IoT セキュリティ・セーフティ・フレームワーク Version 1.0
実践に向けたユースケース集(仮題)

2-3-1.ガス給湯器の遠隔操作

(1) リスク評価、リスク対応に向けた事前準備

① 対象ソリューションの概要

住まい手が外出先よりスマートフォン用のアプリケーションを通じて、居内のガス給湯器[1]を遠隔操作し、自動で浴槽等のお湯張りを実施するケースを想定する。

なお、ガス製品には遠隔操作が禁止されるものも存在するが、本稿では遠隔操作が許容される方式を用いた製品の利用を前提とする。各事業者等において、本稿を参照し、具体的な取組みを進めようとする際には、改めて既存の法律や文献[2]を参照されたい。

- 外出先よりスマートフォンの専用アプリケーションを活用して、自宅のお風呂のお湯張りを行う。
- なお、ガス給湯器のうち、「自然給排気式・開放式」以外を想定。これは、「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）にて「自然給排気式・開放式」の遠隔操作が禁止されているため。（※）

※ 経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」（令和2年7月）では、「自然吸排気式」及び「開放式」以外の機器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。

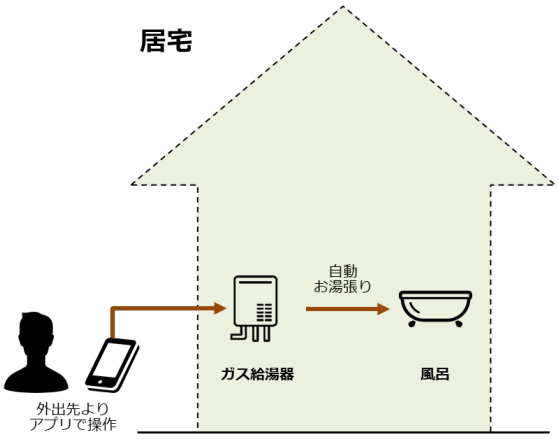

図 1 対象ソリューションの概要

② ステークホルダー関連図

本稿にて示す取組みに関与するステークホルダーとして、以下に示すように、「スマートホーム向け IoT 機器の事業者」、「スマートホームを供給する事業者」、「住まい手」及び「スマートホーム向けにメンテナンスやサポートを行う事業者」を想定している。

なお、本稿では、既に完成している住宅ではなく、新築の住宅に対して IoT 機器・システムを含む設備一式を納入する事例を想定する。具体的には、「スマートホーム向け IoT 機器の事業者」が製造したガス給湯器は、「スマートホームを供給する事業者」を通じて「住まい手」に納入される。また、「スマートホームを供給する事業者」が提供するホームコントローラは、ガス給湯器以外の IoT 機器・システムにも接続され、居内の IoT 機器システムを一括してコントロールすることを想定している。なお、一般にスマート

[1] 経済産業省「液化石油ガス器具等の技術上の基準等に関する省令の運用について」(2020 年 7 月)では、「自然吸排気式」及び「開放式」以外のガス給湯器において「リスク低減策を講じることにより遠隔操作に伴う危険源がないと評価されるもの等の基準に合致し、危険が生ずるおそれがないものは、操作可能」とされている。したがって、本稿では「自然吸排気棄式・開放式」以外のガス給湯器を想定している。

[2] 既存の文献として、経済産業省「電気用品、ガス用品等製品の IoT 化等による安全確保の在り方に関するガイドライン」(2021 年 4 月)等が挙げられる。

ホームとして戸建住宅もしくは集合住宅が扱われ得るが、本稿では戸建住宅を想定している。

● スマートホーム向け IoT 機器・サービスの事業者

スマートホーム向けの IoT 機器を開発・生産・販売する事業者であり、本稿で想定するガス給湯器の遠隔操作を実現するサービスの提供にあたり、中心となって IoT 機器・システムに対して対策を実装すべき主体である。本稿ではガス給湯器の製造元を想定している。なお、スマートホーム向けにメンテナンスやサポートを行う事業者を本事業者とは分けて記載しているが、しばしば同一の事業者が担い得る。

● スマートホームを供給する事業者

IoT 機器の開発・生産自体は行わないが、IoT 機器や IoT 化された住宅設備を住まい手に対して供給・設置する事業者である。本稿ではハウスメーカーや施工業者等を想定している。

● 住まい手

スマートホームの居住者であり、主として IoT 機器を利用したサービスを受ける。本稿では、戸建住宅に設置されたガス給湯器を遠隔操作する主体となる。

● スマートホーム向けにメンテナンスやサポートを行う事業者

スマートホーム向けのサービスや IoT 機器・システムに関して、メンテナンスはじめ、設置・設定・運用などを行う事業者である。本稿では、ガス給湯器の駆け付け修理サービスなどを提供する事業者等を想定する。

