製品分野別セキュリティガイドライン
スマートホーム編

Ver. 0.1

CCDS セキュリティガイドライン WG

スマートホーム SWG

改訂履歴

版数	改訂日	改訂内容
Ver.0.1	2018/11/26	新規発行

■商標について

・本書に記載の会社名、製品名などは、各社の商標または登録商標です。

■おことわり

・本書に記載されている内容は発行時点のものであり、予告なく変更することがあります。

・本書の内容を CCDS の許可なく複製・転載することを禁止します。

目次

1 はじめに

これまで製品業界ごとにセーフティ標準は策定されてきた。一方、サイバーセキュリティ標準をみると、組織運営に関する標準（ISO27001）と製品設計のセキュリティ評価・認証に関する標準（ISO15408）が策定されており、近年では、重要インフラストラクチャー（社会インフラに欠かせないプラントや施設）の制御システムを対象とした標準（IEC62443）も策定されている状況である。

Internet of Things（以下、IoT） の普及に伴い、身の回りにある生活機器が様々なネットワーク接続機能をもつことで、製品のセキュリティ懸念は増しているが、IoT 製品やサービスには欠かせないセキュリティ標準が生活機器に対しては未整備の状況である。欧米の動きをみると、各業界のセーフティ標準からセキュリティ標準を検討する動きが各所にみられる。一方、日本においてもセキュリティに関する懸念は顕在化しており、検討すべき、という声は多いが、具体的検討に入っている分野はまだ少ない状況となっている。

このような状況の中で、一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）は設立された。本協議会では、生活機器セキュリティ標準の策定と、その標準に沿っていることを確認・検証した認証プログラムをセットにすることで、ユーザに安心して IoT 製品を使ってもらえる環境を整備することを目標に活動を行っている。

平成 28 年 7 月 5 日には IoT 推進コンソーシアム、経済産業省、総務省が「IoT セキュリティガイドライン」[1]として策定し、分野全体をカバーする共通事項を中心にまとめられた基本的な指針となっているが、CCDS では個々の製品分野において、具体的にセキュリティをカバーした設計・開発を進めるために、本分野別ガイドラインを策定した。

「IoT セキュリティガイドライン」については、下記 URL のリンク先を参照。
http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html

1.1 スマートホームのセキュリティの現状と課題

スマートホームとは、インターネットに接続され、IoT に対応した住設・家電機器が設置された住宅であり、IoT・AI などの情報技術を活用して、居住者により安全・安心で快適な生活を提供する住まいである。

IoT 機器は、私達により身近なものになり、多種多様な方面で広がりを見せている。例えば家庭内に設置した住宅設備機器を遠隔で操作することを可能にすれば、家の施錠やシャッターの開閉、水回りの設備などをコントロールすることができる。IoT 機器の普及

は著しく、今後はさらに増加すると想定されている。平成 28 年版情報通信白書[2]には、IHI Technology による推定を引用して、2015 年には世界で 約 54 億台であったコンシューマー向け IoT 機器が、2020 年には 2 倍以上の 125 億台になるとの予測が記載されている。

これらの IoT 機器は、インターネットに接続されていることで、様々なサービスの提供が可能であるが、同時に、情報セキュリティの脅威にさらされている。IoT 機器を標的としたマルウェアの存在も確認されており、その脅威は、生命や財産を脅かすものとなる可能性があることが危惧されている。

IoT 機器が攻撃を受ける要因は、利用者と提供者の二つの側面からみることができる。利用者に起因するものとしては、IoT 機器の初期設定での使用や、推測されやすいパスワードの設定、セキュリティへの知識不足などが挙げられる。提供者に起因するものとしては、初期設定で誰でもアクセスできてしまう設計や、利用者のセキュリティへの知識不足の想定が不十分であることなどである。

IoT 機器については、平成 28 年 3 月に独立行政法人情報処理推進機構による「つながる世界の開発指針」[3]が公開され、IoT 機器の開発者が開発時に考慮すべきリスク・対策を指針として明確化された。また、平成 28 年 7 月には経済産業省及び総務省らによる「IoT セキュリティガイドライン」が公開され、IoT 機器やシステム、サービスのセキュリティ対策を検討するための考え方について提供者及び利用者を対象に提示された。例えば、IoT 機器の出荷後もセキュリティ上重要なアップデートを適切に実施することが挙げられている。

そして、CCDS が、ATM・IoT GW・車載器・オープン POS などの製品を横断したセキュリティ認証制度である IoT 機器向け共通認証スキーム（以下、共通認証スキーム）を準備中である。共通認証スキームでは、IoT 機器として満たすべき最低限のセキュリティ要件である認証レベル１と、製品分野ごとに業界団体によって定義される認証レベル２・３が定義されていて、自主評価と第三者認証によってセキュリティ要件を満たすことが確認された製品・サービスについて、認証レベル１には共通認証マーク★、認証レベル２・３には業界認証マーク★★・★★★が付与される仕組みの予定である。

このように IoT 機器が普及する一方、スマートホームはまだ黎明期で、住宅会社での取り組みも本格化しはじめた段階である。スマートホームのセキュリティもガイドライン策定には至っておらず、実証事業を通した検討がされてきた段階である。

