中央大学社会科学研究所年報　第 23 号（2018）

〈査読論文〉

サイバー攻撃に対する制裁の考察

――オバマ政権の対朝，対中，対露制裁を中心に――

出　口　雅　史*

Consideration of Sanctions against Cyber Attacks With a Focus on Sanctions against North Korea, China and Russia in the Obama Administration

Deguchi Masafumi

The growing importance of cyber security has been accompanied by an increase in the threat of cyber attacks. The most remarkable reason for this is the superiority of cyber attacks. The cost of cyber attacks seems to be relatively lower than defense because they do not require expensive hardware; further, the possibility of facing retaliation is low.

However, in recent years, the United States has examined new countermeasures, such as sanctions to deter cyber attacks. This paper will investigate how and why the Obama administration introduced sanctions against cyber attacks. The article focuses, especially, on the sanctions against China, North Korea, and Russia. There are two major reasons underlying the changes in the cyber strategy of the Obama administration and specific factors for each. The purpose of the paper is to explain how the two reasons are related to the sanctions against cyber attacks introduced by the Obama administration.

キーワード：サイバーセキュリティ，サイバー攻撃，サイバー抑止，経済制裁，オバマ政権，アメリカ外交

【目次】

2019 年 3 月 22 日査読審査終了

＊中央大学大学院法学研究科博士後期課程

4．結　　論

1．はじめに

⑴ 問題の所在

現在，日本のみならず世界各国で第 4 次産業革命と呼ばれる社会の電子化が進んでおり，サイバー空間へのヒト，モノ，カネ，情報の接続が急速に拡大している．このような社会の電子化によって，情報通信技術（ICT）の重要性は一層増しつつある一方で，それに比例するようにサイバー攻撃の脅威も増している[1)]．サイバー攻撃の脅威は，サイバー空間で飛び交う攻撃の数が増大するといった量的問題だけでなく，2010 年に発見されたイランの核燃料施設を標的とするマルウェア（不正プログラムの総称）である「スタックスネット」に代表される，物理的損傷を引き起こす種類の攻撃が出現し始めたことから，「質的」にも飛躍的に増していると考えられる．実際に，2015 年のウクライナで発生した停電事件のように，サイバー攻撃による被害はサイバー空間だけの現象に留まらず，日常生活をも脅かす攻撃へと既に転換しつつある[2)]．

このような状況下で，「サイバーセキュリティ」は単に特定のコンピュータやネットワークを技術的に防御するという伝統的な意味を超えて，国家安全保障の一種として考えられるようになったが，サイバーセキュリティ政策を考える上で避けては通れない重大な問題が存在する．それはサイバー空間における攻撃優位性である．サイバー空間において一般的に攻撃が優位であると考えられる最も重要な要因として，サイバー攻撃の「低コスト性」が挙げられる．この場合の「コスト」とは，サイバー攻撃には専用の高価なハードウェアは必要ではなく，少人数や個人でも発動可能であるといった経済的な「コスト」だけでなく，サイバー攻撃の実行主体に対し何らかの報復措置や法律に基づいて罰せられることが少ないという意味で，「リスク」も含むものである．サイバー攻撃の「低コスト性」は，サイバー攻撃の多くが国境を越えたものであり，国際的な捜査協力が成り立ちにくいサイバー空間の状況によって助長されている．

攻撃側の著しい「低コスト性」に反して，防御側は新たな攻撃手段への対応や既存システム

1） 本論文におけるサイバー攻撃の定義は「電子技術を用いてコンピュータシステムを標的とする攻撃の総称」としている．これは一般的に使用されるサイバー攻撃の定義としては最も広義の定義であり，この定義におけるサイバー攻撃は情報の窃取からコンピュータシステムの妨害に至るまでの全ての悪意のあるサイバー活動（Cyber Activities）を含むものである．

2） Ellen Nakashima, *Russian hackers suspected in attack that blacked out parts of Ukraine*, washingtonpost, 2016, URL: https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html?utm_term=.a5382cd5dbc3（2018 年 12 月 1 日アクセス）

の老朽化を防ぐ為に，常態的なコスト投資が必要なことから，攻撃と比較して防御は相対的に高コストであると考えられる[3)]．このような攻撃防御バランスにおけるコストの非対称性を主な理由とする攻撃優位の原則により，純防御的なサイバーセキュリティ政策では近年拡大傾向にあるサイバー攻撃の脅威に対応するのが困難である一方，それではどのような政策や戦略によって国家安全保障としてのサイバーセキュリティを改善することが可能であるのかが課題となってきた．

⑵　本論文の目的

冒頭で述べた国家安全保障としてのサイバーセキュリティの課題を受け，国家がどのような政策でサイバー空間の脅威に対抗することが可能であるか模索する上で，本論文はサイバー攻撃に対する制裁に着目する．サイバー攻撃への制裁に着目する理由は，冒頭で述べた通り攻撃優位性を成り立たせる最大の要因は攻撃側の低コスト性であるが，もし何らかの手段で攻撃側にコストを課すことが出来るならば，そのような低コスト性の原理を覆し得る可能性があるからである．このサイバー攻撃に対する制裁の事例として存在するのが，アメリカのオバマ政権が２期目において北朝鮮，中国，ロシアに対して発動した制裁である．

国家が関与したと考えられるサイバー攻撃は古くは1990年代から存在が指摘されてきたが，長年の間制裁などの対抗措置が実際に取られることはなかった．サイバー攻撃の実行主体に対してコストを課すことは，国家安全保障としてのサイバーセキュリティを改善する上で，極めて重大な要素となり得るが，それにも関わらずオバマ政権の２期目までに，アメリカ政府が制裁を行わなかったのは何故かという疑問が生ずる．

サイバー攻撃への制裁が従来困難であった要因として「アトリビューションプロブレム（帰属問題）」が挙げられる．もし，サイバー攻撃の実行主体に制裁や報復などのコストを課す場合には，その前提として誰が攻撃しているか判明させなければならない．しかし，技術的に洗練された主体であれば，攻撃の経路や場合によっては攻撃の発生そのものを偽装することが可能であり，常にサイバー攻撃の主体が明確になるとは限らないという問題が存在する．また，サイバー攻撃の種類によっては，攻撃の対象や発生時期などから，状況証拠を積み重ねて攻撃主体を推論することが出来たとしても，被害者側が技術的証拠を公開して犯人を立証することは，仮にそのような証拠があったとしても困難が生ずる．何故ならば，サイバー攻撃の技術的根拠を公表することは，自らのセキュリティ能力をある程度周知することにもつながり，それ自体がセキュリティリスクとみなされるからである．このようなサイバーセキュリティの特性

3）伊東寛はサイバー戦において攻撃が有利に働く要因として，秘匿性，非対称性の他，攻撃側が時期や場所を自由に選べることを挙げている．伊東寛，『サイバー戦争論　ナショナルセキュリティの現在』原書房，2016年，95-105ページ．