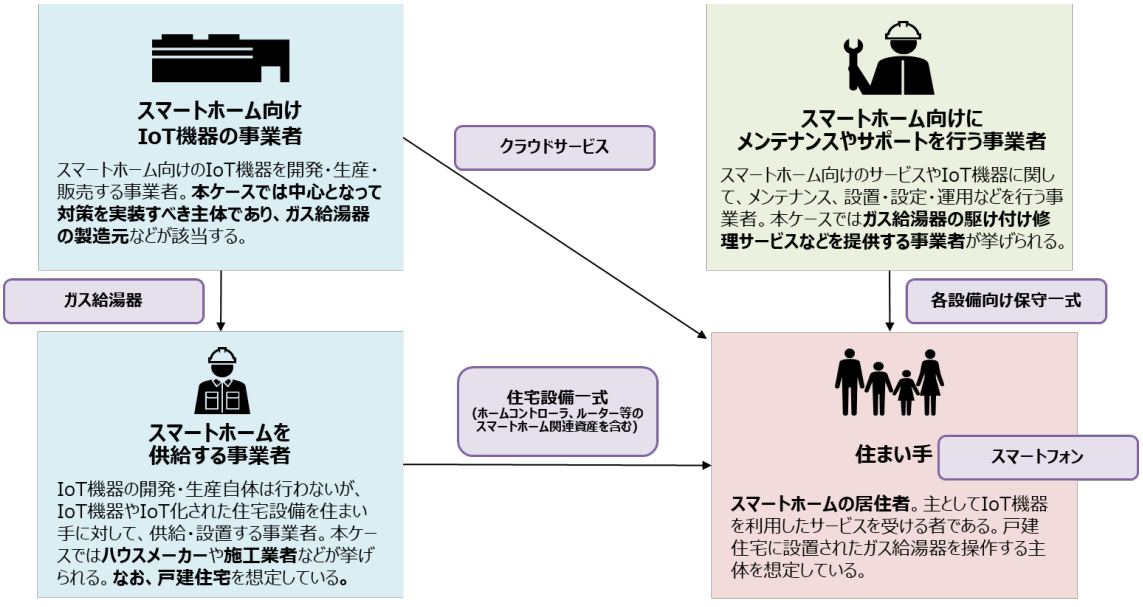

図 2 ステークホルダー関連図

③　システムを構成する機器の一覧

本稿の対象となる機器は以下の通りとする。

表 1 システムを構成する機器の一覧

システムを構成する機器	内容
ガス給湯器	ホームコントローラから指示を受けることで、自動湯沸かし等が可能となる機器。 ガス給湯器内に特定の個人に関する情報を保管しないことを想定する。
ホームコントローラ	スマートフォンから指示を受け、居内内のガス給湯器に指示を出す機器。 ガス給湯器の他にも、居内の他の IoT 家電に対する制御も実施し得ることを想定する。
ルーター	居内に設置され、居内のネットワークおよび居外のネットワークを中継する通信機器。
スマートフォン	専用のアプリケーションをインストールしたスマートフォン。 住まい手は、外出先からスマートフォン上のアプリケーションを操作してガス給湯器の遠隔操作を行う。
クラウドサービス	スマートフォンから指示を受け、インターネット回線を通じてホームコントローラに指示を出すシステム。

④　システム構成図、データフロー図

システム構成図は以下の通りとする。

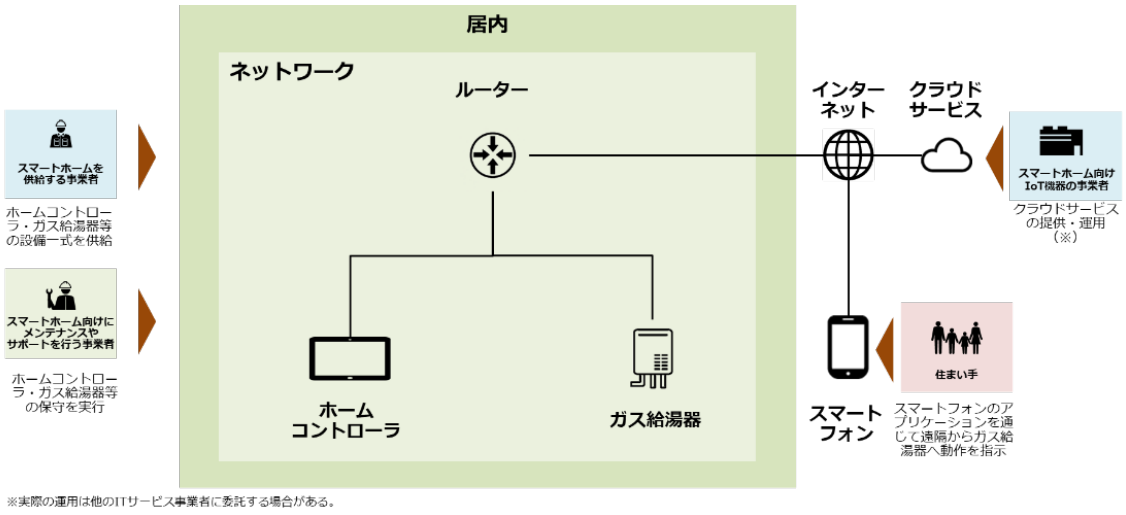

図 3 システム構成図

住まい手が外出先よりスマートフォン専用のアプリケーションを通じて、居内のガス給湯器を遠隔操作し、自動お湯張りを実施する場合のデータフローは以下の通りとする。

1. 住まい手が所有するスマートフォンからクラウドサービスに対して、操作指示を出す。
2. クラウドサービスからインターネットを通じて、ルーター経由でホームコントローラに指示を出す。
3. ホームコントローラから居内のネットワークを通じてガス給湯器に指示を出す。

