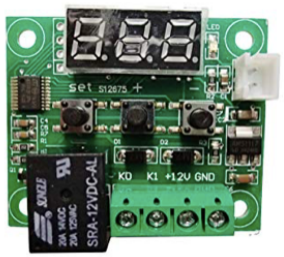
この商品の再入荷予定は立っておりません。

不正確な製品情報を報告。

例題

マイコンで水槽の温度管理がしたいな～

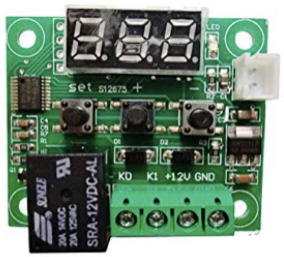
マイコンをとりあえず取り付けるか・・・



例題

マイコンで水槽の温度管理がしたいな～

マイコンをとりあえず取り付けるか・・・

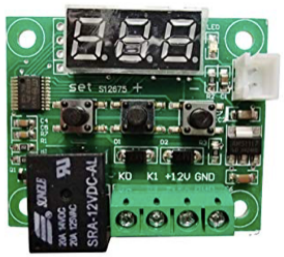


温度計入れとけば？？(笑)

例題

マイコンで水槽の温度管理がしたいな～

マイコンをとりあえず取り付けるか・・・

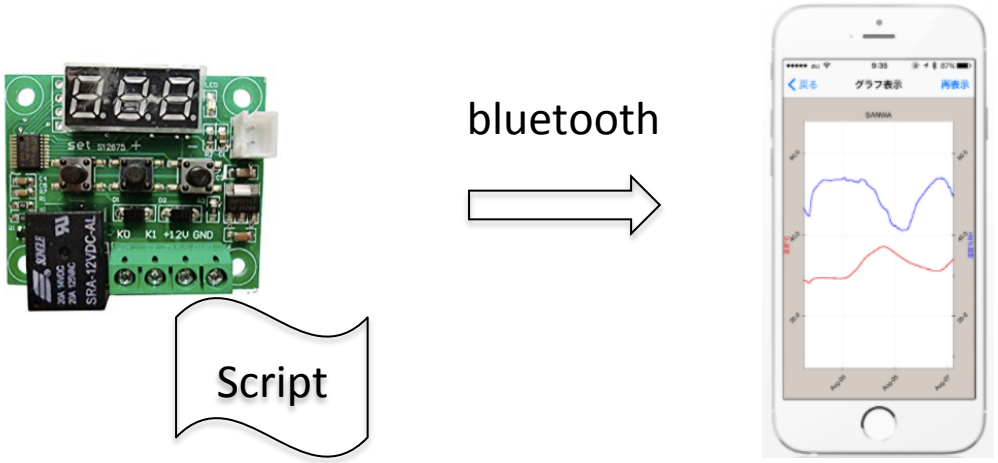


温度を水槽の前に行かなくても見れればな～

IoT

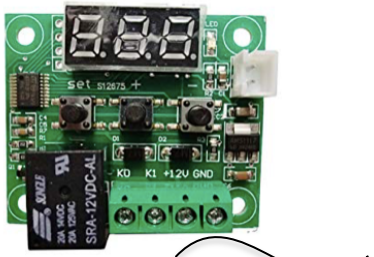
全体図1

Bluetoothを使ってみると・・・



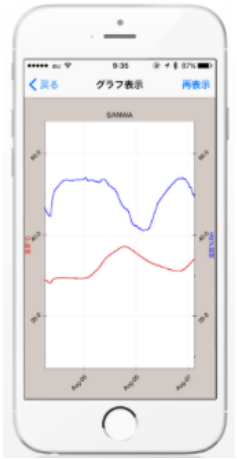
全体図1

Bluetoothを使ってみると・・・



Script

