IPA Better Life with IT

IoTセキュリティ教材サンプル

2020年11月18日

独立行政法人情報処理推進機構（IPA）
社会基盤センター　産業プラットフォーム部

7. 教材の概要（1:カリキュラム）

90分×15コマ分

回	テーマ	項目
1	IoTのビジョンとIoTセキュリティ	IoTの特徴、IoTセキュリティの侵害事例、IoTのアーキテクチャ、他
2	IoTデバイスと実世界インタフェース	組込みシステム、IoTデバイス、MCU、リアルタイム処理、他
3	制御システムセキュリティ	制御とは、センサーとセキュリティ、工場の制御システム、他
4	IoTネットワークとエッジコンピューティング	IoTネットワークに対する脅威、IoT無線ネットワーク、他
5	ハードウェアセキュリティとセキュアデバイス	IoTのハードウェア攻撃、非侵襲攻撃、侵襲攻撃、半侵襲攻撃、他
6	IoTデバイスのセキュリティ(演習)	IoTデバイスのデータ保護、暗号鍵、暗号通信、平文通信、他
7	車載エレクトロニクスのセキュリティ	コネクティッドカーの情報セキュリティと攻撃事例、車載LAN、他
8	IoTの機能安全	機能安全と本質安全、安全分析手法(リスク分析、ハザード分析)、他
9	セキュリティ・バイ・デザインと脅威分析(1)	セキュリティ・バイ・デザインとは、ソフトウェア開発ライフサイクル、他
10	セキュリティ・バイ・デザインと脅威分析(2)	攻撃分析、脅威モデリング、アタックツリー、脅威分析、他
11	IoTの脅威分析(演習)	スマートホームの脅威分析、IoTデバイスの脆弱性検査計画
12	IoTを取り巻く法制度	IoTの法的定義・構造、Internet・of・Thingsそれぞれに関する法、他
13	IoTセキュリティの運用と規格	記録・ログ、セキュリティアップデート、IoTセキュリティ情報の収集、他
14	IoTの脆弱性検査（演習）	スマートホームの脆弱性検査1
15	IoTの脆弱性検査（演習）	スマートホームの脆弱性検査2

1. IoTのビジョンとIoTセキュリティ

IoT(Internet of Things)

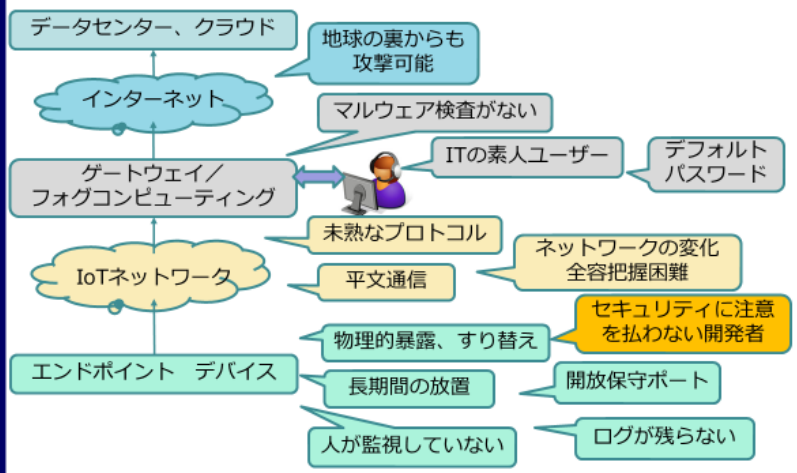
IoTセキュリティ教材

- IDCによるIoTの定義： IP接続を用いて、人間が介在することなく通信する、一意に識別できる末端（または「モノ」）がつながるネットワークのネットワーク
  - 標準に則り、どこからでもつながる （赤外線リモコンなどは除外）
  - モノ同士が、人の見ていないところでM2M通信を行う
    - PCやスマートフォンは、Internet of People
  - 中央集権的コントローラがいない

官民データ活用推進基本法

IoTの弱み

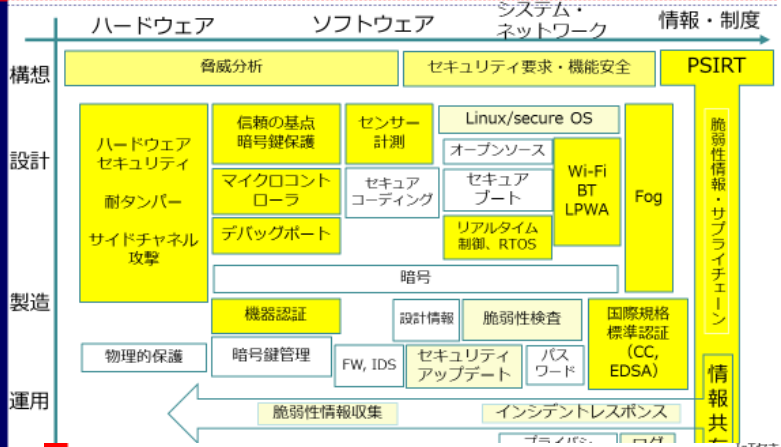
IoTセキュリティ教材



49

IoTセキュリティの構造

IoTセキュリティ教材



ITとIoTのセキュリティ

IoTセキュリティ教材

	IT	IoT
セキュリティ脅威（攻撃目的）	個人情報や営業秘密の漏えい 個人や組織へのいやがらせ ランサムウェア-人間を攻撃	DDoSのボット化 システムの停止、誤動作 機器偽造やなりすまし（すり替え） センサデータ改ざん -機械を攻撃
プラットフォーム	PC、スマートフォン Windows、Linux、Android WWW、データベース	多様なIoTデバイス、非力なMCU リアルタイムOS
ネットワークとプロトコル	光、メタル、無線 TCP/IP, TLS, DNS, POPS,HTTPS	無線（Wi-Fi, Bluetooth, Zigbee, LPWA) TCP/IP、MQTT、HTTP
デバッグポート	Windows update, ssh, https	telnet, jtag, uart
ログイン認証	パスワード、証明書 バイオメトリクス	デフォルトﾊﾟｽﾜｰﾄﾞ、メッセージ認証 埋め込まれた鍵
セキュリティ実行者	ユーザー 情報システム部、専門家	機器の設計・開発者 IoTサービス運用者
攻撃法	不正アクセス、DoS マルウェア、標的型メール	不正アクセス（TCP/IP)、DDoS リバースエンジニアリング、サイドチャネル攻撃

