資料2-1

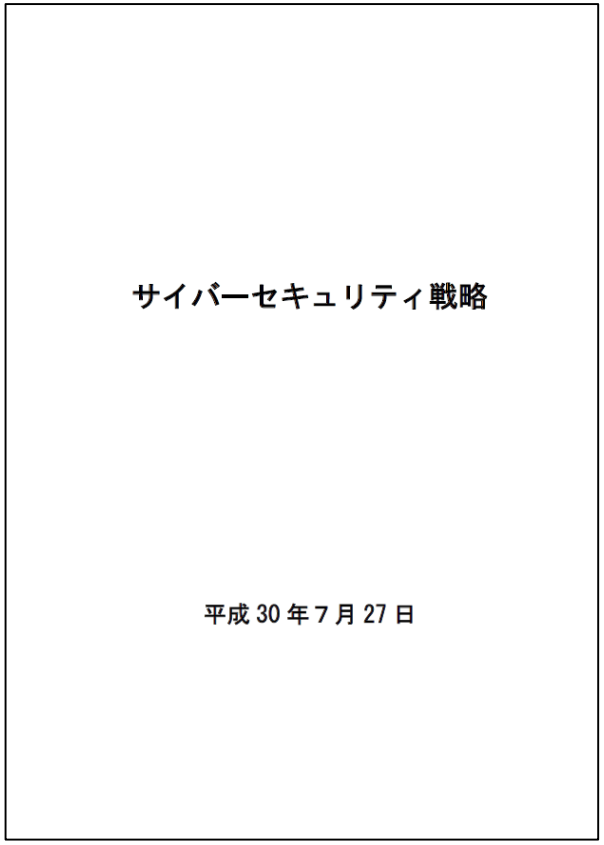
我が国における研究開発の推進に関する検討の方向性について

令和2年11月25日
サイバーセキュリティ戦略本部　研究開発戦略専門調査会

内閣サイバーセキュリティセンター（NISC）

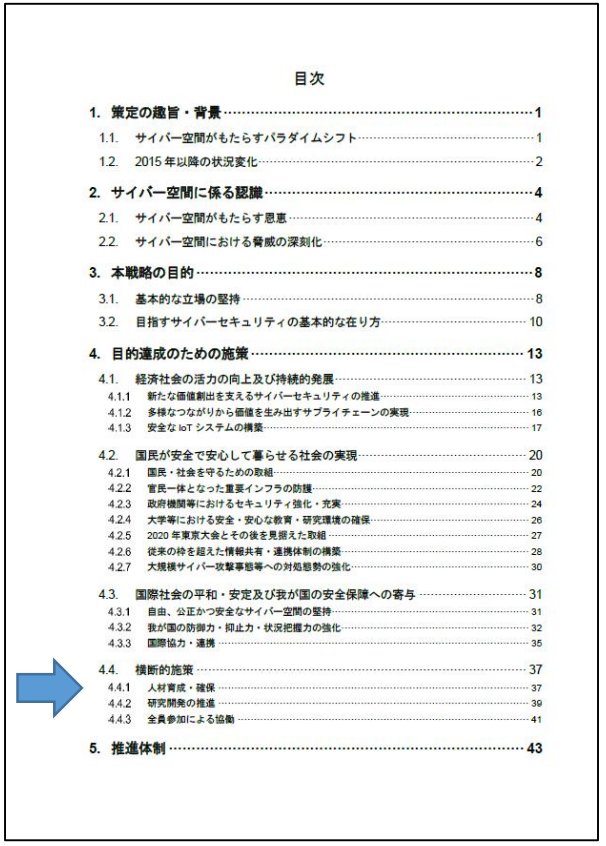
新しい「サイバーセキュリティ戦略」に向けた検討

- 現行の「サイバーセキュリティ戦略」の閣議決定から2年余りが経過。「3年間の諸施策の目標及び実施方針」を示す文書であるところ、新しい「戦略」に向けた検討を開始するタイミング。
- 本日は、**「今後の研究開発の推進に関する検討の方向性」について、ご議論をいただきたい**。



サイバーセキュリティ戦略

平成 30 年 7 月 27 日



目次

本戦略は、こうした今後のサイバーセキュリティに係る我が国としての基本的な立場や在り方を明らかにするとともに、今後３年間の諸施策の目標及び実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるものである。

