NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

IoTセキュリティの課題と解決策
～JNSA IoT Security WGの試み～

日本ネットワークセキュリティ協会
IoT Security Working Group
松岡 正人
(株式会社カスペルスキー)

2017年1月23日

目次

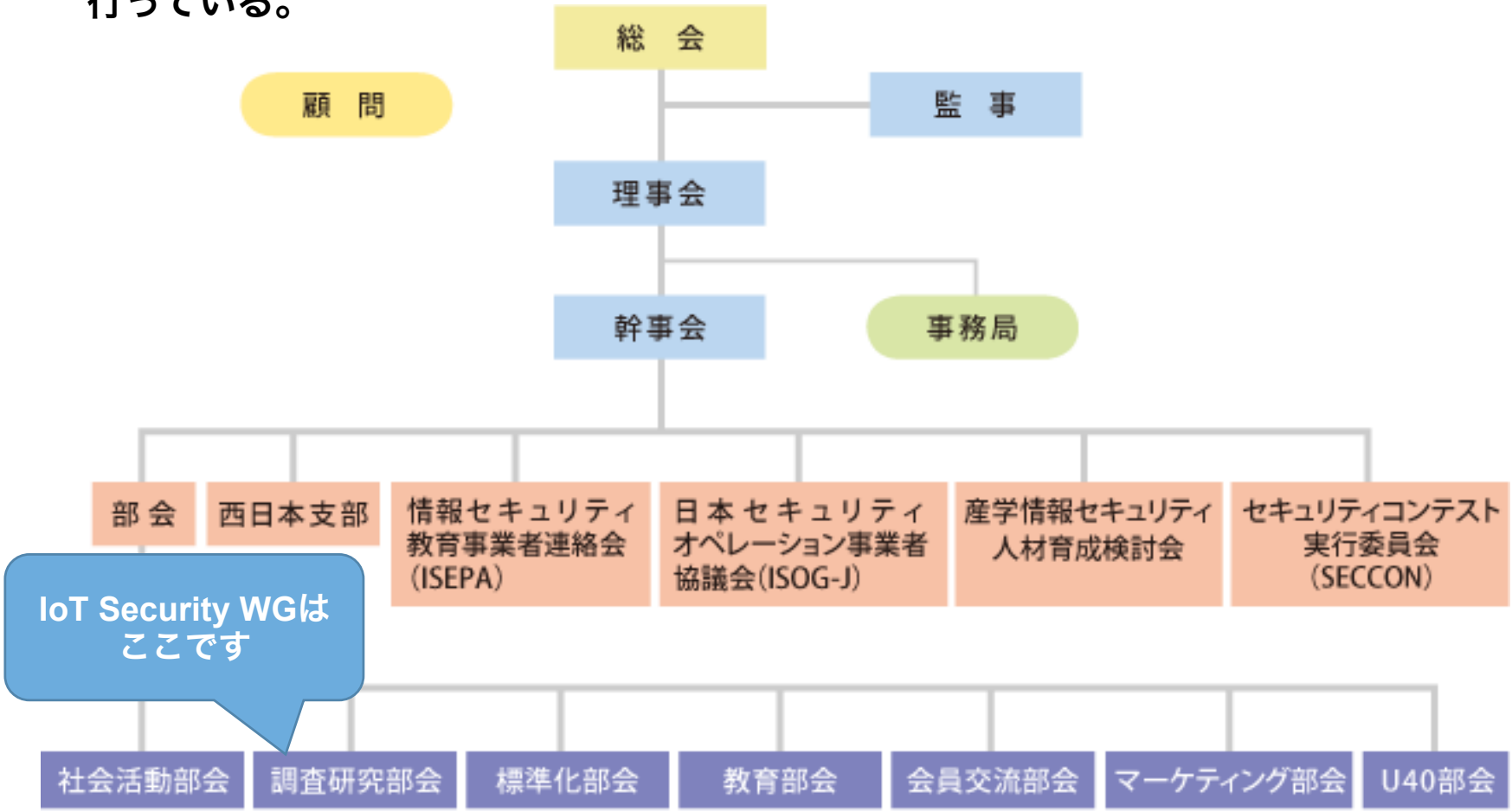
- JNSA IoT Security Working Group
  - JNSAとは？
  - IoT Security Working Group の活動

- 「コンシューマ向けIoT セキュリティガイド」解説
  - ガイドのターゲット
  - 各章概要説明と活用方法

JNSA IoT Security Working Group

JNSAとは？　組織と活動

- ネットワークのセキュリティに関する技術の向上、標準化の推進、一般社会への啓発などについて、社会活動、調査研究、標準化、教育などの各部会が活動を行っている。



部会・支部等はさらに各WGに分かれて活動しています。

IoT Security Working Groupの活動

- 2014/4 発足
- 目的は、IoTの市場調査・アーキテクチャとセキュリティ範囲検討・脅威の洗い出しと調査・調査報告書の取りまとめ
- 市場調査：あまりにも広大なため、終りのない旅に…
- アーキテクチャとセキュリティ範囲：先達の成果物を参照（IoT-A Project，IPA, ISACA, OWASP・・・）
- 脅威の洗い出しと調査
- Raspberry Pi の実装実験
- ガイド作成、2016/6 公開

  http://www.jnsa.org/result/iot/

「コンシューマ向け IoT セキュリティガイド」解説

ガイドを読んでもらいたい人

- 主に**コンシューマー製品の開発販売をおこなう企業や個人**を対象とし、 IoT デバイスのセキュリティ上の課題や問題と想定される一般的な対策の例をを示し、参照すべき情報の一覧を提供することで、より安全な IoT デバイスが提供される一助となることを目指します

