IPA Better Life with IT

「『つながる世界の開発指針』の実践に向けた手引き」の詳細

SECセミナー

2017年11月2日

独立行政法人 情報処理推進機構（IPA)
技術本部　ソフトウェア高信頼化センター（SEC)
研究員　小崎　光義

目次

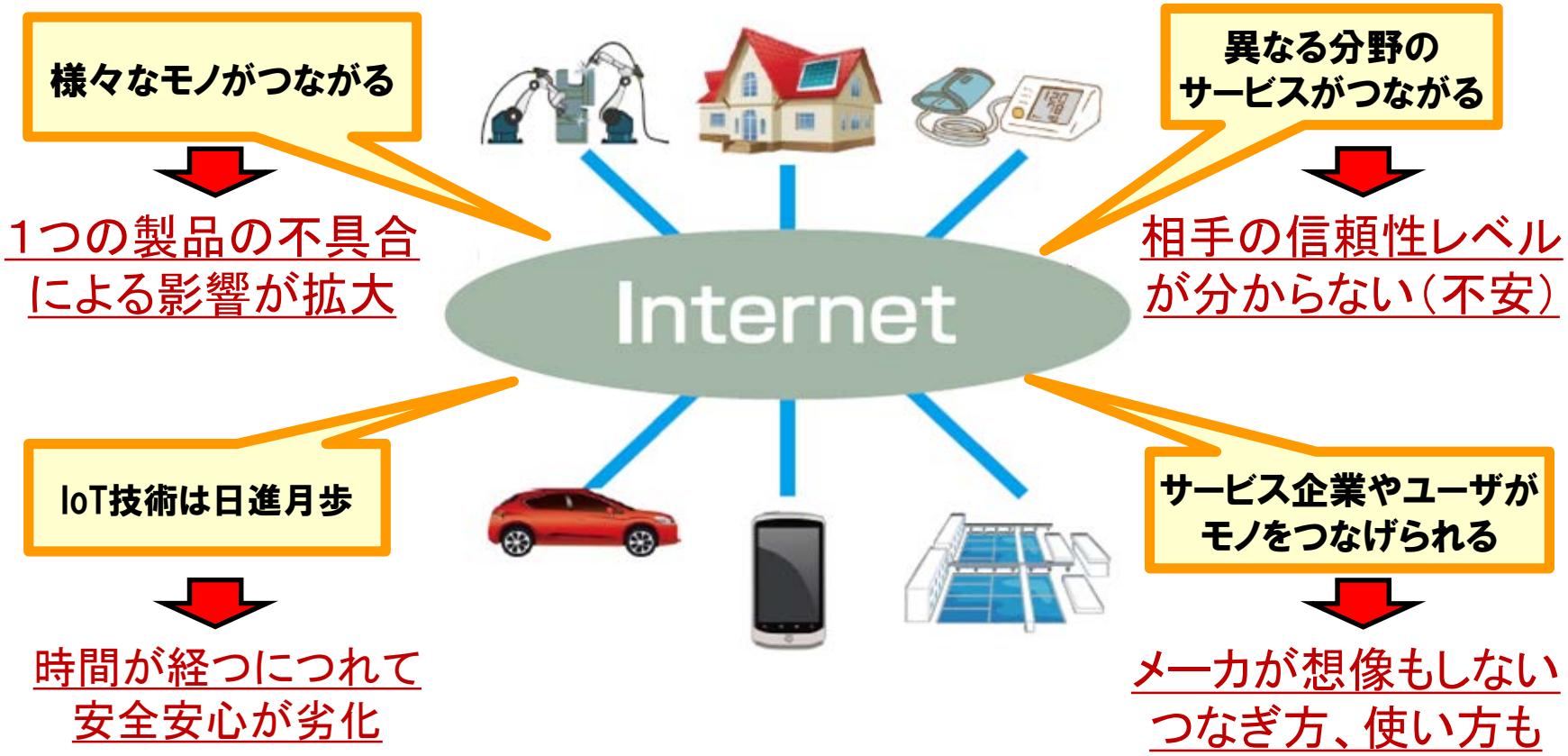
1.背景
IoT時代　新しいサービスが拡大

- モノがネットワークにつながり新しいサービスが拡大
- サービス同士がつながり新サービスが拡大

IoTの様々な課題

SEC
Software Reliability Enhancement Center

- モノがネットワークにつながることにより様々な問題が発生



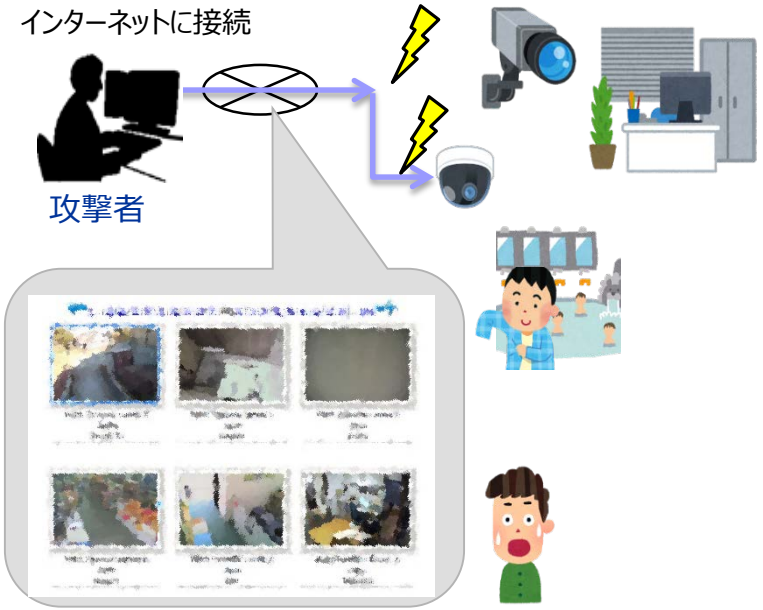
人命や財産を脅かすリスクも！

SEC Software Reliability Enhancement Center

■ セキュリティだけでなく人命や財産を脅かすリスク

監視カメラの映像がインターネット上に公開

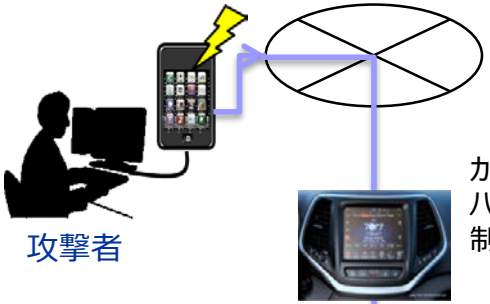
利用者が気づかないまま、WiFi等を通じて
インターネットに接続



セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。
（ID, パスワードなどの初期設定が必要）

自動車へのハッキングよる遠隔操作

携帯電話網経由で遠隔地からハッキング



カーナビ経由で
ハンドル、ブレーキを含む
制御全体を奪取。

人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

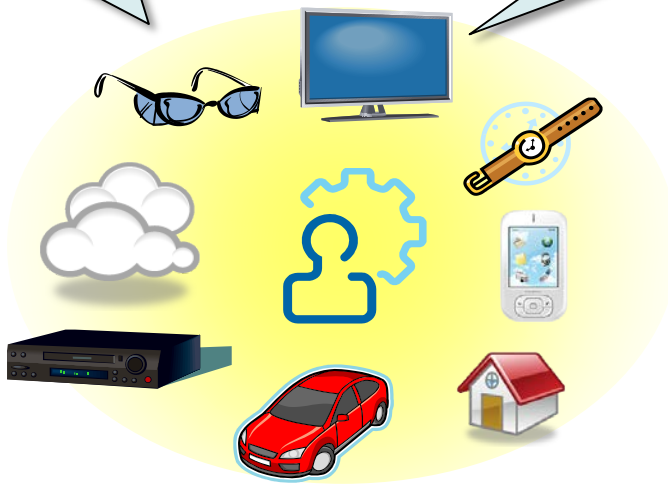
【出典】「経済産業省の取組とIoTセキュリティガイドラインVer1.0の概要」、経済産業省

IoTのリスクを認識し、安全安心への対策が急務！

安全安心なIoT機器・システムの開発における課題

安全安心の機能レベルで記載したIoTのガイド類は少ない

今後普及が見込まれる分野間連携の参考になる例が少ない



サイバー脅威からの防御（セキュリティ）

安定稼働の担保（リライアビリティ）

安全性確保（セーフティ）

2.実践に向けた手引きの概要
「つながる世界の開発指針」の実践に向けた手引き

SEC Software Reliability Enhancement Center

- 開発指針のうち技術面での対策が必要となる部分をさらに具体化
- 2017年5月公開、6月書籍発行：以下のURLにpdf版掲載
  - http://www.ipa.go.jp/sec/reports/20170508.html

