サイバーセキュリティ研究・技術開発取組方針

（案）

2019 年〇月〇日

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

目次

「サイバーセキュリティ研究・技術開発取組方針」（案）

2019 年 5 月　日
サイバーセキュリティ戦略本部報告

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。

1．サイバーセキュリティを取り巻く環境

- 5G や AI、IoT 等の技術の進歩により、サイバー空間と実空間の一体化が進展し、Society5.0 の実現に向け、自動運転、キャッシュレスやスマートライフ等をはじめとした新たな製品・サービスが創出されることが想定される。（参考 1）

- 一方、サイバー攻撃は増加傾向にあり、その態様も複雑化・巧妙化・多様化している。（参考 2）また、新たな脅威（AI, IoT, 5G 等の新技術を用いたプラットフォームやサプライチェーンをターゲットにした攻撃等）の発生や攻撃者優位の拡大（新技術による環境の悪用による攻撃の巧妙化・大規模化等）も予測され、今後もその脅威は増大すると想定される。（参考 3, 4）

- サイバー攻撃の脅威の拡大に伴うリスクの増大により、サイバーセキュリティ製品・サービスの需要も高まっている。世界のサイバーセキュリティ市場は 2018 年に 1,530 億ドル、2022 年に 2,300 億ドルに達するとの予測もあり、我が国のサイバーセキュリティ市場も堅調に拡大を続けている。（参考 5）

- 一方、グローバルな市場における我が国のセキュリティ製品のシェアは低く、米国や欧州との差が開いている状況である。また、サイバー攻撃から守る対象と

なる情報システムや通信ネットワーク機器についても、欧米や中国企業のシェアが高い状態が続いている。（参考 5, 6）

- さらに、近年の企業における研究開発投資額は、米国の ICT 企業が上位を占めており、売上高に占める投資額が 10%を越えている例も多く見られるほか、中国 ICT 大手企業の投資額も拡大している。こうした企業においては、サイバーセキュリティも含めた投資が拡大している状況が見られる[1]。一方、我が国における研究開発投資額上位 10 位の企業における対売上高比 R&D 支出比率は、大半が 10%未満の状況であり、総じて低い状況となっている。（参考 7）

- サイバーセキュリティ分野で活躍している企業のランキング調査等においても、これまでのところ米国やイスラエルの企業が上位を占めているが、我が国においても、政府の支援策等により、サイバーセキュリティ製品・サービスを提供するスタートアップ企業が登場し始めている[2]。（参考 8）

2．我が国の研究・技術開発の取組の現状

サイバー空間と実空間の一体化、サイバー攻撃の脅威の増大、サプライチェーンの複雑化等がもたらすサイバーセキュリティ上の諸課題に対応するため、広範な要素技術に関する研究・技術開発が進められている。（参考 9）

- 産業界の取組

サイバー攻撃の動向や AI、IoT の進展等を踏まえ、各社において個別の取組が進められている。

例えば、情報通信サービスを提供している企業においては、5G や IoT 等の通信インフラを安全・安心に提供するための研究・技術開発に取り組んでいる（参考 10）。また、情報システムを提供している企業においては、情報システム及びそれを活用する重要インフラ等をサイバー攻撃から守るための先進的技術の研究・技術開発や、データ利活用ビジネスを推進するために必要となる研究・技術開発等が行われている。（参考 11）

- 学会・大学の取組

日本国内では、関連の学会等[3]において、各種セキュリティに関する研究発表が行

[1] 2018 年研究開発投資額 1 位(PWC Strategy& 2018 年グローバル・イノベーション 1000 調査結果より)の Amazon.com では、AWS のセキュリティ強化のため、暗号技術者を多数採用する等、サイバーセキュリティに対する積極的な投資活動が見られる。

[2] 法人向け不正アクセス検知サービスを提供しているカウリス社など

[3] 情報処理学会コンピュータセキュリティ協会主催のコンピュータセキュリティシンポジウムや電子情報通信学

われている。研究テーマとしては、暗号理論、セキュリティ応用、サイバー攻撃手法の順に多く、6 割強を占める。とりわけ、暗号については、海外の学会でも一定数の論文が採択されており、我が国が強みを有している分野であると言える[4]。（参考 12）

また、国内の大学においては、一定数の教員及び学生がサイバーセキュリティ分野に携わっているほか、一部の大学においては、情報セキュリティを専門に学ぶ学科も設立されている。これらの学科においては、情報数理・技術やマネジメント等の共通的な科目に加えて、ネットワークセキュリティに関する演習や、企業におけるインターンシップなど、実践的な教育が進められている。

- 政府の取組

新たな戦略において、実践的なサイバーセキュリティの研究・技術開発を進める分野として、以下の取組が盛り込まれている。

- AI、IoT 等の先進的技術を用いたサイバーセキュリティ確保、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
- サプライチェーンにおける信頼の創出や証明、トレーサビリティ確保とこれらに対する攻撃の検知・防御
- 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の効率的な検出、不正なプログラムや回路が仕込まれていないことの検証を行うための体制整備
- 模擬的ネットワークに攻撃者を誘因することによる攻撃活動の把握、ネットワーク上の脆弱な IoT 機器の調査、広域ネットワークスキャンの軽量化
- 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
- 研究開発成果の普及や社会実装の推進、国際的な情報発信、国際標準化

３．取り組むべき課題

近年のサイバーセキュリティに関する脅威の拡大や、我が国の研究・技術開発の動向を踏まえ、以下のような課題が顕在化している。これらの課題に対処していくため、戦略を踏まえた、さらなる取組の具体化や強化が求められている。

(1) サプライチェーンリスクの増大

○　サイバー空間と実空間の一体化の進展や、サプライチェーンのグローバル化により、サプライチェーンリスクの増大が大きな課題となっている。特に、製品やサービスを製造・流通する過程において、不正なプログラムやファームウ

会主催の暗号と情報セキュリティシンポジウムなど

[4] Crypto2018 にて 6 件の論文が採択されている。

ェアの組込み・改ざんが行われるリスクへの対応など、サプライチェーンにおけるサイバーセキュリティ対策の強化が求められている。

○　今後は、一定水準のセキュリティ要件を満たさない事業者、製品、サービスが、国際的な調達要件に適合しなくなる恐れもある[5]。このような観点から、輸出の大部分を占める製造業の参入機会を確保することも重要な課題となる。

○　こうした中、これまで、ソフトウェアのセキュリティを中心に、サプライチェーン全体のセキュリティ確保に必要となる技術の研究開発が進められてきている[6]。一方、最近ではハードウェアに悪意のある機能が組み込まれる懸念も増しており、今後はこれらの取組のいっそうの強化を図るとともに、これに加えて、チップや回路レベルでのハードウェアのセキュリティ確保の研究も求められる。（参考 13）

○　また、IoT 機器に搭載されるソフトウェアを含め、価格や納期の優位性から、オープンソースのソフトウェアを選択する場合も見られるが、問題のある機能が含まれ得ることや、適切なアップデートがなされないといった懸念も想定され、適切な対応が求められる[7]。

○　さらに、これらの技術等を活用して、ICT 製品・サービスのセキュリティに関する検証・評価を行うための推進体制を、適切な活用の仕組みの整備も視野にいれ、官民が連携して、オールジャパンで構築することが必要である。

○　この点について、諸外国においても、サプライチェーンリスクに対応するための研究・技術開発や製品・サービスに関する検証・評価の枠組の構築に向けて様々な動きが見られるところ、これらのグローバルな動向を十分に注視し、必要な連携を図っていく必要がある。

(2) サイバーセキュリティ自給率の低迷

○　我が国のベンダー企業においては、海外のセキュリティ技術を導入・運用する形態が主流となっている。このようなビジネスモデルは、研究開発投資を抑え、事業上のリスクを極小化することができる一方で、利益率が低く、また、コア技術に係るノウハウ・知見を蓄積することが難しい側面がある。（参考 14）

○　また、スタートアップ企業に関して、諸外国においては、投資家がマーケティング等のビジネスに関しても積極的に関与し、製品・サービスのシェア拡大を支援する取組など、研究開発から事業化・産業化に至るまでのプロセスやモデルが確立されている状況が見られる。また、公的機関が採用することで、そ

---

5 米国では NIST SP800-171 にて非政府機関の情報システム等における CUI 保護を目的としたサイバーセキュリティ対策の要件を規定。欧州では NIS Directive にて重要インフラに対し、最新のサイバーセキュリティ対策の実装を要求。

6 戦略的イノベーション創造プログラム第１期「重要インフラ等におけるサイバーセキュリティの確保」、戦略的イノベーション創造プログラム第２期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」等。

7 例えば、スウェーデンメーカーのネットワークカメラにて、オープンソースの gSOAP ライブラリに存在する脆弱性（Devil's Ivy）が問題となるケースがあった。

の後の品質改善や、利用拡大に繋げる状況も見られる。（参考 15）

○　例えば米国では、NIST によるサイバーセキュリティ製品・サービスの評価を、政府調達への活用や海外輸出力の強化にも繋げている側面が見られる。日本においても、評価等の枠組みと技術的な戦略を一体的に考えていくことが重要であると考えられる。（参考 16）

○　我が国企業の国際競争力強化はむろんのこと、政府機関や重要インフラ事業者等のサービスを支えるセキュリティ技術が過度に海外に依存する状況を回避・脱却する観点から、コア技術の開発・運用を中心に、国産技術・産業の育成を進めていくことが重要である。

(3) 研究・技術開発に資するデータの活用

○　AI や IoT 等の進展により、これまでとは異なる新たな脅威の発生が予測される中、リアルタイムでの攻撃把握、予兆の検知、攻撃挙動の分析等の重要性が高まるとともに（参考 17）、新たな脅威を早期に把握するため、観測範囲の拡大といった、攻撃観測基盤の強化等の研究・技術開発が求められる。

○　AI や IoT 等を悪用したサイバー攻撃に対処するためには、既存の人手依存の対応の対策等がいずれ限界となることが想定され、深層学習（Deep Learning）を含む、AI を活用した高度分析等の研究・技術開発も必要となる。

○　また、こうしたサイバー防御に係る研究・技術開発の推進や AI 等の新技術の活用を進めていくための基盤として、サイバー攻撃に関連する各種データの蓄積及びその活用方法の重要性が拡大している。例えば、マルウェア対策研究コミュニティである MWS[8]では、一定の契約のもと攻撃マルウェアデータを研究者に提供する等、実践的な研究・技術開発に寄与している。

○　なお、攻撃者間での攻撃情報・対策情報の共有により攻撃者が優位な状況になっており、それらに対抗し、サイバー防御をより強化するためには、各種攻撃データ及びその解析結果の迅速な共有・対応連携に取り組む必要がある。その際、データ漏えい時の対応等、責任関係の整理等にも留意する必要がある。

(4) 先端技術発展に伴う新たなリスクの出現

○　量子コンピュータ等の先端技術の発展に伴う、既存のセキュリティ技術への影響も指摘されている。例えば、量子コンピュータが実現することで、既存の暗号技術が危殆化する可能性や、一部の暗号アルゴリズムについては、解読可能な量子コンピュータが 2030 年までに実現するとの予測も示されている[9]。

○　また、AI の発展に伴い、AI を悪用した新たな攻撃の増加や、AI そのものへ

---

8 マルウェア対策研究人材育成ワークショップ。情報処理学会コンピュータセキュリティ研究会配下に設置されており、マルウェア解析等に関する発表が多数行われている。

9 M. Mosca:[Oxford] 1996: “20 qubits in 20 years”[NIST April 2015, ISACA September 2015]: “1/7 chance of breaking RSA - 2048 by 2026, ½ chance by 2031” [London, September 2017]:”1/6 chance within 10 years”等

の攻撃といった危険性も生じる可能性もある。加えて、IoT 機器の爆発的な増加とともに、IoT 機器を踏み台とした攻撃への対処の重要性が高まっているほか、IoT 機器のようにリソース（メモリ、CPU 等）の限られた機器でも活用可能な暗号モジュール等のセキュリティ技術の研究開発も必要となってきている。

○　5G についても、IoT、自動走行、フィンテック等、様々な場面での活用が期待される一方、ネットワークの仮想化・高度化の進展[10]や分散型のクラウドコンピューティング（エッジ、ローカル等）の活用により、新たに生じ得るセキュリティリスクに対応するための研究・技術開発について併せて検討していくことも必要となる。

(5) 産学官連携強化の必要

○　サイバーセキュリティの研究・技術開発を進めていく上で、産学官の密接な連携はその礎となる。海外では、欧米を中心に、研究・技術開発とそのための人材育成を一体的に推進するためのコミュニティの形成に向けた取組が進められている。

○　例えば英国においては、ACE(Academic Centers of Excellence in Cyber Security Research)の取組にて、政府が 17 大学をサイバーセキュリティ分野における研究機関として認定し、ACE としての活動費を提供することで、政府機関との間の情報共有や研究活動における連携を強化するといった、研究開発に係るコミュニティ形成が進められている。同様の取組は、米国やイスラエル等においても見られる。

○　我が国においても、一部の大学の自主的・自発的な取組として、国際的な連携組織である「InterNational Cyber Security Center of Excellence (INCS-CoE)」[11]を立ち上げ、諸外国との連携を図る取組が推進されている。

○　こうした取組も踏まえつつ、産学官が連携して、人材育成も視野に入れた、我が国における研究・技術開発のコミュニティを形成するための取組を推進していくことが重要である。

(6) 国際標準化強化の必要

○　サイバーセキュリティの研究・技術開発を進めていく上で、ISO/IEC や ITU-T などの国際標準化との連携強化が重要視されている。例えばクラウドや IoT に関わるセキュリティ分野では、国際標準化で定められる「基準（クライテリア）」や「ガイドライン」に基づき、各国が認証、認定を進めており、研究・技

---

[10] ネットワーク仮想化のための SDN(Software Defined Network)やモバイル網にエッジコンピューティングを実装するための MEC(Mobile Edge Computing)等の技術活用が進むと考えられている。

[11] 2016 年 11 月に慶應義塾大学の呼びかけで設立された米国・英国・日本の大学の有志による国際連携組織。大学という中立的な「場」を提供することで、サイバーセキュリティに関する国際間や組織間の壁を越えた問題に取組む。2018 年 11 月時点で 25 大学が参画。

術開発における「出口」として重要な位置づけとなっている[12]。

○　また、国際標準化に係る作業の参加国においては、国としての戦略的な視点から国際標準化を推進する流れも多く見受けられており、我が国においても国レベルの立ち位置から国際標準化の強化を進めるための議論を行う必要がある[13]。

○　さらに、欧州、米国などの地域標準化と国際標準化の結びつきも強くなりつつある。我が国としては、アジア諸国、とりわけ ASEAN 諸国との連携を視野にいれた国際標準化の推進を進める必要がある。

