見解

安全安心なディジタル社会に向けて

令和５年（２０２３年）９月１９日

日　本　学　術　会　議

情報学委員会

ディジタル社会を支える安全安心技術分科会

この見解は、日本学術会議情報学委員会ディジタル社会を支える安全安心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ディジタル社会を支える安全安心技術分科会

委員長	宮地　充子	（第三部会員）	大阪大学大学院工学研究科電気電子情報工学専攻教授
副委員長	高田　広章	（第三部会員）	名古屋大学未来社会創造機構教授
幹　事	岩村　　誠	（連携会員）	NTT セキュリティ・ジャパン株式会社特別研究員
幹　事	松浦　幹太	（連携会員）	東京大学生産技術研究所教授
	馬奈木俊介	（第一部会員）	九州大学大学院工学研究院都市システム工学講座教授
	木村　通男	（第二部会員）	川崎医療福祉大学医療福祉マネジメント学部医療情報学科特任教授
	澤　　芳樹	（第二部会員）	大阪大学大学院医学系研究科保健学専攻未来医療学寄附講座特任教授
	佐古　和恵	（連携会員）	早稲田大学基幹理工学部教授
	佐藤　一郎	（連携会員）	国立情報学研究所情報社会相関研究系教授・副所長
	柴山　悦哉	（連携会員）	東京大学情報基盤センター教授
	須藤　　修	（連携会員）	中央大学国際情報学部教授、中央大学 ELSI センター所長、公益財団法人東京財団政策研究所研究主幹、東京大学大学院特任教授、東京大学名誉教授
	髙木　直史	（連携会員）	京都大学大学院情報学研究科教授
	中尾　彰宏	（連携会員）	東京大学大学院工学系研究科教授
	安浦　寛人	（連携会員）	九州大学名誉教授

本見解の作成にあたり、以下の職員が事務を担当した。

事務	松室　寛治	参事官（審議第二担当）（令和４年７月まで）
	佐々木　亨	参事官（審議第二担当）（令和４年８月から）
	髙橋　直也	参事官（審議第二担当）付参事官補佐（令和５年３月まで）
	柳原　情子	参事官（審議第二担当）付参事官補佐（令和５年４月から）
	石川　絵里	参事官（審議第二担当）付審議専門職付（令和４年 12 月まで）
	池川　教乃	参事官（審議第二担当）付審議専門職（令和５年３月まで）
	藤田　崇志	参事官（審議第二担当）付審議専門職（令和５年４月から）

要　　旨

１　作成の背景

コロナ禍で、必要な情報やサービスを、必要な人が、必要な時に常に受けられることの重要性が明らかになった。つまり、社会活動の効率化や持続可能性につながるディジタル社会の構築が、国や自治体、また個々人にとっても重要であることが明らかになった。本見解では、アナログの「情報」、「もの」や「サービス」から、ディジタル化された「データ」、「モノ」や「サービス」を活用する社会をディジタル社会と考える。ディジタル社会では、紙の郵送や FAX などのアナログ的送付方法が、ディジタル化されたデータのメールなどによる送付に変わるという簡単な事例から、既存の紙プロセスの自動化など、物質的な情報をディジタル形式に変換するディジタイゼーション[1.1.4]、組織の活動をディジタル形式に一新し活用することで、より良い活動を実現するディジタライゼーション、さらには将来の成長、競争力強化のために、新たなディジタル技術を活用して組織・業務モデルの柔軟な改変・新たな創出をするディジタルトランスフォーメーションが実現される。また、ディジタル社会ではコストや時間の大幅な削減やディジタル化された「データ」の機械学習などを用いた各種社会課題の解決なども期待されている。一方で、ディジタル化された「データ」、「モノ」や「サービス」はサイバー攻撃などのセキュリティリスクやプライバシ侵害などの新たな課題を引き起こす。しかしながら、持続可能な社会活動を可能とするため、課題に遮られてディジタル化をためらうのではなく、課題を克服して安全安心なディジタル社会を構築する必要がある。

ディジタル化が進んでいる組織や世代もあれば、遅れている組織や世代もある。重要なことは、ディジタル化が進んでいる組織や世代においても、セキュリティとプライバシを考慮した安全安心なディジタル化が必ずしも構築されているとは言えないことである。さらに、ディジタル社会ではネットワークで様々な組織や世代がつながるため、一部の組織や世代におけるディジタル化の遅れは、セキュリティ上の問題や不公平な社会につながるおそれがある。よって、社会全体としての安全安心なディジタル社会の構築が重要となる。

本分科会では、絶対なる安全はないという前提において、日本社会全体としてのセキュリティとプライバシを考慮した安全安心なディジタル社会の構築に必要な制度構築について検討した。検討結果を踏まえ、政府及び行政、学術研究機関が取り組むべき課題について、見解を述べる。なお、安全と安心は異なり、安全な技術だけでは国民の安心は得られないことをかんがみ、安全と安心の両観点で本見解は記載する。

２　現状及び課題

安全・安心なディジタル化の構築に向けて、大きく４つの問題点が明確になった。第一の問題点は、各組織で安全安心なディジタル化を推進するための人材が不足していることである。第二の問題点は、各種データのディジタル化に伴い、プライバシ保護を考慮したディジタル化の設計が容易でないことである。第三の問題点は、サイバー攻撃のリスク

を抑えながら、日々進化するサイバー攻撃を見据えたディジタル化の設計は容易でないことである。第四の問題点は、インシデント発生時に組織単独での対応が困難な場合にも、情報共有や相互援助が容易でないことである。

３　見解の内容

安全・安心なディジタル社会の推進に向けて、政府及び行政、学術研究機関、産業界が取り組むべき課題について述べる。

⑴　リカレント教育等によるディジタル人員強化の制度構築

個人の学び直しを阻害する要因として、費用、時間、学び直しの意義が指摘されている。本見解では有職者の社内教育と離職者の就業の２つの観点から、政府に対しては、以下の項目の制度構築が必要と考える。

① 職業情報の可視化
② 個人への学び直しの公的支援の充実
③ 企業・教育機関・地方公共団体等の連携による体制整備

また、学術研究機関におけるリカレント教育に対しては、以下の取組が必要と考える。

A) リカレント教育の質を保証する情報の見える化と人材交流
B) カリキュラム改良に関する連携

⑵　プライバシ保護とディジタル社会の両立

プライバシ情報は、個人情報と違い、その保護対象となる情報が不明確であり、リスクや保護方法は利用形態により異なる。本見解では、政府に対しては、以下の項目の制度構築が必要と考える。

① プライバシガバナンス確立の支援
② プライバシ情報に関する共同利用評価機関の設置

また、学術研究機関に対しては、以下の取組が必要と考える。

A)　プライバシガバナンスの確立

⑶　サイバー攻撃を見据えたディジタル社会の設計

企業、地方自治体等でのサイバーセキュリティ対策を阻害する要因として、対策にかかる費用や、対策の効果が見えないことなどが挙げられる。本見解では、政府に対しては、以下の項目の制度構築が必要と考える。

①　サイバーセキュリティ対策への公的支援
②　サイバーセキュリティ対策の可視化

⑷　インシデント情報共有及び援助の仕組みを備えたディジタル社会の設計

サイバー攻撃の複雑化、巧妙化に伴い、被害組織が単独で分析、対策を実施することも難しくなってきており、適切な対処や再発防止の遅れは更なる被害の拡大を招く。政府に対して、以下の項目の制度構築が必要と考える。

①　インシデント情報の共有と運用の推進
②　サイバーセキュリティ関連の人材交流
③　サイバーセキュリティに関する公的支援
④　サイバー攻撃対策の可視化、啓蒙・広報活動

目　　次

１　はじめに

日本学術会議情報学委員会ディジタル社会を支える安全安心技術分科会は、絶対なる安全はないという前提において、安全安心なディジタル社会の構築に向けて日本社会の解決すべき課題を明確にし、政府及び行政、学術研究機関、産業界が取り組むべき課題を明確にする目的で設立された。コロナ禍で、国や自治体、また個々人にとって、必要な情報やサービスを、必要な人が必要な時に常に受けられることの重要性が明らかになった。つまり、社会活動の効率化や持続可能性につながるディジタル社会の構築は必至の社会的課題と言える。実際、学術会議ではディジタル化に向けた提言[1.1.1]、[1.1.2]が提出され、デジタル庁では重点計画が策定された[1.1.3]。

本見解は、絶対なる安全はないという前提のもと、安心できるディジタル社会の構築に向けて、セキュリティとプライバシの学術的な観点から、上記提言を相補的かつ具体的に補完することを目的とする。

本見解では、アナログの「情報」、「もの」や「サービス」から、ディジタル化された「データ」、「モノ」（IoT 機器）や「サービス」（e-Tax など）を活用する社会をディジタル社会と考える。ディジタル社会では、紙を用いたサービスのディジタル化という簡単な事例から、既存の各種サービスのディジタル化、さらには、それらのサービスの自動処理が進められる。ディジタル社会においては，将来の成長、競争力強化のために、既成概念の破壊を伴いながら組織・業務モデルの柔軟な改変・新たな価値を創出するための改革であるディジタルトランスフォーメーションが実現される[1.1.4]。加えて、ディジタル社会は、コストや時間の大幅な削減や、ディジタル化された「データ」は機械学習などを用いた各種社会課題の解決にも不可欠であり、その遅れは日本の成長の妨げにつながる。ディジタル社会の構築は、例えばコロナ禍のようなパンデミック時にも社会活動を継続できるロバストな社会構築の観点で必要である。しかしながら、ディジタル化された「データ」、「モノ」や「サービス」はサイバー攻撃などのセキュリティリスクやプライバシ侵害などの新たな課題を引き起こす。ディジタル化は医療、行政、教育、産業界など各種業界で必要なため、課題に遮られてディジタル化をためらうのではなく、課題を克服して安全安心なディジタル社会を浸透させることに向けた制度構築が必要と言える。

ディジタル社会の構築に向けた取組は一律ではない。組織としての取組は、分野や業界でも異なる。さらに、同じ分野や業界でも組織の規模により異なる。また、各地方公共団体においても取組は異なる。同様に、国民へのディジタル化の浸透も世代により異なる。ディジタル化が進んでいる分野や世代もあれば、遅れている分野や世代もある。重要なことは、ディジタル化が進んでいる分野や世代においても、セキュリティとプライバシを考慮した安全安心なディジタル化が必ずしも構築されているとは言えないことである。近年の情報漏洩、サイバー攻撃の手法を見ると、安全安心の観点での対策はどの組織、世代でも対応が必要と言える。特に、コロナ禍の間に急速に広がった遠隔業務・在宅勤務業務に伴い、本格的なサイバー攻撃の対象が個人にまで広がっている。また、サイバー攻撃は企業規模や業種に関わらずあらゆる産業活動が対象となる[1.1.5]。さらに IoT 機器[1.1.6]や 、ロシアのウクライナ侵攻に伴い、重要インフラにおけるサイバー攻撃の危険性も高ま

