「先進的サイバー防御機能・分析能力強化」に関する研究開発構想（プロジェクト型）

令和 5 年 10 月
（令和 8 年 4 月改定）

内閣府
経済産業省

目次

1. 事業の背景、目的、内容

（1）事業の目的

① 政策的な重要性

サイバー空間の「公共空間化」が進展し、サイバー空間において提供される多様なサービスが複雑化するに伴いサイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化している。

また、近年では、人工知能（AI）を活用した攻撃に代表される新たなサイバー攻撃のリスクが生じている。例えば、AI が不正メール検知ツールの応答を学習することで検知機能を回避することが可能なメール文面を生成することによる攻撃手法が報告されているほか、アンチウイルスソフトの検知結果を機械学習し、検出を回避するマルウェアの生成手法に関する研究が報告されている。さらに、量子計算機の活用の広がりに伴う既存暗号の危殆化によりデータが漏洩するリスクが顕在化している。

こうした状況にあって、「自由、公正かつ安全なサイバー空間」を確保するためには、これらをとりまく不確実性の変容・増大によって生じるリスクを適切に把握した上で対応していくことが必要となっている。

「経済安全保障重要技術育成プログラム研究開発ビジョン（第二次）」（以下「二次ビジョン」という。）においても、『次々と生まれる新たな攻撃技術に対し、高度なサイバー防御を図るため、サイバー空間の適切な状況把握や攻撃技術に対する知見の蓄積、偽情報の見極めや対策能力の高度化、さらには、ＡＩや量子計算機に対応可能な防御能力の高度化に向けた取組が求められている。』『我が国を取り巻く不確実性の変容・増大に対応するため、「国民の安全と安心を確保する持続可能で強靱な社会」への変革に向けて、サイバー空間と現実空間の融合システムにより安全・安心を確保する基盤の構築に向けた取組を引き続き進める必要がある。』との認識が示されているとおり、先進的なサイバー防御機能や分析能力を強化していくことは、経済安全保障の確保・強化の観点から重要となる。

二次ビジョンでは、領域横断・サイバー空間領域で支援対象とする技術として、

- 先進的サイバー防御機能・分析能力の強化（サイバー空間の状況把握・防御技術、セキュアなデータ流通を支える暗号関連技術）

が挙げられている。先進的なサイバー防御機能や分析能力を強化していくに当たっては、「サイバー空間の情報を収集・調査する状況把握力」「サイバー攻撃から機器やシステムを守る防御力」「サイバー攻撃を抑止する抑止力」の視座に立って、能力の向上に努めることが重要となる。

また、AI の急激な進歩により攻撃手法が多様化しており、更なる先端技術を用いた対策が急務となったことに加え、進歩した AI を用いたセキュリティ技術の研究の必要性も増大していること、懸念国の支援を受けた複数のサイバー関連企業による不正な活動の存在が 2025 年 8 月末に我が国政府を含む関係諸国により公表されるなど、地政学リスクを含むサイバーリスクが高まっていることにより、国内産業基盤の強化を通じた供給力を早急に拡大する必要性が増大している。

以上を踏まえ、サイバー空間の状況把握力や防御力の向上に資する技術や、セキュアなデータ流通を支える暗号関連技術等を開発し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを本構想の目的とする。

② 我が国の状況

AI を活用した攻撃に代表される新たなサイバー脅威の影響が深刻化する可能性があることや、官民におけるデジタルインフラの構築に伴うリスクも新たに発生する可能性があるなど、サイバー攻撃による社会への影響は、技術の進展や環境変化によって深刻度を増す可能性がある。DX の進展にともない企業の IT 依存度が増している中、特定企業へのサイバー攻撃がサプライチェーン全体、ひいては日本社会全体に広く負の影響を及ぼすような事例が多発している。また、生成 AI の普及や量子等の先端的な技術の進展とともに、昨今の国際情勢の複雑化、社会経済構造の変化等により安全保障の裾野が経済を含むサイバー分野に拡大する中、サイバー空間の安全・安心の礎となる研究開発の重要性はますます高まっている。

こうした中、戦略的イノベーション創造プログラム（SIP）においては、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全体を守る「サイバー・フィジカル・セキュリティ対策基盤」を開発し、実稼働するサプライチェーンに組み込み実用化することで、サイバー脅威に対する IoT 社会の強靭化を図るための課題「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（2018 年度～2022 年度）が実施されたところであり、現在、社会実装に向けた取組が進められている。政府内では経済産業省を中心としてサプ

ライチェーン全体、日本社会全体でのサイバーセキュリティを底上げする取り組みが進んでおり、IoT 製品のセキュリティ達成度ラベリング制度である JC-STAR が令和 7 年 3 月から運用を開始した。またサイバー・フィジカル・セキュリティ・フレームワークを元に各業界（ビルシステム、工場システム、半導体工場、スマートホーム、自動車分野、電力分野、宇宙分野等）のサイバーセキュリティガイドラインの制定が進んでおり社会実装が進んでいる。サプライチェーン強化に向けたセキュリティ対策評価制度も令和 8 年度に運用を開始する予定である。

また、経済安全保障重要技術育成プログラム研究開発ビジョン（第一次）では、支援対象とする技術として「AI セキュリティに係る知識・技術体系」が示され、「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」に関する研究開発構想（個別研究型）を内閣府及び文部科学省が策定したところであり、今後、取組が進められる予定である。

我が国の代表的な研究機関の取組としては、国立研究開発法人情報通信研究機構（以下「NICT」という。）が、Beyond 5G、AI 技術、量子技術、サイバーセキュリティを始めとした ICT 分野における世界最先端の研究開発を戦略的に推進している。サイバーセキュリティ分野については、同分野における NICT に対する社会的要請が高まりつつあることに鑑み、サイバー攻撃の観測・分析・可視化・対策技術、大規模集約されたサイバー攻撃情報の横断分析技術、新たなネットワーク環境等のセキュリティ向上のための検証技術、耐量子計算機暗号等を含む新たな暗号・認証技術やプライバシー保護技術の研究開発等に取り組んでいる。さらに、これらの成果を活用して、サイバーセキュリティ人材の育成、サイバーセキュリティに関する研究開発・人材育成の産学官連携拠点（CYNEX）の構築、サイバー攻撃に悪用されうる IoT 機器の調査・注意喚起等を行う取組である NOTICE 等を実施している。

標的型攻撃等のサイバー攻撃対策に係る取組例としては、模擬ネットワークで攻撃者の活動を察知されないようにリアルタイムで長期観測可能とするサイバー攻撃誘引基盤「STARDUST」を開発・運用している。

サイバー脅威情報の観測・集約・分析に係る取組例としては、NICTER 等の各種サイバー攻撃観測分析基盤の開発・運用、これら観測分析基盤からの情報や、OSINT 情報等を自動集約するシステム「EXIST」等からの情報を一元的に集約し横断分析可能とするセキュリティ情報融合基盤「CURE」を開発・運用している。また、サイバー攻撃統合分析プラットフォーム「NIRVANA

改」についても横断分析機能を開発し、複数組織の端末から攻撃情報を収集して組織をまたぐ俯瞰的な分析を可能としている。

マルウェア分析に係る取組例としては、マルウェアの活動活性化の早期検知や、その機能の詳細分析等について、AI の活用も含めて実施している。

暗号技術に係る取組例としては、耐量子計算機暗号を含む暗号技術の安全性評価、検索可能暗号等の高機能暗号の研究開発、準同型暗号等を応用したプライバシー保護技術の研究開発等を実施している。

