資料20－3

今後重点的に取り組むべき研究開発課題について

サイバーセキュリティタスクフォース事務局

令和２年１月27日

有識者ヒアリングについて

サイバーセキュリティ分野において、今後約５年間で重点的に取り組むべき研究開発課題の方向性について、有識者ヒアリングを実施。

✓期間：　令和元年10月～令和２年１月

✓ヒアリング対象：　民間企業・研究機関・大学等におけるサイバーセキュリティ分野の研究者・技術者等約20名

ヒアリング結果について、次ページ以降に概要を示す。

AI（１）

① AIへの攻撃に関し、 特に敵対的サンプル攻撃等に対処することが必要。
② AIを活用したセキュリティ対策については、攻撃の自動化に対応するため、防御側も、自動化が必要。
③ 攻撃側と防御側についてAI同士で戦わせ、将来の攻撃を見据えるなど防御側の能力を高めることが重要。
④ AIに防御の判断を全て任せるのは今後5年程度では困難。最終判断は人間が行い、その判断のための情報を集めるIA（Intelligent Assistance）が重要。

AIとセキュリティ

(1) AIとセキュリティは、①Attack using AI（AIを利用した攻撃）、②Attack by AI（AI自身による自律的な攻撃）、③Attack to AI（AIへの攻撃）、④Measure using AI（AIを利用した対策）の4つの観点がある。それぞれ深めるのも大事であるが、組み合わせることで研究が深まる。

Security for AI

(1) AIへの攻撃については、①学習データの偏在・不正による意図的な不正、②データを入出力させることによる情報漏洩やプライバシー上の問題の発生、③AIの検討プロセスがブラックボックスであることによる、結果に対する説明性の困難さ、の課題がある。本当にAIのエンジンが大丈夫であると保証して、実際AIを使う人が安心して利用できるような仕組みが必要。

(2) AIそのもののセキュリティをどのように守るのかが喫緊の課題。①AIに対して雑音を加えて性能を狂わせる攻撃をどう防ぐか、②異常となったAIをどのように元に戻すか、どのように駆除するのか、について、取り組む必要がある。敵対的サンプル攻撃等に対処するため、防御側も機械学習やAIの専門知識を持って、理論的に立ち向かう必要がある。セキュリティの専門家だけでなく、AIの専門家をセキュリティ分野に巻き込むことが重要。

AI（２）

(3) AIへの攻撃は、データポイゾニング、敵対的サンプル攻撃、情報漏洩の3つに分けられる。
① データポイゾニングは、サプライチェーンリスクにも関連する可能性がある。
② 敵対的サンプル攻撃は、どのような対抗措置をするかということも含めて、セキュリティの学会やAIの学会でも旬な課題。
③ 情報漏洩（Model inversion攻撃）の問題は、これから大きな課題になると想定される。

(4) 自動運転時代の事故対応について、フォレンジックが複雑になると考える。現在はドライバーの証言で対応しているが、AIがその時何を考えていたか、そのログが電子的に残っているのか、改ざんされていないかが問われることが考えられる。その解決策として、電子署名をうまく使って、タイムスタンプ署名と組み合わせて何時何分はこのログだった、とハッシュ値を取ることが考えられるが、信用できるデバイスを車中に置く必要があり、その仕組みについての研究開発があり得ると考える。

AI（3）

AI for Security

(1) AIを利用したセキュリティ対策について、セキュリティ対策は囲碁や将棋のようにルールが明確でないため、難しいかもしれないが、それを意識したサイバーレンジを構築し、攻撃側と防御側のプログラムを入れてシミュレーションさせ、強化学習により防御側を賢くしていくことの可能性が考えられる。また、AIを含めた安全性を確保するためのソフトウェア工学は一つの研究課題。AIが変な挙動をしたとしても、そうしたリスクを低くするためにどうすれば良いかというリスク評価の研究が必要。ベースとなるのはリスクコミュニケーション。

(2) AIを使って、実システムの脆弱性を自動的に見つけて、自動的に攻撃するツールが作り出される可能性がある。防御側として、攻撃してくるAIからシステムを守るAIを作る技術開発が必要。このため、攻撃するAIと防御するAIを作って戦わせる手法が考えられる。

(3) シミュレーション環境を構築し、AI同士で戦わせながら、先の攻撃を見据えていく、人間では発見できないものをAIで見つけるというところが、今継続して取り組むべき一番の課題。