っている[1.1.5]。ディジタル社会では、ディジタル化された様々な情報を介してネットワークで様々な組織や世代がつながるため、一部の組織や世代におけるセキュリティとプライバシを考慮した安全安心なディジタル化の遅れはセキュリティホールや不公平な社会になるおそれがある。つまり、社会全体としての安全安心なディジタル社会の構築が重要となる。

本分科会では、医療、行政、地方自治体、教育、産業界など各種業界におけるディジタル社会に向けた取組事例を収集した。この結果、安全安心なディジタル社会の構築には次の４つの問題点への適切な対処が必要であることが明確になった。第一の問題点は、安全安心なディジタル化を推進する人材が不足していることである。人材の補強には、個人の学び直し、そして教育された人材を活用する設計が必要である。第二の問題点は、各種データのディジタル化に伴い、プライバシを保護したディジタル化の設計が組織、団体によっては容易でないことである。第三の問題点は、日々進化するサイバー攻撃を見据えたディジタル化の設計が容易でない組織が存在することである。第四の問題点は、インシデント発生時に単独での対応が困難な組織に対して、インシデントの情報共有や援助を行う制度が不十分であることである。サイバー攻撃の複雑化、巧妙化に伴い、被害組織が単独で分析、対策を実施することも難しく、適切な対処や再発防止の遅れは更なる被害の拡大を招くため、組織を超えた対応が不可欠である。

さらに、上記４つの問題に加えて、安全安心なディジタル社会の構築に必要な２つの重要な問題点について記載する。第五の問題点はディジタル技術及びそれを実現するシステムに対する社会の受容性の低さである。ディジタル環境の進展は非常に速く、ディジタル技術をあらゆるケースに対して検証し、世の中に提供することは現実的ではない。先端的なディジタル技術に対しては，そのメリットと共に、リスク及び利用の過程で技術が改良されるという前提に対する社会受容性の構築が求められる。第六の問題点は安全安心技術に関する研究力の強化が十分でないことである。ディジタル社会の脅威は日々変化し、進化するという現実をかんがみた恒常的な研究力強化は必要である。重要インフラに対するサイバー攻撃や、コロナ禍における医薬業界における知的財産や機密情報を対象にしたサイバー攻撃の増加はまさに国家の安全保障に関わり、恒常的な安全安心技術に関する研究力の強化が求められる。

上述の調査結果に基づき、以上６つの問題点から特に喫緊の４つの課題、(1)リカレント教育等によるディジタル人員強化の制度構築、(2)プライバシ保護とディジタル社会の両立、(3)サイバー攻撃を見据えたディジタル社会の設計、(4)インシデント情報共有及び援助の仕組みを備えたディジタル社会の設計に対して、安全安心なディジタル社会に向けて、政府及び行政、学術研究機関に対して見解を述べる。なお、日本学術会議の報告[1.1.7]で記載されているように、安全と安心は異なり、安心には安全と信頼が必要となる。本見解は安全と安心の両観点で記載する。

本見解では、２章でディジタル社会の安全を支える２大要素であるセキュリティと個人情報・プライバシ情報の保護の課題について述べ、３章ではディジタル社会の現状として、(1)国家事業の事例、(2) 地方事業の事例、また、社会のライフラインの事例として、

2022 年の大阪の医療センターのサイバー攻撃も踏まえて、(3)医療の事例について述べ、４章で安全安心なディジタル社会の構築に向けた見解について述べる。また、社会受容性の参考情報として、ディジタル社会の推進国の一つであるデンマークにおけるディジタル社会の構築状況と国民への恩恵、背景の調査結果を添付する（参考資料２）。

２　ディジタル社会の構築に向けての課題

(1)　ディジタル社会におけるセキュリティの課題

ディジタル社会では、アナログの「情報」、「もの」や「サービス」がディジタル化され、各種サービスの処理効率化や持続可能性が期待されている。しかしながら、ディジタル社会では、ディジタル化された様々な情報がネットワークでつながるため、サイバー攻撃などの被害が絶えない。ディジタル化の進捗状況は組織や個人により異なる。

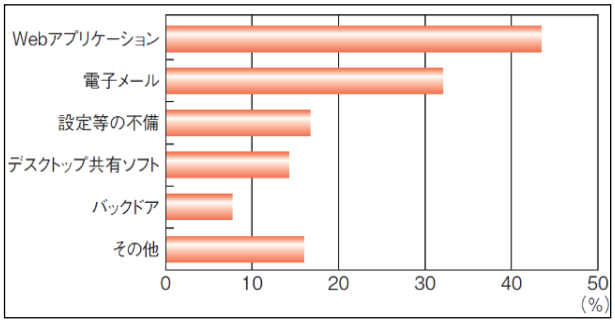

図 2.1.1　情報漏洩／侵害の侵入手口 (2021 年, n=3,279)
（出典）情報セキュリティ白書 2022

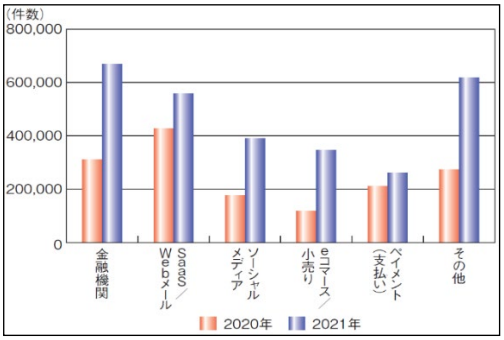

図 2.1.2　業種別のフィッシングサイト件数　(2020 年と 2021 年の比較)
（出典）情報セキュリティ白書 2022

図 2.1.1 の情報漏洩・侵害の手法から、安全安心の観点での対策はどの組織、世代でも対応が必要と言える。コロナ禍で急速に広がった遠隔業務・在宅勤務業務に伴い、あらゆる産業活動から個人に至るまで、サイバー攻撃の対象になっている。ネットワークで様々な組織や世代がつながるため、ディジタル社会におけるセキュリティ対策は必須と言える。

このような背景の下、セキュリティインシデントの情報共有などの取組がされているが、現状、セキュリティインシデントの件数は増えている。警察庁は、2021 年下期のサイバー攻撃の被害報告件数は 2020 年下期の倍と報告している[2.1.2]。また、図 2.1.2、2.1.3 でもサイバー攻撃の件数の増加が見受けられる。以前は、愉快犯によるサイバー攻撃が主な攻撃であったが、近年は、金銭目的による攻撃が増えている（ランサムウェア攻撃など）[2.1.2]。 また、金銭目的によるサイバー攻撃は、米石油供給事業者への攻撃における身代金約５億円の案件[2.1.3]などに見られるように、攻撃専門集団によるものが増えており、一般の民間企業単独では対応するのが難しい。さらに、各組織でのセキュリティ対策には、人的、あるいは、金銭的に厳しい業種もある。

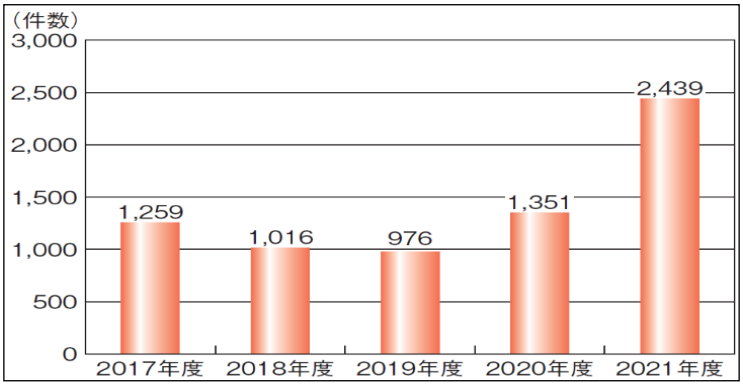

図 2.1.3　Web サイト改ざん年度別件数推移(2017～2021 年度)

（出典）情報セキュリティ白書 2022

(2)　ディジタル社会における個人情報、プライバシ情報の保護の課題

データや各種システムのディジタル化は、収集されたデータの利活用による社会課題の解決と共に、各種サービスの処理効率化をもたらす。その一方で、考慮すべき重要な要素に、データに含まれる個人情報とプライバシ情報の取扱いがある。個人に関わる情報のパーソナルデータには、「個人情報の保護に関する法律」[2.2.1]で保護され

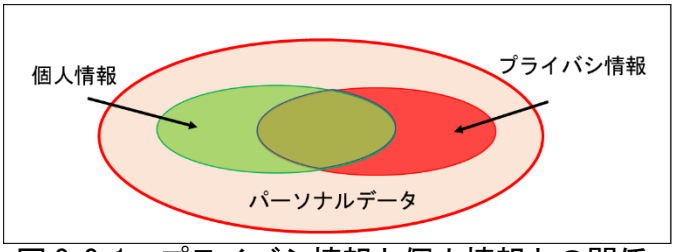

図 2.2.1　プライバシ情報と個人情報との関係

る個人情報（生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの、または個人識別符号が含まれるもの)とプライバシ情報（各個人が干渉・侵害されたくないと考える情報）がある[2.2.2]。個人情報ではないプライバシ情報があることに注意されたい（図 2.2.1)。

ディジタル社会では個人情報とプライバシ情報を適切に扱うことが必要不可欠である。個人情報が漏洩した場合には、業種別の監督官庁に対して、報告を行う必要がある[2.2.1]、[2.2.2]。また、個人情報保護については、利用規定に関するハンドブックが存在する[2.2.3]。一方、プライバシ情報のうち、個人情報とならない情報は、個人情報保護法の対象外である。しかし、個人情報の取扱いは、公法である個人情報保護法の規制に加えて、私法の対象、例えば個人の権利利益の侵害になれば民事訴訟の損害賠償対象になるように、個人情報に該当しないプライバシ情報であっても、個人の権利利益の侵害になれば民事訴訟の対象となる。また、情報技術の発展により、プライバシ情報に関わる個人の権利利益の侵害は起きやすくなっている状況と言える。

現在、データ利活用の必要性は産業分野に留まらない。教育の現場では、教育データの利活用により教育の改善の実現が望まれるし、医療の現場では、医療データの利

活用による難病の解決が望まれる。学術研究機関でも、様々な研究でデータ解析が不可欠になっているが、プライバシ情報の取扱いが障壁になる場合もある。

以上より、事業者も学術研究機関も、個人情報の範囲を超えて、プライバシ情報の保護は避けられない。このような背景のもと、データ利活用に携わる企業に対して、プライバシ情報の取扱いに関するガイドブックが作成されているが[2.2.4]、各組織においてプライバシ情報をどのように取扱うか難しいという課題は残っている。