つながる世界の開発指針

2016年3月

「つながる世界の開発指針」の実践に向けた手引き

2017年5月

①設計段階から考慮して欲しい要件とIoT高信頼化機能の具体例を解説

②IoT機器・システムやサービスのライフサイクルとクラウド・フォグ・エッジ等の機能配置を考慮し網羅的にイメージ

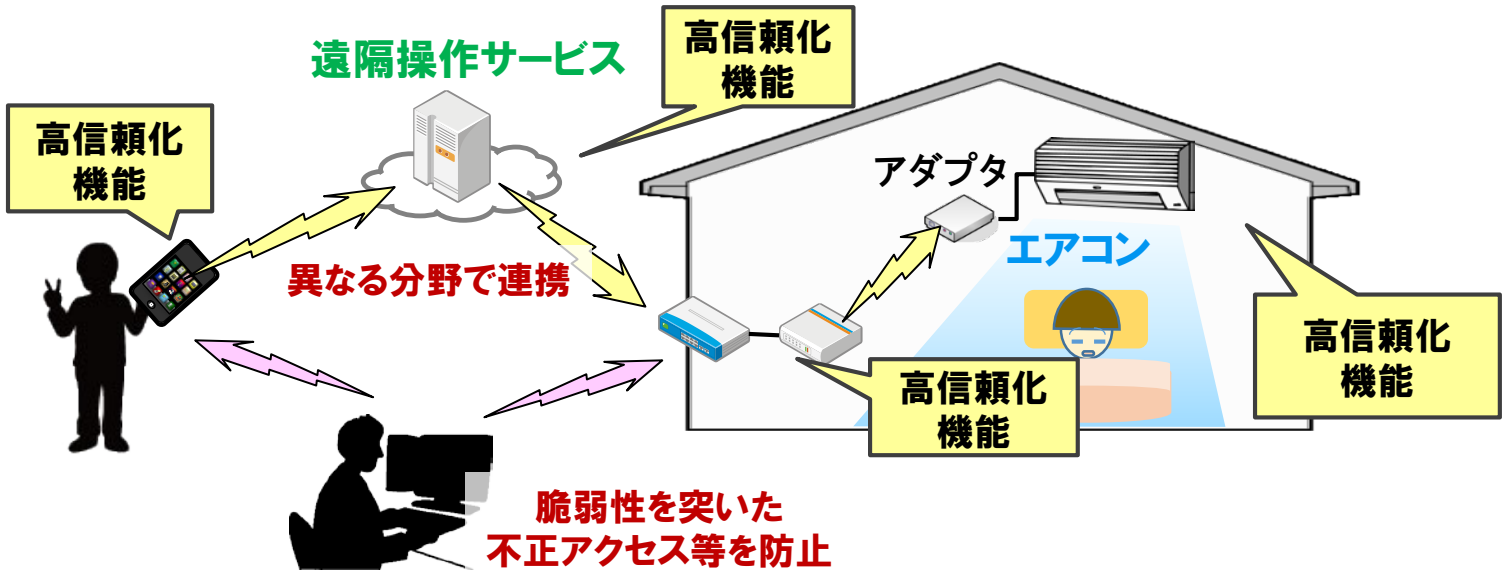
③IoTの分野間連携のユースケースと、リスクや脅威、機能定義や機能配置の具体例

IoTの安全安心のために必要な機能「IoT高信頼化機能」

■ 「実践に向けた手引き」における用語

■ IoT高信頼化機能とは
IoT機器・システムが相互に連携する(つながる)環境において、**安全安心を確保するための機能**

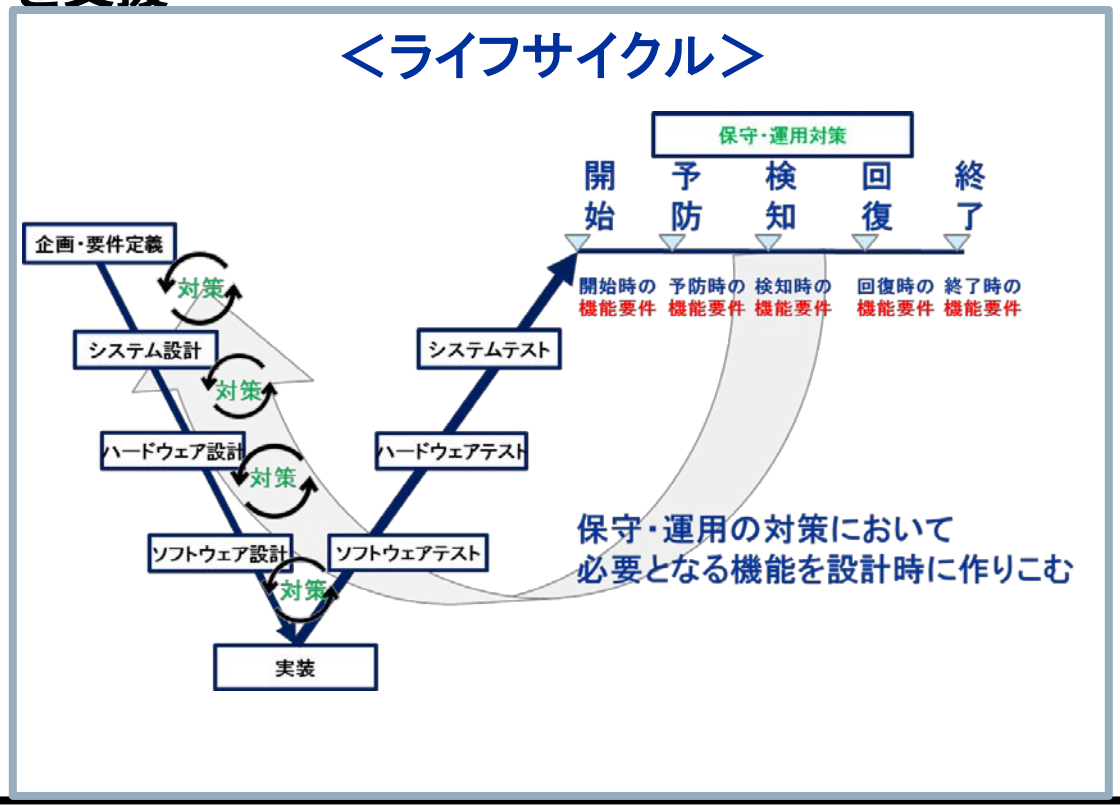
■ IoT高信頼化機能は、様々なIoT機器・システムでの利用を想定

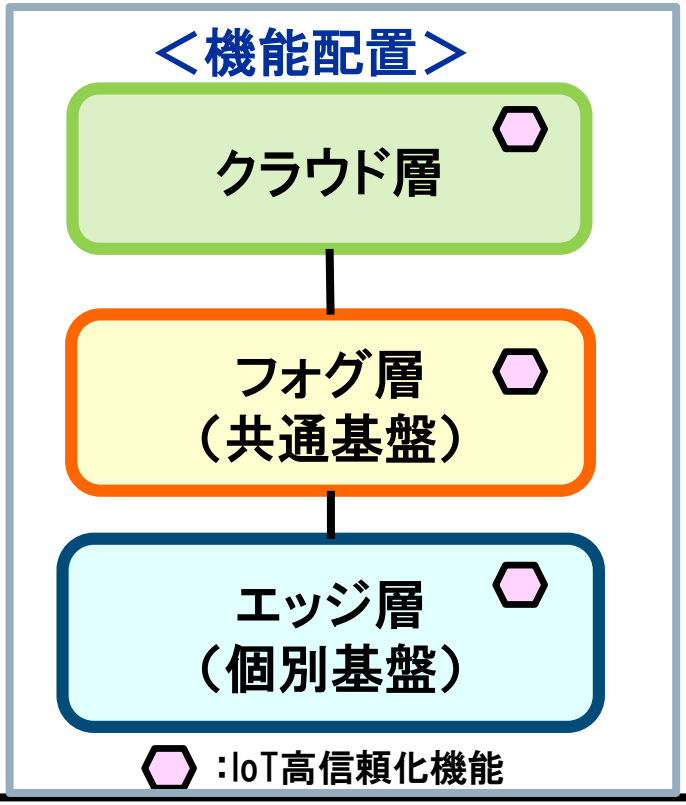


検討のスコープ（ライフサイクルと機能配置）

- IoT機器・システムのライフサイクルを考慮し、保守・運用で起こり得る様々な安全安心を阻害する事象に対応できることを目的に、IoTの**利用開始から予防・検知・回復、終了**の視点で、必要な機能を整理
- **クラウド・フォグ・エッジ**等の機能配置を考慮