(4) 今後5年間で、AIに全ての判断を任せるというのは困難で、最終判断は人間が行い、その判断のための情報を集めるIA（Intelligent Assistance）が重要になる。

(5) マルウェアは、人手で行っていた攻撃を自動化したものともいえる。マルウェアに対抗するために、防御側の自動化、すなわちセキュリティ対策の自動化が必要。

(6) 今のマルウェアは、人間が見つけた脆弱性を利用して、感染させる機能をプログラミングしているが、今後のマルウェアは自分で脆弱性を見つけていき、それに合うように自分でプログラミングして感染を広げていくようになる。マルウェア自体は昔からAIと言われており、人間には止められなくなるだろう。マルウェアの研究は続けていく必要がある。

(7) サイバーセキュリティの分析官の知識をどうAIに持って行くかを検討し続けることが必要。

データ利活用

① サイバー攻撃分析のための実践的なプラットフォームが必要。
② 攻撃の手口に大きな変化はないが、攻撃の対象が拡がることから、サイバー空間における事象を観測し続け、新たな観測手法を開発するとともに、サイバー攻撃情報等を継続的に収集・分析することが重要。

データ利活用

(1) サイバー戦争時代の到来を想定し、被攻撃環境を巧みに構築し、検体の振る舞いを調べたり実践的なインシデントレスポンスを体験できる環境の構築が重要。NICTのSTARDUSTについて、例えば大学と連携させ、大学CSIRTが運用としてSTARDUSTを活用することで、実際に何が起きるのか経験できる人材育成の場として、よりオープンな形で維持・活用していける仕組みを検討すべき。

(2) 今後サイバー攻撃の対象となる機器が益々拡大することから、脆弱性情報の収集・分析について、継続して取り組むべき。

(3) 脅威情報データの収集を民間のみに任せた場合、対価を支払えない者は当該データがセキュリティ対策に使用できなくなるとともに、データソースや活用方法が明らかにされないおそれもある。また、脅威情報データは、国の政策判断にも必要となる。このため、国立研究開発法人のような中立的な機関が脅威情報データを継続的に収集することが重要。また、今後は、収集した膨大なデータを効率的かつタイムリーに分析するため、リアルタイムで定常稼働する機械学習エンジンを開発していくことが重要。

(4) 5～10年前はサイバー攻撃の対象はWindowsだったが、NICTERでも観測されているとおり、昨今ではサイバー攻撃の対象がIoT機器に拡がってきている。5～10年後は、更に小型デバイスや一般ユーザがコンピュータとは想定していないものに拡がっていく。一方で、攻撃手法自体は過去から現在において大きく進化していない。そうした状況において、サイバー空間における事象を観測し続ける仕組みを維持し、攻撃対象が変化したときに、新しい目（観測手法）を作ることが必要。

暗号

① CRYPTRECをはじめとして、日本における暗号研究のレベルは高く、今後も世界における優位性を保つため、取組を強化すべき。
② 耐量子計算機暗号については、安全性評価、高速・小型化実装に注力すべき。
③ 秘密計算技術については、安全なデータ流通の核となる技術。現状、国際的に横一線の状態であり、日本としてもしっかり取り組むべき。

暗号

(1) 日本のCRYPTRECは信頼されていて、レベルは高いと思う。現在、日本は世界に後れは取っていないが、後れを取ることで、中国や米国のものしか使えなくなると非常にデメリットが大きく、暗号の研究は、今後も続けていくべき。

(2) 量子コンピュータ時代の安全な暗号としては、量子暗号及び耐量子計算機暗号（PQC：Post Quantum Cryptography）がある。耐量子計算機暗号を考えるに当たって、要素となるのは、①安全性評価、②高速・小型化実装、③標準化、④新暗号の設計の4つ。

→ ①の安全性評価は、日本が力を持っている分野であり、今後とも世界における優位性を保つためCRYPTRECにおける取組を強化すべき。

→ PQCは、現在の公開鍵暗号に比べ、サイズや必要なメモリが大きいことが課題であり、IoT機器やスマホ等に実装するためには、②の高速・小型実装化の技術開発が必要。

(3) クラウドで使うことが想定される準同型暗号（暗号化したまま計算できる技術）は、今まで計算量が多く処理速度が実用レベルではなかったが、格子暗号の利用やペアリング暗号の利用等により実用化が見えてきた。NICT等は研究を引っ張っている組織であり、研究を更に促進することが重要。

