

- 2017年に、「**サイバーセキュリティ研究開発戦略**」を策定：研究開発に関わる幅広い層が研究開発を検討・推進する際のビジョン（基本的な考え方や方法論など）を整理。
 - 2018年に策定された「**現行のサイバーセキュリティ戦略**」に、その考え方を反映。（「研究開発の推進」として、実践的な研究開発の推進と、中長期的な対応の旨を盛り込み。）
 - 現行戦略の下で、現在、政府の研究開発に係る取組の具体化を図り、5つの方向性を推進。（2019年に、サプライチェーンリスクへの対応や、攻撃把握・分析・共有基盤の強化などを含む「研究・技術開発取組方針」を策定して推進。）
- その方向性の1つである「産学官連携の研究・技術開発のコミュニティ形成」については、研究開発戦略専門調査会及びそのワーキンググループにおいて具体化検討を行ってきたところ、今般、考え方や推進方策が整理。
 - これを受け、「**サイバーセキュリティ研究開発戦略**」に具体テーマに係るビジョンとして章を追記する改訂を行い、今後の関係府省による研究・産学官連携の推進の方向付けに資するとともに、本件を含め現行戦略の下で推進・具体化してきた方向性を「次のサイバーセキュリティ戦略」の検討に反映。

＜改訂の概要＞ ※ なお、既存の章については、内容に変更はなく、策定後の状況を踏まえた時点修正等を行っている。

（新章）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

研究・産学官連携の推進にあたっての考え方や推進方策を第4章として追記。

- ・柔軟で優秀な人材が大きく研究を進展させ得るため、研究費におけるリサーチアシスタント経費の活用と上限柔軟化等により、人に投資すべき。
- ・研究費を人に投入する相応規模の産学共同研究を検討。研究と産学官連携が相互に良い影響を与え発展するよう、研究等を推進。
- ・重点的な研究領域において、研究コミュニティの自主的な発展努力と相まって重点的な研究・産学官連携の強化を図る。など

今後の施策展開

① 関係府省における研究及び産学官連携振興施策の活用を促進し、産学官エコシステム構築に向けた取組を推進。

例）・研究費の活用「戦略的創造研究推進事業」：基礎研究を推進する科学技術振興機構（JST）の事業（令和3年度予算案額：427.9億円）。

令和3年度に研究を開始する戦略目標の1つとして、セキュリティ分野に関連する戦略目標が設定され、今後、研究が推進。

・内閣サイバーセキュリティセンター（NISC）において、産学官にわたるエコシステム構築が図られるよう、産学官の取組状況についてフォローアップ。

② このほか、上記方向性に基づく、関係府省の研究開発に係る取組を推進。

③ ①・②の、現行戦略の下で推進・具体化してきた方向性を「次のサイバーセキュリティ戦略」の検討に反映。

次期戦略期間において、関係府省の取組を促進するとともに、状況をフォローアップし、マッピングによる点検と必要な再整理を行う。

○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。

サイバーセキュリティ研究開発戦略

平成 29 年 7 月 13 日

サイバーセキュリティ戦略本部

【目次】

1. はじめに

2. 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

（1）基本的な考え方

- ① 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）
- ② 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）
- ③ 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）

（2）近い将来の情報通信技術（IT）の利活用

（IoT、AI、ネットワーク技術の変化の流れを捉える必要 等）

（3）セキュリティ研究開発における課題に対応した方法論

- ① 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
- ② 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
- ③ サイバーセキュリティの研究開発に係る制度等の検討
- ④ オープン・クローズ戦略の推進
- ⑤ イノベーションの「シーズ」としての研究開発の推進

3. 中長期を見据えた研究開発戦略

・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につながる。

4. まとめ

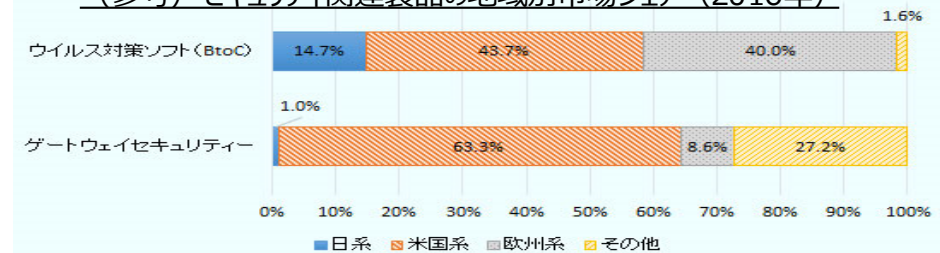
具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討。