bluetooth



使える？？

Bluetoothセキュリティ

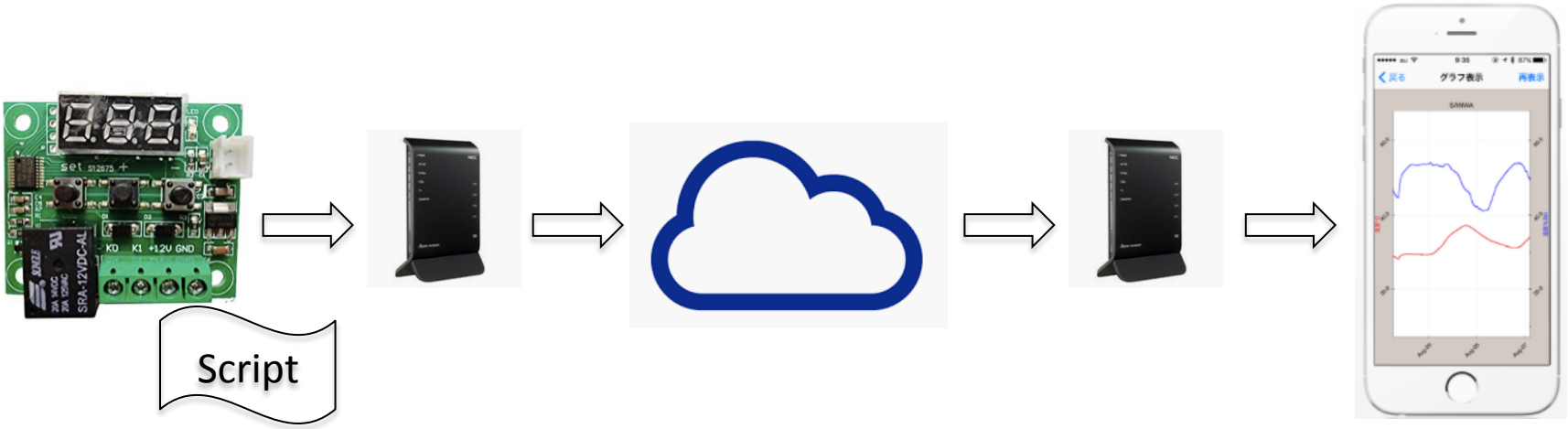
トレンドマイクロの資料

影響は50億台以上の危機に・・・

https://blog.trendmicro.co.jp/archives/15912

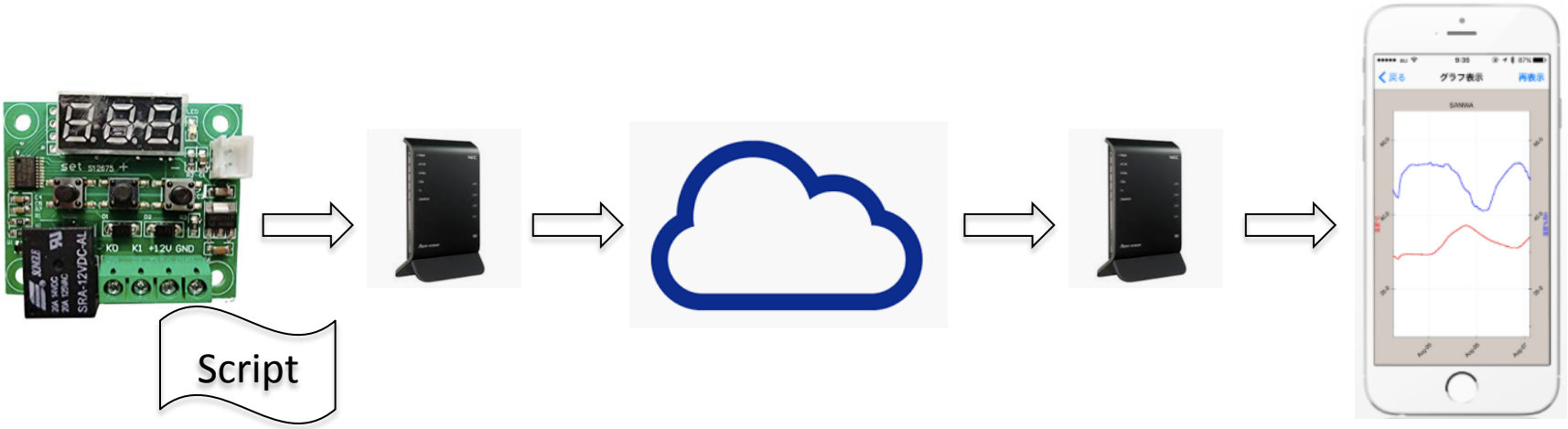
全体図2

Wi-Fiを使ってみると・・・



全体図2

Wi-Fiを使ってみると・・・



データは送られてくるが・・・

ルーターのセキュリティ

BUFFALOのページ

http://buffalo.jp/product/wireless-lan/wi-fi/security/

ルーターのセキュリティ

BUFFALOのページ

http://buffalo.jp/product/wireless-lan/wi-fi/security/

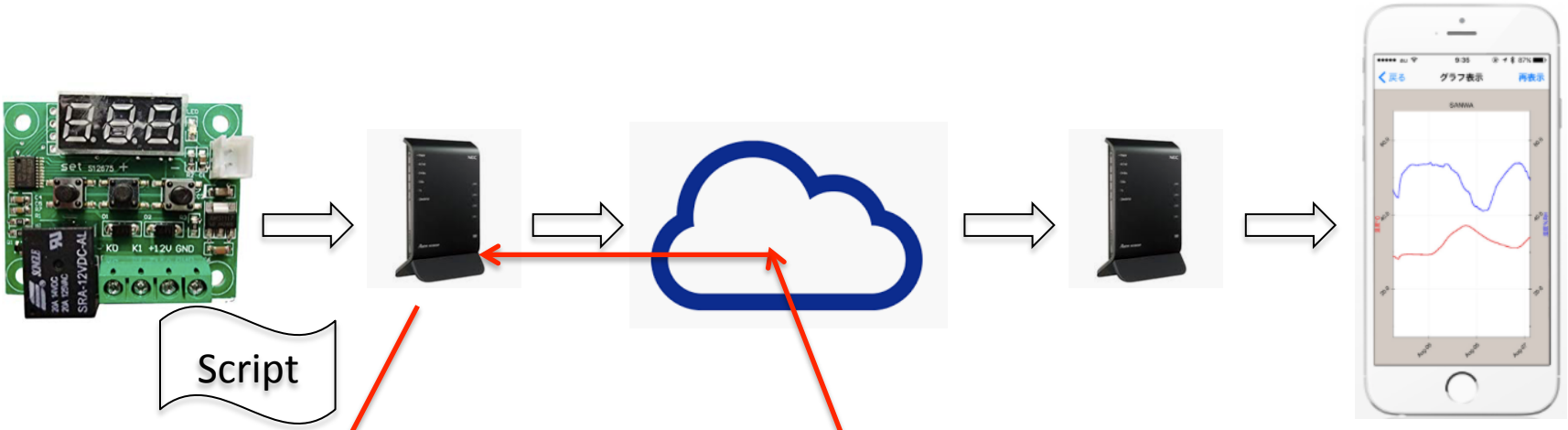
ルーターのセキュリティ

BUFFALOのページ

http://buffalo.jp/product/wireless-lan/wi-fi/security/