なぜか？

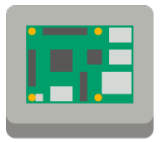
安全なコンシューマ向けIoTとは

そもそも一般利用者は…

- セキュリティの**知識が少なく**
- 多くは**ITスキルが低い**
- 特別な操作はできない

ではセキュリティのための設定は…

- どうしても必要な設定は製品や**マニュアル**の指示で
- それすら難しい場合は**販売時に店頭などで**設定
- あるいは**出荷時に**メーカー側で設定



現実は…

- 提供者の多くはセキュリティはつい**後回し**
- セキュリティを考えていても、利用者に**使いやすいわけではない**

(参考)
コンシューマはセキュリティに関心が薄い？

- 家庭でのセキュリティソフト導入率で見る関心の低さ*
  - 家庭：58.4%
  - 企業：88.3%

- 利用者の関心事はむしろ「プライバシー」や「情報漏洩」
  - 名前や住所、電話番号
  - クレジットカード番号やPIN
  - オンラインバンクのアカウントとPIN/パスワード
  - 電子メールアドレスやSNSアカウントのパスワード
  - 家族（配偶者や子、孫）の個人情報

*（出典）総務省「平成25年通信利用動向調査」

ガイド目次

1. Internet of Things（IoT）の概要
2. IoTのセキュリティの現状

✓ IoTとそのセキュリティについての概要、収集した情報の紹介

3. ベンダーとしてIoTデバイスを提供する際に検討すべきこと
4. ベンダーが、ユーザーのIoT利用に際して考慮すべきこと

✓ 実装時の具体的なセキュリティ考慮点を例示

ガイド前半 ～　概要と技術解説

1. Internet of Things（IoT）の概要
    - 1-1.市場動向と未来予測
    - 1-2.IoTの技術
    - 1-3.IoTの制御技術の例

2. IoTのセキュリティの現状
    - 2-1.セキュリティとプライバシー
    - 2-2.デバイスとシステムのセキュリティ
        - 2-2-1.IoTのセキュリティ（組込み系）
        - 2-2-2.IoTのセキュリティ（無線系）
    - 2-3.IoTのプライバシー
    - 2-4.誰でも作れる IoT

1章の内容紹介

1-2.IoTの技術

IoT 技術は「可視化」、「収集・予測・分析」、「自動制御・最適化」 の組合せから成り立つ。

「可視化」 は UI/UX
「収集・予測・分析」 はセンサー情報の最適な収集とクラウド・人工知能等による高度分析
「自動制御・最適化」はリアルタイム制御またはアプリに応じた最適な制御、セーフティなアクションなど。
単に「モノが Internet繋がった」 ということではなく、高度で知的な制御を含むもので、ユースケースによって異なる。

IoTの研究と標準
*IoTの調査研究と標準化

- IoTを安全かつ効果的に実現するための実証試験や調査研究の代表的なものとしてIoT-Aがあり、IEEE、ITU、ISO/IEC、OMG、など様々な標準化組織により標準化の検討が進められている
- 枠組みやアーキテクチャといったレベルでの検討を経て、現在ではAllseenやoneM2Mのなど複数の企業グループや組織から、実装・実現に必要なコミュニケーション、管理やセキュリティの提案がなされている
- 日本国内でも、当WGの他にIoT推進コンソーシアム、IoT推進研究会などが複数存在し、業種毎にグローバルな標準化の流れを見据えた標準化の検討がなされている

IoT-A , Internet of Things - Architecture : http://www.iot-a.eu/public
IEEE-SA , IoT Steering Committee : http://standards.ieee.org/innovate/iot/
IEEE P2413, Draft Standard for an Architectural Framework for the Internet of Things Working Group : http://standards.ieee.org/develop/project/2413.html
ITU Joint Coordination Activity on IoT (JCA-IoT) : http://www.itu.int/en/ITU-T/jca/iot/Pages/default.aspx
ISO/IEC: JTC1 SWG 5 Internet of Things(IoT) : http://www.iec.ch/dyn/www/f?p=103:14:0::::FSP_ORG_ID,FSP_LANG_ID:10270,25?q=jtc1%20sc%2038
OMG : http://www.omg.org/hot-topics/iot-standards.htm
Industrial Internet Consortium : http://www.industrialinternetconsortium.org/
oneM2M : http://www.onem2m.org/
TTC: 一般社団法人情報通信技術委員会 oneM2M : http://www.ttc.or.jp/j/std/committee/wg/onem2m/onem2mtopics/20141212/
Allseen Alliance : https://allseenalliance.org
Open Connectivity Foundation : http://openconnectivity.org

