

令和5年度
安全・安心に関するシンクタンク機能育成事業
事業項目①：国内需要動向調査
報告書



令和6年（2024年）2月29日

中央大学

本報告書は、内閣府の科学技術振興調査等委託費による委託業務として、学校法人中央大学が実施した令和5年度「安全・安心に関するシンクタンク機能育成事業（事業項目①：国内需要動向調査）」の成果を取りまとめたものです。

従って、本報告書の著作権は、内閣府に帰属しており、本報告書の全部又は一部の無断複製等の行為は、法律で認められたときを除き、著作権の侵害にあたるので、これらの利用行為を行うときは、内閣府の承認手続きが必要です。

安全・安心に関するシンクタンク機能育成事業（事業項目①：国内需要動向調査）
実施者一覧

氏名	所属
大貫 裕之	中央大学大学院 法務研究科 教授、常任理事
佐藤 信行	中央大学大学院 法務研究科 教授、副学長
加藤 俊一	中央大学 工学部ビジネスデータサイエンス学科 教授、副学長
庄司 裕子	中央大学 工学部ビジネスデータサイエンス学科 教授
難波 英嗣	中央大学 工学部ビジネスデータサイエンス学科 教授
大倉 典子	中央大学 研究開発機構 機構教授
久徳 康史	中央大学 研究開発機構 機構教授
浜田 百合	中央大学 研究開発機構 機構助教
加藤 徳子	中央大学 研究開発機構 専任研究員

目 次

1	はじめに.....	1
2	調査方法.....	2
	(1) サーベイ.....	2
	(2) ヒアリング.....	2
	(3) アンケート.....	3
	① 心理測定学に基づく測定.....	4
	② 古典的テスト理論と信頼性、妥当性について.....	4
3	サイバーセキュリティ.....	7
	(1) サーベイ.....	7
	① 前提としてのサイバーセキュリティとデータセキュリティの関係.....	7
	② サーベイ対象設定の枠組み.....	8
	③ 現行法上の枠組みから見たニーズに係る文書の所在と概要.....	9
	④ 特に重要又は特徴的な機関及び文書の分析結果.....	10
	⑤ 政策課題とニーズの整理.....	15
	(2) ヒアリング.....	18
	① 東京大学情報基盤センター教授.....	18
	② 中央大学研究開発機構准教授.....	19
	③ 中央大学研究開発機構教授.....	20
	④ 横浜中央法務事務所 司法書士.....	22
	⑤ 関係府省庁.....	23
	(3) アンケート.....	24
	① 調査1.....	25
	② 調査2.....	27
	③ 調査3.....	28
	④ アンケートからの考察.....	29
	(4) 考察.....	31
4	食料安全保障.....	34
	(1) サーベイ.....	34
	① 基本的な問題・根源的なニーズ.....	34
	② 政策面からの根源的なニーズの分類・整理.....	39
	③ パブリックコメントからみる国民のニーズ意識.....	46
	(2) ヒアリング.....	47
	① 東京農工大学 特別招聘教授.....	47
	② 共立女子大学教授.....	49
	③ 日本女子大学准教授.....	50
	④ 関係府省庁.....	51

(3) アンケート.....	52
① 調査1.....	52
② 調査2.....	54
③ 調査3.....	56
④ アンケート結果に対する考察.....	56
(4) 考察.....	57
5 まとめ.....	61
<参考文献>.....	63
<参考資料1> サイバーセキュリティサーベイ.....	67
<参考資料2> デジタル社会の実現に向けた重点計画等からみた政策課題と技術ニーズ	70

1 はじめに

本報告書は、令和5年度「安全・安心に関するシンクタンク機能育成事業（事業項目①：国内需要動向調査）」の成果をまとめたものである。

2 調査方法

ここでは、全体の方法論の大枠について説明し、個別の方法論は第3章と第4章に記載する。

我が国の経済安全保障に関わる様々なニーズとその構造を明らかにし、それらのニーズに応えるための政策のあり方、特に、技術開発や技術利用に関する政策を展望するための手順を確立するために、本調査では、大枠として以下の手法を試行することとした。

初めに、現状で経済安全保障に必要と認識され、現行の政策でも対応されている、あるいは、対応の必要性が検討されている顕在的なニーズを整理するために、関係府省庁から出されている公開文書を中心にサーベイを行う。顕在的なニーズ群とそれらの相互の関係を分析しつつ、これらを全体的に俯瞰する観点の抽出を試みる。

顕在的なニーズとその構造、全体を俯瞰する観点を踏まえて、各分野への専門家への半構造化形式でのヒアリング調査を行う。これらのニーズ群の背後にある問題点のあぶり出しを通じて、また、現行では検討の進んでいない課題の指摘などを受けて、これからの経済安全保障に必要となりそうな潜在的なニーズの抽出を試みる。

また、並行して、広範な専門家や、経済安全保障の受益者である国民・産業界を対象としたアンケート調査を行う。サーベイやヒアリングから抽出した顕在的・潜在的ニーズの妥当性を確かめるとともに、各ステークホルダの考え方・観点を抽出する。

これらの調査を踏まえて、経済安全保障に資する政策のあり方、特に、技術開発や技術利用に関する政策のあり方についての考察を行う。

(1) サーベイ

本調査では、「サイバーセキュリティ」と「食料安全保障」を個別調査テーマとして、経済安全保障上、必要と認識され、現行の政策でも対応されている、あるいは、対応の必要性が検討されている顕在的なニーズをサーベイにより抽出し整理する。主たる所管の府省、あるいは、関連府省庁から出されている公開文書のうち、直近の約5年間の公開文書を中心にサーベイを行う。通例、各府省庁では約5年ごとに政策の見直しが行われており、現行の政策に直結している公開文書であり、また、近年、急速に我が国を取り巻く安全保障上の情勢が変化しつつあることに鑑み、直近5年間の公開文書の範囲でも適切に調査・分析できると判断した。

また、顕在的なニーズ群とそれらの相互の関係を分析しつつ、これらを全体的に俯瞰する観点の抽出を試み、これを専門家へのヒアリングのベースとしても利用することとする。

(2) ヒアリング

2023年12月から2024年2月にかけて、対面又はオンラインでヒアリングを行う。ヒアリング対象は、関係府省庁や専門家で、その目的は、サイバーセキュリティあるいは食料安全保障において国レベルでのリスクマネジメントを可能にするために、政策的課題及びニーズを明らかにすることである。ヒアリングは半構造化形式で行い、主に以下

の項目について伺う。

1) **重要度・優先度の高い政策課題・ニーズについて**

- 我が国のサイバーセキュリティ（又は食料安全保障）に関して、特に深刻となっている脅威・リスクや喫緊の政策課題・ニーズは何でしょうか？
- それら課題等に対処し、又はニーズを満たすためにどのような対策・取組（技術開発以外も含む。）を実施又は検討していますか？

2) **潜在的な政策課題・ニーズについて**

- 現在は顕在化・深刻化していないが、昨今のトレンド等を踏まえれば、今後（数～数十年後）顕在化・深刻化する可能性のある脅威・リスクや政策課題・ニーズはありますか？
- それら課題等に対処し、又はニーズを満たすためにどのような対策・取組（技術開発以外も含む。）を実施又は検討していますか？

3) **実施・支援している技術開発の取組について**

- 我が国のサイバーセキュリティ（又は食料安全保障）の確保・向上に資する特定の技術の開発を実施又は支援していますか？
- 実施・支援を行っている場合、当該技術はどのような政策課題・ニーズに対応しますか？
- 技術開発に当たっての課題（特に技術的課題）はありますか？

4) **その他**

- 被害にあった個人や組織の事例で印象的だったものはありますか？
- これまでお話しいただいた内容の中で、特に優先度の高い課題があれば教えてください。
- 諸外国のサイバーセキュリティ（又は食料安全保障）対策について、参考となるものがあれば教えてください。

ヒアリングの結果は、文字起こしののち、質的データの分析手法である M-GTA (Modified Grounded Theory Approach) [2. 2. 1] のツールである MAXQDA [2. 2. 2] を用いて解析を行う。

(3) **アンケート**

2023年12月から2024年2月にかけて、「プライバシーマーク®」認定に基づくシステムを持つ調査会社を利用し、オンラインアンケート調査を行う。プライバシーマーク制度により、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者委託する。研究対象はサイバーセキュリティあるいは食料安全保障の関連業務従事者や利用者とし、情報技術や食品技術に対する受容度と拒否感に関連する心理概念を明らかにし、政策的課題及びニーズを明らかにすることである。古典的テスト理論に基づき

信頼性・妥当性が科学的に検証された精度の高いアンケートを用い、心理概念を定量化する。アンケートの方法の詳細に関しては、参考文献[2.3.1]の心理測定学(Psychometrics)に基づく安心の測定に用いたのと同じ手法であり、ここに再掲する。

① 心理測定学に基づく測定

安心を測定するためには、心理測定学を用いたアプローチが有用であろう。心理測定学とは心理の測定に関し、科学的な測定をするために必要となる態度や手法を体系化した学問のことを指し、100年以上の歴史を有する。具現的な現象を観測することができる自然科学とは異なり、心理の測定においては心理測定学に基づき、抽象的な心理特性を観測値が反映していることを確かめる必要がある[2.3.2]。心理特性の測定では、複数の質問項目(Item)から構成される質問票(Questionnaire)に、回答者自身で「1.全くあてはまらない～5.とてもよく当てはまる」などの選択肢を5段(5件法)階から9段階(9件法)などの多項値で、自身の状態にもっとも当てはまる回答をしてもらう。項目の合計点若しくは項目平均点(合計点÷項目数)を算出し尺度化(数値化・定量化)することが一般的である。測定段階が細分化されていると、必ずしも精度が高くなるわけではなく、回答者になるべく正確に回答できる段階数が望ましい。

5件法や7件法、9件法で測定された質問票の各質問項目自体は順序尺度(Rank-order Scale)であり、連続変数(Continuous Variable)とはみなされない。そこで、複数項目から構成され、選択肢が概ね等間隔だとみなせるようなリッカート尺度(Likert Scale)を用いる。この場合、複数項目の合計点や項目当たりの平均点は間隔尺度(Interval Scale)とみなされ定量的変数(数値)として扱うことができる。ただし、質問票を用いた測定では常に測定誤差が含まれるため、尺度の信頼性(尺度内の質問項目の安定性や一貫性の程度を示す指標)や妥当性(測定すべき心理特性が測定されている程度を示す指標)を用いて検証を行う必要がある[2.3.3]-[2.3.9]。以下でこれらの指標について簡単に説明をする。

② 古典的テスト理論と信頼性、妥当性について

古典的テスト理論(Classical Testing Theory: CTT)は、各個人の心理特性には真の値が存在すると仮定する。測定された心理特性の値は、この真値(True Score)とのズレが生じるため測定誤差(Measurement Error)が含まれている(式1)[2.3.10]。

$$\text{測定値} = \text{真値} + \text{測定誤差} \quad \dots \text{式1}$$

1) CTTに基づく信頼性について

測定値の分散に対して真値の分散が占めている割合のことを信頼性(Reliability)と呼ぶ(式2)。また、信頼性の平方根は真値と観測値の相関に相当する。

信頼性＝真値の分散/測定値の分散・・・式2

信頼性の検証には安定性、若しくは一貫性を定量的に検証する方法がとられる。

まず、安定性については複数回測定をした際の安定性の検証について話をします。例えば、体重計の表示する値が不安定であっては、体重の測定値を信用することはできない。同様に心理特性に関しても回答者に複数回調査を実施し、測定値間の相関係数を用いて検証する。この手続を再テスト法 (Test-retest Reliability) と呼ぶ。この際、以前の回答が後の回答にバイアスを与えることを防ぐ目的で、同等の質問票や試験を作成し、その質問票や試験との相関係数を検証する平行テスト (Parallel Forms Reliability) 法を用いることが望ましい。しかし、多くの場合同等の質問票を複数作成することは難しく、現実的ではない。例えば、全く同じ難易度の国語の試験を複数作成しようとしても、多少は難易度が異なってしまふ。

このような障壁の多い複数測定を避け、一度の測定で質問票や試験内の一貫性により信頼性を検証する方法が用いられることも多い。例えば、折半法 (Split-half Reliability) では、質問票や試験内の項目を2グループに分け、スピアマン＝ブラウンの公式 (Spearman-Brown Formula) を適用した上で、2グループ間で補正された相関が高いことを検証する方法である。しかし、項目をグループ分けする方法は多種存在するため、分け方によっては結果が異なることも考えられる。例えば学力試験などの場合、前半の問題が比較的容易で、後半の問題が難しくなる場合がある。その場合は前半と後半で質問項目をグループ分けすることにより正答率が異なり、バイアスが生じるおそれがある。そのため、各項目の関係性を総当たりで検証する内的整合性の指標としてクロンバックの α (Cronbach's α) がある。これは信頼性の下限となる指標であり、0から1までの値をとり、Tavakol & Dennick [2. 3. 14] により.70 から.95 の間の値をとることが推奨されている。上限が設定されている理由としては、同じような内容を聞く質問項目が重複して使われていることを避けるためでもある。例えば、「疲れている」や「疲労感がある」のようにほぼ同じ内容の質問をしていると、項目間の相関が高くなり、本来の一貫性より、値を高くみせかけることもできてしまう。

2) GTTに基づく妥当性について

妥当性 (Validity) に関しては、主なものとして内容的妥当性 (Content Validity)、基準関連妥当性 (Criterion Validity)、構成概念妥当性 (Construct Validity) があげられる [2. 3. 6]。内容的妥当性は専門家などにより、質問票内の項目が測定対象である主観を反映している程度を表す。定性的検証であるため、質問票や試験の作成段階で用いられるべき指標である。例えば、安心感を尺度化する際に心理学の専門家が質問項目の内容が安心感を反映しているかを検討する。基準関連妥当性は、「不安症群の安心得点が不安症ではない群より有意に低い」といった、明確な外部基準 (External Criterion) をもとに定量的な検証を行う方法である。しかし、明確な外

部基準自体が存在しない心理特性も多いため、それに対応して 1950 年代以降に構成概念(Construct)という考え方が広まった。構成概念妥当性は、明確な外部基準がない場合に安心感尺度が理論や仮説通りの働きをするか定量的に検証する方法である。例えば、理論や先行研究により安心感が高い場合はストレスが少なく、ウェルビーイングが高い傾向があることが考えられるとする。その場合、安心感はストレスと負の相関、ウェルビーイングとは正の相関がみられることが考えられる。これらの関係性を総合的に検証する指標が構成概念妥当性である。

3) 信頼性・妥当性以外に考慮すべき点

質問票として用いられる尺度には、信頼性や妥当性だけではなく、使い勝手と効率のよさが望まれる[2.3.9][2.3.11]。また、項目の困難度(Item Difficulty)や弁別性(Item Discriminability)も適切である必要がある。困難度とは、試験の問題であれば正答率のことを指し、質問票では平均点のことを指す。尺度内の他の項目と比較して値が低い項目は、困難度が高いおそれがある。弁別性については、試験の問題であればその項目に正答した受験者群が誤答した受験者群より合計点が高い場合、能力を弁別できているとみなせる。質問票では、ある項目とその項目を除いた他の項目の合計点に相関（修正済み項目合計相関：Corrected Item-total Correlation）がある場合、心理特性の弁別力が高いと言える。弁別力が低い項目は質問票や試験の真値を測定しているとは言い難い。このように、複数項目からなる質問票により回答を得て、信頼性、妥当性、使い勝手の良さ、効率性、適切な困難度と弁別性などが高いと認められたものが心理尺度として、心理特性を測定し数値化に用いることができる。

これらの質問票の内容自体だけではなく、質問する順序により、後の回答が影響を受けないように、質問票や試験をランダム順に測定することや、項目をランダムに測定するなどの調査デザインを工夫することも必要である。紙媒体を用いるなどの理由でランダム化できない場合は質問票や試験の項目を入れ替えた複数のパターンを作成し、順序効果が無かったことを検証した上で解析をする必要がある。そして、不正回答がないようにストレートアンサー（例えば、ずっと「どちらでもない」を回答する）がないことを確認することや、トラップ設問を設ける必要がある。

3 サイバーセキュリティ

本章では、サイバーセキュリティを対象に行ったサーベイ、ヒアリング、アンケート調査の結果について記載し、その結果から考察する。

(1) サーベイ

サイバーセキュリティに関する諸課題は、政府の政策のみならず、企業活動や国民生活の様々な面に深くかかわっており、様々な府省・組織・団体・個人から関連する資料・情報も多数発信されている。

企業活動からの情報発信にも見るべきものは多いと考えられるが、個々の企業の利害というバイアスがかかっている可能性もあり、また、いわゆる多国籍企業や海外資本に多くを依存する企業からの情報発信は、我が国の経済安全保障との整合性の面でも路線が異なる可能性もある。

したがって、本調査の「サイバーセキュリティ」に関するサーベイも、日本社会におけるサイバーセキュリティ確保の重要な担い手であり、かつ、民主制原理の下で相当程度に体系的な情報公表を行っている関係府省庁の公開文書を対象として、サイバーセキュリティに係る既知のリスクとニーズを整理することを行う。なお、対象とした公開文書の一覧は<参考資料1>に掲載する。

① 前提としてのサイバーセキュリティとデータセキュリティの関係

サイバーセキュリティについては、サイバーセキュリティ基本法（平成26年法律第104号）第2条が定義するところ、それは「電子的方式、磁気的方式その他の知覚によつては認識することができない方式…により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体…を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること」というものである。

この定義からは、サイバーセキュリティを次の要素に分解することができる

- (ア) 電磁的方式で記録・発信・伝送・受信される情報の安全管理のために必要な措置
- (イ) 情報システム及び情報通信ネットワークの安全性及び信頼性確保のために必要な措置
- (ウ) 上述2つが講じられている状態が適切に維持管理されていること

このような定義がなされている背景には、社会のデータ化がある。すなわち、今日の社会は、コンピュータと情報通信の結合を重要な基盤とし、そこにおいてデジタル化された情報（データ）を利活用することで成立しており、これらに対する依存度はさらに高まりつつあるから、安全・安心な社会にとって、そのセキュリティは極めて

重要な課題となる。そして、今日の社会が上述構造をもつことから、そこにおけるリスクには、コンピュータ処理される情報（データ）そのものに係るリスクとコンピュータシステム及び情報ネットワークシステムに係るリスクが存在することになる。こうしたリスクのうち前者は、ARPANETを原点とする現在のインターネットが1990年代以降急速に拡大する以前から認識されていたものであるが、2000年代に入り国の政策としても「高度情報通信ネットワーク社会形成」が掲げられ、現実インターネットが社会基盤となるに至ったことから、後者のリスクが強く認識されることとなっている。上述の定義は、こうしたリスク構造を前提として、大きく2種類のセキュリティを「サイバーセキュリティ」として定義しているものである。

ところで、「サイバーセキュリティ」に類似した用語として「データセキュリティ」がある。この「データセキュリティ」については、法律上の定義は存在しないところ、実務的又は講学的には、上述（ア）（及び（ウ））のみを指す場合（狭義のデータセキュリティ）と、サイバーセキュリティと同義（上述（ア）（イ）（及び（ウ））の双方を指す場合）、「サイバーセキュリティ」を含みさらに社会がデータ化していることを背景とする周辺リスクに対するセキュリティを含めて指す場合（広義のデータセキュリティ）の3種がある。

例えば、「デジタル情報とそのライフサイクル全体を通じて不正アクセス、破損又は窃盗から保護すること」（IBMによる定義）、「承認されていないアクセスからデータを保護し、データの機密性、整合性、可用性を維持するために採用される保護手段」（Oracleによる定義）等は、狭義のデータセキュリティを前提として、実質的にはサイバーセキュリティと同意となるように、これを拡張しているものである。これは、上述のサイバーセキュリティ基本法上の定義が、情報ネットワークを前提としないリスク対策をも包含するために、情報処理分野の実務において（ア）を含めて「サイバー」と呼ぶことに違和感があることから、このような用語法を用いているものと考えられる。

他方で、広義のデータセキュリティでは、例えば、「認知バイアスによりデータを正しく評価できない」といったリスクに対する対策や「情報ネットワークシステムが機能不全となった場合を想定した代替マニュアル処理の整備」等も「データセキュリティ」として観念されうる。

そこで、今回のサーベイにおいては、その対象を「サイバーセキュリティ基本法」にいうサイバーセキュリティとし、広義のデータセキュリティのみに係る資料等については調査対象としていない一方で、用語として「データセキュリティ」が用いられていてもサイバーセキュリティと同義としている資料等についても調査対象とした。

② サーベイ対象設定の枠組み

サイバーセキュリティ上のリスクは、直接的には、情報自体、情報システム及び情報通信システムに係るリスクであるが、実質的には、これらを利用している社会システムやインフラそのものに係るリスクであることから、国等の社会システム全体の管

理者から、特定の情報システムの提供者、さらには当該情報システムのエンドユーザまで、多くのステークホルダが存在し、それぞれが求めるセキュリティ確保上のニーズが異なることから多種多様な資料が存在し、公開されている。

そこでサーベイの対象の設定方法として、まず考えられるのは、これらを悉皆的に調査することであるが、これは必ずしも適切なものではないと考えられる。個別企業等の情報システムのエンドユーザのニーズを例とすれば、これは当該企業が公表するIR (Investor Relations) 情報、ビジネス誌等に掲載される関係者のインタビュー記事、当該企業を対象として行われる企業研究論文によって一定程度得ることが可能であるが、これらは、量的に膨大である一方で、当該企業の戦略的情報統制バイアスが含まれており、かつ、体系的な欠点という問題がある。換言すれば、これら企業のニーズは、かならずしも体系的に顕在化しているとはいえないものであって、これらを掘り起こすためには、一方ではサイバーセキュリティ研究者による企業ニーズ先行研究論文のメタ分析、他方では企業における情報システム担当者等に対するヒアリング等を行うことが必要であると考えられる。

そこで、今回は、日本社会におけるサイバーセキュリティ確保の重要な担い手であり、かつ、民主制原理の下で相当程度に体系的な情報公表を行っている政府の文書を対象として、サイバーセキュリティに係る既知のリスクとニーズの整理を行った。

③ 現行法上の枠組みから見たニーズに係る文書の所在と概要

現行法制度の下では、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法（令和3年法律第315号）及びサイバーセキュリティ基本法によって、サイバーセキュリティの基本が定められている。

そこでは、（ア）サイバーセキュリティを定義する（サイバーセキュリティ基本法2条）とともに、（イ）政府に対して「サイバーセキュリティ戦略」を策定することを義務付け（同法第12条）、（ウ）国の行政機関等、重要社会基盤事業者等、民間事業者及び教育研究機関等に対して、それぞれ必要な施策を講じることが定められている。また、（エ）サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣にサイバーセキュリティ戦略本部を置いている（同法第25条以下。本部長＝内閣官房長官のほか、国家公安委員会委員長、デジタル大臣、総務大臣、外務大臣、経済産業大臣、防衛大臣が法律上必須の委員。現在は、他に経済安全保障担当大臣と有識者9名が加わっている）。

そこで、国レベルのニーズについては、まず、上述（イ）「サイバーセキュリティ戦略」の内容に加えて、（エ）のサイバーセキュリティ戦略本部を構成する大臣の所管省庁の文書が重要な資料となる。また、個別政策との関係では、他の個別官庁の文書を検討することも有用である。よって、今回は、＜参考資料1＞に掲げた文書のそれぞれに含まれるサイバーセキュリティに係るリスク認識とニーズについてまとめた。

結論を先取りして述べるならば、これらに共通する傾向として、文書等に示されているサイバーセキュリティ上のリスクとニーズは、個別政策の現状と現時点において

顕現している既知のリスクに対応するニーズがほとんどであり、結果として既存・既知の技術の着実な現場への展開するための環境整備がニーズとなっている。その理由としては、この領域における技術展開は極めて速く、政府文書に各論的言及をすることが困難であることに加えて、攻撃者に対して脆弱性の所在を示すことともなる記述には慎重となる必要性が極めて高いこと、さらには、社会経済活動を背景とする行政活動単位で所管が定まる国の行政組織のあり方からして、セキュリティ技術開発自体を所管しない行政組織においては、各論的技術ニーズ（政策ニーズのうち、技術の研究開発・社会実装等に関するものをいう。以下同じ。）に言及することが難しいといったことがあると推認される。

ただし、いくつかの機関が作成した文書においては、将来を見通したシナリオベースのニーズを示している事例も見られる。こうした機関には、サイバーセキュリティ戦略本部及び内閣官房内閣サイバーセキュリティセンター、デジタル庁、総務省、金融庁等がある。この中では、サイバーセキュリティ戦略本部から総務省までは、サイバーセキュリティ対策「技術」そのものを所管としているともいえ、シナリオベースのニーズ提示を行いやすいと考えられるが、こうした視点からすると、そのような役割が相対的に小さい金融庁がシナリオベースでのニーズ提示をしたことは、今後の政府機関によるサイバーセキュリティに係るリスク認識と対応する技術ニーズを分析するに際して、重要な先行事例と見ることができる。

以下において、特に重要又は特徴的な機関及び文書について、分析結果を示す。

④ 特に重要又は特徴的な機関及び文書の分析結果

1) サイバーセキュリティ本部

(ア) サイバーセキュリティ戦略（2015, 2018, 2021）

この資料に示されるサイバーセキュリティに係る政策ニーズは、資料の性格上、日本における政府からみたニーズの最上位のまとめとすることができるが、その最新版である2021年度版「サイバーセキュリティ戦略」（令和3年9月28日閣議決定。以下「戦略2021」という。）に示された政策ニーズは、概ね次の3つに要約することができる。

第一に、短期的ニーズとして既存の技術をサイバー空間の全ての参加者が利用できるように促進することであり、第二に中長期的には、AI技術と量子コンピュータ技術であり、第三に人材育成である。以下、その構造を示す。

そもそも、「サイバーセキュリティ戦略」は、サイバーセキュリティ基本法に基づき政府が策定することを義務付けられている文書であり、これまでに2015、2018及び2021の各年度に策定されている。この文書は、サイバーリスクが日々変化することに対応して更新されるものであるから、基本的には最新版が重要である。ただし、過去版も当該時点でのリスク認識を知るという歴史的資料の価値を有することに加えて、そこで示されたリスク認識（とりわけ仮定的条件に基づく将来認識）がその後どのように現実になったかを知るための資料としても意味

があるが、2018年度版までは、そのような将来認識に係る記述が多くないことから、今回の分析ではその手法は用いず、単に資料からサイバーセキュリティのニーズに係る記述を抽出する方法を用いた。

戦略2021では、サイバー空間をとりまく課題認識として、国民全体のサイバー空間への参画が進むという前提に立って、あらゆる主体にとってサイバーセキュリティの確保は自らの問題となる（Cyber Security for All）という枠組みが設定されている。その上で、情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携の5つの基本原則を堅持した上で、（ア）デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進、（イ）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保、（ウ）安全保障の観点からの取組強化、の大きく3つの施策を進め、「自由、公正かつ安全なサイバー空間」を確保するとしている。

本サーベイの視点からすると、このような全体構造において、どのような政策ニーズが認識されているかが重要であるが、戦略2021については、資料の全趣旨から、以下の3点を認めることができる。

第一に、短期的には、従来から用いられているセキュリティ技術を前提として、これを「あらゆる主体」において適切に利用することを基本とすることである。例えば、経済活動領域における「トラストサービス」活用によるデータ信頼性確保、ISMAP制度によるクラウドの信頼性向上と民間利用の促進、包括的サイバー防御のための環境整備（脆弱性対策、技術検証、制御システムのインシデント原因究明機能の整備等）等の取組が具体例として示されているのは、こうした特徴をよく示している。

第二に、新規の技術開発ニーズについて、中長期的な方向性としてAI及び量子コンピュータを示しつつも、各論への言及を少なく留めていることである。まず各論への言及が少ないことの背景には、この領域における技術展開は極めて速いことから、当該戦略のような基本文書に各論的言及をすること自体が困難であることに加えて、攻撃者に対して脆弱性の所在を示すことともなる記述には慎重となる必要性が極めて高いということがあると推認される。もっとも、後者の点からは、既に広く知られているリスクに対する警鈴も重要であるから、実践的研究開発の課題として、サプライチェーンリスクへの対応、国内産業の育成・発展、攻撃把握・分析・共有基盤、暗号等の研究の推進、等が上げられているのは、そのような事例とみることができる。他方で、技術開発ニーズの中長期的方向性については、AIを活用したサイバーセキュリティ対策（AI for Security）、AIを使ったサイバー攻撃（Security for AI）、AIそのものを守るセキュリティの3つの観点が示されており、さらには、量子技術の発展に対する対応に直接的な言及があるのが特徴である。特に後者については、既存のサイバーセキュリティの中心にある技術が公開鍵暗号を中心とする現代型暗号であって、計算量の膨大さによってセキュリティを確保するものであることから、サイバーセキュリティ関

係者においては、量子コンピュータの実用化により既存の暗号は事実上無効化されるとの理解がなされているが、これを踏まえて、「実用的で大規模な量子コンピュータが実現することによる既存の暗号技術の危殆化を想定しつつ、耐量子計算機暗号や量子暗号等に関する先進的な研究を推進し、安全性を確保するための基盤を確立する」という記述がなされている。

第三に、人材育成のニーズが強く表現されている。サイバーセキュリティの前提となるリスクは、日々高度化・複雑化するものであるから、将来生じるであろうリスクに対して現時点での技術又はその延長線上にある技術で対応することには、構造的な限界がある。こうした点からすると、人材育成こそが最大の将来的リスク対策であるといえることから、このような強調がなされていることはよく理解できるところである。

なお、戦略 2021 の策定に際しては、パブリックコメントが行われているが、そこに示された意見は、Cyber Security for All の担い手側からのニーズを示すものとして重要である[3.1.1]。具体例としては、意見 22「総合行政ネットワーク（LGWAN）を利用しての通信については、VPN による暗号化には頼らずに、自前での独自の暗号化を行っての通信を行ってほしい。また、日本国における電気通信事業者が提供する電子メール役務について全てインターネット上等において TLS での保護が行われるようにしてほしい。」や意見 78「現在の AI のセキュリティの課題としての、学習データのバイアス、プロセスの不可視性、アルゴリズム固有の脆弱性等を明示して、研究の方向性を追記してほしい。」などがある。

こうしたパブリックコメントに寄せられた意見については、サイバーセキュリティに係るシステム利用者側のリスク認識や技術ニーズを示すものとして、将来的にデータベース化等をして、分析できる環境を整備すべきと考えられる。

(イ) サイバーセキュリティ戦略年次報告・年次計画（2023, 2022, 2021）

この資料に示されるサイバーセキュリティに係る技術ニーズは、それが3年ごとに改訂されるサイバーセキュリティ戦略に係る年次報告・計画書であるという性格上、サイバーセキュリティ戦略を補足する短期的なニーズを示すものということができる。

その最新版である 2023 年度版に示された技術ニーズは、基本的には既存・既知の技術の着実な現場への展開ということができるものであって、新規技術に対するニーズではない。具体的には、「サイバーセキュリティお助け隊サービス」の拡充、SBOM (Software Bill of Materials) の導入、CYNEX (Cyber Security Nexus) に向けたシステム構築、GSOC (Government Security Operation Condition team) 次期システム検討、CRYPTREC 暗号リストの改訂とリスト掲載暗号技術の監視等が示されている。

2) 総務省

総務省は、情報通信政策を所管する機関として、毎年度「ICT サイバーセキュリティ総合対策」という文書を策定している。その最新版である 2023 年度版においては、以下のような具体的技術ニーズが指摘されているのみならず、技術展開に際して、シナリオを利活用したニーズとシーズのマッチングの必要性が提示されている。

具体的には、「情報通信ネットワークの安全性・信頼性の確保」と「サイバー攻撃への自律的な対処能力の向上」の2つのセグメントにおいて、既知のリスクに対応するのみならず、5G セキュリティについて「NICT に構築された 5G セキュリティ検証環境については、引き続き活用を推進するとともに、各ユースケースのグループに共通のアーキテクチャモデルに応じた具体的な脅威シナリオの検討を行うことが適当」であり、「これらの推進に当たっては、国際的にも進展の見られる基地局設備のインターフェースのオープン化や基地局設備自体の仮想化（いわゆる OpenRAN や vRAN）、コアや MEC を含めたクラウド（IaaS）利用も念頭に置くことが適当」とされている。

3) 金融庁

金融庁は、金融分野を所管する機関として、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」を策定している。その最新版である Ver. 3.0（以下「取組方針 V3」という。）は、2022 年 2 月に公表されている。

この「取組方針 V3」は既存のリスクと新規リスクの双方への対応を述べていることが特徴である。前者に係る基本的な方策は、モニタリング・演習の高度化とされており、他の行政機関にも広く見られる既存・既知の技術の着実な現場への展開というアプローチと共通している。

他方で、「取組方針 V3」に特徴的なのは「新たなリスクへの備え」と題する部分で、現時点におけるリスクのみならず、将来想定（仮説）に基づくリスクと政策ニーズ分析を提案していることである。この方法は、まず「取組方針 V3」の前版である 2018 年版（V2）で 5 つのリスク表として示されたものであって、最新版では表形式ではないが、考え方はそのまま引き継がれている。そこで、V2 における 5 つのリスクを示すと、次のとおりである。

- (a) 新たなプレイヤーとの連携、既存業務の外部委託等の進展によるサードパーティ（外部委託）リスク
- (b) IT システムの停止がビジネスそのものの業務継続に直接影響を与えるおそれ（IT リスク管理から危機管理の視点）
- (c) あらゆるシステムが繋がることにより、単一障害点を発端に連鎖的に影響が広範囲に及ぶリスク（最悪の場合決済機能不全に陥ることも）
- (d) 特定事業者や技術への依存度が高まることによる集中リスク（例えばクラウド）
- (e) AI 等のテクノロジーを悪用し、新たな攻撃方法を生み出すことで、既知の対策で検知・対応できなくなるおそれ

「取組方針 V3」においては、これを引き継いだ上で、キャッシュレス決済サービスにおける安全性の確保、クラウドサービスの普及等への対応、サイバーハイジーンの徹底、サイバーレジリエンスの強化という 4 つの対応を提示し、その中で、技術ニーズとして、「外部からの侵入を前提とした境界型セキュリティの手法には限界があるため、アクセスの信頼性を常に検証する「ゼロトラスト」の考え方に基づいた施策が考えられる」といった記述がなされている。

4) デジタル庁

デジタル庁は、2021 年に新たに内閣に置かれた行政機関であり、「デジタル社会の形成に関する内閣の事務を内閣官房と共に助け」、「デジタル社会の形成に関する行政事務の迅速かつ重点的な遂行を図る」（デジタル庁設置法（令和 3 年法律第 36 号）第 3 条第 1 号及び第 2 号）ことを任務としている。同庁は、「情報システムの整備及び管理の基本的な方針」（令和 3 年 12 月 24 日デジタル大臣決定）を策定・公表しているが、その中に「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」を含んでいる。

この方針は、今後の政府情報システムに求められる標準を示すものとして位置付けられており、（ア）共通機能等を前提とした常時診断・対応型のセキュリティアーキテクチャの実装の推進、（イ）サイバーレジリエンスを高めるためのセキュリティ対策の導入、（ウ）セキュリティポリシー及びセキュリティ対策の構造化及び追跡性の確保の 3 点を指摘し、それぞれ次のような対応ニーズを示している。

（ア）については、個別の政府情報システムが独立していた状況から、共通機能を提供するコンポーネントを API 連携で結合するという方向性を提示した上で、「従来の「境界型セキュリティ」の考え方に基づき一定のセキュリティ境界の内部にコンポーネントや情報システムを位置付けるだけではなく、個々のコンポーネントで取り扱う業務・情報やアクセスする者の属性情報を確認しつつ、アクセスを判断する「ゼロトラストアーキテクチャ」の考え方に基づき、常時診断・対応型のセキュリティアーキテクチャの実装を推進し、より高度なセキュリティを確保する」「ゼロトラストアーキテクチャの導入により、従来のアクセスする者やアクセス先の IT 資産に応じてあらかじめ決められたアクセス制御（ロールベースアクセス制御）の考え方に加え、当該属性情報をコンポーネントで連携させ、属性情報に基づいた動的なアクセス制御（属性ベースアクセス制御）の実現も目指す」としている。

（イ）については、「サイバーセキュリティフレームワークを補完的に導入」し、「脆弱性に関するセキュリティ診断、重要な政府情報システムにおける安定的・継続的な稼働の確保等の観点からの検証やバックドアの有無の検証等も重要」としている。

（ウ）については、「常時診断・対応型のセキュリティアーキテクチャの実装の推進」により「セキュリティ対策を含むシステム運用状況のリアルタイムでのデータによるモニタリングを推進」するとしている。

これらは、必ずしも純粋な「新規技術」の開発を求めるものとはいえないが、想定される状況変化に対して、既存技術の発展を必要とする技術開発を求める内容を含んでいるところ、前提とする状況変化が単なる「想定」「予想シナリオ」ではなく、デジタル庁自身が牽引するものであることから、このような形で一定程度踏み込みを行うことが可能となったものと考えられる。

5) 警察庁

警察庁は、サイバー犯罪・攻撃対策等を所管する機関として、多くの情報を発信しているが、その性格上、将来想定に基づく技術ニーズを公表することは少なく、現時点におけるリスクを公表し、警鈴とすることが多い。具体的には「サイバー警察局」のウェブサイトがその典型例である。

現在、14のリスクとそれに対応するニーズが例示的に示されているが、その一覧は次のとおりである。

- ・ランサムウェア被害防止対策
- ・Emotet 対策
- ・フィッシング対策
- ・不正アクセス対策
- ・ウェブサイト改ざん対策
- ・有料サイトの料金請求に注意
- ・サポート詐欺対策
- ・「偽サイト」「詐欺サイト」に注意！
- ・インターネットオークション・フリマサイト利用時のトラブル相談
- ・インターネット上の違法情報・有害情報への対策
- ・インターネット上の誹謗中傷への対応
- ・インターネット上における犯行予告への対応
- ・基本的なセキュリティ対策
- ・ビジネスメール詐欺に注意！

これらのうち、サイバーセキュリティとの関係で技術的対応が急務であるものも一つは、Emotet である。ただし、電子メールの添付ファイルを経路とするマルウェアである Emotet は、ここ数年のサイバー攻撃の典型例であり、多くの被害を発生させているが、それ自体はセキュリティソフトウェアで対応可能なものであって、上述ウェブサイトで述べられているのも、そのような対応である。

⑤ 政策課題とニーズの整理

上で述べたように、政府機関が公表している文書等においては、サイバーセキュリティ上のリスクとニーズは、個別政策の現状と現時点において顕現している既知のリスクに対応するニーズがほとんどであり、結果として既存・既知の技術の着実な現場への展開のための環境整備がニーズとなっている。

他方で、政府は毎年度「デジタル社会の実現に向けた重点計画」（以下「重点計画」という。）を定めており、各省庁はこれを背景として「デジタル・ガバメント中長期計画」を策定しているが、これらの文書は、将来的投資と結びついた政策ニーズを示す側面が強いといえる。そこで、2022年度重点計画（令和4年6月7日閣議決定）を背景とする各省庁の計画及びそれがフィードバックされている2023年重点計画（令和5年6月9日閣議決定。この文書には「デジタル社会を支えるシステム・技術」の章があり、技術側からの議論が纏められている。）について、分析して〈参考資料2〉の表にまとめた。

この〈参考資料2〉の表が示しているのは、現時点における国レベルの政策課題とそれに対する技術ニーズの多くは、既存の行政サービスごとのデジタル化の行程から導かれるものとして提示されているということである。もっとも、「デジタル社会に必要な技術の研究開発・実証の推進」の項においては、将来的社会課題の解決のための技術という視点からみた政府ニーズが示されている。ただし、そこでも具体的な「デジタル社会」が抱える将来的なリスクからバックキャストされた技術ニーズと、現時点において比較的一般に広く知られている新規技術が引き起こすことが推定されるリスクに係る技術ニーズが示されている。もとより安全保障やサイバーセキュリティの観点から、こうした政府文書に、例えば日本のみならず各国における技術動向やシナリオベースでのより詳細な技術ニーズが記載されることは稀であるともいえるが、少なくとも、サイバーセキュリティ領域において、政策的に優先的されるべき技術ニーズを検出する資料としては、粒度が荒いということになる。

そこで、このサイバーセキュリティに関する政府系文書のサーベイから導かれる中間的な結論は次の2点となる。

第1に、〈参考資料2〉に記載されているニーズは、もとより、いずれも喫緊の課題として認識されるべきものであることは理解できるが、そこで示されているものの多くは、現時点での「リスク」や現在進行中の個別政策課題に係るものである。そこで、これらによって、「現在の」対応ができたとしても、サイバーセキュリティの観点からは、「次の」リスクが生じることになる。すなわち、ある一定の段階で知られている最先端のシステムや技術を開発・導入しても、それによって直ちに本質的な政策課題解決を図るとはいえないのであって、さらに踏み込んで、どのような主体が、どのような形で各種政策に関与しているかという点からニーズと技術を整理し直す必要があるということである。

そこで今回は、これまで分析の対象とした文書から得られた知見について、サイバーセキュリティに関わる主体の面から、個人、組織（企業や団体）、地方公共団体、政府（国家）に集約して、また、セキュリティに関わる要素の面から、当面のニーズに対する対応、先端技術の研究開発、サイバーセキュリティ運用基準の整備、人材育成に集約して、政策的に必要性が高いと認識されている顕在的ニーズを整理した。その結果を表3.1.1に示す。ただし、この表は政府系文書から示される各主体のニーズであり、それぞれの主体側の認識を直接示しているものではないことには注意を要

する。

表3.1.1 主体ごとに異なるニーズと対応

	個人（技術者・研究者等）	組織（企業・団体の組織）	地方公共団体	政府（国）
当面のニーズに対する対応	<ul style="list-style-type: none"> ■主に組織構成員としての活動 	<ul style="list-style-type: none"> ■研究開発 ◆個別の業務システムに対するセキュリティリスク強化 ◆技術的攻撃への対応技術（Emotet 対策等） ◆人的攻撃への対応技術（振る舞い検知等） 	<ul style="list-style-type: none"> ■研究開発 ◆個別の行政システムに対するセキュリティリスク評価と対策ニーズの明確化 	<ul style="list-style-type: none"> ■研究開発 ◆個別のシステムに対するセキュリティリスク強化 ◆「デジタル社会の実現に向けた重点計画」「デジタル・ガバナメント中長期計画」等によるニーズの明確化
先端技術の研究開発	<ul style="list-style-type: none"> ■組織構成員及び独立した技術・研究者としての研究開発 ◆サイバーセキュリティの可視化技術 ◆ヒューマンエラー低減技術 	<ul style="list-style-type: none"> ■研究開発 ◆先端的暗号化技術（組織間暗号等） ◆技術的攻撃の検出技術（マルウェア対策等） ◆人的攻撃の検出技術（振る舞い検知等） 	<ul style="list-style-type: none"> ■研究開発への参画・支援 ◆企業や国が行う研究開発への協力（実験・実証フィールドとしての自治体） ◆官民データ活用推進基本法に基づく自治体がもつ情報の研究開発への提供 	<ul style="list-style-type: none"> ■自らによる研究開発と官民連携主導・調整 ◆AI 関連技術 ◆量子コンピュータ関連技術 ◆ゼロトラストアーキテクチャ
サイバーセキュリティ運用基準の整備	<ul style="list-style-type: none"> ■各種基準に従った行動 ◆各種ガイドライン遵守能力の向上 ◆資格制度への対応 	<ul style="list-style-type: none"> ■ハードローに従ったソフトローの整備 ◆組織内及び組織間のサイバーセキュリティ技術の標準化（ガイドラインやマニュアル等） 	<ul style="list-style-type: none"> ■ハードロー及びソフトローの整備 ◆法制度整備（条例等のハードロー） ◆ソフトロー整備（調達基準等を含む） 	<ul style="list-style-type: none"> ■ハードロー及びソフトローの整備 ◆法制度整備（法律等のハードロー） ◆ソフトロー整備（ガイドラインや調達基準等を含む） ◆技術的中立性と特定技術の推進のバランス調整
人材育成	<ul style="list-style-type: none"> ◆サイバースキル教育 	<ul style="list-style-type: none"> ◆組織内技術教育 ◆組織内倫理教育 ◆サイバーセキュリティ人材リスクリソグ 	<ul style="list-style-type: none"> ◆高度サイバーセキュリティ人材育成（高度ホワイトハッカー等） 	<ul style="list-style-type: none"> ◆官民の人材育成連携調整 ◆高度サイバーセキュリティ人材育成（高度ホワイトハッカー等）

中間的な結論の第二は、表3.1.1がもつ性格から、政府以外の主体の立場から見たニーズの認識を確認することが必要であるものの、それらは公開されている文書情報等からは困難であるということである。民間企業の多くは、その技術開発の現況や自社が抱える潜在的ニーズについて、企業間競争や資金調達等のリスクから、意見を表明することを回避する傾向にある。他方で、いわゆる業界団体や士業を中心とする専門家団体は、こうした意見を表明することもあるが、その多くは、業界あるいは専門家集団としての短期的利益の観点が強いことは否めないものである。

そこで、サイバーセキュリティに係るニーズ調査においては、上述サーベイに加えて、次に示すヒアリング、あるいはアンケート等を行い、他の主体の認識を引き出すことが極めて重要となる。

(2) ヒアリング

表 3. 2. 1 はヒアリング対象者一覧である。

表 3. 2. 1 ヒアリング対象者

番号	種別	所属	専門 又は 立場
①	専門家	東京大学情報基盤センター	情報セキュリティ
②	専門家	中央大学研究開発機構 決済サービスコンサルティング株式会社	キャッシュレス決済
③	専門家	中央大学研究開発機構 ソラミツ株式会社	ブロックチェーン
④	専門家	司法書士法人 横浜中央法務事務所	司法書士
⑤	関係府省庁	内閣官房内閣サイバーセキュリティセンター 警察庁 総務省 経済産業省	

このヒアリングでは、主に潜在的な政策課題やニーズについて何う目的で、第2章に示した質問項目は用いず、(1) サーベイの中間報告の結果を事前に見て頂いた上でご意見を頂いた。

① 東京大学情報基盤センター教授

2) 潜在的な政策課題・ニーズについて

- 例えばセキュリティと個人情報の線引きについて、**平時と戦時**（あるいは緊急時）でラインを変えるという観点でのルール作りはあまり行われていないように思う。緊急事態を全部想定することはできないが、考えるリスクに対するルール変更を想定しておいた方が良いのではないか？（例えば、内閣府「防災分野における個人情報の取扱いに関する指針」[3.2.1]）
- セキュリティの**アクセス権限管理に個人情報**を使用しないのは、原理的に不可能（両者は両立しない。）。
- サイバー攻撃からインフラを守るといふときに、**バックに国家**がいるところが攻めてくるかもしれないという想定が必要。
- リスクはインパクトと確率で考えられるが、前者は技術だけの問題ではなく**企業経営や社会**と関わっている。
- リスク管理を従来の縦型の階層構造で考えていると、サプライチェーンなど複数組織の**横展開**でデータや情報を共有する際に、機密性マネジメントが機能しなくなる。

2) 潜在的な 政策課題・ニーズ

セキュリティと個人情報の線引き

- ・平時と戦時(あるいは緊急時)で
ラインを変えるルール作りが必要

アクセス権限管理と個人情報

- ・個人情報を使用しないアクセス
権限管理は不可能

サイバー攻撃からのインフラ防御

- ・バックに国家がいるかもしれない想定

リスクはインパクトと確率

- ・インパクトは企業経営や社会と関わる

図 3. 2. 1 ヒアリング①の概要

② 中央大学研究開発機構准教授

1) 重要度・優先度の高い政策課題・ニーズについて

- クレジットカード不正利用の対策として EMV-3D セキュア、トークナイゼーションといった技術はあるが、日本では普及していない。
- 資金移動における金融システムリスクについて、お金の経路する金融機関や事業者の信頼性が重要であり、倒産しないような事業者を選ぶことが求められる。事業者には扱うお金の分をあらかじめストックさせる法律を作ることも有効である。
- BNPL (Buy Now, Pay Later: 後払い決済) において、日本では後払いの商品を現金化するサービスが出回っており、若者が支払いのための資金を得るために闇バイトに手を出すケースも報告されている。BNPL は海外ではすでに規制に向かっているが、日本ではどこが規制するかが明確でなく、早急に規制を始める必要がある。
- マネーロンダリングに関して、1円オーソリゼーションが手口として利用されており、外国人犯罪者グループに利用されている。現在の法律ではチャージバックにより、被害にあった店が責任を負うことになっているが、こういったリスクについてはカード会社、端末設置会社による店への説明責任がある。また海外の発行カードは怪しい取引があっても報告する義務がなく、犯罪を未然に防ぐことが出来ていない。

2) 潜在的な政策課題・ニーズについて

- 給与デジタル払いが解禁されたが、今後外国人犯罪者グループに狙われる可能

性もあり、対策が求められる。

- CBDC (Central Bank Digital Currency : 中央銀行デジタル通貨) の発行の実現においては、不正利用が多いQRコードの利用は危険である。