全体図2

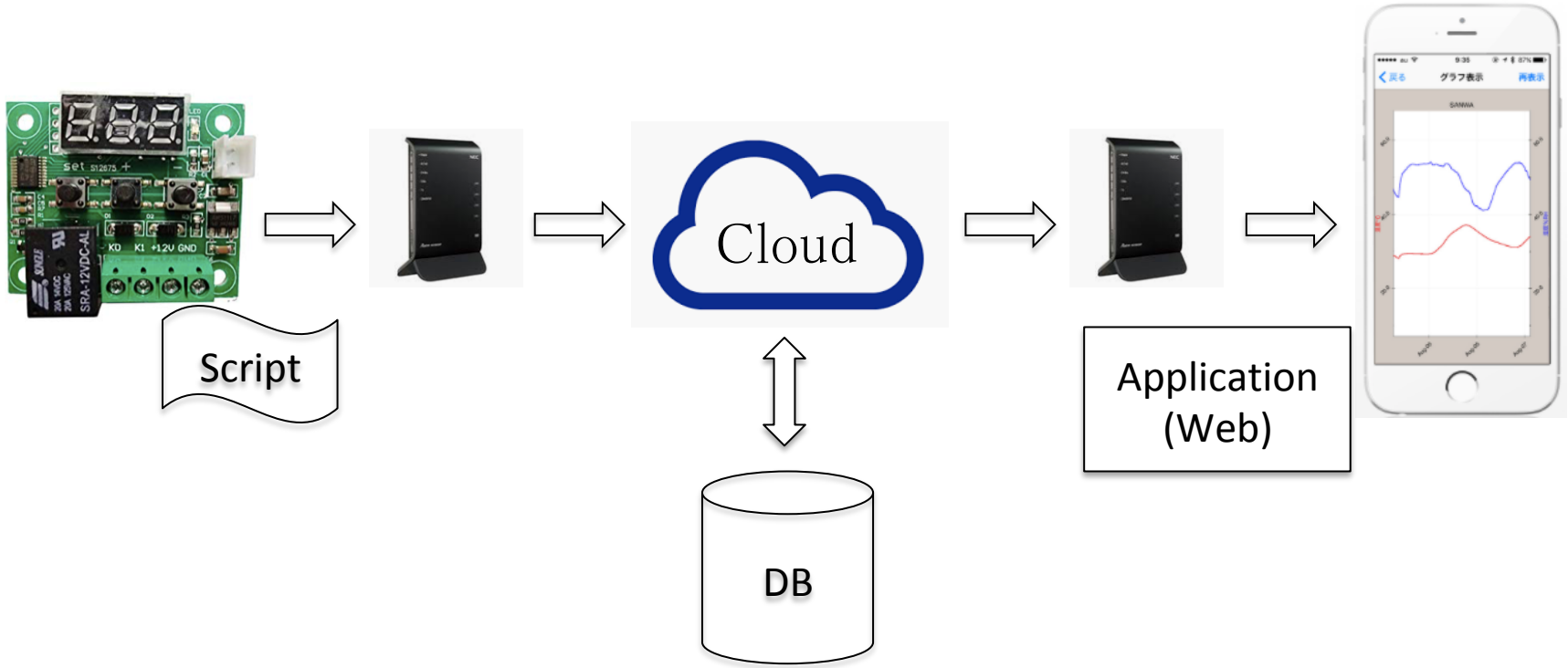
Wi-Fiを使ってみると・・・



防犯・玄関？？　https://japan.cnet.com/article/35111398/

全体図3

データを記録したいな・・・



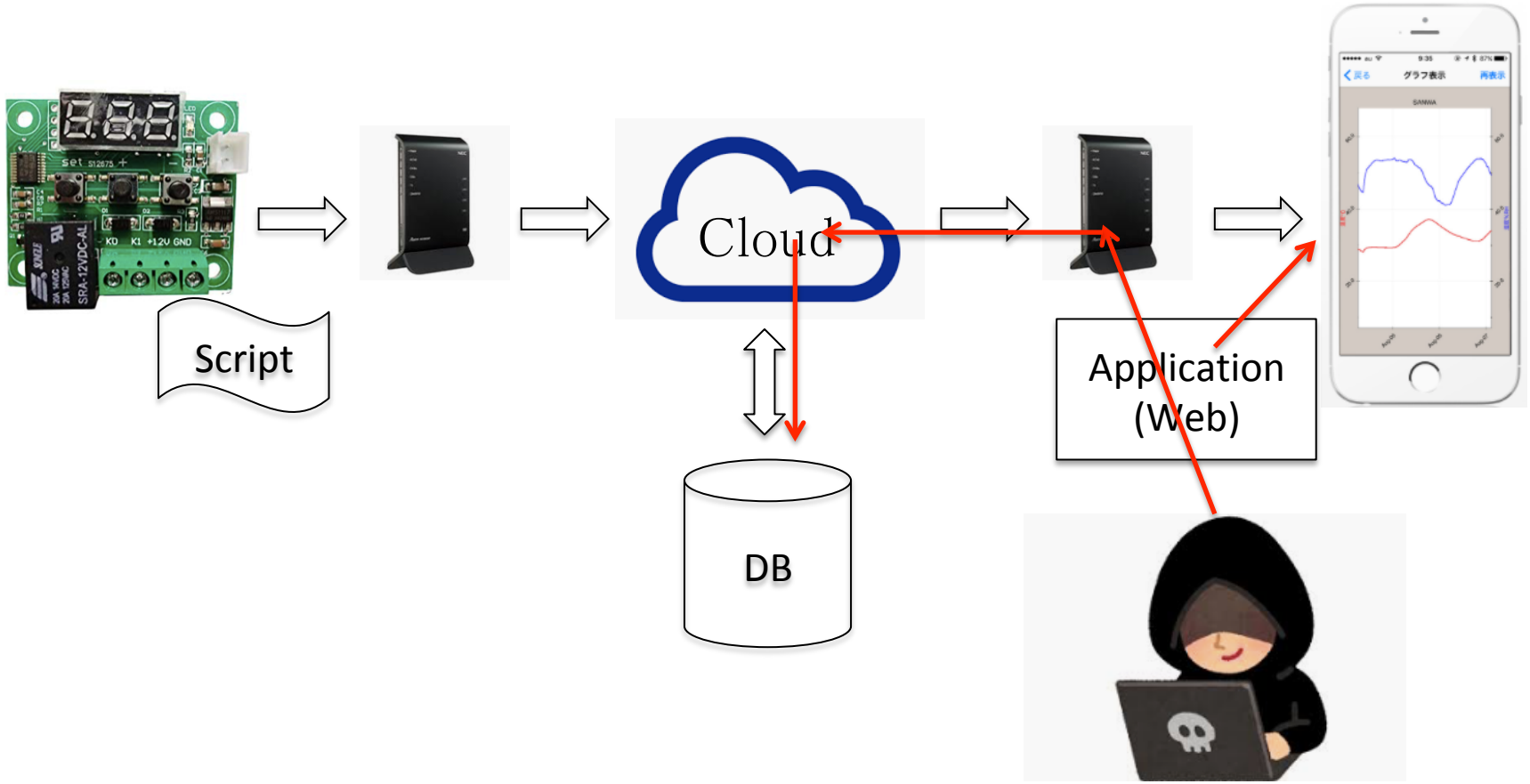
Webのセキュリティ

想定すべきリスク

- データベースへの不正アクセス
- 詐欺サイトの設置
- 不正スクリプトやマルウェアの設置
- 個人情報の流出
- 自身のネットワークに含まれるIoT機器へのリスク
- 他者への脅威に対するリスク

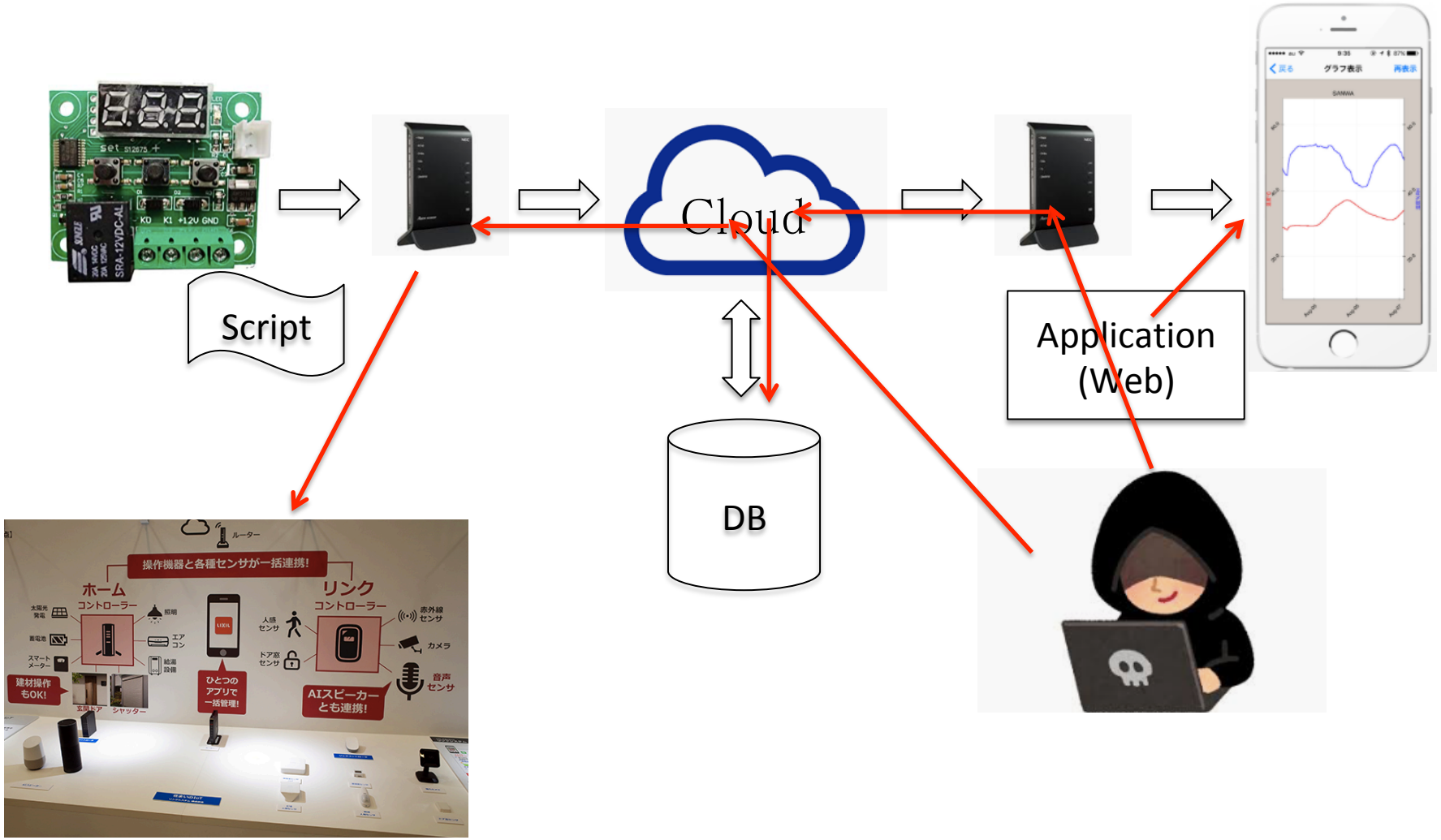
全体図3

データを記録したいな・・・



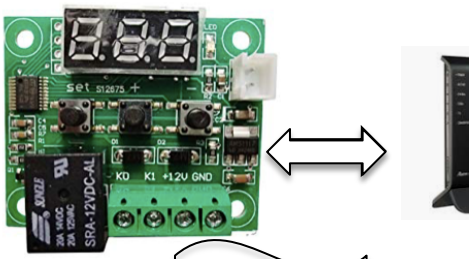
全体図3

データを記録したいな・・・

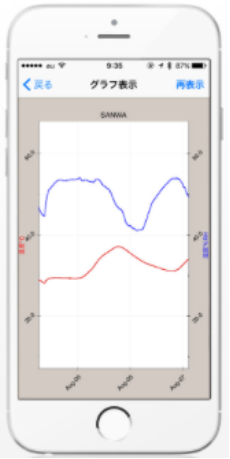


全体図4

AIを利用したいな・・・



Cloud



Script

Application
(Web)