3　ディジタル社会の実現に向けた取組と課題

国家事業、地方事業、医療におけるディジタル社会の実現に向けた取組事例を述べる。

(1)　国家事業の事例

第６期科学技術・イノベーション基本計画（令和３年３月 26 日閣議決定）では、国民の安全と安心を確保する持続可能で強靭な社会への変革が目標として掲げられ、Beyond 5G、スーパーコンピュータ、宇宙システム、量子技術、半導体等の次世代インフラ・技術の整備・開発の推進が戦略の一つとして定められている。国家が主導するディジタル化は、これらの技術革新に支えられており、その技術の適用では、データの利活用における社会受容性や合意形成のプロセスが課題になることが多い。情報通信の進化により、データを大容量かつリアルタイムで収集し、集めたデータを分析してハイレベルな結果を得る部分は技術的に解決できても、データを集めてそれを活用するという段階で国民の合意形成が難しいなどの問題に直面することが増えている。特に、個人情報に関しては、欧州でデータの扱いに関する規則 GDPR(General Data Protection Regulation)があり、我が国でも個人情報保護法の改正などの議論があり、それが国内外で喫緊の課題となっていることが裏付けられている。

新型コロナウイルス感染症に関して国家が主導し、新型コロナ感染症対策の柱の一つに位置づけられていた新型コロナウイルス接触確認アプリ（COCOA)は、感染した人と濃厚接触をした可能性がある場合に通知が送られてくるアプリであり、ディジタル化の国家事業として最も効果が期待されたディジタル化の事例であろう。2020 年６月 19 日に、厚生労働省新型コロナウイルス感染症対策推進本部とデジタル庁国民向けサービスグループにより運用が始められ、ダウンロード数は 2022 年９月時点で 4055 万件であった。接触確認アプリは、本人の同意を前提に、スマートフォンの近接通信機能(ブルートゥース)を利用して、匿名の電波によりプライバシを確保して、新型コロナウイルス感染症の陽性者と接触した可能性について通知を受けることができる。利用者は、陽性者と接触した可能性を知ることで、検査の受診など保健所のサポートを早く受けることができる。利用者が増えることで、感染拡大の防止に繋がることが期待された。

しかし、河野デジタル大臣は、2022 年９月 13 日の閣議後の記者会見で、COCOA の停止方針を明らかにし[3.1.1]、2022 年 11 月 11 日に、厚生労働省とデジタル庁から COCOA の機能停止が発表された[3.1.2]。厚生労働省の調査によれば、COCOA の運用を始めた時点で動作確認が不十分であったことに加え、厚生労働省に専門的な判断ができる人材が不足しており、頻発する別の不具合の対応や改修に追われ、適切に管理できない状態

にあったことなどが報告されている。また、社会受容性と合意形成のプロセスの不備は、指摘されていなかったが重要な課題である。これは、COCOA が個人情報・プライバシ情報の保護の観点で安全であることの理解が国民に浸透しなかったことに繋がる。COCOA の安全性に関しては、東京大学未来社会ビジョン研究センターの調査では、人によってリテラシーの差異もさることながら、個人情報や匿名情報の利用に関する受け取り方は様々で、間違った知識はマイナス要因、公益の意識がプラス要因になるなどそのバランスに大きな差があることが、十分な技術利用の普及に妨げとなったという結果が出ている[3.1.3]。COCOA に限らず、データを扱う新たな技術の社会実装においては、この観点の課題は大きく今後社会全体で取り組む必要がある。

国家において技術の社会実装を進めるには、工学・情報理工学的な観点に加えて、法学・政治学、公共政策研究、経済学、経営学等の社会科学的な視点、心理学・AI 倫理学などに見られるように人文学も合わせて検討する学際的なアプローチが必要であると思われる。データ利活用に当たっては、プライバシ強化技術活用の制度などに関する合意形成、セキュリティ強化とデータ利活用の両立による災害・少子高齢化などの重要社会的課題解決へのアプローチが求められる。換言すれば、情・理・工・医・社・文の協働による、より包摂的なアプローチが求められるだろう。

(2) 地方事業の事例

我が国におけるディジタル化推進においては、意思決定が早くなされるために、規模が小さい地方事業で前例を作り提示することも重要になる。「経済成長」と「社会の豊かさ」は私たちが求める幸福の主要な要素であり、ICT や AI を活用し統計データに立脚した議論を展開することの重要性は以前から認識され、産学官の取組も進んでいる。近年社会課題の価値化や可視化を行うための指標として期待されているのが、新国富指標（Inclusive Wealth Index）である[3.2.1, 3.2.2]。持続可能な社会のための計測として総合的に評価するために 2012 年に国連によって発表された。2018 年版では健康の価値化、2023 年版では教育の価値化も行われ、経済から環境、健康、教育まで包括的に網羅できる指標になっている。この指標を用い継続的に計測していくことで、施策等を実行する優先順位を明確にすることが可能になると考えられる。最終的には、包括的な成長（Inclusive Growth）を目指すことが重要である。包括的な成長は幸福度の向上や社会課題の解決、つまり新国富を増加することで達成できる。そして、そこには個人情報・プライバシ情報を排除した健康などにまつわる個々のデータを集積する企業の参画も必要になる。自治体は企業に場を提供し、企業はそれぞれの技術や製品を自治体や大学に提供し、自治体や大学がそれらの分析を行い、分析結果を自治体に還元する。ディジタル化が推進されることによって、自治体、企業、大学の連携がよりスムーズになり、幸福度を高め持続可能な社会をつくるための福祉へ貢献できるであろう。

この新国富指標[3.2.1, 3.2.2]による目標があるがゆえに自治体で取組が進んでおり、環境分野では国東市（大分県）[3.2.3]と久山町（福岡県）[3.2.4]、医療分野では中間

市（福岡県）[3.2.5]の事例を紹介する。国東市は 2022 年１月 21 日に国内の自治体で初のカーボンネガティブ宣言を行った[3.2.3]。企業と連携し国の補助も活用し、2025 年までに温室効果ガス排出量等の可視化や評価、カーボンクレジットの仕組みを構築するプロジェクトを進めている。これらの結果を国東市では積極的に活用し、自主的 CO_2 市場を九州大学都市研究センターと一般社団法人 Natural Capital Credit Consortium にて構築し、カーボンネガティブへの取組を進めている。同様に、久山町では、九州大学と九電グループとで 2021 年６月から森林資源を活用したカーボンクレジット創出・活用事業を町有林で実施しており、2028 年度までの８年間で合計約 1,500 トン-CO2 のクレジット創出が予定されている[3.2.4, 3.2.6]。

環境分野における課題は、個人属性データの収集・利用と CO2 排出取引市場の創設にある。まず個人の省エネ行動を促すため、環境省は 2017 年度より日本版ナッジ・ユニット事業を実施している[3.2.7]。ナッジは、一人一人の属性情報や価値観に応じた働きかけを行うため、行動科学の知見（Behavioral Insights）と先進技術（Tech）の融合（BI-Tech）により、IoT でビッグデータを収集し、AI で解析してパーソナライズしたフィードバックを行う[3.2.8]。BI-Tech の例としては、スマートメータやスマートフォンアプリを活用して家庭の電気量を元に省エネレポートの送付や、GPS センサで車両の加減速等を計測・評価するアプリを開発しドライバーの行動変容を促すエコドライブナッジがある[3.2.9]。次に、CO_2 排出取引市場の創設にはブロックチェーン技術の応用が期待されており、環境省は 2018 年度より再エネ CO_2 削減価値創出モデル事業を実施している[3.2.10]。これには再エネの環境価値（属性情報）が分かる点と、消費者同士が直接取引する C2C（Customer to Customer）が可能という二つの特徴があり、情報を見ながらリアルタイムで取引を行うことができる。実証事例としては、米子と川崎の個人宅でのライブデモ P2P（Peer to Peer）実証（2018 年７月）や全国の家庭で創出される再生エネの環境価値をレンタル電動二輪車等の利用者に販売・移転する商用利用がある[3.2.11]。ブロックチェーン技術は、クレジット市場にも民間レベルでも提案されている[3.2.12]。

医療分野では、中間市にウェルビーイング住宅と名付けた医療に特化する建築住宅構想がある[3.2.5]。建築住宅構想では既存の技術を結び付け、家の中で様々なセンサを組み合わせて未病を目指すものである。例えば、心筋梗塞などの事前把握、気付かないうちに徐々に進行するリスクを日常生活の中で継続的に測定することで、早期感知、転倒を防止するといった機能を持つ家屋になる。まず、脳血管疾患・虚血性心疾患、骨折に関するデータ収集から始まり、データ活用については民間 IT 企業も参画する[3.2.13]。医療分野における地域のディジタル課題は医療・健康データの相互連携にあり、日本の医療機関では機関同士のデータ連携が進んでおらず、またライフログ等の健康データも様々な形で収集されているが（例、健康診断、IoT 機器)、データ連携が進んでいない。これに対して、例えば、近年システムの種類に関係なく医療データの連携を可能とするため、HL7（1987 年米国で規格化）が医療データの取扱いに関する国際標準規格・FHIR（Fast Healthcare Interoperability Resources）を開発してお

り、短期間で医療情報を相互運用しデータ単位及びAPIを標準化することが期待されている[3.2.14]。

地域では、地方銀行等金融企業の ESG 投資へ向けての取組も加速している [3.2.15]。情報が少ない非上場企業の SDGs の取組をデータで評価し、地域の企業の持続可能を金融面から支援する仕組みを作った。2022 年８月には、政令都市である北九州市（福岡県）から SDGs 経営を手掛ける企業に補助金を交付する事業の一部業務を受託している[3.2.16]。さらに、民間企業によって地域のサプライチェーンの特性の効果測定まで進んでいる[3.2.17]。

上記の事例は社会受容性が適切に機能したことで、地域住民がディジタル化の恩恵を享受するようになったと考えられる。今後、本見解のセキュリティやプライバシの対応を実施することで、より一層、安全安心なディジタル技術の定着が期待される。

(3) 医療の事例

2007 年以降の厚生労働省、経済産業省、総務省の数多くの補助事業にも関わらず、厚生労働省の 2020 年の調査[3.3.1]によると、近隣の病院・診療所がグループとなって患者情報を開示しあう地域医療情報連携ネットワークは延べ 15,492 の参加医療施設数がある。このうち開示施設がたった一つであるという一方通行のものが 59、初期の自治体からの補助金がなくなった後は、自主財源がないものが 79 と、数件の地域連携以外はあまり利用されていない。一方で、CD、DVD（電子記録媒体もしくは光学記録媒体）では、放射線（等）画像には DICOM 規格が浸透しており、連携は日常となっている。検査結果、処方、保険病名を同一形式で蓄積する SS-MIX ストレージは、2022 年には全国に 1,500 以上広がり[3.3.2]、PMDA（独立行政法人 医薬品医療機器総合機構）の薬剤副作用検出の MID-NET や、上記地域連携で利用されている。しかし、疫学研究、臨床研究、そして新型コロナウイルス感染症対策でも電子カルテのデータが利用しにくいという指摘があった。