4) その他

- 日本の仕組みの問題として縦割り省庁の弊害があり、上述の問題に関してどこの省庁の管轄であるかが明確でない。
- キャッシュレス決済の用語の定義が明確でないことが、キャッシュレス決済の普及の妨げとなっている可能性がある。
- 東南アジアは失う不正額より売り上げが多ければよいという考え方であり、不正の多いQRコードの利用も普及している。しかしながら日本は不正を100%防がなければならないという意識であり、キャッシュレス決済における利益と損害についての考え方の線引きについても検討する必要がある。

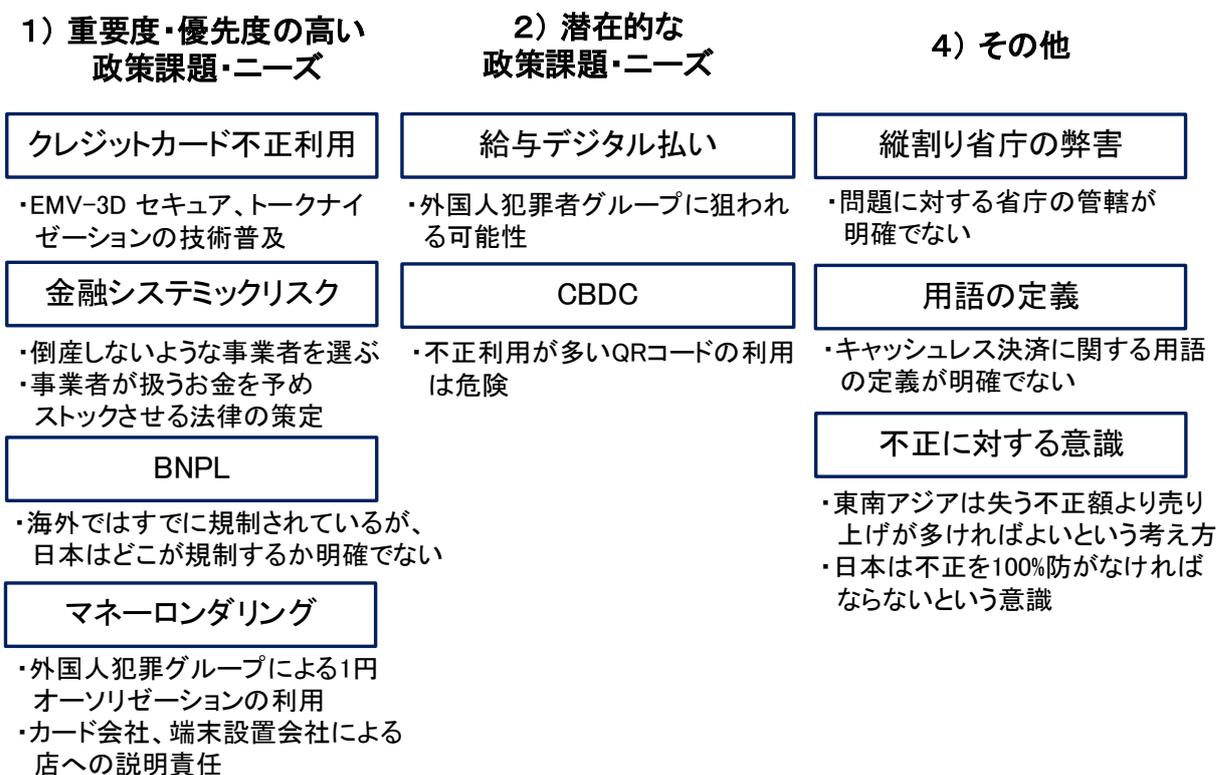


図 3. 2. 2 ヒアリング②の概要

③ 中央大学研究開発機構教授

1) 重要度・優先度の高い政策課題・ニーズについて

- 人材育成・教育が重要である。セキュリティを担保できるような人材の育成や、行政、学校、企業において担当者及び部門を育成することが求められる。不審なメールやURL、添付ファイルを開かないといった意識の徹底や、OSの更新、

ウイルス対策ソフトの導入は必須である。

- **機密情報の漏洩対策**として、UTM (Unified Threat Management : 統合脅威管理) が有効であり、複数のセキュリティ機能を統合的に管理する必要がある。情報へのアクセス対策として、誰がいつどこでどのような情報にアクセスしたかのエビデンスを残し、定期的に監査し、監視ツールにより怪しい動きを発見した際に警告することで情報漏洩を防ぐ必要がある。**機密情報を秘密分散で管理**することも今後の対策として有効である可能性がある。

2) 潜在的な政策課題・ニーズについて

- AI 技術を用いた攻撃の高度化に対する対策を考えていく必要がある。
- AML/CFT (マネーロンダリング及びテロ資金供与対策) が求められており、送金時にマネーロンダリングやテロリストが送金先でないか確認を行わなければならない。
- ブロックチェーンにおける秘密鍵の保護について、基本的にはハードウェアウォレットを使用することが有効であると考えられるが、**秘密分散で秘密鍵を保護**するという手法も対策のひとつである。

3) 実施・支援している技術開発の取組について

- ヒアリング対象者は**秘密分散**の技術開発に携わっており、日本のメーカーや会社と協力し、実装はできている段階である。さらに用途に合わせて3種類ほどの秘密分散は実装できており、**今すぐ使える状態ではあるが**、まだ使用はされていない状況である。
- 技術の普及に当たっては、どのような技術があり何ができるのかを認知し、費用対効果について理解した上で企業等が導入する必要がある。

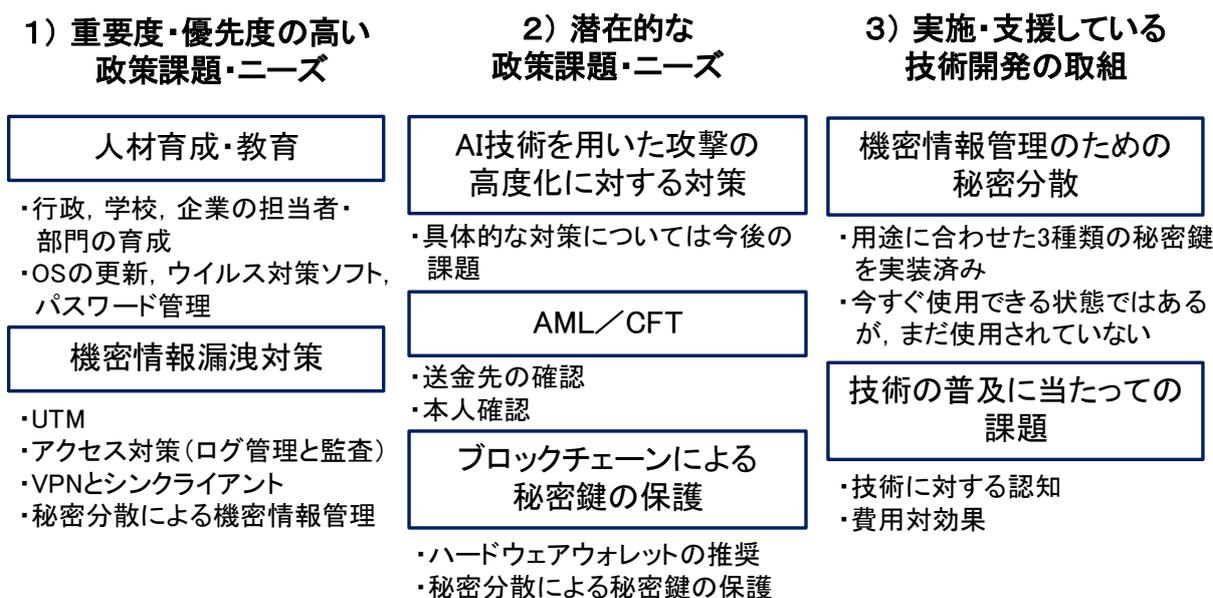


図 3. 2. 3 ヒアリング③の概要

④ 横浜中央法務事務所 司法書士

1) 重要度・優先度の高い政策課題・ニーズについて

- 専門職の情報管理の問題として、専門職が取り扱う過去のデータは原則として10年間記録を残すことになっているが、法律では定められていない。よって、専門職が引退・廃業した後の情報の管理及び処分方法について、法レベルの統一ルール及び各仕業特有のルールを定める必要がある。
- 現在、紙の資料は専門業者による溶解処分が主流であるが、特に電子データをどのように処分するかについては、早急なルール作りが求められる。
- クラウド等の利活用により、専門職の情報をデータベース化するような保管システムの構築も有効であると考えられる。

2) 潜在的な政策課題・ニーズについて

- 不動産登記情報の個人別集約化の問題に対して、申請時に個人番号の登録を義務付けることにより、国民の情報資産の正確性、真正性を担保する仕組みが必要である。
- ブロックチェーン等の暗号化技術による重要書類の偽造変造防止の仕組みにより、不動産の権利書等と個人情報の結びつきの真正性を担保できる。
- 不動産の権利移転と資金移動の同時履行の仕組みづくりとして、アメリカにはエスクローという仕組みがあるが、日本の不動産取引では同時履行を保証できず、仕組みの構築が求められる。
- 休眠会社は社会経済上悪用される可能性があり、会社・各種法人の実在性確認の仕組みについても考える必要がある。営利法人であれば税務申告の有無により実在性を確認できるため、法務局と税務署の情報連携を行うことで可能となる。

3) 実施・支援している技術開発の取組について

- システム構築において、ベンダーは発注者（政府）の意見を重視するが、実際のシステムを利用する利用者の視点に立ったシステム開発及び官民学の連携が重要である。
- 不動産の権利移転と資金移動の同時履行の仕組みについて、ヒアリング対象者は博士論文のテーマとして研究されていたが、技術的な問題により断念されている。現在は若手研究会を立ち上げ、実現に向けて活動されている。この仕組みが構築されれば、詐欺事件の防止等につながることを期待される。

1) 重要度・優先度の高い
政策課題・ニーズ

2) 潜在的な
政策課題・ニーズ

3) 実施・支援している
技術開発の取組

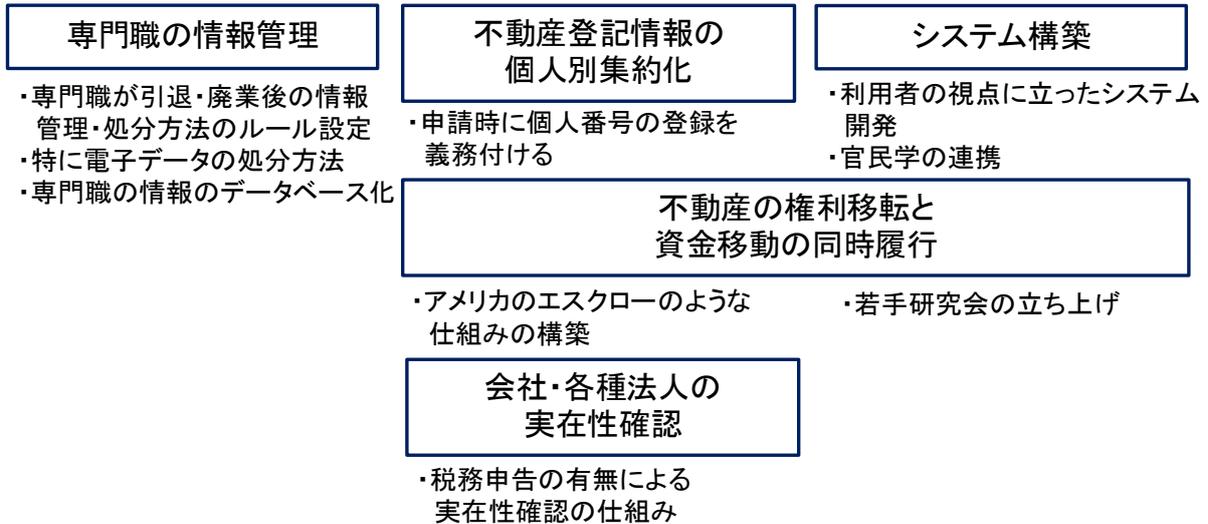


図 3. 2. 4 ヒアリング④の概要

⑤ 関係府省庁

1) 重要度・優先度の高い政策課題・ニーズについて

- 計算機リソースの進化による量子コンピュータ、AI 等の高度なテクノロジーを用いた攻撃及びサプライチェーンの複雑化に伴うリスクが脅威である。
- 機器の信頼性の検証（SBOM の活用等）や、防御側でどのように AI を使っていくかが重要となる。
- AI のセキュリティについては、政府が民間の開発スピードにキャッチアップし、中身を理解していかなければならない。
- フィッシング詐欺及びクレジットカードの不正利用、インターネットバンキングに係る不正送金の被害が増えており、深刻なリスクである。ランサムウェア被害はレピュテーションリスクによって被害申告をためらう傾向にあり、被害申告してもらうための取組が必要である。
- インターネット上の違法情報、有害情報は表現の自由との兼ね合いもあるが、関係機関とも連携しながら対応を推進していく必要がある。
- サイバー攻撃が増大する現状において、DDoS 攻撃（脆弱な IoT 機器等を悪用し、情報通信ネットワークを通じて行われるサイバー攻撃の一種）への対策が求められる。特に原因として一般の利用者が使用している機器がマルウェアに感染することが問題である。
- フィッシングサイトや偽情報を見抜ける技術が求められる。また偽情報の拡散を防止するための技術的な措置等も重要である。
- デジタル空間の拡大・深化に伴い、巧妙な偽・誤情報の生成・拡散、メタバースにおけるデータの取得・利用などの新たな課題が実空間に影響を及ぼしてい

る。

2) 潜在的な政策課題・ニーズについて

- 計算機リソース及びサプライチェーンのリスクは急激に発展しており、予測することが難しく、潜在的な問題でもある。
- 海外では組織的かつ高度な新たなサイバー攻撃が発生しており、**先鋭的な攻撃に対する監視及び対処**が重要なテーマになってくる。高度な攻撃に対して、より専門性を高める必要もある。
- サイバーセキュリティに関する情報共有は官民連携の枠組みで行われているが、**ゼロデイ攻撃への対応**が難しい。機器の不審な挙動を検知し、既存の情報共有のスキームに乗せることが重要である。
- ドローンや自動運転車など、**通信機能を持つIoT機器がサイバー攻撃**を受ける可能性があり、脅威になりうる。

3) 実施・支援している技術開発の取組について

- 政府全体の取組として内閣府が主体となって**経済安全保障重要技術育成プログラム**（通称：K Program）を実施しており、不正機能を検証する技術開発や、AIセキュリティの確立に向けた検証等を行っている。
- ユーザビリティを高めるためにクラウドを利用したシステム移行なども行っていく必要がある一方で、外部のサービスを使うことになるため、**セキュリティとの両立は課題**。
- **セキュア・バイ・デザイン／セキュア・バイ・デフォルト**という概念のもと、エンドユーザが意識しなくても使えるようなセキュアな製品の提供を目指していく。
- 犯罪実行者募集情報と思われる情報を探し当てる技術を有害情報対策に活かしている。
- **デジタル・フォレンジック**の継続的な研究を行っている。
- **サプライチェーンリスク対策等**に係る取組として、通信分野の SBOM の実証実験や、通信アプリに含まれる不正機能の検証に関する実証実験を行っている。
- データに基づく分析・対策等に取り組んでいるが、日本はデータが足りず、技術や製品を作れないためさらにデータが集まらないというネガティブフィードバックに陥っている。
- 電子政府推進暗号の安全性評価・監視や新世代暗号技術に関する研究開発を行っている。

(3) アンケート

情報技術調査に関し、ファイナンスサービス技術を対象とし、1)規制に対する信頼感[3.3.1] [3.3.2]、2)使い易さ[3.3.3] [3.3.4]、3)むずかしさ[3.3.3] [3.3.4]、

4)技術から受けるベネフィット[3.3.3] [3.3.4]、5)周囲からの影響[3.3.5]、6)技術から喚起されるポジティブ感情、7)技術から喚起されるネガティブ感情[3.3.6]、8)利用意図[3.3.3] [3.3.4]を測定し、個人の特性として9)技術に対する保守性[3.3.7]、10)セキュリティに対する危惧[3.3.8]を測定した。各尺度は複数項目5段階(1.まったく当てはまらない~5.とても当てはまる)のリカートタイプスケールで測定され、項目あたりの平均値を解析に用いた。以下の3調査で因子的妥当性(主因子法・プロマックス回転)や信頼性(クロンバックの α 係数)を検証した。調査1において技術に対する保守性は因子として抽出されず、信頼性も低かったため、調査1の解析には用いなかった。他の変数には大きな問題はみられなかった。また、各変数の分布も分析の前提条件から大きな逸脱は見られなかった。そのため、これらの質問票を用い、以下の3調査の解析を行った。また、実験条件(QRコード決済・電子マネー・クレジットカード・オンラインバンキング)と関連しない回答者特性である婚姻状態、子供の有無、個人情報への危惧で有意差がなく、回答者のバイアスが大きくはない状態で割付されていることを確認した。

① 調査1

生活者が各ファイナンスサービス技術(QRコード決済・電子マネー・クレジットカード・オンラインバンキング)に対して、どのようなイメージを抱いているかを検証し(目的1)、どのような心理概念が各技術の受容につながるのかをモデル化すること(目的2)を目的として、オンラインアンケートを用いて調査した。各決済サービス技術で対応のないデザインを用いて各決済サービス300名(計1,200名)から回答を得た。不正回答者を除去した1,197名を以下の解析に用いた。

目的1の各技術(QRコード決済・電子マネー・クレジットカード・オンラインバンキング)に対するイメージ差については、上述のアンケートに記載された心理概念を従属変数として一要因の対応のない多変量分散分析を用いて検証した。必要に応じて、多重比較補正にボンフェローニ法を用いた。

目的2のモデル化は技術やそれに関する環境要因の評価(規制に対する信頼感、セキュリティに対する危惧、使い易さ、むずかしさ、技術から受けるベネフィット)が個人の心理的状态(技術から喚起されるポジティブ・技術から喚起されるネガティブ感情)に影響を与え、行動意図(利用意図; [3.3.9])につながることを理論的に体系化したStimulus-Organism-Response model (SORモデル)に基づき解析をした。具体的には、心理的状态を介して従属変数である行動意図と関わる技術や環境要因を検証した。個人特性ではなく、技術評価や環境要因を明らかにすることで、介入策を模索することが可能になる。事前解析として、変数間の相関行列とステップワイズ回帰分析を行った(|標準化回帰係数| > .15, |相関係数| > .15, |部分相関| > .10)。その後、構造方程式モデリング手続に則り、これらの関係性を包括的に検証した(GFI > .90, SRMR < .10)。回帰分析と同様に基準を満たさないパスや共分散は削除し、修正指数が50を超えたパスと共分散を追加した。

- 目的1 QRコード決済・電子マネー・クレジットカード・オンラインバンキングに対するイメージ

図3.3.1に示すように、他のファイナンスサービス技術と比較して、オンラインバンキングに対して概ね低評価であった。

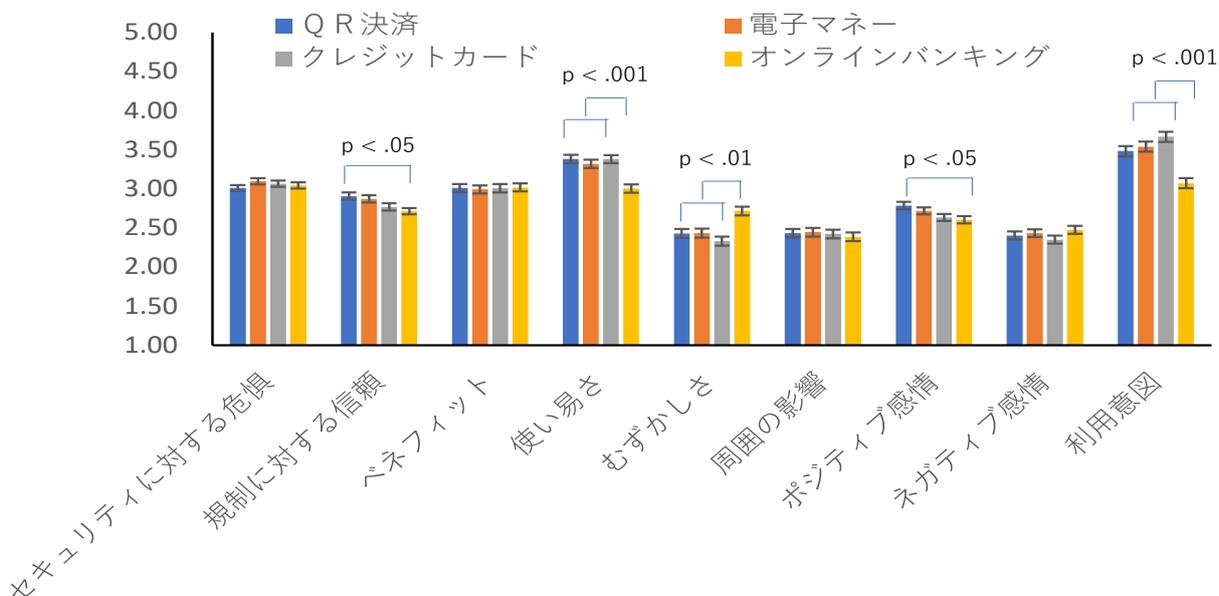


図3.3.1 QRコード決済・電子マネー・クレジットカード・オンラインバンキングに対するイメージ (エラーバーは標準誤差を示す)

- 目的2 決済技術受容モデルの探索

図3.3.2に示すように、SORモデルの0に相当する心理的反応が抽出されず、より簡略なSR (Stimulus-Response) モデルの適合度が高かった。使い易さやベネフィットを感じることで利用意図が高まる関係性がみられるが、決済技術の利用難易度が高いと感じることで、利用意図の妨げになることが示唆された。

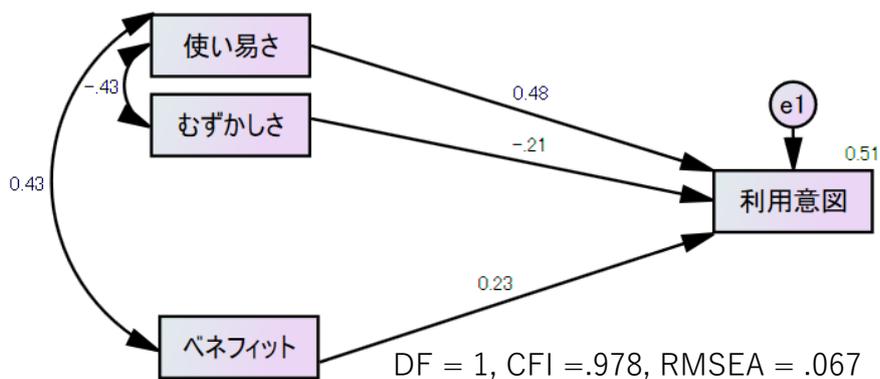


図 3. 3. 2 SOR モデルに基づく探索的解析結果（パスの値は標準化係数）

② 調査 2

調査 1 に加え、利用の有無（利用者各群 150 名× 4 条件・非利用者 150 名× 4 条件）を要因として追加し、二要因の対応のない多変量分散分析を行った（目的 1）。また、調査 1 のモデルの頑健性を検証するために、構造方程式モデリング手続に則り検証をした（目的 2）。分析法や基準値は調査 1 に準ずる。不正回答除去後の回答者数は 1, 191 名を以下の解析に用いた。

- 目的 1 ファイナンシャルサービス技術と利用の有無による交互作用は見られなかった。技術間の主効果は、ベネフィットにのみ小程度以上の効果が見られ、オンラインバンキングの評価(M = 3.28, SE = .05)がQR 決済(M = 2.79, SE = .05) ($p < .001$)や電子マネー(M = 2.95, SE = .05) ($p < .01$)、クレジットカード(M = 2.83, SE = .05) ($p < .001$)よりも高かった。調査 2 では、利用者と非利用者を均等割り付けにした標本抽出法や調査デザインが異なるため、多少調査 1 とは異なる結果になったことが考えられる。また、図 3. 3. 3 が示すように、利用者は非利用者と比較して、ベネフィットと規制に対する信頼、使い易さ、周囲の影響、ポジティブ感情、利用意図が高く、むずかしさとネガティブ感情は低かった。