により，攻撃主体を明確に立証することが困難であることを示す用語が「アトリビューションプロブレム」である[4)]．

この「アトリビューションプロブレム」の問題は，オバマ政権2期目以降においても完全に解消したわけではなく，実際に多数のサイバー攻撃が現在に至るまでアメリカを対象に行われる一方，制裁が発動された事例は限られている．しかし，限定的ではあるが，以前はサイバー攻撃の脅威がありつつも発動されなかった制裁が，オバマ政権2期目の特定の時期以降現れるようになった背景は必ずしも明確になっていなかった．従って，何故オバマ政権の途中からアメリカ政府がサイバーセキュリティ政策を変更し，北朝鮮，中国，ロシアに対するサイバー攻撃を発動したのかという問いに答えるのが本論文の目的である．以上の問いに答える為，サイバー攻撃の制裁と密接な関連があるサイバー抑止に関する戦略変化の要因及び，各事例における個別要因についてそれぞれ検証を行う．

なお，米国によるサイバー攻撃への制裁は，主権国家だけでなく，サイバー犯罪組織やテロリストなどの非国家主体も本来含むものであるが，非国家主体への制裁と主権国家への制裁はそれが国境を越えるものであるかを問わず，外交交渉が可能か否かなど政策手段として根本的に相違があるものという前提に立ち，本論文ではあくまで「他の主権国家からのサイバー攻撃に対する制裁」を考察するものとして，対中，対露，対朝の3カ国への制裁のみを検証の対象とする．

2．アメリカ連邦政府のサイバーセキュリティ戦略の変遷

⑴ クリントン政権・ブッシュ政権のサイバーセキュリティ戦略

「サイバーセキュリティ」の概念は，初期のサイバー攻撃が登場する1980年代にまで遡ることが出来るが，アメリカ政府がサイバーセキュリティ戦略を形成するようになったのはクリントン政権の1998年になってからである．アメリカ政府における初めてのサイバーセキュリティ戦略と言えるのが「PDD-63（Presidential Decision Directive-63）」である．「PDD-63」は，アメリカ大統領が行政権を行使することによって発令することが可能な，大統領令であり，その中において「アメリカが世界的に保持している強大な軍事力と経済力は，重要インフラとサイバー技術による情報システムにますます依存するようになっている」という認識を示し，「物理攻撃，サイバー攻撃の標的となる，サイバーシステムを含む我々の重要インフラが抱えている脆弱性を排除する必要な手段を取るべきである」として，サイバー攻撃が物理攻撃と並列し

4） デービッド・クラークによれば，サイバーセキュリティにおける「帰属」とは，攻撃主体の「アイデンティティ（身分）」を判明させることを意味する．この「アイデンティティ」には攻撃主体の居場所や攻撃手段も含まれる．David D. Clark, Susan Landau, “Untangling Attribution”, in Committee on Deterring Cyberattacks, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, 2010, p.25.

表-1　主なアメリカ政府・企業を対象とするサイバー攻撃の事件・事例

攻撃発生 / 発覚年	事件・事例名	関与が疑われる国家	主な攻撃対象・被害
1998	Moonlight Maze	ロシア	国防総省，NASA，などの連邦政府機関の情報流出
2003	タイタンレイン	中国	国防総省，ロッキードマーチンなどの防衛関連機関，企業の情報流出
2009	ゴーストネット	中国	各国大使館におけるメールなどの情報流出
2009	米韓への大規模サイバー攻撃	北朝鮮	DDoS による米韓政府関連 Web サイトへの攻撃
2010	オーロラ作戦	中国	Google のメールサービスへのハッキング
2014	ソニーピクチャーズへのサイバー攻撃	北朝鮮	ソニーピクチャーズの内部文書や個人情報の流出
2014	アメリカ連邦人事局へのサイバー攻撃	中国	連邦人事局が保有する職員などの個人情報流出
2016	2016 年米大統領選挙への干渉事件	ロシア	民主党全国委員会のメール文書流出等

出典：筆者作成.

て言及されている[5)]．クリントン政権下における「サイバーセキュリティ」とは専ら，情報インフラを外部の脅威からどのように守るかという防御的な政策が中心であり，この時点では他国への制裁など相手にコストを課す手段についての言及はない．

クリントン政権からブッシュ政権に入ると，アメリカのサイバーセキュリティ戦略に大きな影響を及ぼす事件である 2001 年の 9.11 同時多発テロ事件が発生した．航空機を使った攻撃により，世界貿易センタービルが倒壊し数千人もの死者が出た事件は，テロリズムによって国家の重要インフラが破壊されるという現実と共に世界的な衝撃を与えた．この事件自体は，直接的にはサイバー攻撃に関係するものではないが，米連邦政府のサイバーセキュリティ政策を担う重要な組織である国土安全保障省（Department of Homeland Security, 以下 DHS）の設立のきっかけであるという点において，米連邦政府のサイバーセキュリティ政策を変化させる要因になったと位置づけられる．DHS は 2002 年 11 月 25 日に設立され，沿岸警備隊やシークレットサーヴィスなど既存の 22 の機関を統合した組織であるが，その中には，一般調達局（GSA, General Services Administration）傘下にあった連邦コンピュータ事件対応センター（FedCIRC, Federal Computer Incident Response Center）が含まれており，サイバーセキュリティも DHS の任務の 1 つとなった．本来テロ対策を主導する為に設立された DHS にサイバーセキュリティ任務も付与された背景には，FBI，国防総省，商務省など各省庁に分散的に配置されていた

5）White House, *PDD-63*, URL: http://www.fas.org/irp/offdocs/pdd/pdd-63.htm（2018 年 10 月 9 日閲覧）

関連機関を一元化し，連邦政府におけるサイバーセキュリティの司令塔機能を持たせることがあったと考えられる．軍事ネットワークの防衛については依然として国防総省の管轄にある一方，民事セクターの防衛については DHS が統合的に担うようになった．このように 9.11 同時多発テロ事件を契機に，アメリカのサイバーセキュリティ組織は刷新，統合されるようになったが，サイバー攻撃に対する政策の基本的な姿勢は重要インフラの防御でありブッシュ政権のサイバーセキュリティ政策は，クリントン政権の継続であったと考えられる．