医療分野におけるディジタル化を進める利点として、患者にとって１次的には重複検査、重複投薬、重複問診の防止であり、臨床研究、疫学研究のソースとなる点は２次的だが大きなメリットである。その一方で、病院によっては古い仮想の専用回線（Virtual Private Network）を使い続け、サイバー攻撃で身代金が要求された病院の事例もあった[3.3.3]。流出した患者データに対して数億円の要求があるという事例もあった。また、患者にとっては、過去の隠したい病歴が一元化される課題も挙げられる。例えば、日米での市民アンケート[3.3.4]によると、米国では病歴を一元化し生涯カルテにすることに好意的な意見が増えている(2008 46% to 2022 71%)のに対し、患者に病院の選択権のある日本では減っている(2007 76% to 2017 57%)。今後日本でも増加に向けた動きが検討されている。

また、医療分野におけるディジタル化に対する抵抗があることも否めない。インターネットとの接続によるメリットが医療機関にはあまりない。例えば、診療報酬では ICT システムの管理業務コストはインセンティブとして与えられたことはなく、厚生労

働省ガイドライン準拠違反のあった場合のペナルティとして定義されていることも、コスト意識の低下の原因となっている。今後は、外部クラウドや外部の認証システム（例えば保険資格認証システム）との接続は必須となるであろうし、自施設内を守る場合でも職員による不適切なデータ管理などの内なる脅威への対応（教育）が必要となる。つまり、本見解の「ディジタル人員強化の制度構築」で示される、質、量揃ったディジタル人員の充実が医療でも求められる。

医療分野におけるディジタル化の構築では、毎年実施される診療報酬改定対応等の作業効率など、支払基金を含めた診療報酬制度全体にメリットがある。検査の重複防止に加えて、患者にとっての直接的なメリットである重複投薬防止などの医療的メリットを、具体的に提示する必要がある。また、研究、調査にあっては適切な項目の設定も必要である。AAMED（国立研究開発法人日本医療研究開発機構）の大規模研究等では、調査項目が多い研究は登録患者数が少ない傾向がある[3.3.5] 。COVID-19 の全数調査における保健所での入力項目にも同じことが言える。計画立案者が現場の手間、コストを適切に判断することが必要である。

また、医療現場で従事する医療関係者のディジタル化の知識もデータの構造化のリテラシーのレベルまで高める必要がある。

医療分野におけるディジタル化の構築は上述のように容易ではない。一方、画像や検体検査結果は各施設では十分に利用可能なほど標準化・構造化されている。診療報酬の項目も統一化され、日次で把握されている。これら利用され得るデータ種での成果も上がっている（MID-NET、慢性腎臓病 DB など）。ディジタル化が進む分野では、更なるプロジェクトが進むことが望まれる。このように好回転している分野もある。本見解(1) に述べるディジタル人員強化の制度構築の成果が日本全国の医療機関に波及し、受診時の目に見える利得に加えて、医療の質向上に資する分野を広げていくことが、患者、医療、更には国民の、医療におけるディジタル技術の社会受容性につながり、医療におけるディジタル化が進むことに期待したい。

４　安全なディジタル社会構築に向けて取り組むべき課題

本章では、安全安心なディジタル社会の構築に向けて、政府及び行政、学術研究機関が取り組むべき４つの課題、(1)ディジタル人員強化の制度構築、(2) プライバシ保護とディジタル社会の制度構築、(3) サイバー攻撃を見据えたディジタル社会の制度構築、(4) セキュリティインシデントの情報活用と相互援助の制度構築について述べる。また、設計時に考慮すべき課題として (5) ディジタル技術の社会受容性 (6) 研究力強化についても述べる。図 4.1 を用いて、６つの課題がどのように有機的に関与するか説明する。安全安心なディジタル社会の構築に必要な人材を(1)ディジタル人員強化の制度構築で行い、その人材が (2) プライバシ保護とディジタル社会の制度構築、(3) サイバー攻撃を見据えたディジタル社会の制度構築、そして (4) セキュリティインシデントの情報活用と相互援助の制度構築を支える。安全安心なディジタル社会を支える技術であるプライバシ保護とセキュリティ技術に関しては、(2) プライバシ保護とディジタル社会の制度構築と(3)

サイバー攻撃を見据えたディジタル社会の制度構築を行う。現在のサイバー攻撃に対しては、(4) セキュリティインシデントの情報活用と相互援助の制度構築による援助を実施するとともに、提供されるディジタル社会を支える新技術や新制度については(5)ディジタル技術の社会受容性において，国民に安心を与える努力をする。最後に、将来にわたるディジタル社会の安全と安心にむけて(6)研究力強化を実施する。

以下で各課題について詳細に述べる。

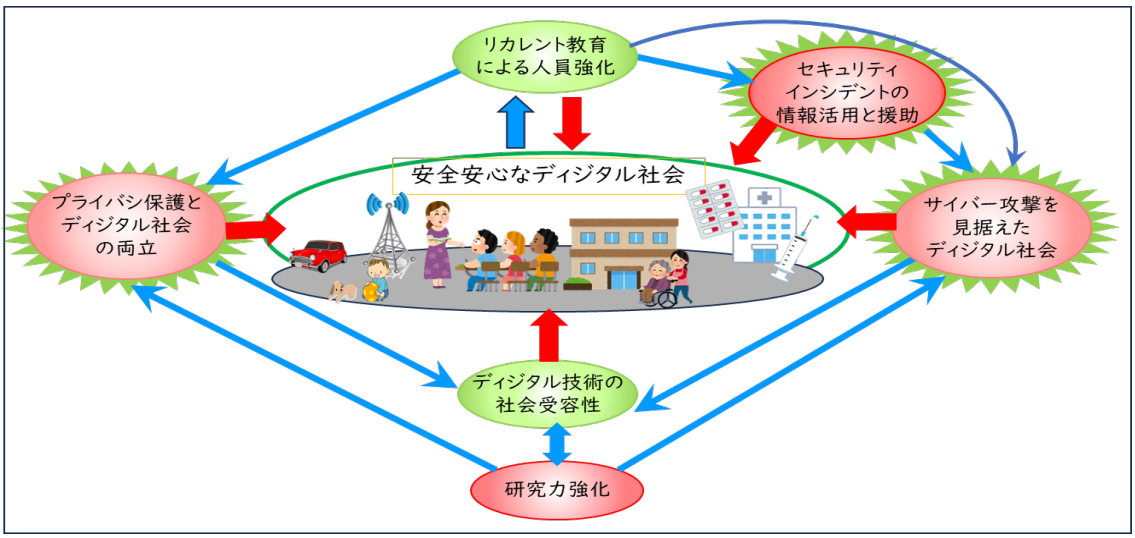

図 4.1 安全安心なディジタル社会の構築に向けて取り組むべき課題

（出典）情報学委員会ディジタル社会を支える安全安心技術分科会にて作成

(1) リカレント教育等によるディジタル人員強化の制度構築

我が国の IT 人材の不足については以前から指摘されているが、社会のディジタル化の進行の中でその需給ギャップは広がっている。ディジタルトランスフォーメーションの取組を進めるに当たっての課題として人材不足を挙げる企業は、我が国においては半数を超えており、海外と比較して高い状況である[4.1.1]。この主な原因として、２つの課題が挙げられる。大学等における IT 関連分野の定員が少ないことと学び直し（リカレント教育）促進の制度構築の遅れである。第一の課題は、情報関連人材における理系学科の出身者は半分程度であり、情報分野を大学等で学んだ人材は 30%程度にとどまることである。教育未来創造会議の第一次提言[4.1.2]においても、これまでの学部・学科の構成を大胆に見直すことが必要とされている。

そこで本見解においては、第二の課題であるリカレント教育の制度構築に着目する。人生 100 年時代の到来に伴い、大学等において学んだスキルだけでディジタル化の加速度的な進展に伴う産業構造の抜本的な変革に対応することは難しく、学び直しによるディジタル人員強化は必至である。閣議決定「経済財政運営と改革の基本方針 2022」[4.1.3]では、ディジタル人材への投資の必要性と学び直し（リカレント教育）促進が挙げられ、教育未来創造会議の第一次提言[4.1.2]では、学び直し成果の適切な評価、学ぶ意欲がある人への支援の充実や環境整備等が挙げられている。しかしながら、我が国においては、リカレント教育が進まない状況がある。我が国の企業は従業員への教育に以前ほど投資しない傾向にあり、個人が自己学習・啓発に取り組まない割合も

海外と比較して顕著に多い。個人の学び直しを阻害する要因として、費用、時間、学び直しの意義が感じられないことが指摘されている。本見解ではこのような状況をかんがみて、政府に対しては、以下の項目の制度構築が必要と考える。

①　職業情報の可視化

職務内容、賃金、雇用見通しなどの職務情報の可視化を進めることにより、個人は希望する職業の職務内容と自己のスキルを比較し、足りないスキルの確認と共に、学び直しによる収入増について確認することが可能である。可視化は学び直しの意義を個人に提供できる。職業情報提供サイト[4.1.4]は米国版[4.1.5]と比べて、具体的な求人情報など改善余地が多い。より分かりやすく詳細な職業情報の提供は、学び直しの意義を個人に与え、学び直しを望む個人の増加につながると考えられる。

②　個人への学び直しに関する公的支援の充実

個人の学び直しには有職者の社内教育の観点と離職者の就業のための学び直しが考えられる。それぞれの場合に対して、費用と時間の両面からのサポートを進める。費用に関しては、専門実践教育訓練給付金が創設されたが、指定講座や地域の多様性など改善の余地は大きい。また、離職者の学び直しに対しては、学習期間中の失業保険の延長や失業保険の受給条件の緩和などの検討の余地もある。一方、有職者に対しては、働きながら教育訓練を受講するための「長期休暇制度」等のガイドラインの策定も重要である。

③　企業・地方公共団体・教育機関等の体制整備

企業や地方公共団体の体制整備では、人的資本投資や学び直し制度を導入する企業等を、情報公開を通じて可視化し、税制や補助金などで優遇することも有効な方策と考えられる。教育機関等の体制整備では、高度なリカレント教育は大学等の実施の必要性が考えられ、教育未来創造会議の第一次提言[4.1.2]においても、大学等におけるリカレント教育の強化に取り組むべきとされている。そのためには、大学等にリカレント教育強化の補助金を出すことも有効であるが、より本質的には、少子化の進行で大学等の規模適正化の必要性が指摘されている中で、リカレント教育を大学等の本来業務の一つと位置付けることで、大学等の自主的な努力を引き出す必要がある。

一方、学術研究機関に対しては、以下の取組が必要と考える。

A)　質保証の見える化と人材交流

リカレント教育の受講者を増やすためには、リカレント教育コース修了者の質保証やその見える化と共に、受講者が社会で評価される仕組みの構築が必要である。さらに、各組織の安全安心なディジタル人材不足の解決にむけて、リカレント教育コースの修了者と人材が必要な組織との交流の構築が重要と考える。

B)　情報交換による継続的なカリキュラム改良実施可能な体制構築

ディジタル技術に対するリカレント教育のカリキュラムは、社会的ニーズに応える必要がある。特に、本見解の (3)、(4) のディジタル技術者への要望を考慮し、情報交換による継続的なカリキュラムの改良を実施可能な体制が必要である。