2章の内容紹介

2-4. 誰でも作れる IoT

IoT は誰でも作れる時代で、廉価なマイコンボード（ラズパイなど）を利用すればプログラミングやハードウェアの詳しい知識がなくとも作れるようになったが、そこにはサイバーセキュリティ対策などが行われず、管理されていない「野良」と言うべきものが増え続けている。当然、プライバシーについても課題があり、画像認識技術の利用の際には留意すべき点がある。

誰でも作れる IoT
*インターネットラジオを作ってみる

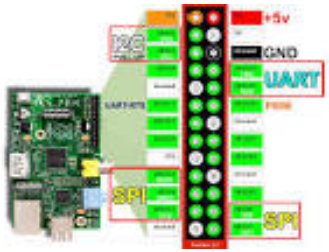
1.秋葉原でPi＋LCDとボリュームつまみ（ロータリーエンコーダー）購入

Raspberry Pi 2　＋　LCD　16x2　＋　RGB-LED付つまみ



2.ハードウェアの組立て

→GPIOの配線と半田での接着



3.インターネットラジオのインストール

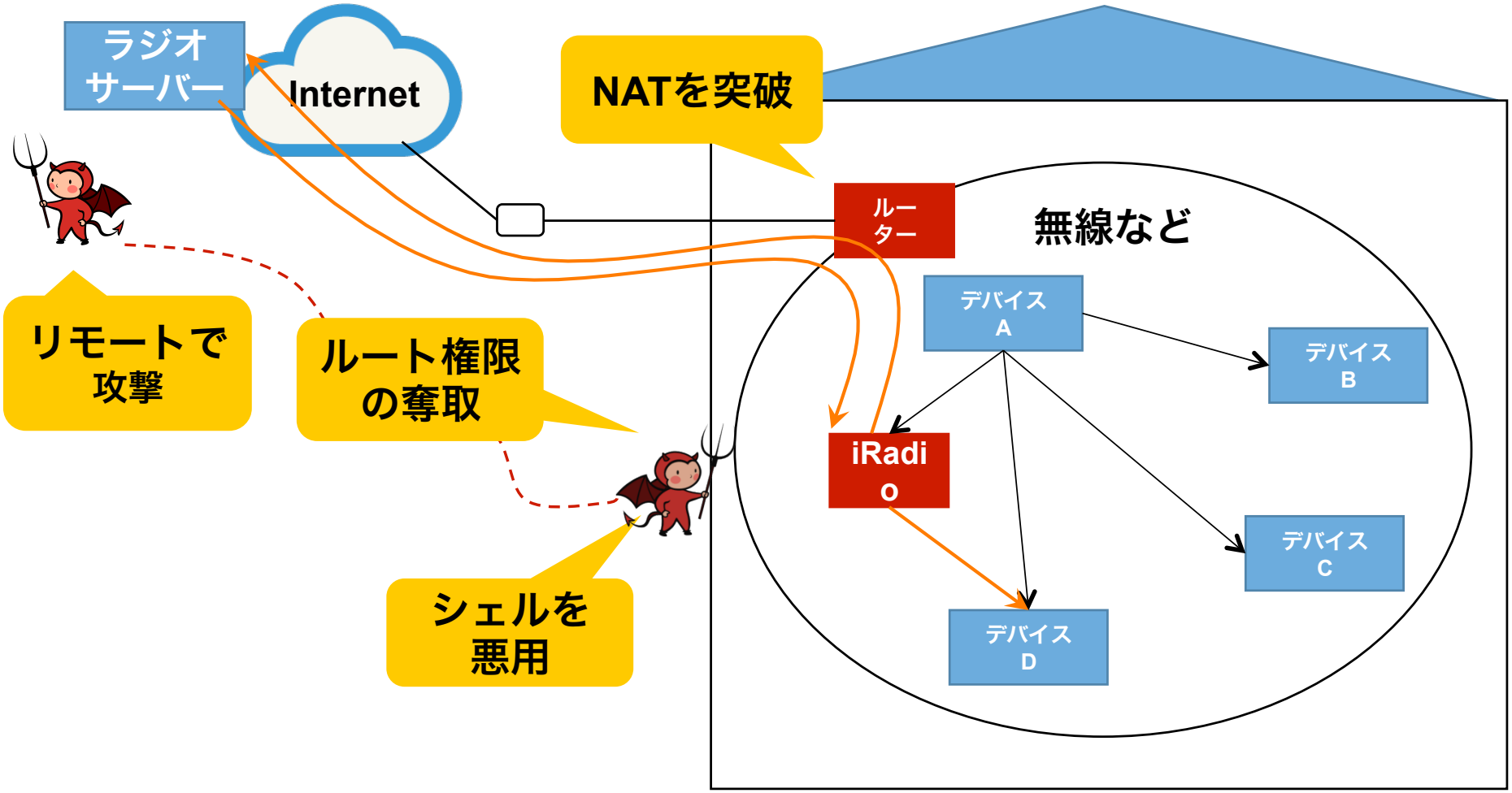
→mpc/mpdを用いる（他に、XBMCを用いる方法もある）

4.プログラミング

→ここで発見・・・（セキュリティの実態）

ラズパイなどで利用可能なホビー用のOSやミドルウェア・アプリケーションは「ルート権限の固まり」だ！

誰でも作れる IoT
*セキュリティの問題とルート権限



ガイド後半 ～　脅威と対策マトリックス

3. ベンダーとしてIoTデバイスを提供する際に検討すべきこと
   ライフサイクルについて
   デバイスの構成と想定される脅威

   - スマートテレビ
   - ウェアラブルデバイス
   - ネットワークカメラ
   - 汎用マイコンボード

4. ベンダーが、ユーザーのIoT利用に際して考慮すべきこと

