\Orchestrating a brighter world NEC

参考資料4

「IT/IoTセキュリティ実践講座」教育プログラム実証講座

オリエンテーション(第二段階)

2019年11月15日 実施

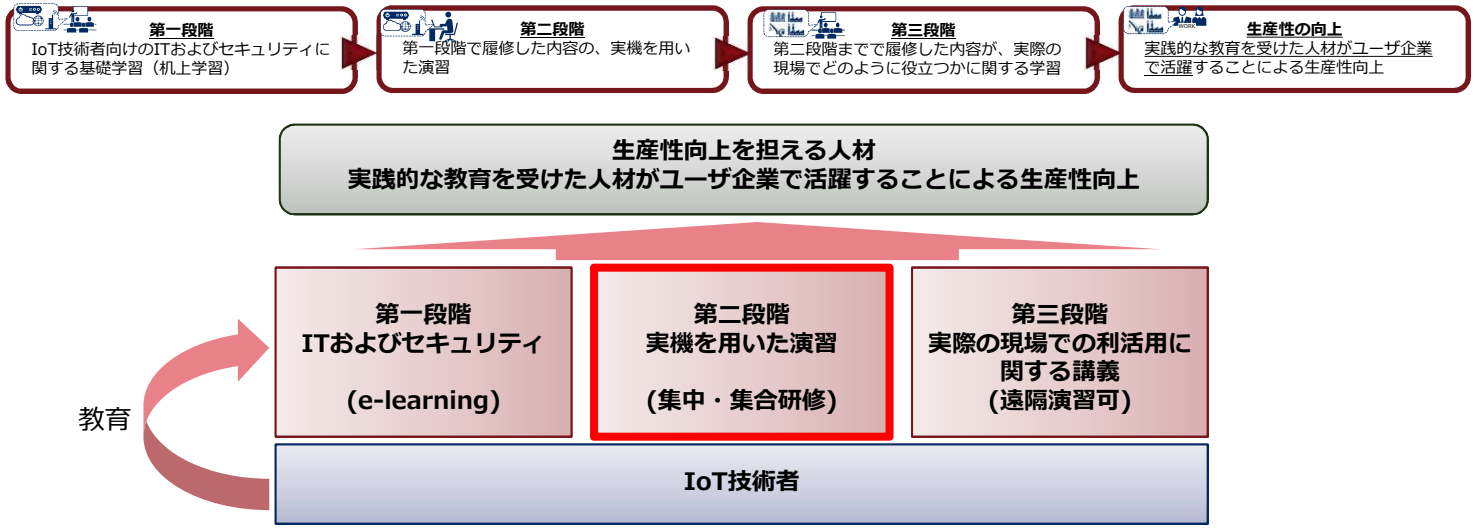
目次

1.今回の第二段階について

1-1.第二段階の到達目標

第二段階の目的

下記の3段階を想定した教育訓練プログラムを受講することにより、教育を受けた人材が企業で活躍できるように、実践的な知識・技術を習得する。



到達目標

1. **第一段階のe-ラーニングで学んだ知識に関する実践力を獲得する**
2. **デバイスに残っている脆弱性とその対象に関する、対策方法を体得する**
3. **IoTセキュリティの重要性を、実社会（スマートホーム）での活用例を通じて、理解を深める**

1-2.第二段階の時間割

1日目　11/15(金)	
時間	項目
10:00 ～ 10:30	**オリエンテーション**
10:30 ～ 11:00	**自己評価（第二段階受講前）**
11:00 ～ 12:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**
12:00 ～ 13:00	**昼休み**
13:00 ～ 17:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**

2日目　11/16(土)	
時間	項目
10:00 ～ 12:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**
12:00 ～ 13:00	**昼休み**
13:00 ～ 13:30	**【講義】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として**
13:30 ～ 17:00	**【実習】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として-**

3日目　11/17(日)	
時間	項目
10:00 ～ 12:00	**【実習】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として- （2日目の午後の続き）**
12:00 ～ 13:00	**昼休み**
13:00 ～ 13:30	**試験の説明**
13:30 ～ 16:30	**実機による試験、試験解答の解説、第二段階の総まとめ**
16:30 ～ 17:00	**自己評価（第二段階受講後）**

1-3.第二段階の実施内容

第一日目～第二日目午前

1. オリエンテーション
2. 実施前自己評価
3. 第二段階で学習するシステムの概観
   - ① 今回の実習環境を適用する環境の利用シーンについて（スマートホーム）
   - ② 一般的な IoT システムの構成要素について
   - ③ スマートホームで利用するプロトコルについて
4. Raspberry Pi上でECHONET Liteを用いたセンサ&LEDの制御
5. データ収集&可視化システムの構築
6. Web インタフェースを用いたデータ検索
7. Wireshark を用いた通信フレームの内容確認

第二日目午後～第三日目午前

8. IoTシステムのセキュリティ
   - **① デバイスに含まれる一般的な脆弱性とその対処**

第三日目午後～

9. 実機による試験
10. 実施後自己評価

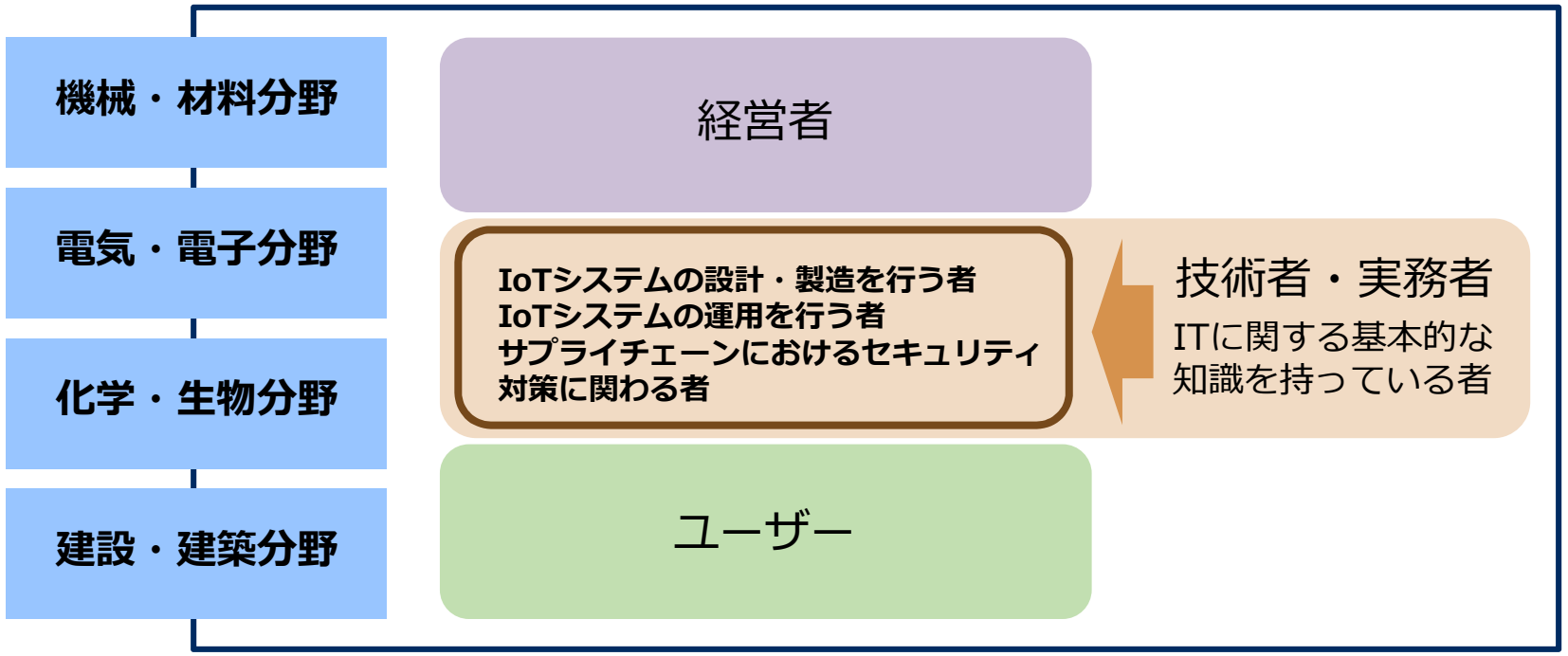
1-4.本講座で育成を目指す人材像

9/13オリエンテーション資料
より引用

本講座では、IT/IoT利用とそのリスクを理解し、各産業分野の特徴を理解した設計・構築・運用のセキュリティ対策が行える人材を育成するための教育プログラム・コンテンツを開発し、キャリアアップを目指すリカレント人材が実践的な知識・技術を習得できる教育訓練プログラムを確立することを目指す。

対象受講者

- **IoTシステムの設計・製造を行う者**
- **IoTシステムの運用を行う者**
- **サプライチェーンにおけるセキュリティ対策に関わる者**



2.今回テーマとするIoTシステムについて

2-1.IoTシステムの概観

2016年の情報通信審議会資料より

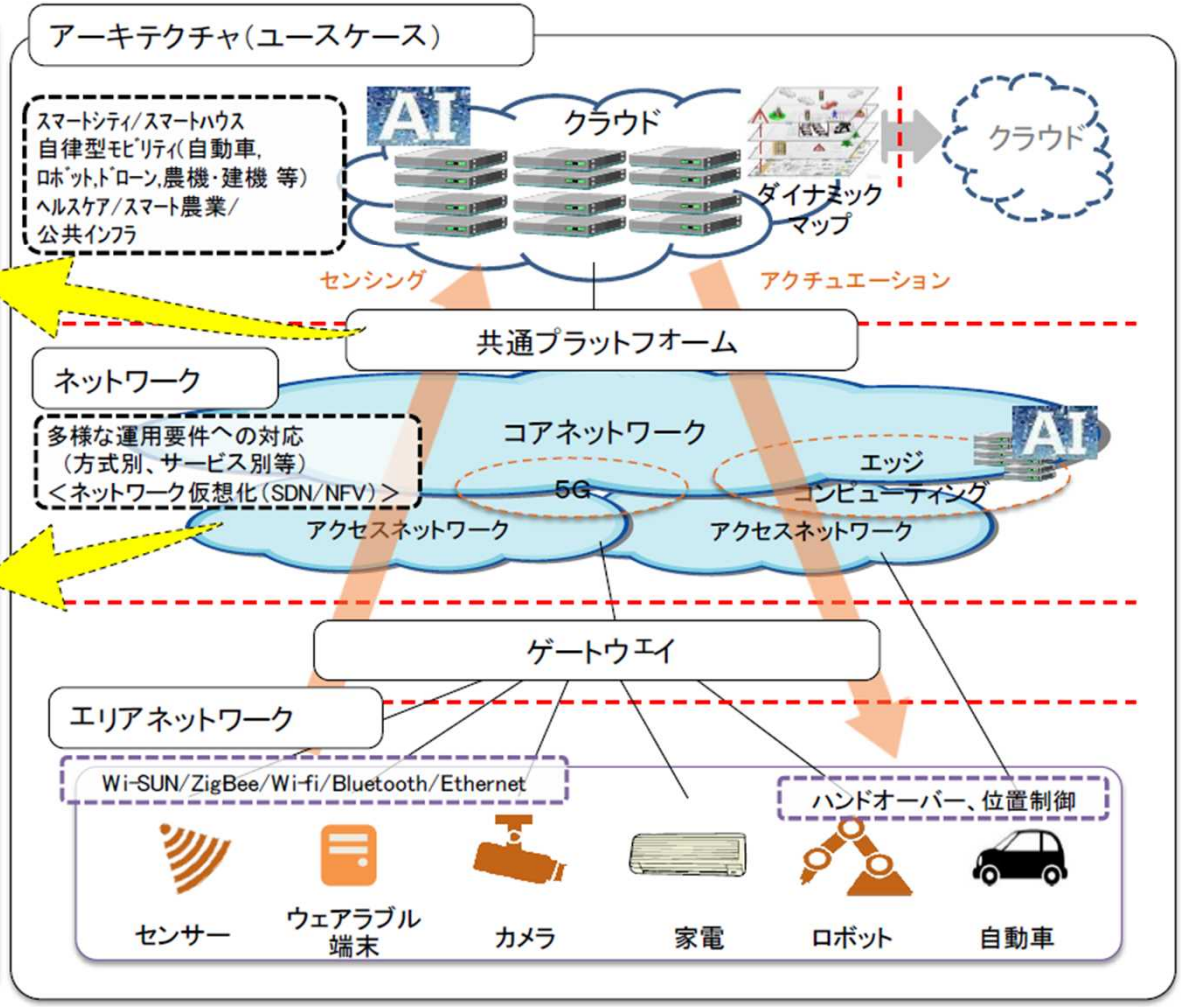
IoT/BD/AI時代の先端IoTシステムの共通プラットフォーム・共通基盤技術の開発

25

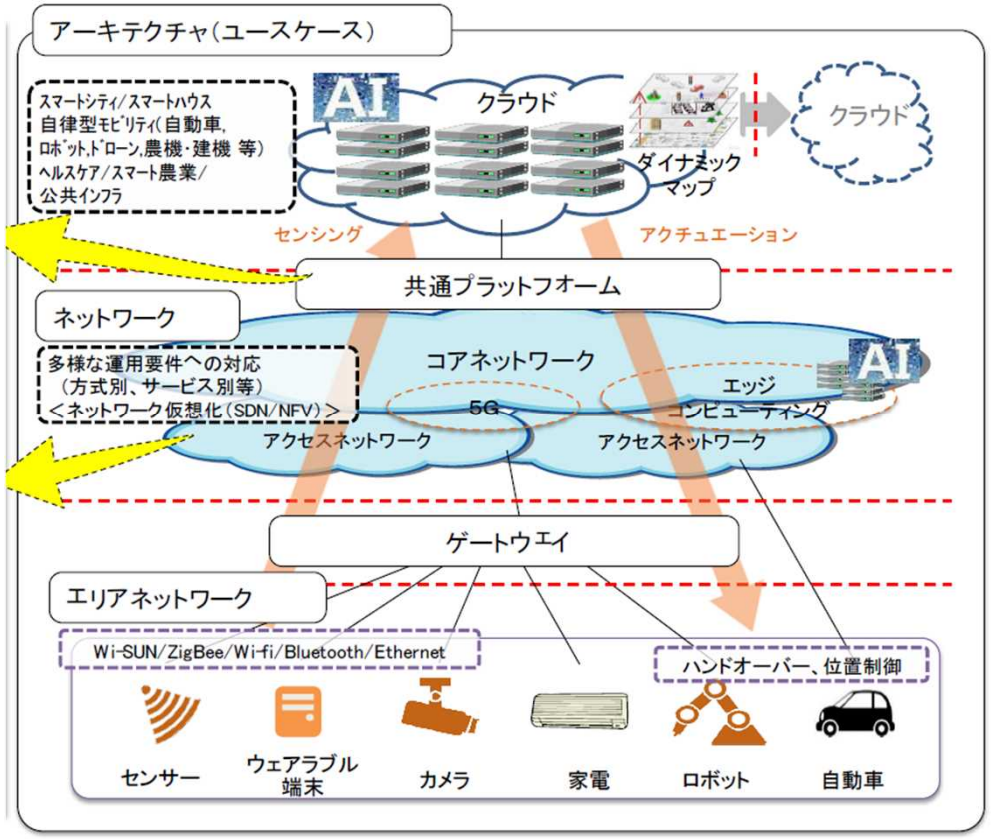
＜取組の方向性＞

◆ 特定サービス毎の垂直統合による囲い込みに対応するため、
① 特定サービスに依存しない、データ収集・利用、デバイス管理
② 異なるベンダー間の相互接続性
③ サービスの重要度に応じたネットワークの資源配分と接続の信頼性確保
を可能とする**IoT共通プラットフォームの実現**。

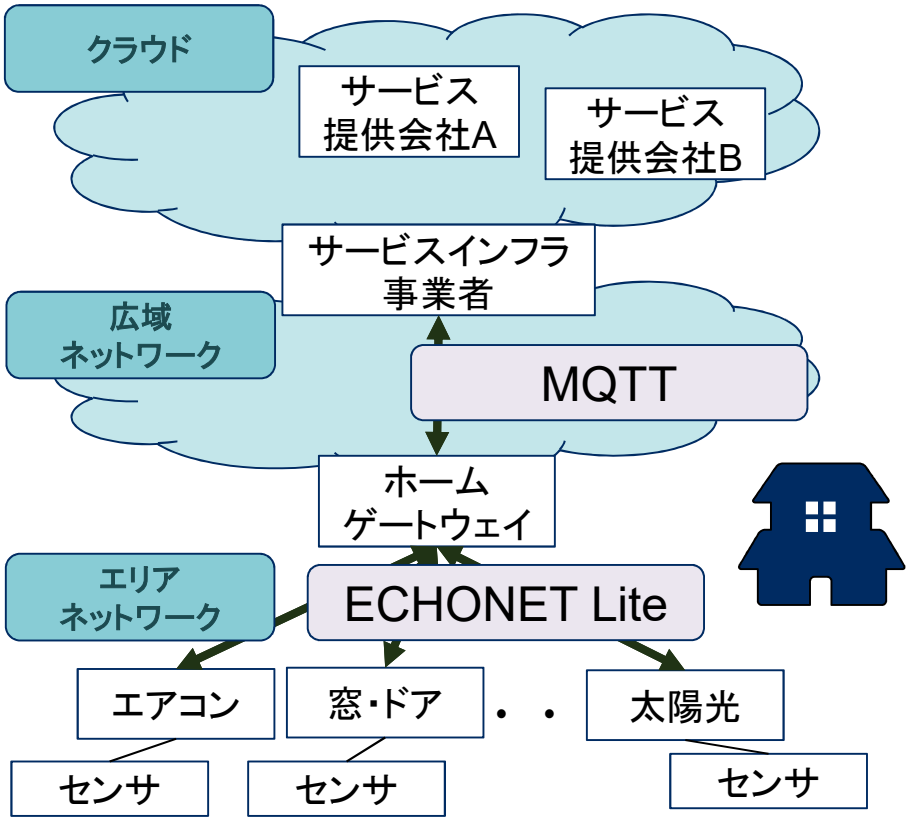
◆ 先端IoTシステムの実現に必要な**共通基盤技術の開発**。
＊超低遅延（1ms程度）
＊超高速（10Gbps）
＊超多数同時接続（100万台/km²）
＊自動走行（100km/h,128台/km²）
＊次世代AI（AI＋脳科学）
＊ユースケースに即した上記機能の選択・対応　等