人材育成に係る取組例としては、実践的サイバー防御演習「CYDER」等を実施するとともに、演習効果の評価手法の調査研究等も実施している。

CYNEX での取組例としては、ペネトレーションテストの実施を担うレッドチームを編成し、セキュリティ製品・技術毎に独自の検証を実施している。

NOTICE での取組例としては、サイバー攻撃への悪用のおそれのある IoT 機器調査（機器の特定等を含む。）や機器利用者への注意喚起を行っている。

また、国立研究開発法人産業技術総合研究所（以下「産総研」という。）が、循環型社会をけん引する技術として、社会の活動全体をサイバー空間に転写し HPC・AI・ビッグデータ技術を駆使して産業や社会変動の予測や最適化を可能にし、更にサイバー空間での計画をフィジカル空間に作用させ介入・評価・改善する一連のプラットフォーム技術を開発することや、それらに係る安全と信頼を担保する、セキュリティ強化技術やセキュリティ評価技術、セキュリティ保証の在り方についての研究開発に取り組んでいる。

さらに、近年は、今後実用化が期待されている量子計算機に対しても安全で、より高い安全性を備えた暗号技術に対するニーズが増している。従来の計算機では安全であった暗号技術が、量子計算機を活用すれば破られることが知られているため、NICT や産総研において、量子計算機にも耐性のある安全な暗号技術（耐量子計算機暗号）の設計と安全性評価といった研究開発や高機能暗号に係る研究開発等が実施されている。また、令和 6 年度より関係府省庁連絡会議を設置し耐量子計算機暗号への移行ロードマップ策定や国際標準化との連携を進めている。くわえて、内閣府で検討されている「量子技術の実用化推進ワーキンググループ」の「量子セキュリティ・量子ネットワークの論点等」では、「量子セキュリティ・量子ネットワークの利用環境整備と利用実証の拡大」の中で、多様な量子・古典暗号のベストミックスと検証環境の在り方の検討が進められている。

なお、関連する主な政府方針としては、「経済財政運営と改革の基本方針 2023」（令和 5 年 6 月 16 日閣議決定）の中で、「サイバーセキュリティ戦略」

（令和 3 年 9 月 28 日閣議決定）に基づく取組などを進めることが示されているほか、サイバー安全保障における取組を関係省庁の枠組みの下で推進することや、サイバー安全保障分野での対応能力を欧米主要国並みに向上させるため、政府のサイバーセキュリティの強化を図る等が示されており、また、「国家安全保障戦略」（令和 4 年 12 月 16 日閣議決定）において、サイバー安全保障分野での対応能力の向上の一環として、サイバーセキュリティに関する世界最先端の概念・技術等を積極的に活用することや、サイバー安全保障分野における情報収集・分析能力を強化すること、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化する等の方針が示されている。量子技術については「量子未来社会ビジョン」（令和 4 年 4 月）及び「量子未来産業創出戦略」（令和 5 年 4 月）に基づき、量子セキュリティ技術についての検討が進められているほか、量子技術の進展を見据えながら、耐量子計算機暗号等に対応する検討も並行して進められている。さらに、近年における状況変化としてサイバー対処能力強化法[1]及び同整備法[2]が 2025 年 5 月に成立・公布したことにより、これまで以上にサイバー安全保障に資する技術が不可欠となっている。

③ 世界の取組状況

米国では、「Federal Cybersecurity Research and Development Strategic Plan（2019 年版連邦サイバーセキュリティ研究開発戦略計画）」が発表されている。この計画では、「サイバーセキュリティの人的側面の理解」「効果的かつ効率的なリスク管理の提供」「悪意のあるサイバー活動を抑止し、対抗するための効果的かつ効率的な手法の開発」「統合的な安全、セキュリティ、プライバシーのフレームワークと手法の開発」「持続可能なセキュリティのためのシステム開発・運用の改善」の 5 項目の研究開発目標が掲げられている。

また、2023 年 3 月、バイデン政権が「National Cybersecurity Strategy（国家サイバーセキュリティ戦略）」を発表している。この戦略では、サイバー空間における役割・責任・リソース配分を根本的に転換する必要があるとしており、以下の 2 点を示している。

---

[1] 重要電子計算機に対する不正な行為による被害の防止に関する法律

[2] 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律

・　サイバー空間の防護責任の再配分：サイバーセキュリティの負担は、個人・中小企業・自治体から切り離し、最高の能力・最適な立場を備えた組織に移す。
・　長期的な投資を促進するインセンティブの再調整：喫緊の脅威からの防護と、未来に向けた戦略的計画・投資のバランスを取る。

これを達成するアプローチとして以下の 5 本の柱を掲げている。

・　重要インフラの防護
・　脅威主体の阻止と解体（Disrupt and Dismantle）
・　セキュリティ及び強靱性強化のための市場原理の形成
・　強靱な未来（Resilient Future）への投資（ポスト量子暗号等）
・　共通の目標を追求する国際パートナーシップの形成

2025 年現在、トランプ政権下で一部に方針変更が見られるが基本的には上記の方針が受け継がれている。

さらに、国家安全保障局は、耐量子計算機暗号アルゴリズムを開発するためのプロジェクトを 2015 年から開始しており、2024 年には耐量子計算機暗号方式として、FIPS203（ML-KEM)、FIPS204(ML-DSA)、FIPS205(SLH-DSA)が、国立標準技術研究所によって正式に PQC の標準として認定された。

欧州では、2020 年、「EU Cybersecurity Strategy（EU サイバーセキュリティ戦略)」が策定されている。セキュリティ研究開発としては、次期長期 EU 予算、特に Digital Europe Program や Horizon Europe 等を通じて、EU のデジタル移行に伴うサイバーセキュリティ戦略の支援に取り組むこととしている。加盟国は、サイバーセキュリティを強化し、EU レベルの投資に見合うべく EU の強靭化のための設備を最大限に活用することが推奨されている。また、EU と各国予算による共同プロジェクトを通じて、サイバーセキュリティにおける産業・技術的能力の強化が目指されており、デジタルサプライチェーン（データとクラウド、次世代プロセッサ技術、超安全な接続、6G ネットワークなど）全体でサイバーセキュリティのリーダーシップが推進されている。また、Horizon Europe は、EU の研究・イノベーション枠組みプログラムであるが、個別プログラムの 1 つである「第 2 の柱：グローバル・チャレンジ・欧州の産業競争力」の中で設定されている社会課題の 1 つである「社会のための市民安全クラスター」において、サイバーセキュリティをテーマとした研究開発公募が実施されている。また包括的な欧州のサイバーセキュリティ指令であ

る NIS2 指令[3]が 2022 年に採択され、旧 NIS 指令が強化されることにより、より広範な業種に厳格なセキュリティ要件が求められるようになった。2024 年にはデジタル製品のセキュリティを強化する規制である CRA 法（サイバー・レジリエンス・アクト）が発行され 2027 年に義務適用開始が予定されている。

④ 本事業のねらい

先進的なサイバー防御機能や分析能力を強化していくに当たっては、

（１）サイバー空間の情報を収集・調査する状況把握力

（２）サイバー攻撃から機器やシステムを守る防御力

（３）サイバー攻撃を抑止する抑止力

（４）サイバー攻撃の多様化に対する更なる先端技術の活用

の視座に立って、能力の向上に努めることが重要となる。サイバー空間は公共空間化しているため、サイバーセキュリティ技術は本来的に民生利用と公的利用の区別のない共通技術という側面を持っており、刻々と変化する国内外の脅威に対応していくためには、産官学の総力を結集することが速やかな研究開発及び公的・民生利用に繋げていくために重要である。