DB

ヒーターの電源 ON / OFF

自動化ルール

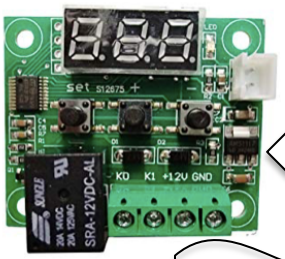
30℃になったらOFF /
28℃になったらON

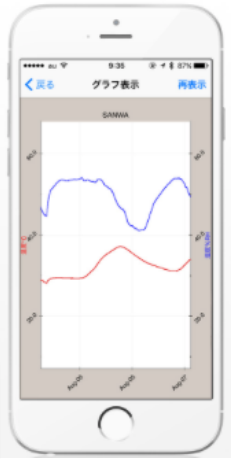
OR

電源On/OFFの
温度を記録して学習

全体図4

どのような脅威が存在する？





Script

Application
(Web)

DB

ヒーターの電源 ON / OFF

自動化ルール

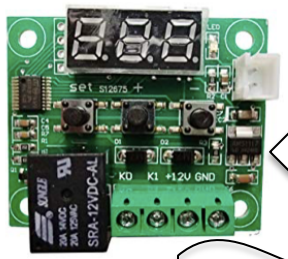
30℃になったらOFF /
28℃になったらON

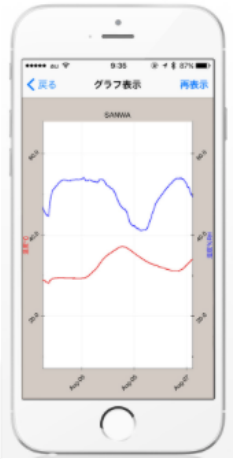
OR

電源On/OFFの
温度を記録して学習

全体図4

どのような脅威が存在する？





Script

Application
(Web)