2-2. IoTシステムの全体像と今回の実習テーマ

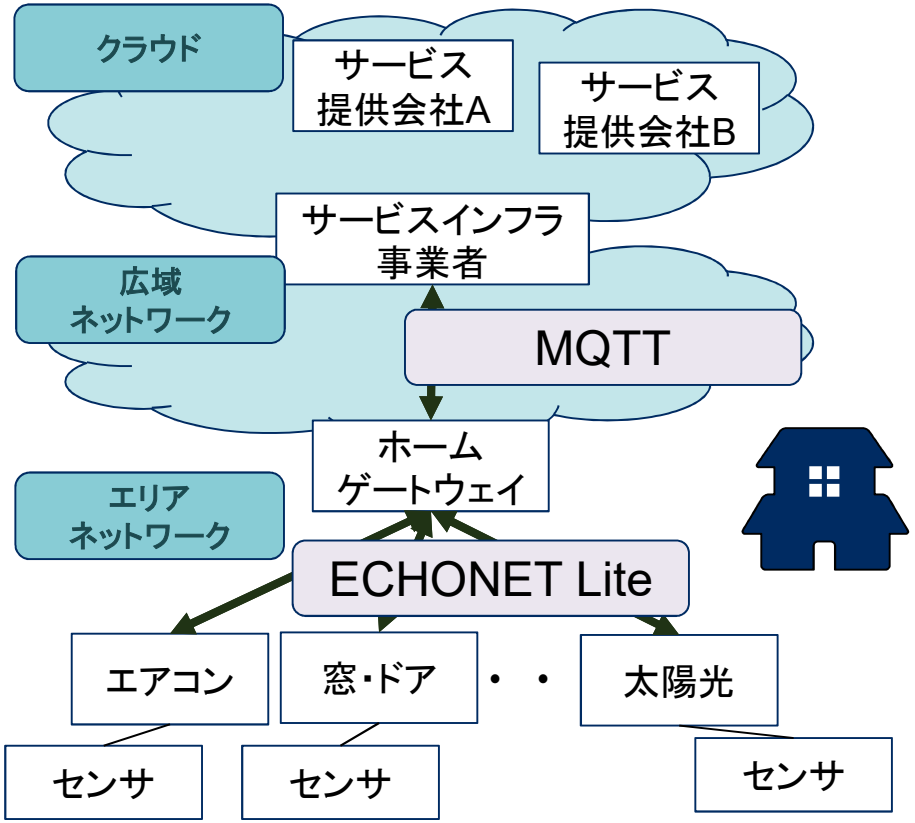


IoTシステムの全体像

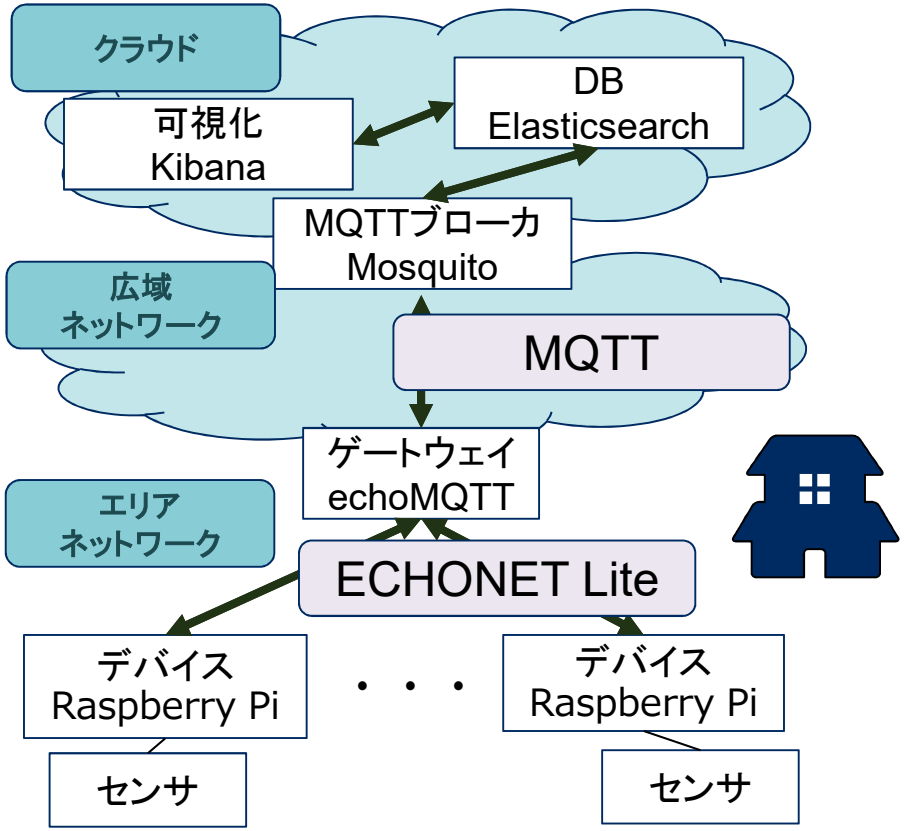


今回の実習テーマ
「スマートホーム」

2-3.今回の実習テーマと実機環境(1)



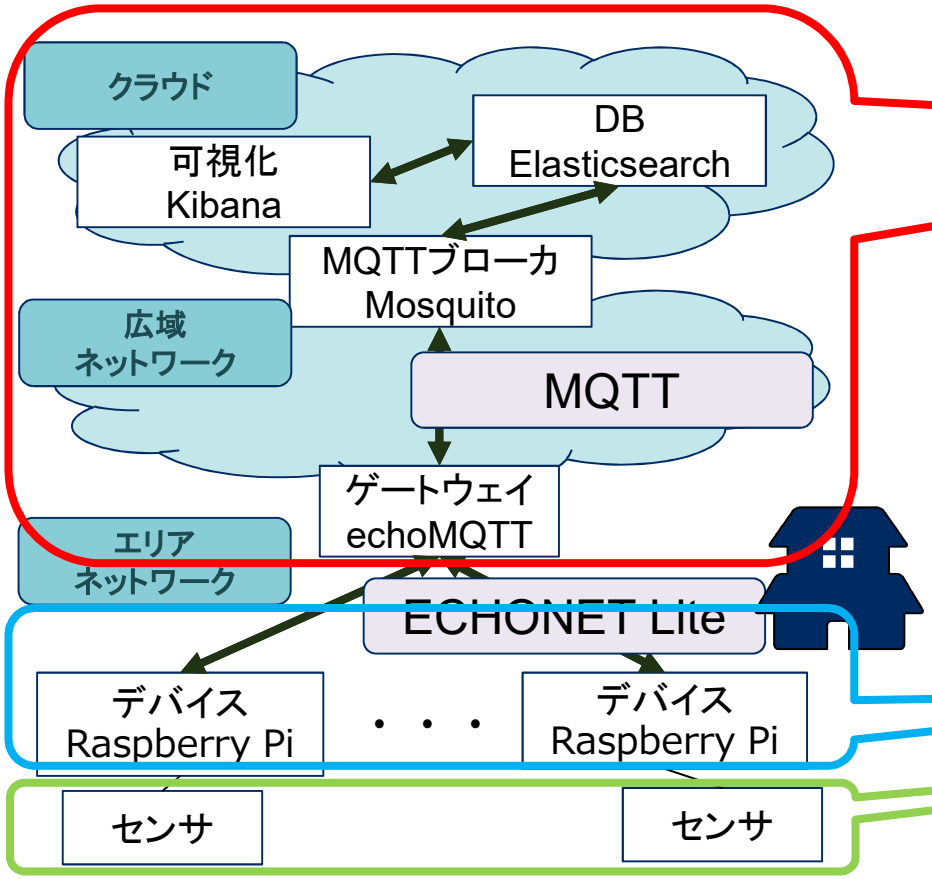
今回の実習テーマ
「スマートホーム」



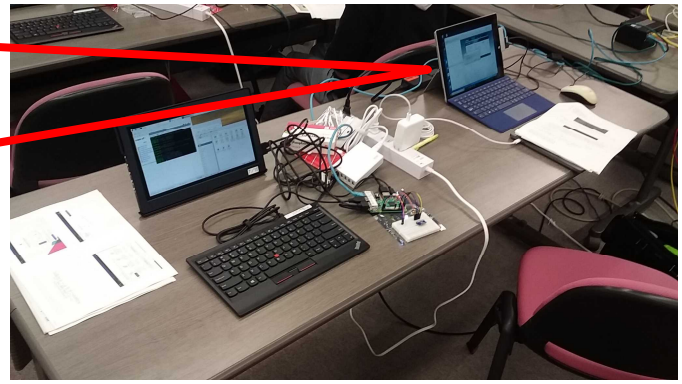
今回の実機環境

今回実習を行っていただく実機環境は、IoTシステムの要素が一つに纏まったものです

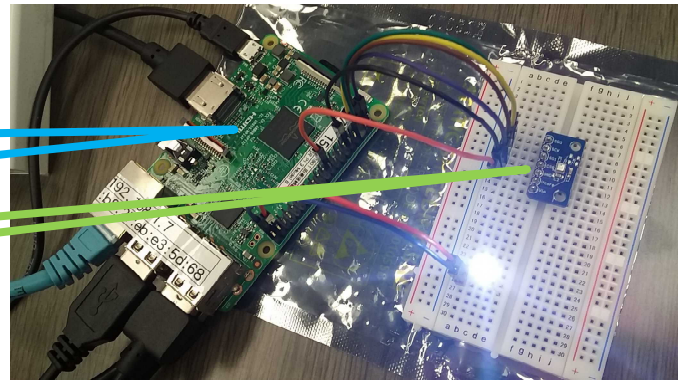
2-3.今回の実習テーマと実機環境(2)



今回の実機環境



受講者毎の実機構成



Raspberry Piとセンサ類

3.第二段階の実機テストについて

3-1.第二段階の実機テストについて

1日目　11/15(金)	
時間	項目
10:00 ～ 10:30	**オリエンテーション**
10:30 ～ 11:00	**自己評価（第二段階受講前）**
11:00 ～ 12:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**
12:00 ～ 13:00	**昼休み**
13:00 ～ 17:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**

2日目　11/16(土)	
時間	項目
10:00 ～ 12:00	**【講義・実習】IoTシステム開発の基礎と実践 ラズパイ環境の説明**
12:00 ～ 13:00	**昼休み**
13:00 ～ 13:30	**【講義】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として**
13:30 ～ 17:00	**【実習】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として-**

3日目　11/17(日)	
時間	項目
10:00 ～ 12:00	**【実習】IoTシステムにおけるセキュリティ-スマートホーム技術におけるIoTシステムを例として- （2日目の午後の続き）**
12:00 ～ 13:00	**昼休み**
13:00 ～ 13:30	**試験の説明**
13:30 ～ 16:30	**実機による試験、試験解答の解説、第二段階の総まとめ**
16:30 ～ 17:00	**自己評価（第二段階受講後）**

3-2.第二段階の実機テストについて

演習（試験）の問題例

- 試験で対応した脆弱性と実施した対策を、各々100文字以内で説明してください。

- 脆弱性に対して、対策を実装してください。
  - 採点方法：講師側から攻撃を行い、対策が出来ているかの確認を行う


Orchestrating a brighter world
NEC

第二段階講義前後における自己評価質問票

参考資料5

下記の設問に関し、ご自身がどれくらいのスキルを有するか、自己評価で自分に近いと思われるレベルを選択してください
（文章の記載の無い偶数のレベルについては、前後の奇数の中間のレベルと考えてください）

1. IoTシステム開発の基礎と実践について

1-1. Linuxの操作

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-2. SSHによる通信

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-3. I2C通信

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-4. RaspberryPIの基本的な操作

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-5. RaspberryPIのIOを用いた入出力

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-6. ECHONET Liteによる制御

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-7. MQTTによる制御

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

1-8. Kibanaによるデーターの可視化

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

下記の設問に関し、ご自身がどれくらいのスキルを有するか、自己評価で自分に近いと思われるレベルを選択してください
（文章の記載の無い偶数のレベルについては、前後の奇数の中間のレベルと考えてください）

1. IoTシステム開発の基礎と実践について

1-9. Elasticsearchによるデーターベースの構築

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2. IoTシステムにおけるセキュリティについて

2-1. デバイスへの攻撃で受ける影響

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-2. デバイスへの攻撃に対する一般的な対処

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-3. ゲートウェイへの攻撃で受ける影響

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-4. ゲートウェイへの攻撃に対する一般的な対処

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-5. クラウドへの攻撃で受ける影響

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-6. クラウドへの攻撃に対する一般的な対処

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-7. デバイスへの不正ログイン

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

下記の設問に関し、ご自身がどれくらいのスキルを有するか、自己評価で自分に近いと思われるレベルを選択してください
（文章の記載の無い偶数のレベルについては、前後の奇数の中間のレベルと考えてください）

1. IoTシステム開発の基礎と実践について

2-8. デバイスのプロパティ値変更

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-9. センサの状態偽装

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-10. 不正センサデータ送信

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

2-11. ポートスキャン

9	8	7	6	5	4	3	2	1
技術を使った業務をチームのリーダーとして遂行することができる		技術を使った業務を遂行することができる		説明することができる		聞いたことがある		全く知らない
0	0	0	0	0	0	0	0	0

参考資料6

IoTシステムにおけるセキュリティ
- スマートホーム技術におけるIoTシステムを例として -

北陸先端科学技術大学院大学 / 情報通信研究機構
丹　康雄

2019.11.16

自己紹介

総務省 情報通信審議会 専門委員
スマートIoT推進フォーラム 技術戦略検討部会　技術・標準化分科会長
情報通信技術委員会(TTC)　特別委員
ITU-T Academia Member Focal Point
ISO/IEC JTC1 SC41 Committee Member / 情報規格調査会 SC41専門委員会　委員
ECHONETコンソーシアム　アドバイザリフェロー
JEITA スマートホーム部会　部会長
IEC TC100 expert / JEITA 客員
スマートコミュニティアライアンス(JSCA)　通信インタフェース SWG　座長
電気学会SGTEC 委員 (IEC TC57 国内委員)
DCアライアンス　議長
内閣府 近未来技術実装有識者会議　委員
北陸先端科学技術大学院大学　　副学長(リカレント教育担当)、CIO
　　高信頼IoT社会基盤研究拠点　拠点長
　　先端科学技術研究科　教授
国立研究開発法人　情報通信研究機構　招聘専門員
早稲田大学　非常勤講師

IoTとは何か

1. 実世界の状況を情報として取得したり、実世界の状況を変化させることのできる要素が、
2. 大規模な記憶容量と、極めて高度な処理能力を有する、大規模な情報処理機構と、
3. 通信ネットワークで常時接続されている

ような情報システム(というか社会基盤)がIoTと今現在呼ばれているもの

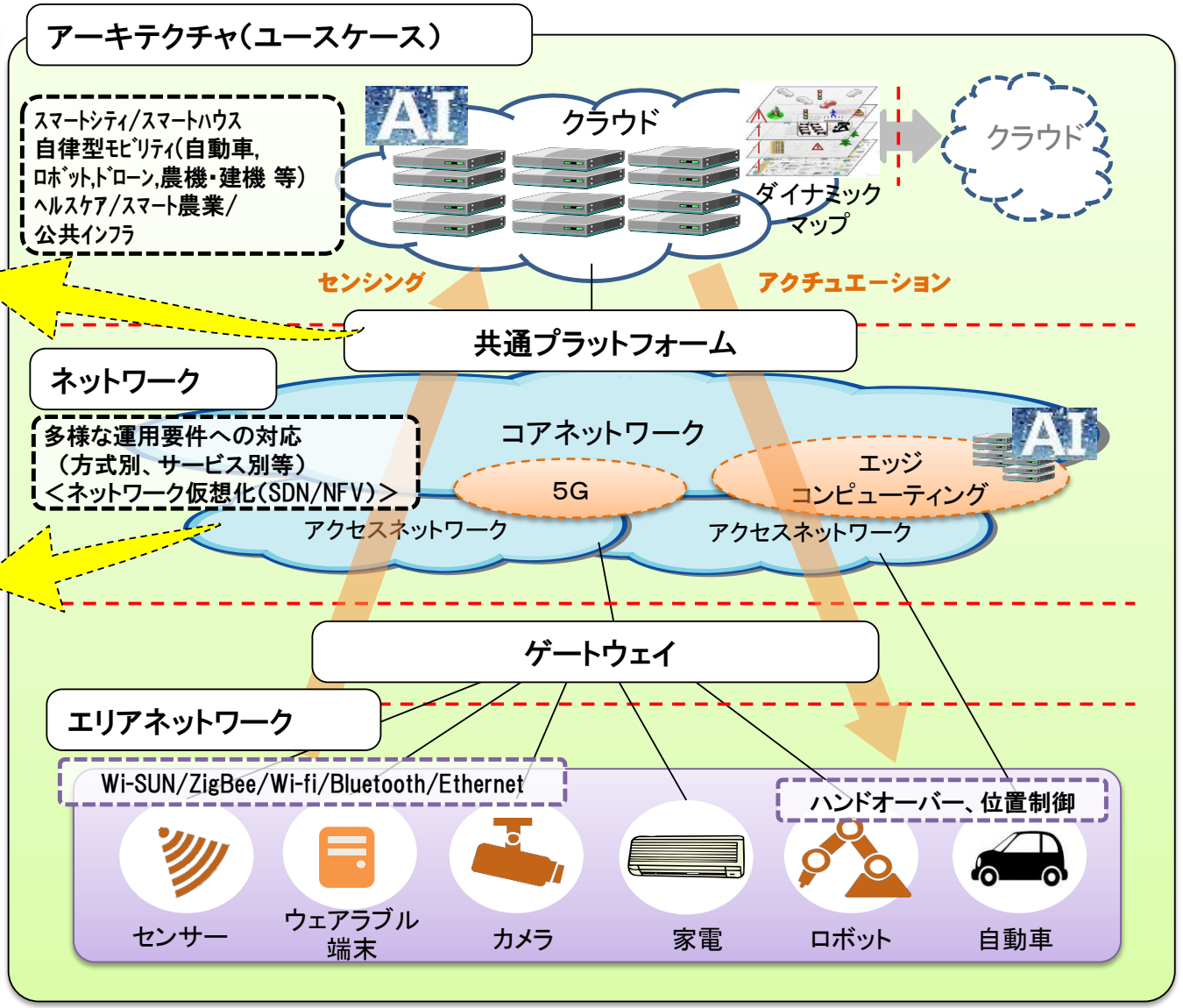
- ITU-T Y.4000(Y.2060) Overview of the Internet of things (2012.06)
- ISO/IEC 30141 Internet of Things (IoT) – Reference architecture (2018.08)

IoT/BD/AI時代の先端IoTシステムの共通プラットフォーム・共通基盤技術の開発 25

＜取組の方向性＞

◆ 特定サービス毎の垂直統合による囲い込みに対応するため、
① 特定サービスに依存しない、データ収集・利用、デバイス管理
② 異なるベンダー間の相互接続性
③ サービスの重要度に応じたネットワークの資源配分と接続の信頼性確保
を可能とするIoT共通プラットフォームの実現。

◆ 先端IoTシステムの実現に必要な共通基盤技術の開発。
＊超低遅延（1ms程度）
＊超高速（10Gbps）
＊超多数同時接続（100万台/km²）
＊自動走行（100km/h,128台/km²）
＊次世代AI（AI＋脳科学）
＊ユースケースに即した上記機能の選択・対応　等

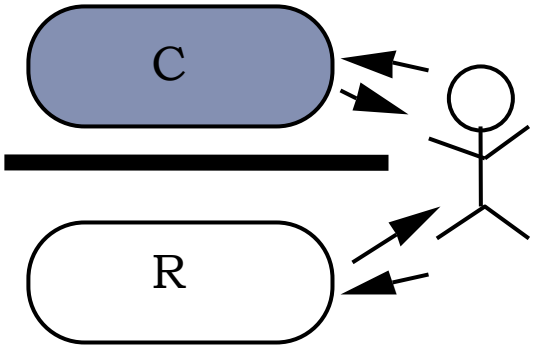


現在に至る情報システムの発展の流れ

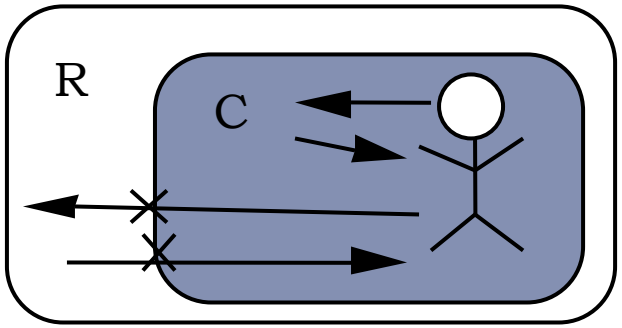
- 1980年代からの実世界指向コンピューティング
  - ユビキタスコンピューティングへの流れ
  - 1990年代には実現
  - 物理世界と計算機世界(仮想世界)との連携
- 2000年前後からのネットワークの浸透
  - 常時接続ブロードバンドインターネットの普及
  - 接続技術の進展と、組込みシステムの高度化
  - 複合的なシステムにならざるを得ない状況に
- Web2.0(2005年)以降のネット内の強力なインテリジェンス
  - 現在のビッグデータ解析に至る急速な流れ
  - 2012年にディープラーニングという形で学習機械のリバイバル
- 2014年頃から上記3つが組み合わされたIoTシステムの存在感が増大
  - 第一次産業をはじめとする全産業への展開、社会システムの見直し
  - ISO, IEC, ITUといった国際標準機関での標準制定
- Industrie 4.0、Society 5.0など、国をあげての取り組み
  - 仕事のしかたや社会的な制度の見直し、職業観の変化といったところまでも