このため、本事業では、上記（１）状況把握力、（２）防御力、（３）抑止力、（４）先端技術の活用を中心に、我が国サイバー防御・分析能力を向上させることを目的とする。

（２）事業の目標

① アウトプット目標

本事業では、サイバー空間の情報を収集・調査する状況把握力及びサイバー攻撃から機器やシステムを守る防御力の向上、並びにそれら能力・技術の評価技術・環境の開発・展開を目的としている。

研究開発項目① サイバー空間の情報を収集・調査する状況把握力の向上

【中間目標】2025 年度まで

・ 高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術、攻撃者からより多くの情報を獲得するための技術等のサイバー空間の情報を収集・調査する状況把握力の向上に資する基礎技術の確立。

[3] https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

【最終目標】2028 年度まで

・　高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術、攻撃を検知した際に即座に対処するような技術、攻撃者からより多くの情報を獲得するための技術等のサイバー空間の情報を収集・調査する状況把握力の向上に資する技術の社会実装。
・　IoT 機器に利用されるファームウェアの大規模な収集・分析による各種セキュリティリスクの可視化・評価をする技術の社会実装。

研究開発項目② サイバー攻撃から機器やシステムを守る防御力の向上

【中間目標】2025 年度まで

・　AI を活用した脆弱性の検知・評価技術、耐量子計算機暗号の実装技術、ペネトレーションテスト等の検証手法自動化技術等の防御力向上に資する基礎技術の確立。

【最終目標】2028 年度まで

・　AI を活用した脆弱性の検知・評価技術、耐量子計算機暗号の実装技術、ペネトレーションテスト等の検証手法自動化技術等の防御力向上に資する技術及び能動的サイバー防御を始めとした攻撃者側に対抗する措置を組み合わせ、サイバー脅威を防止・抑止するために必要な技術、攻撃者の真のサーバーを確実に、短期間で特定する技術の社会実装。
・　耐量子計算機暗号の実用性を、現行の楕円曲線暗号レベルにまで高める。
・　必要とされる様々な耐タンパー性をより経済的に達成する先端的要素技術の開発、指針やガイドラインの策定を目指す。

研究開発項目③ 共通基盤の整備

【中間目標】2025 年度まで

・　情報の効果的な連携方法の開発
・　高度サイバー人材の評価・管理に関する技術や方法の開発

【最終目標】2028 年度まで

・　共通基盤技術の最適化と攻撃の兆候を早期に発見して迅速に対処する技術の研究開発に資する共通基盤の構築
・　高度サイバー人材の評価・管理に関する技術や方法の展開

・　高度サイバー安全保障人材の育成に資する研究開発及びツールの開発
・　攻撃手法への対処も支援するような、国産生成 AI モデル等を活用した海外製品、海外情報源に依存しない国産情報共有基盤の実現

研究開発項目④　セキュアな量子情報通信技術の開発
【中間目標】2025 年度まで
・　QNSC（Y-00 プロトコル）の高速・大容量化に向けた専用のデジタルコヒーレント方式を研究・開発し、論理検証機を試作開発し、実施検証による方式の確認と高速化（単一波長での目標 20Gbps 以上）への見通しを検証。
・　QNSC（Y-00 プロトコル）の DSP を開発し、Y-00 変復調に適した新たに開発した専用 DSP の機能を基本的な検証実験で確認する。また、光ワイヤレス伝送への応用の可能性を示す。

【最終目標】2026 年度まで
・　QNSC システム構成を確立し、単波長 10G bps 以上（目標 20Gbps）の試作機による実験を実施して方式の有効性及び早期実装への検証。
・　光波長多重による多重化伝送試験を実施し、将来的に 100Gbps 以上の伝送を可能とする見通しを得る。

各項目における具体的な技術開発の内容については、（３）事業の内容に示す。

② アウトカム目標
・　本事業で開発した技術が実装されたサービスを通じて、政府や重要インフラ事業者等が機密性の高い情報等を扱うことができる、高い利便性やセキュリティを有する信頼性の高いサイバーセキュリティ基盤を構築可能とする。本事業で開発した検証技術により、情報の効果的な連携を実現するとともに、高度サイバー人材の評価・管理手法を確立する。
・　QNSC の適用の優先順としては、最初に直接、経済安全保障に関わる政府・公共系の重要情報を扱う専用線や重要インフラ系専用線の対策が優先されると考える。次に経済社会を支えている金融機関や重要情報を扱う企業や医療機関の専用線と考える。またそれらの VPN や広域イーサネットの加入者線への導入も考えられる。更には個人向けの FTTH への適用と展開されていくと考えられる。

（３）事業の内容

本事業において対象とする技術は、我が国が経済安全保障活動、社会経済活動を行う上で必須となる技術である。また、本事業で対象とする技術領域は秘匿性が高いため最新の動向を正確に把握することは困難であるが、世界的にも確立されていない技術領域であると考えられる。

本事業と同様の研究開発構想は民生利用のみならず公的利用につなげていくことが前提となっているため、以下の研究開発項目は全て委託で実施するものとする。

研究開発項目① サイバー空間の情報を収集・調査する状況把握力の向上

ア．研究開発の必要性

サイバー攻撃対策に関しては、収集した情報の蓄積と統合、分析能力のばらつきが課題となっている。基本的にサイバー攻撃対策には情報の蓄積が不可欠であり、新たに確認された情報と既知の情報を照合し、対策を実施することが重要である。一方で、被害者が情報公開を拒むこともあり、IR 事業者もすべての情報を公開することはないため、情報も知見もまばらである。また、政府機関における課題として、攻撃主体や攻撃手法、攻撃の高度さは民間企業に対するものと比較して異なる可能性もあり、民間事例で得られた知見について必ずしも十分に活用できない場合がある。このため政府機関は、自らが受けた攻撃を自らで把握・対処できるための技術的能力を獲得する必要があると考えられる。

また、攻撃主体は周到な準備を背景に、一つ一つの攻撃の実行にかける時間が短縮傾向にあると推測されている。サイバー攻撃対策のための情報収集や対処を行うに当たっては、早期発見及び攻撃主体に気づかれずに解析に移行できることが必要であるが、実際には我が国に対しどのような攻撃がなされているかの全容を把握することは非常に困難である。くわえて、従来の防御の取組だけでなく、攻撃を検知した際に即座に対処するような技術の必要性は一層増大しており、未知の脆弱性や攻撃対象機器を早期に特定し、もって各種セキュリティリスクの可視化や横断的なリスク評価を行う技術も必要である。このため、未知の攻撃を含む、攻撃開始時、現在進行形の攻撃中の痕跡を検出し、分析するための技術的能力を構築していくことが重要である。

イ．具体的研究内容

具体的な要素技術については、主に以下のとおり。

〔1〕 アーティファクト分析技術

① マルウェアの機能的特徴の汎用的な自動抽出技術
マルウェアから機能的特徴を抽出するにあたり、耐解析機能や外的要因・環境的要因による影響を極力低減した特徴量を抽出するための技術。

② マルウェアが利用する暗号化アルゴリズム分析の効率化技術
今後も亜種が増え続けるマルウェアを用いたサイバー攻撃の現状を踏まえ、マルウェアが通信・ファイルの暗号化等に利用する暗号化アルゴリズムを短時間に効率良く同定するための技術及び手法。

③ 攻撃の兆候察知時におけるリアルタイムな攻撃の検知･特定に繋がる、攻撃者の特定のための情報収集技術

④ IoT 機器に利用されるファームウェアの大規模な収集・分析による各種セキュリティリスクの可視化・評価に係る技術

〔2〕 攻撃者からより多くの情報を獲得するための技術

① 攻撃検知を感知されないための技術
攻撃を検知した場合において、攻撃者にこれを察知されることなく攻撃を続行させるために、攻撃を受けた被害環境を欺瞞環境に転化させる技術。また、攻撃を検知したことを攻撃者に察知されると、攻撃者はそこで攻撃を中断する、あるいはダミーの挙動を行う等の可能性があり、サイバー攻撃対策に有益な情報を得られない場合があることから、これを回避するための技術。