例えば、平成 28 年度には総務省の IoT サービス創出支援事業として「スマートホームを想定した連携 IoT 機器のセキュリティ検証用テストベッドの構築」が実施された。同事業では、スマートホームのテストベッド環境を構築して、日常生活で使用する IoT 機器の

セキュリティ上の安全性を検証する実証事業が行われた。その結果を踏まえて、スマートホームにおける IoT セキュリティ検証ガイドラインが策定されている。また、平成 29 年度には、経済産業省による「平成 28 年度補正 ＩｏＴを活用した社会システム整備事業（スマートホームに関するデータ活用環境整備推進事業)」が実施された。同事業では、実証実験の結果を踏まえて、スマートホーム分野のセキュリティ・製品安全対策指針（チェックリスト）が策定されている。

スマートホームのセキュリティガイドラインの策定に当たっては、IoT 機器がどのような文脈で利用されるかを踏まえる必要がある。例えば、住宅とその居住者の生命・財産を守るための IoT 機器と、快適さ・便利さを改善するための IoT 機器は、それぞれの IoT 機器と、それを操作するシステムに求められるセキュリティ要件が異なるはずである。しかし、前述の通り、住宅内に設置される IoT 機器は増加しているが、生命・財産に関わる領域にもセキュリティ要件を十分に検討せずに導入される場合も見られる。このため、CCDS 共通認証スキームの認証レベル 2 および 3 について、スマートホーム製品・サービス分野では、保護すべき対象の重要度に応じてセキュリティ要件を策定して、それを満たす製品・サービスに業界認証マーク★★・★★★を付与すべきである。住宅会社および居住者は、導入する IoT 機器の業界認証マークを確認することで、利用目的に適切であるか判断することができる。

本書では、スマートホームの構成要素・ライフサイクルを踏まえて、想定されるセキュリティ上の脅威とその対策をガイドラインとしてまとめる。

1.2　ガイドラインの対象範囲

本書は、住宅（オフィス・施設・店舗などを除く個人向けの戸建て住宅・賃貸住宅・集合住宅を指す）、住設機器を対象とし、スマートホームの設計、開発、運用に際して考慮すべきセキュリティの重要ポイントについて記載する。

1.3　本書の対象者

本書は、スマートホームの企画、設計、施工、運用に関わる企業の開発者を主な対象とし、スマートホームにおいて適切なセキュリティ対策を実施するための、設計から施工後までに考慮すべき設計・開発プロセスをガイドラインとしてまとめたものである。

本書の主な対象は、以下である。

1）住設機器の設計者、開発者、生産者、提供者

2）住設機器の運用保守を行う運用担当者

3）スマートホームの設計者、生産・施工者、監理者、現場監督者

4）スマートホームの運用保守を行う運用担当者

1.4　用語・略称

本書で使用されている用語について説明する。

表 1-1 用語一覧

用語	説明
住宅	人が住むための家。住居。すまい。本書ではオフィス、施設、店舗を除く、一般世帯向けの戸建て住宅、集合住宅、賃貸住宅等を指す。
住宅会社	住宅を企画、販売、設計、施工する会社。ハウスメーカー、工務店、ビルダー、設計事務所など。本書では、スマートホームの企画、販売、設計、施工、運用のいずれかを行う会社を指す。
スマートホーム	インターネットと接続され、IoT に対応した住宅設備・家電機器が設置された住宅。
住宅設備	住宅を構成する、または付随する設備。本書ではインターネットとつながる住宅設備を指す。住設と略記する場合もある。
セキュリティゲートウェイ	スマートホームに設置される通信機器。宅内の住設・家電機器をクラウドから安全に制御する。外部のクラウドとセキュアに接続（例えば、VPN 接続）される。
機器メーカークラウド	住設機器、家電メーカーが自社製品の管理・制御のために提供するクラウド。外部（例えば、第三者）に対し、対象機器の機能や情報へアクセスする API を提供する場合が多い。
現場監督	住宅の施工現場で、作業を指揮、監督すること。また、その人。
監理者	設計図通りに建物ができるよう、工事を指導・監督する人。
HEMS	Home Energy Management System。情報技術を活用して、一般家庭における家電などのエネルギー消費の見える化・効率化を図る管理システム。
エントリーポイント	スマートホームのサービス、IoT 機器、および通信経路において、外部からアクセス可能でセキュリティ上の脅威となりうる箇所。

ユーザーインターフェース	居住者とスマートホームの間で情報をやり取りするための仕組み。スマートフォンのような画面表示と手入力によるものや、スマートスピーカーのような音声発話・認識によるものなど多様な方法がある。
デバイス	スマートホームに設置された住設機器・家電機器・センサーなどの IoT 機器。

本書で使用されている略称について説明する。

表 1-2 略称一覧

略称	名称
API	Application Program Interface
CCDS	Connected Consumer Device Security council
CPU	Central Processing Unit
CVSS	Common Vulnerability Scoring System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
HEMS	Home Energy Management System
IEC	International Electrotechnical Commission
I/F	Interface
IoT	Internet of Things
IoT-GW	Internet of Things-Gateway
IP	Internet Protocol
IPA	Information-technology Promotion Agency
ISO	International Organization for Standardization
LAN	Local Area Network
OTA	Online Trust Alliance
OWASP	The Open Web Application Security Project
VPN	Virtual Private Network
WG	Working Group
Wi-Fi	Wireless Fidelity