ただし，ブッシュ政権の末期にあたる 2007 年を境として既存のサイバーセキュリティの概念を覆す重大な事件が次々と発生するようになる．2007 年にはロシア政府の関与が疑われた事例として，エストニアにおいて赤軍兵士像移設問題を危機に始まった大規模サイバー攻撃が発生した他，翌 2008 年の南オセチア紛争の最中に，グルジアに対する大規模サイバー攻撃が発生し，武力紛争を間接的に支援する種類のサイバー攻撃の事例も存在する．いずれもサイバー攻撃の手段は，DDoS や Web サイトの改ざんなど以前より多用されていた手法であり，それ自体は目新しいものではないものの，非常に大規模かつ長期間の攻撃であったことから，これらは世界初の「サイバー戦争」と目されるほど注目された事例となった．また，同時期の 2007 年には，イスラエルによって行われたシリア国内の核開発施設に対する空爆に伴い，レーダー機能を一時的に無効化することを狙ったサイバー攻撃が発生した[6]．当時のブッシュ政権がこのサイバー攻撃について関知または関与していたかは不明であるものの，ブッシュ政権末期に考案されたと考えられるスタックスネットの機能から，サイバー攻撃が軍事的な利用価値も包含することは当時から認識していたと推測される[7]．このようなサイバー攻撃の技術的向上や実際に発生した重大な事件から，ブッシュ政権 2 期目においてサイバーセキュリティに対する危機感が以前の時代と比べて飛躍的に高まったと考えられるが，具体的な戦略として 2008 年 1 月には，包括的国家サイバーセキュリティ戦略（Comprehensive National Cyber Security Initiative, 以下 CNCI）が形成された[8]．CNCI では，12 のイニシアティヴが含まれているが，その中の多くはサイバー攻撃の侵入を阻止するシステムの開発やサイバーセキュリティ教育の促進など，既存のセキュリティ政策の延長線上に位置するものである．ただし，10 番目のイニシアティヴは「恒久的な抑止技術とプログラムを明確化する」というものであり，こ

6） リチャード・クラーク，ロバート・ネイク（北川智子，峯村利哉訳）『世界サイバー戦争　核を超える脅威：見えない軍拡が始まった』徳間書店．2011 年，19–21 ページ．

7） スタックスネットに関するブッシュ政権の関与については．ニューヨークタイムス紙のサンガー記者の記事を参照．David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks against Iran*, New York Times, 2012, URL: https://www. nytimes. com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran. html（2018 年 12 月 25 日閲覧）

8） White House, *Comprehensive National Cybersecurity Initiative*, 2008, URL: https://www.hsdl.org/?view&did=28609（2018 年 12 月 28 日閲覧）

の文言はアメリカ政府のサイバーセキュリティ戦略において，初めて「サイバー抑止」に言及した文章として注目に値する．ただし，戦略の本文の中にどのような手段を用いて「サイバー抑止」を行うのか具体的な説明は示されていない．このことについて，ブッシュ政権でサイバーセキュリティ担当大統領特別アドバイザーだったリチャード・クラークは「“情報戦における抑止戦略と宣言政策用ドクトリン”を案出する予定だったが，案出作業はほぼ完全に停止してしまった」と述べており，当時のブッシュ政権はサイバー抑止戦略を創出する意図はあったものの実際の戦略策定作業は進んでいなかったことが伺える[9)]．また，CNCI については，そもそもこの戦略自体が当初非公開であり，抑止戦略を公開せずに抑止効果が得られるのか，2008 年 5 月の上院軍事委員会の報告書でも疑問が提示されていた[10)]．以上のように，ブッシュ政権は 9.11 同時多発テロを受け，サイバーセキュリティに関連する組織改編を積極的に進めたが政権期の大部分においては，ブッシュ政権のサイバーセキュリティ政策は本質的に「前政権」の延長であった．政権末期においてサイバーセキュリティ政策を刷新する意図はあったものの，その戦略は具体化されないまま，次のオバマ政権へと引き継がれることになる．

⑵　オバマ政権のサイバーセキュリティ戦略

前項までに説明したように，ブッシュ政権のサイバーセキュリティ戦略は組織改編の他，抑止概念の導入など部分的には以前の戦略を刷新する傾向は存在したものの，本格的な戦略の変化はオバマ政権の誕生以後に見られる．オバマ政権のサイバーセキュリティ戦略の特徴の 1 つとして，CNCI を非公開としていたブッシュ政権と比較すると，政権成立直後からサイバーセキュリティ戦略を積極的に公開していたことが挙げられる[11)]．人事，組織面においては，ブッシュ政権が DHS の組織改編を重視した一方で，当初ホワイトハウスに存在していた「サイバーセキュリティ担当大統領特別アドバイザー」がリチャード・クラークの退任以後廃止されたように，ホワイトハウスが主導するサイバーセキュリティ戦略の形成について必ずしも積極的な姿勢とは言えない状態であったのに対し．オバマ政権は，ホワイトハウス内に「サイバーセキュリティ調整官」を配置することで，政権内のサイバーセキュリティ分野の司令塔機能となるポストを設置し，縦割り行政を解消してホワイトハウス主導でサイバーセキュリティ戦略を立て直す意図があったと考えられる．また，組織改編に関する重大な動きとして，2010 年の

9）　クラーク，前掲書（10），145 ページ．

10）　Committee of Armed Services United States Senate, *S. Rept. 110-335- NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2009*, 2009, pp.389-391.

11）　例えばオバマ政権成立間もない 2009 年 3 月には．ホワイトハウス「サイバー空間政策レビュー」を発表している．Whitehouse, *Cyberspace Policy Review*: *Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, URL: https://fas.org/irp/eprint/cyber-review.pdf（2018 年 1 月 20 日閲覧）

アメリカサイバー軍（USCYBERCOM）の設立が挙げられる．アメリカサイバー軍は，既に戦略軍（USSTRATCOM）の指揮下に置かれていた JTF-GNO（Joint Task Force-Global Network Operations）と JFCC-NW（Joint Functional Component Command for Network Warfare）を統合させた部隊である．JFCC-NW は 2004 年に JTF-GNO と共に NSA の監督下で設置され，グローバルな情報作戦の為に米軍内の協調を監督する機関だった．これらの 2 つの部隊を統合し，アメリカサイバー軍の新しい司令官にはキース・アレクサンダー NSA 長官が兼務することになった[12]．これに呼応するように，アメリカ国防総省の戦略文書である「4 年毎の国防計画見直し（QDR）」においてサイバーセキュリティへの言及回数が急激に増大した．ブッシュ政権期に提出された 2006 年時の QDR では長い文書の中で「Cyber」の単語はわずか 10 回しか出てこなかったことに比べ，2010 年の QDR では 73 回も記述されており，サイバーセキュリティに関する独立した項目が用意されるなどその差は歴然としているが，この 4 年間でアメリカ政府や国防総省の中でサイバー空間への関心が高まっていることを読み取ることが出来る[13]．2010 年の QDR の発表に際して，国防副長官だったウィリアム・J・リンは「一番はサイバー脅威だ．攻撃に際して我々のネットワークを守る能力を維持しなければ，我が軍，我々の安全保障全体にとっての帰結はおそろしいことになる」と述べた[14]．

オバマ政権の誕生によって，アメリカ政府のサイバーセキュリティ戦略の形成は加速し，その中でも特に注目すべき議論が，「サイバー抑止」に関する言及部分である．「サイバー抑止」は 1990 年代半ばより学術的に議論されてきた概念ではあるが，当時はサイバー攻撃の影響は現在と比較して軽微であり，「サイバー抑止」が安全保障研究において注目されるようになったのは 2000 年代末になってからである[15]．特に「サイバー抑止」の概念が整理された代表的な論文として 2009 年のマーチン・C・リビッキの「Cyber Deterrence and CyberWar」が挙げられる．リビッキは「サイバー空間において他者（被抑止主体）が我々（抑止主体）に行おう