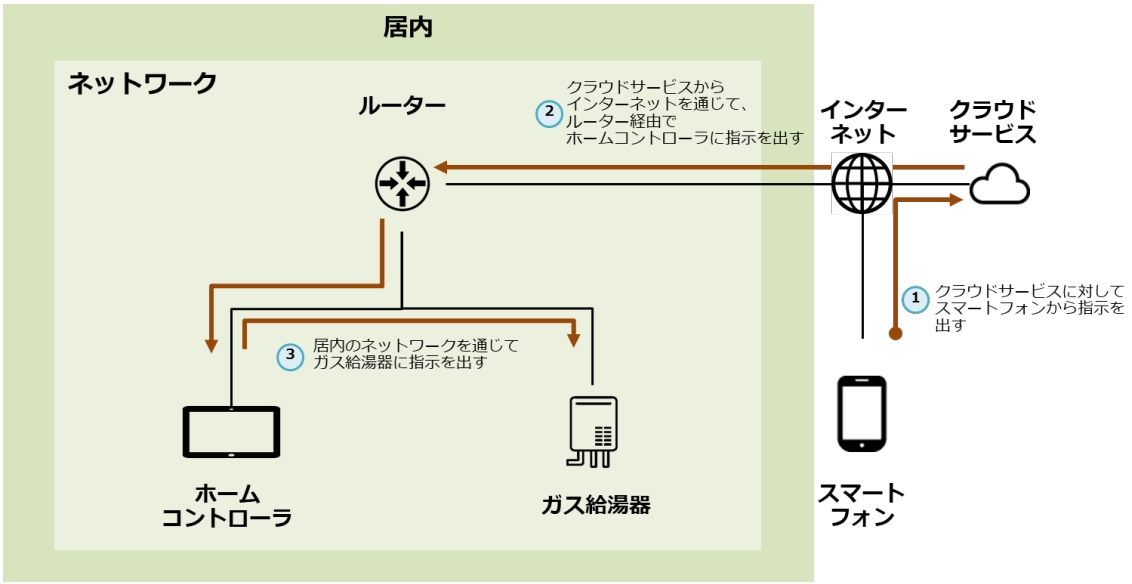

図 4 データフロー図

(2) リスク評価に係る内容

「回復困難性の度合い」及び「経済的影響の度合い」[3]から、ガス給湯器システムのリスク評価を行う。

① 発生したインシデントの影響の回復困難性の度合い

プライバシーの観点及びセーフティの観点から判断した上で、「回復困難性の度合い」の大きさを評価する。

まず、プライバシーの観点では、クラウドサービスもしくはスマートフォンにインストールされたアプリケーションから住まい手のアカウント情報やサービスの利用状況等が流出する可能性があると想定される。また、セーフティの観点では、ガス給湯器が予期せぬ動作をした際に、機器近くにいる利用者がやけど等などの軽傷、あるいはその場の状況によっては重症を負う可能性があると想定される。

プライバシーの観点では住まい手の個人情報が流出する可能性があること、セーフティの観点では状況によっては利用者が重症を負う可能性があることから、「回復困難性の度合い」のレベルは「重大なダメージ」とする。

② 発生したインシデントの経済的影響の度合い（金銭的価値への換算）

「経済的影響の度合い」は、直接的な経済影響及び間接的な経済影響から評価する。なお、直接的な経済影響は「内外への直接影響」、「直接影響の継続時間」及び「代替可能性」の観点から評価する。

「内外への直接影響（内部）」の観点では、ガス給湯器が停止することによって、住まい手による経済活動の中断等は生じ難いと想定される。

「内外への直接影響（外部）」の観点では、ガス給湯器が停止することによって、利用環境(住居)外部の経済影響に対して影響は及びにくいものと想定される。

「直接影響の継続時間」の観点では、ガス給湯器の故障等の不具合が認められた場合、修理や交換

[3] 「経済的影響の度合い」では、経済的影響に加えて、社会的及び生活的影響を考慮するものとする。

に一定の時間を要する可能性があると想定される。

「代替可能性」の観点では、停止期間中、給湯が不可能になるものの、外部のサービスを利用することで機能を代替できる場合が一般的であると想定される。

間接的な経済影響の観点では、ガス給湯器の修理や交換に一定のコストを要する可能性があるものの、それによる経済的な影響の度合いは限定的と想定される。

直接的な経済影響では、「直接影響の継続時間」の観点から影響が一定程度継続し得ることが想定されるものの、住まい手側でしばしば代替的な手段を利用可能であり、間接的な経済影響の観点も含め、「経済的影響の度合い」が大きくなりにくいと想定されることから、「経済的影響の度合い」のレベルは「限定的な経済影響」とする。

③　マッピング結果

フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいて第 1 軸「回復困難性の度合い」及び第 2 軸「経済的影響の度合い」からカテゴライズし、マッピングする。

