2012 年 10 月 25 日

サイバーセキュリティメモ 001

国際公共政策研究センター
主任研究員 益岡 竜介
masuoka@cipps.org

解説: 米国 「サイバー空間の国際戦略」[1]

1. はじめに

米国政府は、2011 年 5 月、サイバー空間の国際戦略、“International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”[2] を発表した。本稿ではその戦略について解説する。

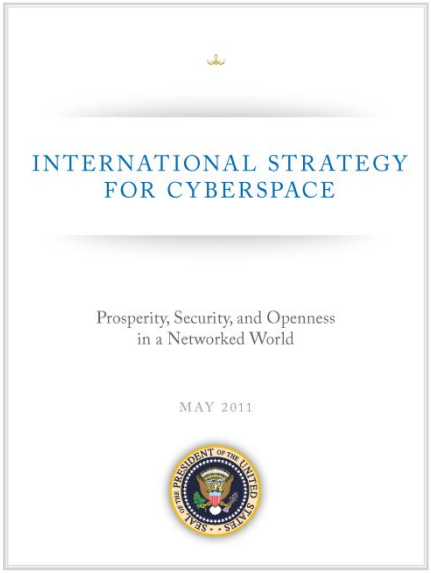

図 1「サイバー空間の国際戦略」の表紙

2. 背景および概要

米国オバマ政権が 2011 年 5 月に発表した米国初の包括的なサイバー空間の国際戦略の文書である。オバマ大統領は選挙戦のときからサイバーセキュリティをトッププライオリティと位置付け、大統領になるとすぐにCyber Security政策の 60 日間での見直しを指示したが、政権当初は経済、戦争、新型インフルエンザ、医療改革など課題山積で、またサイバーセキュリティ対策のコアとなるべき Cyber Security Coordinator が決まらず、前に進まないように見えた。しかし 2009 年 12 月には Howard A. Schmidt 氏が Cyber Security Coordinatorの役に任命され[3]、約 1 年半後のサイバー戦略の文書の発表に至った。

[1] 英文タイトル (English Title): On “U.S. International Strategy for Cyberspace”
[2] United States. (2011). U.S. International Strategy for Cyberspace.: http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace
[3] この時期までの米国のサイバーセキュリティへの取り組みは「米国連邦政府のサイバーセキュリティ政策を巡る動向」に詳しい。: http://www.ipa.go.jp/about/NYreport/201103.pdf

図 2 国際戦略発表の様子 (YouTube より)

この戦略の発表[4] では、オバマ大統領は出席しなかったが、政権で関係する閣僚など 7 名[5] が壇上に揃い、各人が各々の組織を代表する 立場から各国外交官、産業界、教育界、政府関係者を前に 40 分以上に亘ってこの戦略の重要性を説いた。 この模様はもちろんオンラインを通じても公開された。 この発表のホワイトハウスブログや YouTube ビデオのタイトルは “Launching the U.S. International Strategy for Cyberspace” であり、単に文書が完成したことを知らせるだけではなく、18 の省庁や政府機関が協力し、国内外の関係者との数え切れない協議を経て作られた戦略であること、また今後米国はサイバーセキュリティに対してこのような方針で取り組んでいく、という決意宣言の機会であることが分かる。

以下に発表におけるいくつかの注目すべき点を挙げる。 John Brenan国土安全保障及び対テロ担当大統領補佐官が「これは技術文書ではなく、政策文書であることを強調し、これが国際戦略を他から分かつものである」と述べた[6]。 確かに他国のサイバー (セキュリティ) 文書とは異なり、ビジョンや目指す未来が多くを占め、他方具体性はかなり乏しい。 この点については「3. 文書の性格」で詳述する。

John Brenan 氏の発言で興味深いのは、「国外からの来賓への (オバマ) 大統領のメッセージは非常に明確である。 より少ない危険で今と同じ恩恵をもたらすインターネットを希求するなら米国は味方である、安全、プライバシー、表現の自由を損なうことなくより多くの国がこれらの技術にアクセスできる世界を見たいなら、米国は味方である、...」などと高らかに謳い上げた後、「これらはアメリカの価値観ではなく、インターネット自身を定義するに至った価値観である」というものである。インターネットは科学技術ではあるが、一方で米国の価値観の体現でもある[7]。 インターネットの全世界的な広がりを“てこ“に、米国の価値観の押し付けではなく、普遍的な価値観として展開して行くことが、国際戦略の更に上にあるメタ戦略でないか、というのが戦略文書を読了後の著者の感想である。中国やロシア等の価値観とは必ずしも相容れないであろうが、価値観を同じくする仲間をなるべく増やし、囲い込んでいくと考えているのではないだろうか。

他の講演者も言及していたが、Hillary Clinton 国務長官はちょうどアラブの春があった頃でもあり、7 つの政策 (後述 p. 13 参照) の内、特に世界の活動家をサポートする「インターネットの自由」を強調していた。 しかし、英国の新聞 The Guardian はこの発表の翌日の記事 “US calls on its Nato partners to help resist cyber-attacks” において、「世界の活動家をサポートするとあるが、

[4] Launching the U.S. International Strategy for Cyberspace: http://www.youtube.com/watch?v=TcC_5axcWVo

[5] 壇上に立った順に、最初にオバマ大統領の代理として John Brenan 国土安全保障及び対テロ担当大統領補佐官、Hillary Clinton 国務長官、Eric Holder 司法長官、 Gary Locke 商務長官、Janet Napolitano 国土安全保障長官、William Lynn 国防副長官、そして最後を締めくくったのは Howard Schmidt サイバーセキュリティ担当調整官であった。

[6] “It is important to note that this is first and foremost a policy document, not a technical one. ..., and that's part of what sets the international strategy apart.”

