ISFJ2016　政策フォーラム発表論文

サイバーセキュリティ対策を目的とした新税の創設

同志社大学　風間 規男研究会　財政①分科会
三島 望
西村 菜織
東 紗也華
井土 楽
水谷 理菜
岡本 美友香

2016 年 11 月

要約

第 1 章　現状分析・問題意識

近年、サイバー攻撃・犯罪の手口は多様化し、これらが社会に与える脅威は計り知れない。しかし、日本のサイバーセキュリティ対策は多くの問題を抱えている。

まず、日本の情報セキュリティ予算の総額が少ないことである。サイバーセキュリティ対策に対して各府省庁が要求した予算額と実際に政府が割り当てた予算額には大きな差がある。各府省庁が対策に多くの予算が必要であると認識し要求しているにも関わらず、政府は十分な予算を割り当てていないのである。さらに予算には、激しい増減がみられ安定していないこともうかがえる。

日本では、サイバーセキュリティ対策において、各府省庁の縦割り行政が排除しきれていない状況にある。それは、政府全体として十分な連携・調整が図られておらず、それぞれ独立して政策が立案・実施されていることを示す。それに加え、サイバーセキュリティ対策の立案には極めて高い専門性が必要であるにも関わらず、同類の分野に対し複数の各府省庁が取り組んでいる状況にあることから、高水準の知識をもった専門家が政策を主導する環境が整えられているとは言い難い。

昨今サイバー攻撃・犯罪のリスクが高まっており、将来更に高まることが予想されている。しかし、①十分で安定した予算確保がなされていない②縦割り行政により対策が効率的に展開されていないという 2 点が現在のサイバーセキュリティ対策の抱える問題点であると認識し、改善が必要であると考察した。

第 2 章 先行研究

先行研究として、①村野 (2015)「情報通信技術の進展とサイバーセキュリティ（科学技術に関する調査プロジェクト 2014)」、②Sonnenreich, Albanese, and Stout (2006) “Return On Security Investment (ROSI)– A Practical Quantitative Model”、③杉野 (2016)「サイバー攻撃と情報セキュリティ」の 3 つの研究を取り上げた。

まず、村野(2015)は、インターネットの普及とサイバー攻撃・犯罪の関係性を示したが、実際に数値化し検証されてはいない。つぎに、Sonnenreich 他 (2006)の論文では、計算式(ROSI)を作成し、組織のサイバーセキュリティ対策に関する投資対効果を明らかにした。しかし、サイバーセキュリティ対策への投資費用とサイバー攻撃・犯罪の関係性までは言及されていない。最後に、杉野 (2016)は、情報セキュリティ確保のための 7 つの取り組みを示したが、これらは実証分析がされないまま提言されているため、サイバーセキュリティ被害の減少に効果的であるとは言い難い。

そこで我々は、上記 3 つの先行研究の課題を解消するため、①サイバーセキュリティ被害とインターネットの普及および投資の関係の検証と②サイバーセキュリティの被害を効果的に減少させる具体的な取り組みの検証の 2 つの分析を行う。これら 2 つの分析を同時に行った点が、本稿の独自性といえる。

第 3 章 分析

第 1 節では、「サイバー攻撃・犯罪が増える原因として、インターネット端末(携帯電話・パソコン・スマートフォン・タブレット端末)の普及があり、政府の情報セキュリティ関連予算はサイバー攻撃・犯罪を減らす可能性がある」という仮説を立て、パネルデータを用いた多重回帰分析を行った。この分析によって、携帯電話、パソコン、タブレット端末の保有率はサイバー攻撃・犯罪の増加と相関するものであり、情報セキュリティ関連予算総額の上昇は、サイバーセキュリティ対策の向上に有効であることを実証した。

第 2 節においては、「投資を行う効果的な取り組みの実証分析」をして、資金を集中的に投資する重点項目を検討する。この分析に使用する変数として経済産業省「情報処理実態調査」のデータを使用した。そして、2010 年～2014 年の 5 年間のパネルデータを用いて多重回帰分析を行った。この分析によって、セキュリティに関する認識、施策、人材、対策予算の大きさはセキュリティ被害に対して有効であることが明らかとなった。

第 4 章 政策提言

集中的かつ継続的に投資するための安定的な財源確保の手段として、我々は新たな税である「サイバーセキュリティ対策税」を特別財源として徴収することを提言する。

第 1 節では、サイバーセキュリティ対策税の意義を述べた。まず、新税を導入する意義として、第 1 章の現状分析を踏まえて、サイバーセキュリティ対策の緊急性について述べた。次に、予算の増減の激しさに対して、継続的かつ集中的な投資が必要であると主張した。

第 2 節では、サイバーセキュリティ対策税の正当性について議論を展開した。我々は課税対象として、原因の 1 つであるインターネット端末に課税する。この点において、正当性を示すため、サイバーセキュリティ対策税と同様の理由で課税対象を定めた既存の税の中から石油・石炭税、地球温暖化対策税の 2 つを例に挙げた。さらに、公平の原則、中立の原則、簡素の原則という税の三原則すべてに当てはまっていることから、税としての正当性もいえる。加えて、特定財源化の効果として、公平性、安定性、合理性を挙げ、特定財源として新税を導入する利点を示した。最後に、特別会計の 3 つの設置要件もすべて満たしているため、特別財源として徴収することは法律上も可能であることを明らかにした。

第 3 節では、サイバーセキュリティ対策税の制度を詳しく説明した。課税対象は、第 3 章の分析結果を踏まえて、インターネット端末とした。課税対象をインターネット端末とする政策上の利点として、保有率が高く安定した税収が見込めることが挙げられる。徴税方法としては、端末価格に税率を課し、販売事業者が納税する。税率は痛税感を考慮して 1%～3%とする。この税率で税を徴収する場合、年間約 1590～4770 億円の税収を見込むことができる。

第 4 節では、想定される課題として①二重課税②端末 0 円携帯に対する課税③海外での現地購入や海外からの個人輸入④IoT の普及が進む中での課税対象拡大の 4 点を挙げ、考察した。

第 5 節では、税収の使い道について第 3 章で行った分析結果や関連資料から①対処能力の向上（捜査・分析用資機材の整備等を実施）②人材育成・教養・訓練の充実・強化③新技術に関する研究の推進④官民連携の推進⑤国際連携の推進を重点項目とした。

なお、この政策の所管として、既存の機関(内閣府・内閣サイバーセキュリティセンター・総務省・経済産業省)を比較検討し、それぞれに解消しえない問題を抱えていることを明らかにした。そこで我々は、「サイバーセキュリティ庁」新設も選択肢の 1 つであるとした。

第 6 節では、政策実現後のビジョンを示した。我々の問題意識がサイバーセキュリティ対策税導入により、解消される過程は以下の通りである。第 1 項における、「予算の不足・不安定さ」の問題は、サイバーセキュリティ対策税を特定財源として確保することにより、社会情勢・経済状況などの影響を受けにくく、継続的・安定的にサイバーセキュリティ対策に投資することが可能となる。「縦割り行政」の問題は、サイバーセキュリティに関する施策を調整し、有効な政策を開発する「サイバーセキュリティ庁」新設などによる組織改革を進めることで緩和されていくことが期待できる。

第 2 項では、政策実現後の波及的・長期的な効果として①マイナンバーの普及②経済的・政治的打撃の軽減③2020 年東京オリンピック・パラリンピック競技大会（以下東京オリンピック）の安全性の向上④国民のサイバーセキュリティの意識向上をあげた。

我々は、日本のサイバーセキュリティにおける脆弱性を打破し、サイバー攻撃・犯罪を未然に防ぐべく、この政策を提言する。

目次

はじめに

今やインターネットの普及は目覚ましく、日本においては、平成 26 年末のインターネット利用者数は 1 億 18 万人、インターネットの人口普及率は 82.8%である。さらに、世界におけるインターネットの利用者数は、34 億 9 千万人に達するといわれている。そのため、世界中の誰もが容易にアクセスできるサイバー空間は、社会活動、経済活動、軍事活動等のありとあらゆる活動が依拠する場となっている。

その反面、サイバー空間において国家の秘密情報の窃取、重要インフラの破壊など、企業や政府の情報システムを狙うサイバー攻撃・犯罪は頻発しており、その悪質度は増し深刻化しつつある。この脅威に対して、日本では 2014 年のサイバーセキュリティ基本法の制定をはじめ、サイバーセキュリティ対策の強化が進められている。我が国ではサイバーセキュリティ対策が国の重要な政策として早急に取り組まれるべき理由は 2 つあると考えた。1 つ目はマイナンバー制度である。2015 年、社会保障･税制度の効率性･透明性を高め、国民にとって利便性の高い公平･公正な社会を実現するための基盤であるマイナンバー制度が導入された。しかし、現在、普及率は 5%にとどまっている。普及率の低さの原因として情報被害が生じる危険性が挙げられ、セキュリティ強度の向上が課題とされている。2 つ目は 2020 年の東京オリンピックである。2012 年、ロンドンオリンピックでは、オリンピックの公式サイトに対し 2 週間の開催期間で 2 億 2,100 万のサイバー攻撃があった。また、2008 年の北京オリンピックでは 1 日に 1,400 万回のなにかしらの攻撃があったことが明らかになり、日本も未然防止に取り組むべきであることは言うまでもない。

本稿では、サイバーセキュリティの問題にどのようにアプローチしていくべきか探るため、文献調査・インタビュー調査に加えて、データ分析を行う。分析では、インターネットの進展およびサイバーセキュリティ投資がサイバー攻撃・犯罪にどのような影響を与えるのかをパネルデータを用いて多重回帰分析で検証する。それに加えて、より効果的にサイバーセキュリティを向上させるため、対策における重点項目を明らかにする。

この結果をもとに、予算を安定的かつ継続的に投資し、対策を効果的に展開するための体制を整備する「サイバーセキュリティ対策税」を提案する。

この政策の実現によって、対策に応じた継続的な投資が可能になり、政策立案も専門的なものとなり、サイバーセキュリティ対策の一層の強化を目指す。

第 1 章　現状分析・問題意識

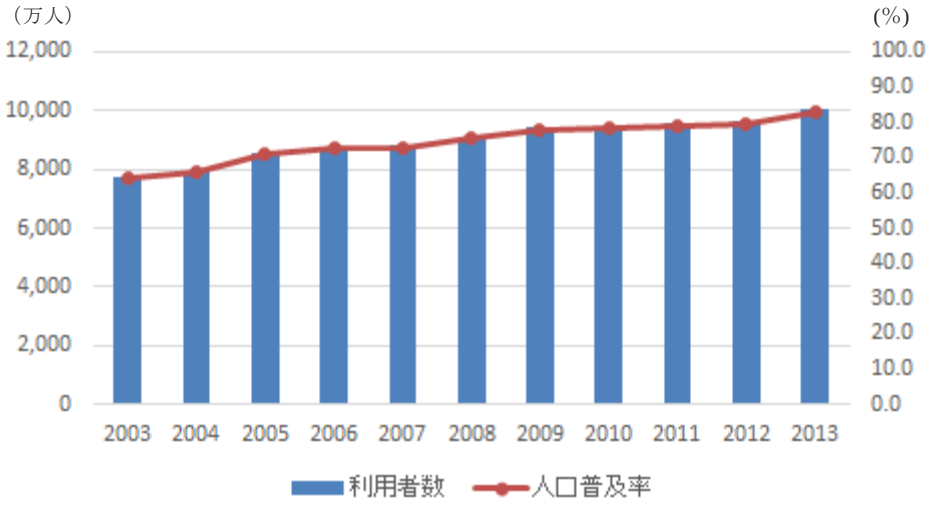
本章では、第 1 節から第 4 節で現状分析について述べ、第 5 節で問題意識について述べる。

第 1 節　インターネットの普及

第 1 項　インターネットの利用動向

日本におけるインターネットの普及は目覚ましい。図 1 は、2003 年から 2013 年までの 11 年間のインターネットの利用者数及び人口普及率の推移を示したグラフである。この図から、利用者及び普及率ともに右肩上がりになっていることが分かる。2013 年においては、利用者数は 1 億人を突破し、普及率は 8 割を越していることから、我々にとってインターネットは欠かせない存在となっている。

図 1　インターネットの利用者数及び人口普及率の推移



総務省（2014）　「情報通信白書」より筆者作成

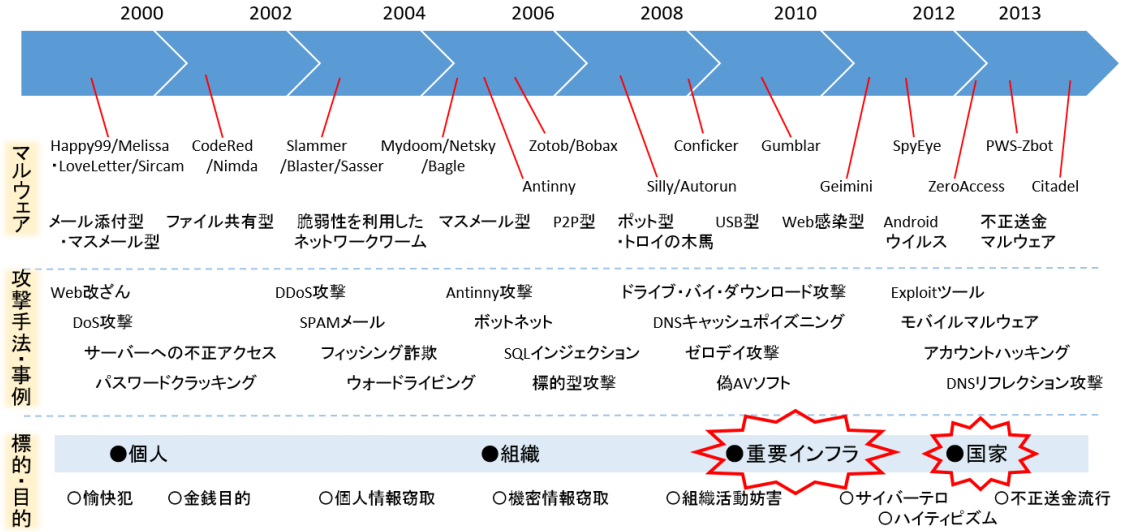
第 2 節　サイバー攻撃・犯罪についての脅威

第 1 項　サイバー攻撃・犯罪の高度化と多様化

本稿の定義としては、サイバー攻撃とは、インターネットサーバーへの不正侵入によるデータ詐欺や破壊、改ざんのことであり、サイバー犯罪とは、不正アクセス禁止法違反、及び、コンピュータ等のネットを利用した犯罪のことを指す。図 2 は、情報セキュリティに係るサイバー攻撃・犯罪の脅威の変遷を示したものである。情報セキュリティすなわち

サイバーセキュリティ[1]とは情報の機密性、完全性及び可用性を維持することの安全性・信頼性の確保のための措置である。また、図 2 から分かる様に、マルウェア[2]、攻撃手法・事例についてはほぼ毎年のように新種の形態が出現しており、標的・目的も個人を標的とした愉快犯から組織・重要インフラ・国家を標的とした経済犯・組織犯に移行している。つまり、情報セキュリティ上の脅威は年々高度化・多様化しているのである。
そして、そのような状況に伴い、実際にサイバー攻撃・犯罪の検挙数も年々増加傾向にある。

