The Journal of Strategic Studies

戦略研究 18

2016

戦略研究学会

特集

戦略と文化

《巻頭言》

戦略的あいまい性(strategic ambiguity)」について　伊藤　剛

戦略と文化
——マクロとミクロの比較の視点から——　寺本 義也

東アジア各国の軍事戦略と政治文化　村井 友秀

アジア・新興国の文化に対応できるグローバル・サービス戦略とビジネス展開　北川 浩伸

サイバー攻撃を行うのは誰か　トマス・リッド　ベン・ブキャナン（土屋大洋訳）

書評論文

中国、北朝鮮、ロシアのサイバー攻撃　——日米欧の対応——　河野 桂子

伊東寛著『「第5の戦場」サイバー戦の脅威』
土屋大洋著『サイバー・テロ　日米 vs. 中国』

書評

佐野秀太郎著『民間軍事警備会社の戦略的意義—米軍が追求する21世紀型の軍隊』　小野 圭司

エドワード・ルトワック著『自滅する中国—なぜ世界帝国になれないのか』　井上 一郎

海外論文翻訳

サイバー攻撃を行うのは誰か*1

トマス・リッド（Thomas Rid）
ベン・ブキャナン（Ben Buchanan）
土屋大洋訳

はじめに

アトリビューションとは罪と罰と同じくらい古い問題に答えるアートである。つまり、誰がやったのかということである。アトリビューションをうまくできるかどうかは、国際的・国内的な強制と抑止のほとんどすべての形の中心にある。うまくできなければ、国家の信用、効率性、そして究極的には自由とセキュリティを損なうことになる。

生死の分かれ目はアトリビューションにある。2013年8月のダマスカス郊外のグータ（Ghouta）における化学兵器使用、2014年夏のウクライナのドネツィク（Donetsk）州近郊でのマレーシア航空17便の墜落、2014年のガザ戦争のきっかけとなった6月のグーシュ・エツヨン（Gush Etzion）での3人のイスラエル少年の誘拐――これらの出来事はすべて、誰も犯行声明をすぐに出さなかった点で共通しており、それに伴う必然的に高度な政治決定がなされなければならない一方で、犯罪者たちのアイデンティティをめぐって激しい議論があった。アトリビューション問題が劇的にそのプロフィールをあらわにしたのはここ数年のことではない。1914年6月28日のオーストリアのフランツ・フェルディナンド（Archduke Franz Ferdinand）皇太子の暗殺が同様の謎を提供している。暗殺者のガヴリロ・プリンツィプ（Gavrilo Princip）とは何者なのか。そして彼はセルビアのエージェントだったのか。

アトリビューションは少しずつほどけていく。こうした国際的なインシデントは、潜在的に巨大な利害関係が現れてきていることを浮き彫りにしている。しかし、それらは、アトリビューションについてのシステマティックな議論には例外的過ぎるし、わかりにくすぎる。もっと秩序だっていて確立さ

れた例証から始めればもっと生産的だろう。法執行においては、重犯罪人の特定は緊急電話への通報から始まる。その次に捜査官たちが来る。警察官たちは現場を保全し、目撃者にインタビューをするだろう。フォレンジック［犯罪科学］の専門家が特定の異変を見つけ、分析しようとするだろう。例えば、犯罪現場で見つかった指紋付きの銃が被害者の体内で見つかった弾丸と一致するかである。すべてがうまく行けば、そうした証拠は事件として整理され、陪審員に提示され、そこでアトリビューションの最終的な問題が確定される。しばしばドラマを伴うものだとしても、それは方法論的で秩序だっており、制度的なアプローチである。

このシナリオは単純だが有益である。それは少なくとも三つの一般的かつなじみのある特徴を明らかにする。アトリビューションは、ほとんどいつも、一人の人間が扱うには広すぎ、複雑すぎるということである。アトリビューションは、専門分野とその下位専門分野に広がる分業を必要とする。そして、アトリビューションは異なるレベルで徐々に進むものであり、証拠の迅速な技術的収集、追跡捜査と分析、訴訟手続き、判決権限を持つ人々の前で競合する証拠に対して自分の主張の正しさを説明することが続く。法執行のシナリオは、学術文献と大衆文化の両方で広範に研究されている。サイバー攻撃を誰かに帰するということは、それよりも単純ということはなく、あまりなじみのない場所でもある。

サイバーセキュリティにおいては、アトリビューション論議は驚くほどゆっくりと展開している＊2。現在のところ三つの共通の仮定がデジタル・アトリビューションに関する議論を支配している。最初の仮定は、アトリビューションは、インターネットの根本的な技術的アーキテクチャ＊3と地理＊4によって作られた新しいフィールドでの最も解決困難な問題＊5の一つであるというものである。その結果、インターネットの技術的なデザインのやり直しだけが、問題を完全に解決し得るということになる＊6。同様のポジションは法的な論議＊7においても優勢である。第二の仮定は、アトリビューションに関する二元論的な見方である。どんなケースに関しても問題は解決し得るか＊8し得ないか＊9のどちらかであるというものである。アトリビューションが犯罪者にたどり着くか、あるいはあるところでなりすましの IP アドレスや不明瞭なログ・ファイル、あるいは効力のない痕跡＊10にたどり着いて終わりになるかだという。第三の仮定は、アトリビューションの証拠は容易に包括的なものであり、主たる挑戦は証拠自体を見つけられるかという

点であり、分析や証拠固め、提示ではないというものである＊11。こうした見方は共通のものであり、直感で理解できるものであり、間違ってはいない。しかし、それらは限定的であり不十分でもある。アトリビューションの現実は、過去10年において大幅に進化してきた。サイバー事案の実際のアトリビューションは、これまでの文献が認めてきたよりももっと微妙なものであり、もっと平凡であり、もっと政治的なものである＊12。

本論文は、こうした固定化された立場を越えてアトリビューションに関する議論を前進させようとするものである。本論文は三つの問題のセットを提示する。我々は、一次的な問題の考察から始める。つまり、アトリビューションが何よりもまず技術的な問題ではないとしたら、それはいったい何なのか。第二の問題がそれに続く。アトリビューションが二元的なものではなく、程度の問題だとしたら、通常のアトリビューションとはどのようなものであり、高品質なアトリビューションと低品質なアトリビューションではどのように違うのか。そして第三に、証拠が目立たないものであり、曖昧なものだとしたら、それはどのように整理され、分析されるべきなのか。全体として、アトリビューションはどのように管理され、第三者に伝えられるべきなのか。

本論文は、アトリビューションとはどのようなものなのかを論じる。ある攻撃を特定の攻撃者に帰するということは、いくつかのレベルで不確実性を最小化することである。技術的なレベルでは、アトリビューションはサイエンスであるとともにアートでもある。正しいアトリビューションのためのレシピは一つではなく、方法論もフローチャートもチェックリストも一つではない。正しい手がかりを見つけるには、訓練された方法で詳細な問題のセットに焦点を絞ることが必要になるが、技術的に熟練したオペレーターの直感もまた必要である。それは、技能に関して確立された［フランス語の］軍事用語を使うならば、「展望（coup d'oeil）」を要するということである＊13。作戦術のレベルでは、アトリビューションは微妙な差異を持つプロセスであり、単純な問題ではない。アトリビューションのプロセスは二元的なものではなく、一様ではない程度で測られ、白黒ではなく、イエス・ノーでもなく、段階的に現れる。結果的に、それはチーム・スポーツでもある。アトリビューションの成功は一人が提供できる技能やリソース以上のものを要する。アウトカムを最適化するには、注意深い管理と組織的なプロセスを要する。戦略的なレベルでは、アトリビューションは政治的に何が問われているかの関数である。政治的な利害関係は広範な要因によって決められるが、最も重要

なのは受けた被害である。被害は、金銭的、物理的、あるいは評判に関わるものであり得る。上から見れば、アトリビューションは、部分的には内部のプロセスのリソース配分と指導の問題であり、最終的な評価と決定における参加の問題であり、第三者と大衆に向けてアウトカムを伝えることでもある。

我々の議論を理解し、アトリビューションの理想的な構成を図示するために、我々はQモデルを導入する（図１参照）＊14。戦術的には、このモデルはアナリストたちが重要問題を最大限問いかけるのを支援し、批判的思考法を促し、調査を文脈に整えることに役立つ＊15。作戦術的には、技術的な情報と非技術的な情報を競合する仮説に統合するのにこのモデルは役立つ。それは異なるレベルでもっと挑戦的な問題を提起することを含み、そうした問題とは広範な分析的・作戦術的な問題だけでなく、きめの細かい詳細な技術的な問題も含む。戦略的にはこのモデルは、適切かつ評価可能な言葉で対外的なプレゼンテーションのためにアトリビューション・プロセスのエッセンスを精製・抽出するのに役立つ。この言語が、重大な帰結を伴う政治的な判断を行う人々に伝えることにもなるかもしれない。

図1　本論文および詳細なグラフの構成（付録を参照）

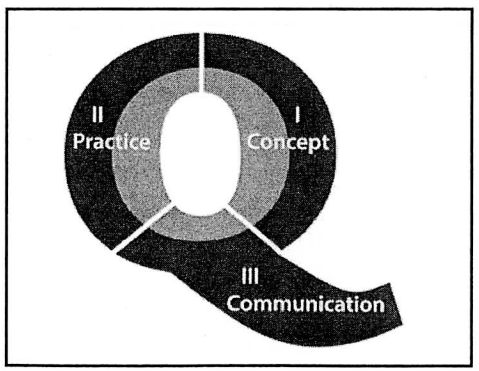


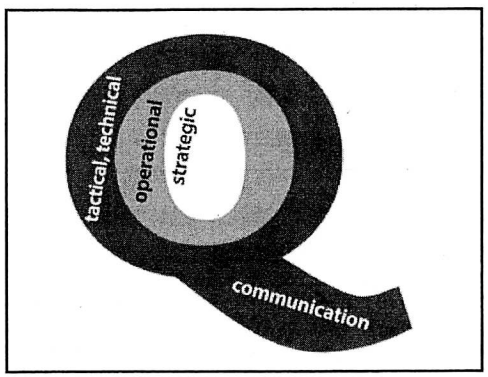
図１は、本論文がこれからどのように進行し、議論がどのように示され、付録で提供されているもっと詳細なモデルの図解をどう読むかを示している。第一部は概念である。モデルを一般的な用語で議論し、いくつかの重要な区別とダイナミクスを用いることによってプロセスとしてのアトリビューションを導入する。第二部は実証である。近年の事例を通じてアトリビューションのプロセスに沿って様々なステップを明らかにする。第三部は、Qの主要部から突き出ているフックの部分について考察する。それはアトリビューション

ョンの可能性と限界について伝え、発見を行動に翻訳するという挑戦である。結論は実績を評価し、いくつかの固定化された問題のある見解を再評価し、サイバー攻撃のアトリビューションの限界を検討する。

Ⅰ　概　念

本研究は、フォレンジック捜査官からインテリジェンス分析者、国家安全保障担当者、高位の行政官、政治指導者、サイバーセキュリティとネットワーク侵入について書いているジャーナリストや研究者たちにまで至るあらゆるレベルでのアトリビューションのプロセスを極めるための概念的・実践的地図として設計されている。

図2　分析の三つのレイヤー



アトリビューション・プロセスのそれぞれのレベルは、個別の分析的な挑戦を示し、特定のインプット・データや特定の専門知識に依拠し、成功するアトリビューションの特定の側面を明らかにする（図２参照）。それぞれのレベルの分析は［自学できるものではなく］他者によって知識を与えられ、鍛えられる必要がある。アトリビューション・プロセスは一般的には始まりと終わりがあるが、仮説が新しい詳細情報に直面し、新しい詳細情報が代わりに新しい仮説を生み出すにつれ、サイクルが特定の順次的・時系列的な秩序に従うわけでは必ずしもない。それにも関わらず、それらのレイヤーは、相互に関係するとしても、個別に分析される別々のタスクを表している。普通は、いわゆる「セキュリティ侵害のインディケーター」がアトリビューション・プロセスを開始させることになる。そうしたインディケーターは特定