上記を踏まえると、「回復困難性の度合い」では、特定条件下で利用者がやけど等の重症を負う可能性があると考えられる。「経済的影響の度合い」では、大規模回収等がない場合には直接的な経済影響及び間接的な経済影響ともに限定的であると考えられる。

「回復困難性の度合い」のレベルは、「重大なダメージ」であるものの、「経済的影響の度合い」では、「限定的な経済影響」となる。

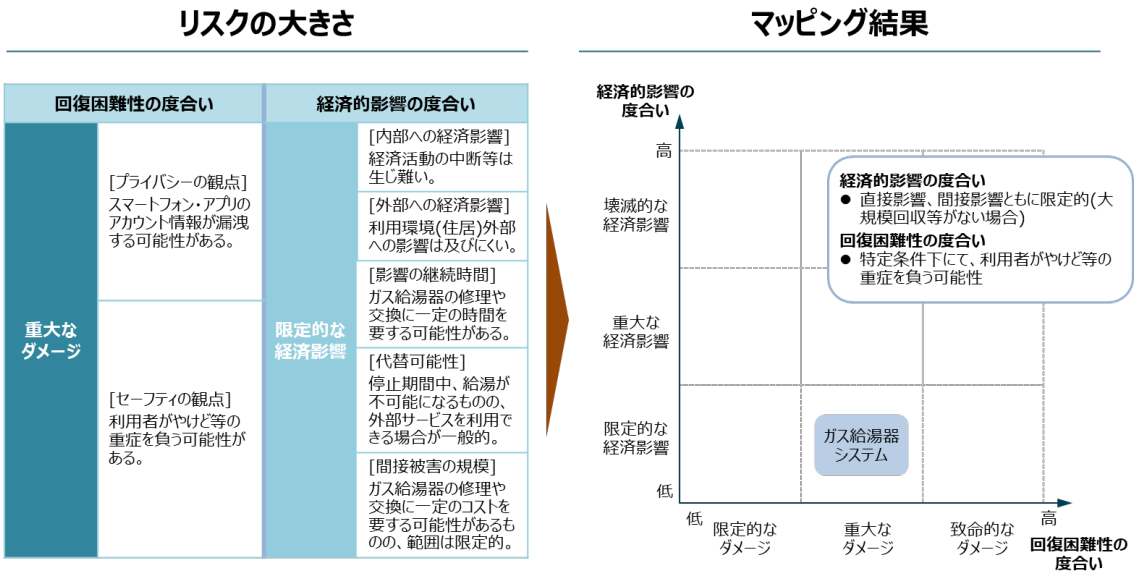

図 5 マッピング結果

(3) リスク対応に係る内容（ステークホルダー別の対策例一覧）

① システムを構成する機器ごとの脅威の整理

システムを構成する機器・システムごとに想定される脅威（例）は以下の通り。

表 2 想定される脅威（例）

システムを構成する機器	想定される脅威（例）
ガス給湯器	情報漏えい
	マルウェア感染
	不正利用
	利用者による誤操作
ホームコントローラ	マルウェア感染
	不正利用
ルーター	不正アクセス
	不正利用
スマートフォン	情報漏えい
	マルウェア感染
	不正利用
	利用者による誤操作
クラウドサービス	データの改ざん
	情報漏えい
	サービス不能
	不正アクセス
	マルウェア感染
	利用者による誤操作

② 脅威に対する対策の整理

想定される脅威を踏まえ、第 3 軸「求められるセキュリティ・セーフティ要求」における観点及び主に対策要件を実装すべき主体ごとに有効と考えられる対策要件を整理する。

表 3 ガス給湯器システムにて想定される対策要件の事例

第 3 軸	適用対象	主に対策要件を実装すべき主体	想定される脅威（例）	対策要件
第 1 の観点	ソシキ・ヒト	スマートホーム向け IoT 機器の事業者	全般[4]	IoT 機器・システムにおけるセキュリティポリシーの策定
			全般	運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
			全般	IoT セキュリティに関するステークホルダーの役割の決定
			全般	IoT 機器・システムに係る要員のセキュリティ確保
	システム	スマートホーム向け IoT 機器の事業者	全般	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
			全般	企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
			不正アクセス	適切な水準のアクセス制御の実施
			データの改ざん	搭載するソフトウェアの改ざん検知機能の実装
			情報漏えい	搭載するソフトウェアに対するインストール対策の実装
			不正アクセス	様々な IoT 機器に接続する際のセキュリティの確保
			データの改ざん 情報漏えい	暗号化によるデータの保護
			データの改ざん 情報漏えい	ライフサイクルに応じた暗号鍵の管理
			マルウェア感染	マルウェア対策の実施
			サービス不能	IoT 機器・システムの十分な可用性の確保
			データの改ざん 不正アクセス	IoT に適したネットワークの利用
			全般	セキュリティ設計と両立するセーフティ設計の仕様化
			全般	セキュアな開発環境と開発手法の適用
			全般	IoT 機器・システムにおけるセキュリティ機能の検証
			不正アクセス マルウェア感染	IoT 機器・システムの出荷時における安全な初期設定と構成
		住まい手	全般	信頼できる IoT 機器やサービスの選定
		スマートホームを供給する事業者	不正アクセス マルウェア感染	IoT 機器・システムにおける運用開始時の正しい設置、設定