図 2　情報セキュリティに係る脅威の変遷



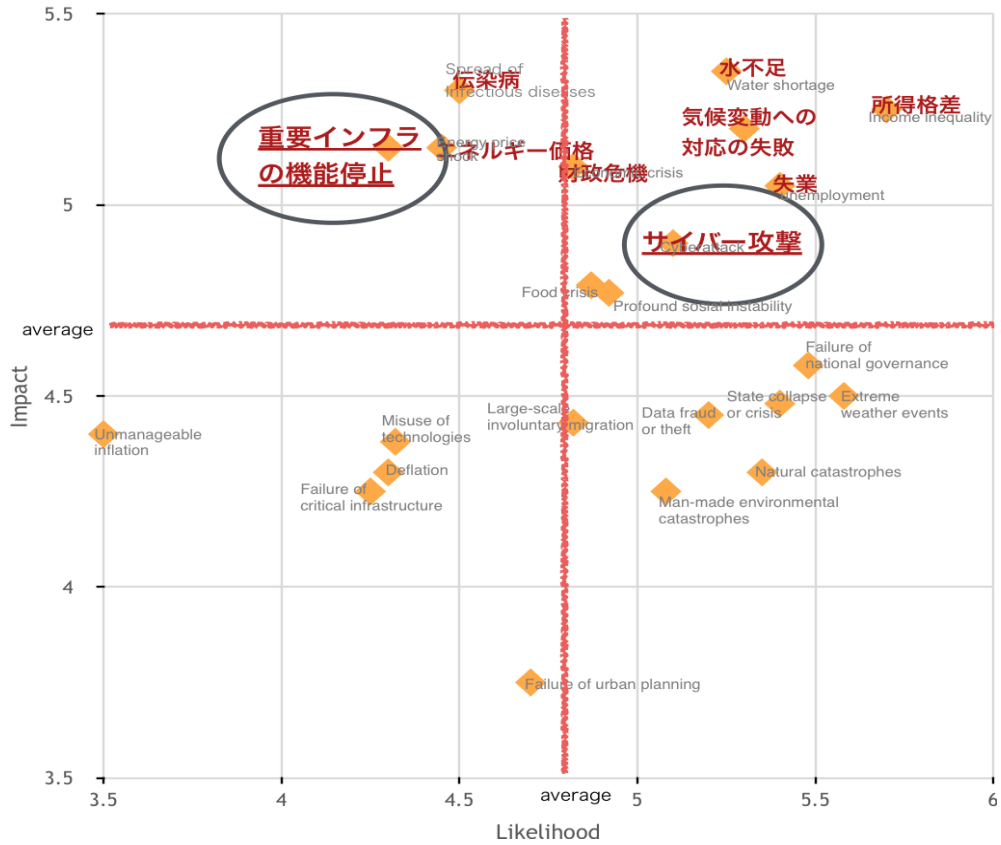
総務省（2014）　「最近の情報セキュリティに係る脅威の動向」より筆者作成

第 2 項　サイバー攻撃のリスク

図 3 は、大規模サイバー攻撃のリスクが、発生確率、発生時の影響度のいずれの側面から見ても、平均的リスクを上回ることを示している。この現状からも分かる様に、技術の進化によってあらゆる情報がサイバー空間に集まるようになった現代社会で、サイバー攻撃・犯罪のリスクは極めて高いといえる。

図 3　サイバー攻撃のリスク

[1] 2014 年 11 月 6 日に成立した「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）では、「サイバーセキュリティ」と「情報セキュリティ」の 2 語使われている部分があるが、本稿は同じ定義と見なしている。
[2] 「マルウェア」とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称



内閣セキュリテイセンター（2015）「『サイバーセキュリティ基本法』制定と日本のサイバーセキュリティ政策について 2015」より筆者作成

第 3 項　サイバー攻撃・犯罪が及ぼす被害

近年、政府機関・重要インフラ[3]へのサイバー攻撃・犯罪による個人情報漏洩は増え続けている。本項では具合例として、日本の政府機関・重要インフラ・民間企業で起こったサイバー攻撃・犯罪の事例を挙げる。

表 1　政府機関・重要インフラ・民間企業のサイバー攻撃・犯罪の事例

[3] 「重要インフラ」は、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの

発生年	名称	概要
2011	三菱重工業・衆参議員等	標的型攻撃によるウイルス感染発覚
	ソニーPSNへの不正アクセス	ソニーが運営するコンピュータゲーム用サービスが不正アクセスされ、利用者7700万人の個人情報が漏洩
2012	原子力安全基盤機構	過去数カ月間の情報流出の可能性確認
2013	農林水産省	TPP情報流出に関するサイバー攻撃事案報道
	宇宙航空研究開発機構	サーバーに対する外部からの不正アクセス発覚
	政府機関等	特定者がウェブ閲覧により感染するゼロディ攻撃
2014	原子力研究開発機構	ウイルス感染による情報の流出の可能性発覚
	ワコール	サーバーが不正アクセスを受け一部のデータが改ざんされる
2015	日本年金機構	約125万件の個人情報流出
	アビッド・ライフ・メディア	同社運営の不倫専用サイトのアシュレイ・マディソンがハッカー集団の「インパクトチーム」からの不正アクセスを受け、会員個人情報が盗取される
	東京大学	東京大学が管理する業務用パソコンがマルウェアに感染し、不正アクセスによって情報の流出被害が確認

※「ゼロディ攻撃」とは、ソフトウェアの脆弱性（セキュリティホール）を標的とした攻撃のうち、脆弱性が発見されてから、開発者によって修正プログラムなどの対策が提供されるまでの時間差を利用して行われる攻撃のこと

内閣サイバーセキュリティセンター(2015)「「サイバーセキュリティ基本法」 制定と日本のサイバーセキュリティ政策について 2015
サイバーセキュリティ戦略本部（2016)「サイバーセキュリティ 2016」『はじめに』
情報セキュリティ政策会議(2013)「サイバーセキュリティ政策に係る年次報告」
サイバーセキュリティ.com「実際の近年のサイバー攻撃による企業の被害額」より筆者作成

まず、表 1 を元に最近起こった主な政府機関・重要インフラ・民間企業のサイバー攻撃・犯罪による被害事例を紹介する。

① 2015 年 6 月、日本年金機構の年金情報管理システムサーバーから外部の不正アクセスにより年金加入者の約 125 万件の個人情報が流出した。漏洩経緯は、日本年金機構の福岡市内オフィスで職員がメールに添付されているファイルを開封した際に、パソコンがウイルスに感染した。そして、このパソコンから機構 LAN に接続され細分化された複数のフォルダから情報を抜き取られたとされている。

② 2014 年 1 月、独立行政法人日本原子力研究開発機構において、「もんじゅ」の発電課当直員が使用する事務処理用パソコン 1 台がコンピュータウイルスに感染し、パソコンに格納されている情報の一部が外部漏洩した可能性があることが判明した。

次に民間企業で起こった事例を紹介する。

① 2011 年 4 月、ソニー・コンピュータエンタテインメント(SCE)と米ソニー・ネットワークエンターテインメント(SNEI)運営の 2 つのネットワークサービスにおいて利用する米カリフォルニア州サンディエゴのデータセンターに不正アクセスが行われ、PSN と Qriocity に登録したユーザー情報が最大 7,700 万件漏洩した。

② 2014 年 3 月、大手下着メーカーのワコールのサーバーが不正アクセスを受け、一部サイトが改ざんされたことがわかった。改ざんされた状態でサイトを閲覧した場合、不正なプログラムが実行され、意図しない第三者のサイトに誘導されたり、誘導先

のサイトでウイルスに感染させられたり、不正プログラムがダウンロードされる等がおきた。

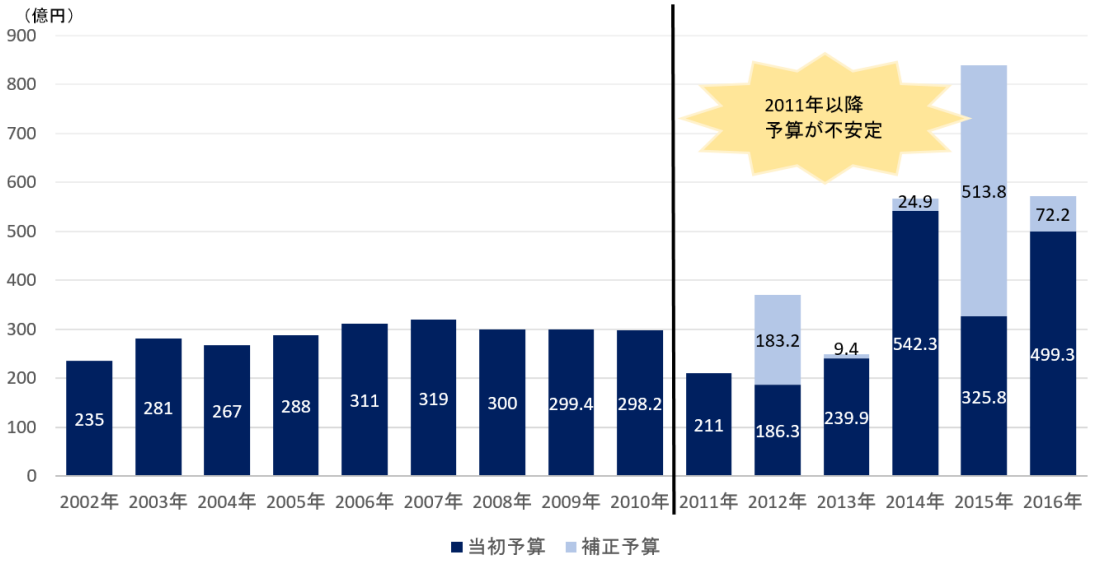
以上述べてきたように、サイバー攻撃・犯罪の被害、手法、ターゲットは多岐に渡っていることが分かる。

第 3 節　日本のサイバーセキュリティ対策の現状

第 1 項　サイバーセキュリティ対策の予算

まず、情報セキュリティ予算の推移を示す。図 5 より、2002 年から 2010 年までは、ほぼ一定の予算が配分されているが、2011 年からの 6 年間は、予算の増減が激しく、不安定であることが見て取れる。また、補正予算を除き、当初予算のみを見ても同様に変化が激しいことがいえる。特に 2015 年に関しては、当初予算の約 1.6 倍もの補正予算が投じられている。

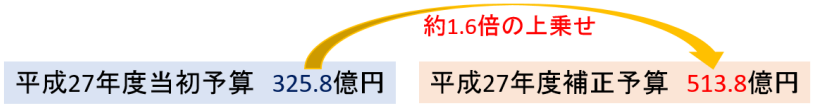
図 4　情報セキュリティ予算の推移



総務省(2016)「政府の情報セキュリティに関する予算」より筆者作成

つぎに、このような予算を使って実際にどのような対策が行われているのか。図 5 は 2015 年度の各府省庁の主な取り組み内容と予算を示したものであり、日本では多くの各府省庁にそれぞれ予算が配分され、独自に対策を行う体制をとっていることが分かる。このため、サイバーセキュリティ関連の各府省庁の事業予算の規模は必然的に小さくなっている。

図 5　平成 27 年度　情報セキュリティ予算　内訳



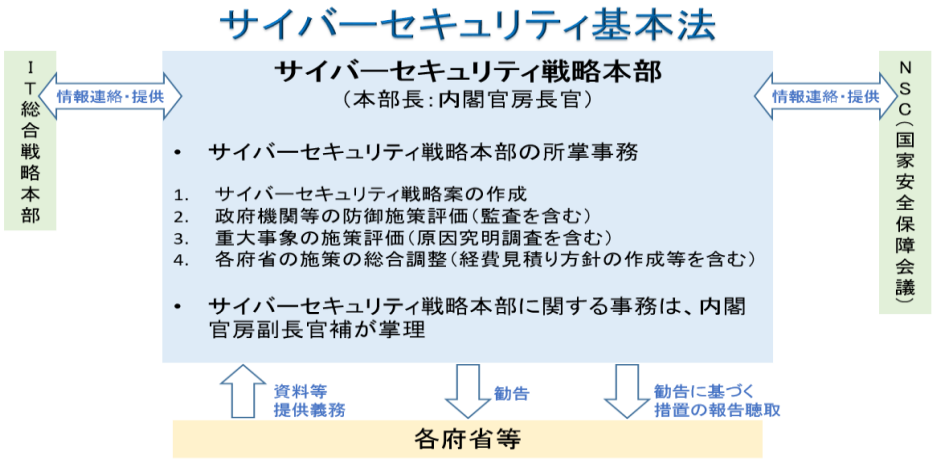
主な施策例・予算		平成27年度当初予算	平成27年度補正予算
【内閣官房】	内閣サイバーセキュリティセンター予算	16.5 億円	68.1 億円
【警察庁】	日本版NCFTAへの参画に伴う経費	1.1 億円	―
【警察庁】	サイバー犯罪等の対処能力強化のための実践的実習環境の整備等	0.6 億円	―
【総務省】	サイバー攻撃複合防御モデル・実践演習等	4.0 億円	13.0 億円
【総務省】	ICT環境の変化に応じた情報セキュリティ対応方策の推進事業	4.0 億円	―
【総務省】	自治体情報セキュリティ対策の抜本的強化	―	255.0 億円
【外務省】	情報セキュリティ対策の強化	4.3 億円	0.6 億円
【外務省】	サイバー空間における外交及び国際連携	0.1 億円	―
【経済産業省】	独法等の監視に係るシステム構築事業等	―	74.9 億円
【経済産業省】	(独法)情報処理推進機構交付金(IPA)交付金	36.1 億円	8.5 億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	17.7 億円	―
【防衛省】	サイバー防護分析装置の整備	4.8 億円	―
【防衛省】	ネットワーク監視器材の整備	29.8 億円	―
【個人情報保護委】	特定個人情報に係るセキュリティ確保のための監視・監視体制整備(マイナンバー関連)	0.6 億円	1.3 億円
【厚生労働省】	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	―	12.7 億円
【文部科学省】	大学や高専におけるセキュリティ人材の育成	1.9 億円	―

総務省(2016)「政府の情報セキュリティに関する予算」より筆者作成

第 2 項　サイバーセキュリティ対策の概要

2014 年 11 月、現状分析（第 1 章第 1 節）で示した現状を背景に「サイバーセキュリティ基本法」が制定された。同法は、サイバーセキュリティという概念を法的に位置づけ、国や地方公共団体などの関係者の責務の明確化をするとともに、サイバーセキュリティ政策に係る政府の司令塔としてサイバーセキュリティ戦略本部を位置づけ、国の行政機関に対する勧告権等の権限を付与した。（図 6 参照）

