資料1-1

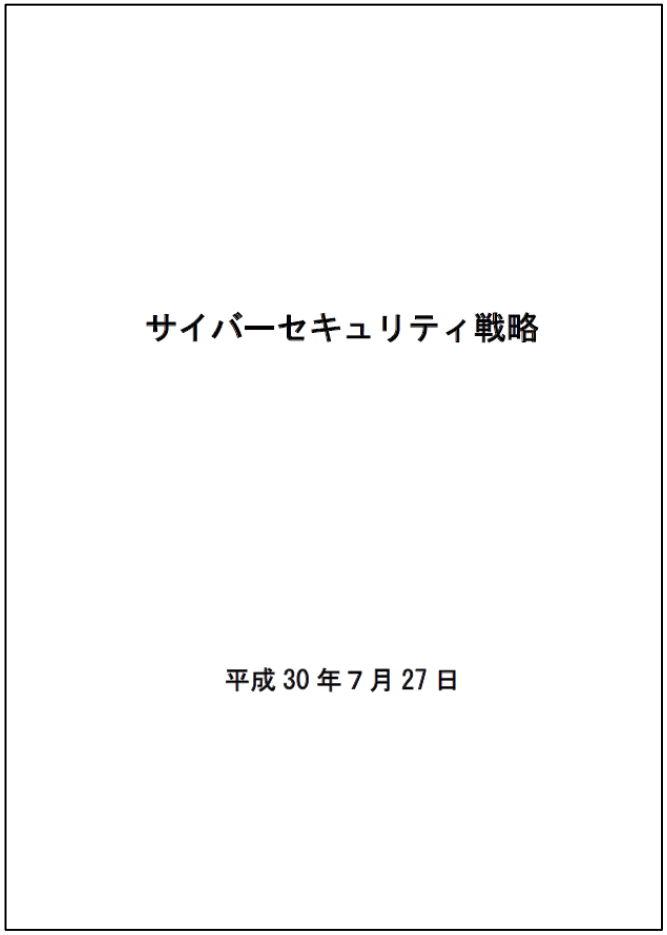
研究開発戦略専門調査会について

令和2年7月9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）

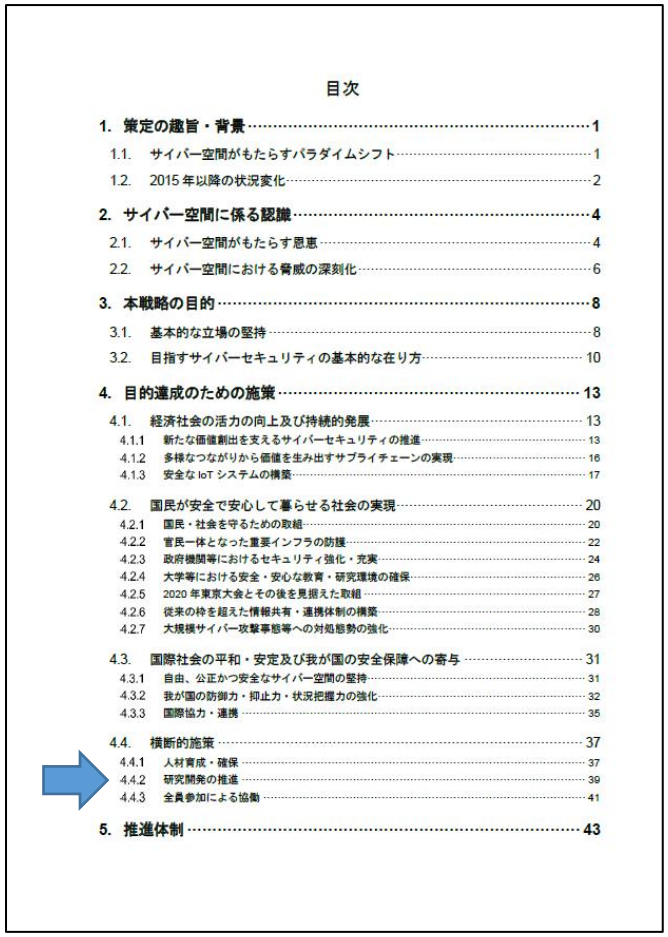
サイバーセキュリティ戦略

平成30年(2018年)7月27日
閣議決定



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

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