→ 経済合理性や寿命を考慮し、全体として高信頼化を達成するための現実解を支援





２３のIoT高信頼化機能

SEC Software Reliability Enhancement Center

- 初期設定や認証など、具体的な機能を紹介
- 一般的な機能名ではあるが、IoTについて考慮した内容としている
  - 例）機器の認証や、軽量暗号、ホワイトリストによるウイルス対策等

IoT高信頼化機能					
1	初期設定機能	9	ウイルス対策機能	17	冗長構成機能
2	設定情報確認機能	10	暗号化機能	18	停止機能
3	認証機能	11	リモートアップデート機能	19	復旧機能
4	アクセス制御機能	12	監視機能	20	障害情報管理機能
5	ログ収集機能	13	状態可視化機能	21	操作保護機能
6	時刻同期機能	14	構成情報管理機能	22	寿命管理機能
7	予兆機能	15	隔離機能	23	消去機能
8	診断機能	16	縮退機能		

記載例

(9) ウイルス対策機能

目的	ウイルス感染の被害を防止する。
説明	ウイルス対策には、検出（侵入、実行、潜伏を含む）、駆除がある。検出には以下のような方式がある。 ・ ホワイトリスト方式 – 特にリソースの少ない IoT 機器の場合においては、登録されたソフトウェアのみ実行を許可することで、未知のウイルスの実行を防止する。 ・ ブラックリスト方式 – ウイルスチェックには、既知のウイルスをパターンファイルに登録し侵入、実行、潜伏を検出する。 ブラックリスト方式は、リソースが少ない場合には実装が難しいことが想定される。
参考	制御システム向けの端末防御技術「ホワイトリスト型ウイルス対策」とは？ http://monoist.atmarkit.co.jp/mn/articles/1404/07/news004.html

IoTについて考慮した事項

各機能の説明は簡潔にまとめ、詳細については参考情報を記載

(12) 監視機能

目的	機器・システムの異常を検知する。
説明	監視機能には以下のような機能がある。 ・ 異常の検知機能 – 障害/故障の検知（ログ分析含む） – セキュリティ異常の検知（ログ分析含む） – 制御の競合の検知　等 ・ 検知した異常の通知機能
参考	

セキュリティだけではなく、セーフティやリライアビリティに関する事項も含む

一般論だけでなく、ユースケース分析から明らかになった事項も記載

設計段階から考慮してほしい要件

SEC Software Reliability Enhancement Center

- 利用開始後の利用条件や環境の変化を見据えた設計が必要
- 保守運用における5つの視点「開始」「予防」「検知」「回復」「終了」で整理し、それをさらに12の機能要件に細分化

IoT高信頼化要件		IoT高信頼化を実現するための機能要件	対応IoT高信頼化機能
開始	導入時や利用開始時に安全安心が確認できる	初期設定が適切に行われ、その確認ができる	1、2
		サービスを利用する時に許可されていることを確認できる	3、4
予防	稼働中の異常発生を未然に防止できる	異常の予兆を把握できる	5、6、7、8、9
		守るべき機能・資産を保護できる	4、5、6、10
		異常発生に備えて事前に対処できる	11
検知	稼働中の異常発生を早期に検知できる	異常発生を監視・通知できる	12、13
		異常の原因を特定するためのログが取得できる	5、6
回復	異常が発生しても稼働の維持や早期の復旧ができる	構成の把握ができる	14
		異常が発生しても稼働の維持ができる	8、15、16、17
		異常から早期復旧ができる	11、18、19、20
終了	利用の終了やシステム・サービス終了後も安全安心が確保できる	自律的な終了や一時的な利用禁止ができる	18、21、22
		データ消去ができる	23

記載例

SEC
Software Reliability Enhancement Center

［要件3］稼働中の異常発生を早期に検知できる

(1) 概説

IoT システムは、一般に多数のセンサーなどの IoT 機器で構成されることが多く、かつ、他の IoT システムと連携してサービスが提供され、複雑な構成となることがある。これらの複雑化した構成の中で、一部の IoT 機器の障害/故障やセキュリティ異常が連携システム全体に影響を及ぼすことが想定されるので、異常の早期発見と被疑箇所の特定が重要となる。そのためには、普段からのシステムの監視や異常の原因を切り分けるための動作ログを収集することが必要である。

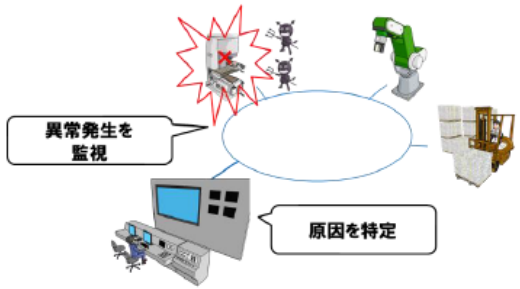


図 3-3 監視と原因特定

(2) 要求される機能

【機能要件6】異常発生を監視・通知できる

IoT 機器・システムの監視では、システムの各構成要素が保有する障害/故障やセキュリティ異常などの監視機能の能力を見極めて、システム全体としてもれなく監視が行き届くような設計が必要である。また、監視対象を明らかにして、その状態を逐次確認することが可能な状態可視化機能が必要である。なお、IoT の監視では、IoT 機器・システムの障害/故障やセキュリティ異常だけでなく、IoT 機器・システムなどに対する制御の競合が発生していないことを監視できる機能も必要である。制御の競合の検知については後述する。

【IoT 高信頼化機能】監視機能[12]、状態可視化機能[13]

IoT高信頼化要件

IoTとして実装上考慮すべき点

(3) 実装上の考慮事項

① **個々での異常検知ができない場合の考慮**

例えば、多数のセンサーが接続されている場合に、個々のセンサーの障害を監視することが困難な場合がある。そのような場合に、複数のセンサーからあげられてくるセンシング値を比較し、「外れ値（統計において他の値から大きく外れた値）」などにより、センサーの異常の推測を行うことが考えられる。このように、個々の IoT 機器での異常検知ができない場合に、異常情報以外の値や複数の情報を用いて、異常を推測することが考えられる。

【IoT 高信頼化機能】監視機能[12]

