CIAJ セキュリティ Information

経済産業省　発刊　「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」のご紹介

2021 年 11 月 4 日

CIAJ 通信ネットワーク機器セキュリティ委員会

はじめに

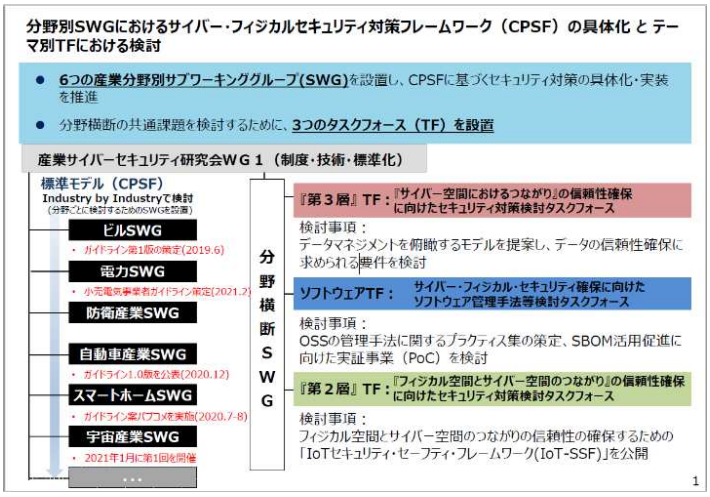
現在、様々な産業分野において IoT 機器や関連システムの開発が進んでいます。しかし、安全安心の基準が異なるシステムが相互接続することで、当初は想定していなかったリスクが顕在化することも懸念されています。

経済産業省産業サイバーセキュリティ研究会ワーキンググループ 1(制度・技術・標準化)は一般社団法人電子情報技術産業協会(JEITA)スマートホーム部会と連係して、2021 年 4 月、「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」（以下、「本書」といいます）を公開しました。

本書は、JEITA スマートホーム部会傘下のスマートホームサイバーセキュリティ WG で作成されましたが、本 WG に CIAJ も委員として参加し、本書の公開に関わりましたので、本書の内容について紹介いたします。

本書の位置づけ

経済産業省では、「Society5.0」、「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策について議論を進め、サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)を策定しました。守るべきものやリスクは産業分野によって違いがあり、各産業分野の特性に応じたセキュリティ対策の検討が必要です。本書は、スマートホーム分野におけるセキュリティ対策の考え方や、各ステークホルダーが考慮すべき対策について規定したガイドラインです。



出典：経産省・産業サイバーセキュリティ研究会 第 8 回 WG1 会合 資料 5（2021 年 3 月 15 日）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/008_05_00.pdf

本書の対象、及び対象者

本書では対象を戸建て住宅や共同住宅等の住宅として、対象者（ステークホルダー）を以下としています。

(1) スマートホーム向け IoT 機器の事業者
(2) スマートホーム向け IoT 機器を遠隔から管理する事業者
(3) スマートホーム向けサービス事業者
(4) スマートホームを供給する事業者
(5) 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
(6) スマートホーム化された分譲共同住宅・団地の管理組合や管理受託会社
(7) スマートホーム化された賃貸住宅の所有者や管理受託会社
(8) スマートホームの住まい手

また、スマートホームを「子育て世代、高齢者、単身者など、様々なライフスタイル／ニーズにあったサービスを IoT により実現する新しい暮らし」を実現するものであるとして、IoT に対応した住宅設備・家電機器などが、サービスと連係することにより、住まい手や住まい手の関係者に便益が提供される住宅を、本書の対象であるスマートホームとして独自に定義しています。

セキュリティ対策の検討の考え方

本書は、以下の段階を踏んで、各ステークホルダーに対するセキュリティ対策のガイドを導出しています。

(1) スマートホームのセキュリティ上の脅威や想定されるインシデント、関連する脆弱性を検討するための想定シーンと脅威を設定
(2) 想定されるインシデント、リスク源（脅威、脆弱性）を抽出
(3) 対策要件について対策例を示すと共に、対策例を他の標準や規格と対比
(4) 対象となるステークホルダー毎に対策要件を整理・要約し、各ステークホルダーに必要な対策のガイドを導出
(5) 導出したセキュリティ対策に対し、補足説明を加えて、ガイドライン文書として整理

スマートホームにおけるセキュリティ上の脅威

本書では、主として住まい手に影響を及ぼすリスク源を抽出することを念頭に想定シーンと脅威を設定しています。

なお、本書では、想定シーンを大きく２つの観点で示しています。一つはスマートホームとサイバー空間との間のデータに関する脅威、もう一つは、物理的なモノを含めた管理上の脅威としています。

＜スマートホームとサイバー空間との間のデータに関する脅威の例＞

- IoT 機器が攻撃を受け、センサでの測定ができない／デジタル情報への変換ができない／データをサイバー空間に送る機能が正しく動作しない。

・　サイバー空間から受け取る通信データが、通信経路において改ざん／暴露される。

＜物理的なモノを含めた管理上の威の例＞

・　共同住宅に新規に設置する IoT 機器が想定された用途・用法に基づき設定されないため、住戸内ネットワークに接続されている既存の IoT 機器に干渉する。
・　転居や販売・譲渡の際に、新たな利用者が前の利用者の個人情報が残存した状態で、IoT 機器やサービスを利用し続けてしまう。

スマートホームに求められる最低限のセキュリティ対策

各ステークホルダーに必要となるセキュリティ対策を示しています。

また、章立てをステークホルダー毎とし、セキュリティ対策１つ１つに詳細、かつ分かりやすい解説を加えています。そのため、読者に必要な章を分かりやすく示しています。

具体的には、以下が挙げられます。

・スマートホーム向け IoT 機器の事業者

（対策例）IoT 機器は出荷時や初期状態からセキュリティを確保する。

・スマートホーム向けのサービス事業者

（対策例）サービスを提供する事業者のシステムを適切に運用・管理する。

・スマートホームを供給する事業者

（対策例）IoT 機器を正しく選定する。

おわりに

スマートホームの安全安心のためには、各ステークホルダーに必要なセキュリティ対策が必要で、そのためにはセキュリティ上の脅威を理解し、その脅威にあった対策を理解して実施することが大切です。本書は読者が理解しやすいような章立てで、分かりやすく解説しているため、ステークホルダーの皆様に是非ご活用いただければと思います。

また、本書を分かりやすく解説した普及パンフレットも合わせて公開されているので、こちらも、活用いただければと思います。

出典：サイバーセキュリティ ｜JEITA スマートホーム部会
https://home.jeita.or.jp/smarthome/security/

著者

CIAJ 通信ネットワーク機器セキュリティ委員会

【参考文献】

・スマートホームの安心・安全に向けた
サイバー・フィジカル・セキュリティ対策ガイドライン

・経済産業省

https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html

・JEITA

https://home.jeita.or.jp/smarthome/security/