「サイバーセキュリティ戦略」(平成30年(2018年)7月閣議決定)に基づき、戦略期間中の実践的な研究・技術開発に関する取組の具体化を図るという目的のもと、研究開発戦略専門調査会において「**サイバーセキュリティ研究・技術開発取組方針**」を策定。

取り組むべき課題

- (1) サプライチェーンリスクの増大
- (2) サイバーセキュリティ自給率の低迷
- (3) 研究・技術開発に資するデータの活用
- (4) 先端技術開発に伴う新たなリスクの出現
- (5) 産学官連携強化の必要
- (6) 国際標準化の必要

(参考) セキュリティ関連製品の地域別市場シェア (2016年)



(出典) 拡大するサイバーセキュリティ市場 (JETRO)
<https://www.ietro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html>

今後の取組強化の方向性

① サプライチェーンリスクへ対応するためのオールジャパンの技術検証体制の整備

- ICT機器・サービスの信頼性・有効性を検証するためのオールジャパンの体制整備
- ハードウェア・ソフトウェア両面の検証技術の研究開発・実用化 (5Gセキュリティ、チップ脆弱性検知、エッジからクラウドに至るまでのハードウェアセキュリティ)

② 国内産業の育成・発展に向けた支援策の推進

- 「Proven in Japan」の推進に向けた、日本発のサイバーセキュリティ製品・サービスの創出・活用及び信頼性を検証するための包括的検証基盤の構築
- 中小企業のニーズに対応したビジネス創出のための支援 (サイバーセキュリティお助け隊、コラボレーション・プラットフォーム)

③ 攻撃把握・分析・共有基盤の強化

- サイバー攻撃を迅速に把握するための観測技術の高度化や、AI等の活用による分析・解析技術の効率化・自動化 (NICTER、STARDUST等)
- サイバー攻撃の把握・分析データを共有する基盤 (CURE) 構築

④ 暗号等の基礎研究の促進

- 耐量子計算機暗号や量子暗号等の安全なセキュリティ技術、IoTデバイスにて活用可能な暗号技術の研究・開発
- 暗号技術、暗号・セキュリティ製品やモジュール認証等の国際標準化促進

⑤ 産学官連携の研究・技術開発のコミュニティ形成

- 産学官によるコミュニティの形成及び諸外国との連携に向けた検討

- 上記の取組強化の方向性に沿って、関係省庁が連携して、具体的・実践的な研究開発を推進
- 個別の研究・技術開発の成果の創出に留まらず、**社会実装までのプロセスを念頭に置きつつ推進**するとともに、**国民社会におけるサイバーセキュリティに関する意識向上**に向けた取組も併せて実施
- 研究開発戦略専門調査会において**定期的に評価**を行い、**必要に応じて方針の見直しを実施**

第1章 はじめに

若く伸びている研究分野

- ・国際的なトップカンファレンスへの論文投稿が2000年に比し約4倍以上。
- ・我が国でも、2010年代に主な研究集会への参加者数が2倍以上に成長。
(サイバー空間の拡大と実空間との融合を背景に、国際的に存在感が高い暗号研究コミュニティの継続的でオープンな発展努力と様々な分野からの研究人口の流入。)

コラボレーションが非常に活発

- ・国際的に、国際共著論文、産学官連携論文が増えている。中国の存在感が年々増大。
- ・デジタル活用とセキュリティ対策の一体性が深くなり、セキュリティに係るアカデミックな研究が、富や活力を生み出す源泉の両輪の一つと理解されている。



今は**産学官にわたるエコシステム**を構築する重要期 / 我が国における**デジタル化**と同時並行で進める必要

第2章 我が国の研究コミュニティの状況を踏まえた推進方策



エコシステム駆動に向けた循環の構築



2.1 研究分野の国際動向と特徴

- ・欧米では博士課程学生がフルタイムで給料を支払われ、貴重な研究戦力に。
- ・本分野では、情報系分野と同様、柔軟で優秀な「人材」が大きく研究を進展させ得る。
(コンピュータサイエンスを基盤とし、プログラミングや試行錯誤が多く必要となる点が特徴。)