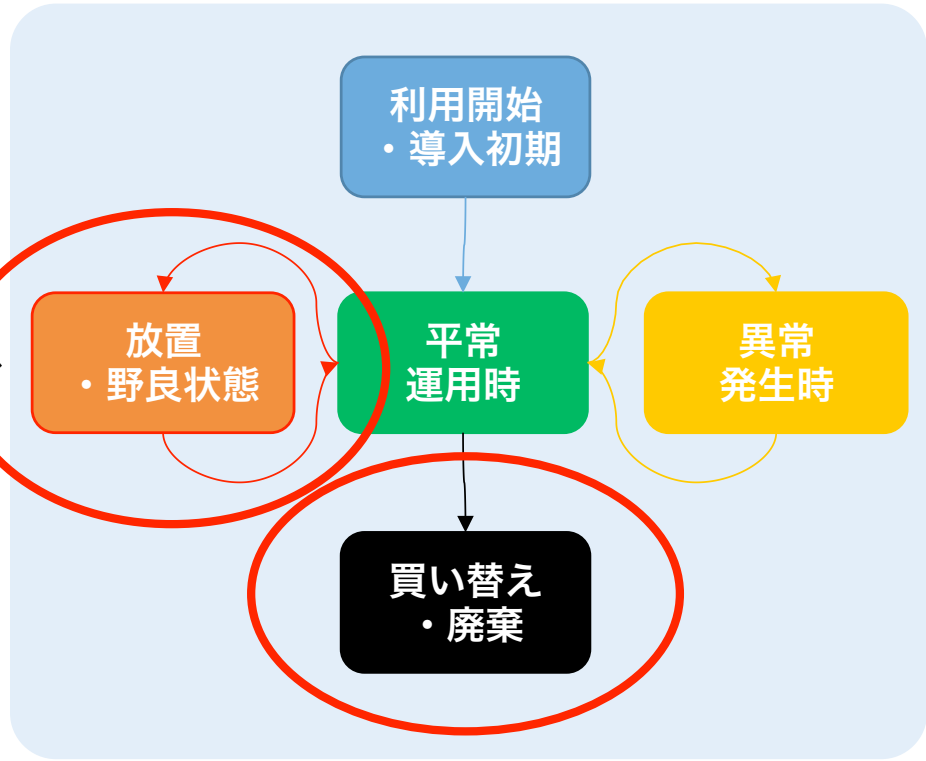
3章の内容紹介

3. ベンダーとして IoT デバイスを提供する際に検討すべきこと

　ベンダー（提供者）は IoT の仕組みや構造について詳細を理解していないユーザー（利用者）が IoT 製品やサービスを安全に利用するために考慮すべき事柄がある。この章では、サイバーセキュリティの観点から企画・開発から製品・サービスの提供にわたり、どのようなことを考慮し、ユーザーに伝えるべきか例示する。

ライフサイクルについて
*ユーザーによる製品の利用

- 利用開始の際に、デバイスの導入設定がユーザーにとって複雑でなく、初期設定に必要な情報などを第三者が再利用することのできない仕組みを提供することが望ましい。
- 利用を開始した後、デバイスに異常が発生した場合、異常を解消して復旧する必要がある
- 利用開始後、長期間にわたって使用せずに稼働させたまま放置することで第三者がデバイスにアクセスすることが可能な状態を「野良」と呼ぶが、セキュリティ上は好ましくない。
- デバイスが不要となる場合には、記録・保存されたデータの消去や初期化についての手順が準備され、ユーザーが対処するか、ユーザーが対処せずともよいような仕組みがあることが望ましい



想定される脅威について

本ガイドでは、IPAが発行した「自動車の情報セキュリティへの 取組みガイド 」を元に、IoT デバイスへの脅威を以下のように定義した。これを異なるデバイスに当てはめて脅威分析を行う。*http://www.ipa.go.jp/security/fy24/reports/emb_car/documents/car_guide_24.pdf

