Sec01-03-12_「サイバーセキュリティ研究開発戦略」の要約

この要約資料の概要

この要約資料の趣旨

- 「サイバーセキュリティ研究開発戦略」の目次と内容を要約したもの
- 「近い将来の情報通信技術の利活用」を認識することにより、対応すべきサイバーセキュリティ対策を想定する

原本

サイバーセキュリティ研究開発戦略

- 概要 https://www.nisc.go.jp/conference/cs/pdf/kenkyu2021-gaiyou.pdf
- 本文 https://www.nisc.go.jp/active/kihon/pdf/kenkyu2021-kettei.pdf

改版履歴

- 2022年1月25日再構成
- 2021年5月27日
- 2021年5月24日
- 2021年5月19日

目次

1．はじめに

- （1）サイバーセキュリティ研究開発戦略策定までの経緯
- （2）本研究開発戦略の趣旨、位置づけ
  - ①これまでの情報通信技術（IT）に関わる進化
  - ②サイバーセキュリティ研究開発の目的
  - ③ 本研究開発戦略の位置づけと構成

2．近い将来の情報通信技術（IT）の利活用を想定した研究開発戦略

- （1）基本的な考え方
  - ①ビジネスのプロセス全体を視野に入れることが重要
  - ②システム運用時に必要なサイバー攻撃の検知・防御だけでなく、ライフサイクル全体で捉えることが必要
  - ③セキュリティ技術だけでなく、多角的なアプローチが重要
- （2）近い将来の情報通信技術（IT）の利活用
  - ①サイバー空間と物理空間の融合（IoT）－つながる－
  - ②AIの高度化・ビッグデータの活用－知能化する－
  - ③ネットワーク関連技術の高度化－広がる－
  - ④ 量子技術の進展
- （3）セキュリティ研究開発における課題に対応した方法論
  - ①国内外における産学官の連携と企業経営層のリーダーシップによる研究開発
  - ②脅威に関する情報やユーザー等のニーズを踏まえた実践的な研究開発
  - ③サイバーセキュリティの研究開発に係る制度等の検討
  - ④ オープン・クローズ戦略の推進
  - ⑤イノベーションの「シーズ」としての研究開発の推進

3．中長期を見据えた考え方

- （1）情報通信技術（IT）の進化による人間の多様な価値観の実現
  - ①つながりの指数関数的な拡大と深化
  - ② AI（人工知能）
  - ③AR（拡張現実）・VR（仮想現実）
  - ④その他の技術の進展（クロスモーダルメカニズムの活用など）
- （2）サイバーセキュリティ研究の広がり
  - ①将来の技術進歩を基本とした考え方（フォアキャスト）
  - ②フォアキャストのアプローチの限界

- ③サイバーセキュリティ研究の広がり
- （３）想定できない変化に対応するための全体設計（デザイン）
- ４．研究・産学官連携の推進方策と産学官エコシステムの構築
  - （１）我が国の研究コミュニティの状況を踏まえた推進方策
    - ① 研究分野の国際動向と特徴
    - ② 人に投資すべき
    - ③ 産学官連携の可能性
    - ④ 研究コミュニティ全体の発展
  - （２）我が国の強み・ポテンシャルと重点的な強化に向けて
    - ① 我が国の強みとポテンシャル
    - ② 重点的な研究領域
  - （３）研究コミュニティの継続的な取組
- ５．まとめ

内容のポイント【マーキング箇所】

1 １．はじめに

2 （１）サイバーセキュリティ研究開発戦略策定までの経緯

本戦略は、将来的なサイバーセキュリティの研究開発を検討・推進するためのビジョン

これまでのサイバーセキュリティに係る研究開発の進捗と、ITの利活用の広がりやサイバー攻撃の脅威の深刻化といった環境の変化を踏まえる

2 （２）本研究開発戦略の趣旨、位置づけ

▶ ①これまでの情報通信技術（IT）に関わる進化

長い人類の歴史を見据えた上で現在を位置付け、未来に向けたサイバーセキュリティの研究開発を考えていくことが必要である。

▶ これまでの人類の知的活動に関する歴史を振り返ると、

「知の継承」（文字と紙の発明）、

「知の流通」（活版印刷の発明）、

「場所や時間の制約に囚われない知の共有・活用」（コンピュータとインターネットの発明）

▶ 知の共有・活用については、

当初は、軍事や設計・研究のために使われる専門家のツールとしての ITから、

パソコンやスマートフォンが普及し、個人、企業、大学、政府等が利用し、情報収集・発信やイノベーションのためのツールとしてのITへと発展した。

そして、近年では、IoTに代表されるように、あらゆる個人とその活動・モノがつながるITへと進化を遂げている 。

▶ こうした進化は、人間と情報の関わり方について、次のことを促してきている

①情報の環境化

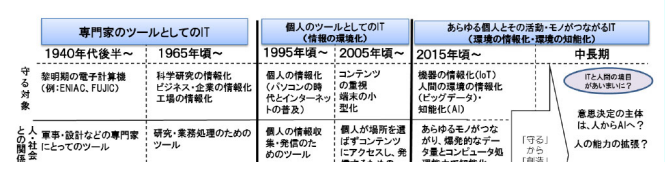
インターネットの普及により、多くの情報が身の回りにあふれること

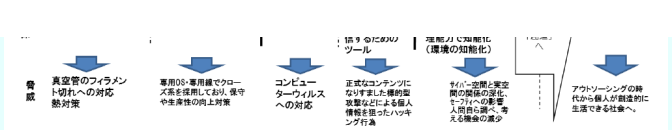
②環境の情報化

IoTにより、ITが実世界と結びつき、センサーが実世界から収集したデータを基に実世界を変えることができる時代

さらには、③環境の知能化

実世界から収集したデータがビッグデータとして蓄積され、そこから有用な情報を取り出すために人工知能が活用されること





（図１）これまでの情報通信技術（IT）の進化

②サイバーセキュリティ研究開発の目的

a.多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、社会システム を創造していく ことを前提として、

b.研究開発を通じて国際競争力を強化すること

c.研究開発で得られた知見により経済成長につながる新産業を創出すること

d.我が国として必要な技術力を獲得・保持すること

③ 本研究開発戦略の位置づけと構成

ITの進化や、人間と情報の関わり方が変化していることを意識しつつ、将来的なサイバーセキュリティ研究開発の方向性についてビジョンを示すものとする。

その際、「近い将来」だけでなく、「中長期的」な社会・経済 の変化 と ITの利活用の進化を視野に入れるものとする。

第2章

近い将来のITの利活用に必要なサイバーセキュリティに関する研究開発を推進するため、その基本的な考え方を示すとともに、サイバー空間と物理空間の融合、AIの高度化・ビッグデータの活用、ネットワーク技術の高度化といった情報通信技術（IT)の利活用の進化の具体例も含め、近い将来の研究開発の今後の課題を提示する。

主に、組織における研究開発に携わる管理職～担当者が、今後の自組織における研究開発の戦略や具体的なプロジェクトの企画・立案を行う際に、この内容を踏まえて取り組むことを想定している。

また、将来の社会像や、サイバー空間とそれを支える技術の進化を踏まえれば、サイバー空間を介して人間の能力が拡張し、これまでの生活や労働をITが代替するにとどまらず、新しい価値を創造し、より良い社会や人々の思いの実現につながっていく可能性がある。

第３章

こうした変化の中で、改めて人間を中心としたサイバーセキュリティ研究の広がりを示し、中長期的な研究開発を検討する際の考え方を提示している。

第４章

研究及び産学官連携の振興に係る検討の具体化として、研究開発の国際競争力を躍進させる産学官エコシステムの構築を目指した推進方策を示した。

本研究開発戦略は、

主に、情報通信技術（IT)やサイバーセキュリティの研究者のみならず、

経営者 や組織の中長期的な経営課題について考えるべき立場 にある者、

さらには、 人文社会科学系の研究に従事している立場にある者を含め、

自組織の中長期的な戦略を議論する際に活用されることを期待している。

1 ２．近い将来の情報通信技術（IT）の利活用を想定した研究開発戦略

2 （１）基本的な考え方

基本的な考え方

従前、サイバーセキュリティ対策については、攻撃に応じて、有効な対策を立てて防御していくということに注力をしてきた。

その際、攻撃者側が日々、攻撃を進化させてきていることや、守るべき情報資産の分類に対応するため 、様々な 手段を使って守りを固める考え が一般的に浸透している。

具体的には、攻撃者のシステムへの侵入等の行為が行われないよう、攻撃を受ける側で過去の攻撃情報の共有を行い、それに基づいて後追い的に技術的な手法を中心として対策が講じられてきた。

こうした仕組みの下では、脆弱性対策をはじめとしたシステム等のメンテナンスや更新 の管理が 肥大化・複雑化する可能性がある。

ビジネス全体を見据えた広い視野がなければ、攻撃が進化すればするほど、サイバーセキュリティ対策に対するコストは上昇し続け、そのコストは、本来のビジネスに対する影響を及ぼす可能性があり、増大するコストは、経営層の正しい認識なしには承認を得られない ことが生じ得る。