「1. 策定の趣旨・背景」より抜粋

【参考】「サイバーセキュリティ戦略」

平成30年(2018年)7月27日
閣議決定

4.4. 横断的施策

4.4.2　研究開発の推進

(1)　実践的な研究開発の推進

(2)　中長期的な技術・社会の進化を視野に入れた対応

4.4. 横断的施策

「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安定及び我が国の安全保障」の３つの政策目標を達成するためには、その基盤として、横断的・中長期的な視点で、人材育成や研究開発に取り組むとともに、サイバー空間で活動する主体としての国民一人一人が、サイバーセキュリティに取り組む

4.4.2　研究開発の推進

サイバー空間と実空間が一体化していく中、サイバー空間におけるイノベーションの進展とそれに対するサイバー攻撃の脅威を踏まえた、実践的なサイバーセキュリティの研究開発が必要である。併せて、中長期的な技術・社会の非連続的進化を視野に入れた対応も必要である。

(1)　実践的な研究開発の推進

39

一方で、こうした技術の活用は、これまでになかった新たな脆弱性を生む可能性がある。このため、AI、ブロックチェーンなどの先進的な技術を用いたサイバーセキュリティ確保の技術、製品・サービスを構成するシステムの中に組み込むセキュリティ技術や、その組み込みの方法に関する実践的な研究開発について重点的に取り組む。特に、サプライチェーンにおける価値創出のプロセスにおける信頼の創出や証明、トレーサビリティ（追跡可能性）の確保とこれらに対する攻撃の検知・防御に関する研究開発を進めるほか、機器に組み込まれた不正なハードウェアやソフトウェアを効率的に検出する技術開発、プラットフォームにおいて利用者の意図しない動作を生じさせるおそれがあるときにもデータや情報の真正性・可用性・機密性を確保するための研究開発を行う。

また、我が国が、サイバー攻撃に対する検知・解析能力を含むサイバー空間の状況把握能力を高め、防御等の対処能力や強靭性の確保等サイバー空間における安全保障の確保にも資する研究開発を推進する。具体的には、政府機関や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃活動を把握することや、ネットワーク上の脆弱なIoT機器の調査のための広域ネットワークスキャンの軽量化を目指した研究開発等を進める。こうした研究開発の実施においては、セキュリティを運用する現場のサイバー攻撃に関する知見をいち早く共有することによって、その知見を研究開発に活かすとともに、研究開発の成果をいち早くセキュリティを運用する現場で活かすといった好循環のサイクルを形成することが重要である。このため、セキュリティ運用を行う事業者と、国の研究機関等とのリアルタイムでの情報共有を推進する。

さらに、政府機関や重要インフラ事業者等のシステムに組み込まれている機器やソフトウェアについて、必要に応じて、不正なプログラムや回路が仕込まれていないことを検証できる手段を確保することが重要である。このため、国が中心となって、必要な技術的検証を行うための体制の整備を図るとともに、そのために必要となる研究開発に取り組む。加えて、計算機技術の発展（例：量子コンピュータ、AI）を意識した暗号技術など安全保障の観点から国として維持することが不可欠な基盤技術についても研究開発を推進する。