の技術的な疑問を提起する。もっと事実が集められるにつれて、さらに質問が続くのが普通である。アトリビューション・プロセスが作戦術ないし戦略的なレベルで始まることもあるかもしれない。時にはインシデントの「第一発見者」が技術的なレベルよりも上にいる場合もある。フォレンジックではないインテリジェンスのソースや広範な地政学的文脈に導かれたり、時には直感によって導かれたりすることによって、悪意のある活動の可能性が、技術的なインディケーターが示すより先に、さらにはそれが始まる前にでも見つかるかもしれない。戦略的・作戦術的なレイヤーが技術的な分析に情報を提供したり、あるいは逆になったりするが、アトリビューションはどちらでも良い。

アトリビューションには広範なスキルが求められる。サイバー脅威は高度に複雑なレベルに達している。そうした脅威を実行したり、属性分析を通じてそれらのアーキテクチャを暴いたりするには、洗練された分業が必要である。制御エンジニアたちが産業プラントに対する標的型のペイロード［データの本体］の特殊なデザインに焦点を絞って調査をするのと平行して、アンチウイルス研究者たちのチームは、特定のマルウェアのインストール・メカニズムのリバース・エンジニアリングに多くの時間とエネルギーを投じるかもしれない。スタックスネット（Stuxnet）［という2010年に見つかったマルウェア］は非常に複雑だったので、複数の企業が、伝搬メカニズム、指揮統制の組織、産業制御システムを狙うペイロードなど、異なる側面の分析に傾注した＊16。軍事的な文脈と同じく、戦術活動の全部の範囲が作戦術的な考察の下に置かれているが、それが不可欠になっている。別々の側面の分析は大きく異なるスキルを要するが、この専門分化は軍事的な作戦でも犯罪捜査においても確固として確立された原則である。反乱軍のネットワークの資金源や爆発物のサプライチェーンの分析に簡易爆発物処理部隊を当てる司令官などいない。F-16 戦闘機のパイロットが自分で標的を選ぶことはない。ミサイルのエンジニアは核戦略を扱わない。サイバー攻撃の文脈においては、そうした要素的な期待が、アトリビューションの仕事に従事する小さな専門家コミュニティの外でいまだ形成されていない。

アトリビューション・プロセスの総合的な目標は、被った被害や潜在的な被害にしばしば依拠している。多くのインシデントが発生しているのに十分な捜査官がいない世界では、生じた被害や危機が迫っている被害の総量が有害な出来事自体をアトリビュートすることに投じられるリソースをしばしば

決定づける。侵害が明白な被害を引き起こさなかった場合には、企業や政府でさえも無視することに決めるかもしれないし、単に不十分な操作をしたり、防衛を改善したりするだけで、一見して取るに足らない侵害の出自に対する広範な捜査を始めることにはならないかもしれない。認知された被害の欠如は、アトリビューション・プロセスを省略することになり得る。ある程度これは避けられない。

戦術的な目標は、主として技術的な側面、つまり、How においてインシデントを理解することである。作戦術的な目標は、攻撃者の高度なアーキテクチャと攻撃者のプロフィール、つまり、What を理解することである。戦略的な目標は、誰が攻撃に責任を負っているのか、攻撃者の動機、重要性、適切な対応、つまり Who と Why を理解することである。最後に、コミュニケーションもまたそれ自身が目標である。労働集約的なフォレンジック捜査のアウトカムを伝えることは、アトリビューション・プロセスの一部であり、低い優先順位で扱うべきではない。実際、アトリビューションを公にするということは重大な効果を持つ。攻撃者は作戦を中止するか。戦術を変えるかもしれない。主張に対して公に反応し、被害者の広範な対応を方向付けることにもなる。

細部が重要である。しかし、細部にわたる情報は量が膨大になる。情報は技術レイヤーから作戦術的・戦略的なレイヤーへと流れるにつれ、合成されなければならない。そうなって初めて情報は理解可能であり有用である。技術的な分析は、インシデントによっては、特定の侵入についての詳細情報の膨大な量を生み出すことになる。これはしばしば、使われた特定の手段、ペイロードのメカニズム、指揮統制インフラ、狙われたデータ、リバース・エンジニアリングの分析、影響を受けたネットワークからの生データを含む。収集された技術上の詳細情報のいくらか、あるいはおそらくほとんどは、限られた重要性しか持たない。いくつかの戦術的に重要な詳細情報は、作戦術的・戦略的なレベルでは重要性を失うかもしれず、それは地政学的な文脈の詳細情報がフォレンジック捜査官にとって限定的な関心を持たないのと同じである。このプロセスは詳細情報からの意味を抽出する。適切な統合の欠如、技術的なフォレンジックの不自然な結果の高集積は、作戦術的・戦略的な質問がより確実性を持って応えられるということを意味するわけではない。詳細情報は、より大きなアトリビューション・プロセスと代替可能ではない。

したがって、確実性は不同ではない。戦術的なレイヤーから作戦術的・戦

略的なレイヤーへと情報が流れるに従い、疑問はより薄く、広範になっていく。そこで、アトリビューションの不確実性は、分析が技術的なレイヤーから政治的なレイヤーへと移行するにつれて増大することが多い。侵入メカニズムが何かというのは、フォレンジック上の不自然な結果に基づいて答えられる疑問である。動機が何かというのは、仮説の設定を要し、その仮説の検証を要する問いかけになる＊17。技術的なフォレンジック上の疑問は、狭く絞られており、確実に答えることが可能である。競合する作戦術上の疑問は、労働集約的なフォレンジック上の評価によって情報を与えられるかもしれないが、入手可能な技術的・非技術的な証拠によって完全に裏打ちされるものではない。戦略的なレベルにおいての結論は、フォレンジック上の不自然な結果からはさらに除外される可能性があり、多くの仮定や判断を含むものかもしれない＊18。上級の意思決定者を教育することがこの問題を管理する際には不可欠である。

アパチャー（aperture：カメラのレンズの口径）の問題がここで出てくる。アトリビューション・プロセスにおける最も難しい要素の一つは、多くのインテリジェンス・コミュニティの関係者がアパチャーと呼ぶものである。それは、特定の捜査に影響する可能性のあるソースの範囲のことであり、光がカメラに入ってくる可変のアパチャーと似たものである。アトリビューションの質は、有用なインテリジェンス・ソースの数が増大するにつれ、上昇することが多い。さらに、広いアパチャーの重要性は、アトリビューション・プロセスのレベルにつれて上昇する。純粋に技術的なレベルで特定のインシデントについてのアパチャーを広げることは可能だが、狭い制約の中でのみである。侵入によって生成されたデジタルのフォレンジックの証拠は、定義上、それが提供する文脈に限定されている。不正コードが動機を明らかにすることはほとんどない。作戦術のレベル、特に戦略のレベルでは、他のインテリジェンスのソース、例えば電話の会話や作戦を命じたり組織したりした者たちの間の電子メールの傍受が大きな絵を明らかにするかもしれない。オールソース・インテリジェンスと広いアパチャーの重要性は、なぜ高度な能力を持つインテリジェンス機関を持つ国が、高度な能力を持つ民間主体よりも、アトリビューション・プロセスを極める体制になっているかを説明する最も強力な理由の一つである。

歴史上、最初の大規模な国家対国家のコンピュータ・ネットワーク侵入事例であるムーンライト・メーズ（MOONLIGHT MAZE）は、オールソース

・インテリジェンスと広いアパチャーの価値を示している。この侵入は1998年に明らかになった＊19。外国のスパイが米国の国防総省（DoD）、エネルギー省、航空宇宙局（NASA）、海洋大気庁（NOAA）、多様な防衛企業、大学を狙った。侵入者たちはヘルメットのデザインから大気のデータに及ぶ様々な情報を盗み出した。FBIの捜査官たちは、最初、圧倒されてしまった。1999年はじめ、国防総省が捜査を支援し始めた。コンピュータ・ネットワーク防衛統合タスクフォース（JTF-CND）は、「どんな石もひっくり返さないでおかない」こととし、彼らは法執行捜査官たちによって集められたデジタル・フォレンジックの証拠から始めたが、しかし、シグナル・インテリジェンス、ヒューマン・インテリジェンス、さらには、最近通信設備が設置されたかどうかを確かめるため、疑われている特定のビルディングの航空写真を過去にさかのぼって含めることにした。実際の侵入に関するデジタル・フォレンジックの不自然な結果を超えたインテリジェンスのソースは、かなりのレベルの確実性でムーンライト・メーズによる情報漏洩がロシア政府によるものと判断することを可能にした＊20。

ネットワーク侵入のアトリビューションを判断する際、個人が重要になる。組織内部の個人に侵入を帰する証拠が精製される場合、アトリビューションはよりいっそう強くなるだろう。これは多くの国際的なインシデント、特に軍事的なインシデントと完全な対照をなす。多くの兵器システムと能力は［各国軍を識別する］マークが付けられており、兵士は軍服を着る。そして、インシデントの地理的な場所はしばしば侵入の裏にある組織のアイデンティティを指し示すことになる。特定の軍事的な標的、例えばシリアの実験的な核施設は、空から攻撃を受けるかもしれない。シリア、あるいは第三国は、地理的な文脈や航空機のタイプ、飛行経路を通じて奇襲攻撃中の F-15 戦闘機をイスラエル空軍のものと識別できるだろう。パイロット個人を識別せずにすべてできる。軍事的な組織は個人や小さな部隊を最初に識別することなしに識別可能であり、これはサイバー作戦と完全に異なる点である。

アトリビューションの究極的な目標は、組織や政府を特定することにあり、個人ではない。しかし、マークや制服、地理の代わりに、個人のオペレーターは、悪意のある不自然な結果と組織の間の強力なリンクになり得る。最も有力な例の一つは、2014年6月9日に公表されたクラウドストライクのパター・パンダ報告書である。同社の英国在住の研究者の一人であるナサニエル・ハートレー（Nathaniel Hartley）は、ある悪意のあるアクターが組織的

な侵害行為において「cpyy」というハンドルネームを使っていることを最初に特定した。次のステップは「cpyy」を実際の人間に紐付けることである。ハートレーは、登録データを用いてそのハンドルネームと実在の人物チェン・ピン（Chen Ping）の関連を突きとめた。今や、チェン、または「cpyy」は、組織につなげられなければならなくなった。ハートレーは、ブログや［グーグルの写真サービスである］ピカサの写真アルバムを含む様々なソースから個人を特定する情報を暴き出した。「オフィス」と名付けられたフォルダに入っていた写真は、チェン、つまり「cpyy」を上海のビルに明らかに結びつけた。それは、軍帽やビル、装備、そしてチェンの写真を含む写真の中の様々な詳細な情報によって可能になった。こうした写真を手がかりに、ハートレーはその場所を北緯31度17分17.02秒、東経121度27分14.51秒にピンポイントで特定し、それが上海の閘北（Zhabei）地区の中心であるとした。その住所は、中国人民解放軍の総参謀部第3部第12局61486部隊の本部を示していた＊21。ハートレーの証拠は複数のソースを組み合わせており、説得的であった＊22。他の事例としては、マンディアントの APT1 報告書と、より限定的な意味では、例外的ともいえる司法省の訴追措置がある＊23。これらのすべての報告書は、オンラインのペルソナを通じて個人と組織の間のリンクを作っている。そのような個人的なリンクは、それだけでは高品質のアトリビューションには不十分かもしれない。しかし、組織を信頼に足る形で特定するには、最初は個人レベルにズームダウンすることが必要であり、そして、組織ないし部隊レベルにズームバックすることになる。このダイナミクスは、入手可能なアパチャーに依存している。もし個人と組織の間のリンクが他の情報源からのインディケーターと合致するなら、証拠はケースをかなり強くすることができる。