② 攻撃意図分析と被害防止を両立するための技術
ホスト上に存在する攻撃者にとって価値のある情報等が不正利用されないように、これらのデータを無害化する等の技術。また、攻撃アクセスを運用環境から欺瞞環境に転化させるに当たり、観測する攻撃を無害化する必要がある一方で、攻撃意図の分析を行うためには、被害環境を忠実に再現する必要があることから、これらを両立するための技術。

③ 攻撃意図分析のための解析・分析技術
収集した情報を蓄積・分析し、統合的な解析を行うための技術。

〔3〕 高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

① センサーエージェント設計技術

検知、分析及び対処を一元的に行うことが可能なエージェントモジュールを設計するために必要となる技術。
※マルウェアの分析技術、証跡を収集するための技術、これらを統合して対処するための技術が含まれる。

② システム設計技術
スレットハンティング、動的ポリシー制御、検知ロジック等の技術。これらの技術を適用し、各種対処を一元的に実施可能なシステムの設計。

③ 通信データ量抑制技術設計
収集する通信データ量を抑制するための技術。
※ユーザーの活動状態を利用したデータの絞り込み等の手法を用い、組織上の多数の端末等から収集される膨大な量のデータを収集・分析するに当たり、現実的な運用を可能とするために必要となる。

ウ．達成目標

【中間目標】 2025 年度まで

〔1〕 アーティファクト分析技術

- マルウェアの機能的特徴抽出・分類システムの要件を確定する。
- マルウェアの暗号化アルゴリズムや設計上のバグを同定するための技術及び手法を確立する。
- 暗号化されたデータの復号ツールの開発に向けた技術及び手法を確立する。

〔2〕 攻撃者からより多くの情報を獲得するための技術

- 被害環境を欺瞞環境に転化させる防御システムの要件を確定する。
- ホスト上に存在する攻撃者にとって価値のある情報等を無害化するシステムの要件を確定する。
- 蓄積した攻撃情報等の分析システムの要件を確定する。

〔3〕 高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

- 既存のマルウェア検知技術に対する回避技術や、攻撃の秘匿化技術等の攻撃技術について体系的に整理する。
- 検知、分析及び対処を行うに当たり必要な情報を収集する仕組み（センサー等）の要件を確定する。

・ スレットハンティング、動的ポリシー制御等の検知ロジックの要件を確定する。
・ 各種攻撃対処を一元的に対応することが可能な仕組み（セキュリティポリシーの策定等）の要件を確定する。
・ 大量のデータを収集・分析する情報収集・分析基盤システムの要件を確定する。

【最終目標】 2028 年度まで

〔1〕 アーティファクト分析技術

・ マルウェアの機能的特徴抽出・分類システムの社会実装に向け、仕様を確定し、機能実証を行う。
・ マルウェアの暗号化アルゴリズムや設計上のバグの同定手法の社会実装に向け、仕様を確定し、機能実証を行う。
・ 暗号化されたデータの復号ツールの社会実装に向け、仕様を確定し、機能実証を行う。
・ 攻撃の兆候察知時におけるリアルタイムな攻撃の検知・特定に繋がる、攻撃者の特定のための情報収集技術の社会実装に向け、仕様を確定し、機能実証を行う。
・ IoT 機器向けファームウェアを自動的に収集・管理する基盤システムの仕様を確定し、社会実装に向けた大規模運用による機能実証を行う。
・ ファームウェアに含まれるファイルシステム・バイナリ等からソフトウェア構成・依存関係を抽出する静的解析フローの仕様を確定し、社会実装に向けた脆弱性・コンポーネント等の検出性能の機能実証を行う。
・ 仮想環境上でファームウェアをエミュレーションし、実行挙動を取得・記録する動的解析フローの仕様を確定し、社会実装に向けたサービス露出等のリスク検出の機能実証を行う。
・ ファームウェアの静的解析及び動的解析の結果を統合し、機器間の類似性・共通コンポーネント・リスク伝搬構造等を可視化する評価システムの仕様を確定し、社会実装に向けた機能実証を行う。

〔2〕 攻撃者からより多くの情報を獲得するための技術

- 被害環境を欺瞞環境に転化させる防御システムの仕様を確定し、社会実装に向けた機能実証を行う。
- ホスト上に存在する攻撃者にとって機微な価値のある情報等を無害化するシステムの仕様を確定し、社会実装に向けた機能実証を行う。
- 蓄積情報の分析システムを開発し、社会実装に向けた機能実証を行う。

〔3〕 高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

- 検知、分析及び対処を行うに当たり必要な情報を収集する仕組み（センサー等）の仕様を確定し、社会実装に向けた機能実証を行う。
- スレットハンティング、動的ポリシー制御等の検知ロジックの仕様を確定し、社会実装に向けた機能実証を行う。
- 各種攻撃対処を一元的に対応することが可能な仕組み（セキュリティポリシーの策定等）の仕様を確定し、社会実装に向け、当該仕組みが攻撃に対して機能するかなどの機能実証を行う。
- 大量のデータを収集・分析する情報収集・分析基盤システムの仕様を確定し、社会実装に向けた機能実証を行う。

エ．その他

サイバーセキュリティに係る技術進展が急速に変化していることを考慮し、国内外の技術開発動向や各国のサイバーセキュリティ技術の導入状況等について情報収集・調査研究を並行して実施する。その結果は、必要に応じ、各研究開発課題の見直し等に活用する。

研究開発項目② サイバー攻撃から機器やシステムを守る防御力の向上

ア．研究開発の必要性

昨今では国家を背景とする攻撃主体の台頭が見られ、このような攻撃主体は、先進技術などを率先して攻撃に転用する傾向がある。このような背景のもと、将来において注視すべき技術分野として、AI、脆弱性探査技術、量子計算機が挙げられる。

AIについては、例えば、自律的・効率的な攻撃にAIが悪用されることが想定される。人間による攻撃からAIによる攻撃への移行、C2サーバーとの通信を行わないAIを用いた自律制御による攻撃が想定される。

脆弱性探査技術については、例えば、ファジング等の脆弱性探査技術の発展や、ゼロデイ脆弱性発見効率の向上、これらを背景とする攻撃の高度化等が想定される。

量子計算機については、計算力の向上による既存暗号の危殆化が想定される。

これらはいずれも既存の攻撃の在り方が変容する可能性を秘めているが、根本的かつ実用的な対処方法は存在していない。このため、AI、脆弱性探査技術、量子計算機の3つの観点において技術の向上に伴うサイバー攻撃手法の変化を検証し、サイバー攻撃から機器やシステムを守る防御力向上のための技術的能力を獲得する必要がある。

また、近年においては従来の防御の取組に加え、能動的サイバー防御を始めとした攻撃者側に対抗する措置を組み合わせ、サイバー脅威を防止・抑止するために必要な技術の必要性が一層増大しているところ、マルウェアの機能停止や攻撃者の正確な情報の特定・評価を通じた防御力向上のための技術的能力を獲得する必要もある。

くわえて、防御能力向上を図る中で利用することになる攻撃者情報や攻撃者が利用するインフラ、あるいは攻撃者の攻撃パターンや特徴などの各種攻撃情報の正確性は効果的な防御を行う上で重要であるところ、その担保を行うための技術的能力を獲得することも必要である。