（参考）諸外国における動向

(ア)米国

- 研究開発に特化した戦略「2016 Federal Cybersecurity Research and Development Strategic Plan 」を策定。 サイバーフィジカルシステム、IoT、クラウドコンピューティング、高性能計算等の分野に注力。4 つのサイバーセキュリティ対策のカテゴリ（阻止、防御、検知、適用）を定義し、それぞれについて、短期・中期・長期の研究開発の取組を規定。
- 毎年度、実行計画「Implementation Roadmap」を策定し、NIST, NSF, NSA, DARPA, DHS, DoD 等を中心に産学官が連携して研究開発を推進[14]。
- CAE-R と呼ばれる DHS と NSA が共同で後援している大学認定プログラムが存在。一定基準をクリアし認定された大学が、サイバーセキュリティ中核組織として機能。

(イ)英国

- 全体戦略の「NATIONAL CYBER SECURITY STRATEGY 2016-2021」において、①DEFEND（防御）, ②DETER（阻止）, ③DEVELOP（開発）を柱に掲げ、特に③の部分で研究開発を位置付け。
- また、NCSC 主導の下、ACE (Academic Centre of Excellence)と呼ばれる政府と大学との連携の枠組を構築。NCSC が策定した基準に基づき、認定された大学が参加（2019 年時点で 17 大学が参加)。認定自体により各大学に付与される予算は 20,000 ポンド/年。
- ICT 機器の認証について、Common Criteria に関する取組に加え、一定

[12] ISO/IEC 27017 に基づくクラウドの認証サービス等

[13] 例えば、IoT 推進コンソーシアムにおいて、総務省、経済産業省主管でとりまとめた「IoT セキュリティガイドライン」や NISC が作成した「安全な IoT システムのためのセキュリティに関する一般的枠組」は、ISO/IEC における国際規格案のベースラインとなっており、我が国における戦略的な国際標準化の推進としての良い例となっている。

[14] 2019 年度要求で 7.4 億ドルの予算を計上。（SUPPLEMENT TO THE PRESIDENT'S FY2019 BUDGET より）

のセキュリティ製品（スマートメーター、ソフトウェア VPN 等）を対象とする検証制度である CPA（Commercial Product Assurance）を運用。

(ウ)イスラエル

- 全体戦略の「ISRAEL CYBER SECURITY STRATEGY」にて、①ロバストネス（頑健性）②レジリエンス（強靭性)、③ディフェンス（防御）の 3 つの柱を掲げ、これらに必要な能力構築の一環として研究開発を位置付け。
- ベングリオン大学、テルアビブ大学等の 6 つの大学において、政策や技術等の異なる分野に焦点を当てたサイバーセキュリティ研究センターを設置。
- 政府主導プロジェクトとして、南部ベルシェバに産・官・学・軍が同居する「サイバースパーク」を設置。サイバー分野でのエコシステムを生み出し、イノベーション活性化を狙う。

(エ) シンガポール

- 全体戦略の「Singapore Cybersecurity Strategy 2016」において、①弾力性のあるインフラ構築、②より安全なサイバー空間の維持、③活気あるサイバーエコシステムの開発、④国際パートナーシップの強化の 4 つの柱を掲げ、特に③の部分で研究開発を位置付け。
- 実行計画である「National Cybersecurity R&D Programme(NCR)」において、2020 年までの R&D 実行計画を策定。
- 産・学・官の連携組織として、シンガポールサイバーセキュリティコンソーシアムを設立。

4．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

＜目指すべきゴール＞

- 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
- 上記を実施する上で必要となる、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、関係機関の連携の下で推進する

＜具体的取組＞

諸外国の取組も参考としつつ、サプライチェーンリスクに対応すべく、ICT 機器・サービスの信頼性・有効性を検証するための体制の整備と技術の確立に向けて、政府一体となって以下の取組を進める。

- 国産技術の確保・育成のための取組や、政府調達における活用も視野に入れつつ、関係省庁と連携して、サプライチェーンリスクに対応するための技術検証体制の整備を進める（内閣官房：参考 19）
- 戦略的イノベーション創造プログラム第 1 期「重要インフラ等におけるサイバーセキュリティの確保」、戦略的イノベーション創造プログラム第 2 期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」等により、セキュアな Society 5.0 の実現に向けた研究開発及びその社会実装を推進する。（内閣府：参考 20）
- サイバーセキュリティ製品の有効性の確認や試行導入・実績公表等を通じ、日本発の製品の創出・活用を推進するとともに、IoT 機器等の信頼性を高度に検証するハイレベルな検証サービスの実証等を通じ、世界に貢献する高水準・高信頼の検証サービスを拡大するため、包括的な検証基盤（「Proven in Japan」）を構築する。（経済産業省 参考：21）
- IoT システムの基盤技術となる第 5 世代移動通信システムに係る各構成要素におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、対策の共有等を図る。（総務省：参考 22）
- チップの設計回路の解析や各種システム／サービスの挙動や動作の観測を通じた悪性機能を検出する技術の研究開発を実施する。（総務省）
- オープンソースソフトウェアを含むソフトウェアの管理手法等について、タスクフォースを立ち上げ、検討を進める（経済産業省）

- エッジからクラウドに至るまで、セキュアな環境下での情報処理を実現するため、ハードウェアセキュリティ等の確保に向けた技術開発を進める。（経済産業省）
- 産業技術総合研究所のサイバーフィジカルセキュリティ研究センターにおいて、サプライチェーンのための新たなセキュリティ技術の研究開発や、ハードウェア等のセキュリティ評価手法の研究開発を、産学官連携により重点的に行い、製品・サービスの検証・評価を行うための研究拠点化を推進する。（経済産業省・AIST）

② 国内産業の育成・発展に向けた支援策の推進

＜目指すべきゴール＞

- 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

＜具体的取組＞

日本発のサイバーセキュリティ製品・サービスの有効性を検証するための包括的検証基盤の構築や、導入実績公表に向けた取組、投資促進に資する税制優遇等の支援策を講じると共に、中小企業の隠れたニーズに対応したビジネスを創出するための支援の取組を行う。加えて、シーズとニーズに係るビジネスマッチングを実施し、市場展開を促進する。

- サイバーセキュリティ製品の有効性の確認や試行導入・実績公表等を通じ、日本発の製品の創出・活用を推進するとともに、IoT 機器等の信頼性を高度に検証するハイレベルな検証サービスの実証等を通じ、世界に貢献する高水準・高信頼の検証サービスを拡大するため、包括的な検証基盤（「Proven in Japan」）を構築する。（経済産業省 参考：21）※再掲
- 一定の品質の維持・向上に努めている情報セキュリティサービスを明らかにするための制度（情報セキュリティサービス審査登録制度）の普及促進とともに、よりよい利用方策についての検討を行い、競争力強化やサイバーセキュリティの成長産業化に取り組む。（経済産業省）
- 中小企業がサイバー攻撃等で困った時の相談窓口、駆けつけ支援体制（サイバーセキュリティお助け隊）の実証事業を全国 8 地域で実施し、その結果を基に、中小企業が利用し易い、支援体制、サイバー保険等について検討、構築

し、普及を図る。(経済産業省・IPA：参考 23)

- 中小企業が、サプライチェーンサイバーセキュリティ対策に関わるセキュリティ基準等（NIST SP800-171 等）を満たすことができるよう、安価で使いやすいセキュリティ対策の普及・創出を促すための実証を実施する。(経済産業省)
- サイバーセキュリティビジネスの振興・活性化を図るため、サイバーセキュリティ対策におけるニーズの明確化・具体化、シーズの発掘やビジネスマッチングを行うメンバーを限定しない情報交流の場を継続して開催する。(経済産業省・IPA：参考 24)

③ 攻撃把握・分析・共有基盤の強化

＜目指すべきゴール＞

- 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

＜具体的取組＞

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、人手に依存する分析・解析技術の効率化・自動化に取り組むとともに、サイバーセキュリティ分野の研究・技術開発を活性化させるべく、当該把握・分析データを共有するための基盤構築に取り組む。

- 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、広域ダークネット(Nicter)や攻撃種別に柔軟に対応するハニーポット技術等を用いて、サイバー攻撃観測技術の高度化に関する研究開発を行う。(総務省・NICT)
- 標的型攻撃の攻撃挙動の把握・解析やそのための迅速の対応（対策）を進めるために、サイバー攻撃誘引基盤（STARDUST）の高度化、及びその活用の拡大を図り、標的型攻撃の具体的な挙動収集や未知の標的型攻撃等を迅速に検知・解析する技術等の研究開発を行う。(総務省・NICT：参考 25)
- 脆弱な IoT 機器の確度の高い把握、及びそのセキュリティ対策のため、通信量の抑制と精度の向上を実現する効率的な広域ネットワークスキャンのための研究開発を行う（総務省）
- ダークネット、ハニーポット等の多くの観測手段により収集したデータに基づき（上記「サイバー攻撃観測技術の高度化」による)、これまで手動解析が

主であったマルウェア起因の挙動解析に対し AI 技術を駆使することで関連する攻撃挙動の解析を自動化する技術の研究開発を実施する。（総務省：参考 26）

- サイバーセキュリティ関連情報を大規模集約し、多種多様な攻撃データによる高度・深層解析を行い、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）を構築するとともに、広範囲なデータを保有する CURE に基づくセキュリティ対策のための自動化技術の確立等を行う。（総務省・NICT：参考 27）
- IoT 機器等の脆弱性対策情報について、経済産業省告示に基づき運用される『情報セキュリティ早期警戒パートナーシップ』[15]の着実な実施や海外の脆弱性情報データベース（CVE）との連携を図る等、情報共有基盤の強化に取り組む（経済産業省）
- インシデント対応支援活動等にて解析したマルウェア検体及びその解析結果について、インターネット定点観測システム（TSUBAME）との連動を図る等、データの有効活用に取り組む。（経済産業省・JPCERT）

④ 暗号等の基礎研究の促進

＜目指すべきゴール＞

- 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、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
- 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

＜具体的取組＞

既存の暗号システムの危殆化につながる量子コンピュータ等の国際動向を把握しつつ、量子暗号等の安全なセキュリティ技術の研究・技術開発に取り組む。併せて、今後、本格的な普及が想定されている IoT デバイスにて活用可能な暗号技術の研究・技術開発に取り組む。

- 量子コンピュータや IoT 等の普及ならびに新たな暗号技術の動向等を踏まえ、我が国の暗号の在り方と課題についての議論や、次期 CRYPTREC 暗号リストが満たすべき条件の整理を進める。（総務省・NICT、経済産業省・IPA）
- 「光・量子飛躍フラッグシッププログラム」により、①量子情報処理（主に量

[15] ソフトウェア製品及びウェブアプリケーションに関する脆弱性関連情報の円滑な流通、および対策の普及を図るため、公的ルールに基づく官民の連携体制として整備された。

子シミュレータ・量子コンピュータ)、②量子計測・センシング，③次世代レーザーの 3 領域における研究開発を着実に推進し、経済・社会的な重要課題を解決につなげることを目指す。(文部科学省：参考 28)

- 量子暗号等を活用した量子情報通信ネットワーク技術の確立に向け、研究開発を実施する。(総務省・NICT：参考 29)
- 盗聴や改ざんが極めて困難な量子暗号通信を、超小型衛星に活用するための技術の確立に向けた研究開発を推進する。(総務省)
- IoT システムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、などを両立させるための革新的、先端的技術の基礎研究に取り組む。(経済産業省・AIST)
- 情報セキュリティ分野と関連の深い国際標準化活動である ISO/IEC JTC1/SC27 が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。(経済産業省・IPA)

⑤ 産学官連携の研究・技術開発のコミュニティ形成

＜目指すべきゴール＞

- サイバーセキュリティの研究・技術開発について、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

＜具体的取組＞

- 諸外国及び国内の取組の現状も踏まえながら、関係者とも連携しつつ、我が国における研究・技術開発の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て、検討を開始する。その際、研究・技術開発に必要となる高度な能力を持つ人材の育成といった観点も重要となることから、これらについても併せて検討を進める。(内閣官房)

５．まとめ

○　戦略期間中においては、以上の取組強化の方向性及び別添のロードマップに沿って、関係省庁が連携して、具体的・実践的な研究開発を推進していくこととする。

○　研究・技術開発の推進に当たっては、個別の研究・技術開発の成果の創出が重要であることは言うまでもないが、それに留まることなく、社会実装までのプロセスを念頭に置きつつ、取組を進めることが重要である。

　加えて、社会実装を促進する上では、サイバーセキュリティの重要性が社会において十分に認識されていることが前提となることから、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する。

○　本取組方針に沿った取組の実施状況については、本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することとする。

