

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を策定

JEITAスマートホーム部会は、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)と連携して、スマートホームにおけるサイバー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を策定しました。

ガイドライン発行の背景・目的

■スマートライフの実現に向けて

スマートライフの中核であるスマートホームは、「子育て世代、高齢者、単身者など、さまざまなライフスタイル／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」であり、IoTに対応した住宅設備・家電機器などがサービスと連携することによって、住まい手ならびに住まい手の関係者に便益が提供されます。

■サプライチェーン全体で対策することが必要

一方で、スマートホーム特有のサイバーセキュリティ上の脅威として、①膨大な攻撃対象(世帯数はおよそ5300万世帯)、②マネジメント不在に起因する脆弱性

(統制された管理・運用がされなく、セキュリティ対策が不十分)、③利用者側の誤操作等による想定外のインシデントなどが挙げられ、スマートホームにおけるサイバーセキュリティは、サプライチェーン全体で守ることが必要です。

しかしながら、スマートホームへのサイバー攻撃は、住まい手の生命財産に直接に影響するにも関わらず、スマートホームの利用者を含む幅広い関係者全体に向けたセキュリティ対策に関する文献はこれまで存在していませんでした。

■ステークホルダー毎の対策指針を整理

そこで、JEITAスマートホーム部会では、スマートホームに関係する家電・住宅設備メーカ、サービス提供事業者、住宅デベロッパー等の幅広い関係者の参加を得て、日本初となるスマートホーム市場に関わるステークホルダー毎の対策指針を経済産業省 サイバーセキュリティ課の委託事業としてまとめました。

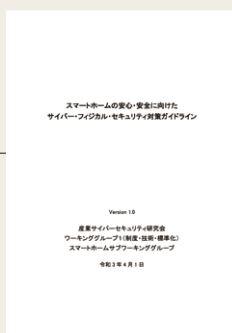
本ガイドラインは、知識やバックグラウンドがさまざまなステークホルダーに対応するため、シンプルな対策ガイドから、具体的な対策要件や国際標準との対比まで、

刊行物のご案内

「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」
2021年4月1日公開

■目次

1. はじめに
2. セキュリティ対策の検討の考え方
3. スマートホームにおけるセキュリティ上の脅威
4. 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
5. おわりに



■添付:

- ・ステークホルダーにおける、機能／想定されるインシデント／リスク源／対策要件
- ・対策の整理と、国際規格などの各種規格との対応
- ・ステークホルダーに向けたガイドと対策要件の対応関係
- ・サイバー攻撃と脆弱性等の事例
- ・用語集
- ・参考文献

■ダウンロード(無償)

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



セキュリティ対策を階層的に整理しています。

本ガイドラインを策定したことにより、スマートホーム分野でIoT機器を通じたさまざまなサービスを利用する上で生じる可能性がある、情報漏洩、サイバー攻撃、フィジカル空間への被害などへの対策を促し、スマートホーム利用における住まい手の安心・安全の確保の一助になることを期待しています。

ガイドライン解説パンフレットの制作

JEITAスマートホーム部会では、ガイドラインを分かりやすく解説した普及啓発パンフレットも併せて制作しました。

スマートホームに関連する事業者向けとスマートホームにお住いの方向けの2種類をご用意しましたので、ご活用ください。

刊行物のご案内

『スマートホームで
便利な暮らしを！』
2021年3月発行



『安心で安全な
スマートホームの実現に向けて』
2021年3月発行



■ダウンロード（無償）

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

今後の取り組み

今回公開したガイドラインをベースとして、JEITAスマートホーム部会では、引き続き、安心・安全なスマートライフ市場の実現に貢献していきます。

今後の取り組みにつきましては、スマートホーム部会のWebサイトにて随時発表いたします。



JEITA スマートホーム部会 Webサイトでは、
スマートホームに関連するトピックや
各種成果物を公開しています。

<https://home.jeita.or.jp/smarthome/>