53

2. IoTデバイスと実世界インタフェース

組込み・非組込みソフトウェア

IoTセキュリティ教材 IPA

	非組込みソフトウェア	組込みソフトウェア
オペレーティングシステム	Windows*, Linux*	RTLinux, RTOS (iTron, Toppers, ThreadX, mbed) , Android, iOS, OSレス
言語開発システム	C++, Java, SQL, Perl, Python, Lisp, PHP, *sh, Eclipse, Struts	C, C++ Matlab Simulink, ICE, CS+, Eclipse
入出力	ハードディスク, キーボード, マウス, 高解像度LCD, スピーカ, マイク	センサ（温度、圧力、加速度、ジャイロ、気圧、画像、3D距離、音響…), ADC, DAC, PWM, I²C、SPI, モーター, 弁, リレー
ネットワーク	Ethernet, USB, TCP/IP	Wi-Fi, USB, Bluetooth, 赤外線, NFC, 3-4G, CAN, ZigBee, LoRa
ミドルウェア	Webブラウザ/サーバ, DBMS, ODBC, コンパイラ, XML, CORBA, Open-CV、Tensorflow	TCP/IPスタック, RTM, ROS
アプリケーシ	オフィスソフト, Webアプリケーション, 会計・金融、科学技術計	プリンタ・複写機, ネットワーク機器, カーナビ, スマートフォン, デジタルカ

リアルタイムカーネル（RT-OS）

IoTセキュリティ教材 IPA

■ リアルタイム処理の実現には、リアルタイム・カーネルが必要。リアルタイムカーネルは、汎用OSのカーネルと何が違うのか？

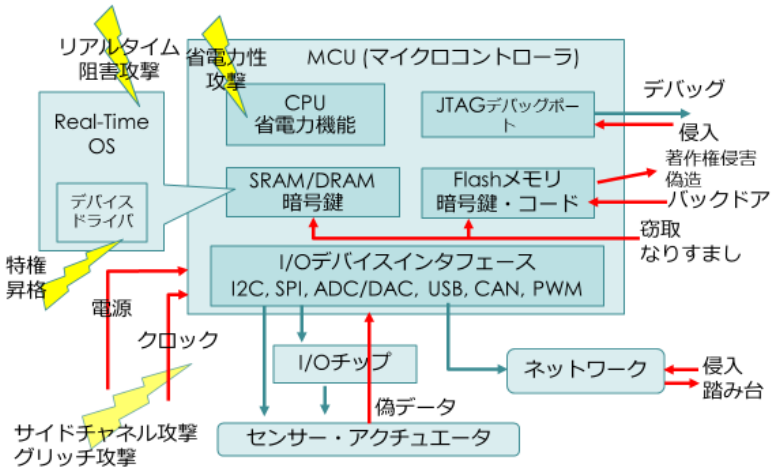
RT-OSでは、
- プロセスの優先度に厳格に従ってスケジューリングする
- 外部割込みで、タイマーを待たず、即座にプロセスを実行させる、プリエンプティブタスクスイッチ
- 専用のレジスタセットを設け、割り込み禁止時間を最低限にする
- μsオーダの指定時刻(周期）でプロセスを起動

汎用OSでは、
- プロセスの優先度は、参考値であって、必ずしも守られない
- プロセススイッチは、10msごとのタイマー割り込み時に限定
- ネットワーク処理などで、長い（10msオーダ）割り込み禁止時間が入る
- 時刻指定は、秒オーダ

- 本当は、作業の終了時刻を制御したいのだが、作業にかかる時間を正確には予測できないので、作業を開始する順序を優先度で制御する
- 仮想記憶、キャッシュメモリなどは、実行時間を変動させるので、リアルタイム

IoTデバイスの構造とセキュリティ

IoTセキュリティ教材 IPA



15

組込み系の各種デバイスインタフェース

IoTセキュリティ教材 IPA

情報系	インタフェース名	使用目的等
ビット	GPIO	スイッチ入力、ロック開閉、LED点滅
ストレージ	SCSI, ATAPI, SATA	HDD接続
パラレル	セントロニクス、GPIB	プリンタや計測器、今では使われない
シリアル	RS-232c, RS-422, RS-485	UART
	I2C, SPI	センサー接続に使われる
	I2S, S/PDIF	オーディオ信号
	JTAG	開発・デバッグ、更新
ネットワーク	Ethernet, CAN, Wi-Fi, Bluetooth	
ディスプレイ	VGA	アナログ
	DVI, HDMI, DisplayPort	デジタル~4k
	LVDS	組み込み用のLCD
アナログ	ADC DAC、PWM	アナログ電圧とデジタル値の変換 PWMは、パルス幅に変換
USB	USB-host, device, OTG	USBの上に、シリアル、ネットワークなどを載せられる

48

3.制御システムセキュリティ

制御とは

IoTセキュリティ教材 IPA

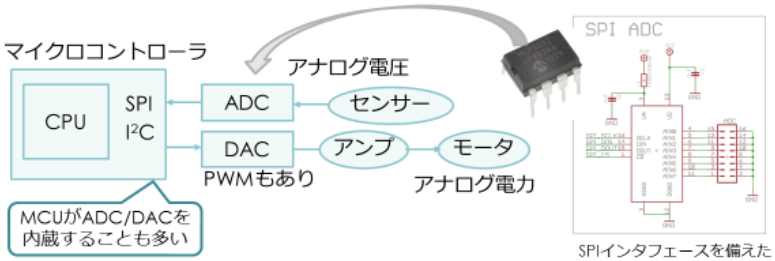
- 対象に期待する動作をさせる
  - 電車を乗客が待つ定位置で止める
  - 部屋の温度を20度に保つ
  - 原子炉内の核分裂を一定の速度で進める
  - マウスの移動に応じて画面のカーソルを移動させる
- 制御を行えるためには
  - 望ましい状態を目標値として表現できる。
  - 現在の状況を測定値として取得できる。
  - 対象の状態を変化させるために、適当な値を加えることができる。
  - 上記の適当なエネルギー操作量を制御アルゴリズム計算で求めることができる。

目で速度や負荷を見て細い鞭を振る

センサーをつなぐ

IoTセキュリティ教材 IPA

- センサーは、力学的、化学的、熱学的物理量をアナログ電圧として得て、ADC(アナログデジタル変換器）でデジタル値に変換
- 時間、ロータリーエンコーダなど、パルスをカウントしてデジタル値を得る場合もある
- デジタル値に変換されたセンサー値は、I²Cや、SPIなどのデバイスインタフェースでマイクロコントローラに送られる。
- アクチュエーションは逆向きに、DACを使ってアナログ値にされる



18

制御システムセキュリティの特性

IoTセキュリティ教材 IPA

- インターネットにつながない
  - ところが、インターネット経由の保守に使い始めた
  - さらに、USBメモリを使うことがある
- 工場用の特殊OS、専用ネットワーク
  - 特殊と言っても規格品、次第に安い汎用品を使い出した
- 実時間制御だけだから抜かれる情報はない
  - システムを停止させたり誤動作させる危険性がある
  - 実時間性が阻害されるので、暗号で守りにくい
- 長期間の安定稼働
  - 古いシステムが使い続けられる
  - セキュリティアップデートできない
- 閉じたコミュニティ
  - 機器の所在を把握可能なことが多い
  - 情報共有が行われにくい

