Society5.0 実現に向けた
スマートライフ分野のサイバーセキュリティ対策の方向性

平成30年8月3日

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
スマートホームサイバーセキュリティWG

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

生活者に、安心・安全、健康、快適、便利なサービスを提供する新たなスマートライフ市場の構築に向け、住宅・住宅設備機器・家電・IT通信機器・サービス等の住まいに関わるあらゆるモノを連携し（Connected化）、業界・業種の枠を超えた「スマートホーム部会」を設置。

スマートホーム部会

■**部会長　丹 康雄　　国立大学法人 北陸先端科学技術大学院大学 教授**

◆**委員　企業）家電・AV関連：**シャープ（株）、パナソニック（株）、ソニー（株）、東芝映像ソリューション（株）、三菱電機（株）
IT・通信関連：富士通クライアントコンピューティング（株）、NECパーソナルコンピュータ（株）
車載関連：（株）JVCケンウッド
住宅設備・サービス：（株）デンソー、（株）LIXIL、TOTO（株）、セコム（株）、関西電力（株）、ソフトバンク（株）、戸田建設（株）

団体・機関）
住宅・住宅設備分野：（一社）住宅生産団体連合会、（一社）不動産協会、（一社）日本建材・住宅設備産業協会、コネクティッドホーム アライアンス
電機・通信分野：（一社）日本電機工業会、（一社）日本照明工業会、（一社）日本冷凍空調工業会、（一社） 電池工業会、（一社）情報通信ネットワーク産業協会、（一社）電動車両用電力供給システム協議会
医療分野：PCHA(パーソナル・コネクテッド・ヘルス・アライアンス）　**研究機関：**国立研究開発法人 産業技術総合研究所

- **スマートホームデータカタログWG**
  ※ データ連携型社会を目指し、機器メーカー・サービス提供事業者が相互に理解できるデータカタログについて検討し、Connected Industries スマートライフ分科会へ提言。
- **スマートホームサイバーセキュリティWG**
  ※ **経済産業省 産業サイバーセキュリティ研究会WG１のスマートホームSWG**として、スマートホーム領域におけるサイバー・フィジカル・セキュリティ対策等について検討。
- **スマートホーム安全標準化WG**
  ※ 住宅向けIoT機器の導入による不安全状態発生を防止するIoT住宅に関する安全標準策定に向け、経済産業省及び関連機関と連携し検討。

一般社団法人 電子情報技術産業協会（JEITA）が目指すスマートホーム像について

スマートホームとは、**持続可能な社会を構築するために**、生活者や住空間等の情報を取扱うシステムと住まい手、住まいのモノ・サービス提供者を含む全ての参加者が効率よく連携し、**互いに支え合いながら限られた資源を最大限活かし、社会の幸せ、住まい手の幸せを実現する場**である。

住まい手は、スマートホームがもたらす様々な選択肢と、自らの意思で、望む暮らしを実現できる。

【家庭の急速な変化への対応に必要なスマートホーム】

家庭の変化

【平均世帯人員】

1953年
約5人

2016年
2.47人

※国民生活基礎調査の概況より

【共働き等世帯数】

1980年
片働き 1,114万世帯
共働き 614万世帯

※総務庁「労働力調査特別調査」

2015年
片働き 687万世帯
共働き 1,114万世帯

※総務省「労働力調査」

＝ 家庭や近隣住民、地域コミュニティによる互助・サポートが希薄になる中、公的・私的なサービスとしての支援（育児・見守り等）を、家をスマート化することで実現する。

【スマートホームがもたらす新たな価値】

製品・技術の高度化による社会サービスの深化

	これまで	スマートホーム
家電製品等	単機能・非NW スマートフォン	高機能/AI化・NW化 センサー・ウェアラブル
技術インフラ	高速処理 有線での限定的な接続 （IT技術）	リアルタイム処理 無線での多様な機器への接続 （IoT技術）
社会サービス （電気・ガス・水道・電話・ 警察・消防・ごみ収集等）	リソース（資源・労働力） を最大活用 ＝個別最適社会	リソース（資源・労働力） を最適活用 **＝全体最適社会 （Society 5.0）**

＝ 家電製品等の機器の進化は様々な生活情報の収集を可能にし、技術インフラの発展は、**生活情報と多様なサービスとのつながりを可能**にする。
その結果、住まいにおける新たな選択肢（社会サービス）が生まれ、**社会課題の解決と住まい手の幸せの両方を実現する。**