2　スマートホームのシステム構成

スマートホームの基本的なシステムモデルを図 2-1 に示す。本モデルの検討では「ＩｏＴ開発におけるセキュリティ設計の手引き」の P55「図 5-3 スマートハウスの脅威と対策の検討例」を参考にした。

スマートホームに設置された機器を活用した居住者の生活を向上させるサービスを提供するために、その基盤となるスマートホーム情報基盤が構築される。スマートホーム情報基盤は、収集・蓄積したスマートホームや居住者の情報に応じて、宅内の機器を操作してサービスを実現する。機器の操作は、居住者が宅内・宅外から行ったり、提供されるサービスによってはサービス提供事業者などの第三者が遠隔で操作したりする場合もある。

スマートホーム情報基盤からの機器の操作は、機器メーカークラウドから提供される API を利用する場合や、スマートホーム情報基盤から直接行う場合がある。後者の直接操作は、宅内ネットワークに接続された HEMS コントローラやエッジサーバを経由して行うため、スマートホーム情報基盤と宅内ネットワークをネットワークで接続する必要がある。特に生命・財産に関わる機器を操作する場合は、より安心・安全に機器を操作できるよう、宅内にセキュリティゲートウェイを設置して、スマートホーム情報基盤との通信をセキュアにする（例えば、VPN で接続する）。

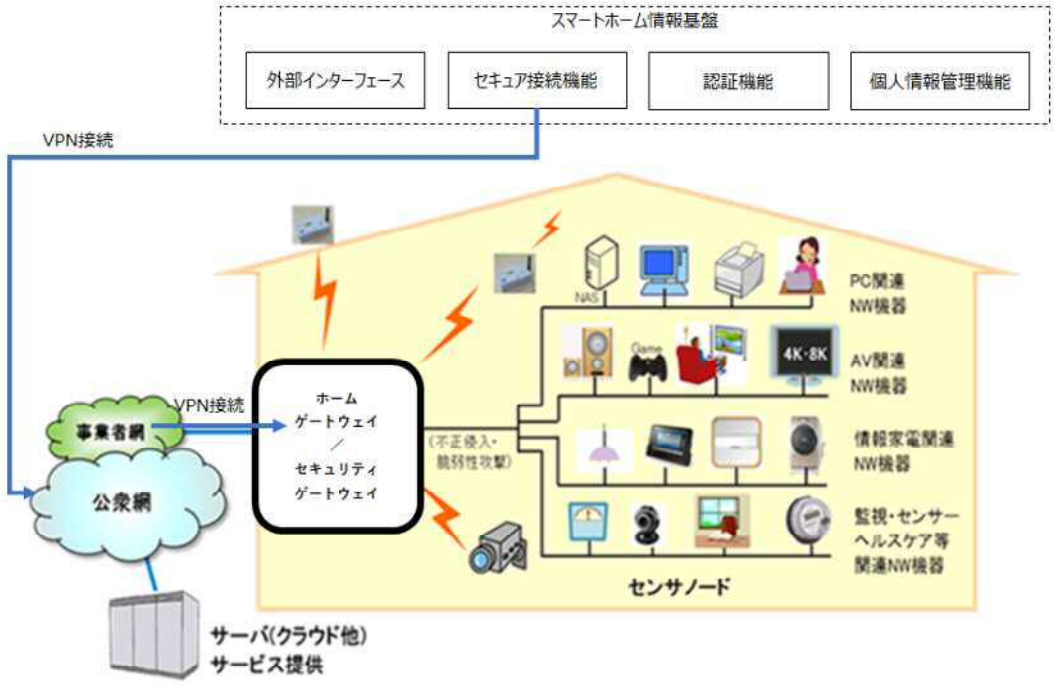

図 2-1 スマートホームのシステムモデル図

システムモデルの構成要素の説明を表 2-1 にまとめる。

表 2-1 システムモデル中の構成要素

名称	説明
■スマートホーム情報基盤	
外部インタフェース機能	スマートホームの居住者や外部のサービス提供事業者に宅内機器の利用手段を提供する。機器メーカークラウドやエッジサーバを経由して、住設・家電機器の情報取得・制御を行う。
セキュア接続機能	スマートホーム宅内に設置された住設・家電機器を安全に制御するために、宅内設置のセキュリティゲートウェイと例えば VPN で接続する。
認証機能	スマートホーム情報基盤の利用にあたり居住者の認証を行う。
個人情報管理機能	スマートホーム情報基盤を利用する居住者のユーザ情報を管理する。
■宅内設備	
Wi-Fi ルータ	インターネットと接続するルータ。Wi-Fi による接続を機器に提供する。
セキュリティゲートウェイ	インターネットと住設・家電機器の間に設置され、機器のセキュリティを担保する。
ユーザーインターフェース（UI）端末 ・スマートフォン、スマートスピーカー等	アプリケーション表示や音声発話・認識で、機器の状態確認や制御、サービスの利用を行う。
住宅設備機器（住設機器）	住宅に設置される照明設備・給湯設備・空調設備などの設備機器。
家電機器	一般家庭に設置されるテレビ・パソコン・冷蔵庫・洗濯機などの電気機器。
センサー類	住宅の温度・湿度・人感などのセンサーおよびカメラなどの機器。