(4) 秘密計算は、データのセキュリティやプライバシーを保護したまま、安全なデータ流通と利活用を実現する技術であり、例えば、複数の医療機関が保有する医療データを暗号化したまま解析したり、複数のクレジットカード会社のデータを互いに開示することなく深層学習により不正取引を検出するなど、幅広い応用が期待できる。国際的に各国横一線の状態であり、世界的にも重要技術であるので、日本はしっかり取り組んでいくべき。

その他（１）

① サプライチェーンリスクの観点から、ハードウェア・ソフトウェアそれぞれについて信頼性を確保するための取組の強化が必須。
② データ駆動型社会の進展に伴い、管理コストの観点等からクラウド化が本格的に進むなか、クラウドのセキュリティについて重点的に取り組むことが重要。

サプライチェーンセキュリティ

(1) ハードウェアのセキュリティについては、チップの中に悪意のあるコード等が仕掛けられていたときに、それに対抗するにはどうするか、というのが課題であり、研究開発を進めるべき。

(2) 5Gのセキュリティの中でも問題になってきているのがオープンソースソフトウェアの扱い。今まで以上にモジュールごとに分かれてものが作られているので、サプライチェーンの問題もある。6Gになったときにアーキテクチャがどんどん変わってもっとオープンになってしまうと、そのポーションごとのセキュリティの観点を考える必要が生じる。

(3) 5Gのエッジサーバは高度な機能を持っているため、物理的なセキュリティも含め、対策が必要。

(4) サプライチェーンの中では、仕様設計の時点、コンパイルする段階、コンパイルされた後のバイナリ等、どこで悪意が混入するかわからない。それぞれの段階でセキュリティを確保していく必要があるが、コストに見合うか、バランスを考えなければならない。ソフトウェア工学に近い話で、例えば仕様書の中の意図を解析するのであれば、セキュリティというより意図解析、自然言語理解のような話になる。セキュリティとソフトウェア工学と心理学、犯罪心理学などの、融合領域・学際領域になるかもしれない。

(5) 色々なものが汎用機器とソフトという形（センサーであれば、Linuxとソフトウェア）になるため、ソフトウェアの信頼性についてさらに強化して見ていくことが重要。

その他（２）

クラウド

(1) データ社会の進展に伴い、個者によるデータ管理コストが増加する中、GAFA等のクラウドサービスを使うことが増えてきている。以前より、クラウドの安全性については議論され、ガイドラインも策定されているが、必ずしもセキュリティを担保できているのか明らかでは無い。安全性を保証できる仕組みを作る必要がある。

(2) ①小さなプラグインやアプリケーションはセキュリティ保証がなく、無審査で行われており、また、②プラグインやアプリケーションの提供元が買収されることにより、製品の性格が突然変わったり、悪意あるものとなることもある。例えば、プラグインにはドキュメントの情報が全部行く場合があり、気づかない内に機密情報が流れてしまう可能性がある。こうしたNo intrusion attack（侵入しない攻撃）は、従来のセキュリティ対策では止められないと思われる。プラグインやクラウドの認証鍵への攻撃が今後の課題になると想定される。

その他（３）

その他

(1) サイバー攻撃による影響を完全に防ぐことは困難。マルウェア等の無害化技術は今後ますます重要となり、研究開発を進めるべき。

(2) 標的型攻撃やハードウェアトロイなど攻撃者の情報が得にくいタイプのサイバー攻撃については、攻撃者に先回りして対策を検討する意味でも攻撃研究（対策側が攻撃側の観点で思考し、様々な攻撃を想定しながら対策を検討する）が必要となる。但し、研究の実施方法や研究結果の発表方法には、十分に注意すべきである。

(3) Safety、Security、Reliability、Privacy、Resilienceの5つをまとめてTrustworthinessと呼んでいる。今後AI、IoTのセキュリティ、安全性はTrustworthinessの方に行くのではないか。そういうものをベースにしたリスク評価ができるようにする必要がある。そこにはファストフォレンジックやライブフォレンジックも関係する。

(4) AIスピーカのように、新しいデバイスが出てくることにより、セキュリティのあるべき姿も変わると思われる。例えば、画面が無いデバイスが普通となったときに、どのように異常をユーザーに伝えるのか。セキュリティの観点からのユーザインターフェースについても検討すべき。