12） 土屋大洋「米国におけるサイバーセキュリティ政策」『米国内政と外交における新展開』日本国際問題研究所，2012 年，139 ページ，URL: http://www2.jiia.or.jp/pdf/resarch/H24_US/08-tsuchiya.pdf（2018 年 12 月 20 日閲覧）

13） US Department of Defense, *Quadrennial Defense Review Report*, 2006, URL: http://www.comw.org/qdr/qdr2006.pdf（2018 年 11 月 25 日閲覧）

US Department of Defense, *Quadrennial Defense Review Report*, 2010, URL: http://archive.defense.gov/qdr/QDR %20as %20of %2029JAN10%201600.pdf（2018 年 11 月 25 日閲覧）

14） 土屋，前掲書（16），76 ページ．

15） 1996 年に発表されたリチャード・ハークネットの論文では，サイバー戦争（Cyber War）を，心理戦などの非軍事分野におけるサイバー戦であるネット戦争（Net War）と，軍事分野におけるサイバー戦であるサイバー戦争（Cyber War）に分け，サイバー抑止は主に後者のサイバー戦争の抑止に適合する概念であり，通常兵器による攻撃の抑止を対象とする「通常抑止」と似た性格を持つと分析している．Richard J. Harknett, “Information Warfare and Deterrence,” *Parameters*, Vol. 26, No. 3, 1996, pp. 93-107.

としているのと同等の方法を用いる抑止」と定義する一方，これらに外交的，経済的な手段は含まず，それらは「サイバー抑止」ではなく抑止よりも強度の低い「サイバー対応（cyber response）」と定義した[16]．リビッキの定義は，「サイバー抑止」の中でも抑止方法を攻撃主体が用いたものと同等の方法に限定しているという点で，狭義の定義であると位置づけられるが，それに対してアメリカ政府の戦略の中で使用される「サイバー抑止」は広義の定義のものであり，経済制裁等も含まれている[17]．このような「サイバー抑止」概念は，安全保障研究における既存の抑止概念の類推から始まったが，特に核抑止から大きく影響を受けている．「サイバー抑止」の前提には，攻撃主体が攻撃を発動する際には合理的な損得計算を行い，攻撃によって得られる利益とコストを比較し，コストよりも利益が上回ると判断した場合のみ，実際に攻撃を着手するだろうという想定があるが，これは前述の既存の抑止の理論と同様である[18]．もし，このような合理的計算が成り立つ状態において，抑止を実現するには，攻撃を着手した場合のコストを引き上げるか，もしくは攻撃によって得られる利益を低減させる必要がある．このうち，コストを引き上げる手法が懲罰的抑止であり，攻撃機の利益を低減させるものが拒否的抑止である．懲罰的抑止の最も典型的な事例は，核抑止における核報復である．敵からの核攻撃に対してたとえ先制攻撃を受けても，「第２撃能力」を維持することで相手に受け入れがたい損害を与える体制を維持することで，先制核攻撃を自制させる，というのが核抑止における懲罰的抑止の基本的な理論である．これに対して，核抑止における拒否的抑止とは例えば，ミサイル防衛（MD）によって核ミサイル攻撃を阻止することで，被抑止対象が先制核攻撃によって獲得する利益を否定するというものである．この概念をサイバー抑止に類推した場合には，懲罰的抑止とはリビッキが言うような「同等の方法」であるサイバー攻撃による報復や，あるいはアメリカ政府が採用する広義の「サイバー抑止」に含まれる法的措置や経済制裁といったものが該当する．これに対して「サイバー抑止」における拒否的抑止とは，攻撃による利益を否定する必要がある為，ファイアウォールなどのセキュリティシステムの開発による攻撃の遮断が考えられる．もっとも，「拒否的抑止」として挙げられる防御的手段は，「サイバー抑止」

16）Martin C. Libicki（2009）, *Cyberdeterrence and Cyberwar,* Pittsburgh: RAND Corporation, pp. 27–28.

17）2017年の国防総省国防科学委員会のサイバー抑止の定義では，サイバー抑止の方法を拒否的抑止（deterrence by denial），懲罰的抑止（deterrence by cost imposition）に分けた上で，懲罰的抑止の中に「外交，法的措置，経済的対応」も含まれる，としている．Department of Defense Defense Science Board（2017）, Final Report of the Defense Science Board（DSB）Task Force on Cyber Deterrence, p.6, URL: https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf（2019年3月10日閲覧）

18）抑止が機能する前提には攻守双方の損得計算に加えて，抑止側が国際秩序を守るという「能力」と「意思」を持っており，そのことが非抑止側に「伝達」され「認識」されなくてはならない．土山實男，『安全保障の国際政治学―焦りと傲り―』有斐閣，2010年，173–178ページ．

という概念が存在する以前の時代から既に実行されてきたものであり，これだけであれば，伝統的な「サイバーセキュリティ」手段を「拒否的抑止」と言い換えているに過ぎない．「拒否的抑止」の新しい手段として，考えられた概念が「レジリエンス」である．レジリエンスとは，伝統的なサイバーセキュリティにおいて重視されてきたのが，不正アクセスやマルウェアの侵入といった「水際防御」であるのに対し，全てのサイバー攻撃を遮断することが困難であるという前提から，ある程度侵入を許したとしても可能な限り被害を低減化することを目的とする「縦深防御」を意味する用語である．このようなレジリエンスの方法として，コンピュータのデータや，システムそのものの，バックアップを常に用意することで，早期復旧することを可能にする体制の構築や，コンピュータネットワークをセグメント化することで，システムの一部が攻撃された際にシステム全体に攻撃が波及することを防ぐといった手段が挙げられる．サイバー攻撃が通信，交通，電力など都市単位，または国家単位という広範囲の重要インフラを混乱，停止させるものが出てきた為，その被害を低減化させる重要性は高まっている．従って，従来からの伝統的なサイバーセキュリティ手段とレジリエンスの組合せが，サイバー抑止における「拒否的抑止」の概念であると考えられる．

このような「サイバー抑止」という概念がアメリカ政府で用いられるようになった背景には，本論文の冒頭において説明したサイバー攻撃の優位性がある．サイバー空間における攻撃優位性の為，実際に多数の攻撃が浸透し，「水際防衛対策」にいくら投資したとしても，根本的に防ぐことは困難ではないかという懸念からサイバー攻撃を未然に防ぐ必要があるという発想が生まれた．しかし，前述の「サイバー抑止」の中で，懲罰的抑止概念についてはオバマ政権においても否定的な見方が存在していた．例えば，オバマ政権の当時の国防副長官であったウィリアム・J・リンは，外交誌『フォーリンアフェアーズ』に投稿した論文「Defending a New Domain」において，サイバー空間を第5の戦場と位置づけ，アメリカの安全保障において死活的利益を分かつ空間であるとしながらも，懲罰的抑止については，アトリビューションの問題からこれに否定的な見解を示し，サイバー抑止は「拒否的抑止」を中心に構築すべきだとしている[19)]．

このように「懲罰的サイバー抑止」が困難であり，サイバー抑止が核抑止のように働くことに否定的な見解が政権内には存在したが，その一方で拒否的抑止の場合には，サイバー攻撃の低コスト性からいくら防衛にコストを投じても何らかの手段によってコストを課さなければ攻撃を抑止することには繋がらず，最終的には伝統的サイバーセキュリティが包含する「攻撃優位性」の原理へと回帰するのではないかという懸念も存在していた．もちろん，防御的なサイバーセキュリティであっても以前と比較して何の進化もなかったということではない．例えば

19） William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, *Foreign Affairs,* Vol.89, No.5, 2010, pp.97-108.