(別紙)取組強化に関する
ロードマップ

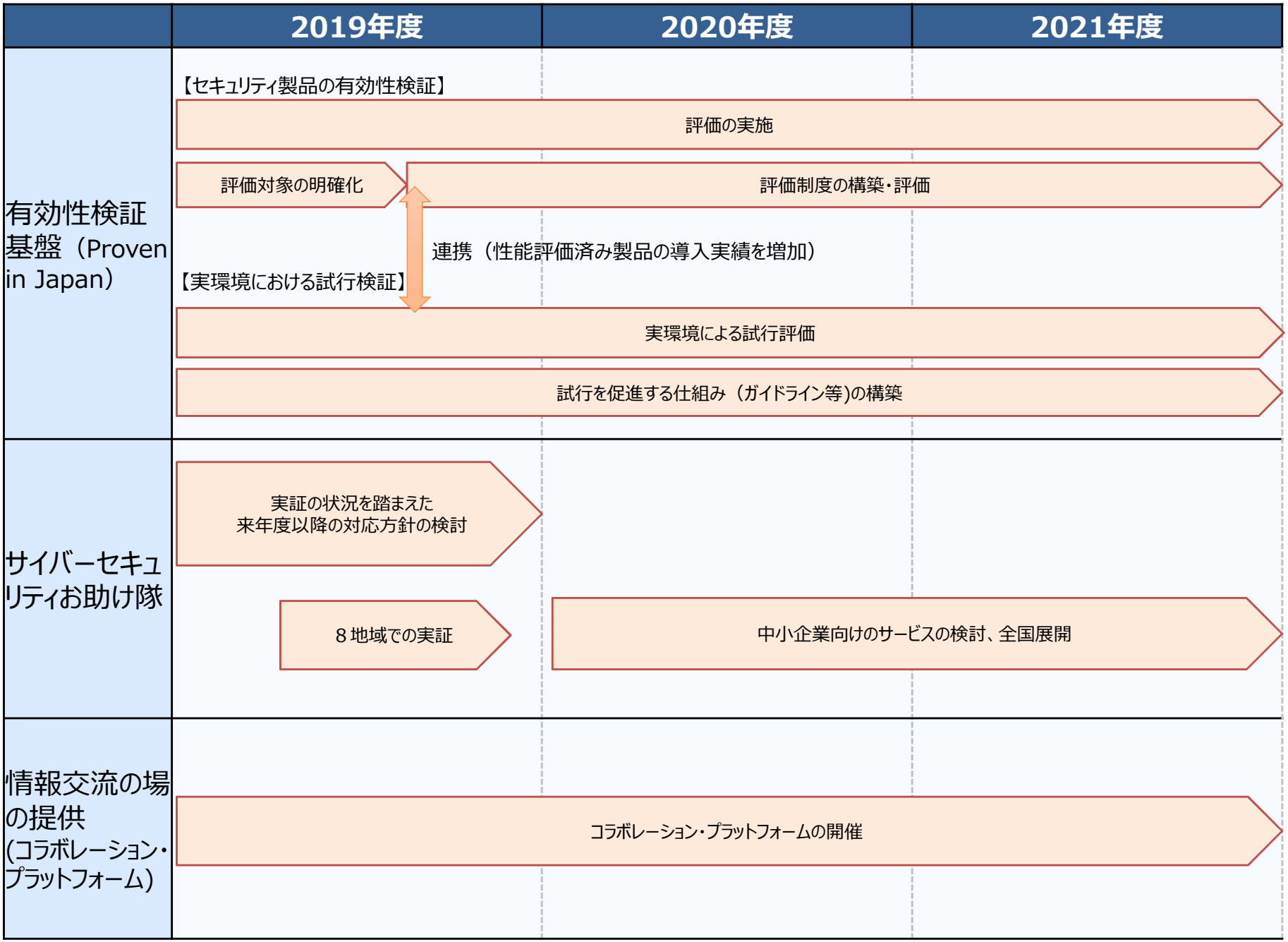
①サプライチェーンリスクへ対応するための、技術的検証体制の整備

	2019年度	2020年度	2021年度
技術検証体制の整備	検証スキームの検討・策定 ※主な検討事項 ・対象製品の選定・評価基準の策定、検証技術のマッピング等	試行運用	技術移転 本格運用
	試験の実施手法・評価方法の検討 試験の実施 ※SIP第２期、Checked by Japan、チップ脆弱性検知技術等の成果も活用		
SIP第２期	技術開発と実フィールド事業者連携 ※実フィールドを持つ事業者やベンダーと密に連携した体制づくり	製造・流通・ビル分野等での実証 ※IoTシステムとサプライチェーンにおいて社会実装を目指した実証実験に順次着手	幅広い産業分野へ拡大 （本格的社会実装）
	海外動向の調査		
	府省庁による制度設計・グローバルな調整		
有効性検証基盤（Proven in Japan）	【攻撃型を含めたハイレベルな検証サービス】		
	製品の評価		
	検証対象・手法の明確化		
	検証主体の確保へ向けた仕組み構築		
5Gに係るセキュリティ	５Ｇネットワークに係る脆弱性の調査 ※オープンソースソフトウェアの解析、ファジング、ホワイトハッカーによる脆弱性調査	関係事業者への周知・啓発	
		知見を活用	
		情報通信ネットワークにおけるサプライチェーンリスクの技術的検証	
チップ脆弱性検知	回路情報を用いて、AI技術により悪性回路を検知するプロトタイプの開発・実装、有効性の検証		商品開発、社会実装
			AIを用いて検知を回避する攻撃を想定したプロトタイプの開発・実装、有効性の検証
	電力波形などのシステムの外部情報を用いて、AI技術により悪性機能を検知する技術の開発		実用化に向けたAI技術の高度化、プロトタイプの開発・実装、有効性の検証
エッジからクラウドに至るHWセキュリティ	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技術の開発		

【目指すべきゴール】

・サプライチェーン全体の信頼確保に向けた、製品・サービスのセキュリティの技術的検証を行う体制を、政府一体となって整備する。
・上記を実施する上で必要となる、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を、関係機関の連携の下で実用化する。

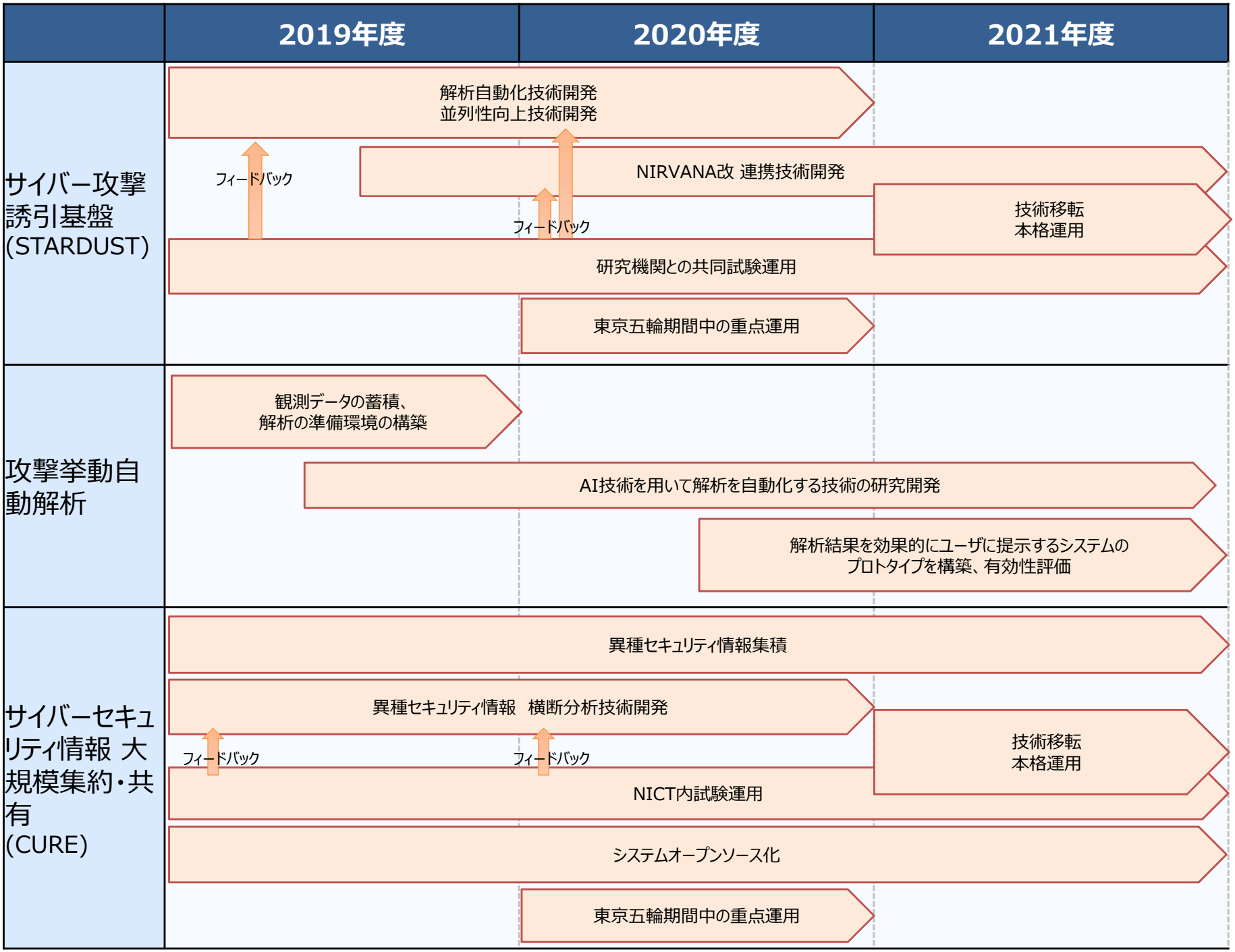
②国内産業の発展に向けた支援策の推進



【目指すべきゴール】

・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

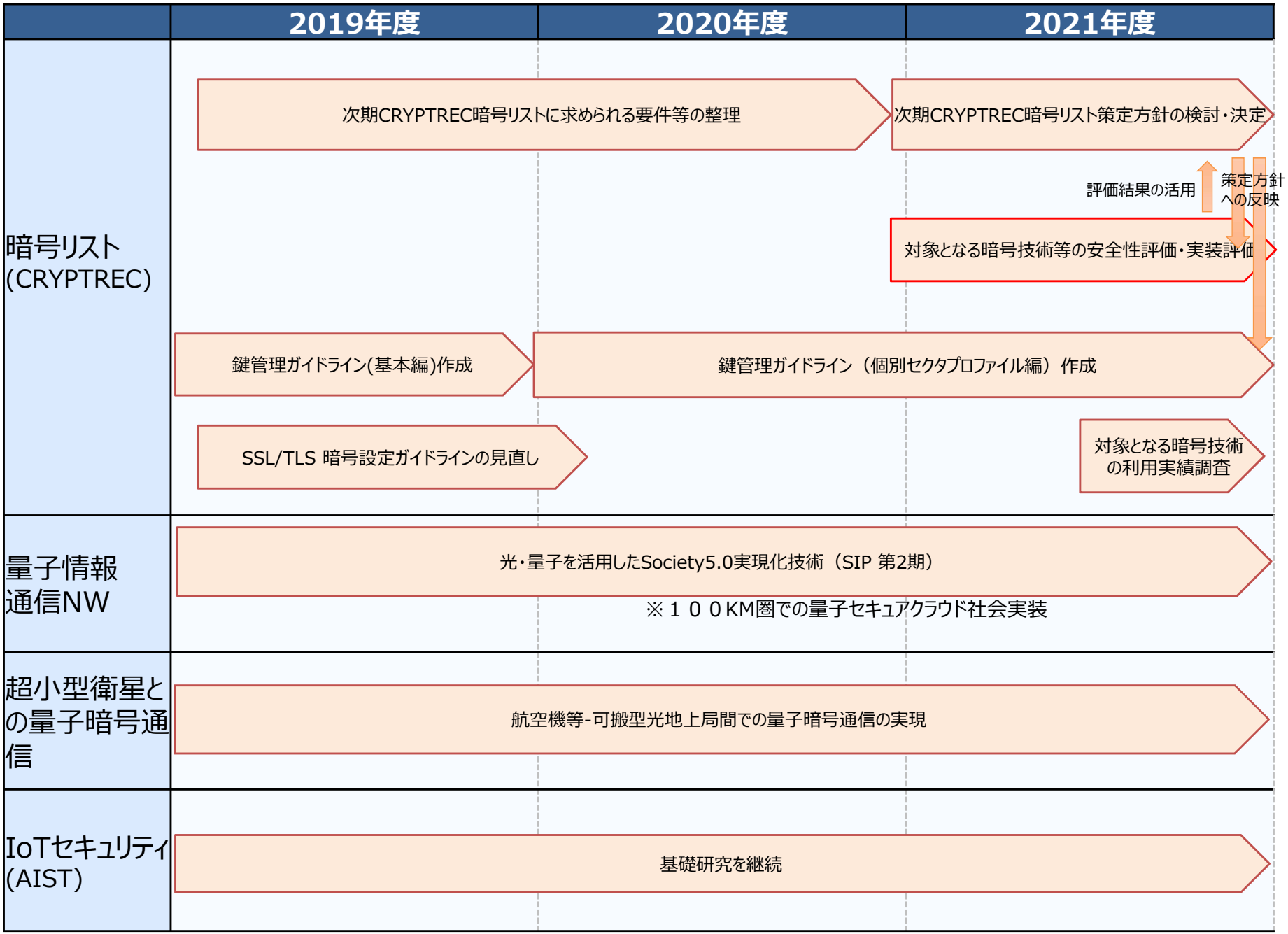
③攻撃把握・分析・共有基盤の強化



【目指すべきゴール】

・サイバー攻撃の巧妙化・複雑化や、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、サイバー攻撃の把握・分析技術や情報共有基盤を強化する。

④暗号等の基礎研究の促進



【目指すべきゴール】

・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、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。

（参考資料集）

参考１

今後のICTの進展

NISC

- 5GやAI，IoT等のテクノロジーの進化により、Society5.0が進展し、自動運転やスマートライフ等の新たなサービスが実現されるなど、サイバー空間と実空間の一体化がより一層進むと想定される。

Society5.0の進展

出典：内閣府　Society5.0のしくみ

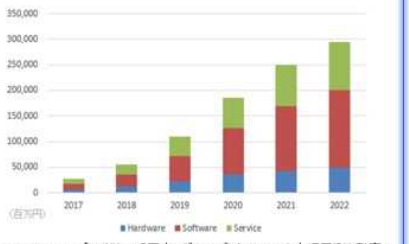
出典：経済産業省　Connected Industries

5Ｇ本格展開

出典：総務省　第5世代移動通信システムの技術的条件

AIの進化

AIシステム市場 ユーザ支出額予測（セグメント別）



（出典）IDC Japan プレスリリース「国内コグニティブ／AIシステム市場予測を発表」

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考２

近年のサイバー攻撃の脅威傾向と将来予測

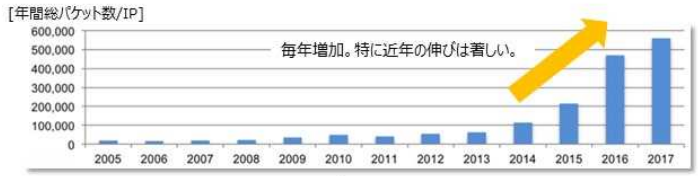
NISC

- ここ数年、観測されるサイバー攻撃の数（疑い含む）は増加傾向にあり、新種のマルウェアも毎年一定数発生。
- また、新たな脅威の発生（AI，IoT，5G等の新技術やサプライチェーンをターゲットにした攻撃等）や攻撃者優位の拡大（新技術の悪用による攻撃の巧妙化・大規模化等）が予測されており、今後もその脅威は増大すると想定される。

近年の脅威傾向

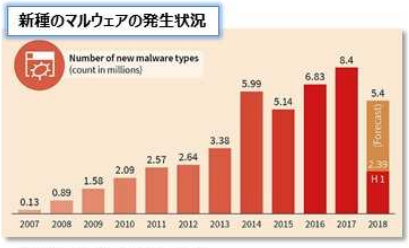
IPアドレスあたりの年間総観測パケット数

NICTの観測システム(Nicter)に届いたパケットの個数。マルウェアに感染した機器からのパケットやDoS攻撃を受けているサーバのパケットなど、サイバー攻撃の疑いの高いパケットが観測される。



（出典）：Nicter観測レポート2017

新種のマルウェアの発生状況



（出典）：G DATA Security Blog：https://www.gdatasoftware.com/blog/2018/09/31037-malware-figures-first-half-2018-danger-web