(5) 脅威に対抗するために、In-Vehicle、車の内部のセキュリティ対策、ファイアーウォールの設置等進んできているが、車の外部通信（ネットワークやサービスをつなぐクラウド）に係るセキュリティ対策も検討しないといけない。

(6) コネクテッドカーの通信部分におけるセキュリティ検証技術が未確立であり、通信機器のセキュリティ検証体制が必要。

(7) LPWA（Low Power Wide Area）では、非IP・標準化されていないプロトコルが使われており、セキュリティについて検討すべきではないか。

その他（４）

研究環境

(1) 大学にセキュリティの学部なり学科を作り、基礎的なことからきちんと教育することが必要。現状はこうした取組がほとんどなく、（年間数千人レベルを目標に）もう少し増やしてもいいのではないか。

(2) サイバーセキュリティ分野では実データを触る機会を増やさなければ実フィールドにあった研究ができず、そうした環境を構築すべき。

(3) NICTのリソースをICT-ISAC等の分析を必要とする組織が手軽に使える環境があるとよい。例えば、NICTの「みんなの自動翻訳」は良い事例。ログなどの観測データについて、NICTのAIエンジンで機械的な分析を行い、その結果をデータ入力者は入手する、NICTはそのデータを研究に使っても良い、といった仕組みを作ることができると良い。

(4) 現在NICTでは、機構内に約20個のセキュリティ機器を並べたセキュリティ技術のテストベッドを構築しており、NICTのCSIRTチームが使い勝手についてレポートをまとめている。人的リソースの観点から正式な体制とはなっていないが、長期運用が可能であり、うまく仕組み化できると国産セキュリティ技術の検証環境として活用できる。

(5) DevOps（Development and Operation）という、開発担当者と運用担当者が連携・協力したソフトウェア開発手法のセキュリティ版であるDevSecOpsの環境をNICTに構築しており、有効に機能しているため、こうした活動の更なる強化が重要。

(6) 信頼のある自由なデータ流通が実現できる、国際間連携、データ利活用の環境の構築が必要。

(7) 暗号技術の研究については、民間単独で取り組んでも少人数で勉強から始めることとなってしまう。国プロのような形で実施すれば、旗を振る大学の先生が中心にいて、その周りに民間含め人が集まり、学びあい、サイクルが回って、人が育つ。量子コンピュータ時代の様々なビジネスを担う人材となり、日本の競争力強化につながる。

(8) 暗号の世界は、物品の購入等では無く、人が大事。例えばNICTに人が集まる仕組みやそこで協力できる場を作り出すことが重要。

その他（５）

人材育成

(1) セキュリティ人材が7万人足りないと以前から言われているが、人材として投入された時に企業が全員雇えるのか疑問。また、セキュリティ業務をAIでどれくらい代替できるのかを考えなければ、人材を育成してできあがった時にはその業務はAIでほとんど置き換えられている可能性がある。AIをセキュリティ対策のどの部分に取り入れるのかを加味した上で人材育成を考える必要がある。

(2) 研究機関の教育の在り方としては、コアとしてこれだけ押さえないといけないという最小セットを切る必要がある。あるいはここまでやれば超エキスパート、のような認証制度も必要。CISSP（セキュリティプロフェッショナル認定資格制度）のように国際的に認知される制度が、日本発でもできれば良い。

(3) SOCの人材育成ができるところがない。人材育成を進めるためには、自前でのSOCの環境が必要となるが、日本は大体の企業がSOCを外注している。

(4) SecHack365の修了生がセキュリティ関係に継続して携われるよう、こうした人材に投資してはどうか。その際、芽が出るのは1割と目標設定することもありえる。大企業向けの大型案件10件より、イノベーティブな人に小規模でも100件取り組んでもらうことで、人材育成を図ることができる。企業と組み、マッチングを図ることも一案。

(5) 若手人材を育てるプログラムは多数提供されつつある。SecHack365について、5-10年の実務経験者向けのコースを新設し、一定期間企業等で経験を積み、特定の分野で技術力を身につけた者がセキュリティの能力を伸ばせる機会を提供してはどうか。