DHS が研究して作られたアインシュタインシステムには，連邦政府のコンピュータネットワークを常態的に探査することで異常を自動的に検知し，攻撃があった場合には警報機能も持たせていた．このような防御システムの考え方は「アクティブサイバーディフェンス（能動的サイバー防御）」という構想に基づくものであり，単なる受動的な防御ではなく，犯人の検出を含む能動的な態勢を築くことが目的とされる．また，オバマ政権になってから，レジリエンス概念が拒否的サイバー抑止として重要視されるようになったという違いも見られる．

ただし，これらの新たな防御的な政策を取り入れたとしても，相手に一切のコストを課さない状況においては，攻撃機会は増えるばかりであり，また現実的に防衛に投資出来るコストに限界があるという問題が付きまとう．実際にオバマ政権が成立して以降も，一貫して連邦政府へのサイバー攻撃件数は増加傾向にあった[20)]．

オバマ政権成立から 2011 年までの，数年間のサイバーセキュリティ政策は，サイバーセキュリティ調整官の設置やアメリカサイバー軍の創設などのポスト創出や組織改編，更には戦略を積極的に公開することなど，いくつかの点でブッシュ政権との違いは見られるが，根本的な政策においては，ブッシュ政権と明確な違いは見られず，この期間にオーロラ作戦における中国から Google へのサイバー攻撃など，国家の関与が疑われる重大な事件が発生した一方で，オバマ政権が具体的な制裁などの対抗措置を取ることはなかった．従ってブッシュ政権の前半がクリントン政権のサイバーセキュリティ政策の継続であるとするならば，オバマ政権成立から数年間の間は，ブッシュ政権末期に作られたセキュリティ政策の継続であると考えられる．

しかし，オバマ政権 1 期目の後期にあたる 2011 年頃から 2 期目にかけて，オバマ政権のサイバーセキュリティ戦略に変化が見られる[21)]．CNCI やオバマ政権初期の戦略でも示された通り「サイバー抑止」という言葉はあったとしても，そこには制裁等の対抗措置は明示されておらず，「抑止」という言葉は使われていても，実際の中身は教育投資やネットワークディフェンスなど以前から存在する政策の延長線にあるものだった．このような傾向の変化が明確にみられるのは，2011 年頃からである．2011 年 5 月にホワイトハウスから公表された『サイバー空間の国際戦略（International Strategy for Cyberspace）』では，13 頁から 14 頁にかけて記述されている「抑止」の項目において，「合衆国は他の領域における脅威に対するのと同様にサイバー空間における敵対的行動に対応する」とした上で，「外交，情報，軍事，経済などの適

20）　連邦政府へのサイバー攻撃件数については以下の報告書を参照．
United States Government Accountability Office, *CYBERSECURITY Actions Needed to Strengthen U.S. Capabilities*, 2018, p.4, URL https://www.gao.gov/assets/690/682756.pdf（2018 年 10 月 20 日閲覧）

21）　川口はオバマ政府における抑止政策の変遷について，2008 年～ 2011 年を「拒否的抑止への傾倒」，2011 年～ 2014 年を「懲罰的抑止力の再興」としている．川口貴久，“米国におけるサイバー抑止政策の刷新 アトリビューションとレジリエンス”，KEIO SFC JOURNAL『特集：新しい安全保障論の展開』慶應義塾大学湘南藤沢学会，2015 年，82–85 ページ．

切な手段を行使する権利を有する」と述べている[22]．CNCIやオバマ政権成立直後に出された「サイバー空間政策レビュー」では，抑止に関する記述が一応は存在していたものの，その中身はほとんど触れられていなかったのに比較すると，軍事的手段にも言及するなど一層踏み込んだ内容になっている．

また，2011 年 11 月に米国国防総省から発表された戦略である『国防総省サイバー空間政策報告』では連邦議会より提出された 13 の質問に，国防総省が回答する形式になっているが，サイバー攻撃に対する報復として，サイバー攻撃だけでなく軍事的な手段も辞さないことが記されており，従来的な防衛力の向上といったセキュリティ対策に加えて，報復による抑止政策がアメリカのサイバーセキュリティにとって主要な手段として追求されるようになったことが示されている．このレポートの中で，国防総省はサイバー抑止について拒否的抑止と懲罰的抑止の両方が必要であると回答しており，その手段として軍事オプションやサイバー攻撃による反撃も視野に入れることが記述されている[23]．

2015 年に公表された「国防総省サイバー戦略」でもサイバー抑止に多くの記述が割かれており，サイバー抑止の為に帰属を探知する技術開発だけでなく，宣言政策を通じて，潜在的な敵対者へ「警告」を行う能力を開発するなど，より包括的な政策として検討していることが伺える．以上のようにオバマ政権のサイバーセキュリティ政策を総括すると次のような特徴がある．政権成立当初はブッシュ政権末期に作成された CNCI を基盤としており，制裁や抑止政策については，CNCI 同様に内容が不透明でありかつ記述も少なかったものの，2011 年頃を境として経済的制裁や軍事的制裁などの，より「攻撃的なオプション」としてサイバー攻撃の実行主体に対しコストを課す姿勢が鮮明になった．これらの戦略文書において示された「変化」の時期は，オバマ政権が 2014 年以降にサイバー攻撃に対する制裁を発動する前段階にあたる時期とみなすことができる．

⑶ オバマ政権の政策変化の要因

このようなオバマ政権の政策の変化により，「サイバー攻撃の実行主体にコストを課す政策」が明確になったが，どのような要因によってこの政策変化がもたらされたのだろうか．2010 年のウィリアム・J・リンの論文に見られるように，オバマ政権成立後から 2011 年までは主に拒否的抑止をサイバー抑止の中心的な方法に据える方向性があったが，その後拒否的抑止への信頼性が失われたことが考えられる．そもそも，拒否的抑止が機能し得るには，実際にサイバ

22） White House, *International Strategy For Cyberspace*, 2011, pp.13–14, URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf（2019 年 1 月 10 日閲覧）

