提案３

（案）

報告

社会の発展と安全・安心を支える情報基盤の普及に向けて

平成２９年（２０１７年）〇月〇日
日　本　学　術　会　議
情報学委員会
安全・安心社会と情報技術分科会

この報告は、日本学術会議情報学委員会安全・安心社会と情報技術分科会の審議結果を取りまとめ、公表するものである。

日本学術会議情報学委員会安全･安心社会と情報技術分科会

委員長	柴山　悦哉	（第三部会員）	東京大学情報基盤センター教授
副委員長	坂井　修一	（連携会員）	東京大学大学院情報理工学研究科教授
幹　事	高田　広章	（連携会員）	名古屋大学教授
幹　事	宮地　充子	（連携会員）	大阪大学大学院工学研究科教授
	安浦　寛人	（第三部会員）	九州大学理事・副学長
	阿草　清滋	（連携会員）	南山大学理工学部ソフトウェア工学科教授
	井上　美智子	（連携会員）	奈良先端科学技術大学院大学情報学研究科教授
	今井　秀樹	（連携会員）	東京大学名誉教授
	岩田　誠	（連携会員）	高知工科大学情報学群教授
	岩野　和生	（連携会員）	三菱商事株式会社ビジネスサービス部門顧問
	菊野　亨	（連携会員）	大阪学院大学情報学部教授
	後藤　滋樹	（連携会員）	早稲田大学理工学術院基幹理工学部情報理工学科教授
	小林　広明	（連携会員）	東北大学大学院情報科学研究科教授
	佐古　和恵	（連携会員）	ＮＥＣ技術主幹
	寶木　和夫	（連携会員）	国立研究開発法人産業技術総合研究所セキュアシステム研究部門副研究部門長
	田中　英彦	（連携会員）	情報セキュリティ大学院大学学長、教授
	玉井　哲雄	（連携会員）	法政大学理工学部教授
	南谷　崇	（連携会員）	東京大学名誉教授
	橋本　周司	（連携会員）	早稲田大学理工学術院教授
	藤原　融	（連携会員）	大阪大学大学院情報科学研究科教授
	松井　知子	（連携会員）	統計数理研究所モデリング研究系研究主幹・教授
	米澤　明憲	（連携会員）	千葉工業大学人工知能・ソフトウェア技術センター所長

本件の作成に当たっては、以下の職員が事務を担当した。

事務	石井　康彦	参事官（審議第二担当）（平成 29 年７月まで）
	粂川　泰一	参事官（審議第二担当）（平成 29 年７月から）
	松宮　志麻	参事官（審議第二担当）付参事官補佐
	水野　雅弘	参事官（審議第二担当）付審議専門職付（平成 28 年３月まで）
	駒木　大助	参事官（審議第二担当）付審議専門職付（平成 28 年４月から）

要　　旨

１　作成の背景

2008 年に、日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会は、20期提言「安全・安心を実現する情報社会基盤の普及に向けて」を取りまとめ公表した。これは、情報社会基盤が抱える脆弱性とその影響を調査し、また我が国の関連する諸制度の状況を整理するとともに、情報社会基盤による安全・安心の実現に向けた検討を行い、行政、学協会、企業が行うべき方策案を提言としてまとめたものである。

しかし、20期提言の公表後も情報技術の急速な進歩と社会への浸透は続いており、当時は顕在化していなかった問題が認識されるようになってきた。また、20期提言の公表後に試みられた諸対策を、最新の知見に基づき見直すことで明確となった問題もある。そこで、これらの問題を中心に、社会の発展と安全・安心に資する情報社会基盤の普及に向けた課題について調査・検討を行い、その結果をとりまとめて公表することとした。

２　現状及び問題点

今日の我々の社会は、コンピュータや情報ネットワークなどを構成要素とする情報基盤（以下、「情報社会基盤」と言う。）に大きく依存している。情報社会基盤がきわめて大きな便益をもたらす反面、その抱えるリスクが顕在化し、様々な問題が発生している。リスクの顕在化が生命、尊厳、健康、財産、信用などの人間の基本権や社会の重要な価値に直接的な被害を及ぼすことも珍しくない。故障や操作ミスによる事故、人間の悪意に基づくサイバー攻撃などに対し、情報社会基盤の強靭化を図ることは喫緊の課題である。

さらに、人々の利害が対立する状況では、情報社会基盤を新たに導入することで、利害関係者の一部が不利益を被ることもある。情報社会基盤の発展の過程で、産業や経済の構造、人と機械の役割分担、人と人のつながり方や情報の流通に大きな変革を生じることは避けがたい。その結果として、基本権を侵害されたり、今までなら得られていたはずの利益を失ったりする人もいる。情報社会基盤の望ましいあり方や導入にともなう制度の変更について、社会的な合意をいかに形成するかが重要な課題となっている。

３　報告の内容

(1)　安全・安心な情報基盤の普及に向けた新たな課題

近年、IoT（Internet of Things)、ビッグデータ、人工知能（AI）が発達し、現在も急速に発達しつつあることから、それに伴う新たな問題が生じている。IoT については、従来のサーバ・クライアント環境で以前に発生していたのと類似の問題も生じている。しかし、安価で非力で大量の機器を、従来と同様の技術で守るのは困難であり、IoT に適合した技術が必要になる。また、それらを組み合わせて重要インフラやライフクリティカルな応用に耐えるソリューションを作り出す技術も必要となる。このような分野では、事故や攻撃による被害が甚大となり、人命を脅かす場合もあるため、一定の規制は必要である。

一方、ビッグデータや人工知能（AI）が発達すると、人間と機械の役割分担に変化が生じる。何を機械に任せるべきか、機械に任せたときの安全性や公平性をいかに担保するか、人間の役割の変化に対応した教育はいかにあるべきか等々の問題を検討する必要がある。このような問題群には唯一の正解があるわけではないため、社会的合意を形成する努力も必要である。これら新しい分野の研究開発や人材育成はまだ緒についたばかりであり、今後大幅に充実させる必要がある。さらに、法整備やマネジメントシステムの開発にも取り組む必要がある。

事故や攻撃については、それを防ぐことに価値があるのは明白であった。一方、近年、情報社会基盤がさらに人々の身近な領域に浸透した結果として、パーソナルデータの保護と利活用のように、単純に善悪を判断できない課題も増えてきた。社会の構成員の間で利害が対立しうる問題については、社会全体として受容できる合意点を見出す努力が必要である。しかし、この判断を行うべき人々の意識や常識が、情報技術によって加速された社会の変化に追いついていない現実もある。スピードも含めたトレードオフを考え、合意を得る社会的仕組みの構築が重要となる。

(2)　安全・安心な情報社会基盤の普及に向けた制度の整備状況

20 期提言「安全・安心を実現する情報社会基盤の普及に向けて」において提言された制度の整備に該当するものとして、サイバーセキュリティ基本法の成立とサイバーセキュリティ戦略本部の設置、個人情報保護委員会の設置、サイバー攻撃等に対する刑事罰適用範囲の拡大、情報技術の安全に関わる初の国家資格の認定開始等が行われた。提言の内容が完全に実施されたわけではないが、一定の進捗があった。一方、情報システムの脆弱性に関する事故調査委員会については、設置に向けた大きな動きはみられなかった。また、情報学に関する教育制度についても、進捗はあったが十分とは言えない。

(3)　安全・安心な情報社会基盤の普及に向けた研究面での課題

現在および将来の課題を解決するために研究開発が必要なことは言うまでもない。しかし、社会の安全・安心を深めるための研究活動では、脆弱性に関するデータや個人情報を含むデータの収集・共有が鍵となるケースが多く、研究を円滑に進めるにあたり、制度面でのハードルが高いこともある。公益に資する研究に対し、研究倫理審査体制の整備なども含め、これを円滑に推進できる仕組み作りも求められている。

目　　次

１　はじめに

今日の我々の社会は、コンピュータや情報ネットワークなどを構成要素とする情報基盤（以下、「情報社会基盤」と言う。）に大きく依存している。世界中に散らばる人や資源を結びつけるために情報ネットワークが活用され、さらに作業の自動化を進めるためにコンピュータが活用される。この組み合わせにより生み出される「世界を結んだ自動化システム」の効率性・利便性はきわめて高い。いわゆる重要インフラに分類される情報通信、電力、ガス、交通、物流、水道、金融、医療、政府・行政などの各種サービスもまた情報社会基盤に多くを依存している。一方で、情報社会基盤が抱えるリスクが顕在化し、様々な問題が発生しているのも事実である。「世界を結んだ自動化システム」という情報社会基盤の特徴が、短時間で世界中に悪影響を伝播し、被害を増幅する元凶ともなりうる。

情報社会基盤の応用分野は多岐に渡り、リスクの顕在化が生命、尊厳、健康、財産、信用などの人間の基本権や社会の重要な価値に直接的な被害を及ぼすことも珍しくない。故障や操作ミスによる事故、人間の悪意に基づくサイバー攻撃などに対し、情報社会基盤の強靭化を図ることは喫緊の課題である。それと同時に、人々の利害が対立する状況では、仮に情報社会基盤が設計意図通りに動作したとしても、利害関係者の一部が不利益を被る可能性に配慮する必要がある。情報社会基盤が社会全体にきわめて大きな便益をもたらすとしても、その発展の過程で、産業や経済の構造、人と機械の役割分担、人と人のつながり方や情報の流通に大きな変革を生じることは避けがたい。その結果として、基本権を侵害されたり、今までなら得られていたはずの利益を失ったりする人もいる。情報社会基盤の望ましいあり方については、社会的な合意を形成する必要がある。

日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会は、提言「安全・安心を実現する情報社会基盤の普及に向けて」（以下、「20 期提言」と言う。）[1]を取りまとめ、2008 年に公表した。これは、情報社会基盤が抱える脆弱性とその影響を調査し、また我が国の関連する諸制度の状況を整理するとともに、情報社会基盤による安全・安心の実現に向けた検討を行い、行政、学協会、企業が行うべき方策案を提言としてまとめたものである。従来個別に研究が行われていたセキュリティとディペンダビリティの知見を統合し、偶然や過失による事故と故意による攻撃の両面から調査・検討を行った点に特徴がある。

