英国のサイバーセキュリティ戦略

―脅威からリスクへの認識変化と組織的対応―

グレゴリー・ディーエル（Gregory Dalziel）[1]

英国政府は、国家サイバーセキュリティ・プログラムを創設した。それによって、多額の予算が確保され、新しい組織が設置され、包括的な戦略が公表されることになった。その背景には、セキュリティの意味が拡大し、幅広い問題を包み込むと同時に、戦略的思考の正当化が「脅威」のロジックから「リスク」のロジックへとシフトしていることがある。本稿では、英国がサイバーセキュリティ戦略においてこれまでにとってきた道のりを検証し、制度的な視点から組織の問題を検討する。英国のサイバーセキュリティに関する認識変化は、三つの期間に分けることができる。そうした認識の変化の結果、セキュリティの意味が広がり、「脅威」よりも「リスク」が好まれるようになり、リスクのロジックを正当化するために新しい組織と慣行が生まれてきたことを論じる。

１．　はじめに

英国政府は、2010 年に発表した国家安全保障戦略において「サイバーセキュリティ」を優先的に取り組むべきリスクとして取り上げた（HM Government 2010a: 16）。その直後、同国政府はサイバーセキュリティ戦略を発表し、サイバーセキュリティに関わる二つの政府機関の新設と 6 億ポンド（約 863 億円 [2]）に及ぶ予算を含んだ「国家サイバーセキュリティ・プログラム」を創設した [3]。英国情報局秘密情報部（通称MI6）長官は、2009 年の議会において「サイバーセキュリティ問題は、急激に政策立案者の関心事となっている」と証言している（Intelligence & Security Committee: 2010）。これらの取り組みを見る限り、英国政府が「サイバーセキュリティ」を深刻に捉えていることが分かる。

英国政府はさらに、2011 年にサイバースペースに関するロンドン会議を主催し、日本政府も参加した。英国のサイバーセキュリティ戦略や政策をめぐるこれまでの試みは、日本の政策決定者にとっても有益な前例となり、示唆を与えるものとなるのだろうか。

サイバーセキュリティ・サミットやその他の協議は、サイバースペースにおける秩序維持のための規制枠組みといった「利用規則」に集中しがちである。しかし、利用規則に焦点を絞ると、組織間のコミュニケーション等、実行に伴い発生する膨大な作業が無視されがちである。そこで本稿では、英国におけるサイバーセキュリティ戦略と政策の進展を、1995 年以降の同国の関連戦略と組織の変化を追いながら、「組織（organizational field）」（DiMaggio and Powell 1991）のレベルから説明する。また、その分析を通じ英

---

[1] 慶應義塾大学グローバルセキュリティ研究所（G-SEC）研究助教

[2] 2013 年 1 月 11 日現在の 1 ポンド＝143.88 円で計算。

[3] 6.5 億ポンドと公表されているが、そのうちの 0.5 億ポンドは政府通信本部（GCHQ）に配分されていることからその分は差し引いた。

国政府がサイバーセキュリティの意味をどのように捉え、組織としてどのように対応してきたかを明らかにする。

本稿は、以下のように構成されている。まず第一節でミッケル・ラスムセン（Mikkel Rasmussen）の研究をもとに、戦略の手段・目標における手段的合理性が、リスクを重視する社会とともにリスク合理性へと変化してきたことを概観する。ラスムセンの考察は、本稿における英国のサイバーセキュリティ戦略分析の骨組みとなる。ただし、ラスムセンの分析はリスクの影響を「認識レベル」でしか捉えていないため、本稿では、リスクが「組織レベル」に与える影響も分析していく。第二節では、分析の手法を示し、第三節では先行研究をたどった上で、本稿の分析枠組みを示す。第四節ではサイバーセキュリティの意味が英国において 1995 年以降どのように変化してきたかを、三つの異なる期間を特定した上で分析する。この分析は、第五節の課題である英国のサイバーセキュリティ戦略の理解にもつながる。第六節では、サイバーセキュリティの意味や戦略の変化が組織と制度に与えた影響を、英国を例に検証する。最後に、結論として本稿の分析の政策的示唆について述べる。

２．　分析の手法

なぜ英国がサイバーセキュリティに関する戦略やアプローチを現在のような形に構築してきたかを考察する上で、国家にとってサイバーセキュリティとは何かを理解することが重要である。政府はどのようにしてサイバーセキュリティの概念を定義するのであろうか。その定義はこれまでどのように変化してきたのであろうか。

言説追跡（discourse tracing）は、質的な文書分析の一手法であり、そこでは「単なる量や、二つ以上の変数間の数量的な関係よりも、内在的な意味やパターン、プロセスの探索を含む、発見と記述に主たる強調が置かれる」（Altheide 2000: 290）。この手法は、多くの点でグラウンデッド・セオリー（grounded theory）に近い（Glaser & Strauss 1967; Charmaz 2006; Corbin & Strauss 2007）。そこでは多様なデータの収集とそのコーディングを重視する。このコーディング・プロセスの相互作用を繰り返し行うことで、特定のテーマとプロセスが見えてくる。

本稿では、英国政府が公開した重要な戦略と年次報告書、それに演説や重要なメディア記事を合わせて収集した。これを通じて、英国政府のサイバーセキュリティについての言説についてのある程度の理解を得た上で、情報データベースを構築し、データをコード化するために NVivo というソフトウェアを用いた。特に注目したのは、(1) サイバーセキュリティについての言説（サイバーセキュリティの概念や意味の変化、そして、リスク、脅威、機会のいずれの文脈において議論されているか）はどのようなものか、(2) 政府のどの機関がサイバーセキュリティについて懸念を抱いているか、(3) サイバー領域によって脅かされていると認識しているのは誰か、(4) セキュリティの意味とは何か、である。

３．　リスク社会、安全保障、戦略

ラスムセンは著書『戦時のリスク社会（The Risk Society at War）』において、ウルリ

ッヒ・ベック（Ulrich Beck）とアンソニー・ギデンズ（Anthony Giddens）の研究を基に（Beck 1998, 2002; Giddens 1991）、「西側社会においてリスクの概念が重要性を増すにつれ安全保障の意味が変化し、そうした新たな安全保障の意味を合理化する戦略の利用のされ方も変化している」と述べている。これは、過去にカール・フォン・クラウゼヴィッツ（Carl von Clausewitz）が述べた戦略的思考における手段・目標という手段的合理性が、西側社会においてリスクの概念の重要性が増すにつれ、リスクを中心とした合理性へ変化したことを意味する。