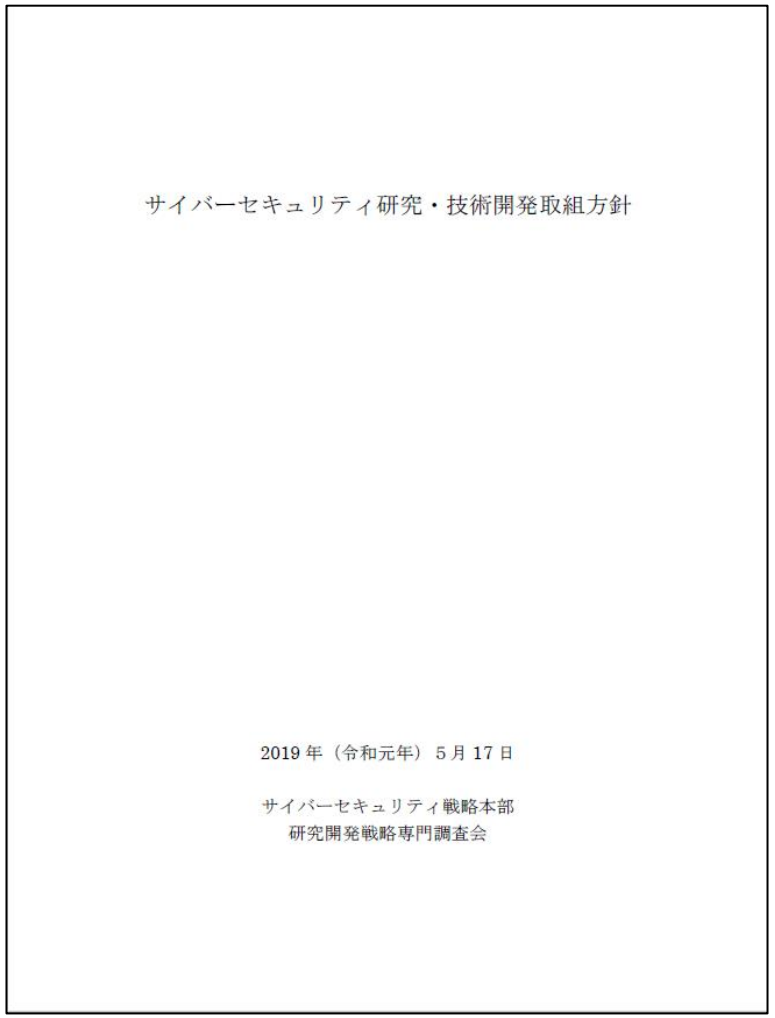
の研究との連携、融

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）

「サイバーセキュリティ研究・技術開発取組方針」



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

「サイバーセキュリティ研究・技術開発取組方針」（概要）

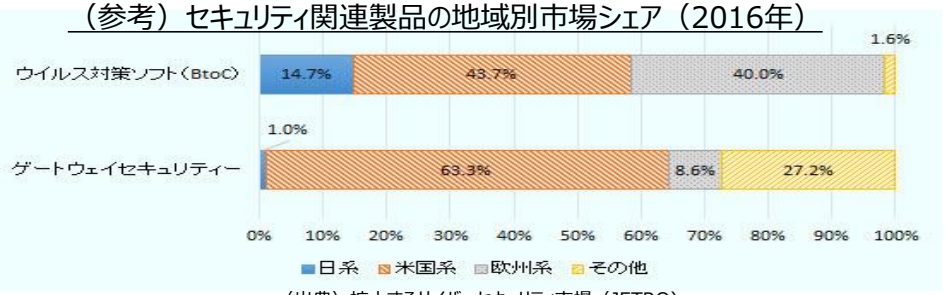
令和元年(2019年)5月17日
サイバーセキュリティ戦略本部
研究開発戦略専門調査会