また、後追い的なセキュリティ対策では、インシデント対応のコストが増加する可能性があり、失われた情報や評判の回復

にリソースを費やすことにもなりかねない。

さらに、このような対策の下では、結果としてサイバーセキュリティの側面だけの部分最適になっている可能性もあり、このような流れに依存するだけでは、問題解決が困難になる可能性がある。

社会的・経済的要因を考慮に入れながら、安全・安心なサイバー空間を発展させ、本来のビジネス等を促すためにすために一貫性を持つ形で、セキュリティの問題を合理的かつ積極的に達成可能なものとしていく視点が必要である。

そのためには、業務、製品・サービス等のデジタル化、さらには変革を伴うDXを含め、ITの利活用の発展を踏まえつつ、視野を広げてサイバーセキュリティ対策を捉えていくことが期待される。

こうした方向に資するようなサイバーセキュリティ対策におけるアプローチを検討した上で、研究開発を進めることが期待されるため、 以下に 基本的な考え方を提示することとする。

①ビジネスのプロセス全体を視野に入れることが重要

従前、我が国の企業における情報通信技術（IT)の利活用は、業務効率化を目的として、基幹系システム（生産・販売、会計、人事、給与、資産等の管理に関する企業内のシステム）や情報系システム（メールや文書作成、スケジュール管理等に関する企業内のシステム）を活用することが中心であった。

近年は、IoT、ビッグデータ、AIなど、ITの利活用によって、新しい価値を創造するような、いわばビジネスにおけるイノベーションを目的としたITの利活用が増加する傾向にある。

特に、IoTシステムの急速な普及は目覚ましく、これによって、サイバー空間と実空間の融合が高度に深化することになる。

こうした中で、市場における個人・企業がIoTシステムを通じたサービスに期待する品質の要素としての安全やセキュリティ、すなわちより高いレベルの「セキュリティ品質」を目指し、企業価値や国際競争力の源泉としていくことが必要である。

その際、これまでの「セキュリティ」品質は、情報システムの信頼性が極めて重要な要素であったが、IoTシステムをはじめとする新しいITの利活用においては、それが提供するサービスを安全かつ持続的に提供すること（機能保証）が求められる。

それは、セキュリティを含めたシステムの個々の構成要素の組み合わせ（システムインテグレーション）によって実現されるものであり、その組み合わせ方を決めるものが「ルール 」である 。

このため、セキュリティ技術やその要素技術はあくまでビジネスのプロセスを実現する一つの手段と考え、「ルール」を含めた情報システムを取り巻くビジネスのプロセス全体を考慮に入れたセキュリティの研究開発が実施されるべきである。

同時に、上述の通り、ビジネスのプロセス全体を考慮に入れ、ビジネスにおける機能保証とセキュリティ品質の向上を目指す場合、機能レベルを含めた脅威やセキュリティの問題点の可視化や評価技術の確立、内外の専門人材と協働し現場の知見を取り入れることなど経営層が認識を深めるための取り組み、対外的なセキュリティ品質等に関する情報発信を含めて取り組んでいくことが重要である。

②システム運用時に必要なサイバー攻撃の検知・防御だけでなく、ライフサイクル全体で捉えることが必要

先述の通り、ITの利活用によって、新たな価値を創造する中で、企業価値や国際競争力の源泉となる高いレベルでの「セキュリティ品質」を実現していくことは重要な課題である。

しかし、セキュリティをシステムの運用が始まった後に、後付けで導入しても、システムは本質的に安全になるものではなく、むしろ単にコストの大幅な増加の要因となる。

また、欧米においては、インダストリー4.0やインダストリアルインターネットに代表される企業間連携や、製品にセキュリティ対策が行われていることを前提とした標準化の動きがあり、サイバーセキュリティ対策は、サイバー攻撃の検知・防御だけでは不十分となりつつある国際的な動向も踏まえた対応が必要である。

この際、連携される既存のシステムを含めて、システム全体の企画・設計段階から、セキュリティの確保を盛り込むセキュリティ・バイ・デザイン（Security By Design）の考え方を推進する。

また、IoTシステムやAI等を活用した新たなビジネスを創出する際、コスト抑制の観点から、安価な機器の調達・導入が選択される可能性があることや、企画・設計から廃棄までのライフサイクルが長いこと、機器の演算処理能力に制限があることなど、IoTシステムにおいては、従来の情報通信機器とは異なるセキュリティに関わる構成要素の特徴 が存在する。

このため、セキュリティの研究開発においては、こうしたシステムの特徴を踏まえつつ、ライフサイクルの各段階において必要な技術の検討を行うことが重要である。

特に、IoTシステムの製造に関わるサプライチェーンシステムの複雑性を踏まえ、製品に組み込まれるICチップを含むハードウェアの真正性の検証技術等は重要である。

③セキュリティ技術だけでなく、多角的なアプローチ（手段）が重要

ITの利活用に関する技術の進歩により、サイバー空間が実空間と融合し、現実社会への影響も大きくなっている。一方で、サイバー攻撃の手段も日々進化している。

こうした中、単に情報システムに対するサイバー攻撃の脅威だけに注目し、その検知・防御等のためのセキュリティ技術による後追い的な対策だけでは、脅威に対抗し、システム全体を守ることは困難になりつつある。
言い換えれば、**攻撃の検知や防御には限界がある可能性を前提とした取り組み**が重要である。

このため、従来から行われてきた検知技術、暗号、認証技術、ネットワークアクセス制御など検知・防御を中心としたセキュリティ技術に関する研究のみならず、

攻撃を受けた場合のシステムの抵抗力や回復力（レジリエンス）の確保

被害を最小化するためのシステム運用技術・ノウハウ、マネジメントやリスクコミュニケーション、

さらには法律や経済・経営、国際関係、安全保障、心理等の社会科学的視点も含め、様々な領域の研究との連携

、融合領域の研究に取り組む

例えば、サイバーセキュリティは、経営層が自ら理解し、必要な判断が求められているため、企業としての「挑戦」と、それに付随する「責任」として、サイバーセキュリティに取り組むための経営に関する研究や、経済や社会との関係において企業に求められるサイバーセキュリティの対応に関する研究などが挙げられる。

2 （２）近い将来のITの利活用

概要

様々なモノが①つながること

近年のITの進化の流れ（トレンド）については、サイバー空間と物理空間の融合（IoT)に代表されるように、様々なモノが①つながること、

モノが②知能化すること

そして、つながるだけでなく、AI の高度化やビッグデータの活用によって、モノが②知能化すること、

③広がること

さらに、そういったものがネットワーク効果（つながるモノが増えれば増えるほど、ネットワークの価値が高まり、モノがより良くなっていくこと）によって、③広がること、が進展していると言える。

④量子技術の進展

また、④量子技術の進展も起きている。

こうした変化の流れ（トレンド）を捉えつつ、サイバーセキュリティの研究開発に係る課題を見いだし、取り組んでいくことが必要である。

①サイバー空間と物理空間の融合（IoT）－つながる－

IoTシステムの普及により、サイバー空間と実空間の融合が高度に深化する。

今後、企業は、こうしたIoTシステムを活用した新たなビジネスの創出や既存ビジネスの高度化を図る方向に向かうと見込まれる。

このため、我が国企業がこうしたビジネスチャンスを確実に捉えることは、我が国の経済社会の活力の向上及び持続的発展にとって極めて重要である。

その際、IoTシステムのサイバーセキュリティを確保することは重要であるが、IoTシステムの特徴を意識しつつ、ビジネス自体の目的や戦略に沿った形で、重点的に取り組むべき事項等の検討が行われることが重要であり、それに資するような研究開発が行われるべきである。

具体的には、IoTシステムについては、先述の通り、特に産業用システムの場合、それを構成する機器のライフサイクルが長いことや、安全性や長時間の安定稼働、さらには、家電などの小型システムの場合に低い演算処理能力の下でのセキュリティ対策 が求められる。

そして、業種・ビジネスモデルによって、システム全体を構成する要求項目が広がる可能性があるとともに、個々の要求項目に対する水準も大きく変わることなど、これまでのコンピュータやサーバーがネットワークにつながった主に業務効率化を目的とした従来型の情報システムとは大きく異なる。

一方で、こうしたIoTシステムを構成する機器が爆発的に増加し、様々な機器が入り混じる形でつながることから、一つ一つの機器を管理し、同じレベルで整合的に技術的な対策を講じることには限界がある可能性がある。

このため、これまで、事業との関係が希薄であった情報システムにおける機密性・完全性・可用性を目指したセキュリティコントロール、例えば、通信の暗号化、アップデートによる脆弱性対策、ウィルス対策等による予防措置、個々の通信監視による検知や冗長化による復旧を、IoTシステムに従来と同様に適用することは適切ではない可能性があるとの認識を持つことが必要である。

むしろ、IoTシステムのセキュリティを単独で企画・設計等を検討するのではなく、IoTシステムにより、新しい価値を生み出すビジネスの創出が促進できるよう、それ以外の強み・弱みを捉え、想定されるビジネス自体の目的や戦略に照らして、ビジネスの品質を決定する一要素としてIoTシステムのセキュリティの考え方を整理することが期待されている。

