

サブワーキンググループの 設置・検討状況について

経済産業省 商務情報政策局
サイバーセキュリティ課

WG1の検討体制とSWGの開催状況

- WG1で検討する『サイバー・フィジカル・セキュリティ対策フレームワーク』の標準モデルを、業界毎に順次展開し、具体的適用のためのセキュリティポリシーを検討。

WG 1 制度・技術・標準化

標準モデル

Industry by Industryで検討 (分野ごとに検討するためのSWGを設置)

ビル (エレベーター、
エネルギー管理等)

2/28 第1回会合開催

設置に向けた検討中

電力

防衛産業

3/29 第1回会合開催

(防衛装備庁 第6回情報セキュリティ官民検討会)

自動運転

設置に向けた検討中

スマートホーム

3/13 第1回会合開催

(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)

その他コネイン関係分野

ビルSWG（座長：江崎 浩 東京大学 教授）

- ビルの情報系・制御系システムに係るサイバー攻撃のリスクと、それに対するサイバーセキュリティ対策について、海外における取組状況を含めて知見を共有
- 共有した知見を踏まえ、ビルに求められるサイバーセキュリティ対策を整理し、ビルに関わるステークホルダーが活用できるガイドライン等を取りまとめる
- オリパラに向けて、各事業者において実施できる分野から実装を目指す

<構成員>

有識者、ビルオーナー、ゼネコン、サブコン、設計事務所
個別システム事業者（ビル管理、空調、エレベーター、ビデオ監視、電力・熱供給 等）
自治体、関係省庁 等

<ガイドラインのとりまとめイメージ>

- ビルシステム全体に共通する最低限の要求をまとめたもの＋より詳細な方策を示したものの二階建て構成
- ガイドラインでは、多くの事業者の取組の参考となるよう優先順位を示した選択肢を提供

内容項目例

- ・ ビルに係わるサイバーセキュリティ上の脅威の現状
- ・ ビルシステムに対して起こりえる攻撃とその影響の予測
- ・ サイバーセキュリティ確保のための対策の概要
- ・ 対策の具体的内容
- ・ 対策実施に向けたチェックリスト

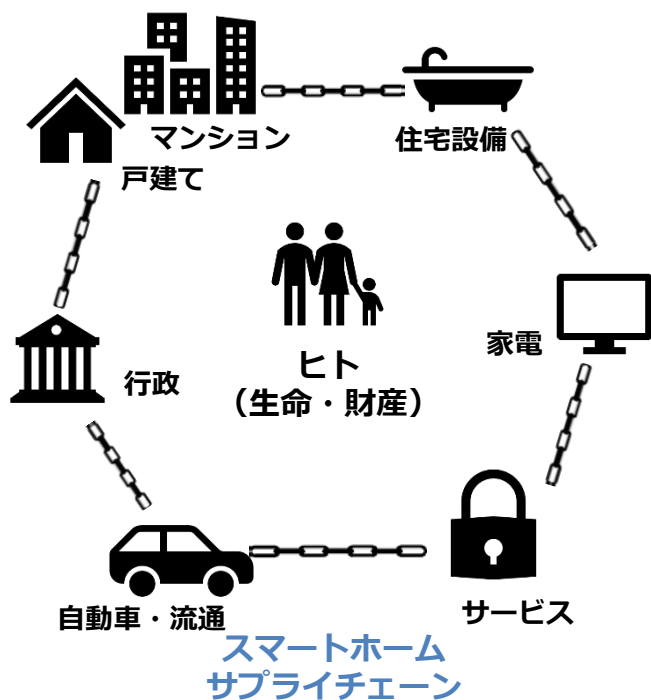
フェーズ	主な要求概要	関係する ステークホルダー
設計	機器、ネットワーク、物理 セキュリティへの要求	設計事務所、オーナー、 ゼネコン、サブコン、 ベンダー
施工／建築	機器単位、システム単位の 施工プロセスへの要求	ゼネコン、サブコン、 ベンダー
竣工検査	全体管理体制、管理結果、 受入検査への要求	ベンダー、ゼネコン、 サブコン、オーナー、 設計事務所
運用・保守	管理体制への要求	オーナー、サブコン、 ベンダー

スマートホームSWG（座長：小松崎 常夫 セコム株式会社 顧問）

- JEITA スマートホーム部会内にスマートホームサイバーセキュリティWGを新たに設置
- ハウスメーカ、システム・インテグレータ、機器メーカ等の住まいに関わる企業、業界団体が参加

＜構成員＞

企業）家電・AV関連、IT・通信関連、車載関連、住宅設備・サービス関連
団体・機関）住宅・住宅設備分野、電機・通信分野、医療分野、研究機関
スマートホーム部会長の丹 康雄教授（北陸先端大）も委員として参画



＜検討項目＞

- Step1 “スマートホーム産業”に求められるセキュリティ対策像を整理し、**住宅・住設・家電・サービス等のスマートホームサプライチェーンで活用できる「サイバー・フィジカル・セキュリティ対策フレームワーク」**を策定する。
- Step2 「サイバー・フィジカル・セキュリティ対策フレームワーク」を概念としてだけでなく、各事業者が実際のセキュリティ対策オペレーションレベルで活用できるよう、実効的な施策について検討を行い、必要に応じて、政府への政策提言を行う。
- Step3 実運用に向けて、消費者へのリスク周知や免責事項、モニタリングの在り方、事業者間の信頼の創出方法等について検討。さらには、スマートホームからスマートライフ分野（街・社会インフラ）に対応したセキュリティ対策についても検討を進めていく。