3 想定されるセキュリティ上の脅威と対策

本章では、保護すべき資産とそれへの脅威を踏まえて、スマートホームの IoT 機器・サービスへのセキュリティ要件を検討する。

スマートホームには、住設・家電機器やセンサーなどの IoT 機器だけでなく、スマートフォン端末や近年に利用が拡大したスマートスピーカーなどのユーザーインターフェースなど、様々な機器が存在する。また、これらの機器を管理して連携させる外部のクラウドの存在も忘れてはならない。このようなスマートホームの特徴を踏まえたセキュリティ要件も合わせて検討する。

3.1 スマートホームの保護すべき資産、考慮すべき影響

スマートホームに設置された IoT 機器の操作は、その状況によっては生命・財産に危害を及ぼす場合が考えられる。例えば、給湯器の温度設定やエアコンの温度設定を、脆弱性を悪用して、居住者による操作結果が改ざんされたり、第三者によって不正に操作されたりした場合、居住者の生命が危険な状態に置かれる結果を招くことになる。そこで、保護すべき資産の重要度に応じてスマートホーム向け製品・サービスを分類して、それへの脅威の分析、およびその脅威から守るためのセキュリティ要件を検討する。

スマートホーム向け製品・サービスの分類を、図 3-1 に示す。

図 3-1 スマートホーム向け製品・サービスの分類

また、それぞれの分類の定義を表 3-1 に示す。

表 3-1 スマートホーム向け製品・サービスの分類

分類	要件	説明
★	インターネットにつながる製品・サービス	センサーや、見える化機器などでインターネットにつながるのみで、機能を伴わないもの。機器単体の認証、PASS 等の機能を有するが、個人認証までは行わない。
★★	スマートホームに対して、快適、便利に寄与する機能や制御を伴うもの。	個人認証等、個人情報を利用したサービスを有するもの。インターネットや通電が遮断された際に、フィジカルに稼働できるようフェイルセーフ機能が備わったもの。
★★★	快適、便利機能を持続的に利用でき、生命や財産に対し、対応を講じられたもの。	インターネットや通電が遮断された際に、フィジカルかつ、デジタル的に継続稼働ができるような対策を講じられたもの。

これらの製品・サービスに対して、関係する IoT 機器・システム・サービス（エントリーポイント）ごとのセキュリティ要件を策定する。

まず、快適・便利さに関わる★★では、個人情報を利用することから、利用者の認証が求められる。またスマートホーム情報基盤・認証基盤（スマートホーム情報基盤に含まれる場合もある)・機器メーカークラウドが連携することから、それぞれにおいてクラウドセキュリティ対策を取ることが求められる。アプリの運用に関わるクラウドが存在する場合、当該クラウドでもクラウドセキュリティ対策が必要である。

一方、生命や財産に関わる★★★では、より安全にデバイスを制御するために、外部のクラウドからスマートホームに設置されたセキュリティゲートウェイを経由して通信が行われ、機器メーカークラウドを経由しない。ただし、スマートホーム情報基盤・認証基盤でクラウドセキュリティ対策を取る必要がある。また、システム全体として操作ログを記録する必要がある。

上記を踏まえて策定されたスマートホーム向け製品・サービス★★・★★★のセキュリティ要件を表 3-2、表 3-3 に示す。これらのセキュリティ要件を満たす製品・サービスに、CCDS 共通認証スキームのスマートホーム向け製品・サービスの業界認証マーク★★・★★★が付与される。

表 3-2 スマートホーム向け製品・サービス★★のセキュリティ要件

対象	想定されるエントリーポイント	脅威	セキュリティ要件
快適さ・便利さを向上する製品・サービス	アプリ	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	スマートホーム情報基盤	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	認証基盤	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	機器メーカークラウド	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	宅内コントローラ ・HEMS コントローラ等	・不正アクセス ・なりすまし ・情報漏洩	① 利用者の認証を行うこと。 ② 施工時に接続先が信頼できることを担保すること。 ③ 宅内コントローラが調達要件（表 3-4）を満たすこと。
	通信機能を搭載した末端デバイス	・不正アクセス ・情報漏洩	① 施工時に接続先が信頼できることを担保すること。 ② 末端デバイスが調達要件（表 3-5）を満たすこと。

表 3-3 スマートホーム向け製品・サービス★★★のセキュリティ要件

対象	エントリーポイント	脅威	セキュリティ要件
生命・財産に関わる製品・サービス	アプリ	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	スマートホーム情報基盤（セキュリティゲートウェイを含む）	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② 操作ログを記録すること。 ③ クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化） ④ セキュリティゲートウェイが調達要件（表 3-6）を満たすこと。
	認証基盤	・不正アクセス ・情報漏洩 ・盗聴・改ざん	① 利用者の認証を行うこと。 ② 操作ログを記録すること。 ③ クラウドセキュリティ対策をとること（データの暗号化・通信の暗号化）
	宅内コントローラ ・HEMS コントローラ等	・不正アクセス ・なりすまし ・情報漏洩	① 利用者の認証を行うこと。 ② 操作ログを記録すること。 ③ 施工時に接続先が信頼できることを担保すること。 ④ 宅内コントローラが調達要件（表 3-4）を満たすこと。
	通信機能を搭載した末端デバイス	・不正アクセス ・情報漏洩	① 利用者の認証を行うこと。 ② 操作ログを記録すること。ただし、システムとして記録されていればこの限りではない。 ③ 施工時に接続先が信頼できることを担保すること。 ④ 末端デバイスが調達要件（表 3-5）を満たすこと。