このため、こうした考え方を踏まえた、必要な技術の研究が進められるべきである。

②AIの高度化・ビッグデータの活用－知能化する－

ａ．人工知能の活用におけるセキュリティ

人工知能に関する研究は、これまで、数学の定理を証明することやチェスを指す人工知能といったコンピュータによる探査・推論によって特定の問題に対して解を提示するもの、コンピュータに知識を与えることで人工知能が実用可能な水準に達し、専門家のように振る舞うことができるもの、そして、 近年では、ビッグデータを用いて、人工知能自体が知識を獲得するディープラーニング（多層構造のニューラルネットワークを用いた機械学習）が実用化されている。

こうした人工知能は、産業、教育、行政など幅広い領域で人間社会に深く浸透することで、人々の生活が豊かになることが期待される一方で、悪用されることにより、公共の利益を損なう可能性も否定できない。こうした観点から、人工知能の活用におけるセキュリティに関し、どのような具体的な課題があるのかという社会全体での議論が期待される。

我が国においては、Society5.0の実現を通じて世界規模の課題の解決に貢献するとともに、我が国自身の社会課題も克服するために、今後のAIの利活用の環境整備・方策を示した「AI戦略2019」（令和元年6月11日統合イノベーシ

ション戦略推進会議決定）が策定されたが、こうした取組の内容を踏まえつつ、AIに関するセキュリティを実現するための研究開発を行うことが期待される。また、AIの高度化と併せて、プライバシーの確保やAIそのものを守るセキュリティに関しても、研究開発の検討においては重要な要素である。

b．サイバーセキュリティ分野における AI の活用

近年、サイバーセキュリティに関する業務においてAIを活用することが注目されている。

これまで、サイバー攻撃に対する検知は、ルールベース（不正が疑われるプログラムの動作を解析し、「ルール」と合致する動作を行うものを判定する方法）やシグネチャーベース（過去に行われた攻撃に関する通信をデータベース化し、通信の内容が一致するものを判定する方法）の防御システムを導入し、そのシステムの設定を調整（チューニング）することで行われてきた。

こうした手法では、情報共有・収集等による過去の攻撃に関する一元的なデータベースの構築を前提としており、攻撃者側のスピードに追い付くことができず全く新しい手法による高度な攻撃に対応することはできない。

このため、特に侵入検知の領域において既にAIの活用が進んでおり、エンドポイント（ネットワークに接続されたサーバー、パソコン等）の振舞いを検知しログを取るエンドポイント分析、ユーザーの行動（メールのやりとりや、システムの操作）の分析、ネットワークトラフィックのビッグデータの分析、これらを総合的に組み合わせた、異常な動きや振舞いの分析に関するさらなる研究開発や実用化が期待されている。

さらに、攻撃者側によるAIの活用が考えられ、こうした動きへの対応も必要である。

加えて、このようにAIがサイバー空間上で攻撃・防御を人間に代わって行うような状況においては、これまでのサイバーセキュリティ対策の常識に囚われず、攻撃者の持つ技術の異次元の高度化に対応した適切なアプローチの在り方に関する研究開発についての検討も必要である。

③ネットワーク関連技術の高度化－広がる－

様々なモノがネットワークにつながるようになり、5Gによってネットワークの拡大と併せて通信容量は大幅に増大するとともに、クラウドサービスをはじめ新しいサービスが登場している。

また、ITの利活用による新しい価値を生み出すビジネスのモデルが時々刻々と変化を遂げる中、ネットワークが提供するサービスのライフサイクルが短くなっている。

こうした中では、通信に求められる品質に応じて通信毎のネットワークの分離を図ることにより、通信の効率化のための制御を実現することや、ビジネスのニーズに対応したネットワークの変更等、ネットワークに高い柔軟性が求められることになる。

さらに、ネットワークが拡大していく中で、つながるモノや人の信頼性（トラスト）の確保が重要となる 。

集中化された信頼の起点に頼る形で多くのネットワークへの参加者のアクセス権を制御することは、単一起点がボトルネックになることや、それ自体の脆弱性が大きな悪影響につながることなど、ネットワーク全体の信頼性の観点からは、分散化、例えばネットワークの参加者相互のコンセンサスによる信頼の確保が有効な可能性がある。

このように、IoT時代において、ネットワークが大幅に拡大していく中で、ネットワークの「効率性」、「柔軟性」、「参加者の相互信頼」を高めることが重要になってくると考えられる。

こうした中、ネットワーク技術の高度化が急速に進展しつつある例えば、昨今、ネットワーク機器の操作・制御の自動化を進め、オペレーションの効率化を進める観点から、幅広い範囲のネットワーク機器を、ソフトウェアによって集中的に制御する、いわゆるSDN（Software Defined Networking）に対応した製品の導入が進められており、データセンター内ネットワーク、データセンター間ネットワーク、クラウド基盤、インターネット・エクスチェンジの運用・管理や地上デジタル放送の中継回線の制御など、一部の大規模ネットワークの運用・管理に導入が進んでいる。

また、機能の定まった個々の機器の制御にとどまらず、ソフトウェアによる「ネットワークの機能の仮想化」(NFV: Network Function Virtualization)により、ネットワークを構成する機器の機能は「所与」のものでなく、機能分担を自由に決定、変更することも可能となってきた。

これらの技術を活用すれば、ネットワークの構築に携わる者自身が、汎用的なハードウェアの上に、ネットワークの構成要素を自由に設計・制作することが可能となる。

さらに、セキュリティに関しては、ネットワーク全体のコントローラの保護を前提として、サイバー攻撃等により問題が生じたネットワークに関して、攻撃された部分を分離し、バーチャルに冗長化された代替のネットワークに切り替えることによって、ネットワークの機能を損なわずに、攻撃された部分の修復を行なうような柔軟な対応が可能となる。

また、シェアリング・エコノミーが広がっていく中で、その要素の一つとして活用が期待されるビットコイン等の価値記録の取引に使用されているブロックチェーン技術は、「取引履歴を暗号技術によって過去から1本の鎖のようにつなげ、ある取引について改ざんを行うためには、それより新しい取引について全て改ざんしていく必要がある仕組みとすることで、正確な取引履歴を維持しようとする技術」である。

その構造上、従来の集中管理型のシステムに比べ、①改ざんが極めて困難であり、②実質ゼロ・ダウンタイムなシステムを、③安価に構築可能、という特性を持つものであり、IoTを含む幅広い分野への応用が期待されている。

これまで、サイバー空間においては、経済活動の基盤となる取引相手の信頼性を担保する手段として、様々な制度や仕組みを構築してきたが、ブロックチェーン技術は、これらの仕組みを代替し、従来の社会システムを大きく変容させる可能性がある。

例えば、参加者同士が対等の関係で相互に協力・監視することで、これまで社会システムを維持するために多大なコストを払って構築してきた中央集権的な第三者機関（中央機関）を不要とする可能性 がある。

このように、こうしたネットワーク技術の発展の方向を見定めつつ、それに関わるセキュリティの問題の研究を適時に実施していくことが望まれる。

④ 量子技術の進展

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におけるセキュリティを支える公開鍵暗号技術が将来的に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、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が進められている。

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、重要な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、かつ改ざんを目指し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

く、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。

2 （３）セキュリティ研究開発における課題に対応した方法論

①国内外における産学官の連携と企業経営層のリーダーシップによる研究開発

これまで、サイバーセキュリティに関する技術の研究開発を行ったとしても、事業化して、その技術そのものが普及するためには、大きな壁があるとさ れてきた。

これはサイバーセキュリティの分野に限らず、いわゆる「死の谷」の問題として研究開発で指摘されてきた問題である。

こうした問題に陥らないようにするため、顧客にとって魅力的で品質の安定した製品・サービスが、現実的な価格で提供できることを想定した研究開発が必要である。ところが、こうした顧客の視点や製品・サービスの品質に関わる事項については、研究者の科学的

知識と能力だけで研究開発に反映できるものではなく、ビジネス戦略上の判断や顧客目線を持った上での研究開発のアプローチが不可欠となる。

例えば、他の異なる企業が持つ技術と組み合わせることや、自組織が持つ技術の改良なのか、新規技術の研究が必要なのかといった判断、技術に期待される品質のプライオリティ、などである。

このような観点で研究開発を行うためには、研究を実施する主体だけが独立して研究を実施するのではなく、国内外の産学官の連携や、企業経営層を巻き込んだ研究開発の推進（例えば、研究機関の幹部と産業界の幹部の連携枠組に基づく、個別の研究の推進）が必要である。

なお、こうした連携を実現するためには、研究の実施機関においても、単に実用化に極めて近い技術だけを追求するのではなく、産学官連携の中で貢献できるような魅力的な基盤技術を高めていくことも重要である。

②脅威に関する情報やユーザー等のニーズを踏まえた実践的な研究開発

未整理

IoTシステムが普及し、世界とのつながりが拡大する中、サイバーセキュリティの研究発は社会的なニーズや世界のトレンドを踏まえ実用化されることが重要であり、研究成果の社会還元の推進が重要である。

このため、情報通信技術（ITの利用者が受けているサイバー攻撃の実態や脅威ITの利用者のニーズ・リテラシーを十分に把握した上で、研究が行われなければ、社会還元を図ること は難しい。
例えば、研究者とサイバーセキュリティの実践側（IT)の利用者やITサービスの提供者）との連携が重要であり、研究者が攻撃者の動向を把握することも重要である。