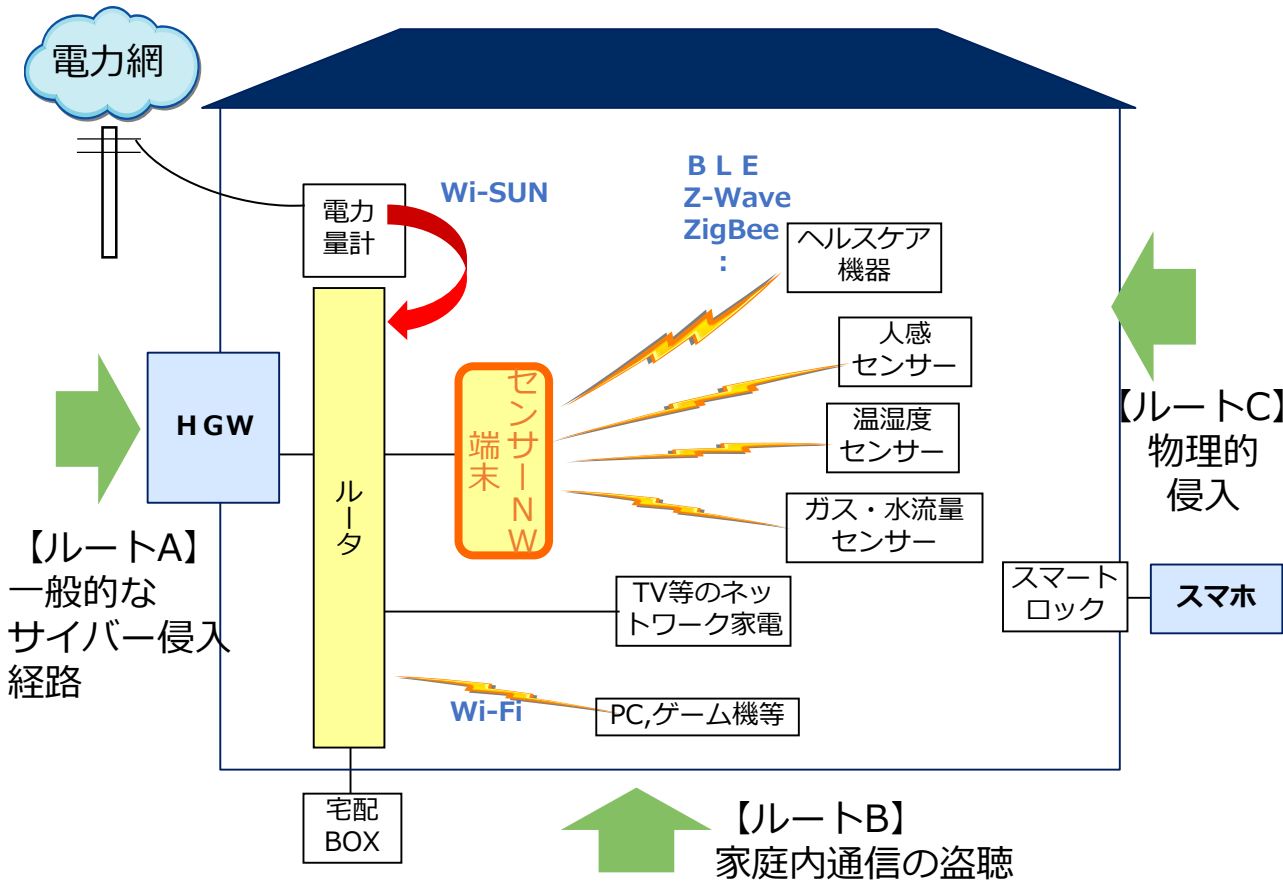
スマートホームにおける標準的な構成要素

- 快適なスマートホームを実現するためには、ネットワークを介してあらゆるモノがつながることになる。その結果、**住まい手にとってのリスク**が**サイバー空間**のみならず、**フィジカル空間にまで広がっている**。
- そこで、スマートホームの標準的なシステム構成の中で、現在どのような脅威（侵入経路とその特徴）があるのか整理する。

【ルートA】 **無差別型攻撃**
遠隔から不特定多数へのアクセスが可能。
主に踏み台等の為にアクセス。（本人への影響は少ない）
場合によっては、標的探しに使う可能性あり。
脅威は国家級にまで広がる。（社会インフラへ影響）

【ルートB】 **標的型攻撃**
具体的な標的としてアクセス。（本人への影響が大きい）
近傍で行う必要があるが、標的なので防げない。
Wi-Fiへの接続は、宅内端末を介して等比較的容易。
他の無線方式もペアリング時等を狙うことで可能。
脅威は悪意のある事業者のほか、近親者・友人などもあり得る。