軍事領域と安全保障領域における戦略は、伝統的に（軍事的）手段と（政治的）目標を連結する「軍事力と政治的目的の間の架け橋」（Gray 2006）と考えられている。B・H・リデル・ハート（B. H. Liddell Hart）による古典的定義でも、戦略は「政治目的を達成するために、軍事的手段を配分・適用する術」（Hart 1967: 321）と捉えられている。このように、国家の安全保障において戦略的思考や戦略学は、軍・武力行使に関するものが中心であった。また、軍事以外の領域においても、「戦略策定は一般的に、目標を達成するために検討され、計画された資源配分と考えられている。意識的選択、手段的合理性、目標指向の行動こそが、戦略的行為の土台である」（Chia and Holt 2009: ix）と言われるように、特定の目標達成のために、手段的合理性を利用し、資源を計画的に配分することが戦略の意味の中心をなしている。

そして、国家の安全保障を害するものが「脅威」と呼ばれてきた。ラスムセンは脅威を「敵対的な目的を実現するために敵が持つ能力で、的確に識別・測定可能な特定の危険」（Rasmussen 2006: 1）と定義している。このように、脅威の概念は敵の意図や能力に焦点を絞っているが、それは後に述べるリスクとは異なる。敵の意図と能力は、目標と手段という手段的合理性に類似している。つまり、意図は人々が望む（達成あるいは回避すべき）「目標」であり、能力はそのような目標を達成するための「手段」である。これは伝統的な戦略的思考において手段的合理性が機能していることを示している。脅威の度合いや、敵の意図の適切な把握について様々な議論が可能だが、いずれの議論においても共通するのは脅威の範囲は限定的で終結可能ということである（Dalziel 2011; Malle et al. 2004; Stech 1979; Stech and Hoffman 1982）。したがって、脅威には打ち勝つことが可能であり、自らの安全を担保することも可能である。

脅威は一般的に限定的で終結可能であるが故に、手段や目標といった手段的合理性から分析可能であるのに対し、リスクは「将来起こり得る」シナリオを基礎としている。本稿ではリスクを「その現実化を防止するために政策提言がなされるようなシナリオ」（Rasmussen 2006: 2）というラスムセンの定義に基づき論述していく。ベックやギデンズによると、「リスク社会」とは、リスクが社会の中心的な構成原理となっている社会である。それは、再帰性および未来との関わりによって特徴付けられる。人々が自己と自己の行動をどう考えるかという再帰性は、それ自体が対処すべき新たなシナリオを作り出す。将来起こり得るシナリオは、一般的には将来的な失敗という悲観的なものであり、それと同時に、その悲観的シナリオの実現を避けるための活動を生み出す（Dalziel 2011）。つまりリスク合理性では、リスク自体が問題を構成するだけでなく、そのような問題を回避するための活動をも生み出すのである。さらに重要なのは、リスク社会ではますます焦点になるということであり、未来の潜在的なシナリオの生成、そしてそれへの対応を行うた

めに数々の組織や慣行を作り出していくことになる。

そのような活動は、脅威の撃退や抑止のためではなく、悲観的な将来の回避を保証するためにある。シナリオが現実に起こらなかったという事実は、将来このシナリオが決して起こらないことを保証するわけではない。脅威は限定や特定された問題であるが、将来の予測は我々人間の想像によってなされるため、想像の限界のみがその限界である。したがって、リスク社会における戦略は、脅威の撃退や抑止から、それらが不可能なリスクの対処に移行していく（Rasmussen 2006）。実際、英国の「戦略防衛安全保障レビュー」では、主要な目的の一つとして「いかにリスクに対処するか」を説明することが挙げられている（HM Government 2010b: 19）。

この「リスクの対処」と「未来との関わり」が、リスク合理性の主な特徴であるが、ラスムセンがそのほかに挙げたリスク合理性の特徴に「ブーメラン効果」がある。ブーメラン効果とは、知識、意識、行動によって社会自体が新たな脆弱性を創造し、それにより対処が必要な新たなリスクが創出されることを意味する。これはリスク社会の特徴である再帰性による影響のもう一つの見方といって良い。「リスク社会」についての主要な論者の一人であるウルリッヒ・ベックは、「リスクは、リスク拡散における社会的なブーメラン効果を示す」と書いている（Beck 1992：37）。これはよく言われる「トレードオフ」の単なる言い換えに過ぎないという指摘があるかもしれない。また、「予期せぬ帰結（unanticipated consequences）」について社会学者のロバート・マートン（Robert K. Merton）による影響力の大きい論文を指摘する人もいるかもしれない（Merton 1936）。これは確かにその通りだが、トレードオフの考え方は、リスク領域に存在していないような意思決定上の確実性の程度を示していることが多い。実際、トレードオフとブーメラン効果という関連する概念の間には三つの違いがある。

第一に、リスク社会においては、反射性（reflexivity）が意思決定におけるトレードオフに関する単純な自己認識以上のものへとつながる。つまり、この反射性から生じる多様な慣行の制度化である。ブーメラン効果を予期し、軽減し、管理するために設計された組織や慣行の増加を見ることができる。

第二に、多数のアクターがおり、意図せぬ帰結を伴う環境においては、多様なアクターがリスクに対して多様な許容範囲を持つかもしれない。ラスムセンが書いているように、「ある人が非常に危険とみなすシナリオが、他者にとっては許容可能かもしれない」（Rasmussen 2006：40）。リスクに対する許容範囲（つまりリスク文化）、そしてこの戦略的な効果は、しばしばトレードオフの概念によって覆い隠されてしまう。

最後に、ブーメラン効果は、「あらゆる行動が新しいリスクを伴うために政策担当者が麻痺してしまう」（Rasmussen 2006：39）とき、いわゆる「リスク・トラップ」へとつながる可能性がある。