可用性と安全性の重視！？パスワードを忘れても困らないようにマニュアルで迂回方法が説明してある場合もある。認証に時間をかけることは危険との考えもある。

制御システムに学ぶIoTセキュリティ

IoTセキュリティ教材 IPA

	制御システム	IoT
プラットフォーム	Linux、RTOS、独自OS	Linux、RTOS、OSレス
アプリケーション	固定的	固定的、開放的
ライフサイクル	長期運用	長期運用、放置
セキュリティ・アップデート	システムを止められない場合、困難	監視が行き届かない場合は困難
保守ポート	TELNET, USB	telnet, USB JTAG, OBDⅡ
ネットワーク	有線LAN、フィールドバス	無線LAN、公衆3G/4G、Bluetooth, CAN, LPWA
設定・管理	専門家	素人ユーザー

63

4. IoTネットワークと エッジコンピューティング

Wi-Fiのセキュリティ対策？

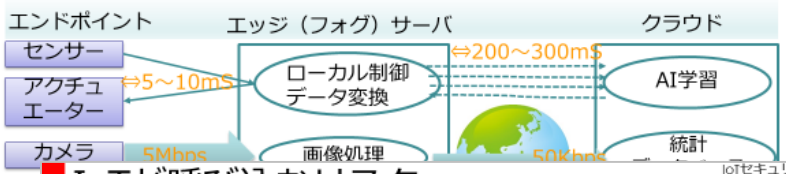
IoTセキュリティ教材 IPA

- SSID(Service Set ID)ステルス機能
  - アクセスポイントの識別子SSIDを非公開とする
  - しかし、SSIDは暗号化されておらず、解析ツールを使えば容易にわかる。また、自動接続を設定した子機はSSIDを発呼し続ける。
- MACアドレスフィルタリング
  - アクセスポイントに登録したMACアドレスを持つ端末だけを接続許可
  - しかし、MACアドレスは容易に偽装が可能。
- WEP
  - 暗号鍵はアクセスポイントに一つで子機に共通なので、危険性大
  - 暗号化に使う鍵データの生成方法が単純で、数秒で解析可能
  - 通信データの改ざん検知ができない。
- WPA
  - 親機に登録するパスフレーズをもとに、子機ごとに異なる暗号鍵を生成
  - WPA2完成までの暫定リリース

エッジ（フォグ）コンピューティング

IoTセキュリティ教材 IPA

- クラウドコンピューティングでは、毎回海外のDCまで通信が往復する遅延 (200～300mSなど)によって、実時間処理が困難
- 個人情報や産業情報が海外のクラウドに流出する懸念がある
- エッジコンピューティングは、電話局や構内、車内など、エンドポイントに近いところに中間サーバを設置し、ローカルにリアルタイム処理を行う
  - フォグコンピューティングは、さらにエンドポイント近くに置く
- IoTアーキテクチャで述べた、IoTゲートウェイの役割も果たす



IoT無線ネットワークまとめ

IoTセキュリティ教材 IPA

1. IoTでは、速度よりも、消費電力、到達距離を優先するため、新しい変調方式とインフラ(物理層)、またプロトコル(DL層)が必要となる。
2. IoT向けのプロトコルは多数提案されており、現状では統一は難しい。
   - SIGFOX: 免許不要で、上りの小容量通信に特化し到達距離が長い。
   - LoRaWAN: 免許不要で、双方向通信可能でWi-Fiより距離が長い。
   - NB-IoT: LTEの追加規格で、携帯電話網でグレードが高い。
   - Wi-Fi, Bluetooth, ZigBeeなどの既存規格もIoT向きの拡張が施されている
3. IoT通信方式に脆弱性の見つかる可能性が残っている
   - KRACKs、BlueBourneなど。
   - LoRaWAN 1.0ではいくつかの脆弱性が指摘された
   - ハードウェアで実現される場合、ファームウェア更新による対策が困難
4. 現状では、IoTネットワークの使用には、強い警戒が必要
   - モニタリングやログを残す仕組み
   - 運用中のアップデートの仕組み

53

IoTが呼び込むリスク

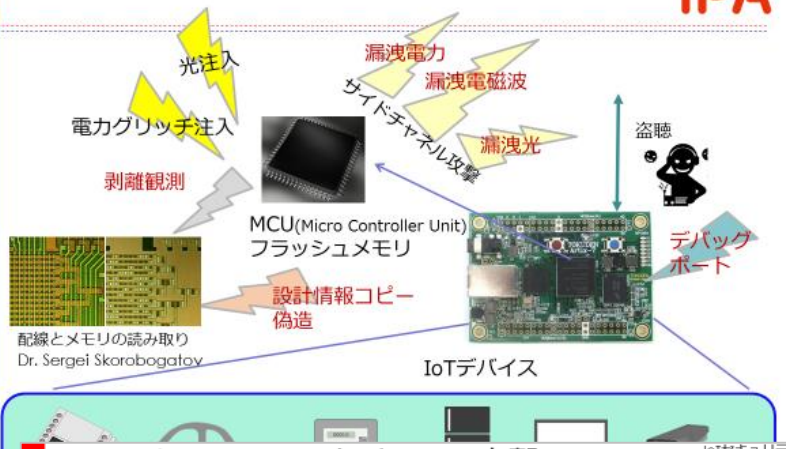
IoTセキュリティ教材 IPA

1. 近距離無線だから大丈夫/構内は安全
   - Wi-Fiと同じ電波を使ったLPWAの飛距離は10kmを超える
   - 様々な機器が電波でインターネットに勝手につながるし持込機器もある
2. パスワードやペアリングで守れば大丈夫
   - 無線をオンにしただけで感染し、乗っ取られる脆弱性も
3. ハードウェアだから侵されないだろう
   - 専用チップ内でもOS同様のプログラムが動いていて脆弱性もありうる
   - むしろアップデートが困難で危険なまま放置になりやすい
4. Linux(専用OS)だから大丈夫
   - Linuxも多数の脆弱性がある、RTOSの脆弱性はほとんど未知
   - 専用といいつつLinuxを流用していることが多い
5. マイナーなデバイスで話題になってないから大丈夫
   - 新しいデバイスやプロトコルには、未知の脆弱性が潜在する

85

5. ハードウェアセキュリティとセキュアデバイス

ハードウェア攻撃の概要



IoTにおけるハードウェア攻撃

- サーバー室に保護されるITシステムと異なり、IoTデバイスは、攻撃者の手の届く場所に設置される。したがって、ネットワークから侵入するのではなく、ハードウェアを物理的に操作することで、情報を抜き取ったり、偽造したり、破壊することが可能になる。
- 攻撃目的
  - メモリ→暗号鍵、パスワードや機密文書などの情報窃取、プログラムの解析・改ざん
  - アクセスカード→入退室やアクセス制限の破壊、突破
  - マネーカード→金額書き換え、複製
  - ドングル、半導体→デバイスの複製を作る、デバイスの偽造
  - ソフトウェアを改変する経路を開く
    - ◆ネットワークデバイス→ボット化して、DoS攻撃を仕掛ける
    - ◆ECU(Electronic Control Unit)、車載ネットワーク→自動車盗、遠隔制御、事故誘発
- トラストへの脅威
  - ソフトウェアは書き換えられたり、マルウェアを仕込まれるリスクを想定するが、ハードウェアの改竄や情報抽出は、見逃しがち。