しかし、20 期提言の公表後も情報技術の急速な進歩と社会への浸透は続いており、2008 年当時には顕在化していなかった問題が認識されるようになってきた。また、近年になって、第４次産業革命や超スマート社会[2]のような新しいビジョンも提唱されており、情報技術が今まで以上に社会に浸透し、社会の構造をも大きく変えていくことが予見されている。さらに、緩やかではあるが制度面でも変化が見られる。

本報告は、20 期提言以降に顕在化した問題を中心に、社会の発展と安全・安心に資する情報社会基盤の普及に向けた課題について新たな調査・検討を行い、その結果をとりまとめて公表するものである。

２　20 期提言「安全・安心を実現する情報社会基盤の普及に向けて」の概要

20 期提言は、社会の安全・安心のために解決すべき情報社会基盤に関わる諸問題を、セキュリティとディペンダビリティの２つの観点から調査・検討し、その結果を基に提言を行ったものである。提言の内容は２つの大項目に分かれている。１つ目の大項目は、緊急に対処を要する重要案件に関するものであり、これは次の４つの小項目から構成される。

- 情報社会基盤に関する法制度及び資格認定制度の整備
- 安全で安心な情報社会基盤の管理・運用体制の整備
- 情報学に関する教育制度の構築
- 情報システムの脆弱性に関わる事故調査委員会の設置

まず、事故や攻撃が情報社会基盤にきわめて重大な被害を及ぼしうることから、適切な管理・運営に公の関与を求めている。具体的には、個々の実務者のための資格認定制度（第１小項目）、組織全体としての管理・運用体制（第２小項目）、万一の事故が発生したときに、その教訓を将来に活かすための調査体制（第４小項目）の整備がこれに該当する。加えて、意図的にサイバー攻撃等を行った者を、適切に処罰できる法制度の整備（第１小項目）を求めている。さらに、情報社会基盤の健全な発展とそれによる社会の安全・安心の向上のためには、社会を構成するすべての人々が、情報社会基盤の基本的な仕組みとそれが社会に及ぶ善悪両面の影響に対して一定の知識を持つ必要があるとの考えから、教育制度の整備（第３小項目）も求めている。

２つ目の大項目は、情報社会基盤の問題を取り扱う一元的な機関の設立に関するものである。情報社会基盤を社会の中で有効に活用して行くとともに、その安全性を守るためには、制度設計、研究開発と普及活動、教育と啓発等のさまざまな施策が必要である。これらについての戦略の策定、個別計画の企画・実施・評価等を統合的な枠組みで行っていくための一元的な機関の設置を求めている。

これら各項目の現状については、４節で改めて検討を行う。

３　安全・安心な情報社会基盤の普及に向けた新たな課題

情報社会基盤の脆弱性に起因する問題はかなり昔から発生しており、20 期提言でも代表的な問題事例を取り上げている。この章では 20 期提言以降に深刻さが増大した諸分野の問題を中心に、その背景と課題について述べる。

歴史的には、次のような変化に注目すべきである。

- 情報社会基盤の役割が増大し、人や社会にとって重要性が高い情報・システムの管理・制御を担うケースが増えた。その結果、情報社会基盤が内包する脆弱性が原因となり、きわめて深刻な事態を招く可能性も増えた。
- 従来は情報の取得や流通が困難であったため、結果的に守られていたプライバシーなどの人間の諸権利が、情報技術の発達により脅かされるようになった。

これらは情報技術の「影」の側面である。これと不可分な「光」の側面も確実に存在する。

- 情報社会基盤が発達したことで、世界に散らばっていた知識や知恵を集約することが、以前に比べてはるかに容易となった。そして、新たな社会的価値を創造する源泉としての情報社会基盤の役割が増大した。

この「光」の側面の意義は非常に大きく、学術活動でも産業活動でも、インターネット、Web、検索エンジンなどがなかった時代のやり方に戻ることは、もはや不可能である。

大きな価値を生み出す情報社会基盤はさらに利用が進み、その結果、さらに問題を引き起こしているのが現状である。「影」の影響を抑えるために、問題の発現防止や被害の緩和を行う技術の研究開発を推進する必要がある。同時に、次々に現れる新しいタイプの事故や攻撃を防止し、利害対立を調停するための制度設計も必要である。

(1)　制御システム・IoT の活用とリスクの拡大

制御システムは、他の機器やシステムの制御を司る情報システムであり、制御システムの停止や誤動作は、制御対象となる機器やシステムに多大な影響を及ぼす恐れがある。制御対象には、停止や誤動作が人の生命や健康に影響を及ぼすライフクリティカルな機器やシステムも含まれており、医療機器、自動車、プラントなどもこの部類に入る。このような制御システムに障害が発生した場合、安全な状態でシステムを停止させることが多いが、鉄道や電力などの重要インフラの場合、長時間の停止は社会に大きな影響を及ぼすことから、障害からの迅速な復帰など、障害時にもシステムの停止を最小限にすることが求められる。

旧来の制御システムは、インターネットなどの広域的なネットワークからは隔離されていることが多かったが、近年では、インターネットに積極的に機器を接続しようとする IoT（Internet of Things）も急速に普及しつつあり、製造・流通システム、医療・健康、マーケティングなど様々な分野での利用が始まっている。

①　20 期提言以降の状況の変化

制御システムの活用は、20 期提言以降もますます拡大しており、重要インフラへの適用やライフクリティカルな応用も増加している。これに伴い、サイバー攻撃の潜在

的対象が増加するとともに、被害が発生した場合の影響範囲も広がっている。20 期提言では、駅の自動改札機の停止や航空機の欠航により多くの乗客に影響が及んだ事例を紹介しているが、これらはシステム障害が原因であった。一方、近年では、重要インフラの制御システムもサイバー攻撃の影響を受けている。一例をあげると 2015 年 12 月にはウクライナで停電が発生した[3]。また、2015 年 7 月には、遠隔操作可能な脆弱性が見つかったことを理由に、米国で 140 万台の自動車のリコールが発表された[37]。個々の機器を制御するソフトウェアの大規模化・複雑化とこれらの機器を構成要素とするシステム全体の大規模化・複雑化も進行しており、不具合や脆弱性が増える傾向にある。

IoT が普及すると、安価な機器が大量にインターネットからアクセス可能性となる。機器が安価であるということは、セキュリティ対策に使える経費が少ないということである。また、大量の機器をネットワークに接続するということは、守るべき箇所が多いということである。結果的に、適切に管理されていない機器の増加につながる。安価な機器でも大量に乗っ取られると、それらの機器を踏み台にした大規模なサイバー攻撃が可能となり、社会に大きな悪影響を及ぼす可能性がある。実際に起こった事例を 1 つあげると、2016 年 10 月には、監視カメラ等の多数の乗っ取られた機器を利用し、1.2Tbps（毎秒 1.2 兆ビット）に達する大量の通信を発生させ、攻撃対象を麻痺状態にする DDoS（Distributed Denial of Service）攻撃が行われている[38]。この事例は、この種の攻撃として史上最大規模のものであった。このときの攻撃対象は、Web やメールの利用に必須となる DNS（Domain Name System）のサービスであり、これを利用していた多数の Web サイト等がつながりにくくなる問題も発生している。

サイバー攻撃はインターネット経由で行われることが多いが、それが唯一の経路ではない。広域的なネットワークからは隔離され、遠隔地からのサイバー攻撃は不可能という前提で設計されてきた旧来の制御システムにも、メンテナンス用のアクセス経路を介した内部からの侵入等は可能である。20 期提言以降に注目を集めた事例としては、2010 年に発見された Stuxnet を用いた攻撃が有名である。Stuxnet は、インターネットに接続された PC に感染し、その PC から USB メモリ経由で別の PC に感染する能力を持っており、イランのウラン濃縮用遠心分離機を稼働不能にした。インターネットからの隔離が機能しなかったこと、未知の脆弱性を利用したいわゆるゼロディ攻撃が行われたこと、米国およびイスラエルが国家として関与していた疑いがあること[4]など、防御を考えることが厳しい条件の事例である。

② 対応の現状

重要インフラの制御システムやライフクリティカルな応用では、事故発生時の損害が大きく、問題が発生してから対応するだけでは不十分である。システムの設計開発時の活動を通じてディペンダビリティとセキュリティを確保することが求められる。設計時にセキュリティを作り込む考え方は、セキュリティバイデザイン（SbD）と呼ばれ、その実現のためには、セキュリティ要求分析と開発プロセスが重要となる。

制御システムのディペンダビリティとセキュリティの確保のために、各種の規格やガイドラインの策定が進められている。ディペンダビリティの諸特性の中で制御システムにおいて最も重視される安全性に関しては、機能安全に関する分野非依存の基本規格として、国際電気標準会議（IEC）の IEC 61508 が策定されており、これをベースに、特定の製品分野固有のニーズに対応した分野別規格も次々に制定されている。その代表的なものとして、自動車を対象とした国際標準化機構（ISO）の ISO 26262 がある。これらの規格では、システムの安全性を確保するための機能要件の設定手法と、設定された機能の信頼性の確保手法に関して、システムの全ライフサイクルをカバーして言及されている。セキュリティに関しては、制御システム向けの汎用的なセキュリティ規格として IEC 62443 の策定が進められており、分野別規格の動きもある。例えば自動車向けには、現時点では SAE J3061 と呼ばれるガイドラインが公表されている。また、IoT のセキュリティに関しては、2016 年８月に内閣サイバーセキュリティセンター（NISC）が「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」[5]を、同７月に IoT 推進コンソーシアム、総務省、経済産業省が「IoT セキュリティガイドライン」[6]を、同３月に情報処理推進機構（IPA）が「つながる世界の開発指針」[7]を公表している。一方で、ガイドラインが乱立しているという課題も指摘されている。