ユビキタス
他のアプローチとの比較

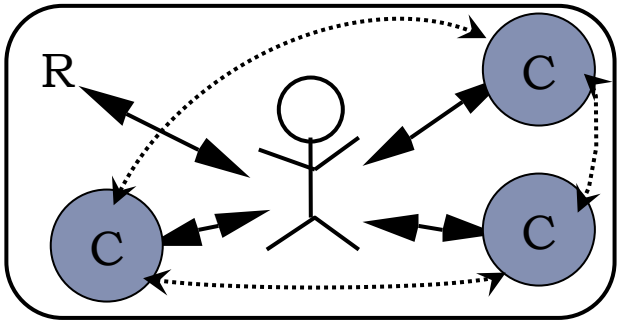
- 我々の住む実世界にネットワーク機能も含めた計算機内の仮想世界を持ち出す



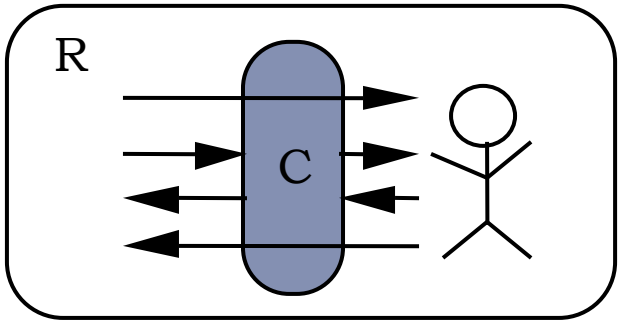
(a) GUI



(b) Virtual Reality



(c) Ubiquitous computing



(d) Augmented/Mixed Reality/Virtuality

Web2.0の変革ポイント

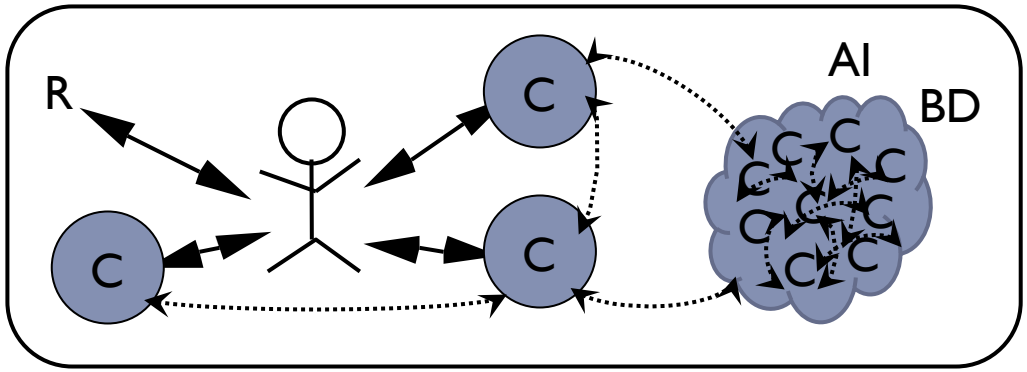
- 価値を持つもののシフト
  - 最初はハード
    - IBM PCが、いわばオープンソースハードとして登場することでコモディティ化が進み、一番価値のあるものではなくなる
    - Windows, Officeのようなソフトに価値が移る
  - 次はソフト
    - Linuxに代表されるオープンソースの流れがソフトのコモディティ化をもたらす
    - ソフトではなく、利用者がどのように使うか、何をするかのデータに価値が移る
- データこそが現在の価値の源泉
  - 「集合知」 2006年くらいの流行語
  - 何かの目的のために誰かがコストをかけて集めたデータではない
  - 利用者がそれぞれの目的のために活動すると、自動的にたまっていくデータ
    - かな漢字変換への自分の名前の登録
  - 現在では、テキストに代表される高次概念のデータからセンサデータに代表される生データへのシフト
  - データの目的外利用こそがポイント

IoTという新しい段階への到達

- ユビキタスコンピューティングが前世紀末にほぼ実現してしまった際、そのままではあまり役に立ちそうもないことも明らかになってきた
- 足りなかったのは「インテリジェンス」
- テキスト(文字)が中心のインテリジェンスはWeb2.0として姿を現しつつあった
- ユビキタスコンピューティングにWeb2.0をくっつけたようなものが必要なのは自明となり、それを何という名称で呼ぶかについては多くの議論が起こった。日本で「スマートユビキタス」という言葉が作られたのもその一つ
- Web2.0の時代からビッグデータ処理、2012年の深層学習などを経て、テキストではない生データに対するインテリジェンスが語れる段階に入り、機は熟した

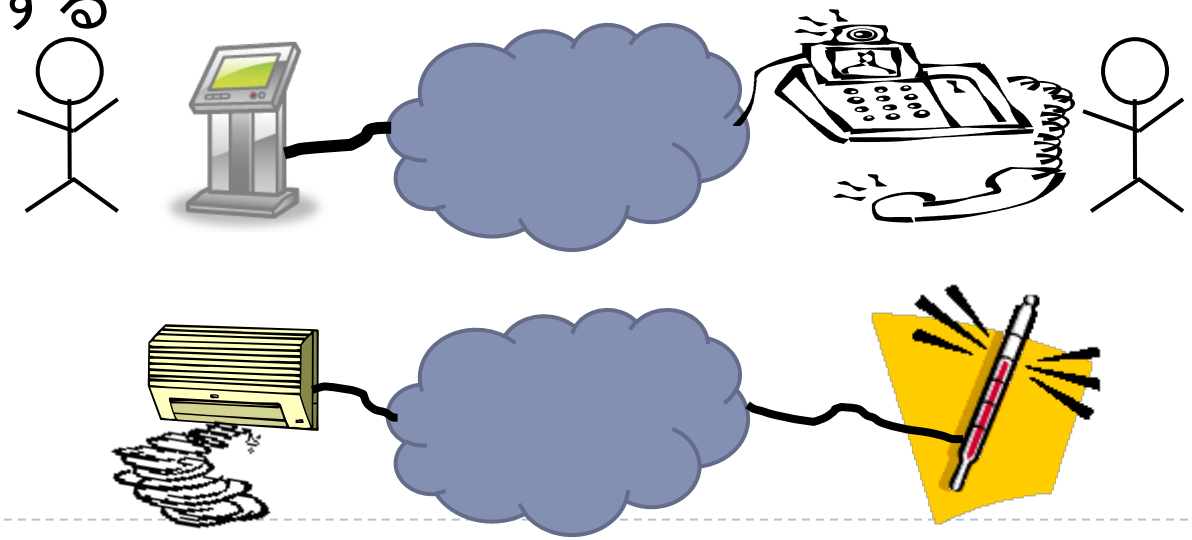
IoTシステム

- 従来型の計算機(IT)システムとも、組込み計算機(ET)システムとも異なる
- その二つの融合した形態に近い
  - 実世界とのやりとりがあること
    - センサ　アンド　アクチュエータ
    - CPS(Cyber Physical Systems)
  - ネットワークを利用し、個々の要素が連携すること
    - M2M(Machine to Machine), IoT(Internet of Things), IoE(Internet of Everything)
    - SoS(System of Systems)
  - インテリジェンスがネットワークのどこかにあること
    - クラウド
    - ビッグデータ

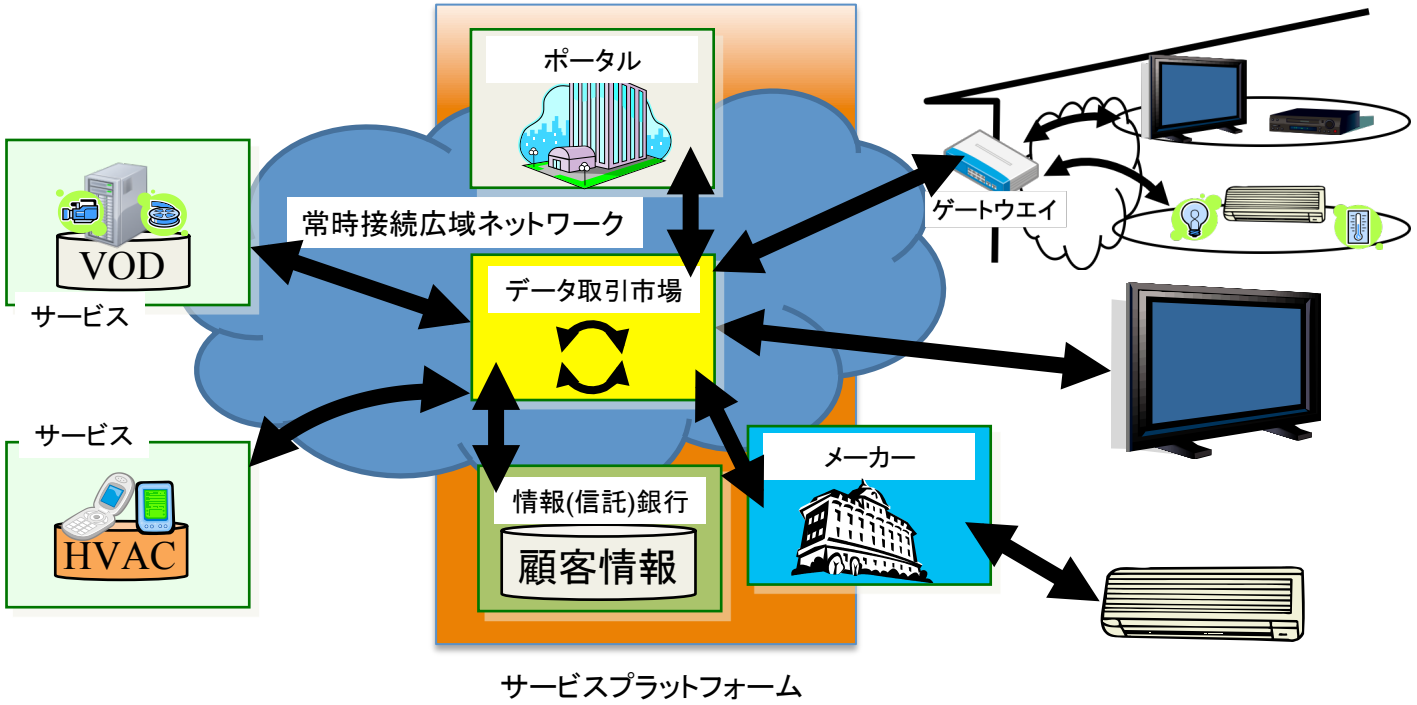


Machine to Machine (M2M)の通信

- ヒトとヒトではなく、モノとモノの通信
- ヒトとヒトの通信でも両側に端末が存在するが、ヒトがインテリジェンスを持つ
- M2Mの場合には端末の後ろにヒトがいない
  - 高度な状況判断ができるヒトが通信のすぐそばにいない
- ヒトとモノが同じ空間内に存在していることで間接的にヒトに貢献する



最近の日本型スマートホームシステム



2019年10月開始の一般家庭向け補助金

経済産業省平成30年度補正予算「生活空間におけるサイバー/フィジカル融合促進事業費補助金」

LIFE UP プロモーション

つながることで、広がる未来がある。

住まいの設備や身近な家電等が
インターネットとつながることで、
あなたの毎日をバージョンアップする
「スマートライフ」の世界。

つながるIoT家電・機器や
情報プラットフォームと連携した
サービスを生み出すさまざまな事業を
サポートする取組みが、
「LIFE UPプロモーション」です。

「LIFE UP プロモーション」とは？

対象のIoT家電・機器を活用したサービスを利用している消費者に対して、ポイント・ディスカウント等の特典を付与する販促活動費用の一部を補助する事業です。2019年10月1日より各社の事業が開始します。

「LIFE UP プロモーション」の特典の受け取り方

対象サービス※1の契約 ▶ 一定期間※2の継続利用 ▶ ポイント・ディスカウントなどの特典がもらえる

※1 対象サービス一覧は裏面下WEBページを参照　※2 コンソーシアムによって個別に条件が異なります。

「LIFE UP プロモーション」の対象機器・サービスのイメージ

LIFE UP プロモーション対象サービス

シャープコンソーシアム

■ サービス例

ヘルシオの調理履歴から好みを学習し、ぴったりなおすすめメニューを提案します。

■ LIFE UP プロモーション特典例

商品券提供
機器購入値引き
サービス利用料値引き
サービス利用クーポン提供 …など

■ 参画事業者

シャープ（株）
KDDI（株）
セコム（株）
（株）tsumug
中部テレコミュニケーション（株）
静岡ガス（株）
セコムトラストシステムズ（株）

キーウェアソリューションズコンソーシアム

■ サービス例

血圧計や活動量計のデータを基に、配食サービスが最適な献立にカスタマイズされます。

■ LIFE UP プロモーション特典例

Amazon ギフト券提供
配食サービス利用料値引き …など

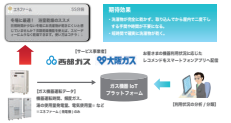
■ 参画事業者

グローバルキッチン（株）
（株）アコーズ
（株）エー・アンド・デイ
テルモ（株）
日本精密測器（株）
山佐時計計器（株）

大阪瓦斯コンソーシアム

■ サービス例

ガス機器の運転データを基に、給湯器や浴室暖房乾燥機等の、最適な使い方をリコメンドします。



■ LIFE UP プロモーション特典例

Amazon ギフト券提供
（スマートフォンアプリのプッシュ通知）
…など

■ 参画事業者

大阪瓦斯（株）
西部瓦斯（株）
アイシン精機（株）
（株）ノーリツ
リンナイ（株）
パーパス（株）
（株）オージス総研
関西ビジネスインフォメーション（株）

対象サービス

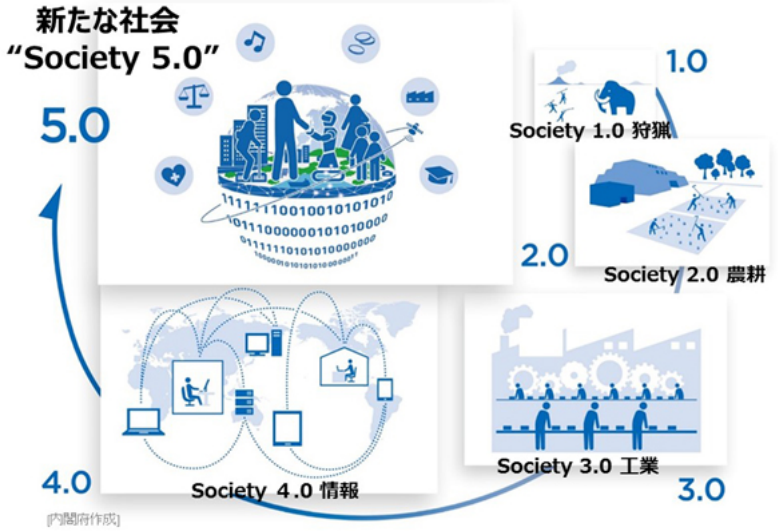
対象サービスは、適宜追加・変更があります。WEBページにて最新情報を更新いたします。 https://lifeup.cyber-physical.jp/service/

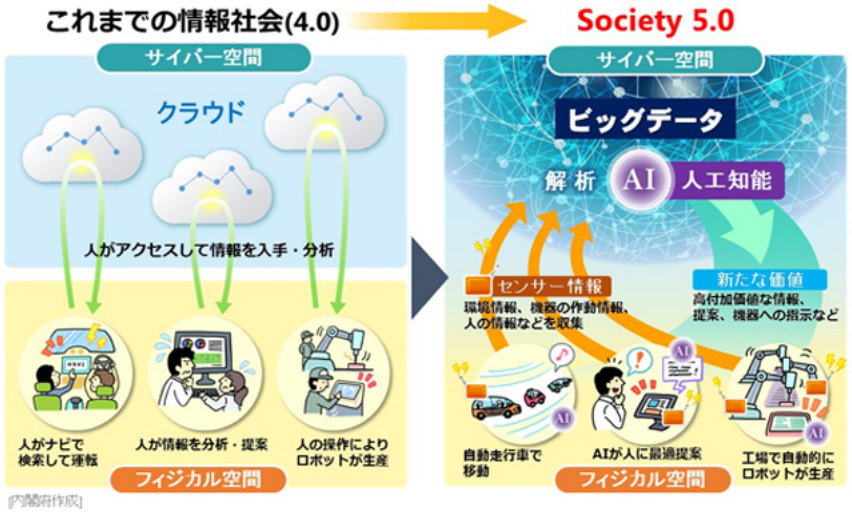
LIFE UP プロモーションは、経済産業省平成30年度補正予算「サイバー/フィジカル融合促進事業費補助金」に基づき、一般社団法人環境共創イニシアチブ（SII）が事務局を運営しています

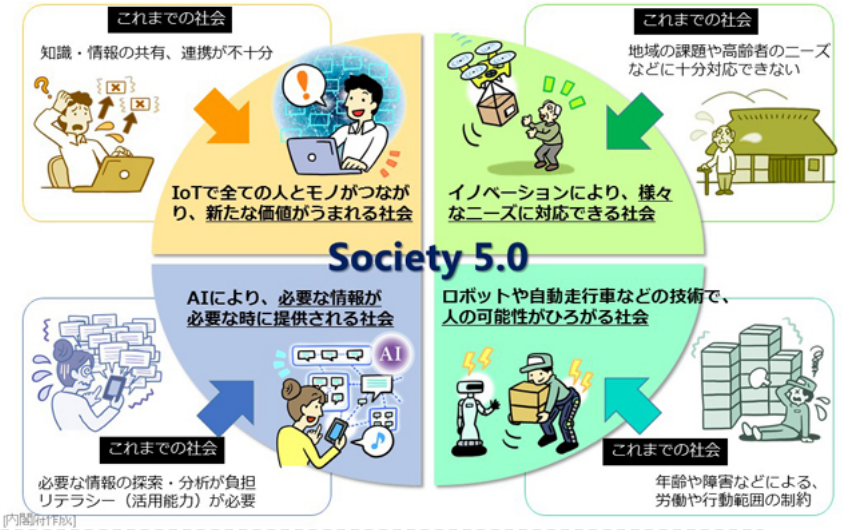
Society 5.0

https://www8.cao.go.jp/cstp/society5_0/index.html

- 日本政府としてのIoT時代の国のあり方
- 技術的、制度的裏付けがあるわけではなく、それをこれからつくる段階







と、ここまでくればIoTセキュリティとは…

- 今までのサイバーセキュリティ
  - ＋ 組込みシステムのセキュリティ
  - ＋ クラウドセキュリティ
  - ＋ AIセキュリティ
  - ＋ データ信頼性
  - ＋ 機能安全
  - ＋ まだあるかも
- 現状は、「IoTシステムを構成するネットワークデバイスのサイバーセキュリティ」が、IoTセキュリティと呼ばれている
  - それでも、IoTシステム特有の技術に依存したセキュリティの課題がある
    - エンドノードの構成、使われるデータリンク技術、等

情報セキュリティの定義

- JIS Q 27002 (ISO/IEC 27002)
  - 機密性 (confidentiality): 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
  - 完全性 (integrity): 情報が破壊、改ざん又は消去されていない状態を確保すること
  - 可用性 (availability): 情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること
- 以上3点を維持すること。さらに、以下の4点を含めて定義してもよい
  - 真正性 (authenticity): ある主体又は資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
  - 責任追跡性 (accountability): あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性。
  - 否認防止 (non-repudiation): ある活動又は事象が起きたことを、後になって否認されないように証明する能力
  - 信頼性 (reliability): 意図した動作及び結果に一致する特性

情報セキュリティから サイバーセキュリティに

- 情報セキュリティに対する脅威の高度化
  - 大規模化、手口の巧妙化
  - 純粋に技術的な方法だけではなく、普段の慣習、人間同士の信頼関係を利用したソーシャルエンジニアリングの手口も
- サイバー空間の発展
  - インターネットに始まった情報ネットワークは、クラウド、ビッグデータと、加速度的に広まる
  - ネットワークにつながっていない計算機はほとんど役に立たず、ネットワークのどこかにデータもアプリケーションも存在して、単に人間の相手をする部分だけが手元にある、という状況に近づきつつある
- 情報セキュリティの技術を使って、サイバー空間内での治安維持、防衛をする時代に
  - 事件が起らないのを目指すのではなく、事件が大きな問題とならないように被害を抑えこむという考え方に

サイバーセキュリティとIoTセキュリティ

- IoTセキュリティには大きくわけて二つの観点がある
  - ネットワークにつながるノード(=サイバーセキュリティの対象)が極めて多くなる
    - ノードの多くがリソース不足で十分なセキュリティ対策が行われない
    - ノードが多すぎて管理の手が回らない
  - IoTシステムのノードは、実世界とのインタラクションを有する
    - 物理的に危害を加えることができる
    - 物理的な情報を取得、収集することができる
- これらとは別に、システムとしてみたときのIoTシステムの特徴も
  - 設置される場所の広がり
  - 複合型、統合型のシステム

IoTセキュリティを巡るいくつかの論点

- セキュリティとプライバシの関係?
  - セキュリティとプライバシには密接な関連はあるものの、集めたデータが誰のものなのか、どういった目的まで利用可能なのかがプライバシであり、本質的に別の話
    - プライバシを実現するための一技術としてのセキュリティ
    - プライバシ問題は最終的には社会的コンセンサス (事故がなくせなくても自動車はなくならない)
- 時代の変遷による落としどころの変化
  - 社会的コンセンサスの変化 (酔っぱらい運転の例)
  - コスト見合いでの妥当性の変化 (対策にかかるコストの急速な変化)
- この分野における「出口対策」とは?
  - エンタープライズ系のセキュリティで当然のこととなっている出口対策のIoT版は何に当たるか
  - アクチュエーションした結果が事故(accident)を起こさなければ良しとするのであれば、情報システム内というよりも、物理空間内での防止という観点も出てくる
  - その意味で、「機能安全」は、IoTセキュリティと極めて密接な関係を持っている
  - 安全性を担保するための専門のシステムの必要性と、「IoTシステムが対象とする空間までを把握したOSのようなもの」への組み込みが必要