2.2 人に投資すべき

- ・博士課程では、本分野でも、専門分野の知識・方法論の修得が基本だが、一定の実社会経験が重要。
(インターンや産学共同研究など。セキュリティの現場とデジタルの現場の両面で機会の創出・拡大が望ましい。)
- ・リサーチアシスタント(RA)経費の有効活用と上限柔軟化が重要。
(研究プロジェクトや産学共同研究費にて、RA経費で優秀な博士課程学生を迎えて大きく研究を進める。上限の柔軟な設定・運用が非常に重要。そのための人材公募も。)
- ・RA経費の活用で、社会人を含む博士課程進学の様々な形態を可能に。
(さらに、次世代にとってのキャリアパスの魅力向上と博士人材のキャリア形成支援に取り組む。研究室を越えてコンソーシアム的に取り組むことが効果的かつ重要。)

2.3 産学官連携の可能性

- ・連携相手は潜在的に多い。欧米では相応規模のデータや研究費の授受を伴う共同研究。我が国でも、研究費を人に投入する産学共同研究が今後検討されるべき。
(通信事業者、ITベンダー企業、セキュリティベンダー企業に加え、インターネット企業やDXを進める様々な企業等を連携相手とし、経営的かつ潜在的なニーズに応え得る研究構想が重要。)
- ・アカデミア発ベンチャーも、一つの産学官連携の形態として注目される。

2.4 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が重要。
(国やファンディング機関の企画立案に当たり、研究コミュニティの状況や動向が良く踏まえられることで、活発な提案申請がなされやすい。本分野の研究コミュニティの活力や様々な研究構想を結びつけていくことが重要。)
- ・科学的基礎の構築、プロシーディング論文を含む柔軟な研究実績の評価
(他分野や実社会との協働において科学的手法が提供できる価値の中心的概念を言語化。情報・セキュリティ系分野では重要なプロシーディング論文も、ファンディング申請等で研究実績に含まれる旨を明確化するべき。)
- ・研究者や研究機関の国際交流・国際展開を活発に行うことが重要。
(海外武者修行を含めた国際的に活躍する若手研究者の育成や国際共同研究の振興等に取り組む。)

第3章 我が国の強み・ポテンシャルと重点的な強化に向けて

3.1 我が国の強みとポテンシャル

- ・IoTセキュリティやデータセキュリティ・プライバシー保護など米欧に比肩する研究領域がある。
- ・Society 5.0の実空間・サイバーの融合領域に係る研究領域、暗号研究の強みを活かした研究領域等には、ポテンシャルとして強みがある。

3.2 重点的な研究領域

- ・上記を踏まえ、知的価値及び社会的価値・経済的価値への寄与が大きいと考えられる等の理由で、重点的な強化が図られることが望ましい研究領域は以下の通り。
(※研究者の自由な発想に基づく研究も、発想・学理・シーズの源泉として引き続き重要。)

安全・安心な 社会基盤	デジタルインフラ（IoT、5G、クラウド等）セキュリティ データセキュリティ・プライバシー保護	サプライチェーンセキュリティ 実装セキュリティ（ハードウェアセキュリティ含）	
将来を見据えて 取り組むべき分野	AIセキュリティ	自動車セキュリティ	
攻撃者優位を覆し 先手を打つアプローチ	攻撃の視点から知見を得る （オフェンシブセキュリティ）研究	実データの観測・分析 に基づく研究	人的要素 セキュリティ

産学官の様々なステークホルダーから期待を持ってもらうため、具体例を提示。
(※今後適時リバイス・ビボットされ得る。他にも新たな構想が生まれてくることを奨励・歓迎。)

3.3 研究構想の具体例

- ◆DFFT (信頼ある分散型データ活用) 研究
 - A 社会的・経済的データ共有・分析基盤
 - B 攻撃観測データ共有・分析基盤
 - C 共通技術の深化・高度化
DFFT: 信頼性のある自由なデータ流通
- ◆人工知能セキュリティ研究
 - A 機械学習のCIA確立
 - B 機械学習のセキュリティ技術への応用
CIA: 信頼性セキュリティの重要3要素

3.4 産学共同研究構想の具体例

- ◆サービスのセキュリティ強度評価手法
大学 × インターネット企業/ユーザ企業
- ◆ソフトウェア堅牢化手法の有効性研究
大学 × ソフトウェア開発企業
- ◆端末利用者のリスク低減研究
大学 × セキュリティベンダー企業

第4章 むすびと今後の展望

- ・我が国のサイバーセキュリティ研究開発の国際競争力を躍進させるため、産学官エコシステムの構築を中心ビジョンとして、課題解決を実現するための方策を多角的に議論、整理。
- ・本WGの取組をきっかけとして、今後も議論・意見交換が持続的になされていくことを期待。