イ．具体的研究内容

具体的な要素技術については、主に以下のとおり。

〔1〕 AIを活用した脆弱性探査技術

① 効率的な脆弱性探査を行うための技術

ファジング等の脆弱性探査技術を用いるに当たって、有限の計算リソースを効率的に運用するための技術やデバイスに存在する脆弱性の早期発見・修正するための技術。

② ネットワーク上の対象に対する脆弱性探査からの防御技術

AIを利用した脆弱性評価の学習を速やかに実施すること等により、ネットワーク経由で行われる脆弱性探査を検知し防御するための技術及び手法。

③ 攻撃兆候の察知時に、リアルタイムで既に侵入しているマルウェアを機能停止させる技術。

④ 攻撃元等の情報に関して、客観的な指標に基づいてその正確性を評価し、情報の品質を担保する技術。

〔2〕 AI 等を活用した防御能力の評価・向上技術

① ペネトレーションテストの自動化技術

ペネトレーションテストを自動化するために必要な技術。

※自動化に当たっては、適切な攻撃手法をシステムが自動的に選択する必要がある。

ペネトレーションテストにおける各段階における攻撃手段について、「攻撃の成功確率」「攻撃の発覚リスク」「得られる効果」などを基に数値化し、プロトタイプ実証などを基に、自動的に適切な攻撃手段を選択する技術。

② 攻撃に資する露出情報の秘匿・欺瞞技術

攻撃者が攻撃を成功させるために必要な情報を特定し、秘匿・欺瞞する技術。

③ リスクの可視化・リスクレベルの判定技術

攻撃者が最も大きく効果を得られる対象が最もリスクが高いため、これを可視化し、侵入の容易性や獲得可能であった情報の重要度等に応じたリスクレベルを判定する技術。

※攻撃者が容易に侵入できるほど、あるいは獲得可能であった情報の有用性が高いほど、リスクレベルが高いと考えられるので、これを可視化する。具体的には、公開情報（SNS 等）分析や自律的 AI による攻撃主体分析が挙げられる。

〔3〕 AI を活用した OT ペネトレーションフレームワーク技術

OT システムは多種多様なハードウェアやプロトコルで構成されており、IT のペネトレーションツールが使えない場合が多い。また、現状のペネトレーションは専門家のノウハウにより製品やシステムの差異を吸収しており、全製品やシステムをペネトレーションすることは困難といった課題がある。このため、我が国の基幹インフラ及びその重要構成要素について、構築段階でペネトレーションテストを漏れなく実施することにより脆弱性を事前に発見・修正する体制を確立する。

① テスト実施のため仕様開発

テスト実施のために製品提供側で用意すべきデジタルツインや動作仕様(形式記述) 及び具備するインタフェースの要件。

② インタフェース要件の開発

テストを実施する AI を Pluggable に追加・選択できる、ペネトレーションテスターのインタフェースの要件。

③ テスト手法の開発

ペネトレーションテストの十分性を評価するための手法。

④ レポート様式の整備

対処を実施するために必要な人や機械の可読性が高い結果レポートの様式。

⑤ AI 技術

OT 固有の特徴を踏まえたペネトレーションを自動化する AI 技術。

〔4〕 耐量子計算機暗号技術

① 耐量子計算機暗号実装技術

IoT の進展を支える末端機器のセキュリティ強化には、その信頼の基点たる暗号モジュールが必須である。現行の非耐量子計算機暗号の公開鍵暗号（楕円曲線暗号など）においては、ハードウェア実装された暗号エンジンにそれへのアクセス制御機能を結合した SCU（セキュア暗号ユニット：SIP 第 1 期で開発し、SIP 第 2 期でそれを内蔵したマイクロコントローラ半導体チップを試作）などの技術がある。また、高速性（低レイテンシ、高スループット）が要求されるサーバー（クラウド）に向けの非耐量子計算機暗号のハードウェア実装技術とソフトウェアからのハードウェアの効率的な利用技術も確立されている。

前者はハードウェア実装による小型化・省エネルギー性の追求であり、後者はハードウェア実装とソフトウェア技術による省エネルギー性を考慮した超高速性の追求である。

耐量子計算機暗号の公開鍵暗号においてもこれらが必要であるため、

1) ハードウェア実装による極小面積・省エネルギー性の追求に基づく末端デバイスへの耐量子計算機暗号実装技術の確立

2) ハードウェア実装とソフトウェア技術による省エネルギー性を考慮した超高速性の追求に基づくサーバー向け耐量子計算機暗号実装技術の確立

を実施する。また、社会実装を見据えては、実装面での性能向上も必要であることから、耐量子計算機暗号において、リング署名、しきい値署名、しきい値暗号などの高機能性の獲得に向けた研究開発も実施する。

〔5〕 耐タンパー性向上技術

① 耐タンパープロセッサ/FPGA 構築技術

電子回路のサイドチャネル攻撃耐性やフォールト注入攻撃耐性を高め、全体としての耐タンパー性が極めて高いマイクロプロセッサ／マイクロコントローラ、あるいは、FPGA（フィールドプログラマブルゲートアレイ）を構成する技術を開発する。

② フォールト脆弱性検出技術

サイバー攻撃と協調した新種のフォールト攻撃の脅威が高まっている。このようなフォールト攻撃に関連した脆弱性検出手法が提案されているが十分なレベルに達していない。このため、既存手法の定量的評価を行い、新たな脆弱性検出手法を開発する。

③ ロジックロッキング（IP 保護技術）

ハードウェアの知的財産（IP）侵害、リバースエンジニアリングの脅威に対し、正しい鍵が入力された場合にのみ論理回路が正常動作するロジックロッキングという対策手法が注目されている。ロジックロッキングの評価手法及び強固な対策手法を開発する。

④ チップレット対応耐タンパー技術

専用の半導体チップ（チップレット）を組合せて実装するチップレット実装が多用される傾向にある。このようなチップレット実装に適した経済的な耐タンパー技術を開発する。

⑤ 脆弱性探査の阻害技術

ソフトウェアに対するアンチファジング技術を含む耐タンパー性を獲得するための技術を開発する。

ウ．達成目標

【中間目標】 2025 年度まで

〔1〕 AI を活用した脆弱性探査技術

・ 脆弱性探査を効率的に行うためのシステムの仕様を策定する。
・ ネットワークを介した脆弱性探査からの防御のための AI による学習環境の要件を策定する。

〔2〕 AI 等を活用した防御能力の評価・向上技術

・ 攻撃手法の選定に関する各種要素の検討と算定方法を確立する。
・ 対象組織などのリスク可視化の基礎技術を確立する。
・ リスクレベルの判定に関わる基礎技術を確立する。
・ Cyber Attack Kill Chain 各段階で必要となる情報の AI 技術による統計的評価を実施する。

〔3〕 AI を活用した OT ペネトレーションテスト技術

・ AI を活用した OT 等の設備向けペネトレーションテスト技術のプロトタイプを作成する。

〔4〕 耐量子計算機暗号技術

・ 耐量子計算機暗号を実装させる機器への実装設計や面積が極小化されたチップの試作、性能評価を行うことにより、耐量子計算機暗号の実装技術や高機能性獲得の基礎技術を確立する。

〔5〕 耐タンパー性向上技術

・ 耐タンパー強度と経済性をそれぞれ追及した耐タンパー性の基礎技術を確立する。
・ ソフトウェアに対するアンチファジング技術を含む耐タンパー性を付与するツールの要件を確立する。
・ 関係機関の協力を得つつ耐タンパー性向上技術の実装を円滑化・促進するための指針やガイドライン案を作成する。