図 6　サイバーセキュリティ基本法　概要

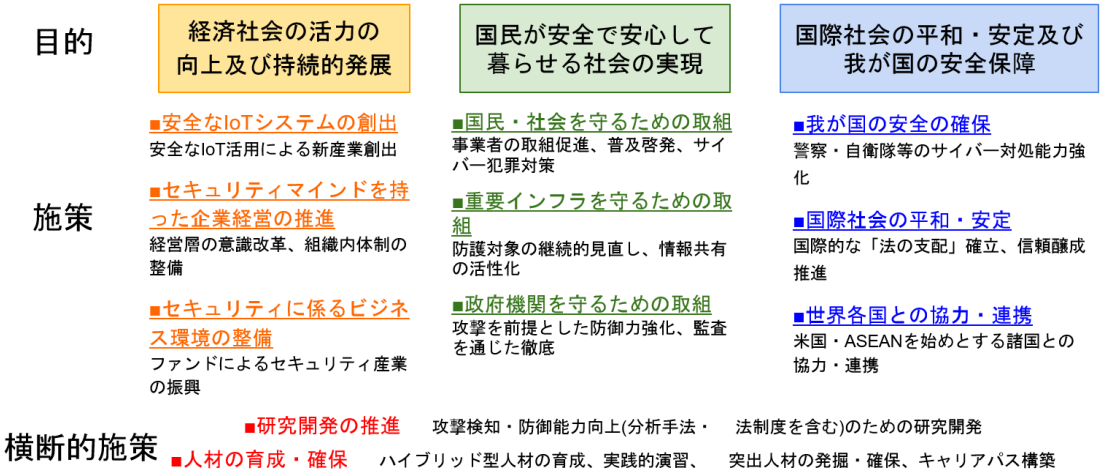


総務省(2016)「政府の情報セキュリティに関する予算」　より筆者作成

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ことを目的として、サイバーセキュリティ基本法は、2015 年 1 月に全面施行された。同法の規定に基づき、サイバーセキュリティ政策に関する新たな国家戦略である「サイバーセキュリティ戦略」が 2015 年 9 月 4 日に閣議決定された。

サイバーセキュリティ戦略は、2020 年東京オリンピックの開催や 2020 年代初頭までの将来を見据えつつ、今後 2、3 年程度の基本的な施策の方向性を示すものである。この戦略では、サイバー空間に対する日本の方針を国内外に明確化し、様々な施策を推進することがうたわれている。この戦略について簡単にまとめたものが図 7 である。

図 7　サイバーセキュリティ戦略の概要



内閣サイバーセキュリティセンター(2015)「サイバーセキュリティ戦略」より筆者作成

第 3 項　各府省庁のサイバーセキュリティ対策

ここでは、各府省庁の取り組み内容をサイバーセキュリティ戦略で推進されている次の 5 つに分類した。（図 8 参照）

① 「経済社会の活力の向上及び持続的発展」を目的とした取り組み
② 「国民が安全で安心して暮らせる社会の実現」を目的とした取り組み
③ 「国際社会の平和・安定及び我が国の安全保障」を目的とした取り組み
④ 研究開発の推進
⑤ 人材の育成・確保

図 8 について詳しく説明していく。

①の取り組みは大きく 3 つある。まず、IoT システムのセキュリティが確保された形での新規事業の振興やガイドラインの策定などの制度整備、技術開発を進める「安全な IoT システムの創出」である。これは、総務省が所管している。

つぎに、セキュリティリスクの把握や経営資源に係る投資判断を適切に行い、製品・サービスへのセキュリティ機能の実装の推進や、組織能力の向上等を図る「セキュリティマインドを持った企業経営の推進」。これに関しては、内閣官房・金融庁・経済産業省がそれぞれ施策を行っている。

最後に、サイバーセキュリティ産業が成長産業となるよう、国内外で大規模に活躍できる企業やベンチャー企業の育成等によりこれを振興していくことなどの「セキュリティに係るビジネス環境の整備」がある。これについては、総務省・経済産業省がそれぞれ施策を行っている。

②の取り組みも大きく3つある。まず、サイバー空間を構成する機器やサービスが安全かつ安定的に提供され続けるよう、事業者の取り組みの促進、普及啓発や、サイバー犯罪対策などを行う「国民・社会を守るための取組」。
つぎに、防護対象の継続的見直しや、情報共有の活性化を行う「重要インフラを守るための取組」。
最後に、攻撃を前提とした防御力の強化や、監査を通じた徹底を行う「政府機関を守るための取組」。これに関しては、すべての府省庁で行われている。

③の取り組みも大きく3つに分けられる。増大するサイバー空間の脅威に適切に対処し、日本の安全を確保するため、対処機関の能力強化、先端技術の活用や防護、政府機関・社会システムの防護に努めている「我が国の安全の確保」。これは警察庁・防衛省がそれぞれ施策を行っている。
つぎに、国際的「法の支配」の確立や相互の理解と信頼醸成を進める「国際社会の平和・安定」。これに関しては、内閣官房・外務省がそれぞれ施策を行っている。
最後に、「世界各国との協力・連携」に関しては、総務省・外務省でそれぞれ施策が行われている。

④に関しては、内閣府・警察庁・総務省・外務省・文部科学省・防衛省でそれぞれ研究開発が行われている。

⑤に関しては、すべての府省庁で職員の教育や研修など様々な人材の育成が行われている。

以上のことから、現在の日本のサイバーセキュリティ対策の体制は、同じような目的に対して各府省庁が重なり合う形で対策を行っており、非効率であることがいえる。また、各府省庁がそれぞれに予算を組んで取り組んでいることから、各対策に集中的に多くの予算を充てることが困難な状況にあるといえる。

図 8　各府省庁の取り組み　目的別

サイバーセキュリティ戦略本部（2016）「サイバーセキュリティ政策に係る年次報告（2015 年度）　より筆者作成

第 4 項　民間企業のサイバーセキュリティへの取り組み

企業が自発的に行うサイバーセキュリティに対する取り組みの促進を目的とし、2015 年 9 月に閣議決定したサイバーセキュリティ戦略を踏まえ、2015 年 12 月、経済産業省は「サイバーセキュリティ経営ガイドライン[4]」を発表した。

このガイドラインが策定された背景には、企業が保有する個人情報などへのサイバー攻撃・犯罪の増加や、それに対し企業の対応が不十分であることが挙げられる。

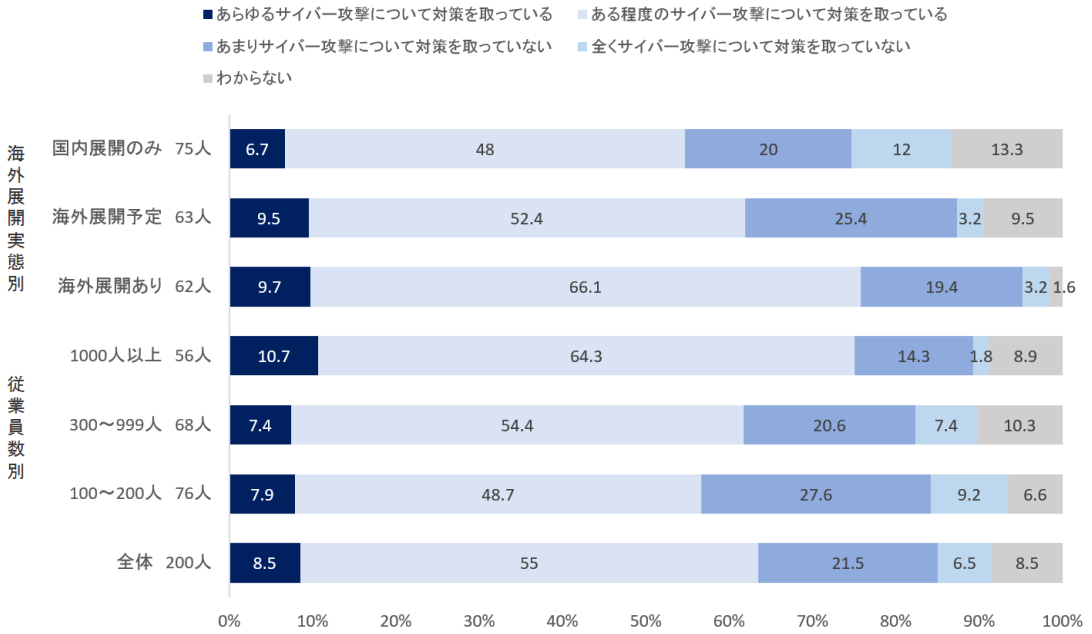
ガイドラインが発表されて 2016 年の情報セキュリティ投資額は 2015 年に続き増加傾向だが、6 割超の企業ではセキュリティ投資額に変化が見られない。

そこで企業のサイバーセキュリティ対策の状況を表したのが図 9 である。

この表からわかることは、「あまり対策を取っていないと思う」「まったく対策をとっていないと思う」「わからない」という回答の合計が全体の 3 割に近いことである。

[4] 「サイバーセキュリティ経営ガイドライン」は、大企業及び中小企業のうち、IT に関するシステムやサービス等を供給する企業、及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのものである。

図 9 企業のサイバーセキュリティ対策の状況



リスク対策.com（2015）「経営層の情報漏えいリスクに対する意識」より筆者作成

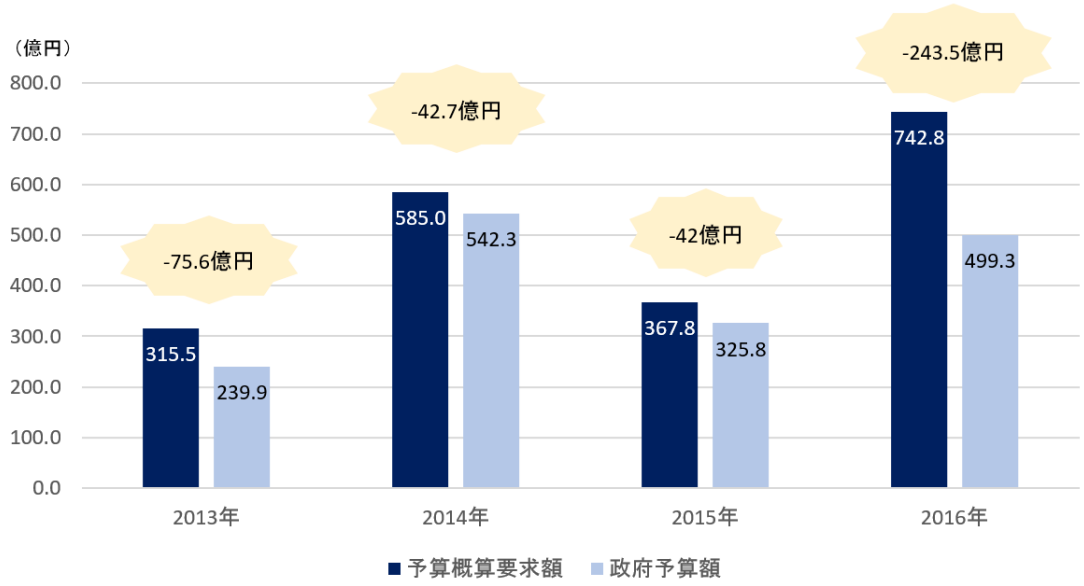
第 4 節　政府のサイバーセキュリティ対策の問題点

本節では、サイバーセキュリティの取り組みに共通する問題点を 2 点挙げ、日本のサイバーセキュリティ対策が抱える問題点を明確にする。

第 1 項　予算の不十分・不安定性

ここでは、サイバーセキュリティ対策に対する予算概算要求額と政府予算額を比較した。図 10 を見ると、ここ 4 年間、予算概算要求額よりも、実際の予算額がマイナスになっており、要求が通っていないことが分かる。このデータから、担当省庁は各府官庁が立案・実施するサイバーセキュリティ対策に多くの予算が必要であると認識し、要求しているにも関わらず、政府は十分な予算が投じられていない現状が見て取れる。

図 10　サイバーセキュリティ　予算概算要求額と実際の政府予算額の差



内閣サイバーセキュリティセンター「情報セキュリティ政策会議」　より筆者作成

さらに、現状分析で述べたように、サイバーセキュリティ対策において 2011 年から特に予算の激しい増減がみられる。一般財源であることから、ふくらむ社会保障費・国債費他等の他の分野の影響で増減していることが考えられる。

そのため、サイバー攻撃・犯罪のリスクが高まっている中、安定的かつ必要に応じて予算の割り当てるために、さらなる財源確保が必要であると考察した。

第 2 項　縦割り行政

政府は、政府全体の情報セキュリティ政策の司令塔として、2005 年より情報セキュリティ政策会議(議長:官房長官)及び内閣官房情報セキュリティセンター(NISC)を設置して情報セキュリティ政策を推進している。土屋(2010)によると、これらが内閣における総合調整の担い手となることが想定されている。しかし、韓国と日本のサイバーセキュリティ対策における取り組みを比較すると、問題点が浮き彫りになってくる。韓国では国家サイバー安全戦略会議が大きな権限を持ち、国家情報院を中心としたガバナンスが機能している。

一方、日本で同会議として当てはまるのが情報セキュリティ政策会議[5]であるが、各府省庁の大臣が構成員とする調整組織であり、サイバーセキュリティ対策の中心としてガバナンスが機能しているとはいえず、各府省庁において個別に政策が開発され実施されているのが現状である。これは、依然として各府省庁の縦割り行政が排除し切れておらず、政府全体として十分な連携・調整が図られているとは言いがたい状況であると言及している。さらに、縦割り行政の排除と責任体制の明確化の必要性も土屋(2010)は述べている。

そして、縦割り行政の弊害で、各府省庁に立案者が存在することとなり、高い専門性を有した立案者が政策を主導していると言い難いことが挙げられる。太田大州は FUJITSU

[5] 現在　サイバーセキュリティ戦略本部となっている

JOURNAL でサイバー攻撃対策について専門知識が必要であることを述べている。しかし日本の現状は、同類の分野に複数の府省庁が取り組む縦割り行政（現状分析第 3 節第 3 項図 8）であり、立案者の専門性の欠如による政策のクオリティ低下という問題を抱えているといえる。

第 5 節　問題意識

インターネットの普及は、利用人口の増加の一途をたどっている。 世界中の誰もが容易にアクセスできるサイバー空間は、その利便性から社会活動、経済活動、軍事活動等のありとあらゆる活動が依拠する場となっている。その反面、サイバー空間では、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、企業や政府の情報システムを狙うサイバー攻撃およびサイバー犯罪が起こっており、その頻度と悪質さは増し、リスクが深刻化しつつある。また、現状分析（第 1 章 第 2 節 第 1 項）でも示した様に、サイバー攻撃・犯罪の手口が高度化・多様化し、脅威の規模は拡大を続けている。さらに、現在マイナンバー導入に際しての個人情報の保護、2020 年東京オリンピックに際してサイバーセキュリティの強化は日本にとっての重要課題である。

しかし、政府のサイバーセキュリティ対策の問題点（第 1 章第 4 節）でも述べたように、現在のサイバーセキュリティ対策は予算の不足・不安定の問題、さらに各府省庁が独自に取り組みを行っていることで専門的で効果的な政策の提案・実施につながらない可能性が高いという問題があり、結果的にサイバー攻撃・犯罪の被害を食い止めることにつながっていない。

この様な現状の中、政府はサイバー攻撃・犯罪を未然防止すべく、国防として政府および民間企業のサイバーセキュリティを強化する政策を展開する必要がある。我々は、この日本にとって重要課題であるサイバーセキュリティに対して、予算が安定せず、効果的な政策が行われていない現状が問題であり、その結果被害を抑制することができていないと捉えた。

以上のことを踏まえインターネットの普及やサイバーセキュリティ予算がサイバー攻撃・犯罪の増加の原因となっているという仮説を立てた。次章以降では、それを実証するため先行研究を探し、不足していると思われる点を独自で分析をして検証する。そして政策を提言する。

第 2 章　先行研究

第 1 節　先行研究の概要

本章では、①インターネットの普及とサイバー攻撃・犯罪の関係を示した研究、②サイバーセキュリティへの投資対効果を明らかにした研究、③サイバーセキュリティを確保するための対策を示した研究の 3 つを先行研究として取り上げる。