将来の脅威予測

シマンテックの予測

- 攻撃者は、人工知能（AI）システムに侵入し、攻撃にも AI 支援を利用する
- 防御側も、脆弱性を見極め反撃するために AI への依存度を強める
- 5G の配備と導入が進み、攻撃の範囲が拡大する
- IoT ベースの普及で、大規模 DDoS 攻撃を超えた新しく危険な攻撃が出現する
- サプライチェーンを悪用する攻撃が、質量ともに増大する

（出典）：シマンテック公式ブログ https://www.symantec.com/connect/ja/blogs/2019

McAfeeの予測

- 将来の回避技術における人工知能（AI）の更なる活用
- 音声認識機能を活用したIoTデバイスへの攻撃が次なる標的に

（出典）：McAfee公式ブログ https://blogs.mcafee.jp/mcafee-labs-2019-threats-predictions

トレンドマイクロの予測

- AI技術を利用した高度な標的型攻撃が確認される
- サイバー犯罪者同士によりIoTをめぐる「ワーム戦争」が勃発する

（出典）：トレンドマイクロ：2019年セキュリティ脅威予測 https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20181213-01.html

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考３

国内外のサイバー攻撃等の事案

NISC

【重要インフラ等の業務・機能・サービス障害】　○…国内　□…海外

□ Miraiによる大規模DDoS攻撃（2016年9月）
IoT機器に感染し史上最大規模のDDoS攻撃を仕掛ける新型マルウェア（いわゆる"Mirai"）が登場した。2016年9月、米セキュリティサイトKrebs on Security が、ピーク時665GbpsのDDoS攻撃によって一時的にサイト閉鎖に追い込まれ、同22日には、フランスのインターネットサービスプロバイダーであるOVH社が、1.1Tbpsに達する大規模なDDoS攻撃を受けた。

□ ウクライナ電力供給会社（2016年12月）
2016年12月17日深夜、ウクライナの国営電力会社Ukrenergoの変電所がサイバー攻撃を受け、キエフ北部及び周辺地域で約1時間の停電が発生

□ 英国の病院、仏ルノー等（2017年5月）
ランサムウェア「WannaCry」の感染により、英国の国民保険サービス（NHS）関連システムが停止し、多数の病院で医療サービスが中断するなどの被害が続出。また、仏ルノーでは車両の生産ラインの稼働が停止。その他にも、スペインのテレフォニカ、独のドイツ鉄道、米国のFedEx等、世界各国で被害あり。
2017年12月に、米国は、このサイバー攻撃が北朝鮮によるものであるとして、北朝鮮を非難する旨発表。同日、我が国も米国を支持し、北朝鮮を非難

【情報（個人情報・知的財産等）の毀損及び漏えい】

○ 日本年金機構への不正アクセス（2015年5月）
日本年金機構において、外部からの標的型メールに添付されたウイルスに感染したことにより、不正アクセスが行われ、個人情報約125万件が外部に流出した。

□ 米Facebook（2018年9月）
2018年9月、Facebook社はハッキングの被害を受け、約5,000万件の利用者情報が流出したおそれがあると発表

□ 米マリオット（2018年11月）
2018年11月30日、ホテルの予約データベースに不正なアクセスがあり、最大で約５億人の利用客情報が流出したおそれがあると発表。
2018年12月12日、米国務長官は、このサイバー攻撃に中国が関与していると指摘

○□ 中国を拠点とするAPT10の活動（2018年12月）
中国を含むG20メンバー国は、知的財産の窃取等の禁止に合意している中、中国を拠点とするAPT10といわれるグループからの日本の民間企業、学術機関等を対象とした長期にわたる広範な攻撃を確認。
12月20日から21日にかけて、英国・米国等からAPT10に関して声明文が発表。12月21日、我が国もこれらの国を支持し、外務報道官談話を発出

【金銭の窃取・詐取】

○ 国内大手航空会社ビジネスメール詐欺（2017年12月）
国内大手航空会社が、偽の請求書メールにより、航空機リース料等の支払要求に応じ、３億円を超える詐欺被害に遭った。

○ 仮想通貨が不正に送信されたとみられる事案（2018年１月）
国内仮想通貨交換業者から約580億円相当の仮想通貨（NEM）が不正に送信されたとみられる事案が発生した。

○ 仮想通貨が不正に送信されたとみられる事案（2018年９月）
国内仮想通貨交換業者から合計約70億円相当の仮想通貨（Bitcoin, Monacoin, Bitcoin Cash）が不正に送信されたとみられる事案が発生した。

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考４

サイバー攻撃の現状

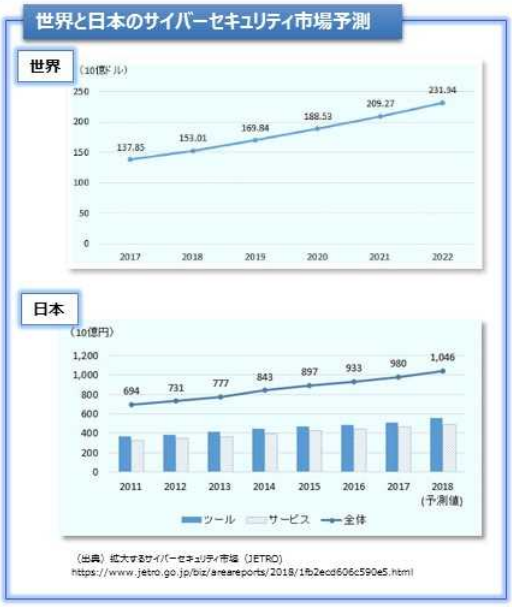
- NICTによるサイバー攻撃観測：1500億回スキャン/2017年、5300スキャン/秒（スキャン：攻撃の予備活動として、標的を調査する活動）
- マルウェア発生の頻度：2017年：1億２千万/年、36万/日（以前と比較：９千/日：2007年、40/日：1997年）、実際のハッキング数（約2000件/日（2017年））
- 100以上の高度に洗練された攻撃グループが世界中に存在（標的：金融機関、重要インフラ（制御系システムを含む）、製造業、運輸業などへと拡大化（多くが金銭目的））
- テロリズム（妨害活動）による被害：ドイツ（製鋼所）：2014、ウクライナ（送電網）：2015-2016、英国/ドイツ等（病院等）：2017、韓国（冬季オリンピック）：2018などで多発
- セキュリティ対応費用の増大等：ランサムウェア（暗号化し金銭をとるマルウェア）/80億ドル（世界）、50%費用増加（日本）、内部犯行事例の増加（攻撃全体の約20%に）
- 最近の急増するビジネス環境による脆弱点の多様化：クラウド、ビックデータ、IoT、サプライチェーン、5G（第5世代ワイヤーレス通信）等への変化

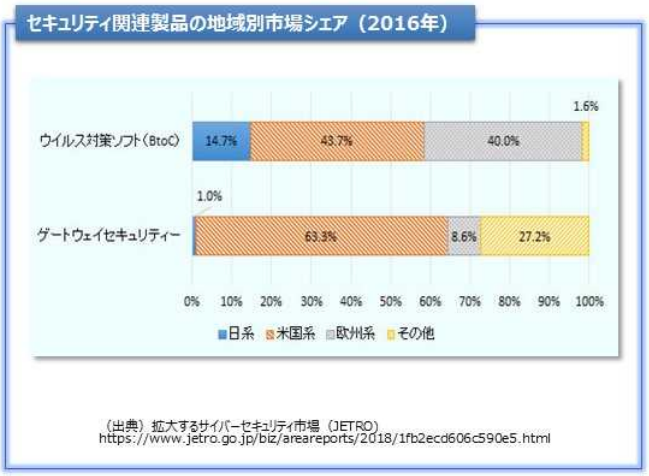
（出典）研究開発戦略専門調査会第 10 回会合　中尾補佐官発表資料

参考５

世界のサイバーセキュリティ市場予測と日本の状況

- サイバー攻撃の脅威の高まりとともに、サイバーセキュリティ製品・サービスの需要も高まっており、世界のサイバーセキュリティ市場は2018年に1,530億ドルに達し、2022年には2,300億ドルに至ると予測されている。同様に日本のサイバーセキュリティ市場も年々伸びている。
- 一方で、世界における我が国のセキュリティ製品シェアは低く、米国や欧州との差が大きい状況。また、日本市場への外資系企業の参入も相次いでいる。



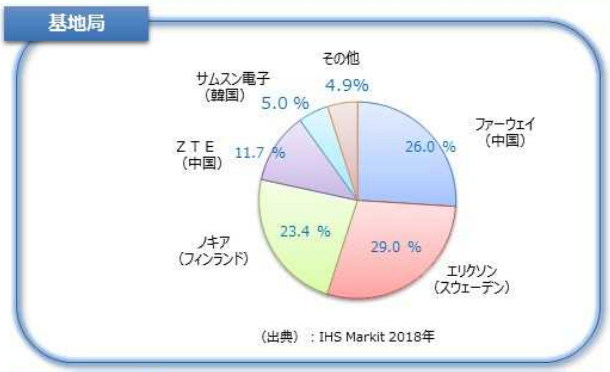


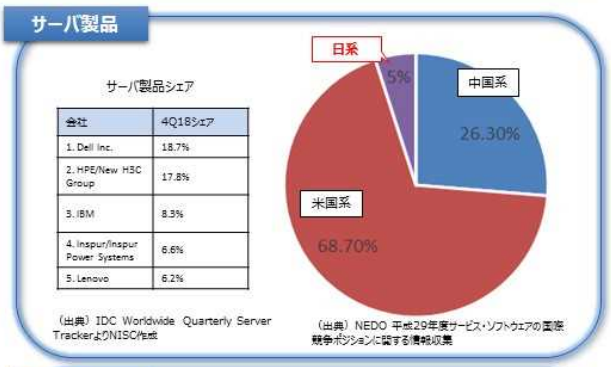
（出典）研究開発戦略専門調査会第９回会合　事務局資料

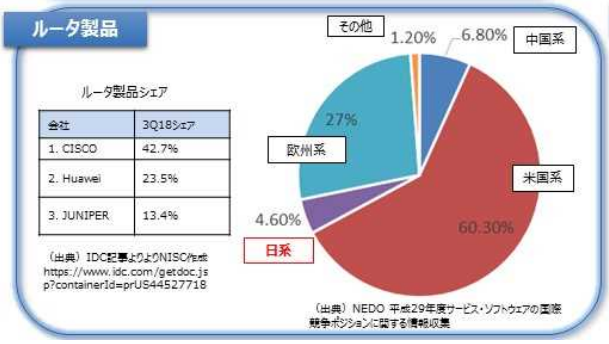
参考６

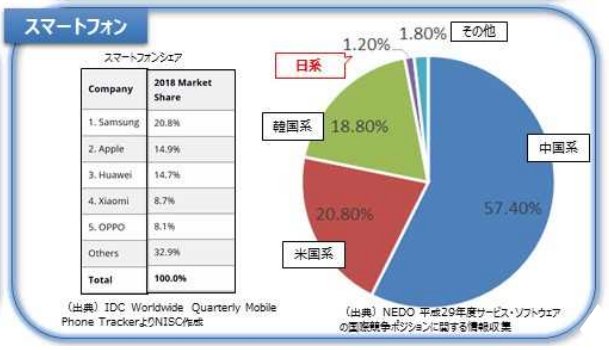
ICT製品の市場シェアの状況

- サイバー攻撃から守る対象となる各種ICT製品についても、欧米や中国のシェアが高く、日本のシェアは低い状況。









（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考７

グローバル企業と日本企業の研究開発投資額の比較

NISC

- 研究開発投資額のランキングを見ると、Amazon, Alphabet(Google親会社)等の世界で活躍しているICT企業が上位にラインクイン。両社とも売上高に占める研究開発投資額が10%を越えている。また、中国ICT大手企業の研究開発投資額も伸びている。
- 一方、日本企業は、ヘルスケア分野を除き10%未満の状況であり、総じて低い。

研究開発投資額グローバルランキング

順位(2018)	順位(2017)	順位の変化	社名	本社所在地	業種	R&D支出(10億ドル)	売上高(10億ドル)	対売上高R&D支出比率(%)
1	1	0	アマゾン	北米	ソフトウエア・インターネット	22.6	177.9	12.7%
2	2	0	アルファベット	北米	ソフトウエア・インターネット	16.2	110.9	14.6%
3	5	+2	フォルクスワーゲン	欧州	自動車	15.8	277.0	5.7%
4	4	0	サムスン	その他	コンピュータ・エレクトロニクス	15.3	224.3	6.8%
5	3	-2	インテル	北米	コンピュータ・エレクトロニクス	13.1	62.8	20.9%
6	6	NA	マイクロソフト	北米	ソフトウエア・インターネット	12.3	90.0	13.7%
7	9	+2	アップル	北米	コンピュータ・エレクトロニクス	11.6	229.2	5.1%
8	7	-1	ロシュ	欧州	ヘルスケア	10.8	57.2	18.9%
9	12	+3	ジョンソン・エンド・ジョンソン	北米	ヘルスケア	10.6	76.5	13.8%
10	8	-2	メルク・アンド・カンパニー	北米	ヘルスケア	10.2	40.1	25.4%
11	11	0	トヨタ自動車	日本	自動車	10.0	259.9	3.9%
12	10	-2	ノバルティス	欧州	ヘルスケア	8.5	50.1	17.0%
13	15	+2	フォード	北米	自動車	8.0	156.8	5.1%
14	20	+6	フェイスブック	北米	ソフトウエア・インターネット	7.8	40.7	19.1%
15	14	-1	ファイザー	北米	ヘルスケア	7.7	52.6	14.6%

（出典） PWC Strategy& 2018年グローバル・イノベーション1000調査結果概要
（ただし中国企業は除く）

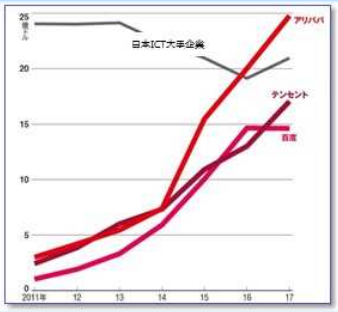
日本ランキング

順位(2018)	順位(2017)	グローバル順位(2018)	社名	業種	R&D 支出(10億ドル)	売上高(10億ドル)	対売上高R&D支出比率(%)
1	1	11	トヨタ自動車	自動車	10.0	259.9	3.9%
2	2	18	本田技研工業	自動車	7.1	131.8	5.4%
3	3	37	日産自動車	自動車	4.6	110.4	4.2%
4	4	38	ソニー	コンピュータ・エレクトロニクス	4.3	71.6	6.0%
5	5	39	パナソニック	コンピュータ・エレクトロニクス	4.2	69.2	6.1%
6	6	40	デンソー	自動車	4.2	42.6	9.9%
7	8	51	日立製作所	コンピュータ・エレクトロニクス	3.1	86.3	3.6%
8	9	53	武田薬品工業	ヘルスケア	3.1	16.3	18.8%
9	10	54	キヤノン	コンピュータ・エレクトロニクス	2.9	36.2	8.1%
10	7	55	東芝	工業製品	2.8	46.2	6.0%