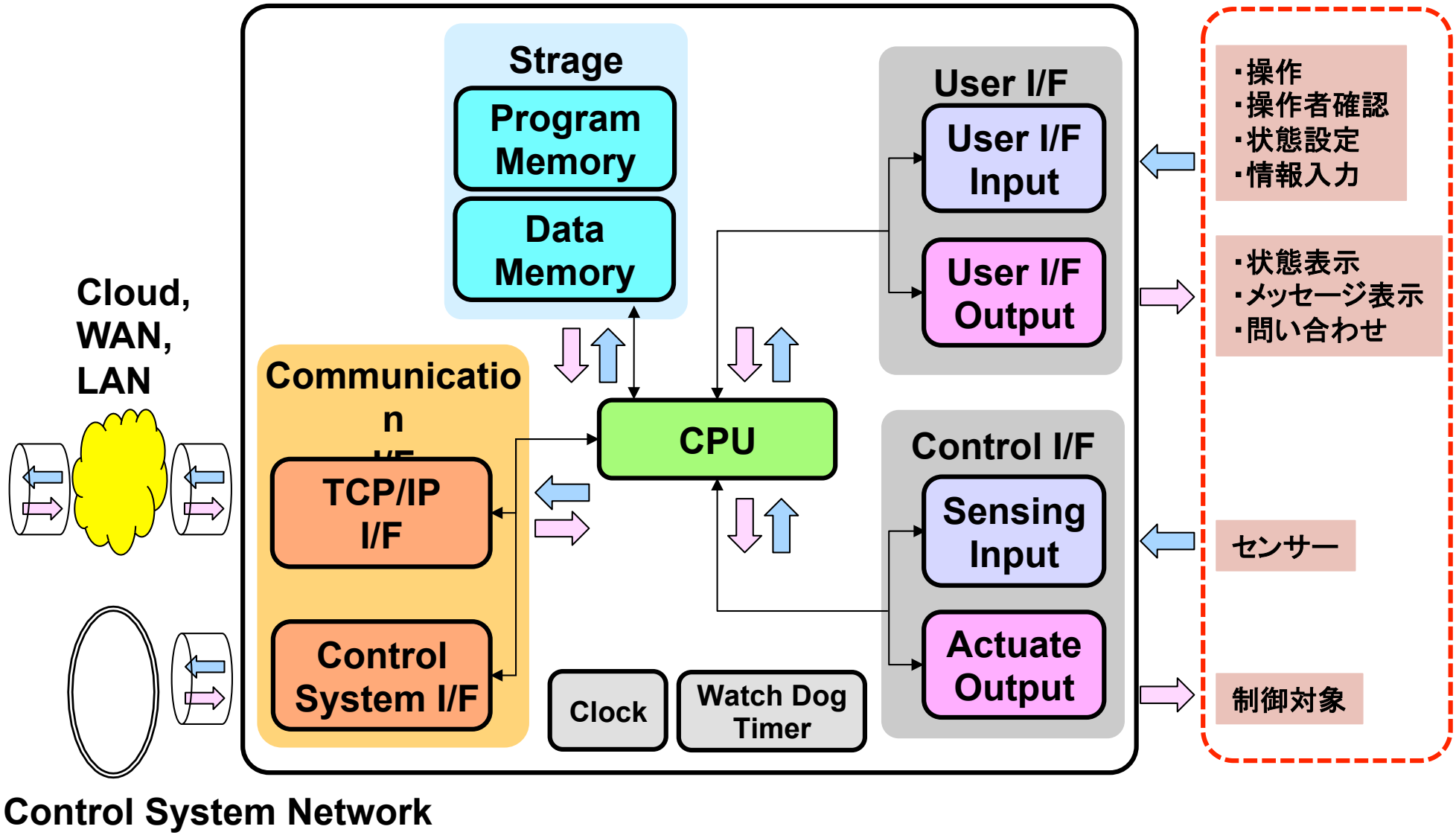
- 利用者による操作に起因する脅威
  1. 操作ミス　デバイスやシステムを誤動作させられてしまう
  2. ウィルス感染　デバイスやシステムが有する情報やデータが漏れるか誤動作させられてしまう
- 攻撃者による干渉に起因する脅威
  3. 盗難　デバイスが盗まれてしまう
  4. 破壊　デバイスが破壊されてしまう
  5. 盗聴　通信内容を他人に知られてしまう
  6. 情報漏えい　知られたくない情報を盗まれてしまう
  7. 不正利用　他人にシステム、デバイス、ネットワークを使用されてしまう
  8. 不正設定　他人にシステム、デバイス、ネットワークを設定変更されてしまう
  9. 不正中継　無線や近接による通信内容を傍受されるか、書き換えられてしまう
  10. DoS攻撃　システム、デバイスの機能やサービスが利用できなくなる
  11. 偽メッセージ　偽メッセージによるシステム、デバイスが誤動作してしまう
  12. ログ喪失　動作履歴が無いため、問題発生時に対処方法がわからなくなる