【参考④】JST戦略的創造研究推進事業

○文部科学省が定めた戦略目標の下、組織・分野の枠を越えた時限的な研究体制を構築し、イノベーションの源泉となる基礎研究を戦略的に推進する科学技術振興機構（JST）の事業（令和3年度予算案額：427.9億円）。

例） CREST 対象：チーム型研究、研究期間：5.5年以内、総額：1.5～5億円程度／チーム

さがけ 対象：個人型研究、研究期間：3.5年以内、総額：3～4000万円程度／課題

○JSTに係る令和3年度戦略目標の7つのうち1つとして、セキュリティ分野に関連する「Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術」が定められた。

Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術

多様な情報システムや大量のデータを使いこなして、質の高い豊かで安心な生活を実現するSociety 5.0時代には、“データの漏えい・流出”や“なりすまし”、“プライバシーの侵害”等の多くの危険が存在

⇒ 情報基盤分野の研究者の力を結集し、日本発の基盤ソフトウェア技術で安心・安全・信頼を確保

なぜ、基盤ソフトウェア技術？

- デジタル化への急速な流れ
- ・デジタル庁の創設
 - ・コロナ新時代の新たなライフスタイルへの移行
 - ・Society 5.0の早期実現

しかし、我が国は・・・

デジタル化のためのハードウェア、OS、クラウド等の大部分を海外に依存
→ リスク管理も海外依存となってしまっているのか？

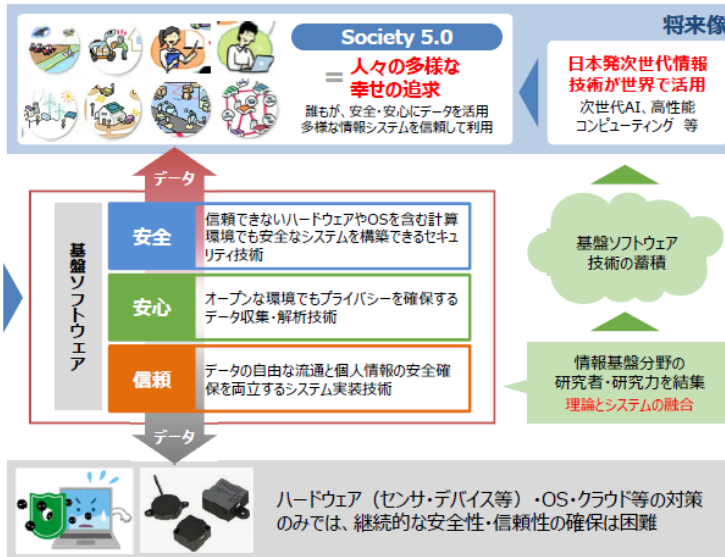
そこで、

- 情報基盤分野の研究力を再強化
- ・研究コミュニティの再構築
 - ・理論とシステムの研究者の連携



日本発の基盤ソフトウェア※で課題解決
・クラウド等の対策のみに頼らず、データや情報システムの安心・安全・信頼を確保

※基盤ソフトウェア＝アプリとクラウド等を繋ぐソフトウェア



※ 具体的な研究例

(1) 信頼できないハードウェアやOSを含む計算環境で安全なシステムを構築可能とするセキュリティ技術の創出

- ・OSの権限分散・階層化等による安全性指向コンピュータアーキテクチャ技術
- ・信頼できる隔離実行環境の構築技術（次世代TEE等）
- ・エッジからクラウドまでの総合的なセキュリティを実現するセキュアOS技術
- ・安全な実行環境を実現するための形式検証技術

(2) オープンな環境でもプライバシーを確保するデータ収集・解析技術の創出

- ・準同型暗号やマルチパーティ計算等の秘密計算によるトラスト確保技術
- ・相互に信頼できる範囲や開示レベルを動的に制御可能な分散認証技術
- ・差分プライバシーやローカル差分プライバシーを用いた分散データ収集・解析技術

(3) データの自由な流通と個人情報の安全性確保を両立するシステム実装技術の確立

- ・様々な実行環境（CPU、OS、仮想化）からなる分散データ処理環境の管理・制御技術
- ・セキュリティ・プライバシー処理の高性能実装技術
- ・データの真正性証明や来歴保証技術
- ・ハードウェアの直接監視によるソフトウェア実行時の異常・攻撃検知