これらの規格やガイドラインに準拠していることを認証する仕組みについても、徐々に整備が進められている。規格への準拠性の認証については、民間企業による認証が大きな役割を果たしている。

また、サイバー攻撃に関する情報共有の仕組みとして、ISAC（Information Sharing and Analysis Center）の設立が、様々な業界で進められている。例えば、米国の自動車業界では、Auto-ISAC が設立されている。我が国では、重要インフラの機器製造業を中心に、複数業界にまたがる情報共有のため、サイバー情報共有イニシアティブ（J-CSIP）[8]が 2011 年に設立されている。

③　残る課題

上述のような対応が進められているとは言え、まだまだ多くの課題が残されている。

最大の課題としては、セキュリティ基準の策定の必要性が挙げられる。セキュリティ対策に多くのコストをかければかけるほど、価格競争力を失う可能性が増えるため、セキュリティ対策は抑制されがちである。そのため、ライフクリティカルな応用や重要インフラの制御システムなど、事故・攻撃が社会に大きな影響を与えるシステムにおいては、実質的な強制力を持ったガイドライン化や規制の導入の必要性についても検討すべきである。

また、危殆化したシステムの扱いに関する課題も大きい。制御システムの中には、寿命が 10～20 年以上と長いものも多く、情報システムのライフサイクル、特に情報システムが危殆化する速度との間にギャップがある。製品寿命の途中で危殆化した場合、その対策費用を誰が負担すべきかは難しい課題である。メーカからは、一定期間過ぎ

ると製品を機能停止する（または、ネットワーク接続ができなくなる）ようにしたいとの声もあるが、ユーザが受け入れてくれるかどうかが問題である。

さらに最近では、センサーを誤動作させる攻撃など、制御対象となる機器に対する物理的な攻撃手法の報告が増えている。サイバー空間と物理空間の相互作用を踏まえた対応も大きい課題である。

その他に、制御システムとセキュリティ技術の両方を理解できる人材の育成、AI を用いたシステムでの認識技術の限界による安全性の喪失に対する考え方、脆弱性を明らかにする研究を実施する上での法的な問題など、課題は多い。

⑵　パーソナルデータの利活用と保護

①　個別化とアルゴリズムによる選別

サイバー空間でも物理空間でも、人の属性や行動に関する大量のデータ取得が行われる機会が増えており、いわゆるビッグデータ解析が盛んに行われるようになった。その結果、さまざまな分野で利用者に合わせたサービスや製品の個別化が進んでいる。個別化医療や精密医療はその一例であり、患者の遺伝子型、生活環境、生活スタイルなどを反映したより良い治療が期待されている。

一方で、人を対象とした個別化の要素技術は、人を選別する目的で利用される懸念もある。従来から、合格・不合格や無罪・有罪の決定などで人による人の選別は行われてきた。そして、社会的公平性が求められる場面では、性別、人種、宗教などによる差別の禁止を制度化することで一定の公平性を保ってきた。しかし、機械による選別が行われるようになると、アルゴリズムの選択や機械学習（machine learning）訓練データの集め方が原因で、公平性からの逸脱が起こる可能性がある。そのため、公平性をいかに実現するかが課題となる。2016 年に米国の Executive Office of the President が公表したレポート[39]では、ケーススタディとして与信、就職、入学、刑事司法の意思決定を取り上げた議論が行われている。技術的には透明性や説明責任をいかに担保し、公平性を保証するかが重要となる。ただし、公平性の基準は社会的合意により決められるものであり、技術的な検討だけで決められるものではないことには注意が必要である。

②　パーソナルデータ利活用の便益と懸念

「世界最先端 IT 国家創造宣言」[9]及び「日本再興戦略 2016－第４次産業革命に向けて－」[10]では、パーソナルデータやオープンデータの利活用が国家戦略として示されている。パーソナルデータの有効な利活用が大きな便益を生むこと自体に異論はないであろう。一方で、パーソナルデータの積極的な利活用に不安を感じる人々は少なくない。2014 年には通信教育の大手企業から、2015 年には日本年金機構から個人情報が大量に漏洩し、世間の注目を集めていることを考えると、これは自然な反応である。事業者側でも、事件発生時の評判を恐れ、パーソナルデータの利活用に二の足を踏む状況が散見される。

このような総すくみ状態を脱却し、パーソナルデータの保護と利活用を高いレベルで両立させるためには、安全性を保証する技術の研究開発・普及と安心につながる制度・体制の確立が必要である。技術に関しては、事業者が管理するパーソナルデータをサイバー攻撃や内部犯行者から守る技術、個人が識別できない形でパーソナルデータの第三者提供を可能とする技術などが特に重要である。なお、2015 年に改正され、2017 年５月 30 日に全面施行される「個人情報の保護に関する法律」(個人情報保護法)では、匿名加工情報という概念が導入される。本人同意なしで第三者提供を可能とするためのものであり、基準は個人情報保護委員会規則で定める。ただし、どんな技術を用いても 100%の安全性は保証できない。そこで、制度や体制の設計を工夫して、問題が発生する可能性が十分に低い技術や管理方式の採用、万一問題が発生した時の被害軽減や補償のあり方などを定めることが重要となる。

③　パーソナルデータ保護の制度

20 期提言以降、我が国では②でも言及した通り個人情報保護法が改正された。EU においても、「一般データ保護規則 General Data Protection Regulation」が 2016 年に採択され、2018 年５月 25 日から運用が開始される。以前に比べ、個人の行動データなどを大量かつ容易に取得できるようになり、さらに多様な情報源から集められたデータの統合解析も容易になったこと、すなわち、IoT やビッグデータの発展がこのような動きの一因である。

この EU の一般データ保護規則では、個人が自分のデータを自分でコントロールできることをめざし、「データポータビリティの権利」が定められている。これは、企業や組織が収集したパーソナルデータを本人も活用し、本人から別の企業に提供できるよう扱いやすい形で提供してもらう権利である。この権利によって、個人が自らのデータを収集管理し、本人の意思に基づいてデータ流通を実現する社会を描いている。このような社会では、パーソナルデータを必要とする企業に対して、利用目的を明確にした上で提供し、さらに対価を交渉できる可能性がある。これにより、活発で健全なデータ流通が実現できることが期待される。企業にとっても、自前でパーソナルデータを収集し、高い管理コストを払って漏洩リスクを抱えながら保有するより、必要な時に最新のデータを本人の許可のもと入手できる方が、メリットが大きい可能性がある。そして、実際に、英国の midata[40]、米国の Smart Disclosure[41] などの動きが始まっている。国内でも「世界最先端 IT 国家創造宣言」では、データ流通における個人の関与の仕組みや、個人が自らのデータを信頼できる者に託し本人や社会のために活用する仕組みが想定され始めている。

今後、個人主導のデータ管理基盤、データ連携基盤、データ処理基盤に係わる技術の深耕が必要になる。イノベーティブな新事業・新サービスをもたらすデータドリブンの研究活動は、この構想を基盤に、安心・安全・公平で健全なデータ流通を前提としたものであることが望ましい。

⑶ 情報ネットワークのセキュリティと基本権

① 情報ネットワークの運用

情報ネットワークは、情報社会基盤を構成する不可欠の要素であるとともに、遠隔地からのサイバー攻撃が必ず通る経路としても使われる。今日、サイバー攻撃の影響はきわめて深刻となっており、これを防ぐための一手段として、攻撃経路である情報ネットワークを監視することが有効と考えられる。一方で、日本国憲法第 21 条第２項は、検閲の禁止と通信の秘密の不可侵性を定めており、通信の秘密は人間の基本権の１つと考えられる。実効性を持たせるためには、公権力だけではなく事業従事者の行為も規制する必要がある。そのため、電気通信事業法では第３条で「検閲の禁止」、第４条で「秘密の保護」、第 179 条で関連する罰則を規定しており、通信の秘密の侵害は、未遂でも刑事罰の対象となる。さらに、電気通信事業法を補完するものとして、有線電気通信法と電波法にも、通信の秘密の保護と対応する罰則が定められている。情報ネットワークによる通信にも憲法やこれら諸法の規程は当然適用される。

通信の秘密の保護は一般には好ましいことであるが、杓子定規に適用すると、犯罪や反社会的な活動も保護する恐れがある。そのため、通信の秘密はきわめて重要ではあるが、すべてに優先するとは考えられていない。社会的な利益と不利益を勘案して、別の社会的な価値を優先することもありうる。例えば、犯罪捜査のための通信傍受に関して、通信の秘密に一定の例外があることが最高裁の判例[11]でも示されている。ただし、例外と認められるためには厳しい要件を満たす必要がある。

インターネットの接続を提供する通信事業者（ISP, Internet Service Provider）は、通信の秘密を保護するという基本姿勢のもとで合理的な対応がとれるように検討を重ねている。これまで、インターネット上の自殺予告事案への対応に関するガイドライン[12]、インターネット上の違法な情報への対応に関するガイドライン[13]、電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン[14]などを公開している。このように諸権利が対立し、同時にすべてを守ることができないケースについては、社会の変化を見据えつつ、調停の努力を続ける必要がある。

② 情報ネットワークに関する研究

情報ネットワークのセキュリティや安定性を守るための研究活動でも、観測データの取得や活用が、通信の秘密やパーソナルデータの保護と対立することがある。情報ネットワークの研究用のデータとしては、サイバー攻撃の被害、マルウェアの活動の実態を含むデータが情報処理学会のコンピュータセキュリティ研究会 MWS 組織委員会によってMWS Datasets として整備されている[15]。実用的な研究を進めるためには、現実を反映したデータの取得と利用が不可欠であり、このデータセットを利用した研究の例は多い。