第 2 節　インターネット普及とサイバー攻撃・犯罪の関係を示した研究

インターネット普及とサイバー攻撃・犯罪の関係を示した研究として、村野 (2015)「情報通信技術の進展とサイバーセキュリティ（科学技術に関する調査プロジェクト 2014)」 を取り上げる。この研究では、情報通信技術（所謂コンピュータ技術及びコンピュータと統合された通信技術の進展）が多くの問題を引き起こしていると論述している。その主要な問題としてサイバーセキュリティの問題をあげ、インターネットが身近に伴い、サイバー攻撃・犯罪が増加傾向にあるとした。

村野の論文では、情報通信技術の普及と攻撃の多様化によりサイバー攻撃・犯罪が発生していることに関して、その関係は示されてはいるものの、質的な研究であり、実際に数値で検証する実証分析はなされていない。

第 3 節　サイバーセキュリティへの投資対効果を明らかにした研究

サイバーセキュリティへの投資の効果を測定する計算式を示した研究として、Sonnenreich, Albanese, and Stout (2006) “Return On Security Investment (ROSI)– A Practical Quantitative Model” がある。この研究は、①サイバーセキュリティ対策を強化し、サイバー攻撃やサイバー犯罪を抑制した場合にかかる処理費用と②対策を行わず被害を受けた場合にかかる処理費用を比較している計算式(ROSI)を独自で作成し、サイバーセキュリティ対策の投資対効果を示している。しかし、この計算式は、リスクの大きさや被害を受けた後の対処にかかる費用等全て仮定された数値を用いているため、投資対効果の正確な測定は不可能であると自ら問題点を述べている。仮定された数値を用いている理由は、筆者は論文内でこれらを数値化しようと試みたが、困難であったためである。

しかし、一方で彼らは計算式（ROSI）のもととなった Return On Investment (ROI)モデルが同様の不確実性を有しながらも、広告代理店等の業界で使用され、成功しているため、この計算式（ROSI）には、一定の意義があるものとしている。

彼らの論文では、サイバーセキュリティ対策の費用対効果の有無を明らかにするモデル式が提示されている。しかし、サイバーセキュリティ対策への投資費用とサイバー攻撃・犯罪の関係性までは言及されていない。

第 4 節　サイバーセキュリティを確保するための対策を示した研究

杉野 (2016)「サイバー攻撃と情報セキュリティ」は、サイバー攻撃の実態及びインターネットの利用形態の多様化から、インターネットが及ぼす社会的脅威について解説し、情

報セキュリティを確保するための対策について述べている。そこで、サイバーセキュリティ対策の必要性を述べた上で、情報セキュリティ確保に向けた対策のあり方として 7 つの施策を挙げ、それぞれの必要性と具体的な取り組みについてまとめている。以下は、杉野が実際に提唱する施策だ。

(1) 重要情報へのアクセス源の見直し
(2) 情報セキュリティ上の被害を最小限に抑える等の取り組みの実施
(3) 脆弱性対策のための最高情報セキュリティ責任者等の設置
(4) 監視の強化、発見時の対応手順の整備、定期的訓練の実施
(5) 情報セキュリティ人材の育成
(6) 情報セキュリティ上の被害情報の共有
(7) サイバー空間利用者の情報セキュリティ意識の向上

杉野の研究では、いかにサイバーセキュリティ対策が必要であるか示され、それを踏まえ、 7 つの取り組みが明示された。しかし、上記の取り組みがサイバーセキュリティ被害を減少させることに効果的であるかについて実証分析はされていない。

第 5 節　本稿の位置付け

本稿では、以上 3 つの先行研究を踏まえ、2 つの分析を行う。

1 つ目は、インターネットの普及およびサイバーセキュリティ対策への投資によるサイバー攻撃・犯罪に及ぼす影響の重回帰分析である。この分析を行う目的は、インターネットの普及および政府によるサイバーセキュリティ対策への投資とサイバー攻撃・犯罪の関係を測定するためである。

2 つ目は、投資を行う効果的な取り組みについての実証分析である。これは、サイバーセキュリティ被害を減少させる取り組みを明らかにするためである。

先ほど先行研究で挙げた 3 つの論文の不十分な点をもう一度指摘する。

まず、村野 (2015) は、インターネットの普及が原因でサイバーセキュリティ被害は増えていることを前提としている点である。サイバーセキュリティ対策強化を唱えた研究は多数存在するものの、それを実際に分析した研究は非常に少ない。

次に、Sonnenreich, Albanese, and Stout (2006)の論文においては、投資対効果の測定やセキュリティリスクを定量化する計算式が提示されており、サイバーセキュリティへの投資が被害に及ぼす影響について実証分析した研究も少ない。

最後に、杉野 (2016)の研究は、被害を減少させる取り組みについての分析は行われていない。杉野は、サイバーセキュリティ対策が必要であると述べており、主に 7 つの取り組みが明示されている。しかし、杉野が提唱するこれらの施策はサイバーセキュリティ強化に効果的な取り組みとは言い難い。なぜなら、実証分析がされておらず、7 つの取り組みがサイバーセキュリティ被害を減少させると検証されていないためである。

そこで、我々は、以上 3 つの先行研究の課題を解消するため、①サイバーセキュリティ被害とインターネットの普及および投資の関係の検証と②サイバーセキュリティの被害を効果的に減少させる具体的な取り組みの検証の 2 つの分析を行う。これら 2 つの分析を同時に行った点が、本稿の独自性といえる。

第 3 章　分析

第 1 節　インターネットの普及およびサイバーセキュリティ対策への投資によるサイバー攻撃・犯罪に及ぼす影響の実証分析

第 1 項　検証仮説

本項で我々は、独自性として「サイバー攻撃・犯罪が増加する原因は、インターネットに接続できる端末の普及にあり、また、減少させる可能性を持つのは政府の情報セキュリティ予算総額である」という仮説を立て、検証を行う。そこで、我々は本項における検証仮説を以下のように設定した。

仮説①　インターネット端末の普及はサイバー攻撃・犯罪に対して正の影響を与える。

インターネットの発達は、我々の生活に大きな変革をもたらした。インターネットの利用目的は多岐に渡るようになり、我々の日々の生活から切り離すことができないものとなっている。そのような状況の推進力となっているのは、インターネット端末である。多様化したこれら情報通信機器の普及によりインターネット接続が容易となり、我々が使用する頻度はさらに増えた。

だが、この普及がサイバー攻撃・犯罪を発生させ、新たな被害につながったともいえる。しかし、情報通信機器にはあまたの種類があり、そのすべてがこの被害を受けているというわけではない。例えば、インターネットに接続可能な媒体として家庭用ゲーム機等も挙げられるが、我々は、一般的に使用頻度が高く、年齢問わず国民の生活に密接に関係した媒体であることを重要視し、仮説を立てるにあたり携帯電話・パソコン・スマートフォン・タブレット端末の 4 つに分析対象を限定した。

仮説②　政府による、情報セキュリティ関連予算総額はサイバー攻撃・犯罪に対して負の影響を与える。

日本政府は毎年、情報セキュリティ対策として「情報セキュリティ関連予算」を設定し多額の投資を行っているが（第1章第3節参照）、被害は依然として増加傾向にある。我々はこの現象に対し、サイバーセキュリティ対策に政府が投資することと被害の間に相関関係があるのかという点に根本的な疑問を抱き、上記の仮説を立て検証を試みた。

本稿では、入手できた下記の 3 つのデータを用い、2002 年から 2015 年の 14 年分のデータを用いたパネルデータ分析を行う。

第 1 に、サイバー攻撃・犯罪の検挙件数

第 2 に、政府情報セキュリティ予算

第 3 に、インターネット端末(携帯電話、パソコン、スマートフォン、タブレット端末)の保有率

尚、変数選択については第 3 節で述べていく。

第 2 項　分析の概要

以下ではモデル式及び変数名について記す。ただし、α、$\beta_{1\sim5}$ は推定されるパラメータとし、u を誤差項とする。分析は固定効果モデルを採択している[6]。変数の出所は表 2 に、基本統計量は表 3 にまとめている。我々は以下の変数を用いて多重回帰分析を行った。

モデル式：　$\mathbf{Y_t=\alpha+\beta_1X_{1t}+\beta_2X_{2t}+\beta_3X_{3t}+\beta_4X_{4t}+\beta_5X_{5t}+u_t}$

(t=2002~2015)　　標本数：14

変数名：

$\mathbf{Y_t}$ ：サイバー攻撃・犯罪検挙件数
$\boldsymbol{\alpha}$ ：定数項
$\mathbf{X_{1t}}$ ：携帯電話の保有率
$\mathbf{X_{2t}}$ ：パソコンの保有率
$\mathbf{X_{3t}}$ ：スマートフォンの保有率
$\mathbf{X_{4t}}$ ：タブレット端末の保有率
$\mathbf{X_{5t}}$ ：政府の情報セキュリティ予算総額
$\mathbf{u_t}$ ：誤差項

第 3 項　変数選択

<u>被説明変数</u>

・サイバー攻撃・犯罪検挙件数

被説明変数には、警察庁「サイバー空間をめぐる脅威の情勢について」からサイバー犯罪の検挙件数の推移を変数として採用した。「検挙」とは、検察官・警察職員などが認知した犯罪行為について被疑者を取り調べることであり、検挙件数とは、その数のことを指す。検挙件数を採用した理由は、サイバー攻撃・犯罪における被害件数、被害額があいまいとなっており、パネルデータで各年示すことが困難であったためである。その原因は、サイバー攻撃・犯罪ともに、被害の有無、大小にばらつきがあり、二次被害の発生など、明確な数字として示すことが難しいためだと考えられる。それに対し検挙件数は、明確にサイバー攻撃・犯罪の程度の増減が分かり、減少が対策に繋がると考えたため被説明変数として採用した。

<u>説明変数</u>

・携帯電話保有率

この変数は 2002 年から 2015 年までの 14 年間の携帯電話の保有率の推移を示す。14 年間を通し、保有率が安定的に最も高く 90%を超える高水準となっている。この保有率の高さは、携帯電話が我々の生活において必要不可欠な生活必需品となっていることを物語っている。しかしその反面、不正アクセスや、ネットワーク利用犯罪など、携帯電話のサイバー犯罪が多く存在している現状である。以上から我々は当変数が検挙件数に対して正でかつ多大な影響を与えると考える。変数値は百分率で示している。

[6] F 検定の結果、固定効果モデルが採択された。

・パソコン保有率
この変数は 2002 年から 2015 年までの 14 年間のパソコンの保有率の推移を示す。パソコンの保有率は、携帯電話に次いで、第 2 位の高水準であり、携帯電話と同様、我々の必需品となっている。しかし、本体に導入されている各種ソフトウェア（統計ソフト、文書作成ソフト等）の被害などもあることから、検挙件数に対して正の影響を与えると考える。変数値は百分率で示している。

・スマートフォン保有率
この変数は 2010 年から 2015 年までの 6 年間のスマートフォンの保有率の推移を示す。スマートフォンは、2010 年に登場した携帯電話端末であるが、元来のものと異なり、パソコン同様の機能を果たせる端末であると言える。この高機能な側面が人気を博し、保有率は急速に上昇している。しかし、マルウェア攻撃など、スマートフォン登場により生じたサイバー被害の問題などを抱えており、また検挙件数が 7000 件を越したのはスマートフォンの登場以降であり、以上のことから検挙件数に対して正の影響を与えると考える。変数値は百分率で示している。

・タブレット端末保有率
この変数は 2010 年から 2015 年までの 6 年間のタブレット端末の保有率の推移を示す。タブレット端末もスマートフォンと同様に、2010 年に登場した携帯端末だが、パソコンの機能がタブレット 1 つに盛り込まれているという魅力もあり、保有率は 2010 年の登場から 4 倍以上となっている。しかし、タブレット端末もスマートフォンと同様の被害もあり、また登場がスマートフォンの登場と同時期である点からも、検挙件数に対して正の影響を与えると考える。変数値は百分率で示している。

・政府の情報セキュリティ関連予算
この変数は 2002 年から 2015 年までの 14 年間の情報セキュリティ関連予算の推移を示す。サイバーセキュリティ対策に関する予が数ある中で、我々が当変数を選択した理由は、政府のサイバーセキュリティ対策の予算総額がサイバー攻撃・犯罪にどのような影響を与えるかを検証するためである。我々は当変数が検挙件数に対して負の影響を与えると予想した。

表 2：「変数出所」

変数名	出所
サイバー犯罪・サイバー攻撃検挙件数	警察庁 「平成27年におけるサイバー空間をめぐる脅威の情勢について」 「平成23年におけるサイバー空間をめぐる脅威の情勢について」 「平成19年におけるサイバー空間をめぐる脅威の情勢について」 「平成16年におけるサイバー空間をめぐる脅威の情勢について」
携帯電話保有率	総務省「通信利用動向調査の結果」
パソコン保有率	総務省「通信利用動向調査の結果」
スマートフォン保有率	総務省「通信利用動向調査の結果」
タブレット端末保有率	総務省「通信利用動向調査の結果」
情報セキュリティ関連予算	内閣サイバーセキュリティセンター 「政府のサイバーセキュリティに関する予算」　各年データ

(筆者作成)

表 3：「基本統計量」

変数名	平均	標準偏差	最小	最大	標本数
サイバー犯罪・サイバー攻撃検挙数	5409.1429	2379.5697	1606	8113	14
携帯電話保有率	93.6071	170.6692	87.6	96.3	14
パソコン保有率	66.5857	2.3956	0	91.2	14
スマートフォン保有率	20.5214	36.51	0	72	14
タブレット型端末	8.0357	28.7314	0	33.3	14
政府の情報セキュリティ関連予算	331.9714	11.5503	183	840	14

(筆者作成)

第 4 項　分析結果

推定結果は表 4 にまとめている。

表 4：「分析結果」

変数	係数	
携帯電話保有率	321.3959	**
パソコン保有率	31.5278	***
スマートフォン保有率	-118.9935	
タブレット端末保有率	462.3531	**
情報セキュリティ予算	-7.2549	**
切片	-25640.0967	**
R-squared(witin)	0.971723	
R-squared(between)	0.944246	
R-squared(overall)	0.904421	
有意水準	*10%有意 **5%有意　***1%有意を示す	

(筆者作成)