DB

ヒーターの電源 ON / OFF

自動化ルール

30℃になったらOFF /
28℃になったらON

改ざん / 妨害

OR

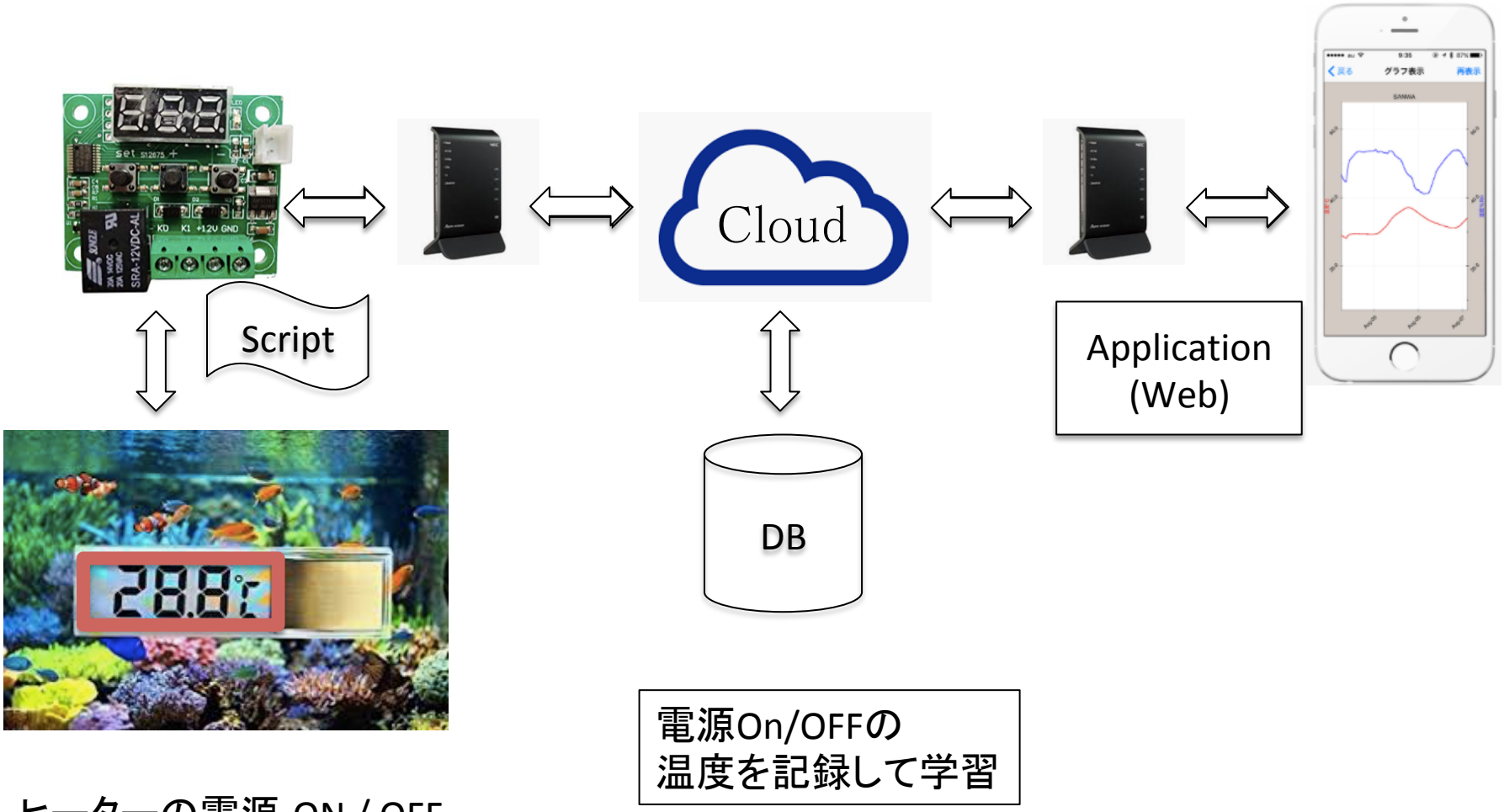
もしこれが貴重なら・・・

電源On/OFFの
温度を記録して学習

サービスを提供する側の観点

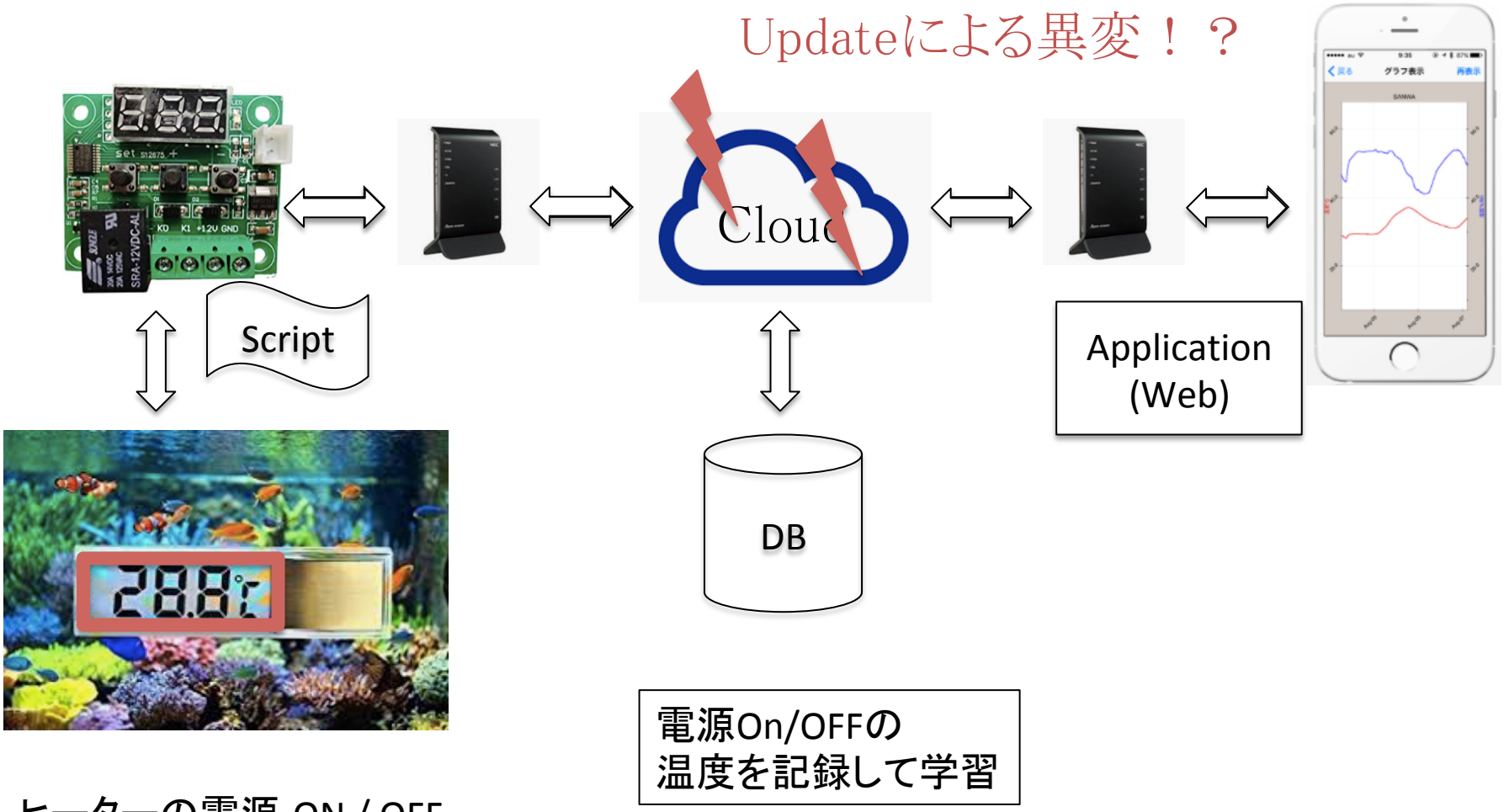
全体図4

リスクとして何を想定すべき？？



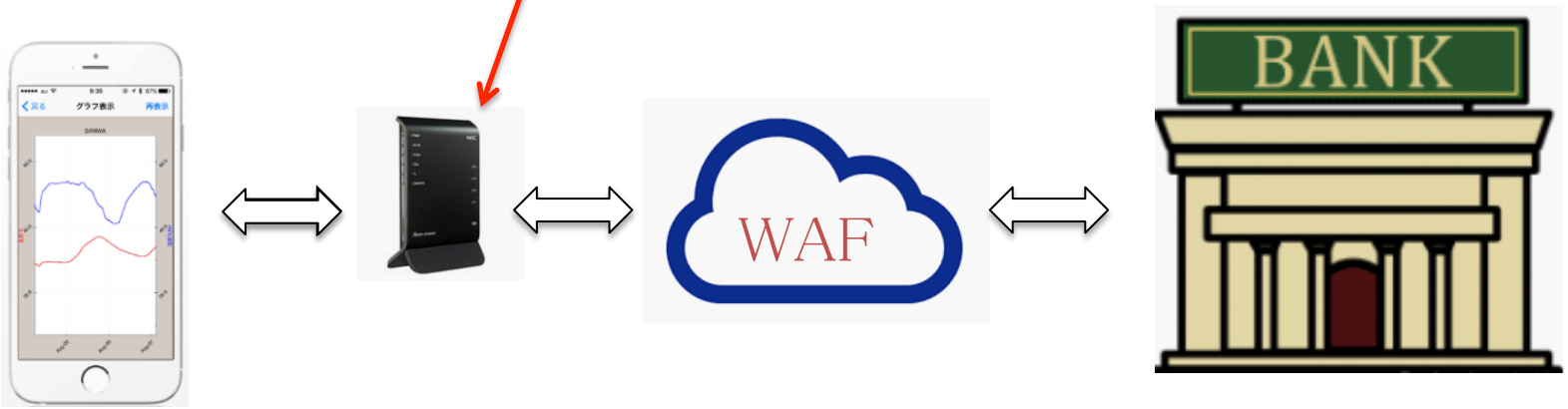
全体図4

リスクとして何を想定すべき？？



サービスに関するセキュリティ

