資料 1-4

サイバーセキュリティ研究における科学的基礎の検討状況

2020 年 9 月

以下はサイバーセキュリティの研究における科学的基礎について、WG 有志で議論中のドラフトである。検討をすすめるにあたり、NSTC による報告書[1]を参考にしている。

1. 対象となるシステムに対し、その構成、脅威モデル、および防御機構を形式的な手法で検証、評価するフレームワーク

2. 安全なシステムの設計において、そのシステムが満たすべきセキュリティ特性を証明可能、あるいは検証可能とする方法論

3. 破壊的イノベーションにより生まれた新たなテクノロジーに対して潜在的に生じ得る脅威を予見し、未然に防ぐ方法論

4. 社会で用いられるシステムにおける個人、組織、社会の要求、期待、および行動を司る原理を理解することにより、潜在的なセキュリティ脅威を同定する方法論

5. 以上のフレームワーク、方法論は、いずれも科学的な手法に基づき記述され、客観的に再現性がある形で実行されるべきである

[1] CYBER SECURITY AND INFORMATION ASSURANCE INTERAGENCY WORKING GROUP, SUBCOMMITTEE ON NETWORKING & INFORMATION TECHNOLOGY, RESEARCH & DEVELOPMENT COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE of the NATIONAL SCIENCE & TECHNOLOGY COUNCIL “FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN 2019,”

https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf