参考資料4

AI・量子の研究開発に係る政策動向

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）

ＡＩ戦略2019 ～人・産業・地域・政府全てにＡＩ～【抜粋】

令和元年(2019年)6月11日
統合イノベーション戦略推進会議

Ⅲ．産業・社会の基盤作り

Ⅲ－２．データ関連基盤整備

（２）トラスト・セキュリティ

＜具体目標2＞
年々複雑化・巧妙化するサイバー攻撃に対し、「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を確立

（取組）

○AIを活用したサイバー対策を行う民間を後押しするための仕組み、国の研究成果の実用化・技術移転に関する支援策を整備（2019年度）
【経】

○国として加速化して重点的に取り組むべき研究開発を明確化し、（別表2）を参考に、以下の技術を実現するための工程表を作成（2019年度）
【NISC・CSTI・総・経】
予防のためのAI：ハードウェアの動作特性把握による不正機能検出等
検知のためのAI：大量パケット情報解析による攻撃手法検知等
対処のためのAI：緊急対応が必要なアラートの自動抽出等

○5年～10年先に実現を目指す長期的取組（サイバーセキュリティ確保のためのAIそのものを守る技術等）についての検討（2019年度）
【NISC・CSTI・総・経】

【※AIに関する脚注】

AI（artificial intelligence）については、例えばECハイレベルエキスパートグループ報告書においては、「環境や入力に対応して知的な動作（一定の自律性を有することもある）を行うシステム」とされているが、「知的な動作」の実体は解釈に依存する側面もある。また、2016年に米国で発表されたAI100報告書では、学問分野としてのAIを、「知能を持った機械を作る研究であり、知能とは置かれた環境中で適切に、かつ何らかの洞察を持って機能すること」というNils J. Nilssonの定義を引用しているが、この定義も大きな曖昧性を持ったものである。実際、同報告書では、AIの定義が曖昧であること自体が、AIの研究を加速している肯定的な側面があるともしている。これらの状況を鑑みると、何を以て「AI」または「AI技術」と判断するかに関して、一定のコンセンサスはあるものの、それをそこに利用される技術などを基盤にことさらに厳密に定義することは意味があるとは言えない。同時に、このようなシステムは、高度に複雑なシステムに組み込まれることも留意する必要がある。さらに、大規模データを収集・蓄積し、アクセスする基盤、超高速通信網、センサー群、ロボットなどがなければAIシステムの実装はおぼつかない。サイバーセキュリティやAI倫理など、このようなシステムの安全性や健全性を担保する技術の開発や実装が行われなければ、AIが広く受容されることも困難となる。AIは、知的とされる機能を実現する広範なシステムを包含するとともに、今後の社会や産業から日常生活、また、科学研究や技術開発まで、あらゆる領域に展開されることが予想される。よって、本戦略の対象は、これらの領域も統合的に構想する必要がある。

ＡＩ戦略2019 ～人・産業・地域・政府全てにＡＩ～【抜粋】

令和元年(2019年)6月11日
統合イノベーション戦略推進会議

（別表 2）サイバーセキュリティ対策のための AI 応用開発・実証

今後の研究開発・実証重点項目	個別項目	達成時期	担当
予防のための AI	知識ベースを用いた自動的な脆弱性診断	2022 年度	(民間が主導)
	対象システムに関する新たに登録された脆弱性情報の深刻度の自動評価	2022 年度	【経】
	ファジング技術等に基づく単体のハードウェアの動作特性の把握による不正機能検出	2022 年度	【総・経】
	機器やソフトウェアに、不正なプログラムや回路が仕込まれていないことの技術的検証を行うための体制整備	2022 年度	【NISC・CSTI・総・経】
検知のための AI	検知ロジックおける AI 活用により未知/新種のマルウェアの自動検出	2022 年度	(民間が主導)
	大量なマルウェア情報を用いた自動解析による、マルウェア機能体系の自動分類	2022 年度	(民間が主導)
	攻撃と推定される超大量のパケット情報に対して AI 技術を活用して攻撃手法や攻撃傾向自動把握・検知	2022 年度	【総】
対処のための AI	AI によるフォレンジック解析支援	2022 年度	(民間が主導)
	セキュリティアラートの中から真に緊急対応が必要なアラートの自動抽出	2022 年度	【総・経】
	脅威インテリジェンス情報との関連付けの一部自動化	2022 年度	【経】