（出典） PWC Strategy& 2018年グローバル・イノベーション1000調査結果概要

中国ICT大手の研究開発投資額の推移

アリババ、テンセント、百度は2013年頃から売上高の10%前後を研究開発に投資



（出典） 米PWC調査をもとにNISC作成

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考８

スタートアップを取り巻く環境と日本のプレゼンス

NISC

- 高度化・巧妙化するサイバー攻撃に対抗すべく、世界的に先端技術を開発する新興企業が多数生まれているが、米国やイスラエルが中心。
- サイバーセキュリティ分野で活躍している企業のランキング調査等においても、日本企業は上位にランクインしていない。また、スタートアップの成長しやすい拠点ランキングでも同様の結果が出ている。
- 一方で、日本でもスタートアップを支援する施策によりサイバーセキュリティ関連のスタートアップ企業も出てきている。

サイバーセキュリティ トップ500

Cybersecurity 500

Meet the world's hottest and most innovative cybersecurity companies to watch in 2018. Press Release

Cybersecurity 500 By The Numbers: Breakdown By Region

#	Company	Cybersecurity Sector	Corporate HQ
1	Herjavec Group	Information Security Services	Toronto, Canada
2	KnowBe4	Security Awareness Training	Clearwater FL
3	CyberArk	Privileged Access Security	Petach-Tikva, Israel
4	Raytheon Cyber	Cyber Security Services	Waltham MA
5	Cisco	Threat Protection & Network Security	San Jose CA
6	IBM Security	Enterprise IT Security Solutions	Waltham MA
7	Microsoft	Datacenter to Endpoint Protection	Redmond WA
8	Amazon Web Services	Cloud-Powered Security	Seattle WA
9	FireEye	Advanced Threat Protection	Milpitas CA
10	Lockheed Martin	Cybersecurity Solutions & Services	Bethesda MD
11	Check Point Software	Unified Threat Management	Tel Aviv, Israel
12	RSA	Intelligence Driven Security	Bedford MA
13	Symantec	Endpoint, Cloud & Mobile Security	Mountain View CA

500社中、日本は3社のみ。上位へのランクインはない。
（出典）CYBERSECURITY VENTURES Cybersecurity 500

スタートアップの成長しやすい拠点

（出典）Startup Genome：Global Startup Ecosystem Report 2017

上記はICT全体のランキング。サイバーセキュリティ分野では、ニューヨーク、ボストン、シリコンバレー、フェニックス、トロント・ウォータールー、オタワ、ハーグ、フランクフルト、ベルリン、プラハ、テルアビブ、ベエルシェバが主要拠点とされている。

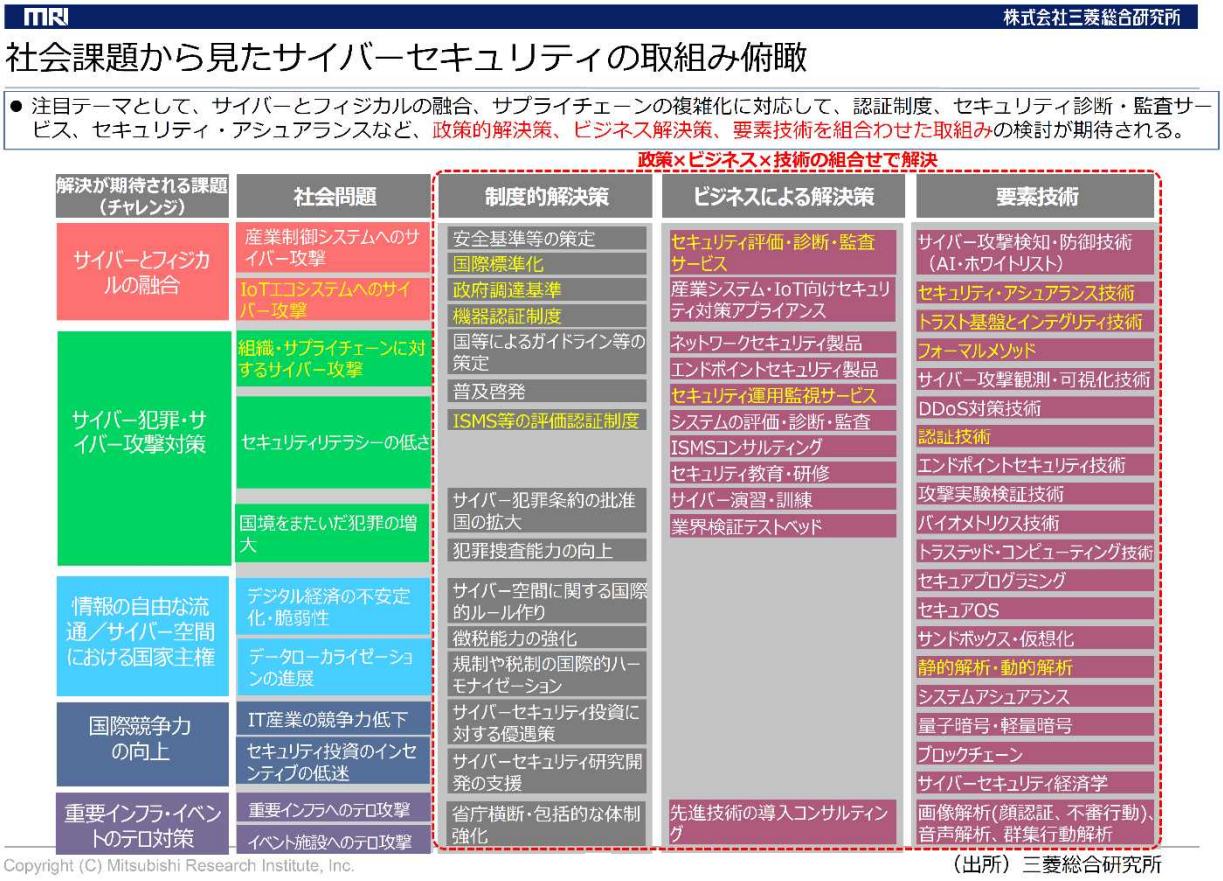
日本のスタートアップ支援プログラム

J-Startup

- 世界で戦い、勝てるスタートアップ企業を生み出し革新的な技術やビジネスモデルで世界に新しい価値を提供するスタートアップ企業の育成支援プログラム。
- プリファードネットワークス社（深層学習フレームワークの開発・提供等）やカウリス社（法人向け不正アクセス検知サービスの提供）が参画。

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考９



（出典）研究開発戦略専門調査会第９回会合　株式会社三菱総合研究所発表資料

参考 10

5Gで想定されるセキュリティ脅威

性能要求の変化	
大容量	攻撃トラヒックも大容量化
多接続	大規模なボットが形成
低遅延	低オーバヘッド優先でセキュリティ低下

アーキテクチャ／NW機能の変化

インフラのソフトウェア化／サードパーティアプリ導入で脆弱性が増加

標準化動向

3GPPでは、5G導入初期(Phase1)の仕様策定を完了。NWスライスなど5G新機能のセキュリティ課題はPhase2で議論。

技術的課題と対策

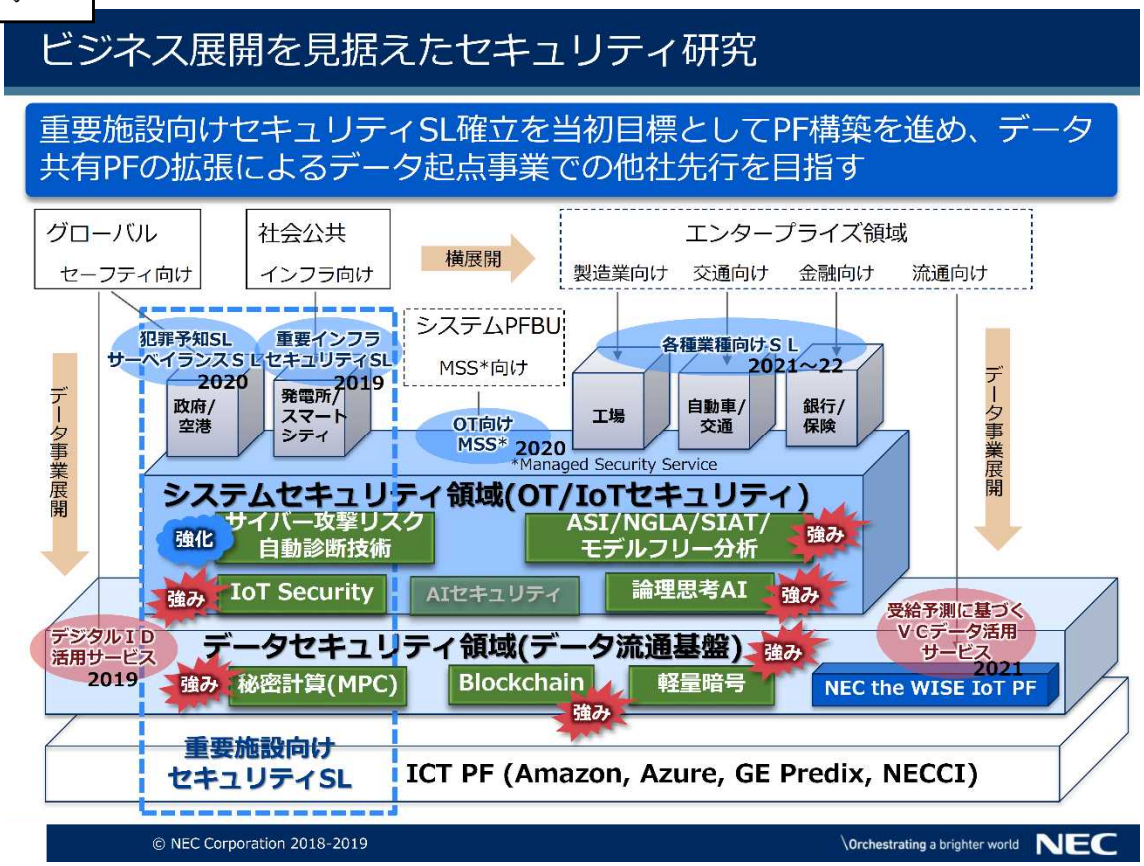
- スライス等、新技術における信頼性の確保➡セキュリティ評価基準の確立
- 大容量･多接続による脅威の増大➡攻撃の早期検知、AIによる省力化･自動化

設計･評価	検　知	対　策
VNF･サービスの実装／導入／開始前にセキュリティ評価、**脆弱性を未然に防ぐ**	5G内のセキュリティイベントを早期に検知、**脅威の顕在化を未然に防ぐ**	検知したイベントを自動的に解決、**脅威による被害の長期化を防ぐ**

VNF: Virtual Network Function

（出典）KDDI 提供資料

参考 11



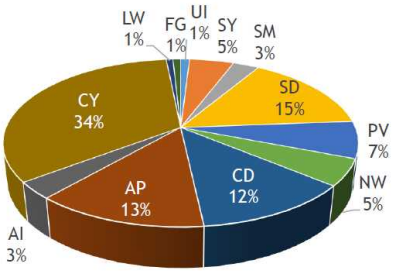
（出典）研究開発戦略専門調査会第９回会合　日本電気株式会社発表資料

参考 12

UNIVERSITY OF NAGASAKI

国内研究領域動向

- 過去3年間のSCIS，CSSに投稿公表された論文計1,664編を，JNSAのSecBOKの分類に従って分類した．（SecBokにない領域は適宜追加．例：プライバシー技術）
- 暗号理論，セキュリティ応用，サイバー攻撃手法の順に多く，6割強を占める．他方，ユーザインタフェース，システムマネジメント，フォレンジック，制度は少ない



*注：セッション名で判断しているため，厳密なデータではないが概要を知ることを目的としている

©Ayako Komatsu,2019

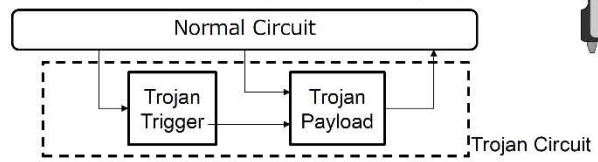
AI:　人工知能関連
AP：セキュリティ応用（ブロックチェーン，Fintechなど）
CD:サイバー攻撃手法，マルウエア解析
CY：暗号理論，実装，暗号プロトコル，認証，計算理論
NW：ネットワークセキュリティ，侵入検知，脆弱性診断
PV：プライバシー保護関連
SD：セキュアシステム設計・構築，IoTセキュリティ，制御セキュリティ
SM:　セキュリティマネジメント，セキュリティ対策推進
SY:システムセキュリティ，Webセキュリティ，サプライチェーンセキュリティ
UI：ユーザインタフェース
FG:フォレンジック
LW：制度，規定，標準

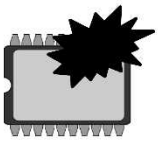
（出典）研究開発戦略専門調査会第９回会合　小松委員発表資料

参考 13

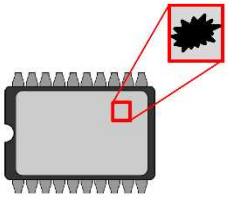
IoT時代の新たな脅威ーハードウェアトロイ

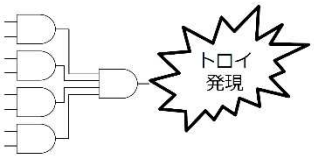
- ハードウェアトロイとは
  - ハードウェアに組み込まれた**悪意のある機能**





- ハードウェアトロイの特徴
  - 元の回路に比べ**小規模**
    ICベンダやユーザから自身の存在を隠すため，
    回路規模が小さく収められている．
  - ある**一定の条件で**ハードウェアトロイの機能が発現
    普段は正常に動作するのに，ある特定の条件
    （特定の入力や，回路の内部状態）をトリガとして
    悪意ある機能が作動する．
  - **トリガ条件がなく**発動し続けるものもある
    電力消費を増大させる
    サイドチャネルに情報を漏洩





（出典）研究開発戦略専門調査会第 8 回会合　戸川委員発表資料

参考 14

国内産業の育成

海外製品の活用メリットとデメリット

メリット

エンドユーザー
- 既に実績のある技術を使える。対策が大失敗するリスクを回避できる

セキュリティベンダー
- 研究開発リスクを回避。投資回収も容易。事業上のリスクを極小化
- 研究開発の実施体制を作る必要がない。採用・育成等リスクの高い課題に取り組まなくて良い
- 実績作りなどマーケティング面で難しいハードルを越える必要がない

デメリット

エンドユーザー
- 要望やトラブル発生の際、マーケットサイズに応じた対応
  日本固有の事象についてはフィルタされる事も
- 基礎技術が蓄積できない。日本独自で対応できない