多くのグローバリゼーションに関する文献は、グローバリゼーションを利益や機会（経済や、人とモノの流れ）を増加させるものである一方、この再帰性によるリスク（国際犯罪、流行病、テロリズム）の源泉であるとも捉えている。サイバー領域も同じような形で見られている。それは国家、民間のビジネス、そして個々の市民に広範な恩恵をもたらす。しかし、そのような恩恵をもたらすサイバー領域の利用の増大と依存は、管理されなくてはならない巨大な脆弱性を生み出すことになる。

このようなラスムセンのリスク社会研究と安全保障・戦略研究を統合させる試みは「認識レベル」に止まっており、戦略の実行における「組織」（DiMaggio and Powell 1991）の変化を分析対象には含んでいない。そこで次節以降では、リスク社会におけるサイバーセキュリティの意味変化を分析し、その変化とリスク合理性への移行がどのようにして組織に変化をもたらしたかを英国を例に説明していく。

４．　英国におけるサイバーセキュリティの意味の変化

言説追跡分析を用いると、英国のサイバーセキュリティの考え方は、三つの期間に分けることができる。これらの三つの期間は、サイバー領域についての一般的に流布している言説と、そのような問題を懸念する政府組織に加えてセキュリティとの関係によって代表される。1990 年代中盤から始まる第一の期間は、「情報戦争」や「サイバー犯罪」という概念に集中していたことが特徴である。2000 年から始まる第二の期間では、サイバー犯罪という概念が引き継がれる一方、情報戦争は「情報保証」と呼ばれる概念へと移行する。そして 2008 年あたりから始まる最後の期間では、「サイバーセキュリティ」の概念が普及し始める。このような変化は、英国の安全保障領域における戦略の位置づけが変化していることを表している。

当初、サイバー領域における、もしくはそれを媒介した脅威というのは、国家や国家の情報システムを想定したものであった。情報戦争に焦点を当てていたのも、軍事機関がサイバー領域を武力行使の文脈でいかに利用するかを考慮していたことを反映している。サイバー領域は、敵の認識・行動に影響を与えたり、理解を妨げたりするための手段と考えられていた（例えば、Libicki 1995）。1990 年代のインテリジェンス・安全保障委員会の年次報告書は、主としてスパイ活動目的の政府ネットワークへの浸透に焦点を絞っている（Johnston 1996; Tenner 1997 も参照）。このような焦点の移動は、ソビエト連邦の崩壊や冷戦の終結を伴う 1990 年代はじめに起きていた安全保障の考えの広範な変化と同じであり、それは安全保障に関する学術的な分権においていまだにしばしば議論されている（例えば Allison & Treverton 1992; Baldwin 1997; Booth 1991; Buzan 1991, 1997; Buzan et al. 1998; Campbell 1992; Katzenstein 1996; Mathews 1989 を参照）。

第二の期間では、情報戦争から情報保証へと移行していく。「情報保証（information assurance）」とは、悪意あるアクターやデータの偶発的な紛失・損害からのデータとシステムの安全確保を指している。後に触れるサイバーセキュリティの曖昧な定義とは対照的に、情報保証は多くの行政機関でより具体的に定義付けがなされている（Cabinet Office 2007, 2011; Home Office 2010）。情報保証への移行はサイバー領域の利用拡大やそれへの依存がリスクになるという考えの拡大に起因している。またそれは、リスク社会における「ブーメラン」効果の認識と、現代の戦略を象徴するリスク合理性への移行も示している。1990 年代中盤から注目され始めた「2000 年問題 [4]」はサイバー領域への依存によって生じるリスクの象徴的事例である。

---

[4] 2000 年問題は、西暦 2000 年を想定していないコンピュータ・プログラムが暴走したり、停止してしまったりするのではないかという問題である。結果的には、事前対処によって深刻な問題はほとんど起きなかった。

> ミレニアム・バグ［2000 年問題］による警鐘は、我々の社会がいかにコンピューター・システムに依存しているのかを鮮明に証明した。コンピューター・システムの安全の担保は我々の生活にとって不可欠であり、「情報戦争」に付随する機会やリスクの適切な認識が必要である。最近の個人ハッカーによる主要な軍事施設への侵入は、無害な事件と見られるかもしれないが、システム的な観点と敵の意図をたどれば、これらが壊滅的な効果をもたらし得たことが分かる。（括弧内は筆者による補足。）（Intelligence & Security Committee 1998: viii）

情報システムへの依存度の高まりにより、システム維持の重要性が増し、その監視や管理のための情報技術（IT）の専門家の数も増加した。システムへの依存はリスクの増大をもたらしたが、この当時のリスクは情報技術という比較的狭い分野に限定的であった。この二つの期間における安全保障の位置づけは、依然として国家とその情報システムに焦点が絞られており、あくまでも軍やインテリジェンスが取り扱う分野と考えられていた。一方、二つの期間に共通しているサイバー犯罪の分野は警察が取り扱う分野という明確な区分があった。実際に、最初のサイバー犯罪対策組織は、情報戦争の概念が登場する以前の 1985 年に設置されたロンドン警視庁の詐欺調査班であった（Sommer 2004）。

サイバー犯罪や e–犯罪と称される用語は英国において使用されてきたものの、未だに法的な定義は設定されていない（House of Lords 2007: 64）。内務省は「合法か違法かは使われた手段ではなく、行動の実態によって決まるものであり、オフラインで違法なものはオンラインでも違法であるべきだ」と述べている（Home Office 2009）。

国家犯罪捜査当局（後に重大組織犯罪局、通称 SOCA［Serious Organised Crime Agency］に吸収合併された）が 1999 年に実施した「プロジェクト・トローラー（Project Trawler）」では、サイバー犯罪を「コンピューター・ネットワークが犯罪を実行する上で直接的または明確な手段となっている違反行為。コンピューターの相互接続性が重要な特徴」（National Criminal Intelligence Service 1999）と定義している。当時、英国政府がサイバー領域を介した悪意ある行動（ハッキング、不正詐欺、データの窃盗）と定義したものは、安全保障における脅威ではなく、刑事罰や警察による対応が必要なものと考えられていた。