[7] Richard Clarke 氏らによる「世界サイバー戦争」の p. 103, 特に「だから、現在でもインターネットの奥底には、当時の大学生の感受性と政治信条が息づいている。」はその点をうまく表現している。

一方で“法の支配”の必要性を述べ WikiLeaks のようなものは許さないという点で偽善である。」という内容の指摘をする。

この国際戦略発表の 2 ヵ月後 (2011 年 7 月) には、国防面での戦略を具体化する「サイバー空間作戦戦略」[8] が発表された。但し、John Brenan国土安全保障及び対テロ担当大統領補佐官がその前週に米国政権で初めて国会に送ったサイバーセキュリティ法案の提案について、時間のかなりの部分をかけて述べているが、現時点 (2012 年 10 月) で未だにサイバーセキュリティ法案は成立していない。サイバーセキュリティの緊急性を鑑み、大統領命令 (executive order) を出すことも検討されているが、大統領選前の微妙な状況の中、動きはない可能性が高く、大統領選が終わるまではサイバーセキュリティ対策も足踏みの状況が続きそうである。国際協力を謳う国際戦略ではあるが、その発表は Geneva で世界情報社会サミット (World Summit on the Information Society (WSIS)) が開かれている最中、Washington, D.C. で開かれ [9]、また最近 (2012 年 6 月) に至るまで国際戦略の趣旨に沿うと思われる国連のサイバーセキュリティ同盟であるInternational Multilateral Partnership Against Cyber Threats (IMPACT) にもコンタクトしていない [10]。対外的にはすぐには大きな進展は見られそうになく、むしろ米国の影響力に陰りが出始めているようにさえ見えていた。ただ 2012 年 10 月に Leon Panetta 国防長官のスピーチでサイバー先制攻撃の可能性、サイバー攻撃元特定技術の進展、サイバー空間での新たな交戦規定の決定が最終段階にあること、サイバー法成立への呼びかけ、サイバー空間での「判断ミス」を防ぐために互いに透明性を高める必要性など一歩踏み込んだ発言を行った [11]。これが今後どのような影響を持つかは引き続き見ていく必要がある。

国際戦略の文書は冒頭にホワイトハウス (オバマ大統領) からの 1 ページのカバーレターから始まる。サイバー空間が世界経済や開かれた政府の基盤であり、サイバーセキュリティは政府や社会の義務 (obligation) であり、未来に向けたビジョン (“vision for the future”) を他国とともに実現していくとある。続く本文は以下の三章と最後のまとめ章の「IV. これから (Moving Forward)」からなる。

I. サイバー空間政策を作る (Building Cyberspace Policy)
II. サイバー空間の未来 (Cyberspace’s Future)
III. 優先政策 (Policy Priorities)

第 I、第 II、第 IV 章は、理想主義的な論調で、革新に対して開かれていて、世界中相互運用性があり、人々の信頼を得るのに十分安全であり、人々の仕事を支えるのに十分な信頼性がある、サイバー空間の実現を目指すことが書かれている。その目指す世界に到達するための政策は

[8] Department of Defense Strategy for Operating in Cyberspace: http://www.defense.gov/news/d20110714cyber.pdf
[9] 国際戦略で WSIS の Tunis 合意を目標を説明する部分で引用しているにも関わらずにである。
[10] Westby, Jody. (June 4, 2012). Forbes.: http://www.forbes.com/sites/jodywestby/2012/06/04/u-s-administrations-reckless-cyber-policy-puts-nation-at-risk/
[11] Leon Panetta 国防長官のスピーチの米国防省による全文: http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136

第 III 章に示されているが、概念的であり、主に他国に向けての内容である。

「4. 防衛の方針」で詳しく解説するが、この国際戦略では軍事的にサイバーの脅威を他の脅威と同様に扱うとしている。 その一つの帰結として、サイバーの脅威に対しては、物理的、かつリアルな軍事力で対抗する可能性を明確にした。 日本のメディアではあまり取り上げられていないが、もう一つ重要な帰結は米国の軍事同盟国がサイバーの脅威を受けた際に、米国が物理的かつリアルな軍事力で対抗する可能性である。 即ち、「集団安全保障」がサイバーの脅威にも適用されるということである。 当然、米国の軍事同盟国である日本がサイバー攻撃にあった場合にも適用されると想定される。

国家レベルのサイバー攻撃ではなく、個人や犯罪組織によるサイバー犯罪に関してはサイバー犯罪条約に基づき、互いに協力していく方針である。 またサイバー犯罪の温床にならないこと、開かれた政府で安定した国になること、サイバー犯罪での協力ができること等のためにも、開発途上国等を中心に国際開発・協力を進めていく、としている。

以下、「米国サイバー空間の国際戦略」の文書から読み取れることを「3. 文書の性格」、「4. 防衛の方針」に、目標、国内の体制・組織、予算規模、国際連携、政策などメトリック項目について「5 その他」にそれぞれ記述する。「6. 文書の抄訳」にホワイトハウスからのレター全文の翻訳、および各章の概要を説明する。

3. 文書の性格

戦略の発表で John Brenan 国土安全保障及び対テロ担当大統領補佐官が述べたように、これは政策文書である。 しかし、他国のサイバーセキュリティに関する戦略文書 (英国 “UK Cyber Security Strategy”[12]、 豪州 “Australian Government Cyber Security Strategy”[13]、日本の「情報セキュリティ 2012」[14] 等) も政策文書の性格があるはずだが、それらとは全く性格を異にする。国際戦略の Fact Sheet にあるように「米国サイバー空間の国際戦略はサイバー空間の未来に対する我々のビジョンの概略を述べ、他国及びその人々とパートナーを組んでそのビジョンを実現するための重要課題を提示する」のであって、政策の具体的な要素は含んでいない。