まとめ

- IoTということばは、単にネットワークインターフェースを有する機器、を指しているわけではない
- ビッグデータ、AIを前提としてあらゆるものをネットワークにつなぐというのが本質
- セキュリティ面では今までのサイバーセキュリティ全部に物理的要素を加えたような話になってくる
- 現在、IoTセキュリティとして報道されているのはIoT機器のサイバーセキュリテイであり、実世界とのインタラクションがあるという本質的なところにまだ踏み込んでいない
- 将来的にはサイバーセキュリティとは結構異なる対策が必要になるが、さしあたりはサイバーセキュリティ部分を潰すだけでも大変

参考文献

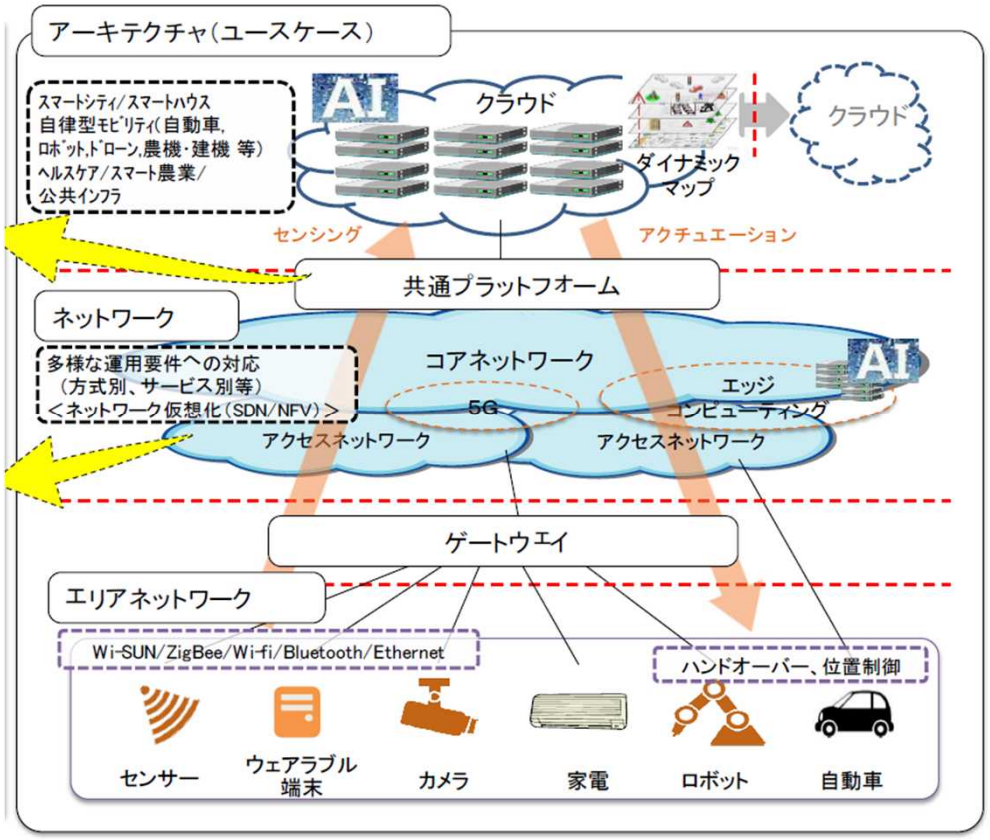
1. 丹 康雄監修、宅内情報通信・放送高度化フォーラム編、「ユビキタス技術 ホームネットワークと情報家電」、オーム社、2004.09
2. 丹 康雄、”(解説論文)ホームネットワークの現状と標準化動向”、電子情報通信学会通信ソサエティマガジン B-plus、Vol.22 (2012.9) (https://www.jstage.jst.go.jp/article/bplus/6/2/6_90/_pdf より入手可能)
3. 丹 康雄、門馬 弘、牧野 淳一、「ホームネットワークシステムの概要と現状」、一般財団法人テレコム先端技術研究支援センター 報告書、2015.03 (http://www.scat.or.jp/research/SCAT_research1503.pdf より入手可能)
4. 丹 康雄、門馬 弘、牧野 淳一、「ホームネットワークシステムの概要と現状(続編)」、一般財団法人テレコム先端技術研究支援センター 報告書、2016.03 (http://www.scat.or.jp/research/SCAT_research1603.pdf より入手可能)
5. ITU-T勧告文書は https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx より入手可能
6. TTC標準文書等は http://www.ttc.or.jp/document_db より入手可能

参考資料7

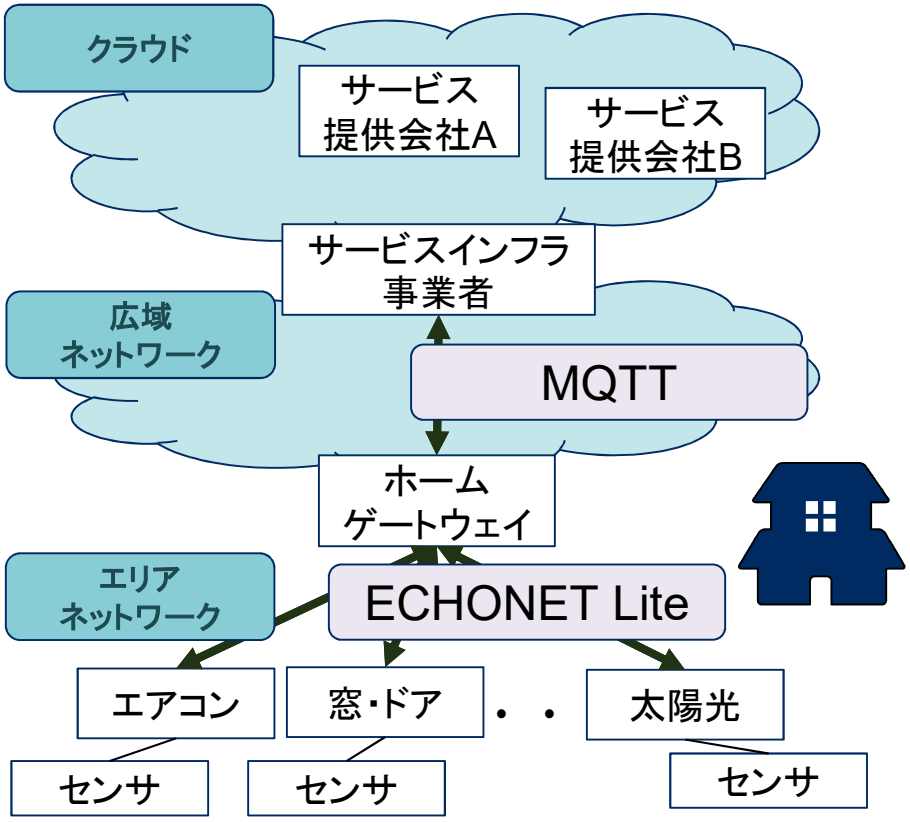
IoTセキュリティ講座
セキュリティ

※JPCERT/CC発行「IoTセキュリティチェックリスト」を参考としています
https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

IoTシステムの全体像と今回の実習テーマ

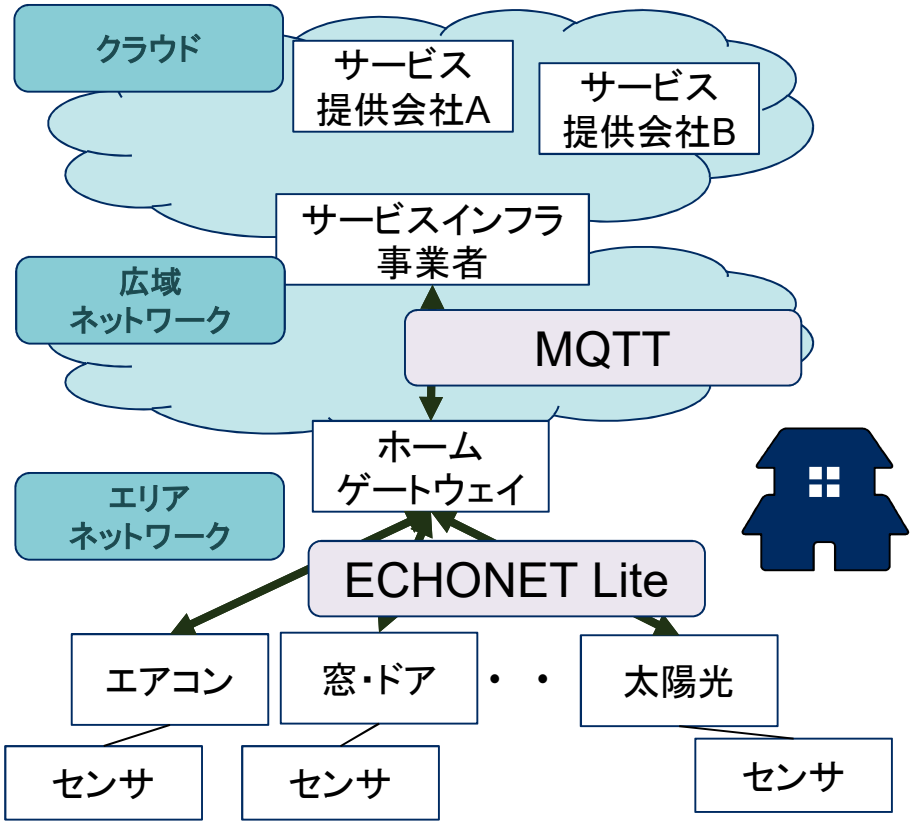


IoTシステムの全体像

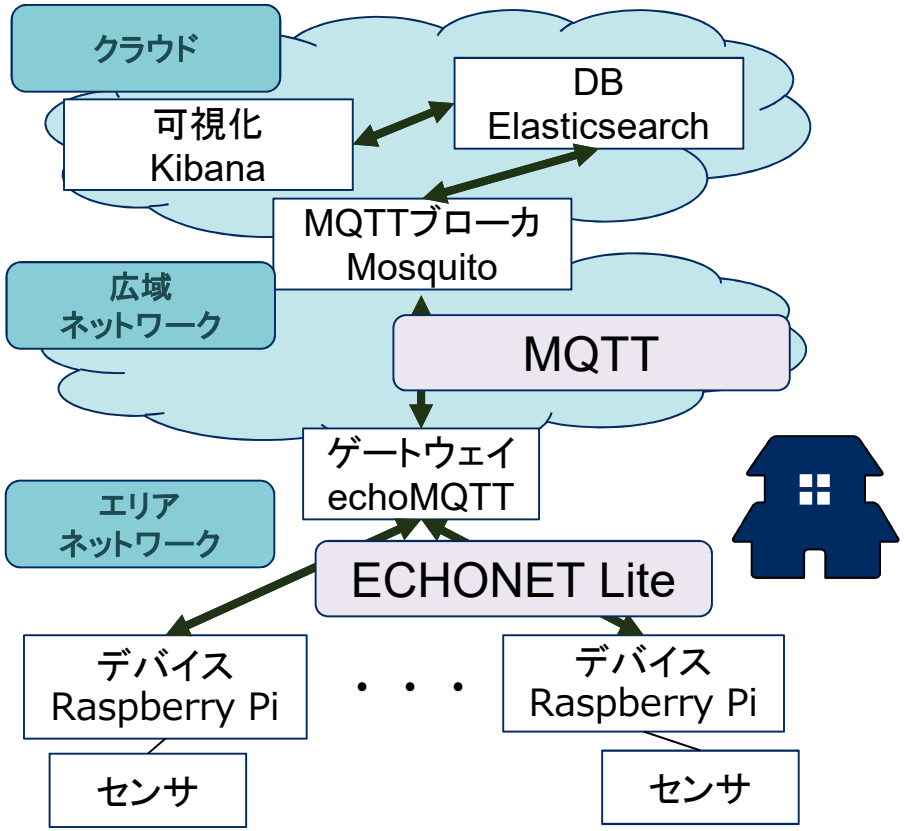


今回の実習テーマ
「スマートホーム」

今回の実習テーマと実機環境



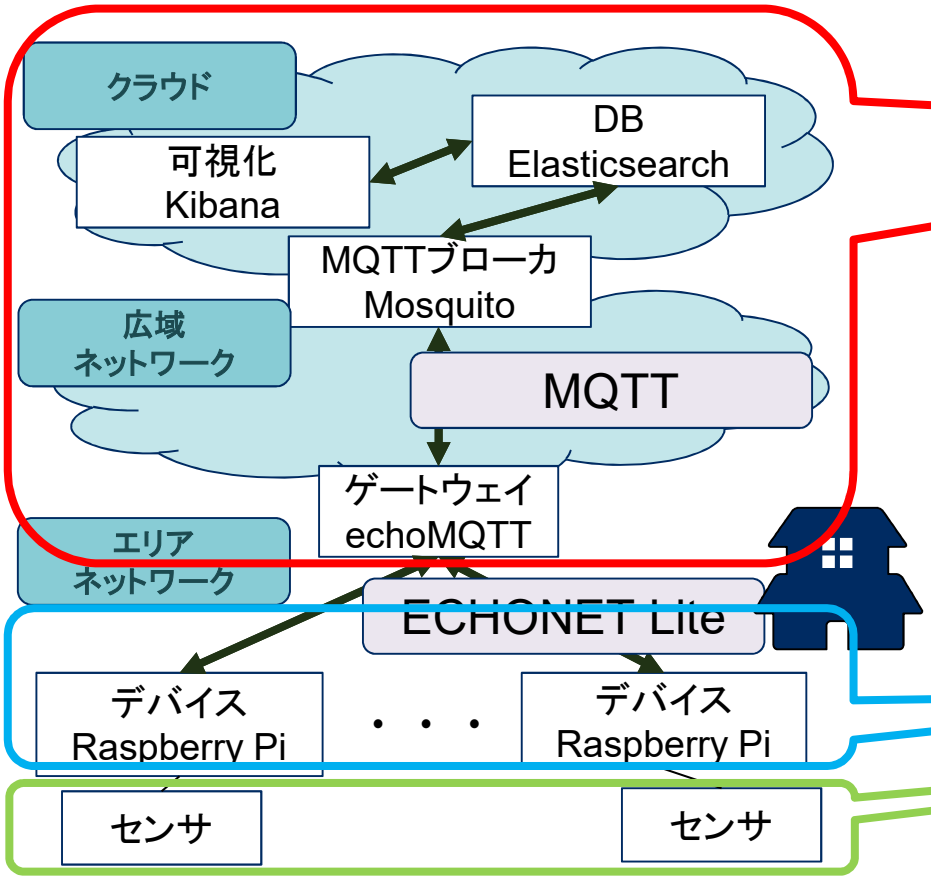
今回の実習テーマ「スマートホーム」



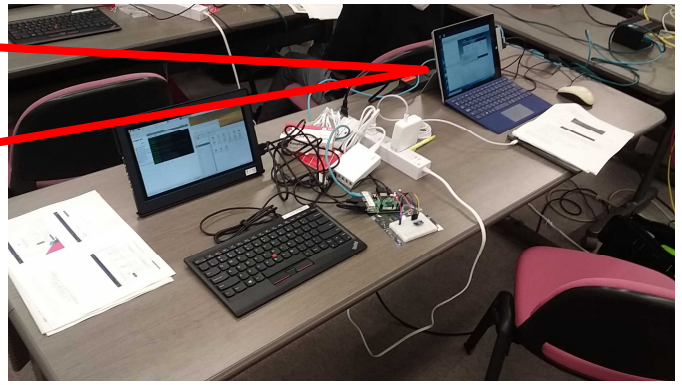
今回の実機環境

今回実習を行っていただく実機環境は、IoTシステムの要素が一つに纏まったものです

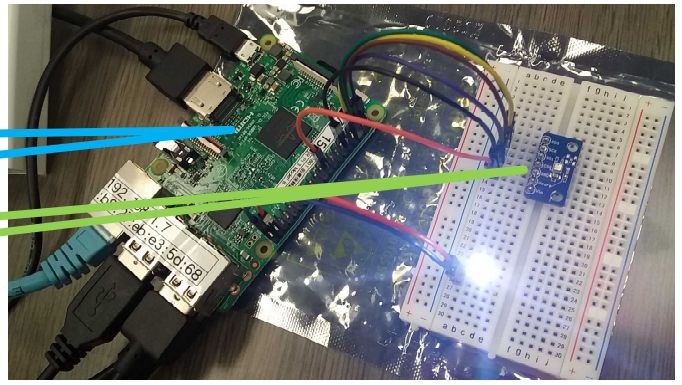
実機構成



今回の実機環境



受講者毎の実機構成

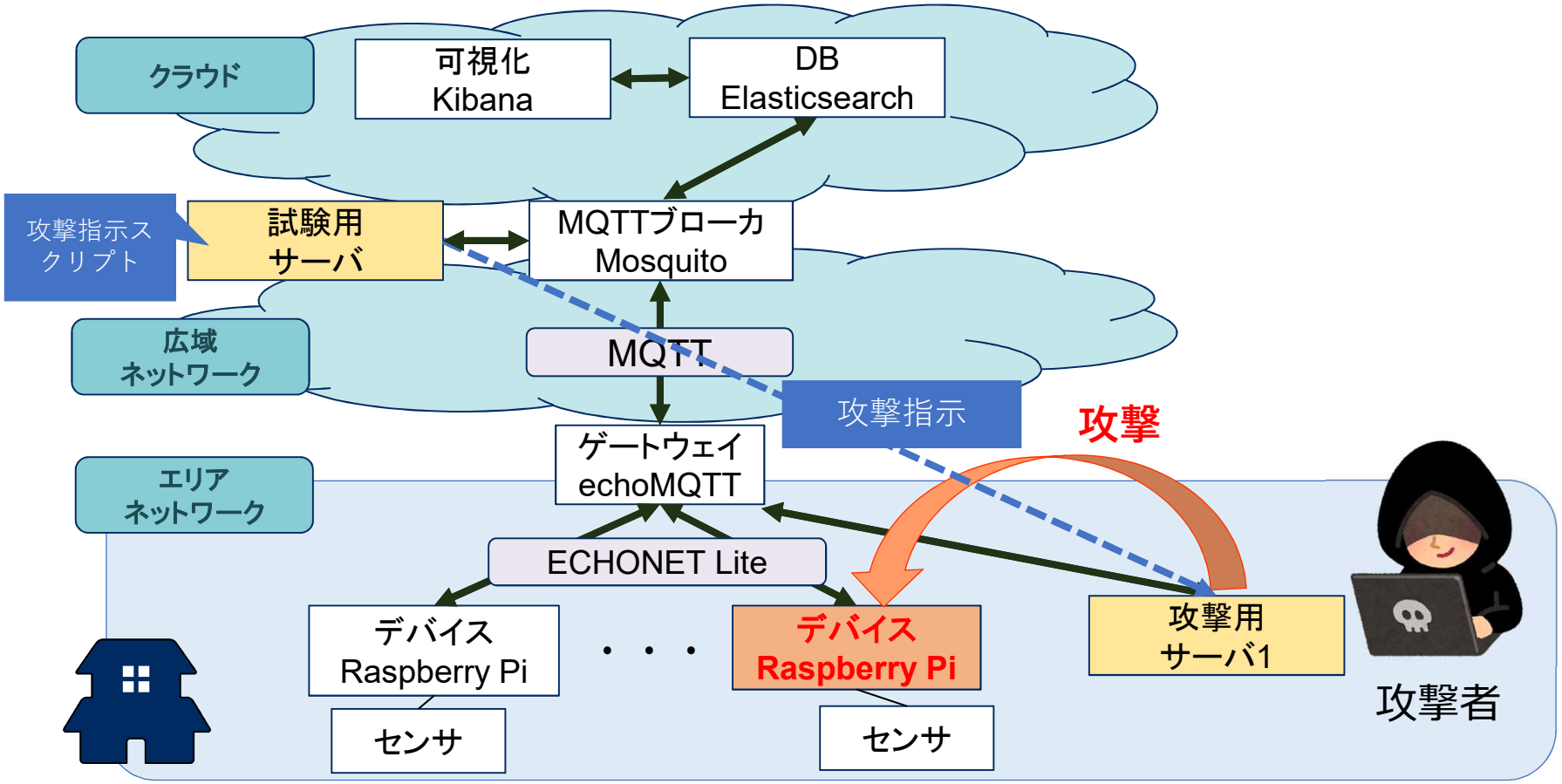


Raspberry Piとセンサ類

リスクポイントと攻撃の種類の例

- デバイスへの攻撃
  - 1-1 デバイスへの不正ログイン
  - 1-2 センサの状態偽装
  - 1-3 デバイスのプロパティ値変更
  - 1-4 不正なセンサデータ送信
  - 1-5 ポートスキャン
- ゲートウェイへの攻撃
  - 2-1 不正なデバイスからのデータ送信
- クラウドへの攻撃
  - 3-1 クラウド側の要塞化(外との通信)
  - 3-2 クラウド側の要塞化(クラウドアプリケーション間の通信)