10

攻撃法の分類

- **非侵襲**攻撃　-内科的方法
  - LSIチップのパッケージを開封せず、ピンからの信号の観測を中心にした、物理的な破壊を伴わない攻撃
    - ◆サイドチャネル攻撃(非侵襲)
      - ➢ 電源、電磁波などで漏えいするアナログ信号から情報抽出
- **侵襲**攻撃　-外科的方法
  - LSIパッケージを開封して半導体チップ（ダイ）から直接に光学的、電磁気的に情報を得る
  - 攻撃者の高度な知識の他に、高価な装置が必要
    - ◆装置には、半導体の製造および試験用の機器が使える
- **半侵襲**攻撃
  - パッケージを開けるが、保護層以上には手を触れない
- 故障注入(非侵襲、侵襲)　fault generation　(injection)

非侵襲攻撃の例

- サイドチャネル攻撃

  対象物の消費電力、音、温度、電磁波等の副次的な生成物から秘密情報を推測する攻撃。
  - タイミング攻撃
  - 電力解析攻撃
  - 電磁波解析攻撃　など
- テンペスト攻撃

  電子機器類から発生する電磁波を傍受し、それを解析することで元の情報の再現を試みる攻撃。
- 故障注入攻撃

  故障を注入して処理の誤りを発生させることで秘密情報を推測する攻撃。
  - グリッチ攻撃　など

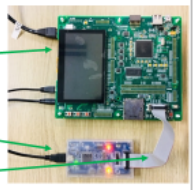
14

6. IoTデバイスセキュリティ(演習)

演習機器と配布物

IoTセキュリティ教材

- 1 – 3 人で構成するチームごと
  - 受講生PC (Dell)
  - RX65N基板
  - USB-JTAGインタフェース、E2-Lite
  - USBケーブル×2 (E2-Lite用、デバッグコンソール用)
  - JTAGケーブル (灰色フラットケーブル)
  - ACアダプター
  - LANケーブル×2 (RX65N基板用、受講生PC用)
- 2チーム共通の通信先となるサーバPC
  - サーバPC（Acerなど）
  - サーバPC用LANケーブル
  - Dumb Hub…通信の観測に用いる
- チーム設定シート（チームに1枚）

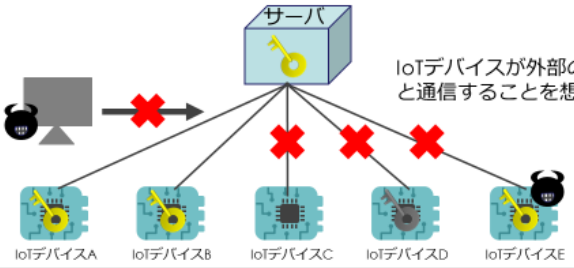


氡名、同チーム員氏名、チーム番号を記入

演習シナリオ

IoTセキュリティ教材

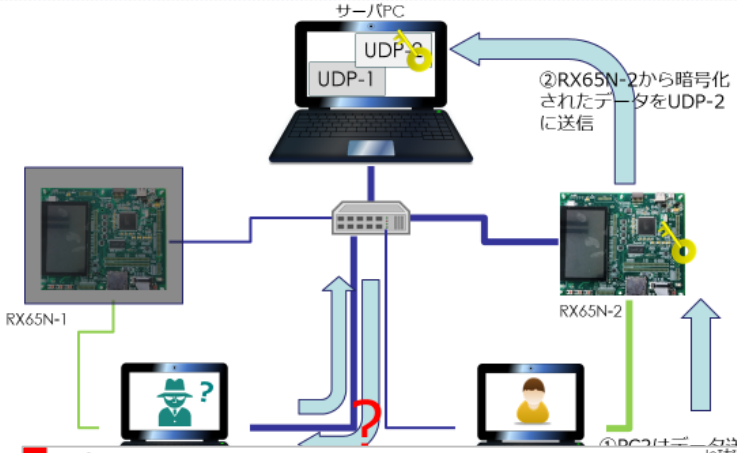
- 各チームのIoTデバイス-RX65Nが、サーバPCと通信を行う
  1. 平文の通信
     - ◆パケットキャプチャで通信文が読めるか？
  2. ソフトウェア暗号化
     - ◆暗号鍵を窃取してなりすませるか？
  3. ハードウェア（TSIPによる）暗号化
     - ◆暗号鍵が秘匿できるか？
     - ◆暗号化速度は？