第三の期間であるサイバーセキュリティ時代へと英国が移行するにあたり、実際には「サイバーセキュリティ」という単語は、初版の「サイバーセキュリティ戦略」でも、その改訂版においても定義されていない。また、いかなる政府出版物や議会における証言においても、サイバーセキュリティに関する公式の定義を見つけることはできなかった。言説追跡を通じてサイバーセキュリティの定義を推察することは可能かもしれないが、英国政府がこの「曖昧性」そのものを利用していることは注目に値する（Eisenberg 1984）。サイバーセキュリティの意味の曖昧さは、サイバーセキュリティ戦略を策定した管轄領域が広い内閣府のような組織の産物といえるが、概念の曖昧さは、多くの組織アクターによる多大な関与を可能にした。これは、情報保証が情報技術関連機関の技術専門家の管轄領域と捉えられていたのとは対照的である。

サイバーセキュリティ戦略において明確に定義されているものもある。「サイバー領

域」は、「あらゆる種類のネットワーク、デジタル活動であり、これらにはデジタルネットワークを介するコンテンツや活動もふくまれる」と定義されている（Cabinet Office 2009）。したがって、「デジタル活動」やデジタルコンテンツを侵害または妨害するものは何でも、サイバー領域の安全に影響を与えるものだと考えることも可能である。

このサイバー領域の定義は、著作権侵害といった問題をも安全保障領域に持ち込んだ。またこの定義は、サイバー領域が「脅威」に晒されているのではなく、むしろサイバー領域そのものが管理されるべき「脅威の源泉」として捉えられていることを示している。国家、民間部門、個人の安全は、サイバー領域内や、サイバー領域経由で脅かされている。そのためサイバー領域は、それ自体を守らなくてはならないと同時に、サイバー領域からも守られなくてはならない。これは、目標と手段の合体であり、ラスムセンが主張する戦略的思考におけるリスク合理性の典型である。こうした状況では脅威の撃退、抑止は不可能であるが、リスクへの対処だけは可能なのである。

５．　英国におけるサイバーセキュリティ戦略の策定

英国政府にとってサイバー領域は、手段と目標、利益と脆弱性の根源でもある。英国政府は 2009 年のサイバーセキュリティ戦略において、このようなリスク合理性を以下のように強調している。

> 市民、企業、政府は、安全で、確実で、復元力のあるサイバースペースの恩恵を最大限受けることが可能である。しかしそのためには、すべての関係者が、リスクを理解及びそれに対処すべく、そして犯罪者やテロリストが利益を享受することがないよう、また、英国の安全保障と社会の回復力を強化のためにサイバースペースにおける機会を活かすべく、英国内外において協力しなければならない（Cabinet Office 2009: 3）。

このようなサイバー領域の見方は、非常に首尾一貫している。ジャック・ストロー（Jack Straw）元内務大臣は 2001 年に国家ハイテク犯罪対策ユニット（National Hi Tech Crime Unit）の設置を発表する際に以下のように発言している。

> 政府は、英国を e コマース活動において世界で最良かつ最も安全な場所とするためハイテク犯罪に立ち向かっている。インターネットのような現代技術は多大な合法的利益をもたらすが、一方でそれは金融詐欺や幼児関連犯罪といった非合法活動を行う犯罪者にも多大な機会を与える。本日発表する資金の投入は、コンピューターを介した幼児関連犯罪、不正行為、恐喝、ハッキングといった犯罪に対する警察の捜査能力を高めることになるだろう（Home Office 2000）。

以上のような発言は、インターネットが利益と脅威を同時にもたらすという戦略における「リスク合理性」の特徴を表して示している。だが、このジャック・ストロー元内務大臣の発言の最も注目すべき点は、この時点ではハッキングや詐欺といったサイバーセキュリティへの認識が、「安全保障」としてではなく「犯罪」として認識されていたことにあ

る。「英国を、e コマース活動において、世界で最良かつ最も安全な場所とする」という英国の目標は、前述のサイバーセキュリティ戦略と大差はない。しかし、いずれも「良い」未来を示す一方で、2009 年のサイバーセキュリティ戦略では、悲観的な未来（リスク）の認識が高まり、それと共に安全保障の意味も拡大している。以上のような意味の変化は、後に触れる安全保障領域の拡大、特に関係するアクターの拡大の要素ともなっている。

2009 年に初めて発表され、2011 年に改訂されたサイバーセキュリティ戦略は、サイバーリスクの根源を、犯罪者（詐欺、・窃盗）、国家（スパイ活動、サイバー領域を利用したインフラ破壊）、テロリスト（通信、プロパガンダ、資金調達）の三つに大きく分けているが、サイバー犯罪は既に現在進行中で顕在化している主要な脅威として認識されている（Cabinet Office 2009, 2011; Intelligence & Security Committee 2011: 53）。一方で、治安当局は、国家によるスパイ活動を主要な懸念事項として挙げている。この二つの現在進行中での顕在化している脅威において着目すべき点は、サイバーセキュリティ戦略が公表される以前から、これらのリスクにいかに対処すべきかを記載した戦略が既に公表されていたことにある。サイバー犯罪については以前から様々な戦略（ACPO 2009; Home Office 2010）が発表されており、情報窃盗（スパイ活動）についても様々な情報保証に関する戦略やドクトリンの中で言及されている。

国家情報保証戦略（National Information Assurance Strategy: NIAS）は 2003 年に公表され、サイバーセキュリティ戦略が発表される 2 年前の 2007 年に改訂されている。ハッキング、データの窃盗や紛失、情報システムへの依存によるリスクに注目していることから、NIAS はサイバーセキュリティ戦略の構築に影響を与えただろうと考えられることもあるが、実際にはほとんど反映されていない。

NIASは戦略の中で、三つの機関によって構成される、より広範な情報保証センター（Wider IA Centre）の創設を企図していた。その三つのうち一つ目は、内閣府 [5]に所属する情報保証中央スポンサー（Central Sponsor for Information Sponsor）、二つ目は、政府通信司令部に所属する電子通信セキュリティ・グループ（Communications-Electronics Security Group）、三つ目は、内務省に所属する国家インフラ保護センター（Centre for the Protection of National Infrastructure: CPNI）で、CPNIは民間企業システムへの脅威に関する情報の連絡と提供を中心に取り扱う。さらにNIASは、ビジネス・企業・規制改革省（2009 年にはビジネス・イノベーション・職業技能省に改名された）、内務省、SOCAにおけるe-犯罪ユニットの役割についても記述している。