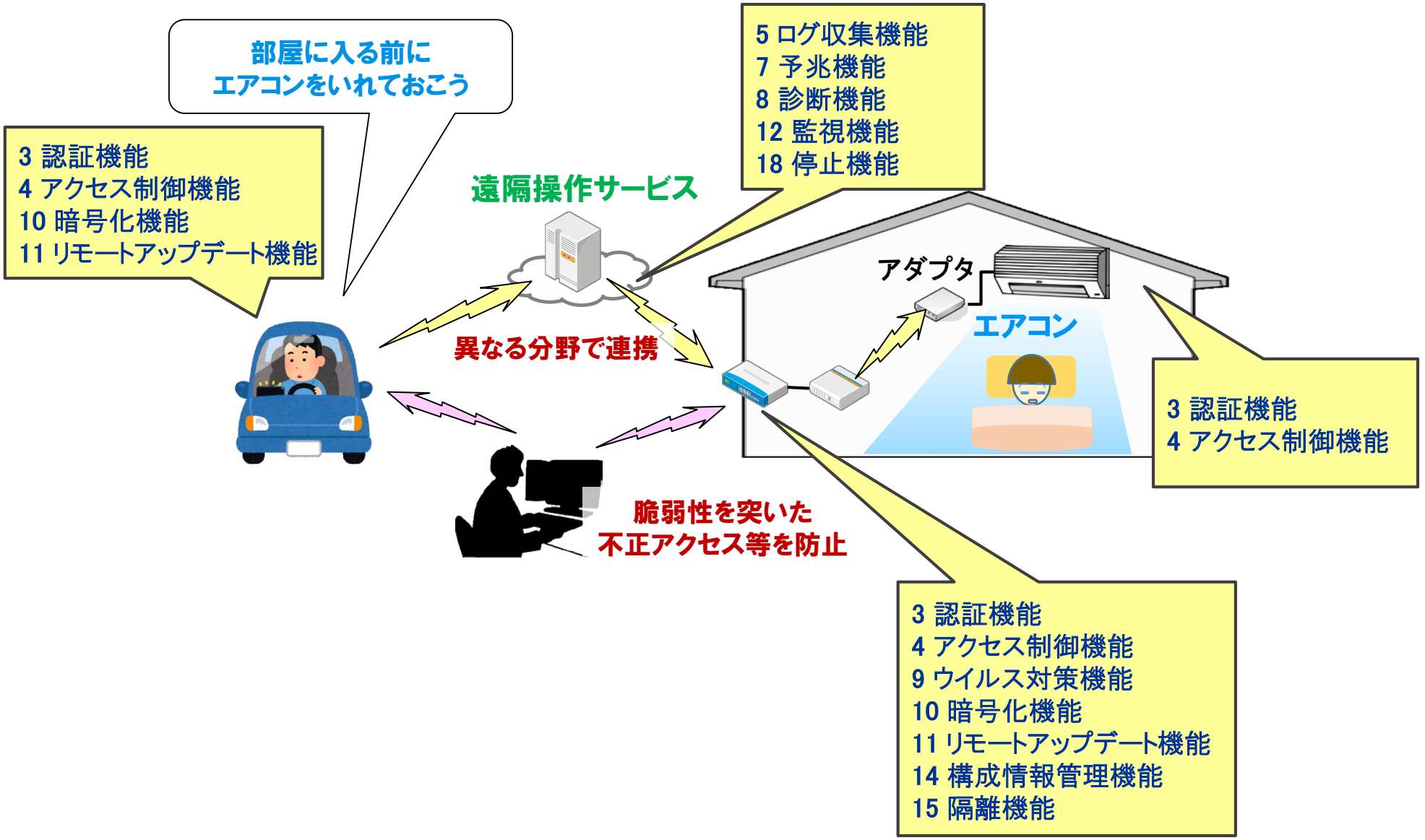
② **競合への考慮**

IoT では、各種サービスが複雑に連携するケースが想定され、一つの IoT 機器・システムが同時に複数のサービスから相反する指示を受けることがある。例えば、住宅の中で、快適サービスからは、暑くなってきたので窓を開ける指示と、一方、防犯サービスでは、窓を閉める指示が出されるなど、制御が競合する場合がある。競合の状況が検知できることが重要であり、競合状況としては、互いに正常な指示の競合だけでなく、一方が不正な指示による競合も想定が必要となる。

要求される機能

IoT高信頼化を実現するための機能

機能適用イメージ


部屋に入る前に
エアコンをいれておこう
3 認証機能
4 アクセス制御機能
10 暗号化機能
11 リモートアップデート機能
遠隔操作サービス
5 ログ収集機能
7 予兆機能
8 診断機能
12 監視機能
18 停止機能
アダプタ
エアコン
異なる分野で連携
3 認証機能
4 アクセス制御機能
脆弱性を突いた
不正アクセス等を防止
3 認証機能
4 アクセス制御機能
9 ウイルス対策機能
10 暗号化機能
11 リモートアップデート機能
14 構成情報管理機能
15 隔離機能

ユースケース一覧

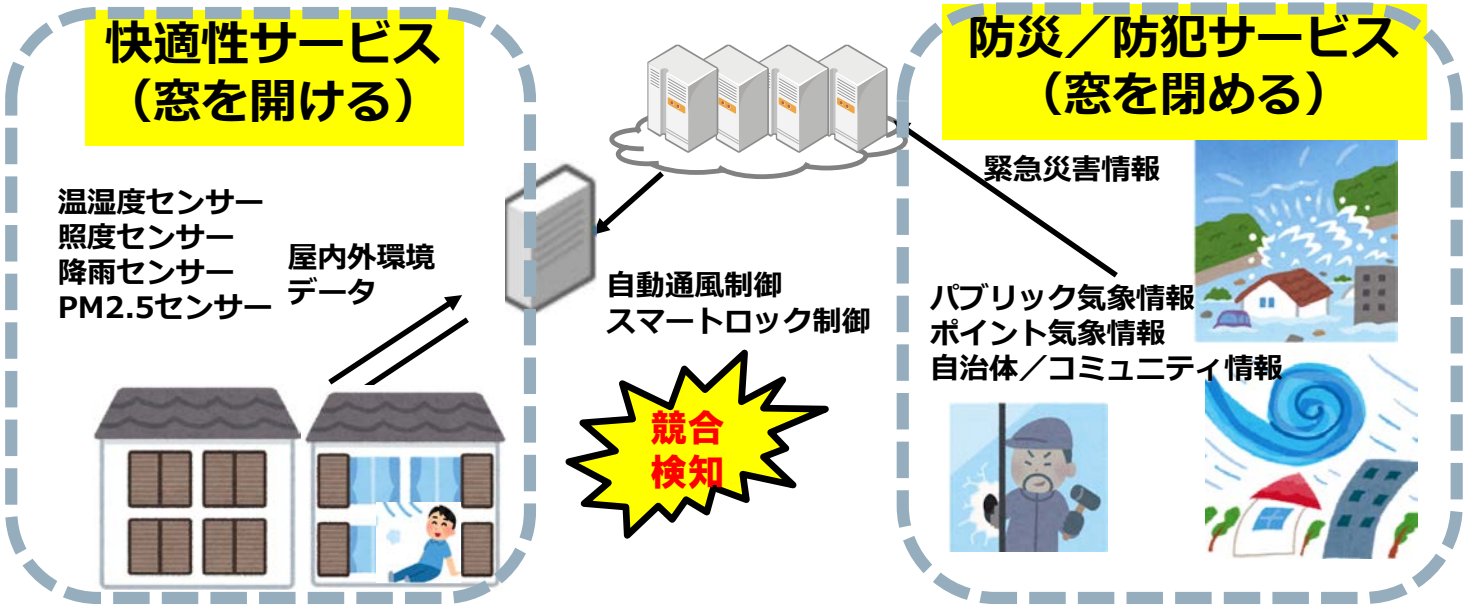
- 現状実現できるものや今後想定されるものから、IoTの分野間連携の5つのユースケースを想定
- ユースケースによっては、複数の連携モデルの要素を含むことが分かり、特徴的なモデル（表の◎）を中心に分析

ユースケース		ECモデル	FCモデル	CCモデル	補足説明
UC1	車両と住宅の連携			◎	クラウドが活用されており、リアルタイム性は要求されないのでCCモデル。
UC2	VPPと分散型電源監視サービスとの連携	○		◎	複数のサービスの連携を実施する。HEMSサーバ機能がクラウド上にあるモデルと需要家機器内にあるモデルがあり前者をCCモデルとして選定。
UC3	宅内機器連携	◎			HEMSのデバイスやコントローラ間の連携 フォグやクラウドまでは利用しない
UC4	戸締り競合制御	◎	○	○	ホームGW／エッジサーバ内の複数の制御ソフト間で競合解決
UC5	産業ロボットと電力管理の連携	○	◎		複数のサービスを連携し、判断の応答性が重視されるフォグ連携システムとして選定

ユースケースの例

- **ユースケース名：**戸締り競合制御
- **概要：**宅内における快適性制御のための自動通風システムと緊急災害、防犯対策システムとの競合
- **想定される脅威/被害：**制御ロジックが競合し安全性が損なわれる

競合検知が監視機能として必要に！



4.要件・機能詳細
IoTにおける脅威の事例

SEC Software Reliability Enhancement Center

- **IoT機器を狙うマルウェア「Mirai」**
  - 組み込みLinuxおよび軽量UNIXコマンドツールBusyBoxの上に実装されたIoT機器が感染対象
  - 感染したIoT機器は、同様に感染可能なIoT機器を探索して攻撃者に報告しボットネット構築に利用される
- **IoT機器が「Mirai」に感染した理由**
  - ポート番号23または2323でtelnetが動作していた
  - ユーザ名、パスワードが初期値のまま動作していた
  - Flashpoint社の調査によると、この条件を満たすIoT機器が世界中に51万5千台以上発見されている

[第14回情報セキュリティEXPO　IPA　「顕在化したIOTのセキュリティ脅威と対策（https://www.ipa.go.jp/files/000059579.pdf）から引用]

この事例からだけでもいくつかの機能の必要性がわかる
① 不要なサービスの公開の停止
② ユーザ名、パスワードを初期値のまま
③ さらに感染しても動作しないようにする仕組み