研究開発をより実践的なものとし、効果・成果をあげるために、具体的な事象などの脅威に関する情報やユーザー等のニーズに関する情報共有などを促していくことが重要である。

③サイバーセキュリティの研究開発に係る制度等の検討

先端のサイバーセキュリティの研究開発を推進していくため、必要な制度の見直しを柔軟に検討していくことが重要である。

例えば平成30年度にセキュリティ目的のリバースエンジニアリングに関する適法性の明確化 を含む 著作権法改正が行われた 。

関連して、サイバーセキュリティ対策の実施において参照すべき法制度に関する整理が行われている「サイバーセキュリティ関係法令Q&Aハンドブック」（令和元年度） 。

また、サイバーセキュリティに関連する技術の発展に伴い、社会との接点で生じる様々な倫理的 ・ 法的 ・
社会的課題（ELSI）に対する適切な配慮が必要である。

④ オープン・クローズ戦略の推進

a.オープン・クローズ戦略に関わるセキュリティ

我が国は、これまで現場の「カイゼン」によって、匠の技を磨き、品質が高く、生産性の高い「もの」づくりを実現してきた。

しかし、付加価値が「もの」そのものから、「サービス」「ソリューション」に移っており、3Dプリンターなどのデジタルファブリケーションの登場等により、単に良い「もの」をつくるだけでは企業が生き残れない時代に入っている。

さらに、サイバー空間が、「サービス」「ソリューション」における価値の形成において、大きな役割を担うようになってきている。こうした中、ビジネスモデルについては、近年、オープン・クローズ戦略が重要になっている。

これは、国際連携によって、様々なプレーヤーが自由に参加し、切磋琢磨しながらイノベーションを生み、その恩恵を参加者が得て、市場全体を広げる領域（オープン領域）と、外部のプレーヤーには参加を許さず、技術や仕組みそのものを独自の取り組みによってブラックボックス化する領域（クローズ領域）を明確にすることである。

セキュリティの問題についても、これまでは各企業がクローズに個々の製品やITサービスと並んで、セキュリティ製品・サービスも提供してきた 。

しかし、これからの付加価値の力点が「サービス」「ソリューション」に移ると、例えば、利益率の低い傾向にあるオープン領域の製品に関する研究開発でしのぎを削るのか、利益率の高い傾向にあるサービス・ソリューションにおいてクローズ領域を設定し、全体のビジネスモデルを描く立場になるのかといった検討が必要になってくる。

また、IoTシステムの場合には、サイバー空間（例：ソフトウェアやデータ）と物理空間（例：ハードウェアやモノづくり）をクローズ領域にし、これらの空間をつなぐ領域は標準化を推進し、オープン領域に位置付け、市場の拡大を図りながら利益を得ていく、といった戦略の検討も必要である。

そして、これらのオープン領域・クローズ領域それぞれにおいて、必要なセキュリティの研究開発をどのように
位置付けて行うのかを考える ことが重要である。

この際、標準化されたオープン領域とクローズ領域が決まっているプラットフォーム以外でビジネスをしようとするとコストが非常に高くなり、プラットフォームのルールに従わざるを得ない状況となる 。

このため、このプラットフォームそのものを自社の競争優位にはたらくよう設計していく中での一要素としてサイバーセキュリティを位置づけ、どのようにその研究開発に取り組み、セキュリティ品質を高めていくのか、検討が必要である。

b.セキュリティ技術のオープン・クローズ戦略

サイバー攻撃は国境を越えて行われることから、高度化・巧妙化するサイバー脅威に対処するための技術的な取り組みに当たっては、国際的に連携して対応することが求められる。

そのためには、各国が「強み」を有する技術を有機的に組み合わせ、発展させることが有効である。

このため、研究の内容や我が国の安全保障上の問題にも留意しつつ、我が国の取り組みを積極的に海外に対して発信し、国際連携による研究開発を積極的に行っていくことが必要である。

同時に、様々な国際標準化の取り組みが行われている中で、セキュリティ技術を中心とした様々な国際標準の策定・普及についても推進することが必要である。

こうしたオープン領域に係る戦略と併せて、我が国の安全保障や競争力の観点から、外部にはオープンにしない独自の研究開発（クローズ領域）も重要である。

こうしたクローズ領域の研究開発を行うためは、コンピュータやシステム等の原理・仕組みなどの理解と、それを自ら考え開発するために必要なコア技術が必要となる。

これらの基盤技術自体は、直ちにビジネスにつながらないものであっても、クローズ領域の取り組みを図る上では必要となる可能性があるため、そうした技術を特定し、研究開発を推進することが重要である。

いずれにしても、このように、国際連携によってオープンに研究開発を行うべき技術と、クローズ領域において必要な技術について、ポジショニングを行い、戦略的にセキュリティ技術の研究開発を進めていくことが必要である。

⑤イノベーションの「シーズ」としての研究開発の推進

ビジネスにおけるイノベーションからの「ニーズ」に応じて行うサイバーセキュリティの研究だけでなく、ビジネスのイノベーションにつながるような革新的なサイバーセキュリティ技術を生み出すための研究開発、換言すれば、ビジネスイノベーションに対する「シーズ」となるサイバーセキュリティ技術の研究開発についても、研究開発の検討においては考慮すべきである。

例えば、公開鍵暗号方式（相手には公開鍵を伝え暗号化して送信をしてもらい、対となる秘密鍵で復号する方式。）の発明により、正規の受信者のみ安全に情報を得ることができる仕組みが実現し、電子商取引の発展などに大いに貢献したとされている。

1 3．中長期を見据えた考え方

概要

我が国が超高齢化社会と人口減少社会といった課題に直面する中、サイバー空間においては、IoTやAI、AR・VRにより、実空間とサイバー空間の融合が高度に深化していく。

それによって、人間の能力は拡張し、これまでの生活や労働を代替するにとどまらず、新たな価値を創造していくと考えられる。そして、より良い社会や人々の思いの実現につながっていく可能性がある。

一方で、このように実空間とサイバー空間の融合が高度に深化していく中で、顕在化している目下の課題だけに囚われていると、現時点では容易に想定することが難しい未来の変化に対して脆弱な状況に陥る可能性がある。

例えば、人間がネットワークに常時つながり、AIなどによって能力が拡張した場合、自分の判断の主体は、自分なのか、ネットワークに常時つながった他者なのか、あるいはAIなのかが明確ではなくなり、自分と他者、組織、社会との境界、すなわち自己の概念が曖昧になっていく可能性がある。

こうした中で、サイバーセキュリティの考え方として、サイバー空間を構成する情報システムに対する脅威への対応のみならず、人間社会を構成し、個々の機能を持つ様々なモジュール（人間とAIが一体になったもの（能力が拡張された人間）や、人間を取り巻く環境など）同士の関係性に着眼し、「人間とは何か」という問いかけをしながら、「情報システム」だけでなく、「人間」や「社会」を一体として捉えることが重要になってくると考えられる。

本章では、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムの実現に向け、想定することが難しい未来が起こりうる中長期を見据え、各組織が研究開発の方向性やテーマを議論するためのサイバーセキュリティの一つの考え方を示すこととする。

2 （１）情報通信技術（IT）の進化による人間の多様な価値観の実現

概要

歴史的に、人間は「道具」を使い、「環境」を変えること、いわば人間の能力の拡張によって、文明が発展し、人間の生活を安全で豊かなものにしてきた。

そして、１．（２）①で触れたように、人間は、情報通信技術（IT）の進歩によって、人間と情報の関係性については、①情報の環境化、②環境の情報化、さらには、③環境の知能化を実現してきた。

こうしたサイバー空間の発展は、超高齢化社会と人口減少社会といった課題に直面する我が国において、質の高い遠隔医療や遠隔教育等をもたらすだけでなく、グローバルには、公共領域において必ずしも声を持てなかった社会的弱者や途上国の村落部に住む人々にもサイバー空間にアクセスし、情報収集や発信を可能とする変化をもたらすに至っている。

今後さらに、全てがつながる環境が整備され（全てがつながることが発展し）、さらに以下に記載するようなAIやAR・VR等の情報通信技術（IT）のより一層の進化により、サイバー空間は、多様な価値観を承認し、人々の期待、物理的な欲求のみならず精神的な欲求をも満たし、より良い社会を形成する基盤として拡張していく可能性がある。

①つながりの指数関数的な拡大と深化

IoTの普及によって環境の情報化が進んでいく中で、モノ同士の関係、人間とモノの関係や、社会とモノの関係、さらには、人間同士の関係までもが変化し、より密接で価値のあるつながりへと深化していく可能性がある。

そして、今後は、人やモノから取得したデータの共有や活用にとどまらず、多様な物事のプロセスや人の豊かな体験までも結びつけるようになっていく可能性がある 。

② AI（人工知能）

いままでの人工知能は、人間が現実世界の対象物を観察し、「どこに注目」するかを見ぬいて（特徴量を取り出して）、モデルの構築を行った上で、その後の処理についてコンピュータを用いて自動で行うものであった。