脅威一覧表の目的と使いかた

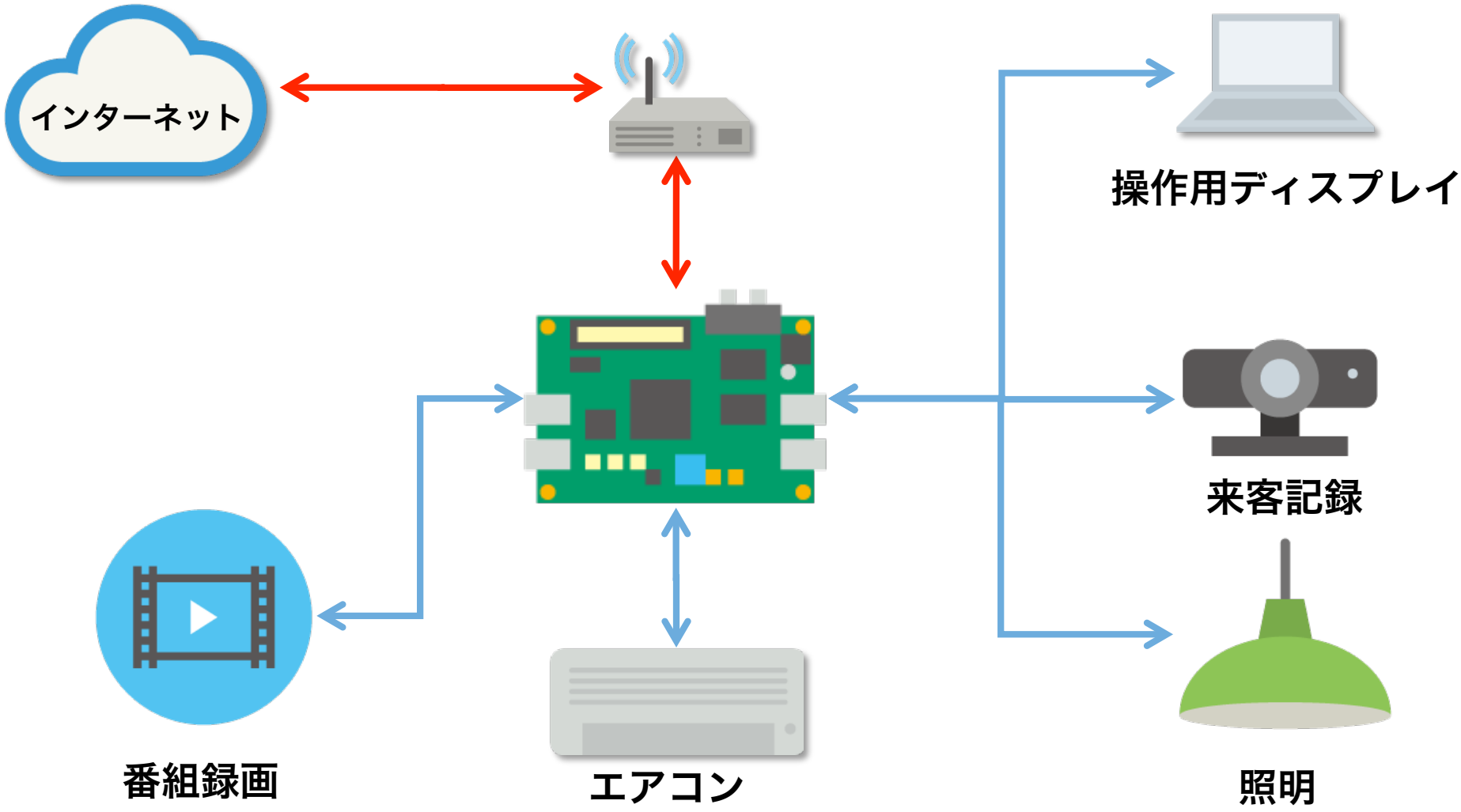
- 本章で扱う「4種の IoT 機器」は、それぞれユースケースが異なるため、前出の「12種類の想定される脅威」を縦軸、5つの状態で示されるライフサイクルを横軸とし、各脅威の各状態において取り得る対策の例を列挙している
- 例えば、「スマートテレビ」が「平常運用時」において「盗難」にあった場合、「スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる」という対策を例示する
- 「ウェアラブル」が「平常運用時」において「盗難」にあった場合、「GPSなどを利用してデバイスの位置を把握することができるようにする」および「リモートワイプできるようにする」が付け加えられる

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• N/A	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• スマートテレビがネットワークから切断されたことを検知し、ユーザーに通知し、利用できなくなる	• N/A

汎用マイコンボード：システム構成



汎用マイコンボード：システム構成



想定される脅威：汎用マイコンボード
表1：設定ミス、ウィルス感染

利用者による操作に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
操作ミス	• IoT デバイス内のユーザインターフェイスを介して、利用者が行った操作・設定が誤っていたことによりひきおこされる脅威 • 意図しないサービス事業者に個人情報を送付してしまう、通信の暗号機能を OFF にしてしまい通信情報が盗聴される、等	• ID、パスワード、通信先などデフォルト設定の確認・変更機能を実装する • 通信の暗号化機能はデフォルトONにす（特にroot権限やコマンド、レスポンスのやりとり） • テスト（試行）による動作確認を実装する	• 定期的な認証情報の更新ができる • 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ログの取得による不正動作の検知ができるようにする	• 通信先などの異常を自動検知してメール等で通知する • 異常の種類が判別できる • 設定のロールバックができるようにする • 問題発生時の問い合わせ先を明示する	• 動作監視（モニタリング） - ランプ - 遠隔通知 • 認証情報に有効期限を設ける	• デバイス内の設定の初期化ができるようにする • 廃棄時は物理的に読み出し不可にするようガイドする • ラベルや注意書き等、システムの構成や制御内容、取扱うデータ、管理者などが類推可能となるおそれのある情報を削除するようガイドする • 連携先に廃棄を連絡するガイドまたは機能を実装する
ウイルス感染	• 利用者が外部から持ち込んだ機器や記録媒体によって、IoTシステムがウイルスや悪意あるソフト ウェア（マルウェア等）等に感染することによりひきおこされる脅威 • IoTデバイスに感染したウイルスがネットワークを通じて更に他のIoTデバイスに感染、等	• ボード購入元の信頼性を確認する（ウィルスが仕込まれていないか） • ネットワークなど安全な環境下で設定を行うようガイドする • 実際のシステムに接続する前にセキュリティの設定が行われるようにする • 最新のセキュリティパッチを適用されるようにする	• 定期的なウィルスチェックができるようにする ・製造元からの脆弱性情報を配信する • ログの取得による不正動作の検知ができるようにする	• 動作状況のわかりやすい表示 • 安全なシーケンスで再起動を実行するようにする • 安全な停止、入出力やネットワークの切り離しができるようにする	• 定期的なウィルスチェックができるようにする	