悪意のある攻撃やマルウェアのデータ（black）は、通信の当事者が意図的に収集する、あるいは納得して提供する場合には通信の秘密を侵さない。しかし、機械学習を用いた研究では、悪意のあるデータ（black）だけではなく、平常時の通信のデータ

（white）が学習や評価のために重要になる。情報ネットワークにおける個人情報、通信の秘密の保護の基準は国によって違いがある。保護が十分に行われない国の方が、研究開発用のデータ（black and white）を得やすいという皮肉な現状がある。

情報ネットワークにおける個人情報、通信の秘密を保護しながら、この分野の研究開発を推進するためには、対象となるデータを安全かつ遵法的に共有するための技術、制度、ガイドラインの整備が必要である。保護が必要な研究用データの共有については、５(1)で改めて検討を行う。

(4) 情報の信頼性・信憑性

① 社会を脅かす情報の偽造

社会を構成する人々の間の信頼関係が崩れると、その社会は安定性を失う。情報社会基盤には、生活や産業を支える重要インフラの制御系としての信頼性だけでなく、人々の間でやりとりされる情報の信頼性・信憑性に悪影響を与えないことも求められる。情報が主として紙でやりとりされていた時代にも、情報の改竄が社会や国家に多大な悪影響を及ぼす可能性は知られており、我が国の刑法では、通貨、文書、有価証券、印章・署名等に関する偽造罪が昔から定められている。これらの情報の改竄が、情報ネットワークを介して通貨、文書、署名等のやりとりが可能となった今日では、情報社会基盤へのサイバー攻撃により起こりうる。

警察庁の調べでは、2015 年の我が国におけるインターネットバンキングの不正送金事犯の被害額は約 30 億円に達している[16]。海外では、2016 年２月にバングラディッシュ中央銀行が、不正アクセスにより１億米ドルを超える被害（一部は回収された）を受けている。また、選挙の電子投票が発達した国や地域では、電子投票システムに対するサイバー攻撃が、民主主義の根幹に影響を及ぼす可能性も無視できない。インターネット投票の先進国であるエストニアで実際に使われている投票システムの脆弱性を指摘する学術論文も存在する[42]。これらの事例は氷山の一角であり、今後、さまざまなタイプの情報改竄の被害が増える可能性がある。

② アルゴリズムによる情報の選択と拡散

善悪の区別がつきやすい通貨や署名の偽造だけが、情報の信頼性や信憑性に対する脅威ではない。世界最大規模のソーシャルネットで、人気のニュースを表示する機能（Trending Topics）の編集者が、保守派メディアを意図的に排除したとの疑惑が 2016 年５月に浮上した。この段階では人間の偏向の問題と捉えられ、編集者の一斉解雇と自動処理への置き換えが行われた。ところが、2016 年８月になると、この自動処理のアルゴリズムにより、事実誤認が明らかなニュースが表示される事件が起こった[17]。サイバー社会には多数の読者を有するデマサイトが少なからず存在し、「世界を結んだ自動化システム」としての情報社会基盤が、虚偽情報を拡散する装置としても機能しうるのである。

一方、我が国では 2016 年末に、まとめサイト（キュレーションサイト）の大手企業

が、医療情報サイトを始め、運営するすべてのまとめサイトを閉鎖する事件が起こった。ページビューを稼いで多くの広告収入を得ることを優先し、内容の妥当性には問題がある記事を安価かつ大量に作成して掲載したためである。高品質ページに高順位を与える意図で設計された検索エンジンの裏をかき、低品質ページであっても高順位になるような操作が行なわれた。

現代人は膨大な情報に囲まれて生活しており、一人の人間の能力では、そのうちのごく一部に触れることしかできない。そのため、見るべき情報の選別をアルゴリズムに頼らざるを得ない。主要な検索エンジンのアルゴリズムの裏をかく行為は、少なくとも現時点では、社会全体にとっての脅威となりうる。

このような自動化システムによる選別に加えて、ソーシャルネットによる虚偽情報の拡散は重大な問題である。自分が信頼する人の発言を、人は信用する傾向がある。そして、ソーシャルネットは、信頼関係にある人同士を結びつけている。そのため、ソーシャルネットを介した情報の拡散はきわめて効果的に行われる。情報が客観的な事実を伝えるかどうかより、誰がその情報を伝えているかを重視することが少なくない。

③　信頼性・信憑性の向上に向けて

情報の偽造や虚偽情報の拡散に対し、中央集権的な権力や権威を仮定せずに対抗する可能性として、多数による監視に基づく方式が考えられる。20 期提言が公開された数ヶ月後にビットコインの論文[43]が公開され、その後、ブロックチェーンによる分散型の台帳管理が注目を集めるようになった。これは、非中央集権的な手法で情報の偽造を防止するための有力な考え方である。ただし、非中央集権的な手法は、通常、多数決の考え方に依存するため、偽造に加担する側が一定数を超えると機能しなくなる。このような限界はあるものの、一定の条件下でならアルゴリズミックに真偽が判定できるタイプの問題は、比較的対処しやすい。

一方、見解の相違が生じうる状況での虚偽情報の拡散防止は容易でない。万人が書き込めるにも関わらず、虚偽情報を抑え込むことにある程度成功している事例として Wikipedia がある。過去の変更履歴をすべて記録してバージョンの復帰を容易に行えるようにする技術とコミュニティの信任投票により管理者を選ぶ方式が比較的うまく機能していると思われる。しかし、世の中に流通している情報は、科学的プロセスを経て受け入れられた「事実」だけではなく、異なる文化圏に属する者が異なる「真実」を信じている場合も少なくない。複数の対立する見解を許容しつつ、科学的プロセスを経て検証された「事実」が多くの人々に共有されるような仕組みづくりが望まれる。ここでもまた社会的合意を欠かすことはできないが、受容と選択に関する合意プロセス自体が、今日では情報社会基盤の力を借りて実施される点には注意が必要である。

(5)　知的システムと社会との関わり

20 期提言以降も情報技術の進歩に伴い、妥当なコストで機械化できる作業は増え続け

ている。結果的に、社会全体の自動化が進んでおり、従来は人間が行っていた作業や従来は存在しなかった作業を機械が担う局面が増えている。これにより、生産性が向上し、社会が豊かになる可能性がある反面、さまざまな懸念も増えている。特に近年は、人工知能（AI）の研究が躍進をとげ、従来よりも知的なシステムがネットワーク化された形で、社会に浸透する姿が予見されるようになってきた。

知的なシステムの倫理的、法的、社会的問題(ELSI - Ethical, Leagal Social Issues)に関する議論が現在世界中で活発に行われているところである。 我が国では、人工知能学会が倫理委員会を設け、2017年２月には倫理指針を公表している[18]。これは、主として学会員に対する倫理の指針を示すものである。海外の学会でも検討が行われており、電気電子工学と情報学に関連する最大規模の学会であるInstitute of Electrical and Electronics Engineers（IEEE）ではGlobal Initiative for Ethical Considerations in Articial Intelligence and Autonomous Systems が2016年にレポート[44]を公表している。これは、人工知能や自律システムが人間社会の価値に適合した存在であるための諸課題について議論したものであり、自律兵器も対象としている。また、主として情報学に関連した学会の中で最大規模のAssociation for Computing Machinery（ACM）ではUS Public Policy Council が2017年にアルゴリズムによる意思決定(algorithmic decision making）について声明[45]を公表している。

安全性や遵法的・倫理的な動作を保証することが、知的なシステムを構築・利用する際の大きな課題となる。システムの内部構造、知識・知恵を獲得した過程などがきわめて複雑となり、分析・追跡が困難になると動作の保証も難しくなる。そのため、透明性の確保や説明責任が重要な課題となる。(2)①で述べた人間の選別にアルゴリズムが用いられるケースでの公平性とそのための透明性・説明責任も、このような課題の一種と考えることができる。

また、機械が人間の仕事を奪うことに対する懸念もある。これは、一般向けの書籍でも語られるテーマである（[46]など)。単に雇用の数の変化に注目するだけでなく、知的システムが社会に浸透し、人間と機械の役割分担が変わることで、人間に期待される仕事の内容も変わる点に注意が必要である。社会全体では、今までより少ない労働時間で豊かな生活を実現できる可能性がある反面、個々人にとっては職を失い貧困に陥ったり、新たなストレスに見舞われたりする危険性もある。貧困の拡大などの悪しきシナリオを避けるためには、教育システムの大幅な改革も必要と予想される[47]。

４　安全・安心な情報社会基盤の普及に向けた制度の整備状況

20 期提言では、緊急に対処を要する重要案件を４つ取り上げ、主に制度に関する提言を行っている。さらに情報社会基盤に関わる課題を一元的に取り扱う機関の設置を求めている。これらに関する 20 期提言以降の変化を、４つの重要案件については(1)～(4)に、一元的機関については(5)にまとめる。

(1)　情報社会基盤に関する法制度及び資格認定制度の整備

①　サイバー犯罪の加害者への罰則適用

コンピュータウイルスの作成・配布に関しては、2011 年の刑法改正による「不正指令電磁的記録に関する罪」の新設、フィッシング詐欺に関しては、2013 年の「不正アクセス行為の禁止等に関する法律」の改正による「不正取得罪」、「不正保管罪」の新設など、サイバー犯罪の刑事罰化には一定の進展があった。より広い範囲のサイバー攻撃に刑事罰を適用する根拠を与えた点では意味があるが、定義の仕方には改善の余地があるとの指摘もある。しかし、その後も標的型攻撃、ランサムウェアなどによる攻撃は続いており、大きな被害も発生している。国外からの攻撃も多く、国内法の整備だけでは実効性が伴いにくいという問題もある。なお、「不正指令電磁的記録に関する罪」の検挙件数は年間数十件程度である[19]。

一方、内部犯行の場合の罰則適用については、通信教育の大手企業からの顧客情報漏洩事案なども踏まえて、営業秘密保護強化の方向で、2015 年に不正競争防止法が改正されている。「個人情報の保護に関する法律」にも 2015 年の改正により、個人情報データベース等提供罪が導入された。名簿の意図的漏洩に対しては、一定の歯止めになることが期待される。