第 5 項　分析結果の解釈

本節では、分析結果をもとに仮説を検証する。我々が現状分析(第 1 節)で立てた仮説に対して、分析の結果は以下のようになった。

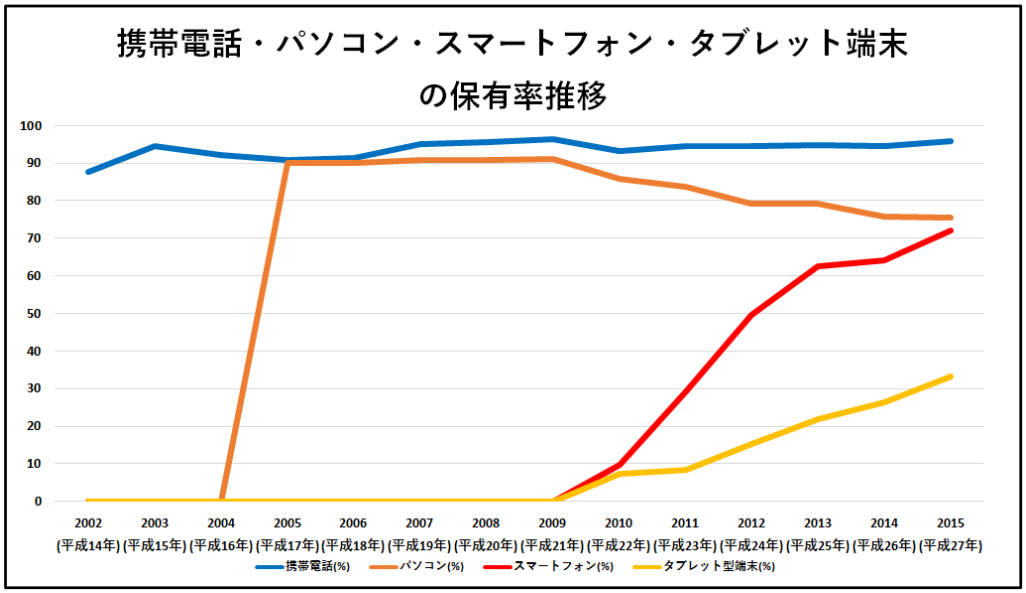
仮説①　インターネット端末の普及はサイバー攻撃・犯罪に対して正の影響を与える。

「インターネット端末の普及」における説明変数として設定した、4 つのうち「携帯電話保有率」「パソコン保有率」「タブレット端末保有率」は正に有意な結果となり仮説が支持された。この結果からインターネット端末(携帯電話・パソコン・タブレット端末)の普及はサイバー攻撃・犯罪を生じさせる一因であることが分かる。情報通信機器は我々の生活に豊かさをもたらしたが、その普及は結果的にサイバー攻撃・犯罪を生み出し続けているといえる。

しかし、一つ疑念が残る。それは説明変数の一つである「スマートフォン保有率」が、有意水準ではないという結果についてである。このような結果が生じた理由に、サンプル数の少なさが挙げられる。スマートフォンとタブレット端末は 2010 年に登場した新しい情報通信機器であり、保有率の推移は 6 年間しか追うことができなかった。（図 10 参照)

また、タブレット端末が有意水準に達しているのに対してスマートフォンが該当しない原因は、スマートフォンの保有率の伸びがタブレット端末に比べて急速であったためと解釈した。現段階では「スマートフォン保有率」はサイバー攻撃・犯罪に対して、影響を及ぼすとは言い難い。しかし、図 11 から見ても分かるようにスマートフォンの保有率は右上がりに傾いており、これからも一層保有率は伸びていくと予測されるため、今後更なる脅威となる存在であると我々は判断する。

図 11 携帯電話・パソコン・スマートフォン・タブレット端末の保有率推移



総務省(2015)「通信利用動向調査」より筆者作成

仮説② 政府による、情報セキュリティ関連予算総額はサイバー攻撃・犯罪に対して負の影響を与える。

次に情報セキュリティ関連予算総額に関する変数についての解釈を行う。説明変数として設定した、政府の情報セキュリティ関連予算総額は、負に有意な結果となり、仮説が支持された。これはやはり、政府の情報セキュリティ関連予算総額を増やすことは、サイバー攻撃・犯罪の検挙件数を減少させることを表している。

以上、検証仮設①の分析から、「情報通信機器の普及は、サイバー攻撃・犯罪の検挙件数を増加させる。」また、検証仮設②の分析から「政府の情報セキュリティ関連予算総額を増加させることはサイバー攻撃・犯罪を減らすことに有効である。」ということが証明された。

第 2 節　投資を行う効果的な取り組みの実証分析

第 1 項　分析の導入

第 1 節の分析結果より、政府の情報セキュリティ関連予算は、サイバー攻撃・犯罪の検挙件数に対して負の影響を及ぼすということを実証した。そこで、次に第 2 節で「投資を行う効果的な取り組みの実証分析」を行い、資金を集中的に投資する重点項目を分析していく。

第 2 項　分析の概要

以下ではモデル式及び変数名について述べる。ただし、α、β1~10 は推定されるパラメータ、u は誤差項である。分析では固定効果モデルを採択している[7]。変数の出所は表 5 に、基本統計量は表 6 にまとめている。

モデル式：

$$Y_{pt}=\alpha+\sum_{k=1}^{10}\beta_k X_{kpt}+u_{pt}$$

(p=1~47, t=2010~2014)　標本数：235

変数名：

Y_{pt}：情報セキュリティ被害の発生率

α ：定数項

＜セキュリティに対する認識の影響をコントロールする変数＞

X_{1pt}：情報セキュリティトラブルの重要性に対する認識

＜セキュリティに関する施策の影響をコントロールする変数＞

X_{2pt}：情報セキュリティの対策状況 対策状況　組織的対策

[7] F 検定の結果、固定効果モデルが採択された。

X_{3pt}：情報セキュリティの対策状況 対策状況　技術的対策
X_{4pt}：情報セキュリティの対策状況 対策状況　監視体制

＜セキュリティに関する人材の影響をコントロールする変数＞
X_{5pt}：情報処理要員の状況（割合）
X_{6pt}：情報セキュリティ業務の専任担当者の状況
X_{7pt}：情報セキュリティ教育の実施状況

＜セキュリティ対策予算の影響をコントロールする変数＞
X_{8pt}：情報セキュリティの対策費用の額
X_{9pt}：情報セキュリティの対策費用の情報処理関係支出総額費

＜サイバー犯罪・サイバー攻撃における時代の流れをコントロールする変数＞
X_{10pt}：時点
u_{pt}　：誤差項

第 3 項　変数選択

被説明変数
被説明変数として、経済産業省「情報処理実態調査」内の「情報セキュリティ被害の状況」を選んだ。これは、47 都道府県別で見た日本企業の情報セキュリティ被害の発生率を示したものである。当変数を選んだ理由は、日本企業の被害を受けた割合を 47 都道府県で見ることで、企業の視点から、日本の情報セキュリティ被害の発生率を詳細に知ることができると考察したからである。当変数を被説明変数として置き、我々が考えた行うべき施策を説明変数に加えていく。

説明変数
説明変数には、セキュリティに対する認識の影響をコントロールする変数、セキュリティに関する施策の影響をコントロールする変数、セキュリティに関する人材の影響をコントロールする変数、セキュリティ対策予算の影響をコントロールする変数、サイバー犯罪・サイバー攻撃における時代の流れをコントロールする変数を用いる。こちらも被説明変数同様、47 都道府県のデータを用いた。理由は上記の通り、企業の視点から日本でセキュリティ対策において重点的に取り組むべきものを詳細にみることができるからである。

＜セキュリティに対する認識の影響をコントロールする変数＞
・情報セキュリティトラブルの重要性に対する認識
セキュリティに関してどのような認識であるのかを調べたものである。表示が「非常に重要である」「どちらかと言えば重要である」「重要ではない」「分からない」と 4 つに分かれており、「分からない」を省いて、上からそれぞれ 3 点、2 点、1 点と我々が独自で点数化し、本変数とした。予想される係数の符号は負である。

＜セキュリティに関する施策の影響をコントロールする変数＞

・情報セキュリティの対策状況　組織的対策

「情報セキュリティの対策状況　組織的対策」は現在、企業が行っている組織的対策状況のことを表している。表示は「既に対策を実施している」「トラブルがあったので対策を講じた」「対策は実施していないが検討している」「対策も検討もしていない」と 4 つに分かれており、それぞれ上から 4 点、3 点、2 点、1 点と我々が独自で点数化し、その平均値を各都道府県別に並べ説明変数に加えた。予想される係数の符号は負である。

・情報セキュリティの対策状況　技術的対策

「情報セキュリティの対策状況　技術的対策」は現在、企業が行っている技術的対策状況のことを表している。表示は「既に対策を実施している」「トラブルがあったので対策を講じた」「対策は実施していないが検討している」「対策も検討もしていない」と 4 つに分かれており、それぞれ上から 4 点、3 点、2 点、1 点と我々が独自で点数化し、その平均値を各都道府県別に並べ、説明変数に加えた。予想される係数の符号は負である。

・情報セキュリティの対策状況　監視体制

「情報セキュリティの対策状況　監視体制」は現在、企業が行っている監視体制状況のことを表している。表示は「既に対策を実施している」「トラブルがあったので対策を講じた」「対策は実施していないが検討している」「対策も検討もしていない」と 4 つに分かれており、それぞれ上から 4 点、3 点、2 点、1 点と我々が独自で点数化し、その平均値を各都道府県別に並べ、説明変数に加えた。予想される係数の符号は負である。

＜セキュリティに関する人材の影響をコントロールする変数＞

・情報処理要員の状況（1 社あたり何人か）

情報処理とは、電子機器を使用して、情報を計算処理することをいう。それに長けた人材が情報処理要員である。また、現在、情報処理要員を増やそうと情報処理推進機構(IPA)が取り組んでおり、国家試験として情報処理技術者試験なども設けられている。それらの試験内容には、セキュリティ対策に関する知識も必要なため、今回変数に加えた。表示は、「社内雇用者」と「外部要員」に分けられており、それらを足して「回答企業従業者数」で割り、都道府県別に並べた。予想される係数の符号は負である。

・情報セキュリティ業務の専任担当者の状況

情報セキュリティ業務の専任担当者とはその名のとおり、社内で情報セキュリティを業務とした人材のことを指す。この要員は、セキュリティ被害が起きた際の対処などに長けており、セキュリティにおいて非常に重要な人材である。こちらも情報処理推進機構(IPA)が情報セキュリティマネジメント試験を設けている。具体的な計算方法は「情報セキュリティに関する業務の専任担当者の数」を「回答企業従業者数」で割り、それを都道府県別に並べた。予想される係数の符号は負である。

・情報セキュリティ教育の実施状況

社内で情報セキュリティ業務が実施されているか否かを表す変数である。表示は「実施している」と「実施していない」となっており、我々独自で前者を 0 点、後者を 1 点と我々独自で点数化をして後者の企業数を回答企業数で割り、その値を各都道府県別に並べ変数に加えた。予想される係数の符号は負である。

＜セキュリティ対策予算の影響をコントロールする変数＞

・情報セキュリティの対策費用の額

社内での情報セキュリティ対策費用の額を示したものである。第 3 章の分析で政府の情報セキュリティ関連予算は、サイバー攻撃・犯罪に対して負の効果をもたらすことが分かったが、企業の場合でも同じことがいえるのかどうかについて検証を試み、変数に加えた。表示は「50 万円未満」「50~100 万円」「100~150 万円」「150~200 万円」「200~400 万円」「400~600 万円」「600~800 万円」「800~1000 万円」「1000~1500 万円」「1500~2000 万円」「2000~3000 万円」「3000 万円以上」となっており、それぞれ 1 点から 12 点に我々独自で点数化し、その平均値を各都道府県別に並べ、変数に加えた。予想される係数の符号は負である。

・情報セキュリティの対策費用の情報処理関係支出総額比

これは情報処理関係の支出のうち、情報セキュリティに関連した支出の割合を示したものである。表示は「1%未満」「1~3%未満」「3~5%未満」「5~7%未満」「7~10%未満」「10%以上」となっており、それぞれ 1 点から 6 点まで我々独自で点数化し、その平均値を各都道府県別に並べ、変数に加えた。予想される係数の符号は負である。

＜サイバー攻撃・犯罪における時代の流れをコントロールする変数＞

・時点

サイバー攻撃・犯罪は時代の流れとともに刻一刻と変化している。ここでは、時点がサイバー攻撃・犯罪にどのような影響を及ぼしているかを検証するため、変数に加えた。今回パネルデータ分析を用いるにあたり、2010 年から 2014 年の 5 年間のデータを使用した。従って、この 5 年間を「時点」として各都道府県別に投入した。

表 5：変数出所

変数名	出所
被説明変数 （情報セキュリティトラブルの発生状況）	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 （情報セキュリティトラブルの重要性に対する認識）	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 組織的対策の実施	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 技術的対策の実施	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 監視体制	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報処理要員の状況)	経済産業省「情報処理実態調査」 （詳細1：情報処理要員等の概要） 各2010～2014年データ
説明変数 （情報セキュリティ業務の専任担当者の状況）	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティ教育の実施状況)	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティの対策費用の大きさ)	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
説明変数 (情報セキュリティの対策費用の情報処理関係支出総額比)	経済産業省「情報処理実態調査」 （詳細3：情報セキュリティ等の概要） 各2010～2014年データ
時点	特になし

表 6：基本統計量

変数名	平均	標準偏差	最小	最大	標本数
被説明変数 （情報セキュリティトラブルの発生状況）	20.8485	7.7908	0	42.1052	235
説明変数 （情報セキュリティトラブルの重要性に対する認識）	2.7253	0.0736	2.4593	2.9347	235
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 組織的対策の実施	3.2101	2.3956	2.0967	3.9596	235
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 技術的対策の実施	3.5045	0.2211	2.8666	4	235
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 監視体制	2.6898	0.3033	1.7058	3.6363	235
説明変数 (情報処理要員の状況)	3.0459	2.0345	0.4651	12.2509	235
説明変数 （情報セキュリティ業務の専任担当者の状況）	0.1124	0.0982	0.0052	1.0229	235
説明変数 (情報セキュリティ教育の実施状況)	70.178	25.495	21.4285	100	235
説明変数 (情報セキュリティの対策費用の大きさ)	310.768	159.4018	62.5	862.8697	235
説明変数 (情報セキュリティの対策費用の情報処理関係支出総額比)	3.59191	0.4449	2.4285	5.2857	235
時点	2012	1.4172	2010	2014	235

(筆者作成)

第 4 項　分析結果

推定結果は表 7 にまとめている。

表 7：分析結果

変数名	係数	
説明変数 （情報セキュリティトラブルの重要性に対する認識）	-4.876862	**
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 組織的対策の実施	-0.290339	*
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 技術的対策の実施	-5.840938	*
説明変数 (情報セキュリティの対策状況～対策の実施状況～) 監視体制	-2.301320	
説明変数 (情報処理要員の状況)割合	-1.178037	
説明変数 （情報セキュリティ業務の専任担当者の状況）	-4.272865	**
説明変数 (情報セキュリティ教育の実施状況)	-0.088101	***
説明変数 (情報セキュリティの対策費用の大きさ)	-0.001944	**
説明変数 (情報セキュリティの対策費用の情報処理関係支出総額比）	2.073230	
時点	0.359342	
切片	-721.216598	
Prob > F	0.000000	
R-squared(witin)	0.453282	
R-squared(between)	0.205465	
R-squared(overall)	0.147150	
有意水準	*10%有意 **5%有意　***1%有意 を示す	

筆者作成

第 5 項　分析結果の解釈

本項では、説明変数の分析結果に基づき「セキュリティに対する認識の影響をコントロールする変数」「セキュリティに関する施策の影響をコントロールする変数」「セキュリティに関する人材の影響をコントロールする変数」「セキュリティ対策予算の影響をコントロールする変数」「サイバー攻撃・犯罪における時代の流れをコントロールする変数」について、それぞれ以下のとおり解釈を行う。

第 1 に、セキュリティに対する認識の影響をコントロールする変数についてである。この変数は「情報セキュリティトラブルの重要性に対する認識」であったが、負に有意な結果となった。この結果から、セキュリティに対して重要性が高まるほど被害の発生率を下げる効果があることが分かる。そして、セキュリティ被害の重要性を認識する企業ほど、被害を防ぐための対策を積極的に行っていると推測ができる。