23） Department of Defense（2011）, *Department of Defense Cyberspace Policy Repor*t, pp.2–5, URL: https://fas.org/irp/eprint/dod-cyber.pdf（2018 年 12 月 20 日閲覧）

ー攻撃を阻止するだけの防御的能力が発揮されなければならない．しかし，連邦政府機関からDHSに報告されたサイバー攻撃件数は，2009年の29,999件から2013年の61,214件にまで増加しており，この期間において一貫して増加傾向にあることが確認出来る[24]．このことに加えて，アメリカ連邦政府機関をサイバー攻撃から防御する柱としてDHSが開発していたアインシュタインシステムの開発費が高騰し，2012年に開発プログラムが縮小する事態も発生した．このことは，単にサイバー攻撃の総数が増えているというだけでなく，将来に渡って拒否的抑止を発揮するほどのコストをかけることが困難であることも示唆していた[25]．

一方，懲罰的抑止について，最大のネックとなっていたのはアトリビューション（帰属問題）であったが，この問題を解消する動きが国防総省を中心に見られた．2011年の「国防総省サイバー空間政策報告」の中で，国防総省はアトリビューションの制限の中で効果的な報復や抑止がどのように機能し得るか，という質問に対し，民間セクターと共同で攻撃の起源を追跡する技術開発を行い，攻撃主体を発見することが可能になると回答している[26]．2013年にアメリカのセキュリティ企業から公開された中国61398部隊の活動を報告したレポートは，部隊の活動時間や拠点となる建造物の住所まで記述されており，以前と比較してサイバー攻撃の追跡技術が向上していると考えられる[27]．これらの要因によって，攻撃主体の利益を否定する「拒否的抑止」に対する信頼性が低下した一方，従来は実現困難だと思われてきた「懲罰的抑止」の実現性が向上したことで，「サイバー攻撃の実行主体にコストを課す政策」にアメリカ政府がサイバー抑止の比重を移すことになったと考えられる．

このような政策上の変化に加え，2014年以降オバマ政権が制裁を発動する対象となる重大なサイバー攻撃の事件が発生することとなる．次に，対北朝鮮，対中国，対ロシアへのサイバー攻撃の制裁の事例を対象に，何故これらの事例において制裁を発動したのか個別要因を検証する．

3．オバマ政権によるサイバー攻撃への制裁

⑴　北朝鮮への制裁

アメリカが本格的に主権国家への制裁を発動するきっかけとなったのが，2014年11月に発

24）United States Government Accountability Office（2018），*CYBERSECURITY Actions Needed to Strengthen U.S. Capabilities*, p.4, URL: https://www.gao.gov/assets/690/682756.pdf（2019年3月11日閲覧）

25）United States Government Accountability Office（2016），*DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, URL: https://www.gao.gov/assets/680/674829.pdf（2018年3月12日閲覧）

26）Department of Defense（2011），op.cit., p.4.

27）Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, 2013, p.3.

生したソニーピクチャーズへのサイバー攻撃事件である．「ザ・インタビュー」という 2014 年 12 月に公開予定であったコメディ映画の中に，北朝鮮の最高指導者である金正恩第一書記の暗殺シーンや彼を揶揄するような内容が含まれており，それを理由として配給元であるソニーピクチャーズへの攻撃が行われたと考えられる．2014 年 12 月 19 日には，FBI がこのサイバー攻撃の犯人は北朝鮮政府であると断定し[28)]，オバマ大統領もこの攻撃を「安全保障問題である」と宣言し[29)]，北朝鮮へのサイバー攻撃を理由とする制裁に踏み切った．北朝鮮に対しては，既に核実験や弾道ミサイル発射実験を理由に経済制裁が発動されていた為この制裁は追加制裁となるが，2015 年 1 月 2 日にサインされた大統領令（Executive Order）13687 に基づき，商務省によって発表された 10 人の個人と朝鮮人民軍総参謀部偵察局，朝鮮鉱業開発貿易会社，朝鮮檀君貿易会社の 3 つの組織が追加制裁の対象となった[30)]．

この事例における北朝鮮への制裁は追加制裁とはいえ，サイバー攻撃を理由とした経済制裁は当時としては世界でも類を見ないケースであったが，北朝鮮からアメリカを標的とするサイバー攻撃自体は，例えば 2009 年にアメリカ独立記念日である 7 月 7 日に発動された大規模な DDoS 攻撃など以前から繰り返されていたものであり，攻撃の規模や被害を鑑みてもこの攻撃が以前のケースより特異であったとは言い難い．また，サイバー攻撃のアトリビューションにはある程度時間がかかる場合もあるが，本件では事件の発生から北朝鮮が犯人であるとアメリカ政府が認定しかつ制裁が発動されるまでの期間は，およそ 1 か月半程度と非常に短い期間で進展していることも異例である．このような異例の対応の背景として，サイバー攻撃の行為主体の目的と事件の発生要因である「ザ・インタビュー」という映画との関連性が明確であり，他の事件と比較して「状況証拠」におけるアトリビューションが容易であるという点が挙げられる．企業を標的とするサイバー攻撃自体は決して珍しいものではなく，またその中には国家が関与するものも存在する．例えば北朝鮮が関連していると考えられているサイバー攻撃として，バングラディシュ中央銀行の口座に不正アクセスを行い不正に送金した事件が挙げられる．ただし，金銭目的のサイバー攻撃というのは北朝鮮が関与するものに限らず世界中で発生しているものであり，このような事例においては実行主体と攻撃の要因との関連性という「状況証拠」のみで，北朝鮮を犯人と見出すことは困難である．それに対してソニーピクチャーズとい

28） FBI National Press Office, *Update on Sony Investigation*, URL: https://www. fbi. gov/news/pressrel/press-releases/update-on-sony-investigation（2018 年 12 月 20 日閲覧）

29） White House, *Remarks by the President in Year-End Press Conference*, URL: https://obamawhitehouse. archives. gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference（2018 年 12 月 20 日閲覧）

30） Department of Treasury, *Issuance of a new North Korea-related Executive Order; North Korea Designations*, 2015, URL: https://www.treasury.gov/resource-center/sanctions/ofac-enforcement/pages/20150102.aspx（2018 年 12 月 20 日閲覧）

う映画配給会社をピンポイントで標的としたサイバー攻撃は，攻撃が行われた時期や目的と，北朝鮮との因果関係は相対的に明確であり，この明確性がオバマ政権の迅速な対応に繋がったと考えられる．また国連安保理決議に違反する核実験や弾道ミサイルを強行していた北朝鮮に対しては既に経済制裁を発動しており，その対象を拡大するに過ぎない．2015 年 1 月の制裁は既存の制裁に上乗せする形式になる為，サイバー攻撃のアトリビューションについては必ずしも神経質になる必要がなかったことも迅速な対応の要因に挙げられる．