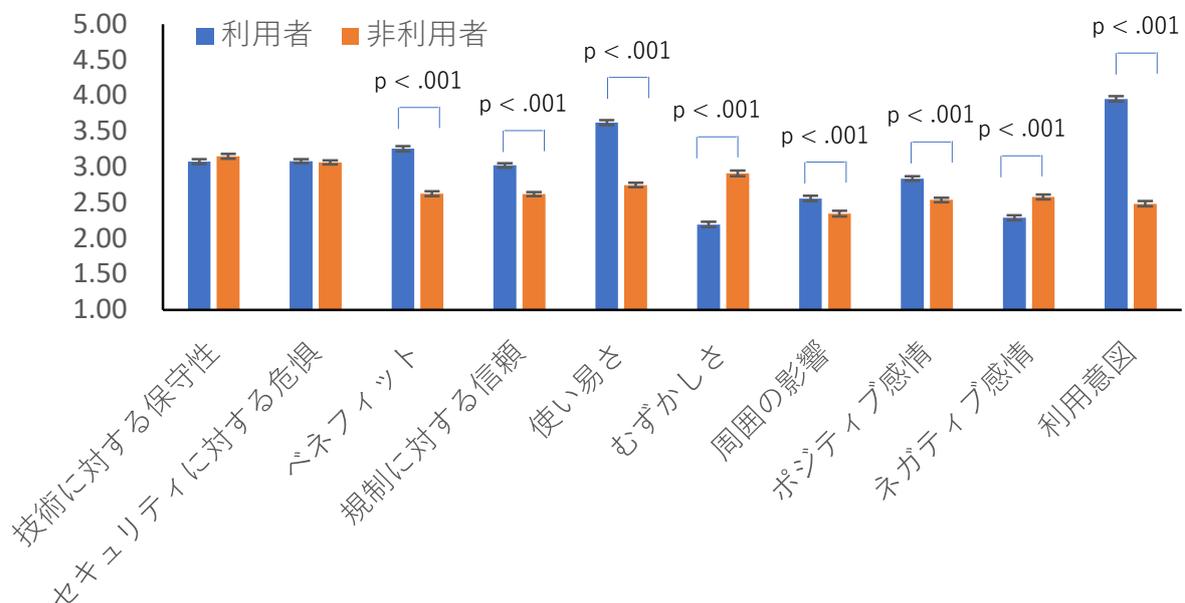


図 3. 3. 3 利用の有無によるイメージの違い（エラーバーは標準誤差を示す）

- 目的 2 決済技術受容モデルの検証

図 3. 3. 4 に示すように、調査 1 のモデルと同様のモデルの適合度は高く、再

現性が認められた。SOR モデルの 0 に相当する心理的反応が抽出されず、より簡略な SR モデルの適合度が高かった。使い易さやベネフィットを感じることで利用意図が高まる関係性がみられるが、決済技術を利用する際に難易度が高いと感じることで、利用意図の妨げになることが示唆された。

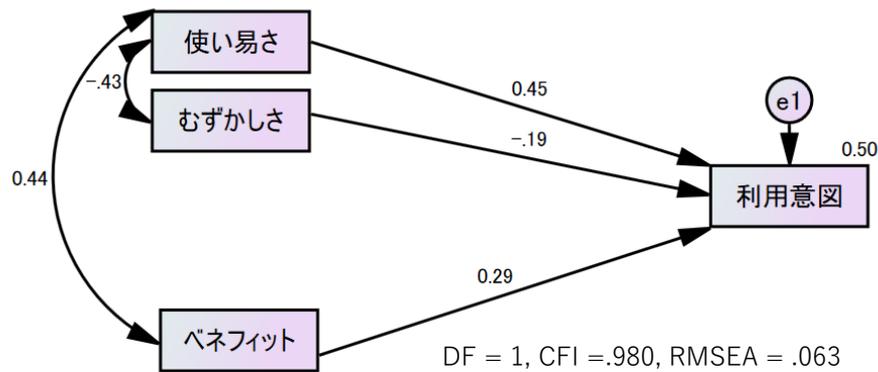


図 3. 3. 4 SOR モデルに基づく確証的解析結果（パスの値は標準化係数）

③ 調査 3

調査 1 に加え、利用トラブルの有無（利用トラブルを被った方 150 名× 4 条件・それ以外の方 150 名× 4 条件）を要因として追加し、二要因の対応のない多変量分散分析を行った。分析法や基準値は調査 1 に準ずる。不正回答除去後の回答者 1, 168 名を以下の解析に用いた。なお、本調査のみトラブル経験のある回答者の年齢が若く ($p < .001$)、男性に多かった ($p < .001$)。

● 目的 ファイナンシャルサービス技術間とトラブルの有無による評価の違い

交互作用は見られなかった。図 3. 3. 5 が示すように、調査 1 と同様オンラインバンキングの評価が低いことがうかがえる。また、図 3. 3. 6 が示す様に、トラブル経験のある利用者の方が個人情報への危惧やネガティブ感情が高いにも関わらず、概ねイメージは好評価であった。

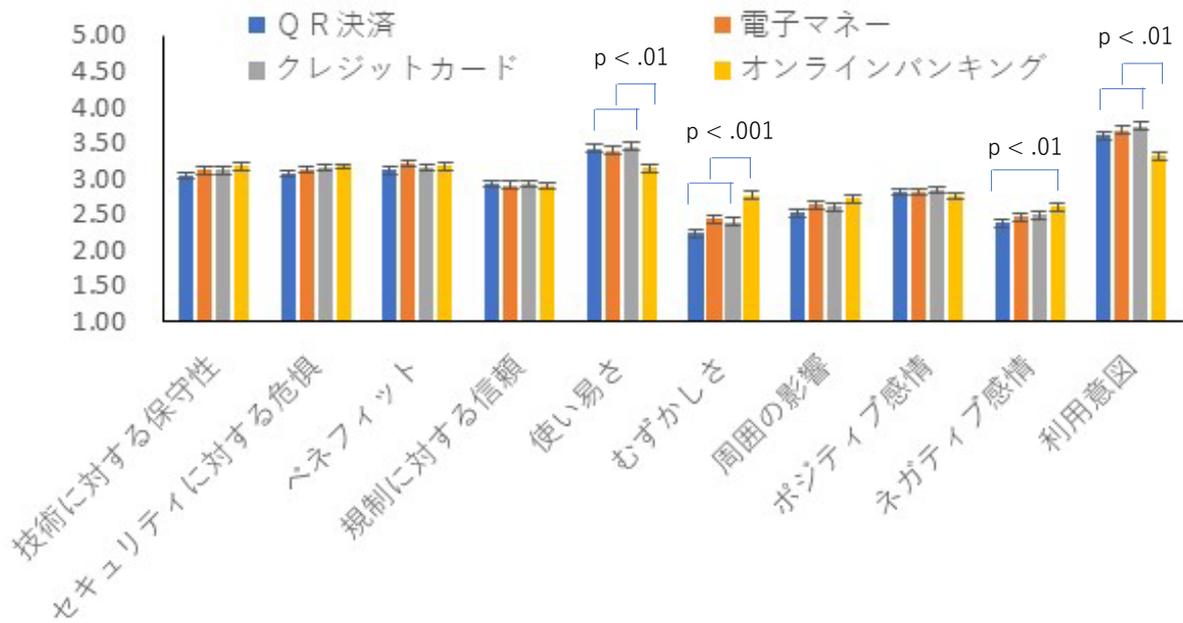


図3.3.5 QRコード決済・電子マネー・クレジットカード・オンラインバンキングに対するイメージ（エラーバーは標準誤差を示す）

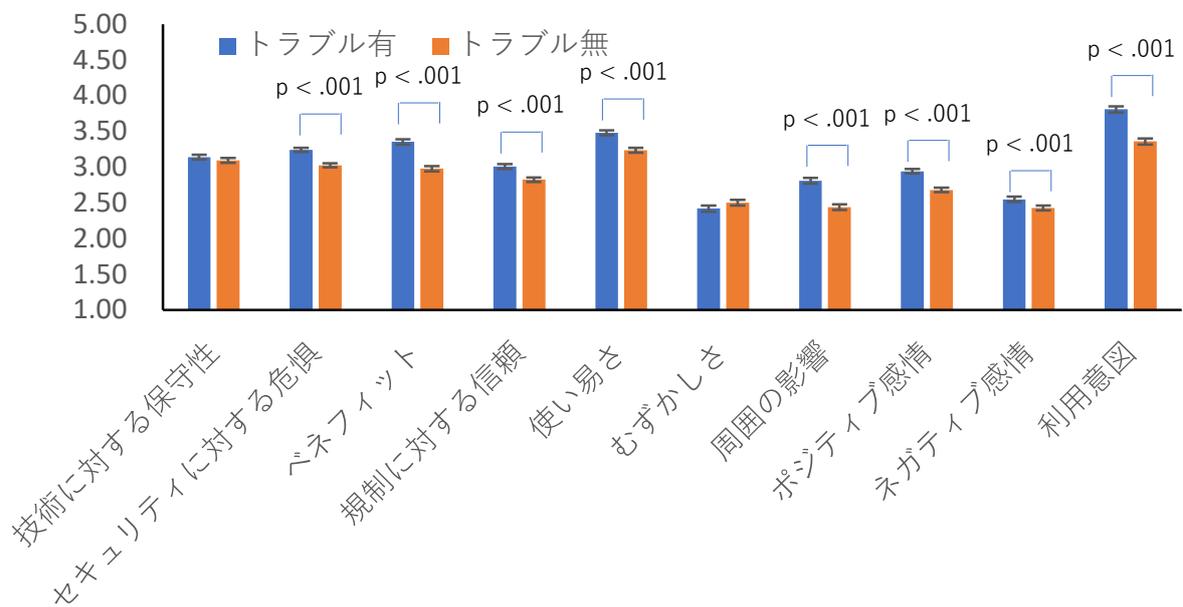


図3.3.6 トラブルの有無によるイメージの違い（エラーバーは標準誤差を示す）

④ アンケートからの考察

ファイナンスサービス技術間（QRコード決済・電子マネー・クレジットカード・オンラインバンキング）の評価に差があるか（調査1目的1）、また、これらの技術

の評価が利用者と非利用者の間でどのように異なるか（調査2目的1）、トラブルの有無でどのように評価が異なるか（調査3・目的1）を検証した。さらに、これらの技術の受容につながるモデル（調査1目的2）の構築と再現性の検証（調査2目的2）を試みた。

調査1目的1の解析結果により、オンラインバンキングの利用には障壁が高いことが明らかになった。近年登場したQRコード決済などは、その使い易さや困難度の低さから、抵抗なく受け入れられていることがうかがえる。この結果から、必ずしも新しい技術が受け入れられないのではなく、利用者にとって使い易く便益がある場合は普及が進むことが考えられた。これらの関係性は調査1・目的2のモデルによって、ファイナンシャルサービス技術の利用意図には、容易で便益が得られることが重要であることが支持されたことから外的外れではないと思われる。また、利用する際に難易度が高く感じられてしまうことが、普及の障壁となることもうかがえる。可視化されたモデルに感情の盛り上がり（ポジティブ感情）など、SORモデルのOに相当する心理的反応がモデルに組み込まれなかった。このことから、例えば次章の図4.3.2に示す受容モデルに反映された食品の摂取意図とつながるプロセスとは異なり、決済サービスは、消費目的自体ではなく、道具・手段的として利用されていることが考えられる。魅力的なサービス技術を提供することも重要であろうが、それよりも使い易いことや使い易いことが利用者に伝わることで、便益を感じ、普及の促進につながるのではないだろうか。

調査2・目的1の解析結果により、利用者と非利用者でファイナンシャルサービスに対する評価が大きくことなることが分かった。利用することにより評価が高いのか、評価が高いから利用するのかは明らかではないが、評価が低いことと利用意図の低下には関連が見られた。調査2目的2により、調査1の利用意図モデルの再現性が高いことが明らかになった。これらのことより、使い易さや、ベネフィットを感じられることがサービス普及につながることを考えられる。また、標本抽出法や調査デザインが調査1とは異なることにより、評定の点数は影響を受けてしまうが、評価変数間の関係性の検証は調査手法として比較的頑健であることがうかがえる。

調査3より、調査1と同様に、他のファイナンシャルサービス技術と比較してオンラインバンキングの評価が低いことが示唆された。また、直感に反しトラブル経験のある利用者の方がファイナンシャルサービス技術に対する評価が概ね高いことが分かった。これは、利用経験が多いことで、トラブルに遭う機会が生じたことが考えられる。そのため、単純にトラブルを経験することにより不安が高まり普及が妨げられることは考えづらい。情報技術サービスの普及を促進するためには、利用する際の障壁を下げ便益を感じられることが重要であることが示唆された。

これらの調査より、ファイナンシャルサービス技術は簡便で効率化などの便益が得られる場合に利用者に受け入れられ、むずかしさを感じることで利用の障壁となることが分かった。また、トラブルを経験したからと言って、それが利用の障壁とはならなかったことは興味深い。

(4) 考察

本章ではここまで、サイバーセキュリティを対象に行ったサーベイ、ヒアリング、アンケート調査の結果について記載した。これらの調査から、サイバーセキュリティという問題領域の特徴として以下の点が挙げられる。

① 技術革新や新たな脅威出現のスピードの速さ

情報技術の進展は日進月歩であり、新たな技術が生まれることはセキュリティ確保に資すると同時に新たな脅威の誕生につながる。サイバー社会が肥大化し悪意を持った人・組織が攻撃をしかける手口も高度化し続けている。サイバーセキュリティ対策は不可欠であるが、万全と思われる対策をしてもゼロリスクを望むことは不可能である。一旦対策を講じても新たな脅威には無防備となる可能性は常に存在する。

② 関係する場面や関係者の範囲の広さ

情報を扱う場面や状況ではサイバーセキュリティに関する問題を考慮する必要がある。特に近年、AI や IoT 技術の進展により DX 化が進む中で、サイバーセキュリティ問題の範囲は増大する一方である。コンピュータ端末で扱う情報だけでなく様々なデバイス、サプライチェーン全体を含めてセキュリティ対策を考える必要がある。利用者は自分の情報が盗まれるか否かを気にしがちであるが、一旦盗まれた情報がその後誰にわたりどのように利用されるかまで考慮する必要がある。情報ネットワークを介せば世界中のあらゆる個人・組織にわたってしまうリスクがあり、関係範囲の特定が難しい。

③ 情報が漏洩した場合のインパクトの大きさ

情報漏洩は個人のクレジットカード暗証番号漏洩のようなケースだけでなく、場合によっては国家を揺るがすインパクトの大きなものまで含まれる。セキュリティホールが空いてしまえば情報ネットワークを経由して国家機密に攻撃がしかけられる可能性は否定できない。サイバー攻撃の背後に国家が存在する可能性があるが、一般利用者に国家的な脅威への警戒を日常的に求めることは困難である。

④ ユーザビリティとベネフィットを重視する利用者

情報システムの利用者は個人・組織など様々であるが、特に一般的な個人利用者は、サイバーセキュリティ対策の必要性を常識としては知っていても、難しい操作や煩雑な手続があると技術や制度の利用を忌避する傾向にある。また、ポイントなどの特典が受けられるといった明示的なベネフィットがあれば個人利用者の受容性が高まるが、明示的なベネフィットが感じられなければ受容しない。セキュリティ対策を怠る利用者は自身のリスクが高まるだけでなく、国家・社会全体としてもリスクを高めてしまう要因となる。

上述のようなサイバーセキュリティという問題領域に固有の特殊性ゆえ、セキュリティ対策には終わりではなく、個人・組織・社会全体として継続的なセキュリティ対策にコストを費やす努力が必要である。個々の利用者の意識や努力だけで実現することは現実的でなく、受容されやすく、かつ、継続的に実践可能な支援策や適用技術が求められる。そのために求められることを以下にまとめる。

① 速さ・広さ・インパクトを考慮したサイバーセキュリティ対応施策

● インパクトの大きな機密情報保護の支援技術

サイバーセキュリティというと単に「情報が流出しないために保護すること」と考えられがちであるが、個人のクレジットカード暗証番号のような個人情報と、漏洩した場合に国家を揺るがす危険のあるインパクトの大きな機密情報は区別して考えるべきである。人々は日常的にはその差異を明確には意識しにくい。重要な機密情報には秘密分散を図るための技術が求められる。元情報から秘密分散した分散片は一定個数を揃えなければ元情報を復元できず、また復元には膨大な処理コストがかかるため、情報保護の安全性が担保される。

● 機密情報へのアクセス対策とルールの整備

機密情報保護を徹底したとしても、利用のためにはアクセス権限は必須である。セキュリティのアクセス権限管理に個人情報を使用しないのは原理的に不可能である。一旦取得された情報がその後どのように利用されるか、利用後に適切に消去されるかを確実に把握することは必ずしも容易ではない。技術論だけではなく情報利用に関するルールの整備と適切なマネジメントが求められる。

② セキュリティ対策のルーティン化と透明化

● 利用者が簡便・快適に使える透明性の高いセキュリティ支援技術

専門知識の少ない利用者は難しく面倒な手続を忌避する傾向にあるため、ユーザビリティとセキュリティを両立することは難しい。煩雑な操作や手続をせずにセキュアな情報環境のメリットを享受できる、利用者にとって透明性の高いセキュリティ対策技術・ツールが求められる。

● 日常生活におけるセキュリティ対策のルーティン化とその支援

セキュリティ対策は一旦講じれば終わりではなく、定常的にモニタリングして新たな脅威に対する対策を継続する必要がある。日々の利用の中でルーティンとしてソフトウェアやパスワードの更新、データバックアップなどのセキュリティ対策作業を埋め込むことが望まれる。利用者が意識的に努力せずにルーティン化できる支援技術・ツールが求められる。

③ 技術や制度をうまく機能させる仕組みの実現

● 脅威とそれに対処する技術・制度に対する知識の共有と組織連携

新奇の脅威をAI技術を用いて予測・発見するなどの研究開発は常に必要であるが、「いちごっこ」の状態は今後も変わらないと思われる。現実的には、新たな脅威に対する被害が報告された場合に、社会全体で情報共有し被害を大きくしない取組が必要である。セキュリティ技術は民間主導の側面もあるが、有用な情報にリーチできない個人・組織を出さないため、組織の壁を越えた官民での協力体制や国際的な連携体制が求められる。

- **複数のシステムを連携させられる体制の構築**

個々のサービスでセキュリティが達成されたとしても、複数のサービス間での連携がうまくいかない場合には中継部分がセキュリティ上のリスクとなる。電子化された情報申請サービスであっても、途中で書類に印刷して人手でチェックすればヒューマンエラーが発生するリスクがある。個々のシステムやサービスだけを対象にセキュリティを捉えるのではなく、社会活動全体の動きを考慮してトータルな支援が行える体制の構築が求められる。行政においては省庁の壁を越えた連携が必要であり、個々の利用者にとっては自分の利用する種々のコンテンツやサービスをトータルに管理するツールが必要となる。

④ インシデント発生時の救済・補償・支援体制の整備

- **サイバーセキュリティ被害に遭遇した場合の保険・補償制度**

サイバーセキュリティのリスクをゼロにすることは難しく、一旦脅威にさらされると被害が甚大になる場合も多い。被害を過度に恐れると利用の促進が進まないため、利用者が安心してサービスを受容するためには、被害に遭遇した場合の保険・補償制度が求められる。自動車保険や火災保険に比べ、サイバーセキュリティの被害は評価のための数値的な指標が未だ確立されておらず、先行する米国の事例などを参考にして相場感の形成が待たれる。

- **サイバーセキュリティ被害に関するワンストップ相談窓口の整備**

サイバーセキュリティは社会生活の様々な場面に関係するため、セキュリティ被害に遭遇した場合に利用者がどこに相談すればいいか迷うことも多い。行政においてもサイバーセキュリティに関する窓口は各省庁に存在し、一般的な利用者が適切な選択ができるとは限らない。縦割り行政による省庁の壁や、国ごとの制度の違いを越え、サイバーセキュリティについての相談を行えるワンストップサービスの実現が望まれる。

4 食料安全保障

本章では、食料安全保障を対象に行ったサーベイ、ヒアリング、アンケート調査の結果について記載し、その結果から考察する。

(1) サーベイ

① 基本的な問題・根源的なニーズ

食料安全保障に関する農林水産省の公開文書を中心に、関連省庁の報告書等も含めサーベイした。

1) 食料安全保障の現状での定義

日本では、1999年に制定された「食料・農業・農村基本法」(平成11年法律第106号)[4.1.1]において、以下のように定められている。

(食料の安定供給の確保)

第二条 食料は、人間の生命の維持に欠くことができないものであり、かつ、健康で充実した生活の基礎として重要なものであることにかんがみ、将来にわたって、良質な食料が合理的な価格で安定的に供給されなければならない。

2 国民に対する食料の安定的な供給については、世界の食料の需給及び貿易が不安定な要素を有していることにかんがみ、国内の農業生産の増大を図ることを基本とし、これと輸入及び備蓄とを適切に組み合わせて行われなければならない。

3 食料の供給は、農業の生産性の向上を促進しつつ、農業と食品産業の健全な発展を総合的に図ることを通じ、高度化し、かつ、多様化する国民の需要に即して行われなければならない。

4 国民が最低限度必要とする食料は、凶作、輸入の途絶等の不測の要因により国内における需給が相当の期間著しくひっ迫し、又はひっ迫するおそれがある場合においても、国民生活の安定及び国民経済の円滑な運営に著しい支障を生じないように、供給の確保が図られなければならない。

(不測時における食料安全保障)

第十九条 国は、第二条第四項に規定する場合において、国民が最低限度必要とする食料の供給を確保するため必要があると認めるときは、食料の増産、流通の制限その他必要な施策を講ずるものとする。

国内生産の増大を図ることを基本に、輸入及び備蓄を適切に組み合わせることで、食料の安定供給が確保されていれば、平時における食料の安全保障は確保できるとしており、国際貿易が極度に制限される場合や、国内の凶作のような不測時においてはじめて生産・流通・販売全体に取組が必要となるとして、「食料安全保障」は不測時の危機対応としての食料政策に限定されていた。

一方、国際連合食糧農業機関 (FAO) では食料安全保障の定義は「食料安全保障は、

全ての人が、いかなる時にも、活動的で健康的な生活に必要な食生活上のニーズと嗜好を満たすために、十分に安全かつ栄養ある食料を、物理的にも社会的にも経済的にも入手可能であるときに達成される。」と定められている(「日本と世界の食料安全保障」[4.1.2]引用)。

2) 情勢変化とそれに伴う課題

上述1)の考えのもと政策がとられてきたが、制定後20年を経て、日本をとりまく情勢が変化したことで食料安全保障に関するニーズが多様化してきたため、現在、検証部会によって食料安全保障の定義を含め、現行法の見直しがされている[4.1.3]。

現行基本法の見直しの中で言及されている情勢の変化は以下の通りである[4.1.4]。

- ・ **国際的な食料需要の増加と食料生産・供給の不安定化**
世界人口増加、気候変動による異常気象頻発に起因する生産の不安定化
- ・ **食料供給及び農業をめぐる国際的な議論の進展**
食料安全保障、環境等の持続可能性に配慮した農業・食品産業に関する議論の進展
- ・ **国際的な経済力の変化と日本の経済的地位の低下**
輸入国としての影響力の低下(買い負け)、経済的理由による食品アクセス問題、価格形成機能の問題
- ・ **我が国の人口減少・高齢化に伴う国内市場の減少**
国内市場の縮小、食料を届ける力の減退、国際的な食市場の拡大
- ・ **農業者の急減と生産性を高める技術革新**
農業者の急減と経営規模の拡大、スマート農業・農業DXによる生産性向上
- ・ **農村人口の減少、集落の縮小による農業を支える力の減退**
用排水路管理・農地保全等の集落機能の低下

ア) 国際社会の一員としての食料安全保障の視点

・ 世界の食料安全保障との関係

前掲のFAOによる食料安全保障の定義を踏まえ、国際社会の取組である①持続可能な食料システムの構築の促進、②安定的な農産物市場・貿易システムの形成、③脆弱な人々に対する支援・セーフティネット、④気候変動や自然災害などの緊急事態に備えた体制づくり、に積極的に貢献することで、世界の食料安全保障の強化を通じて、日本国内においても、不測時のみならず、平時から国民一人一人が食品へ安心してアクセスできるよう、日本における食料の安定的な供給を確保するとしている。

・ 環境負荷軽減の視点

また、地球の限界「プラネタリー・バウンダリー」とSDGsに関しても国際社

会で積極的に議論されている。プラネタリー・バウンダリーとは、地球の自然資源の使用と回復の許容範囲を超え、人類が環境へ与える影響によって不可逆的壊滅的な環境資源の損失を与えないように、地球の環境容量を科学的に示し、9つの分野で具体的な評価をしたものである。食料生産も環境へ負担をかけるものであり、すでに「窒素・リンの循環」(肥料問題に關係)や「気候変動」で高リスクと評価されている現状において、今後の食料生産システムの改革へ「持続可能性」の視点が求められてくる[4.1.5][4.1.6]。

