

諸外国のサイバーセキュリティ研究開発に関する戦略や計画等の構成

米国

FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN (連邦サイバーセキュリティ研究開発戦略計画) [2019年12月 国家科学技術評議会 (NSTC) ]

目次

Executive Summary (概要)

Introduction (はじめに)

Strategic Framing (戦略的フレーム)

Cybersecurity Context (サイバーセキュリティの背景)

Challenges (挑戦)

Approach (アプローチ)

The Defensive Elements (防御要素)

Deter (抑止)

Protect (保護)

Detect (検知)

Respond (対応)

Priority Areas (重点分野)

Artificial Intelligence (AI)

Quantum Information Science (量子情報科学)

Trustworthy Distributed Digital Infrastructure (信頼できる分散デジタルインフラ)

Privacy (プライバシー)

Secure Hardware and Software (安全なハードウェアとソフトウェア) ← 安全なサプライチェーン等

Education and Workforce Development (教育と労働力開発)

Critical Dependencies (重要事項) ※研究開発を進めるにあたって重要な事項

Human Aspects (人的側面)

Research Infrastructure (研究基盤)

Risk Management (リスクマネジメント)

Scientific Foundations (科学的基礎) ← 科学的基礎の重要性につき引き続き指南

Transition to Practice (実用化への移行)

Implementing the Plan (計画の実施)

Recommendations for Supporting Activities (支援的活動に関する助言)

Abbreviations (略語)

2016年にはなかったもの。本計画で初めて6つの分野を同定(国家サイバー戦略2018(2018 National Cyber Strategy)と2021年度研究開発予算優先事項覚書(FY2021 Research and Development Budget Priorities Memorandum)を受けて)

AIとサイバーセキュリティの相互のニーズとメリットに焦点

量子技術によるサイバーセキュリティへの影響と、量子コンピューティングインフラや量子情報技術を攻撃から守る手法

5Gやポスト5G、IoT、サイバーフィジカルシステム等

出所：ホームページ

<https://www.nitrd.gov/news/Federal-Cybersecurity-RD-Strategic-Plan-2019.aspx>

※翻訳および注釈は事務局にて付記したもの

Analysis of the European R&D priorities in cybersecurity (サイバーセキュリティにおける

欧州の研究開発優先事項) [2018年12月 欧州ネットワーク情報セキュリティ庁 (ENISA) ]

目次 研究開発の戦略的優先事項勧告のベースとして、2025年の欧州のシナリオをもとに、脅威を同定し、それを軽減できる可能性のある領域を提案している。同定された戦略的トピックスの詳細分析と研究における課題はAnnex AとBで議論されている。

Executive Summary (概要)

- 1. Introduction (はじめに)
- 2. Our Europe in 2025: a plausible scenario (2025年のもっともらしいシナリオ)
- 3. Key Messages and Recommendations (主なメッセージと推奨事項) ←

Annex A: Awareness and education challenges (意識と教育の課題)

- A.1 Awareness building - societal challenge (意識向上 - 社会的課題)
- A.2 Capacity building - educational challenge (能力開発 - 教育的課題)
  - A.2.1 Enabling the multidisciplinary approach (学際的なアプローチを可能にする)
  - A.2.2 Cybersecurity in computing (コンピューティングにおけるサイバーセキュリティ)
  - A.2.3 Simulation and visualisation (シミュレーションと可視化)

Annex B: Existential Threats (存在する脅威)

- B.1 Artificial intelligence: the new frontier in cybersecurity (AI:サイバーセキュリティの新たなフロンティア)
  - B.1.1 Artificial Intelligence in the world of Internet of Everything (全てのインターネット(IoE)の世界におけるAI)
  - B.1.2 A few applications of AI today (今日のAIのアプリケーション)
  - B.1.3 Research for an explainable robust and safe AI (説明可能な堅牢かつ安全なAIのための研究)
  - B.1.4 Adversarial machine learning intelligence and the challenge to recognize the unknowns (敵対的機械学習インテリジェンスと未知の認識への挑戦)
  - B.1.5 Artificial intelligence and ethics (AIと倫理)
- B.2 Quantum technology (量子技術) ←
- B.3 Complexity, cascade effect and supply chain threat (複雑さ、カスケード効果、サプライチェーンの脅威)

量子コンピューティングを利用した攻撃への耐性を提供する技術的手法 (耐量子計算機暗号、耐量子安全性暗号(QSC)) および量子鍵配送に代表される量子効果を利用する技術的手法

- B.4 Cybercrime: Detection, Mitigation and Attribution of attacks against Cyber threats (サイバー犯罪: サイバー脅威に対する検知、軽減、攻撃の属性)
- B.5 Privacy threat and the innovation brought by the GDPR (プライバシーの脅威とGDPRによってもたらされるイノベーション)

Annex C: Methodology, policy context and R&D funding scheme

- (方法論、政策的背景、研究開発ファンディングスキーム)
- C.1 Methodology used in the report (レポートで使用された方法論)
- C.2 European Policy Context (欧州政策の背景)
- C.3 R&D activities and funding schemes (研究開発活動とファンディングスキーム)

出所: ホームページ

<https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity>  
※翻訳および注釈は事務局にて付記したもの

英国

Interim Cyber Security Science & Technology Strategy (暫定サイバーセキュリティ科学技術戦略) [2017年11月 英国政府 内閣府]

目次

Introduction (はじめに)

Our Approach (我々のアプローチ)

Scope and Structure of this Document (ドキュメントの範囲と構造)

Part 1: IDENTIFY Emerging Technologies and Trends (新興技術とトレンドの同定)

Key Technology Trends (鍵となる技術トレンド)

Internet of Things (IoT) and Smart Cities (IoT とスマートシティ) サイバーセキュリティの脅威の特定と  
対処に重要なツールとしてAIを活用

Data and Information (データと情報)

Automation, Machine-learning and Artificial Intelligence (AI) (自動化、機械学習、AI)

Human Computer Interaction (人間とコンピュータの相互作用) 量子技術や Fintech を含む

Other Technologies and Our Ongoing Response (その他の技術と継続的対応)

Risks and Opportunities (リスクと機会)

Risks (リスク)

Opportunities (機会)

パート1で多くの重要な新興技術を、学会、業界、技術者、英国政府の科学技術コミュニティ等の専門家と相談した結果をもとに同定し、パート2で、これら新興技術トレンドに対する幾つかの初期的な政策対応を開発

Part 2: DEVELOP Policy Response to these Emerging Technology Trends

(これら新興技術トレンドへの政策対応の開発)

Growth and Innovation (成長とイノベーション)

Creating Secure, Trusted Technologies (セキュアで信頼できる技術の作成)

Focus: Connected Medical Devices (接続された医療機器)

Focus: Connected and Autonomous Vehicles (接続された自動運転車)

Skills (技量)

Focus: Smart Cities (スマートシティ)

Helping Individuals and Organisations Secure Themselves (個人や組織による自助の支援)

Government Security (政府のセキュリティ)

Part 3A: Creating a Single Authoritative UK Government Voice for Cyber Security Science and Technology (サイバーセキュリティの科学技術に対する英国政府の一つの機関の構築)

Part 3B: UK Capability and EXPERTISE (英国の能力と専門知識)

Part 4: ASSESS Our Performance (パフォーマンスの評価)

出所: ホームページ

<https://www.gov.uk/government/publications/interim-cyber-security-science-and-technology-strategy>

※翻訳および注釈は事務局にて付記したもの