インターネットから設定変更
できないように対策

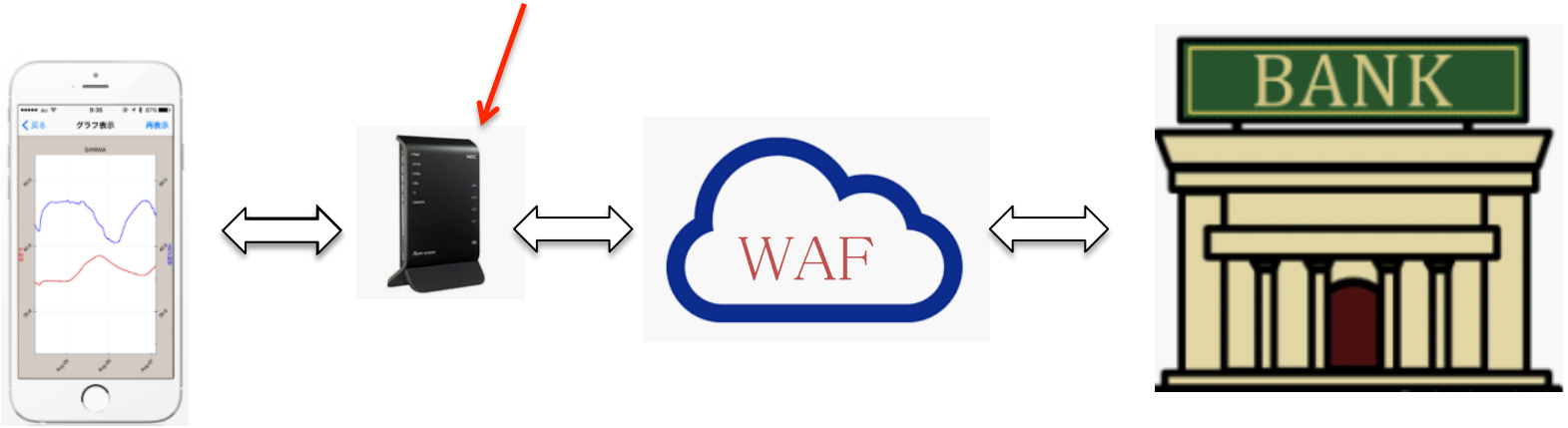


XSS対策

盗聴のリスクはあるか？

サービスに関するセキュリティ

インターネットから設定変更
できないように対策

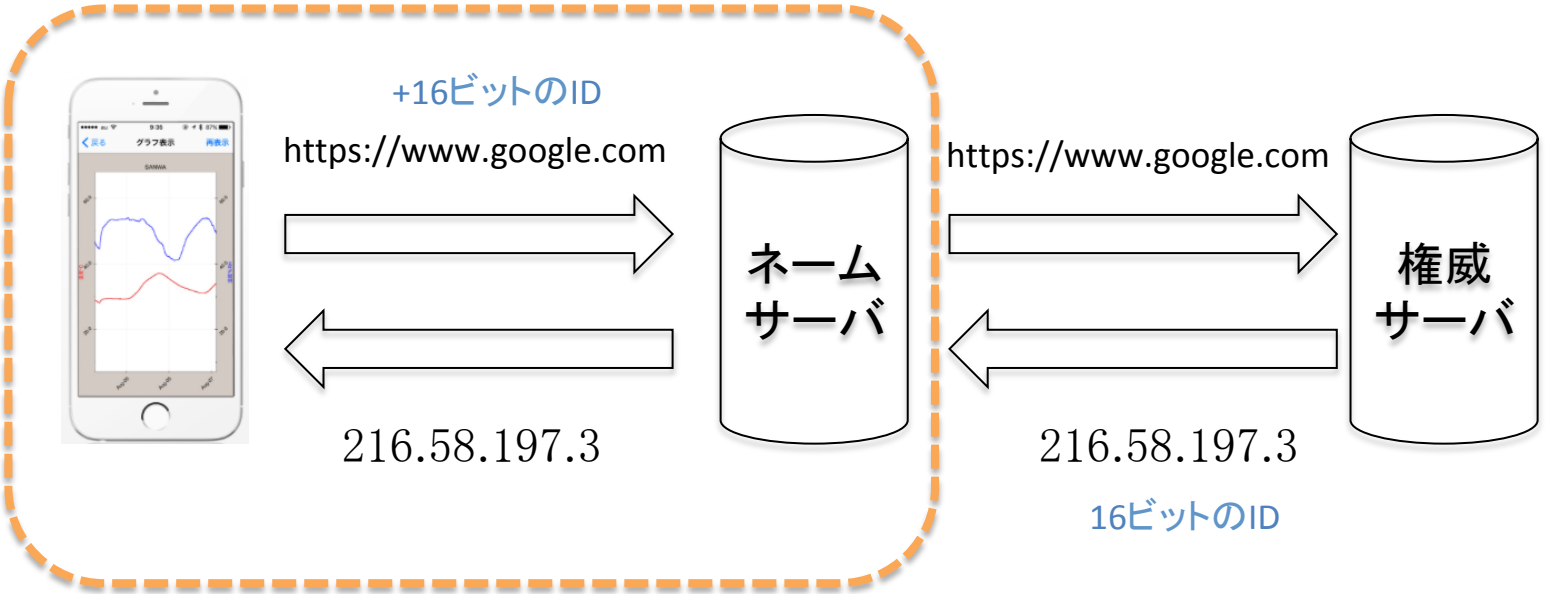


XSS対策

不正送金が発覚！？
どういうリスクがある？

DNSキャッシュポイズニング

DNSとは？



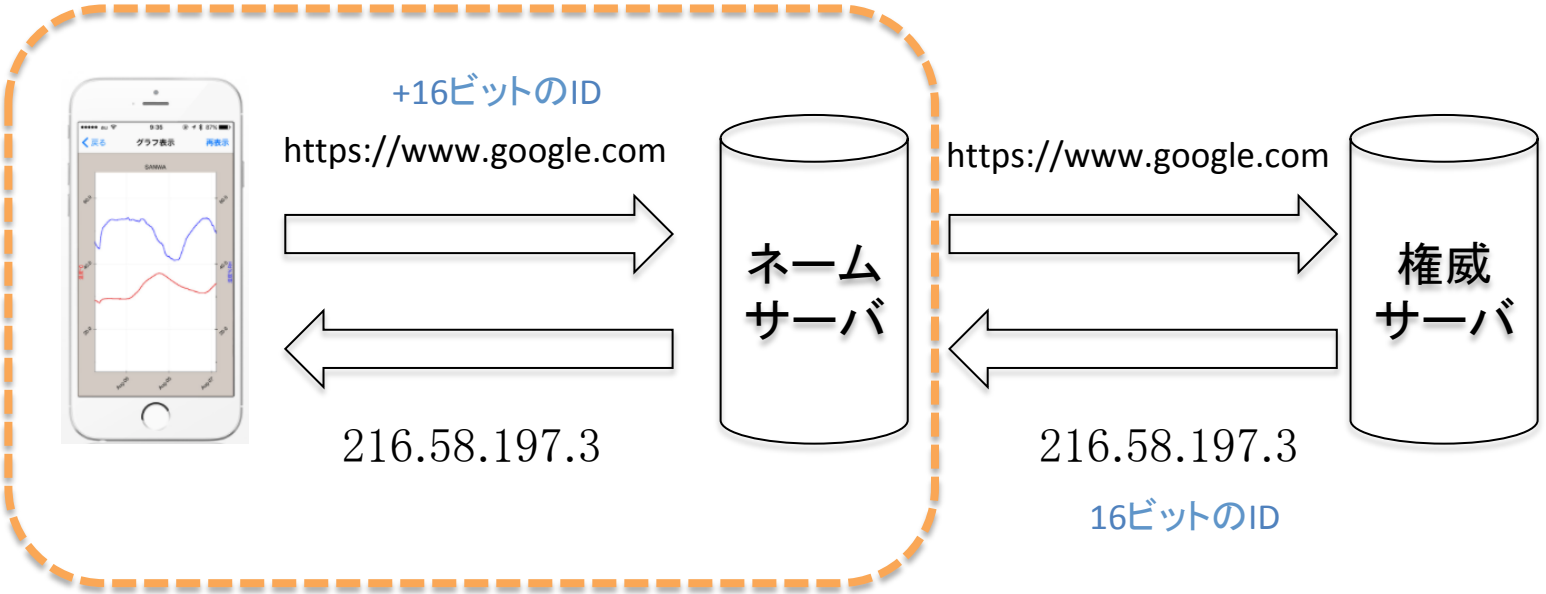
DNSキャッシュ：一時的に保存　TTL(time to live)