タイトルでは他国のものとは (1) 米国のものは「サイバーセキュリティ」ではなく「サイバー空間」である、 (2) 米国のものには他国のものに入っていない「国際」 (“International”) が入っている、の 2 点で異なっているが、この文書を最も顕著に他から分かつのは (2) の点の方である。 (1) については確かに、技術革新や、開発途上国などにネットワーク技術を提供して世界のどこからでもアクセスできるようにするといった国際開発等セキュリティとは異なる面も含むが、やはりサイバーセキュリティに関連したことが文書の殆どを占め、その点で他国のものとさほど違わない。

米国の文書は他国の文書とは、その対象とする読者、目的などが全く異なり、それがタイトルの “International” に表れている。 他国のサイバー (セキュリティ) 戦略の文書が主に自国の国民に

[12] United Kingdom. (2011). UK Cyber Security Strategy.: http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf
[13] Australian Government. (2009). Australian Government Cyber Security Strategy.: http://www.ag.gov.au/Cybersecurity/Pages/
[14] 情報セキュリティ政策会議. (2012). 情報セキュリティ2012.: http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf

向け、政府のサイバーの課題に対する方針や対策を具体的に説明するのに対し、米国のものは国内よりむしろ全世界に向けて、「米国はこのようなビジョンでこのようにやっていく、仲間は同様に一緒にやっていこう」というメッセージ、あるいは宣言であるようだ。

オバマ大統領のカバーレターから始まり、本文も含め、文書全体に亘り、米国が尊重する価値観や原則である、表現や結社の自由といった基本的自由 (Fundamental Freedoms)、プライバシー (Privacy)、自由な情報の流れ (Free Flow of Information) を前面に押し出し、最後までこれらの原理原則に基づいて展開されている。そのため全体に具体性が非常に弱いのであるが、この文書の目的を考えるとメッセージ性を高めるためにも、敢えて具体的な「戦略」というより「ビジョン」や「想い」という色合いが濃く、理想主義的な論調にしているのだとも考えられる。 30 ページの文書の中で日和見的な部分として指摘できるのは、インターネット統治の部分で国際電気通信連合（ITU）を推す勢力を牽制し現状維持しようとしている部分とプライバシーに関するソーシャルメディア企業への配慮の部分くらいであった。

更に細かく文章を見ていくと、この文書の読者が誰なのか明確になってくる[15]。

サイバー空間あるいはインターネットに相当するフレーズが文脈によって 20 種類以上も現われる[16]。民間企業などに対して整合性のある用語を使い、技術的な正確さを期するよりも、文脈によってサイバー空間の役割を表現する方が大事と考えたのではないか。

第 II 章 サイバー空間の未来 (II. Cyberspace's Future) では、安全保障や国際関係論の分野などで使われる単語をそのまま使っていて、それらの単語の通常の意味だけでは解釈し難い部分が何箇所かある。

米国より前に 2009 年に発表された豪州のサイバーセキュリティ戦略の文書では国民に分かり易く政策、国内の組織・体制などを具体的に記述しているが、この米国の文書で政策が書かれている第 III 章は具体性が乏しく、例えば米国の政府の機関の名称が全く出てこず、一方で多国間機関の名称はかなり出てくる。政策の内容も他国への呼びかけの形が取られている。

まとめの第 IV 章では、「この戦略は米国政府機関にとってのロードマップ (roadmap) であり、民間部門、市民団体、一般ユーザに対する呼びかけ (call) でもあるが、最も大事な点は、これが他国やその人々への招待状 (invitation) である。」と述べているが、実際には国内や国外も含めた民間部門、市民団体、一般ユーザに対する呼びかけの部分は僅かである。 他国、それも外交官のような人々に向けたメッセージがこの文書の殆どを占め、その本質だと考えられる。

4. 防衛の方針

この国際戦略で指摘するのを忘れてならないのは、サイバーの脅威を他の脅威と同様に扱うとし

[15] 以下の分析は、故意にそのようにしたというより、そのままで良いとした点に意図が表れていると考えている。

[16] 厳密には意味に多少違いはあるが次のようにいろいろな種類の表現が使われている。: Internet, cyberspace, networked information systems, interconnected networks, networks, digital networks, computer networks, global networks, networked infrastructure, networked machines, networked systems, networked world, national and international networks, globally distributed network, interconnected networks, networks worldwide, globally interconnected networks, global networks, networked systems, network of networks, shared networks, information systems, communications infrastructure, networked information systems, International information infrastructures, networks and information infrastructures, communications systems, digital infrastructure, digital networks, digital systems

たことである。 (その一節の翻訳は p. 12 に記した。) その一つの帰結として、サイバーの脅威であっても、物理的、かつリアルな軍事力で対抗する可能性を明確にした。サイバー攻撃では攻撃者の特定が難しいが、一定の抑止力にはなるであろう。「**何に**対する**どんな脅威**に**どのような手段**で対抗する」可能性があるかが記述されているが、この帰結は「どんな脅威」という中に今回サイバーの脅威が入ったということである。 ちなみに「どのような手段」は全ての必要な手段であるが、具体的に外交的、軍事的、経済的な手段に加えてサイバー (informational) な手段も明記された。

上の帰結は日本のメディアや本などでは取り上げられていないようだが、サイバーの脅威を他の脅威と同様に扱うことにしたことは、もう一つの重要な帰結がある。 それは「何に」対してかであり、それは「自国、同盟国、友好国、国益」とされている。特に軍事同盟国については、明確に「サイバー空間を通じて行われるある種の敵対行為は軍事同盟国に対する我々の責任により、行動を起こすことを余儀なくされることがある」と書かれている [17]。 すなわち米国への脅威は勿論だが、軍事同盟国に対するサイバーの脅威に対しても、軍事力を含む全ての手段を採る可能性があるということであり、「集団安全保障」がサイバーの脅威にも適用される。 この一節にはなく、またこれより少し弱い文脈ではあるが、第 III 章の軍に関する優先政策の中に、NATO およびその諸国が同盟国として具体的に挙げられている。 挙げられてはいないが、米国と軍事同盟を結ぶ日本や韓国も軍事同盟国として対象であるのは明らかであろう。