[4] 「全般」は特定の脅威でなく、様々な脅威に対して共通に有効な対策であることを示す。

第 2 の観点	ソシキ・ヒト	スマートホーム向け IoT 機器の事業者	全般	利用者へのリスクの周知等の情報発信
			全般	運用中における IoT セキュリティを目的とした体制の確保
			全般	過去の対応事例からの学習
		スマートホーム向けにメンテナンスやサポートを行う事業者	全般	サービス提供や管理のポリシーの提示・遵守
	プロシージャ	スマートホーム向け IoT 機器の事業者	全般	インシデント対応手順の整備と実践
			全般	運用手順や利用手順の文書化と提示
		スマートホーム向けにメンテナンスやサポートを行う事業者	全般	サービスと IoT 機器・システムのガイドに従った保守、管理
		住まい手	不正利用 不正アクセス 誤操作	IoT 機器・システムの用途・用法を守った使用
	システム	スマートホーム向け IoT 機器の事業者	全般	運用中における法令および契約上の要求事項の遵守
			不正アクセス マルウェア感染	継続的な資産管理の実施
			全般	プログラムソースコード及び関連書類の保護
			不正利用 不正アクセス	IoT 機器・システムのモニタリング及びログの取得、分析
			全般	脆弱性対応の実施
			情報漏えい	IoT 機器・システムの安全な廃棄または再利用
第 3 の観点	ソシキ・ヒト	スマートホーム向け IoT 機器の事業者	全般	IoT 機器・システムの運用・管理を行う者への要求事項の特定
			全般	IoT 機器・システムの運用・管理を行う者への要求事項の遵守の確認

122

③　整理した対策に対する意思決定

対策等を検討する際には、インシデントによる影響の度合いだけでなく、その起こりやすさも踏まえ、システム全体としてのリスクを低減するような対策を検討する。なお、ここで優先度が必ずしも高くないとされる対策であっても、事業者のリスクに対する認識やセキュリティ対策に割けるリソース、IoT 機器の利用環境等によっては積極的に実装を検討すべき項目となる場合がある。したがって、以下に記載されていない対策についても何ら実装を妨げるものではない。

- 対策の適用対象（どの機器を中心に検討するか）

想定しているインシデントが発生した際に想定される被害の大きさ及び起こりやすさ等を考慮して、資産であるガス給湯器、ホームコントローラ、ルーター、スマートフォン・アプリ、クラウドサービス等から、特に対策を検討すべき資産を検討する。

被害の大きさという観点では、本稿で想定する環境に所在する「住まい手」以外のヒトや、居内に設置されているガス給湯器システム以外の機器・システムにも影響すると思われる以下の資産を中心として対策を検討すべきである。

- クラウドサービス、スマートフォン・アプリ
  特定の利用者だけでなく、同様のアプリケーションを利用する者全体に対して影響が波及し得る。
- ルーター、ホームコントローラ
  居内のネットワークに接続するガス給湯器システム以外の機器・システムにも被害を拡大させる恐れがある。

また、「起こりやすさ」の観点では、外部からのネットワーク経由での攻撃に対して十分に対処する必要があるため、インターネットに直接接続されている資産(例：ルーターやクラウドサービス等)を中心として対策を検討することが望ましい。

- 適用する対策の内容（どのように対策を実施するか）

対策一覧より、より効率的・効果的にリスクを低減できるものを中心として対策を検討する。具体的には、深刻とされているリスクに対してセキュリティ上、基本的かつ確実に効果が期待できる対策や、一つの対策で複数の脅威に対処できるものを実施することが望ましい。

例えば、ホームコントローラやガス給湯器等の IoT 機器を対象とする初期設定パスワードの変更、脆弱性に関する情報の公開、セキュリティアップデートに関する対策は、これらに該当するとしている例がある[5]。それらの動向も踏まえ、以下の対策については優先的に検討することが望ましい。

- IoT 機器・システムの出荷時における安全な初期設定と構成
- 利用者へのリスクの周知等の情報発信
- 脆弱性対応の実施

[5] 英国デジタル・文化・メディア・スポーツ省 ”Code of Practice for consumer IoT security”（2018 年 10 月）参照