前述の通り、サイバーセキュリティ戦略の枠組みにおいて、NIAS の構想はあまり反映されていないが、共通点もみられる。両戦略はいずれも内閣府から発表されており、複数の省庁間協力の調整、民間セクターとの連絡、伝統的に安全保障と無関係な組織の関与を試みている。

一方、サイバーセキュリティは情報保証の概念よりも、リスクと安全保障に関するより広範な定義を必要とするため、サイバーセキュリティ戦略では、NIAS と比較し安全保障の領域は拡張され、より悲観的な未来が含まれる。また、内閣府の（理論上の）影響力や

[5] NIAS は内閣府が発行している。

管理・調整の領域が拡大されている。

こうした状況では、脅威やリスクは「外部（例えば敵）」に存在するものではなく、自らの行動の結果によって生じる（ブーメラン効果）。同じことが安全保障以外の戦略においてもみられる。2009 年に英国政府が発表したデジタル・ブリテン（Department for Business, Innovation & Skills 2009）の、インターネットの経済的効果の利用に関する政府戦略には、（1）英国のネットワークの安全性及び信頼性の認知、（2）知的財産権の保護、（3）オンライン・ビジネス取引数の増加、（4）オンラインを利用した公共事業業務による「効率向上と費用削減」が掲げられている。

このような楽観的な未来への志向は、悲観的なシナリオも同時にもたらす。安全で信頼のおけるネットワークの認知度向上には、技術ドクトリンだけでなく、知的財産権保護のための、法整備、監視、執行といった認識や行動を具体化させるための戦略的コミュニケーション・キャンペーンが必要となる。民間ビジネスか公共事業業務かに関わらず、オンライン取引数増加は脆弱性やリスクの増大を必然的にもたらす。英国政府がオンラインへ移行すればするほど、英国政府と市民がより多くのリスクに晒される。それへの対処に新たな組織、戦略、資金が必要になる。こうした自己誘導的な脆弱性は、サイバーセキュリティ戦略に以下のように明確に述べられている。「政府の事業効率改善の中には、税額控除、消費税、所得税のオンライン申告といった、より便利なサービスの提供に向けた取り組みがある。こうした取り組みは、公共事業関連詐欺や証明書の不正入手を狙うサイバー犯罪のリスクに晒されている。我々はそうした犯罪の発生を確実に防がなければならない。」（Home Office 2010: 6）

英国のこうした戦略の普及や増加は、英国政府による対処の合理性が再帰的であることを示している。ロバート・C・H・チア（Robert C.H. Chia）とロビン・ホルト（Robin Holt）による組織の戦略研究では、英国のサイバーセキュリティや安全保障ガバナンスの戦略や慣行で見られるリスク考慮の傾向は、一般的に考えられているほどリスクの制御を行うことはできないと記述している（Chia and Holt 2009: 44）。むしろそれは、いっそうのリスクと不確実性しか生み出さない。事実、英国はオンラインの活用を利益の源泉と捉えている一方で、それをリスクの根源としても捉えている。つまり、多くのユーザーがサイバー領域で活動するほど、ユーザーは潜在的により多くのリスクに晒されるのである。

リスク社会では、領域が不明確になる。目標と手段に関する明確な記述がないだけでなく、安全保障と非安全保障の領域間の境目は明確に定義しづらくなっている。個別に明確な領域が存在することで人々は集団内において一貫性を保つことが可能だが、明確な領域の欠如は人間関係や組織の輪を乱す原因となる（Zerubavel 1991）。安全保障領域におけるアクターの数は増加しており、新たな組織だけでなく、拡大された領域の調整や統制を行うための新たな慣行を組織内に生み出している。次節では、英国でサイバーセキュリティ領域を管轄としている組織を取り上げる。

６．　英国における国家サイバーセキュリティ・プログラムとサイバーセキュリティの組織

サイバーセキュリティ戦略では、内閣府が英国のサイバーセキュリティを主導すること

となっているが、同組織はサイバーセキュリティ戦略を策定した張本人でもある。サイバーセキュリティ戦略を実行に移す過程で、国家サイバーセキュリティ・プログラム（National Security Programme: NCSP）の発足とともに、6 億ポンド（約 863 億円）の財政支出が行われた。この資金の主要な内訳は、安全保障とインテリジェンスを管轄する三つの省庁に 56%、国防省（Ministry of Defence）に 15%、内務省に 11%、政府官房情報局（Government Chief Information Office）に 10%となっている。

また、内閣府内に新しい二つのユニットが発足した。一つはサイバーセキュリティ局（Office of Cyber Security: OCS）と呼ばれ、国家安全保障事務局（National Security Secretariat）に属しており、近年ではサイバーセキュリティ情報保証局（Office of Cyber Security and Information Assurance: OCSIA）へと改名された。同ユニットは NCSP を管理、調整（予算の管理も含む）と、英国のサイバーセキュリティの合理化が主な取り組みのようである。サイバーセキュリティ戦略の中でも「既存の原則、政策、法律、規制枠組み間のギャップを特定する」（Cabinet Office 2009: 18）ことを求められている。この種の取り組みは、領域が拡大し、領域横断的なリスクを合理化する上で重要である。戦略策定はしばしば、組織における一貫性を創造する試み（Chia and Holt 2009）として行われるが、OCSIA も「政府全体のサイバーセキュリティや情報保証を主導するための、戦略と政策の一貫性を提供する」（Intelligence & Security Committee 2011: 56）ことを主たる目標としている。国防省内においても、「サイバー攻撃の脅威に対する統合ないし統一された対応を策定する」（Kelly 2011: 11）ために「サイバーセキュリティ政策チーム（Cyber Security Policy Team）」と呼ばれる OCSIA と似た組織が設立された。