セキュリティベンダー
- ビジネス上スケールメリットのある部分を奪われる。利益率が悪い
- ビジネスの多くが人依存。仕組みの台頭でビジネスが駆逐されるリスク

両者
- 最先端の術を利用する事が難しい
  （セキュリティベンダーのリスクヘッジのため、実績のあるもののみ展開）

（出典）研究開発戦略専門調査会第 10 回会合　鵜飼委員発表資料

参考 15

国内産業の育成

海外と日本の違い

- 日本におけるメリット（？）
  → 研究開発リスク、営業マーケティングリスクをヘッジできる
  しかし、北米ではこれらリスクをヘッジできる仕組みがある

- 研究開発リスク
  – 研究開発人材や資金が非常に豊富
  – 研究、開発、事業化、産業化に至るプロセスやモデルが確立

  技術者が起業しても大きくできる仕組みがある
  （VCのハンズオン、政府調達による実績作り、豊富な専門人材など）

- 技術力(質)そのものには大きな違いはない
  – アイデアやシーズを事業化、産業化する仕組みが大きく異なる
  – 日本のセキュリティ業界にとっては変化のインセンティブは薄い

（出典）研究開発戦略専門調査会第 10 回会合　鵜飼委員発表資料

参考 16

NISTの概要

NIST National Institute of Standards and Technology U.S. Department of Commerce

沿革とミッション

- 1988年、規格基準局を改組する形で設立。米商務省傘下の連邦研究機関。法的拘束力を持たない非規制機関の位置づけ。
- 経済保障を強化し生活の質を高めるよう科学的測定方法・標準・技術を改善し、米国の技術革新及び産業競争力を強化することがミッション。

機能

ナノテクノロジーや国土安全保障、情報技術、先進製造業などの先進分野を対象に、計測システムの改善、新技術の開発、標準規格の策定・促進、技術評価ツールの提供などを担う。

組織

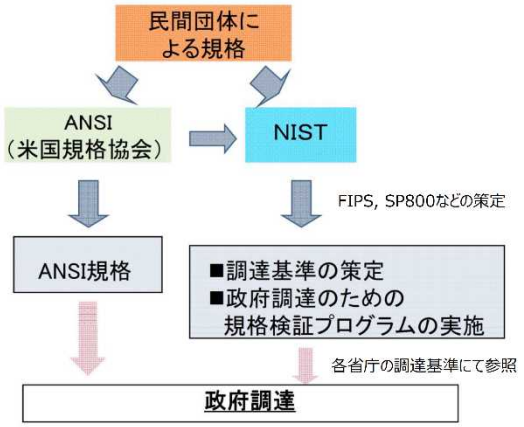
約3,500名の連邦職員が所属。以下3部門より構成される。

1. 研究所プログラム部門：組織内プログラムを統括
   （サイバーセキュリティを所管するITL*1 CSD*2などが所属）
2. 業界・イノベーションサービス部門：組織外プログラムを統括
3. 管理リソース部門：人材、設備等をサポート

*1…Information Technology Laboratory
*2…Computer Security Division

技術標準の策定、検証プログラムの実施

情報セキュリティ標準（FIPS*3）及びガイドライン（SP*4）などを連邦政府機関向けに策定し、同規格に基づく検証プログラムを提供。これらが政府調達に採用されるとともに、民間企業にも参照されることで、技術標準として普及する流れが出来ている。



出典：株式会社三菱総合研究所　調達における標準化機関の役割をもとにNISC作成

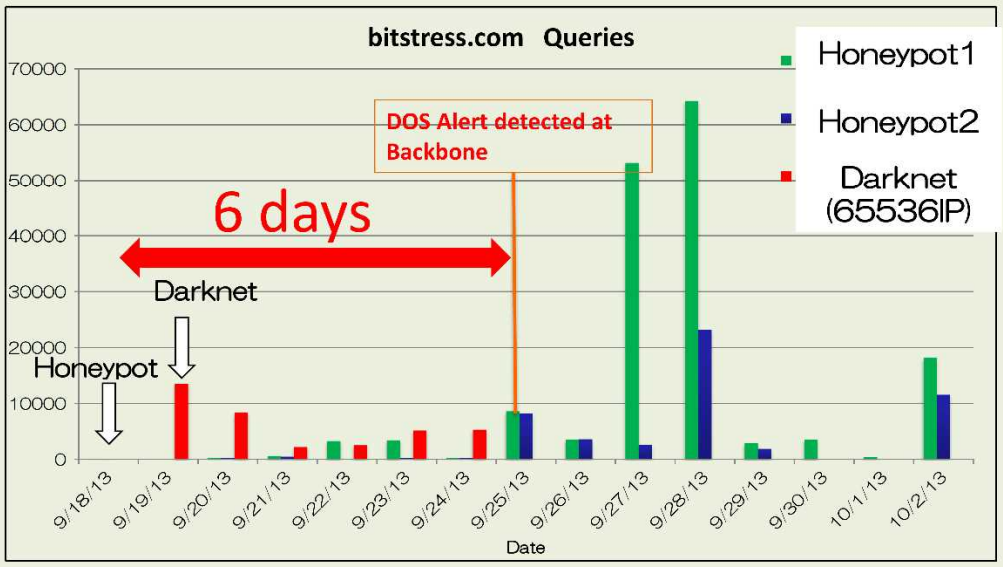
*3…Federal Information Processing Standards
*4…Special Publications

（出典）研究開発戦略専門調査会第 10 回会合　事務局資料

参考 17

早期のDRDoS攻撃の検知が可能

実際の大量はDoS攻撃の前に、不正なあるレベルの大量な攻撃を検知した。
攻撃者は、実際の攻撃の前に試験的にテスト攻撃をしたり、徐々に攻撃が増えていく傾向にある様子。



（出典）研究開発戦略専門調査会第 10 回会合　中尾補佐官発表資料

参考 18

諸外国のサイバーセキュリティ研究開発に関する取組

NISC

米国 （参考1）

- 研究開発に特化した戦略「2016 Federal Cybersecurity Research and Development Strategic Plan 」を策定。 4つのサイバーセキュリティ対策のカテゴリ（阻止、防御、検知、適用）を定義し、それぞれについて、短期・中期・長期の研究開発の取組を規定。
- 毎年度、実行計画「Implementation Roadmap」を策定し、NIST, NSF, NSA, DARPA, DHS, DoD等を中心に産学官が連携して研究開発を推進。
- 2019年度要求で7.4億ドルの予算を計上。

英国 （参考2）

- 全体戦略の「NATIONAL CYBER SECURITY STRATEGY 2016-2021」において、①DEFEND（防御），②DETER（阻止），③DEVELOP（開発）を柱に掲げ、特に③の部分で研究開発を位置付け。
- 「cyber security science & technology strategy」において重点分野（IoTとスマートシティ，データと情報保護，自動化、機械学習とAI等）を特定。
- 政府主導の下、ACE (Academic Centre of Excellence)と呼ばれる枠組みの下、認定基準をクリアした大学が中心となって研究開発を推進。

イスラエル （参考3）

- 全体戦略の「ISRAEL CYBER SECURITY STRATEGY」にて、①ロバストネス（頑健性）②レジリエンス（強靭性）、③ディフェンス（防御）の3つの柱を掲げ、これらに必要な能力構築の一環として研究開発を位置付け。
- ベングリオン大学、テルアビブ大学等の６つの大学において、政策や技術等の異なる分野に焦点を当てたサイバーセキュリティ研究センターを設置。
- 政府主導プロジェクトとして、南部ベルシェバに産・官・学・軍が同居する「サイバースパーク」を設置。サイバー分野でのエコシステムを生み出し、イノベーション活性化を狙う。

シンガポール （参考4）

- 全体戦略の「Singapore Cybersecurity Strategy 2016」において、①弾力性のあるインフラ構築、②より安全なサイバー空間の維持、③活気あるサイバーエコシステムの開発、④国際パートナーシップの強化の４つの柱を掲げ、特に③の部分で研究開発を位置付け。
- 実行計画である「National Cybersecurity R&D Programme(NCR)」において、2020年までのR&D実行計画を策定。
- 産・学・官の連携組織として、シンガポールサイバーセキュリティコンソーシアムを設立。

（出典）研究開発戦略専門調査会第 9 回会合　事務局資料

参考 18

米国の連邦サイバーセキュリティ研究開発戦略プラン

NISC

○　国家科学技術会議（NSTC）が主導して策定した「2016年連邦サイバーセキュリティ研究開発戦略プラン」に基づいて具体的な注力分野を特定。
○　研究開発の実行計画を年度ごとに策定し、産学官において推進。

✓ 4つのサイバーセキュリティ対策のカテゴリ（Deter：阻止, Protect：防御, Detect：検知, Adapt：適用）を定義し、短期、中期、長期の取組を規定。
加えて、上記を活かす先端的技術として、以下の分野の研究開発に注力。
①サイバーフィジカルシステム, IoT　④自律システム
②クラウドコンピューティング　⑤モバイル機器
③高性能計算

✓ NIST, NSF, NSA, DARPA, DHS, DoD等が、本戦略に基づく実行計画を年度ごとに策定し、産・学と連携しながら研究開発を推進。2019年度要求で7.4億ドルの予算を計上(プライバシー分野も含む)。

	Deter（阻止）	Protect（防御）	Detect（検知）	Adapt（適用）
短期	• 攻撃レベルの測定基準 • 攻撃抑止と犯罪・経済制裁の関係性評価	• セキュアなアップデートメカニズムの開発 • エビデンスベースのアセスメント技術 • 軽量暗号、プライベートデータベース、耐量子計算機暗号	• ネットワークをマップするための自動化ツール • セキュリティオペレーションツールのUI改善	• 攻撃が発生しても、重要な資産の利用継続が可能となる技術
中期	• リアルタイムのアトリビューション	• 脆弱性を減らす静的・動的解析ツール • セキュリティポリシー導出自動化ツール • 98%の確率でSWとHWの真正性を検証するツールと技術	• 悪意のあるサイバー活動の特定（フォルスポジティブ率、フォルスネガティブ率の低減）	• 相互依存システムの機能のタイムリーな回復
長期	• 正確かつ効率的な攻撃者の特定	• 10万行のコードあたり1つの欠陥を持つソフトウェアの開発をサポートするツール • 10年間で2桁のオーダーでセキュリティ制御の有効性と効率を向上	• 自動サイバー脅威予測ツール	• 適応的で効果的な集団防御

（出典）研究開発戦略専門調査会第９回会合　事務局資料

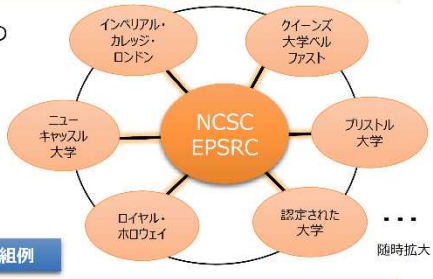
参考 18

英国のACE (Academic Centre of Excellence)の概要

NISC

○　英国サイバーセキュリティセンター（NCSC）と工学・物理科学研究評議会（EPSRC）による認定基準をクリアした大学により構成されるACE(Academic Centre of Excellence)の枠組みを中心に、サイバーセキュリティの研究開発を推進。

✓ 2001年に、「英国のサイバー攻撃に対するレジリエンス向上」のための産学官連携を目的としてEPSRCとGCHQによりACEの枠組みを立上げ（その後、GCHQの役割をNCSCが継承）。
✓ 2019年1月時点で17の大学が認定を受けて参加。
✓ 認定された大学に対して、毎年約20,000ポンドの助成金を付与。



参加大学が注力している研究分野

- 暗号、鍵管理および関連プロトコル
- 情報リスクマネジメント
- システムエンジニアリングとセキュリティ解析
- 情報保証の方法論
- 運用保証技術
- 戦略技術と製品の安全性に関する研究
- サイバーセキュリティと人的要因の科学
- 信頼性と信頼性の高いシステムの構築

ACE 認定大学の取組例

大学名	専門分野
インペリアル・カレッジ・ロンドン	以下を含むセキュアかつレジリエントなソフトウェアシステム工学 ・運用システムと情報アシュアランス ・セキュリティ分析とシステム検証
ニューキャッスル大学	・ソーシャル技術を用いたサイバー犯罪 ・インフラのセキュリティアシュアランス ・サイバーセキュリティ科学
クイーンズ大学ベルファスト	・サイバーフィジカルシステムセキュリティ ・リアルタイムネットワーク分析と仮想化 ・高機能/省電力暗号アーキテクチャ
ロイヤル・ホロウェイ	・理論的かつ実践的な暗号アプリケーション ・サイバーセキュリティの社会的、技術的、組織的観点 ・RFIDタグやスマートタグ、組込機器の情報アシュアランス

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考 18

イスラエルのサイバーセキュリティエコシステム

○ 軍・産・官・学が連携したサイバーセキュリティエコシステムが特徴。サイバーセキュリティ研究センターを中心とした学術エコシステムとスタートアップを多数輩出するサイバースパークが存在。

✓ **安全保障分野を端緒とした学術エコシステム**

- ベングリオン大学、テルアビブ大学等の６つの大学に、政策や技術等の異なる分野に焦点を当てたサイバーセキュリティ研究センターを設置。学術エコシステムとして機能している。
- 国防分野におけるサイバーセキュリティへの投資がエコシステムの原動力。
- 人材育成においては、中等教育と兵役期間中の専門教育の影響大。高校からサイバー分野の教育を実施し、サイバー分野の適性のある者は、高校卒業後の兵役期間中にサイバー関連部署に配属されて専門能力を習得。兵役終了後、大学や民間で活躍。

✓ **サイバースパークの設立**

- ネタニヤフ首相及び国家サイバー局のイニシアチブにより、南部都市ベルシェバに2014年に設置。サイバー分野のエコシステム活性化を狙う地理的な産・官・学・軍のクラスター。
- 企業では、ドイチェテレコム、EMC、ロッキードマーティン、オラクル、IBMなどの多国籍企業やJVPなどのベンチャーキャピタルが入居しており、多数のスタートアップが活動中。