パーセプションもまた重要である。予想、予断、先入観、そして心理的・政治的なバイアスはアトリビューションに影響する可能性がある。その原動力は内的および外的な側面を持っている。内的には、分析者や管理者たちは、すべてのレベルにおいて、期待される知見を生み出し、特定の光で証拠を解釈したくなる可能性がある。組織的な原動力は、内部の報告書が上げられるにつれてこの問題を増幅する可能性がある。「政策的な前提がパーセプションを構成し、管理的な仕事量が内省を制約する」と1978年のインテリジェンスの失敗に関する著名な研究は述べている＊24。ある事例がこの点を描き出しているといえるかもしれない。サウジ政府は、「正義の剣（Cutting

Sword of Justice)」、つまりは少数のサウジ在住のシーア派活動家たちで構成されており、2012年のサウジ・アラムコに対するシャムーン（Shamoon）攻撃をやったと主張しているグループを発見できたはずである。スンニ派が多数派を占める国におけるシーア派活動家に対する潜在的な偏見から、サウジの捜査官たちは、そのグループがイランの権威者によって命じられていると想定したい誘惑に駆られていた。入手可能な証拠はシーア派のバックグランドを持つサウジ市民をイランのテヘランに結びつけることを完全には支持していなかった［シャムーン攻撃はイランではなく米国のインテリジェンス機関が関与したというのが通説］にもかかわらずである。内的なパーセプションのバイアスが大きくなるほど、高く付く間違いのリスクもまた大きくなる。

II　実　証

アトリビューションの質は、正しい質問をするかということの関数である。モデルのそれぞれのレイヤーは、そのレベルにおけるプロセスを駆動する特定の問いかけのセットを持っている。一つのレイヤーからの疑問に対する答えは、次のレイヤーにおけるスタート地点に情報を提供することになる。チームが全体のプロセスをより良く見渡すことができるほど、アトリビューションの質は上昇する。このプロセスはダイナミックであり非線形である。それぞれのケースは異なっており、捜査に対する硬直的なフローモデルや線形の「チェックリスト」のアプローチは問題が多い＊25。以下の段落では、このプロセスをレイヤーごとに論じる。戦術＝技術的な考察から始め、ゆっくりと戦略的考察へと上がっていく。それぞれの側面で可能ならば実証的な証拠に短く言及して明らかにしていく＊26。

技術的なレイヤーはしばしば捜査の出発点となる。それは広範であり深遠でもある。ここはスタッフに大きな挑戦を課することになる。分析者たちは、コンピュータ・コード、ネットワーク活動、言語、その他についての質問に答えるべく、効率的でチーム重視の方法で働くことを期待される。多くのケースにおける技術的な証拠は、アトリビューション・プロセスの基礎をなす。この証拠を掘り出すことは必ずしも魅惑的ではないが、不可欠である。

不正侵入のインディケーター（indicators of compromise）は、捜査を始めるきっかけとなることが多い。不正侵入のインディケーターはネットワー

ク侵入や悪意のある活動についての技術的に不自然な結果のことであり、しばしば技術的な業界用語でIOCと略される。そうしたインディケーターは、広範囲にわたる自動スキャンや異常なコンピュータの振る舞いを通じて明かされることが多い。たくさんのコンピュータそれぞれに通常の深いフォレンジック的分析を実施するのは、ネットワーク管理者にとってしばしば高く付きすぎる。IOC は、追加捜査の範囲を狭めるために有用なヒューリスティック（発見的問題解決法）となっている。ある影響力のある研究は、IOCを三つの大きなカテゴリーに分けている。つまり、原子的なインディケーター、計算によるインディケーター、振る舞いインディケーターである＊27。

「原子的なインディケーター」とは、フォレンジックな価値を失うことなく構成要素に分割することができない個別のデータのピースのことである。原子的インディケーターは、それ自体で悪意のある活動を正確に示している。一般的なものは IP アドレス、電子メールアドレス、ドメインネーム、文章の小さなかけらといったものを含む。「計算によるインディケーター」は同じような個々のデータのかけらだが、それらはコンピュータによる処理の要素を含んでいる。例えば、「ハッシュ値」であり、これは、パスワードやプログラムといったインプット・データから計算される独自のシグニチュアである。ネットワークのコンピュータで動くプログラムのハッシュ値が、悪意があるものとして知られているプログラムのハッシュ値と合致するかもしれない。「振る舞いインディケーター」とは、活動とその他のインディケーターを組み合わせたもので、悪意のある活動を明らかにするとともに、いくつかのケースでは、過去に同様の行動を用いた特定の敵を示すこともある。振る舞いインディケーターは、特定のスタイルを持つソーシャル・エンジニアリングの試みの繰り返しであるかもしれない。それらはネットワークにおける足がかりを獲得するために職位の低い従業員に対して電子メールを送り、その後、ネットワークの他のコンピュータへ許可されていないリモート接続を行い、マルウェアを送りつけようとする。コンピュータ・ネットワーク防衛に留意する組織は、侵害の三つのインディケーターすべてを収集し、それらを探すためにネットワークとコンピュータを定期的にスキャンする。侵害の証拠が見つかると、もっと多くの技術的な疑問が続くことになる。その順序は、インディケーター、敵、脅威によって異なってくる。

ほとんどすべての侵入者が一つの挑戦を克服しなくてはならない。侵入口である＊28。あらゆる攻撃者は、許可されていないシステムにおいてコード

を実行する能力を獲得しなければならない。そうしたコードは、システムの脆弱性を悪用し、攻撃者にいっそうのアクセスや機能をもたらすようにする。コードを送り込む方法としては、技術的な脆弱性の悪用よりも人間の弱さにつけ込む方が一般的である。スピア・フィッシングとは、利用者にある行動をだましてとらせるようにするため、ソーシャル・エンジニアリングの手法を用いたメッセージを送り込むことである。セキュリティ会社 RSA の有名な侵害事例は、職位の低い従業員の小さなグループに送られた電子メールから始まった。「2011年の採用計画」と題された電子メールは、ジャンク・メール・フォルダから従業員の一人が取り出し、添付ファイルを開くのに十分なほど説得的であった。それは悪意のある罠が仕込まれたエクセル・ファイルで、攻撃者がシステムにアクセスできるようにするものだった＊29。そうした出来事はかなり頻繁に起きており、ターゲットが重要人物であっても同様である＊30。捜査官はそうした出来事によって得られるアトリビューションへの手がかりにどんなものがあるかを検討するため関心を向ける。技術的なデータがスピア・フィッシングに関連づけられる。例えば、電子メールの出所である。しかし、ソーシャルなデータもまたそうである。言語上のミスやターゲティングにおける洗練度などである。別の侵入方法は、リモート・アクセス・ソフトウェアに感染した USB ドライブに依拠する。これらは攻撃者自身やその協力者、あるいは汚染された USB デバイスを使うターゲット組織の不注意な従業員などによって挿入される。さらに純粋に技術的な侵入方法もある。よくある方法が水飲み場攻撃である。このアプローチは、ターゲットが訪れる可能性のあるウェブサイトをハッキングするもので、テイクアウト・レストランのサイトといった一見すると無害なところが狙われる＊31。そのため、狙われた従業員がそのサイトを訪れると、ウェブ・ブラウザーの脆弱性を通じて彼または彼女のコンピュータが破られてしまう。たくさんの侵入方法が、ネットワークのインフラストラクチャをコントロールすることによって無害なサイトへの正当なウェブ・リクエストを操作したりごまかしたりする。いわゆる「中間者攻撃（'man-in-the-middle' attack）」や、攻撃者がノードをコントロールしていないがデータを挿入できる場合には「側面者攻撃（'man-on-the-side' attack）」が使われる＊32。

ターゲットの選び方は、侵害のタイプや侵入者のタイプに光を当てることができる。クレジットカード情報とその他の簡単に換金できるターゲットは組織犯罪者を指し示す。製品デザインを求めるのは、経済的なスパイ活動に

従事している国々における競合会社に範囲を絞ることになる。政治的・軍事的な戦略の詳細を求めるのは、インテリジェンス機関である。技術的なレイヤーは、作戦術のレイヤーでの作業想定に情報を与えるようなターゲット選びに関連する特定の不自然な結果提供することができる。例えば、侵入されたネットワークにおけるコンピュータ間の侵入者の動きを見ることによって、攻撃者が何を求めているのか捜査官たちはひらめきを得ることができるかもしれない。攻撃者が使った特定のコマンドを再構成することによって、捜査官たちは感染したマシンのメモリーから攻撃者が何か特定のものを探していたのか、あるいは広範に価値あるものを探そうとしていたのかを知ることができるかもしれない。しばしば、コードもまた検索用語を含んでいる場合がある。2014年に明らかにされたウロボロス（Ouroboros）という作戦では、「NATO」や「EU エネルギー対話」といった検索語が含まれていた＊33。

ターゲットの分析はまた攻撃者の組織的な構成を明らかにするのに役立つこともある。攻撃者が持ち込もうとするリソースは、攻撃者がターゲットをどれだけ高く評価しているかを示すインディケーターである。もしある攻撃が必要とされる以上のリソースを使っているなら、例えば低レベルのスパイ活動に洗練されたルートキット［不正侵入した後に使用するソフトウェアの一種］を使っているとすれば、ターゲット選びに効率性を重視するグループの仕業とは考えにくいという示唆になる。同様のインディケーターは冗長なターゲット選びである。ある攻撃者たちは、ある侵入の試みが成功した後でも同じターゲットに同じ手法を何度も使う。そうした努力の冗長性は、おそらく混乱したタスク構成を持つ大きな組織を攻撃者たちが代表しているというインディケーターかもしれない。たくさんのターゲットに［すでに対応済みという目印として］「スプレーをかける」のは、攻撃者側で突破者と細工者の分業があることを示しているのかもしれない＊34。

インフラストラクチャは、ほとんどの悪意のある活動に必要とされている。サービス拒否攻撃の場合は、意味のない情報でターゲットのコンピュータの処理能力をあふれさせることに依拠しており、インフラストラクチャが実際に攻撃を実行する。その他の悪意のある活動においては、インフラストラクチャはしばしば起点として使われたり、乗っ取られたマシンのコードに指示を送る（技術的な業界用語ではコマンド・アンド・コントロール）ために使われたりする。効率性を最大化し、ロジスティックのコストを最小化するため、悪意ある侵入は、ある侵害行為から次の侵害行為へと物理的なデジタル

・インフラストラクチャをしばしば再利用するだろう。それゆえ、それはアトリビューション・プロセスにおいて価値ある手がかりになり、異なる作戦の間をつないだり、潜在的には異なるグループの間をつないだりするリンクを形成することになる。5人の中国人民解放軍将校を米国が訴追した事案では、検察官は、アトリビューション・プロセスの一環としてオペレーターたちによるドメイン・ネーム・サーバーの利用に言及した＊35。攻撃者は様々なレベルのインフラストラクチャの支配権を獲得することができる。例えば、コンピュータは正当な所有者が知らないうちに「ボット」としてハイジャックすることができる。サーバーはサービス事業者から正当にレンタルすることができ、悪意のある目的に使うことができる。あるいは、攻撃者自らインフラストラクチャを所有し物理的に保持することもできる。攻撃者が権限を有するインフラストラクチャへのリンクのタイプが分かれば、それに続く疑問がたくさんの形で決まることになる。例えば、バーチャル・マシンとサーバーのようなレンタルのインフラストラクチャでは、サービス事業者を通じてより多くの登録情報やログ情報がアクセス可能になるかもしれない。敵が所有し保持するインフラストラクチャは、敵の物理的な位置への手がかりとなり得る。いずれの場合も、敵のインフラストラクチャをモニターすることは、分析の新しい手がかりを開き、将来の作戦を阻止するのに役立つ。結果として狡猾なアクターは、自分たちのインフラストラクチャをもっとうまく隠そうとするステップをとっている＊36。