第 2 に、セキュリティに関する施策の影響をコントロールする変数についてである。「組織的対策の実施」と「技術的対策の実施」は負に有意な結果が得られた。この結果から、個人ではなく組織でセキュリティ対策に取り組む必要があることがいえる。それに加え、セキュリティ対策として技術の導入が重要であることも分かった。しかし、「監視体制の実施」は統計的に有意な結果は得られなかったため、監視体制は組織的対策・技術的対策に比べるとさほど重要とは言えない。

第 3 に、セキュリティに関する人材の影響をコントロールする変数についてである。「情報セキュリティ業務の専任担当者の状況」と「情報セキュリティ教育の実施状況」の 2 つが負に有意な結果が得られた。この結果から、社内におけるセキュリティ業務の充実化・セキュリティに関する教育・人材育成は、サイバー攻撃・犯罪を防ぐために有効であることが分かった。しかし、「情報処理要員の状況」は統計的に有意な結果を得ることができなかった。その理由は、情報処理要員は電子機器を使用し情報を計算処理する要員のことで、情報セキュリティ業務に対して直接的な関係がないためであると考えられる。このことから、サイバー攻撃・犯罪の対策はセキュリティ対策強化に関する専門性を持った人材が必要であり、そのような人材を育成していくことが必要不可欠であるといえる。

第 4 に、セキュリティ対策予算の影響をコントロールする変数についてである。ここでは、「情報セキュリティ対策費用の大きさ」において負に有意な結果が得られた。第 3 章の第 1 節で行った分析と同様に、47 都道府県別の企業を見てもこのような結果が得られた。これはすなわち、対策費用の大きさは重要な対策の 1 つであることを示している。しかし、「情報セキュリティの対策費用の情報処理関係支出総額比」は統計的に有意な結果が得られなかった。この結果から、セキュリティ対策において予算の総額自体が重要であり、割合は重要ではないということが分かった。

第 5 に、サイバー攻撃・犯罪における時代の流れをコントロールする変数についてである。「時点」を変数に加えたが、統計的に有意な結果を得ることはできなかった。この理由は、サイバー攻撃・犯罪は刻一刻と変化しており、規模や性質等が変化しているためと考えられる。

本節の実証分析では、分析に使用する変数として経済産業省「情報処理実態調査」を用いて 2010 年～2014 年の 5 年間のパネルデータを用いた多重回帰分析を行った。各企業のセ

キュリティに関する状況が 47 都道府県別に表されているデータを用いることで、「企業」の視点から日本の情報セキュリティについて詳細に知ることができる。しかし、本来ならば、「企業」の視点からのデータだけではなく、国家規模のサイバーセキュリティのデータも用いるべきであると考えるが、数値化が難しく、被害状況や対策状況が明確でないためデータ入手が困難であった。そのため、本稿では「企業」の視点から分析し、政府がサイバー攻撃・犯罪から企業または国を守るべき対策を挙げた。

以上の分析から、セキュリティに関する認識、組織的・技術的施策、人材、対策予算の大きさはセキュリティ被害に対して有効であるということが明らかとなった。

この分析結果に基づいて、次章では、政策提言を行う。

第４章　政策提言

現状分析(第 1 章)と先行研究(第 2 章)では、サイバー攻撃・犯罪のリスクの高まりとこれらの未然防止に投資する必要性を述べた。このサイバー空間において高まるリスクに対して、集中的かつ継続的に投資するための安定的な財源確保の手段として、新税である「サイバーセキュリティ対策税」を特定財源として徴収することを提言する。

本税は、分析(第 3 章)の分析結果で、サイバー攻撃・犯罪の 1 つの原因として挙げられたインターネット端末に 1%～3%の税率で課税をする。徴税方法は、端末価格に税率を課し、販売事業者が納税する。

次節から、サイバーセキュリティ対策税の意義、正当性、概要について述べていく。

第 1 節　サイバーセキュリティ対策税の意義

我々は、増税・予算整備という方法ではなく、新しく税を導入し、特定財源として財源を確保することを提言する。本節では、この意義について論述していく。

第 1 項　新税導入の意義

現状分析(第 1 章)から分かるように、手口の多様化・高度化によりサイバー攻撃・犯罪の脅威は高まっており、その被害は民間レベルから国レベルまで甚大なものとなっている。

このリスクに対するサイバーセキュリティ対策の強化において、集中的・継続的な投資を行うことは、重要でありかつ急務であるといえる。

しかし、現状分析(第 1 章)より、対策における予算は不十分であり、現在日本のサイバーセキュリティ対策への配当予算には増減の激しさが見られる。集中的かつ継続的で十分な投資が行われていないのである。

そこで、国家の経済活動、政治活動を大きく左右させるサイバーセキュリティ対策に集中的かつ継続的に投資をするため、新しく税を導入し財源を確保することは望ましいといえる。

第 2 項　特定財源である意義

我々は、特定財源として税を徴収することを提案しているが、現在では特定財源に対して否定的な意見が多い。以下にサイバーセキュリティ対策税を特定財源として徴収する理由を 2 つ挙げる。

1 つ目は、一般財源は継続的に一定の財源を 1 つの分野に投資することは困難であるのに対し、特定財源は継続的かつ集中的に 1 つの分野に投資を行うことが可能であるからだ。サイバーセキュリティ対策には継続的投資が必要不可欠であるため、経済活動に左右されず、継続的に資金を投資するために特定財源として徴収することが最適である。

2 つ目は、特定財源は、一般財源と比較して経理を明らかにすることが可能であるからだ。現状分析(第 1 章第 2 節第 2 項)で述べたように、サイバー攻撃・犯罪のリスクは高く、今後さらに高度化することが予測される。この緊急性の高い問題に対して、経理を明確化させることは重要であるといえる。

第 2 節　サイバーセキュリティ対策税の正当性

第 1 項　類似した目的税

本項では、サイバーセキュリティ対策税同様、問題の原因に課税し、そこで得た税収を問題解決の費用に充てている既存の目的税を挙げる。ここから、サイバーセキュリティ対策税の正当性を示す。

1 つ目は、石油・石炭税である。これは、石油一般の利用に共通する便益性に着目し、原油・石油製品・ガス状炭化水素・石炭を課税対象としている。各燃料の CO2 排出量に応じた税率を上乗せする、地球温暖化対策のための税である。財源の使い道は、エネルギー対策特別会計のもとで、エネルギー起源 CO2 の排出抑制対策に真に有効な対策に充てられるとされている。地球温暖化問題を引き起こす主要原因である CO2 排出源（石油・石炭）に課税をすることは、サイバー攻撃・犯罪の主要原因であるインターネット端末に課税することと、類似した考えを持っているといえる。

2 つ目は、地球温暖化対策税である。これは、課税対象を全化石燃料(原油・石油製品・ガス状炭化水素・石炭等)とし、それぞれ CO2 排出量に応じて税率を上乗せするものである。CO2 を排出してエネルギーを利用する消費者や事業者に広く薄く、CO2 排出量に応じ、公平に負担をかける税である。税収は、エネルギー起源の CO2 削減に有効な多種多様な対策費に充てられている。

こちらも、石油・石炭税同様、サイバーセキュリティ対策税と類似した考えのもと存在している。

これら 2 つの税のように、ある問題の原因に対し課税をし、使途が特定されている税が既に存在していることから、我々が提案するサイバーセキュリティ対策税は一定の正当性を有しているといえる。石油・石炭税においては、財源はエネルギー対策特別会計に組み込まれている。以上の例から、サイバーセキュリティ対策のためにサイバー攻撃・犯罪の原因の 1 つであるインターネット端末に課税をし、その財源を特別会計に組み込むサイバーセキュリティ対策税は、実現可能であることがいえる。

第 2 項　税の三原則

税導入にあたり、本項では税の三原則を検討する。

1 つ目に、公平の原則[8]だ。本税は、サイバー攻撃・犯罪が行われるサイバー空間に接続可能な端末に課税するものである。この点において、対象端末価格を課税対象とし、サイバー空間を利用するすべての人々に同等の税率を課していることから、公平性は有しているといえる。

2 つ目に、中立の原則[9]だ。この点に関しては、過去にも消費税増税やインターネット端末の高額化があったにも関わらず現状分析で示した様にすべてのインターネット端末においてその保有率は増加傾向にあることから、個人や企業の経済活動における選択に大きな影響を与えないことが予見される。さらに 1%～3%という比較的低い税率で設定されていることも大きな影響を及ぼさないと予測される要因の一つといえる。

[8]「公平の原則」とは、人々がそれぞれの負担能力に応じて税金を分け合うことを指し、経済力が同等の人には同等の負担を求める「水平的公平」と、経済力のある人にはより大きな負担を求める「垂直的公平」がある。

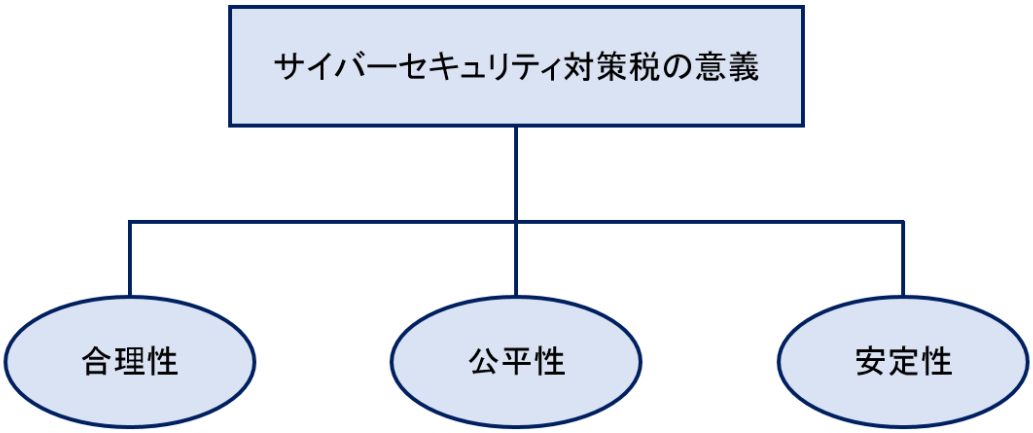
[9]「中立の原則」とは、税制が個人や企業の経済活動における選択を歪めないものであること。

3 つ目に、簡素の原則[10]だ。これは、課税方法としてインターネット端末購入に際し税を支払うことや納税者がインターネット端末販売事業者である点が、考えられ得る手法の中で最も簡素であり、望ましい形であるといえる。

第 3 項　特定財源化の利点

特定財源化の利点として受益者負担の原則から以下の 3 点を挙げる。
以下の 3 点は、特定財源として徴収されていた、道路特定財源の意義に本税をあてはめたものである。

図 12 サイバーセキュリティ対策税の特定財源化の利点



筆者作成

1 つ目は、公平性である。サイバーセキュリティ対策税は、インターネット端末に課税することで、インターネット利用者からのみ徴収している。そのため、公平性を有しているといえる。
2 つ目は、安定性である。サイバーセキュリティ対策税は、特定財源化されるため、景気や財政政策の動向に左右されずに安定した財源を確保できる。
3 つ目は、合理性である。サイバーセキュリティ対策税は、利用者の負担がすべてサイバーセキュリティ強化に充当されるため、納税者の理解を得られやすいことがあげられる。

第 4 項　特別会計の設置要件

特別会計を設置するにあたり、財政法第 13 条第 2 項では以下の要件が求められている。
1 つ目は、国が特定の事業を行う場合であること。
2 つ目は、特定の資金を保有してその運用を行う場合であること。
3 つ目は、その他特定の歳入をもって特定の歳出に充て、一般の歳入歳出と区分して経理する必要がある場合であること。

[10] 「簡素の原則」とは課税対象及び、徴税方法が国民一般から認識しやすいものであること。

サイバーセキュリティ対策税は上記の 3 要件すべてに当てはまり、特定財源として徴収することは法律上も可能であるといえる。

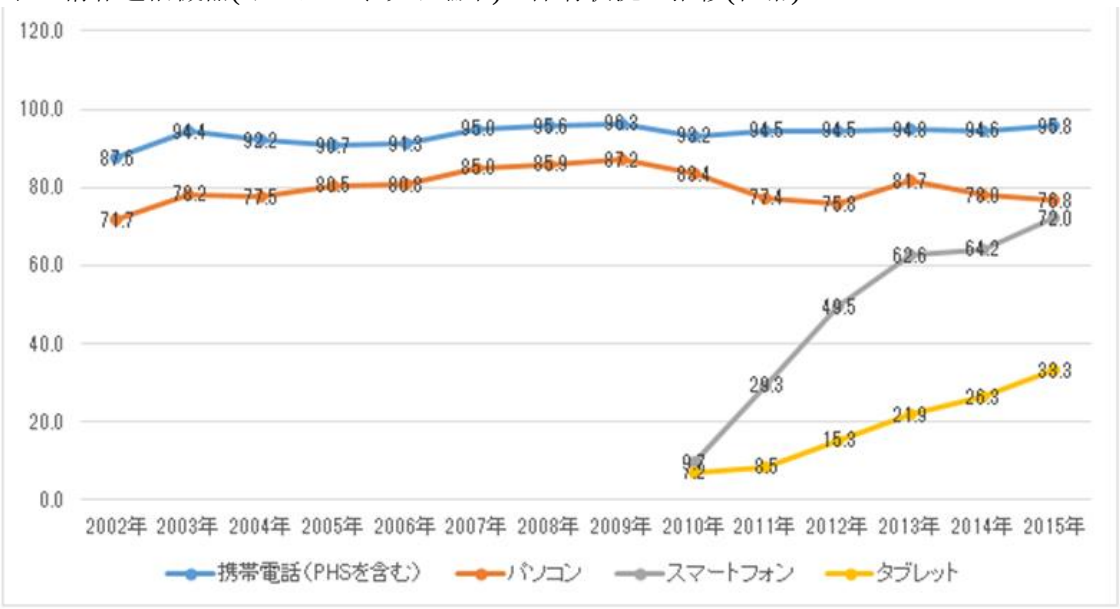
第 3 節　サイバーセキュリティ対策税の概要

本節では、サイバーセキュリティ対策税の詳しい概要について言及する。

第 1 項　課税対象

課税対象はインターネット端末とし、具体的には携帯電話・パソコン・スマートフォン・タブレット端末に対し課税を行う。分析(第 3 章第 1 節)の結果から、サイバー攻撃・犯罪が増加した原因の 1 つとして、インターネット端末の普及があげられた。ここからインターネット端末の普及の増加がサイバー攻撃・犯罪の増加に影響を与えている可能性が高いことがいえるため、これに対し課税することに意義があるといえる。また、インターネット端末に課税する上で注目すべきは、その保有率の高さだ。

図 13 情報通信機器(インターネット端末)の保有状況の推移(世帯)



平成 27 年通信利用動向調査 より筆者作成

図 13 の様に、2015 年携帯電話保有率は 95.8%。パソコン保有率は 76.8%。近年急激な増加をみせるスマートフォンは保有率 72.0%。緩やかな上昇を続けるタブレット端末は保有率 38.3%である。

上記のようにこれらインターネット端末は、国民の多くが保有していることから広く薄く課税をすることが可能であり、今後の保有率の更なる上昇も期待されることから安定した税収が見込める点が課税対象とする大きな利点である。