【最終目標】 2028 年度まで

〔1〕 AI 等を活用した脆弱性探査技術

・ 探査対象における脆弱性種別ごとの影響度を可視化するシステムについて、社会実装に向けた機能実証を行う。

・　ネットワークを介した脆弱性探査からの防御について、社会実装に向けた機能実証を行う。
・　マルウェア自身の機能あるいは、ネットワーク技術を活用すること等により環境内のマルウェアを被害なく効果的に無力化するための技術を確立し、社会実装に向けた機能実証を行う。
・　環境内に侵入しているマルウェアに対し有効な機能停止手法を体系的に整理し、方法論として確立し、実検体を利用した評価を元に、社会実装に向けた実証を行う。
・　攻撃元等の情報について、客観的事実に基づき正確性を評価する指標を確立し、実運用を模した運用評価を通してその実用性を評価し、社会実装に向けた実証を行う。

〔2〕 AI 等を活用した防御能力の評価・向上技術
・　AI を活用しペネトレーションテストを自動的かつ効率的に行うための仕様を確立し、社会実装に向けた機能実証を行う。
・　リスクレベルの自動判定システムの仕様を確立し、社会実装に向けた機能実証を行う。
・　情報の秘匿・偽装による欺瞞防御システムの仕様を確定する。

〔3〕 AI を活用した OT ペネトレーションテスト技術
・　AI を活用した OT 等の設備向けペネトレーションテスト技術について、社会実装に向けた機能実証を行う。

〔4〕 耐量子計算機暗号技術
・　耐量子計算機暗号を実装させる機器への実装設計や面積が極小化されたチップの試作、性能評価を行うことにより得られた耐量子計算機暗号の実装や高機能性獲得の基礎技術を活用し、クラウドや末端デバイスおける耐量子計算機暗号の機能実証を行うなど、社会実装に向けた実証を行う。

〔5〕 耐タンパー性向上技術
・　耐タンパー強度と経済性について、機器ごとに最適な耐タンパー技術を確立し、社会実装に向けた機能実証を行う。

・　ソフトウェアに対するアンチファジング技術を含む耐タンパー性を付与するツールの仕様を確立し、社会実装に向けた機能実証を行う。
・　耐タンパー性向上技術の実装を円滑化・促進するための指針やガイドラインについて、関係機関に提示する。

エ．その他

サイバーセキュリティに係る技術進展が急速に変化していることを考慮し、国内外の技術開発動向や各国のサイバーセキュリティ技術の導入状況等について情報収集・調査研究を並行して実施する。その結果は、必要に応じ、各研究開発課題の見直し等に活用されることとする。

研究開発項目③ 共通基盤の整備

ア．　研究開発の必要性

被害情報や OSINT 等により得られた情報から、有用な情報を抽出するために必要な集約・分析方法の在り方や、効果的な連携方法、フォーマットを研究し、各種攻撃・攻撃者の分析・分類結果を統一的に集約・管理・共有する手法を確立する必要がある。

また、情報収集・偵察能力、無力化、痕跡・ログの証拠能力、検知されない能力の評価、及びそれに対抗するための対応・防御力、組織力の評価など、様々な側面から高度サイバー人材を評価・管理できる仕組みを開発する必要がある。

さらに、AI 等の技術進歩による攻撃手法の多様化、検知困難化の情勢を鑑み、攻撃の兆候を早期に発見して迅速に対処する技術の演習が可能な設備が国内に必要。また経済安全保障の観点から海外に依存せず攻撃手法への対処やセキュリティ業務の支援・効率化を行える国産生成 AI モデル等を活用した海外製品、海外情報源に依存しない国産情報共有基盤の整備が必要。

イ．　具体的研究内容

具体的な要素技術については、主に以下のとおり。

〔1〕　情報の効果的な連携に関わる技術

①　サイバー脅威情報集約、連携の様式等

サイバー脅威情報を集約しデータ連携するために必要となる、様式の整備等の技術。

② マルウェア設計実装情報の連携分析技術
マルウェアの設計や実装等に関するサイバー脅威情報の収集、集約のための技術。

〔2〕 高度サイバー人材の評価・管理に関する技術
① 評価技術
高度ペネトレーションテストやその防御に関わる能力の評価技術とこれらを支援するための技術。
② 管理技術
高度サイバー人材の管理のための技術。
③ 高度サイバー安全保障人材育成のための研究開発等
高度サイバー安全保障人材の育成に資する研究開発及びツールの開発。

〔3〕 経済安全保障の観点で他国技術に依存しないセキュリティ技術
① 国産セキュリティ基盤のための技術
国産生成 AI モデル等を活用した国産セキュリティ情報共有基盤の技術。

ウ. 達成目標
【中間目標】 2025 年度まで
〔1〕 情報の効果的な連携に関わる技術
・ サイバー情報集約、連携の様式等を整備する。
・ マルウェア設計実装情報の連携のための技術を確立する。

〔2〕 高度サイバー人材の評価・管理に関する技術
・ 高度サイバー人材の評価・管理手法の要件及び仕様を確立する。
・ 高度サイバー人材の評価・管理のための支援ツールの要件を確立する。

【最終目標】 2028 年度まで
〔1〕 情報の効果的な連携に関わる技術
・ 解析業務ツール・プラグイン等の開発を行い、社会実装に向けた機能実証を行う。

・　サイバー情報集約、連携の様式やマルウェア設計実装情報の連携技術を活用し、社会実装に向けた機能実証を行う。

〔2〕 高度サイバー人材の評価・管理に関する技術

・　高度サイバー人材の評価・管理手法の社会実装に向けた機能実証を行うとともに、具体的な社会実装の仕組みを構築する。
・　高度サイバー人材の評価・管理のための支援ツールの仕様を確立し、社会実装に向けた機能実証を行う。
・　高度サイバー安全保障人材の育成に資する研究開発を実施し、ツールを開発する。

〔3〕 経済安全保障の観点で他国技術に依存しないセキュリティ技術

・　経済安全保障の観点から他国技術に依存しないセキュリティ特化型の国産生成 AI モデル等を整備し、社会実装する。

エ．その他

サイバーセキュリティに係る技術進展が急速に変化していることを考慮し、国内外の技術開発動向や各国のサイバーセキュリティ技術の導入状況等について情報収集・調査研究を並行して実施する。その結果は、必要に応じ、各研究開発課題の見直し等に活用する。

研究開発項目④ セキュアな量子情報通信技術の開発

ア．研究開発の必要性

我が国が目指す Society 5.0 の発展とともに、様々な産業や社会活動において、情報通信で扱う情報は増大し、かつ非常に重要で機密性の高いものへと変化している。これらは、高速・大容量、低遅延を要求され、更にデータセンタ間の接続から IoT に至るまで、広範にセキュリティも要求されており、その対策が急務となっている。国内における量子技術分野の研究開発では、暗号鍵を配送する QKD（Quantum Key Distribution）の研究は進められているが、物理レイヤでのデータ伝送に対する盗聴などへの対策は、AES（Advanced Encryption Standard）などの上位レイヤでの既存暗号の計算量的安全性に頼ることに留まっている。

QNSC の Y-00 プロトコルは、物理的な観測の複雑性（物理測定量的安全性）を量子雑音で実現しており、物理レイヤでの信号変調と同時に暗号化するため高速・低遅延であり、安全性が計算機の能力に影響されないため耐量子計算の安全性を実現でき、現在光ファイバ通信を基盤として研究開発が進んでいる。また、本プロトコルは、様々な変調方式に対応可能と考えられており、高速・大容量伝送を実現するための、伝送効率の高い変調方式の適用や光ワイヤレス通信への適用も期待できる。