モジール方式はコンピュータ・コードの最も優れた帰結の一つである。効率性のため、悪意のあるアクターたちはしばしばわかりきったことをやり直すのを避け、作戦における基本的なタスクを達成するためにソフトウェアを再利用するだろう。攻撃の一環として、頻繁にこのソフトウェアはターゲットのネットワークへ直接送り込まれ、捜査官たちによって後で分析されることになる。しばしば、そのソフトウェアは攻撃者自身のシグニチュアと顕著な特徴を有しており、侵入者や支援者のアイデンティティに関する洞察を与えることになる。大手のセキュリティ会社であるファイア・アイは、いわゆるデジタル操舵手（digital quartermasters）に関する報告書で明らかにしている。デジタル操舵手は関係する悪意のあるグループに広範に同じソフトウェアを提供する主体である＊37。こうした種類の分析はケースによりけりで、効用は様々に分かれる。モジュールの形でパッケージ化されたコードは、侵入において頻繁に共通して使われているため、攻撃者を特定する有用なイ

ンディケーターとはならなくなっている。スタックスネットやデューク一（Duqu）のマルウェアの共通のコードの場合は、非常に難解あるいは複雑なため、特定するのに非常に有用である＊38。こうした捜査では、スタックスネットの作者がデューク一も作成したと研究者たちはかなり確信することになる。なぜなら二つのマルウェアは重要なモジュールを共有し、コードは広範に入手可能ではなかったからである＊39。

侵入行為の生活パターンは、不正捜査の重要な一部である。あらゆる組織は効率性を最大化するためにスケジュールとルーティーンに依拠している。ハッキング・グループも例外ではない。タイミングとその他の活動パターンは、彼らの場所とアイデンティティへの手がかりを与えることになる。例えば、5人の人民解放軍メンバーに対する米国政府の訴追は、オペレーターたちが作業スケジュールにかなり従っていたことを示している。工作員たちは、彼らのコマンド・アンド・コントロールのインフラストラクチャをセットし、勤務時間の間だけ指示を求めるピンを打つようにしており、ランチタイムや夜、週末にはスイッチを落とすことさえしていた＊40。こうした行為は上海のビジネス・アワーと一致しており、米国政府はそこが拠点だと想定することになった。別の例では、クラウドストライクは攻撃的なキャンペーン［一連の作戦］をロシアにいる攻撃者に帰している。なぜならコンパイルの時刻、つまりソフトウェアがパッケージ化された時刻のほとんどが、ロシアの勤務時間の間に起きていたからである＊41。生活パターンはごまかすのが簡単だが、しかし、捜査官の作業想定を裏付けるために広く使われている。

マルウェアの言語のインディケーターもまたアトリビューションへの手がかりを与えてくれる。言語のインディケーターには二つの主要なカテゴリーがある。第一に、特定の事柄、例えば変数の名前やフォルダ、ファイルといったものに対して攻撃者が選ぶ言葉を明らかにすることである。第二に、一般的な設定状態を明らかにするコンピュータの不自然なインディケーターである。どちらも洗練された「フォールス・フラッグ（偽の旗）」作戦においては偽装するのが比較的簡単である。しかし、それにもかかわらず、言語分析はアトリビューション・プロセスにおける価値ある部分になっている。事例はたくさんあるが、最近のものではカスペルスキーが発見したカレト（Careto）［スペイン語で醜い顔の意］マルウェアの例がある。カレトは、スパイ活動の乗り物［であるマルウェア］に収められた二つの主要なモジュールのうちの一つにマルウェアの作者が付けた名前である。よくある通り、

作戦のコマンド・アンド・コントロール・サーバーは多くの国に散らばっており、そのほとんどはマレーシア、オーストリア、チェコ、シンガポール、米国といった非スペイン語圏の国々にあった。しかし、言語の痕跡は別の話を物語っている＊42。最初のインディケーターは、スペイン語の新聞を意味するたくさんのサブドメインであり、おそらくはスピア・フィッシングに用いられた（英国と米国の新聞もなりすまされていた）＊43。第二のインディケーターは、スペイン語の設定を持つマシンでコードが開発されたことを設定データが明らかにしていたことである。第三のインディケーターは、ロシアの研究者たちが疑ったところでは、「スペイン語ネイティブ話者ではない人たちにおいては非常にまれな」スラングが使われていたことである＊44。彼らはそのようなスラングの例を三つ出している。「顔」や「マスク」を意味する「careto」という言葉の繰り返し利用、設定ファイルに収められていた暗号鍵の名前が「Caguen1aMar」となっており、おそらくこれは Me cago en la mar の省略形で、カスペルスキーのスタッフたちはスペイン語で「f…」［英語の下品な4文字語］を示しているとしている。そして、以下のファイル・パス

c:¥Dev¥CaretoPruebas3.0¥release32¥CDllUninstall32. pdb

がスペイン語で「テスト」を意味する「pruebas」という言葉を含んでいる。

ミスはしばしば暴露的である。エラーは、侵入者が隠したかった情報を直接的に暴露する。人やファイルの名前、本当の IP アドレス、古い電子メールアドレス、コードの中の暴露コメントといったものである。二つの最近の事例が秀逸である。第一に、違法な麻薬販売を行っていることで知られているサイトであるシルク・ロード（Silk Road）のオペレーターは、彼の違法な事業のマーケティングをするウェブ投稿と、数年前に技術的なヘルプを求める投稿に同じユーザーネームを使っていた。後者の投稿には彼の本当の名前と電子メールアドレスが含まれており、捜査官たちにとっては明確な手がかりとなった＊45。第二に、ハッキング集団であるアノニマスのリーダーの一人、ヘクター・サビエル・「サブ」・モンセガー（Hector Xavier 'Sabu' Monsegur）は、FBI が不正操作していたアノニマスのチャット・システムにログインする前に匿名化サービスのトーア（Tor）にログインするのを忘れ、彼の本当の IP アドレスをさらしてしまった＊46。両名とも逮捕された。ミスは直接的に情報を明らかにしない場合でも重要な手がかりとなり得る。例えば、よく使われるコマンドにおける頻繁な打ち間違いは、素養に関する

一般的な手がかりになる。経験則として官僚的な性質の組織では、より経験を積んだオペレーターと標準化された手続きがあり、単独の活動家よりもミスが少なくなる傾向がある＊47。

皮肉なことに、ステルスもまた暴露的である。あらゆる作戦において、ステルスとスピードとの間にはトレードオフが存在し、手がかりをあらわにする。フォレンジックに対抗しようとする活動は、検知と後の捜査を回避するようデザインされたステップだが、不完全であり、時間の浪費である。アンチ・フォレンジックを攻撃者が利用すると、意図、報復に対する恐れ、洗練度といったものを明らかにしてしまう。アンチ・フォレンジック行動のいくつかはありふれており、かなり簡単で、ミッションの成功に直結している。例えば、攻撃者は、ネットワークから出て行く価値あるファイルを探すような自動化された防衛システムを邪魔するため、データを抜き出す前に暗号化するかもしれない。その他のアンチ・フォレンジック行動はもっと困難で、それほどありふれてはいない。例えば、事後の捜査を難しくするためにログ・ファイルの中のタイムスタンプを改ざんするツールを使うがもしれない。慎重さを評価することは難しい。しかし、攻撃者が痕跡を隠そうとする試みが見つかれば、非常に示唆的である。

いくつかの国では、その行政府、軍、インテリジェンス機関を法的な監査の下に置く。これは、情報収集と特に破壊作戦が、そうした活動をしばしば制約する司法府によって承認されなければならないということを意味する。こうした制約の存在は、技術的な分析からしばしば明白になることがあり、アトリビューションに情報をもたらすことがある。元［米国政府の］カウンターテロおよびサイバーセキュリティ担当官のリチャード・クラーク（Richard Clarke）は、スタックスネットが「ワシントンの弁護士たちのチームによって書かれた、あるいは統治されたような感覚を強く感じた」としている。なぜなら、ターゲットの検証手続きが巻き添え被害を最小化するように設計されているからである＊48。

アトリビューション・プロセスの作戦術のレイヤーは、多様な個別のソースからの情報を総合的に扱うように設計されている。これらのソースには、技術レイヤー、非技術分析、地政学的文脈の情報が含まれる。作戦術のレイヤーで動いている分析者たちは、インシデントを説明する競合的な仮説を作り出す。

コンピュータ・ネットワーク・エクスプロイテーションは準備を要する。

特定のネットワークに侵入するのに必要な能力の分析は、アトリビューション・プロセスにおける有用な手がかりになり得る。イランの厳重に警備された核濃縮施設へのスタックスネット攻撃は非常に労働集約的である。マルウェアのペイロードは、最高のターゲット特定情報を必要とした。例えば、モーターの回転スピードを制御するのに使われる特定の周波数変換機のドライブについての入手しにくい詳細情報、あるいはナタンズにあるイランのIR-1 遠心分離機の詳細な技術パラメーター、そうした機器の特定の設定状況において［遠心分離機同士を］共振させる入力周波数などである＊49。スタックスネットは、4〜5個という前例のない数のゼロデイ脆弱性も使っており、（産業用機械を制御するのに使われる）PLC（programmable logic controller）のための史上初めてのツールキットも示した＊50。こうした特徴は、可能性のある攻撃者の数を劇的に減らすことになった。他の準備活動としては、ターゲット偵察やペイロード・テスト能力もある。再びスタックスネットは有用な事例である。スタックスネット攻撃は、物理的な効果を得るためにシステムを制御するプログラムを改変した。これは事前のテストを必要とする＊51。テスト環境は IR-1 遠心分離機を使う必要があるだろう。そうしたマシンは高価で入手が困難である。非国家アクターはいうに及ばず、政府でもスタックスネットをテストする能力を持つところはほとんどないだろう。ましてや開発し、配備するのはきわめて困難である。これによって可能性はさらに狭まることになる。

攻撃は多様である。一つのターゲットに対する孤立したインシデントの場合もあるし、多様な犠牲者にわたる大きなキャンペーンの一環かもしれない。長期間にわたって大きな地理的な領域に広がっているかもしれない。こうした多段階のキャンペーンを持つ作戦を実施する攻撃は、しばしば APT（Advanced Persistent Threats）と呼ばれる。これらのグループはしばしば戦術、インフラストラクチャ、そして一つのオペレーションから次へと一般的なターゲット・セットを維持しており、そのため APT の概念はアトリビューション・プロセスにおける重要なヒューリスティック（発見的問題解決法）である。著名な例は APT1 あるいはコメント・クルー（Comment Crew）として知られるグループで、中国のハッカーたちで構成されていると信じられており、ソーシャル・エンジニアリングの戦術と特定のインフラストラクチャをぞんざいに繰り返し使用することで知られている＊52。もう一つの、おそらくもっと経験を積んだグループは、セキュリティ会社のシマ

ンテックによるエルダーウッド・プロジェクト（Elderwood Project）として知られる努力において追跡されている。このグループは貴重な脆弱性をあり得ないほど繰り返し使うことで知られ、ハイドラク（Hydraq）として知られる悪意のあるコードに依存していて、防衛、情報技術、非営利セクターにターゲットを絞っている＊53。どのようにして一連のまとまりを持つ出来事を APT として定義するかは手法による。範囲に関して区別をすることになる手法は、情報セキュリティ・コミュニティの中でもまちまちである。結果として、ある会社やインテリジェンス機関が、一つのキャンペーンを、別の分析者グループが考えるよりも小さい、あるいは大きいと結論づけることもあるかもしれない＊54。

多数のステージを持つ攻撃もある。異なるステージは、キャンペーンの全体像を感づかれるのを避けるため異なる犠牲者を狙っているかもしれない。いいかえれば、ある不正活動は、より大きく複雑な不正活動を可能にするための一つのステージに過ぎないかもしれない。そうした大きな攻撃の要素は、大きく枝分かれしており、かけらを元に戻すのを難しくしている。例えば、セキュリティ会社の RSA に対する2011年のハッキングはマルチステージの作戦であり、より大きな作戦の一部であった。この侵害は、RSA が販売し、政府や企業によって広く使われていた SecurID システムを侵害した。それに続くロッキード・マーチンへの侵入は、侵入口を獲得するために SecurID の侵害をテコにしたといわれている＊55。ひょっとするともっと精巧なステージ化された攻撃はデジノタール（DigiNotar）の事例である。自称イラン人ハッカーの「コモドハッカー（Comodohacker）」が最初にデジノタールに侵入した。デジノタールはオランダ政府が関係する認証機関であり、ウェブ・サーバーを認証している。彼はこの認証機関を侵害するやいなや、膨大な数の偽の証明書を発行し、グーグルやその他のサイトのふりをした。これらの認証は、30万人もの疑うことを知らないイラン人の暗号化された電子メール・トラフィックの傍受を可能にした＊56。