デバイスへの攻撃
攻撃イメージ図

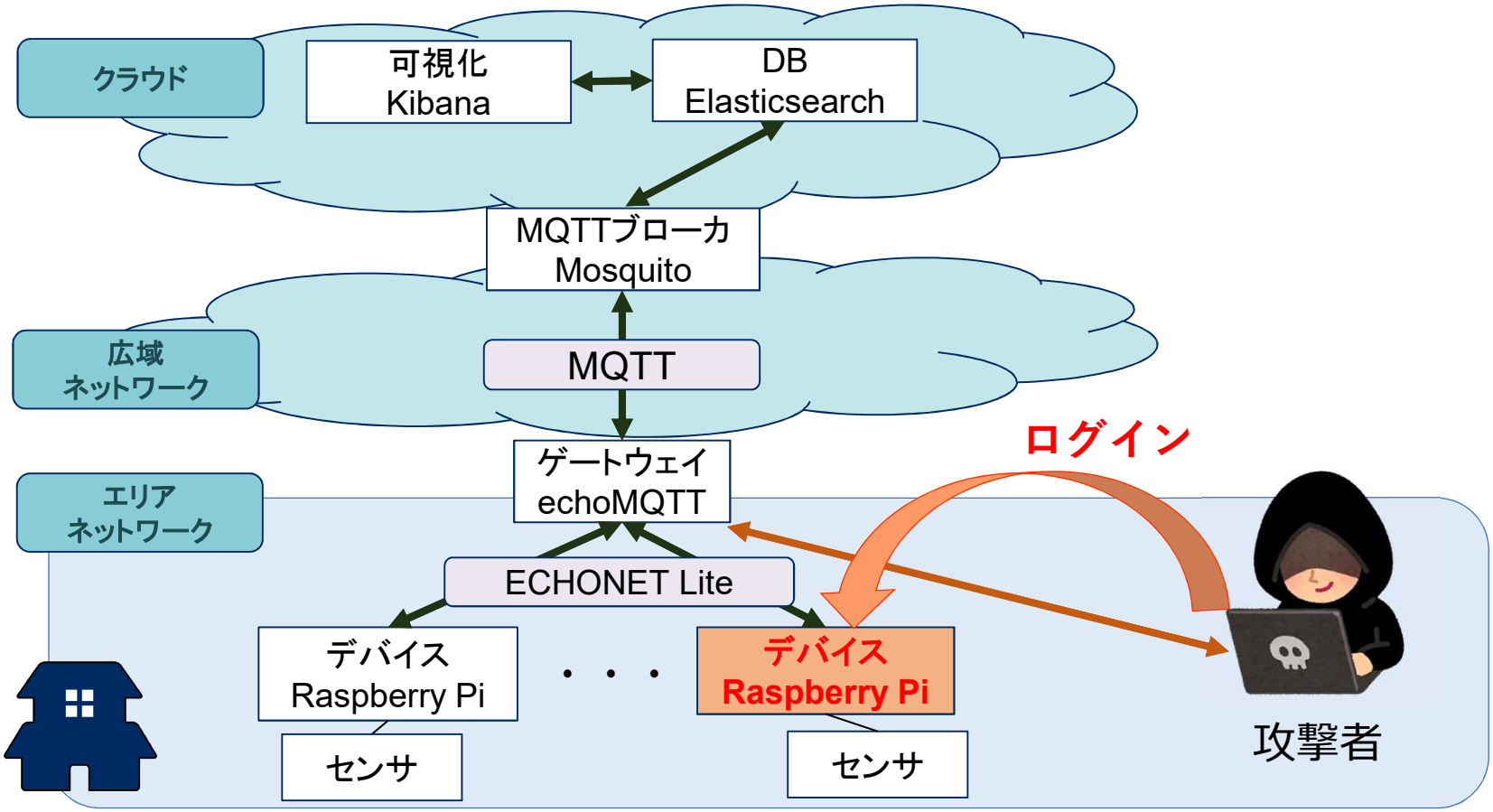


今回の実機環境

1-1 デバイスへの不正ログイン概要

- 攻撃対象
  - デバイス
- 攻撃手法
  - ブルートフォース、辞書攻撃
- 脆弱性
  - デフォルトパスワード/ポート番号、パスワードの使い回し
- 防御
  - IoTデバイスのパスワードの変更
  - アカウントロック
  - IoTデバイスのsshポート番号の変更
  - ログ情報の収集と分析
- 影響
  - デバイスへの不正ログインにより、不正操作や障害の発生といった攻撃を受ける
  - 攻撃の踏み台とされることが想定

1-1 デバイスへの不正ログイン 攻撃イメージ図



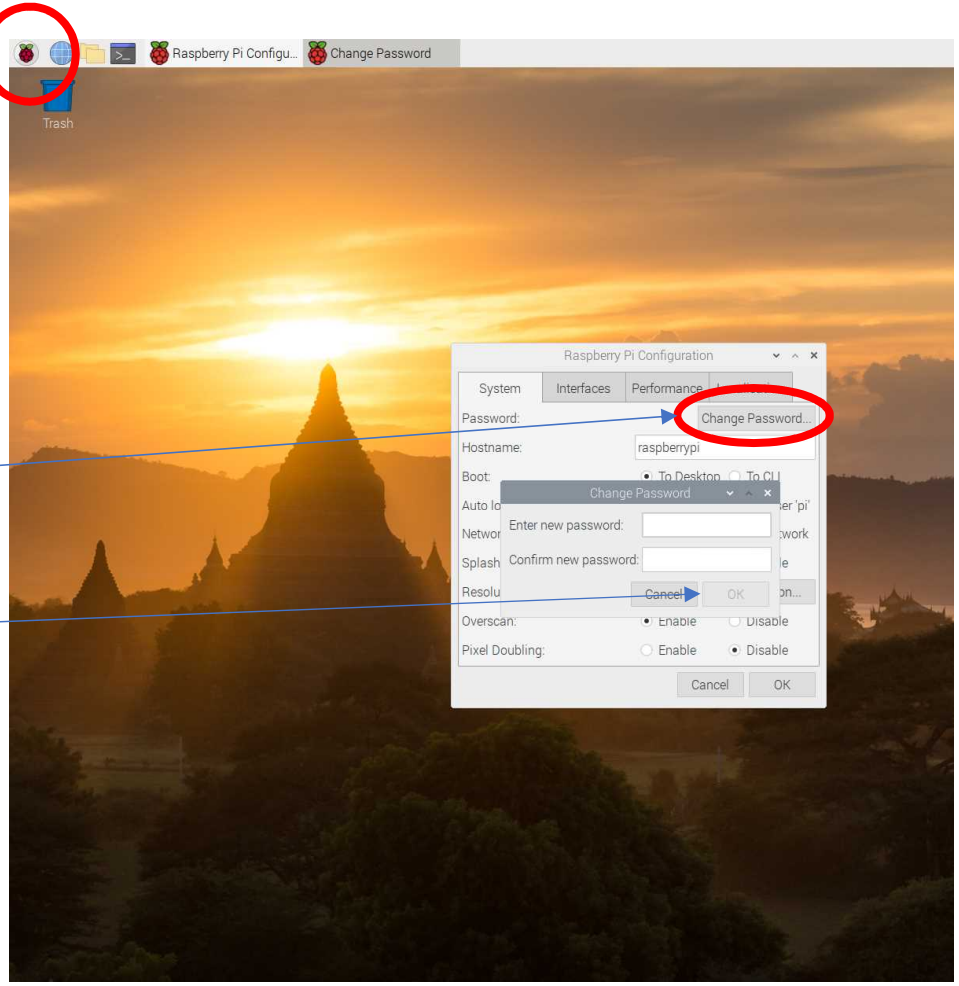
今回の実機環境

1-1 デバイスへの不正ログイン 実習内容

- 問題
  - Raspberry Pi でデフォルトパスワードが設定されている
    - ユーザID: pi
    - パスワード: raspberry
- 攻撃内容
  - 遠隔からログインしてホームディレクトリ内にファイルを追加
- 対策
  - パスワードの変更
- 防御の可否
  - 不正ログイン成功: 赤LED1が点灯
  - 不正ログイン失敗: 青LED1が点灯

1-1 デバイスへの不正ログイン対策手順例

- パスワードの変更
  - 左上のスタートボタン＞Preferences＞Raspberry Pi Configurationをクリック
  - Change Passwordをクリックし、パスワードを設定後OKをクリック

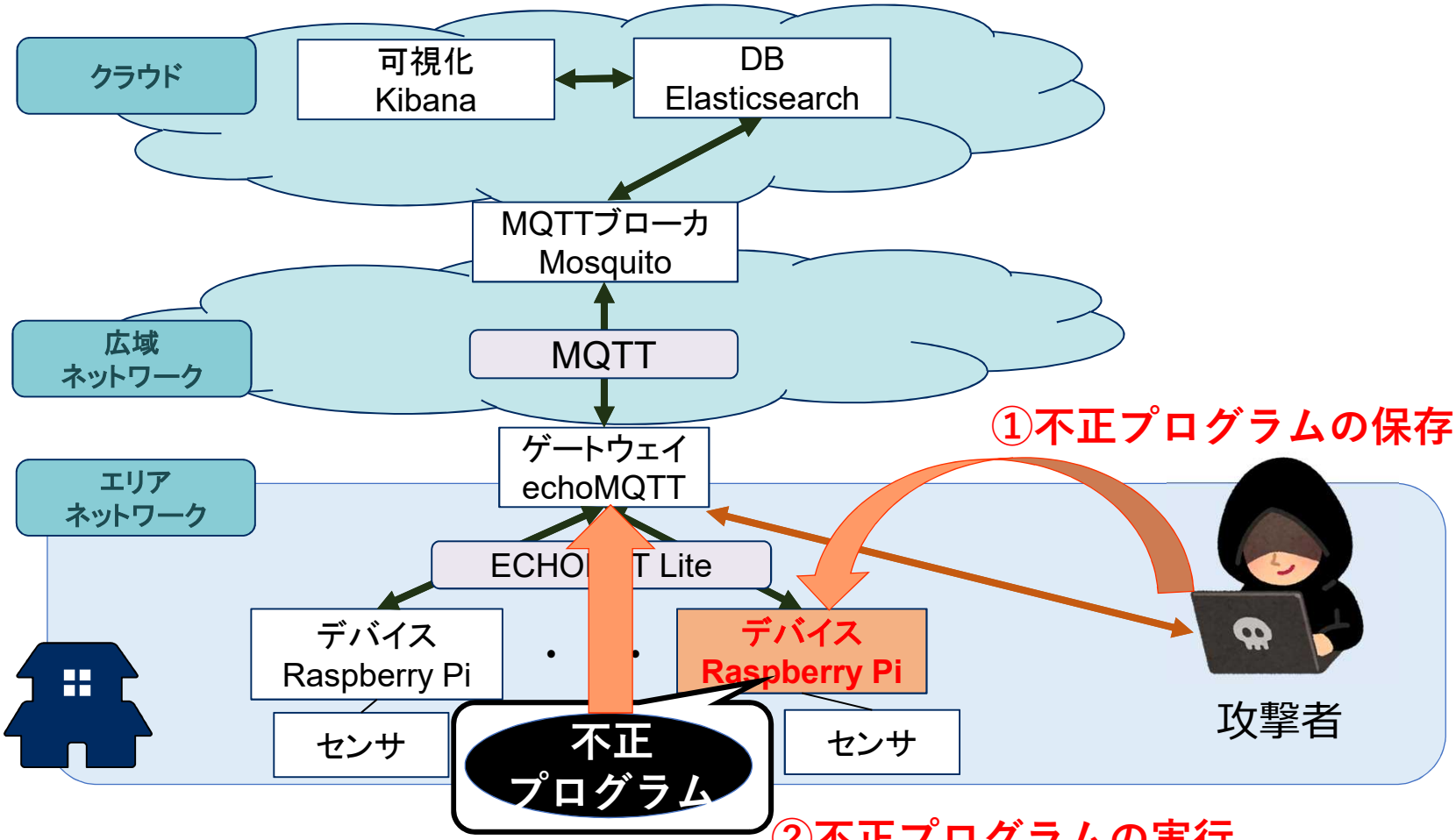


- 変更により不正ログインが失敗したことをLEDの点灯状況から確認

1-2 センサの状態偽装
概要

- 攻撃対象
  - デバイス
- 攻撃手法
  - 不正なプログラムの実行により、間違ったセンサ情報をゲートウェイに送信
- 脆弱性
  - 不正なプログラムがデバイス上で実行可能
- 防御
  - デバイスへの不正アクセスの禁止
  - 動作しているプログラムの監視
  - クラウドの情報とセンサの実際の状態を比較して監視
- 影響
  - エアコンやセンサが故障しているという嘘の情報を提供したり、人感センサから間違った情報が提供される

1-2 センサの状態偽装
攻撃イメージ図



今回の実機環境

1-2 センサの状態偽装
実習内容

- 問題
  - センサの状態を偽装したフレームを送信する
  - 不正なプログラムが仕込まれていて、センサの状態が操作される
- 攻撃内容
  - 不正なプログラムが仕込まれ、センサの状態が変更される
  - デバイス内の不正プログラムによりセンサが故障しているというフレームを送信されることにより、データベースが攻撃されセンサが故障状態に変更される
    - ECHONET Liteでは故障時のエラーコードが規定
- 対策
  - デバイスが生成するデータの監視と分析
  - デバイスの状態の監視
  - デバイスへの不正アクセス対策
  - デバイスのプロセスを確認し、不正なプロセスを停止
- 防御の可否
  - 故障しているというフレーム送信成功: 赤LED1が点灯
  - 故障しているというフレーム送信失敗: 青LED1が点灯

1-2 センサの状態偽装 対策手順例

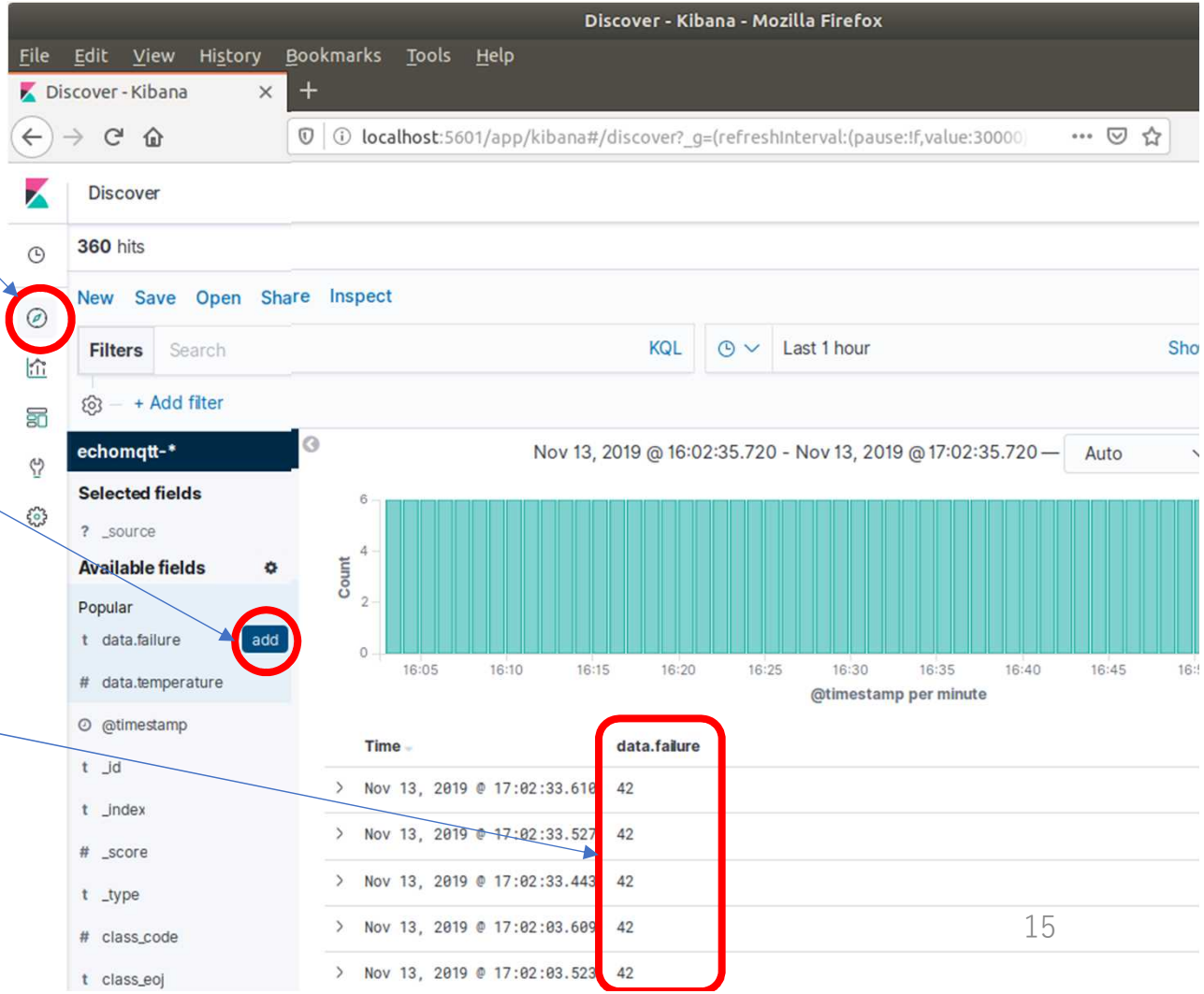
- 正常な状態の確認
  - Kibanaで正常な状態を確認
    - 次のページの手順に従う
  - lsofコマンドを実行し、正常な状態を確認
    - lsofコマンド…開かれているファイルのリストを表示
      - $ lsof -i
- Raspberry Piで不正プログラムを実行
  - $ cd ensemble_malware
  - $ java –jar ensemble.jar –i eth0 script.js
- Raspberry Pi内の不正なプログラムの発見と停止および削除
  - Kibanaで異常な状態を確認
    - 次のページの手順に従う
  - 不正プログラムを動かしているウィンドウとは別のTerminalウィンドウを立ち上げる
  - 開かれているファイルのリストを詳細表示し、不正なプログラムを発見
    - $ lsof -i
    - $ lsof –V|grep <PID> |head
  - killコマンド…プロセスにkillシグナルを送信し、不正なプログラムを停止
    - $ sudo kill <PID>
  - 不正なプログラム本体の削除
    - $ rm ensemble_malware
  - 再度、lsofコマンドでプロセスが停止されていることを確認
  - Kibanaで正常な状態に戻っていることを確認

1-2 センサの状態偽装
対策手順例
(Kibanaの故障状態の確認手順)

①Discoverをクリック

②data.fallureを探し
addをクリック

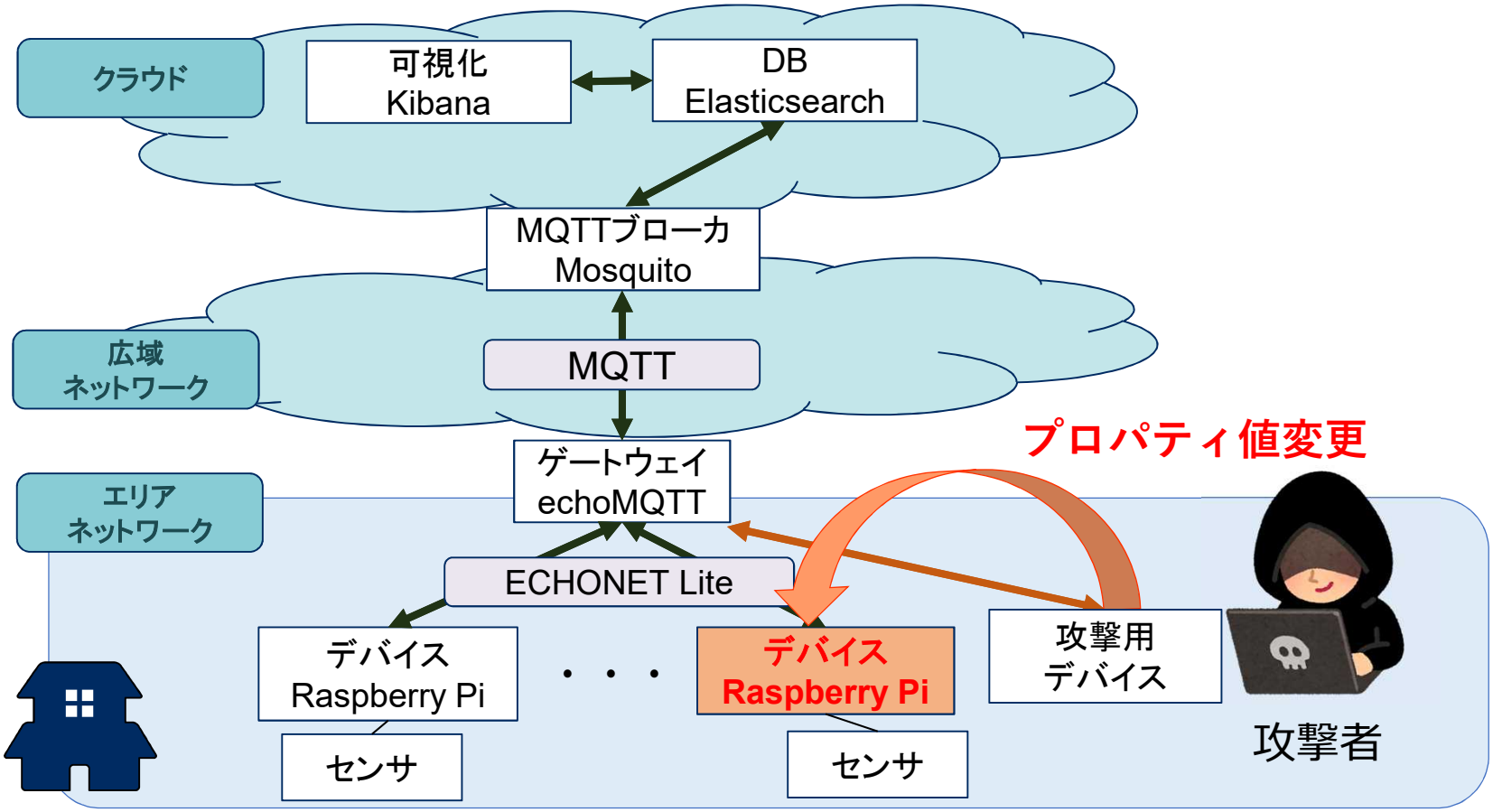
③data.failureの値を確認
Echonet Liteの仕様では、
41 :故障
42 :正常