想定される脅威：汎用マイコンボード
表2：盗難、破壊、盗聴

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
盗難	• IoTデバイスが盗まれることで、リバースエンジニアリングや、サービスの不正利用などが行われる脅威 • IoTデバイスを誰かが持ち去る、など	• ユースケースに応じた損害の算定をする	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知できるようにする • 盗難を検知した場合には起動しないよう実装する	• 盗難を検出した場合には自ら機能を停止する • 重要なデータはあらかじめ適当なタイミングでバックアップをとれるようにする	• デバイスがネットワークから切断されたことを検知し、ユーザーに通知するできるようにする	• N/A
破壊	• IoTデバイスが破壊されることで、サービスが利用できなくなるか、サービスそのものが提供できなくなる脅威 • IoTデバイスが潰される、あるいは燃やされるなどにより使用できなくなる、等	• ユースケースに応じた損害の算定をする	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。	• 重要なデータはあらかじめ適当なタイミングでバックアップをとる	• 破壊されることで デバイスがネットワークから切断されたことを検知し、ユーザーに通知する。	• N/A
盗聴	• IoTデバイス内部やIoTデバイス同士の通信や、IoTデバイスと周辺システムとの通信を権利を有しない第三者に盗み見られる脅威 • センサーノードなどから得られた気温や湿度、放射線量などの情報が途中経路で盗聴される、等	• 通信経路の確認ができるようにする • 通信の暗号化ができるようにする • 相互認証機能を利用する • Firewallや、侵入検知機能のあるネットワークの利用をガイドする	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • 定期的な暗号化鍵の変更を可能にする	• N/A	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • 定期的な暗号化鍵の変更を可能にする	• 耐タンパ性を持つ製品を使用する

想定される脅威：汎用マイコンボード
表3：情報漏洩、不正使用

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
情報漏えい	• IoT システムにおいて保護すべき情報が、許可のされていない者に入手される脅威 • 蓄積されたコンテンツや、各種サービスのユーザ情報が、機器への侵入や通信の傍受によって不正に読み取られる、等	• アクセス制御設定ができ（ユーザー認証・権限分離）設定 • 脆弱性チェックの実施 • 脆弱性チェック済みデバイスの使用 • 通信が暗号化できるようにする • 重要なシステムはFirewallや、侵入検知機能のあるネットワークを利用する	• ・動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある　（構成情報更新時にメール通知など） • 通信の暗号化ができるようにする • 不正な通信の遮断・検（Firewallなど） • 通信相手が正しいことを常にモニターできる • ・ログが取得できるようにする（正常ログ、異常ログ）	• N/A	• 動作監視（モニタリング）機能がある • 通信の暗号化ができるようにする • 不正な通信の遮断・検知（Firewallなど） • 通信相手が正しいことを常にモニターできる	• 耐タンパ性を持つ製品を使用する
不正使用	• なりすましや機器の脆弱性の攻撃によって、正当な権限を持たない者にIoTシステムの機能などを利用される脅威 • 認証用の通信をなりすます事により、サービスを不正に利用する、等	• 認証情報をデフォルト値から変更する ・脆弱性チェックの実施 • ・脆弱性チェック済みデバイスの使用	• 認証情報の定期的な変更 • 変更時には安全なモードで行う（ペアリングのような） • 動作監視（モニタリング） • デバイスの認証（デバイスID管理などの偽物対策） • ログを取得できるようにする（正常ログ、異常ログ）	• 不正利用を検出した場合に動作を停止させる	• 認証情報の定期的な変更ができるようにする • 設定変更時には専用のモードで行うようにする • 動作監視（モニタリング）機能がある • デバイスID管理などにより偽デバイスを判定できる仕組みを用意しておく	

想定される脅威：汎用マイコンボード
表4：不正設定、不正中継、DoS 攻撃

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
不正中継	• 通信経路を操作し、正規の通信を乗っ取ったり、不正な通信を混入させる脅威 • NFC(RFIDとか)の電波を不正に中継し、攻撃者が車の鍵の通信を鍵の近くから中継して遠隔から鍵を解錠する、等 • 近接通信であるから安全とした前提を利用するもの	• 読み取り防止機能の追加 • 使わないときにはOFFとなる機能を設ける（単に近くにいるだけでONにはしない機能）	• ・動作監視（モニタリング） ・設定変更されていないことの確認 • 通信遅延の検知（ベンダー側） • ログの取得（正常ログ、異常ログ）	• 完全停止する • 停止したことがシステム側で判断出来る	• 動作監視（モニタリング） • 設定変更時の通知機能 • 不正な通信／アクセスの検知（※どこまで出来る？） • 通信相手が正しいことのモニタできる	• 耐タンパ性を持つ製品を使用する
DoS 攻撃	• 不正もしくは過剰な接続要求によって、システムダウンやサービスの阻害をひきおこす脅威 • IoTデバイスやサービスゲートウェイに過剰な通信を実施し、利用者の要求（エアコンの遠隔制御など）をできなくさせる、等	• コネクションフラッド、SYNフラッド、UDPフラッドに耐えるシステム構造 • セッションタイムアウトの設定 • DoSを受けI/F部分が麻痺しても基本機能は動く構造	• ログの取得（正常ログ、異常ログ）	• DoS攻撃が終わったら速やかに機能回復できる • 再起動による回復 • サービス不能期間のデータのバッファリングと再送機能 • データが来なくてもダウンしない機能がある	• N/A	• N/A