⑵　プライバシ保護とディジタル社会の制度構築

プライバシに関する情報の利用と保護を両立させるためには、両者が相反するという間違った思い込みを捨てることが第一歩となる。実際、適切なプライバシ保護を行うことで、個人の信頼を得ることができれば、その個人はより詳細な個人情報・プライバシ情報を事業者や学術研究機関に提供してくれる可能性がある。一方で事業者や学術研究機関がプライバシの保護を軽視すれば、個人はその事業者や学術研究機関に対してプライバシに関する情報は提供しない。プライバシの軽視は、プライバシ侵害の被害が起こり得ることのみならず、情報提供を受けられないことにより、事業者の事業を阻害し、学術研究機関の研究活動に深刻な問題をもたらすことになる。

プライバシ情報は、個人情報と違い、その保護対象となる情報が不明確であり、対象が広い。このため、事業者や研究機関がプライバシ情報をすべからく保護しようとすると、事業や研究活動が成立しなくなる可能性がある。また、プライバシ情報の利用形態や保護方法により、プライバシリスクは変わる。したがって、事業者又は研究機関自身が、個人の権利利益の侵害を含むプライバシリスクを明確にして、保護対象及び利用対象となるプライバシ情報を定めること、それらの保護方法及び利用方法を決めてそれを実践することが重要となる。

このことから、事業者も学術研究機関も、保護対象情報や利用対象情報の選別や、その保護方法及び利用方法に関わるプライバシガバナンスが求められる。総務省と経済産業省によるガイドブック [2.2.4]では、①体制の構築（内部統制、プライバシ保護組織の設置、社外有識者との連携)、②運用ルールの策定と周知（運用を徹底するためのルールを策定、組織内への周知)、③企業内のプライバシに係る文化の醸成（個々の従業員がプライバシ意識を持つよう企業文化を醸成)、④消費者とのコミュニケーション（組織の取組について普及・広報、消費者と継続的にコミュニケーション)、⑤その他のステークホルダーとのコミュニケーション（ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション）を求めている。事業者を主な対象として記述されているが、学術研究機関にも応用できると言える。

学術研究機関に関しては、個人情報保護法において、個人情報を学術研究目的に利用する際の適用除外規定が設けられている。2021 年改正個人情報保護法では、個人情報を学術研究目的に利用する際の適用除外では、①利用目的変更の制限の例外に関するもの、②要配慮個人情報の取得の制限の例外に関するもの、③個人データの第三者提供の制限の例外に関するものが制定されたが、これらの適用除外に関する条文には、いずれも「個人の権利利益の侵害の恐れがある場合を除く」という条件が課せられた。つまり、個人の権利利益の侵害の恐れがある場合は、学術研究目的の利用であっても、個人情報は一般の利用と同様に規制されることになる。また、この「個人の権利利益の侵害」の状況とは、憲法 13 条に基づく人権保護の観点で解釈すべきであろう。さらに、学術研究機関等の責務として「個人情報取扱事業者である学術研究機関等は、学術研究目的で行う個人情報の取扱いについて、この法律の規定を遵守するとともに、

その適正を確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。」とある。このため、個人情報に起因する場合に限らず、プライバシ情報も含めて対応する必要があり、上述のガイドブック相当の対応を求められていると考えることできる。

本見解では以上をかんがみて、政府に対しては、以下の項目の制度構築が必要と考える。

① プライバシガバナンス確立の支援

事業者や学術研究機関において、プライバシ保護に関する適切なリスク管理と信頼の確保に向けて、組織全体でプライバシ保護に取り組むための体制であるプライバシガバナンスが確立されるような支援が必要である。

② プライバシ情報に関する共同利用評価機関の設置

小規模な事業者や学術研究機関においては、プライバシガバナンス体制を内部で構築することが難しい場合が多い。その場合は、第三者を含めた評価体制を構築することが望ましいが、中小企業や学術研究機関などが共同で利用できる評価機関が設置されることが望ましい。

一方、学術研究機関に対しては、以下の取組が必要と考える。

A) プライバシガバナンスの確立

学術研究機関が個人情報を学術研究目的に利用する際の適用除外規定は、学問の自由を守るという趣旨に加えて、学術研究機関に対する社会からの信頼を背景にしたものである。社会からの信頼を得る上でも、プライバシガバナンスを率先して確立することが必要である。

(3) サイバー攻撃を見据えたディジタル社会の制度構築

ディジタル社会が進展すると、多くの社会活動や価値ある資産はサイバー空間へ移行することとなり、サイバー攻撃にはこれまで以上に注意が必要となる。昨今、医療やエネルギーといった社会インフラに対するサイバー攻撃により、国民生活に影響が及ぶ状況も現実のものとなってきている。また、取引先企業のサイバー攻撃により、関連するサプライチェーンの事業継続ができなくなるという事件も起こっている。

サイバー攻撃への備えとしては、システムを設計する段階からセキュリティに配慮することや、実装段階のセキュリティ上の欠陥を削減するセキュアコーディング等の取組があり、今後もその重要性が増していくことに疑いの余地はない。ただ、システム稼働前にすべての欠陥を取り除くことが困難であることも認識しておく必要がある。加えて、サイバー攻撃手法は日進月歩で進化しているため、システム開発段階では知られていなかった種類の脆弱性が明らかになり、その対応を迫られるケースもある。こうした状況をかんがみ、システム稼働後もセキュリティ上の欠陥に対処できる体制や仕組みが重要である。特に保守期間終了後も利用可能な買い切りの製品等については、セキュリティ上の欠陥が発覚した際の対応について注意が必要である。これまで、保守期間の終了後にセキュリティ上の欠陥が発見され、製品の利用停止を促すといっ

た事例も報告されており、ディジタル社会の安全を確保するには、こうした利用者へ注意喚起の重要性はますます高まってくるであろう。また不具合を改修した後に、それをシステムに反映する手段も重要である。システムの遠隔更新機能の悪用による攻撃事例も報告されているため、十分に安全に配慮した仕組みが求められている。

システムを活用する側としては、これまで通りシステムの最新化や不要なシステムの停止、撤去の徹底が重要である。一方で、サイバー攻撃の中にはシステムを最新化していても防ぐことができない、未修正のセキュリティ上の欠陥を狙うゼロデイ攻撃も存在する。そのため、サイバー攻撃による被害を前提とした社会活動が重要である。日ごろからシステムを監視することはもちろん、セキュリティインシデントが発生した場合には被害を最小化し、再発防止のために原因を解明する体制を事前に検討しておくことが求められる。

このようにサイバーセキュリティ対策は企業の事業継続性の観点では必至であるが、多くの中小企業等での対策が進んでいない。この理由として、サイバーセキュリティ対策にかかる費用、また対策の効果が見えないことなどが挙げられる。

本見解では以上をかんがみて、政府に対しては、以下の制度構築が必要と考える。

① サイバー攻撃対策の可視化

サイバーセキュリティリスク分析、評価などの技術を保証する資格として、情報処理安全確保支援士がある。企業における情報処理安全確保支援士の人数を可視化するなど、各事業主が実施しているサイバーセキュリティ対策の可視化は重要である。

② サイバーセキュリティに関する公的支援

防衛機密保護に対する税制優遇などが検討されているが、全ての企業においても、セキュリティ対策には費用が発生する。セキュリティ対策を実施した組織への税制優遇など、各企業が積極的にセキュリティ対策を実施する体制作りが必要である。

③　取引先企業を含めたサイバーセキュリティ対策の指導

大企業ではサイバーセキュリティ対策ができつつあるが、サプライチェーンを構成する中小企業におけるセキュリティ対策が不十分であるという課題がある。大企業に対して、関連するサプライチェーンの企業におけるサイバーセキュリティ対策の指導を行う体制が必要である。

⑷　セキュリティインシデントの情報活用と援助の制度構築

セキュリティインシデントが発生した際、適切な対処や再発防止を講じないと更なる被害拡大を招く。しかし、セキュリティインシデントには、その原因が一つの組織に留まらず被害組織だけでは全容解明が困難な場合がある。これを解決するためには、サイバーセキュリティ関係組織等とセキュリティインシデントに関する情報を共有することが重要となる。また、ある組織でのセキュリティインシデントに関する情報は、他の組織におけるセキュリティ対策にも直結するため、被害組織のみならず社会全体にとっても有益となる。一方で、セキュリティインシデントに関する情報には、組織の機密や評判に関わる情報が含まれており、情報共有を妨げる要因となっている。例

えば、サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会[4.4.1]では、セキュリティ対策や再発防止に必要な技術情報と、組織の機密や評判に関わる情報を選別し、前者の情報が円滑に共有される仕組みの検討が進んでいる。また、サイバーセキュリティ協議会[4.4.2]では、行政機関、社会基盤を提供する事業者、サイバー関連事業者等の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報の迅速な共有を行っている。情報共有の際には、罰則により担保された高度な守秘義務、法律に規定された情報提供義務等により、機微な情報の共有を目標としている。また、一般社団法人 ICT-ISAC [4.4.3]では、会員企業、団体のサイバー攻撃に関する情報を踏まえ、送信元特定のための調査研究を進めることで、電気通信事業者と連携して、攻撃通信の発生を電気事業者が防止する取り組みを進めている。ICT-ISAC 以外に、金融 ISAC、電力 ISAC、Software ISAC、J-Auto ISAC WG、医療 ISAC、日本貿易会 ISAC、交通 ISAC などの情報共有の組織が設置されている。運用状況は各業界によって異なり、J-Auto ISAC は一般社団法人 Japan Automotive ISAC に組織変更を行っている。このような、業界団体ごとのより一層の情報共有を進めるために、情報共有することのインセンティブやセキュリティインシデント発生時の共有可能な情報の選別判断基準を示すこと、さらに、共有された情報を適切に運用することや、情報共有が実施できていない業界の扱いは、今後の課題と言える。

サイバー攻撃の複雑化、巧妙化に伴い被害組織が単独で分析、対策を実施することも難しくなってきている。このような時には、他組織からのサイバー攻撃に対する援助が重要になる。独立行政法人情報処理推進機構（IPA）では、中小企業を対象にサイバー攻撃への対処として不可欠なサービスを実現する「サイバーセキュリティお助け隊サービス」制度を推進している。これにより、人材や資金が限定的な中小企業に対して、効果的かつ安価なセキュリティ対策の提供が試みられている。しかしながら、IPA による「2021 年度中小企業における情報セキュリティ対策に関する実態調査」[4.4.4]に見られるように、このような活動に対する認知度は、非常に低い（中小企業の情報セキュリティ対策ガイドライン　14.1%、SECURITY ACTION　5.8%、サイバーセキュリティお助け隊サービス　4.1%）。アンケートには、業界基準の制定、業界団体の呼びかけの必要性も指摘されている。サイバー攻撃は、国民に対しても課題になっており、警察庁がサイバー犯罪相談窓口を設置する等、サイバー攻撃に関する公的な取組はいくつか存在している。しかしながら、こうしたサイバーセキュリティに関する取組に関して、国民の認知度がかなり低いという問題がある。