1-3 デバイスのプロパティ値変更概要

- 攻撃対象
  - デバイス
- 攻撃手法
  - デバイスを攻撃者が発見し、 ECHONET Lite上で攻撃を実施
  - デバイスのECHONET Liteのプロパティ値変更、デバイスの不正制御
- 脆弱性
  - エリアネットワークで利用するプロトコルのセキュリティ機能欠如
  - エリアネットワークで利用するプロトコルを介した無制限アクセス許可
- 防御
  - 接続の認証
    - デバイス側で、攻撃者からの接続を許可しないようにする(MACアドレスやIPアドレスでフィルタリングする)
  - デバイスが接続するネットワークの物理的なセキュリティ(ポートを物理的に塞ぐなど)
  - 無線LANのセキュリティ強化
- 影響
  - エアコン等が不正に制御され、消費電力量の増大や屋内環境の悪化による健康被害等が想定

1-3 デバイスのプロパティ値変更 攻撃イメージ図



今回の実機環境

1-3 デバイスのプロパティ値変更 実習内容

- 問題
  - ECHONET Liteデバイスは、 ECHONET Liteの通信をすべて受信してしまい、ECHONET Liteデバイスのプロパティにアクセス可能
- 攻撃内容
  - エリアネットワークに不正に設置されたデバイスからECHONET Liteのプロパティ値を変更
- 対策
  - デバイスのファイアウォールの設定を変更することで指定されたゲートウェイ以外からのアクセスを禁止
- 防御の可否
  - ECHONET Liteのプロパティ値変更成功: 赤LED1が点灯
  - ECHONET Liteのプロパティ値変更失敗: 青LED1が点灯

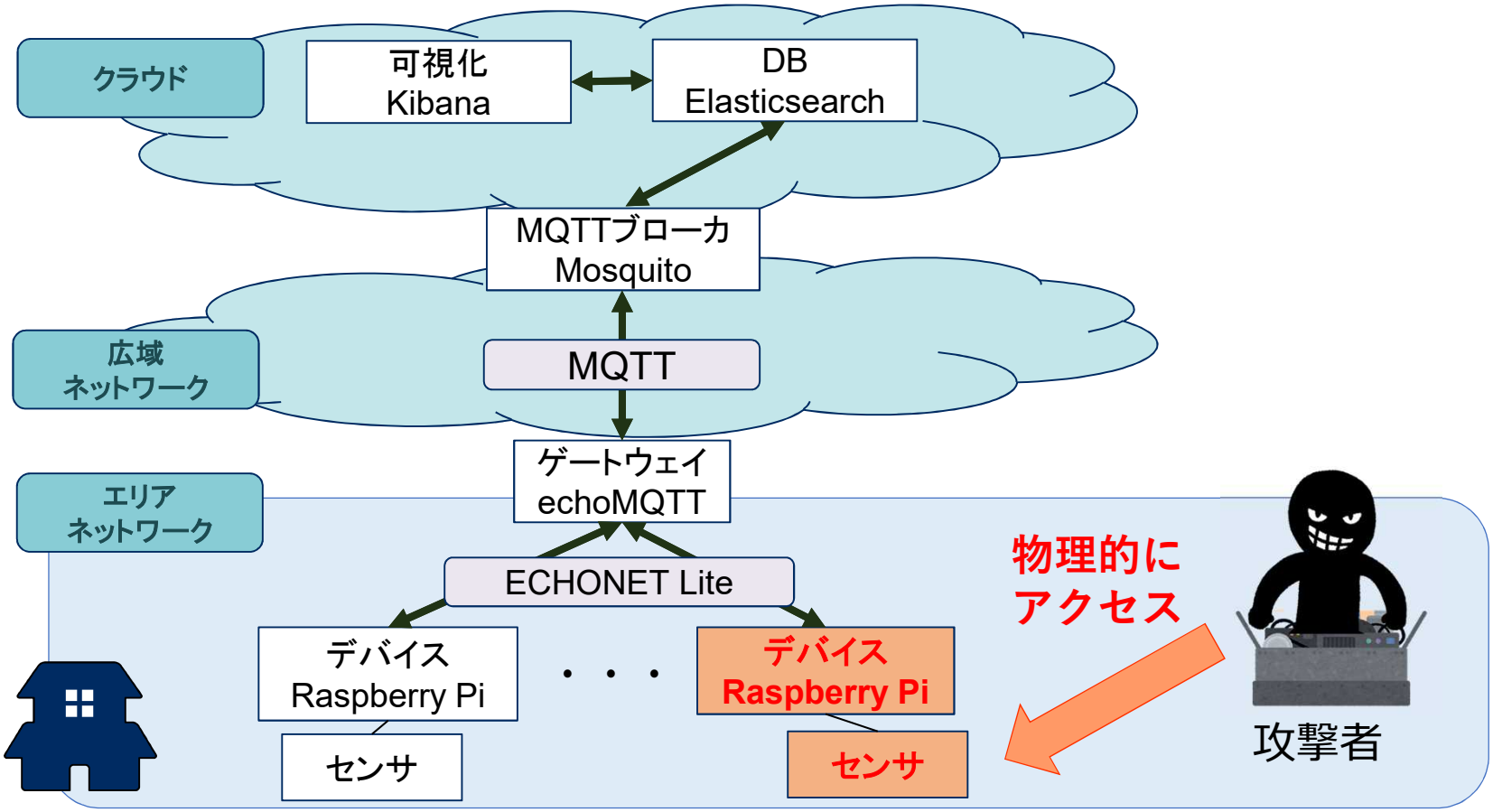
1-3 デバイスのプロパティ値変更対策手順例

- ECHONET Liteが利用するプロトコルとポート番号
  - プロトコル：UDP
  - ポート番号：3610
- 接続を許可するゲートウェイのIPアドレスを調査
  - $ ip addr
- 上記の通信のデバイス側でのフィルタリング設定を実施
  - 許可するゲートウェイからのUDPパケットのみACCEPT
    - $ sudo iptables -A INPUT -p udp --dport 3610 –s 10.10.XXX.YYY -j ACCEPT
  - 全てのECHONET Liteパケット(3610番ポート)をDROP
    - $ sudo iptables -A INPUT -p udp --dport 3610 -s 0.0.0.0/0 -j DROP
  - iptableの表示
    - $ sudo iptables -L

1-4 不正なセンサデータ送信概要

- 攻撃対象
  - デバイス
- 攻撃手法
  - センサへの物理的にアクセス(ヒータを不正に追加され、温度を上げられてしまう)
  - センサアクセス網(I2C等)への不正アクセス
  - 正常に動作しないセンサの設置
- 脆弱性
  - センサへの物理的なアクセスが可能
  - I2C通信のセンサアクセス網にセキュリティ機能が存在しない
- 防御
  - センサへの物理的アクセスの制限
  - デバイスのセンサデータの監視
- 影響
  - 間違った温度や湿度などのセンサ情報をデバイスが取得しクラウドに送信することで、温熱環境の制御などを混乱させる

1-4 不正なセンサデータ送信 攻撃イメージ図



今回の実機環境

1-4 不正センサデータ送信
実習内容

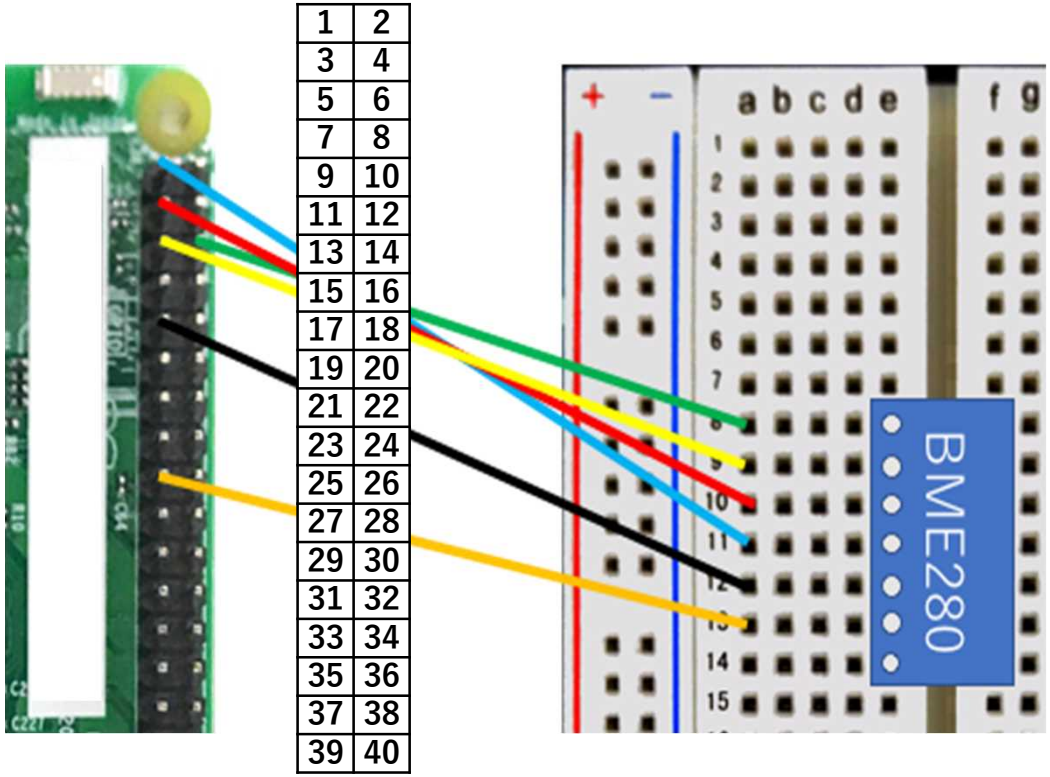
- 問題
  - ヒータにより不正なセンサ値が生成
- 攻撃内容
  - 不正な動作をするセンサに置き換えられ、センサデータが改ざんされる
- 対策
  - 通常状態を監視しておき、異常状態にあるセンサを発見し除去
- 防御の可否
  - 不正センサデータ送信成功：Kibanaに不正なセンサ値が表示
  - 不正センサデータ送信失敗：Kibanaに正常なセンサ値が表示

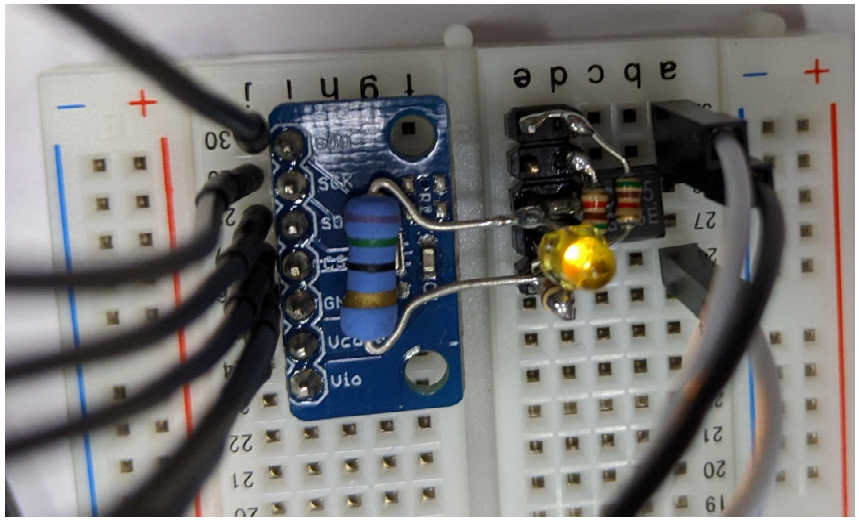
1-4 不正センサデータ送信 対策手順例

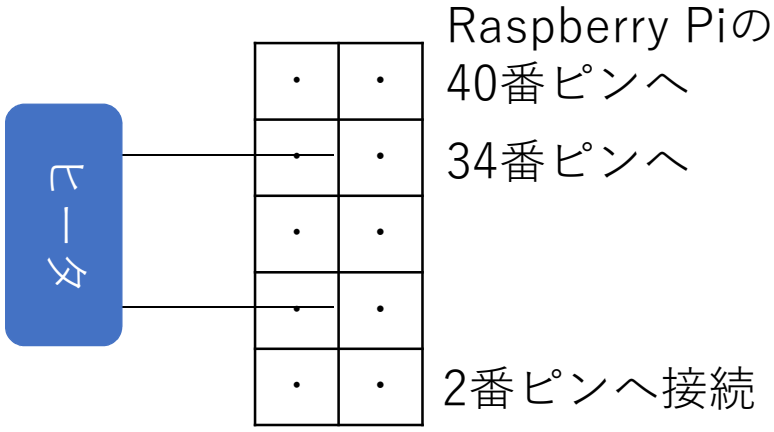
- Kibanaによるデータ可視化手順書を参照
  - 正常状態 (温度、気圧、湿度)を監視
- 不正なデータを生成するヒータを設置
  - 次のページのヒータ設置手順に従う
  - 設置後、ヒータの電源を入れる
    - $ sh ~/ exercise/humming/heater_on.sh
- Kibanaで異常状態になっていることを発見
  - センサデータの可視化
- デバイスにヒータが設置されていることを目視で確認
- 不正に設置されたヒータなので除去
- Kibanaで状態を確認し、正常状態に戻っていることを確認

1-4 不正センサデータ送信 対策手順例(ヒータの設置)

Raspberry Piの
ピン配置



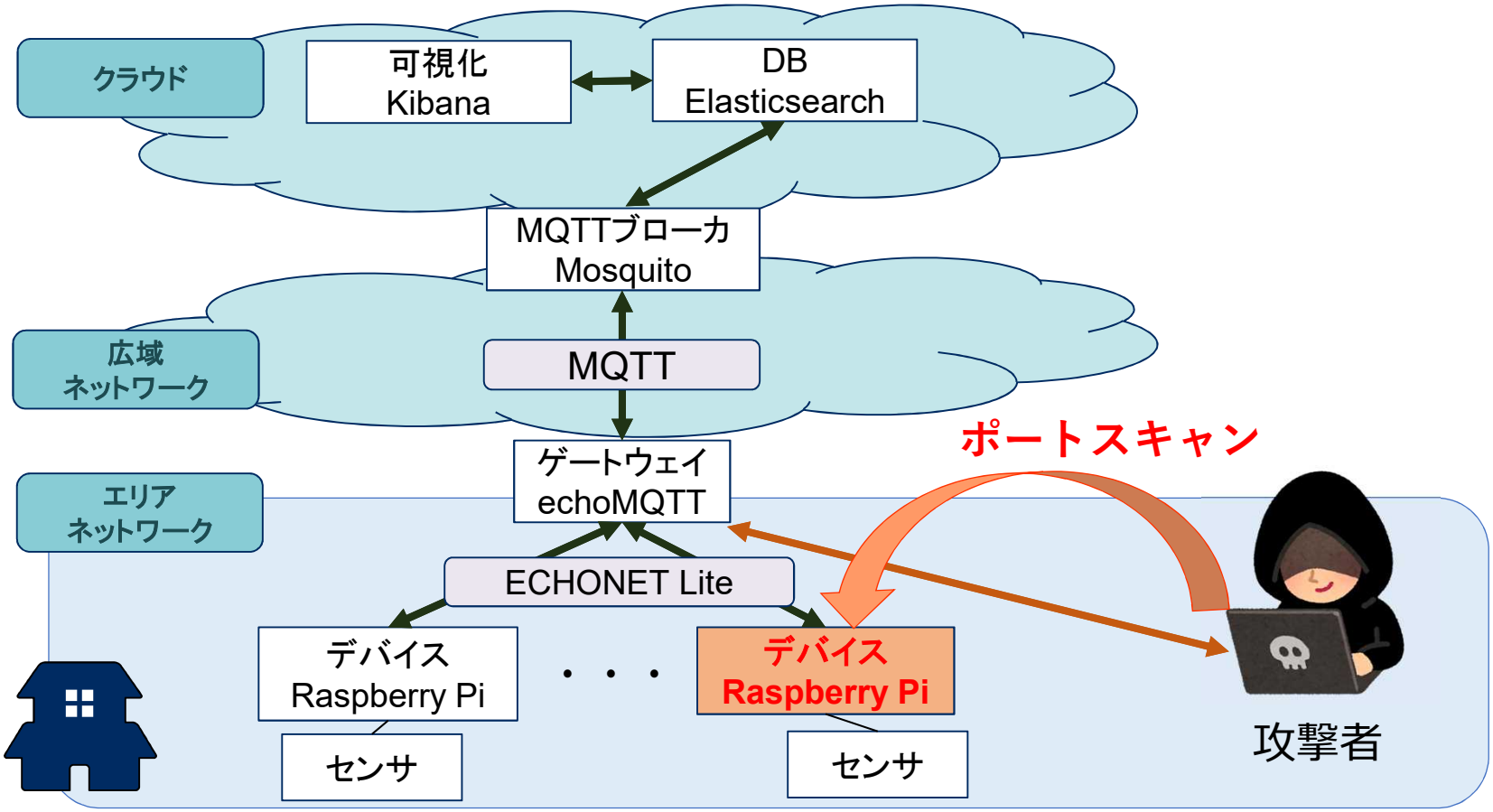




1-5 ポートスキャン概要

- 攻撃対象
  - デバイス
- 攻撃手法
  - 攻撃に利用できるポートの調査
- 脆弱性
  - 不要なポートが開いている
- 防御
  - 不要なポートを閉じる
- 解説
  - 攻撃に利用できるポートの調査に基づいた攻撃を受ける可能性があるため、ポートスキャンを受けないよう対策をする必要がある
  - デバイス以外のシステムでも同様の対策が必要

1-5 ポートスキャン 攻撃イメージ図



今回の実機環境

1-5 ポートスキャン
実習内容

- 問題
  - 不要なプログラムが利用するポートや、脆弱性のあるプログラムが利用するポートが開いている
- 攻撃内容
  - エリアネットワーク内に不正に設置されたデバイスがポートスキャンを行い、不用意に開かれたポートが存在するか調査
  - PCからRaspberry Piに対してポートスキャンを行い、不要なポートが開いているか調査
- 対策
  - Raspberry Piで外部からのアクセスは許可するポート(ssh)以外禁止する
  - netstatコマンド(listenポートの一覧)をRaspberry Piで実行する
- 防御の可否
  - 許可するポート以外が開いている: 赤LEDが点灯
  - 許可するポートのみ開いている: 青LEDが点灯

