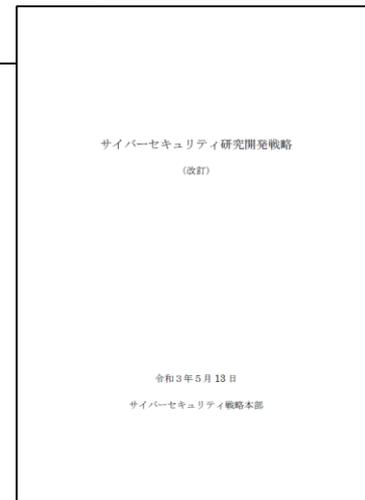


「サイバーセキュリティ研究開発戦略（改訂）」（概要）

令和3年(2021年)5月13日
サイバーセキュリティ戦略本部決定

○研究開発に関わる幅広い層（政府機関から研究者まで）を対象として、将来的なサイバーセキュリティ研究開発を検討・推進するためのビジョン（基本的な考え方や方法論など）を提示。



【目次】

- はじめに
- 近い将来の情報通信技術（IT）の利活用を想定した研究開発
 - 基本的な考え方**
 - ビジネスのプロセス全体を視野に入れることが重要
（セキュリティ技術はあくまで一手段と考え全体を考慮した研究開発をすべき 等）
 - システム運用時に必要なサイバー攻撃の検知・防御だけでなく、ライフサイクル全体で捉えることが必要
（システムの企画・設計段階からセキュリティの確保を盛り込む 等）
 - セキュリティ技術だけでなく、多角的アプローチが重要
（様々な領域の研究との連携、融合領域の研究に取り組む 等）
 - 近い将来の情報通信技術（IT）の利活用
（IoT、AI、ネットワーク関連技術、量子技術の変化の流れを捉える必要 等）
 - セキュリティ研究開発における課題に対応した**方法論**
 - 国内外における産学官の連携と企業経営層のリーダーシップによる研究開発
 - 脅威に関する情報やユーザー等のニーズを踏まえた実践的な研究開発
 - サイバーセキュリティの研究開発に係る制度等の検討
 - オープン・クローズ戦略の推進
 - イノベーションの「シーズ」としての研究開発の推進
- 中長期を見据えた考え方
人文社会科学と様々な分野との協業により、情報システムだけでなく、社会や人間を一体として捉えることで、サイバーセキュリティ研究における新たなテーマや未知のテーマの発見やその広がりにつながる。
- 研究・産学官連携の推進方策と産学官エコシステムの構築
- まとめ
具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討。

令和3年5月改訂時 追加箇所

- 我が国の研究コミュニティの状況を踏まえた推進方策
 - 研究分野の国際動向と特徴
（情報系と同様、柔軟で優秀な「人材」が大きく研究を進展させ得る 等）
 - 人に投資すべき
（研究プロジェクトや産学共同研究費においてRA（リサーチアシスタント）経費の上限を柔軟に設定し、優秀な人材を迎える形態が必要 等）
 - 産学官連携の可能性
（インターネット企業やDXを進める企業の経営的かつ潜在的ニーズに応え得る産学共同研究が今後検討されるべき 等）
 - 研究コミュニティ全体の発展
（ファンディングの機会と研究費の活用、科学的基礎に係る概念の言語化、プロシーディング論文を含む柔軟な研究実績の評価 等）
- 我が国の強み・ポテンシャルと重点的な強化に向けて
 - 我が国の強みとポテンシャル
（IoTセキュリティ、データセキュリティ及びプライバシー保護など欧米に比肩、サイバー・フィジカル融合領域、暗号研究の強みを活かす領域にポテンシャル 等）
 - 重点的な研究領域
（重点的な強化が図られることが望ましい研究領域を整理）
- 研究コミュニティの継続的な取組