「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

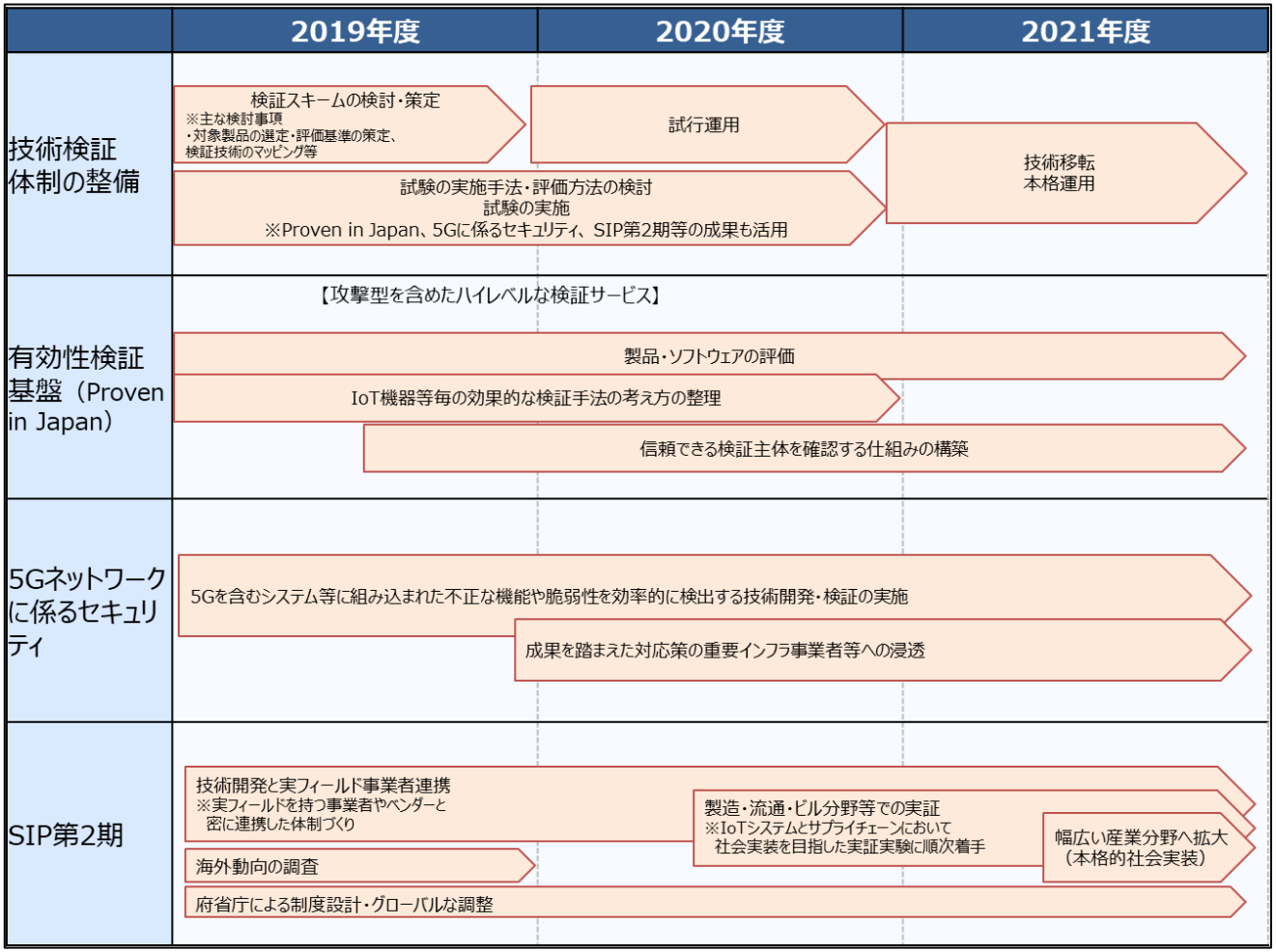
⑤産学官連携の研究・技術開発のコミュニティ形成

・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**

「サイバーセキュリティ研究・技術開発取組方針」の取組状況

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



2019年度は**技術検証に関する技術動向や諸外国の制度の状況について調査**を実施。
2020年度は**実際の製品に不正機能や当該機能につながりうる未知の脆弱性が存在しないかどうかに関する技術検証の取組を推進**。（NISC）

2019年度は**選定された製品の検証項目を策定**し**各製品の有効性評価のトライアルを実施**。
2020年度は**セキュリティ製品・サービスの有効性を検証する基盤の構築**及び**ビジネスマッチング**を実施。
（経済産業省）