27

想定される脅威：汎用マイコンボード
表5：偽メッセージ、ログ喪失（証跡）

攻撃者による干渉に起因する脅威		対策の為の機能およびサービス				
脅威	説明	利用開始・導入初期	平常運用時	異常発生時	放置、野良状態	買い替え・廃棄時
偽メッセージ	• 攻撃者がなりすましのメッセージを送信することにより、IoTシステムに不正な動作や表示を行わせる脅威 • エアコンの遠隔操作のメッセージを改ざんし、設定温度を高くする、等	• 認証機能の利用（IoT側とサーバー側の両方） • 認証情報をデフォルト値から変更できる • 脆弱性チェックの実施 • 脆弱性チェック済みデバイスの使用 • データの安全な暗号化機能がある • 安全な暗号を用いたプロトコルの利用 • メッセージ値の正常範囲の確認　（例：エアコンの温度が常識的な範囲） • 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離する	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ログの取得（正常ログ、異常ログ）	• 偽メッセージを検出した場合に動作を停止させる	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） •	• N/A
ログ喪失（証跡）	• 操作履歴等が消去または改ざんされ、後から確認できなくなる脅威 • 攻撃者が自身の行った攻撃行動についてのログを改ざんし、証拠隠滅を図る、等	• ログ情報の保護 • バックアップ機能を持つ（安全な場所） • 管理操作用通信を暗号化できる • 管理者権限と一般ユーザー権限が分離する	• 動作監視（モニタリング）機能がある • 設定変更されていないことの確認機能がある（構成情報更新時にメール通知など） • ログファイルへのアクセスの検知、記録 • ログの取得（正常ログ、異常ログ）	• バックアップから復帰可能な機能	• 動作監視（モニタリング）機能がある • ログファイルへのアクセスの検知、記録	• 耐タンパ性を持たせる

さまざまなIoTについて、
この表を使って対策を検討
できる！

４章の内容紹介

4. ベンダーが、ユーザーの IoT の利用に際して考慮すべきこと

ユーザー（利用者）は IoT の仕組みや構造について詳細を理解していなくてもベンダー（提供者）が提供する情報から個々の IoT 製品やサービスについて安全に利用できる必要がある。この章では、サイバーセキュリティの観点からユーザーに対してベンダーが配慮すべき項目を解説する。

4．ベンダーがユーザーの IoT の利用に際して考慮すべきこと

4章の概要

- 4章では3章で提示したベンダー向けのガイドと視点を変え、ベンダーや開発者が専門知識のないユーザーに対して安全な仕組みを提示できるようにすることを目的とする
- ベンダーはIoTデバイスの企画・開発、販売に際して、IoTデバイスおよびデバイスで利用するインターネット上のサービスに対し、サイバーセキュリティ対策を施し、ユーザーが行なう必要のある操作や作業を特定して適切なガイドを行なう必要がある
- ユーザーに適切なセキュリティ機能を提示することは、ベンダーのインシデント対応コストを下げることにもつながる

● 要諦は以下の三点

1. デフォルト設定をセキュアに！
2. 問題発生を想定する
3. 廃棄まで責任を持つ

まとめ

まとめ

- IoTは仕組み全体でセキュリティを考える必要があります
- ビジネス系 IoTは事業としての責任を果たしましょう！
- コンシューマ系 IoTも事業として責任を果たしましょう！
- ガイド　第4章だけでも読んでください！

「利用者」にセキュリティ対策を委ねない！

JNSA IoT Security WGへ
あなたも参加しましょう！

おしらせ　**参加費無料**

コンシューマIoT向けセキュリティガイドに掲載した「脅威一覧表」を作成するワークショップを開催します。

開催日時：2017/3/1（水）、13:00～17:00

会場：カスペルスキー本社 トレーニングルーム

※お申し込みは office@jnsa.org 、お名前、組織名、連絡先をご連絡ください

●ガイド作成メンバー：

阿部真吾	JPCERTコーディネーションセンター
兜森清忠	オブザーバ
桐山隼人	オブザーバ
酒井美香	日本IBMシステムズ・エンジニアリング株式会社
杉浦昌	日本電気株式会社
玉木誠	SCSK株式会社
洞田慎一	JPCERTコーディネーションセンター
福田尚弘	パナソニック株式会社
松岡正人	株式会社カスペルスキー

*五十音順

問い合わせ先

NPO **日本ネットワークセキュリティ協会 事務局**
sec@jnsa.org