「ＡＩ戦略2019」フォローアップ【抜粋】

令和2年(2020年)6月26日
統合イノベーション戦略推進会議

Ⅲ．産業・社会の基盤作り

Ⅲ－2．データ関連基盤整備

（2）トラスト・セキュリティ

＜具体目標2＞
年々複雑化・巧妙化するサイバー攻撃に対し、「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を確立

（取組）

○【更新】2019年度に策定した評価項目や手引き等を踏まえ、AIを活用したサイバー対策を行う民間を後押しするための仕組み、国の研究成果の実用化・技術移転に関する支援策を整備（2020年度）【経】

○【新規】2019年度に作成した工程表に基づき、各省において研究開発・実証を推進（2022年度）【NISC・CSTI・総・経】

○【新規】５年～１０年先での実現を目指す、サイバーセキュリティ確保のためのAIそのものを守る技術等について、2019年度の検討結果を踏まえ、開発に着手するとともに、状況変化に応じた検討見直しや新たに取り組むべき事項を継続し検討（2020年度）【NISC・CSTI・総・経】

量子技術イノベーション戦略（最終報告）【抜粋】

令和2年(2020年)1月21日
統合イノベーション戦略推進会議

Ⅳ. 量子技術イノベーション実現に向けた5つの戦略

1. 技術開発戦略

（1）主要技術領域

ⅲ）量子通信・暗号

〇近年、計算技術やAI、医療技術等の発展により、機密性の高い重要なデジタル情報が次々に生み出されている状況にある。こうした重要情報が漏えいした場合、社会的・経済的な影響は甚大であることから、超長期にわたる機密性と完全性の確保は、極めて重要な課題である。

〇ゲート型量子コンピュータの急速な進展により、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。

〇我が国では、株式会社東芝やNECが世界最高速のBB84量子暗号装置を製造し、また情報通信研究機構（NICT）や東京大学、日本電信電話株式会社（NTT）、三菱電機株式会社等が、理論研究及び実証で世界を先導している。NICTが量子通信・暗号送受信装置の開発を進め、都市圏テストベッド「Tokyo QKD Network」で世界最長期間の運用実績を有するなど、世界をリードしている。東京大学は、量子コンピュータでも解読できない暗号アルゴリズム研究を推進している。衛星量子通信に関しては、中国が独自開発した衛星「墨子」を用いて地上との間での量子通信に成功したと発表し、世界を驚かせた。我が国では、NICTが低軌道衛星と地上局間での実証実験に成功した。

〇暗号送受信装置については、我が国の企業が早期の製品化・事業化に向けた取組を進めており、NICTとともに、欧州電気通信標準化機構（ETSI）や、国際電気通信連合（ITU）において標準化活動を推進しており、世界を先導している。

〇量子中継技術（量子メモリ・量子もつれ等）は、大阪大学やNTT、NICT等が冷却原子量子メモリと光子の間の量子もつれや、全光量子中継方式等の原理実証で世界を先導している。長距離伝送の実証や多重化・集積化・大規模化等が課題である。欧米や中国等で多数の研究開発プロジェクトが立ち上がるなど国際競争が激化している。

〇ネットワーク化技術（構築、運用、保守等）は、量子メモリ・量子中継が原理実証段階にあるため、現在のインターネットに代わる量子インターネットの実現には未だ時間を要する。このため、量子通信に係るトラステッドノードのアーキテクチャが検討されており、ITU-Tでは本アーキテクチャを前提とした標準化の議論が進んでいる。

〇我が国としても、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、国をあげて取り組むことが極めて重要である。

＜重点技術課題＞

・量子通信・暗号リンク技術

＜基礎基盤技術課題＞

・量子中継技術（量子メモリ・量子もつれ等）・ネットワーク化技術（構築、運用、保守等） 等

＜個別方針＞

・量子通信・暗号リンク技術のうち、光ファイバーを用いた量子通信は、送受信装置の基盤技術が確立し、我が国企業による実用化・事業化の段階にあるため、研究開発等に加えて、政府も関与する形で、短中期の国内外で事業展開を実現するための戦略的な取組を推進するとともに、産学官が密接に連携・協力し、国際標準化活動を推進。