サイバー攻撃があった時に米国に防衛してもらえるのは好都合かも知れないが、The Guardian の記事 [18] では、サイバー攻撃が常態化しつつある中、 NATO の一国に対するサイバー攻撃を NATO 全体に対する攻撃とみなすのは危険な展開であるかも知れないと指摘する。2007 年に NATO の同盟国であるエストニアが本格的なサイバー攻撃を受けたヨーロッパにとっては絵空事ではないのである。

5. その他

目標

目標は “Our Goal” として国際戦略の文書の p.8 に囲みの中に次の内容が与えられている。

> **我々の目標**
>
> 米国は世界経済のサポート、国際的安全保障の強化、表現の自由とイノベーションの促進を実現する、**開かれて、相互運用性があり、安全で、信頼性の高い**情報通信基盤を推進する努力を国際的に行っていく。そのために、**責任のある行動規範**が国の行動を導き、協力体制を維持し、サイバー空間の法の支配をサポートするような環境を築き、維持していく。

[17] メディア他で取り上げられなかったのは、この国際戦略のサマリーに相当する Fact Sheet からこの一文がすっぽり抜け落ちていたためもあると考えられる。 この一文がないと「同盟国、友好国、国益」の部分は何に対しても行動を起こせる権利を留保しておくために入れているだけのように取れたのではないかと推測する。 Fact Sheet: http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

[18] US calls on its Nato partners to help resist cyber-attacks. The Guardian. (May 17, 2011).: http://www.guardian.co.uk/technology/2011/may/17/us-nato-cyber-attacks-report

国際戦略を短く説明する Fact Sheet では、 目指すのは「革新に対して開かれていて、世界中相互運用性があり、人々の信頼を得るのに十分安全であり、人々の仕事を支えるのに十分な信頼性がある、サイバー空間」と表現をしている。

国内の体制・組織、予算規模など

この文書の性格から、このビジョンをどう実現していくかについての米国内の体制・組織、予算規模などの記述は特にない。 予算規模について、別のソース [19] の想定によると 2012 年度情報セキュリティ関連予算に 80 億ドルをかけている。

国際連携

国家によるサイバーの脅威については「4. 防衛の方針」で詳しく述べたように、自国、同盟国、友好国、国益を守るために、サイバーの脅威に対してどんな手段をも用いることを明確にした。 特に軍事同盟国へのサイバーの脅威であっても、米国がどんな手段をも用いる可能性を留保した。

但し、犯罪者や、国家ではない集団などからのサイバー攻撃に対してはサイバー犯罪条約 [20] に基づいて各国と協調して対処していくとする。

それ以外については、色々な地域・多国間・技術の場（フォーラム）を通じての国際的協力をしていくとする。 文書中に具体的にリストされている場（フォーラム）は以下のようなものがある。

- Organization of American States (OAS),
- Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF)
- Asia-Pacific Economic Cooperation Organization (APEC)
- Organization for Cooperation and Security in Europe (OSCE)
- African Union (AU)
- Organization for Economic Cooperation and Development (OECD)
- Group of Eight (G-8)
- European Union (EU)
- United Nations (UN)
- Council of Europe
- Internet Governance Forum
- Meridian Conference

[19] これでいいのか日本の情報セキュリティ予算---こんなに違う日米の予算規模:
http://itpro.nikkeibp.co.jp/article/COLUMN/20120327/388102/
[20] この条約は 2001 年に発行し、米国は 2006 年に批准している。Budapest Convention on Cybercrime:
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

政策

第 III 章の「優先政策 (Policy Priorities)」には以下のような 7 つの政策がリストされているが、どれも主に他国に向けたもので、また抽象的なものであり、米国内の具体的な政策等についての言及はない。

- 経済: 国際標準および革新をもたらす開かれた市場を推進する
- 我々のネットワークを守る: 安全、信頼性、回復力の向上
- 法執行: 協力と法の支配を拡げる
- 軍: 21 世紀の安全保障の課題に対して準備する
- インターネット統治: 効率的かつ包括的な枠組みの推進
- 国際開発: 能力、安全、繁栄を築く
- インターネットの自由: 基本的自由とプライバシーを支持する

6. 文書の抄訳

ホワイトハウスのカバーレター

サイバー空間とそれを可能にする技術によって、あらゆる国籍、人種、信仰、信条の人々が今までになかったレベルでやり取りし、協力し、繁栄することが可能になった。今日、米国の会社が世界中どこでもビジネスを行うことができ、そのことが数知れない職や機会を支えている。アフリカの田舎の母親が自分とは関係のない南アメリカの家族に手工芸品を売ることができ、アジアで作られた機器と北米で書かれたソフトを使いヨーロッパの研究所がその分野を変えるような研究を行い、オーストラリアと中東の学生がビデオ会議システムを通じ一緒に学ぶことができる。そして世界中の益々多くの市民が情報技術により、それぞれの政府がより開かれ、より迅速に対応するように仕向けるようになった。

今日、我々を取り囲むネットワークを国家や人々が活用するとき、我々には選択肢がある。我々はネットワークがもたらすであろうより大きな繁栄とセキュリティの可能性を引き出す努力をすることもできるし、ネットワークの進展を制約するような狭い利益やいわれのない恐怖に屈することもできる。サイバーセキュリティはそれ自身が目的ではない; そうではなく、イノベーションが確実に花開き、市場を活性化し、生活を向上させるために、政府や社会が進んで取り組むべき義務である。ネットワークの外での犯罪や攻撃による問題がデジタル世界にもたらされることになったが、我々は我々が大切にする原則、すなわち表現と結社の自由、プライバシー、そして情報の自由な流れに基づき立ち向かっていく。