［開始］導入時や利用開始時に安全安心が確認できる

SEC Software Reliability Enhancement Center

- 初期設定の不備をなくすとともに、許可された者か・アクセス可能なデバイスかなどの設定や確認を行う

		1 初期設定機能	2 設定情報確認機能	3 認証機能	4 アクセス制御機能
【機能要件1】初期設定が適切に行われ、その確認ができる		✔	✔		
	安全安心に係る初期設定が適切に行われる				
	初期設定が適切であることを確認できる				
【機能要件2】サービスを利用する時に許可されていることを確認できる				✔	✔
	接続されるときに本人や正しい機器であるかを確認できる				
	設定された情報にもとづき利用の許可/制限ができる				
	相互の信用度を確認して接続の可否判断ができる				

IoT高信頼化機能

（１）初期設定機能

目的	システムの構築・接続時や利用開始時に必要な設定が実施されるようにする。
説明	初期設定機能には以下のような機能がある。 ・ 各種情報の範囲設定 ・ 管理者権限、利用者権限などのパスワード設定（デフォルトパスワードからの変更機能、強固なパスワード設定を促すガイド機能含む） ・ アクセス制御の設定 ・ 不要なポート・サービスの停止 ・ ソフトウェアのアップデートの設定 ・ 信用度に関する情報の設定　など 未設定の場合には、システムの利用を開始できないようにする
参考	

接続する機器数が膨大になる場合を考慮しよう

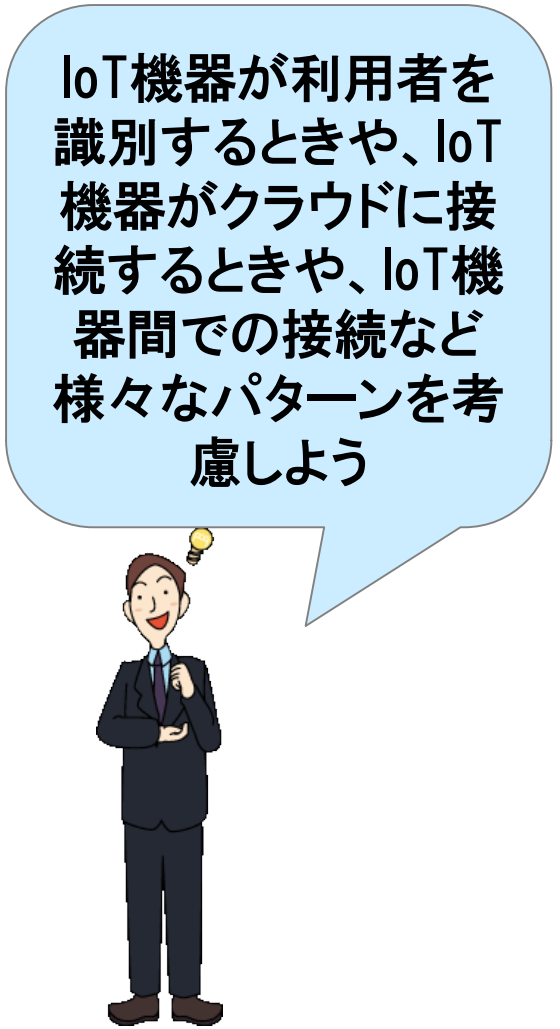
（２）設定情報確認機能

目的	機器・システムの設定情報の確認を行う
説明	設定情報確認機能には以下のような機能がある。 ・ システムの構築・接続時や利用開始時に、個々の機器やシステムの初期設定が適切に実施されていない場合の警告 ・ システム全体において設定情報をわかりやすく確認
参考	

IoT高信頼化機能

（３）認証機能

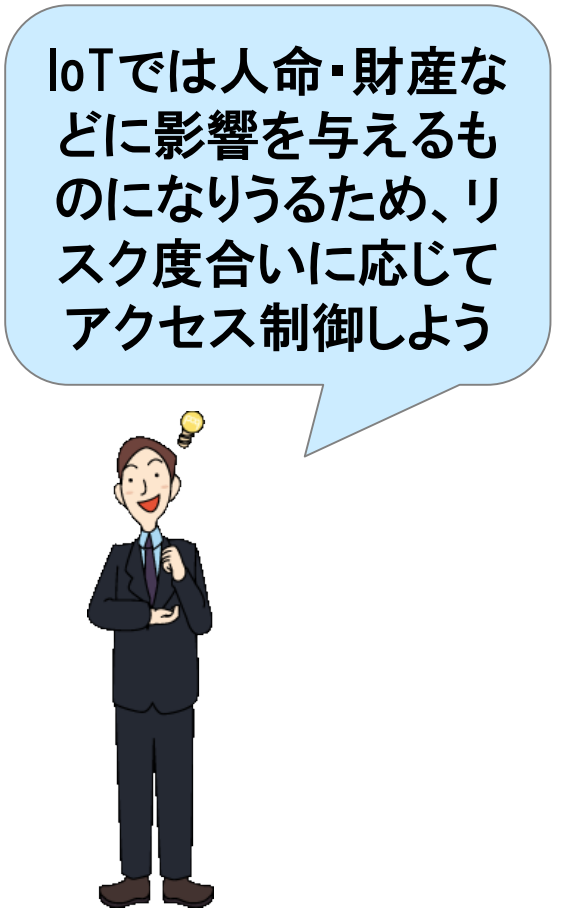
目的	利用者、機器などを一意に識別し、本人、あるいは、正しいものであるかどうかを確認する。
説明	認証方式には以下のような方式がある。 ・ 接続するIoT機器のなりすまし防止 – IoT機器の識別子による認証 – クライアント証明書による認証 – メッセージ認証 ・ 利用者のなりすまし防止 – ID・パスワードによる認証 – ICカードなどの所有物による認証 – 生体認証 ・ 接続する相手のシステム・サービスのなりすまし防止 – 接続する相手のシステム・サービス相互で鍵・電子証明書等を使用した認証 上記の、いくつかの方式を組み合わせた多要素認証などの方式もある。 また、一定回数以上の認証に失敗した場合にロックする機能などがある。
参考	・ [IoT推進コンソーシアム]IoTセキュリティガイドライン http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf ・ [CSA]IoT早期導入者のためのセキュリティガイダンス https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf ・ [CRYPTREC]電子政府推奨暗号の利用方法に関するガイドブック http://www.cryptrec.go.jp/report/c07_guide_final.pdf



IoT高信頼化機能

（４）アクセス制御機能

目的	守るべきものを保護するために、守るべきものに対する操作を制限する。
説明	アクセス制御は認証によって識別されたIDに基づいて、守るべきものに対する操作を許可、または拒否する。 アクセス制御方式には、以下のような方式がある。 ・ 任意アクセス制御(DAC) ・ 強制アクセス制御(MAC) ・ ロールベースアクセス制御(RBAC)
参考	



［予防］稼働中の異常発生を未然に防止できる

SEC Software Reliability Enhancement Center

■ 異常の発生を予知や、守るべきもの保護や、問題の事前対処を行う

	4 アクセス制御機能	5 ログ収集機能	6 時刻同期機能	7 予兆機能	8 診断機能	9 ウイルス対策機能	10 暗号化機能	11 リモートアップデート機能
【機能要件3】異常の予兆を把握できる		✔	✔	✔	✔	✔		
異常の発生を予測し、それを通知する								
ハードウェアの正常動作の確認やウイルス対策を行う								
【機能要件4】守るべき機能・資産を保護できる	✔	✔	✔				✔	
守るべきものを特定し保護する								
保護状態が維持できているかを確認する								
【機能要件5】異常発生に備えて事前に対処できる								✔
遠隔で改修できる								