・また、衛星量子通信に関しては、国及び国民の安全・安心や産業政策上の重要性に鑑み、短中期・中長期の両側面から、研究開発等を重点的に推進するとともに、通信環境整備など、実用化等に向けた戦略的な取組を展開。

量子技術イノベーション戦略（最終報告）【抜粋】

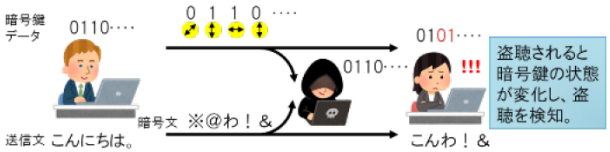
令和2年(2020年)1月21日
統合イノベーション戦略推進会議

主要技術領域③ 量子通信・暗号

○**量子暗号**により、**絶対に破られない暗号サービスが実現**されるため、**セキュリティの危殆化の懸念なく高秘匿情報をインターネット上でやり取りすることのできる社会が実現**される。

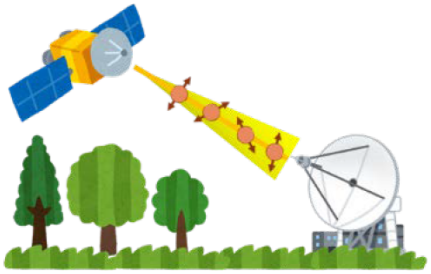
量子暗号|光ファイバー

- ✓ **暗号鍵データを光子に乗せ、光ファイバーで量子鍵を配送。**あらゆる**盗聴攻撃を検知**し、**情報理論的安全性が証明**されている唯一の暗号方式
- ✓ 日本の**強みは、高性能な量子暗号装置。**一方で、**低価格化やアプリケーションとの融合が課題**
- ✓ データ保存や秘匿計算を組合わせた**我が国独自のシステムを開発し、社会実装につなげる**ことが重要



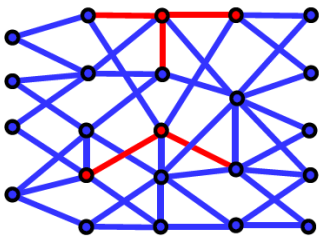
量子暗号|衛星通信

- ✓ **衛星間や衛星-地上局間で量子鍵配送を実施**し、**大陸間で高秘匿通信を可能**とする技術
- ✓ 日本でも、光通信分野では**世界最小となる超小型衛星を開発**し、予備実験を実施
- ✓ 本技術の実現に向け、**光子伝送の高速化、高精度レーザー捕捉追尾技術等の開発**を行うことが重要



量子通信

- ✓ **光子の重ね合わせや量子もつれ状態などの伝送・制御により、超高効率の通信を実現**する技術
- ✓ **ネットワークアーキテクチャや集積化**に向けた開発、超高効率通信に向けた**量子受信機の研究開発が課題**
- ✓ 超高効率通信以外にも、**量子情報を量子コンピュータへ伝送する手段などへの応用も期待**



量子中継

- ✓ 量子暗号は**光の損失により100km程度の通信距離が限界。**現在、物理的に盗聴者を侵入させない古典的手法で中継しており、**理論上安全な中継技術は未確立**
- ✓ 日本には、半導体技術やダイヤモンド結晶成長技術など、量子**中継デバイスの集積化の強みとなり得る技術がある。**
- ✓ 一方、実現には伝送速度、誤り訂正などの課題があり、**長期的視点から取り組む必要**がある。

量子技術イノベーション戦略（最終報告）【抜粋】

令和2年(2020年)1月21日
統合イノベーション戦略推進会議

（2）量子融合イノベーション領域

〇量子コンピュータ技術の進展に伴い、現在の公開鍵暗号技術等が解読される可能性が生じる中、国及び国民の安全・安心の確保の観点から、量子・古典技術を融合してネットワークセキュリティ高度化を図る「量子セキュリティ技術」は、極めて重要な技術領域である。欧米や中国が大規模な研究開発等を進める中、我が国も、先駆的な取組を進めており、これを確固たる基盤技術として発展させることが急務である。