例えば、サイバーセキュリティ対策における制度上の課題に関

40

する調査・研究を推進

これらのサイバー

会実装を推進する。

報発信を行いつつ、

実施や研究成果の国

(2)　中長期的な技術・

サイバー空間と実空

によ

る

野に入れて、サイバー

科学的視点、さらに

の研究との連携、融

の成果が人間社会に悪影響を及ぼすものであってはならないということは言うまで

もない。

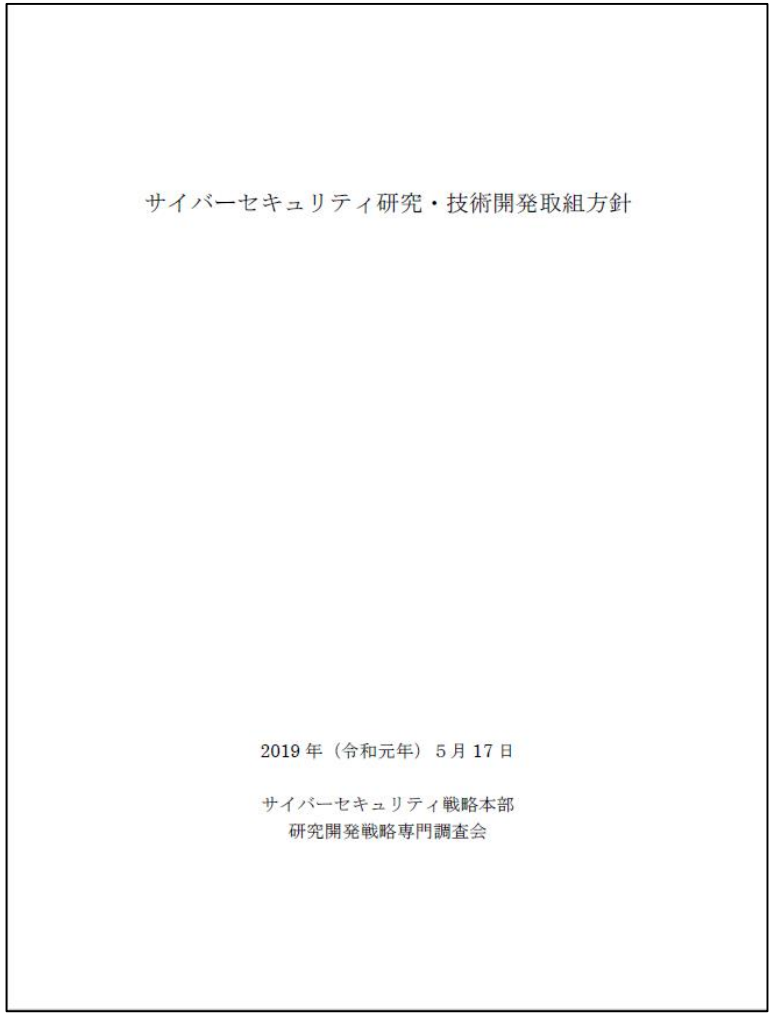
担当府省庁一覧（注）

項目	担当府省庁 （◎：主担当、○：関係府省庁）
4.1.　経済社会の活力の向上及び持続的発展	
4.1.1　新たな価値創出を支えるサイバーセキュリティの推進	
(1)　経営層の意識改革	◎：NISC[87]、経済産業省 ○：金融庁
(2)　サイバーセキュリティに対する投資の推進	◎：総務省、経済産業省
(3)　先端技術を利用したイノベーションを支えるサイバーセキュリティビジネスの強化	◎：経済産業省 ○：総務省
4.1.2　多様なつながりから価値を生み出すサプライチェーンの実現	
(1)　サイバーセキュリティ対策指針の策定	◎：経済産業省
(2)　サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築	◎：内閣府 ○：総務省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(3)　中小企業の取組の促進	◎：NISC、総務省、経済産業省
4.1.3　安全なIoTシステムの構築	
(1)　IoTシステムにおけるサイバーセキュリティの体系の整備と国際標準化	◎：NISC、総務省、経済産業省
(2)　脆弱性対策に係る体制の整備	◎：NISC、警察庁、総務省、経済産業省
4.2.　国民が安全で安心して暮らせる社会の実現	
4.2.1　国民・社会を守るための取組	
(1)　知見の共有・政策調整	◎：NISC、警察庁、総務省、経済産業省、防衛省 ○：法務省
(2)　事故対応等に係る国際連携の強化	◎：NISC、経済産業省 ○：警察庁、外務省
(3)　能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省
4.4.　横断的施策	
4.4.1　人材育成・確保	◎：NISC ○：総務省、文部科学省、経済産業省
(1)　戦略マネジメント層の育成・定着	◎：NISC、文部科学省、経済産業省
(2)　実務者層・技術者層の育成	◎：警察庁、総務省、文部科学省、厚生労働省、経済産業省、防衛省 ○：NISC
(3)　人材育成基盤の整備	◎：総務省、文部科学省、経済産業省
(4)　各府省庁におけるセキュリティ人材の確保・育成の強化	◎：NISC、総務省 ○：その他の府省庁
(5)　国際連携の推進	◎：NISC、経済産業省
4.4.2　研究開発の推進	
(1)　実践的な研究開発の推進	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(2)　中長期的な技術・社会の進化を視野に入れた対応	◎：NISC ○：その他の府省庁
4.4.3　全員参加による協働	◎：NISC、総務省、文部科学省、経済産業省 ○：法務省
5.　推進体制	◎：NISC、内閣官房 ○：総務省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）