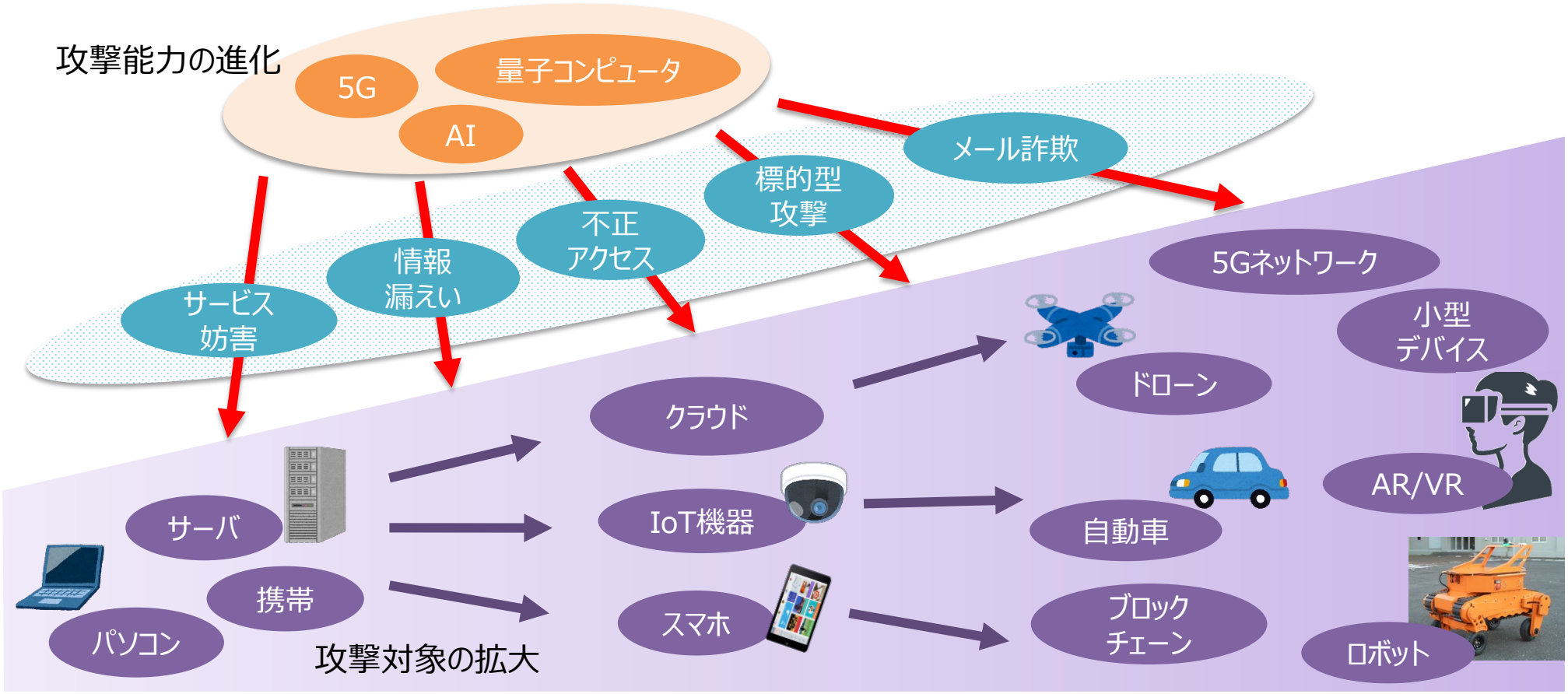
(6) 企業におけるインシデント発生時に、マルウェア解析をセキュリティ事業者に頼むと1検体何十万、何百万とかかる。本解析を、研究対象にして良いとの前提のもと、NICTや大学の研究者に解析を依頼する仕組みがあっても良いのではないか。

有識者ヒアリングを踏まえた方向性案（１）

今後のサイバー攻撃・脅威動向

① 今後、クラウドの普及や、インターネットに接続される機器の更なる増加に伴い、攻撃対象の拡大が想定される。ほとんどの機器がソフトウェアで制御されるようになり、サプライチェーンリスクも増大する。

② 攻撃の手口については従来から大きな変化はないと想定される。一方で、AIの進展等に伴い、攻撃手法・能力は複雑化・巧妙化・大規模化していく。



有識者ヒアリングを踏まえた方向性案（２）

今後重点的に取り組むべき研究開発の方向性案

① サイバー攻撃対象の拡大等に伴い、サイバー攻撃に関するデータが膨大となり、データの高効率・有効活用がより重要になってきている。

（研究開発の方向性）

膨大なデータについて、観測・可視化・分析する技術の更なる高度化を図ることで、サイバー攻撃に対し適時適切に対処出来る環境を構築すべきではないか。また、こうしたサイバー攻撃情報や脅威情報等を集約し、セキュリティ検証を行ったり、人材育成にも活用できるサイバーセキュリティ統合テストベッドの構築が必要ではないか。