効率化！！

保存されているキャッシュを改ざん

DNSキャッシュポイズニング

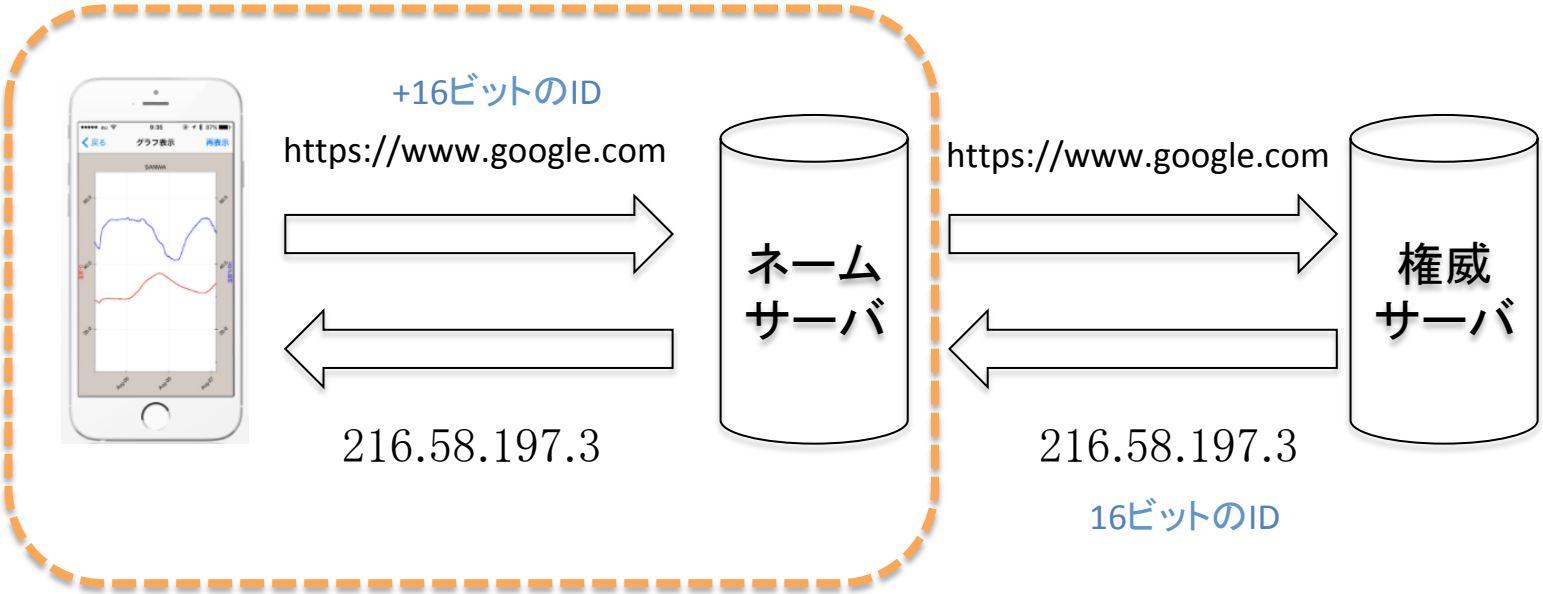
DNSキャッシュポイズニング



通信はUDP:
信頼性や通信の効率性を
提供する機能がない

16ビットのIDが命綱

DNSキャッシュポイズニング



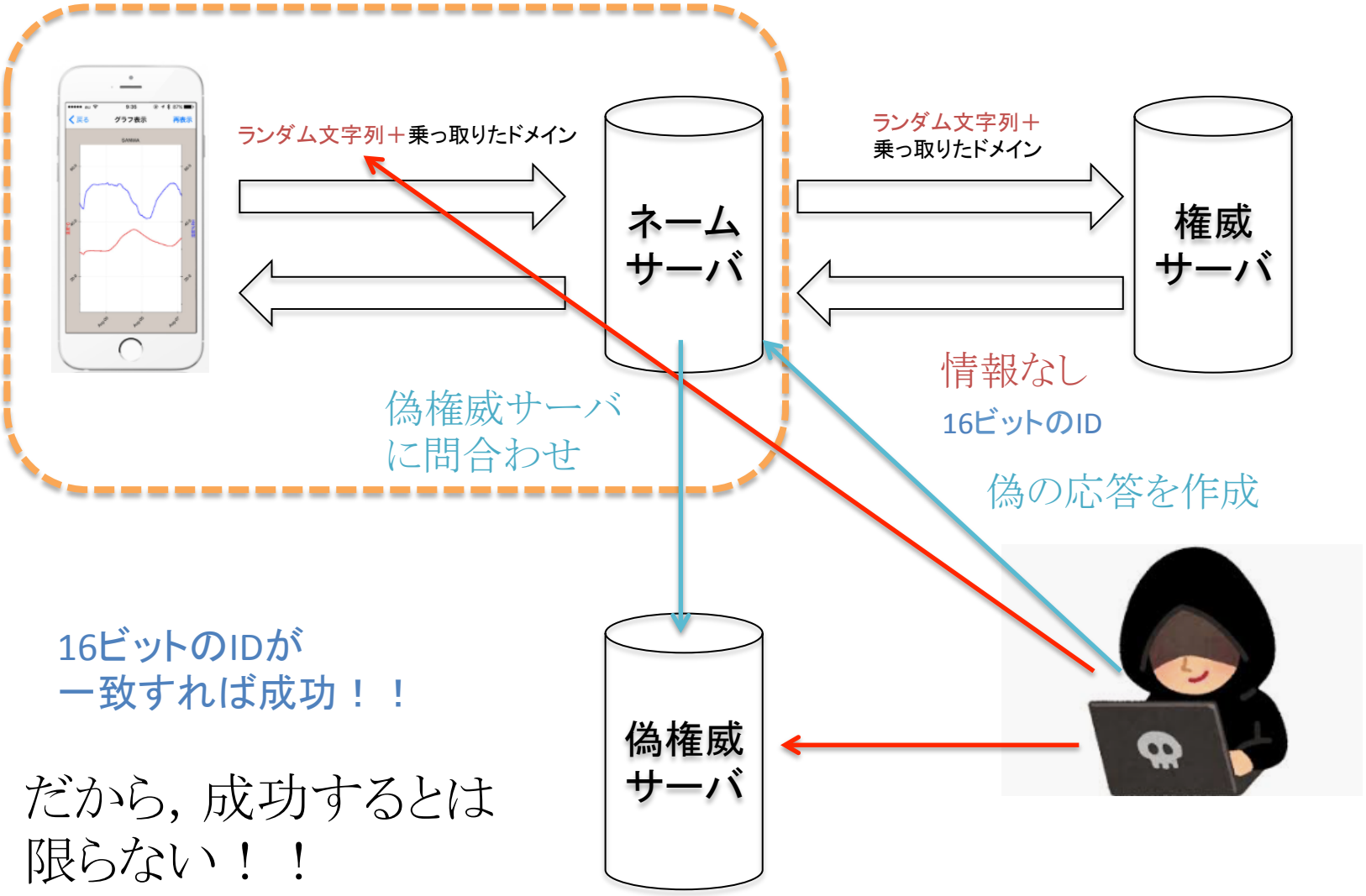
攻撃を成功させるには？

キャッシュサーバが問い合わせで使用したIDと偽装応答パケットのIDを一致させる
権威サーバからの応答よりも早く偽の応答パケットを送り込む
キャッシュに存在しない、あるいはキャッシュの有効期限が切れている時だけ有効

結構難し・・・かった

DNSキャッシュポイズニング

しかし，手強い手法が存在する



だから，成功するとは
限らない！！

DNSキャッシュポイズニング

攻撃が成功した場合、

- Web
- メール
- FTP

など被害は大きい

トレンドマイクロのページ

https://is702.jp/news/3315/

DoS攻撃 (Denial of Service Attack)

サーバーなどのサービスを妨害する攻撃

非常に単純な攻撃例

F5攻撃：

Webページの更新 (リロード) を行う

F5を連打するだけでは無理！？

ではどうする？？

F5攻撃

```
# coding: utf-8

from selenium import webdriver
from selenium.webdriver.common.keys import Keys

cnt = raw_input()

driver = webdriver.Firefox()
driver.get("http://sun.ac.jp")

for i in range(0, int(cnt)):
    driver.find_element_by_tag_name("body").send_keys(Keys.F5)

driver.close()
```

F5攻撃の検知

誰がやっているか分かれば良い

⇨
- IPアドレスを監視
- アクセス回数をカウント
- 一定数以上のアクセス数を超えたら遮断

⇩ 複数の端末から攻撃されたら・・・

DDoS攻撃

Distributed Denial of Service Attack

DDoS攻撃の対策

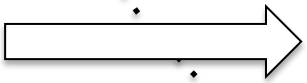
対策は容易ではない・・・

DDoSの実例

リスクをどのように想定する？

Phishing

大まかな全体像



BANK
(正規サイト)

見分けがつかない

Proxy業者
(偽サイト)