デジタル世界はもはや無法のフロンティアでもないし、少数のエリートからなる町でもない。 それは国家や人々の、責任があり、公平で、平和な行動規範が根付き始めた場である。 社会、学術研究機関、民間部門や政府が一体となり民主的に効率的な管理を確保する努力をすることにより、

自己組織的に実現したコミュニティの素晴らしい一例である。最も重要なことは、このサイバー空間は、その始まりよりずっとそうであったように、繁栄、セキュリティ、そして許容を育て、発展させ、増進し続けるものである。このことこそが、国際的な環境の中でインターネットを特別のものとして際立たせるものであり、守ることが非常に重要となる理由である。

この精神に従って、私は米国のサイバー空間の国際戦略を発表する。私の政権は今までにも関連技術に関わる政策課題に取り組んできたが、サイバーの課題全般にわたって他国との関与にどう統一的にアプローチしていくかを提示するのは今回が初めてである。それゆえこの戦略は未来のサイバー空間に対するビジョンの概略を示すだけではなく、そのビジョンを実現するための計画も示す。我々の優先事項や、サイバー空間の特質を守り我々が直面する脅威を減ずるために如何に協力するかを、我々の国内外のパートナーが理解するための文脈を与えるものである。

インターネットだけでは国際的な協力の新たな時代をもたらし得ず、その取り組みは受益者たる我々にかかっている。 我々は共に、開かれ、相互利用可能で、安全かつ信頼性のあるサイバー空間の未来を築き上げることができる。これが我々の求めているサイバー空間の未来であり、すべての国家や人々にその実現のための活動への参加を呼び掛けるものである。

［Barrack Obama 大統領のサイン］

I. サイバー空間政策を作る (I. Building Cyberspace Policy)

この章は、報告書 “Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communication Infrastructure” の発表に当たってのオバマ大統領の 2009 年 5 月の演説[21]からの引用「我々はこのサイバー空間に依存しない日は一日たりともない。… サイバー空間は人類の歴史が始まって以来人類を互いにもっとも結びつけるようになった。」で始まる。この引用を受けておおよそ以下のように展開する。

> *情報化社会基盤 (digital infrastructure) は繁栄する経済、活気のある研究コミュニティ、強い軍隊、透明性の高い政府、そして自由な社会のバックボーンになり、生活のあらゆる面に入り込み、すぐに国家の重要な基盤になるであろう。このサイバー空間のもたらす利益を実現するためにはサイバー空間を信頼性が高く、安全にする必要がある。 そのため米国そして国際的な政策を刷新し、強化し、法による支配 (rule of law) を築かなくてはならない。*

そして戦略的なアプローチとして、

> *米国の国際サイバー空間政策の基礎は、サイバー空間は米国および世界に大きな可能性を秘めるという信念に基づく。 この 30 年に亘って、我々、米国はこれらの技術が我々の経*

[21] Remarks by the President on Securing Our Nation's Cyber Infrastructure. (May 29, 2009).: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

済に革命を起こし、日々の生活を変えていくのを見た。 サイバー空間外の搾取や攻撃などの問題がサイバー空間に入っていくのも見た。 我々がそれらの問題に対処するように変革していくとき、米国は自ら模範となり先導する。米国は、経済を活性化し、また国内外の生活を向上させるイノベーションを促進する国際サイバー空間政策を目指す。その際、米国の外交政策にだけではなく、インターネット自身の未来にとって本質的な原則に従う。

と指摘した後、以下の三つの戦略をあげている。

- 成功を基に進める (Building on Successes)
  米国は我々の社会や経済にサイバー空間の利益を保持し、更に高めることをコミットする
- 課題を認識する (Recognizing the Challenges)
  米国はサイバー空間の発展が米国及び、世界の国家や経済のセキュリティに対し新たな課題をもたらすことを認める.
- 原則に基づく (Grounded in Principle)
  米国はそれらの課題に立ち向かっていくが、同時にコアとなる原則を守っていく

原則 (Principles) としてあげられているのは、基本的自由 (Fundamental Freedoms)、プライバシー (Privacy)、自由な情報の流れ (Free Flow of Information) である。「基本的自由」と児童ポルノ、暴力の扇動、テロ行為の組織化など、「プライバシー」と法執行者が必要とする適切な捜査権限、「自由な情報の流れ」とサイバーセキュリティの確保、それぞれの原則に対しバランスを取らないとならないことがあるとは指摘するが、最後は「法の支配が … 米国の国家安全保障と我々の共通の価値を助長することを支える」と締めくくっている。

II. サイバー空間の未来 (II. Cyberspace's Future)

この章の前文ではまず、どこからでも簡単に、国境をも自由に越えて、自分の言語で情報を入手でき、個人でも企業でも誰でも簡単に online presence を安全に実現でき、世界中の技術者が協力してイノベーションを加速させ、サイバー犯罪があれば各国が協力して解決する … といった未来を描いてみせ、その実現には、各国が責任ある主体として協力し、規律を持ってあたっていく必要があると説く。

我々が希求する未来 (Future We Seek)

このセクションでは、この章の前文をまとめる形で、

我々が希求するサイバー空間環境は、イノベーションに報い、個人の自己実現を助ける; 人々をつなぎコミュニティを強化する; よりよい政府を築き、責任のある世界を広める; 基本的自由を担保し、個人のプライバシーを高める; 理解を築き、行動規範を明確にし、国内・国際的な