侵入は進化し得る。事前に準備したステージに対応しないやり方で時間をかけて発展するキャンペーンもある。こうした発展は変化する政治的・技術的現実と目的に対する手がかりを提供することになる。スタックスネットは再び特筆すべき例を提供している。遠心分離機を破壊させるマルウェアは異なる亜種となって現れた、とスタックスネットの分析に貢献した制御システムの専門家であるラルフ・ラングナー（Ralph Langner）は書いている＊57。

こうした亜種は異なる手法を用い、異なる時期にリリースされている。2010年7月に主たるマルウェアが発見された後の遡及的な分析によれば、先駆的な攻撃ツールの第一バージョンは2005年11月にすでに観察されていたことが明らかになった。最初期のバージョンは異なる伝搬メカニズムを持っており、マイクロソフトのゼロデイを持たず、後のバージョンで不使用にされたシーメンス417型 PLC に対して動くペイロードを持っていた＊58。そうした戦術のシフトは、優先順位と状況の変化を示している。

出来事の地政学的な文脈は兆候になり得る。後知恵では特定のインシデントの地政学的文脈は明らかに見えるかもしれない。例えば、2007年のエストニアにおける DDoS 攻撃の後や、2008年のジョージア（グルジア）戦争の間がそうである＊59。しかし、これらのケースはおそらく例外である。侵入の地政学的な文脈を解釈することは、特定のアクターと組織についての特定の地域、歴史、そして政治的な知識を必要とする。一つの例は、2012年夏に明らかになったレバノンの金融機関に対する標的型キャンペーンのガウス（Gauss）である＊60。観察者たちは、キャンペーンの理由はヒズボラの資金洗浄を明らかにすることだと疑った＊61。誰も犯行声明を出していない高度な狙い撃ちをする侵害では特に、地政学的な文脈が容疑者の数を大幅に狭めることになる。技術的な分析者たちはこうした分析を実施する準備ができていない。

従業員や請負業者は組織にとっての最大の強みでもあり、同時に最大のリスクでもある。2013年の［米国通信大手の］ベライゾン社の報告書は、組織にとっての最大のリスクの一つは、インサイダーの脅威と誤用であると特定した。特権的アクセスを持つ個人が関与したインシデントが１万1000件以上あったと報告している＊62。最も高く付いた攻撃の一つとして知られているサウジ・アラムコのシャムーン攻撃は、インサイダーによって可能になったと考えられている＊63。産業制御システムの意図的な破壊に成功した数少ないインシデントの中では、インサイダーが最も多い原因だった。特筆すべきケースとしては、2000年3月にオーストラリアのクイーンズランドにあるマルーチー・ウォーター・ビーチ（Maroochy Water Breach）＊64と、まだサイバー攻撃によるものとは確定していないものの、同じ年に起きたガスプロム（Gazprom）でのパイプラインのインシデントである＊65。たくさんのインサイダーによって実行された制御システムのインシデントがそれ以降起きていてもおかしくないが、そうしたインシデントは公に報告されていないか

もしれない。インサイダーが悪意のある出来事を手助けする可能性は、そうした活動が入手困難な独占的知識を要する場合には高くなり、最初から除外されるべきものでは決してない。

戦略的なレベルでは、リーダーやトップ分析者たちは、作戦術的な疑問に対する答えを集約し、意味のある結論を導き出すという課題に取り組んでいる。プロセスの戦略的な要素は、リーダーとハイレベルの分析者たちが予備分析を批判的に検討し、詳細を求め、別の説明を求めるとき、最高の状態になる。

サイバー攻撃は生まれながらに平等に作られてはいない。引き起こされる被害はネットワーク侵害の最も重要かつ際だった特徴の一つである。サイバー攻撃の被害は、物理的な暴力を伴う攻撃とは対照的に、突き止め、定量化するのがほとんどいつも難しい。被害は四つの大きなセットに分かれる。第一に、コストは直接的で即時的である。例えば、サーバーの利用可能時間が減ることで下がってしまうファイルの入手可能性、データの整合性の低下、侵入者によって使用不能にされてしまうハードウェアといったコストである。こうした種類の最も即時的なコストを伴った侵害の例は、2012年8月のサウジ・アラムコに対するシャムーン攻撃で、一気に3万台のワークステーションを不能にしてしまった*66。第二に、コストは直接的で遅発性の場合もある。スタックスネットはイランの核遠心分離機の部品にストレスをかける形で操作した。数年ではないにしても数カ月にわたってコードによって誘発される損耗キャンペーンが計画的な機械故障へとつながった*67。第三に、コストは間接的で即時的でもあり得る。例えば、評判に傷を付けることや機密性の喪失である。この例は、1億4500万人もの顧客情報が侵害された eBay への巨大侵害である*68。最後に、コストは間接的で遅発性にもなる。知的財産の喪失がその例であり、競争相手がこっそり盗んだものを活用すれば、競争関係が厳しくなるだろう。論争になっている例としては、カナダのネットワーク機器製造業者だったノーテルの崩壊である*69。一般的に、コストが間接的でより遅発的になればなるほど、それを定量化するのが難しくなる。

被害の形態は、特に作戦術のレベルで適切に文脈設定がされていれば、攻撃者の意図をあらわにする。経験則では、破壊活動は、公然とやるにしても秘密にやるにしても、直接的なコストを最大化する一方で、収集は、探知を避け、将来の収集を可能にすることが目的のため、被害者に直接的なコストを与えないようにする。もちろん、被害を被るターゲットのタイプも、意図

への手がかりを与える。異なる攻撃者は異なることを優先するからである。

意図的かつ実際の被害は二つに分かれる。第一の可能性は、被害が意図されたものであるが、実現しなかったものである。サウジ・アラムコは2012年に大きな侵害に苦しんだが、アラムコの生産設備を動かす制御システムの破壊を狙ったにもかかわらず失敗したのではないかと同社の幹部たちは疑っている。反対のシナリオは、被害が起きたものの、意図的ではなかったというものである。コンピュータ・システムは複雑であり、攻撃者たちはネットワークのトポロジーを知らないかもしれない。そこで、偵察活動をしている際に不注意で被害を引き起こしてしまうかもしれない。分析者たちは、他の分野の分析と合わせて被害の評価を文脈化しなければならない。小さな停電を引き起こすサイバー攻撃は威嚇射撃や大きな戦略的ネットワーク侵害の失敗例かもしれず、あるいは偵察活動の不注意な結果かも知れない。

侵入の動機を理解することは難しいが、きわめて重要である。相手のモチベーションと行動を知ることは、将来の侵害行為の軽減を簡単にする。そのような戦略的な分析は定義上、非技術的なものである。例えば、地政学的な文脈における作戦術的なレイヤーからの確固たる情報と分析に依拠する。こうした状況を背景に、目的の分析もまた、他国の優先順位の理解を要する。本質的に商業的か、軍事的か、あるいは経済的なものなのか。このすべてが、サイバー攻撃が何を目指しているのかを文脈化する。それは敵の将来の行動への手がかりも提供する。作戦が失敗した場合には、それがなぜ失敗し、その失敗を修正するために敵が将来何をするかを理解することが、軽減と対応のために有用である。

サイバー作戦は非常に新しいので、なんでも「最初の××」というのがめずらしくない。こうした先例を分析し、何が将来の前兆となるのかを暴こうとする試みは簡単ではない。新しい手法は1回限りのものかもしれないし、新しいトレンドの始まりかもしれない。産業制御システムのコントロールを可能にするスタックスネットの PLC ルートキットのように、新しい可能性を切り開くものもあるかもしれない。あるいは他のものは2012年秋の米国の銀行に対する DDoS 攻撃におけるハイジャックされたデータ・センターの利用のように、新しいがたいして重要でないものかもしれない。つまり、新しい技術的なステップだが、より大きな戦略的な重要性を持っていないものである*70。出来事が意味ある先例となるかどうかを判断することは、アトリビューション・プロセスと対応のヒントとなるだろう。

アトリビューション・プロセスのアウトカムの精査は大変重要である。入手可能な証拠と暫定的な結論は検証を要する。フォレンジックの専門家は、ログ・ファイルやコードの行といった形の最も具体的な証拠に一番近い。作戦術の分析者たちはその他のソースに沿ってこの仕事を進める。戦略的なレベルでは、政策立案者たちとハイレベルの分析者たちが、下位レベルによって作られた競合する仮説を全体として精査することによって、プロセスに対して最大の貢献をする。分析をストレス・テストにかけることで、薄弱な仮定、想像力の欠如、そしてグループ思考が明らかになる。追加的な詳細情報や別の説明を求めて説得し精査することになれば、プロセスについての詳細な知識が必要になる。この分析とモデルはそうした精査を可能にするように設計されている。状況の危険度が十分に高い場合には、専門のレッド・チームがプロセス全体を再度やり直したり、元のチームの作業をダブルチェックしたりするよう求められるかもしれない。ウインストン・チャーチル（Winston Churchill）がいったように、「精査することは常に正しい*71。」

Ⅲ　可能性と限界

アトリビューションを伝えることは、アトリビュートすることの一部である。複雑なシナリオにおいては、アトリビューション・プロセスのほんの一断片だけが高官や政治家たちには見えるだけだし、一般大衆にはさらに小さいかけらだけだろう。その部分を準備し管理することは、政治的なリーダーたち、技術的な専門家コミュニティ、そして一般大衆によって機関の活動がどのように認知されるかを決めることになる。多くの場合、プロセスのコミュニケーションは、他のプロセスを特徴付けることになる。インテリジェンスを公表すればソースと手法に害を及ぼすことになる。リリースの決定は難しく、注意と秘密の側に立ちすぎて役人たちは失敗するだろう。そうなる多くの理由が存在する。しかし、秘密の文化の中にどっぷりつかった人たちにとっては、おそらく直感に反するだろうが、いっそうの公開性は三つの重要な恩恵を持っている。より詳細な情報を伝えることは、信頼性を高め、アトリビューションを改善し、防衛を強固にする。

第一に、より詳細な情報をリリースすることで、メッセンジャーとメッセージの両方の信頼性を増強することになるだろう。二つの米国の事例が教訓的な対照をなしている。2012年10月11日、米国防総省は史上最も高度な攻撃

の一つについてコメントした。当時のペンタゴンの長官だったレオン・パネッタ（Leon Panetta）は、イントレピッド海上航空宇宙博物館の上でビジネス・リーダーたちに有名な演説を行った。その舞台装置は隠された強力な意味を持っていた。その博物館は、退役したエセックス級の空母で、第二次世界大戦で試された米軍艦イントレピッドであり、ニューヨーク市のハドソン川に係留されていた。

> 過去２年間、国防総省はアトリビューションの問題に対処するべくフォレンジックに多大な投資をしてきており、今やそうした投資に対するリターンを見ることになっています。潜在的な攻撃者たちは、米国とその利害を傷つける行動に責任を持つ彼らの居場所を特定し拘束する能力を米国が持っていることに気づくべきでしょう*72。

この演説において、米国の国防長官は、２カ月前に起きた「ただならぬ」インシデントに言及した。つまり、「シャムーン」と呼ばれる洗練されたウイルスにサウジアラビアの石油会社アラムコのコンピュータが感染したことである。パネッタ長官は攻撃の実施について二、三の詳細を提供したが、しかし、アトリビューションに関する証拠を明示的に提供しなかった。それから彼は、マルウェアに言及した数パラグラフ後でテヘランについて言及した。「イランもまたサイバースペースをそのアドバンテージとなるよう使うための一致した努力を行ってきた。」各国のプレスは、米国の高官がイランを名指ししたものとして広く解釈した。しかし、世界の最も洗練したシグナル・インテリジェンス組織を指揮する米国の最高位の高官は、単にヒントを出しただけで、イランとアラムコ攻撃の間の明示的なリンクを示さなかった。