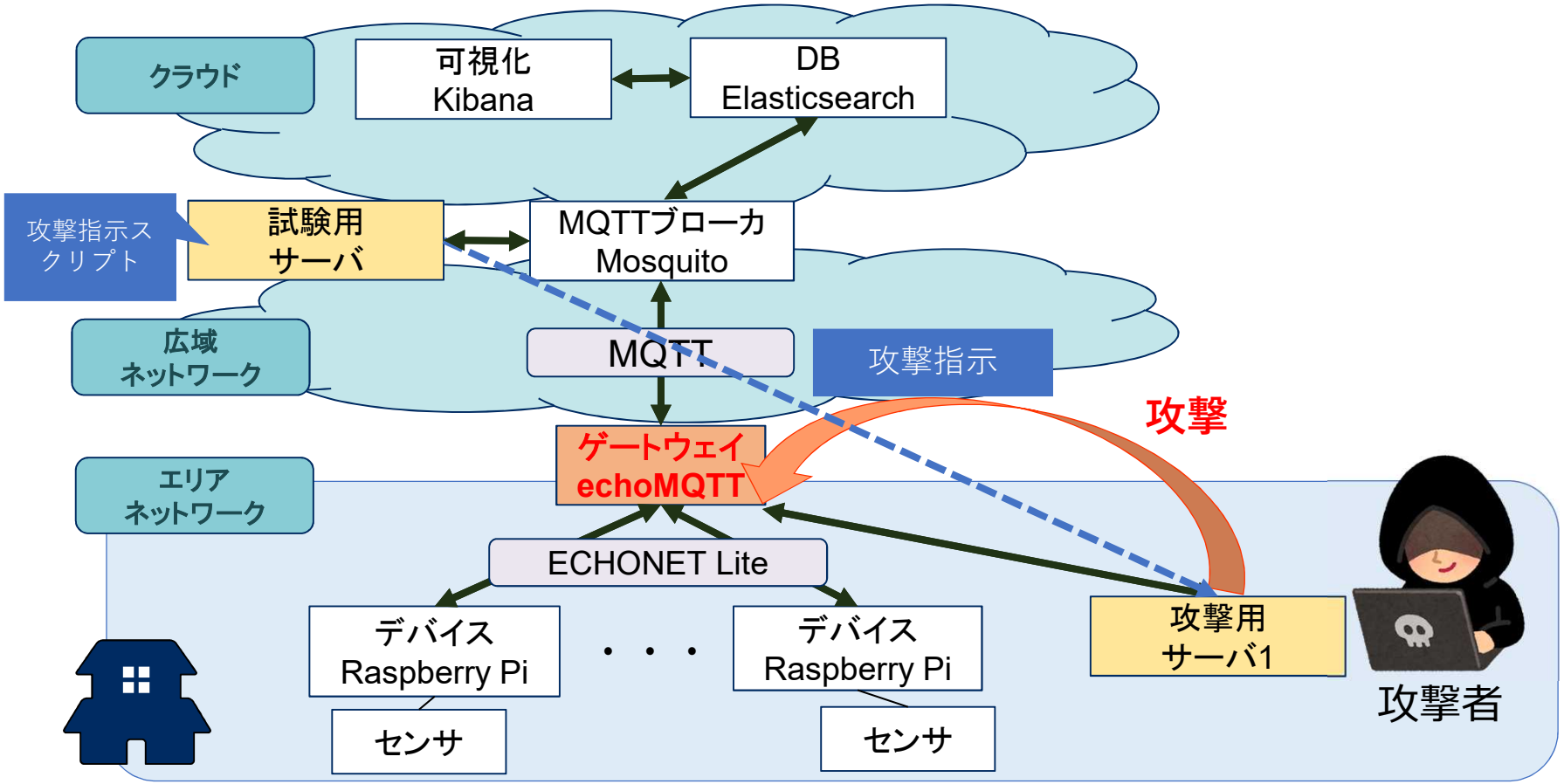
1-5 ポートスキャン 対策手順例

- 該当のプロセスを止める
- 該当のプロセスをアンインストールする
- ファイアーウォールで塞ぐ

など

対策方法は受講者皆様で調べてみてください

ゲートウェイへの攻撃
攻撃イメージ図

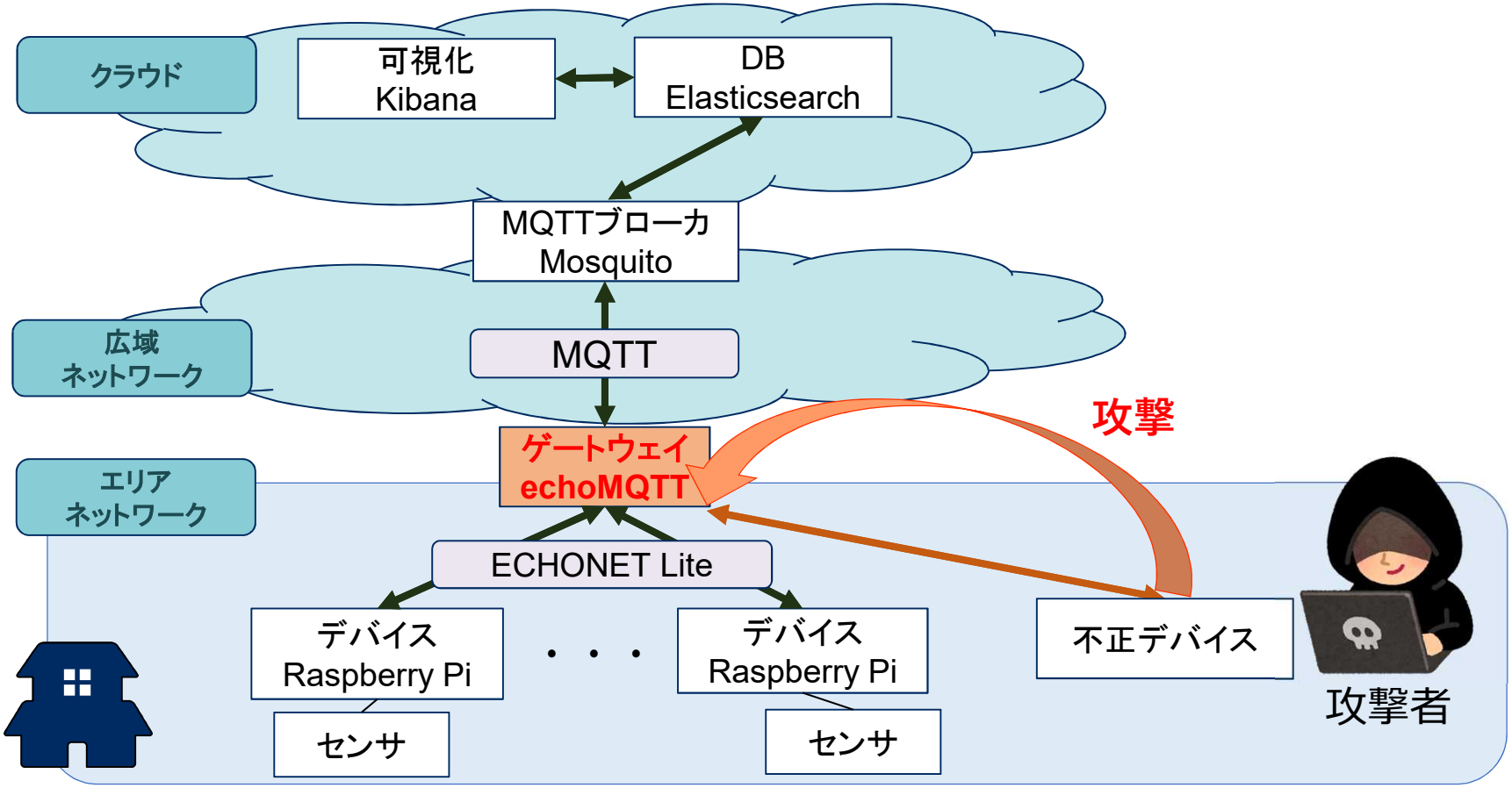


今回の実機環境

2-1 不正なデバイスからのデータ送信概要

- 攻撃対象
  - ゲートウェイ
- 攻撃手法
  - 不正なデバイスをエリアネットワークに接続
  - 事実と異なるセンサデータをゲートウェイに送信(エリアネットワークに不正デバイスを設置され、誤った温度データを送信される)
- 脆弱性
  - エリアネットワークのセキュリティ機能欠如
  - エリアネットワーク内の全てのデバイスのデータを受信
- 防御
  - デバイスとゲートウェイ間で認証を行うようにする
  - ゲートウェイ側のフィルタリングにより、指定したデバイス以外からのデータを受信しない
- 影響
  - 不正なデータが蓄積され、エアコン等の消費電力量の増大や屋内環境の悪化による経済、健康被害

2-1 不正なデバイスからのデータ送信
攻撃イメージ図



今回の実機環境

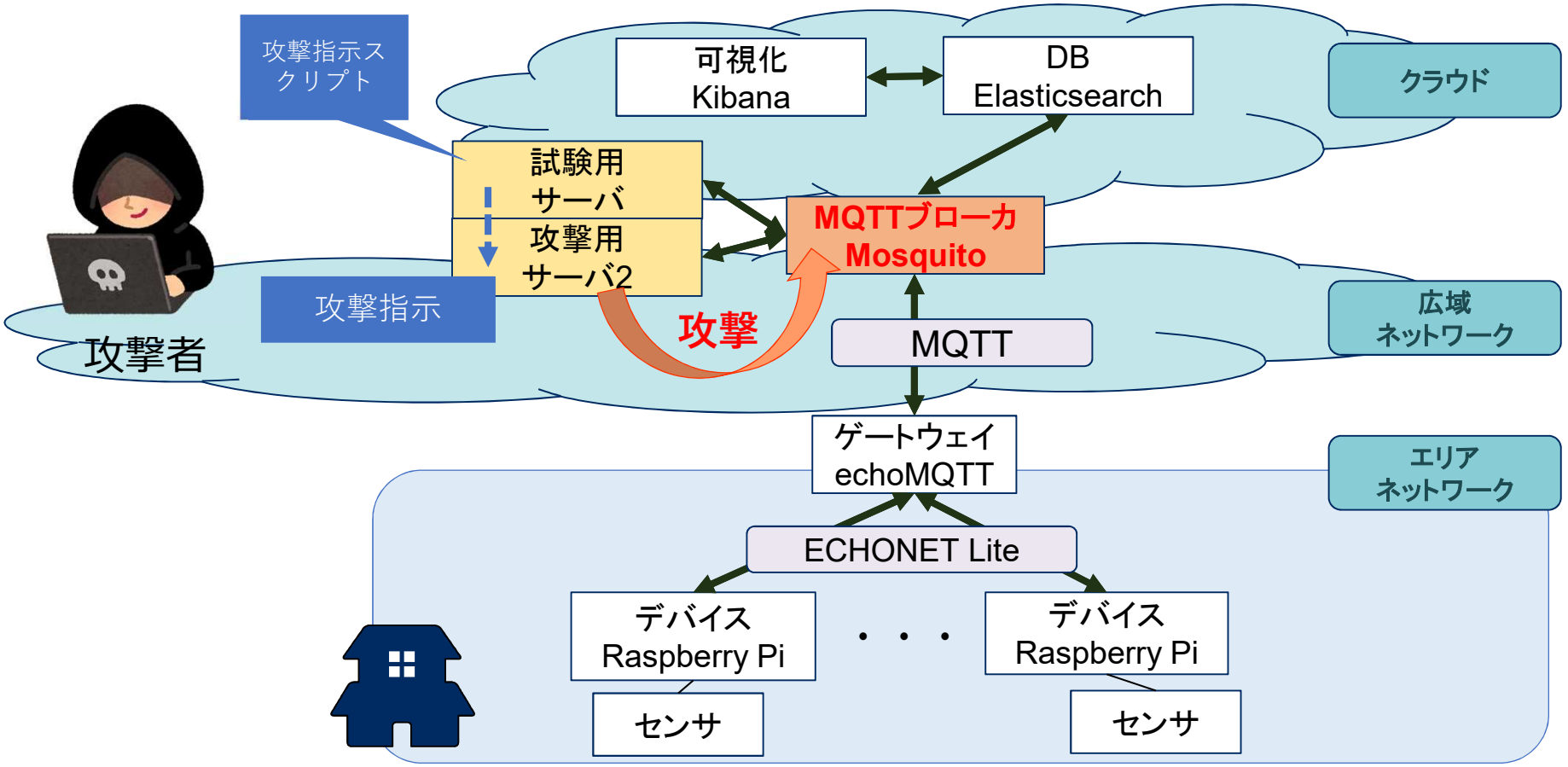
2-1 不正なデバイスからのデータ送信 実習内容

- 問題
  - エリアネットワークに不正なデバイスが設置されている
- 攻撃内容
  - 不正に設置されたデバイスが不正なセンサ値を保持するECHONET Liteデバイスとして動作
- 対策
  - 許可したデバイス以外からのデータをゲートウェイが受信しないようにファイアウォールを設定
- 防御の可否
  - 不正なデバイスからのデータ受信あり: 赤LED1が点灯
  - 不正なデバイスからのデータ受信なし: 青LED1が点灯

2-1 不正なデバイスからのデータ送信対策手順例

- Kibanaを参照し、正常状態を確認する
- Raspberry Pi(正常なデバイス)のIPアドレスを確認
  - $ ip addr
- 講師側の不正デバイスプログラム実行後、Kibanaを参照し、異常状態であることを確認
- ゲートウェイの設定ファイルを書き換えることでデバイスを指定
- ファイアウォールの設定をUDPに対して行う
  - sudo iptables -A INPUT -p udp --dport 3610 –s 10.10.XXX.YYY -j ACCEPT
    - 10.10.XXX.YYYはRaspberry PiのIPアドレス
  - sudo iptables -A INPUT -p udp --dport 3610 –s 0.0.0.0/0 -j DROP
  - sudo Iptables -L
- Kibanaを参照し、データが正常状態に戻ることを確認する

クラウドへの攻撃
攻撃イメージ図

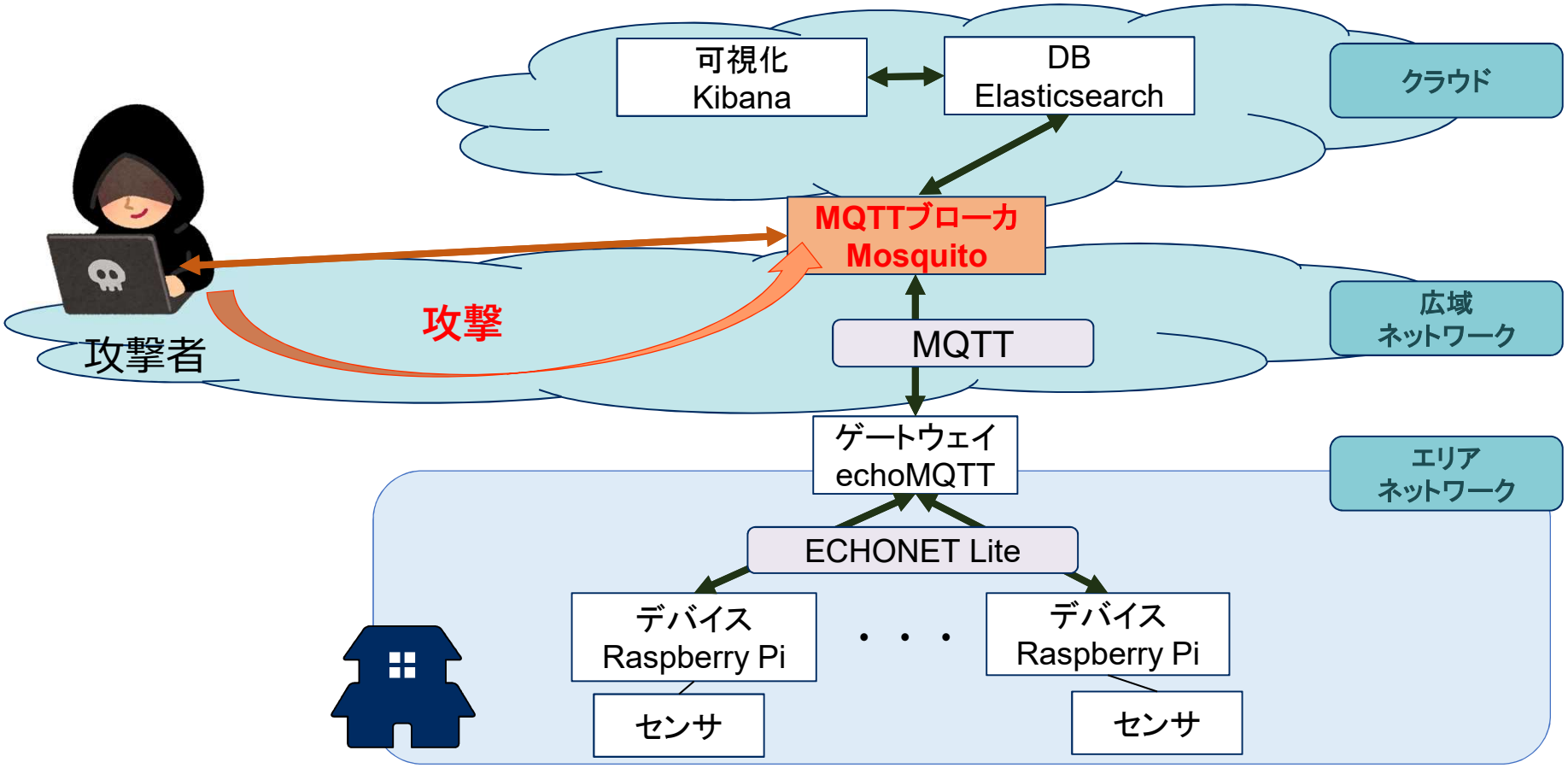


今回の実機環境

3-1 クラウド側の要塞化(外との通信) 概要

- 攻撃対象
  - クラウド
- 攻撃手法
  - 攻撃者がクラウドに不正に接続
  - 事実と異なる値のセンサデータをクラウドに送信
- 脆弱性
  - クラウドのセキュリティ強度が低い
  - クラウドは、アクセス制限がなく、すべての通信を受け取る
- 防御
  - クラウドのファイアウォール設定を行う
  - クラウドに接続してくるゲートウェイの認証を行う
- 影響
  - 不正なデータが蓄積され、温熱環境や電力利用の学習データが最適化されないことによる、機器の異常動作や経済被害

3-1 クラウド側の要塞化（外との通信）
攻撃イメージ図



今回の実機環境

3-1 クラウド側の要塞化(外との通信)
実習内容

- 問題
  - クラウド(MQTTブローカ)が全てのゲートウェイからの通信を受信可能
- 攻撃内容
  - 攻撃用サーバが事実と異なるセンサデータをクラウド(MQTTブローカ)に送信
- 対策
  - 許可するゲートウェイ以外のアクセスを禁止する
- 防御の可否
  - 攻撃用サーバがクラウド（MQTTブローカ）へ通信成功: 赤LED1が点灯
  - 攻撃用サーバがクラウド（MQTTブローカ）へ通信失敗: 青LED1が点灯