さらに、過去に行われたインターネット端末に課税する新税導入の構想を先行事例として紹介する。2013 年にフランス政府が提唱した「スマートフォン・タブレット税」である。これは、スマートフォンやタブレット端末を課税対象とし、1～3%の税率を定めた。また、

徴税方法として、スマートフォン・タブレット端末を販売する企業から徴収し、1%の税率の場合税収規模は年間 8,600 万ユーロ（約 112 億円）と見込んでいる。上記の点からも分かる様に、我々のサイバーセキュリティ対策税と酷似している。一方、相違点として財源が優秀な映画や音楽活動の支援に充てられることが検討されていた点が挙げられる。

第 2 項　徴税方法

徴税方法は、端末購入時にその端末価格に規定された税率をかけ徴税するものとする。この点において、我々はプロバイダ料金、通信量、契約料金などに課税することも検討したが、以下の様な問題が生じた。

第 1 に、プロバイダ料金・通信量・契約料金すべてにいえることだが、これらから徴税する場合、それぞれとの契約内容を国が管理しなければならない状況に陥る問題である。さらに、この様な膨大な作業は実現不可能であり、煩雑であることは言うまでもない。先ほど述べた、税の三原則である「簡素の原則」を考慮にいれ、端末価格に課税をすることが最も理想的あるとした。

第 2 に、各種携帯会社の契約料金から徴税する場合、現在の多様化した料金プラン上、キャリアによって差が出てしまう可能性が高く、税の三原則である「公平性の原則」の観点から見ても不向きである。したがって、消費税同様、購入した端末の価格から徴税するという方法をとった。

さらに、これらの税はインターネット端末の販売事業者から徴収する。その理由は、サイバーセキュリティ対策税の課税対象は端末の販売価格であるからである。

第 3 項　税率

税率は 1～3%とする。この税率を決める上で、我々が参考にしたものは以下の 3 点である。

まず、消費税との関係性だ。後に検討するが、サイバーセキュリティ対策税は二重課税の問題を抱えている。したがって、まず 8%以下の税率でなければならないという上限を取り入れた。

つぎに、徴税方法が似ている税として消費税導入の経緯を調査した。第 35 回衆議院議員総選挙において大平正芳首相が一般消費税を、税率 5%として導入を検討したが、各方面から反論が上がり実現には至らなかった。しかし、後の竹下内閣時に、税率を 3%に引き下げ、導入を検討したところ実現に至った。もちろん、実現に漕ぎ着けた要因として税率の引き下げは一要因であるという解釈もあるが、税率を低く設定し、国民の痛税感を軽減したことは、消費税が広く受け入れられるものとなった一因であることは明白である。したがって、8%以下かつ低めの税率(3%未満)とし、税率の幅を検討した。この税率で税を徴収する場合、年間約 1590～4770 億円の税収が見込まれる。

15.9 兆円（現在のインターネット端末の売上額）×1～3%（税率）＝1590～4770 億円

第 4 節　税導入に際して想定される課題

本節では、サイバーセキュリティ対策税を導入する際に、考えられる課題について述べていく。

第 1 項　二重課税

現在、二重課税が行われている例で、ガソリン価格を挙げる。ガソリン価格は、 ガソリン税[11]、石油税、消費税が課された状態である。原則として、二重課税は避けるのが適当であるが、上記の他にも避けることができていない事例は多数存在している。したがって、我々は消費税とサイバーセキュリティ対策税の二重課税は、原則としては望ましいとは言えない可能性があるが、特出すべき問題ではないとした。

第 2 項　端末 0 円携帯に対する課税

2015 年末総務省より、「0 円携帯廃止」命令が発表された。総務省は「事業者は、スマートフォンを購入する利用者には、端末を購入しない利用者との間で著しい不公平を生じないよう、端末の調達費用に応じ、合理的な額の負担を求めることが適当である。」とし、契約種別 や端末機種によって著しく異なる端末購入補助の是正等により、利用者の負担が合理的な額となるよう端末購入補助を縮小するようにもとめている。

2016 年 10 月にはスマートフォンの「実質ゼロ円」での販売を規制したガイドラインに違反したとして、NTT ドコモ、KDDI（au）、ソフトバンクの携帯電話大手 3 社が総務省により行政指導を受けた。これに対し、大手 3 社はそれぞれ「真摯に対応する」としている。

この総務省の方針とキャリアに対する厳重注意、注意後のキャリアの対応を考慮に入れて、我々は今後「端末料金 0 円携帯」は今後減少傾向にあり、特出すべき問題でないと考えた。

第 3 項　海外で現地購入した場合や海外より輸入した場合

本項では、海外で現地購入した場合や海外より輸入した場合、生じるフリーライダー問題(課税対象者漏れ)について説明する。前提として、我々が提言するサイバーセキュリティ対策税は、日本国内でのみ適応される税であるため、海外の事業者へ適応されることは困難である。

しかし、海外とのインターネットを通した売買が一般化した現状を十分に考慮した上でも、すべての国民が同様の行動をとることは考えにくい。それに加え、この様な人々はわずかであり、税収には大きく影響しないと想定されるため、彼らを対象に法や制度をより複雑化することは非現実的であるとした。

第 4 項　IoT の普及が進む中での課税対象

IoT とは、“モノ、ヒト、サービスの全てを包括したインターネット化による価値創造”である。IT に特化したコンサルティング企業であるアイ・ティ・アールは 2016 年 10 月 19 日、国内企業を対象とした「国内 IT 投資動向調査 2017」の調査結果概要を発表した。この調査により、IoT・AI といった新テクノロジーへの投資意欲が明確に伸びていること、セキュリティ対策予算が過去最高を更新していることがいえると明言した。一般企業でも、上記の様な動向がうかがえる中で、今後、政府や一般市民の生活も例外なく IoT 化が促進され我々の課税対象であるインターネット端末が増加されることが予測される。この動きに対し、我々は、課税対象を拡大し課税漏れを防ぐことを検討している。

[11] 正式には「揮発油税及び地方揮発油税」をいう。

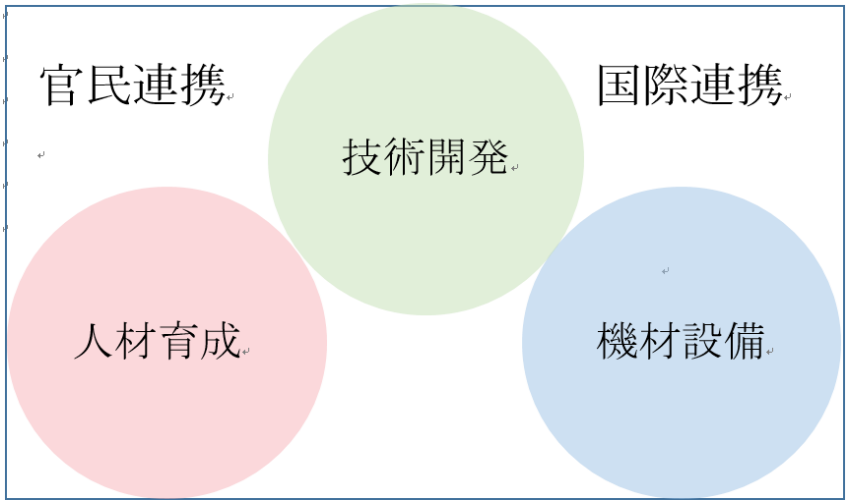
第 5 節　税収の使い道

第 1 項　税収の使い道の概要

我々は、サイバー攻撃・犯罪対策に有効な以下の 5 つの施策に重点的に充てるとする。

①対処能力の向上：捜査・分析用資機材の整備等を実施
②人材育成・教養・訓練の充実・強化
③新技術に関する研究の推進
④官民連携の推進
⑤国際連携

図 14　主な 5 つの取り組み



(筆者作成)

使い道の①②③については、分析(第 3 章第 1 節)から、税収を充てることがサイバーセキュリティ対策強化において効果的だということが分かった。これは、図 14 の中心部分にあたる。その一方で、使い道④⑤にあたる官民連携と国際連携については、分析で示すことが困難であった。その理由は、官民連携の推進や国際連携を数値化したデータは存在せず、分析不可能であるからである。しかし、この 2 つは図 14 で示されるように、国際連携と官民連携は①②③全ての取り組みを行う上で必要なため、国家安全保障戦略等関連資料を用い、官民連携の推進や国際連携の必要性を述べる。

＜官民連携の必要性＞

国家安全保障戦略 (2013)で、政府はサイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を唱え、被害発生の把握、被害の拡大防止、原因の分析究明等の観点から官民連携は重要であるとしている。それに加え、警察庁（2012)は報告書の中で、1 つの組織だけでサイバー攻撃・犯罪を未然防止することは不可能であり、関係省庁、民間事業者等による官民を挙げた連携・協力が重要であると明言した。

＜国際連携＞

サイバー防衛報告書で、技術責任者である、Purser 氏は、「サイバーセキュリティは、国境内だけでは意味をなさず、グローバルに接続している。そのため、国際的な協力関係

を構築できなければ、一国でのアプローチも効果はない。」と述べ、サイバーセキュリティにおいて国際協力の必要性を訴えている。
また、Dorgrul, Aslan, and Celik (2011)は論文の中で、現在、サイバー攻撃・犯罪において世界規模での対策は取り組まれていないが、世界規模での解決が必要だとし、具体的に国際法を整備やサイバー攻撃・犯罪に対し国際連携の整備を提案している。

我々はサイバーセキュリティ対策税導入により得られた税収を上記の 5 項目に重点的に投資していく。

第 2 項　所管

我々は、この政策の所管として以下のつ 3 つを検討した。

内閣府・内閣サイバーセキュリティセンター

長所は、内閣府は特定の事項について恒常的・専門的総合調整を行う機能を有するため、現在様々な府省庁が関わる横断的な問題であるサイバーセキュリティ対策を担う所管として望ましいといえることだ。
短所は、内閣府は調整官庁であるため、財務省の様に巨額の予算配分は難しい点が挙げられる。

総務省

長所は、現在サイバーセキュリティ関連の主な政策は総務省が所管しているためこれまでの経緯を考慮に入れると、最も自然であるといえることだ。
短所は、1 つの省庁が所管するため多様な側面から政策を立案・実施し、横断的な対策が困難であることだ。

経済産業省

長所は、現在の民間企業向けのサイバーセキュリティ対策を担う官庁であるため、その分野において最も専門的に政策立案・実施を行うことができるからだ。我々は民間企業向けのサイバーセキュリティ対策を政府のサイバーセキュリティ強化と同様に政策提言の中枢として捉えているため、民間企業向けのサイバーセキュリティ対策を実際に行う高い専門性と経験は高い評価に値する。
しかし一方で、総務省同様、1 つの省庁が所管するため多様な側面から政策を立案・実施し、横断的な対策が困難であることが短所として挙げられる。

以上、所管について考え得るものを検討してきたが、それぞれに解消しえない問題を抱えていることが分かる。そこで我々は、以下の 3 条件がすべてあてはまる所管として「サイバーセキュリティ庁」新設を最も望ましい所管とした。
①巨額な予算を適切に配分する機能を有する
②複数の官庁をまたがる横断的な対策を調整し、効率的な対策を実施する機能を有する
③サイバーセキュリティ対策に対し高水準の専門性をもち、実現可能の高い政策を立案・実施する機能を有する
3 条件がどの様にあてはまるかは、以下の通りだ。
①財務省やその他事業官庁が巨額な予算を配分する機能をサイバーセキュリティ庁に与える
②既存の省庁に属さないため、横断的な対策に対して俯瞰的な視野で政策を調整することが可能である

③サイバーセキュリティに関して極めて高い専門性をもつ人々が 1 つの組織に所属することは、より効果的な政策立案・実施を可能にする。また、予算配分においても、スペシャリストが担当することで、適切な配分に繋がる。

現在、緊急性・重要性が高いものに対してスポーツ庁、復興庁といった新庁が続々と組織されている。大掛かりな組織改革が考えられるが、2020 年の東京オリンピックを目前に控え、サイバーセキュリティ対策の緊急性・重要性が広く認識され得る今、サイバーセキュリティ庁新設は可能であるとした。

第 6 節　政策実現後のビジョン

第 1 項　政策提言の効果

我々が提案する政策の実現によって、問題意識(第 1 章第 4 節)で示した問題の解決につながる。

まず、現状分析(第 1 章第 1 項)で述べた「予算の不足・不安定」の問題は、サイバーセキュリティ対策税により解決する。新しく税を導入し、サイバーセキュリティ対策のための財源を確保することで、対策に見合った予算を充てることが可能である。さらに、課税対象であるインターネット端末の保有率の推移から、安定的な徴税が可能であることがいえる。それに加え、サイバーセキュリティ対策税は、使途が特定される特別財源として徴収することから、社会情勢・経済活動・政治活動の影響を受けることなく、継続的・安定的にサイバーセキュリティ対策に投資可能であるため、予算が不安定という問題も同時に解決する。

つぎに、現状分析(第 1 章第 2 項)で述べた「縦割り行政」の問題は、サイバーセキュリティ庁新設により解消されるだろう。その理由は、サイバーセキュリティ庁は、様々な省庁が取り組んでいるサイバーセキュリティに関する施策を、一括して実施することが可能であるからだ。また、副次的な効果としてサイバーセキュリティに関する豊富な知識を持つ人物が集められ、一括して政策を立案・実施を担うことでより効果的な政策に予算を投じることが可能であることもいえる。

第 2 項　政策提言の副次的効果

サイバーセキュリティ対策税が導入され、日本のサイバーセキュリティが強化されることによる副次的な効果は、主に以下の 3 つの点が考えられる。

1 つ目に、サイバーセキュリティ対策強化によるマイナンバーの普及である。2015 年、社会保障･税制度の効率性･透明性を高め、国民にとって利便性の高い公平･公正な社会を実現するための基盤であるマイナンバーが導入された。しかし、現在、普及率は 5%にとどまっている。普及率の低さの理由は、マイナンバー制度に関する世論調査（平成 27 年 7 月）によると、以下の 2 点が大きな割合を占めていることが分かる。

①「個人情報が漏えいすることにより，プライバシーが侵害されるおそれがあること」が 34.5％

②「マイナンバーや個人情報の不正利用により，被害にあうおそれがあること」が 38.0％

上記のように、マイナンバーの普及のためには、サイバーセキュリティ対策を強化し、国民の不信感を拭う必要があることは明確である。

2 つ目に、2020 年東京オリンピックにむけて日本のサイバーセキュリティを強化することである。内閣サイバーセキュリティセンターの報告資料は、『2020 年東京オリンピックを成功へと導くためには、大会の開催・運営を支える重要サービスにおけるサイバーセキュリティを確保し、安定したサービスを供給することが不可欠』としている。2020 年東京オリンピックに際し、国際的に注目が集まる中で、日本も例外なく標的にされる可能性が高いことは確実である。サイバーセキュリティ対策強化に集中的にかつ継続的に資金を投資することは、オリンピックを開催する際に極めて重要な課題である。

3 つ目は、税導入により、サイバーセキュリティに対する認識の向上が期待されることである。直接目で見ることができず、対策の緊急性が見えにくいサイバー攻撃・犯罪への対策の意義が国民に広く認識されることは、今後さらなるインターネットベースの情報処理が進む中で、極めて重要であるといえる。