【ルートC】 **物理的侵入**
旧来型のドロボーの領域で、盗聴器を仕掛けるなど。



※　住まい手にとってのリスク評価・対策検討は、機器の使われ方によって変化する。

スマートホームが設置される「家庭」の特性と特有の脅威について

【スマートホーム特有の脅威】

① 膨大な攻撃対象（世帯数はおよそ5300万世帯 ※総務省統計局「平成27年国勢調査結果」）

スマートホームを構成するシステムは世帯の数だけ存在する。そして、セキュリティレベルは一部でも低いところがあれば、全体のレベルはその一番低いレベルになってしまう。

② マネジメント不在に起因する脆弱性 (選定、設置、保守、破棄に対する妥当性のチェックが働きにくい)

家庭では、スマートデバイスの導入や利用に計画性がないことも多い。どんな機器をつないでいるか把握し、ファームウェア更新の保全をしているか等、運用をチェックする機構が働かない。

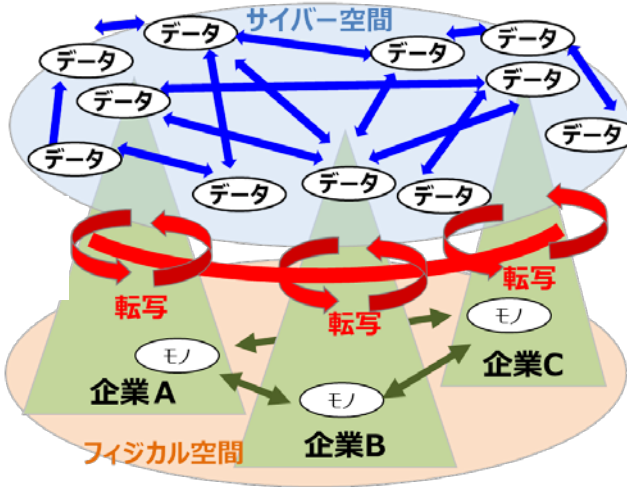
③ 利用者側のリテラシー不足による想定外のインシデント

家庭では、子供や高齢者等様々な人が暮らしており、誤使用によるインシデント発生の可能性があり、機器単体のセキュリティ対策だけでは不十分である。

Society5.0の起点はすべての家庭にある。
家庭のスマートホーム化なくしてSociety5.0は実現できない。

スマートホームにおけるサイバー・フィジカル・セキュリティ対策フレームワークの方向性

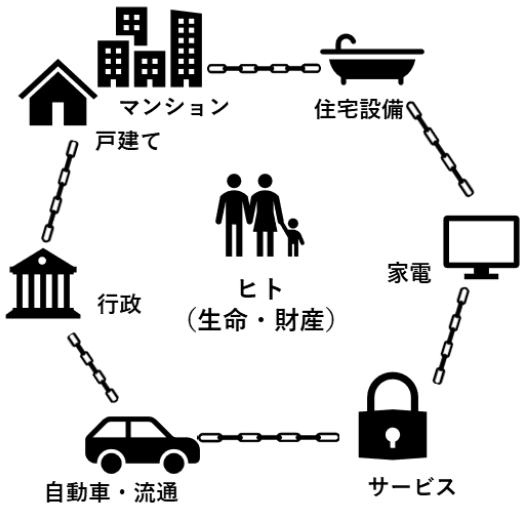
- スマートホームでは、家電やウェアラブル、センサー等の多様な機器で収集された生活データが連携し、サービス（オペレーションまで含めた）として住まい手に提供される**価値創造過程（バリュークリエイションプロセス）が生まれる**。しかし、スマートホーム特有の脅威に備えた対策ができていない。
- スマートホームの特徴を踏まえ、住まい手まで含めたステークホルダーが**サイバー・フィジカル・セキュリティ対策フレームワーク**を構築していくことが重要。



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）
（第2回）-配布資料より抜粋

加工
流通
取得
サービス
データ

レイヤー構造	プレイヤーイメージ	求められる行動
【3層】 サービス クラウド	サービス事業者、 情報連携事業者（プラットフォーマー）	データが正しく流通・加工されるよう保全する
【2層】 機器クラウド	ネットワーク機器メーカー（住設機器・家電・ヘルスケア機器・通信機器メーカー等）	機器が正確なデータを取得できるように保全する
【1層】 ローカル ネットワーク	住まい手 （住まい手から委託される事業者含む）	目的に合った正しい機器を設置・設定する



第1層で収集されたデータは第2層で転写され、第３層で**オペレーションレベルを含めたサービス**となって第１層の住まい手に提供され、**生活のQOLが高まる**ことになる。
サービスクオリティを担保するために、各層のプレイヤーにおいて価値創造への取り組みを検討していくことが重要。**JEITAでは、価値創造を支える、信頼の創出、信頼チェーンの構築・維持等の仕組み構築に向けたフレームワークの検討を行っていく。**