20カ月後、米国政府は、明らかに異なるコミュニケーション戦略をとった。2014年5月、米国司法省は、まったくもって普通ではないステップを踏んだ。外国のインテリジェンス組織の5人の現役メンバーを訴追したのである。中国人民解放軍の61398部隊の5人で、コンピュータ詐欺と悪用、コンピュータの損傷、悪質なアイデンティティ窃盗、そして経済的なスパイ活動の疑いである。文書は並外れて詳細だった。それは、非常にめずらしく、ペンシルベニア州西部地区の六つの被害組織、抜き取られたデータの性質と価値、抜き取られたセンシティブなファイルのタイミングを並べ立てた。しかし、訴追はアトリビューションにつながる証拠の多くは示さなかった。「共謀者た

ちは犠牲者たちを研究するために飛び石を使い、スピア・フィッシングの電子メールを送り、追加的なマルウェアを貯蔵・配布し、マルウェアを管理し、そして抜き取ったデータを転送した」という言及があった*73。隠された意味は、政府がそうした特定の IP アドレス、電子メール、マルウェアのサンプル、盗まれた文書を提供できるということだが、訴追そのものはフォレンジック上の詳細情報をほとんど提供しなかった。この点では司法省の文書は、15カ月前に公開された同じ人民解放軍部隊に関するマンディアントの APT1 報告書よりも詳しくはない。それにもかかわらず、これらの詳細をリリースしたことは、政府の主張とアトリビューションに関する全体的な信頼性を強固にすることになった。

リリースを支持する第二の理由はこうである。より詳細な情報を公開することでアトリビューション自身を改善することになる。あるケースとその詳細情報が公になると、アトリビューションの質は上がることが多い。おそらく、最も印象的な例は、スタックスネットのコードに関するマルチレイヤーかつ高度に革新的な集団分析であろう。多様な会社と研究機関がそのマルウェアを分析し、作戦の異なる側面について焦点を絞った高度に詳細な報告書が広く生み出された*74。別の例は、中国のスパイ活動キャンペーンに関するよりいっそう詳細な報告書が、部分的にはセキュリティ会社間の競争に刺激されて出てきたことである*75。その結果、アトリビューションの市場は大きく成長してきた。一般に入手可能で最も有益かつ詳細なアトリビューション報告書は、政府ではなく企業によって公開されてきた。本研究で用いたほとんどすべての証拠と例は、公開された企業報告書から来ている。政府のインテリジェンス機関はアトリビューションを何十年、いや何世紀も実践してきた。しかし、彼らは相対的な鎖国の中でそうしてきており、革新を駆動するような公開の競争ではなく非公開の競争を行ってきた。この原動力の一つの帰結は特筆すべきものである。つまり、アトリビューション・プロセスは公刊することで終わりではなく、新しいステージへと移りつつある。代わりに、この新しいステージは、新しい証拠と分析を生み出し、評価とアウトリーチ・キャンペーンの両方を適応させるよう求めている。

公開性の第三の恩恵は、最も重要なものだろう。より詳細な情報を公にすれば、集団的な防衛を強固にできる。発見を伝えることは、個々のケースについてだけでなく、集団的なセキュリティを改善することにもなる。例えば、ある侵入において使われたインフラストラクチャを詳細に議論することで、

その他のネットワークの管理者たちがそうした侵入を防ぐことができる。マルウェアの新しいシグニチュアを生成することは同様に有益なものであり、その他の管理者たちがダウンロードし、自分たちの自動侵入検知システムに載せることができる。特定の恩恵がなくとも、攻撃者による新手のテクニックについての詳細な技術議論は、その他のケースの捜査官たちに有益な情報を提供する。そうしたインディケーターとより良い防衛に値段を付けて提供するのがサイバーセキュリティ会社のビジネス・モデルである。この原動力に政府がどのように対応するかは、公開かつ重要な問題である。

攻撃の公表はしばしば公表された活動そのものに影響する。予期しない公表にどのように特定の攻撃者が反応するかを研究することは、より多くのアトリビューション報告書が現れてくることによって可能になる。例えば、カスペルスキー・ラボが2014年2月10日にスペイン語の一連の侵入プログラムについての「カレト」報告書を発表した時、作戦は「1時間以内に」中止された*76。2012年5月にフレーム（Flame）報告書が出たときは、侵入者たちが作戦をシャットダウンするのにほぼ2週間を要した*77。作戦がシャットダウンされる様子は追加的なアトリビューションの手がかりを提供する。例えば、シャットダウンが作戦のセキュリティを高いレベルで維持しながらプロフェッショナルに行われるか、あるいは、作戦のシャットダウンする決定をオーソライズする巨大な官僚組織の存在を示す可能性があるほどゆっくりと行われるか。抜け目のない作戦であるデュークーが明らかにされたとき、オペレーターたちはファイルを細かく刻むことを忘れたので、ファイルは削除されていたが復元可能であり、作戦についての詳細を示すことになった*78。カスペルスキーが暴いた侵入のいくつかは最初の公開の後に消えたが、いくつかは他のものより素早く、スムーズでもあった。レッド・オクトーバー（Red October）が消え、ミニデューク（Miniduke）とアイスフォグ（Icefog）も消えた。すべて2013年である*79。後の二つの例は注目に値する。なぜならカスペルスキーの報告書は疑わしい攻撃者や国を特定しなかったからである。それにもかかわらず侵入者たちは撤退した。最も注目すべきことに、フレームの取扱者たちは、カスペルスキーの報告書が公になる2週間前の2012年5月14日に高度に精緻なコマンド・アンド・コントロールのインフラストラクチャを取り壊し始めた。それは並外れた洗練度と、おそらくは事前警告があったことを示している*80。2013年2月18日にマンディアントが APT1 報告書を発表した時、かなり知れ渡った報告書の中で暴露され

た悪意のある活動は、最初は41日間ストップし、そして暴露後、約160日間、通常より低いレベルが維持された＊81。その3月、バージニアに拠点を置くマンディアントのウェブサイトは長く続く中国からの DoS にほぼ圧倒された＊82。中国からの侵入は、技術的にはそれほど進んでいないとしても、アトリビューション報告書が作戦についてのセンシティブな詳細を明らかにした後でも、通常はかなり執拗であった＊83。

最後に、一般大衆とのコミュニケーションは、アトリビューションが段階的なものであり、絶対的なものではないことを反映しなければならない。セキュリティ会社と政府はそれゆえに、よく確立された慣習に留意すべきである。つまりは、評価可能な蓋然性を持つ言葉を使うということである。「他の職業と同じく、インテリジェンスにおける評価見積もりとは、分かっていないからこそするものである」と、インテリジェンス分析のパイオニアであるシャーマン・ケント（Sherman Kent）は1968年に書いている＊84。時代を超えるケントのフレーズでは、評価可能な言葉とは、「事実と判断のミックス」である。事実と判断のミックスは、サイバーセキュリティの文脈では特に重要である。見積もりは脆弱なやり方で慎重に表現され、それ故に批判に対して開かれている。文書が知識の限界と見積もりの性質について正直であればあるほど、全体の分析は信用を増すことになる。ケントの言葉をもう一度引用すれば、インテリジェンスの見積もりとは「知ることの次に良いこと」である＊85。

結　論

本研究は、サイバー攻撃のアトリビューションのためのシステマティックなモデルを導入し、三つの中核的な議論を述べた。第一に、アトリビューションはアートだということである。シンプルだろうが複雑だろうが、純粋に技術的なルーティーンは、アトリビューションを公式化したり、計算したり、定量化したり、あるいは完全に自動化することはできない。高品質のアトリビューションは、スキル、ツール、そして組織的な文化に依存している。良い状態のチーム、有能な個人、苦労して手に入れた経験、そしてしばしば、「何かがおかしい」という直感的で明確にはいえない感覚が求められる＊86。第二の議論は、アトリビューションは微妙な差異を持つ多レイヤーのプロセスであり、単純に解決できる・できないという問題ではないということである。このプロセスは注意深い管理、トレーニング、そしてリーダーシップを必要とする。第三の議論は、アトリビューションは政治的な状況に依存するということである。特定のインシデントの帰結が深刻であればあるほど、被害が大きければ大きいほど、政府は犯人を特定するためにより多くのリソースと政治資本を投じることになる。アトリビューションは根源的なものである。特定の攻撃に対するほとんどあらゆる対応は、法執行であろうと、外交であろうと、軍事であろうと、攻撃者をまず特定する必要がある。政府はアトリビューションをどのように行うか、そして、いつになったらアトリビューションが行動に移すのに十分なのかを決断しなければならない。

アトリビューションの実践に関する我々の分析は、サイバーセキュリティに関する議論において共通にとられているポジションのいくつかに疑問を呈することになる。その一つは、犯罪者からスパイ、妨害工作員に至る攻撃者たちが、彼らの痕跡を隠し、オンラインで匿名を保ち、アトリビューション問題の後ろに隠れることができるというものである＊87。しかし、アトリビューションは単純に可能というだけではない。それは長い間成功してきている。攻撃者たちは、匿名性のヴェールの下で深刻な害と被害をもたらしてそのまま逃げおおせると想定することはできない。アトリビューション問題は原理上解決できないとしても、原理上管理され得るものである。

第二の陳腐な見解は、インターネットが国家からパワーを奪い、弱い非国家アクターや民間の主体、そして犯罪者たちに与えているというものである。つまりは、技術が競争環境を平準化しているということである＊88。アトリビューションにおいては反対である。国家だけが最も洗練された作戦を高い確度でアトリビュートできるに十分なほどアパチャーを開かせるリソースを持っている。2013年に起きた［米国の］国家安全保障局（NSA）と［英国の］政府通信本部（GCHQ）の漏洩は、隠されていた能力を暴露しただけではない。この漏洩は、皮肉にも、それらの能力を過大評価しているという気になっていた多くのアウトサイダーの目に、これらの機関によるアトリビューションの信頼性を強めることになった。

第三の共通の仮定は、最も産業化され接続された国々が最も脆弱な国であり、遅れた国と価値のない国が優位を持っているというものである＊89。アトリビューションはまたもやこのロジックを逆にする。政府の技術的な能力が大きくなればなるほど、自由になる才能とスキルのある人材のプールが大きくなればなるほど、自身の秘密作戦を隠し、他者のそれを暴き出し、適切

に対応する国家の能力は大きくなる。

本分析が挑戦するさらにもう一つの定番議論は、インターネットは「攻撃が支配する」環境であるというものである＊90。この見解によれば、侵入者たちは防御者たちに対して構造的な優位を持っており、その優位はインターネットの技術的なアーキテクチャに根ざしているという。防御側はいつも正しくしていないといけない。攻撃側は一度だけそうすれば良い。またもやアトリビューションでは逆が真になる。侵入者たちがたった一つでもミスをすれば、防御側のフォレンジック分析は作戦を暴くための手がかりを見つけさえすれば良い。

それにもかかわらず、アトリビューションの限界をつぶさに見ておくことが不可欠である。最初の深刻な限界はリソース、特にスキルと能力に関するものである。アトリビューションの質は、利用可能なリソースの関数である。最高のフォレンジックのスキルと、複雑な作戦における組織的な経験は希少なままであり、急速に成長する国際的なサイバーセキュリティ市場でもそうである。アトリビューションのために利用可能なリソースが減れば減るほど、質は下がるだろう。第二の深刻な限界は時間である。アトリビューションの質は利用可能な時間の関数である。短い時間枠の中でうまく考えられた作戦を分析するのは、最もプロフェッショナルで最もリソースを持つチーム、企業、政府機関にとっても大きな挑戦である。深刻なケースのプレッシャーのかかる状況でハイレベルの決定がなされなければならない時、政治的な展開のスピードがアトリビューション・プロセスのスピードを上回るかもしれない。アトリビューションのための時間が少なくなるほど、質は下がるだろう。