しかし、近年のコンピュータの演算能力の向上等により、人間の発達と同じような技術進化（認識能力の向上、運動能力の向上、言語の意味理解という順で技術が進展）が可能なディープラーニングによって、「与えられた目的」に対して、それを実現する手段は、学習を通じてますます賢くできるようになる。

これによって、いままでは人間がモデルを改善することによって工業化を進めてきたが、モデルそのものが認識能力や運動能力を持つことによって根本的に産業の仕組を変える可能性がある。

一方で、人工知能は、目的を与えられたときに、問題解決をすることにとどまり、生命のように自己の保存や複製、仲間を守るなどといった目的を持つものではない。

このため、今後は、人間が人工知能に対して与える目的自体の是非の議論のほうがより重要となってくることに留意すべきである。

③AR（拡張現実）・VR（仮想現実）

サイバー空間においては、AR・VR技術などによって、人間の物理空間の感覚をサイバー空間上で実現しようとする取り組みが行われている。

AR技術は、物理空間とバーチャル空間が連続することによって、高齢化社会においても、物理的・身体的制約のない生産、労働、創造性の提供が可能となる可能性がある。

また、VRは、身体を介した一人称の体験をパブリッシュ（本人が知覚可能な体験として、コピー・伝送・再生）することが可能なシステムであり、その一つであるテレイグジスタンスによって、地域間の格差を減らすことが出来ることや、サイバー空間を使って他人に変身することによって、人種的な偏見の減少やうつ病の治療に貢献できる可能性がある。

これらは、人間にこれまでになかった体験を提供し、人間の精神的な豊かさなどの高次の欲求を満たす上で、大いに貢献することが期待される技術である。

④その他の技術の進展（クロスモーダルメカニズムの活用など）

AIやAR・VRのように、既にその技術の実用化が進められており、人間が知っている能力の拡張だけでなく、今後、研究が進むことによって発見される、人間が未だ知らない能力の拡張の可能性があることにも留意をしていくことが必要である。

また、人間の脳と機械の情報伝達を仲介する機器の研究によって、バイオニック義肢を実現し、それは通常の人間の強度を超えたものとなる可能性も存在している。

2 （２）サイバーセキュリティ研究の広がり

概要

普通に使っている言葉が見方を縛ってしまうことがある。

辞書に載っている意味も含めてその概念の中に既に現代的な偏りが潜んでいるので、このことを認識した上で考えていかないと創造的な発想は生み出されない。

例えば、「サイバー」という言葉が、対象でしかないコンピュータネットワークに視野が限られていることで、主体としての人間の能力やその変化に対する考察が弱くなっている可能性がある。

情報機器によって構成される仮想上の空間としての「サイバー空間」のコントロールという議論だけになってしまうと、人間の能力の拡大や衰弱、感覚やリアリティの変化のコントロールが見落とされる危険性がある。

①将来の技術進歩を基本とした考え方（フォアキャスト）

これまで、サイバーセキュリティについては、情報通信技術（IT）の進歩を見据え、攻撃に対する防御の構図の中で、予防・検知・防御・復旧のプロセスを着実に行うことを中心に、必要な制度設計や技術開発等が進められてきた。

具体的には、マルウェア対策やDDoS対策、暗号、認証、マネジメント等が挙げられ、これらの技術は、これまでの構図の中で一定程度、有効に機能してきた。

また、近い将来においては、攻撃に対して技術的な防御を高めていくアプローチだけでは問題解決が困難な可能性があることから、第２章で述べたように、今後は、ビジネスのプロセスやライフサイクルを含めて取り組み、多角的なアプローチによって対策が行われることも重要である。

さらに、（１）で示したように、コンピュータ能力の急速な向上をはじめとして情報通信技術（IT）は急速な進歩を遂げていることに加え、IoTやAIといった現時点で時代の主流となっている技術の先の様々な独自性の高い技術開発も行われている。

これらの将来の技術の進歩が、攻撃に対する防御の構図の中で、人間に与える影響を見通す（フォアキャスト）ことにより、様々な研究開発のアイデアが生まれる可能性がある。

例えば、以下に示すような、新たなサイバー空間上における攻防の問題が起こる可能性もある。

□個人Ａの脳と連携したAI・ロボットが個人Ｂにより不正に操作され、個人Ｂが個人Ａを利用して犯罪を実行する、人間に対する乗っ取りのリスク
□ロボットにより摂取する情報等を操作されることにより、利用者の意思決定や判断のプロセスが操作されるリスク

②フォアキャストのアプローチの限界

概要

将来の技術進歩の外挿（フォアキャストによるアプローチは重要である一方、現在の社会システムや人間観、世界観、倫理の常識が、未来においては根本的に変化してしまう可能性があるにもかかわらず、これらの常識を前提として技術進歩を外挿していくフォアキャストのアプローチのみでは限界が来る可能性がある。

サイバー空間における情報通信技術(IT)の進化は、これまでの経済社会の中で形成されてきた、「雇用／被雇用」や「

生産者／消費者」といった様々な関係が変質していく可能性を内包するものである。

そして、潤沢な情報資源が共有され個々人に届けられる社会においては、アウトソーシングする時代から、創造的に生活する個々人の時代へと回帰し、他者に依存していた自分の生活を、自分のこととして創意工夫し自己実現を図り、それを人々の多様なつながりで共有することによって、さらなる創造を図ることが可能となる。

こうした考察から明らかなように、前提となっている知識を外し、壊すことによって、問題解決に向けた「問い」が深まり、動いていくということに留意する必要がある。

その中で、サイバー空間が人間や社会にもたらすことについて、以下に関連する問題の例を示す。

a.感覚の一部が制限されたコミュニケーションによる影響

人間がサイバー空間に対して意識を向ける時間が増加し、現実空間において積み重ねる人生の「経験」よりも、サイバー空間における「経験」が増えている可能性すらある。

サイバー空間への過剰な接続・依存は、人間にとって不変の生物学的条件としての感覚の一部が制限された状態のコミュニケーションに偏ることになり、情動や信頼に基づく人間関係や人間の「こころ」に影響を及ぼす可能性がある。

b.人間 の環境への適応 の問題

人間の環境への適応を前提にすれば、新しい技術による環境の知能化によって、人間はその環境に適応する可能性がある。

例えば、情報通信技術（IT）の進展によって、モビリティの自動操縦の可能性が高まっているが、その結果、人間は操縦に必要な身体の能力が低下するリスクが挙げられる。

情報通信技術（IT）の急速な発展によって人間の身体そのものに対し、何らかの影響を及ぼす可能性がある。

c.知能化した環境からの影響により、 自己の意志 が希薄になる問題

人間にとってサイバー空間は、人間がつくりあげた道具にすぎない。しかし、サイバー空間においては、物理空間同様に、人間が意識を向けることによって人間が経験をし、影響を受ける場である。

人間が、知能化した環境であるサイバー空間を通じて様々な恩恵を受ける一方で、サイバー空間に人間が操られるようにすらなる可能性や、自分そして、自分のまわりの社会は、どうありたいかといった自己の意志が希薄になっていく可能性がある。

d.サイバー空間において異質性が共存するための調整

サイバー空間においては、物理空間における人間関係とは大きく異なり、人・モノの一部の側面がインターネットにより地球規模でつながっているため、むしろ、つながる人・モノの物理空間における経験などの違いに起因する異質性が顕著になっている可能性がある。

サイバー空間は、物理空間も含めた様々な環境や経験に基づく、多様な価値観を持った異質性が共存していることにより、イノベーションを生み出す場でもあると同時に、異なる価値観による対立を生み出す場ともなり得る。

こうした対立の調整が様々な方法によって適切に行われることが必要である。

③サイバーセキュリティ研究の広がり

概要

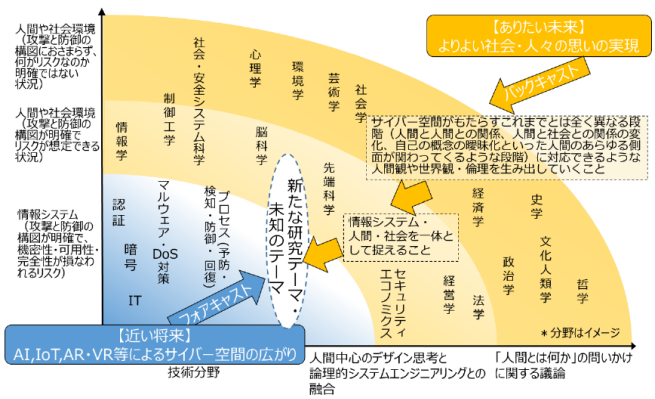
前提となっている知識を外し、壊した上で、未来の問題解決に向けた「問い」を深めていく上で、人間を中心に考えていくアプローチが重要になっている。

サイバー空間がもたらす、これまでとは全く異なる段階（人間と人間との関係、人間と社会との関係の変化、自己の概念の曖昧化といった人間のあらゆる側面が関わってくるような段階）に対応できるような人間観や世界観・倫理を生み出していくことが人文社会学者に求められている。