＜量子融合イノベーション領域＞

・量子セキュリティ技術（例：量子セキュアクラウド、光・量子ネットワーク暗号化等）

＜全体方針＞

・量子融合イノベーション領域は、我が国が特に強み・競争力を保持し、かつ、可能な限り早期に高い確度で実用化・事業化等を実現することで、我が国の産業・イノベーションに大きな寄与・貢献が期待される技術領域を対象に設定。

・それぞれの量子融合イノベーション領域について、中長期の視野に立ち、国をあげて最重点を置いた研究開発等を推進するとともに、既存（古典）技術と組み合わせることで、短中期に、関連・周辺技術への波及・展開（スピンアウト）も含めた実用化・事業化等を実現するための戦略的な取組を展開。

＜具体的方策＞

・国は、関係府省等の連携・協力の下、量子融合イノベーション領域を対象として、関連技術・周辺技術も含む技術体系の全体像を俯瞰した上で、中長期的観点から今後20年程度の間に取り組むべき戦略的かつ具体的な方策を示した「融合領域ロードマップ」を作成し、本戦略と一体的に策定。

・国は、「融合領域ロードマップ」に基づき、各量子融合イノベーション領域を対象として、国直轄の大規模なプロジェクトや大型の研究開発ファンディング等を通じた重点的な研究開発支援等を行うとともに、これらを基に民間から積極的に投資を呼び込み、産学連携・官民協働による研究開発や実用化等に向けた幅広い取組を推進・展開。

量子技術イノベーション戦略（最終報告）【抜粋】

令和2年(2020年)1月21日
統合イノベーション戦略推進会議

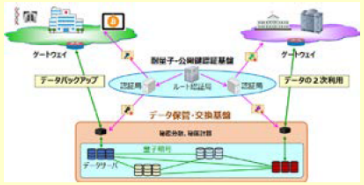
量子融合イノベーション領域③　量子セキュリティ技術のイメージ

○近年、量子コンピュータでも解読困難な**耐量子計算機暗号技術**や現在の公開鍵認証基盤からの移行技術に関する検討が活発化している。また、クラウドサービス向けの**秘密分散や秘密計算**も実用化されつつある。
○これらの技術を量子暗号と統合することにより「超長期の機密性、改竄耐性、可用性、計算機能を有する量子セキュリティ技術」を実現でき、将来にわたり堅牢なセキュリティを持ったサイバー空間を構築することができる。

量子セキュアクラウド

- ✓ **量子暗号、秘密分散、秘密計算、耐量子計算機暗号**を統合
- ✓ 将来にわたり盗聴や改竄を防ぎ、秘匿性を保ったまま計算を実行

→ **事業継続性のあるデータバックアップや安全なデータ2次利用を実現し、社会保障費の削減や新サービスを創出**

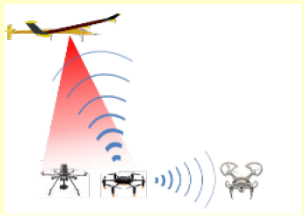


（出典：NICT）

適応的物理レイヤ暗号

- ✓ **光や電波の量子的、電磁気的性質に基づく無線暗号通信技術**を開発
- ✓ 通信路の状況に応じて**最適な電磁波帯域を用いて情報理論的に安全な暗号通信**を実現

→ **IoT機器やドローン等が、いつでもどこでも高速かつ安全な通信ができるサービスを提供**

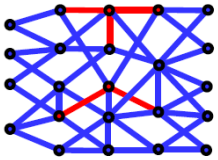


量子暗号
不確定性原理、物理乱数
×
情報セキュリティ
現代暗号、計算機科学、ネットワーク理論

光・量子ネットワーク暗号化

- ✓ **量子暗号、秘密分散、ネットワーク理論**を統合
- ✓ **複数のノードとリンクで分散的に符号化・暗号通信する光・量子ネットワーク暗号化技術を開発**

→ **サービス停止攻撃耐性や可用性に優れたスケーラブルな秘匿通信ネットワークを実現**



量子セキュア移動通信ネットワーク

- ✓ **衛星、ドローン、コネクテドカー**等の移動体に量子セキュリティ技術を実装
- ✓ モビリティ、接続性、安全性に優れた移動通信技術を開発

→ **宇宙、成層圏、高高度から地上網まで網羅する大容量かつ安全な移動通信ネットワークを実現**

（出典：NICT）

量子セキュリティ技術により、永続的セキュリティを持ったサイバー空間を構築！