（出典）研究開発戦略専門調査会第９回会合　事務局資料

参考 18

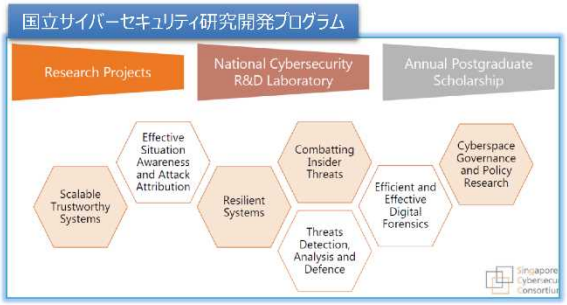
シンガポールの国立サイバーセキュリティ研究開発プログラム

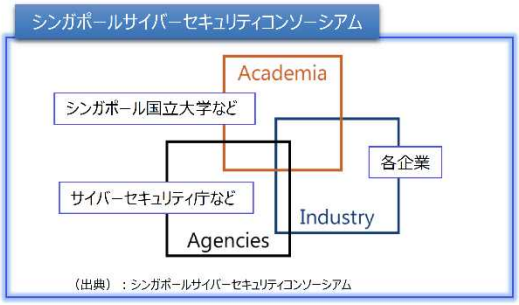
○ 2013年に策定した「サイバーセキュリティ研究開発プログラム」に基づき、シンガポール国立大学、国立研究財団（NRF）が中心となり、サイバーセキュリティに係る研究開発を推進。
○ また、産学官連携組織としてシンガポールサイバーセキュリティコンソーシアムを設立。

✓ 研究開発の注力分野として以下の6つテーマを挙げ、シンガポール国立大学、国立研究財団（NRF）が中心となって研究開発を推進。2020年までに総額1.9億ドルを予算として計上。

①拡張性のあるトラスト確保システム（Scalable Trustworthy Systems）
②レジリエントシステム（Resilient Systems）
③効果的な啓発と攻撃の特定（Effective Situation Awareness and Attack Attribution）
④内部犯行（Combatting Insider Threats）
⑤脅威検出、分析、防御（Threats Detection, Analysis and Defence）
⑥効率的かつ効果的なデジタルフォレンジック（Efficient and Effective Digital Forensics）

✓ また、2016年にサイバーセキュリティにおける研究、人材育成、啓発を目的とした産学官連携組織としてシンガポールサイバーセキュリティコンソーシアムを設立。





（出典）研究開発戦略専門調査会第９回会合　事務局資料

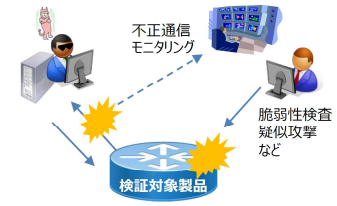
参考 19

サプライチェーンリスク対応のための技術検証体制の整備について

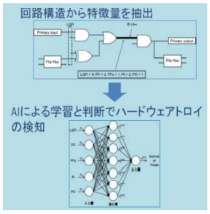
- **Society5.0の進展、サイバー攻撃の複雑化・巧妙化に伴い、サプライチェーンリスクの問題が顕在化。諸外国においても、対応強化のための取組が進められている。**
- **我が国においても、ICT機器の信頼性を検証するための技術開発と推進体制の構築を進め、サプライチェーンリスクに対応するための技術検証体制の整備を推進することが必要。**

（１）検証技術の開発

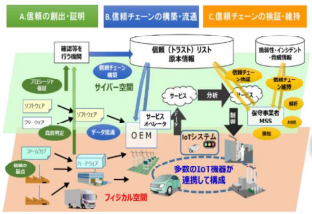
脆弱性、不正機能のチェック



ハードウェアトロイの検出



信頼性・安全性確保のための基盤構築



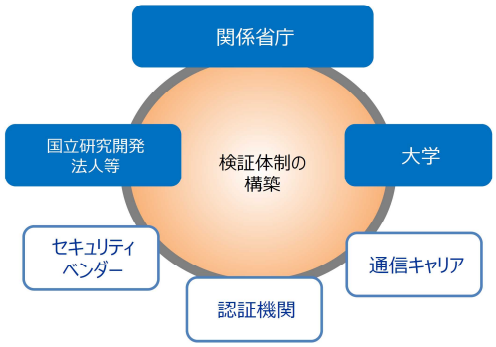
サプライチェーン全体を守るための『サイバー・フィジカル・セキュリティ対策基盤』の開発

【成果の一例】
信頼の起点となる暗号モジュール，セキュリティチップ等の開発など

（２）推進体制の整備

推進体制の整備

オールジャパンの官民連携体制の構築



検証結果の活用方策の推進

政府機関や重要インフラ事業者等のシステムで活用するための措置を推進

（出典）NISC 作成資料

参考 20

戦略的イノベーション創造プログラム（SIP）第2期
IoT社会に対応したサイバー・フィジカル・セキュリティ

プログラムディレクター：後藤厚宏（情報セキュリティ大学院大学 学長）
実施期間：2018年度～2022年度　　平成31年度予算案：22.0億円（平成30年度：25.0億円）

目指す姿

概要

セキュアな Society 5.0 の実現に向け、様々なIoT機器を守り社会全体の安全・安心を確立するため、IoTシステム・サービス及び中小企業を含む大規模サプライチェーン*1全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行う。多様な社会インフラやサービス、幅広いサプライチェーンを有する製造・流通・ビル等の各産業分野への社会実装を推進する*2。

*1: 自動車産業の延べサプライヤー数は100万社超（2012年）　*2:「未来投資戦略 2017」閣議決定（2017年6月）

目標

スマート家電等の一般消費者向けの機器から産業用システムまで、多様なIoT機器・システム・サービスのセキュリティを確保できる『サイバー・フィジカル・セキュリティ対策基盤』を確立する。実証を通じて有効性を確認し、実稼働するサプライチェーンに組み込み実用化する。本基盤の社会実装を他国に先駆けて推進することで、サイバー脅威に対するIoT社会の強靭化を図り、我が国のセキュアなSociety5.0実現に寄与する。

出口戦略

当初から課題認識のある製造・流通・ビル等のユーザ企業と連携した研究開発と実証実験を進め、参画企業が主体的に製品化・事業化。欧米の基準とすり合わせながら府省による制度整備と連携してIoTシステム・サービスやサプライチェーンへの導入を促進し、2030年までにサプライチェーン対策が求められる中小企業の50%に成果の導入を目指す。

社会経済インパクト

IoT社会の強靭化（サイバー犯罪による経済損失回避）により、Society5.0の実現がもたらす約90兆円の価値創出を支える。さらにグローバルなサプライチェーンに参画する要件*3となるセキュリティ確保を適切なコストで実現することにより、日本の製品・サービスの国際競争力を強化（輸出主体の製造業の参入機会の確保）する。

*3: 米国のNIST SP800-171や、欧州のサイバーセキュリティ認証フレームワーク等の動き

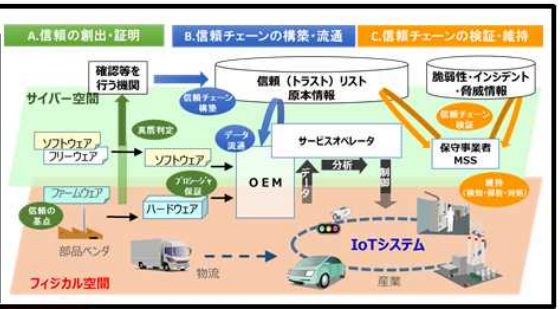
達成に向けて

研究開発内容

IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、IoTシステム・サービス及びサプライチェーン全体のセキュリティを確保するため、

A. 信頼の創出・証明　（IoT機器向け真贋判定技術 等）
B. 信頼チェーンの構築・流通　（トラストリストを用いた信頼チェーン構築技術 等）
C. 信頼チェーンの検証・維持　（インシデントの検知・解析・対処など信頼チェーンの維持技術 等）

及び、その他、必要な研究開発・動向調査を行い、実サービスや各産業分野において実証を行う。



関係府省：総務省、経済産業省、NISC、IT室、警察庁、防衛省、厚生労働省

（出典）研究開発戦略専門調査会第 10 回会合　内閣府発表資料

参考 21

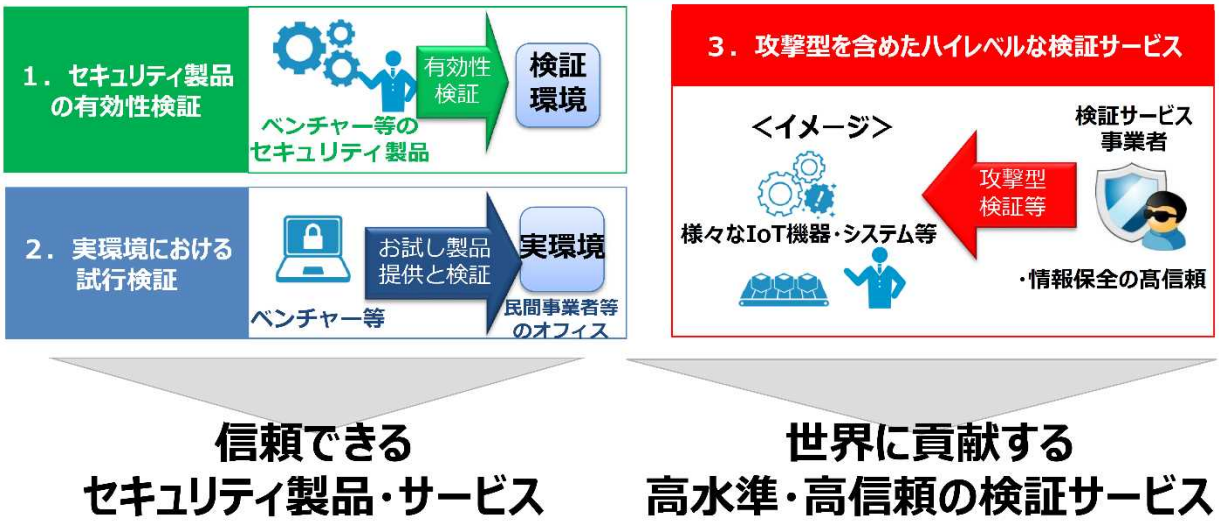
※名称については Proven in Japan 等、他の候補含め検討中

包括的なサイバーセキュリティ検証基盤を構築し、『Checked by Japan（Proved by Japan）』を促進

- 「Checked by Japan」では、2つの方向を追求し、**セキュリティビジネスの成長を促進。**

① 有効性確認等を通じ、日本発のサイバーセキュリティ製品のマーケット・インを促進

② IoT機器等の信頼性を高度に検証するハイレベル検証サービスの拡大



信頼できるセキュリティ製品・サービス

世界に貢献する高水準・高信頼の検証サービス

（出典）研究開発戦略専門調査会第 10 回会合　経産省発表資料

参考 22

5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

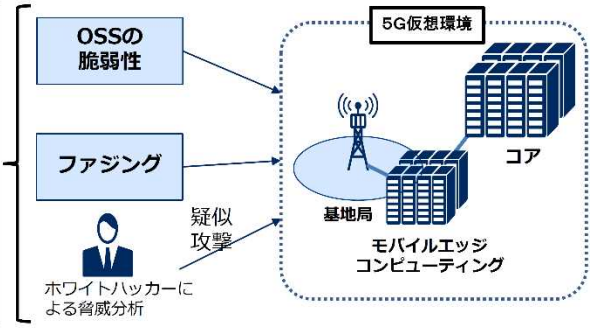
第５世代移動通信システム（５G）は、IoTシステムの基盤技術であるため、５Gに係る各構成要素（デバイス、クラウド、アプリ等）におけるセキュリティを総合的かつ継続的に担保する仕組みを整備し、対策の共有等を図ることを通じ、５Gを活用する重要インフラ事業者等への周知・啓発を図る。

＜基本的考え方＞

- ネットワークインフラとしての機能維持のためには、コア網の機器調達のみに留意すれば良いわけではない。ネットワークのエッジ（基地局の直前）に位置するモバイルエッジコンピューティングのセキュリティが確保されない限り、機能停止/不正動作等のおそれあり。
- 重要通信については、SDN/NFV/スライス等のネットワーク制御技術のセキュリティ対策に加え、５G環境下でのネットワークサービスの各構成要素（デバイス、クラウド、アプリ等）全体を考慮することが必要。

＜平成31年度実施内容＞

- ５Gの仮想環境を構築し、以下の手法により、ネットワークに潜在する脆弱性調査及びセキュリティ課題の洗い出しを実施。
  - ①５Gに実装されるオープンソースソフトウェア等の解析
  - ②多種多様なパターンのデータ送付（ファジング）による異常動作の確認
  - ③ホワイトハッカーによる脆弱性調査、脅威分析
- その結果を踏まえた対応策の策定とその周知・啓発を図る。

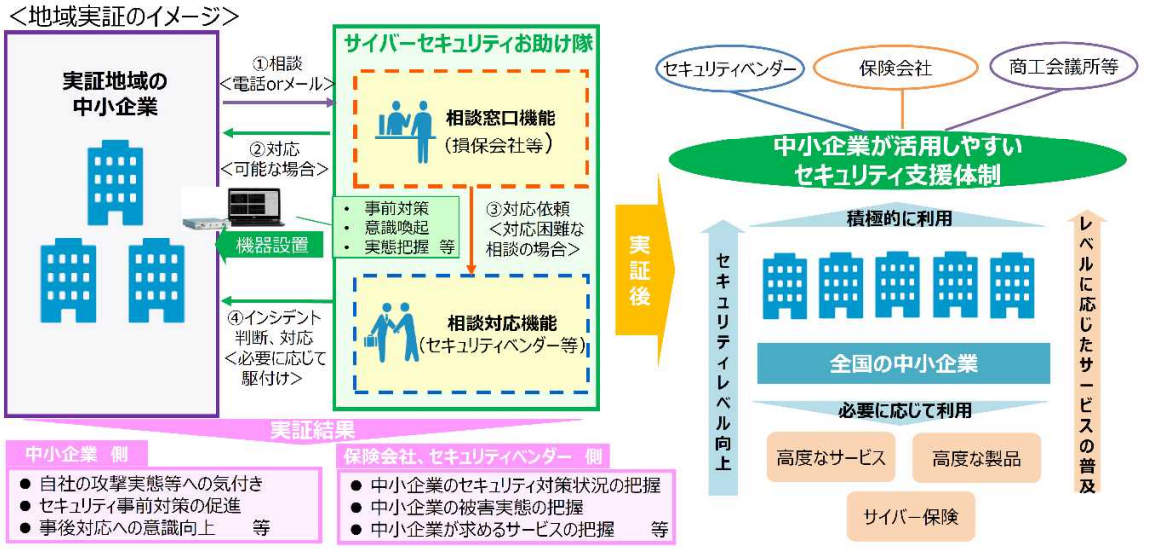


（出典）研究開発戦略専門調査会第 10 回会合　総務省発表資料

参考 23

サイバーセキュリティお助け隊の実証

- 中小企業向けにサイバーセキュリティに関する支援の仕組みを新たに構築し、全国最大8地域を対象に地域の団体、企業等と連携した実証を行い、サイバー攻撃の実態や対策のニーズを把握するとともに、中小企業の事前対策の促進、意識喚起を図る。
- 実証後は、保険機能とも連動した中小企業が利用しやすい支援体制の構築を目指す。