上記のように数々の取組がされているが、現状では、このような取組が適切に活用されていない中小企業や各種地方公共団体等の組織が存在する。

本見解では以上をかんがみて、政府に対しては、以下の制度構築が必要と考える。

①　インシデント情報の共有と運用の推進

業界によってはインシデント情報の共有が進められているが、インシデント情報の中には、組織にとっての機密情報や保護を要する情報が含まれていることがあり、十分な情報共有と運用は必ずしも実現されていない。その守秘義務や情報提供義務に

関する法制度等の整備が重要と考える。また、情報共有ができていない業界への働きかけが求められる。

② サイバーセキュリティ関連の人材交流

セキュリティインシデントを未然に防ぐためには、攻撃の予兆を捉えて先んじて対策を講じることも重要である。それには様々な組織が連携し、人材交流により、サイバー攻撃に関連する情報の共有などを推進していく必要がある。

③ サイバーセキュリティに関する公的支援制度

ディジタル化の進展と共にサイバー攻撃が社会に与える影響は大きくなっており、IT との関りが少なかった個人や組織がサイバー攻撃による被害を受けることも増加するであろう。ディジタル社会の安全・安心を実現するためには、サイバー空間における国民生活の安全・安心を守る行政や、被害を受けた際に公的支援を受けられる制度の整備が重要になると考えられる。

④ サイバー攻撃対策の可視化、啓蒙・広報活動

サイバーセキュリティに関する取組に関して、国民の認知度は低い。内閣サイバーセキュリティセンターは、毎年２月１日～３月 18 日をサイバーセキュリティ月間として、サイバーセキュリティに対する国民の関心・理解を高める取組を実施している。こうした活動を更に推し進めることで、多くの国民が警察や消防・救急の連絡先を把握しているように、サイバー攻撃発生時の相談窓口等の知名度を向上させるように啓蒙していくことが肝要である。

(5) ディジタル技術の社会受容性

我が国におけるディジタル化の遅れの要因の一つとして、ディジタル技術及びそれにより実現するシステムに対する社会の受容性の低さが挙げられる。社会受容性には経済原理など様々な要素が考えられるが、ここでは、セキュリティとプライバシなどの安全安心の観点からの社会受容性について考える。

ディジタル化の推進のためには、利用者（国民）にディジタル化のメリットを十分に説明すると共に、セキュリティ脅威、個人情報漏洩、プライバシ侵害等についての懸念を低減し安心感を与えることが重要である。一般に、新たな技術、例えば AI などの利活用では、FATE（Fairness、Accountability、Transparency、Explainability)、つまり、公平性、答責性又は説明責任、透明性、そして説明可能性又は解釈可能性という観点が重要であると言われている。合意形成のプロセスが難しいということは、同時にアカウンタビリティ、つまり問題が起きた時の責任の明確化も重要である。また、上記の FATE は、技術の提供側がどのような観点に留意するべきかを規定しているが、前述のように、利用者（国民）の心情は本来制御不能であり、社会実装された技術を使う利用者（国民）側を巻き込んで社会受容性を高める、サービス提供側と受益側の渾然一体のコミュニティ運用が課題となると考えられる。

学術的な観点からは、技術だけではなくその利用の社会受容性の考慮、合意形成のプロセスをコミュニティで考えるという学際的なアプローチが必須であることは言う

までもない。先端技術の研究開発を担う学術研究者は、今のように技術を開発した後で受容性を考えるというアプローチではなく、不完全・不正確であったとしても、可能な限り個人情報・プライバシ情報を取得せずに目的を達成する技術を開発するなど先見の明を持つことが必須である。

一方、社会科学・法学・政治学・公共政策を専門とする学術研究者は、先端技術の研究開発を専門とする学術研究者と連携し、新たな技術の利用に関するルール作りを考えていく必要がある。また、学術だけではなく、産業界・官界や技術の利用者（国民）を含めて、社会の仕組みを一体で考える「包摂性」が今後の国家のディジタル化の推進には必須だろう。

セキュリティ対策としては、「サイバーセキュリティ基本法」[4.5.1]に基づき、国の行政機関及び独立行政法人等の情報システムの開発・運用に関して、「政府機関等のサイバーセキュリティ対策のための統一基準群」[4.5.2]が定められている。また、地方自治体も情報システムの開発・運用に関してガイドラインを定めている。個人情報については、「個人情報保護法」[2.2.1]が３年ごとに検討、必要に応じて改正されることになっており、個人情報保護委員会が「個人情報保護法についてのガイドライン」[4.5.3]を制定している。ディジタルシステムの開発・運用、収集した個人情報の扱いにおいて、これらの基準やガイドラインを遵守することはもちろんであるが、ディジタルシステムの開発・運用がこれらの基準やガイドラインを遵守して行われていることを利用者（国民）に説明し、安心感を与えることも重要である。基準やガイドラインを遵守しても 100%安全であることはあり得ない。インシデントが発生し、利用者に不利益が生じた場合の救済措置や補償についても基準を定め、予め利用者（国民）に説明することが重要である。

今後、ディジタルシステムの開発において、迅速性・適応性を重視し、早期に実践投入を行って利用者に素早く価値を届け、投入後に改善を行うアジャイル開発（工程を機能単位の小さなサイクルで繰り返す開発手法）が重要となる。システムをアジャイル開発する際には、利用者（国民）に、初期に実践投入されたシステムが完全なものではなく、利用者（国民）からのフィードバックによって改善されるものであることを受け入れてもらう必要がある。一方で、初期に実践投入されたシステムにおいて重大なインシデントが発生すれば、その後いくら改善しても利用者（国民）の信頼を得られない恐れがあるので、初期システムにおいて許容されるリスクの設定が必要であり、リスクを利用者（国民）に説明し、理解を得ることが重要である。

ディジタル化を推進するためには、利用者（国民）のガイドラインに従って開発・運用されるシステムを受容する態度、アジャイル開発を受容する態度を涵養することが重要である。具体的なプロセスとしては、パブリック・インボルブメント、ワークショップ、中等教育における問題認識の深化などが挙げられ、これらを活性化する施策が必要である。デンマークの成功事例を参考資料２に示すが、日本に適合しているかは検討が必要である。

以上をかんがみて、政府及び学術研究者に対し、次の項目が必要と考える。

① ディジタル化の必要性とリスクの可視化

ディジタル化の推進のためには、利用者（国民）にディジタル化のメリットを十分に説明するとともに、セキュリティ脅威、個人情報漏洩、プライバシ侵害等についての懸念を低減し安心感を与えることが重要である。

② 技術とその利用に向けた合意形成プロセスの構築

技術の提供だけではなく、その利用に対する社会受容性、合意形成のプロセスを構築することまで踏まえた施策が必要である。

(6) 研究力強化

ディジタル社会における脅威は、変化し、進化する。よって、現時点での防御が不十分な場合はもちろん、例え十分そうな場合でも、安全安心なディジタル社会を推進するためにはセキュリティとプライバシに関わる研究が不可欠である。また、脅威だけでなく、防御側も変化するということを忘れてはならない。実際、本見解で扱っているようにディジタル社会の推進を図るということは、IT の利活用が広がるなどして使う側も変化するということである。利活用が広がれば、直接関わる利害関係者も増え、多様になる。これは、プライバシに関係する問題が示唆しているように、工学などの自然科学だけでなく人文・社会科学的な研究もまた重要であることを意味する。

研究力強化を論じる時に大切なのは、このように異なる利害関係者に目を配り、現状だけでなく将来の変化を見据えた戦略を練ることである。例えば、政府のサイバーセキュリティ戦略本部が 2021 年５月に公表した「サイバーセキュリティ研究開発戦略」（改訂）[4.6.1]は、「環境の変化を踏まえ、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として、研究開発戦略専門調査会における議論を通じて策定」するというプロセスを経て作成された。同戦略における「ビジネスのプロセス全体を視野に入れることが重要」「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」「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」といった知見がこうしたプロセスの結果として指摘された、ということに留意したい。

研究力の強化には、研究者が安心して最先端の研究に取り組める環境の整備が必要である。例えば、倫理的な研究プロセスの普及啓発活動は日本学術振興会サイバーセキュリティ第192委員会（当時）の「サイバーセキュリティの研究倫理を考えるWG」からの支援(2018年～2020年)を基にして、進められている[4.6.2]。この活動では、「前例が十分にない倫理的領域を取り扱う機会が出てきた」ことを重く見て、「ステークホルダ(利害関係者)の明確化、インパクトの見積もり、リスクの最小化努力、Responsible disclosure(研究成果の社会的な影響を考慮して、事前に必要な手続きを踏んだ後、研究成果を開示すること)を実施し、自身の研究を研究倫理的観点から実践して論じることの必要性が高まってきている」という認識のもと、実際の学会における研究者からの相談受付窓口の設置運用など、具体的な取組がなされている。こういった国内の環境整備は、当該分野における国際競争力に良い影響を与える可能性がある。

一方、投資や、投資対象となる人や組織の行為に関する適正利用についての科学的なアプローチとして、例えば情報セキュリティ経済学がある[4.6.3]。そのトップコンファレンスには 20 年以上の歴史があり、一つの研究コミュニティが形成されている[4.6.4]。先の「サイバーセキュリティ研究開発戦略」（改訂）[4.6.1]においても、当該分野における研究の科学的基礎の一つとして「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」が挙げられている。様々な意思決定や制度構築に関して、単に持論を主張するのではなく、中立的で客観的な論を科学的に展開することが益々重要になるだろう。

折しも、令和３年４月に施行された「科学技術基本法等の一部を改正する法律」により、「人文科学のみに係る科学技術」が科学技術基本法の対象に加えられた。第６期科学技術・イノベーション基本計画で ELSI（Ethical、 Legal and Social Issues）に関して明示的に言及されたことも注目されるなど[4.6.5]、人文・社会科学を科学技術・イノベーション政策の中に明確に位置づける流れがある。なお、この法改正を受け止める際に、学術の健全な発展を展望し「人文科学の特徴である『リフレクティブ・キャパシティ（オルタナティブを構想するための社会の知的奥行き）』を働かすべき」という指摘がある[4.6.6]。安全安心なディジタル社会に向けての取組においても、人文・社会科学との協働や合意形成を考慮し、かつ実効性のある展開が求められよう。

以上をかんがみて、政府、学術研究機関及び学会に対し、次の項目が必要と考える。

①　柔軟かつ時宜を考慮した研究戦略の立案

ディジタル社会における脅威は、変化し、進化する。環境の変化を踏まえた柔軟かつ迅速な研究戦略を立案することが重要である。

②　倫理的な研究プロセスの普及啓発活動の推進

研究者が安心して最先端の研究に取り組める環境整備の構築には、政府及び学会の対話を重視した倫理的な研究プロセスの普及啓発活動を推進することが必要である。これらの取組がセキュリティ分野の我が国の国際競争力向上につながると考える。

５　まとめ

本見解では、絶対なる安全はないという前提において、安全安心なディジタル社会の構築に必要な制度構築について検討し、政府及び行政、学術研究機関が取り組むべき課題とその解決方針について見解を述べた。特に、４つの問題点への適切な対処が必要である。