13

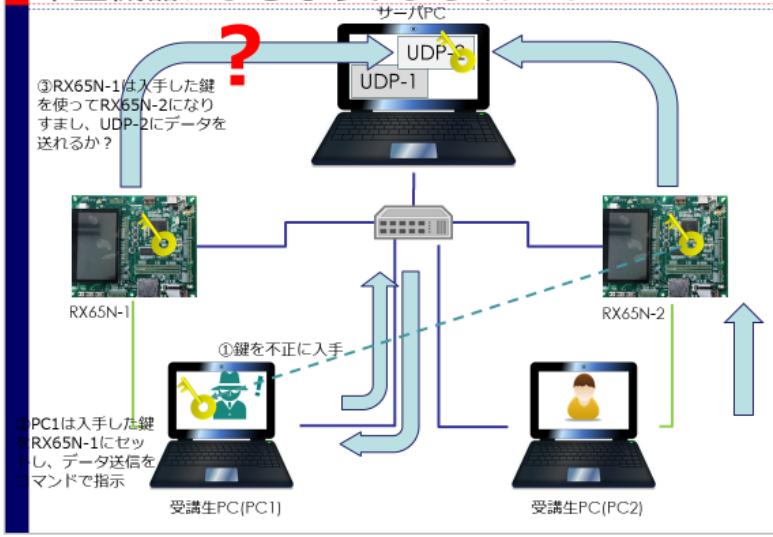
(演習②-1) ソフトウェア暗号化による暗号通信

IoTセキュリティ教材



(演習②-2) 不正機器によるなりすましイメージ

IoTセキュリティ教材



49

7. 車載エレクトロニクスのセキュリティ

IPA

IoTセキュリティ教材

コネクティッドカーの情報セキュリティ

- 自動車に高機能な機器や多様なサービスが備わる

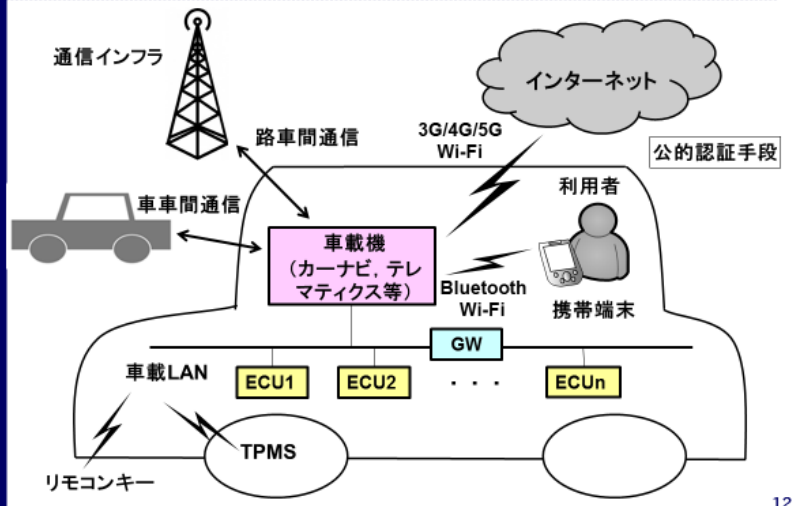
例：高機能カーナビ
テレマティクス機器など

□広域ネットワークと通信
- ◆データ通信網の高速化，低価格化
- ◆路車間，車々間通信
- ◆クラウドサービスの導入

□車載LANに接続
- ◆ECU（電子制御ユニット）から送信されるメッセージを利用
- ◆特定の動作をさせるメッセージをECUに送信

IoTセキュリティ教材

コネクティッドカーのセキュリティモデル（例）



12

IoTセキュリティ教材

CANプロトコルの特徴と問題点

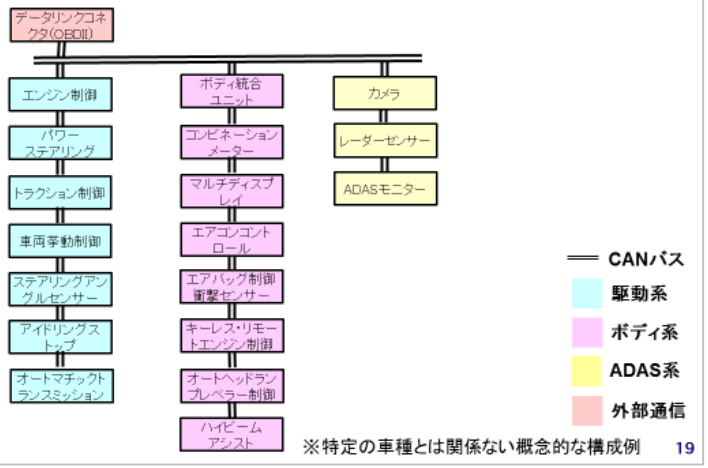
CANの特徴

□ペイロードが小さい	最大8byte
□ソースアドレスがない	宛先アドレス(CAN ID)しかない
□共有バスである	通信が丸見え、他から注入も可能
□認証や暗号化の仕組みがない	
□通信速度が低い	500kbps（0.5Mbps）

IoTセキュリティ教材

実際の車両のECUの構成例

- 公開情報（ディーラーで販売している車両整備書）の回路図を分析することで、ECUの機能や種類、構成が得られる



※特定の車種とは関係ない概念的な構成例

19

8. IoTの機能安全

なぜ、機能安全をやるのか

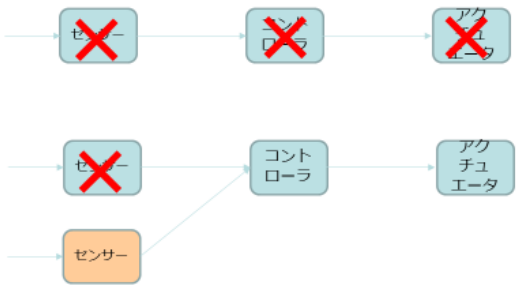
IoTセキュリティ教材 IPA

- 多くの組み込み分野では、機能安全の保証の方が昔から行われてきた
- セキュリティ対策の方がむしろ後手
- そもそもセキュリティとセーフティって違うの？
- セーフティ対策に加え、セキュリティもやる必要がある？
- セキュリティ対策に加え、セーフティもやる必要がある？
- 上記を理解するため、セーフティ(機能安全)とはそもそも何かについて学ぶ
- セキュリティとセーフティの違いについては、講義の後半で

機能安全をどう実現するか(1)

IoTセキュリティ教材 IPA

- 例:冗長化
  - 1つのセンサーが壊れたら？→全機能停止では困る
    →センサーを多重化(冗長化)で対応



18

リスク分析・ハザード分析の手順

IoTセキュリティ教材 IPA

1. 計画と方針策定
2. 対象記述
3. 危険要因特定
4. 頻度分析と結果分析
5. リスク評価
6. 許容可能なリスクについては7.へ、許容不可能なリスクについてはリスク軽減対策策定後3.へ
   許容不可能なリスクの軽減対策をしても許容可能にならないときはこの手順を抜ける
7. 講じた方がよい対策があるかどうかを検討して終了

セキュリティとセーフティの違いって？

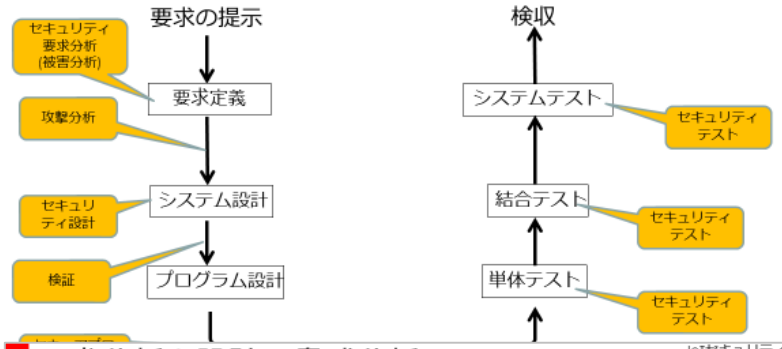
IoTセキュリティ教材 IPA

- 日本語ではどちらも「安全」
- フランス語でも両者の区別はない
- 品質としては相違がある
  - セキュリティ:悪意による攻撃/脅威から守られていること
  - セーフティ:安全に対するリスクが一定基準以下におさえられていること
- 上記定義からすると、両者は直交関係にあり、共通部分もあれば相違点もある
- 開発現場において、両者の品質確保/保証はいっぺんにしたいが、上記理由から、残念ながらそうはいかないようである
- 詳細は、講義の後半で

66

9. セキュリティ・バイ・デザインと脅威分析(1)