②　情報社会基盤の脆弱性を発見した研究者の保護

我が国の著作権法では、ソフトウェアの脆弱性の調査に通常必要となる作業が、複製権や翻案権の侵害になる恐れがあり、現実の脆弱性に関する研究を阻害する要因となっている。今後も、IoT の発展により、インターネットに接続される機器は急激に増加することが予想される。これらの機器に対する善意による脆弱性研究を円滑に進め、情報社会基盤を安全・安心なものとするためには、この点での制度整備は必須である。なお、米国においては、Digital Millenium Copyright Act (DMCA)に 2015 年から 3 年間の期限付きで設けられた例外処置が 2016 年にようやく承認され、一定の条件のもとで、機器に内蔵されたソフトウェアの脆弱性の研究が可能となった[48]。この対象には自動車も含まれる。我が国においても同様の例外処置が望まれる。

③　情報社会基盤を構築・運用するための資格認定制度の整備

2016 年に「情報処理の促進に関する法律」が改正され、国家資格として情報処理安全確保支援士が新設された。サイバーセキュリティの確保の支援を業とするものであり、資格維持のための講習の義務化、違反すると刑事罰の対象となる守秘義務などが

定められている。この分野初の国家資格の整備という意味では一歩前進した。しかし、業務独占資格（独占的に行える業務を法令で定めた資格）ではないため、実効性を持たせるための普及活動や有資格者による実績作りが今後必要である。

(2) 安全・安心な情報社会基盤の管理・運用体制の整備

① ライフサイクル全般に渡る対策

故障や攻撃から情報社会基盤および情報そのものを守るために、まず重要なのは情報社会基盤の脆弱性を減らすことである。これは主に設計開発の段階で解決すべき課題である。一方、実際に問題が発生するのは運用の段階である。不適切な利用の防止、万一の場合の緊急時対応などはこの段階の課題である。一般に、情報システムのライフサイクルには、要件定義、設計、実装、テスト、運用・保守、廃棄などの段階が存在する。運用開始後に改修のために要件定義に戻るサイクルを頻繁に繰り返すものもあれば、そうでないものもある。どちらの場合においても、それぞれの段階で、適切な技術と管理体制を用いることが重要である。

このようなライフサイクルを意識した開発・運用の重要性については、20 期提言が公表された 2008 年には既に知られていた。ライフサイクルを意識したセキュリティの向上については、米国 NIST (National Insistute of Standards and Technology) が SP800-64[49]の Rev. 1 を 2004 年、Rev. 2 を 2008 年に発表している。また、多くの開発者に影響力を持つと思われるマイクロソフト社の Security Development Lifecycle (SDL) を解説した書籍[50]も 2006 年に出版されている。しかし、日本語の情報源は必ずしも多くなく、開発者に情報が伝わるまでには時間がかかるため、基本的な考え方が認知され始めたのが、20 期提言が公表された前後の時期であった。その後、考え方の共有が進みつつある。

② 標準、ガイドライン、ベストプラクティス、認証

３(1)②で言及した制御システムや IoT のものを含め、多数の標準やガイドラインが公表されており、分野によっては乱立している感もある。標準には認証機関による認証をともなうものもある。また、ベストプラクティスを集積する活動も進められており、米国 US-CERT (United States Computer Emergency Readiness Team) の Build Security In[51]などが有名である。また、我が国では情報処理推進機構が、一般向けや経営者向けなど、技術者・管理者以外を対象とした資料も公開している[20]。情報技術のフロンティアは拡大を続けており、今後も、新しい状況に合わせた標準やガイドラインの策定、ベストプラクティスの集積が必要である。

以下では、国際標準に基づく認証制度に絞り、組織的な管理と製品の安全に関する事例を紹介する。(1)③でとりあげた個人の資格認定制度とは相補的なものであり、個人、組織、製品のそれぞれの観点での基準が求められる。

情報セキュリティマネジメントに関する国際標準としては ISO/IEC 27000 シリーズがあり、国内では日本工業規格（JIS）による JIS Q 27000 シリーズが対応している。

情報セキュリティマネジメントは、主として、組織が保有する情報資産を守るためのものである。情報セキュリティマネジメントシステム（ISMS）適合性評価制度[21]において、適合性を審査する際の基準として JIS Q 27001 が用いられる。ISO/IEC 27000 シリーズの前身となる ISO/IEC 17799 は 2000 年に出版されており、基本的な概念は 20 期提言以前からよく知られていた。しかし、20 期提言以降も改訂・増補が続いている。例えば、クラウドコンピューティング分野を対象とする ISO/IEC 27017 は 2015 年に発行された。

一方、製品のセキュリティ評価の国際標準としては ISO/IEC 15408 があり、その国内版に相当するのが JIS X 5070 である。７段階のレベル(EAL, Evaluation Assurance Level)があり、最も下位の EAL1 では機能テストのみが評価の対象となるが、中位の EAL4 以上では設計も評価の対象となる。最上位の EAL7 では形式検証が要求される。20 期提言以降、バージョン 3.1 リビジョン４が 2012 年に公開されている。IT セキュリティ評価及び認証制度（JISEC）[22]の評価は ISO/IEC 15408 に基づいて行われる。

(3) 情報学に関する教育制度の構築

① 初等中等教育での情報学と情報技術

社会での情報機器の利用拡大、利用者や利用機器の多様化、利用場面の拡大に伴い、情報学の教育の重要性はますます増大している。20 期提言で提示した、初等中等教育における情報学に関係する教育の改善は、順調に進んでいるとは言い難いが、一方で教育現場への情報機器の利用と導入は急速に進んでいる。文部科学省では、デジタル教科書の導入の検討も進めており、小学校では 2020 年に予想される次期学習指導要領の実施に合わせた導入が望ましいとする検討会の「最終まとめ」[23]が発表されている。教育現場の情報化の進展に合わせた教育制度の整備は、喫緊の課題である。

② 大学での情報学教育

大学教育においては、2016 年３月に、日本学術会議情報学委員会情報科学技術教育分科会より、「大学教育分野別質保証のための教育課程編成上の参照基準　情報学分野」[24]が公表され、情報学を専門とする教育だけでなく、教養教育としての情報教育についても言及されている。情報学を「広く市民が持つべき教養の一部」と捉え、初等中等教育から大学教育まで、市民一人一人の情報技術への造詣とスキルを向上させることの重要性を指摘している。さらに、それだけではなく、情報技術の利用法を間違えることで社会の安全を脅かす可能性を認識させることの重要性も指摘している。

③ 大学での一般教育としての情報倫理・サイバーセキュリティ

基本的な情報倫理教育に関しては、2003 年に当時の国立大学情報処理教育センター協議会 情報倫理教育教材タスクフォースが初版を作成し、その後改訂を重ね、現時点で最新の第６版は大学 ICT 推進協議会(AXIES)が企画・制作している情報倫理デジタルビデオ小品集[25]などが、多くの大学の基礎教育に導入されている。一部の高等学

校でもこのビデオを教材として採用しており、徐々にではあるが基本的な情報倫理および情報技術の利用に関する危険性に関する教育は改善されている。しかし、情報技術の社会への浸透は、予測を超える勢いであり、現場の教育制度の迅速な改革が必要である。

大学の一般的な教育の中に、サイバーセキュリティに関する講義を導入する取り組みも始まっている。例えば、九州大学では、2014 年度よりサイバーセキュリティ基礎論を全学共通教育で開講し、すべての学部の１年生を対象とした教育を始めている[26]。そして、2017 年度からは、卒業に必要な必修単位とすることを予定している。このような取り組みを、多くの大学へ広げていくことが望まれる。

④　大学・大学院でのサイバーセキュリティ専門教育

サイバーセキュリティに関する専門教育としては、2007 年から先導的 IT スペシャリスト育成推進プログラムの「社会的 IT リスク軽減のための情報セキュリティ技術者・管理者育成」（奈良先端科学技術大学院大学、京都大学、大阪大学、北陸先端科学技術大学院大学）と「研究と実務融合による高度情報セキュリティ人材育成プログラム」（情報セキュリティ大学院大学、中央大学、東京大学）が始まった。それぞれ、社会的 IT リスク軽減のための情報セキュリティ技術者・管理者、及び、研究と実務融合による高度情報セキュリティ専門家を育成することを目的としたものである。2011 年度にプロジェクト自体は終了したが、その後も一部の大学院で自主的に教育を継続している。

2012 年度からは「分野・地域を超えた実践的情報教育協働ネットワーク（enPiT）」のセキュリティ分野（enPiT-Security, SecCap）として５つの連携大学（情報セキュリティ大学院大学、奈良先端科学技術大学院大学、北陸先端科学技術大学院大学、東北大学、慶應義塾大学）が中心となり、大学院修士課程を対象として、社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を、技術面・管理面で牽引できる実践リーダーの育成を目指す教育プロジェクトが始動している。さらに、2016 年 10 月から、学部学生を対象とした enPiT-Security の実践的人材育成コース「Basic SecCap」[27]が開始され、2016 年度は 11 大学が連携して講義及び演習を担当した。各科目は、連携校相互、及び各地の参加校に提供されるため、連携校以外の多くの大学でも実践的人材育成の教育を受けることができるようにする計画である。このように、サイバーセキュリティに関する専門人材の育成については、急速に教育体制が整えられている。

(4)　情報システムの脆弱性に関わる事故調査委員会の設置

20 期提言以降現在に至るまで、情報社会基盤の事故全般を対象とする事故調査委員会を設置する動きはない。航空・鉄道・船舶の事故を扱う運輸安全委員会[28]、医療事故を扱う医療事故調査制度[29]に相当する組織や制度は現状存在しない。しかし、ここで重要なのは、「事故調査委員会」という名称の組織の設立ではなく、事故の教訓を将来に