第三の重要な限界は、敵の行動に関わる。アトリビューションの質は、敵の洗練度との関数である。すでに検証されたケースの中で公にされた最も一般的に説得力のある証拠は、オペレーターが犯したミスの帰結であるか、特定のフォレンジック手法による追求の可能性を考慮しなかった結果である。洗練された敵は、彼らが残すフォレンジック的痕跡を最小化し、分かりにくくするために、入念な作戦術的セキュリティを持っている可能性が高い。これによって複数のソースから証拠を集めなくてはならなくなり、アトリビューションを高価にしてしまう。希望の兆しは、敵が確実にミスを犯してくれるということだけになってしまう。完全なサイバー攻撃は、完全犯罪と同じく見えない。敵の洗練度が上がれば上がるほど、アトリビューションは時間がかかり、困難になるだろう。

アトリビューションはその中核的な特徴を未来にも保持しそうである。ウェブは1999年以降劇的に進化してきた。しかし、インターネットはそうではない。ネットの根幹のアーキテクチャはゆっくりとしか変化していない。したがって、アトリビューションも同じくゆっくりと変化しているが、それは進化しており、矛盾するやり方で進化している。一方では、アトリビューションは容易になりつつある。より良い侵入検知システムが、より多くのデータをいっそう速く使いながら、リアルタイムで侵入を特定できるだろう。より適応可能なネットワークが攻撃活動のコストを上げ、乱雑を取り除き、ハイプロフィールの侵害をよりうまく特定するためのリソースの制限を取り払うだろう。多くのサイバー犯罪は、友好的ではない国々の間でも法執行協力の改善を促すようになり、国家対国家のスパイ活動は隠すのが難しくなり、もっと政治的にコストのかかるものになるだろう。

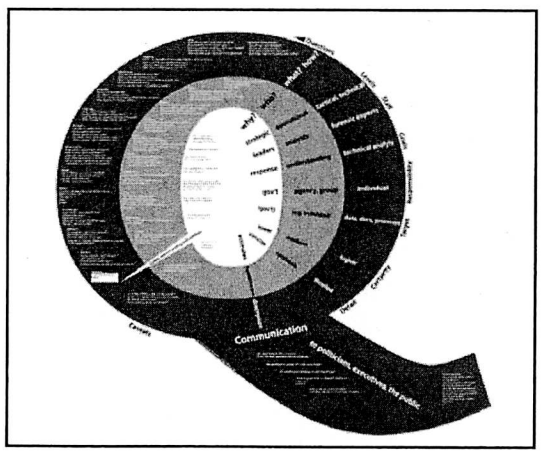
しかし、アトリビューションは難しくもなっている。攻撃者たちは公表されたミスから学ぶ。強力な暗号の利用上昇は、フォレンジック上の問題を作り出し、［データの］大量収集の有用性を制限している。誇大な宣伝と危機が微妙なコミュニケーションを阻害する可能性がある。アトリビューションの疲労が始まるかもしれない。実際、意味のある帰結がなければ、単に国家と非国家アクターが捕まる恐れを抱かなくなり、結果を無視するという緩んだ事実上の規範が現れる。皮肉にもこれは、公的に説明義務を負うリベラルな民主主義国よりも非民主的な国家がアトリビューションを恐れなくなるということを意味するだろう。そこで、議論は中心的な出発点に戻る。時間、リソース、政治的な資本を投資し、敵を打ち負かそうとすることによるアトリビューションという技術＝政治的な問題とは、いったい何なのか。

アトリビューションの中核的な限界もまた、本研究の限界を指し示すことになる。最も重要なアトリビューションの業績でも、多くの国でまだ隠されたもの、機密扱いになっているものがある。将来は、政府機関やセキュリティ会社は追加的なツールを開発し、ツールを公にするかもしれない。それによって新しいアトリビューションの観点を切り開くかもしれない。シグナル・インテリジェンスの能力には、アトリビューション・プロセスのアパチャーをすでに広げているものもある。ほとんどあるいはまったくミスをしない非常に洗練された敵でさえ、理論的には見つけられてしまう。本研究は、パブリック・ドメインにおいて入手可能になっていない開発や能力への洞察から恩恵を受けることはできなかった。それにもかかわらず、本研究はかなり

の有効期間を持つだろう。アトリビューションの中核的な変数は、1998年にムーンライト・メーズという最初の国家対国家のキャンペーンが発見されて以来、驚くほど一定のままである。

本論文は二つの目標に向けて前進することを意図していた。第一に、官僚的なアウトプットの質を上げることである。時間的な制約が、特に危機的な状況が高いときには、高品質のアトリビューションに多大なストレスをかける。それゆえ、本論文のモデルは、質を確保し、アトリビューションをより効率的かつ回復力のあるものにするよう設計されている。どのように証拠が生成されるかを理解し、より知悉した質問を投げかけ、パーセプションのバイアスを見いだし、アウトプットを精査し改善するよう、詳細なグラフが行政府と立法府の高位のリーダーたちを手助けすることを我々は希望している。同時にこのモデルは、あらゆるレベルの分析者たちが複雑な政治プロセスの大きな文脈に貢献できるようにするだろう。より幅のあるサイバーセキュリティ論議の質は、残念なくらいに低い。それは世界のベストなニュース媒体における技術のカバレッジも含む。政治学や国際関係論の学術的な文献は技術的な詳細や限界への注目から大きな恩恵を受けられるだろう。Qがこうしたスタンダードを上げることになることを我々は希望している。

図3　詳細なQモデル



付録

Qの図はアトリビューション・プロセスの地図として設計されている。技術的なバックグランドを持たない個人が低解像度でアトリビューションを鳥

の目で見られるようにしている。学者や政治家、重役たちがかなりの技術的詳細にズームインし、技術専門家たちと意味のある会話に入れるようにしてある。逆に、フォレンジック分析者たちが戦略的・政治的な文脈を理解することが可能になる。

本論文のオンライン PDF バージョンでは、上図は解像度の制約がない。別の図が http://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382 にある。

最善のフォーマットはA0版で、印刷サイズは814ミリメートル×1,189ミリメートルである。

＊1 本論文は Journal of Strategic Studies 第38号第1・2号（2015年）に掲載されたトーマス・リッド氏およびベン・ブキャナン氏による "Attributing Cyber Attacks" を著者たちの許可を得て翻訳したものである。訳文については小宮山功一朗氏と川口貴久氏の助言を得た。

＊2 初期の貢献としては、以下を参照。David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* (Alexandria, VA: Institute for Defense Analysis, 2003); Richard Clayton, "Anonymity and Traceability in Cyberspace," Technical Report, vol. 653, (Cambridge: Univ. of Cambridge Computer Laboratory, 2005); Susan Brenner, "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare," *Journal of Criminal Law & Criminology*, Vol. 97, No. 2 (2007), pp. 379-475. 初期のケース・スタディとしては、以下を参照。Clifford Stoll, *The Cuckoo's Egg* (New York: Doubleday, 1989).

＊3 例えば以下を参照。W. Earl Boebert, "A Survey of Challenges in Attribution," Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks* (Washington DC: National Academies Press, 2011), pp. 51-52. 以下も参照。Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), p. 43.

＊4 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006).

＊5「おそらく、最も難しい問題は、アトリビューションである。」P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York/Oxford: Oxford University Press, 2014, p. 73. 以下も参照。David Betz and Tim Stevens, *Cyberspace and the State, Adelphi Series* (London: IISS/Routledge, 2011), pp. 75-6.

＊6 Mike McConnell, "How to Win the Cyberwar We're Losing," Washington Post,

28 February 2010.

＊7 以下を参照。Matthew C. Waxman, "Cyber-Attacks and the Use of Force," *Yale Journal of International Law*, Vol. 36 (2011), pp. 421?59, 447; Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict & Security Law*, Vol. 17 (2013), pp. 229-44. 武力行使に必要なアトリビューションのレベルに関する議論については以下を参照。Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), pp. 33-40.

＊8 レオン・パネッタ元米国防長官は、米海軍のイントレピッド［現在は退役して洋上博物館］の艦上で、「サイバー敵対勢力の抑止をもっと複雑にする問題の解決、つまり攻撃の出元を特定するのが困難という問題において国防総省は大きな前進をしている」と述べた。Leon Panetta, "Remarks on Cybersecurity to the Business Executives for National Security, New York City," Washington DC: Department of Defense, 12 October 2012.

＊9 David D. Clark and Susan Landau, "Untangling Attribution," Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks* (Washington DC: National Academies Press, 2011). 以下も参照。Jason Healey, *A Fierce Domain* (Washington DC: The Atlantic Council, 2013), p. 265.

＊10 Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace, Planning for the Future of Cyber Attack," Washington DC: Subcommittee on Technology and Innovation, 111th Congress, 15 July 2010.

＊11 侵入分析に関する最も影響力のある論文は、証拠が自ら語るものだと想定しているようで、技術を専門としない聴衆に結果を伝えるという問題に焦点を当てていない。二つの最も影響力があり有益な貢献は、「キル・チェーン」分析と「ダイアモンド・モデル」である。以下を参照。Sergio Caltagirone, Andrew Pendergast and Christopher Betz, *The Diamond Model of Intrusion Analysis*, ADA586960 (Hanover, MD: Center for Cyber Threat Intelligence and Threat Research, 2013). Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Bethesda, MD: Lockheed Martin Corporation, 2010).

＊12 以下を参照。Boebert, "A Survey of Challenges in Attribution," pp. 41-54. より広い視野では以下を参照。Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence,'" *International Studies Perspectives*, 2014, pp. 1-21.

＊13 カール・フォン・クラウゼヴィッツは、良い司令官がストレスとあふれる情報

と時間的な制約の下で、正しい戦術的な決定を可能にする「軍事的な才」や「内なる目」を述べるために coup d'oeil を用いた。以下を参照。Carl von Clausewitz, *On War*, translated by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976), pp. 100-12.

＊14 Q は多くのことを暗に示している。第一に、アトリビューションの最も大事な点であるクエスチョンを示している。Q はまた、海軍で信号と操舵に特定の責任を持つオフィサーである操舵手につながる。「サイバー」の語源は操縦するという意味のκυβερνώ（kyvernó）である。

＊15 このモデルは意図的にフローチャートやチェックリストとしてはデザインされていない。オペレーターたちとの何度かのフォーカス・グループ・セッションを通じて、直線的な描写では彼らが取り扱う広範なケースのユニークさと不等流を反映することができないということが明らかになった。

＊16 概説には以下を参照。Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013), pp. 365-404.

＊17 例外はいくつかの犯罪形態である。金銭的な動機を特定することは、政治的な動機を検証するよりも容易である。

＊18 もっと理論的・幾何学的な訓練を受けたスタッフ、例えば数学のバックグランドを持つ者は、サイバーセキュリティ問題を形式化したがる。これは非生産的になり得る。抽象化はひらめきの欠如を隠すことになる。非常に問題のある形式化と人工的精度の例については以下を参照。Robert Axelrod and Rumen Iliev, 'Timing of Cyber Conflict," *PNAS*, No. 111/4 (28 January 2014), pp. 1298-1303. 侵入分析のためのモデル、いわゆる「ダイアモンド・モデル」、として広く使われている数学的な公式化でさえ、誇張された精度を示しているかもしれない。Caltagirone, Pendergast and Betz, *The Diamond Model of Intrusion Analysis*.

＊19 ムーンライト・メーズについては以下を参照。Adam Elkus's chapter in Healey, *A Fierce Domain*, pp. 152-63.

＊20 JTF-CND およびムーンライト・メーズのタスクフォースの元メンバーとのインタビュー。2014 年 9 月から 11 月にワシントン DC で実施。

＊21 Nathaniel Hartley, "Hat-tribution to PLA Unit 61486," CrowdStrike, 9 June 2014. 以下も参照。Putter Panda, CrowdStrike, 9 June 2014.