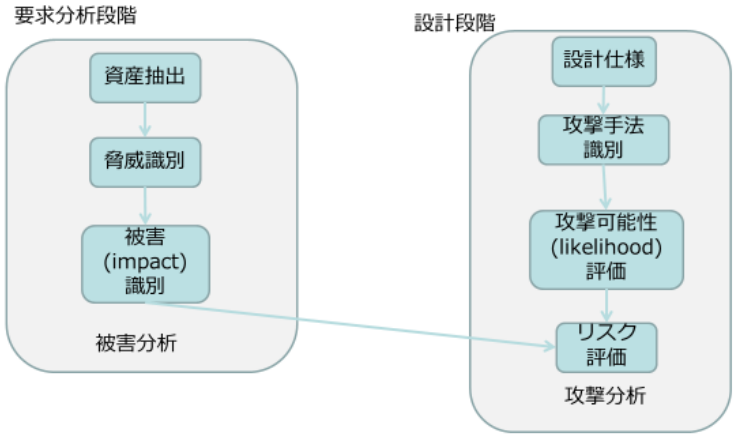
セキュリティバイデザイン全体像



被害分析の要素

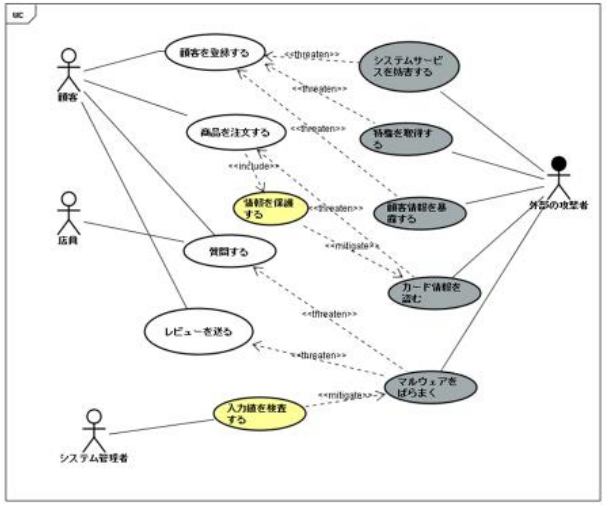
- 資産
  - 何を守るべきか
  - 個人情報データ、パスワード、重要な機能etc
  - 資産を明確にする=守る対象を限定=責任の明確化
    資産を明確に認識すると、脅威を想定しやすい
- セキュリティ目標
  - 資産をどう守るかの目標
  - 機密性、完全性、可用性などのセキュリティ特性の観点で規定
- 脅威
  - 対策しない場合に起きうるリスクの原因
- インパクト
  - 脅威による被害の大きさを評価
- セキュリティ要求
  - 脅威にどのような対策を行い、セキュリティ目標を達成すべきかを
    セキュリティ要求として明確に

要求分析と設計の脅威分析 被害分析と攻撃分析



37

ミスユースケース図

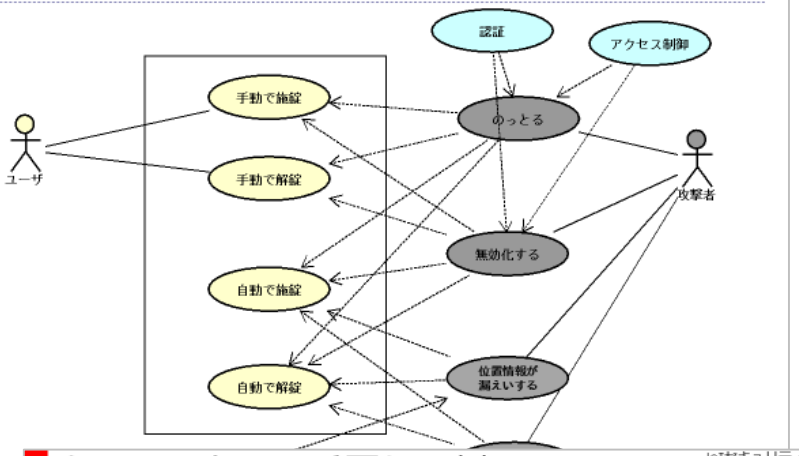


59

10.セキュリティ・バイ・デザインと脅威分析(2)

5. セキュリティユースケースの追加

IoTセキュリティ教材 IPA



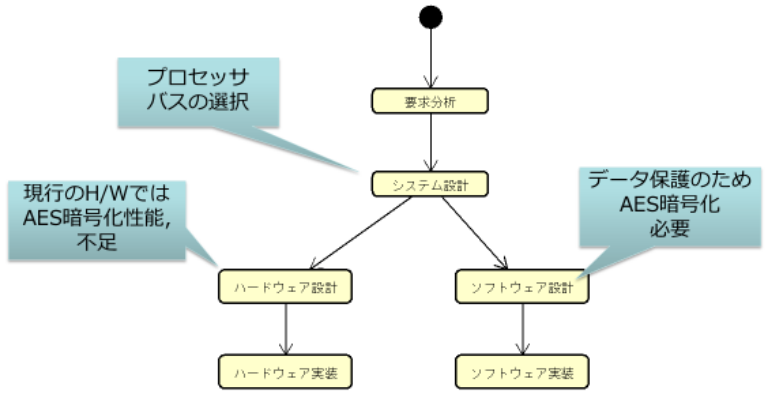
脅威モデリング

IoTセキュリティ教材 IPA

- Microsoftが考案した脅威分析手法
  - 脅威分析の中では一般に最もよく使われている
- 設計したシステムにおける脅威分析(脅威の抽出、評価)を行う手法
  - Data Flow Diagram(DFD)を用いた脅威抽出
  - STRIDEによる脅威発見
  - アタックツリーによる脅威のリスク評価
- アーキテクチャが明確なとき、脅威抽出の手法としては有効
- 参考書
  - [HL04]M.Howard, D.LeBlanc: WRITING SECURE CODE, Microsoft press,2004.
  - [Swiderski05] Swiderski, F. and Snyder, W. : 脅威モデル ― セキュアなアプリケーション構築, 日経BPソフトプレス (2005).
  - [Sho14] A.Shostack: Threat Modeling , Wiley (2014).