（出典）研究開発戦略専門調査会第 10 回会合　経産省発表資料

参考 24

コラボレーション・プラットフォームの今後の方向性

- 新規参加企業の増加を促し、人脈形成の機会を強化するとともに４つの観点でのコラボレーションの実現を目指す。

【政策とのコラボレーション】

政策に関する意見交換の機会を増やし、**参加者からのご意見を着実に政策に反映**。

※ コラボレーション・プラットフォームだからこそ実現可能。

【シーズサイドのコラボレーション】

ベンダー企業間で連携を図り、**より大きなソリューションを市場に流通**。

※ ベンダー同士でチームを組むことにより、解決できる課題や販売網の拡大を期待。

【ニーズサイドのコラボレーション】

ユーザ企業や大学等の間で課題を共有し、**セキュリティに関するニーズを具体化**。

※ セキュリティ担当者が少ない企業からは、悩みを共有できる仲間がいなくて困っているとの声も。

【ニーズとシーズのコラボレーション】

ニーズサイドとシーズサイドの連携を図り、**ビジネスマッチング**につなげる。

※ 規模の小さな企業からはユーザ企業等とのパスがなく事業拡大が困難との声も。

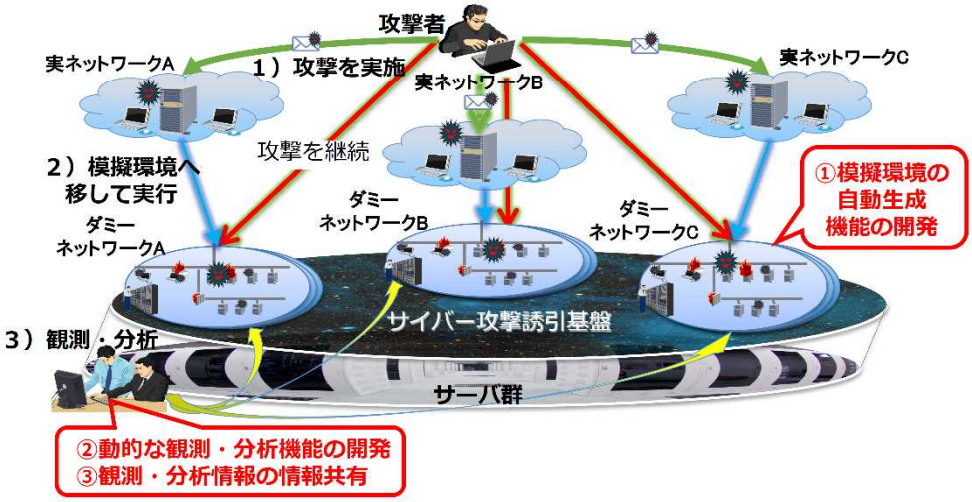
（出典）研究開発戦略専門調査会第 10 回会合　経産省発表資料

参考 25

サイバー攻撃誘引基盤の構築（STARDUST）

○　高度かつ複雑なサイバー攻撃に対処するため、政府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、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することが可能な、高度で効率的なサイバー攻撃誘引基盤を構築。

○　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実証を行うための研究開発環境を、情報通信研究機構（NICT）に整備。分析結果は、セキュリティ対策機関等と連携して情報共有を図り、安全なサイバー空間を実現。

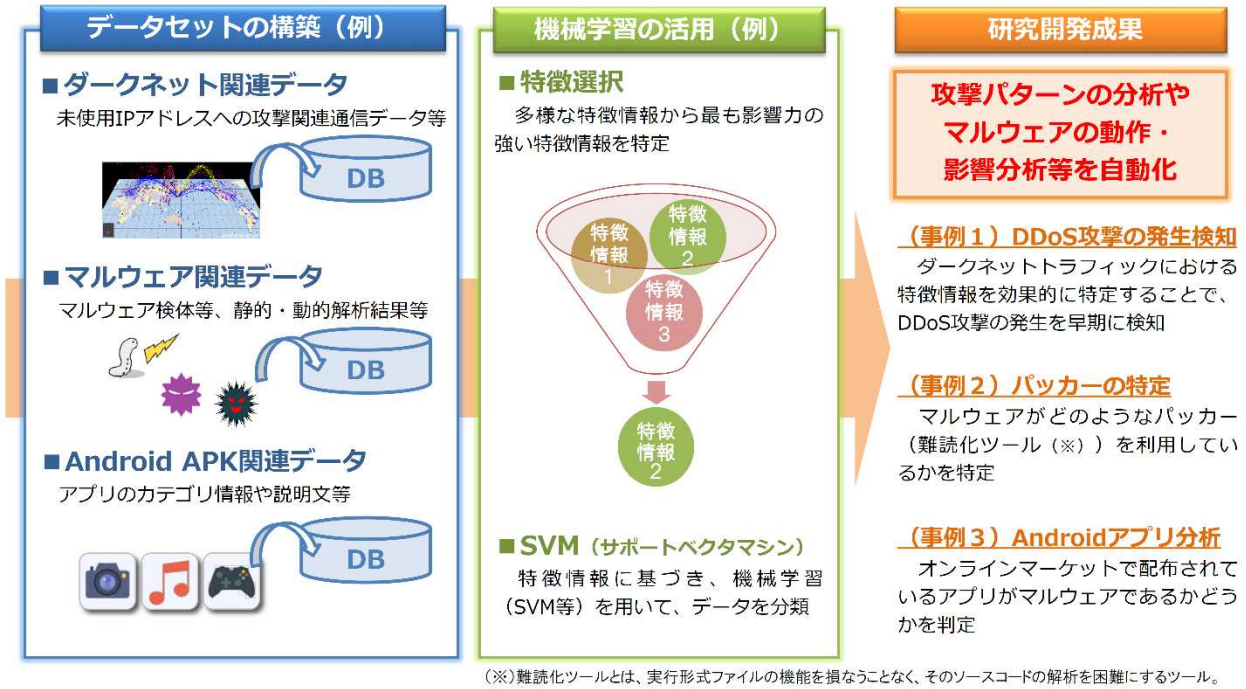


（出典）研究開発戦略専門調査会第 10 回会合　総務省発表資料

参考 26

機械学習（AI技術）を活用したサイバーセキュリティの研究開発

○　NICTでは、巧妙化・高度化するサイバー攻撃に対して、機械学習を始めとするAI技術を活用したサイバーセキュリティの研究開発に取り組んでいる。

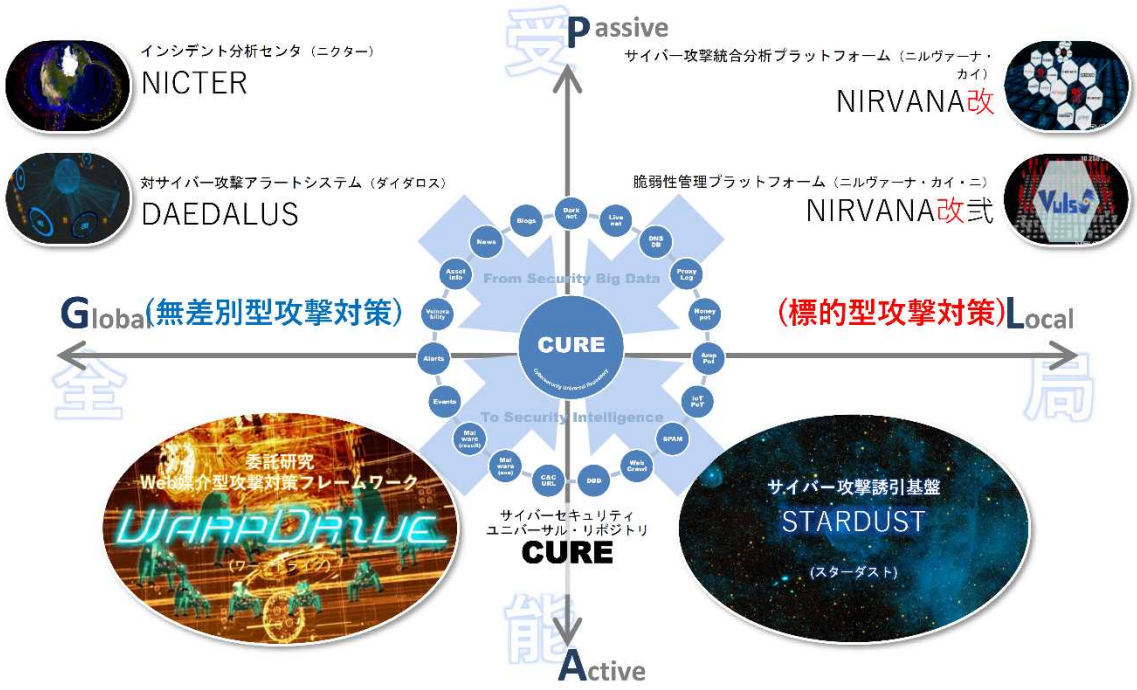


（※）難読化ツールとは、実行形式ファイルの機能を損なうことなく、そのソースコードの解析を困難にするツール。

（出典）研究開発戦略専門調査会第 10 回会合　総務省発表資料

参考 27

事例：高度分析のためのデータ収集（NICT）



（出典）研究開発戦略専門調査会第 10 回会合　中尾補佐官発表資料

参考 28

光・量子飛躍フラッグシッププログラム（Q-LEAP）

2019年度予算額（案）　：2,195百万円
（前年度予算額　　：2,200百万円）

背景・課題

- ✓ 量子科学技術は、近年の技術進展により、**超スマート社会**（Society5.0）実現に向けた社会課題の解決と産業応用を視野に入れた**新しい技術体系**が発展する兆し。
- ✓ 欧米等では「第２次量子革命」とうたい、**世界的に産学官の研究開発競争が激化**※。我が国の**官民研究開発投資を拡大**し、量子科学技術の研究開発を強化し、他国の追随に対し、**簡単にコモディティ化できない**知識集約度の高い技術体系を構築することが重要。
- ✓ **日本の優れた量子科学技術の基礎研究をいち早くイノベーションにつなげ、「生産性革命」の実現に貢献**することが必要。

※ Google：Quantum AI研究所を設立（2013～）、英国：5年間で£270Mの研究イニシアチブ（2014～）、EU：€1B規模の「量子技術Flagship」 中国（2019～）等

事業概要

【事業の目的】
- ✓ **Q-LEAPは、経済・社会的な重要課題に対し、量子科学技術を駆使して、非連続的な解決（Quantum leap)を目指す研究開発プログラム**

【事業概要・イメージ】
- ✓ 異分野融合、産学連携の**ネットワーク型研究拠点**による研究開発を推進
- ✓ 技術領域毎に**PDを任命**し、**適確なベンチマーク**のもと、実施方針策定、予算配分等、**きめ細かな進捗管理**を実施
- ✓ ネットワーク型研究拠点の中核となる**Flagshipプロジェクト**は、**HQ**を置き**研究拠点全体の研究開発マネジメント**を行い、事業期間を通じて**TRL6(プロトタイプによる実証)**まで行い、企業（ベンチャー含む）等へ橋渡し
- ✓ **基礎基盤研究**はFlagshipプロジェクトと**相補的かつ挑戦的な研究課題**を選定

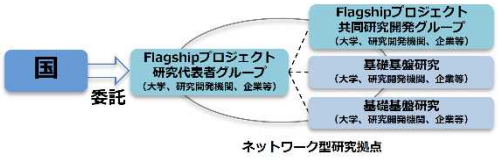
【対象技術領域】

① **量子情報処理（主に量子シミュレータ・量子コンピュータ）**
- ・材料科学や創薬、AI、最適化問題などへの適用を視野に、社会・経済に大きなインパクトを与え得る**汎用量子コンピュータ等のプロトタイプを開発**し、クラウドサービスによる利用者への提供等を実現

② **量子計測・センシング**
- ・**従来技術を凌駕する精度・感度**により、室温で高感度計測を実現する**ダイヤモンドNVセンタを用いて**脳磁計測システムやエネルギーデバイスの電流・温度の計測等を実現

③ **次世代レーザー**
- ・**電子の動きの計測・制御**を実現する**アト(10⁻¹⁸)秒スケールの極短パルスレーザーの開発・活用**により、化学反応メカニズム解明等を実現
- ・加工学理や機械学習を活用し、ワンストップで最終形状に仕上げが可能な高精度・低コストの**CPS（サイバー・フィジカル・システム）型次世代レーザー加工技術**を実現

【事業スキーム】
- ✓ 事業規模：6～8億円程度／技術領域・年
- ✓ 事業期間：**最大10年間**、ステージゲート評価の結果を踏まえ研究開発を変更又は中止



（出典）研究開発戦略専門調査会第 10 回会合　文科省発表資料

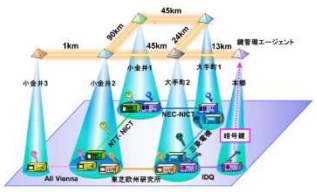
参考 29

我が国の取り組みの経緯と現状

2010年 → 2018年 → 2023年

NICT委託研究 → **ImPACT** → **SIP第2期**

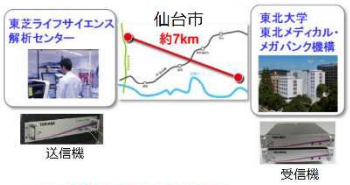
2010年、東京量子暗号ネットワークテストベッドを構築



✓ 動画の量子暗号化を世界で始めて実現

NEC：サイバーセキュリティ関連施設で試験運用

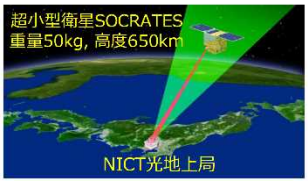
東芝：ゲノム解析データの暗号通信



✓ **世界最高速の装置**を開発
300kbps @45km （東芝）
海外製の**10倍高速、2倍長距離**

✓ 鍵管理アーキテクチャ確立

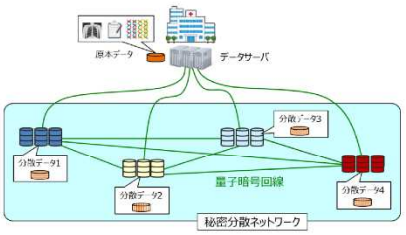
✓ 新たなアプリの開発
「超長期セキュアデータ保管」
(**量子暗号x秘密分散**)



✓ NICTが超小型衛星で量子通信を実証（2017年）

光・量子を活用したSociety5.0実現化技術

量子セキュアクラウド技術を開発し、将来にわたり安全なデータ保管と利活用を実現



➢ 専用用途での量子暗号サービス
政府重要拠点間等での利用を検討 ⇒ 民間用途への展開

➢ 標準化、運用ガイドライン案を策定

➢ 量子セキュアクラウドシステムの社会実装

総務省・委託研究 →
衛星通信における量子暗号技術

（出典）研究開発戦略専門調査会第 11 回会合　NICT 発表資料