これは、人文社会科学が、突出した技術社会を監督・制御する構図ではなく、人文社会科学の役割について新たなフロンティアが出現しているとも言え、情報通信技術（IT)と関連する様々な分野との協業により、よりよい社会や人々の思いが実現できるようなありたい未来に向けて、新たな人間観・世界観・倫理が醸成されていくことが期待される。

そして、その人間観・世界観・倫理の下で、「情報システム」だけでなく、「人間」や「社会」を一体として捉えることで、サイバーセキュリティ研究における新たなテーマや未知のテーマの発見やその広がりにつながるものと考えられる。

それにより、多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造し、人類社会の持続可能性という課題を世界に先駆けて解決することにつながる。



（図２）サイバーセキュリティ研究の広がり

（３）想定できない変化に対応するための全体設計（デザイン）

バックキャストによるアプローチにおいて、想定できない変化に対応したサイバーセキュリティを考え、「情報システム」「社会」「人間」を一体として捉え研究開発の内容を検討する際、科学技術をベースとして、供給者主導で行うものだけでなく、社会的なプロセスやコミュニティによる需要者主導で行うものも必要である。

その際の全体設計の方法論として、目的思考的に俯瞰性と系統性を論理的に考えるシステムエンジニアリングと、論理性では見えてこない人の感情的・感覚的側面を人間中心的に扱いながら多様性を活かして試行錯誤を繰り返すデザイン思考とを融合するアプローチが有効な可能性がある。

人間には知らないことの存在すら認識していないことがあり、こうした問題はそれを取り巻く状況の変化によって顕在化する可能性がある。

例えば、サイバー空間でいえば、電子メールの黎明期の1980年代に「標的型メール攻撃について知らない」ということを多くの人は意識していなかった可能性があり、標的型メール攻撃対策技術が進んだのは、2010年以降である。

このような過去の例を踏まえると、①その仕組みの中で、「知らないこと」、すなわち知らないリスクや脅威があることを前提にした設計をすること、あるいは、②知らないリスクや脅威（未知のリスクや脅威）を明らかにしようとする努力、を実践していれば、その分野のセキュリティ技術で先手を打つことができる。

特に、①のような設計は、デザイン思考でも行なわれているように、知らないことを見つけ出すための人間中心の試行錯誤的活動を内包した設計を目指したものであり、知らないリスクや脅威がどのようなものであったとしても、安全・安心を適切に確保できるようなシステムを考えることから始まるものである。

その際、社会を構成する多様な人間の価値観や規範が多様であることを想定しておく必要があるすなわち、対象（物）そのものに関する複雑性や不確実性だけでなく、向き合う人間の側からみたリスクや脅威に対する多義性を意識することが必要である。

その中で、何を削減・回避すべき重大なリスクとみなすか、因果連鎖のうちでどこまで危害や便益として考慮すべき影響範囲とするかは一義的には決まらず、根本的には個人の価値判断に依存する。

このため、合意形成の在り方については、必ずしも一意的なものではなく、リスクや脅威に対する多義性の中で、様々な考え方が共存する可能性がある。

このような、知らない（未知の故障原因も含めてカバーしつつ、知っている（既知の故障原因については、レスポンスの速度を確保するために設計に組み込むといった考え方、さらには、人々の異なる価値観や規範の多様性に起因するリスクの多義性を視野に入れる考え方は、情報通信技術（IT)の急速な進歩の中で、社会が変化し、多様な価値観を承認することにより人々の精神的な欲求までも満たせるようになっていく中で、情報システム、社会、人間を一体として捉え、安全・安心の観点を含めて全体を設計（デザイン）していく上で、活用できる可能性がある。

４．研究・産学官連携の推進方策と産学官エコシステムの構築

概要

第２章で示した基本的な考え方や方法論を踏まえ、本章では、サイバーセキュリティ分野のアカデミックな研究と産学官連携が相互に良い影響を与えながら発展するために重要と考えられる推進方策を示す。

国際的にアカデミックな研究が活発化し、国境や産学官の垣根を超えた共同研究等が行われる中で、我が国の産学官にわたる関係の者や組織において、研究及び産学官連携の推進・振興に係る取組を強化し、研究開発の国際競争力を躍進させる産学官エコシステムの構築を目指すことが重要である。

（１）我が国の研究コミュニティの状況を踏まえた推進方策

① 研究分野の国際動向と特徴

サイバーセキュリティ分野のトップカンファレンスでは、論文投稿が増加し、国境を越えたあるいは産学官の垣根を越えたコラボレーションが活発化している。

その中心として、米国の大学等が長らく非常に高い存在感を示しているが、欧州の大学等がそれに次ぐ存在感を示している。

我が国大学・研究機関の存在感は限定的であるが、採択論文は増加傾向にある。なお、サイバーセキュリティ分野のうち、暗号研究分野では、トップカンファレンスで我が国の一定の高い存在感が認められる。

このアカデミックな研究活動を支える基盤として、米国では、DARPAやIARPA、全米科学財団（NSF）といった様々なファンディング機関が存在し、欧州においても、EUのHorizon 2020が継続的な公募プログラムを運営している。

さらに、人的な面では、欧米では博士課程学生がフルタイムで給料を支払われて、研究グループにとっての貴重な研究戦力になっていることが指摘されているが、これが欧米の旺盛な研究活動の基盤のもう一つの側面となっているものと考えられる。

サイバーセキュリティ研究では、サイバー空間におけるシステムに係る現象・事象を対象とすることが多い。

そして、システムの観測や模擬システムの構築、それらの解析や対策研究において、コンピュータサイエンスを基盤とし、研究行為としてコンピュータを用いたプログラミングやその試行錯誤を中心としたものが多く必要となる点が特徴として挙げられる。

すなわち、柔軟な発想ができ、進展の速い最新の計算機・プログラミング環境を駆使できる、優秀な「人材」が大きく研究を進展させ得る分野と言える。

また、システムに係る研究は、時には研究室を越えて様々な強みを持つ「人材」が連携し組織的に研究を進めることで進展することもある。

研究が構想され、資金が獲得され、その資金を「人」に投入して、研究を進める。研究の中で育った「人」が、さらに学問を発展させ、研究拠点や研究グループを作り、産学官連携を進め、次の研究を構想する。

欧米の動向はもとより、研究分野の特徴を踏まえれば、こういった循環により研究推進を図ることが非常に重要である。本分野の研究コミュニティは、若いコミュニティがゆえ、コミュニティ全体としての発展をこれから模索できる段階にある。この循環構築に向け取り組むことが、エコシステムを駆動する鍵になると考えられる。

② 人に投資すべき

概要

本分野では、研究費を人に投資する、すなわち、研究費を柔軟で優秀な博士課程学生やポスドクに大胆に投入して鍛えるなど、研究を

本分野では、研究費を人に投資する、すなわち、研究費を柔軟で優秀な博士課程学生や求人ラクに大胆に投入して迎え入れ、研究を進展させる観点が重要である。

a.博士課程学生

欧米大学では、博士課程学生が研究プロジェクトの研究戦力になっている。一方で学生の教育や学位取得の厳格さも重要である。

一般的に、博士課程では、近年、アカデミックな研究職のみならず、企業をはじめとする社会の多様な場で活躍する人材の輩出が期待されてきた。

すなわち、アカデミアでは知的価値、社会的価値や経済的価値の基礎となる研究成果を生み出し、産業界ではイノベーション創出の中核を担い、あるいは、産学協働の場では産学にまたがる知識の全体を俯瞰し異分野を融合するリーダーとなる者を育成することが期待されている。

サイバーセキュリティ分野においても、他分野と同様、専門分野の知識や方法論を強みとして身に付けることが基本となるが、上記の人材像を念頭に、一定の種々の実社会経験を通じ、経験の幅に加え俯瞰力と独創力を養うことが重要である。

インターンシップ、企業との共同研究、社会人ドクターとの深いディスカッションの実施等が考えられ、大学と企業が一体となって育成を行うことも考えられる。

その際、サイバーセキュリティ対策につきCSIRT等の現場経験、デジタル技術の活用やDXにつき企業の現場経験など、サイバーセキュリティとデジタル技術の活用の両面から実社会を経験する機会の創出・拡大を図ることが望ましい。

b.リサーチアシスタント

博士課程への進学を検討する者にとって、経済的支援が十分であるかどうかは重要な判断要素である。

情報・セキュリティ系の分野では、研究者が獲得する研究費で研究を進める際、博士課程学生を研究戦力として迎えることで大きく進む研究があり、研究の内容に応じてそうした選択肢を柔軟に選択できることが合理的、かつ、研究分野全体の発展に資すると考えられる。

また、情報・セキュリティ系の分野では、AI等の進展もあり民間企業の給与水準が一般的に高くなっており、優秀な人材を博士課程に迎えるには、現状多く見られる程度の支給額では、現実的な経済的インセンティブが働かないと考えられる。