セキュリティ要件で参照された調達要件は以下の通りである。

表 3-4 宅内コントローラの調達要件

No.	要件	対策の内容
1	共通認証マーク★の取得	機器が CCDS の共通認証マーク★を取得していること。
2	整理中	

表 3-5 末端デバイスの調達要件

No.	要件	対策の内容
1	共通認証マーク★の取得	機器が CCDS の共通認証マーク★を取得していること。
2	整理中	

表 3-6 セキュリティゲートウェイの調達要件

No.	要件	対策の内容
1	共通認証マーク★の取得	機器が CCDS の共通認証マーク★を取得していること。
2	整理中	

なお、アプリが動作するスマートフォンのセキュリティ対策はその利用者に委ねられ、スマートホームのサービスでは管理できないことから、本ガイドラインではセキュリティ要件を規定しない。

3.2　スマートホームの特徴とセキュリティへの影響

スマートホームの特徴と、それによるセキュリティへの影響は以下の通りである。

3.2.1　関係する要素の多様性

2 章で説明したシステムモデルの通り、スマートホームの構成要素は多種多様であり、セキュリティ上の脅威と対策を検討する方針が見えにくい問題がある。

この問題に対しては、スマートホームの構成要素が、居住者に提供する価値の面から、個々の IoT 機器と、それらを活用したサービスに大きく分けられる点に着目して、個々の IoT 機器とサービスの観点に分けて検討することで対応する。

本ガイドラインでは、スマートホームが提供するサービスについて、セキュリティ上の脅威と対策を検討して、評価する。また、個別の IoT 機器は、それぞれのガイドラインを作成して、同様に脅威と対策の検討と評価を行う。

3.2.2　製品安全（セーフティ）への対応

IoT 機器を含めた電気用品の遠隔操作は、電気用品安全法（電安法）の技術基準別表第八の 1（2）ロ[4]において、「手元操作が最優先されること」「遠隔操作による動作が確実に行われるよう、操作結果のフィードバック確認ができること」などの構造を備えることが規定されている。また、平成 30 年 3 月には、日本から国際電気標準会議（IEC）に、機能安全に関する基本規格 IEC 61508（電気・電子・プログラマブル電子安全関連の機能安全）に沿って、スマートホームで同時に動作する複数の機器・システムの機能安全を国際標準化する提案が出され、承認されている。他にも、製造物責任法（PL 法）や消費生活用製品安全法（消安法）に該当する IoT 機器の場合、遠隔操作がそれらの法令を遵守しているか確認が必要である。

また、スマートホーム情報基盤および関係するクラウドに何らかの障害が発生してサービスの提供が停止した場合でも、その影響を最小限に留めるように、フェイルセーフ・フェイルソフトなどの製品安全が講じられている必要がある。

3.2.3　機器の連携

スマートホームには多数の IoT 機器が設置されるが、これらの機器は単独で動作するだけでなく、互いに連携して動作する場合がある。

また、機器の連携は多層防御の狙いで行われることもある。これは、セキュリティ対策の弱い製品の前段に、よりセキュリティ対策の強い製品を置いて連携させることで、システム全体としてセキュリティ対策を向上させる方法である。

しかし、異なる機器が連携する場合、次の 2 点の問題がある。①連携先の機器のセキュリティ対策の内容・水準が適切であるか不明であり、全体として適切なセキュリティ対策が取られているか判断できない問題がある。②セキュリティ水準の異なる複数の機器が連携する場合、そのシステムのセキュリティは最も低い機器の水準になるため、セキュリティの評価、対策の検討において考慮が必要である。

これらの問題に対しても、CCDS 共通認証スキームで IoT 機器に発行された認証マークを利用する対策が考えられる。①連携先の IoT 機器が取得すべき業界認証マークを指定することで、連携先の IoT 機器が備えるセキュリティ要件を想定できる。②個々の IoT 機器が取得した業界認証マークの組み合わせに対して、それらが連携したシステム全体のセキュリティレベルを評価して、要求される水準に達しているか判断することができる。つまり、個々の IoT 機器が取得すべき業界認証マークを指定することで、全体としてのセキュリティレベルを指定することができる。

個々の IoT 機器が取得すべき業界認証マークを調達要件や設計条件に指定することで、それらが連携したサービスを提供する場合も、スマートホームのセキュリティを講じた設計ができる。

3.2.4 居住者・サービス提供事業者による IoT 機器の設置・撤去

住宅に設置される機器は、住宅会社が設定する調達基準を満たす製品が採用される。スマートホームの場合は、セキュリティ対策を有する製品であることを確認する必要があり、それを満たした機器が設置されると考えられる。

しかし、住宅が住宅会社から居住者に引き渡された後に、居住者またはサービス提供事業者が独自に選んだ機器が後付け設置される可能性がある。このような機器については、製品に取られているセキュリティ対策の内容・水準が不明であることも考えられる。このような機器の設置により、スマートホームのセキュリティ水準が引き下げられる場合が想定される。このため、居住者・サービス提供事業者が独自に設置する機器を含めたスマートホームのセキュリティを担保する方法を考える必要がある。