2019年度は**5Gネットワークの仮想環境の基本部分を構築し、脆弱性評価・検証**を実施。
2020年度は**ソフトウェアを中心とした脆弱性、及びAIを活用したハードウェア脆弱性の検知手法に関する技術的検証を推進。**（総務省）

2019年度はSIP2期について、**基本方式の設計とデモシステムの開発を実施**。
2020年度は**研究開発を本格化し製造・ビル等の分野での実証実験**を開始。（内閣府）

➡ *取組が具体化し進んでいる*

「サイバーセキュリティ研究・技術開発取組方針」の取組状況

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

・我が国発のサイバーセキュリティ製品・サービスの創出・活用を促進するため、2019年度より**選定された製品の検証項目を策定**し**各製品の有効性評価のトライアルを実施**。2020年度は**セキュリティ製品・サービスの有効性を検証する基盤の構築**及び**トライアル検証を実施したセキュリティ製品・サービスのビジネスマッチング**を実施。（経済産業省）【再掲】

・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、地域SECUNITY）

・サイバーセキュリティお助け隊について、2019年度においては**実証事業を全国８地域で実施**。**約1,000社の中小企業が実証に参加**し、中小企業の実態・ニーズを明確化。2020年度も**地域実証を実施し、中小企業のサイバーセキュリティへの意識向上を図るとともに、中小企業の実態やニーズをよりきめ細かく把握**。2021年度以降に民間によるサイバーセキュリティ簡易保険含めた対策支援サービスの創出を目指す。（経済産業省）

・地域の関係者間でのセキュリティに関する「共助」の関係構築のためセキュリティ・コミュニティ（地域SECUNITY）の形成に向けた取組を実施。2019年度においては各地域においてセキュリティに関連するセミナー等を開催。2020年度も継続して各地域の総合通信局、経済産業局等と連携し開催。（総務省・経済産業省）

➡ *取組が具体化し進んでいる*

「サイバーセキュリティ研究・技術開発取組方針」の取組状況

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

・模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）について、 2019年度においては並列性向上や解析自動化等の高度化を図り、**攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発**を実施。2020年度も継続して本技術等の研究開発を実施。（総務省）

・巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、新たなハニーポット技術等の研究開発に基づく**サイバー攻撃観測技術の高度化**、機械学習等を応用した**通信分析技術**や**マルウェア自動分析技術**、さらに**アラート自動分析技術**の高度化等の**アドバンスト・サイバーセキュリティ技術の研究開発を実施**。 2020年度も継続して本技術等の研究開発を行う。 （総務省）

・サイバー攻撃の把握・分析データを共有する基盤構築

・2019年度においては、サイバーセキュリティ関連情報を大規模集約し、安全かつ利便性の高いリモート情報共有を可能とする**サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）を開発・実装**するとともに、**試験運用を実施**。2020年度は各種通信、マルウェア、脆弱性情報、イベント情報、インシデント情報等の**集約を更に進める**とともに、異種情報間の**横断分析等の更なる高度化を図り定常運用を開始**。 （総務省）

取組が具体化し進んでいる

「サイバーセキュリティ研究・技術開発取組方針」の取組状況

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

・2019年度は**暗号技術評価委員会及び暗号技術活用委員会を開催**し、**CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を実施**。**量子コンピュータ時代に向けた暗号の在り方検討タスクフォースを設置**し、大規模な量子コンピュータの動向を踏まえた次期CRYPTREC暗号リストに求められる要件等について検討を実施。2020年も引き続き活動を継続する。（総務省・経済産業省）

・**距離に依らない堅牢なグローバル量子暗号通信網の研究開発を実施**（研究開発期間は2020年度～2024年度）（総務省）

・**超小型衛星に搭載可能な量子暗号通信技術の研究開発を実施**（2018年度～2022年度）（総務省）

・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

・2019年度は、情報セキュリティに関する標準化を担当するISO/IEC JTC 1/SC 27のWG2コンビーナ、WG3副コンビーナとして、**暗号とセキュリティメカニズムの国際標準化について**中心的役割を担うとともに、**日本の意見を反映**。（経済産業省・IPA）

取組が具体化し進んでいるが
基礎研究の促進は引き続き必要

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

・2019年度は研究開発戦略専門調査会等を通じて、**国際的な研究動向や産学官連携事例について分析**を行うとともに、**研究コミュニティとの議論**を実施。（NISC）

これから更なる取り組みが必要