第一の問題は、人材不足である。この問題への対策として、リカレント教育のインセンティブ向上につながる職業情報の可視化や、費用と時間の両面で公的支援を充実させることが重要である。そして、対策の有効性を高めるために、異種セクタで連携した体制を整備することが求められる。企業等におけるリカレント教育投資の促進及び大学が質を保証したリカレント教育を提供することと、それを本来業務として推進できるようにする施策が、特に有効性を高めるであろう。

第二の問題は、プライバシ保護とディジタル化の両立である。各ステークホルダーがプライバシ保護に関する正しい認識を持つことが、まず必要である。その上で、対策として、プライバシガバナンスの確立の支援や、プライバシガバナンスに関する客観的な評価を受けられるよう組織内あるいは外部に適切な仕組みを確保すること、また、確保できるような施策を力強く推進することが有効である。

第三の問題は、日々進化するサイバー攻撃への対応である。システムの設計段階からセキュリティに配慮することと、それでもシステム稼働前に全ての欠陥を取り除くことはできないので製品やサービスのライフサイクルをセキュリティの観点でよく考えることが、まず必要である。その上で、対策として、サイバー攻撃に備えた取組状況の可視化や、業種に依らない公的支援や指導の充実が有効である。

第四の問題は、インシデントの情報共有や組織を超えた援助を可能とする制度が設計されていないことである。この問題への対策として、情報共有に係る適切な機密保護がなされることと、情報共有のインセンティブが付与されること、それらを担うサイバー攻撃対策人材の交流が有効である。また、必要な時に相談や通報をする連絡先等の情報を可視化し普及させることによって、必要な対応をより迅速かつ的確にできるようになり、ディジタル社会が浸透した際の安心感が格段に高まると期待される。

さらに、上記４つの問題に加えて、安全安心なディジタル社会の構築に必要な２つの重要な要素についても記載する。第五の問題は、ディジタル技術及びそれを実現するシステムに対する社会の受容性の低さである。ディジタル環境の進展は非常に速く、構築されたディジタル技術をあらゆるケースに対して動作検証を実施してから、世の中に提供することは現実的ではない。先端ディジタル技術に対しては，メリットと併せ、リスクを広く国民に周知すると共に、利用の過程で技術が改良されるという運用に対するリスクの社会受容性の構築が求められる。第六の問題点はディジタル社会の脅威は日々変化し、進化するという現実の下での、安全安心技術の研究力の強化の必要性である。ロシアによるウクライナ侵攻後に大幅に増えた重要インフラに対するサイバー攻撃や、コロナ禍における医薬業界における知的財産や機密情報を対象にしたサイバー攻撃の増加はまさに国家の安全保障に関わり、恒常的な安全安心技術の研究力の強化が求められる。

安全安心なディジタル社会の課題解決に向けて、適切な可視化や情報共有、第三者評価、人材交流等の社会ネットワークすなわち異なるステークホルダーの結び付きを通じて強化され、セキュリティとプライバシが真にソーシャル・キャピタルとして定着することが重要といえる。安全を高めることは安心を高めることにつながるが、本見解の制度構築の要素として取り上げた可視化や情報共有、第三者評価、人材交流等は安心を促すと同時に、安全を高めることにもつながる。なお、ディジタル化による社会課題の解決や新たな価値の創造に、セキュリティとプライバシだけが重要というわけではない。だからこそ、ディジタル社会における社会効率の効果を考慮し、様々なステークホルダーの対話を進めながら、上述の問題を解決する社会ネットワークと関連制度を設計することで、安全安心なディジタル社会を構築することが重要である。

＜参考文献＞

[1.1.1] 日本学術会議心理学・教育学委員会・情報学委員会合同教育データ利活用分科会、提言「教育のデジタル化を踏まえた学習データの利活用に関する提言 -エビデンスに基づく教育に向けて-」、2020 年９月 30 日.

[1.1.2] 日本学術会議第二部大規模感染症予防・制圧体制検討分科会情報学委員会ユビキタス状況認識社会基盤分科会、提言「感染症対策と社会変革に向けた ICT 基盤強化とデジタル変革の推進」、2020 年９月 15 日.

[1.1.3] デジタル庁「デジタル社会の実現に向けた重点計画」、2023 年６月９日.
https://www.digital.go.jp/policies/priority-policy-program/#document

[1.1.4] 総務省 令和３年版 情報通信白書、 2021 年７月.
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd112210.html

[1.1.5] 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/policy/group/infra/index.html

[1.1.6] 内閣府 IoT 社会に対応したサイバー・フィジカル・セキュリティ推進委員会
https://www8.cao.go.jp/cstp/gaiyo/sip/iinkai2/cybersecurity.html

[1.1.7] 日本学術会議総合工学委員会・機械工学委員会合同工学システムに関する安全・安心・リスク検討分科会、報告「工学システムに対する安心感と社会」、2020 年８月 25 日.

[2.1.1] IPA 情報セキュリティ白書 2022、 2022 年７月 15 日.
https://www.ipa.go.jp/security/publications/hakusyo/2022.html

[2.1.2] 「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」(警察庁)、2022 年４月７日.
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

[2.1.3] THE WALL STREET JOURNAL, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, May 19, 2021.
https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

[2.2.1] 個人情報の保護に関する法律
https://elaws.e-gov.go.jp/document?lawid=415AC0000000057

[2.2.2] JIPDEC プライバシーマーク制度
https://privacymark.jp/wakaru/kouza/theme1_03.html

[2.2.3] 個人情報保護委員会、「民間事業者向け 個人情報保護法ハンドブック」、2022 年４月.
https://www.ppc.go.jp/files/pdf/APPI_handbook_for_company2022.pdf

[2.2.4] 経済産業省、総務省、「DX 時代における企業のプライバシーガバナンスガイドブック ver1.2」、2022 年２月 18 日.
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000140.html

[3.1.1] NHK 政治マガジン、2022 年９月 13 日.

https://www.nhk.or.jp/politics/articles/lastweek/89057.html
[3.1.2] https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html
[3.1.3] 渡部俊也, 平井祐理、「データ提供における懸念点と公益貢献意識効果の影響: COCOA 利用に関する質問票調査から」、日本知財学会誌、18(3)、29-38、2022 年３月 20 日.
[3.2.1] Managi, S., Kumar, P. Inclusive wealth report 2018: Measuring progress towards sustainability. Routledge, London, 2018 年７月 24 日.
https://doi.org/10.4324/9781351002080
[3.2.2] Managi, S., Keeley, A. R., & Takeda, S., Policy Briefs T20 for the Presidency of G20 in 2022, The G20 Insights Platform, Global Solutions Initiative Foundation, An Inclusive Evaluation Framework for Sustainable Investment, 2022, available online (https://www.global-solutions-initiative.org/policy_brief/an-inclusive-evaluation-framework-for-sustainable-investment/ accessed on December 11, 2022)
[3.2.3] 大分県国東市、国東市カーボンネガティブ宣言～温室効果ガス排出実質マイナスをめざして～、2022 年１月 21 日.
https://www.city.kunisaki.oita.jp/uploaded/attachment/18621.pdf
[3.2.4] 九州電力、「森林資源を活用したＪ－クレジット創出・活用事業」を開始します－福岡県久山町にて事業の実行性・有効性を実証－、2021 年６月 22 日.
https://www.kyuden.co.jp/press_h210622-1.html
[3.2.5] 九州大学、「新国富指標」を活用したまちづくりに福岡県中間市と連携、2020 年 12 月 15 日. https://www.kyushu-u.ac.jp/ja/topics/view/1638
[3.2.6] 九州電力、福岡県久山町での「森林資源を活用した Jークレジット創出・活用事業」についてプロジェクト登録申請が承認されましたー創出した Jークレジットをカーボンオフセットに活用ー、2022 年７月１日.
https://www.kyuden.co.jp/press_h220701-1.html
[3.2.7] 環境省、日本版ナッジ・ユニットを発足します！～平成 29 年度低炭素型の行動変容を促す情報発信（ナッジ）による家庭等の自発的対策推進事業の採択案件について～、2017 年４月 14 日. https://www.env.go.jp/press/103926.html
[3.2.8] 環境省、成長戦略・統合イノベーション戦略・AI 戦略等の政府方針に位置付けられた BI-Tech（バイテック）について（ナッジ関連）、2019 年７月５日. https://www.env.go.jp/press/106977.html
[3.2.9] Kurokawa, H., K. Igei, A. Kitsuki, K. Kurita, S. Managi, M. Nakamuro, and A. Sakano. ″Improvement Impact of Nudges Incorporated in Environmental Education on Students’ Environmental Knowledge, Attitudes, and Behaviors″, Journal of Environmental Management 325, Part B, 116612, 2023 年１月１日.
[3.2.10] 環境省、平成 30 年度ブロックチェーン技術を活用した再エネ CO2 削減価値創出モデル事業の公募について、2018 年１月 30 日.
https://www.env.go.jp/press/105059.html
[3.2.11] 環境省、「ブロックチェーン技術を活用した再エネ CO2 削減価値創出モデル事業」

における成果の社会実装・商用利用に向けたC2C取引プラットフォーム実証の開始について、2019年８月26日. https://www.env.go.jp/press/107117.html
[3.2.12] ナチュラルキャピタルクレジットコンソーシアムへの参画について～独自ブロックチェーン技術を活用し、カーボンクレジット市場を活性化～、ジャスミー株式会社、2022年12月16日.
https://prtimes.jp/main/html/rd/p/000000047.000025296.html
[3.2.13] 株式会社インクルーシヴシティ. https://www.inclusivecity.co.jp/
[3.2.14]厚生労働省、HL7 FHIRに関する調査研究の報告書、2020年３月.
https://www.mhlw.go.jp/stf/newpage_15747.html
[3.2.15] 株式会社サステナブルスケール. https://www.s-scale.co.jp/
[3.2.16] 株式会社サステナブルスケール、～北九州市SDG－Xリーディングプロジェクト補助金～審査基準にSustainable Scale Indexが採用されることについて、2022年８月31日. https://www.s-scale.co.jp/pdf/20220831_ssnews.pdf
[3.2.17] aiESG https://urban-institute.kyushu-u.ac.jp/aiesg
[3.3.1] 厚生労働省、地域医療情報連携ネットワークの現状について、2021年
https://www.mhlw.go.jp/content/10800000/000683765.pdf
[3.3.2] SS-MIX普及促進コンソーシアム、http://www.ss-mix.org/cons/
[3.3.3] https://www.yomiuri.co.jp/national/20211126-OYT1T50244/
[3.3.4] Kimura M、 Watanabe H、 Surveys Aimed at General Citizens of the US and Japan about their Attitudes toward Electronic Medical Data Handling - 10 Years Change、Before and After Covid-19、 2022年10月26日、 Studies in Health Technology and Informatics (accepted、 in press).
[3.3.5] http://j-ckd-db.jp/
https://jdreams.jp/category/contributions/
[4.1.1] 情報処理推進機構:「IT人材白書2020」、2020年８月31日.
[4.1.2] 教育未来創造会議: 「我が国の未来をけん引する大学等と社会の在り方について（第一次提言)」、 2022年５月10日.
[4.1.3] 閣議決定: "経済財政運営と改革の基本方針2022"、 2022年６月７日.
[4.1.4] Job Tag (日本版 O-NET)
https://shigoto.mhlw.go.jp/User/
[4.1.5] O*NET OnLine
https://www.onetonline.org/
[4.4.1] サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html
[4.4.2] サイバーセキュリティ協議会
https://www.nisc.go.jp/council/cs/kyogikai/index.html
[4.4.3] 一般社団法人ICT-ISAC https://www.ict-isac.jp/outline/
[4.4.4] 情報処理推進機構「2021年度 中小企業における情報セキュリティ対策に関する