3-1 クラウド側の要塞化(外との通信)対策手順例

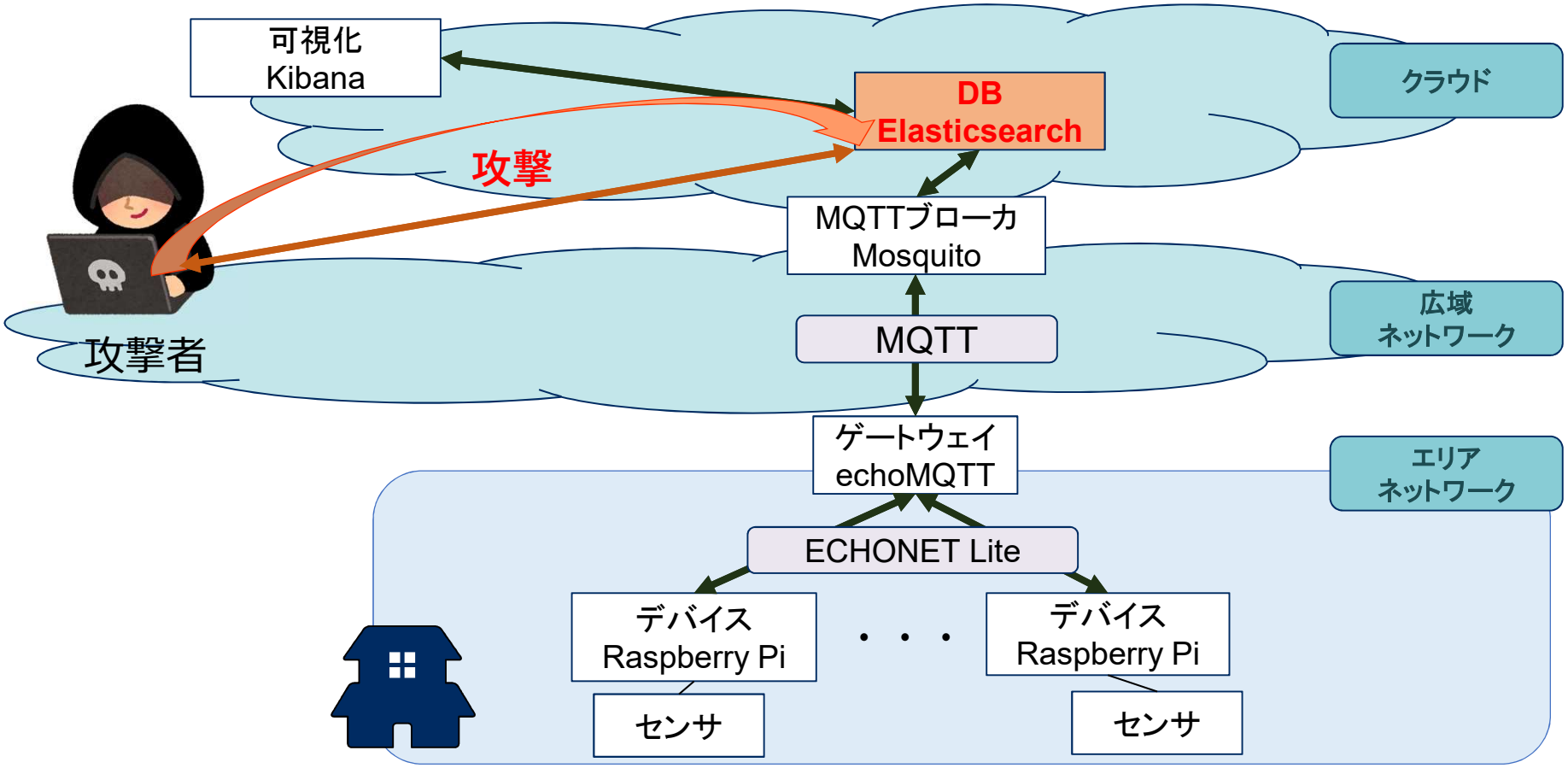
- Kibanaを参照し、正常状態を確認する
- 講師側の攻撃プログラム実行後、Kibanaを参照し、異常状態であることを確認
- クラウド側のファイアウォールの設定を変更し必要なサーバの通信のみ許可する設定とする
  - $ sudo iptables -I DOCKER-USER –i eno1 –p tcp –s 0.0.0.0/0 --dport 1883 –j DROP
  - $ sudo iptables –I DOCKER-USER –p tcp –s 10.10.99.14 --dport 1883 –j ACCEPT
  - $ sudo iptables –L
- Kibanaを参照し、データが正常状態に戻ることを確認

3-2 クラウド側の要塞化 (クラウドアプリケーション間の通信)

概要

- 攻撃対象
  - クラウド
- 攻撃手法
  - 攻撃者がクラウドに不正に接続し、センサデータを削除する
- 脆弱性
  - クラウド(Elasticsearch)は、ユーザ権限設定が設定できない
- 防御
  - クラウド(Elasticsearch)がセットアップされているサーバにファイアウォール設定を行う
- 影響
  - センサデータや個人データの改ざんや削除、情報流出がなされ、企業イメージの低下や対応費用などの経済被害

3-2 クラウド側の要塞化（クラウドアプリケーション間の通信）攻撃イメージ図



今回の実機環境

3-2 クラウド側の要塞化 (クラウドアプリケーション間の通信)

実習内容

- 問題
  - Elasticsearchにアクセス制限が設定されていない
- 攻撃内容
  - 攻撃者がElasticsearchにアクセスし過去1時間のデータを削除する
- 対策
  - 外部からのElasticsearchへのアクセスを禁止
- 防御の可否
  - デバイスがデータ削除に成功: 赤LEDが点灯
  - デバイスがデータ削除に失敗: 青LEDが点灯

3-2 クラウド側の要塞化 (クラウドアプリケーション間の通信) 対策手順例

- Kibanaを参照し、正常状態を確認する
- 講師側の攻撃プログラム実行後、Kibanaを参照し、異常状態であることを確認
- ファイアウォールの設定を変更
  - Elasticsearchの利用するポート(9200番)の全てのTCPパケットをDROP
    - $ sudo iptables -I DOCKER-USER –i eno1 –p tcp –s 0.0.0.0/0 --dport 9200 –j DROP
  - 10.10.99.14からのみをACCEPT
    - $ sudo iptables –I DOCKER-USER –p tcp –s 10.10.99.14 --dport 9200 –j ACCEPT
  - iptableの表示
    - $ sudo iptables –L
- Kibanaを参照し、データが正常状態に戻ることを確認

参考資料8

IoTシステムにおけるセキュリティ
-スマートホーム技術におけるIoTシステムを例として-

試験準備

試験で利用する環境

- 実習で利用したIoTシステム環境をそのまま利用する
  - IoTデバイス
    - Raspberry Pi + センサ + LED + ヒータ
  - ゲートウェイ
    - PC内で動作させるechoMQTT
  - クラウド
    - PC内で動作させるKibana、Elasticsearch、Fluentd、MQTTブローカ

試験準備

- 試験用SDカードを配布
- (PCのファイアウォールを初期化)
- IoTシステム環境の動作
  - デバイス(Raspberry Piのhumming)
  - ゲートウェイ(PCのechoMQTT)
  - クラウド(PCのdocker環境)

試験内容

- 試験環境(PC(ゲートウェイやクラウド)、Raspberry Pi)に仕組まれた脆弱性や攻撃について調査し対策を行う。

要求事項

- Raspberry Pi
  - ECHONET Liteデバイスとして動作しゲートウェイからのリクエストを処理
  - センサからの情報を正しくゲートウェイに送信
  - エリアネットワーク内のデバイスやゲートウェイからsshによるリモートログインを許可
- PC
  - デバイスから送信されたセンサ情報(温度、湿度、気圧)を収集しElasticsearchに保存
  - 保存したデータはKibanaで可視化
  - 試験用サーバ(10.10.99.15)からのMQTT(TCP ポート1883)への接続を許可
  - 試験用サーバ(10.10.99.15)からのElasticsearch(TCP ポート9200)への接続を許可

ヒント

- 間違えてiptablesを実行してしまった場合の対処方法
  - 詳細を表示するためのコマンド
    - sudo iptables –L
  - ルール番号の確認方法
    - sudo iptables –L --line-numbers
  - ルールの削除方法
    - sudo iptables –D INPUT (ルール番号)
    - sudo iptables –D DOCKER-USER (ルール番号)

参考資料9

IoTシステムにおけるセキュリティ
-スマートホーム技術におけるIoTシステムを例として-

試験内容

1-1デバイスへの不正ログイン

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - Raspberry Piのユーザpiにデフォルトパスワードが設定されている
  - 脆弱なアカウントが追加されている

1-2 センサの状態偽装

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - センサの状態を偽装したフレームを送信するプログラムがRaspberry Pi上に存在し起動時に実行

1-3 デバイスのプロパティ値変更

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - エリアネットワークに不正に接続されたデバイスがLEDを制御するECHONET Liteリクエストを Raspberry Piに送信

1-4 不正なセンサデータ送信

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - 物理的にセンサにヒータ取り付け
  - ヒータをコントロールし、１分ごとにオンとオフを繰り返すプログラムが起動時に実行

1-5 ポートスキャン

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - Webサーバ(Apache2)が起動時に実行
  - ファイル共有サーバ(Samba)が起動時に実行

2-1 不正なデバイスからのデータ送信

- 攻撃対象
  - ゲートウェイ(PC)
- 問題
  - エリアネットワークの不正なデバイス設置
  - 不正なデバイスが異常なセンサ値を持つECHONET Liteデバイスとして動作

3-1 クラウド側の要塞化(外との通信)

- 攻撃対象
  - クラウド(PC)
- 問題
  - 攻撃システムが不正なセンサ値を持つMQTTメッセージをクラウドに送信

3-2 クラウド側の要塞化(クラウドアプリケーション間の通信)

- 攻撃対象
  - クラウド(PC)
- 問題
  - 攻撃システムがデータ消去リクエストをクラウド(Elasticsearch)に送信

参考資料10

IoTシステムにおけるセキュリティ
-スマートホーム技術におけるIoTシステムを例として-

試験解説

1-1デバイスへの不正ログイン

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - Raspberry Piのユーザpiにデフォルトパスワードが設定されている
  - 脆弱なアカウントが追加されている
    - ID: user
    - Pass: 123456
- 対策例
  - ユーザpiのパスワード変更
  - userアカウントの削除
    - $ sudo userdel –r user
- 検査方法
  - sshでデフォルトユーザ(pi)にデフォルトパスワードでログイン可能であるか確認
  - sshでuserアカウントにログイン可能であるか確認

1-2 センサの状態偽装

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - センサの状態を偽装したフレームを送信するプログラムがRaspberry Pi上に存在し起動時に実行
    - 実行スクリプト: /usr/local/echonet/run.sh
- 対策例
  - lsofによりプログラムの場所を確認
  - /usr/local/echonetの削除
  - 問題のあるプロセス停止

- 検査方法
  - データベース(Elasticsearch)にアクセスし過去5分間に故障しているという情報が存在するか確認

1-3 デバイスのプロパティ値変更

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - エリアネットワークに不正に接続されたデバイスがLEDを制御するECHONET Liteリクエストを Raspberry Piに送信
- 対策例
  - 指定されたゲートウェイ以外からの接続を拒否するようにRaspberry Piのファイアウォールの設定を行う
  - ファイアウォール設定例(10.10.xxx.yyy はゲートウェイのIPアドレスを指定)
    - /sbin/iptables -A INPUT -p udp --dport 3610 –s 10.10.xxx.yyy -j ACCEPT
    - /sbin/iptables -A INPUT -p udp --dport 3610 -s 0.0.0.0/0 -j DROP
    - /sbin/iptables –L
- 検査方法
  - エリアネットワーク内に設置した不正デバイスからRaspberry Piに対してECHONET LiteによるLED制御を行い、その可否を確認

1-4 不正なセンサデータ送信

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - 物理的にセンサにヒータ取り付け
  - ヒータをコントロールし、１分ごとにオンとオフを繰り返すプログラムが起動時に実行
    - /usr/local/bin/heater.sh
- 対策例
  - /usr/local/bin/heater.shを削除
  - センサからヒータを取り外す
- 検査方法
  - ヒータがオンとオフを繰り返しているか目視する

1-5 ポートスキャン

- 攻撃対象
  - デバイス(Raspberry Pi)
- 問題
  - Webサーバ(Apache2)が起動時に実行
  - ファイル共有サーバ(Samba)が起動時に実行
- 対策例
  - netstatでポートが開いていることを確認
  - ポートを開けているプロセスの確認
  - Webサーバ停止
    - sudo systemctl stop apache2
  - ファイル共有サーバ停止
    - sudo systemctl stop smbd
    - sudo systemctl stop nmbd
- 検査方法
  - 攻撃システムからポートスキャンを行うことでSamba及びApache2関連のTCPポートの開閉状態を確認
  - 攻撃システムからポートスキャンを行うことでSamba関連のUDPポートの開閉状態を確認

2-1 不正なデバイスからのデータ送信

- 攻撃対象
  - ゲートウェイ(PC)
- 問題
  - エリアネットワークの不正なデバイス設置
  - 不正なデバイスが異常なセンサ値を持つECHONET Liteデバイスとして動作
  - データベースに異常なセンサ値のデータ登録
    - 温度センサ: 3000度, 湿度: 0%, 気圧: 10hPa
- 対策例
  - 設置したデバイス以外との間でECHONET Lite通信を行わないようにPCのファイアウォールを設定(10.10.XXX.YYY はRaspberry PiのIPアドレス)
  - iptables -A INPUT -p udp --dport 3610 –s 10.10.XXX.YYY -j ACCEPT
  - iptables -A INPUT -p udp --dport 3610 –s 0.0.0.0/0 -j DROP
  - Iptables -L
- 検査方法
  - データベース(Elasticsearch)にアクセスし過去5分間に異常なセンサ値の情報が存在するか確認

3-1 クラウド側の要塞化(外との通信)

- 攻撃対象
  - クラウド(PC)
- 問題
  - 攻撃システムが不正なセンサ値を持つMQTTメッセージをクラウドに送信
    - 温度センサ: -3000度, 湿度: -100%, 気圧: -3000hPa
- 対策例
  - 試験用サーバから送られるMQTTメッセージのみ受信を許可
  - $ sudo iptables -I DOCKER-USER –i eno1 –p tcp –s 0.0.0.0/0 --dport 1883 –j DROP
  - $ sudo iptables –I DOCKER-USER –p tcp –s 10.10.99.15 --dport 1883 –j ACCEPT
  - $ sudo iptables -L
- 検査方法
  - データベース(Elasticsearch)にアクセスし過去5分間に異常なセンサ値の情報が存在するか確認

3-2 クラウド側の要塞化(クラウドアプリケーション間の通信)

- 攻撃対象
  - クラウド(PC)
- 問題
  - 攻撃システムがデータ消去リクエストをクラウド(Elasticsearch)に送信
- 対策例
  - 攻撃システムのIPアドレスからのメッセージの受信を禁止
  - $ sudo iptables -I DOCKER-USER –i eno1 –p tcp –s 0.0.0.0/0 --dport 9200 –j DROP
  - $ sudo iptables –I DOCKER-USER –p tcp –s 10.10.99.15 --dport 9200 –j ACCEPT
  - $ sudo iptables -L
- 検査方法
  - 攻撃システムからElasticsearchにアクセスしデータの量を確認

参考資料11

第二段階自己評価フィードバック質問票

2019/12/20

項番	項目1	項目2	設問	選択肢	必須
（1～10）振り返りで回答頂く項目【必須】					
第二段階自己評価結果をフィードバックします。結果を確認の上、質問へのご回答をお願い致します。					
1	第二段階自己評価	I.第二段階自己評価について	あなたは、第二段階自己評価結果を見て、受講前・受講後の自分の能力の変化を実感できましたか？	1.出来た 2.やや出来た 3.どちらともいえない 4.あまり出来なかった 5.まったく出来なかった	必須
2	第二段階自己評価	I.第二段階自己評価について	1.の回答の理由を、自由に記述してください。	自由記述	必須
3	第二段階自己評価	Ⅱ.学習成果について	あなたは、第二段階の学習を通し、各知識・技術項目のうち、どの項目に関して、最も知識を増やすことができたと感じましたか？知識・技術項目を一つ選び、理由を記述してください。	1-1.Linuxの操作 1-2.SSHによる通信 1-3.I2C通信 1-4.RaspberryPIの基本的な操作 1-5.RaspberryPIのIOを用いた入出力 1-6.ECHONET Liteによる制御 1-7.MQTTによる制御 1-8.Kibanaによるデーターの可視化 1-9.Elasticsearchによるデーターベースの構築 2-1.デバイスへの攻撃で受ける影響 2-2.デバイスへの攻撃に対する一般的な対処 2-3.ゲートウェイへの攻撃で受ける影響 2-4.ゲートウェイへの攻撃に対する一般的な対処 2-5.クラウドへの攻撃で受ける影響 2-6.クラウドへの攻撃に対する一般的な対処 2-7.デバイスへの不正ログイン 2-8.デバイスのプロパティ値変更 2-9.センサの状態偽装 2-10.不正センサデータ送信 2-11.ポートスキャン	必須
4	第二段階自己評価	Ⅱ.学習成果について	3.の理由を、自由に記述してください	自由記述	必須
5	第二段階自己評価	Ⅱ.学習成果について	あなたは、第二段階の学習を通し、各知識・技術項目のうち、どの項目に関してさらに知識を増やす必要があると感じましたか？知識・技術項目を一つ選び、理由を記述してください。	1-1.Linuxの操作 1-2.SSHによる通信 1-3.I2C通信 1-4.RaspberryPIの基本的な操作 1-5.RaspberryPIのIOを用いた入出力 1-6.ECHONET Liteによる制御 1-7.MQTTによる制御 1-8.Kibanaによるデーターの可視化 1-9.Elasticsearchによるデーターベースの構築 2-1.デバイスへの攻撃で受ける影響 2-2.デバイスへの攻撃に対する一般的な対処 2-3.ゲートウェイへの攻撃で受ける影響 2-4.ゲートウェイへの攻撃に対する一般的な対処 2-5.クラウドへの攻撃で受ける影響 2-6.クラウドへの攻撃に対する一般的な対処 2-7.デバイスへの不正ログイン 2-8.デバイスのプロパティ値変更 2-9.センサの状態偽装 2-10.不正センサデータ送信 2-11.ポートスキャン	必須
6	第二段階自己評価	Ⅱ.学習成果について	5.の理由を、自由に記述してください	自由記述	必須
7	第二段階自己評価	Ⅱ.学習成果について	あなたは、第二段階の学習を通し、各知識・技術項目のうち、どの項目が実業務に活用できそうだと感じましたか？知識・技術項目を一つ選び、理由を記述してください。	1-1.Linuxの操作 1-2.SSHによる通信 1-3.I2C通信 1-4.RaspberryPIの基本的な操作 1-5.RaspberryPIのIOを用いた入出力 1-6.ECHONET Liteによる制御 1-7.MQTTによる制御 1-8.Kibanaによるデーターの可視化 1-9.Elasticsearchによるデーターベースの構築 2-1.デバイスへの攻撃で受ける影響 2-2.デバイスへの攻撃に対する一般的な対処 2-3.ゲートウェイへの攻撃で受ける影響 2-4.ゲートウェイへの攻撃に対する一般的な対処 2-5.クラウドへの攻撃で受ける影響 2-6.クラウドへの攻撃に対する一般的な対処 2-7.デバイスへの不正ログイン 2-8.デバイスのプロパティ値変更 2-9.センサの状態偽装 2-10.不正センサデータ送信 2-11.ポートスキャン	必須
8	第二段階自己評価	Ⅱ.学習成果について	7.の理由を、自由に記述してください	自由記述	必須
9	第二段階自己評価	III.総合評価	あなたにとって第二段階の学習は、どの程度役に立ちましたか？	1.大変役だった 2.役だった 3.どちらともいえない 4.役立たなかった 5.まったく役だだなかった	必須
10	第二段階自己評価	III.総合評価	第二段階の学習は、ほかの人に推薦したいと思いますか？	1.とてもそう思う 2.そう思う 3.どちらともいえない 4.そう思わない 5.まったくそう思わない	必須
（11～21）第二段階教育全体に関するご意見について【必須】					
第二段階に関してのご意見をお伺い致します。既に皆様より頂きました意見のうち、代表的な意見につきましては、以下の問11～21に記載をしておりますので、各ご意見に関し3択(そう思う・そう思わない・その他)でお答えください。追加のご意見があれば、自由記述欄に記載をお願いいたします。					
11	第二段階教育全体	シラバス	実習ではLinux OSを利用するため、受講前提条件に「Linuxの基本操作ができること」があると良い。	1.そう思う 2.そう思わない 3.その他	必須
12	第二段階教育全体	シラバス	Raspberry Pi とセンサを接続する手順を、細かくステップに分けると良い。	1.そう思う 2.そう思わない 3.その他	必須
13	第二段階教育全体	シラバス	コマンド操作に慣れていない受講者のため、シェルスクリプトを事前に配布すると良い。	1.そう思う 2.そう思わない 3.その他	必須
14	第二段階教育全体	シラバス	実習で取り上げた各技術（ECHONET Liteなど）に対し、セキュリティ観点で気を付けるポイントの説明があると良い。	1.そう思う 2.そう思わない 3.その他	必須
15	第二段階教育全体	シラバス	実習に際し、各章の冒頭で、システム概要図を示すだけでなく実機でのデモを行うと、イメージが湧きやすいと感じた。	1.そう思う 2.そう思わない 3.その他	必須

参考資料11

第二段階自己評価フィードバック質問票

2019/12/20

項番	項目1	項目2	設問	選択肢	必須
16	第二段階教育全体	シラバス	脆弱性の対処後、対策が出来ているか分かりやすくするため、攻撃者画面を示すなどビジュアルで説明すると良い。	1.そう思う 2.そう思わない 3.その他	必須
17	第二段階教育全体	シラバス	実際の運用時には、脅威分析が必要になると思われるため、講義内容に盛り込むと良い。	1.そう思う 2.そう思わない 3.その他	必須
18	第二段階教育全体	シラバス	脅威分析については、講師より、実務での経験に基づく解説があると良い。	1.そう思う 2.そう思わない 3.その他	必須
19	第二段階教育全体	シラバス	各受講者の進捗を確認できるツールを使うと、実習がスムーズに進行できると感じた。	1.そう思う 2.そう思わない 3.その他	必須
20	第二段階教育全体	シラバス	第一段階(e-learning)と第二段階(実習)の繋がりについて、戸惑いを感じた。	1.そう思う 2.そう思わない 3.その他	必須
21	第二段階教育全体	テスト	プレゼン用にテンプレートがあると、作成しやすいと感じた。	1.そう思う 2.そう思わない 3.その他	必須
自由記述【任意】					
-			自由記述	自由記述	