IoT高信頼化機能

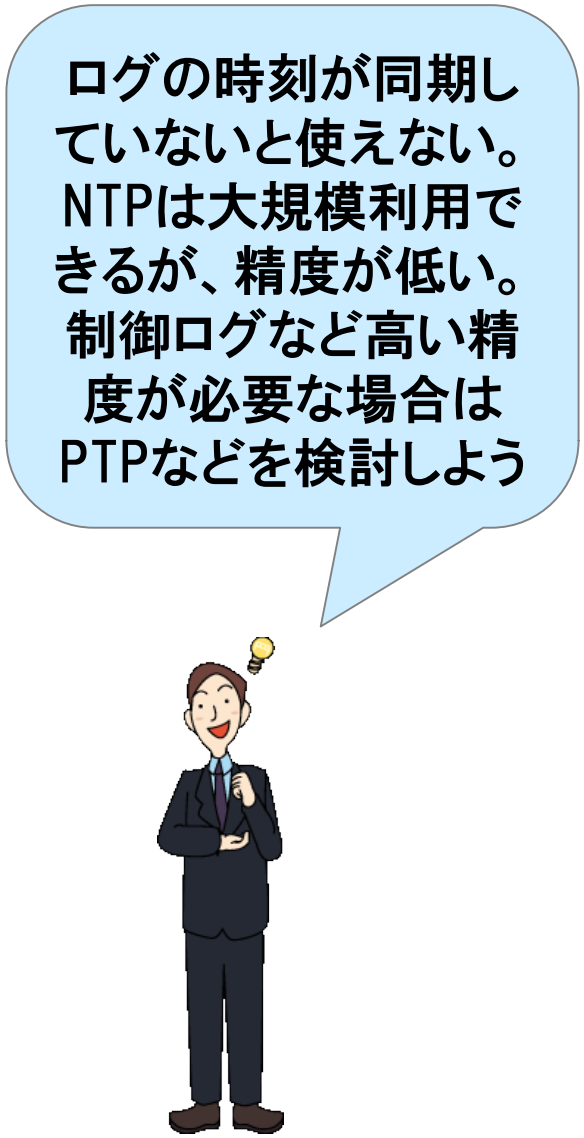
（5）ログ収集機能

目的	機器やシステム上で発生した事象を追跡可能とするために、発生したイベントに関する情報を蓄積する。
説明	ログ収集機能には以下のような機能が含まれる。 ・ 特定のイベントに関連した記録をするための情報に関するログ生成 ・ リソースの少ないIoT機器などの場合に、他の機器へのセキュアなログ転送 ・ ログの保存 – ログの保存においては、リソースが限られている場合のローテーションやログ喪失防止のためのバックアップがある – 保存したログの保護にはアクセス制御、暗号化、追記のみ可能とするなどの方法がある ・ 不要となったログの破棄 記録する内容の例 ・ セキュリティ解析用：攻撃、ユーザ認証、データアクセス、構成管理情報更新、アプリケーション実行、ログの記録開始・停止、通信、扉の開閉、チェックサム、移動履歴 ・ セーフティ解析用：故障情報（ハードウェア/ソフトウェア） ・ リライアビリティ解析用：結果情報、状態情報、動作環境情報（温度、湿度、CPU負荷、ネットワーク負荷、リソース使用量等）、ソフトウェアの更新
参考	[NIST] SP800-92 コンピュータセキュリティログ管理ガイド http://www.ipa.go.jp/files/000025363.pdf

IoT高信頼化機能

（６）時刻同期機能

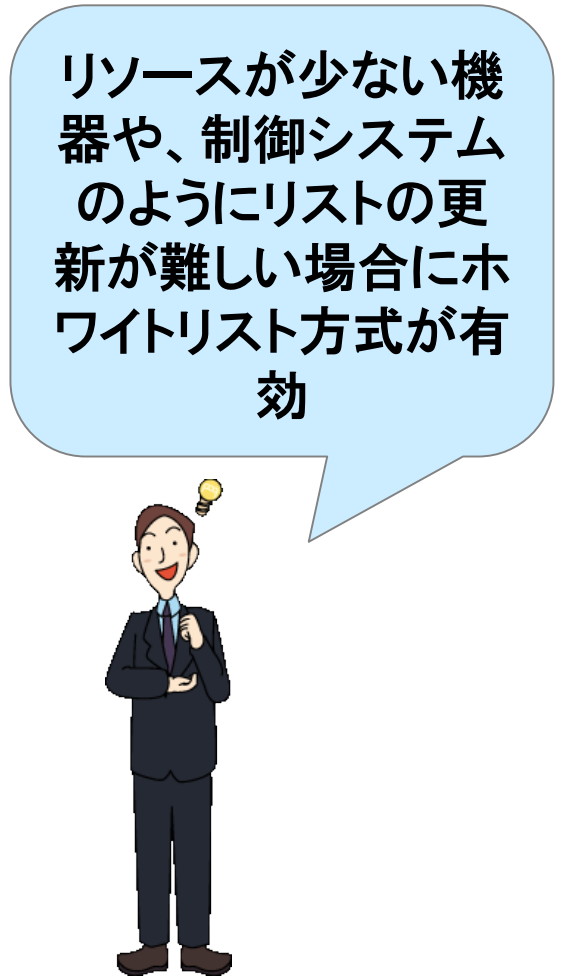
目的	機器・システム間で時刻を合わせる。
説明	時刻同期には、基準となる絶対時刻に合わせる方式と、つながる機器・システム間で相対的な時刻のずれがないように合わせる方式があり、例えば以下のような方式がある。 ・ 絶対時刻にあわせる方式 – 10ms程度の精度のNTP ・ 相対的な時刻に合わせる方式 – 1μs以下の精度のIEEE1588 PTP – 無線LANにおける時刻同期のためのIEEE802.11　TSF
参考	• NTP http://www.ntp.org/ • IEEE1588　PTP(Precision Time Protocol) • IEEE802.11　TSF(Timing Synchronization Function) • IEEE802.1 TSN(Time Sensitive Networking) • IEEE802.15.4 Time-slotted communication model https://standards.ieee.org/から購入が必要



IoT高信頼化機能

（9）ウイルス対策

目的	ウイルス感染の被害を防止する。
説明	ウイルス対策には、検出（侵入、実行、潜伏を含む）、駆除がある。検出には以下のような方式がある。 ・ ホワイトリスト方式 – 特にリソースの少ないIoT機器の場合においては、登録されたソフトウェアのみ実行を許可することで、未知のウイルスの実行を防止する。 ・ ブラックリスト方式 – ウイルスチェックには、既知のウイルスをパターンファイルに登録し侵入、実行、潜伏を検出する。 ブラックリスト方式は、リソースが少ない場合には実装が難しいことが想定される。
参考	制御システム向けの端末防御技術「ホワイトリスト型ウイルス対策」とは？ http://monoist.atmarkit.co.jp/mn/articles/1404/07/news004.html



（10）暗号化機能

目的	機器やシステムに格納されたデータ、または通信経路上のデータを、暗号技術を用いて電子署名や暗号化を行う。
説明	暗号化機能の詳細は参考に示す文献に記述されている。 暗号化する際は、適切なセキュリティ強度を持った暗号アルゴリズム、鍵長の使用や、鍵の適切な管理が必要となる。リソースの限られたデバイスにも実装可能な「軽量暗号」も開発されている。 暗号化機能は、認証や改ざん検知などでも用いられる。
参考	・ [IPA]IoT開発におけるセキュリティ設計の手引き https://www.ipa.go.jp/files/000052459.pdf ・ [CRYPTREC] 電子政府推奨暗号の利用方法に関するガイドブック http://www.cryptrec.go.jp/report/c07_guide_final.pdf ・ [CRYPTREC] 暗号技術調査 WG（軽量暗号）報告書 https://www.cryptrec.go.jp/estimation/techrep_id2406.pdf

計算量がすくなく、コストも抑えることができる軽量暗号の開発が進んでいる

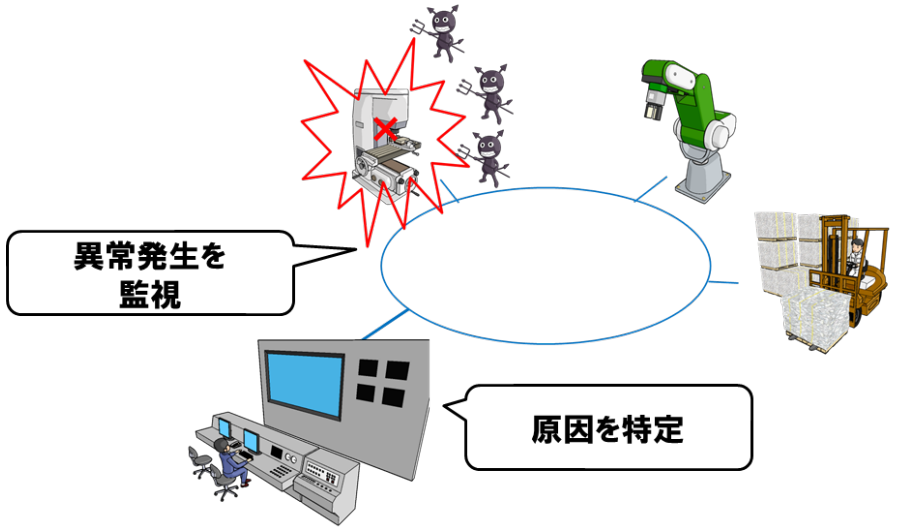
（11）リモートアップデート機能

目的	ソフトウェアの不具合や脆弱性を改修するために、遠隔で更新を行う。
説明	リモートアップデート機能には以下のような機能が含まれる。 ・アップデートファイルの暗号化、署名 ・改修した箇所の記録（ログ収集機能） ・アップデートスケジューリング ・アップデート優先度設定 ・アップデート、及び失敗した場合のバージョンダウン アップデートは遠隔での実行に限らないが、IoT機器・システムでは、特に離れた場所での保守が見込まれるため、リモートアップデート機能に注目した。
参考	