実態調査」、2022年３月31日.
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html
[4.5.1] https://elaws.e-gov.go.jp/document?lawid=426AC1000000104
[4.5.2] https://www.nisc.go.jp/policy/group/general/kijun.html
[4.5.3] https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/
[4.6.1] サイバーセキュリティ戦略本部: “サイバーセキュリティ研究開発戦略（改訂)”、2021年５月13日.
[4.6.2] マルウェア対策研究人材育成ワークショップ: “サイバーセキュリティ研究における倫理的な研究プロセスについて、 http://www.iwsec.org/mws/ethics.html (accessed on July 21、 2022)
[4.6.3] Ross Anderson and Tyler Moore: “The Economics of Information Security、Science、 Vol.314、 Issue 5799、 pp.610-613、 2006年10月27日.
[4.6.4] Alessandro Acquisti、 Ross Anderson、 Rainer Böhme、 L. Jean Camp、 Lawrence Gordon、 Martin Loeb、 Kanta Matsuura、 and Andrew Odlyzko: “WEIS at 20 Years”、Panel discussion at the 20th Annual Workshop on the Economics of Information Security (WEIS 2021)、 2021年６月29日.
[4.6.5] 科学技術振興機構研究開発戦略センター: “ELSI からRRI への展開から考える科学技術・イノベーションの変革－政策・ファンディング・研究開発の横断的取り組みの強化に向けて－”、 CRDS-FY2021-RR-07、 2022年３月.
[4.6.6] 中村征樹: “科学技術基本法改正と人文・社会科学”、 学術の動向、 Vol.26、No.5、 pp.36-41、 2021年５月１日.

○＜参考資料２＞デンマークの事例
以下[5.4.1]から[5.4.4]については、参考資料２の参考文献。
[5.4.1] Department of Economic and Social Affairs、 United Nations: “E-Government Syrvey 2020: Digital Government of Action for Sustainable Development with Addendum on COVID-19 Response”、2020年７月.
https://publicadministration.un.org/en/Research/UN-e-Government-Surveys
(accessed on August 26、2022)
[5.4.2] Keegan McBride: “Sailing towards digitalization when it doesn’t make cents? Analysing the Faroe Islands’ new digital governance trajectory”、 Island Studies Journal、 Vol.14、 No.2、 pp.193-214、 2019年11月.
[5.4.3] 安岡美佳: “電子政府と強制力―電子政府の進捗にいかに強制力が活用されたか―”、 Nextcom、 Vo.47、 pp.22-31、 2021年９月１日.
[5.4.4] 科学技術振興機構 研究開発戦略センター: “The Beyond Disciplines Collection―デジタルトランスフォーメーションに伴う科学技術・イノベーションの変容”、 CRDS-FY2020-RR-01、 2020年４月.

＜参考資料１＞審議経過

2021 年

１月 13 日 ディジタル社会を支える安全安心技術分科会（第１回）
今期の活動計画に関する論議

３月 31 日 ディジタル社会を支える安全安心技術分科会（第２回）
木村通男（浜松医科大学医学部附属病院医療情報部・教授）、馬奈木俊介（九州大学大学院工学研究院・教授）より話題提供及び議論

７月 12 日 ディジタル社会を支える安全安心技術分科会（第３回）
澤芳樹（大阪大学大学院医学系研究科・名誉教授）、楠正憲（政府 CIO 補佐官）より話題提供及び議論

９月 13 日 ディジタル社会を支える安全安心技術分科会（第４回）
後藤厚宏（情報セキュリティ大学院大学・教授）、佐藤一郎（国立情報学研究所・教授）より話題提供及び議論

12 月 14 日 ディジタル社会を支える安全安心技術分科会（第５回）
松元照仁（地方公共団体情報システム機構（J-LIS）・理事）、小山 覚（エヌ・ティ・ティ・コミュニケーションズ株式会社 情報セキュリティ部・部長） より話題提供及び議論

2022 年

３月 14 日 ディジタル社会を支える安全安心技術分科会（第６回）
野原 佐和子、馬奈木 俊介、安岡 実佳、楠 正憲、後藤 厚宏より話題提供および議論

５月 23 日 ディジタル社会を支える安全安心技術分科会（第７回）
見解に関する議論

７月６日 ディジタル社会を支える安全安心技術分科会（第８回）
佐藤 一郎（国立情報学研究所情報社会相関研究系 教授）中澤 恵太（文部科学省高等教育局専門教育課 企画官）より話題提供及び議論

10 月３日 ディジタル社会を支える安全安心技術分科会（第９回）
見解に関する議論

10 月 28 日 ディジタル社会を支える安全安心技術分科会（第 10 回）
見解に関する議論

2023 年

１月 10 日 ディジタル社会を支える安全安心技術分科会（第 11 回）
見解に関する議論

４月７日 ディジタル社会を支える安全安心技術分科会（第 12 回）
見解に関する議論

７月 28 日 ディジタル社会を支える安全安心技術分科会（第 13 回）
見解に関する議論

８月 25 日 科学的助言等対応委員会承認
見解「安全安心なディジタル社会に向けて」

＜参考資料２＞デンマークの事例

ディジタル化推進に際し、他国の事例から学ぶことも重要である。１つの着眼点として電子政府に関する国際的なランキングを参照すべく、国際連合が、概ね２年に１度発表している調査報告書の2020年版[5.4.1]を見ると、上位10カ国のうち６カ国が欧州の国々である。ここでは、その中でも最上位に位置するデンマークの事例に着目したい。

デンマークをはじめとする北欧諸国のディジタル化成功要因として小国であるという点が強調されることがあるが、費用対効果等を考えると、小国であることは必ずしもディジタル化に有利ではない[5.4.2]。そこには、むしろ困難を克服した成功要因として、政府による強制力が有効に機能した背景があった[5.4.3]。具体的には、民主主義国家において政府が何かを強制的に実施するとネガティブに捉えられがちであるにも関わらずデンマークのディジタル化で強制力が有効に機能した理由が、４つ考えられている。１つ目は、長期的な取組や戦略的な政策実施によって、市民にある種の義務感を浸透させたことである。例えば、政府と市民との間のコミュニケーションに関するディジタル化には 11 年ほどが費やされており、公共機関への導入から段階を踏んで実施されてきた。また、個人番号の利用は、1968 年の住民登録法改正に遡り、50 年以上かけて現行のシステムへと進化している。この間、広報が戦略的に行われ、必要性と共に免除事項（身体的・精神的な理由による免除）も明示され、免除対象となる超高齢者らへの対応にコストをかける（優先的に対応する人員を配置する）という姿勢が見せられた。こうして「やらざるを得ない」「やるべきである」という意識が醸成された、という見方である。同様に、２つ目の理由として、長い時間をかけて確立されてきた政府への信頼感が挙げられている。３つ目の理由は、使い勝手への配慮である。すなわち、電子政府が提供するサービスやアプリのユーザビリティとアクセシビリティの高さであり、それを支えた開発体制である。実際、設計の初期段階でデザインを専門とするコンサルタントと連携して当事者や現場理解に時間がかけられるという参加型設計によって仕様が定められた。また、電子化庁にはユーザーエキスペリエンスやユーザーインターフェースの専門家が雇用され、行動経済学等の科学的な知見を採用して使い勝手の向上が図られたという。４つ目の理由は、IT の利用に困難を感じる人に対する友人や家族らによるインフォーマルなサポートである。すなわち、同国で高齢者らの IT リテラシーがもともと高かったなどということはなく、市民側でも弱者をサポートすることが大切という指摘である。ただし、前提条件として、最初の３つの理由（市民の義務感、政府への信頼感、システムの使い勝手の良さ）があってこそ身近な人によるサポートが可能になる、と分析されている。

EU は、2015 年５月にディジタル単一市場戦略（Digital Single Market Strategy：DSM）を発表し、その中間評価（2017 年５月）では、今後更なる取組が必要な３つの分野として、「データエコノミーの最大限の活用」「サイバーセキュリティ強化による欧州の資産保護」「オンラインプラットフォームの推進」が特定された[5.4.4]。既にランキング上位に位置する地域においてこれらの取組が充実した場合にどうなるか、注視する必要があるだろう。

＜参考資料３＞用語の説明

ESG 投資：投資家が企業の株式などに投資する時、投資先の価値を測る材料として環境(Environment)、社会 (Social)、企業統治(Governance)に関する取組を考慮する投資のこと。

アジャイル開発：ディジタルシステムの開発において、迅速性・適応性を重視し、早期に実践投入を行って利用者に素早く価値を届けるべく工程を機能単位の小さなサイクルで繰り返す開発手法。早期投入後に改善を繰り返し行う。

（セキュリティ）インシデント：情報セキュリティに関する事故や事件。情報セキュリティに関するということが文脈から明らかでない場合にはセキュリティインシデントといい、明らかな場合には単にインシデントという。

環境価値：「大気中の二酸化炭素を増加させない」といった環境の観点で見た付加価値のこと。

データ意味構造：文章表現では説明が困難な複雑な因果関係を明らかにできるように、あるいは、効率的な検索が可能となるように、データを適切に表現する構造。

フィッシングサイト：一般ユーザを騙して誘導し、ID やパスワード、クレジットカードに関する情報等の重要な情報を詐取する目的で設置された、偽物の Web サイト。

プライバシ強化技術：プライバシ保護の原則を実現・強化する技術の総称。プライバシを保護しながら、データ共有と分析を可能にする。

ブロックチェーン技術：ネットワーク上に分散した多くの端末に、取引や処理の記録を安全に追記していく技術。端末同士のやり取りは、特定の管理サーバを介さず、直接行われる。ブロックと呼ばれる単位でデータが取りまとめられ、それが時間順に鎖のように連結されていく。

ライフサイクル：人の誕生から死までの過程を円環状の図（サイクル）で表現したもの。転じて、ビジネスの分野で、製品やサービスなどが生まれてから消えるまでの全ての過程のこと。さらに狭義に、情報セキュリティ分野においては、防御対象が生まれてから消えるまでの全ての過程のこと。

ライブデモ P2P 実証：参加者がリアルタイムで情報を見ながら、個人間で直接取引する仕組みを実際に使うことができると実証すること。