活かす体制の確立である。以下では、２件の事例に基づき、事故調査委員会がない状態で、教訓を将来に活かすことがどこまでできたかを検討する。

2015 年に発生した日本年金機構での個人情報流出事案では、流出の規模が大きかったこと、多くの国民にとって重要な年金を扱う組織であったこと、完全に防ぐのが難しい標的型攻撃が行われたことなどから、人々の注目を集めた。この事案に関しては、サイバーセキュリティ戦略本部と内閣サイバーセキュリティセンター（NISC）による調査結果[30]が公表されている。この調査は、2014 年に制定されたサイバーセキュリティ基本法を根拠に行われている。また、結果の公表は、我が国の企業や個人のサイバーセキュリティの能力向上の参考に供することも企図したものである。これらのことより、独立行政法人を含む政府機関のサイバーセキュリティ事案に対し、制度的にこのような調査が可能であり、また本件に関する限り、サイバーセキュリティ戦略本部が事故調査委員会に期待される機能を担ったと考えることができる。なお、サイバーセキュリティ事案の調査においては、結果を公表することで、調査した組織の能力を間接的に公表してしまう可能性がある。上記の調査結果は、このデメリットをも考慮した上で、総合的にはメリットの方が勝ると判断して公表されている。

一方、民間の事故で大きな経済的損失が発生し、当事者間でその負担が争われる場合には、将来の再発を防止するための事故調査は難しいのが現実である。2005 年に、証券会社が株を大量に誤発注（「61 万円１株」を「１円 61 万株」と誤って発注）した事案では、注文の取り消しが受理されなかったことを理由に、証券会社が証券取引所に損害賠償を求める訴訟を起こした。414 億円の請求に対し、最終的に証券取引所に 107 億円の支払が命じられている。一般に、一方の当事者に不利な情報を、係争中に事故調査で聞き出すのは容易ではない。このケースでは、裁判中に、システムのソースコードの一部が任意開示され、裁判に関係する限られたソフトウェア工学の専門家が閲覧を許された。発注取り消し処理にバグがあることは明らかとなったが、再発防止の知見を社会で共有するために重要と思われるソフトウェアのアーキテクチャ、開発組織の体制などについて、開示された情報のみから十分な分析を行うには至らなかった[52]。民間で発生した重大な事故の教訓を将来に活かす仕組みの構築は、依然として残る課題である。

(5)　情報社会基盤に関わる課題を一元的に取り扱う機関

①　サイバーセキュリティに関する事項

(4)の前半で取り上げたサイバーセキュリティ戦略本部と内閣サイバーセキュリティセンター（NISC）は、2014 年のサイバーセキュリティ基本法の成立を受け、2015 年に設置された組織である。これらは、以前の情報セキュリティ政策会議と内閣官房情報セキュリティセンターを強化したものと考えることができる。

サイバーセキュリティ戦略本部は、国の行政機関、地方公共団体、独立行政法人等に対し、サイバーセキュリティに関する必要な資料や情報の提供を求め、勧告を行う権限を有している。また、府省横断的な計画を含むサイバーセキュリティ施策の実施、評価、総合調整などもつかさどる事務に含まれている。総合すると、国家としてのサ

イバーセキュリティ戦略の策定、公的機関のサイバーセキュリティの確保、サイバーセキュリティに関する施策の実施・評価・調整などを一元的に行う機能を有している。また、NISC は、JPCERT コーディネーションセンター、情報処理推進機構、情報通信研究機構、産業技術総合研究所とパートナーシップを結んでいる。20 期提言以降、この分野での一元化は進んだと考えられる。

② 個人情報保護に関する事項

マイナンバーの導入にともなう「行政手続における特定の個人を識別するための番号の利用等に関する法律」（番号法）が 2013 年に制定され、さらに個人情報保護法の改正が 2015 年に行われた。これらの結果、2014 年には特定個人情報保護委員会が設置され、さらに 2016 年に個人情報保護委員会に改組された。従来、各事業分野の主務大臣が有していた個人情報の保護に関する権限を、個人情報保護委員会に集約したという意味で一元化は進んだと考えられる。また、同委員会の設置により、行政機関から独立した個人情報保護を担当する第三者機関がようやく我が国にも生まれることとなった。

5　安全・安心な情報社会基盤の普及に向けた研究面での課題

(1)　研究情報の共有

IoT、ビッグデータ、AI などの技術分野の発展は、学術研究の進め方にも大きな影響を与えている。大量データの取得と蓄積が以前に比べてはるかに容易となり、統計処理や機械学習に基づくモデル化や分析の技術も進歩した。これらの技術を用い、より広範かつ大量の研究データを取得・分析することが、学術の発展に結びつく可能性は増えている。一方、経済的には、データのコピーのコストは取得のコストよりはるかに安価な場合が多い。したがって、個々の研究グループが独立に研究データを取得して囲い込むよりも、コミュニティ全体で研究データを共有・共用する方が、学術の発展にとって望ましい。日本学術会議においても、2014 年には情報学委員会国際サイエンスデータ分科会がオープンデータとデータジャーナルに関する報告[31]、2016 年にはオープンサイエンスの取り組みに関する検討委員会がオープンデータに関する提言[32]を発表している。これらも基本的には研究データの共有を促す方向のものである。

情報社会基盤の安全・安心に関わる学術分野もこの潮流と無縁ではない。現実の事故、攻撃、脆弱性などに関するデータを研究者が手分けして収集し、それを共有して研究に活かすことは、研究の発展にとって有益である。また、共通のデータをベンチマークに用い、異なるグループの研究成果を統一的尺度で評価できるようにすることで、健全な競争を促す効果もある。これらの効果により発展した研究の成果は、将来社会の安全・安心に資するものになると考えられる。しかし、この分野の特性として、悪意ある攻撃者が存在するため、悪用される可能性のあるデータは隠す必要がある。

そのため、完全にオープンな共有を目指すのは難しく、一定の条件を満たす研究者等が共有できるデータの整備を行うのが現実的である。３(3)②で言及した MWS Datasets[15]はこのような事例の１つであり、当初はサイバークリーンセンター (CCC)、現在は後継の CCC 運営連絡会（日本データ通信協会テレコム・アイザック推進会議、JPCERT コーディネーションセンター、情報処理推進機構の 3 者から構成される）がデータを提供している。海外では、世界中に観測網を持つセキュリティ分野の事業者が、研究者に情報を提供する仕組みを構築している例も見られる[53]。また、日本学術会議のマスタープラン 2017[33]に掲載された計画の中にも、攻撃手法と脆弱性のデータベースを整備し、学術機関での研究に提供することを目指したものがある[34]。

国内の他分野でも、一定の条件を満たす研究者等が共有できるデータの整備を行なっているケースがある。例えば、統計センターは、統計の調査票データをオンサイトの施設内で研究者がアクセスできるサービスを提供している[35]。これは統計法に基づくものである。また、厚生労働省はレセプト情報・特定健診等情報を提供するにあたり、ガイドラインを作成している[36]。これらの事例を踏まえるとともに、分野の特性を十分に考慮し、今後より良い体制の検討を進めることが望まれる。

(2)　研究倫理

情報社会基盤の脆弱性に関する調査研究は、法律や倫理の問題を起こしやすい。４

(1)②で述べたように、我が国ではソフトウェアの脆弱性調査に通常必要となる作業が、複製権や翻案権の侵害になる恐れがある。インターネットに接続された機器の脆弱性調査でも、不用意に行うと不正アクセス禁止法に違犯する可能性がある。また、攻撃者側のコミュニティを分析するために、そのコミュニティの内部に入り込むと、攻撃が行われているのを座視し、結果として被害を黙認してしまうなど、倫理的には問題となる行為に結びつく可能性がある。

他のケースとして、研究者が具体的な脆弱性を発見した場合、製造者によるセキュリティアップデート等が利用可能となる前にその情報を開示すると、それが原因となってサイバー攻撃を誘発し、第三者が被害を受ける可能性がある。これは被害者にとって不利益となるシナリオだが、逆に、研究者が自分の研究成果を公表できない事態に追い込まれる場合もある。2013 年には、車両盗難防止用のイモビライザーの脆弱性に関する論文を国際会議で発表しようとした研究者達が、英国の裁判所に発表差し止め命令を受ける事案が発生している[54]。この研究者達の場合、2 年後の 2015 年に開催された同じ国際会議で、特別講演の形で発表を行うことができた。

このような事情もあり、セキュリティ研究に関する国際会議等では、研究倫理に対する考え方が厳しくなっている。一方、我が国の学術機関では、セキュリティ研究に関する倫理審査に慣れていないところも少なくないのが現状である。この分野の研究を我が国でも活発に行うためには、国際的に通用する審査の手順やガイドラインを整備する必要がある。

６　おわりに

情報社会基盤における事故と攻撃は、20 期提言の頃と変わらず、現在でも依然として大きな問題であり続けている。これらを防ぐ技術、あるいはその被害を軽減する技術は確実に進歩している。しかし、情報社会基盤がより広範に利用され、より複雑化していること、サイバー攻撃に関しては攻撃側の技術がより巧妙となっていることなどから、近い将来において、抜本的解決の目処はたっていない。今後も、防御を強化するための研究開発、専門家の育成と万人向けの教育・啓発を続ける必要がある。

これら従来型の問題の他に、近年では IoT、ビッグデータ、AI が発達し、現在も急速に発達しつつあることから、それに伴う新たな問題も生じている。IoT については、サーバ・クライアント環境で以前に発生していたのと類似の問題も生じている。しかし、安価で非力で大量の機器を、従来と同様の技術で守るのは困難であり、IoT に適合した技術が必要になる。また、それらを組み合わせて重要インフラやライフクリティカルな応用に耐えるソリューションを作り出す技術も必要となる。このような分野では、事故や攻撃による被害が甚大となり、人命を脅かす場合もあるため、一定の規制は必要である。