この問題に対しても、CCDS 共通認証スキームによる認証マーク制度で対策できる。住宅会社は、スマートホームにサービスを提供するときのセキュリティ要件を IoT 機器・サービスが取得した業界認証マークを使って居住者・サービス提供事業者に指定できる。居住者・サービス提供事業者は指定された業界認証マークを指標として、自身で IoT 機器を購入して設置できる。

3.2.5 スマートホーム情報基盤のセキュリティ対策

スマートホーム情報基盤は、生命・財産に影響がある情報を扱ったり、実際に機器を制御したりする可能性がある。また、場合によっては居住者の不在時に第三者に制御を許可することもあり得る。

したがって、スマートホーム情報基盤では、特になりすましと盗聴・改ざんの脅威に留意すべきである。次に考慮点を挙げる。

- クラウド上のシステムとして十分なセキュリティ対策を講じること。
- サービスの運用施設に物理的セキュリティ対策を講じること。
- 住設機器(あるいはゲートウェイ)からスマートホーム情報基盤の認証、スマートホーム情報基盤から住設機器の認証の両方を実施すること。
- スマートホーム情報基盤と住設機器(あるいはゲートウェイ)間、スマートホーム情報基盤と機器メーカークラウド間、機器メーカークラウドと住設機器(あるいはゲートウェイ)間について、セキュアな通信手段、プロトコルとすること。
- 不正な操作が行われたときに、その操作元・操作内容を追跡できるよう、機器の操作ログを採取すること。

3.3　スマートホームのサービス提供におけるセキュリティ対策

3 章で述べたスマートホームにおけるセキュリティ上の脅威への対策を以下にまとめる。

表 3-7 スマートホームにおけるセキュリティ対策

No.	対策	対策の内容	期待される結果
1	サービス全体の保護すべき資産と脅威の特定、リスク分析	・企画したサービスの全体について、概要、利用環境、前提条件、保護すべきデータ、想定する脅威、類似サービスで知られる既知の問題などの要素を元に保護すべき資産および脅威の特定を行う。 ・特定した保護すべき資産と、脅威を考慮し、5 章、6 章で後述するようなリスク分析・評価方法によりリスク分析を行い、設計および運用にて対策を施す。	・サービス全体として、リスクの大きい部分を把握できる。 ・セキュリティ対策の漏れがないか把握できる。 ・使用する IoT 機器が満たすべきセキュリティ水準を決定できる
2	IoT 機器・サービスの業界認証マークの指定	・スマートホームの設計時に、設置される IoT 機器、提供されるサービスのセキュリティ要件として業界認証マークを指定する。 ・スマートホーム向けサービスの提供にあたり、利用可能な IoT 機器の業界認証マークを指定する。 ・IoT 機器・サービスの追加時に、指定された業界認証マークを取得しているか確認する。	・スマートホームに設置された IoT 機器、提供されるサービスのセキュリティ水準を具体的に想定できる。 ・サービスで利用される IoT 機器に必要なセキュリティ対策がなされることを担保できる。
3	機器の連携による多層防御	セキュリティ対策の弱い機器は、他のセキュリティ対策が施された機器を前段に置いて防御する。	・多層防御によりセキュリティ対策が向上される。

No.	対策	対策の内容	期待される結果
4	クラウドセキュリティ対策	・総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）」を理解し、対策を行う。	・クラウドへのセキュリティ上の脅威に対応できる。
5	物理的セキュリティ対策	・運用保守を行う施設については、作業場所の分離、入館入室の管理を徹底する。 ・防犯カメラ等でモニタリングを行う。 ・ドアや窓の破壊に備え、警報装置の設置、警備員の配置を実施する。	・物理的な要因によるセキュリティ上の脅威に対応できる。
6	業界認証マークの取得	・IoT 機器・サービスが満たすべきセキュリティ要件に応じて業界認証マークを取得する。	・保護すべき対象に応じて適切なセキュリティ対策の取られた機器・サービスであることを周知できる。

4　スマートホーム開発のフェーズとセキュリティ

スマートホームのセキュリティ対策においては、IoT 機器のライフサイクル（購入、故障、転売、廃棄）による機器の入れ替わりだけでなく、IoT 機器が変わらずその利用者が変わる場合も考慮する必要がある。

なお、本書ではフェーズ検討の対象を戸建て住宅とし、集合住宅、賃貸住宅等については今後の検討とする。

4.1　ライフサイクルにおけるフェーズの定義

住宅のライフサイクルは、大きく「設計」、「生産・施工」、「アフター」、「リフォーム」、「転売」「解体」の６フェーズに分類される。提供するスマートホームサービスにおいて十分なセキュリティを確保するには、各フェーズにおいて十分な対策を施し、製品のセキュリティ品質を確実なものとするべきである。

図 4-1 ライフサイクルにおけるフェーズ

表 4-1 フェーズの定義

フェーズ	説明
設計	IoT 住宅設備を含めたスマートホーム住宅の設計を行う
生産・施工	IoT 住宅設備を含めたスマートホーム住宅の生産、施工を行う
アフター	施工後に家主が居住を開始し、スマートホーム住宅の情報活用、運用、メンテナンスを行う
リフォーム	スマートホーム住宅のリフォームを行う
転売	スマートホーム住宅の家主の変更を行う
解体	スマートホーム住宅の使用を終了し、解体を行う