159 ➢ 運用手順や利用手順の文書化等の運用・管理を行う者への支援の実施

160

161 上記を踏まえて、本稿で実装することとするステークホルダーごとの対策要件は以下の通りである。

162

163 ● スマートホーム向け IoT 機器の事業者

164

165 表 4 スマートホーム向け IoT 機器の事業者における実際に講じる対策要件の例

No	第 3 軸	適用対象	対策要件	実際に講じる対策の例
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定	● ガス給湯器システムを含む自社が提供する IoT 機器・システムを対象としたセキュリティポリシー（情報セキュリティ関連規定を含む）の策定及び適切な承認権限を有する者の承認 ● 定められた期間ごとの当該ポリシーのレビュー
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保	● ガス給湯器システムを対象としたセキュリティ管理責任者及びセキュリティ対策担当者の任命 ※ 上記の管理責任者及び開発担当者は、ガス給湯器システムのライフサイクルの各段階（例：開発、運用、保守）において明確化されていることが望ましい。
3			IoT セキュリティに関するステークホルダーの役割の決定	● IoT 機器・システムのセキュリティ対策の設計・開発・運用等における関係各社の責任範囲の決定 ● 運用中に発生したセキュリティインシデントにより損害が発生した場合の責任範囲（役割分担や損害賠償）の決定
4			IoT 機器・システムに係る要員のセキュリティ確保	● 委託する業務に関わる者に対するセキュリティ上の要求事項の規定（退職後も含む） ● 自社内の要員に対する適切な訓練及びセキュリティ教育の実施
5		システム	運用前（設計・製造段階）における法令および契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化	● ガス給湯器システムの企画・設計時におけるリスクアセスメントの実施、セキュリティ要件の特定、要件の実装に係る費用の確保 ● 必要なセキュリティ仕様が組み込まれているかを確認する設計レビューの実施
7			適切な水準のアクセス制御の実装	● 想定されるリスクの大きさを考慮した方式による、ユーザーや IoT 機器の認証

				● クラウド上のアプリケーションへの特権アクセスに対して、多要素認証等の強度の高い認証方式の適用認証済みのユーザーまたはアプリケーション等に対する最小権限の原則の適用 [6] ● パスワード等の認証情報の安全管理（例：ハッシュ化のうえ保管、通信経路上での保護）
8			搭載するソフトウェアの改ざん検知機能の実装	● ガス給湯器システムのソフトウェアに関する完全性の検証機能の実装
9			搭載するソフトウェアに対するインストール対策の実装	● ガス給湯器システムにインストール可能なソフトウェアの種類に関する厳密な方針の策定及び実装
10			様々な IoT 機器に接続する際のセキュリティの確保	● ガス給湯器等を他の IoT 機器等に接続する際のホワイトリストの適用 ● 識別情報を登録している機器（ガス給湯器等）によるクラウドサービスへの接続に限り許可
11			暗号化によるデータの保護	● 適切な強度の方式による通信経路（住居内及び住居外）の暗号化 ● クラウドサービス上に保管されている利用者データ等の暗号化 ※ ガス給湯器等に対して暗号化等のデータ保護措置を十分に講じることが難しい場合、当該機器に機微なデータが保管しない等の代替的な措置をとる。
12			ライフサイクルを通じた暗号鍵の管理	● 暗号鍵の利用，保護及び有効期間に関するポリシーの策定及び遵守
13			マルウェア対策の実施	● クラウドサービスにおけるマルウェア対策ソフトウェアの導入 ● ルーターにおけるマルウェア対策ソフトウェアの導入
14			IoT 機器・システムの十分な可用性の確保	● ガス給湯器システムを構成するクラウドサービス等に対する(D)DoS 攻撃を想定し、一定レベルの負荷に耐える容量を確保 ● クラウドサービスにおいて不審な通信（例：特定の IP アドレスからの大量のリクエスト）を検知し、適宜遮断等する ● アプリケーションのテスト段階における一定レベルの負荷試験の実施
15			IoT に適したネットワークの利用	● 適切な強度の暗号通信機能（例：TKIP、AES）を有した居内無線 LAN への対応
16			セキュリティ設計と両立するセーフティ設計の仕様化	● ガス給湯器の近くにいる人や機器の周辺への危害を回避するための安全機能（本質安全設計、予防安全機能 [7]等）の実装 ● ガス給湯器に実装された安全機能と外部との通信回線との分離
17			セキュアな開発環境と開発手法の適用	● セキュアコーディング手法の適用

[6] JPCERT/CC によると、最小特権の原則とは場面に応じて必要最小限の権限だけを与えるようにする原則であり、この原則を守ることで、実際にインシデントが発生した場合の被害を最小限に抑えることができるとされている。

[7] 「予防安全機能」の概要については、経済産業省「電気用品、ガス用品等製品の IoT 化等による 安全確保の在り方に関するガイドライン」の「5．予防安全機能について」を参照