イ) 国外の情勢変化に起因する課題

・世界人口の増加と輸入に関するリスク

不測時のみならず、平時からの国民一人一人の食料安全保障を確立するために重要視される、輸入・備蓄・国内生産のうち、日本は輸入に大きく依存している。日本の食料自給率は37%(カロリーベース、令和4年度)であり、輸入なしには国民の食生活を支えることはできない。しかし、減少傾向にある日本とは反して、新興国や途上国を中心に世界人口は依然として増加しており、それに伴い食料需要も増加、既に顕在化している水需要のひっ迫が加速することが考えられる[4.1.7]。また、新興国等の経済的発展により、食料消費量が増加、食生活も変化しつつあり(畜産物や食用油の需要が増大。畜産物生産に必要な飼料穀物の需要も増大すると考えられる。)、これにより食料や肥料などの生産資材の輸入量も急増し、買付けをめぐる競争が激化している。また、畜産用飼料だけでなく、バイオ燃料用など食用以外としての穀類の需要増加も今後予測される。

加えて、輸入に関するリスクとしては、気候変動や地政学的リスクもあげられる。

・気候変動

近年、温暖化などの気候変動によって高温、干ばつ、大規模な洪水等の異常気象が頻発し、世界各地で局所的な不作が発生しているため、数年毎に穀物価格の高騰と暴落を繰り返している。これにより、長期的かつ安定的な調達に困難になりつつある状況が顕在化している。局所的・広域的、一時的・長期的など被害(不作)の程度にもよるが、今後も食料の供給を不安定化させるリスクである。また、海外での水不足等の問題は、日本と無関係ではない。バーチャルウォーター(食料を輸入している国(消費国)において、もしその輸入食料を生産するとしたら、どの程度の水が必要かを推定したもの)という概念が表すように、食料の輸入は形を変えた水の輸入でもあることから、食料自給率が諸外国と比較して低い日本は、水利用における国外依存度は世界で最も高いとされる。気候変動により、今後、さらに世界各地で食料と水の安全保障が低下すると予測されているため、食料等の価格高騰など日本への影響も考慮する必要がある[4.1.8]。

・地政学的リスク

地政学的な情勢の不安定化によって、輸入に大きく依存している日本の食料供給に深刻な影響を受ける可能性がある。ロシアによるウクライナ侵略など、紛争等の人為的な原因によって、輸出の制限・停滞、肥料原料の高騰など世界の食料供給を一層不安定化させる事態が発生したことを契機に、このような地政学的リスクによって、世界の食料供給や国内外の物流、サプライチェーンに大きな影響を及ぼすことが改めて認識された[4. 1. 9]。

・日本の経済的地位の低下

上述のように、世界的な食料需要の高まりや食料供給が不安定化の中、今後、価格高騰や輸入競争の激化が予測できるが、国際社会において経済的地位が低下しつつある日本においては、世界中から必要な食料や生産資材を容易に輸入できる状況ではなくなってきている。

ウ) 国内の情勢変化に起因する課題

このような状況において、複合的なリスクによって著しく輸入量が減少した場合や、輸入代替国からの輸入量と国内備蓄を合わせても国内需要を満たせないような不測時を避けるべく、「緊急事態食料安全保障指針」(令和3年7月農林水産省)[4. 1. 10]に基づき平時から情勢を監視しているものの、輸入に関するリスクを減らすためには、輸入に依存している食料・生産資材を備蓄、国内生産への転換を行い、かつ、国内生産を増大させることが必要である。

・農業人口の急減と農地管理

日本の人口減少と高齢化が急速に進む中、農林水産省による食料の安定供給へのリスク分析・評価では、労働力不足、関係人材・施設の減少リスクが顕在化しつつあるとされ[4. 1. 11]、農業人口の急減が問題視されている。国内生産の増大を図るためには、少ない農業人口でも生産性を高くする技術革新が必要である。また、農業人口そのものを増加させるために、いかに技術の継承などを行い、新規の農業関係者を獲得するかを検討しなくてはならない。農業人口の減少に伴い、農地の転用や管理が行き届かず荒廃農地になる場合も増加しており、政府は「食料安全保障の根幹は人と農地の確保」である[4. 1. 12]として、食料生産の基盤である農地の総量確保と適正利用のための措置を強化することを検討している。現状では、自然条件が悪いことや所有者の高齢化、労働力不足により荒廃農地になり、またその大半が再生利用困難となっている。また、荒廃地の増加により鳥獣被害や病害虫が発生し、周辺農地へ影響を与えるリスクにも対策しなくてはならない[4. 1. 11]。

・国内における気候変動の影響

気候変動は日本においても国内生産へ影響を与えている。温暖化・高温化によ

って節足動物媒介性感染症の活動範囲の広域化、時期の長期化が予測されるなど、家畜の感染症対策が必要である。また、異常気象により農作物の品質低下や、家畜の生育不調なども顕在化しているため、温暖化に耐えうる農作物の品種改良などに取り組む必要がある。異常気象は国内の渇水や洪水なども引き起こす。世界ではすでに水需要に関して問題視されているものの、日本国内ではあまり認識されていない。しかし、洪水によって農業用地が被害を受ける場合や、水が汚染されてしまう場合、また渇水などにより水が必要な時期に十分に作物に水が行きわたらないことが品質の低下や収量の低下につながる場合など、対策を講じなくてはならない。

・肥料の国内生産

日本では、農作物の生育に欠かせない肥料の原材料の多くは海外から輸入しているほか、特にリン酸アンモニウムと塩化カリウムは少数の国が世界全体の輸出量の大半を占めており、不測の事態の場合、代替国の選択肢は狭く、かつ、遠方の国が多いため、国内での生産増大が求められている[4.1.13]。この点、下水汚泥はリンや窒素を含有しているため、コンポストの肥料利用や、リンの回収などが取り組まれているものの、下水道に対する忌避感や散布・施肥方法に関するノウハウ不足や、リン回収施設のコストが高いなどの課題があり、まだ広く普及されていない[4.1.14]。

・肥料や食料等の備蓄

肥料に関しては、需給がひっ迫した場合にあっても肥料の国内生産を継続し得る体制を構築するため、肥料関係事業者による備蓄への支援に取り組んでおり、令和9年度までに、年間需要量の3か月分に相当する数量を恒常的に保有する体制を構築し、肥料の安定供給を確保することを目標としている[4.1.13]。また、食料や飼料などの備蓄に関しても、備蓄技術の向上や、長期保存可能な加工技術など、効率的・効果的な備蓄に取り組まなくてはならない。加えて、備蓄スポットに関しても効率的な選定が必要である。製粉・飼料工場などが太平洋側に偏在しているため、南海トラフ地震等の大地震の際に代替が困難になることが予測されるなど、対策が必要である[4.1.11]。

・物流問題

食料安全保障において物流も課題である。日本人口の減少により過疎地だけでなく都市部でも食品にアクセスできない食品アクセス困難者が増加していることや、消費者に届くまでのラストマイル、生産者からのファーストマイルにおける物流の停滞、「2024年問題」（2024年度から働き方改革により、自動車運送事業の時間外労働の上限規制等が適用されるため、労働時間規制等による物流の停滞等が懸念されている）やドライバー不足問題など多様な課題がある[4.1.15]。ま

た、過去の震災などにおいて食料の物流拠点の機能不全や物流経路の断絶等による物流の一時的な途絶があったため、緊急時においてもサプライチェーンの機能が維持できる体制にできるよう物流の検証など対策を講じている段階である[4.1.16]。

エ) 「不測時」と「平時」の課題

いわゆる「平時」であっても、既に気候変動などリスクが顕在化しつつあるものがあり、また、農業などはその性質から長期的に取り組まねばならない(ここで「長期的」としたのは、農産物の品種改良などは一時の取組だけではなく継続しなくてはならない点、将来顕在化するリスクに対して取り組む場合であっても生産が定着するまで数年を要するため早くから着手する必要がある点に留意する必要があるためである)。平時は不測時のための準備検討期間でありながらも、継続して短期・中期・長期的に課題解決に取り組む必要がある。

また、「不測時」に関して、これまでの「緊急事態食料安全保障指針」では「不測時」の定義がなされていないことに加え、法的強制力が与えられていなかったため、「不測時における食料安全保障に関する検討会」では不測の事態の定義、不測時における基本的な対処方針、平時と不測時の切り替え、関係省庁の連携のための対応根拠となる法整備の検討がなされているところである[4.1.9][4.1.10]。

予測できうる将来のニーズにあった食料安全保障の定義はまだ議論の途中であり、関係機関において食料安全保障問題への体系的な取組はまだ十分とはいえない。

② 政策面からの根源的なニーズの分類・整理

以上の情勢の変化と関係省庁の公開文書から、政策面からの根源的なニーズを食料の各段階である、生産・物流・備蓄の観点で整理した(図4.1.1)。

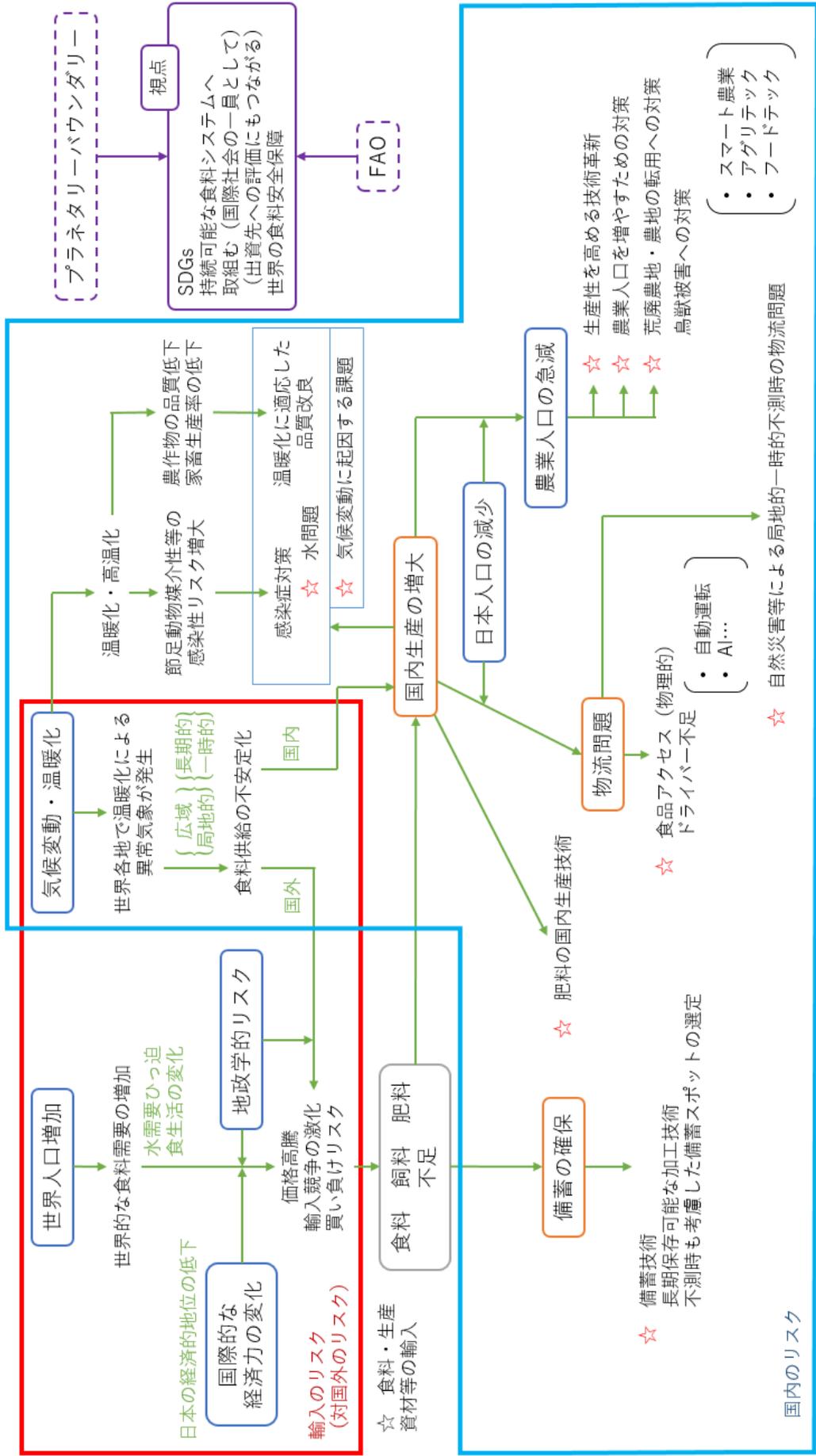


図 4. 1. 1 国内外における情勢の変化とニーズの整理

結果として抽出された、政策面からの根源的なニーズは以下のとおりである。

国内生産の増大

(A) 気候変動に起因する課題

A-a) 感染症・病害虫対策

「気候変動影響評価報告書」(令和2年12月環境省)[4.1.17]によると、気候変動による気温上昇に伴い、国内では見られなかった熱帯・亜熱帯地域に分布する牛の節足動物媒介性ウイルスが、九州以北の地域で流行していることが確認されるなど、既に影響が出ている。

病害虫に関しても、「気候変動影響評価報告書」では、気温の上昇によって、害虫の分布域の拡大や発生量の増加、水田の害虫・天敵の構成変化、海外からの飛来する害虫の種類と数の増加、病害においても発生地域の拡大をもたらす可能性があるとしている。害虫では分布域の北上・拡大、発生量の増加が既に生じており、今後も継続すると予測されていることから、害虫被害の増加あるいは発生地域の拡大、防除のための労力の増大が懸念される。病害では、高温による被害の甚大化や気温上昇によって発生地域が北上しており、今後、気温上昇による被害の増大が予測されている事例もある。よって、重大性は「特に重大な影響が認められる」とし、緊急性は「高い」と評価されている。

A-b) 気候変動に適応した品種改良等の対策

農業では、気温上昇や降水の時空間分布の変化等によって、水稻における一等米比率の低下、野菜の生育不良や果樹の生理障害等、作物の品質や収量の低下が多く品目で全国的に生じている。畜産分野においても気温上昇による飼料摂取量や消化吸収能の低下による成育の悪化や繁殖機能の低下など、暑熱ストレスの影響が顕在化している。「気候変動影響評価報告書」では、野菜や花きは生育期間が比較的短いため、適正な品種選択を組み合わせたり、栽培時期をずらしたりすることで栽培そのものは継続可能な場合が多いと想定されるものの、影響の重大性は「特に重大な影響が認められる」、緊急性は「高い」と多くのもので評価されている。

(B) 水問題

日本では既に降水の時空間分布が変化しており、無降雨・少雨が続くこと等により日本各地で渇水が発生し、給水制限が実施されている。北日本と中部山地以外では近い将来(～2039年)から渇水の深刻化が予測されており、また、融雪時期の早期化による需要期の河川流量の減少、これに伴う水の需要と供給のミスマッチが生じると、農業用水に影響を与える可能性があると予測されている。以上より、「気候変動影響評価報告書」では、水資源に対する影響の重大性等について、「特に重大な影響が認められ」、緊急性は「高い」と評価されている。

(C) 生産性を高める技術革新

日本の人口減少、少子高齢化により、農業従事者の高齢化が進行しており、今後一層の担い手減少が見込まれるため、労働力不足等は深刻な課題である。「食料の安定供給に関するリスク検証（2022）」（令和4年6月農林水産省）では、手作業が多い労働集約的な品目（野菜、果実等）で、将来、労働力不足になる可能性（リスク検証内では「起こりやすさ」と表現）が高く、畜産物、水産物については既に労働力不足が顕在化しつつあると評価されている。「影響度」については、「起こりやすさ」が高い品目は総じて影響度が大きいとし、「重要なリスク」と評価された。一方で、土地利用型作物など、一定程度機械化が進んでいる品目については、「起こりやすさ」、「影響度」ともに比較的小さくなると評価されている。

「フードテック推進ビジョン」（令和5年2月21日フードテック官民協議会）[4.1.18]では、「世界の食料需要の増大に対応した持続可能な食料供給を実現する」「食品産業の生産性の向上を実現する」「個人の多様なニーズを満たす豊かで健康な食生活を実現する」ことを目的に、プラントベースフード、昆虫を活用した食品、食品製造現場へのAI・ロボットの導入などの新しい技術の社会実装を推進している。

今後も労働力不足の傾向が加速することが予測されるため、少ない労働力でも生産性を高める技術革新が求められる。

(D) 農業人口を増やすための対策

(C)生産性を高める技術革新と同様に、今後の農業人口の急減に対応するため、農業人口の増加をスマート技術によってサポートすることも求められている。

(E) 農地管理の対策

E-a) 荒廃農地・農地の転用への対策

日本は山地が大部分を占めるという国土の特徴から、農地を開拓することに限界がある。また、農地面積は減少傾向にあり、理由の大半が荒廃農地の発生と非農業用途への転用である。「食料の安定供給に関するリスク検証（2022）」では、生産基盤の脆弱化のリスクの「起こりやすさ」については、農業従事者の高齢化、減少や労働力不足等により、ほとんどの農作物の品目で中程度以上とし、平地と比較して耕作条件が厳しい中山間地での栽培が多い品目（果実、茶）については高いと評価された。「影響度」については、土地利用型作物を中心に、米、麦、大豆等では中程度とし、「注意すべきリスク」と評価されている。

政府は「食料安全保障の根幹は人と農地の確保」である[4.1.12]として、食料生産の基盤である農地の総量確保と適正利用のための措置を強化することを検討していることから、対策していかななくてはならない。

E-b) 鳥獣被害への対策

荒廃地の増加により鳥獣被害や病害虫が発生し、周辺農地へ影響を与えるリスクにも対策しなくてはならない[4.1.11]。

(F) 肥料等生産資材の国内生産技術向上

肥料・飼料などの生産資材の多くは、海外に大きく依存している。

肥料は、経済安全保障推進法（令和4年法律第43号）に基づく特定重要物資として指定されている[4.1.19]。農作物の収量の維持及び農業経営の継続において、肥料は不可欠な生産資材であり、日本の食料の安定供給に極めて重要な役割を果たしているが、肥料の粗原料となるリン鉱石、加里鉱石等の天然資源が少ないことから、肥料原料の多くを海外からの輸入に依存している。肥料原料の国際価格の高騰や原料供給国の政情等に大きな変動があった場合でも、肥料の安定供給を可能にする体制を構築する必要がある、肥料のサプライチェーンの強靱化の一環として、国内生産の増大が求められている[4.1.13]。「みどりの食料システム戦略」（令和3年5月農林水産省）における目標「2050年までに、輸入原料や化石燃料を原料とした化学肥料の使用量の30%低減を目指す」（中間目標:2030年までに化学肥料の使用量を20%低減）も踏まえ、効率的な施肥技術の導入や家畜排せつ物、下水汚泥資源等の国内資源の循環利用に向けた取組が推進されている。下水汚泥中のリンや窒素を含有しているため、コンポストの肥料利用や、リンの回収などが取り組まれているものの、下水道に対する忌避感や散布・施肥方法に関するノウハウ不足や、リン回収施設のコストが高いなどの課題があり、まだ広く普及されていない[4.1.14]。

需給がひっ迫した場合にあっても肥料の国内生産を継続し得る体制を構築するため、令和9年度までに、年間需要量の3か月分に相当する数量を恒常的に保有する体制を構築し、肥料の安定供給を確保することを目標とする[4.1.13]など、早急な対策が求められている。

令和4年度（概算）の全体の飼料自給率は26%とほとんどを輸入に依存しているが、このうち、粗飼料自給率は78%、濃厚飼料自給率は13%となっている。また、不測時に備え、国内の流通在庫を含め100万トン程度（とうもろこし約1か月分の需要量に相当）を民間備蓄しているものの、その1か月の間に代替輸入国からの供給を確保しなくてはならない状況である。コスト面においても、酪農・肉用牛では経営コストの3～5割程度を飼料費が占めており、持続的な畜産物生産のためにも、国産飼料の生産・利用の拡大を進め、飼料費の低減を目指すことが重要とされている。農林水産省では、2030年度に飼料全体の自給率を34%（粗飼料100%、濃厚飼料15%）にすることを目標としており、粗飼料については草地の生産性向上、濃厚飼料についてはエコフィード（食品残さ利用飼料）や飼料用米の利用拡大等によって自給率の向上を図っている。しかしながら、草地等の生産性の向上のためには、規模拡大による草地管理時間の減少、草地改良率の低下や難防除雑草の繁茂

が課題である上、異常気象により、草地改良や飼料生産に悪影響が発生している。飼料用米については、与える畜種によっては消化向上などの理由で粉碎等の加工を必要とする場合があるが、飼料用米の利用を進めることで、輸入とうもろこしの供給状況に左右されにくい国産飼料による畜産経営が可能になると期待されている[4.1.20][4.1.21]。

(G) 輸入依存の高い作物の国内生産拡大

海外依存の高い小麦・大豆・飼料作物等の国内生産の拡大と安定供給のために、施設整備、水田の汎用化・畑地化等を強力に推進するとともに、米粉の普及に向けた設備投資等を支援することで、2030年までに2021年比で小麦+9%、大豆+16%、米粉用米+188%生産面積の拡大を目標にしている。また、それ以外の海外依存度の高い品目も含め、国内でも生産できるように新たな品種開発も求められている。輸入に依存している小麦などの食品原材料の国産転換等を進めることで、耕地利用率や農地集積率等も向上させつつ、食料安全保障強化を目指している。

(H) 海外需要に対応した技術革新

日本の人口減少に伴い、今後、国内市場は縮小していくと考えられるため、海外市場をターゲットとした、海外の規制やニーズに対応した輸出作物（食品）の開発も求められる。世界情勢が大きく変化している中で、現状日本で大きな問題となっていない課題について先行して取り組むことで、先進技術の水準を保ち、リードすることも、日本の経済的優位性の確保のために重要であると考えられる。

物流問題

(I) 物流問題

I-a) 食品アクセス問題

日本人口の減少により過疎地だけでなく都市部でも食品にアクセスできない食品アクセス困難者が増加していることが問題視されている。消費者に食品が渡る「ラストマイル」をいかに効率よく流通させるかを検討するため、自治体を支援し、道の駅等を拠点とした自動運転サービスの社会実証・実装を推進するなど取組がされている[4.1.15]。

I-b) ドライバー不足等による物流の停滞

農林水産物の流通は、生産構造や品目の特性、消費者ニーズ等に対応するため、全国から迅速に集分荷する多段階の流通形態に発展しており、食品流通は約97%をトラック輸送に依存している。結果として、トラック輸送に大きな負荷を与えている構造となっている上、いわゆる物流の「2024年問題」も相まって輸送能力の約3割が不足するとの懸念がある[4.1.22]。食品の物流に限らず、物流プロセスにおいて荷積み・荷待ちなど各段階において待ち時間などの拘束時間が

発生しており、非効率さも問題視されている。トラックドライバーをはじめとする食品流通に係る人手不足は恒常化しており、「2024年問題」も相まって物流コストの上昇も不可避であり、モノを届けられない問題はより深刻化することも考えられるため、早急な対策が必要である。「食料の安定供給に関するリスク検証（2022）」では、野菜や果実、生乳、水産物など季節や品目により主産地が変化し、生鮮品で穀物等と比較して日持ちしないものに関して、サプライチェーンの混乱の「起こりやすさ」と「影響度」は中程度とされ、「注意すべきリスク」として評価されている。

(J) 自然災害等による局地的・一時的・不測時の物流問題

過去の震災などにおいて食料の物流拠点の機能不全や物流経路の断絶等による物流の一時的な途絶があったため、緊急時においてもサプライチェーンの機能が維持できる体制とするよう物流の検証など対策を講じている段階である[4.1.16]。「食料の安定供給に関するリスク検証（2022）」においては、大規模な台風、豪雨、地震等の災害や停電等により、港湾、保管、輸送等の活動に支障が生じる可能性のあることが言及されている。

備蓄の確保

(K) 備蓄の確保

K-a) 備蓄技術の向上や長期保存可能な加工技術

肥料だけでなく、食料や飼料等も、効率的な備蓄や、備蓄期間中の品質の低下を防ぐ管理技術などをスマート技術等で効率的に行うことで、不測時にも考慮した備蓄の確保ができると考えられる。また、備蓄期間中の品質の低下を防ぐことに加え、食料や生産資材そのものを長期保存可能なような加工技術を開発することにより、不測時にも対応するための備蓄の確保ができると考えられる。

K-b) 不測時も考慮した備蓄スポットの選定

備蓄スポットに関しても効率的な選定が必要である。「食料の安定供給に関するリスク検証（2022）」においては、小麦や大豆、なたね、砂糖類、飼料穀物について、製粉・油脂製造・精製糖・飼料工場が太平洋側に偏在しており、南海トラフ地震等の大地震の際に、代替地での製造が難しいことから、「影響度」は大きいとされ、「注意すべきリスク」と評価されている。

これらのニーズを、政策で想定している時期と食料に関する各段階によって整理した(表4.1.1)。表中の(A)～(K)、a～bは上述の各ニーズの通し番号に対応している。