※本文抜粋は【参考資料1】を参照。

政府の取組の具体化・強化に向けた対応状況

- 昨年5月に、「政府の取組の具体化及び強化を図る」ことを目的として、「サイバーセキュリティ研究・技術開発取組方針」を策定。この方向性に沿って、関係省庁が連携して、実践的な研究開発を推進している。
- 新しい「戦略」では、**本「取組方針」で示した方向性について位置付け**を行う必要性がある。



サイバーセキュリティ研究・技術開発取組方針

2019 年（令和元年）５月 17 日

サイバーセキュリティ戦略本部
研究開発戦略専門調査会

はじめに

○　平成 30 年 7 月に閣議決定された新たな「サイバーセキュリティ戦略」（以下、「戦略」という。）において、研究開発は、サイバーセキュリティを支える基盤的取組として位置付けられている。

○　研究開発戦略専門調査会においては、戦略に基づき、サイバーセキュリティに関する実践的な研究・技術開発の具体的な推進方策に関する検討を行うため、我が国の取組の現状、諸外国の動向、取り組むべき方向性や方策について議論を行った。

○　本取組方針は、同専門調査会における議論を踏まえ、戦略期間中における政府の取組の具体化及び強化を図るものである。

「サイバーセキュリティ研究・技術開発取組方針」より抜粋

【参考】「サイバーセキュリティ研究・技術開発取組方針」（概要）

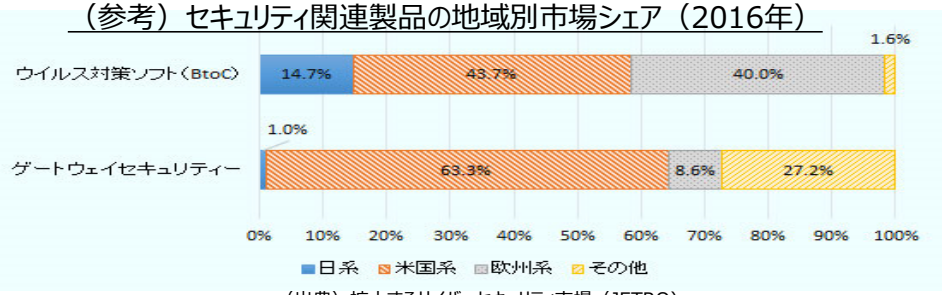
令和元年(2019年)5月17日
サイバーセキュリティ戦略本部
研究開発戦略専門調査会

「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.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html

今後の取組強化の方向性

（１）実践的な研究開発の推進

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

（２）産学官にわたるエコシステムの構築

・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**

※ 取組状況は【参考資料2】を参照。

今後の研究開発の推進に関する検討の方向性【1/2】

（１）実践的な研究開発の推進

➢ サプライチェーンリスクの増大やサイバーセキュリティ自給など、安全保障の観点を含め我が国を取り巻く現下の課題認識に基づき策定された**「サイバーセキュリティ研究・技術開発取組方針」の取組強化の方向性を、「サイバーセキュリティ戦略」の中に位置付け**、以下の4つの方向性については、実践的な研究開発の推進として取組を進めていくこととしてはどうか。

①サプライチェーンリスクに対応するためのオールジャパンの技術検証体制の整備

不正なプログラムや回路が仕込まれていないことを確認するためのソフトウェア・ハードウェア両面の検証技術の研究開発・実用化を推進するとともに、サプライチェーン全体の信頼確保に向けた、ICT機器・サービスのセキュリティの技術検証を行うための推進体制を、政府一体となって整備する。

②国内産業の育成・発展に向けた支援策の推進

サイバーセキュリティ産業の育成・発展を目指し、製品・サービスを安心して利用するための検証基盤や、中小企業のニーズに対応したビジネス創出など国内産業のビジネス環境を整備するとともに、市場展開のための枠組みを確立する。