＊22 2014年8月6日の電子メールによる著者とのコミュニケーション。ペルソナ研究の重要性は、主要なサイバーセキュリティ企業の間でかなり論争的であり、ファイア・アイやカスペルスキーはより懐疑的である。2014年9月15日にバージニア州レストンで行ったファイア・アイのスタッフとのフォーカス・グループ・セッション、および2014年10月8日にバルセロナのカスペルスキーのスタッフと行ったフォーカス・グループ・セッションに基づく。

＊23 司法省による訴追については本論文の広範でいくらか詳細に論じる。

＊24 Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (October 1978), pp. 61-89, 61.

＊25 分析者たちは2014年の夏に実施した官民の両方における多くのフォーカス・グループ・セッションにおいて線形的な「チェックリスト」に対する疑念を繰り返し全会一致で表明した。

＊26 我々は、これらの事例を詳細に紹介する紙幅がない。それゆえに、それぞれのケースにおける最も権威のあるソースへの言及を提供する。これらのソースは時に学術的な公刊物だが、多くは企業の報告書である。

＊27 Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Bethesda, MD: Lockheed Martin Corporation 2010), p 3.

＊28 例外は、サービス拒否攻撃である。これは、基本的でしばしば意味のないデータをあふれかえらせることで特定のコンピュータ・システムの利用可能性を否定することである。

＊29 Uri Rivner, *Anatomy of an Attack*, RSA, 1 April 2011.

＊30 ウィキリークスによって公になった国務省の公電によれば、2002年以来、［米国政府の］組織はソーシャル・エンジニアリングを使ったオンライン攻撃のターゲットにされており、数百の米国政府組織やセキュリティ・クリアランスを取得した防衛企業のシステムへのアクセスをとられることになったという。Brian Grow, and Mark Hosenball, "Special report: In Cyberspy vs. Cyberspy, China has the edge," *Reuters*, 14 April 2011.

＊31 Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines," *New York Times*, 8 April 2014, A1.

＊32 例えば以下を参照。 "Is This MITM Attack to Gmail's SSL?," Google Product Forums, <http://bitly.com/alibo-mitm+>. また、以下も参照。Seth Schoen and Eva Galperin, "Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities," *Electronic Frontier Foundation*, 29 Aug. 2011. 以下も参照。S Nicholas Weaver, "A Close Look at the NSA's Most Powerful Internet Attack Tool," *Wired*, 13 March 2014.

＊33 *The Epic Turla Operation*, Kaspersky Lab, 7 Aug. 2014.

＊34 2014年夏の様々な事業者たちとの著者のインタビュー。

＊35 *United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, Criminal Nr 14-118, Erie, PA: US District Court Western District of Pennsylvania, 1 May 2014, Exhibit F.

＊36 例えば2014年8月6日、ファイア・アイは「正当なドメインにビーコンを送っていると見られるマルウェア」の作戦について情報を公開した。これは「防御者をまちがったセキュリティ感覚に陥らせる」試みだったと見られる。以下を参照。Ned Moran, Joshua Homan and Mike Scott, "Operation Poisoned Hurricane," FireEye, 6 Aug. 2014.

＊37 Ned Moran and James Bennett, "Supply Chain Analysis: From Quartermaster to Sun- shop," FireEye Labs, 11 Nov. 2013.

＊38 以下を参照。Costin Raiu, "Inside the Duqu Command and Control Servers," presentation at SOURCE Boston, 2012, 4 May 2012, <http://youtu.be/nWB_5KC7LE0>.

＊39 デューク一に関するシマンテックの報告書は、「デューク一はかなりのコードをスタックスネットと共有している。しかし、ペイロードは完全に異なる。産業制御システムを破壊するようデザインされたペイロードの代わりに、一般的なリモート・アクセス能力と置き換えられた。デューク一の作成者たちは、スタックスネットのバイナリー（コンパイルされたバージョン）だけでなく、ソース・コードにアクセスできた」と書いている。W32.Duqu, Version 1.4, *Symantec*, 23 Nov. 2011, 3.

＊40 United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui, Criminal Nr 14-118, Erie, PA: US District Court Western District of Pennsylvania, 1 May 2014, 12-13, Exhibit F.

＊41 2014年9月15日にバージニア州アーリントンで行ったディミトリ・アルパロヴィッチ（Dmitri Alperovich）との著者のインタビュー。以下も参照。Global Threat Report, Arlington, VA: CrowdStrike, 22 January 2014, p. 18.

＊42 Unveiling "Careto," Version 1.0, Kaspersky Lab, 6 Feb. 2014, p. 46.

＊43 例えば、elpais.linkconf[dot]net/および elespectador.linkconf[dot]net である。注34を参照。

＊44 Ibid., 46.

＊45 Nate Anderson, and Cyrus Farivar, "How the feds took down the Dread Pirate Roberts," *Ars Technica*, 3 October 2013.

＊46 John Leyden, "The One Tiny Slip that Put LulzSec Chief Sabu in the FBI's pocket," *The Register*, 7 March 2012.

＊47 Dan Verton, *Confessions of Teenage Hackers* (New York: McGraw Hill 2000), p. 83.

＊48 Ron Rosenbaum, "Cassandra Syndrome," *Smithsonian Magazine*, Vol. 43, No. 1, (April 2012), p. 12.

＊49 Ivanka Barzashka, "Are Cyber-Weapons Effective?," *RUSI Journal*, Vol. 158, No. 2 (April/May 2013), pp. 48?56, 51.

＊50 Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired Magazine*, 11 July 2011.

＊51 William Broad et al., "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, 15 Jan. 2011.

＊52 APT1, Alexandria, VA: Mandiant, 18 Feb. 2013.

＊53 Gavin O'Gorman and Geoff McDonald, "The Elderwood Project," Symantec, 6 September 2012.

＊54 2014年春と夏にトロント、ロンドン、ワシントンで行われた多様な分析者たちとの筆者の会話に基づく。

＊55 Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *New York Times*, 3 June 2011.

＊56 このインシデントの詳細な説明は以下を参照。Thomas Rid, *Cyber War will Not Take Place* (Oxford/New York: Oxford University Press, 2013), pp. 26-29.

＊57 Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, 19 Nov. 2013.

＊58 Geoff McDonald, Liam O' Murchu, Stephen Doherty and Eric Chien, "Stuxnet 0.5: The Missing Link, Version 1.0," Symantec, 26 Feb. 2013.

＊59 Ronald J. Deibert, Rafal Rohozinski and Masashi Crete-Nishihata, "Cyclones in Cyberspace," *Security Dialogue*, Vol. 43, No. 1 (2012), pp. 3-24.

＊60 Gauss, Kaspersky Lab, 9 August 2012.

＊61 以下を参照。David Shamah, "New Virus May be US, Israeli Digital Strike against Hezbollah," *Times of Israel*, 13 August 2012.

＊62 "2014 Data Breach Investigations Report," Verizon, 22 April 2014, p. 23.

＊63 Jim Finkle, "Exclusive: Insiders suspected in Saudi cyber attack," *Reuters*, 7 September 2012.

＊64 Jill Slay and Michael Miller, "Lessons Learned from the Maroochy Water Breach," in E. Goetz and S. Shenoi, eds., *Critical Infrastructure Protection*, Vol. 253 (Boston, MA: Springer 2008), pp. 73-82.

＊65 Paul Quinn-Judge, "Cracks in the System," *Time*, 9 June 2002.

＊66 Christopher Bronk and Eneken Tikk, "The Cyber Attack on Saudi Aramco," *Survival*, Vol. 55, No. 2 (April?May 2013), pp. 81-96.

＊67 Ralph Langner, "Stuxnet's Secret Twin," *Foreign Policy*, 19 November 2013. スタックスネットの詳細な議論については以下を参照。Kim Zetter, *Countdown to Zero Day* (New York: Crown, 2014).

＊68 Andrea Peterson, "eBay Asks 145 Million Users to Change Passwords after Data Breach," *Washington Post*, 21 May 2014.

＊69 Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach,"

Wall Street Journal, 14 February 2012.

＊70 Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *New York Times*, 8 January 2013.

＊71 Winston S. Churchill, *The Gathering Storm: The Second World War*, Volume 1 (New York: Rosetta Books, 2002), p. 415.

＊72 Leon Panetta, "Remarks on Cybersecurity to the Business Executives for National Security," New York City, Washington DC: Department of Defense, 12 October 2012.

＊73 *United States of America v Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, Criminal Nr 14-118, Erie, PA: US District Court Western District of Pennsylvania, 1 May 2014, 11.

＊74 概観するには以下を参照。Kim Zetter, *Countdown to Zero Day* (New York: Crown, 2014).

＊75 最も著名な報告書のうち二つは、APT1とパター・パンダである。APT1, Alexandria, VA: Mandiant, 18 Feb. 2013; Putter Panda, CrowdStrike, 9 June 2014.

＊76 2014年10月8日のバルセロナにおけるコスティン・ライウ（Costin Raiu）、アレックス・ゴステフ（Aleks Gostev）、カート・バウムガートナー（Kurt Baumgartner）、ヴィンセント・ディアズ（Vicente Diaz）、イゴール・ソウメンコフ（Igor Soumenkov）、セルゲイ・ミネーブ（Sergey Mineev）との著者によるインタビュー。以下も参照。"Unveiling 'Careto,'" Version 1.0, Kaspersky Lab, 6 Feb. 2014.

＊77 Alexander Gostev, "The Flame: Questions and Answers," Kaspersky Lab, 28 May 2012.

＊78 Vitaly Kamluk, "The Mystery of Duqu: Part Six," Securelist, 30 November 2011.

＊79 "'Red October' Diplomatic Cyber Attacks Investigation, Version 1.0," Kaspersky Lab, 14 Jan. 2013; Costin Raiu, Igor Soumenkov, Kurt Baumgartner and Vitaly Kamluk, "The MiniDuke Mystery," Kaspersky Lab, 25 Feb. 2013; "The 'Icefog' APT," Kaspersky Lab, 25 Sept. 2013.

＊80 2014年10月8日、バルセロナにおけるカスペルスキー・ラボとのフォーカス・グループ・セッション。2014年10月12日11:49 BSTにおけるコスティン・ライウ（Costin Raiu）との電子メール・コミュニケーション。

＊81 "Threat Report: Beyond the Breach," Reston, VA: Mandiant, 18 February 2014, 18.

＊82 2014年10月11日01:41 BSTにおけるリチャード・ベイトリック（Richard

Bejtlich）との電子メール・コミュニケーション。

＊83 一つの例は、いわゆるネットトラベラー（NetTraveler）キャンペーンで、これは単純にコマンド・アンド・コントロールのサーバーを香港に移し、その後、そこから作戦を続けた。2014年10月12日11:49 BST におけるコスティン・ライウ（Costin Raiu）との電子メール・コミュニケーション。以下を参照。"The NetTraveler," Kaspersky Lab, 4 June 2013.

＊84 Sherman Kent, "Estimates and Influence," *Studies in Intelligence*, Vol. 12, No. 3 (Summer 1968), pp. 11-21.

＊85 Ibid.

＊86 2014年夏に行った官民の分析者たちとのフォーカス・グループ・セッション。

＊87 おそらくこの見解の最善の言明については以下を参照。Richard Clayton, "Anonymity and Traceability in Cyberspace," Vol. 653, *Technical Report* (Cambridge: Univ. of Cambridge Computer Laboratory, 2005).

＊88 例えば、以下を参照。Joseph S. Nye, *Cyber Power* (Fort Belvoir, VA: Defense Technical Information Center, 2010).

＊89 例えば以下を参照。Michael McConnell, "Cyberwar is the New Atomic Age," *New Perspectives Quarterly*, Vol. 26, No. 3 (Summer 2009), pp. 72-77.

＊90 最初に言及したものの一つとしては以下を参照。John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996), p. 94. また、以下も参照。Department of Defense, Cyberspace Policy Report, Nov. 2011, p. 2.