内閣府内に発足した新たなユニットの二つ目は、サイバーセキュリティ運用センター（Cyber Security Operations Centre: CSOC）である。組織上は内閣府に属しているが、実質は通信傍受を担うインテリジェンス機関である政府通信本部（GCHQ）に置かれている。この組織は、「サイバースペースの展開の監視（中略）趨勢の分析やサイバー事件に対応するための技術的向上」（Cabinet Office 2009: 17）に権限を有する。最初に発表されたサイバーセキュリティ戦略では、CSOC の優先事項を、(1)「サイバースペースの健全性と事件対応の調整の能動的監視」、(2)「ネットワークやユーザーに対するサイバー攻撃の理解促進」、(3)「ビジネスや民間へのリスクに関する助言や情報の提供」と述べている（Cabinet Office 2009: 5）。しかし、CSOC の取り組みが、どれほど他の組織の取り組みと重複しているかは不明である。例えば事件対応の調整の場合、CSOC がいかに GovCertUK、CSIRTUK（CPNI）、MODCERT（国防省）といった主要なサイバー対応チームと連携を取り合うのかについては不明確である。また三つ目の優先事項では、CPNI とビジネス・イノベーション・職業技能省（Department for Business, Innovation and Skills: BIS）に属するサイバーセキュリティ・チームの権限との間に矛盾が生じている。

サイバーセキュリティに関する政府の責務は内閣府が担うことになっているが、常にそうだったというわけではない。当初、内閣府に属する OSCIA（OCS）、CSOC が NCSP を主導するとされていたが、その政府の責務は内閣府ではなく内務省の安全保障担当大臣（Minister for Security）が担っていた。情報・安全保障委員会（議会の監視委員会）は、

このような責務や人的資源の分断について懸念を抱いておりそれを指摘している。当時の担当安全保障大臣であるポウリーン・ネビルネヴィルージョーンズ女性男爵（Baroness Pauline Neville-Jones）は、それに対し同委員会で「あなた方はそれが制度における公的な抜け穴であると指摘しているが、私はそれが存在する可能性に異議を唱えない」（Intelligence & Security Committee 2011: 56）と回答している。2011 年 5 月に、サイバーセキュリティに関する政府の責務は内閣府大臣へと正式に移行移管され、ねじれは解消された。

このような状況が異常であったのは、内閣府大臣が、情報保証の戦略である NIAS の責務を担う一方、情報保証分野も含むサイバーセキュリティ戦略の責務は安全保障担当大臣が担っていた点にある。また、サイバーセキュリティ戦略における情報保証分野の責任は安全保障大臣にあるのか、内閣府大臣にあるのか明確な記載はない。しかしこうした状況は、少なくともサイバーセキュリティが、当初内務省の管轄である犯罪や犯罪行為の枠組みとして理解されていた事実を反映している。また、同状況はサイバー犯罪（内務省管轄）と情報保証（内閣府管轄）の分断を示しており、サイバーセキュリティ戦略は、これらを合理的に一つの枠組みにまとめ上げる試みといえる。

情報・安全保障委員会の 2010～2011 年の年次報告によると、英国では 18 の省庁がサイバーセキュリティに関わっている（Intelligence & Security Committee 2011: 55）。同委員会は、多数の関係省庁によって多くの活動が重複し、無駄な資源が投じられている可能性について憂慮しており、明らかな問題として取り上げている。

ただし、同報告書におけるサイバーセキュリティに関わる省庁や組織の総計は低く見積もられている。その数は、サイバー犯罪（サイバーセキュリティの一分野）に関わる省庁を含めれば増加する。情報保証活動（サイバーセキュリティの一分野）に関わる省庁は、過去の報告では 30 以上と言われており、それらを含めれば、さらにその数は増加する。オープン・ソースを利用した筆者の独自の調査では、最低でも 40 の省庁が関係している。これらの数字の乖離は、サイバーセュリティの概念の差に由来するものと考えられるが、そもそも政府が広範なサイバーセキュリティ分野に取り組む組織の広さ（数）と深さ（構成）を完全に把握していないことが根底にある。組織の調整の欠如には負の効果があるのかは不明であるが、政府（少なくとも内閣府と監視委員会）は明らかに、サイバーセキュリティ・ガバナンスに関与する組織をまとめるための合理化を強く望んでいる。

すでに触れたような、安全保障の意味の拡大や領域横断的リスクは、OCSIA と CSOC といった新たな組織を設立するだけでなく、安全保障に無関係の組織も安全保障におけるアクターとして取り扱わせるようになった。例えば知的財産権の保護は、現在では安全保障領域に含まれると考えられている。そのため、BIS のような産業界の知的財産権の保護に関する組織や、「2012 年のオリンピックに関するオンラインの著作権」（Home Office 2010: 22）を管轄した文化省（Department for Culture, Media and Sport）のような、かつては安全保障と無関係であった組織も、今や安全保障領域を管轄する組織と考えられるようになった。また、保健省（Department of Health）傘下の医薬品及びヘルスケア製品規制庁（Medicines and Healthcare Products Regulatory Agency）も 、今や医薬や医薬製品のオンライン詐欺に対処しなくてはならない（Home Office 2010: 24）。代替エネルギー供給やスマートグリッド技術水準の発展に努めるエネルギー気候変動省

（Department of Energy and Climate Change）も、インフラ破壊やサイバー領域を介した日常的な「前払い詐欺のような貨幣利得を目的とした詐欺」（Department of Energy & Climate Change 2011: 47）といったシナリオにおける、サイバーセキュリティのリスクと脅威の調査を行っている。

現在でも国家は安全保障やリスクへの対処における最大の統率者であるものの、安全保障を取り扱うアクターは、民間企業や個人にまで広がっている。この一般市民に対するリスクへの対処の委託によって、新たな組織や慣行（もしくは別の領域では昔からある慣行）が生まれている。この最もよい例は、「戦略的コミュニケーション」運動の広がりだろう。それにより、市民の「認知度の向上」や、市民の「行動の変化」を促す。安全保障領域が個人へと拡大しただけでなく、リスク社会では個人にもリスクが及び、なおかつ個人の行動自体がリスクを生み出すためにこうした現象が起きているのである。