③攻撃把握・分析・共有基盤の強化

サイバー攻撃の巧妙化・複雑化・多様化や、IoT機器の普及に伴う脆弱性拡大等のサイバー攻撃の脅威動向に適切に対処するため、AI等の先端技術も活用しつつ、サイバー攻撃の観測・把握・分析技術や情報共有基盤を強化する。

④暗号等の研究の推進

量子コンピュータの実現による既存の暗号システムの危殆化を想定しつつ、耐量子計算機暗号や量子暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立する。また、IoT等のリソースの限られたデバイスにおいても、安全な通信が可能となるよう、軽量な暗号技術を確立する。

（２）産学官にわたるエコシステムの構築

● 「サイバーセキュリティ研究・技術開発取組方針」の方向性のうち、「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、今回、「研究・産学官連携戦略ワーキンググループ」の検討を通じて深堀りが行われた。

➢ **「サイバーセキュリティ戦略」においても新たに項を設け**、「産学官の関係者が連携し、相互の取組の情報共有や研究活動における連携を図るためのエコシステムの構築に向け、基礎となる体制を整備する」ことを推進してはどうか。

今後の研究開発の推進に関する検討の方向性【2/2】

（３）中長期的な技術トレンドを視野に入れた対応

- 研究開発の推進にはIT関連技術の進展に応じた観点も重要と考えられる。
- 中長期的な視点から技術トレンドを捉え研究開発を推進していくことが重要であり、特に、**AI技術・量子技術の進展を見据えた対応が求められる**のではないか。
- それぞれの技術進展に関し、**以下のような状況認識に基づいて、取組を推進していく**必要性があるのではないか。

①AI（人工知能）技術の進展を踏まえた対応　（※資料2-2参照。ここでのAIは機械学習のことを指している。）

AI（人工知能）技術は、近年、加速度的に発展しており、世界の至るところでその応用が進むことにより、広範な産業領域や社会インフラなどに大きな影響を与えている。サイバーセキュリティとの関係では、AIを活用したサイバーセキュリティ対策、AIを使ったサイバー攻撃、AIそのものを守るセキュリティの3つの観点があると考えられる。

まず、AIを活用したサイバーセキュリティ対策（AI for Security）では、実際にAIを利用したセキュリティ製品やサービスは既に商用化が進んでおり、国は、2019年に策定した「AI戦略2019」等に基づき、AIを活用した民間のサイバー対策を引き続き後押しするとともに、「予防」「検知」「対処」の各フェーズにおいてAIを活用した高効率かつ精緻な対策技術の確立を推進していく。

また、AIを使ったサイバー攻撃に対処する観点からも、攻撃者の防御側に対する非対称性をさらに拡げないために、AI for Securityの取組は重要となる。その際、攻撃の視点から知見を得て、先手を打ってセキュリティ対策を高度化するプロアクティブな研究のアプローチが重要であると考えられる。

さらに、AIそのものを守るセキュリティ（Security for AI）では、AIのセキュリティ面での脆弱性がどのようなものかまだ十分に理解されていないと考えられるところ、学術面では、例えば、機械学習の誤認識を誘発し得る敵対的サンプルの生成を試みる研究がなされる一方で、その防御の研究も海外では多くなっている。我が国においても基礎的な研究を振興するとともに、5年～10年先に実現を目指す長期的取組として引き続き検討を進める。

②量子技術の進展を踏まえた対応　（※「量子技術イノベーション戦略」（参照資料４）参照。）

量子コンピュータの進展により、現代のインターネットセキュリティを支える公開鍵暗号技術が解読される可能性が生じ、国際的に耐量子計算機暗号に関する検討が進められている※。一方、耐量子計算機暗号においても危殆化のリスクがあるため、米国や中国をはじめ、各国が安全保障にも関わる重大脅威との認識の下、原理的に安全性が確保される量子通信・暗号に関する研究開発を急速に進めている。

※我が国においても、2019年に策定した「サイバーセキュリティ研究・技術開発取組方針」に基づき、耐量子計算機暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立することとしている。

我が国としても、2020年に策定した「量子技術イノベーション戦略」に基づき、国及び国民の安全・安心の確保、産業競争力の強化等の観点から、重要デジタル情報を安全に保管する手段として、機密性・完全性等を有し、かつ市場化を見据えて国際競争力の高い、量子通信・暗号に関する研究開発や、その事業化・標準化等に取り組んでいく。