一方、ビッグデータや AI が発達すると、人間と機械の役割分担に変化が生じる。何を機械に任せるべきか、機械に任せたときの安全性や公平性をいかに担保するか、人間の役割の変化に対応した教育はいかにあるべきか等々の問題を検討する必要がある。このような問題群には唯一の正解があるわけではないため、社会的合意を形成する努力も必要である。これら新しい分野の研究開発や人材育成はまだ緒についたばかりであり、今後大幅に充実させる必要がある。さらに、法整備やマネジメントシステムの開発にも取り組む必要がある。

事故や攻撃については、それを防ぐことに価値があるのは明白であった。一方、20 期提言後には、情報社会基盤がさらに人々の身近な領域に浸透した結果として、パーソナルデータの保護と利活用のように、単純に善悪を判断できない課題も増えてきた。社会の構成員の間で利害が対立しうる問題については、社会全体として受容できる合意点を見出す努力が必要である。しかし、この判断を行うべき人々の意識や常識が、情報技術によって加速された社会の変化に追いついていない現実もある。しかも、より早く合意することで、より早く新しい果実を受け取れることを期待する人々もいれば、自分を取り巻く社会の変化を不安に思う人々もいる。スピードも含めたトレードオフを考え、合意を得る社会的仕組みの構築が重要となる。

このような現在および将来の課題を解決するために研究開発が必要なことは言うまでもない。しかし、社会の安全・安心を深めるための研究活動では、脆弱性に関するデータや個人情報を含むデータの収集・共有が鍵となるケースが多く、研究を円滑に進めるにあたり、制度面でのハードルが高いこともある。公益に資する研究に対し、研究倫理審査体制の整備なども含め、これを円滑に推進できる仕組み作りも求められている。

＜用語の説明＞

○ セキュリティ

本報告では、この用語を情報セキュリティの意味で用いる。ISO/IEC 27000 の定義によると、情報セキュリティとは、情報の機密性（confidentiality)、完全性（integrity)、可用性（availability）を維持することであり、さらに真正性、責任追跡性、否認防止および信頼性の維持を含めてもよいとされる。本報告では、情報そのものだけではなく、情報システムを不正アクセス､乗っ取り､破壊や停止を意図した攻撃等から守ることも含む。次項の「ディペンダビリティ」に比べ、不正アクセスなど悪意の攻撃に対する耐性を表すことが多い。

○ ディペンダビリティ

情報処理国際連合（International Federation of Information Processing, IFIP）の WG 10.4 では、「高い信頼性をもって安全にユーザの望む処理を行う情報システムの能力」（the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers）と定義している。安全性(safety)、信頼性(reliability)､可用性(availability)､完全性(integrity)､保全性(maintainability)などを統合する包括的な概念である。前項の「セキュリティ」に比べ、偶発的な故障などに対する耐性を表すことが多い。

○ IoT（Internet of Things）

日本語では「モノのインターネット」とも呼ばれ、多種多様な「モノ」がインターネットに接続され、相互に情報を交換することで、全体として大量の情報を生成・流通・利用する仕組み。

○ 脆弱性

攻撃等に対する弱点。

○ DDoS（Distributed Denial of Service）攻撃

情報システムのサービスを停止させる攻撃を一般に DoS（Denial of Service）攻撃と呼ぶ。典型的な攻撃手法として、多数のリクエストを送りつけ、当該情報システムを過負荷状態に追い込むものがある。この攻撃を、多数の機器から分散的に行うのが DDoS 攻撃である。

○ DNS（Domain Name System）のサービス

コンピュータ等の機器につけられた www.scj.go.jp のような形式の名前を、数値で表現されたインターネット上のアドレス（IP アドレス）に変換するサービス。

○ ゼロディ攻撃

セキュリティパッチの配布等の対策がまだ取られていない未知あるいは未公表の脆弱性をついた攻撃。

○ セキュリティ要求分析

システムやソフトウェアの新規構築や更新のための開発を行う際に、セキュリティに関して必要な要件を調査・分析・特定する作業。

○ 機能安全

監視や制御を行う装置の機能により安全性を高める（リスクを低減する）考え方。

○ 危殆化

周辺の状況の変化（暗号解読能力の向上や新しい脆弱性の発見など）により、危険性が増大すること。

○ アルゴリズム

問題を解くための手順を形式的に定義したもの。ユークリッドの互除法もアルゴリズムであり、歴史的には、デジタルコンピュータより古くから知られている。しかし、今日では、機械による自動処理を暗に仮定することが多い。

○ 機械学習と訓練データ

人間の学習に近い処理を機械に行わせるもの。学習用の訓練データから、ルール、パターン、判断基準などを学び、その学習結果を用いて、各種の判断や将来予測を行う。近年、深層学習（Deep Learning）の発達により、応用分野が急速に広がりつつある。

○ パーソナルデータ

本報告では、EU における personal data、すなわち個人識別された自然人に関するあらゆるデータという意味で用いる。EU においては、パーソナルデータの保護（protection of personal data）が基本権の一つとされている。

○ 匿名加工情報

個人情報を加工して、個人を識別したり、元の個人情報を復元したりできないようにしたもの。個人情報の提供者から許諾を得ることなく、事業者が第三者に情報の提供を行えるようにするために 2015 年改正の個人情報保護法で導入された。

○ マルウェア

コンピュータウイルスのような悪意を持って作成され、攻撃対象に悪影響を及ぼすソフトウェアの総称。Malicious Software を略したもの。

○ キュレーションサイト

美術館などで作品収集や展示会企画を行うキュレータ（curator）と同様に、インターネットで公開された情報を、ある価値観に従い、選別してまとめた結果を公開するサイト。

○ ページビュー

Web ページが見られた回数。ページビューの多い Web ページ（あるいは Web サイト）の方が少ない Web ページ（あるいは Web サイト）より広告媒体として優れており、広告収入を得やすい傾向がある。

○ ブロックチェーン

分散型で改竄が困難なデータベースの一種。ブロックと呼ばれる単位の連鎖的な構造を作ることで改竄を困難にしているため、ブロックチェーンと呼ばれる。ビットコインの実現技術として有名になった。

○ フィッシング詐欺

典型的には、本物そっくりの偽の Web ページを用いて、騙された被害者が入力したパスワードやクレジットカード情報を搾取する詐欺。

○ 標的型攻撃

特定の個人や組織を狙い撃ちにするタイプのサイバー攻撃。被害者が普段やり取りしているメールとよく似たウイルスつきメールを送りつけるなどの攻撃手法が用いられる。被害者が怪しいと感じにくいこと、同一の攻撃を受ける対象が限定され、セキュリティ対策サービスを提供するベンダーでも入手・解析が困難なことから、一般に防ぐのが難しい。

○ ランサムウェア

感染したコンピュータ上のファイルを暗号化する等の方法でそのコンピュータを使えない状態とし、元に戻すための身代金（ransom）を被害者に要求するマルウェア。

○ Digital Millenium Copyright Act

2000 年に施行された米国著作権法等を改正する法律。

○ 形式検証

曖昧さを排して機械的に扱える表記法でソフトウェア等の仕様を記述し、さらにその仕様からのプログラム自動生成、仕様に照らした設計やプログラムの正しさの自動証明または証明の自動チェックにより、検証を行う手法。

○ データジャーナル

通常の論文ではなく、研究用の（メタ）データを投稿・掲載の対象とする論文誌。

○ レセプト情報

保険診療の診療報酬明細書（レセプト）の情報。2016 年 4 月時点で約 110 億件のレセプト情報を厚生労働省が提供している。

＜参考文献＞

[1] 日本学術会議情報学委員会セキュリティ・ディペンダビリティ分科会，提言 安全・安心社会を実現する情報社会基盤の普及に向けて，2008 年６月 26 日. http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-20-t58-4.pdf

[2] 閣議決定，科学技術基本計画，2016 年１月 22 日. http://www8.cao.go.jp/cstp/kihonkeikaku/5honbun.pdf

[3] 佐々木弘志，ウクライナのサイバー攻撃が示す本当の脅威，McAfee Blog，2016 年１月 27 日. http://blogs.mcafee.jp/mcafeeblog/2016/01/post-748a.html

[4] 和田恭，米国におけるサイバーセキュリティ政策の最近の動向（前編），2013 年４月. http://www.ipa.go.jp/files/000026543.pdf

[5] 内閣サイバーセキュリティセンター，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，2016 年８月 26 日. http://www.nisc.go.jp/active/kihon/res_iot_fw2016.html

[6] IoT 推進コンソーシアム，総務省，経済産業省，IoT セキュリティガイドライン ver 1.0，2016 年７月. http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf

[7] 情報処理推進機構，「つながる世界の開発指針」を公開，2016 年３月 24 日. http://www.ipa.go.jp/sec/reports/20160324.html

[8] 情報処理推進機構，サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ）），http://www.ipa.go.jp/security/J-CSIP/index.html

[9] 閣議決定，世界最先端 IT 国家創造宣言の変更について，2016 年５月 20 日. http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20160520/siryou1.pdf

[10] 閣議決定，日本再興戦略 2016－第４次産業革命に向けて－，2016 年６月２日. http://www.kantei.go.jp/jp/singi/keizaisaisei/pdf/zentaihombun_160602.pdf

[11] 最高裁判例，覚せい剤取締法違反、詐欺、同未遂被告事件，平成９(あ)636，1999 年 12 月 16 日.