［検知］稼働中の異常発生を早期に検知できる

SEC Software Reliability Enhancement Center

■ 異常の早期発見・被疑箇所の特定、そのために監視やログの収集を行う



		5 ログ収集機能	6 時刻同期機能	12 監視機能	13 状態可視化機能
【機能要件6】異常発生を監視・通知できる				✔	✔
	障害/故障やセキュリティ異常などをシステム全体としてもれなく監視する				
	監視対象を明らかにして、その状態を逐次確認する				
	制御の競合を監視する				
【機能要件7】異常の原因を特定するためのログが取得できる		✔	✔		
	障害/故障やセキュリティ異常を切り分けする				
	各IoT機器から取得したログの時刻を合わせる				

IoT高信頼化機能

（12）監視機能

目的	機器･システムの異常を検知する。
説明	監視機能には以下のような機能がある。 ・ 異常の検知機能 – 障害/故障の検知(ログ分析含む) – セキュリティ異常の検知(ログ分析含む) – 制御の競合の検知　等 ・ 検知した異常の通知機能
参考	

複数のIoTに接続することによる制御の競合を検知できるようにしよう

［終了］利用の終了やシステム・サービス終了後も安全安心が確保できる

SEC Software Reliability Enhancement Center

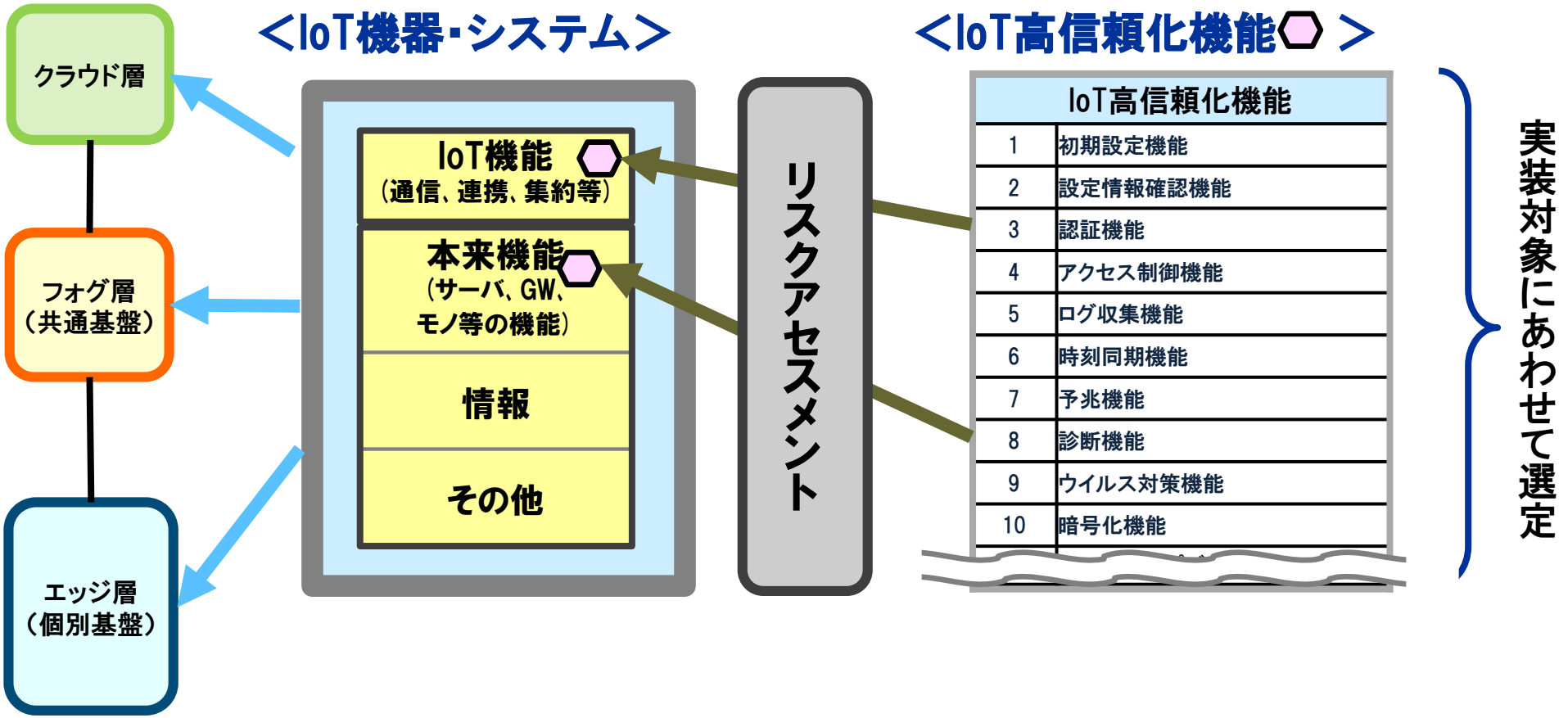
- 正常な終了処理を忘れた場合でも安全保ち、また終了時にはデータを消去する

	18 停止機能	21 操作保護機能	22 寿命管理機能	23 消去機能
【機能要件11】自律的な終了や一時的な利用禁止ができる	✔	✔	✔	
長時間稼働状態のままの場合に自律的に終了				
放置や盗難時において一時的に利由を禁止				
使用期間や稼働時間満了時の利用者への通知				
【機能要件12】データ消去ができる				✔
セキュアにデータ消去できる				

（23）消去機能

目的	機器やシステムを破棄するときなどの情報の漏えいを防止する。
説明	ファイルの削除や、初期化（USBメモリのフォーマット等）では、特殊な方法で復元することが可能な場合がある。ここでいう消去は、完全にデータを読めなくすることである。消去機能では設定した情報や、保存したデータを消去する。 消去機能では磁気的に記憶された情報を完全に消去する必要があり、例えば以下のような方式がある。 ・ NSA方式 ・ DoD方式 ・ Peter Gutmann方式　など
参考	・ NSA/CSS Policy manual 9-12 https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf ・ DoD 方式（DoD5220.22-M） http://www.dss.mil/documents/odaa/nispom2006-5220.pdf ・ Secure Deletion of Data from Magnetic and Solid-State Memory https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