このように、税を導入し、継続的かつ集中的にサイバーセキュリティ対策に投資することは、長期的な目線において意義があるといえる。我々は、国防として日本のサイバーセキュリティにおける脆弱性を打破し、サイバー攻撃・犯罪を未然に防ぐべく、この政策を提言する。

おわりに

本稿では、日本のサイバーセキュリティにおいて、政府の情報セキュリティ予算・施策を行う組織体制に問題があるとし、これに対しての効果的な政策の立案を研究テーマとし、取り組んできた。

この問題にどのようにアプローチしていくべきか探るため、文献調査・インタビュー調査に加えて、2 つの実証分析を行った。この分析により、効果的に投資すべき施策を実証分析したが、税新設後の便益効果を分析することができなかった。また、本来ならば、「企業」の視点からのデータだけではなく、国家規模のサイバーセキュリティのデータも用いるべきであると考えるが、数値化が難しく、被害状況や対策状況が明確でないため、データ入手が困難であった。そのため、本稿では「企業」の視点から分析し、政府としてサイバー攻撃・犯罪から企業または国を守るべき対策を挙げた。

さらに政策提言での所管の点では、比較検討したうえで最もよいとされたものを提案したが具体化できていない。
今後はこのような点を研究課題としていきたい。

本稿では、執筆にあたりヒアリング調査にご協力いただいた中山泰秀衆議院議員から熱心かつ有益な情報を得ることができた。ここに感謝の意を表したい。

本稿の研究が、我が国のサイバーセキュリティ対策に寄与することを願い、本稿の締めとする。

先行研究・参考文献・データ出典

＜ヒアリング先＞

中山泰秀衆議院議員
中山康秀議員事務所　〒530-0055 大阪市北野区野崎町 6－7　大阪北野ビル 8F
℡：06-6363-9330

我々は、2014 年の中山泰秀衆議院議員の「携帯電話税構想」について詳細を伺うため、ヒアリング調査を行った。インターネット上では、携帯電話 1 台につき、毎月数百円の課税をし、一般財源として国の財源強化に充てるというものであった。

しかし、ヒアリング調査でお話を伺ったところ、この構想はマスコミが勝手に作り上げたものだとわかった。

中山氏の構想は、納税率を上げることを目的に税申請の際に携帯電話を使おうとしたものであった。つまり、従来の紙媒体ではなく、携帯電話を使おうとしたものであり、課税対象という意味ではなかった。

したがって、この事例は先行事例として取り上げることができなかったため、ここで記載する。

＜先行研究＞

・村野正泰 (2015)「情報通信技術の進展とサイバーセキュリティ（科学技術に関する調査プロジェクト 2014)」 株式会社三菱総合研究所 情報通信政策研究本部
・Sonnenreich, W., Albanese, J., and Stout B. (2006) “Return On Security Investment (ROSI)– A Practical Quantitative Model” Australian Computer Society Inc. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006 pp. 45-56
・杉野隆 (2016) 「サイバー攻撃と情報セキュリティ」　オペレーションズ・リサーチ

＜参考文献・データ出典＞

・総務省（2014）「情報通信白書」
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc253120.html） 2016/11/4 データ取得
・ITU World Telecommunication /ICT Indicators database
（http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx） 2016/11/4 データ取得
・ 経済産業「マルウェアとは」（http://www.jnsa.org/ikusei/） 2016/10/13 データ取得
・内閣サイバーセキュリティセンター（NISC）「『サイバーセキュリティ基本法』制定と日本のサイバーセキュリティ政策について（2015）」
・内閣サイバーセキュリティセンター(2015)「重要インフラ防護に対する考え方」
（http://www.nisc.go.jp/active/infra/outline.html） 2016/11/4 データ取得
・警察庁(2016)「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」
・総務省（2014）「最近の情報セキュリティに係る脅威の動向」
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc143210.html ） 2016/10/20 データ取得
・内閣サイバーセキュリティセンター（NISC）副センター長 内閣審議官 谷脇 康彦（2015）「我が国のサイバーセキュリティ戦略」
・IT 用語辞典 BINARY「ゼロディ攻撃」
（http://www.sophia-it.com/content/ゼロデイ攻撃) 2016/11/03 データ取得

・内閣サイバーセキュリティセンター(2015)「重要インフラ防護に対する考え方」
（http://www.nisc.go.jp/active/infra/outline.html） 2016/11/4 データ取得
・内閣サイバーセキュリティセンター（NISC）基本戦略グループ 丹羽 良太（2015）「『サイバーセキュリティ基本法』制定と日本のサイバーセキュリティ政策について」
・サイバーセキュリティ戦略本部 「サイバーセキュリティ 2016」『はじめに』
・情報セキュリティ政策会議「サイバーセキュリティ政策に係る年次報告（2013 年度)
・独立行政法人日本原子力研究開発機構(2014)「コンピュータウイルス感染による情報漏えいの可能性について」（http://www.jaea.go.jp/02/press2013/p14010601/） 2016/10/19 データ取得
・小山安博「ソニー、PSN 情報漏洩の詳細発表 - 最大で個人情報 7700 万件、カード 1000 万件」マイナビニュース,2011 年 5 月 2 日（http://news.mynavi.jp/articles/2011/05/02/psn/ ） 2016/10/18 データ取得
・サイバーセキュリティ.com
「サイバーセキュリティガイド」『02.実際の近年のサイバー攻撃による企業の被害事例』
（
https://cybersecurity-jp.com/cyber-security-guide/2-by-actual-recent-cyber-attack-damage-case-of-companies） 2016/10/30 データ取得
・総務省(2016)「政府の情報セキュリティに関する予算」
・内閣サイバーセキュリティセンター(2015)「サイバーセキュリティ戦略」
・内閣サイバーセキュリティセンター(2016)「政府の情報セキュリティに関する予算　資料 5」
・サイバーフォース：全国の警察職員から選抜され、サイバー攻撃・犯罪において高度かつ専門的な知識及び技術を有する者で構成された技術部隊
（http://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_2_6.html） 2016/11/03 データ取得
・日本経済新聞「サイバー防御策開発へ、防衛省と情報通信機構」
（http://www.nikkei.com/article/DGXNASFS24001_W4A520C1MM0000/） 2016/11/14 データ取得
・社会保険労務士井上徹事務所「IT 情報」
・IDC Japan 株式会社「2016 年国内企業の情報セキュリティ対策実態調査結果を発表」
（http://www.idcjapan.co.jp/Press/Current/20160414Apr.html） 2016.11.3 データ取得
・リスク対策.com（2015）「経営層の情報漏えいリスクに対する意識」
（http://www.risktaisaku.com/articles/-/827）2016.11.3 データ取得
・経済産業省　「経済産業省の主なサイバー攻撃対策　資料 5」
・日本経済新聞　「外務省、サイバー攻撃対策の国際ルールづくり主導へ」
（http://mw.nikkei.com/sp/#!/article/DGXLASFS12H1Y_S6A710C1PP8000/） 2016/10/29 データ取得
・サイバーセキュリティ戦略本部「サイバーセキュリティ政策に係る年次報告 (2015 年度) 」
・「サイバー攻撃との終わらない戦いから会社を守るには？太田大州 0 に聞く（後編）」
FUJITSU JOURNAL,2014 年 10 月 6 日（http://journal.jp.fujitsu.com/2014/10/06/01/） 2016/11 /04 データ取得
・総務省「平成 27 年通信利用動向調査」
・2015 年スマホ EC 市場｜市場規模・利用率・時間帯・比率など」『個人消費動向に関する市場規模調査』ミナクル,2014 年 01 月 29 日（http://minakul.jp/smartphone-ec-260 ） 2016/10/29 データ取得
・財務省　「もっと知りたい税のこと」『税の意義と役割』
（http://www.mof.go.jp/tax_policy/publication/brochure/zeisei2507/01.htm） 2016/11/1 データ取得

・内閣官房「内閣官房・内閣府の業務見直しに伴う各省の政策調整機能の強化について　資料7－2」
・Tom Jowitt,“France Will Tax Smartphones To Support Culture”Tech week Europe,May 16, 2013,（http://www.techweekeurope.co.uk/workspace/france-smartphone-tax-116473） 2016/10/25 データ取得
・(株)情報通信総合研究所　グローバル研究グルー 佐藤　仁 「フランス：スマートフォン・タブレット税はフランスの文化振興になる(2013)
（http://www.icr.co.jp/newsletter/global_perspective/2013/Gpre201357.html） 2016/10/16 データ取得
・THE NEW YORK TIMES”As Culture Movies Online,France Tries to Follow It With a Tax”May 14, 2013 （http://www.nytimes.com/2013/05/15/business/global/france-urged-to-impose-tax-on-smartphones-and-tablets.html） 2016/10/20 データ取得
・Pierre LESCURE(2013)”Contribution aux politiques culturelles à l'ère numérique”
・Hugh Carnegy “France set to tax smartphones to protect culture in digital age”FINANCIAL TIMES 2013.5.14
（https://www.ft.com/content/eb6f49f8-bbd1-11e2-a4b4-00144feab7de） 2016/10/22 データ取得
・「次は『携帯電話課税』か…消費税 10％だけでない、財務省がもくろむ新たな増税ネタ」 産経 WEST,2013 年 12 年 23 日（http://www.sankei.com/west/news/131223/wst1312230045-n2.html） 2016/10/22 データ取得
・「携帯電話税を自民議連が検討　自動車税の代わりか」 The Huffington Post ,2014 年 06 月 19 日（http://www.huffingtonpost.jp/2014/06/18/mobile-phone-tax_n_5509951.html） 2016/9/30 データ取得
・経済産業省資（2003）源エネルギー庁「石炭政策について」『石油石炭税法等の改正に伴う石炭への課税について』
（http://www.enecho.meti.go.jp/category/resources_and_fuel/coal/tax.html）2016/10/2 データ取得
・「暮らしのお役立ち情報」『CO2 排出を抑制するため、地球温暖化対策のための税が始まります！』あしたの暮らしをわかりやすく　政府広報オンライン 2012 年 10 月 1 日
（http://www.gov-online.go.jp/useful/article/201210/1.html）2016/10/31 データ取得
・「国家安全保障戦略について」（平成 25 年 12 月 17 日国家安全保障会議決定及び閣議決定）pp.7-8, 15
・警察庁（2012)『平成 23 年　回顧と展望　特集「サイバー攻撃の情勢と対策」警備情勢を顧みて』焦点　第 280 号　平成 24 年 3 月
・McAfee An Intel Company & SDA (2012)「サイバー防衛報告書　『サイバーセキュリティ　：世界ルールの主たる争点』概要」”Cyber-security : The vexed question of global rules”
・佐藤　仁「『Defending a New Domain：Pentagon's Cyberstrategy』（2010）に見る米国のサイバー戦略」InfoCom ニューズレター,2012 年 6 月 13 日
（http://www.icr.co.jp/newsletter/global_perspective/2012/Gpre201246.html） 2016/9/15 データ取得
・総務大臣 山本 早苗（2015）「スマートフォンの料金及び端末販売に関して講ずべき措置について（要請）」
・総 務 省（2016）「 スマートフォンの端末購入補助の適正化に関するガイドライン」
・志田義寧「総務省が携帯 3 社に行政指導、スマホ「実質 0 円」販売規制に違反」REUTERS ロイター,2016 年 10 月 7 日
（http://jp.reuters.com/article/japan-smart-phone-idJPKCN1270KL） 2016/10/24 データ取得

・ITmedia「総務省、スマホ「実質 0 円」販売で大手キャリアを行政指導　3 社『真摯に対応する』」ITmedia ニュース,2016 年 10 月 07 日
（http://www.itmedia.co.jp/news/articles/1610/07/news116.html） 2016/10/28 データ取得
・総務省平成 27 年度版情報通信白書「第 2 部　ICT が拓く未来社会」『（1）ユビキタスから IoT へ』
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc254110.html） 2016/10/30 データ取得
・みずほ情報総研株式会社　株式会社みずほ銀行（2015）
「IoT（Internet of Things）の現状と展望」
（https://www.mizuho-ir.co.jp/publication/report/2015/iot1508.html） 2016/10/27 データ取得
・「国内 IT 投資動向調査報告書 2017」「製品／サービス分野では、『IoT』『AI／機械学習』への新規投資需要が拡大」（https://www.itr.co.jp/report/itinvestment/S17000100.html）
2016/10/28 データ取得
・総務省「マイナンバー制度の施行状況について（資料 2）」
・「マイナンバーカード普及率 5%で、大失敗に終わった住基カードに酷似か」@nifty ニュース,2016 年 10 月 16 日（https://news.nifty.com/article/domestic/society/playboy-68276/）
2016/10/16 データ取得
・内閣府政府広報室（2015)「『マイナンバー（社会保障・税番号）制度に関する世論調査』の概要」『2 マイナンバー制度に対する懸念』
・NISC「2020 年東京オリンピック・パラリンピック競技大会に向けた取組」資料 5
・ (株)情報通信総合研究所グローバル研究グループ　佐藤　仁 「ロンドン五輪を狙っていたサイバー攻撃」InfoCom ニューズレター,2013 年 10 月 23 日
（http://www.icr.co.jp/newsletter/global_perspective/2013/Gpre2013115.html） 2016/11/1 データ取得
・甲斐賢(2012) 「ヒューマンファクタによる情報リスクを技術で低減するオフィスセキュリティ(Dissetation_全文）」京都大学 京都大学学術情報レポジトリ紅
・土屋大洋(2010)『警察と軍におけるサイバーセキュリティ対策に関する国際比較研究』慶應義塾大学グローバルセキュリティ研究所 財団法人社会安全研究財団 2010 年度一般研究助成報告書
・村野正泰 (2015)「情報通信技術の進展とサイバーセキュリティ（科学技術に関する調査プロジェクト 2014」 株式会社三菱総合研究所 情報通信政策研究本部
・Sonnenreich, W., Albanese, J., and Stout B. (2006) “Return On Security Investment (ROSI)– A Practical Quantitative Model” Australian Computer Society Inc. Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006 pp. 45-56
・ Rowe, B.R., and Gallaher, M.P. (2006) “Private Sector Cyber Security Investment Strategies: An Empirical Analysis” Technology Economics and Policy RTI International
・Dorgrul, M., Aslan, A., & Celik, E. (2011) “Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism” Turkish Air War College
・ McAfee An Intel Company & SDA (2012)「サイバー防衛報告書　『サイバーセキュリティ：世界ルールの主たる争点』概要」”Cyber-security : The vexed question of global rules”
・環境省「（2008）税収の使途について」『3. 目的税・特定財源に関する考え方』
・国土交通委員会調査室 畠山肇　村田和彦「道路整備費の財源等の特例に関する法律の一部を改正する法律」
・決算委員会調査室　櫻井 真司「決算から見た目的税・特定財源の課題 ～道路以外の特定財源にも見直しの余地はあるか？～ 」『4. 石油石炭税』
・財務省主計局(2006) 「特別会計のはなし」『第 I部 特別会計とは何か』

・日本統計学会(2012)　『統計検定 3 級対応　データの分析』　東京図書
・日本統計学会(2012)　『統計検定 2 級対応　統計学基礎』　東京図書
・高杉豊・馬場敬之(2014)　『演習統計学』　マセマ
・山本拓・竹内明香(2013)　『入門計量経済学』　新世社
・山本勲(2015)　『実証分析のための計量経済学』　中央経済社