⑵ 大統領令 13694

北朝鮮へのサイバー攻撃に対する制裁を発動した 3 か月後にあたる，2015 年 4 月 1 日に，オバマ大統領は大統領令（Executive Order）13694 に署名をした．この大統領令は米商務省に対して「悪意のあるサイバー攻撃を米国に対して実行する個人・組織」に対して「SDN（Specially Designated Nationals and Blocked Persons）リスト」に入れる権限を付与するものである．このリストに基づき商務省外国資産管理局（OFAC: Treasury's Office of Foreign Assets Control）が経済制裁の運用を行う．この大統領令の特色は，北朝鮮への制裁の根拠となる大統領令 13687 と異なり，特定の制裁対象を規定しているのではなく，商務省に対し恒久的にサイバー攻撃への制裁を行う法的根拠を付与していることになる．制裁の方法については，北朝鮮に対する制裁と同様に，資産凍結や取引規制が主な手段となる．ただし，この大統領令 13694 は，署名されてからしばらくは実際に発動されず，2016 年 12 月に大統領選挙への干渉を理由とする対ロシア制裁になって初めて使用されることになる．

⑶ 中国への制裁

オバマ政権 2 期目に行われた中国への制裁として挙げられるのが，2014 年 5 月中国人民解放軍「61398 部隊」が関与する事件に関連して，米司法省が 5 人の関係者を起訴した事例である．ただし，この措置は前述の北朝鮮のような経済制裁ではなく，米国内に在住していない個人の起訴に留まることから，実効的な制裁というよりも「政治的な示威行為」としての「名指しの批判」であると考えられる．ただし，中国による知的財産権の侵害として古くは 2003 年頃に始まったと考えられている「タイタンレイン」の事件から，中国政府のアトリビューションに関わる情報が公表されていたにも拘わらず，アメリカ政府は具体的な対抗措置を取らなかったが，2014 年になって初めてこのような措置に踏み切ったことは，中国についても今後一層の制裁を課すことを示唆するものであった．

また，中国に関しては，制裁自体は行われなかったものの，制裁の議論が外交交渉に影響を及ぼしたと考えられる事例が存在する．前述の大統領令 13694 が発表された 2 か月後の 2015 年 6 月に，米連邦人事管理局に対するサイバー攻撃で元職員や採用候補も含む連邦政府職員等

2000 万人以上の個人情報が流出した事件が発生した．この事件において中国の関与が指摘されると，ルビオ上院議員が「米中戦略経済対話（S&ED）で中国政府に対してサイバー攻撃に対する制裁を考慮していると伝えるべきだ」と提言した[31)]．2015 年 9 月に予定されていた米中首脳会談前には，米メディアにおいて対中制裁の発動が報道されるようになった[32)]．この交渉の過程は公開されておらず，実際にアメリカ政府が制裁を考慮していると伝えたかは明らかではない．とはいえ，北朝鮮への制裁や，大統領令 13694 の存在から，以前と比較して中国への制裁の発動は現実味を帯びていると中国に警告をするシグナルになったと考えられる．この 2015 年 9 月 25 日の米中首脳会談においては，南シナ海と並ぶ安全保障上の最重要課題としてサイバーセキュリティが議題となり「米中サイバー協定（U.S.–China Cyber Agreement）」が合意された．合意内容は知的財産権の窃取を目的としたサイバー攻撃の支援を相互に控え，定期的にサイバー攻撃に関する情報交換を行い，「米中サイバー犯罪に関するハイレベル（閣僚級）対話」を開くというものであった．この合意については，合意遵守メカニズムが存在せず，合意が守られたかどうかの検証（査察）も，合意が破られた場合のペナルティも規定されていないという批判があったが，その後連邦政府へのサイバー攻撃件数や特定の中国のハッカー組織による対米サイバー攻撃が減少したデータが存在する等一定の効果があったと考えられる[33)]．従って中国については，実際に発動されたサイバー攻撃への制裁は限定的であったが，制裁に関する議論自体が中国とのサイバーセキュリティ交渉へ一定の貢献を果たしたという評価が可能である．

⑷ ロシアへの制裁

2016 年 11 月 8 日に行われたアメリカ大統領選挙に関連して，共和党候補であるトランプを支持する目的で発動したと疑われたのがロシアによるサイバー攻撃疑惑である．このサイバー攻撃が報道された発端は，民主党全国委員会のサーバーがサイバー攻撃を受け，委員のメールがウィキリークスに掲載されるなどの事態が発生したことだった．このサイバー攻撃によって公開されたメールによって，本来中立的であるはずの民主党全国委員会がクリントンのライバル候補であったサンダースを落選させるよう働きかけていたことが分かり，既に本選への進出

31） Congressional Documents and Publications, *As U.S.-China Dialogue Begins, Rubio Urges Obama To Seek Change In Chinese Behavior*, Federal Information & News Dispatch; Lanham, 2015.

32） Ellen Nakashima, *U.S. developing sanctions against China over cyberthefts*, Washingtonpost, 2015, URL: https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html?utm_term=.f50b4aeeb00e（2018 年 12 月 20 日閲覧）

33） United States Government Accountability Office, op. cit., p.4

が事実上決まっていたヒラリークリントンのイメージダウンを狙い，クリントンと本選を戦うトランプを支援する目的があったのではないかと疑惑を受けた[34]．この他にも 10 月 1 日には国土安全保障省（DHS）が各州の投票関連システムが不正アクセスを受けたことが公表され，同じ 10 月にはウィキリークスにクリントンの選対責任者ジョン・ポデスタのメール内容が流出する事件も起きた．当時クリントンが否定的な態度を取っていた TPP を賞賛する内容が含まれていたことから，当選後には TPP 賛成に転ずるのではないかという疑いを抱かせるものだった．このように大統領選挙に関わるサイバー攻撃の事件が複数存在している状況下で，11 月 8 日に当初劣勢が予想されていたトランプが勝利すると，オバマ大統領は情報機関にレポートをまとめるよう指示した．オバマ大統領の要求に基づいて，トランプ政権が正式に発足するまでに 2 つのレポートが提出され，いずれもロシア政府に関与する組織の犯行だったと断定している[35]．その中でも 1 月 6 日 CIA，FBI，NSA の 3 つの情報機関が合同で分析したレポートでは，ロシア政府とプーチン大統領がトランプを支持する目的があったことを強調し，特にプーチン大統領がサイバー攻撃を命令していたことを断言する内容となっている[36]．

なお 1 月 6 日に公開された報告書は，秘密区分を除いたバージョンであるが，公開された部分に指摘されているロシア政府の関与を示す根拠は「状況証拠」による判断がほとんどであり，プーチン大統領主導だと判断した確実な証拠が提示されたとは言い難い．とはいえ，秘密区分を除いてまでこのようなレポートを公開したことは，オバマ大統領と情報機関からのロシア政府及びサイバー攻撃の成果を否定するトランプ次期大統領に対する強い政治的メッセージを含むものと見るべきであり，これ自体が「名指しでの非難」による制裁の一部だと考えられるだろう．

オバマ政権は 12 月 29 日にロシアに対する制裁措置を発表し，在米ロシア大使館に勤務していたロシアの情報機関職員 35 人の国外追放，情報収集関連の目的で使用されているロシア関連施設 2 か所の閉鎖，個人 2 人の米国内の資産凍結と米企業との取引禁止が盛り込まれていた．ロシアに対しては，北朝鮮と同様に既にウクライナ紛争を巡って制裁を発動しており，この制

34）無神論者とも言われるサンダースの信仰問題を取り上げる試みなどが記述されている．
Aaron Blake, *Here are the latest, most damaging things in the DNC's leaked emails*, Washington Post, July. 25, 2016.