安全保障を強化するものである。

と述べ、その環境を維持するには国際協力が第一原則である、と述べた上で、「我々の目標」を囲いの中に以下のように示す。(元の文で太字になっている部分を同様に太字にした)。

我々の目標

米国は世界経済のサポート、国際的安全保障の強化、表現の自由とイノベーションの促進を実現する、**開かれて、相互運用性があり、安全で、信頼性の高い**情報通信基盤を推進する努力を国際的に行っていく。そのために、**責任のある行動規範**が国の行動を導き、協力体制を維持、サイバー空間の法の支配をサポートするような環境を築き、維持していく。

以下の通り、この目標に関して三点の説明を加えている。

1. "Open and Interoperable: A Cyberspace That Empowers" では、開かれて、相互運用性があることが、ネットワークの拡大を経済的に促進するだけでなく、世界情報社会サミット チュニスコミットメントで確認された原則である、自由な情報の流れにとっても重要なことが述べられる。
2. "Secure and Reliable: A Cyberspace That Endures" では、サイバー空間が持ちこたえていくためには、安全で、信頼性が高い必要があり、技術的な面だけでなく、経済的、政治的、社会的な面からも、脆弱性や世界スケールでのリスクを減らし、インシデントに対応するようにしていかないとならないという。
3. "Stability Through Norms" には、米国は同じ意見の国々と、安定を高め、国際的な行動が必要になったときの基礎を与えるべく、行動規範を築いていくとある。

サイバー空間の未来での我々の役割 (Our Role in Cyberspace's Future))

このセクションでは前セクションで述べた未来を実現し、前向きの規範を広げていくために米国は外交、防衛、そして開発を組み合わせて繁栄、安全、そして開放性を高めていくとする。その外交、防衛、開発のそれぞれについて更に詳しく説明している。

外交についての "Diplomacy: Strengthening Partnerships" では、目標を以下とする。

外交目標

米国は、各国が、開かれて、相互運用性があり、安全で、信頼性の高いサイバー空間の固有の価値を認める各国が責任ある利害関係者として一緒に努力し、行動する、そういった国際的な環境へ向けた動機付けを行い、その環境についてのコンセンサスを築いていく。

この目標のために、できるだけ広く、エンドユーザから多国間のフォーラムのレベルまで、また民間も含めていくとする。国家レベルに関しては意見を同じくする国の二国間や多国間での明確な

合意から始め、地域組織、そして国際的な組織に展開していくとある。

防衛についての “Defense: Dissuading and Deterring”[22] では、テロリスト、サイバー犯罪者、国家またその代理からのどこからの攻撃でも米国はそのネットワークを守るとし、目標を以下とする。

> **防衛目標**
> 米国は他国と共に、責任ある行動を助長する一方で、ネットワークやシステムを乱そうとするものには対抗していく。後者においては悪意を持ったものへ拒否的および懲罰的抑止を行うが、同時にこれら国家の重大な基盤を必要に応じまた適切に防衛する権利を留保する。

拒否的抑止では今までも進めてきた状況認識 (situational awareness) と緊急対応 (incident response) の防衛モデルを国内では公共・民間部門に渡って拡充し、国外においては他国を助けながら世界的に広げていくとある。

懲罰的抑止では、まず犯罪者や国家ではない組織がサイバー攻撃をしてきた際はサイバー犯罪条約 (Budapest Convention on Cybercrime) の枠組みで各国の法執行機関と協調して、捜査、逮捕、起訴などを進めていくとする。

国家からの場合は、米国はサイバー攻撃に対しても、物理的な戦争をその対抗手段としてとりうるとする。 この部分は重要なのでこの一節を全て以下に訳す。

> *正当であれば、米国はサイバー空間における敵対的な行為に対して、我が国に対する他の脅威と同様に対応する。すべての国家は固有の自衛権を持ち、またサイバー空間を通じて行われるある種の敵対行為は軍事同盟国に対する我々の責任により、行動を起こすことを余儀なくされることがある。自国、同盟国、友好国、国益を守るために、我々は外交的、サイバー、軍事的、そして経済的なものを含む全ての必要な手段を取る権利を留保する。 その際には，できる限り軍事力行使の前に全ての選択肢を使い切るようにし；行動のコストとリスクを行動しないことのコストに対し慎重に勘案し；できる限り幅広い国際的なサポートを得るように努めながら、我々の価値観を反映し、我々の正当性を強化するようなあり方で行動する。*

最初の一文にあるサイバーの脅威を他の脅威と同様に扱うということが主張で、残りはそれがどういう意味かを説明する。米国への脅威はもちろん、軍事同盟国に対するサイバーの脅威に対しても、また「自国の利益」を守るためでも、軍事力を含む全ての手段を採る可能性があることを意味する。

---

[22] 米国の安全保障戦略で Dissuasion (拒否的抑止) は「もし特定の行動をとったとしても、こちらの防御手段・損害限定能力の故に意味がないと認識させることで、特定の行動をとることを思いとどまらせる」ことで、Deterrence (懲罰的抑止) は「相手が恐れる報復措置や脅しによって、特定の行動をとることを思いとどまらせる」ことである。いわば Dissuasion は盾、Deterrence は矛に相当する。

開発についての“Development: Building Prosperity and Security”[23] では、目標を以下とする。

開発目標

米国は二国間あるいは多国間組織を通じて、他国におけるサイバーセキュリティ能力育成を促進し、各国が自らのデジタル基盤を守り、グローバルなネットワークを強化し、開かれ、相互運用性があり、安全で、信頼性のあるネットワークに対する合意における密接な協力関係を築くための手段を持つことができるようにする。