本研究では、Society5.0 に向けた通信ネットワークの物理層における情報セキュリティの社会実装を目的とし、高速・大容量・低遅延な光ファイバ伝送と光ワイヤレス通信に確固たるセキュリティの付加を目指すべく、QNSC 方式の研究開発を実施する。

イ．具体的研究内容

具体的な要素技術については、主に以下のとおり。

〔1〕 Y-00 のデジタルコヒーレントの開発

QNSC（Y-00 プロトコル）では、基本となる変調方式を多値化しデータを埋め込む処理を行うため、一般的なデジタルコヒーレント技術とは異なることから、専用のデジタルコヒーレント方式を新たに開発する。

① デジタル変復調技術の開発

変調方式の候補として、大学等の基礎研究により QNSC の有効性が検討されている、ASK（振幅変調）、PSK（位相変調）、QAM（直交振幅変調）の 3 つの変調方式についてデジタルコヒーレント技術の適用を机上検討し、特に本事業では、基本である ASK をベースに高速伝送への適応性を重視して PSK、QAM の実用化を中心に試作開発を進める。

② リアルタイム処理の開発

デジタルコヒーレントの処理においては、QNSC の暗号化、復号化を含む光変復調の処理時間を μsec オーダー以下で開発し、低遅延のリアルタイム伝送を実現する。

③ デジタル歪補正の開発

変復調とともに、高速・大容量伝送において新たに必要な機能として、様々な環境変化に伴い変化する信号波形や検波条件を、高速伝送に必要な精度で自動的にチューニングすることのできる QNSC（Y-00 プロトコル）専用のデジタル信号処理（DSP）を開発する。

④ 論理検証機(FPGA)の作成

上記機能を備えたFPGAベースの論理検証機を試作し、各種性能評価を実施する。

〔2〕 Y-00の高速光ファイバ通信の開発

高速なFPGAベースの専用DSPの開発を行う。目標の20Gbps以上の高速・大容量を実現するため、伝送品質補償に高速で精度の高い制御を行う必要がある。DSPは、高品質伝送のみならずY-00プロトコルも実現する必要があるため、Y-00専用の構成になる。また、高速動作のためには、高精度のタイミング同期方式を新たに開発する必要がある。リアルタイム制御を実現するためにはY-00プロトコルの最適化と共に新たな制御方式、及びそれを実現するための回路の開発が必要となる。また、セキュリティシステム運用を考慮し、無線等の通信で利用されている方式の応用検討を行い、光ファイバ伝送や次のステップで行う光ワイヤレス伝送を実現するための要素技術開発を行う。

① 光デバイス構成の開発

光学系デバイス部品を中心に、高速動作を実現するため、実装における性能劣化やデバイス特性に制限を与えない小型モジュール化を実施し、試作機に導入する。

② セキュア管理システムの開発

QNSCを既存の通信システムに導入する場合、安全性を確保した初期共通鍵の運用や鍵交換、ネットワーク制御等の通信システムとしてのシステム開発も必要であり、既存の通信インフラを可能な限り利用し、耐量子コンピュータ性能を備えたシステム構成を開発する。

③ 光ファイバ伝送 20Gbps試作機の開発

ステップ1での成果を踏まえ、上記のような開発を行い目標の単一波長20Gbps伝送が可能なQNSC（Y-00プロトコル）の機能を備えた試作機を開発する。この試作機を使用し、既存の光ファイバ回線を利用した伝送実験を行い、その有効性と実用化への課題を抽出する。

〔3〕 Y-00の高速光ワイヤレス通信の開発

QNSC（Y-00プロトコル）を適用した光ワイヤレス伝送を実現するための光アンテナを開発する。光ワイヤレス伝送においては光ファイバ伝送とは異なり、送受信機間の光軸を最適に自動調整する必要があるため、高速で高精度な光軸自動調整システムの開発が必須となる。

① 光ワイヤレス通信専用の DSP の開発
ワイヤレス環境下に対応する新たな DSP をステップ１、２で開発した DSP を改良し開発する。

② 光アンテナとの結合を想定した専用光モジュール開発
光ワイヤレス伝送では、送受機信間で光学系（レンズ等の光学部品等）を備えたインタフェースを開発する。

③ 光ワイヤレス伝送に適したセキュア管理システムの開発
伝送空間の環境変化等で見通しが悪くなるとリンクの切断や受信感度の劣化が起こるため、それらを想定した QNSC（Y-00 プロトコル）のリンクプロトコルが必要となる。これらは耐量子コンピュータ性能を備えた新たなシステムを開発する。

④ 光空間伝送 QNSC 試作機の開発
本ステップでは、光アンテナを備えた光ワイヤレス伝送用の試作機を開発し、光ワイヤレス伝送における実機検証を行う。

ウ．達成目標

〔1〕 Y-00 のデジタルコヒーレントの開発

大容量通信で利用できる、QNSC 専用のデジタルコヒーレント方式の実現性の見通しを得る。

伝送速度：1Gbps 以上で実現し 10Gbps 以上での適用性に見通しをつける

変調方式：ASK、PSK、QAM

伝送距離：50km 以上（光ファイバ無中継伝送）

DSP：ハードウェア処理が可能な DSP 方式の開発

〔2〕 Y-00 の高速光ファイバ通信の開発

QNSC 専用のデジタルコヒーレント方式を用いた目標の単一波長 20Gbps 以上の高速な光ファイバ伝送を実現する。

伝送速度：単一波長 10Gbps（目標 20Gbps）以上

変調方式： PSK、QAM

遅延時間：1msec 以下

伝送距離：50km 以上（無中継伝送）、500km 以上（光増幅器中継）

DSP：ハードウェア処理化が可能なリアルタイム DSP 方式の開発
（DSP 方式は FPGA により実現）

〔3〕 Y-00 の高速光ワイヤレス通信の開発

目標の 20Gbps 以上の光空間通信を実現し、QNSC（Y-00）による光ファイバ通信/光空間通信それぞれを試験できる試験機を実現。光ファイバ通信では既存の空き光ファイバ回線、光空間通信では大学や会社施設内の空きスペースでの試験を行う。

2. 実施方法、実施期間、評価、社会実装に向けた取組

（1）事業の実施・体制

本事業は、内閣官房及び内閣府が定める「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき事業を実施する。

研究推進法人（Funding Agency: FA）は、国から示された研究開発ビジョン及び研究開発構想に基づき、公募により研究開発課題を採択するとともに、その進捗管理・評価等の責務を担う。本事業の FA は、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）である。

研究開発課題の実施責任者（以下「研究代表者」という。）の所属する機関は、国内に研究開発拠点を有し、我が国の法律に基づく法人格を有している機関とする（以下「研究代表機関」という）。また、研究代表者及び主たる研究分担者は我が国の居住者であることとする。（ここでいう居住者とは外為法の居住者（特定類型該当者を除く）であること。）

本事業の公募では、個別事業ごとの提案を想定しており、研究開発項目①～③及び④はそれぞれ別に事業を実施するものとする。

（2）事業の実施期間

本研究開発構想に基づく本事業は、研究開発項目①②③について 2024 年度から 2029 年度にかけての 5 年間とし、研究開発項目④について 2024 年度から 2027 年度にかけての 3 年間とする。研究開発はステージゲート方式を採用し、図 1 に示すスケジュールで実施するものとする。