このため、本分野において、RA経費をはじめとする経済的支援の上限を柔軟に設定・運用できることが非常に重要である。

c.社会人を含む博士課程進学の様々な形態

これまで社会人博士課程に多く見られた例として、企業に在籍したまま企業から給与を受け大学院に進学し、学位を取得し、元の企業で勤続するという形態がある。

そして、今後、本分野で研究者が獲得した研究費を「人」に投入することが進めば、新たな形態となり、様々な選択肢が社会人並びに修士課程からの進学者を含め可能となる。

それは、国・ファンディング機関から獲得する研究プロジェクトや、企業から獲得する産学共同研究費において、申請・立案時にRA経費の上限を柔軟に設定し、その研究期間内に優秀な博士後期課程学生を迎え入れ、標準修業年限を終えるという形態である欧米大学のように研究プロジェクトに係る人材公募を広く行うことも考えられ、博士課程への入学選抜も行われる。

これにより、研究面では、大学側だけでなく企業側も柔軟で優秀な人材を得て研究を大きく進めることができ、人材にとっては、フルタイムでの進学検討のインセンティブとなるような経済的支援が得られ、最先端の研究プロジェクトや産学共同研究への参画で実践的な素養・能力を培って実績を得られるとともに、学位取得につなげられ、キャリアアップの可能性が拓けるというメリットがある 。

これまで我が国では見られなかった形態であるが、可能な研究グループから試みて研究推進と人材育成の幅を広げることにより、次世代にとって魅力的なキャリアパスを形成していくことが重要と考えられる。

なお、推進に当たっては、研究プロジェクトや産学連携への従事と、博士号取得に至る専門性や独創力等の養成をどう両立させるかといった学生の教育の方法論につき研究コミュニティとして議論を深めることが重要と考えられる。

d.次世代にとってのキャリアパスの魅力向上とキャリア形成支援

本節の博士課程に関する推進方策は、進学者や社会人、さらには次世代にとって、博士課程修了後のキャリアアップの可能性を高めるものと考える。

中でも、 a で示した、産学で協働した実社会経験の機会の創出・拡大は、博士課程学生がその後のキャリアをイメージするためにも、学の側が企業等とのネットワークを博士人材へのキャリア形成支援に活かすためにも重要と考えられる。

この一環として、一つの研究室・研究組織に留まらず、産業界を含む研究コミュニティで、広域連携その他の方法により、有志等によりコンソーシアム的に取り組むことが効果的かつ重要と言え、具体の取組が望まれる。

さらに、次世代という観点で言えば、各種の次世代のサイバーセキュリティ人材育成プログラムは、優秀な技術者を育て裾野を広げているが、こういった中からも、アカデミックな研究に興味を持ち、進学・従事・関与する者が益々増えることで我が国の産学官のエコシステムがさらに重層的なものになるといった視点も重要と考えられる。

③ 産学官連携の可能性

概要

a.研究費を人に投入する相応規模の産学共同研究

b.ベンチャー起業

c.共同研究強化のためのガイドライン

④ 研究コミュニティ全体の発展

概要

本分野は、若く伸びている分野として、研究コミュニティ全体としての発展をこれから模索できる良い

段階にあると考えられ、①に示した循環を構築する好機である。

a.ファンディングの活用

国の方針に基づき研究領域等が定められその中で研究者が提案するファンディングでは、国やファンディング機関が行う企画立案に当たり、研究コミュニティの状況や動向をよく踏まえたものとなれば、活発な提案申請がなされやすい。

また、企画立案に当たって研究者を交えたワークショップ等が開催される場合もある。

これらの機会を研究コミュニティ全体として活用し、研究構想を実現し、研究拠点や研究グループを形成していくことが重要である。

そして、ファンディングの企画立案に、研究コミュニティの活力とそこから生み出される研究構想を結び付けていくことが重要と考えられる。

研究コミュニティの発展に向けて、様々な研究構想がなされ、研究提案がなされることが望ましい。

なお、その中で、研究構想が持つべき基本的な特性として、以下が挙げられる。

（研究構想が持つべき基本的な特性として考えられるもの）

□国際通用性

例えば、国際的なカンファレンスで発表する、世界のトップレベルと交流する、世界と渡り合える研究グループが育つもの。

□人材育成

例えば、次の世代を担う博士号取得者が 育つもの。

□次につながる

例えば、産業界や投資家に出口戦略が見え、大きな関心が示され、共同研究やベンチャー起業を複層的に生み出すもの。重点的な研究開発プロジェクト（国プロ）に発展し得るような研究成果を複層的に生み出すもの。

研究コミュニティの発展において、研究拠点の形成は、象徴的な意味合いを持つ重要な取組となる。

我が国の国際的な顔となり、次世代にアピールし、「人」が集まって流動し、研究構想や産学共同研究を複層的に生むベースとなる。

その形態としては、サイバー空間を対象としているという特徴を活かして、PIを結ぶネットワーク型の拠点形成と一定のPIが集まる物理的な拠点形成のハイブリッド型の形成などが考えられよう。

また、大学だけでなく公的研究機関が関与する形態も構想され得ると考えられる。

b.科学的基礎の構築

本分野は、急速に発展している若い分野であり、いわゆる統一的な理論や定番的な教科書といったものが現時点で存在するわけではないが、科学的基礎に基づくセキュリティ対策への需要は広がる一方と考えられる。

現在の内外のセキュリティ対策において、科学的に確立され十分に理解された解決策は、分野・領域や文脈に特有のものが多いと考えられる。また、数学的及び実証的な妥当性が十分に検証されておらず、有効性や効率性が考慮されていない場合もあると考えられる。

このような対症療法的で発見的（ヒューリスティック）な手法は、進化する技術や変化する脅威や攻撃に対して、信頼できるシステムを維持するためには不十分・不完全で、重要な脆弱性を見落とし得ると言える。このため、引き続き、科学的基礎を構築していくことが重要である。

また、研究コミュニティにとって、様々な応用的な他分野・実社会との接点が拡大することが想定され、これら他分野・実社会から、本分野のアカデミックな研究と協働することで何が期待できるか、科学的手法が提供できる価値の中心的な概念は何か、理解してもらう必要性は高まろう。

このため、これまで培われ、共有され、発展してきた科学的基礎に係る概念を言語化する作業を以下の通り行った。

これについては新たな知見や学問の発展等とともに見直されるものである。また、この科学的基礎自体について、その確立・構築・発展を目指して取り組む理論的な研究はさらに重要になってくると考えられる。

（サイバーセキュリティ研究の科学的基礎）

1.システムを評価する際において、
脅威を定量的に測定する方法、セキュリティを測定可能な形で保証する方法、防御機構と攻撃者を効果的・効率的に評価する方法

2.セキュアなシステムを設計する際において、システムが満たすべきセキュリティの特性と効果を証明可能あるいは定量的に検証可能とする方法

3.破壊的イノベーションなど新たに生まれるテクノロジーや急激に変化する攻撃者によって生じ得る脅威を予見する、あるいは未然に防ぐ方法

4.社会で用いられるシステムにおけるセキュリティ・セーフティ・プライバシーに関する、個人・組織・社会の要求、期待及び行動原理を理解するための理論とモデル

以上の方法は、いずれも科学的な手法に基づき記述され、客観的に再現性がある形で実行されるべきである。

c.プロシーディング論文を含む柔軟な研究実績の評価

研究者の研究実績として評価されるものとして、論文誌（ジャーナル）での論文成果（ジャーナル論文）と研究集会（カンファレンス）での論文成果（プロシーディング論文）が挙げられるが、後者が評価されにくい場合があるとの指摘がある。

プロシーディング論文は、査読・フィードバック・掲載が迅速であることから、研究の進展が速い情報・セキュリティ系の研究分野において馴染みが深く、中でも査読付きで評価の高いものは、国際通用性のある研究実績とされることが

系の研究分野において論文の分量が少なく、中でも査読付きで評価の高いものは、国際通用性のある研究実績とされることが多い。

実際、海外ではトップ級のカンファレンスでの論文成果が評価され、近年は日本からも重要なカンファレンスに採択されるプロシーディング論文が増えてきている。

一方、その重要性は、他分野の研究コミュニティからは必ずしも理解されにくい。

研究費の申請書においても、研究実績はジャーナル論文であることが前提であるかのように誤解し得る記入例が示されている事例が存在する。

特に情報・セキュリティ系の分野では、査読付きで研究コミュニティ内でも評価の高いプロシーディング論文が研究業績として適切に認められることが、研究者にとって、さらには当該分野の発展にとって、極めて重要である。

また、その評価のあり方が分野の内外に伝わるよう、積極的に発信する必要がある。

このため、事業の特性を踏まえつつ、情報・セキュリティ系の研究分野では、ファンディング機関等における研究費申請書において、プロシーディング論文も研究実績に含まれる旨を明確化すべきである。

d.国際交流・国際展開

研究コミュニティ全体が発展していく上で、世界の産学官ネットワークの一角に位置付けられ、存在感を示して発展につなげる観点、また、世界の知を取り込み、国際競争力を強化する観点から、研究者や研究機関の国際交流・国際展開を活発に行うことが非常に重要である。

このため、海外での武者修行を含めた国際的に活躍する若手研究者の育成や国際共同研究の振興に取り組む。国際関係の支援制度の活用が期待されるほか、各研究機関における留学制度等の独自の取組や公的な留学制度の活用も奨励される。