参照している公開文書中に想定している時期が明記されていない場合は、その課題の性質上、品種改良のように実現までに長期間かかる場合は短期(=すぐに取組むべ

き課題)、活発な議論が行われていない課題については長期、と区分している。また、「気候変動影響評価報告書」は「重大性」と「緊急性」(「影響の発現時期」と「適応の着手・重要な意思決定が必要な時期」の双方を評価)で評価され、「食料の安定供給に関するリスク検証(2022)」では「影響度」と「起こりやすさ」(その事象がどの程度将来起こりうるのか)によって評価されているため、既に顕在化している状況かつ影響度が高いものほど短期・喫緊、と区分している。不測時における課題に関しては、南海トラフ地震等のリスクもあり、また、検証も必要であることから、早期に取り組むべき課題として短期・喫緊と区分した。

表 4. 1. 1 各政策ニーズの想定時期の整理

政策	短期/喫緊	中期	長期
生産	A-a) 感染症・病虫害対策 A-b) 気候変動に適応した品種改良等の対策 B) 水問題 C) 生産性を高める技術革新 F) 肥料等生産資材の国内生産技術向上 G) 輸入依存の高い作物の国内生産拡大 H) 海外需要に対応した技術革新	D) 農業人口を増やすための対策 E-a) 荒廃農地・農地の転用への対策	E-b) 鳥獣被害への対策
物流	I-b) ドライバー不足等による物流の停滞 J) 自然災害等による局地的・一時的な不測時の物流問題	I-a) 食品アクセス問題	
備蓄	K-b) 不測時も考慮した備蓄スポットの選定		K-a) 備蓄技術の向上や長期保存可能な加工技術

③ パブリックコメントからみる国民のニーズ意識

国の行政機関が政令や省令等を定めようとする際に、事前に案を公表し、広く一般から意見を募ることで、国民の権利利益の保護に役立てることを目的として、パブリックコメントを募集している。

生産の面では、「食料・農業・農村基本法の検証・見直しに関する国民からの意見・要望」[4.1.23]において種子、肥料、食料自給率などのキーワードが多くみられた。特に「種子の国内生産」に関しては強い言葉でのコメントも多く、重要であると考えている人が多いと推察できる。また、「フードテック推進ビジョン」(案)へのパブリックコメント[4.1.24]では、昆虫を活用した食品やゲノム編集技術応用食品に対し、安全面を疑問視する意見や忌避感を訴えるコメントが見られ、「安心」を重視する声も多く寄せられている。

物流の面では、「持続可能な物流の実現に向けた検討会 最終取りまとめ(案) に対

する意見公募手続の結果について」[4.1.25]において、加工食品物流の長時間の荷待ちや手積み・手卸しによる荷役作業、非効率な検品作業等への取組やドローン配送についての意見がみられた。また、大規模災害などの不測時における緊急輸送ネットワークについてのコメントもあった。

パブリックコメントも参照することで、国民が関心をもっていることを読み取れる。

(2) ヒアリング

表4.2.1はヒアリング対象者一覧である。

表4.2.1 ヒアリング対象者

番号	分類	所属	専門 又は 立場
①	専門家	東京農工大学	精密農業
②	専門家	共立女子大学	昆虫食
③	専門家	日本女子大学	食品学・食品包装学
④	関係府省庁	農林水産省	

① 東京農工大学 特別招聘教授

このヒアリングでは、(1)サーベイには無い側面について何う目的で、第2章に示した質問項目は用いず、サーベイの中間報告の結果を事前に見て頂いた上でご意見を頂いた。

2) 潜在的な政策課題・ニーズについて

- 食料供給農場がサイバー攻撃を受けた場合に温度管理が適切に行われなくなり食料調達に乱れが生じうる。
- 農地を守るのと農家を守るのは別の問題である。**農地を守り**、食料の安定供給を実現することが重要である。
- 食料安全保障をコンセプトとして、食料生産システムにおいて、技術を身に付けて使いこなせる人から新しい人への技術の伝承が必要である。新しい人は、理解した上で自分なりに新しく開発して初めて技術が伝わる。単に農地や農業機械やロボットがあれば良いという話ではない。イノベーションが必要になってくるかもしれない。食料安全保障というコンセプトで新しいエコシステムを作るというプロセスが、食料生産システムにおける技術の伝承である。

3) 実施・支援している技術開発の取組について

- ロシアにはダーチャという都市家庭菜園やそこでの収穫物の非公式な市場（バザール）があり、食料バッファの役割を果たしてきた。我が国でも、農地を住宅地や工業用地に転換する法律が見直され、**都市農業基本計画**ができた。この都市農業の文脈で、都市緑化、震災時の避難場所、新鮮な野菜の提供等の目的以外

に、災害時の安全保障としての食料をバッファに使う。例えば埼玉県で生産される農産物に対し、物流拠点をストック（備蓄）の拠点にもすることで、震災時には食料の集配拠点になる（例えば埼玉県の花園）。

- 図4.2.1で、農地で作物が栽培されているのは自然の貯蔵庫（生産）、その前の種子生産（育苗・育種）、逆にその後の物流サービス（加工・流通）とその後の外食・消費、このサプライチェーンを作り、それぞれのところでバッファを設けて、何かが起こった時にバッファをチェーン全体で管理すれば、それが食料安全保障になる。



図4.2.1 スマートフードチェーンシステムのシステム化概要
(H27 CSTI 地域資源戦略協議会より)

4) その他

- 「食料安全保障」というのは、国防であり、コンセプト（概念）あるいはフィロソフィー（哲学）である。これを軸に各種施策を考えることが重要である。
- システムを1から構築するのではなく、それぞれの地域ごとに既存のシステムを再評価して、ストックマネジメントやバッファの観点から見直せば、それが食料安全保障の役割を果たすことになる。

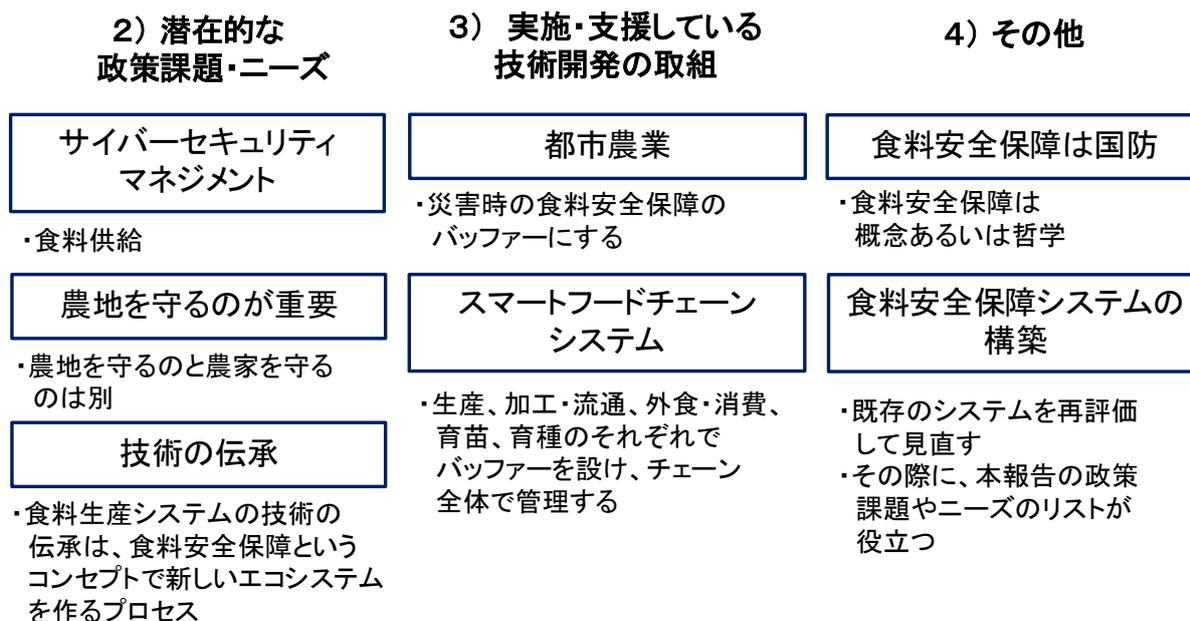


図4.2.2 ヒアリング①の概要

② 共立女子大学教授

1) 重要度・優先度の高い政策課題・ニーズについて

- 昆虫食に対する国民の拒絶反応は自明である。
- 人が昆虫を食すのではなく、養殖の魚に餌（飼料）として昆虫を与え、養殖の魚を人が食すという、**昆虫の変換機構としての役割**が期待される。
- 昆虫を原料とした飼料によるマダイの養殖については、愛媛大学大学院農学研究科と太陽石油株式会社によって実証試験が行われている。
- 昆虫の天然の色素としての利活用も期待できる。

2) 潜在的な政策課題・ニーズについて

- 昆虫は甲殻類に近い種族であるため、エビやカニのアレルギーを持つ人には昆虫もアレルギーとなる可能性があり、**昆虫食によるアレルギー反応の解明**が望まれる。

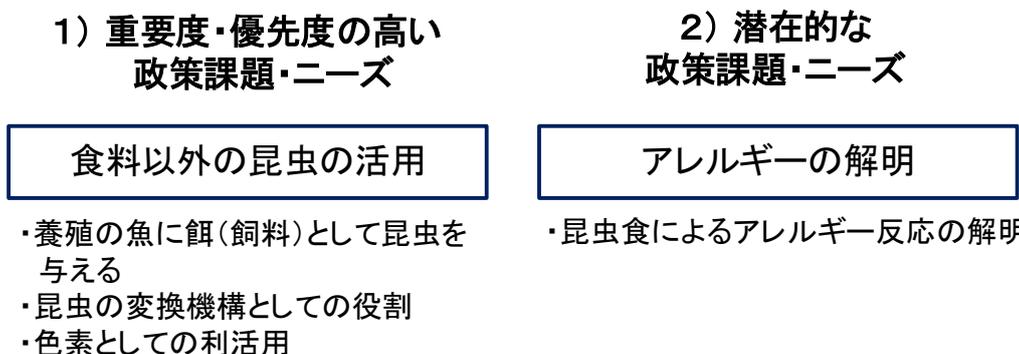


図4.2.3 ヒアリング②の概要

③ 日本女子大学准教授

1) 重要度・優先度の高い政策課題・ニーズについて

- 食品包装に関しては、過剰包装による環境問題が先行しているが、包装を使わないことによるロスもあり、**適正包装**が求められる。
- 食品包装に求められる機能として、保護性（一次機能）、利便性（二次機能）、情報伝達（三次機能）がある。これまでは保護性に着目した食品ロス対策が行われてきたが、これからは**利便性**に着目した対策が求められる。具体的には、食品を容器から取り出しやすく改良することで、取り残しによる食品ロス削減が期待できる。
- 青果物の酸素量・温度を調整する包装により保存期間を延ばす技術はあるが、サプライを安定させる体制の確保や、収穫から時間が経った青果物を消費者が受け入れられるかという問題もある。
- 物流の2024年問題に際し冷蔵・冷凍車が不足することによる廃棄ロスが予想され、鮮度を保つ技術が求められる。農産物に関しては傷つくことを防ぐための技術が重要である。
- ライフサイクルアセスメント（LCA: Life Cycle Assessment）により、フルーツキャップを使用すれば一連のプロセスにおける二酸化炭素の排出量は少なくなるという報告もあり、プラスチックも適切に使用する必要がある。

2) 潜在的な政策課題・ニーズについて

- 情報伝達（三次機能）における内容物の情報の伝え方により、消費者の購買意欲をコントロールできる可能性もある。
- 日本の包装技術は過剰包装というネガティブな側面もあるが、果物の緩衝容器や野菜の保存技術が輸出に役立つ事例があり、今後も応用が期待される。ただし、包装の経費は農家負担であり、仕組みを考える必要がある。

3) 実施・支援している技術開発の取組について

- 取り残し防止に関してはヒアリング対象者が2023年度に日本女子大学に着任してから取り組んでいる。
- 損傷防止はテーマとして継続して取り組んでおり、最近では加工食品（乾物、クッキー等）への応用を考えている。具体的にはクッキーの粉なども積もり積もってロスになっており、このようなロスを考慮した緩衝設計も必要である。
- 保護性（一次機能）、利便性（二次機能）、情報伝達（三次機能）の組み合わせによる概念構築とロスのデータ化に取り組んでいきたい。

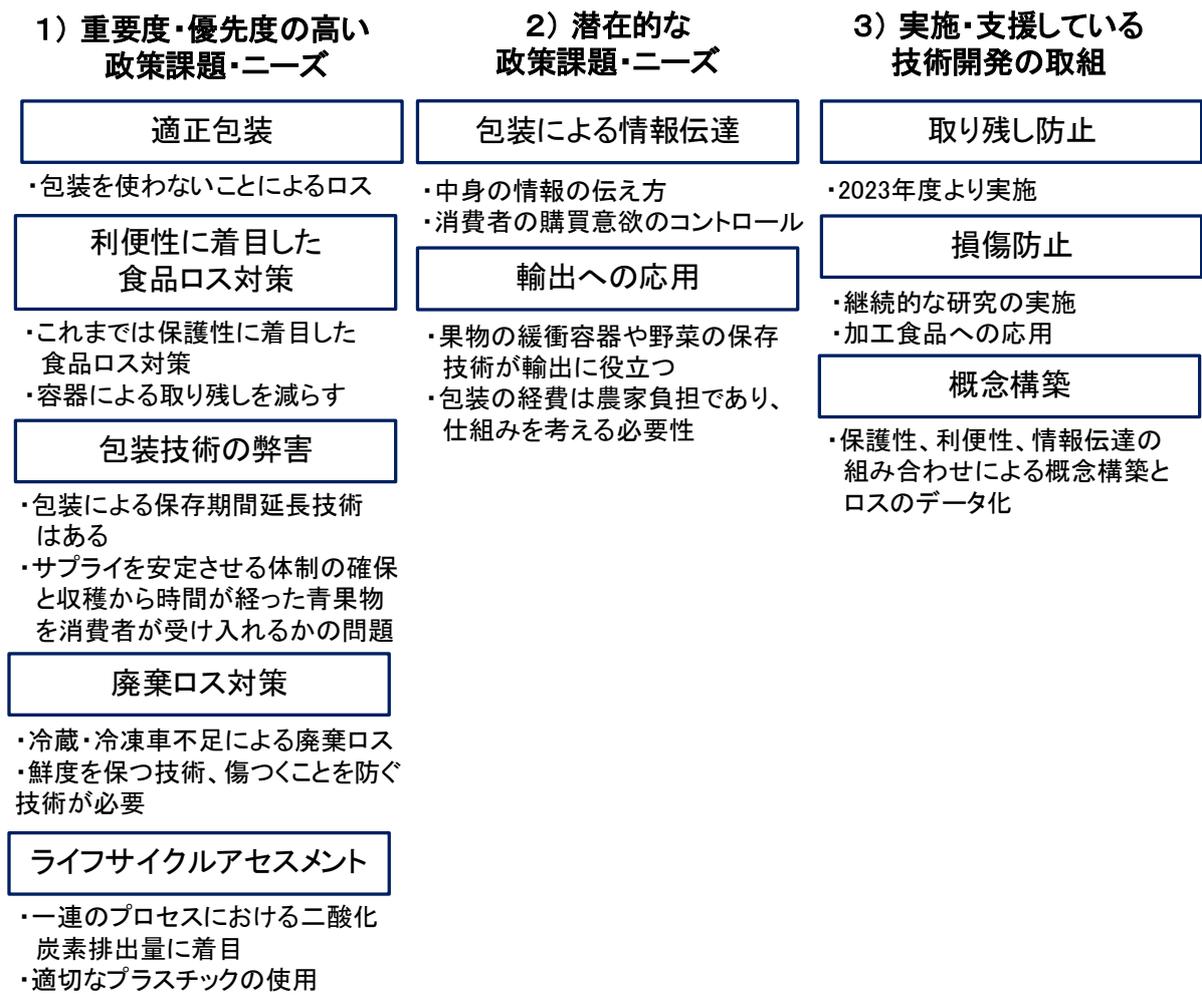


図4.2.4 ヒアリング③の概要

④ 関係府省庁

1) 重要度・優先度の高い政策課題・ニーズについて

- 気候変動、世界的な人口増加、食料需給のひっ迫が深刻な脅威となっており、主要な穀物価格の価格高騰や肥料の調達などに影響が出ている。
- 食料・農業・農村政策の見直しを進めており、新たな展開方向として4つの柱（食料安全保障の強化、スマート農業、農林水産物・食品の輸出促進、農林水産業のグリーン化）を打ち立てた。この新たな展開方向に基づき、食料・農業・農村基本法等の改正や施策の具体化を進める。
- 食料安全保障の強化については、不測時に備えて平時から対策を講じておくという考え方が重要である。輸出の促進について国内生産基盤の維持にも資するものとして新たに位置付けるとともに、国内生産で国内需要を満たすことができない食料については平時から安定的な輸入の確保を図る必要がある。
- 人口減少下においても生産水準が維持できる生産性の高い食料供給体制を確立するためには、スマート農業技術の現場導入を一層加速することが不可欠であり、スマート農業技術等の研究開発・実用化と、スマート農業技術の活用とこ

れに適合するための生産・流通・販売方式の見直しを一体的に推進するための法制度を検討している。

- 食料の安定供給を図るために、スマート農業の促進、新品種の開発による生産性向上、知的財産の確保・活用による付加価値の向上が求められる。

2) 潜在的な政策課題・ニーズについて

- 世界的な大干ばつや台風、異常気象の頻発といった**気候変動のリスク**や、近隣諸国との関係に基づく食料や肥料の調達の問題などの**地政学リスク**への対策が求められる。

3) 実施・支援している技術開発の取組について

- スマート農業への期待が高まっており、生産現場での導入実証が進められているが、スマート農機の価格が高い、技術に詳しい人材が不足しているなどの課題が明らかになっている。
- スマート農業技術の現場導入を加速するため、野菜や果樹の収穫等の実用化に至っていない難易度の高い分野における研究開発等の促進や、機械作業が容易な樹形への転換等のスマート農業技術の活用とこれに適合する生産・流通・販売方式の見直しを一体的に推進する必要がある。

(3) アンケート

食品技術調査に対しては、1)規制に対する信頼感[3.3.1][3.3.2]、2)食品技術を用いたベネフィット[3.3.5]、3)食品技術による損害[3.3.1]、4)周囲からの影響[3.3.5]、「5)食品技術から喚起されるポジティブ感情[3.3.6]、6)食品技術から喚起されるネガティブ感情[3.3.6]」、7)利用(摂食)意図[4.3.1]、8)拒絶[3.3.5]を測定し、個人の特性として9)食品技術に対する保守性、10)食料不足見込み[4.3.2]を測定した。各尺度は複数項目5段階(1.まったく当てはまらない~5.とても当てはまる)のリカートタイプスケールで測定され、項目あたりの平均値を解析に用いた。以下の各調査で因子的妥当性や信頼性(クロンバックの α 係数)を検証し、大きな問題はみられなかった。また、分布も分析の前提条件から大きな逸脱は見られなかった。そのため、これらの質問票を用い、以下の3調査の解析に用いた。また、実験条件と関連しない回答者特性である婚姻状態、子供の有無、食品技術に対する保守性と食料不足見込みは各条件間で有意差がなく、回答者がバイアスなく割付されていることを確認した。

① 調査1

生活者が遺伝子組み換え食品・代替肉・培養肉・昆虫食品に対して、各食品技術にどのようなイメージを抱いているかを検証し、(目的1)どのような心理概念が各食品技術の受容・拒絶につながるのかをモデル化すること(目的2)を目的として、上述のオンラインアンケートを用いて調査した。対応のないデザインを用い各食品技術

300名（計1,200名）に回答を得た。不正回答者を除去した1,180名を以下の解析に用いた。

目的1の各食品技術（遺伝子組み換え食品・代替肉・培養肉・昆虫食品）に対するイメージ差については、上述のアンケートに記載された心理概念を従属変数として一要因の多変量分散分析を用いて検証した。多重比較補正はボンフェローニ法を用いた。

目的2のモデル化は技術やそれに関する環境要因の評価（規制に対する信頼感、食品技術を用いたベネフィット、食品技術を用いた際の損害、周囲からの影響）が個人の心理的状态（食品技術から喚起されるポジティブ・食品技術から喚起されるネガティブ感情）に影響を与え、行動意図（摂食意図・拒絶；[4.3.3]）につながることを理論的に体系化したSORモデルに基づき解析をした。具体的には、心理的状态を介して従属変数である行動意図と関わる技術や環境要因を検証した。個人特性ではなく、技術評価や環境要因を明らかにすることで、介入策を模索することが可能になる。事前解析として、変数間の相関行列とステップワイズ回帰分析を行った（|標準化回帰係数| > .15, |相関係数| > .15, |部分相関| > .10）。回帰分析と同様に基準を満たさないパスや共分散は削除し、修正指数が50を超えたパスと共分散を追加した。結果は以下の通りである。

● 目的1 遺伝子組み換え食品・代替肉・培養肉・昆虫食品に対するイメージ

図4.3.1に示すように、各食品技術に対して心理概念が大きく異なることが明らかになった。

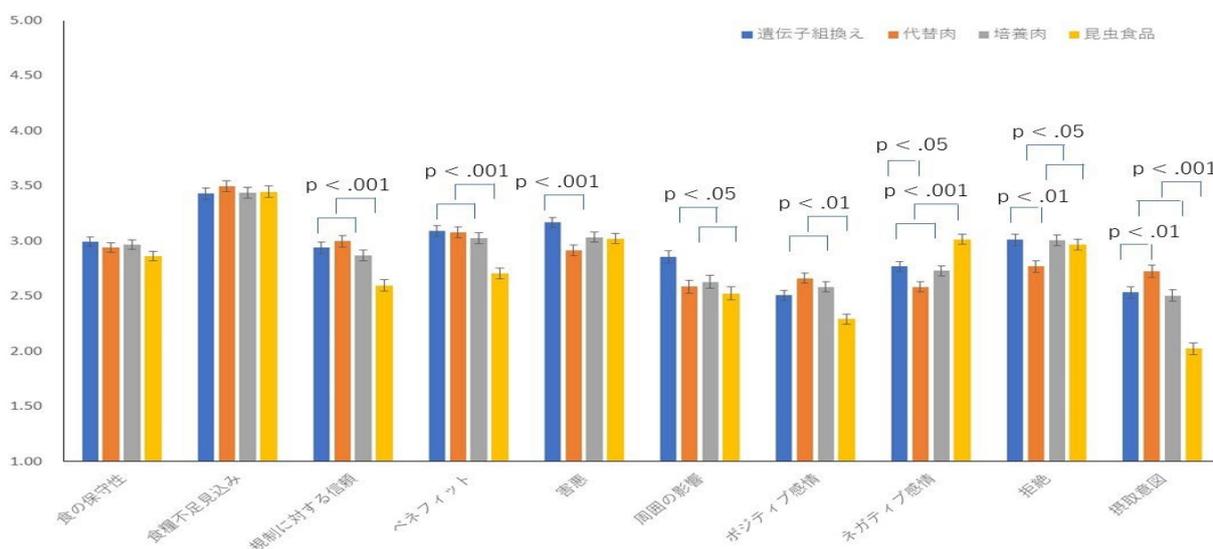


図4.3.1 遺伝子組み換え食品・代替肉・培養肉・昆虫食品に対するイメージ（エラーバーは標準誤差を示す）

● 目的2 食品技術受容・拒絶モデル

図4.3.2に示すように、食品技術に対する受容・拒絶モデルの適合度は高か

った。周囲からの影響や食品技術によるベネフィットがポジティブ感情を介して摂食意図を高めることが示唆された。また、規制に対する信頼や食品技術によるベネフィットが直接摂食意図を高めることも示唆された。反面、食品技術から受ける害悪を感じることで、ネガティブ感情を介して間接的、又は直接的に食品技術の拒絶につながるということが示唆された。

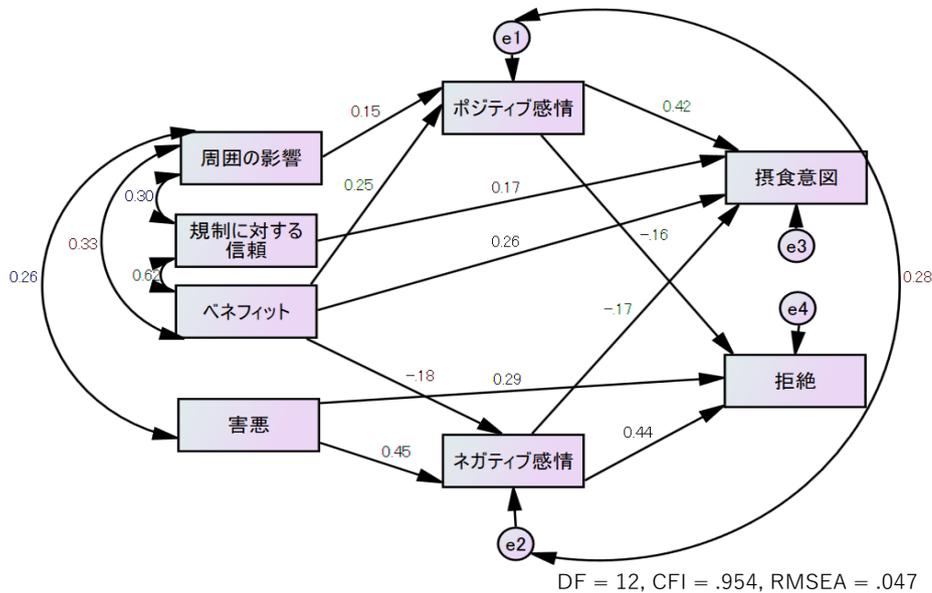


図 4. 3. 2 SOR モデルに基づく解析結果 (パスの値は標準化係数)