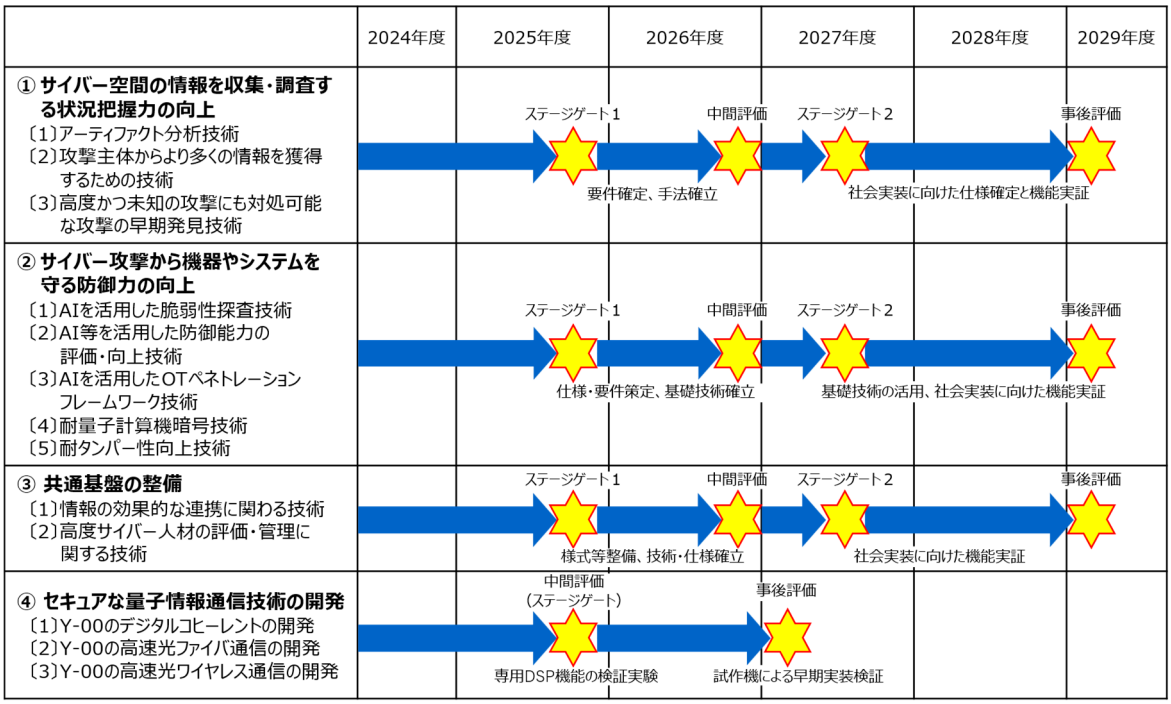

図 1　研究開発のスケジュール

（3）評価に関する事項

本事業は、「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき、評価を実施する。

研究代表者は自己評価を毎年実施し、PD に報告する。NEDO は外部評価として、研究開発項目①②③について、評価の時期は中間評価を 2026 年度（事業開始から 3 年目）、事後評価を 2029 年度（事業終了年）に実施することとし、事業の進捗等に応じて評価時期を早める場合は、PD 及び所管省庁と連携して、あらかじめ適切な実施時期を定める。

研究開発項目④について、評価の時期は中間評価を 2025 年度（事業開始から 2 年目）、事後評価を 2027 年度（事業終了年）に実施することとし、事業の進捗等に応じて評価時期を早める場合は、PD 及び所管省庁と連携して、あらかじめ適切な実施時期を定める。

（4）社会実装に向けた取組

本事業は、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 4 3 号）に基づく指定基金協議会を設置した上で推進していく。これにより、本事業によって生み出される研究成果等を活用し、民生及び公的な利用を促進するとともに社会実装につなげ、国際連携を進めていくことを目指し、その実現に向け、潜在的な社会実装の担い手として想定される関係行

政機関や民間企業等による伴走支援を可能とするとともに、参加者間で機微な情報も含む有用な情報の交換や協議を安心かつ円滑に行うことのできるパートナーシップを確立していく。

本事業により開発を行う先進的なサイバー防御能力や分析能力は、次々に新たな攻撃技術が生まれる中において、我が国のサイバーセキュリティの確保に貢献し、経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現に資することが想定される。このため、サイバーセキュリティの確保を行う場合の将来的に想定される具体的なユースケースやビジネスモデル、その実現のために必要な制度・標準・機能等や普及の在り方、求められるセキュリティの強度、世界の市場動向等の情報を共有しつつ研究開発を進めることは、研究開発成果を将来の社会実装に円滑につなげていく上で、大きな意義がある。また、国際連携についてサイバーセキュリティ関連の国際会議・団体との意見交換等を行っていく。

本事業に係る協議会については、研究開発課題の採択後に、関係行政機関、PD、研究代表者等の協議会への参画者における十分な相談を行いつつ、運営していく。なお、協議会の詳細は別に示す。

（５）総予算

本事業の予算は、研究開発項目①②③については 376 億円を超えない範囲、研究開発項目④については 30 億円を超えない範囲とする。各研究開発項目、フェーズ毎の配分については、必要に応じて、経済産業省からの指導に基づき目安を示す。これを変更する場合も同様とする。

（６）経済産業省の担当課室

本事業の運営に係る経済産業省の担当課室は、研究開発項目①②③を商務情報政策局サイバーセキュリティ課とし、研究開発項目④を製造産業局航空機武器宇宙産業課とする。また、研究開発構想全体の取りまとめなどを行う主担当原課は、商務情報政策局サイバーセキュリティ課とする。

3. その他重要事項

（１）研究開発成果の取扱い

① 共通基盤技術の形成に資する成果の普及

研究開発課題実施者は、研究成果を広範に普及するよう努めるものとする。経済産業省及び NEDO は、経済安全保障の観点を留意しつつ、研究開発課題実施者による研究成果の広範な普及を促進する。

経済安全保障の観点から、経済産業省は必要に応じて NEDO に対して助言を行い、NEDO は本助言を踏まえて、成果の普及について検討することとする。

② 標準化施策等との連携

研究開発実施者は、安全性検証手法等に関する研究開発成果の着実な実用化のため、本研究開発の終了後に実施すべき取組の在り方や検証・認証機関の構築及びビジネスモデルについて立案する。また、経済産業省、NEDO 及び研究開発課題実施者は、安全性基準等の国際標準化を戦略的に推進する仕組みを構築する。

③ 知的財産権の帰属、管理等の取扱い

研究開発成果を民生利用のみならず公的利用につなげていくことを指向し、社会実装や市場の誘導につなげていく視点を重視するという本プログラムの趣旨にのっとり、研究代表機関、研究代表者は、PD 及び研究分担者との協議の上、知的財産権の利活用方針を定めることとする。その際には、研究開発途中及び終了後を含め、知的財産権の利活用を円滑に進めることができるように努めることとする。

なお、研究開発成果の利活用に当たりその成果にバックグラウンド知的財産権が含まれる場合には、その利活用についても同様に努めること。

（２）「研究開発構想」の見直し

経済産業省は、NEDO、PD 及び関連省庁と連携して、当該研究開発の進捗状況及びその評価結果、社会・経済的状況、国内外の研究開発動向、政策動向、研究開発費の確保状況等、事業内外の情勢変化を総合的に勘案し、必要に応じて、達成目標、実施期間等、本研究開発構想の見直しを行う。

（３）研究開発の対象経費

「経済安全保障重要技術育成プログラムの運用・評価指針」に基づき、運用する。大学・研究開発法人等以外に関する間接経費の額の設定については、事業の性質に応じて経済産業省の担当課室から別に示す場合を除き、業務委託契約標準契約書に基づくものとする。

4. 研究開発構想の改定履歴

（１）令和５年 10 月、制定。
（２）令和８年４月、改定