この個人への拡大は、人々が「より安全な（もしくはより低リスクの）」オンライン活動にたずさわれるよう、不正行為に対する一般人の脆弱性を軽減させるキャンペーンを引き起こした。NCSP が実施した主なキャンペーンには（1）オンラインでの安全の確保（Get Safe Online）、（2）シンク・U・ノウ（Think U Know）、（3）賢くクリック、安全にクリック（Click Clever, Click Safe）、（4）サイバーセキュリティ・チャレンジ（Cyber Security Challenge: CSC）の四つがある。最初の三つは、人々の行動が不正行為を引き起こす、あるいは児童ポルノに巻き込まれるリスクの軽減に関連している。

最後の CSC は、サイバーセキュリティの専門職への関心を高めるために展開された。このプログラムでは、リスクの再帰的な性質やラスムセンが述べた「ブーメラン効果」を利用している点が興味深い。サイバー領域は機会を提供するが、依存の深化は脆弱性をもたらす。これこそが、ブーメラン効果と再帰的リスクであるが、CSC は、より多くの人間がデジタル経済に関わることで、より多くの人間がサイバーリスクの対処に関わることになることを利用し、同分野の職業へ人々を引き付けようとしているのである。

サイバーセキュリティ戦略では、様々な組織に、サイバーセキュリティ固有の産業の確立や促進といった課題を与えている。そうした課題は、組織に組織間の調整業務、諮問機関設置、民間企業や学界への資金提供といった新たな対応を余儀なくさせる。そうした組織の中には、BIS に属するサイバーセキュリティ・チームだけでなく貿易投資総省も含まれおり、サイバーセキュリティ戦略において以下のように記述されている。

> 安全保障部門の貿易団体と協働し、この増大する国内の力を梃子にして、英国企業の輸出を支援する。脅威を機会へと転換し、強いサイバーセキュリティをすべての英国企業にとってポジティブなもの、そして英国の競争力とする（Cabinet Office 2009: 33）。

７．　おわりに

本稿では、英国のサイバーセキュリティに関する戦略的思考の特徴を分析した。分析を通じサイバー領域におけるリスクや脅威をめぐる言説は、情報戦争から情報保証、サイバー犯罪へ、さらに現在のサイバーセキュリティへと移行してきたことが明らかになった。過去の戦略は、領域が限定的で、敵の意図や能力によって合理化可能な脅威に着目してい

たのに対し、現在の安全保障は、リスクや不確実性によって特徴づけられる。リスク合理性への移行は、(1) リスクへの対処、(2) 未来との関与、(3) 再帰的な「ブーメラン効果」という三つの慣行をもたらした。戦略的思考における合理性の変化に従い、国家安全保障の意味も変化し、それにより新たな制度や組織、慣行が創出された。

最後に、本稿の結論から得られる三つの含意について言及しておきたい。一つ目は範囲が限定的な「脅威」と、範囲が不明確な「リスク」との間にある矛盾が、国家の限りある資源の分配を困難にすること、二つ目はリスク合理性への移行が、リスクへの対処、将来に向けた取り組み、新たなシナリオ作成のための新たな組織や慣行を創出すること、そして三つ目は、拡大する安全保障領域に新規にアクターが参加することで、ある種のパラドックスが作り出されることである。この安全保障領域の成長は、国家の一部の省庁にそれらを管理、調整しようとさせ、その結果、政策や戦略を合理化し実践するための新たな組織の創設が促されることになる。しかし、戦略と慣行を正当化するという役割の組織を単に創設しても、そうした帰結には必ずしもつながらない。実際、同じ安全保障領域の一部を担うもっと大きな組織に直面したとき、そうした新しい組織は資源も正当性も欠いているかもしれない。最終的な結果は、もっと戦略や報告書を書くことだけを目的とした政府機関がまたできるだけである。そこでの調整は、実際に達成すべきゴールではなく、一種のレトリックになってしまう。

サイバーセキュリティの問題に対処するといったような不確実な環境を理解し、それに対応しようとする組織は、ベストな慣行や組織形態の源泉として、成功と見なされている他の組織を使おうとする。このプロセスは既存研究では「制度的同型写像（institutional isomorphism)」と呼ばれるが（DiMaggio and Powell 1991)、組織同士を似たようなものにし、違いをなくさせる原因となる。

サイバーセキュリティの事例では、例えば、サイバーセキュリティに対処するための組織形態や種類、戦略、政策、慣行についてのアイデアを求めて各国が英国を見るということになる。しかし、英国でのサイバーセキュリティは、政府情報システムを守ることから、知的財産権の名を借りた企業の権利保護、さらには警察や詐欺の領域にあったことまでカバーするようになってしまっている。コンピューター・システム上でデータが保護されるようにする実際のボルトとナットを超えた一連の幅広い慣行が見られるようになってしまっている。つまり、未来のシナリオの生成、行動を導くための戦略の策定、予算の調整、広範な組織政策の調整、個人の行動を変えるためのコミュニケーション・キャンペーンなどである。警察、インテリジェンス、安全保障、そして軍の機能における区別は非常に曖昧になっている。

それゆえに、英国のようなリスク社会に基づくサイバーセキュリティ戦略は、他国にとっては有益なモデルではないかもしれない。表面的には、英国のサイバーセキュリティ戦略とそれを支えるレトリックは、戦略と慣行の正当化に加え、コントロールと調整のような事柄に焦点を絞りながら、国の官僚制度に働きかけ、その変更を促している。しかし、英国におけるサイバーセキュリティについての変化する言説と慣行を分析して分かるのは、これらの特徴の多くが、手段と目標の合理的な適用というよりは、リスク社会の自己屈折的な複雑性への対応と管理になっているということである。つまり、英国の文脈や状況においてのみ適合的であるかもしれず、他国が単純に英国の制度をまねたからといって、そ

れぞれの状況にうまく適合するかどうかは不透明である。したがって、日本がサイバーセキュリティにおける英国モデルの適用を検討する際には慎重でなくてはならない。

参考文献

[1] Allison, G. and G. F. Treverton, (eds), *Rethinking America's Security: Beyond Cold War to New World Order*, New York: W.W. Norton & Co., 1992, USA

[2] Altheide, D. L., "Ethnographic Content Analysis," *Qualitative Sociology*, Vol. 10, No. 1, pp. 65-77, 1987, USA