② 調査 2

調査 1 の結果をもとに受容度が高かった代替肉に対して代替肉を日ごろから利用する生活者と利用しない生活者を対象として調査を実施した。まず、どのように利用者と非利用者が代替肉に抱く心理概念が異なるかという差の検証 (目的 1) 代替肉を利用する使用者がどのように受容し、利用しない消費者が拒絶することにつながるのかモデル化すること (目的 2) を目的として、上述のアンケートを用いて調査した。対応のないデザインを用い各群 300 名 (計 600 名) の回答を得た。結果を以下に示す。

● 目的 1 代替肉利用者と非利用者の差

図 4. 3. 3 に示すように、代替肉利用者の代替肉に対する評価が、非利用者より顕著に好意的であることが明らかになった。

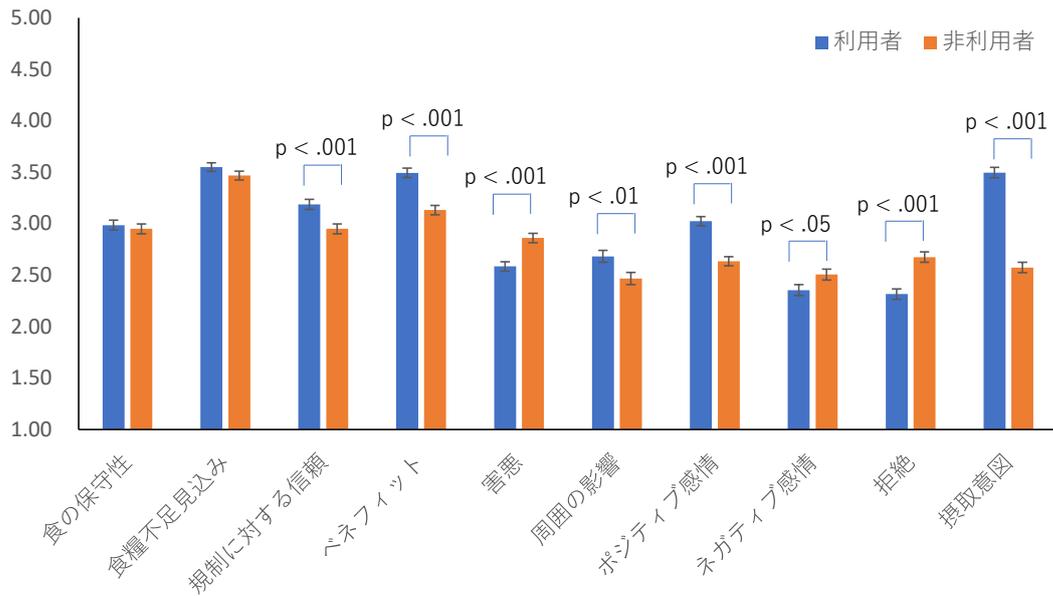


図 4. 3. 3 代替肉に対する評価（エラーバーは標準誤差を示す）

● 目的 2 代替肉利用者モデルと非利用者モデル

図 4. 3. 4 に示すように、代替肉利用者モデルは適合度が高く、周囲からの影響や規制に対する信頼感がポジティブ感情を通し摂食意図が高まること示唆された。代替肉によるベネフィットを感じることで直接摂食意図が高まることも示唆された。また代替肉非利用者モデルでは、基準より適合度が低かった。周囲からの影響がネガティブ感情を高めており、周囲でも代替肉に対して否定的な生活者が居ることがうかがえる。また、代替肉によるベネフィットを感じることでネガティブ感情を抑制し、拒絶感を弱めることが示唆された。代替肉による害悪を感じることは間接的・直接的に拒絶感を高めることが示唆された。

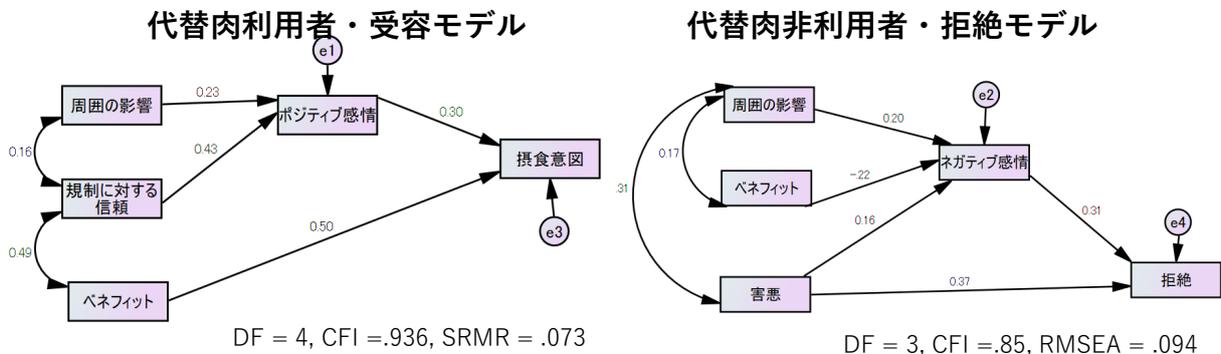


図 4. 3. 4 代替肉利用者モデルと非利用者モデル（パスの値は標準化係数）

③ 調査3

調査1の結果から受容度が高かった代替肉に対して再度調査を実施した。食品事業従事者と非従事者の間でどのように代替肉に対する心理概念が異なるかという差の検証（目的1）を目的とし、上述のアンケートを用いて調査した。対応のないデザインを用い各群300名（計600名）の回答を得た。その結果、図4.3.5に示すように、食品業従事者とその他の生活者の間に有意差はみられなかった。

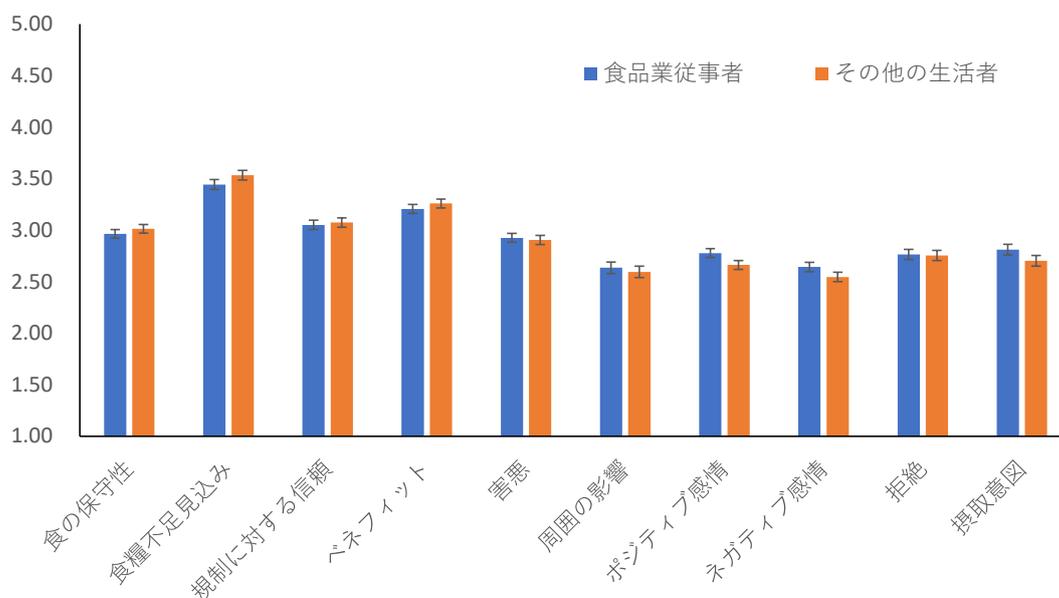


図4.3.5 代替に対する心理概念の食品業従事者とその他の生活者の差
（エラーバーは標準誤差を示す）

④ アンケート結果に対する考察

食品技術間（遺伝子組み換え食品・代替肉・培養肉・昆虫食品）の受容・拒絶感に差があるか（調査1目的1）、また、これらの食品技術の中で比較的受け入れられている代替肉の利用者非利用者間（調査2目的1）、食品業従事者と非従事者間（調査3）で心理概念の差の検証をした。さらに、食品技術の受容モデル（調査1・目的2）、代替肉の受容・拒絶モデル（調査2目的2）の構築を試みた。

調査1・目的1の解析結果により、生活者により将来的に食料不足が懸念は高いにも関わらず、代替肉以外の食品技術への受容度が低いことが明らかになった。特に遺伝子組み換え食品から受ける害悪や昆虫食へのネガティブ感情が高いため普及へのハードルが高いことがうかがえる。喫緊の課題ではないが、時間をかけて対応し変化を生むことが望まれる。

調査1・目的2の解析結果により、生活者の遺伝子組み換え食品、代替肉、培養肉、昆虫食品と言った食品技術に対する摂食意図、拒絶感につながるイメージや心理的反応を定量的にモデル化することで、介入効果が得られる変数が明らかになった。具体

的には、ポジティブ感情やネガティブ感情を介し、周囲の影響、規制に対する信頼、食品技術から感じるベネフィットが摂食意図につながる事が明らかになった。各個人の行動変容を促すことは難しいかもしれないが、周知活動によって社会規範や規制に対する信頼感、食品技術より得られるベネフィットの理解などが高まることにより、食品技術の受容が進む可能性が考えられる。反して、他の要因からのバッファ効果も見られるが、食品技術から受ける害悪が想起されてしまうとネガティブ感情を介して拒絶感が高まってしまうことが示唆された。リスクを恐れすぎること、食品技術の発展が妨げられることが危惧される。

調査2・目的1の代替肉利用者と非利用者の差の検証により、利用者の代替肉に対する評価が顕著に高いことが明らかになった。この結果だけでは、利用しているから評価が高いのか、評価が高いから利用しているのかは明らかではない。今後の実験的検証で、食経験が評価を高めるのか、評価が高いと言う認識を持つことで摂食行動につながるのかを解明する必要がある。また、利用者・非利用者共に周囲の影響やベネフィットは、それぞれポジティブ・ネガティブ感情を介して摂食意図・拒絶と関連することが示唆された。ベネフィットが感じられると摂食意図を高め、害悪が感じられてしまうと拒絶に直結することが明らかになった。この様に食品技術から害悪が感じられてしまうと、摂食の大きな妨げとなる。

調査3により、食品業に従事しているかいないかは、代替肉に対する評価に差がないことが明らかになった。しかしながら、食品研究や開発に関わる方に絞っての検証や、受容度が低い遺伝子組み換え食品などを対象とすると差がみられると考えられるが、これらは今後の課題である

これらの調査により、食品技術や食品に対する心理概念、食経験により摂食行動が異なるため、情報提供や食経験を通して拒絶が減少し、新たな食品技術により生まれた食品に対する摂食行動が増えることが考えられる。

(4) 考察

本章ではここまで、食料安全保障を対象に行ったサーベイ、ヒアリング、アンケート調査の結果について記載した。これらの調査から、食料安全保障という問題領域の特徴として以下の点が挙げられる。

① 変化・危機の実感しづらさと施策への反応の緩慢さ

日本の食料自給率の低さや生産者人口の減少などは既に社会的課題として認知されているものの、日常生活の中で急に食材が不足するわけではない。個々の消費者は物価高騰の変化には敏感であるが、食料安全保障について危機意識を持つのは容易ではない。一方、食料の安定供給に資する新たな施策が実施された場合の効果も、どの施策でどの効果が出ているのかを消費者は直接的には実感しにくい。また、生産・流通のサイクルを経て消費者に届くまでに一定の時間を要するため、即効性のある効果を望むのは困難である。さらに、効果があったとしてもそのメリットを消費者が直接

実感することも難しい。

② サプライチェーンにおける要素の多さと関係の複雑さ

食料の生産・加工・流通・消費・備蓄を含めたサプライチェーンには多くの構成要素が含まれ、新たな技術が導入された場合に要素単独での効果の評価が容易ではない。また、食品の消費期限は限定的であるため、ある食品の生産性が向上しても需要が向上しなければ価格低下や廃棄につながり逆効果に陥りかねない。社会全体としてはある程度の食料を常に備蓄する必要があるが、個々人に備蓄を強制することや特定の場所に確保することは現実的でない。食料のサプライチェーン全体を含めて食料安全保障対策を考える必要がある。

③ 食に対する消費者ニーズの高さと繊細さ

四季に恵まれ海に囲まれた日本では、季節の素材を活かしつつ海外からの影響も受容し、多様な食文化を発展させてきた。日本の食文化には、素材だけでなく旨味という味わいを際立たせた高度な調理技術、繊細で美しい盛り付けや食器、おもてなしまでが含まれる。和食は文化的な価値だけでなく栄養バランスにも優れた健康的な食事としても世界的に評価されており、ユネスコ無形文化遺産にも登録されている。このように豊かな食文化を背景として、日本の消費者は食品の味や見かけに対する要求水準が高い。特に昨今、健康志向と安全志向の高い消費者は産地やブランドに敏感である。食品は体内に摂取するものであるため、未知の食材や流通加工プロセスが不明な製品には警戒感を示す消費者も多い。一方で、産地やブランドを妄信する傾向にある消費者ほど、産地偽装食品に騙されてしまう傾向も否めない。

上述のような食料安全保障の問題領域に固有の特徴を踏まえ、生産者から消費者に至るサプライチェーン全体で効率的に食料を備蓄しリスクに備えるための工夫や努力が必要である。個々の関係者の意識や努力でサプライチェーン全体の改善への効果が見込めるとは限らず、関与する産業従事者や消費者に受容されやすく、かつ、継続的に実践可能な支援策や適用技術が求められる。そのために求められることを以下にまとめる。

① 日常的なサイクル随所への非常時対応用バッファの組み込み

● 非常時用の備蓄として機能しうる分散バッファ導入の施策

食料安全保障の観点からは国内にある程度の食料備蓄が必要である。米や小麦粉など常に国がストックしている食料もあるが、多様な食品の全てを国が備蓄することは現実的でない。また個々の消費者が災害対策などでストックできる食料はそれほど多くはなく、保存や衛生管理面でのリスクもある。生産・加工・流通を通じた食料のサプライチェーンの各段階で一定量のバッファを設けることを促す施策により、非常時のための備蓄として機能させることが求められる。

- **消費可能期間を延ばす保存・保管・包装技術**

食料サプライチェーンの随所に分散バッファが整備されれば、消費期限の長いものは供給の安定化が図れるが、消費期限の短い食材・食品については安全な保管方法がなければ廃棄量が増えるリスクとなる。美味しく食べられる期間が長くなればそれだけサプライチェーン全体として有事に対する備えとして効果的である。美味しく食べられる消費可能期間を延ばすための保存・保管・冷凍・包装などに関する技術のさらなる進展が求められる。

- **輸出用食料を迅速に国内需要に転用する施策**

日本は食糧自給率が低く食料に関しては輸入の話題が先行しがちであるが、2022年の農林水産物輸出は1.4兆円に上り過去最高となった。さらに政府は2025年に2兆円、2030年には5兆円の輸出額を目標に掲げて多岐にわたる輸出支援を推進している。平時には輸出している食料を、非常時には迅速に輸入を停止してスムーズに国内向けに転用するための施策が求められる。品目によっては現在すでに取組が開始されているが、多様なものについて迅速な転用が可能となることが望まれる。

② 食料不足をカバーできる食材開発技術・調理加工技術の実現

- **代替食材の開発と多様な用途に適応できる調理加工技術の実現**

代替肉などの代替食材はすでに開発されているが、食料の安定供給を図るためにはさらなる技術革新が求められる。国内で安定的かつ効率的に生産可能で、多様な食材の代替素材として利用可能な食品素材の開発が求められる。たとえ非常時であっても、毎日同じものを食べて過ごすのは現実的ではない。菌ごたえと旨味のある代替肉を作る試みは既に実践されているが、美味しさとリアリティのある多様な代替食品とそれを実現するための適切な調理加工技術が求められる。

- **輸入に頼らない肥料・飼料の開発**

農林水産物を生産するには肥料や飼料が不可欠であるが、日本では肥料・飼料の輸入依存率が高い。国際紛争など有事の際に肥料・飼料が不足すると食料不足につながってしまう。上述の分散バッファで備蓄するだけでなく、国内で産出可能な肥料・飼料を開発することも課題である。例えば、昆虫は人間が食すには拒否感も大きいですが、タンパク質としては比較的良質で生産するのも比較的容易でローコストである。昆虫食には添加物の観点から未知の部分もあるため、含有成分を把握し、生態系への影響も考慮した上で安全な利用技術が開発されれば魚や鶏の餌として使用できる可能性はある。昆虫に限らず、非常時には国内で調達可能な肥料・飼料の開発が望まれる。

③ 消費者の受容性向上を促す啓蒙活動

● 新素材への受容性向上を促す施策

食料は人の体内に摂取するものであり、有害なものを食べると健康や生命を脅かすことになる。新奇な食材に拒否感を示すのは人間の動物的本能とも言える。食料が不足する非常事態になって突然、食べつけない食材を与えられても受容することは困難である。平時から新しい食材やその美味しい食べ方に関する広報活動を行い、消費者の受容性向上を促す取組が求められる。

● 調理技能を継承させる装置としての代替食材の位置づけとその周知

人は、代替食材に対して「まがいもの」「もどき食品」といった偏見を持つ傾向にある。また、養殖素材は天然素材に比べて劣ると思われる傾向も強い。しかしながら、有事にあつて望ましい食材が調達できなくなる場合や、環境変化で天然の農水産物が育たなくなる可能性もある。日本の豊かな食文化は食材の素晴らしさだけでなく、高度な調理技術・技能に支えられている。例えば、養殖魚を否定した状態で天然の魚が獲れなくなった場合、その魚を調理する技能も発揮しようがなく廃れてしまう。技術・技能はソフトウェアであり、ハードウェアとしての食材や道具がなければ実践できず、ノウハウを継承することもできない。食料の問題には急な対応が難しく、食材が不足してから対策しても間に合わない。代替食材は、日本の豊かな食文化を支えるソフトウェアとしての調理技能を継承させる装置として有意義である。その意義を調理する側、消費する側双方に認知させる啓蒙活動が求められる。

5 まとめ

本報告書では、サイバーセキュリティと食料安全保障を対象として、公開文書のサーベイ、専門家へのヒアリング、利用者へのアンケートを通して技術開発や技術利用に関する政策ニーズを取りまとめた。

① サーベイ

まず、公開文書を中心としたサーベイを実施し、現在既に必要と認識され、現行の政策でも対応されているか対応が検討中である顕在的なニーズを整理した。そして、顕在的なニーズ群とそれらの相互の関係を分析しつつ、対象領域を全体的に俯瞰する観点の抽出を試みた。

② ヒアリング

サーベイによって整理した顕在的なニーズとその構造、全体を俯瞰する観点を踏まえて、各分野の専門家に対してヒアリング調査を実施した。ヒアリングを通して、顕在的なニーズ群の背後にある問題点を抽出し、現行では検討の進んでいない課題の指摘などを受けて、これからの経済安全保障に必要となりそうな潜在的なニーズの抽出を行った。

③ アンケート

並行して、受益者である国民・産業界を対象としたアンケート調査を実施した。アンケート調査では、サーベイやヒアリングから抽出した顕在的・潜在的ニーズの妥当性を確かめるとともに、技術に対する受容性や拒否感について検討した。

これらの調査を通して、サイバーセキュリティと食料安全保障という各々の問題領域の特徴を整理し、望まれる施策や対処すべき課題を第3章と第4章の考察にまとめた。

【サイバーセキュリティと食料安全保障との特徴比較から】

① 相違点：目標の明確さとスピード感覚

サイバーセキュリティは、情報を守る必要性や漏洩するリスクについては明確な問題意識が共有しやすいが、技術革新のスピードが非常に速く、対策を講じても次々に新たな脅威が出現する。新たな脅威を素早く発見して適切な技術開発や施策を準備することが常に重要である。それに対し食料安全保障に関しては、日常生活の中でひっ迫した課題として危機意識を抱くことが難しく、施策に対する効果を直接的に実感することは難しい。また、サイバーセキュリティの「情報を漏らさない」という問題意識自体が明確であるのに対し、食料の生産・流通・保存・消費のサイクルは多くの構成要素から成り、技術や施策の単独の評価が難しい。このように、今回対象とした2つの問題は特徴が大きく異なり、求められる政策や支援すべき技術課題も必然的に異なるものであった。

② 共通点：問題空間の複雑さと広大さ

一方、サイバーセキュリティと食料安全保障に共通する点として、関係する範囲が広大であり、ステークホルダとなる組織や人も多種多様であることが示された。個々の要素技術や施策が有用であったとしても、他の部分とうまく連携しなければ全体としての効果が発揮されない。したがって2つの問題領域ではいずれも、技術や制度をうまく機能させるための知識共有や組織間連携などマネジメント的側面が重要である。省庁による縦割り行政の壁を越え、官民学で連携した取組が求められる。

③ 問題領域の特徴に応じた社会受容性

アンケートでは利用者・消費者側からの観点を調べた。サイバーセキュリティについては、利用者は操作が簡単で利用メリットがあれば情報技術を受容する傾向にあり、食料安全保障に関しては心理的な拒否感がある場合には受容しにくい傾向にあることが示された。したがって、新しい情報技術の受容に当たっては、利用者の簡便さや快適性といったユーザビリティが重視され、食料技術については消費者の心理的受容性を重視した施策が求められる。安全保障に資する技術や制度が揃っても、利用者に安心して使ってもらえるとは限らない。実際に利用されるには一定の社会受容性が必要である。社会受容性を向上させるために必要なことは問題領域ごとに異なるため、対象課題の特徴を把握して適切な施策を行うことが求められる。

【調査手法の効率化に向けて】

本報告書では、サイバーセキュリティと食料安全保障という2つの問題領域の特徴を整理し、望まれる施策や対処すべき課題をまとめた。実施した調査方法は意義あるものであると考えられる。しかしながら、サーベイやヒアリング、アンケートの実施には多くの労力と時間を要する作業であり、多くの問題領域を取り扱う場合には効率化を図ることが課題となる。(なお事業項目④：統合需要分析・政策提言の報告書では、サーベイやヒアリング、アンケートの効率化を目的とした提案を行う。)

<参考文献>

- [2.2.1] 木下康仁, 定本 M-GTA : 実践の理論化をめざす質的研究方法論、医学書院, 2020.
- [2.2.2] MAXQDA maxqda.com/jp 2024年1月26日取得
- [2.3.1] 久徳康史、質問票を用いた安心感の測定に向けて, 感性工学, Vol. 19, No. 4, pp.175-178, 2022.
- [2.3.2] Carmines, E. G., & Zeller, R. A. : RELIABILITY AND VALIDITY ASSESSMENT, SAGE, 1979
- [2.3.3] 小塩真司, 西口敏文 : 質問紙調査の手順, ナカニシヤ出版, 2007
- [2.3.4] 鎌原雅彦, 宮下一博, 大野木裕明, 中澤潤 : 心理学マニュアル 質問紙法, 北大路書房, 1998
- [2.3.5] 宮本聡介, 宇井美代子 (編) : 質問紙調査と心理測定尺度—計画から実施・解析まで, サイエンス社, 2014
- [2.3.6] DeVellis, R.F. : Scale Development—Theory and Applications (4th), Sage, 2014
- [2.3.7] Finch, W.H., Immekus, J.C., & French, B.F. : Applied Psychometrics Using SPSS and AMOS, LAP, 2016
- [2.3.8] Kaplan, R.M., Saccuzzo, D.P. : Psychological Testing (7th), Wadsworth Cengage Learning, 2009
- [2.3.9] Nunnally, J.C., & Bernstein, I.H. : Psychometric Theory, McGraw Hill, 1994
- [2.3.10] Tavakol, M., & Dennick, R. : Making sense of Cronbach's alpha, International Journal of Medical Education, 2, 53-55, 2011
doi: [10.5116/ijme.4dfb.8dfd](https://doi.org/10.5116/ijme.4dfb.8dfd)
- [2.3.11] 村上宣寛 : 心理尺度の作り方, 北大路書房, 2006
- [3.1.1] <https://www.nisc.go.jp/pdf/council/cs/dai31/31shiryoku01.pdf>
- [3.2.1] 内閣府 : 防災分野における個人情報の取扱いに関する指針
<https://www.bousai.go.jp/taisaku/kojinjyouho/shishin.html>
- [3.3.1] Chen, M-F, & Li, H-F., The consumer's attitude toward genetically modified foods in Taiwan, Food Quality and Preference, Vol. 18 No.4, pp.662-674, 2007.
- [3.3.2] Gaskell, G., Stares, S., Allansdottir, A., Allum, N., Corchero, C., Fischler, C., Hampel, J., Jackson, J., Kronberger, N., Mejlgaard, N., Revuelta, G., Torgersen, H., & Wagner, W. Europeans and Biotechnology in 2005: patterns and Trends. European Commission, 2006.