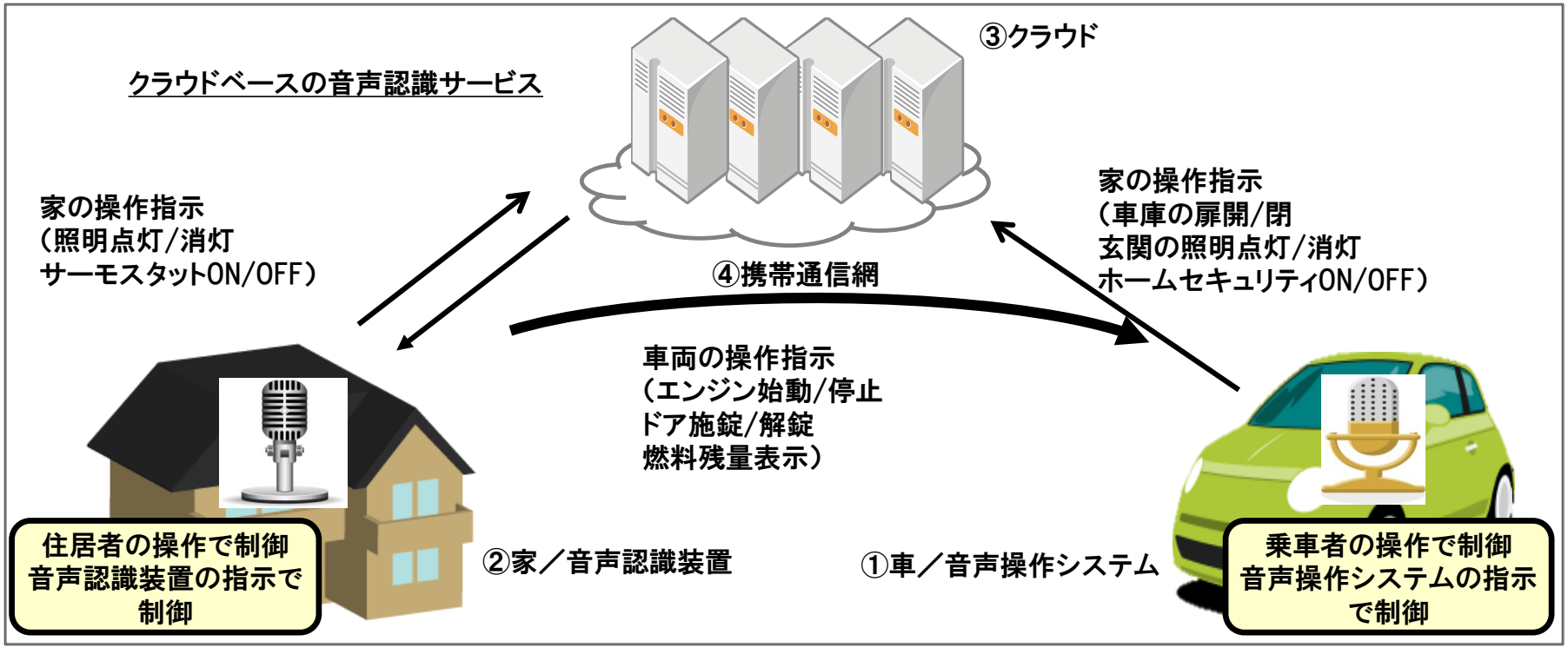
5．IoT高信頼化機能の適用の考え方



リスク評価に使用したユースケース

■ 車両と自動車の連携

- 車両の運転手は車載の音声システムを通じて住宅を操作
- 住居者は自宅から家のクラウドベースの音声認識サービスを経由して車両を操作



リスク評価例（前半）

SEC Software Reliability Enhancement Center

- ６つのリスク特性（分野固有・共通、脅威の分類、接続I/F、誰がつなげたか、何が危害をうけたか、どこで発生したか）で整理

No.	想定脅威	想定被害	対象機器	分野固有・共通	脅威の分類	接続I/F（侵入ルート）	who 誰がつなげたか	whom 何が危害をうけたか	where どこで発生したか
1	車／音声操作システムウイルス感染（※システム全体のうち、車が攻撃される）	異常操作による人体への悪影響(e.g.大音量)	車載器	分野固有	ウイルス感染	USB	ユーザー（意図的）	身体や財産	サービス用I/F
2	家／音声認識装置からの異常操作情報（※システム全体のうち、家が攻撃される）	交通事故(e.g.エンジン停止)	宅内機器	共通	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
3	他の家／音声認識装置からの誤操作情報（※他のシステムから、自システムの車が攻撃される）	交通事故(e.g.エンジン停止)	車載器	分野固有	不正利用	3G/GSM	メーカーや関連企業	身体や財産	サービス用I/F
4	家／音声認識装置ウイルス感染（※システム全体のうち、家が攻撃される）	異常操作による人体への悪影響(e.g.過剰な光)、住居・家財の災害(e.g.火事・盗難)	宅内機器	共通	ウイルス感染	USB	ユーザー（意図的）	身体や財産	サービス用I/F
5	車／音声操作システムからの異常操作情報（※システム全体のうち、車が攻撃される）	同上	車載器	分野固有	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
6	他の車／音声操作システムからの誤操作情報（※他のシステムから、自システムの家が攻撃される）	同上	宅内機器	共通	不正利用	3G/GSM	攻撃者	身体や財産	サービス用I/F
7	クラウドサーバの情報漏洩	個人情報の悪用	サーバ	共通	情報漏えい	インターネット	攻撃者	データ	サービス用I/F
8	クラウドサーバのサービス停止	連携機能の停止	サーバ	共通	DoS攻撃	インターネット	メーカーや関連企業	本来機能	サービス用I/F
9	通信データの改ざん、なりすまし	異常操作による人体への悪影響(e.g.大音量) 交通事故(e.g.エンジン停止)	サーバ	共通	盗聴	インターネット	攻撃者	本来機能	サービス用I/F
10	車／盗難	個人情報の悪用	車載器	分野固有	情報漏えい	USB	攻撃者	データ	物理的接触
11	車／廃棄時の情報漏えい	個人情報の悪用	車載器	分野固有	情報漏えい	USB	攻撃者	データ	物理的接触

リスク評価例（後半）

SEC Software Reliability Enhancement Center

CRSSによるリスク評価

			CRSS（CVSSの応用）								
No.	想定脅威	想定被害	AV 攻撃元区分	AC 攻撃条件の複雑さ	Au 攻撃前の認証要否	攻撃容易性	C 機密性への影響	I 完全性への影響	A 可用性への影響	影響度	リスク値
1	車／音声操作システムウイルス感染（※システム全体のうち、車が攻撃される）	異常操作による人体への悪影響(e.g.大音量)	ローカル	低	単一	3.14	甚大	甚大	甚大	10.00	6.77
2	家／音声認識装置からの異常操作情報（※システム全体のうち、家が攻撃される）	交通事故(e.g.エンジン停止)	隣接	中	単一	4.41	甚大	甚大	軽微	9.54	7.04
3	他の家／音声認識装置からの誤操作情報（※他のシステムから、自システムの車が攻撃される）	交通事故(e.g.エンジン停止)	ネットワーク	中	複数	5.49	軽微	軽微	軽微	6.44	5.36
4	家／音声認識装置ウイルス感染（※システム全体のうち、家が攻撃される）	異常操作による人体への悪影響(e.g.過剰な光)、住居・家財の災害(e.g.火事・盗難)	ローカル	低	単一	3.14	甚大	甚大	甚大	10.00	6.77
5	車／音声操作システムからの異常操作情報（※システム全体のうち、車が攻撃される）	同上	ネットワーク	中	複数	5.49	甚大	甚大	軽微	9.54	7.55
6	他の車／音声操作システムからの誤操作情報（※他のシステムから、自システムの家が攻撃される）	同上	ネットワーク	中	複数	5.49	軽微	軽微	軽微	6.44	5.36
7	クラウドサーバの情報漏洩	個人情報の悪用	ネットワーク	高	複数	3.15	甚大	なし	なし	6.87	4.57
8	クラウドサーバのサービス停止	連携機能の停止	ネットワーク	高	複数	3.15	なし	なし	甚大	6.87	4.57
9	通信データの改ざん、なりすまし	異常操作による人体への悪影響(e.g.大音量) 交通事故(e.g.エンジン停止)	ネットワーク	高	複数	3.15	甚大	甚大	軽微	9.54	6.45
10	車／盗難	個人情報の悪用	ローカル	中	単一	2.70	甚大	なし	甚大	9.21	6.00
11	車／廃棄時の情報漏えい	個人情報の悪用	ローカル	中	単一	2.70	甚大	なし	なし	6.87	4.35

リスク評価例

SEC Software Reliability Enhancement Center

IoT高信頼化機能による対策検討例

IoT高信頼化機能要件	主に関連するリスク(リスク番号)	優先度	対策	対策として適用できる主な機能
【機能要件1】初期設定が適切に行われ、その確認ができる	他の家/音声認識装置からの操作(3)	M	正当性が確認できるように設定を行う(機能要件2の対策に関連)	初期設定機能
	他の車/音声操作システムからの操作(6)	M		
【機能要件2】サービスを利用する時に許可されていることを確認できる	他の家/音声認識装置からの操作(3)	M	正当性を確認し正当でない場合は通信遮断、ユーザ通知	認証機能 アクセス制御機能
	他の車/音声操作システムからの操作(6)	M		
【機能要件3】異常の予兆を把握できる	車/音声操作システムウイルス感染(1)	M	ウイルス感染を防止する	ウイルス対策機能
	家/音声認識装置ウイルス感染(4)	M		
【機能要件4】守るべき機能・資産を保護できる	情報漏えい(7)、通信データの改ざん、なりすまし(9)	M	データを保護する	暗号化機能認証機能(メッセージ)
【機能要件5】異常発生に備えて事前に対処できる	家/音声認識装置からの異常操作(2)	C	脆弱性を潰し不正操作されないようにする	リモートアップデート機能(ローカルなアップデート含む)

ご清聴ありがとうございました。