35）FBI と DHS のレポートの中では．ロシアの情報機関と関連がある「APT28」及び「APT29」という 2 つのハッカー組織が．1 年間に渡って民主党全国委員会を標的に攻撃していたことが報告されている．FBI, DHS（2016）, *GRIZZLY STEPPE – Russian Malicious Cyber Activity*, URL: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf（2018 年 12 月 25 日閲覧）

36）Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution*, 2017, URL: https://www.dni.gov/files/documents/ICA_2017_01.pdf（2018 年 12 月 25 日閲覧）

裁も従来の制裁対象を拡大した追加制裁であり，大統領選挙への介入という個別事件の特性に加えて，元々米露関係においては制裁を発動しやすい措置があったと考えられる．

4．結　　論

以上の論考の結果，本論文の目的である「何故アメリカがオバマ政権の 2 期目において北朝鮮，中国，ロシアを対象にサイバー攻撃を理由とする制裁を発動するようになったか.」という問いに対して以下のように回答することが出来る．

まず，オバマ政権がコストを課す制裁の方針を明確化するようになった理由として挙げられるのが，オバマ政権の 1 期目の後半から 2 期目の初めの期間にあたる 2011 年から 2014 年の時期において，政権当初は重視されてきた拒否的抑止に対する信頼性が低下するデータの存在や，連邦政府の防衛システム構築コストの増加という問題が生じ，一方当初軽視されていた懲罰的抑止については最大の障害であったアトリビューション能力の改善が見られることが挙げられる．このような状況の変化によって，コストを課すことでサイバー攻撃を抑止する為，制裁を発動するインセンティブが政権内で拡大したことが考えられる．

もっとも，オバマ政権のサイバーセキュリティ戦略が変化して以降，非常に多数のサイバー攻撃がアメリカを標的に行われているが，その中で国家を標的とした制裁が発動されたのは本論文中で挙げたようにわずかな事例しか存在しない．この背景には，それぞれの事例において，各サイバー攻撃に対する制裁を発動させる誘因となる個別要因があるものと考えられる．

ソニーピクチャーズと関連する北朝鮮からのサイバー攻撃への制裁の場合，攻撃主体と攻撃手段，そして被害者の関連性からサイバー攻撃のアトリビューションが比較的明確であったことが最大の原因と考えられる．北朝鮮からのサイバー攻撃は，米韓を標的とする 2009 年の攻撃のように以前から行われていたと考えられるが，オバマ政権の戦略変化が生じた後もっともアトリビューションが容易な事例であった為，経済制裁の前例作りという側面があったことも考えられる．

ロシアへの制裁については，大統領選挙への介入という政治的正統性に関わる重大な事件だったことが他の事例と異なり，特に厳しい対応をアメリカ政府が取る原因になったと考えられる．それに加えて，大統領選介入へのロシアの関与に否定的だったトランプの態度を受けて，次期政権へのメッセージも対露制裁に含まれていたということも考えられる．

一方，対朝，対露制裁に比較すると，中国の場合には制裁対象となるサイバー攻撃自体は，必ずしも事例として特異なものであるわけではない．タイタンレインやオーロラ事件に見られる中国からの代表的なサイバー攻撃は，それぞれ知的財産の窃取や個人情報の流出といった一般的にみられる被害であり，中国への制裁は実際に発動されたのは 61398 部隊への法的措置のみであり，経済制裁はオバマ政権においては見送られたことも北朝鮮とロシアへの対応と異な

る点である．それにも関わらず限定的であるが，制裁が発動または検討された背景には，事例自体の特異性よりも中国という攻撃主体の性格が考慮されたと考えられる．中国は，将来的にアメリカの GDP を上回ることも予想される経済大国であり，軍事的にアメリカの競争者として台頭することが明確になりつつあった．中国からアメリカへのサイバー攻撃は，知的財産の窃取や F-35 に関する情報漏洩など，米中間の覇権競争に深刻な影響を及ぼす可能性があるものも含まれており，長期的，戦略的観点からこのような中国のサイバー攻撃を牽制する必要があったものと考えられる．一方で，中国への制裁が中途半端なものに終わった要因としては，北朝鮮やロシアと比較し，経済的相互依存が深い中国に対する経済制裁はアメリカ経済にとってもリスクとなり得る為，2015 年の段階では経済制裁が見送られることになったと推論される．この点については．実際にオバマ政権が米中サイバー交渉に際して，交渉が決裂した場合には，中国側への制裁を発動する意図が実際にあったか，中国に制裁を発動する意図を伝えていたのかなど，検証する要素が残されていることは留意する必要がある．

また，サイバー攻撃の総数に比して発動された制裁の事例は限られており，これらの事例の存在をもってアメリカのサイバー攻撃に対する制裁が，今後他の事例においても一般的に適用可能だと結論づけるには不十分である．ただし，オバマ政権 2 期目までは国家に対する制裁は，実際に深刻な被害をもたらすサイバー攻撃の存在が確認されていたにも拘わらず，1 つも行われていなかったことを考慮すれば，本論文で検証した政策変更の要因が実際の制裁発動に大きな影響を及ぼしたと考えられる．事例自体の希少性から，どのような事件が制裁の対象となるか一般化させることは現時点では困難であるが，本稿の考察から，アトリビューションの確実性，サイバー攻撃による被害の性質，制裁対象となる国家との関係性の 3 点が，特に制裁の有無を分けるものと推論される．

参 考 文 献

Department of Defense, *The Department of Defense Cyber Strategy*, 2015, URL:http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf（2018 年 12 月 25 日閲覧）

Department of Homeland Security, *Creation of the Department of Homeland Security*, URL: https://www.dhs.gov/creation-department-homeland-security（2018 年 12 月 20 日閲覧）

Department of Homeland Security, *Einstein*, URL: https://www.dhs.gov/einstein（2018 年 12 月 25 日閲覧）

Dorothy E. Denning, “Stuxnet: What Has Changed?”, *Future Internet* 2012, issue. 4, 2012, pp.672-687

Jason Healey, *A Fierce Domain: Conflict in Cyberspace,* Virginia; Cyber Conflict Studies Association, 2013, pp.152-164

James P. Farwell, Rafal Rohozinski, “Stuxnet and the Future of Cyber War”, *Survival*, Vol.53, No.1, 2011, pp.23-40