クリティカルな手戻りの例

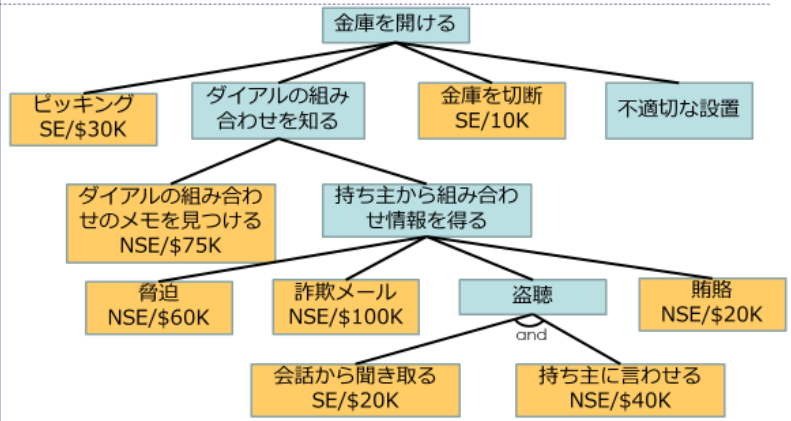
IoTセキュリティ教材 IPA



16

リスク評価の例

IoTセキュリティ教材 IPA



SE(Special Equipment):特殊な器具が必要
NSE:特殊な器具を必要としない

https://www.schneier.com/academic/archives/1999/12/attack_trees.html を基に作成

40

11. IoTの脅威分析(演習)

演習

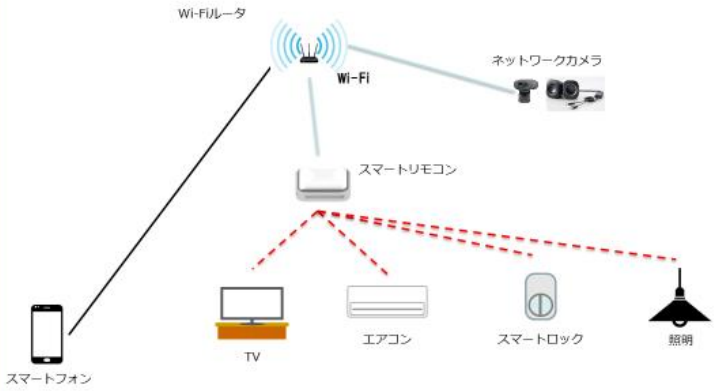
IoTセキュリティ教材

具体的なシステムを開発することを想定し、脅威分析(攻撃分析)を体験

- 脅威モデリング手法を用い、脅威の詳細と、必要な対策についてグループごとにまとめる
- 先日の被害分析の結果と合わせて提出
  最低限以下を含むこと。
  - 資産一覧の表（Excel）
  - ミスユースケース図(draw.ioなど)
  - DFD（draw.ioなど）
  - アタックツリー（draw.ioなど）
  - リスク評価結果（Excel）
- 提出先:classroomの課題
  - 提出は、個人ごとに違う内容を提出でも、グループで同じ内容でもいいですが、代表者が提出の場合はグループメンバー全員の氏名を課題に明

システム設計例

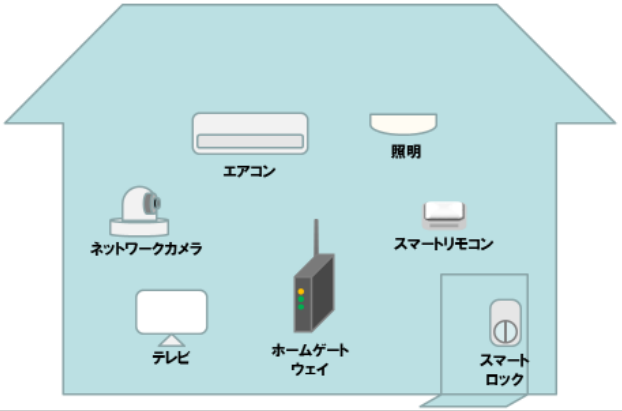
IoTセキュリティ教材



分析対象のシステム

IoTセキュリティ教材

- 疑似スマートホーム
- カメラで家の状況を監視
- スマートリモコンを用いて、家電が操作できる



2

演習で行う手順(脅威分析)

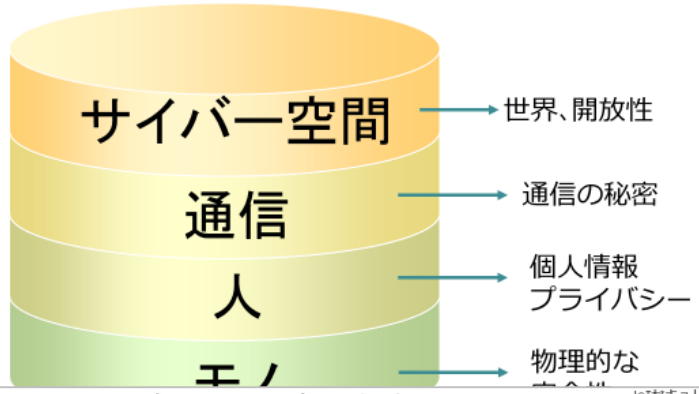
IoTセキュリティ教材

1. DFDで対象ソフトウェアをモデル化
   エントリーポイントで脅威のポイントを発見
2. STRIDEなどを使い、どんな脅威があるかを見つける
3. アタックツリーなどを用い、脅威の詳細化とリスク評価を行う
   リスクの高いものについては対策仕様を考える

4

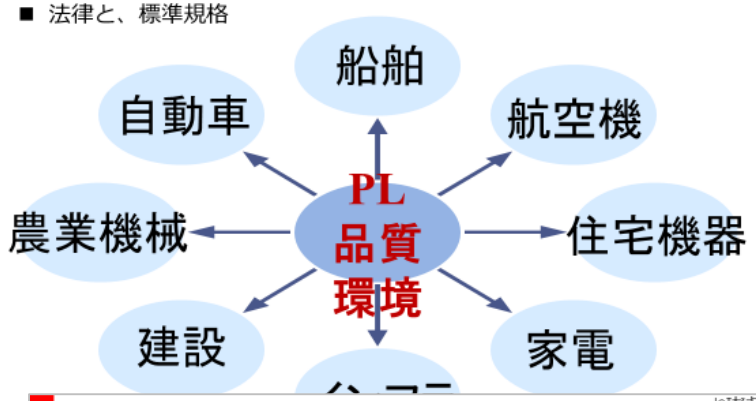
12. IoTを取り巻く法制度

IoTの法的構造



Thingsに関する規制

- 領域ごとの規制
- 法律と、標準規格



IoTを取り巻く法制度の概観

Internetに関する法
- 憲法
- 電気通信事業法
- 不正アクセス禁止法
- 刑法
- 他

ofに関する法
- IoT技術の保護（知的財産）
- 技術標準、国際標準
- 他

Thingsに関する法
- 民法
- 製造物責任法（PL法）
- 個別事業分野の規制法
- 環境に関する法律（廃棄物処理法などの各種の環境法）
- 他

利用者の保護に関する法
- プライバシー
- 個人情報保護
- 消費者保護
- 他

12

課題

- 権利性が不明なもの
  - モノの一部なのか人の属性なのか
  - 誰に法的な権利があるのか
    - ◆IoT機器が生成するログデータ
    - ◆センサーデータ
    - ◆スマートメーターのデータ

基本的に、権利は、人に属するので、機械が自動で学習したデータには権利が生じないとする解釈がある

- モノをインターネットに接続して使用するユーザー個人の使用状況や、モノに付着するセンサ等により掌握される周囲の個人の動向が、インターネットを通じて収集される場合
  - ユーザー個人のプライバシー、個人情報の保護
- インターネットに接続することによって、人の介在を必要としないで動作するモノが増える
  - その動作によって生じた結果についての責任の問題
  - 誰が責任を負うのか
  - 人工知能の規制