[12] 電気通信事業者協会，他，インターネット上の自殺予告事案への対応に関するガイドライン，2005 年 10 月. http://www.telesa.or.jp/wp-content/uploads/consortium/suicide/pdf/guideline_suicide_051005.pdf

[13] 電気通信事業者協会，他，インターネット上の違法な情報への対応に関するガイドライン，2014 年 12 月改定. http://www.telesa.or.jp/ftp-content/consortium/illegal_info/pdf/20141215guideline.pdf

[14] インターネットの安定運用に関する協議会，電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン第４版，2015 年 11 月 30 日. https://www.jaipa.or.jp/other/mtcs/guideline_v4.pdf

[15] マルウェア対策研究人材育成ワークショップ 2016（MWS2016）. http://www.iwsec.org/mws/2016/about.html

[16] 警察庁，平成 27 年中のインターネットバンキングに係る 不正送金事犯の発生状況

等について，2016 年３月３日.
https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf
[17] 瀧口範子，シリコンバレーNEXT 偽記事を取り上げた Facebook のアルゴリズム、人間排除で失態、日経テクノロジーonline，2016 年９月 14 日.
http://techon.nikkeibp.co.jp/atcl/column/15/425482/091300176/
[18] 人工知能学会倫理委員会，「人工知能学会　倫理指針」について，2017 年２月 28 日. http://ai-elsi.org/archives/471
[19] 警察庁，平成 28 年上半期におけるサイバー空間をめぐる脅威の情勢等について，2016 年９月 15 日.
http://www.npa.go.jp/kanbou/cybersecurity/H28_kami_jousei.pdf
[20] 情報処理推進機構，情報セキュリティ 普及啓発資料.
http://www.ipa.go.jp/security/keihatsu/index.html
[21] 日本情報経済社会推進協会，ISMS 適合性評価制度,
https://www.isms.jipdec.or.jp/isms.html
[22] 情報処理推進機構，IT セキュリティ評価及び認証制度（JISEC），
https://www.ipa.go.jp/security/jisec/index.html
[23] 文部科学省初等中等教育局教科書課，「デジタル教科書」の位置付けに関する検討会議 最終まとめ，2016 年 12 月.
http://www.mext.go.jp/b_menu/shingi/chousa/shotou/110/houkoku/1380531.htm
[24] 日本学術会議情報学委員会情報科学技術教育分科会，報告 大学教育の分野別質保証のための教育課程編成上の参照基準 情報学分野，2016 年３月 23 日.
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-h160323-2.pdf
[25] 大学 ICT 推進協議会，情報倫理ビデオ，https://axies.jp/ja/video
[26] 九州大学サイバーセキュリティセンター: 講義. http://staff.cs.kyushu-u.ac.jp/ja/lecture/index.html
[27] enPiT-Security，Basic SecCap コース. https://www.seccap.jp/basic/
[28] 国土交通省，運輸安全委員会の業務，http://www.mlit.go.jp/jtsb/gyoumu.html
[29] 厚生労働省，医療事故調査制度について,
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000061201.html
[30] サイバーセキュリティ戦略本部，日本年金機構における個人情報流出事案に関する原因究明調査結果，2015 年８月 20 日.
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
[31] 日本学術会議情報学委員会国際サイエンスデータ分科会，報告 オープンデータに関する権利と義務 - 本格的なデータジャーナルに向けて -，2014 年９月 30 日.
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-22-h140930-3.pdf
[32] 日本学術会議オープンサイエンスの取り組みに関する検討委員会，オープンイノベーションに資するオープンサイエンスのあり方に関する提言，2016 年７月６日.
http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-t230.pdf

[33] 日本学術会議科学者委員会学術の大型研究計画検討分科会，提言 第23期学術の大型研究計画に関するマスタープラン（マスタープラン2017），2017年２月８日. http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-t241-1-0.pdf
[34] 安全・安心社会を実現するセキュリティ・リスク制御研究機関，計画番号94，in [33]，2017年２月８日. http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-t241-1-22.pdf
[35] 統計センター，オンサイト利用，http://www.nstac.go.jp/services/on-site.html
[36] 厚生労働省，レセプト情報・特定健診等情報の提供に関するガイドラインの改正等について，2016年８月31日. http://www.mhlw.go.jp/stf/shingi2/0000135204.html
[37] National Highway Traffic Safety Administration, http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM483033/RCAK-15V461-4967.pdf
[38] Scott Hilton, Dyn Analysis Summary of Friday October 21 Attack, October 26, 2016. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[39] Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights, May 2016. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf
[40] Department for Business, Innovation & Skills and The Rt Hon Edward Davey: The midata vision of consumer empowerment, November ３, 2011. https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
[41] National Science and Technology Council, Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure, May 2013. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/report_of_the_task_force_on_smart_disclosure.pdf
[42] Drew Springall et al., Security Analysis of the Estonian Internet Voting System, 2014, Proceedings of ACM SIGSAC Conference on Computer and Communications Security (ACM CCS), pp. 703-715, 2014.
[43] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. https://bitcoin.org/bitcoin.pdf
[44] The IEEE Global Initiative for Ethical Considerations in Articial Intelligence and Autonomous Systems, Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Articial Intelligence and Autonomous Systems, December 13, 2016. http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf
[45] Association for Computing Machinery, USACM Issues Statement on Algorithmic Transparency and Accountability, January 12, 2017.

https://www.acm.org/articles/bulletins/2017/january/usacm-statement-algorithmic-accountability
[46] Erik Brynjolfsson, Andrew McAfee, Race Against the Machine: How the Digital Revolution Is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy, Lightning Source Inc, 2011. （訳）村井章子, 機械との競争, 日経BP社, 2013.
[47] Executive Office of the President, Artificial Intelligence, Automation, and the Economy, December 2016.
https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy
[48] Aaron Alva, DMCA security research exemption for consumer devices, October 28, 2016. https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices
[49] Richard Kissel et al., Security Considerations in the System Development Life Cycle, NIST Special Publication 800-64 Revision 2, October 2008.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf（翻訳監修）情報処理推進機構, NRIセキュアテクノロジーズ, 情報システム開発ライフサイクルにおけるセキュリティの考慮事項
https://www.ipa.go.jp/files/000025343.pdf
[50] Michael Howard, Steve Lipner, The Security Development Lifecycle, Microsoft Press, 2006.
[51] United States Computer Emergency Rediness Team, Build Secruity In,
https://www.us-cert.gov/bsi
[52] Tetsuo Tamai, Software Engineering View of a Large-Scale System Failure and the Following Lawsuit, Proceedings of the Second International Workshop on Software Engineering Research and Industrial Practice, pp. 18-24, 2015.
[53] Symantec, Data Sharing,
http://securityresponse.symantec.com/about/profile/universityresearch/sharing.jsp
[54] The Guardian, Scientist Banned from Revealing Codes Used to Start Luxury Cars, July 26, 2013.
https://www.theguardian.com/technology/2013/jul/26/scientist-banned-revealing-codes-cars

＜参考資料１＞審議経過

平成 27 年

３月９日　安全・安心社会と情報技術分科会（第１回）
第 23 期の活動について

８月 31 日　安全・安心社会と情報技術分科会（第２回）
大型研究計画のマスタープランについて
提言について

平成 28 年

１月 12 日　安全・安心社会と情報技術分科会（第３回）
大型研究計画のマスタープランについて
提言について

３月８日　安全・安心社会と情報技術分科会（第４回）
大型研究計画のマスタープランについて
提言について

８月 30 日　安全・安心社会と情報技術分科会（第５回）
意思の表出について
今後の分科会活動について

平成 29 年

１月 12 日　安全・安心社会と情報技術分科会（第６回）
意思の表出について
今後の分科会活動について

３月 28 日　安全・安心社会と情報技術分科会（第７回　メール審議）
報告案「社会の発展と安全・安心を支える情報基盤の普及に向けて」承認

〇月〇日　日本学術会議幹事会（第〇回）
報告「社会の発展と安全・安心を支える情報基盤の普及に向けて」について承認

提言等の提出チェックシート

このチェックシートは、日本学術会議において意思の表出（提言・報告・回答、以下「提言等」という）の査読を円滑に行い、提言等（案）の作成者、査読者、事務局等の労力を最終的に軽減するためのものです。

提言等（案）の作成者は提出の際に以下の項目をチェックし、提言等（案）に添えて査読時に提出してください。

	項目	チェック
1. 表題	表題と内容は一致している。	✔1. はい 2. いいえ
2. 論理展開 1	どのような現状があり、何が問題であるかが十分に記述されている。	✔1. はい 2. いいえ
3. 論理展開 2	特に提言については、政策等への実現に向けて、具体的な行政等の担当部局を想定している（例：文部科学省研究振興局等）。	✔1.部局名：文部科学省研究振興局，経済産業省商務情報政策局，総務省情報流通行政局，内閣サイバーセキュリティセンター 2. 特に無い
4. 読みやすさ 1	本文は 20 ページ（A4、フォント 12P、40 字×38 行）以内である。※図表を含む	✔1. はい 2. いいえ
5. 読みやすさ 2	専門家でなくとも、十分理解できる内容であり、文章としてよく練られている。	✔1. はい 2. いいえ
6. 要旨	要旨は、要旨のみでも独立した文章として読めるものであり 2 ページ（A4、フォント 12P、40 字×38 行）以内である。	✔1. はい 2. いいえ
7. エビデンス	記述・主張を裏付けるデータ、出典、参考文献をすべて掲載している。	✔1. はい 2. いいえ
8. 適切な引用	いわゆる「コピペ」（出典を示さないで引用を行うこと）や、内容をゆがめた引用等は行わず、適切な引用を行っている。	✔1. はい 2. いいえ
9. 既出の提言等との関係	日本学術会議の既出の関連提言等を踏まえ、議論を展開している。	✔1. はい 2. いいえ
10. 利益誘導	利益誘導と誤解されることのない内容である。	✔1. はい 2. いいえ
11. 委員会等の趣旨整合	委員会・分科会の設置趣旨と整合している。	✔1. はい 2. いいえ

※チェック欄で「いいえ」を記入した場合、その理由があればお書きください

記入者（委員会等名・氏名）：

情報学委員会安全・安心社会と情報技術分科会・柴山悦哉

参考：　日本学術会議会長メッセージ、「提言等の円滑な審議のために」(2014 年 5 月 30 日)。

http://www.scj.go.jp/ja/head/pdf/140530.pdf