4.2　各フェーズにおけるセキュリティへの取組み

前節で概説したライフサイクルの各フェーズにおいて実施すべきセキュリティへの取組みを説明する。

4.2.1　設計フェーズ

製品のセキュリティ品質を確保するには、より上位からのセキュリティ設計が必要となる。ここでは製品企画におけるセキュリティ品質の確保について述べる。

表 4-2 設計フェーズでのセキュリティへの取組み

No.	説明
1	**ニーズ調査** ・利用するサービス内容の確認と選定、インフラの確認を行う。
2	**入居者同意取得** ・個人情報等の取り扱いについて説明し、同意を得る。 ・責任分界点の明示および説明を実施する。
3	**設置機器の特定** ・使用機器（ゲートウェイ、センサー、など）を特定する。
4	**設計図書への表記・指示** ・使用機器を設計図書（システム系統図など）へもれなく表記する。

4.2.2　生産・施工フェーズ

生産・施工フェーズでのセキュリティへの取り組みを以下に示す。

表 4-3 生産・施工フェーズでのセキュリティへの取組み

No.	説明
1	**使用機器等の発注** ・設計図書との整合性を確認する（ゲートウェイ、センサー、配線、など）。
2	**使用機器等の管理・監督** ・不正な機器の導入がないか、使用機器に不具合がないか、を確認する。

3	**施工確認** ・契約者、使用機器、オプションの状況を確認する。 ・施工時および施工後の設計図書、発注明細との整合性確認および監理を行う（※ただし、写真等での記録も可とする）。 ・使用機器等の施工後の動作確認を行う。 ・システム全体の正常性確認を行う。
4	**提供物確認** ・キー、カード等の払い出し数と引き渡し数を突き合わせる。
5	**使用機器およびサービス利用方法の説明** ・使用機器やサービスの利用方法について、入居者に説明する。
6	**取扱説明書の提供** ・免責事項、不具合時の対応方法や連絡先などを記載する

4.2.3 アフターフェーズ

アフターフェーズでのセキュリティへの取り組みを以下に示す。

表 4-4 アフターフェーズでのセキュリティへの取組み

No.	説明
1	**取扱説明書の提供** ・免責事項にしてほしいことがあれば、取扱説明書に必ず書いておく。 ・販売するときは、こういうことを考慮した製品になっていると表示するようにする。
2	**運用時の使われ方の定義** ・運用時の使われ方の範囲や使用時の前提条件をきちんと定義して運用者・居住者に伝える。
3	**ユーザへの注意喚起** ・不審な機器が接続されている場合や、おかしな挙動を検知した場合に、ユーザに注意をうながす表示をする等の工夫をする。 ・初期設定のまま、設定ミスのまま使われない工夫をする。

4	**最新の脆弱性への対応** ・使用している OS、boot プログラム、アプリケーションに脆弱性がないかどうかを、脆弱性関連情報を常にウォッチし、関連する脆弱性の場合、プログラムのアップデートを実施する。
5	**機器利用制限** ・今現在十分と考えられているアルゴリズムや鍵長も、将来的には不十分になる可能性があり、ユーザへある時点で機器利用の停止を推奨することを検討する。 ・利用期間が長いと想定される IoT-GW においては、ベンダーとして保守期間を明確化し、マニュアルや HP 上でユーザに周知する。
6	**提供物管理** ・キー、カード等の払い出し数と引き渡し数を突き合わせる。 ・紛失時に提供物の情報を更新する。

4.2.4 リフォームフェーズ

リフォームフェーズでのセキュリティへの取り組みを以下に示す。

ただし、リフォームにおける設計および生産・施工フェーズについては、表 4-2 および表 4-3 を参照。

表 4-5 リフォームフェーズでのセキュリティへの取組み

No.	説明
1	**既導入機器との互換性確認** ・使用機器等の追加・入替えおよび情報の追加・更新を行う際、既導入機器類に影響を及ぼさないか確認する。
2	**機器廃棄方法の周知** ・使用機器等の撤去・廃棄および情報の削除を適切にする。 ・機器内にデータが残留したまま廃棄することで想定される脅威、リスクを取扱説明書等で明示する。 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する。 ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等でユーザに明示する。

No.	説明
	・廃棄する場合は、リユースされないようにきちんと破壊されたことを確認するよう取扱説明書等で推奨する。

4.2.5 転売フェーズ

転売フェーズでのセキュリティへの取り組みを以下に示す。

表 4-6 転売フェーズでのセキュリティへの取組み

No.	説明
1	**提供物管理** ・キー、カード等の払い出し数と引き渡し数を突き合わせる。
2	**転売後の管理** ・次入居者へセキュリティの取り組みを周知する。 ・セキュリティの取り組みについては、**表 4-4** を参照。

