第 3 回 STAMP ワークショップ一般講演応募要領

タイトル

STAMP/STPA を用いたリスクコミュニケーションツール

Cybersecurity Assessment with STAMP/STPA

著者・発表者

東京電機大学　サイバーセキュリティ研究所　林　浩史・髙橋　雄志

Tokyo Denki Univ. Cyber security Lab　Hayashi, Hiroshi / Takahashi, Yuji

概要

サイバーセキュリティの対策において、リスクコミュニケーションは最も重要なプロセスの一つである。

特に近年急速に発展している IoT デバイスは、サイバーセキュリティとセーフティに関する要件・対策が混在しており、リスクコミュニケーションの重要度が増すと同時に困難なものとなっている。

我々は、このサイバーセキュリティとセーフティが混在する IoT デバイスにこそ STAMP/STPA が有効であると考え、STAMP/STPA を用いたリスクコミュニケーションツール MRC-IoT の開発を行った。このツールは、IPA STAMP/STPA Workbench の出力を活用し、リスクの準定量分析を行うツールである。

これにより、STAMP/STPA により抽出された膨大なハザードや脅威に対する対策に優先順位をつけ、ステークホルダー間のリスクコミュニケーションを潤滑に行うことが可能となる。

STAMP/STPA でサイバーセキュリティを取り扱う手法は、STAMP/STPA-sec や STAP/STPA-safesec などいくつかの手法が提案されている。我々は、STAMP/STPA に対してヒントワードの拡張を行うことで、サイバーセキュリティに関する分析を行うことが可能であると考えている。

IPA STAMP/STPA Workbench は、ヒントワードのカスタマイズ機能をもっており、これを活用することで、IoT デバイスのサイバーセキュリティおよびセーフティの両方を同時に取り扱うことが可能である。さらに、excel フォーマットでの出力機能を活用し、分析結果をリスクの準定量分析部(MRC-IoT)に接続することで、STAMP/STPA により抽出された脅威やハザードをリスクコミュニケーションに活用することができた。

本講演では、具体的な事例を使い、IPA STAMP/STPA　Workbench での出力を MRC-IoT の入力とし、準定量分析を行った上でリスクコミュニケーションに活用する事例を合わせて紹介する

キーワード

(1) リスクコミュニケーション

(2) IoT

(3) MRC-IoT

(4) サイバーセキュリティ

(5) IPA STAMP/STPA Workbench