この目標に関して “Building Technical Capacity,” “Building Cybersecurity Capacity,” “Building Policy Relationships” といった段階的なアプローチを考えている。まずネットワークの基盤がない、あるいは、殆どない地域にネットワークをもたらす。これは主に民間部門の役割になるが米国政府はそれがやり易い環境を作る。勿論、米国がサポートするのは、情報の自由な流れを保障するなど米国の考えに沿ったプロジェクトである。

ネットワークがつながれば、サイバーセキュリティが必要で、特に開発途上国の国レベルのサイバーセキュリティを向上するのが短期・長期の利益であるとする。 サイバーセキュリティは各国がやるべきことであるが、米国は戦略、ネットワークセキュリティ、CERT の設立、国際的な法執行、防衛協力、民間・市民団体などの面で助けるとする。

それらのネットワークやサイバーセキュリティの能力育成から、徐々に経済、技術、法執行、防衛、外交などの互いの関心事における協力についての対話に移行し、また地域フォーラムや技術団体を通じてサイバーセキュリティ能力を開発する国々との関係推進を行っていくとある。

III. 優先政策 (III. Policy Priorities)

この文書で述べてきた、開かれて、相互運用性があり、安全で、信頼性の高いネットワークを築き、維持していくための活動を、「米国政府は、それぞれに国内外、民間部門との協力を求めていく 7 つの独立した活動領域に整理する」とあり、「ここで概要を示した優先政策が個々の活動を呼びかけ、導く」とある。

どの政策も概念的なもので、米国の具体的な政策などについての言及はなく、他国に対するメッセージの要素が大きい。 以下その 7 つの政策について紹介する。

経済: 国際標準および革新をもたらす開かれた市場を推進する (Economy: Promoting International Standards and Innovative, Open Markets)

サイバー空間が、我々の経済とイノベータたちを支え続けるために、この政策では以下の三点をあげている。

[23] ここでの“development”は国際関係論における“development theory”の“development”にあたり、一般的な「開発」でなく、他国の開発を意味する。

- どこからでも接続でき、世界中を結ぶネットワークに関する技術革新を促進する自由貿易環境を維持する (Sustain a free-trade environment that encourages technological innovation on accessible, globally linked networks)
- 企業秘密を含む知的財産権を窃盗から守る (Protect intellectual property, including commercial trade secrets, from theft)
- 技術専門家により決められる相互運用性があり、安全な技術標準を第一に優先することを確実にする (Ensure the primacy of interoperable and secure technical standards, determined by technical experts)

特に知的財産権については、「企業、大学、政府機関から今までにない量の情報が盗まれ、被害は何十億ドルになり得る。また、企業だけでなく国家へのインパクトはそれ以上であり、米国は犯罪者、外国企業、他国のそのような行為が違法で許されず、行為者に責任を取らせる国際環境を作っていくことを推進する」とある。

我々のネットワークを守る: 安全、信頼性、回復力の向上
(Protecting Our Networks: Enhancing Security, Reliability, and Resiliency)

強固なサイバーセキュリティが最も広く国家および経済の安全保障に重大な意味を持つことを理由として、この政策では以下の四点を挙げている。

- 二国間および各種の多国間の組織やパートナーシップにおいて、サイバー空間における協力、特に国家とサイバーセキュリティについての行動規範についての協力を推進していく (Promote cyberspace cooperation, particularly on norms of behavior for states and cybersecurity, bilaterally and in a range of multilateral organizations and multinational partnerships)
- 米国ネットワークへの侵入および妨害を減らす (Reduce intrusions into and disruptions of U.S. networks)
- 情報基盤のための、しっかりとしたインシデント管理、回復、原状復帰能力を確実にする (Ensure robust incident management, resiliency, and recovery capabilities for information infrastructure)
- 産業界と相談しながら、ハイテク製品のサプライチェーンの安全保障を向上する (Improve the security of the high-tech supply chain, in consultation with industry)

最初の項目で挙げている多国間組織やパートナーシップは具体的には (これらに限定せずに) 以下のものである。

- Organization of American States (OAS),
- Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF)

- Asia-Pacific Economic Cooperation Organization (APEC)
- Organization for Cooperation and Security in Europe (OSCE)
- African Union (AU)
- Organization for Economic Cooperation and Development (OECD)
- Group of Eight (G-8)
- European Union (EU)
- United Nations (UN)
- Council of Europe

こうした対話にまだあまり参加していない地域、特にアフリカや中東などへ広げていくのも歓迎であるとも述べている。

最後の項目は、他国のコンピュータチップやネットワークルーターなどの製品に最初から脆弱性を仕込まれる危険性に対するものである。

法執行: 協力と法の支配を拡げる
(Law Enforcement: Extending Collaboration and the Rule of Law)

サイバー空間への信頼を高め、ネットワークを不正利用するものを追い詰めるためとして、この政策では以下の四点をあげている。

- 国際的なサイバー犯罪政策の発展に全面的に関与する (Participate fully in international cybercrime policy development)
- ブタペストサイバー犯罪条約への加盟拡大を通じて、国際的にサイバー犯罪法を整合させていく (Harmonize cybercrime laws internationally by expanding accession to the Budapest Convention)
- サイバー犯罪法は、インターネットへのアクセスの制限ではなく、不正な活動と戦うことにフォーカスする (Focus cybercrime laws on combating illegal activities, not restricting access to the Internet)
- テロリストや犯罪組織がインターネットを使っての計画、資金調達、また攻撃ができないようにする (Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing, or attacks)

ブタペストサイバー犯罪条約が何回か言及されており、サイバー犯罪の国際的な面に対してはこのサイバー犯罪条約を中心に据えていくようである。

軍: 21 世紀の安全保障の課題に対して準備する
(Military: Preparing for 21st Century Security Challenges)