4.2.6 解体フェーズ

解体フェーズでのセキュリティへの取り組みを以下に示す。

表 4-7 解体フェーズでのセキュリティへの取組み

No.	説明
1	**機器廃棄方法の周知** ・機器内にデータが残留したまま廃棄することで想定される脅威、リスクを取扱説明書等で明示する。 ・廃棄時には機器の設定やメモリ内のデータを初期化(工場出荷状態)することを取扱説明書等で推奨する。 ・破壊し廃棄することを推奨する場合には、各自治体の規則に従って廃棄処分する旨を取扱説明書等でユーザに明示する。 ・廃棄する場合は、リユースされないようにきちんと破壊されたことを確認するよう取扱説明書等で推奨する。

5 リスク分析・評価

5.1 保護すべき資産と重要度の定義

整理中

5.2 想定脅威と発生頻度の定義

整理中

5.3 想定インシデントとリスク値の定義

整理中

6 まとめ

6.1 「IoTセキュリティガイドライン」との関係

本書はIoT推進コンソーシアムが公開している「IoTセキュリティガイドライン」を詳細化した内容になっている。「IoTセキュリティガイドライン」の指針と本書の対応を表6-1に示す。

表 6-1 IoTセキュリティガイドラインと本書の対応

IoTセキュリティガイドライン			本書での対応箇所	
大項目		指針	章番号	概要
方針・管理	方針1 IoTの性質を考慮した基本方針を定める	要点1 経営者がIoTセキュリティにコミットする	記述なし	
		要点2 内部不正やミスに備える	4.2.2 4.2.3 4.2.5	・配線等の施工確認 ・居住者への提供物確認。
分析	方針2 IoTのリスクを認識する	要点3 守るべきものを特定する	3.3	・保護すべき資産の特定
		要点4 つながることによるリスクを想定する	3.3	・脅威の特定
		要点5 つながりで波及するリスクを想定する	3.3	・リスク分析
		要点6 物理的なリスクを認識する	3.3	・リスク分析
		要点7 過去の事例に並ぶ	3.3	・脅威の特定
設計	方針3 守るべきものを守る設計を考える	要点8 個々でも全体でも守れる設計をする	3.3	・業界認証マークの指定 ・機器の連携による多層防御
		要点9 つながる相手に迷惑をかけない設計をする	3.3	・業界認証マークの指定 ・クラウドセキュリティ対策
		要点10 安全安心を実現する設計の整合性をとる	3.3	・業界認証マークの指定 ・クラウドセキュリティ対策
		要点11 不特定の相手とつなげられても安全安心を確保できる設計をする	3.3	・業界認証マークの指定 ・機器の連携による多層防御
		要点12 安全安心を実現する設計の検証・評価を行う	3.3	・リスク分析

構築	方針 4 ネットワーク上での対策を考える	要点 13 自身がどのような状態かを把握し、記録する機能を設ける	3.3	・クラウドセキュリティ対策 ・業界認証マークの取得
		要点 14 機能及び用途に応じて適切にネットワークを接続する	3.3 4.2.2	・クラウドセキュリティ対策 ・業界認証マークの取得 ・配線の施工確認
		要点 15 初期設定に留意する	4.2.2 4.2.3	・施工確認 ・ユーザへの注意喚起
		要点 16 認証機能を導入する	3.3	・クラウドセキュリティ対策 ・業界認証マークの取得
運用・保守	方針 5 情報発信・共有を行う	要点 17 出荷・リリース後も安全安心な状態を維持する	4.2.3	・最新の脆弱性への対応 ・アップデート
		要点 18 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える	4.2.2 4.2.3 4.2.5	・取扱説明書の提供 ・ユーザへの注意喚起 ・転売後の管理
		要点 19 つながることによるリスクを一般利用者に知ってもらう	4.2.2 4.2.3 4.2.4 4.2.6	・取扱説明書の提供 ・ユーザへの注意喚起 ・機器廃棄方法の周知
		要点 20 IoT システム・サービスにおける関係者の役割を認識する	4.2.2 4.2.3	・使用機器等の管理・監督 ・運用時の使われ方の定義
		要点 21 脆弱な機能を把握し、適切に注意喚起を行う	4.2.3	・最新の脆弱性への対応
一般利用者向け	ルール 1 問い合わせ窓口やサポートがない機器やサービスの購入・利用を控える		3.3	・業界認証マークの指定
	ルール 2 初期設定に気を付ける		4.2.2 4.2.3	・取扱説明書の提供 ・ユーザへの注意喚起
	ルール 3 使用しなくなった機器については電源を切る		4.2.3	・機器利用制限
	ルール 4 機器を手放すときはデータを消す		3.3 4.2.4 4.2.6	・業界認証マークの指定 ・機器廃棄方法の周知

6.2　まとめ

整理中

引用/参考文献

[1] IoT セキュリティガイドライン、IoT 推進コンソーシアム・総務省・経済産業省

http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

[2] 平成 28 年版情報通信白書 第 1 部 第 2 章 第 1 節 1 p.80、総務省

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n2100000.pdf

[3] つながる世界の開発指針　～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～、独立行政法人情報処理推進機構　技術本部　ソフトウェア高信頼化センター

https://www.ipa.go.jp/files/000051411.pdf

[4] 「別表第八 電気用品安全法施行令（昭和三十七年政令第三百二十四号）別表第一第六号から第九号まで及び別表第二第七号から第十一号までに掲げる交流用電気機械器具並びに携帯発電機」

http://www.meti.go.jp/policy/consumer/seian/denan/kaishaku/gijutsukijunkaishaku/beppyoudai8.pdf