31

13. IoTセキュリティの運用と規格

指針14：時間がたっても安全を維持する機能 変化する脅威

IoTセキュリティ教材 IPA

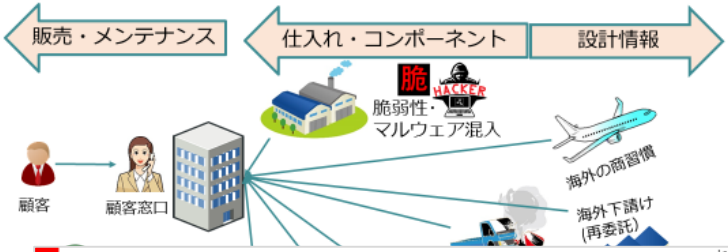
- 新たな脆弱性
  - 新たな脆弱性を含むコンポーネントの導入
  - 新たな攻撃法、マルウェアの流通
  - 長期運用における暗号の危殆化
- 新たなリスク
  - 営業秘密の漏洩、マルウェアの流入
    - ◆他者との競合・摩擦の増大
    - ◆組織の拡大、企業統合、新たな子会社、また運用体制の変更
    - ◆秘密を知る従事者の退職
- アタックサーフェスの拡大
  - 新ソフトウェア、新プロトコル、認証法の変更
  - ネットワークの拡大、新たな機器の接続
  - 想定外の機器の使用法

設計時に万全なセキュリティが達成できていたとしても、長期間維持できるとは限らない

サプライチェーン・リスク

IoTセキュリティ教材 IPA

- IoTは、多数のコンポーネントから構成される大規模なシステム
- 製品が、どのようなコンポーネントで構成されるか、源流と開発者チームの把握
- コンポーネントの設計･製造の外部委託
  - コンポーネントへのマルウェア混入などの攻撃
  - 委託先企業へのサイバー攻撃によって設計情報の漏洩



制御システムの長期運用

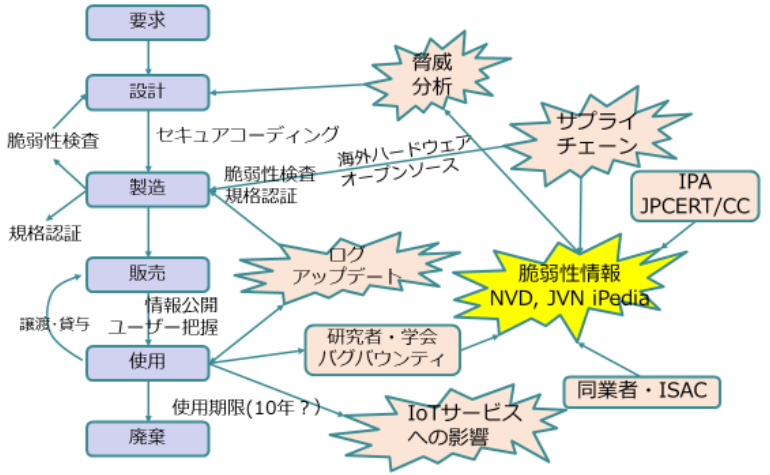
IoTセキュリティ教材 IPA

- 制御システムなど、大規模な設備に用いられるIoTデバイスは、長期間、継続運用され、アップデートが適用できない場合がある
  - アップデートによって装置が動かなくなるかもしれない
    - ◆セキュリティ機能と運転機能の干渉
  - 単体では動作しても、システム全体では動作しないかもしれない
    - ◆老朽化等によって装置を入れ替えなければならない時は、全部を入れ替える
- 動的なアップデートを可能にするには、事前の検証が必要
  - ソフトウェアシミュレーションによる検証
  - 本システムをそっくりに縮小した試験系でテストする
    - ◆開発時に構築した開発系を試験系として維持する
  - 二重系（duplex)による検証
- 新装置を組み込みやすい、互換性の高いシステム構成とする
  - プロトコルのバージョンによって処理を切り替えられる構造にする
  - ただし、旧・新版が同居するシステムでは、旧版がセキュリティホールとなりうる。速やかに全装置を切り替えるのが望ましい

18

セキュリティ・ライフサイクル

IoTセキュリティ教材 IPA



40

14.、15. IoTの脆弱性検査 （演習）

IPA

受講にあたってのご注意

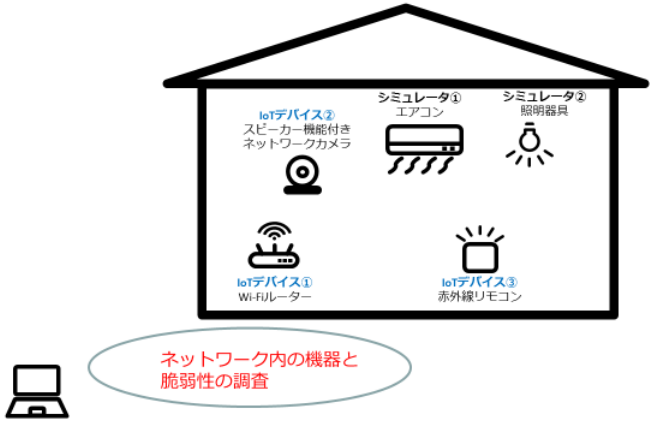
IoTセキュリティ教材 IPA

■今回学習するセキュリティ検証方法について、許可されていないシステムや他人の所有物に対して行うと**法律に抵触**して罰せられることがあります。
上記のような行為や、実施の是非の判断ができない場合は絶対に実行しないでください。

2

演習2,3,4　スマートホームLAN内機器の調査

IoTセキュリティ教材 IPA



10

始めるにあたって：脅威分析の考え方を応用する

IoTセキュリティ教材 IPA

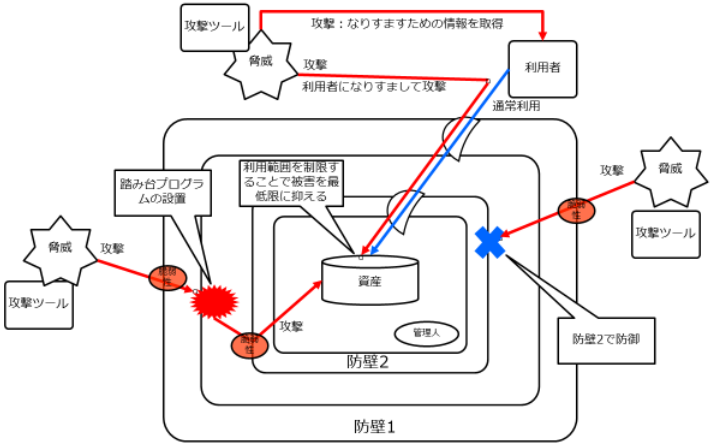
ステップ１：検証対象の脅威分析をする
　考えるためのガイド
- スマートホームの中にある機器を探る方法は？
- 機器の脆弱性を調査する方法は？
- スマートホームへのエントリーポイント（アタックサーフェス）はどこだろうか？

ステップ２：疑似スマートホームのハッキングの手順を考えてみる
- スマートホームの全体構成図（ネットワーク図）を想定してみよう
- どこからは侵入できるだろうか？
- これまで学んできた知識やツール類が「できること」で試してみる

5

資産と脅威と脆弱性について

IoTセキュリティ教材 IPA



30