我々が我が市民、同盟国、そして利益を守る責任はそれらが脅かされうるどの場所にも及ぶとして、この政策では以下の三点をあげている。

- 信頼性が高く安全なネットワークに対する軍隊の増大する必要性を認識、適応する (Recognize and adapt to the military's increasing need for reliable and secure networks)
- サイバー空間の潜在的な脅威に立ち向かうため、軍事同盟を構築また既存のものを強化する (Build and enhance existing military alliances to confront potential threats in cyberspace)
- 集団安全保障を向上させるため、サイバー空間での同盟国やパートナーとの協力を拡大する (Expand cyberspace cooperation with allies and partners to increase collective security)

第 II 章の防衛目標の説明にもあるように、サイバー空間の脅威も通常の脅威と同様に捉え、集団安全保障の枠組みの中で対処し、今まで想定されていなかったサイバー空間の脅威に対する部分を強化していくとことと理解される。同盟国として具体的に挙げられているのは NATO だが、当然日本や韓国も含まれていると考えられる。

インターネット統治: 効率的かつ包括的な枠組みの推進
(Internet Governance: Promoting Effective and Inclusive Structures)

すべてのインターネットユーザの要望を効率的に満たすインターネット統治の枠組みを推進していくためにとして、この政策では以下の三点をあげている。

- インターネットにおける開放性とイノベーションを優先する (Prioritize openness and innovation on the Internet)
- ドメインネームシステム (DNS) を含む、世界的なネットワークの安全と安定を保持する (Preserve global network security and stability, including the domain name system (DNS))
- 各界関係者がインターネット統治の課題を議論する場を推進、強化していく (Promote and enhance multi-stakeholder venues for the discussion of Internet governance issues)

最初の項目ではインターネット統治の枠組みなどが変えられて、自由な情報の流れが妨げられることがあってはならないとしている。この政策は全体として、国連の組織である国際電気通信連合（ITU）の関与を強めたいというグループに対して、現状維持を推進していくことが感じられる。 最後の項目のインターネット統治の課題を議論する場の一つとして Internet Governance Forum (IGF) があげられている。

国際開発: 能力、安全、繁栄を築く

(International Development: Building Capacity, Security, and Prosperity)

ネットワーク技術の利益を全世界的に推進し、我々が共有するネットワークの信頼性を高め、サイバー空間における責任のある関係者のコミュニティを構築するためとして、この政策では以下の 4 点をあげている。

- 技術的またサイバーセキュリティ能力を築こうとする国へ必要な知識、トレーニング、その他のリソースを提供する (Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity)
- サイバーセキュリティのベストプラクティスを国際的に、継続的に発展させ、定期的に共有する (Continually develop and regularly share international cybersecurity best practices)
- 各国のサイバー犯罪と戦う能力を向上させる – 特に警察、科学捜査専門家、法律関係者、立法関係者らへのトレーニング (Enhance states' ability to fight cybercrime—including training for law enforcement, forensic specialists, jurists, and legislators)
- 政策立案者が関係を発展させ、専門家と対応する米国政府担当者の間の定期的かつ継続的な接触を提供して、技術的能力構築を推進する (Develop relationships with policymakers to enhance technical capacity building, providing regular and ongoing contact with experts and their United States Government counterparts)

インターネットの自由: 基本的自由とプライバシーを支持する

(Internet Freedom: Supporting Fundamental Freedoms and Privacy)

サイバー空間における基本的自由とプライバシーを守るために、この政策では以下の四点をあげている。

- 表現と結社の自由のための、信頼性があり、安全で安心なプラットフォームを実現することで、市民組織の活動家を支持する (Support civil society actors in achieving reliable, secure, and safe platforms for freedoms of expression and association)
- 市民組織や NPO と協力して、彼らのインターネット上の活動を違法なデジタルな侵入から守る手段を確立する (Collaborate with civil society and nongovernment organizations to establish safeguards protecting their Internet activity from unlawful digital intrusions)
- 企業データにおける効率的なプライバシー保護に向かって、国際的な協力を促進する (Encourage international cooperation for effective commercial data privacy protections)
- すべての人がアクセスできるインターネットの端から端までの相互運用性を確保する (Ensure the end-to-end interoperability of an Internet accessible to all)

第一、二、四項目は世界中の市民組織や NPOs などがサイバー空間上での表現や集会の自

由を確保することをサポートしていくということである。 第三項目はソーシャルメディアに集まりつつある個人データについてであると考えられ、「技術革新に必要な柔軟性を持たせながら」といったソーシャルメディア企業に配慮した表現もある。

The Guardian の 2011/5/17 の記事、“US calls on its Nato partners to help resist cyber-attacks”では、この国際戦略では世界の活動家をサポートしていくとあるが、一方で “法の支配” の必要性を述べて WikiLeaks のようなのは許さないという面で偽善であると指摘している。

IV. これから (IV. Moving Forward)

最後の章はこれまでを表現豊かにまとめる。「開かれて、相互運用性があり、安全で、信頼性の高いサイバー空間でなくてはならず、世界中多くの人が日常生活をサイバー空間に依存している。米国は想像力を掻き立て、次の大きな革新が起きるような世界の実現にコミットする」と最初の二つのパラグラフで述べている。

この章の最後のパラグラフでは、「この戦略は米国政府機関にとってのロードマップ (roadmap) で、民間部門、市民団体、一般ユーザに対する呼びかけ (call) でもあるが、最も大事な点は、これが他国やその人々への招待状 (invitation) である」と述べ、この文書の主たる読者が他国やその人々であることを明確にしている。

この招待状では我々のネットワーク化された世界において、繁栄、安全、開放性のビジョンを一緒に実現しようと誘い、最後の文では「これらの理想が、我々が知るサイバー空間を守り、また一緒に我々が希求する未来を創り出すのに中心的な役割を果たす」と呼びかけている。