参考資料2

「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

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）

「サイバーセキュリティ研究・技術開発取組方針」（概要）

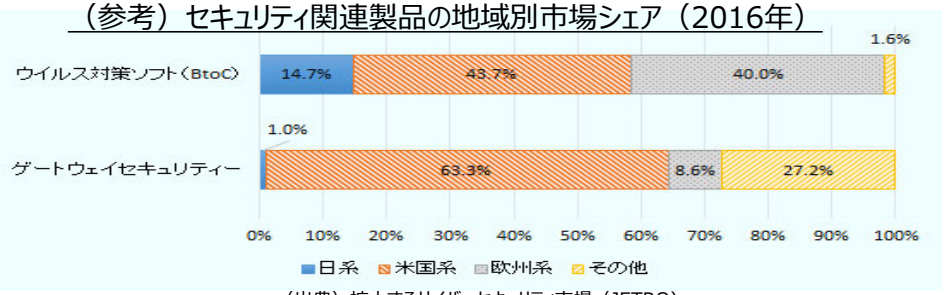
令和元年(2019年)5月17日
サイバーセキュリティ戦略本部
研究開発戦略専門調査会

「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

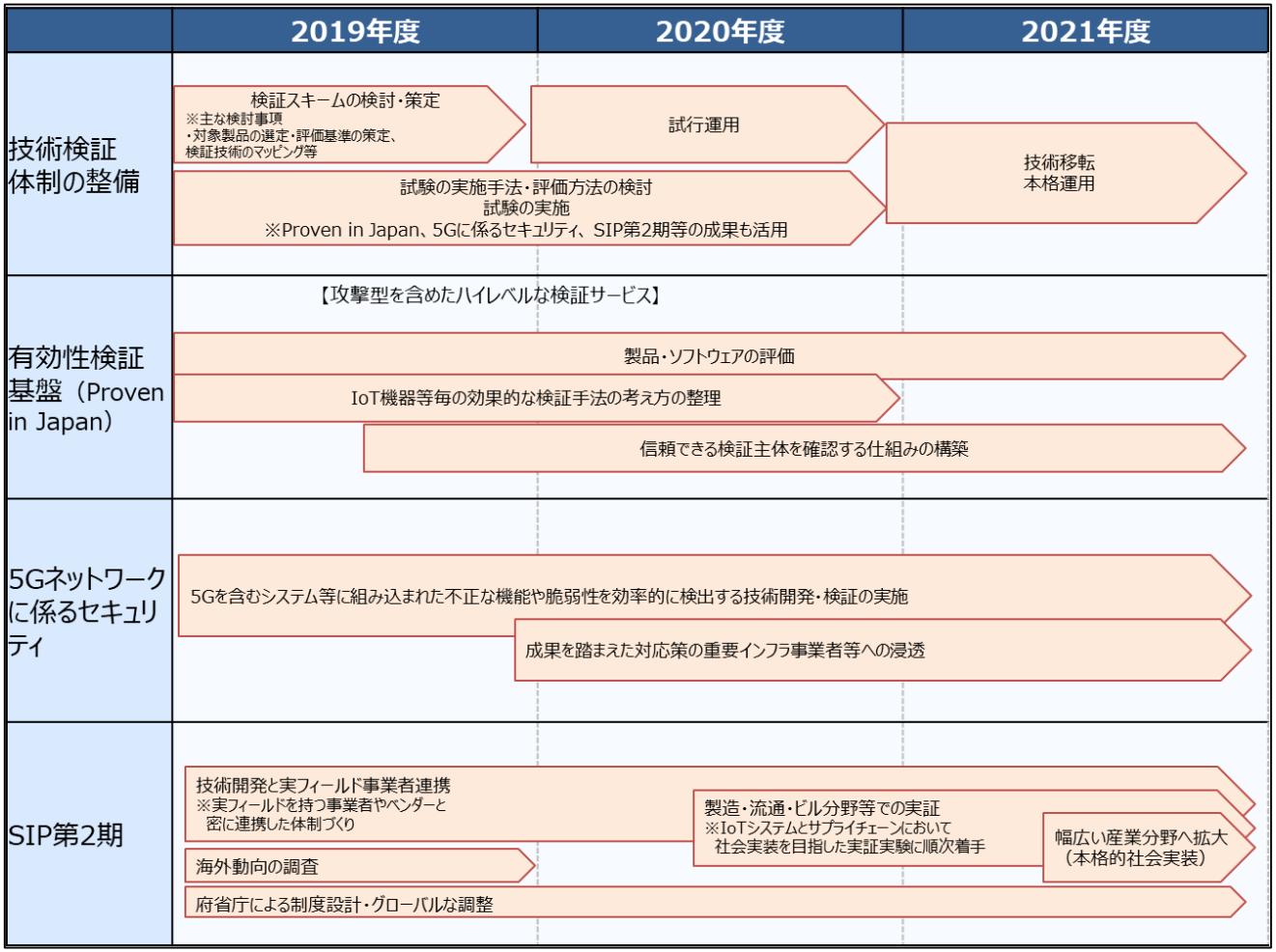
・上記の取組強化の方向性に沿って、関係省庁が連携して、具体的・実践的な研究開発を推進
・個別の研究・技術開発の成果の創出に留まらず、**社会実装までのプロセスを念頭に置きつつ推進**するとともに、**国民社会におけるサイバーセキュリティに関する意識向上**に向けた取組も併せて実施
・研究開発戦略専門調査会において**定期的に評価**を行い、**必要に応じて方針の見直しを実施**

「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

令和２年(2020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
第14回資料より抜粋

※赤字は、上記以降取組が進んだ箇所及び今後取組が考えられる箇所

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

令和２年(2020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
第14回資料より抜粋

※赤字は、上記以降取組が進んだ箇所及び今後取組が考えられる箇所

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**15チームが実証を実施し、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**。2020年度に設立されたサプライチェーン・サイバーセキュリティ・コンソーシアム等と連携し、2021年度以降は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・普及を推進していく。（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・2020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の開催や情報共有のための連絡会の立上げ等を実施。2021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

令和２年(2020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
第14回資料より抜粋

※赤字は、上記以降取組が進んだ箇所及び今後取組が考えられる箇所

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

令和２年(2020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
第14回資料より抜粋

※赤字は、上記以降取組が進んだ箇所
及び今後取組が考えられる箇所

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*

「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

令和２年(2020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
第14回資料より抜粋

※赤字は、上記以降取組が進んだ箇所及び今後取組が考えられる箇所

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。
2020年度は研究開発戦略専門調査会の下に「研究・産学官連携戦略ワーキンググループ」を設置し、「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」に向けた議論を数次にわたって行い「中間報告」をとりまとめるとともに、我が国の主な研究集会であるコンピュータセキュリティシンポジウムにおいて研究コミュニティとの意見交換を実施した。（NISC）

年度内に最終報告をまとめ、
コミュニティ形成に向けた取組を推進