（課題）

NICTで研究開発を進めているNICTERやCUREが中核的な役割を果たすことが想定されるが、これらの環境について、よりオープンかつ簡易な方式で研究機関等が活用出来るようにするために、どのようなリソースや運用方法が必要となるか。

② 機械学習の活用等によるサイバーセキュリティ対策の一部自動化が進みつつあるが、サイバー攻撃において自動化が更に進展するなか、防御側についても、高度な自動化が必要となってきている。

（研究開発の方向性）

防御側についてもAIの活用等により高度な自動化を進めるとともに、将来的には、攻撃側と防御側についてAI同士で戦わせ、AIの研究者も交えつつ防御側の能力を高めていくことも重要でないか。

（課題）

AIによる攻撃等の高度なサイバー攻撃に対処出来る能力を高めるための攻撃手法の研究開発に関して必要とされる研究環境について、どのように構築し、運用することが望ましいか。

有識者ヒアリングを踏まえた方向性案（３）

③ マルウェアの高機能化、攻撃の巧妙化等により、従来の技術（ハニーポット等）ではその振る舞いを調べ対処に役立てることが難しくなってきている。

（研究開発の方向性）

サイバー攻撃に対する実践的な対応能力の底上げを図るため、被攻撃環境を巧みに構築し、検体の振る舞いを調べたり実践的なインシデントレスポンスを体験できる環境の構築を進めるべきではないか。サイバー攻撃による影響を完全に防ぐことは困難であり、マルウェア等の無害化技術に積極的に取り組んでいくべきではないか。また攻撃者の視点で考え、先回りして攻撃を予測し、対策を事前に講じる技術について研究を行うべきではないか。

（課題）

研究者が安心して検体の振る舞いを調べたり、模擬的な攻撃を通じて高度な研究を進めたりするために、どのような環境を構築すべきか。

④ 技術の進歩に伴い、サイバー攻撃の対象がコネクテッドデバイス等の従来想定していなかったものにも拡がるとともに、５G等の進展によりサプライチェーンリスクも高まっている。また、データ駆動型社会の進展に伴い、管理コストの観点等からクラウド化が本格的に進んできている。

（研究開発の方向性）

安心して新技術の恩恵を享受できるよう、次世代ネットワークやコネクテッドデバイス等のセキュリティ検証技術の開発や、ハードウェア・ソフトウェアの両面から、信頼性を確保するための取組を重点的に進めていくことが必要ではないか。クラウド上のデータの安全性や信頼性の担保を含む、クラウドのセキュリティについても本格的に取り組むべきではないか。

（課題）

サプライチェーンリスクやクラウドのセキュリティに関し、技術が急速に進展し、また、多様な主体が関与する中で、対処すべき事項をどのように抽出するか。また、研究開発課題が多岐に渡ることが想定される中で、産官学の役割分担はどのようにあるべきか。

有識者ヒアリングを踏まえた方向性案（４）

⑤ 暗号研究分野については、採算が取れない等の理由から、企業による取り組みが縮小されつつある一方、耐量子計算機暗号や秘密計算技術については、世界的にも研究途上であるものの進展が見込まれる分野である。

（研究開発の方向性）

今後、日本が世界をリード出来る可能性のある耐量子計算機暗号については、特に日本が強みを有する安全性評価、高速・小型化実装に注力すべきではないか。また、秘密計算技術については、安全なデータ流通の核となる技術であり、様々な分野での応用が期待されている。日本が強みを有する分野であり、取組をより強化していくべきではないか。

（課題）

暗号分野は、物品購入等ではなく人が資産であり、一社単独では人材育成が困難であることから、人が集まる仕組みやそこで協力できる場が必要ではないか。その構築のために、具体的にどのような方策が必要か。

⑥ 優れた若手セキュリティ人材が、必ずしもセキュリティ分野に携わり続けられている状況ではない。また企業等で実務経験を積んだ者が、高度なセキュリティ研修を受けられる機会が限られている。

（方向性）

SecHack365の修了生等の若手人材に対し、研修等の終了後も一定期間研究を続けられる環境を何らかの形で提供出来ないか。また、学生等の若手だけではなく、一定期間企業等で実務経験を積み、特定の分野で技術力を身につけた者が、セキュリティの能力を伸ばせる機会についても、検討してもよいのではないか。