- [3.3.3] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D., User acceptance of information technology: Toward a unified view. *MIS quarterly*, Vol. 27 Number 3, pp.425-478, 2003.
- [3.3.4] Venkatesh, V., Thong, J. YL., Xu, Xin., Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, Vol.36 No.1, pp.157-178, 2012.
- [3.3.5] Rodríguez-Entrena, M., & Salazar-Ordóñez, M., Influence of scientific-technical literacy on consumers' behavioural intentions regarding new food, *Appetite*, Vol. 60, pp. 193-202, 2013.
- [3.3.6] Jang, S. & Y. Namkung, Perceived quality, emotions, and behavioral intentions: Application of an extended Mehrabian-Russell model to restaurants, *Journal of Business Research*, Vol. 62 No.4, pp.451-460, 2009.
- [3.3.7] Workman, M., Bommer, W. H., & Straub, D., Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, Vol. 24 No. 6, pp.2799-2816, 2008.
- [3.3.8] Li, J., Ren, Y., Ma, W., & Yu, T., Food Safety and Rural Parents in China: Investigating an Effective Path for Risk Communication, *Health Communication*, Vol. 35 No. 14, pp. 1762-1771, 2020.
- [3.3.9] Lee, Y., Kozar, K. A., & Larsen, K. R. T., "The Technology Acceptance Model: Past, Present, and Future," *Communications of the Association for Information Systems*: Vol. 12, 2003.
- [4.1.1] 食料・農業・農村基本法(平成11年法律第106号) <https://elaws.e-gov.go.jp/document?lawid=411AC0000000106>
- [4.1.2] 日本と世界の食料安全保障(令和2年8月)
<https://www.mofa.go.jp/mofaj/files/000022442.pdf>
- [4.1.3] 食料・農業・農村政策審議会基本法検証部会(農林水産省HP)(令和5年12月閲覧)
<https://www.maff.go.jp/j/council/seisaku/kensho/index.html>
- [4.1.4] 食料・農業・農村政策審議会 答申(令和5年9月)
<https://www.maff.go.jp/j/council/seisaku/kensho/attach/pdf/17siryo-9.pdf>
- [4.1.5] みどりの食料システム戦略 本体(令和3年5月)
<https://www.maff.go.jp/j/kanbo/kankyo/seisaku/midori/attach/pdf/index-10.pdf>
- [4.1.6] 食料安全保障強化政策大綱(令和4年12月)
https://www.kantei.go.jp/jp/singi/nousui/pdf/20221227anpokyokka_honbun.pdf
- [4.1.7] 水資源問題の原因(国土交通省HP)(令和5年12月閲覧)
https://www.mlit.go.jp/mizukokudo/mizsei/mizukokudo_mizsei_tk2_000021.html
- [4.1.8] 第六次環境基本計画に向けた基本的事項に関する検討会 取りまとめ(令和5年

- 4月) <https://www.env.go.jp/content/000136282.pdf>
- [4.1.9] 不測時における食料安全保障に関する検討会 取りまとめ(令和5年12月)
<https://www.maff.go.jp/j/zyukyu/ampo/attach/pdf/kentoukai-72.pdf>
- [4.1.10] 緊急事態食料安全保障指針(令和3年7月)
<https://www.maff.go.jp/j/zyukyu/ampo/attach/pdf/shishin-16.pdf>
- [4.1.11] 食料の安定供給に関するリスク検証(令和4年6月)
https://www.maff.go.jp/j/zyukyu/ampo/attach/pdf/risk_2022-5.pdf
- [4.1.12] 食料安定供給・農林水産業基盤強化本部(第6回資料「農地の総量確保と適正・有効利用に向けた農地法制の見直し」)
https://www.kantei.go.jp/jp/singi/nousui/shokunou_dai6/siryoku4.pdf
- [4.1.13] 肥料に係る安定供給確保を図るための取組方針(令和4年12月)
<https://www.maff.go.jp/j/press/nousan/gizyutu/attach/pdf/221228-1.pdf>
- [4.1.14] 下水汚泥資源の肥料利用の拡大に向けた官民検討会(第1回資料「下水汚泥資源の肥料利用に関する現状について」)
<https://www.mlit.go.jp/mizukokudo/sewerage/content/001517796.pdf>
- [4.1.15] 総合物流施策大綱(2021年度~2025年度)(令和3年6月)
<https://www.maff.go.jp/j/shokusan/ryutu/attach/pdf/buturyu-68.pdf>
- [4.1.16] 緊急事態食料安全保障指針(局地的・短期的事態編)(令和3年7月)
<https://www.maff.go.jp/j/zyukyu/ampo/attach/pdf/shishin-19.pdf>
- [4.1.17] 気候変動影響評価報告書 総説・詳細(令和2年12月)
<https://www.env.go.jp/content/900516663.pdf>
<https://www.env.go.jp/content/900516664.pdf>
- [4.1.18] フードテック推進ビジョン(令和5年2月)
<https://www.maff.go.jp/j/shokusan/sosyutu/attach/pdf/index-19.pdf>
- [4.1.19] 重要物資の安定的な供給の確保に関する制度
https://www.cao.go.jp/keizai_anzen_hosho/supply_chain.html
- [4.1.20] 飼料をめぐる情勢
https://www.maff.go.jp/j/chikusan/sinko/lin/l_siryoku/attach/pdf/index-1012.pdf
- [4.1.21] 飼料用米をめぐる情勢について
<https://www.maff.go.jp/j/seisan/kokumotu/attach/pdf/siryokuqa-124.pdf>
- [4.1.22] 持続可能な物流の実現に向けた検討会 最終取りまとめ(令和5年8月)
https://www.meti.go.jp/shingikai/mono_info_service/sustainable_logistics/pdf/20230831_1.pdf
- [4.1.23] 食料・農業・農村基本法の検証・見直しに関する国民からの意見・要望(令和5年9月)
<https://www.maff.go.jp/j/council/seisaku/kensho/attach/pdf/17siryoku-7.pdf>
- [4.1.24] 「フードテック推進ビジョン(案)」及び「ロードマップ(案)」に対する御意

見の概要と御意見に対する考え方 <https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000249722>

- [4.1.25] 持続可能な物流の実現に向けた検討会 最終取りまとめ（案）に対する意見公募
手続の結果について <https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000258846>

- [4.3.1] Prati, G., Peitranтони, L., & Zani, B. The prediction of intention to consume genetically modified food: Test of an integrated psychosocial model, *Food Quality and Preference*, Vol. 25 No. 2, pp.163-170, 2012.
- [4.3.2] Folwarczny, M., Li, N. P., Sigurdsson, V., Tan, K. L., & Otterbring, K. Development and psychometric evaluation of the Anticipated Food Scarcity Scale (AFSS), *Appetite*, Vol.166, pp.105474, 2021.
- [4.3.3] Laumer, S., & Eckhardt, A., Why do people reject technologies: a review of user resistance theories. *Information Systems Theory: Explaining and Predicting Our Digital Society*, Vol. 1, pp. 63-86, 2012.

<参考資料 1> サイバーセキュリティサーベイ

(1) サイバーセキュリティ戦略と附属文書

- ・サイバーセキュリティ戦略本部 サイバーセキュリティ戦略（令和 3 年 9 月 28 日）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf>
- ・サイバーセキュリティ戦略本部 サイバーセキュリティ戦略（平成 30 年 7 月 27 日）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2018.pdf>
- ・サイバーセキュリティ戦略本部 サイバーセキュリティ戦略（平成 27 年 9 月 4 日）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku.pdf>
- ・サイバーセキュリティ戦略本部 サイバーセキュリティ 2023（2022 年度年次計画・2023 年度年次報告）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023.pdf>
- ・サイバーセキュリティ戦略本部 サイバーセキュリティ 2022（2021 年度年次計画・2022 年度年次報告）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf>
- ・サイバーセキュリティ戦略本部 サイバーセキュリティ 2021（2020 年度年次計画・2021 年度年次報告）
<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf>

(2) サイバーセキュリティ本部構成員が主任の大臣等である行政機関のサイバーセキュリティに関する文書

- ・サイバーセキュリティ戦略本部 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針
<https://www.mlit.go.jp/sogoseisaku/jouhouka/content/001310076.pdf>
- ・総務省 ICT サイバーセキュリティ総合対策 2023
https://www.soumu.go.jp/main_content/000895981.pdf
- ・総務省 国民のためのサイバーセキュリティ
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html
- ・総務省 サイバーセキュリティ対策についての産業界へのメッセージ
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20220411.pdf
- ・総務省 無線 LAN (Wi-Fi) の安全な利用 (セキュリティ確保) について
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/index.html
- ・総務省 テレワークにおけるセキュリティ確保
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/index.html
- ・デジタル庁 情報システムの整備及び管理の基本的な方針
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/06ecbaa1-128e-4435-856d-591adb3369ea/20211224_development_management_02.pdf

- ・警察庁 サイバー警察局の取組 <https://www.npa.go.jp/bureau/cyber/index.html>
- ・金融庁 金融分野におけるサイバーセキュリティ強化に向けた取組方針（令和4年2月、Ver. 3.0）
<https://www.fsa.go.jp/news/r3/cyber/cyber-policy.pdf>
- ・金融庁 金融分野におけるサイバーセキュリティ強化に向けた取組方針（平成30年10月、Ver. 2.0）
<https://www.fsa.go.jp/news/30/20181019/cyber-policy.pdf>
- ・厚生労働省 産業サイバーセキュリティ研究会の各種ドキュメント
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/
- ・厚生労働省 サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書 <https://www.meti.go.jp/press/2023/11/20231122002/20231122002.html>
- ・国土交通省 鉄道分野における情報セキュリティ確保に係る安全ガイドライン 第4版
<https://www.mlit.go.jp/common/001283894.pdf>
- ・国土交通省 物流分野における情報セキュリティ確保に係る安全ガイドライン 第4版
<https://www.mlit.go.jp/common/001283898.pdf>
- ・国土交通省 航空分野における情報セキュリティ確保に係る安全ガイドライン 第5版
<https://www.mlit.go.jp/common/001283895.pdf>
- ・国土交通省 空港分野における情報セキュリティ確保に係る安全ガイドライン 第2版
<https://www.mlit.go.jp/common/001283896.pdf>
- ・外務省 エンドツーエンド暗号化及び公共の安全に関する国際・ステートメント https://www.mofa.go.jp/mofaj/la_c/sa/co/page22_003432.html

(3) デジタル社会の実現に向けた重点計画関連文書

- ・デジタル庁 デジタル社会の実現に向けた重点計画（令和5年6月9日）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
- ・デジタル庁 同工程表
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/5f426b4a/20230609_policies_priority_outline_07.pdf
- ・デジタル庁 同施策集
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/1f29f2f7/20230609_policies_priority_outline_09.pdf
- ・デジタル庁 同施策集の別表
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-

(4) デジタル・ガバメント中長期計画関連文書

- ・総務省 総務省デジタル・ガバメント中長期計画
https://www.soumu.go.jp/main_content/000841514.pdf
- ・法務省 法務省デジタル・ガバメント中長期計画
<https://www.moj.go.jp/content/001381116.docx>
- ・外務省 外務省デジタル・ガバメント中長期計画
<https://www.mofa.go.jp/mofaj/files/100442628.docx>
- ・財務省 デジタル社会の実現に向けた重点計画に基づく財務省中長期計画
https://www.mof.go.jp/about_mof/other/e-j/zaimu-honbun.pdf
- ・文部科学省 「デジタル社会の実現に向けた重点計画」に基づく「文部科学省における中長期的な計画」
https://www.mext.go.jp/content/20220831-mxt_kanseisk01-000024737_1.docx
- ・厚生労働省 厚生労働省における政府情報システムの整備及び管理に関する中長期計画
<https://www.mhlw.go.jp/content/001011828.pdf>
- ・農林水産省 デジタル社会の形成に向けた農林水産省中長期計画
<https://www.maff.go.jp/j/kanbo/dx/attach/pdf/degigov-10.pdf>
- ・経済産業省 経済産業省デジタル・ガバメント中長期計画
https://www.meti.go.jp/policy/digital_transformation/asset/meti-dx/20221014/honbun-dejigaba-chuchouki-keikaku-meti.pdf
- ・国土交通省 デジタル社会の実現に向けた重点計画に基づく国土交通省における中長期計画
<https://www.mlit.go.jp/appli/content/001585525.pdf>
- ・環境省及び原子力規制委員会 環境省及び原子力規制委員会におけるデジタル社会の実現に向けた中長期的な計画
<https://www.env.go.jp/content/000109033.pdf>
- ・防衛省 防衛省デジタル・ガバメント中長期計画
<https://www.mod.go.jp/j/policy/hyouka/jyouhouka/pdf/honbun.pdf>
- ・デジタル庁 情報システムに関する中長期計画
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/06ecbaa1-128e-4435-856d-591adb3369ea/ee5934d2/20221014_policies_development_management_plan_01.docx
- ・警察庁 デジタル社会の実現に向けた重点計画に基づく警察庁中長期計画
https://www.npa.go.jp/policies/policy/digital/honbun_npa.pdf
- ・金融庁 金融庁デジタル・ガバメント中長期計画
https://www.fsa.go.jp/policy/digital_government/20220916fsadigital_government.docx

<参考資料2> デジタル社会の実現に向けた重点計画等からみた政策課題と技術ニーズ

表 デジタル社会の実現に向けた重点計画等からみた政策課題と技術ニーズ

	方針	ルール	システム	具体的又は短期的技術ニーズ	当面の追加的ニーズ	中長期的な研究開発ニーズ
国の情報システムの刷新	デジタル庁による方針策定等	「デジタル・ガバメント推進標準ガイドライン」改訂				
	各府省庁の中長期計画	デジタル庁によるシステム関連予算の一括計上				
	デジタル庁と各府省の協働プロジェクト推進		登記情報、国税情報、社会保険オンライン、ハローワーク、特許事務等の各システム等	共通機能の活用		
	クラウド化の推進	ガバメントクラウドの推進	Government Solution Service (GSS)	マルチクラウド	独法、地方公共団体、準公共分野への展開	
	ネットワーク整備	国のネットワークの全体最適かつ効果的なネットワーク構成	Government Solution Service (GSS)	オーバーレイネットワーク	国・地方を通じたデジタル基盤の将来像・実現シナリオ	
	府省LANと認証基盤の統合		GSS 情報ポータル、職員認証システム (GIMA)	ゼロトラストアーキテクチャ	地方公共団体職員の考慮	
	運用監視	統合運用監視				
地方の情報システムの刷新	20 業務の標準化	「地方公共団体情報システムの標準化に関する法律」、「標準化基準」	標準化システム	標準化された基幹業務 (20 業務) システム (各ベンダー開発 + 自治体の適合性確認)		
	クラウド化の推進	ガバメントクラウドの推進		追加業務システム、標準化システムとの連携 API		
デジタル化を支えるインフラの整備	高度情報通信ネットワークの整備	「デジタル田園都市国家インフラ整備計画」	光ファイバ (人口カバー率 99/9%=2027 末)、5G (4G と合わせて国道・高速道路カバー率 99%=2030 末)	・5G 光ファイバの大容量化技術 ・非地上系ネットワークの整備	・光ファイバの大容量化 ・Beyond 5G ・デジタルライフライン全国総合整備計画策定	
	半導体戦略の具体化	「半導体・デジタル産業戦略」			人材育成に向けた産官学連携と拠点形成	
	データの分散立地推進等	「デジタル田園都市国家インフラ整備計画」		分散型クラウド関連技術 (消費電力効率化技術を含む)	東京・大阪を補完代替する中核拠点整備	

	国際的なデータ流通のハブとしての機能強化		日本周回海底ケーブル	・日本海側国内海底ケーブルの整備 ・国際海底ケーブルや陸揚局安全対策技術		
	デジタルライフレイン整備	「デジタルライフレイン全国総合整備計画」	・送電塔等に係るドローン航路の設定 ・自動運転車用レーンの設定(新東名高速) ・地下空間情報のデジタルツイン	・自動車の自動運転技術 ・デジタルツイン技術	デジタル田園都市国家構想総合戦略を踏まえた計画策定	
国や地方公共団体の手続等の更なるデジタル化に関する具体的な施策	裁判関連手続のデジタル化		・Web会議システム ・準備書面等電子提出システム		民事執行・民事保全・倒産・家事事件等の手続のデジタル化	
	司法試験及び司法試験予備試験のデジタル化		Computer Based Test (CBT) システム			
	警察業務のデジタル化		・運転者管理システム ・遺失物管理システム ・交通反則金の納付方法の多様化に対応するシステム			
	港湾業務(港湾管理分野及び港湾インフラ分野)のデジタル化		・港湾管理者が提供するサービスに係るシステム ・港湾台帳情報等を電子化し、港湾インフラの整備・保全に関する他の主体の保有する情報と連携するシステム		・港湾の計画から維持管理・利用までの適切なアセットマネジメント手法構築 ・港湾業務(港湾管理分野及び港湾インフラ分野)のデジタル化と港湾(港湾物流分野)のデジタル化を合わせたサイバーポート3分野での一体運用	
	公文書管理のデジタル化	「デジタル時代の公文書管理について」	公文書管理システム		新しいルールに合わせたシステムのあり方の検討	
	情報公開事務のデジタル化	「規制改革実施計画」			順次の実現	
	人事管理のデジタル化	勤務時間管理をはじめとする各府省の人事管理の効率化・高度化	人事管理システム		勤務時間管理システム等の他システムとの連携	

	政府調達システムのシステム連携		請求書等とのデータ連携システム			
	行政の手続におけるキャッシュレス化		政府共通決済基盤		機能拡張	
	旅券（パスポート）申請のデジタル化		戸籍情報連携システムにより提供される戸籍電子証明書を利用できるオンライン申請システム		配送交付	
	入国手続等のデジタル化	入国手続（検疫、入国審査、税関申告）の利便性向上と効率化	Visit Japan Web		機能拡充	
	国税関係手続のデジタル化	納税者の自発的な納税義務の履行を円滑かつ適正に実現するためのデジタルの活用	<ul style="list-style-type: none"> ・国税庁ホームページ ・チャットボット ・確定申告書等作成コーナー ・国税電子申告・納税システム（e-Tax） 	機能の整理と連携に必要な技術	既存システムのマイナポータルとの連携拡充 年末調整控除申告書作成用ソフトウェア等の利用促進	
デジタル社会に必要な技術の研究開発・実証の推進	技術水準の向上によるデジタル技術応用先飛躍的拡大を通じたユーザーの利便性向上、日本産業の国際競争力大幅強化					
	うち、高度情報通信環境の普及促進に向けた研究開発・実証	2023年度（令和5年度）以降にローカル5Gの柔軟な運用を可能とする制度整備		ローカル5G技術	制度整備	

	<p>うち、高度情報通信環境の普及促進に向けた研究開発・実証</p>	<p>Beyond 5G (6G) について情報通信審議会中間答申(2022年(令和4年)6月30日)を踏まえ、重点技術分野を中心として、社会実装・海外展開を目指した研究開発推進</p>		<p>Beyond 5G 技術</p>	<ul style="list-style-type: none"> ・通信インフラの超高速化・超低遅延化・超省電力化等を実現するためのオール光ネットワーク技術 ・陸海空をシームレスに繋ぐ通信カバレッジの拡張を実現するための衛星・HAPS 等の非地上系ネットワーク (NTN) 技術 ・利用者にとって安全で高信頼な通信環境を確保するためのセキュアな仮想化・統合ネットワーク技術
	<p>うち、データ活用を支える高度コンピューティング技術の研究開発・実証:AI の社会実装に向けた取組の加速</p>	<p>AI に対する不安の払しょくに向け、AI による処理の根拠を人が理解できるようにすること(取組) 「AI 戦略 2022」</p>		<ul style="list-style-type: none"> ・データ秘匿性を担保したまま機械学習の処理を行うための研究開発 ・研究データ基盤の改善等 	<ul style="list-style-type: none"> ・AI 利活用を支えるデータの充実等に向けた研究開発 ・創薬・材料科学など、我が国が強みを有する分野における AI の利活用研究開発
	<p>うち、データ活用を支える高度コンピューティング技術の研究開発・実証: 情報処理の高度化のための次世代コンピューティング技術: エッジコンピューティング</p>	<p>高速化と低消費電力化を両立する次世代コンピューティング技術</p>		<p>エッジコンピューティング ・エッジコンピューティング用 AI 半導体技術 ・AI 半導体等に係るチップレット技術 ・インターフェースの実施技術研究</p>	<ul style="list-style-type: none"> ・エッジコンピューティング技術及び AI の応用として、防災・減災に資するリモートセンシングデータをリアルタイムに提供する AI 等を活用したデータ圧縮・復元技術の研究開発 ・古典コンピュータと量子コンピュータ等の資源を連合学習や秘密計算、光伝送などの技術で安全に繋ぐ研究開発 ・様々な計算資源を最適に制御する計算資源マネージャの研究開発

	うち、データ活用を支える高度コンピューティング技術の研究開発・実証：情報処理の高度化のための次世代コンピューティング技術：量子技術	高速化と低消費電力化を両立する次世代コンピューティング技術 「量子技術イノベーション戦略」 「量子未来社会ビジョン」		量子技術 ・量子コンピュータ技術（NISQ 量子コンピュータ における 100 量子ビット実装とそのクラウドサービス開始＝2025 まで等） ・古典コンピュータと量子コンピューティングを繋いで量子アプリケーションを開発する技術（環境）	①重点領域の設定、②量子拠点の形成、③国際協力の推進	量子コンピューティング及び量子通信技術 ・誤り耐性型汎用量子コンピュータの2050年（令和32年）までの実現 ・量子暗号通信に関する研究開発
	うち、安全・安心なデジタル社会を支える高度セキュリティ技術：サイバーセキュリティ	「サイバーセキュリティ戦略」		不正なプログラムが仕込まれていないことを確認するためのソフトウェアの研究開発 サイバー攻撃の観測・把握・分析技術の研究開発 サイバー攻撃に係る情報共有基盤の研究開発 自由で安全・安心なデータ流通と両立する収集・解析・連携基盤の構築に係る技術の研究開発	研究開発の国際競争力の強化や産学官エコシステムの構築と、実践的な研究開発の推進	量子コンピュータに対抗する技術開発 ・耐量子計算機暗号 ・量子暗号通信 ・量子インターネット
	うち、安全・安心なデジタル社会を支える高度セキュリティ技術：秘密計算	情報漏洩の防止やプライバシー保護と高度なデータ分析の両立		復号・復元をせずにデータ処理を行える技術	社会実装に向けた検討（これまで扱えなかった情報を扱うことへの理解など）	秘密計算の早期実用化に向けた研究開発

	<p>うち、研究開発・実証を支えるデータ利活用の環境整備とデータ駆動型研究の推進</p>	<p>新たな科学的手法を発展させ、生産性を飛躍的に向上させる</p>	<p>国レベルの研究デジタルインフラの（「富岳」、HPCI（革新的ハイパフォーマンス・コンピューティング・インフラ）、「SINET」、研究データ基盤）等が高度化されたシステム</p>	<ul style="list-style-type: none"> ・気候変動・レジリエンス分野における観測・予測データの共有・利活用や分野横断的な研究開発を促進するデータ・解析プラットフォームの形成 ・防災情報等の先進的なセンシング・モニタリング手法の開発とデータの統合基盤の整備・活用を通じた防災・減災に資する情報プロダクツの創出や災害対応 DX の研究開発 ・マテリアル分野でのマテリアルデータを全国で一元的に利活用するためのシステム 	<p>膨大な量で高品質なデータを戦略的に収集・共有・利活用するための仕組みの構築</p>	<ul style="list-style-type: none"> ・マテリアル、ライフサイエンス、気候変動・レジリエンス、人文社会等における各分野の特性・状況に応じた価値創造を目指した研究データの戦略的な創出・統合・利活用 ・「研究 DX プラットフォーム」の構築
--	--	------------------------------------	---	--	--	--

※この表のうち、「短期的又は具体的技術ニーズ」の欄が空欄であるものは、既存技術の適用又は応用で対応できることを示す。