日本国内への中継

大量のID/passを販売

Phishingメール

MUFGフィッシング

無線LANブロードバンドルータ

Wi-Fiのタダ乗り

ロジテック製品の脆弱性

前例から考えるIoTセキュリティ

ルーター経由からの侵入：

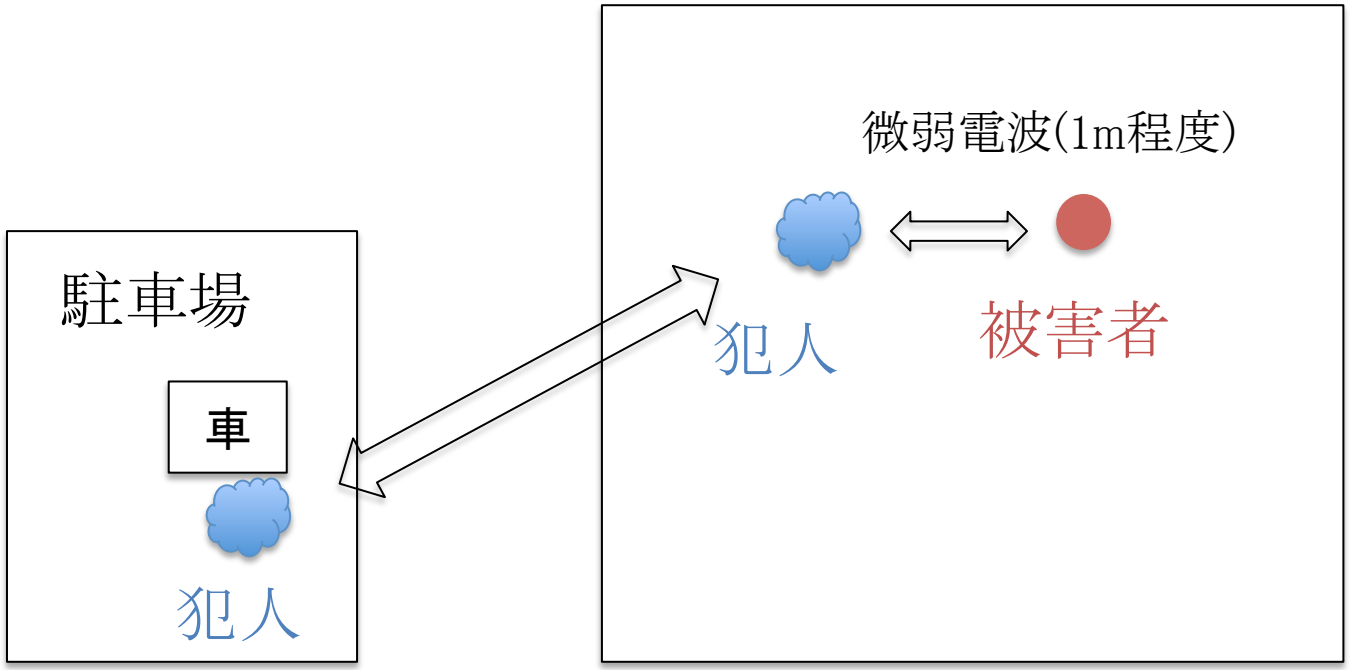
- インターネット経由で設定画面が見えないか？
- Wi-Fiのタダ乗りの危険性はないか？

異常が発生したことにどう気づく？？

対策は，色々と考えられる

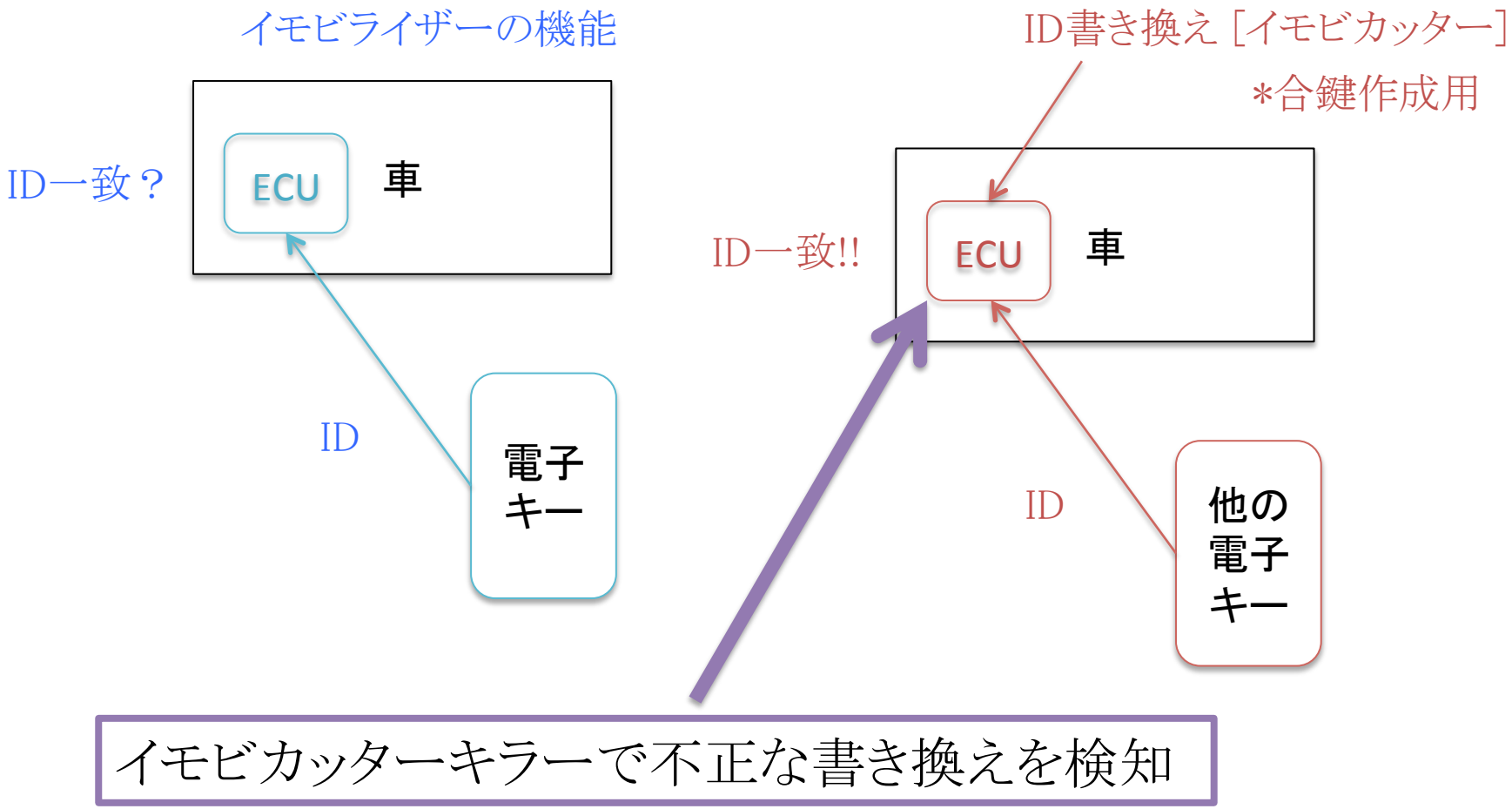
前例から考える車のセキュリティ

リレー アッタク



前例から考える車のセキュリティ

イモビカッター /イモビカッターキラー



前例から考える車のセキュリティ

メーターの改ざん

アナログメーターは取り外して
ダイヤルを回すだけ

中古車を高く売る？？

検知：傷を見つける？？

ディジタルデータの場合は？

ドラログの活用？？
（カーナビのIoT化）

IoTのセキュリティ

サイバー攻撃の現状

Check Point Research：2018 セキュリティ・レポート
http://www.checkpoint.co.jp/resources/cyber-security-report-2018/2018-security-report-web_Low-Reso.pdf

1. 97%の組織が最新のサイバーセキュリティ技術を未導入
2. 94%の企業がモバイルデバイスへの攻撃が増えると予想？
3. 77%のITエンジニアが自社のセキリティ対策に不安を感じている
4. 82%の製造業者が過去1年にフィッシング詐欺に遭っている
5. 防御技術を導入している組織は検知と是正の処理を30%効率化

組織が侵入に気づくまで200日程度かかるという話も・・・

IoTとリアルタイムOS

短時間で決められた処理をこなす（リアルタイム性）

- 処理に優先度がある
- 優先度が高い処理は低い処理の実行権を横取りできる

ソフトバンクのページ ⟹ IoT機器のOSは、Windows CE

IoTとリアルタイムOS

Windows CE

Sharpのページ

電子辞書にも
利用されている

http://www.sharp.co.jp/support/dictionary/product/pw-hc6.html

RTOS

日本製のOS「トロン」

マイクロTカーネル2.0 (ワンチップマイコン向け)がIEEEで
世界基準規格に！！

日本のOSのメリットは？？

IoT機器の導入について

システムデザインの設計やセキュリティ評価だけでは不十分！？