				● 委託先を含む開発人員向けのセキュリティ対策、開発環境やコードへのアクセスの制御、開発環境と運用環境の分離等、安全な開発環境に必要な対応の実施 ● 設計書、プログラム、バイナリ等のバックアップ
18			IoT 機器・システムにおけるセキュリティ機能の検証	● コード分析ツール又は脆弱性スキャナのような自動化ツール等を活用したセキュリティ機能に関する検証の実施 ● クラウドサービス（アプリケーション部分）及びガス給湯器に対するペネトレーションテストの実施
19			IoT 機器・システムの出荷時における安全な初期設定と構成	● ガス給湯器システムを構成する機器の不要なネットワークポート、その他 USB やシリアルポートなどの物理的または論理的な閉塞 ● 出荷時点で明らかに不要な IoT 機器・システムが提供する機能、サービス、アプリケーション、アカウントの削除または無効化 ● 初期パスワードの変更を促す機能の実装 ● 暗号通信機能（例：TKIP、AES）を有した居内無線 LAN への接続を促すガイダンスの提供
20	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信	● スマートフォン上のアプリケーションや企業ホームページ等を通じたサポート期間終了の予告及び通知、機器・システムの重大な脆弱性、ユーザー情報の漏えいや機器のマルウェア感染等のインシデントに関する情報発信等、ガス給湯器システムに対するリスクやスマートホームを供給する事業者または住まい手で対応すべき点に関する情報提供の実施
21			運用中におけるIoTセキュリティを目的とした体制の確保	● セキュリティ管理責任者及びセキュリティ対策担当者が異動した場合の後任の選任
23			過去対応事例からの学習	● 発生したセキュリティインシデントの分析や解決から得られた知見の将来的なインシデント抑制への活用（他社の IoT 機器・システムにおけるセキュリティインシデントを含む）
24		プロシージャ	インシデント対応手順の整備	● ガス給湯器システムその他の自社が提供する IoT サービスに適応したインシデント対応手順の整備 ● 各要員の役割と責任の識別及び指定された個人によって実行されるアクションの定義・伝達 ● 事業継続上重要な機能を有する外部サービスプロバイダに対する自組織のインシデント対応手順の伝達および内容調整 ● インシデント対応手順の定期的な訓練（自組織と外部プロバイダとの間で連携を要する部分も含む） ● ※ セキュリティの観点に加え、セーフティの観点を考慮する。
25			運用手順や利用手順の文書化と提示	● 住まい手に対する、以下の内容を含むガス給湯器システムの運用手順や利用手順の作成及び提示

				- 初期設定の手順 - 提供者が想定する安全な利用方法 - 不適切な使用によって生じ得るセキュリティ関連のリスク - 不具合を発見した際の連絡先 ● 運用・管理を行う者へのガイドの作成及び提示
26		システム	運用中における法令および契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守
27			継続的な資産管理の実施	● クラウドサービスに接続するガス給湯器等に関する資産目録（機器上に実装されたソフトウェアおよびファームウェア、工場出荷時の設定等を含む）の作成・維持
28			プログラムソースコード及び関連書類の保護	● 確立した手順に従ってプログラムソースコード管理する ● 施錠可能な文書保管庫での及び関連書類（設計書、仕様書、検証計画書、妥当性確認計画書）の保護の管理
29			IoT 機器・システムのモニタリング及びログの取得、分析	● ガス給湯器システムを構成するクラウドサービスやスマートフォン上のアプリケーションを対象にした各種ログ（例：ユーザー認証、ネットワークトラフィック）の取得及び保護 ● 取得したログの安全な入手 ● 取得したログの定期的な分析及び異常の検知
30			脆弱性対応の実施	● 新たに検知されたクラウドサービス、スマートフォン上のアプリケーション及びガス給湯器に係る脅威や脆弱性の報告窓口の設置 ● 報告された脅威及び脆弱性によって影響を受け得る範囲（例：機器及びその構成要素）の特定 ● 開発委託先等への修正プログラム等開発の依頼 ● スマートホーム向けにメンテナンスやサポートを行う事業者へのセキュリティパッチの提供
31			IoT 機器・システムの安全な廃棄または再利用	● ガス給湯器システムを構成する機器（例：クラウドサーバーやホームコントローラ）内部に保存されている情報の削除（読み取り不可処理を含む）
32	第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者への要求事項の特定	● 以下の内容を含む、住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の明確化 - 使用条件 - 使用上のリスク・注意点 - 使用上のリスク・注意点、異常通知があった場合に取るべき対応（手元操作の優先、近くにいる使用者による通信回線切り離し） - ソフトウェアアップデート時の注意事項
33			IoT 機器・システムの運用・管理を行う者に対す	● 明確化した住まい手に能動的な行動を促すためのスマートホーム向けにメンテナンスやサポートを行う事業者への要求事項の遵守の確認

			る要求事項の遵守の確認	● ソフトウェアアップデート時の注意事項の遵守の確認

166

167 ● スマートホームを供給する事業者

168

169 表 5 スマートホームを供給する事業者における実際に講じる対策の例

No	第 3 軸	適用対象	対策要件	実際に講じる対策例
1	第 1 の観点	システム	IoT 機器・システムにおける運用開始時の正しい設置、設定	● IoT 機器の事業者から提供されたガイドに従った設置、設定 ● IoT 機器の事業者の想定する仕様に適合したネットワーク環境の整備

170

171 ● スマートホーム向けにメンテナンスやサポートを行う事業者

172

173 表 6 スマートホーム向けにメンテナンスやサポートを行う事業者における実際に講じる対策の例

No	第 3 軸	適用対象	対策要件	実際に講じる対策例
1	第 2 の観点	ソシキ・ヒト	サービス提供や管理のポリシーの提示・遵守	● ガス給湯器システムを対象としたサービス提供や管理のポリシー提示及び遵守 ● セキュリティパッチの適用手順の提示
2		プロシージャ	サービスと IoT 機器・システムのガイドに従った保守、管理	● スマートホーム向け IoT 機器の事業者が提示するガイドに従った保守、管理