[3] Altheide, D. L., "Tracking Discourse and Qualitative Document Analysis," *Poetics*, Vol. 27, No. 4, pp. 287-299, 2000, USA

[4] Association of Chief Police Officer of England, Wales & Northern Ireland [ACPO], *ACPO e-Crime Strategy Version 1.0*, 2009, USA

[5] Baldwin, D. A., "The Concept of Security," *Review of International Studies*, Vol.23, No.1, pp.5-26, 1997, USA

[6] Beck, U., *Risk Society: Towards a New Modernity*, London: SAGE Publications, 1992, USA

[7] Beck, U., *World Risk Society*, Cambridge, UK: Polity Press, 1998, USA

[8] Beck, U., "The Terrorist Threat: World Risk Society Revisited," *Theory, Culture & Society*, Vol.19, No.4, pp.39-55, 2002, USA

[9] Booth, K., "Security and Emancipation," *Review of International Studies*, Vol.17 No.4, pp.313-326, 1991, USA

[10] Buzan, B., *People, States, and Fear: An Agenda for International Security in the Post-Cold War Era*, Boulder, CO: Lynne Reiner, 1991, USA.

[11] Buzan, B., *Rethinking Security after the Cold War*, *Cooperation and Conflict*, Vol.32, No.1, pp.5-28, 1997, USA

[12] Buzan, B., O. Waever, and J. De Wilde, *Security a New Framework for Analysis*, Boulder, CO: Lynne Riener, 1998, USA

[13] Cabinet Office (UK), *A National Information Assurance Strategy*, 2007, UK

[14] Cabinet Office (UK), *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, 2009, UK

[15] Cabinet Office (UK), *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, 2011, UK

[16] Campbell, D., *Writing Security: United States Foreign Policy and the Politics of Identity*, Minneapolis: University of Minnesota Press, 1992, USA

[17] Charmaz, K., *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*, New York: SAGE Publications, 2006, USA

[18] Chia, R. C. H. and R. Holt, *Strategy without Design: The Silent Efficacy of Indirect Action*, Cambridge, UK: Cambridge University Press, 2009, UK

[19] Corbin, J. and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, New York: SAGE Publications, 2007,

USA
[20] Dalziel, G. R., “Assessing the Terrorist Threat to the Food Supply: Food Defence, Threat Assessments, and the Problem of Vulnerability,” *International Journal of Food Safety, Nutrition and Public Health*, Vol.4, No.1, pp. 12-28, 2011, Switzerland
[21] Department for Business, Innovation & Skills [BIS] (UK), *Digital Britain Final Report*, 2009, UK
[22] Department of Energy & Climate Change (UK), *Smart Metering Implementation Programme*, 2011, UK
[23] DiMaggio, P. J. and W. W. Powell, “The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organization Fields,” pp. 62-82 in P. J. DiMaggio and W. W. Powell eds., *The New Institutionalism in Organizational Analysis*, Chicago: The University of Chicago Press, 1991, USA
[24] EastWest Institute, *Mobilizing for International Action*, 2011, 2011, USA
[25] Eisenberg, E. M., “Ambiguity as Strategy in Organizational Communication,” *Communication Monographs*, Vol. 51, No. 3, pp. 227-242, 1984, UK
[26] Giddens, A., *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Cambridge, UK: Polity Press, 1991, UK
[27] Glaser, B. and A. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*, New York: Aldine Transaction, 1967, USA
[28] Gray, C., *Strategy from History: Essays on Theory and Practice*, London: Routledge, 2006, UK
[29] Hart, B. H. L., *Strategy*, New York: Faber, 1967, USA
[30] HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010a, UK
[31] HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010b, UK
[32] Home Office (UK), “New Hi-Tech Crime Investigators in £25million Boost to Combat Cybercrime” [Press Release], 2000, UK, http://www.cyberrights.org/ documents/ hi-tech.htm (2011/9/25 最終アクセス)
[33] Home Office (UK), *Cyber Crime Strategy*, 2010, UK
[34] House of Lords (UK), *Personal Internet Security Report 2006-7*, 2007, UK
[35] Intelligence & Security Committee, *Annual Report 1997-1998*, 1998, UK
[36] Intelligence & Security Committee, *Annual Report 2009-2010*, 2010, UK
[37] Intelligence & Security Committee, *Annual Report 2010-2011*, 2011 UK
[38] Johnston, C., “Prepare for Infowar,” *The Guardian* (London) May 30, 1996, UK
[39] Katzenstein, P.J. (ed.), *The Culture of National Security: Norms and Identity in World Politics*, New York: Columbia University Press, 1996, USA
[40] Kelly, T., “Combating Cyber Attacks,” *Defence News*, 2011, UK
[41] Libicki, M. C., *What is Information Warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University,

1995, USA
[42] Malle, B. F., L. J. Moses, and D. A. Baldwin, *Intentions and Intentionality: Foundations of Social Cognition*, Cambridge, MA: MIT Press, 2004, USA
[43] Mathews, J.T, "Redefining Security," *Foreign Affairs*, Vol.68, No.2, pp.162-177, 1989, USA
[44] Merton, R. K., "The Unanticipated Consequences of Purposive Social Action," *American Sociological Review*, Vol.1, No.6, pp.894-904, 1936, USA
[45] National Criminal Intelligence Service (UK), *Project Trawler: Crime on the Information Highways*, 1999, UK
[46] Rasmussen, M. V., *The Risk Society at War: Terror Technology and Strategy in the Twenty-First Century*, Cambridge, UK: Cambridge University Press, 2006, UK
[47] Sommer, P., "The Future for the Policing of Cybercrime," *Computer Fraud & Security*, Vol. 2004, No. 1, pp. 8-12, 2004, Netherlands
[48] Stech, F. J., *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of Naval Research, 1979, USA
[49] Stech, F. J., and K. C. Hoffman, *Methods of Estimating Strategic Intentions*, Office of Naval Research, 1982, USA
[50] Tenner, E. "Batten Down the Hatches for Infowar," *The Guardian* (London), February 13, 1997, UK
[51] Zerubavel, E., *The Fine Line: Making Distinctions in Everyday Life*, Chicago: University of Chicago Press, 1991, USA