中でも、我が国と相手国のファンディング機関で国際共同研究の共同公募（ジョイントコール）や共同支援が連携して行われる制度は、両国連携のワークショップ等が開催され交流の機会が拡大し得るほか、相手国の共同研究者に当該国側から研究費が措置されるため、相手のインセンティブやモチベーションが高い中で共同研究が推進できる。

積極的な活用が期待されるとともに、このようなファンディングの企画立案にも、研究コミュニティの活力と研究構想を結び付けていくことが重要である。

さらに、国際的なカンファレンスのプログラム委員や実行委員等の運営側への就任は、論文採択を含めた存在感の向上、意義あるカンファレンス等の我が国への招致、国際的な研究動向等に相通じた我が国研究コミュニティの発展と世界的な貢献にとって重要である。

今後、これらのプログラム委員や実行委員等を増やす努力を行うとともに、研究コミュニティ全体として努力を適切に評価しこれらの委員を支援していくことが重要である。

e.最先端の研究活動のための取組

前例のない先進的なサイバーセキュリティ研究を推進するためには、社会に受容されるような倫理的配慮が必要となる。

しかし、倫理的配慮の名の下に先進的研究をストップさせるような圧力になることは避けるべきである。

先進的研究を「萎縮させない」ためにも、各組織の経営層を含め、様々な議論や活動を通じて理解が醸成され、適切な倫理的配慮を実施する土壌が広がることが望まれる。

また、2020年からの新型コロナウイルス感染症の影響により、研究活動においても制約が生じているが、オンラインによる地理的な制約を超えたコミュニケーションが一般的かつ容易になった面があり、研究コミュニティの発展につながる活動において一定の可能性を広げていると言える。

オンライン活用のさらなる工夫により、最先端の研究活動を模索することも望まれる。

2 （２）我が国の強み・ポテンシャルと重点的な強化に向けて

概要

我が国の本分野の研究競争力を高め、国際的な存在感を増し、産学官のプレーヤーとのコラボレーション等を通じてサイバーセキュリティに係る知見の増大と技術革新を生んでいくためには、アカデミックな研究の重点的な強化が欠かせない。

それには、知的価値及び社会的価値・経済的価値への寄与が大きいと考えられるとともに、研究コミュニティの発展可能性を高め、様々な研究構想や研究提案がなされ、「人」が育ち、研究拠点や研究グループが作られていくような研究領域を見出し、研究コミュニティの自主的な発展努力と相まって重点的な強化が図られることが重要である。

① 我が国の強みとポテンシャル

上記研究領域を見出すため、まずは我が国の現在の国際的な立ち位置に基づく強みとポテンシャルを踏まえることが重要である。

分析を行った結果、ほとんどの領域で米国あるいは米欧が強いが、IoTセキュリティ研究領域や、データセキュリティ及びプライバシー保護研究領域など、米欧に比肩する領域があり、国際的な受賞など我が国の顕著な活動・成果が見えている領域や我が国が上昇傾向にある領域が存在する。

一方、我が国の研究コミュニティの特性や、社会や産業等の特性を考慮して、ポテンシャルとしての我が国の強みには、以下が挙げられると考えられる。

（ポテンシャルとしての我が国の強み）

□IoTや自動車など実空間技術とサイバーとの融合領域（Society5.0）は、我が国として強みかつ力を入れるため、そのセキュリティを研究する、IoTセキュリティ研究領域や自動車セキュリティ研究領域といったサイバーフィジカルシステム（CPS）に係るセキュリティは、日本の強みとなるポテンシャルがある。

□我が国の暗号研究は国際的に見ても強みを有しており、暗号研究の強みを活かしたセキュリティ評価・リスク評価研究領域（システムのセキュリティ設計やセキュリティ分析に係るもの）や、データセキュリティ及びプライバシー保護研究領域（個人データの利活用を促進するための加工技術に係るデータ保護（匿名化技術）・秘密計算（マルチパーテ

ィ計算など））などは、日本の強みとなるポテンシャルがある。

□セキュリティ製品やシステムの品質や実運用への配慮にも現れる細やかさは、我が国の社会や産業等の特性の一つと考えられ、その基盤を支え、フィードバックが得られる可能性がある人的要素セキュリティ研究領域は、日本の強みとなるポテンシャルがある。

② 重点的な研究領域

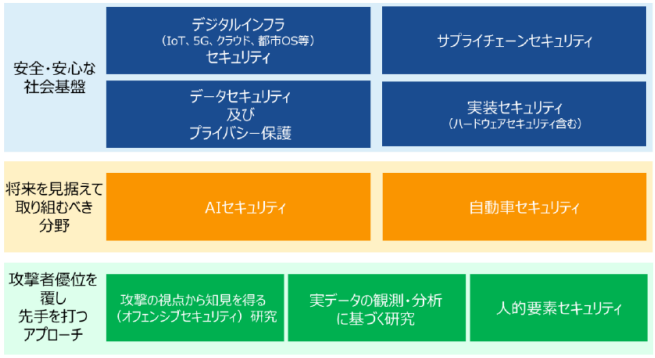
上記の強みとポテンシャルを踏まえ、知的価値及び社会的価値・経済的価値への寄与が大きいと考えられる研究領域は以下の通りである。

（現状では強みが必ずしも認められないもののポテンシャルや価値への寄与が大きい研究領域、強み分析の個々の研究領域に当てはまらないものの横断的な手法・アプローチとして重点的な振興が重要と考えられる研究も含め、三つの観点からグループに分け整理している。）

我が国のアカデミックな研究の強化に向けて、当面、これら研究領域を念頭に、研究コミュニティの自主的な発展努力と相まって重点的な強化が図られることが望ましいと考える。もちろん、暗号研究分野の継続的な振興と国際的存在感の維持・向上、実践的なサイバーセキュリティ研究との相互発展も極めて重要である。

なお、科学研究費助成事業等による研究者の自由な発想に基づく研究は、発想・学理・シーズの源泉として極めて重要であり、これら研究領域に限らず、個々の研究者の自由な発想に基づき、引き続き推進されるべきものである。

さらに、科学的基礎の確立・構築・発展に取り組む理論的な研究が今後益々重要性を増すと考えられる。



（図３）重点的な研究領域

2 （３）研究コミュニティの継続的な取組

本分野の研究コミュニティは若いコミュニティであり、コミュニティ全体の発展に向けた道筋を大胆に模索できる点にアドバンテージがある。

研究コミュニティとしての取組が、中長期的視点や国際的視点を持ちつつ、様々な面で開始され、拡大され、継続されること、また、国や公的機関、さらには産業界による研究及び産学官連携の推進・振興の取組が研究コミュニティの取組と相まって相乗効果をもたらすことが重要である。

研究コミュニティとしての議論・意見交換が持続的になされていくこと、そして本章に示す推進方策の実施と成功により、研究を担う博士課程学生、及びアカデミックな研究に従事する若手研究者が増え、また様々な場で研究構想や産学共同研究構想が提案され、我が国の産学官のエコシステムが重層的なものになること、さらにその結果として研究開発の国際競争力が大いに躍進することが期待される。

1 ５．まとめ

・サイバーセキュリティの研究開発において多様な価値観を持つ人間の思いが実現でき、人間が安心して暮らすことのできる社会システムを創造していくことを前提として、イノベーションを起こし、国際競争力の強化等を図っていくためには、近い将来と中長期的な社会・経済と情報通信技術（IT)の利活用の進化を視野に入れることが重要である。

・基本的な考え方として、近い将来においては、後追い的なサイバーセキュリティだけでは対処が困難な可能性があり、視野を広げてサイバーセキュリティ対策を捉え、研究開発に取り組んでいくことが期待されることを示した。

・また、中長期的な視点においては、アウトソーシングする時代から、創造的に生活する個々人の時代へと回帰し、自分の生活を創意工夫して自己実現を図り、それを生活者同士で共有することによって、さらなる創造や共創が可能となるような時代へと変化する可能性を示唆し、サイバーセキュリティ研究の広がり（「情報システム」だけでなく、「社会」や「人間」を一体として捉えた新たなテーマ・未知のテーマの発見がもたらす将来の可能性を示した。

そして、サイバー空間がもたらす、これまでとは全く異なる段階（人間と人間との関係、人間と社会との関係の変化、自己の概念の曖昧化といった人間のあらゆる側面が関わってくるような段階）に対応できるような人間観や世界観・倫理を生み出していくこと が 重要で あることを示した。

・今後、こうした考え方について、これまでのサイバーセキュリティ技術の専門分野にとどまらず、人文社会科学も含めた国内外の幅広い分野における研究組織や研究者に対し発信し、普及啓発活動に取り組むこととする。

総合科学技術・イノベーション会議やIT総合戦略本部等における取り組みとの連携を図りつつ、内閣サイバーセキュリティセンターNISC）を中心に、我が国のサイバーセキュリティに関連する研究開発の状況について把握に努め、本戦略の内容について、フォローアップを行うこととする。

併せて、NISC及び関係府省庁の連携の下、具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討することとする。

・最後に、本戦略が我が国の研究機関・組織におけるサイバーセキュリティの研究開発について議論・検討を行う上で活用され、我が国の強みを活かしたイノベーションが実現し、各研究組織における取り組みがグローバルなサイバーセキュリティの向上に貢献できることを期待する。