174

175 ● 住まい手

176

177 表 7 住まい手における実際に講じる対策の例

No	第 3 軸	適用対象	対策要件	実際に講じる対策例
1	第 1 の観点	システム	信頼できる IoT 機器やサービスの選定	● 個人情報を含む様々なデータ管理などのポリシーやセキュリティ対策に留意した上で、適切なガス給湯器及びクラウドサービスの選択
2	第 2 の観点	プロシージャ	IoT 機器・システムの用途・用法を守った使用	● 仕様書や手順書を把握し、想定された用途・方法でのガス給湯器の使用
3		システム	法的及び契約上の要求事項の遵守	● 情報セキュリティに関連する法的、規制（例：製品安全関連法）又は契約上の義務に対する違反を避けるための要求事項の遵守

178

添付 A　対策要件

「IoT セキュリティ・セーフティ・フレームワーク」の第 3 軸「求められるセキュリティ・セーフティ要求」における 4 つの観点を参照しつつ、有効と考えられる対策要件を以下に整理する。

対策要件の適用対象は、「ソシキ・ヒト」、「プロシージャ」及び「システム」に分けられる。

「ソシキ・ヒト」には、「バリュークリエーションプロセスに参加する組織・団体・組織」や「その組織に属する人及び価値創造過程に直接参加する人」のセキュリティ向上を目的とした非技術的な対策要件（例：セキュリティ対応組織の設置や関連するポリシーの策定等）が該当する。

「プロシージャ」には、セキュリティ能力の向上を目的として、「目的を達成するための一連の活動の手続き」を定めた非技術的な対策要件（例：脆弱性対応に必要な手順等の整備と実践等）が該当する。

「システム」には、「目的を実現するためにモノで構成される仕組み・インフラ」のセキュリティ能力の向上を目的とした技術的な対策要件が該当する。

「システム」に該当する対策要件は、IoT 機器・システムにて一般的に想定されるライフサイクルの段階の順で示す。

例えば、第 1 の観点は以下の段階の順で示す。

- 企画・設計（例：企画・設計段階におけるセキュリティ要求事項の分析及び仕様化）
- 開発（例：適切な水準のアクセス制御の実装）
- 試験（例：IoT 機器・システムにおけるセキュリティ機能の検証）
- 設置（例：IoT 機器・システムにおける運用開始時の正しい設置、設定）

第 2 の観点は、以下の段階の順で示す。

- 運用（例：継続的な資産管理の実施）
- 廃棄（例：IoT 機器・システムの安全な廃棄または再利用）

表 A-1 対策要件の例

No	第 3 軸	適用対象	対策要件
1	第 1 の観点	ソシキ・ヒト	IoT 機器・システムにおけるセキュリティポリシーの策定
2			運用前（設計・製造段階）における IoT セキュリティを目的とした体制の確保
3			IoT セキュリティに関するステークホルダーの役割の決定
4			IoT 機器・システムに係る要員のセキュリティ確保
5		システム	運用前（設計・製造段階）における法令および契約上の要求事項の遵守
6			企画・設計段階におけるセキュリティ要求事項の分析及び仕様化
7			適切な水準のアクセス制御の実装
8			搭載するソフトウェアの改ざん検知機能の実装
9			搭載するソフトウェアに対するインストール対策の実装
10			様々な IoT 機器に接続する際のセキュリティの確保
11			暗号化によるデータの保護

12			ライフサイクルを通じた暗号鍵の管理
13			マルウェア対策の実施
14			IoT 機器・システムの十分な可用性の確保
15			IoT に適したネットワークの利用
16			適切なネットワークの分離
17			IoT 機器・システムの設置場所等に対する物理的アクセスの制御
18			IoT 機器システムの構成要素（機器、ネットワーク等）の物理的保護
19			セキュリティ設計と両立するセーフティ設計の仕様化
20			セキュアな開発環境と開発手法の適用
21			IoT 機器・システムにおけるセキュリティ機能の検証
22			信頼できる IoT 機器やサービスの選定
23			IoT 機器・システムの出荷時における安全な初期設定と構成
24			IoT 機器・システムにおける運用開始時の正しい設置、設定
25	第 2 の観点	ソシキ・ヒト	利用者へのリスクの周知等の情報発信
26			サービス提供や管理のポリシーの提示・遵守
27			運用中における IoT セキュリティを目的とした体制の確保
28			過去の対応事例からの学習
29		プロシージャ	脆弱性対応に必要な手順等の整備と実践
30			インシデント対応手順の整備と実践
31			事業継続計画の策定と実践
32			運用手順や利用手順の文書化と提示
33			サービスと IoT 機器・システムのガイドに従った保守、管理
34			IoT 機器・システムの用途・用法を守った使用
35		システム	運用中における法令および契約上の要求事項の遵守
36			継続的な資産管理の実施
37			プログラムソースコード及び関連書類の保護
38			IoT 機器・システムのモニタリング及びログの取得、分析
39			脆弱性対応の実施
40			IoT 機器・システムの安全な廃棄または再利用
41	第 3 の観点	ソシキ・ヒト	IoT 機器・システムの運用・管理を行う者に対する要求事項の特定
42			IoT 機器・システムの運用・管理を行う者に対する要求事項の遵守の確認
43	第 4 の観点	ソシキ・ヒト	賠償等の対処を実施することが容易ではないケース等における 社会的なセーフティネットの構築

204